社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2007－ＣＳＥＣ－38（２）
2007／7／19

情報セキュリティデータベースを用いたインターネット優先転送方式

岡田　康義†　　佐藤　直‡

†情報セキュリティ大学院大　〒105-0123　神奈川県横浜市神奈川区鶴屋町 2-14-1

E-mail:　† okada223@goo.jp,　sato@iisec.ac.jp

あらまし　本稿では，交通制度を参考にして，情報セキュリティデータベースを用いたインターネットの優先 転送方式を提案する。本方式では、受信者の負荷削減、不正サクセス、匿 名犯罪等の 削減に関して以下の３つの効果が期待される。　（１）ネット２階層のプロトコルで情報セキュリティをチェックすることで，受信者だけで，背負っていた情報セキュリティによる負荷を軽減できる．（２）管理網をネット網と区別することで，情報セキュリティデータベースから各情報セキュリティ情報を吸い上げることや、ネットの輻輳や不正アクセス等を回避することができる．（３）通信相手先情報を受け取ることによって，情報セキュリティデータベースにより 通信非匿名性による不正行為や犯罪等を防ぐことができる．本稿では、スパムメール，ウィルスやフィッシングサーバを例にとって、本方式の実現方法や長所と短所について考察した結果を報告する

キーワード　セキュリティデータベースを用いたインターネット優先転送方式、情報セキュリティサービス

A preference transmission method with information security database systems on the Internet

Yasuyoshi Okada†　　Naoshi Sato

† Institute of Information Security, Graduate School of Information Security

2-14-1　Tsuruya,　Kanagawaku, Yokohama-shi, Kanagawa, 221-0835 Japan

E-mail:　† okada223@goo.jp,　sato@iisec.ac.jp

Abstract　The number of computer viruses or illegal accesses on the Internet is rapidly increasing. According to information technology promotion agency Japan, a variety of problems are cause D By lack of security management on the Internet. For the purpose of improving security, personal users are continually devising countermeasures against computer viruses, illegal computer use, nuisance e-mail messages (spam), information leakage, toxic sites, toxic contents, and illegal acts of the computer E-Commerce. They have been received security services in various kinds levels from many vendors.　However, personal users, LAN managers, ISP managers, and carrier managers do not have sufficient rules to cooperate with them. Also, countermeasures are coped with partial solution. Personal users' loads are increasing very much. As a solution to some of these problems, this paper proposes　A preference transmission method with information security database systems on the Internet, viewing the situation in telecommunications as being analogous to the vehicular traffic system and merits and demerits　of the proposed systems　in case of spam males,　viruses and phishing servers　are shown in this paper.

Keyword　A preference transmission method with information security database systems on the Internet,　information security, Security of services.

1. はじめに

インターネットは「誰でもが自由に使える」という利便性を旗印にたゆまない発展を続けている．現状，利用者は高度情報化社会のインフラとしてインターネットの利便性を十分享受できる段階に至っている．一方で，コンピュータ・ウィルスや不正アクセス等の情報セキュリティ上の脅威も増大の一途を辿っており，健全な高度情報化社会の実現を阻害している．

このような脅威が増す大きな要因として，インターネット利用に関する制限あるいは社会制度が殆ど設けられていないことが上げられる．そこで，本稿では，自動車運転資格証制度の

類推からセキュリティデータベースを用いたインターネットワーク利用優先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インターネットワーク利用優先資格証を発行し,セキュリティデータベース基づく優先転送方式を導入することを提案する．このような方式導入によって，セキュアなインターネットひいては安心して利用できる情報通信環境の実現が可能になると期待される．

2章では，インターネットにおける情報セキュリティの現状，3章では情報セキュリティデータベースを用いたインターネット優先転送方式導入とその効果，4章では，インターネット管理組織と役割，5章は運用イメージ，6 章では提案内容を実現する技術及びシステム概要について考察し，7章では課題，8章では，結びを述べる．

