疑わしい通信の検知支援を目指した クライアント計算機向け通信視覚化システムの提案

後藤 颯† 高田 哲司†

† 電気通信大学
182-8585 東京都調布市調布ケ丘 1-5-1
hayate.goto @ uec.ac.jp, zetaka @ computer.org

あらまし 攻撃手法の変化にともない，クライアント計算機が攻撃対象になる場合が増加している．クライアント計算機のセキュリティに関する対策はファイアウォールとアンチウイルスソフトウェアが主流であるが，遠隔操作ウイルス事件にも見られるようにそれらだけでは不十分になりつつある．そこで本論文では，クライアント計算機のネットワーク通信を把握可能にするエンドユーザ向けの情報視覚化システムを提案する．提案システムによりエンドユーザのログ閲覧の負担を減らし，継続的に利用することで，エンドユーザによるネットワーク利用傾向の正常状態の把握と不正行為に起因すると推測される通信の検知を支援する．

Visual Awareness Support System for Network Anomaly Detection on a Client Computer

Hayate Goto† Tetsuji Takada†

†The University of Electro-Communications.
1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, JAPAN
hayate.goto @ uec.ac.jp, zetaka @ computer.org

Abstract

In this paper, we propose a visual anomaly detection system of network connections on a client computer. End users have been exposed to security threats and they are still vulnerable to unknown emerging threats because current tools such as anti-virus software and firewall can only handle known threats. Proposed system aims to become a complementary security tool for end users by visualizing network connections from and to their computer. Our system helps users to build a normal usage model in their mind and it assists them to be aware of suspicious network traffic on their computers by finding a visual difference between images. We also show four detection examples of anomalous network traffics by the proposed system. Their examples show that our tool has a potential to detect anomalous network communications.

1 はじめに

2012 年，遠隔操作ウイルス事件が発生した．この事件では，インターネット掲示板に犯罪予告が書き込まれ，書き込みがされたとされる計算機の所有者が逮捕された．しかし捜査の結果，その計算機はマルウェアに感染しており，第三者から遠隔操作されていたことが明らかになった．当時そのマルウェアは既知のマルウェアではなく，犯人により作成されたものであったため，アンチウイルスソフトウェアでは検出することができなかった．

最近は攻撃手法も変化してきている．前述の事件に加え，クライアント計算機を攻撃対象とした水飲み場型攻撃 [1] も発生している．攻撃者によって攻

撃コードを仕掛けられたウェブサイトに攻撃対象のユーザがアクセスすることで，そのユーザの計算機はマルウェアに感染してしまう．このように，現在は攻撃目標に能動的に攻撃するのではなく，受動的な攻撃手法を使用する場合が増えている．このような攻撃はクライアント計算機の脆弱性を利用してユーザの許可無く実行されるため，被害者が気づくことは難しい．

これらのことから言えるのは，既存のサーバ計算機の対策や組織単位によるセキュリティだけでは不十分であるということである．アンチウイルスソフトウェアの検知対象は既知のマルウェアであり，未知のマルウェアを検知することは難しい．また，アンチウイルスソフトウェアベンダのマルウェア入手・シグネチャ作成の処理がマルウェアの増加とともに追いつかなくなりつつある．特に，標的型攻撃など特定の標的にしか流布されないマルウェアはそれ自体が入手困難であり，さらに対策が遅れることとなる．そのため，アンチウイルスソフトウェアではクライアント計算機のマルウェア感染を完全に防ぐことは不可能である．アンチウイルスソフトウェアベンダの幹部は “anti-virus software is dead” [2] と語っている．このような現状から，未知のセキュリティ脅威に対するクライアント計算機のユーザ向けのセキュリティが十分であるとは言いがたい．IDS には，未知の脅威に対して「異常検知」という検知手法が提案されているが，設定や運用に専門的な知識が要求されるため，エンドユーザが運用することは難しい．よって，クライアント計算機における補完的な手段として，悪意のある振る舞いに対する気づきを促すシステムが必要であると考える．

以降本論文では，第 2 章でクライアント計算機のネットワーク視覚化システムの設計方針について議論する．第 3 章で実装と視覚化手法を詳細に説明する．第 4 章で疑わしい通信の視覚化例を示す．そして第 5 章で関連研究，セキュリティ向上に関する限界，今後の課題を議論する．

