# IP Matrix：広域ネットワーク監視のための視覚化手法

大野一広[†] 小池英樹[†] 小泉芳[††]

インターネット定点観測システムは，インターネット上に設置された監視センサで攻撃の検知を行う．監視センサから得られた情報は統計解析され，その結果を視覚化する．しかし既存のシステムは解析結果の国別表示や時間ごとの変化量として提示するにすぎない．これらのシステムの利用者は攻撃者の場所や攻撃者との距離，そして攻撃者と攻撃先との関連を把握することは困難である．本論文では，IP アドレスの 2 次元マトリクス表示を用いた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について述べる．本視覚化システムの利点は，1) IP アドレスの近接関係が自然に表現可能である点，2) IP アドレス空間の経済的な視覚化が可能である点である．本提案手法を用いることにより，コンピュータワームの拡散を視覚化可能とした．

# IP Matrix: A Visualization Framework for Wide Area Network Observation

Kazuhiro Ono,[†] Hideki Koike[†] and Kanba Koizumi[††]

An Internet cyber threat monitoring system detects cyber threats using network sensors deployed at particular points on the Internet, statistically analyses the time of attack, source of attack, and type of attack, and then visualizes the result of this analysis. Existing systems, however, simply visualize country-by-country statistics of attacks or hourly changes of attacks. Using these systems, it is difficult to understand the source of attack, the diffusion of the attack, or the relation between the target and the source of the attack. This paper described a method for visualizing cyber threats by using 2-dimensional matrix representation of IP addresses. The advantages of this method are that: (1) the logical distance of IP addresses is represented intuitively, (2) Internet address space is visualized economically. By using this visualization framework, propagation of the computer worms are visualized.

## 1. はじめに

近年，インターネットワームや DDoS（分散サービス妨害攻撃）などのサイバー攻撃が社会生活において大きな問題となっている．これらの大規模攻撃はすでに重要な情報インフラとなっているメールシステムや Web システムを停止させることから，経済活動や公共サービスに大きな影響を与えている．

サイバー攻撃の早期検知およびトレンド分析を目的として，警察庁や国内外のネットワーク事業者などがインターネット広域監視システムと呼ばれるシステムを稼働させている[1)~5)]．これらのシステムはインターネット上の複数の位置にセンサとしてネットワーク型侵入検知システム（NIDS）を設置する．そこから得られた大量のログデータを統計的に解析し，結果を視覚的に提示する．視覚化の手法は，攻撃を国別に表すものと攻撃の数を時系列グラフで表すものの 2 種類がある．しかしこれらは攻撃者の具体的な IP アドレスや攻撃の広まり具合，攻撃者と被害者との関係を把握することは困難である．このことがインターネット広域監視システムを利用しにくくする要因となっている．

本論文ではサイバー攻撃の効果的なモニタリングに適した視覚化フレームワームを提案する．特に我々はインターネットワームやネットワークスキャンなど自動化攻撃に着目し，我々のシステムで実際にとらえた攻撃をこのフレームワークに適用した．

次章ではインターネットワームの伝播アルゴリズムに着目することで広い範囲のネットワーク情報を効果的に視覚化する手法について議論する．3 章で我々が実装を行った広域ネットワーク監視システムについて述べる．4 章はシステムの実行例を示す．続いて 5 章で考察を行い，6 章でまとめる．

† 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
†† 慶應義塾大学大学院政策・メディア研究科
Graduate School of Media and Governance, Keio University

## 2. 広域ネットワーク視覚化手法の検討

### 2.1 インターネットワームの感染手法

現在インターネット上で大規模攻撃の主流となっているインターネットワーム（以下ワームと省略する）の伝播アルゴリズムについてはSymantecなどで詳細な動作アルゴリズムの解析が行われている[16]．それによるとワームは自身のプログラムを他の計算機に感染させるため，次のターゲットとなる計算機の調査を行う．ワームがターゲットとする計算機のIPアドレスは自分自身が持っているIPアドレスの値を変化させたものを用いる．ワームが用いるターゲットのIPアドレスの決定方法には大別して以下の2種類が存在する．

- ランダムスキャン：自身のIPアドレスの32 bit値をランダムに変化させ，計算機のスキャンを行う．
- ローカルスキャン：IPアドレスの上位8 bitもしくは上位16 bitを固定し，以下をランダムに変化させスキャンを行う．

ランダムスキャンの例にはCodeRedやSQL Slammerなどがある．これは32 bitのIPアドレス空間をすべてスキャンするため非効率的である．また近年発生したWelchia[18]，Sasser.Dワームなどはランダムスキャンとローカルスキャンを併用するため，より効率的である．

### 2.2 視覚化手法

現在のサイバー攻撃の多くは計算機に付加されているIPアドレスを元にしたものである．仮に自分の組織と地理的に近い場所でコンピュータワームの被害が発生したとしても，それがすぐに自分に感染するとは限らない．広域監視での視覚化において重要な点は攻撃者と自分との地理的な関連ではなく，IPアドレスの近接関係である，

