IP ネットワークのセキュリティ機能高度化の検討

小宮　康裕†
mgs085513@iisec.ac.jp

西川　康宏†
mgs075507@iisec.ac.jp

堀　琢磨†
mgs075516@iisec.ac.jp

岡田　康義†
dgs074104@iisec.ac.jp

佐藤　直†
sato@iisec.ac.jp

†情報セキュリティ大学院大学
〒221-0835　神奈川県横浜市神奈川区鶴屋町 2-14-1

あらまし　インターネットは「誰でも自由に使える」という発想で発展し，現在では高度情報化社会のインフラとして欠かせないものとなっているが，その自由度故に悪意ある利用が絶えず，情報セキュリティ上の脅威も増大し安全性が大きく損なわれ，セキュリティ対策のためユーザに大きな負担がかかっている．本学では，IP ネットワークの安全性向上，及びユーザの負担軽減を目指し，高信頼ネットワーク構築のための研究を行なっているが，今回，私的及び公的セキュリティポリシを用い，IP ネットワーク内のトラヒック量をコントロールするセキュリティ機能の研究について紹介する．

A study on advanced security function for IP networks

Yasuhiro Komiya†
mgs085513@iisec.ac.jp

Yasuhiro Nishikawa†
mgs075507@iisec.ac.jp

Takuma Hori†
mgs075516@iisec.ac.jp

Yasuyoshi Okada†
dgs074104@iisec.ac.jp

Naoshi Sato†
sato@iisec.ac.jp

†Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-shi, Kanagawa 221-0835,Japan

Abstract　The Internet has been promoted with the concept of " Everyone can freely use it ", and is one of social infrastructures. However, its safety is often degraded by attacks from some malicious users, and general users are compelled to take much load for keeping convenience of the Internet. We have discussed improving the networks security and reducing the load of users. This paper proposes the advanced security function on IP networks, which manages the network traffics based on both private and public security policies.

1.　はじめに

インターネットは「誰でも自由に使える」という発想で発展し，現在では高度情報化社会のインフラとして欠かせないものとなっているが，その自由度故に悪意ある利用が絶えず，情報セキュリティ上の脅威も増大し安全性が大きく損なわれ，セキュリティ対策のためユーザに大きな負担がかかっている．具体的な悪意あるユーザからの脅威としては，コンピュータウィルス，マルウェアなどの感染，それらの配布手段としてのスパムメール，DoS 攻撃によるサービス不能などである．一般ユーザはこれらの

脅威から身を守るため，OS のパッチ適用やアンチウィルスソフトの導入とそのメンテナンスなど，セキュリティ対策に無駄な労力と支出を強いられている．また，悪意が無くとも一般ユーザが他の一般ユーザに不利益を与えている場合がある．例えばボットに感染するとボットネットの一部として，スパムメールのばらまきやDDoS 攻撃などに加担してしまうことがあり，他の一般ユーザに迷惑をかけてしまうこととなる．そこで我々は，ユーザの負担を低減しつつ安心して IP ネットワークが利用できるような, 高信頼 IP ネットワークの構築を目指し研究を行なっているが，本稿では私的及び公的セキュリティポリシを用い，IP ネットワーク内のトラヒック量をコントロールするセキュリティ機能について提案する．

2. IP ネットワークのセキュリティ課題と対策

現在のインターネットには様々な危険が存在する．その危険を取り除くためには，利用ユーザの努力だけでは困難なところがある．そのため, より安全な IP ネットワークが必要である．

2.1. インターネットの不正利用対策

現状，インターネットのユーザはセキュリティ対策として OS へのパッチ適用，アンチウィルスソフトの導入，また，それらのメンテナンスに多くの労力をかけることが求められている．これらの作業は，慣れたユーザでも手間がかかる作業であるし，PC に詳しくないユーザにしてみれば，難解な作業である．また，それらには金銭的負担が必要な場合もある．企業にしてみても同様にそれらの作業があるほか，社内のネットワークを悪意ある利用から守るため，IDS などの機器やそれらのメンテナンス，維持費などが必要である．つまり，一般ユーザにしても企業にしてみても，セキュリティ対策に無駄な労力や金銭的負担を強いられていることになる．