2　設計方針

本章では，疑わしい振る舞いに対する気づきを促すシステムの設計に必要な方針について述べる．前提として，クライアント計算機で動作するため，利用対象者はエンドユーザとなる．エンドユーザは専門的な知識を持たないため，通信ログをそのまま提示してもそこから疑わしい通信を見出すことは困難である．知識のないエンドユーザが計算機上の疑わしい通信を発見するには，まず正常状態を知る必要がある．それを知る上で毎日の通信状況をエンドユーザが把握しておくことが重要である．そこで，我々は通信ログの情報視覚化という手段を用いる．ユーザにとって馴染みのないログを視覚化することで，ログの内容把握をより簡単に短時間で行えることを目指す．そうすることができれば，ユーザにとってログ閲覧の負担は軽くなり，毎日目を通す可能性が高まる．

さらに視覚化を行う上で，次のような方針を考えた．

エンドユーザがネットワーク通信のログをひとつひとつ調査し，それが異常かどうかを判断するのは不可能である．それはポート番号などの情報から正常か異常かを判断する知識が無いためである．そこで提案システムでは，ひとつひとつのログを個別に視覚化するのではなく，一定時間ずつログをまとめた「ログブロック」を 1 つの図として視覚化する．この手法により，ユーザは計算機の利用傾向を視覚化画像として捉えることができ，その傾向から正常状態のモデルをユーザの中に構築することが可能になる．そしていつも見ている視覚化表示と異なる画像が発生した場合には気づくことができる．また，ひとつひとつのログを視覚化するのではなくある程度の時間ごとのログをまとめて 1 つの図として視覚化するため，閲覧量の抑制が可能である．結果として，エンドユーザが提案システムを継続利用する際の負担を軽減させることができる．

前述の仕組みによりログブロックを視覚化して把握可能になったとしても，その視覚化表示が 1 つだけの状況での異常判定は容易ではない．単一の視覚化表示では，その通信がいつも通りのものであるかの判断ができないからである．複数の視覚化図を見比べることでこれまでの傾向と同一かどうかの判定を可能にする必要がある．そのため，ログブロックの視覚化画像を時間順に複数個並べて表示する．この仕組みにより，ネットワーク通信の時系列変化の把握・比較を可能にする．

さらに，ユーザが疑わしいログを発見することを支援するため，疑わしい通信である可能性が高いものを視覚的に強調して表示する．そのためには，疑わしい通信をシステム上で見出すための指標が必要となる．

3　提案システム

本章では，提案する視覚化システムについて述べる． 図 1 は，提案システムのシステム構成図である．提案システムは「通信記録部」および「視覚化処理部」から構成されており，どちらもクライアント計算機内で実行される． 通信記録部がクライアント計算機でのネットワーク利用状況をログに記録し，そのログが視覚化システムの入力データとなる．以降では，この 2 つのモジュールについて解説する．

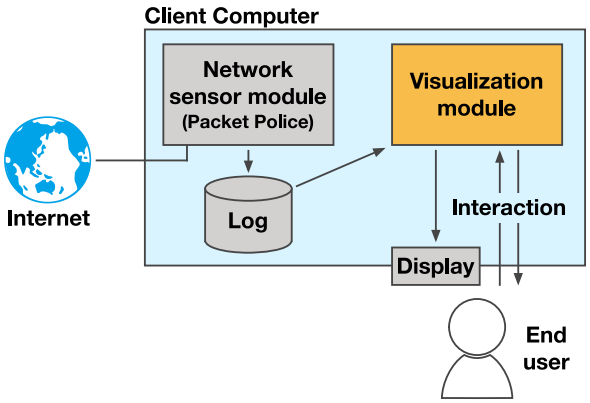

図 1: システムの構成

3.1　通信記録部

通信記録部は，計算機で発生したネットワーク通信を捉えログファイルに記録する．SoftEther 社より公開されている “パケット警察 for Windows”[3] というフリーウェアを利用している． このソフトウェアは，2012 年に発生した遠隔操作ウイルス事件を受けて開発・公開された，犯罪捜査時の証拠の一つとすることを目的としたツールである．Windows 計算機上で送受信される TCP, UDP, IP, Ethernet の通信を記録する． 記録されるログは 15 個の要素情報によって構成されている．図 2 はログフォーマットを示している．

