E-25

グラフを用いたトラフィックデータ参照システム

The Traffic Data Analyzing System Refered by Describing the Graph

井尾 明日香†[1]　　川橋 裕†[2]
Asuka Io　　Yutaka Kawahashi

１．はじめに

今日，インターネットは個人や企業・大学を問わずさまざまな社会システムに活用されるインフラストラクチャとなった．社会システムの基盤として高い利便性をもたらす一方で，システムに障害が発生した際には重大な影響をおよぼす危険がある．

このため，近年までのネットワーク運用管理では，障害が起こらないシステム環境の構築および管理が理想とされてきた．しかし，インターネットの急激な拡大やネットワーク構成の複雑化にともない，障害を起こさない対策を実現することは極めて困難となっている．

上記に起因して，経済産業省から「障害は起こりうるものである」という事故前提社会[1][2][3]の考え方が提唱されている．事故前提社会では，インシデントの予防や被害の最小化・局所化，回復力の高い仕組みの構築が要求される．すなわち，ネットワーク運用管理者（以下管理者）は，障害に迅速に対応し，どのような経緯で障害が発生したか原因を究明が必要不可欠となった．

事故前提社会において重要となるのが，内部ネットワークと外部ネットワークの間で，過去にどのような通信がおこなわれたかの記録（以下，通信記録）の把握である．通信記録は，インターネットにおける電話の通話記録に類似した管理情報であり，「誰と誰が，いつ，どのくらいの情報を量的にやりとりしていたか」の記録である．

通信記録の解析によってネットワーク内の障害を把握するケースが存在する．例として，端末の接続相手数による P2P ファイル共有ソフトウェア利用の発見，ウイルス・ワームの感染経路の特定，対外接続部の帯域占有によるネットワーク接続困難・接続不可の解決などが挙げられる．しかし，通信記録で管理する問題点として，管理者や通信記録を検索するシステムへの負荷が大きいということが挙げられる．これは，内部ネットワークと外部ネットワークの間では膨大な量の情報がやりとりされているからである．

管理者が障害を発見し，原因を究明するには，現時点の通信記録だけではなく過去の通信記録を参照する場面も多い．しかし，和歌山大学の対外接続部を例に挙げると，1 日のうち最も通信が多い時間帯で毎秒約 1 万パケット（10Kpps）もの情報がやりとりされている．このような状況下において，管理者が通信記録だけを用いて監視することは事実上困難である．したがって，管理者に対して，通信記録のどの情報が障害を解決するために必要であるか示す必要がある．

本誌では，トラフィックを「量」と「質」から分析するというネットワーク監視の方法から，通信記録の活用を考える．本誌では，内部ネットワークと外部ネットワークの境界部となる対外接続部におけるトラフィック量をトラフィックの量的情報として定義する．さらに，対外接続部において端末同士の個々の通信量，時刻，および通信相手先などの情報をトラフィックの質的情報として定義する．

トラフィックを「量」の視点で分析すると，どの時間帯にトラフィックが増減するかといった，トラフィックの全体像を分析が可能になる．さらに，中・長期的にトラフィックを分析することで，トラフィックの増減傾向からネットワークの異常を発見可能である．一方，トラフィックを「質」の視点で分析すると，対外接続部を圧迫している通信端末の特定や，ウイルス・ワームの感染元の端末特定などが可能となる．すなわち，トラフィックの量的な分析によって障害を発見し，その結果をもとに，質的な分析によって障害の原因を発見する．通信記録とは、上記のトラフィックの質的な分析であるため，通信記録を活用するためにはトラフィックの量的な分析を付加する必要があると言える．

本誌では，対外接続部における通信記録の保存，および量的なトラフィックを管理者に提示し，質的な分析を支援するシステムを提案する．具体的には，TCP・UDP における内部ネットワークから外部ネットワークへの通信（以下，outgoing），外部ネットワークから内部ネットワークへの通信（以下，incoming）をそれぞれ通信記録として保存する．データ転送量をグラフとして可視化し，このグラフをトリガとして通信記録を参照するシステムである．加えて，IP アドレス単位でのトラフィック量のランキング，IP アドレス単位での通信相手数のランキング，IP アドレス検索機能から，通信記録の利用を支援するシステムを構築する．

本誌では，システムに必要な技術概要を説明した後，実装したシステムの構成と動作について説明し，最後に和歌山大学内（以下，学内）ネットワークで運用実験した評価と考察をおこなう．

