# 大学ネットワークにおけるサブネット管理者との ネットワークセキュリティ・トラフィック情報の共有

細川 達己，金子 康樹

慶應義塾インフォメーションテクノロジーセンター本部

hosokawa@keio.jp, yasuki.kaneko@keio.jp

# Sharing Network Security and Traffic Information with Subnet Administrators in University Network

Tatsumi Hosokawa, Yasuki Kaneko

Information Technology Center, Keio University

**概要**

慶應義塾においては、歴史的に多くのサブネットが存在しているが、昨今セキュリティ面での問題が深刻化している。その対策の 1 つとして、L7 ファイアウォールや基幹ルータなどから提供されるトラフィックのデータを格納し、高速な検索を可能とするデータベースと、そのデータベースを用いて異常な動作を抽出するためのトラフィック情報提供システムを構築した。

2017 年 1 月から、本システムを利用して、サブネット毎に分類されたトラフィック情報を、直接サブネット管理者に配信する機能の試験運用を開始した。まだ小規模な試験運用のため、顕著な成果は出ていないが、今後さらに広範囲なサブネットに提供先を拡張することで、管理者のセキュリティ意識やスキル向上に効果を発揮することを期待している。

## 1 本学のネットワークの現状

本学では比較的初期からインターネットに接続していたためか、特に理工学部のある矢上キャンパスを中心に、学内ネットワークが次のような特徴を持つ傾向がある[1]。

- 多くの研究室や部門がパブリックアドレスのサブネットを割り当てられている。
- そのサブネット上で様々なサーバやクライアントマシン、複合機、ファイルサーバ等を運用している。
- 昨今の状況から、そのようなサーバやクライアントマシン、複合機、ファイルサーバ等でセキュリティインシデントが頻発している。
- インシデント発生時に、研究室や部門のネットワーク管理者への連絡先が不明だったり、連絡がつかなかったりする。
- 仮に連絡がついても、管理者のスキル不足などの原因で十分な対応が取られない場合がある。
- 学生がサブネット管理者となることが多いが、学生は数年で卒業・修了してしまうことが多く、その際に知識やノウハウなどが継承されないケースが散見される。

これらの問題が本学固有の問題かというと、たとえば 2013 年頃からしばしばメディアに取り上げられている、複合機等からの情報漏洩などに関する報道を見るかぎり[1]、似た問題を抱えた大学も多いと想像できる。

これらの問題に対して、本学では次のような対応を今まで行ってきた。

- Web サイトやメールサーバなど、わざわざ自分でサーバを立ち上げる必要性が低下したサービスに関しては、学外のホスティングサービスや SaaS のクラウドサービスへの移行を支援する。
- L7 ファイアウォールや基幹ルータ等の出す情報を分析して、概要や警告を提供するシステムを構築する。
- 複合機、ファイルサーバなどの調査を行

[1] 本学の湘南藤沢キャンパスと、それ以外のキャンパスとはネットワークの運用体制が異なる。本稿の内容は、主に湘南藤沢キャンパス以外のキャンパスにおけるネットワークの運用管理に関するものである。