このツールを通信記録部として選択した理由は 2 つある．1 つ目は，このソフトウェアは遠隔操作ウイルス事件を受けて開発されたもので，本研究の目的と合致しているためである．2 つ目は，ユーザが専門知識を持っていなかったとしても，簡単に導入し使いはじめることができるように配慮されているためである．

3.2　視覚化処理部

視覚化処理部は通信記録部で記録されたネットワーク通信ログを入力データとし，それを視覚化してユーザに提示するとともに，ユーザからの対話的操作を受け付ける．

図 3 は視覚化処理部によって生成されたシステムの表示画面例である．この画面は 3 つの表示部にわかれており，各表示部は画面左から「時系列表示部」「通信閲覧部」「該当通信リスト表示部」と呼ぶ．時系列表示部は現在の実装では 3 分間の通信状況を示す視覚化画像が時間順に 20 個配置されており，1 時間の通信状況の時間変化を視覚化している．この表示から通信状況の時間変化を把握することができる．通信閲覧部では時系列表示部で選択された視覚化画像が拡大表示される．最も右の該当通信リスト表示部では，通信閲覧部で選択された通信のポート番号，IP アドレス，通信回数がリスト形式で表示される．これらの 3 つの表示部の連携動作により，通信データの閲覧・調査において概要把握から詳細情報取得までシームレスに行うことが可能である．ユーザは時系列表示部によってログ内容の時間変化を把握し，興味深い視覚化画像を 1 つ選択する．これにより通信閲覧部にその視覚化画像が拡大表示される．通信閲覧部にはカーソルがあり，マウスやキーボードでそのカーソルを操作しポート番号，IP アドレスを示す軸上の任意の値に合わせると，カーソルの値に該当する通信が該当通信リスト表示部に表示される．

ログブロックを視覚化した視覚化画像のことを本論文では “Summary Viz Block”(SVB) と呼ぶ．これは時系列表示部と通信閲覧部を構成する基本単位となっている．次の節でこの視覚化表現の詳細について説明する．

Summary Viz Block の視覚化手法

“Summary Viz Block”(SVB) の視覚化手法について説明する (図 4 参照)．SVB の入力データは前述の通り一定時間ごとに通信ログをまとめたログブロックである．現在の実装では，ログファイル内の記録を 3 分毎に分割してログブロックを生成し，それぞれを SVB に変換している (図 5)．

