［論文］

セキュリティポリシーに基づくネットワークトラヒック制御の提案

岡田 康義、西川 康宏、堀 琢磨、佐藤 直

要 旨

インターネット等の TCP/IP をベースとした公衆ネットワークを利用する際は，ユーザが個々に保有するホスト端末や LAN 等の情報システムにセキュリティ対策を実施しているのが現状である．一般に，ネットワークがブロードバンド化され利便性が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する傾向がある．この原因は，セキュリティの観点からインターネットを流れるトラヒックを監視・管理する十分な機能が公衆ネットワーク側に備わっていないためである．そこで，本文では，私的セキュリティポリシーおよび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公衆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．ここで，私的セキュリティポリシーは従来ユーザが個々に実施しているセキュリティ対策機能であり，同機能をネットワーク側に移行して実施することで，ユーザのセキュリティ対策に関する負担を軽減する．また，公的セキュリティポリシーは，ユーザの情報通信システムの脆弱性検査結果に基づき，セキュリティレベルが高いユーザに優先的に帯域を割り当てることで，公衆ネットワークのトラヒックの安全性を高める．インターネットへのアクセスネットワークである NGN を対象にして本提案の適用例を示し，計算機シミュレーションにより有効性を検証した．具体的に，私的セキュリティポリシーについては，UDP フラッド攻撃に対する私的セキュリティポリシーを適用し，NNI でパケットフィルタリングする例を示した．NS2 を用いた計算機シミュレーションにより，UDP フラッド攻撃パケットがフィルタリングできることを確認した．同時に，私的セキュリティポリシーは適用したユーザのみならず，アクセスネットワークを共同利用する他のユーザの利用帯域も確保することがわかった．また，公的セキュリティポリシーについては，セキュリティレベルに応じた 3 つのクラスを設け，優先制御する例を示した．同様の計算機シミュレーションにより，Diffserv と WRR のサービス品質技術を組み合わせてこの公的セキュリティポリシーが実現できることを確認した．また，セキュリティ攻撃はセキュリティレベルの低いユーザの情報通信システムを踏み台に行われることが多いことから，公的セキュリティポリシーは DNS リダイレクト攻撃のような異常トラヒックが発生した場合でも正常なトラヒックを確保できることがわかった．

Abstract

The users of TCP/IP based public information-and-telecommunication networks such as the Internet are implementing security countermeasures to their information systems such as terminals and LAN on their own responsibilities. The more broadband services increase user convenience, the more security countermeasures the users tend to be burdened with. The above security issues are believed to be due to lack of sufficient monitoring and managing functions on the public networks. So this paper proposes a traffic control method for network security, which uses private and/or public security policies. The private security policy deserves the conventional security function implemented at the individual user information system. The paper proposes to move the conventional security function to the public networks and ease the users' burden. The public security policy aims to increase security of packet traffic on the public networks, and is developed on the basis of on vulnerability assessment of the individual user information systems. According to vulnerability assessment results, broader bandwidth is allocated to the user of higher security. In order to discuss the proposal practically, the paper especially focuses NGN as both public networks and access networks to the Internet, and describes some examples of mapping of the private and public security policies on packet transmission function on NGN. As for the example of applying the private security policy, it is verified through a computing simulation by NS2 that the proposed method can successfully filter traffic due to UDP flood attack at NNI. Further it is found that the private security policy maintains bandwidth of the other user who shares NGN but does not use any private security policy, as well as that of the user applying the private security policy. As for the example of the public security policy, the paper gives three classes to IP packets in accordance with assessed security level, and discusses packet transmission with priority. By the similar computing simulation, it is demonstrated that the combination of two QoS technologies; Diffserv and WRR effectively can make the public security policy into practice successfully. As a second effectiveness of introducing the public security policy, it is also found that abnormal traffic due to security attacks like DNS redirection attack can be blocked by applying the policy, because information system of low security tend to be easily compromised and most security attacks with the abnormal traffic are actually done via the compromised user information systems.

A Proposal on Network Traffic Control Based on Security Policy

Yasuyoshi Okada, Yasuhiro Nishikawa, Takuma Hori, Naoshi Sato

情報セキュリティ大学院大学

Institute of Information Security

［論文］2012 年 08 月 04 日受付
2013 年 12 月 30 日受理

1 はじめに

現在のインターネットは「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，安心や安全への対策も基本的に端末 (ユーザ) 側へ依存している．インターネットが近年急成長を成し遂げた背景には，上記の発想が大きく寄与している．他の社会インフラと異なり，管理組織がなく，容易にネット

ワークの拡張や端末の接続が可能なことで利便性が飛躍的に高まったのは事実である．ところが，組織的に管理をおこなわないことから，悪意をもった者にとっても好都合な利用環境となっている．さらに，情報通信システムの脆弱性を突いた攻撃の手口は巧妙かつ高度なものへと変化しているため，従来のようにユーザ側の情報セキュリティ（以下セキュリティと呼ぶ）対策だけでは十分対応することが困難になっている．

上述した問題を解決するには，ユーザ側のみならず，ネットワーク側でも一定のセキュリティ機能を持ち，ユーザ側のセキュリティ機能と協調して，安全なネットワーク利用環境を実現するのが望ましいと考える．本稿ではこの安全なネットワーク利用環境を実現する一つの手段として，インターネットを含む公衆ネットワーク側に私的あるいは公的セキュリティポリシーを反映してトラヒックを制御する手法を提案する．

以下,第 2 章では研究の背景と目的を述べる．次に，第 3 章でセキュリティの観点からみたトラヒック制御について，既存検討や本文における検討指針を示す．第 4 章で提案内容を示す．第 5 章では提案の適用例を示し，トラヒック制御効果を計算機シミュレーションで確認する．第 6 章で本提案の適用について工学および社会学の視点から考察を行い，最後に第 7 章で検討結果をまとめる．

2 研究の背景と目的

2.1 セキュリティ対策の実態と課題

現状,インターネット等の TCP/IP をベースとしたネットワークサービスの企業ユーザや個人ユーザは複数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，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，幾重にもセキュリティ対策を施している．ネットワークサービスが趣味嗜好の用途にのみ利用されるのであれば,それらの安全性はユーザ自らが責任を負うべきであり，このような多くの負担を容認することも考えられる．しかし，TCP/IP が従来のネットワークをも包含する全てのネットワークの主要プロトコルとなり，提供されるネットワークサービスが社会生活全般の基盤となった今日，社会システムの安全性を確保するためにも，セキュリティの観点からネットワークの運用管理手法を確立する必要性があると考えられる．

2.2 セキュリティポリシーと課題

情報セキュリティマネジメントシステ ISMS（Information Security Management System）の国際規格 ISO/IEC 27001[1]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[2]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，インターネット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.しかしながら，一方では，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[3].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的な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るため，セキュリティポリシーを適用することが肝要であると考えられる．

2.3 研究の目的

2.1 と 2.2 で示した課題から，本文では，二つのトラヒック制御技術の確立を目的とする．最初に，私的セキュリティポリシーを用いたトラヒック制御技術の確立を図る．すなわち，悪意のあるパケットがユーザに到達しにくくするために，LAN 等各ユーザのネットワークに適用

していた私的セキュリティポリシーをインターネットのような公衆ネットワーク側で実施してトラヒック制御する技術を確立する．本技術により，悪意のあるパケットのユーザ自身のネットワークへの流入を防止し，ユーザが利用する通信帯域を確保する．

