Vol.2012-IOT-16 No.52
2012/3/16

過去の状況の変化をさかのぼって表示できる LAN 内通信可視化システム

山之上卓[†]・小田謙太郎[†]・下園幸一[†]

LAN 内通信の状況の変化を２時限平面上で可視化するシステムについて述べる。スクロールバーを操作することにより、現在-過去の間でどのように通信状況が変化したかを把握することができる。

A LAN Traffic Visualization System which can Show Changes of traffic between Past and Now

Takashi Yamanoue[†] Kentaro Oda[†] and
Koichi Shimozono[†]

This paper discusses a LAN traffic visualization system which can show changes of traffic between past and now on a 2D plane. The user of this system can grasp changes by operating a scroll bar.

1. はじめに

多くの組織ではセキュリティの強化のため，ネットワークの監視を行っている [7]．それを実施するためのツールとして，Wireshark などの LAN アナライザーが広く利用されている．Wireshark はそれが動作するホストのネットワークインターフェースに到達するフレームを受信し，記憶し，プロトコルを解析し，利用者に分かりやすい形式で表示する機能を持っている．フレームやパケットの情報をまとめて統計処理などを行い，整理し，利用者に示す機能も持っている．しかしながら Wireshark の基本的な表示形式は一次元的なフレームの列挙であり，LAN の状況を直感的に把握するためのツールではない．

LAN の状況を直感的に把握するため，様々なネットワーク通信の視覚化システムが存在する．そのようなシステムの一つとして，我々は IP パケットのアドレスの一部を X 軸の値に割り当て，TCP/UDP のポートの一部を Y 軸の値に割り当てることによって２次元平面を構成し，1 つのパケットをこの２次元平面の点で表し，同じアドレス-ポートを持つパケットの量を点の色で表す視覚化システムの研究を行っている [6]．このシステムで LAN 内通信を視覚化した場合，port scan などの vertical scan が行われると，その名の通り垂直線が表示され，horizontal scan が行われると，水平線が表示される．点をクリックすると，その点が表す IP アドレスとポートを持ったパケットが到達時間準に並んだ表が表示される．この機能により，特定の通信だけを選んで，その経過を表示することが簡単にできる．たまたま X 軸の値と Y 軸の値が重なった複数の通信があった場合，それぞれの通信を表す複数の表がタブ形式で表示される．

今回，この視覚化システムを拡張し，スクロールバーを操作することにより，LAN の状況の観察を行っている時間内の，任意の時間の様々な時間間隔の通信を２次元表示できるように拡張した．スクロールバーを動かすことにより，LAN 内通信の状況の変化を直感的に把握できるようになった．これにより，一定間隔ごとに外部と通信を行うソフトウェアの存在の把握が容易になったり，ホストが外部のホストと通信する際の，DNS アクセスとその後の TCP 通信のような，通信間の関連の把握が容易になったりした．

この視覚化システムは，Wiki と携帯型遠隔操作機器を使ったネットワークセキュリティ監視システムに，その携帯型遠隔操作機器の視覚化部分として，組み込まれている [9]．ネットワーク管理者が設定したパケットが受信された場合，視覚化システムの２次元平面上で，そのパケットを表す点を通常とは異なる色で表すことにより，利用者に示す機能も持っている．

[†] 鹿児島大学
Kagoshima University

2. システム概要

この視覚化システムを組み込んでいる監視システムは，ノートパソコンにネットワークインターフェースを追加した携帯型遠隔操作デバイスと，このデバイスを遠隔操作し，その操作結果を確認するための Wiki (PukiWiki) サイトで構成されている(図 1). 携帯型遠隔操作デバイスは，NAT（ブロードバンドルータ）または L3 スイッチと，NAT-LAN の LAN(Sub-LAN)の部分との間に接続する.

ブロードバンドルータが持っている LAN ポートに直接パソコン等が接続されている場合は，スイッチを別に用意して，このスイッチとブロードバンドルータの間にこのデバイスを接続する. ブロードバンドルータが無線 LAN アクセスポイントの機能を持っている場合は，その無線 LAN アクセスポイントの機能を停止させ，別の無線 LAN アクセスポイントを Sub-LAN に接続する. このことにより, Sub-LAN に接続されたホストの, LAN 外のすべてのホストとの通信を取得し，それを視覚化することが可能になる.