†[1]和歌山大学 システム工学研究科
Graduate School of Systems Engineering，Wakayama University
†[2]和歌山大学 システム情報学センター
Center for Information Science，Wakayama University

2． 技術概要

2.1 ネットワーク運用管理における本誌の位置づけ

ネットワーク運用管理とは，対象であるシステムを効率よく，円滑かつ安全に利用できるようにする業務である．業務内容は，構成管理，障害管理，性能管理，設備管理，セキュリティ管理の 5 つの管理項目が挙げられる．

本誌では，障害管理，性能管理の面から研究を進めた．障害管理とは，ネットワークで発生する障害ごとに，検出方法や対策を検討し実施することである．性能管理とは，帯域幅やトラフィック量，各機器の CPU やバッファの使用率に対して閾値を設定し，ネットワークの可用性を維持することである．

本誌では，トラフィック量の可視化によって性能管理をおこない，ランキングや IP アドレス検索から障害管理をおこなう．

2.2 用語の定義

2.2.1 フロー

本誌では，送信元 IP アドレス・宛先 IP アドレス・送信元ポート番号・宛先ポート番号が全て一致する一連のパケット群をフローと定義する．

2.2.2 トラフィックの量的情報

トラフィックの量的情報とは，ネットワーク全体でどれくらいの量の通信がやりとりされているかという情報である．本誌では，通信記録におけるデータ転送量の総計がトラフィックの量的情報にあたる．通信時間帯ごとにトラフィックの量的情報を監視することによって，どのような時間帯にトラフィックが増減するかといった，トラフィックの全体像を分析が可能になる．さらに，中・長期的にトラフィックデータを分析すれば，トラフィックの増減傾向からネットワークの異常を発見できる．

2.2.3 トラフィックの質的情報

トラフィックの質的情報とは，ネットワーク内において，どの端末同士が，いつ，どのくらい通信していたかという端末単位での情報と定義する．トラフィックの質的情報では，送信元 IP アドレスや宛先 IP アドレスから，ウイルス・ワームの感染経路を特定できる．さらに，対外接続部のトラフィックの占有によるネットワーク接続困難・接続不可の解決も可能になる．これに加えて，端末の接続相手数から P2P ファイル共有ソフトウェア利用の発見に繋げることも可能である．

2.2.4 通信記録

広義の通信記録

インターネットにおける電話の通話記録と類似した管理情報であり，「誰と誰が，いつ，どのくらいの情報を量的にやりとりしたか」という情報の記録である．

広義の通信記録は，トラフィックの質的情報と同義である．本誌では，1 章から 3 章までに用いられる通信記録を，広義の通信記録としてあつかう．

狭義の通信記録

本誌の 4 章以降に用いられる通信記録は，狭義の通信記録としてあつかう．具体的には，トラフィックの質的情報から，送信元 IP アドレス・宛先 IP アドレス・送信元ポート番号・宛先ポート番号・データ転送量・パケット数・通信時間帯をそれぞれフロー単位で記録したものである．個人のプライバシー保護の観点から，本誌において保存する通信記録は，TCP・UDP および IP におけるヘッダからのみの情報である．

2.3 技術概要・研究

2.3.1 MRTG（The Multi Router Traffic Grapher）

MRTG[4]は，SNMP エージェントから取得したデータを加工してグラフとして可視化するソフトウェアである．MRTG では，監視対象の機器に対して SNMP リクエストを送信し，取得したデータを PNG 形式として incoming と outgoing の 2 系列のグラフを出力する．監視対象のシステムから収集したすべてのデータは過去 2 年間分保持され，過去 1 日間・1 週間・1 ヶ月間・1 年間のトラフィックのグラフ生成に利用する．出力されるグラフの例として，過去 1 日間のトラフィック量のグラフを図 1 に示す．加えて，過去 1 週間のトラフィック量のグラフを図 2 に示す．グラフ化できるデータとしては，SNMP で取得可能なトラフィック量・CPU LoadAverage・Disk 使用率・メモリ空き容量などが挙げられる．MRTG では HTML 形式のページを生成するため，Apache など HTTP デーモンが動作しているサーバで利用することによって，Web ブラウザ経由で閲覧可能である．