次に，公的セキュリティポリシーを用いたトラヒック制御技術の確立をめざす．ここで，公的セキュリティポリシーとは，公衆ネットワークのユーザに共通的に適用するもので，セキュリティの観点からユーザの公衆ネットワーク利用環境を評価し，他のユーザに対するセキュリティ上の脅威を減少させる．本技術により，セキュリティの高いユーザほど高優先でインターネットを利用できるようにする．同時に，不正パケットが公衆ネットワークで転送される可能性を低減させる．

3 既存検討と本研究における検討指針について

インターネットでは，P2P へビーユーザのファイル共有によるネットワーク帯域の占有が恒常化しており，他の一般ユーザの通信速度低下を招いている.そこで,社団法人日本インターネットプロバイダー協会（JAIPA）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，インターネットサービスプロバイダ（以下 ISP と略す）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［4]．しかし，このガイドラインは，セキュリティ対策の視点が十分でないように見受けられ，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，これらの問題の解決に向け，具体的に，以下のような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）私的セキュリティポリシーの導入に基づく DoS 攻撃抑制

DoS 攻撃の抑制に関するユーザ毎の私的なセキュリティポリシーをユーザのネットワークのみならず,公衆ネットワークに設定･運用する．

従来技術では，WAN と LAN の境界にファイアウォールを設置して DoS 攻撃をブロックする際,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ている.そのため,DoS 攻撃のトラヒックの流入を防ぐ観点からみると，当該ユーザのネットワークへの流入は防げるが，公衆ネットワークを共有する他のユーザの受信帯域は確保されないため，効果が限定的であった．そこで，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へ拡張することで同ユーザの負担を軽減し，さらに，公衆ネットワークの受信帯域もより正常に維持することを目的とする．本文では，具体的な DoS 攻撃として UDP フラッドを例にして，私的セキュリティポリシーを公衆ネットワークに導入する．具体的には，UDP フラッドに占有される帯域を利用可能帯域の一定の割合以下に抑えるようポリシー設定する．この私的セキュリティポリシーをユーザの属する通信事業者のアクセスネットワークに導入することで，ポリシー設定したユーザへの UDP フラッドの被害を緩和するとともに，直接に攻撃対象ではないその他のユーザに与える影響も小さくする．

指針 2）公的セキュリティポリシーの導入に基づくパケット優先転送

公的なセキュリティポリシーとは，端末や LAN といったユーザの利用環境に関する脆弱性検査指針を定め，セキュリティレベル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しようとするものである．この公的セキュリティポリシーは公衆ネットワーク利用ユーザ全体のコンセンサスに基づき導入する．本ポリシーの導入により，ユーザのセキュリティ意識を向上させるとともに，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．

従来，企業等のプライベートネットワークでは，端末や LAN の脆弱性検査指針を定め，同指針に適合した場合にのみネットワーク利用を許可することが多い．本指針は，このようなプライベートネットワークにおける利用指針を公衆ネットワークに適用しようというものである．

なお，セキュリティレベルの低い端末や LAN からのトラヒックを禁止するのではなく，サー

ビス品質技術（QoS）を用いて，パケット転送を差別化することを特徴とする．なお，この指針2 は憲法や電気通信事業法で禁止されている「通信の秘密」に抵触しないことを前提に検討する．具体的には，ユーザが送受信する情報（コンテンツ）の内容を検査するのではなく，ユーザの利用環境のセキュリティレベルを調べ，その結果に応じて，パケット送出側の利用帯域を制御することとする．

指針 3）指針 1 と指針 2 はインターネット等のアクセスネットワーク(ユーザが,家庭やオフィスからパソコンなどでインターネットを利用する場合に，パソコンを直接接続するネットワーク）に適用する．

すなわち，指針 1 については，私的セキュリティポリシー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こととする．指針 2 については，全ての ISP が共通の公的セキュリティポリシーに即してエンド・エンドでトラヒック制御することが望ましいが，ISP のネットワーク管理の独自性を損なうことから現実的でない．そこで，指針 2 についてもアクセスネットワークで実施することとする．

本論文では，セキュリティポリシーに基づくトラヒック制御のしやすさから NGN（Next Generation Network）を適用対象として検討することとする．また，なお，指針 1 と指針 2 は独立なセキュリティポリシーであることから，独立に検討する．

次に，本検討と関連する既存検討について述べる．指針 1 により DoS 攻撃を抑えるための既存技術として，パケットフィルタリングによりトラヒック制御する Moving FireWall 技術[5]がある．同技術は，ユーザが DoS 攻撃に伴うトラヒック異常を検出すると，攻撃元に向かってフィルタリング機能を移動させるという特徴を有するが，インターネットのような公衆ネットワークの全体にわたってトラヒックの正常性を確保しようとすると，トラヒック異常検出機能およびフィルタリング機能を中継ネットワークに多く設定する必要があり，指針 3 でも述べたように拡張性の面で難点がある．また，指針 2 の QoS の適用に関しては，QoS の持つ優先転送制御機能により DoS 攻撃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おこなわれている[6]．しかし，セキュリティポリシーの設定やその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．

4 セキュリティポリシーに基づくトラヒック制御の提案

前章までの議論を踏まえて，私的及び公的セキュリティポリシーに基づくトラヒック制御を提案する．以降，図 1，図 2 のようなトラヒック制御モデルを例に検討する．両図においてユーザはインターネットへのアクセスネットワークとして NGN を利用している．本文で提案する私的及び公的セキュリティポリシーの適用対象として，NGN は以下のような利点を有する．すなわち，NGN は比較的低速なアクセスネットワークであり，高速な中継ネットワークよりも技術的に実施しやすい．また，ネットワーク層レベルのトラヒック制御機能を有する．なお，他のアクセスネットワークであっても，ネットワーク層レベルのトラヒック制御機能を有する場合は同様に提案が適用可能である．図 1，図 2 に示すように，NGN はユーザ側とインターネット側に対しそれぞれ UNI（User-Network Interface），NNI（Network-Network Interface）でインタフェースする[7]．UNI と NNI にはエッジルータ ER（各々，UER，NER)が設置され，セキュリティポリシー設定やトラヒック制御の実施主体となる．また，必要に応じてコアルータ(CR)が UER と NER の中間に位置しトラヒック制御に関わる．