通信ログに含まれる 15 個の要素情報のうち，SVB の視覚化には利用計算機のポート番号，通信先計算機のポート番号と IP アドレス，プロトコル名の 4

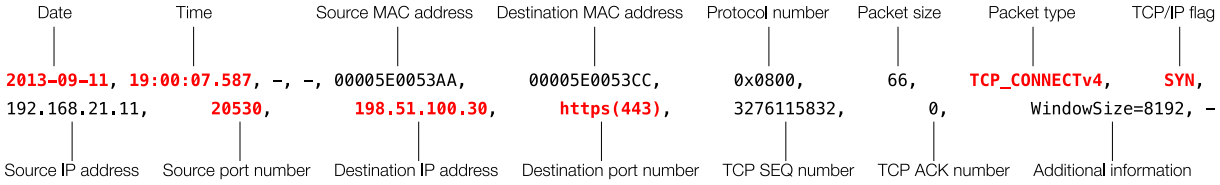

図 2: パケット警察が生成するログのフォーマット

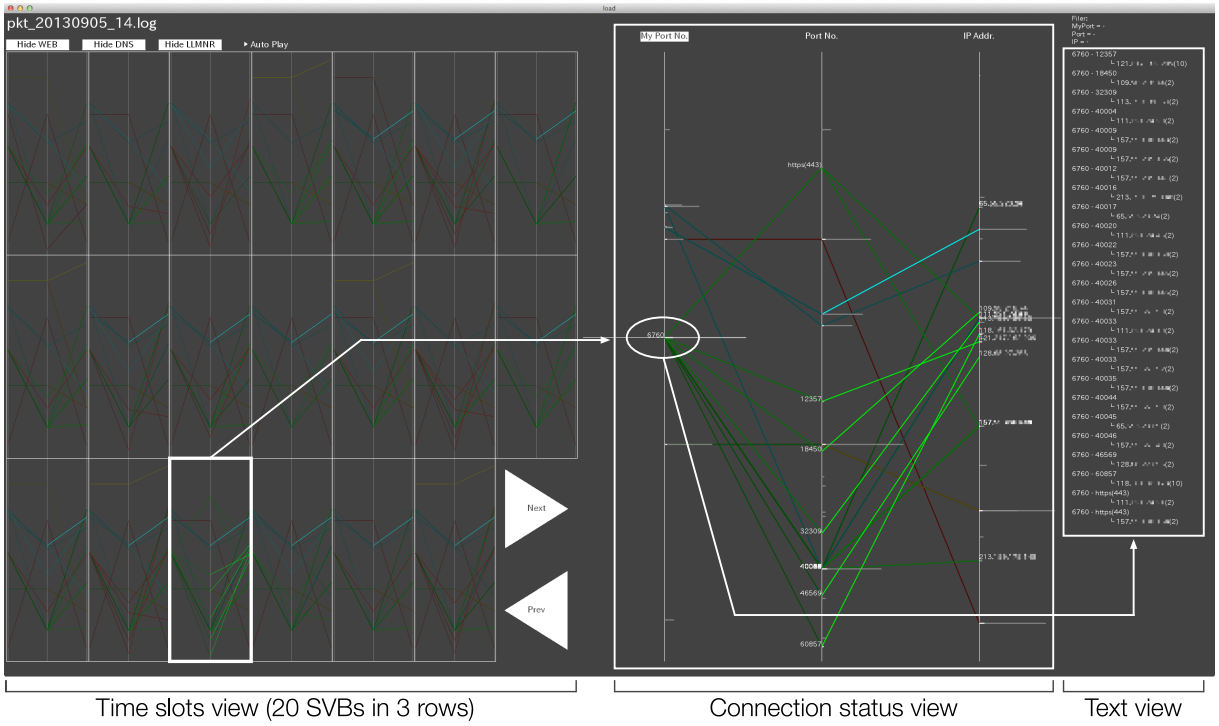

図 3: 視覚化システムのスクリーンショット

つの要素情報を使用している (図 2)．利用計算機の IP アドレスは常に利用計算機を指すために使用しない．

SVB には 3 本の縦軸があり，左からそれぞれ利用計算機のポート番号，通信先計算機のポート番号，通信先計算機の IP アドレスを示している．それぞれの軸は上から下に向かって最小値から最大値を割り当てている．例えば，IP アドレスの軸は最小値である 0.0.0.0 が最上部，最大値である 255.255.255.255 が最下部に割り当てられている．通信情報の各値を基に 3 本の縦軸上に 3 点をプロットし，直線で結ぶ．つまり 1 つの通信ログが 1 本の折れ線で視覚化される．直線の色は第 4 層のプロトコルの種類 (TCP または UDP) を示し，利用計算機がサーバであるかクライアントであるかということや通信方向によって決定される．色の割り当ては図 4 に示す．

頻度解析による疑わしい通信の表示

複数の通信記録が同一の SVB 内に視覚化されるため，複数の折れ線が描画されることになる．よって類似した要素値を持つ通信記録はほぼ同一の直線として描画される．例えば 80 番ポート，81 番ポートを使用した通信が発生した場合，それらを見分けることは難しい．提案システムでは正常な通信に紛れた異常と疑われる通信の検知を支援するため，ポート番号と IP アドレスをもとにした頻度解析を行っている．これは「不正行為や攻撃に関連する通信は正常な通信と比較して頻繁には発生しない」という推測に基づいたものである [4]．発生頻度の低い通信

