博　士　論　文

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

Yasuyoshi　Okada

岡田康義

情報セキュリティ大学院大学

情報セキュリティ研究科

情報セキュリティ専攻

２０１４年３月

目次

第 1 章　緒論

1.1　研究の背景

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，安心や安全への対策も基本的に端末（ユーザ）側へ依存しているのが実情である．インターネットを含めた情報通信ネットワーク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ことはいうまでもない．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できる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，この発想はネットワークには利用制限を持たせないといったことと同じであり，悪意をもった者にとっても好都合な環境となっている．事実，サイバー犯罪は毎年増加の一途をたどっており，その手口も巧妙かつ高度なものへと変化してきているため，従来のようにユーザ側だけの対処で解決するのは限界となっている．

さらに代表的なソーシャル・ネットワーキング・サービス（Social Networking Service，以下 SNS と略す）の主目的は，人と人とのコミュニケーションにある．友人・知人間のコミュニケーションを促進する手段や場，あるいは趣味や嗜好，居住地域，出身校，「友人の友人」といった，自身と直接関係のない他人との繋がりを通じて新たな人間関係を構築する場を提供しているが，なりすまし等の犯罪も起きている．知り合い関係だけに特化してソーシャルシステムを形成しているだけにダメージが大きく，SNS に関してもなんらかのセキュリティ対策が求められている．

1.2　研究の位置づけと目的

1.2.1　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．

さらに，SNS ではなりすましの犯罪やウィルス感染等の問題も起きている．知り合い関係だけに特化してソーシャルシステムを形成しているだけにダメージが大きく，SNS に関してなんらかのセキュリティ対策が求められている．

1.2.2　セキュリティポリシーおよび SNS に関する社会制度の課題

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[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．

さらに，SNS については，マルウェア（不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称）感染や詐欺行為のプラットフォームとしての利用されたり，なりすまし犯罪の場ともなっていることから，NPO 日本ネットワークセキュリティ協会はガイドライン「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」[4]を示しているが十分に効果的な対策にはなっていないように見受けられる．

1.2.3　研究の目的

1.2.1 と 1.2.2 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流入することを防止し，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．

さらに，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．

1.3　研究の概要

本研究では，インターネットのような情報通信ネットワークや SNS へも一定のセキュリティ機能を持たせ，ユーザ側のセキュリティ機能と協調した上で，安心して利用することができる安全なネットワーク環境の構築を実現するために，以下の点を検討し，考察を行う．

第 2 章，第 3 章では，技術的な観点から検討を行い，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[5]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．一般に，ネットワークがブロードバンド（電気信号や光信号などの周波数帯域幅が広いこと．また，それを利用した高速・大容量な通信回線や通信環境）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ネットワークを流れるトラヒックを監視・管理する十分な機能がネットワーク側に備わっていないためである．

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 パケットのトラヒックを制御することを提案する．具体的には，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．

インターネットへのアクセスネットワークである NGN（Next Generation Network）[6]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 2 章と第 3 章におけるセキュリティに関する検討は，基本的に工学的視点に立って行っている．ここで，パケットフィルタリングは，ルータやファイアウォールが持っている機能の一つで，送られてきたパケットを検査して通過させるかどうか判断する．パケットのヘッダにはプロトコル種別や送信元アドレス，あて先アドレスやポート番号などの情報が含まれており，これを参照して通過するかどうかが決定される．通過できなかったパケットは送信元に通知されたり，破棄されたりする．どのような方針に基づいて通過／非通過を判断するかは，そのネットワークの管理者が任意に設定することができる．

第 4 章では，第 2 章と第 3 章とは独立な章として，情報セキュリティデータベース（以下 DB と示す）を用いた SNS 会員資格制度提言[7]を行う．将来 SNS での情報セキュリティを維持するために必要と考えられる SNS 会員資格について，社会制度の提言を行っている．本章では，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ている．

第 5 章では，第 2 章の私的セキュリティポリシーを用いたトラヒック制御法，第 3 章の公的セキュリティポリシーを用いたトラヒック制御法，第 4 章の情報セキュリティ DB を用いた SNS 会員資格制度提言についてフィージビリティ（実現性）を検討する．

1.4　既存検討と本研究における検討指針

1.4.1　第 2 章と第 3 章の検討指針

インターネットでは，P2P ヘ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の低下を招いている．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[8]．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る．例えば，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）ネットワークのユーザ全体のコンセンサスを得た公的な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；Quality of Service）を用いて，パケット転送を差別化することとする．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．

ここで，アクセスネットワークとは，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直接的に接続する（アクセスする）ネットワークである．具体的に，インターネットの場合は，ユーザ宅からインターネット・サービス・プロバイダ（ISP）までの間のネットワークのことを指す．このアクセスネットワークとして，以前は公衆電話網や ISDN（Integrated Services Digital Network）網などが利用されていたが，最近では，より高速化したブロードバンド・ネットワーク（アクセスネットワーク）として CATV や ADSL，FTTH など有線系のネットワークが広く普及している．また，最近ではワイヤレス・ブロードバンド（無線アクセスネットワーク）として無線 LAN あるいはモバイル（3G/3.5G）が普及しており，さらに WiMAX などもアクセスネットワークとして利用されている．

［本提案の検討の範囲と既存研究の検討状況］

私的セキュリティポリシーに関する指針 1 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して検討する．

公的セキュリティポリシーに関する指針 2 の実施について，インターネットのような複数 ISP にまたがった場合においても全ての ISP が同じ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のみで実施することとして検討する．

次に，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や QoS の適用を検討する．パケットフィルタリングによりトラヒック制御する既存技術として Moving FireWall 技術[9]がある．同技術は分散サービス不能攻撃 DDoS（Distributed DoS）を対象にしたもので，被攻撃側で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．しかし，インターネットのような公衆ネットワーク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，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 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[10]が，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．

1.4.2　第 4 章の研究に関する検討指針

第 4 章の研究に関する検討指針として指針 4 を設ける．

指針 4）将来，セキュリティデータベース(以下セキュリティ DB と記す)を用いた SNS 会員資格制度の創設が必要となるという仮設を立てる．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，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可能にする．

第 2 章　私的セキュリティポリシーを用いたトラヒック制御

2.1　まえがき

第 2 章では，インターネットでの私的セキュリティポリシーを用いたトラヒック制御法について述べる．近年，インターネットは，高度情報化社会の根幹を支えるインフラとして普及・発達し，国民生活における利便性の向上へ貢献し，一般生活に深く浸透してきた．一方で，悪意を持った利用者による不正アクセスの脅威は数的には年々減少しているが，依然として高い水準で推移している．本文で対象とする NGN を介してインターネット接続サービスを利用する場合においても，インターネットからの不正アクセスの脅威は変わることがないと考えられる．

本文では，不正アクセスにおける脅威を軽減し，安心，安全，快適に NGN を利用できる環境の提供を目指すため,私的セキュリティポリシーを利用し,NGN に流入する IP(Internet Protocol）パケットにマーキングを行い IP パケットの差別化を図る．さらに経路制御する際，NGN に流れる IP パケットにマーキングを施し，通信経路の差別化を図る．本差別化を利用し不正アクセスの 1 つである DoS 攻撃の抑制手法について提案を行う．

2.2　研究の位置づけと目的

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負担を軽減するとともに，悪意のある IP パケット（以下単にパケットと呼ぶ）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ことを目的に，パケット発信元のセキュリティレベルに応じてトラヒックを制御する技術の確立を目指す．

2.3　私的セキュリティポリシーを用いたトラヒック制御の提案

前節までの議論を踏まえて，私的セキュリティポリシーを用いたトラヒック制御を提案する[11][12]．以降，本提案を実施するユーザはアクセスネットワークとして次世代ネットワーク NGN（Next Generation Network）を利用してインターネットと接続しているもの

とする．議論の前にNGN周辺の用語を定義する．

＜NGNの基本的な定義＞

ITU-Tの勧告（TTC標準JY－Y2001v1）によれば，NGNは次のように定義されている．

(1)電気通信サービスの提供が可能であること．

(2)広帯域（ブロードバンド）でなおかつQoS制御が可能であり，さまざまなトランスポート（転送）技術を活用することが可能なパケット・ベースのネットワークであること．

ここでQoSとは，ネットワーク上で提供する機能を安定的に稼働させるために行うサービス品質管理技術である．ネットワークにはさまざまなデータが流れ，時には多くのデータが集中的に流れて滞留が起こり，ネットワークを使って動作している機能に支障をきたすことがあるので，個々の機能の特性が損なわれないように，QoSによりネットワークの設定を調整を行う．

(3)サービス関連機能がトランスポート関連技術と独立していること．

(4)利用者は，ネットワークに自由に接続でき，さらに競合するサービス・プロバイダーやサービスを自由に選択できること．

(5)普遍的モビリティをサービスして，利用者に対して一貫したかつユビキタスなサービスの提供を可能とすること．

ここで普遍的モビリティとは，ユーザや他のモバイル・エンティティ（携帯端末や通信機能をもつ車両等）が，場所や技術環境の変化に関係なく通信でき，サービスを利用できる能力のことである．

図2.1を用いてNGNのインタフェースを説明する．NGNの具体的な物理的なインタフェースとして，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）と呼ばれるインタフェースを有する．さらに，NGNから直接，ユーザにアプリケーションを提供するサーバのインタフェースSNI(application

Server-Network Interface)を有する.

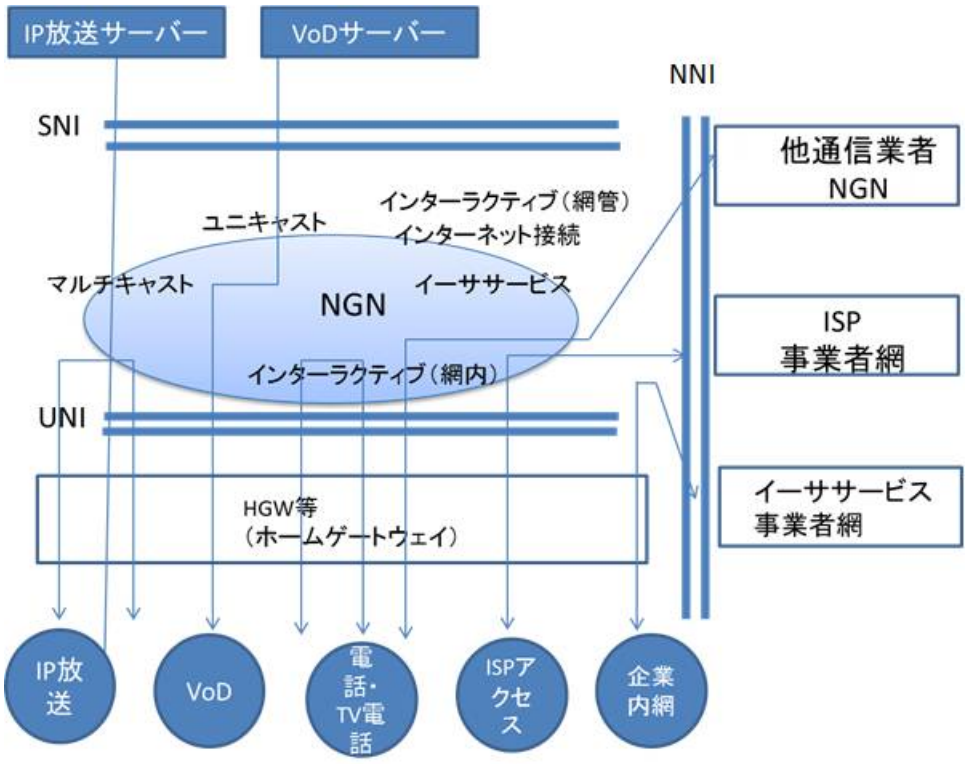


図 2.1　NGN の UNI, NNI, SNI

［NGN の周辺の用語詳細］

(1) UNI (User-Network Interface)

公衆通信ネットワークで，通信事業者の設備と加入者の設備を接続するインターフェース(接続点，責任分界点)である．具体的な仕様は通信技術やサービスによって異なり，それぞれ標準規格が定められる．例えば，ISDN の場合について述べる．ISDN は交換機・中継回線・加入者線まで全てデジタル化された，パケット通信・回線交換データ通信にも利用できる公衆デジタル回線ネットワークである.ISDN はモデムで接続する既存のアナログ交換電話網（PSTN；Public Switched Telephone Networks ）をデジタル化することで，高速で高品質な回線サービスを提供する．この ISDN の場合，ITU-T（国際電気通信連合の部門の一つで，通信分野の標準策定を担当する電気通信標準化部門）によって世界共通の I シリーズ規格として定められている．この ISDN では，ターミナルアダプタ（TA）が備え

るT点がUNIとなっている．FTTHでは，光回線終端装置（ONU；Optical Network Unit）がUNIとなっている．ここで，ONUは光通信ネットワークを終端するために設置され，光信号・電気信号間の変換と光信号の多重・分離をおこなう．ONUのUNIランプが消灯していると，電気通信事業者とONUが接続されていないことを表す．正しく接続してもUNIランプが消灯している場合は電気通信事業者に連絡し，回線の修理やONUを交換する必要がある．なお，電気事業者側では回線を終端するため，ISDNの場合はSLT（Subscriber Line Terminal）を，FTTHではOLT（Optical Line Terminal）をそれぞれ設置する．

（2）NNI（Network-Network Interface）

ネットワーク間インタフェースであり，ネットワーク（NGN）と他のネットワーク（例：ISPが運営するネットワーク）の接続点である．また，NNIはネットワーク同士を接続するためのインターフェース仕様（規定）でもあり，ネットワークの接続点となるスイッチ同士を接続するために適用される．

（3）SNI（application Server-Network Interface）

アプリケーションサーバ・ネットワークインタフェースはアプリケーションサーバとネットワーク（NGN）の接続点である．例えば，インタラクティブな通信アプリケーションである，IPTV電話，電話会議，映像配信VoD（ビデオオンデマンド．視聴者が観たい時に様々な映像コンテンツを視聴する事が出来るサービス）を提供する場合のインタフェースとなる．インタラクティブな通信アプリケーションの通信形態は種々提供されている．例えば，映像配信の場合，ユニキャスト通信やマルチキャスト通信など，複数の通信形態があるが，SNIが規定する通信形態に合致する必要がある．なお，ユニキャスト通信は1対1の通信形態である．マルチキャスト通信とは，コンピュータネットワークにおいて，決められた複数のネットワーク端末（ノード）に対して，同時にパケット（データ）を送信する1対多の通信形態である．

インタラクティブな通信アプリケーションを提供する場合，NGNのセッション制御機能IMS（IP Multimedia Subsystem）が利用される．IMSは通信の開始や切断を行うセッション制御機能を有する．このセキュリティ制御に，IETFによって標準化された，SIP（Session Initiation Protocol）といわれるプロトコルを利用することで，パケットを「最優先クラス」，「優先クラス」といった複数の品質クラスに分類し，転送を差別化することもできる．

＜ルータの定義＞

ルータ（Router）は，コンピュータネットワークにおいて，データを 2 つ以上の異なるネットワーク間で中継する通信機器である．通信プロトコルに TCP/IP が使われるようになってから普及した．データをネットワーク層で，どのルートを通して転送すべきかを判断するルート選択機能を持つ（図 2.2)．

＜エッジルータの定義＞

エッジルータ(er)は UNI と NNI に設置され，サービス受付制御，セキュリティポリシー設定，あるいはトラヒック制御の実施主体となる．主に通信事業者や大企業のネットワークの端に設置され，ネットワーク末端で外部のネットワークやホストとの接続に用いられるルータである．

＜コアルータの定義＞

ココアルータ(CR)は,ER と ER の中間に位置しトラヒックを中継するために設置される．コアルータはエッジルータと連携して，トラヒック制御に関わる．

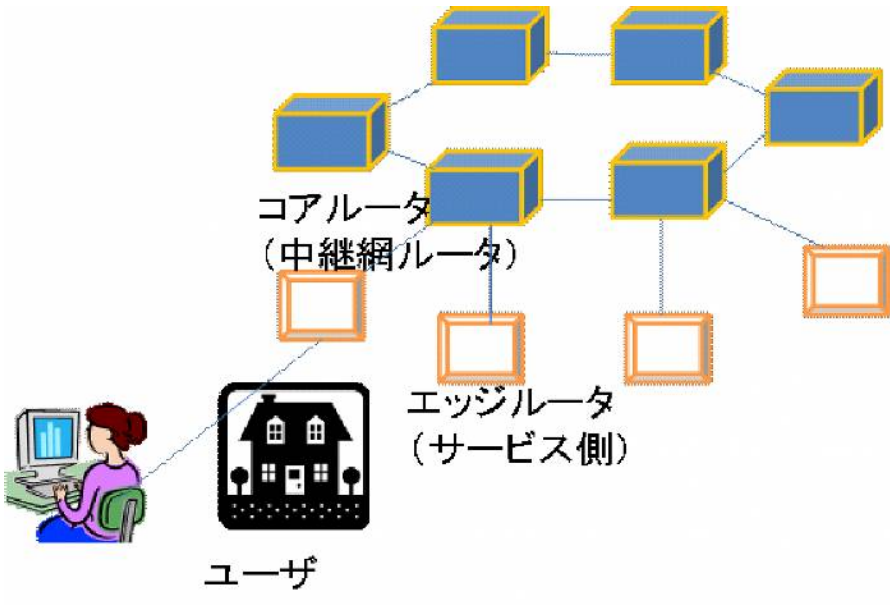


図 2.2　エッジルータとコアルータ

＜SIP の定義＞

SIP は，「Session Initiation Protocol」の略で，IP ネットワーク上でさまざまな音声，データ，画像などのマルチメディア通信を行うためにアプリケーション間の関連付けを実行したり，アプリケーションを終了したりするために利用するのに欠かせない通信手順である．Session（セッション）とは，アプリケーションの関連付けのことで，Initiation（イニシエーション）は，セッションを開始することを指す．これらを行うための手順（プロトコル）が，セッション･イニシエーション･プロトコル，すなわち SIP である．

＜SIP の特徴＞

SIP は，「セッションの開始，終了」などの基本的な機能しか提供せず，SIP を利用する際には下記のプロトコルなどと併せて使用することが前提である．

・RTP （Real-time Transport Protocol）：メディアの送受信，QoS 制御
・RTSP （Real-Time Streaming Protocol）：ストリーミングメディアの制御
・SDP （Session Description Protocol）：マルチメディア・セッションの制御
・MEGACO （Media Gateway Control）：PSTN ネットワークへのゲートウェイの制御

SIP は，基本的なセッション制御のみを行い，他プロトコルでその機能を補う形態を取る．このようなプロトコル形態を取っているため，SIP が単純かつ拡張性が高い理由でもあり，また特徴である．ここで，SIP で言うセッションとは，アプリケーション間の関連付けである．IP 電話の例で説明すると，電話は発信者と着信者の電話が接続されることによって通話ができるようになる．つまり，発信者の電話アプリケーションと着信者の電話アプリケーションが関連付けされることで通話が成立する．この関連付け（接続）のことを「セッション」と呼ぶ．

＜SIP サーバの定義＞

SIP サーバとは，SIP と呼ばれるプロトコルを利用して，電話番号を IP アドレスと対応付けたり，相手を呼び出してつなぐといった呼制御を行うサーバのことである．SIP サーバの基本機能はプロキシ・サーバ（企業などの内部ネットワークとインターネットの境にあって，直接インターネットに接続できない内部ネットワークのコンピュータに代わっ

て，代理としてインターネットとの接続を行うサーバ，およびそのための機能を実現するソフトウェアを指す）である．SIP サーバはユーザのドメインごとに配置され，ネットワークにおける案内人，いわゆる DNS（Domain Name System）サーバのような役割をする．従来の IP 電話サービスや NGN で利用される．ここで，ドメインに関して，ドメイン名（Domain Name）は，IP ネットワークにおいて個々のコンピュータを識別する名称の一部である．インターネット上においては ICANN（The Internet Corporation for Assigned Names and Numbers）という組織が一元管理しており，世界中で重複しないようになっている．通常，IP アドレスとセットでコンピュータネットワーク上に登録される．多くの場合，ドメイン名はその下位に 1 つまたは複数のホスト名を連ねる．またドメイン名自身もホスト名として機能する．

＜NGN における SIP サーバの特徴＞

NGN においては，その最大の特徴である帯域制御を指示したり，課金・認証情報を外部サーバに提供するといった機能を備えており，NGN のサーバ群の中でも中心的な役割を担っている．SIP サーバには，汎用サーバに実装するソフトウェアタイプと，SIP サーバソフトを搭載したハードウェアごと提供すルータイプがある．NGN は後者のタイプを適用しており，高信頼性と高速処理能力を備える．