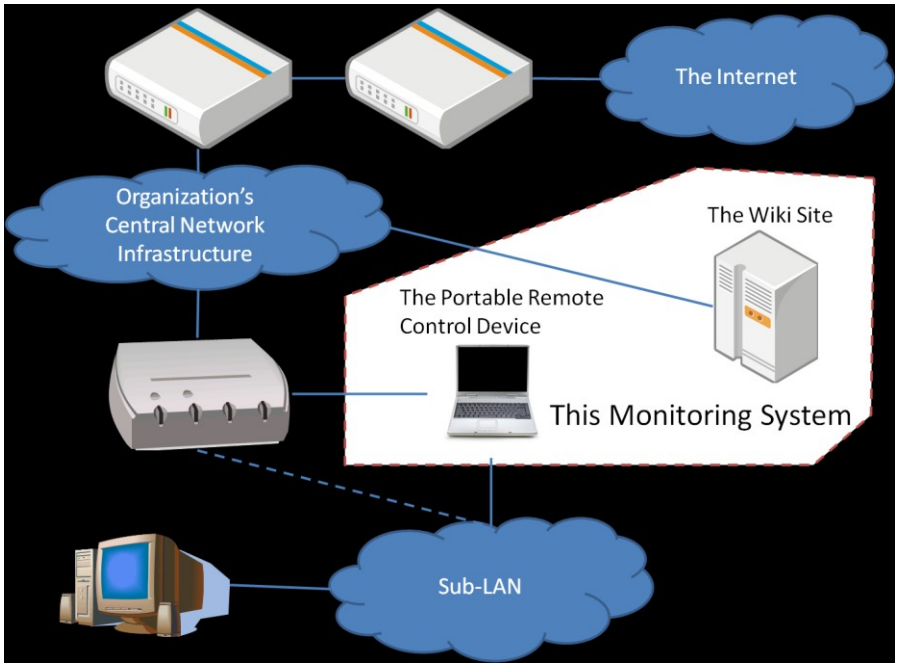


図 1　本システムの概要

図 2 に携帯型遠隔操作デバイスの構成を示す. ノートパソコン内に Linux の仮想マシンを搭載する. 仮想マシンのブリッジにより，NAT またはルータと，Sub-LAN が接続される. また，このブリッジに DAQ(Data Acquisition Library) も接続される. DAQ として, JNetPcap を利用している. DAQ で取得されたパケットは，本視覚化システム(Visualizer)に送られるのと同時に，Filter に記載されたパターンと合致した場合，このパケットの情報が Wiki ページに書きこまれる. このことは視覚化システム側にも通知され，該当するパケットを表す点が通常とは違う色で表わされる.

2.1 基本的な機能

図 3 に本視覚化システムで 1 台のパソコンの通信を視覚化し，表示している例を示す. この例は，2 月 12 日 21:11 から 21:21 の間の, YouTube を視聴しているときの通信状況を表している. X 軸は IP アドレスの下 8bit, Y 軸は TCP/UDP のポート番号の下 8bit を表している. このパソコンの IP アドレスは, 192.168.1.2 である.