2. インターネットにおける情報セキュリティの現状

インターネットのようなオープン化システムの情報セキュリティの問題に関しては，商用化が始まった1990年代からさまざまな方面から指摘されてきた(表1参照)．近年になり，インターネット上でのビジネスがさらに盛んになり，インターネットの重要性が高まるにつれ，情報セキュリティ対策の重要性が一段とクローズアップされてきた． コンピュータウィルス、フィッシングサーバ、不正アクセスの急増も相まって,多種多様なインターネット化に伴う課題が浮き彫りにされてきている．インターネットを取り巻く情報セキュリティに関する関心は，否が応でも高まっている．独立法人情報処理機構[1]には多数のコンピュータウィルス・不正アクセスの状況について報告がある．それに応じて，さまざまな情報セキュリティ対策が組織や個人レベルで行われつつあるが，それらには，以下の2．1に述べるような浮き彫りになり，高度な情報セキュリティ対策が要求されるようになってきている．

表1 インターネットの歴史

年代	インターネット利用目的
1970～1990年	研究用情報交流
1990－2000年	初期の商用ネット
2000年～今日	ブロードバンド発展後の生活基盤としてのインターネット

2．1 情報セキュリティ対策の実施主体と現状

インターネットにおける情報セキュリティ対策の主体は，個人ユーザとネットワーク管理組織の2つがある．表2にこれら実施主体の現状を示す．個人ユーザとしては ウィルス対策，不正対策，迷惑メール(スパムメール)，情報漏えい，スパイウェア，有害サイト，有害コンテンツ，コンピュータ不正使用等対策さまざまなレベルでの情報セキュリティ対策ソフトウェア等の各種・多様なサービスを受けることが必要であり，さまざまな対策にコスト及び負荷が多くかかっている．ネットワーク管理組織を見ると個人ユーザを管理するLAN管理者，ISP管理者，キャリア情報連携のルールが十分でない．また，現在のセキュリティ対策は，対処療法的，個別的なものにとどまっていて，総合的なセキュリティ方策は十分であるとは言えない．さらに，インターネット管理組織として，どの省庁が対応すべきであるかどうかの役割分担が明確ではないために，トラブルが起こったときに，トラブル対応部署が存在しない，または,情報伝達の漏れから対応に手間取るという問題が生じている．このように，セキュリティ対策実施主体間の連携が出来ていない．

表2 情報セキュリティ対策の実施主体と現状

主体	現状
個人ユーザ	多種・多様セキュリティサービス受信が必須で，負担が多い
ネットワーク管理組織	部署間での役割分担があいまいで，連携が十分とは言えない．

2.2 情報セキュリティ対策の課題

2.1のように様々な課題があるが、独立行政法人情報処理推進機構[1]によると世界のインターネットトラヒックの８０％－９０％はスパムメールであり、ウィルスも横行している。またその他、インターネットWWWの中でフィッシングサイト等不正や犯罪も増加しているという報告があり、具体的には、以下をもたらしている。

（1）ＩＳＰでスパムメール負荷によるユーザトラヒックへの影響が大きい。

（2）ユーザはスパムメール対策に追われている

（3）警察もインターネットフィッシング等不正や犯罪も増加に対応しきれない。

3. 情報セキュリティデータベースを用いたインターネット優先転送方式導入とその効果

本章では，2.3 節のインターネット発展における情報セキュリティ対策の現状をもたらしている原因について以下の仮説を置いてみた．

（仮説） 生活基盤となりつつあるインターネットは，他の生活基盤に比べ， 社会制度が未成熟であることが原因である．

たとえば,同じ流通分野にある自動車交通制度と比較すると,インターネットは，車のようなライセンス制度や車検制度等の社会制度がない．このため匿名ユーザが不正な行為をした場合に，それを特定したり，アクセスしているサーバが犯されていないかどうかをチェックできない．