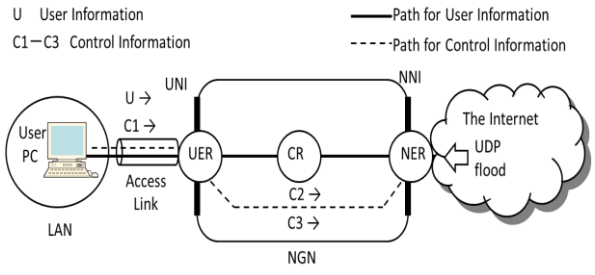

図 1　私的セキュリティポリシーに基づくトラヒック制御モデル

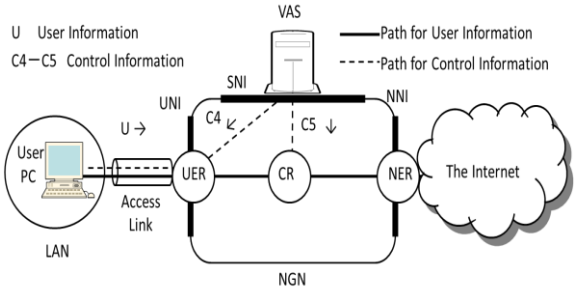

図 2　公的セキュリティポリシーに基づくトラヒック制御モデル

4.1 私的セキュリティポリシーに基づくトラヒック制御

前章でも述べたように，企業等のユーザが現実に直面しているセキュリティ攻撃として DoS 攻撃がある．代表的な DoS 攻撃として SYN フラッド，ICMP フラッド，UDP フラッドといったフラッド攻撃がある．いずれもユーザに大量のパケットを送りつける量的な攻撃で，パケット個々にセキュリティ上の問題があるか否かを区別することが難しいため，ユーザの受信側アクセスネットワークの帯域を消費させるのに効果的な攻撃である．このようなフラッド攻撃に対しては単位時間あたりの受信パケット量に対する閾値を予め定め，同閾値を超えた場合，フラッド攻撃と判定してトラヒック制御することが必要になる．このフラッド攻撃による影響を軽減するには，ユーザから見てより攻撃元に近い場所でトラヒック制御するのが望ましい．そこで，フラッド攻撃が生じても受信側アクセスネットワークの帯域を確保しやすくするため，UNI より上流に位置する NNI でトラヒック制御することを提案する．

次に，私的なセキュリティポリシーとして以下を提案する．すなわち，イニシエータ（通信開始者）が私的セキュリティポリシー設定ユーザからみて外部のユーザであり，この外部のユーザから受信するトラヒックがアクセスネットワークのユーザの利用可能帯域の一定割合を超えたらフラッド攻撃とみなして同トラヒックを NNI で遮断する，ことを提案する．前述したように，該当するフラッド攻撃は複数あるが，なかでも UDP フラッドはアクセスネットワークの帯域を占有するのに比較的効果が大きい．そこで，以下，UDP フラッド攻撃に対するトラヒック制御について，この私的セキュリティポリシーを定め，その運用を実施する[8][9]．

4.1.1 私的セキュリティポリシーの決定

アクセスネットワークの帯域を消費させる DoS 攻撃の例として UDP フラッドを対象に検討する．ここで，ユーザが下記のようにインターネット接続サービスを利用していることを仮定する．すなわち，Web サーバを用いて，大規模映像ライブ配信や蓄積型大規模動画配信ストリームサービス等を提供している企業ユーザがあるとする．上記のような Web サーバを公開サーバとして設置し，TCP により，比較的広帯域を使用して顧客と通信することが多い．一方，UDP を利用した通信として DNS や IP 電話等があるが，TCP に比べて狭い帯域で十分であることが多い．なお，利用帯域はトラヒックの変動を考慮して，ISP との契約帯域の 7 割程度で運用するのが一般的である．また，UDP による外部からのアクセスを許可するのは，原則として，予めホワイトリストに登録されている送信者の場合とする．しかし，全ての UDP 送信者を登録するのは困難なため，使用帯域が微小ならば未登録の送信者からの UDP トラヒックの流入も許容しているものとする．

上記のようにインターネット接続サービスを利用している場合，私的セキュリティポリシーを次の例のように設定することが考えられる．すなわち，未登録の送信者からの UDP トラヒックが受信側契約帯域の 3 割を超えたことをもって UDP フラッドが発生したものと判断し，該当する UDP トラヒックを制御する．この UDP トラヒック制御の具体的なアクションとして，該当トラヒックをファイアウォールで全て遮断する（パケットを廃棄する），あるいは，QoS を用いて低優先での通信を許可することが考えられる．前者は正常な UDP トラヒックを異常と誤判定する可能性があり，後者は UDP による不正アクセスを見逃す可能性があるため，完全な UDP フラッド検出を期すのは困難であるが，いずれかの制御アクションを採択するものとする．

次に，NGN における UDP フラッド検出とトラ

ヒック制御の実施ポリシーを定める．図 1 のように，インターネットからユーザにパケットが到達する経路が一つであれば，UDP フラッド検出とトラヒック制御をともに NNI で実施できるが，マルチホーミングで複数の ISP と契約するなど，インターネット接続に冗長性を持たせ信頼性を高めることもある．この場合，複数個所の NNI から UDP フラッドパケットがユーザに到達し,攻撃が成功する危険性が大きい.そこで，このような複数経路による UDP フラッドに備えるため，NNI ではなく UNI で UDP フラッドを検出し，検出結果を NNI にリアルタイムに伝え，NNI でトラヒック制御を実施するものとする．

4.1.2 私的セキュリティポリシー設定とトラヒック制御実施までの流れ

前節で決定された私的セキュリティポリシーを NGN に設定し，トラヒック制御するまでの流れを検討する．私的セキュリティポリシーをオフラインでユーザが NGN 事業者に伝え，手動で静的に設定することも考えられるが，動的に設定できれば，迅速かつ柔軟なトラヒック制御が可能となる．そこで，オンラインでの設定を行うものとする．

まず，ユーザは SIP 等による制御信号（図 1 の C1）を用いて，予め定めた UDP フラッド検出とトラヒック制御に関するポリシーを UNI の UER に伝える．次に，UNI の UER は自身にこの UDP フラッド検出ポリシーを設定するとともに，NGN 内の制御信号（C2）を用いて，トラヒック制御の実施ポリシーを NNI の NER に伝える.UNI の UER で UDP フラッドを検出した場合，同様に制御信号（C3）が NNI の NER にリアルタイムに伝えられ,NNI の NER は先に設定されたポリシーに基づき UDP トラヒックを制御する．

以上のように，私的セキュリティポリシーを決定・設定・実施することによって，NNI の NER において UDP フラッドを無力化する．ICMP フラッドのような他のフラッド攻撃についても同様なトラヒック制御が可能と考えられる．

4.2 公的セキュリティポリシーに基づくトラヒック制御

企業ユーザは，インターネット接続された情報通信システムが外部からの攻撃に対して安全かどうか，攻撃手法を試しながら安全性を検証する脆弱性検査，いわゆる，ペネトレーションテスト（疑似侵入試験）[10]をおこなうことがある．脆弱性検査に精通している社員が企業内にいることは少ないため，多くの場合セキュリティベンダに委託して定期的に遠隔から脆弱性検査を受けている．検査の結果，新たなセキュリティ対策が必要な場合はセキュリティベンダのアドバイスに基づき実施してインターネット利用の安全を向上することができる．現状，この脆弱性検査は企業等が設置している Web サーバ等の公開サーバを対象としていることが多い，検査内容はセキュリティベンダのノウハウとなっており公開されていない．しかし，将来的には，対象を個人ユーザに拡大するとともに，標準的な実施ガイドラインを策定してインターネット等の公衆ネットワークの利用条件の一つとして適用することが考えられる．ただし，検査結果によって公衆ネットワークの利用の可否を二者択一的に制御することは許容されないであろう．そこで，本節では，脆弱性検査の結果に基づいてインターネット等の公衆ネットワークの利用帯域を差別化することを提案する．すなわち，公的セキュリティポリシーとは，端末や LAN 等の公衆ネットワーク利用環境のセキュリティレベルを評価し，その結果を用いてパケット転送の差別化を行うことである．

具体的には，脆弱性が少なくセキュリティレベルが高い利用環境からのパケットを優先転送し,そうでない場合は非優先とする.すなわち，脆弱性を持つような利用環境からのトラヒックは，帯域の大きい高速ネットワーク（サービス）ではなく，帯域の小さい低速ネットワークで転送するという考え方をとる．このような優先転送制御のユーザに与える影響としては，脆弱性の少ない利用環境を使用しているユーザの利用帯域を増大し，応答遅延などのサービス品質を向上することが考えられる．さらに，ユーザのセキュリティ意識や情報モラルの向上，ひいては，ネットワークセキュリティの全体的な向上が期待できる．

以下，このような利用環境のセキュリティレ

ベルに応じたトラヒック制御について，公的セキュリティポリシーを定め，そのポリシーに基づき運用する手順を提案する[11].

