推薦論文

# 内部ネットワーク監視を目的とした時間・論理・地理情報の統合的視覚化システム

向坂真一[†1] 小池英樹[†1]

内部ネットワーク監視の重要性が増している．外部から攻撃されている内部計算機だけでなく，外部へ攻撃している内部計算機の早期発見，および適切な事後対応のためには，攻撃の時間情報，IP アドレスなどの論理情報に加え，計算機の物理的場所，つまり地理情報が重要である．本論文では，時間情報，論理情報，地理情報を 3 次元空間内に統合的に視覚化するシステムについて述べた．各情報を 3 次元空間に適切に配置することで，個々の情報を把握しつつ互いの関係をも把握することができるようになった．また，膨大なセキュリティログ視覚化時に起こる表示の複雑さを解決するために，ポート番号，inbound/outbound トラフィック，特定の IP アドレスブロックなどによるフィルタリング機能を実装した．システム管理者は GUI だけでなくコマンド入力によって対話的操作を行うことができる．本システムを著者らの所属する大学の情報基盤センターで運用し，効率的な監視が可能となることを示した．

# An Integrated Visualization System of Temporal, Logical and Geographical Information for Internal Network Monitoring

Shinichi Mukosaka[†1] and Hideki Koike[†1]

Monitoring internal network is getting more and more important. In order to detect computers being attacked from external network as well as computers attacking the external network, and to act properly, it is important to know geographical information as well as temporal and logical information. This paper described the system which visualizes temporal, logical, and geographical information simultaneously in 3-D space. By laying out these information adequately in 3-D space, it becomes possible to focus on each information as well as to see their mutual relation. The user can narrow down his/her investigation by setting his/her focus on port number, inbound/outbound traffic, or any particular IP address block. The system allows command input as well as GUI interaction. The system was used in the computer center of our university, and we found the system was practical and useful to find attacks.

## 1. はじめに

現在，多くの企業や大学などの組織においてネットワークセキュリティ監視が行われている．これらは主として，コンピュータウィルスや不正アクセスなど，外部ネットワークから内部ネットワークへの攻撃を監視し防止することが目的である．各種攻撃をファイアウォール（FW）や不正侵入検知システム（IDS）で検知し，必要に応じてポートを閉じるなどの対策をとることで，攻撃が内部ネットワークに到達しないように監視を行っている．

これに対し，近年，内部ネットワーク監視の重要性が高まっている．内部ネットワーク監視とは，上に述べた外部から内部への攻撃の監視に加えて，内部から外部への攻撃および内部から内部への攻撃をも監視しなければならない．たとえば，内部の計算機がウィルスに感染して踏み台化され，外部の計算機に対して攻撃を行っている場合，これをいち早く検知して停止させなければ，その組織は責任を問われる．あるいは，内部の計算機において P2P ソフトが稼働し，音楽や動画などの著作権コンテンツを外部から不正にダウン

†1 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, University of Electro-Communications

本論文の内容は 2006 年 10 月のコンピュータセキュリティシンポジウム 2006（CSS2006）にて報告され，CSEC 研究会主査により情報処理学会論文誌への掲載が推薦された論文である．

ロードしている場合にも，迅速にこれを停止させなければ損害賠償を請求されうる．

こうしたネットワークセキュリティ監視には視覚化が有効であることが報告されている[1),7),8),10)]．FW や IDS の出力する膨大な量のログは，そのままでは解析に適当でないが，これを視覚化表示することで適度な抽象化を行い，人間の視覚的認知能力を利用して必要な情報を迅速に発見することができる．しかしながら，セキュリティ監視に利用されるログの量は非常に膨大で，単純に視覚化を行うと，画面が乱雑になるだけで，なんら有益な情報を得ることができない．対象分野の特徴を考慮したうえで，見やすい視覚化設計が重要である．

本論文では，内部ネットワーク監視を目的とした視覚化システムについて述べる．本システムの第 1 の特徴は，内部ネットワーク監視において重要な，時間情報，論理情報，地理情報を 3 次元空間内に適切に配置することで，個々の情報を把握しつつ互いの関係をも同時に把握できるようにしたことである．特に地理情報は内部ネットワーク管理において有効である．ユーザは GUI およびコマンド入力を利用して対話的に操作を行うことができる．第 2 の特徴は，大規模なセキュリティログの視覚化によって生じやすい表示の複雑化を回避するために実装した各種フィルタリング機能である．システムは事前のネットワークスキャン結果を利用して，IDS ログ内の明らかな誤検知を除外したうえで視覚化を行う．そのうえで，ユーザはポート番号指定，inbound/outbout 指定などを対話的に行うことで，情報の絞り込みが可能である．

本論文の構成は以下のとおりである．次章では，内部ネットワーク監視における課題とその解決策について述べる．3 章では実装したシステムの詳細について述べる．4 章では著者らの所属する大学の情報基盤センターでの運用例を示す．5 章は考察，6 章は関連研究，7 章でまとめを述べる．

## 2. 内部ネットワーク視覚化における課題とその解決策

### 2.1 地理情報の重要性

後述する関連研究にも見られるように，一般のネットワーク監視においては，時間情報と論理情報がよく利用される．時間情報は攻撃の発生した時間に関する情報である．論理情報は攻撃元（source）あるいは攻撃先（destination）の IP アドレスやポート番号などに関する情報である．