そこで，上記の仮設を前提として，自動車交通制度を参考にして,インターネットの利用優先制度導入が重要であると考え、そのためには、セキュリティデータベースを用いた優先転送方式が重要であると考える。3．1では、本仮説に基づき、2．2節での解決策を考察した。

表3 自動車交通とインターネットの制度比較

項目	自動車交通	インターネット
ユーザライセンス	免許有	なし
利用媒体	車両	パソコン, LAN 等
検定制度	車検制度	検定なし
登録先	警察	なし

3.1 情報セキュリティ対策課題の解決策

解決策として以下の(1)-(3)がある。

（1）インターネット利用に関して、以下の公的資格証・検査証を与える。

- 利用優先資格証
- 情報通信機器検査証、NW 検査証（LAN,AS）

（2） ブラックリスト等の非公開情報および調査結果の管理機関等での流通

（3）公開、非公開部分を分離したセキュリティＤＢ管理

- ＤＢ管理でセキュリティレベルに公開部分
- 第三者機関による商用サーバのセキュリティレベルの格付けが必要。

＜第三者評価機関＞としては、

各種情報セキュリティ対策のためには、情報セキュリティ DB に登録各データセキュリティレベルの信頼性を第三者機関として評価することが必要である(図 1 参照)。

3.2 セキュリティデータベース利用および効果

スパムメール、ウィルス、WWWサーバのフィッシング等の例にとって、ISP、ユーザ、警察等の各機関等への利用および効果をいかに述べる。

★ISP 等：セキュリティ対策としてスパム等のパケットを制限することで、スパムトラヒックの大幅削減が見こまれ、サービス帯域の有効利用が図れる。およびセキュリティデータベースシステムを用いた通信相手先のセキュリティレベルを知らせるサービスも可能である。

★ユーザ：SPAM メール等で利用優先資格証を持ってないユーザは、ISP レベルで区別できるので、素性が分からないユーザからの通信は最初から拒絶できるため、セキュリティ対策の負荷軽減が可能である

★DB(警察)：公的機関　（公開情報）

犯罪時データの管理および犯罪情報により円滑な対応が可能である。

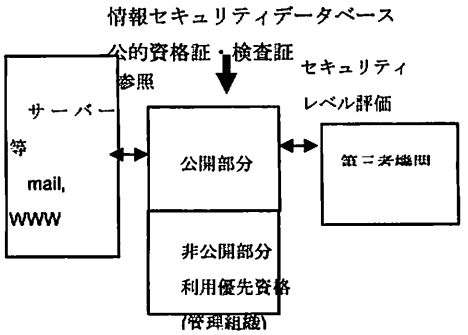

図１．　情報セキュリティデータベース

4．インターネット管理組織と役割

提案方式を実施するために必要なインターネット管理主管組織，サポート組織とそれぞれの役割を以下に示す．

4.1 管理主管組織と役割

■証明書類

提案方式を実施するために必要な主な各種証明書類を以下に記載する。

・インターネット利用優先資格証:利用者本人の身元やセキュリティレベルの情報

・情報通信機器検査証：ユーザのインターネット接続のための端末のセキュリティ対策状況に関する情報

・LAN・AS 検査証：ユーザの利用する LAN のセ脆弱性やセキュリティ対策状況の情報

■管理組織と役割

＜インターネット利用優先資格証＞:公的位置づけおよび犯罪捜査の観点から、警視庁のサイバー警察署等で実行・管理するのが，望ましい．

＜情報通信機器検査＞:車検と同様なシステムとして，警視庁インターネット情報管理局(警視庁インターネット情管局と略す)を組織して、実行・管理するのが望ましいと思われる．

＜LAN・AS 検査証＞

組織は犯罪では，ある特定ドメインからの違法なパケットの発出が多いため，取締りのために、警視庁インターネット情官局が実行・管理するのが望ましい．

表4 組織と役割

組織	役割
警視庁サイバー警察署	インターネット利用優先資格証の発行
警視庁インターネット情官局	情報通信機器を登録・管理，LAN/ASを登録・管理

4.2 サポート組織と役割

4.1 で述べた主管組織だけでは，実際の運用が無理なため，サポート部隊を置くことが必須である.表5は，サポート組織と役割を示している.