4.2.1 公的セキュリティポリシーの決定

最初に，インターネット等の公衆ネットワークの利用条件として,脆弱性検査により,セキュリティレベルを評価する．次に，このセキュリティレベルに基づいてパケットを優先転送制御する.

(1)脆弱性検査によるセキュリティレベルの評価

前述したように，脆弱性検査の内容は公開されていないが，広く実施されており技術的には確立されている[10]と見受けられるので，概ね従来技術をそのまま適用すればよいと考える．さらに，以下の①，②に示すような，脆弱性検査の実施およびセキュリティレベルの評価を提案する.

① 脆弱性検査の実施

情報通信システムの脆弱性を定義したデータベースとして広く利用されているものに共通脆弱性識別子 CVE(Common Vulnerabilities and Exposures)データベースがある[12]．CVE は基本 OS やアプリケーションソフト等情報通信システムを構成する個別製品中の脆弱性の識別子である．脆弱性検査のための各種ツールが提供されており，多くのツールはこの CVE に対応している．そこで，この CVE をもとにユーザの利用製品が関連する脆弱性項目について疑似攻撃を実施して脆弱性の有無（セキュリティ攻撃の可否）を判断する.

② キュリティレベルの評価

個々の脆弱性の深刻度を評価する標準的な方式として，共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）がある[13]． この CVSS では基本評価基準，現状評価基準，環境評価基準を設けている．基本評価基準は各セキュリティ攻撃が成功した場合の影響の深刻さを，現状評価基準は各セキュリティ攻撃の発生状況や対策技術の実現状況を考慮した深刻さを，環境評価基準は各ユーザの利用環境を含めた最終的な深刻さをそれぞれ評価する．各基準による評価値は基本値，現状値，環境値と呼ばれ，算出法が規定されている．これらの評価値を計算するツールも公開されている．本検討はユーザの利用環境を含めて脆弱性を検査することから，セキュリティレベルの評価は環境値に基づくのが適切であると考えられる．そこで，①で脆弱性有りと判断された個別製品の脆弱性について環境値を単純加算する，あるいは，環境値の最大値をとる，ことで利用環境（全体）の環境値とする．このように評価することから，脆弱性が多いほど，あるいは，深刻な脆弱性があるほど利用環境の環境値は大きく，セキュリティレベルが低いと評価される.

(2)セキュリティレベルに基づくパケット優先転送制御

次に，以上のような，セキュリティレベルの評価結果を用いた優先転送制御のための公的セキュリティポリシーを決定する．例えば，前述の環境値の最大値が 4 未満ならセキュリティレベルは High，4 以上 7 未満なら Middle，7 以上なら Low とし，このセキュリティレベルに対応する優先度情報をパケットヘッダのオプションフィールド等に記載・参照して優先転送制御する．すなわち，セキュリティレベルが High／Middle／Low なら高優先／中優先／低優先でパケットを転送する，というように公的セキュリティポリシーを設定するものとする.

4.2.2 公的セキュリティポリシー設定とトラヒック制御実施までの流れ

上述の公的セキュリティポリシーは NGN 事業者が図 2 の UNI の UER と，UNI と NNI の中間に位置する CR に設定する．また，セキュリティレベルは，NGN 事業者自身あるいは NGN 事業者から委託を受けたセキュリティベンダが，図 2 の SNI(application Server Network Interface)を介し，脆弱性検査サーバ VAS（Vulnerability Assessment Server）からリモートで定期的に，あるいは，重大なセキュリティインシデントが発生した場合等，必要に応じて脆弱性検査を実施し，ユーザのインターネット利用環境のセキュリティレベルを評価する．脆弱性検査の際は端末の使用を停止するなど，ユーザの協力が必要になると想定されることから，実施スケジュールについて予めユーザ個々の了解をとり

つけることが求められる．また，脆弱性検査の結果をユーザに報告しセキュリティ対策に関する指導を行う，といった業務も行う．

次に，公的セキュリティポリシーによるトラヒック制御技術を考察する．優先度を定めて相対的にパケット転送品質を差別化するサービス品質技術 QoS として Diffserv (Differentiated Service) [14]が広く適用されている．Diffserv ではパケットヘッダに搭載された品質クラス情報に基づいて優先転送制御を行うが，この品質クラス情報と同様に前述の優先度情報を設定することで本提案を実現できる．具体的に，図 2 の VAS は SIP 等による制御信号（C4）を用いてユーザ毎のセキュリティレベル評価値を UNI の UER に伝える．UER は同ユーザの利用環境から送信されるパケットのヘッダにセキュリティレベル評価値に応じた優先度情報を記載して CR に転送する．また，VAS は制御信号（C5）を用いて，DiffServ 実施のための PHB（Per Hop Behavior）を CR に設定する．この PHB はヘッダに記載された優先度情報に基づく優先転送動作の仕様である．公的セキュリティポリシーの運用により，UNI から NGN に流入したパケットは UER および CR によりトラヒック制御される．

5 トラヒック制御シミュレーション

本文で提案したトラヒック制御の有効性を計算機シミュレーションで確認する．計算機シミュレーションにはネットワークシミュレータとしてよく用いられる NS2[15]を用いる．

5.1 私的セキュリティポリシーとトラヒック制御特性の評価

私的セキュリティポリシーに基づいたトラヒック制御のシミュレーションを 2 つのモデル；モデル 1 とモデル 2 について実施した．モデル 1 では提案の有効性を私的セキュリティポリシー実施ユーザ（提案実施ユーザと呼ぶ）の視点から確認する．モデル 2 では提案実施ユーザの以外のユーザ(他ユーザと呼ぶ)のトラヒックにも提案が間接的な効果があることを示す．

(1)モデル 1

モデル 1 とそのシミュレーション結果をそれぞれ図 3，図 4 に示す．

＜シミュレーションの前提＞

図 3 において，TCP および正常な UDP のトラックが NNI の NER0 から CR へ，さらに UNI の UER を介して提案実施ユーザに対して転送されるものとする．ここで，TCP と正常な UDP のトラヒックは予めホワイトリストに登録された送信者からのトラヒックである．また，100 個の送信元から UDP フラッドが同ユーザに送信されるものとする．NNI における 10 個の NER；NER1～NER10 を経由して，UDP フラッドが NGN に流入する．各 NER には各々10 個の送信元からの UDP フラッドが流入するものとする．NER1～NER10 と CR，および UER と提案実施ユーザ間の通信速度は 10Mb/s とする．CR と UER の間の通信速度は 20Mb/s とする．次に，TCP のアプリケーションは FTP で 4Mb/s の帯域が与えられている．正常な UDP は 2Mb/s の CBR（Constant Bit Rate）である．各 UDP フラッドの通信速度は 0.5Mb/s より大きいものとする．なお，キューマネジメントは Drop tail（バッファメモリがあふれている場合到着したパケットを破棄する方法）で，ラウンドロビン（Round Robin. 以下 RR と略す）によりスケジューリングするものとする．上記以外のトラヒックの影響は無視できるものとする．また，私的セキュリティポリシーとして，UNI において UDP トラヒックが 3Mb/s を超えた時，無登録の UDP のトラヒックは UDP フラッドとみなし，NER1～NER10 で該当パケットを全て廃棄する．

