SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

自己組織化マップを用いたネットワークインシデント分析の研究
A Study on Network Incident Analysis Using Self-Organizing Maps

大河内 一弥[*†] 力武 健次[*] 中尾 康二[*‡]
Kazuya Ohkouchi[*†] Kenji Rikitake[*] Koji Nakao[*‡]

あらまし 本稿ではサーバのログなどに記録されるインシデント情報に SOM（自己組織化マップ）を適用し，特徴的な挙動を示すホストのセグメント（集合）を抽出する手法について検討した結果を報告する．具体的には，パケットキャプチャのログを分析対象とし，前処理としてこのデータを一定時間単位でホストごとに集約した上でこれを入力として SOM のアルゴリズムを適用した．その際，入力順序に因らず同一の結果が得るため，主成分分析を用いて初期化を行い，一括学習型のアルゴリズムを用いた．また，出力された SOM から，特徴的な振る舞いを示すホストのセグメントを抽出し追跡するための機能を追加した．本稿ではこの手法を実際の DDoS 攻撃データの解析に適用し，その結果と今後の課題について考察する．

キーワード ネットワークセキュリティ，インシデント分析，パケットキャプチャログ，プロファイリング，データマイニング，自己組織化マップ，視覚化

1 はじめに

ブロードバンドインターネット環境の普及に伴って，情報通信基盤がますます重要な社会インフラとなる一方，ワームやウィルスなどによるネットワークへの被害の拡散はより広範囲，かつ急速なものとなっている．

このため，ネットワークにおけるリスク状況を迅速に把握し，的確な対策に基づくリスク回避やリスクの低減を行う技術の開発が期待されており，国内外において JPCERT/CC[1]，@police[2]，DShield.org[3] などの団体や，Internet Motion Sensor[4] などのシステムにより，ネットワーク上のインシデントの監視が行われるようになってきている．

われわれのグループにおいても，インターネットリスク分析モデルに関する研究を行っており[5]～[11]，具体的なシステム化，国内インターネットプロバイダとの連携などについて検討を続けている．インターネットリスク分析モデルでは，従来の取り組みに加えて以下のような点を達成すべく検討を行っている．

(1) 単に測定したインシデントの列挙にとどまるのみではなく，異なるプロトコルで起こるイベントの相関がどのような意味を持つかについて統計解析やデータマイニングの手法により解釈を見出す．

(2) 複数のネットワーク間で同時多発的に起こるイベントについて，偶然の一致なのか，あるいは組織的に意図されたものなのかを区別する．

(3) 過去の脆弱性等の情報との関連性を分析し，イベントが全く新しい脆弱性を示しているのか，あるいは過去の脆弱性の変種や亜種であるのかに関する判断する．

(2)については，他のネットワークプロバイダや企業，学術機関との連携による広域的なデータの収集分析，(3)についてはデータの時系列変化に着目した詳細な分析など，それぞれ検討を進めている[9][10][11]．これらは本稿の範囲外であり，詳細は割愛する．

本報告では，この中の特に(1)に関係する分析として，データマイニングの一手法として知られている，自己組織化マップ(Self-Organizing Map; 以下 SOM)[12][13]をインシデント分析に適用することに関する研究の結果を報告する．

本研究では，単位時間あたりのインシデント情報をホスト(IP アドレス)ごとに集約した特徴ベクトルを作成し(このプロセスを報告者は「プロファイリング」と呼んでいる)，特徴ベクトル間の距離関数が小さいホスト同士が近くに集まるように学習が行われることが特徴である SOM のアルゴリズムを適用した．

本研究の目的は，SOM の出力であるマップから，特

* 独立行政法人 情報通信研究機構 セキュリティ高度化グループ
〒184-8795 東京都小金井市貫井北町 4-2-1
Security Advancement Group, National Institute of Information and Communications Technology, 4-2-1, Nukui-Kitamachi, Koganei City, Tokyo, 184-8795, Japan

† 株式会社日立製作所 システム開発研究所
Systems Development Laboratory, Hitachi Ltd.