しかし，MRTG はトラフィックの量的情報のみを監視しており，グラフ化したデータに対応する質的情報を見ることができないという問題点がある．

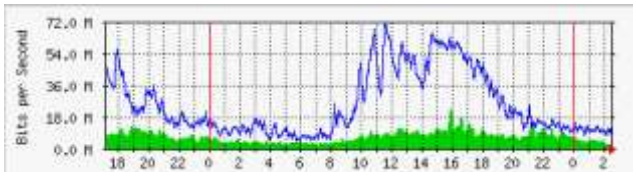

図 1　過去 1 日分のトラフィック量のグラフ

図 2　過去 1 週間のトラフィック量のグラフ

2.2.1 TRAUMAN（Trailer and Authenticated Unit Management system）

TRAUMAN[5]は，受動的にトラフィックの質的情報を保存するシステムである．Snort を用いたトラフィック監視・検出，p0f（passive OS fingerprinting tool）の OS タイプ検出，IPTraf を用いたトラフィック情報の検出をおこなう．

Snort はシグネチャタイプのネットワーク型 IDS であり，シグネチャと呼ばれるルールパターンとトラフィックを照合するソフトウェアである．ルールパターンと一致すれば警告とログをファイルに生成し，管理者への警告もおこなう．それに対し TRAUMAN では，各情報機器の詳細情報を取得するようにシグネチャを設定している．p0f では，まず受動的に TCP の SYN フラグを検出する．検出した SYN パケットを，ウィンドウサイズなど 7 項目の OS 独自のトラフィックパターンと照合し，OS を特定する．IPTraf は，受動的にネットワーク上のトラフィックを監視し，検出するコンソールベースネットワーク統計ソフトウェアである．検出できる統計情報は，日付と時間・プロトコルの種類・データ転送量・送信元 IP アドレス・宛先 IP アドレス・送信元ポート番号・宛先ポート番号・インタフェースの動作・パケット数・総パケットデータ転送量である．TRAUMAN では，上記の検出内容を通信記録としてそれぞれデータベースに保存する．統計データは手動で検索できる．さらに，1 週間毎に統合したデータのレポートを作成する．

このように，TRAUMAN はトラフィックの質的情報の保存のみをおこなうシステムである．そのため，障害の発見および原因究明において，管理者はトラフィックの質的情報から必要な情報を取得する必要がある．しかし，情報量が膨大になるため，必要な情報の取捨選択は困難である．加えて，TRAUMAN では，トラフィックの質的情報をパケット単位でデータベースに保存されるため，検索効率が悪いという問題点もある．

3． 研究目的

3.1 研究目的

近年のネットワーク運用管理では「障害は起こりうるもの」という事故前提社会の考え方が提唱されている．このため，管理者は障害の原因を究明する必要があり，過去にどのような通信がおこなわれたか把握しなければならなくなった．そこで管理者による通信記録の監視が重要となる．しかし，通信記録は情報量が膨大となるため，通信記録のみを用いて障害の発生を発見し原因を究明することは非常に困難である．

通信記録の利用を支援するものとして，トラフィックの量的情報を用いて障害を発見する手法がある．この手法は，管理者がトラフィックの全体像を把握し，トラフィックの増減傾向からネットワークの異常を発見する方法である．この結果をもとに，通信記録から回線を占有している通信を探ることで，障害の原因を特定可能となる．しかし前章で述べたように，既存技術・研究では，トラフィックの量的情報もしくは通信記録の一方から監視をおこなう手法しか存在していないのが現状である．

本誌では，トラフィックの量的情報と通信記録の両方の側面から，障害の発見および原因究明をおこなうシステムの構築を研究目的とする．加えて，トラフィックの増減傾向から障害を発見し，通信記録から原因端末を特定することを研究目的とする．

研究目的を実現するために用いた手法について次節で述べる．

3.2 提案手法

本誌では，通信記録を一定時間のフローで保存する．通信記録をフローにまとめることによって，トラフィックの利用度を出力可能である．利用度はランキングとして表現できる．

本誌では，端末ごとのデータ転送量のランキングおよび通信相手数のランキングにおいて利用度を調べる．端末ごとのデータ転送量のランキングでは，どの端末がどれくらいの量の通信をおこなっているかをランキングで知ることができる．すなわち，回線の占有度合いが高い端末を調べることが可能である．端末ごとの通信相手数のランキングでは，P2P ファイル共有ソフトウェアの使用やワームに感染している可能性の高い端末の発見を支援する．一般に，短時間での通信相手数が多い通信は，P2P ファイル共有ソフトウェアを利用している可能性が高い．加えて，送信元の端末と同一のネットワークセグメントへ多数の通信をおこなっている端末は，ワームに感染している可能性が高い．すなわち，P2P ファイル共有ソフトウェアの利用およびワームの検出は，通信相手数によるランキング抽出が有効と言える．次に，通信記録に保存された IP アドレスを検索する機能を作成する．IP アドレス検索では，端末ごとの通信記録を出力する．トラフィックの利用度が異常な端末について通信記録を調べ，障害の特定をおこなう．

