「トラフィック情報提供システム」の機能強化

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

Enhancement of “Traffic Information Providing System”

Tatsumi Hosokawa, Yasuki Kaneko

Information Technology Center, Keio University

概要

慶應義塾インフォメーションテクノロジーセンター（以下 ITC）は、ITC のセキュリティ担当スタッフや学内の各サブネット管理者に対して、ネットワークセキュリティやトラフィックに関する情報を提供するためのシステム「トラフィック情報提供システム」を運用している。2018 年 2 月に本システムのハードウェアをリプレースする際にシステムの大幅な改修を行い、これによってインシデントの発見や対応に関する本システムの有用性が大きく向上した。一方、それによって解決が困難な新しい課題も見えてきている。

1 はじめに

慶應義塾インフォメーションテクノロジーセンター（以下 ITC）は、ネットワークセキュリティやトラフィックに関する情報を収集・分析し、それを共有するための「トラフィック情報提供システム」を 2003 年から運用している。

このシステムはもともと、ITC のセキュリティ担当スタッフに対して、インシデント発見・対応のための情報を提供することが目的であった。しかし 2016 年から 2017 年にかけて、学内の各サブネット管理者に対して、管理対象のサブネットに関するネットワークトラフィックやセキュリティに関する情報を提供し、迅速なインシデントに関する連絡を入れることを一つの目的とした、大規模改修を行った[1]。

さらに 2018 年の 2 月、本システムのハードウェアをリプレース（ハードウェアとしては 2003 年の最初の導入から 5 世代目にあたる）し、それにともない前システムにおいて課題となっていた問題点のいくつかについて、再び大規模な改修を行った。本稿ではこの最新の改修内容とその効果について報告する。

2 システムの仕様

新しいサーバのハードウェアは、改修前と同様に 1 台の PC サーバであり、主なスペックは以下の通りである。

- CPU：Intel Xeon Silver 4114（10 コア 2.2GHz）×2
- メモリ：96GB
- SSD : NVMe PCIe 4TB×2（DB 用）、NVMe PCIe 1.6TB×1（作業用）、DOM SATA 64GB×1（起動用）
- HDD：SATA RAID 16TB（バックアップ用）
- NIC：1000Base-T×2
- OS：FreeBSD 11
- データベース: PostgreSQL 10

3 主な機能

「トラフィック情報提供システム」の主な機能を紹介する。

3.1 トラフィック・セキュリティ情報の取得

本システムは、学内にある L7 ファイアウォールのログや基幹ルータからの Netflow 情報、DNS サーバのクエリログ等を収集し、データベースに格納することで横断的な高速検索を可能とする。

