（ 続紙 １ ）

京都大学	博士（　　情報　　学）	氏名	鈴木 和也
論文題目	Studies on Network Monitoring Systems to Reveal Suspicious Activities （不正なアクセスを検出するネットワーク監視システムに関する研究）		

（論文内容の要旨）

本論文は、ネットワーク管理者がネットワークの状況を把握するための情報を提供するネットワークモニタリングシステムに関するもので全５章から構成されており、それぞれの章の内容は以下の通りである。

第１章は緒論であり、本研究の背景と目的および全体の構成と各章の概要について説明している。

第２章では、複数の手法による解析を支援するトラヒックデータ配送システムのアーキテクチャを提案し、実装と評価を行っている。管理者によるネットワークの状況把握のためには、複数の視点でのトラヒック解析を迅速かつ同時に実行する必要がある。提案システムは、解析対象データを採取するセンサ群、センサからデータを受信する収集サーバ、トラヒックの解析を行う解析モジュール、各解析モジュールがデータを送受信するデータバスから構成される。データバスをマルチキャストで実装したことにより、解析対象データだけでなく、解析モジュールによる解析結果データも複数のモジュールで共有できる。

第３章では、管理者が正常な通信を含めたトラヒック全体を迅速かつ直感的に把握するためのトラヒック可視化システムを提案している。パケットの送信元のアドレス／ポートを軸とする二次元平面と宛先のアドレス／ポートを軸とする二次元平面を対向配置した三次元空間に個々のパケットをアニメーションで描画し、スキャンやDDoS攻撃などの挙動を判別しやすいようにしている。またトラヒックの地域性を考慮し、パケットの送信元および宛先のアドレスが割り当てられている国を判別して世界地図上にアニメーションで描画する機能も実装している。管理者がトラヒックデータを保存しておき、指定した時刻のトラヒックを再現して可視化する機能も実装している。

第４章では、管理者が、未利用アドレスブロックに到達するトラヒックを補助的に用いてネットワークの状況を把握するためのトラヒック解析システムを提案している。提案システムでは、到達するトラヒックを振舞いに基づいて特徴づけ、高速に分類を行う。解析はネットワーク層およびトランスポート層のパラメータのみを用い、宛先アドレスやポートなどの分布に着目して、三段階で実行される。第一段階では、観測ネットワークに到達するパケットを送信元アドレスごとに分け、最初のパケットから一定時間以内に到達したパケットの群を一つのイベントとしてまとめる。第二段階では、宛先ポート番号およびプロトコルフラグに着目してアクセスの仕方を分類する。第三段階では、宛先アドレスおよび宛先ポートが単数か複数かで分類を行う。この解析結果により、同じ挙動を示すホスト群が抽出され、管理者の状況把握を支援する。提案システムは実ネットワークにおいて運用され、広域で連携したネットワーク監視に貢献している。

第５章では、結論と今後の展望について述べている。

（続紙 ２ ）

（論文審査の結果の要旨）

ネットワークを安定運用するためには、ネットワーク管理者が正常通信を含めたトラヒックの状況をリアルタイムに把握しておく必要がある。本論文は、管理者にネットワークの状況を迅速にかつ分かりやすい形で提示し、不正なアクセスを検出することを支援するネットワーク監視システムを主題としている。

ネットワークの状況を提示するシステムはいくつか提案されているが、本論文では、管理者が常時ネットワークのトラヒックを監視している状況において不正なアクセスの検出を支援することに重きをおいている。そのために、トラヒックを可視化するシステム、トラヒックを解析するシステム、これらの各システムにデータを配送するシステムから構成されるアーキテクチャを提案し、それぞれをシステムとして設計、実装している。それぞれのシステムでは以下の特徴的な手法が提案されている。

（１）トラヒックデータ配送システムにおいては、データバスと呼ぶ共有バス型のアーキテクチャを用いてデータを共有している。データバスはUDPマルチキャストを用いて実装され、クライアントはここからストリームデータを取得し、処理して、必要であれば再びデータバスに送出する。データバスアーキテクチャにより、モジュール間の同期などが不要となる簡素な並列・分散処理が実現されている。配送されるデータ量が増大した場合においても、運用するサーバを複数にすることで、容易に拡張することが可能な設計となっている。

（２）トラヒック可視化システムでは、ネットワークに到着する個々のパケットすべてを可視化し、パケットの到達の様子が理解しやすいように描画する。ネットワーク越しの攻撃の多くはネットワーク層・トランスポート層のパラメータに特徴があることに着目し、送信元アドレス／ポート、宛先アドレス／ポートによるアニメーション表示を採用することで、ネットワーク管理者が通常の状態を把握した上で攻撃やその準備行為などの不審なトラヒックを視認することを助けている。

（３）トラヒック解析システムでは、未利用アドレスブロックへ到達するトラヒックを、送信元ホスト毎に特徴を用いて分類している。特徴づけは、ネットワークプログラミングの観点から行い、Windows系OSを対象として10秒程度の時間幅を設定し、その間に到着した同一送信元アドレスのパケットをひとまとめにして扱い、それらの出現頻度を分析して特徴化している。これにより、スキャンがシーケンシャルなものかランダムかの違いなど管理者が不正アクセスを識別するのに有用なアクセスパターンの違いを、約10秒間分のパケットについて1秒程度の遅延で出力できる高性能を達成している。

ネットワーク管理者が、膨大なトラヒックデータの中から日々現れる新種の攻撃を検知しなければならない現状に鑑み、本研究が、トラヒックを高速に解析して管理者に情報をわかりやすい形で提示することができるようにした点は意義深い。本研究に基づくシステムは、独立行政法人情報通信研究機構などにより実運用され、得られた情報は国際的な監視網でも共有されて広域での早期警戒に活用されている点も特筆すべきである。よって本論文は博士（情報学）の学位論文として価値あるものと認める。

また、平成２２年２月１４日論文内容とそれに関連した口頭試問を行った結果合格と認めた。