

AR を活用したリアルタイム通信可視化システムの提案

須藤 文仁 寺田 真敏
東京電機大学

1. はじめに

セキュリティ対策が不十分な中小企業や医療機関を狙ったサイバー攻撃が増加する一方で、サイバー攻撃はその非可視性により、脅威を直感的に理解することが困難である。このため、リスクが軽視される傾向にあり、組織全体でのセキュリティ対策の重要性が十分に認識されにくい。こうしたサイバー攻撃に対する対策の重要性を啓発するには、一人一人がサイバー攻撃の脅威を具体的にイメージし、自分事と考える必要がある。

本研究は、サイバー攻撃の脅威を自分事と考える(以降、サイバー脅威の自分事化)、セキュリティ対策を促進するために、XR 技術を用いたサイバー空間と実空間との融合を通して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、攻撃の起点となり、目に見えないネットワークの通信を、AR を用いて可視化することをコンセプトとした可視化手法と、スマートフォン向けに実装したプロトタイプシステムについて報告する。

2. 関連研究

2.1 通信可視化手法

サイバー脅威の自分事化にあたり、通信の可視化手法を、当事者間と第三者間という視点から整理する(表 1)。当事者間とは、利用者自身が使用する端末の受発信を対象に可視化するものであり、第三者間とは、利用者が使用している端末以外での受発信を対象に可視化する。前者はサイバー攻撃の脅威を自分事として捉えやすく、後者は組織や世界で起こるサイバー攻撃の脅威を把握しやすい。

表 1: 通信可視化手法の分類と関連研究

通信の関係	関連研究
当事者間 自分事への効果: 高	NetVision [1], 3d-tcpdump [2]
第三者間 自分事への効果: 中	EyeSec [3], NIRVANA [4], Cyberthreat Real-time Map [5]

2.2 AR の活用

2016 年以降、現実世界に仮想の世界を重ねて拡張する AR 技術が発展し、様々な分野で活用されている。保守管理の分野では、無線センサネットワーク機器のタグ表示を AR で可視化することで機器の管理効率化を行っている[3]。自然災害対策の分野では、避難ルートと組み合わせて浸水被害の状況を AR で可視化することで、災害に対する意識啓発を図っている[6]。本研究の目的は、サイバーセキュリティの分野

において、ネットワーク通信の可視化に AR を適用することによって、サイバー脅威の自分事化を行い、セキュリティ対策を促進することにある。

3. AR を用いた通信可視化手法

本章では、AR を用いた通信可視化手法を実現するにあたり、当事者間と第三者間という視点、一人称と三人称という視点から整理した結果について述べる。

3.1 一人称視点と三人称視点

一人称視点とは、自分の視線を基点とした主観的なアプローチで、AR を用いたコンテンツではより没入感を高めるため、一人称視点での可視化を行うことが多い。三人称視点とは、自分から見たという客観的なアプローチで、既存の通信可視化システムでは、通信全ての様子を把握できるよう、三人称視点で可視化している。

3.2 視点を交えた通信可視化手法

一人称と三人称という視点に、2.1 節で分類した当事者間と第三者間という視点を組み合わせると、AR を用いた通信可視化手法には、3つのアプローチが考えられる(表 2)。

表 2: 通信可視化手法のイメージ

		視点	
		一人称視点	三人称視点
通信の関係	当事者間		
	第三者間		

(1) 三人称視点からの当事者間通信、第三者間通信の可視化(表 2 の右列)

サイバー空間のみでの可視化の場合、地球儀やネットワーク図上に通信の様子を可視化するに留まるが[1][4]、AR を利用すると、現実世界の機器に直接可視化が可能となる[3]。

(2) 一人称視点からの当事者間通信の可視化(表 2 の左上)

通信可視化における一人称は、通信の到達点からの視点で可視化する。本アプローチは、AR デバイスが通信の到達点となり、利用者は普段実世界で見ている視点から通信を見ることが可能となる。

3.3 AR 適用によるサイバー脅威の自分事化

前節より、一人称視点からの当事者間通信の可視化は、利用者が実世界で見ている視点で利用者端末の受発信を対象

とした可視化をしていることから利用者自身に焦点を当てたアプローチであり、サイバー攻撃の脅威を自分事として捉えやすい。すなわち、ネットワーク通信の可視化にARを適用し、サイバー脅威の自分事化するには、一人称視点で当事者間通信を可視化するアプローチが良いと言える。

4. プロトタイプシステム

本章では、検討に基づき一人称視点から当事者間通信を可視化するスマートフォン向けに実装したARプロトタイプシステムについて述べる。

4.1 システム要件

スマートフォン向けARプロトタイプシステムの実装にあたっては、著者らが個人利用PC向けに開発した通信可視化システムNetVisionと同一のシステム要件である「いつでも、どこでも、見える化」という3つの要件を設定する。これにより、通信の可視化手法によるサイバー脅威の自分事化へのアプローチの一貫性を保つこととした。

