バージョン7.2

ユーザーズガイド

株式会社 アールワークス

特記事項

株式会社 アールワークスは、本書を「そのまま」の状態で、明示的であると暗黙的であるとにかかわらず一切の保証なしで提供するものとします。ここでいう保証には、市場性や特定の目的に対する適合性を含みますが、それに限定されるものではありません。

株式会社 アールワークスは、本書をいつでも予告なしに変更することがあります。株式会社 アールワークスは、本書の内容が正確であるように細心の注意を払っていますが、本書に含まれている誤りについては一切の責任を負いません。また、本書を提供すること、本書の機能、本書を使うことに関連して発生する可能性のある直接の損害、間接の損害、特別の損害、偶発的な損害、結果的に起こる損害についても一切の責任を負いません。

ASTEC Eyes on the net バージョン 7.2
マニュアルバージョン 7.200

株式会社 アールワークス
〒103-0022 東京都中央区日本橋室町 4 丁目 3-18 東京建物室町ビル 3 階
FAX: 03-4496-4339　FAX: 03-5946-8400 (代表)

目次

3 章 ログ機能

4 章 レポート機能

5 章 キャプチャ機能

6 章　デコード機能

9章 フィルタエディタ

10 章 エキスパート機能

12 章　ホスト名の表示

13 章　その他の機能

はじめに

ASTEC Eyes on the net は、ネットワークのトラフィックを計測したり、ネットワークのパケットを収集して分析するためのネットワークアナライザです。 ASTEC Eyes on the net (これ以降 ASTEC Eyes と省略します) を使うことにより、ネットワークトラブルを未然に防いだり、起ってしまったトラブルを解決するための情報を得ることができます。

本書について

本書では、 ASTEC Eyes の機能について説明します。 ASTEC Eyes の主な機能としては、

- モニタ機能
- キャプチャ機能
- デコード機能
- ログ機能
- レポート機能
- リモート監視機能
- エキスパート機能
- トラフィックジェネレータ機能

があります。

まず、各機能を使う前の準備について説明します。次に、それぞれの機能について説明し、最後に、オプションの設定とその他の機能について説明します。

お使いの Windows のバージョンによって、画面の表示が本書のものとは異なることがあります。

表記について

本書では、以下の表記法を使います。

表記	意味
`computer text`	この文字列を示された通りにキーボードから入力します。たとえば `192.168.0.1` を入力します。 という指示は、文字どおり 192.168.0.1 と入力することを意味します。ファイル名、 ディレクトリ名、あるいは値を表わすためにもこの字体を使います。
italic text	適当な文字列を指定します。たとえば、 *savedir* にある `Setup.exe` をダブルクリックします。 は *savedir* の部分を実際のディレクトリ名で置き換えることを意味します。
強調	**強調**を強調します。
<Key>	キーボード上の対応するキーを押すことを意味します。
<Modifier-Key>	**<Modifier>** を押しながら **<Key>** を押すことを意味します。

また注意が必要な場所には次のような説明があります。

モニタの種類によっては、棒グラフ、円グラフを表示しないものもあります。

製品サポートについて

ご不明な点がございましたら、電子メールまたは FAX にて弊社サポートまでお問い合わせください。

電子メール: support@asteceyes.com
FAX: 03-4496-4339

1章

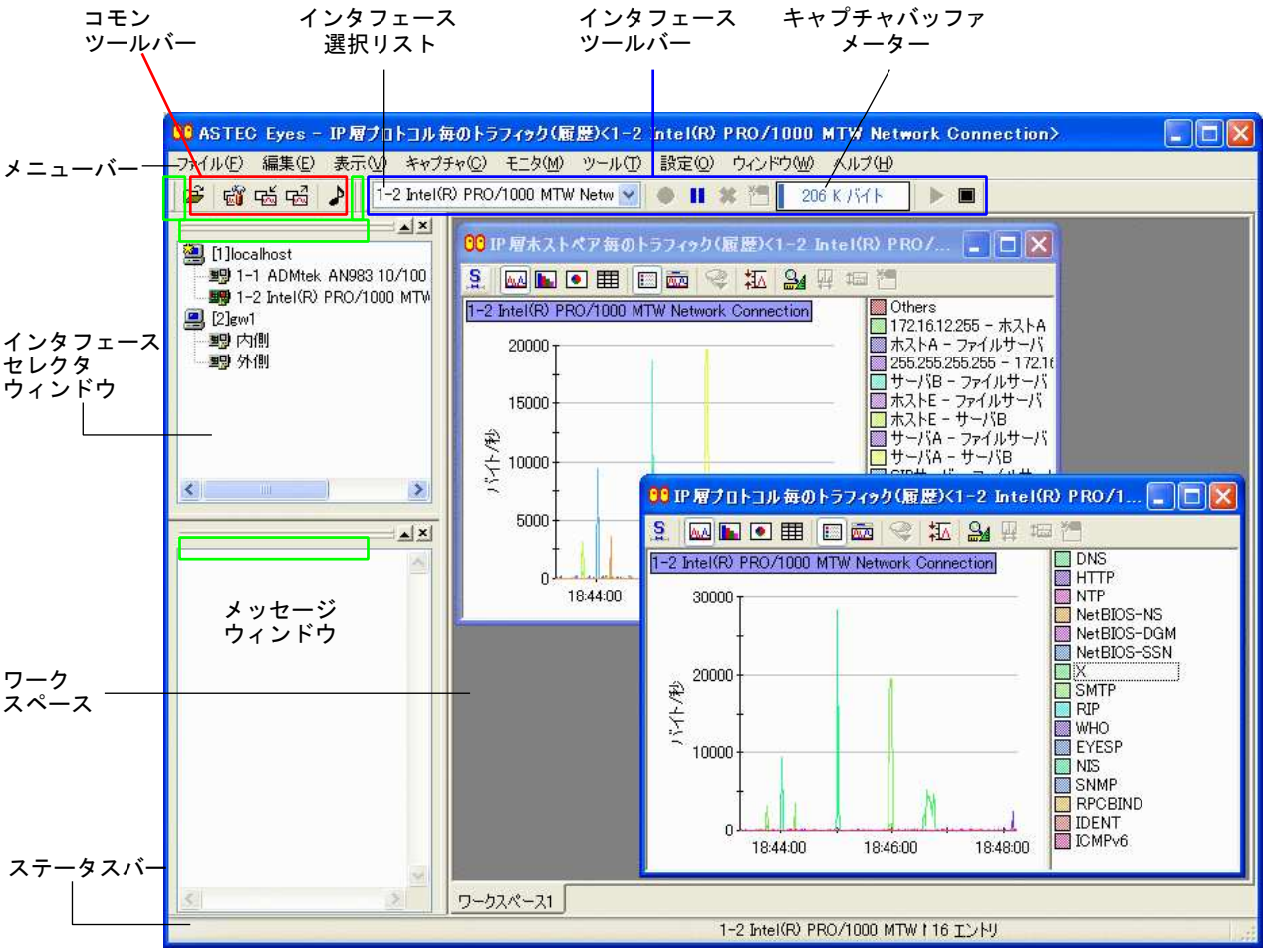
各機能を使う前の準備

ここでは、各機能について説明する前に、 ASTEC Eyes のメインウィンドウとネットワークインタフェースを選ぶ手順について説明します。

ASTEC Eyes の多くの操作はインタフェースごとに行います。 1 台の PC に複数のネットワークインタフェースカードがインストールされている場合には、どのネットワークについて操作を行うのか決めておく必要があります。

1.1 ASTEC Eyes のメインウィンドウ

図 1-1 に、 ASTEC Eyes のメインウィンドウを示します。メインウィンドウには、メニューバー、コモンツールバー、インタフェースツールバー、ステータスバー、ワークスペース、インタフェースセレクタウィンドウ、およびメッセージウィンドウがあります。



で囲まれている部分はグリップバーです

図 1-1: メインウィンドウ

コモンツールバー、インタフェースツールバー、ステータスバー、インタフェースセレクタウィンドウ、およびメッセージウィンドウは非表示にすることもできます。

コモンツールバー、インタフェースツールバー、インタフェースセレクタウィンドウ、およびメッセージウィンドウの表示と非表示を切り替える方法は 2 通りあります。

- ツールバーやウィンドウのグリップバーを右クリックすると、ポップアップメニューが現れます。ポップアップメニューから表示と非表示を切り替える対象を選びます。
- メインウィンドウの**表示(V)** メニューから表示と非表示を切り替える対象を選びます。

ステータスバーの表示と非表示を切り替えるには、メインウィンドウの**表示(V)** メニューから**ステータスバー(S)** を選びます。

1.1.1 ツールバー

ASTEC Eyes の操作には、ネットワークインタフェースに関係なく行う操作と、ネットワークインタフェースごとに行う操作があります。**コモンツールバー**には、選択中のインタフェースに依存しない操作を行うボタンがあります。 **インタフェースツールバー**には、選択中のインタフェースに対して操作を行うボタンがあります。

コモンツールバーおよびインタフェースツールバーはカスタマイズできます。それぞれのツールバーに、よく使う機能のボタンを追加したり、あまり使わない機能のボタンを削除できます。ツールバーをカスタマイズするには、次のいずれかの方法で「ツールバーの変更」ダイアログを開きます。

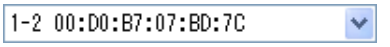
- メインウィンドウの**設定(O)** メニューから**コモンツールバーの設定(C)**. . . または**インタフェースツールバーの設定(I)**. . . を選びます。
- コモンツールバーを右クリックしてポップアップメニューを開き、**コモンツールバーの設定**. . . を選びます。
- インタフェースツールバーを右クリックしてポップアップメニューを開き、**インタフェースツールバーの設定**. . . を選びます。

次に、デフォルトでツールバーにあるボタンを示します。

表 1-1: デフォルトでコモンツールバーにあるボタン

ボタン	アイコン	機能
キャプチャデータを開く		ファイルに保存してあるキャプチャデータを開いてデコードし、デコードビューを表示します。
設定情報の読み込み		設定情報を読み込みます。
設定情報の保存		設定情報を保存します。
オプション設定		「オプション設定」ダイアログを開きます。
通話シミュレーション		「通話シミュレーション」ダイアログを開きます。 ASTEC Eyes *for* VoIP の機能です。

表 1-2: デフォルトでインタフェースツールバーにあるボタン

ボタン	アイコン	機能
キャプチャ開始		キャプチャを開始します。
キャプチャ停止		キャプチャを停止します。
キャプチャデータの削除		キャプチャバッファのデータを削除します。
デコードビュー作成		キャプチャバッファのデータをデコードしデコードビューを表示します。
モニタ開始		モニタを開始します。
モニタ停止		モニタを停止します。
インタフェース選択リスト		操作の対象とするインタフェースを選びます。

1.1.2 ステータスバー

メインウィンドウのステータスバーには、次のような情報が表示されます。

- ASTEC Eyes の状態
- アクティブなウィンドウのネットワークインタフェースのラベル
- トラフィックウィンドウに表示されているグラフアイテム数
- トラフィックウィンドウで選択中のグラフアイテムの名前
- トラフィックウィンドウのグラフから読み取った値
- ツールバーのボタンやメニューの簡単な説明
- IP 層アドレス帳の行数および選択中の行のアドレスと名前

- MAC 層アドレス帳の行数および選択中の行のアドレスと名前
- デコードビューのサマリ領域で選択中の行の行番号、フレーム ID、 IP アドレスまたは MAC アドレス、最上位のアプリケーション名
- ストリームビューのサマリ領域で選択中の行の行番号、ストリーム ID、 IP アドレス、最上位のアプリケーション名
- パケット編集ウィンドウのサマリ領域で選択中の行の行番号、フレーム ID、 IP アドレス、最上位のアプリケーション名
- デコードビューに表示されているパケットの総数
- ストリームビューに表示されているレコードの総数
- パケット編集ウィンドウに表示されているパケットの総数
- デコードビュー、ストリームビュー、パケット編集ウィンドウのダンプ領域で選択中のデータの位置と長さ

1.1.3 メッセージウィンドウ

メッセージウィンドウには、 ASTEC Eyes の重要なメッセージが表示されます。たとえば、トラフィックウィンドウから読み取った折れ線グラフの値やホスト名を検索中の IP アドレスなどを表示します。

メッセージウィンドウにフォーカスを移すには、メッセージウィンドウをマウスでクリックするか、 **<Alt-2>** キーを押します。

1.1.4 インタフェースセレクタウィンドウ

インタフェースセレクタウィンドウでは、インタフェースを選んだり、リモートモジュールと接続したり、インタフェースに関する操作や設定を行ったりすることができます。

インタフェースセレクタウィンドウにフォーカスを移すには、インタフェースセレクタウィンドウをマウスでクリックするか、 **<Alt-1>** キーを押します。

以下に、インタフェースセレクタウィンドウに現れるアイコンの一覧を示します。

表 1-3: インタフェースセレクタウィンドウに現れるエントリのアイコン

アイコン	説明
	設定権限のあるホスト
	設定権限のないホスト
	選択中のネットワークインタフェース (緑色)
	選択していないネットワークインタフェース (灰色)
	ログ
	ログまたは連続キャプチャデータのディレクトリ
	連続キャプチャデータ

インタフェースセレクタウィンドウに表示されるアイコンとそのラベルを合わせて、**エントリ**と呼びます。

リモートモジュールを使う方法やインタフェースの操作などについては、 8 章「リモート監視機能」 (188 ページ) を参照してください。

1.1.5 ワークスペース

ASTEC Eyes でウィンドウを開く操作をした場合、ダイアログ以外の新しいウィンドウは選択中のワークスペース上に現れます。ワークスペースは複数作ることができ、ウィンドウはワークスペース間を移動できるので、ワークスペースを使ってウィンドウを整理できます。また、ワークスペースに表示されているトラフィックウィンドウをレポートに出力できます。

ワークスペースにフォーカスを移すには、ワークスペースをマウスでクリックするか、または **<Alt-0>** キーを押します。

ワークスペースについては、「13.2 ワークスペース」 (347 ページ) を参照してください。

1.2 インタフェース

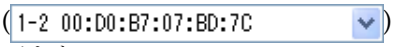
ASTEC Eyes でインタフェースとは、ホストにインストールしてあるネットワークインタフェースカード (NIC) を指します。

1 台のホストに複数のネットワークインタフェースカードをインストールしている場合は、モニタやキャプチャなどの操作を行う前に、対象とするインタフェースを選びます。

また、リモートモジュールを使う場合は、 ASTEC Eyes を起動したローカルな PC のインタフェースに加えて、リモートモジュールが動作しているホストのインタフェースも選択の対象となります。

1.2.1 インタフェースを選ぶ

インタフェースを選ぶ方法は 3 通りあります。

- メインウィンドウのインタフェースツールバーにあるインタフェース選択リスト () をクリックして、現れたインタフェースの一覧から選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリをマウスでクリックします。
- **<Alt-1>** キーを押してインタフェースセレクタウィンドウにフォーカスを移します。上下のカーソルキー (**<↑>** 、 **<↓>**) を押してフォーカスを移動し、 **<Enter>** キーを押します。

インタフェースセレクタウィンドウ内では、選んだインタフェースのアイコンが緑色 () に変わります。

ASTEC Eyes は、複数のインタフェースを同時にモニタまたはキャプチャできます。インタフェースを選んでからモニタまたはキャプチャの操作を繰り返してください。

1.2.2 インタフェースの情報を見る

インタフェースの状態や MAC アドレス、 NIC の情報などを見ることができます。これらインタフェースの情報は、「インタフェースのプロパティ」ダイアログに表示されます。「インタフェースのプロパティ」ダイアログを開くには、次のようにします。

1. インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックします。ポップアップメニューが現れます。
2. ポップアップメニューから**プロパティ(P)**... を選びます。

「インタフェースのプロパティ」ダイアログが現れます。

「インタフェースのプロパティ」ダイアログには、次の情報が表示されます。

- インタフェースのラベル
  ラベルは変更できます。ラベルを変更する方法については、「13.5.2　インタフェースのエントリのラベルを変える」 (356 ページ) を参照してください
- 状態
  ASTEC Eyes が把握しているインタフェースの状態を表示します。
  正常に動作しているときは、「有効」と表示されています。
  インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**インタフェースを無効にする(D)** を選んだ場合は「無効」と表示されます。
  エラーが起きたときには、ここにエラー情報が表示されます。
- MAC アドレス
- ベンダ ID
- 説明
  NIC の説明を表示します。
- 最大フレームサイズ
- リンクスピード
- プロミスキャスモードの状態
- リンクの検出
  インタフェースが使える状態かどうかを表示します。
- 検出可能なエラー
  NIC が CRC エラー、アライメントエラー、オーバーランエラーを検出できる場合、 ASTEC Eyes はそれらの統計情報を「MAC 層エラーフレーム数」のウィンドウに表示します。
  検出できるかどうかは、 NIC の仕様によります。

インタフェースツールバーをカスタマイズして「インタフェースのプロパティ」ダイアログを表示するボタン () を追加することもできます。カスタマイズの方法については、「1.1.1 ツールバー」 (6 ページ) を参照してください。

2章

モニタ機能

ネットワークの現在の状態を表示する機能です。

ASTEC Eyes は以下の情報 (モニタ情報と呼びます) を収集して、表示します。

- トラフィックの統計情報
- MAC アドレス
- IP アドレス
- TCP 接続の状態
- ホストのポートの状態

この章ではモニタ機能について説明します。

2.1 モニタの開始と停止

モニタの開始および停止は、ネットワークインタフェースごとに行います。

ネットワークのモニタを開始するには、

1. 対象となるネットワークインタフェースを選び、
2. モニタを開始し、
3. 見たい情報を表示するためのモニタウィンドウを開きます。

ネットワークのモニタを停止するには、

1. 対象となるネットワークインタフェースを選び、
2. モニタを停止します。

ネットワークインタフェースを選ぶ方法については、「1.2.1 インタフェースを選ぶ」 (10 ページ) を参照してください。

2.1.1 モニタを開始する

モニタを開始する方法は 3 通りあります。

- 対象とするインタフェースを選び、メインウィンドウのインタフェースツールバーの**モニタ開始**ボタン( ) をクリックします。
- 対象とするインタフェースを選び、メインウィンドウの**モニタ(M)** メニューから**モニタ開始(B)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタ開始(B)** を選びます。

2.1.2 モニタウィンドウを開く

モニタを開始しただけでは、モニタ情報は表示されません。モニタ情報を表示するためには、モニタウィンドウを開きます。モニタウィンドウを開く方法は 2 通りあります。

- 対象とするインタフェースを選び、メインウィンドウの**モニタ(M)** メニューから表示したいモニタ情報を選びます。

- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタウィンドウ(M)** をポイントし、表示したいモニタ情報を選びます。

モニタウィンドウは、選択中のワークスペース上に現れます。

2.1.3 モニタウィンドウの種類

ASTEC Eyes はモニタ情報を表示するモニタウィンドウとして、以下のウィンドウを用意しています。

- 13 種類のトラフィックを表示するトラフィックウィンドウ
  ネットワークに流れているパケットのトラフィックを計測し、その統計情報を表示するモニタウィンドウのことを、特に**トラフィックウィンドウ**と呼びます。
- MAC アドレス表
- IP アドレス表
- MAC アドレス - IP アドレス対応表
- 「TCP ステータス情報」のウィンドウ

それぞれのモニタウィンドウに表示する内容について、説明します。

「MAC 層トラフィック」のウィンドウ
MAC (Media Access Control) 層で計測したパケットの総量を表示します。

「MAC 層発信元毎のトラフィック」のウィンドウ
パケットを MAC 層の発信元で分類して表示します。

「MAC 層受信先毎のトラフィック」のウィンドウ
パケットを MAC 層の受信先で分類して表示します。

「MAC 層ホストペア毎のトラフィック」のウィンドウ
パケットを MAC 層の発信元と受信先の組み合わせ (ホストペア) で分類して表示します。

「MAC 層プロトコル毎のトラフィック」のウィンドウ
パケットを MAC 層のプロトコルで分類して表示します。

「IP 層トラフィック」のウィンドウ
IP (Internet Protocol) 層で計測したパケットの総量を表示します。

「IP 層発信元毎のトラフィック」のウィンドウ
パケットを IP 層の発信元で分類して表示します。

「IP 層受信先毎のトラフィック」のウィンドウ
パケットを IP 層の受信先で分類して表示します。

「IP 層ホストペア毎のトラフィック」のウィンドウ
パケットを IP 層の発信元と受信先の組み合わせ (ホストペア) で分類して表示します。

「IP 層プロトコル毎のトラフィック」のウィンドウ
パケットを IP 層のプロトコルで分類して表示します。

「MAC 層アドレスタイプ毎のトラフィック」のウィンドウ
パケットを MAC 層のアドレスタイプ (ユニキャスト、マルチキャスト、またはブロードキャスト) で分類して表示します。

「MAC 層サイズ毎のフレーム数」のウィンドウ
MAC 層のパケットの大きさで分類して表示します。

「MAC 層エラーフレーム数」のウィンドウ
エラーと判断されたパケットをエラーの種類によって分類して表示します。

MAC アドレス表 モニタ中に得られた MAC アドレスとベンダ名、ホスト名の一覧を表示します。

IP アドレス表 モニタ中に得られた IP アドレスとホスト名の一覧を表示します。

MAC アドレス - IP アドレス対応表
モニタ中に得られた MAC アドレスと IP アドレスの対応を表示します。

「TCP ステータス情報」のウィンドウ
TCP 接続の状態を表示します。

ホストのポートの状態は、「ポートの状態一覧」ダイアログに表示されます。詳しくは「2.9 ホストごとのポートの状態を表示する」 (46 ページ) を参照してください。

2.1.4 モニタを停止する

モニタを停止する方法は 3 通りあります。

- 対象とするインタフェースを選び、メインウィンドウのインタフェースツールバーの**モニタ停止**ボタン(▣) をクリックします。
- 対象とするインタフェースを選び、メインウィンドウの**モニタ(M)** メニューから**モニタ停止(U)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタ停止(T)** を選びます。

2.2 トラフィックウィンドウの表示をカスタマイズする

モニタウィンドウの中でも、特にネットワークのトラフィックの統計情報を表示する 13 種類のウィンドウのことを**トラフィックウィンドウ**と呼びます。

トラフィックの統計情報を目的に合わせて見やすく表示できるように、トラフィックウィンドウをカスタマイズできます。この節では、トラフィックウィンドウのカスタマイズについて説明します。

ASTEC Eyes は次に示す項目についてトラフィックウィンドウをカスタマイズできます。

- 凡例およびツールバーの表示、非表示を切り替える
- 表示形式
- Y 軸の単位
- Y 軸の範囲
- 棒グラフ、円グラフ、および表に表示するデータの範囲
- グラフの色
- タイムスパン

2.2.1 凡例およびツールバーの表示と非表示を切り替える

トラフィックウィンドウの構成を図 2-1 に示します。

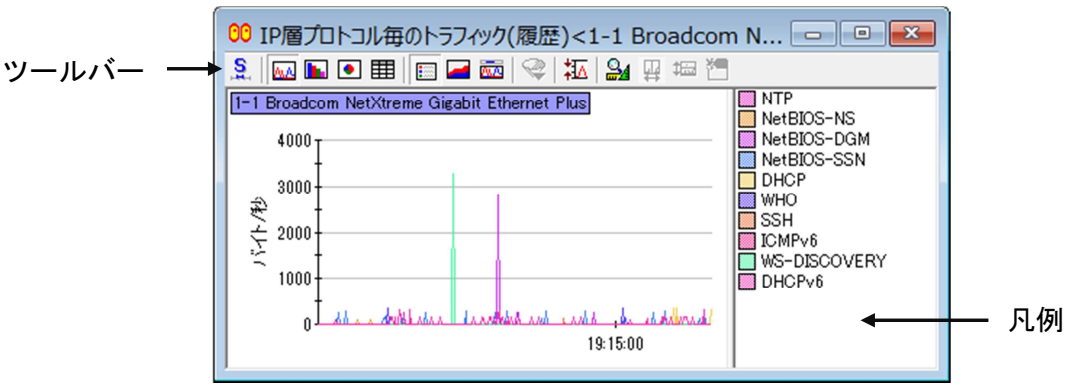


図 2-1: トラフィックウィンドウの構成

デフォルトの設定では、凡例もツールバーも表示されます。凡例やツールバーを非表示にできます。

凡例の表示、非表示を切り替えるには、トラフィックウィンドウのツールバーの**凡例**ボタン()をクリックするか、トラフィックウィンドウを右クリックしてポップアップメニューを開き、**凡例(G)** を選びます。

ツールバーの表示、非表示を切り替えるには、トラフィックウィンドウを右クリックしてポップアップメニューを開き、**ツールバーの表示(T)** を選びます。

2.2.2 表示形式

トラフィックウィンドウの初期状態は、折れ線グラフの形式です。統計情報を折れ線グラフ、棒グラフ、円グラフ、および表の形式で表示できます。

表示形式を切り替える方法は 2 通りあります。

- **トラフィックウィンドウのツールバーのボタンを使う**
  -  折れ線グラフに替わります。
  -  棒グラフに替わります。
  -  円グラフに替わります。
  -  表に替わります。
- **ポップアップメニューを使う**
  トラフィックウィンドウを右クリックしてポップアップメニューを開き、**表示形式(V)** をポイントし、表示形式を選びます。

「MAC 層トラフィック」のウィンドウ、「IP 層トラフィック」のウィンドウ、および「MAC 層エラーフレーム数」のウィンドウを円グラフ形式にすることはできません。

 ボタンで、折れ線グラフの表示を積み重ね形式にするかどうか指定できます。 積み重ね折れ線グラフにすると、それぞれのグラフアイテムに対応する領域が塗りつぶされ、境界は黒い線で区切られます。

2.2.3 Y 軸の単位

グラフの Y 軸の単位は、デフォルトでは**バイト数**です。 Y 軸の単位は、**フレーム数**または**使用率**に切り替えられます。

ポップアップメニューを使って Y 軸の単位を切り替える

トラフィックウィンドウを右クリックしてポップアップメニューを開き、**データの単位(U)** をポイントし、単位を選びます。

使用率(U) が選べるのは、「MAC 層トラフィック」のウィンドウだけです。

「グラフのプロパティ」ダイアログを使って Y 軸の単位を切り替える

1. トラフィックウィンドウを右クリックしてポップアップメニューを開き、**プロパティ(O)**. . . を選びます。
   「グラフのプロパティ」ダイアログが現れます。
2. **「グラフ」**のタブをクリックします。
   「グラフ」のページに切り替わります。そのようすを図 2-2 に示します。

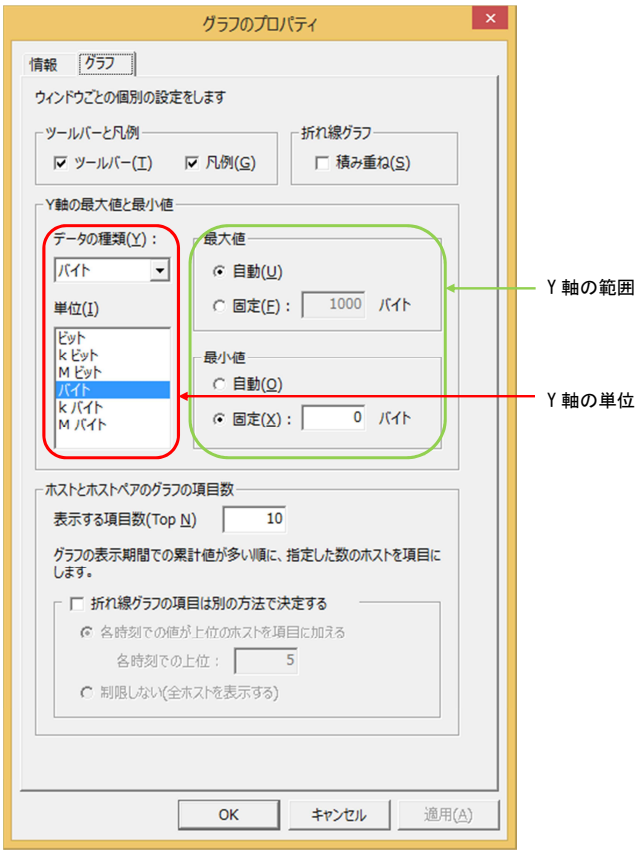


図 2-2: 「グラフのプロパティ」ダイアログ (「グラフ」のページ)

3. **データの種類(Y)** のドロップダウンリストボックスから、「バイト」または「フレーム」を選びます。
   選んだデータの種類によって、**単位(I)** のリストの内容が変わります。
4. **単位(I)** のリストから単位を選びます。
5. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

「グラフのプロパティ」ダイアログの「グラフ」のページで設定できる項目は、グラフのデフォルトのオプションの項目と同じです。ただし、設定した値はアクティブになっているトラフィックウィンドウだけに適用されます。

ネットワークの使用率を調べる

「MAC 層トラフィック」のウィンドウの Y 軸の単位を「使用率」にすると、ネットワークの使用率が分かります。

また、ネットワークのリンクスピードは「グラフのプロパティ」ダイアログの「情報」のページで見ることができます。「グラフのプロパティ」ダイアログを開くには、トラフィックウィンドウを右クリックしてポップアップメニューを開き、**プロパティ(O)**... を選びます。

ASTEC Eyes では、次の式でネットワークの使用率を算出しています。

$$\text{使用率}[\%] = \frac{(\text{データ量}[\text{バイト}/\text{秒}] + \text{パケット数}[1/\text{秒}] \times 24[\text{バイト}]) \times 8[\text{ビット}/\text{バイト}]}{\text{リンクスピード}[\text{ビット}/\text{秒}]} \times 100$$

24 という定数は、プリアンブル 8 バイト、 CRC 4 バイト、およびインターフレームギャップ 12 バイトを加えた値です。この式は、 10Mbps、 100Mbps および 1Gbps の Ethernet について成り立ちます。しかし、 IEEE 802.11b の無線 LAN などの場合、必ずしも本来の使用率を表すことができません。参考程度にご覧ください。

リモートモジュールが監視しているネットワークの場合、リンクスピードが分からないことがあります。そのような場合は、「リンクスピードの設定」ダイアログが現れ、リンクスピードをたずねます。リンクスピードが分からない場合は、システム管理者に問い合わせてください。

2.2.4 Y 軸の範囲

トラフィックウィンドウが折れ線グラフ形式または棒グラフ形式のとき、グラフに表示する Y 軸の範囲を指定できます。 Y 軸の範囲を指定する方法は 2 通りあります。

マウスのドラッグ操作で Y 軸の範囲を指定する

1. トラフィックウィンドウのツールバーの **Y 軸の範囲**ボタン() をクリックします。
2. マウスの左ボタンを押したまま上下に動かし、新しく設定する Y 軸の範囲を決めます。

Y 軸をグラフのデフォルトに戻すには、トラフィックウィンドウを右クリックしてポップアップメニューを開き、 **Y 軸を戻す(Y)** を選びます。

「グラフのプロパティ」ダイアログを使って Y 軸の範囲を指定する

1. トラフィックウィンドウを右クリックしてポップアップメニューを開き、**プロパティ(O)**. . . を選びます。
   「グラフのプロパティ」ダイアログが現れます。
2. **「グラフ」**のタブをクリックします。
   「グラフ」のページに切り替わります (図 2-2 参照)。
3. 最大値と最小値を指定します。

ASTEC Eyes をインストールした直後は、 Y 軸の範囲は最大値が**自動**で、最小値が**固定値 0** に設定されています。

グラフのデフォルトは、「オプション設定」ダイアログの「グラフ」のパネルで設定します。詳しくは、「11.7　グラフのオプションを設定する」 (300 ページ) を参照してください。

2.2.5　棒グラフ、円グラフ、および表に表示するデータの範囲

デフォルトでは、棒グラフ、円グラフ、および表に表示するデータの範囲は**タイムスパン内に計測した**値です。

データの範囲を**モニタを開始してから (もしくはモニタをリセットしてから) の全て**に切り替えられます。

データの範囲を切り替えるには、トラフィックウィンドウを右クリックしてポップアップメニューを開き、**データの範囲(R)** をポイントし、**累計値(T)** を選びます。

タイムスパン内のデータの表示に戻すには、**過去 *T* 間(R)** を選びます。

過去 *T* 間(R) の *T* はタイムスパンとタイムスパンの期間によって変わります。詳しくは、「2.2.7 タイムスパン」 (23 ページ) 、および「11.6　モニタのオプションを設定する」 (298 ページ) を参照してください。

2.2.6 グラフの色

トラフィックウィンドウの前景色 (グラフの目盛りと凡例の文字の色)、背景色、およびグラフアイテムの色を変更できます。グラフアイテムの色と背景色が似ていて見にくい場合など、どちらかの色を変えるとよいでしょう (グラフアイテムについては「2.3　グラフアイテム」 (24 ページ) を参照してください)。

背景色と前景色は、「オプション設定」ダイアログで変えます。

グラフアイテムの色を変える方法は 2 通りあります。

- 「オプション設定」ダイアログを使う
  「11.8　グラフの色のオプションを設定する」 (304 ページ) を参照してください。
- ポップアップメニューを使う

1. 色を変えたいグラフアイテムを選びます。グラフアイテムを選ぶ方法については、「2.3.1 グラフアイテムを選ぶ」 (24 ページ) を参照してください。
2. トラフィックウィンドウを右クリックしてポップアップメニューを開き、**色の設定(C)**... を選びます。
   図 2-3 のような、「色の設定」ダイアログが現れます。

図 2-3: 「色の設定」ダイアログ

3. 任意の色を指定して、 **OK** ボタンをクリックします。

2.2.7 タイムスパン

タイムスパンとは、トラフィックの統計情報の表示期間のことです。短期、中期、長期のタイムスパンを切り替えて表示できます。それぞれのタイムスパンの期間を設定できます。短期タイムスパンとして設定できる期間は 5 分から 30 分です。中期タイムスパンでは 1 時間から 6 時間です。長期タイムスパンでは 1 日から 6 日です。

タイムスパンごとに統計データを作る間隔 (統計の粒度) が異なります。より長期のタイムスパンほどデータの粒度は粗くなります。短期タイムスパンの場合は 1 秒ごとに、中期タイムスパンの場合は 10 秒ごとに、長期タイムスパンの場合は 5 分ごとに統計データを作成します。

タイムスパンを切り替える方法は 2 通りあります。

- トラフィックウィンドウのツールバーのタイムスパンのボタンをクリックします。**タイムスパン切り替え**ボタン()、**タイムスパン切り替え**ボタン()、および**タイムスパン切り替え**ボタン() があります。これらのボタンをクリックするたびに、 3 つのタイムスパンが切り替わります。
- トラフィックウィンドウを右クリックしてポップアップメニューを開き、**タイムスパン(P)** をポイントし、**短期(S)**、**中期(M)**、 または**長期(L)** を選びます。

タイムスパンの期間を長くすると、メモリの使用量が多くなります。

各タイムスパンの期間は、「オプション設定」ダイアログで設定します。詳しくは「11.6 モニタのオプションを設定する」 (298 ページ) を参照してください。

2.2.8 トラフィックウィンドウの表示形式を保存する

トラフィックウィンドウの表示形式を設定ファイルに保存しておけば、次に ASTEC Eyes を起動したとき、設定ファイルを読み込むだけで、トラフィックウィンドウを開いて同じ見た目にすることができます。設定ファイルに保存される設定情報は、次のとおりです。

- トラフィックの種類
- 表示形式 (折れ線グラフ、棒グラフ、円グラフ、表のいずれか)
- トラフィックウィンドウのジオメトリ
- 凡例の表示、非表示、および凡例の領域のサイズ
- タイムスパン (短期、中期、長期のいずれか)

詳しくは「11.11 設定情報を保存する」 (318 ページ) を参照してください。

2.3 グラフアイテム

折れ線グラフの場合、折れ線でトラフィックの推移を表します。棒グラフの場合は、棒の高低でトラフィックの合計を、円グラフの場合は、扇形でトラフィックの比率を表します。それぞれの、折れ線、棒、扇形の要素のことを**グラフアイテム**と呼びます。

2.3.1 グラフアイテムを選ぶ

次の操作を行うためには、着目するグラフアイテムを選んでおく必要があります。

- 特定のグラフアイテムだけを表示する
- 特定のグラフアイテムを隠す
- 特定のグラフアイテムの内訳を表示する
- グラフアイテムが表すホストの名前を検索する
- グラフアイテムの色を変える
- グラフアイテムが表すホストが開いているポートの一覧を表示する
- 選んだグラフアイテムを基にモニタフィルタの条件を自動生成する

グラフアイテムの表示、グラフアイテムを隠す、およびグラフアイテムが表すホスト名の検索については、複数のグラフアイテムを指定することができます。

グラフアイテムを選ぶ方法は 4 通りあります。

- グラフアイテムを直接クリックする
  選んだグラフアイテムが強調表示さます。 **<Ctrl>** キーを押しながらクリックすると複数のグラフアイテムを選べます。
  折れ線グラフのグラフアイテムを選ぶときは、折れ線の頂点付近をクリックしてください。
- 凡例の項目をクリックする
  グラフアイテムをクリックしにくい場合は、凡例に表示されている項目をクリックすることによって、グラフアイテムを選べます。 **<Ctrl>** キーを押しながら凡例に表示されている項目をクリックすれば、複数のグラフアイテムを選べます。選んだグラフアイテムの凡例の項目は反転します。
- **<↑>** キー と **<↓>** キーを使う
  <↑> キーまたは **<↓>** キーを押すと、選択したグラフアイテムが順に変わります。
  <Ctrl> キーを押しながら **<↑>** キーまたは **<↓>** キーでフォーカスを移動し **<Space>** キーで選択すると、複数のグラフアイテムを選べます。

- 表形式にして選ぶ
  トラフィックウィンドウのツールバーの**表 (詳細)** ボタン() をクリックして表形式に切り替え、選びたいグラフアイテムに対応する行をクリックします。 **<Ctrl>** キーを押しながらクリックすれば、複数のグラフアイテムを選べます。
  グラフアイテムが多い場合は、検索機能が使えるので便利です。

メインウィンドウのステータスバーに、選んだグラフアイテムの名前が表示されます。棒グラフ形式の場合は、名前に加えてバイト数またはフレーム数の合計も表示されます。円グラフ形式の場合は、名前と比率が表示されます。

複数のグラフアイテムを選んだときは、グラフアイテムの名前は表示されません。

グラフアイテムが何も選択されていない状態にするには、トラフィックウィンドウの何も表示されてない部分をクリックするか、 **<Ctrl-Space>** キーを押します。

2.3.2 トラフィックウィンドウに表示するグラフアイテムの数

折れ線グラフおよび棒グラフ形式では、トラフィックの種類によって、すべてのグラフアイテムを表示するものと、トラフィックの多い順に上位のグラフアイテムのみを表示するものがあります。

すべてのグラフアイテムを表示するトラフィック

- MAC 層プロトコル毎のトラフィック
- IP 層プロトコル毎のトラフィック
- MAC 層アドレスタイプ毎のトラフィック
- MAC 層サイズ毎のフレーム数
- MAC 層エラーフレーム数

上位 *N* 項目のグラフアイテムを表示するトラフィック

- MAC 層発信元毎のトラフィック
- MAC 層受信先毎のトラフィック
- MAC 層ホストペア毎のトラフィック
- IP 層発信元毎のトラフィック
- IP 層受信先毎のトラフィック
- IP 層ホストペア毎のトラフィック

上位のグラフアイテムのみを表示するトラフィックのグラフアイテム数 (*N*) は、グラフの表示形式によって、次のようになります。

- 折れ線グラフ形式の場合
  折れ線グラフの場合、設定によって 2 種類の表示ができます。
  1 番目の表示方法では、トラフィックの表示期間中 (タイムスパン) の累計値が、上位 *N* 項目に含まれているグラフアイテムを表示します。 *N* のデフォルト値は 10 です。
  2 番目の表示方法では、統計データを作成した時点 (グラフのプロット点) で上位 *N* 項目に含まれていたグラフアイテムを表示します。 *N* のデフォルト値は 5 です。グラフアイテムの表示数を制限せず常にすべてのホストを表示させることもできます。
  いずれの表示方法でも、トラフィックの表示期間中に一度も上位 *N* 項目に入らなかったグラフアイテムについては、 `Others` というグラフアイテムにまとめて表示されます。
- 棒グラフ形式の場合
  上位 *N* 項目に含まれているグラフアイテムを表示します。トラフィックウィンドウのタイトルには「TopN」が付きます。 *N* のデフォルト値は 10 です。
- 円グラフ形式の場合
  上位 *N* 項目に含まれているグラフアイテムを表示します。 *N* のデフォルト値は 10 です。

N はグラフのデフォルトのオプション、または「グラフのプロパティ」ダイアログの「グラフ」のページで設定できます。
グラフのデフォルトのオプションについては、「11.7　グラフのオプションを設定する」 (300 ページ) を参照してください。
タイムスパンについては、「2.2.7　タイムスパン」 (23 ページ) を参照してください。

2.3.3　表形式のグラフアイテム

表形式のトラフィックウィンドウでは、 1 行がグラフアイテム 1 つに対応します。

表は次のカラムから構成されています。それぞれのカラムの見出しをクリックすると、カラムの内容に従って行を並べ替えることができます。

- トラフィックの種類
- タイムスパン内の 1 秒あたりのバイト数の平均値
- タイムスパン内のバイト数の合計値
- タイムスパン内の 1 秒あたりのフレーム数の平均値
- タイムスパン内のフレーム数の合計値

特定のグラフアイテムを見つけたい場合などは文字列を検索できます。 検索するには、メインウィンドウの**編集(E)** メニューから**検索(F)** を選ぶか、 **<Ctrl-F>** キーを押します。 「検索」ダイアログが現れるので、探したい文字列を入力して**次を検索(F)** ボタンをクリックします。

検索する文字列に正規表現を使うこともできます。正規表現を指定する場合は、**正規表現(E)** にチェックを付けます。正規表現については、「6.8.2　正規表現を用いた検索」 (147 ページ)を参照してください。

タイムスパンとは、トラフィックの統計情報を表示する期間のことです。タイムスパンの期間は変更できます。詳しくは、「2.2.7　タイムスパン」 (23 ページ)、および「11.6　モニタのオプションを設定する」 (298 ページ) を参照してください。

2.3.4 「MAC 層トラフィック」のウィンドウのグラフアイテム

「MAC 層トラフィック」のウィンドウには、 MAC 層で計測したパケットの総量の 1 秒当たりの平均値を折れ線グラフで、 MAC 層で計測したパケットの累計値を棒グラフで表示します。

一般に、折れ線グラフ形式のトラフィックウィンドウには、ヒストグラムとしての値を表示しています。ログなどプロット間隔が長くなると、ある瞬間のピーク値 (最大値) の情報は失われてしまいます。ネットワークを監視するためにピーク値が必要になることがあります。

そのため、次の条件を満たす「MAC 層トラフィック」のウィンドウには、ヒストグラムの各区間内のピーク値も表示します。

- 中期と長期のタイムスパン、またはログを表示しているとき
- Y 軸の単位がバイト数または使用率のとき

短期タイムスパンでは、ピーク値のグラフアイテムは表示されません。

図 2-4 に、中期タイムスパンに切り替えた「MAC 層トラフィック」のウィンドウを示します。平均値を表すグラフアイテムは赤色の実線で、ピーク値を表すグラフアイテムは薄紫色の破線で表示します。

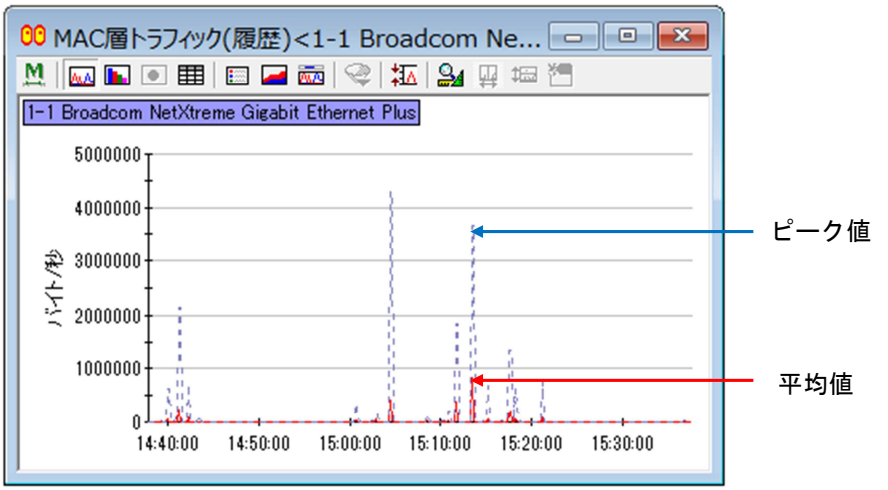


図 2-4: 「MAC 層トラフィック」のウィンドウ

単位を使用率にした場合のピーク値は、「使用率の最大値」ではなく、「バイト数が最大値」になった時点の使用率を表しています。

2.3.5 Unknown TCP Protocol、Unknown UDP Protocol、Unknown Protocol

TCP または UDP の上位層のプロトコルには、プロキシサーバーの設定によって Well known ポートとは異なるポートを使っているプロトコルや、 Well known ポートを持たないプロトコルがあります。

それらのプロトコルのグラフアイテムは「IP 層プロトコル毎のトラフィック」のウィンドウでは「Unknown TCP Protocol」または「Unknown UDP Protocol」と表示されます。

正しいプロトコル名で表示するためには、デコードヒントを設定します。デコードヒントを設定する手順については、「11.3　デコードヒントを設定する」 (289 ページ) を参照してください。

「Unknown Protocol」は、 IPv4 ヘッダーの Protocol フィールドの値または IPv6 ヘッダーの Next Header フィールドの値が ASTEC Eyes に登録されていないパケットが流れたときに、「MAC 層プロトコル毎のトラフィック」のウィンドウに現れます。

2.4 内訳を見る

一つのグラフアイテムに着目して、その内訳を見ることができます。

内訳を見るには、次のようにします。

1. グラフアイテムを選びます。
2. トラフィックウィンドウを右クリックしてポップアップメニューを開き、**内訳(D)** をポイントし、内訳の種類を選びます。
   内訳の種類には、次のようなものがあります。

   発信元毎(S) 選択中のグラフアイテムの内訳を発信元毎に分類して表示します。

   受信先毎 D) 選択中のグラフアイテムの内訳を受信先毎に分類して表示します。

   ホストペア毎(H) 選択中のグラフアイテムの内訳をホストペア毎に分類して表示します。

   プロトコル毎(P) 選択中のグラフアイテムの内訳をプロトコル毎に分類して表示します。

   トラフィックウィンドウは内訳を表示したグラフに切り替わります。

内訳の種類を選ぶときに、**<Shift>** キーを押しながら選ぶと、新たに内訳を表示したトラフィックウィンドウが現れます。

2.5 折れ線グラフの値を読み取る

折れ線グラフの X 軸の時刻や Y 軸の値、また特定のグラフアイテムのプロット点の値を読み取ることができます。グラフの値を読み取るには、次のようにします。

1. トラフィックウィンドウのツールバーの**グラフ解析機能**ボタン() をクリックします。
   グラフの更新が止まり、グラフの値を読み取る状態になります。グラフの値を読み取る状態になると、次のことができなくなります。
   - ポップアップメニューを開くことができません。
     そのため、特定のグラフアイテムの内訳を表示したり、表示のカスタマイズができなくなります。
   - ツールバーにあるいくつかのボタンが押せなくなります。
     グラフの値を読み取る状態で押せるボタンは、次の通りです。
     - **凡例**ボタン()
     - **キャプチャデータインディケータ**ボタン()
     - **グラフ解析機能**ボタン()
     - **垂直カーソル**ボタン()
     - **水平カーソル**ボタン()
     - **デコードビュー**ボタン()
   - グラフアイテムを複数選ぶことはできません。

グラフアイテムを複数選んでいるときには、**グラフ解析機能**ボタン() をクリックできません。

2. **垂直カーソル**ボタン() または**水平カーソル**ボタン() をクリックします。
   マウスカーソルが十字カーソルに変わります。
   水平カーソルボタン() をクリックしたときは、水平方向の破線が現れます。これを**水平カーソル**と呼びます。
   水平カーソルが表示されたトラフィックウィンドウを図 2-5 に示します。

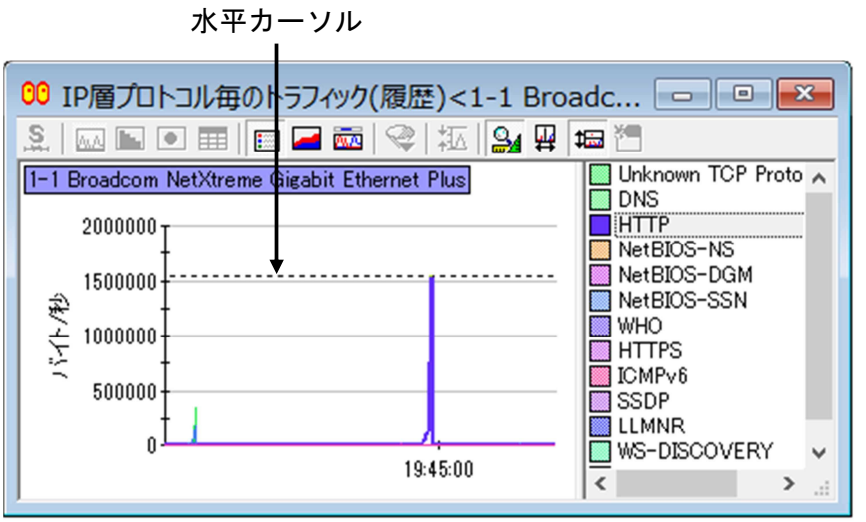


図 2-5: 水平カーソルの現れたトラフィックウィンドウ

マウスを上下に動かすと、水平カーソルの位置の値がステータスバーに表示されます。
垂直カーソルボタン(🖽) をクリックしたときは、垂直方向の破線が現れます。これを**垂直カーソル**と呼びます。
垂直カーソルが表示されたトラフィックウィンドウを図 2-6 に示します。

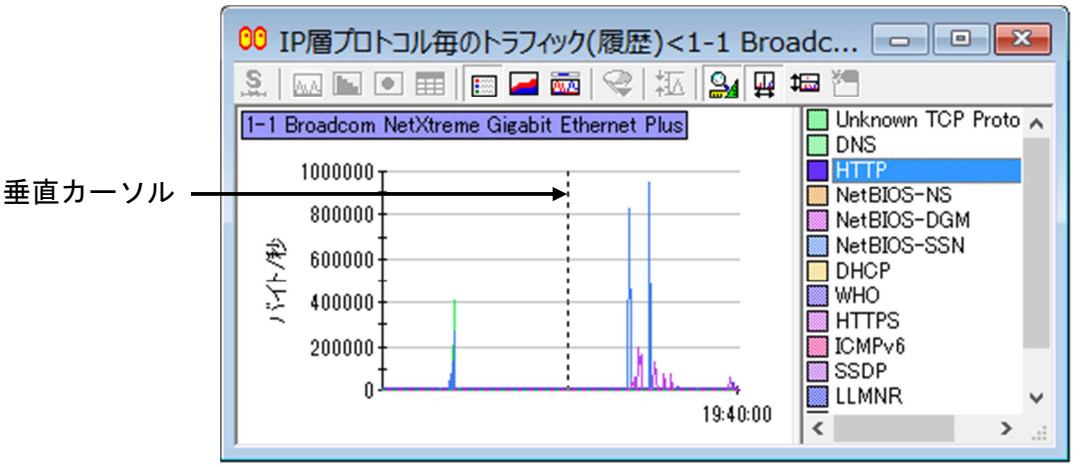


図 2-6: 垂直カーソルの現れたトラフィックウィンドウ

マウスを左右に動かすと、垂直カーソルの位置の時刻がステータスバーに表示されます。グラフアイテムを選んでいるときは、垂直カーソルが示す時刻に対応するグラフアイテムの値の位置に水平カーソルが現れ、時刻と値 (バイトまたはフレーム数) がステータスバーに表示されます。そのようすを図 2-7 に示します。

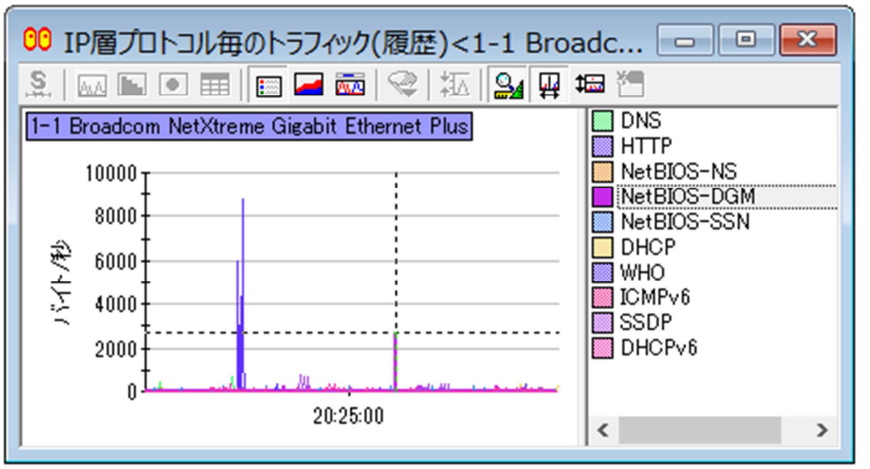


図 2-7: グラフアイテムを選んでいるときの垂直カーソルと水平カーソル

3. 値を読み取りたい位置でマウスの左ボタンをクリックするか、読み取りたい範囲をドラッグ操作で指定します。
   クリックすると、クリックした位置に実線が表示され、その位置の値を読み取ります。ドラッグすると、ドラッグした範囲が反転表示され、その範囲の値を読み取ります。読み取った値はメッセージウィンドウに表示されます。

読み取る値は、垂直カーソルを選んでいるのか水平カーソルを選んでいるのか、また、グラフアイテムを選んでいるのかどうかによって異なります。表 2-1 に垂直カーソルを選んでいるときに読み取る値を、表 2-2 に水平カーソルを選んでいるときに読み取る値を示します。

表 2-1: 垂直カーソルを選んでいるときに読み取る値

	マウスをクリック	マウスをドラッグ
グラフアイテムを選んでいないとき	垂直カーソルの位置の時刻	ドラッグの始点および終点の時刻 ドラッグの始点から終点までの時間
グラフアイテムを選んでいるとき	グラフアイテム名 垂直カーソルの位置の時刻 グラフアイテムの値	グラフアイテム名 ドラッグの始点の時刻 ドラッグの始点から終点までの時間 ドラッグの始点から終点までのグラフアイテムの値の累計値、最大値、最小値、平均値

表 2-2: 水平カーソルを選んでいるときに読み取る値

	マウスをクリック	マウスをドラッグ
グラフアイテムを選んでいないとき	水平カーソルの位置の値	ドラッグの始点および終点の値 ドラッグの始点の値と終点の値の差分
グラフアイテムを選んでいるとき	グラフアイテム名 水平カーソルの位置のグラフアイテムの値、およびその値をプロットしたすべての時刻	グラフアイテム名 ドラッグの始点および終点の値 ドラッグの始点の値と終点の値の差分

グラフの値を読み取る状態から、グラフの更新を行う状態に戻るには、もう一度**グラフ解析機能**ボタン() をクリックします。
グラフの値を読み取る状態になっている間、グラフの値を読み取るためにグラフの更新は止まりますが、モニタは続いています。グラフの更新を行う状態に戻すと、一度にグラフが更新されます。

読み取る点または範囲を解除するには、別の点または範囲を指定するか、右クリックします。

グラフの値はキー操作でも読み取ることができます。詳しいキーバインドについては、「B.3.4 モニタウィンドウのキーバインド」 (400 ページ) を参照してください。

2.5.1 グラフの値を読み取る状態でグラフアイテムを選ぶ

グラフの値を読み取る状態で、グラフアイテムを選ぶには、 **<Alt>** キーを押しながら、目的のグラフアイテムをクリックします。

凡例を表示している場合は、グラフの更新を行う状態と同じように、対応する項目をクリックして選択できます。

2.5.2 垂直カーソルおよび水平カーソルの動き

垂直カーソルは、マウスを左右に動かすと滑らかに左右に移動します。

水平カーソルの動きは、グラフアイテムを選んでいるかどうかで異なります。グラフアイテムを選んでいないときは、マウスを上下に動かすと滑らかに上下に移動します。グラフアイテムを選んでいるときは、プロット点から点へ上下に移動し、プロット点のない位置にカーソルを合わせることはできません。

2.5.3 値を読み取りやすいようにグラフを拡大する

小さく値が変動しているようなグラフの場合、目的の場所のグラフを拡大すると便利です。

グラフを拡大するには、 **<Shift>** キーを押しながら、マウスの左ボタンを押し下げ、斜め下または斜め上にドラッグして、拡大する範囲を指定します。マウスの左ボタンを放すと選んだ範囲だけを表示するようにグラフが拡大されます。

拡大を解除するには、 **<Shift>** キーを押したまま、右クリックします。

グラフの値を読み取る状態からグラフの更新を行う状態に戻ると、自動的に拡大は解除されます。

2.6 モニタフィルタを使う

特定の条件に合致するトラフィックだけを見たいことがあります。そのような場合、モニタフィルタを使って、モニタするパケットを絞り込むことができます。

たとえば、折れ線グラフ表示において、タイムスパン内に一度も上位 *N* 項目に入らなかったために、 `Others` にまとめられてしまったトラフィックを表示したい場合などは、 モニタフィルタを使うと良いでしょう。

統計情報はすべて収集し、表示するときに指定されたモニタフィルタの条件に合うものだけを表示します。そのため、統計情報は失われません。複数のモニタフィルタを用意しておき、何度でも適用するモニタフィルタを替えて、さまざまな角度からトラフィックを分析できます。

ASTEC Eyes のモニタフィルタは、 MAC アドレスと IP アドレスの対応関係を使って、MAC 層と IP 層のトラフィックの対応付けを行っています。 MAC アドレスと IP アドレスの対応がパケットの往路と復路で異なるトラフィックを計測した場合、 MAC 層と IP 層の間の統計データの整合性が保てなくなります。モニタフィルタとして設定する条件によっては、トラフィックの表示が不正確になることがあります。

2.6.1 モニタフィルタを用意する

モニタフィルタは最大 250 個まで作ることができます。それぞれのモニタフィルタの条件は、フィルタエディタで設定します。

フィルタエディタを起動するには、メインウィンドウの**編集(E)** メニューから**フィルタエディタ(E)**... を選ぶか、 **<Ctrl-E>** キーを押します。

フィルタエディタでは、論理式を編集してモニタフィルタの条件を設定します。ただし、トラフィックウィンドウに表示されているグラフアイテムであれば、ドラッグアンドドロップ操作やポップアップメニューを使って、そのグラフアイテムを特定する論理式を生成できます。

フィルタエディタでモニタフィルタの条件を設定する方法については、 9 章「フィルタエディタ」 (195 ページ) を参照してください。

グラフアイテムを特定する論理式を自動的に生成する方法については、「2.6.4　モニタフィルタを自動的に生成する」 (38 ページ) を参照してください。

2.6.2 モニタフィルタを適用する

モニタフィルタはネットワークインタフェースごとに適用されます。たとえば、1 つのネットワークをモニタするために、3 つのトラフィックウィンドウを表示している場合、モニタフィルタを適用すると、3 つのトラフィックウィンドウは、モニタフィルタで指定した条件に合致するトラフィックだけを表示するようになります。

用意したモニタフィルタを適用する方法は 4 通りあります。

- メインウィンドウのメニューを使う
  1. モニタフィルタを適用したいインタフェースを選びます。
  2. メインウィンドウの**モニタ(M)** メニューから**モニタフィルタ(F)** を選びます。
     サブメニューが現れます。サブメニューの項目は、用意されているモニタフィルタ名の一覧です。
  3. サブメニューから適用したいフィルタを選びます。
- インタフェースセレクタウィンドウを使う
  インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタフィルタ(F)** をポイントし、適用したいフィルタを選びます。
- トラフィックウィンドウのツールバーを使う
  1. トラフィックウィンドウのツールバーの**モニタフィルタ**ボタン() をクリックします。
     メニューが現れます。メニューの項目は、用意されているモニタフィルタ名の一覧です。
  2. 適用したいフィルタを選びます。
- トラフィックウィンドウのポップアップメニューを使う
  トラフィックウィンドウを右クリックしてポップアップメニューを開き、**モニタフィルタ(F)** をポイントし、適用したいフィルタを選びます。

モニタフィルタを適用すると、フィルタ名がトラフィックウィンドウのタイトルおよびインタフェースセレクタウィンドウのインタフェースのラベルの横に表示されます。

定義されているモニタフィルタが 11 個以上ある場合、現れるメニューに**候補リスト(T)**... というメニュー項目があります。**候補リスト(T)**... を選ぶと、「候補リスト」ダイアログが現れます。「候補リスト」ダイアログには定義されているすべてのモニタフィルタが表示されます。

モニタフィルタを適用しても、次のモニタウィンドウは影響を受けません。

- 「MAC 層サイズ毎のフレーム数」のウィンドウ
- 「MAC 層エラーフレーム数」のウィンドウ
- IP アドレス表
- MAC アドレス表
- MAC アドレス - IP アドレス対応表
- 「TCP ステータス情報」のウィンドウ

モニタフィルタを適用しているときに、適用しているモニタフィルタの条件を変えることはできません。モニタフィルタの条件を変えたいときは、新しい条件を設定したモニタフィルタを用意し、それを適用してください。

2.6.3 モニタフィルタを解除する

適用したモニタフィルタを解除する方法は 4 通りあります。

- メインウィンドウのメニューを使う
  1. モニタフィルタを解除したいインタフェースを選びます。
  2. メインウィンドウの**モニタ(M)** メニューから**モニタフィルタ(F)** を選びます。
  3. サブメニューから**フィルタ解除(R)** を選びます。
- インタフェースセレクタウィンドウを使う
  インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタフィルタ(F)** をポイントし、**フィルタ解除(R)** を選びます。
- トラフィックウィンドウのツールバーを使う
  1. トラフィックウィンドウのツールバーの**モニタフィルタ**ボタン() をクリックします。
  2. 現れたメニューから**フィルタ解除(R)** を選びます。
- トラフィックウィンドウのポップアップメニューを使う
  トラフィックウィンドウを右クリックしてポップアップメニューを開き、**モニタフィルタ(F)** をポイントし、**フィルタ解除(R)** を選びます。

フィルタ解除(R) を選ぶ代わりに、別のモニタフィルタを選んだ場合は、先に適用されていたモニタフィルタが自動的に解除され、新しく選んだモニタフィルタが適用されます。

2.6.4 モニタフィルタを自動的に生成する

限られた条件であれば、論理式を入力せずにモニタフィルタを使うことができます。マウス操作だけで、トラフィックウィンドウで選んだグラフアイテムを特定する論理式を生成できます。

次のトラフィックウィンドウから使うことができます。

- MAC 層発信元毎のトラフィック
- MAC 層受信先毎のトラフィック
- MAC 層ホストペア毎のトラフィック
- MAC 層プロトコル毎のトラフィック
- IP 層発信元毎のトラフィック
- IP 層受信先毎のトラフィック
- IP 層ホストペア毎のトラフィック
- IP 層プロトコル毎のトラフィック
- MAC 層アドレスタイプ毎のトラフィック

上記以外のトラフィックウィンドウのグラフアイテムを基に生成される条件論理式 は、モニタフィルタでは使えない条件論理式です。そのため、ドラッグしたり、ポップアップメニューから選んだりできないようになっています。

ドラッグアンドドロップを使う方法とポップアップメニューを使う方法があります。

ドラッグアンドドロップを使う

フィルタエディタを起動しておき、トラフィックウィンドウのグラフアイテムをドラッグし、フィルタエディタ内のモニタフィルタの条件グループ上にドロップします。生成された論理式をさらに編集することもできます。

生成される論理式は、ドラッグしたグラフアイテムによって異なります。詳しくは「9.6.1 トラフィックウィンドウから自動生成できる論理式」 (225 ページ) の表 9-3を参照してください。

ポップアップメニューを使う

トラフィックウィンドウのグラフアイテムまたは凡例の項目を右クリックしてポップアップメニューを開き、**フィルタの生成(I)** をポイントします。**一時的に生成して適用する(I)** または**フィルタエディタに送る(F)** をポイントし、フィルタの条件を選びます。

一時的に生成して適用する(I) をポイントしたか、**フィルタエディタに送る(F)** をポイントしたかによって、 ASTEC Eyes の動作が変わります。

一時的に生成して適用する(I) をポイントした場合

モニタフィルタの条件となる論理式が生成され、選択中のインタフェースに適用されます。フィルタエディタは現れません。また、生成された論理式を保存したり、変更することもできません。トラフィックウィンドウのタイトルおよびインタフェースセレクタウィンドウのインタフェースのラベルに、「一時モニタフィルタ」と表示されます。

フィルタエディタに送る(F) をポイントした場合

論理式が生成され、生成された論理式が追加された状態のフィルタエディタが現れます。ここからは手作業で論理式を編集する場合とまったく同じです。

生成される論理式は、選んだグラフアイテムによって異なります。詳しくは「9.6.1　トラフィックウィンドウから自動生成できる論理式」 (225 ページ) の表 9-3を参照してください。

複数のグラフアイテムを選択しているときには、モニタフィルタを自動的に生成する操作は行えません。

2.7 MACアドレス表とIPアドレス表

モニタ中に流れたパケットから得られた MAC アドレスと IP アドレス、および MAC アドレスと IP アドレスの対応を表示できます。 IP アドレスと MAC アドレスはインタフェースごとに管理されます。

MAC アドレスの一覧表には、収集されたすべての MAC アドレスが表示されます。 MAC アドレス、ベンダ名、ホスト名の 3 つのカラムがあります。ホスト名のカラムには、パケットをキャプチャしてデコードした結果から得られたもの、またはユーザーが定義したものが表示されます。

IP アドレスの一覧表には、収集されたすべての IP アドレスが表示されます。 IP アドレスとホスト名の 2 つのカラムがあります。ホスト名のカラムには次に示す方法で得られたホスト名が表示されます。

- モニタ中に見つかったもの
- ログに記録されていたもの
- ホスト名の検索によって見つかったもの
- パケットをキャプチャしてデコードした結果から得られたもの
- ユーザーが定義したもの

MAC アドレスと IP アドレスの対応表には、 MAC アドレスと IP アドレスの対応が取れているものだけを表示します。 MAC アドレス、ベンダ名、 IP アドレス、ホスト名の 4 つのカラムがあります。ホスト名のカラムには、 IP アドレスの一覧表と同じものが表示されます。

それぞれの表を表示するモニタウィンドウを開く方法は 2 通りあります。

- メインウィンドウのメニューを使う
  インタフェースを選び、メインウィンドウの**モニタ(M)** メニューから **MAC アドレス表(M)**、 **IP アドレス表(I)**、または **MAC アドレス - IP アドレス対応表(T)** を選びます。
- インタフェースセレクタウィンドウを使う
  インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタウィンドウ(M)** をポイントし、 **MAC アドレス表(M)**、 **IP アドレス表(I)**、 または **MAC アドレス - IP アドレス対応表(T)** を選びます。

カラムの見出しをクリックすると、カラムの内容に従って、行を並べ替えることができます。一度クリックすると降順に並び、もう一度クリックすると昇順に並びます。クリックした見出しのカラムの値が、複数の行にわたって同じ値になるときは、一つにまとめて表示します。

たとえば、一つの MAC アドレスに複数の IP アドレスが対応しているとき、 MAC アドレスの内容に従って並べ替えると、図 2-8 のような表示になります。

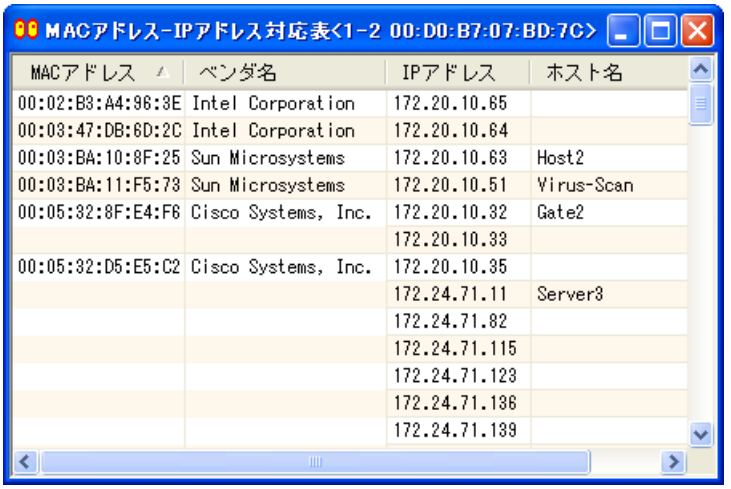


図 2-8: MAC アドレスの内容で並べ替えた MAC アドレス - IP アドレス対応表

モニタを開始しないと MAC アドレス表、 IP アドレス表、および MAC アドレス - IP アドレス対応表 には何も表示されません。

MAC アドレス表、 IP アドレス表、 MAC アドレス - IP アドレス対応表 では、文字列を検索できます。検索するには、メインウィンドウの**編集(E)** メニューから**検索(F)** を選ぶか、 **<Ctrl-F>** キーを押します。 「検索」ダイアログが現れるので、探したい文字列を入力して**次を検索(F)** ボタンをクリックします。
検索する文字列に正規表現を使うこともできます。正規表現を指定する場合は、**正規表現(E)** にチェックを付けます。正規表現については、「6.8.2　正規表現を用いた検索」 (147 ページ)を参照してください。

2.8 TCP のステータス情報を見る

通常、 TCP 接続は 3-way handshake と呼ばれるパケットのやり取りで確立します。データの転送が終了した場合は、 FIN パケットを送り、受信先が ACK を送り返すことを双方向に行うことで接続は終了します。

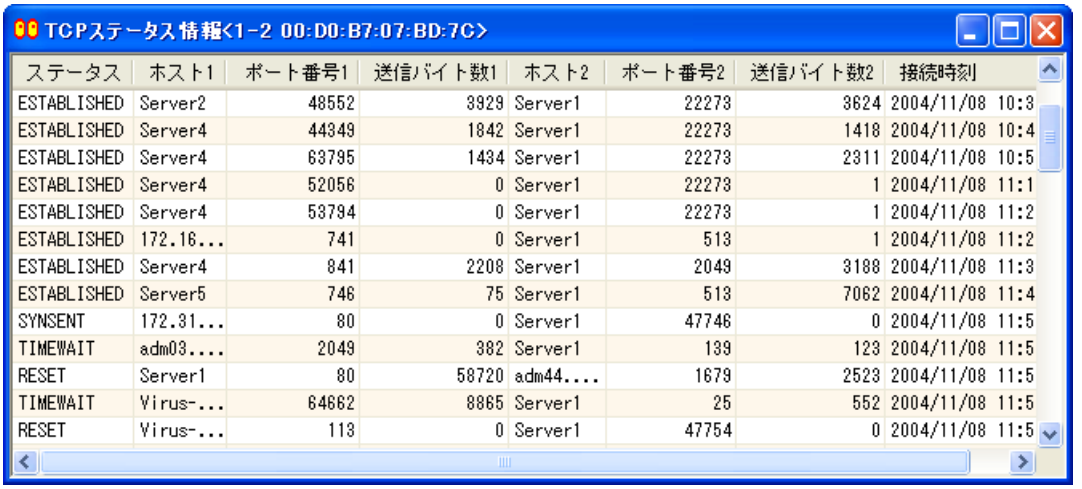
TCP ヘッダーの Sequence Number フィールドの値や Acknowledgement Number フィールドの値、 Flags フィールドの値をモニタすることで、 TCP 接続の状態がわかります。 ASTEC Eyes は、モニタによって得られた TCP 接続の状態を「TCP ステータス情報」のウィンドウに表示します。

2.8.1 「TCP ステータス情報」のウィンドウを表示する

「TCP ステータス情報」のウィンドウを表示する方法は 2 通りあります。

- メインウィンドウのメニューを使う
  インタフェースを選び、メインウィンドウの**モニタ(M)** メニューから **TCP ステータス情報(P)** を選びます。
- インタフェースセレクタウィンドウを使う
  インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタウィンドウ(M)** をポイントし、 **TCP ステータス情報(P)** を選びます。

図 2-9 に示すような「TCP ステータス情報」のウィンドウが、選択中のワークスペース上に現れます。



ステータス	ホスト1	ポート番号1	送信バイト数1	ホスト2	ポート番号2	送信バイト数2	接続時刻
ESTABLISHED	Server2	48552	3929	Server1	22273	3624	2004/11/08 10:3
ESTABLISHED	Server4	44349	1842	Server1	22273	1418	2004/11/08 10:4
ESTABLISHED	Server4	63795	1434	Server1	22273	2311	2004/11/08 10:5
ESTABLISHED	Server4	52056	0	Server1	22273	1	2004/11/08 11:1
ESTABLISHED	Server4	53794	0	Server1	22273	1	2004/11/08 11:2
ESTABLISHED	172.16...	741	0	Server1	513	1	2004/11/08 11:2
ESTABLISHED	Server4	841	2208	Server1	2049	3188	2004/11/08 11:3
ESTABLISHED	Server5	746	75	Server1	513	7062	2004/11/08 11:4
SYNSENT	172.31...	80	0	Server1	47746	0	2004/11/08 11:5
TIMEWAIT	adm03....	2049	382	Server1	139	123	2004/11/08 11:5
RESET	Server1	80	58720	adm44....	1679	2523	2004/11/08 11:5
TIMEWAIT	Virus-...	64662	8865	Server1	25	552	2004/11/08 11:5
RESET	Virus-...	113	0	Server1	47754	0	2004/11/08 11:5

図 2-9: 「TCP ステータス情報」のウィンドウ

「TCP ステータス情報」のウィンドウは表形式で、 8 個のカラムがあります。カラムの見出しをクリックすると、カラムの内容に従って行を並べ替えることができます。次に、各カラムの名前と表示する情報を示します。

- **ステータス**
  TCP 接続の状態を表示します。 CLOSED、 SYNSENT、 SYNRECEIVED、 ESTABLISHED、 FINWAIT、 CLOSEWAIT、 LASTACK、 RESET、 TIMEWAIT のいずれかを表示します。 TCP 接続の状態については、「2.8.2 TCP のステータス」 (44 ページ) を参照してください。
- **ホスト 1、ホスト 2**
  TCP で接続しているホストの名前または IP アドレスを表示します。
- **ポート番号 1、ポート番号 2**
  ホスト 1 とホスト 2 の TCP ポート番号を表示します。
- **送信バイト数 1、送信バイト数 2**
  各ホストが転送したデータ (ペイロード) の累計値をバイト数で表示します。
- **接続時刻**
  ホスト 1 とホスト 2 の間でやり取りされたパケットのうち、 1 番最初のパケットをモニタした時刻を表示します。

「TCP ステータス情報」のウィンドウでは、文字列を検索できます。検索するには、メインウィンドウの**編集(E)** メニューから**検索(F)** を選ぶか、 **<Ctrl-F>** キーを押します。 「検索」ダイアログが現れるので、探したい文字列を入力して**次を検索(F)** ボタンをクリックします。検索する文字列に正規表現を使うこともできます。正規表現を指定する場合は、**正規表現(E)** にチェックを付けます。正規表現については、「6.8.2　正規表現を用いた検索」 (147 ページ)を参照してください。

2.8.2　TCP のステータス

図 2-10 に、 TCP 接続が確立するまでの流れと、切断の手続きを開始してから終了するまでの流れ、およびステータスカラムの表示の移り変わりを示します。

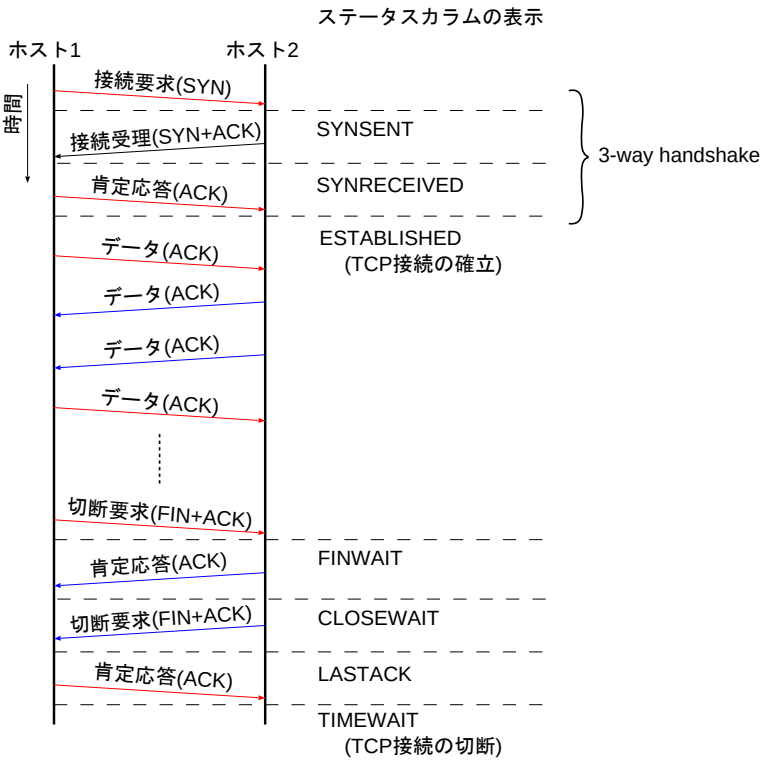


図 2-10: TCP 接続の確立から切断まで

ステータスカラムの表示が RESET になるのは、 TCP ヘッダーの Flags フィールドの RST ビットが ON になっているパケットをモニタしたときです。

ステータスが TIMEWAIT または RESET になってから 2MSL が経過した接続のエントリは、「TCP ステータス情報」のウィンドウから消えます。

MSL とは「Mean Segment Lifetime」の略で、 ASTEC Eyes で使っている値は 60 秒です。すなわち、 2MSL は 120 秒となります。

2.9 ホストごとのポートの状態を表示する

モニタしたパケットから得られた情報を基に、特定のホストのポートの状態を表示します。選んだホストが開いているポートについて、接続に成功した回数、接続要求に応えなかった回数、接続を拒否した回数を表示します。

ホストごとのポートの状態を表示するには、次のようにします。

1. 次のいずれかのモニタウィンドウを開きます。
   - IP アドレス表
   - MAC アドレス - IP アドレス対応表
   - 「IP 層発信元毎のトラフィック」のウィンドウ
   - 「IP 層受信先毎のトラフィック」のウィンドウ
   - 「IP 層ホストペア毎のトラフィック」のウィンドウ

   モニタウィンドウを開く方法については、「2.1.2 モニタウィンドウを開く」 (13 ページ)を参照してください。
2. ポートの状態を見たいホストの行またはグラフアイテムを右クリックしてポップアップメニューを開き、**ポートの状態一覧(S)** を選びます。
   図 2-11 に示すような「ポートの状態一覧」ダイアログが現れます。

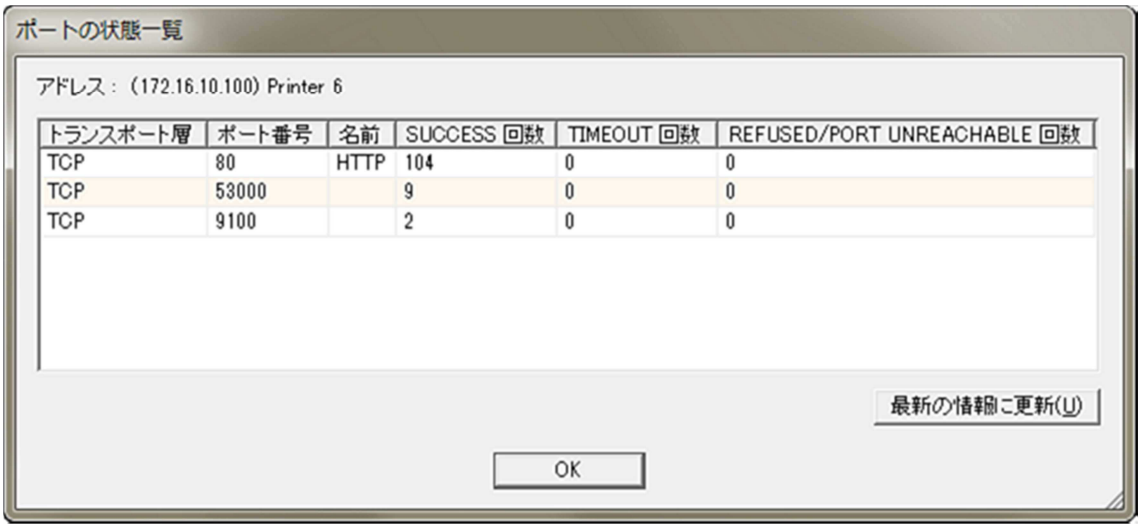


図 2-11: 「ポートの状態一覧」ダイアログ

「ポートの状態一覧」ダイアログには 6 つのカラムがあります。それぞれのカラムに表示する情報は次のとおりです。

トランスポート層 UDP または TCP が表示されます。

ポート番号 UDP または TCP のポート番号が表示されます。

名前 ポート番号から認識できるプロトコル名を表示します。

SUCCESS 回数 TCP 接続が確立した回数を表示します。

具体的には、表示されているポートへの TCP の SYN パケットを観測した後、表示ポートから送り出された SYN/ACK パケットを観測すると、SUCCESS 回数が 1 増えます。

TIMEOUT 回数 TCP 接続が一定時間内に確立できなかった回数を表示します。

具体的には、表示されているポートへの TCP の SYN パケットを観測した後、表示ポートからの SYN/ACK パケットを 2MSL 時間内に観測できなかった場合、 TIMEOUT 回数が 1 増えます。

REFUSED/PORT UNREACHABLE 回数

TCP または UDP の接続要求が拒否された回数を表示します。

具体的には、次の 2 つの状態を観測したときに REFUSED/PORT UNREACHABLE 回数が 1 増えます。

- 表示されているポートへの TCP の SYN パケットを観測した後、表示ポートから送り出された RST パケットを観測した場合
- 表示ポートから送り出された ICMP の Port Unreachable パケットを観測した場合

MSL とは「Mean Segment Lifetime」の略で、 ASTEC Eyes で使っている値は 60 秒です。すなわち、 2MSL は 120 秒です。

キャプチャモジュールはプロキシサーバーなどが利用する代表的なポート番号を区別します。区別しないポート番号については、ポート状態の情報をまとめます。

- ポート番号が空白で、名前が「Other」の行
  キャプチャモジュールが区別していないポート番号の情報をまとめたものです。
- ポート番号が表示されていて、名前が空白の行
  キャプチャモジュールが区別しているポート番号ですが、該当するプロトコル名が GUI モジュールには登録されていないものです。デコードヒントを入力すれば、名前を表示できるようになります。

2.10 モニタ情報を csv 形式などで保存する

ASTEC Eyes には、モニタウィンドウに表示されているモニタ情報をファイルに保存したり、コピーアンドペーストを使って他のアプリケーション (Microsoft Word や Microsoft Excel、ワードパッド、メモ帳など) に貼り付ける機能があります。

2.10.1 モニタ情報をファイルに保存する

ファイルに保存する場合は、ファイルの形式を選べます。選べるファイルの形式は次のとおりです。

- CSV (カンマ区切り) 形式 (*.csv)
- ビットマップ形式 (*.bmp)
- PNG 形式 (*.png)

モニタ情報をファイルに保存するには、次のようにします。

1. 保存したいモニタ情報を表示しているモニタウィンドウをアクティブにします。
2. メインウィンドウの**ファイル(F)** メニューから**モニタ情報の保存(G)**. . . を選びます。

2.10.2 モニタ情報をコピーする

コピーアンドペースト操作でモニタ情報をコピーする場合、貼り付け先のアプリケーションによってデータの形式が変わります。貼り付け先のアプリケーションによっては、貼り付けるデータの形式を選べるものもあります。トラフィックウィンドウに表示されているグラフを Microsoft Word や Microsoft Excel に貼り付ける場合は、視覚的な効果を期待して、そのまま画像として貼り付けることもできますし、グラフに表示しているデータを、テキストまたは CSV 形式のテキストとして貼り付けることもできます。

グラフ形式のトラフィックウィンドウからコピーする

グラフ形式 (折れ線グラフ、棒グラフ、円グラフ) のトラフィックウィンドウに表示されているモニタ情報をコピーして、他のアプリケーションに貼り付けるには、次のようにします。

1. コピーしたいトラフィックウィンドウをアクティブにします。
2. メインウィンドウの**編集(E)** メニューから**コピー(C)** を選ぶか、 **<Ctrl-C>** キーを押します。
3. 貼り付け先のアプリケーションをアクティブにします。