内部ネットワーク監視においてはこれに加えて地理情報が必要となることが多い．組織内においてなんらかの攻撃を検知した場合，システム管理者は攻撃先（元）の IP アドレスを特定し，そのサブネット管理者に対してメールあるいは電話で警告を行う．ところが，登録されたサブネット管理者が存在しなかったり，不在だったりすることがある．緊急を要する事件の場合には，システム管理者は直接その場に赴き，当該計算機をネットワークから切断したり，停止させたりするなどの措置をとらなければならない．このような場合，当該計算機の IP アドレスだけでなく，実際の設置場所を知る必要がある．そこで本研究では，従来の時間，論理情報に加え，地理情報をも表示することとした．

### 2.2 時間，論理，地理情報の統合表示

次に，これらの 3 つの情報を視覚化する場合，考えられる 1 つの方法はマルチウィンドウを利用して，各情報をそれぞれ別々なウィンドウに表示することである．しかし，互いに密接に関連する複数の情報を異なるウィンドウに表示すると，相互の関連性や全体のコンテキストを見失うという欠点が指摘されている[6)]．

これに対し，3 次元空間を有効に利用することで，複数の情報とその関連性を同時に把握することができる．本研究ではこの 3 次元視覚化の概念を導入することで，時間，論理，地理という 3 つの互いに関連する情報を同時に表示することとした．

### 2.3 表示の複雑化への対応

情報視覚化における主たる問題点の 1 つが，表示情報の増加にともなう表示の複雑化である．本来，図の利用によって人間の視覚的認知能力を効果的に活用しようとしているにもかかわらず，表示の複雑化によりそれが阻害されてしまう．特に IDS のログはそのサイズが大きく，単純な視覚化は単に複雑な図を作り出すだけとなってしまう．

この問題に対し，いくつかのフィルタリング機能を導入することで解決を試みた．単純なフィルタリングは，IP アドレス，ポート番号，inbound/outbound の別，IDS のシグネチャによるフィルタリングである．また本研究において特徴的なのは，事前ネットワーク調査に基づくフィルタリングである．これについては 3.4.3 項で述べる．

### 2.4 熟練管理者への対応

一般に，マウス操作を主とする GUI システムは計算機専門家以外の人々には評判が良い．一方で，計算機専門家の中にはキーボード操作を中心としたシステムを好む人が多い．この主たる理由は，キーボード入力（CUI）の方が操作が速いからである．本システム

の対象ユーザは熟練ネットワーク管理者であるため，キーボードによる迅速なコマンド入力を支援する必要がある．

そこで本システムでは，GUI 操作と同時に CUI をも実装することとした．これにより，UNIX などに習熟した熟練管理者が行っているようなキーボード入力により，高速な操作が可能となる．これについては 3.4.2 項で述べる．

## 3. 統合的視覚化システム

### 3.1 概　　要

前章までの考察をもとに，時間情報，論理情報，地理情報を統合した内部ネットワーク監視システムを構築した．

**図 1** にシステムの処理フローを示す．システムはまず Nmap[12] によるネットワーク調査結果と事前に登録してある IP アドレスと建物の関係を読み込む．次に IDS のログを読み込む．最後にユーザ入力でフィルタリングされた結果を画面に視覚化する．システム全体は C++で記述され，描画部分には OpenGL を用いている．

### 3.2 ログの取得

IDS としては Proventia[5] もしくは Snort[16] が使用できる．

ログの読み込みにはオフラインモードとオンラインモードがある．オフラインモードはすでに記録されているログを読み込むモードで，1 時間分読み込んでは 1 秒間読み込みをスリープし視覚化に反映するという操作を 24 時間分繰り返すため読み込みの終了には最低でも 24 秒かかる．Apple PowerBook G4 1.67 GHz，メモリ 2 GB で実行したところ，Proventia 6.7 MB のログの読み込みに 30 秒程度かかった．オンラインモードは最初オフラインモードと同様にログを読み込むが，すべてのログを読み込んだ後は 10 秒ごとにログの新しいエントリを調べ視覚化に反映する．参考までに，フィルタリングには Proventia のログ（6.7 MB）で 1 秒未満，Snort のログ（345 MB）で約 5 秒を要した．

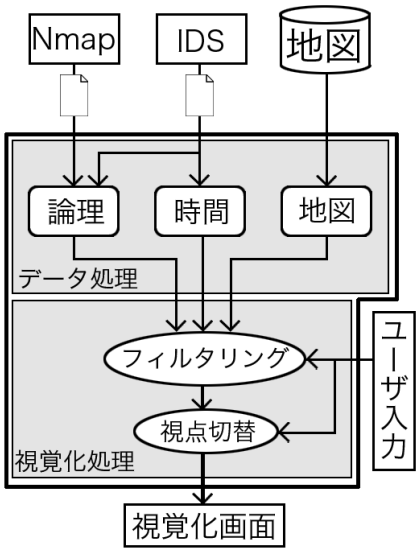


**図 1** 処理の流れ
Fig. 1 Processing flow.

### 3.3 視　覚　化

**図 2** はシステムの画面スナップショットである．画面左に時間情報を表す時系列グラフ，その右に論理情報を表す IP Matrix[7]，下に地理情報を表す地図が，立方体の互いに垂直な平面に表示される．以下にそれぞれについて説明する．

#### 3.3.1 論 理 情 報

論理情報である IP アドレス空間を示す手法として IP Matrix を用いた．IP Matrix は IP アドレスの上位 16 bit もしくは下位 16 bit を二次元に視覚化する手法である．本研究の対象とするネットワークはクラス B なので，上位 16 bit である第 1 オクテットと第 2 オクテットが共通なので，下位 16 bit を視覚化する IP Matrix を使うことで内部ネットワークのすべての計算機を表現することができる．この IP Matrix を用いて縦軸に IP アドレスの第 3 オクテットを，横軸に第 4 オクテットをとってプロットした．