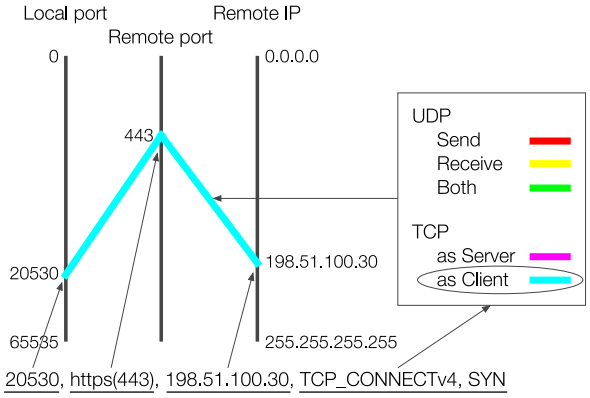

図 4: SVB の視覚化手法

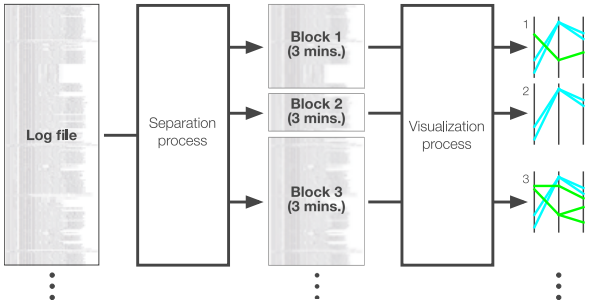

図 5: 視覚化処理部の SVB 生成プロセス

ほど明るく強調され，前面に表示される．このような手法で重要なデータを見落とすことを防ぐ．

対話的操作による表示制御

提案システムでは対話的操作によりユーザの興味に基づいたフィルタリングが可能である．

1) 特定プロトコルの表示制御

クライアント計算機の一般的な使用において，多数の通信が発生するネットワークプロトコルがいくつか存在する．典型的なものとしてはホスト名解決プロトコル (DNS や LLMNR)，そしてウェブブラウジング関連プロトコル (HTTP や HTTPS) がある．提案システムではこれらの通信を画面左上にあるボタンを押すことで簡単に消すことができる．正常と思われる通信を表示データから除外することで，視覚的な煩雑さを抑制することができ，疑わしい通信の調査に集中することができる．

2) ポート番号や IP アドレスによる絞込表示

提案システムはユーザが興味のあるデータのみを表示するフィルタリング機能も実装している．通信閲覧部のカーソルを操作することでポート番号や IP アドレスによる絞り込み条件を設定することができる．図 6 はポート番号によってフィルタリングする前後の表示の違いを示したものである．

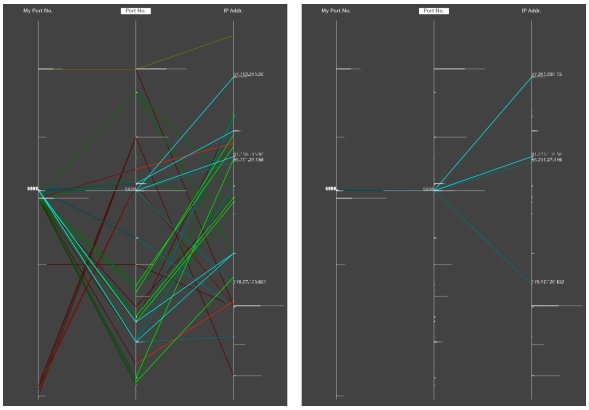

図 6: フィルタリング機能による視覚化表示の変化

4 検知事例

本章では，提案システムが異常な通信を検知可能であることを示すために 3 つの検知事例を紹介する．

4.1 マルウェアによる通信

一つ目の視覚化事例を図 7 左図に示す．この図では時系列表示部の下側二段にある複数の SVB 内に山型の折れ線が明るい線で描画されている．これは，それまで使用されていなかったポート番号 (999 番) と IP アドレス宛に対する通信がある時刻から継続して行われていることを示している．実際，これはトロイの木馬により発生したネットワーク通信の例である．このトロイの木馬に感染すると，攻撃者からの命令により感染計算機のデスクトップ画面のリアルタイムキャプチャ，ファイルシステムの読み書き，パケットの盗聴などが実行可能になる．このため，攻撃者からトロイの木馬への命令と，命令による実行結果を攻撃者側に送信するため，ネットワーク通信が必要となる．今回の視覚化事例ではネットワーク通信で使用されたポート番号と IP アドレス

