暫定公開版

IPtalk関連マニュアル＃103

通信モニターソフト
TCP Monitor Plusの説明

2014年12月31日版

これは、IPtalk関連マニュアルの暫定公開版です。

動作確認の手間をNCKの会員にお願いして、IPtalk9tのマニュアルを作成しようと思ったのですが、栗田が書くこと自体に時間を取ることができず「IPtalk9tの全機能」どころか「よく使う機能」の説明でさえ「いつになるか分からない」という状況が続いています。そこで、「機能限定でも役に立つ」という暖かい意見も頂戴していることもあり、書いたマニュアルは、できるだけ暫定でも公開したいと考えます。何時の事になるか分かりませんが、最終的には、1つのマニュアルにまとめたいと考えています。

【使用の制限】

・このマニュアルは、個人的な使用に限定します。

・ホームページなどに掲載して不特定多数に配布することは禁止します。

【連絡先】 office@nck.or.jp

2014年12月31日　栗田

【履歴】

2012年12月30日 NCK会員向け初版

2014年12月31日 暫定一般公開

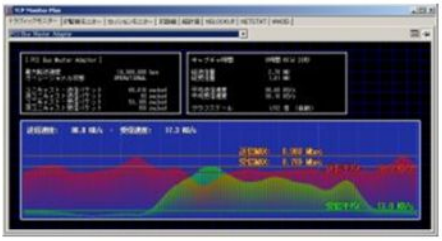
【TCP Monitor Plusについて】

TCP Monitor PlusのHPは以下です。

http://hp.vector.co.jp/authors/VA032928/

e-MAIL : oga@dream.plala.or.jp

TCP Monitor Plus



・IPtalkの表示が出ない、8人モニターが見えないなどの不具合が起こる時は、①通信に問題がある時と②ファイアウォールなどパソコンの設定に問題がある場合があります。
・通信モニターを使うと、①と②の問題の切り分けが簡単にできます。

・TCP Monitor Plusは、パソコンの通信をモニターするフリーソフトです。
・パソコン間の通信をモニターしたり、通信量をリアルタイムで表示することができます。

このマニュアルを作った理由は、IPtalkの表示不良の問題切り分けを簡単にするためです。

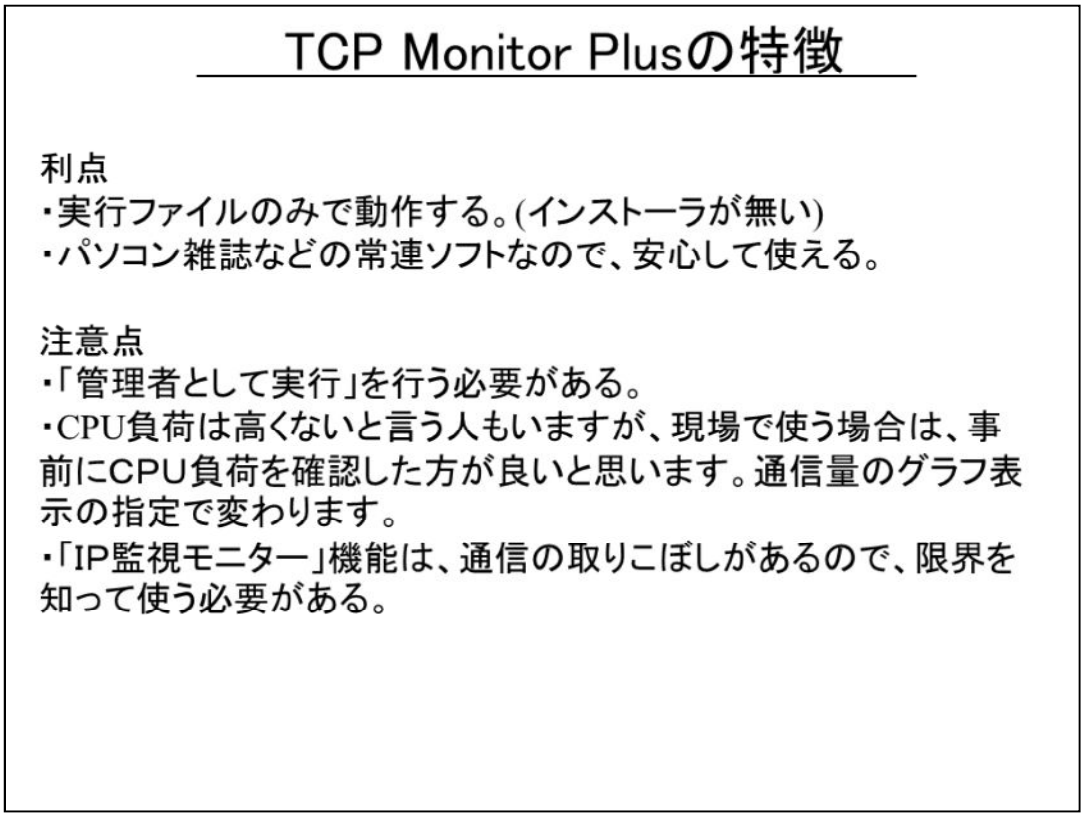
「表示が出ない」という不具合があった時、①送信側に問題がある、②通信経路に問題がある、③受信側に問題がある、の3つのケースがあります。