ポートスキャンツールである Nmap を用いて事前ネットワーク調査を行った．Nmap は空いているポート番号と OS の種類が分かる．これによって得られた OS の種類を異なる色でプロットした．また後述するフィルタリングによってポート番号を指定した場合には，そのポートが空いている計算機のみをプロットした．詳細な OS のバージョン番号はマウスカーソルを

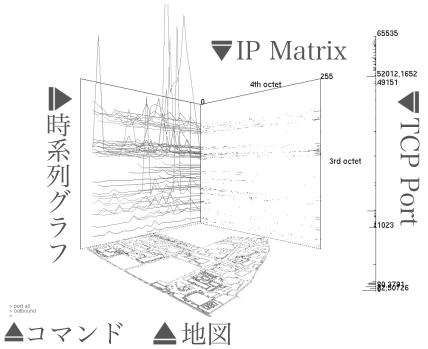


**図 2** 視覚化画面
Fig. 2 A snapshot of the system.

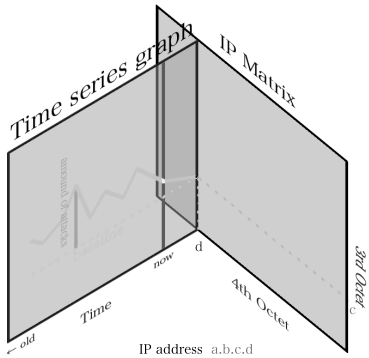


**図 3** IP Matrix と時系列グラフの関係．時系列グラフは IP Matrix に垂直に移動できる
Fig. 3 IP Matrix and time diagram. The time diagram can be moved in perpendicular to the IP Matrix.

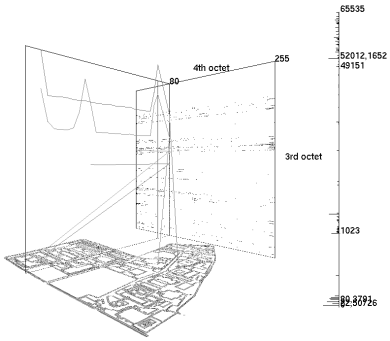


**図 4** 第 4 オクテットの変更
Fig. 4 Changing the focused 4th octet by moving the time graph plane.

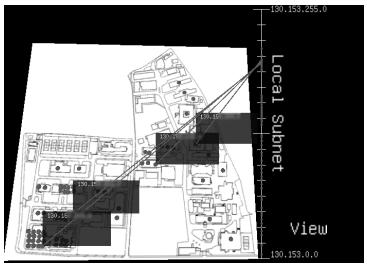


**図 5** ネットワークアドレスと建物の対応関係の入力ツール
Fig. 5 A tool for defining relation between network address and buildings.

プロットした点に重ねることでテキストで表示した．

ネットワーク攻撃は特定の OS，特定のサービスに対してのみ有効な攻撃が多いため，論理情報を攻撃の有効性の判断に用いることができる．また，後述するフィルタリングによって特定の OS への攻撃のみを表示できるようにした．

### 3.3.2 時 間 情 報

時系列グラフは IP Matrix に垂直な面に表示される（**図 3**）．IP Matrix 上の IP アドレスから垂直な線を時系列グラフのベースラインとした．横軸は時間であり，右にいくほど新しい．縦軸は IDS が検知した攻撃量である．各線の色はデータの区別のためだけに用いた．セキュリティ監視においては，具体的な攻撃量の数値よりもネットワーク間の比較が重要である．たとえば，同時に攻撃が増えている，あるいは減っている現象や，他が同じ挙動をしているのに 1 つだけ異なるといった現象である．この時系列グラフでは攻撃量の具体的な数値は分かりにくいが，攻撃量の変化が分かりやすい．たとえば複数の計算機への攻撃量が同時に増えているときや，1 つだけ異なる波形をしているときに，視覚的に把握しやすい．

時系列グラフの面は IP Matrix に垂直なまま横軸の方向に平行移動することができ，それによって表示する第 4 オクテットを変更することができる（**図 4**）．ただし第 4 オクテットが 0 のときはサブネットごとの攻撃量の和を示すようにした．第 4 オクテットが 0 とはネットワークアドレスのことを示すので，熟練管理者にとってはネットワークアドレス全体の挙動を把握しやすい．

監視業務において管理者は全体から詳細へとフォーカスを移す．サブネットごとにまとめられた情報によって全体を見ることができる．さらにこのグラフの 1 つをクリックすることで，そのネットワークアドレスにある各計算機のグラフのみを表示するようにした．

### 3.3.3 地 理 情 報

地理情報として内部ネットワークのすべての計算機の位置を表示できるように地図を用いた（**図 5**）．

一般に IP アドレス空間と地図上の位置に規則性はない．大規模 LAN では使用する IP アドレスもコンピュータの数も多く，IP アドレスからどの建物にある計算機かを瞬時に判断することは難しい．ただし，同一の建物や部屋には連続したアドレスブロックが割り当てられることが多い．

そこで IP アドレスと地図との対応を示すために，IP Matrix 上の点からそのアドレスの計算機が存在する建物の位置に線をひいた．線の色は前述の時系列グラフにおいてその計算機の状態を示す折れ線と同じ色を使った．ただし，地図と IP Matrix の対応の線が多すぎると，画面奥行き方向の図が隠されてしまう問題，いわゆるオクルージョン[3] が発生するため，後述するフィルタリングによって該当する IP アドレスの数が閾値（100 hosts）以下のときのみ表示させた．