上記に加えて，トラフィックの量的情報の可視化を折れ線グラフによっておこなう．

提案システムを利用して，管理者が障害を発見し原因を究明する流れは以下の通りである．

1. グラフによるトラフィックの監視
2. 異常トラフィックの発見
3. トラフィックの利用度を調査
4. 障害の原因と思われる端末の絞り込み
5. IP アドレス検索で端末の詳細情報を取得
6. 原因端末の特定および，原因究明

4． システム設計

4.1 ハードウェア環境

提案システムでは，以下の性能の機器を用いて実装した．これらは現在の市場で一般的に取り扱われているハードウェアと同等程度の性能であると考える．

- CPU : Intel(R)Core(TM)2Duo CPU E8400 @ 3.00GHz
- Memory : 4.00GB
- Storage : HDD 300GB

4.2 ソフトウェア環境

次節で述べるシステムを，CentOS，Apache，MySQL を用いて実装した．同ソフトウェアのバージョンは以下の通りである．

- OS: CensOS 5.6
- Web Server: Apache 2.2.3
- Database Server: MySQL 5.0.95

4.3 システム構成

提案するシステムは，データベース部・データ取得部・管理インタフェースの 3 つから構成される．提案システムのシステム構成および機能を図 3 に示す．

提案システムのデータベース部では通信記録の保存をおこなう．ここで保存される通信記録は 1 日分と 1 週間分の情報である．データ取得部では，データベース部において保存された通信記録を，1 日分と 1 週間分のトラフィックの量的情報に加工し取得する．管理インタフェースでは，データベース部で保存した通信記録をもとに，ランキング機能や IP アドレス検索機能の作成をおこなう．さらに，データ取得部で取得したトラフィックの量的情報から，ネットワークの全体像をグラフとして可視化する．作成されたシステムは Web ブラウザで閲覧可能である．

それぞれの構成要素について以降の項で説明する．

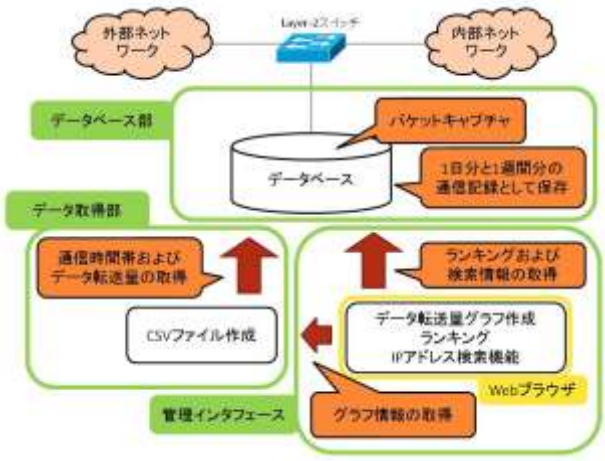

図 3　システム構成・機能

4.3.1 データベース部

データベース部では通信のパケット情報を通信記録として保存する．内部ネットワークと外部ネットワークの境界部にある L2 スイッチからポートミラーリングされたパケットの情報を 5 分ごとにデータベースに保存する．提案システムでは，incoming および outgoing について，それぞれパケットキャプチャをおこなっている．

データベース部において，作成される通信記録は以下の 8 種類である．1 日分の通信記録は，過去 1 日の通信記録を 5 分間隔のフローとして保存している．1 週間分の通信記録では，過去 1 週間の通信記録を 30 分間隔のフローとして保存している．

- 1 日分の TCP 通信（incoming）
- 1 日分の TCP 通信（outgoing）
- 1 日分の UDP 通信（incoming）
- 1 日分の UDP 通信（outgoing）
- 1 週間分の TCP 通信（incoming）
- 1 週間分の TCP 通信（outgoing）
- 1 週間分の UDP 通信（incoming）
- 1 週間分の UDP 通信（outgoing）

