

ネットワーク異常の検出と原因特定方式に関する研究

東北大大学院情報科学研究科 和泉勇治

2006年10月27日

1 まえがき

ネットワークの安全で安定した運用のためには、ネットワーク状態を適切に把握し、効果的にネットワークの異常状態を検知することが重要である。ネットワークトラヒックの異常状態を自動検知するためには、トラヒックの通常状態を何らか数理的なモデルで表現し、そのモデルからの逸脱の程度を定量的に評価する技術が利用され、多数の研究がなされている[1]-[9]。

文献[1], [2]は、人工ニューラルネットワークやSupport Vector Machineにより、学習時の観測量の分布を推定し、検査時の観測量の異常の程度を評価する手法である。これらの手法は、多次元空間にクラスタを形成して分布する観測量の分布形状を評価する方式であると見なすことが可能で、通常状態と異常状態は、空間の異なる位置に分布していることを仮定している。観測量の時間的推移を評価する手法としてHidden Markov Modelを用いた異常検知技術も提案されている[3]。System callなどの呼び出し順などのモデル化に適した技術で、観測対象の発生に因果関係があり、発生順に一定の法則があることを前提としているものである。同様に、観測量や通信ログなどの異常イベントの発生順に対しデータマイニング技術を適用した手法の研究も行われている[4]-[6]。

また、観測量間の相関関係に着目した方式として、主成分分析[7][8]やSpline曲線を用いた方式[9]がある。これらは、観測量間に相関関係が存在することを仮定し、観測量が、多変量の空間において、直線や曲線、平面状に分布していることを前提としている。

観測量間の相関関係は、プロトコルによる制約により生じ得るものであると考えられ、これらの手法によるネットワークトラヒックのモデル化は妥当なものであると考えられる。しかし、多次元のベクトルで構成される観測量を単一の曲線などでモデル化した場合、異常発生時の観測量の逸脱の程度を高精度に評価出来たとしても、その逸脱の原因となつた観測量を発見し、その異常発生の原因を特定することが困難であるとの問題がある。

そこで我々は、ネットワークトラヒックの相関関係を利用し、更に、異常発生の原因となつた観測量の特定が可能な異常検知方式として、相関係数ヒストグラム[10]によるネットワーク異常検知方式を提案する。相関係数ヒストグラムは、ネットワークトラヒックの観測量間の相関係数の発生確率をヒストグラムとしてモデル化し、その確率の大小によって、ネットワーク状態を評価する方式である。この方式は、相関係数の値域が-1から+1となり、その発生確率のヒストグラム化が容易である特徴を利用したものである。更に、観測対象種別のパケットが観測されない場合や観測量の変動が無い場合など、相関係数の算出が不可能な場合にも対応可能とするために、「算出不可クラス」をヒストグラムに加える拡張を行う。このモデルは、任意の観測種別間に、どのような相関関係がどの程度の頻度で発生し得るのかを定量的に評価したものであり、相関関係に変動が存在する場合のモデル化も可能であるという特徴を有している。この評価方式は、検査対象の観測量から算出された相関係数の発生確率が閾値を下回った組み合わせの総数に基づき異常の程度を評価し、ネットワークトラヒックの異常検知の基準として用いる。

本研究では、上記の手法により算出された相関係数の発生確率を要素とした行列と、それを利用した異常度の算出、類似事象の検索方式を提案する。5ヶ月間のネットワークトラヒックを利用した評価実験により、異常トラヒック検知と異常原因トラヒックの特定、類似事象の検索が可能であることを示す。

2 相関係数ヒストグラム

本研究で提案するネットワークトラヒックの評価方式は、一定期間のネットワークトラヒックの観測量間の相関係数の発生確率の分布を表すヒストグラムを生成する学習過程と、そのヒストグラムに基づきネットワークトラヒック状態を評価する評価過程からなる。本章では、ヒストグラムを生成する学習過程について述べる。