最初に調べたいのは、この3つの内、どれに当たるかです。

IPtalkにも、いつくつかの通信をモニターする機能があるのですが、充分とは言えません。

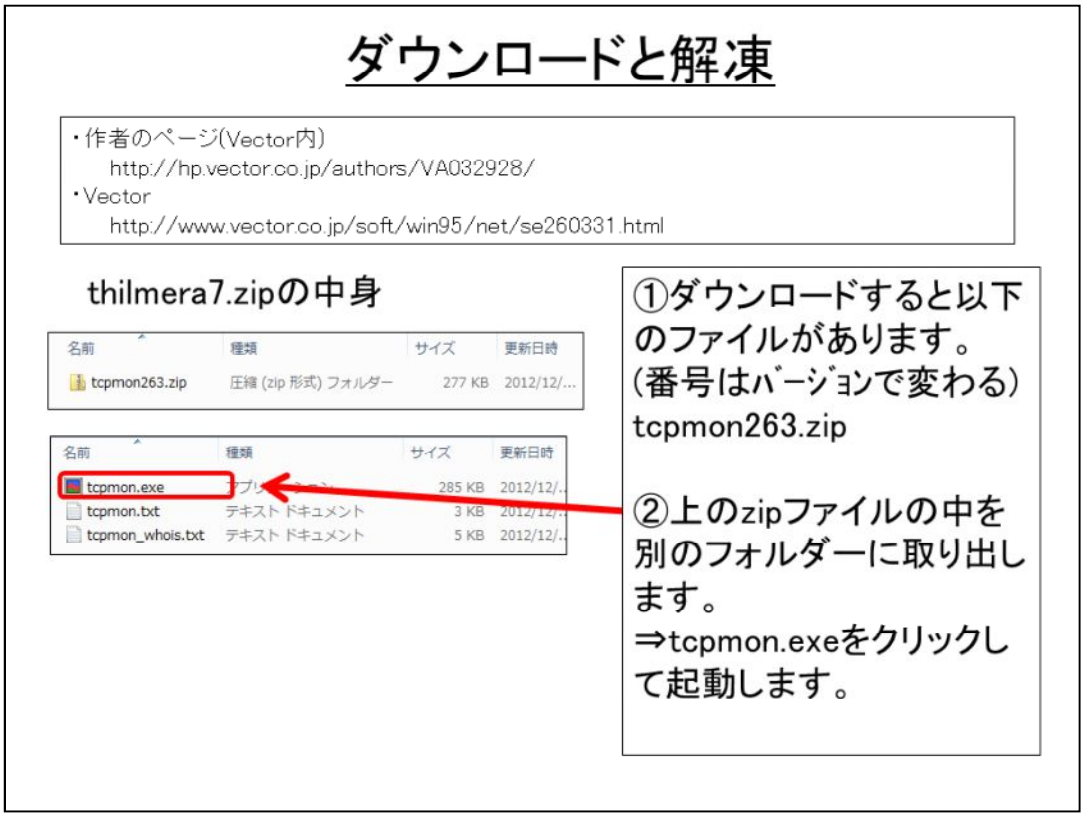
通信モニターを送信側と受信側のパソコンで立ち上げれば、通信を直接モニターできるので、3つのケースのどれに当たるか、問題を切り分けることができます。

2012年12月30日　栗田



IPtalkと同じように、インストーラが無いので、気楽に実行できるのが良いと思います。

また、TCP Monitor Plusの負荷が気になる場合は、タクスマネージャーでCPU負荷を計測しながら、thilmera7を起動したり、停止したりして、変化をみてください。