‡ KDDI 株式会社 情報セキュリティ部
Information Security Department, KDDI Corporation

表 1　プロファイリング項目の一例

(1) データセット A

#	属性項目名	説明
1	IP_address	IP アドレス
2	incoming_packet	上り／下りのパケット数，ペイロード長の合計
3	outgoing_packet	
4	incoming_payload	
5	outgoing_payload	
6	TCP	プロトコルごとのパケット数
7	UDP	
8	ICMP	
9	dest_port_135	目的ポートごとのパケット数
10	dest_port_445	
11	dest_port_1434	
12	packet_size_16	パケットサイズ別のパケット数
13	packet_size_128	
14	packet_size_1024	
15	packet_size_over1024	
16	ICMP_large_packet	巨大 ICMP パケット

(2) データセット B

#	属性項目名	説明
1	IP_address	IP アドレス
2	incoming_packet	上り／下りのパケット数，ペイロード長の合計
3	outgoing_packet	
4	incoming_payload	
5	outgoing_payload	
6	TCP	プロトコルごとのパケット数
7	UDP	
8	ICMP	
9	HTTP_GET_TOP_10	HTTP メソッドごとのパケット数
10	HTTP_GET_TOP_11	
11	HTTP_POST_TOP_10	
12	HTTP_POST_TOP_11	
13	HTTP_POST_CGI_10	
14	HTTP_POST_CGI_11	

徴的な挙動をするホストの集合(クラスタ)を抽出し，ウィルスやワームの特性の把握，亜種の検出などに役立てることである．

以下，第 2 節では SOM の入力となるデータを作成するための前処理について述べる．第 3 節では，本報告で用いた SOM のアルゴリズムについて解説する．第 4 節では，本研究に伴って開発した，SOM のツールについて解説する．第 5 節では，これらの手法を実際の DDoS データに適用した事例を報告する．

2　データの前処理

インターネットリスク分析モデルでは種々のオンライン，オフラインデータソースよりデータを収集するが，一般にこれらのデータはデータ量，データ形式の点で，そのまま分析に用いるには適していない．このため，収集されたデータは前処理において，データ量の削減，およびデータに内在する特徴の抽出を行うことが必要になる．特にデータの特徴をよくあらわすような特徴量の抽出は，後段の分析でよい結果を得るために非常に重要な作業である．ここではこの作業のことをプロファイリングと呼ぶことにする．

プロファイリングを行うにあたっては，まず基本となる単位レコードの定義を検討する必要がある．

本研究では，ホスト(IP アドレス)を単位レコードと定義してプロファイリングを行うことにした．これは，(a)インターネットリスク分析モデルにおいては，インシデントはホスト単位で検知される事，(b)分析後のアクションはホスト単位で取ることが可能であること，などの理由による．

次に，プロファイリングによって作成される属性項目であるが，属性項目の検討においては，分析対象のデータの特徴をできるだけ顕在化させるように，集約の粒度，項目を選ばなければならない．

本研究ではインシデント情報のログから以下の項目を属性項目としてホストごとのデータを作成した．属性項目の表を表 1 に示す．元データは (1) あるネットワークセグメントへのパケットをキャプチャしたログ，(2) あるサイトへの DDoS 攻撃のキャプチャログであり，このデータを，SOM を用いて実際に分析を行った結果と考察を第 5 節で述べている．

3　SOM のアルゴリズム

SOM は，入力データとなる各ベクトルを 2 次元の格子点に写像することにより，入力データに内在する特徴を直観的に把握することを支援するアルゴリズムである．ネットワークインシデント分析では，具体的には，類似した挙動を示すホスト同士でクラスタを構成し，あゆの発見や，ホストの挙動を分析する際にキーとなる属性項目を発見することが目的となる．