さらに広域監視の観点から見た場合，IPアドレスの位置関係を視覚化するとともに，広い範囲にわたるIPアドレス空間の状況を俯瞰できることが求められる．ネットワーク空間を俯瞰することで，自己の組織の周囲ではどのような被害が発生しているかの把握や，自己の組織への被害の予測を立てることが可能になると考えられるためである．そのためにはIP空間を経済的に視覚化することが求められるが，ネットワーク情報の視覚化には物理的な表示領域の制限を考慮に入れる必要がある．現在主に利用されているIPv4空間を例にあげると，32 bitのIPアドレス空間を視覚化するためには，$2^{32}$個の要素が必要である．1要素を計算機画面表示の最小単位である1ピクセルで表示すると$2^{32}$個のピクセル数に相当する．最も経済的に2次元平面の正方形で配置すると65,536 × 65,536個の解像度が必要になる．これは現在の計算機の標準的な解像度と比較すると表示が困難な大きさになる．

現在インターネット空間を利用している組織の大半はIPアドレスの上位8 bitあるいは16 bitの値で区別できる場合が多い．これはネットワーククラスBやネットワーククラスCといった，旧来の組織へのIPアドレスの割り当て方法に起因している．ただしこの方法ですべての組織が区別できるわけではなく，例外も存在する．しかし歴史的な事情により事実上多くの組織を判別できることから，本論文ではIPアドレスの上位16 bitの空間が特定の組織を示すものと見なし，以下これをサイトと呼ぶ．

視覚化手法を検討するにあたり，先に述べた近年のサイバー攻撃の主流となっているワームの感染アルゴリズムを考えてみる．WelchiaやSasser.Dといった最近の大規模ワームは次の感染ターゲットを決定する際にローカルスキャンを用いる．ローカルスキャンにかかる時間はきわめて短時間である．これはあるIPアドレス（a.b.c.d）からの攻撃が観測された場合，そのIPアドレスを含む下16 bit（a.b.(0-255).(0-255)）の計算機空間ではすでに感染が蔓延している可能性が高いことを示す．したがって広域監視の立場から考えた場合，攻撃者のIPアドレスすべてを視覚化する必要はなく，主な攻撃先を代表している上位16 bitが分かれば十分である．逆にあるサイト内部の感染の程度を知るためには，下位16 bitが視覚化されていればよい．これは多くの組織において下位16 bitの空間を，組織内部に配置する計算機に割り当てていることが多いためである．

### 2.3 IPアドレスのマトリクス表示

以上の考察をもとに，我々はIPアドレスのマトリクス表示を採用した．**図1**にその概念図を示す．IPマトリクスはA.B.C.Dとして表されるIPアドレスの第1オクテット（A）を縦軸に，第2オクテット（B）を横軸に表した2次元マトリクス表示である．同様に下位16 bitについても第3オクテット（C）を縦軸に，第4オクテット（D）を横軸にとる．前者は各サイトごとの情報を表示するために使用する．後者はサイト内の個々のアドレスごとの情報を表示するために使用する．例として図1のようにIPアドレス130.152.X.Xのサイトから Welchia ワームの発生が観測された場合，Welchia ワームはローカルスキャンの終了後第2オクテットの値をシフトして次のローカルスキャンを開始する．そのため上位IPアドレスが130.153.X.X

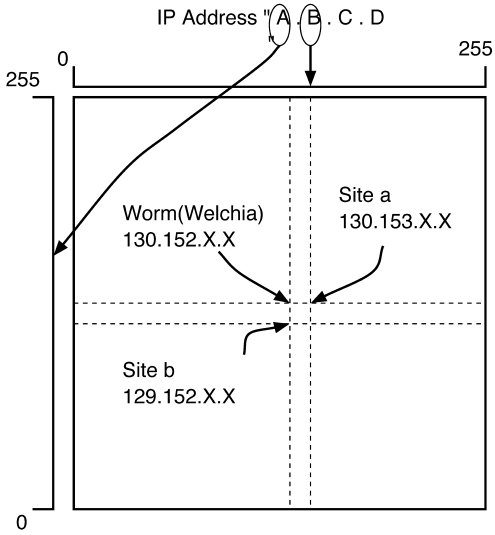



**図 1** IP アドレスのマトリクス表示
Fig. 1 A matrix layout of IP Address.

のサイトに所属するサイト a に含まれる計算機はその後ワームの被害を受ける可能性が高い．それに対して 129.152.X.X のサイト b に所属するユーザはこの Welchia ワームがローカルスキャンを行う経路にないため，サイト a と比較するとワームの対処を行う猶予があると考えられる．このようにマトリクス表示は IP アドレスの近接関係を直感的に判断することが可能である．

## 3. IP Matrix：広域ネットワーク監視のための視覚化フレームワーク

既存のインターネット観測システムの課題と広域監視の観点から見たネットワーク情報の視覚化を行う際の考察をもとに，我々は広域ネットワーク監視のための視覚化フレームワーク “IP Matrix” を構築した．

### 3.1 システム構成

我々の研究グループでは，2003 年 5 月よりインターネット広域観測システムを立ち上げ，インターネット上で発生する攻撃状況の調査を行っている．観測点の内訳は大学ネットワークが 3 拠点，企業ネットワークが 2 拠点である．監視を行う計算機の OS には RedHat Linux9.0，MacOS 10.2，組み込み用 Linux を使用している．

各観測点の計算機には攻撃情報を取得するためにネットワーク型侵入検知システムとして Snort [17] バージョン 2.1 を使用し，すべての不正アクセスを検知するため，ルールセットをすべて有効な設定にしている．各観測点からは 1 時間ごとにログサーバへ自動的に転送する．これは各観測点の計算機上で cron デーモンを