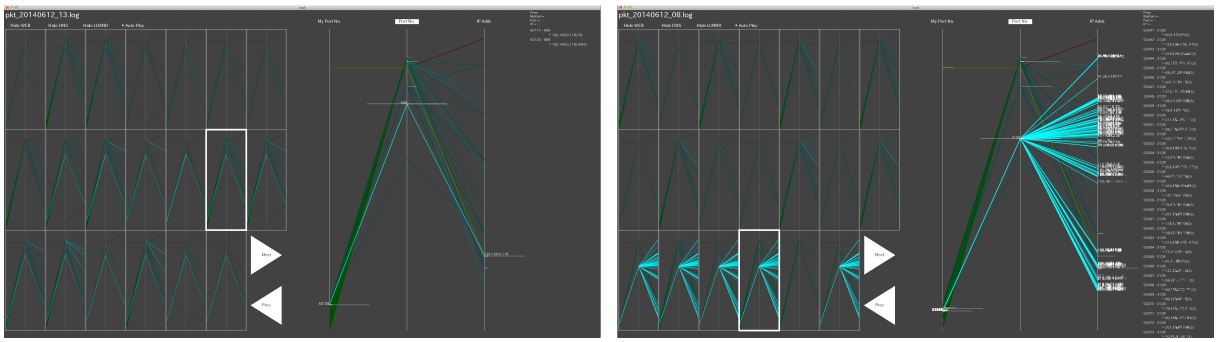

図 7: トロイの木馬による通信 (左) とネットワークスキャン (右) の視覚化事例

の組による通信はこれまで発生していなかったため，明るい線で描画され，結果として感染に気づけた事例である．

もう 1 つの視覚化事例を図 7 右図に示す．この例では時系列表示部の最下段にある複数の SVB 内に明るい線が描画されている．さらに詳しく調査するため，その 1 つを通信閲覧部に拡大表示させた．拡大表示した SVB を見ると，通信先のポートと IP の軸の間には多数の線が描画されていることがわかる．この表示から，多数の計算機の特定ポート (3128 番) に対して監視計算機から通信を試みていることが理解できる．これは，いわゆるネットワークスキャンであると結論づけられる．このような状況は，計算機に感染したワームがさらに感染を広げるために行う処理であることが知られており，マルウェア感染を疑って詳細な調査を行うべき状況にあることがわかる．

4.2 ポートスキャンにより発生した通信

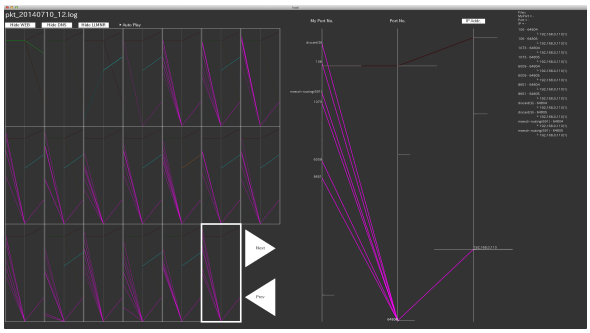

図 8: ポートスキャンと推測される通信の視覚化事例

図 8 の視覚化表示から，監視計算機側の多数のポートへアクセスしてきていること，このネットワークアクセスはしばらくの間続いていることがわかる．これらから，特定 IP を持つ計算機から監視対象計算機に対して時間をかけたポートスキャンが行われたと推測される．攻撃者が攻撃の事前調査としてポートスキャンを行う場合には，IDS などによる検知を回避するため，時間をかけて調査を行う場合がある．このように，悪意のある通信が時間をかけて行われた場合，もし単一の SVB のみを表示するような視覚化システムでは誤った判断をしてしまう可能性があるが，本システムでは時系列表示部の仕組みにより，より良い判断をすることができる．