4.3.2 データ取得部

データ取得部では，データベース部でデータベースに保存された通信記録から，過去 1 日分と過去 1 週間分のトラフィックの量的情報を取得し，CSV ファイルとして保存する．保存される情報は，通信時間帯，その通信時間帯における incoming のデータ転送量の総計，outgoing のデータ転送量の総計である．ここで取得される通信時間帯は，パケットキャプチャをおこなった時間と同義である．

データ取得部で作成される CSV ファイルの種類は以下の 4 種類である．

- 1 日分の TCP 通信におけるデータ転送量
- 1 日分の UDP 通信におけるデータ転送量
- 1 週間分の TCP 通信におけるデータ転送量
- 1 週間分の UDP 通信におけるデータ転送量

上記の CSV ファイルはデータベース部で作成される通信記録が更新されるたびに新しく作成される．

4.3.3 管理インタフェース

管理インタフェースでは，次の 4 つのシステムを 1 日分および 1 週間分についてそれぞれ作成した．

- データ転送量のグラフによる可視化
- 通信相手数によるランキング作成
- データ転送量によるランキング作成
- IP アドレス検索機能

以下で作成したシステムについて述べる．

データ転送量のグラフによる可視化

Web ブラウザ上でグラフを表示するにあたり，インタープリタ型のプログラミング言語である JavaScript を使用した．グラフの作成には，オープンソースのウェブウィジェットである SIMILE Widgets の Timeplot[6]を使用した．Timeplot は CSV 形式のテキストファイルに対応しており，指定したテキストファイルを自動で読み込

みグラフを作成できる．1 つのグラフ内に複数のグラフを表示することも可能である．

提案システムでは，データ取得部において作成される CSV ファイルを用いて，以下の 4 つのグラフを作成し，それぞれに incoming と outgoing を表示させた．

- 1 日の TCP 通信における 5 分間のデータ転送量
- 1 日の UDP 通信における 5 分間のデータ転送量
- 1 週間の TCP 通信における 30 分間のデータ転送量
- 1 週間の UDP 通信における 30 分間のデータ転送量

表示例として，1 日の UDP 通信における 5 分間のデータ転送量のグラフを図 4 に示す．1 週間の TCP 通信における 30 分間のデータ転送量のグラフを図 5 に示す．図 4 と図 5 はいずれも横軸が時間であり，縦軸がその時間におけるデータ転送量である．

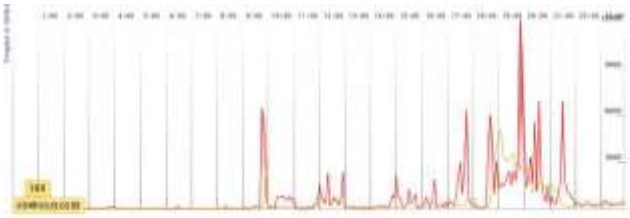

図 4　1 日の UDP 通信における 5 分間のデータ転送量

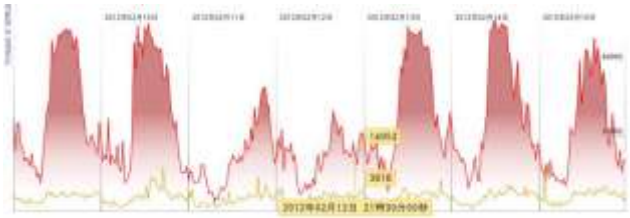

図 5　1 週間の TCP 通信における 30 分間のデータ転送量

ランキングおよび IP アドレス検索機能の作成

ランキングおよび IP アドレス検索は，データベースで SQL 文を実行することによって通信記録の検索を実現できる．提案システムでは，管理インタフェース内の Web サーバ上にある PHP を用いてデータベースに接続して SQL 文を実行する．管理者は作成したいランキングの種類や，検索対象の IP アドレス，時間帯を選択するだけで Web ブラウザを用いて管理インタフェースにアクセスし，通信記録を閲覧できる．

