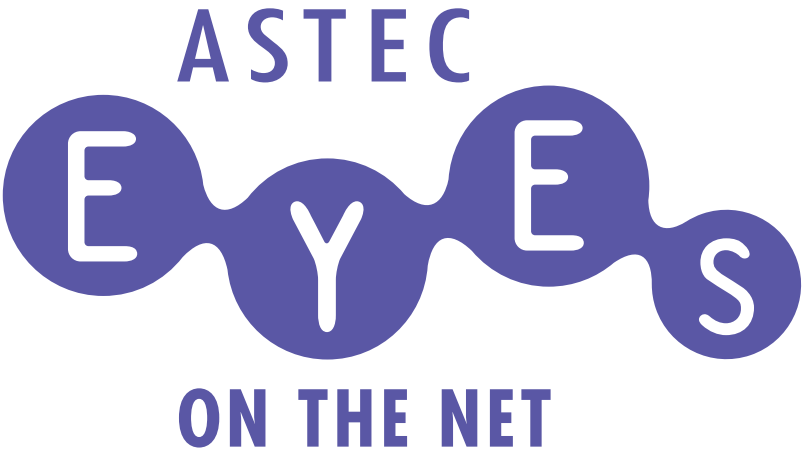


バージョン7.2

ASTEC Eyes入門

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　TEL: 03-5946-8400 (代表)

目次

はじめに

本書について 1
表記について 2
製品サポートについて 3

1 章　ASTEC Eyes の起動と終了

ASTEC Eyes 基本パッケージ の起動と終了 5
ASTEC Eyes 基本パッケージを起動する 5
ASTEC Eyes 基本パッケージ を終了する 7
Windows 用リモートモジュールの起動と終了 8
リモートモジュールを起動してサービスに登録する 8
Windows 用リモートモジュールを停止する 9

2 章　ネットワークのトラフィックを見る

モニタするネットワークインタフェースを選ぶ 11
モニタを開始する 12
モニタウィンドウを開く 13
グラフの内訳を見る 15

3 章　ネットワークのパケットを分析する

キャプチャするネットワークインタフェースを選ぶ 20
キャプチャを開始する 21
キャプチャを停止する 22
デコードビューを生成する 23

TCP ストリームを再構成してデコードする 25
デコード結果を絞り込む 27

4 章　長期間にわたるトラフィックのトレンドを調べる

ログの出力を開始する 31
ログを見る 33
ログの出力を停止する 36

5 章　リモートモジュールを使う

リモートモジュールに接続する 38

6 章　その他の機能

付録 A　用語集

索引

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 の基本的な機能について、実際に操作しながら説明していきます。

☞ 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

ASTEC Eyes の起動と終了

ここでは、 ASTEC Eyes 基本パッケージ、およびリモートモジュールの起動と終了の手順について説明します。

1.1 ASTEC Eyes 基本パッケージ の起動と終了

ASTEC Eyes 基本パッケージの起動と終了の手順について説明します。

1.1.1 ASTEC Eyes 基本パッケージを起動する

ASTEC Eyes 基本パッケージを起動するには、 Windows の [スタート] メニューを開いて [プログラム (P)] または [すべてのプログラム (P)] の [ASTEC Eyes on the net] から [ASTEC Eyes] を選びます。

または、スタート画面の「アプリ」の部分から ASTEC Eyes を選びます。

☞ ASTEC Eyes 基本パッケージ を起動するには、 Administrator 権限が必要です。

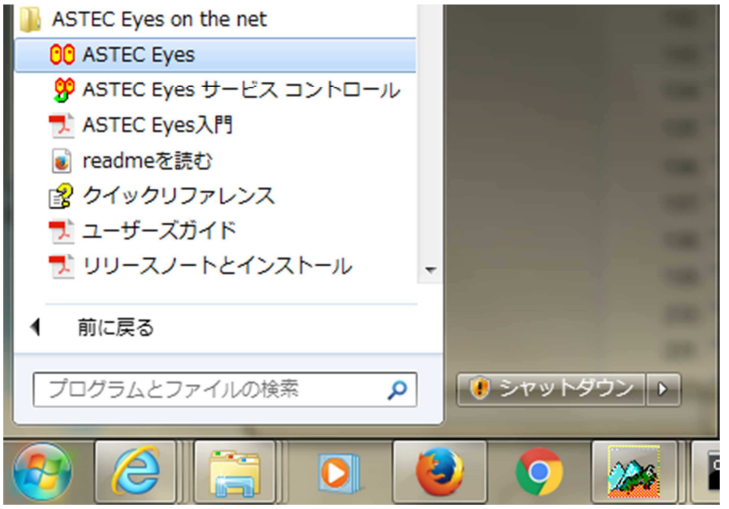


図 1-1: スタートボタンから ASTEC Eyes を起動する

ASTEC Eyes が起動すると、メインウィンドウが現れます。

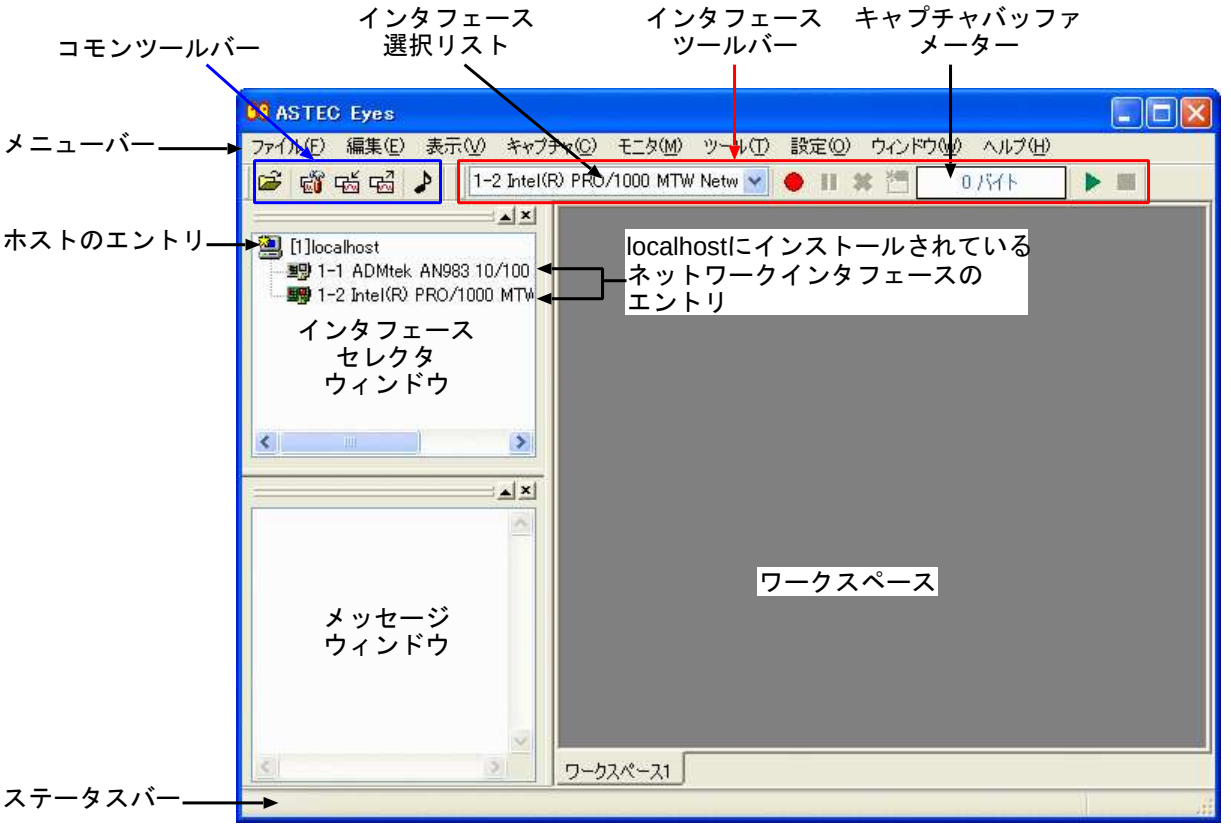


図 1-2: メインウィンドウ

ASTEC Eyes のメインウィンドウは次の部品から構成されます。

メニューバー　さまざまな操作を行うメニューがあります。

コモンツールバー　ネットワークインタフェースに関連しない操作を行うためのボタンがあります。表示しないようにすることもできます。また、ボタンをカスタマイズすることもできます。

インタフェースツールバー
ネットワークインタフェースに関連する操作を行うためのボタンがありま

す。表示しないようにすることもできます。また、ボタンをカスタマイズすることもできます。

ワークスペース
モニタウィンドウやデコードビューなど、ダイアログ以外のウィンドウを表示します。複数のワークスペースを作ることができます。詳しくは『ASTEC Eyes ユーザーズガイド』の 13 章「その他の機能」の「ワークスペース」の節を参照してください。

インタフェースセレクタウィンドウ
ネットワークインタフェースを選んだり、リモートモジュールに接続するなどさまざまな操作を行います。

メッセージウィンドウ
読み取ったグラフの値や、さまざまなメッセージを表示します。表示しないようにすることもできます。

ステータスバー
選んでいるグラフアイテム名などを表示します。表示しないようにすることもできます。

メインウィンドウ の詳しいことについては、『ASTEC Eyes ユーザーズガイド』の 1 章「各機能を使う前の準備」の「ASTEC Eyes のメインウィンドウ」の節を参照してください。

1.1.2 ASTEC Eyes 基本パッケージ を終了する

ASTEC Eyes 基本パッケージ を終了するには、メインウィンドウの**ファイル(F)** メニューから **ASTEC Eyes の終了(X)** を選びます。