システムの構成概要を図 1 に示す。ログの発生から 2 分程度（Netflow は 5 分程度）で、データベースから SQL で検索可能となる。

3.2 情報の解析・共有

データベースに格納された情報に対して様々な検索を行うスクリプトが定期的に実行される。その解析結果のうちの一部分は、学内のサブネット

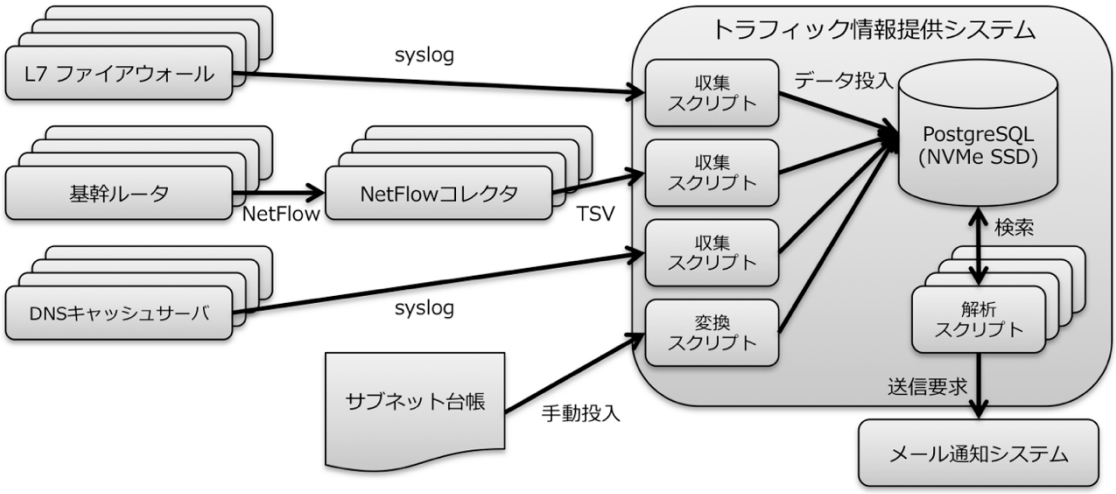

図 1　トラフィック情報提供システムの構成概要

管理者に対してメールで共有される。

現在、サブネット管理者に対して提供している情報は当該サブネットに関するデータと全学的な統計データのみであり、具体的には以下の通りである。

- 学外向けの脅威検出情報
- 一定頻度以上の学外向け SSH, RDP, SMTP 通信要求に関する情報
- 大容量通信ホストの情報とその通信に関する統計情報
- L7 ファイアウォールで特定不能な通信に関する情報

また、ITC のセキュリティ担当のスタッフには、上記以外にも様々な情報や警告を提供している。

4　最新の改修点

2018 年 2 月、本システムのハードウェアをリプレースし、大幅な改修を行った。ここでは今回の主な改修点を紹介する。

4.1　ハードウェア全般の強化

旧システムで特に不足していたのは、CPU のコア数(4 コア)とデータベース用 SSD 容量(1.6TB)であった。今回はこれらをそれぞれ 20 コア、8TB に増強することで多くのジョブを回すことを可能とし、またログデータを高速検索が可能なデータベース上により長期間残すことが可能となった。

4.2　高速・低遅延データ格納

旧システムでは syslog などで取得するデータの処理に以下の問題を持っていた。

- 一次記録場所としてハードディスクを利用したため、物理的なランダムアクセスを多発していた。
- syslog ファイルの末尾を監視して、追加される新データを取得し続ける構成だったため、効率が悪く、異常発生時のリカバリも不十分であった。
- L7 ファイアウォールなどの標準 syslog フォーマットに本システムでは不要なデータが多く、またデータベースに格納するための文字列処理が複雑であったため、無駄が多かった。

これらの問題に関して、今回の改修で、次に示す改善を行った。

- 一次記録場所として作業用の SSD を用意し、ハードディスクはバックアップ専用とした。
- rsyslogd のテンプレート機能を活用し、「毎分ごとに別のファイルにログを記録する」構成に変更した。このように分割された各ファイルに対する DB 格納作業状況を管理することで、処理の効率化と同時に、異常発生時のリカバリも容易となった。
  これによって、以前はログ発生から 5 分以上かかっていた DB への記録が 2 分以内に完了するようになった。
- syslog ソース側で適切にカスタムログフォーマットを設定し、不要な項目の送信を抑制した上で、PostgreSQL にインポートしやすい形式（TSV）に設定することで、文字列パースのコストを抑えられるようにした。

4.3　記録データ項目追加

以前は L7 ファイアウォールの標準 syslog ログ

フォーマットを用いていたが、それには以下の項目が含まれていなかったため、カスタムログフォーマット化する際に追加した。

- セッション開始時刻
- セッション持続時間
- 送信パケット数
- 受信パケット数
- 送信バイト数
- 受信バイト数

ログ生成時刻、総パケット数、総バイト数は以前から記録していたが、それらを補完するデータとしてこれらの項目は機能する。

4.4 PostgreSQL 10 新機能の活用（宣言的パーティション・パラレルクエリ）

本システムにおいては、2016 年から「1 日分のデータは 1 つのテーブルに格納する」という構成をとっていた。これは、PostgreSQL において単一のテーブルにデータを置いて、新しいデータを末尾に追加して古いデータを先頭から消していくような FIFO 更新を続けると、消したはずのデータ領域が回収されずに残ってしまうためである。

これに対して、たとえば日付毎にテーブルを分割し、古いデータをテーブルごと消去する構成にすれば、消去された領域は瞬時に回収される構成にできるが、一方で日付をまたがった検索・集計が難しくなるという問題があった。