データ転送量によるランキングの管理画面・通信相手数によるランキングの管理画面・IP アドレス検索の管理画面をそれぞれ図 6，図 7 および図 8 に示す．

図 6　データ転送量によるランキングの管理画面

図 7　通信相手数によるランキングの管理画面

図 8　IP アドレス検索の管理画面

データ転送量によるランキングの管理画面では，利用するデータベースのテーブルの種類および incoming と outgoing の選択，ランキングを作成する時間帯の指定が可能である．データ転送量の多い順に送信元 IP アドレスとデータ転送量を 100 件表示する．データ転送量によるランキングの出力例を図 9 に示す．通信相手数によるランキングおよび IP アドレス検索の管理画面においても，同様の選択をおこなうことで結果を出力可能である．通信相手数によるランキングおよび IP アドレス検索の出力例をそれぞれ図 10 と図 11 に示す．

```
[src_ip] = 23.3.
[SUM(packet_len)] = 73662598

[src_ip] = 188.65.
[SUM(packet_len)] = 35876089

[src_ip] = 124.83.
[SUM(packet_len)] = 31626474

[src_ip] = 74.125.
[SUM(packet_len)] = 26348121

[src_ip] = 23.3.
[SUM(packet_len)] = 25980648

[src_ip] = 150.100.
[SUM(packet_len)] = 25000545
```

図 9　データ転送量によるランキングの出力例

```
[dst_ip] = 133.42.
[COUNT(DISTINCT src_ip)] = 136

[dst_ip] = 133.42.
[COUNT(DISTINCT src_ip)] = 96

[dst_ip] = 133.42.
[COUNT(DISTINCT src_ip)] = 61

[dst_ip] = 133.42.
[COUNT(DISTINCT src_ip)] = 59

[dst_ip] = 133.42.
[COUNT(DISTINCT src_ip)] = 57

[dst_ip] = 133.42.
[COUNT(DISTINCT src_ip)] = 54
```

図 10　通信相手数によるランキングの出力例

```
Details : 133.42.

[DataSize]
36590576

[COUNT src_ip]
57

[Connection IPaddress]
110.44.
110.44.
110.44.
110.44.
110.44.
110.44.
110.44.
114.31.
119.27.
```

図 11　IP アドレス検索の出力例

5．運用実験

5.1　実験環境

提案システムを学内ネットワークに導入する運用実験を実施した．本実験では，和歌山大学の対外接続部における L2 スイッチのポートミラーリング機能でパケットキャプチャをおこなった．運用実験は 2012 年 2 月 9 日の 0 時 0 分から 2012 年 2 月 15 日の 23 時 59 分までの 1 週間で実施した．

5.2　検出結果および検証

本実験では 2012 年 2 月 15 日時点のグラフ出力結果において検証する．今回の実験で 1 日分の TCP 通信を表示したグラフと 1 週間分の UDP 通信を表示したグラフに異常トラフィックを発見した．それぞれの検出結果および検証を以下で述べる．

5.2.1　1 日分の TCP 通信を表示したグラフの検出結果および検証

1 日分の TCP 通信を表示したグラフを図 12 に示す．図 12 は横軸が時間であり，縦軸はその時間におけるデータ転送量である．発見した異常トラフィックは図 12 の円で囲まれた outgoing の部分である．

本グラフをもとに，2 月 15 日の 1 時 41 分から 1 時 59 分について，TCP 通信における outgoing の利用度を調査した．調査の結果，データ転送量によるランキングにおいて特出して大量のデータ転送をおこなっている端末を発見した．この結果から，異常トラフィックを発生させている端末は，学内の公開サーバであることが判明した．

次に，発見した端末について IP アドレス検索をおこなった．データ転送量は多いが通信相手数が少ないため，ワームや P2P ファイル共有ソフトの利用によるトラフィックではないことが分かった．異常トラフィック発生時間における通信記録を閲覧した結果，学内ユーザが和歌

山大学外から SSH 通信に対応したポートを利用していることが分かった．

上記の結果から，学内の公開サーバに対して SSH 通信で和歌山大学外からログインし，ファイルを持ち出していることが判明した．すなわち，図 12 で異常トラフィックとして発見された通信は不正通信ではないと言える．ユーザアカウントのクラックによるファイルの持ち出しも考えられるが，これは公開サーバのログイン情報から判断が可能である．この判断はプライバシーの問題が絡むため管理者が適切におこなう必要があると考える．

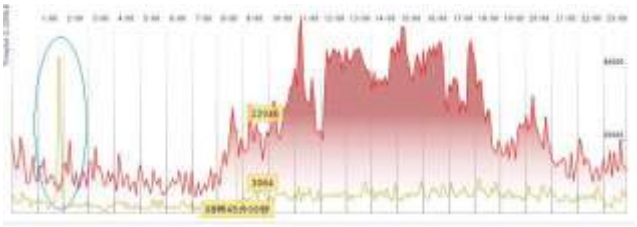

図 12　1 日の TCP 通信におけるデータ転送量のグラフ

5.2.2　1 週間分の UDP 通信を表示したグラフの検出結果および検証

1 週間分の UDP 通信を表示したグラフを図 13 に示す．図 13 は横軸が時間であり，縦軸がその時間におけるデータ転送量である．図 13 の円で囲まれた incoming の部分が発見した異常トラフィックである．

