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

A study of network traffic control based on security information

岡田 康義
Yasuyoshi Okada

要 旨

第 1 章では，緒論として，研究の背景，研究の位置づけと目的，および検討指針を述べる．

＜研究の背景＞

情報通信ネットワーク（以下単にネットワークと呼ぶ）は本来，安心で安全な環境で利用できるに越したことはない．現在のインターネットはその成り立ちから一貫して「ネットワークは簡易に，端末は高機能に」という思想のもとに構築されてきており，安心や安全といったものは基本的に端末側へ依存しているのが実情である． しかし，近年のサイバー犯罪やネットワークトラヒックを鑑みると端末側だけの対処で解決するには限界にきている．加えて，近年代表的なインターネットサービスとなったソーシャル・ネットワーキング・サービス（以降は SNS と略す）の主な利用目的は，人が人とコミュニケーションをすることにある．SNS は，友人・知人間のコミュニケーションを促進する手段や場を提供する．しかしながら，SNS ではなりすましやウィルス感染等の犯罪も起きている．

＜研究の位置づけと目的＞

インターネット等の TCP/IP をベースとしたネットワークを利用している企業ユーザや個人ユーザは，現在，いくつものセキュリティ対策を実施している．すなわち，従来からの境界型ファイアウォールに加え，ユーザは，侵入検知システム，脆弱性検査システム，検疫システム，ウィルス対策ソフト，パーソナルファイアウォール等を導入している．

セキュリティのポリシーおよび SNS に関する社会制度の課題についても様々な議論がある．情報セキュリティマネジメントシステム ISMS（Information Security Management System）の国際規格 ISO/IEC 27001 をはじめとしてセキュリティポリシーの設定や実施手順を記したガイドラインがいくつか公開されおり，関連の認証制度も広く普及している．このセキュリティポリシーの適用対象は，概ねコンテンツである“情報資産”やそれを扱うアプリケーションが主体である．具体的に，児童ポルノ等の有害コンテンツとその流通が規制されている．

しかしながら，ネットワークの低レイヤ機能であるパケット転送については，ネットワークの利用の公平性といった，社会的にセンシティブな課題とも関わることから，セキュリティポリシーのあり様や枠組みは明確に結論づけられていない．

一方で，政府や企業を標的とした標的型メール攻撃，サービス不能（DoS；Denial of Service）攻撃，ユーザの意図しない動作をするソフトウェアをダウンロードさせる攻撃，といったセキュリティ攻撃が増加している．これらのセキュリティ攻撃に対処するには，私的あるいは専用的なネットワーク

のみならず，インターネットのような公衆ネットワークにおいても，パケット転送について一定の制限を設け，セキュリティポリシーを適用することが肝要である．

さらに，SNS では，マルウエア感染や詐欺行為のプラットフォームとしての利用やなりすましの犯罪やウィルス感染等に関して「SNS の安全な歩き方～セキュリティとプライバシーの課題と対策」としてNPO 日本ネットワークセキュリティ協会が報告しているが十分に効果があがっていない．

本研究の目的は，前出した課題を踏まえて，以下の3つとする．

(1) セキュリティ対策機能の一部をユーザ側からネットワーク側に持つことでユーザ負担を軽減する．

(2) 悪意のあるパケットがユーザに到達する可能性を低減し，セキュリティ対策機能が不完全なユーザ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する．

(3) SNS でのなりすまし犯罪やウィルス感染等の問題に対応する制度の提言を行う．

＜検討指針＞

私的セキュリティポリシーを用いたトラヒック制御法，公的セキュリティポリシーを用いたトラヒック制御法に関する検討指針を説明する．

インターネットでは，P2P ヘビーユーザや DoS 攻撃への対策として，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 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．

(1) 従来の対策では，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 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，といった問題がある．

本文では，上記問題の解決に向け，以下の三つの指針でトラヒック制御する手法を検討する．

指針 1） 従来，WAN と LAN の境界にファイアウォールを設置して外部からの不正パケットをブロックする際，このファイアウォールには私的なセキュリティポリシーが設定され運用されるが，この私的なセキュリティポリシーによるトラヒック制御を公衆ネットワークでも実施する．

指針 2）ネットワークの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．従来，企業等では，従来，端末やLANといったネットワーク利用環境に関する脆弱性評価指針を定めてある．本研究では，このような脆弱性評価指針を一般ユーザにまで拡大し，脆弱性の評価結果に応じて公衆ネットワークの利用帯域を差別化する．このようにすることで，一般ユーザのセキュリティ意識を向上させ，公衆ネットワークで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ことを前提に検討する．これらの指針を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．

次に，第 1 章で示した，研究の目的および検討指針に従い，第 2 章と第 3 章では，それぞれ私的及び公的セキュリティポリシーを用いたトラヒック制御法を提案している．