今回の更新で新たに導入された PostgreSQL 10 には「宣言的パーティション」という機能が導入されている。これは、テーブル中の特定のパラメータの値やその範囲を振り分け基準として、複数のテーブルを 1 つのテーブルのように見せる機能である（以前も SP を用いて同様の機能を実現する事は可能だったが、性能のオーバーヘッドが非常に大きかった）。

そこで、タイムスタンプを振り分け基準とした宣言的パーティションを用いることで、以前のバージョンでは困難だった、複数の日付にまたがる検索が簡単に行うことができるようになった。また、データ格納時には、日付が改まる午前 0 時近くのデータを、どちらの日付のテーブルに入れるべきかという処理の判断が正確になった。

また、PostgreSQL 10 では、複数プロセスに検索ジョブを分割して割り振る、「パラレルクエリ」機能も追加された。本機能はマルチコアシステムを前提としたものであり、今回の新ハードウェアで増強された CPU のコア数を、検索性能の大幅な向上に役立てることができるようになった。

4.5 選択的リストア機能

実際にインシデントが発生し、詳細な調査が必要となった場合には、かなり以前のデータまで検索する必要が生じることがある。一方で、高速な検索が可能な SSD の容量は限られており、長期間分のデータのリストアは難しい。

このような場合に、ハードディスクに保存したバックアップ用データやソースの syslog データから、指定した正規表現にマッチした行のみを SSD 上のデータベース領域にリストアする機能を追加した。

4.6 DNS・IP アドレスブラックリスト機能

学外のセキュリティ機関等から提供される、マルウェアに関するインディケーター情報を活用するため、DNS・IP アドレスに対するブラックリスト機能を追加した。

DNS に関しては FQDN の完全一致もしくは後方部分一致のワイルドカードが、IP アドレスに関しては完全一致の IPv4/IPv6 アドレスをブラックリストに登録可能である。

ブラックリストにマッチしたアクセスが検出された場合は直ちに、ITC のセキュリティ担当スタッフに通知される。

なお、部分一致検索は誤検知を多く含むため、ホワイトリストの登録も可能となっている。

4.7 DNS 更新履歴監視機能

最近、無料ダイナミック DNS サーバの検索結果を動作のトリガーに利用するマルウェアが多く存在する（リゾルブ結果をプライベートやリンクローカルアドレス等から C2 サーバの実パブリックアドレスに更新する等）。

ところが、現状として DNS はクエリログのみの取得・記録であり、レスポンスのログは取得していない。これを実現するには DNS インフラに比較的大きな手を入れる必要があるためである。そこで、ブラックリストにある特定の学外ドメインの DNS 情報を Google public DNS 経由で定期的に収集し、更新があった場合に管理者に知らせる機能を追加した。

外部の DNS サーバを利用するのは、本学内からの検索であることを隠すためである。

4.8 JSON 形式のレポート

本システムのデータを、分散型 SOC の実現に向けた共同研究において、セキュリティ情報ソースの一つとしても利用し始めている[2]。その過程で

脅威情報などを JSON 形式でエクスポート可能とする機能を追加した。データは PostgreSQL の JSONB 型でデータベースに格納される。

現在進行中の Google Classroom を用いたサブネット管理者との情報共有・コミュニケーション用システムの開発にも、この機能を利用している。

5　性能

5.1　データ格納性能

データの格納に関しては、意味のあるベンチマークテストを行うことが難しい。実績としては、大規模なスキャンの影響で、通常の日の 5〜6 倍に相当する 1 日に約 12 億 4000 万行（平均毎秒約 14,300 行）のデータ格納を行った日があったが、何の問題もなくシステムは動作し続けており、検索性能にも大きな影響は見られなかった。

5.2　データ検索性能

データ検索性能も、様々な要因に大きく影響されるため、正確な使用感を反映した測定をすることは非常に難しい。

現行のシステムでは、L7 ファイアウォールのセッションログデータを約 70 億件、データベースに格納しているが、そこをソースとするセッションデータが 1 件以上記録されていた学内の IP アドレスのサンプル約 1,300 個について、ソース IP アドレスごとに合計セッション数を検索するクエリを投げ、横軸に検索結果数、縦軸に検索時間（秒）を取ったグラフを図 2 に示す（検索結果数を示す横軸は対数目盛にしてある）。