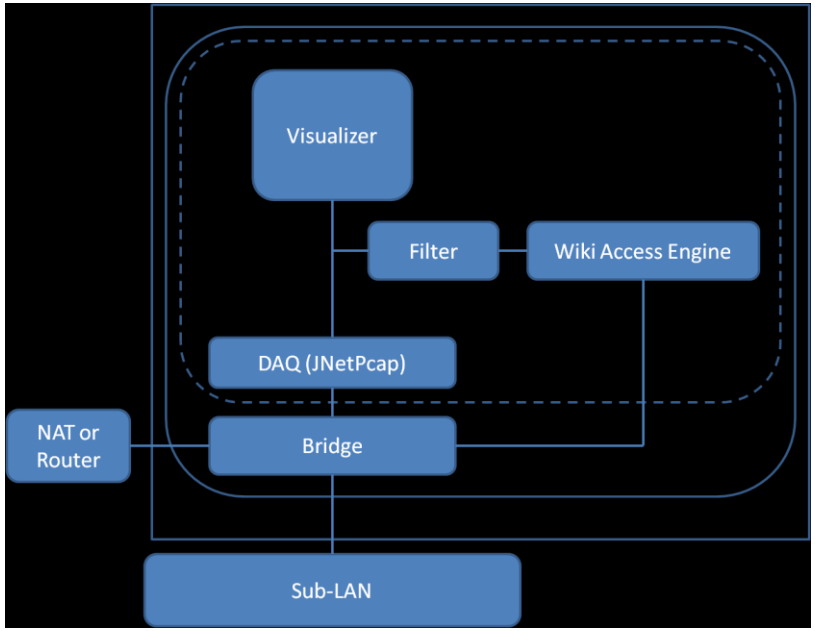


図 2　携帯型遠隔デバイス(The Portable Remote Device)の構成

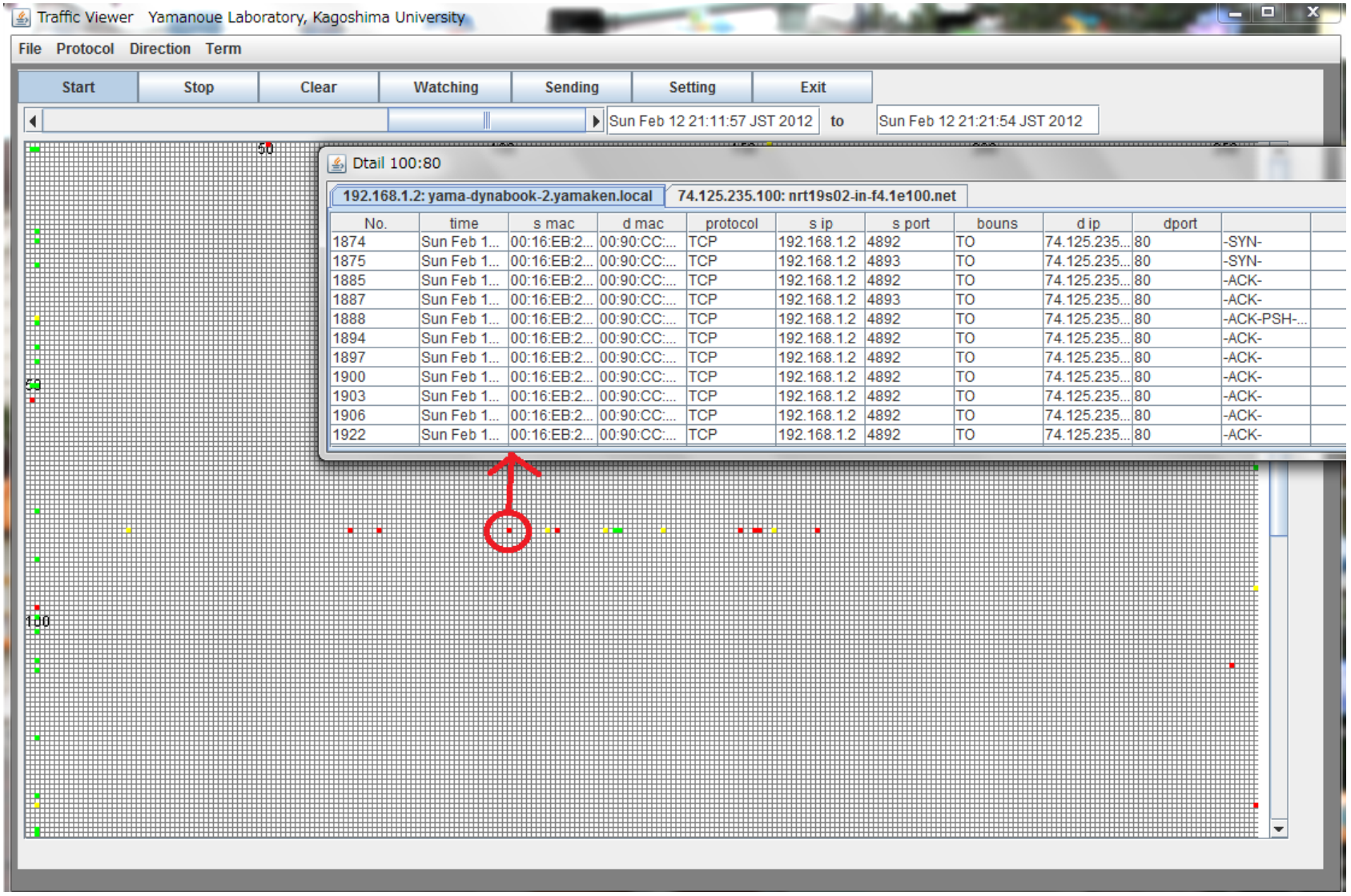


図 3. 本視覚化システムの表示例

Y 軸の 2 の位置の垂直線上に多数の点が表れている．この点をクリックすることにより，この通信の多くは DNS の 53 番ポートとの UDP パケットであることが確認できる．X 軸の 80 の位置の水平線上の多くの点は，様々な，異なる Web サーバとの間で通信があったことを表す．(100,80)の位置にある赤い点をクリックすると，表示している時刻の範囲内において，IP アドレスの下 8bit が 100，ポート番号の下 8bit が 80 のパケットの一覧表が，取得された時間，そのパケットを含むイーサーネットフレームの送信元・宛先 MAC アドレスと共に表示される．この表のタブの表示は，送信元アドレスとそのドメイン名を表している．各欄は左から，パケット番号，パケット取得時間，送信元 MAC アドレス，宛先 MAC アドレス，IP パケットのプロトコル，送信元 IP アドレス，送信元ポート番号，LAN 内と LAN 外の送信の向き(TO は LAN 内から LAN 外への通信を表す)，宛先 IP アドレス，宛先ポート番号，TCP の場合は syn, ack, fin, psh, rst などのフラグの表示，TCP/UDP のペイロードの ASCII 表示を表している．

2.2 表示期間の変更

本視覚化システムが起動されたときの表示は，図 4 のようになっている．「Start」，「Stop」，「Clear」，「Watching」，「Sending」のボタンの下の細長い領域が，表示する期間を操作するためのスクロールバーである．スクロールバーの右にある 2 つのテキストフィールドが，表示期間の開始時刻と終了時刻を表す．起動直後の終了時刻は，最後のパケットが取得された時刻となる．起動直後の表示期間は最後のパケットを取得する 1 分前から最後のパケットを取得した時間までとなっている．「Start」ボタンをクリックすると，通信取得とその表示が開始される．

図 5 はパケット取得・表示開始後，2 分余り経過したときの表示を示している．なにも操作しなければ，経過時間が増加し，表示期間は変わらないため，その後，図 6 から図 7 のようにスクロールバーのノブの長さが小さくなっていく．

