BackOffice 原稿(７回目)
「入門・ビギナーのためのネットワークトラブル対策」

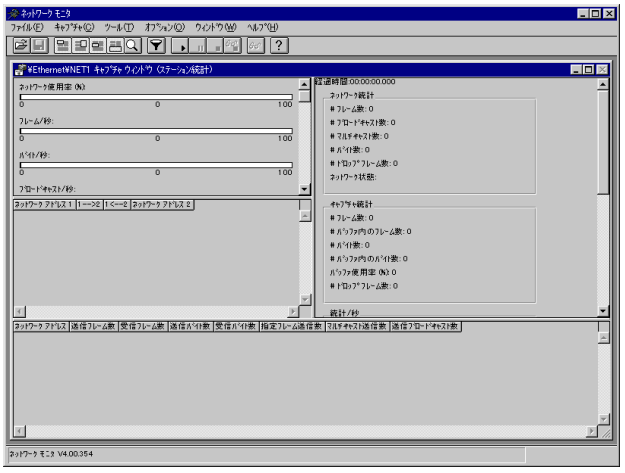
奥川博司

ネットワークモニタの使い方

今回は、前回の後半にてトラブル解決のために役に立つ手段として紹介したSMSネットワークモニタの使い方について紙面の許す範囲で詳しく説明していきます。*1

ネットワークモニタは、キャプチャウィンドウと フレームビューアウィンドウという２種類のウィンドウを持っており、どちらのウィンドウがアクティブになっているかによってメニューやツールバーの項目も変化します。
キャプチャウィンドウでは、キャプチャの開始や停止など 実行系のコマンドになっており、フレームビューアウィンドウではキャプチャ済みのデータに対する表示系のコマンドが主になっています。
ネットワークモニタを起動した直後は、キャプチャウィンドウだけが表示された状態になっており、表示すべきデータがまだ存在していないためフレームビューアウィンドウは表示されていません。(図１)

図１.ネットワークモニタの実行画面



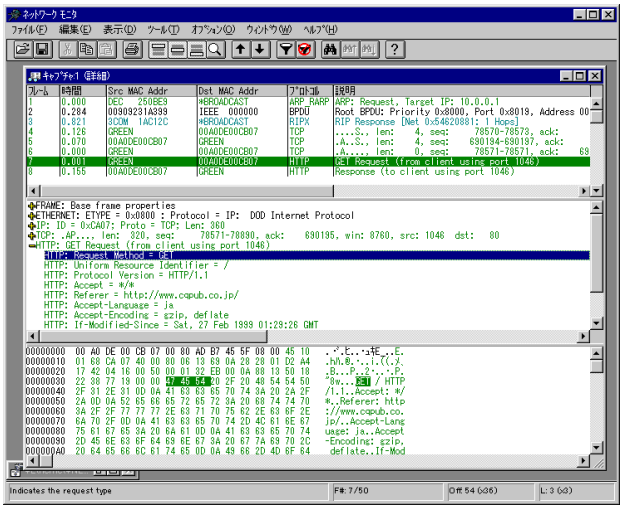
◇ キャプチャウィンドウの説明

キャプチャウィンドウに表示されている項目について簡単に説明していきます。画面は図１を参照。
画面左上(グラフパネル)には、キャプチャ実行中のネットワーク使用率や、フレーム(パケットの別の言い方。ネットワーク上を流れる情報のまとまりである最小単位。今回はフレームという呼び方で統一します)、バイト、ブロードキャスト*2、マルチキャスト*3の量などが表示されます。
画面左中段(セッション統計パネル)には、通信相手とのペアであらわされた通信状況が表示されます。
画面下段(ステーション統計パネル)には、各ノード毎の送受信フレーム数、送受信バイト数、単一ノードに対する送信フレーム数、マルチキャスト送信数、ブロードキャスト送信数が表示されます。キャプチャを開始するとネットワークモニタが各ノードから送信されたフレームを検出することでデータが増えていくのを見て取ることができると思います。各カラムのヘッダをダブルクリックすることで表示順序を変更できるので どのノードが一番フレームを送信しているのかといったことも簡単に調べることができます。
画面右上段(合計パネル)には、ネットワーク統計、キャプチャ統計、統計/秒、ネットワークカード(MAC)統計、ネットワークカード(MAC)エラー統計に関する情報が、各カテゴリに分類されて表示されます。表示項目の一覧を表１に示します。ネットワークカードから得る統計情報は利用しているネットワークカードによってはサポートされていなかったり(「サポート外」と表示される)、数字が表示されたとしても正しい値を返さない場合もあるので目安程度に考えたほうが良いかもしれません。
これらそれぞれのパネルは、[ウィンドウ]メニューを使用して、表示・非表示を切り替えたり拡大表示を行うことができます。