4. **<Ctrl-V>** キーを押します。
   トラフィックウィンドウのデータが、アプリケーションに貼り付けられます。 Microsoft Word や Microsoft Excel などの場合は、メニューバーの**編集(E)** から**形式を選択して貼り付け(S)** を選ぶこともできます。

表形式のモニタウィンドウからコピーする

表形式のモニタウィンドウに表示されているモニタ情報をコピーして、他のアプリケーションに貼り付けるには、次のようにします。

1. モニタウィンドウを右クリックしてポップアップメニューを開き、**すべてコピー(W)** を選びます。
2. 貼り付け先のアプリケーションをアクティブにします。
3. **<Ctrl-V>** キーを押します。
   モニタウィンドウのデータが、アプリケーションに貼り付けられます。 Microsoft Word や Microsoft Excel などの場合は、メニューバーの**編集(E)** から**形式を選択して貼り付け(S)** を選ぶこともできます。

2.11 モニタをリセットする

インタフェースを別のネットワークにつなぎ替えるなど、ネットワークの構成を変えたときに使う機能です。

モニタをリセットすると、 ASTEC Eyes またはリモートモジュールを起動してから、もしくは前回モニタをリセットしてから収集されたモニタ情報が初期化されます。収集した統計情報や IP アドレス、 MAC アドレスは失われます。

モニタをリセットするためには、対象とするインタフェースがインストールされているホストに対して設定権限が必要です。

設定権限があるかどうかは、インタフェースセレクタウィンドウのアイコンで確認できます。ホストのアイコンが「**設定権限のあるホスト** () 」の場合は設定権限があります。「**設定権限のないホスト** () 」の場合は設定権限がありません。設定権限を取得する方法について、詳しくは「8.3　設定権限の取得と解放」 (192 ページ) を参照してください。

モニタをリセットする方法は 2 通りあります。

- 対象とするインタフェースを選び、メインウィンドウの**モニタ(M)** メニューから**モニタリセット(R)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタリセット(R)** を選びます。

本当にモニタをリセットしてしまってよいのかどうかをたずねるウィンドウが現れます。モニタをリセットするときは、**はい(Y)** ボタンをクリックします。リセットしないときは、**いいえ(N)** ボタンをクリックします。

モニタをリセットすると、モニタは停止し、モニタウィンドウは何も表示されていない状態になります。

リセットするインタフェースを複数の ASTEC Eyes でモニタしている場合、モニタ情報が初期化されるのはリセットを実行したホストのインタフェースだけです。

3章

ログ機能

ASTEC Eyes には、一定時間ごとにトラフィックの統計情報やイベント情報、アドレスの一覧をファイルに出力する機能があります。この機能を**ログ機能**と呼びます。また、ファイルに出力する情報のことを**ログ**、出力するファイルを**ログファイル**と呼びます。

長期間にわたるトラフィックのトレンドを調べるためには、ログ機能を使います。ネットワークのトラフィックが一番多いのは何時ごろか、またそのときどのようなプロトコルが多く使われているのかなどを調べるには、ログ機能が役に立つでしょう。

ログは、ネットワークからリアルタイムに情報を収集しているモニタ機能と同じようにモニタウィンドウに表示されます。ただし、次の点が異なります。

- 表示するときに、折れ線グラフのデータをプロットする間隔を選べます。
- TCP 接続の状態はログファイルに保存されないので、表示できません。

ログの設定はインタフェースごとに行います。ログを見るだけの場合は、設定権限は必要ありませんが、**ログの出力を開始したり、停止したりするためには、対象とするインタフェースがインストールされているホストに対して、設定権限が必要です。**

設定権限があるかどうかは、インタフェースセレクタウィンドウのアイコンで確認できます。ホストのアイコンが「**設定権限のあるホスト** () 」の場合は設定権限があります。「**設定権限のないホスト** () 」の場合は設定権限がありません。設定権限を取得する方法について、詳しくは「8.3　設定権限の取得と解放」 (192 ページ) を参照してください。

3.1 ログの出力を開始する

デフォルトでは、ログは出力しないようになっています。ログを出力するには、次のようにします。

1. 「ホストのプロパティ」ダイアログを開きます。
   「ホストのプロパティ」ダイアログを開く方法は 2 通りあります。
   - **「ホストのプロパティ」ダイアログを開く方法 1**
     (1) インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
     (2) **「ログ」**のタブをクリックします。
   - **「ホストのプロパティ」ダイアログを開く方法 2**
     (1) メインウィンドウの**設定(O)** メニューの**ログ機能(G)** をポイントします。
     (2) サブメニューからホストを選びます。

   現れた「ホストのプロパティ」ダイアログのようすを図 3-1 に示します。

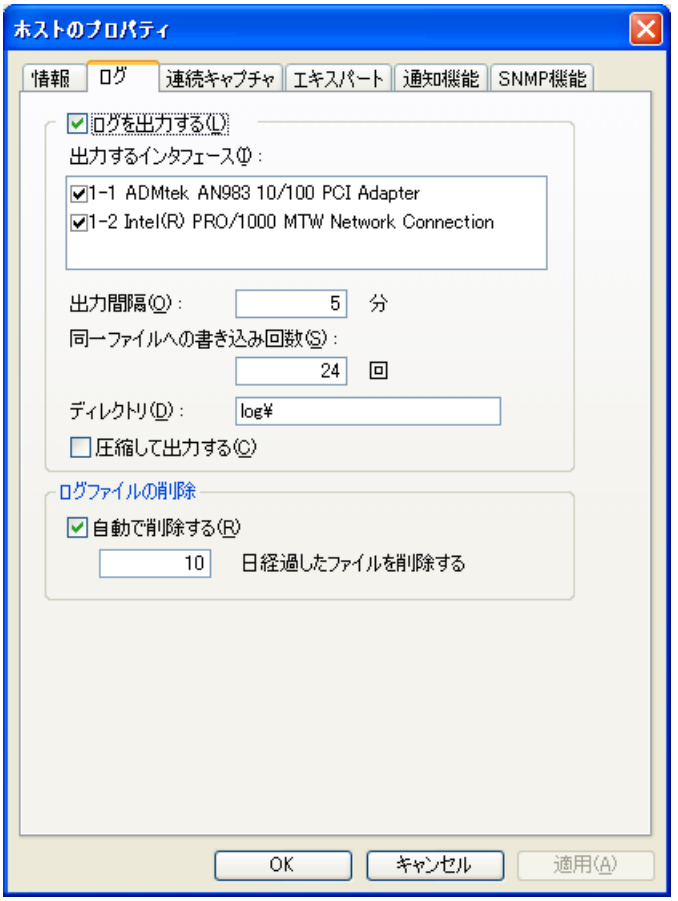


図 3-1:「ホストのプロパティ」ダイアログ (ログ)

2. **ログを出力する(L)** にチェックを付けます。
3. **出力するインタフェース(I)** のリストで、ログを出力するインタフェースを確認します。
   ログを出力するインタフェースにチェックを付けます。
   ログを出力しないインタフェースからチェックを外します。
4. **出力間隔(O)** を指定します。
   ログを作成する間隔です。デフォルトは 5 分です。何分ごとにログを作成するのか指定します。指定できる値の範囲は 5 ≤ 値 ≤ 720 (分) です。

5. **同一ファイルへの書き込み回数(S)** を指定します。
   1 つのログファイルにログを複数回書き込めます。 1 つのログファイルに書き込むログのうち初回分はすべての統計情報を保存しますが、効率がよいように、残りは直前の統計情報からの差分を記録します。デフォルトは 6 回です。指定できる値の範囲は 1 ≤ 値 ≤ 24 (回) です。
6. **ディレクトリ(D)** にログファイルを出力するディレクトリを入力します。
   ASTEC Eyes および Windows 用のリモートモジュールの場合は、インストールしたディレクトリからの相対パスで指定します。ディレクトリはあらかじめ作っておかなければなりません。また、このディレクトリは ASTEC Eyes またはリモートモジュールをインストールしたディレクトリのサブディレクトリである必要があります。
   ASTEC Eyes が動作しているローカルなホスト (localhost) および Windows 用のリモートモジュールの場合、デフォルトのディレクトリは `log` です。デフォルトのディレクトリはインストール時に作成されます。
   UNIX 用のリモートモジュールの場合は、設定ファイルで設定します。詳しくは『ASTEC Eyes UNIX 版リモートモジュールマニュアル』を参照してください。
7. ログファイルを圧縮して保存する場合は、**圧縮して出力する(C)** にチェックを付けます。
   チェックを付けると bzip2 で圧縮します。
8. ログファイルを自動的に削除したい場合は、**自動で削除する(R)** にチェックを付け、削除するまでの日数を入力します。削除するまでの日数に指定できる値の範囲は 1 日以上 365 日以下です。
   ここで指定した日数を経過したログファイルは自動的に削除されます。
9. **OK** ボタンまたは**適用(A)** ボタンをクリックします。
   出力するインタフェース(I) のリストでチェックの付いているインタフェースでログの出力が始まります。
   OK ボタンをクリックした場合は、ダイアログが閉じます。

書き込み中のログファイルの情報を参照したり、表示することはできません。ログの情報を表示できるようになるまでの待ち時間は (出力間隔 × 同一ファイルへの書き込み回数) です。そのため、出力間隔や同一ファイルへの書き込み回数の値を大きくすると、ログの情報を表示できるようになるまでの時間が長くなります。

ログを出力するように設定すると、 ASTEC Eyes を終了した後もログを出力するプロセスが動き続けます。また、 PC を再起動したときは、自動的に出力が再開されます。

インタフェースツールバーに「ホストのプロパティ」ダイアログを表示するボタン () を追加することもできます。このボタン () を押したときにプロパティが表示されるホストは、選択中のインタフェースが属すホストです。
ツールバーのカスタマイズの方法について、詳しくは「1.1.1　ツールバー」 (6 ページ) を参照してください。

3.2 ログの出力を停止する

1. 「ホストのプロパティ」ダイアログを開きます。
   「ホストのプロパティ」ダイアログを開く方法は 2 通りあります。
   - **「ホストのプロパティ」ダイアログを開く方法 1**
     (1) インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**... を選びます。
     (2) **「ログ」**のタブをクリックします。
   - **「ホストのプロパティ」ダイアログを開く方法 2**
     (1) メインウィンドウの**設定(O)** メニューの**ログ機能(G)** をポイントします。
     (2) サブメニューからホストを選びます。

   図 3-1 のような「ホストのプロパティ」ダイアログが現れます。
2. すべてのインタフェースでログの出力を停止したい場合は、**ログを出力する(L)** のチェックを外します。
   特定のインタフェースでログの出力を停止したい場合は、**出力するインタフェース(I)** のリストで、ログの出力を停止したいインタフェースのチェックを外します。
3. **OK** ボタンをクリックして、「ホストのプロパティ」ダイアログを閉じます。

ASTEC Eyes をアンインストールするときは、ログの出力を停止する必要があります。ログを出力しているときは、 ASTEC Eyes を終了してもログを出力するプロセスが動き続けるため、正常にアンインストールできません。

ログの出力を開始しても、指定した出力間隔以内にログを停止し、かつ ASTEC Eyes を終了した場合、ログファイルは出力されません。

インタフェースツールバーに「ホストのプロパティ」ダイアログを表示するボタン () を追加することもできます。このボタン () を押したときにプロパティが表示されるホストは、選択中のインタフェースが属すホストです。
ツールバーのカスタマイズの方法について、詳しくは「1.1.1 ツールバー」 (6 ページ) を参照してください。

3.3 ログを見る

ログを見る方法は 2 通りあります。

1 つは、 ASTEC Eyes またはリモートモジュールにログファイルの出力先として設定したディレクトリのログを見る方法です。この方法では、ログを出力した (している) ホストで ASTEC Eyes またはリモートモジュールが動作している必要があります。ログを見ている間もログを出力し続けている場合、最新のログを表示するように指定したウィンドウでは、グラフや表が更新されます。

もう 1 つは、 ASTEC Eyes やリモートモジュールと関係なく、ログファイルを保存しているディレクトリを指定して見る方法です。この方法では、ログを保存しているホストで ASTEC Eyes またはリモートモジュールが動作している必要はありません。

3.3.1 ログファイルの出力先のディレクトリのログを見る

1. インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**ログの一覧を作成(L)** を選びます。
   「ホストのプロパティ」ダイアログの「ログ」のページで指定したディレクトリ (図 3-1 参照) に保存されているログファイルの解析が始まります。ログファイルを解析している間、「ASTEC Eyes」ダイアログが現れ、進捗を示します。
   ログはインタフェースごとに分類されます。解析が終わると、インタフェースセレクタウィンドウ内に、インタフェース毎のログのエントリが現れます。そのようすを図 3-2 に示します。

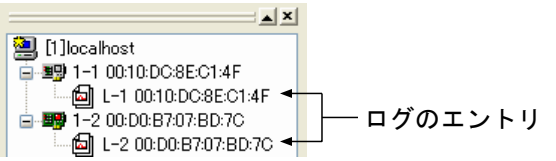


図 3-2: ログのエントリが現れたインタフェースセレクタウィンドウ

2. インタフェースセレクタウィンドウ内のログのエントリを右クリックしてポップアップメニューを開き、**ログを表示(L)**. . . を選びます。
   図 3-3 のような「ログの表示」ダイアログが現れます。

図 3-3: 「ログの表示」ダイアログ

3. 表示期間を指定します。
   表示期間 領域で、**最新(N)** または**範囲(R)** を選びます。
   最新(N) を選んだ場合は、どのくらい前までさかのぼって見るのかを指定します。
   範囲(R) を選んだ場合は、**開始時刻(B)** と**終了時刻(L)** を指定します。**開始時刻(B)** と**終了時刻(L)** を指定する方法として、キー入力する代わりに、期間指定バーを使うこともできます。 期間指定バーについては、「3.3.3 (緑色の) 期間指定バーを使う」 (62 ページ) を参照してください。
4. プロットの間隔を指定します。
   プロット間隔 領域で、折れ線グラフ形式のデータをプロットする間隔を選びます。
5. **ログのグラフを表示**...ボタンをクリックし、表示したいモニタウィンドウまたはイベントビューアを選びます。

ログを出力していたときにはインストールされており、現在はホストにインストールされていないネットワークインタフェースのログも表示されます。

3.3.2 ディレクトリを指定してログを見る

1. ログのディレクトリを指定するために、「ディレクトリの参照」ダイアログを開きます。
「ディレクトリの参照」ダイアログを開く方法は 2 通りあります。

   - メインウィンドウの**ファイル(F)** メニューから**ログのディレクトリを開く(L)**... を選びます。
   - インタフェースセレクタウィンドウ内の何も表示されていない部分を右クリックしてポップアップメニューを開き、**ログのディレクトリを開く(L)**... を選びます。

2. 「ディレクトリの参照」ダイアログでディレクトリを指定します。
インタフェースセレクタウィンドウにディレクトリのエントリとログのエントリが現れます。そのようすを図 3-4 に示します。

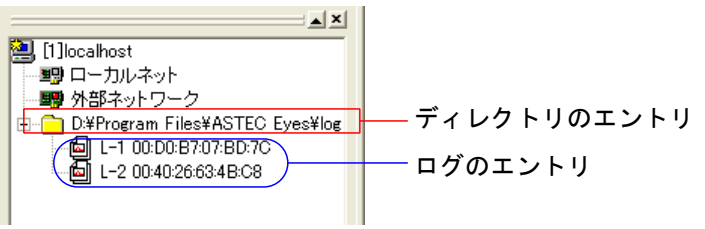


図 3-4: ディレクトリのエントリとログのエントリが現れた
インタフェースセレクタウィンドウ

3. インタフェースセレクタウィンドウ内のログのエントリを右クリックしてポップアップメニューを開き、**ログを表示(L)**... を選びます。
図 3-5 のような「ログの表示」ダイアログが現れます。

図 3-5: 「ログの表示」ダイアログ

4. 表示期間を指定します。
   表示期間 領域で、**最新(N)** または**範囲(R)** を選びます。
   最新(N) を選んだ場合は、どのくらい前までさかのぼって見るのかを指定します。
   範囲(R) を選んだ場合は、**開始時刻(B)** と**終了時刻(L)** を指定します。**開始時刻(B)** と**終了時刻(L)** を指定する方法として、キー入力する代わりに、期間指定バーを使うこともできます。 期間指定バーについては、「3.3.3 (緑色の) 期間指定バーを使う」 (62 ページ) を参照してください。
5. プロットの間隔を指定します。
   プロット間隔 領域で、折れ線グラフ形式のデータをプロットする間隔を選びます。
6. **ログのグラフを表示**...ボタンをクリックし、表示したいモニタウィンドウまたはイベントビューアを選びます。

3.3.3 (緑色の) 期間指定バーを使う

(緑色の) 期間指定バーは、マウス操作だけで期間を指定するためのもので、「ログの表示」ダイアログ (「3.3 ログを見る」 (58 ページ) を参照) および「キャプチャデータマネジャー」ダイアログ (「6.10 キャプチャデータマネジャーを使う」 (159 ページ) を参照) にあります。

(緑色の) 期間指定バーの使い方を図 3-6 を例にとって説明します。

図 3-6: 「ログの表示」ダイアログ

図 3-6 は、 9 日から 15 日までのログがあることを示しています。たとえば、 11 日のログを見たい場合、 11 日のところにマウスカーソルを合わせて、クリックします。選択した時刻が **開始時刻(B)** と **終了時刻(L)** に反映されます (図 3-7 参照)。

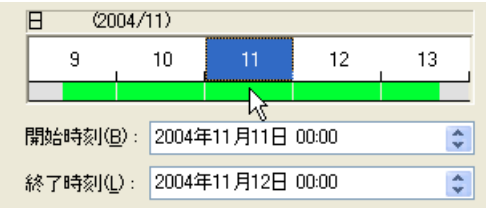


図 3-7: 11 日をクリックした後

さらに、時間を指定したい場合は、 11 日をダブルクリックするか、 11 日を選んだ状態で **<Enter>** キーを押します。期間指定バーの目盛りが日付単位から時間単位に変わります。そのようすを図 3-8 に示します。

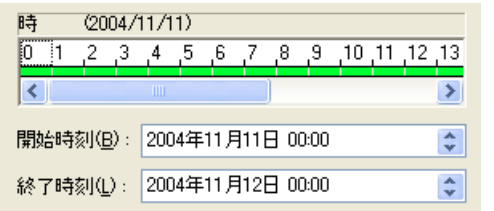


図 3-8: 時間を選べるようになる

たとえば、 2 時から 5 時までの時間を指定したい場合は、図 3-9 のようにマウスをドラッグします。ドラッグするにつれて、**開始時刻(B)** と **終了時刻(L)** の表示が変わります。

図 3-9: 2 時から 5 時までドラッグしたところ

入力し直したいときは、右クリックするか、 **<Backspace>** キーを押します。

3.4 ログのプロパティを見る

「ログのプロパティ」ダイアログには、ログを収集したネットワークインタフェースカードの情報や NIC ID、期間が表示されます。 NIC ID は、キャプチャモジュールが NIC を一意に識別できるように割り当てた ID です。

「ログのプロパティ」ダイアログを開くには、インタフェースセレクタウィンドウ内のログのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。

図 3-10 のような「ログのプロパティ」ダイアログが現れます。

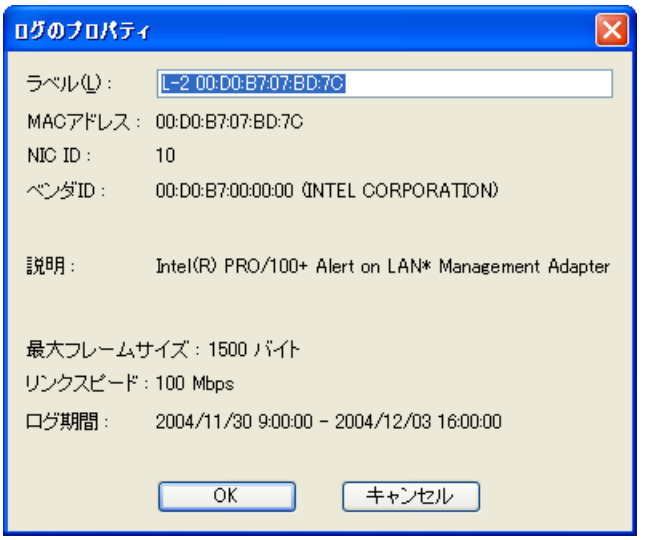


図 3-10: 「ログのプロパティ」ダイアログ

このダイアログでログのエントリのラベルを変更することもできます。詳しくは「13.5 インタフェースセレクタウィンドウのラベルを変える」 (354 ページ) を参照してください。

3.5 ログを表示しているモニタウィンドウの操作

ネットワークの現在の状態を表示しているモニタウィンドウとまったく同じ操作が、ログを表示しているモニタウィンドウでも行えます。

- トラフィックウィンドウの表示をカスタマイズする
  「2.2 トラフィックウィンドウの表示をカスタマイズする」 (17 ページ) を参照してください。
- グラフアイテムの内訳を見る
  「2.4 内訳を見る」 (29 ページ) を参照してください。
- 折れ線グラフの値を読み取る
  「2.5 折れ線グラフの値を読み取る」 (30 ページ) を参照してください。
- モニタフィルタを適用する
  モニタフィルタはログを表示しているトラフィックウィンドウにも適用できます。
  まず、フィルタエディタを使って、モニタフィルタを定義します。次に、インタフェースセレクタウィンドウ内のログのエントリを右クリックしてポップアップメニューを開き、**モニタフィルタ(F)** から定義してあるモニタフィルタを選びます。
  同一インタフェースのログを表示しているトラフィックウィンドウすべてに、モニタフィルタが適用されます。
  モニタフィルタについては、「2.6 モニタフィルタを使う」 (35 ページ) を参照してください。
- モニタウィンドウに表示されている情報を保存する
  モニタウィンドウに表示されている情報をファイルに保存したり、コピーアンドペーストを使って他のアプリケーション (Microsoft Word や Microsoft Excel、ワードパッド、メモ帳など) に貼り付けることができます。
  その手順については、「2.10 モニタ情報を csv 形式などで保存する」 (49 ページ) を参照してください。

4章

レポート機能

モニタやログで表示しているグラフをレポートとして HTML 形式のファイルに出力する機能です。出力したファイルを印刷して報告書として利用したり、ファイルのまま Web ブラウザで見ることができます。

4.1 レポートの出力方法と形式

レポートは出力方法によって 3 種類に分類されます。

- **最新の状態に更新するレポート**
- **定期的に出力するレポート**
- **手動で出力するレポート**

最新の状態に更新するレポートでは、一定の時間間隔で同じファイルにレポートを上書きします。このファイルを Web ブラウザで表示すれば、常に最新の状態を見ることができます。

定期的に出力するレポートは、指定した日時に定期的にレポートを作成したり、一定の時間間隔でレポートを作成します。作成したレポートは新しいファイルに書き出し、以前に作ったレポートのファイルはそのまま残ります。

出力したレポートのファイルには、前後のレポートを参照する HTML のリンクが埋め込まれます。また、リンクの一覧ファイルも作られるので、 Web ブラウザでクリックしながらトラフィックの変化を確認できます。

手動で出力するレポートは手動でレポートを出力します。**定期的に出力するレポート**の場合と同様、作成したレポートは新しいファイルに書き出し、前後のレポートへの HTML のリンクが埋め込まれます。**定期的に出力するレポート**と**手動で出力するレポート**が混在しているときには、時間順に並ぶようにリンクやリンクの一覧ファイルが作られます。

図 4-1は、出力されたレポートを Web ブラウザで表示したようすです。

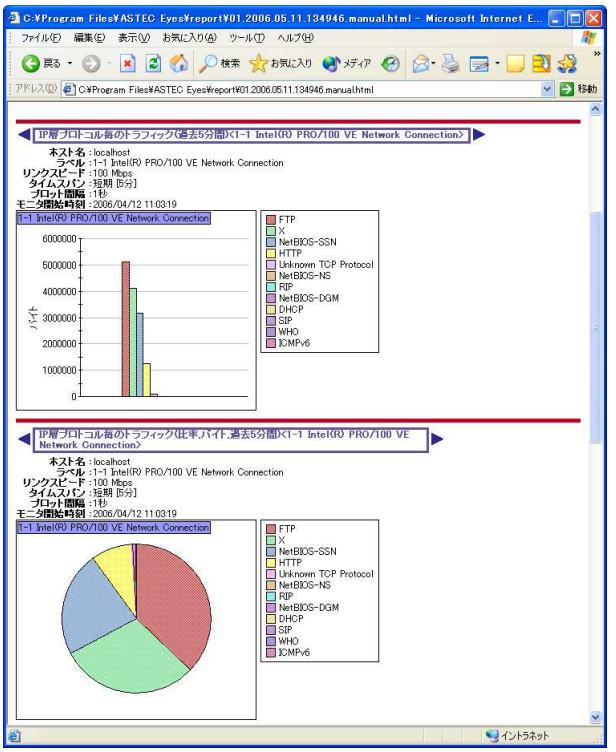


図 4-1: レポートの表示

4.2 ウィザードを利用したレポートの作成

レポートの出力はワークスペースごとに設定します。

レポート設定の追加ウィザードを利用すれば、簡単な操作で定期的にレポートを作成するように設定できます。

1. メインウィンドウの**設定(O)** メニューから**レポート設定の追加**を選びます。
2. 図 4-2に示したような、ワークスペースを選択するページが表示されます。

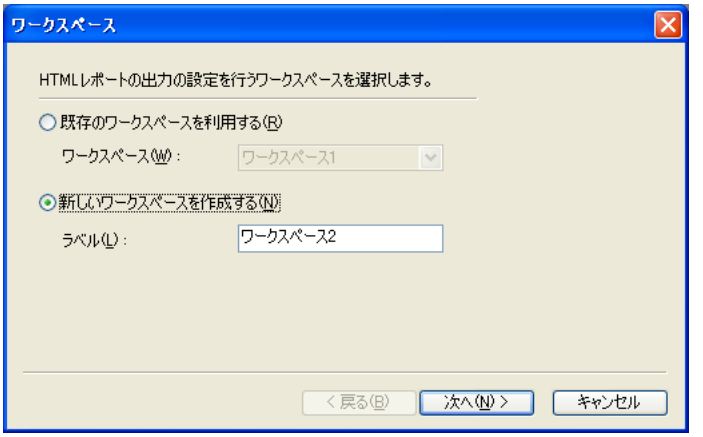


図 4-2: レポート設定の追加ウィザード (ワークスペース)

既存のワークスペースにレポートの設定を追加するか、新しいワークスペースを作成してレポートの設定を行うかを指定します。
次へ(N) ボタンをクリックします。

3. グラフのサイズを指定します。

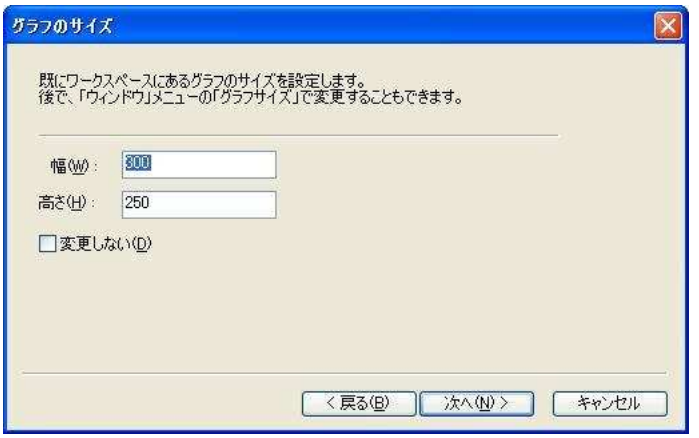


図 4-3: レポート設定の追加ウィザード (グラフのサイズ)

サイズを指定すると、ウィザード終了時に対象となるワークスペース上のすべてのグラフが、指定した大きさになります。また、レポートに出力されるグラフも指定したサイズに揃います。

変更しない(D) にチェックを付けるとグラフの大きさは変更されず、ワークスペースに表示されているサイズでレポートにも出力されます。

次へ(N) ボタンをクリックします。

メインウィンドウの**ウィンドウ(W)** メニューから**グラフサイズ(G)** を選んで、グラフのサイズを指定することもできます。

4. レポートの出力方法と出力タイミングを指定します。**次へ(N)** ボタンをクリックします。

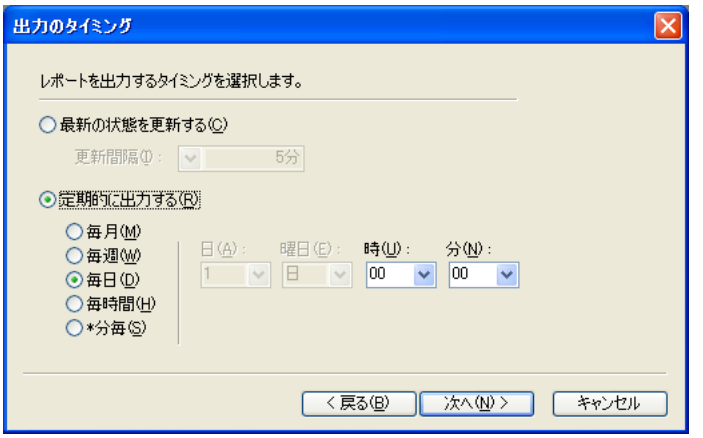


図 4-4: レポート設定の追加ウィザード (出力のタイミング)

5. レポートを出力するディレクトリを指定します。

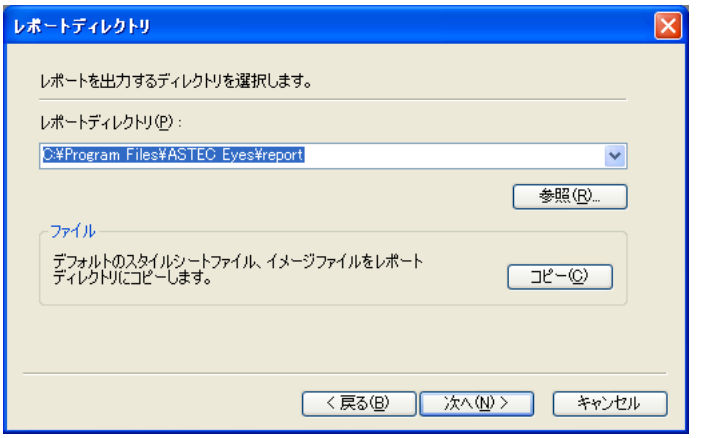


図 4-5: レポート設定の追加ウィザード (レポートディレクトリ)

レポートから参照されるファイルがまだ存在しないときには、**コピー(C)** ボタンをクリックして必要なファイルをコピーします。
次へ(N) ボタンをクリックします。

6. テンプレートファイルを指定します。
   デフォルトのテンプレートファイルは、
   `C:￥Program Files￥ASTEC Eyes ￥template ￥template.html`
   です。
   次へ(N) ボタンをクリックします。

テンプレートファイルをカスタマイズすれば、レポートのレイアウトを変更できます。

7. レポートをすぐに出力するかどうかを指定します。
   ウィザード終了後、一度レポートを出力する(T) にチェックを付けるとレポートをすぐに出力します。
   完了ボタンをクリックし、ウィザードを終了します。

レポートの設定が追加されているワークスペースのタブには、  が表示されます。また、指定したタイミングでレポートを出力します。

4.3 ワークスペースのグラフをレポートに出力

ワークスペースにレポートの設定を追加したり、既存の設定を変更することができます。

レポートの設定を行うには、次のようにします。

1. ワークスペースを選びます。
2. ワークスペース内のウィンドウが表示されていない部分、またはワークスペースのタブを右クリックしてポップアップメニューを開き、**レポートの設定(H)**... を選びます。
   図 4-6 に示すような「HTML レポート」ダイアログが現れます。

図 4-6: 「HTML レポート」ダイアログ (レポートページ)

3. レポートの出力方法と出力タイミングを指定します。その場で 1 度だけ出力する場合は、**今すぐ出力する(T)** ボタンをクリックします。

4.4 レポートの表示

レポートを表示する方法は 2 通りあります。

- **「レポート」**のページから表示
  図 4-6に示した**「レポート」**のページの、**自動更新ページ**、**一覧ページ**、または**ページ**に表示されたレポートのファイル名をクリックします。 Web ブラウザが起動してレポートが表示されます。
- **「表示」**のページから表示

1. **「表示」**のタブをクリックします。図 4-7 に示すようなページが表示されます。

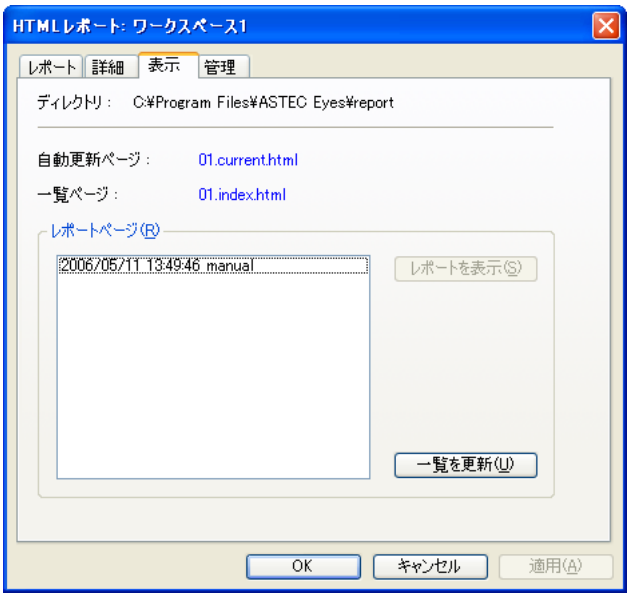


図 4-7: 「HTML レポート」ダイアログ (表示ページ)

2. **自動更新ページ**や**一覧ページ**のファイル名をクリックするか、**レポートページ(R)** 領域で表示させたいページを選び、**レポートを表示(S)** ボタンをクリックします。

4.5 レポート設定の管理

「HTML レポート」ダイアログではレポートの設定や出力したレポートの管理を行うことができます。

4.5.1 出力先ディレクトリを変更する

1. 「HTML レポート」ダイアログを開きます。
2. **「詳細」**のタブをクリックします。
   図 4-8 に示すようなページが表示されます。

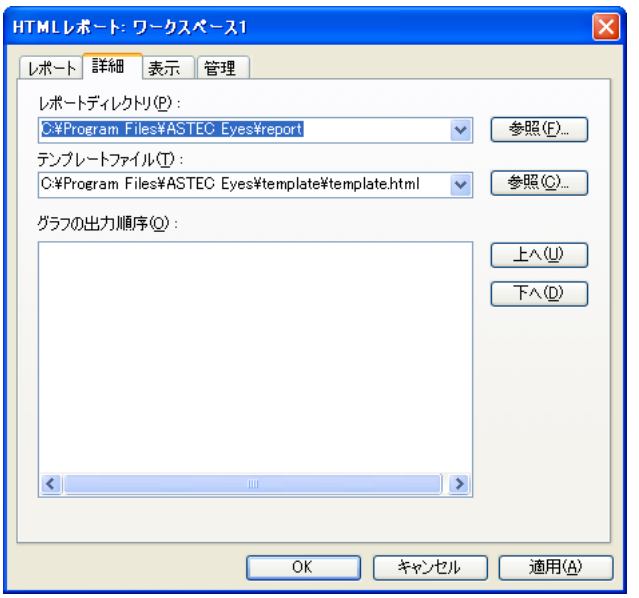


図 4-8: 「HTML レポート」ダイアログ (詳細ページ)

3. **レポートディレクトリ(P)** にレポートの出力先のディレクトリを入力します。
4. **適用(A)** ボタンをクリックします。
5. **「管理」**のタブをクリックします。
   図 4-9 に示すようなページが表示されます。

図 4-9: 「HTML レポート」ダイアログ (管理ページ)

6. **コピー(C)** ボタンをクリックします。
   レポートの表示に必要なファイルが、レポートの出力先ディレクトリにコピーされます。

レポートの出力先のディレクトリは、あらかじめ作成しておく必要があります。

4.5.2 レポートのレイアウトを変更する

レポートに表示するグラフの順序やテンプレートファイルを変更できます。

グラフの順序の変更

1. 「HTML レポート」ダイアログを開きます。
2. **「詳細」**のタブをクリックします。
3. **グラフの出力順序(O)** に表示されているグラフのうち、順序を変更したいものをクリックします。
4. **上へ(U)** ボタンや**下へ(D)** ボタンをクリックして、順序を変更します。

テンプレートファイルの変更

テンプレートファイルの特定の記述を、グラフのイメージデータやリンクに置き換えることによって、レポートを作成しています。

テンプレートファイルを変更すれば、タイトルを変更したり、説明やロゴマークを追加することができます。

テンプレートファイルは次の方法で変更します。

1. 「HTML レポート」ダイアログを開きます。
2. **「詳細」**のタブをクリックします。
3. **テンプレートファイル(T)** にテンプレートファイルのパスを入力します。
4. **適用(A)** ボタンをクリックします。

テンプレートファイルの記述方法については、「4.6　テンプレートファイルのカスタマイズ」(78 ページ) を参照してください。

4.5.3　レポートを削除する

古いレポートを手動や自動で削除して整理することができます。レポートを手動で削除するには、つぎのようにします。

1. 「HTML レポート」ダイアログを開きます。
2. **「管理」**のタブをクリックします。
3. **日付(D)** を入力します。指定した日付を含み、それよりも古いレポートが削除されます。
4. **削除(T)** ボタンをクリックします。

レポートを自動で削除するには、つぎのようにします。

1. 「HTML レポート」ダイアログを開きます。
2. **「管理」**のタブをクリックします。
3. **自動で削除する(M)** チェックボックスにチェックを付けます。
4. 何日経過したレポートを削除するか、その日数を入力します。
5. **適用(A)** ボタンをクリックします。

定期的に出力するレポートや**手動で出力するレポート**を削除すると、一覧ファイルに含まれているリンクや、前後のレポートへのリンクを修正する必要があります。**再構築(R)** ボタンをクリックすれば、リンクが最新の状態になるようにレポートを再構築します。

4.6 テンプレートファイルのカスタマイズ

テンプレートファイルをカスタマイズすれば、レポートのレイアウトを変更できます。

4.6.1 テンプレートファイルの形式

テンプレートファイルには、前後のページへのリンクやレポートの情報などを挿入する位置を示した、テンプレート文字列を埋め込みます。

テンプレート文字列には、グラフや表を挿入する領域を示す**レポート項目領域開始**文字列と**レポート項目領域終了**文字列、およびその他の項目の挿入位置を示す**項目開始**文字列と**項目終了**文字列があります。

レポート項目領域開始文字列と**レポート項目領域終了**文字列で挟まれた領域 (レポート項目領域) には、グラフや表を繰り返し出力します。

レポート項目領域開始と**レポート項目領域終了**の形式を次に示します。

レポート項目領域開始

```
<!-- ==================== $$BEGIN-ITEM-AREA$$ ==================== -->
```

レポート項目領域終了

```
<!-- ==================== $$END-ITEM-AREA$$ ==================== -->
```

項目開始文字列と**項目終了**文字列の形式を次に示します。**項目名**は挿入する項目の種類です。

項目開始 `<!--{{`項目名 `-->`

項目終了 `<!--}}` 項目名 `-->`

項目開始と**項目終了**の間に、指定された項目が HTML 形式で挿入されます。

たとえば、コンピュータやワークスペースなどのレポート情報を意味する REPORT-INFO の場合は次のように出力されます。

```
<!--REPORT-INFO-->
 レポート情報の記述
<!--REPORT-INFO-->
```

4.6.2 項目開始と項目終了

項目開始や**項目終了**で指定する項目には、任意の位置に埋め込むことができるものと、レポート項目領域の内側だけに埋め込むことができるものがあります。

表 4-1: 任意の位置に埋め込むことができるテンプレート文字列の項目

項目名	挿入される内容
EYES-REPORT-HEAD	レポート機能が一覧ページやリンクを再構築する際に内部的に利用するデータ
PREV-LINK-HEAD	前のレポートへのリンクの開始タグ
PREV-LINK-TAIL	前のレポートへのリンクの終了タグ
TOP-LINK-HEAD	一覧ページへのリンクの開始タグ
TOP-LINK-TAIL	一覧ページへのリンクの終了タグ
NEXT-LINK-HEAD	次のレポートへのリンクの開始タグ
NEXT-LINK-TAIL	次のレポートへのリンクの終了タグ
REPORT-INFO	レポートの情報 <table class="info"> <tr><th class="info">Computer Name</th> <td class="info"> マシン名 </td> </tr>. . . </table>

表 4-2: レポート項目領域に埋め込むことができるテンプレート文字列の項目

項目名	挿入される内容
ITEM-INDEX	レポート項目のアンカー
ITEM-LABEL	レポート項目のタイトル文字列
ITEM-INFO	レポート項目の情報。出力する項目の種類によって内容が異なります
ITEM-BODY	グラフのイメージや表の情報
ITEM-PREV-HEAD	前のレポートのレポート項目へのリンクの開始タグ
ITEM-PREV-TAIL	前のレポートのレポート項目へのリンクの終了タグ
ITEM-NEXT-HEAD	次のレポートのレポート項目へのリンクの開始タグ
ITEM-NEXT-TAIL	次のレポートのレポート項目へのリンクの終了タグ

4.6.3 リンクの書き換え

リンクに対応した項目に関しては、それぞれ対応する *item*-HEAD と *item*-TAIL の間のデータが、リンクを示すための文字列に置換されます。

たとえば前のレポートへのリンクを表す PREV-LINK-HEAD と PREV-LINK-TAIL は対で利用し、

```
<!--PREV-LINK-HEAD-->
<!--PREV-LINK-HEAD-->
PREV
<!--PREV-LINK-TAIL-->
<!--PREV-LINK-TAIL-->
```

のように記述します。

このとき、リンク先のレポートが存在すれば、出力されたレポートは次のようになります。

```
<!--PREV-LINK-HEAD-->
<a class="lnk" href="ファイル名 ">
<!--PREV-LINK-HEAD-->
<img class="lnk" src="left.png>
<!--PREV-LINK-TAIL-->
</a>
<!--PREV-LINK-TAIL-->
```

4.6.4 レポートで使用するスタイル

デフォルトのテンプレートファイルでは、 eyes.css をスタイルシートとして指定しています。

以下の表はデフォルトのテンプレートに含まれるスタイル、およびレポート作成時に生成される HTML のスタイルを定義するクラスです。

表 4-3: デフォルトのテンプレートに含まれるスタイル

タグとクラス	スタイルで定義する内容
H3.title	レポートのタイトル
HR.item	レポート項目間のライン
DIV.item	レイアウト用の DIV タグ
TABLE.label	レイアウト用の TABLE タグ
TD.label	レイアウト用の TABLE タグ

表 4-4: レポート作成時に生成されるスタイル

タグとクラス	スタイルで定義する内容
A.lnk	レポート間のリンク
IMG.lnk	レポート間のリンクに使われるイメージ
TABLE.info	「レポート情報」テーブル
TH.info	「レポート情報」ヘッダ
TD.info	「レポート情報」項目
A.itemlnk	レポート項目間のリンク
IMG.itemlnk	レポート項目間のリンクに使われるイメージ
TABLE.gprop	レポート項目情報のテーブル
TH.gprop	レポート項目情報テーブル
HD.gprop	レポート項目情報テーブル
IMG.graph	レポート項目がグラフの場合のイメージファイルへのリンク
TABLE.tbl	レポート項目が表の場合のテーブル
TH.thl	ヘッダ左寄せ
TH.htr	ヘッダ右寄せ
TD.tdl	ヘッダ左寄せ
TD.tdr	ヘッダ右寄せ
SPAN.msg	レポート項目出力に関するエラーメッセージ

5章

キャプチャ機能

ネットワークに流れているパケットを ASTEC Eyes に取り込む機能です。パケットの内容を詳細に解析するためには、パケットをキャプチャする必要があります。

ASTEC Eyes には、通常のキャプチャ、リアルタイムデコードキャプチャ、連続キャプチャの 3 種類があります。

通常のキャプチャは**キャプチャバッファ**と呼ぶ、メモリ上に確保された ASTEC Eyes の内部バッファにデータを取り込みます。 リアルタイムデコードキャプチャはキャプチャバッファを利用してデータを取り込みながら、同時にデコードして解析結果を表示します。連続キャプチャは取り込んだデータをファイルに保存します。

5.1 通常のキャプチャ

キャプチャの開始および停止は、ネットワークインタフェースごとに行います。また、キャプチャバッファはネットワークインタフェースごとに用意されます。

5.1.1 キャプチャを開始する

キャプチャを開始する方法は 3 通りあります。

- 対象とするインタフェースを選び、メインウィンドウのインタフェースツールバーの**キャプチャ開始**ボタン( ) をクリックします。
- 対象とするインタフェースを選び、メインウィンドウの**キャプチャ(C)** メニューから**キャプチャ開始(S)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**キャプチャ開始(S)** を選びます。

ネットワークインタフェースを選ぶ方法については、「1.2.1 インタフェースを選ぶ」 (10 ページ) を参照してください。

パケットがキャプチャバッファに取り込まれると、キャプチャバッファメーターのバーが右方向に伸び、バッファに取り込まれたバイト数が表示されます。バーの長さは、バッファサイズに対して実際に取り込まれたパケットのサイズの比率を表しています。キャプチャバッファメーターの表示は、取り込まれたパケットが増えるにしたがって変わります。

キャプチャバッファがいっぱいになったとき、キャプチャを停止するように設定している場合は、キャプチャバッファメーターのバーとバイト数は紺色 (354 K バイト) で表示されます。キャプチャを停止せずに、バッファの中の最も古いデータから上書き (オーバーライト) するように設定している場合は、緑色 (353 K バイト) で表示されます。

キャプチャバッファがいっぱいになった時の動作の設定については、「11.1 キャプチャのオプションを設定する」 (283 ページ) を参照してください。

5.1.2 キャプチャを停止する

キャプチャを停止する方法は 3 通りあります。

- 対象とするインタフェースを選び、メインウィンドウのインタフェースツールバーの**キャプチャ停止**ボタン( ) をクリックします。
- 対象とするインタフェースを選び、メインウィンドウの**キャプチャ(C)** メニューから**キャプチャ停止(I)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**キャプチャ停止(I)** を選びます。

ネットワークインタフェースを選ぶ方法については、「1.2.1 インタフェースを選ぶ」 (10 ページ) を参照してください。

5.1.3 キャプチャバッファのデータを保存する

キャプチャバッファに取り込んだデータをファイルに保存できます。

キャプチャしたデータをファイルに保存しておけば、いつでもデータを分析できます。キャプチャしたデータを保存したファイルを**キャプチャファイル**と呼びます。

キャプチャバッファのデータをファイルに保存するには、メインウィンドウの**ファイル(F)** メニューから**キャプチャバッファの保存(T)**. . . を選びます。

キャプチャしたデータを保存するファイルのフォーマットは、 Sniffer 互換の非圧縮フォーマット (拡張子 `.enc`) です。また、 bzip2 で圧縮してから保存することもできます。その場合の拡張子は`.ebz` となります。
bzip2 については、 http://www.bzip.org/ を参照してください。

5.1.4 キャプチャバッファのデータの削除

キャプチャバッファからデータを削除する方法は 3 通りあります。

- 対象とするインタフェースを選び、メインウィンドウのインタフェースツールバーの**キャプチャデータの削除**ボタン( ) をクリックします。
- 対象とするインタフェースを選び、メインウィンドウの**キャプチャ(C)** メニューから**キャプチャデータの削除(A)** を選びます。

- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**キャプチャデータの削除(A)** を選びます。

キャプチャッファのデータをファイルに保存していない場合は、本当に削除してよいかどうかをたずねる「ASTEC Eyes」ダイアログが現れます。削除するときは **OK** ボタンをクリックします。削除を中止したい場合は**キャンセル**ボタンをクリックします。

<Shift> キーを押しながら操作した場合は、「ASTEC Eyes」ダイアログは現れません。直ちにキャプチャバッファのデータを削除します。

5.1.5 キャプチャを再開する

キャプチャを停止して、キャプチャバッファのデータを削除せずに再度キャプチャを開始すると、新たにキャプチャしたパケットはキャプチャバッファに追加されます。

キャプチャバッファに空きがない状態でキャプチャを開始したときの動作はキャプチャバッファの設定によって異なります。バッファフル時の動作が**オーバーライト**のときは、既存のデータを新しいデータで上書きします。バッファフル時の動作が**キャプチャ停止**のときは、図 5-1 のような「ASTEC Eyes」ダイアログが現れます。

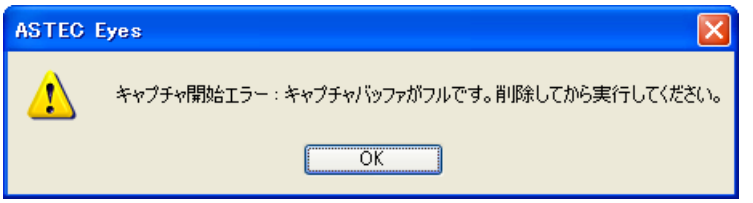


図 5-1: キャプチャバッファに空きがないときに現れるダイアログ

キャプチャバッファがいっぱいになった時の動作の設定については、「11.1 キャプチャのオプションを設定する」 (283 ページ) を参照してください。

5.1.6 クイックリターン機能を使う

ネットワークの状態を調べるときは、パケットのキャプチャとデコードを繰り返すことがあります。そのような場合、キャプチャの停止、デコードビューの作成、キャプチャバッファのデータの削除、キャプチャの開始という一連の操作を繰り返す必要があります。この一連の操作を

一つの機能としてまとめたものがクイックリターン機能です。クイックリターン機能はリアルタイムデコードモードのときには利用できません。

クイックリターン機能を使う方法は、 2 通りあります。

- インタフェースを選んだ後、メインウィンドウの**キャプチャ(C)** メニューから**クイックリターン(Q)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**クイックリターン(Q)** を選びます。

キャプチャ中にクイックリターン機能を使うと、一旦キャプチャを停止して、キャプチャバッファのデータのデコードを開始します。このときキャプチャバッファのデータはデコード用にコピーが作成されます。デコードの開始直後にキャプチャバッファのデータを削除し、キャプチャを再開します。

デフォルトの状態では、インタフェースツールバーに**クイックリターン**ボタン( ) はありません。インタフェースツールバーをカスタマイズして**クイックリターン**ボタン( ) を追加できます。ツールバーのカスタマイズについて、詳しくは「1.1.1　ツールバー」 (6 ページ) を参照してください。

5.2 リアルタイムデコードキャプチャ

リアルタイムデコードキャプチャの開始および停止は、ネットワークインタフェースごとに行います。また、キャプチャデータを取り込むときに一時的に利用されるキャプチャバッファと、デコードしたデータを保持するバッファはネットワークインタフェースごとに用意されます。

リアルタイムデコードは ASTEC Eyes 基本パッケージをインストールしたホストのネットワークインタフェースに対してのみ実行できます。リモートモジュールのネットワークインタフェースに対しては実行できません。

5.2.1 リアルタイムデコードキャプチャを開始する

リアルタイムデコードを行うにはあらかじめ、「オプション設定」ダイアログの「キャプチャ」のパネルで**リアルタイムデコード(R)** にチェックを付け、**保持するパケットの総バイト数(H)** にデコードしたパケットをどれだけ保持するかを入力します。リアルタイムデコードの設定については、「11.1 キャプチャのオプションを設定する」 (283 ページ) を参照してください。

リアルタイムデコードキャプチャを開始する方法は 3 通りあります。

- 対象とするインタフェースを選び、メインウィンドウのインタフェースツールバーの**キャプチャ開始**ボタン(●) をクリックします。
- 対象とするインタフェースを選び、メインウィンドウの**キャプチャ(C)** メニューから**キャプチャ開始(S)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**キャプチャ開始(S)** を選びます。

ネットワークインタフェースを選ぶ方法については、「1.2.1 インタフェースを選ぶ」 (10 ページ) を参照してください。

リアルタイムデコードキャプチャを開始するとリアルタイムデコードビューが現れます。キャプチャしたデータはいったんキャプチャバッファに取り込まれ、その後デコードした結果がリアルタイムデコードビューに表示されます。

ネットワークを流れるデータの量が多すぎて、デコードする前にキャプチャバッファがいっぱいになったときには、データの取りこぼしが発生します。データの取りこぼしについては、「6.2.5 パケットの取りこぼしの表示」 (110 ページ) を参照してください。

リアルタイムデコードキャプチャのときは、キャプチャバッファメーターはデコードしたパケットの量を示します。キャプチャデータをデコードすると、オレンジ色のバー (

)

が右方向に伸び、デコードしたバイト数が表示されます。バーの長さは、リアルタイムデコードビューに保持するパケットの総バイト数に対して、実際にデコードしたパケットのサイズの比率を表しています。

デコードしたデータを保持するバッファがいっぱいになった時の動作の設定については、「11.1 キャプチャのオプションを設定する」 (283 ページ) を参照してください。

リアルタイムデコードキャプチャでは、キャプチャバッファのデータの保存や削除はできません。リアルタイムデコードビューに取り込んだデータを保存するには、一旦、デコードビューを表示してから保存してください。

5.2.2 リアルタイムデコードキャプチャを停止する

リアルタイムデコードキャプチャを停止する方法は 3 通りあります。

- 対象とするインタフェースを選び、メインウィンドウのインタフェースツールバーの**キャプチャ停止**ボタン( ) をクリックします。
- 対象とするインタフェースを選び、メインウィンドウの**キャプチャ(C)** メニューから**キャプチャ停止(I)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**キャプチャ停止(I)** を選びます。

ネットワークインタフェースを選ぶ方法については、「1.2.1 インタフェースを選ぶ」 (10 ページ) を参照してください。

5.2.3 リアルタイムデコードキャプチャを再開する

リアルタイムデコードキャプチャを停止して再度開始すると、既にキャプチャしていたデータに新しくキャプチャしたデータが追加されます。

デコードしたデータのサイズが**保持するパケットの総バイト数**の設定値を超えたときの動作は、**この値を超えたらリアルタイムデコードを停止する**の設定によって異なります。リアルタイムデコードを停止する設定のときは、パケットのキャプチャが停止します。停止しない設定のときは、リアルタイムデコードビューの既存のデコードデータを新しいデータで上書きします。

5.3 連続キャプチャ

通常のキャプチャでは、キャプチャしたデータはキャプチャバッファに保存されます。キャプチャバッファはメモリ上に取られるので、その大きさは実メモリサイズの 1/4 までという制限があります。

場合によっては、より大きなデータをキャプチャし続けたいことがあるでしょう。 ASTEC Eyes には、連続的にキャプチャを行い、キャプチャしたデータを直接ファイルに保存する**連続キャプチャ機能**があります。

連続キャプチャを行うためには、対象とするインタフェースがインストールされているホストに対して設定権限が必要です。

設定権限があるかどうかは、インタフェースセレクタウィンドウのアイコンで確認できます。ホストのアイコンが「**設定権限のあるホスト** () 」の場合は設定権限があります。「**設定権限のないホスト** () 」の場合は設定権限がありません。設定権限を取得する方法について、詳しくは「8.3　設定権限の取得と解放」 (192 ページ) を参照してください。

5.3.1 連続キャプチャを開始する

連続キャプチャの開始はインタフェースごとに行います。

1. 「ホストのプロパティ」ダイアログを開きます。
   「ホストのプロパティ」ダイアログを開く方法は 2 通りあります。
   - **「ホストのプロパティ」ダイアログを開く方法 1**
     (1) インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
     (2) **「連続キャプチャ」**のタブをクリックします。
   - **「ホストのプロパティ」ダイアログを開く方法 2**
     (1) メインウィンドウの**設定(O)** メニューの**連続キャプチャ機能(J)** をポイントします。
     (2) サブメニューからホストを選びます。

インタフェースツールバーに「ホストのプロパティ」ダイアログを表示するボタン () を追加することもできます。このボタン () を押したときにプロパティが表示されるホストは、選択中のインタフェースが属すホストです。
ツールバーのカスタマイズの方法について、詳しくは「1.1.1　ツールバー」 (6 ページ) を参照してください。

現れた「ホストのプロパティ」ダイアログを図 5-2 に示します。

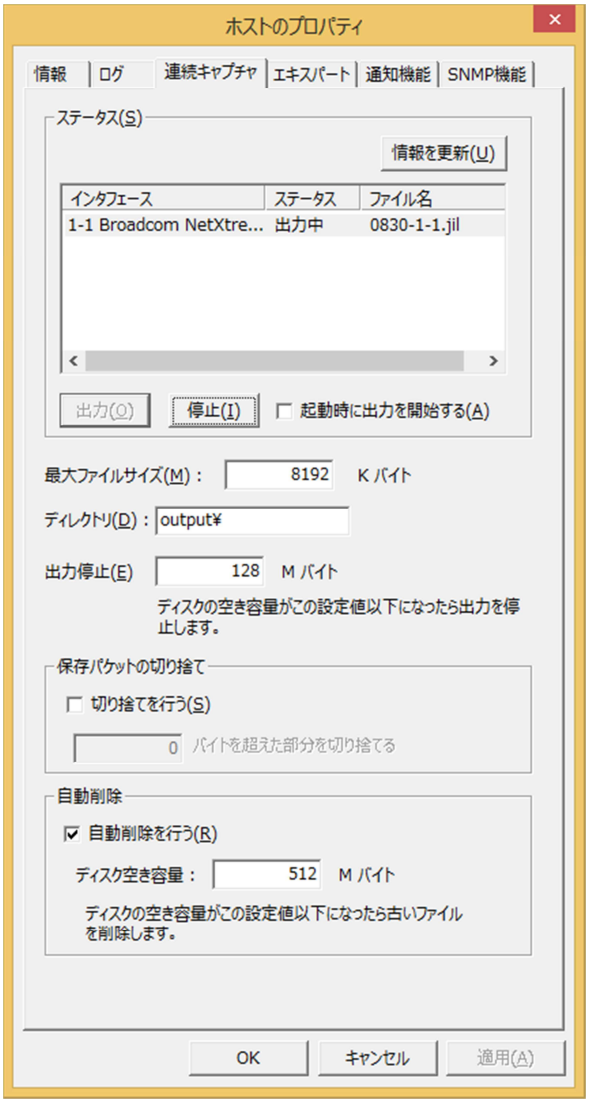


図 5-2: 「ホストのプロパティ」ダイアログ (連続キャプチャ)

2. **ステータス(S)** 領域で「停止」と表示されているインタフェースを選び、**出力(O)** ボタンをクリックします。
   ステータスが「出力中」に変わり、選んだインタフェースでキャプチャが開始されます。
3. **OK** ボタンをクリックして「ホストのプロパティ」ダイアログを閉じます。

連続キャプチャしたデータを保存するファイルのフォーマットは、 ASTEC Eyes 独自のもので、拡張子は.jil です。保存するファイル名を指定することはできません。**ステータス(S)** 領域のファイル名のカラムに、出力中のファイル名を表示します。

「ホストのプロパティ」ダイアログの「連続キャプチャ」のページの **ステータス(S)** 領域に表示される情報は、自動的には更新されません。最新の情報を見たい場合は、**情報を更新(U)** ボタンをクリックしてください。

ファイルに出力したキャプチャデータは、拡張子.enc や.ebz のファイルと同じように、デコード機能を使って解析できます。

ファイルにデータを出力している途中、**最大ファイルサイズ(M)** に指定した大きさに達したら、次のファイルを作ります。また、指定した大きさに達しなくても、日付が変わったら、次のファイルを作ります。

5.3.2 連続キャプチャを停止する

連続キャプチャの停止はインタフェースごとに行います。

1. 「ホストのプロパティ」ダイアログを開きます (図 5-2 参照)。
2. **ステータス(S)** 領域で「出力中」と表示されているインタフェースを選び、**停止(I)** ボタンをクリックします。
   ステータスが「停止」に変わり、選んだインタフェースで連続キャプチャが停止します。
3. **OK** ボタンをクリックして「ホストのプロパティ」ダイアログを閉じます。

5.3.3 連続キャプチャの設定を行う

連続キャプチャに関する設定は、ホストごとに行います。

1. 「ホストのプロパティ」ダイアログを開きます (図 5-2 参照)。
2. 自動開始するかどうかを指定します。
   起動時に連続キャプチャを自動的に開始するには、**起動時に出力を開始する(A)** にチェックを付けます。
3. **最大ファイルサイズ(M)** に、キャプチャしたデータを出力するファイルの大きさの上限を入力します。
   最大ファイルサイズに指定できる値の範囲は、 $1024 \leq$ 値 $\leq 65536\,(K$バイト$)$ です。ファイルにデータを出力している途中で、指定された大きさに達したら、次のファイルを作ります。

4. **ディレクトリ(D)** に、ファイルを保存するディレクトリを入力します。
   ASTEC Eyes 基本パッケージ および Windows 用のリモートモジュールの場合は、インストールしたディレクトリからの相対パスで指定します。ディレクトリはあらかじめ作っておかなければなりません。また、このディレクトリは ASTEC Eyes またはリモートモジュールをインストールしたディレクトリのサブディレクトリである必要があります。
   ASTEC Eyes が動作しているローカルなホスト (localhost) および Windows 用のリモートモジュールの場合、デフォルトのディレクトリは `output` です。デフォルトのディレクトリはインストール時に作成されます。
   UNIX 用のリモートモジュールの場合は設定ファイルで設定します。詳しくは『ASTEC Eyes UNIX 版リモートモジュールマニュアル』を参照してください。
5. 自動停止させるハードディスクの空き容量 (残量) を指定します。
   連続キャプチャしている間、 ASTEC Eyes またはリモートモジュールが動作している PC のハードディスクの空き容量は減り続けます。ハードディスクの空き容量がなくなるまでキャプチャし続けるのは、好ましくありません。そのため、 ASTEC Eyes はハードディスクの空き容量が**出力停止(E)** に指定された値より少なくなったら、連続キャプチャを自動的に停止します。
   デフォルトは 128M バイトです。 10M バイト以上の値を指定します。
6. パケットの先頭部分のみを保存するかどうかを指定します。
   大量のトラフィックがある一方、パケットの保存に使えるハードディスクの容量が限られている場合には、各パケットの詳細な情報が失われても長期間の (多数の) パケットを保存して概要の情報を得たいことがあるでしょう。
   パケットの先頭部分のみ保存するには、**切り捨てを行う(S)** にチェックを付けて、その下にパケットの切り捨てを行う位置をバイト数で指定します。
   切り捨て位置の下限は 68 バイトです。パケットの先頭部分が 68 バイト以上あれば、発振元、送信先、アプリケーションプロトコルなどの情報がわかるでしょう。
7. 自動削除するかどうかを指定します。
   ハードディスクの空き容量が指定した値以下になったら、古い連続キャプチャファイルを削除して、連続キャプチャが停止しないようにできます。自動削除を行わない場合は、ハードディスクの空き容量が**出力停止(E)** に指定した値以下になったら連続キャプチャは停止します。
   自動削除する場合は、**自動で削除する(R)** にチェックを付けて、**ディスク空き容量**に削除を開始するディスクの空き容量を入力します。 20M バイト以上の値を指定します。
8. **OK** ボタンをクリックして「ホストのプロパティ」ダイアログを閉じます。

古い連続キャプチャファイルを削除して、連続キャプチャし続けるためには、**出力停止(E)** の値より大きい値を**ディスク空き容量**に指定しなければなりません。小さい値を設定すると、削除が始まる前に連続キャプチャが停止してしまいます。

自動削除を設定して、連続キャプチャが停止しないようにしておいても、 ASTEC Eyes 以外のアプリケーションがハードディスク容量を消費してしまい、出力停止のハードディスク容量以下になった場合は、連続キャプチャは停止します。

5.4 フィルタを使う

通常のキャプチャ、およびリアルタイムデコードキャプチャに対しては、**キャプチャフィルタ**、**キャプチャ開始トリガ**、**キャプチャ停止トリガ**の 3 種類のフィルタが用意されています。連続キャプチャに対しても同様に、**連続キャプチャフィルタ**、**連続キャプチャ開始トリガ**、**連続キャプチャ停止トリガ**、の 3 種類のフィルタが用意されています。

それぞれのフィルタの条件はフィルタエディタで設定します。

フィルタエディタを起動するには、メインウィンドウの**編集(E)** メニューから**フィルタエディタ(E)**. . . を選ぶか、 **<Ctrl-E>** キーを押します。フィルタエディタの詳しい使い方については、9 章「フィルタエディタ」 (195 ページ) を参照してください。

5.4.1 キャプチャフィルタを使う

基幹ネットワークなど、さまざまなパケットが大量に流れるネットワークでキャプチャするような場合、多くの不必要なパケットをキャプチャすることになるでしょう。また、たくさんのデータが流れるのにキャプチャバッファの大きさは限られているので、欲しいデータをキャプチャし損なうかもしれません。そのような場合、**キャプチャフィルタ**を設定すれば、欲しいパケットだけをキャプチャできます。

キャプチャフィルタの条件はフィルタエディタでインタフェースごとに設定します。

キャプチャフィルタを設定したら、キャプチャを開始します。キャプチャフィルタの論理式が真となるパケットだけがキャプチャされます。

フィルタエディタで論理式を定義する方法については、9 章「フィルタエディタ」 (195 ページ) を参照してください。
トラフィックウィンドウに表示されているグラフアイテムやデコードビューのサマリ領域の行、アドレス帳の行などをドラッグして、フィルタエディタにドロップすることにより、論理式を自動的に生成することもできます。詳しくは「9.6　論理式を自動的に生成する」 (223 ページ) を参照してください。

5.4.2 キャプチャ開始トリガを使う

ある特定のパケットがネットワークに流れたことなどをきっかけにして、キャプチャを開始できます。このきっかけを定義する論理式のことを**キャプチャ開始トリガ**と呼びます。

キャプチャ開始トリガの条件はフィルタエディタでインタフェースごとに設定します。

キャプチャ開始トリガを設定したら、キャプチャを開始します。定義した論理式が真になるまではキャプチャは行われず、キャプチャバッファメーターに「待機中」と表示されます。論理式が真となってキャプチャが始まると、「待機中」の文字は消え、キャプチャバッファに取り込まれたバイト数が表示されます。

キャプチャ開始のきっかけとなったパケットもキャプチャされます。

5.4.3 キャプチャ停止トリガを使う

ある特定のパケットがネットワークに流れたことなどをきっかけにして、キャプチャを停止できます。このきっかけを定義する論理式のことを**キャプチャ停止トリガ**と呼びます。

キャプチャ停止トリガの条件はインタフェースごとにフィルタエディタで設定します。

キャプチャ停止トリガを設定したら、キャプチャを開始します。定義した論理式が真になるまではキャプチャ停止トリガを設定していない場合と同じようにキャプチャが行われるので、キャプチャバッファメーターの表示はキャプチャバッファに取り込まれたバイト数に従って変わります。論理式が真になると、自動的にキャプチャが停止します。

キャプチャ停止のきっかけとなったパケットもキャプチャされます。

5.4.4 連続キャプチャフィルタを使う

連続キャプチャフィルタを設定すれば、欲しいパケットだけを連続的にキャプチャできます。

連続キャプチャフィルタの条件はフィルタエディタでインタフェースごとに設定します。連続キャプチャフィルタを設定したら、連続キャプチャを開始します。連続キャプチャフィルタの論理式が真となるパケットだけがキャプチャされます。

フィルタエディタで論理式を定義する方法については、9 章「フィルタエディタ」 (195 ページ) を参照してください。
トラフィックウィンドウに表示されているグラフアイテムやデコードビューのサマリ領域の行、アドレス帳の行などをドラッグして、フィルタエディタにドロップすることにより、論理式を自動的に生成することもできます。詳しくは「9.6　論理式を自動的に生成する」 (223 ページ) を参照してください。

5.4.5 連続キャプチャ開始トリガを使う

ある特定のパケットがネットワークに流れたことなどをきっかけにして、連続キャプチャを開始できます。このきっかけを定義する論理式のことを**連続キャプチャ開始トリガ**と呼びます。

連続キャプチャ開始トリガの条件はフィルタエディタでインタフェースごとに設定します。連続キャプチャ開始トリガを設定したら、連続キャプチャを開始します。定義した論理式が真になるまではキャプチャは行われず、「ホストのプロパティ」ダイアログの「連続キャプチャ」のページの **ステータス(S)** 領域には、「待機中」と表示されます。

キャプチャ開始のきっかけとなったパケットもキャプチャされます。

「ホストのプロパティ」ダイアログの「連続キャプチャ」のページの **ステータス(S)** 領域に表示される情報は、自動的には更新されません。最新の情報を見たい場合は、**情報を更新(U)** ボタンをクリックしてください。

5.4.6 連続キャプチャ停止トリガを使う

ある特定のパケットがネットワークに流れたことなどをきっかけにして、連続キャプチャを停止できます。このきっかけを定義する論理式のことを**連続キャプチャ停止トリガ**と呼びます。

連続キャプチャ停止トリガの条件はインタフェースごとにフィルタエディタで設定します。連続キャプチャ停止トリガを設定したら、連続キャプチャを開始します。定義した論理式が真になるまでは連続キャプチャ停止トリガを設定していない場合と同じようにキャプチャが行われるので、「ホストのプロパティ」ダイアログの「連続キャプチャ」のページの **ステータス(S)** 領域には、「出力中」と表示されます。論理式が真になると、自動的に連続キャプチャが停止します。

キャプチャ停止のきっかけとなったパケットもキャプチャされます。

「ホストのプロパティ」ダイアログの「連続キャプチャ」のページの **ステータス(S)** 領域に表示される情報は、自動的には更新されません。最新の情報を見たい場合は、**情報を更新(U)** ボタンをクリックしてください。

5.5 キャプチャデータインディケータを表示する

キャプチャバッファやリアルタイムデコードビューに保持されているデータのうち、最も古いパケットをキャプチャした時刻と最新のパケットをキャプチャした時刻の範囲をトラフィックウィンドウに表示できます。また、連続キャプチャで保存されているデータのうち、最も古いパケットをキャプチャした時刻と最新のパケットをキャプチャした時刻の範囲をログのトラフィックウィンドウに表示できます。これをキャプチャデータインディケータと呼びます。

キャプチャデータインディケータを表示させる方法は 2 通りあります。

- トラフィックウィンドウのツールバーの**キャプチャデータインディケータ**ボタン( ) をクリックします。
- トラフィックウィンドウを右クリックしてポップアップメニューを開き、**キャプチャデータインディケータ(A)** を選びます。

キャプチャデータインディケータの現れたトラフィックウィンドウを図 5-3 に示します。グラフの上部に表示されたキャプチャデータインディケータは、青い斜線の期間にキャプチャしたデータがキャプチャバッファにあることを示しています。

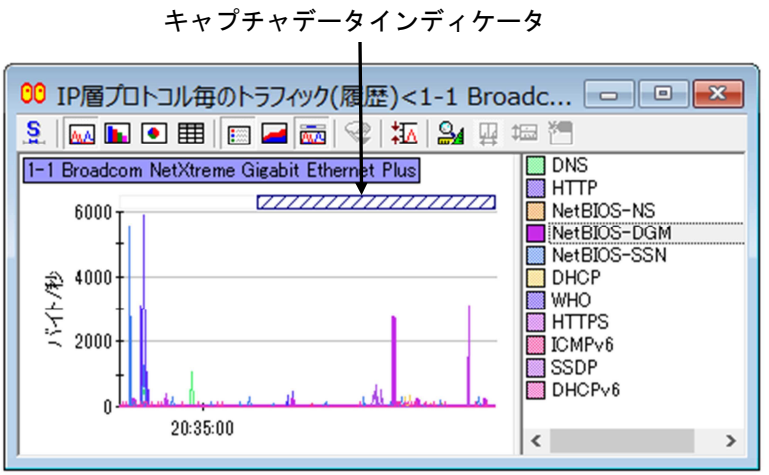


図 5-3: キャプチャデータインディケータの現れたトラフィックウィンドウ

クイックリターン機能を使うときなど、キャプチャデータインディケータを表示しておけば、**クイックリターン**ボタン( ) をクリックする目安になるでしょう。

5.6 キャプチャ時間を同期する

ネットワークトラブルの解析を行うときに、ネットワークの異なる場所でキャプチャしたデータを比較して、ネットワークのどこで問題が起こっているか調べたい場合があるでしょう。

このときキャプチャしたパケットに付与される時間 (キャプチャ時間と呼ぶことにします) の基準がキャプチャした場所によって異なると、別の場所でキャプチャされた同じパケットを対応付けることが困難になります。

そのため、キャプチャしたパケットの時間を GUI 部の動作する PC のシステム時間と同期して、パケットの対応をわかりやすくすることができます。その方法は 2 通りあります。

- インタフェースセレクタウィンドウのホストのエントリを右クリックすると表示されるメニューから**キャプチャ時間を同期(Y)** を選びます。
  この操作には設定権限が必要です。
- インタフェースセレクタウィンドウ内の何も表示されていない部分を右クリックすると表示されるメニューから**キャプチャ時間を同期(Y)** を選びます。
  接続中で設定権限のあるすべてのリモートモジュールおよびキャプチャ部について、キャプチャ時間を同期します。

この同期を解除して元の状態に戻すには、上と同じメニューで**キャプチャ時間の同期を解除(R)** を選びます。この操作にも設定権限が必要です。

時間の差がどのくらいあるか見るためには、上と同じメニューで**キャプチャ時間を取得(T)** を選びます。設定権限は必要ありません。

GUI が動作する PC でのキャプチャ時間も、その PC のシステム時間と一致しているとは限らないので、必要に応じて同期します。
この不一致は、複数のパケットのキャプチャ時間の差を正確に表示することを優先するため生じます。

GUI 付属のキャプチャ部および Windows 系 OS のリモートモジュールは、次の場合にキャプチャ時間をそれぞれが動作する PC のシステム時間に同期します。

- PC のシステム時間がステップモードで変更された場合
  ステップモードでは、時間の変更を徐々にではなく瞬時に行います。
- Windows が提供する高分解能パフォーマンスカウンタがラップした場合
  高分解能パフォーマンスカウンタは 64 ビットのカウンタですが、分解能が 3 MHz 前後 (PC により異なります) のため、一定の期間ごとにオーバーフローして 0 に戻ります。

リモートモジュールの場合は、接続している GUI が動作する PC のシステム時間との同期が解除されることになるので、再度同期する必要が生じます。

6章

デコード機能

キャプチャデータを解析する機能です。 データを解析することをデコードと呼びます。

パケットを一つずつ、どのようなプロトコルから構成されているかを解析し、それぞれのプロトコルに基づいてデータを解釈した結果を**リアルタイムデコードビュー**や**デコードビュー**に表示します。また、特に TCP プロトコルの上位層のプロトコルについては、 TCP ストリームを再構成して解析する機能があります。その結果は**ストリームビュー**に表示します。

6.1 デコードを行う

6.1.1 リアルタイムでデコードする

キャプチャしながら即座にデコードすることを、**リアルタイムデコード**と呼びます。リアルタイムデコードはローカルホストのインタフェースに対してのみ実行できます。

リアルタイムデコードを実行するには、あらかじめ「11.1 キャプチャのオプションを設定する」 (283 ページ) に従ってリアルタイムデコードの設定を行ったうえで、インタフェースを選び、リアルタイムデコードキャプチャを実行します。

リアルタイムデコードキャプチャを実行する方法は 3 通りあります。

- メインウィンドウの**キャプチャ(C)** メニューから **キャプチャ開始(S)** を選びます。
- メインウィンドウのインタフェースツールバーの**キャプチャ開始**ボタン( ) をクリックします。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**キャプチャ開始(S)** を選びます。

リアルタイムデコードキャプチャを開始するとリアルタイムデコードビューが表示され、キャプチャ中のデータの解析結果が自動的に表示されます。

リアルタイムデコードビューを閉じてもリアルタイムデコードキャプチャ中はデータをキャプチャし続けます。次の操作のいずれかを行うと再度リアルタイムデコードビューが開きます。このとき、閉じている間にキャプチャしたデータの解析結果も表示します。

- メインウィンドウの**キャプチャ(C)** メニューから**リアルタイムデコードビュー(V)** を選びます。
- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**リアルタイムデコードビュー(V)** を選びます。

6.1.2 キャプチャバッファのデータをデコードする

キャプチャバッファは、インタフェースごとに用意されているので、あらかじめインタフェースを選んでおきます。キャプチャバッファのデータをデコードする方法は 3 通りあります。

- メインウィンドウのインタフェースツールバーの**デコードビュー**ボタン( ) をクリックします。
- メインウィンドウの**キャプチャ(C)** メニューから**デコードビュー(N)** を選びます。

- インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**デコードビュー(N)** を選びます。

6.1.3 キャプチャファイルをデコードする

キャプチャファイルを開いてデコードする方法は 5 通りあります。

- メインウィンドウのコモンツールバーの**キャプチャデータを開く**ボタン() をクリックします。
  「開く」ダイアログが現れるので、デコードしたいファイルを指定します。
- メインウィンドウの**ファイル(F)** メニューから**キャプチャデータを開く(O)**. . . を選びます。
  「開く」ダイアログが現れるので、デコードしたいファイルを指定します。
- **<Ctrl-O>** キーを押します。
  「開く」ダイアログが現れるので、デコードしたいファイルを指定します。
- Windows のエクスプローラやフォルダからデコードしたいファイルのアイコンをドラッグして、 ASTEC Eyes のメインウィンドウにドロップします。
- Windows のエクスプローラやフォルダで、デコードしたいファイルのアイコンをダブルクリックします。この方法は、ファイルの拡張子が `.enc`、`.ebz`、`.jil`、`.cap` の場合に使えます。

開いてデコードできるファイルのフォーマットは、次のとおりです。

表 6-1: デコードできるファイルのフォーマット

ファイルのフォーマット	ファイルの拡張子
Sniffer 互換の非圧縮フォーマット	`.enc`、`.cap`
Sniffer 互換の圧縮フォーマット	`.enc`
Sniffer 互換の非圧縮フォーマットのファイル (拡張子 `.enc`) を bzip2 で圧縮したもの	`.ebz`、`.enc.bz2`
連続キャプチャの出力ファイル	`.jil`
連続キャプチャの出力ファイルを bzip2 で圧縮したもの	`.jil.bz2`
Microsoft Network Monitor 互換の非圧縮フォーマット	`.cap`
WildPackets EtherPeek 互換フォーマット	`.pkt`
Novell LANalyzer 互換フォーマット	`.tr1`
tcpdump の出力ファイル (libpcap のバージョン 2 以降)	不定
snoop の出力ファイル	不定

次のフォーマットのファイルについては、 bzip2 コマンドで圧縮したもの (拡張子.bz2) も開いてデコードできます。

- Sniffer 互換の非圧縮フォーマット (拡張子 .enc.bz2)
- 連続キャプチャの出力ファイル (拡張子 .jil.bz2)
- tcpdump の出力ファイル
- snoop の出力ファイル

サイズの大きなファイルについては、キャプチャデータマネジャーを使って、その一部だけをデコードすることもできます。詳しくは「6.10　キャプチャデータマネジャーを使う」 (159 ページ) を参照してください。

非圧縮のキャプチャファイルについては、メモリマップドファイルを使って、スワップ領域を圧迫することなくデータを読み込みます。圧縮したキャプチャデータがメモリ不足によりデコードできない場合は、ファイルを展開した後に読み込むとデコードできることがあります。

Windows Vista および Windows 7 では、 UAC がオンの場合はドラッグアンドドロップによるデコードを行うことはできません。
Windows 8.1 および Windows 10 では、 UAC の設定を最低にしてもドラッグアンドドロップによるデコードを行うことはできません。
キャプチャファイルをダブルクリックする、ポップアップメニューから「開く」などの別の方法を使ってください。

6.2 リアルタイムデコードの結果を見る

6.2.1 リアルタイムデコードビューの表示

図 6-1 にリアルタイムデコードビューを示します。

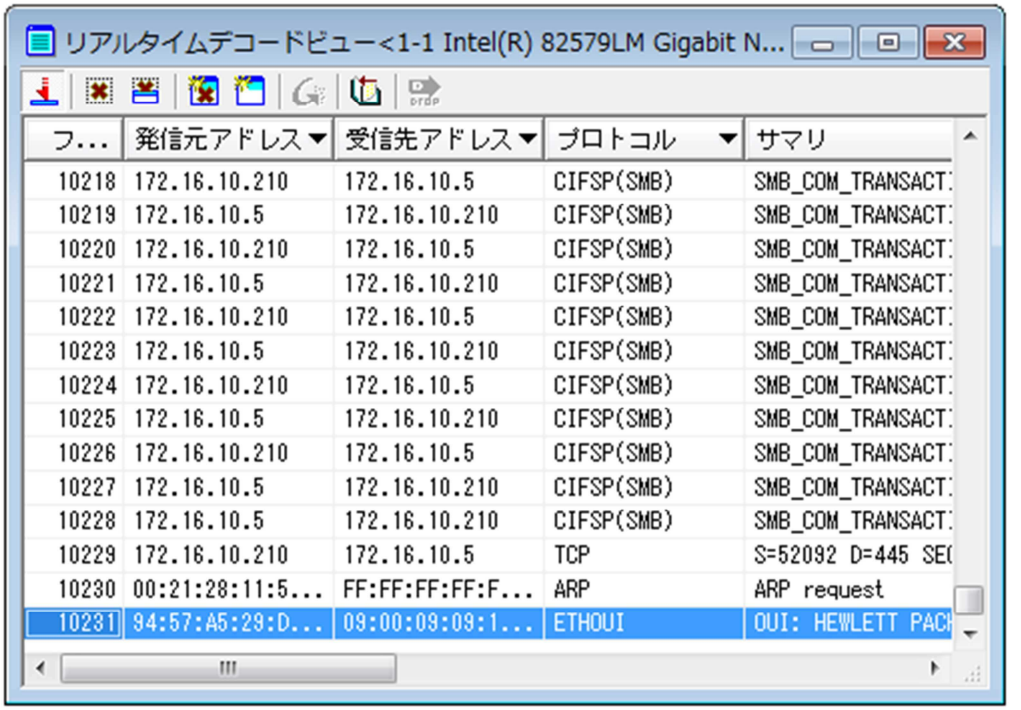


図 6-1: リアルタイムデコードビュー

リアルタイムデコードビューはパケットの概要を表示します。 1 行は 1 パケットに対応し、キャプチャ中のパケットの解析結果は順にウィンドウの最後に追加されます。

ツールバーの**最新のパケットを選択**ボタン( ) をクリックすると、常にリアルタイムデコードビューの最後のパケットを選択した状態になり、最新の解析結果を表示し続けます。

リアルタイムデコードビューは次のカラムから構成されています。

表 6-2: リアルタイムデコードビューのカラム

カラム名	表示する内容
フレーム ID	パケットの ID を表します。先頭を 0 とした連番です。
発信元アドレス 受信先アドレス	パケットの構成に IPv4 または IPv6 が含まれている場合は、 IP アドレスを、そうでない場合は MAC アドレスを表示します。アドレスに対応するホスト名が見つかっていて、ホスト名を使うように設定している場合は、ホスト名を表示します。
プロトコル	最上位層 (最もアプリケーション寄りの層) のプロトコル名を表示します。
サマリ	最上位層のプロトコルをデコードした結果の要約を表示します。
長さ	パケットの長さです。 MAC 層の CRC フィールド (4 バイト) は除いた値です。
相対時間	このパケットをキャプチャした時刻と、フレーム ID 0 のパケットをキャプチャした時刻の差を表示します。
デルタ時間	このパケットをキャプチャした時刻と、 1 行上のパケットをキャプチャした時刻の差を表示します。
時刻	パケットをキャプチャした時刻です。
発信元ポート番号 受信先ポート番号	パケットの構成に TCP または UDP のプロトコルが含まれている場合に、 TCP または UDP のポート番号を表示します。

6.2.2 カラムのカスタマイズ

リアルタイムデコードビューのカラムや、デコードビュー、ストリームビューおよびパケット編集ウィンドウのサマリ領域のカラムはカスタマイズできます。表示するカラムを指定したり、カラムの順番を変えたりすることができます。

ポップアップメニューを使ってカラムを指定する

1. 見出しを右クリックします。
   図 6-2 に示すような、カラムの一覧をメニュー項目とするポップアップメニューが現れます。

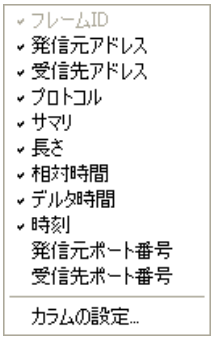


図 6-2: リアルタイムデコードビューの見出しから現れるポップアップメニュー

   チェックの付いているカラムがリアルタイムデコードビューに表示されています。
2. カラムに対応するメニュー項目はトグルになっています。カラムに対応するメニュー項目を選んで、チェックを付けたり外したりします。
   ただし、フレーム ID カラムを隠すことはできません。