全体を見ると、検索結果数 100 万件弱を境に別のグラフになっているようにも見えるが、その近辺で、PostgreSQL のオプティマイザが「1 プロセスの index only scan」から、パラレルクエリを用いた「7 プロセスの bitmap index scan」に検索プランを変更しているのが原因であると思われる。

数字としては、概ね検索結果が 1 万件程度であれば数秒以内に、1,000 万件でも 10 分以内に検索できている。そしてこのグラフ中で最大の検索結果が 5,300 万件の場合でも、約 15 分で検索が完了している。

なお、検索結果が 0 個だった場合の検索所要時間は、平均 36.8ms（標準偏差 20.1ms、サンプル数

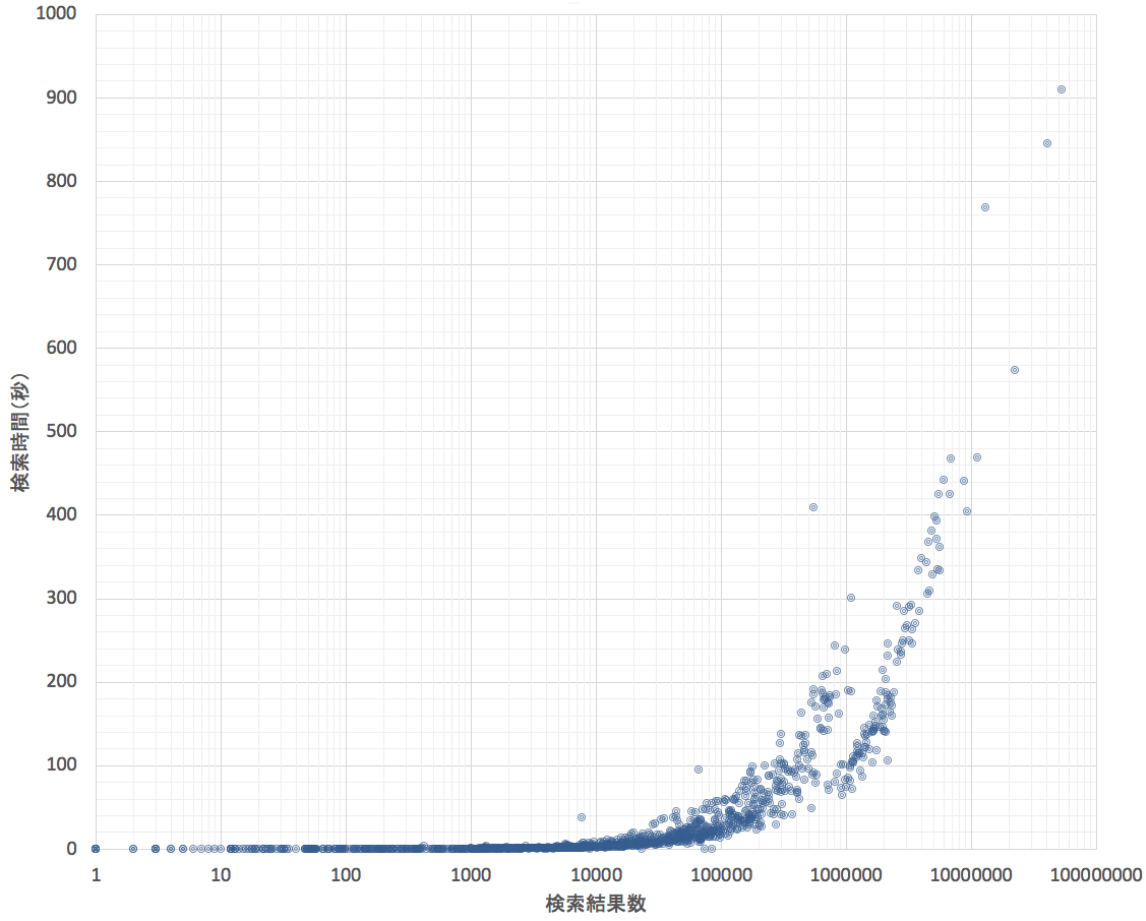

図 2　検索結果数と検索時間との関係

約 23,300 件）であった。

実際の利用時は、これに期間などの他の条件を加えて検索することが多いため、ほとんどの単純な検索は瞬時に結果が出てくる。

6 改修の効果

今回の改修により、インシデントの発見や対応のための作業を効率化する、次のような効果があった。

- 高速かつ複雑なデータ検索が可能な範囲が広がり、計算能力も増強された（ハードウェア増強の効果）ことで、以前よりも長期間のデータに対して、インシデントの探索を行うことが可能となった。
- 多くの情報ソースを追加することが可能となり、また大規模スキャンによる突発的な大量アクセス増加にも、十分な性能で対応可能であった（高速・低遅延データ格納の効果）。
- 複数日にまたがるデータの検索が容易となり（宣言的パーティションの効果）、また効率化された（パラレルクエリの効果）ため、学外のセキュリティ機関等からのインディケーター情報に対する対応が非常に容易となった。また SQL が書きやすくなったことで、新機能の追加が容易となった。
- 以前はログ生成日時だけで時間を判断していたが、セッション開始時間、持続時間が入ったことで、より正確なインシデント調査が可能となった。また、パケット数やバイト数を総数ではなく送受信別々に記録できるようになったことで、主に学外から学内にデータが流れたのか、それとも逆か、などの問題を適切に判断できるようになった（記録データ項目追加の効果）。
- インシデント調査のためにかなり古い情報に対して複雑な検索を行いたい場合も、遡及が容易となった（選択的リストア機能の効果）。
- ホスト名や IP アドレスを含むインディケーター情報やその他関連情報、そして学内で発見されたマルウェアの分析情報等から、他のマルウェアを早期発見できるようになった（ブラックリスト機能の効果）。
- マルウェアの動作トリガーとして機能している思われる DNS の更新を直ちに知ることが可能となった（DNS 更新監視機能の効果）。
- 分散 SOC 関連実験やサブネット管理者との新しい情報共有システムの開発において、脅威情報のエクスポートが容易となった（JSON 形式レポート機能の効果）