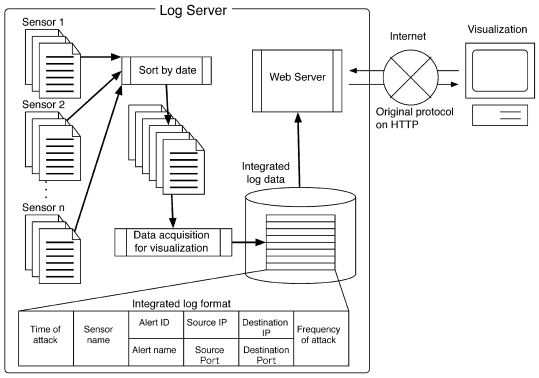



**図 2** ログサーバの詳細
Fig. 2 Log server.

稼働させ，ssh，rsync コマンドにより実現している．

ログサーバでは各観測点から収集したデータを統合する処理を行う．**図 2** にログサーバの詳細を示す．各観測点から得られた Snort 警告情報を時間順に並べ替えて統合する．その後視覚化に使用する情報を抽出し統合ログデータとして格納する．情報は，1) 警告の発生日時，2) 観測を行ったセンサの名前，3) Snort ルールセットで定義された警告 ID，4) 警告名，5) 送信元 IP アドレス．6) 送信元ポート番号，7) 送信先 IP アドレス，8) 送信先ポート番号，9) 同じ警告が連続して発生した回数である．

視覚化システムは，ログサーバ内のログ情報をネットワークを通じて取得する．データは既存の Web サーバ内に組み込まれたサーバプログラムを経由して通信を行う．システムで使用している Web サーバは Apache バージョン 2.0.40 である．通信の際のプロトコルは HTTP 上に独自に定義したプロトコルを用いている．そのためログ情報は企業内ネットワークなどファイアウォールなどを備えた環境でも取得することが可能である．

### 3.2 視覚化手法

ログサーバへ集められたログ情報をもとに，攻撃情報を統合して視覚化を行う．**図 3** に IP Matrix の画面を示す．本システムでは 2 つのマトリクスを用いて IP アドレス空間の上位 16 bit（以下インターネットレベルと呼ぶ）と下位 16 bit（以下ローカルレベルと呼ぶ）の状況を表示する．

本システムでは画面左側でインターネットレベル，画面右側でローカルレベルのネットワークの視覚化を行う．インターネットレベルでは攻撃元 IP アドレスの上位 16 bit を使用し 1 サイトを 1 ピクセルで表示を行う．ローカルレベルではセンサが置かれているネットワーク内の状況を表示する．本システムは単位時間

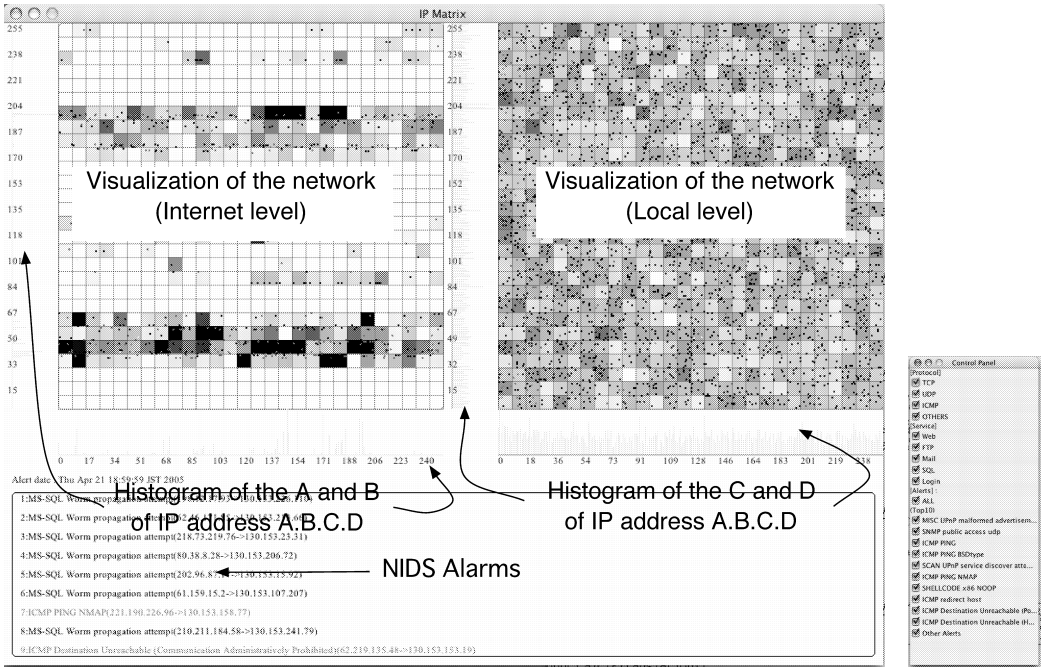



**図 3** IP Matrix
Fig. 3 IP Matrix.

ごとに定期的に警告情報を取得する．取得した情報はマトリクス上にそのサイトを点で表示を行う．点は攻撃に付加された ID 番号に応じて色分けして着色している．またマトリクスは一定の大きさで格子状の区画を設定し，その区画内で最も多かった攻撃の種別を格子の背景色とする．