手順 1 と 2 を繰り返して、望みのカラムがすべて表示されるようにします。

「カラムの設定」ダイアログを使ってカラムを指定する

1. 見出しを右クリックしてポップアップメニューを開き、**カラムの設定**... を選びます。
   図 6-3 のような「カラムの設定」ダイアログが現れます。

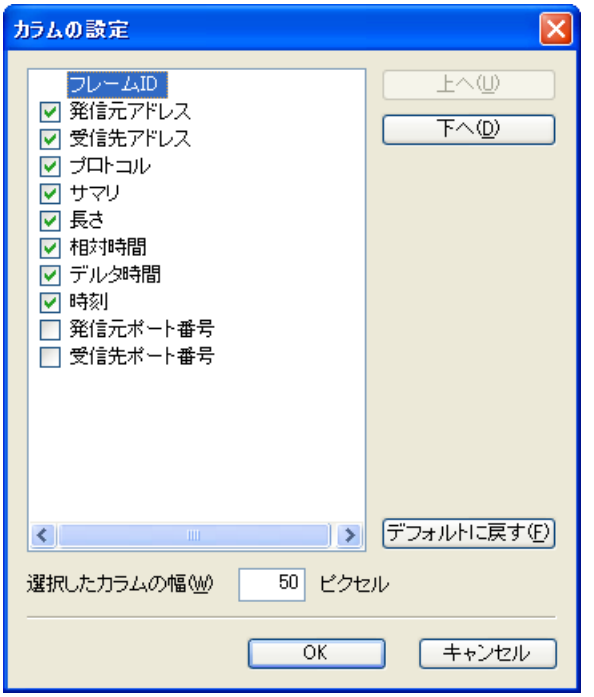


図 6-3: 「カラムの設定」ダイアログ

2. 表示したいカラムにチェックを付け、隠したいカラムからチェックを外します。
   ただし、フレーム ID からチェックを外すことはできません。
   デフォルトに戻す(F) ボタンをクリックすると、デフォルトに戻ります。
   選択したカラムの幅(W) に値を入力してカラムの幅を指定することもできます。

マウス操作でカラムの順番を変える

1. マウスカーソルをカラムの見出しの中心付近に合わせ、マウスの左ボタンを押し下げます。
2. マウスのボタンを押したまま左右にドラッグして、カラムを移動します。

マウスカーソルは、カラムの見出しの中心あたりに合わせるようにします。カラムの端の方に合わせると、カラムの幅を変える操作のためのカーソルに変わります。

「カラムの設定」ダイアログを使ってカラムの順番を変える

1. 見出しを右クリックして、ポップアップメニューを開きます (図 6-2 参照)。
2. ポップアップメニューから**カラムの設定...** を選びます。
   図 6-3 のような「カラムの設定」ダイアログが現れます。
   左のカラムから順番に一覧表示されています。
3. 移動したいカラムをクリックしてます。
4. **上へ(U)** ボタンまたは**下へ(D)** ボタンをクリックして、順番を入れ替えます。
   デフォルトに戻す(F) ボタンをクリックすると、デフォルトに戻ります。
   選択したカラムの幅(W) に値を入力してカラムの幅を指定することもできます。

6.2.3 詳細なデコード結果を表示する

リアルタイムデコードビューで表示されるのはパケットの概要です。より詳しい解析結果はデコードビューで見ます。デコードビューを開く方法は 2 通りあります。

- リアルタイムデコードビューのツールバーの**デコードビュー表示**ボタン() をクリックします。
- リアルタイムデコードビューのツールバーの**デコードビュー表示 (パケット削除)** ボタン() をクリックします。

デコードビュー表示 (パケット削除) ボタン() はデコードビューを開いたときに、リアルタイムデコードビューのデータは削除します。

6.2.4 リアルタイムデコードビューのデータの削除

リアルタイムデコードビューに表示されているデータを削除する方法は 3 通りあります。

- リアルタイムデコードビューのツールバーの**全パケット消去**ボタン() をクリックします。
  リアルタイムデコードビューのすべてのデータが削除されます。

- リアルタイムデコードビューのパケットの行をクリックしてから、ツールバーの**選択まで削除**ボタン() をクリックします。
  クリックした行も含めて、それよりも前の行のデータが削除されます。
- リアルタイムデコードビューのツールバーの**デコードビュー表示 (パケット削除)** ボタン() をクリックします。
  デコードビューが開き、リアルタイムデコードビューのすべてのデータが削除されます。

6.2.5 パケットの取りこぼしの表示

リアルタイムデコードはデータをいったんキャプチャバッファに取り込みます。ネットワークを流れるデータの量が多すぎて、デコードする前にキャプチャバッファがいっぱいになったときには、データの取りこぼしが発生します。

リアルタイムデコードビュー上では、取りこぼしたパケットの直後のパケットがオレンジ色にハイライト表示されます。また**次のドロップ**ボタン() をクリックすると、次のオレンジ色の行にフォーカスを移動します。

リアルタイムデコードで取りこぼしが起きる場合は、キャプチャバッファのサイズを大きくします。詳しくは「11.1 キャプチャのオプションを設定する」 (283 ページ) を参照してください。

6.3 デコードビューでデコード結果を見る

6.3.1 デコードビューの構成

図 6-4 にデコードビューを示します。

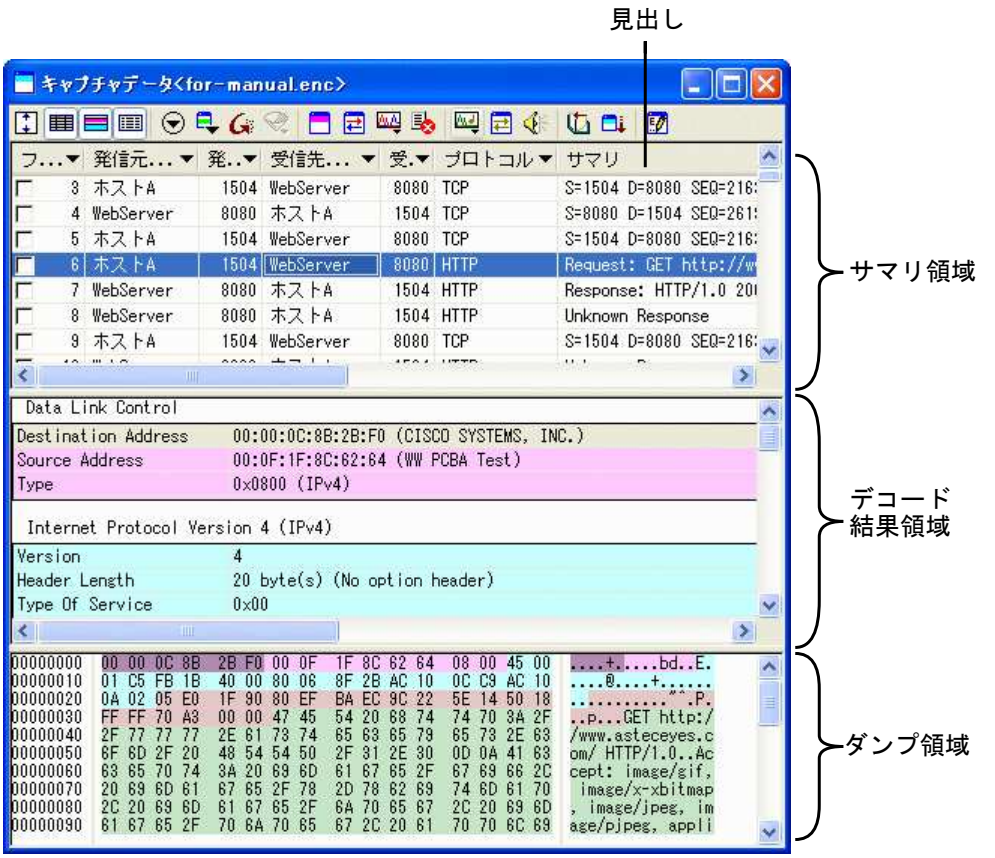


図 6-4: デコードビュー

デコードビューは、大きく 3 つの領域に分けられます。 **サマリ領域**と**デコード結果領域**と**ダンプ領域**です。 サマリ領域はパケットの概要を表示します。サマリ領域の 1 行は 1 パケットに対応します。デコード結果領域は、サマリ領域で選んだ行のパケットを解析した結果を表示します。ダンプ領域は、パケットのデータを 16 進ダンプの形式で表示します。

サマリ領域のカラムはリアルタイムデコードビューのカラムと同じです。詳しくは表 6-2を参照してください。

カラムの表示はリアルタイムデコードビューと同じようにカスタマイズできます。詳しくは「6.2.2　カラムのカスタマイズ」 (107 ページ) を参照してください。

6.3.2　パケットのデコード結果を見る

サマリ領域で見たいパケットの行をクリックします。クリックしたパケットを詳細に解析した結果がデコード結果領域に表示されます。

デコード結果領域の行をクリックすると、ダンプ領域の対応する部分が強調されます。逆にダンプ領域をクリックすると、対応するデコード結果領域の行が強調されます。

また、メインウィンドウのステータスバー (メインウィンドウの一番下の部分です) にも次の情報が表示されます。

- 選択中のパケットの行番号
- デコードビューに表示しているパケットの総数
- 選択中のパケットのフレーム ID
- 選択中のパケットの発信元と受信先のアドレス
- 選択中のパケットの最上位のプロトコル名

デコード結果領域に表示したフィールドや値の意味は、 RFC などプロトコルを定義しているドキュメントを参照してください。

デコードビューは、 1 パケットずつ解析します。 TCP 上のアプリケーションプロトコルの 1 レコードが複数のパケットに分割されているような場合、適切に解析できないことがあります。そのような場合は、ストリームビューを使ってください。

6.3.3　デコードヒントを使う

TCP または UDP の上位層のプロトコルのうち、プロキシサーバーの設定によって Well known ポートとは異なるポートを使っているプロトコルや、 Well known ポートを持たないプロトコルは、そのままでは正しくデコードできません。そのような場合はデコードヒントを設定します。 デコードヒントを設定する手順については、「11.3　デコードヒントを設定する」 (289 ページ) を参照してください。

表示されているデコードビューに設定したデコードヒントを反映するには、再デコードする必要があります。

再デコードを行う方法は 2 通りあります。

- デコードビューまたはストリームビューの**再デコード**ボタン() をクリックします。
- デコードビューまたはシーケンスモードでないストリームビューを右クリックしてポップアップメニューを開き、**再デコード(Q)** を選びます。

デコードヒントを設定できるのは、 TCP または UDP の上位層のプロトコルだけです。

6.3.4 見たいパケットへジャンプする

フレーム ID を指定して、見たいパケットへ移動できます。

1. 「ジャンプ」ダイアログを開きます。
   そのためには、 **<Ctrl-G>** キーを押すか、 デコードビューを右クリックしてポップアップメニューを開き、**ジャンプ(J)**. . . を選びます。
2. 目的のフレーム ID を入力して、 **<Enter>** キーを押すか、 **OK** ボタンをクリックします。

指定したフレーム ID へ移動します。

ストリームビューの場合はストリーム ID を指定します。指定したストリームの先頭のレコードへ移動します。

6.3.5 日本語のエンコードを変える

日本語の文字列を含むデータをデコードした場合、 ASTEC Eyes はデコード結果を日本語で表示します。通常、自動的にエンコードを判別しますが、短い文字列の場合など、エンコードの判別を誤ることがあります。このような場合エンコードを指定してデコードをやり直すことができます。

プロトコルとしてエンコードが固定されている場合は、エンコードは変えられません。この操作を行ってもデコード結果に影響は与えられません。

特定のパケットまたはレコードのエンコードを変える

1. デコードビューまたはストリームビューを右クリックしてポップアップメニューを開き、**日本語エンコード(C)** をポイントします。

2. サブメニューからエンコードを選びます。

デコードビューやストリームビューのどこを右クリックしてもメニューは現れますが、サマリ領域をクリックするときには注意が必要です。クリックした行が選ばれます。エンコードを変えたい行 (パケットまたはレコード) をクリックするようにします。

表示されているデータのエンコードを変える

選択中のパケットまたはレコードだけでなく、表示されている全データのエンコードを一度に変えられます。

1. デコードビューまたはストリームビューを右クリックしてポップアップメニューを開き、**日本語エンコード(C)** をポイントします。
2. **表示行を全て変更**をポイントします。
3. サブメニューからエンコードを選びます。

デコードビューやストリームビューにフィルタをかけるなどして、表示されているパケットやレコードが制限されている場合、表示されていないパケットやレコードのエンコードは変わりません。

ASTEC Eyes バージョン 7.2 がサポートしているエンコードは、 JIS、 EUC、 SJIS、および Unicode (UCS-2 と UTF-8) です。

6.3.6 キャプチャデータのプロパティを見る

キャプチャデータの

- ファイル名
- パケット数
- データ開始時刻
- データ終了時刻
- ファイルのフォーマット

を見ることができます。

そのためには、デコードビューを右クリックしてポップアップメニューを開き、**プロパティ(R)**. . . を選びます。

6.4 ストリームビューを使う

ストリームビューは、 TCP のパケットヘッダーの Sequence Number を基に、データを並べ替え、重複を省いて TCP ストリームを再構成し、上位層のプロトコルのデータを見やすく表示します。

ストリームビューを開く方法は 2 通りあります。

- デコードビューのツールバーの**ストリームビュー**ボタン( ) をクリックします。
- ストリームを再構成したいデコードビューを右クリックしてポップアップメニューを開き、**ストリームビュー(S)** を選びます。

6.4.1 ストリームビューの構成

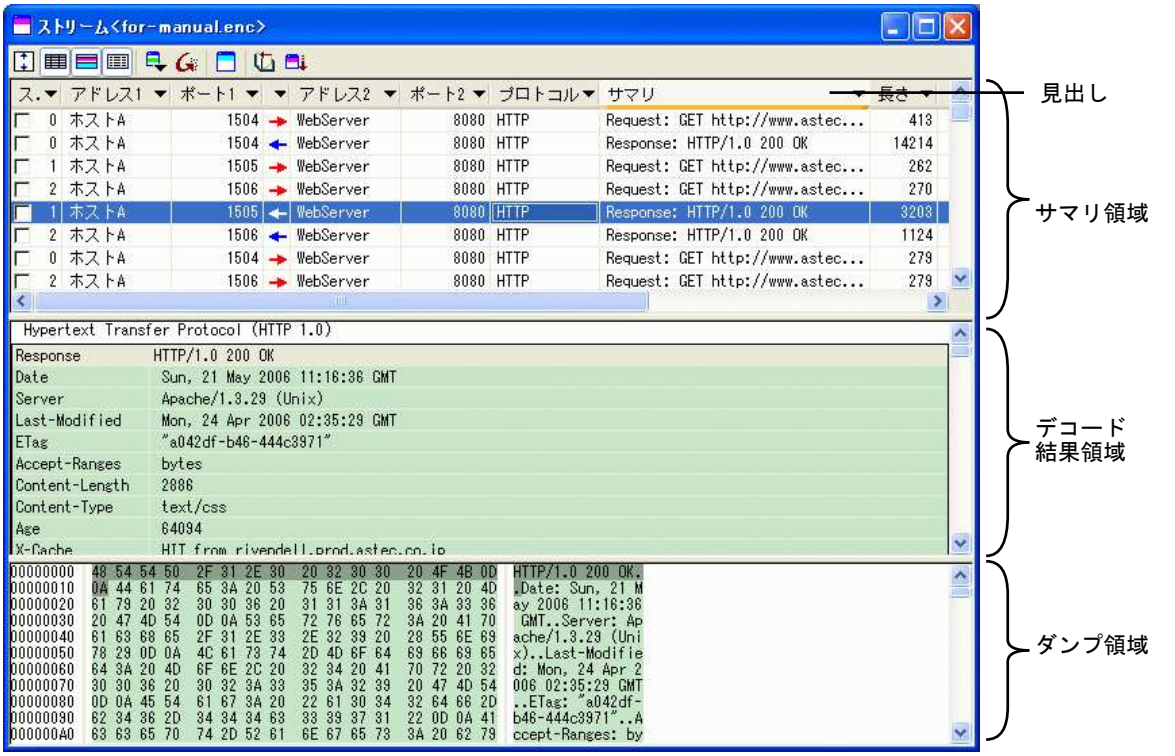


図 6-5: ストリームビュー

ストリームビューもデコードビューと同じように、大きく 3 つの領域に分けられます。**サマリ領域**と**デコード結果領域**と**ダンプ領域**です。 サマリ領域の 1 行は TCP の上位層のプロトコルが定義する 1 レコードに対応します。サマリ領域で選んだ行のレコードを解析した結果が、デコード結果領域に表示されます。また、レコードのデータを 16 進ダンプの形式で表したものをダンプ領域に表示します。

サマリ領域は次のカラムから構成されます。

表 6-3: ストリームビューのサマリ領域のカラム

カラム名	表示する内容
ストリーム ID	TCP のストリームごとに付けられた ID です。
アドレス 1 ポート 1 アドレス 2 ポート 2	ストリームの両端のアドレスとポート番号を表示します。
向き	アドレス 1 からアドレス 2 へ送信されたデータであるか、その逆であるかを矢印の向き (← 、→) で表示します。
プロトコル	ストリームの最上位層 (最もアプリケーション寄りの層) のプロトコル名を表示します。
サマリ	最上位層のプロトコルをデコードした結果の要約を表示します。
長さ	レコードの長さです。 TCP 層以下のプロトコルヘッダー長は含まれません。
相対時間	この行に表示されている時刻と、先頭行に表示されている時刻の差を表示します。
デルタ時間	この行に表示されている時刻と、 1 行上に表示されている時刻の差を表示します。
時刻	レコードを構成するパケットの中で、最初にキャプチャされたパケットのキャプチャ時刻を表示します。

カラムの表示はリアルタイムデコードビューやデコードビューと同じようにカスタマイズできます。詳しくは「6.2.2　カラムのカスタマイズ」 (107 ページ) を参照してください。

6.4.2 レコードのデコード結果を見る

サマリ領域の行をクリックします。クリックされたレコードを詳細にデコードした結果がデコード結果領域に表示されます。

また、デコードビューのサマリ領域では、クリックしたレコードを構成するパケットが緑色でハイライト表示されます。そのようすを図 6-6 に示します。

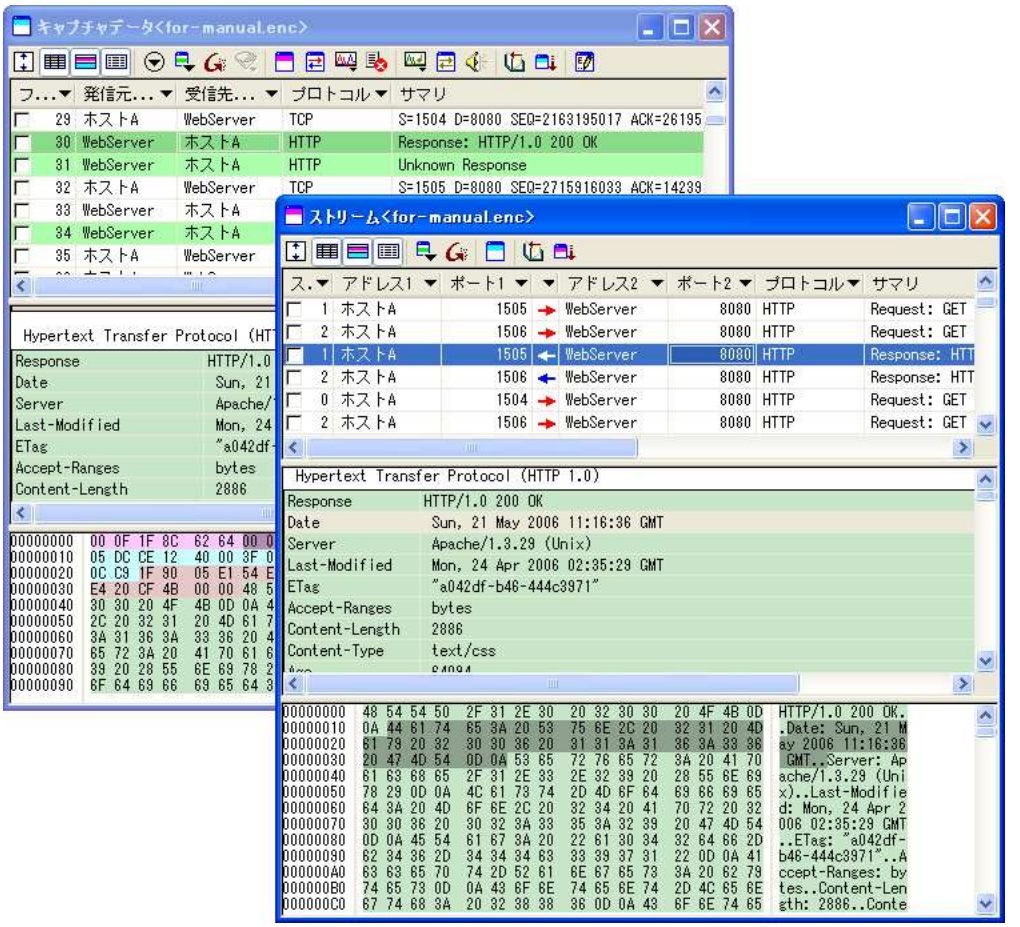


図 6-6: ストリームビューで選んだレコードと対応するパケット

デコード結果領域の行をクリックすると、ダンプ領域の対応する部分が強調されます。逆にダンプ領域をクリックすると、対応するデコード結果領域の行が強調されます。

メインウィンドウのステータスバーには次の情報が表示されます。

- 選択中のレコードの行番号
- ストリームビューに表示しているレコードの総数
- 選択中のレコードのストリーム ID
- 選択中のレコードの発信元と受信先のアドレス
- 選択中のレコードの最上位のプロトコル名

デコードビューのサマリ領域に緑色でハイライトされた行があるとき、フレーム ID カラムの見出しフィルタのメニューには、**緑色の行にチェックをつける(G)** というメニュー項目があります。**緑色の行にチェックをつける(G)** を選ぶと、ハイライトされた行にチェックをつけることができます。また、**<Shift>** キーを押しながら**緑色の行にチェックをつける(G)** を選ぶと、ハイライトされた行にチェックをつけ、チェックの付いた行だけを表示するようにフレーム ID カラムに見出しフィルタが適用されます。

6.4.3 特定のパケットが属すストリームだけを表示する

解析した結果から、あるパケットが属しているストリームだけを抜き出して見るには、デコードビューのサマリ領域で、着目するパケットの行を右クリックしてポップアップメニューを開き、**選択されたパケットのストリーム(P)** を選びます。

ストリームビューがまだ作られていない場合は、ストリームビューが作られ、着目したパケットが属すストリームだけを表示した状態で現れます。

すでにストリームビューがある場合は、着目したパケットの属しているストリームだけを表示した状態に変わります。

どちらの場合も、ストリームビューのストリーム ID カラムの文字列は、フィルタが適用されていることを示すために青で表示されます。

着目するパケットのストリームがない場合 (クリックしたパケットのトランスポート層のプロトコルが UDP である場合など) は、すべてのストリームを表示します。
表示する前に「ASTEC Eyes」ダイアログが現れて、フィルタをかけずにすべてのストリームを表示することを知らせます。ストリーム ID のカラムの文字列は黒で表示されます。

ストリームビューのレコードを、ストリーム ID 毎にまとめて表示することもできます。詳しくは「11.2　デコードのオプションを設定する」 (286 ページ) を参照してください。

6.4.4　特定のレコードを構成するパケットを見つける

レコードは 1 パケットだけから構成されていることもあれば、 10 パケットから構成されていることもあります。逆に、 1 パケットに 3 レコードが含まれていることもあります。

解析中にストリームビューで特定のレコードに着目し、そのレコードを構成するパケットを見つけたいことがあります。構成するパケットを見つける方法は、 2 通りあります。

- レコードを構成するパケットを見つける方法 1
  ストリームビューのサマリ領域で、着目するレコードの行を右クリックしてポップアップメニューを開き、**構成しているパケットを表示(P)** を選びます。
- レコードを構成するパケットを見つける方法 2

  1. ストリームビューのサマリ領域で、着目するレコードの行をクリックします。
  2. 対応するデコードビューをアクティブにします。
     デコードビューボタン( ) をクリックすると簡単です。
  3. **<Alt-↑>** キーまたは **<Alt-↓>** キーを押します。

選んだレコードを構成するパケットが緑色でハイライト表示されます。

6.4.5 ストリームを構成するパケットが欠けていた場合の表示

何らかの原因でストリームを構成するパケットが欠けていることがあります。

パケットの欠けたデータをデコードしたときのストリームビューのようすを図 6-7 に示します。

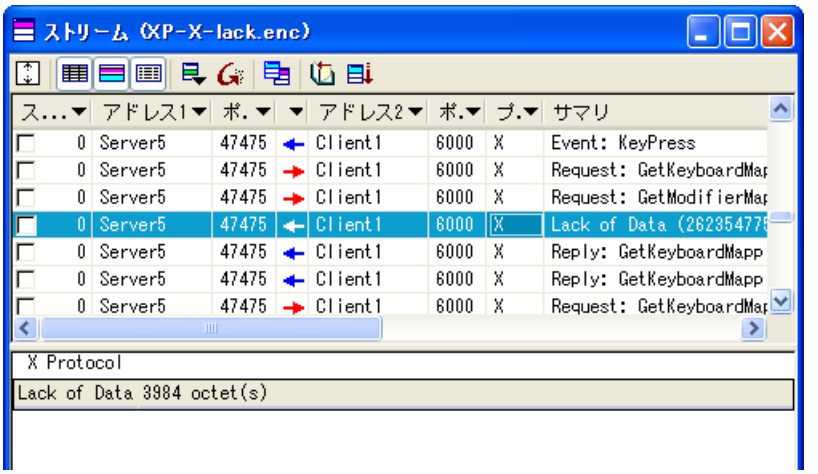


図 6-7: ストリームの欠けたデータを表示したストリームビュー

パケットの経路が変わった場合や、処理が間に合わずにパケットをキャプチャできなかった (ドロップした) 場合など、何らかの原因によってデータが本当に欠けたのではない場合でも、データが欠けていると表示されることがあります。
パケットは、 TCP のシーケンス番号順に到着するとは限りません。キャプチャを開始または停止したタイミングによって、途中のパケットが抜け落ちたキャプチャデータになってしまうことがあります。そのようなキャプチャデータをデコードすると、データが欠けていると表示されてしまいます。

パケットの欠けたデータは、正しくデコードできないことがあります。

6.5 ストリームビュー (シーケンスモード) を使う

ストリームビューは TCP ストリームを再構成し、上位層のプロトコルのデータをセッションごとにまとめて表示します。

ストリームビュー (シーケンスモード) を開く方法は 2 通りあります。

- デコードビューのツールバーの**ストリームビュー (シーケンスモード)** ボタン( ) をクリックします。
- ストリームを再構成したいデコードビューを右クリックしてポップアップメニューを開き、**ストリームビュー (シーケンスモード)(M)** を選びます。

6.5.1 ストリームビュー (シーケンスモード) の構成

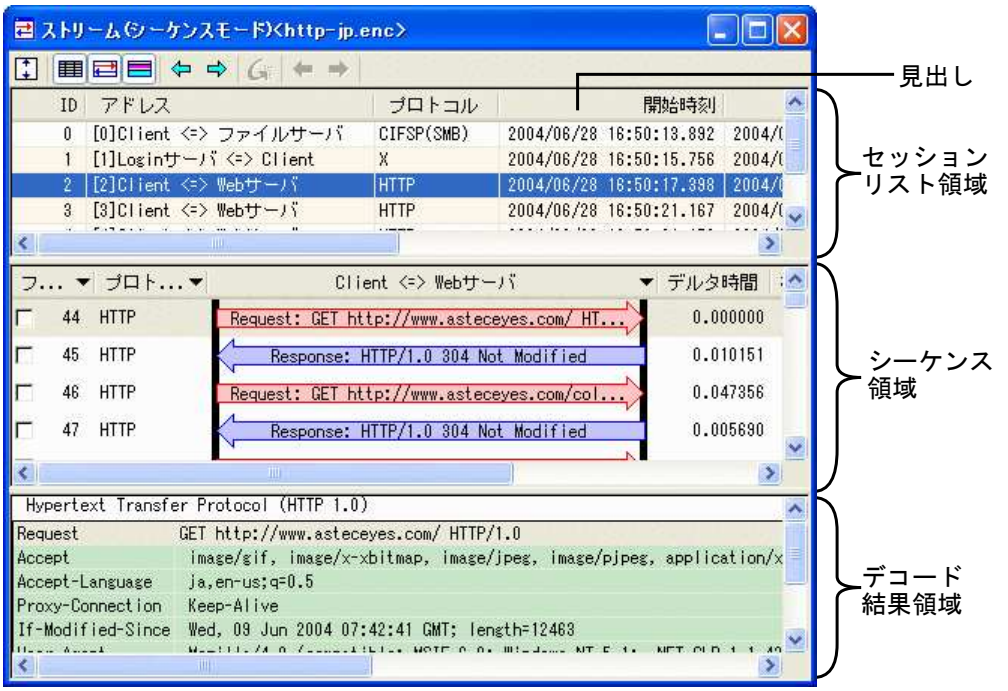


図 6-8: ストリームビュー (シーケンスモード)

ストリームビュー (シーケンスモード) は、**セッションリスト領域**、**シーケンス領域**、**デコー**

ド結果領域の 3 つの領域から構成されています。

セッションリスト領域には TCP のセッションの一覧が表示されます。セッションリスト領域の 1 行は 1 つのセッションに対応します。シーケンス領域にはセッションリスト領域で選んだセッションのシーケンスが表示されます。シーケンス領域の 1 行は TCP の上位層のプロトコルが定義する 1 レコードに対応します。シーケンス領域で選んだ行のレコードを解析した結果が、デコード結果領域に表示されます。

セッションリスト領域

セッションリスト領域は次のカラムから構成されます。

表 6-4: ストリームビュー (シーケンスモード) のセッションリスト領域のカラム

カラム名	表示する内容
ID	TCP のセッションごとに付けられた ID です。
アドレス	セッションに関わるホストをすべて表示します。
プロトコル	ストリームの最上位層 (最もアプリケーション寄りの層) のプロトコル名を表示します。
開始時刻	セッションの一番最初のパケットをキャプチャした時刻です。
終了時刻	セッションの一番最後のパケットをキャプチャした時刻です。
エラー	セッション中に含まれるエラーの数です。
警告	セッション中に含まれる警告ーの数です。
レコード数	セッション中に含まれるレコードの総数です。
情報	ASTEC Eyes バージョン 7.2 ではこのカラムに表示される情報はありません。

セッションリスト領域のカラムを非表示にしたり、順番を入れ替えたりすることはできません。

シーケンス領域

シーケンス領域は次のカラムから構成されます。

表 6-5: ストリームビュー (シーケンスモード) のシーケンス領域のカラム

カラム名	表示する内容
フレーム ID	レコードの先頭のパケットのフレーム ID です。
プロトコル	ストリームビューのプロトコルのカラムと同じです。
関連ホスト	セッションリスト領域のアドレスのカラムと同じです。セッションごとに見出しが変わります。
デルタ時間	この行に表示されている時刻と、 1 行上に表示されている時刻の差を表示します。
相対時間	この行に表示されている時刻と、先頭行に表示されている時刻の差を表示します。
時刻	レコードを構成するパケットの中で、最初にキャプチャされたパケットのキャプチャ時刻を表示します。
長さ	レコードの長さです。 TCP 層以下のプロトコルヘッダー長は含まれません。

デコード結果領域

シーケンス領域のレコードをクリックすると、そのレコードを詳細に解析した結果がデコード結果領域に表示されます。デコード結果領域に表示される内容は、ストリームビューのデコード結果領域に表示される内容と同じです。

6.5.2 セッションを選ぶ

ストリームビュー (シーケンスモード) でセッションを選ぶ方法は 4 通りあります。

- セッションリスト領域の対応する行をクリックします。
- ツールバーの**次のセッション**ボタン (⇨) または**ひとつ前のセッション**ボタン (⇦) をクリックします。
- シーケンス領域で右クリックしてポップアップメニューを開き、**次のセッション(N)** または **前のセッション(P)** を選びます。
- セッションリスト領域で、 **<↓>**、 **<↑>** を押すか、シーケンス領域で **<Ctrl-↓>**、 **<Ctrl-↑>** を押します。

6.5.3 ストリームビュー (シーケンスモード) とデコードビューの連携

セッションリスト領域でセッションを選ぶと、シーケンス領域にシーケンスが表示されると共に、デコードビューのサマリ領域ではセッションを構成するパケットがオレンジ色でハイライトされます。

そのようすを図 6-9 に示します。

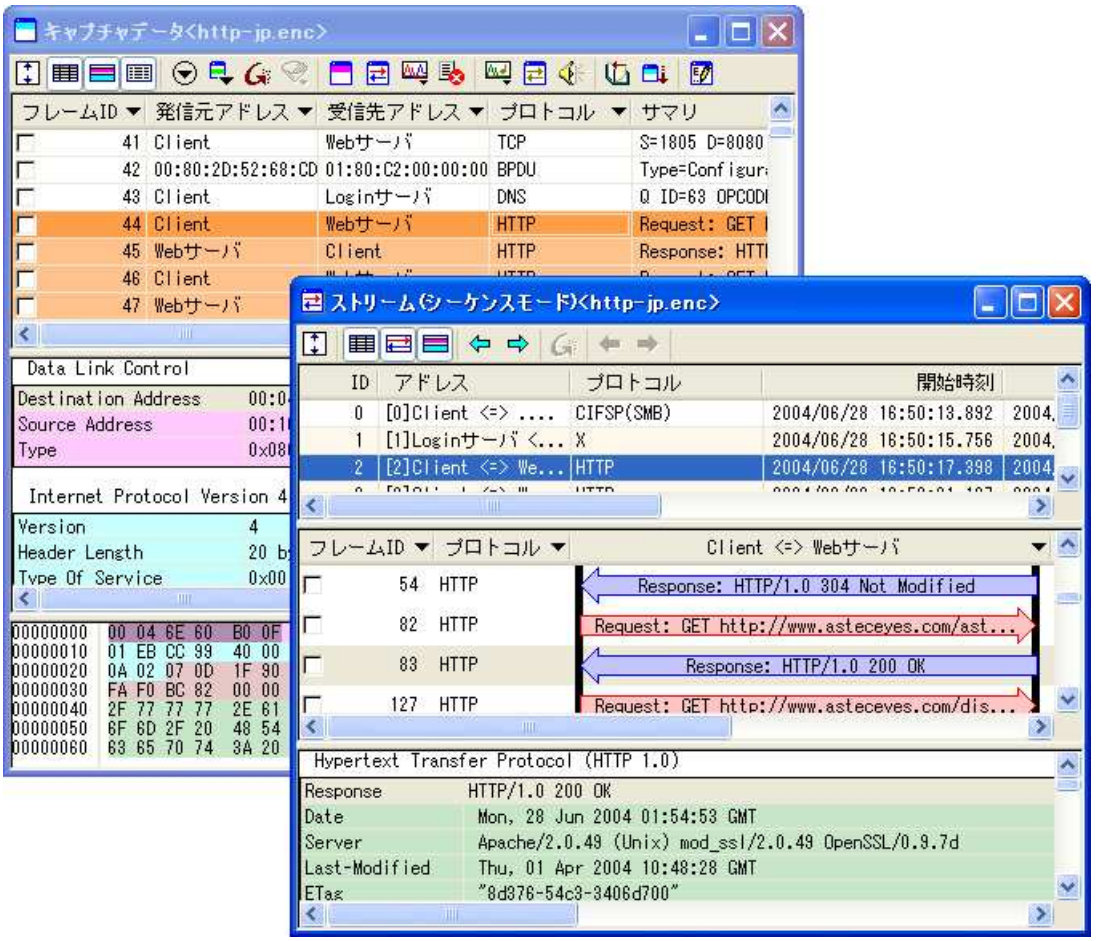


図 6-9: ストリームビュー (シーケンスモード) とデコードビュー

デコードビューのサマリ領域にオレンジ色でハイライトされた行があるとき、フレーム ID カラムの見出しフィルタのメニューには、**オレンジ色の行にチェックをつける(O)** というメニュー項目があります。**オレンジ色の行にチェックをつける(O)** を選ぶと、ハイライトされた行にチェックをつけることができます。また、 **<Shift>** キーを押しながら**オレンジ色の行にチェックをつける(O)** を選ぶと、ハイライトされた行にチェックをつけ、チェックの付いた行だけを表示するようにフレーム ID カラムに見出しフィルタが適用されます。

シーケンス領域の行をクリックすると、選んだレコードを構成するパケットが緑色でハイライト表示されます。

デコードビューのサマリ領域に緑色でハイライトされた行があるとき、フレーム ID カラムの見出しフィルタのメニューには、**緑色の行にチェックをつける(G)** というメニュー項目があります。**緑色の行にチェックをつける(G)** を選ぶと、ハイライトされた行にチェックをつけることができます。また、 **<Shift>** キーを押しながら**緑色の行にチェックをつける(G)** を選ぶと、ハイライトされた行にチェックをつけ、チェックの付いた行だけを表示するようにフレーム ID カラムに見出しフィルタが適用されます。

6.5.4 正しくデコードできないレコードを見つける

ストリームを構成するパケットが欠けているときや、誤ったデコードヒントを設定したときには、正しくデコードできないことがあります。

セッションに正しくデコードできないレコードが含まれているとき、セッションリスト領域の警告カラムにそのレコード数が表示され、警告行に移動することができます。

警告行に移動する方法は 3 通りあります。

- ツールバーの**次のエラー**ボタン (➡) または**前のエラー**ボタン (⬅) をクリックします。
- **<Alt-↓>** キーまたは **<Alt-↑>** キーを押します。
- シーケンス領域で右クリックしてポップアップメニューを開き、**次のエラー(T)** または**前のエラー(V)** を選びます。

6.5.5 シーケンス領域の関連ホストの順番を入れ替える

シーケンス領域の関連ホストに表示されるホストの順番を並べ替えることができます。

1. 黒い縦線にマウスカーソルを合わせます。
2. カーソルが左右に拡大 / 縮小用のもの (⟷) に変わったら、マウスの左ボタンを押し下げ、押したまま左 (右) に移動します。
3. 左 (右) の黒線を越えたところで、マウスボタンを離します。

6.6 フィルタを使う

膨大な数のパケットの中に見たいパケットがとびとびに現れる場合など、見たいパケットだけを表示させたいことがあります。条件を指定して表示するパケットを制限するためには、フィルタを使います。

デコード機能に関しては、次のようなフィルタが用意されています。

ディスプレイフィルタ
フィルタエディタでフィルタの条件を論理式で指定し、値が真となったパケットのみを表示します。

簡易フィルタ あらかじめ論理式を指定する必要はありません。 GUI の操作だけで手軽にパケットやレコードを絞り込めます。簡易フィルタは 3 種類あります。

- **見出しフィルタ**
- **ヘッダー属性フィルタ**
- **デコード結果フィルタ**

デコードビューでは、すべてのフィルタが使えます。シーケンスモードでないストリームビューでは見出しフィルタとデコード結果フィルタが、シーケンスモードのストリームビューでは見出しフィルタが使えます。

6.6.1 見出しフィルタ

見出しフィルタは、サマリ領域やシーケンス領域のカラムに表示されている値を 1 つ選び、その値と一致する行だけを表示するフィルタです。複数のカラムに見出しフィルタを適用できます。

見出しフィルタを使う

見出しフィルタを使うには、デコードビューのサマリ領域またはストリームビューのサマリ領域やシーケンス領域でカラムの見出しをクリックしてメニューを開き、項目を選びます。

プロトコルのカラムおよびフレーム ID のカラムの見出しをクリックしたときに現れるメニューを図 6-10 に示します。

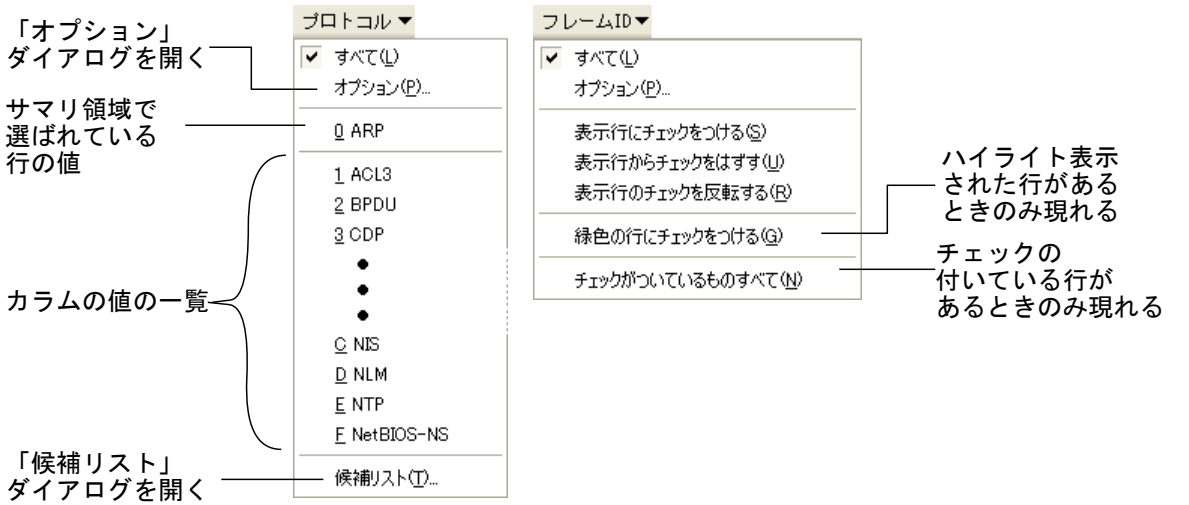


図 6-10: 見出しフィルタのメニュー

見出しフィルタのメニュー項目

メニューから項目を選ぶと、次のようになります。

特定の値に対応する項目
選んだ値と一致する行だけが表示されるようになります。

すべて(L) 選んだカラムに適用されている見出しフィルタを外します。

オプション(P)... 「オプション」ダイアログが現れます。詳しくは「6.6.4 「オプション」ダイアログ」 (134 ページ) を参照してください。

表示行にチェックをつける(S)
表示されている行にチェックを付けます。チェックの付いた行がある場合、フレーム ID カラムから現れるメニューには、**チェックがついているものすべて(N)** があります。

表示行からチェックをはずす(U)
表示されているすべての行のチェックを外します。

表示行のチェックを反転する(R)
チェックのついた行からはチェックを外し、チェックのついていない行にチェックを付けます。

緑色の行にチェックをつける(G)

緑色でハイライト表示されている行にチェックを付けます。

緑色の他、青色、海老茶色、紫色、オレンジ色などもあります。

<Shift> キーを押しながら選ぶと、ハイライト表示されている行だけを表示するようになります。

チェックがついているものすべて(N)

チェックの付いた行だけが表示されるようになります。

候補リスト(T)... 「候補リスト」ダイアログが現れます。このメニュー項目は、カラムの値の種類が 17 個以上ある場合に現れます。詳しくは「6.6.5 「候補リスト」ダイアログ」 (135 ページ) を参照してください。

■ デコード時にエラーの起きたパケットまたはレコードのみが表示されます。このメニュー項目は、デコード時にエラーが起きた場合に現れます。

□ デコード時にエラーの起きていないパケットまたはレコードのみが表示されます。このメニュー項目は、デコード時にエラーが起きた場合に現れます。

見出しフィルタを使って表示する行を制限すると、フィルタが適用されていることを示すために、見出しの右端の▼とフレーム ID またはストリーム ID カラムの文字列の色が青に変わります。そのようすを図 6-11 に示します。

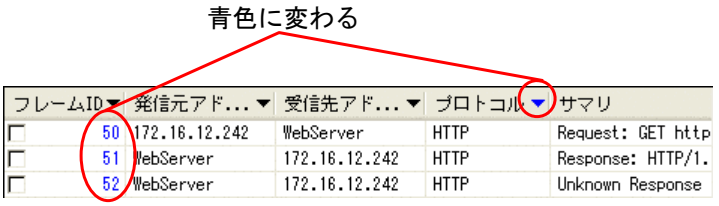


図 6-11: 青色に変わったフレーム ID の値と見出しの▼

見出しフィルタを使うために、見出しの▼をクリックする必要はありません。見出しのどこをクリックしてもメニューは現れます。

見出しフィルタが使えるカラム

すべてのカラムで見出しフィルタが使えるわけではありません。見出しフィルタが使えるカラムの見出しには、右端に▼が付いています。

6.6.2 ヘッダー属性フィルタ

トラフィックウィンドウは、パケットヘッダーのさまざまなフィールドの値からトラフィックを分類して表示します。同じように、デコードしたパケットヘッダーのフィールドの値を元にパケットを分類し、表示する行を制限するフィルタを**ヘッダー属性フィルタ**と呼びます。

ヘッダー属性フィルタを使う

ヘッダー属性フィルタを使うには、メニューを開いて項目を選びます。

メニューを開く方法は 2 通りあります。

- デコードビューのツールバーの**ヘッダー属性フィルタ**ボタン(⊛) をクリックします。
- デコードビューを右クリックしてポップアップメニューを開き、**フィルタ(F)** をポイントし、**ヘッダー属性フィルタ(A)** を選びます。

ヘッダー属性フィルタのメニュー項目

ヘッダー属性フィルタのメニュー項目を図 6-12 に示します。

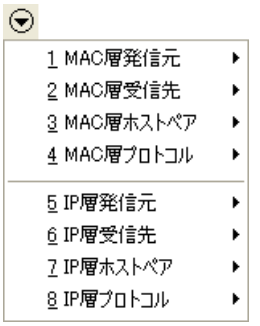


図 6-12: ヘッダー属性フィルタのメニュー

それぞれのメニュー項目から、サブメニューが現れます。

サブメニューは見出しフィルタのメニューと同じ構造になっています。サブメニューから項目を選ぶと、次のようになります。

特定の条件に対応する項目
選んだ条件と一致する行だけが表示されるようになります。

すべて(L) 選んだ属性に適用されているヘッダー属性フィルタを外します。

オプション(P)... 「オプション」ダイアログが現れます。詳しくは「6.6.4 「オプション」ダイアログ」 (134 ページ) を参照してください。

候補リスト(T)... 「候補リスト」ダイアログが現れます。このメニュー項目は、サブメニューの項目が 17 個以上ある場合にあります。詳しくは「6.6.5 「候補リスト」ダイアログ」 (135 ページ) を参照してください。

ヘッダー属性フィルタを適用すると、フィルタが適用されていることを示すために、**ヘッダー属性フィルタ**ボタン(▼) の色とフレーム ID のカラムの文字列の色が青に変わります。そのようすを図 6-13 に示します。

図 6-13: 青色に変わったフレーム ID の値とヘッダー属性フィルタボタン

ヘッダー属性フィルタの IP 層プロトコルの値は、モニタと同じく IP ヘッダー、 UDP ヘッダー、 TCP ヘッダーの情報のみから判定しています。従って、デコードビューのプロトコルのカラムに表示されるものとは異なる値が表示されることがあります。

6.6.3 デコード結果フィルタ

デコード結果フィルタは、デコードビューまたはストリームビューのデコード結果領域に表示する文字列や値を利用して、パケットまたはレコードを絞り込むフィルタです。

デコード結果フィルタを使う

1. 「デコード結果フィルタ」ダイアログを開きます。「デコード結果フィルタ」ダイアログを開く方法は 2 通りあります。
   - デコードビューまたはストリームビューのツールバーの**デコード結果フィルタ**ボタン( )をクリックします。
   - デコードビューまたはストリームビューを右クリックしてポップアップメニューを開き、**フィルタ(F)** をポイントし、**デコード結果フィルタ(F)**... を選びます。

   図 6-14 のような「デコード結果フィルタ」ダイアログが現れます。

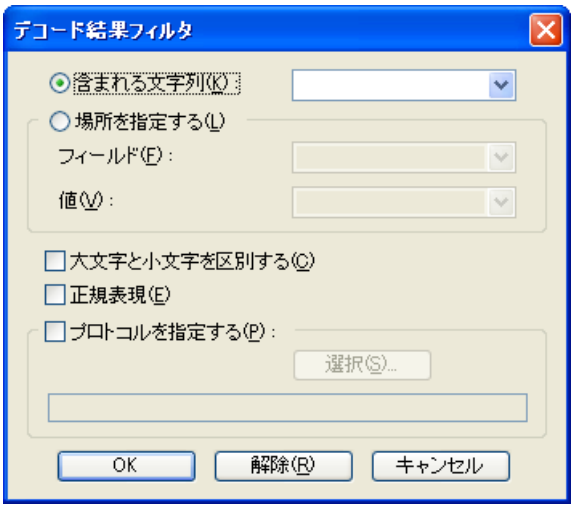


図 6-14: 「デコード結果フィルタ」ダイアログ

2. フィルタの条件を指定します。
   - デコード結果に、ある文字列を含むパケットまたはレコードだけを表示したい場合は、**含まれる文字列(K)** に文字列を入力します。
   - 特定のフィールドの値が特定の値であるものだけを表示したい場合は、**場所を指定する(L)** を選び、フィールド名とその値に含まれる文字列を入力します。

- 検索する文字列に正規表現を使うこともできます。**含まれる文字列(K)**、**フィールド(F)**、および**値(V)** の入力領域で正規表現を含む文字列を指定できます。正規表現を指定する場合は、**正規表現(E)** にチェックを付けます。
- **プロトコルを指定する(P)** にチェックを付けてプロトコルを指定すると、指定されたプロトコルのデコード結果だけが対象になります。プロトコルを指定するには、**選択(S)...** ボタンをクリックし、「候補リスト (複数選択)」ダイアログを開きます。複数のプロトコルを指定できます。

3. **OK** ボタンをクリックします。
   デコードビューまたはストリームビューに表示されているすべてのパケットまたはレコードを詳細にデコードし、指定した条件に合致するパケットまたはレコードだけを表示した状態になります。
   デコードおよび検索の処理中は、「ASTEC Eyes」ダイアログが現れて、進捗状況を表示します。

中止する場合は、**キャンセル**ボタンをクリックします。

「デコード結果フィルタ」ダイアログが適用されると、デコードビューのツールバーにある**デコード結果フィルタ**ボタン( ) が に変わります。

正規表現について、詳しくは「6.8.2　正規表現を用いた検索」 (147 ページ) を参照してください。

6.6.4 「オプション」ダイアログ

「オプション」ダイアログは、見出しフィルタおよびヘッダー属性フィルタのメニューから**オプション(P)**. . . を選ぶと現れます。

図 6-15 に「オプション」ダイアログを示します。

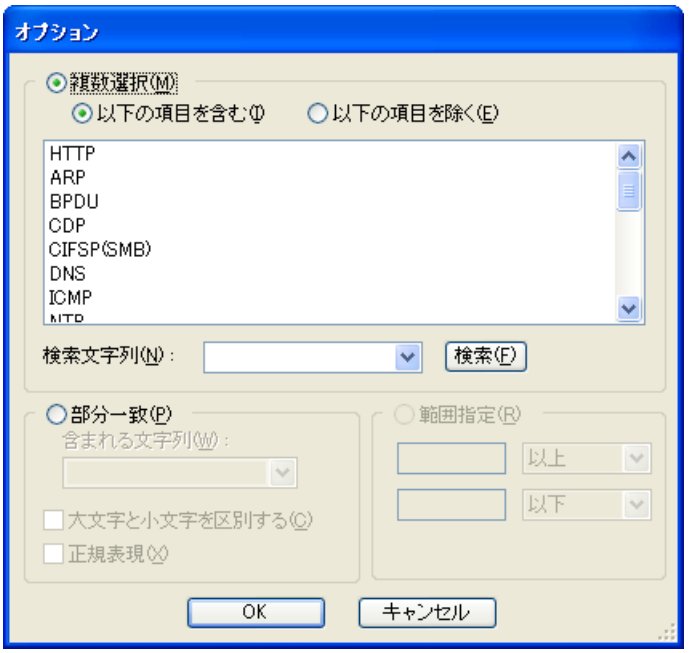


図 6-15: 「オプション」ダイアログ

「オプション」ダイアログでは、次の 3 つの方法で表示する行を指定できます。

複数選択 複数の項目を選び、選んだ項目と一致する行だけを表示させることができます。逆に、選んだ項目と一致しない行だけを表示させることもできます。リストに表示されている文字列を検索できます。

部分一致 入力した文字列が、カラムの値に含まれる行だけを表示させることができます。

正規表現を含む文字列を指定することもできます。正規表現を使う場合は、**正規表現(X)** にチェックを付けます。詳しくは「6.8.2 正規表現を用いた検索」 (147 ページ) を参照してください。

範囲指定 範囲指定は、表示する値を範囲で指定します。

「部分一致」と「範囲指定」はどちらか一方しか使えません。

ヘッダー属性フィルタのメニューから開いた「オプション」ダイアログの場合、使えるのは「部分一致」だけです。

見出しフィルタのメニューから開いた「オプション」ダイアログの場合、どちらが使えるかはクリックしたカラムによります。

「部分一致」が使えるカラムは、次のとおりです。

- 発信元アドレス
- 受信先アドレス
- プロトコル
- サマリ
- アドレス 1
- アドレス 2
- 関連ホスト

「範囲指定」が使えるカラムは、次のとおりです。

- フレーム ID
- ストリーム ID
- 長さ
- 発信元ポート番号
- 受信先ポート番号
- ポート 1
- ポート 2

6.6.5 「候補リスト」ダイアログ

「候補リスト」ダイアログは、見出しフィルタおよびヘッダー属性フィルタのメニューから**候補リスト(T)**... を選ぶと現れます。

候補リスト(T)... は、見出しフィルタやヘッダー属性フィルタのメニューの項目数が 17 個以上になると追加されるメニュー項目です。

図 6-16 に「候補リスト」ダイアログを示します。

図 6-16: 「候補リスト」ダイアログ

表示されているリストを検索できます。項目数が多くて、目的のものを見つけにくいときなどに便利です。

6.6.6 簡易フィルタを組み合わせて使う

簡易フィルタは現在デコードビューまたはストリームビューに表示されている行に対してのみ適用されます。複数の簡易フィルタを適用すれば、複数の条件に合致する行だけを表示させることができます。

複数の条件のいずれかに合致する行を表示させるには、フレーム ID またはストリーム ID のチェックマークを使います。

例として、ホスト *example_host* が発信または受信したパケットを表示させる手順を示します。

1. 発信元アドレスの見出しをクリックし、現れたメニューから *example_host* を選びます。
2. フレーム ID の見出しをクリックし、**表示行にチェックをつける(S)** を選びます。
3. 発信元アドレスの見出しをクリックし、**すべて(L)** を選びます。
4. 受信先アドレスの見出しをクリックし、 *example_host* を選びます。
5. フレーム ID の見出しをクリックし、**表示行にチェックをつける(S)** を選びます。
6. 受信先アドレスの見出しをクリックし、**すべて(L)** を選びます。
7. フレーム ID の見出しをクリックし、**チェックがついているものすべて(N)** を選びます。

6.6.7 簡易フィルタを解除する

見出しフィルタおよびヘッダー属性フィルタを解除する

条件を設定したメニューをひとつずつ開き、**すべて(L)** を選びます。

デコード結果フィルタを解除する

デコード結果フィルタボタン() をクリックして「デコード結果フィルタ」ダイアログを開き (図 6-14 参照)、**解除(R)** ボタンをクリックします。

すべての簡易フィルタを一度に解除する

すべての簡易フィルタを一度に解除する方法は 2 通りあります。

- デコードビューまたはストリームビューのツールバーにある**フィルタ解除**ボタン() をクリックします。
- デコードビューまたはストリームビューを右クリックしてポップアップメニューを開き、**フィルタ(F)** をポイントし、**フィルタ解除(R)** を選びます。

6.6.8 ディスプレイフィルタ

簡易フィルタではできない複雑な条件を設定したい場合はディスプレイフィルタを使います。

ディスプレイフィルタの条件はフィルタエディタで定義します。インタフェースに関係なく、複数のディスプレイフィルタを用意しておき (最大 250 個まで)、必要なものを選んで適用できます。

フィルタエディタを起動するには、メインウィンドウの**編集(E)** メニューから**フィルタエディタ(E)**. . . を選ぶか、 **<Ctrl-E>** キーを押します。

条件を設定する方法など、フィルタエディタの詳しい使い方については、 9 章「フィルタエディタ」 (195 ページ) を参照してください。

ディスプレイフィルタをデコードビューに適用するには、次のようにします。

1. ディスプレイフィルタのメニューを開きます。
   - デコードビューのツールバーの**ディスプレイフィルタ**ボタン() をクリックします。
   - デコードビューを右クリックしてポップアップメニューを開き、**フィルタ(F)** をポイントし、**ディスプレイフィルタ(D)** を選びます。

   設定されているディスプレイフィルタの名前の一覧をメニュー項目とするメニューが現れます。

2. 適用したいフィルタの名前を選びます。

選んだディスプレイフィルタの論理式が真になるパケットだけを表示したデコードビューが新たに現れます。このデコードビューのフレーム ID のカラムの文字列は緑色で表示されます。また、タイトルには、元のデコードビューのタイトルのラベルと適用したディスプレイフィルタのフィルタ名が表示されます。ディスプレイフィルタを適用したデコードビューを図 6-17 に示します。

図 6-17: ディスプレイフィルタを適用したデコードビュー

ストリームビューでディスプレイフィルタを使うことはできません。ディスプレイフィルタを適用したデコードビューからストリームビューを作ります。

6.6.9 ディスプレイフィルタを自動的に生成する

限られた条件であれば、論理式を自動的に生成してディスプレイフィルタを使うことができます。マウス操作だけで、たとえば、デコードビューまたはストリームビューで選択中の行が属すコネクションを抜き出すような論理式を生成できます。

ドラッグアンドドロップを使う方法とポップアップメニューを使う方法があります。

ドラッグアンドドロップを使う

1. フィルタエディタを起動します。
   そのためには、メインウィンドウの**編集(E)** メニューから**フィルタエディタ(E)**. . . を選ぶか、**<Ctrl-E>** キーを押します。
2. デコードビューまたはストリームビューのサマリ領域の行をドラッグし、フィルタエディタ内のディスプレイフィルタの条件グループ上にドロップします (図 6-18 参照)。

図 6-18: ディスプレイフィルタの条件をドラッグアンドドロップで生成する

3. ポップアップメニューからフィルタの条件を選びます。

ポップアップメニューの項目はドラッグした行によって異なります。メニュー項目には、次のようなものがあります。

- **コネクションを指定(C)**
- **ホストペアとプロトコルを指定(C)**
- **ホストペアを指定(H)**
- **ポート番号を指定(P)**
- **フレーム ID を指定(F)**
- **日付を指定(D)**

ドラッグした行と選んだメニュー項目によって、生成される論理式が異なります。生成される論理式の例については、「9.6.3　デコードビューまたは ストリームビューから自動生成できる論理式」 (229 ページ) の表 9-7 を参照してください。

ポップアップメニューを使う方法

1. デコードビューのサマリ領域の行を右クリックし、**フィルタ(F)** をポイントします。
2. **フィルタの生成(I)** をポイントします。
3. **一時的に生成して適用する(I)** または**フィルタエディタに送る(F)** をポイントします。
4. フィルタの条件を選びます。

階層化されたメニューの例を図 6-19 に示します。メニュー項目はサマリ領域でクリックした行によって異なります。

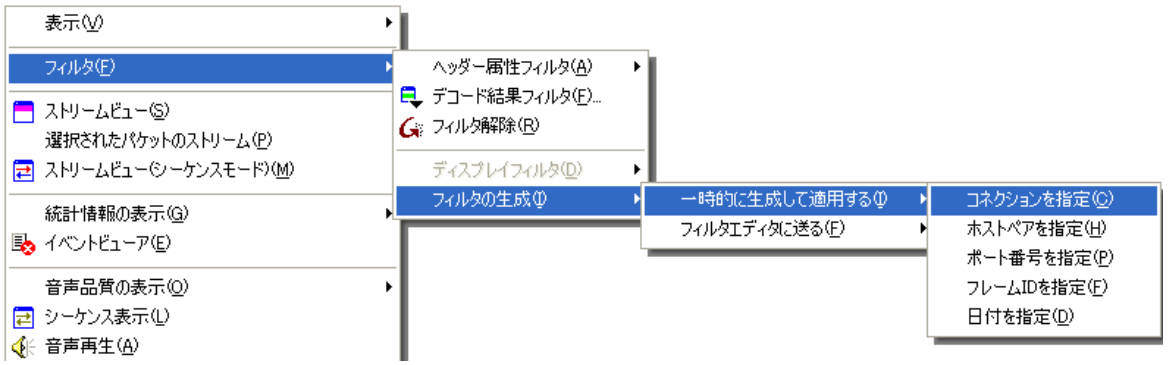


図 6-19: ディスプレイフィルタを自動的に生成するための階層化されたメニュー

サマリ領域でクリックした行、ポイントしたメニュー項目、および選んだフィルタの条件によって、生成される論理式が異なります。生成される論理式の例については、「9.6.3　デコードビューまたは ストリームビューから自動生成できる論理式」 (229 ページ) の表 9-7 を参照してください。

手順 3 で**一時的に生成して適用する(I)** をポイントしたか、**フィルタエディタに送る(F)** をポイントしたかによって、 ASTEC Eyes の動作が異なります。それぞれ次のようになります。

一時的に生成して適用する(I) をポイントした場合

ディスプレイフィルタの条件となる論理式が生成されますが、フィルタエディタは現れません。ディスプレイフィルタを適用した状態のデコードビューが現れます。生成された論理式を保存したり、変更することはできません。手作業で条件を設定してフィルタを適用した場合と同じように、フレーム ID のカラムの数字が緑色で表示されます。

フィルタエディタに送る(F) をポイントした場合

論理式が生成され、生成された論理式が追加された状態のフィルタエディタが現れます。ここからは手作業で論理式を編集する場合とまったく同じです。

フィルタエディタについては、9 章「フィルタエディタ」 (195 ページ) を参照してください。

6.7 デコードしたデータの統計情報を表示する

デコードしたデータに対して統計処理を行い、その結果をネットワークから収集した統計情報と同じようにグラフや表 (モニタウィンドウ) に表示できます。

1. デコードビューのメニューバーの**統計情報の表示**ボタン() をクリックするか、または、デコードビューを右クリックしてポップアップメニューを開き、**統計情報の表示(G)** を選びます。
2. メニューから項目を選ぶと、選んだ項目に対応したモニタウィンドウが現れます。

デコードしたデータの統計情報を表示したトラフィックウィンドウでも、ネットワークから収集した統計情報を表示しているトラフィックウィンドウと同じように、表示形式を変えたり、グラフアイテムを選んで、その内訳を見たり、ポップアップメニューを開いたりすることができます。

ただし、次に示す点が異なります。

- 「MAC 層トラフィック」のウィンドウには、ピーク値は表示されません。
- 「MAC 層エラーフレーム数」のウィンドウは開けません。
- タイムスパンは切り替えられません。
- 折れ線グラフ形式のトラフィックウィンドウでは、プロット間隔を変えられます。詳しくは、 次の「プロット間隔を変える」を参照してください。

6.7.1 プロット間隔を変える

ネットワークから収集した統計情報を折れ線グラフ形式でリアルタイムに表示しているトラフィックウィンドウの場合、統計情報を作成し、プロットする間隔はタイムスパンごとに決まっており、変えられません。短期タイムスパンの場合は 1 秒間隔、中期タイムスパンの場合は 10 秒間隔、長期タイムスパンの場合は 5 分間隔でプロットします。

デコードしたデータから作る場合は、プロット間隔 (統計情報の粒度) を変えられます。

最初はデコードしたデータのサイズによってプロット間隔を決め、トラフィックウィンドウにグラフを表示します。その後、プロット間隔を変えられます。プロット間隔は 1 ミリ秒から 12 時間の範囲で選べます。

プロット間隔を変えるには、次のようにします。

1. トラフィックウィンドウを右クリックしてポップアップメニューを開き、**プロット間隔(L)**. . . を選びます。

図 6-20 に示すような「プロット間隔」ダイアログが現れます。

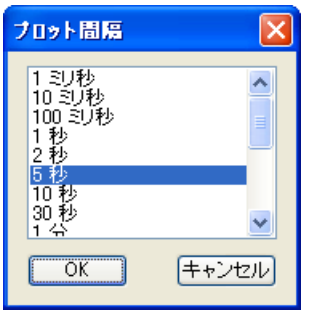


図 6-20: 「プロット間隔」ダイアログ

2. 「プロット間隔」ダイアログのリストからプロット間隔を選び、 **OK** ボタンをクリックします。

1 つのデータから複数のトラフィックウィンドウを表示させている場合、操作を行ったトラフィックウィンドウだけでなく、すべてのトラフィックウィンドウのグラフのプロット間隔が変わります。

6.7.2 デコードしたデータの統計情報を読み取る

デコードしたデータの統計情報を表示したトラフィックウィンドウのグラフの値を読み取ることができます。操作はネットワークの状態をリアルタイムに表示しているトラフィックウィンドウと同じです。グラフの値を読み取る操作については、「2.5 折れ線グラフの値を読み取る」 (30 ページ) を参照してください。

ネットワークの状態をリアルタイムに表示しているトラフィックウィンドウと異なるのは、マウスをドラッグした範囲の値を読み取るとき、ドラッグした範囲に含まれるパケットに対応するデコードビューのサマリ領域の行が海老茶色でハイライト表示されることです。このとき、サマリ領域はハイライト表示された行の先頭が表示されるように自動的にスクロールされます。また、ハイライト表示されたパケットから構成されるレコードに対応するストリームビューのサマリ領域の行もハイライト表示されます。

海老茶色でハイライト表示されたデコードビューとストリームビューのようすを図 6-21 に示します。

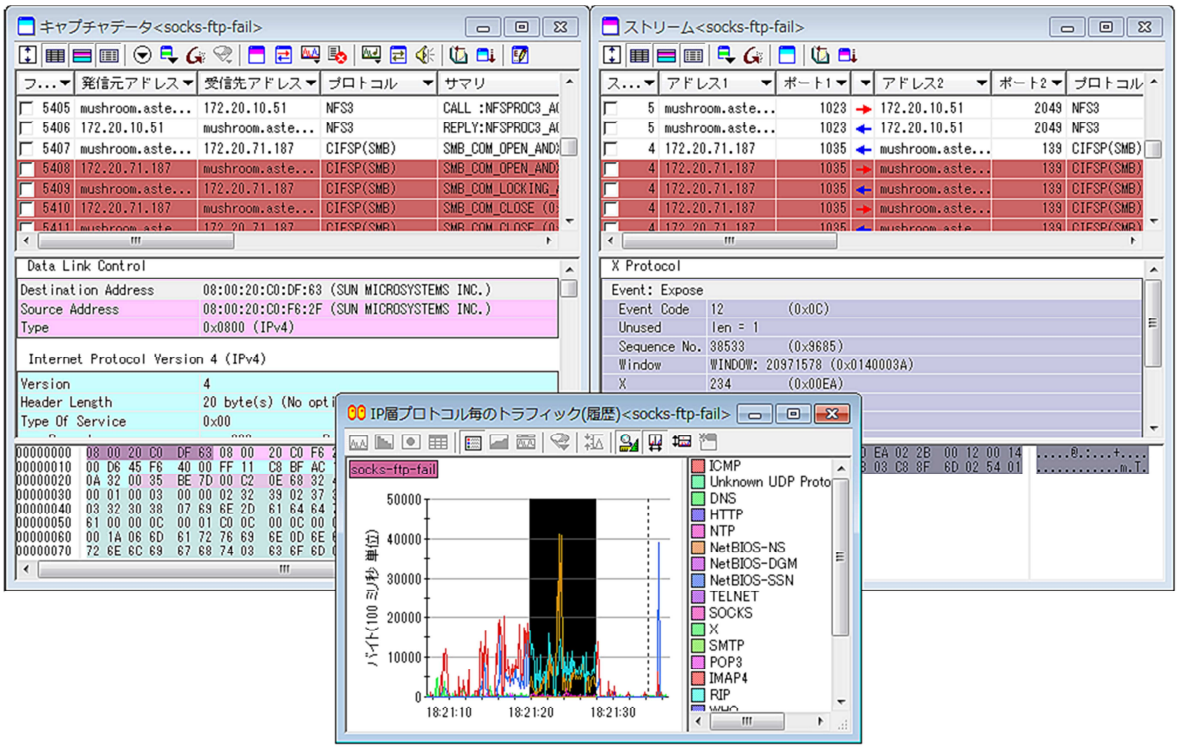


図 6-21: 海老茶色でハイライト表示されたデコードビューとストリームビュー

6.7.3 データをキャプチャしたときのネットワーク使用率を調べる

「MAC 層トラフィック」のウィンドウの Y 軸の単位を「使用率」にすると、データをキャプチャしたときのネットワークの使用率が分かります。

キャプチャデータには、ネットワークのリンクスピードが保存されていません。キャプチャファイルを開いてデコードした場合など、リンクスピードが分からないことがあります。

そのような場合は、リンクスピードを指定する必要があります。リンクスピードを入力するには、次のようにします。

1. 「MAC 層トラフィック」のウィンドウを右クリックしてポップアップメニューを開き、**プロパティ(O)**... を選びます。
   「グラフのプロパティ」ダイアログが現れます。
2. リンクスピードを入力し、**OK** ボタンまたは**適用(A)** ボタンをクリックします。

「グラフのプロパティ」ダイアログでリンクスピードを指定せずに Y 軸の単位を「使用率」に変えようとした場合は、「リンクスピードの設定」ダイアログが現れ、リンクスピードをたずねます。リンクスピードがわからない場合は、システム管理者に問い合わせてください。

「リンクスピードの設定」ダイアログでリンクスピードを指定したとき、**デフォルトに設定する (D)** にチェックを付けておくと、別のキャプチャファイルからネットワークの使用率を計算するときにも、同じリンクスピードが使われます。
また、「オプション」ダイアログであらかじめデフォルトのリンクスピードを設定しておくこともできます。詳しくは「11.2　デコードのオプションを設定する」 (286 ページ) を参照してください。

フィルタを適用してキャプチャしたデータから、正しいネットワークの使用率を求めることはできません。

6.8 文字列の検索とコピー

リアルタイムデコードビューやデコードビュー、ストリームビューでは、文字列を検索したりコピーしたりできます。

6.8.1 文字列を検索する

文字列の検索は各領域 (サマリ領域、デコード結果領域、ダンプ領域、セッションリスト領域、シーケンス領域) ごとに行います。

検索するには、次のようにします。

1. 探したい領域をクリックして、フォーカスを移します。
2. メインウィンドウの**編集(E)** メニューから**検索(F)** を選ぶか、 **<Ctrl-F>** キーを押します。

「検索」ダイアログが現れるので、探したい文字列を入力して**次を検索(F)** ボタン をクリックします。

デコード結果領域やシーケンス領域で検索する

デコード結果領域で検索する場合、現在表示されているデコード結果のみが検索の対象となります。

「検索」ダイアログで **パケット・レコードを越えて検索(W)** や**セッションを越えて検索(W)** にチェックを付けると、全パケットまたは全レコードのデコード結果が検索の対象となります。

ダンプ領域で検索する

ダンプ領域は、縦線によって 3 つに分かれています。一番左にはパケットの先頭を 0 とするデータのアドレスが表示されていて、ここは検索の対象になりません。中央の 16 進表示部と右側のキャラクタ表示部が検索の対象です。ダンプ領域では、 16 進表示または文字列で検索できます。

たとえば、「Keep」という文字列を探す場合、「検索」ダイアログの**検索する文字列(N)** に「Keep」と入力しても探すことができますし、「4b656570」または「4b 65 65 70」と入力しても探すことができます。

キャラクタとして表示できないデータを検索するときは、ダンプ領域でデータの 16 進表示を入力して検索します。

6.8.2 正規表現を用いた検索

「検索」ダイアログ、「オプション」ダイアログ、および「デコード結果フィルタ」ダイアログでは、正規表現によるパターンマッチングをサポートしています。

正規表現について

通常の文字列の検索では、ユーザーが指定した 1 個の文字列を検索します。これに対し、たとえば複数の文字列を同時に検索できると便利なことがあります。このような場合、複数の文字列や、もっと一般的に文字列の集合をパターンと呼ばれる記号列で表現し、ユーザーがパターンを指定して検索を行うことをパターンマッチングと呼びます。また、パターンが表現する文字列が検索対象に現れることを、パターンがマッチすると言います。

一例として、文字列 foo または文字列 bar に一致する箇所を検索する場合を考えます。このときパターンマッチングでは、文字列 foo または文字列 bar に一致するパターン foo|bar をユーザーが指定して検索できます。パターン foo|bar は、文字列 aaafoobbb や文字列 cccbar、あるいは文字列 barfoo 等にマッチします。

文字列の集合を表現するパターンにはさまざまな種類がありますが、その中でも正規表現 (regular expression) が良く使われます。 UNIX 系 OS でファイルの内容のパターンマッチングを行う grep や egrep コマンドをはじめ、多くのテキストエディタでも正規表現がサポートされています。

正規表現には、簡単なパターンで多様な文字列を表現できるという点に加え、その検索がバックトラック (後戻り) をせずに効率良く行えるという特長があります。

表 6-6 に示す要素の組み合わせで表されるパターンのことを、一般に正規表現と呼びます。

表 6-6: 正規表現のパターン

パターン	説明
文字	一つの文字は、正規表現で最も基本的なパターンです。このパターンはその文字自身にマッチします。たとえば A というパターンは、検索対象の文字列に A が含まれている場合にマッチします。 正規表現の中で特別な意味を持つ文字 (メタキャラクタと呼びます) を本来の文字として扱う場合には、その直前に \(バックスラッシュ) または¥(半角の円記号) を置きます。 たとえば * という文字を検索する場合は *(アスタリスク) がメタキャラクタなのでパターンとして * を指定します。 **ASTEC Eyes の正規表現におけるメタキャラクタ**は \ ^ $ (|) . [-] * + ? { , } の 16 文字です。 文字として日本語の文字 (Shift JIS コードの 2 バイト文字) も指定できます。
文字列 (パターンの連結 (concatination))	文字を連結した文字列をパターンとして指定できます。たとえば flags というパターンは、検索対象に 'f', 'l', 'a', 'g', 's' という文字がこの順序で現れた場合にマッチします。文字に限らず一般的なパターンも同様にして連結できます。パターン R とパターン S を連結したパターン RS は、 R にマッチした直後に S にマッチすることを表します。
| (選択肢 (alternative))	パターン R にマッチするか、またはパターン S にマッチするパターンを R|S と書きます。 foo|bar は、文字列 foo にマッチするかまたは文字列 bar にマッチするパターンです。
* (閉包 (closure))	* の直前のパターンを 0 回以上の任意回数連結したパターンにマッチするパターンを表します。たとえば ab* は、 a, ab, abb, abbb, abbb … b という文字列にマッチします。
'(' および ')' (グルーピング)	括弧は、パターンのグループを示すために使います。たとえば a(bc)* は、 a, abc, abcbc, abcbcbc, abcbcbc … bc という文字列にマッチします。また foo (bar|baz) は、 foobar または foobaz にマッチします。

これ以外にも、良く使うパターンを簡単に表現できるように、 ASTEC Eyes では次のメタキャラクタを定義しています。

表 6-7: ASTEC Eyes が定義しているメタキャラクタ

メタキャラクタ	機能
.	任意の一文字にマッチします。すべての文字を	でつなぎ、全体を括弧でくくったパターン (a|b|c| … |0|1|2| … |あ|い|う| …) と等価です。
'[' および ']'	文字の集合を表します。 '[' と ']' で囲まれた文字のいずれかとマッチします。 [abc] は、 a または b または c とマッチするパターンで、 (a|b|c) と等価です。 -(マイナス記号) で文字の範囲を指定できます。 [A-Za-z] は、大文字と小文字のアルファベットいずれかにマッチします。文字の範囲は ASCII コードを基に定義されます。また、 '[' の直後に ^(サーカムフレックス) を置くと否定の意味になります。 [^0-9] は、数字以外の任意の文字にマッチします。 '[' と ']' は、 1 バイト ASCII コードの集合を表します。日本語の文字 (Shift JIS コードでの 2 バイト文字) は、直接表現できません。 '[' と ']' で囲まれた場所では、 \^-] の 4 文字以外のメタキャラクタは通常の文字として扱います。また、 [の直後以外では ^ も通常の文字として扱います。このとき、これらの文字の直前に \(バックスラッシュ) を置く必要はありません (置いても意味は変わりません)。
{*m*,*n*}	直前のパターンの *m* 回以上、 *n* 回以下の繰り返しを表します。 *m* は 0 以上の整数、 *n* は 1 以上の整数です。ここで $m \leq n$ である必要があります。また、 {*m*,} は *m* 回以上の任意回の繰り返しを表します。 {,*n*} は {0,*n*} と等価です。 {*n*} は {*n*,*n*} と等価で、ちょうど *n* 回の繰り返しを表します。
?	直前のパターンの 0 回または 1 回のマッチを表します。パターン R に対し、 R? は R{0,1} と等価です。
+	直前のパターンを 1 回以上の任意回数連結したパターンを表します。パターン R に対し、 R+ は RR* または R{1,} と等価です。
^	検索対象文字列の先頭にマッチします。 ^foo は、 foobar にはマッチしますが、 barfoo にはマッチしません。
$	検索対象文字列の末尾にマッチします。 foo$ は、 barfoo にはマッチしますが、 foobar にはマッチしません。

^$-, の 4 文字は、特定のパターンにおいてのみメタキャラクタとして扱います。そのパターンを表 6-8 に示します。この表以外のパターンでは、通常の文字として扱います。このとき、直前に \(バックスラッシュ) を置く必要はありません (置いても意味は変わりません)。

表 6-8: 特定のパターンにおいてのみメタキャラクタとして扱う文字

文字	メタキャラクタとして扱うパターン
^	パターンの先頭にある場合。または、 [の直後にある場合。
$	パターンの末尾にある場合。
-	'[' と ']' で囲まれている場合。
,	'{' と '}' で囲まれている場合。

\(バックスラッシュ) を前に置くと特別な意味をもつ文字があります。この \(バックスラッシュ) と文字の組み合わせは、エスケープシーケンスと呼ばれます。 ASTEC Eyes の正規表現がサポートするエスケープシーケンスの一覧を次に示します。

表 6-9: ASTEC Eyes がサポートするエスケープシーケンス一覧

エスケープシーケンス	意味
\a	0x07 (BEL, Alert)
\b	0x08 (BS, Back Space)
\d	数字 ([0-9] と等価)
\D	数字以外 ([^0-9] と等価)
\f	0x0c (FF, Form Feed)
\n	0x0a (NL, New Line)
\r	0x0d (CR, Carriage Return)
\s	空白文字 ([\t\r\n\f] と等価)
\S	空白文字以外 ([^ \t\r\n\f] と等価)
\t	0x09 (HT, Horizontal Tab)
\w	英数字 ([0-9a-zA-Z] と等価)
\W	英数字以外 ([^0-9a-zA-Z] と等価)
\x*hh*, \X*hh*	*hh* は 1 桁または 2 桁の 16 進数 (0-9, a-f, A-F)

6.8.3 文字列をコピーする

リアルタイムデコードビューやデコードビュー、ストリームビューに表示されている文字列をコピーできます。文字列はクリップボードにコピーされるので、ダイアログの入力領域や他のアプリケーションに貼り付けることができます。

コピーする範囲は、ウィンドウの種類や領域によって異なります。

リアルタイムデコードビューでは、白い枠で囲まれているセル内の文字列をコピーします。

デコードビューや シーケンスモードでないストリームビューで、フォーカスがサマリ領域またはデコード結果領域にある場合は、白い枠で囲まれているセル内の文字列をコピーします。フォーカスがダンプ領域にある場合は、反転表示されている部分の 16 進ダンプをテキストとしてコピーします。

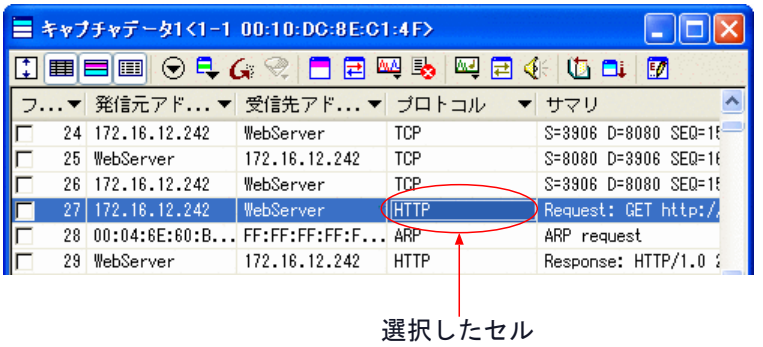


図 6-22: デコードビューで選択したセル

文字列をコピーするには、 **<Ctrl-C>** キーを押すか、または、メインウィンドウの**編集(E)** から**コピー(C)** を選びます。

6.9 データを保存する

デコードビューのデータ、デコード結果などをファイルに保存できます。また、データの一部をバイナリモードで保存することもできます。

6.9.1 デコードしたデータを保存する

デコードビューに表示されているデータの種類は大きく 3 種類に分けられます。

- キャプチャファイルのデータ (改めて保存する必要はありません)
- デコードしたキャプチャバッファのデータ
- フィルタなどで絞り込んだデータ

デコードしたキャプチャバッファのデータ

キャプチャを停止してデコードビューを生成するとき、 ASTEC Eyes はデコード用にコピーを作ります。キャプチャバッファのデータを削除したり、削除せずにキャプチャを再開すると、デコードビューに表示されているデータとキャプチャバッファのデータは同一ではなくなります。「デコードしたキャプチャデータを保存する」とは、デコードビューを作成した時点でのキャプチャバッファのスナップショットを保存することです。

デコードしたキャプチャデータをファイルに保存するには、

1. 保存したいデータを表示しているデコードビューをアクティブにします。
2. メインウィンドウの**ファイル(F)** メニューから**デコードしたキャプチャデータの保存(S)**. . . を選ぶか、 **<Ctrl-S>** キーを押します。

フィルタなどで絞り込んだデータ

簡易フィルタやディスプレイフィルタを適用するなどして、デコードビューに重要なパケットだけを表示している場合、表示されているデータだけを保存しておくと、後から見直す作業が容易になります。

表示されているパケットのデータのみを保存するには、

1. 保存したいデータを表示しているデコードビューをアクティブにします。
2. メインウィンドウの**ファイル(F)** メニューから**表示されているパケットのみ保存(D)**. . . を選びます。

データを保存するファイルのフォーマットは、キャプチャバッファのデータを保存する場合と同じで、 Sniffer 互換の非圧縮フォーマット (拡張子 .enc) です。また、 bzip2 で圧縮してから保存することもできます。その場合の拡張子は.ebz となります。
bzip2 については、 http://www.bzip.org/ を参照してください。

デコードしたデータを保存しなかった場合、デコードビューを消すときに、デコードしたデータを保存するかをどうかをたずねる「ASTEC Eyes」ダイアログが現れます。ただし、 **<Shift>** キーを押しながらデコードビューを消す操作を行えば「ASTEC Eyes」ダイアログは現れず、直ちにデコードしたデータを削除します。

6.9.2 デコード結果を csv 形式などで保存する

デコードビューまたはストリームビューに表示されているデコード結果を保存できます。

テキストファイルに保存することもできますし、コピーアンドペーストを使って他のアプリケーション (Microsoft Word や Microsoft Excel、ワードパッド、メモ帳など) に貼り付けることもできます。

デコード結果をファイルに保存する

デコード結果をファイルに保存するには、次のようにします。

1. デコード結果を保存したいデコードビューまたはシーケンスモードでないストリームビューをアクティブにします。
2. **ファイル(F)** から**デコード結果の保存(F)**. . . を選びます。
   図 6-23 に示すような「出力内容」ダイアログが現れます。

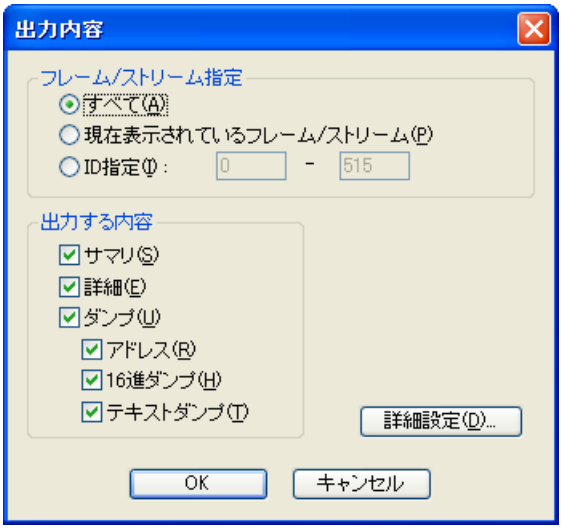


図 6-23: 「出力内容」ダイアログ

3. **フレーム / ストリーム指定** 領域で、出力する範囲を指定します。
   すべて(A) を選ぶと、すべてのパケットまたはレコードのデコード結果を出力します。
   簡易フィルタまたはディスプレイフィルタなどで表示するパケットやレコードを絞り込んでいる場合は、**現在表示されているフレーム / ストリーム(P)** を選びます。
   ID 指定(I) を選んで、フレーム ID またはストリーム ID で範囲を指定することもできます。
4. **出力する内容** 領域で、デコードビューまたはストリームビューのどの領域の内容を出力するかを指定します。
   デフォルトでは、すべての領域の内容を出力するようになっています。必要のない領域からチェックを外します。
5. **OK** ボタンをクリックします。
   「名前を付けて保存」ダイアログが現れるので、ファイル名を指定します。