2.1 観測量間の相関係数の変化

図1、2に、通信の開始を示すTCPのSYNパケット数と、通信の終了をFINパケット数を、それぞれ、10秒と1800秒の観測スロットでカウントし、30スロット毎に相関係数の場合の相関係数の時間変化を示す。観測したネットワークは約50台のクライアントPCと外部に公開しているWebサーバ1台、SMTPサーバ1台が稼働するネットワークである。

TCPの動作を考えた場合、SYNパケットとFINパケットはコネクションの開始と終了に対応するため1対1の割合で発生し、高い相関を保持することが予想される。しかし、図から分かるように、相関係数の値は大きく変動している。観測スロット幅を1800秒と大きくした場合においても、相関係数の値が0.2に低下する場合があり、プロトコルの動作から予想される相関関係とは異なる挙動が実際のネットワークトラヒックでは生じていることが分かる。

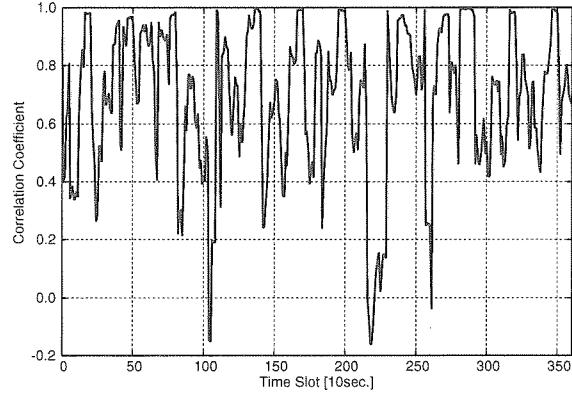


図1：相関係数の時間変化（観測スロット幅：10sec.）

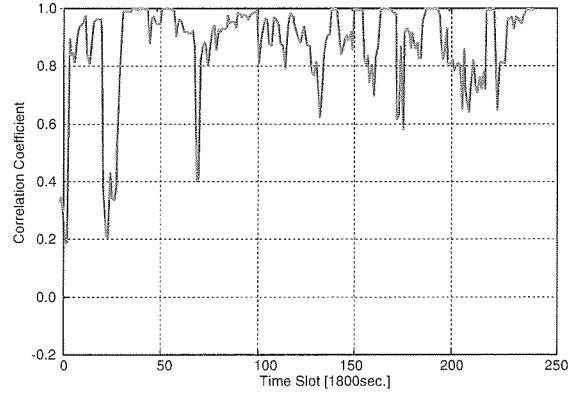


図2：相関係数の時間変化（観測スロット幅：1800sec.）

2.2 相関係数ヒストグラム

前節に示したように、相関係数は一定の値をとることは希であると言える。そこで本研究では、一定期間の相関係数の発生確率をヒストグラムで表現し、その値の変動も考慮したモデル化を行う。相関係数は -1 から $+1$ の値を取るため、ヒストグラムとして表現することが容易であるという利点がある。しかし、相関係数は、該当観測量に変動が全く無い場合、つまり、観測量の標準偏差が0になる場合は相関係数の算出が算出が不可能となる。そのような場合は、式(1)に示すように、相関係数を求める二つの変量のうち標準偏差が0となる組合せに応じ相関

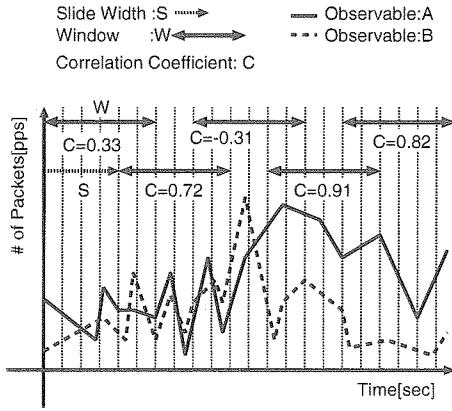


図 3: 相関係数の算出

係数 r 値を 1.1, 1.2, 1.3 と定義し、その値を「算出不可クラス」という新たな階級としてヒストグラム追加する。

$$r = \begin{cases} \frac{\text{Cov}(x,y)}{\sigma(x)\sigma(y)} & (\sigma(x) \neq 0 \wedge \sigma(y) \neq 0) \\ 1.1 & (\sigma(x) = 0 \wedge \sigma(y) = 0) \\ 1.2 & (\sigma(x) = 0 \wedge \sigma(y) \neq 0) \\ 1.3 & (\sigma(x) \neq 0 \wedge \sigma(y) = 0) \end{cases} \quad (1)$$