2 つのマトリクスの左側と下側には，それぞれマトリクスの縦軸，横軸の値に対応した警告の出現ヒストグラムを描画している．これにより画面の点の密度などの量的な情報に隠れた警告量の特徴を示すことが可能である．また画面の下側には，最近発生した警告の詳細情報を記述している．

### 3.3 対話的機能

1 つ目はアニメーション表示である．本システムは画面上に一度にデータを表示するタイムスパンを指定し，それらを連続してアニメーション表示することが可能である．タイムスパンの種類は期間の長い順に 1 カ月，1 日，1 時間の 3 種類である．これは攻撃の分析をより細かく行うことを目的としている．たとえば 1 カ月分を表示することは，あるワームの発生から死滅までの長期的なワームの生存サイクルの分析に有効である．また 1 日分を表示することで，ワームのスキャン範囲や移動方向の検証ができると考えられる．さらに 1 時間分の警告を表示することで，より実時間に近い攻撃情報の把握が可能であると考えられる．

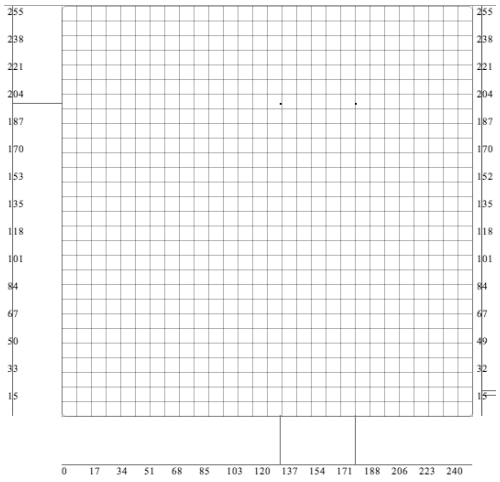
2 つ目はマウスとキーボードによる操作機能である．本システムではマウス操作による警告情報の詳細表示を行うことが可能である．マウスのシングルクリックによって単一の警告情報の表示を行い，ラバーバンド操作による選択で複数の警告の表示を行う．またコントロールパネルによって視覚化を行う属性の選択や表示のフィルタリングを行う．本システムでは最近多く発生した上位 10 件の警告名の集計を行っている．それらはコントロールパネルに反映され，上位 10 件の警告それぞれについて画面への表示あるいは非表示の選択を行うことが可能である．

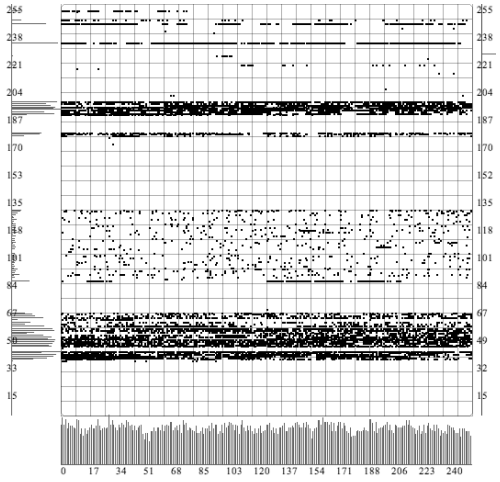
## 4. システムの実行例

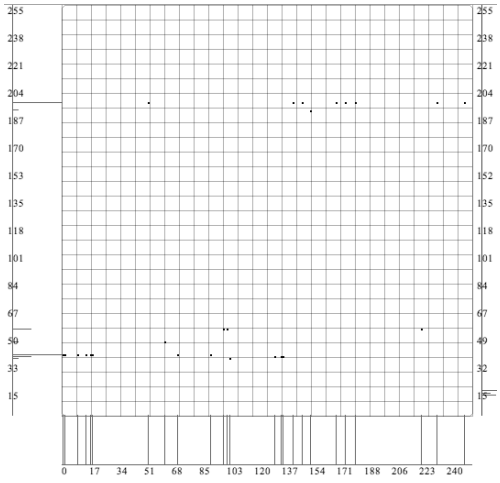
### 4.1 視覚化例：Welchia

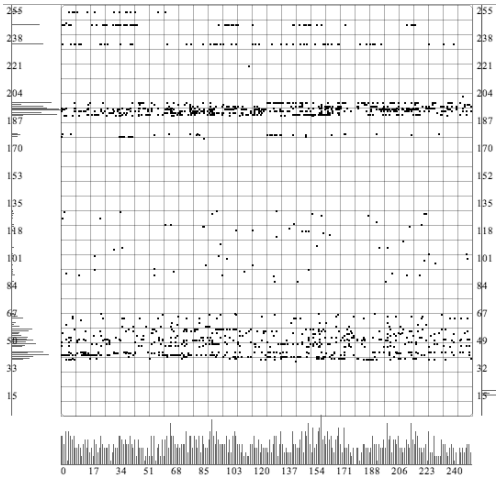
**図 4** は 2003 年 8 月 17 日に発生した Welchia ワームの感染状況である．本例はあらかじめ観測環境で取得したネットワークパケットを事後検証し視覚化したものである．