1.2 Windows 用リモートモジュールの起動と終了

Windows 用リモートモジュールを起動してサービスに登録する方法、およびリモートモジュールを終了する手順について説明します。

☞ リモートモジュールを起動するには、 Administrator 権限が必要です。

1.2.1 リモートモジュールを起動してサービスに登録する

1. Windows の [スタート] メニューを開いて、 [プログラム (P)] または [すべてのプログラム (P)] の [ASTEC Eyes on the net] から [ASTEC Eyes サービスコントロール] を選びます。

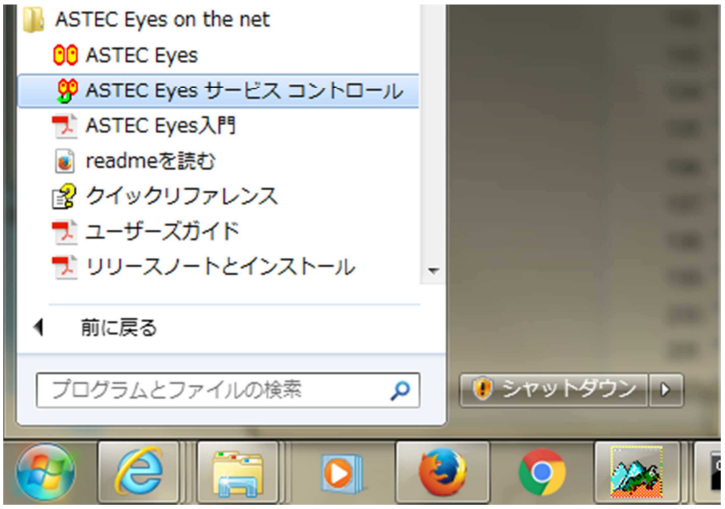


図 1-3: スタートボタンから ASTEC Eyes サービスコントロールを起動する

図 1-4 のような「ASTEC Eyes on the net サービスコントロール」ウィンドウが現れます。

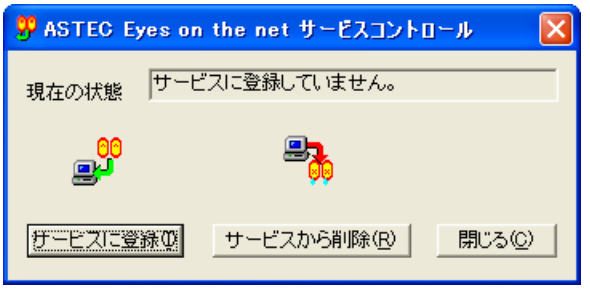


図 1-4: ASTEC Eyes on the net サービスコントロール

2. **サービスに登録(I)** ボタンをクリックします。
   現在の状態が、「モニタ中です。」になったことを確認してください。
3. **閉じる(C)** ボタンをクリックします。

1.2.2 Windows 用リモートモジュールを停止する

1. Windows の [スタート] メニューを開いて、[プログラム (P)] または [すべてのプログラム (P)] の [ASTEC Eyes on the net] から [ASTEC Eyes サービスコントロール] を選びます。
   図 1-5 のような「ASTEC Eyes on the net サービスコントロール」ウィンドウが現れます。

図 1-5: ASTEC Eyes on the net サービスコントロール

2. **サービスから削除(R)** ボタンをクリックします。
   現在の状態が、「サービスに登録していません。」になったことを確認してください。
3. **閉じる(C)** ボタンをクリックします。

2章

ネットワークのトラフィックを見る ～モニタ機能～

トラフィックとは、ネットワークを流れているデータの量のことです。ネットワークの異常をいち早く発見するためには、トラフィックを把握することが重要です。

ネットワークのトラフィックを見るには、**モニタ**機能を使います。

トラフィックを計測し、統計情報をモニタウィンドウに表示するためには、

1. モニタす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. モニタウィンドウを開きます。

2.1 モニタするネットワークインタフェースを選ぶ

インタフェースセレクタウィンドウに表示されているインタフェースのアイコンとそのラベルを「インタフェースのエントリ」と呼びます。図 2-1 にインタフェースのエントリを示します。

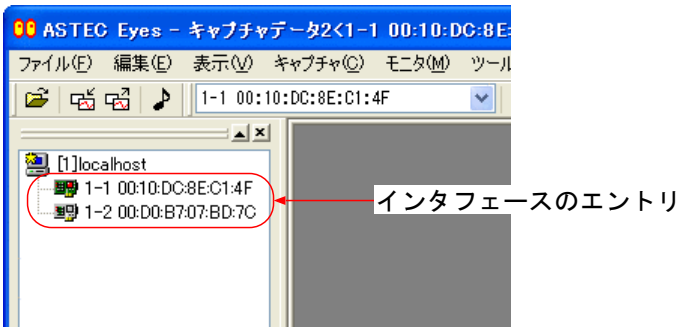


図 2-1: インタフェースのエントリ

選択中のインタフェースは (緑色) のアイコンで、その他のインタフェースは (灰色) のアイコンで表示されます。

ネットワークインタフェースを選ぶには、インタフェースセレクタウィンドウに表示されているインタフェースのエントリをクリックします。

選んだインタフェースのアイコンが (緑色) になったことを確認してください。

メインウィンドウのインタフェース選択リスト (1-2 00:D0:B7:07:BD:7C) を使って、ネットワークインタフェースを選ぶこともできます。

2.2 モニタを開始する

モニタを開始するには、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(図 2-2 参照)。

図 2-2: モニタを開始する

モニタを開始しただけでは、モニタウィンドウは表示されません。次に、トラフィックの統計情報を表示するモニタウィンドウを開いてみましょう。

2.3 モニタウィンドウを開く

モニタウィンドウを開くには、メインウィンドウの**モニタ(M)** メニューから表示したい項目を選びます。

モニタウィンドウには、トラフィックを表示するものや IP アドレスの一覧を表示するもの、MAC アドレスの一覧を表示するもの、 TCP のステータス情報を表示するものがあります。モニタウィンドウの中でもトラフィックを表示する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。

例として IP 層のトラフィックをプロトコル毎に分類したトラフィックを表示するトラフィックウィンドウを開いてみましょう。図 2-3 のように、メインウィンドウの**モニタ(M)** メニューから **0 IP 層プロトコル毎のトラフィック**を選びます。

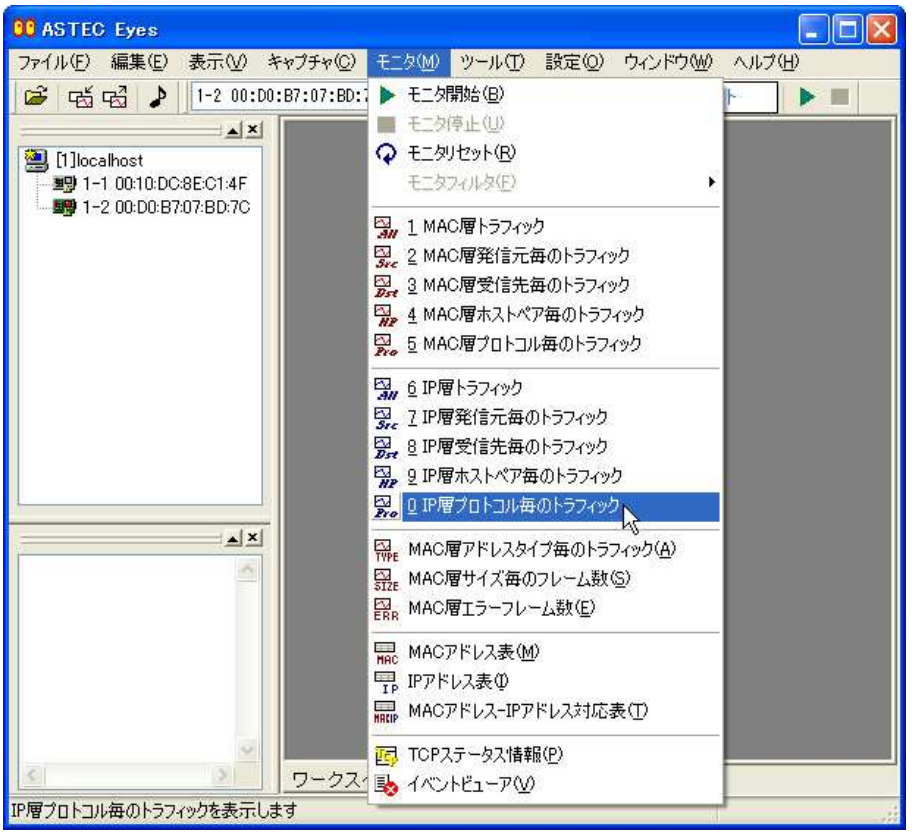


図 2-3: IP 層プロトコル毎のトラフィックを選ぶ

図 2-4 のような「IP 層プロトコル毎のトラフィック」のウィンドウが現れ、過去 5 分間の履歴が折れ線グラフで表示されます。

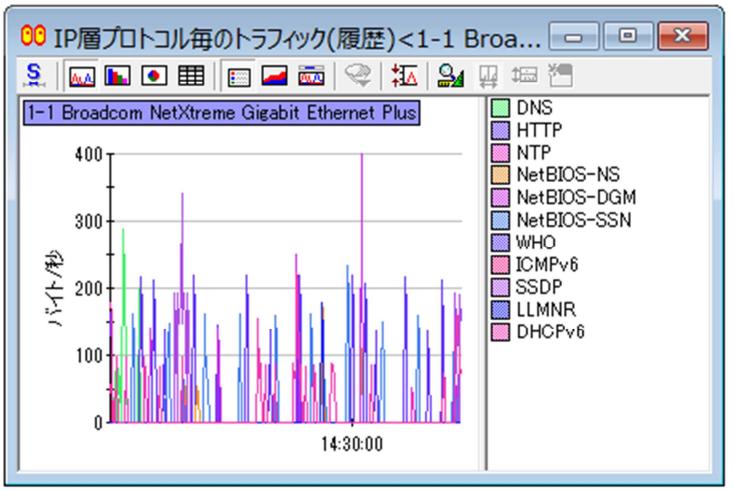


図 2-4: 「IP 層プロトコル毎のトラフィック」のウィンドウ

2.4 グラフの内訳を見る

トラフィックを分析していると、グラフに表示されている特定のトラフィックの内訳を見たいことがあります。 ASTEC Eyes は対話的な操作でグラフの内訳を表示できます。