ダウンロードすると「tcpmon263.zip」が手に入ります。

「263」などの番号は、バージョン番号なので、最新のバージョンでは番号が変わっていると思います。

エキスプローラで、zipファイルは普通に中を見ることはできますが、実行することはできません。

そこで、zipファイルの中を全部選択して、適当なフォルダーの中にコピーします。

コピー先のフォルダーの中の「tcpmon.exe」をダブルクリックして起動します。

初めて起動した時

・「トラフィックモニター」ページで、モニターする通信ディバイスが「Bluetooth」になっている。

初めて起動すると、上のような画面が出ます。
いろいろなタブがあるのは、IPtalkに似ています。

初めて起動した時は、「トラフィックモニター」ページが出ていると思いますが、何も表示さないと思います。
モニターしているのが、「Bluetooth」になっているからです。

「▼」のプルダウンメニューから、モニターする通信ディバイスを選択します。

上の例では「Interl(R) 82577LM Gigabit Network Connection」をマウスでクリックします。

すると、プルダウンメニューの枠に入り、通信量がグラフで表示されます。

グラフが出ない時は、他の通信ディバイスを選んでください。

グラフが出ないということは、その通信ディバイスでは通信していないということです。

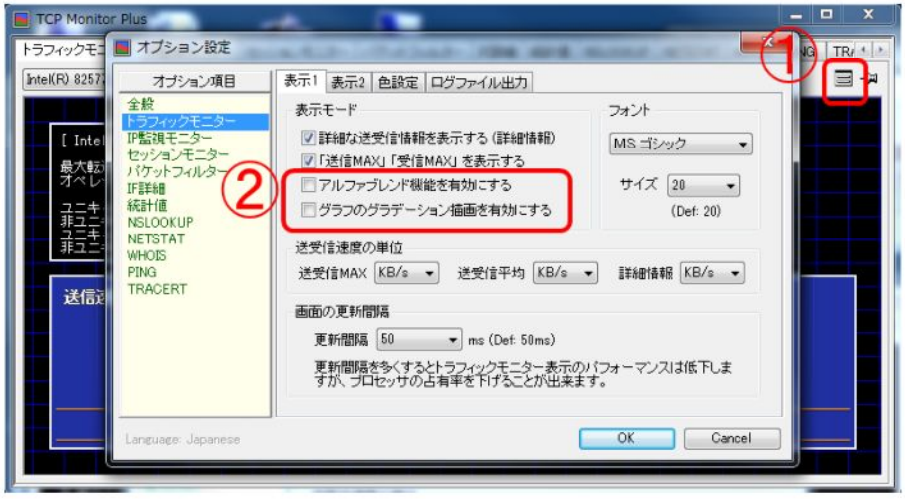
このマニュアルでは、通信量をモニターする方法を説明するのが目的ではありませんが・・

【ヒント】

イーモバイルのGP02は以下です

HUAWEI Mobile Connect – Network Adapter

トラフィックモニターの表示設定を変更します。



・右上のアイコンをクリックすると、オプション設定のウィンドが開きます。
・「アルファブレンド」と「グラデーション」をオフにします。

このマニュアルは、通信量をモニターすることが目的ではないのですが、通信量表示のグラフは、ディフォルトではCPU負荷が大きいので、設定変更の方法を説明します。

①右上のアイコンをクリックすると「オプション設定」ウィンドが開きます。

「トラフィックモニター」ページを開いていた場合は、自動的に左の「オプション項目」が「トラフィックモニター」が選択されています。

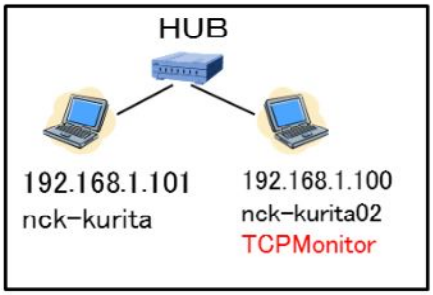
②描画のCPU負荷を下げるために、以下のチェックを外します。

・「アルファブレンド機能を有効にする」

・グラフのグラディーション描画を有効にする。」

ピンのマークは「常に前面に表示」です。

IPtalkの通信をモニターしてみます。(LAN)