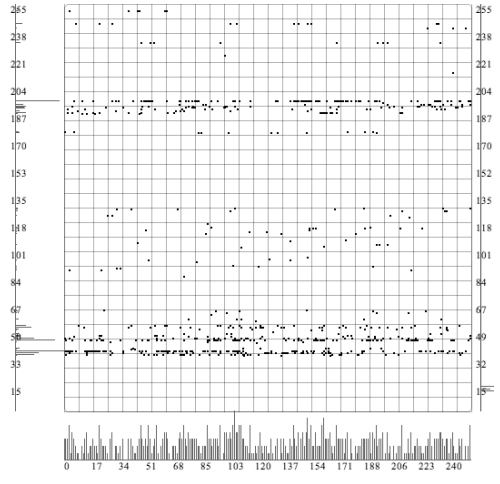
それぞれのマトリクスの右上に，1 日における観測された数を記入している．Symantec などのウイルスベンダの報告ではワームの発生日が 18 日となっているが，図 4 のとおり我々の観測データでは 8 月 17 日から警告が発生していた．Welchia は発生が観測されてからから 3 日目（8 月 19 日）ですでに世界中のサイトで感染が急速に広まったことが分かる．



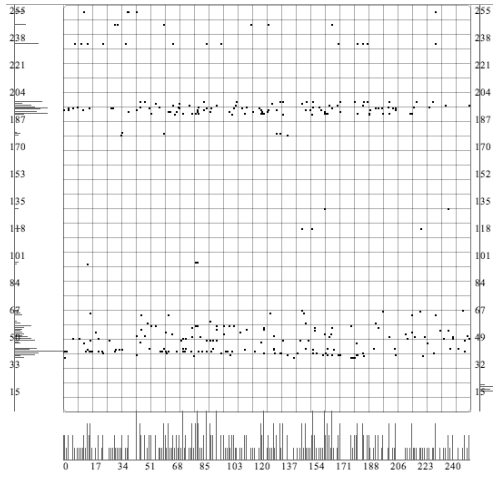




**図 4** Welchia ワームの拡散状況
Fig. 4 Infection of Welchia.

本提案手法で使用した NIDS（Snort）は不正アクセスのパターンデータベースを用いた不正検知種別のシステムである．そのため設計上は既知の不正アクセスの検知を想定しているが，Snort のパターンデータベースは多様かつ大量に提供されている点と，未発見の新種の不正アクセスに関しても侵入手法は過去の事例を参考にしている場合がほとんどであるため，Snort によって未知と考えられる不正アクセスをとらえることが可能な場合がある．

本例で示した Welchia ワームは，Snort では “ICMP PING CyberKit 2.2 Windows” という名称の別の不正アクセスのパターンとして検出された．我々が設置している複数の観測環境では，従来この警告はまったく発生しておらず，8 月 17 日よりはじめて観測されるようになった．このことから Welchia ワームの分析では，8 月 17 日に発生した “ICMP PING CyberKit 2.2 Windows” 不正アクセスと公式発表である 8 月 18 日以降に発生した同名称の不正アクセスとは同じものである可能性が高いと考え，8 月 17 日より警告が発生していたと記述している．

Welchia の特徴に，2004 年 1 月 1 日をもって自己消滅するようプログラムされている点がある．図 4 の 2003 年 12 月から 2004 年 6 月までを見ると，Welchia が月を追って徐々に減少している様子が分かる．実際には 2004 年 1 月 1 日にすべて消滅することはなく，現在も一定数生存している．この理由として，コンピュータに感染したワームは再起動されるまで消滅せず，連続稼働している計算機がこれらの発生源に該当していることや，OS にセキュリティパッチを当てたもののワーム本体の駆除までは行わず計算機内にプログラムがとどまり続けていることに気がついていないユーザが他数存在することなどが考えられる．

また Welchia ワームのランダムスキャンでの IP アドレスの決定アルゴリズムの 1 つに，辞書を用いたアドレス決定方法がある．Welchia は 61，202，203，210，211，218，219，220 の値を辞書として持ち，最初の 8 bit にこれらのいずれかを使用する手法をとる場合がある．これに第 2 オクテットのシフトを併用する．たとえばワームの感染元が A.B.C.D で表される IP アドレスのとき，A.(B+1).C.D，A.(B+2).C.D，A.(B+3).C.D とアドレスを変化させ，その後ローカルスキャンを行うものである．図 4 ではターゲットの IP アドレスの決定に辞書を用いる効果が点の集中度で確認できる．本システムでは点が集中している箇所の位置を見ることで，ワームの空間的な分布を効果的にとらえることが可能である．