表5 サポート組織と役割

組織	役割
情報通信機器ベンダ	DBを作成と管理
OS・アプリケーションソフトベンダ	DBを作成と管理
セキュリティ対策ソフトベンダ	ソフト更新管理
検疫サービス事業者	検疫サービスの実施
加入ISP	利用優先資格証発行
中継ISP	利用優先資格証・通行証の検証

5運用イメージ

運用の全体フローとしては，以下の（1）から運（3）までの流れがある.

（1）セキュリティＤＢへの登録

（2）パソコン、サーバ（メールサーバ、WWWサーバ）およびＬＡＮ機器ＡＳ等のウィルスや脆弱性等のセキュリティの検証

（3）警察署により違反処理

以降（1）－（3）までを順に述べる.

5．1 セキュリティＤＢへの登録

インターネット利用者優先者のセキュリティ DB への登録および利用優先資格証の発行方法について説明する.

表6は，利用優先資格証と運転免許証を示す.

運転免許証を参考にすると利用優先資格証では，表６の左の列のような情報を記載しておく必要がある．これをセキュリティ DB へ登録する.

5．1．1 インターネット利用優先資格証の登録手続き

インターネット利用優先資格証の登録手続きの仕方は，以下の①―③のような手続きで行う.

① 市役所等の公的機関や所属組織が発行する証明書（例．住民票，身分証明書）を添えて，管轄の証明書管理機関に申請する.

② 証明書管理機関では，この申請内容を確認した後，交付年月日，交付番号，証明書管理機関名を加えたインターネット利用優先資格証（平文）とそれをハッシュ化した値をユーザに交付する．このハッシュ値が IP パケットのヘッダで転送される.

③ 証明書管理機関ではこのインターネット利用優先資格証に関する電子証明書を作成し，要請に応じて公開する．すなわち，平文のインターネット利用優先資格証とハッシュ値を合わせ，証明書管理機関の秘密鍵で暗号化した（電子署名した）ものを電子証明書とする.

5．1．2 インターネット利用優先資格証の発行

インターネット利用優先資格証はユーザ各自で登録申請し交付される．登録・交付のタイミングとしては，ユーザが新しく LAN に収容された時，あるいは，その属人的情報（例えば，姓や所属部署）が変更になった場合である．一般家庭の場合，引越し等で住所が変わった場合に登録が必要になる．表６に示す自動車運転免許証と対応している。ユーザのインターネット利用に関する属人性は一通りではなく，複数のインターネット利用優先資格証を交付することが考えられる．例えば，個人として，あるいは，勤務する会社の社員として，というように，別のインターネット利用優先資格証を交付する．なお，個人としてインターネット利用優先資格証を所持する場合，氏名，生年月日，本籍，現住所等の情報については，住民基本台帳の記載情報と関連しうることから，台帳の記載番号等を記載することも考えられる.

<インターネット利用条件>

インターネット利用条件について考察する．自動車運転免許証の場合は自動車を運転する能力に対して免許が与えられるが，情報セキュリティに関する能力を尺度化して管理することは考えにくい．セキュリティデータベースを用いたインターネット利用優先方式導入の目的が，ユーザのインターネット利用が情報セキュリティ上の脅威となることを防止すること，であることを考慮すると事

件・事故を発生した履歴で減点することが考えられる．ここで，事件・事故とは，故意にウィルス感染用プログラムをインターネット上に発信させた，迷惑メールの踏み台になるようなサーバ設定を行い再三の勧告にも関わらず是正措置をとらなかった，フィッシング行為を行った，等である．現在でも事件・事故を起こしたユーザは警察やISPの監視機関のブラックリストに掲載される．そこで，このようなブラックリスト化を公的な制度として運用し，同リストに基づいて減点していくことが考えられる．累積減点値がある閾値を超えた場合，事件・事故の内容に応じて，当該ユーザのインターネットアクセス（情報発信や受信方法）に制限を加える，あるいは，一定期間免許を停止するなどの罰を科すことにする．