ここで、 Cov , σ は、それぞれ、共分散と標準偏差を表す。この算出不可能な場合も含めたヒストグラムを本研究で提案する相関係数ヒストグラムとし、この相関係数ヒストグラムの算出過程を学習過程とする。

相関係数ヒストグラムは、任意の二つ観測量の全ての組合せに対して生成する。例えば、ネットワークトラヒックの観測対象が IP, TCP, UDP パケット数 3 種類である場合、その組合せ数の $3(3-1)/2 = 3$ 個のヒストグラムが生成されることになる。また、相関係数の算出においては複数のサンプルが必要となるため、2.1 と同様に、複数の連続した観測スロットの集合を Window とし、その Window 内の複数のスロットを利用し相関係数を算出する(図 3)。2.1 の例では、30 スロットを 1 つの Window として相関係数を算出していることになる。

図 4, 5 に、図 1, 2 に基づき生成した相関係数ヒストグラムを示す。ヒストグラムからも TCP の SYN

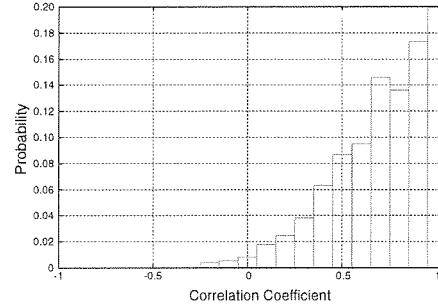


図 4: 相関係数ヒストグラム(観測スロット幅:10sec.)

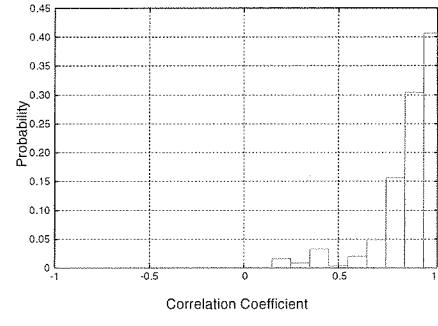


図 5: 相関係数ヒストグラム(観測スロット幅:1800sec.)

パケットと FIN パケットの相関が大きく変動していることが分かる。

このように相関係数ヒストグラムは、任意の二つの観測量の発生のバランスを相関係数により評価し、そのバランスがどのような確率で出現するのか、という観点でネットワークトラヒックをモデル化しているものであると解釈できる。

3 相関係数発生確率行列に基づいたネットワークトラヒック評価方式

学習過程によって作成された相関係数ヒストグラムを利用して、ネットワークトラヒックの状態を定量的に評価するために、評価対象の期間に算出され

た相関係数の発生確率を行列としてのネットワークトラヒックの評価方式と、それに基づき異常状態を検知する方式を提案する。

3.1 相関係数発生確率行列

評価対象のWindow内の観測量の全ての組合せに関する相関係数の値の発生確率を学習過程で生成した相関係数ヒストグラムに基づき算出し、その発生確率を要素とした行列を生成する。この行列を相関係数発生確率行列と呼び、次のように定義する。

任意の二つの観測種別 i と j の該当 Window 内の観測量の相関係数を r_{ij} としたとき、相関係数発生確率行列 \mathbf{P} の要素 p_{ij} は、

$$p_{ij} = h_{ij}(r_{ij}) \quad (2)$$

となる。ここで、 h_{ij} は、観測種別 i と j の相関係数ヒストグラムであり、 r_{ij} の発生確率を返す。

3.2 異常度の算出

ネットワークの異常状態を検知するために、3.1で定義した相関係数発生確率行列から異常の程度を表す異常度 (AS) を算出する。異常度は、任意の観測種別 i に関する組合せの相関係数の発生確率が閾値以下となったものの総数に基づき式(3)のように算出される。

$$AS = \sum_i (\sum_j as_{ij})^s \quad (3)$$

ここで θ を異常を表すための p_{ij} に対する閾値をすると、 as_{ij} は、

$$as_{ij} = \begin{cases} 1 & p_{ij} \leq \theta \\ 0 & p_{ij} > \theta \end{cases} \quad (4)$$