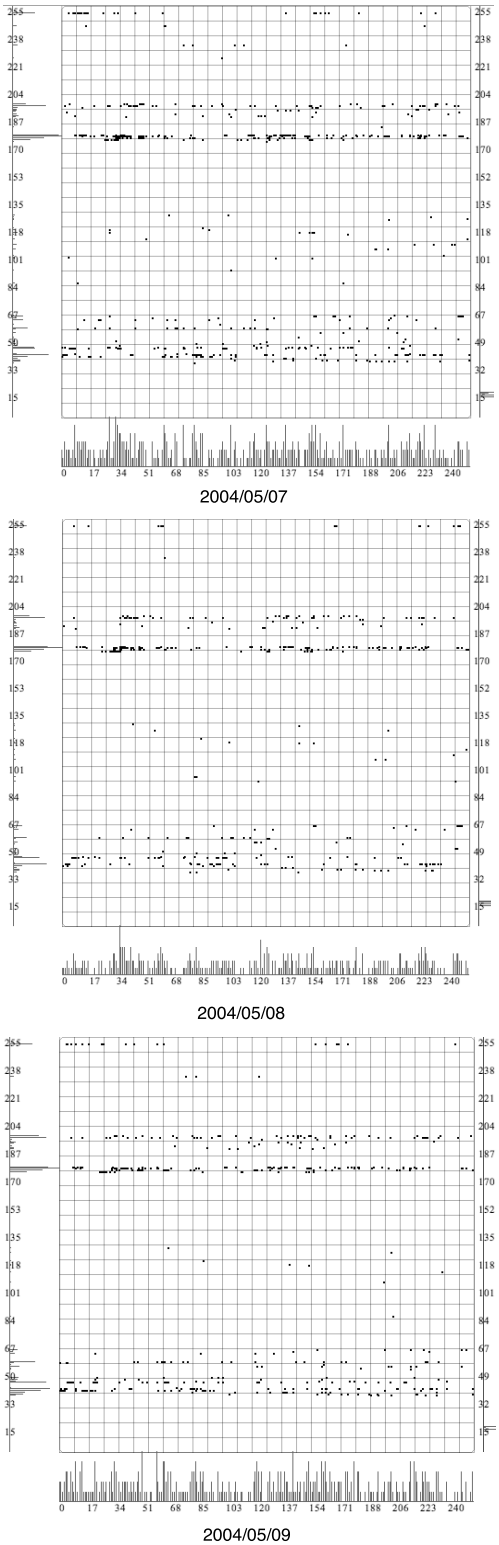



**図 5** Sasser ワームの拡散状況
Fig. 5 Infection of Sasser.D.

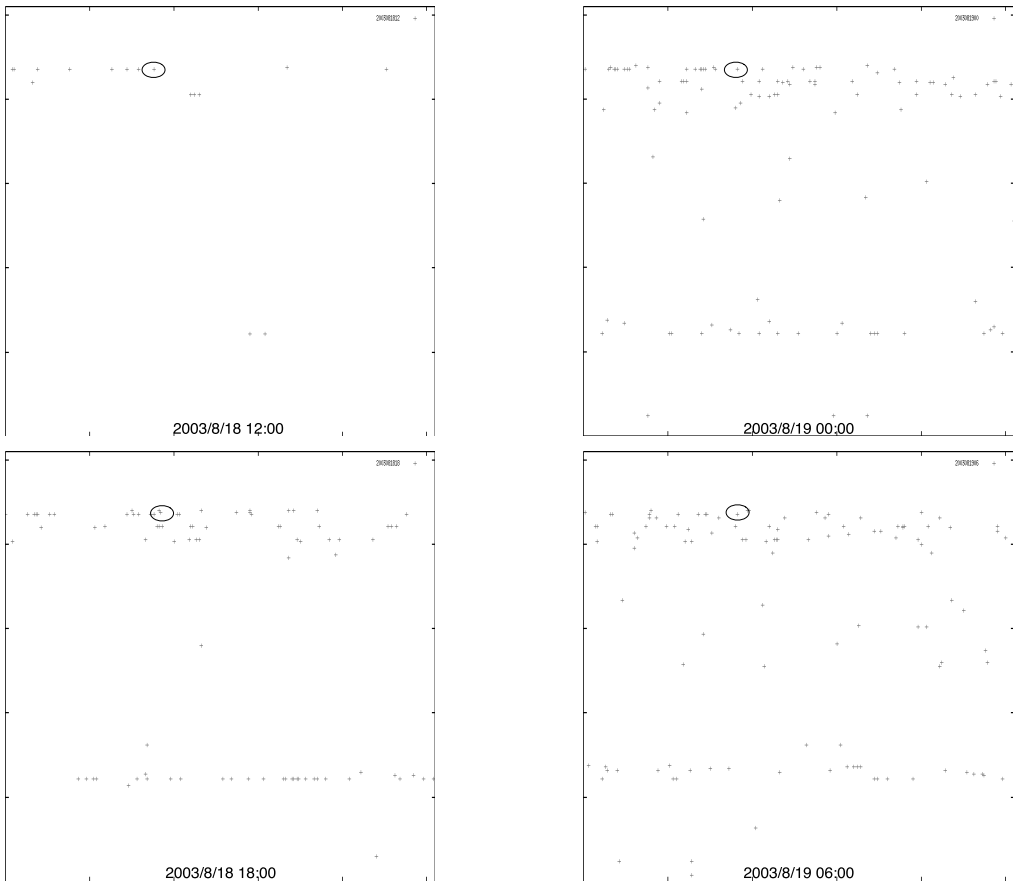



**図 6** アニメーション効果を利用した例
Fig. 6 An example using animation effects.

### 4.2 視覚化例：Sasser.D

**図 5** に 2004 年 5 月 3 日に発生した Sasser.D ワームの感染状況を示す．それぞれのマトリクスの右上に，観測された数を記入している．我々の観測点では 5 月 7 日から発生が観測された．その後数日にわたり感染を広げていくが，Sasser.D は Welchia と類似した感染手法であるにもかかわらず，感染規模が小さいものであった．この理由の 1 つとしては，前年の Welchia の大流行を契機にセキュリティ対策を施すシステムが増えたためであると予想される．また攻撃に使用されているポート番号の違いも原因の 1 つであると考えられる．Welchia が突いたポートは 135 番ポートである．これは Windows 系 OS で機器間の連係に頻繁に使用されるポートで，一般的な設定ではつねに待ち受けされている．これに対して，Sasser が用いた 445 番ポートはローカルネットワーク上でのファイル共有に使用されるポートであるため，直接インターネット上に接続されているサーバなどの計算機では使用する頻度が低いことが Welchia との感染度合いの差に現れたと考えられる．