この写像は，類似する入力ベクトル同士が近くに配置されるように学習を行うことにより決定される．「入力ベクトルが類似している」とは，入力ベクトル間の距離関数を設定し，この関数の値が小さいことを意味する．

以下に本研究で用いた SOM のアルゴリズムを示す[14]．第 2 節の前処理で作成した属性値を要素とする各レコードを，SOM を学習するための入力ベクトルとして定義する．入力ベクトルの各値は，場合によっては正規化を行う．SOM アルゴリズムを，初期化フェイズと学習フェイズに分けて解説する．

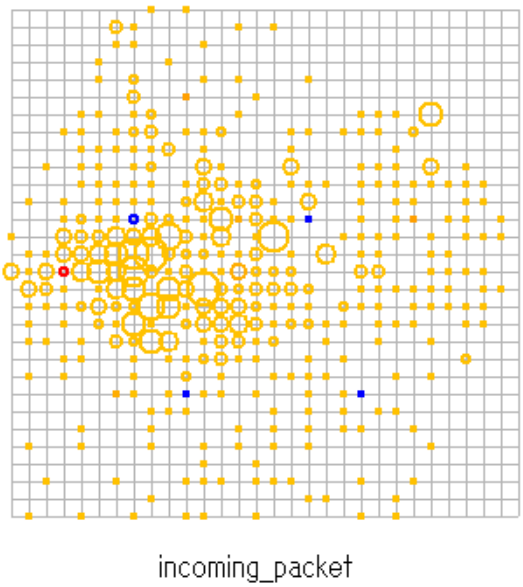


図 1　SOM の一例

初期化フェイズ

入力データを写像する 2 次元の格子点を用意する．X 軸方向の格子点の数を I，Y 軸方向の数 J とする．SOM では，各格子点に入力ベクトルと同じ次元を持つ参照ベクトルが割り当てられている．本手法ではこれらの参照ベクトルの初期化を，主成分分析を用いて行う．初期の SOM では参照ベクトルを乱数を用いて初期化する手法が提案されていたが，今回のような分析では結果の再現性が重要であるため，入力データによって一意に初期値が決まる手法が用いられる[14].

2 次元の格子点 (i, j) に対応する参照ベクトル $R_{i,j}$ の値を以下の式によって定義する．

$$R_{i,j} = x_{ave} + c_1\sigma_1 v_1\left(\frac{i - I/2}{I}\right) + c_2\sigma_2 v_2\left(\frac{j - J/2}{J}\right) \cdots\cdots\cdots (1)$$

ここで v_1，v_2 はそれぞれ第一，第二主成分ベクトル，x_{ave} は平均ベクトル，σ_1，σ_2 はこれらの 2 軸に対する入力ベクトル全体の標準偏差，c_1，c_2 は定数である．

学習フェイズ

学習フェイズでは，以下に述べる手順を一回の単位として，参照ベクトルの更新が行われる．

まず，全ての入力ベクトルについて，参照ベクトルとの距離関数を計算し，その値が最小となる参照ベクトルにその入力ベクトルを分類する．距離関数としては，本研究ではベクトル間のユークリッド距離を用いている．

次に，次式により，参照ベクトルの更新を行う．

$$R_{i,j}^{(t+1)} = R_{i,j}^{(t)} + \alpha^{(t)}\left(\frac{\sum_{x_k \in S_{i,j}} x_k}{N_{i,j}} - R_{i,j}^{(t)}\right) \cdots\cdots (2)$$

ここで，領域 $S_{i,j}$ は格子点 (i, j) の近傍となる格子点の集合を意味するものであり，$i - \beta^{(t)} \le i_N \le i + \beta^{(t)}$，$j - \beta^{(t)} \le j_N \le j + \beta^{(t)}$ を満たす格子点 (i_N, j_N) がこれに含まれる．$N_{i,j}$ は近傍 $S_{i,j}$ に含まれる入力ベクトルの数，t はこの更新の回数を示している．また α は参照ベクトルの更新量を決定する係数，β は近傍を決定する係数であり，以下の式の値を用いる．