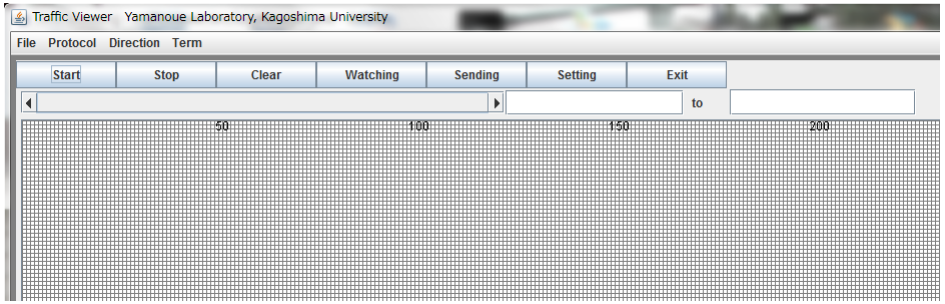


図 4. 起動直後の表示

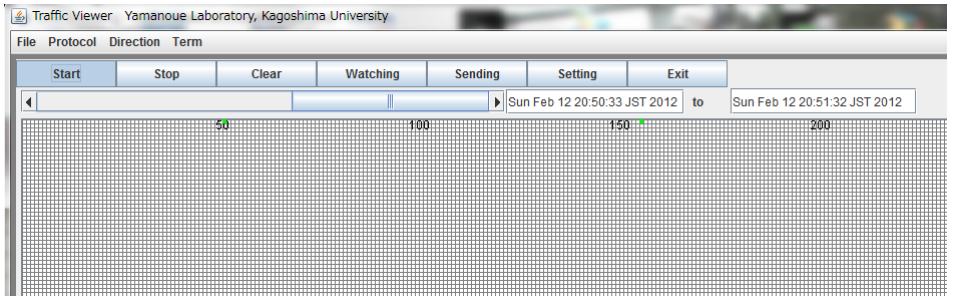


図 5. 開始から 2 分余り経過したときの表示

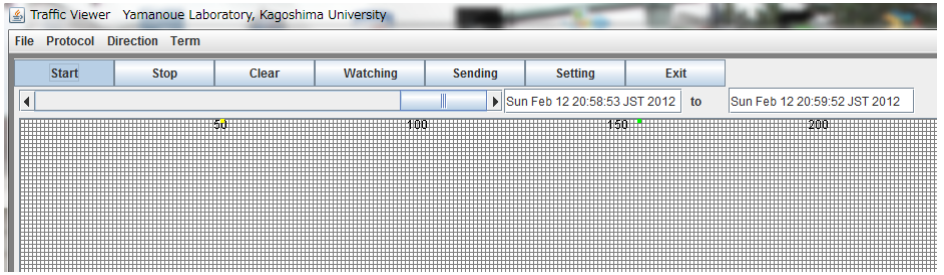


図 6. 開始から 5 分程度経過した時の表示

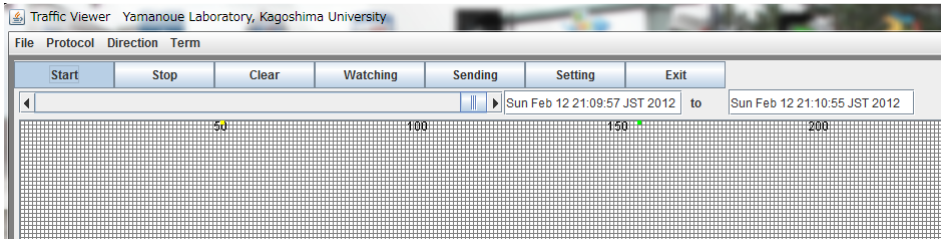


図 7. 開始から 1 0 分余り経過した時の表示

表示期間を変更するには，メニューバーの「Term」の部分をクリックし，ここで表示されるメニューの中から表示期間を選択する．最初に「Term」をクリックすると図 8 のように 1 分間が選択している．ここで 10 分間を選択し，しばらくすると図 9 の

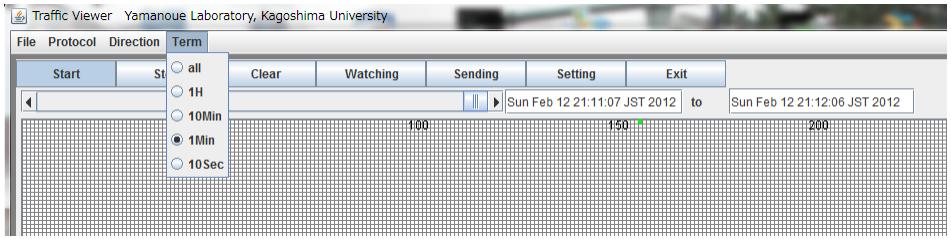


図 8. 表示期間が 1 分間の場合の表示

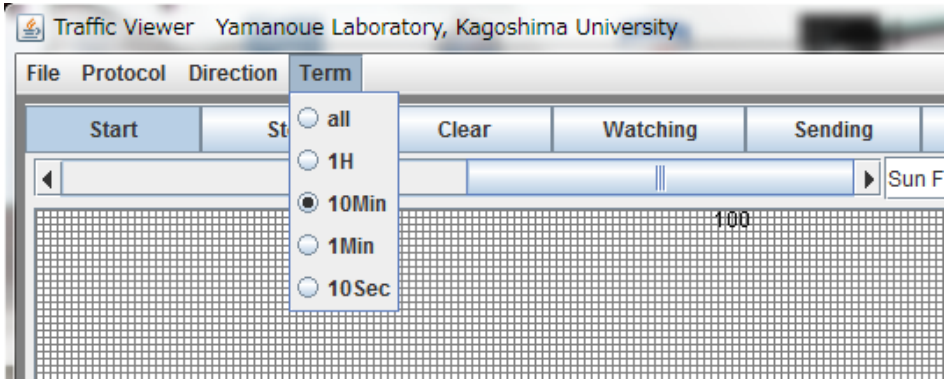


図 9. 表示期間を 10 分間に変更したときの表示

ように，スクロールバーのノブが長くなる．

スクロールバーのノブの位置をドラッグして位置を移動させることにより，図 10 や図 11 のように，通信取得開始から現時点までの任意の時間の通信状況を確認することができる．またノブをゆっくり左右に移動させることにより、通信状況の変化を把握することができる．