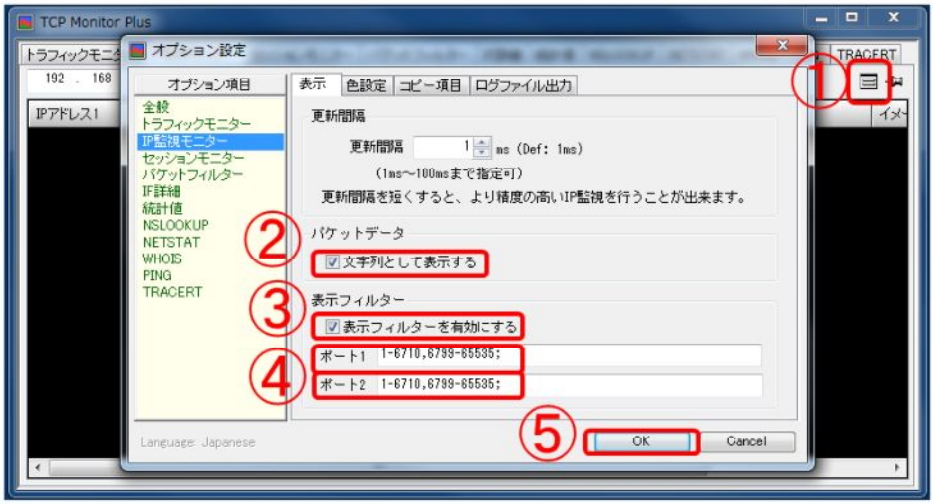
HUBで2台のパソコンを接続して、IPtalkの通信をモニターしてみます。

192.168.1.100(nck-kuri02)がTCP Monitorで通信をモニターします。

IPtalkの通信をモニターしてみます。
2台のパソコンをHUBで接続します。ルーターでも構いません。
両方のパソコンで、IPtalkを起動します。
tcpmonを起動している片方のパソコンで、、通信をモニターしてみます。

IPtalkの通信をモニターしてみます。(LAN)

IP監視モニターの設定



・「IP監視モニター」ページを開きます。
・IPtalkの通信をモニターするには、　④の「ポート1」「ポート2」に「1－6700，6800－65535」と入力します。

「IP監視モニター」ページを開きます。

①右上のアイコンをクリツクすると「オプション設定」ウィンドの「IP監視モニター」ページが開きます。

②「文字列として表示する」のチェックを入れます。

　このチェックを入れると、通信している文が表示されます。(暗号化されていない場合)

③「表示フィルターを有効にする」のチェックを入れます。

④「表示しないポート範囲」を指定します。表示する範囲ではないことに注意してください。

　「ポート1」は、自分のパソコンのポート範囲、「ポート2」は、他のパソコンのポート範囲です。

　IPtalkの通信をモニターするには、両方とも「1－6700，6800－65535」と入力します。

⑤「OK」ボタンを押します。

IPtalkの通信をモニターしてみます。(LAN)

モニター開始

・「開始」ボタンを押すとモニターを開始します。
・プロトコルの「UDP(DL)」(緑)は受信したデータ、「UDP(UL)」(赤)は送信したデータです。
・「IPアドレス1」「ホスト1」「ポート1」は自分のパソコンです。
・「IPあどれす2」「ホスト2」「ポート2」は、他のパソコンです。

①「ホスト名を取得」のチェックを入れます。

「ホスト1」「ホスト2」をパソコンの名前で表示できる場合は、IPアドレスではなくパソコン名で表示します。

②「開始」ボタンを押すと、通信モニターを開始します。

IPtalkで「今日は、」と入力しています。

③に8人モニターに表示している入力文が表示されています。(暗号化していない場合)

・「ポート1」「ポート2」で何の通信か分かります。(上の例では、6721なので8人モニターの通信です)

6711は、表示部、6721は、8人モニターです。

詳細は以下のURLを参照してください。

http://www.geocities.jp/shigeaki_kurita/manual/9i9s/9i9smanual/6zatta/6-16-14port_no.htm

【ヒント】

通信のモニターは、できるだけ短時間にするのがコツです。

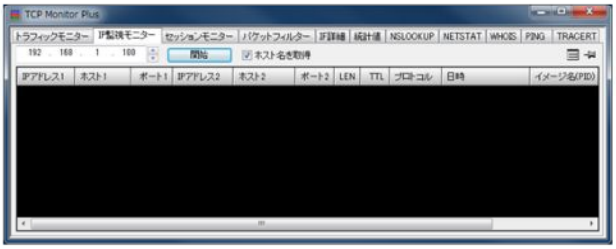
最初は、「開始」ボタンを押して、IPtalkを操作して、「停止」ボタンを押し、ログを解析する、という手順を繰り返すのが良いと思います。