＜SIP サーバの呼制御機能＞

SIP サーバは呼制御サーバとして次の 3 つの機能を有する．

・レジストラ機能（Registrar）

IP 電話機の電話番号，SIP アドレス，IP アドレスの管理機能．なお，SIP アドレスは，一般的にユーザ名とドメイン名で構成される．

・プロキシ・サーバ機能（Proxy Server）

接続要求を他の呼制御サーバに転送する機能．ユーザ認証，アクセス許可，アクセス制御なども行う．

・リダイレクト・サーバ機能（Redirect Server）

接続要求内容が変更されていた場合，発信者側呼制御サーバ（プロキシ・サーバ）へ正しい内容を返送し再アクセスを促す機能．

図 2.3 は SIP を使用した場合の通話開始前から終了までのイメージ図である．まず，IP 電話機の受話器をあげるとダイヤルトーン（ツーという音）が聞こえる．この時点で SIP での呼制御が始まっている．相手の番号を入力すると，SIP サーバ群の中で番号照会が行われ，対応する IP アドレスを取得し，その IP アドレスが割り当てらている IP 電話機に呼び出し音を鳴らす（①）．そして，相手側が IP 電話機の受話器もあげると，セッションが確立し通話が開始される（②）．通話は IP 電話同士で P2P で通信することになる．なお，SIP サーバの設定によっては SIP サーバが通話を中継することもある．最後に受話器をおろすと，セッションが終了され，一連の電話プロセスが終わる（③）

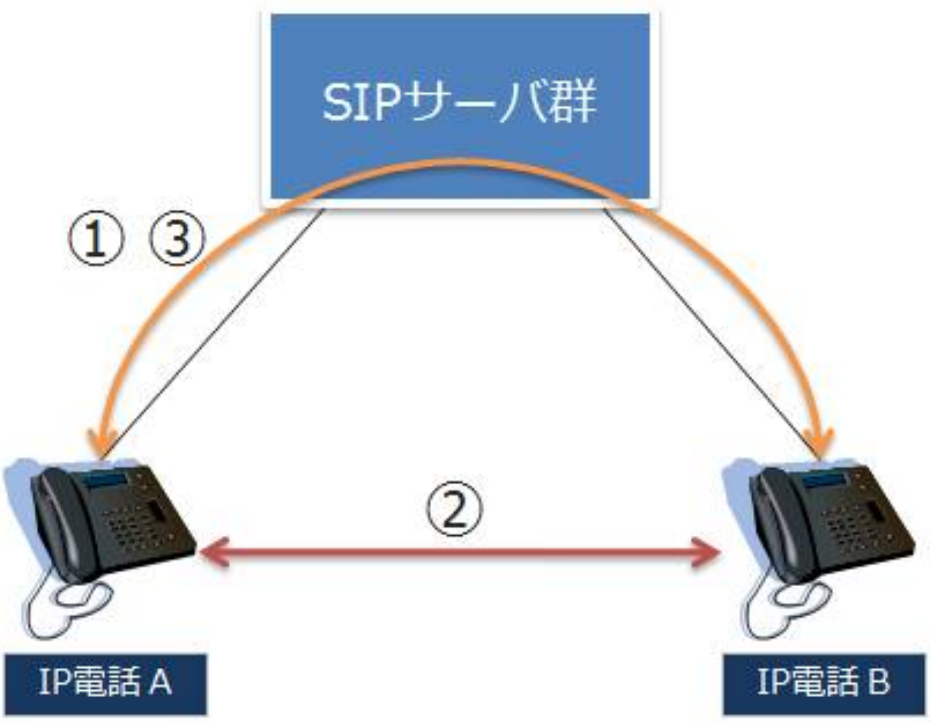


図 2.3　SIP サーバのイメージ図

［NGN とインターネットの SIP サーバの違い］

インターネットと異なり，NGN のおける SIP はルーティング・エンジンとしての役割だけでなく，セッション情報に応じて，QoS による帯域制制御，ファイアウオール等による

セキュリティ制御機能を担う．NGN における SIP サーバの制御イメージを図 2.4 に示す．

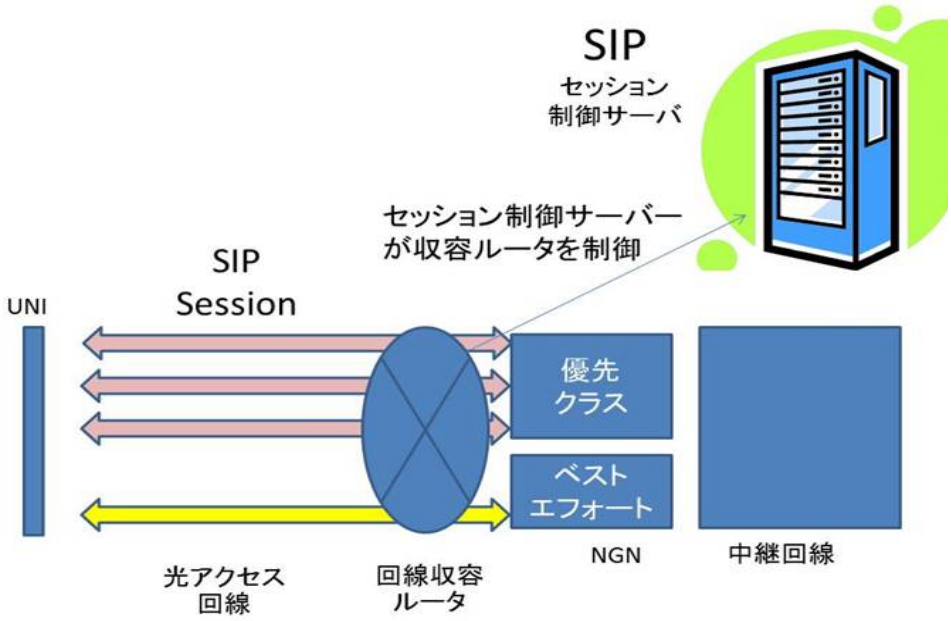


図 2.4　SIP サーバによる QoS 制御のイメージ

［NGN を利用する目的］

本文で NGN を利用する理由の一つは，ネットワークにおける QoS 制御が通常のインターネットに比較して容易に行えるためである．ネットワークにはさまざまなデータが流れるが，データトラヒックが集中的に発生してパケットの滞留が起こり，ネットワーク上で動作している機能に支障をきたすことがある．そこで個々の機能の特性が損なわれないようにトラヒック調整するのが QoS 制御である．

＜本研究の基本的なアイデア＞

NGN の広帯域（ブロードバンド）通信環境において，SIP サーバの呼制御と QoS 制御とを組み合わせて，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負担を軽減する手法を提案し，その有効性を明らかにする．

提案手法では，具体的に，悪意のあるパケットが標的とするユーザに到達する可能性を，NNI で制御して，当該ユーザのみならず，その他のユーザへの影響も低減する．さら

に，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．これら 2 つのアイデアを実現するため，ネットワークにおけるトラヒックを制御する技術を確立する．

＜従来の研究＞

従来の研究としては，第 1 章で述べたように，パケットフィルタリング（ルータやファイアウォール組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム）によりトラヒック制御する既存技術として Moving FireWall 技術[6]がある．同技術は分散サービス不能攻撃 DDoS（Distributed DoS）を対象にしたものである（ここで，DDoS 攻撃とは，踏み台と呼ばれる多数のコンピュータが，標的のサーバなどに対して攻撃を行うことである．別名として，協調分散型 DoS 攻撃，分散型サービス拒否攻撃などがある．単一のホスト(通信相手)からの攻撃ならばそのホストとの通信を拒否すればよいが，数千・数万のホストから攻撃を受ける場合は個々に対応することが難しい．したがって，通常の DoS 攻撃よりも防御が困難であり，攻撃による被害は単なる DoS 攻撃よりも大きくなると考えられる．攻撃を受けたサーバには踏み台となったコンピュータが攻撃元として誤認識されることもある．Moving FireWall 技術では，DDoS による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多くの場所に設定する必要があり，本提案と比較して拡張性の面で難点がある．

2.3.1　私的セキュリティポリシーを用いたトラヒック制御

＜セキュリティポリシーの定義＞

セキュリティポリシーとは,組織内のセキュリティに関する基本的な方針や行動指針のことである．何をどのような手段で守るべきか，それにどの程度のコスト（人的な要素も含む）を投じるべきかは組織によってさまざまであり，そうした方針のもととなるのがセキュリティポリシーである．ファイアウォールの設定や，ネットワークアプリケーションの利用基準の判断，組織内のユーザをアクセス権限ごとにグループ分けするなど，セキュリティポリシーが扱う項目はさまざまであり，汎用的なものはない．

セキュリティポリシーは組織が必要とするネットワークの利用法や,組織内にあるリソースの量や質，そして業務内容にも関連する．セキュリティポリシーは，こうした複雑な要素を総合的に判断して策定される．そして，ネットワーク環境を構成する個々の要素それぞれにセキュリティポリシーを設定するとともに，そのポリシーに適合するよう維持，運用していく．ただし，セキュリティポリシーは不変ではなく，新しいネットワークアプリケーションの出現や，新たなセキュリティ侵害手法の登場などを受けて刻々と変化し続けるものである．

前節でも述べたように，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 フラッドや UDP フラッドといったフラッド攻撃がある．いずれも大量のパケットを送りつける量的な攻撃であるが，パケット個々はプロトコルに違反していないため，攻撃パケットか否かを区別することが難しい．このため，ユーザのアクセス回線の帯域を消費させるのに効果的な攻撃としてもよく実施される．ここで，SYN フラッド 攻撃では，攻撃者は大量の SYN パケット（TCP で接続を確立する際にクライアントからサーバに最初に送られるパケット．TCP ヘッダの制御フラグで SYN フィールドがセットされたパケット）を標的に送り付ける．TCP では，通常，まずクライアントがサーバに SYN パケットを送り，サーバがクライアントに SYN/ACK パケット［ACK フラグと SYN フラグをセットしたパケット］を返信し，最後にクライアントがサーバに ACK パケット[ACK フラグをセットしたパケット]を送ることで接続が確立する．一般に,SYN フラッド攻撃では攻撃者は送信元を偽って SYN パケットを大量に送る.このため,サーバがクライアントに SYN/ACK パケットを送ったとしても,受信ホストは SYN パケットを送っていないため，このサーバの返答を無視する．このため，サーバは予めタイムアウトとして設定された一定時間が経過するまで記憶領域を保持しつづけなければならず，この間通常のユーザの接続は受けられない．また，UDP フラッドとは，大量の UDP パケットを送りつける攻撃である．

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のが一般的である．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，NGN の場合，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，私的セキュリティポリシー設定ユーザがUNIで受信するトラヒックがアクセスネットワーク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フラッド攻撃は，一方的に大量のUDPパケットを送るだけで，アクセスネットワークの帯域を占有することが可能なため，DoS 攻撃として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.

＜私的セキュリティポリシーを用いた制御の定義＞

私的セキュリティポリシーを用いた制御とは，各ユーザが各アプリケーションに対する利用帯域の制限を NGN 側の NNI で制限することを言う．NNI 側で制限することにより，ユーザ側のみならず,公衆ネットワークである NGN への不要なトラヒック流入を防ぐことになり,ひいては,NGNを利用する全ユーザのトラヒックの混雑を緩和することができる.

＜私的セキュリティポリシーの例(図 2.5)＞

私的セキュリティポリシーの例を示す.UDPを利用したDoS攻撃を検知するパラメータとして，単位時間（sec）のUDPパケット数（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，単位時間のUDPパケット利用可能帯域を決定する.

例として，UDP フラッド攻撃を検知するための，私的セキュリティポリシー(図 2.5)へ登録するパラメータ内容を以下に示す．ここでは，NGNからLANへ送信されるIPパケットが利用可能な帯域は30Mbpsで，UDPパケットが10%（3Mbps）以上の帯域を利用した場合，DoS攻撃として検知するものとする．また，UDPパケットの利用する帯域が10Mbps以下となる様にDoS攻撃を抑制するものとする.

・単位時間のUDPパケット数（帯域利用率）に10%（3Mbps）と登録する.
・単位時間（秒）のUDPパケット利用可能帯域に10Mbpsと登録する.

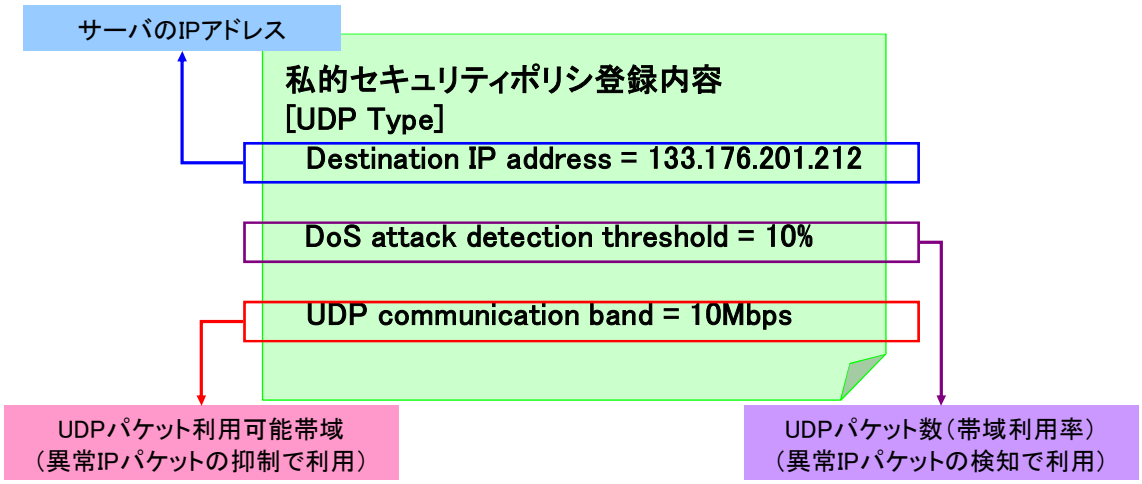


図 2.5　私的セキュリティポリシーの設定例

2.3.2　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．ここで，UDP フラッドとは，コネクションレス型通信である UDP の特徴（コネクションレス型通信では情報を伝えるということを相手に知らせずにデータを送信する．コネクションレス型通信では相手が受け取れるか確認せずに送信するので，データの到達性が保証されない）を利用するもので，いきなり非常に大きなサイズの UDP パケットを大量に送りつける攻撃である．

［インターネット接続サービス利用の前提条件］

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．ここでホワイトリス

トとは，対象を選別して受け入れたり拒絶したりするためのもので，受け入れる対象を列挙した目録である．送信者がホワイトリストに載っていない場合データ受信を拒絶する．

しかし，全ての UDP 送信者を登録するのは困難なため，使用帯域が微小であれ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の契約帯域の 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．

[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の定め方]

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．私的セキュリティポリシーを用いたトラヒック制御の検討モデルを図 2.6 に示す．

図 2.6 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（企業などのネットワークからインターネットなど外部へ接続する際に，複数の ISP を使って接続すること）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．

なお，マルチホーミングは単一の ISP に依存する場合（シングルホーミング）に比べ，耐障害性の向上や回線負荷の軽減などが期待できる．すなわち，マルチホーミングとすることにより，インターネット接続に冗長性（障害に備えて機材や回線などを複数用意し，並列に使用したり，一部をすぐ使える状態で待機させたりすること）を持たせ信頼性を高めることができる．

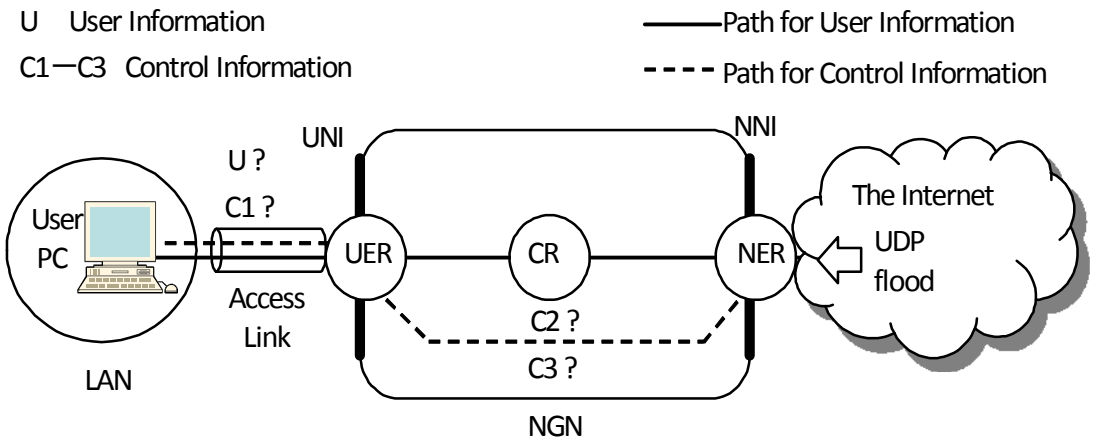


図 2.6　私的セキュリティポリシーを用いたトラヒック制御の検討モデルと情報の流れ

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．

2.3.3　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 2.6 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 のエッジルータ ER（以降 UER と記す）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（図 2.6 の C2）を用いて，トラヒック制御の実施ポリシーを NNI のエッジルータ ER（以降 NER と記す）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（図 2.6 の 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．SYN フラッドや 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．

また，提案したトラヒック制御によれば，NGN 内への異常トラヒックの流入を防ぐことから，私的セキュリティポリシーを適用したユーザ以外のユーザの利用帯域の低下を防ぐという効果もある．

2.4　トラヒック制御シミュレーションによる評価

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[13]を用いる．以下，QoS のキューイング（送信を待つデータを保存するメモリーをキューと呼ぶ．キューイングとはこのキューへの入力を管理する方式）に関する専門的術語を使用するが文献[14][15]等の関連文献を参考にされたい．

2.4.1　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 について実施する．

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をもたらすことを示す．

(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 2.7，図 2.8 に示す．

＜シミュレーションの前提＞

図 2.7 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.

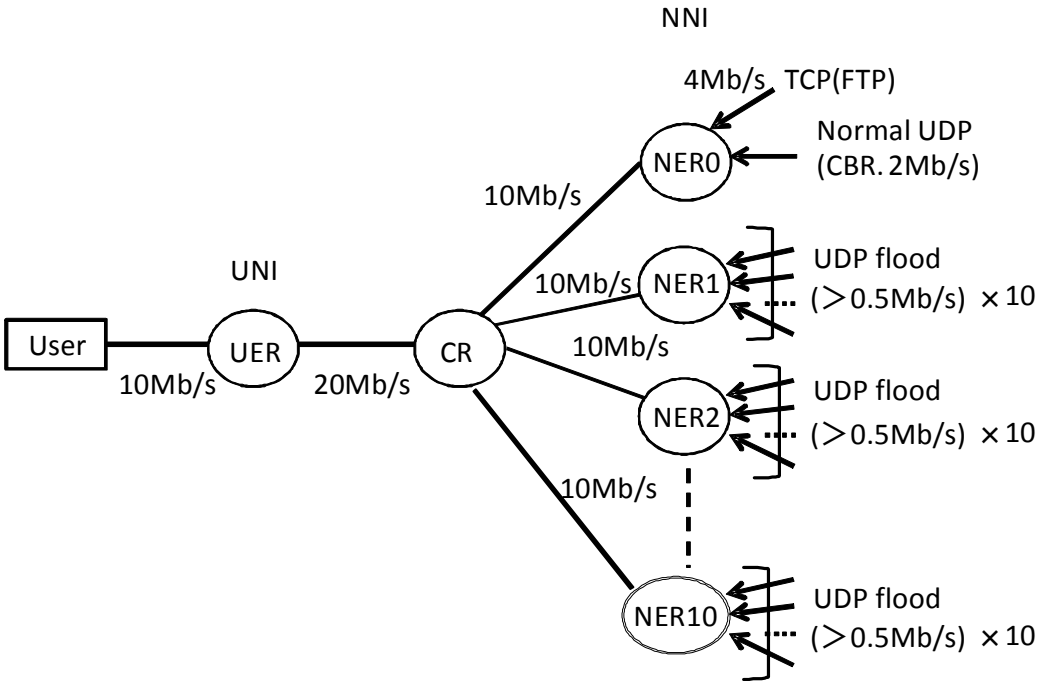


図 2.7　モデル 1

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，外部から 4Mb/s の帯域が与えられている．正常な UDP は 2Mb/s の CBR である．ここで，CBR（Constant Bit Rate）とは，コーデックの出力データの送信レート（速度）が一定であることを意味する．容量に制限のある通信路では最大ビットレートが通信路の容量を超えないようにする必要があるため，CBR はマルチメディアコンテンツのストリーミングに適しており，容量ぎりぎりまで利用することができる．複雑な部分に十分なデータを割り当てず品質や音質が低下する反面，単純な部分ではデータを無駄に使うため，CBR は情報を保存する用途には適さない．

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,スケジューリング(キューからデータを取り出す方式)はラウンドロビン(Round Robin. 以下 RR と略す）とする．ここで，ラウンドロビンスケジューリングは，オペレーティングシステムにおけるプロセスに関する単純なスケジューリングアルゴリズムの一種である．処理待ち状態のプロセスに対し，順番に同じタイムスライスを割り当てる方式を指すことによりスケジューリングする．なお，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 において受信 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，NNI の NER 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 2.8 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（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．全部で 100 経路の UDP フラッドは 1 経路ずつ 15 秒から 0.05 秒間隔で順次発生し，20 秒で全ての UDP フラッドが発生する．また，30 秒から 0.05 秒間隔で 1 経路ずつ順次停止し，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．Drop tail とは，輻輳状態になると，到着パケットがすべてキューの入口で破棄するキュー管理方式である．ここで，キューにデータを一時的に保管し，一定の規則に従ってデータを取り出し送出することをキューイングあるいはキューマネジメントと呼ぶ．通信分野では，優先制御を実現する主要技術としても使われる．なお，キューイングマネジメントとスケジューリングを合わせてキューイングと総称することがある．

