L-020

情報セキュリティ啓発を目的とした ポータブルなリアルタイム通信可視化システムの提案
A Proposal of a Portable Real-time Network Traffic Visualization System for Information Security Awareness

須藤 文仁† 寺田 真敏†
Fumihito Sudo Masato Terada

1. はじめに

インターネットを介した情報通信が社会基盤として確立する一方で，サイバー攻撃による様々な脅威も増加し多様化している．特に，コロナ禍以降のテレワークの普及に伴い，組織単位での境界防御だけでなく個人単位でのセキュリティ対策の重要性が高まっている．本研究は，モバイル端末を含む個人利用端末におけるセキュリティ対策を促進するために，通信の可視化を通して情報セキュリティ啓発を図ることを目的としている．

本稿では，サイバー攻撃による脅威を意識させるため，個人利用端末での通信を現実世界と対応付けながら，いつでもどこでも利用できることをコンセプトとしたポータブルなリアルタイム通信可視化システムである NetVision について報告する．

2. 関連研究

2.1 通信の可視化

通信の可視化をセキュリティ意識向上に役立てるアプローチとしては，観測センターや SOC が検知した通信を鳥瞰的に可視化する方法と利用者 PC で検知した通信のふるまいを可視化する方法がある．

(1) 通信を鳥瞰的に可視化

鳥瞰的な可視化については，通信を世界地図上にマッピングする方法[1][2]と，実ネットワーク構成にマッピングする方法[3]がある．前者は広域ネットワークの傾向を可視化するためマクロな観測に，後者は実ネットワークの機器間の通信を可視化するためミクロな観測を向いており，さらに可視化により攻撃通信などの異常を直感的に把握できる．

(2)通信のふるまいの可視化

通信のふるまいの可視化では，通信の発生形態を地図や地球儀にマッピングすることで，利用者自身が攻撃通信などの異常を直感的に把握できるようにしている[4][5].

2.2 解決したい課題

いずれのアプローチも，地図，地球儀，実ネットワーク構成などを利用し，現実世界と対応付けながら通信の可視化を実現している．しかし，通信の可視化を，モバイル端末を含む個人利用端末におけるセキュリティ対策の啓発に活用するためには，通信データのプライバシーを考慮しながら，いつでもどこでも気軽に利用できることが重要となる．本報告では，地図や地球儀などを利用し，現実世界と対応付けつつ，既存アプローチにおける次の課題を解決することにある．

(1)場所に依存しない可視化

観測センターや SOC が検知した攻撃通信を鳥瞰的に可視化する方法は，検知地点を地図上で固定することを前提としている．個人利用端末の場合，移動しながら，あるいは，遠隔出張先での利用など，検知地点が移動することを前提に可視化する．

(2)個人利用端末を対象としたリアルタイムの可視化

通信のふるまいの可視化では，可視化の期間が短い，記録した通信データに基づき可視化しているなどの制限がある．また，攻撃通信を鳥瞰的に可視化する方法は，通信をリアルタイムに可視化してはいるが，個人利用端末向けに利用することは難しい．

3. ポータブルなリアルタイム通信可視化システム NetVision

本章では，2.2 節に示した課題を解決するポータブルなリアルタイム通信可視化システム NetVision について述べる．

3.1 システム要件

システムを実現するにあたり，2.2 節に示した課題を，次に示す要件として設定した．

要件 1：場所に依存しない可視化
　個人利用端末の位置に応じて，検知地点が移動することを前提とすること．

要件 2：リアルタイムの可視化
　パケットキャプチャから可視化までをリアルタイムで処理することにより，その時点の状況を把握できるようにすること．

要件 3：情報セキュリティ啓発につながる可視化
　不正な発信元からのアクセス，大量トラフィックを伴うアクセスなど，個人利用端末がサイバー攻撃にあう可能性があることを意識させること．

3.2 機能概要

本節では，要件 1～要件 3 を実現するためのキャプチャ機能，検知位置情報取得機能，通信可視化機能の処理概要について述べる．

(1) キャプチャ機能

キャプチャ機能はリアルアイム可視化を実現する．起動時に IP アドレスを位置情報に変換するデータ，不正利用に関する判定データを取得し，バックエンドプログラム内

† 東京電機大学 Tokyo Denki University

のデータベースに格納する．その後，ネットワークインタフェースに流れるネットワークトラフィックを監視し，1 秒間の間に到達するパケットをまとめて取得することで，すべてのパケットをリアルタイムに取得する．図 2 の可視化プログラムとキャプチャプログラム間では WebSocket を使用することでリアルタイム可視化を実現している．

(2) 検知位置情報取得機能

場所に依存しない可視化のため，ブラウザの Geolocation API を用い，可視化プログラムが緯度経度を取得することで，検知地点が移動することに対応している．

(3) 通信可視化機能

サイバー攻撃による脅威を意識させるため，3 次元の地球儀上に通信を発信元から送信先へと弧を描くと共に，次のような描画を取り入れている(図 2).