本グラフをもとに，2 月 10 日の 4 時 00 分から 4 時 59 分について，UDP 通信における incoming の利用度を調査した．その結果，多数の端末から情報を取得している端末を発見した．

次に，発見した複数の端末に対してそれぞれ IP アドレス検索をおこなった．検索の結果，不特定多数の通信相手から大量のデータを受信していることが分かった．短時間に不特定多数の通信相手からデータを受信するという動作は，P2P ファイル共有ソフトウェアを利用した典型的な挙動である．すなわち，図 13 で異常トラフィックとして発見された通信は P2P ファイル共有ソフトウェアの利用によるものと推測できる．

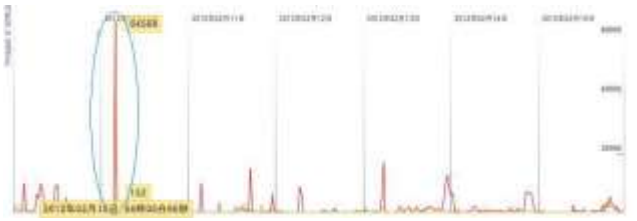

図 13　1 週間の UDP 通信におけるデータ転送量のグラフ

6．評価・考察

6.1　MRTG との比較評価

MRTG はトラフィックの量的情報をグラフとして可視化するソフトウェアである．過去 1 年間について，トラフィックの全体像の把握や，トラフィックの増減傾向から異常を発見できる．しかし 2.3.1 項で述べた通り，MRTG はトラフィックの質的情報を保持しないため，MRTG のみを用いた監視では異常トラフィックを発見することに限界がある．障害の原因究明が困難であるのに加え，発見した異常トラフィックが正規通信か障害かの判断も容易でない．

提案システムは，情報を保持する期間は劣るが，出力するグラフはほぼ同様である．加えて，通信記録を保存し活用することによって MRTG の問題点を克服した．運用実験においても，異常トラフィックの原因となった端末や挙動を特定できた．

以上のことから，提案システムは MRTG に比べ監視できる期間は短いが，障害に対する原因究明において優れていると考える．

6.2　TRAUMAN との比較評価

TRAUMAN は受動的にトラフィックの質的情報を保存するシステムである．TRAUMAN ではデータベースを利用してトラフィックの質的情報を保存しているため，保存情報の検索が可能である．トラフィックの質的情報を利用することで，管理者は障害の原因を究明が可能となる．しかし 2.3.2 項で述べた通り，TRAUMAN はトラフィックの質的情報の保存のみをおこなうシステムのため，管理者が障害の発生を発見することは困難である．上記の問題点に加えて，TRAUMAN ではトラフィックの質的情報をパケット単位で保存しているという点が挙げられる．このため検索効率が悪い．

提案システムでは，トラフィックの量的情報の可視化をおこなったため，トラフィックの全体像を把握が可能である．運用実験においても，トラフィックの増加傾向から異常トラフィックを発見が可能であった．さらに提案システムでは，フロー単位で通信記録を保存することにより，検索効率を向上させた．

以上のことから，提案システムは TRAUMAN に比べ，通信記録利用時の検索効率および監視ネットワーク内の障害発見において優れていると考える．

6.3　考察

本誌では，トラフィックの量的情報と質的情報の両方の側面から，管理者による障害の発見および原因究明を支援するシステムの構築を研究目的とした．

管理者による障害の発見を支援するシステムは，トラフィックの量的情報をグラフとして可視化することにより実現した．このグラフによって，トラフィックの全体像を把握するとともに，トラフィックの増減傾向から障害を発見が可能となる．

障害の原因究明に関しては，発見した障害に対してトラフィックの利用度を調べ，利用度の高い端末についてIPアドレス検索をおこなうことで実現した．端末ごとのデータ転送量のランキングと通信相手数のランキングの2種類のランキングによってトラフィックの利用度が把握できる．端末ごとのデータ転送量のランキングでは，回線の占有度が高い端末の発見が可能である．一方，通信相手数のランキングでは，P2Pファイル共有ソフトウェアの利用やワーム感染の可能性が高い端末を発見できる．IPアドレス検索で，これら端末の通信記録を監視することで障害の特定が可能となる．