と定義され、式(3)はある観測種別 i に関する相関係数の発生確率が異常に低いものの個数の s 乗の総和を表すことになる。ここで、 s は感度を表し、観

測種別 i に関する異常な相関係数の値の個数を強調する機能であると解釈できる。また、提案する異常度は、ある観測量とその他の観測量との間の異常な相関係数が多い程、高い値を取ることになる。高い異常度を算出する原因となった観測量が、その異常の原因と判断することが可能である。

3.3 異常状態検出実験

本章で提案した相関係数発生確率行列を利用し、ネットワークトラヒックの異常状態検出実験を行う。実験で利用するネットワークトラヒックデータは、約 50 台のクライアント PC と外部に公開している Web サーバ 1 台、SMTP サーバ 1 台からなるネットワークを対象とし、対象ネットワークとインターネットとの出入りのトラヒックを流入、流出を独立に観測する。観測種別は表 1 に示す 66 種類のトラヒックで、流入と流出を別に観測するため 132 種類のトラヒックの観測することになり、学習過程で生成されるヒストグラムの総数は、その組合せの $132(132 - 1)/2 = 8646$ 個になる。

実験では、該当種別のトラヒックを 10 秒のタイムスロットにより観測した。相関係数を求める Window の幅は 300 秒 (30 スロット)、異常度算出の閾値は $\theta = 0.01$ とした。実験期間は、2005 年の 1 月 1 日から 2005 年 5 月 31 日の 5 ヶ月間で、観測されたパケットの総数は 1132900380 個であった。相関係数ヒストグラムの作成と相関係数発生確率行列、異常度の算出は 1 日単位で行い、相関係数ヒストグラムの作成は相関係数発生確率行列と異常度の算出の前日のデータを用いる。つまり、1 月 2 日の異常度を算出する場合は、1 月 1 日のデータから作成した相関係数ヒストグラムを用いることになる。

図 6, 7 に実験期間で最も高い異常度と 2 番目に高い異常を示した Window の相関係数発生確率行列を示す。異常度算出時の感度は $s = 1, 2, 3$ の 3 つの値を利用し、図 6, 7 は、そのいずれの場合においても、最も高い異常度と 2 番目に高い異常度を示したものである。図の画像は、発生確率が閾値 θ 以下と

表 1: 対象観測量

| 番号 | 観測種別 |
|-------|--|
| 1 | 全てのパケット |
| 2-3 | ARP, その他の Ether フレーム |
| 4 | IP パケット |
| 5-7 | TCP, UDP, ICMP パケット |
| 8 | 他の IP パケット |
| 9-14 | TCP フラグ (URG, ACK, PSH, RST, SYN, FIN) |
| | TCP ソースポート番号毎 |
| 15-22 | 20, 21, 22, 25, 80, 110, 143, 443 |
| 23-31 | 上記を除く他の範囲を 9 分割 (0~79, 81~109, 111~142, 144~442, 444~1023, 1024~2999, 3000~5999, 6000~9999, 10000~65535) |
| | TCP ディスティネーションポート番号毎 |
| 32-40 | 20, 21, 22, 25, 80, 110, 143, 443 |
| 40-48 | 上記を除く他の範囲を 9 分割 (0~79, 81~109, 111~142, 144~442, 444~1023, 1024~2999, 3000~5999, 6000~9999, 10000~65535) |
| | UDP ソースポート番号毎 |
| 49-51 | 53, 123, 520 |
| 52-57 | 上記を除く他の範囲を 6 分割 (0~52, 54~122, 124~519, 521~1023, 1025~9999, 10000~65535) |
| | UDP ディスティネーションポート番号毎 |
| 58-60 | 53, 123, 520 |
| 61-66 | 上記を除く他の範囲を 6 分割 (0~52, 54~122, 124~519, 521~1023, 1025~9999, 10000~65535) |