不具合が出た瞬間をモニターできれば、ベストです。

IPtalkの通信をモニターしてみます。(LAN)

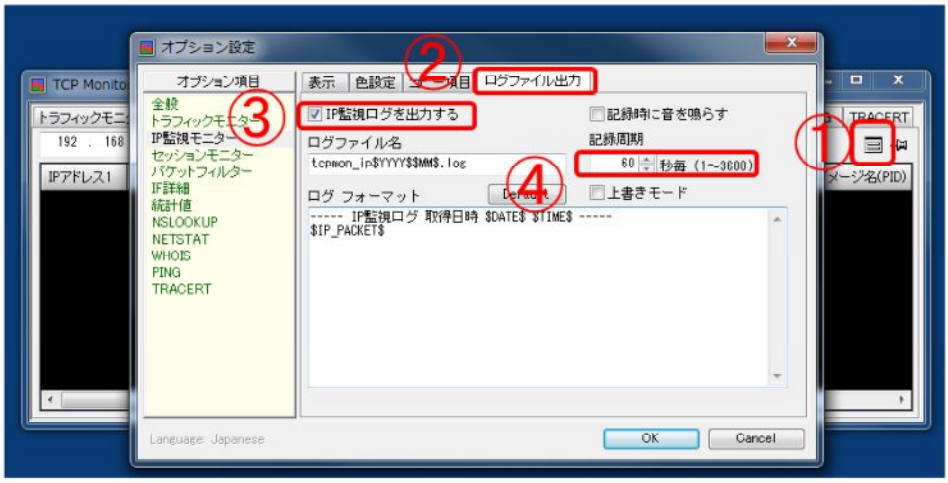
通信ログを消す

・通信枠で右クリックするとメニューがでます。
・「すべての項目を削除」をクリックするとログが消えます。



IPtalkの通信をモニターしてみます。(LAN)

通信ログを保存する



・「オプション設定」の②「ログファイル出力」の③「IP監視ログを出力する」チェックを入れます。
・記録周期④でファイルが分割されて記録されます。

ログファイル名は、「$DD$$HH$$MM$」などの指定もできます。

【注意】

スカイプの音声通信などのように多量の通信をモニターすると自動保存の時に異常終了します。

自動保存は、モニター中でないと動作しないので、そのような時は、手間ですが、スカイプの通信を止めるなどして、自動保存します。

TCP Monitorの利用方法と注意点

【利用方法】
・IPtalkで入力班を作った時に、表示が出ないとか（入力文は「データ」の欄で見ることができます）、入力班に入れないなどの場合に、通信がちゃんと届いているかを簡単に確認することができます。
⇒届いていない時は、ファイアウォールやLANケーブルの断線を疑います。

【注意点】
・TCP Monitorは、パケットの取りこぼしがあります。例えば、「メンバーを探す」ボタンを押した場合、A⇒B、B⇒A、A⇒Bと3回通信しています。
ところが、TCP Monitorでは、「 B⇒A 」や「 A⇒B、A⇒B 」などしかモニターできない事が多いようです。