◇ フレームビューアウィンドウの説明

次に、キャプチャしたデータを見るためのフレームビューアウィンドウについて説明していきます。(図２)

図２.フレームビューアウィンドウ



画面上段(概要パネル)には、１フレームが１行にて表示されます。表示される項目を表２に示す。(表示位置は、カラムヘッダをマウスでドラッグすることで変更可能)

*1 この記事は、SMSのネットワークモニタ V4.00.354 に基づいて説明しています。
*2 ネットワーク上の全機器に対するデータの送信。
*3 ネットワーク上の特定のグループに対するデータの送信。

表1. キャプチャウィンドウの合計パネルでの表示項目

カテゴリ	項目
ネットワーク統計	フレーム数
	ブロードキャスト数
	バイト数
	ドロップフレーム数
	ネットワーク状態
キャプチャ統計	フレーム数
	バッファ内のフレーム数
	バイト数
	バッファ内のバイト数
	バッファ使用率
	ドロップフレーム数
統計/秒	ネットワーク使用率(%)
	フレーム/秒
	バイト/秒
	ブロードキャスト/秒
	マルチキャスト/秒
ネットワークカード(MAC)統計	フレーム数
	ブロードキャスト数
	マルチキャスト数
	バイト数
ネットワークカード(MAC)エラー統計	CRC エラー数
	ドロップフレーム数(バッファなし)
	ドロップフレーム数(ハードウェア)

Tips.*4

表2. 概要パネルに表示されるカラム

名称	意味
フレーム	キャプチャしたフレーム番号
時間	システム時刻、キャプチャ開始からの経過時間、直前にキャプチャしたフレームからの経過時間の何れか。 ([表示] - [オプション]メニューにて設定)
Src MAC Addr	送信元 MAC アドレス([オプション] - [アドレス名の表示]、[製造元名の表示]設定によって表示形式が変化)
Dst MAC Addr	送信先 MAC アドレス(同上)
プロトコル	プロトコル名。
説明	フレーム内の最後のプロトコル(最上層)あるいは、表示フィルタの設定に基づいて最も重要だと判断されたプロトコルの概要情報。
Src Other Addr	送信元アドレス(MAC アドレスとは別の種類のもの、IP アドレスや、IPX/XNS のネットワークアドレスなど)
Dst Other Addr	送信先アドレス(同上)
Type Other Addr	「Src Other Addr、Dst Other Addr」として 表示しているアドレス種別。

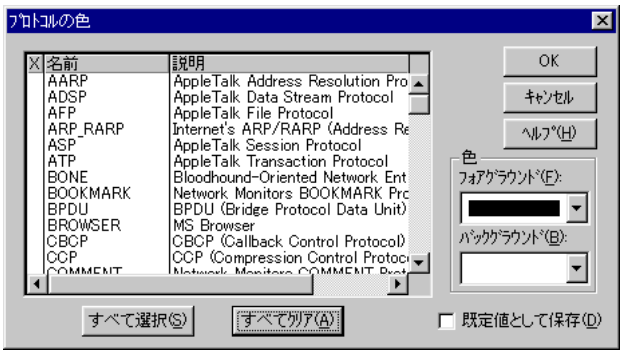
*4 パネル内にてダブルクリックを行うとパネルが拡大されます、目当てのフレームを探すときに便利です。