現状のインターネットの問題点として，
① ユーザ側の作業負担が大きい
② セキュリティレベルが不均一
③ セキュリティ対策コストが大きい
④ ネットワークの悪意利用が可能である
ということが挙げられる．インフラとしての要件は，誰もが安価に安心して利用できる社会基盤ということであり，情報化社会のインフラとして成長したインターネットは，社会基盤としての要件を満たすには問題が残っていると考えられる．

2.2. 高信頼 IP ネットワーク

現在のインターネットを構成するユーザの端末及び IP ネットワークは, ユーザの端末はより高機能になり，IP ネットワークは逆にシンプルに構成されている．IP ネットワークはユーザ及びユーザの端末をセキュリティ的脅威から守るような機能は基本的に持っていないため，ユーザは自分で自分を守らなくてはならなず，この作業が大変な負担となっている．そこで，インターネットの不正使用に対し，ネットワーク側にユーザをセキュリティ的脅威から守るような機能を持たせたセキュアな IP ネットワークの構築が必要であると考えている．

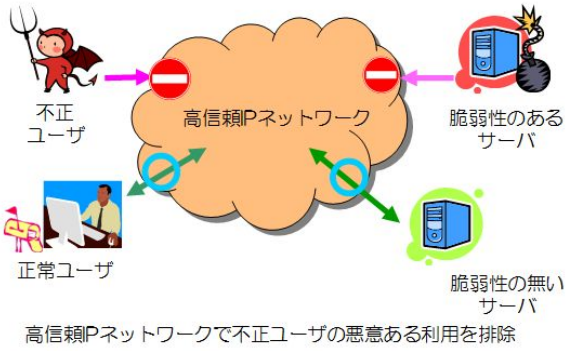

図 1　高信頼 IP ネットワークイメージ

すなわち，図 1 にあるように，不正ユーザや脆弱性のあるサーバを IP ネットワークから排除し，正常なユーザや脆弱性の無いサーバが安心して IP ネットワークを利用できるような高

信頼 IP ネットワークの構築である. この高信頼 IP ネットワークの目標は,

① ユーザ側の作業負担が少ない
② セキュリティレベルが均一
③ セキュリティ対策コストが少ない
④ ネットワークの悪意利用が不可

を実現することである. これらの実現には, ネットワーク側で高機能なセキュリティ対策, サービスを実現する必要があると考えている. 図 2 に, インターネットと高信頼 IP ネットワークの違いを示す.

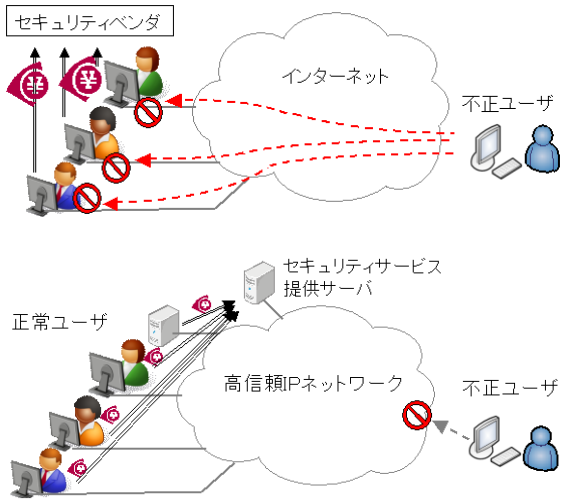

図 2　インターネット(上)と
高信頼 IP ネットワーク(下)の比較

インターネットでは, ユーザが各々セキュリティベンダにお金を支払ったり難しい作業をして自分の PC を自分で守る. これにより不正ユーザからの通信を遮断するが, どこまでセキュリティ対策を実施しているかなど個々のセキュリティレベルはまちまちであるため, 脆弱性が残った端末からコンピュータウィルスに感染していってしまう. また, 端末で不正ユーザの通信を遮断するため, インターネット上は不正な通信であふれてしまうことになる. これに対し高信頼 IP ネットワークでは, ネットワークのセキュリティサービスという形でユーザが少しづつお金を支払うことにより, ネットワーク全体でセキュリティ対策を実施してもらう. これにより, 高信頼 IP ネットワークの目標が達成できると考えている.