### 4.3 継続して発生しているホストの検出

次に本システムのアニメーション効果を使用した分析の例を示す．**図 6** はある観測点における Welchia ワームの発生時からの様子を 6 時間ごとに表示した図である．本システム上で情報の閲覧を行っていたところ，特定の場所からのアクセスが継続して現れ続けていることが分かった．これは特定のアドレスから観測点への継続したアクセスが発生していることを示す．本手法を用いることで，このような注意を要すると考えられる IP アドレスの検出を容易にする．

## 5. 考　　察

### 5.1 システムの利点

我々が提案する視覚化手法の利点を述べる．1 つめは IP アドレスのマトリクス表示により IP アドレスの近接関係を自然に表現可能な点である．現在主流となっている大規模攻撃の基礎は IP アドレスである．IP アドレスから見た攻撃者と自分との論理的な位置関係

を把握することで，防御の対策を事前にとることができると考えられる．応用例として，広域監視の課題である攻撃予知への可能性がある．NIDS による監視は既知の攻撃を検知可能である．それに加えて現在のインターネット定点観測で用いられる時間変化のグラフを見ることで攻撃の流行分析が可能になっている．さらに我々が提案する視覚化手法による攻撃の空間的な関係を把握することで，従来よりもより具体的な攻撃の予知が可能になると考えられる．たとえば Welchia ワームなどはローカルスキャンと特定位置のアドレスシフトを組み合わせる．そのため画面では直線の形状を表す．サイトの管理者は自己の組織がその線に乗っているかを確認することで，攻撃が届く見通しを立てることが可能であると考えられる．

2 つめは同様にマトリクス表示を用いたことにより，膨大な IP アドレス空間を経済的に表示することが可能になった点である．IP アドレスの上位 16 bit のマトリクス表示と下位 16 bit のマトリクス表示を並列に表示することで，サイトレベルとローカルレベルの状況を制限のある計算機の画面上で経済的に視覚化することができた．

### 5.2 システムの問題点

本システムの問題点として未使用のアドレス空間の存在がある．インターネット上では実際に使用されていない IP アドレスが他数存在しており，本システムの視覚化画面でも使用されていない領域が空白となっている．この領域は画面の使用効率から考えた場合無駄な領域になる．2 次元平面をより経済的に使用するためには，なんらかの工夫が必要である．しかし実際には IP アドレスの詐称など，本来使用されていないアドレス空間を用いる攻撃も存在するため，この領域を不用意に削ることはできない．また空白を含む $256 \times 256$ の正方形はサイトの位置関係を把握する面からみると直感的である．

本システムのもう 1 つの課題は他の不正アクセス手法への対応についてである．例としてメールを介したワームがある．これらはメールサーバを経由して計算機へ感染後，計算機内のアドレス帳やハードディスク内の文書を検索して次のターゲットを決定する．この場合次のターゲットの基準はメールアドレスとなり，IP アドレスの情報は関係がなくなるため，攻撃の予知という観点から見ると本システムでは効果がなくなると考えられる．

### 5.3 関 連 研 究

#### 5.3.1 ネットワーク情報の視覚化

MRTG [9] と RRDTOOL [10] は計算機やネットワーク機器の状態を観測するためのツールである．単一計算機上のリソース状況の表示やルータなどのネットワーク機器の負荷状態などを時系列グラフとして表示する．これらのシステムはネットワーク上の個々の計算機の状態を知るために有効な手段であるが，内部ネットワーク全体の計算機の状況を把握することは困難である．

カルフォルニア大学サンディエゴ校の Cooperative Association for Internet Data Analysis（CAIDA）[6] では，ネットワークトラフィックや計算機の接続情報などを収集し，それらを視覚化するツールを多数公開している．Skitter [7] は円形または球形にグラフを配置し，インターネット上のネットワークトポロジやパケットの到達時間を視覚化するシステムである．また IPv4 でネットワークの割当てに用いられるクラス別の計算機の密集度や利用されている国情報などを視覚化したものがある [8]．Skitter では，Hyperbolic Tree や無向グラフの構造を採用している．これらは膨大な IP 空間すべてを限られた画面領域で視覚化する方法としては優れているが，インターネット監視の側面から見た場合，これらの視覚化では各要素の位置関係が壊れているため，即座に IP アドレスの近接関係を認識することは難しい．これらの視覚化システムは “Focus + Context” 手法を用いて内部情報を拡大する方法も備えているが，これらの手法は縮小されている特定の情報を見ようとする際にその周辺が縮小され情報が隠蔽されてしまう．そのため広域ネットワーク監視の用途にはそぐわない．

#### 5.3.2 セキュリティ情報の視覚化

Security Incident Fusion Tools（SIFT）ではセキュリティ情報の視覚化を行っている．NVisionIP 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，視覚化を行うシステムである [13]．VisFlowConnect は内部ネットワークと外部ネットワーク間で発生するトラフィック情報を線とアニメーションによる視覚化を行う．