画面中段(詳細パネル)には、概要パネルにて選択されているフレームが、ネットワークモニタによって人が見て分かり易い形に解読されて表示されます。
表示されているプロトコルによって解読される形は異なります。任意の行を選択して右クリックメニューより[フィルタへの追加...]メニューを呼び出して表示フィルタの設定を行うことも可能です。
画面下段(16進パネル)には、概要パネルにて選択されているフレームのデータが 16進表記にて表示されます。反転表示されている部分は、詳細パネルにて選択されている行に対応したデータを示しています。
データの先頭部分から順にFRAME→ETHERNET→IP→TCP→HTTP といったように段々上層のプロトコルへとなっていきます。データなどはフレームの最後に書かれているので調べる対象とするプロトコルによっては、16進パネルの最後尾部分に注視して探す方が効率が良いことがあります。(表示フレームは概要フレームをクリックしカーソルキーの上下にて順に変更できます)

◇ キャプチャした結果を見やすくする(表示のカスタマイズ)
デフォルトの設定では、キャプチャしたフレームの表示時に黒色のみで表示されますが、プロトコル別に色分けをすることが可能になっています、この設定を行うことによってキャプチャ結果を確認する際の視認性が高まるので設定しておくことをお勧めします。以下に設定手順を示します。

1. 「フレームビューアウィンドウ」の[表示]メニューから[色...]を選択します。
2. 「プロトコルの色」ダイアログが表示されます。(図3)

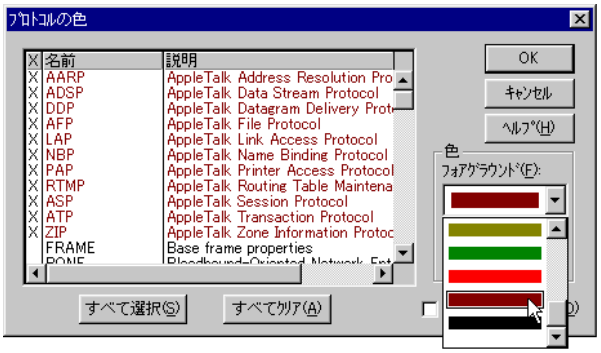
図3-1. プロトコルの色ダイアログ



3. 最初は、プロトコルの名前順でソートして表示されていますがプロトコルの意味別で色分けをするために 「説明」と書かれたカラムヘッダをダブルクリックして説明文でソートされるようにします。説明文の最初にはAppleTalkや、Internet's、Netware などといったようにそのプロトコル種別を表すものが書かれているため関係のあるものは ほぼひとかたまりになって表示されているはずです。
4. 色を設定する際は、同じ色にしたいプロトコルをクリック(あ

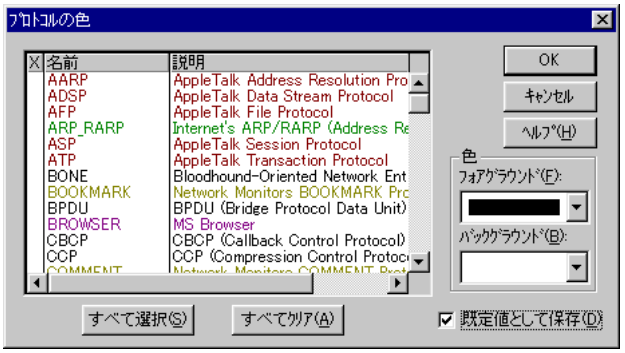
るいは、[スペースキー]を押下)して 'X'マークを付けていき、ダイアログ右側にある 色のコンボボックスから設定したい色を選択します。

図3 - 2



5. 色を設定したらダイアログ下部にある[すべてクリア]ボタンを押して 'X'マークを一旦 すべて消します。
6. (2)～(4)の操作を繰り返して各プロトコルに対して好みの色(筆者は、AppleTalk は赤、TCP/IP は緑、Netware は水色、NetBIOS 系は紫といった具合にしています)を設定していきます。
7. 設定が完了したら、ダイアログ右下の[既定値として保存]をチェックして、[OK]ボタンを押してダイアログを閉じます。