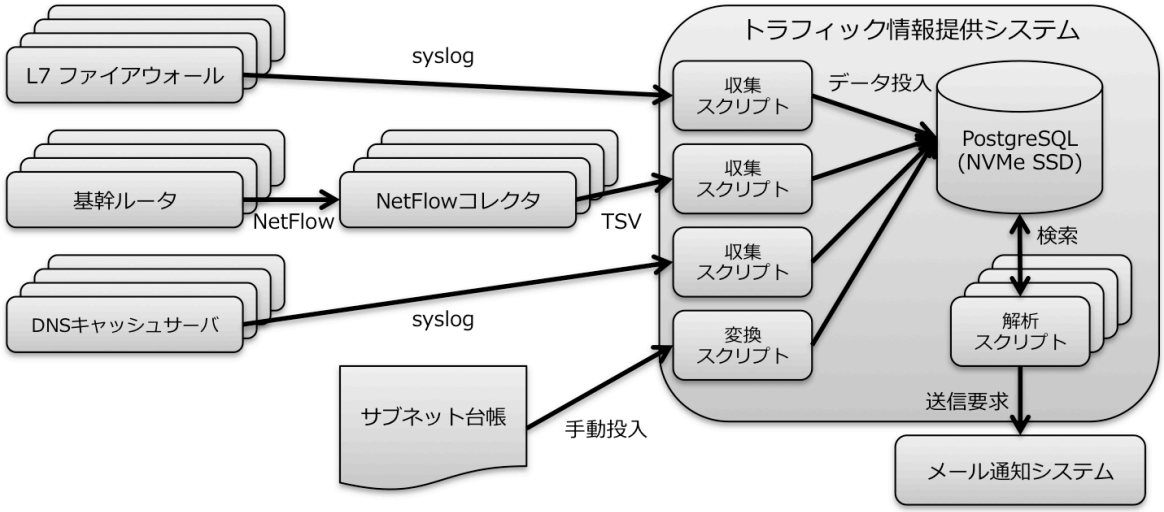



図 1　トラフィック情報提供システムの構成概要

い、脆弱な設定の機器の存在するサブネット管理者に警告する。

- インシデント発生時の、サブネット管理者への連絡体制を整備する。

## 2　トラフィック情報提供システム

以上の対策のうち、「L7 ファイアウォールや基幹ルータ等の出す情報を分析して、概要や警告を提供するシステム」に関して紹介する。

2003 年、本学ではファイル共有ソフトウェアの適切な利用に関するポリシーを決定した[2]。その概要は次の通りである。

- 学内で、特定のファイル共有ソフトを利用するにはインフォメーションテクノロジーセンター（以下 ITC）に対する申請が必要である。
- 利用目的は研究・教育目的に限る。
- 申請のない利用はしてはならない。
- これらの目的を達成するため、ITC は適切なネットワークの監視を行う。
- 問題があれば ITC はサブネット管理者に調査・対象を依頼する。
- 対処が不十分な場合は、ITC は通信制限を行うことができる。

このポリシーに基づきネットワークを運用していくため、ITC では、ルータの ACL ログからファイル共有ソフトの利用が疑われるトラフィックを検出するシステムを構築した。

このシステムは、さらに汎用的なセキュリティ情報収集・分析目的のために機能強化が行われた。何度かの大きな改修を重ね、トラフィックデータのソースはルータの ACL ログから L7 ファイアウォールに移行し、さらに DNS キャッシュサーバのログや、基幹ルータの NetFlow 情報なども格納するように強化された。現状のシステム構成の概要を図 1 に示す

現在では、1 日あたり約 2 億行のデータが、発生から数分以内に SQL データベースに格納され、即座に高速な検索が可能な体制となっている。このデータベースは、高速な NVMe SSD 上にデータを持つ PostgreSQL で実現されている。このサーバのハードウェア、ソフトウェア仕様を表 1 に示す。

| | |
|---|---|
| CPU | Intel Xeon E5-2407 (4Core, 2.20GHz) ×2 |
| メモリ | 24GB |
| SSD | Intel SSD DC P3600 1.6TB (SSDPEDME016T4) |
| OS | FreeBSD 10.3-RELEASE |
| RDBMS | PostgreSQL 9.5.3 |

表 1 トラフィック情報提供システムサーバ仕様

このデータベース上で、平均的な L7 ファイアウォールによるトラフィック情報 1 日分（約 8000 万件）に対して、学内の宛先 IPv4 アドレス全て（ネットマスク 16 ビット= 65,536 件）毎に、すべてのトラフィック情報を検索した場合の、検索時間（ms 単位）の分布を示したグラフを図 2 に示す。

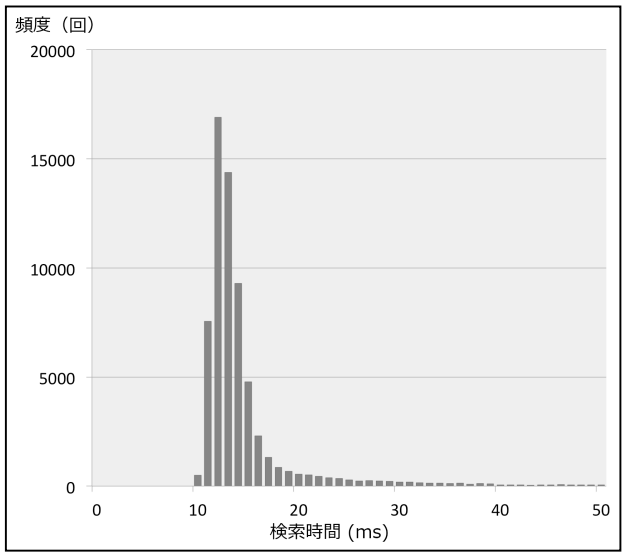



図 2　トラフィックデータベースの検索性能

グラフ上は検索時間 50ms までのデータを示しているが、この範囲内に全データの 97.6%が含まれている。検索時間の全体平均は 17.3ms である（なおこの例では、トラフィック情報の収集スクリプト等を実行した状態で、性能測定を行っている。検索時間は、psql コマンドで出力先に/dev/null を指定した状態で、timing メタコマンドで測定を行った）。改修時、SQL データベース以外の採用も検討したが、このように性能的にまだ十分単体の PostgreSQL でカバー可能であることから見送った。