1. 図 2-5 に示すように、トラフィックを表す折れ線の頂点付近をマウスでクリックします。
   トラフィックを表す折れ線を**グラフアイテム**と呼びます。

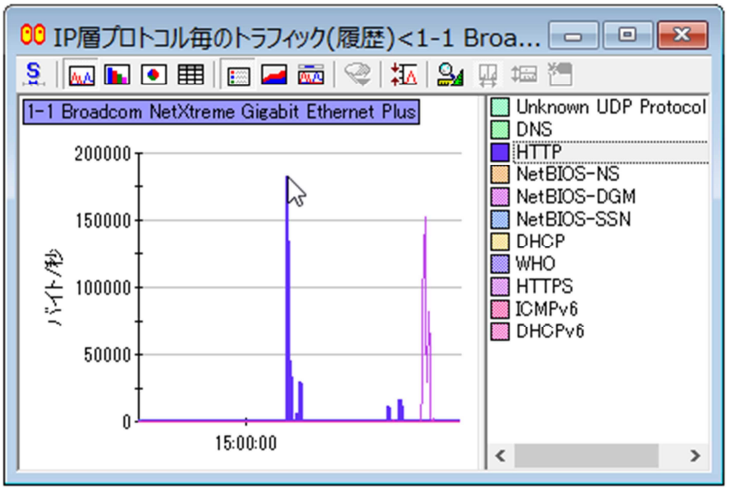


図 2-5: グラフアイテムを選ぶ

   図 2-5 は、 HTTP のグラフアイテムを選んでいます。

2. トラフィックウィンドウを右クリックします。
   図 2-6 のようなポップアップメニューが現れます。

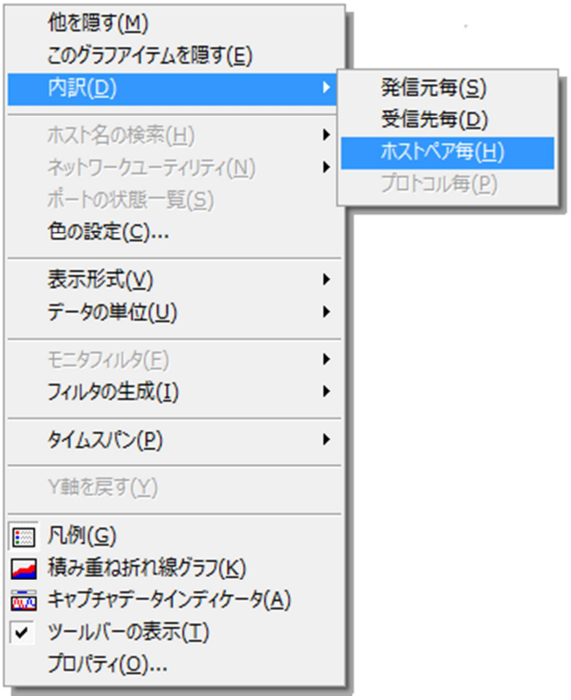


図 2-6: トラフィックウィンドウのポップアップメニュー

3. **内訳(D)** をポイントします。
   サブメニューが現れます。サブメニューには、表示できる内訳の種類を示すメニュー項目があります。
4. サブメニューから内訳の種類を選びます。
   ここでは、**ホストペア毎(H)** を選びます。トラフィックウィンドウの表示が、 IP 層のトラフィックをプロトコル毎に分類したグラフから HTTP のトラフィックの内訳を表示するグラフに変わります。そのようすを図 2-7 に示します。

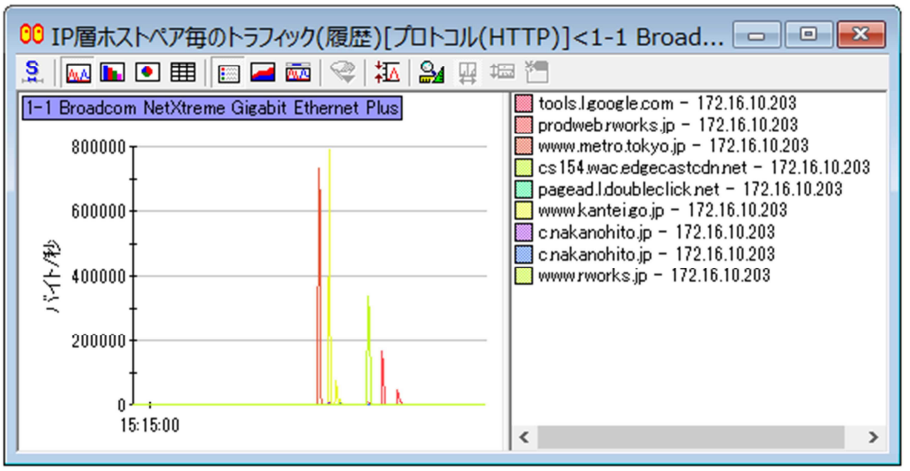


図 2-7: HTTP プロトコルを指定したホストペア毎の内訳

内訳を表示する前のグラフに戻すには、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、**元のグラフに戻る(B)** を選びます。

ここでは、トラフィックを分析する機能の 1 つとして、内訳を表示する機能をご紹介しました。 ASTEC Eyes は、他にもトラフィックの分析に役立つさまざまな機能を備えています。

モニタフィルタを使う

トラフィックウィンドウに表示するトラフィックを絞り込むことができます。複数のモニタフィルタを定義しておき、さまざまな角度からトラフィックを分析できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「モニタフィルタを使う」の節を参照してください。

表示形式を切り替える

折れ線グラフ以外に、棒グラフ、円グラフ、表形式でトラフィックを表示できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「トラフィックウィンドウの表示をカスタマイズする」の節の「表示形式」を参照してください。

Y 軸の単位を変える

Y 軸の単位をフレームや使用率に変えられます。また、バイト単位およびフレーム単位の場合の補助単位 (k ビット、 M バイト、 k フレーム、 M フレームなど) を選ぶこともできます。詳しくは『ASTEC Eyes ユーザー

ズガイド』の 2 章「モニタ機能」の「トラフィックウィンドウの表示をカスタマイズする」の節の「Y 軸の単位」を参照してください。

タイムスパンを切り替える

トラフィックの推移を表示する期間を切り替えることがきます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「トラフィックウィンドウの表示をカスタマイズする」の節の「タイムスパン」を参照してください。

Y 軸の範囲を指定する

対話的な操作で、 Y 軸の上限と下限を固定することができます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「トラフィックウィンドウの表示をカスタマイズする」の節の「Y 軸の範囲」を参照してください。

グラフの値を読み取る

折れ線グラフの値を読み取ることができます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「折れ線グラフの値を読み取る」の節を参照してください。

グラフアイテムの色をカスタマイズする

グラフアイテムやトラフィックウィンドウの前景色、および背景色を変更できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「トラフィックウィンドウの表示をカスタマイズする」の節の「グラフの色」を参照してください。

グラフの情報 (モニタ情報) を保存する

モニタ機能を使って収集した統計情報やアドレスの一覧を、 csv 形式などでファイルに保存できます。 詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「モニタ情報を csv 形式などで保存する」の節を参照してください。

モニタ情報を印刷する

モニタウィンドウに表示されているモニタ情報を印刷できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 13 章「その他の機能」の「印刷」の節を参照してください。

3章

ネットワークのパケットを分析する
～デコード機能～

ネットワークの状態を調べるためには、トラフィックを監視するだけでなく、実際にネットワークを流れているデータ (パケット) の内容を分析しなければならないことがあります。

パケットを分析するためには、まずネットワークを流れるパケットを**キャプチャバッファ**に取り込みます。これをパケットの**キャプチャ**と呼びます。取り込んだデータは**キャプチャデータ**と呼びます。

次に、キャプチャデータをそれぞれのプロトコルに基づいて解析します。キャプチャしたデータを解析することを**デコード**と呼びます。 デコードした結果はデコードビューに表示します。

具体的には、

1. キャプチャするネットワークインタフェースを選び、
2. キャプチャを開始し、
3. キャプチャを停止し、
4. デコードビューを生成します。

3.1 キャプチャするネットワークインタフェースを選ぶ

インタフェースセレクタウィンドウに表示されているインタフェースのアイコンとそのラベルを「インタフェースのエントリ」と呼びます。図 3-1 にインタフェースのエントリを示します。