本システムを様々なネットワークに応用するには，地図と IP アドレスを対応付ける必要がある．現段階

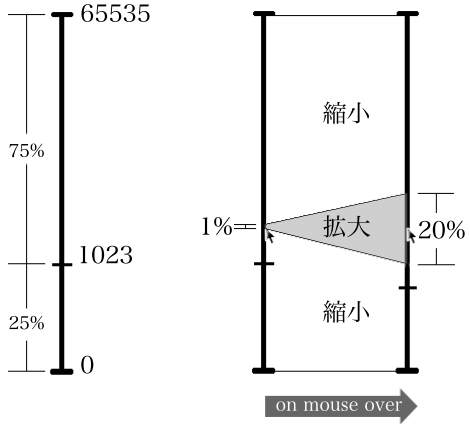


**図 6** TCP ポートの視覚化とズーミングインタフェース
Fig. 6 Visualization of TCP port and zooming interface.

では本システム自体は IP アドレスと地図上の位置の対応付けを対話的に入力する機能は持っていないが，我々は本システムとは別個に対話的な入力ツールを作成し利用した．これはサブネットアドレスを指定した後，地図上の点をマウスでクリックすることで両者の対応関係のリストを作成する．これには地図の区画数と管理されるサブネットアドレス数に比例した工数を必要とする．

#### 3.3.4 ポート情報

一般に攻撃の送信先ポートを見ることでどのサービスへ攻撃したかが分かる．本監視システムでは，画面の右側に TCP の送信先ポートを表示した．縦軸はポート番号を示し，横軸は攻撃量の対数をとった棒グラフになっている．縦軸の下から 25% は well known port と呼ばれる 1024 番までのポートを表示し，その上は 65535 番までを示している．well known port はウェブやメール，DNS などの重要なサービスが多く，そのため攻撃の対象にもなりやすい．もしすべてのポートを等間隔で表示すると，well known port は全体の 1.56% に表示されてしまうため，重要な情報を見落としてしまうおそれがある．ポート番号を示す軸に対数や立方根をとる方法[10] もあるが，数字の小さいポートに無駄な領域が発生する．

攻撃量の多いポートは疑わしいので，攻撃量の多い上位 3 つのポート番号と攻撃件数を棒グラフの右側に表示した．この軸には LensBar [11] のようなズーミングインタフェースを用いた．マウスカーソルをのせると，カーソルを中心として全体の 1% の場所にあるデータが**図 6** の右側のように，カーソルのある座標を中心に 20% に拡大される．このとき，拡大された範囲にあるデータの右側にポート番号と攻撃件数が表示される．その状態でクリックすると拡大した状態が維持され，マウスを動かしても拡大した部分は移動しなくなる．もう 1 度クリックすることでポートを選択し，フィルタリングをかけることができる．

また，後述するコマンド操作でもフィルタリングが可能である．

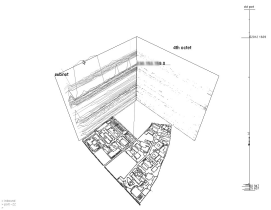

**図 7** 全体からから疑わしいサブネットのグラフを選択
Fig. 7 Select a suspicious graph of subnet.

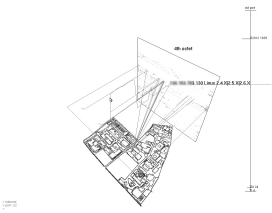

**図 8** サブネットから疑わしい IP のグラフを選択
Fig. 8 Select a suspicious graph of a host.

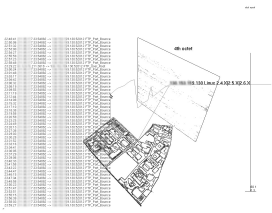

**図 9** 詳細なアラートをテキストで表示
Fig. 9 Put texts of detail alerts.

### 3.4 対話的操作

内部ネットワークの情報は膨大で 1 度に見ることができない．そこで本システムは対話的に操作することで表示する情報の切替え・絞り込みをできるようにした．これは全体的な情報から必要な詳細情報へとユーザの入力によって適切に表示することを目的としている（**図 7**，**図 8**，**図 9**）．マウス操作によるポート番号のフィルタリングと OS の詳細情報の表示についてはすでに述べた．また，計算機の熟練ユーザである管理者にとって使いやすいコマンド入力も可能にした．

#### 3.4.1 絞り込み操作

起動直後はサブネットごとの時系列グラフを表示することで全体情報を表示しているが，この画面からど

**表 1** 利用可能なコマンド一覧
Table 1 Command list.

| コマンド名 | 内容 |
|---|---|
| inbound | 外部から内部への攻撃を表示 |
| outbound | 内部から外部への攻撃を表示 |
| view | 視点の切り替え |
| list | 該当する IP アドレスのリストと該当する件数の出力 |
| detail | IDS のアラートを出力 |
| port | ポート番号によるフィルタリング |
| ip | IP アドレスによるフィルタリング |
| os | OS によるフィルタリング |
| signature | IDS のシグネチャによるフィルタリング |
| save | フィルタを保存 |
| load | フィルタを読み込む |
| exit | システムを終了 |

れが障害のある計算機であるかを対話的な操作によって絞り込んでいく必要がある．サブネットを表示している場合に選択すると，そのサブネットの各計算機の時系列グラフが表示されるようになり，さらにその中の 1 つを選択するとその IP アドレスのみの時系列グラフが表示されるようにした．また時系列グラフをマウスオーバすることで，OS の詳細情報を示すようにした．