表６　利用優先資格証と運転免許証

利用優先資格証	運転免許証(参考)
氏名	氏名
生年月日	生年月日
本籍	本籍
ホームネットワークアドレス ネットワークIPアドレス， グローバルIPアドレス （固定的アドレスの場合），	現住所
交付年月日	交付年月日，
免許シーケンス番号	免許シーケンス番号
利用条件：	利用条件：眼鏡等
ネット利用有効期間	免許有効期間
証明書管理機関	証明書管理機関

＜インターネット利用優先資格証の検索要求に対する公開に関して＞

このインターネット利用優先資格証に関する検索要求に対する公開およびその条件について考える．６章の提案方式式を実現する技術およびシステムの概要で説明する電子証明書に用いた秘密鍵に対応する公開鍵が公開鍵基盤（通称PKI）の認証局に登録されているものとすると，ユーザのインターネット利用優先資格証の内容を検索したり，あるいはそのハッシュ値の真正性を確認したりする場合は，この公開鍵を認証局から取り寄せてその真正性を確認できるものとする．ただし，インターネット利用優先資格証は個人情報の一種と考えられるため無条件での公開は望ましくない．そこで，公開の条件としては，以下の①と②を満たす場合である．

① 要求者の真正性が明らかである．

② 要求者がユーザからインターネット利用優先資格証のハッシュ値を受け取ったことが確認できる．

５．２　パソコンおよびＬＡＮ機器ＡＳ等のセキュリティの検証について，

図２において，情報通信機器検査証は，ユーザが使用するハードウェアである，ホスト端末，すなわち，クライアント端末およびサーバ端末について，セキュリティ上の安全性を証明するものであり，表７に示すように，自動車運転免許制度における自動車検査証（車検証）に相当する．情報通信機器検査証の発行については LAN 単位で発行，管理する．以下，このような管理主体を前提として検討する．ただし，ユーザがどのような情報通信機器を利用しているかについては，インターネット利用優先資格証の交付と無関係ではないので，情報通信機器検査証の管理主体はユーザを収容する LAN（個人ユーザの場合は契約している ISP を想定する）とするが，検査結果や情報通信機器検査証の写しは公的証明書管理機関に転送し，保存しておくものとする．

一方、脆弱性検査サービスプロバイダは LAN や AS に対して，第三者組織として位置づけられる．従来，この脆弱性検査サービスは，セキュリティ確保の必要性が高い組織を中心に任意加入となっている．情報通信機器検査に関わるベンダと同様，LAN 検査証あるいは AS 検査証といったネットワーク的要素について，公的検査制度を適用しようとすると，加入義務を負わせる必要がある．

表７　車検証と情報通信機器検査証との比較

制度	自動車運転免許制度	インターネット利用優先資格制度
対象	自動車	クライアント端末・サーバ
検査証	車検証	情報通信機器検査証

５．３ 違反処理等に関して，セキュリティＤＢの利用

故意にスパムメール等を送信して事件・事故を起こした

ユーザは警察や ISP の監視機関のブラックリストに掲載される．コンピュータあるいはネットワーク犯罪の抑制あるいは事後の迅速な捜査のためセキュリティＤＢを利用することによって，情報セキュリティ上の大きな進歩が得られると期待される．

６．提案方式を実現する技術及びシステムの概要

6．1　ネットワークの構成

提案方式を説明するためのネットワーク構成を図２に示す．提案方式は，ユーザにサービスしているユーザ網でインターネット網と本方式の制御信号を送る管理網から構成及びセキュリティデータベース(セキュリティDBと略す)から成る．

(1)ユーザ情報転送網(インターネット:図２の上半分)