出力したファイルの扱い方や扱うツールに合わせて、出力フォーマットを詳細に指定したいことがあります。たとえば、 Microsoft Excel に読み込む場合などです。

出力フォーマットを詳細に指定するためには、 **OK ボタンをクリックする前に**、次のようにします。

1. **詳細設定(D)**. . . ボタンをクリックします。
   図 6-24 のような「出力詳細」ダイアログが現れます。

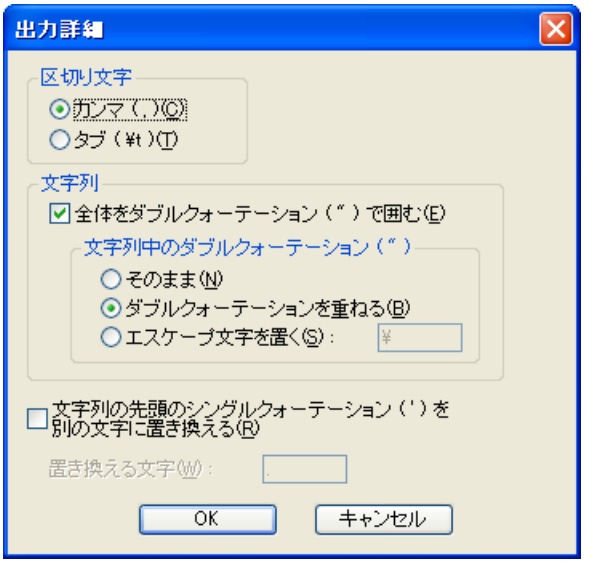


図 6-24: 「出力詳細」ダイアログ

2. **区切り文字** 領域で、カラムの値の間を区切る文字を指定します。
   カンマ(,)(C) または**タブ(¥t)(T)** を選べます。
3. **文字列** 領域で、文字列の値をダブルクォーテーション (") で囲むかどうかを指定します。
   デフォルトでは、囲むようになっています。囲みたくない場合は、**全体をダブルクォーテーション (") で囲む(E)** のチェックを外します。
   囲むように指定した場合は、デコード結果の文字列に含まれているかもしれないダブルクォーテーションの扱い方を指定する必要があります。次の 3 つから選べます。
   - そのままにしておく (何もしない)
   - ダブルクォーテーションを 2 つ重ねる
   - ダブルクォーテーションの前にエスケープ文字 (たとえば、バックスラッシュ'\') を置く
4. 文字列の先頭がシングルクォーテーション (') だった場合、それを別の文字に置き換えるかどうかを指定します。
   デフォルトでは、置き換えないようになっています。置き換えるように指定した場合は、置き換える文字を指定します。
5. **OK** ボタンをクリックします。

リアルタイムデコードビューやシーケンスモードのストリームビューでは、デコード結果を保存できません。

たとえば、 Microsoft Excel などにデコード結果を読み込む場合などは、ダブルクォーテーション (") で囲むかどうかで表示が変わることがあるので、注意が必要です。また、デコード結果の文字列中のダブルクォーテーションについては、**ダブルクォーテーションを重ねる(B)** を選んでおかないと、文字列中のダブルクォーテーションが区切り文字として扱われることがあります。
デコード結果領域の値とダンプ領域の値は、すべてダブルクォーテーションで囲まれます。サマリ領域の値は、次に示すカラムの値のみダブルクォーテーションで囲まれます。
- 発信元アドレス - 受信先アドレス - プロトコル - サマリ
- 時刻 - アドレス 1 - アドレス 2 - 向き

Microsoft Excel では、文字列の先頭のシングルクォーテーション (') は、特別扱いされます。表示されなかったり、ファイルに保存する場合になくなってしまうことがあります。これを避けるために、別の文字に置き換えられます。

デコード結果をコピーする

デコードビューやシーケンスモードでないストリームビューでは、各領域 (サマリ領域、デコード結果領域、ダンプ領域) ごとにデコード結果をコピーアンドペースト操作で他のアプリケーションに貼り付けることができます。

1. コピーしたいデコード結果を表示しているデコードビューまたはストリームビューをアクティブにします。
2. コピーしたい領域 (サマリ領域、デコード結果領域、またはダンプ領域) を右クリックしてポップアップメニューを開き、**領域全体をコピー(W)** を選びます。
3. 貼り付け先のアプリケーションをアクティブにします。
4. **<Ctrl-V>** キーを押します。
   デコード結果が、アプリケーションに貼り付けられます。 Microsoft Word や Microsoft Excel などの場合は、メニューバーの**編集(E)** から**形式を選択して貼り付け(S)** を選ぶこともできます。

デコードビューやシーケンスモードでないストリームビューでデコード結果をコピーする場合、デコードビューまたはストリームビュー全体をコピーすることはできません。領域ごとにコピーします。

シーケンスモードのストリームビューでは、 **<Ctrl-C>** キーで領域全体をコピーします。
また、リアルタイムデコードビュー、あるいはデコードビューやシーケンスモードでないストリームビューのサマリ領域やデコード結果領域にフォーカスがある場合、 **<Ctrl-C>** キーを押すと、白い枠で囲まれたセルの中の文字列だけがコピーされます。ダンプ領域にフォーカスがある場合は、反転表示されている部分だけがコピーされます。
詳しくは「6.8　文字列の検索とコピー」 (146 ページ) を参照してください。

6.9.3　キャプチャデータの一部をバイナリモードでファイルに保存する

キャプチャデータの一部をバイナリモードでファイルに保存できます。

たとえば、 HTTP の Message Body の部分だけをファイルに保存し、 Web ブラウザなどで開いて見たい場合に使います。

1. デコードビューまたはシーケンスモードでないストリームビューを右クリックしてポップアップメニューを開き、**バイナリ保存(B)**. . . を選びます。
   図 6-25 のような「バイナリデータを保存」ダイアログが現れます。

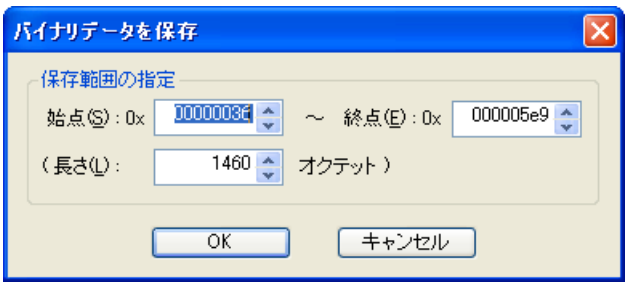


図 6-25: 「バイナリデータを保存」ダイアログ

始点(S) の値は、ダンプ領域で反転している部分の一番小さいアドレスです。**終点(E)** の値は、一番大きいアドレスです。

2. **始点(S)**、**終点(E)**、**長さ(L)** を変えて、保存する範囲を指定します。
3. **OK** ボタンをクリックします。

「名前を付けて保存」ダイアログが現れるので、保存するファイル名を指定します。

複数のパケットまたはレコードにわたってデータを保存することはできません。

データの一部を保存したい場合、右クリックするのはダンプ領域がよいでしょう。
デコードビューやストリームビューのどこを右クリックしてもメニューは現れますが、サマリ領域やデコード結果領域をクリックするとクリックした行が選ばれるので、ダンプ領域で反転していた範囲がずれてしまいます。

6.10 キャプチャデータマネジャーを使う

キャプチャデータマネジャーでは、次のことができます。

- 1 つ以上のファイルを同時に開けます。
- デコードする前に統計データのグラフを見て、デコード範囲を絞り込むための参考にできます。
- 期間でデコード範囲を絞り込めます。
- パケットのヘッダー属性を利用して、デコード範囲を絞り込めます。

キャプチャデータマネジャーを使うには、次のようにします。

1. メインウィンドウの**ファイル(F)** メニューから**キャプチャデータマネジャーで開く(E)**... を選びます。
   「開く」ダイアログが現れます。
2. 「開く」ダイアログで 1 つ以上のファイルを指定します。
   複数のファイルを指定した場合、ファイル内のパケットはマージされ、キャプチャされた時刻順に並べられます。
   図 6-26 のような「キャプチャデータマネジャー」ダイアログが現れます。

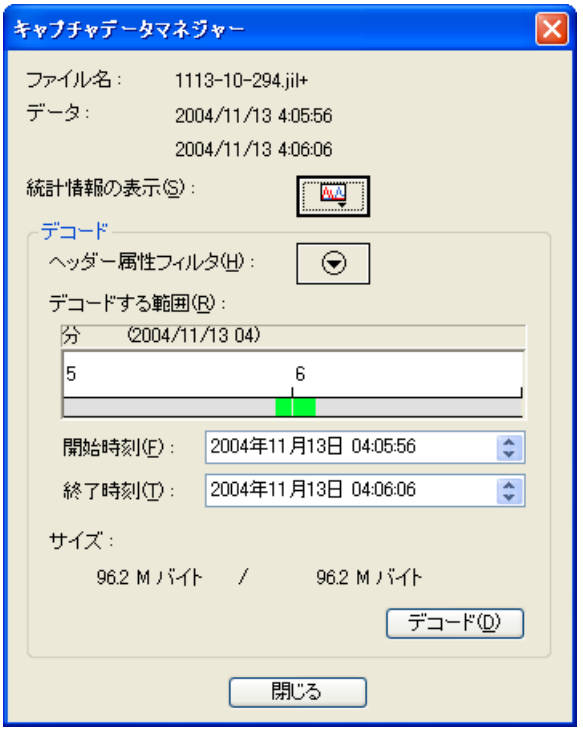


図 6-26: 「キャプチャデータマネジャー」ダイアログ

表示されている**サイズ**は、指定したファイルのサイズではなく、ファイルのデータを ASTEC Eyes に読み込んだ場合のメモリ使用量です。

複数のディレクトリにわたって、ファイルを指定することはできません。複数のファイルを指定したい場合、指定するファイルは同一のディレクトリ内に置いてください。

3. 統計データのグラフを見たい場合は、**統計情報の表示**ボタン() をクリックします。図 6-27 のようなメニューが現れます。

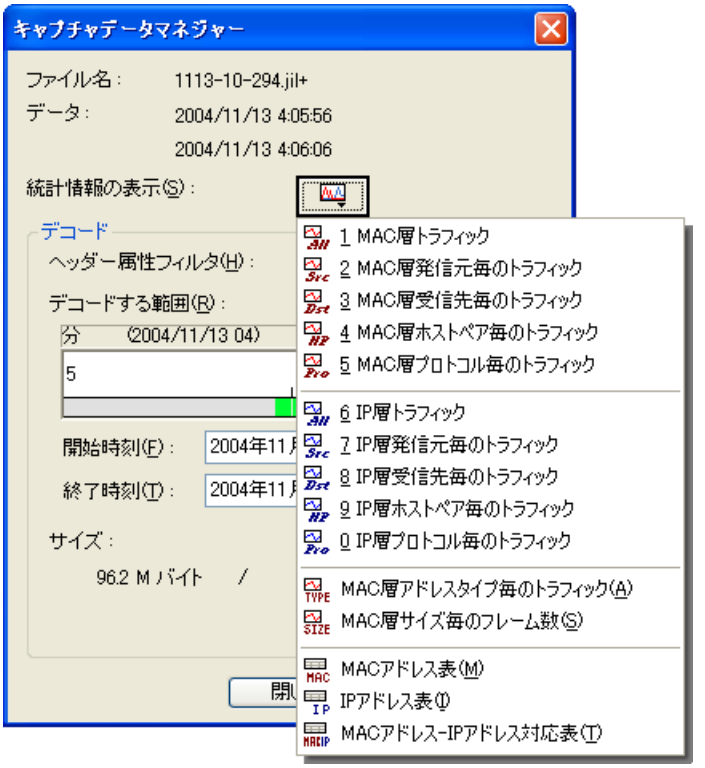


図 6-27: 「キャプチャデータマネジャー」ダイアログ (統計情報の表示ボタンをクリックしたところ)

メニューからトラフィックを選ぶと、指定したファイルのデータを統計処理し、その結果を表示したグラフまたは表が現れます。
この操作は、必ずしも必要なものではありませんが、デコードする範囲を指定するときに参考になるでしょう。

4. デコードする範囲を指定します。
   デコードする範囲を指定する方法は 2 通りあります。 2 つの方法を組み合わせて指定できます。

   - **時刻で範囲を指定する**
     ダイアログを開いたとき、**開始時刻 (F)** および**終了時刻 (T)** には、ファイルの中の最も古いパケットをキャプチャした時刻と最も新しいパケットをキャプチャした時刻が表示されます。
     開始時刻 (F) にデコードの開始時刻を、**終了時刻 (T)** に終了時刻を入力します。
     キー入力する代わりに、グラフの値を読み取る機能、または期間指定バーを使うこともできます。
     グラフの値を読み取る機能を使うには、次のようにします。

     (1) **統計情報の表示**ボタン() をクリックして統計データのグラフを表示させます (トラフィックの種類は何でもかまいません)。

     (2) トラフィックウィンドウの**グラフ解析機能**ボタン() をクリックします。

     (3) **垂直カーソル**ボタン() をクリックします。

     (4) トラフィックウィンドウ上デコードしたい範囲をマウスでドラッグします。

     期間指定バーの使い方については、「3.3.3　(緑色の) 期間指定バーを使う」 (62 ページ) を参照してください。
     グラフの値を読み取る機能については、「2.5　折れ線グラフの値を読み取る」 (30 ページ) を参照してください。

   - **パケットのヘッダー属性を基にデコードするパケットを制限する**
     ヘッダー属性フィルタボタン() をクリックします。
     図 6-28 のようなメニューが現れます。

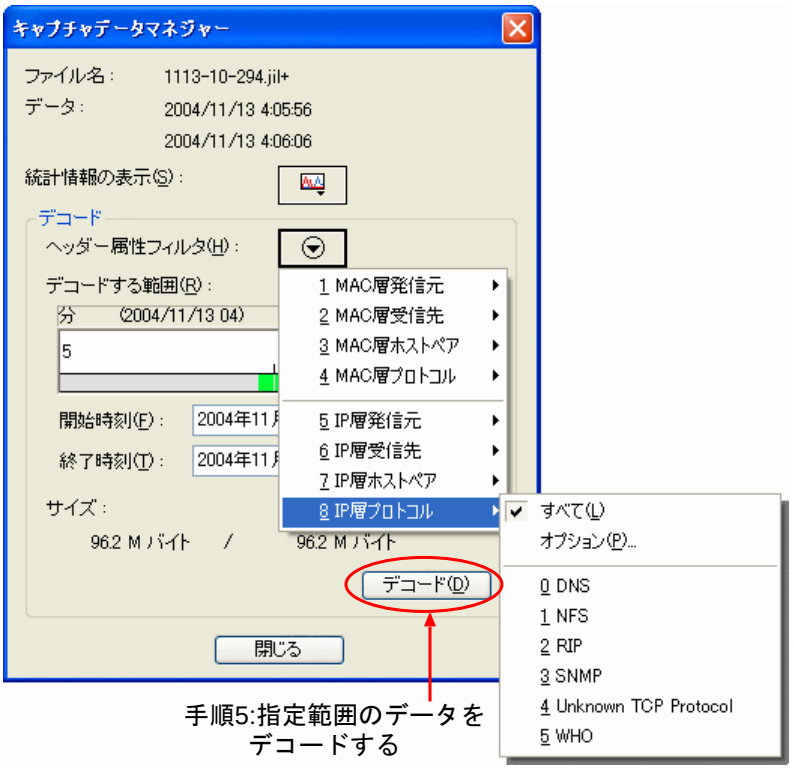


図 6-28: 「キャプチャデータマネジャー」ダイアログ (ヘッダー属性フィルタボタンをクリックしたところ)

メニューから項目と選ぶと、**ヘッダー属性フィルタ**ボタン(▼) の色が青に変わり、選んだ項目と一致する属性を持つパケットだけがデコードの対象となます。

範囲を指定すると、指定範囲のデータを読み込むために必要なメモリ使用量を表す**サイズ**が変わります。

5. **デコード(D)** ボタンをクリックします。

指定した範囲のパケットだけをデコードし、結果を表示したデコードビューが現れます。

6.11 連続キャプチャデータをデコードする

連続キャプチャデータは、 1 つずつ開いてデコードすることもできますが、デコードする範囲 (期間) を指定してデコードすることができます。

連続キャプチャデータをデコードする方法は 2 通りあります。

ひとつは、 ASTEC Eyes またはリモートモジュールに連続キャプチャデータの出力先として設定したディレクトリのデータを見る方法です。この方法では、連続キャプチャデータを出力した (している) ホストで ASTEC Eyes またはリモートモジュールが動作している必要があります。

もう一つは、 ASTEC Eyes やリモートモジュールと関係なく、連続キャプチャデータを保存しているディレクトリを指定して見る方法です。この方法では、連続キャプチャデータを保存しているホストで ASTEC Eyes またはリモートモジュールが動作している必要はありません。

6.11.1 連続キャプチャの出力先のディレクトリのデータをデコードする

1. インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**連続キャプチャデータの一覧を作成(A)** を選びます。
   「ホストのプロパティ」ダイアログの「連続キャプチャ」のページで指定したディレクトリに保存されている連続キャプチャデータの解析が始まり、進捗状況が「ASTEC Eyes」ダイアログに表示されます。
   連続キャプチャデータはネットワークインタフェースごとに分類されます。
   解析が終わると、インタフェースセレクタウィンドウ内に、ネットワークインタフェース毎の連続キャプチャデータのエントリが現れます。そのようすを図 6-29 に示します。

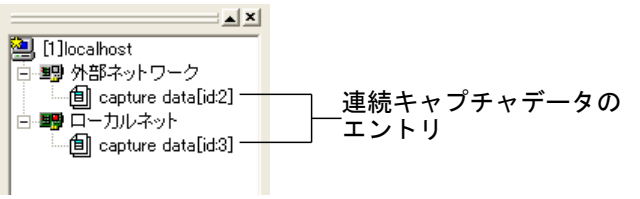


図 6-29: 連続キャプチャデータのエントリが現れたインタフェースセレクタウィンドウ

2. インタフェースセレクタウィンドウ内の連続キャプチャデータのエントリを右クリックしてポップアップメニューを開き、**連続キャプチャデータをデコードする(D)**. . . を選びます。
   図 6-30 のような「連続キャプチャデータの表示」ダイアログが現れます。

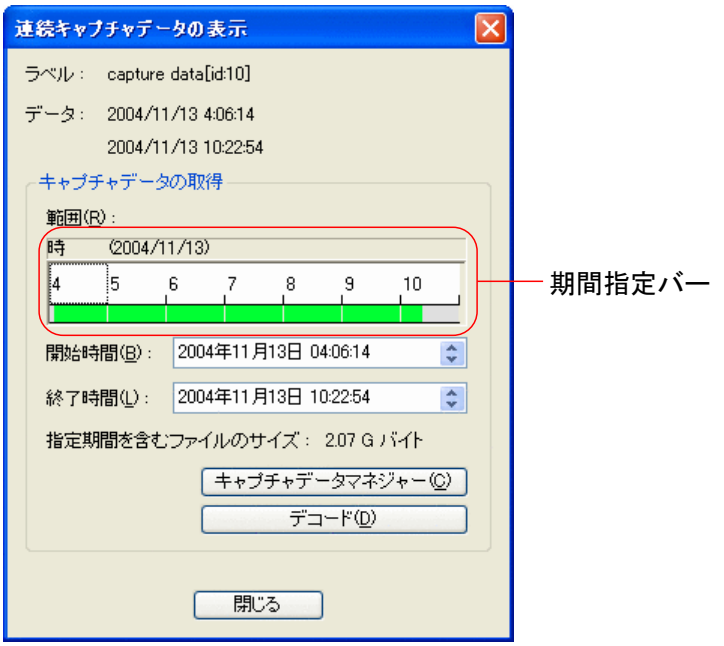


図 6-30: 「連続キャプチャデータの表示」ダイアログ

3. デコードする期間を指定します。
   開始時刻(B) と **終了時刻(L)** に日付と時刻を入力します。キー入力する変わりに、期間指定バーを使うこともできます。期間指定バーについては、「3.3.3　(緑色の) 期間指定バーを使う」 (62 ページ) を参照してください。
   期間を指定すると、「指定期間を含むファイルのサイズ」の値が変わります。ここの値は、指定した期間内のデータを含む 1 つ以上の**ファイルの合計サイズ**を表しています。
   指定した期間のデータを読み込むために必要なメモリのサイズではありません。
4. 指定した 期間内の全パケットをデコードする場合は、**デコード(D)** ボタンをクリックします。

4′. 指定した期間内のデータを読み込むために必要なメモリのサイズを知りたい場合や、パケットのヘッダー属性を使ってデコードするパケットを絞り込みたい場合は、**キャプチャデータマネジャー(C)** ボタンをクリックします。
   キャプチャデータマネジャーの使い方については、「6.10　キャプチャデータマネジャーを使う」 (159 ページ) を参照してください。

6.11.2 ディレクトリを指定して連続キャプチャデータをデコードする

1. 連続キャプチャデータのディレクトリを指定するために、「ディレクトリの参照」ダイアログを開きます。
   「ディレクトリの参照」ダイアログを開く方法は 2 つあります。
   - メインウィンドウの**ファイル(F)** メニューから**連続キャプチャのディレクトリを開く(J)**... を選びます。
   - インタフェースセレクタウィンドウ内の何も表示されていない部分を右クリックしてポップアップメニューを開き、**連続キャプチャのディレクトリを開く(J)**... を選びます。
2. 「ディレクトリの参照」ダイアログで連続キャプチャデータを保存してあるディレクトリを指定します。
   インタフェースセレクタウィンドウにディレクトリのエントリと連続キャプチャデータのエントリが現れます。そのようすを図 6-31 に示します。

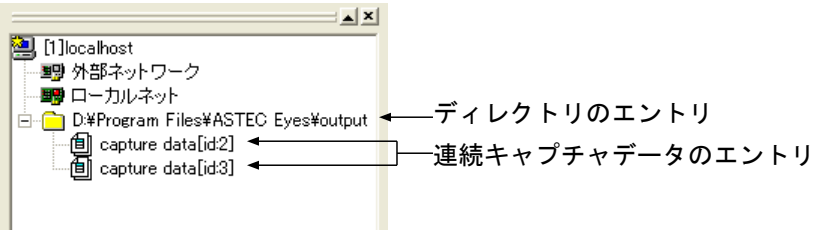


図 6-31: ディレクトリのエントリと連続キャプチャデータのエントリが現れたインタフェースセレクタウィンドウ

3. インタフェースセレクタウィンドウ内の連続キャプチャデータのエントリを右クリックしてポップアップメニューを開き、**連続キャプチャデータをデコードする(D)**... を選びます。
   図 6-32 のような「連続キャプチャデータの表示」ダイアログが現れます。

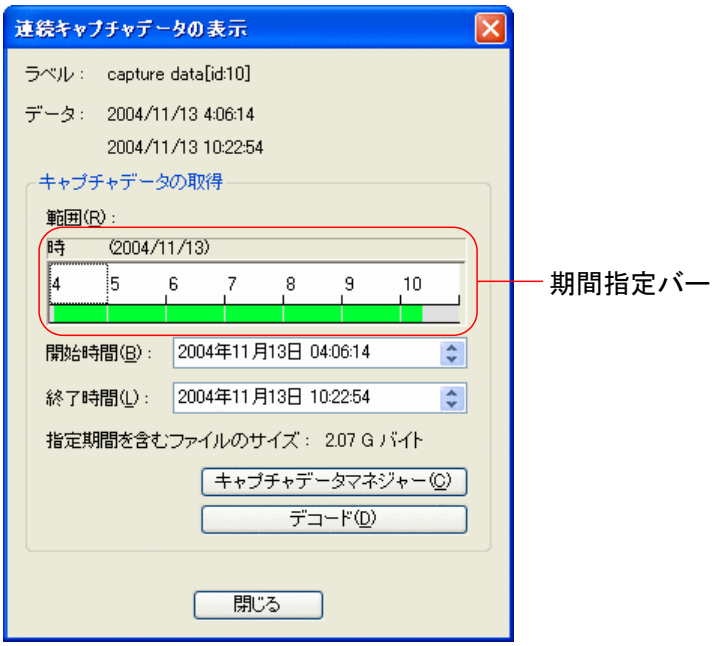


図 6-32: 「連続キャプチャデータの表示」ダイアログ

4. デコードする期間を指定します。
   開始時刻(B) と **終了時刻(L)** に日付と時刻を入力します。キー入力する変わりに、期間指定バーを使うこともできます。期間指定バーについては、「3.3.3　(緑色の) 期間指定バーを使う」 (62 ページ) を参照してください。
   期間を指定すると、「指定期間を含むファイルのサイズ」の値が変わります。ここの値は、指定した期間内のデータを含む 1 つ以上の**ファイルの合計サイズ**を表しています。
   指定した期間のデータを読み込むために必要なメモリのサイズではありません。
5. 指定した 期間内の全パケットをデコードする場合は、**デコード(D)** ボタンをクリックします。

5′. 指定した期間内のデータを読み込むために必要なメモリのサイズを知りたい場合や、パケットのヘッダー属性を使ってデコードするパケットを絞り込みたい場合は、**キャプチャデータマネジャー(C)** ボタンをクリックします。
   キャプチャデータマネジャーの使い方については、「6.10　キャプチャデータマネジャーを使う」 (159 ページ) を参照してください。

6.11.3 連続キャプチャデータのプロパティを見る

「連続キャプチャデータのプロパティ」ダイアログには、連続キャプチャデータのファイルの数やサイズ、 NIC ID、期間が表示されます。 NIC ID は、キャプチャモジュールが NIC を一意に識別できるように割り当てた ID です。

「連続キャプチャデータのプロパティ」ダイアログを開くには、インタフェースセレクタウィンドウ内の連続キャプチャデータのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**... を選びます。

図 6-33 のような「連続キャプチャデータのプロパティ」ダイアログが現れます。

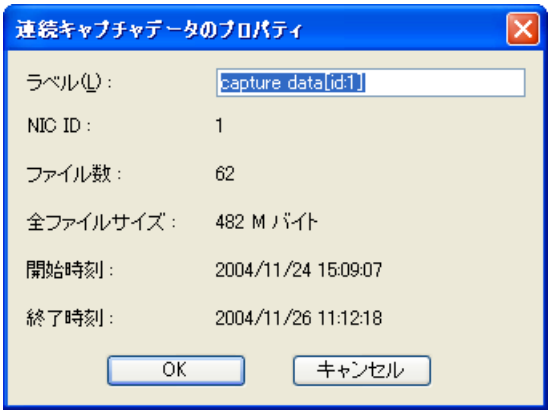


図 6-33: 「連続キャプチャデータのプロパティ」ダイアログ

このダイアログで連続キャプチャデータのエントリのラベルを変更することもできます。詳しくは「13.5 インタフェースセレクタウィンドウのラベルを変える」 (354 ページ) を参照してください。

6.12 ログのウィンドウで範囲を指定してデコードする

ログと連続キャプチャデータを関連付けると、ログを表示しているトラフィックウィンドウを見ながら、マウスのドラッグ操作でデコード範囲を指定できます。

ログを表示したトラフィックウィンドウで、連続キャプチャデータの範囲を指定してデコードするには、

手順 1　ログと連続キャプチャデータを関連付け (2 つの方法があります)、
手順 2　ログのトラフィックウィンドウを表示してから、範囲を指定してデコードします。

6.12.1 手順 1: ログと連続キャプチャデータを関連付ける (その 1)

ログと連続キャプチャデータを関連付ける方法は 2 通りあります。

ここでは、 ASTEC Eyes またはリモートモジュールにログおよび連続キャプチャデータの出力先として設定した 2 つのディレクトリを関連付ける方法を説明します。

この方法では、ログおよび連続キャプチャデータを出力した (している) ホストで ASTEC Eyes またはリモートモジュールが動作している必要があります。

1. インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**ログの一覧を作成(L)** を選びます。
   インタフェースセレクタウィンドウ内に、ネットワークインタフェース毎のログのエントリが現れます。
2. インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**連続キャプチャデータの一覧を作成(A)** を選びます。
   インタフェースセレクタウィンドウ内に、ネットワークインタフェース毎の連続キャプチャデータのエントリが現れます。そのようすを図 6-34 に示します。

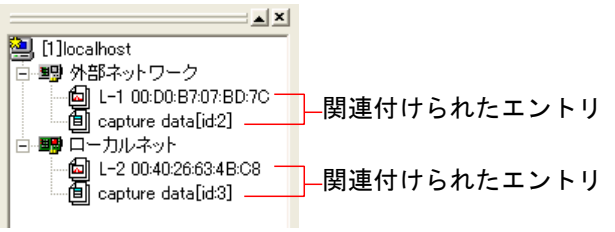


図 6-34: ログのエントリと連続キャプチャデータのエントリが関連付けられた状態

ここまでの操作でログと連続キャプチャデータは、ネットワークインタフェースごとに自動的に関連付けられます。

6.12.2 手順 1: ログと連続キャプチャデータを関連付ける (その 2)

ログと連続キャプチャデータを関連付ける方法は 2 通りあります。ここでは、ログおよび連続キャプチャデータを保存しているディレクトリを 1 つずつ指定して関連付ける方法を説明します。

この方法では、ログおよび連続キャプチャデータを保存しているホストで ASTEC Eyes またはリモートモジュールが動作している必要はありません。

1. ログのディレクトリを指定するために、「ディレクトリの参照」ダイアログを開きます。
「ディレクトリの参照」ダイアログを開く方法は 2 通りあります。
   - メインウィンドウの**ファイル(F)** メニューから**ログのディレクトリを開く(L)**... を選びます。
   - インタフェースセレクタウィンドウ内の何も表示されていない部分を右クリックしてポップアップメニューを開き、**ログのディレクトリを開く(L)**... を選びます。
2. 「ディレクトリの参照」ダイアログでログを保存してあるディレクトリを指定します。
インタフェースセレクタウィンドウにディレクトリのエントリとログのエントリが現れます。
3. 連続キャプチャデータのディレクトリを指定するために、「ディレクトリの参照」ダイアログを開きます。
「ディレクトリの参照」ダイアログを開く方法は 2 通りあります。
   - メインウィンドウの**ファイル(F)** メニューから**連続キャプチャのディレクトリを開く(J)**... を選びます。
   - インタフェースセレクタウィンドウ内の何も表示されていない部分を右クリックしてポップアップメニューを開き、**連続キャプチャのディレクトリを開く(J)**... を選びます。
4. 「ディレクトリの参照」ダイアログで連続キャプチャデータを保存してあるディレクトリを指定します。
インタフェースセレクタウィンドウにディレクトリのエントリと連続キャプチャデータのエントリが現れます。そのようすを図 6-35 に示します。

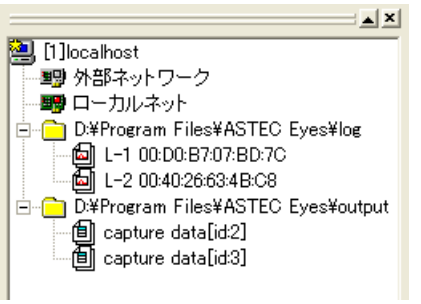


図 6-35: ログ、ディレクトリ、および連続キャプチャデータのエントリが現れたインタフェースセレクタウィンドウ

5. 連続キャプチャデータのエントリにマウスカーソルを合わせ、マウスの左ボタンを押し下げます。ボタンを押したままドラッグして、ログのエントリに重ねます。そのようすを図 6-36 に示します。

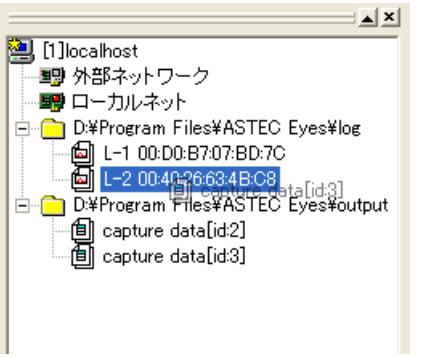


図 6-36: 連続キャプチャデータのエントリをログのエントリに重ねる

6. 連続キャプチャデータのエントリがログのエントリに重なったところで、マウスのボタンを放します。
ログのエントリの下に連続キャプチャデータのエントリが移動します。そのようすを図 6-37 に示します。

図 6-37: ログのエントリの下に移動した連続キャプチャデータのエントリ

ここまでの操作で、ログと連続キャプチャデータが関連付けられます。

ログのエントリと連続キャプチャのエントリを関連付ける際には、それぞれのプロパティに表示される NIC ID の値が対応するものを選ぶと良いでしょう。

6.12.3 手順 2: ログのウィンドウで範囲を指定してデコードする

手順 2 の操作は、連続キャプチャデータのエントリとログのエントリが関連付けられていることが前提です。

1. インタフェースセレクタウィンドウ内のログのエントリを右クリックしてポップアップメニューを開き、**ログを表示(L)**. . . を選びます。
   「ログの表示」ダイアログが現れます。
2. 「ログの表示」ダイアログで期間、プロット間隔、およびトラフィックの種類を指定して、トラフィックウィンドウを表示させます。
   詳しい操作方法については、「3.3.2 ディレクトリを指定してログを見る」 (60 ページ) を参照してください。
3. キャプチャデータインディケータを表示させます。
   そのためには、
   - トラフィックウィンドウのツールバーの**キャプチャデータインディケータ**ボタン() をクリックするか、
   - トラフィックウィンドウを右クリックしてポップアップメニューを開き、**キャプチャデータインディケータ(A)** を選びます。

   キャプチャデータインディケータの現れたトラフィックウィンドウのようすを図 6-38 に示します。

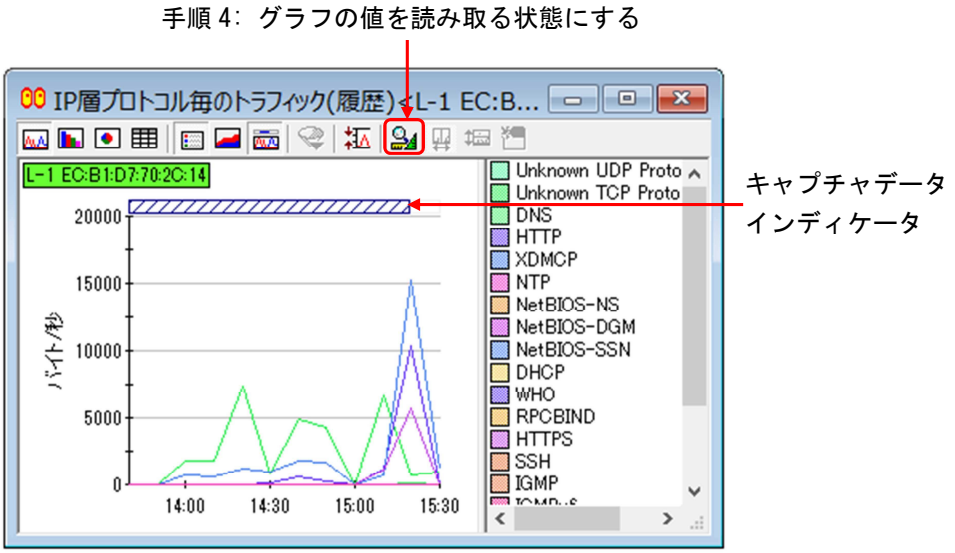


図 6-38: キャプチャデータインディケータの現れたトラフィックウィンドウ

青い斜線が引かれている部分は、連続キャプチャデータのある期間です。

4. ツールバーの**グラフ解析機能**ボタン() をクリックします。
5. ツールバーの**垂直カーソル**ボタン() をクリックします。
6. グラフの部分でマウスをドラッグして、デコード範囲を選びます。
   青い斜線が引かれている部分を選ぶようにします。デコード範囲を選んだ状態のトラフィックウィンドウのようすを図 6-39 に示します。

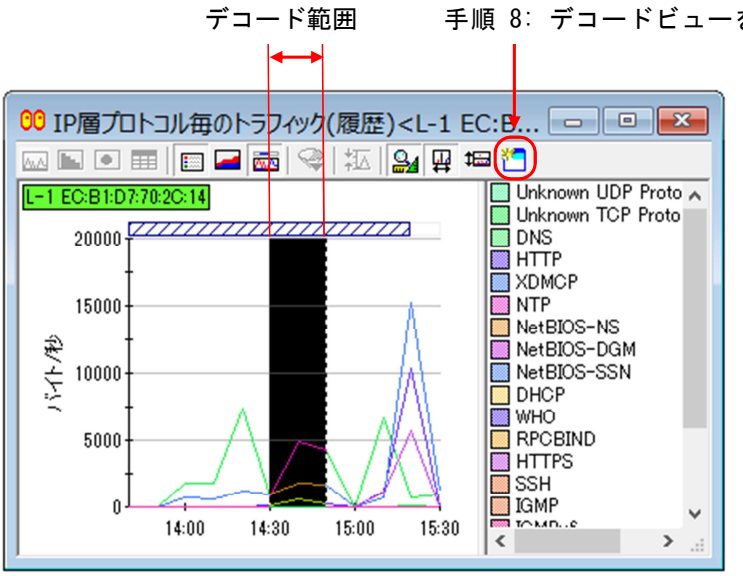


図 6-39: キャプチャデータインディケータの現れたトラフィックウィンドウ

青い斜線の区間内に必ずしもデータがあるわけではありません。キャプチャデータインディケータは指定した期間内において、最も古いパケットをキャプチャした時刻と最新のパケットをキャプチャした時刻の範囲を表しています。連続キャプチャを一時的に止めていた期間やパケットがまったく流れなかった期間にも青い斜線が表示されます。

7. ツールバーの**デコードビュー**ボタン( ) をクリックします。
「キャプチャデータマネジャー」ダイアログが現れます。「キャプチャデータマネジャー」ダイアログでデコード範囲をさらに絞り込むこともできます。
キャプチャデータマネジャーの使い方については、「6.10　キャプチャデータマネジャーを使う」 (159 ページ) を参照してください。
8. 「キャプチャデータマネジャー」ダイアログの**デコード(D)** ボタンをクリックします。
指定した範囲のデータをデコードしたデコードビューが現れます。

6.12.4　ログと連続キャプチャデータの関連付けを解除する

ディレクトリを指定してログと連続キャプチャデータを関連付けた場合は、関連付けを解除できます。

そのためには、インタフェースセレクタウィンドウ内の連続キャプチャデータのエントリを右クリックしてポップアップメニューを開き、**関連付けを解除(U)** を選びます。

6.13 デコード時のエラー

間違ったデコードヒントを設定してデコードしたときや、誤りを含むデータをデコードしたときなど、正しくデコードできないことがあります。

パケットのデコード時にエラーが起きた場合、デコードビューのサマリ領域のフレーム ID のチェックボックスが赤に変わります (■)。 また、メインウィンドウのメッセージウィンドウにデコードできなかったパケットのフレーム ID とプロトコル名を含むメッセージを表示します。

エラーが起きたことを表わすメッセージの例を次に示します。

```
!!! DECODER EXCEPTION [frameid 2467] (0xE0000006 in EVAL_PACKET of FTP) !!!
!!! DECODER EXCEPTION [frameid 2469] (0xE0000006 in EVAL_PACKET of FTP) !!!
!!! DECODER EXCEPTION [frameid 2471] (0xE0000006 in EVAL_PACKET of FTP) !!!
```

上記のようなエラーメッセージが表示された場合は、必要なデータ (設定情報とキャプチャデータ) を保存して、 ASTEC Eyes を一旦終了されることをおすすめします。また、デコードヒントを正しく設定しているにもかかわらず、エラーが起きた場合には、サポートまでご連絡ください。

7章

トラフィックジェネレータ機能

新たに作成したパケットやキャプチャしたパケットをネットワークに送信する機能です。キャプチャしたパケットの内容は変更してから送信できます。また、送信の際の時間間隔を指定することもできます。

7.1 新たにパケットを作成して送信する

7.1.1 新しいパケットを作成する

メインウィンドウの**ツール(T)** メニューから**パケット送信(M)**... を選び、ダイアログを開きます。

図 7-1にパケットを作成するダイアログを示します。

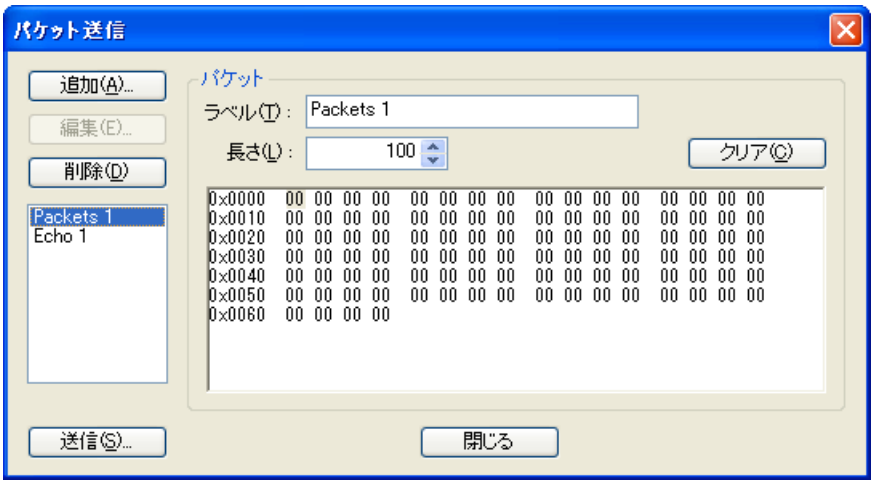


図 7-1: パケットを作成するダイアログ

追加(A)... ボタンをクリックしてメニューを開き、パケットの種類を選びます。

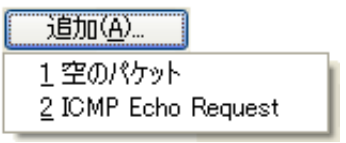


図 7-2: 追加(A)... ボタンのメニュー

1 空のパケットを選ぶと、すべてのデータの値が 0x00 である新しいパケットが作られます。
2 ICMP Echo Request を選ぶと、パケットの内容を入力する「パケット生成パラメータ」ダイアログが現れます。

図 7-3: パケットを作成するダイアログ

「パケット生成パラメータ」ダイアログでは、 MAC アドレスと IP アドレスを指定できます。また、 ICMP Echo リクエストパケットのデータも編集できます。

データは編集は次のようにします。

1. **データ** 領域の**長さ(L)** にデータの長さを入力します。
2. **パケット編集** 領域のデータをクリックします。クリックしたデータが反転します。
3. データの値を 16 進数で入力します。

7.1.2 パケットの内容を編集する

作成したパケットは「パケット送信」ダイアログ (図 7-1) の左側に表示されている**パケットリスト**に追加されます。

パケットのデータは、「パケット送信」ダイアログの**パケット** 領域で変更できます。

1. **パケットリスト**で変更したいパケットをクリックします。
2. **長さ(L)** にパケットの長さを入力します。

3. **パケット編集** 領域のデータをクリックします。クリックしたデータが反転します。
4. データの値を 16 進数で入力します。

クリア(C) ボタンをクリックするとパケットのすべてのデータを 0x00 に初期化します。

ラベル(T) にラベルを入力すると、**パケットリスト**に表示されるパケットのラベルを変更できます。

ICMP Echo リクエストパケットの場合は、**パケット編集ウィンドウ**ボタン() をクリックして「パケット生成パラメータ」ダイアログで再編集できます。

パケットを送信する前にダイアログを閉じても、次に開いたときには直前に作成したパケットが表示されます。

7.1.3 パケットを削除する

不要なパケットを作ってしまったときには削除できます。

1. **パケットリスト**で不要なパケットをクリックします。
2. **削除(D)** ボタンをクリックします。

7.2 パケットを送信する

パケットの送信は、ローカルホストのネットワークインタフェースから行います。リモートモジュールのネットワークインタフェースからはパケットを送信できません。

パケットを送信するには、次のようにします。

1. 送信に使うネットワークインタフェースを選びます。
2. 「パケット送信」ダイアログ (図 7-1) で**送信(S)**. . . ボタンをクリックします。図 7-4に示すようなパケットを送信するダイアログが現れます。

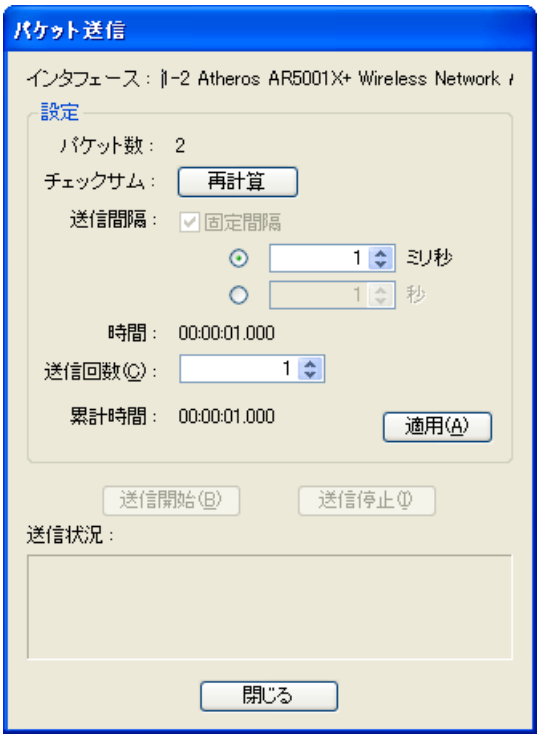


図 7-4: パケットを送信するダイアログ

3. チェックサムを計算させてパケットに設定する場合は、チェックサムの**再計算**ボタンをクリックします。パケットに設定できるのは、 IP ヘッダー、 ICMP ヘッダー、 TCP ヘッダー、および UDP ヘッダーのチェックサムです。

4. **送信間隔**にはパケットを送信するときの時間間隔を入力します。

送信間隔として 0 ミリ秒または 0 秒を選ぶと、可能な限り短い時間間隔で送信します。

5. **送信回数(C)** には送信の繰り返し回数を入力します。 5 個のパケットを作成し、送信回数を 2 回にしたときは、全部で 10 個のパケットが送信されます。
6. **適用(A)** ボタンをクリックします。**時間**にはパケット列を 1 回送信するのにかかる時間が、**累計時間**には全部のパケットを送信するのにかかる時間が表示されます。
7. **送信開始(B)** ボタンをクリックします。

ネットワークインタフェースを選ぶ方法については、「1.2.1　インタフェースを選ぶ」 (10 ページ) を参照してください。

送信状況 領域にパケットの送信状況が表示されます。また、パケットの送信中に**送信停止(I)** ボタンをクリックすると、送信が停止します。

7.3 キャプチャしたパケットを編集して送信する

7.3.1 パケット編集ウィンドウを開く

キャプチャしたパケットの一部を送信したり、内容を編集してから送信することができます。

キャプチャしたパケットを送信するには、最初にパケット編集ウィンドウを開きます。

1. 送信したいパケットを表示しているデコードビューをクリックします。
2. デコードビューのツールバーの**パケット編集ウィンドウ**ボタン( ) をクリックします。図 7-5に示すようなパケット編集ウィンドウが表示されます。

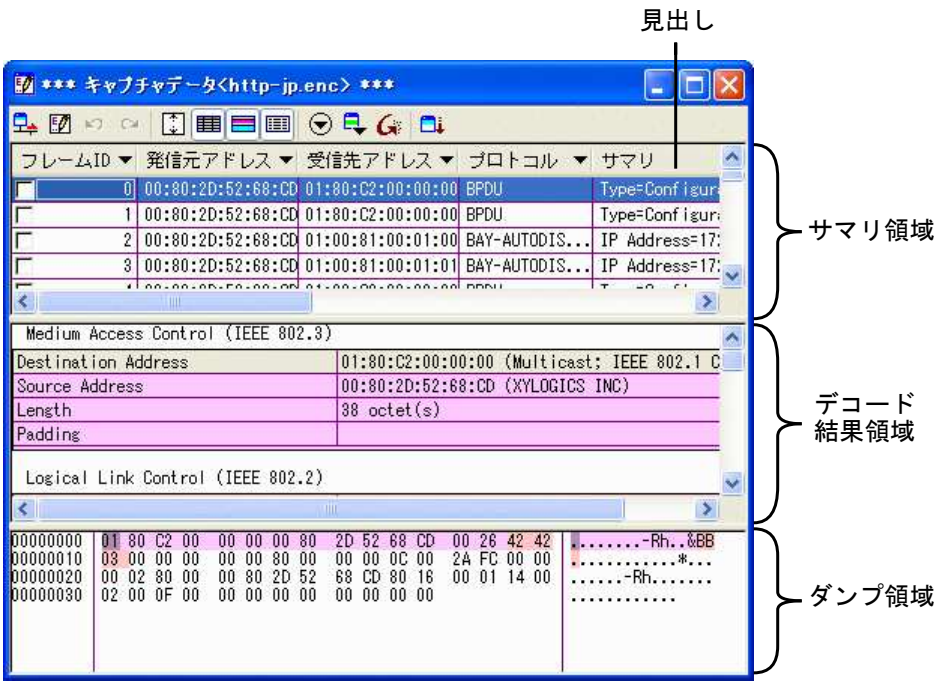


図 7-5: パケット編集ウィンドウ

パケット編集ウィンドウもデコードビューと同じように、大きく 3 つの領域に分けられます。サマリ領域とデコード結果領域とダンプ領域です。サマリ領域はパケットの概要を表示します。デコード結果領域は、サマリ領域で選んだパケットの解析結果を表示します。ダンプ領域

は、パケットのデータを 16 進ダンプの形式で表示します。また、パケットのデータの編集もダンプ領域で行います。

送信されるパケットを制限するには、フィルタを使ってデコードビューに表示するパケットを制限してから、パケット編集ウィンドウを開きます。

パケット編集ウィンドウでもデコードビューと同じように、見出しフィルタやヘッダー属性フィルタ、デコード結果フィルタを利用できますが、パケット編集ウィンドウ上のパケットは表示、非表示に関わらず送信されます。

7.3.2 パケットの内容を編集する

パケットの内容を編集するには、次のようにします。

1. サマリ領域で編集したいパケットをクリックします。
2. ダンプ領域で編集したいデータをクリックします。クリックしたデータが反転します。
3. データの値を 16 進数で入力します。

変更したパケットについては、サマリ領域のフレーム ID の前に * マークが表示されます。変更後のパケットの解析結果を表示するには、パケット編集ウィンドウのツールバーの**再デコードボタン**() をクリックします。

7.3.3 パケット編集ツールを使う

パケット編集ツールを使えば、アドレスやプロトコルの特定のフィールドの値を容易に変更できます。また、複数のパケットのデータをまとめて変更することもできます。

パケット編集ツールを開くには、パケット編集ウィンドウのツールバーの**パケット編集ツール**ボタン ( ) をクリックします。図 7-6に示すようなダイアログが表示されます。

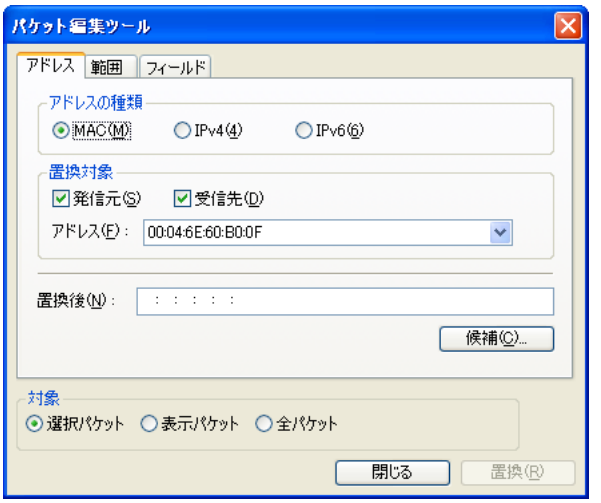


図 7-6: パケット編集ツール (「アドレス」のページ)

「アドレス」のページでは変更前のアドレスと変更後のアドレスを指定して、パケットに含まれるアドレスの情報を書き換えます。変更できるアドレスの種類は、 MAC アドレス、 IPv4 アドレス、 IPv6 アドレスの 3 種類です。

変更するアドレスを指定したら、変更するパケットの範囲を**選択パケット**、**表示パケット**、**全パケット**から選び、**置換(R)** ボタンをクリックします。

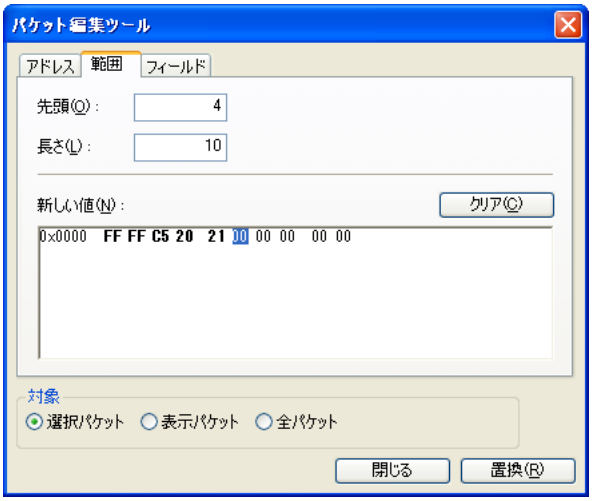


図 7-7: パケット編集ツール (「範囲」のページ)

「範囲」のページでは指定した範囲のデータを変更します。**先頭(O)** には変更する最初のデータの位置を、**長さ(L)** には変更するデータの長さ (バイト数) を入力します。パケットの最初のデータから変更するときには、**先頭(O)** に 0 を入力します。

指定した長さのデータが**新しい値(N)** に表示されるので、変更後の値に書き換えます。

対象領域から変更する範囲を選んで**置換(R)** ボタンをクリックします。

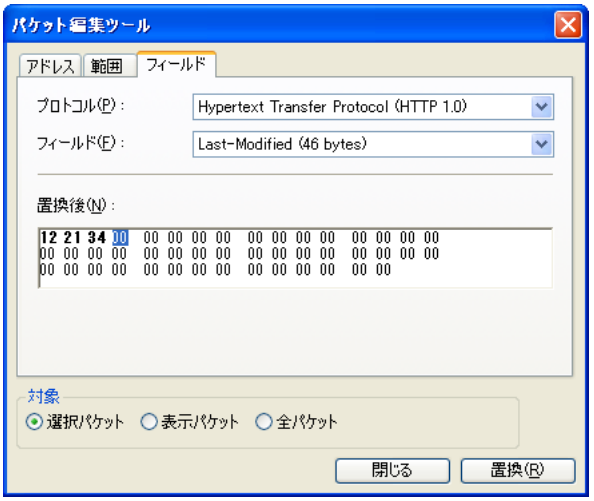


図 7-8: パケット編集ツール (「フィールド」のページ)

「フィールド」のページではプロトコルのフィールドの値を変更します。**プロトコル(P)** で選んだプロトコルと、**フィールド(F)** で選んだフィールドに対応する長さのデータが**置換後(N)** に表示されます。データをマウスでクリックして変更後の値に書き換えます。

選択しているパケットに含まれるプロトコルの一覧が、**プロトコル(P)** の項目として表示されます。

対象領域から変更する範囲を選んで**置換(R)** ボタンをクリックします。

アドレス、範囲、フィールドのうち複数を指定した場合でも、**置換(R)** ボタンをクリックしたときに表示されているページで指定した変更だけが反映されます。

7.3.4 編集の取り消しと繰り返し

編集作業を取り消して編集前の内容に戻したり、取り消した編集作業をもう一度実行したりできます。

編集作業を取り消すには、パケット編集ウィンドウのツールバーの**元に戻す**ボタン ( ) を、もう一度実行するには**やり直し**ボタン ( ) をクリックします。

7.3.5 パケット編集ウィンドウのパケットを送信する

パケット編集ウィンドウのツールバーの**パケット送信**ボタン ( ) をクリックします。図 7-4に示したパケットを送信するダイアログが表示されます。

パケットを送信する方法については、「7.2 パケットを送信する」 (180 ページ) を参照してください。

8章

リモート監視機能

スタンドアローンの ASTEC Eyes が監視できるのは、リピータハブ (シェアードハブ) で接続されている同一セグメント内のトラフィックだけです。スイッチングハブの異なるポートに接続されたネットワークのトラフィックは見えません。

お使いのスイッチングハブにポートミラーリングの機能がある場合は、ポートミラーリングの機能を設定すれば、指定したポートのトラフィックを見ることができるでしょう。しかし、スイッチングハブにポートミラーリングの機能がない場合や、あっても設定が煩雑である場合などは、 ASTEC Eyes のリモートモジュールを使うと便利です。リモートモジュールを使えば、簡単に別のセグメントのトラフィックを監視できます。

リモートモジュールには、 ASTEC Eyes 基本パッケージと同じモニタ機能、キャプチャ機能、ログ機能、およびエキスパート機能があります。離れた場所にあるホストにリモートモジュールをインストールしておけば、ローカルホストで ASTEC Eyes を起動してリモートモジュールに接続するだけで、離れた場所にあるネットワークの状態を監視できます。その操作は、ローカルホスト (localhost) が接続しているネットワークに対して行う操作とまったく同じです。別の PC にインストールした ASTEC Eyes をリモートモジュールとして接続することもできます。

接続しているリモートモジュールのホスト名、インタフェース、およびその状態はインタフェースセレクタウィンドウに表示されます。

8.1 リモートモジュールに接続する

リモート監視機能を使うには、別のホスト上で動作しているリモートモジュールまたは ASTEC Eyes に接続します。接続するだけで、ローカルホストで動作している ASTEC Eyes とまったく同じように、リモートモジュールを操作できるようになります。

8.1.1 インタフェースセレクタウィンドウにエントリの無いホストに接続する

1. 「接続」ダイアログを開きます。
   「接続」ダイアログを開く方法は 2 通りあります。
   - メインウィンドウの**ファイル(F)** メニューから**リモートへの接続(C)**... を選びます。
   - インタフェースセレクタウィンドウ内の何も表示されていない部分を右クリックしてポップアップメニューを開き、**リモートへの接続(C)**... を選びます。

   図 8-1 ような「接続」ダイアログが現れます。

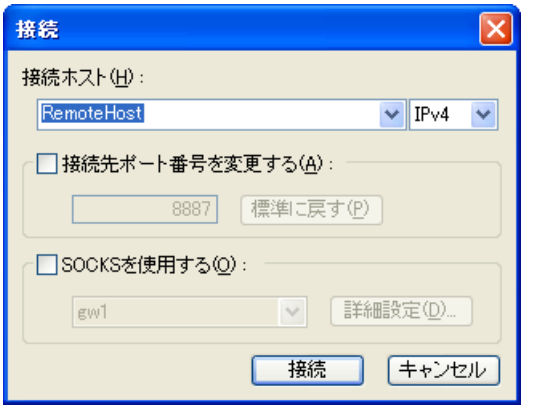


図 8-1: 「接続」ダイアログ

2. **接続ホスト(H)** に IP アドレスまたはホスト名を入力します。
   これまでに入力したことのあるホストであれば、ドロップダウンコンボボックスから選ぶこともできます。
   ローカルホストが識別できる NetBIOS 名や DNS 名、 IP アドレスなどを指定します。
   また、リモートモジュールの動作しているホストと IPv6 で接続する場合は、ホスト名の右側にあるドロップダウンボックスで **IPv6** を選びます。

3. ASTEC Eyes は TCP プロトコルのポート番号 8887 を使ってリモートモジュールと接続します (『ASTEC Eyes リリースノートとインストール』の 2 章「インストール」の「ASTEC Eyes 基本パッケージとリモートモジュール」の節を参照してください)。
   SSH のポートフォワーディングなどを使っていて、標準とは異なるポート番号に接続したい場合は、ポート番号を指定します。
4. 接続するリモートモジュールに直接接続できない場合、 ASTEC Eyes は SOCKS サーバー経由で接続することもできます。
   SOCKS サーバーの設定については、「11.9　SOCKS のオプションを設定する」 (313 ページ) を参照してください。
5. **接続**ボタンをクリックします。

指定したホストで動作しているリモートモジュールと接続できた場合は、ホストのエントリとインタフェースのエントリがインタフェースセレクタウィンドウに現れます。そのようすを図 8-2 に示します。

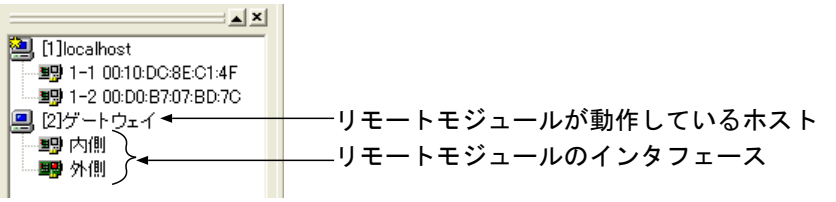


図 8-2: インタフェースセレクタウィンドウに現れたリモートモジュールのホストとインタフェース

接続できなかった場合は、エラーメッセージを表示したダイアログが現れます。

8.1.2 インタフェースセレクタウィンドウにエントリのあるホストに接続する

インタフェースセレクタウィンドウのホストのアイコンに**使えない状態にあることを示す** (✕) が重なって表示されている場合、そのホストとは接続が切れていることを表します。

接続の切れているホストに再接続するには、インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**接続(C)** を選びます。

インタフェースセレクタウィンドウにエントリのないホストと接続するときと同じようにして、「接続」ダイアログを使うこともできます。

8.2 リモートモジュールとの接続を切る

リモートモジュールとの接続を切るには、インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**切断(S)** を選びます。

図 8-3 に示すように、接続の切れたホストのアイコンの上には、**使えない状態にあることを示す** (✕) が重なって表示されます。

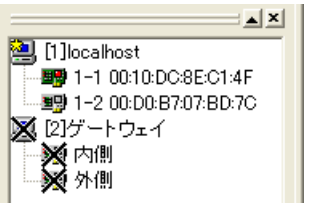


図 8-3: 接続の切れたリモートモジュールのホストとインタフェース

接続が切れると、モニタ、キャプチャ、およびログの表示などはできなくなります。

インタフェースセレクタウィンドウから接続を切ったホストのエントリを削除したい場合は、インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**削除(D)** を選びます。

8.3 設定権限の取得と解放

次の操作を行うためには、設定権限が必要です。

- 連続キャプチャ機能を設定する
- 連続キャプチャフィルタ、連続キャプチャ開始トリガ、および連続キャプチャ停止トリガを適用する。
- ログ機能を設定する
- インタフェースのラベルを変えて記憶させる
- モニタをリセットする
- インタフェースを有効または無効にする
- モニタエキスパート機能を設定する
- 通知機能を設定する
- SNMP 機能を設定する

設定権限があるかどうかは、インタフェースセレクタウィンドウのホストのアイコンで確認できます。ホストのアイコンが「**設定権限のあるホスト** () 」の場合は設定権限があります。「**設定権限のないホスト** () 」の場合は設定権限がありません。

8.3.1 設定権限を得る

リモートモジュールの設定権限を得る方法は 2 通りあります。

- **設定権限を得る方法 1** インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**設定権限を取得(G)** を選びます。
- **設定権限を得る方法 2**
  1. インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。「ホストのプロパティ」ダイアログが現れます。
  2. **取得(G)** ボタンをクリックします。

設定権限が得られた場合は、ホストのアイコンが**設定権限のあるホスト** () に変わります。

他の ASTEC Eyes が設定権限を持っている場合、設定権限は取得できません。

ローカルホストについては、 ASTEC Eyes を起動したときに自動的に設定権限の取得を試みます。

8.3.2 設定権限を解放する

設定権限を解放する方法は 2 通りあります。

- **設定権限を解放する方法 1** インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**設定権限を解放(F)** を選びます。
- **設定権限を解放する方法 2**
  1. インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。 「ホストのプロパティ」ダイアログが現れます。
  2. **解放(R)** ボタンをクリックします。

設定権限を解放できた場合は、ホストのアイコンが**設定権限のないホスト** () に変わります。

8.4 基本パッケージとリモートモジュール間の通信

リモートモジュールと接続した場合、リモートモジュールと ASTEC Eyes 基本パッケージとの間で情報をやり取りするために、ネットワークのトラフィックが増えます。モニタの場合は、ネットワークの状態にも依存しますが、 3~4Kbps くらいの帯域を使います。リモートモジュールでキャプチャしたデータをデコードする場合は、デコードビューを作成する際にキャプチャした全データがそのまま転送されます。そのため、キャプチャしたデータ量に比例して使う帯域が増加します。

キャプチャしたデータを転送する際、データを圧縮することによって転送量を減らすことができます。そのためには、次の設定を行います。

1. 「オプション設定」ダイアログを開きます。「オプション設定」ダイアログを開く方法は 2 通りあります。
   - コモンツールバーの**オプション設定**ボタン() をクリックします。
   - メインウィンドウの**設定(O)** メニューから**オプション設定(O)**. . . を選びます。
2. ダイアログの左側にあるツリーの中の**キャプチャ**をクリックします。
3. 圧縮するかどうかは、インタフェースごとに設定します。
   インタフェース(I) のドロップダウンリストボックスでインタフェースを選びます。
4. **データを圧縮して取り込む(C)** にチェックを付けます。
5. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

9章

フィルタエディタ

フィルタエディタでは、次のフィルタを使うために必要な論理式を編集します。

ディスプレイフィルタ
デコードビューに表示する解析結果を絞り込むために使います。

モニタフィルタ トラフィックウィンドウに表示する統計情報を絞り込むために使います。モニタフィルタの設定が有効になるトラフィックウィンドウは次の通りです。

- MAC 層トラフィック
- MAC 層発信元毎のトラフィック
- MAC 層受信先毎のトラフィック
- MAC 層ホストペア毎のトラフィック
- MAC 層プロトコル毎のトラフィック
- IP 層トラフィック
- IP 層発信元毎のトラフィック
- IP 層受信先毎のトラフィック
- IP 層ホストペア毎のトラフィック
- IP 層プロトコル毎のトラフィック
- MAC 層アドレスタイプ毎のトラフィック

イベントフィルタ エキスパート機能でイベントを検出する条件を指定します。

キャプチャフィルタ キャプチャするパケットを絞り込むために使います。

キャプチャ開始トリガ キャプチャを開始するきっかけとなる条件を指定します。

キャプチャ停止トリガ キャプチャを停止するきっかけとなる条件を指定します。

連続キャプチャフィルタ
連続キャプチャをするとき、キャプチャするパケットを絞り込むために使います。

連続キャプチャ開始トリガ
連続キャプチャを開始するきっかけとなる条件を指定します。

連続キャプチャ停止トリガ
連続キャプチャを停止するきっかけとなる条件を指定します。

9.1 フィルタエディタを起動する

フィルタエディタを起動する方法は 2 通りあります。

- メインウィンドウの**編集(E)** メニューから**フィルタエディタ(E)**... を選びます。
- **<Ctrl-E>** キーを押します。

図 9-1 に示すような、フィルタエディタが現れます。

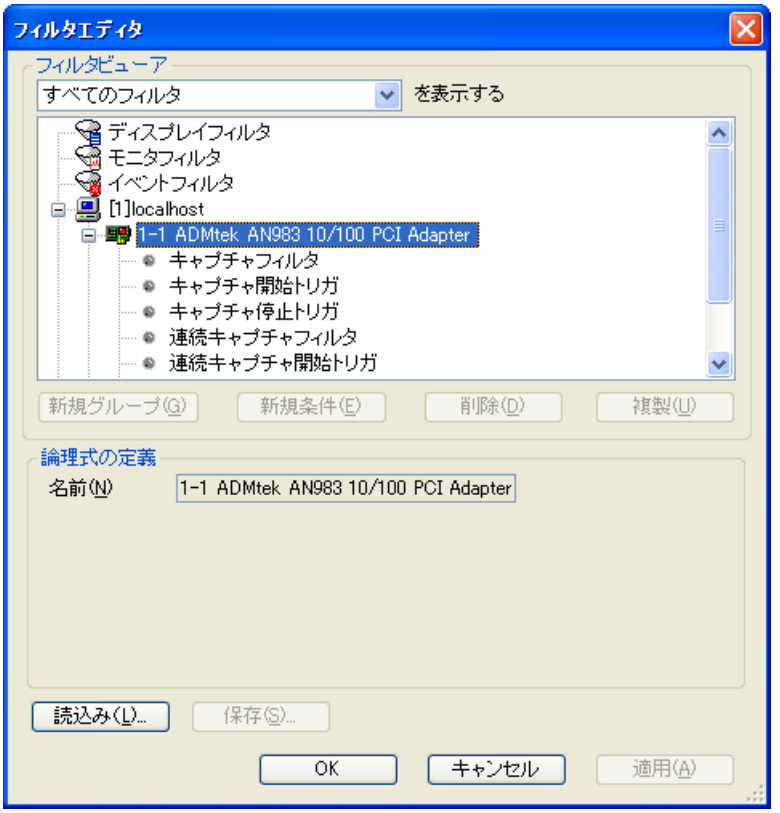


図 9-1: フィルタエディタ

9.1.1 フィルタエディタの構成

フィルタビューア領域

フィルタ別の論理式をツリーで表示します。操作の対象となるフィルタや論理式を選びます。コピーアンドペーストやドラッグアンドドロップの操作が行えます。ポップアップメニューを使うこともできます。上部にあるドロップダウンリストボックスを使うと、ネットワークインタフェースやフィルタの種類によって、表示内容を制限したり分類したりすることができます。

論理式の定義領域 フィルタビューア領域で条件論理式を選んでいる場合は、具体的な値を設定します。また、条件グループの名前や条件を変えたり、ディスプレイフィルタとモニタフィルタの名前を変更できます。

「条件論理式」および「条件グループ」については、「9.2 論理式を構成する部品」 (200 ページ) を参照してください。

読み込み(L)... ボタン、保存(S)... ボタン

編集したフィルタをファイルに保存したり、ファイルから読み込んだりするためのボタンです。

9.1.2 フィルタビューア領域で使われるアイコン

フィルタビューア領域で論理式の状態をわかりやすく表示するために、いくつかのアイコンを使います。

(灰色のアイコン)

キャプチャフィルタ、キャプチャ開始トリガ、キャプチャ停止トリガ、連続キャプチャフィルタ、連続キャプチャ開始トリガ、および連続キャプチャ停止トリガのフィルタ名の左側に表示されます。論理式が何も入力されていないことを表します。

(ピンク色のアイコン)

フィルタ名の左側に表示されます。適用されていない論理式があることを表します。

(緑色のアイコン)

フィルタ名の左側に表示されます。正しい論理式が入力され、適用されていることを表します。

(赤色のアイコン)

適用(A) ボタンまたは **OK** ボタンをクリックすると、 ASTEC Eyes は入力した論理式を評価し、正しければ適用します。正しくない論理式が見つかった場合、その論理式の左側に赤色のアイコンを表示します。論理式が修正されるまで適用されません。

(黄色のアイコン)

無効にされている論理式の左側に表示されます。

(赤色のアイコン)

ドラッグアンドドロップ操作で論理式を移動したとき、ドラッグした論理式に含まれる条件論理式がドロップ先のフィルタでは使えないことを示します。コピーアンドペースト操作で論理式を複製したとき、コピーした論理式に含まれる条件論理式がペースト先のフィルタでは使えないことを示します。

9.2 論理式を構成する部品

フィルタエディタでは、論理式を構成する 2 種類の部品が提供されます。一つは**条件グループ**で、もう一つは**条件論理式**です。

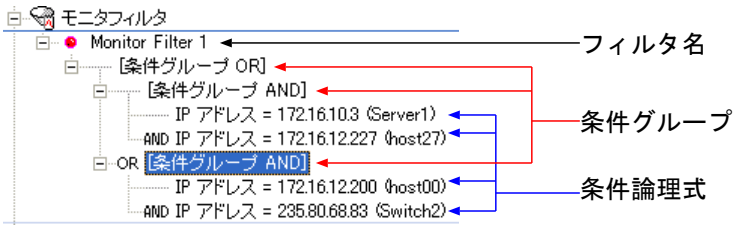


図 9-2: 条件グループと条件論理式

9.2.1 条件グループ

条件グループとは、その下にある複数の論理式の結合条件を決める部品です。**条件グループ AND** はその下にある複数の論理式を AND で結合します。 **条件グループ OR** はその下にある複数の論理式を OR で結合します。条件グループの下には、条件グループまたは条件論理式が必要です。条件グループだけの論理式は無効です。条件グループは、それ自身を 1 階層と数えます。

9.2.2 条件論理式

条件論理式とは、具体的な値を設定するための部品です。必ず条件グループの下に置かれ、設定する条件によって別の条件グループまたは条件論理式と OR または AND で結合します。

表 9-1 に条件論理式の一覧を示します。フィルタによって、使えない条件論理式もあります。各フィルタで使える条件論理式にチェックマークを付けています。

表 9-1: 条件論理式の種類

	ディスプレイフィルタ	モニタフィルタ	イベントフィルタ	キャプチャフィルタ キャプチャ開始トリガ キャプチャ停止トリガ 連続キャプチャフィルタ 連続キャプチャ開始トリガ 連続キャプチャ停止トリガ
MAC アドレス	✓	✓	✓	✓
IEEE 802 Encapsulation	✓		✓	✓
Ethernet ヘッダーの Type フィールド	✓	✓	✓	✓
Ethernet アドレスタイプ	✓	✓	✓	✓
Ethernet サイズ	✓		✓	✓
LLC Service Access Point	✓	✓	✓	✓
IP アドレス	✓	✓	✓	✓
IP ネットワークアドレス	✓	✓	✓	✓
IP ヘッダーの Protocol フィールド	✓	✓	✓	✓
IPv6 アドレス	✓	✓	✓	✓
IPv6 マスクアドレス	✓	✓	✓	✓
IPv6 ヘッダーの Next Header フィールド	✓	✓	✓	✓
UDP ポート番号	✓	✓	✓	✓
TCP ポート番号	✓	✓	✓	✓
TCP ステータス			✓	✓
TCP ヘッダーの Flags フィールド	✓		✓	✓
解析パケットのステータス			✓	✓
データ比較	✓		✓	✓
キャプチャ開始タイマー				キャプチャ開始トリガおよび 連続キャプチャ開始トリガのみ
キャプチャ停止タイマー				キャプチャ停止トリガおよび 連続キャプチャ停止トリガのみ
フレーム ID	✓			
時刻	✓			
プロトコル			✓	✓
エキスパートイベント数			✓	✓

9.3 フィルタ別の制約

フィルタによって、次のような制約があります。

- ディスプレイフィルタ
- モニタフィルタ
- イベントフィルタ
  - ネットワークインタフェースに関係なく 250 個まで定義できます。
  - 論理式の階層は 250 階層まで定義できます。
- キャプチャフィルタ
- キャプチャ開始トリガ
- キャプチャ停止トリガ
  - ネットワークインタフェース 1 つにつき 1 つずつ定義できます。
  - フィルタの名前は変えられません。
- 連続キャプチャフィルタ
- 連続キャプチャ開始トリガ
- 連続キャプチャ停止トリガ
  - ネットワークインタフェース 1 つにつき 1 つずつ定義できます。
  - フィルタの名前は変えられません。
  - フィルタを設定するためには、連続キャプチャを行うインタフェースがインストールされているホストに対して設定権限が必要です。
  - 接続したリモートモジュールにこれらのフィルタが設定されている場合、接続時に自動的に読み込みます。

9.4 論理式の編集

この節では、フィルタエディタで論理式を編集する手順について説明します。論理式の入力はキー入力以外に、コピーアンドペーストやドラッグアンドドロップ操作が使えます。

9.4.1 論理式の編集を始める

ディスプレイフィルタまたはモニタフィルタの編集を始める方法は 2 通りあります。

- **ボタンを使う**
  1. フィルタビューア領域で編集したいフィルタのアイコンまたはそのラベルをクリックします。
  2. **新規グループ(G)** ボタンまたは**新規条件(E)** ボタンをクリックします。
- **ポップアップメニューを使う**
  1. フィルタビューア領域で編集したいフィルタのアイコンまたはそのラベルを右クリックして、ポップアップメニューを開きます。
  2. ポップアップメニューから**新規グループ(G)** または**新規条件(E)** を選びます。

1 階層目の論理式として条件グループ OR が作られます。 2 階層目の論理式はどちらを選んだかで異なります。**新規グループ(G)** を選んだ場合は条件グループ AND が、**新規条件(E)** を選んだ場合は条件論理式が作られます。論理式を 3 階層より多くしたいときは**新規グループ(G)** を、 3 階層までの場合は**新規条件(E)** を選びます。

ディスプレイフィルタをクリックして**新規グループ(G)** を選ぶと、図 9-3 のようになります。「Display Filter 1」というフィルタの 1 階層目の論理式として条件グループ OR が、 2 階層目の論理式として条件グループ AND が作られます。 3 階層目には、条件グループでも条件論理式でも追加できるようになっています。「Display Filter 1」の左側のアイコンは (ピンク色) です。

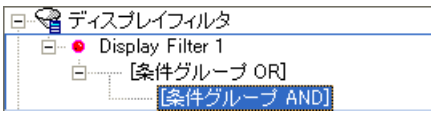


図 9-3: ディスプレイフィルタをクリックして、新規グループを選んだところ

モニタフィルタをクリックして**新規条件(E)** を選ぶと、図 9-4 のようになります。「Monitor Filter 1」というフィルタの 1 階層目の論理式として条件グループ OR が、 2 階層目の論理式

として条件論理式が作られます。「Monitor Filter 1」の左側のアイコンは (ピンク色)です。

図 9-4: モニタフィルタをクリックして、新規条件を選んだところ

9.4.2 条件論理式を編集する

条件論理式に具体的な条件項目と値を設定するには、次のようにします。

1. フィルタビューア領域で編集したい条件論理式を選びます。
   論理式の定義領域で**種類(T)**、**条件(O)**、および**値(V)** が設定できるようになります。
   そのようすを、図 9-5 に示します。

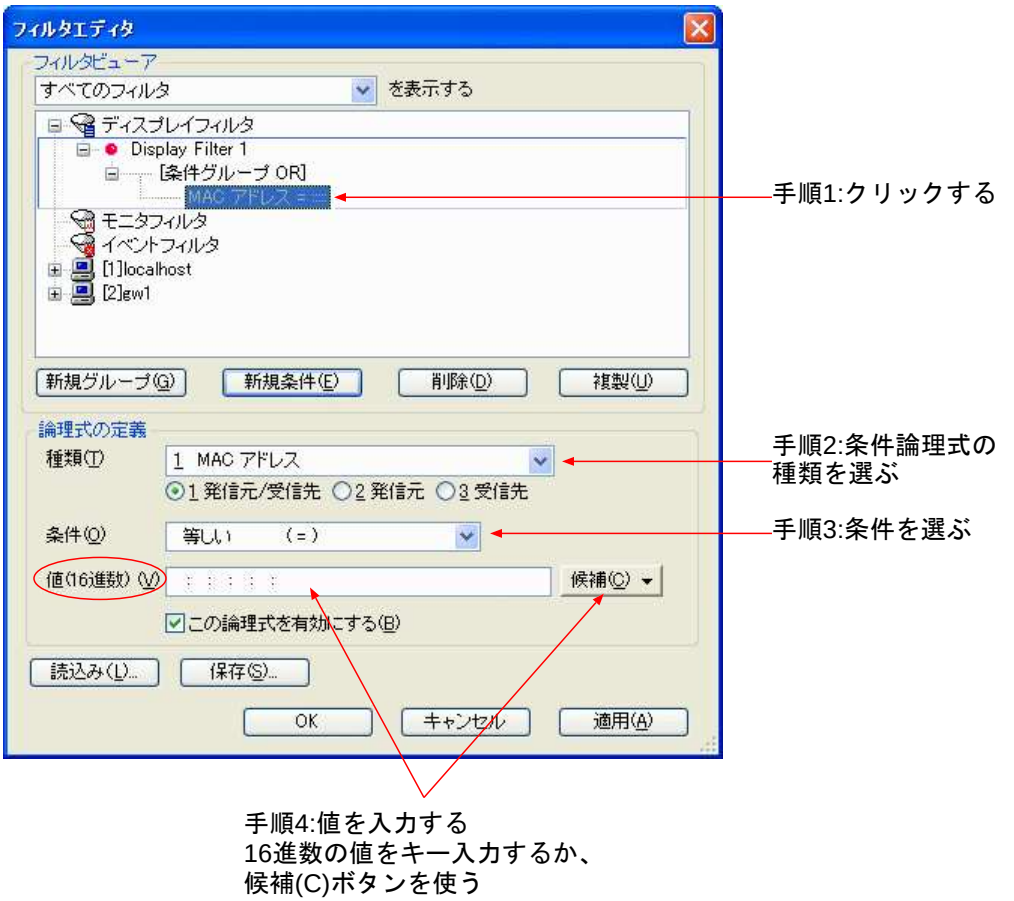


図 9-5: 条件論理式を編集中のフィルタエディタ

2. **種類(T)** のドロップダウンリストボックスから条件論理式の種類を選びます。
   選んだ条件論理式によっては、ラジオボタンが現れます。
3. **条件(O)** のドロップダウンリストボックスから条件を選びます。リストの項目は、手順 2 で選んだ条件論理式の種類によって異なります。
4. 値を設定します。
   設定する値は、手順 2 で選んだ条件論理式の種類によって異なります。 10 進数、 16 進数、または条件論理式に固有の値を設定します。どのような値を入力するのかは、値のラベルで示します。

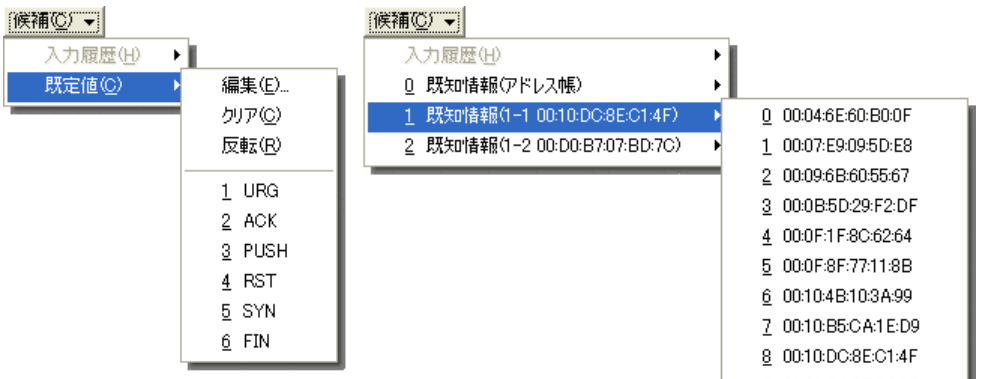
ラベル	入力する値および入力方法
値 (10 進数)(V)	10 進数の値を入力するか、**候補(C)**... ボタンを使う
値 (16 進数)(V)	16 進数の値を入力するか、**候補(C)**... ボタンを使う
値 (候補)(V)	**候補(C)**... ボタンを使う

候補(C)... ボタンについては、次の「候補ボタン」を参照してください。
条件論理式に設定する値については、「9.4.3　条件論理式の種類と設定する値」 (209 ページ) を参照してください。

候補ボタン

候補(C)... ボタンをクリックすると、**入力履歴(H)**、**既知情報**、および**既定値(C)** を項目とするメニューが現れます。それぞれのメニュー項目から、サブメニューが現れます。サブメニューの項目は、条件論理式の種類によって異なります。

例として、「TCP ヘッダーの flags フィールド」と「MAC アドレス」の条件論理式を編集しているときに、**候補(C)**... ボタンをクリックしたときのようすを、図 9-6 に示します。



「TCPヘッダーのFlagsフィールド」の条件論理式を編集中に候補ボタンをクリックしたところ

「MACアドレス」の条件論理式を編集中に候補ボタンをクリックしたところ

図 9-6: **候補(C)**... ボタンから現れるメニュー

- **入力履歴(H)** を選ぶと、以前に入力したことのある値をメニュー項目とするサブメニューが現れます。メニュー項目を選ぶと、選んだ値が**値(V)** に入力されます。