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 2.8 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．NNI の 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．同図では，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ことがわかる．

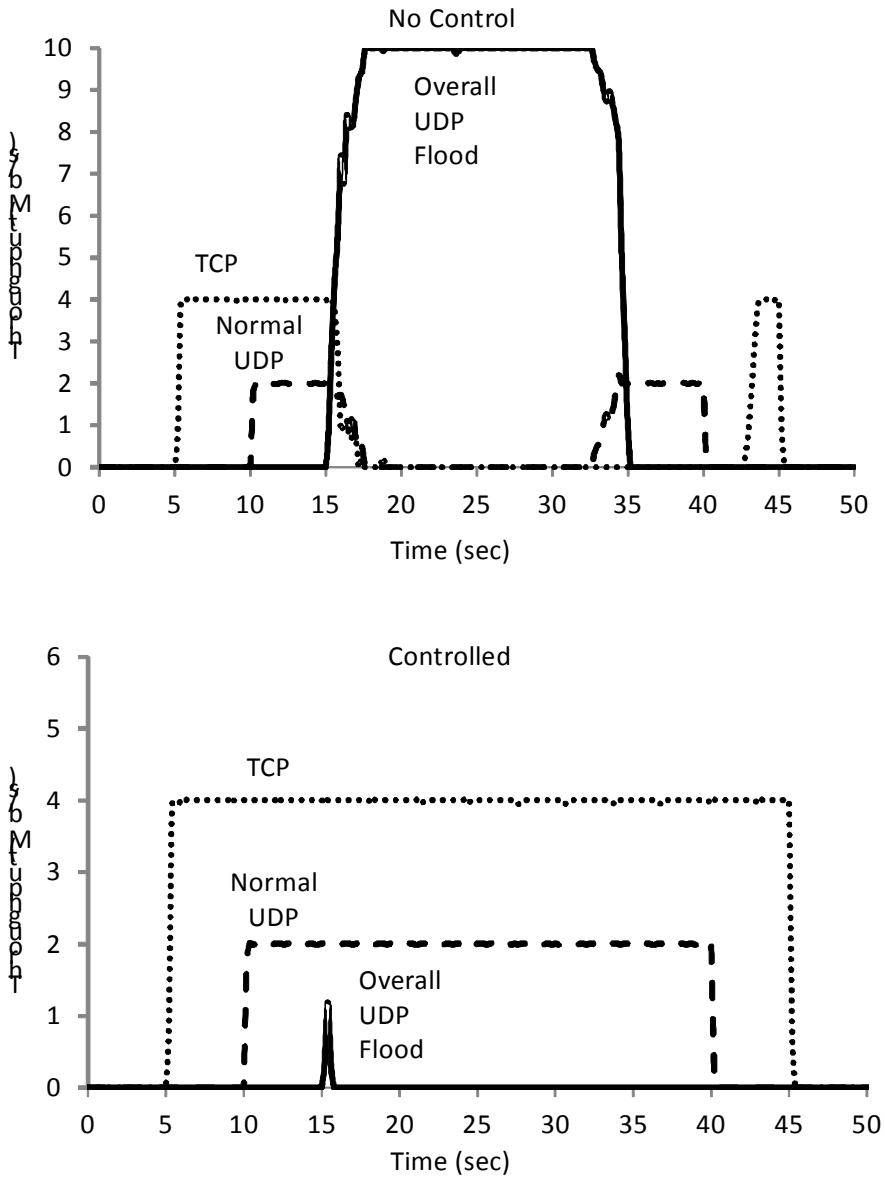


図 2.8　モデル 1 の計算機シミュレーション結果

(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 2.9，図 2.10 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 2.9 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．他ユーザについては，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．TCP のアプリケーションは FTP で，外部から 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．

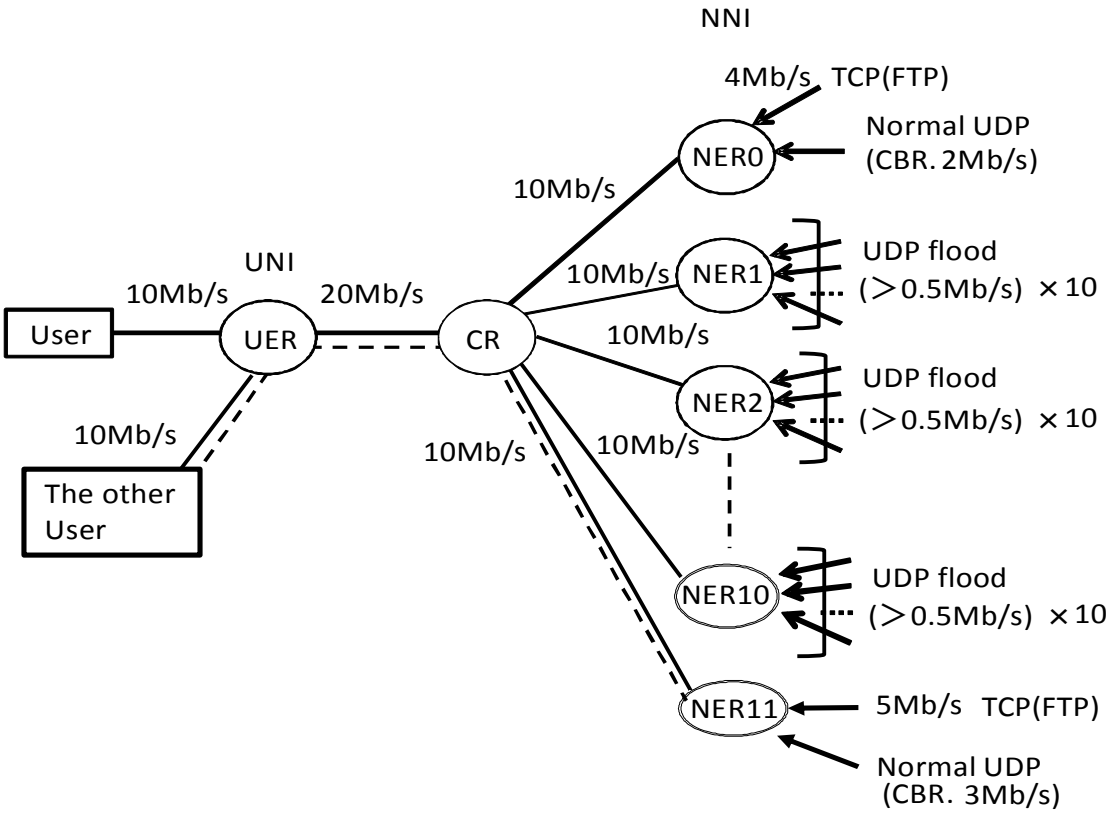


図 2.9　モデル 2

＜シミュレーション結果＞

図 2.10 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，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．なお，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 のシミュレーション結果（図 2.8 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 NNI 内の 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 2.10 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．モデル 1 のシミュレーション結果（図 2.8 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，アクセスネットワークを共同利用している（帯域を共有している）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．

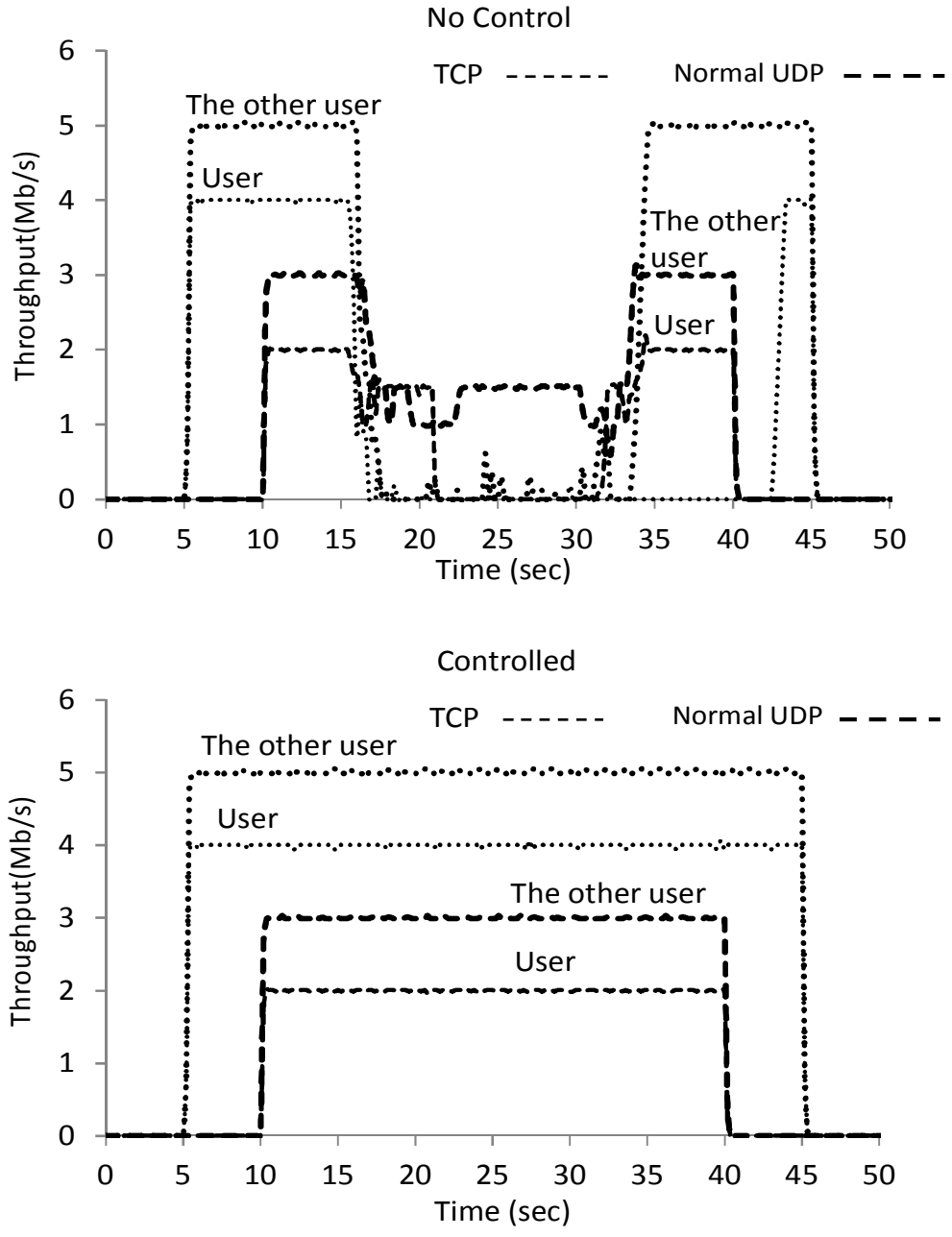


図 2.10　モデル 2 の計算機シミュレーション結果

2.5　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の適用効果について考察する．次に，本提案の影響と課題を，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．最後に，工学的視点および社会学的視点から考察をまとめる．

2.5.1　適用効果

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，シミュレーション結果でも示したように，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．

2.5.2　本提案の影響と課題

(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．しかし，通信事業者が適正に契約を履行しているかどうかはユーザに見えにくいため，通信事業者が本提案によるサービスの提供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．

最後に本章の検討全体について，工学的考察および社会学的考察をまとめる．

［工学的考察］

本文ではユーザが実施しているセキュリティ対策の一部を情報通信ネットワークが請け負う形で実施することを提案した．該当する具体的な要素技術はパケットフィルタリングである．パケットフィルタリングは，ルータやファイアウォールが持っている機能の一つで，送られてきたパケットを検査して通過させるかどうか判断する機能である．パケットのヘッダにはプロトコルや送信元アドレス，送信先アドレスやポート番号などの情報が含まれており，これを参照して通過するかどうかが決定される．通過できなかったパケットは送信元に通知されたり，破棄されたりする．どのような方針に基づいて判断するかは，そのネットワークの管理者が任意に設定することができる．

本堤案はユーザからすると，単にファイアウォールが LAN と WAN の境界から NNI に移動したものであり適用イメージは明確であろう．

一般にセキュリティの良否の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．本提案は私的セキュリティポリシーの運用で「発生確率」を低減する．従って，個々のコンピュータウィルスや迷惑メールの「影響度」が不変であるならば，不正トラヒックが少なくなった分だけ「リスク」も小さくなる事になる．

本文の例でいえば，UDP フラッドのような攻撃トラヒックのユーザへの到達性が低減された分だけユーザの「リスク」を軽減することになる．具体的な「リスク」を数値的に表現することは本検討の段階では困難であり今後の検討課題であるが，本提案がセキュリティリスクの低減に有効であることはシミュレーション結果からも明らかであろう．

［社会学的考察］

本提案を実施し，セキュリティ対策の主体を情報通信ネットワーク側に移すと，悪意のあるトラヒックがユーザに到達しにくくなるため，ユーザ負担も軽減することが予想される．一方，情報通信ネットワーク側の負担は従来に比べ増加する事になるがセキュリティ対策機能が集約されるため情報通信システム全体的としての負担は低減することが見込まれる．

本提案の導入にあたって検討すべき課題として，情報通信ネットワーク側の導入負担とセキュリティのバランス，さらに，社会的コンセンサス，法制度といった問題がある．情報通信ネットワーク側は，情報通信ネットワークの利用帯域が有効に利用されるので，私的セキュリティポリシー導入には好意的と予想されるが，一方で導入費用負担も発生するため双方のトレードオフになる．また，送信側ユーザからすれば，悪意がないのにもかかわらず，UDP フラッド等が発生している場合に，UDP パケットを落とされることがあるので，通信の秘密や自由を束縛するという見方もあろう．

私的セキュリティポリシー導入によるセキュリティ向上の情報通信ネットワーク側の導入負担およびメリットが利便性低下によるデメリットを上回るという根拠を示して社会的コンセンサスをとることが必要となる．

［本件の参考］

フラッド型攻撃に関する通信の秘密の考え方として，「電気通信事業者[16]における大量通信等への対処と通信の秘密に関するガイドライン」等[17][18]が参考になる．すなわち，そこでは，受信者又は受信回線の加入者から個別の同意を取得して，大量通信等への対処を行う場合には通信の秘密の侵害にはならない，方向性が示されている．本

提案についても同様な考え方が適用とされるものと推察されるが，今後関係者との議論が必要となろう．

2.6 まとめ

本文では 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，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．さらに，本提案の影響と課題を，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，の各視点から考察し，整理した．

第 3 章　公的セキュリティポリシーを用いたトラヒック制御

3.1　まえがき

企業等では，ネットワーク接続された情報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ことがある．情報セキュリティに関する脆弱性検査はペネトレーションテスト（疑似侵入試験）[19]とも呼ばれ，今日では広く実施されている．

＜ペネトレーションテストの定義＞

ペネトレーションテストとは,コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで,システムを実際に攻撃して侵入を試みる手法である．特に,ネットワーク接続された情報システムが外部からの攻撃に対して安全かどうか,実際に攻撃手法を試しながら安全性の検証を行う．不正に侵入できるかどうかだけでなく,DoS(サービス拒否)攻撃にどれくらい耐えられるかを調べたり,侵入された際にそこを踏み台にして他のネットワークを攻撃できるかどうかなどを調べる場合もある．

セキュリティ対策用のソフトなどを導入しても,設定が十分でなかったり,新たにセキュリティホールが見つかって攻撃手法が開発されたりする場合がある．そこで,多くのセキュリティ事業者が侵入テストサービスを提供しており,定期的にテストをすることによりシステムの安全を保つことができる．

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テストを受けている．テストの結果，セキュリティ対策が新たに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利用環境の安全を維持することができる．

現状，このペネトレーションテスト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く，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，対象を個人ユーザの PC 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る．ただし，評価結果によって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あろう.

3.2 研究の位置づけと目的

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，以下のような公的セキュリティポリシーを用いたトラヒック制御を提案する．脆弱性検査と,QoS の一方式である Diffserv 等の優先制御を合わせ行って,セキュリティ的に脆弱であると判断されるユーザの利用環境を事前に振り分ける．さらに，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につながると考えられる．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，公衆ネットワークを運用する手順を提案する[20].

本提案は,通常利用する大きな帯域を持つネットワークへの有害トラヒックの流入を回避することが可能である．また，本提案における優先転送制御は，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も向上するため，ユーザのセキュリティ意識や情報モラルの向上が期待される．

ここで，優先転送制御とは，IP ネットワークなどパケット通信ネットワークを流れるパケットに何段階かの優先順位を付けてクラス分けしサービス品質（QoS）に差を付けることである．従来の QoS はアプリケーションの重要度を複数に分類し，重要度の高いアプリケーションのパケットを優先して転送している．このように，従来の QoS は貴重な伝送データを遅延やパケット破棄から救済できる機能として広く適用されている．

3.3 公的セキュリティポリシーを用いたトラヒック制御の提案

本節では，公的セキュリティポリシーの決定，および公的セキュリティポリシー設定からトラヒック制御実施までの流れ，について示す．

3.3.1　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，脆弱性検査の詳細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[19]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．本文では，さらに，以下に示すような，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．

＜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[21]．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．

＜セ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[22]．　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，脆弱性検査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，ことでネットワーク利用環境（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，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，表 3.1 のように，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．なお，ウィルス感染していると判定される場合は接続を拒否するものとする．

表 3.1　セキュリティレベルと優先転送制御

Security Level	Evaluate Value	Priority Control	Diffserv PHB
High	0.0～3.9	高優先	Expedited Forwarding
Middle	4.0～6.9	中優先	Assured Forwarding
Low	7.0～10.0	低優先	Best Effort
-	ウィルス感染している場合	接続拒否	―

3.3.2　公的セキュリティポリシーの設定

公的セキュリティポリシーを用いたトラヒック制御の検討モデルと情報の流れを図3.1に示す．上述の公的セキュリティポリシーはNGN事業者が図3.1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3.1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．ここでセキュリティインシデントとは情報漏えい,不正アクセス,ウイルス感染といった情報セキュリティに関わる事件･事故である．

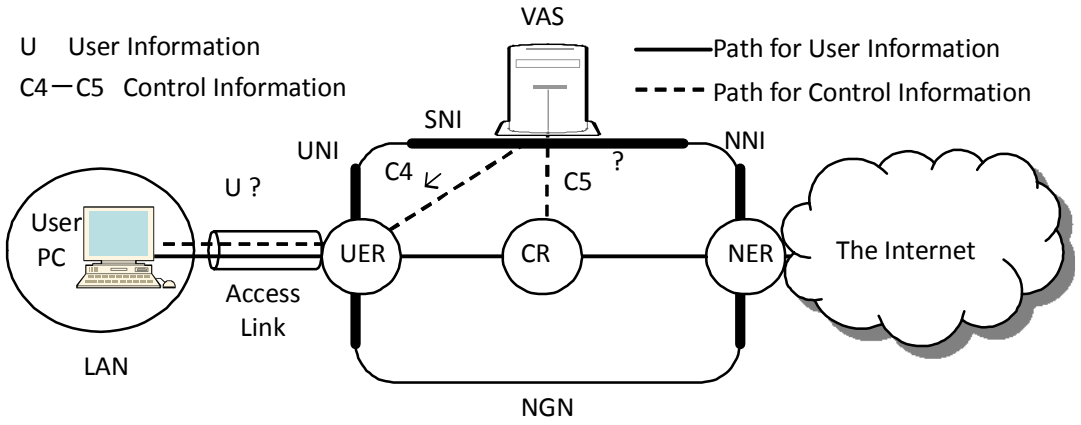


図3.1　公的セキュリティポリシーを用いたトラヒック制御の検討モデと情報の流れ

3.3.3　トラヒック制御実施までの流れ

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. DS. ディフサーブ）[15]が広く適用されている.

＜Diffserv とは＞

Diffserv とは IP ネットワークにおいて Intserv （Integrated Services. イントサーブ）のように通信フローごとに QoS 保証（通信品質保証）を行うのでなく,複数のフローをまとめて（アグリゲートして）数個程度のクラスを作り,クラスごとに決まった品質保証法を適用する QoS 技術である. IETF の RFC 2475[23] などの標準ドキュメントによって規定されている.

＜Diffserv ベース QoS＞

Diffserv ベース QoS は,ルータが入力されたパケットの IP ヘッダの DS フィールド中 の 6 ビットの DSCP（Differentiated Service Code Point）値を参照し,DSCP 値により定義される PHB（Per-Hop Behavior. ルータの Diffserv に関する処理動作の仕様）に応じてパケットをクラス分けする QoS である. Diffserv ベース QoS 各クラスにおける優先転送の様子を図 3.2 に示す. 図 3.2 において，クラス分けされたキューごとに，スケジューラで優先制御もしくはシェーピングによる帯域制御が実施される. ここで，シェーピングとは，通信量を一定の水準に抑えるためにパケットの間隔（遅延）を制御する方式の一つで，規定の通信容量を超えるデータをルータに保存し，容量に空きができたときに送信する方式である.