- 発信元から送信先の線に沿って立方体を移動させることで通信量を示す．ここで，単位時間あたりのパケット数の量が大きい場合には立方体のサイズも大きくなる．
- 発信元 IP アドレスの地図上の位置に，パケット数の累積を 3D の棒グラフを表示する．
- 発信元 IP ドレスが不正利用に関すると判定された場合には，発信元から送信先の線の色を赤色，それ以外を緑色とすることで，通信の違いを意識できるようにしている．

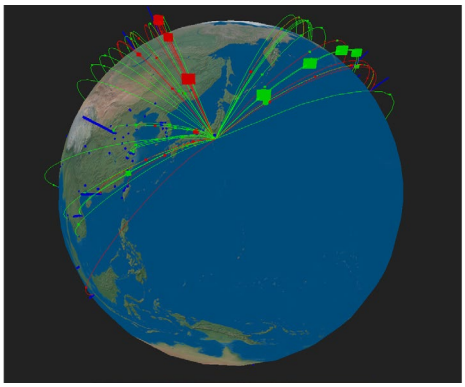

図 1　NetVision による可視化

3.3 システム構成

NetVision のシステム構成を図 21 に示す．本システムは，通信をキャプチャし，通信データを管理するバックエンドプログラムと利用者のブラウザ上で動作させる可視化プログラムから構成している．また，セットアップ手順簡略化のため，Windows 版の exe 形式での配布とし，パケットキャプチャライブラリ(Npcap または libpcap)のインストール，exe 形式から起動により利用できるようにしている．

(1) バックエンドプログラム

キャプチャ機能を実装したバックエンドプログラムでは，通信をキャプチャした後， 起動時にローカルに保存した DB-IP Lite Database[7]と，Spamhaus の DROP リスト[8]を利用して IP アドレスの位置情報への変換と不正判定をしている．これにより，発信元 IP アドレスだけではなく，発着信 IP アドレスの関係性についての情報も，バックエンドシステムに留めている．このように可能な限り通信に関するデータを個人利用端末外部に持ち出さない構成とすることで，情報セキュリティ啓発を図りつつ，いつでもどこでも利用できるようにしている．

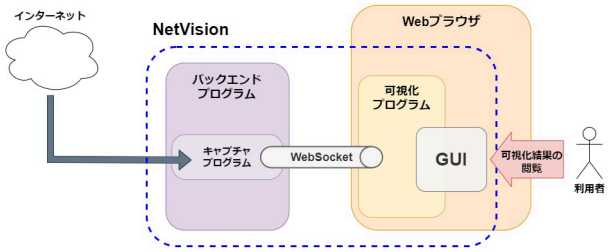

図 2 システム構成図

(2) 可視化プログラム

検知位置情報取得機能，通信可視化機能を実装した可視化プログラムでは，直感的に通信を理解できるよう，通信を発信元から送信先へと弧を描きながら移動するアニメーションとして 3 次元の地球儀上に描画する．アニメーション中は，発信元から送信先を線で結び，どこから来たパケットなのか利用者が理解できるようにしている．なお，可視化を行うのは発信元が発呼したインバウンドのパケットのみで，個人利用端末が発呼したパケットは描画の対象外となる．

4. おわりに

本稿では，サイバー攻撃による脅威を意識させるため，個人利用端末での通信を現実世界と対応付けながら，いつでもどこでも利用できることをコンセプトとしたポータブルなリアルタイム通信可視化システムである NetVision について提案した．

今後，一般利用者に興味を持ってもらい，啓発につながるような可視化としてアニメーションによる表現方法や，AR，VR の適用などによる改善，さらに，スマートフォンなどのモバイル端末での可視化について検討していきたいと考えている．

参考文献

[1] 井上 大介, サイバーセキュリティの可視化技術, 可視化情報学会誌, 2016, 36 巻, 141 号, p.27-31
[2] Kaspersky, Kaspersky Cyberthreat real-time map, https://cybermap.kaspersky.com/ja (参照 2023-06-15)
[3] 鈴木 宏栄ほか, 実ネットワークトラフィック可視化システム NIRVANA の開発と評価, 情報通信研究機構季報 2011, 57 巻, 3-4 号, p. 63-80
[4] 田村 尚規ほか, パケット情報を用いたトラフィック可視化システムの作成, 2015, FIT2015(第 14 回情報科学技術フォーラム)
[5] 加藤 里奈ほか, Google Maps を用いた一般利用者のセキュリティ意識を高めるための通信可視化システム, マルチメディア, 分散協調とモバイルシンポジウム 2017 論文集, p1823-1826.
[7] Free IP geolocation databases, https://db-ip.com/db/lite.php (参照 2023-06-15)
[8] The Spamhaus Don't Route Or Peer Lists, https://www.spamhaus.org/drop/ (参照 2023-06-15)