5X-01

小規模ネットワークの稼働ログと構成の可視化*

渡邉 公輔†, 北 直樹‡, 斎藤 隆文§

東京農工大学 工学部情報工学科¶

1 はじめに

ネットワークに接続されているコンピュータは常に脅威に曝され続けている．特に多くの人や物が利用するようなオープンなコンピュータであればあるほどその脅威は大きくなる．もし脅威に侵されたならば，いち早く察知し迅速に対処することが求められる．ところが実際には予期していない脅威に対してはインシデントが発生してからでないと気づかないことも多い．IPA のサイバー攻撃事例 [1] などによると，セキュリティホールが認知されていなかったり対策が講じられていなかったりすることによってよくインシデントが発生している．要因として主に次の 2 点が考えられる．すなわちインシデントの予兆が「気づきにくい」こととエラーなどを「無視してしまう」ことである．1 つ目の「気づきにくい」ことの理由は情報の集約化とビジュアル化が十分にできていないからだと考えられる．2 つ目の「無視してしまう」ことの理由はエラーやワーニングが必ずしもインシデントに直結しないからだと考えられる．これらの問題点を踏まえ，本研究では小規模ネットワークの管理者の情報認知向上を目指し管理者のインシデント対策を援助するシステムを提案・開発する．

2 提案手法

本研究ではインターネットに公開されている小規模コンピュータネットワークを効率的に管理できる web サービスを作成する．大規模になると商用の専用ハードウェアなどが販売されているが，小規模ネットワーク管理は専用ハードウェアを導入できないこともある．そのため安価で簡単に導入できることも重要だと考えられる．また効率的に管理するためにインシデントの未然防止や迅速な対処を行えるよう，視覚的なデータの分析や認知しやすいエラーレポートなどを行えるようにすることを提案する．

2.1 簡単な導入

導入コストを下げるため，より簡単な導入方法として Docker を利用した導入を提案する．Docker を用いることで本システムを管理対象のコンピュータの構成を大きく変えずに利用でき，可用性も高くなることが見込まれる．本研究では本システムを管理対象のコンピュータがあるサブネット内に設置し，それぞれのコンピュータのログを Fluentd で ElasticSearch に送信するだけで導入を完了するものを提案する．これにより，導入コストだけではなくネットワークの増築時などでも簡単に本システムのホストとクライアントを繋ぐことができ，拡張性に富む．

2.2 視覚的なデータ分析

視覚的なデータ分析は見やすくわかりやすい分析をすることによって正確かつ的確に必要なデータを理解するための材料になる．そのためグラフや図形などといった直感的にわかるような表現でデータを伝えることを提案する．視覚的なデータの表現については situ[2] や vulnus[3] などのような先行研究を踏まえつつ，Google analytics[4] などのようなモダンなツールなどを参考にする．それらは管理者が見て正確に情報を理解することを主な目的としているため，本項目が提案しているものに近い．しかし本システムが管理するネットワークは小規模なものを想定しており，特定の用途や特異な状況下のような場合も十分に考えられる．そのため自由度が高く柔軟で統合的な方が管理効率がよいと考える．

2.3 認知しやすいエラーレポート

日々エラーやワーニングが発生し続けるとその通知に慣れてしまい，本当に重要なレポートを見逃してしまうということが発生する．そこでその発生を防ぐためエラーやワーニングに重要度を付け通知回数を減らすことで対処したり，一目でわかるようなエラーレポートにすることで認知しやすくしたりすることを提案する．通知回数が多いために慣れてしまうのであれば通知の回数を絞れば改善する．しかしそれだけではなく一目で「何の」「どのような」レポートなのか分かりやすくすることで，通知やエラーレポートに慣れていたとしても瞬時に理解できるため認知されやすいと考えた．

---

*Visualization of small network operations logs and configurations

†Kosuke Watanabe

‡Naoki Kita

§Takafumi Saito

¶Department of Computer Science, Faculty of technology, Tokyo Universiy of Agriculture and Technology