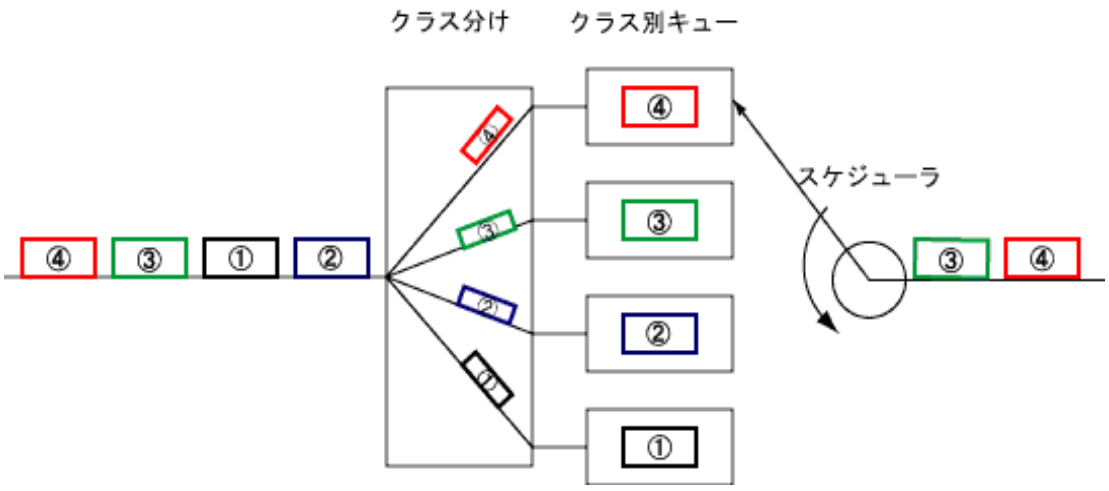


図 3.2　Diffserv での優先転送

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，この品質クラスをセキュリティレベルに置き換える事によって本提案を実現できる．具体的に，公的セキュリティポリシー設定は，図 3．1 で以下のように実施される．

まず，NNI を介して，脆弱性評価サーバ VAS は SIP 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を UNI の UER に伝える．次に，UER は端末認証（NGN の場合は端末とアクセス回線を識別情報として用いる回線認証）を実施して，ユーザの真正性を確認し，同ユーザの利用環境から送信されるパケットヘッダにセキュリティレベル情報を記載して CR に転送する．ここで，端末認証とは，ネットワークへアクセスを試みようとしている端末が正当なものであるか否かを，固有の MAC アドレスや通信時の IP アドレス，もしくは他の ID・パスワードなどによって認証する仕組みのことである．また，回線認証とは，「このユーザは確かにこの場所（回線）から通信してきた」ということを確認するためのユーザ認証技術である．NGN における回線認証・端末認証の様子を図 3.3 に示す．

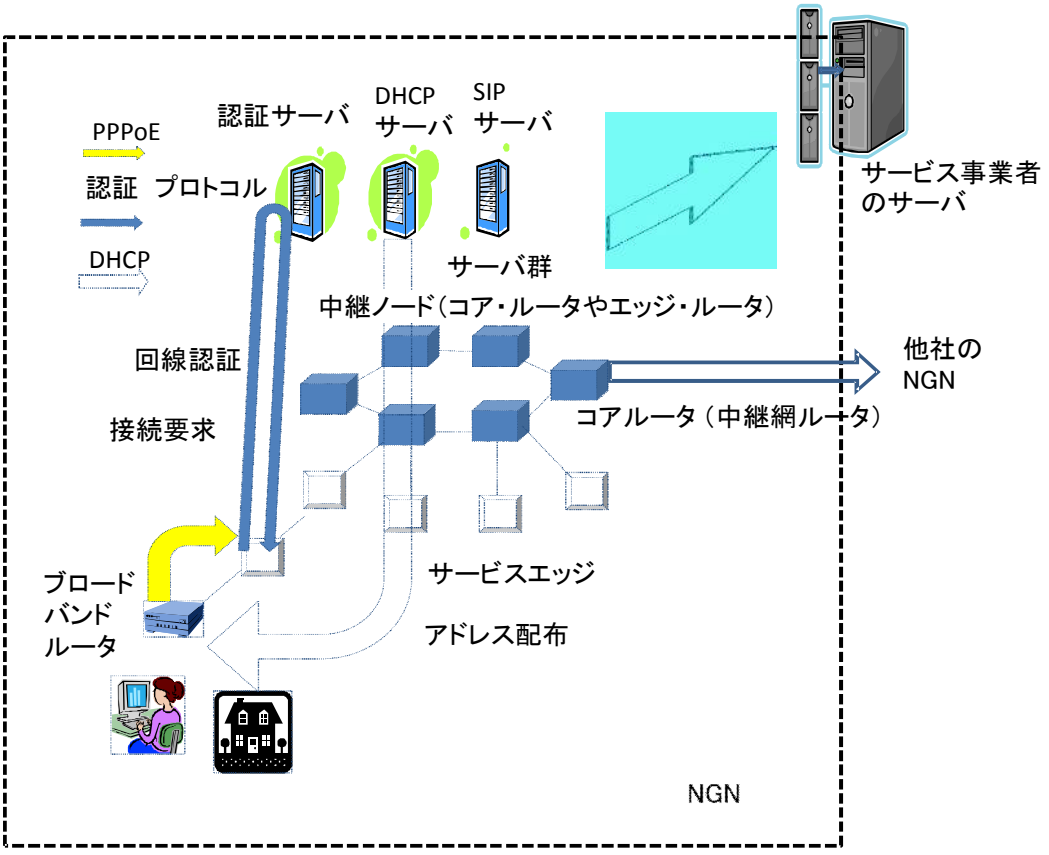


図 3.3　NGN における回線認証・端末認証

この端末認証を終えると，図 3.1 において，脆弱性評価サーバは制御信号（C5）を用いて，Diffserv 実施のための PHB を CR に設定する．本提案の場合，この PHB は IP ヘッダに記載されたセキュリティレベル情報に基づく優先転送動作仕様である．

以上のように設定された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 UNI の UER および CR によりトラヒック制御される．

3.4 トラヒック制御シミュレーションによる評価

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[13]を用いる．以下，QoS のキューイングに関する専門的術語を使用するが文献[14][15]等の関連文献を参考にされたい．

3.4.1　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

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 について実施する．

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 3.4，図 3.5 に示す．

＜シミュレーションの前提＞

図 3.4 において，セキュリティレベルが High／Middle／Low（表 3.1）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するものとする．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ラウ

ンドロビン RR で，適用する場合は重みづけ RR，すなわち WRR（Weighted RR）でスケジューリングするものとする．例えば，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）とした．ここで，RED とは，輻輳防止アルゴリズムの一種でもある[14]．

＜キューマネジメント RED＞

従来からある Drop tail 方式では，ルータなどのネットワーク機器は可能な限り多くのパケットを溜め込み，バッファに入りきらなくなったパケットを単に捨ててしまう．バッファが常に満杯なら，ネットワークは輻輳状態である．Drop tail では，バースト的にパケットが廃棄されるため不公平なキューマネジメントであると言われている．また Drop tail は TCP グローバル同期の原因にもなり，全ての TCP コネクションが同時に待ち状態になり，同時に再開しようとする状態が発生しやすい．ネットワークは利用率が低下していくことになる．RED はこの問題への対処として適用されている．

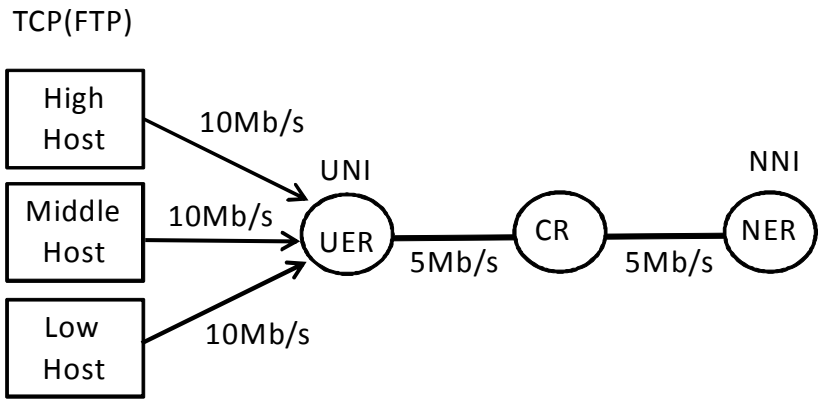


図 3.4　モデル 3

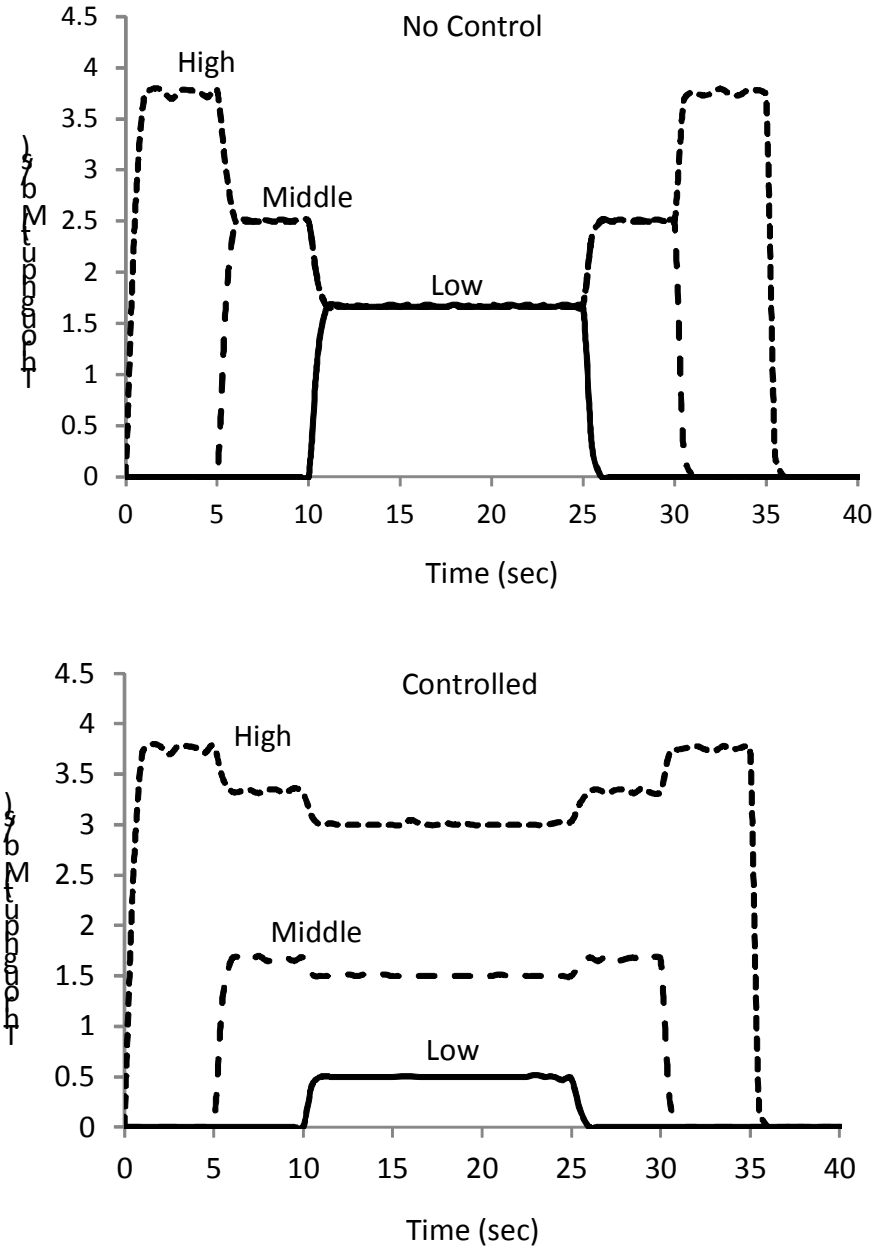


図 3.5　モデル 3 の計算機シミュレーション結果

＜シミュレーション結果＞

図 3.5 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 3.5 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 3.6，図 3.7 に示す.

＜シミュレーションの前提＞

図 3.6 のモデル 4 は，セキュリティレベルが各々High／Middle／Low（表 3.1 参照）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.

なお，インターネットには無数の DNS サーバが存在しており，ドメイン名に対応した階層構造になっている．最上位に位置する DNS サーバは「ルートサーバ」と呼ばれ，全世界に 13 台が分散配置されている.

図 3.6 において,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（もしくは，DNS amp）と呼ばれる攻撃[24]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 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 3.6 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.

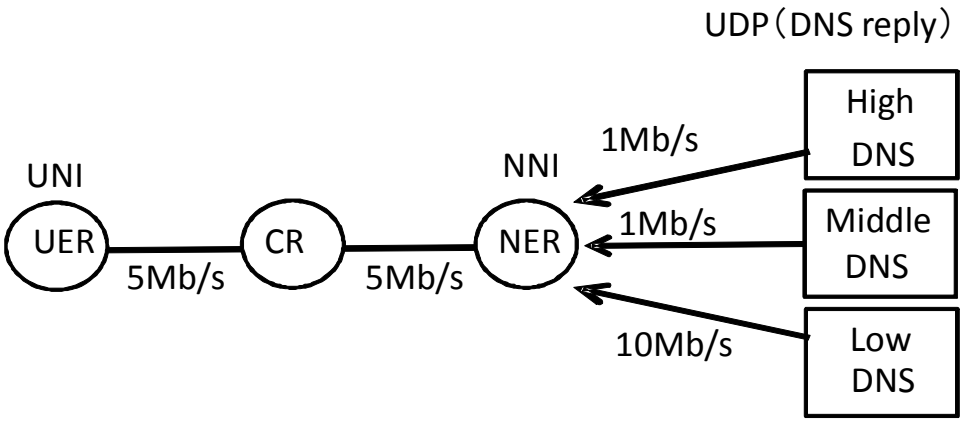


図 3.6　モデル 4

＜シミュレーション結果＞

図 3.7 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，UNI では，NNI 側からユーザ側の方向に通過する 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 パケッとである 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 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 3.7 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 3.7 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．

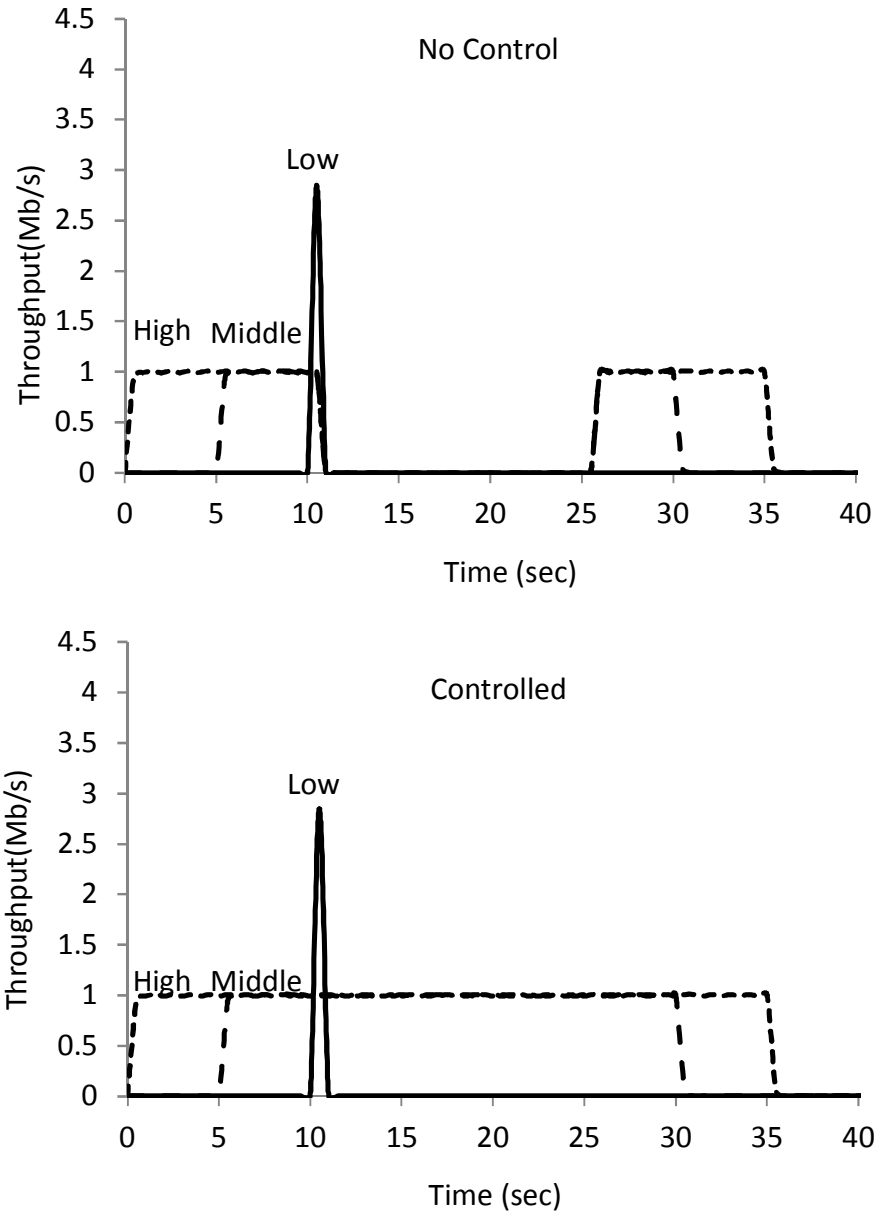


図 3.7　モデル 4 のシミュレーション結果

3.5 考察

ここでは，最初に，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，本提案の影響と課題を，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．最後に，工学的視点および社会学的視点から考察をまとめる．

3.5.1 適用効果

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，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．公的セキュリティポリシーの適用は脅威の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，セキュリティレベルの高いトラヒックが増える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利用リスクを軽減することになる．

3.5.2 本提案の影響と課題

(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，ユーザ個々に独自のポリシーを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，脆弱性検査や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．

なお，本提案ではユーザ個々に直接に脆弱性検査を行うことを前提にしているが，脆弱性の有無は，OS やアプリケーションのパッチ等が最新のものであるか，あるいはセキュリティ対策ソフトが定常的に更新されているか，によっても間接的に判断可能な場合が多い．これらの OS やアプリケーションのパッチのバージョン，セキュリティ対策ソフトの更新状況はそれぞれのベンダがユーザ個々にネットワーク経由でモニタしている．そこで，これらのモニタ情報を利用すれば,間接的に脆弱性の有無は判断でき,ことさら,ユーザ個々の脆弱性検査を行わなくとも済むことが予想される．すなわち，ベンダが把握しているユ

ーザのセキュリティ対策情報を利用することで，本提案が実施できる可能性がある．その場合，上述したような脆弱性検査のための費用は不要になり，本提案の導入が現実的になると予想される．ただし，この場合もベンダがユーザ個々の情報をネットワークプロバイダに渡すことになるため，ユーザのコンセンサスを事前に取り付ける必要があろう．

(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．

最後に本章の検討全体について，工学的考察および社会学的考察をまとめる．

［工学的考察］

本文ではLANで実施されている検疫あるいは脆弱性検査といったセキュリティレベルの評価とそれに基づくトラヒック制御を公衆ネットワークに適用することを提案した．該当する具体的な要素技術はQoSである．QoSについてはパケット転送品質保証という従来のQoSの目的とは異なる目的に使う事になるので，併用する場合に生じる問題について検証が必要である．

次に，QoSの実施に関する拡張性を考察する．本文では公的セキュリティポリシーの実施にDiffservを用いているので，この場合について考える．UNIのERにおいてIPヘッダに優先転送情報を書き込み，それに基づいてCRで優先転送制御するという手順は，従来のパケット転送品質保証と同様であることから，端末のセキュリティレベル決定後のDiffservの実施に関する拡張性はパケット転送品質保証とほぼ同じということができる．

ただし，パケット転送品質保証の場合はユーザと情報通信事業者の契約内容が頻繁には変わらないことから，IP ヘッダに書き込む優先転送情報も一定であるのに対し，本提案の場合，端末の脆弱性評価を頻繁に実施しなければ情報通信ネットワークの安全性が確保できないため，結果として IP ヘッダに書き込む優先転送情報も頻繁に変わる事になる．従って，脆弱性評価情報とそれを基にした優先転送情報の管理についても拡張性を検討する必要がある．また，ペネトレーションテストでは疑似的な侵入や攻撃をおこなうことで脆弱性評価の正確性を期すが，逆に評価対象の構成に影響を与えてしまい，OS を再インストールしなければならないといった事態も生じうる．このような弊害を少なくするテスト手法の確立も求められる．

さらに，本提案のセキュリティ改善効果について考察する．一般にセキュリティの良否の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と同様，公的セキュリティポリシーの運用も「発生確率」を低減する．従って，個々のコンピュータウィルスや迷惑メールの「影響度」が不変であるならば，不正トラヒックが少なくなった分だけ「リスク」も小さくなる事になる．本文の例でいえば，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を設定した情報通信ネットワークの「リスク」を軽減する事になる．具体的な「リスク」を数値的に表現することは本検討の段階では困難であり今後の検討課題であるが，本提案がセキュリティリスクの低減に有効であることはシミュレーション結果からも明らかであろう．