4.3 特徴的な視覚化表示を示す通信

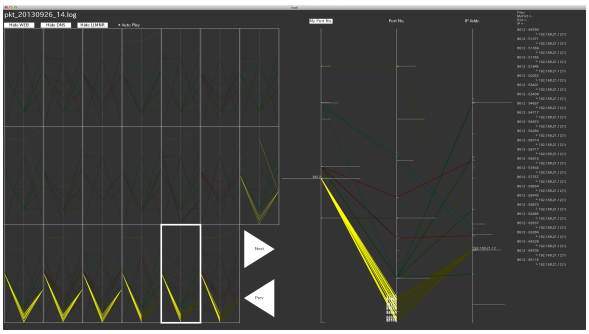

図 9: プリンタユーティリティソフトウェアによる特徴的な通信の視覚化事例

図 9 では，LAN 内にある計算機から，監視対象計算機の 8612 番ポートへ UDP で通信が発生した際の視覚化例である．その通信は明るい線として描画されていることから，これまでは観測されてなかったポート番号による通信だということがわかる．ま

た時系列表示部の描画から，該当通信はある時間から少なくとも 15 分以上にわたって継続して発生していたことも視認できる．この通信について調査を行ったところ，Canon 製プリンタのユーティリティソフトウェアがネットワーク上に存在するであろう同社製のプリンターを見つけるために行うブロードキャスト通信であることがわかった．実際にそのパケットの送信元となっていた計算機を調査したところ，確かに Canon 製のプリンタユーティリティソフトウェアがインストールされていることがわかった．

5　考察

本章では，関連研究との比較，セキュリティ向上に関する限界，そして今後の課題について述べる．

5.1　関連研究

ネットワークセキュリティを高めたり，システム管理者の作業を支援することを目的とした視覚化システムは多数提案されている [5, 6, 7, 8, 9]．これに対して，クライアント計算機を対象とした視覚化システムは文献調査した範囲において数えるほどしかないのが現状である．

“Sesame”[10] はクライアント計算機向けに設計されたネットワーク視覚化システムであり，我々のシステムと目的や調査対象が同じである．Sesame もクライアント計算機のネットワーク通信に注目し，利用計算機内で動作しているプログラム，プログラムによって表示されている GUI ウィンドウ，プログラムと通信を行っている通信先ホストの 3 点の関係性を視覚化している．しかしながら，この視覚化表現は実際の計算機モデルに基づいているために，そのモデルに関する知識が要求される．さらに，Sesame は 1 つの視覚化画像しか表示しないため，複数の視覚化画像の比較による発見は困難だと考える．

5.2　セキュリティ向上に関する限界

提案システムでは検知することが難しい脅威もある．

例えば提案システムでは頻度解析を行い，今までには使用されていなかったポート番号や IP アドレスと通信が行われた場合にはその通信に該当する直線を明るく強調してユーザに提示するが，通信の初期段階で問題のない通信であるという誤った判断がされた場合には，それ以降で再度発見することは難しい．これは頻度解析結果の視覚化反映手法に伴う問題である．

また，よく使われるポート番号を使用したマルウェアの通信は，他の多数の通信に紛れてしまうため，発見することが難しい．例えばウェブブラウジングに関連するプロトコル (HTTP や HTTPS) が使用する 80 番と 443 番ポートの通信は，初めて閲覧するウェブサイトがあるたびに明るい直線で描画される．マルウェアがそれらのポートを使用した場合，初めての通信でも発見することが難しい，

5.3　今後の課題

本節では，前節に挙げた限界を踏まえ，提案システムに関する今後の課題について 3 点ほど述べる．

1 つ目は視覚化手法の検証と改良である． 本システムではログブロックの時間間隔，SVB の視覚化手法，通信頻度と明るさの関係など，著者らの経験則に基づいて視覚化手法を決定している点がいくつかある．これらの決定に関して妥当性を評価し，必要に応じて改良を行う必要がある．

2 つ目は疑わしいネットワーク通信の検知を支援する検知支援機能の充実である．現在実装されている頻度解析に基づく強調表示は，初期の通信で誤った判断をしてしまった場合にそれ以降の検知が難しい．そのような場合にも検知が可能になる改良や，他の指標を使用した抽出支援機能の追加を行う．

最後は，エンドユーザによる異常の判定をより容易にするために別の情報もシステムに取り込むことである．現在のシステムでは，様々なプログラムによって使用されるネットワークプロトコルに紛れた異常な通信は発見することが難しい，この問題を解決するために，ネットワーク通信の分析を支援する情報の追加を検討する．