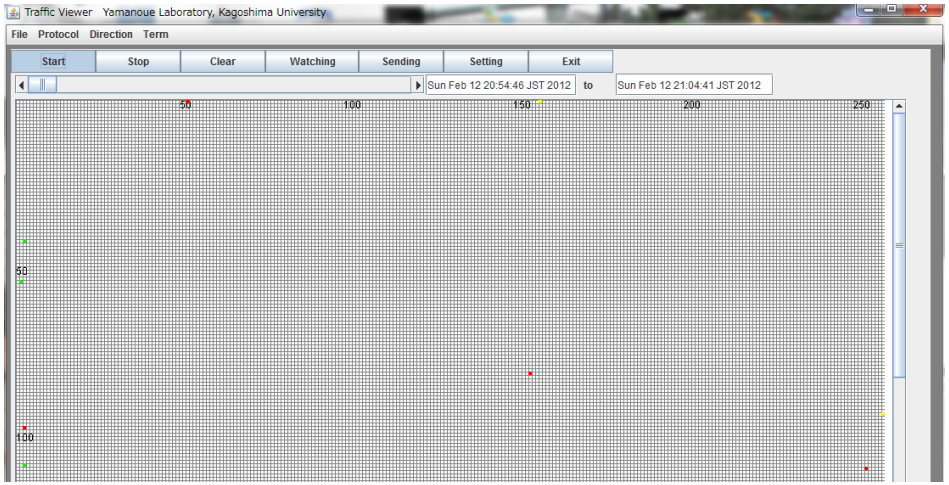


図 10. 通信取得開始から最初の１０分間の通信の表示

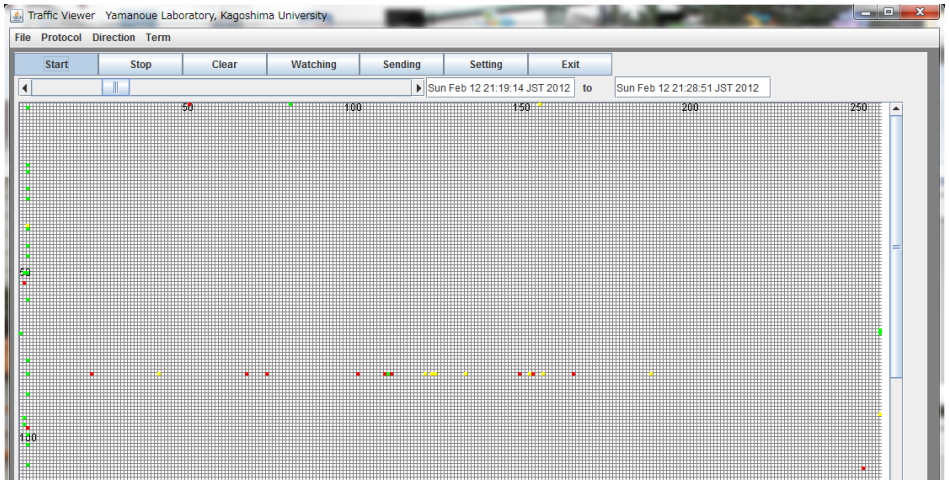


図 11. 通信開始から 25 分程度経過したときから後の１０分間の通信の表示

Vol.2012-IOT-16 No.52
2012/3/16

3. 利用例

3.1 定期的な通信の把握

ウィルスは外部のホストと定期的に通信を行う場合がある．Wireshark で定期的な通信を行うソフトの通信を把握しようとする場合，そのソフトの通信相手先が分かっていれば，その相手先 IP アドレスで表示のフィルターをかけることにより通信を特的することができる．しかし，相手先 IP アドレスがわからない場合は他の通信に埋もれて特定が難しい場合がある．本視覚化システムはこれをある程度可能にする．以下に，定期的な通信を把握する場合の例を示す．

表示期間をいろいろ変更し，スクロールバーのノブを左右に動かすと，定期的に点滅する点が表れる場合がある.図 12-図 16 は表示期間を 1 分間とし，スクロールバーのノブを左右に動かして特定の点が点滅する例を示す．表示開始時刻を 21:02:41 付近にしたとき，(2,187)付近に赤い点が表示される(図 12)．スクロールバーを少し右に移動するとこの点が消え(図 13)，もう少し右に移動させ表示開始時刻が 21:06:06 付近にしたとき，同じ位置にまた点が表示される(図 14)．以降，図 15,図 16 のように同じ場所で点が点滅する．これにより定期的な通信が行われている可能性を知ることができる．ここで，表示期間を 10 分間に伸ばし，同じ場所に表示された点をクリックすると，図のように 10 分間の通信の詳細が表示される．この詳細を見ることにより，通信の相手先の IP アドレスや通信間隔を知ることができる．

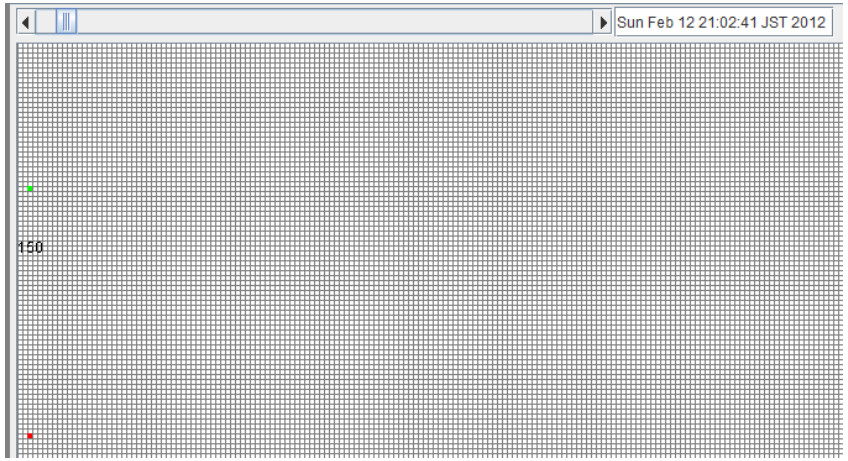


図 12．定期的な通信(1)