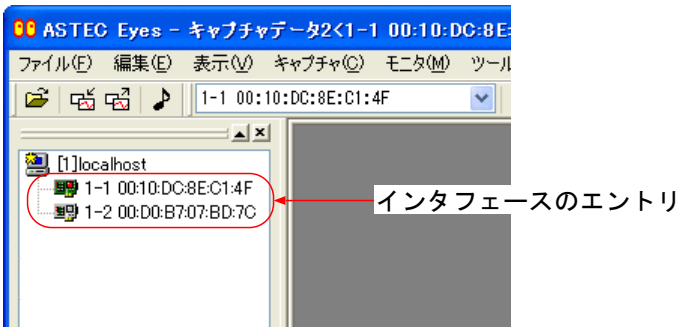


図 3-1: インタフェースのエントリ

選択中のインタフェースは (緑色) のアイコンで、その他のインタフェースは (灰色) のアイコンで表示されます。

ネットワークインタフェースを選ぶには、インタフェースセレクタウィンドウに表示されているインタフェースのエントリをクリックします。

選んだインタフェースのアイコンが (緑色) になったことを確認してください。

☞ メインウィンドウのインタフェース選択リスト (1-2 00:D0:B7:07:BD:7C) を使って、ネットワークインタフェースを選ぶこともできます。

3.2 キャプチャを開始する

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。 (図 3-2 参照)。

クリックするとキャプチャが開始する

図 3-2: キャプチャを開始する

キャプチャバッファにデータが取り込まれるにつれて、キャプチャバッファメーターのバーが右方向に伸びます。

3.3 キャプチャを停止する

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。 (図 3-3 参照)。

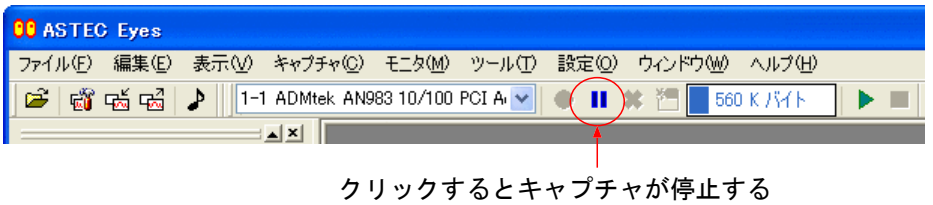


図 3-3: キャプチャを停止する

3.4 デコードビューを生成する

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。

キャプチャバッファのデータをデコードし、その結果を表示したデコードビューが現れます。そのようすを図 3-4 に示します。

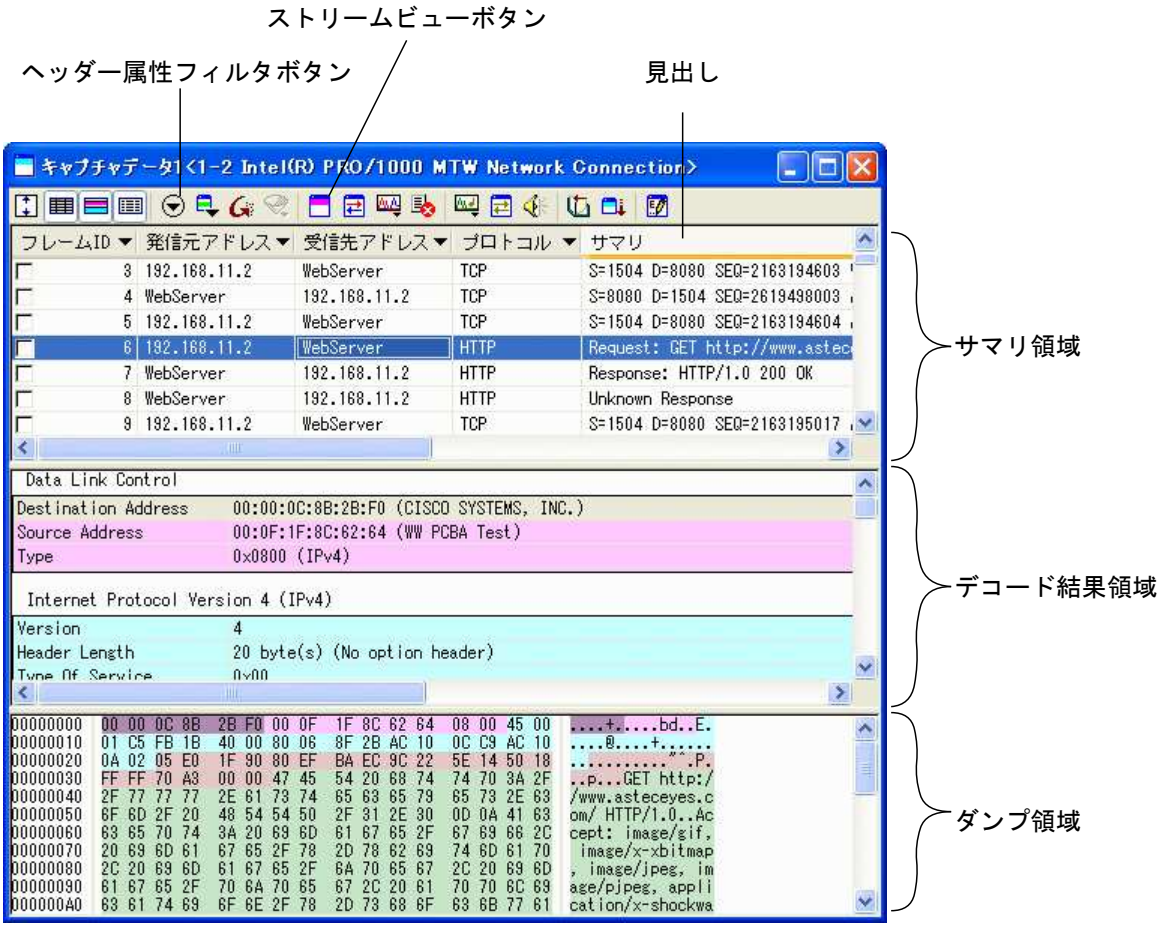


図 3-4: デコードビュー

デコードビューは、サマリ領域、デコード結果領域、ダンプ領域の 3 つの領域に分かれていま

す。

サマリ領域　パケットの概要を表示します。 1 行が 1 パケットに対応します。

デコード結果領域

パケットを詳細に解析した結果を表示します。各フィールドとその値の意味については、プロトコルを定義している RFC などのドキュメントを参照してください。

ダンプ領域　パケットのデータを 16 進ダンプの形式で表示します。

☞ インストール CD には、 RFC のドキュメントが含まれています。
たとえばインストール CD を D ドライブに挿入した場合、 RFC はディレクトリ
`D:¥Unsupported¥rfc¥`
にあります。

3.5 TCP ストリームを再構成してデコードする

ASTEC Eyes には、 TCP ストリーム (TCP のデータ部分) を再構成して表示する機能があります。

ストリームビューを開くには、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。図 3-5 のようなストリームビューが現れます。

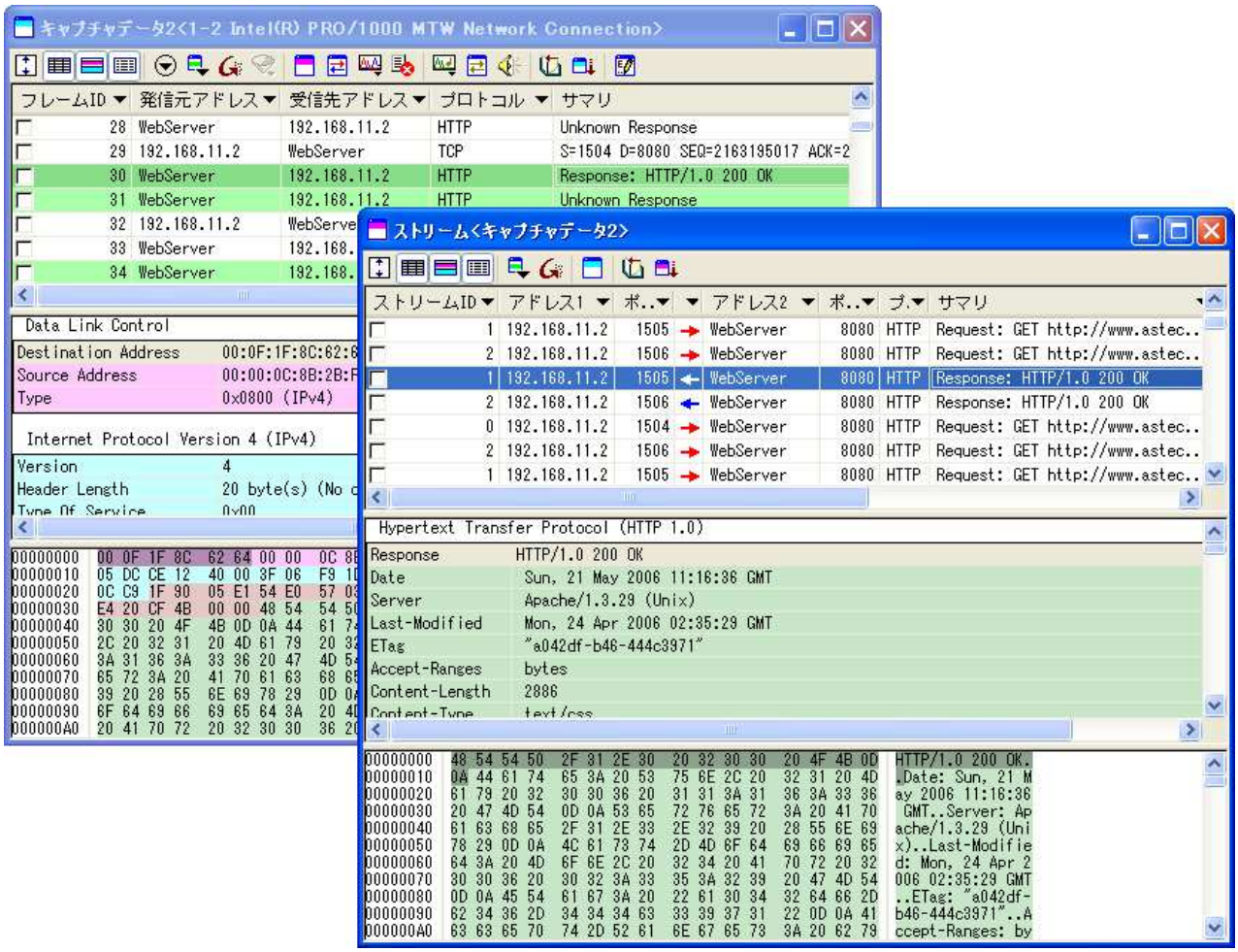


図 3-5: ストリームビューのレコードとデコードビューのパケットの関係

図 3-5 のデコードビュー (左側のウィンドウ) のフレーム ID 31 のパケットのサマリのカラムには、「Unknown Response」と表示されています。これはフレーム ID 30 のパケットの続きです。 HTTP プロトコルの 1 つのレスポンスが複数のパケットに分割されてしまったため、2 つ目以降のパケットは、パケット単体では正確にデコードできていません。アプリケーションによって定義される 1 つのレコードを複数のパケットに分割して送信することは、 TCP を使ったアプリケーションではよくあることです。