［社会学的考察］

本提案の導入にあたって検討すべき課題として，ユーザの利便性とセキュリティのバランス，さらに，社会的コンセンサスや法制度の問題がある．公的セキュリティポリシーによるトラヒック制御が運用された場合，端末の脆弱性評価が実施されるため，ユーザの利便性が現状より低下するのは避けられない．特に，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ないユーザは，情報通信ネットワークの利用帯域が低減されるので，公的セキュリティポリシー導入に反対する事になろう．このため，公的セキュリティポリシー導入によるセキュリティ向上のメリットが利便性低下によるデメリットを上回るという根拠を示して社会的コンセンサスをとることが必要となる．

さらに，憲法や電気通信事業法で定めている「通信の自由」や「通信の公平性」といっ

た原則の議論が必要である．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遵守することは当然であるが，インターネットのように高度情報通信ネットワークが普及している今日，「通信の安全」の制度化についても本検討のような技術的検討と並行した議論が求められる．

3.6　まとめ

本文では 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 に公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 からユーザの SNS 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．さらに，本提案の影響と課題を，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，の各視点から考察し，整理した．今後は前節で示した課題について検討し，本提案の実用化を目指す．

第 4 章　情報セキュリティ DB を用いた SNS 会員資格制度提言

4.1　まえがき

最近，インターネット上のサービスである“Twitter（ツイッター)”などのミニブログサービスや，“mixi（ミクシィ)”，“Facebook（フェイスブック)”，“Google+（グーグルプラス)”などの SNS（ソーシャルネットワーキングサービス）が人気である．

SNS とは，人と人とのつながりを促進・サポートする，コミュニティ型の Web サイトである．友人・知人間のコミュニケーションを円滑にする手段や場を提供したり，趣味や嗜好，居住地域，出身校，あるいは「友人の友人」といったつながりを通じて新たな人間関係を構築する場を提供する，会員制のサービスである．人のつながりを重視して「既存の参加者からの招待がないと参加できない」というシステムになっているサービスが多いが，最近では誰も自由に登録できるサービスも増えている．

SNS には，自分のプロフィールや写真を会員に公開する機能や，互いにメールアドレスを知られること無く別の会員にメッセージを送る機能，新しくできた「友人」を登録するアドレス帳，友人に別の友人を紹介する機能，会員や友人のみに公開範囲を制限できる日記帳，趣味や地域などテーマを決めて掲示板などで交流できるコミュニティ機能，予定や友人の誕生日などを書き込めるカレンダー機能，などを持つサービスが増えている．

これらのサービスは，今の自分の行動や考えを簡単にインターネット上に発信できることや，同じ趣味や考えを持つ利用者同士の交流の場として利用できることが特徴となっており，多くの利用者を集めている．その反面，悪意ある者からサービス利用者が狙われるようになった．

このような脅威が増す大きな要因として，SNS 利用に関する利用規則，セキュリティチェックや検疫が十分行われていないことが挙げられる．

そこで，本文では，将来，情報セキュリティデータベース(以下セキュリティ DB)を用いた SNS 会員資格制度の創設が必要と仮設を立て，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，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．

以降では，4.2 では SNS における情報セキュリティの現状と対策の課題，4.3 では解決

への指針，4.4 では情報セキュリティ DB を用いた SNS 会員資格制度提言，4.5 では組織体制， 4.6 では考察，4.7 ではまとめ，をそれぞれ示す．

4.2 SNS における情報セキュリティの現状と対策の課題

4.2.1 SNS における情報セキュリティの現状

SNS は，知り合い関係に特化してソーシャルシステムを形成しているだけに，一旦セキュリティインシデント（情報漏えい，不正アクセス，ウイルス感染，その他の事件や事故）が発生するとそのダメージが大きく，マルウェア感染や詐欺行為のプラットフォームとしての利用やウイルス感染の危険度はメールより 10 倍も高いといわれている[25]．また，著名人の「なりすまし」も Twitter で相次いでいる[26]．

4.2.2 SNS における情報セキュリティ対策の課題

日本 SNS セキュリティ協会が，セキュリティとプライバシーの課題と対策に関する報告書[4]を提出して，ユーザに警告を行っているが，知識の乏しいユーザがセキュリティ対策を理解して，十分に実行することは難しいと考える．また内閣官房情報セキュリティセンター情報セキュリティ政策会からも対策指針[27]が示されているが，関連部署がうまく連携して十分な効果をあげているとは言い難い．

4.3 解決への指針

SNS における情報セキュリティ問題の原因について以下の仮説を考える．

（仮説） SNS の情報セキュリティレベルが低いのは社会制度が未成熟なためである．

表 4.1 は自動車交通と SNS の制度を比較したものであるが，何かを運ぶということで類似している運輸交通制度と比較して，SNS では，運用に関するライセンス制度や車検制度といった社会制度がないので,不正行為をした匿名ユーザを特定したり，アクセスサーバのウィルス感染を検証したりすることが困難である．そこで，上記の仮設を前提として，SNS での会員資格制度導入が必要であると考え,セキュリティ DB を用いた会員資格制度を検討する[7][28]．

表 4.1　自動車交通と SNS での制度比較

項目	自動車 交通	SNS
ユーザ ライセンス	有	なし
利用媒体	車両	パソコン, LAN 等
安全性 検定制度	車検制度	検定なし
ライセンス 登録先	警察	なし

4.4　情報セキュリティ DB を用いた SNS 会員資格制度提言

前節までの考察から，セキュリティ DB を用いた SNS 会員資格制度を提言する．転送という機能の点で類似している運輸交通システムと比較しつつ検討する．具体的には，会員資格を示す証明書として，SNS 会員証，セキュリティ検査証明書，アクセス査証の三つを提案する．

＜情報セキュリティ DB の定義＞

情報セキュリティ DB とは，提案した以下の三つの証明書および関連するセキュリティ情報を DB 化したものである．

・SNS 会員証

・セキュリティ検査証明書

・アクセス査証

＜提案の前提条件＞

提案の前提条件としては，なりすましを防止するため，SNS 利用に際し，以下の証明書

等の提示が求められるものとする．

(1)SNS 会員証

公衆道路で自動車を運転する場合，自動車運転免許証を所持していることが求められる．現在，SNS 利用において同等の公的利用資格は存在しないが，SNS の安全性（セキュリティ）を維持するため導入することが望ましいと考える．SNS 利用に関する資格証，すなわち SNS 会員証を取り入れることによって，SNS の不正使用を抑止しサイバー犯罪を未然に防止する効果が見込まれる．

表 4.2 で SNS 会員証と運転免許証を比較する．同表のように自動車運転免許証には，氏名，生年月日，本籍，交付年月日，免許番号，免許の種別と免許の条件，有効期間，発行機関（都道府県の公安委員会），優良ドライバであるか否か，が記載されている．また，免許所持者の顔写真が添付される．

SNS 会員証は，自動車運転免許証の SNS 版に相当し，基本的な記載事項は自動車運転免許証と同様に，氏名,生年月日,本籍,SNS アドレス,交付年月日,会員証シーケンス番号,利用条件,SNS 利用有効期間,証明書発行機関である．

＜SNS 会員証の取得条件＞

自動車運転免許証がドライバの運転能力を保証しているのに対し，SNS 利用に関して能力を問う必要性はないと考えられることから，原則全てのユーザに対して発行するものとする．また，自動車運転免許証で優良ドライバの表示を行い，運転の適正性を評価しているのと同様に，SNS 会員証では優良ユーザの表示を行い，サイバー犯罪履歴やセキュリティ上の過失が無いことを保証する．このような評価を行うことによって，ユーザのセキュリティ意識を高め，適正な SNS 利用を促進することが期待される．

なお，周知のように，自動車運転免許証は点数制度をとっており，事故や違反を犯すことによって減点され，減点の累積値が規定値を超えると免許停止などの処罰が行われる．SNS 会員証の場合にも同様の点数制度を適用し，SNS 利用を規制もしくは停止するなどの処罰を行う．

この SNS 会員証の発行・管理は SNS プロバイダが主幹する．SNS 会員証の記述様式や失効管理は，公開鍵暗号方式における電子証明書と同様に行う．なお，ユーザは SNS 利用に

際して，SNS 会員証の提示が求められるが，自動車運転免許証と異なり，利用の都度，SNS 間の全ての検査箇所でその具体的記載事項を検査するとなると，SNS 入口のゲートウェイでの処理負荷が大きくなる．これを防ぐためには，送信者が所属する SNS の一つで利用の適切性を詳細にチェックし，予め信頼関係を結んだ SNS 間ではその結果のみを簡易に調べて，通過もしくは受信を許可するものとする．

表 4.2　SNS 会員証と運転免許証

SNS 会員証	運転免許証
氏名	氏名
生年月日	生年月日
本籍	本籍
SNS アドレス	現住所
交付年月日	交付年月日,
会員証シーケンス番号	免許シーケンス番号
利用条件：SNS 名等	利用条件：眼鏡等
SNS 利用有効期間	免許有効期間
証明書発行機関	証明書発行機関

(2)セキュリティ検査証明書

SNS 会員証がユーザとしての適格性を示すのに対して，PC やネットワーク機器等，ユーザの SNS 利用環境の適格性を保障するセキュリティ検査証明書[29]を導入する．このセキュリティ検査証明書とは運輸交通ネットワークにおける車検（自動車検査証）に相当する．すなわち，セキュリティ検査証明書は接続使用機器や LAN について，セキュリティ攻撃に対する脆弱性，および他を攻撃する危険性，がないことを検査した証しとなる．検査対象の識別情報として，対象が LAN のようなネットワークであれば管理者情報が記載され，接続機器であれば製造情報や所有者情報が記載される．

また，共通して記載される事項としては，ハードウェアや搭載されているソフトウェア

の情報，およびセキュリティ対策とその検査情報が記載される．なお，脆弱性を指摘したり，最新のセキュリティ環境に更新するサービスはすでに多く実施されている．すなわち，企業ユーザであれば LAN を対象にセキュリティベンダの脆弱性検査サービスを受けたり，検疫ネットワーク技術を採用している場合が多い．また，多くの個人ユーザはセキュリティ対策ソフトをインストールし，更新サービスを受けている．しかし，これらのセキュリティ検査は独自に実施されており，その内容も公開されていないのが現状である．この理由は，インターネットサービス利用の安全性はユーザ個々に，特に受信側の自己責任で攻撃を防御する，という発想に基づいているためである．換言すれば，SNS の入り口でセキュリティ上の脅威を排除し，公的にセキュリティレベルを保証しようという趣旨で実施されているものはない．

＜セキュリティ検査証明書の取得条件＞

このセキュリティ検査証明書は，末端のクライアントコンピュータから始まって，公開サーバやルータといった情報通信機器毎に発行される．また，これらの機器を管理する LAN や ISP に発行される．従って，対象となる機器やネットワークの種類に応じて，所要の検査項目や評価方法をルール化しておく必要がある．

検査周期について，車検のような年単位では目まぐるしく変化するセキュリティ環境に対応できない．このため，長くとも四半期あるいは月単位の周期とする必要があると考えられる．なお，セキュリティ検査は対象の包含関係に応じて階層的に実施され，複数 SNS を経由する場合は予め結ばれた信頼関係により，同時に参加している２番目以降の SNS では検査が省略あるいは簡略化される．表 4.3 に車検証と情報通信機器検査証との比較を示した．

表 4.3　車検証と情報通信機器検査証との比較

制度	SNS 会員制度	自動車運転免許制度
検査対象	クライアント端末・サーバ	自動車
検査証	セキュリティ検査証明書	車検証

(3)アクセス査証

アクセス査証とは，海外渡航に必要な査証に相当するもので，SNS あるいはユーザが独自のセキュリティポリシーに基づいて発行管理する．

＜アクセス査証の取得条件＞

SNS 会員証やセキュリティ検査証明書が SNS を利用するための一般的資格条件であるとすれば，このアクセス査証は個別の SNS として利用者に付与する特殊な利用資格条件となる．このアクセス査証を用いない場合のアクセス条件は一般的資格条件と同じとみなされる．なお，このアクセス査証の登録管理はセキュリティ検査証と同様に階層構造をなし，同様に信頼関係に基づいて検査される．

以上，本章では SNS の会員資格を示す証明書として，SNS 会員証，セキュリティ検査証明書，アクセス査証の三つを提案し，その概要と検査方法を示した．これらの証明書類の内容は多くの場合，攻撃者にとっても有益な情報となるため，転送にあたっては，認証技術によって送受信双方の真正性を確認するとともに．暗号化技術によって十分な秘匿性を確保して転送することが求められる．

4.5　組織体制

ここでは，提案した SNS 会員資格制度を実現する組織とその役割（機能）を考察する．組織体制は管理組織と実行支援組織に分けられる．

4.5.1　管理組織

提案制度を SNS 単位で適用すると想定し，SNS における管理体制を検討する．自動車運転免許証や車検証は警察署が発行・管理しているのに対して，SNS 会員証やセキュリティ検査証明書を発行・管理する主管は SNS プロバイダということになろう．また，ユーザや接続使用機器等の登録・管理は管理組織が関連データベースを連携して実施することになる．

以上から，SNS プロバイダの管理組織としての業務は以下のとおりとなる．すなわち，

SNS サービスプロバイダは，加入ユーザからの利用要求があった時，受付ゲートウェイにおいて，SNS 会員証，セキュリティ検査証明書，およびアクセス査証に基づいて，利用の適格性を検査・判断し，送受信情報の通過／拒否を実施する．また，この結果をユーザ毎に管理する．なお，他の SNS にもセキュリティ検査証が発行・管理される．管理組織と役割の例を表 4.4 に示す．

表 4.4　管理組織と役割の例

管理組織	役割
SNS サービスプロバイダ	SNS 会員証発行
サイバー警察署	セキュリティ検査証明書を発行・管理
地方自治体，総務省，経済産業省	情報通信機器を登録・管理，LAN/AS を登録・管理
外務省，防衛省，公安調査庁等	犯罪の種類に応じて

4.5.2　実行支援組織

SNS 会員証やセキュリティ検査証明書の発行管理や事件発生後の調査等のアクションは，SNS プロバイダが主管になると考えられるが，日常のセキュリティ検査やその結果に基づく SNS 運用は多くの民間組織が実行支援することになろう．以下，この民間組織を 4 つ（①～④）に分類し，各組織の役割分担を示す．

①情報通信機器ベンダ

ユーザとユーザのコンピュータやルータ等ハードウェア利用状況を管理（以下，ユーザ管理と呼ぶ）する．

②OS・アプリケーションソフトベンダ

OS およびアプリケーションソフトのユーザの利用状況を管理するとともに，発見された脆弱性や危険性に関する情報を登録管理する．

③セキュリティ対策ソフトベンダ

セキュリティ対策ソフトのユーザの利用状況を管理する．また，日々の検査結果を管理する．

④セキュリティ検査サービスプロバイダ

脆弱性検査サービス，検疫サービスを実施し，検査結果を管理する．

なお，上述した組織はすでに存在しているものばかりであり，提案制度適用に必要な関連情報（例．OS・アプリケーションソフト登録情報，セキュリティ検査結果）も実際に個々に管理されている場合が多い．しかし，データは組織毎独立に管理され，連携して利用されいないのが実態である．提案制度に用いる各種情報には，個人情報や機密情報に相当するものが多いが，提案制度を確立するには，適用規則を公開し，関連組織が協調してデータ管理する必要がある．実行支援組織と役割の例を表 4.5 に示す．

表 4.5　実行支援組織と役割の例

実行支援組織	役割
情報通信機器ベンダ	ユーザとユーザのコンピュータやルータ等ハードウェア利用状況を管理
OS・アプリケーションソフトベンダ	OS およびアプリケーションソフトのユーザ毎の管理，発見された脆弱性や危険性に関する情報を登録管理
セキュリティ対策ソフトベンダ	セキュリティ対策ソフトのユーザ毎の管理，日々の検査結果を管理．
セキュリティ検査サービスプロバイダ	脆弱性検査サービス，検疫サービスの検査結果管理

4.5.3　実現イメージ

提案した SNS 会員資格制度の実現システムのイメージを示す．一例として，ある SNS サービスに加入している個人ユーザが，自身が作成したコンテンツを商用サーバにアップロードし，公開しようとしているケースについて示す（図 4.1）． なお，前節で示した管理組織および実行支援組織の機能が SNS 内で実現される．また，本制度に係る種々の情報がデータベース化されディレクトリサービスにより提供されるものとする．なお，認証・暗号機能については省略して説明する．

図 4.1 において，まず個人ユーザは自身の SNS 会員証を管理機能を通じて取得するとともに，自身が所持・使用する情報通信機器を実行支援機能を通じて登録する．次に，セキュリティ検査を受けてセキュリティ検査証明書を取得する．また，公開サーバより予めアクセス査証を得ておくものとする．これらの証明書類はディレクトリサービス（データベース）に登録・保管されており，個人ユーザの利用履歴も同じくデータベースに保管される．これらのデータは必要に応じて更新される．個人ユーザが公開サーバによるサービスをうける場合，呼設定の過程において，SNS 会員証，セキュリティ検査証明書，アクセス査証が SNS の端に設置された受付ゲートウエイに送信される．受付ゲートウェィはこれらの免許・証明書情報を検証して SNS 利用可否の判断を行う．利用可の場合は接続が許可され，個人ユーザの IP パケットには検証済みの情報を記して公開サーバに転送する．利用不可と判断された場合，すなわち，個人ユーザがサイバー犯罪履歴が持つため SNS 利用が許可されていない，使用するアプリケーションプログラムでサービス不能攻撃する可能性がある，年齢制限などにより公開サーバ利用条件を満たしていない，などと判断された場合，接続が許可されない．

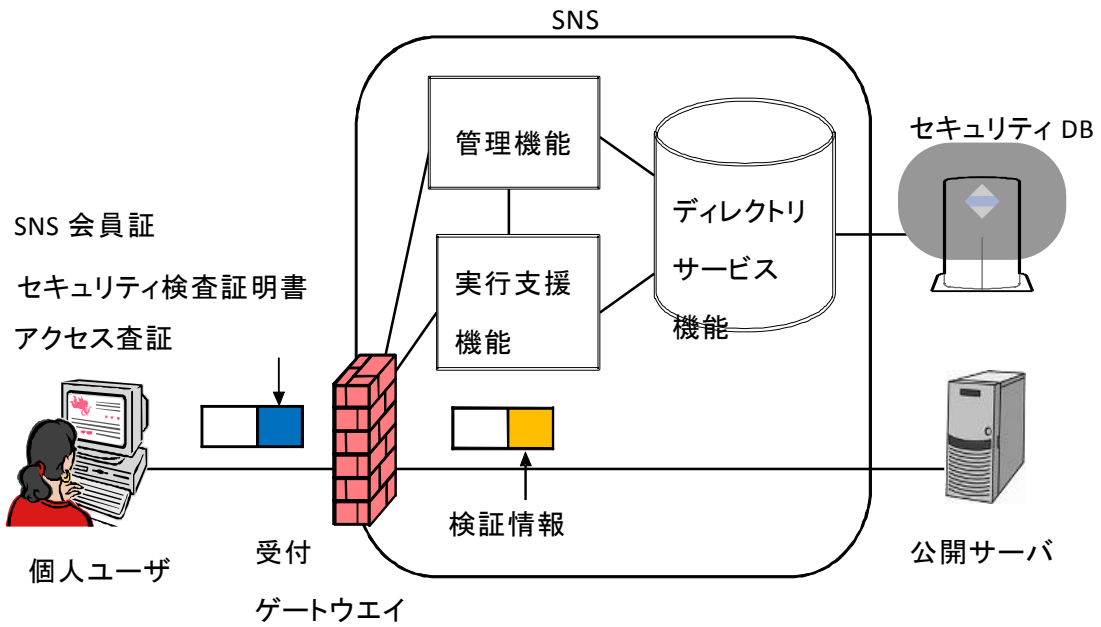


図 4.1　SNS 会員資格制度の実現イメージ

4.6 考察

提案したSNS会員資格制度が導入された場合の効果を以下の①から③にまとめて記す.

①ユーザのセキュリティ対策負担の軽減

現在，セキュリティ対策は主にユーザが個々に負担している．本制度導入により，セキュリティ対策の主体がSNSに代わると,悪意のある情報がユーザに到達しにくくなるため,ユーザ負担が大幅に軽減する．SNS 側の負担は従来より増加するが対策機能が集約されるため全体的としての負担は低減する.

②SNS資源の有効利用

受付ゲートウエイにおいて，送信者側の攻撃性をチェックするため，迷惑メールやマルウェアといった有害情報のSNS流入を防ぐことができる．このため，SNSの利用帯域その他の資源がより有効に活用される.

③セキュリティ事件・事故の減少

本提案制度は属人的側面と技術的側面を合わせ持っているため，ボットネットによる組織的な犯罪や機密情報の漏洩拡散，といった事件・事件の防止に役立つ．さらに，利用ユーザ間のセキュリティポリシーが統一化され向上する，あるいは，犯罪捜査機関との連携が円滑化される，といった効果が期待できる.

一方，導入にあたって検討すべき課題として，以下の④，⑤がある.