ユーザ情報転送網では，表8－1に示すようなユーザインターネットメンバーで構成される．そこでは，以下のような構成の特徴がある．

- エンド-エンドユーザ LAN を含む AS，および中継 AS で接続されている．
- 各エンドユーザのLAN(およびAS)には，優先転送を行う送信元ゲートウェイおよびあて先ゲートウェイがあり，そこには，検証用サーバを接続している．
- 中継ルータには，異常パケットや異常トラヒックを監視するトラヒック監視用サーバが接続されている．

(2)　制御情報転送網(管理ネットワーク:図２の下半分)

表8－2に示すような，管理インターネットメンバーで構成される．そこでは，以下のような構成の特徴がある．

- ISP(またはキャリア)および情報通信機器ベンダ，セキュリティ対策ソフトベンダ，基本・応用ソフトベンダ，脆弱性検査サービスプロバイダが参画する．
- 上記メンバーを管理している証明書管理機関

(3)　前述した情報セキュリティレベルに関するセキュリティDB であり，インターネット犯罪履歴に関するデータベースも含まれている．

以下では，ネットワークの基本機能について述べる．

表8－1 ユーザインターネットメンバー

送信ユーザ
受信ユーザ

表 8－2 管理インターネットメンバー

情報通信ベンダー
セキュリティソフトベンダー
基本・応用ソフトベンダー
脆弱性・検査サービスプロバイダー

6．1．1　管理網の基本的機能

管理網はユーザ網と分離している．ユーザ網と独立に管理網があるため，セキュリティ情報のやりとりに関して，ユーザトラヒックの輻輳が管理網に影響しない．アプリケーション層とトランスポート層のプロトコルが連携している．

ネット利用優先資格証，情報通信機器検査証，LAN検査証，AS検査証に関するチェックは当該網で行う．　管理網では，以下のデータをユーザ情報転送網からネットから吸い上げ，セキュリティデータベースに蓄える．

(1)　情報通信機器検証情報

・パソコンのウィルスチェックの有無

・LAN，ファイアウォール機器(サービスポート等の制限がポリシー通りに設定の有無

(2)　LAN・AS，ソフトウェアの脆弱性情報

・サーバ(WWW，メールサーバ)の脆弱性のチェック

(3)　証明書情報

- 所定の証明書の有無

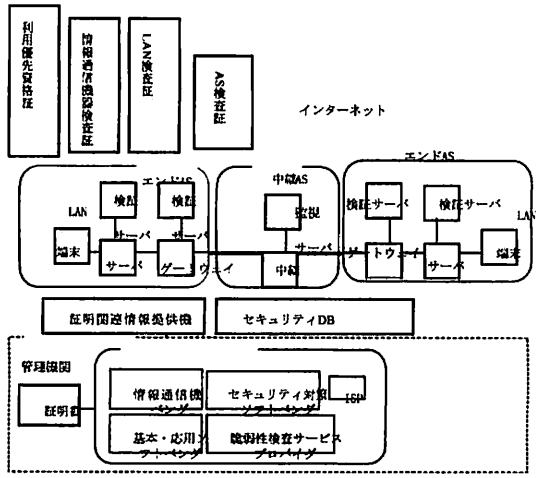

図２　提案方式を実現する技術及びシステムの構成

6．1．2 AS送信元ゲートウェイおよびASあて先ゲートウェイでの優先転送方式の前提となる基本機能:

- 証明方法と電子証明

送信元ゲートウェイおよび AS あて先ゲートウェイで

は，2 階層プロトコルにて通信相手をエンド AS にて認証する．このとき，認証は，IEEE802.1X と呼ばれる認証方式を用いる． ITU-T[4]により，認証局の X.509 の様式で記述されており，電子署名（秘密鍵で暗号化）で電子証明書の真正性を保証する．ネット利用優先資格者はトランスポート層にて，まず,トランスポート層で通過かどうかを判定する．それ以外のユーザは，アプリケーション層の詳細データをセキュリティ保証データベースで検索して，ユーザに通信相手の証明書情報を送る．