上記のことから，提案システムはトラフィックの量的情報と質的情報を用いて，管理者による障害対応を支援するシステムであると考える．事故前提社会が提唱されている現在のネットワーク運用管理において，障害の発見および原因究明を支援する提案システムは有用であると考える．

7． 今後の課題

7.1 表示項目の追加

提案システムでは，通信記録のデータ転送量の総計を監視することによって異常トラフィックを発見し，障害解決への支援をおこなっている．このため，提案システムで発見できる障害は，データ転送量に起因して異常トラフィックを発生させる障害に限られるといった問題がある．

上記の問題は，管理者に提供するグラフを詳細化することで改善が可能だと考える．例えば，通過パケット数や単位時間のフロー数，ショートパケットの数に関するグラフなどである．今後，どのような情報の追加が効果的か調査する．

7.2 管理インタフェースにおけるユーザビリティ向上

実装した管理インタフェースでは，ランキングの作成やIPアドレス検索において，指定する時間やIPアドレスを実際に打ち込む必要があった．提案システムで障害の原因を究明する場合，上記の動作を複数回にわたっておこなう必要があり，非常に手間である．今後はこの手間を省いていく必要がある．例えば，時間指定では，グラフ上の時間軸を指定することで自動的に時間帯を指定できるような改良が有効である．IPアドレスの指定では，ランキングで出力される各IPアドレスに対してリンクを貼り，ワンクリックで対応するIPアドレス検索をおこなう方法が考えられる．

7.3 他の研究との統合

本研究は，障害の発見および原因究明の足がかりとなる研究である．このため，ネットワーク運用管理に関する他の技術との親和性が高いと考える．

現在，我々の研究室において管理者のネットワーク運用管理を支援するさまざまな研究が存在する．P2Pファイル共有ソフトウェア検出システム[7]や，DoS攻撃に対する防御システム[8]，組織内ネットワークにおけるIPアドレスの利用管理システム[9]などである．今後は上記の研究とのシステム統合をおこない，管理者へのさらなるネットワーク運用管理の支援をおこないたい．

8． おわりに

本誌では，トラフィックの量的情報と質的情報の両方の側面から，管理者による障害の発見および原因究明を支援するシステムの構築をおこなった．学内のネットワークでおこなった提案システムの運用実験では，トラフィックの量的情報から異常を発見し，質的情報を用いた障害の原因究明に成功した．今後は，運用実験をおこない管理インタフェースの改善をおこなう．さらに，7.3節で紹介した研究との統合を視野に入れて研究を進めたい．

参考文献

[1] “時期情報セキュリティ基本計画に向けた第1次提言”
2008年6月19日　情報セキュリティ政策会議基本計画検討委員会
http://www.nisc.go.jp/active/kihon/pdf/jiki1teigen.pdf

[2] “事故前提社会　―「次期情報セキュリティ基本計画に向けた第1次提言」について―”
2008年10月　財団法人　関西情報・産業活性化センター情報化推進グループ
http://www.kiis.or.jp/research/kiisquarterly/_userdata/kq002_2.pdf

[3] “「情報セキュリティ総合戦略」の概要”
http://www.meti.go.jp/policy/netsecurity/downloadfiles/Strategy_Summary.pdf

[4] “MRTG:The Multi Router Traffic Grapher”
http://www.mrtg.jp/doc/

[5] 伊与田弘樹　“受動的接続監視に基づくネットワーク利用状況記録システムTRAUMANの構築”
2003年度卒業論文　和歌山大学システム工学部情報通信システム学科

[6] “SIMILE Widgets — Timeplot”
http://www.simile-widgets.org/timeplot/

[7] 阪上竜太，　川橋裕　“ファイル共有ソフトウェア利用検出システムの精度向上と運用支援に関する一考察”
電子情報通信学会　信学技報，vol．111，no．245，　IN2011-80，pp．7-12，　2011年10月．

[8] 澤和晃　“トラフィック監視によるホスト・サービス単位の境界型ネットワーク防御システムの構築”
2010年度卒業論文　和歌山大学システム工学部情報通信システム学科

[9] 吉田祐亮，　高山卓也，　川橋裕　“組織内ネットワークにおける不正利用端末検出および利用位置特定システムの構築”
電子情報通信学会　信学技報，vol．111，　no．245，　IN2011-85，　pp．37-42，　2011年10月．