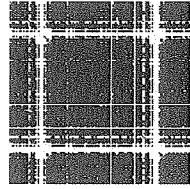


図 6: 異常発生時の相関係数発生行列 1

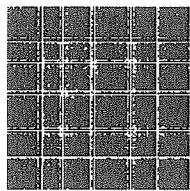


図 7: 異常発生時の相関係数発生行列 2

なった要素に白画素, θ より大きい要素に黒画素を割り当て, 相関係数発生確率行列を画像化したものである.

図 6, 7 は, それぞれ異なる日時のものであるが, ネットワーク異常としては, 複数のポートに対するスキャンが行われていた. 画像中の直線は, スキャンに利用されたポート番号を含む観測種別に対応するもので, そのポートを利用したパケット数の通常時では起こり得ない増加が, 他の観測量との通常時の相関関係を崩し, 異常な相関係数が算出されたため生じたものである. つまり, 相関係数発生確率行列中で発生確率の低い相関係数が直線上に並んでいるものを効率良く検知できれば, 異常の原因を含めた形で異常状態の検知が可能になると考えられる.

そこで, 異常度 AS に対する検知基準を画像中の縦横それぞれに一つの直線が存在する場合の大きさ程度に設定し, 該当する異常状態の検知した. 観測種別は, 66 種類でネットワークの流入と流出を別に観測するため, 合計で 132 種類となる. そのため, 若干の誤差を許容するように, $s = 1$ の場合, 検知対象の異常度の範囲を $264(132 \times 2) \sim 280(140 \times 2)$ とした. $s = 2, 3$ の場合は, 感度 s によって強調されるのは行列の行のみであるため, 横の直線状の異

常な発生確率の個数のみ s 乗され, 縦の異常な発生確率の個数はそのまま加算されるだけである. つまり, $s = 2, 3$ の場合の検知対象の異常度の範囲は, それぞれ, $17556(132^2 + 132) \sim 19740(140^2 + 140)$, $2300100(132^3 + 132) \sim 2744140(140^3 + 140)$ となる.

図 8 に検知結果の一例を示す. 図から, 異常度の検知範囲を適切に設定することによって, ある一つの観測量により生じた異常の検知が可能であることが分かる. 表 2 に, 検知された異常事象を示す.

それぞれのパケットが観測された前後の 12 時間のデータを調査したが, $s = 1, 3$ の場合, 該当パケットを送信したホストからの通信は発見されなかった. そのため, 何らかの異常や不正によるパケットや, それらに伴う backscatter が観測されたと考えられる. これは, 5ヶ月の実験期間で記録された 11 億個のパケットから 1~3 個の異常パケットを発見した結果であり, 本提案手法の有効性を証明するものである. また, 図 9 には, $s = 2$ の場合に検知されたパケットを送信したホストに関するトラヒックダンプデータを示す. 図中の下線部のパケットが異常原因として検知されたパケットである. このように検知されたパケットに関するホストの通信を解析することによっても, 一連の異常な通信の抽出が可能となっていることが示されている.

図 10 には, $s = 1$ の場合にのみ生じた誤検知の例を示す. $s = 1$ の場合, 異常な発生確率が分散してしまっていても, その総数が検知の閾値以上になると誤検知を起こしてしまうことになる. 一方, 感度 s を 1 より大きく設定した場合, 直線上に並んだ異常確率を強調して全体の異常度を算出することになる. 特に, 感度 s を 2 以上とし, 直線上に異常発生確率が並んだ場合, その一行の異常度は発生確率行列の全要素数以上となり, 行列内に分散して異常確率が生じた場合よりも有意に大きな異常度が算出されることになる. そのため, $s = 1$ では誤検知が生じたが, $s = 2, 3$ の場合にはそのような現象が観測されなかったと考えられ, 感度を導入した異常度の算出式 (3) は有効なものであると言える.