④利便性とセキュリティのバランス

提案制度が導入された場合にユーザの利便性が現状より低下するのは避けられない．セキュリティと利便性をどうバランスさせるのが望ましいか，あるいは止揚策があるのか国民的な議論が必要である.

⑤制度及び社会的コンセンサス

導入にあたっては，電気通信事業法[16]で定めている，検閲の禁止，秘密の保護，利用の公平，と提案制度との整合性について検討する必要がある．このような法制度面からみた検討の他，ユーザ，管理組織，実行支援組織を交えた議論による社会的コンセンサスの

醸成が必須となる．

ここで，検閲の禁止，秘密の保護，利用の公平とは，以下のⅰからⅲである．

ⅰ．検閲の禁止

第三条　電気通信事業者の取扱中に係る通信は，検閲してはならない．

ⅱ．通信の秘密

第四条１　電気通信事業者の取扱中に係る通信の秘密は，侵してはならない．

ⅲ．利用の公平

第七条　電気通信事業者は，電気通信役務の提供について，不当な差別的取扱いをしてはならない

4.7　まとめ

本章では，情報セキュリティデータベースを用いた SNS 会員資格制度の提案を行った．SNS の情報セキュリティを確保するには，セキュリティデータベースを用いた SNS 会員資格制度の創設が必要になるというと仮説のもと，SNS 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，セキュリティデータベースに基づく会員資格方式を導入することによって，セキュアな SNS 環境が実現できることを示した．具体的には，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，セキュリティデータベースに基づく 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，提案制度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提案制度の実現性，利点と課題を考察した．今後，本提案の実現にむけ関係諸氏との議論を進めていく．

第 5 章　フィージビリティ（実現性）について

第 5 章では,NGN[30][31]に関して,ある通信事業会社トライアルネットワーク(図 5.1),および，エッジルータ・サービスエッジ[32]（図 5.2）の概要，を用いて，前章までの提案のフィージビリティについて考察する．ここで，サービスエッジとは，アクセス回線を直接収容し，QoS などの NGN 特有の機能を提供する要となるネットワーク機器である．このサービスエッジと，基本的に電気通信業者の各収容局に設置される．

以降，(a) 技術的実現性，(b) 拡張性，(c)導入コストという観点から第 2 章から第 4 章までの提案した方式及び社会制度提言の実現性を考察する．

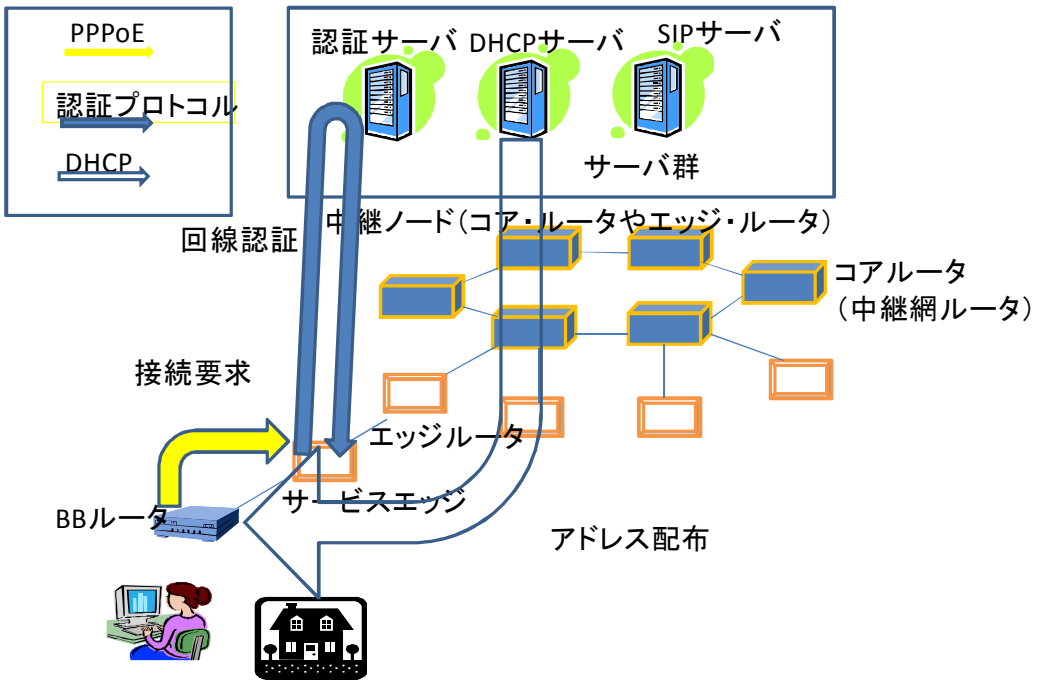


図 5.1　ある通信事業会社の NGN トライアルネットワーク

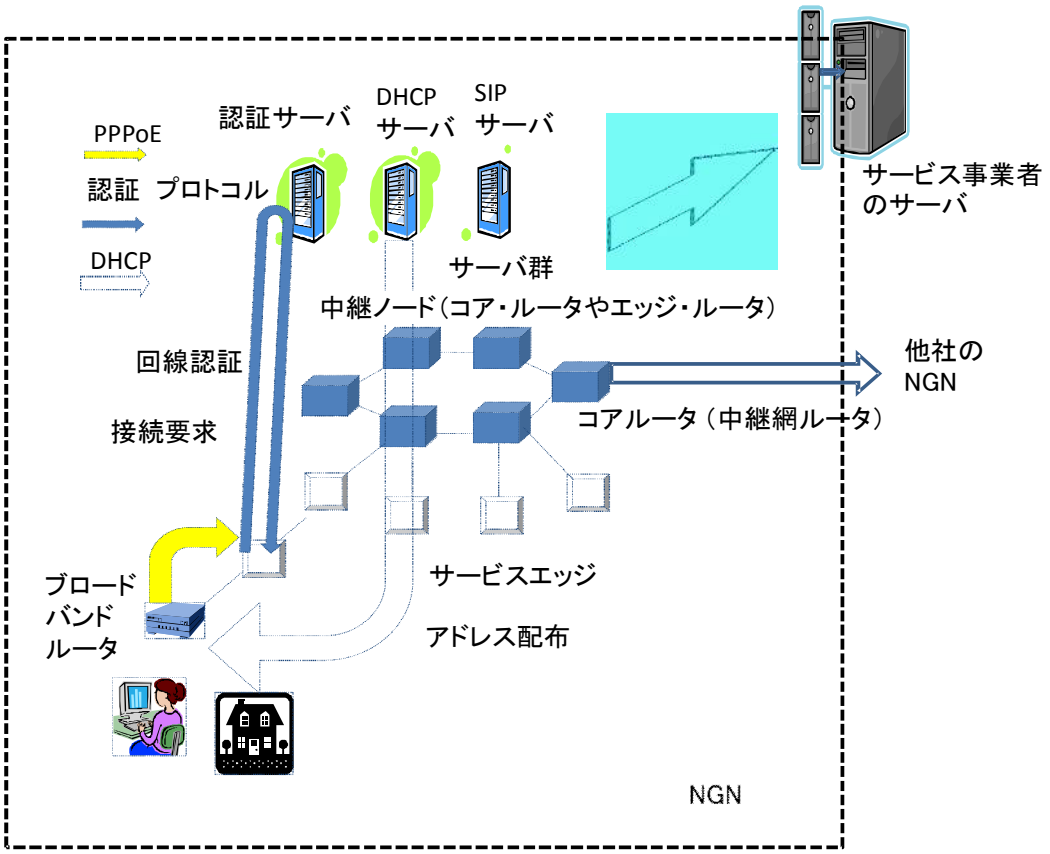


図 5.2　NGN のエッジルータ・サービスエッジの概要（図 3.3 再掲）

5.1　私的セキュリティポリシーを用いたトラヒック制御法

(a)技術的実現性

私的セキュリティポリシーを用いたトラヒック制御法における機能と実現可能性は，第 2 章を引用すると以下の①～⑤のようになる．

① SIP 等による制御信号（図 2.6 の C1）を用いて，ユーザが定めた 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 ER に伝える機能

［実現可能性］：SIP サーバは SIP と呼ばれるプロトコルを利用して，電話番号を IP アド

レスと対応付けたり，相手を呼び出してつなぐといった呼制御（電話回線や端末の接続や解放，監視などの制御）を実施する．インターネットのような，電話網以外のネットワークにおいても，音声通信を中心としたコネクション型通信を行う場合は，電話ネットワークと同等の呼制御手続きをすることが多い．なお，電話網では，呼制御のために設けられた専用の共通線信号網を利用する．

一方，TCP/IP を用いるネットワークにおいて IP 電話サービスを提供する場合，呼制御プロトコルとして H.323 や SIP などを利用することが多い．これらのプロトコルは従来より，IP 電話サービス（IP 電話サービスは，広い意味では電話網の一部もしくは全てに VoIP 技術を利用する電話サービスである．音声のみのものが多いが，動画も利用できるテレビ電話サービスなども可能である）に広く適用されてきた実績があり，NGN においても利用されている．

IP 電話サービスを提供する場合は，優先転送制御あるいは帯域制御（帯域制御とは，ユーザが利用する帯域を確保する目的で，コンピュータネットワークにおいてネットワークトラヒックやパケットの測定・制御を行うことである）といった品質制御に関わる技術が必須となる．NGN はこの品質制御技術がインターネットに比べて比較的充実している．品質制御を実施するにはルータ間で帯域情報を交換する，制御のタイミングを指示する，課金・認証情報を外部サーバに提供する，といった制御情報の転送機能を備えていることが求められる．NGN などで使用されている SIP は，このような制御情報の転送に適したプロトコルである．したがって，①の機能を達成するには，ユーザ(端末機器)と UNI の ER(UER)の間でやりとりされる SIP に同機能を追加することで実現可能である．

② UNI の ER(UER)が自身に UDP フラッド検出ポリシーを設定する機能

［実現可能性］: UDP フラッド検出ポリシー設定は，ネットワーク側から流入する UDP パケット数の閾値を UNI の ER(UER)に設定することと等価であり，容易に実現可能である．

③ NGN において，制御信号(図 2.6 の C2) を用いて，トラヒック制御の実施ポリシーを UNI の ER(UER)から NNI の ER (NER) に伝える機能

［実現可能性］: NGN 内では，前述のように，全てのルータや接続インタフェースが SIP に

よる制御情報の転送をサポートしている．このため，SIP を用いて，制御信号（C2）を UNI の ER(UER)から CR を経由して NNI の ER（NER）に伝えることができる．

④　UNI の ER(UER)で UDP フラッドの検出機能

[実現可能性]：UNI の ER(UER)で一番低い階層のルータは，「サービス・エッジ(図 5.2 参照)」と呼ばれてアクセス回線を直接収容している．サービス・エッジは，QoS などの NGN 特有の機能を提供する要となるネットワーク機器である．基本的には，NTT の各収容局に設置される．UNI の ER(UER)と連携したサービスエッジで，ネットワーク側から流入する UDP パケット数を単位時間（例．秒）ごとに測定し，その値が前述の閾値を超えたとき，フラグを上げることで UDP フラッドの検出が可能となる．

⑤　制御信号(図 2.6 の C3)により，UNI の ER(UER)における UDP フラッド検出結果を NNI の ER（NER）にリアルタイムに伝え，先に設定された私的セキュリティポリシーに基づき UDP トラヒックを制御する機能．

[実現可能性]：③と同様に，SIP を用いて，制御信号（C3）を UNI の ER(UER)から CR を経由して NNI の ER（NER）に伝えることにより，NNI の ER（NER）で UDP トラヒックを制御することが可能である．

(b)拡張性

図 5.2 のサービス･エッジは各都道府県市町村の旧電話局に全て設置される．このため，本提案を利用するユーザが増加しても，各サービス・エッジで吸収可能と考えられる．昨今は高性能のエッジルータ（図 5.1 の中央下付近）も続々導入されている[33][34][35]．このため，ユーザ増加にも各都道府県市町村レベルで容易に対応できる．

(c) 導入コスト

導入に必要な主なコストは，災害時の電話等の発信規制機能と同様なレベルの機能を開発するためのコストと考えられる．開発し導入するかどうかは，本提案により DoS 攻撃防御するのに必要なネットワークリソースと本サービスを利用するユーザ課金で得られる

収入見込み額とのトレードオフで判断できる.

すなわち，導入コストに関わるパラメータとして以下の A，B，C，D の諸量を用いて，

A＝[主な開発コスト]＝ER（サービス・エッジを含む）[追加機能開発費用]＋CR[追加機能開発費用]＋SIP[サーバ開発機能]

B＝[主な運用・保守コスト]＝ER[運用・保守コスト]＋CR[運用・保守コスト]＋SIP[運用・保守コスト]

C＝[本提案によるネットワークリソース効率化費用]

D＝[本提案による収入見込み額]

とすると，

A+B＜C+D　を満たす場合,本提案を導入するものと推定される.

なお，上述の発信規制とは，輻輳発生時にシステムダウンを防止するため通信トラヒックをコントロール（通信規制）する機能である．発信規制には自動規制と人為的に行う手動規制がある.

5.2　公的セキュリティポリシーを用いたトラヒック制御法

(a) 技術的実現性

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おける機能と実現可能性は，第 3 章を引用すると以下の①～⑥のようになる.

① NGN 事業者が図 3.1 の UNI の ER（UER）と，UNI と NNI の中間に位置する CR に公的セキュリティポリシーを設定する機能：

[実現可能性]：私的セキュリティポリシーの設定と同様に SIP を用いることによって，容易に UER と CR に公的セキュリティポリシー設定することが可能である.

② 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 3.1 の SNI（application Server-Network Interface）を介し，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，必要に応じて測定する．

[実現可能性]:ユーザのセキュリティレベル情報を SNI を仲介して入手する機能を開発し，VAS に導入することで可能である．

③　VAS が SNI を介して SIP 等による制御信号（図 3.1 の C4）を用いてユーザ毎のセキュリティレベル情報を UNI の ER へ伝送する機能

［実現可能性］: 同様に SIP を用いることによって容易に実現可能である．

④　UNI の ER（UER）で端末認証（NGN の場合は端末とアクセス回線を識別情報をもとにした回線認証）を実施して，ユーザの真正性を確認し，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を記載して CR に転送する機能．

［実現可能性］: UER は通常の NGN での端末認証（図 3.3 の NGN 回線認証）を実施して，ユーザの真正性を確認している．この確認過程のあと，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を記述し，CR に転送する機能を追加することで実現可能となる．

⑤　また，脆弱性評価サーバは制御信号（図 3.1 の C5）を用いて，Diffserv 実施のための PHB（Per Hop Behavior）を CR に設定する機能．なお，この PHB は IP ヘッダに記載された DSCP（Differentiated Service Code Point）値に基づく Diffserv 動作仕様である．

［実現可能性］: PHB を CR に設定する機能を追加することで実現される．この場合，PHB はセキュリティレベル情報で優先転送動作する仕様となる．

なお，PHB に DSCP 値を IP ヘッダに設定する方法は以下の通りである．

[PHB に DSCP 値を IP ヘッダに設定する方法]

PHB ごとに使用する DSCP 値が IETF で標準化している．PHB と対応する DSCP 値として，標準化された 次の 4 種類の IP 優先度（IP precedence）を使用する．

(1)Expedited Forwarding PHB (EF) - 端点間の帯域保証をおこなう仮想専用線サービスのための PHB である. Diffserv ネットワークのエッジルータにおいて契約分のみのトラヒックを通過させ, コアルータにおいては契約分の総和を上回る帯域を確保する (オーバープロビジョンする). コアルータでは, 優先キューイングを用いてトラヒックを制御する. EF においては 1 個だけの DSCP を使用する.

(2)Assured Forwarding PHBs (AF) - EF よりゆるい保証サービス, すなわち最低帯域保証つきのベストエフォート・サービスのための PHB である. Diffserv ネットワークのエッジルータにおいて契約分をこえたトラヒックに属するパケットにマークをつけ, コアルータが混雑した場合にはマークがついたパケットを優先的に破棄する. AF のためには AF1 ～ AF4 という 4 つのクラスが標準化されているが, 各 AF クラスは 3 個の DSCP を使用する. したがって, DSCP の値としては AF11 ～ AF43 という 12 個が使用される.

(3)Default Forwarding PHB (DF) - 最小限の資源を割り当てる条件があることを除いて, ベストエフォートを意味する. Best Effort PHB (BE) と呼ばれることもある. DF のための DSCP は 0 (だけ) である.

(4)Class Selecor PHB (CS) - Cisco が実装している IP 優先度 (IP precedence) を使用する QoS 保証法と互換性のある PHB である. CS のためには 8 個の DSCP が割り当てられている.

ここでなお, IP ヘッダの Diffserv フィールドの上位 6 ビットは DSCP (Differentiated Service Code Point) 値転送用として使用される.

⑥ 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が UNI の ER (UER) および CR によりトラヒック制御する機能.

[実現可能性]: 上記の①～⑤を用いた公的セキュリティポリシーの運用により, ⑥は実施可能である.

(b) 拡張性

5.1 の議論と同様に, 機能の追加やユーザの増加に関しては, すべて図 5.1 のサービス・エッジ (旧電話局にある) で吸収可能であり, 高性能のエッジルータ (図 5.1 の中央下付近) も続々と導入されているため, 容易に対応できると推察される.

(c)導入コスト

導入に必要な主なコストは，災害時の電話等の発信規制機能と同様なレベルの機能を開発するためのコストと考えられる．開発し導入するかどうかは，導入コストと本提案によるネットワークリソース効率化費用とのトレードオフで判断できる．

すなわち，導入コストに関わるパラメータとして以下の A，B，C の諸量を用いて，

A＝[主な開発コスト]＝ER（サービス・エッジを含む）[追加機能開発費用]＋CR[追加機能開発費用]＋SIP[サーバ開発機能]

B＝[主な運用・保守コスト]＝ER[運用・保守コスト]＋CR[運用・保守コスト]＋SIP[運用・保守コスト]

C＝[本提案によるネットワークリソース効率化費用]

とすると，

A+B＜C を満たす場合,本提案を導入するものと推定される．

5.3　情報セキュリティ DB を用いた SNS 会員資格制度提言

情報セキュリティ DB を用いた SNS 会員資格制度について，技術的にはすべて既存技術の組み合わせであり，(a) 技術的実現性については問題がないと考えられる．(b) 拡張性や(c)導入コストについては，SNS の規模に左右される．Twitter のような世界規模のパブリック SNS では，比較的大容量の DB が必要となり，導入コストも大きくならざるを得ない．ただし，今日では，クラウド技術の適用により，世界的規模の DB を構築・運用するのは従来に比べ困難でなくなっており,社会のコンセンサス（利用ユーザや SNS のスポンサーの同意）が得られ，かつ組織体制ができれば (b) 拡張性や(c)導入コストにおいても問題は少ないと推察される．

5.4　まとめ

第 5 章では，第 2 章の私的セキュリティポリシーに基づくトラヒック制御法，第 3 章の公的セキュリティポリシーを用いたトラヒック制御法，第 4 章の情報セキュリティ DB を用いた SNS 会員資格制度提言に関して，技術的実現性，拡張性，導入コストの観点からフィージビリティ（実現性）について考察した．3 つの提案について総括すると以下のよう

になる．

いずれの提案も技術的には，既存技術の延長，あるいは，比較的軽微な機能追加で実現できるという見通しを得た．

拡張性について，私的セキュリティポリシーに基づくトラヒック制御法はユーザ数に応じて規模が大きくなりかつ個別の機能設定が必要になるため，他の 2 提案に比べて不利と考えられる．しかし，利用ユーザ間の調整や社会的コンセンサスが不要であるという点からすると導入の実現性は高いように考えられる．一方，公的セキュリティポリシーを用いたトラヒック制御法，および，SNS 会員資格制度については，ユーザ数に応じて関連 DB は大きくなるものの，機能面においてはユーザの独自性がないことから，拡張性は高いと考えられる．

導入コストについて，私的セキュリティポリシーに基づくトラヒック制御法については，それを負担する利用ユーザの個々の評価に依存する．一方，公的セキュリティポリシーを用いたトラヒック制御法，および SNS 会員資格制度については，通信事業者，SNS プロバイダ，および全ユーザが負担を分かち合うことから，三者によるコンセンサスの成否に依存する．

第 6 章　結論

インターネットのような情報通信網や SNS へも一定のセキュリティ機能を持たせ，ユーザ側のセキュリティ機能と協調した上で，安心して利用することができる安全な網環境の構築を実現するために，以下の 3 つを提案し，最後にフィージビリティ（実現性）について考察した．

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

本文では 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，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．

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

本文では 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，SNI からユーザの公衆ネットワーク利用環境に関する脆弱性検査を行い，設定された公的セキュリティポリシーに従って，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．

なお，本文では，私的セキュリティポリシーを用いたトラヒック制御法，およ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について，現状トラヒック制御機能を備える NGN に適用して検討した．今後，OpenFlow[36]などトラヒックをソフトウエアで制御する SDN（Software Defined Network/Networking）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．

3.　情報セキュリティ DB を用いた SNS 会員資格制度

本文では，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．具体的には，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，提案制度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提案制度の実現性，利点と課題を考察した．

最後に，提案した，私的セキュリティポリシーに基づくトラヒック制御法，公的セキュリティポリシーを用いたトラヒック制御法，情報セキュリティ DB を用いた SNS 会員資格制度に関して，技術的実現性，拡張性，導入コストの観点からフィージビリティ（実現性）について考察した．

その結果，概ね，いずれの提案も技術的には，既存技術の延長，あるいは，既存のネットワークやシステムへの比較的軽微な機能追加で実現できるという見通しを得た．

また，私的セキュリティポリシーに基づくトラヒック制御法については，個別の機能設定が必要になるため，拡張性が他の 2 提案に比べて不利と考えられることがわかった．また，本提案はユーザが個別に選択するサービスとして提供されるため，導入コストは市場性と合わせて検討する必要があることがわかった．

一方，公的セキュリティポリシーを用いたトラヒック制御法および SNS 会員資格制度については，ユーザごとに独自に追加する機能がないため，拡張性については比較的優れていることがわかった．しかし，導入コストについては，通信事業者，SNS プロバイダ，ユーザ間で分担することになるため，コンセンサスが得られるかどうかがポイントとなることがわかった．

今後，以上の提案の実現にむけ関係諸氏との議論を進めていく．

謝辞

終始熱心なご指導を頂いた佐藤直教授に感謝の意を表します．また発表内容に関して，貴重なコメントを頂戴いたした田中学長，小柳教授，及びに土井教授に深謝いたします．また佐藤ゼミの研究室のメンバーには常に刺激的な議論を頂き，精神的にも支えられました．多くの方々のご協力を頂き，多くの刺激と示唆を得ることができました．感謝の念にたえません．本当にありがとうございました．

付録

本文の検討に参考となる内容を以下の付録 1 から付録 4 に記載する.