このような場合にストリームビューを使います。ストリームビューには、 TCP ストリームを再構成してデコードした結果を表示します。

ストリームビューのサマリ領域の 1 行は、それぞれのプロトコルで定義される 1 レコードに対応します。ストリームビューのサマリ領域の行をクリックすると、クリックしたレコードを構成する (デコードビューの) パケットが緑色でハイライト表示されます。

図 3-5 のストリームビュー (右側のウィンドウ) のサマリ領域のサマリのカラムに、「Unknown Response」という表示はありません。 TCP ストリームを再構成して、データを正しく解析できています。

3.6 デコード結果を絞り込む

デコードビューに表示されているデコード結果から目的のパケットを見つけたり、ストリームビューで特定のストリームだけを追いたいときなど、フィルタを使ってデコード結果を絞り込むことができます。

デコード結果を絞り込むフィルタは 4 種類あります。

見出しフィルタ
サマリ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。詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「見出しフィルタ」を参照してください。

ヘッダー属性フィルタ
パケットのヘッダーのさまざまな属性 (たとえば、 IPv4 プロトコルの発信元アドレスや TCP のポート番号など) を基にパケットを分類し、指定された属性に合致するパケットだけを表示するフィルタです。詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「ヘッダー属性フィルタ」を参照してください。

デコード結果フィルタ
デコード結果領域に表示した内容を対象として、指定した文字列を含むパケットまたはレコードだけを表示するフィルタです。詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「デコード結果フィルタ」を参照してください。

ディスプレイフィルタ
フィルタの条件をユーザーが定義できるフィルタです。フィルタの条件となる論理式は、フィルタエディタで定義します。

論理式を定義する方法については、『ASTEC Eyes ユーザーズガイド』の 9 章「フィルタエディタ」を参照してください。

論理式で定義されたフィルタを適用する方法については、『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「ディスプレイフィルタ」を参照してください。

ここでは、ヘッダー属性フィルタを使ってみます。

1. デコードビューのツールバーにある**ヘッダー属性フィルタ**ボタン() をクリックします。
   次のようなメニューが現れます。

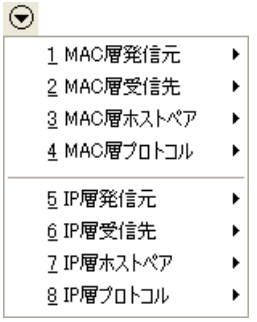


図 3-6: ヘッダー属性フィルタのメニュー

2. **7 IP 層ホストペア**を選びます。
   デコードビューに表示されているパケットを IP 層の発信元と受信先のホストペアで分類した結果をメニュー項目とするサブメニューが現れます。
3. サブメニューから適当なメニュー項目を選びます。
   WebServer- 172.16.12.242 というメニュー項目を選んでいるようすを図 3-7 に示します。

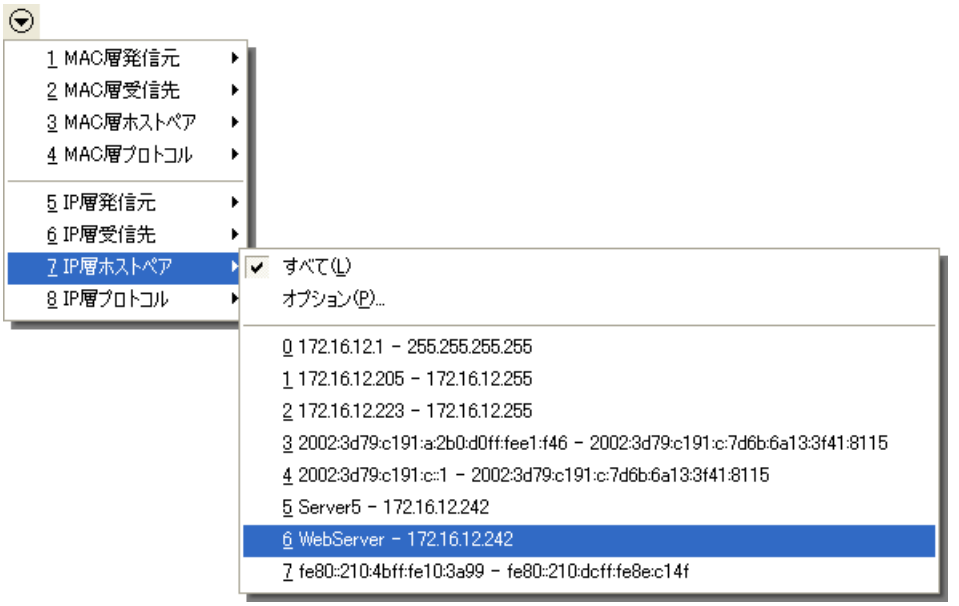


図 3-7: IP 層のホストペアを選ぶ

デコードビューは、 WebServer と 172.16.12.242 の間でやり取りされた IP 層のパケット

だけを表示するようになります。
ヘッダー属性フィルタボタンのアイコンは、フィルタが適用されていることを示すために青(⊕) に変わります。

デコードビューのツールバーにある**フィルタ解除**ボタン(G) をクリックすると、適用されているフィルタがすべて解除され、すべてのパケットを表示するようになります。

4章

長期間にわたるトラフィックのトレンドを調べる ～ログ機能～

長期間にわたるトラフィックのトレンドを調べるには、ログを出力して分析します。

ログとは、一定時間毎にファイルに出力するネットワークのトラフィックの統計情報のことです。

4.1 ログの出力を開始する

ログの出力を開始するには、次のようにします。

1. メインウィンドウの**設定(O)** メニューから**ログ機能(G)** を選びます。
2. サブメニューからログの出力を開始したいホストを選びます。
   「ホストのプロパティ」ダイアログが現れます。

図 4-1: 「ログ」のページを表示した「ホストのプロパティ」ダイアログ

3. **ログを出力する(L)** にチェックを付けます。
4. **OK** ボタンをクリックします。

デフォルトでは、 5 分間隔でログを作り、 6 回分のログを 1 つのファイルに書きます。

ログファイルにログを書いている間は、ログを見ることができません。そのため、最低 1 つのログファイルを書き終わるまではログを表示できません。デフォルトの設定では、ログの出力を開始してから 30 分後 (5 分 × 6 回 = 30 分間) にログを表示できます。

ログの設定について、詳しくは『ASTEC Eyes ユーザーズガイド』の 3 章「ログ機能」を参照してください。

4.2 ログを見る

この節は、ログの出力を開始してから、少なくとも (ログの出力間隔 × 同一ファイルへの書き込み回数) 分が経過した後に行ってください。デフォルトの設定でログの出力を開始した場合は、開始してから 30 分以上経過した後に行ってください。

ログを見るためにログの出力を停止する必要はありません。

ログを見るには、次のようにします。

1. ログを出力している (出力していた) ホスト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**ログの一覧を作成(L)** を選びます。
   ログファイルの解析が行われます。解析が終わるとログ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 4-2 に示します。

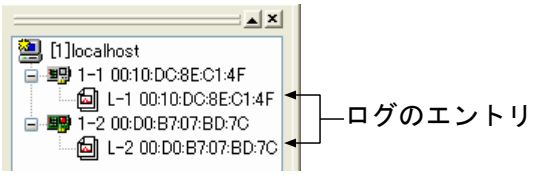


図 4-2: ログのエントリが現れたインタフェースセレクタウィンドウ

3. ログ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。
4. ポップアップメニューから**ログを表示(L)**. . . を選びます。
   図 4-3 のような「ログの表示」ダイアログが現れます。

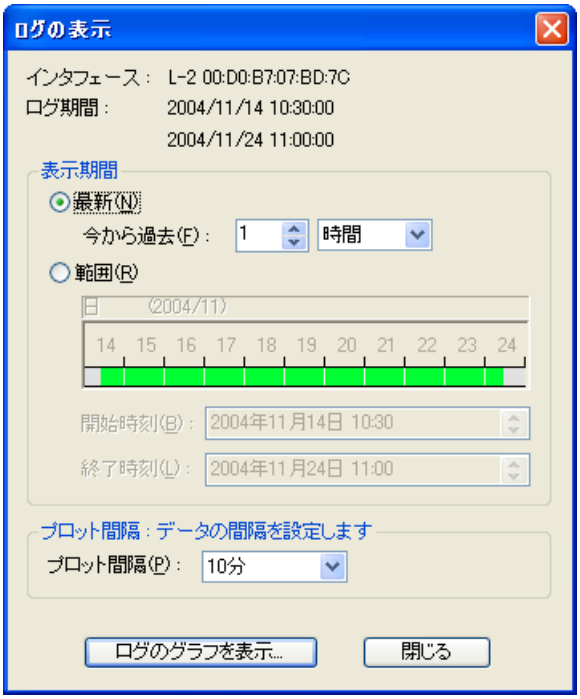


図 4-3: 「ログの表示」ダイアログ

5. **ログのグラフを表示...** ボタンをクリックします。
   メニューが現れます。メニューには表示できるトラフィックの種類があります。そのようすを図 4-4 に示します。