要件1: リアルタイムの可視化 (いつでも)
すぐに、その時点での状況を把握できること。

要件2: 場所に依存しない可視化 (どこでも)
物理的な位置の移動にも対応できること。

要件3: 情報セキュリティ啓発につながる可視化 (見える化)
セキュリティをより自分事と考えてもらえるように、ARを用いて外部からアクセスがあることを意識できること。

4.2 プロトタイプシステムの実装

プロトタイプシステムではAndroidを対象とし、いつでも、どこでも、見える化を実現するために、外部サーバなどを利用せず、スマートフォン単体で操作する構成を前提とした。

4.2.1 リアルタイムの可視化

リアルタイムの可視化にあたっては、スマートフォンで発生する通信をリアルタイムにキャプチャする機能が必要となる。実装にあたっては、VPNService API[7]をベースに、デバイスの通信をすべて経由させる仮想ネットワークインターフェースを作成し、管理者権限などの例外的な操作を必要としないようにした。なお、このAPIを使用する際は、利用者に対してその旨を通知し使用許可を求める仕様となっているため、プライバシーについても考慮されている。

4.2.2 場所に依存しない可視化

場所に依存しない可視化については、位置情報を取得するAPIを使用し、逐次的に緯度経度を取得することで、「どこでも」を実現した。

4.2.3 情報セキュリティ啓発につながる可視化

啓発につながる可視化にあたっては、スマートフォン以外から自身に向けてのアクセスがあることを意識してもらうために、送信元から自身までの通信をARで現実世界と対応付け可視化するアプローチを採用した(図1)。通信の流れは、送信元IPアドレスの緯度経度から自身への方角を計算し、その方角からパケットが飛来しているようにアニメーションを行った。さらに、パケットの飛来を擬人化した立方体と組合せてアニメーション化することで、データ量、正規・不正などの通信区別、セキュリティへの興味促進を図った(図1の①)。

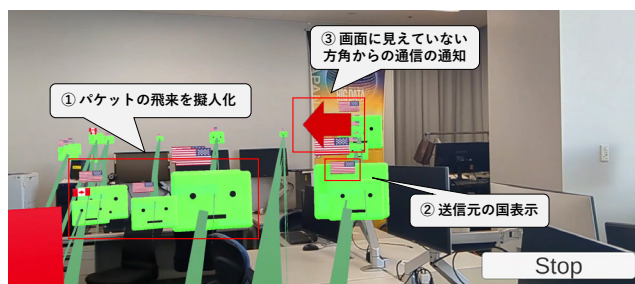


図1: プロトタイプシステムによる可視化

また、サイバー空間に可視化するNetVisionに対しプロトタイプシステムは、サイバー空間の規模が拡大すると、現実世界の機器への直接可視化は困難となる。この問題解決にあたって、次の機能を追加実装することで対処した。

- 送信元の国表示

パケットが飛来してくる方角のみでは、利用者は具体的にどこからの受発信が把握できない。このため、パケットに国旗を併記表示することとした(図1の②)。

- 画面に見えていない方向からの通信の通知

画面に見えていない方角、例えば、利用者の背面方向からパケットが飛来した場合、画面上に通信の流れを表示できず、利用者はその通信に気付けない。このため、矢印を用いてパケットの飛来が画面外の左右どちらであるか通知することとした(図1の③)。

5. おわりに

サイバー脅威の自分事化のため、攻撃の起点となり、目に見えないネットワークの通信を、ARを用いて可視化することをコンセプトとした可視化手法と、スマートフォン向けに実装したプロトタイプシステムについて報告した。

今後は、サイバーセキュリティ分野において通信可視化以外でのAR適用や、VRやMRなど他のXR技術を適用した通信可視化システムについて検討していきたい。

参考文献

- [1] 須藤 文仁ほか: 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可視化システムの提案, FIT2023(第22回情報科学技術フォーラム) (2023)
- [2] 斉藤 匡人ほか: 通信トラフィックとネットワーク情報の三次元視覚化ソフトウェアの提案, マルチメディア通信と分散処理ワークショップ論文集, Vol.2006, No.15, pp.109-114 (2006)
- [3] Martin, Rolfes, et al.: EyeSec: A Retrofittable Augmented Reality Tool for Troubleshooting Wireless Sensor Networks in the Field, Proceedings of the 2019 International Conference on Embedded Wireless Systems and Networks (EWSN), pp.184-193 (2019)
- [4] 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, Vol.57, No.3-4, pp.63-80 (2011)
- [5] Kaspersky, Kaspersky Cyberthreat real-time map, <https://cybermap.kaspersky.com/ja> (参照 2023-12-22)
- [6] PLATEAU, ARを活用した災害リスク可視化ツール, <https://www.mlit.go.jp/plateau/use-case/uc22-026/> (参照 2023-12-22)
- [7] Android Developers, VPN, <https://developer.android.com/guide/topics/connectivity/vpn?hl=ja> (参照 2023-12-22)