3.　IP ネットワークのセキュリティ機能高度化

我々は, インターネットのセキュリティ的問題点を解決するための一助として, セキュアな IP ネットワークの構築のための研究を行っている. その一部, 私的セキュリティポリシによるネットワークサービス, 公的セキュリティポリシによるネットワークサービスについて提案する.

3.1.　私的セキュリティポリシによるネットワークサービス

私的セキュリティポリシとは, プライベートネットワーク毎のセキュリティ方針のことである. 現状では, ユーザ自ら策定してセキュリティシステムを構築したり, セキュリティベンダが提供するセキュリティサービスメニューを選択して実施しているが, 私的セキュリティポリシでは, 各ネットワークの管理者がセキュリティ方針を決め, それを各自のネットワークに適用する. 例えば, 「決まったセキュリティソフトを導入する」「迷惑メールはコンテンツでフィルタリングする」「P2P アプリケーションの利用は認めない」などを, 各々管理するネットワークに適用する. 図 3 に概念図を示す.

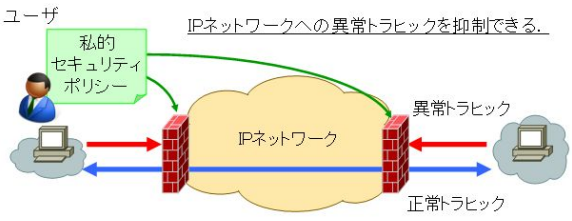

図 3　私的セキュリティポリシ概念図

以下に, 私的セキュリティポリシを利用したセキュリティ対策の具体的な提案を示す.

・私的セキュリティポリシを利用した DoS 対策 [1]

本提案では，IP ネットワークの入り口にユーザが決めたセキュリティポリシを適用することで，そのセキュリティポリシに合わないトラヒックは遮断し，正常なトラヒックのみ通すことで，異常トラヒックを抑制するものである．この提案では，DoS 攻撃を検出するパラメータとして，単位時間あたりの UDP 帯域利用率，UDP を利用した DoS 攻撃を抑制するパラメータとして，単位時間あたりの UDP パケット利用可能帯域を用いている．エッジルータにおいて，ユーザが設定した単位時間あたりの UDP 帯域利用率を超えた場合，DoS 攻撃と判断し，IP ネットワーク内で該当パケットの遅延を発生させることで通信の抑制を図っている．また，IP ネットワークの出口側エッジルータで検出された DoS 攻撃は，制御網を利用して入口側エッジルータにも通知し，IP ネットワークの入口でも同様に抑制を実施する．そのため，IP ネットワーク内で攻撃パケットを遅延，抑制させるだけでなく，IP ネットワーク内への DoS 攻撃トラヒックの流入も防止できる，という効果も併せ持つ．本研究のシュミレーション結果を図 4 に示す．

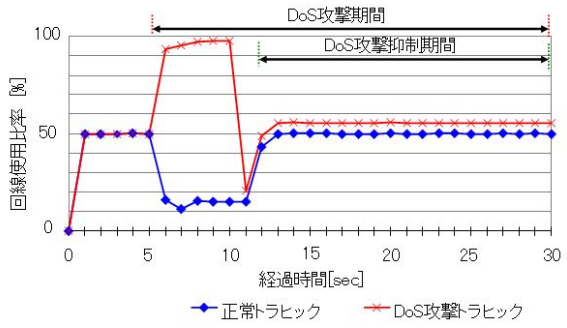

図 4　シミュレーション結果

本研究の適用前は DoS 攻撃を受けたことによって回線のほとんどが DoS 攻撃トラヒックに占有されてしまっている．本提案を適用すると，DoS 攻撃による回線使用率が半減していることが分かる．