1. NGN 概要及びセキュリティ関連機能と標準化動向
2. CVSS 算出方法
3. SNS におけるセキュリティやプライバシー問題
4. OpenFlow などトラヒックをソフトウエアで制御する SDN

付録１. NGN 概要及びセキュリティ関連機能と標準化動向

NGN 概要及びセキュリティ関連機能と標準化動向を JPNIC の調査[37]に基づき以下に示す.

[NGN 概要]

ITU-T や ETSI(欧州電気通信標準化機構)では NGN(Next Generation Network)の標準化作業が 2000 年代前半に活発に行われた. NGN とは, QoS やセキュリティを向上させた統合 IP 網を構築し, 電話網を代替できる次世代の通信インフラとしてその上でサードパーティが多様なサービスを展開できるようにし, ユビキタスネットワーク社会の実現を目指そうというものである. NGN は網内に QoS 制御や認証を行う機能モジュールを備え, 3GPP (Third Generation Partnership Project) が開発した IMS(IP Multimedia Subsystem)という SIP サーバ群を用いてセッション制御を行う.

1.1 NGN が目指すもの

NGN とは, IP 技術を用いて電話網を構築し直すことにより, 電話網の安心感や簡便さを保ちつつ, 電話やテレビ会議, ストリーミングなど多様なサービスを柔軟に提供できる統合 IP 網を提供する技術である. 回線交換技術を使う電話網が将来廃棄された時, 替わって社会インフラとなる通信網を提供する.

NGN は, 信頼性や安心感の欠如が指摘される現在のインターネットに対する, 電話網からの回答であるとみなせる. 社会インフラとして各種サービスの基盤となる通信網は今後,

IP 技術を用いて提供されるべき事は明らかである．しかし，現在の IP 網では QoS の保証や通信相手の認証などが十分に行われているとは言い難く，その結果としてテレビ会議システムが必ずしも正常に動作しなかったり，スパムやウイルスが蔓延して絶え間ないパッチ当てが必要となったりしている．これでは自覚ある先進ユーザにしか使えない．社会インフラには，医療システムなど生命がかかった通信を任せられる信頼性，お年寄りや子供でも不安を覚えずに使える安心感が必要である．インターネット発展の原動力である多様なアプリケーションを生み出す力，新規業者の参入を容易にするオープン・インターフェースの提供，ユーザの平等な取り扱い，等々を損なうことなく提供し，それらを通じてユビキタス・ネットワーク社会を実現することが NGN のゴールとなる．

この実現のため，ITU-T の Y.2001 勧告では NGN が備えるべき様々な特徴を規定した．重要なものとしてはまず，エンドツーエンド QoS 保証の提供が挙げられる．NGN では多様なアクセス網(xDSL や WiFi，携帯電話など)や端末(電話機や PC，情報家電など)，多様なアプリケーションが使われる．この環境下で端末と網とが QoS をネゴシエーションし，上位アプリケーションに提供できる必要がある．

次がモビリティのサポートである．一台の PC を携帯して家庭内では xDSL，外出先では WiFi，オフィスでは FTTH と様々なアクセス網経由で通信したり，オフィス内の移動や出張などにより多数の PC から通信したりしてもサービスが受けられることが求められる．この他に，後述する網の転送機能と制御機能の分離，多様なアクセス網のサポート，固定網と移動網の融合，緊急通信や合法的盗聴などの規制への適合などが規定される．

1.2　標準化体制

NGN の標準化は,電話網の標準化に大きな役割を果たしてきた前記 ITU-T をはじめ,ETSI などで検討が進められた．

ITU-T の NGN 標準化では，他の標準化機関との連携が重視されている．NGN の重要な構成要素である IMS は第 3 世代携帯電話の標準化団体である 3GPP が開発したものであり，そこで使われる SIP 他のプロトコルの多くは IETF で開発されたものである．これら他の機関で開発された標準は可能な限り再利用し，変更や拡張が必要な場合はその機関へ要望を出すことで実現する．IETF との連携は特に重要であり，2005 年 5 月には NGN をテーマとした初の合同ワークショップが開催され，意識合わせが行われた．

ITU や ETSI での標準化の特徴として，最初に目的や要求条件を定め，次に必要となる機能ブロックを規定し，最後にプロトコルを決めることが挙げられる．このため，NGN の標準化ではプロトコルのみならず，提供するサービスや機能アーキテクチャも規定されることとなる．また NGN は巨大システムであり，現行の電話網からの移行方法も重要な検討対象とされる．ネットワークの相互接続には必ずしも必要ではないが，プロトコルの利用方法まで規定することで意識合わせができ，相互接続が容易となっている．

1.3　提供するサービス

ITU-T では，NGN が提供するサービスを以下の６種類に分類して例示している．これら全てが提供されるとは限らず，またこれら以外のサービスも将来的には通信事業者自身やサードパーティにより提供されることが期待されている．

(1) PSTN/ISDN エミュレーション

従来の電話網との互換サービスである．ユーザは NGN への切り替えを意識せず，従来の電話機もそのまま利用できる．

(2) PSTN/ISDN シミュレーション

同じく電話サービスであるが，電話機とのインターフェースは IP とし，従来の電話機はアダプタを介して接続する．後方互換性よりも将来への拡張性や作りやすさを重視する．

(3) マルチメディアサービス

IP 網ならではのサービスである．公衆網と接続可能な音声通話，PTT (Push To Talk)，SMS 等の各種メッセージング，テレビ電話やゲーム，e ラーニングなどの一対一・多人数マルチメディア通信，プレゼンス，位置情報を使ったガイド等のサービス，などが提供される．またテレビ放送も実現されている．

(4)インターネットアクセス

インターネットへの接続も NGN を介して可能である．

(5) その他

VPN，ファイル転送等のデータサービス，センサー・ネットワーク，ユーザの機器の管理を代行する Over The Network (OTN)デバイス管理，などが挙げられる．

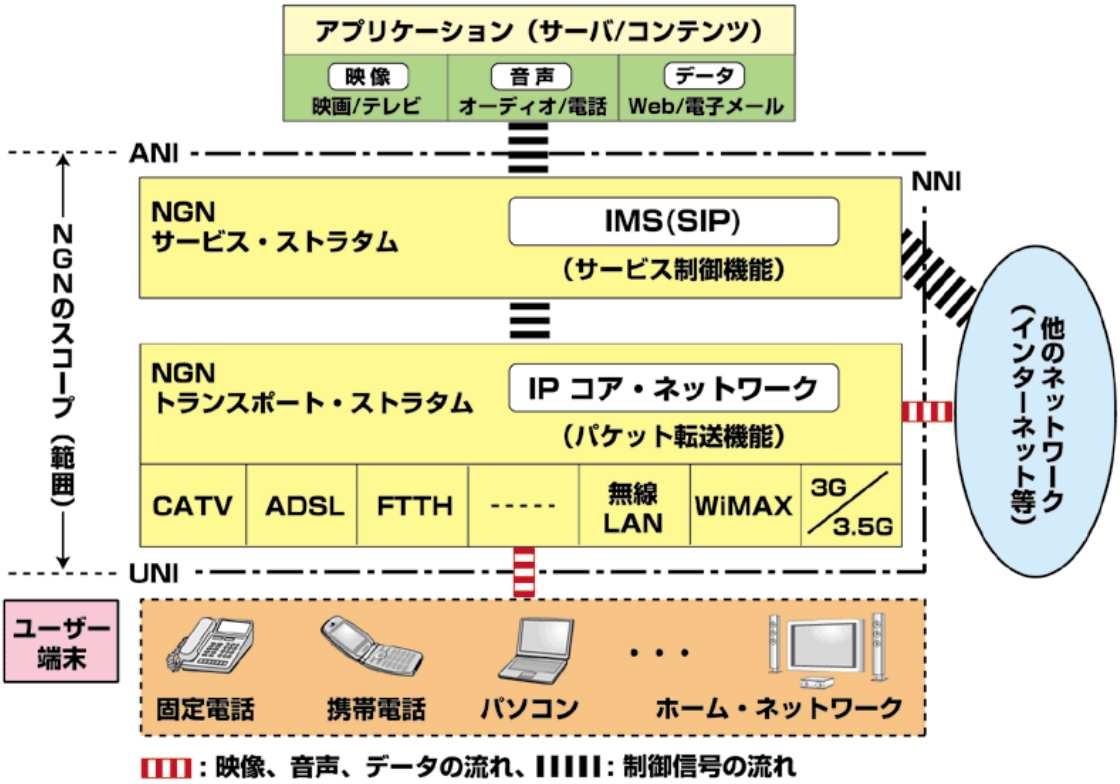
(6) 公衆サービス

110 番などの緊急通信，警察による合法的盗聴，身障者への対応，サービス・プロバイダーの選択，プライバシーの保護，悪意あるユーザの追跡など，社会インフラならではの

サービスである．こうしたサービスは国毎に法規制が異なるため，それらへの適合が重要である．

1.4　機能アーキテクチャ

こうした多様なサービスを実現するため，NGN では様々な機能ブロックを規定し，それらをオープンなインターフェースで結ぶアーキテクチャをとる．その概要を付図 1 に示す．



付図 1　NGN の機能アーキテクチャ[37]

本アーキテクチャは，大別してエンドユーザ機能(端末やカスタマ網)，音声や画像，データなどのユーザのデータを実際に転送するトランスポート・ストラタム，それを制御するサービス・ストラタム，それらを管理する管理機能，サービス・ストラタム上でサードパーティから提供される各種のアプリケーション，および他の網（PSTN/ISDN 網，NGN 網，インターネットなど)から構成される．なお，これ上図は機能を示した図であって物理的な機器とは必ずしも一致しない．

トランスポート・ストラタムは，実際のパケット転送機能を担うトランスポート機能と，認証や IP アドレス払い出し等，ある端末をその網に接続する際の一連の処理を行うネットワーク・アタッチメント制御機能，QoS 保証のための受付制御を行う網リソース制御機能，そのためのユーザプロファイル・データベースで構成され，QoS が制御されたパケット転送網を提供する．

サービス・ストラタムは，コネクションの設定や帯域を管理する SIP サーバ群であるサービス制御機能と，Web との連携や付加価値サービスを実現するアプリケーション/サービス機能，およびユーザプロファイル・データベースから構成される．

エンドユーザ機能では，認証のため，全端末に SIM カード相当の機能を持たせることが検討されている．網管理機能は，電話網の管理に使われてきた Telecommunications Management Networks (TMN) の枠組みを利用する．

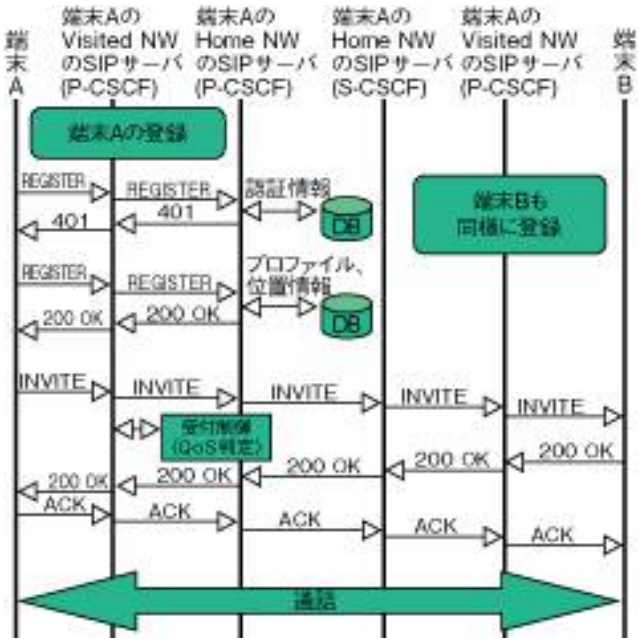
本アーキテクチャを特徴づける，転送機能を担うトランスポート・ストラタムと，その制御を担うサービス・ストラタムの分離は，ルータにおいてフォワーディング機能とルーティング機能を分離し，その間にオープンなインターフェースを設けることに似ている．このような構成とするのは，新サービスを提供しやすくするためである．パケット転送機能はいかなるサービスでも必要なので「高品位テレビ会議で必要な帯域は 6Mbps」といったサービス毎に異なる必要があるサービス制御機能とは分離した．

このアーキテクチャの特徴として，網内に様々な機能を盛り込んだことが挙げられる．端末にインテリジェンスを持たせて網は簡素にするステューピッド・ネットワークとはしない．この構成を採るのは，一つには責任の所在を明らかにするためである．社会インフラの提供者は，サービス提供に失敗したら(例えば 119 番が繋がらず救急車の到着が遅れたり，遠隔医療の最中に QoS 劣化が起きて手術が失敗，患者が死亡した場合)社会的責任が問われる．責任が問われる以上「我々は最善を尽くす，あとは端末が努力する」という，他者に依存した構成は採用しにくいのである．次の理由は，ステューピッド・ネットワークでセキュリティを保つのは，現実には難しいことが挙げられる．ユーザに高度な知識があるならば，端末にインテリジェンスを持たせるのが最高のセキュリティ提供方法である．しかし，ソフトウェアを常に設定ミスせず最新に保つことが，近い将来小学生やお年寄りにできるようになるとは思えない，また「皆が信頼する誰か」ではセキュリティ機構構築は難しいのである．相互認証手続きは複雑化するし，悪意あるノードの混入防止も難しく，中継ノードが突然通信を妨害し始める，といった恐れも出てくる．そして最後の理由とし

て，ユーザは，あるサービスが賢い網，賢い端末いずれのアプローチで提供されているかなど気にしないことがあげられる．これらの理由により，NGN は(少なくとも中核的サービスに関しては)網に機能を持たせている．

1.5 SIP による呼制御

サービス制御機能は SIP サーバ群で構成され，SIP プロトコルを用いて端末のレジストレーションやセッションの設定を行う．この方法は 3GPP で開発されたものを使用しており，基本的な考え方は IETF SIP に従いるが，レジストレーションの方法などが異なる．付図 2 に端末の登録とセッション確立のフローの主要部を示す．端末 A，B は(海外出張等により)自分が契約していないプロバイダーのサービスエリアにいるものとする．



付図 2　端末の登録とセッション確立のフロー[37]

各端末は最初に，その網の Proxy Call Session Control Function(P-CSCF)と呼ばれる SIP サーバに登録要求を出する．この要求は P-CSCF から自分が契約している事業者の Serving CSCF(S-CSCF) と呼ばれる SIP サーバに転送され，認証情報の照合，ユーザ・プロファイルの引き出し，位置情報の登録などが行われることで登録が完了する．セッション確立要求も同様に，最初は P-CSCF に送られ，そこから関連する SIP サーバに転送され

ることで実現される．その際にはQoS制御のために十分なリソースがあることの確認がトランスポート・ストラタム内の網リソース制御機能に対して行われる．このように，常にP-CSCFを介して制御を行うのが，最初からホームのSIPサーバ(S-CSCF)に直接アクセスするIETFのSIPとの大きな違いである．またSIPプロトコルの違いとしては，途中経過を示すメッセージでもPSTNとの接続のため高信頼な転送が要求されること，解釈が義務づけられた拡張ヘッダが定義されていること，などがある．

P-CSCFを設けるの理由は，一つには，アクセス網を提供する移動先の事業者が自網に接続されている端末を管理するため，一つにはP-CSCF～端末間のメッセージは圧縮して拡張ヘッダも制限し，それをP-CSCFが通常のSIPに戻して網内を転送することにより，無線区間の帯域を節約し，またセキュリティを向上させるためである．

付録2.　CVSS算出方法

CVSS(Common Vulnerability Scoring System) 算出方法を共通脆弱性評価システムCVSS概説[38]に基づき記載する．

共通脆弱性評価システム CVSS は，情報システムの脆弱性に対するオープンで包括的，汎用的な評価手法の確立と普及を目指し，米国家インフラストラクチャ諮問委員会（ NIAC: National Infrastructure Advisory Council ）のプロジェクトで 2004年10月に原案が作成された．その後，CVSSの管理母体として FIRST(Forum of Incident Response and Security Teams)が選ばれ，FIRSTのCVSS-SIG(Special Interest Group)で適用推進や仕様改善が行われており，2005年6月にCVSS v1が，2007年6月にCVSS v2が公開された．CVSSは，現在，30を超える組織で採用されている．

日本のIPAもCVSS-SIGに参画しており，脆弱性対策情報データベース JVN iPedia や，脆弱性関連情報の調査結果のウェブサイトでCVSS v2基本値を公表している．(2007年8月20日にCVSS v1からCVSS v2へ移行した)．また，CVSS計算ソフトウェアの多国語版も提供している．

本文はFIRSTから2007年6月に公開されたCVSS v2の資料を基に作成している．詳細は，CVSS-SIGの「A Complete Guide to the CVSS Version 2.0」 を参照されたい．

2.1 概要

CVSS は，情報システムの脆弱性に対するオープンで汎用的な評価手法であり，ベンダーに依存しない共通の評価方法を提供している．CVSS を用いると，脆弱性の深刻度を同一の基準の下で定量的に比較できるようになる．また，ベンダー，セキュリティ専門家，管理者，ユーザ等の間で，脆弱性に関して共通の言葉で議論できるようになる．CVSS では次の 3 つの基準で脆弱性を評価する．

(1) 基本評価基準 (Base Metrics)

脆弱性そのものの特性を評価する基準である．情報システムに求められる 3 つのセキュリティ特性,「機密性 (Confidentiality Impact)」,「完全性(Integrity Impact)」,「可用性(Availability Impact)」に対する影響を，ネットワークから攻撃可能かどうかといった基準で評価し，CVSS 基本値(Base Score)を算出する．

この基準による評価結果は固定していて，時間の経過や利用環境の異なりによって変化しない． ベンダーや脆弱性を公表する組織などが，脆弱性の固有の深刻度を表すために評価する基準である．

(2) 現状評価基準 (Temporal Metrics)

脆弱性の現在の深刻度を評価する基準である．攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し，CVSS 現状値(Temporal Score)を算出する．この基準による評価結果は，脆弱性への対応状況に応じ，時間が経過すると変化する．

ベンダーや脆弱性を公表する組織などが，脆弱性の現状を表すために評価する基準である．

(3) 環境評価基準 (Environmental Metrics)

製品利用者の利用環境も含め，最終的な脆弱性の深刻度を評価する基準である．攻撃を受けた場合の二次的な被害の大きさや，組織での対象製品の使用状況といった基準で評価し， CVSS 環境値 (Environmental Score) を算出する．

この基準による評価結果は，脆弱性に対して想定される脅威に応じ，製品利用者毎に変化する．製品利用者が脆弱性への対応を決めるために評価する基準である．

2.2 脆弱性評価基準

2.2.1 基本評価基準 (Base Metrics)

AV ：攻撃元区分 (Access Vector)

脆弱性のあるシステムをどこから攻撃可能であるかを評価する．以下，AV に使用する諸量を■で示し内容を説明する（以下同様である)．

■ローカル

・対象システムを物理アクセスやローカル環境から攻撃する必要がある．

・例えば，IEEE 1394 ， USB 経由，ローカルアクセス権限で攻撃が必要など．

■隣接

・対象システムを隣接ネットワークから攻撃する必要がある．

・例えば，ローカル IP サブネット，ブルートゥース， IEEE 802.11 など．

■ネットワーク

・対象システムをネットワーク経由でリモートから攻撃可能である．

・例えば RPC バッファオーバーフロー攻撃など．

AC ：攻撃条件の複雑さ (Access Complexity)

脆弱性のあるシステムを攻撃する際に必要な条件の複雑さを評価する．

■高

・攻撃前に，権限昇格や偽装，疑われやすい方法での情報収集が必要である．

・対象システムが特定の設定の場合のみ攻撃可能である．

■中

・特定のグループのシステムやユーザに対してのみ攻撃可能である．

・攻撃前にいくつかの情報収集が必要である．

・攻撃するには，標準以外の設定になっている必要がある．

■低

・特別な攻撃条件を必要とせず，対象システムを常に攻撃可能である．

Au ：攻撃前の認証要否 (Authentication)

脆弱性を攻撃するために対象システムの認証が必要であるかどうかを評価する.