＜シミュレーション結果＞

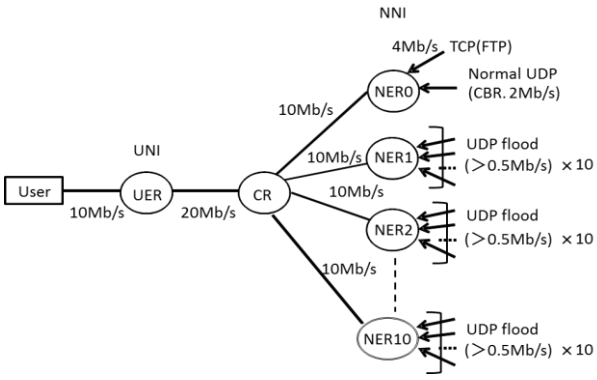

図 3　モデル 1

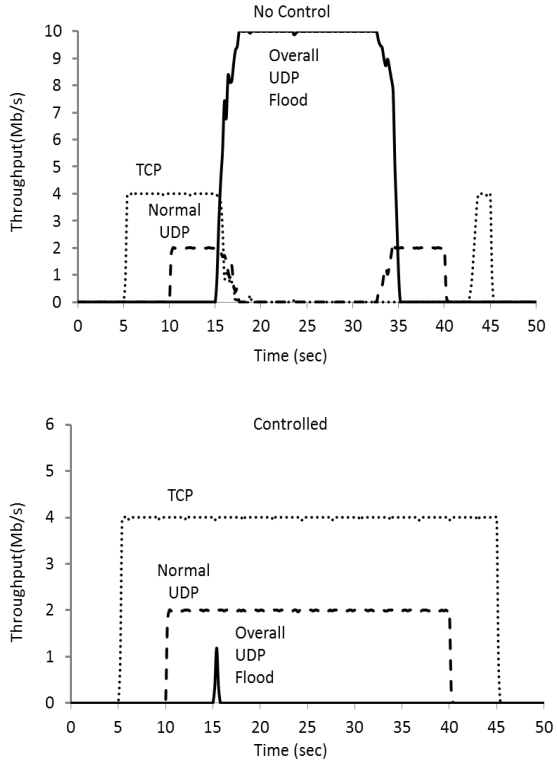

図 4　モデル 1 のシミュレーション結果

図 4 の上の図は，本提案を適用しない場合のシミュレーション結果（提案実施ユーザの受信速度）である．TCP の通信時間は 5 秒～45 秒，正常な UDP の通信時間は 10 秒～40 秒である．100 経路からの UDP フラッドは 15 秒から 0.05 秒間隔で順次発生し，20 秒で全ての UDP フラッドが発生している．また，30 秒から 0.05 秒間隔で順次停止し，35 秒で全ての UDP フラッドが停止している．提案を適用しない場合は，TCP と正常な UDP，および UDP フラッドのトラヒックを分類せず，一つのバッファメモリを全てのトラヒックが共有し，Drop tail でパケットを廃棄する．同図から分るように，UDP フラッドが発生しなければ，TCP は 4Mb/s に，正常な UDP の帯域は 2Mb/s に保たれるが，UDP フラッドが発生すると帯域（10Mb/s）が占有され，TCP や正常な UDP の通信ができないことが分る．図４の下の図は，本提案を適用した場合のシミュレーション結果である．NER1～NER10 では入力トラヒックを，送信者が登録された TCP と UDP，無登録の UDP，に分類し，それぞれに対応するバッファメモリを用いてキューイングを行う．図４の下の図では，UDP フラッドの帯域が 1Mb/s に達した 15 秒で UDP フラッドが検出され，以降廃棄されている．この制御のため，登録された TCP と UDP の NNI 内および提案実施ユーザの帯域が確保されている．

(2)モデル 2

モデル 2 とそのシミュレーション結果をそれぞれ図 5，図 6 に示す．

＜シミュレーションの前提＞

モデル 2 はモデル 1 の提案実施ユーザの他に，提案を実施しない一人の他ユーザ（The other user）とそのトラヒック（破線で示した）を追加して実施する．この追加された他ユーザは UDP フラッドの直接的攻撃対象ではない．図５において，この他ユーザは UNI において提案実施ユーザと同一の UER に収容され，10Mb/s で接続されている．他ユーザに対しては，TCP および正常な UDP のトラックが NNI の NER11， CR，さらに UNI の UER を介してパケットが転送されるものとする．

次に，TCP のアプリケーションは FTP で，5Mb/s の帯域が与えられている．正常な UDP は 3Mb/s の CBR である．TCP および正常な UDP のトラックの開始や終了は提案実施ユーザと同一である．

＜シミュレーション結果＞

図 6 の上の図は，本提案を適用しない場合のシミュレーション結果，すなわち，提案実施ユーザおよび他ユーザの受信トラヒックの通信速度特性である．ただし，煩雑になるため，UDP フラッドの特性は省いてある．モデル 1 のシミュレー

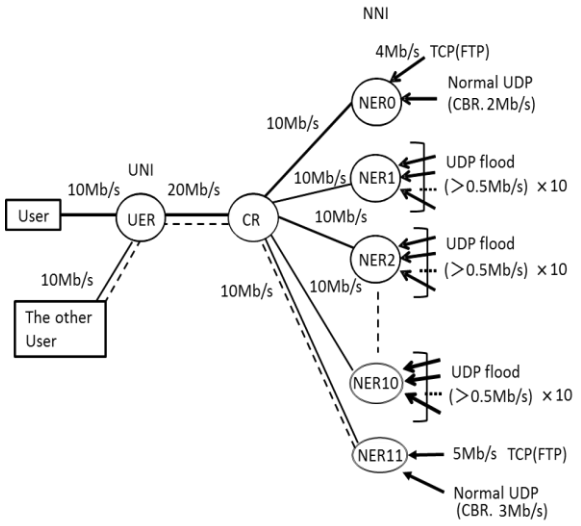

図 5　モデル 2

ション結果(図4の上の図)と同様に,UDPフラッドが発生しなければ,TCPや正常なUDPの帯域は正常に保たれるが,UDPフラッドが発生するとCRからUERの帯域20Mb/sが占有され,他ユーザは攻撃対象ではないにも関わらず,TCPや正常なUDPの通信ができないことが分る.図6の下の図は,本提案を適用した場合のシミュレーション結果である.モデル1のシミュレーション結果(図4の下の図)と同様にUDPフラッドが発生しても,提案法により,NNI内の帯域が正常に確保されるため,提案実施ユーザ,他ユーザともに正常に通信できることがわかる.このように,私的セキュリティポリシーによるトラヒック制御は,UDPフラッドのように通信帯域を消費してしまうDoS攻撃が発生した場合,提案実施ユーザのみならず他ユーザのトラヒックの正常性を保つのにも有効であるといえる.