### 3.4.2 コマンド入力

一般に操作方法には GUI を利用した方法とコマンド入力がある．マウスは視覚化システムを対話的に直接操作できるが，正確な操作には時間がかかる．本システムでは熟練管理者が使うことを想定している．そのため GUI だけでなく，熟練者が普段から用いているコマンド入力も可能とした．コマンドは画面の左下に描画され，緻密な操作が可能となる．**表 1** は本システムで使用可能なコマンドの一覧である．このコマンドの中には外部から内部への攻撃，内部から外部への攻撃の切替え，IP アドレスや OS 種別，攻撃名称によるフィルタリングなどがある．

### 3.4.3 フィルタリング

大規模内部ネットワークのログは膨大であるため，すべてを見ることは難しい．そのため，実際にネットワーク管理でログを解析する際には “grep” コマンドを用いてフィルタリングしている．同様に視覚化システムは全体が見えることのほかに，フィルタリングによって特定の情報を抽出する機能が必要である．本システムではポート番号によるフィルタリングをマウス操作でできるだけでなく，IP アドレス，IDS アラートのシグネチャによってフィルタリングすることができる．これによって特定の条件のみを表示することや特定の条件以外を表示することができる．たとえば，SSH 以外を表示させたければコマンド入力で “`port -22`” と入力すればよく，ポート 6000 から 8000 までを表示させたければ “`port 6000:8000`” と入力すればよい．

セキュリティ監視において，IDS が生成する警告量の多さは監視を困難とする大きな理由の 1 つである．さらに悪いことに，その警告の多くが誤検知である．無思慮に警告すべてを視覚化してしまうと図が複雑化するだけで，効率的な監視はできない．そこで本システムでは事前ネットワークスキャンを行うことで明らかな誤検知のフィルタリングをも行った[17]．具体的には，実際に稼働している計算機とその OS 情報などを取得しておくことで，存在しない IP アドレスへの攻撃に関する警告や，実際に稼働しているのとは異なる OS への攻撃に関する警告は誤検知と見なし，除外することができる．こうしたネットワークスキャンは，外部ネットワークに対しては一般に許されないが，内部ネットワークの場合，組織のセキュリティポリシに基づき，事前通知をしたうえで実施することが可能である．

以上のような操作によってフィルタリングするとその条件にあてはまるデータのみで時系列グラフを再作成して描画する．特別にポート番号の選択においては IP Matrix にはそのポートが空いている計算機がプロットされる．フィルタリングの結果，表示するデータの量が減ったことで該当する IP アドレスが閾値（100 hosts）以下になった場合には IP Matrix と建物の対応関係を線で表示させた．また，実際の管理では既知の誤検知を除去するため，同じフィルタリングを用いることがある．そこで本システムではフィルタの保存と読み込みを実装した．

### 3.4.4 視点切替え

オクルージョンの問題を防ぐことと，正確に読み取るために視点切替え機能を実装した．本システムでは全体を見下ろす俯瞰図と，IP Matrix，時系列グラフを正面から見た図と，各面が展開した図の 4 つをアニメーションで切り替えて表示することができる．それぞれの視点は一長一短であるため，必要に応じて切替えを行う．俯瞰図は全体を把握することに優れているため，初期画面として用いた．IP Matrix と時系列グラフは正面から見ることで正確に観測できる（**図 10**，**図 11**）．展開図は立方体表示の各面を同一平面上に展開したものである．これはすべてを正面から見ることができるが，IP Matrix と時系列グラフの関連性が分かりにくくなる（**図 12**）．3 次元視覚化では視点を自由に変更できるものが多い．一方で，自由な視点移動は 3 次元空間における迷子問題を生じる．本システム

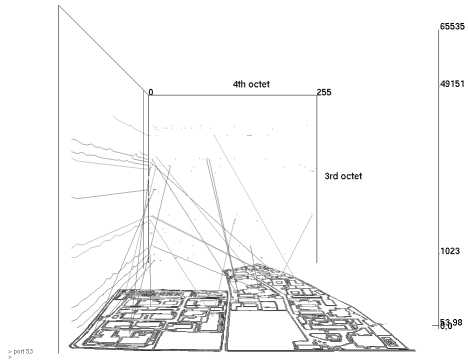


**図 10** IP Matrix 用の視点
Fig. 10 A viewpoint focusing on IP Matrix.

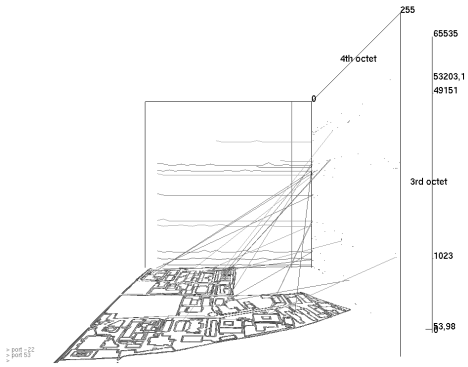


**図 11** 時系列グラフ用の視点
Fig. 11 A viewpoint focusing on time diagram.

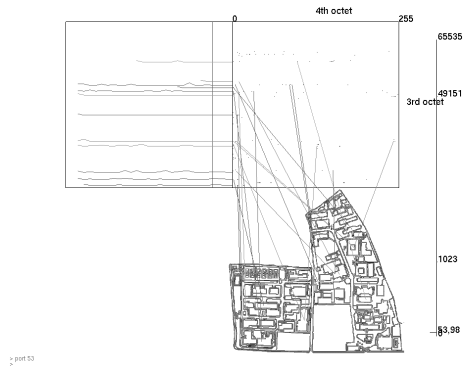


**図 12** 展開図
Fig. 12 Expansion view.

では正確にデータを読み取れる視点のみがあればよいので，特定の視点のみを切り替えるようにした．

## 4. 運 用 例

本システムは電気通信大学の情報基盤センターにおいて 2006 年 12 月から実際に運用されている．当該ネットワークはクラス B のネットワークアドレスを持つ．システムのユーザは同センターでネットワーク監視を行っているネットワーク管理者で，ネットワーク知識，セキュリティ知識ともに高い熟練度を持っている．