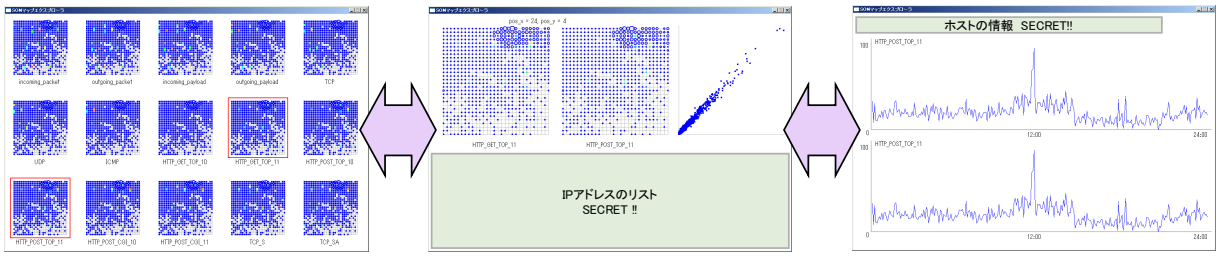
$$\alpha^{(t)} = \max\left(\alpha_{\min}, \alpha_{ini}(1 - t/T)\right) \cdots\cdots\cdots\cdots (3)$$

$$\beta^{(t)} = \max\left(\beta_{\min}, \beta_{ini} - t\right) \cdots\cdots\cdots\cdots\cdots (4)$$

ここで α_{ini} は学習係数の初期値，$\alpha_{\min}$ は学習係数の最小値，β_{ini} は近傍領域の初期値，$\beta_{\min}$ は近傍領域の最小値である．従って式(3)(4)は，学習が進むにつれて参照ベクトルの更新量が斬減し，また更新の対象となる近傍領域が狭まっていくことを示している．

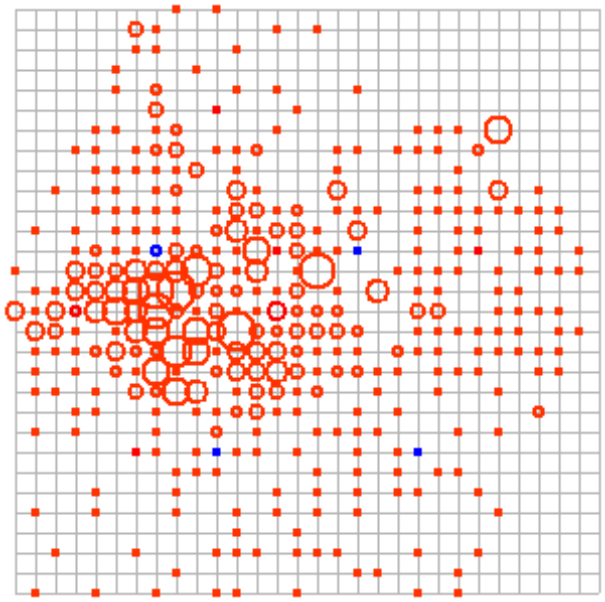
以上の更新を単位として，これを設定した回数 T 繰り返すことで学習を行う．

これによって得られた SOM の図の一例を図 1 に示す．通常 SOM では，入力ベクトルのある属性項目に着目し，これに対応する参照ベクトルの要素の値をサーモグラフィのように色付けすることで視覚化を行う．本研究では，これに加え，各格子点に写像されている入力データの数を半径として円を書くことにより，入力データがどのようなクラスタを構成しているかがより容易に把握できるように工夫した手法を開発した．