3 制作

本システム全体は前述の通り，図1のようになっている．Fluentd でログを各監視対象システムから収集し本システムのデータベースである ElasticSearch へ送信・保存する．Fluentd はログ収集をするために一般的に使われるデータ収集ツールであり，ElasticSeach は分散型のオープンソースの検索分析エンジンでデータ分析などで一般的に使われるデータベースである．その保存されたデータから本システムは可視化やエラーレポートをするためのデータを抽出する．ElasticSearch へデータが格納できさえすればすべて本システムで扱うことができるため，WAF 等の外部のサービスなども監視可能である．

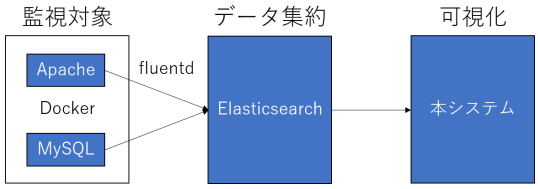

図 1: 本システムのデータフロー

また，Apache(version: 2.4) と MySQL(version: 8.0) を用いてログ収集と可視化を行った．図 2 では上段に日ごとの Apache へのアクセス数，下段に国ごとのアクセス数を示している．また，右下にあるピンク色のバーは Apache へのアクセスを検知した際に表示される通知バーである．本システムでは Python などのスクリプトによって ElasticSearch のデータから任意の種類とデータのグラフを作成可能かつ任意のタイミングと種類の通知をすることが可能である．任意の通知を本システム上で得ることで本システム上の可視化情報と合わせて見ることができ効率的なデータ分析に役立つと考える．

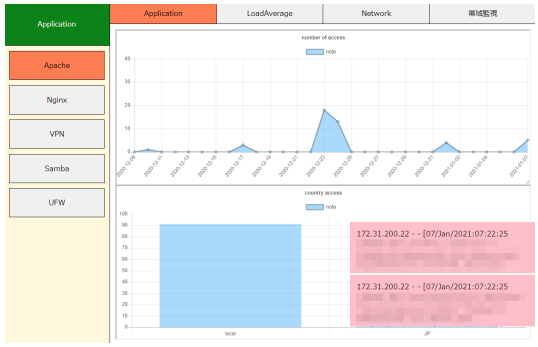

図 2: 可視化・通知システム

可視化システムは図 2 で描写した javascript の Chart.js 以外にも Python の Matplotlib での描写にも対応している．Python と連携できることによって ElasticSearch のログデータから特定の行動や傾向などを機械学習によって分析しその分析結果も本システム内に埋め込むことができる．通知システムは単独の webAPI としても動作可能となっているため，スマートフォンやその他の端末でもその通知を受け取ることができる．

4 おわりに

本研究では小規模ネットワークの管理者がインシデントを未然に防ぐために的確な情報を迅速に認知する手法を提案した．そのためシステムのもつ機能より情報認知の向上などを目指す．これらの機能を使うことで DoS 攻撃検知や時間帯におけるアクセス数の分析などが可能となり，障害発生の未然防止へ寄与すると考えている．既存ツールでは補えなかった柔軟な通知機能やグラフ描画ツールを作成した．今後は小規模ネットワークを管理するうえで必要となる機能をさらに実装し，実際に小規模ネットワーク下での振る舞いや UIUX の度合いを評価したいと考えている．具体的には帯域監視やロードアベレージの監視などを追実装していきたいと考えている．

参考文献

[1] IPA 独立行政法人 情報処理推進機構 , サイバー攻撃被害一覧 - IPA 独立行政法人 情報処理推進機構 , https://www.ipa.go.jp/files/000056149.xlsx , (参照 2021/01/03)

[2] John R. Goodall, , Eric D. Ragan, , Chad A. Steed, Senior , Joel W. Reed, G. David Richardson, Kelly M.T. Huffer, Robert A. Bridges, and Jason A. Laska , Situ: Identifying and Explaining Suspicious Behavior in Networks , IEEE Transactions on Visualization and Computer Graphics, Vol. 25, No. 1, pp. 204-214, (2019).

[3] Marco Angelini, Graziano Blasilli, Tiziana Catarci , Simone Lenti, and Giuseppe Santucci , Vulnus: Visual Vulnerability Analysis for Network Security , IEEE Transactions on Visualization and Computer Graphics, Vol. 25, No. 1, pp. 183-192, (2019).

[4] Google , アナリティクス , https://marketingplatform.google.com/about/analytics/ , (参照 2021/01/03)