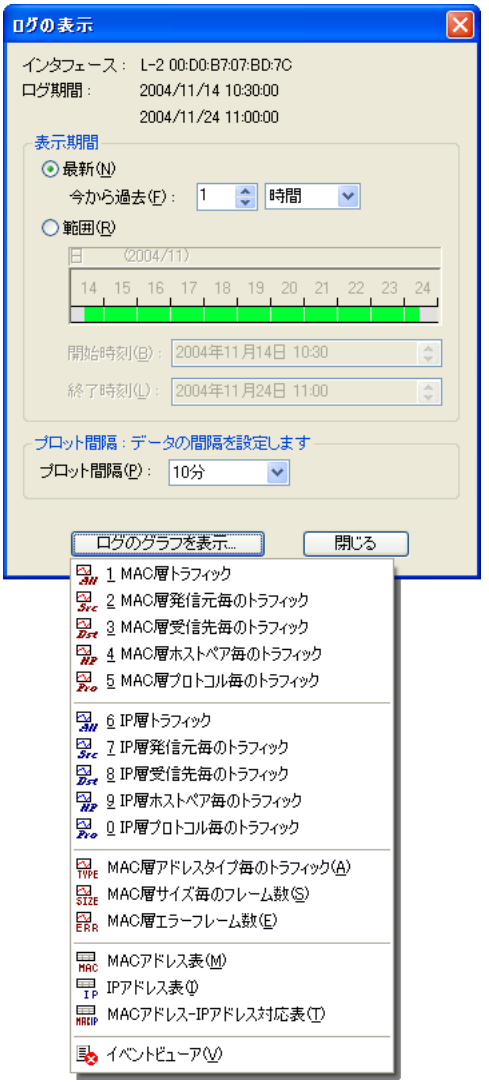


図 4-4: トラフィックの種類を表示した「ログの表示」ダイアログ

6. メニューから項目を選ぶと、ログを表示したモニタウィンドウが現れます。

ログを見る方法について、詳しくは『ASTEC Eyes ユーザーズガイド』の 3 章「ログ機能」の「ログを見る」の節を参照してください。

4.3 ログの出力を停止する

ログの出力を停止するには、次のようにします。

1. メインウィンドウの**設定(O)** メニューから**ログ機能(G)** を選びます。
2. サブメニューからログの出力を停止したいホストを選びます。「ホストのプロパティ」ダイアログが現れます (図 4-1 参照)。
3. **ログを出力する(L)** のチェックを外します。
4. **OK** ボタンをクリックします。

5章

リモートモジュールを使う

離れた場所にあるホストで動作しているリモートモジュールに**接続するだけ**で、リモートモジュールが接続しているネットワークを監視できます。

リモートモジュールが接続しているネットワークのトラフィックを見たり、パケットをキャプチャする方法は、ローカルホストが接続しているネットワークの場合とまったく同じです。

5.1 リモートモジュールに接続する

リモートモジュールに接続するには、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何も表示されていない部分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**リモートへの接続(C)**... を選びます。
   図 5-1 のような「接続」ダイアログが現れます。

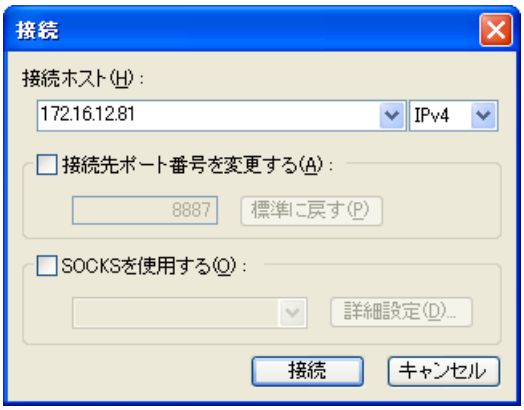


図 5-1: 「接続」ダイアログ

3. **接続ホスト(H)** にホスト名を入力します。
   NetBIOS 名や DNS 名、 IP アドレスなど、ローカルホストが認識できるホスト名を指定します。
4. **接続**ボタンをクリックします。
   接続に成功した場合は、インタフェースセレクタウィンドウにリモートモジュールのホストのエントリとインストールしてあるネットワークインタフェースのエントリが現れます。そのようすを図 5-2 に示します。

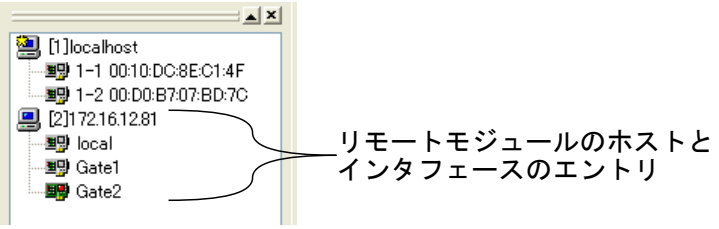


図 5-2: リモートモジュールのホストとインタフェースのエントリが現れた
インタフェースセレクタウィンドウ

リモート監視機能について、詳しくは『ASTEC Eyes ユーザーズガイド』の 8 章「リモート監視機能」を参照してください。

6章

その他の機能

これまでご紹介した機能の他にも ASTEC Eyes にはさまざまな機能があります。詳しくは、『ASTEC Eyes ユーザーズガイド』を参照してください。

エキスパート機能　モニタエキスパート機能とデコードエキスパート機能があります。

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 (イベントと呼びます) を発見し、表示する機能です。

デコードエキスパート機能は、キャプチャデータをデコードする際に、トラブルの元となるかもしれないイベントを見つけ、表示する機能です。詳しくは『ASTEC Eyes ユーザーズガイド』の 10 章「エキスパート機能」を参照してください。

通知機能　モニタエキスパート機能により検出したイベントをメールや SNMP で通知する機能です。詳しくは『ASTEC Eyes ユーザーズガイド』の 10 章「エキスパート機能」の「通知機能の設定」の節を参照してください。

トラフィックジェネレータ機能

新たに作ったパケットやキャプチャしたパケットを編集して、ネットワークへ送信する機能です。詳しくは『ASTEC Eyes ユーザーズガイド』の 7 章「トラフィックジェネレータ機能」を参照してください。

ホスト名の検索　IP アドレスに対応するホスト名を DNS、 WINS (NetBIOS)、および NIS ネームサービスを利用して検索できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 12 章「ホスト名の表示」の「ホスト名の検索」の節を参照してください。

アドレス帳　ホストを識別しやすいように、ユーザーが適切な名前を付けることができます。詳しくは『ASTEC Eyes ユーザーズガイド』の 12 章「ホスト名の表示」の「アドレス帳を使う」の節を参照してください。

ワークスペース
複数のワークスペースを作り、ウィンドウを整理できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 13 章「その他の機能」の「ワークスペース」の節を参照してください。

グラフ (モニタ情報) の保存
モニタウィンドウに表示されている情報 (モニタ機能を使って収集した統計情報やアドレスの一覧) を、 csv 形式などでファイルに保存できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「モニタ情報を csv 形式などで保存する」の節を参照してください。

レポート機能
ワークスペースに表示されているモニタやログのウィンドウを、 HTML 形式のレポートとして出力できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 4 章「レポート機能」を参照してください。

印刷
モニタウィンドウに表示しているモニタ情報、デコードビューやストリームビューに表示しているデコード結果を印刷できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 13 章「その他の機能」の「印刷」の節を参照してください。

連続キャプチャ機能
連続的にキャプチャを行い、直接ファイルにキャプチャデータを保存できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 5 章「キャプチャ機能」の「連続キャプチャ」の節を参照してください。

デコードヒント
プロキシサーバーを利用している場合など、 Well known ポートとは異なるポートを使っているプロトコルのトラフィックを正しくモニタしたり、デコードしたりするためには、デコードヒントの設定が必要です。詳しくは『ASTEC Eyes ユーザーズガイド』の 11 章「オプションの設定」の「デコードヒントを設定する」の節を参照してください。

グラフ解析機能
トラフィックウィンドウに表示されている折れ線グラフの値を読み取ることができます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「折れ線グラフの値を読み取る」の節を参照してください。

音声品質の測定
ASTEC Eyes *for* VoIP では、 IP 電話などの音声品質を測定できます。詳しくは『ASTEC Eyes *for* VoIP』を参照してください。

シーケンス表示
ASTEC Eyes *for* VoIP では、 IP 電話のシーケンス (H323 または SIP による呼制御のようすと RTP による音声データのやり取りのようす) を見ることができます。詳しくは『ASTEC Eyes *for* VoIP』を参照してください。

音声の再生

ASTEC Eyes *for* VoIP に VoIP Player オプションを追加すれば、キャプチャデータに含まれる音声データを抽出し、再生できます。詳しくは『ASTEC Eyes *for* VoIP』を参照してください。

付録 A

用語集

本書で使っている用語について説明します。

RFC (Request for Comments)

インターネットに関する技術情報や仕様、運用規則などを定める文書です。インターネットに関する技術の標準を定める団体である IETF (Internet Engineering Task Force) が発行、管理しています。