TCP Monitorは、パケットの取りこぼしがあります。

この点は、注意する必要があります。

具体的には、①発信側と受信側の両方でモニターする、②何度も計測する。③、「取りこぼし」があるかもしれないことを考慮する。などです。

しかし、非常に手軽に通信を見ることができることを考えれば、TCP Monitorは、「ちょっと通信を見てみる」という時には役立つだろうと思います。

また、通信データを日本語を表示してくれるのは、通信パケットの解析がとても簡単になります。

限界はあるのですが、それを知って使えば、TCP Monitorの「IP監視モニター」機能は、とても役立つと思います。

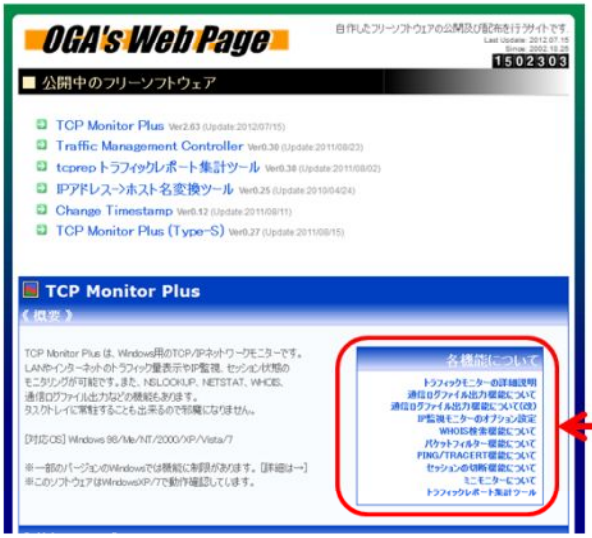
（元々は、通信のトラフィックモニターとして作られたソフトのようですから「IP監視モニター」機能は素晴らしいと思います。）

・本格的に通信の解析をしたい場合は、マイクロソフトが無償で提供している「ネットワークモニター」が良いと思います。

http://support.microsoft.com/kb/933741

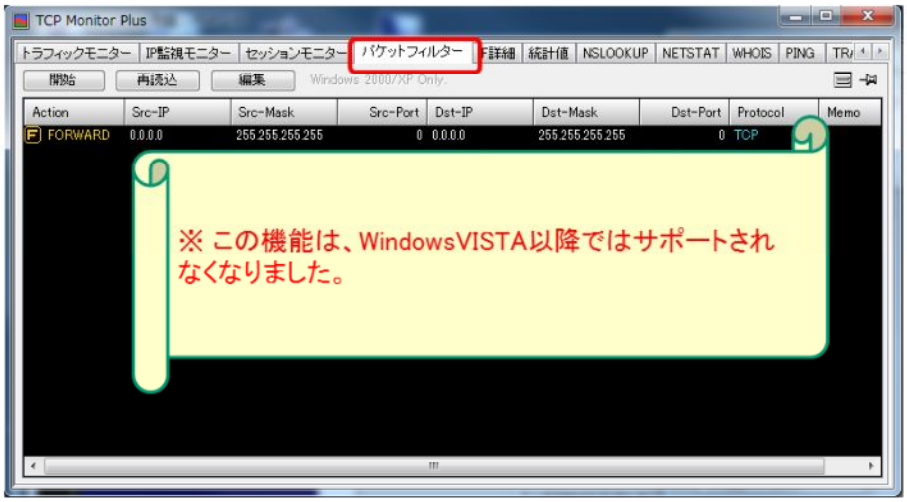
マニュアルの在り処

TCPMonのマニュアルは、概要が以下のURLにあります。
http://hp.vector.co.jp/authors/VA032928/



ソフトの使い方の説明なので、「パソコンの通信の知識」がある程度ないと読むのは難しいかもしれません。

「パケットフィルター」ページ



このページの「フィルタールール」は使いません。

余談

・今更、言うまでもないと思いますが、通信モニターを使えば、同じHUBに接続している他のパソコンの入力を（大抵の場合）モニターできます。
・つまり、暗号化されていなければ、メールの内容や、入力したパスワードなどを見ることができてしまいます。
・そのような使い方はしないと思いますが、パソコンの通信には、そのような危険があることは認識しておくのが良いと思います。

・IPtalkが暗号化の機能を持っているのは、そのためです。

通信をモニターすると、パソコンがどうやって動いているか良く分かります。
パソコンを2台立ち上げて、いろいろと試してるみると良いと思います。

トラブルシュート

http://hp.vector.co.jp/authors/VA032928/filter.html

IP監視モニターで送信パケットが取得出来ない場合
TCP Monitor Plus のIP監視モニターで、送信パケットが取得出来ない場合、インターネット接続共有サービス(ICS)を有効にすることで取得出来るようになります。

■ Windows7の場合
Windows7でTCP送信パケットが捕捉できない場合がありますが、Windowsファイアウォールを無効にする事で対応できます。
ただ、ファイアウォールを無効化することは推奨されませんのでサードパーティ製品を導入するなどの対策をして下さい。

・「メンバーを探す」などの、LANですぐに戻って来る通信は、取りこぼしがあります。(片側しか表示されない)

・手で入力する8人モニターなどは、ほとんど表示されますが、モニターできなかった場合でも、通信が来なかったという確証はありません。

・本格的に通信の解析をしたい場合は、マイクロソフトが無償で提供している「ネットワークモニター」が良いと思います。

http://support.microsoft.com/kb/933741

おわり