表 2: 検知事象例

| 感度 (s) | 事象 | 発生日時 | 該当パケット数 |
|------------|---------------------------------|---------------------|---------|
| 1 | RST パケット流入 | 2005/05/24 07:59 | 4 |
| 2 | UDP パケット流入 (src port 54~122) | 2005/05/15 00:53 | 1 |
| 3 | ack パケット流入 (src port 81~109) | 2005/02/01 15:57 | 2 |

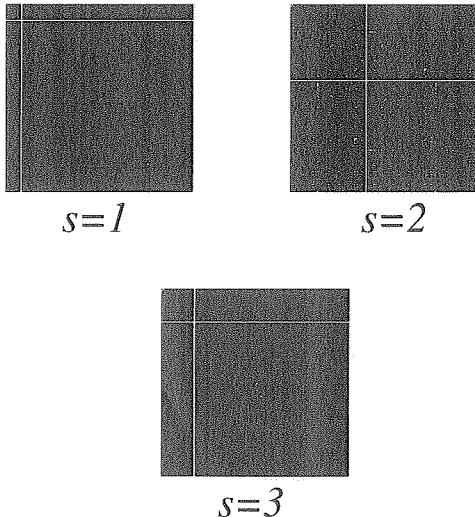


図 8: 一つの観測種別が原因となった異常の検知

```

00:53:51.298753 IP srcIP > dstIP:  
icmp 40: echo request seq 1  
00:53:51.298874 IP srcIP.80 > dstIP.53:  
. ack 0 win 1400  
00:53:51.299623 IP srcIP.53 > dstIP.53:  
S 4264028687:4264028687(0) win 140  
00:53:51.300498 IP srcIP.55 > dstIP.49153:  
UDP, length: 10  
00:53:51.597704 IP srcIP.53 > dstIP.53:  
R 4264028688:4264028688(0) win 140  
00:53:51.598453 IP srcIP.53 > dstIP.53:  
R 4264028688:4264028688(0) win 0

```

図 9: 検知されたトラヒック

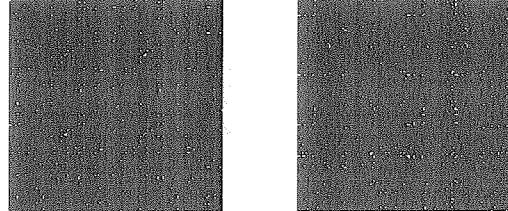


図 10: 感度 $s = 1$ での誤検知

4 相関係数発生確率行列を用いた類似事象検索

前章の実験から、相関係数発生確率行列はネットワークで生じている異常状態に対応した構造を持つことが明らかとなった。この特性を利用し、類似事象の検索方式を提案する。

4.1 相関係数発生確率行列の類似性評価指標

相関係数の発生確率行列の類似度を式 (5) により定量的に評価する。任意の二つの相関係数の発生確率行列を A , B とした場合、類似度 S を次のように定義する。

$$S = \sum_i \sum_j d_{ij} \quad (5)$$

$$d_{ij} = \begin{cases} 1 & (A_{ij} \leq \theta \wedge B_{ij} \leq \theta) \\ 1 & (A_{ij} > \theta \wedge B_{ij} > \theta) \\ -1 & (A_{ij} \leq \theta \wedge B_{ij} > \theta) \\ -1 & (A_{ij} > \theta \wedge B_{ij} \leq \theta) \end{cases}$$

θ は、式 (4) で用いた異常を判断する閾値である。式 (5) は、行列 A, B の異常な発生確率となる要素が一致している場合、つまり、行列 A, B 間で同一の観測量が異常原因となっている場合に高い類似度を示すことになる。

4.2 類似事象検索実験

相関係数発生確率行列の類似度を利用し、類似事象の検索実験を行う。実験には 3.3 と同様のパラメータと実験データを利用する。類似事象の検索基準としては、図 8 の $s = 2$ 場合の 1 個の UDP パケットが検知された事象を用いる。