TCP ステータス情報

TCP の接続状態で、モニタウィンドウに表示されます。

インタフェース

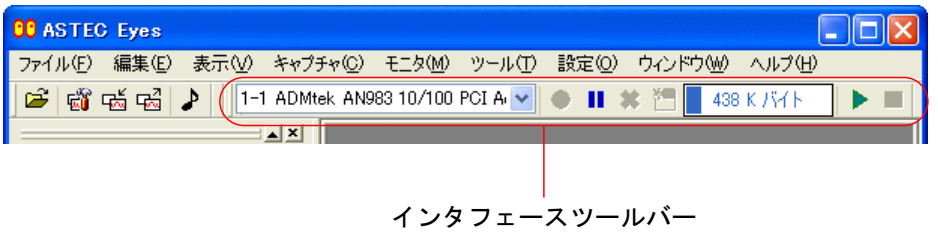
ネットワークインタフェースのことです。

インタフェースセレクタウィンドウ

インタフェースを選ぶ、リモートモジュールと接続するなど、インタフェースに関する操作を行う機能を備えたウィンドウです。

インタフェースツールバー

メインウィンドウにあるツールバーです。モニタを開始または停止したり、キャプチャを開始または停止するなど、選んでいるインタフェースに対して操作を行うためのボタンがあります。また、ボタンはユーザーがカスタマイズできます。



詳しくは『ASTEC Eyes ユーザーズガイド』の 1 章「各機能を使う前の準備」の「ASTEC Eyes のメインウィンドウ」の節の「ツールバー」を参照してください。

エキスパート機能

モニタエキスパート機能とデコードエキスパート機能があります。

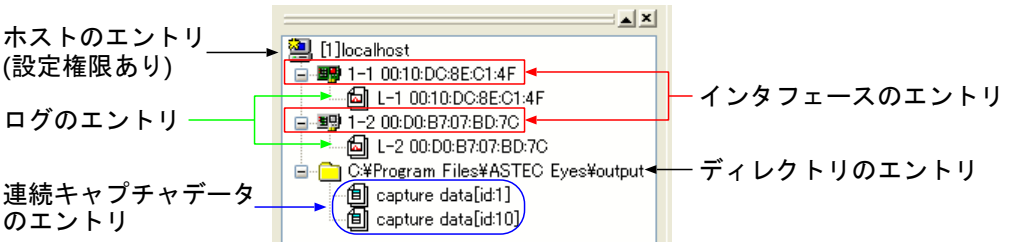
モニタエキスパート機能は、ネットワークのモニタ中に、トラブルの予兆 (イベントと呼びます) を発見し、表示する機能です。

デコードエキスパート機能は、キャプチャデータをデコードする際に、トラブルの元となるかもしれないイベントを見つけ、表示する機能です。

どちらのエキスパート機能も検出するイベントをユーザーが設定できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 10 章「エキスパート機能」を参照してください。

エントリ

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、ネットワークインタフェース、ログ、連続キャプチャデータ、およびディレクトリのアイコンとそのラベルを指します。



簡易フィルタ

デコードビューやストリームビューで、GUI 操作だけで手軽にパケットやレコードを絞り込むフィルタです。簡易フィルタには、見出しフィルタ、ヘッダー属性フィルタ、およびデコード結果フィルタがあります。

期間指定バー

「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」ダイアログで、データの範囲を指定するためのものです。データの範囲を指定するための開始時刻と終了時刻をマウス操作で入力できます。

キャプチャ開始トリガ

特定のパケットがネットワークに流れたことをきっかけにしてキャプチャを開始する機能です。キャプチャ開始トリガはインタフェースごとにフィルタエディタで定義します。

キャプチャ停止トリガ

特定のパケットがネットワークに流れた事をきっかけにしてキャプチャを停止する機能です。キャプチャ停止トリガはインタフェースごとにフィルタエディタで定義します。

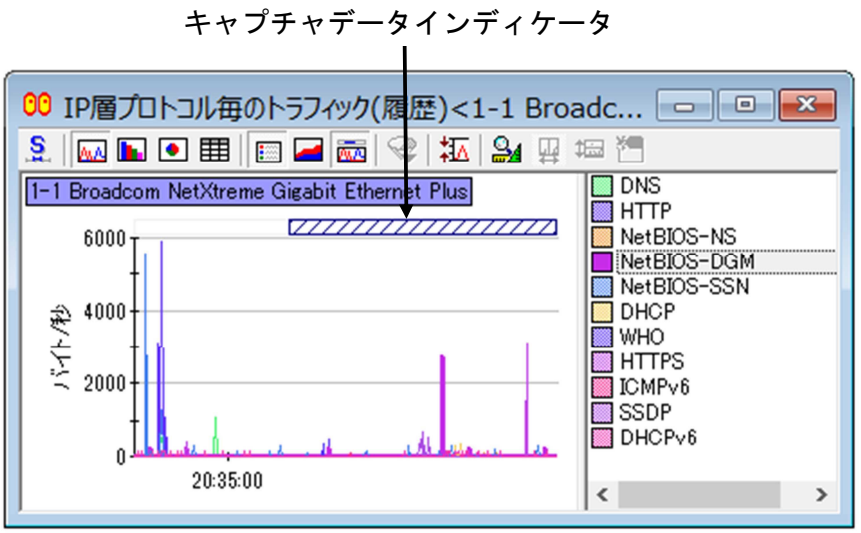
キャプチャデータ

キャプチャまたは連続キャプチャしたパケットのデータのことです。

キャプチャデータインディケータ

トラフィックウィンドウにおいては、キャプチャバッファ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表すものです。

ログを表示しているウィンドウにおいては、ログと関連付けられた連続キャプチャデータのうち、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表すものです。



キャプチャデータマネジャー

1 つ以上のキャプチャファイルをマージし、1 つのキャプチャデータとして扱うための機能です。デコードする範囲を期間やパケットヘッダーの値で制限できます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「キャプチャデータマネジャーを使う」の節を参照してください。

キャプチャバッファ

パケットを取り込むためのバッファです。 ASTEC Eyes またはリモートモジュールが動作しているホストのメモリ上に確保されます。キャプチャバッファのサイズやキャプチャバッファがフルになったときの動作を設定できます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 11 章「オプションの設定」の「キャプチャのオプションを設定する」の節を参照してください。

キャプチャフィルタ

特定の条件を満たすパケットのみをキャプチャするためのフィルタです。キャプチャフィルタはインタフェースごとにフィルタエディタで定義します。

グラフアイテム

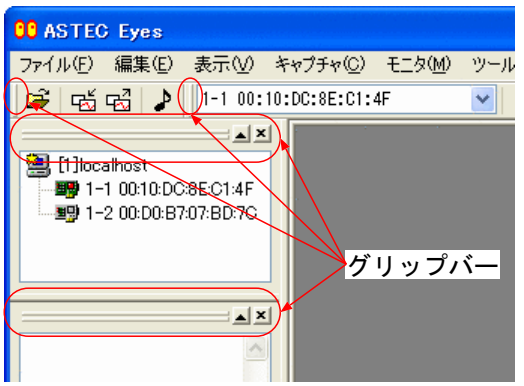
グラフに表示されている折れ線、棒、または扇形の各要素のことです。

グラフ解析機能

トラフィックウィンドウを折れ線グラフ表示にしているときに、グラフの値を読み取る機能です。読み取った値はメッセージウィンドウに表示されます。

グリップバー

コモンツールバーや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、メッセージウィンドウのサイズや位置を変えたり、ドッキング状態とフローティング状態の切り替えをするために使います。



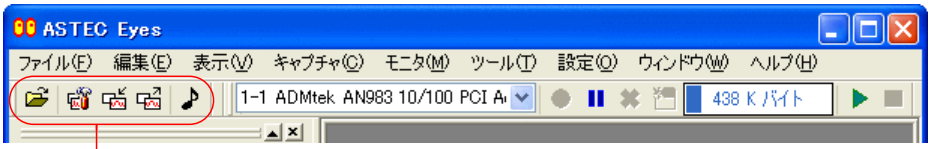
更新間隔

トラフィックウィンドウのグラフを更新する間隔です。短期タイムスパンのときは、更新間隔を選べます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 11 章「オプションの設定」の「モニタのオプションを設定する」の節を参照してください。

コモンツールバー

メインウィンドウにあるツールバーです。ファイルに保存してあるキャプチャデータの読み込みや、設定情報の保存または読み込みなど、選択中のインタフェースに依存しない操作を行うためのボタンがあります。また、ボタンはユーザーがカスタマイズできます。



コモンツールバー

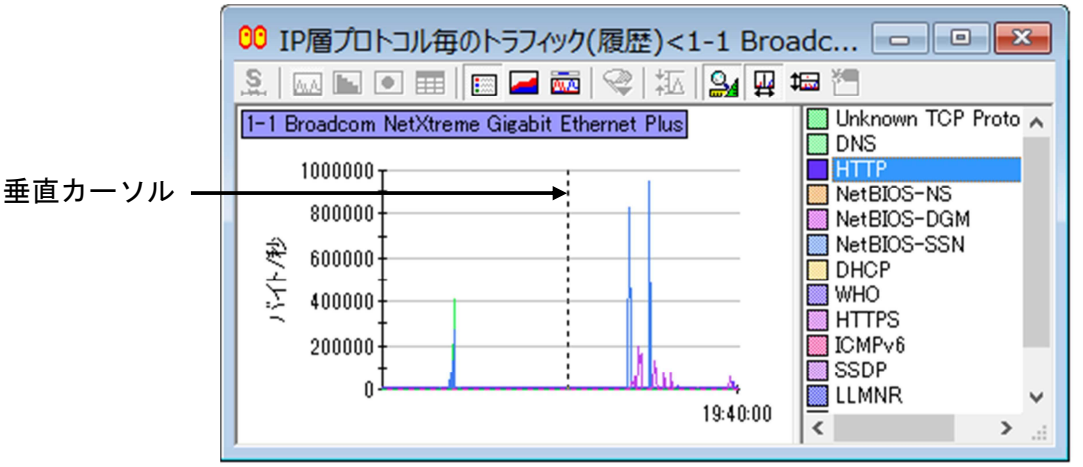
詳しくは『ASTEC Eyes ユーザーズガイド』の 1 章「各機能を使う前の準備」の「ASTEC Eyes のメインウィンドウ」の節の「ツールバー」を参照してください。