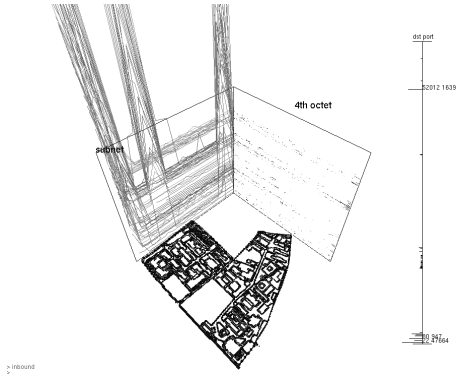


**図 13** 外部ネットワークからの攻撃
Fig. 13 Visualizing all attacks from external network.

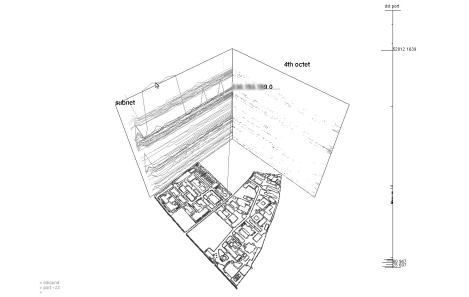


**図 14** フィルタリングで不要な SSH への攻撃を除外
Fig. 14 After filtering out the attacks to SSH.

IDS としては Snort と Proventia が，どちらも内部ネットワークと外部ネットワークの間の通信を監視できるように設置してある．Snort のログは毎日約 500 MB，Proventia のログは毎日 20 MB から 100 MB 程度出力されている．どちらのログも 1 日ごとに個別のアスキーファイルとして保存されている．

### 4.1 FTP への攻撃

**図 13** は Proventia のログを用いて外部ネットワークから内部ネットワークへの攻撃を視覚化したものである．瞬間的に多量の攻撃が来ているが，これは SSH brute force attack である．SSH brute force attack とはパスワードを次々に変えて試行し，無理矢理 SSH にログインする攻撃手法である．この攻撃では 1 回の認証の試行で 1 つのコネクションを作るため，警告の数が他の攻撃に比べて非常に多く表示される．この攻撃によって他の攻撃が隠されてしまうことが多々ある．そこで 22 番ポートを不可視にすることで，**図 14**

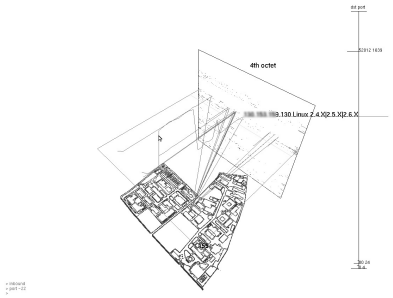


**図 15** サブネットから疑わしい IP のグラフを選択
Fig. 15 Selecting a suspicious graph.

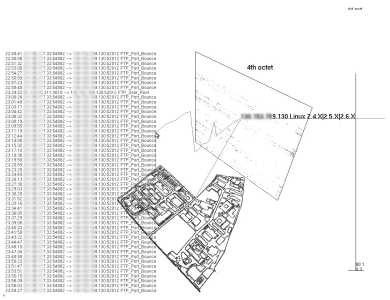


**図 16** 詳細なアラートをテキストで表示
Fig. 16 Displaying detail alerts in text.

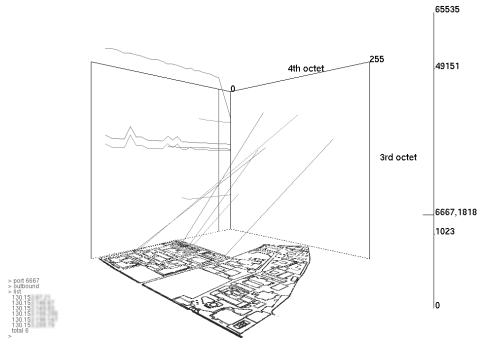


**図 17** 6667 番ポートに着目した例
Fig. 17 An example visualization when focusing on port 6667.

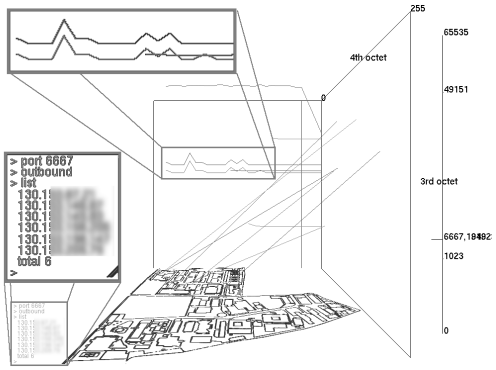


**図 18** ボットネットの挙動．異なる建物に存在する 2 つのホストが 6667 番ポートを通じて同じ挙動を示している
Fig. 18 Two hosts in the different building are showing the similar communication patterns via port 6667.

