4ZD-03

通信遮断による標的型攻撃対応のための影響範囲 VR 可視化システムの開発

小森 工† 嶋田 創† 長谷川 皓一†

1 背景

近年，標的型攻撃の脅威は深刻化の一途を辿っている．標的型攻撃では対象に特化したマルウェアが新規に開発されることも多いため，アンチウイルスソフト等で検知することが難しい．そのため，マルウェアの侵入を完全に防ぐ試みよりも，マルウェアの侵入を検知し，素早く適切な対応をとることが重要視されてきている．

組織の通常業務に対する影響を最小限に抑えつつ適切にマルウェアに対処できる判断を下すことは極めて難しい．例えば組織内ネットワークを完全にインターネットから切り離す対策は確実にマルウェアによる情報漏洩を防ぐことができるため最も効果は高いが，メールの送受信や外部への Web サービスの提供といった通常の業務が完全に遂行できなくなってしまう．逆に感染端末のみをネットワークから切断した場合，他の端末による業務は問題なく遂行できるものの，すでにネットワーク内部でマルウェアの感染が拡大していた場合は被害を抑えることができない．以上のように，マルウェアに感染した一刻を争う事態において適切な対処を行うことは困難である．

この問題の解決策の一つとして，標的型攻撃への対処を支援するためのシステムが提案されている [1]．文献 [1] では組織内ネットワークにおいて不審な通信を検知し，その送信元（マルウェア感染端末）と送信先を隔離する適切な対処を複数提案する．このシステムを利用することで，ネットワーク管理者はマルウェア検出時に素早く適切な対応をとることが可能になる．しかしながら大規模なネットワークで利用する場合，限られたディスプレイ面積では全体を視覚化することが困難になる．そのため理想的には超大型のディスプレイを備えた専用の部屋においてネットワーク全体を可視化できることが望ましいが，一般的なオフィスルームに設置した中小規模 SOC ではそのように広いスペースを設けることが難しい．

本研究では VR を用いてネットワーク構成を可視化し，オフィス内の狭いスペースにおいても文献 [1] を用いた標的型攻撃への対処が容易に行えるシステムを開発する．VR 可視化デバイスには，Oculus Quest を利用した．

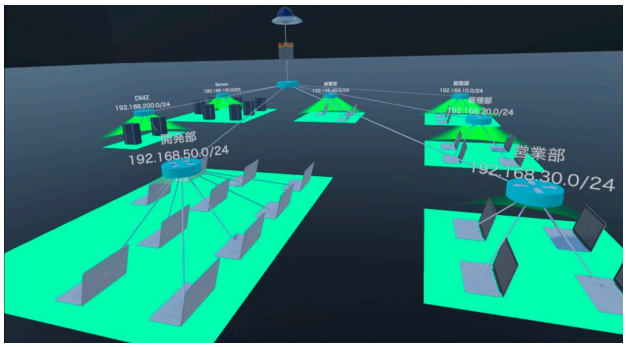

図 1 プログラム実行時の全体像

本研究と関連する研究として，攻撃検知を目的としたトラフィック可視化の 3D 実装では，IP アドレス間の通信をポート番号を高度として表す NICTER が有名である [2]．また，トラフィック可視化の VR 実装としては，宮本による通信量を球体とし，IP アドレスとポート番号をもとに 3 次元空間にマッピングする PACTER VR が存在する [3]．

2 機能

2.1 ネットワーク構成の視覚化

提案システム利用時の視界の一例を図 1 に示す．ネットワーク構造が視覚化され，端末やスイッチの接続が 3D オブジェクトにより表現されている．

図 1 の視界の最上部に位置しているオブジェクトはインターネットであり，その下にはファイアウォールが配置されている．図 1 の構成ではファイアウォールの下にルートスイッチがあり，さらに各部署の LAN が存在している．ネットワーク末端の LAN は緑色の矩形によりハイライトされる．

スイッチは自身の名称とサブネットのアドレス範囲を属性として保持しており，画面上ではスイッチの 3D オブジェクト上部にテキストとして表示される．このテキストは常にカメラの方向を向き続けるよう制御されている．またラップトップとサーバも自身の IP アドレスや利用者名，サーバ名の属性を保持している．これらの情報はカメラが接近した場合にのみ表示される．