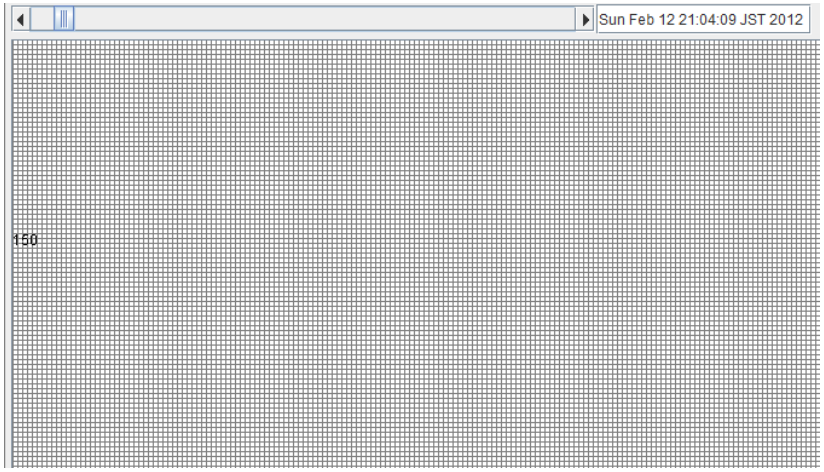


図 13．定期的な通信(2)

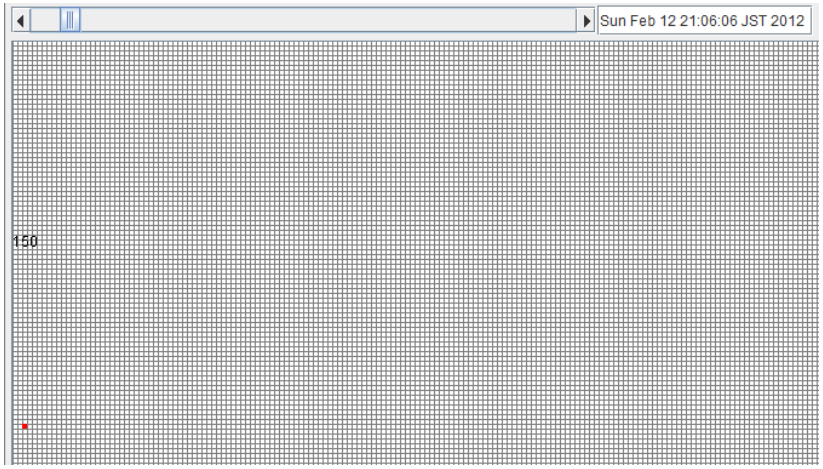


図 14．定期的な通信(3)

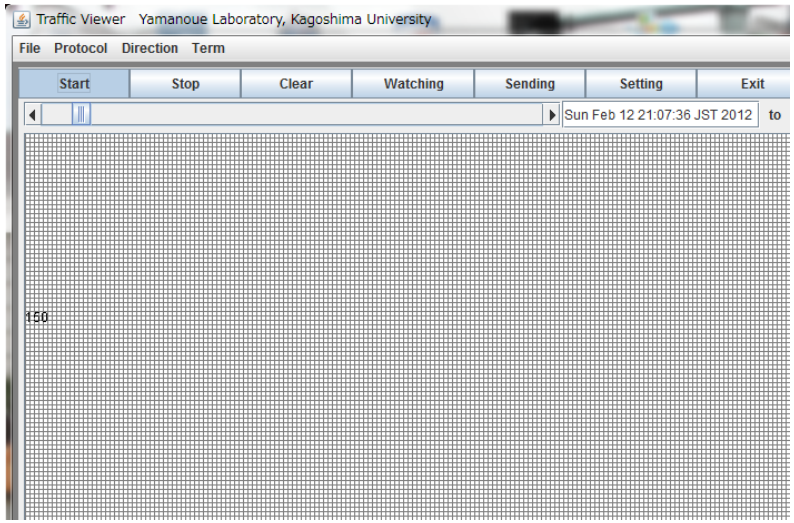


図 15. 定期的な通信(4)