5.2 公的セキュリティポリシーとトラヒック制御特性の評価

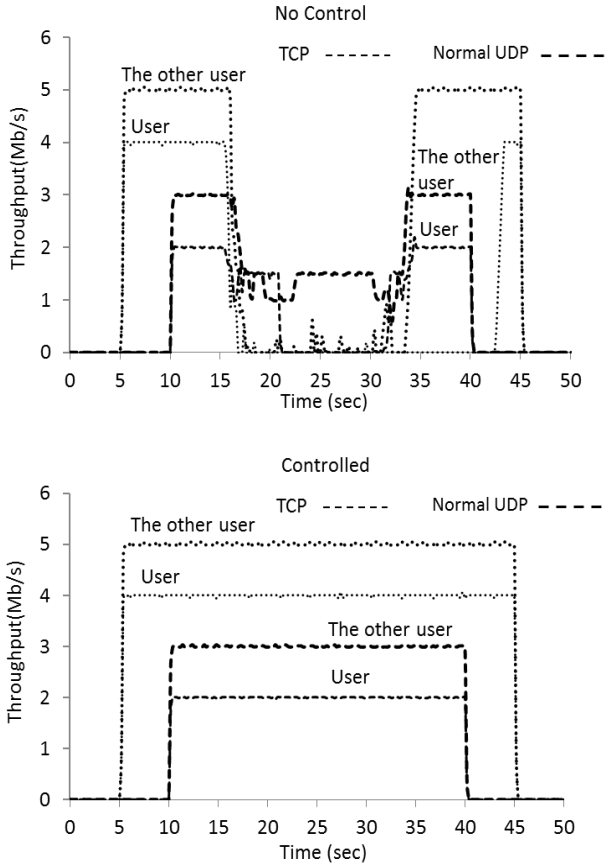

図6　モデル2のシミュレーション結果

公的セキュリティポリシーに基づいたトラヒック制御のシミュレーションを2つのモデル;モデル3とモデル4について実施した.モデル3では提案の有効性を帯域制御の視点から確認する.モデル4では提案が異常トラヒック対策としても有効であることを示す.

(1)モデル3

モデル3とそのシミュレーション結果をそれぞれ図7,図8に示す.

＜シミュレーションの前提＞

図7において,セキュリティレベルがHigh／Middle／Low(表1)である3つのユーザ端末(Host)が同じ速度(10Mb/s)でUNIにアクセスするものとする.3つの端末はNNIにおいて5Mb/sの契約帯域を共有してインターネット接続しているものとする.アプリケーションはいずれもFTPである.公的セキュリティポリシーを実施する場合,UNIのUERはセキュリティレベルHigh／Middle／Lowに応じて高優先／中優先／低優先の情報をIPヘッダに付してCRに転送する.CRは公的セキュリティポリシーを適用しない場合はRRで,適用する場合はWRR(Weighted RR)[16]でスケジューリングするものとする.WRRでは6:3:1で高優先／中優先／低優先パケットに帯域を割り当てるものとする.なお,いずれの場合もキューマネジメントはRED(Random Early Detection)[16]とした.

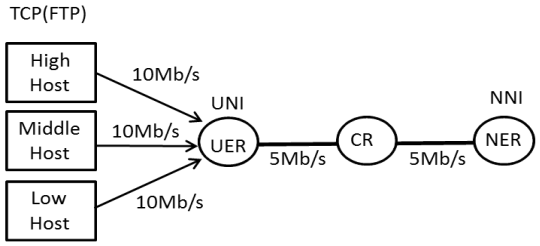

図7　モデル3

表1　セキュリティレベルと優先度

セキュリティレベル	脆弱性評価値(CVSS環境値)	優先度(Diffserv PHB)
High	4未満	高優先
Middle	4以上7未満	中優先
Low	7以上	低優先

＜シミュレーション結果＞

図 8 の上の図は，本提案を適用しない場合のシミュレーション結果（NNI の NER における通信速度）である．セキュリティレベル High／Middle／Low 端末の通信時間はそれぞれ 0 秒～35 秒，5 秒～30 秒，10 秒～25 秒である．同図では，優先転送制御をおこなわないため，割り当て帯域の比率はトラヒック量にのみ依存する．すなわち，よりセキュリティレベルの低いトラヒックが増えるとセキュリティレベルの高いトラヒックの帯域が圧迫されることが分る．図 8 の下の図は，本提案を適用した場合のシミュレーション結果である．3 つの端末は同一のアプリケーション，同一のアクセス条件でネットワーク利用しているにも関わらず優先転送制御によって利用帯域が差別化されていることが分る．

(2) モデル 4

モデル 4 とそのシミュレーション結果をそれぞれ図 9，図 10 に示す．

＜シミュレーションの前提＞

図 9 は，セキュリティレベルが各々High／Middle／Low（表 1）である 3 つの DNS サーバからの名前解決応答（DNS リプライ）パケットが NNI・CR・UNI 経由でユーザに UDP で転送されるモデルである．NNI と CR の間，CR と UNI の間の利用可能帯域はともに 5Mb/s である．通常，この DNS リプライパケットのトラヒックは比較的小さい．ここでは High と Middle の DNS サーバからのトラヒックとしてともに平均 1Mb/s を見込む．また，Low の DNS サーバとしては，いわゆるオープンサーバと呼ばれ，管理が十分行き届いておらずセキュリティ攻撃に利用されやすいものを想定する．いま， DNS リダイレクトと呼ばれる攻撃[17]が発生し，Low の DNS サーバから大量の不正 DNS リプライパケットが 10Mb/s で NNI に流入しユーザ側に向けて発信されるものとする．一般に ISP や NGN 事業者はこのような異常トラヒックに対する検出閾値を予め設定し，その閾値を超える