6．2　優先転送方式

6．2．1　優先転送方式:実現例

優先転送方式実現には，以下の 3 つフェーズが必要である．

- 送信元ホスト優先情報入力
- 送信元ゲートウェイ検証
- あて先ゲートウェイ検証

図 3 はインターネット優先転送方式の上記フェーズ（1）－（3）を以下に，その内容を示す．

(1)　送信元ホスト優先情報入力フェーズ，

ユーザのネット利用優先資格証内容をパケットに入力する．このとき，表 2 の利用優先資格証の情報に加えて，項目毎にパラメータ化，表 6 の利用優先資格の条件，たとえば，ユーザの利用優先資格の取得，情報通信媒体のセキュリティレベルを保証するける検査証を有するか否か等を各項目毎に，1（有，0（否） 等のビット列で情報として送る．これは，IPv6(江崎[3])では，IP パケットの拡張ヘッダーに記載して，送信元ゲートウェイに送る．

(2)　送信元ゲートウェイ転送フェーズ

送信元ゲートウェイは，自身の検証ポリシーとあて先の検証ポリシーの両方に適合した場合のみ，ネットに同 IP パケットを送出することが可能となる．この場合，ネットワーク同士で相互認証が行われ，あて先の検証ポリシーで検証されていることが保証される． 本方式ではあて先ネットワークにおける検証が不要になる．本方式において IP パケットのヘッダで転送する情報は，ユーザのネット利用優先資格証やゲートウェイの検証のほか，情報通信機器検査証，LAN 検査証や AS 検査証を追記した総合的な検査情報を圧縮したものとすることが考えられる．

・本手段では，LAN ゲートウェイや AS ゲートウェイを通過する際に，書き換えられることになる．

(3)　あて先ゲートウェイ転送フェーズ

あて先ホストの検証ポリシーを掌握するため，あて先ホスト検証方式のように，あて先ホストが検証しない，といった脅威を実質的に回避できる．送信元ゲートウェイで実施した検証をあて先ゲートウェイでも実施あるいは常時確認することを方式として選択すれば，検証の信頼性の向上が図れる．この場合，ネットセキュリティレベル統一といった点からも望ましいが，二重の検証が行われるため，IP パケット転送の実効速度が他方式よりも低下する（転送遅延が増加する）ことは避けられない．上記問題は，将来のゲートウェイの性能向上により解決されるものと予想される．

6．2.2　情報セキュリティに関する優先転送方式とQoS･Diffserv と比較

本提案方式は，従来のインターネット QoS サービスの 1 つである Diffserv サービスと類似のサービスである．図 3 のインターネット優先転送方式では，送信元ゲートウェイで IP ヘッダーフィールドと受信先ポリシーがマッチングしていることを示している．フェーズ 1 では，IP パケットヘッダーへの埋め込みが行われる．フェーズ 2 で，送信者のセキュリティレベルが，表 9 のように，評価されている．送信あて先のセキュリティポリシーとマッチングすれば，高速網へ流し，マッチングしなければ，低速網へ流し，検証 OK の項目は，1 他は 0 で表示されて，結果のみがフェーズ 3 に渡される．フェーズ 3 では，これらを受け取り，一定のセキュリティレベルを満たしているかどうかの判定基準情報として，扱われる．これは，現在インターネット上で行われている通信品質（QoS: Quoality of Service）の 1 つである Diffserv（Differential Services）と類似である．類似点として，Diffserv では，複数の優先クラス間で相対的な転送差をつけることによって，トラフィックの優先制御を行うのに対して，本提案システムでは，情報のセキュリティレベル（SoS: Security of Service）によって，複数の優先クラスでそタイ的な優先制御を行う．一方，大きな相違点としては，Differv では，ISP や LAN 管理者等の主観で優先クラスを決定するのに比べて，本システムでは，情報セキュリティ上のデータベースを有し，そのデータベースの情報のセキュリティレベルと送信先のゲー