† 名古屋大学

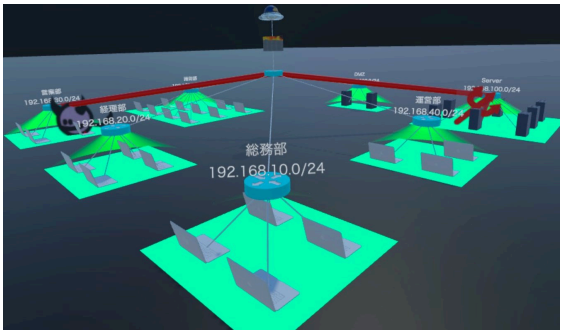

図 2　不審な通信の視覚化

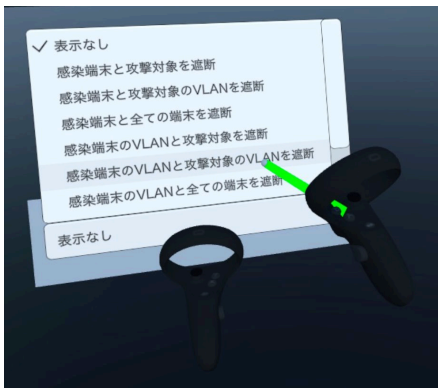

図 3　切断箇所候補の選択

2.2　マルウェアによる不審な通信の視覚化

本ソフトウェアは図 2 に示すように，不審なパケットの送信元と送信先を表示する機能を持つ．図 2 では，送信元（マルウェア感染端末）と送信先（攻撃対象端末）の端末にアイコンが表示され，その間の接続が強調されている．

2.3　ネットワーク切断箇所候補の表示

本ソフトウェアは文献 [1] によるネットワーク切断箇所候補の表示機能を持つ．ユーザは図 3 に示すインターフェースにより切断箇所候補を選択することができる．コントローラの 3D オブジェクトは実際のユーザの手の位置に合わせて表示され，左手側に選択肢が表示される．右手からはレーザポインタが出ており，これをマウスカーソルのように使用して選択を行う．選択された候補に基づき，切断される接続が画面上で点滅する．例えば「感染端末を全ての端末から切り離す」選択の場合，感染端末とスイッチの間にある接続の表示/非表示が周期的に切り替わる．一方「感染端末と攻撃対象の通信を遮断する」場合（特定の通信のみを遮断し，全ての通信を遮断するわけではない），それら 2 端末を結ぶ接続の強調表示の有効/無効が周期的に切り替わる．

2.4　VR 空間内でのワープ移動

実空間（オフィス内）での移動なく VR 空間内で移動を可能とするため，本ソフトウェアではワープ移動を実装している．ワープ時には図 3 と同様に右手のコントローラからレーザポインタが出力される．これをワープしたい地点の床に照射することで移動先を選択する．

3　実装

提案システムの実装には C#言語を用いた．スイッチ，ルータ，ラップトップを抽象化したクラスは全て同一のルートクラスから派生する設計となっている．必要な操作は抽象メソッドとしてルートクラスに定義されているため，全てのネットワーク構成要素を画一的に扱うことができる．スイッチは自身の LAN に接続された要素をルートクラスのインスタンスとして再帰的に保持しており，ネットワーク構造が保持される．

ネットワークの構成は JSON により記述されており，起動時にリモートサーバから HTTP リクエストにより取得される．3D オブジェクトの配置は JSON データに基づき動的に行われるため，ネットワーク構成の変更にも柔軟な対応が可能である．また，切断箇所候補についても，文献 [1] のシステムからネットワーク越しに取得する．

4　まとめ

本研究ではネットワーク構成および文献 [1] による切断箇所候補を VR 空間内で可視化するソフトウェアを開発した．本ソフトウェアを用いることで，ユーザはワープ移動により VR 空間内を移動しながら大規模なネットワークの構成と切断による影響を直感的に視認することができる．このとき現実世界ではユーザはほぼ動作しなくて良いため，オフィス空間内の限られたスペースにおいても利用が可能である．以上より，利用できるスペースの限られるオフィス等における標的型攻撃への対処に本ソフトウェアを活用することが期待される．将来的な発展としては，リアルタイムトラフィックの重畳が挙げられる．

参考文献

[1] 長谷川皓一ら：標的型攻撃に対するインシデント対応支援システム，情報処理学会論文誌，Vol. 57, No. 3, pp. 836–848 (2016).
[2] 鈴木和也ら：迅速な障害対応を支援するトラヒック可視化システムの構築と評価，電子情報通信学会論文誌 B，Vol. J92-B, No. 7, pp. 1072–1083 (2009).
[3] 宮本大輔：探索的データ解析を目指すトラフィック解析についての一検討，情報処理学会研究報告，Vol. 2018-CSEC-80, No. 2, pp. 1–8 (2018).