図3 - 3



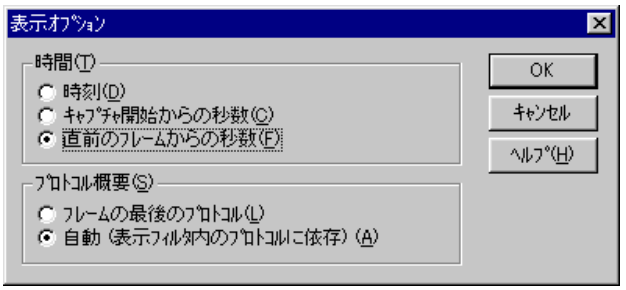
8. [表示]-[設定の保存]メニューを選択して、設定を保存します。(これを忘れると、次回起動時にまたデフォルトに戻ってしまうのでご注意)

このとき、フォントのサイズ指定や [表示]-[オプション...]メニューにて行う表示オプションも一緒に設定しておくと良いでしょう。(図４)

◇ 必要なフレームのみをキャプチャする(フィルタの設定)

漠然とネットワークの状況を見る場合には、流れているフレーム全てをキャプチャするのもよいですが、なにかトラブルが発生したときにフレームをキャプチャして調べるときはフィルタ設定をしてキャプチャされるフレームを絞り込んだほうが調べ

図４. 表示オプションダイアログ



やすくなり、またキャプチャバッファの使用量も抑制できるため長時間のキャプチャが可能になります。なおフィルタには、キャプチャ時のフィルタと、表示時のフィルタがありますが ここではキャプチャ時のフィルタについて説明します。

キャプチャフィルタとして指定可能な要素として以下の３種類のものがあります。

・アドレス
・プロトコル
・データパターン

「アドレス」ではフレームの送信元や送信先によってフィルタ指定を行います、手軽に設定できるうえにその効果も大きいので一番 利用頻度が高い方法です。

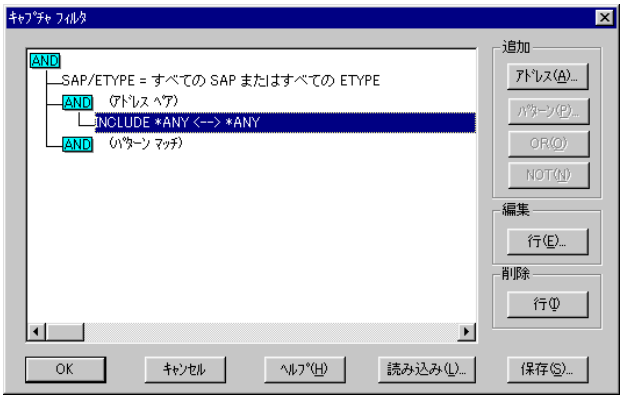
「プロトコル」では、プロトコルの種類(SAP/ETYPE)によってフィルタ指定が可能ですが、適切に設定しないと期待した動作にならないため通常はすべてのプロトコルをキャプチャする設定のままで使用することをお勧めします。

「データパターン」では、フレームのパターンに一致しているかどうかでフィルタを指定します。この設定も少々難解なため慣れるまでは「アドレス」によるフィルタが良いでしょう。

以下にアドレスによるフィルタ設定の手順を示します。

1. 「キャプチャウィンドウ」の[キャプチャ]-[フィルタ...]メニューを選択します。
2. 「キャプチャフィルタ」ダイアログが表示されます(図５)。

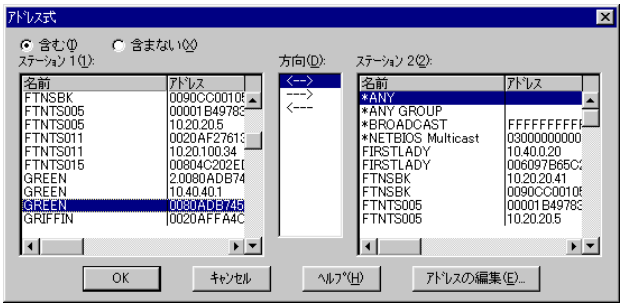
図５. キャプチャフィルタダイアログ



3. [アドレス...]ボタンをクリックします。
4. 「アドレス式」ダイアログが表示されるので、キャプチャに"