サマリ領域

デコードビューまたはストリームビューで、パケットまたはレコードの概要を表示する領域です。デコードビューおよびストリームビューの一番上の領域です。

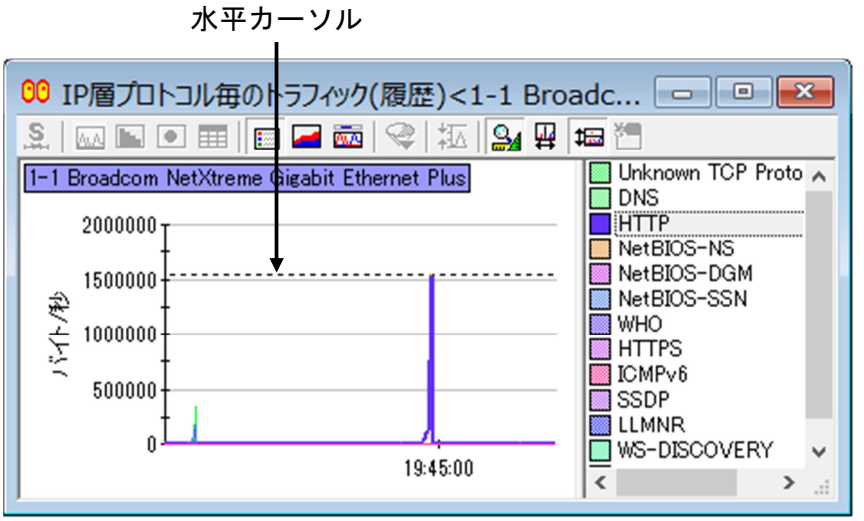
垂直カーソル

トラフィックウィンドウに表示されているグラフの値を読み取る状態で、**垂直カーソル**ボタン( ) をクリックすると現れるカーソルです。破線で示されます。



水平カーソル

トラフィックウィンドウに表示されているグラフの値を読み取る状態で、**水平カーソル**ボタン( ) をクリックすると現れるカーソルです。破線で示されます。



ステータスバー

ASTEC Eyes の状態やモニタウィンドウで選んでいるグラフアイテムの名前など、さまざまな情報を表示します。図 1-2 を参照してください。

ストリームビュー

TCP ストリームを再構成してデコードした結果を表示するウィンドウです。

設定権限

ログや連続キャプチャの開始および停止、インタフェースのラベルを変えるなど、特定の操作を行うために必要な権限です。詳しくは『ASTEC Eyes ユーザーズガイド』の 8 章「リモート監視機能」の「設定権限の取得と開放」の節を参照してください。

選択したセル

表形式のモニタウィンドウ、デコードビューおよびストリームビューのサマリ領域、「オプション」ダイアログの「デコードヒント」のパネルなどにおいて、編集または操作の対象としているセルのことです。白い枠で囲まれています。

タイムスパン

トラフィックの統計情報を表示する期間のことです。短期、中期、長期の 3 つのタイムスパンを切り替えて表示できます。詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「トラフィックウィンドウの表示をカスタマイズする」の節の「タイムスパン」を参照してください。

ダンプ領域

デコードビューまたはストリームビューでパケットまたはレコードのデータを 16 進ダンプの形式で表示する領域です。デコードビューおよびストリームビューの一番下の領域です。

デコード結果フィルタ

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。

詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「デコード結果フィルタ」を参照してください。

デコード結果領域

デコードビューまたはストリームビューでパケットまたはレコードを解析した結果を表示する領域です。デコードビューおよびストリームビューの中央の領域です。

デコードビュー

キャプチャバッファのデータやキャプチャファイルのデータをデコードした結果を表示するウィンドウです。

デコードヒント

TCP または UDP ポートとプロトコルを関連付けるための情報です。特定の IP アドレスを指定して、ポート番号とプロトコルを対応させることもできます。たとえば、プロキシサーバーで Well known ポート以外のポートを使っている場合に、その情報をデコードヒントとして設定します。

詳しくは『ASTEC Eyes ユーザーズガイド』の 11 章「オプションの設定」の「デコードヒントを設定する」の節を参照してください。

ディスプレイフィルタ

デコードビューに表示するパケットを絞り込むためのフィルタです。複数のディスプレイフィルタをフィルタエディタで定義できます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「ディスプレイフィルタ」を参照してください。

トラフィックウィンドウ

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
- MAC 層サイズ毎のフレーム数
- MAC 層エラーフレーム数

ネットワークインタフェース

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) のことです。 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を行う前に、対象とするネットワークインタフェースを選ぶ必要があります。

詳しくは『ASTEC Eyes ユーザーズガイド』の 1 章「各機能を使う前の準備」の「インタフェース」の節を参照してください。

フィルタエディタ

フィルタエディタは、次のフィルタを定義するための論理式を編集するためのエディタです。

- ディスプレイフィルタ
- モニタフィルタ
- 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

詳しくは『ASTEC Eyes ユーザーズガイド』の 9 章「フィルタエディタ」を参照してください。

ヘッダー属性フィルタ

パケットヘッダーの値を基に、デコードビューに表示するパケットを絞り込むためのフィルタです。

ヘッダー属性フィルタについて、詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「ヘッダー属性フィルタ」を参照してください。

見出しフィルタ

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。デコードビューとストリームビューのサマリ領域、およびイベントビューアのカラムのうち、見出しに▼がついているカラムで使えます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 6 章「デコード機能」の「フィルタを使う」の節の「見出しフィルタ」を参照してください。

メッセージウィンドウ

ASTEC Eyes の重要なメッセージを表示するウィンドウです。トラフィックウィンドウのグラフから読み取った値を表示したり、ホスト名を検索中の IP アドレスなどを表示します。図 1-2 を参照してください。

モニタウィンドウ

モニタ情報を表示するウィンドウです。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。

詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「モニタと開始と停止」の節の「モニタウィンドウを開く」を参照してください。

モニタ情報

トラフィックの統計情報や IP アドレス、 MAC アドレス、 TCP の接続に関する情報など、モニタ中に収集した情報のことです。

モニタフィルタ

モニタするパケットを絞り込むためのフィルタです。複数のモニタフィルタをフィルタエディタで定義できます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 2 章「モニタ機能」の「モニタフィルタを使う」の節を参照してください。

リモートモジュール

ASTEC Eyes 基本パッケージと同じ情報収集力を持ったソフトウェアで、複数の ASTEC Eyes 基本パッケージに接続して、収集した情報を送ることができます。離れた場所にあるホストにインストールしておけば、ローカルホストで動作している ASTEC Eyes で離れた場所にあるネットワークを監視できます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 8 章「リモート監視機能」を参照してください。

連続キャプチャ

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出力する機能です。

詳しくは『ASTEC Eyes ユーザーズガイド』の 5 章「キャプチャ機能」の「連続キャプチャ」の節を参照してください。

連続キャプチャフィルタ

連続キャプチャを行う際、特定の条件を満たすパケットのみをキャプチャするためのフィルタです。連続キャプチャフィルタはインタフェースごとにフィルタエディタで定義します。

連続キャプチャ開始トリガ

特定のパケットがネットワークに流れたことをきっかけにして連続キャプチャを開始する機能です。連続キャプチャ開始トリガはインタフェースごとにフィルタエディタで定義します。

連続キャプチャ停止トリガ

特定のパケットがネットワークに流れた事をきっかけにして連続キャプチャを停止する機能です。連続キャプチャ停止トリガはインタフェースごとにフィルタエディタで定義します。

ログ

一定時間ごとにファイルに出力するモニタ情報およびイベントのことです。詳しくは『ASTEC Eyes ユーザーズガイド』の 3 章「ログ機能」を参照してください。

ワークスペース

モニタウィンドウ、デコードビュー、ストリームビューなど、ダイアログ以外のウィンドウを表示する領域です。 ASTEC Eyes では、複数のワークスペースを切り替えて使うことができます。

詳しくは『ASTEC Eyes ユーザーズガイド』の 13 章「その他の機能」の「ワークスペース」の節を参照してください。

索引

A

Administrator 権限 5
ASTEC Eyes のメインウィンドウ 6
ASTEC Eyes の起動 4

C

csv (モニタ情報の保存) 18

い

インタフェースのエントリ 11, 20
インタフェースを選ぶ 11, 20

き

起動 (ASTEC Eyes) 4
起動 (リモートモジュール) 8
キャプチャデータの
デコード (解析) 19, 23

さ

サマリ領域 (デコードビュー) 24

す

ストリームビュー 26

せ

製品サポート 3

だ

ダンプ領域 (デコードビュー) 24

で

デコード (キャプチャデータ) 19, 23
デコード結果領域
(デコードビュー) 24
デコードビュー 23

と

トラフィックを見る 10

ね

ネットワークインタフェースを選ぶ
11, 20
ネットワークのトラフィックを見る 10

ぱ

パケットのキャプチャ 19

ひ

表記法 2

ふ

フィルタ (ヘッダー属性フィルタ)
27

へ

ヘッダー属性フィルタ 27

め

メインウィンドウ 6

も

モニタ機能 10

り

リモートモジュールの起動 8
リモートモジュールを使う 37

ASTEC Eyes on the net バージョン 7.2
ASTEC Eyes 入門

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)