のように他の攻撃が顕著に分かるようになった．このグラフをマウスで選択すると，**図 15** のようにそのサブネットの各計算機の時系列グラフが視覚化される．この画面からある 1 つの計算機に対して攻撃がきていることが分かる．さらにここで “`detail`” とコマンド入力することで**図 16** のように IDS のログに類するフォーマットで詳細情報をテキスト表示させた．これによって FTP_Port_Bounce という攻撃を受けていたことと，その攻撃対象の位置が分かった．

### 4.2 ボットネット

**図 17** はボットネットと思われる不審な IRC chat の警告が出たときのものである．ボットネットとは外部から不正に遠隔操作された計算機（ボット）で構成された悪意のあるネットワークのことである．ボットは命令を受けるために IRC サーバに接続し，ハーダと呼ばれるボットネットを操る攻撃者の命令を待つ．IRC サーバは一般に 6667 番ポートを使っているため，この図の不審な IP アドレスへの接続はボットネットの疑いがある．6667 番ポートのみが表示されるようにフィルタリングを行い，outbound の攻撃を選んだ．今回使用したログは Snort のものである．

数カ所の IP アドレスから 6667 番ポートへのアクセスで警告が出ていることが分かる（**図 18**）．その中で（実際の画面では水色と紫色の）2 つのデータがほぼ同一の攻撃量の変化を示していることが分かる．この 2 つの計算機がまったく別の場所にあることから，異なる研究室に属する計算機が別個にボットに感染し，ハーダの命令を受けて同時に IRC サーバへの接続を行っていることが確認された．

## 5. 考　　察

本システムは設計・開発の初期段階から，熟練ネットワーク管理者との意見交換を行い，その要望を反映してきた．地理情報の表示やコマンド入力機能などはその例である．結果として，熟練者の使用にも耐えるシステムとなった．また，約 500 MB/日という大規模な IDS ログの視覚化に耐えられる点も，熟練管理者からは高く評価された．

さらに，大規模な IDS ログの視覚化の際に生じる表示の複雑化問題を重視し，表示情報量を削減する機

能を実装した．たとえば，事前に行ったネットワークスキャンの結果を利用した誤検知判別や各種フィルタリング機能は，表示情報の削減に非常に役に立った．

今後の課題としてまず第 1 にあげられるのは，ネットワークスキャンの自動化である．現在は，ある時点で行ったデータを利用しているが，時間が経つとこのスキャン結果も古くなってしまう．そこで定期的にポートスキャンを行う方法と，p0f のような passive fingerprinting を使う方法が考えられる．

第 2 の課題としては，異なる時系列グラフの表示である．現在は攻撃量を縦軸とした時系列グラフを表示しているが，実際のネットワーク監視では通信量の時間的変化に着目することがある．

第 3 の課題としてサブネットへの対応がある．現在はクラス B のアドレスのみを表示しているが，実際にはその下にサブネットを構成している部署もある．こうした計算機への対応も今後の課題である．

## 6. 関 連 研 究

内部ネットワーク監視のための視覚化には以下のようなシステムがある．

IDS RainStorm [1] では大規模 LAN として Georgia 工科大学のネットワークを視覚化した．この大学のネットワークはクラス B のネットワーク 2.5 個分の大きさがある．縦軸に IP アドレス，横軸に時間をとって表示している．縦軸の IP アドレスは 20 アドレスを 1 ピクセルで表示しており，プロットされた色は緑，黄，赤の順に危険度が高くなる．IDS Rainstorm は大量の IP アドレスとそのアクティビティの時間変化を効率的に視覚化しているが，時間変化はピクセルの色のみで表されるため，攻撃量の変化が把握しにくい．また，IP アドレスと地理的な位置関係は分からない．

Security Incident Fusion Tools（SIFT）では様々なセキュリティ情報の視覚化を行っている．NVisionIP [8] は小規模ネットワークで発生する計算機の接続やデータ転送をプロトコルまたはポート単位で統計解析を行い，視覚化を行う．Passive Visual Fingerprinting [2] と Spinning Cube [9] はともに IP アドレスとポート番号に着目した視覚化システムである．Passive Visual Fingerprinting はネットワーク攻撃の特徴を 2 次元画面に点と線とで視覚化する．Spinning Cube は立方体の 2 軸でネットワークアドレス，もう 1 軸でポート番号を視覚化している．以上のシステムでは時間情報，地理情報が欠落している．

Secure Decisions [15] では計算機のある建物のフロアと計算機の種類によって分類した二次元マトリックスと，攻撃の危険性を関連づけて視覚化している．しかし，時間情報が欠落しているため，攻撃量の時間変化が分からない．

上記すべてのシステムにおいて，表示量の削減に関する議論がない．このため，大規模なデータを視覚化した場合には，画面の複雑化が避けられない．

多次元情報を視覚化するシステムとしては，Starlight [14] や ZASH [13] がある．これらは 3 次元空間を利用して多次元情報を視覚化したものであるが，セキュリティデータのような大規模なデータへの対応や，表示量の削減手法などは議論されていない．

Starmine [4] は本システムの前身にあたり，広域監視を対象として時間情報，論理情報，地理情報を統合的に視覚化したものである．3 次元視覚化の枠組みは共通するが，広域監視と内部ネットワーク監視との相違，リアルタイムでの監視機能がないこと，ネットワークスキャンの利用，フィルタリング操作による表示情報削減機能などの点で異なる．