- **既知情報**を選ぶと、モニタ中に見つかった値やキャプチャデータをデコードした結果見つかった値をメニュー項目とするサブメニューが現れます。メニュー項目を選ぶと、選んだ値が**値(V)** に入力されます。
  既知情報の情報源が複数個ある場合は、メニュー項目が複数現れます。
- **既定値(C)** を選ぶと、サブメニューが現れます。サブメニューの項目は、条件論理式によって異なります。メニュー項目を選ぶと、選んだ値が**値(V)** に入力されます。
  次のような特殊なメニュー項目がある場合もあります。
  - **候補リスト(T)**...
    「候補リスト」ダイアログを開きます。メニュー項目が 10 個以上ある場合に現れます。
    「候補リスト」ダイアログで選んだ値が**値(V)** に入力されます。
  - **編集(E)**...、**クリア(C)**、**反転(R)**
    「TCP ヘッダーの Flags フィールド」または「解析パケットのステータス」の条件論理式の場合にあります。この 2 つの条件論理式は、ビットフィールドの値を設定します。
    編集(E)... を選ぶと、「候補リスト (複数選択)」ダイアログが現れます。「候補リスト (複数選択)」ダイアログでは、チェックを付けたビットが 1 になります。
    クリア(C) を選ぶと、全ビットを 0 にします。
    反転(R) を選ぶと、各ビットを反転します。

アドレスをドラッグアンドドロップで入力する

次の条件論理式の値は、ドラッグアンドドロップ操作で入力できます。

- MAC アドレス
  - 「MAC 層発信元毎のトラフィック」ウィンドウのグラフアイテム
  - 「MAC 層受信先毎のトラフィック」ウィンドウグラフアイテム
  - 「MAC 層ホストペア毎のトラフィック」ウィンドウのグラフアイテム
  - MAC アドレス表の行
  - MAC 層アドレス帳の行
  - デコードビューのサマリ領域で MAC アドレスが表示されている行
- IP アドレス、 IP ネットワークアドレス、 IPv6 アドレス、 IPv6 マスクアドレス
  - 「IP 層発信元毎のトラフィック」のウィンドウのグラフアイテム
  - 「IP 層受信先毎のトラフィック」のウィンドウのグラフアイテム
  - 「IP 層ホストペア毎のトラフィック」のウィンドウのグラフアイテム
  - IP アドレス表の行
  - IP 層アドレス帳の行

- デコードビューのサマリ領域で IP アドレスが表示されている行
- ストリームビューのサマリ領域で IP アドレスが表示されている行

「MAC 層ホストペア毎のトラフィック」のウィンドウ、「IP 層ホストペア毎のトラフィック」のウィンドウ、デコードビュー、またはストリームビューから論理式の定義領域の**値(V)** の入力行にドロップした場合は、2 つのアドレスをメニュー項目とするポップアップメニューが現れます。そのようすを図 9-7 に示します。入力したいアドレスを選びます。

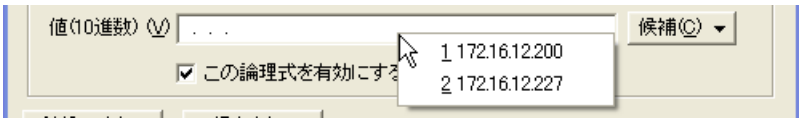


図 9-7: ドラッグアンドドロップでアドレスを入力するときに現れるポップアップメニュー

9.4.3 条件論理式の種類と設定する値

表 9-2: 条件論理式の種類と設定する値

種類	設定する値
1 MAC アドレス	MAC 層アドレスの値を設定します。 **1 発信元／受信先**、**2 発信元**、**3 受信先**のラジオボタンが現れます。 MAC アドレスの 6 つのオクテットを 16 進数で入力します。ドラッグアンドドロップ操作で入力することもできます。詳しくは「アドレスをドラッグアンドドロップで入力する」 (207 ページ) を参照してください。
2 IEEE 802 Encapsulation	次の 4 つの条件を AND で結んだ論理式を設定します。値を入力することはできません。 • Ethernet フレームが LLC (IEEE 802.2) ヘッダー付き • SSAP および DSAP フィールドが 0xAA • Control フィールドが 0x03 • Organization Code が 0
3 Ethernet ヘッダーの Type フィールド	Ethernet(DLC) ヘッダーの Type フィールドの値を設定します。 16 進数の値をキー入力するか、**候補(C)**... ボタンをクリックして、**既定値(C)** のリストから適切なものを選びます。
4 Ethernet アドレスタイプ	Ethernet アドレスのタイプを指定します。 値をキー入力することはできません。**候補(C)**... ボタンをクリックし、**既定値(C)** のサブメニューから**マルチキャスト**、**ブロードキャスト**、または**ユニキャスト**を選びます。
5 Ethernet サイズ	Ethernet フレームの大きさを設定します。 バイト単位の大きさを 10 進数で入力します。 Ethernet の FCS (CRC) フィールドの長さ (4 バイト) を除いた値を指定します。
6 LLC Service Access Point	LLC (IEEE 802.2) の DSAP (受信先) フィールドおよび SSAP (発信元) フィールドの値を設定します。 **1 発信元／受信先**、**2 発信元**、**3 受信先**のラジオボタンが現れます。 DSAP フィールドまたは SSAP フィールドの値を 16 進数で入力します。

次ページへ続く

種類	設定する値
7 IP アドレス	IP 層 (IPv4) アドレスの値を設定します。 **1 発信元／受信先、 2 発信元、 3 受信先**のラジオボタンが現れます。 IP アドレスの 4 つのオクテットを 10 進数で入力します。 ドラッグアンドドロップ操作で入力することもできます。詳しくは「アドレスをドラッグアンドドロップで入力する」 (207 ページ) を参照してください。
8 IP ネットワークアドレス	IP 層 (IPv4) のネットワークアドレスの値を設定します。 **1 発信元／受信先、 2 発信元、 3 受信先**のラジオボタンが現れます。 IP アドレスの 4 つのオクテットとサブネットマスクの有効ビット数を 10 進数で入力します。 ドラッグアンドドロップ操作で入力することもできます。詳しくは「アドレスをドラッグアンドドロップで入力する」 (207 ページ) を参照してください。
9 IP ヘッダーの Protocol フィールド	IP ヘッダー (IPv4) の Protocol フィールドの値を設定します。 **Well known(W)** および **Unknown(K)** のラジオボタンが現れます。ラジオボタンで **Well known(W)** を選んだ場合は、 10 進数の値をキー入力するか、**候補(C)**... ボタンをクリックし、**既定値(C)** のサブメニューから適切なものを選びます。 **Unknown(K)** を選ぶと、値を入力できなくなります。これは、 Protocol フィールドの値として ASTEC Eyes がサポートしていない値を持つパケットをフィルタリングする場合に選びます。
A IPv6 アドレス	IP 層 (IPv6) アドレスの値を設定します。 **1 発信元／受信先、 2 発信元、 3 受信先**のラジオボタンが現れます。 IPv6 アドレスの 8 つの 16 ビット整数を 16 進数で入力します。 ドラッグアンドドロップ操作で入力することもできます。詳しくは「アドレスをドラッグアンドドロップで入力する」 (207 ページ) を参照してください。
B IPv6 マスクアドレス	IP 層 (IPv6) アドレスの上位 *N* ビットまたは下位 *N* ビットを指定します。 **1 発信元／受信先、 2 発信元、 3 受信先**のラジオボタンが現れます。 IPv6 アドレスの 8 つの 16 ビット整数を 16 進数で、マスクの有効ビット数を 10 進数で入力します。 ドラッグアンドドロップ操作で入力することもできます。詳しくは「アドレスをドラッグアンドドロップで入力する」 (207 ページ) を参照してください。

次ページへ続く

種類	設定する値
C IPv6 ヘッダーの Next Header フィールド	IP ヘッダー (IPv6) の Next Header フィールドの値を設定します。 **Well known(W)** および **Unknown(K)** のラジオボタンが現れます。ラジオボタンで **Well known(W)** を選んだ場合は、 10 進数の値をキー入力するか、**候補(C)**... ボタンをクリックし、**既定値(C)** のサブメニューから適切なものを選びます。入力した値は IPv6 ヘッダーにある最後の Next Header フィールドの値と比較されます。 **Unknown(K)** を選ぶと、値を入力できなくなります。これは、 Next Header フィールドの値として ASTEC Eyes がサポートしていない値を持つパケットをフィルタリングする場合に選びます。
D UDP ポート番号 E TCP ポート番号	UDP または TCP のポート番号の値を設定します。 ラジオボタンが現れます。モニタフィルタの場合は、 **Well known(W)** と **Unknown(K)** のラジオボタンが、それ以外の場合は、 **1 発信元／受信先**、 **2 発信元**、 **3 受信先**、および **Unknown(K)** のラジオボタンが現れます。 10 進数の値をキー入力するか、**候補(C)**... ボタンをクリックして**既定値(C)** のサブメニューから適切なものを選びます。サブメニューから**候補リスト(T)**... を選んで「候補リスト」ダイアログを開いた場合、「候補リスト」ダイアログのリストには、 ASTEC Eyes のサポートしているプロトコルの TCP/UDP ポート番号の一覧とデコードヒントで IP アドレスと「任意」と設定して登録したプロトコルのポート番号があります。 ASTEC Eyes がサポートしておらず、かつデコードヒントにも登録していないプロトコルを指定する場合は、 **Unknown(K)** を選びます。
F TCP ステータス	TCP のステータス (CLOSED、 SYN_SENT など) を設定します。 値をキー入力することはできません。**候補(C)**... ボタンをクリックして、**既定値(C)** のサブメニューから適切なものを選びます。
G TCP ヘッダーの Flags フィールド	TCP ヘッダーの Flags フィールドの値を設定します。 ビットフィールドの値を設定しますが、キー入力することはできません。**候補(C)**... ボタンをクリックして、**既定値(C)** を選びます。**既定値(C)** から現れるサブメニューには、 Flags フィールドの各ビット (6 ビット) に対応する項目と、**編集(E)**...、**クリア(C)**、**反転(R)** があります。 各ビットに対応する項目はトグルになっています。 2 つ以上のビットを設定したい場合は、**編集(E)**... を選ぶと良いでしょう。 **クリア(C)** を選ぶと、すべてのビットが 0 になります。 **反転(R)** を選ぶと、各ビットが反転します。

次ページへ続く

種類	設定する値
H 解析パケットのステータス	ASTEC Eyes のエキスパート機能が検出するイベントを設定します。 ビットフィールドの値を設定しますが、キー入力することはできません。**候補(C)**...ボタンをクリックして、**既定値(C)** を選びます。**既定値(C)** から現れるサブメニューには、 ASTEC Eyes のエキスパート機能が検出するイベントに対応する項目と、**編集(E)**...、**クリア(C)**、**反転(R)** があります。 各ビットに対応する項目はトグルになっています。 複数のイベントを選びたい場合は、**編集(E)**... を選ぶと良いでしょう。 **クリア(C)** を選ぶと、すべての選択を解除します。 **反転(R)** を選ぶと、選択されている項目の選択は解除され、これまで選択されていなかった項目が選択されます。
I データ比較	パケット内のデータと比較する値を設定します。 ディスプレイフィルタ以外の場合、**第 1 段階**、**第 2 段階**、**第 3 段階**、および**第 4 段階**のラジオボタンが現れます。 ラジオボタンでプロトコルの段数 *N* を指定します。第 *N* 段階のプロトコルのデータの先頭からのオフセットと比較に使うデータを 16 進数で入力します。オフセットは 2 バイトで指定します。オフセットが 10 であれば、 `000a` と入力します。比較に使うデータは 32 バイトまで指定できます。
J キャプチャ開始タイマー	トリガとなるパケットを検出してから、実際にキャプチャを開始するまでの時間を指定します。キャプチャ開始トリガとして、キャプチャ開始タイマー以外に何も条件を指定していないときは、 1 つ目のパケットを検出してからキャプチャを開始するまでの時間となります。 時、分、秒を 10 進数で入力します。 1 時間 2 分 30 秒後にキャプチャを開始する場合、 `1 h 2 m 30 s` と入力します。
K キャプチャ停止タイマー	トリガとなるパケットを検出してから、実際にキャプチャを停止するまでの時間を指定します。 キャプチャ停止トリガとして、キャプチャ停止タイマー以外に何も条件を指定していないときは、 1 つ目のパケットを検出してからキャプチャを停止するまでの時間となります。 時、分、秒を 10 進数で入力します。 1 時間 2 分 30 秒後にキャプチャを停止する場合、 `1 h 2 m 30 s` と入力します。
L フレーム ID	デコードビューに表示する行をフレーム ID で制限します。
M 時刻	デコードビューに表示する行を時刻で制限します。
N プロトコル	TCP または UDP 上のアプリケーションプロトコルを設定します。キー入力することはできません。**候補(C)**...ボタンをクリックして、**既定値(C)** のサブメニューから適切なものを選びます。

次ページへ続く

種類	設定する値
Qエキスパートイベント数	エキスパートイベントの種類と発生頻度を指定します。 発生頻度については、トータルの発生回数の上限または下限を指定するか、10秒毎の発生回数の上限または下限を指定を指定します。

IP アドレスの条件論理式には、そのパケットが IP プロトコルのパケットであるという条件が同時に適用されます。
たとえば、**「IP アドレス = 192.168.0.1」** という条件を設定すると、パケットが IP プロトコルのパケットであり、かつそのアドレスが 192.168.0.1 であるときに真になります。
「IP アドレス NOT= 192.168.0.1」 という条件を設定すると、パケットが IP プロトコルのパケットでないか、または IP プロトコルのパケットでそのアドレスが 192.168.0.1 でないときに真になります。
IP プロトコルのパケットで、そのアドレスが 192.168.0.1 でないときに真になるような条件を設定するには、次のように入力します。

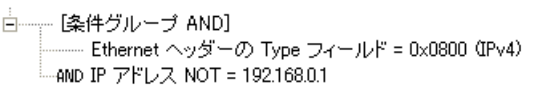


図 9-8: IP パケットでそのアドレスが 192.168.0.1 ではないときに真となる条件

データ比較の条件論理式を指定する場合の注意と制限

データ比較の条件論理式では、プロトコルスタックの段数と指定した段数のデータの先頭からのオフセットと比較データを指定します。

プロトコルスタックを段数として数え、物理層に近い方のプロトコルを第 1 段階とし、第 3 段階までのプロトコルのヘッダーをスキップできます。パケットの先頭から比較したい場合は、第 1 段階を指定します。

たとえば、HTTP プロトコルの GET リクエストだけをキャプチャするようなフィルタを定義できます。そのためには、**「データ比較 = 第 4 段階 offset:0000 data:47 45 54」** という条件を指定します。

ただし、段数とプロトコルの関係において、論理式を編集するときに注意しなければならないこと、および制限があります。

段数とプロトコルの関係について

第 1 段階を選んだ場合は、パケットのデータの先頭からのオフセットと、比較データの値を 16 進数で入力します。

第 2 段階を選んだ場合は、物理層に一番近い方のプロトコルのヘッダーをスキップして、第 1 段階のプロトコルのペイロードの先頭、つまり第 2 段階のプロトコルのヘッダーの先頭からのオフセットと、比較データの値を 16 進数で入力します。

第 3 段階を選んだ場合は、物理層に一番近い方のプロトコルのヘッダーと次のプロトコルのヘッダーをスキップして、第 2 段階のプロトコルのペイロードの先頭、つまり第 3 段階のプロトコルのヘッダーの先頭からのオフセットと、比較データの値を 16 進数で入力します。

第 4 段階を選んだ場合は、物理層に近い方からプロトコル 3 つ分のヘッダーをスキップして、第 3 段階のプロトコルのペイロードの先頭、つまり第 4 段階のプロトコルの先頭からのオフセットと、比較データの値を 16 進数で入力します。

各段のプロトコルの例として、次のようなものが挙げられます。

- 第 1 段階 DLC Ethernet
- 第 2 段階 IPv4, IPv6, LLC, ARP, PPPoE など
- 第 3 段階 TCP, UDP, ICMPv4, ICMPv6 など
- 第 4 段階 TELNET, FTP などのアプリケーション層のプロトコル

プロトコルは段数に固定されているわけではありません。たとえば、多くの場合 IPv4 は第 2 段階になります。しかし、第 2 段階に LLC や PPPoE がある場合、 IPv4 は第 3 段階または第 4 段階になります。

段数とプロトコルの制限について

- **第 3 段階**を選んだ場合、第 2 段階のプロトコルは IPv4 または IPv6 である、という条件が暗黙的に追加されます。
  そのため、第 2 段階のプロトコルが IPv4 または IPv6 でないパケットの場合、論理式は偽になります。
- **第 4 段階**を選んだ場合、第 3 段階のプロトコルは UDP、 TCP、 ICMP、または ICMPv6 である、という条件が暗黙的に追加されます。
  そのため、第 3 段階のプロトコルが UDP、 TCP、 ICMP、または ICMPv6 でないパケットの場合、論理式は偽になります。
- Ethernet(DLC) ヘッダーに VLAN (802.1Q) のタグがあるパケットでは、第 3 段階以降の論理式はすべて偽になります。

例として、 TCP を含むパケットをキャプチャする場合を考えます。第 2 段階が IPv4 である場合は、**「データ比較 = 第 2 段階 offset:0009 data:06」**という条件論理式で TCP を含むパケットをキャプチャできます。 DLC と IPv4 の間に LLC があるパケットについては、**「データ比較 = 第 3 段階 offset:0009 data:06」**という条件論理式でキャプチャできそうですが、バージョン 7.2 では「第 2 段階のプロトコルが IPv4 または IPv6 ではない場合、論理式は偽になる」という制限があるため、キャプチャできません。

9.4.4 条件グループを編集する

条件グループの名前と条件は変えられます。

1. フィルタビューア領域で編集したい条件グループを選びます。
2. 名前を変えます。
   条件グループは、デフォルトでは条件グループ AND (一番上の階層の場合は条件グループ OR) という名前が付けられます。**名前(N)** のテキストボックスに任意の 1 文字以上、 100 文字以下の名前を入力します。
3. ディスプレイフィルタまたはモニタフィルタの場合は、条件を変えられます。
   条件(O) のドロップダウンリストボックスから AND または OR が選べます。

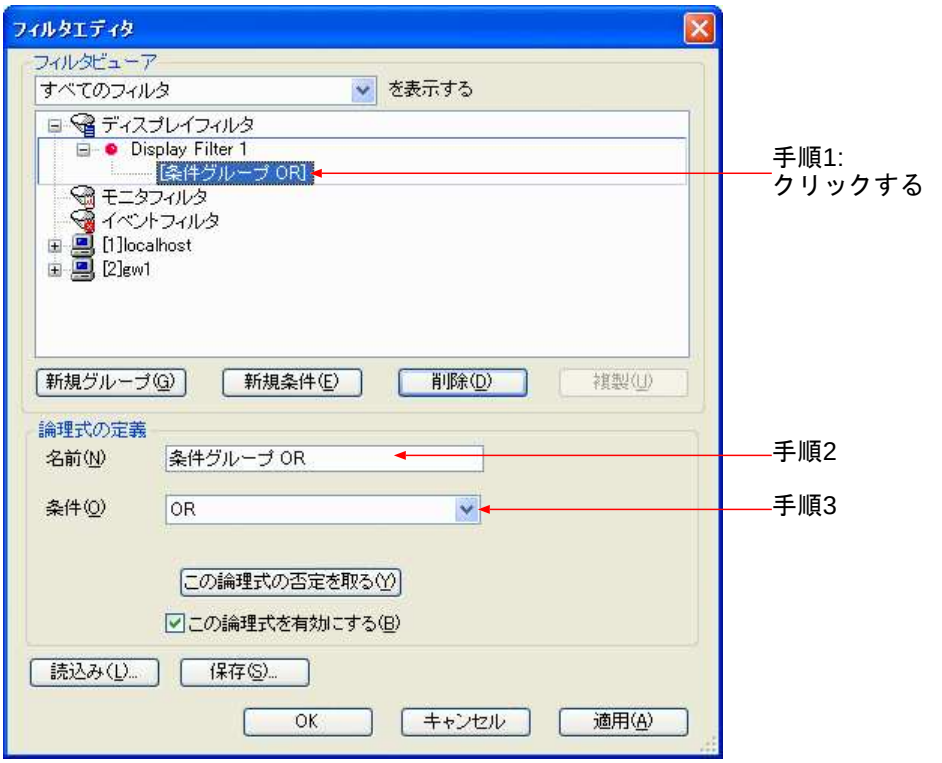


図 9-9: 条件グループを編集する

デフォルトの名前を使っている場合は、選んだ条件によって名前も変わります。条件グループ OR の条件を AND に変えると、その名前は条件グループ AND になります。

9.4.5 ディスプレイフィルタ、モニタフィルタ、イベントフィルタの名前を変える

ディスプレイフィルタ、モニタフィルタ、およびイベントフィルタは、ネットワークインタフェースに関係なく、それぞれ 250 個まで定義できます。デフォルトでは、ディスプレイフィルタには「Display Filter *N*」という名前が、モニタフィルタには「Monitor Filter *N*」という名前が、イベントフィルタには「Event Filter *N*」という名前が付けられます。これをわかりやすい名前に変えられます。

フィルタビューア領域で、変えたいディスプレイフィルタまたはモニタフィルタの名前を選ぶと、論理式の定義領域に**名前(N)** のテキストボックスが表示されます。任意の 1 文字以上の名前を入力します。

9.4.6 論理式を追加する

論理式を追加するには、 2 つの方法があります。

- フィルタビューア領域で論理式を選び、**新規グループ(G)** ボタンまたは**新規条件(E)** ボタンをクリックします。
- フィルタビューア領域で論理式を右クリックしてポップアップメニューを開き、**新規グループ(G)** または**新規条件(E)** を選びます。

新規グループ(G) を選んだ場合は条件グループが、**新規条件(E)** を選んだ場合は条件論理式が追加されます。

その結果は、次のようになります。

- 条件グループ OR を選んで追加したとき
  選んだ条件グループ OR の下の階層に、条件グループ AND または条件論理式が追加されます。選んだ条件グループ OR の下の階層にすでに論理式がある場合は、その論理式と OR で結合します。
- 条件グループ AND を選んで追加したとき
  選んだ条件グループ AND の下の階層に、条件グループ AND または条件論理式が追加されます。選んだ条件グループ AND の下の階層にすでに論理式がある場合は、その論理式と AND で結合します。
- 条件論理式を選んで追加したとき
  選んだ条件論理式の 1 つ上の階層の条件グループを選んだ場合と同じ結果になります。

9.4.7 論理式を複製する

論理式を複製する方法は 3 通りあります。

- フィルタビューア領域で複製したい論理式を選んで、**複製(U)** ボタンをクリックします。
- フィルタビューア領域内の複製したい論理式を右クリックし、現れたポップアップメニューから**複製(U)** を選びます。
- コピーアンドペーストを使う。この方法については、「コピーアンドペーストを使う」 (218 ページ) を参照してください。

選んだ論理式が複製され、同じ階層に置かれます。

選んだ論理式の 1 つ上の階層が条件グループ OR の場合、複製された論理式は選んだ論理式と OR で結合します。

選んだ論理式の 1 つ上の階層が条件グループ AND の場合、複製された論理式は選んだ論理式と AND で結合します。

選んだ論理式が条件グループを含んでいる場合は、その条件グループ以下の階層すべてが複製されます。

条件論理式をひとつも持たない条件グループだけの論理式は複製できません。

フィルタ全体を選んで複製したときは、一番上の階層の条件グループを選んで複製した場合と同じ結果になります。

コピーアンドペーストを使う

コピーアンドペーストの機能を使って論理式を複製することもできます。

- キー操作でコピーアンドペーストの機能を使う
  1. フィルタビューア領域にフォーカスを移し、上下のカーソルキー (**<↑>**、 **<↓>**) を使ってコピーしたい論理式を選びます。
  2. **<Ctrl-C>** キーを押します。
  3. 上下のカーソルキー (**<↑>**、 **<↓>**) を使って貼り付け先を選びます。
     貼り付けたい階層の条件論理式、または貼り付けたい階層の 1 つ上の条件グループを選びます。
  4. **<Ctrl-V>** キーを押します。
- マウス操作でコピーアンドペーストの機能を使う
  1. フィルタビューア領域内のコピーしたい論理式を右クリックします。
     ポップアップメニューが現れます。
  2. ポップアップメニューから**コピー(C)** を選びます。
  3. 選んだ論理式を貼り付けたい階層の条件論理式、または貼り付けたい階層の 1 つ上の条件グループを右クリックします。
     ポップアップメニューが現れます。
  4. **貼り付け(P)** を選びます。

その結果は、次のようになります。

- 貼り付け先として条件グループ AND を選んだとき

複製された論理式はその 1 つ下の階層に置かれます。その 1 つ下の階層にすでに論理式がある場合は、 AND で結合します。

- 貼り付け先として条件グループ OR を選んだとき
  複製された論理式はその 1 つ下の階層に置かれます。その 1 つ下の階層にすでに論理式がある場合は、 OR で結合します。
- 貼り付け先として条件論理式を選んだとき
  複製された論理式は、貼り付け先の条件論理式と同じ階層に置かれます。選んだ条件論理式の 1 つ上の階層が条件グループ AND である場合は、選んだ条件論理式と AND で結合します。選んだ条件論理式の 1 つ上の階層が条件グループ OR である場合は、選んだ条件論理式と OR で結合します。
- 貼り付け先としてフィルタを選んだとき
  一番上の階層の条件グループを選んで貼り付けた場合と同じ結果になります。

9.4.8 論理式を削除する

論理式を削除するには、次の 3 つの方法があります。

- フィルタビューア領域で削除したい論理式を選んで、**削除(D)** ボタンをクリックします。
- フィルタビューア領域内の削除したい論理式を右クリックし、現れたポップアップメニューから**削除(D)** を選びます。
- 上下のカーソルキー (**<↑>**、 **<↓>**) を押してフィルタビューア領域で 削除したい論理式を選び、 **<Delete>** キーを押します。

選んだ論理式が条件グループを含んでいる場合は、その条件グループ以下の階層すべてが削除されます。また、フィルタを選んで削除したときは、フィルタに定義されているすべての論理式が削除されます。

9.4.9 ドラッグアンドドロップ操作で論理式を移動、コピーする

ドラッグアンドドロップ操作で論理式を移動するには、次のようにします。

1. フィルタビューア領域で移動したい論理式にマウスカーソルを合わせ、左ボタンを押し下げます。
2. 左ボタンを押したまま、選んだ論理式をドロップしたい階層の条件論理式、またはドロップしたい階層の 1 つ上の条件グループまで移動します。
3. 左ボタンを離します。

その結果は、次のようになります。

- 条件論理式にマウスカーソルを合わせて左ボタンを離したとき
  その条件論理式と同じ階層に移動します。
  その条件論理式の 1 つ上の階層が条件グループ AND である場合、既存の論理式と AND で結合します。その条件論理式の 1 つ上の階層が条件グループ OR である場合、既存の論理式と OR で結合します。
- 条件グループ AND にマウスカーソルを合わせて左ボタンを離したとき
  その 1 つ下の階層に移動します。その条件グループ AND の下に論理式がある場合は、AND で結合します。
- 条件グループ OR にマウスカーソルを合わせて左ボタンを離したとき
  その 1 つ下の階層に移動します。その条件グループ OR の下に論理式がある場合は、 OR で結合します。
- フィルタにマウスカーソルを合わせて左ボタンを離したとき
  一番上の階層の条件グループに合わせたときと同じ結果になります。

<Ctrl> キーを押しながらドラッグアンドドロップ操作を行うと、論理式は移動ではなく、コピーされます。

9.4.10 論理式を一時的に無効にする

フィルタを定義して実際に使っているときに、フィルタを外したくなることがあります。フィルタを外すために、論理式を削除する必要はありません。論理式を一時的に無効にする機能が用意されています。フィルタを外したいときは、論理式全体を無効にします。また、フィルタの条件を変えるために、部分的に無効にすることもできます。

論理式を無効にするには、 2 つの方法があります。

- フィルタビューア領域で論理式を選び、論理式の定義領域の下の方にある**この論理式を有効にする(B)** のチェックを外します。
- フィルタビューア領域内の論理式を右クリックし、現れたポップアップメニューから**無効にする(B)** を選びます。

クリックした論理式とその下の階層のすべての論理式に、 が表示されます。

9.4.11 論理式の否定を取る

フィルタを適用した後、絞り込まれたパケットまたはトラフィックの補集合を見たいことがあります。ディスプレイフィルタおよびモニタフィルタの場合は、定義している論理式の否定 (NOT) を取ることができます。

論理式の否定を取るには、 2 つの方法があります。

- フィルタビューア領域で、条件グループを選び、論理式の定義領域にある**この論理式の否定を取る(Y)** ボタンをクリックします。
- フィルタビューア領域内の条件グループを右クリックし、現れたポップアップメニューから**否定を取る(Y)** を選びます。

9.4.12 元に戻す、やり直し機能を使う

誤って論理式を削除するなど、意図しない編集を行ってしまったときに、編集前の状態へ戻すことができます。一旦、編集前の論理式に戻した後、編集後の論理式になるように編集のやり直しをすることもできます。

元に戻す機能を使うには次のようにします。

- **<Ctrl-Z>** を押します。

または

- フィルタビューア領域を右クリックし、現れたポップアップメニューから**元に戻す(N)** を選びます。

やり直し機能を使うには次のようにします。

- **<Ctrl-Y>** を押します。

または

- フィルタビューア領域を右クリックし、現れたポップアップメニューから**やり直し(O)** を選びます。

元に戻せるのは、過去 5 回分の操作までです。

9.5 論理式を適用する

編集が終わったら、**OK** ボタンまたは**適用(A)** ボタンをクリックします。変更されたすべてのフィルタが一度に適用されます。

不正な論理式がある場合は、「ASTEC Eyes」ダイアログが現れ、不正な論理式があることを知らせます。不正な論理式は (赤色) で、サポートしていない論理式は (赤色) で表示されています。不正な論理式を修正または削除してから、再度 **OK** ボタンまたは**適用(A)** ボタンをクリックします。

また、条件論理式を持たない条件グループだけの論理式は削除されます。

フィルタが適用されると、フィルタのアイコンが (ピンク色) から (緑色) に変わります。

OK ボタンをクリックしたときは、フィルタエディタが閉じます。

条件論理式の編集を途中で止めたため、条件論理式の値が設定されていない場合などは、不正な論理式になります。

9.6 論理式を自動的に生成する

ASTEC Eyes には、よく使われる条件の論理式をマウス操作だけで作る機能があります。

次の 3 つの方法があります。

- ドラッグアンドドロップを使う方法
- トラフィックウィンドウのポップアップメニューを使う方法
- デコードビューのポップアップメニューを使う方法

ドラッグアンドドロップ操作で論理式を生成する

1. 次の項目のいずれかにマウスカーソルを合わせ、マウスの左ボタンを押し下げます。
   - トラフィックウィンドウのグラフアイテムまたは凡例の項目
   - トラフィックウィンドウの背景 (内訳を表示している場合のみ)
   - IP アドレス表および MAC アドレス表の行
   - IP 層アドレス帳および MAC 層アドレス帳の行
   - デコードビューおよびストリームビューのサマリ領域の行
2. マウスの左ボタンを押したままフィルタエディタのフィルタビューア領域までドラッグし、論理式を追加したい階層、または追加したい階層の 1 つ上の条件グループにマウスカーソルを合わせます。
3. マウスの左ボタンを放します。
   単一の論理式しか候補がない場合は、論理式が生成されます。生成される論理式は、ドラッグした項目によって異なります。
   複数の論理式が考えられる場合は、ポップアップメニューが現れます。ポップアップメニューから項目を選ぶと、論理式が生成されます。ポップアップメニューのメニュー項目は、ドラッグした項目によって異なります。

生成される論理式については、「9.6.1　トラフィックウィンドウから自動生成できる論理式」(225 ページ) 、「9.6.2　MAC アドレス表、 IP アドレス表、 MAC 層アドレス帳、 IP 層アドレス帳から自動生成できる論理式」 (228 ページ) 、および「9.6.3　デコードビューまたはストリームビューから自動生成できる論理式」 (229 ページ) を参照してください。

トラフィックウィンドウのポップアップメニューを使って論理式を生成する

トラフィックウィンドウのポップアップメニューを使って生成できるのは、モニタフィルタの論理式です。

1. トラフィックウィンドウのグラフアイテムまたは凡例の項目を右クリックしてポップアップメニューを開き、**フィルタの生成(I)** をポイントします。
2. **一時的に生成して適用する(I)** または**フィルタエディタに送る(F)** を選びます。
   一時的に生成して適用する(I) を選んだ場合、モニタフィルタの条件となる論理式が生成され、選択中のインタフェースに適用されます。フィルタエディタは現れません。また、生成された論理式を保存したり、変更することもできません。トラフィックウィンドウのタイトルおよびインタフェースセレクタウィンドウのインタフェースのラベルの横に、「一時モニタフィルタ」と表示されます。
   フィルタエディタに送る(F) を選んだ場合、論理式が生成され、生成された論理式が追加された状態のフィルタエディタが現れます。

生成される論理式については、「9.6.1　トラフィックウィンドウから自動生成できる論理式」(225 ページ) の表 9-3を参照してください。

デコードビューのポップアップメニューを使って論理式を生成する

デコードビューのポップアップメニューを使って生成できるのは、ディスプレイフィルタの論理式です。

1. デコードビューのサマリ領域の行を右クリックしてポップアップメニューを開き、**フィルタ(F)** をポイントします。
2. **フィルタの生成(I)** をポイントします。
3. **一時的に生成して適用する(I)** または**フィルタエディタに送る(F)** をポイントします。
   どちらをポイントした場合でも、サブメニューが現れます。サブメニューには、次に示すメニュー項目があります (クリックしたサマリ領域の行によっては選べないものもあります)。
   - **コネクションを指定(C)**
   - **ホストペアとプロトコルを指定(C)**
   - **ホストペアを指定(H)**
   - **ポート番号を指定(P)**
   - **フレーム ID を指定(F)**
   - **日付を指定(D)**

4. サブメニューから項目を選びます。
   手順 3 で**一時的に生成して適用する(I)** をポイントしたか、**フィルタエディタに送る(F)** をポイントしたかによって、 ASTEC Eyes の動作が異なります。

   一時的に生成して適用する(I) をポイントした場合

   ディスプレイフィルタの条件となる論理式が生成されますが、フィルタエディタは現れません。ディスプレイフィルタを適用した状態のデコードビューが現れます。生成された論理式を保存したり、変更することはできません。手作業で条件を設定してフィルタを適用した場合と同じように、フレーム ID のカラムの数字が緑色で表示されます。

   フィルタエディタに送る(F) をポイントした場合

   論理式が生成され、生成された論理式が追加された状態のフィルタエディタが現れます。ここからは手作業で論理式を編集する場合とまったく同じです。

   クリックした行および手順 4 で選んだメニュー項目によって、生成される論理式が異なります。
   生成される論理式の例については、「9.6.3　デコードビューまたは ストリームビューから自動生成できる論理式」 (229 ページ) の表 9-7 を参照してください。

9.6.1　トラフィックウィンドウから自動生成できる論理式

トラフィックウィンドウから自動的に生成できる論理式は、選んだグラフアイテムや凡例の項目によって異なります。

また、「MAC 層トラフィック」のウィンドウ、「IP 層トラフィック」のウィンドウ、および「MAC 層エラーフレーム数」のウィンドウのグラフアイテムを元に生成できる有効な条件論理式はありません。

表 9-3 にトラフィックウィンドウのグラフアイテムを元に自動的に生成できる論理式の例を、グラフアイテムごとに示します。

表 9-3: トラフィックウィンドウのグラフアイテムを元に生成される論理式

グラフアイテム	生成される論理式の例
「MAC 層発信元毎のトラフィック」の グラフアイテム	発信元 MAC アドレス = 20:53:52:43:00:00
「MAC 層受信先毎のトラフィック」の グラフアイテム	受信先 MAC アドレス = 44:45:53:54:00:00
「MAC 層ホストペア毎のトラフィック」の グラフアイテム	[条件グループ AND] MAC アドレス = 20:53:52:43:00:00 AND MAC アドレス = 44:45:53:54:00:00
「MAC 層プロトコル毎のトラフィック」の グラフアイテム	Ethernet ヘッダーの type フィールド = 0x0800 (IP version 4)
「IP 層発信元毎のトラフィック」の グラフアイテム	発信元 IP アドレス = 192.168.0.1 または 発信元 IPv6 アドレス = fe80:0:0:0:210:4bff:fe10:3a99
「IP 層受信先毎のトラフィック」の グラフアイテム	受信先 IP アドレス = 192.168.0.1 または 受信先 IPv6 アドレス = ff02:0:0:0:0:0:0:1
「IP 層ホストペア毎のトラフィック」の グラフアイテム	[条件グループ AND] IP アドレス = 192.168.0.1 AND IP アドレス = 192.168.0.2 または [条件グループ AND] IPv6 アドレス = fe80:0:0:0:210:4bff:fe10:3a99 AND IPv6 アドレス = ff02:0:0:0:0:0:0:1
「IP 層プロトコル毎のトラフィック」のグラフアイテム TCP 上のプロトコルの場合: UDP 上のプロトコルの場合: 上記以外のプロトコルの場合:	TCP ポート番号 = 23 (TELNET) UDP ポート番号 = 69 (TFTP) [条件グループ OR] IP ヘッダーの Protocol フィールド = 1 (ICMP) OR IPv6 ヘッダーの Next Header フィールド = 1 (ICMP)
「MAC 層アドレスタイプ毎のトラフィック」の グラフアイテム	Ethernet アドレスタイプ = マルチキャスト
「MAC 層サイズ毎のフレーム数」の グラフアイテム	[条件グループ AND] Ethernet サイズ >= 1024 AND Ethernet サイズ <= 1517

内訳を表示しているトラフィックウィンドウから自動生成できる論理式

内訳を表示しているトラフィックウィンドウのグラフアイテムを元に生成される論理式は、選んだグラフアイテムを特定するための複数の論理式を AND で結合したものになります。

また、内訳を表示しているトラフィックウィンドウからは、グラフアイテムだけでなく背景もドラッグして、論理式を自動的に生成できます。ただし、背景を右クリックしてもポップアップメニューは現れません。背景を元に生成される論理式は、内訳の元のグラフアイテムを特定する論理式になります。

たとえば、「IP 層プロトコル毎のトラフィック」のウィンドウに表示されている TELNET のグラフアイテムを選び、ホストペア毎の内訳を表示した状態のトラフィックウィンドウを考えます。グラフアイテムと背景をそれぞれ選んで論理式を生成した場合、次のようになります。

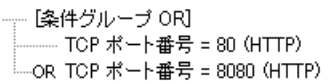
表 9-4: 内訳を表示しているトラフィックウィンドウから生成される論理式

選ぶ項目	生成される論理式
グラフアイテム "192.168.0.1 -192.168.0.2"	[条件グループ AND] IP アドレス = 192.168.0.1 AND IP アドレス = 192.168.0.2 AND TCP ポート番号 = 23 (TELNET)
背景	TCP ポート番号 = 23 (TELNET)

複数のポート番号が割り当てられているプロトコルのグラフアイテムから自動生成できる論理式

プロキシサーバーを使っている場合など、1 つのプロトコルに複数の TCP または UDP ポート番号が割り当てられていることがあります。そのようなプロトコルのグラフアイテムを元に生成される論理式は、それぞれポート番号を特定する論理式を OR で結合したものになります。

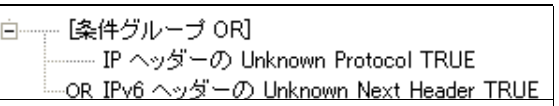
たとえば、 TCP ポート番号 8080 が HTTP であるというデコードヒントを設定しているときに、 HTTP のグラフアイテムをドラッグまたはクリックした場合、次のような論理式が生成されます。



Unknown と分類されているグラフアイテムから自動生成できる論理式

「MAC 層プロトコル毎のトラフィック」のウィンドウまたは「IP 層プロトコル毎のトラフィック」のウィンドウに表示されている「Unknown Protocol」、「Unknown TCP Protocol」、「Unknown UDP Protocol」のグラフアイテムを元に生成される論理式を表 9-5 に示します。

表 9-5: Unknown を元に生成される論理式

グラフアイテム	生成される論理式の例
Unknown Protocol	
Unknown TCP Protocol	TCP Unknown ポート番号 TRUE
Unknown UDP Protocol	UDP Unknown ポート番号 TRUE

9.6.2 MAC アドレス表、IP アドレス表、MAC 層アドレス帳、IP 層アドレス帳から自動生成できる論理式

MAC 層アドレス帳、 IP 層アドレス帳、 MAC アドレス表、および IP アドレス表の行を元に論理式を自動生成する場合は、ドラッグアンドドロップによる方法しか使えません。

表 9-6: MAC 層アドレス帳、 IP 層アドレス帳、 MAC アドレス表、 IP アドレス表から自動生成される論理式

グラフアイテム	生成される論理式の例
「MAC アドレス表」の行	MAC アドレス = 50:41:49:52:00:00
「IP アドレス表」の行	IP アドレス = 192.168.0.1 または IPv6 アドレス = ff02::9
「MAC アドレス - IP アドレス対応表」の行 1 *MAC* アドレスを選んだ場合: 2 *IP* アドレスを選んだ場合:	「1 *MAC* アドレス」、「2 *IP* アドレス」という 2 つのメニュー項目を持つポップアップメニューが現れます。 MAC アドレス = 50:41:49:52:00:00 IP アドレス = 192.168.0.1 または IPv6 アドレス = ff02::9
MAC 層アドレス帳の行	MAC アドレス = 50:41:49:52:00:00
IP 層アドレス帳	IP アドレス = 192.168.0.1 または IPv6 アドレス = ff02::9

9.6.3 デコードビューまたは ストリームビューから自動生成できる論理式

ドラッグアンドドロップによる方法を使う場合は、デコードビューおよびストリームビューのサマリ領域の行をドラッグできます。しかし、ストリームビューのサマリ領域の行を右クリックしてポップアップメニューを開いても、**フィルタの生成(I)** というメニュー項目はありません。ポップアップメニューによる方法が使えるのは、デコードビューからポップアップメニューを開いた場合だけです。

表 9-7: パケットまたはレコードの情報を元に生成される論理式

メニュー項目	条件または選んだパケットの構成		生成される論理式の例
コネクションを指定(C)	IPv4 または IPv6 が含まれ、かつ TCP または UDP が含まれる場合のみ選べる		[条件グループ OR] [条件グループ AND] 発信元 IP アドレス = 172.16.12.228 AND TCP 発信元ポート番号 = 6000 (X) AND 受信先 IP アドレス = 172.20.10.50 AND TCP 受信先ポート番号 = 45166 OR [条件グループ AND] 発信元 IP アドレス = 172.20.10.50 AND TCP 発信元ポート番号 = 45166 AND 受信先 IP アドレス = 172.16.12.228 AND TCP 受信先ポート番号 = 6000 (X)
ホストペアとプロトコルを指定(C)	IPv4 または IPv6 が含まれている		[条件グループ AND] IP アドレス = 204.152.184.98 AND IP アドレス = 202.239.16.2 AND IP ヘッダーの Protocol フィールド = 1 (ICMP)
	IPv4 も IPv6 も含まれていない	LLC が含まれている	[条件グループ AND] MAC アドレス = 20:53:52:43:00:00 AND MAC アドレス = 44:45:53:54:00:00 AND LLC 発信元 Service Access Point = 0x42 AND LLC 受信先 Service Access Point = 0x42
		LLC は含まれていない	[条件グループ AND] MAC アドレス = 08:00:20:C0:F6:2F AND MAC アドレス = FF:FF:FF:FF:FF:FF AND Ethernet ヘッダーの Type フィールド = 806 (ARP)
ホストペアを指定(H)	IPv4 または IPv6 が含まれている		[条件グループ AND] IP アドレス = 172.16.12.228 AND IP アドレス = 172.20.10.50
	IPv4 も IPv6 も含まれていない		[条件グループ AND] MAC アドレス = 00:00:0C:38:9A:26 AND MAC アドレス = 08:00:20:04:BD:18

次ページへ続く

<table>
<tr><th>メニュー項目</th><th colspan="2">条件または選んだパケットの構成</th><th>生成される論理式の例</th></tr>
<tr><td rowspan="3">ポート番号を指定(P)</td><td rowspan="2">IPv4 または IPv6 が含まれている</td><td>TCP または UDP が含まれている</td><td>[条件グループ OR]
TCP ポート番号 = 6000 (X)
OR TCP ポート番号 = 45166</td></tr>
<tr><td>TCP も UDP も含まれていない</td><td>IP ヘッダーの Protocol フィールド = 1 (ICMP)</td></tr>
<tr><td>IPv4 も IPv6 も含まれていない</td><td>LLC が含まれている</td><td>[条件グループ AND]
MAC アドレス = 20:53:52:43:00:00
AND MAC アドレス = 44:45:53:54:00:00
AND LLC 発信元 Service Access Point = 0x42
AND LLC 受信先 Service Access Point = 0x42</td></tr>
<tr><td>LLC は含まれていない</td><td>Ethernet ヘッダーの Type フィールド = 806 (ARP)</td></tr>
<tr><td>フレーム ID を指定(F)</td><td colspan="2" rowspan="2">これらのメニュー項目はドロップ先がディスプレイフィルタの場合のみ選べる</td><td>フレームID = 4</td></tr>
<tr><td>日付を指定(D)</td><td>時刻 = 2002/2/28 20:19:43.836</td></tr>
</table>

9.7 フィルタの保存と読み込み

よく使うフィルタが決まっているような場合は、フィルタをファイルに保存しておくと便利です。

9.7.1 フィルタの保存

フィルタをファイルに保存するには、**保存(S)**. . . ボタンをクリックします。図 9-10 のような「名前を付けて保存」ダイアログが現れます。

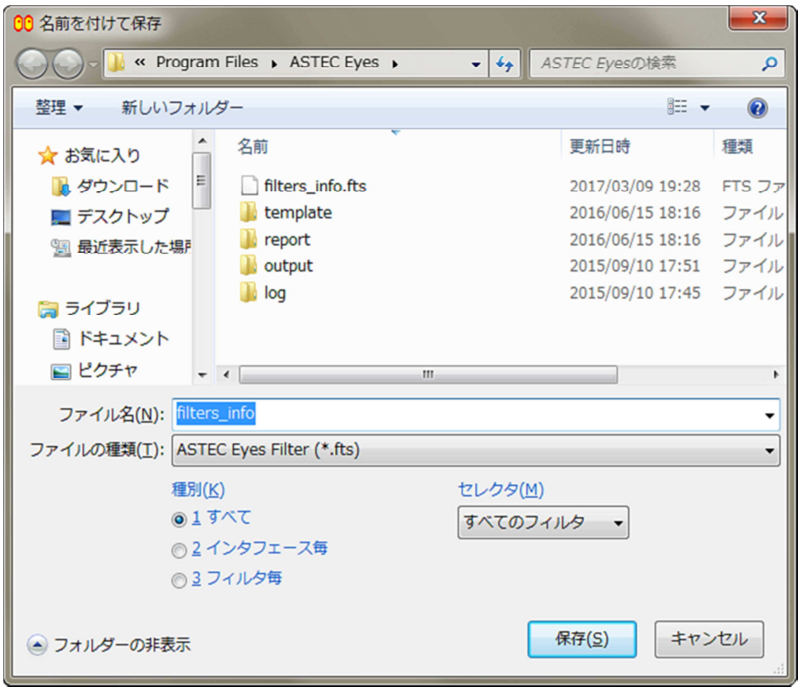


図 9-10: フィルタを保存するための「名前を付けて保存」ダイアログ

保存するフィルタの範囲を**種別(K)** ラジオボタンと**セレクタ(M)** のドロップダウンリストボックスで指定します。

種別を **1 すべて**にすると、フィルタエディタに表示されているすべてのフィルタを 1 つのファイルに保存します。

種別を **2 インタフェース毎**にした場合は、**セレクタ(M)** のドロップダウンリストボックスからネットワークインタフェースを選びます。フィルタエディタで編集したフィルタのうち、選んだネットワークインタフェースのフィルタを 1 つのファイルの保存します。ディスプレイフィルタは保存されません。

種別を **3 フィルタ毎**にした場合、**セレクタ(M)** のドロップダウンリストボックスには変更したフィルタが現れます。選んだフィルタだけが保存されます。

フィルタを保存するファイルの拡張子は`.fts` です。

次のフィルタは、 ASTEC Eyes の実行形式 (`EYES.exe`) があるディレクトリに、`default-filters.fts` というファイル名で保存しておけば、 次に ASTEC Eyes を起動したときに自動的に読み込みます。

- モニタフィルタ
- ディスプレイフィルタ
- イベントフィルタ
- ローカルホストのキャプチャフィルタ
- ローカルホストのキャプチャ開始トリガ
- ローカルホストのキャプチャ停止トリガ

上のフィルタのうち、ローカルホストのキャプチャフィルタ、キャプチャ開始トリガ、およびキャプチャ停止トリガは自動的に適用されます。
自動読込みファイル名ボタン () をクリックすると、**ファイル名(N)** の入力行に`default-filters.fts` が入力されます。

連続キャプチャフィルタ、連続キャプチャ開始トリガ、および連続キャプチャ停止トリガは、それぞれ個別のファイルに保存しておき、設定権限を取得した上で、個別に読み込む方が良いでしょう。

9.7.2 フィルタの読み込み

フィルタをファイルから読み込むには、**読み込み(L)**... ボタンをクリックします。「開く」ダイアログが現れるので、ファイル名を指定します。このとき、複数のファイルを指定して同時に読み込むことができます。

ファイルに含まれているディスプレイフィルタおよびモニタフィルタは、既にあるディスプレイフィルタまたはモニタフィルタのそれぞれのリストに追加されます。それ以外のフィルタは、フィルタエディタで該当するフィルタが編集されていなければ、そのまま読み込まれます。編集されている場合は、ファイルの内容で置き換えるかどうかをたずねるダイアログが現れます。

フィルタのファイルを読み込んだとき、 ASTEC Eyes のフィルタの論理式としてとして不適切なものがあった場合、不適切なものがあったフィルタには何も読み込みません。
たとえば、キャプチャフィルタとモニタフィルタが 3 つ定義されているファイルを読み込もうとしたとき、モニタフィルタのうちの 1 つに不適切なものがあった場合、キャプチャフィルタの定義は読み込まれますが、モニタフィルタの定義は 1 つも読み込まれません。
フィルタのファイルをテキストエディタなどを用いて編集すると、誤って不適切なものを入力してしまう可能性があります。フィルタの編集はフィルタエディタで行ってください。

10章

エキスパート機能

ASTEC Eyes には 2 つのエキスパート機能があります。**モニタエキスパート機能**と**デコードエキスパート機能**です。

モニタエキスパート機能は、ネットワークのモニタ中にトラブルの予兆を発見し、表示する機能です。

トラブルの予兆となるようなイベントを監視し、見つかったイベントをイベントビューアに表示します。モニタエキスパート機能が検出するイベントを**モニタイベント**と呼びます。モニタイベントとは、 ASTEC Eyes が検出するネットワークの状態の変化、および ASTEC Eyes のキャプチャモジュールの状態の変化のことです。

また、見つけたモニタイベントをメールや SNMP トラップで知らせることもできます。

デコードエキスパート機能は、キャプチャデータの解析中にトラブルの種になりうるイベントを発見し、表示する機能です。ネットワーク機器の設定が適切でない可能性や、トラブルの種になる可能性のあるパケットが流れたことを表示します。

10.1 イベントを見る

モニタイベントもデコードイベントもイベントビューアに表示されます。ここでは、イベントビューアを開く方法について説明します。

10.1.1 モニタイベントを見る

モニタを開始すると自動的にモニタイベントの検出が始まります。

検出されたモニタイベントは、インタフェースごとにイベントビューアに表示されます。

モニタを開始する方法については、「2.1.1 モニタを開始する」 (13 ページ) を参照してください。

- **イベントビューアを開く方法 1**
  1. インタフェースを選びます。
  2. メインウィンドウの**モニタ(M)** メニューから**イベントビューア(V)** を選びます。
- **イベントビューアを開く方法 2**
  インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**モニタウィンドウ(M)** をポイントし、**イベントビューア(V)** を選びます。

図 10-1 のようなイベントビューアが現れます。

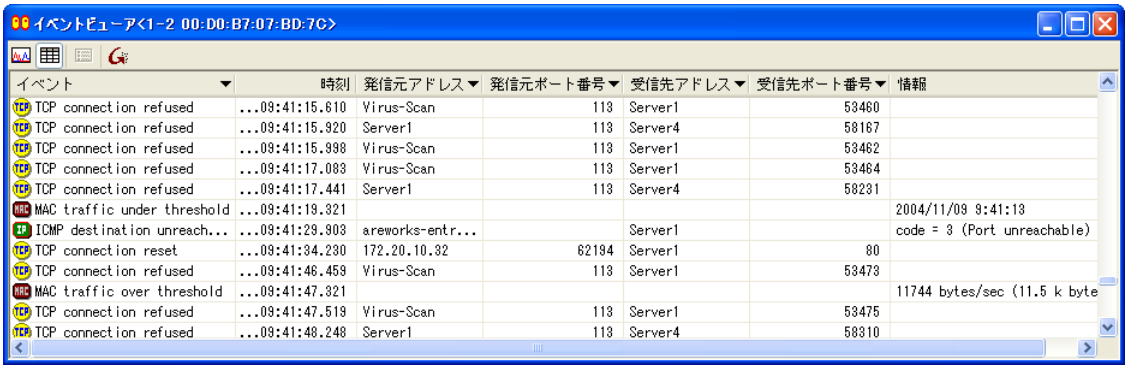


図 10-1: イベントビューア

検出するモニタイベントを選択できます。モニタイベントを選んだり、各モニタイベントの設定を行う方法については、「10.3.1　モニタイベントの設定」 (244 ページ) を参照してください。

10.1.2　デコードイベントを見る

デコードイベントはデコード時に検出します。検出するデコードイベントの詳細な設定や検出の抑制については、「10.3.2　デコードイベントの設定」 (247 ページ) を参照してください。

- **イベントビューアを開く方法 1**
  1. デコードイベントを見たいデコードビューをクリックします。
  2. デコードビューのツールバーの**イベントビューア**ボタン( ) をクリックします。
- **イベントビューアを開く方法 2**
  デコードビューを右クリックしてポップアップメニューを開き、**イベントビューア(E)** を選びます。

図 10-2 のようなイベントビューアが現れます。

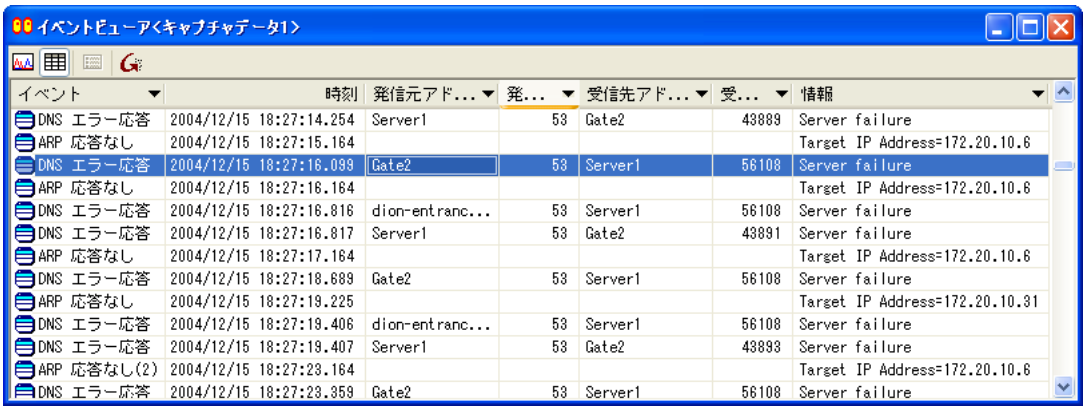


図 10-2: イベントビューア

10.1.3 イベントビューアに表示する情報

イベントビューアに表示する情報を表 10-1に示します。

表 10-1: イベントビューアのカラム

カラム名	表示する内容
イベント	イベントの種類
	MAC 層で計測したパケットの総量に関連したモニタイベントを表します。
	IPv4 プロトコルに関連したモニタイベントを表します。
	IPv6 プロトコルに関連したモニタイベントを表します。
	UDP プロトコルに関連したモニタイベントを表します。
	TCP プロトコルに関連したモニタイベントを表します。
	連続キャプチャの開始と停止、およびユーザー定義のモニタイベントを表します。
	NIC ドライバの開始と停止、およびリンクの状態のモニタイベントを示します。
	イベントを表すものではありません。一番下の行を表します。この行を選んでおけば、画面上に常に最新のモニタイベントが表示されるように、画面が自動的にスクロールします。
	ASTEC Eyes *for* VoIP が見つけた RTP 損失のイベントを表します。
	デコードエキスパート機能で見つけたデコードイベントを表します。
時刻	モニタイベントを検出した時刻またはデコードイベントの対象のパケットをキャプチャした時刻
発信元アドレス 受信先アドレス	UDP または TCP プロトコルに関連したイベントの場合、ホストの IP アドレスを表示します。
発信元ポート番号 受信先ポート番号	UDP または TCP プロトコルに関連したモニタイベントの場合、 UDP または TCP のポート番号を表示します。
情報	イベントに固有の情報

イベントビューアの情報のカラムに表示されるモニタイベントに固有の情報を表 10-2 に示します。

表 10-2: モニタイベント固有の情報

モニタイベント	表示する情報
TCP retransmission	TCP パケットのデータ長
TCP window frozen TCP long ack time	最後の ACK を検出した時刻
TCP checksum error UDP checksum error	TCP または UDP ヘッダーの Checksum フィールドの値と計算して得た正しいチェックサムの値
ICMP Destination unreachable ICMPv6 Destination unreachable	ICMP または ICMPv6 ヘッダーの Code フィールドの値とその意味を表す文字列
IP fragment timeout IP fragment error	IPv4 ヘッダーの Identification フィールドに示されている識別子
IP header checksum error	IPv4 ヘッダーの Header Checksum フィールドの値と計算して得た正しいチェックサムの値
IP duplicate IP address	IPv4 アドレスとそのアドレスが割り当てられている複数のネットワークインタフェースの MAC アドレス
IPv6 fragment timeout IPv6 fragment error	IPv6 のフラグメントヘッダーの Identification フィールドに示されている識別子
MAC traffic under threshold	モニタイベントが発生し始めたときの時刻
MAC traffic over threshold	閾値を越えた時点での 1 秒当たりトラフィック

10.2 イベントビューアの操作

イベントビューアでは、同じイベントをまとめて表示したり、見出しフィルタを使ったり、表示形式を変えることができます。

10.2.1 同一イベントの集約表示

イベント、発信元アドレス、発信元ポート番号、受信先アドレス、および受信先ポート番号が同じで、発生した時刻だけが異なるイベントはまとめて表示できます。

図 10-3: 同一イベントの集約表示

図 10-3 のイベントカラムの右端の括弧内の数値は、集約されたイベントの数です。

集約表示を止める

デフォルトでは、イベントは集約表示されるようになっています。個々のイベントが発生した時間を見る場合は、集約表示を止めます。すべてのイベントを展開するすることもできますし、特定のイベントだけを展開することもできます。

- **すべて展開する方法**
  イベントビューアを右クリックして、ポップアップメニューを開き、**集約表示(C)** を選びます。

集約表示に戻したい場合は、ポップアップメニューを開いて、もう一度**集約表示(C)** を選びます。

- **特定の集約表示を展開する方法**
  目的のイベントの行をダブルクリックします。展開されている部分は、淡いピンク色で表示されます。
  集約表示に戻したい場合は、もう一度ダブルクリックします。

10.2.2 イベントビューアで見出しフィルタを使う

イベントビューアでも見出しフィルタが使えます。見出しフィルタを使って、表示するイベントを絞り込めます。

見出しフィルタは、カラムに表示されている値を 1 つ選び、その値と一致する行だけを表示するフィルタです。複数のカラムに見出しフィルタを適用できます。

見出しフィルタの使えるカラムの見出しには▼が付いています。次のカラムで見出しフィルタが使えます。

- イベント
- 発信元アドレス
- 発信元ポート番号
- 受信先アドレス
- 受信先ポート番号
- 情報

見出しフィルタを適用する

1. カラムの見出しをクリックします。
   メニューが現れます。メニューの項目は、**オプション(P)**. . . 、およびクリックしたカラムに表示されている値の一覧から成ります。
2. メニューから項目を選びます。
   - 特定の値を選ぶと、選んだ値と一致する行だけが表示されます。
   - **オプション(P)**. . . を選ぶと、「オプション」ダイアログが現れます。「オプション」ダイアログについては、「6.6.4 「オプション」ダイアログ」 (134 ページ) を参照してください。

フィルタが適用されると、クリックしたカラムの見出しの▼が▼に変わります。

見出しフィルタを解除する

見出しフィルタは複数のカラムに適用できます。特定のカラムの見出しフィルタだけを解除するすることもできますし、すべてのカラムの見出しフィルタを一度に解除することもできます。

- 特定のカラムの見出しフィルタを解除する
  ▼が付いているカラムの見出しをクリックし、**すべて(L)** を選びます。
- すべての見出しフィルタを解除する
  - ツールバーの**フィルタ解除**ボタン() をクリックするか、
  - イベントビューアを右クリックしてポップアップメニューを開き、**フィルタ解除(R)** を選びます。

10.2.3 イベントビューアの表示形式を変える

イベントビューアは折れ線グラフ形式で表示できます。折れ線グラフ形式では、イベント数の推移を表します。

折れ線グラフに切り替える方法は 2 通りあります。

- イベントビューアのツールバーの**折れ線グラフ (履歴)** ボタン() をクリックします。
- イベントビューアを右クリックしてポップアップメニューを開き、**表示形式(V)** をポイントし、**折れ線グラフ(H)** を選びます。

図 10-4 に、折れ線グラフ形式に切り替えたイベントビューアを示します。

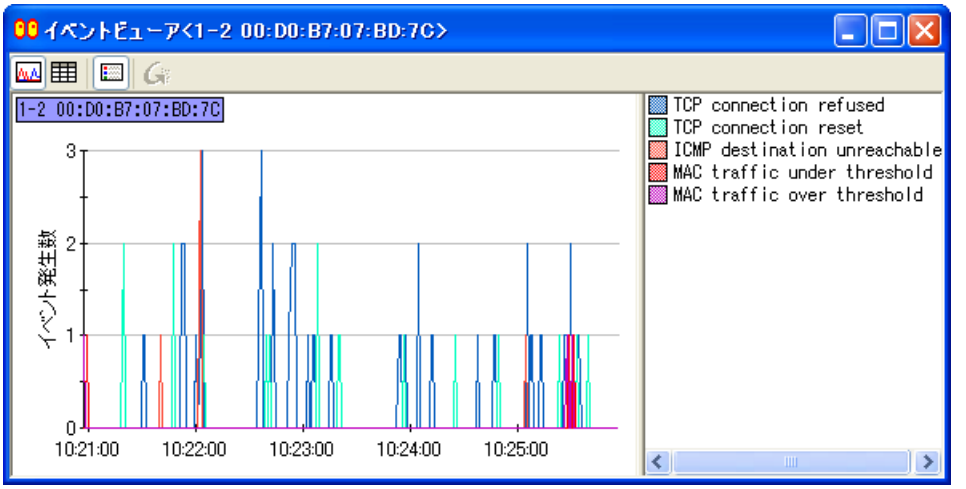


図 10-4: イベントビューアの折れ線グラフ形式の表示

トラフィックウィンドウと同じ操作で、グラフアイテムを選んだり、グラフアイテムの色を変えたり、選んだグラフアイテムだけを表示したりするようにできます。トラフィックウィンドウの操作については、「2.2　トラフィックウィンドウの表示をカスタマイズする」 (17 ページ) を参照してください。

表形式に切り替える方法は 2 通りあります。

- イベントビューアのツールバーの**表 (詳細)** ボタン(▦) をクリックします。
- イベントビューアを右クリックしてポップアップメニューを開き、**表示形式(V)** をポイントし、**表形式(T)** を選びます。

表形式の場合は、目的のイベントを見つけるために検索機能が使えます。検索するには、メインウィンドウの**編集(E)** メニューから**検索(F)** を選ぶか、 **<Ctrl-F>** キーを押します。 「検索」ダイアログが現れるので、探したい文字列を入力して**次を検索(F)** ボタンをクリックします。検索する文字列に正規表現を使うこともできます。正規表現を指定する場合は、**正規表現(E)** にチェックを付けます。正規表現については、「6.8.2　正規表現を用いた検索」 (147 ページ) を参照してください。

10.2.4 モニタイベントの表示期間を変える

モニタイベントを表示したイベントビューアを折れ線グラフ形式にしているとき、表示期間を切り替えられます。デフォルトでは、モニタウィンドウの短期タイムスパンと同じ期間内に発生したイベントだけを表示していますが、**履歴表示**にすると、 1000 件分を上限として記録されているモニタイベントをすべて表示します。

折れ線グラフの表示期間を切り替えるには、イベントビューアを右クリックして、ポップアップメニューを開き、**履歴を表示(H)** を選びます。

短期タイムスパンと履歴表示が交互に切り替わります。

短期タイムスパンで選べる期間は 5 分から 30 分です。短期タイムスパンの期間は「オプション設定」ダイアログで選びます。詳しくは「11.6　モニタのオプションを設定する」 (298 ページ) を参照してください。

10.3 イベントの設定

デフォルトでは、すべてのモニタイベントを検出するように設定されています。また、デコードイベントもすべて検出するように設定されています。この節では、検出する必要のないイベントを指定したり、閾値の必要なモニタイベント (MAC traffic under threshold、 TCP connection table threshold over、 TCP long ack time、 TCP window frozen time) の値を設定する方法について説明します。

10.3.1 モニタイベントの設定

モニタイベントはインタフェースごとに設定します。**モニタイベントを選ぶためには、対象とするインタフェースがインストールされているホストに対して設定権限が必要です。**

設定権限があるかどうかは、インタフェースセレクタウィンドウのアイコンで確認できます。ホストのアイコンが「**設定権限のあるホスト** () 」の場合は設定権限があります。「**設定権限のないホスト** () 」の場合は設定権限がありません。設定権限を取得する方法について、詳しくは「8.3　設定権限の取得と解放」 (192 ページ) を参照してください。

モニタイベントの設定を行うには、次のようにします。

1. 「ホストのプロパティ」ダイアログを開きます。「ホストのプロパティ」ダイアログを開く方法は 2 通りあります。
   - **「ホストのプロパティ」ダイアログを開く方法 1**
     (1) インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**... を選びます。
     (2) **「エキスパート」**のタブをクリックします。
   - **「ホストのプロパティ」ダイアログを開く方法 2**
     (1) メインウィンドウの**設定(O)** メニューの**エキスパート機能(E)** をポイントします。
     (2) サブメニューからホストを選びます。

現れた「ホストのプロパティ」ダイアログのようすを図 10-5 に示します。

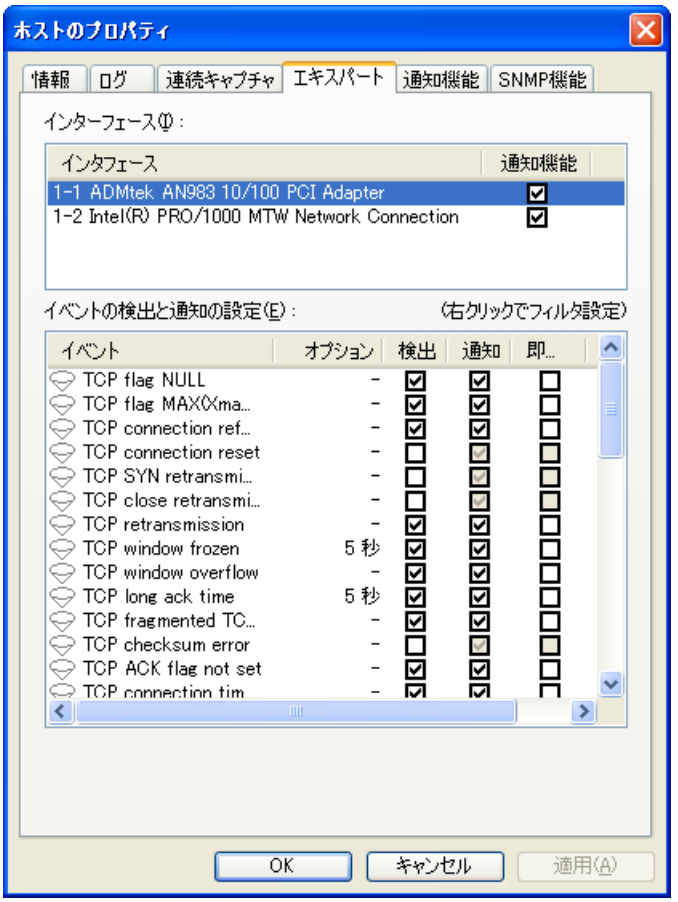


図 10-5: 「ホストのプロパティ」ダイアログ (モニタエキスパート機能)

2. インタフェースを選びます。
   インタフェース(I) のリストには、選んだホストにインストールされているインタフェースの一覧があります。
   モニタイベントの設定を行いたいインタフェースをクリックします。
3. 検出するモニタイベントを選びます。
   ASTEC Eyes は、**検出**カラムにチェックが付いているモニタイベントを検出します。デフォルトでは、ほとんどのイベントを検出するように設定されています。検出する必要のないモニタイベントからチェックを外します。

4. フィルタを設定します。
   イベントが検出される条件を追加で設定できます。**イベント**カラムの  を右クリックしてポップアップメニューを開き、イベントフィルタを選びます。
   イベントフィルタを作成していない場合には、ポップアップメニューから**フィルタエディタ(F)** を選んでイベントフィルタを作成してから、改めてフィルタを設定します。
5. 閾値を設定します。
   MAC traffic under threshold、 TCP connection table threshold over、 TCP long ack time、および TCP window frozen time は閾値が必要です。
   閾値のデフォルト値と設定できる値の範囲は次の通りです。

イベント	デフォルト値	値の範囲
MAC traffic under threshold	2097152	2048 ≤ 値 ≤ 4294967295 (バイト)
TCP connection table threshold over	2000	30 ≤ 値 ≤ 8000 (カウント)
TCP long ack time	5	1 ≤ 値 ≤ 65535 (秒)
TCP window frozen time	5	1 ≤ 値 ≤ 65535 (秒)

   これらのイベントの閾値を変えたい場合は、オプションカラムに閾値を入力します。
   入力するには、次のようにします。

   (1) 閾値を入力したい行をクリックしてます。
   クリックした行が青く反転します。
   (2) オプションカラムをクリックするか、 **<F2>** キーを押してオプションカラムに入力できる状態にします。
   (3) 値をキー入力します。
   (4) **<Enter>** キーを押します。
   <Enter> キーを押さないと、元の値に戻ってしまいます。
6. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

インタフェースツールバーに「ホストのプロパティ」ダイアログを表示するボタン () を追加することもできます。このボタン () を押したときにプロパティが表示されるホストは、選択中のインタフェースが属すホストです。
ツールバーのカスタマイズの方法について、詳しくは「1.1.1　ツールバー」 (6 ページ) を参照してください。

10.3.2 デコードイベントの設定

デコードイベントの設定は「オプション設定」ダイアログで行います。

1. 「オプション」ダイアログを開きます。「オプション設定」ダイアログを開く方法は 2 通りあります。
   - コモンツールバーの**オプション設定**ボタン() をクリックします。
   - メインウィンドウの**設定(O)** メニューから**オプション設定(O)**... を選びます。
2. ダイアログの左側にあるツリーの中の**デコードエキスパート**をクリックします。
3. **デコードエキスパート機能を利用する(D)** にチェックを付けます。あるいは、チェックを外します。
4. **イベントの検出の設定(E)** のリストに、デコードエキスパート機能で検出できるイベントの一覧があります。 ASTEC Eyes は**検出**カラムにチェックが付いているデコードイベントを検出します。検出する必要のないデコードイベントからチェックを外します。
5. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

すでに表示されいるデコードビューに設定を反映するには、再デコードが必要です。

デコードイベントを検出するように設定すると、デコードにかかる時間が長くなります。また、消費するメモリも増えます。

10.4 イベント一覧

10.4.1 モニタイベント一覧

ASTEC Eyes が検出するモニタイベントの一覧を表 10-3 に示します。

表 10-3: モニタイベントとモニタイベントが発生する条件

モニタイベント	発生条件
TCP flag NULL	TCP ヘッダーの Flags フィールドの URG、 ACK、 PSH、 RST、 SYN、 FIN のすべてのビットが OFF であるパケットを検出します。
TCP flag MAX (Xmas scan)	TCP ヘッダーの Flags フィールドの URG、 ACK、 PSH、 RST、 SYN、 FIN のすべてのビットが ON であるパケットを検出します。
TCP connection refused	TCP の接続を確立するために SYN パケットを送った結果、 RST パケットを受け取ったことを検出します。
TCP connection reset	TCP connection refused 以外の状況で RST パケットを受け取ったことを検出します。
TCP SYN retransmission	TCP ヘッダーの Sequence Number が同じ SYN パケットを 2 回以上受け取ったことを検出します。
TCP close retransmission	TCP の FIN パケットを送った後に再送が起きたことを検出します。
TCP retransmission	TCP SYN retransmission と TCP close retransmission 以外の状況で、 TCP パケットの再送が起きたことを検出します。
TCP window frozen	TCP のウィンドウサイズが 576 バイトより小さい状態が指定した時間以上続いていることを検出します。
TCP window overflow	TCP のウィンドウサイズより多くのデータを含んでいるパケットを検出します。
TCP long ack time	指定した時間を過ぎてから受け取った TCP の ACK パケットを検出します。
TCP fragmented TCP data	IP 層でフラグメント化された TCP パケットを検出します。
TCP checksum error	TCP のチェックサムが誤っているパケットを検出します。
TCP ACK flag not set	一番最初に送る SYN パケット以外のパケットで、 TCP ヘッダーの Flgas フィールドの ACK ビットが OFF のパケットを検出します。
TCP connection timeout	TCP の接続を確立するときに、応答パケットが送られないまま一定時間が経過したことを検出します。
TCP connection table threshold over	TCP ステータス情報のエントリ数が指定数を超えたことを検出します。

次ページへ続く

モニタイベント	発生条件
UDP checksum error	UDP のチェックサムが誤っているパケットを検出します。
ICMP destination unreachable	ICMP の destination unreachable パケットを検出します。
ICMP checksum error	ICMP のチェックサムが誤っているパケットを検出します。
ICMPv6 destination unreachable	ICMPv6 の destination unreachable パケットを検出します。
ICMPv6 checksum error	ICMPv6 のチェックサムが誤っているパケットを検出します。
IP fragment timeout	IP 層で IPv4 のパケットがフラグメント化されている場合に、一定時間内に届かなかったフラグメントがあることを検出します。
IP fragment error	IP 層で IPv4 のパケットがフラグメント化されている場合に、フラグメントから再構成したパケットが不完全であることを検出します。
IP header checksum error	IPv4 のチェックサムが誤っているパケットを検出します。
IP invalid IP length	IPv4 ヘッダーの Total Length フィールドに示されているバイト数と実際のデータ長が異なるパケットを検出します。
IP duplicate IP address	異なる MAC アドレスに同じ IPv4 アドレスが付けられていることを検出します。
IPv6 fragment timeout	IP 層で IPv6 のパケットがフラグメント化されている場合に、一定時間内に届かなかったフラグメントがあることを検出します。
IPv6 fragment error	IP 層で IPv6 のパケットがフラグメント化されている場合に、フラグメントから再構成したパケットが不完全であることを検出します。
MAC traffic under threshold	MAC 層で計測した 1 秒あたりのバイト数が指定した閾値を越えていたことを検出します。閾値を超えていた期間の最後に発生するイベントです。
MAC traffic over threshold	MAC 層で計測した 1 秒あたりのバイト数が指定した閾値を越えたことを検出します。閾値を越えた直後に発生するイベントです。
NIC monitor reset	モニタがリセットされたことを検出します。
NIC driver started	ネットワークインタフェースカードのドライバが開始したことを検出します。
NIC driver terminated	ネットワークインタフェースカードのドライバが終了したことを検出します。
NIC link speed changed	ネットワークインタフェースカードのリンクスピードが変化したことを検出します。
NIC link up	ネットワークインタフェースカードのリンクアップを検出します。
NIC link down	ネットワークインタフェースカードのリンクダウンを検出します。
NIC capture file output started	連続キャプチャを開始した後に、初めてパケットをキャプチャしたことを検出します。
NIC capture file output stopped	連続キャプチャが停止したことを検出します。

次ページへ続く

モニタイベント	発生条件
NIC capture file roll	連続キャプチャを行っているときに、次のファイルを書き出し始めたことを検出します。
NIC packet send start	トラフィックジェネレータがパケットの送信を開始したことを検出します。
NIC packet send stop	トラフィックジェネレータがパケットの送信を停止したことを検出します。
NIC user filter	ユーザーが定義したイベントを検出します。

10.4.2 デコードイベント一覧

ASTEC Eyes が検出するデコードイベントの一覧を表 10-4 に示します。

表 10-4: デコードイベントとデコードイベントが発生する条件

デコードイベント	発生条件
TCP 接続拒否	TCP の接続を確立するために SYN パケットを送った結果、 RST パケットを受け取ったことを示します。
TCP 再送	TCP の再送が起きたことを示します。
TCP データを送らずに接続終了	1 バイトもデータを送っていない状態で FIN パケットを受け取ったことを示します。
TCP 不正な checksum 値	TCP のチェックサムが誤っているパケットであることを示します。
UDP 不正な checksum 値	UDP のチェックサムが誤っているパケットであることを示します。
ICMP4 Destination Unreachable	ICMP の destination unreachable パケットであることを示します。
ICMP4 Source Quench	ICMP の source quench パケットであることを示します。
ICMP4 Redirect	ICMP の redirect パケットであることを示します。
ICMP4 Time Exceeded	ICMP の time exceeded パケットであることを示します。
ICMP4 Parameter Problem	ICMP の parameter problem パケットであることを示します。
ICMP4 Traceroute	ICMP の traceroute パケットであることを示します。
ICMP4 Conversion Failed	ICMP の conversion failed パケットであることを示します。
ICMP4 Security Failure	ICMP の security failure パケットであることを示します。
ICMP6 Destination Unreachable	ICMPv6 の destination unreachable パケットであることを示します。
ICMP6 Time Exceeded	ICMPv6 の time exceeded パケットであることを示します。

次ページへ続く

デコードイベント	発生条件
ICMP6 Parameter Problem	ICMPv6 の parameter problem パケットであることを示します。
ICMP6 Redirect	ICMP の redirect パケットであることを示します。
FTP 接続エラー	FTP で接続できなかったことを示します。
FTP 認証エラー	FTP で認証に失敗して接続できなかったことを示します。
FTP ファイルアクセスエラー	FTP でファイルにアクセスできなかったことを示します。
SOCKS 接続エラー	SOCKS で接続できなかったことを示します。
SOCKS リクエストエラー	SOCKS のリクエストが失敗したことを示します。
DNS エラー応答	DNS のエラー応答を示します。
DNS 応答なし	DNS のクエリーに対応する応答がないことを示します。
ARP 応答なし	ARP のリクエストに対応する応答がないことを示します。
RARP 応答なし	RARP のリクエストに対応する応答がないことを示します。
DHCP 応答なし	DHCP のリクエストに対応する応答がないことを示します。
BOOTP 応答なし	BOOTP のリクエストに対応する応答がないことを示します。
IPv4 分割パケットの再構成に失敗	分割された IPv4 パケットのデータ部分を再構成できなかったことを示します。
IPv6 分割パケットの再構成に失敗	分割された IPv6 パケットのデータ部分を再構成できなかったことを示します。

10.5 通知機能の設定

検出したモニタイベントをメールや SNMP トラップで通知することもできます。通知機能を使うためには、次の設定が必要です。

- 通知するインタフェースとイベント
  通知するかどうかは、インタフェース単位およびイベント単位で指定できます。
- メールの設定
  通知するメールの宛先や、メールのフォーマット、何分ごとに通知メールを送信するのか、などをホストごとに指定します。
- SNMP トラップの設定
  SNMP トラップの通知先ホストと SNMP コミュニティを指定します。

10.5.1 通知するインタフェースとイベントを指定する

デフォルトでは、メールで通知するように設定したホストにインストールされているすべてのインタフェースで発生したすべてのイベントを通知します。特定のインタフェースで発生したイベントのうち、特定のイベントだけを通知し、必要のないイベントは通知しないように設定できます。

通知するイベントを指定するには、次のようにします。

1. 「ホストのプロパティ」ダイアログを開きます。
   「ホストのプロパティ」ダイアログを開く方法は 2 通りあります。
   - **「ホストのプロパティ」ダイアログを開く方法 1**
     (1) インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**... を選びます。
     (2) **「エキスパート」**のタブをクリックします。
   - **「ホストのプロパティ」ダイアログを開く方法 2**
     (1) メインウィンドウの**設定(O)** メニューの**エキスパート機能(E)** をポイントします。
     (2) サブメニューからホストを選びます。

   現れた「ホストのプロパティ」ダイアログのようすを図 10-6 に示します。

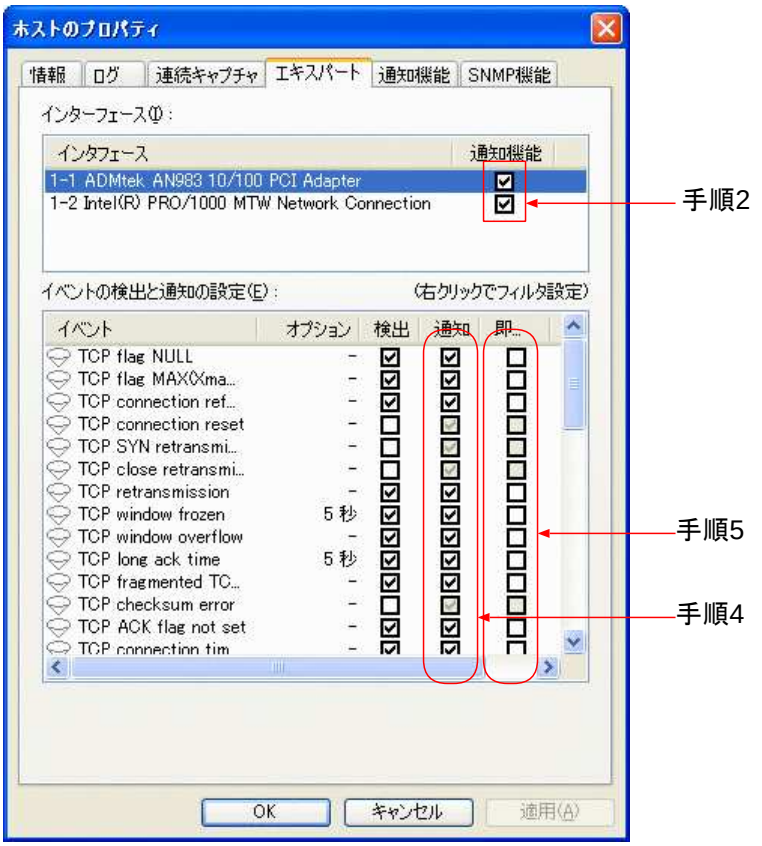


図 10-6: 「ホストのプロパティ」ダイアログ (エキスパート)

2. まず、インタフェースごとに通知機能を有効にするかどうかを指定します。
   デフォルトでは、すべてのインタフェースで通知機能が有効になっています。イベントを通知する必要のないインタフェースについては、**インタフェース(I)** のリストの通知機能カラムからチェックを外します。
   通知機能カラムからチェックを外すと、**イベントの検出と通知の設定(E)** のリストの通知および即時配信カラムは灰色に変わり、個々のイベントの設定が無効になったことを示します。
3. 次に、イベントごとに通知するかどうかを指定します。
   インタフェース(I) のリストをクリックして、通知機能カラムにチェックの付いているインタフェースを選びます。
4. **イベントの検出と通知の設定(E)** のリストには、イベントの一覧が表示されています。検出

カラムにチェックを付けているイベントのうち、メールで通知したいイベントの通知カラムと SNMP トラップで通知したいイベントの SNMP トラップカラムにチェックを付けます。必要のないイベントからはチェックを外します。
検出カラムにチェックが付いていないイベントについては、通知や SNMP トラップカラムにチェックを付けても、イベント自体を検出しないので通知されません。

5. 通知カラムにチェックを付けたイベントのうち、検出したらすぐに通知したいイベントは、即時配信カラムにもチェックを付けます。
   通常、検出したイベントはまとめて定期的に通知しますが、即時配信カラムにチェックの付いたイベントが発生すると、直ちにメールを送信します。
6. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

インタフェースツールバーに「ホストのプロパティ」ダイアログを表示するボタン () を追加することもできます。このボタン () を押したときにプロパティが表示されるホストは、選択中のインタフェースが属すホストです。
ツールバーのカスタマイズの方法について、詳しくは「1.1.1　ツールバー」 (6 ページ) を参照してください。