■複数

・攻撃する場合，2つ以上の認証（ログイン等）が必要である.

■単一

・攻撃前に認証（ログイン等）が必要である.

■不要

・攻撃前に認証（ログイン等）が不要である.

C ：機密性への影響 （情報漏えいの可能性， Confidentiality Impact）

脆弱性を攻撃された際に，対象システム内の機密情報が漏えいする可能性を評価する.

■なし

・システムの機密性に影響はない.

■部分的

・一部の機密情報が参照可能である

・一部の重要なシステムファイルが参照可能である.

■全面的

・メモリやファイルにある機密情報が全て参照可能である.

・重要なシステムファイルが全て参照可能である.

I ：完全性への影響 （情報改ざんの可能性， Integrity Impact）

脆弱性を攻撃された際に，対象システム内の情報が改ざんされる可能性を評価する.

■なし

・システムの完全性に影響はない.

■部分的

・一部の情報が改ざん可能である.

・一部のシステムファイルが改ざん可能である.

■全面的

・システム全体の情報が改ざん可能である.

・システム保護機能を全て回避し，情報が改ざん可能である.

A ：可用性への影響 （業務停止の可能性， Availability Impact）

脆弱性を攻撃された際に，対象システム内の業務が遅延・停止する可能性を評価する.

■なし

・システムの可用性に影響はない.

■部分的

・リソース（ネットワーク帯域，プロセッサ処理，ディスクスペースなど）を一部枯渇させることが可能である.

・業務の遅延や一時中断が可能である.

■全面的

・リソースを完全に枯渇させることが可能である.

・システムを完全に停止させることが可能である.

2.2.2 現状評価基準 (Temporal Metrics)

E ：攻撃される可能性 (Exploitability)

攻撃コード・攻撃手法が実際に利用可能であるかを評価する.

■未実証

・実証コードや攻撃コードが利用可能でない.

・攻撃手法が理論上のみで存在している.

■実証可能

・実証コードが存在している.

・完成度の低い攻撃コードが存在している.

■攻撃可能

・攻撃コードが存在し，ほとんどの状況で使用可能である.

■容易に攻撃可能

・攻撃コードがいかなる状況でも利用可能である

・攻撃コードを必要とせず，攻撃可能である.

■未評価

・この項目を評価しない.

RL ：利用可能な対策のレベル (Remediation Level)

脆弱性の対策がどの程度利用可能であるかを評価する.

■正式

・製品開発者からの正式対策が利用可能である.

■暫定

・製品開発者からの暫定対策が利用可能である.

■非公式

・製品開発者以外からの非公式な対策が利用可能である.

■なし

・利用可能な対策がない.

・対策を適用できない.

■未評価

・この項目を評価しない.

RC ：脆弱性情報の信頼性 (Report Confidence)

脆弱性に関する情報の信頼性を評価する.

■未確認

・未確認の情報が 1 件のみ存在している.

・いくつかの相反する情報が存在している.

■未確証

・セキュリティベンダーや調査団体から，複数の非公式情報が存在している.

■確認済

・製品開発者が脆弱性情報を確認している.

・脆弱性情報が実証コードや攻撃コードなどにより広範囲に確認されている.

■未評価

・この項目を評価しない.

2.2.3 環境評価基準 (Environmental Metrics)

CDP ：二次的被害の可能性 (Collateral Damage Potential)

対象システムが脆弱性を攻撃された場合の物理的な機器への被害や，生活基盤，身体などへ及ぼす二次的な被害の可能性を評価する.

■なし

・攻撃されても二次的な被害が発生しない.

■軽微

・攻撃が成功すると軽微な被害が発生する可能性がある.

■中程度

・攻撃が成功すると中程度の被害が発生する可能性がある.

■重大

・攻撃が成功すると重大な被害が発生する可能性がある.

■壊滅的

・攻撃が成功すると壊滅的な被害が発生する可能性がある.

■未評価

・この項目を評価しない.

TD ：影響を受ける対象システムの範囲 (Target Distribution)

利用環境の中で，脆弱性を攻撃される可能性のある対象システムを利用している範囲を評価する.

■なし

・対象システムが全く存在しない.

・対象システムが物理的に隔離されていて，利用環境へのリスクがない.

■小規模

・対象システムが存在するが，小程度の範囲で，利用環境の 1 ～25% にリスクがある.

■中規模

・対象システムが存在するが，中程度の範囲で，利用環境の 26 ～75% にリスクがある.

■大規模

・対象システムが広範囲に存在し，利用環境の 76～100% にリスクがある.

■未評価

・この項目を評価しない.

CR, IR, AR ：対象システムのセキュリティ要求度(Security Requirements)

対象システムが要求されるセキュリティ特性に関して，その該当項目（「機密性（C)」，「完全性（I)」，「可用性（A)」）を重視する場合，その該当項目を高く評価する．該当項目毎に，「機密性の要求度(Confidentiality Requirement, CR)」，「完全性の要求度(Integrity Requirement, IR)」，「可用性の要求度(Availability Requirement, AR)」を評価する．

■低

・対象システムの該当項目を失われても，一部の影響にとどまる．

■中

・対象システムの該当項目を失われると，深刻な影響がある．

■高

・対象システムの該当項目を失われると，壊滅的な影響がある．

■未評価

・この項目を評価しない

2.3. 値の算出方法と算出例

2.3.1 CVSS 基本値（Base Score）

影響度 = 10.41×（ 1 -（ 1 - C ）×（ 1 - I ）×（ 1 - A ））　…式(1)

攻撃容易性 = 20×AV×AC×Au　…式(2)

f(影響度) = 0(影響度が 0 の場合)，1.176(影響度が 0 以外の場合)　…式(3)

基本値 =（(0.6× 影響度)+(0.4× 攻撃容易性)-1.5)×f(影響度)　…式(4)

（小数点第 2 位四捨五入）

基本評価基準（Base Metrics）

評価結果値

AV ：攻撃元区分(Access Vector)

■ローカル 0.395 ，■隣接 0.646，■ネットワーク 1.0

AC ：攻撃条件の複雑さ(Access Complexity)

■高 0.35，■中 0.61，■低 0.71

Au ：攻撃前の認証要否(Authentication)

■複数 0.45，■単一 0.56，■不要 0.704

C ：機密性への影響（情報漏えいの可能性）(Confidentiality Impact)

■なし 0.0 , ■部分的 0.275 , ■全面的 0.660

I ：完全性への影響（情報改ざんの可能性）(Integrity Impact)

■なし 0.0 , ■部分的 0.275, ■全面的 0.660

A ：可用性への影響（業務停止の可能性）(Availability Impact)

■なし 0.0 , ■部分的 0.275, ■全面的 0.660

2.3.2 CVSS 現状値 (Temporal Score)

現状値 = 基本値 ×E×RL×RC （小数点第 2 位四捨五入） …式(5)

現状評価基準 (Temporal Metrics)

評価結果値

E ：攻撃される可能性(Exploitability)

■未実証 0.85, ■実証可能 0.90, ■攻撃可能 0.95, ■容易に攻撃可能 1.00,

■未評価 1.00

RL ：利用可能な対策のレベル(Remediation Level)

■正式 0.87, ■暫定 0.90, ■非公式 0.95, ■なし 1.00, ■未評価 1.00

RC ：脆弱性情報の信頼性(Report Confidence)

■未確認 0.90, ■未確証 0.95, ■確認済 1.00, ■未評価 1.00

2.3.3 CVSS 環境値 (Environmental Score)

調整後影響度 = min(10.0,10.41×(1-(1-C×CR)×(1-I×IR)×(1-A×AR))) …式(6)

調整後現状値 = 式(3), 式(4)の影響度に, 式(6)の調整後影響度の計算結果を代入し, 基本値を再計算する. その基本値で式(5)の現状値を再計算する. …式(7)

環境値 =(調整後現状値 +(10- 調整後現状値)×CD)×TD …式(8)

（小数点第 2 位四捨五入）

環境評価基準 (Environmental Metrics)

評価結果値

CD ：二次的被害の可能性(Collateral Damage Potential)

■なし 0.0, ■軽微 0.1, ■中程度 0.3, ■重大 0.4, ■壊滅的 0.5, ■未評価 0

TD ：影響を受ける対象システムの範囲(Target Distribution)

■なし 0.00, ■小規模 0.25, ■中規模　0.75, ■大規模 1.00, ■未評価 1.00

CR ：機密性の要求度(Confidentiality Requirement)

■低 0.5, ■中 1.0, ■高 1.51, ■未評価 1.0

IR ：完全性の要求度(Integrity Requirement)

■低 0.5, ■中 1.0, ■高 1.51, ■未評価 1.0

AR ：可用性の要求度(Availability Requirement)

■低 0.5, ■中 1.0, ■高 1.51, ■未評価 1.0

付録 3．SNS におけるセキュリティ，プライバシー問題

日本ネットワークセキュリティ協会の「SNS の安全な歩き方」[4]では，「SNS のプライバシーとセキュリティの問題と対策」として以下の問題点をあげでいる[39].

＜プライバシー情報の蓄積＞

・不用意な公開

住所，電話番号，家族構成，ライフスタイル，行動などを公開してしまうこと．公開した情報はインターネットに半永久的に残ってしまうとしている．

・設定の不備

SNS ではデータの使用権から収益を得ていることから，基本的に情報を公開する方向で運用されている．特に Facebook では，個人情報の初期設定が「公開」になっているので，必ず設定変更が必要である．

・知識不足

自分のコメントや「いいね！」などが初期設定で公開になっていることなどを認識していない（公開範囲の問題）．写真のジオタグ（GPS などによる位置情報），Facebook などでのチェックインの情報が公開になっている（位置情報の問題）．SNS の友達関係を利用した詐欺メッセージなども多い（詐欺行為の問題）．広告の審査がない場合が多いため，詐欺広告が出ることがある（オンライン広告の問題）．

・アプリケーションによる公開

Facebook 内でのアプリでの利用情報公開の問題．アプリの利用履歴などからプライバシーが漏れる場合もある．

・友達による情報の公開

参加したイベントで友達が勝手に写真をアップするなど，友達による情報公開の問題．写真へのタグ付け機能，チェックイン機能などでトラブルが起きる．

・他の情報との関連付け

他の SNS やウェブサイト，Twitter との連携で，個人情報が漏れる．

・SNS のポリシー変更

ここまでは Facebook でのプライバシーの問題だである．この他にも詐欺行為・問題行為として，「マルウェア感染や詐欺行為のプラットフォームとしての利用」「偽アカウント・アカウントの乗っ取り」「不適切な発言・行為」といった事例が紹介されている．

[安全に歩くための 10 項目]

このように SNS では，本人が意図せずに，もしくは設定の不備などで，プライバシーがネット上に漏れる場合がある．「Facebook では基本データとして記入する住所や電話番号が，初期設定で“公開”，つまり誰でも閲覧できる状態になっている」として注意を呼びかけている．

日本ネットワークセキュリティ協会では，SNS でのトラブルを避けるために，注意点として 10 項目をあげている[4].

1：常に公開・引用・記録されることを意識して利用する．

2：複雑なパスワードを利用し，セキュリティを高める設定を利用する．

3：公開範囲を設定し，不必要な露出を避ける．

4：知らない人とむやみに“友達”にならない．知っている人でも真正の確認をする．

5：“友達”に迷惑をかけない設定を行う．

6：“友達”からの削除は慎重に，制限リストなどの利用も考慮する．

7：写真の位置情報やチェックインなど，技術的なリスクを理解して正しく利用する．

8：むやみに“友達”のタグ付けや投稿を行わない．

9：対策ソフトを利用し，危険なサイトを利用するリスクを低減する．

10：企業などの組織においては，SNS ガイドラインを策定し遵守する．

付録 4. OpenFlow などトラヒックをソフトウエアで制御する SDN

Windows Server Insider の調査[40]に基づき，SDN と従来のネットワークの課題，SDN への注目と OpenFlow の台頭，SDN ではネットワークはダイナミックに一括制御のため変化が可能，といったことについて以下に示す．

＜SDN と従来のネットワークの課題＞

「Software-Defined Network（以下 SDN)」[41]とは，ネットワークの構成，機能，性能などをソフトウェアの操作だけで動的に設定，変更できるネットワーク，あるいはそのためのコンセプトを指す．従来のネットワークでは，例えばネットワークにサーバを追加する際，1 つのネットワークを複数に分割する際，あるいはアプリケーションごとの QoS を設定する際などには，ケーブルの接続をやり直したり，1 つ 1 つのルータやスイッチごとにネットワーク管理者が設定をしなければならなかった．

しかし，ネットワーク上に仮想サーバが多数存在するようになり，しかもそれが動的に生成，消滅し，ときにライブ・マイグレーションによってネットワーク内を移動するようになると，そのたびにネットワーク管理者がネットワーク機器をいちいち設定する必要がり，実有用に難があった．ここで，ライブ・マイグレーションとは，ある仮想マシンで稼働している OS やソフトウェアを停止させずに，丸ごと別の物理コンピュータに移動させること，また，仮想マシンモニタなどが持つそのような機能のことである．ハードウェアのメンテナンスや部品の交換が必要になったときサービスを停止させずに対応することができる．そこで，ネットワークのあらゆる構成や機能をソフトウェアだけで設定できるようにすることを目指す SDN が注目された．

＜SDN への注目と OpenFlow の台頭＞

SDN が注目され始めたもう 1 つの理由が，「OpenFlow」と呼ばれるネットワーク標準の登場である．JPNIC によると 「OpenFlow」 [42] では，スイッチの動作を定義するとともに，そのスイッチを制御するためのプロトコルも定義している．これまでネットワーク機器を制御するためのプロトコルや API はベンダ固有のものしかなく，それがマルチ・ベンダ環境でのネットワーク構成を自動化する上での障害になっていた．各ベンダが OpenFlow に対応した機器をリリースすることで，標準プロトコルによって統合的にネットワーク機器の設定が可能になる，

＜SDN ではネットワークはダイナミックに一括制御のため変化が可能＞

SDN では，個々のネットワーク機器をそれぞれ制御するのではなく，ネットワーク全体を俯瞰した上でソフトウェアによって一括制御するため，はるかに管理が容易になる．これは，SDN では，設定するのはあくまでネットワーク全体であり，個別のネットワーク機器は（設定の面では）あまり意識されなくなるからである．

参考文献

[1] ISO/IEC 27001,″Information security management. Specificatio ネットワーク ith 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 23 年報,”2012 年 3 月

[4] NPO 日本ネットワークセキュリティ教会 (SNS セキュリティワーキンググループ),“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,”2012.11.19 http://www.jnsa.org/result/2012/SNS.html 2014 年 3 月現在

[5] 岡田康義, 西川康宏, 堀琢磨, 佐藤直,“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,”情報システム学会誌 Vol. 9, No2 2014 年 3 月 (掲載予定)

[6] 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

[7] Y.Okada, K.Ishii,and N.Sato,″ Proposal of SNS Membership Qualification System Using Security Information Database,″ KasPerasky Academy Cyber Security Academy for the next Generation in Singapore, 2013.3

[8] 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 6 月

[9] E.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, 200 年 9 月

[10] A. Garga, and A.L. N. Reddy,″Mitigation of DoS attacks through QoS regulation,″IEEE Microcessors and Microstems 2004,Vol.28, Issue 10, pp.521-530, 2004.2

[11] 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

[12] Y.Okada, Y.Nishikawa, and N.Sato,″ DoS attack countermeasures in NGN using private security policy,″ IEEE APSITT2010, A-1-2, 2010.6

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

[14] 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

[15] 長健二朗,“インターネットにおける QoS 制御技術～ Diffserv,” 1999 年 12 月 14 日 http://www.nic.ad.jp/ja/materials/iw/1999/notes/C8.PDF 2014 年 3 月現在

[16] 電気通信事業法（昭和 59 年法律第 86 号）

[17] 社団法人日本インターネットプロバイダー協会他,“電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン,”第 2 版 P7,P10 ,2011 年 3 月 25 日

[18] 総務省,“電気通信事業分野におけるプライバシー情報に関する懇談会(第 18 回会合)議事要旨,”
http://warp.ndl.go.jp/info:ndljp/pid/286922/www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/060123_1.html 2014 年 3 月現在

[19] 古川泰弘, 吉成大知,“ペネトレーションテスト入門－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

[20] 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,”信学技報 ISEC2008-103, pp. 15-22, 2009 年 3 月

[21] Mitre,″ Common Vulnerabilities and Exposures,″ http://cve.mitre.org/, 2014 年 3 月現在

[22] 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, 2014 年 3 月現在

[23] IETF, ″RFC2475 An Architecture for Differentiated Services,″ 1998.12

[24] Microsoft Technet,“DNS のセキュリティ情報,”
http://technet.microsoft.com/ja-jp/library/cc755131.aspx 2014 年 3 月現在

[25] 斉藤栄太,“「SNS でのウイルス感染の危険度はメールより 10 倍も高い」ウイルス専門家が最新動向を報告,”2010.11.26
http://itpro.nikkeibp.co.jp/article/NEWS/20101126/354594/ 2014 年 3 月現在

[26] J－Cast News,“著名人の「なりすまし」 Twitter で相次ぐ,”2009/7/22
http://www.j-cast.com/2009/07/22045839.html 2014 年 3 月現在

[27] 内閣官房情報セキュリティセンター情報セキュリティ政策会議,“情報セキュイリティ 2011,”2011.7.8 http://www.nisc.go.jp/active/kihon/pdf/is2012.pdf 2014 年 3 月現在

[28] 岡田康義，石井和行，佐藤直，“情報セキュリティ DB を用いた SNS 会員資格制度の提案，”信学技報 SITE2013-3，pp. 11-16，2013 年 3 月

[29] 佐藤直，“検証ベースインターネットの提案，”2006 年電子情報通信学会総合大会，通信 Vol. 2，216 頁　2006 年 3 月

[30] 笠原英樹，錦戸淳，織田一弘，大西邦宏，梶山義夫，“次世代ネットワークを支えるネットワーク基盤技術，”NTT 技術ジャーナル 2007 年 4 月，pp. 39-43

[31] 村上龍郎，中島伊佐美，大羽巧，“世界のキャリアが取り組む NGN(Next Generation Networks)の技術的要素，”情報処理，Vol.47　No.10，pp. 1091-1099，2006 年 10 月

[32] 高橋健太郎，“NTT の NGN はどんなしくみ？，”日経 NETWORK 2006 年 12 月号 72 頁

[33] 高橋健太郎，“NGN エッジ・ルーターの詳細が明らかに ，”日経コミュニケーション 2008 年 4 月 15 日号 20 頁

[34] 國谷武史，“NGN がターゲット――シスコが新世代エッジルータを発表，” ITmedia 2008 年 03 月 05 日
http://www.itmedia.co.jp/enterprise/articles/0803/05/news076.html 2014 年 3 月現在

[35] インプレス R&D 標準技術編集部 / ランドッグ・オーグ 平野正喜 ，“ジュニパーネットワークスの NGN 戦略を聞く：コア・ルータ，エッジ・ルータ向けなどに特化，”2007.12.25，　http://wbb.forum.impressrd.jp/feature/20071114/502 2014 年 3 月現在

[36] G.Parulkar, J.Reijendam and J.Little,″OpenFlow/SDN:A New Approach to Networking,″
http://cenic2012.cenic.org/program/slides/CenicOpenFlow-3-9-12-submit.pdf, 2014 年 3 月現在

[37] JPNIC 日本ネットワークインフォメーションセンター　ニュースレター
No.31/2005 年 11 月発行
https://www.nic.ad.jp/ja/newsletter/No31/020.html 2014 年 3 月現在

[38] IPA 独立行政法人 情報処理推進機構，“共通脆弱性評価システム CVSS 概説，”
http://www.ipa.go.jp/security/vuln/CVSS.html 2014 年 3 月現在

[39] YOMIURI ONLINE4，“覚えておきたい「SNS の安全な歩き方」，”（2012 年 12 月 7 日 読

売新聞）
http://www.yomiuri.co.jp/net/security/goshinjyutsu/20121207-OYT8T00820.htm
2014 年 3 月現在
[40] Windows Server Insider, “SDN (Software Defined Networking)とは,”
http://www.atmarkit.co.jp/ait/articles/1304/08/news098.html 2014 年 3 月現在
[41] インプレス社クラウド Watch, “【SDN 特集】第一回クラウド時代の仮想ネットワーク技術, SDN と OpenFlow を解説する,”
[42] http://cloud.watch.impress.co.jp/docs/special/20121018_566558.html 2014 年 3 月現在
[43] JPNIC「OpenFlow」ニュースレター No.5.2/2012 年 11 月発行
https://www.nic.ad.jp/ja/newsletter/No5.2/0800.html 2014 年 3 月現在