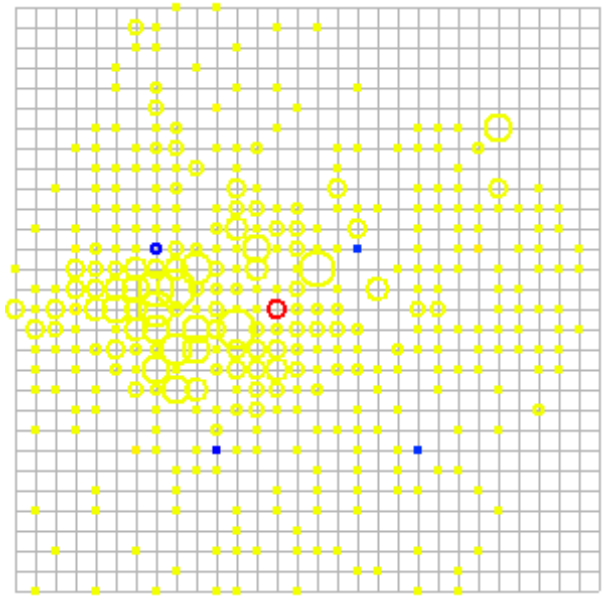


自己組織化マップの一覧表示　　詳細表示(特徴量ごとの散布図・相関、IPアドレスなど)　　ホストの挙動の詳細

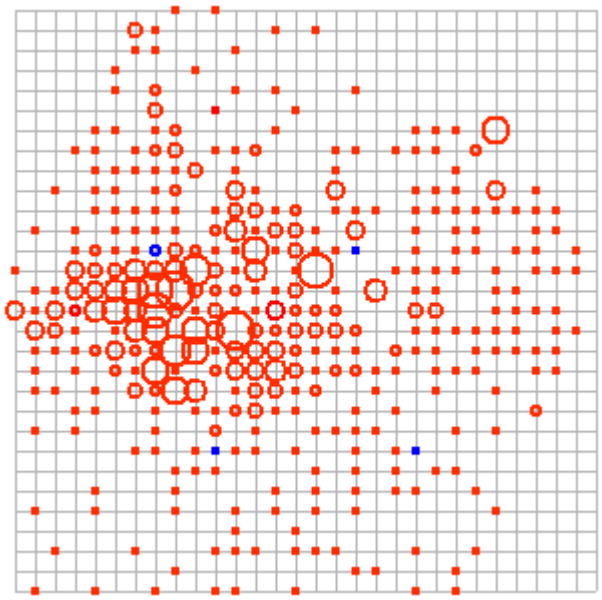
図 2　SOM 視覚化ツールの画面例



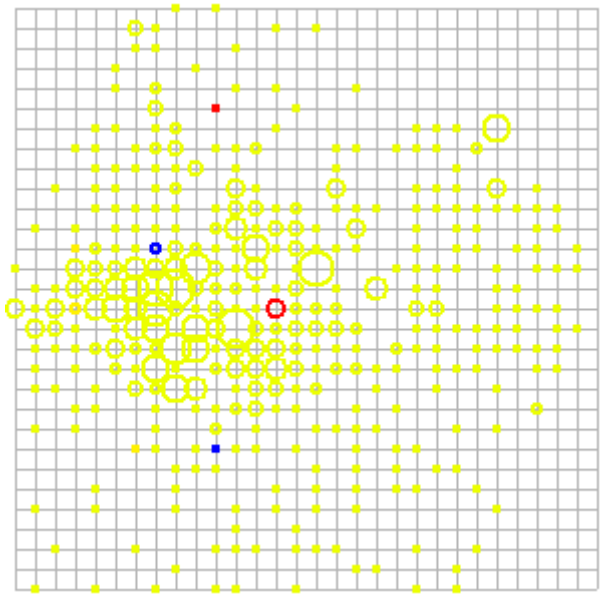
(a) dest_port_445



(c) ICMP



(b) dest_port_1434



(d) ICMP_laege_packet

図 3 自己組織化マップ実験結果 (データセット A)

4 SOM 視覚化ツール解説

本研究に伴って，第 3 節で述べたアルゴリズムと，結果の表示，SOM に写像された各ホストのアクセス履歴の表示を行うツールのプロトタイプの開発を行った．本節ではこのツールについて解説を行う．

