98-01043

教育用計算機システムにおける利用者認証機構に関する研究

代表研究者　松浦　敏雄　大阪市立大学 学術情報総合センター教授
共同研究者　中西　通雄　大阪大学サイバーメディアセンター助教授
共同研究者　山井　成良　岡山大学総合情報処理センター助教授
共同研究者　石橋　勇人　大阪市立大学 学術情報総合センター講師
共同研究者　安倍　広多　大阪市立大学 学術情報総合センター講師

1　研究の目的

大学や企業など各組織では、ネットワークを通じて、電子メール、ネットワークニュース、ウェブをはじめ様々なアクセスサービスを提供している。これらのサービスを受けるには、自組織内の計算機端末、電話回線からの利用、情報コンセントを介した個人のパソコン、インターネットプロバイダ経由の利用など様々な利用形態が考えられる。

いずれの利用形態においても、部外者の利用を阻止でき、許可された正規の利用者のみが利用できるような仕組みが必要である。 また、正規の利用者であっても、他人を偽って不正な行動が起こせないような仕組み、もしくは、不正な行動の記録が取れる仕組みが望まれる。

このような不正利用を防ぐためには、利用者計算機をネットワークに接続する際に、利用者認証を行なう必要がある。組織内の計算機端末の場合、UNIXもしくはWindowsNTのようなログイン認証機能を備えたものであれば、利用者認証は可能である。また、電話回線からの利用の場合、回線接続時の認証機構は既存のものが存在する。しかし、情報コンセントを介した利用に対しては、管理の手間がかからず、かつ、MACアドレスやIPアドレスの偽造にも対応した有効な方法は知られていなかった。

本研究の目的は、まず、情報コンセントにおけるネットワーク接続時の利用者認証の方法を考案し、その実現方法を明らかにすることである。この実現に際して、IPアドレスおよびMACアドレスの偽造にも対応できること、および、これらのアドレスの事前登録は不要であるなど、管理の手間も考慮したものであること[11, 20]が要求される。また、利用者の資格等に応じた自由度の高いアクセス制御機構であることが望ましい。

さて、接続時の認証ができたとしても、それだけでは十分なセキュリティーを確保できない。 ネットワークの個々のサービス毎の認証も必要となる。例えば、電子メールのようなサービスは、各々の端末から、直接メールサーバにメールの投函を依頼するが、このとき、通常認証は行なわれない[1]ので認証させるような仕組みも存在するが、端末側に特別なソフトウェアを用意しないといけないなどの制約がある。また、通信回線経由や情報コンセントを介したアクセスの場合、通常、端末側の管理は個人に任されており、端末を信用することはできないので、メールの発信者を詐称することは容易である。

本研究では、接続時の認証が行なえるという前提のもとに、このような電子メールの発信人の詐称を防止する方法を考案し、その実現方法を明らかにする[19]。

実現に際して、 信頼できる認証サーバの存在を仮定する。回線接続時に、 認証サーバによって、 予め登録されたユーザ名・パスワードの組で利用者認証を行い、 メールの発信時に認証サーバにより 利用者の確認を行う。 メールの発信者欄が正規の利用者でないとき, 正規の利用者名を別のヘッダとして付加してメールを送信する. これによってメールの偽造を抑止している。この方法では, クライアント側には一切の仮定を設ける必要はないという特徴を有している。

以下、2および3では、情報コンセントにおける接続時の利用者認証機構について述べ、4では、電子メールの発信時の認証機構について詳述する。

[1] 認証させるような仕組みも存在するが、末端側に特別なソフトウェアを用意しないといけないなどの制約がある。また、通信回線経由や情報コンセントを介したアクセスの場合、通常、末端側の管理は個人に任されており、末端を信用することはできない。