3.2.　公的セキュリティポリシによるネットワークサービス

公的セキュリティポリシとは，公衆ネットワークの利用に関する法律やガイドラインのことである．現在定められているものとしては，ネットワーク提供者に対する電気通信事業法や，ネットワーク利用者に対する不正アクセス禁止法，迷惑メール法などがそれに当たる．前者は，ネットワークの運用管理について「検閲の禁止」，「通信の秘密」，「利用の公平」が義務付けられており，後者は，意図的な不正利用（能動的攻撃）を個々に禁止する法律として規定されている．しかし，これら法律やガイドラインでは，ネットワーク提供者が，意図的な不正利用（能動的攻撃）全般を防止できる権限が無い．またネットワーク利用者は，意図しない不正利用（受動的攻撃）を防止する義務が無い．そのため，ネットワーク提供者には利用者のセキュリティレベルに応じてネットワーク利用を制御できる仕組みや，ネットワーク利用者にはセキュリティ意識を高める（インセンティブを与える）仕組み作りが必要であると考えている．以下に，公的セキュリティポリシを利用したセキュリティ対策の提案を以下(1)～(3)に示す．

(1)情報セキュリティデータベースを用いたインターネット優先転送方式[2]

インターネットにおいて前述のような脅威が増す大きな要因として，インターネット利用に関する制限あるいは社会制度が殆ど設けられていないことが挙げられる．例えば，公道を走る自動車を運転するためには運転免許が必要であったり車自体が整備してあるかどうかの車検制度があるが，公衆ネットワークであるインターネットの利用にはユーザ自身にもユーザの端末に対しても，そのような制度は無い．このため，匿名ユーザが不正な行為をした場合にそれを特定する術がない．そこで，自動車交通制度を参考にして，インターネットの利用優先制度を導入し，公的な資格のデータベースと

してセキュリティデータベースを構築する．そのデータベースを利用し，利用者の資格に応じた優先転送を行なうことについて下記の方法を提案した．

① インターネットの利用に関して，以下の公的資格証・検査証を与える．
  - 利用優先資格証
  - 情報通信機器検査証，NW 検査証

② ブラックリスト等の非公開情報及び調査結果の管理機関等での流通

③ 公開，非公開部分を分離したセキュリティ DB 管理
  - 第三者機関による商用サーバのセキュリティレベルの格付けが必要

利用優先資格証とは免許証のようなものであり，ユーザがネットワークを利用する上での資格を証明する．情報通信機器検査証とは端末の正常性を証明し，NW 検査証は企業などを含むユーザの LAN や，ISP が所有するネットワーク，また ISP 同士を接続したりバックボーンである WAN など，全ての IP ネットワークを対象に，その正常性を証明する．これにより，ユーザについては一定の利用資格を割り当てることができ，端末，IP ネットワークにも安全性が確保されたものが使用される．そのユーザの資格や端末・IP ネットワークの安全性はセキュリティ DB に蓄積され，その DB に基づき，ネットワークの利用が制御される．問題が発生した場合には公的機関により利用状況とセキュリティ DB を調査し，該当者に注意を促すことができる．このようにすることで，不正利用を抑えようとするものである．

(2)情報セキュリティのための IP ネットワーク利用制御[3]

インターネットは電話網のようにネットワーク全体を統合的に管理・制御する機構を持たないのが特徴である．このため，ネットワークの拡張性と利用の自由度を高めたが，一方で悪意ある利用も促進する結果となってしまっている．そこで我々は，IP ネットワークも電話網同様に通信事業者らによる管理された IP ネットワークの構築を提案した．この管理された IP ネットワークは，利用者の通信を転送する「転送系」と，セキュリティの観点から通信接続やパケット転送を管理・制御する「管理・制御系」の 2 層構造を成している．また，IP ネットワークは利用者のセキュリティに関する証明書を発行・管理する機能を持ち，IP ネットワーク利用にあたってはゲートウェイで利用資格を検証し，その検証結果によって管理・制御系において通信の接続やパケット転送の制御を行なう．

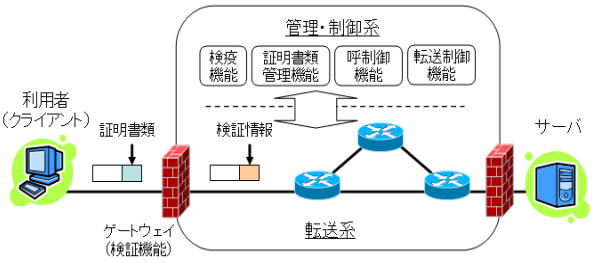

図 5　管理・制御された IP ネットワーク構築

(3)ユーザの安全性評価に基づいたネットワーク利用制御[4]