インターネット等の TCP/IP をベースとした情報通信ネットワークを利用する際は，ユーザが自ら

の責任でセキュリティ対策を実施しているのが現状である． このようなネットワークセキュリティについて以下が言える．

・ネットワークがブロードバンド化され利便性が高まれば高まるほど，ユーザのセキュリティ対策に関する負担が増加している．

・これは，ネットワークを流れるトラヒックをセキュリティの観点から監視・管理する機能がネットワーク側に十分に備わっていないことが原因である．

本文では，セキュリティ対策機能をユーザ側からネットワーク側に移行してユーザのセキュリティ対策に関する負担を軽減すると同時に，より安全に利用できるようにするため，セキュリティポリシーに基づきネットワークにおける IP パケット（以下単にパケットと呼ぶ）のトラヒックを制御することを提案する．

具体的に，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ネットワークに設定し，パケットフィルタリング技術およびサービス品質技術を用いてネットワーク層でトラヒック制御することを提案する．

次に，インターネットへのアクセス網である NGN（Next Generation Network）を対象にして本提案の適用例を示す．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確認する．

第 4 章では，情報セキュリティデータベース（DB）を用いた SNS 会員資格制度の提言を行う．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 会員資格制度の導入を提案する．将来，情報セキュリティ DB を用いた SNS 会員資格制度の創設が必要になるという仮設を立て，情報の提供者および受容者としての条件を満たす利用者に SNS 会員資格証を発行し，情報セキュリティ DB に基づく会員資格方式を導入することにより，セキュアな SNS ひいては安心して利用できる情報通信環境の実現を目指すことを提案する

第 5 章は，第 2 章から第 4 章に関して，フィージビリティ（実現性）の検討を行う．このフィージビリティ（実現性）の検討については，我が国における通信会社の実際のアクセスネットワークを例にとって，本研究の実現性を示す．

最後に第 6 章では結論を述べる．すなわち，本研究の結果は以下のようになる．

1. 私的セキュリティポリシーを用いたトラヒック制御法

本研究では TCP/IP をベースにした公衆ネットワークに私的なセキュリティポリシーを導入し，トラヒック制御（パケットフィルタリング）することを提案し，計算機シミュレーションによりその有効性を確認した．

2. 公的セキュリティポリシーを用いたトラヒック制御法

本研究では TCP/IP をベースにした公衆ネットワークに公的なセキュリティポリシーを導入し，サービス品質技術 Diffeserv を用いて，ユーザのネットワーク利用環境のセキュリティレベルに応じてトラヒック制御（優先制御）することを提案し，計算機シミュレーションによりその有効性を確認した．

3. 情報セキュリティDBを用いたSNS会員資格制度提言

本研究では，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 会員資格制度の導入を提案した．具体的に，3 種類の資格証明書（SNS 会員証，セキュリティ検査証明書，アクセス査証）を発行・管理し，情報セキュリティDBに基づくSNS会員資格制度を確立してセキュアな SNS を運用することを提案した．さらに，提案を実現するための組織体制，実現イメージを示すとともに，技術および社会の両面から実現性，利点と課題を明らかにした．

Abstract

Chapter1 describes background of the research, positioning and purpose of the research, and guidelines of the study, as a preface.

< Background of the research>

The network should be maintained so available that every user could communicate safely. The Internet has been built under the consistent thought that ″the network is simple, and the terminal has high-performance.″ Actually, the function on safety and security for the users is mainly embedded in only terminals, and transmission protocols seem not to work well for the safety and security. In addition, social networking services (hereafter abbreviated as SNS) in recent years are used primarily for communicating the people who are known to each other. However, also in the SNS, cyber crimes such as spoofing and virus infection have occurred.

< Positioning and purpose of the research>

Currently, business users and individual users utilizing the network based on TCP / IP on the Internet, have a number of security measures. That is, in addition to traditional boundary firewall, they have to introduce intrusion detection systems, vulnerability inspection system, quarantine systems, anti-virus software, and a personal firewall. There are various discussions on issues of social systems which are concerned with security policies and SNS. Procedures and implementation of security policy settings are exposed as a guideline. One of the guidelines is a typical example of the ISO / IEC 27001 international standard for information security management system ISMS (Information Security Management System) and the related certification are also widely used.

In general, the contents covered by policies of this security are called ″information assets″ and their applications provide harmful pornography with a restricted sales flow. However, functions of the IP packets (Hereinafter simply referred to as packets) at lower layer forwarding in the network are involved with socially sensitive issues such as fairness in network utilization. Therefore, both definite conclusion about how there should be and a framework for their security policies are not yet available. On the other hand, there are many (Denial of Service) DoS attacks and malicious e-mails that target the government or companies. One of these attacks is to download the software that operates the user does not intend. Of course, this is because there is a problem with security.