トラフィック情報提供システムのサーバ上では、多くの解析スクリプトが動作しており、この高速なトラフィックデータベースに数多くのクエリを送ることで、様々なインシデントに繋がる情報を抽出し、提供している。

また、インシデント発生時は、このデータベースを検索することで、同様の問題が発生していないかどうか、あるいは被害が拡散していないかどうか、等の検索を非常に効率的に行うことが可能である。さらに必要であればそこで得られた知見を解析スクリプトに反映することで、情報抽出能力の向上に役立てている。

また、外部機関から提供される DNS ブラックリスト情報なども、随時このデータベースに追加している。

## 3　サブネットデータベースの統合

2016 年に行った本システムの大規模な改修では、大幅な性能向上を実現すると同時に、IPv4/IPv6 アドレスとネットマスクの包含関係による検索が可能となった（この機能は PostgreSQL の INET データ型と包含関係演算子を利用している）。

現在、学内に登録されているサブネット数は、IPv4 が約 660 個、IPv6 が約 190 個ある。これらのサブネット情報とサブネット管理者の情報を、トラフィック情報警告システムの PostgreSQL データベースに格納することで、以前から構想していた「システムの出す警告や各種情報を、サブネット管理者ごとに仕分けして提供する」システムの実現が非常に容易なものとなった。

これは、サブネット管理者に対して、自分の管理下のネットワークで何が起こっているかを直接可視化することによって、次の目的を実現することを意図していたものである。

- サブネット管理者のセキュリティ方面の意識向上とスキル向上
- 時間がかかりがちなサブネット管理者への連絡パスの簡素化（少なくとも、ITC スタッフの不在時でもサブネット管理者に直接情報が提供される）

## 4　試験運用開始

2017 年 1 月 26 日から、理工学部の矢上キャンパスを中心に、ITC が任意の申込みを募る形で、本システムの試験運用を開始した。矢上キャンパスでは、サブネット管理者などを対象に、ネットワーク管理に関する講習会を不定期に開催しているが、その席などでも、試験運用開始に関する広報を行った。

試験運用を公開するにあたって、システムの全機能を公開するのではなく、まずは偽陽性の検知が比較的少なく、また理解が容易であると考えられる警告や情報提供に限って運用を開始することとした。一般の研究室に対して提供される警告・情報提供は以下のとおりである。

- 学外向け SSH, RDP, SMTP セッション数の異常上昇（随時）
- L7 ファイアウォールが検出した学外への脅威トラフィック（随時、毎日）
- L7 ファイアウォールが識別不能としたトラフィックに関する各種情報（毎日）
- 非常に大容量の通信を行っているホスト

とその通信プロトコル等に関する情報（4時間ごと）

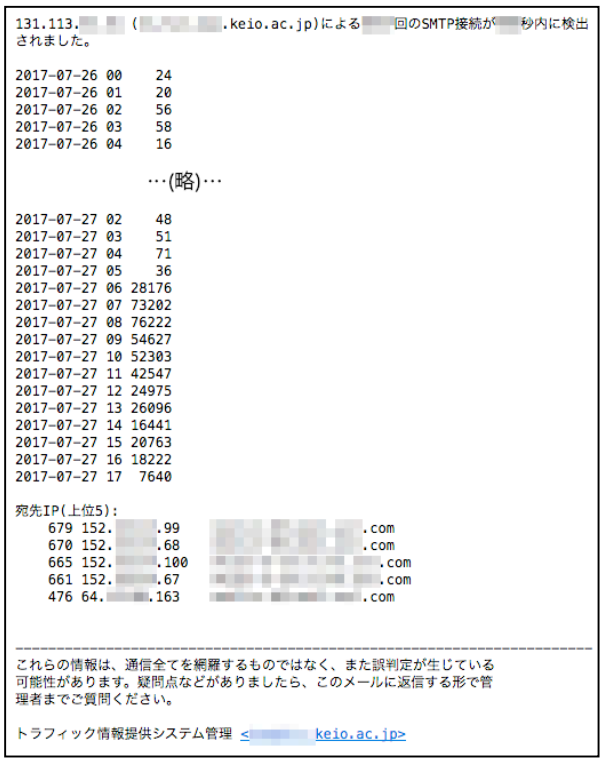
この情報提供メールの例を図 3 に示す。これは学内のある IP アドレスに対して、SMTP 通信が急増したことを知らせるメールで、過去 2 日間の 1 時間毎の SMTP 通信量の推移と、通信相手の IP アドレス上位 5 位を示している。