含めたい"あるいは"除外したい"２つのアドレスペアとその通信方向を指定します。(図６)
例えば、特定のノードが通信しているフレームだけをキャプチャしたい場合は、そのノードのアドレスと *ANYとの双方向を含むという設定で作成します。アドレスの一覧にそのノードが見つからない場合は、しばらくフィルタ設定なしでキャプチャを行ってから「すべての名前を検索」コマンドを実行するか、[アドレスの編集...]ボタンを押してアドレスデータベースのそのノードのアドレスを登録しておきます。

図６. アドレス式ダイアログ



フィルタ設定で注意したいのは、「含まない(EXCLUDE)」という設定は、「含む(INCLUDE)」よりも優先されるということです、フィルタ設定をした後 思っていたようにフレームがキャプチャできないときは設定を確認してみてください。
また、アドレスの形式はプロトコルによって違うため、一台の端末に対して MAC アドレスに加えてIP アドレス、IPX/XNS など複数のアドレスが割り当てられていることがあります。通常はMAC アドレスでフィルタ指定を行うようにすれば良いでしょう。

◇ ネットワークモニタのコマンドの説明

ネットワークモニタの各メニュー項目について簡単に説明します。なお、[オプション]メニューは 「キャプチャモード」と「表示モード」で重複している項目が多い為、キャプチャウィンドウの方にまとめて書いてあります。[ウィンドウ]メニューと[ヘルプ]メニューの説明は省略しております。

● キャプチャウィンドウ

[ファイル]メニュー

[開く...] 既存のキャプチャファイルを開きます。*5

[名前を付けて保存...] キャプチャしたデータを保存します。保存するフレーム範囲の指定が可能です。

[ネットワークモニタの終了] ネットワークモニタを終了します。

[キャプチャ]メニュー

[開始] キャプチャを開始します。

[停止] キャプチャを停止します。

[停止して表示] キャプチャを停止し、キャプチャしたデータを表示します。

[一時停止] キャプチャを一時停止します。

[再開] 一時停止したキャプチャを再開します。

[キャプチャデータの表示] キャプチャしたデータを表示します。

[すべての名前を検索] キャプチャデータから、各ネットワークアドレスに対応したコンピュータ名などを探します。

[統計のクリア] グラフ、セッション統計、ステーション統計のデータをクリアします。

[アドレス...] アドレスデータベースの編集を行います。

[バッファの設定...] キャプチャバッファの設定を行います。

[フィルタ...] キャプチャフィルタの設定を行います。フィルタ設定の読みこみや保存も可能です。

[ネットワーク...] キャプチャを行うネットワークを選択します。(ネットワークカードが複数使用していたり、リモートのモニタエージェントを利用する場合に使います)

[トリガ...] トリガとなるイベント条件や、トリガ発生時の動作の指定を行います。

[キャプチャモードのみ] キャプチャモードの切り替えを行います。

[設定の保存] 設定を保存します。

[ツール]メニュー

[ネットワークモニタユーザーの確認...] ネットワーク上に存在する、他のネットワークモニタを検索して一覧を表示します。

[ルーターの検索...] ネットワーク上に存在しているルータをフレームをキャプチャして探し出します。

[名前からアドレスを解決...] DNS 、NetBIOS、SAP プロトコルや、ネットワークモニタのアドレスデータベースを利用して、名前からそのアドレスを探して表示します。

[パフォーマンスモニタ] パフォーマンスモニタを起動します。

[オプション]メニュー

[ツールバーの表示] ツールバーを表示します。

[アドレス名の表示] MAC アドレスの表示にてアドレスデータベースに登録されている名前を使用します。

[製造元名の表示] MAC アドレスにベンダー名を表示します。

[ボタンのヒントの表示] ツールボタン上にマウスカーソルが置かれたときチップヘルプを表示します。

[データの保存の確認] ウィンドウを閉じる際に保存していないデータがあれば確認のダイアログを表示します。

[デフォルトパーサー...] キャプチャしたフレームを解析する際に使用する「パーサー」を選択するためのダイアログを表示します。キャプチャしたフレームが解析されない場合に使用されているパーサーの設定を確認するぐらいで通常は、この