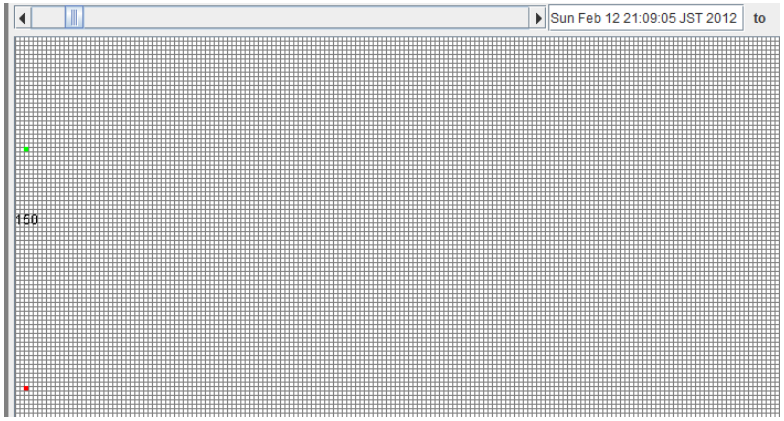
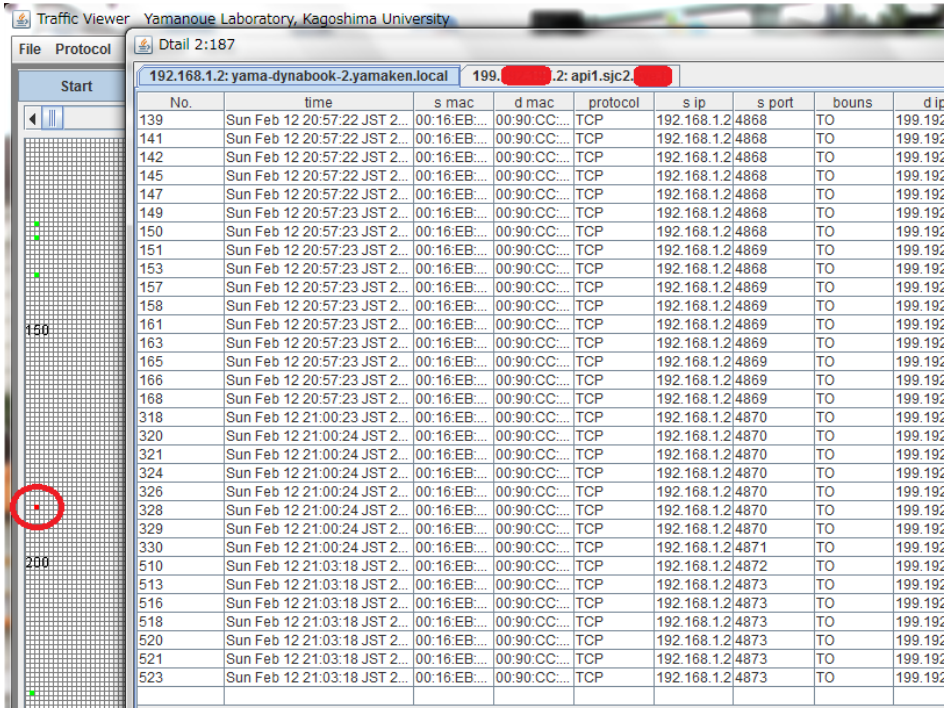


図 16. 定期的な通信(5)



No.	time	s mac	d mac	protocol	s ip	s port	bouns	d ip
139	Sun Feb 12 20:57:22 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
141	Sun Feb 12 20:57:22 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
142	Sun Feb 12 20:57:22 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
145	Sun Feb 12 20:57:22 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
147	Sun Feb 12 20:57:22 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
149	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
150	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
151	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
153	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4868	TO	199.192
157	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
158	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
161	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
163	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
165	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
166	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
168	Sun Feb 12 20:57:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4869	TO	199.192
318	Sun Feb 12 21:00:23 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4870	TO	199.192
320	Sun Feb 12 21:00:24 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4870	TO	199.192
321	Sun Feb 12 21:00:24 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4870	TO	199.192
324	Sun Feb 12 21:00:24 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4870	TO	199.192
326	Sun Feb 12 21:00:24 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4870	TO	199.192
328	Sun Feb 12 21:00:24 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4870	TO	199.192
329	Sun Feb 12 21:00:24 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4870	TO	199.192
330	Sun Feb 12 21:00:24 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4871	TO	199.192
510	Sun Feb 12 21:03:18 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4872	TO	199.192
513	Sun Feb 12 21:03:18 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4873	TO	199.192
516	Sun Feb 12 21:03:18 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4873	TO	199.192
518	Sun Feb 12 21:03:18 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4873	TO	199.192
520	Sun Feb 12 21:03:18 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4873	TO	199.192
521	Sun Feb 12 21:03:18 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4873	TO	199.192
523	Sun Feb 12 21:03:18 JST 2...	00:16:EB:...	00:90:CC:...	TCP	192.168.1.2	4873	TO	199.192

図 17. 定期的な通信をおこなうホスト間通信の 10 分間の詳細表示

3.2 通信の関係の把握

ローカルホストと外部のホスト間で通信が行われる場合，最初に DNS を使ったドメイン名から IP アドレスへの変換が行われる場合が多い．このとき，ローカルホストと DNS 間で通信が発生する．その直後，ローカルホストと外部のホスト間の通信が発生する．図 3 で示したように， 本システムで表示させることにより，DNS へのアクセスとローカルホストと外部のホスト間の通信がほぼ同時に行われていることを確認することができる．ウィルスが近隣のホストに感染を広げたり，ウィルスに感染したホスト同士で通信が行われたりする場合もこのようにして把握できる可能性がある。

3.3 特定のアドレスやペイロードを持った通信の把握

本システムはネットワーク管理者が指定した特定のアドレスやペイロードを持った通信を見つけたとき，それを表示する機能も持つ．図 18 は TCP/UDP のペイロードが

IRC 通信で使われるコマンドを持つ場合，その通信を表示している例を示す．管理者が指定したパターンと合致した通信が見つかった場合，視覚化平面上で通常とは異なる色で点が表示される．この点をクリックすると，通信の詳細が表示され，管理者が指定した特定のパターンを持つ通信については，そのパターンも一緒に表示される．