視覚化ツールは，大きく 3 種類の画面で構成されている．各属性項目によって色付け，描画した SOM を一覧する画面，任意に選択した SOM を拡大して表示し，写像されているホストを選択する画面，前記の画面で選択したホストの過去のアクセス履歴を表示する画面である．

この視覚化ツールは，SOM の出力を分析し，特徴的なホストの挙動把握への解析を支援することを目的としている．

マップ一覧画面

マップ一覧画面では，各属性項目で色付けしたマップを一覧表示する画面である．この画面では，分析者が多数のマップを直観的に比較し，色付けの類似しているマップやアクセスの特徴が出ている点を検討する．分析者は詳細に調査したいマップを 2 つ選択し，マップ詳細画面で詳しく検討することができる．

マップ詳細画面

マップ詳細画面では，一覧画面で選択した 2 つの画面を拡大して比較する．マップのある格子点をクリックす

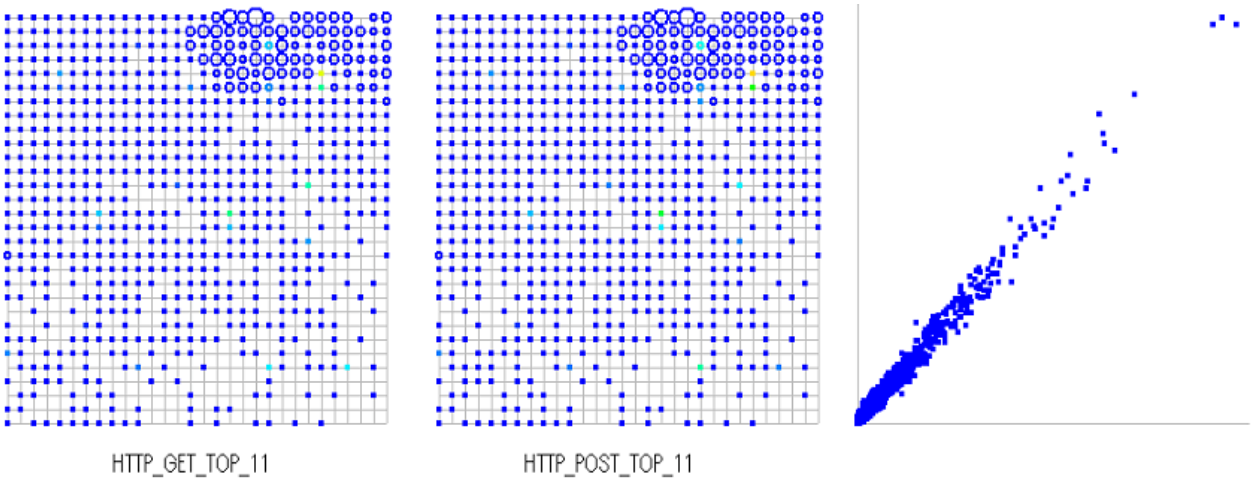


図 4 自己組織化マップ実験結果 (データセット B)

ると，その格子点に写像されているホストの IP アドレスが，画面下部に表示される．また画面右にはその 2 つの項目の散布図が表示され，2 つの項目間の相関を見ることができる．IP アドレスを選択すると次の画面で，ホストの過去のアクセス履歴を見ることができる．

ホスト挙動追跡画面

ホスト挙動追跡画面では，詳細画面で指定したホストについて，属性項目の値の遷移を過去にさかのぼって参照することができる．

このツールは現在，インシデント分析を支援するためのツールとして実験運用を行っている．

5 実験と考察

以上で解説した方法を DDoS データなど実際のデータに適用し，有効性の検証を行った．

データセット A — ネットワークセグメントの監視

データセット A はあるネットワークセグメントへのパケットをキャプチャしたものである．SOM の分析に使用した属性項目を 2 節の表 1 に示してある．また，SOM の出力結果の一部を図 3 に示す．図 3 の(a)(b)のマップは，非常に良く似ているが，445 番，1434 番のポートへのパケット数に着目して描画した別のマップである．これは，これらのポートへのアクセス行動が類似していることを示している．