## 7. お わ り に

内部ネットワーク監視に焦点を当て，時間情報，論理情報，地理情報を統合的に監視することのできる 3 次元視覚化システムを開発した．大規模な IDS ログの視覚化に対応するため，事前ネットワークスキャン，各種フィルタリング機能を実装した．大学の情報基盤センターで運用し，FTP への攻撃とボットネットの視覚化を通じてその有効性を確認した．

**謝辞** 本システムに対する有益な助言と，システムの運用に協力していただいた電気通信大学情報基盤センター土屋英亮准教授と才木良治技官に感謝いたします．

## 参 考 文 献

1) Abdullah, K., Lee, C., Conti, G.J., Copeland, J.A. and Stasko, J.T.: IDS RainStorm: Visualizing IDS Alarms, *Proc. IEEE Workshop on Visualization for Computer Security* (*VizSEC 2005*), pp.1–10, IEEE Computer Society (2005).
2) Conti, G. and Abdullah, K.: Passive Visual Fingerprinting of Network Attack Tools, *Proc. 2004 ACM Workshop on Visalization and Data Mining for Computer Security* (*VizSEC/DMSEC-2004*), pp.45–54 (2004).
3) Conti, G., Ahamad, M. and Stasko, J.: Attacking information visualization system usability overloading and deceiving the human, *Proc. 2005 Symposium on Usable Privacy and Secu-*

*rity* (*SOUPS '05*), pp.89–100 (2005).
4) Hideshima, Y. and Koike, H.: STARMINE: A Visualization System for Cyber Attacks, *Proc. Asia Pacific Symposium on Information Visualisation* (*APVIS2006*), pp.131–138 (2006).
5) Internet Security Systems. http://www.iss.net/
6) Koike, H.: The role of another spatial dimension in software visualization, *ACM Trans. Information Systems*, Vol.11, No.3, pp.266–286 (1993).
7) Koike, H., Ohno, K. and Koizumi, K.: Visualizing Cyber Attacks using IP Matrix, *Proc. IEEE Workshop on Visualization for Computer Security* (*VizSEC 2005*), pp.91–98, IEEE Computer Society (2005).
8) Lakkaraju, K., Bearavolu, R., Slagell, A., Yurcik, W. and North, S.: Closing-the-Loop in NVisionIP: Integrating Discovery and Search in Security Visualizations, *Proc. IEEE Workshops on Visualization for Computer Security* (*VizSEC 2005*), pp.75–82, IEEE Computer Society (2005).
9) Lau, S.: The Spinning Cube of Potential Doom, *Comm. ACM*, Vol.47, No.6, pp.25–26 (2004).
10) Lee, C.P., Trost, J., Gibbs, N., Beyah, R. and Copeland, J.A.: Visual Firewall: Real-time Network Security Monitor, *Proc. IEEE Workshop on Visualization for Computer Security* (*VizSEC 2005*), pp.129–136, IEEE Computer Society (2005).
11) Masui, T.: LensBar – Visualization for Browsing and Filtering Large Lists of Data, *Proc. 1998 IEEE Symposium on Information Visualization* (*INFOVIS '98*), pp.113–120 (1998).
12) Nmap. http://insecure.org/nmap/
13) Orimo, E. and Koike, H.: ZASH: A Browsing System for Multi-Dimensional Data, *Proc. 1999 IEEE Symposium on Visual Languages* (*VL'99*), pp.266–286 (1999).
14) Risch, J.S., May, R.A., Dowson, S.T. and Thomas, J.J.: A Virtual Environment for Multimedia Intelligence Data Analysis, *IEEE Computer Graphics and Applications*, Vol.16, No.6, pp.33–41 (1996).
15) Secure Decisions. http://www.securedecisions.com/
16) SNORT: The Open Source Network Intrusion Detection System. http://www.snort.org/
17) 大野一広，浅沼　格，小池英樹：内部ネットワーク監視への IP Matrix の応用，コンピュータセキュリティシンポジウム（CSS2005），pp.403–408，情報処理学会 (2005).

(平成 19 年 4 月 27 日受付)
(平成 19 年 10 月 2 日採録)

## 推　薦　文

本研究は従来効果的な利用先に乏しかった地理的な情報を内部ネットワークの監視手法へ取り入れ，その効果を示している．内部ネットワークの監視においては単純に通信を遮断するだけでなく，被害者および所属組織への通知など具体的な対応が求められる．本研究は IP アドレスなどの論理的な情報と建屋などの地理的な情報を効果的に組み合わせており，内部ネットワーク監視の効果が高いと考えられる．

（コンピュータセキュリティ研究会主査　寺田真敏）

**向坂　真一**（学生会員）

2005 年横浜市立大学理学部機能科学科卒業．2007 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士前期課程修了．同年日本電子株式会社入社．現在に至る．

**小池　英樹**（正会員）

1991 年東京大学大学院工学系研究科情報工学専攻博士課程修了．工学博士．同年電気通信大学電子情報学科助手．1994 年同大学大学院情報システム学研究科助教授．1994〜1996 年，1997 年 U.C.Berkeley 客員研究員．2003 年 Sydney 大学客員研究員．2006 年電気通信大学大学院情報システム学研究科教授．現在に至る．情報視覚化の研究に従事．Focus+Context 技術，大規模ログの解析/視覚化，やわらかい認証方式，Honeypot 技術，画像認識を利用した HCI 等に興味を持つ．1991 年日本ソフトウェア科学会高橋奨励賞，2000 年情報処理学会 DICOMO 2000 最優秀論文賞，2001 年 IEEE VR2001 Honorable Mention for the Outstanding Paper Award 受賞．ACM，IEEE/CS，日本ソフトウェア科学会各会員．