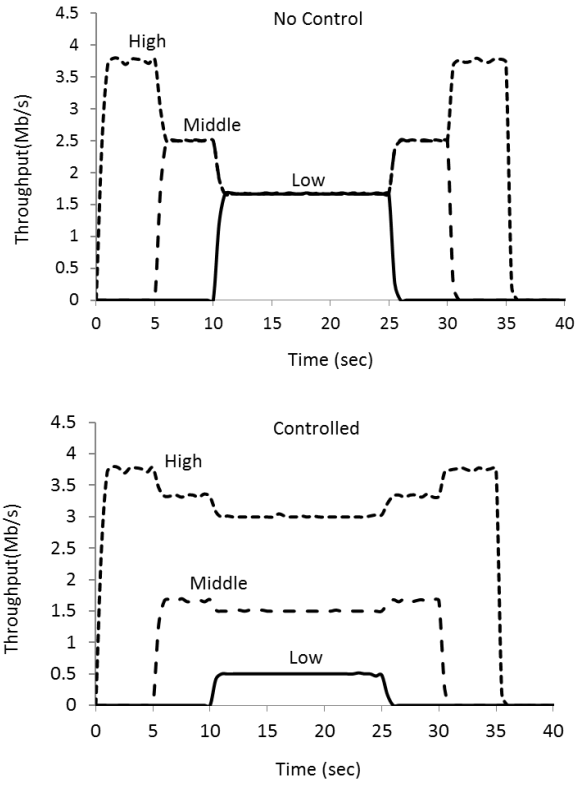

図 8 モデル 3 のシミュレーション結果

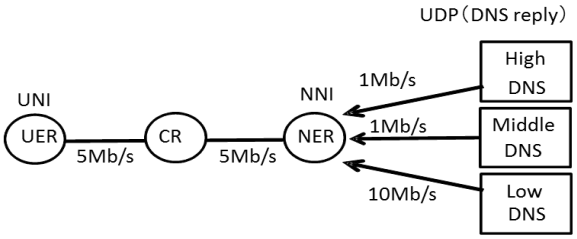

図 9　モデル 4

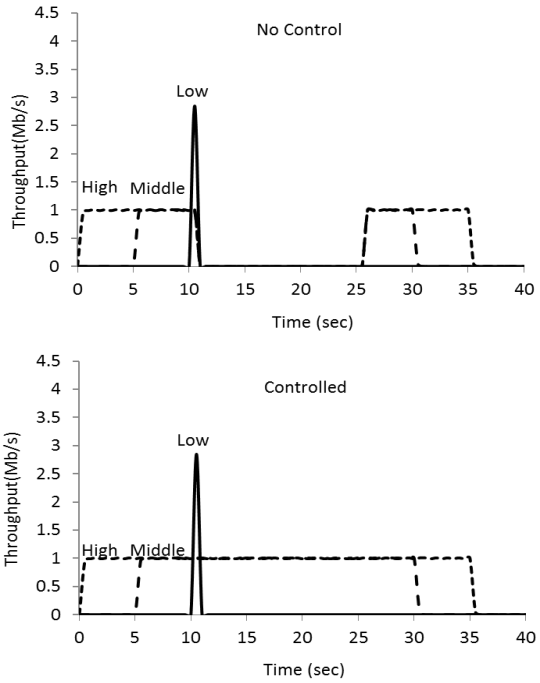

図 10 モデル 4 のシミュレーション結果

UDP トラヒックが発生した場合，それぞれが管理する公衆ネットワークの入り口において（図９では NNI の NER において）ファイアウォールを用いて該当する種類のパケットを廃棄する．

＜シミュレーション結果＞

図 10 の上の図は，本提案を適用しない場合のシミュレーション結果（UNI の UER における通信速度特性）である．UNI における異常トラヒック検出閾値は 4Mb/s に設定している．すなわち，NNI 側からユーザ側の方向で UNI を通過する UDP パケット（ここでは DNS リプライパケット）が 4Mb/s を超えると，どのような DNS サーバから発せられたものか区別する手段を持たないため，すべての DNS リプライパケットを廃棄する．セキュリティレベル High／Middle／Low の DNS サーバの通信時間はそれぞれ 0 秒～35 秒，5 秒～30 秒，10 秒～25 秒である．時刻 10 秒において，DNS リダイレクト攻撃用のパケットが発生すると，UDP パケット（DNS リプライパケット）が上記閾値を超えるので，25 秒までの間，正常／異常を問わず全ての DNS リプライパケットがユーザに転送されないことがわかる．この図では，セキュリティレベルが High もしくは Middle であり，攻撃に加担していない正常な DNS サーバからのパケットも廃棄されるという不都合が生じることが確認できる．

図 10 の下の図は，本提案を適用した場合のシミュレーション結果である．ここでは，Low の DNS サーバからのトラヒックに対してのみ異常トラヒック検出閾値を設け 2Mb/s に設定している．図 10 の上の図と同様に，セキュリティレベル High／Middle／Low の DNS サーバの通信時間はそれぞれ 0 秒～35 秒，5 秒～30 秒，10 秒～25 秒である．時刻 10 秒において，DNS リダイレクト攻撃用のパケットが発生し，上記閾値を超えると，NNI の NER では Low の DNS サーバからのリプライパケットのみ廃棄する．このため，セキュリティレベルが High もしくは Middle で正常な DNS リプライパケットは廃棄されず，DNS リダイレクト攻撃中であってもユーザに転送されることがわかる．このように，本提案のように予めサーバのセキュリティレベルに応じてトラヒックを差別化しておくことにより，異常トラヒックに対する対策が，従来に比べて適切に実施できることがわかる．

6 考察

ここでは，最初に，私的セキュリティポリシーによるトラヒック制御，および，公的セキュリティポリシーによるトラヒック制御，の適用効果について考察する．次に，両案の影響と課題を，情報システムの構成および機能，制御トラヒック，適否の判断，適用した場合の運用のポイント，法制度，の各視点から考察する．

6.1 本提案の適用効果

6.1.1 私的セキュリティポリシーによるトラヒック制御

本提案は，従来，ユーザ側に設定しているファイアウォール機能の一部をアクセスネットワークで実現する．ファイアウォール機能を加入アクセスネットワーク側に移行することでユーザのセキュリティ管理上の負担が軽減される．また，エンドポイントではなく，トラヒック的に上流の位置で異常トラヒックを遮断することで，アクセスネットワークの帯域が確保できる．さらに，前章のシミュレーションでも示したように，本提案を適用したユーザのみならず，アクセスネットワークを共同利用しており，本提案を適用していない他ユーザの利用帯域も確保できるという効果もある．

6.1.2 公的セキュリティポリシーによるトラヒック制御

本提案により，脆弱性検査結果に応じてトラヒックが差別化されることから，ユーザのセキュリティ対策意識が向上し，社会全体のセキュリティの向上につながる．さらに，前章のシミュレーションでも示したように，現状のセキュリティ攻撃は，脆弱性のあるユーザの情報システムを介して実施されることから，異常なトラヒックによる攻撃が発生した場合でも，正常なトラヒックを損ねることなく，同攻撃を緩和できるという効果が見込まれる．

なお，一般に，セキュリティの総合的指標としてセキュリティリスクが使用される．このセキュリティリスクは脅威の発生確率と脅威が具現化

された場合の影響度の積で与えられる．私的セキュリティポリシー，公的セキュリティポリシーはいずれの運用も発生確率を低減することが可能である．従って，コンピュータウィルスや迷惑メールといった脅威の影響度が一定であるならば，不正あるいは異常トラヒックが少なくなった分だけリスクも小さくなることになる．本文の例でいえば，UDP フラッドのトラヒックが低減された分だけ私的セキュリティポリシーを設定したユーザのリスクを，また，セキュリティレベルの高いトラヒックが増えた分だけ公的セキュリティポリシーを設定した公衆ネットワークのリスクをそれぞれ軽減することになる．

6.2 本提案の影響と課題

6.2.1 私的セキュリティポリシーによるトラヒック制御

(1) 情報システムの構成および機能

本提案を実現するためには，単にファイアウォール機能をネットワーク側に移行するという構成上の変化だけでなく，私的セキュリティポリシーをユーザからネットワーク側に，さらに，関連するネットワーク装置間で（本文の例では UNI と NNI の間で）制御情報を伝える機能が新たに必要になる．この機能は，提案を適用するユーザ毎に必要に提供することになるので，ネットワーク側設備の拡張性（スケーラビリティ）の確保が課題となる．

(2) 制御トラヒック

私的セキュリティポリシーおよび制御情報を転送するための制御トラヒックが新たに必要になる．しかし，このトラヒックの発生頻度は比較的小さく，私的セキュリティポリシーの変更や関連するセキュリティ攻撃が頻発しない限り，特に大きな問題とはならないであろう．

(3)適否の判断

本提案は一種のネットワークサービスとして有償で提供されることが考えられる．そのため，通信事業者は同サービスの市場性に応じて提供の可否を判断することになろう．また，ユーザは通信事業者が提供するサービスメニューと価格とから加入するかどうか判断することになろう．

(4) 適用した場合の運用のポイント

本提案を具現化する場合，ユーザが要望する，あるいは，通信事業者が提供できる，ファイアウォール機能について，相互に理解し，祖語のないよう調整する必要がある．実際にセキュリティ攻撃を受けた場合，ファイアウォールの動作記録を詳細に分析し，所定のファイアウォール機能が実現できているか検証することも必要になる．