7 近日中に顕在化が予想される問題点

昨今の傾向から想定して、近日中に次のような問題が発生する、もしくはすでに発生していて気がついていない、という事を予想している。

1. マルウェア検出に重要な役目を果たす情報の中で数少ない非暗号化通信の一つであった DNS が、DNS over TLS/DTLS や DNS over HTTPS 等の技術で暗号化されつつあるため、今後のさらなる検出率の低下が予想される。
2. 既に予兆はあるが、マルウェア自身が 443/tcp を用いる DNS over HTTPS のリゾルバを自前で持つようになった場合、OP53B（これも機微な問題を含むので本学では実施していない）的な手段でも副作用が強すぎて防ぐことができない。

以上の理由で、今後数年にわたって、本システムが現在の能力を発揮し続けられる可能性は低い。DNS に関しては今後の趨勢を見守りたい。

8 今後の課題

その他、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。

- Google Classroom を用いた情報共有・コミュニケーションシステムを実現し、より広い範囲のサブネット管理者とより情報共有を容易とする。
- 複数ディスクへのアクセスをより分散させる。複数の SSD をシステムに積んでいるが、RAID ではなく、テーブルスペースで制御している。このアクセスが片方のディスクに集中する傾向がある。これを平均化したい。
- データベースストレージのさらなる高速化と大容量化を実現する。本システムの性能における現在のボトルネックは SSD の性能であり、より多くのデータを検索するのに必要なのは SSD の容量である。
- L7 ファイアウォール、Netflow、DNS 等とは全く異なるセキュリティ情報のソースを追加する。L7 ファイアウォールや Netflow で取得できる情報には限りがあり、また DNS は先述のように、近日中に有用性が低下していくと考

えられる。何らかの他の情報との相互補完が必要である。

- 専用の C2 サーバを用意されるケース等を想定すると、DNS のアクティブな更新履歴監視は無力であるどころか有害である。DNS インフラの改修に合わせて、パッシブな DNS レスポンスログの記録を実現したい。

参考文献

[1] 細川達己，金子康樹、「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」、大学 ICT 推進協議会 2017 年次大会、2017、https://reg.axies.jp/pdf2017/FC3-3.pdf

[2] 近藤賢郎, 細川達己, 重本倫宏, 藤井康広, 中村修「分散型 SOC アーキテクチャに基づいた複数組織間におけるセキュリティ・オペレーションの連携」、マルチメディア，分散，協調とモバイル(DICOMO2018)シンポジウム、2018.