表 3 と図 11, 12 に、それぞれ、類似事象の発生日時と発生確率行列、ネットワークトラヒックダンプデータを示す。図 11 から類似した発生確率行列が適切に検索されていることが分かる。また、図 12 に示されるように、類似事象の検索によって、検索基準となった 2005 年 5 月 15 日のトラヒックと同様の UDP パケットが原因となった異常を検索できている。表 3 とパケットの観測時刻に誤差があるが、これは、相関係数の算出ウインドウが (10 秒幅の観測スロット) \times (30 スロット) = 5 分 となっているからである。

本実験から、相関係数発生確率行列の異常な確率を持つ要素の分布状態の類似性を適切に評価することにより、数カ月に渡る期間を対象に解析を行ったとしても、同様の異常パケットを発見可能であることが明らかとなった。

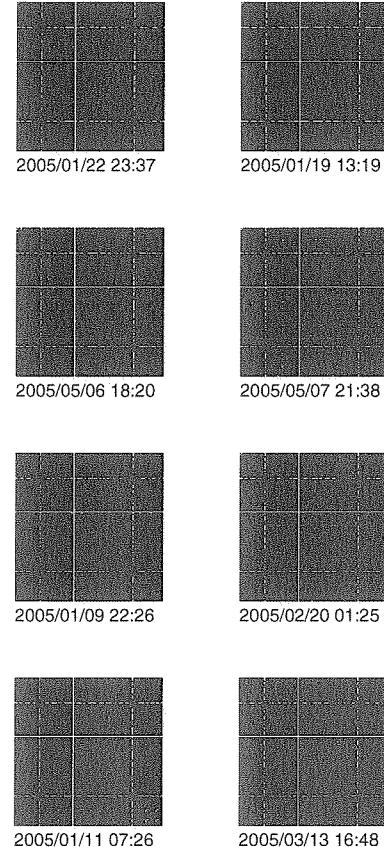


図 11: 類似事象の発生確率行列

5 本研究の応用例

本研究は、ネットワーク管理システムのデータのスクリーニングや可視化機能として応用可能である。現時点では、関連特許の出願中で、独立行政法人科学技術振興機構 (JST) による海外出願支援も決定し、作業を進めている所である。

また、地域企業による製品化を想定したプロトタイプ開発も行われている。図 13 に可視化システムとしてのプロトタイプを示す。相関係数行列よ相関係数発生確率行列を同時に可視化することにより、異常を示す観測量の効率的な特定が可能となっている。

表 3: 類似事象検索結果

| 日時 | 異常度 | 日時 | 異常度 |
|------------------|-------|------------------|-------|
| 2005/01/22 23:37 | 16764 | 2005/01/19 13:19 | 16764 |
| 2005/05/06 18:20 | 16748 | 2005/05/07 21:38 | 16736 |
| 2005/01/09 22:26 | 16720 | 2005/02/20 01:25 | 16700 |
| 2005/01/11 07:26 | 16680 | 2005/03/13 16:48 | 16676 |

```

23:38:16.522838 IP srcIP1.55 > dstIP1.49153: UDP, length:10
13:20:11.045304 IP srcIP1.55 > dstIP2.49153: UDP, length:10
18:20:56.941355 IP srcIP2.55 > dstIP1.49153: UDP, length:10
21:40:35.737303 IP srcIP3.55 > dstIP2.49153: UDP, length:10
22:27:57.656383 IP srcIP3.55 > dstIP1.49153: UDP, length:10
01:29:53.431819 IP srcIP1.55 > dstIP2.49153: UDP, length:10
07:30:53.329319 IP srcIP1.55 > dstIP2.49153: UDP, length:10
16:48:56.757771 IP srcIP3.55 > dstIP2.49153: UDP, length:10

```

図 12: 類似事象のトラヒック

6 むすび

本研究では、ネットワークトラヒックの異なる観測種別の発生数のバランスを相関係数として算出し、その相関係数の値の発生確率をヒストグラムでモデル化する手法と、そのヒストグラムに基づき算出した相関係数の発生確率を行列として表すネットワークトラヒック評価方式を提案した。提案方式により、異常原因の特定も含めたネットワーク異常状態検知が可能であることが明らかとなった。