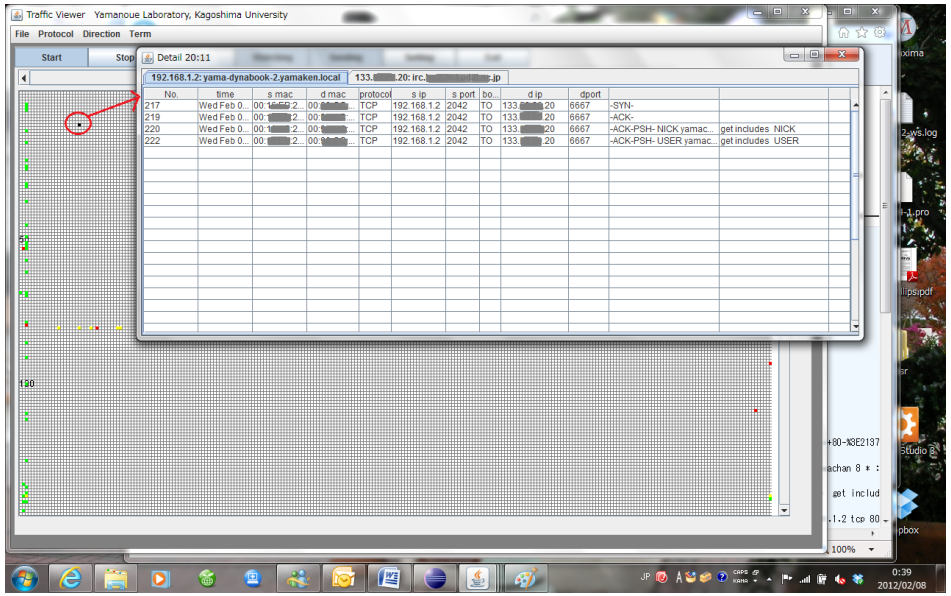


図 18　IRC 通信と思われる通信パターンを見つけそれを表示した例

4. 関連研究

文献 1)は一般的なログの視覚化について述べている．この視覚化は情報セキュリティにも役立つ．しかしながら基本的には時間軸にそった 1 次元情報の視覚化である．
文献 2)は IP アドレスとポート番号から構成される 3 次元空間上に点を配置して視覚化を行うシステムについて述べている．しかしながら，空間上の点を指定することによる詳細表示の機能はない．
文献 3)4)は IP アドレスの一部を X 軸と Y 軸に割り当てた視覚化を行うシステムについて述べている.しかしながらこれらのシステムはポート番号をどちらかの軸に割り当てるものではない．
文献 3)のものは，本システムと類似したアニメーション機能を持っている．しかしながらこれも 2 次元平面上の点をクリックすることによる詳細表示機能は持っていない．
文献 5)はホスト間通信を時間軸にそって視覚化するシステムについて述べている．このシステムも基本的には 1 次元情報の視覚化である．
文献 8)は TCP コネクション単位で通信を視覚化するシステムについて述べている．このシステムも基本的には時間軸にそった視覚化を行っている．

5. おわりに

LAN の状態の変化を把握できる視覚化システムについて述べた．このシステムにより，定期的な通信を行うウィルスなどの識別が容易になる可能性がある．今後，本システムを Wireshark と連携させることなどを検討している．

参考文献

1) 高田哲司，小池英樹:見えログ: 情報視覚化とテキストマイニングを用いたログ情報ブラウザ, 情報処理学会論文誌, Vol.41, No.12, pp.3265-3275, (December 2000).
2) Stephen Lau: The Spinning cube of Potential Doom, Communications of the ACM, Vol.47, No.6, pp.25-26(2004).
3) 小池英樹，大野一広，小泉芳：広域ネットワーク監視のための視覚化手法の提案と実装, pp319-323，日本ソフトウェア科学会第 21 回大会，(2004).
4) 堀良彰，櫻井幸一：ネットワークセキュリティのための Quadtree mapping 法を使用した情報可視化，電気関係学会九州支部連合大会研究報告，10-2A-10，pp539．(2004).
5) John r. Goodall, Wayne G. Lutters, Penny Rheingans, Anita Komlodi: Preserving the Big Picture: Visual Network Traffic Analysis with TNV, Workshop on Visualization for Computer Security, pp.47-54, Oct. 26, Minneapolis, MN. USA(2005).
6) 新川拓也，山之上 卓: IP アドレスとポートによる二次元平面を用いた通信トラフィックの可視化について，情報処理学会研究報告 2006-DSM-043,pp.31-36(2006)
7) Masato Masuya, Takashi Yamanoue, Shinichiro Kubota: An Experience of Monitoring University Network Security Using a Commercial Service and DIY Monitoring, Proceedings of the 34nd annual ACM SIGUCCS conference on User services, pp.225-230, Edmonton, Alberta, Canada. 5-8 Nov.(2006).
8) 宇都木進，渡邊晶: TCP コネクション単位でトラフィックの視覚化を行うツールの開発，情報処理学会研究会報告 2012-IOT-7 , pp. 1-5,(2009)
9) 山之上卓，白澤竜馬，小田謙太郎，下園幸一: Wiki と携帯型遠隔操作機器を使ったネットワークセキュリティ監視システム，情報処理学会研究会報告 2012-IOT-16 (2012)(予定)