Passive Visual Fingerprinting [14] と Spinning Cube [15] はともにセキュリティ情報を視覚化するために提案されたシステムである．Passive Visual Fingerprinting はネットワーク攻撃の特徴を 2 次元画面に点と線で視覚化し，Spinning Cube は立方体上にネットワーク情報とポート番号をマッピングしている．画面は動的に変化するため，不正アクセスの状況を視覚的にとらえることが可能である．これらのシステムについては，主に中規模なローカルサイトのネットワー

ク状況の視覚化を対象としている．計算機が増加すると画面が線画で覆われるため判別が困難になり，インターネットなどの大規模ネットワークの監視には適していない．

## 6. おわりに

本論文では既存のインターネット定点観測システムおよびその他のネットワーク視覚化システムの問題点について考察を行った．その結果，IP アドレスの近接関係の視覚化を行い，かつ IP アドレス空間の経済的な視覚化を行う必要があるという結論を得た．

そこで広域ネットワーク監視のための視覚化手法として，IP アドレスのマトリクス表示を用いたシステム “IP Matrix” の提案と実装を行った．IP Matrix は IP アドレスを 2 次元平面にマトリクス表示することにより，IP アドレス空間の経済的な表示を実現している．また攻撃者とシステムの利用者との IP アドレスから見た近接性を自然に表示することが可能である．

今後は本研究で提案したシステム運用の継続による不正アクセスの検知，視覚的な手法から見たサイバー攻撃の特徴抽出を行っていく予定である．

## 参考文献


1) 警察庁セキュリティポータルサイト@Police. http://www.cyberpolice.go.jp/detect/observation.html
2) JPCERT/CC Internet Scan Data Acquisition System (ISDAS). http://www.jpcert.or.jp/isdas/
3) IPA インターネット定点観測システムについて（プレス発表）．http://www.ipa.go.jp/about/press/20040511.html
4) DShield. http://www.dshield.org/
5) SANS Internet Storm Center. http://www.incidents.org/
6) Cooperative Association for Internet Data Analysis (CAIDA). http://www.caida.org/
7) AS Internet graph. http://www.caida.org/analysis/topology/as_core_network/AS_Network.xml
8) IP v4 Address Space Utilization. http://www.caida.org/outreach/resources/learn/ipv4space/
9) MRTG: The Multi Router Traffic Grapher. http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
10) RRDtool. http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
11) Security Incident Fusion Tools (SIFT). http://www.ncassr.org/projects/sift/
12) Lakkaraju, K., Bearavolu, R. and Yurcik, W.: NVisionIP — A Traffic Visualization Tool for Security Analysis of Large and Complex Networks, *International Multiconference on Measurement, Modelling, and Evaluation of Computer-Communications Systems* (*Performance TOOLS*) (2003).
13) Yin, X., Yurcik, W., Li, Y., Lakkaraju, K. and Abad, C.: VisFlowConnect: Providing Security Situational Awareness by Visualizing Network Traffic Flows, *Workshop on Information Assurance* (*WIA04*) *held in conjunction with the 23rd IEEE International Performance Computing and Communications Conference* (*IPCCC 2004*) (2004).
14) Conti, G. and Abdullah, K.: Passive Visual Fingerprinting of Network Attack Tools, *Conference on Computer and Communications Security* (*CCS2004*), *Proc. 2004 ACM workshop on Visualization and data mining for computer security* (*VizSEC'04*), pp.45–54 (2004).
15) Lau, S.: The Spinning Cube of Potential Doom, *Comm. ACM*, Vol.47, Issue 6, pp.25–26 (2004).
16) Symantec Corp. http://www.symantec.com/region/jp/
17) Snort NIDS. http://www.snort.org
18) Welchia ワーム情報, トレンドマイクロ株式会社 (2003). http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_NACHI.A
19) 小泉　芳，小池英樹，高田哲司，安村通晃，石井威望：情報エントロピーを用いたネットワーク侵入検知システム解析手法の提案，コンピュータセキュリティシンポジウム（CSS2003），情報処理学会 (2003).
20) 小泉　芳，小池英樹，安村通晃：サイトレベルプロファイリングを用いたワームの感染規模推定方法の提案，情報処理学会研究報告，コンピュータセキュリティ 2004-CSEC-26, 情報処理学会 (2004).
21) 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，日本ソフトウェア科学会第 21 回大会（2004 年度）論文集，日本ソフトウェア科学会 (2004).
22) 大野一広，小池英樹：ワームの伝播アルゴリズムを考慮した広域ネットワーク視覚化システムの提案，コンピュータセキュリティシンポジウム（CSS2003），情報処理学会 (2004).


(平成 17 年 7 月 8 日受付)
(平成 18 年 2 月 1 日採録)

**大野　一広**（学生会員）

2003 年電気通信大学大学院情報システム学研究科博士前期課程修了．現在，同大学院情報システム学研究科博士後期課程在学中．情報視覚化，不正侵入検知に興味を持つ．

**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 年同大学院情報システム学研究科助教授．現在に至る．1994〜1996 年，1997 年 U.C.Berkeley 客員研究員．2003 年 U.Sydney 客員研究員．情報視覚化の研究に従事．特に視覚化へのフラクタルの応用，Perceptual User Interface，情報セキュリティへの視覚化の応用に興味を持つ．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．

**小泉　　芳**（正会員）

2005 年慶應義塾大学大学院政策・メディア研究科修士課程修了．政策・メディア修士．現在，防衛庁陸上自衛隊通信団勤務．暗号，コンピュータウイルスに興味を持つ．