C-09

IP アドレスのマスク検索を用いた通信記録の管理改善による ネットワーク管理支援システム TRAFL の活用手段の向上

片山 裕太　　川橋 裕
Yuta Katayama　　Yutaka Kawahashi

1. はじめに

インターネットは，教育機関や企業などの組織から個々人に至るまで広く利用され，インターネットを利用したサービスは増加傾向にある．一方で，サービスの増加によるネットワークの多様化，急増するスマートデバイスによるネットワークの複雑化といった，様々な問題が組織のネットワークには存在する．これらの問題が存在する中で，未然に障害を防ぐということは極めて困難である．これを鑑みて「事故前提社会」という概念を経済産業省が提唱している．障害はおこりうるものと考え，障害の発生時に，被害の最小化と局所化，復旧といった作業が迅速に行える環境を構築しておくことが重要となっている．

事故前提社会に対応した環境を実現する手法の 1 つとして，通信の記録を収集する方法が挙げられる．通信記録には通信内容は含まないため，通信の秘匿性は確保される．通信記録を用いることで，管理者は障害の原因や現状を後から調査できる．しかし，膨大な数の通信がおこなわれる中，特定の通信を絞り込むのは難しい．そのため，運用管理を支援するシステムを利用することで、通信記録の管理を補助することが可能である．

2. 用語定義

フロー

フローとは，特定の識別要素が等しいパケットを 1 つのレコードとしてまとめたものである．先行研究の TRAFL では 4 つの識別要素を有する．TRAFL が有する識別要素の詳細を下記に示す．

- 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

本論文では，これらの 4 つの識別要素が一致したパケットのまとまりをフローと定義する．

3. 先行研究　TRAFL

3.1　TRAFL の構成

TRAFL の構成は，ネットワークサイド，サーバサイド，ユーザサイドの 3 つに分類される．TRAFL の構成を図 1 に示す．

ネットワークサイドでは，監視するポジションのスイッチからポートミラーリング機能を活用し，複製したパケットを TRAFL に転送する．監視対象となったネットワーク機器への負担は，複製したパケットの送信のみで済むため，

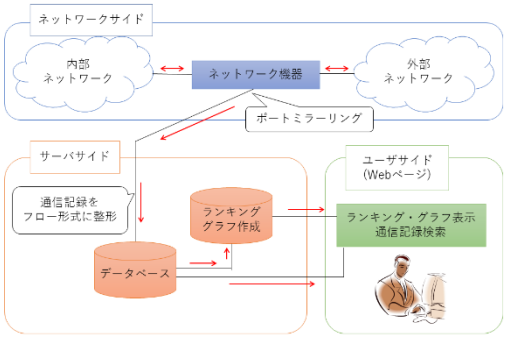

図 1　TRAFL の構成図

NetFlow に比べて負荷が低減する．また，TRAFL が停止した場合にも，ネットワーク機器を通過する通信に影響がないという利点がある．サーバサイドでは，ネットワークサイドから受信したパケットを管理する．しかし，取得したパケットを直接データベースで管理すると，レコード数が膨大となり処理に時間がかかると同時に目的の通信を探す際にも影響が出る．TRAFL ではこの問題に対して，宛先・送信元 IP アドレスとポート番号が一致したものは同一のフローとして加工し，整形後のデータを管理している．ユーザサイドでは，Web ブラウザから TRAFL に保存されたデータを閲覧可能にする．時間ごとのトラフィックを，グラフやランキングで表示し，特定の通信を通信記録から検索するなどの機能により，管理者は容易にネットワークの状況を確認できる．

3.2　問題点

TRAFL では，監視ネットワークのグラフ表示とランキング機能により，ネットワークの異常を感知し原因究明を行うことが可能である．しかし，今相手サービスを利用している端末は何台あるかといった情報を調べることができないという問題がある．グラフ表示やランキング機能を用いて異常な 1 対 1 の通信を確認し，同じ IP アドレスと通信している端末を調査できる．だが，相手サービスの所有する IP アドレスは 1 つとは限らないため，確認できた相手の IP アドレス以外との通信を検索することができない．

4. 提案手法

本研究では，相手サービスを利用する端末やその通信量を確認できるようにするため，IP アドレスの一部にマスクをかけて検索できるようにした．マスク検索により，図 2 のように，IP アドレスのプレフィックスが一致する通信をまとめて確認することができる．