トウェイでのポリシーと合致するかどうかを判定することで，優先クラスを決定していることである。

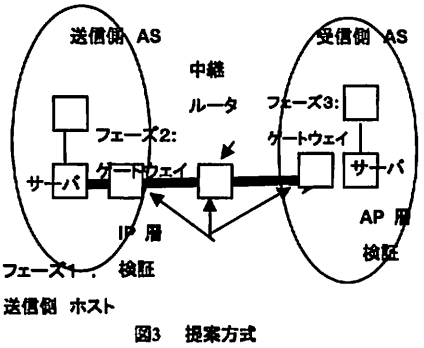

図3 提案方式

表9 セキュリティレベル評価

対象	検証項目	結果
ユーザ	資格証の有無	無し
パソコン	ウィルスチェック	良好
LAN	ファイアーウォール設定	良好
AS	ルータでのフィルターの設定	良好
総合評価	やや良好	

6.3 優先転送方式の長所と短所

ISP、ユーザ、警察等の各機関等への利用および効果をいかに述べる。

＜長所＞：

- 【ISP】は、セキュリティ対策としてスパム等のパケットを非優先網へ転送することで、スパムトラヒックの大幅削減が見こまれ、サービス帯域の有効利用が図れる。
- 【ユーザ】は、SPAMメール等で利用優先資格証を持ってない素性が分からないユーザからの通信は最初から拒絶できるため、セキュリティ対策の負荷軽減が可能である。
- 【DB(警察)】では、公的機関 (公開情報) 犯罪時データの管理および犯罪情報により円滑な対応

＜短所＞：

【ISP】では、本提案技術で、ルータサーバ・サーバの負荷があがる。

・【全体】では、本方式導入のコスト負担がかかる。

7．課題

- 村上[5]等解説するNGNや海外接続へ発展する場合に本方式を導入する前提としては，国際標準化であるITU-T，IETFを経て，国際標準化を進めていく必要がある.
- 本提案方式を実行するにあたっては，ISPやキャリア網への実装が考えられる．そのコストは誰が負担するのかが課題である.

8. 結び

本文では公的インフラであるインターネットのセキュリティ向上を狙いとして，セキュリティデータベースを用いたインターネット利用優先転送の提案を行った．情報流通と物流という違いはあるが，流通という社会的機能におきて，情報通信は交通運輸と類似している．このことから，先行している交通運輸分野における安全性確保のための各種証明書類，すなわち，自動車運転免許証，自動車検査証をヒントに，インターネット利用のための各種証明書類を検討し、スパムメール、ウィルス、フィッシングサーバを例にとって、その期待される効果を示した．次に，ユーザ個人毎に発行するインターネット利用優先資格証，使用するホスト端末に発行する情報通信機器検査証，LANやAS単位に与えるLAN検査証，AS検査証を提案し、次に，既存のセキュリティ対策技術や検査サービスが提案する本方式実現時における役割を考察し，それらの連携によるシステム化を検討した結果を報告した。今後は、提案方法における実現方法について、さらに、具体化を行う。

文 献

[1] 独立行政法人情報処理推進機構:「１０大脅威の”見えない“化が加速する．！」，pp29，『情報セキュリティ白書2007年版』，2007.

[2] 佐藤直，“検証ベースIPネットワークの提案，”通信Nov2, pp.216，(社)電子情報通信学会総合大会，2006.

[3] 江崎浩：『IPv6教科書』IDGジャパン，2002

[4] ITU-T (2000)：「Recommendation X.509；Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks」

[5] 村上，中島，大羽：「世界のキャリアが取り組むNGN(Next Generation Networks)の技術的要素」『財団法人情報処理学会会報誌』情報処理，Vol.47 No.10，2006

[6] 尾家祐二，後藤滋樹，小西和憲,西尾章治郎：『インターネット入門』岩波書，2001