10.5.2　メールを設定する

メールの設定はモニタイベントを検出するホストごとに行います。

メールの設定には、モニタイベントの検出対象とするホストに対して設定権限が必要です。

設定権限があるかどうかは、インタフェースセレクタウィンドウのアイコンで確認できます。ホストのアイコンが「**設定権限のあるホスト** () 」の場合は設定権限があります。「**設定権限のないホスト** () 」の場合は設定権限がありません。設定権限を取得する方法について、詳しくは「8.3　設定権限の取得と解放」 (192 ページ) を参照してください。

メールの設定は、次のようにします。

1. 「ホストのプロパティ」ダイアログを開きます。
   「ホストのプロパティ」ダイアログを開く方法は 2 通りあります。
   - **「ホストのプロパティ」ダイアログを開く方法 1**
     (1) インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
     (2) **「通知機能」**のタブをクリックします。
   - **「ホストのプロパティ」ダイアログを開く方法 2**
     (1) メインウィンドウの**設定(O)** メニューの**通知機能(N)** をポイントします。

(2) サブメニューからホストを選びます。

現れた「ホストのプロパティ」ダイアログのようすを図 10-7 に示します。

図 10-7: 「ホストのプロパティ」ダイアログ (通知機能)

2. **通知機能を有効にする(E)** にチェックを付けます。
3. **SMTP サーバー(S)** にローカルホストまたはリモートホストが認識できるメールサーバーのホスト名を入力します。
4. **To ヘッダー(T)** にメールの宛先を入力します。メールサーバーによっては、ドメイン名も含めて入力する必要があります。
5. **From ヘッダー(F)** にメールの差出人のアドレスを入力します。メールサーバーによっては、

ドメイン名も含めて入力する必要があります。

6. **メール本文の形式(B)** でメールの本文の部分の形式を選びます。
   プレーンテキストまたは CSV 形式が選べます。
7. **メール件名の形式(J)** でメールの件名 (サブジェクト) 部分の形式を選びます。
8. **メールの送信間隔(I)** にメールの送信間隔を入力します。
   デフォルトは 5 分です。 5 分間の間に発生したイベントを 1 本のメールにまとめて **To ヘッダー(T)** で指定した宛先へ送ります。
   ただし、「インタフェースのプロパティ」ダイアログの「エキスパート」のページの**イベントの検出と通知の設定(E)** の即時配信カラムにチェックを付けたイベントが発生した場合は、直ちにメールを送ります。
9. 通知メールを送った先のメールサーバーからエラーが返された場合、**送信に失敗したときは通知機能を停止する(P)** にチェックを付けておくと、メールの送信を停止します。
10. **適用(A)** ボタンをクリックします。
11. 設定内容を確認するために、**テスト送信(N)** ボタンをクリックします。
    「テスト送信」ダイアログが現れて、状況を表示します。
    正常終了のメッセージが表示されなかった場合は、**閉じる(C)** ボタンをクリックして「テスト送信」ダイアログを閉じ、手順 3 に戻って設定を確認します。

インタフェースツールバーに「ホストのプロパティ」ダイアログを表示するボタン () を追加することもできます。このボタン () を押したときにプロパティが表示されるホストは、選択中のインタフェースが属すホストです。
ツールバーのカスタマイズの方法について、詳しくは「1.1.1　ツールバー」 (6 ページ) を参照してください。

10.5.3　メールの送信状況を見る

何通メールを送ったのか、送ったメールのうち正常に送れたのは何通だったのか、などを見ることができます。

メールの送信状況は「ホストのプロパティ」ダイアログの「通知機能」のページの **ステータス情報** 領域に表示されます。「ホストのプロパティ」ダイアログを開く方法については、「10.5.2 メールを設定する」 (254 ページ) を参照してください。

「ホストのプロパティ」ダイアログを図 10-8 に示します。

図 10-8: 「通知機能」のページに表示されるメールの送信状況

ステータス情報 領域に、「ホストのプロパティ」ダイアログを開いた時点のメールの送信状況が表示されます。

シーケンス番号は、キャプチャモジュールが起動してから送信したメールの数を示しています。**リセット(R)** ボタンでリセットすることはできません。キャプチャモジュールが再起動したときにリセットされます。その他のカウンタは**リセット(R)** ボタンで 0 に戻せます。

ステータス情報 領域に表示されている情報は、自動的に更新されません。更新するには、**情報を更新(U)** ボタンをクリックします。

10.5.4 SNMP トラップを設定する

SNMP トラップの設定はモニタイベントを検出するホストごとに行います。

SNMP トラップの設定には、モニタイベントの検出対象とするホストに対して設定権限が必要です。

設定権限があるかどうかは、インタフェースセレクタウィンドウのアイコンで確認できます。ホストのアイコンが「**設定権限のあるホスト** () 」の場合は設定権限があります。「**設定権限のないホスト** () 」の場合は設定権限がありません。設定権限を取得する方法について、詳しくは「8.3　設定権限の取得と解放」 (192 ページ) を参照してください。

SNMP トラップの設定は、次のようにします。

1. 「ホストのプロパティ」ダイアログを開きます。
   「ホストのプロパティ」ダイアログを開く方法は 2 通りあります。
   - **「ホストのプロパティ」ダイアログを開く方法 1**
     (1) インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
     (2) **「SNMP 機能」**のタブをクリックします。
   - **「ホストのプロパティ」ダイアログを開く方法 2**
     (1) メインウィンドウの**設定(O)** メニューの **SNMP 機能(S)** をポイントします。
     (2) サブメニューからホストを選びます。

   現れた「ホストのプロパティ」ダイアログのようすを図 10-9 に示します。

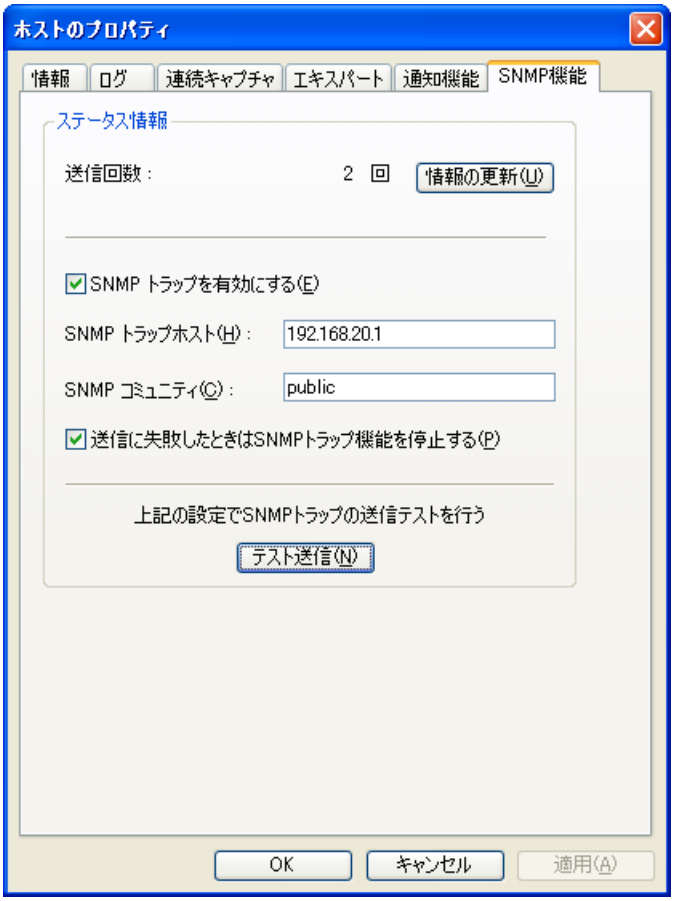


図 10-9: 「ホストのプロパティ」ダイアログ (SNMP トラップ)

2. **SNMP トラップを有効にする(E)** にチェックを付けます。
3. **SNMP トラップホスト(H)** にローカルホストまたはリモートホストが認識できる SNMP トラップの送信先ホスト名を入力します。
4. **SNMP コミュニティ(C)** に SNMP のコミュニティ名を入力します。
5. SNMP トラップを送った先のホストからエラーが返された場合、**送信に失敗したときは SNMP トラップ機能を停止する(P)** にチェックを付けておくと、 SNMP トラップの通知を停止します。
6. **適用(A)** ボタンをクリックします。
7. 設定内容を確認するために、**テスト送信(N)** ボタンをクリックします。

「テスト送信」ダイアログが現れて、状況を表示します。
正常終了のメッセージが表示されなかった場合は、**閉じる(C)** ボタンをクリックして「テスト送信」ダイアログを閉じ、手順 3 に戻って設定を確認します。

10.6 セキュリティに関する情報

モニタエキスパート機能では、ネットワークの性能低下のほかに、セキュリティ上の弱点を攻撃するいくつかの攻撃パターンも検出できます。以下では、典型的な攻撃パターンについて説明します。

10.6.1 ポートスキャン攻撃

ポートスキャンは多くのホストや特定のホストの TCP や UDP のポートに順次アクセスして、さまざまな情報を入手し、セキュリティ上の弱点を探す攻撃の総称です。

たいていの場合、ポートスキャンは情報を集めるだけで被害を与えませんが、悪意のユーザーは集めた情報をもとにして、既知のセキュリティホールからの侵入を試みるので、セキュリティ上の弱点がある場合は弱点を修正するパッチを適用するなどの対策が必要です。

ポートスキャンには送るパケットやアクセス方法が違うさまざまな手法があり、探し出せる弱点や情報が異なります。たとえば、攻撃対象のホストが存在しているかどうかやポートの状態のほか、攻撃対象のホスト上で動作している OS やアプリケーションの種類が分かることもあります。また、ポートスキャンを実行したことを悟られにくいように、ログに記録を残さないアクセス方法もあります。

一般に、特定の範囲のポートすべて、または特定の範囲のランダムなポート番号がポートスキャンの対象にされる場合と、侵入口になる可能性のある telnet や ftp、またはホストの情報を返す可能性がある smtp や http などの Well known ポートがポートスキャンの対象にされる場合とがあります。

セキュリティチェック用のアプリケーションの中には、ホストの弱点を調査するためにポートスキャンを実行するものもあります。

以下は典型的なポートスキャンの手法です。

NULL スキャン　TCP ヘッダーの flags フィールドのすべてのビットを OFF にしたパケットを送ります。 RFC にしたがえば、ホストは閉じたポートに届いたパケットに対して RST パケットを送り返さなくてはなりません。

攻撃した側は、送り返されたパケットからポートが開いているかどうかを知ることができます。

Xmas スキャン　Xmas スキャンは、 TCP ヘッダーの flags フィールドのいくつかのビットを ON にしたパケットを送ります。 flags フィールドのどのビットを ON にするかはポート

スキャンプログラムの種類によって異なりますが、通常は FIN、 URG、 PSH と他のビットのいくつかまたはすべてを ON にしたパケットを使います。

NULL スキャンと同様、閉じたポートにパケットが届いたときは RST パケットが送り返されます。

攻撃した側は、送り返されたパケットからポートが開いているかどうかを知ることができます。

FIN スキャン　TCP ヘッダーの FIN ビットを ON にしたパケットを送ります。 NULL スキャンと同様、閉じたポートにパケットが届いたときは RST パケットが送り返されます。

攻撃した側は、送り返されたパケットからポートが開いているかどうかを知ることができます。

10.6.2 DoS (Denial of Service) 攻撃

短時間に大量のパケットを送り込む、巨大なデータを送る、ブロードキャストを使ってネットワークを高トラフィック状態にする、既知の脆弱性を利用してサービスできない状態にするなど、攻撃対象のホストやネットワークの運用を妨害する攻撃を総称して **DoS (Denial of Service** — サービス運用妨害) 攻撃と呼びます。

ポートスキャン攻撃とは違い、 DoS 攻撃は実際の被害を伴います。たとえば、 WWW ページにアクセスできなくなったり、メールが送受信できなくなったり、場合によっては攻撃を受けたホストが停止・クラッシュすることもあります。

以下は典型的な DoS 攻撃の手法です。

SYN flood 攻撃　攻撃対象のホストに対して、短時間に大量の TCP の SYN パケットを送ります。

SYN パケットを受け取ったホストは TCP の接続シーケンスにしたがって ACK パケットを返し、接続処理の途中であることをバッファに記録して、相手のホストから確認の ACK パケットが送られてくるのを待ちます。攻撃する側は ACK パケットを送らないで次々と新しい SYN パケットを送り込むため、攻撃を受けているホストの接続処理用のバッファがあふれ、新しい接続要求を受け付けられなくなります。

SYN flood 攻撃では TCP のコネクションの作成が完成しないため、攻撃されたホストの通常のログに記録が残りません。そのため、攻撃する側にとって、どこから攻撃しているかを知られにくいという利点があります。

フラグメント攻撃　フラグメント攻撃では、攻撃対象のホストに対して IP 層でフラグメント化されたパケットを送ります。

よく知られている攻撃パターンは、再構成が難しかったり再構成できないランダムなフラグメントを大量に送り込む手法です。フラグメントを受け取ったホストはパケットを再構成しようとしますが、正しく組み立てられないフラグメントばかりが届くため、メモリや CPU を圧迫します。結果的にホスト全体の負荷が上昇して他の処理が遅くなったり実行できなくなります。

OS によっては、フラグメント化されたパケットの再構成に関する既知の弱点を持つものがあります。既知の弱点を攻める特定のパターンのパケットを送る攻撃もあります。

10.6.3　なりすまし攻撃

IP アドレス、メールアドレス、あるいはログイン ID を詐称してパケットを入手したり、他人になりすましてホストにアクセスする攻撃を総称して**なりすまし攻撃**と呼びます。

特に、 IP アドレスを詐称する方法は **IP スプーフィング (IP spoofing)** と呼ばれ、パケットレベルで通信をのぞき見したり、パケットを横取りするのと同時に本当の通信相手に対して同じパケットを送りだして、のぞき見していることを悟られないようにする場合もあります。

10.7 モニタイベントの分析

ここでは各モニタイベントが発生する状況や注意すべき点について説明します。これらの記述を参考に、モニタイベントが発生した状況を分析してください。

10.7.1 TCP flag NULL

TCP ヘッダーの Flags フィールドの URG、 ACK、 PSH、 RST、 SYN、 FIN のすべてのビットが OFF であるパケットを検出します。

ポートスキャンの一種である **NULL スキャン**は、 Flags フィールドのすべてのビットが OFF であるパケットをスキャン対象のホストに送ります。ポートスキャンについては、「10.6 セキュリティに関する情報」 (261 ページ) の「ポートスキャン攻撃」を参照してください。

以下は、受信先ホストに対してポートスキャンが実行された際の典型的な状態です。

- 短時間のうちに頻繁に (数秒間に 1 回から 1 秒間に数回以上) モニタイベントが発生
- 受信先のポートが Well known ポート

10.7.2 TCP flag MAX (Xmas scan)

TCP ヘッダーの Flags フィールドの URG、 ACK、 PSH、 RST、 SYN、 FIN のすべてのビットが ON であるパケットを検出します。

通常の通信では、 Flags フィールドのすべてのビットが ON のパケットが送られることはありません。

ポートスキャンの一種である **Xmas スキャン**は、 Flags フィールドのいくつかのビットが ON であるパケットをスキャン対象に送ります。 flags フィールドのどのビットを ON にするかはポートスキャンプログラムの種類によって異なります。 ASTEC Eyes は、すべてのビットが ON であるパケットを検出したらモニタイベントを発生します。ポートスキャンについては、「10.6 セキュリティに関する情報」 (261 ページ) の「ポートスキャン攻撃」を参照してください。

以下は、受信先ホストに対してポートスキャンが実行された際の典型的な状態です。

- 短時間のうちに頻繁に (数秒間に 1 回から 1 秒間に数回以上) イベントが発生
- 受信先のポートが Well known ポート

10.7.3 TCP connection refused

TCP の接続を確立するために SYN パケット (SYN ビットが ON のパケット) を送った結果、RST パケット (RST ビットが ON のパケット) を受け取ったことを検出します。

閉じているポートに、 TCP の接続の確立を要求する SYN パケットが届いたとき、受信先のホストは RST パケットを送り返してポートが閉じていることを発信元のホストに伝えます。

TCP connection refused イベントが発生する状況として、次のような場合が考えられます。

- 利用しようとしたネットワークサービスが動作していなかった (閉じているポートに接続しようとした)
- ポートスキャン攻撃

たとえば、 telnet サービスを提供していないホストに対して telnet コマンドで接続しようとしたときに、イベントが発生します。

短時間のうちに頻繁に (数秒間に 1 回から 1 秒間に数回以上) イベントが発生したときには、発信元ホスト (RST パケットを送ったホスト) がポートスキャン攻撃を受けている可能性があります。

ポートスキャンについては、「10.6　セキュリティに関する情報」 (261 ページ) の「ポートスキャン攻撃」を参照してください。

10.7.4 TCP connection reset

TCP connection refused 以外の状況で RST パケット (RST ビットが ON のパケット) を受け取ったことを検出します。

TCP connection reset イベントが発生する状況として、次のような場合が考えられます。

- 接続中の通信を強制的に切断した
- ポートスキャン攻撃

アプリケーションによっては、通信中の TCP の接続を即座に切断するために、 RST パケットを送るものがあります。たとえば、 WWW ページの表示を中止したときに、 WWW サーバに対して RST パケットを送るブラウザがあります。

ポートスキャンの一種である **FIN スキャン**は、 FIN パケット (FIN ビットが ON のパケット) をスキャン対象のホストに送ります。接続が確立していないときに FIN パケットが届くと、 RST パケットが送り返されます。短時間のうちに頻繁に (数秒間に 1 回から 1 秒間に数

回以上) イベントが発生したときには、発信元ホスト (RST パケットを送ったホスト) がポートスキャン攻撃を受けている可能性があります。

ポートスキャンについては、「10.6　セキュリティに関する情報」 (261 ページ) の「ポートスキャン攻撃」を参照してください。

10.7.5　TCP SYN retransmission

TCP ヘッダーの Sequence Number が同じ SYN パケット (SYN ビットが ON のパケット) が 2 回以上送られたことを検出します。

たとえば、特定のホストに対して telnet コマンドや ftp コマンドを実行したとき、 TCP の接続を確立するために 1 回目の SYN パケットが送られます。このとき、

- 接続先のホストが停止している、またはネットワークが切断している
- 通信経路の途中でパケットが破棄された
- 接続先のホストやネットワークの性能が低下していて、パケットの配送が遅れた

などの理由から、 ACK パケットを受け取らないうちにタイムアウト時間 (通常は数秒程度) が過ぎると、発信元のホストはもう一度接続を試みます。 2 回目は 1 回目の SYN パケットと同じ Sequence Number 値を設定した SYN パケットを送ります。 2 回目以降も応答がなければ、タイムアウト時間を変えながら何回か SYN パケットを再送します。 2 回目またはそれ以降の SYN パケットの再送を検出するたびに、 TCP SYN retransmission イベントが発生します。

TCP SYN retransmission イベントは、 **SYN flood 攻撃**のような **DoS** (**Denial of Service** — サービス運用妨害) 攻撃を受けて、ネットワークの性能が低下したときにもしばしば発生します。高い頻度で (1 秒間に数回またはそれ以上) イベントが発生したときには、受信先ホストが DoS 攻撃を受けている可能性があります。

DoS 攻撃については、「10.6　セキュリティに関する情報」 (261 ページ) の「DoS (Denial of Service) 攻撃」を参照してください。

10.7.6　TCP close retransmission

TCP の FIN パケットを送った後に再送が起きたことを検出します。

次のような状況のときにこのイベントが発生します。

- FIN パケットの再送

- **ハーフクローズ** (TCP の接続の片側が閉じている) 状態のときに、閉じていない側で再送が発生した

TCP close retransmission イベントは、次の TCP retransmission イベントと同様の状況で発生します。また、ルーターなどのネットワーク機器の設定ミスで発生する可能性もあります。

ネットワーク機器のなかには次のような目的のために、 FIN パケットをフィルタリングする機能を持つものがあります。

- 終了時に FIN パケットを送るアプリケーションがあり、 FIN パケットを送るためだけにダイアルアップルーターが電話をかける問題を回避する必要がある
- FIN スキャンによるポートスキャン攻撃を防ぐ

FIN パケットのフィルタリングの設定が誤っていると、アプリケーションから送られた正常な FIN パケットが破棄されてしまい、アプリケーションが FIN パケットを再送し続けるという現象が起こります。

10.7.7 TCP retransmission

TCP SYN retransmission、 TCP close retransmission 以外の状況で、 TCP パケットの再送が起きたことを検出します。

TCP retransmission イベントが発生する状況として、次のような場合が考えられます。

- 接続先のホストが停止している、またはネットワークが切断している
- 経路の途中でパケットが破棄された
- 接続先のホストやネットワークの性能が低下していて、パケットの配送が遅れた

たとえば、特定のホストに対して telnet コマンドや ftp コマンドを実行しているとき、送ったパケットに対して ACK パケットを受け取らないうちにタイムアウト時間 (通常は数秒程度) が過ぎると、発信元のホストはもう一度同じパケットを再送します。 2 回目以降も応答がなければ、タイムアウト時間を変えながら何回かパケットを再送します。 2 回目またはそれ以降のパケットの再送を検出するたびに、 TCP retransmission イベントが発生します。

インターネット上のホストや使用頻度の高いホストと通信しているときには、しばしば TCP retransmission イベントが発生します。

ローカルなネットワーク間の通信でも、 Ethernet のコリジョンでパケットが失われたときや、応答が遅い場合はイベントが発生します。 TCP retransmission イベントが頻繁に発生するよ

うであれば、ネットワークが高トラフィック状態であったり、ホストの負荷が高くて処理能力が低下している可能性があります。

TCP retransmission イベントが高い頻度で (1 秒間に 1 回またはそれ以上) 継続的に発生するときには、 DoS (Denial of Service) 攻撃を受けている可能性もあります。

DoS 攻撃については、「10.6　セキュリティに関する情報」 (261 ページ) の「DoS (Denial of Service) 攻撃」を参照してください。

10.7.8　TCP window frozen

TCP のウィンドウサイズが 576 バイトよりも小さい状態が、指定した時間以上続いていることを検出します。

TCP プロトコルではデータ転送を効率よく行うために、発信元ホストは ACK パケットを受け取る前でもウィンドウサイズ分だけのデータを連続して送ってよいと決めています。受信先ホストは受け取ったデータをいったん受信バッファに保存し、処理するとバッファから削除します。つぎに、 ACK パケットを返すときには、受信先ホストは TCP ヘッダーの Window Size フィールドに、バッファの現在の空き容量を意味するウィンドウサイズを設定します。発信元ホストは ACK パケットのウィンドウサイズから、一度に送ることができるデータのサイズを知ることができます。

TCP window frozen イベントの原因として、受信先ホストの処理能力が低下していて、受け取ったパケットの処理が間に合っていないことが考えられます。このイベントは受信先ホストの負荷が高いときにしばしば現れます。

TCP のウィンドウサイズが小さいと、長いデータは小さなパケットに分けて何回も送らなくてはならないため、データ転送の効率が低下します。

このイベントは、 TCP の通信性能の低下を知るために用意されています。 TCP ウィンドウサイズが小さい状態が何秒以上続いたらイベントを発生させるかは、ユーザーが設定できます。詳しくは「10.3.1　モニタイベントの設定」 (244 ページ) を参照してください。

10.7.9　TCP window overflow

TCP のウィンドウサイズより多くのデータを含んでいるパケットを検出します。

TCP プロトコルではデータ転送を効率よく行うために、発信元ホストは ACK パケットを受け取る前でもウィンドウサイズ分だけのデータを連続して送ってよいと決めています。受信先ホストは受け取ったデータをいったん受信バッファに保存し、処理するとバッファから削除します。つぎに、 ACK パケットを返すときには、受信先ホストは TCP ヘッダーの Window Size フィールドに、バッファの現在の空き容量を意味するウィンドウサイズを設定します。発

信元ホストは ACK パケットのウィンドウサイズから、一度に送ることができるデータのサイズを知ることができます。

TCP window overflow イベントは、受信先ホストが Window Size フィールドに設定したウィンドウサイズよりも大きなパケットを、発信元ホストが送ったときに発生します。

10.7.10 TCP long ack time

指定した時間を過ぎてから受け取った TCP の ACK パケットを検出します。

インターネット上のホストなど、ネットワーク的に遠距離にありパケットが到達するまでに時間がかかるホストとの通信では、しばしば TCP long ack time イベントが発生します。

ローカルなネットワーク間での通信でも、ネットワークが高トラフィック状態であったり、ホストの負荷が高くて処理能力が低下しているときにはイベントが発生する可能性があります。

どのくらい遅れてとどいたパケットに対して TCP long ack time イベントを発生させるかは、ユーザーが設定できます。詳しくは「10.3.1　モニタイベントの設定」 (244 ページ) を参照してください。

10.7.11 TCP fragmented TCP data

IP 層でフラグメント化された TCP パケットを検出します。

送った TCP パケットの長さよりも、経路の MTU (最大転送ユニット) が短いときにフラグメント化が起きて、イベントが発生します。

RFC では TCP のコネクションを作成するときに、**パス MTU** (パケットが流れる経路上の最小の MTU) を調べるように規定されています。 MTU を調べることができて、パケット長が MTU 以下になるように TCP 層で調整されたときには、フラグメント化は起きません。 MTU が調べられずデフォルトの MTU (576 バイト) を使ったときや、 TCP 層でパケット長を調整しないときには、パケットがフラグメント化される可能性があります。

MTU は通常は MAC 層のメディアの種類によって決まりますが、ルーターの設定によって MTU を調整することもできます。たとえば、音声などをリアルタイムで配送するとき、 1000 バイトを超えるような比較的長いデータのパケットと比較的短い音声のパケットが同じ経路にあると、長いパケットによって音声パケットの配送が遅延し、リアルタイムに音声を再構成できなかったり、雑音が混ざったりします。この問題の対策として、長いパケットを 2 ～ 3 百バイト程度の短いパケットにフラグメント化して、リアルタイム性を損なわないように設定できるルーターもあります。

一般にフラグメント化が発生すると、次のような理由から通信の効率が低下します。

- フラグメント化する処理のオーバーヘッド
- フラグメント化したパケットからもとのパケットを再構成する処理のオーバーヘッド
- フラグメント化されたパケットの一部を失った場合には、もとのパケット全体を再送する

DoS (Denial of Service) 攻撃の手法の一つに、もとのパケットを再構成できないような偽のフラグメントを送り、攻撃対象のホストを混乱させ、処理能力を低下させたり場合によってはクラッシュさせるものがあります。

このイベントが高い頻度で (1 秒間に 1 回から数回以上) 連続的に発生するようであれば、 DoS 攻撃を受けている可能性があります。

特定の相手先や経路に対して定常的に TCP fragmented TCP data イベントが発生する場合には、通信性能が低下している可能性があります。

フラグメント化が起きる経路を通る場合、パケット長が MTU 以上で ‘‘Don’t Fragment’’ ビットが ON のパケットは破棄されます。このような場合は正常に通信できなくなります。

10.7.12 TCP checksum error

TCP ヘッダーのチェックサムが誤っているパケットを検出します。

TCP checksum error の原因として、次のことが考えられます。

- パケットの破損
- TCP チェックサム・オフロード機能を持ったネットワークインタフェースカードを使用している

発信元のホストは、 TCP パケットのヘッダーとデータ全体のチェックサム値を計算して、TCP ヘッダーの Checksum フィールドに設定します。受信先のホストはパケットを受け取るとチェックサム値を計算して Checksum フィールドの値と照合し、チェックサム値が一致しなければそのパケットは破損しているとみなして破棄されます。パケットの破棄が頻繁に発生すると、通信性能が低下します。

TCP チェックサム値の照合とパケットの破棄は、通常は TCP 層で行われますが、 TCP チェックサム値を照合する機能を持つネットワークインタフェースカードもあります。ネットワークインタフェースカードの TCP チェックサム値の照合機能を有効にしているとき、 TCP ヘッダーの Checksum フィールドには正しいチェックサム値が設定されていない場合があり、イベントが発生します。

10.7.13 TCP ACK flag not set

一番最初の SYN パケット以外のパケットで ACK ビットが OFF のパケットを検出します。

ACK ビットは Acknowledgment Number フィールドに確認応答番号が設定されているかどうかを示します。 ACK ビットも Acknowledgement Number フィールドも TCP の固定ヘッダーの一部に含まれているため、余分なデータを必要としません。そこで、通常はデータとともに ACK もつけたパケットを送るため、いったん TCP の接続が確立すると ACK ビットは ON になります。

10.7.14 TCP connection timeout

TCP の接続を確立するために SYN パケット (SYN ビットが ON のパケット) を送ったあと、応答パケットが送られないまま一定時間が経過したか、または、 SYN パケットに対して、応答の ACK パケットが返されたが、その次の ACK パケットが返されないまま一定時間が経過したことを検出します。

TCP connection timeout イベントが発生する状況として、次のような場合が考えられます。

- 接続先のホストが停止している、またはネットワークが切断している
- 経路の途中でパケットが破棄された
- 接続先のホストやネットワークの性能が低下していて、パケットの配送が遅れた

10.7.15 TCP connection table threshold over

TCP ステータス情報のエントリ数が指定した数を超えたことを検出します。

TCP ステータス情報のウィンドウには、現在、接続しようとしていたり、接続中の通信、または、先ほどまで接続していた通信などの状態の一覧が表示されます。

TCP connection table threshold over イベントは、一覧に表示されているエントリ数 (接続の数) が指定した値を超えたときに発生します。

このイベントは、ネットワークサービスの利用が増えたり、 DoS 攻撃などで TCP によるアクセスが急激に増えたことを知るために用意されています。エントリ数がどれだけの数になったときにイベントを発生させるかは、ユーザーが設定できます。詳しくは「10.3.1　モニタイベントの設定」 (244 ページ) を参照してください。

10.7.16 UDP checksum error

UDP ヘッダーのチェックサムが誤っているパケットを検出します。

UDP checksum error の原因として、次のことが考えられます。

- パケットの破損
- UDP チェックサム・オフロード機能を持ったネットワークインタフェースカードを使用している

発信元のホストは必要があれば、 UDP パケットのヘッダーとデータ全体のチェックサム値を計算して、 UDP ヘッダーの Checksum フィールドに設定します。受信先のホストは必要があれば、受け取った UDP パケットのチェックサム値を計算して Checksum フィールドの値と照合し、チェックサム値が一致しなければそのパケットは破損しているとみなして UDP 層で破棄されます。パケットの破棄が頻繁に発生すると、通信性能が低下します。

UDP チェックサム値の照合とパケットの破棄は、通常は UDP 層で行われますが、 UDP チェックサム値を照合する機能を持つネットワークインタフェースカードもあります。ネットワークインタフェースカードの UDP チェックサム値の照合機能を有効にしていると、 UDP ヘッダーの Checksum フィールドに正しいチェックサム値が設定されない場合があり、イベントが発生します。

IPv4 の UDP ではチェックサムの照合は必須ではありません。多くのホストではチェックサムが無効になっていて、必ずしもチェックサムが照合されるとは限りません。

10.7.17 ICMP destination unreachable

ICMP の destination unreachable (宛先到達不能) パケットを検出します。

ICMP は、ネットワークの接続状態を調べるために使われるプロトコルです。パケットが受信先のホストまで配送できなかったときや、 UDP パケットの受信先のポートが閉じていたときに、配送経路の途中のルータや受信先のホストが、発信元のホストに destination unreachable パケットを送り返します。

このイベントは次のような状況のときに発生します。

- 動作していない UDP のサービスを使おうとした
- ネットワークが切断しているなど、到達できないホストと通信しようとした
- セキュリティ等の目的でルータにパケットのフィルタが設定されており、パケットを配送できなかった

10.7.18 ICMP checksum error

ICMP ヘッダーのチェックサムが誤っているパケットを検出します。

ICMP checksum error の原因として、パケットの破損が考えられます。

発信元のホストは、 ICMP パケットのヘッダーとデータ全体のチェックサム値を計算して、 ICMP ヘッダーの Checksum フィールドに設定します。受信先のホストはパケットを受け取るとチェックサム値を計算して Checksum フィールドの値と照合し、チェックサム値が一致しなければそのパケットは破損しているとみなして破棄されます。パケットの破棄が頻繁に発生すると、通信性能が低下します。

10.7.19 ICMPv6 destination unreachable

ICMPv6 の destination unreachable (宛先到達不能) パケットを検出します。

ICMPv6 は、ネットワークの接続状態を調べるために使われるプロトコルです。パケットが受信先のホストまで配送できなかったときや、 UDP パケットの受信先のポートが閉じていたときに、配送経路の途中のルータや受信先のホストが、発信元のホストに destination unreachable パケットを送り返します。

このイベントは次のような状況のときに発生します。

- 動作していない UDP のサービスを使おうとした
- ネットワークが切断しているなど、到達できないホストと通信しようとした
- セキュリティ等の目的でルータにパケットのフィルタが設定されており、パケットを配送できなかった

10.7.20 ICMPv6 checksum error

ICMPv6 ヘッダーのチェックサムが誤っているパケットを検出します。

ICMPv6 checksum error の原因として、パケットの破損が考えられます。

発信元のホストは、 ICMPv6 パケットのヘッダーとデータ全体、および IPv6 の擬似ヘッダーのチェックサム値を計算して、 ICMPv6 ヘッダーの Checksum フィールドに設定します。受信先のホストはパケットを受け取るとチェックサム値を計算して Checksum フィールドの値と照合し、チェックサム値が一致しなければそのパケットは破損しているとみなして破棄されます。パケットの破棄が頻繁に発生すると、通信性能が低下します。

10.7.21 IP fragment timeout

IP 層で IPv4 パケットがフラグメント化されている場合に、一定時間内に届かなかったフラグメントがあることを検出します。

IP fragment timeout イベントの原因として、次のことが考えられます。

- 一部のフラグメントが破棄された
- 一部のフラグメントの到着が遅れた
- DoS (Denial of Service) 攻撃

受信先のホストはパケットが IP 層でフラグメント化されているとき、届いたフラグメントをもとにパケットを再構成します。このとき、到着していないフラグメントが 1 つでもあれば、完全なパケットを再構成できないため、届いているフラグメントすべてを破棄します。この状態が頻繁に起これば通信性能が低下します

フラグメント攻撃として知られている DoS 攻撃手法では、フラグメント化されたパケットを攻撃対象のホストに大量に送ります。 OS の種類によってはフラグメント攻撃に対して脆弱で、OS の処理能力が極端に低下したり、場合によってはクラッシュすることがあります。このイベントが高い頻繁で (1 秒間に数回以上) 連続的に発生するようであれば、フラグメント攻撃を受けている可能性があります。

フラグメント化された IPv6 パケットの一部のフラグメントが一定時間内に届かなかったときには、 IPv6 fragment timeout イベントが発生します。詳しくは「IPv6 fragment timeout」を参照してください。を参照してください。

10.7.22 IP fragment error

IP 層で IPv4 パケットがフラグメント化されている場合に、フラグメントから再構成したパケットが不完全であることを検出します。

このイベントが発生する原因として、次のことが考えられます。

- 一部のフラグメントが破棄された
- DoS (Denial of Service) 攻撃

受信先のホストはパケットが IP 層でフラグメント化されているとき、届いたフラグメントをもとにパケットを再構成します。このとき、到着していないフラグメントが 1 つでもあれば、完全なパケットを再構成できないため、届いているフラグメントすべてを破棄します。この状態が頻繁に起これば通信性能が低下します

IPv6 パケットのフラグメントから再構成したパケットが不完全な場合には、 IPv6 fragment error イベントが発生します。詳しくは「IPv6 fragment error」を参照してください。

10.7.23 IP header checksum error

IPv4 ヘッダーのチェックサムが誤っているパケットを検出します。

IP header checksum error の原因として、次のことが考えられます。

- パケットの破損
- IP チェックサム・オフロード機能を持ったネットワークインタフェースカードを使用している

発信元のホストは、 IPv4 パケットのヘッダーのチェックサム値を計算して、 IPv4 ヘッダーの Header Checksum フィールドに設定します。受信先のホストはパケットを受け取るとチェックサム値を計算して Header Checksum フィールドの値と照合し、チェックサム値が一致しなければそのパケットは破損しているとみなして破棄されます。パケットの破棄が頻繁に発生すると、通信性能が低下します。

チェックサム値の照合とパケットの破棄は、通常は IP 層で行われますが、 IP チェックサム値を照合する機能を持つネットワークインタフェースカードもあります。ネットワークインタフェースカードの IP チェックサム値の照合機能を有効にしていると、 IP 層のレベルではパケット Header Checksum フィールドに正しいチェックサム値が設定されていない場合があり、イベントが発生します。

10.7.24 IP invalid IP length

IPv4 ヘッダーの Total Length フィールド値と実際のデータ長が異なるパケットを検出します。このイベントは IPv4 でのみ発生します。

送信元はヘッダーとデータを含めた IPv4 パケット全体の長さを IPv4 ヘッダーの Total Length フィールドに設定します。通常の正常な通信では、 Total Length フィールド値と一致しないパケットが送信されることはありません。

このイベントが発生する原因としてパケットの破損が考えられます。

IPv4 パケット全体の長さが Total Length フィールド値よりも短いパケットは、エラーパケットとして IP 層によって破棄されます。 IPv4 パケットが頻繁に破棄されれば、通信効率が低下します。

このイベントが頻繁に発生するようであれば、ネットワーク機器の障害やネットワークケーブ

ルの接触不良の可能性もあります。

10.7.25 IP duplicate IP address

異なる MAC アドレスに同じ IPv4 アドレスが付けられていることを検出します。

IP duplicate IP address イベントが発生する状況として、次のような場合が考えられます。

- IP アドレスの設定誤りで、複数台のホストに同じ固定 IP アドレスが同時に割り当てられた
- DHCP を使っているとき、複数台のホストに同じ動的 IP アドレスが同時に、または異なった時間帯で割り当てられた
- ダイアルアップ接続により、複数台のホストに同じ動的 IP アドレスが同時に、または異なった時間帯で割り当てられた
- クラスタシステムで、複数のネットワークインタフェースに同一 IP アドレスを割り当てている
- IP アドレスのなりすまし攻撃

手動で固定 IP アドレスを割り当てたり、 DHCP やダイアルアップ接続で動的な IP アドレスを割り当てるときに、設定ミスなどによって 2 台以上のホストに同時に同一の IP アドレスを割り当てると、 IP アドレスの重複が発生します。同一 IP アドレスのホストが、直接通信可能なネットワーク上に 2 台以上存在する状況では、ホスト間でパケットの奪い合いが発生し、正しく通信できません。

DHCP やダイアルアップ接続では、 2 台以上のホストに対して重ならない時間帯で同じ IP アドレスが割り当てられることがあります。たとえば、ダイアルアップ接続でインターネットにつながっていたホストが接続を切ると、そのホストが使用していた IP アドレスは解放され、後でダイアルアップ接続した別のホストに先ほどと同じ IP アドレスが割り当てられることがあります。この場合にも、 IP duplicate IP address イベントが発生します。

クラスタシステムとは、複数台のホストや内部的に多重化されたホストが協調して動作するシステムで、複数のホストやネットワークインタフェースに同一の IP アドレスを割り当てるものがあります。電子商取引や検索サービスを提供している WWW サーバーでは、フェイルオーバーやロードバランスのためにクラスタシステムの採用が増えています。

悪意のユーザーが**なりすまし攻撃**を行う目的で、意図的に既存のホストの IP アドレスを使うこともあります。 IP アドレスを詐称したホストがネットワーク上に存在した場合にも、 IP duplicate IP address イベントが発生します。

なりすまし攻撃については、「10.6　セキュリティに関する情報」 (261 ページ) の「なりすまし攻撃」を参照してください。

10.7.26 IPv6 fragment timeout

IP 層で IPv6 パケットがフラグメント化されている場合に、一定時間内に届かなかったフラグメントがあることを検出します。

IPv6 fragment timeout イベントの原因として、次のことが考えられます。

- 一部のフラグメントが破棄された
- 一部のフラグメントの到着が遅れた

受信先のホストはパケットが IP 層でフラグメント化されているとき、届いたフラグメントをもとにパケットを再構成します。このとき、到着していないフラグメントが 1 つでもあれば、完全なパケットを再構成できないため、届いているフラグメントすべてを破棄します。この状態が頻繁に起これば通信性能が低下します

フラグメント化された IPv4 パケットの一部のフラグメントが一定時間内に届かなかったときには、 IP fragment timeout イベントが発生します。詳しくは「IP fragment timeout」を参照してください。

10.7.27 IPv6 fragment error

IP 層で IPv6 パケットがフラグメント化されている場合に、フラグメントから再構成したパケットが不完全であることを検出します。

このイベントの原因として、一部のフラグメントが破棄されたことが考えられます。

受信先のホストはパケットが IP 層でフラグメント化されているとき、届いたフラグメントをもとにパケットを再構成します。このとき、到着していないフラグメントが 1 つでもあれば、完全なパケットを再構成できないため、届いているフラグメントすべてを破棄します。この状態が頻繁に起これば通信性能が低下します

IPv4 パケットのフラグメントから再構成したパケットが不完全な場合には、 IP fragment error イベントが発生します。詳しくは「IP fragment error」を参照してください。

10.7.28 MAC traffic under threshold

MAC 層で計測した 1 秒あたりのバイト数が指定した閾値を越えたことを検出します。

このイベントは通信量が閾値を越えていた期間の最後の時点で発生します。

MAC traffic under threshold イベントは、ネットワークが高トラフィック状態にあることをユーザーに知らせるために用意されています。通常は、 MAC 層で計測した 1 秒あたりのバ

イト数は、 MAC 層の理論的な最大転送バイト数を超えることはありません。理論的な MAC 層の最大転送速度がわかっている場合には、それよりも小さな値を閾値として設定してください。

一般に、 Ethernet のような CDMA/CD 方式では、転送路の使用率が 20% を超えると、コリジョンの頻度が増えネットワークの性能 (転送率) が急激に低下します。 Full duplex のスイッチングハブを利用している場合などでは、コリジョンが発生する頻度が低いため、より大きな使用率でも安定して通信できます。

MAC traffic under threshold イベントは、 MAC traffic over threshold イベントと同じ状況で発生しますが、イベントを発生するタイミングは閾値を越えていた通信量が閾値以下になった時点です。

10.7.29 MAC traffic over threshold

MAC 層で計測した 1 秒あたりのバイト数が指定した閾値を越えたことを検出します。このイベントは通信量が閾値を越えた時点で発生します。

MAC traffic over threshold イベントは、 MAC traffic under threshold イベントと同じ状況で発生しますが、イベントを発生するタイミングは通信量が閾値を越えた直後です。

10.7.30 NIC monitor reset

ネットワークインタフェースカード (NIC) に対するモニターがリセットされたことを検出します。

このイベントは、ユーザーがモニタリセットを実行したときに発生します。

10.7.31 NIC driver started

ネットワークインタフェースカード (NIC) のドライバが開始したことを検出します。

このイベントは、キャプチャ部が起動したときや、 OS の機能を使って無効になっていた NIC を有効にしたときになどに発生します。

10.7.32 NIC driver terminated

ネットワークインタフェースカード (NIC) のドライバが終了したことを検出します。

このイベントは、 OS の機能を使って NIC を無効にしたときなどに発生します。

10.7.33 NIC link speed changed

ネットワークインタフェースカード (NIC) のリンクスピードが変化したことを検出します。

OS の機能を使って NIC のリンクスピードを変更したときや、異なったリンクスピードに自動的に対応するように設定された NIC に対して、接続先の HUB を変えたときなどに、 NIC link spped changed イベントが発生します。

10.7.34 NIC link up

ネットワークインタフェースカード (NIC) のリンクアップを検出します。

このイベントは、ネットワークケーブルを接続したとき、あるいはネットワークケーブルの接続先の HUB やスイッチの電源を入れて、 NIC がネットワークにつながったときなどに発生します。

10.7.35 NIC link down

ネットワークインタフェースカード (NIC) のリンクダウンを検出します。

このイベントは、ネットワークケーブルをはずしたとき、あるいはネットワークケーブルの接続先の HUB やスイッチの電源を切って、 NIC がネットワークから切り離されたときなどに発生します。

10.7.36 NIC capture file output started

連続キャプチャを開始した後に、初めてパケットをキャプチャしたことを検出します。

連続キャプチャフィルタ、および連続キャプチャ開始トリガを設定していないときには、連続キャプチャ開始の操作を行ったあと、初めてパケットがネットワークを流れたときに NIC capture file output started イベントが発生します。

連続キャプチャフィルタ、または連続キャプチャ開始トリガを設定しているときには、連続キャプチャ開始の操作を行ったあと、フィルタで設定した条件を満たすパケットが初めてネットワークを流れたときに NIC capture file output started イベントが発生します。ただし、フィルタで設定したパケットが流れないまま連続キャプチャ停止操作を行ったときには、停止操作を行った時点で NIC capture file output started イベントと NIC capture file output stopped イベントが発生します。

10.7.37 NIC capture file output stopped

連続キャプチャが停止したことを検出します。

連続キャプチャ停止の操作を行ったとき、およびディスクの空き容量が設定値以下になって自動的に連続キャプチャの出力が停止したときに NIC capture file output stopped イベントが発生します。

連続キャプチャ停止トリガを設定しており、連続キャプチャ開始トリガを設定していないときには、連続キャプチャ停止トリガで設定した条件を満たすパケットがネットワークを流れた時点で連続キャプチャが停止し、 NIC capture file output stopped イベントが発生します。

10.7.38 NIC capture file roll

連続キャプチャを行っているときに、次のファイルを書き出し始めたことを検出します。

10.7.39 NIC packet send start

このイベントは、トラフィックジェネレータがパケットの送信を開始したことを検出します。

10.7.40 NIC packet send stop

このイベントは、トラフィックジェネレータがパケットの送信を停止したことを検出します。

10.7.41 NIC user filter

ユーザーがイベントフィルタで定義したイベントを検出します。

特定のパケットが流れたときにイベントを発生させたり、頻度が高い場合だけイベントを発生させることができます。

11章

オプションの設定

オプションは、「オプション設定」ダイアログで設定します。「オプション設定」ダイアログを開く方法は 2 通りあります。

- コモンツールバーの**オプション設定**ボタン() をクリックします。
- メインウィンドウの**設定(O)** メニューから**オプション設定(O)**. . . を選びます。

「オプション設定」ダイアログには、次に示すオプションを設定するためのパネルがあります。

- 基本
  - キャプチャ
  - デコード
  - デコードヒント
  - デコードエキスパート
  - ホスト名
  - モニタ
  - グラフ
  - グラフの色
  - SOCKS
  - その他
- VoIP
  (ASTEC Eyes *for* VoIP のオプションです。『ASTEC Eyes *for* VoIP』をご覧ください。)
  - R 値測定 (パラメータ)
  - R 値測定 (コーデック)
  - 音声の再生

ダイアログの左側にあるツリーの中の設定したい項目をクリックします。それぞれのオプションを設定するパネルが開きます。

オプションをすべて設定し終わったら、**適用(A)** ボタンまたは **OK** ボタンをクリックします。変更したオプションが一度に適用されます。 **OK** ボタンをクリックした場合は、「オプション設定」ダイアログが閉じます。

「オプション設定」ダイアログで設定する情報のうち、ローカルホストに関するものは、設定ファイルに保存できます。詳しくは「11.11　設定情報を保存する」 (318 ページ) を参照してください。

11.1 キャプチャのオプションを設定する

キャプチャのオプションを設定するパネルは、図 11-1 のようになっています。

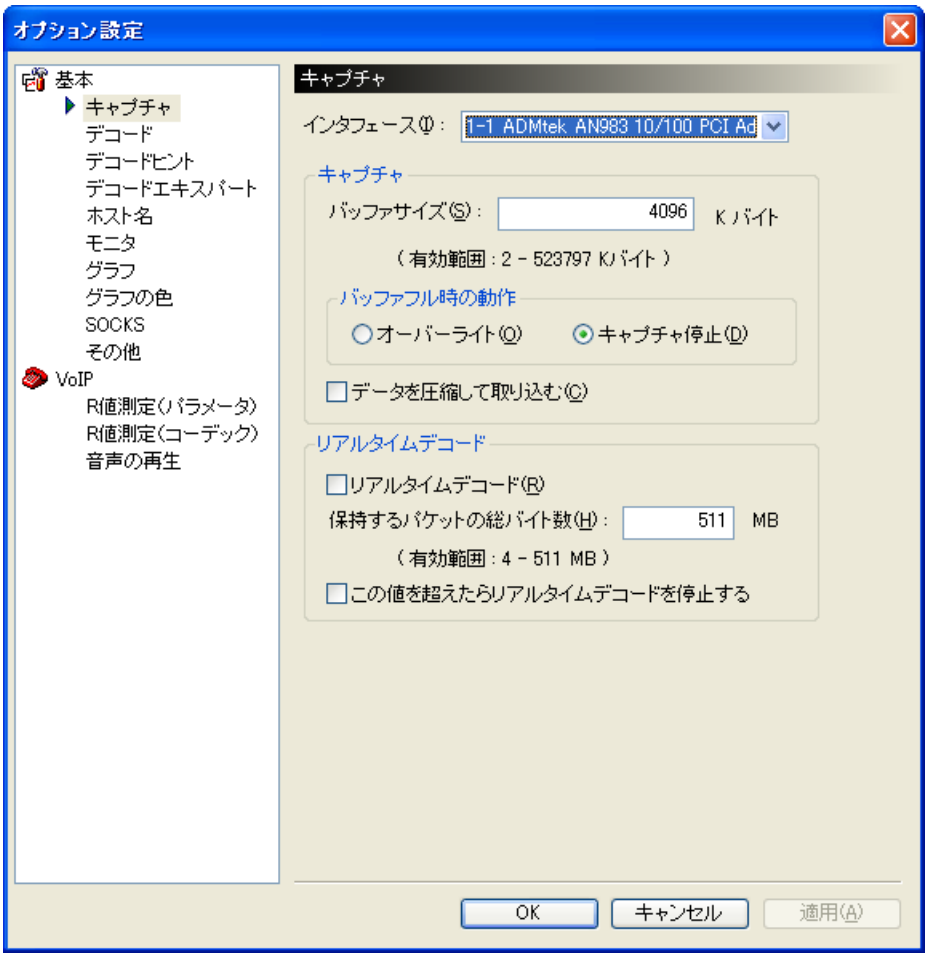


図 11-1: 「オプション設定」ダイアログ (「キャプチャ」のパネル)

1. **インタフェース(I)** のドロップダウンリストボックスでインタフェースを選びます。
   キャプチャのオプションはネットワークインタフェースごとに設定します。
2. バッファサイズ、バッファフル時の動作、およびリモートモジュールでキャプチャしたデータを転送するときに圧縮するかどうかを設定します。

バッファサイズ　キャプチャバッファの大きさを K バイト (1024 バイト) 単位で指定します。デフォルトのサイズは 4096 K バイトです。

バッファフル時　キャプチャバッファがいっぱいになったときの動作を指定します。

オーバーライトを選ぶと、バッファの中の最も古いデータから上書きします。

キャプチャ停止を選ぶと、自動的にキャプチャを停止します。

デフォルトの動作は、「キャプチャ停止」です。

データを圧縮して取り込む(C)

リモートモジュールのインタフェースでキャプチャしたデータをデコードする場合、キャプチャしたデータはローカルホストまで転送されます。転送量を減らすために、キャプチャしたデータを圧縮できます。圧縮したい場合は、チェックを付けます。

バッファサイズに指定できる値は、最小値が 2K バイト、最大値は実メモリサイズの 1/4 までです。リモートモジュールのインタフェースの場合は、最大値はリモートモジュールが動作している計算機の実メモリサイズの 1/4 になります。
インタフェースのドロップダウンリストボックスでインタフェースを選ぶと、設定できるサイズの範囲が表示されます。

---

3. ローカルホストの場合は、リアルタイムデコードを行うかどうか、リアルタイムデコードビューのパケットサイズ、バッファフル時の動作を設定します。

リアルタイムデコード

チェックを付けるとリアルタイムデコードを行います。チェックを外すといったんキャプチャを停止してからデコードビューを表示するモードになります。

保持するパケットの総バイト数

リアルタイムデコードビューに保持するパケットサイズを、 M バイト (1024K バイト) 単位で指定します。

この値を超えたらリアルタイムデコードを停止する

チェックを付けると、保持するパケットの総バイト数を超えてデコードしようとしたときに、リアルタイムデコードを中止します。チェックを外すと、古いデータを新しくデコードしたデータで上書きします。

保持するパケットの総バイト数で指定できる値は、最小値が 4M バイト、最大値は実メモリサイズの 1/4 までです。

リモートホストでは、リアルタイムデコードは実行できません。

11.2 デコードのオプションを設定する

デコードのオプションを設定するパネルは、図 11-2 のようになっています。

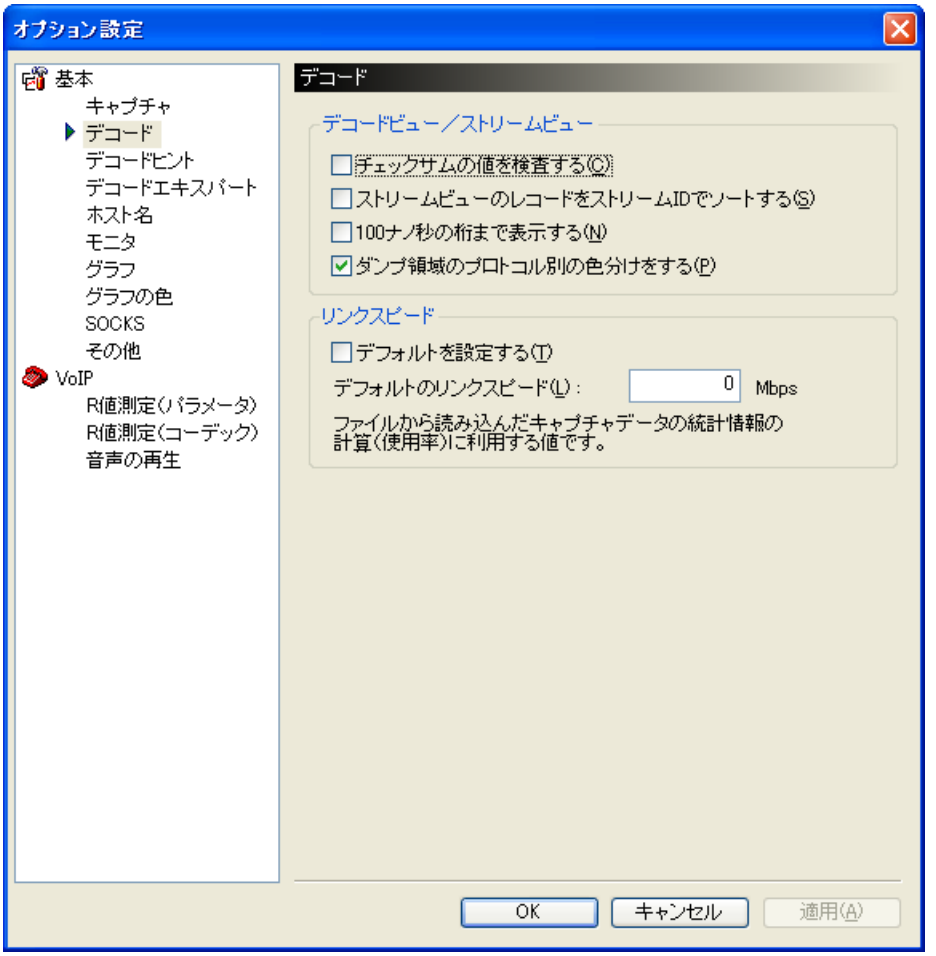


図 11-2: 「オプション設定」ダイアログ (「デコード」のパネル)

デコードのオプションには、次のようなものがあります。

- **チェックサムの値を検査する(C)**†
  チェックを付けておくと、デコード時に IPv4、 UDP および TCP のチェックサム値の検

査を行います。詳しくは「11.2.1　チェックサムの検査」 (288 ページ) を参照してください。

- **ストリームビューのレコードをストリーム ID でソートする(S)**†
  チェックがついていない場合、ストリームビューに表示されるレコードは、レコードを構成するパケットの到着時刻順に並びます (パケットの到着が前後した場合を除く)。
  チェックを付けておくと、ストリーム ID ごとにまとめて表示します。同じストリーム ID 内では、レコードを構成するパケットの到着順に並びます。
- **100 ナノ秒の桁まで表示する(N)**
  チェックがついていない場合、デコードビューまたはストリームビューの時刻カラムに表示する値は、ミリ秒の単位まで表示します。
  チェックが付いている場合、 100 ナノ秒の単位まで表示します。
- **ダンプ領域のプロトコル別の色分けをする(P)**
  チェックを付けておくと、ダンプ領域の背景色をプロトコル別にデコード結果領域と同じ色にします。
- **リンクスピード**
  デコードしたデータを基に表示した「MAC 層トラフィック」のウィンドウでは、 Y 軸の単位を「使用率」に変えるとき、リンクスピードが分からないことがあります。それぞれのキャプチャファイルに対してリンクスピードを指定できますが、指定しなかった場合に使うデフォルト値を設定しておくことができます。
  デフォルト値を設定するには、**デフォルトを設定する(T)** にチェックを付け、**デフォルトのリンクスピード(L)** にリンクスピードを入力します。
  それぞれのキャプチャファイルについてリンクスピードを設定する方法については、「6.7.3 データをキャプチャしたときのネットワーク使用率を調べる」 (144 ページ) を参照してください。

---

†の付いているオプションを、すでに表示されているデコードビューおよびストリームビューに反映させるには、再デコードする必要があります。
再デコードするには、

- デコードビューのツールバーの**再デコード**ボタン( ) をクリックするか、
- デコードビューまたはシーケンスモードでないストリームビューを右クリックしてポップアップメニューを開き、**再デコード(Q)** を選びます。

11.2.1 チェックサムの検査

ASTEC Eyes は、**チェックサムの値を検査する(C)** にチェックがついている場合、 IPv4、UDP、および TCP プロトコルのデータをデコードする際に、パケットのデータからチェックサムの値を再計算し、チェックサムのフィールドの値と照合してデータの誤りを検出します。誤りが見つかった場合は、上位層のプロトコルのデコードは行いません。

ネットワークインタフェースカード (NIC) の種類によっては、 NIC (ハードウェア) がチェックサムを計算するものがあります。そのような NIC をインストールしてあるホストで動作している ASTEC Eyes またはリモートモジュールでキャプチャを行うと、その NIC から発信するパケットについては、チェックサムを計算する前のパケットがキャプチャされるため、デコードするとエラーになってしまいます。

このような NIC をお使いの場合は、**チェックサムの値を検査する(C)** からチェックを外します。チェックサム値の照合を行わずにアプリケーション層までデコードできます。

チェックサムの値を検査する(C) からチェックを外すと、誤りを含むパケットを検出することはできなくなります。

11.3 デコードヒントを設定する

デコードヒントを設定するペインは、図 11-3 のようになっています。

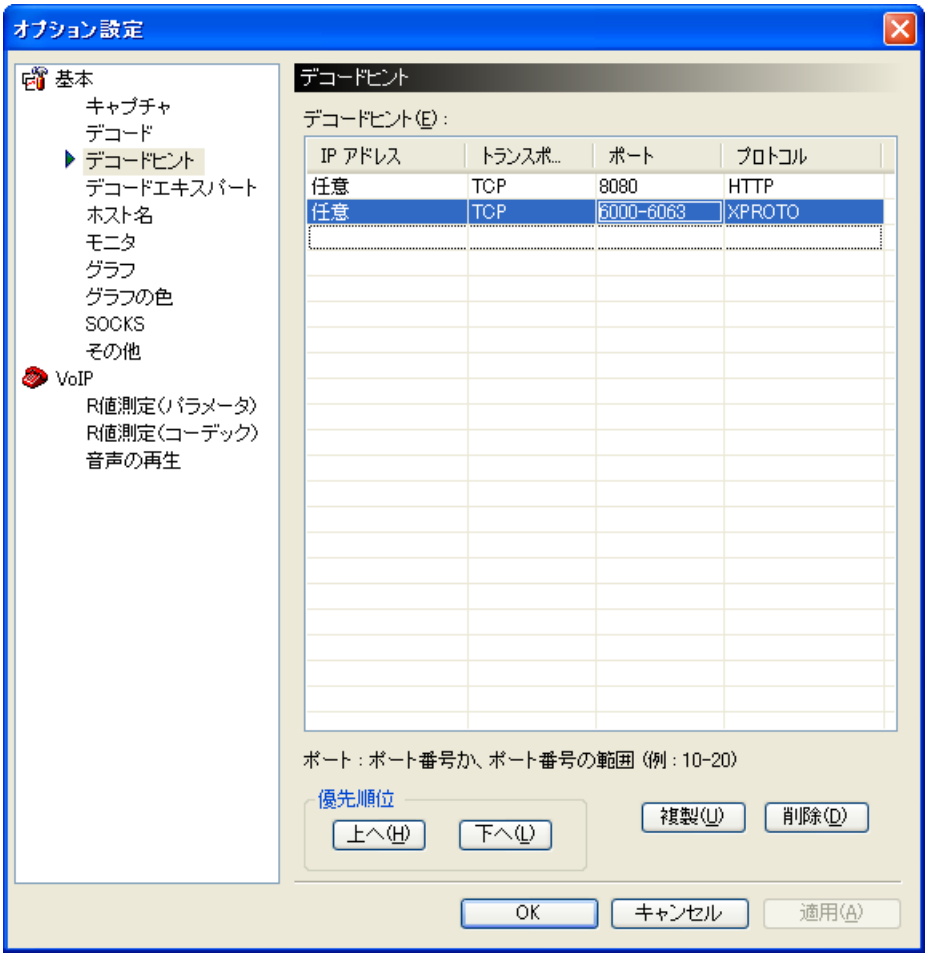


図 11-3: 「オプション設定」ダイアログ (「デコードヒント」のパネル)

TCP または UDP の上位層のプロトコルのうち、プロキシサーバーの設定によって Well known ポートとは異なるポートを使っているプロトコルや、 Well known ポートを持たないプロトコルは、正しくデコードできなかったり、「IP 層トラフィック」のウィンドウに「Unknown TCP Protocol」または「Unknown UDP Protocol」という表示になったりします。

そのような場合はデコードヒントを設定します。

デコードヒントに必要な情報は、 IP アドレス、トランスポート層、ポート番号、プロトコルです。複数のデコードヒントを登録できます。 1 行につきデコードヒントを 1 つ設定します。

IP アドレス ドロップダウンコンボボックスになっています。このリストには、**任意**という項目があります。すべての IP アドレスを対象とするデコードヒントを設定する場合は、**任意**を選びます。特定の IP アドレスを対象とするデコードヒントを設定する場合は、 IP アドレス (IPv4 または IPv6 アドレス) を入力します。

トランスポート層 ドロップダウンリストボックスから「UDP」、「TCP」、または「UDP or TCP」のいずれかを選びます。

ポート ポート番号またはポート番号の範囲を入力します。範囲を指定する場合は、'-' (ハイフン) でつなぎます (例 `6000-6063`)。

デコードビューおよびストリームビューのサマリ領域のポート番号が表示されている行をドラッグして、ドロップすることもできます。

プロトコル ドロップダウンコンボボックスになっています。リストには ASTEC Eyes がサポートするアプリケーションプロトコルの一覧があります。リストからプロトコルを選ぶか、プロトコル名をキー入力します。

図 11-3 の例では、任意のアドレスの TCP のポート `8080` 番を使っているパケットは `HTTP` プロトコルのデータとして表示し、デコードします。

11.3.1 デコードヒントを入力する

以下に、デコードヒントを入力する手順を示します。

1. デコードヒントが設定されていない一番上の行をクリックするか、カーソルキー (**<↑>** 、**<↓>**) を押して、デコードヒントが設定されていない行を選びます。
   選んだ行が青く反転します。マウスでクリックした場合は、クリックした位置のカラムが白い枠で囲まれます。カーソルキーを押した場合は IP アドレスのカラムが白い枠で囲まれます。
2. 値を設定したいカラムをクリックします。クリックしたカラムが入力できる状態になります。
   キーボードで操作する場合、入力できる状態になっていないときは、 **<←>** または **<→>** キーで入力したいカラムまで白い枠を移動し、 **<F2>** キーを押します。入力できる状態に

なっているときは、 **<Tab>** キーまたは **<Shift-Tab>** キーを押して入力したいカラムまで移動します。

3. 値を入力します。
4. すべてのカラムに適切な値を入力し終わるまで、 2 と 3 の手順を繰り返します。

入力済みの行を選んで**複製(U)** ボタンをクリックすると、同じ値のデコードヒントが複製され、選んだ行の下に追加されます。

ドラッグアンドドロップ操作で入力する

次の項目をドラッグし、デコードヒントを入力する表の領域にドロップすれば、デコードヒントに必要な情報を入力できます。

- デコードビューのサマリ領域の IP アドレスが表示されている行
- ストリームビューのサマリ領域の行
  IP アドレスカラム、トランスポート層カラム、ポートカラムに、パケットまたはレコードから得られた値が入力されます。ポート番号が Well known ポート番号であるか、すでにデコードヒントに登録されているポート番号である場合は、プロトコル名も入力されます。
- 「IP 層発信元毎のトラフィック」のウィンドウのグラフアイテム
- 「IP 層受信先毎のトラフィック」のウィンドウのグラフアイテム
- 「IP 層ホストペア毎のトラフィック」のウィンドウのグラフアイテム
- IP アドレス表の行
- IP 層アドレス帳の行
  IP アドレスが入力されます。「IP 層ホストペア毎のトラフィック」のウィンドウからドラッグした場合は、 2 つの IP アドレスがひとつずつ別々の行に入力されます。
- 「IP 層プロトコル毎のトラフィック」のウィンドウのグラフアイテム
  プロトコル名が入力されます。

コピーアンドペースト操作で入力する

次のウィンドウの白い枠で囲まれているカラムの文字列をコピーして、デコードヒントを入力する表のカラムに貼り付けることができます。

- 表形式のモニタウィンドウ
- IP 層アドレス帳
- デコードビューおよびストリームビューのサマリ領域

コピーアンドペーストを使うには、次のようにします。

1. 上記のウィンドウでコピーしたいカラムを選びます。
2. メインウィンドウの**編集(E)** メニューから**コピー(C)** を選ぶか、 **<Ctrl-C>** キーを押します。
3. 「オプション設定」ダイアログをアクティブにします。
4. 貼り付けたいカラムを入力できる状態にします。
   入力できる状態にするには、
   - 目的のカラムを 2 回クリック (ダブルクリックではありません) するか、
   - 矢印キー (**<↑>**、 **<↓>**、 **<←>**、 **<→>**) を使って、白い枠を目的のカラムまで移動し、**<F2>** キーを押します。
5. 右クリックしてポップアップメニューを開き、**貼り付け(P)** を選ぶか、 **<Ctrl-V>** キーを押します。

11.3.2 デコードヒントの優先順位

デコードヒントには、優先順位があります。たとえば、次のようなデコードヒントが設定されている場合を考えます。

IP アドレス	トランスポート層	ポート	プロトコル
11.11.11.11	TCP	1080	SOCKS
22.22.22.22	TCP	1080	DNS

11.11.11.11 アドレスの TCP の 1080 番ポートから 22.22.22.22 アドレスの TCP の 1080 番ポートへ送られたパケットは DNS として解析するべきでしょうか。それとも、 SOCKS として解析するべきでしょうか。

ASTEC Eyes では、テーブルの上の行の方が高い優先順位を持っています。そのため、上の例では SOCKS として解析します。

優先順位を変えるには、

1. 優先順位を変えたい行をクリックします。
2. **上へ(H)** ボタンまたは**下へ(L)** ボタンをクリックします。

11.3.3 デコードヒントを削除する

デコードヒントを削除するには、

1. 削除したい行をクリックします。
2. **削除(D)** ボタンをクリックします。

11.3.4 デコードヒントの設定例

発信元のポートも受信先のポートも Well known ポートになることがあります。 ASTEC Eyes がどちらのプロトコルと判定するかは、ポート番号の大小に依存します。

たとえば、 TCP ポート 53 (DNS) と 1080 (SOCKS) の間で SOCKS のパケットがやり取りされる場合、 ASTEC Eyes は小さい方のポート番号の方を優先して、 DNS プロトコルのパケットがやり取りされているものと判定します。

このような問題は、デコードヒントを設定することで回避できます。この例では、特定アドレスの TCP ポート 1080 が SOCKS であるというデコードヒントを設定するのが適切です。特定アドレスの TCP ポート 53 が SOCKS であるというデコードヒントは適切ではありません。

11.4 デコードエキスパートのオプション設定をする

デコードエキスパートのオプションを設定するペインは、図 11-4 のようになっています。

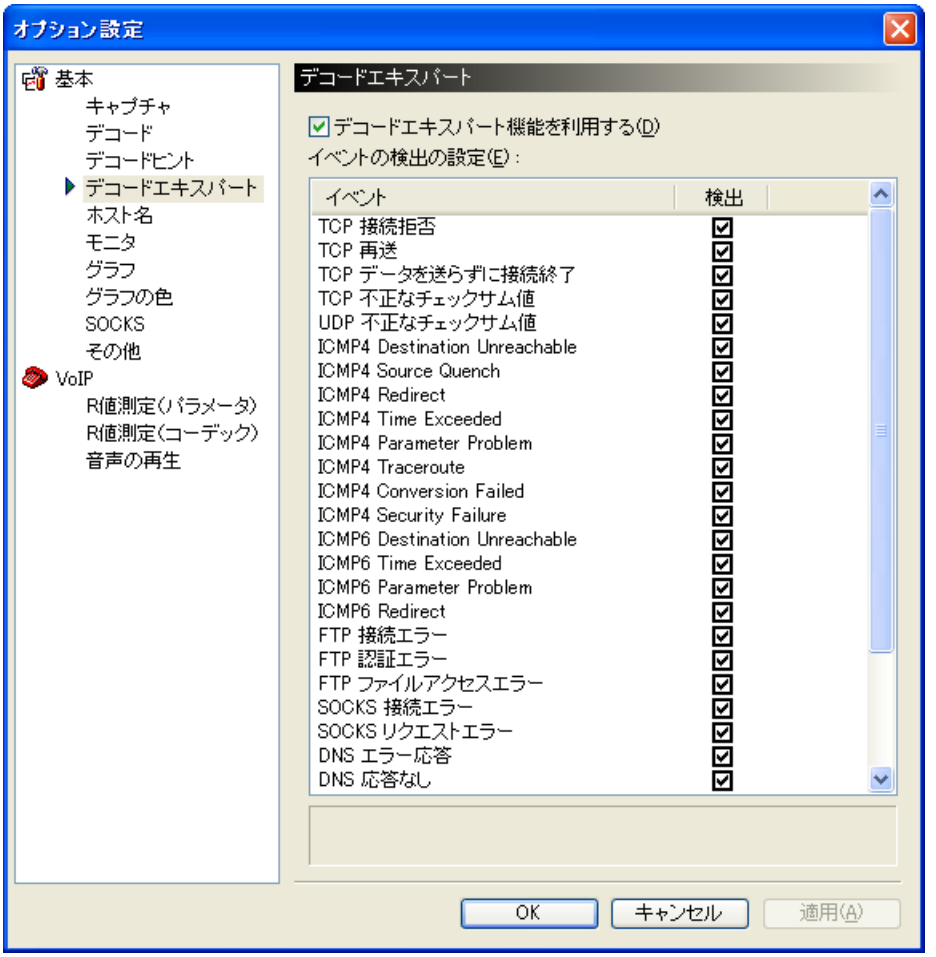


図 11-4: 「オプション設定」ダイアログ (「デコードエキスパート」のパネル)

デコードエキスパート機能を使う場合は、**デコードエキスパート機能を利用する(D)** にチェックを付けます。

イベントの検出の設定(E) のリストに、デコードエキスパート機能で検出できるイベントの一

覧があります。検出したいデコードイベントの**検出**カラムにチェックを付けます。検出する必要のないデコードイベントからチェックを外します。

11.5 ホスト名のオプションを設定する

ホスト名のオプションを設定するペインは、図 11-5 のようになっています。

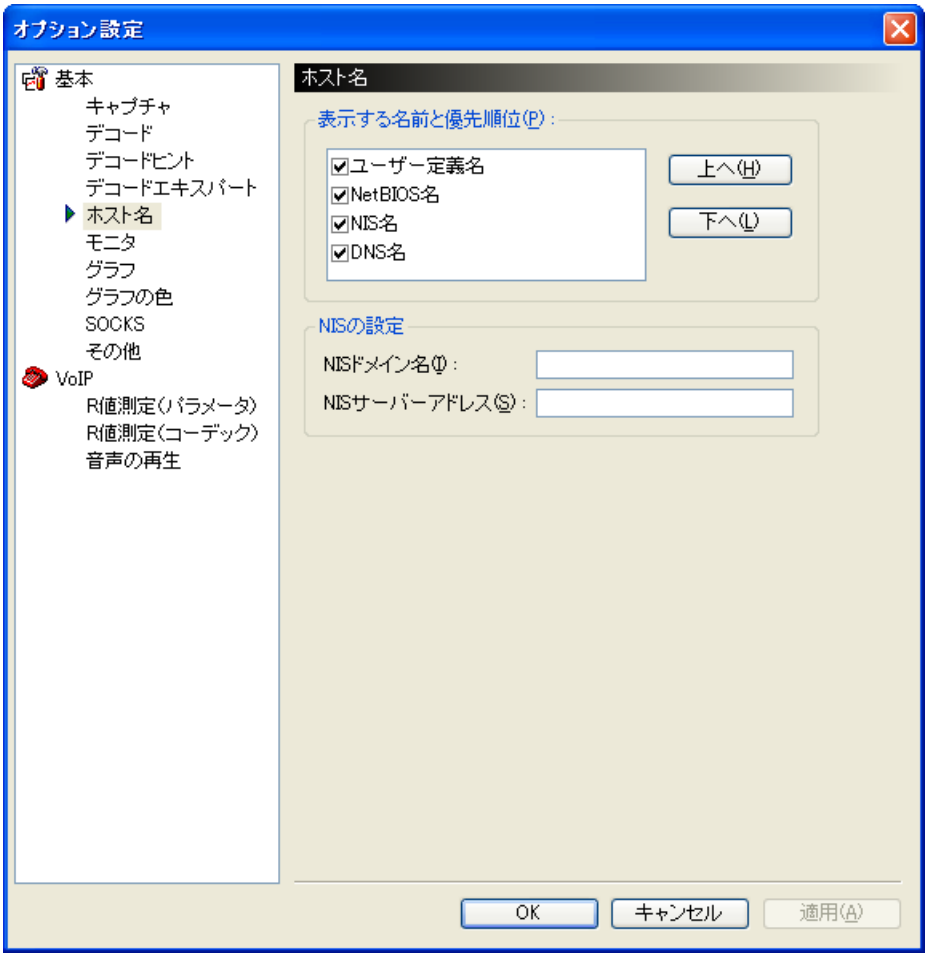


図 11-5: 「オプション設定」ダイアログ (「ホスト名」のパネル)

ASTEC Eyes は、 3 つのネームサービスをサポートしています。

「ホスト名」のパネルでは、次のオプションを設定できます。

- ホスト名を使うかどうか

使うホスト名にチェックを付けます。 IP アドレスだけを使いたい場合は、すべてチェックを外します。

- 複数のネームサービスにホスト名が登録されている場合の優先順位
  ホスト名は優先順位の高い順に並んでいます (優先順位の高いホスト名が上です)。優先順位を変えたいホスト名をクリックし、優先順位を上げたい場合は、**上へ(H)** ボタンをクリックします。優先順位を下げたい場合は、**下へ(L)** ボタンをクリックします。
- NIS ドメイン名と NIS サーバーアドレス
  NIS を利用してホスト名を検索するときに必要です。 NIS を利用する場合は、 NIS ドメイン名を**必ず指定**してください。 NIS サーバーは、指定されなければブロードキャストで自動的に探します。 NIS サーバーアドレスは、 IP アドレスでもホスト名でもかまいません。

IPv6 アドレスの検索に WINS を使うことはできません。

ユーザー定義名は、アドレス帳で入力できるホスト名です。アドレス帳を編集して、 IP アドレスまたは MAC アドレスに任意のホスト名を設定できます。アドレス帳の編集については、「12.2　アドレス帳を使う」 (331 ページ) を参照してください。

IP 層アドレス帳および MAC 層アドレス帳には、チェックの付いているホスト名のカラムだけが表示されます。

11.5.1　ホストを IP アドレスで表示する

ホスト名より IP アドレスの方が分かりやすいという場合は、すべてのホスト名のチェックを外します。

11.6 モニタのオプションを設定する

モニタのオプションを設定するペインは、図 11-6 のようになっています。

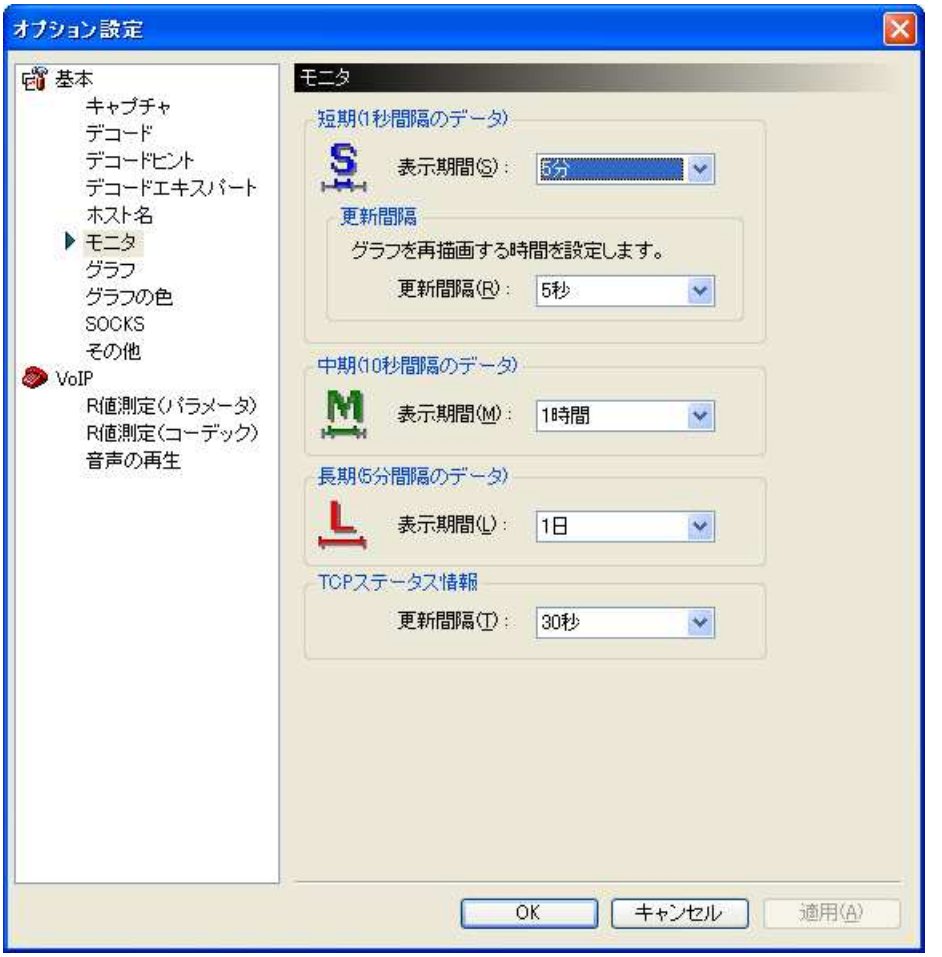


図 11-6: 「オプション設定」ダイアログ (モニタ)

モニタのオプションには、次の 3 つがあります。

- トラフィックウィンドウの各タイムスパンの期間の設定
  タイムスパンとは、トラフィックの統計情報を表示する期間です。 短期、中期、長期のタ

イムスパンそれぞれの期間をカスタマイズできます。
各タイムスパンごとにドロップダウンリストボックスから表示期間を選びます。
デフォルトでは、短期タイムスパンが 5 分間、中期タイムスパンが 1 時間、長期タイムスパンが 1 日です。

- トラフィックウィンドウを短期タイムスパンで表示しているときのグラフの更新間隔
  トラフィックウィンドウを短期のタイムスパンで表示しているときは、グラフを更新する間隔を選べます。デフォルトの更新間隔は 5 秒です。ドロップダウンリストボックスから選びます。
  中期または長期のタイムスパンで表示しているときは、グラフの更新間隔は選べません。中期のタイムスパンを表示しているときの更新間隔は 10 秒、長期のタイムスパンを表示しているときの更新間隔は 5 分です。
- 「TCP ステータス情報」のウィンドウの情報の更新間隔
  「TCP ステータス情報」のウィンドウの情報を更新する間隔をドロップダウンリストボックスから選びます。

中期のタイムスパンを表示している場合、モニタを開始してから 10 秒が経過しないと、トラフィックウィンドウには何も表示されません。
長期のタイムスパンを表示している場合、モニタを開始してから 5 分が経過しないと、トラフィックウィンドウには何も表示されません。

更新間隔を長くすると、 CPU の負荷が減少します。

11.7　グラフのオプションを設定する

グラフのオプションを設定するペインは、図 11-7 のようになっています。

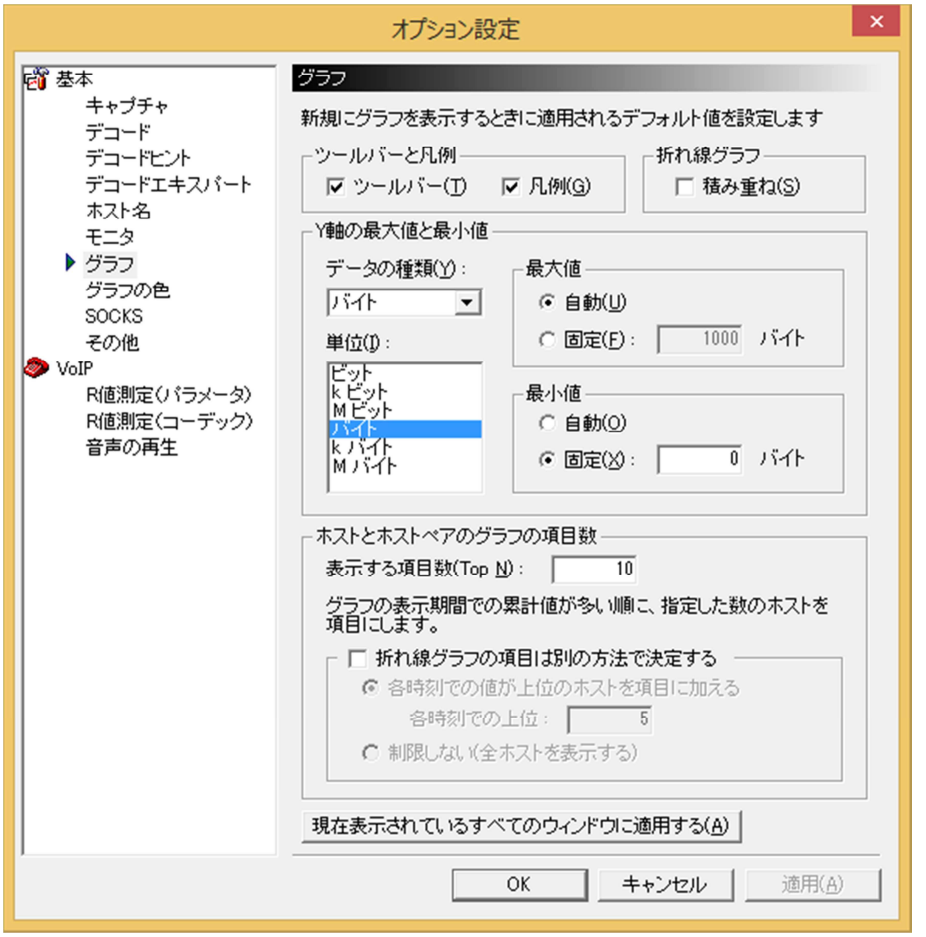


図 11-7:「オプション設定」ダイアログ (グラフ)

このペインでは、グラフの表示に関する次の項目のデフォルトの値を変更できます。

- ツールバーと凡例の表示、非表示
- Y 軸の最大値と最小値、および Y 軸の補助単位

- ホストとホストペアのグラフの項目数の設定

「オプション設定」ダイアログの「グラフ」のパネルで設定した値は、新たに開くトラフィックウィンドウに適用されます。すでに表示されているトラフィックウィンドウには適用されません。
すでに表示されているトラフィックウィンドウの表示を変えるには、「グラフのプロパティ」ダイアログを使います。「グラフのプロパティ」ダイアログを開くには、トラフィックウィンドウを右クリックしてポップアップメニューを開き、**プロパティ(O)**... を選びます。「グラフのプロパティ」ダイアログの「グラフ」のページで設定する内容は、「オプション設定」ダイアログの「グラフ」のパネルと同じです。

