博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：セキュリティ情報に基づくネットワークトラヒック制御に関する研究
申請者　：岡田　康義
審査委員会　：主査　教授　田中 英彦
副査　教授　小柳 和子
副査　教授　土井　洋
副査　教授　佐藤　直

I. 論文内容の要旨

本論文は、「セキュリティ情報に基づくネットワークトラヒック制御に関する研究」と題し、６章と付録からなる。現在の情報システムは、インターネットが重要な要素であるが、その構成は過去、自由に構成されてきた。その結果として、ネットワーク自体に流すトラヒックの内容に応じた制御は行われず、またそれを使う利用者は誰でもが自由に使えることを原則としている。それは、ある意味自由を担保するという機能を持っているが、逆にネットワーク上で何をすることも可能で、情報セキュリティ上様々な問題を引き起こしていることも事実である。今後を展望するとき、今一度そのあり方を再検討することも意義があるのではないか。そのような観点からネットワークの制御を考えたのがこの論文である。

第１章は「緒論」で、研究の背景、研究の位置づけと目的、研究の概要並びに研究の研究指針について述べている。

第２章は「私的セキュリティポリシーを用いたトラヒック制御」で、第３章は、 「公的セキュリティポリシーを用いたトラヒック制御」であり、これらの章では、ユーザ毎に設定する私的セキュリティポリシーおよび社会的コンセンサスとして認められ適用される公的セキュリティポリシーという二つのタイプのセキュリティポリシーを IP（Internet Protocol）ネットワーク（以下、ネットワークと略す）に設定し、ネットワーク層でトラヒック制御することを提案している。

これらの章では、最初に、既存検討と本研究に関する検討指針を述べている。すなわち、インターネットでは、P2P（Peer to Peer）ヘビーユーザや DoS（Denial of Service）攻撃の従来の対策として、社団法人日本インターネットプロバイダー協会が中心となり帯域制御の運用基準に関するガイドラインを定め、ISP（Internet Service Provider）毎にアプリケーション規制方式や総量規制方式を実施しているが、 以下の問題があることを指摘している。

（１）セキュリティ対策に関するユーザ個々の意思が反映されていない。
（２）セキュリティ対策が不十分な端末あるいは LAN（Local Area Network）から送信されたパケットであっても暗号化されている場合は、 不正パケットかどうかの判定ができずトラヒック制御が十分に行えない。

本文では、これらの問題の解決に向け、以下のような三つの指針でトラヒックを制御する手法を検討している。

指針 1）従来、LAN に設置しているファイアウォールを WAN にも設置し、これにユーザ毎の私的なセキュリティポリシーを設定してトラヒックを制御する。

指針 2）ネットワークユーザ全体のコンセンサスに基づく公的なセキュリティポリシーを設定し運用する。具体的には、端末や LAN といったユーザ利用環境に関する脆弱性評価を実施し、その結果に応じてネットワークの利用帯域を差別化することで、ユーザのセキュリティ意識を向上させ、流通する不正トラヒックを抑制する。

指針 3）指針 1 と指針 2 はアクセスネットワークで実施する。すなわち、指針 1 と指針 2 を複数 ISP にまたがる中継ネットワークに適用することは拡張性の点で困難であることから、対象となるユーザを収容するアクセスネットワークで実施する。

また、本研究が目指すトラヒック制御を行うための技術として、パケットヘッダ情報をもとにしたパケットフィルタリング技術や QoS（Quality of Service）技術の適用を示している。類似の既存パケットフィルタリング技術として Moving FireWall があるが、それらは拡張性の面での点があること、また、QoS 技術の適用に関しては、DoS とみられる異常トラヒックの帯域を抑制するための理論的検討があるが、本提案のようにセキュリティポリシーの設定や具体的な運用手順まで踏み込んだ検討例は見受けられないこと、を述べている。

その後、インターネットへのアクセス網である NGN（Next Generation Network）を対象に本提案の適用例を示し、計算機シミュレーションにより、本提案が、悪意のあるパケットがユーザに到達する可能性や、セキュリティ対策機能が不完全なネットワーク利用環境から発信されたパケットがネットワークを流通する割合を抑制できることを示して、提案の有効性を確認している。

第 4 章は「情報セキュリティ DB を用いた SNS 会員資格制度提言」である。運輸交通制度からの類推により、情報セキュリティを確保するための SNS（Social Network Service)会員資格制度の導入を提案している。SNS の情報セキュリティを確保するために、個人のサイバー犯罪履歴やセキュリティ上の過失を蓄積した第三者機関としてのセキュリティデータベースに基づいて会員資格を判断する方式である。本章では、これによって、セキュアな SNS 環境が補強されることを示すとともに、提案制度導入のインパクトと今後考察すべき問題を整理している。

第 5 章は「フィージビリティ（実現性）について」であり、提案の実現性を吟味要約している。

第 6 章は「結論」で、検討のまとめと今後の課題を述べている。

Ⅱ. 論文審査結果の要旨

これを要するに本論文は、インターネットの情報セキュリティ向上を目指して、ネットワークに個人のポリシーや公的なポリシーを設定しそれを満たさないトラヒックを排除するという手法を提案するとともに、SNS 会員資格証明書を発行し利用することで不要な利用者を除くということを通して、抜本的なセキュリティ向上を図ることができるという可能性を与えたものである。これらの採用は社会的にも議論の多い所であろう。しかし、その可能性の検討自体は十分意義があると考えられ、両者併せてこれらの研究は、情報学に貢献するところが少なくない。

よって、本論文は、博士（情報学）の論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、平成 25 年 3 月 5 日に論文内容について口述試問を行い、博士論文として合格と判断した。その後、平成 26 年 2 月 17 日最終試験を実施し、合格と判定した。