6　おわりに

既存の対策だけでは，最近のクライアント計算機に対する気づかれにくい攻撃や多数発生するマルウェアに対応することが難しくなってきている．そこで我々は既存の対策に加えて補完的に使える調査手段として，疑わしい通信への気づきを支援するシ

ステムを提案した．提案システムはクライアント計算機を対象に設計されており，ネットワーク通信を視覚化し，エンドユーザによる疑わしい通信の発見を支援する．

提案システムはログを一定時間ごとのログブロックにまとめて視覚化することで，ユーザの中に視覚的な正常状態のモデルを構築することを可能にした．これにより，ユーザは視覚化画像を見比べることで，疑わしい通信が発生しているかどうかに気づくことができる．さらに，時系列に複数の視覚化画像を並べ，通信頻度の指標により疑わしいと判断された通信の表示を強調してユーザの異常発見を支援する．提案システムによりログ閲覧の負担が減少すれば，ユーザが毎日ログを見る可能性が高まり，正常状態の正確なモデルを構築することが可能になる．

検知事例では提案システムによる 4 つの事例を紹介した．どの事例もその通信の特徴を視覚的に表現することができている．プリンタユーティリティソフトウェアによる通信の例は，異常な通信ではなかったものの，提案システムが疑わしい通信を検知できる可能性を示している．提案システムが提示する視覚化表現を見れば，エンドユーザは視覚化画像の違いを識別することによって，異常な通信を認知できると考えている．今後はシステムのログブロックの時間間隔，SVB の視覚化手法，頻度と明るさの関係などの妥当性を検証し改良を行う．また，現在の視覚化手法以外の手法も検討する．これらの課題を改善することで，クライアント計算機にとってよりよいセキュリティツールにするべく研究を続ける．

参考文献

[1] 株式会社ラック：ラック、日本でも発生した『水飲み場型攻撃』に対して注意喚起，入手先 ⟨ http://www.lac.co.jp/news/2013/10/09_press_01.html⟩ (参照 2014-08-24)．

[2] Gibbs, S.: Antivirus software is dead, says security expert at Symantec, theguardian.com, available from ⟨http://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec⟩(accessed 2014-08-25).

[3] ソフトイーサ株式会社：パケット警察 for Windows，入手先 ⟨http://www2.softether.jp/jp/packetpolice/download.aspx⟩(参照 2014-08-25)．

[4] Takada, T., Koike, H.: MieLog: A Highly Interactive Visual Log Browser Using Information Visualization and Statistical Analysis, *In Proc. of the 16th USENIX Conf. on System Administration*(LISA'02), pp.133-144, ACM (2002).

[5] Goodall, J.R., Lutters, W.G., Rheingans, P., et al.: Preserving the big picture: visual network traffic analysis with TNV, *In Proc. of the IEEE workshop on Visualization for Computer Security*(VizSEC'05), pp.47-54, IEEE (2005).

[6] Tricaud, S.: Picviz: finding a needle in a haystack, *In Proc. of the 1st USENIX conf. on Analysis of system logs*(WASL'08), 9 pages, ACM (2008).

[7] Inoue, D., Eto, M., Yoshioka, K, et al.: nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis, *In Proc. of Workshop on Information Security Threats Data Collection and Sharing*(WISTDCS'08), pp.58-66, IEEE (2008).

[8] Inoue, D., Eto, M., Suzuki, K., et al.: DAEDALUS-VIZ: novel real-time 3D visualization for darknet monitoring-based alert system, *In Proc. of the 9th Int'l Symp. on Visualization for Cyber Security*(VizSec'12), pp.72-79, ACM (2012).

[9] 株式会社ディアイティ：CAPLogger (Communcation And Process Logger)，入手先 ⟨http://www.dit.co.jp/products/caplogger/⟩(参照 2014-08-25)．

[10] Stoll, J., Tashman, C.S., Edwards, W. K., et al.: Sesame: Informing User Security Decisions with System Visualization, *In Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*(CHI'08), pp.1045-1054, ACM (2008).