和歌山大学大学院，Wakayama University

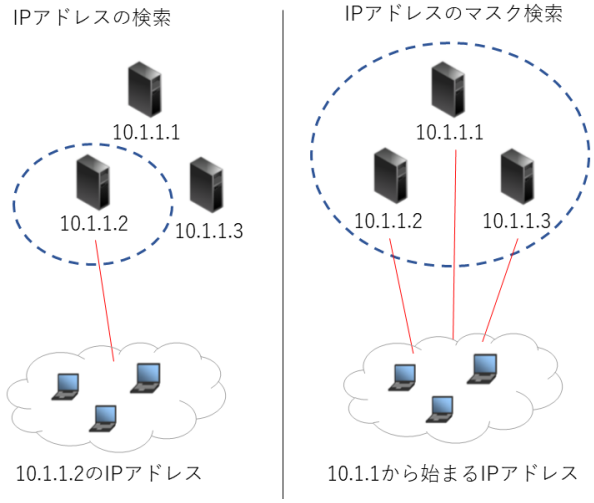

図 3　IP アドレスのマスク検索

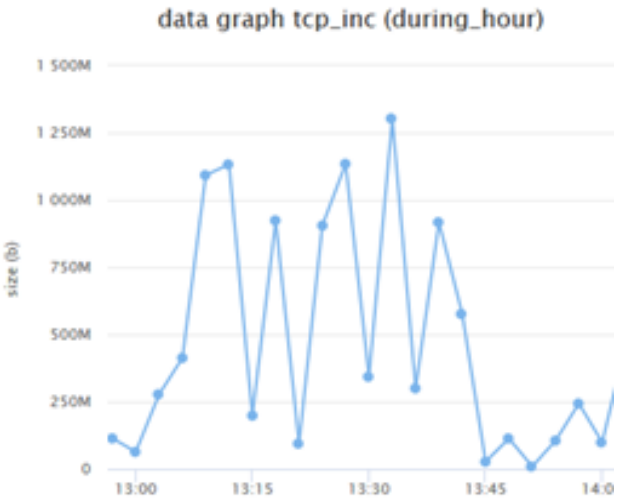

図 2　相手先との通信量グラフ

特定のサブネットマスク範囲が一致した IP アドレスを取得する SQL を入力する必要がある．しかし，IP アドレスのサブネットマスク長は，8 や 16 といった切れ目の良い範囲とは限らない．IP アドレスが 192.168.123.200，サブネットマスク長が 26 の通信の場合，マスク検索では，192.168.123.193 から 192.168.123.254 の範囲の IP アドレスを検索する SQL を入力する必要がある．そのような SQL を記述する場合，正規表現を用いた複雑な SQL になるため現実的ではない．

本研究では，Web ユーザインタフェースを拡張しマスク検索機能を実装する．管理者は Web 上からサブネットマスクの範囲の指定をおこなえば，容易に IP アドレスのマスク検索をおこなうことができる．

IP アドレスのマスク検索をグラフ表示と合わせることにより，通信相手先ごとにグラフを表示可能にする．通信相手先ごとのグラフを確認することで，相手サービスとの通信量や通信量の変化といった通信の特徴を得ることが可能となる．また，特定の端末との通信を切り出して表示することにより，1 つの端末が特定の相手先とどのような通信をおこなうかを確認することができる．

5. 実験

本実験では，構築した提案システムを用いて，実際に 2018 年 1 月 17 日に本学で発生した通信障害の原因調査が可能か実験をおこなった．

同時刻に検知できた通信量の多い相手先と，授業で使われた IP アドレスとの間で行われた通信量グラフを図 2 に示す．

図 3 から，特定の相手先と多量の通信をおこなっていることが確認できた．また，通信相手先は Microsoft 社であった．これらの情報から，BYOD の端末で WindowsUpdate が発生したと考えられる．WindowsOS の月例アップデートは日本時間で毎月第 2 週の水曜日におこなわれる．この関係上，水曜日に授業をおこなうことは難しいと判断できる．また，今回の実験データは第 3 水曜日のため，1 週間の期間があってもアップデートをおこなわない所有者が多数存在することがわかる．稚拙な意見ではあるが，自宅でおこなう課題といった，端末の自宅利用の機会を増やす必要があるだろう．

本研究を用いることで，障害の原因を具体的な数値で確認できたほか，運用の結果といった情報を確認することができた．

6. 今後の課題

本研究を用いることで相手先ごとに通信の切り分けが可能になった．しかし，特定の通信相手とのトラフィックグラフを生成する処理については，非常に時間を要する結果となった．データベースの検索をおこなうプログラムの改善や，グラフ表示の際，ある程度のデータの加工処理を予めおこなっておくといった方法を考えている．また本研究を用いて，一定期間の相手先との通信頻度を確認できるようにし，通信頻度から相手先の信頼性を判断する方法を考えている．

参考文献

[1] 経済産業省
"「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
[2] 釼本　倫章　"トラフィックグラフとフローに基づくネットワーク管理支援システム TRAFL の構築と運用"
2015 年度卒業論文　和歌山大学大学院システム工学研究科
[3] 陰地　健太　"トラフィックとフロー数の検索情報に基づいたネットワーク障害の調査支援するための TRAFL の拡張"
2016 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
[4] 小原　康平　"TRAFL ランキング機能のインタフェース見直しおよび機能拡張"
2016 年度卒業論文　和歌山大学大学院システム工学研究科
[9] "Cisco IOS NetFlow"'
https://www.cisco.com/c/ja_jp/products/ios-nx-os-software/ios-netflow/index html