相関係数の値の発生確率を表す相関係数ヒストグラムは、ネットワークトラヒックの状態において相関係数の算出が不可能になる場合に対応するために、「算出不可クラス」ヒストグラムに追加する工夫を行っており、この算出不可クラスにより、通常時では観測されずに相関関係の情報が得られないようなトラヒック種別に対しても異常の程度を定量的に評価することを実現した。また、ネットワークトラヒックの評価時においては、新たに算出された相関係数の発生確率を要素とする相関係数発生確率行列として表し、異常な発生確率が行列内において直線上に分布している観測種別の異常度を強調するような異

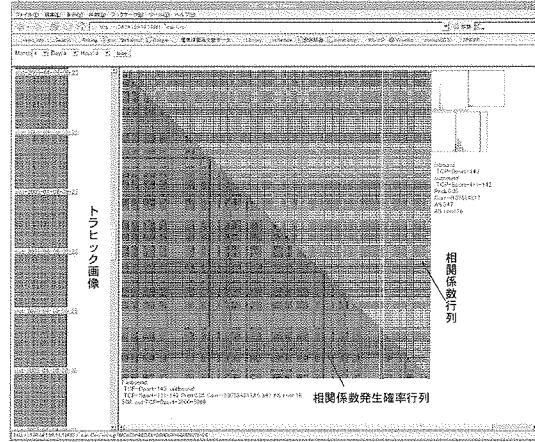


図 13: 可視化システムのプロトタイプ

常度算出式を提案し、異常原因の容易な特定を実現した。

これらネットワークトラヒックのモデル化と異常度算出方式により、11億個以上のパケットからたった1個の異常パケットをシグネチャなどを利用せずに発見することが可能であることを示し、本論文での提案手法の有効性を示すことが出来た。

参考文献

- [1] Lippmann and S. Cunningham, "Improving intrusion detection performance using keyword selection and neural networks," Computer Networks 34 (2000) (4), pp. 597-603.

- [2] Sang-Jun Han and Sung-Bae Cho,"Detecting intrusion with rule-based integration of multiple models," Computers and Security 22 (October 2003) (7), pp. 613-623.
- [3] S.-B. Cho and H.-J. Park, "Efficient anomaly detection by modeling privilege flows with hidden Markov model," Computers and Security 22 (2003) (1), pp. 45-55.
- [4] Stefanos Manganaris, Marvin Christensen, Dan Zerkle and Keith Hermiz, "A data mining analysis of RTID alarms," Computer Networks, Volume 34, Issue 4, pp.571-577, Oct. 2000
- [5] H. Mannila, H. Toivonen, A.I. Verkamo, "Discovering frequent episodes in sequences," Proc. of the First International Conference on Knowledge Discovery and Data Mining, pp.259-289, Montreal, Canada, Aug. 1995
- [6] R. Agrawal, R. Srikant, "Mining sequential patterns," Proc. of the International Conference on Data Engineering (ICDE), pp.3-14, Taipei, Taiwan, Mar. 1995
- [7] Mei-Ling Shyu, Shu-Ching Chen, Kanok-sri Sarinnapakorn, LiWu Chang, "A Novel Anomaly Detection Scheme Based on Principal Component Classifier," Proc. of ICDM Foundation and New Direction of Data Mining workshop, pp 172-179, 2003.
- [8] 佐藤 陽平, 和泉 勇治, 根元 義章, "複数の検出モジュールの組み合わせによるネットワーク異常検出の高精度化," 電子情報通信学会技術研究報告, NS2004-144, pp.45-48, Oct, 2004
- [9] Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham and Vitorino Ramos, "Intrusion detection systems using adaptive regression splines." 6th international conference on enterprise information systems, vol.3, pp. 26-33, 2004.
- [10] 廣瀬 淳一, 和泉 勇治, 角田 裕, 根元 義章, "トライピック種別間の相関関係に基づいたネットワーク状態の評価方式", 電子情報通信学会技術研究報告, NS2005-112, pp.5-8, Nov, 2005