11.7.1 ツールバーと凡例の設定

デフォルトでは、トラフィックウィンドウにはツールバーと凡例が表示されます。

ツールバーを非表示にするには、**ツールバー(T)** のチェックを外します。

凡例を非表示にするには、**凡例(G)** のチェックを外します。

11.7.2 Y 軸の設定

Y 軸の最大値と最小値 領域では、トラフィックウィンドウの Y 軸の設定をします。

トラフィックウィンドウの Y 軸の単位は切り替えることができます。**バイト**、**フレーム**、および**使用率** (「MAC 層トラフィック」のウィンドウの場合のみ) の 3 つを切り替えて表示できます。

Y 軸を**バイト**にした場合、**フレーム**にした場合、**使用率**にした場合のそれぞれについて、

- Y 軸の最大値と最小値
- 補助単位

を設定できます。

Y 軸の補助単位と最大値、最小値を設定する手順を次に示します。

1. **データの種類(Y)** のドロップダウンリストボックスからデータの種類を選びます。「バイト」、「フレーム」、または「使用率」が選べます。
   選んだデータの種類によって、**単位(I)** のリストの項目が変わります。
2. **単位(I)** のリストから単位を選びます。

3. 最大値を設定します。
   固定しない場合は**自動(U)** を選びます。固定する場合は**固定(F)** を選んで、値を入力します。
4. 最小値を設定します。
   固定しない場合は**自動(O)** を選びます。固定する場合は**固定(X)** を選んで、値を入力します。

デフォルトの状態に戻すには、最大値を自動に、最小値を固定値 0 に設定します。

11.7.3 ホストとホストペアのグラフの項目数の設定

ホストとホストペアのグラフの項目数 領域では、折れ線グラフ、棒グラフ、円グラフのトラフィックウィンドウに対して、グラフに表示されている期間の累計値で、上位いくつまでのグラフアイテムを表示するか指定します。

折れ線グラフと円グラフについては、表示期間中に上位に含まれなかったグラフアイテムを `Others` という項目にまとめて表示します。

TopN(N) に指定できる値の範囲は $1 \leq$ 値 ≤ 1024 です。

折れ線グラフについては、表示期間の累計値で表示するかどうかを決める以外に、

- 各時刻での値が上位のホストを項目に加える
- 制限しない (全ホストを表示する)

の 2 通りの表示方法も選択できます。

ASTEC Eyes では、トラフィックのデータは、フレーム数 (パケット数) とパケットのバイト数を常に集計し、一定間隔で統計データを作成しています。**各時刻での値が上位のホストを項目に加える**を選択した場合は、統計データを作成した各時点においてトラフィックの上位 *N* 項目に含まれている項目のみを表示します。タイムスパン内に一度もトラフィックの上位 *N* 項目に入らなかったグラフアイテムについては、 `Others` という項目にまとめて表示します。

制限しない (全ホストを表示する) を選択した場合には、すべてのグラフアイテムが表示されます。

グラフアイテムが多いときは、項目数を制限することをお薦めします。すべてのグラフアイテムを表示すると、メモリの使用量が増えてグラフの描画が遅くなることがあります。また、グラフも見づらいものになるかもしれません。

タイムスパンとは、トラフィックの統計情報を (折れ線グラフで) 表示する期間のことです。タイムスパンはカスタマイズできます。詳しくは「11.6　モニタのオプションを設定する」 (298 ページ) を参照してください。

11.8 グラフの色のオプションを設定する

グラフの色のオプションを設定するペインは、図 11-8 のようになっています。

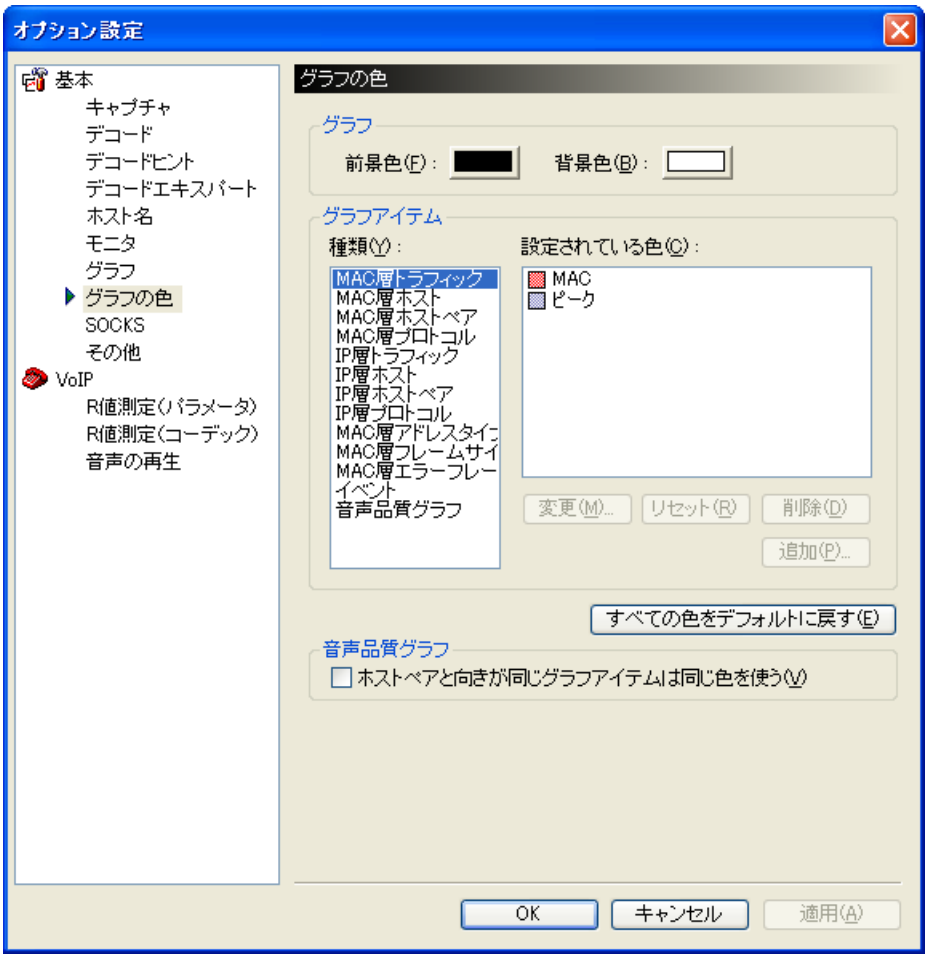


図 11-8: 「オプション設定」ダイアログ (グラフの色)

モニタウィンドウのグラフおよび音声品質のグラフの

- 前景色
- 背景色

- 個々のグラフアイテムの色

を設定できます。

11.8.1 グラフの前景色および背景色を変える

グラフの前景色とは、グラフの目盛りの数字、および凡例の文字列の色を指します。

前景色および背景色を変えるには、次のようにします。

1. **グラフ** 領域の**前景(F)** ボタンまたは**背景(B)** ボタンのボタンをクリックします。
   図 11-9 のような「色の設定」ダイアログが現れます。

図 11-9: 「色の設定」ダイアログ

2. 「色の設定」ダイアログで色を指定して **OK** ボタンをクリックします。
   「色の設定」ダイアログが閉じて、**前景(F)** ボタンまたは**背景(B)** ボタンの色が変わります。
3. 「オプション設定」ダイアログで **OK** ボタンまたは**適用(A)** ボタンをクリックすると、変えた前景色または背景色が、現在開いているすべてのモニタウィンドウのグラフおよび音声品質のグラフに反映されます。また、新たに開くモニタウィンドウのグラフおよび音声品質のグラフの前景色および背景色にも設定した色が使われます。

11.8.2 グラフアイテムの色を変える

個々のグラフアイテムの色を変えるには、次のようにします。

1. **種類(Y)** のリストから、グラフアイテムの種類を選びます。
   - MAC 層トラフィック、IP 層トラフィック、MAC 層アドレスタイプ、MAC 層フレームサイズ、MAC 層エラーフレーム、イベントを選んだ場合
     設定されている色(C) のリストにグラフアイテムが表示されます。グラフアイテムは固定で、削除することも追加することもできません。
   - MAC 層ホスト、MAC 層ホストペア、MAC 層プロトコル、IP 層ホスト、IP 層ホストペア、IP 層プロトコル、音声品質のグラフを選んだ場合
     設定されている色(C) のリストには何も表示されません。
     ただし、トラフィックウィンドウのポップアップメニューを使って「色の設定」ダイアログを開き、特定のグラフアイテムの色を指定している場合は、指定したグラフアイテムに対応する項目があります。
     色を変えたいグラフアイテムを**設定されている色(C)** に追加します。
     追加する手順については、この節の「グラフアイテムを**設定されている色(C)** のリストに追加する」の項を参照してください。
2. **設定されている色(C)** のリストから項目を選び、**変更(M)** ボタンをクリックします。
   「色の設定」ダイアログが現れます (図 11-9 参照)。
3. 「色の設定」ダイアログで色を指定して、**OK** ボタンをクリックします。
   項目名の左側に表示されている色が変わります。
4. 「オプション設定」ダイアログで **OK** ボタンまたは**適用(A)** ボタンをクリックすると、指定したグラフアイテムの色が、現在開いているすべてのトラフィックウィンドウに反映されます。また、新たに開くトラフィックウィンドウに色を変えたグラフアイテムが現れた場合も、設定した色が使われます。

現在トラフィックウィンドウに表示されていないグラフアイテムの色も変更できます。

グラフアイテムを設定されている色(C) のリストに追加する

グラフアイテムを**設定されている色(C)** に追加する方法は 2 通りあります。ドラッグアンドドロップを使う方法とダイアログを使う方法です。

- **ドラッグアンドドロップを使う方法**
  ドラッグできる項目は、**種類(Y)** のリストで選んでいるものによって異なります。ドロップ先は**設定されている色(C)** のリストです。

表 11-1: 設定されている色(C) のリストにドロップできる項目

種類(Y)	ドロップできる項目
MAC 層ホスト	MAC 層発信元毎のトラフィックのグラフアイテム MAC 層受信先毎のトラフィックのグラフアイテム MAC 層ホストペア毎のトラフィックのグラフアイテム MAC アドレス表の行、 MAC 層アドレス帳の行 デコードビューおよびストリームビューのサマリ領域で MAC アドレスが表示されている行
MAC 層ホストペア	MAC 層ホストペア毎のトラフィックのグラフアイテム デコードビューおよびストリームビューのサマリ領域で MAC アドレスが表示されている行
MAC 層プロトコル	MAC 層プロトコル毎のトラフィックのグラフアイテム デコードビューおよびストリームビューのサマリ領域で MAC アドレスが表示されている行
IP 層ホスト	IP 層発信元毎のトラフィックのグラフアイテム IP 層受信先毎のトラフィックのグラフアイテム IP 層ホストペア毎のトラフィックのグラフアイテム IP アドレス表の行、 IP 層アドレス帳の行 デコードビューおよびストリームビューのサマリ領域で IP アドレスが表示されている行 音声品質のウィンドウのグラフアイテム
IP 層ホストペア	IP 層ホストペア毎のトラフィックのグラフアイテム デコードビューおよびストリームビューのサマリ領域で IP アドレスが表示されている行 音声品質のウィンドウのグラフアイテム
IP 層プロトコル	IP 層プロトコル毎のトラフィックのグラフアイテム デコードビューおよびストリームビューのサマリ領域で IP アドレスが表示されている行
音声品質のグラフ	音声品質のウィンドウのグラフアイテム IP 層ホストペア毎のトラフィックのグラフアイテム

- ダイアログを使う方法
  追加(P)...ボタンをクリックします。現れるダイアログは、**種類(Y)** のリストで選んでいるものによって異なります。

  - **種類(Y) で、 MAC 層ホスト、 MAC 層ホストペア、 IP 層ホスト、 IP 層ホストペアを選んでいるとき**
    図 11-10 に示すような「ホストセレクタ」ダイアログが現れます。

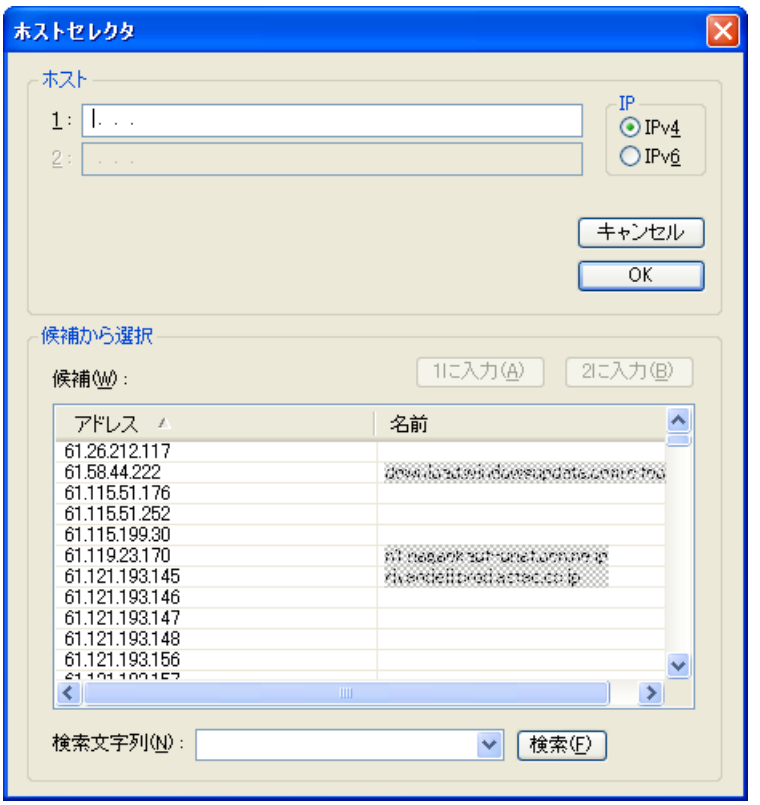


図 11-10: 「ホストセレクタ」ダイアログ

1. IP 層ホストおよび IP 層ホストペアの場合は IP のバージョンを選びます。
2. **候補(W)** のリストに表示されているアドレスの中から、**ホスト**領域の **1:** または **2:** に入力したいアドレスをクリックして選びます。
   目的のアドレスを見つけるために**候補(W)** リストを検索することもできます。
3. **1 に入力(A)** ボタンまたは **2 に入力(B)** ボタンをクリックします。

ホスト領域の **1:** および **2:** に直接キー入力することもできます。

4. **OK** ボタンをクリックします。
「ホストセレクタ」ダイアログが閉じ、**設定されている色(C)** のリストに選んだグラフアイテムが現れます。

- **種類(Y) で MAC 層プロトコルを選んでいるとき**
図 11-11 に示すような「MAC 層タイプセレクタ」ダイアログが現れます。

図 11-11: 「MAC 層タイプセレクタ」ダイアログ

ASTEC Eyes が解析できるプロトコルのタイプがリストに表示されます。
MAC 層プロトコル(M) の入力行に 16 進 4 桁の値をキー入力するか、リストをクリックしてタイプを選び、 **OK** ボタンをクリックします。
「MAC 層タイプセレクタ」ダイアログが閉じ、**設定されている色(C)** のリストに選んだグラフアイテムが現れます。

- **種類(Y) で IP 層プロトコルを選んでいるとき**
  図 11-12 に示すような「候補リスト」ダイアログが現れます。

図 11-12: 「候補リスト」ダイアログ

ASTEC Eyes が解析できるプロトコル、および Unknown Protocol、 Unknown TCP Protocol、 Unknown UDP Protocol がリストに表示されます。
リストをクリックしてプロトコルを選び、 **OK** ボタンをクリックします。
「MAC 層タイプセレクタ」ダイアログが閉じ、**設定されている色(C)** のリストに選んだグラフアイテムが現れます。

- **種類(Y)** で音声品質のグラフを選んでいるとき
  図 11-13 に示すような「候補リスト」ダイアログが現れます。

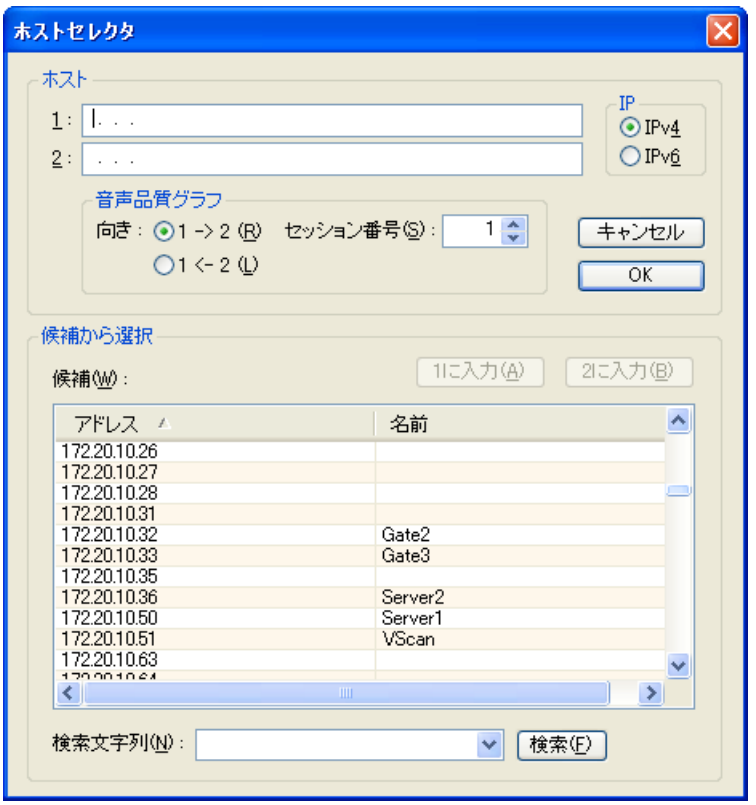


図 11-13: 「ホストセレクタ」ダイアログ

1. IP のバージョンを選びます。
2. 「向き」と「セッション番号」を選びます。
3. **候補(W)** のリストに表示されているアドレスの中から、**ホスト**領域の **1:** または **2:** に入力したいアドレスをクリックして選びます。
   目的のアドレスを見つけるために**候補(W)** リストを検索することもできます。
4. **1 に入力(A)** ボタンまたは **2 に入力(B)** ボタンをクリックします。
   ホスト領域の **1:** および **2:** に直接キー入力することもできます。
5. **OK** ボタンをクリックします。

「ホストセレクタ」ダイアログが閉じ、**設定されている色(C)** のリストに選んだグラフアイテムが現れます。

グラフアイテムを設定されている色(C) のリストから削除する

追加したグラフアイテムを削除するには、**設定されている色(C)** のリストからグラフアイテムを選び、**削除(D)** ボタンをクリックします。

デフォルトの色に戻す

特定のグラフアイテムの色をデフォルトに戻したい場合は、**設定されている色(C)** のリストで項目を選び、**リセット(R)** ボタンをクリックします。

すべての色の指定をデフォルトに戻したい場合は、**デフォルトに戻す(F)** ボタンをクリックします。前景色、背景色を含むすべての色の指定がデフォルトに戻され、**設定されている色(C)** のリストに追加した項目も削除されます。

音声品質のウィンドウのグラフアイテムの色

音声品質のウィンドウに表示するグラフアイテムの色は、

- ホストペア
- データの向き (ホスト *A* からホスト *B* へのデータなのか、ホスト *B* からホスト *A* へのデータなのか)
- セッション番号

の組み合わせで決められますが、セッション番号を無視して、色を決めるようにすることができます。

そのためには、**ホストペアと向きが同じエントリは同じ色を使う (V)** にチェックを付けます。

11.9 SOCKS のオプションを設定する

その他のオプションを設定するペインは、図 11-14 のようになっています。

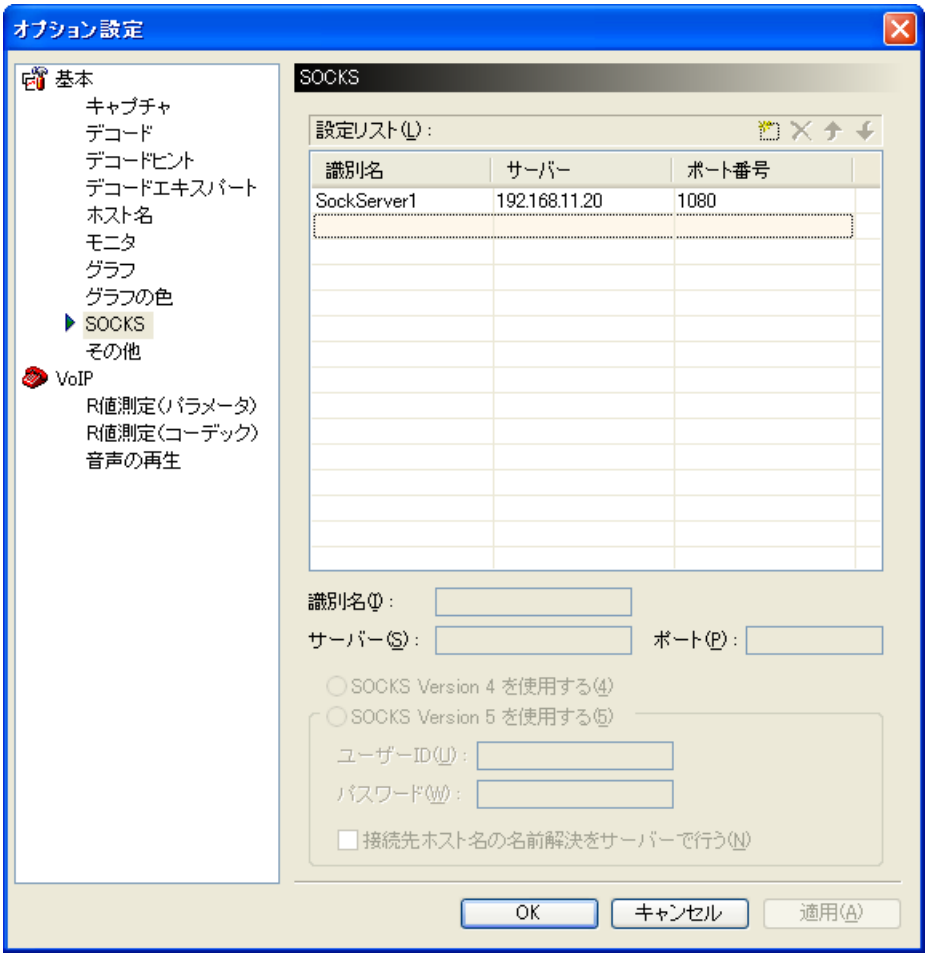


図 11-14: 「オプション設定」ダイアログ (SOCKS)

リモートモジュールに接続するために直接接続できない場合や、 whois コマンド、 ping コマンド、および traceroute コマンドを使うためのデータを直接送れない場合に SOCKS サーバーを利用できます。

SOCKS サーバーの設定は複数用意しておくことができます。

SOCKS サーバーの設定を追加するには、次のようにします。

1. **新規作成**ボタン () をクリックするか、**設定リスト(L)** の空の行をクリックします。
2. **識別名(I)** に任意の識別名を入力します。
   ここで入力した識別名が「接続」ダイアログ、「Whois」ダイアログ、「Ping」ダイアログ、および「Traceroute」ダイアログの SOCKS サーバーを選ぶためのドロップダウンリストボックスに現れます。
3. **サーバー(S)** に SOCKS サーバーの名前を入力します。
   NetBIOS 名や DNS 名、 IPv4 アドレスなど、ローカルホストが識別できる名前を入力します。
4. **ポート(P)** に SOCKS サーバーのポート番号を入力します。
5. バージョン 5 の SOCKS サーバーを使う場合は、 **Socks Version 5 を使用する(5)** を選びます。
   - バージョン 5 の SOCKS サーバーがユーザー ID とパスワードによる認証を行っている場合は、**ユーザー ID(U)** と**パスワード(W)** を指定します。
     認証を行っていない場合は、指定する必要はありません。
   - バージョン 5 の SOCKS サーバーを使う場合、**接続先ホスト名の名前解決をサーバーで行う(N)** にチェックを付けておけば、指定した Whois サーバーや、 ping コマンドまたは traceroute コマンドの対象とするホストの名前解決を、ローカルホストではなく、SOCKS サーバーで行うことができます。
6. 複数の SOCKS サーバーを指定する場合は、手順 1 から 5 を繰り返します。すべての SOCKS サーバーの設定が終わったら、 **OK** ボタンをクリックしてダイアログを閉じます。

入力した行を削除したいときは、削除したい行をクリックし、**削除 (Delete)** ボタン () をクリックするか、 **<Delete>** キーを押します。

サーバー(S) に IPv6 アドレスを入力することはできません。

ASTEC Eyes は、 SOCKS バージョン 5 の認証方式として、ユーザー ID とパスワードによるもののみサポートしています。
SOCKS サーバーの設定が分からないときは、システム管理者に問い合わせてください。

11.10 その他のオプションを設定する

その他のオプションを設定するペインは、図 11-15 のようになっています。

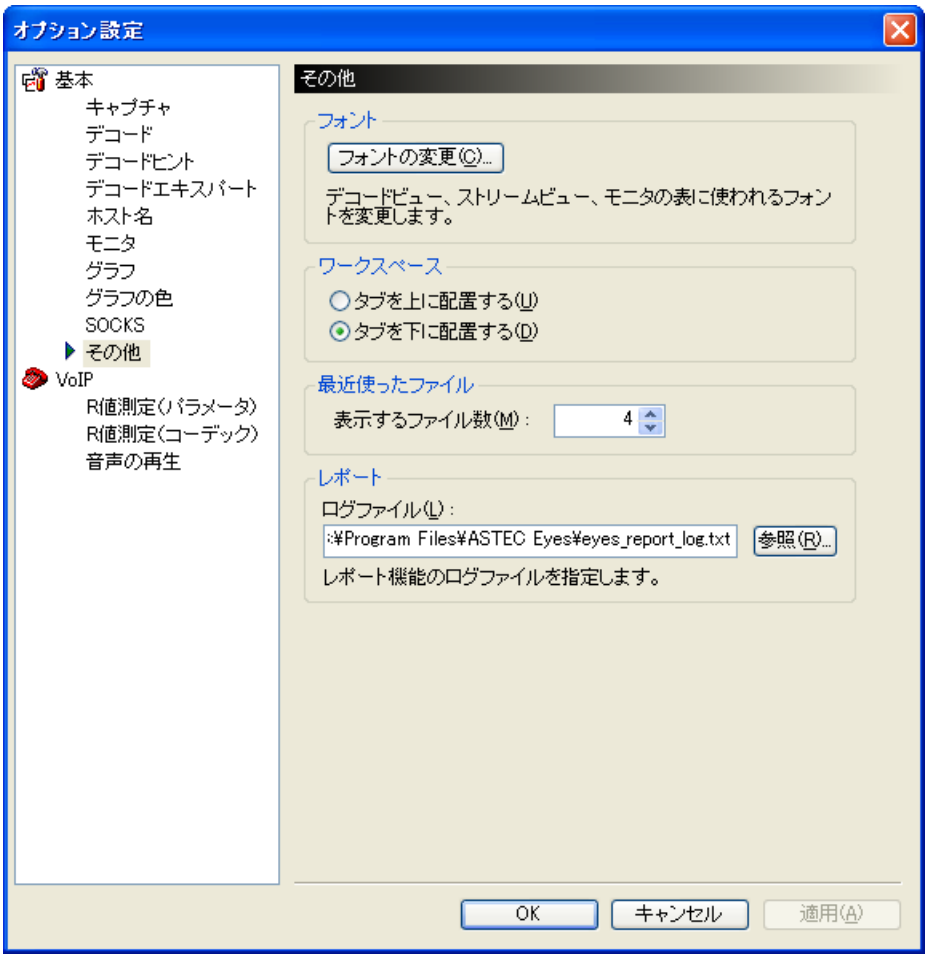


図 11-15: 「オプション設定」ダイアログ (その他)

その他のオプションとして、次の 4 つを設定できます。

- フォント
- ワークスペースのタブの位置

- メインウィンドウの**ファイル(F)** に表示する最近使ったファイルの数
- レポート機能のログファイルの出力先

11.10.1 フォントの設定

次のウィンドウで使われるフォントを変更できます。

- デコードビュー
- ストリームビュー
- 表形式のモニタウィンドウ
- イベントビューア
- IP 層アドレス帳および MAC 層アドレス帳

フォントを変えるには、**フォント** 領域の**変更(C)** ボタンをクリックします。図 11-16 のような、「フォント」ダイアログが現れます。

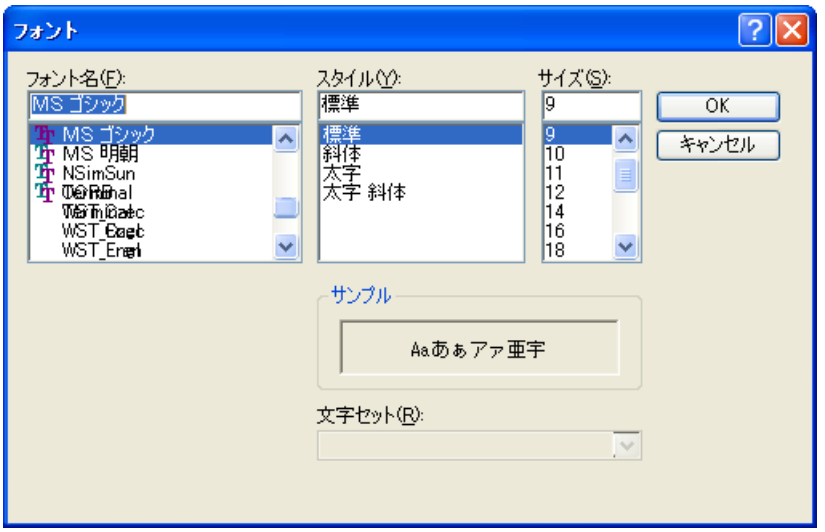


図 11-16:「フォント」ダイアログ

フォント名、スタイル、およびサイズのリストボックスから値を選んで、フォントを指定します。どのようなフォントになっているのか、**サンプル** 領域の表示で確認してください。フォントが決まったら、 **OK** ボタンをクリックします。

フォント名 (F) からは日本語のフォントを選んでください。日本語以外のフォントを選んだ場合は正しく表示されません。

11.10.2 ワークスペースのタブ

ワークスペースを選ぶタブは、デフォルトでは下の方に配置されています。これを上の方に配置するように変更できます。

ワークスペースのタブを上の方に配置するには、**ワークスペース** 領域の**タブを上に配置する (U)** をクリックします。

11.10.3 最近開いたキャプチャファイル

キャプチャファイルを開いてデコードすると、メインウィンドウの**ファイル(F)** メニューに履歴が残ります。デフォルトでは 4 つ分の履歴が残るように設定されていますが、最大 15 個分まで増やせます。

11.10.4 レポート機能のログ

レポートを作成したり削除したりするとログファイルに履歴が残ります。ログファイル名は変更できます。

11.11 設定情報を保存する

ASTEC Eyes を終了しても、次に起動したときに設定ファイルを読み込めば、同じ見た目にすることができ、デコードヒントなどを設定し直す必要もありません。

レジストリに自動的に保存される情報と設定ファイルに保存する情報があります。

11.11.1 設定ファイルに保存する情報

ASTEC Eyes が動作しているホストに関する次の情報を設定ファイルに保存できます。

- ワークスペースの情報
  - ワークスペースの構成およびワークスペースのプロパティ
  - レポートの設定情報
- 表示しているトラフィックウィンドウの情報
  - トラフィックの種類とその表示形式
  - 凡例の表示、非表示、および凡例の領域のサイズ
  - ジオメトリ情報
  - 選択中のタイムスパン
- 表示している「TCP ステータス情報」のウィンドウのジオメトリ情報
- 表示しているモニタのイベントビューアの情報
  - 表示形式
  - 凡例の表示、非表示、および凡例の領域のサイズ
  - ジオメトリ情報
  - 履歴で表示するか、短期タイムスパンで表示するか
- キャプチャのオプション
  - キャプチャバッファのサイズ
  - キャプチャバッファがいっぱいになった時の動作
  - データを圧縮して転送するかどうか
  - リアルタイムデコードを行うかどうか
  - リアルタイムデコードウィンドウのバッファサイズ
  - リアルタイムデコードウィンドウのバッファがいっぱいになった時の動作

- デコードのオプション
  - IPv4、 UDP、および TCP のチェックサムの値をデコード時に検査するかどうか
  - ストリームビューに表示するレコードの並び順 (時系列に表示するか、またはストリーム ID ごとに表示するか)
  - ダンプ領域にフォーカスがないとき、デコード結果領域で選択中の行に対応するダンプ領域の強調部分の色を濃くするかどうか
  - サマリ領域の時刻カラムの値の桁 (ミリ秒または 100 ナノ秒)
  - ダンプ領域の背景色をプロトコルごとに変えるかどうか
  - デフォルトのリンクスピード
- デコードヒント
- デコードエキスパート
  - デコード時にイベントを検出するかどうか
  - 検出するイベントの種類
- ホスト名のオプション
  - 表示するホスト名の種類と優先順位
  - NIS ドメイン名
  - NIS サーバーのアドレス

  「ホスト名の検索」ダイアログで入力した NIS ドメイン名と NIS サーバーのアドレスも保存されます。
- モニタのオプション
  - 各タイムスパンの期間
  - 短期タイムスパンを選んでいるときのグラフの更新間隔
  - 「TCP ステータス情報」のウィンドウのデータの更新間隔
- グラフのオプション
  - 凡例の表示、非表示
  - ツールバーの表示、非表示
  - Y 軸の各データの種類 (バイト、フレーム、使用率) における Y 軸の単位、 Y 軸の最大値、および Y 軸の最小値
  - ホストとホストペアのグラフで表示する項目数
  - 折れ線グラフでの、ホストとホストペアのグラフの表示方法

- グラフの色のオプション
  モニタウィンドウ、イベントビューア、音声品質のウィンドウの前景色、背景色、およびグラフアイテムの色
- SOCKS のオプション
  各 SOCKS サーバーの設定情報と履歴
- その他のオプション
  - フォント情報
  - ワークスペースのタブの位置
  - 最近開いたキャプチャファイルの履歴数
  - レポートの出力結果を記録するログファイル
- インタフェースセレクタウィンドウに表示されるホスト名のラベルとホストにインストールされているネットワークインタフェースのラベル
- R 値の測定のパラメータ
- R 値の測定のコーデックのパラメータ
- 音声の再生の設定

設定情報をファイルに保存する

設定情報をファイルに保存する方法は 2 通りあります。

- メインウィンドウのコモンツールバーの**設定情報の保存**ボタン() をクリックします。
- メインウィンドウの**設定(O)** メニューから**設定情報の保存(W)**... を選びます。

「名前を付けて保存」ダイアログが現れるので、ファイル名を指定します。設定情報を保存するファイルの拡張子は`.wsi` です。

「名前を付けて保存」ダイアログで**自動読込みファイル名**ボタン () をクリックすると、**ファイル名(N)** の入力行に `default-workspace.wsi` と入力されます。
`default-workspace.wsi` というファイル名で、`EYES.exe` があるディレクトリに保存すれば、 ASTEC Eyes が起動したときに、設定情報を自動的に読み込みます。

設定情報をファイルから読み込む

設定情報をファイルから読み込む方法は 2 通りあります。

- メインウィンドウのコモンツールバーの**設定情報の読み込み**ボタン() をクリックします。
- メインウィンドウの**設定(O)** メニューから**設定情報の読み込み(L)**... を選びます。

「開く」ダイアログが現れるので、ファイル名を指定します。

起動時に自動的にモニタを開始する

ローカルホストのインタフェースであれば、 ASTEC Eyes の起動時に自動的にモニタを開始できます。

そのためには、**モニタを行っている状態で、** `EYES.exe` をインストールしたディレクトリの `default-workspace.wsi` に設定情報を保存します。

11.11.2 レジストリに保存する情報

次の情報は自動的にレジストリに保存され、 ASTEC Eyes を起動すると自動的に読み込まれます。

- 接続ホストの履歴
  最近接続したことのあるホストは、「接続」ダイアログで接続するときに、ホスト名を入力しなくてもリストから選ぶことができます。
- 開いたキャプチャファイルの履歴
  最近開いたことのあるキャプチャファイルは、メインウィンドウの**ファイル(F)** メニューから選ぶだけで、開いてデコードできます。
- メインウィンドウのジオメトリ
- メッセージウィンドウのジオメトリ
- インタフェースセレクタウィンドウのジオメトリ
- デコードビューおよびストリームビューのサマリ領域のカラムに関する次の情報
  - 表示するカラム
  - 各カラムの幅
  - カラムの並び順
- コモンツールバーおよびインタフェースツールバーにあるボタンとジオメトリ
- 「開く」ダイアログおよび「名前を付けて保存」ダイアログで指定するパス
  最後に保存または読み込みを行ったディレクトリのパスを、ファイルの種類ごとに保存します。
- Whois コマンドに関する情報
  - WHOIS サーバーの履歴
  - whois コマンドの引数として指定した検索キーの履歴
  - SOCKS サーバーの選択状態

- ステータスバーの表示、非表示
- レポートの設定
  - 出力先ディレクトリの履歴
  - テンプレートファイルの履歴
- 通話シミュレーションモジュールの設定
  - 音声ファイル名の履歴
  - コーデックの設定
  - 接続先ホストの履歴
  - ポート番号、送信回数などの設定

11.11.3 キャプチャモジュールに保存する情報

次の情報はキャプチャモジュールに保存されます。変更するためには、設定権限が必要です。

- インタフェースのラベル
  「インタフェースのプロパティ」ダイアログで**ラベル(L)** にインタフェースを識別するための任意のラベルを入力し、**ラベルをリモートモジュールに登録する(R)** ボタンをクリックすると、入力したラベルがキャプチャモジュールに保存され、別の PC で動作する ASTEC Eyes からも参照されるようになります。
- ログ
  - ログを出力するかどうか
  - ログを出力するインタフェース
  - ログの出力間隔
  - ログの同一ファイルへの書き込み回数
  - ログファイルを出力するディレクトリ
  - ログファイルを圧縮するかどうか
  - ログファイルを自動的に削除するかどうか、また、削除する場合の経過日数
- 連続キャプチャ
  - 連続キャプチャを行うインタフェース
  - 連続キャプチャファイルの最大サイズ
  - 連続キャプチャを出力するディレクトリ
  - ディスクの残りが何 M バイトになったら連続キャプチャを停止するか

  - 自動削除を行うかどうか、また、自動削除を行う場合、ディスクの残りが何 M バイトになったら自動削除を始めるか

- モニタイベント
  - モニタイベントの検出を行うインタフェース
  - 検出するモニタイベントの種類
  - 検出したモニタイベントをメールで通知するかどうか
  - 検出したモニタイベントをメールで直ちに通知するかどうか
  - 検出したモニタイベントを SNMP トラップで通知するかどうか
  - モニタイベントに設定したフィルタ
- 通知機能の設定
  - SMTP サーバー
  - メールの送り先 (TO ヘッダー)
  - メールの送り元 (FROM ヘッダー)
  - メール本文の形式 (プレーンテキストまたは CSV 形式)
  - メール件名 (サブジェクト) の形式
  - メールの送信間隔
  - メールの送信に失敗したとき、通知を止めるかどうか
- SNMP トラップ機能の設定
  - SNMP トラップを有効にするかどうか
  - SNMP トラップホスト
  - SNMP コミュニティ
  - 送信に失敗したときに SNMP トラップ機能を停止するかどうか

12章

ホスト名の表示

ASTEC Eyes では、ホストを識別するために MAC アドレス、 IP アドレスだけでなく、ホスト名が使えます。アドレスよりもホスト名を使うほうがわかりやすいことがあります。そのために、ホスト名を検索したり、ホスト名を管理するためのアドレス帳を編集したりすることができます。

この章では、ホスト名の検索とアドレス帳の機能について説明します。

12.1 ホスト名の検索

「ホスト名の検索」ダイアログを使って複数のホスト名を一度に検索することもできますし、さまざまなウィンドウに表示される IP アドレスに対応するホスト名を、その場から検索することもできます。

次のウィンドウからポップアップメニューを開いて、ホスト名を検索できます。

- トラフィックウィンドウ
- IP アドレス表
- MAC アドレス - IP アドレス対応表
- デコードビューおよびストリームビュー
- イベントビューア
- IP 層アドレス帳
- 音声品質のウィンドウ

12.1.1 「ホスト名の検索」ダイアログを使ってホスト名を検索する

複数の IP アドレスのホスト名を網羅的に検索したい場合は、「ホスト名の検索」ダイアログを使うとよいでしょう。

1. 「ホスト名の検索」ダイアログを開きます。
   「ホスト名の検索」ダイアログを開く方法は 2 通りあります。
   - メインウィンドウの**ツール(T)** メニューから**ホスト名の検索(H)**. . . を選びます
   - **<Ctrl-L>** キーを押します

   図 12-1 に示すような、「ホスト名の検索」ダイアログが現れます。

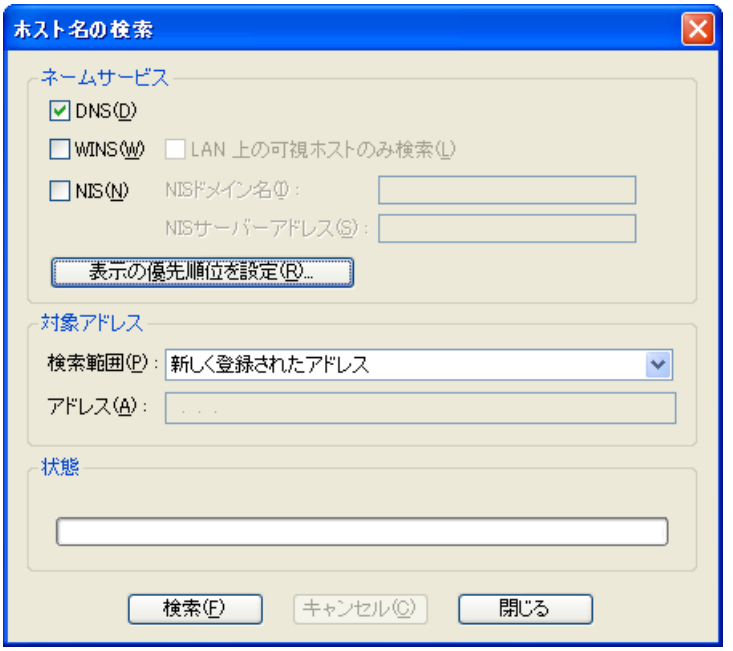


図 12-1: 「ホスト名の検索」ダイアログ

2. **ネームサービス** 領域で、検索に利用するネームサービスにチェックを付けます。
   DNS、 WINS、および NIS が使えます。
   NIS を選んだ場合は、 NIS のドメイン名とサーバーを指定します。 NIS ドメイン名は**必ず指定**してください。 NIS サーバーは、指定されなければブロードキャストで自動的に探します。 NIS サーバーアドレスは、 IP アドレスでもホスト名でもかまいません。
   WINS にチェックを付けると、 **LAN 上の可視ホストのみ検索(L)** にチェックを付けられるようになります。これにチェックを付けると、 Windows のエクスプローラで「マイ ネットワーク」または「ネットワーク コンピュータ」にある「ネットワーク全体」以下に表示されるコンピュータだけを検索の対象とします。

IPv6 アドレスの検索に WINS を使うことはできません。

3. **対象アドレス** 領域で検索の対象となるアドレスの範囲を指定します。
   指定できる範囲には、次のようなものがあります。

   - **新しく登録されたアドレス**
     新しく見つかったアドレスだけを検索します。すでに検索したアドレスについては再検索しません。

- **これまでに登録されたすべてのアドレス**
  これまでに見つかったすべてのアドレスについて検索します。かなり時間がかかることがあります。途中で検索を中止したい場合は、**キャンセル(C)** ボタンをクリックします。
- **これまでに検索が失敗したアドレス**
  以前検索に失敗したアドレスについてのみ検索します。
- **特定の IPv4 アドレス**および**特定の IPv6 アドレス**
  指定された IPv4 または IPv6 アドレスに対応するホスト名を検索します。
  これを選ぶと IP アドレスを入力できるようになります。 IP アドレスを入力する方法はいくつかあります。
  - キー入力する。
  - クリップボードから貼り付ける。
    ただし、クリップボードに保存されている文字列が、 IPv4 または IPv6 のアドレス表記として適切でない場合は貼り付けられません。
  - 次に示す項目をドラッグし、アドレスの入力行にドロップする。
    * トラフィックウィンドウの IP アドレスを表すグラフアイテム
    * デコードビューまたはストリームビューのサマリ領域の IP アドレスが表示されている行
    * IP アドレス表の行
    * IP 層アドレス帳の行
    * 音声品質のウィンドウの IP アドレスを表すグラフアイテム
- **IPv4 ネットワークアドレス**
  これまでに登録された IPv4 アドレスのうち、特定のネットワークセグメントのホストだけを検索の対象にしたいときに選びます。たとえば、 IPv4 アドレスの上位 24 ビットが同じコンピュータを検索対象にするには、 `111.22.11.0/24` のように入力します。
- **IPv6 マスクアドレス (上位ビットにマスク)**
  IPv6 アドレスの上位から *N* ビットを指定し、これまでに登録された IPv6 アドレスのうち、指定された *N* ビットと同じアドレスを持つホストだけを検索の対象にします。
- **IPv6 マスクアドレス (下位ビットにマスク)**
  IPv6 アドレスの下位から *N* ビットを指定し、これまでに登録された IPv6 アドレスのうち、指定された *N* ビットと同じアドレスを持つホストだけを検索の対象にします。

4. **検索(F)** ボタンをクリックします。

検索している間、使っているネームサービスと処理の進捗が **状態** 領域に表示されます。見つかったホスト名は、 IP 層アドレス帳に登録されます。

複数のネームサービスでホスト名が見つかった場合など、1 つの IP アドレスに対して複数のホスト名が見つかることがあります。どのホスト名が表示されるかは、ホスト名の表示の優先順位によります。

ホスト名の表示の優先順位を指定するには、**ネームサービス** 領域にある **表示の優先順位を設定(R)** ボタンをクリックします。「表示する名前と優先順位」ダイアログが現れます。優先順位を設定する具体的な方法については、「11.5　ホスト名のオプションを設定する」 (296 ページ) を参照してください。

次のような場合は、見つかったホスト名は自動的にアドレス帳に登録されるので、検索しなくてもホスト名が表示されます。

- モニタ中に IP アドレスとホスト名を対応付ける DNS のパケットが流れた場合
- 読み込んだログファイルに、ホスト名 (DNS 名) が記録されていた場合
- MAC アドレスまたは IP アドレスとホスト名を対応付けるパケットを含むキャプチャデータをデコードした場合
- アドレス帳を読み込んだ場合

ホスト名の検索機能を使うと、 ASTEC Eyes がネットワーク上にネームサービスのパケットを生成するので、ネットワークのトラフィックが増えます。

NIS ドメイン名と NIS サーバーアドレスは「オプション設定」ダイアログでも設定でき、設定ファイルに保存できます。詳しくは「11.5　ホスト名のオプションを設定する」 (296 ページ) を参照してください。

12.1.2　トラフィックウィンドウのグラフアイテムのホスト名を検索する

IP アドレスを表すグラフアイテムのホスト名を検索できます。

IP アドレスを表すグラフアイテムの例としては、「IP 層発信元毎のトラフィック」のウィンドウのグラフアイテムや、ホストペアの内訳を表示しているトラフィックウィンドウのグラフアイテムがあります。

1. トラフィックウィンドウでグラフアイテムを選びます。
2. トラフィックウィンドウを右クリックしてポップアップメニューを開き、**ホスト名の検索(H)** をポイントし、ネームサービスを選びます。

メッセージウィンドウには、探しているホストの IP アドレスと状態が表示されます。

見つかったホスト名は IP 層アドレス帳に登録され、トラフィックウィンドウの凡例にはホスト名が表示されるようになります。

「ホスト名の検索」ダイアログまたは「オプション設定」ダイアログで NIS のドメイン名を指定していない場合は、 NIS は選べないようになっています。

12.1.3 デコードビューおよびストリームビューのホスト名を探す

デコードビューおよびストリームビューのサマリ領域に表示されている IP アドレスに対応するホスト名を検索できます。

IP アドレスが表示されている行を右クリックしてポップアップメニューを開き、**ホスト名の検索(H)** をポイントし、ネームサービスを選びます。

メッセージウィンドウには、探しているホストの IP アドレスと状態が表示されます。

見つかったホスト名は IP 層アドレス帳に登録され、デコードビューまたはストリームビューの表示が変わります。

12.1.4 イベントビューアのホスト名を探す

表形式のイベントビューアに表示されている IP アドレスに対応するホスト名を検索できます。

IP アドレスが表示されている行を右クリックしてポップアップメニューを開き、**ホスト名の検索(H)** をポイントし、ネームサービスを選びます。

発信元アドレスのカラムと受信先アドレスのカラムに表示されている IP アドレスに対応するホスト名を検索します。メッセージウィンドウには、探しているホストの IP アドレスと状態が表示されます。

見つかったホスト名は IP 層アドレス帳に登録され、イベントビューアの表示が変わります。

12.1.5 IP 層アドレス帳、 IP アドレス表、 MAC アドレス - IP アドレス対応表 のホスト名を探す

IP 層アドレス帳、 IP アドレス表、および MAC アドレス - IP アドレス対応表 に表示されている IP アドレスに対応するホスト名を検索できます。

検索したい IP アドレスの行を右クリックしてポップアップメニューを開き、**ホスト名の検索(H)** をポイントし、ネームサービスを選びます。

メッセージウィンドウには、探しているホストの IP アドレスと状態が表示されます。

見つかったホスト名は IP 層アドレス帳に登録され、それぞれのウィンドウに表示されます。

12.1.6 音声品質のウィンドウのグラフアイテムのホスト名を探す

音声品質のウィンドウのグラフアイテムのホスト名を探す手順は、トラフィックウィンドウのグラフアイテムのホスト名を探す手順と同じです。詳しくは「12.1.2 トラフィックウィンドウのグラフアイテムのホスト名を検索する」 (328 ページ) を参照してください。

12.1.7 ホスト名を反映する

ホスト名を検索して新たにホスト名が見つかったときや、ホスト名の表示の優先順位を変えたとき、モニタウィンドウには自動的に反映されます。

しかし、デコードビューおよびストリームビューには、デコードビューまたはストリームビューから探した場合を除いては、明示的に指示しないと反映されません。

デコードビューおよびストリームビューにホスト名を反映する方法は 2 通りあります。

- デコードビューまたはストリームビューのツールバーにある**ホスト名の更新**ボタン() をクリックします。
- デコードビューまたはシーケンスモードでないストリームビューを右クリックしてポップアップメニューを開き、**ホスト名の更新(U)** を選びます。

12.2 アドレス帳を使う

ASTEC Eyes には 2 つのアドレス帳があります。 IP 層用のものと MAC 層用のものです。アドレス帳を使えば、ホストに任意のわかりやすい名前を付けられます。また、 1 つのネームサービスにおいて、複数の名前が 1 つのホストに対して付けられている場合、どの名前を使うか選ぶことができます。

12.2.1 IP 層アドレス帳

IP 層アドレス帳を開くには、メインウィンドウの**編集(E)** メニューから **IP 層アドレス帳の編集(I)** を選びます。図 12-2 のような IP 層アドレス帳が現れます。

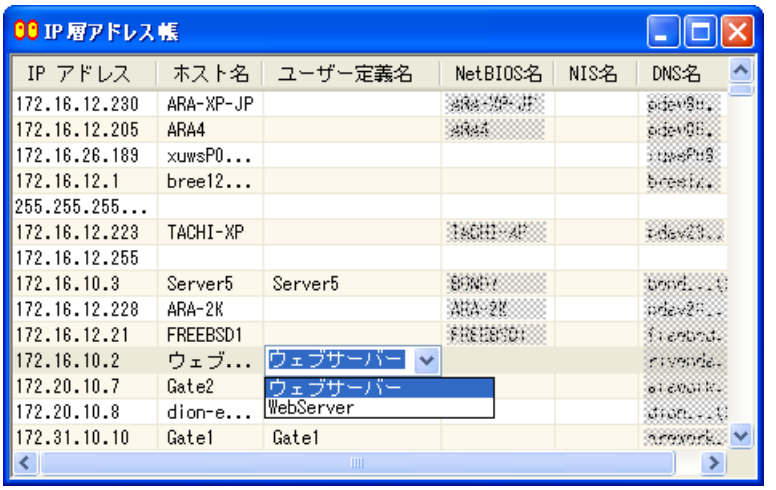


図 12-2: IP 層アドレス帳

IP 層アドレス帳には、

- モニタ中に見つかったもの
- ログに記録されていたもの
- キャプチャデータをデコードして見つかったもの
- アドレス帳のファイルから読み込んだもの

が表示されます。

IP 層のアドレス帳は最大 6 つのカラムから構成されます。各カラムの見出しをクリックすると、そのカラムの内容に従って、行を並べ替えることができます。

IP アドレス IPv4 または IPv6 の IP アドレスを表示します。

ホスト名 現在使われているホスト名を表示します。

ユーザー定義名 ユーザーが任意の名前を入力できます。コンボボックスになっていて、複数の名前を入力できます。

入力する手順については、「12.2.3 ユーザー定義名の入力」 (334 ページ) を参照してください。

NetBIOS 名、 NIS 名、 DNS 名
それぞれのネームサービスを使って見つかった名前を表示します。複数の候補がある場合はドロップダウンリストボックスから選べます。

ユーザー定義名、 NetBIOS 名、 NIS 名、および DNS 名の 4 つのカラムは、「オプション設定」ダイアログの「ホスト名」のパネルのホスト名に対応しています。「ホスト名」のパネルでチェックが付いているホスト名のカラムだけが有効です。チェックが付いていないホスト名のカラムの罫線は破線で表示されます。

また、「オプション設定」ダイアログで設定した優先順位に従ってカラムの並びが決まります。たとえば、ホスト名の優先順位が

1. ユーザー定義名
2. NetBIOS 名
3. NIS 名
4. DNS 名

となっている場合、左からユーザー定義名、 NetBIOS 名、 NIS 名、 DNS 名の順に並びます。

ホスト名の優先順位を変える方法やホスト名を使わないようにする方法については、「11.5 ホスト名のオプションを設定する」 (296 ページ) を参照してください。

アドレス帳は IP 層用のものと MAC 層用のものが ASTEC Eyes に 1 つずつあります。アドレス帳は、ネットワークインタフェースごとに管理されているわけではありません。複数のネットワークインタフェースをモニタしている場合、複数のインタフェースで見つかったすべての IP アドレスが IP 層のアドレス帳に、 MAC アドレスが MAC 層のアドレス帳に表示されます。

12.2.2 MAC 層アドレス帳

MAC 層のアドレス帳を開くには、メインウィンドウの**編集(E)** メニューから **MAC 層アドレス帳の編集(M)** を選びます。図 12-3 のような MAC 層アドレス帳が現れます。

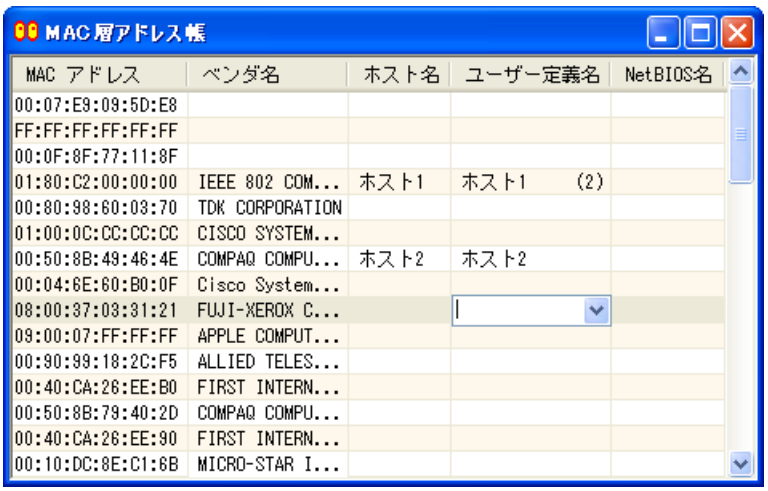


図 12-3: MAC 層アドレス帳

MAC 層アドレス帳には、

- キャプチャデータをデコードして見つかったもの
- アドレス帳のファイルから読み込んだもの

が表示されます。

MAC 層のアドレス帳は 5 つのカラムからなっています。各カラムの見出しをクリックすると、そのカラムの内容に従って、行を並べ替えることができます。

MAC アドレス MAC アドレスを表示します。

ベンダ名 MAC アドレスのベンダ名を表示します。

ホスト名 現在使われているホスト名を表示します。

ユーザー定義名 ユーザーが任意の名前を入力できます。コンボボックスになっていて、複数の名前を入力できます。

入力する手順については、「12.2.3 ユーザー定義名の入力」 (334 ページ) を参照してください。

NetBIOS 名 キャプチャデータをデコードして得られた NetBIOS 名を表示します。複数の候補がある場合はドロップダウンリストボックスから選べます。

ユーザー定義名および NetBIOS 名のカラムは、「オプション設定」ダイアログの「ホスト名」のパネルのホスト名に対応しています。「ホスト名」のパネルでチェックが付いているカラムだけが有効です。チェックが付いていないホスト名のカラムの罫線は破線で表示されます。

また、「オプション設定」ダイアログで設定した優先順位に従ってカラムの並びが決まります。たとえば、ホスト名の優先順位が

1. ユーザー定義名
2. NetBIOS 名

となっている場合、左からユーザー定義名、 NetBIOS 名の順に並びます。

12.2.3 ユーザー定義名の入力

ユーザー定義名のカラムに分かりやすい名前を入力して、ホスト名として表示させることができます。複数の名前を入力できます。

ユーザー定義名を入力するには、次のようにします。

1. 入力できる状態にします。そのための方法は 4 通りあります。
   - 入力したいユーザー定義名のセルをダブルクリックします。
   - 入力したいユーザー定義名のセルを 2 回クリックします。
   - 上下のカーソルキー (**<↑>** 、 **<↓>**) を押して入力したい行を選び、 **<F2>** キーを押します。
   - 入力したいユーザー定義名のセルを右クリックしてポップアップメニューを開き、**編集 (E)** を選びます。

入力できる状態になると、コンボボックスが表示されます。

2. コンボボックスに任意の名前を入力します。

複数の名前を入力できます。複数の名前を入力した場合は、セルの右端に候補の数が表示されます。

12.2.4 ホスト名を削除する

ホスト名を削除するには、次のようにします。

1. ホスト名が複数ある場合、コンボボックスまたはドロップダウンリストボックスから削除したい名前を選んで、削除したいホスト名が表示されている状態にします。
2. 削除したいホスト名のセルを右クリックしてポップアップメニューを開き、**名前の削除(D)** を選びます。

ユーザー定義名の場合は、次のようにして削除することもできます。

1. 削除したいユーザー定義名のセルを入力できる状態にして、コンボボックスから削除したいユーザー定義名を選びます。
2. **<Delete>** キーまたは **<Backspace>** キーを押して名前を消します。
3. **<Enter>** キーを押します。

削除したホスト名を元に戻す方法はありません。ユーザー定義名の場合は、再入力してください。その他のホスト名については、ホスト名の検索を行ってください。ただし、削除したものと同じ名前が見つかる保証はありません。

12.2.5 アドレス帳の表示を変える

デフォルトでは、アドレス帳のユーザー定義名および各ネームサービスのカラムには、名前と候補数が表示されます。表示されているホスト名を得た方法も表示するように、アドレス帳の表示を切り替えられます。

また、 IP 層アドレス帳の場合は、 IP アドレスの各桁 (. または : で区切られた数字) をそろえて表示するようにもできます。

アドレス帳を詳細表示にする

アドレス長を詳細表示にするには、アドレス帳のウィンドウを右クリックしてポップアップメニューを開き、**表示(V)** をポイントし、**詳細(D)** を選びます。

詳細表示では、ホスト名の他に、ホスト名の候補の数とホスト名を得た方法を表示します。ホスト名を得た方法として表示するのは、次の 5 つです。

検索	ASTEC Eyes の検索機能を使って見つけたもの
ファイル	ファイルから読み込んだもの
ユーザー入力	ユーザーがアドレス帳で入力したもの
デコーダ	キャプチャデータを解析した結果見つかったもの
モニタ	モニタ中に流れたパケットから得られたもの
ログ	ログファイル中に記録されていたもの

詳細表示にした IP 層アドレス帳のようすを図 12-4 に示します。

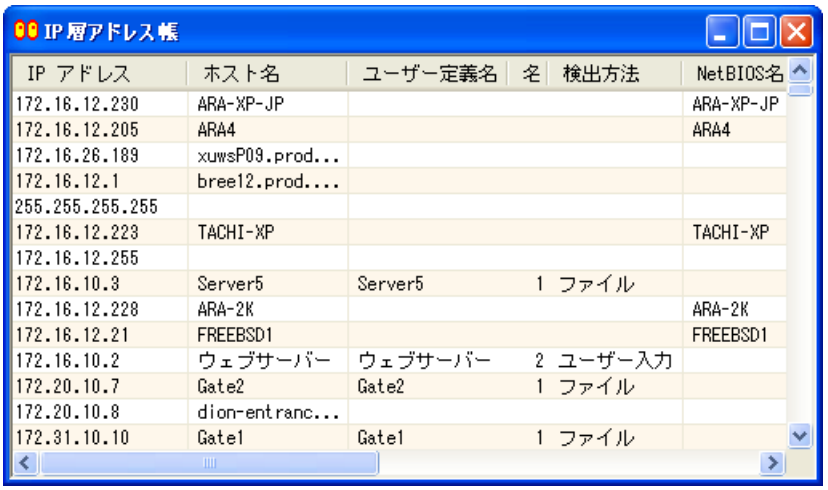


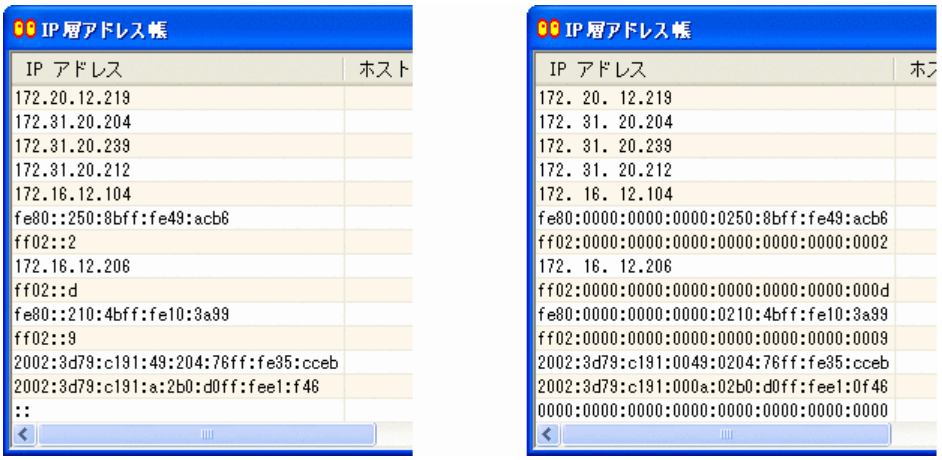
図 12-4: 詳細表示の IP 層アドレス帳

名前と候補数だけの表示に戻すには、アドレス帳を右クリックしてポップアップメニューを開き、**表示(V)** をポイントし、**一覧(L)** を選びます。

IP アドレスの桁を揃えて表示する

デフォルトの表示では、各桁は揃っておらず、 IPv6 のアドレスは省略表記されています (図 12-5 の左側)。

IP アドレスの桁を揃えて表示するには、アドレス帳のウィンドウを右クリックしてポップアップメニューを開き、**各桁を揃える(A)** を選びます。



デフォルトの表示　　各桁をそろえた表示

図 12-5: デフォルトの表示と各桁を揃えた表示

デフォルトの表示に戻すには、アドレス帳のウィンドウを右クリックしてポップアップメニューを開き、もう一度**各桁を揃える(A)** を選びます。

12.2.6　アドレス帳で文字列を検索する

IP 層アドレス帳や MAC 層アドレス帳で文字列を検索できます。

検索するには、メインウィンドウの**編集(E)** メニューから**検索(F)** を選ぶか、 **<Ctrl-F>** キーを押します。 「検索」ダイアログが現れるので、探したい文字列を入力して**次を検索(F)** ボタンをクリックします。

検索する文字列に正規表現を使うこともできます。正規表現を指定する場合は、**正規表現(E)** にチェックを付けます。正規表現については、「6.8.2　正規表現を用いた検索」 (147 ページ)を参照してください。

12.2.7 アドレス帳の保存と読み込み

アドレス帳のデータ (アドレスとホスト名) は、ファイルに保存したり、ファイルから読み込んだりすることができます。 IP 層アドレス帳と MAC 層アドレス帳のデータはまとめて 1 つのファイルに保存されます。ファイルからアドレス帳のデータを読み込めば、ホスト名を検索しなくてもホスト名を表示できます。

アドレス帳のデータをファイルに保存する

メインウィンドウの**編集(E)** メニューから**アドレス帳の保存(W)**... を選びます。

「名前を付けて保存」ダイアログが現れるので、ファイル名を指定して保存します。

ASTEC Eyes の実行形式 (`EYES.exe`) があるディレクトリに、 `default-address.txt` というファイル名で保存すれば、次に ASTEC Eyes を起動したときに自動的に読み込みます。「名前を付けて保存」ダイアログにある**自動読込みファイル名**ボタン () をクリックすれば、`default-address.txt` が**ファイル名(N)** に入力されます。

アドレス帳のデータをファイルから読み込む

メインウィンドウの**編集(E)** メニューから**アドレス帳の読み込み(A)**... を選びます。

「開く」ダイアログが現れるので、ファイル名を指定します。

DHCP などを使って IP アドレスを取得している場合は、コンピュータを起動し直したとき、以前と同じ IP アドレスを取得できるとは限りません。そのため、実際の IP アドレスとホスト名の対応が、アドレス帳に保存されているものとは異なることがあります。

13章

その他の機能

ASTEC Eyes には、主だった機能に分類できないいくつかの便利な機能があります。ここでは、それらの機能について説明します。

13.1 ネットワークユーティリティ

ネットワークの状態やホストに関する情報を調べるために、 whois、 ping、および traceroute の各コマンドを ASTEC Eyes から実行できます。

実行するためには、それぞれの引数を入力するためのダイアログを開きます。

13.1.1 ネットワークユーティリティのダイアログを開く

メインウィンドウから開く

メインウィンドウの**ツール(T)** メニューから **Whois ツール(W)**. . . 、 **Ping ツール(P)**. . . 、または **Traceroute ツール(T)**. . . を選びます。

メインウィンドウ以外の場所から開く

ネットワークユーティリティのダイアログは次の場所から開くことができます。

- メインウィンドウから
- トラフィックウィンドウから
- デコードビューおよびストリームビューから
- IP アドレス表から
- MAC アドレス - IP アドレス対応表 から
- IP 層アドレス帳から
- 音声品質のウィンドウから

1. ウィンドウに表示されているグラフアイテムまたは行を右クリックしてポップアップメニューを開き、**ネットワークユーティリティ(N)** をポイントします。
2. **Whois(W)**、 **Ping(P)**、または **Traceroute(T)** を選びます。
3. 手順 1 でクリックしたグラフアイテムや行によっては、コマンドの引数として指定できるホスト名や IP アドレス、ドメイン名の候補が複数得られることがあります。そのような場合は、ホスト名や IP アドレス、ドメイン名をメニュー項目とするサブメニューが現れます。サブメニューから引数として指定したいものを選びます。

13.1.2 Whois

図 13-1 に、 whois コマンドの引数を指定するためのダイアログを示します。

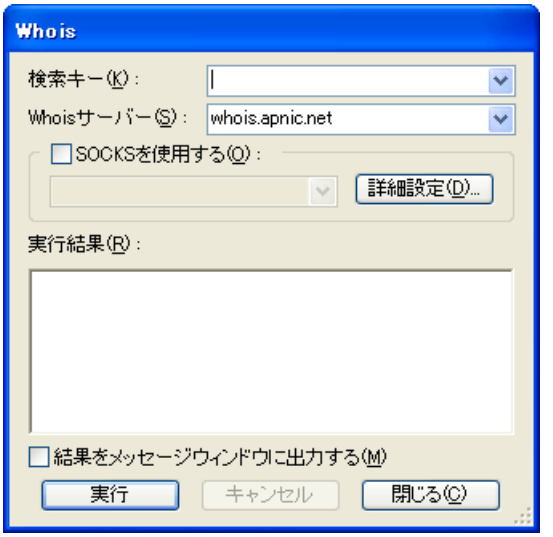


図 13-1: whois コマンドを実行するためのダイアログ

whois を実行するには、次の項目を設定して、**実行**ボタンをクリックするか、 **<Enter>** キーを押します。

検索キー(K) 検索したいドメイン名またはハンドルを指定します。

キー入力することもできますし、次の項目をドラッグして、ドロップすることもできます。

- 「IP 層発信元毎のトラフィック」、「IP 層受信先毎のトラフィック」、または「IP 層ホストペア毎のトラフィック」のグラフアイテム (IPv4 アドレスを表すもの)
- デコードビューおよびストリームビューのサマリ領域の IP アドレスが表示されている行
- IP アドレス表の IPv4 アドレスの行
- IP 層アドレス帳の IPv4 アドレスの行
- 音声品質のウィンドウのグラフアイテム

Whois サーバー(S)

Whois サーバーを指定します。リストには、次の 4 つの Whois サーバーがあります。リストから選ぶか、任意のサーバー名をキー入力します。

- whois.apnic.net
- whois.jp
- rs.internic.net
- www.tonic.to

SOCKS を使用する(O)

デフォルトでは、 SOCKS は使わないようになっています。 SOCKS を使う場合は、 **SOCKS を使用する(O)** にチェックを付けて、ドロップダウンリストボックスから SOCKS サーバーを選びます。

SOCKS サーバーを設定していない場合は、ドロップダウンリストボックスは空です。**詳細設定(D)**... ボタンをクリックして SOCKS サーバーを設定します。 SOCKS サーバーの設定については、「11.9　SOCKS のオプションを設定する」 (313 ページ) を参照してください。

結果をメッセージウィンドウに出力する(M)

チェックが付いていない場合、実行結果は**実行結果(R)** 領域に表示されます。チェックを付けると、メインウィンドウのメッセージウィンドウに表示されます。

13.1.3 Ping

図 13-2 に、 ping コマンドの引数を指定するためのダイアログを示します。

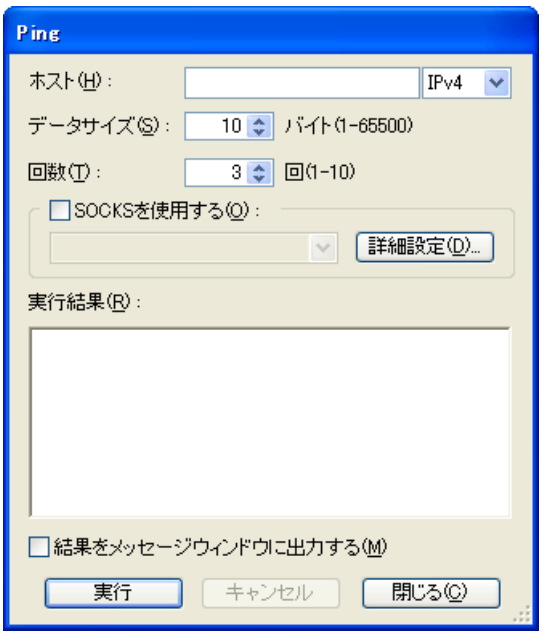


図 13-2: ping コマンドを実行するためのダイアログ

次の項目を設定して、**実行**ボタンをクリックするか、 **<Enter>** キーを押します。

ホスト(H) ICMP の ECHO REQUEST データグラムを送りたいホストやゲートウェイを指定します。 NetBIOS 名や DNS 名、 IP アドレスなど、ローカルホストが識別できる名前を入力します。

キー入力するか、または次に示す項目をドラッグして、ドロップします。

- 「IP 層発信元毎のトラフィック」、「IP 層受信先毎のトラフィック」、または「IP 層ホストペア毎のトラフィック」のグラフアイテム
- デコードビューおよびストリームビューのサマリ領域の IP アドレスが表示されている行
- IP アドレス表の行
- IP 層アドレス帳の行

IPv6 で ICMP パケットを送る場合は、**ホスト(H)** の右側にあるドロップダウンリストボックスから IPv6 を選びます。

データサイズ(S) 送信するデータをバイト数で指定します。

SOCKS を使って LAN の外側にあるホストを対象とする場合は、指定できません。

回数(T) ECHO REQUEST データグラムを送る回数を指定します。指定回数だけ送ると停止します。

SOCKS を使って LAN の外側にあるホストを対象とする場合は、指定できません。

SOCKS を使用する(O)

デフォルトでは、 SOCKS は使わないようになっています。 SOCKS を使う場合は、 **SOCKS を使用する(O)** にチェックを付けて、ドロップダウンリストボックスから SOCKS サーバーを選びます。

SOCKS サーバーを設定していない場合は、ドロップダウンリストボックスは空です。**詳細設定(D)**... ボタンをクリックして SOCKS サーバーを設定します。 SOCKS サーバーの設定については、「11.9 SOCKS のオプションを設定する」 (313 ページ) を参照してください。

結果をメッセージウィンドウに出力する(M)

チェックが付いていない場合、実行結果は**実行結果(R)** 領域に表示されます。チェックを付けると、メインウィンドウのメッセージウィンドウに表示されます。

SOCKS を使う場合は、バージョン 5 の SOCKS サーバーを選んでください。バージョン 4 の SOCKS は ping をサポートしていません。

SOCKS を使って ping コマンドを実行した場合、**キャンセル**ボタンをクリックするまで icmp パケットを送り続けます。適当な結果が得られたら、**キャンセル**ボタンをクリックしてください。

13.1.4 Traceroute

図 13-3 に、 traceroute コマンドの引数を指定するためのダイアログを示します。

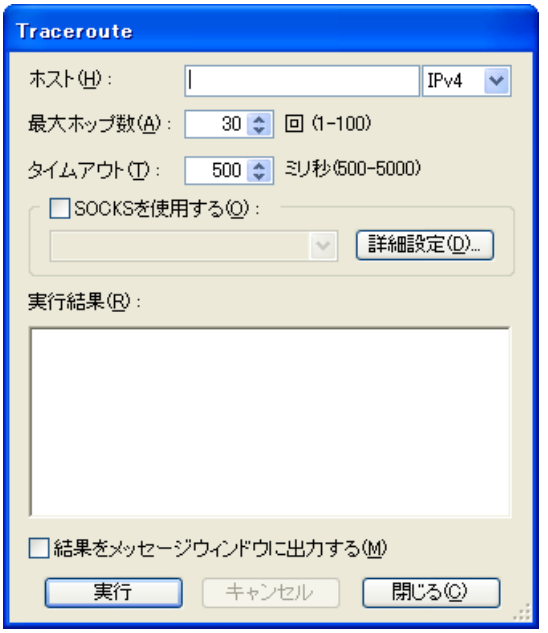


図 13-3: traceroute コマンドを実行するためのダイアログ

次の項目を設定して、**実行**ボタンをクリックするか、 **<Enter>** キーを押します。

ホスト(H)

指定したホストまでの経路を調べます。ホストやゲートウェイを指定します。 NetBIOS 名や DNS 名、 IP アドレスなど、ローカルホストが識別できる名前を入力します。

キー入力するか、または次に示す項目をドラッグして、ドロップします。

- 「IP 層発信元毎のトラフィック」、「IP 層受信先毎のトラフィック」、または「IP 層ホストペア毎のトラフィック」のグラフアイテム
- デコードビューおよびストリームビューのサマリ領域の IP アドレスが表示されている行
- IP アドレス表の行
- IP 層アドレス帳の行

IPv6 で ICMP パケットを送る場合は、**ホスト(H)** の右側にあるドロップダウンリストボックスから IPv6 を選びます。

最大ホップ数(A) ホップ回数の最大値を指定します。

SOCKS を使って LAN の外側にあるホストを対象とする場合は、指定できません。

タイムアウト(T) タイムアウトまでの時間をミリ秒で指定します。

SOCKS を使って LAN の外側にあるホストを対象とする場合は、指定できません。

SOCKS を使用する(O)

デフォルトでは、 SOCKS は使わないようになっています。 SOCKS を使う場合は、 **SOCKS を使用する(O)** にチェックを付けて、ドロップダウンリストボックスから SOCKS サーバーを選びます。

SOCKS サーバーを設定していない場合は、ドロップダウンリストボックスは空です。**詳細設定(D)**... ボタンをクリックして SOCKS サーバーを設定します。 SOCKS サーバーの設定については、「11.9 SOCKS のオプションを設定する」 (313 ページ) を参照してください。

結果をメッセージウィンドウに出力する(M)

チェックが付いていない場合、実行結果は**実行結果(R)** 領域に表示されます。チェックを付けると、メインウィンドウのメッセージウィンドウに表示されます。

SOCKS を使う場合は、バージョン 5 の SOCKS サーバーを選んでください。バージョン 4 の SOCKS は traceroute をサポートしていません。

13.2 ワークスペース

ASTEC Eyes でウィンドウを開く操作をした場合、ダイアログ以外の新しいウィンドウは、選択中のワークスペース内に現れます。

ワークスペースにフォーカスを移すには、ワークスペースをマウスでクリックするか、または **<Alt-0>** キーを押します。

ワークスペースは複数作ることができ、ワークスペース間でウィンドウを移動することもできます。ワークスペースは、ウィンドウを整理するのに役に立ちます。

この節では、ワークスペースの操作について説明します。

13.2.1 新しいワークスペースを作る

新しいワークスペースを作る方法は 3 通りあります。

- メインウィンドウの**表示(V)** メニューから**ワークスペースの追加(A)** を選びます。
- ワークスペース内のウィンドウが表示されていない部分、またはワークスペースのタブを右クリックしてポップアップメニューを開き、**ワークスペースの追加(A)** を選びます。
- ワークスペース内に表示されているウィンドウのタイトルバーを右クリックしてポップアップメニューを開き、**新しいワークスペース(N)** を選びます。
  この方法でワークスペースを作ると、右クリックしたウィンドウは、新たに作られたワークスペースに移動します。

新しいワークスペースが作られると、メインウィンドウの下の方に、新しいワークスペースのタブが追加されます。また、メインウィンドウの**表示(V)** メニューに新しいワークスペースを選ぶためのメニュー項目が追加されます。

13.2.2 ワークスペースを選ぶ

ワークスペースを選ぶ方法は 4 通りあります。

- 目的のワークスペースのタブをクリックします。
- メインウィンドウの**表示(V)** メニューから目的のワークスペースを選びます。
- ワークスペース内のウィンドウが表示されていない部分を右クリックしてポップアップメニューを開き、目的のワークスペースを選びます。
- **<Ctrl-Alt-←>** キー、 **<Ctrl-Alt-→>** キー、 **<Ctrl-PageUp>** キー、または **<Ctrl-PageDown>** キーを押します。

13.2.3 ウィンドウを別のワークスペースに移動する

ウィンドウを別のワークスペースに移動する方法は 2 通りあります。

- 移動したいウィンドウのタイトルバーを右クリックしてポップアップメニューを開き、移動先のワークスペースを選びます。
- 移動したいウィンドウをアクティブにし、メインウィンドウの**ウィンドウ(W)** メニューから**ワークスペースへ移動(M)** をポイントし、移動先のワークスペースを選びます。

13.2.4 ワークスペースのタブの位置を変える

ワークスペースのタブの位置は、デフォルトでは下ですが、上に変えられます。

1. メインウィンドウの**設定(O)** メニューから**オプション設定(O)**... を選びます。
2. ダイアログの左側にあるツリーの中の**その他**をクリックします。
3. **タブを上に配置する(U)** を選びます。
4. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

ワークスペースのタブの位置が上に替わります。下に戻したいときは、**タブを下に配置する(U)** を選びます。

13.2.5 ワークスペースのプロパティを変える

ワークスペースには、次のプロパティがあります。

ワークスペースのラベル
: 「ワークスペース 1」や「ワークスペース 2」に替わるラベル名を指定できます。

インタフェースの自動選択
: ワークスペースをインタフェースに関連付けておけば、そのワークスペースを選んだとき、関連付けられたインタフェースが自動的に選択された状態になります。

  インタフェースの選択については、「1.2.1 インタフェースを選ぶ」 (10 ページ) を参照してください。

ワークスペースのプロパティを変えるには、次のようにします。

1. ワークスペースを選びます。
2. ワークスペース内のウィンドウが表示されていない部分、またはワークスペースのタブを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
   図 13-4 に示すような「ワークスペースのプロパティ」ダイアログが現れます。

図 13-4: 「ワークスペースのプロパティ」ダイアログ

3. **ラベル(L)** に、ワークスペースのタブに表示したいラベル名を入力します。
4. ワークスペースをインタフェースに関連付けたいときは、**インタフェースに関連付ける(B)** にチェックを付け、ドロップダウンリストボックスからインタフェースを選びます。

13.2.6 ワークスペースを削除する

ワークスペースを削除する方法は 2 通りあります。

- 削除したいワークスペースに移動して、メインウィンドウの**表示(V)** メニューから**ワークスペースの削除(D)** を選びます。
- 削除したいワークスペースを選び、ワークスペース内のウィンドウが表示されていない部分、またはワークスペースのタブを右クリックしてポップアップメニューを開き、**ワークスペースの削除(D)** を選びます。

削除したいワークスペース内にウィンドウがある場合は、ワークスペースと同時にウィンドウも削除してよいかどうかをたずねる「ASTEC Eyes」ダイアログが現れます。

そのまま削除してもよい場合は、**OK** ボタンをクリックします。ワークスペース内にあるウィンドウとともにワークスペースが削除されます。

そうでない場合は、**キャンセル**ボタンをクリックして、いったん操作を中止し、必要なウィンドウを別のワークスペースに移動してからやり直します。

ワークスペースが 1 つしかないときは削除できません。

ワークスペースの数やプロパティ (ラベルおよびインタフェースの自動選択を行うかどうか) は、設定ファイルに保存できます。詳しくは「11.11　設定情報を保存する」 (318 ページ) を参照してください。

13.3 プロトコル情報

ASTEC Eyes がサポートしているプロトコルに関する次の情報を表示できます。

- プロトコルの簡略化していない名称
  モニタウィンドウやデコードビューのサマリ領域などでは、煩雑にならないように簡略化したプロトコル名を表示しています。
  たとえば、「Address Resolution Protocol」は、「ARP」と表示しています。プロトコルの仕様を調べる場合など、簡略化していない名称が役に立つことがあります。
- プロトコルの識別情報
  ASTEC Eyes はパケットを物理層に近い方 (Data Link Control プロトコル) から順に、プロトコルスタックに従って解析していきます。一般には、あるプロトコルのヘッダーを解析して、そのプロトコルのペイロード部分のプロトコルを判別します。たとえば、 DLC の Type フィールドの値が 0x800 であれば、 DLC の上位のプロトコルは IPv4 であると判別します。
  そのような判別の基準となる、
  - DLC の Type フィールドの値
  - IPv4 の Protocol フィールドの値
  - IPv6 の Next Header フィールドの値
  - TCP および UDP の Port Number フィールドの値

  を表示します。

プロトコル情報を表示するには、メインウィンドウの**ツール(T)** メニューから**プロトコル情報(I)**. . . を選びます。図 13-5 のような「プロトコル情報」ダイアログが現れて、プロトコル名と識別情報をプロトコル名順に表示します。

識別情報(D) を選ぶと、プロトコルの識別情報で分類しなおして、表示します。

プロトコル情報を選んだ状態　　識別情報を選んだ状態

図 13-5: 「プロトコル情報」ダイアログ

13.4 ウィンドウの操作

使っているうちに、モニタウィンドウやデコードビューなど、たくさんのウィンドウが開いてしまい、ウィンドウを見やすく整理したくなることがあるでしょう。

ワークスペース内のウィンドウを整理するには、メインウィンドウの**ウィンドウ(W)** メニューを使います。

新しいウィンドウを開く(N)
アクティブなウィンドウと同じ内容のウィンドウがもうひとつ現れます。

重ねて表示(C) すべてのウィンドウをタイトルが重ならないように並べます。

上下に並べて表示(H) または 左右に並べて表示(T)
選択中のワークスペース内のすべてのウィンドウが重ならないように、ウィンドウのサイズを変えて並べます。

アイコンの整列(A) アイコン化されているウィンドがある場合、ワークスペースの下の方にアイコンを整列します。

グラフサイズ(G)
ワークスペース内のすべてのグラフを指定したサイズに変更します。

ワークスペースへ移動(M)
アクティブなウィンドウを別のワークスペースへ移動します。

閉じる(L) アクティブなウィンドウを閉じます。

すべて閉じる(S) ワークスペース内のウィンドウを全て閉じます。

その他に、メインウィンドウの**ウィンドウ(W)** メニューには、選択中のワークスペース内にあるウィンドウに対応するメニュー項目があります。メニュー項目を選ぶと、選んだウィンドウがアクティブになります。