出力結果のマップの分析，およびこれをきっかけにした詳細分析を行うことにより，以下の知見が得られた

- 445 番ポート, 1434 番ポートには一様に同じ程度のパケットが飛んできている．(マップの(a)(b)) これは Sasser のパケットである．
- これとは別に，ICMP のパケットを送ってきている少数のホストが存在する．(マップ(c))
- ICMP にパケットを送ってくるホストの中には，非常に大きいサイズのパケットを送ってくるものがある．(マップ(c)(d))

このデータセットの記録されたパケットは，ほとんどが Sassor のパケットであったが，SOM を利用することによりその中に少数存在する別の攻撃行動を捕らえることができた．

データセット B — DDoS 攻撃データ

データセット B はあるサイトへの DoS 攻撃のパケットをキャプチャしたものである．実験に使った属性項目は，データセット A と同様，表 1 に示してある．このサイトは文献で実験を行ったものと同じであるが，パケットをキャプチャした時期が異なっている．

このデータセットに本報告の手法を適用し，HTTP メソッドについて視覚化ツールで描画を行った図を図 4 に示す．この図より、POST による DoS を行う攻撃ホストと、GET を用いる攻撃ホストの攻撃行動が類似しており，相関があることがわかる．前回行った分析により，ログに記録されている DDoS の攻撃は，大きく 3 種類あることが明らかになったが，今回本報告で開発したツールで分析を行うことにより，その中の 2 種類はほぼ同一の攻撃ホストにより行われている，という新たな知見を得ることができた．

SOM および視覚化ツールを用いた分析では，特にデータセット A の実験で明らかになったように，小数のホストによって行われている攻撃行動を発見できる可能性がある，という特徴がある．このような少数データは，単にデータ全体の相関を取った場合には，大多数のデータに埋もれてしまう可能性が高く，SOM を活用するメリットであると言える．

6 分析シナリオに関する考察

以上で提案した手法，および開発したツールはインターネットリスク分析モデルの中で実運用に組み込んでゆくことを目的としている．

分析モデルにおいては，SOM の他にリアルタイムにインシデントを検出できるモジュールが複数動作している．SOM は計算量が大きいというアルゴリズムの性質

上，実時間で何らかの結果を出すことは難しい．しかし，他のリアルタイムモジュールでインシデントが通知された時，分析者がアクセスログなどを分析する際に SOM の結果を直ちに利用して詳細な分析が行えることが望ましい

この点を考慮して以下のようなシナリオを考案した．

バッチプロセスによる SOM 実行

考案の手法では，リアルタイムで処理しているログを一定時間ごとに取得し，プロファイリングおよび SOM の処理を行い，マップ描画用の出力ファイルを作成しておく．現在，1 時間ごとにデータを取得して SOM を実行することを検討している．

緊急時の視覚化ツールを用いた詳細分析

インシデント情報が通知された場合には，分析者が必要に応じて該当時間の SOM 出力ファイルを参照し，視覚化ツールを用いて詳細な分析を行う．

リアルタイム分析へのフィードバックなど

分析結果としては，特徴的な挙動を示すホストの集合や属性項目などを得られることが期待できる．

従って，分析後のアクションとしては，

- 分析で得られた特徴的な属性項目をリアルタイム分析へフィードバックする．
- 特徴的な挙動を示すホストの集合の抽出，レポートの作成する．
- ここで着目した事柄(属性項目，ホストのセグメント)を，より詳細な分析への手ががりとする．

などを行うことを想定している．

ここで述べた分析シナリオに沿った運用を行うため，現在，実験システムの構築を行っており，2005 年 12 月の本原稿執筆時点では，プロトタイプの運用試験を開始している．