この例では、7 月 27 日の朝 6 時台から、明らかに異常な量の SMTP 通信が発生していることが容易に見てとることができる。

2017 年 9 月現在、理工学部矢上キャンパスを中心とした 28 の組織（主に研究室）が利用を開始している。これらの組織が利用しているサブネットの合計は、IPv4 が約 180 個、IPv6 が約 80 個である。組織数が少ない割に多くのネットがカバーされているのは、大量のサブネットを管理している ITC が含まれるためであり、これを除くと IPv4 が約 60 個。IPv6 が約 10 個となる（全学の IPv4 アドレスのカバー率としては、未だ約 5%にすぎない）。

## 5　導入の効果

導入の効果であるが、まず「トラフィック情報提供システム」自体は、2003 年の導入から実に 14 年が経過しており、その間多くのインシデントを



131.113.[redacted] ([redacted].keio.ac.jp)による[redacted]回のSMTP接続が[redacted]秒内に検出されました。

2017-07-26 00　24
2017-07-26 01　20
2017-07-26 02　56
2017-07-26 03　58
2017-07-26 04　16

…(略)…

2017-07-27 02　48
2017-07-27 03　51
2017-07-27 04　71
2017-07-27 05　36
2017-07-27 06 28176
2017-07-27 07 73202
2017-07-27 08 76222
2017-07-27 09 54627
2017-07-27 10 52303
2017-07-27 11 42547
2017-07-27 12 24975
2017-07-27 13 26096
2017-07-27 14 16441
2017-07-27 15 20763
2017-07-27 16 18222
2017-07-27 17　7640

宛先IP(上位5):
679 152.[redacted].99 [redacted].com
670 152.[redacted].68 [redacted].com
665 152.[redacted].100 [redacted].com
661 152.[redacted].67 [redacted].com
476 64.[redacted].163 [redacted].com

これらの情報は、通信全てを網羅するものではなく、また誤判定が生じている可能性があります。疑問点などがありましたら、このメールに返信する形で管理者までご質問ください。

トラフィック情報提供システム管理 <[redacted]keio.ac.jp>

図 3　大量 SMTP 通信情報メールの例

発見し、また外部組織からのインシデント情報提供に対して、迅速な影響範囲の調査や原因究明、再発防止に役立ってきたという実績がある。

一方で、このトラフィック情報のサブネット管理者に対する直接提供に関しては、従来は ITC からサブネット管理者に対して、インシデントに関する連絡をする一方通行だったものが、逆にサブネット管理者から「この情報は問題のあるものか」という質問がしばしば聞かれるようになったことは一つの成果であるといえる。しかし、全体的には未だ大きな成果を上げているとは言い難い。これにはいくつかの原因が考えられる。

- 試験運用段階ということもあり、まだカバーしている IP アドレスの範囲は、全学のネットワークに比してごく狭い範囲である（先述の通り、ITC を除いた IPv4 アドレスのカバー率は約 5%）。
- 任意で参加研究室を募っているため、一般的にセキュリティ意識の高いサブネットや、最近何かインシデントを起こしたことがあるために、危機意識が強くなっているサブネットの参加が多い。

このため、今後理工学部でより広い範囲に参加を募ったり、あるいは他キャンパスに募集を広げたりすることで、対象となるサブネットを広げていけば、より顕著な導入効果が現れてくることもあるのではないかと考えている。

## 6　今後の課題

本システムに関する今後の課題として、以下の内容を検討している。

- メールでの情報提供に代えて、何らかの Web 系のアプリケーションで情報提供とサポートを行う。タスク管理ツールの他、LMS 系のツールも採用を検討中である。
- さらに広範囲のサブネット管理者に、試験運用への参加を呼びかける。
- 現状では NetFlow のデータをあまり活用できていないので、NetFlow を含めた解析を行うようにシステムを改良する。
- PostgreSQL 9.6 以降にアップグレードすることで、シーケンシャルスキャン、結合、集約の並列処理による検索の高速化を図る。

- さらに多様な解析の実験を行い、広く有用なものはサブネット管理者にも提供していく。

## 参考文献


[1] 日本経済新聞、「複合機の情報、ネットで丸見え、東大など、コピーやスキャンした文書、内部に蓄積」、日本経済新聞 2013 年 11 月 8 日付朝刊、p.43、2013.

[2] 慶應義塾インフォメーションテクノロジーセンター、「ファイル共有ソフトウェアについて」、http://www.itc.keio.ac.jp/ja/software_fileshare.html、2013.