(5) 法制度

本提案はユーザと通信事業者間の個別の契約によって提供されると考えられるため，提供内容に法制度が関与することはないと考えられる．ただし，通信事業者が適正に契約を履行しているかどうかがユーザに見えにくいため，通信事業者が事業実績を適切に情報公開するように監督官庁が行政指導することが考えられる．

6.2.2 公的セキュリティポリシーによるトラヒック制御

(1) 情報システムの構成および機能

本提案を実現するには，ユーザ毎に脆弱性検査を実施してセキュリティレベル評価結果をデータベースに記録する機能，さらに，同セキュリティレベル評価データを基にパケットを優先制御（トラヒック制御）するための QoS 機能を，新たにアクセスネットワークに追加することが必要になる．私的セキュリティポリシーと異なり，公的セキュリティポリシーは社会的コンセンサスを得たうえで実施されるため，ユーザ個々に動的に設定する必要はないが，代わりに，加入ユーザ数に見合った実現リソース，特にセキュリティレベル評価データの保存に関わるリソースを確保することが求められる．

(2) 制御トラヒック

脆弱性検査を実施するためのトラヒックが新たに生じる．脆弱性検査の周期として，週や月といった単位とすることが考えらえる．脆弱性検査に関わるトラヒックは，OS やアプリケーションの更新，ウィルス対策ソフトのパッチのダウンロード，といった現状の制御トラヒックと同程度以下と考えられるため大きな問題とならないであろう．

(3)適否の判断

最初に，本提案が社会的コンセンサスを得られるかどうかが課題となる．本提案の効果の恩恵を

受けるのはウィルス対策ソフトなどのセキュリティ対策を充分にとっているユーザであり，適用に賛同することが想定されるが，そうでないユーザは，利用帯域が低減されるので，適用に反対するであろう．このため，セキュリティ向上のメリットを全ユーザが納得して受容するかが社会的コンセンサス形成上の大きな課題となる．

次に，本提案のコストの多くは脆弱性検査に関わるもので，本提案の適否は脆弱性検査に要するコストの大小によっても判断されることが考えられる．脆弱性検査の費用に関する統計的データは見受けられないが，Web サイトでの公表例として，各種アプリケーションを搭載したサーバの侵入試験を実施した場合 150 万円／台，同サーバ以外のホスト端末のセキュリティホール検出試験は 8 万円／端末，という数値があった．これまでの脆弱性検査は，主に企業ユーザを対象にしたものであるため，対象を一般ユーザに拡大して定期的に実施する場合は割引き可能であると推定される．ちなみに，一般ユーザを対象としたウィルススキャンサービスはクラウドを利用したもので，年間 1 万円程度で提供されており，この程度までに費用を抑えることが望まれる．本提案の実施費用を通信料金に転嫁させたとしても，現状のユーザが支払っている通信料，および得られるセキュリティ上の効果からみて，適切な費用であればユーザは受け入れるであろう．

(4) 適用した場合の運用のポイント

ユーザの利用環境によっては，ユーザの情報システムの稼働を中止して脆弱性検査を実施しなければならない場合がある．この場合，ユーザのネットワーク利用の利便性が現状より低下するのは避けられない．このため，脆弱性検査の実施日時および実施内容，ユーザの利用環境への外部からのアクセス条件，などをユーザと通信事業者が合意したうえで実施する必要がある．また，脆弱性検査結果が外部に漏えいすると逆に標的になりやすいため，関連データの十分な機密保持が求められる．

(5) 法制度

本提案を適用するためには，「通信の自由」や「通信の公平性」の見直しが必要である．これらは電気通信事業の黎明期から制度化されてきたものであり，原則として遵守すべきであるが，インターネットのように高度な公衆ネットワークが普及している今日，さらに「通信の安全」の制度化についても議論することが求められる．

7 まとめ

本文では TCP/IP をベースにした，インターネットのような公衆ネットワークに，私的あるいは公的なセキュリティポリシーを導入しトラヒック制御することを提案した．具体的には，インターネットへのアクセスネットワークである NGN を対象に，UNI および NNI に私的セキュリティポリシーを反映し，外部からの不正トラヒックを遮断することを提案した．また，SNI を介してユーザのインターネット利用環境に関する脆弱性検査をおこない，公的なセキュリティポリシーを用いて，セキュリティレベルの高いユーザのトラヒックを優先転送することを提案した．さらに，計算機シミュレーションにより提案の有効性を確認した．今後は前章で示したような課題について検討し，本提案の実用化を目指す．

なお，本文では，トラヒック制御機能を備える NGN に提案内容を適用して検討した．今後，OpenFlow[18]などトラヒックをソフトウエアで制御する SDN（Software Defined Network/Networking）[18]が一般化すれば インターネットにおいても提案と同様なトラヒック制御を具現化できると期待される．

参考文献

[1] ISO/IEC 27001, “Information security management. Specification with guidance for use,” 2005-10

[2] 日本情報処理推進協会（JIPDEC），“情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要，”2007 年 11 月

[3] 警視庁情報通信局情報技術解析課，“情報技術解析平成 24 年報，”2013 年 8 月

[4] 日本インターネットサービスプロバイダ協会（JAIPA），“「帯域制御の運用基準に関するガイドライン」の改定について，”2010 年 8 月

[5] Eric Y. Chen，柏大，冨士仁，米澤明憲，“Moving Firewall における DDoS 攻撃対策システムの評価,”電子情報通信学会情報ネットワークシステム研究会， 信学技報 NS2002-121，pp.73-78，2002 年 9 月

[6] A. Garga, and A.L. N. Reddy, ” Mitigation of DoS attacks through QoS regulation,” IEEE Microprocessors and Microsystems 2004, Vol.28, Issue 10, pp.521–530, 2004-12

[7] 井上友二，“そこが知りたい最新技術 NGN 入門，” インプレス R&D，2007 年 2 月

[8] 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，" 電子情報通信学会 2009 年暗号と情報セキュリティシンポジウム，2E3-3，2009 年 1 月

[9] Y.Okada, N.Nishikawa, and N.Sato, ”DoS attack countermeasures in NGN using private security policy,” IEEE APSITT2010, A-1-2, 2010-6

[10] 古川泰弘，吉成大知，“ペネトレーションテスト入門ー情報システムセキュリティの実践的監査手法 ，”ソフトバンククリエイティブ，2006 年 12 月

[11] 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，” 電子情報通信学会情報セキュリティ研究会，信学技報 ISEC2008-103，pp. 15-22，2009 年 3 月

[12] Mitre, “Common Vulnerabilities and Exposures,” http://cve.mitre.org/, 2013 年 12 月現在

[13] 情報処理推進機構 IPA，“共通脆弱性評価システム CVSS 概説，” http://www.ipa.go.jp/security/vuln/CVSS.html，2013 年 12 月現在

[14] IETF, “RFC2475 An Architecture for Differentiated Services,” 1998-12

[15] 銭飛，“NS2 によるネットワークシミュレーション，”4 章，森北出版，2006 年 11 月

[16] 戸田巌，“詳解ネットワーク QoS 技術，” 第 3 部，オーム社，2001 年 5 月

[17] DNS のセキュリティ情報 http://technet.microsoft.com/ja-jp/library/cc755131.asp, 2013 年 12 月現在

[18] G.Parulkar, J.Reijendam and J.LiHle, “OpenFlow/SDN:A New Approach to Networking, ” http://cenic2012.cenic.org/program/slides/CenicOpenFlow-3-9-12-submit.pdf, 2013 年 12 月現在