*5 Network General社の「Sniffer」で保存したデータも開けるようです(対応するバージョンなどは未確認)

設定を変更する必要はありません。(キャプチャウィンドウのみのメニュー)

● フレームビューアウィンドウ

[ファイル]メニュー

[開く...]既存のキャプチャファイルを開きます。

[名前を付けて保存...]　キャプチャしたデータを保存します。保存するフレーム範囲の指定やフィルタの適応が可能です。

[閉じる]開いているキャプチャデータを閉じます。

[印刷...]キャプチャデータを印刷します、テキスト形式にファイルに保存するときもこのメニューを使用します。

[ネットワークモニタの終了]　ネットワークモニタを終了します。

[編集]メニュー

[切り取り]　選択しているフレームを切り取ります。

[コピー]選択しているフレームの詳細データをクリップボードにコピーします。

[貼り付け]　切り取ったフレームを張りつけます。

[読み取り専用]　キャプチャデータを読み取り専用するかどうかを選択にします。(通常は読み取り専用です)

[表示]メニュー

[次のフレーム]　次のフレームに移動します。

[前のフレーム]　前のフレームに移動します。

[指定したフレームへ...]　指定したフレームに移動します。

[フレームの検索...]　フレームを検索します。(検索方法は概要パネルや詳細パネルで選択している箇所に対応したプロトコルで指定します。)

[次を検索]　次を検索します。

[前を検索]　前を検索します。

[フィルタ...]表示フィルタの設定を行います。

[フィルタを無効にする]　表示フィルタの有効/無効を切り替えます。

[アドレス...]アドレスデータベースを編集します。

[すべての名前を検索]キャプチャデータから、各ネットワークアドレスに対応したコンピュータ名などを探します。

[フォント...]フォントの設定を行います。

[色...]　プロトコル毎の表示色の設定を行います。

[オプション...]　オプションの設定を行います。

[設定の保存]設定を保存します。

[ツール]メニュー

[パフォーマンスモニタ]　パフォーマンスモニタを起動します。

[転送許可]　ネットワークへのフレームの転送(送信)の許可/不許可を切り替えます。

[転送するネットワークの選択...]　フレームを転送するネットワークを選択します。

[フレームの転送]選択しているフレームの転送(送信)を行います。

[キャプチャの転送...]キャプチャしたデータをネットワークに転送(送信)します。(フレームの範囲の指定や、送信間隔の設定が可能です。)[*6]

[コメントフレームの挿入...]　しおりの役割をするフレームを挿入します。

[最上位ユーザーの検索...]キャプチャしたデータから、最も通信量の多いユーザ(ノード)を上位から順に表示します。

[ルーターの検索...]　キャプチャしたデータから、ネットワーク上に存在しているルータを探し出します。

[名前からアドレスを解決...]　DNS 、NetBIOS、SAP プロトコルや、ネットワークモニタのアドレスデータベースを利用して、名前からそのアドレスを探して表示します。

[プロトコルの分類...]キャプチャしたデータから、プロトコル別の統計情報を表示します。

最後に

ネットワークモニタはネットワーク上を流れるデータを見ることができるためトラブル対策には強力な武器となりますが、その反面 他の人の通信を覗き見るといった行為も可能になってしまいます、特にメールを読むために使用するPOP プロトコルではパスワードも暗号化されずにネットワークを流れているためその気になればすぐに調べることが可能です。プライバシーの侵害にならないよう、節度を守って使用するようにしてください。

参考文献

Microsoft ネットワークモニタのヘルプファイル
OPEN DESIGN No.3 「イーサネットと TCP/IP」CQ 出版社

[*6] 転送系のコマンドは、ネットワークに重大な影響を及ぼす可能性があるので取り扱いに注意してください。