7　おわりに

本報告では SOM を用いて，特徴的な挙動をするホストの集合や属性項目を抽出する方法について，アルゴリズム，視覚化，分析シナリオなどの検討を行った．

本手法は，普通に相関を取っただけではわからない，非線形で局所的なホストの振る舞いを捕らえることができるため，亜種の検出や，特徴的な属性の抽出などの問題に対して，インシデント分析の有効な手法の一つとなると予想できる．

今後の課題としては，第 2 節で述べたプロファイリング項目の最適化，SOM のパラメータのチューニング，インターネットリスク分析モデルの中における新たな分析シナリオの創出などが挙げられる．

今後は，第 6 節で示した運用など，様々なデータソースで実験を繰り返しながら，手法のブラッシュアップや上記課題の検討を行ってゆく予定である．

謝辞

本報告の研究内容に関してアドバイスやアイデア，技術的なサポートを提供して下さった横河電機の鈴木和也氏，馬場俊輔氏，NICT の関係各位にここでお礼を申し上げます．また，実験データの取得，提供にご協力頂いた関係各社の方々についても，ここで厚くお礼を申し上げます．ありがとうございました．

参考文献

[1] JPCERT/CC Internet Scan Data Acquisition System (ISDAS)

URL: http://www.jpcert.or.jp/isdas/

[2] 警察庁セキュリティポータルサイト@police

URL: http://www.cyberpolice.go.jp/

[3] DShield.org—Distributed Intrusion Detection System

URL: http://www.dshield.org/

[4] Evan Cooke, Michael Bailey, David Watson, Farnam Jahanian, and Jose Nazario “The Internet motion sensor: A distributed global scoped Internet threat monitoring system.” Technical Report CSE-TR-491-04, University of Michigan, Electrical Engineering and Computer Science, July 2004.

[5] 中尾, 丸山, 大河内, 松本, 守山, 武智, “インターネットリスク分析モデルに関する考察”，暗号と情報セキュリティシンポジウム SCIS 2005, pp.1531-1536, 2005.

[6] 芦田,前田,高橋, “データマイニングにおける特徴的ルール生成方式”，情報処理学会第 50 回全国大会, 1995.

[7] K.Yamanishi, J.Takeuchi, “A Unifying Approach to Detecting Outliers and Change-Points from Non stationary Data" The Eighth ACM SIGKDD International Conference on Data Mining and Knowledge Discovery, ACM Press, pp.676-68, 2002.

[8] Y.Maruyama, K..Yamanishi, “Dynamic Model Selection and Its Applications to Computer Security”, The IEEE Information Theory Workshop 2004.

URL: http://ee-wcl.tamu.edu/itw2004/

[9] 中尾, 力武, 竹内, 大河内, 吉岡, 衛藤, 守山, 松本, “インターネットにおける実時間イベント分析の研究開発”, 暗号と情報セキュリティシンポジウム SCIS 2006, 2006, 掲載予定

[10] 松本, 堀,, 力武, 中尾, “ネットワークインシデント分析システム構築運用における ユーザインタフェースの検討”, 暗号と情報セキュリティシンポジウム SCIS 2006, 2006, 掲載予定

[11] 竹内, 佐藤, 力武, 中尾, “変化点検出エンジンを利用したインシデント検知システムの構築”, 暗号と情報セキュリティシンポジウム SCIS 2006, 2006, 掲載予定

[12] Kohonen, T., “Self-Organizing Maps”, Springer, Berlin, Heidelberg, 1995.

[13] T.コホネン著, 徳高, 岸田, 藤村訳, “自己組織化マップ,” シュプリンガー・フェアラーク東京, 1996.

[14] 阿部, 金谷, 木ノ内, 池内, “ゲノムDNA配列に潜んでいる生物種の個性を明らかにする新規な統計数理的手法”, 統計数理, pp.207-215, 2004.