本提案は，IP ネットワークに接続しようとするユーザの端末を，IP ネットワーク側においてその安全性を評価し，より安全な端末の通信は優先度を高く，逆に安全性の低い端末の通信は優先度を低くすることで，IP ネットワークの利用を制御しようとするものである．概要図を図 6 に示す．ネットワーク利用者が IP ネットワークに接続しようとした際に，検疫ネットワークのようにユーザの端末に対してアンチウィルスソフトのパターンファイルのチェックや OS のパッチの有無などの検証を行う．検証を行うデータベースサーバには，セキュリティベンダ等より常時最新のパターンファイル，パッチファイルの状況が蓄積されている．その検証結果により，ユーザの安全性を評価し，その評価レベルによって通信できるトラヒック量をコントロールする．この研究では，ユーザの安全性

評価に「共通脆弱性評価システム（CVSS v2)」を活用している．また，IP ネットワーク内での利用制御には DiffServ の QoS のメカニズムを利用し，CVSS v2 の評価結果を用いて利用制御を実現している．

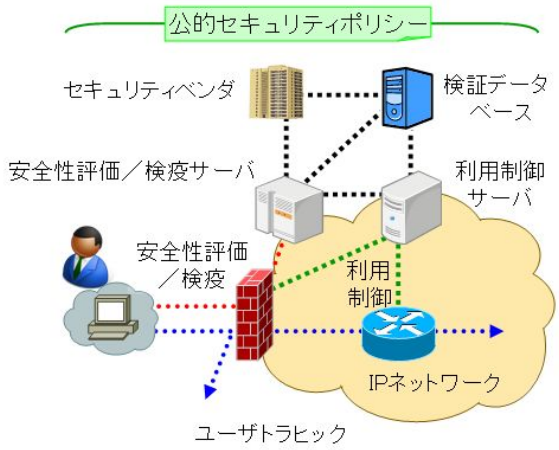

図 6　ユーザの安全性評価に基づいたネットワーク利用制御

この研究のシミュレーション結果を図 7 に示す．ユーザの評価が良い順に，ユーザ A，ユーザ B，ユーザ C が居たとする．本研究の利用制御実施前（利用制御無し）ではどのユーザも均一に通信できていたのに対し，利用制御実施後（利用制御有り）では，評価の良いユーザ A はより多くの通信が可能になり，評価の低いユーザ C は通信が抑制されている様子が分かる．

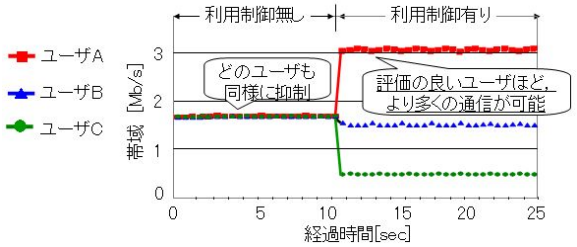

図 7　シミュレーション結果

4.　おわりに

安心して利用できる IP ネットワーク実現のために様々な研究がなされている．IP ネットワークから不正利用を排除しようとした時，インターネットの自由度に比べれば，その自由度が多少は損なわれる可能性はある．しかし，十分な管理機能を持つ IP ネットワークの構築によるネットワーク利用の正常化や，コスト負担のシフト（ユーザ側からネットワーク側へ）等，ユーザが安心･安全に利用できる IP ネットワークの構築は必要であると考える．今回我々もその一部を提案した．今後も引き続きユーザが安心･安全に利用できる IP ネットワークの構築を目指していきたい．

参　考　文　献

[1] 西川康宏，岡田康義，佐藤直，“私的セキュリティポリシを利用した NGN における DoS 対策の考察” SCIS2009，2E3，2009,1

[2] 岡田康義，佐藤直，“情報セキュリティデータベースを用いたインターネット優先転送方式”，信学技報 ISEC2007-17，2007.7

[3] 佐藤直，岡田康義，“情報セキュリティのための IP ネットワーク利用制御”，情報処理学会第 70 回全国大会，5E-6，2008.3

[4] 堀琢磨，岡田康義，佐藤直，“ユーザの安全性評価に基づいたネットワーク利用制御”，電気情報通信学会，2009,3