To address the security attacks in not only network exclusively or private, even a public network such as the Internet, security policies and certain limitations packet forwarding should be introduced and performed in the near future. As a reference, the NPO Japan Network Security Association is considering ″measures – security and privacy issues and how to walk safely SNS″. This is because the current SNS is actually supposed to be a platform for spoofing and malware infection. Unfortunately effective security measures are not sufficiently present against the current SNS.

Based on the previous issues, the objectives of this study are the following three.

(1) The network side has a security feature in behalf of the user side. Then it is possible to reduce the burden users.

(2) Packets originating from a malicious user reduce the probability of reaching the other users. Packets that a user with the capability of security measures incomplete originated suppress the flowing percentage through the network.

(3) This paper shows a social system that can solve the problem such as impersonation and virus infection in the SNS.

<Guidelines of this study>

With respect to conventional measures against the abnormal traffic due to Denial of Service (abbreviated DoS) attacks and P2P heavy usage, Internet Providers Association of Japan shows a guideline for operational standards bandwidth control and an implementation scheme to suppress total amount control method of the abnormal traffic. However, there are still the following problems.

(1) In the conventional measures, the users' request on the security measures has not been reflected.

(2) When packets are enciphered, the conventional security measures doesn't work well and it cannot be determined whether they are malicious or not.

For solving these problems, the paper discusses traffic control method in the following three guidelines.

Guideline 1) To block malicious packets from outside of the LAN, the firewall at boundary between LAN and WAN conventionally operates based on the private security policy. The paper applies this private security policy also in the network.

Guideline 2) To maintain overall security of the network, the paper introduces the public security policy based on the consensus of the entire public users of the network.

The vulnerability assessment guidelines have been established for the environment for using the terminal and the user, such as a conventional LAN. This study shows that it is possible to suppress the traffic fraud that differentiates the bandwidth usage of the network according to the results of the evaluation of vulnerability, to improve the security awareness of users.

Guideline 3) Guideline 1 and Guideline 2 are considered on the assumption that it will be implemented in the access network. Be applied to the relay network security policy guidelines for private one, it is difficult in terms of scalability. So we consider it as implemented in the access network that accommodates the user in question.

According to the guidelines 1 to 3, in Chapters 2 and 3, we propose a method for traffic control using private and public security policy, respectively. If the user uses the information communication network and TCP / IP-based, such as the Internet, the user himself is responsible, at present, it is the security measures. In addition to it, so that you can safely use the network, this paper proposes a traffic control based on the security policy. More specifically, the network security policy is set to two types. The first is to set the security policy for each user private. Second, set the public security policy that is applied as a social consensus. This paper proposes that the traffic control at the network layer would be executed by the packet filtering technology or quality of service. This paper shows an example application of the proposal can be developed in the NGN (Next Generation Network) as an access network to the Internet. Using a computer simulation, two things are confirmed. The first is the percentage of malicious packets to reach the user. Second is the ratio of suppressing the packets flowing through the network, where vulnerability of network usage environments such as host computers and LAN is assessed by penetration tests and the security level as the result of the tests are attached to the packets originated from the concerned users.

With respect to SNS membership system using security information DB, from the analogy of transportation system, Chapter4 proposes the introduction of SNS membership qualification certificates and licenses. Future, as a guide to the study of SNS membership qualification system using security information DB in Chapter4, we hypothesized that there must be the creation of a system using a SNS membership database security. For the SNS users who qualify as a recipient and the provider of the information, issue a certificate of membership SNS. By the introduction of the scheme membership based on security DB, secure SNS, and thus, implementation of information and communications environment that can be used with confidence is possible.

Chapter5 investigates the feasibility of the proposals presented from Chapter2 to Chapter4. It shows the feasibility of the three proposals in this paper on the actual network.

Finally, Chapter6 summarizes the conclusions of three proposals as below.
As a first conclusion, with respect to traffic control method using private security policy, this paper has proposed a study of traffic control (packet filtering) using a policy of personal security to the

public network. Finally, using a computer simulation, this paper shows the effectiveness of the proposal.

As a second conclusion, with respect to traffic control method using public security policy, this paper proposes a study of priority control of traffic (Diffserv) using the users' vulnerability level which is evaluated by penetration tests. Then this paper showed the effectiveness using computer simulations.

The third conclusion, with respect to membership SNS system using security information DB, from the analogy of transportation system, this paper proposed the introduction of SNS membership qualification system with security information. The system issues and manages three kinds of certificates; SNS membership certificate, Security check certificate, and access visa. Finally, this paper considers the introduction of this system from technical and sociological viewpoints.