アイコンが別のウィンドウで隠されてしまうなどして直接クリックできなくなっているときは、**ウィンドウ(W)** から対応するメニュー項目を選ぶとよいでしょう。アイコン化されたウィンドウが元のサイズで表示されます。

13.5 インタフェースセレクタウィンドウのラベルを変える

インタフェースセレクタウィンドウに表示されているホストやインタフェース、ログ、連続キャプチャのエントリのラベルを分かりやすいものに変更できます。

13.5.1 ホストのエントリのラベルを変える

インタフェースセレクタウィンドウに表示されるホストのラベルは、ローカルホストの場合は `localhost`、リモートホストの場合は接続時に使ったホスト名になっています。これを変更できます。

1. インタフェースセレクタウィンドウ内のホストのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**... を選びます。
   図 13-6 のような「ホストのプロパティ」ダイアログが現れます。
2. **ラベル(L)** のテキストボックスに新しいラベルを入力します。
3. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

インタフェースツールバーに「ホストのプロパティ」ダイアログを表示するボタン () を追加することもできます。このボタン () を押したときにプロパティが表示されるホストは、選択中のインタフェースが属すホストです。
ツールバーのカスタマイズの方法について、詳しくは「1.1.1 ツールバー」 (6 ページ) を参照してください。

図 13-6: 「ホストのプロパティ」ダイアログ (「情報」のページ)

ラベルの他に、「情報」のページには

- ホスト名
- IP アドレス
- OS の種類
- キャプチャモジュールが起動された時刻

が表示されます。

13.5.2 インタフェースのエントリのラベルを変える

インタフェースセレクタウィンドウに表示されるインタフェースのラベルは、デフォルトでは MAC アドレスを含む文字列になっています。これを変更できます。

1. インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
   図 13-7 のような「インタフェースのプロパティ」ダイアログが現れます。
2. **ラベル(L)** のテキストボックスに新しいラベルを入力します。
3. **OK** ボタンまたは**適用(A)** ボタンをクリックします。
4. 設定権限があるときは、**ラベルをリモートモジュールに登録する(R)** ボタンをクリックできます。
   ラベルをリモートモジュールに登録する(R) ボタンをクリックすると、入力したラベルは ASTEC Eyes 基本パッケージまたはリモートモジュールのキャプチャモジュールに登録されます。そのため、 ASTEC Eyes を再起動したときやリモートモジュールに再接続したときも登録したラベルが使われます。また、他の PC で動作している ASTEC Eyes から接続したときも登録したラベルが使われます。

ローカルホストのホストのラベルとインタフェースのラベルは設定情報にも保存されます。設定情報に保存したインタフェースのラベルと**ラベルをリモートモジュールに登録する(R)** ボタンをクリックしてキャプチャモジュールに登録したインタフェースのラベルが異なる場合、設定情報に保存したラベルの方が優先されます。

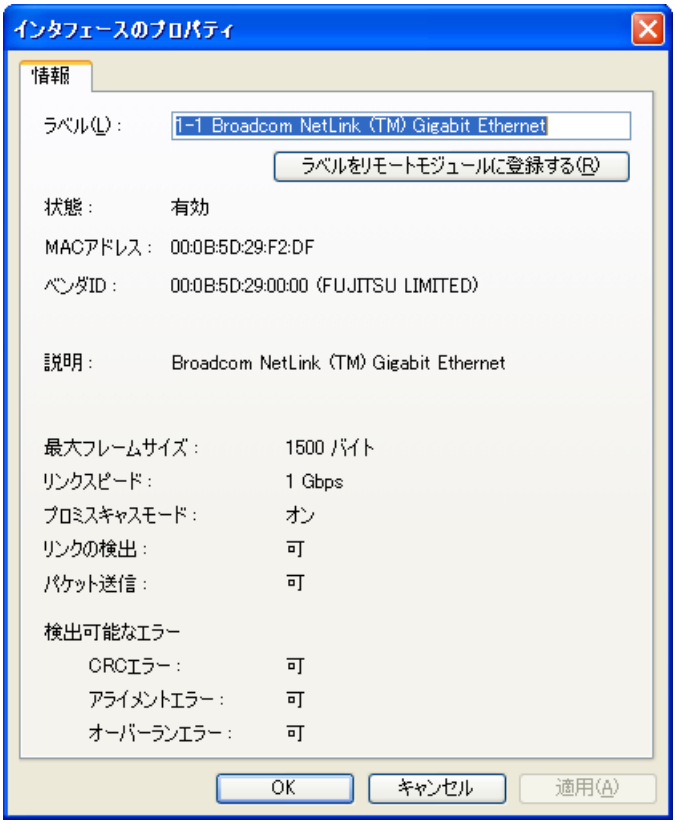


図 13-7: 「インタフェースのプロパティ」ダイアログ (「情報」のページ)

ラベルのほかに、「情報」のページには次のようなネットワークインタフェースカードに関する情報が表示されます。

- MAC アドレス
- ベンダ ID
- 最大フレームサイズ
- リンクスピード
- プロミスキャスモードの状態
- リンクの検出が可能かどうか
- 検出可能なエラー

13.5.3 ログのエントリのラベルを変える

インタフェースセレクタウィンドウに表示されるログのラベルは、デフォルトでは MAC アドレスを含む文字列になっています。これを変更できます。

1. インタフェースセレクタウィンドウ内のログのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
   図 13-8 のような「ログのプロパティ」ダイアログが現れます。
2. **ラベル(L)** のテキストボックスに新しいラベルを入力します。
3. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

図 13-8: 「ログのプロパティ」ダイアログ

NIC ID は、キャプチャモジュールが NIC を一意に識別できるように割り当てた ID です。

13.5.4 連続キャプチャデータのエントリのラベルを変える

インタフェースセレクタウィンドウに表示される連続キャプチャデータのラベルは、デフォルトでは `capture_data[id:N]` という文字列になっています。これを変更できます。

1. インタフェースセレクタウィンドウ内の連続キャプチャデータのエントリを右クリックしてポップアップメニューを開き、**プロパティ(P)**. . . を選びます。
   図 13-9 のような「連続キャプチャデータのプロパティ」ダイアログが現れます。
2. **ラベル(L)** のテキストボックスに新しいラベルを入力します。
3. **OK** ボタンまたは**適用(A)** ボタンをクリックします。

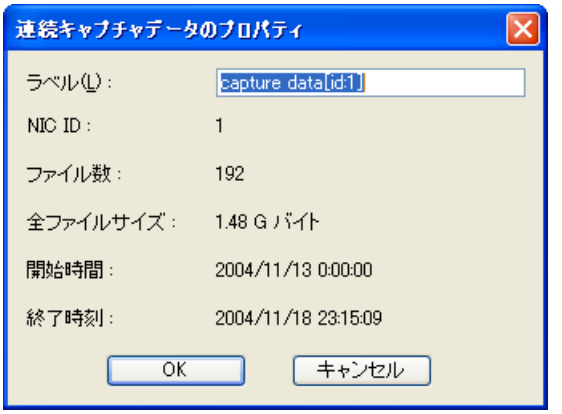


図 13-9: 「連続キャプチャデータのプロパティ」ダイアログ

NIC ID は、キャプチャモジュールが NIC を一意に識別できるように割り当てた ID です。

13.6 印刷

次に示すウィンドウの情報を印刷できます。

- モニタウィンドウに表示されているモニタ情報
- デコードビューまたはストリームビューに表示されているデコード結果
- IP 層アドレス帳および MAC 層アドレス帳に表示されているアドレスとホスト名の一覧

13.6.1 印刷する

印刷したいウィンドウをアクティブにし、メインウィンドウの**ファイル(F)** メニューから**印刷(P)**. . . を選ぶか、 **<Ctrl-P>** キーを押します。

モニタウィンドウおよびアドレス帳の場合は、「印刷」ダイアログが現れます。

デコードビューまたはストリームビューの場合は、図 13-10 のような「印刷内容」ダイアログが現れます。

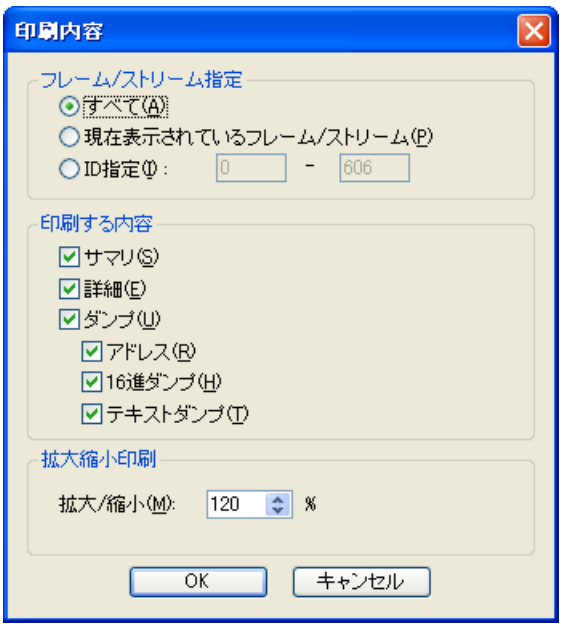


図 13-10: 「印刷内容」ダイアログ

1. **フレーム / ストリーム指定** 領域で、印刷する範囲を指定します。
   - **すべて(A)** を選ぶと、デコードビューの全パケットまたはストリームビューの全レコードを印刷します。
   - デコードビューまたはストリームビューにフィルタを適用して表示するパケットを絞り込んでいるような場合は、**現在表示されているフレーム / ストリーム(P)** を選ぶと、現在表示されているパケットまたはレコードだけを印刷します。
   - **ID 指定(I)** を選んだ場合は、フレーム ID またはストリーム ID で印刷する範囲を指定します。
2. **印刷する内容** 領域で、印刷したい領域にチェックを付けます。印刷したくない領域からはチェックを外します。
3. 拡大または縮小率を変えると、フォントの大きさが変わります。
4. **OK** ボタンをクリックすると「印刷」ダイアログが現れます。

13.6.2 プレビューする

印刷する前に、どのように印刷されるのかを確認できます。

メインウィンドウの**ファイル(F)** メニューから**印刷プレビュー(V)**... を選びます。

モニタウィンドウまたはアドレス帳の場合は、直ちにメインウィンドウ全体がプレビュー表示に変わります。

デコードビューまたはストリームビューの場合は、**印刷(P)**... を選んだときと同じように、「印刷内容」ダイアログが現れます。「印刷内容」ダイアログで必要な設定を行い、 **OK** ボタンをクリックすると、プレビュー表示に変わります。

通常の表示に戻すには、**閉じる(C)** ボタンをクリックするか、 **<Esc>** キーを押します。

13.7 ASTEC Eyes が異常終了する場合

ASTEC Eyes を使いつづけるうち、まれに PC の使用可能なメモリが極端に少なくなったり、致命的なエラーが起きることがあります。このような場合、 ASTEC Eyes は次のようなダイアログを表示します。

図 13-11: 異常時に現れるダイアログ

OK ボタンをクリックすると、異常な状態に関する情報を ASTEC Eyes をインストールしたディレクトリの **Emergency.log** というファイルに書き出した後、 ASTEC Eyes は終了します。

Emergency.log を添えて、サポートまでご連絡ください。

付録 A

ASTEC Eyesの時間

ASTEC Eyes で表示する時間は、表示する箇所により基準が異なります。

デコードで表示するキャプチャ時間

通常のキャプチャや連続キャプチャのデコード結果やリアルタイムデコードのキャプチャ時間 (パケットに付与される時間) は、すべてキャプチャした計算機のローカルな時間です。

キャプチャしたときのタイムゾーンや夏時間の設定は ASTEC Eyes ではわかりません。

モニタのグラフや表の時間

GUI が動作する PC のローカルの時間で表示します。

異なるタイムゾーンで動作するリモートモジュールのモニタであっても GUI が動作する PC のローカルな時間で表示します。

ログのグラフや表の時間

ログを取得した計算機のローカルな時間です。

キャプチャデータを基にしたグラフや表の時間

キャプチャした計算機のローカルな時間です。

イベントの時間

イベントを検知した計算機のローカルな時間です。

異なるタイムゾーンで動作するリモートモジュールで検知した場合は、現地の時間です。

キャプチャ時間の同期

タイムゾーンや夏時間を考慮して同期します。

たとえば、日本の GUI と時差 -1 時間のシンガポールのリモートモジュールで同期を行った場合は、 GUI で 3 時ならモートモジュールは 2 時 (現地のタイムゾーンで) で同期することになります。

付録 B

ツールバー、ポップアップメニュー、キーバインド一覧

B.1 ツールバー

B.1.1 メインウィンドウのツールバー

ASTEC Eyes の操作には、ネットワークインタフェースに関係なく行う操作と、ネットワークインタフェースごとに行う操作があります。

メインウィンドウには、 2 種類のツールバーがあります。コモンツールバーとインタフェースツールバーです。図 B-1 に 2 つのツールバーを示します。

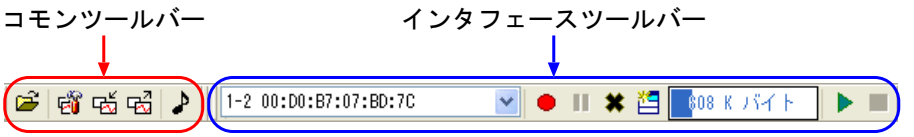


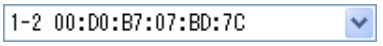
図 B-1: メインウィンドウの 2 つのツールバー

コモンツールバーには、選択中のネットワークインタフェースに依存しない操作を行うボタンがあります。**インタフェースツールバー**には、選択中のネットワークインタフェースに対して操作を行うボタンがあります。コモンツールバーとインタフェースツールバーに置くボタンはカスタマイズできます。

表 B-1: デフォルトでコモンツールバーにあるボタン

ボタン	アイコン	機能
キャプチャデータを開く		ファイルに保存してあるキャプチャデータを開いてデコードし、デコードビューを表示します。
オプション設定		「オプション設定」ダイアログを開きます。
設定情報の読み込み		設定情報を読み込みます。
設定情報の保存		設定情報を保存します。
音声データ送信		「通話シミュレーション」ダイアログを開きます。 ASTEC Eyes *for* VoIP の機能です。

表 B-2: デフォルトでインタフェースツールバーにあるボタン

ボタン	アイコン	機能
キャプチャ開始		キャプチャを開始します。
キャプチャ停止		キャプチャを停止します。
キャプチャデータの削除		キャプチャバッファのデータを削除します。
デコードビュー作成		キャプチャバッファのデータをデコードしデコードビューを表示します。
モニタ開始		モニタを開始します。
モニタ停止		モニタを停止します。
インタフェース選択リスト		操作の対象とするインタフェースを選びます。

コモンツールバーとインタフェースツールバーのカスタマイズ

コモンツールバーとインタフェースツールバーはカスタマイズできます。よく使う機能をツールバーに追加し、あまり使わない機能のボタンを削除できます。

ツールバーをカスタマイズするには、「ツールバーの変更」ダイアログを使います。

- コモンツールバーをカスタマイズするための「ツールバーの変更」ダイアログを開く方法は 2 通りあります。
  - メインウィンドウの**設定(O)** メニューから**コモンツールバーの設定(C)**... を選びます。

- コモンツールバーを右クリックしてポップアップメニューを開き、**コモンツールバーの設定**... を選びます。

- インタフェースツールバーをカスタマイズするための「ツールバーの変更」ダイアログを開く方法は 2 通りあります。
  - メインウィンドウの**設定(O)** メニューから**インタフェースツールバーの設定(I)**... を選びます。
  - インタフェースツールバーを右クリックしてポップアップメニューを開き、**インタフェースツールバーの設定**... を選びます。

B.1.2 トラフィックウィンドウのツールバー

表 B-3: トラフィックウィンドウのツールバーのボタン

ボタン	アイコン	機能
タイムスパン切り替え	S M L	タイムスパンを切り替えます。クリックするたびに、短期、中期、長期の 3 つのタイムスパンが切り替わります。
折れ線グラフ (履歴)		折れ線グラフ形式に切り替えます。
棒グラフ (トータル)		棒グラフ形式に切り替えます。
円グラフ (比率)		円グラフ形式に切り替えます。
表 (詳細)		表形式に切り替えます。
凡例		凡例の表示、非表示を切り替えます。
積み重ね折れ線グラフ		折れ線グラフの表示を標準か、積み重ね形式にするかを切り替えます。
キャプチャデータインディケータ		キャプチャデータインディケータの表示、非表示を切り替えます。
モニタフィルタ		モニタフィルタを適用または解除します。サブメニューから適用したいモニタフィルタまたは**フィルタ解除(R)** を選びます。
Y 軸の範囲		このボタンを押すと、トラフィックウィンドウ上に水平カーソルが現れます。マウスを上下にドラッグして、表示したい Y 軸の範囲を指定します。

次ページへ続く

ボタン	アイコン	機能
グラフ解析機能		グラフの値を読み取る状態になり、グラフは更新されなくなります。トグルボタンになっています。
垂直カーソル		トラフィックウィンドウ上に垂直カーソルが現れます。グラフの値を読み取る状態のときだけクリックできます。
水平カーソル		トラフィックウィンドウ上に水平カーソルが現れます。グラフの値を読み取る状態のときだけクリックできます。
デコードビュー作成		ログと連続キャプチャデータが関連付けられており、ログを表示しているトラフィックウィンドウがグラフの値を読み取る状態にあるとき、垂直カーソルで選んだ範囲内に連続キャプチャデータがある場合にクリックできます。クリックすると、指定時間範囲のデータをデコードし、デコード結果をデコードビューに表示します。詳しくは、「6.12　ログのウィンドウで範囲を指定してデコードする」 (169 ページ) を参照してください。

B.1.3　リアルタイムデコードビューのツールバー

表 B-4: リアルタイムデコードビューのツールバーのボタン

ボタン	アイコン	機能
最新のパケットを選択		トグルボタンになっています。 新しくキャプチャしたパケットはリアルタイムデコードビューの最後尾に追加され、常に最新のパケットを表示します。
全パケットを消去		リアルタイムデコードビュー上のすべてのパケットを削除します。
選択まで削除		選択行を含みそれよりも前のパケットを削除します。
デコードビュー表示 (パケット削除)		デコードビューを開き、詳細な解析結果を表示します。リアルタイムデコードビューのパケットは削除されます。

次ページへ続く

ボタン	アイコン	機能
デコードビュー表示		デコードビューを開き、詳細な解析結果を表示します。リアルタイムデコードビューのパケットは削除されず、そのまま残ります。
フィルタ解除		適用されている簡易フィルタをすべて解除します。
ホスト名の更新		新たにホスト名が見つかった場合やホスト名の表示の優先順位を変えた場合、アドレス帳を編集した場合など、リアルタイムデコードビューに表示されているホスト名を最新のものに更新します。
次のドロップ		キャプチャし損ねて取りこぼしたパケットの直後のパケットは、オレンジ色にハイライト表示されます。このボタンをクリックすると次のオレンジ色の行にフォーカスを移動します。

B.1.4 デコードビューとストリームビューのツールバー

ストリームビューのツールバーにあるボタンはモードによって異なります。

表 B-5: デコードビューとストリームビュー (シーケンスモードでない場合) のツールバーのボタン

ボタン	アイコン	機能
拡大表示		トグルボタンになっています。 サマリ領域、デコード結果領域、ダンプ領域の 3 つの領域が表示されている場合は、フォーカスのある領域だけをウィンドウいっぱいに拡張します。 逆に、 1 つの領域だけがウィンドウいっぱいに拡張されている場合は、 3 つの領域がすべて表示されるようにします。
サマリ領域		サマリ領域の表示と非表示を切り替えます。
デコード結果領域		デコード結果領域の表示と非表示を切り替えます。
ダンプ領域		ダンプ領域の表示と非表示を切り替えます。

次ページへ続く

ボタン	アイコン	機能
ヘッダー属性フィルタ		デコードビューだけにあります。ヘッダー属性フィルタのメニューを開きます。詳しくは「6.6.2　ヘッダー属性フィルタ」 (130 ページ) を参照してください。
デコード結果フィルタ		「デコード結果フィルタ」ダイアログを開きます。詳しくは「6.6.3　デコード結果フィルタ」 (132 ページ) を参照してください。
フィルタ解除		適用されている簡易フィルタをすべて解除します。
ディスプレイフィルタ		デコードビューだけにあります。定義されているディスプレイフィルタ名の一覧をメニュー項目とするメニューが現れます。 メニューから望みのフィルタ名を選ぶと、フィルタに指定した論理式が真になるパケットだけを表示したデコードビューが新たに現れます。 詳しくは「6.6.8　ディスプレイフィルタ」 (137 ページ) を参照してください。
ストリームビュー		デコードビューだけにあります。対応するストリームビューをアクティブにします。
ストリームビュー (シーケンスモード)		デコードビューだけにあります。対応するシーケンスモードのストリームビューをアクティブにします。
デコードビュー		ストリームビューだけにあります。対応するデコードビューをアクティブにします。
統計情報の表示		デコードビューだけにあります。デコードしたデータについて統計処理を行い、その結果をグラフや表 (モニタウィンドウ) に表示します。
イベントビューア		デコードビューだけにあります。デコード時に見つけたデコードイベントを表示するイベントビューアを開きます。
音声品質の表示		デコードビューだけにあります。 RTP パケットのデータから音声品質を計算し、グラフや表に表示します。 ASTEC Eyes *for* VoIP の機能です。

次ページへ続く

ボタン	アイコン	機能
シーケンス表示		デコードビューだけにあります。 VoIP のシーケンスを表示する「シーケンス表示」ウィンドウを開きます。 ASTEC Eyes *for* VoIP の機能です。
音声再生		デコードビューだけにあります。 RTP パケットのデータから音声データを再構成し、「音声再生」ウィンドウを開きます。 ASTEC Eyes *for* VoIP の VoIP Player オプションの機能です。
ホスト名の更新		新たにホスト名が見つかった場合やホスト名の表示の優先順位を変えた場合、アドレス帳を編集した場合など、デコードビューまたはストリームビューに表示されているホスト名を最新のものに更新します。
再デコード		変更されたオプションを反映させるためにデコードをやり直します。次のオプションを変更したときに再デコードが必要です。 • デコードヒント • チェックサム値の検出 • ストリームビューのレコードの並び順
パケット編集ウィンドウ		デコードビューだけにあります。トラフィックジェネレータのためのパケット編集ウィンドウを開きます。

表 B-6: ストリームビュー (シーケンスモード) のツールバーのボタン

ボタン	アイコン	機能
拡大表示		トグルボタンになっています。 セッションリスト領域、シーケンス領域、デコード結果領域の 3 つの領域が表示されている場合は、フォーカスのある領域だけをウィンドウいっぱいに拡張します。 逆に、 1 つの領域だけがウィンドウいっぱいに拡張されている場合は、 3 つの領域がすべて表示されるようにします。

次ページへ続く

ボタン	アイコン	機能
セッションリスト領域		サマリ領域の表示と非表示を切り替えます。
シーケンス領域		シーケンス領域の表示と非表示を切り替えます。
デコード結果領域		デコード結果領域の表示と非表示を切り替えます。
フィルタ解除		適用されている簡易フィルタをすべて解除します。
ひとつ前のセッション		ひとつ前のセッションにフォーカスを移動します。
次のセッション		次のセッションにフォーカスを移動します。
前のエラー		前のエラーのレコードにフォーカスを移動します。
次のエラー		次のエラーのレコードにフォーカスを移動します。

B.1.5 パケット編集ウィンドウのツールバー

表 B-7: パケット編集ウィンドウのツールバーのボタン

ボタン	アイコン	機能
パケット送信		パケットを送信するためのダイアログボックスを開きます。
パケット編集ツール		パケット編集ツールを開きます。 アドレスや特定のプロトコルのフィールドの内容をまとめて変更できます。
元に戻す		編集した内容を取り消して元に戻します。
やり直し		取り消した編集を再度実行します。
拡大表示		トグルボタンになっています。 サマリ領域、デコード結果領域、ダンプ領域の 3 つの領域が表示されている場合は、フォーカスのある領域だけをウィンドウいっぱいに拡張します。 逆に、1 つの領域だけがウィンドウいっぱいに拡張されている場合は、3 つの領域がすべて表示されるようにします。

次ページへ続く

ボタン	アイコン	機能
サマリ領域		サマリ領域の表示と非表示を切り替えます。
デコード結果領域		デコード結果領域の表示と非表示を切り替えます。
ダンプ領域		ダンプ領域の表示と非表示を切り替えます。
ヘッダー属性フィルタ		ヘッダー属性フィルタのメニューを開きます。詳しくは「6.6.2　ヘッダー属性フィルタ」 (130 ページ) を参照してください。
デコード結果フィルタ		「デコード結果フィルタ」ダイアログを開きます。詳しくは「6.6.3　デコード結果フィルタ」 (132 ページ) を参照してください。
フィルタ解除		適用されている簡易フィルタをすべて解除します。
再デコード		変更されたオプションを反映させるためにデコードをやり直します。次のオプションを変更したときに再デコードが必要です。 • デコードヒント • チェックサム値の検出

B.1.6　イベントビューアのツールバー

表 B-8: イベントビューアのツールバーのボタン

ボタン	アイコン	機能
折れ線グラフ (履歴)		折れ線グラフ形式に切り替えます。
表 (詳細)		表形式に切り替えます。
凡例		折れ線グラフ形式のとき、凡例の表示、非表示を切り替えます。
フィルタ解除		適用されている見出しフィルタをすべて解除します。

B.2 ポップアップメニュー

B.2.1 IP アドレス表のポップアップメニュー

IP アドレス表を右クリックすると現れます。

ホスト名の検索(H)
選択中の行のホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

ネットワークユーティリティ(N)
whois、 ping、および traceroute コマンドを使うためのダイアログを開きます。詳しくは「13.1 ネットワークユーティリティ」 (340 ページ) を参照してください。

ポートの状態一覧(S)
「ポートの状態一覧」ダイアログを開きます。右クリックした行のホストが開いているポートに関してネットワークのパケットから得られた情報を表示します。詳しくは「2.9 ホストごとのポートの状態を表示する」 (46 ページ) を参照してください。

すべてコピー(W) 表示されているすべての IP アドレスとホスト名をクリップボードにコピーします。

整列(A) 表示されている行を並べ替えるためのサブメニューが現れます。

- **IP アドレス順(I)** 各行を IP アドレス順に並べ替えます。
- **ホスト名順(H)** 各行をホスト名順に並べ替えます。

B.2.2 IP 層アドレス帳のポップアップメニュー

IP 層アドレス帳のウィンドウ内を右クリックすると現れます。

アドレス帳のポップアップメニューは、クリックした位置 (行やセル) によってメニュー項目や動作が異なります。

編集(E) ユーザー定義名のセルをクリックした場合は、ドロップダウンコンボボックスが現れ、ホスト名を入力したり選んだりできる状態になります。

複数の候補があるホスト名のセルをクリックした場合は、ドロップダウンリストボックスが現れ、ホスト名を選べる状態になります。

それ以外の場合は、選べないようになっています。

名前の削除(D) 表示されているホスト名を削除します。

ホスト名の検索(H)

選択中の行のホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

ネットワークユーティリティ(N)

whois、 ping、および traceroute コマンドを使うためのダイアログを開きます。詳しくは「13.1　ネットワークユーティリティ」 (340 ページ) を参照してください。

表示の優先順位を設定(P). . .

「表示する名前と優先順位」ダイアログを開きます。

チェックのついているホスト名に対応するカラムだけがアドレス帳で有効になります。また、アドレス帳のカラムは左から優先順位の高い順に並びます。

すべてコピー(W) 表示されているすべての IP アドレスとホスト名をクリップボードにコピーします。

最新の情報に更新(R) 表示されている情報を、ただちに最新のものに更新します。

表示(V) 表示を切り替えるための、サブメニューが現れます。

- **一覧(L)** ホスト名と候補数 (複数のホスト名の候補がある場合) だけを表示します。デフォルトの表示形式です。
- **詳細(D)** ホスト名、ホスト名の候補数、およびホスト名を得た方法を表示します。
- **各桁を揃える(A)** IP アドレスの各桁を揃えます。

整列(A) 表示されている行を並べ替えるためのサブメニューが現れます。

- **アドレス順(A)** 各行をアドレス順に並べ替えます。
- **ホスト名順(H)** 各行をホスト名順に並べ替えます。
- **ユーザー定義名順(U)** 各行をユーザー定義名順に並べ替えます。

NetBIOS 名順(B) 各行を NetBIOS 名順に並べ替えます。

NIS 名順(N) 各行を NIS 名順に並べ替えます。

DNS 名順(D) 各行を DNS 名順に並べ替えます。

DNS 名のトップレベル順(T)
各行を DNS 名のトップレベルの方からアルファベット順に並べ替えます。

「各桁を揃える」と、

```
111.222.33.44
55.66.77.88
```

という表示が、

```
111.222. 33. 44
 55. 66. 77. 88
```

のように変わります。

最新の情報に更新(R) を選ばなくても、 IP 層アドレス帳に表示されている情報は、モニタウィンドウの更新間隔ごとに更新されます。また、モニタ中にホスト名が見つかった場合にも更新されます。

B.2.3 MAC アドレス - IP アドレス対応表 のポップアップメニュー

MAC アドレス - IP アドレス対応表 を右クリックすると現れます。

ホスト名の検索(H)
選択中の行のホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

ネットワークユーティリティ(N)
whois、 ping、および traceroute コマンドを使うためのダイアログを開きます。詳しくは「13.1 ネットワークユーティリティ」 (340 ページ) を参照してください。

ポートの状態一覧(S)
「ポートの状態一覧」ダイアログを開きます。右クリックした行のホストが開いているポートに関してネットワークのパケットから得られた情報を

表示します。詳しくは「2.9　ホストごとのポートの状態を表示する」 (46 ページ) を参照してください。

すべてコピー(W) 表示されているすべての MAC アドレス、ベンダ名、 IP アドレス、およびホスト名をクリップボードにコピーします。

整列(A) 表示されている行を並べ替えるためのサブメニューが現れます。

MAC アドレス順(M) 各行を MAC アドレス順に並べ替えます。

ベンダー名順(V) 各行をベンダー名順に並べ替えます。

IP アドレス順(I) 各行を IP アドレス順に並べ替えます。

ホスト名順(H) 各行をホスト名順に並べ替えます。

B.2.4　MAC アドレス表のポップアップメニュー

MAC アドレス表を右クリックすると現れます。

すべてコピー(W) 表示されているすべての MAC アドレスとそのベンダ名、ホスト名をクリップボードにコピーします。

整列(A) 表示されている行を並べ替えるためのサブメニューが現れます。

MAC アドレス順(M) 各行を MAC アドレス順に並べ替えます。

ベンダー名順(V) 各行をベンダー名順に並べ替えます。

ホスト名順(H) 各行をホスト名順に並べ替えます。

B.2.5　MAC 層アドレス帳のポップアップメニュー

MAC 層アドレス帳のウィンドウ内を右クリックすると現れます。

アドレス帳のウィンドウ内を右クリックすると現れます。

アドレス帳のポップアップメニューは、クリックした位置 (行やセル) によってメニュー項目や動作が異なります。

編集(E) ユーザー定義名のセルをクリックした場合は、ドロップダウンコンボボックスが現れ、ホスト名を入力したり選んだりできる状態になります。

複数の候補があるホスト名のセルをクリックした場合は、ドロップダウンリストボックスが現れ、ホスト名を選べる状態になります。

それ以外の場合は、選べないようになっています。

名前の削除(D) 表示されているホスト名を削除します。

表示の優先順位を設定(P)...
「表示する名前と優先順位」ダイアログを開きます。

チェックのついているホスト名に対応するカラムだけがアドレス帳で有効になります。また、アドレス帳のカラムは左から優先順位の高い順に並びます。

すべてコピー(W) すべての MAC アドレスとホスト名をクリップボードにコピーします。

最新の情報に更新(R)
表示されている情報を、ただちに最新のものに更新します。

表示(V) 表示を切り替えるための、サブメニューが現れます。

- **一覧(L)** ホスト名と候補数 (複数のホスト名の候補がある場合) だけを表示します。デフォルトの表示形式です。
- **詳細(D)** ホスト名、ホスト名の候補数、およびホスト名を得た方法を表示します。

整列(A) 表示されている行を並べ替えるためのサブメニューが現れます。

- **アドレス順(A)** 各行をアドレス順に並べ替えます。
- **ベンダー名順(V)** 各行をベンダー名順に並べ替えます。
- **ホスト名順(H)** 各行をホスト名順に並べ替えます。
- **ユーザー定義名順(U)** 各行をユーザー定義名順に並べ替えます。
- **NetBIOS 名順(B)** 各行を NetBIOS 名順に並べ替えます。

最新の情報に更新(R) を選ばなくても、 MAC 層アドレス帳に表示されている情報は、モニタウィンドウの更新間隔ごとに更新されます。また、モニタ中にホスト名が見つかった場合にも更新されます。

B.2.6 「TCP ステータス情報」のウィンドウのポップアップメニュー

「TCP ステータス情報」のウィンドウ内を右クリックすると現れます。

すべてコピー(W) 表示されているすべての行をクリップボードにコピーします。

ホスト名の検索(H)

選択中の行のホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

B.2.7 イベントビューアのポップアップメニュー

イベントビューアを右クリックすると現れます。

†のついている項目は表形式のときのみ現れます。
‡のついている項目は折れ線グラフ形式のときのみ現れます。

ホスト名の検索(H)†

選択中の行のホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

他を隠す(M)‡ 選択中のグラフアイテムだけを表示し、それ以外のグラフアイテムは非表示にします。

元のグラフに戻る(B)‡

表示するグラフアイテムを制限している場合のみ選べます。元のグラフに戻ります。

色の設定(C)...‡ 選択中のグラフアイテムの色を変えるための「色の設定」ダイアログを開きます。

表示形式(V) 表示形式を切り替えます。サブメニューから**折れ線グラフ(H)** と**表形式(T)** を選びます。

凡例(G)‡ 凡例の表示と非表示を切り替えます。

履歴を表示(H)‡ 1000 件分を上限として、記録されているイベントをすべて表示するように、表示期間を切り替えます。

フィルタ解除(R)† 表形式のときのみ選べます。適用されている見出しフィルタをすべて解除します。

集約表示(C)† 集約された表示と展開された表示を切り替えます。集約表示にすると、イベントと発信元、および受信先が同じで、発生した時刻だけが異なるイベントをまとめて表示します。このメニュー項目は、トグルになっています。メニュー項目にチェックが付いているときは、集約表示です。

すべてコピー(W)† 表形式のときのみ選べます。表示されているすべてのイベントとその付属の情報をクリップボードにコピーします。

ツールバーの表示(T)
ツールバーの表示と非表示を切り替えます。

B.2.8 インタフェースセレクタウィンドウのポップアップメニュー

インタフェースセレクタウィンドウ内の何も表示されていない部分を右クリックすると現れます。

リモートへの接続(C)...
リモートモジュールに接続するための 「接続」ダイアログを開きます。

ログのディレクトリを開く(L)...
ログのディレクトリを開くための「ディレクトリの参照」ダイアログを開きます。

連続キャプチャのディレクトリを開く(J)...
連続キャプチャデータのディレクトリを開くための「ディレクトリの参照」ダイアログを開きます。

キャプチャ時間を取得(T)
接続中のすべてのリモートモジュールおよびキャプチャ部について、キャプチャしたパケットに付与する時間を取得します。メッセージウィンドウに GUI が動作する PC の時間との差を表示します。

キャプチャ時間を同期(Y)†
接続中で設定権限のあるすべてのリモートモジュールおよびキャプチャ部について、キャプチャしたパケットに付与する時間を GUI が動作する PC の時間と同期します。

キャプチャ時間の同期を解除(R)†
接続中で設定権限のあるすべてのリモートモジュールおよびキャプチャ部について、パケットに付与する時間と GUI が動作する PC の時間の同期を解除します。

B.2.9 ホストのエントリのポップアップメニュー

インタフェースセレクタウィンドウのホストのエントリを右クリックすると現れます。

†のついた項目は、設定権限が必要です。

接続(C) リモートモジュールに再接続します。接続に成功すると、**使えない状態にあることを示す** (✕) が消えます。

切断(S) リモートモジュールとの接続を切断します。切断すると、そのホストのインタフェースに対する操作 (モニタやキャプチャなど) は何もできなくなります。また、ホストとそのインタフェースのアイコン上に**使えない状態にあることを示す** (✕) が重なって表示されます。

削除(D) 切断された状態のリモートモジュールのホストのエントリをインタフェースセレクタウィンドウから削除します。

設定権限を取得(G) 設定権限を取得します。

設定権限が得られると、インタフェースセレクタウィンドウに表示されるアイコンは**設定権限のあるホスト** () に変わります。

設定権限を解放(F) 設定権限を解放します。

設定権限を解放すると、他の ASTEC Eyes が設定権限を取得できるようになり、インタフェースセレクタウィンドウに表示されるアイコンは**設定権限のないホスト** () に変わります。

ログの一覧を作成(L)

「ホストのプロパティ」ダイアログの「ログ」のページで指定したディレクトリにあるログファイルを解析します。連続キャプチャデータの一覧ができているときは、連続キャプチャデータとの関連付けを行います。ログについては、 3 章「ログ機能」 (52 ページ) を参照してください。

ログの一覧を閉じる(X) インタフェースセレクタウィンドウからログのエントリを削除します。

連続キャプチャデータの一覧を作成(A)

「ホストのプロパティ」ダイアログの「連続キャプチャ」のページで指定したディレクトリの連続キャプチャデータを解析します。ログの一覧ができているときは、ログとの関連付けを行います。連続キャプチャデータのデコードについては、「6.11　連続キャプチャデータをデコードする」 (164 ページ) および「6.12　ログのウィンドウで範囲を指定してデコードする」 (169 ページ) を参照してください。

連続キャプチャデータの一覧を閉じる(Z)
インタフェースセレクタウィンドウから連続キャプチャデータのエントリを削除します。

キャプチャ時間を取得(T)
リモートモジュールもしくはキャプチャ部がキャプチャしたパケットに付与する時間を取得します。メッセージウィンドウに GUI が動作する PC の時間との差を表示します。

キャプチャ時間を同期(Y)†
リモートモジュールもしくはキャプチャ部がキャプチャしたパケットに付与する時間を GUI が動作する PC の時間と同期します。

キャプチャ時間の同期を解除(R)†
リモートモジュールもしくはキャプチャ部がキャプチャしたパケットに付与する時間と GUI が動作する PC の時間の同期を解除します。

プロパティ(P)... 「ホストのプロパティ」ダイアログを開きます。
「ホストのプロパティ」ダイアログでは、ログ、連続キャプチャ、エキスパート、および通知機能の設定ができます。

B.2.10 インタフェースのエントリのポップアップメニュー

インタフェースセレクタウィンドウ内のインタフェースのエントリを右クリックすると現れます。

†のついた項目は、設定権限が必要です。

キャプチャ開始(S) キャプチャを開始します。

キャプチャ停止(I) キャプチャを停止します。

クイックリターン(Q)
キャプチャを停止し、キャプチャバッファのデータをコピーし、キャプチャバッファのデータを削除して、直ちにキャプチャを再開します。コピーしたキャプチャデータはデコードされ、デコード結果はデコードビューに表示されます。

キャプチャデータの削除(A) キャプチャバッファのデータを削除します。

デコードビュー(N)
キャプチャバッファのデータをデコードし、デコードビューを生成します。

リアルタイムデコードビュー(V)
リアルタイムデコードビューを開き、リアルタイムにデコードした結果を表示します。

モニタ開始(B) モニタを開始します。

モニタ停止(T) モニタを停止します。

モニタリセット(R)† モニタをリセットします。

モニタフィルタ(F) モニタフィルタを適用または解除します。サブメニューから適用したいモニタフィルタまたは**フィルタ解除(R)** を選びます。

モニタウィンドウ(M)
メインウィンドウの**モニタ(M)** メニューと同じ項目を持つサブメニューが現れます。サブメニューから項目を選ぶと、選んだ項目に対応するウィンドウが現れます。

インタフェースを有効にする(W)†
インタフェースを使えるようにします。

インタフェースを無効にする(D)†
インタフェースを使えないようにします。

プロパティ(P)... 「インタフェースのプロパティ」ダイアログを開きます。

B.2.11 ウィンドウのタイトルバーのポップアップメニュー

ワークスペース内に表示されているウィンドウのタイトルバーを右クリックすると現れます。

ポップアップメニューには、**新しいワークスペース(N)** と既存のワークスペースに対応するメニュー項目があります。

既存のワークスペースに対応するメニュー項目を選ぶと、クリックされたウィンドウが選んだワークスペースに移動します。

新しいワークスペース(N) を選ぶと、新しいワークスペースが追加され、クリックされたウィンドウが新しいワークスペースに移動します。

B.2.12 ツールバーとグリップバーのポップアップメニュー

メインウィンドウの コモンツールバー、インタフェースツールバー、インタフェースセレクタウィンドウのグリップバー、およびメッセージウィンドウのグリップバーを右クリックすると現れます。

コモンツールバーの設定...
「ツールバーの変更」ダイアログを開きます。コモンツールバーをクリックした場合にだけあります。

インタフェースツールバーの設定...
「ツールバーの変更」ダイアログを開きます。インタフェースツールバーをクリックした場合にだけあります。

インタフェースセレクタ
インタフェースセレクタウィンドウの表示、非表示を切り替えます。

メッセージウィンドウ
メッセージウィンドウの表示、非表示を切り替えます。

コモンツールバー
コモンツールバーの表示、非表示を切り替えます。

インタフェースツールバー
インタフェースツールバーの表示、非表示を切り替えます。

B.2.13 デコードビューとストリームビューのポップアップメニュー

デコードビューまたはストリームビューを右クリックすると現れます。ストリームビューのポップアップメニューはモードによって異なります。デコードビューまたはストリームビュー (シーケンスモードでない場合) には、次のポップアップメニューが現れます。

†のついている項目はデコードビューのポップアップメニューだけにあります。
‡のついている項目はストリームビュー (シーケンスモードでない場合) のポップアップメニューだけにあります。

表示(V) 次をメニュー項目とするサブメニューが現れます。

拡大表示(M) フォーカスのある領域を拡大します。フォーカスのない領域は見えなくなります。

サマリ領域(S) サマリ領域の表示、非表示を切り替えます。

デコード結果領域(R)
デコード結果領域の表示、非表示を切り替えます。

ダンプ領域(D) ダンプ領域の表示、非表示を切り替えます。

フィルタ(F)

ヘッダー属性フィルタ(A)
ヘッダー属性フィルタを使うためのメニューが現れます。詳しくは「6.6.2 ヘッダー属性フィルタ」 (130 ページ) を参照してください。

デコード結果フィルタ(F)...
「デコード結果フィルタ」ダイアログを開きます。詳しくは「6.6.3 デコード結果フィルタ」 (132 ページ) を参照してください。

フィルタ解除(R) 適用されている簡易フィルタをすべて解除します。

ディスプレイフィルタ(D)
定義されているディスプレイフィルタ名をメニュー項目とするメニューが現れます。項目を選ぶと、選んだディスプレイフィルタを適用したデコードビューが現れます。

フィルタの生成(I) ディスプレイフィルタを自動的に生成するためのサブメニューが現れます。

- **一時的に生成して適用する(I)**
  ディスプレイフィルタの条件となる論理式を生成し、ディスプレイフィルタを適用した状態のデコードビューを開きます。
- **フィルタエディタに送る(F)**
  ディスプレイフィルタの条件となる論理式を生成し、生成した論理式を追加した状態のフィルタエディタを起動します。

詳しくは「6.6.9 ディスプレイフィルタを自動的に生成する」 (139 ページ) を参照してください。

ストリームビュー(S)†
対応するストリームビューをアクティブにします。

デコードビュー(D)‡
対応するデコードビューをアクティブにします。

ストリームビュー (シーケンスモード)(M)†
対応するストリームビュー (シーケンスモード) をアクティブにします。

選択されたパケットのストリーム(P)†
クリックしたパケットが属すストリームだけを表示したストリームビューを作ります。すでにストリームビューが表示されている場合は、クリックしたパケットが属すストリームだけを表示した状態に変わります。

構成しているパケットを表示(P)‡
選択中のレコードを構成しているデコードビュー上のパケットを緑色でハイライト表示します。

統計情報の表示(G)†
デコードしたデータについて統計処理を行い、その結果をグラフや表 (モニタウィンドウ) に表示します。

イベントビューア(V)† デコード時に見つけたデコードイベントをイベントビューアに表示します。

音声品質の表示(O)† RTP パケットのデータから音声品質を計算し、音声品質のウィンドウに表示します。 ASTEC Eyes *for* VoIP の機能です。

シーケンス表示(L)† 「シーケンス表示」ウィンドウを開きます。 ASTEC Eyes *for* VoIP の機能です。

音声再生(A)† RTP パケットのデータから音声データを再構成し、「音声再生」ウィンドウを開きます。 ASTEC Eyes *for* VoIP の VoIP Player オプションの機能です。

ホスト名の検索(H) サマリ領域のクリックした行の IP アドレスに対応するホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

ホスト名の更新(U) 新たにホスト名が見つかった場合やホスト名の表示の優先順位を変えた場合、アドレス帳を編集した場合など、デコードビューまたはストリームビューに表示されているホスト名を最新のものに更新します。

ネットワークユーティリティ(N)
whois、 ping、および traceroute コマンドを使うためのダイアログを開きます。詳しくは「13.1　ネットワークユーティリティ」 (340 ページ) を参照してください。

ジャンプ(J)... 「ジャンプ」ダイアログを開きます。デコードビューの場合はフレーム ID を指定します。指定したフレーム ID の行が選択されます。ストリームビューの場合はストリーム ID を指定します。指定したストリームの先頭のレコードが選択されます。

領域全体をコピー(W)
デコードビューまたはストリームビューでフォーカスのある領域に表示されているすべての文字列をクリップボードにコピーします。

バイナリ保存(B)... 「バイナリデータを保存」ダイアログを開きます。キャプチャデータの一部をバイナリモードでファイルに保存します。詳しくは「6.9.3 キャプチャデータの一部をバイナリモードでファイルに保存する」 (157 ページ)を参照してください。

再デコード(Q) 変更されたオプションを反映させるためにデコードをやり直します。次のオプションを変更したときに再デコードが必要です。

- デコードヒント
- チェックサム値の検出
- ストリームビューのレコードの並び順

ツールバーの表示(T) ツールバーの表示と非表示を切り替えます。

日本語エンコード(C) 日本語のエンコードを指定します。サブメニューからエンコードを選ぶと、デコードし直した結果を表示します。**表示行を全て変更**を選ぶと、表示されているすべてのパケットまたはレコードのデコードをやり直します。

プロパティ(R)... 「キャプチャデータのプロパティ」ダイアログを開きます。

ストリームビュー (シーケンスモード) のシーケンス領域を右クリックすると、次のポップアップメニューが現れます。

前のセッション(P)
ひとつ前のセッションにフォーカスを移動します。

次のセッション(N)
次のセッションにフォーカスを移動します。

フィルタ解除(R) 適用されているフィルタをすべて解除します。

前のエラー(V) 前のエラーのレコードにフォーカスを移動します。

次のエラー(T) 次のエラーのレコードにフォーカスを移動します。

B.2.14 パケット編集ウィンドウのポップアップメニュー

パケット編集ウィンドウを右クリックすると現れます。

表示(V) 次をメニュー項目とするサブメニューが現れます。

- **拡大表示(M)** フォーカスのある領域を拡大します。フォーカスのない領域は見えなくなります。
- **サマリ領域(S)** サマリ領域の表示、非表示を切り替えます。
- **デコード結果領域(R)** デコード結果領域の表示、非表示を切り替えます。
- **ダンプ領域(D)** ダンプ領域の表示、非表示を切り替えます。

フィルタ(F)

- **ヘッダー属性フィルタ(A)** ヘッダー属性フィルタを使うためのメニューが現れます。詳しくは「6.6.2 ヘッダー属性フィルタ」 (130 ページ) を参照してください。
- **デコード結果フィルタ(F)...** 「デコード結果フィルタ」ダイアログを開きます。詳しくは「6.6.3 デコード結果フィルタ」 (132 ページ) を参照してください。
- **フィルタ解除(R)** 適用されている簡易フィルタをすべて解除します。
- **フィルタの生成(I)** ディスプレイフィルタを自動的に生成するためのサブメニューが現れます。
  - **一時的に生成して適用する(I)** ディスプレイフィルタの条件となる論理式を生成し、ディスプレイフィルタを適用した状態のデコードビューを開きます。
  - **フィルタエディタに送る(F)** ディスプレイフィルタの条件となる論理式を生成し、生成した論理式を追加した状態のフィルタエディタを起動します。

  詳しくは「6.6.9 ディスプレイフィルタを自動的に生成する」 (139 ページ) を参照してください。

統計情報の表示(G) デコードしたデータについて統計処理を行い、その結果をグラフや表 (モニタウィンドウ) に表示します。

イベントビューア(V)
デコード時に見つけたデコードイベントをイベントビューアに表示します。

ホスト名の検索(H) サマリ領域のクリックした行の IP アドレスに対応するホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

ホスト名の更新(U) 新たにホスト名が見つかった場合やホスト名の表示の優先順位を変えた場合、アドレス帳を編集した場合など、デコードビューまたはストリームビューに表示されているホスト名を最新のものに更新します。

ネットワークユーティリティ(N)
whois、 ping、および traceroute コマンドを使うためのダイアログを開きます。詳しくは「13.1　ネットワークユーティリティ」 (340 ページ) を参照してください。

ジャンプ(J)... 「ジャンプ」ダイアログを開きます。指定したフレーム ID の行が選択されます。

領域全体をコピー(W)
フォーカスのある領域に表示されているすべての文字列をクリップボードにコピーします。

バイナリ保存(B)... 「バイナリデータを保存」ダイアログを開きます。キャプチャデータの一部をバイナリモードでファイルに保存します。詳しくは「6.9.3　キャプチャデータの一部をバイナリモードでファイルに保存する」 (157 ページ) を参照してください。

再デコード(Q) 変更されたオプションを反映させるためにデコードをやり直します。次の操作を行ったときに再デコードが必要です。

- デコードヒントを変更したとき
- チェックサム値の検出状態を変更したとき
- パケットを編集したとき

ツールバーの表示(T) ツールバーの表示と非表示を切り替えます。

日本語エンコード(C) 日本語のエンコードを指定します。サブメニューからエンコードを選ぶと、デコードし直した結果を表示します。**表示行を全て変更**を選ぶと、表示されているすべてのパケットまたはレコードのデコードをやり直します。

プロパティ(R)... 「キャプチャデータのプロパティ」ダイアログを開きます。

B.2.15 トラフィックウィンドウのポップアップメニュー

トラフィックウィンドウを右クリックすると現れます。

表示形式(V) トラフィックウィンドウの表示形式を切り替えます。サブメニューから表示形式を選びます。

- **折れ線グラフ(H)** 折れ線グラフ形式に切り替えます。
- **棒グラフ(B)** 棒グラフ形式に切り替えます。
- **円グラフ(P)** 円グラフ形式に切り替えます。
- **表形式(T)** 表形式に切り替えます。

データの単位(U) 統計データの表示単位を切り替えます。サブメニューから表示単位を選びます。

- **バイト(Y)** バイト数単位の表示に切り替えます。トラフィックウィンドウが表形式のときは、このメニュー項目はありません。
- **フレーム(F)** フレーム数単位の表示に切り替えます。トラフィックウィンドウが表形式のときは、このメニュー項目はありません。
- **使用率(U)** 「MAC 層トラフィック」のウィンドウでのみ選べます。折れ線グラフの Y 軸の単位をメディアのトラフィックの上限に対する使用率に切り替えます。
- **バイト単位(Y)** バイト数表示の補助単位を指定するためのサブメニューが現れます。**ビット(B)**、**k ビット(K)**、**M ビット(M)**、**バイト(Y)**、**k バイト(T)**、**M バイト(E)** から選べます。
- **フレーム単位(R)** フレーム数表示の補助単位を指定するためのサブメニューが現れます。**フレーム(F)**、**k フレーム(K)**、**M フレーム(M)** から選べます。

データの範囲(R) トラフィックウィンドウが棒グラフまたは円グラフ形式のときのみ選べます。サブメニューから期間を選びます。

過去 *T* 間(R) 過去 *T* 間に流れたパケットの合計または比率を表示します。 *T* は選択中のタイムスパンの種類とその設定値によって変わります。デフォルトでは、 5 分です。

タイムスパンについては、「2.2.7　タイムスパン」 (23 ページ) および「11.6　モニタのオプションを設定する」 (298 ページ) を参照してください。

累計値(T) ASTEC Eyes またはリモートモジュールを起動したときから計測した全パケットの合計または比率を表示します。モニタリセットを行った場合は、モニタリセットを行った時点から計測した全パケットの合計または比率になります。

モニタフィルタ(F) モニタフィルタを適用または解除します。サブメニューから適用したいモニタフィルタまたは**フィルタ解除(R)** を選びます。

フィルタの生成(I) モニタフィルタを自動的に生成するためのサブメニューが現れます。

- **一時的に生成して適用する(I)**
  モニタフィルタの条件となる論理式を生成し、選択中のインタフェースにモニタフィルタを適用します。
- **フィルタエディタに送る(F)**
  モニタフィルタの条件となる論理式を生成し、生成した論理式を追加した状態のフィルタエディタを起動します。

詳しくは「2.6.4　モニタフィルタを自動的に生成する」 (38 ページ) を参照してください。

タイムスパン(P) タイムスパンを切り替えるためのサブメニューが現れます。

短期(S) 短期タイムスパンに切り替えます。

中期(M) 中期タイムスパンに切り替えます。

長期(L) 長期タイムスパンに切り替えます。

Y 軸を戻す(Y) 折れ線グラフまたは棒グラフ形式で、 Y 軸の範囲を変えた場合に選べます。 Y 軸の範囲をグラフのデフォルトに戻します。

凡例(G) 凡例の表示と非表示を切り替えます。

キャプチャデータインディケータ(A)
キャプチャデータインディケータの表示と非表示を切り替えます。

ツールバーの表示(T) ツールバーの表示と非表示を切り替えます。

プロパティ(O)... 「グラフのプロパティ」ダイアログを開きます。

「グラフのプロパティ」ダイアログには「情報」のページと「グラフ」のページがあります。

「情報」のページには、ホスト名やファイル名、モニタ開始時刻、プロット間隔など、トラフィックウィンドウに表示しているグラフのデータに関連する情報が表示されます。

「グラフ」のページではグラフの表示をカスタマイズできます。設定する内容はグラフのデフォルトのオプションと同じですが、設定した値はポップアップメニューを開いたウィンドウだけに適用されます。設定する内容については、「11.7 グラフのオプションを設定する」 (300 ページ) を参照してください。

元のグラフに戻る(B)

トラフィックウィンドウに内訳を表示している場合や表示するグラフアイテムを制限している場合に選べます。元のグラフに戻ります。

他を隠す(M) トラフィックウィンドウが折れ線グラフ形式のときのみ選べます。選択中のグラフアイテムだけを表示し、それ以外のグラフアイテムは非表示にします。ただし、選択中のグラフアイテムが Others の場合は、このメニュー項目は選べないようになっています。

このグラフアイテムを隠す(E)

トラフィックウィンドウが折れ線グラフ形式のときのみ選べます。選択中のグラフアイテムを隠します。

内訳(D) 選択中のグラフアイテムの内訳を表示するためのサブメニューが現れます。

発信元毎(S) 選択中のグラフアイテムを発信元毎に分類して表示します。

受信先毎 D) 選択中のグラフアイテムを受信先毎に分類して表示します。

ホストペア毎(H) 選択中のグラフアイテムをホストペア毎に分類して表示します。

プロトコル毎(P) 選択中のグラフアイテムをプロトコル毎に分類して表示します。

ホスト名の検索(H)

IP 層のホストを表すグラフアイテムを選んでいるとき、そのホスト名を検索します。サブメニューから検索したいホスト名 (ネームサービス) を選びます。

ネットワークユーティリティ(N)

whois、 ping、および traceroute コマンドを使うためのダイアログを開きます。詳しくは「13.1　ネットワークユーティリティ」 (340 ページ) を参照してください。

ポートの状態一覧(S)

IP 層のホストを表すグラフアイテムを選んでいるとき、そのホストが開いているポートに関してネットワークのパケットから得られた情報を表示するための、「ポートの状態一覧」ダイアログを開きます。詳しくは「2.9 ホストごとのポートの状態を表示する」 (46 ページ) を参照してください。

色の設定(C)...　選択中のグラフアイテムの色を変えるための「色の設定」ダイアログを開きます。トラフィックウィンドウが表形式の場合、このメニュー項目はありません。

すべてコピー(W)　トラフィックウィンドウが表形式のときのみ選べます。ウィンドウに表示されているすべての文字列をクリップボードにコピーします。

B.2.16　ネットワークユーティリティのダイアログのポップアップメニュー

「Whois」ダイアログ、「Ping」ダイアログ、「Traceroute」ダイアログを右クリックすると現れます。

コピー(C)　**実行結果(R)** 領域に表示されている文字列を選んでから、このメニュー項目を選ぶと、選んだ文字列がクリップボードにコピーされます。

すべて選択(A)　**実行結果(R)** 領域に表示されている文字列全体を選択された状態にします。

クリア(R)　**実行結果(R)** 領域に表示されているメッセージをすべて削除します。

B.2.17　フィルタエディタのポップアップメニュー

フィルタエディタの フィルタビューア領域を右クリックすると現れます。

新規グループ(G)　条件グループを追加します。

新規条件(E) 条件論理式を追加します。

削除(D) 論理式を削除します。選んだ論理式が階層になっている場合は、選んだ論理式とその下の階層をすべて削除します。

複製(U) 論理式を複製します。選んだ論理式が階層になっている場合は、選んだ論理式とその下の階層をすべて複製します。

無効にする(B) および 有効にする(B)
トグルになっています。

無効にされている論理式を選んでポップアップメニューを開いた場合は、**有効にする(B)** があります。選んだ論理式を有効にします。

有効な論理式を選んでポップアップメニューを開いた場合は、**無効にする(B)** があります。選んだ論理式を無効にします。

否定を取る(Y) 論理式の否定を取ります。

コピー(C) 論理式を内部のバッファにコピーします。選んだ論理式が階層になっている場合は、選んだ論理式とその下の階層をすべてコピーします。

貼り付け(P) 内部のバッファに保存されている論理式を貼り付けます。

元に戻す(N) 論理式を変更するひとつ前の状態に戻します。

やり直し(O) **元に戻す(N)** で戻す前の状態にします。

B.2.18 メッセージウィンドウのポップアップメニュー

メインウィンドウのメッセージウィンドウを右クリックすると現れます。

コピー(C) メッセージウィンドウに表示されている文字列を選んでから、このメニュー項目を選ぶと、選んだ文字列がクリップボードにコピーされます。

すべて選択(A) メッセージウィンドウに表示されている文字列全体を選択された状態にします。

クリア(R) メッセージウィンドウに表示されているメッセージをすべて削除します。

B.2.19 連続キャプチャデータのエントリのポップアップメニュー

インタフェースセレクタウィンドウ内の連続キャプチャデータのエントリを右クリックすると現れます。

連続キャプチャデータをデコードする(D)...
「連続キャプチャデータの表示」ダイアログを開きます。

プロパティ(P)... 「連続キャプチャデータのプロパティ」ダイアログを開きます。

関連付けを解除(U) 連続キャプチャデータとログの関連付けを解除します。

B.2.20 ログのエントリのポップアップメニュー

インタフェースセレクタウィンドウ内のログのエントリを右クリックすると現れます。

ログを表示(L)... 「ログの表示」ダイアログを開きます。

モニタフィルタ(F) モニタフィルタを適用または解除します。サブメニューから適用したいモニタフィルタまたは**フィルタ解除(R)** を選びます。

プロパティ(P)... 「ログのプロパティ」ダイアログを開きます。

B.2.21 ワークスペースのポップアップメニュー

ワークスペースのタブまたはワークスペース内の何もウィンドウが表示されていない部分を右クリックすると現れます。

ワークスペースの追加(A)
新しいワークスペースを追加します。

ワークスペースの削除(D)
クリックしたワークスペースを削除します。

プロパティ(P)... 「ワークスペースのプロパティ」ダイアログを開きます。

レポートの設定(H)... 「HTML レポート」ダイアログを開きます。

上記のメニュー項目以外に、既存のワークスペースに対応するメニュー項目があります。既存のワークスペースに対応するメニュー項目を選ぶと、選んだワークスペースに移動します。

B.3 キーバインド

B.3.1 リアルタイムデコードビューのキーバインド

キー	動作
<↑> **<↓>**	選択行を 1 つ上または下に移動します。
<←> **<→>**	選択カラムを 1 つ左または右に移動します。
<Shift-↑> **<Shift-↓>**	垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。
<Shift-←> **<Shift-→>**	水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。
<Page Up> **<Page Down>**	選択行を数行上または下に移動します。 何行移動するかは、ウィンドウの大きさによります。
<Home> **<End>**	先頭または末尾の行が選択された状態になります。
<Ctrl-C>	白い枠で囲まれたセルの文字列をクリップボートにコピーします。コピーした内容は他のアプリケーションなどへ貼り付けることができます。

B.3.2 デコードビューとストリームビューのキーバインド

ストリームビューのキーバインドはモードによって異なります。

表 B-9: デコードビューおよびストリームビュー (シーケンスモードでない場合) のキーバインド

キー	サマリ領域	デコード結果領域	ダンプ領域
<Tab> **<Shift-Tab>**	デコードビューまたはストリームビューの中のフォーカスをサマリ領域、デコード結果領域、およびダンプ領域の間で移動します。		
<↑> **<↓>**	選択行を 1 つ上または下に移動します。		アドレスの小さい方または大きい方の領域に移動します。
<←> **<→>**	選択カラムを 1 つ左または右に移動します。		アドレスの小さい方または大きい方の領域に移動します。

次ページへ続く

キー	サマリ領域	デコード結果領域	ダンプ領域
<Shift-↑> **<Shift-↓>**	垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。		それぞれ **<↑>** **<↓>** キーと同じ働きをします。
<Shift-←> **<Shift-→>**	水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。		それぞれ **<↑>** **<↓>** キーと同じ働きをします。
<Alt-↑> **<Alt-↓>**	デコードビューでのみ有効です。ストリームビューで選択しているレコードに対応するパケットは、デコードビューのサマリ領域で、緑にハイライト表示されます。これらのキーでハイライト表示されたパケットにジャンプできます。		
<Page Up> **<Page Down>**	選択行を数行上または数行下に移動します。 何行移動するかは、ウィンドウの大きさによります。		アドレスの小さい方または大きい方が見えるように画面をスクロールします。選択されている部分は移動しません。
<Home> **<End>**	先頭または末尾の行が選択された状態になります。		アドレスの先頭または末尾が見えるように画面をスクロールします。選択されている部分は移動しません。
<Z>	デコードビューまたはストリームビューの 3 つの領域がすべて表示されている場合、フォーカスのある領域だけがウィンドウいっぱいに拡大され、他の 2 つの領域は見えなくなります。逆に、どれか 1 つの領域だけが表示されている場合は、 3 つの領域すべてが見えるようになります。		
<Ctrl-↑> **<Ctrl-↓>** **<Ctrl-Home>** **<Ctrl-End>**	フォーカスがどの領域にあっても、それぞれサマリ領域で **<↑>**、 **<↓>**、 **<Home>**、および **<End>** キーを押したのと同じ働きをします。 サマリ領域へフォーカスを移さずにパケットまたはレコードの選択を変えられます。		
<Shift-Ctrl-↑> **<Shift-Ctrl-↓>**	サマリ領域に垂直スクロールバーが表示されているとき、フォーカスがどの領域にあっても、サマリ領域を上下にスクロールします。選択行は移動しません。		
<Shift-Ctrl-←> **<Shift-Ctrl-→>**	サマリ領域に水平スクロールバーが表示されているとき、フォーカスがどの領域にあっても、サマリ領域を左右にスクロールします。選択カラムは移動しません。		
<Ctrl-C>	白い枠で囲まれたセルの文字列をクリップボートにコピーします。コピーした内容は他のアプリケーションなどへ貼り付けることができます。		反転している部分をクリップボードにコピーします。コピーした内容は他のアプリケーションなどへ貼り付けることができます。
<Space>	チェックマークが付いていない場合はチェックを付けます。付いている場合はチェックを外します。		

次ページへ続く

キー	サマリ領域	デコード結果領域	ダンプ領域
<Ctrl-G>	「ジャンプ」ダイアログを開きます。デコードビューの場合は、フレーム ID を指定します。 **OK** ボタンをクリックすると、指定したフレーム ID が選択されます。ストリームビューの場合は、ストリーム ID を指定します。 **OK** ボタンをクリックすると、指定したストリーム ID の先頭のレコードが選択されます。		
<Ctrl-T>	サマリ領域の表示、非表示を切り替えます。		
<Ctrl-M>	デコード結果領域の表示、非表示を切り替えます。		
<Ctrl-B>	ダンプ領域の表示、非表示を切り替えます。		

表 B-10: ストリームビュー (シーケンスモード) のキーバインド

キー	セッションリスト領域	シーケンス領域	デコード結果領域
<Tab> **<Shift-Tab>**	フォーカスをセッションリスト領域、シーケンス領域、およびデコード結果領域の間で移動します。		
<↑> **<↓>**	選択行を 1 つ上または下に移動します。		
<←> **<→>**	水平スクロールバーが表示されているとき、左右にスクロールします。		選択カラムを 1 つ左または右に移動します。
<Shift-↑> **<Shift-↓>**	それぞれ **<↑> <↓>** キーと同じ働きをします。		垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。
<Shift-←> **<Shift-→>**	それぞれ **<↑> <↓>** キーと同じ働きをします。		水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。
<Alt-↑> **<Alt-↓>**	1 つ前または後ろのエラーの行にフォーカスを移動します。		
<Page Up> **<Page Down>**	選択行を数行上または下に移動します。 何行移動するかは、ウィンドウの大きさによります。		
<Home> **<End>**	先頭または末尾の行が選択された状態になります。		
<Z>	3 つの領域がすべて表示されている場合、フォーカスのある領域だけがウィンドウいっぱいに拡大され、他の 2 つの領域は見えなくなります。逆に、どれか 1 つの領域だけが表示されている場合は、 3 つの領域すべてが見えるようになります。		

次ページへ続く

キー	セッションリスト領域	シーケンス領域	デコード結果領域
<Ctrl-↑> **<Ctrl-↓>** **<Ctrl-Home>** **<Ctrl-End>**	フォーカスがどちらの領域にあっても、それぞれセッションリスト領域で **<↑>**、**<↓>**、**<Home>**、および **<End>** キーを押したのと同じ働きをします。セッションリスト領域へフォーカスを移さずにセッションの選択を変えられます。		シーケンス領域で **<↑>**、**<↓>**、**<Home>**、および **<End>** キーを押したのと同じ働きをします。シーケンス領域へフォーカスを移さずにレコードの選択を変えられます。
<Ctrl-C>	領域全体をクリップボートにコピーします。コピーした内容は他のアプリケーションなどへ貼り付けることができます。		白い枠で囲まれたセルの文字列をクリップボートにコピーします。
<Space>		チェックマークが付いていない場合はチェックを付けます。付いている場合はチェックを外します。	
<Ctrl-T>	セッションリスト領域の表示、非表示を切り替えます。		
<Ctrl-M>	シーケンス領域の表示、非表示を切り替えます。		
<Ctrl-B>	デコード結果領域の表示、非表示を切り替えます。		

B.3.3 パケット編集ウィンドウのキーバインド

表 B-11: パケット編集ウィンドウのキーバインド

キー	サマリ領域	デコード結果領域	ダンプ領域
<Tab> **<Shift-Tab>**	フォーカスをサマリ領域、デコード結果領域、およびダンプ領域の間で移動します。		
<↑> **<↓>**	選択行を 1 つ上または下に移動します。		選択バイトを 1 つ上または下に移動します。
<←> **<→>**	選択カラムを 1 つ左または右に移動します。		選択バイトを 1 つ左または右に移動します。
<Shift-↑> **<Shift-↓>**	垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。		それぞれ **<↑>** **<↓>** キーと同じ働きをします。
<Shift-←> **<Shift-→>**	水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。		それぞれ **<↑>** **<↓>** キーと同じ働きをします。

次ページへ続く

キー	サマリ領域	デコード結果領域	ダンプ領域
<Page Up> **<Page Down>**	選択行を数行上または下に移動します。 何行移動するかは、ウィンドウの大きさによります。		アドレスの小さい方が見えるように画面をスクロールします。選択されている部分は移動しません。
<Home> **<End>**	先頭または末尾の行が選択された状態になります。		アドレスの先頭または末尾が見えるように画面をスクロールします。選択されている部分は移動しません。
<Z>	3 つの領域がすべて表示されている場合、フォーカスのある領域だけがウィンドウいっぱいに拡大され、他の 2 つの領域は見えなくなります。逆に、どれか 1 つの領域だけが表示されている場合は、 3 つの領域すべてが見えるようになります。		
<Ctrl-↑> **<Ctrl-↓>** **<Ctrl-Home>** **<Ctrl-End>**	フォーカスがどの領域にあっても、それぞれサマリ領域で **<↑>**、 **<↓>**、 **<Home>**、および **<End>** キーを押したのと同じ働きをします。 サマリ領域へフォーカスを移さずにパケットまたはレコードの選択を変えられます。		
<Shift-Ctrl-↑> **<Shift-Ctrl-↓>**	サマリ領域に垂直スクロールバーが表示されているとき、フォーカスがどの領域にあっても、サマリ領域を上下にスクロールします。選択行は移動しません。		
<Shift-Ctrl-←> **<Shift-Ctrl-→>**	サマリ領域に水平スクロールバーが表示されているとき、フォーカスがどの領域にあっても、サマリ領域を左右にスクロールします。選択カラムは移動しません。		
<Ctrl-C>	白い枠で囲まれたセルの文字列をクリップボートにコピーします。コピーした内容は他のアプリケーションなどへ貼り付けることができます。		反転している部分をクリップボードにコピーします。コピーした内容は他のアプリケーションなどへ貼り付けることができます。
<Space>	チェックマークが付いていない場合はチェックを付けます。付いている場合はチェックを外します。		
<Ctrl-G>	「ジャンプ」ダイアログを開きます。指定したフレーム ID が選択されます。		
<Ctrl-T>	サマリ領域の表示、非表示を切り替えます。		
<Ctrl-M>	デコード結果領域の表示、非表示を切り替えます。		
<Ctrl-B>	ダンプ領域の表示、非表示を切り替えます。		
<0> ～ **<9>**、 **<A>** ～ **<F>**			選択している部分のデータを書き換えます。

B.3.4 モニタウィンドウのキーバインド

モニタウィンドウのキーバインドは、モニタウィンドウの状態によって異なります。また、グラフの値を読み取る状態では、水平と垂直どちらのカーソルを選んでいるか、またグラフアイテムを選んでいるかどうかによってもキーバインドが異なります。

- モニタ情報の更新を行う状態 (表 B-12)
- グラフの値を読み取る状態
  キー操作が有効になるのは、一度マウスでトラフィックウィンドウのグラフ部分をクリックするか、ドラッグした後です。
  - 垂直カーソルを選んでいるとき (表 B-13)
  - 水平カーソルを選んでいるとき
    * グラフアイテムを選んでいないとき (表 B-14)
    * グラフアイテムを選んでいるとき (表 B-15)

表 B-12: モニタ情報の更新を行う状態のトラフィックウィンドウのキーバインド

キー	動作
<↑> **<↓>**	グラフ形式の場合は、凡例の反転している項目の 1 つ上または下の項目を反転します。対応するグラフアイテムが選択された状態になります。 表形式の場合は、選択行を 1 つ上または下に移動します。
<←> **<→>**	表形式の場合に、選択カラムを 1 つ左または右に移動します。
<Shift-↑> **<Shift-↓>**	表形式で垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。
<Shift-←> **<Shift-→>**	表形式で水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。
<Ctrl-Space>	グラフアイテムの選択と非選択を切り替えます。
<Ctrl-C>	グラフ形式の場合は、モニタ情報をクリップボードにコピーします。 表形式の場合は、白い枠で囲まれたセルの文字列をクリップボードにコピーします。
<Backspace>	内訳を表示している場合やいくつかのグラフアイテムを隠している場合、元のグラフに戻ります。

キーボードでの操作は、凡例を表示していない場合でも同じことができます。

表 B-13: 垂直カーソルを選んでいるときに有効なキーとその動き

キー	グラフ部分をクリックした後	グラフ部分でドラッグした後
<←>	5 つ前のプロット位置に実線が移動します。	ドラッグの終点を 5 つ前のプロット位置に変えます。
<→>	5 つ後のプロット位置に実線が移動します。	ドラッグの終点を 5 つ後のプロット位置に変えます。
<Ctrl-←>	1 つ前のプロット位置に実線が移動します。	ドラッグの終点を 1 つ前のプロット位置に変えます。
<Ctrl-→>	1 つ後のプロット位置に実線が移動します。	ドラッグの終点を 1 つ後のプロット位置に変えます。
<Shift-←>	**<←>** に同じ	ドラッグの始点を 5 つ前のプロット位置に変えます。
<Shift-→>	**<→>** に同じ	ドラッグの始点を 5 つ後のプロット位置に変えます。
<Shift-Ctrl-←>	**<Ctrl-←>** に同じ	ドラッグの始点を 1 つ前のプロット位置に変えます。
<Shift-Ctrl-→>	**<Ctrl-→>** に同じ	ドラッグの始点を 1 つ後のプロット位置に変えます。

表 B-14: 水平カーソルを選んでいるときに有効なキーとその動き (グラフアイテムを選んでいないとき)

キー	グラフ部分をクリックした後	グラフ部分でドラッグした後
<↑>	Y 軸の範囲の 1/100 を単位として、1 単位上に実線が移動します。	Y 軸の範囲の 1/100 を単位として、1 単位上にドラッグの終点が移動します。
<↓>	Y 軸の範囲の 1/100 を単位として、1 単位下に実線が移動します。	Y 軸の範囲の 1/100 を単位として、1 単位下にドラッグの終点が移動します。
<Ctrl-↑>	短期タイムスパン表示の場合は、1 バイト / 秒または 1 フレーム / 秒を単位として、1 単位上に実線が移動します。その他の場合は、0.1 バイト / 秒または 0.1 フレーム / 秒を単位として、1 単位上に実線が移動します。	短期タイムスパン表示の場合は、1 バイト / 秒または 1 フレーム / 秒を単位として、1 単位上にドラッグの終点が移動します。その他の場合は、0.1 バイト / 秒または 0.1 フレーム / 秒を単位として、1 単位上に上にドラッグの終点が移動します。
<Ctrl-↓>	短期タイムスパン表示の場合は、1 バイト / 秒または 1 フレーム / 秒を単位として、1 単位下に実線が移動します。それ他の場合は、0.1 バイト / 秒または 0.1 フレーム / 秒を単位として、1 単位下に実線が移動します。	短期タイムスパン表示の場合は、1 バイト / 秒または 1 フレーム / 秒を単位として、1 単位下にドラッグの終点が移動します。その他の場合は、0.1 バイト / 秒または 0.1 フレーム / 秒を単位として、1 単位下にドラッグの終点が移動します。
<Shift-↑>	**<↑>** に同じ	Y 軸の範囲の 1/100 を単位として、1 単位上にドラッグの始点が移動します。
<Shift-↓>	**<↓>** に同じ	Y 軸の範囲の 1/100 を単位として、1 単位下にドラッグの始点が移動します。
<Shift-Ctrl-↑>	**<Ctrl-↑>** に同じ	短期タイムスパン表示の場合は、1 バイト / 秒または 1 フレーム / 秒を単位として、1 単位上にドラッグの始点が移動します。その他の場合は、0.1 バイト / 秒または 0.1 フレーム / 秒を単位として、1 単位上にドラッグの始点が移動します。
<Shift-Ctrl-↓>	**<Ctrl-↓>** に同じ	短期タイムスパン表示の場合は、1 バイト / 秒または 1 フレーム / 秒を単位として、1 単位下にドラッグの始点が移動します。その他の場合は、0.1 バイト / 秒または 0.1 フレーム / 秒を単位として、1 単位下にドラッグの始点が移動します。

表 B-15: 水平カーソルを選んでいるときに有効なキーとその動き (グラフアイテムを選んでいるとき)

キー	グラフ部分をクリックした後	グラフ部分でドラッグした後
<↑> **<Ctrl-↑>**	選択中のグラフアイテムのプロット点のうち、次に大きい値の点に実線が移動します。	選択中のグラフアイテムのプロット点のうち、次に大きい値の点にドラッグの終点が移動します。
<↓> **<Ctrl-↓>**	選択中のグラフアイテムのプロット点のうち、次に小さい値の点に実線が移動します。	選択中のグラフアイテムのプロット点のうち、次に小さい値の点にドラッグの終点が移動します。
<Shift-↑> **<Shift-Ctrl-↑>**	**<↑>** に同じ	選択中のグラフアイテムのプロット点のうち、次に大きい値の点にドラッグの始点が移動します。
<Shift-↓> **<Shift-Ctrl-↑>**	**<↓>** に同じ	選択中のグラフアイテムのプロット点のうち、次に小さい値の点にドラッグの始点が移動します。

B.3.5 インタフェースセレクタウィンドウのキーバインド

表 B-16: インタフェースセレクタウィンドウのキーバインド

キー	動作
<↑> **<↓>**	インタフェースセレクタウィンドウ内でフォーカスのあるエントリをひとつ上または下に移動します。
<←>	インタフェースセレクタウィンドウ内でフォーカスのあるエントリに包含されるエントリがあって、包含されるエントリが展開されている場合は縮小します。 たとえば、ホストのエントリにフォーカスがあって、そのホストのインタフェースのエントリが展開されている場合は、インタフェースのエントリを縮小します。
<→>	インタフェースセレクタウィンドウ内でフォーカスのあるエントリに包含されるエントリがあって、包含されるエントリが縮小されている場合は展開します。 たとえば、ホストのエントリにフォーカスがあって、そのホストのインタフェースのエントリが縮小されている場合は、インタフェースのエントリを展開します。
<Enter>	インタフェースのエントリにフォーカスがある場合、そのインタフェースが選択されます。

B.3.6 デコードヒントの入力のキーバインド

編集中の行は青く反転表示されています。入力の対象となっているカラムは白い枠で囲まれています。

表 B-17: デコードヒントの入力のキーバインド

キー	動作
<↑> **<↓>**	編集する行を 1 つ上または下に移動します。
<←> **<→>**	編集する行の中で、入力の対象とするカラムを 1 つ左または 1 つ右に移動します。
<Shift-↑> **<Shift-↓>**	垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。
<Shift-←> **<Shift-→>**	水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。
<F2>	カラムに入力できる状態と入力できない状態を切り替えます。
<Tab> **<Shift-Tab>**	カラムに入力できる状態のとき、入力できる状態を保ったまま、対象とするカラムを次または前のカラムに移動します。
<Esc>	カラムに入力できる状態のとき、入力できない状態にします。

B.3.7 アドレス帳のキーバインド

表 B-18: アドレス帳のキーバインド

キー	動作
<↑> **<↓>**	編集する行を 1 つ上または下に移動します。
<←> **<→>**	白い枠で囲まれたセルを移動します。
<Shift-↑> **<Shift-↓>**	表形式で垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。
<Shift-←> **<Shift-→>**	表形式で水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。
<F2>	ユーザー定義名を入力できる状態にします。入力できる状態にあるときは、入力できない状態にします。
<Enter>	入力したユーザー定義名を確定します。

B.3.8 イベントビューアのキーバインド

表 B-19: イベントビューアのキーバインド

キー	動作
<↑> **<↓>**	グラフ形式の場合は、凡例の反転している項目の 1 つ上または下の項目を反転します。対応するグラフアイテムが選択された状態になります。 表形式の場合は、選択行を 1 つ上または下に移動します。
<←> **<→>**	表形式の場合に、選択カラムを 1 つ左または右に移動します。
<Shift-↑> **<Shift-↓>**	表形式で垂直スクロールバーが表示されているとき、上下にスクロールします。選択行は移動しません。
<Shift-←> **<Shift-→>**	表形式で水平スクロールバーが表示されているとき、左右にスクロールします。選択カラムは移動しません。
<Ctrl-Space>	グラフアイテムの選択と非選択を切り替えます。
<Ctrl-C>	折れ線グラフ形式の場合は、表示されているイベントをクリップボードにコピーします。貼り付け先のアプリケーションによっては、データの形式を選ぶことができます。 表形式の場合は、白い枠で囲まれたセルの文字列をクリップボードにコピーします。

B.3.9 期間指定バーのキーバインド

(緑色の) 期間指定バーは、図 B-2 に示すような期間を指定するためのもので、「ログの表示」ダイアログ、「キャプチャデータマネジャー」ダイアログ、「連続キャプチャデータの表示」ダイアログにあります。

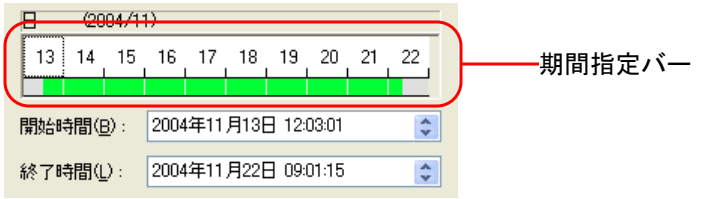


図 B-2: 期間指定バー

表 B-20: 期間指定バーのキーバインド

キー	動作
<←>、 <→>	選択されている 1 区間を左右に移動します。
<Shift-←>	区間の終点を 1 つ左に移動します。
<Shift-→>	区間の終点を 1 つ右に移動します。
<Enter>	選んだ 1 区間内の一部を選択するために、期間指定バーの単位を 1 つ下の単位に切り替えます。 たとえば、期間指定バーの目盛りが「日」のとき、 10 日を選ぶと、開始時間は「200Y 年 XX 月 10 日 00:00:00」、終了時間は「200Y 年 XX 月 11 日 00:00:00」になります。その状態で **<Enter>** キーを押すと、期間指定バーの目盛りの単位は「時」に変わります。
<Backspace>	初期状態に戻ります。

B.3.10 ショートカットキー

表 B-21: ショートカットキー

キー	動作	
<Alt-0>	ワークスペースにフォーカスを移します。	
<Alt-1>	インタフェースセレクタウィンドウにフォーカスを移します。	
<Alt-2>	メッセージウィンドウにフォーカスを移します。	
<Ctrl-C>	フォーカスがグラフ形式のウィンドウにあるとき	トラフィックの統計情報またはイベント情報をクリップボードにコピーします。
	フォーカスが表形式のウィンドウにあるとき	白い枠で囲まれたセルの文字列をクリップボードにコピーします。
<Ctrl-E>	フィルタエディタを起動します。	
<Ctrl-F>	「検索」ダイアログを開きます。	
<Ctrl-L>	「ホスト名の検索」ダイアログを開きます。	
<Ctrl-O>	「開く」ダイアログを開きます。「開く」ダイアログで指定したファイルはデコードされます。	
<Ctrl-P>	「印刷」ダイアログを開きます。	
<Ctrl-S>	デコードしたデータを保存するための「名前を付けて保存」ダイアログを開きます。	
<Ctrl-Alt-←> **<Ctrl-PageUp>**	複数のワークスペースがある場合、選択中のワークスペースを 1 つ前のワークスペースに切り替えます。	
<Ctrl-Alt-→> **<Ctrl-PageDown>**	複数のワークスペースがある場合、選択中のワークスペースの 1 つ後ろのワークスペースに切り替えます。	

索引

記号

A

B

C

D

E

F

I

J

M

N

O

P

R

S

T

U

W

X

Y

あ

い

う

え

お

か

き

く

ぐ

こ

さ

し

じ

す

せ

た

だ

ち

つ

て

で

と

ど

な

に

ね

は

ば

ぱ

ひ

ふ

ぶ

ぷ

へ

ほ

ぽ

み

め

も

ゆ

り

れ

ろ

わ

ASTEC Eyes on the net バージョン 7.2
ASTEC Eyes ユーザーズガイド

マニュアルバージョン 7.200

著作 : 株式会社 アールワークス

2017 年 1 月 17 日 発行

〒103-0022
東京都中央区日本橋室町 4 丁目 3-18 東京建物室町ビル 3 階
FAX: 03-4496-4339　TEL: 03-5946-8400 (代表)