2　情報コンセントの利用者認証

2.1　要求項目

本稿において想定している利用環境では、情報コンセントは例えば図書館や情報センターなど不特定多数の人が出入り

する場所に設置されている。利用者は個人で所有する(もしくは管理する)計算機を情報コンセントに接続し、IPアドレス割り当てサーバから動的にIPアドレスの割り当てを受け、ネットワークにアクセスする。

本稿で述べる不正アクセス防止方式の目的は、このような環境において正規の利用者だけが情報コンセントに接続された計算機からネットワークに正規のIPアドレスを持つパケットを送出できるようにアクセス制御を行ない、またネットワーク利用時に誰がいつどこからどのIPアドレスを使ってアクセスしたかを記録できるようにすることである。そのためには、次の各機能が必要となる。

1. 利用者認証機能・アクセス記録機能
   ネットワークにアクセスしようとしている利用者が利用資格を有するかどうかを確認するために、利用者認証の機能が必要である。また、認証の際に、時刻、利用者名、情報コンセントの位置、割り当てたIPアドレスを記録する機能が必要である。
2. アクセス制御機能
   認証を受けた利用者だけが外部ネットワークにパケットを送出できるようにアクセス制御を行なう機能が必要となる。
3. 送信元IPアドレス偽造防止機能
   送信元IPアドレスは、IPネットワークにおいて送信元計算機を特定するための識別子である。IPアドレスの値は利用者が自由に設定できるが、IPアドレスから利用者を特定できるようにするためには、システムから割り当てたアドレス以外は使用できないようにしておく必要がある。すなわち、利用者が勝手なIPアドレスを使用すること、特に、送信元IPアドレスを他の利用者のIPアドレスへと偽造することを防止できる必要がある。
4. 送信元MACアドレス偽造防止機能
   送信元MACアドレスは、Ethernetなどのデータリンク層において送信元計算機を特定するための識別子である。ある送信元IPアドレスが、偽造されたものではなく、本来その計算機に割り当てられたものであることを確認するためには、送信元IPアドレスと計算機との対応をつける必要がある。このとき、計算機を識別するために必要となるのが送信元MACアドレスなので、これが偽造されないようにしておく必要がある。

2.2 不正アクセスの防止原理

本方式に基づくシステムは、利用者認証サーバ、IPアドレス割り当てサーバ、フレームフィルタ、情報コンセントハブから構成される（図1)。情報コンセントハブは利用者の計算機を接続する複数のポートを持ち、利用者の計算機からパケットを受け取って必要に応じて他のポートへ中継する。各ポートにはそれぞれポート識別子（たとえば、逐次的に振られた番号）を用意しておき、受け取ったパケットは各々ポート識別子に対応づけることができるものとする（このためには、例えばポート毎に接続可能なMACアドレスを限定できれば良い。詳しくは後述)。フレームフィルタは2つのネットワークインタフェースを持ち、情報コンセントハブから送られてきたフレームを（IPアドレス、MACアドレス、ポート識別子の3つ組に基づいてIPアドレス割り当てサーバ、利用者認証サーバ、およびバックボーンネットワークに中継するか破棄するかを制御できる。

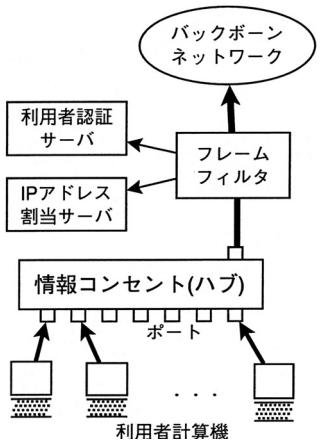

図1　情報コンセントにおける利用者認証システム

本システムは次のように動作する。

1. 初期状態では、情報コンセントの各ポートに接続された利用者計算機からはIPアドレス割り当てサーバに対してのみアクセス可能な状態としておく。

2．利用者は自己の計算機*C*を情報コンセントのポート*P*に接続する。
3．*C*は、IPアドレス割り当てサーバからIPアドレス*I*の割り当てを受ける。このIPアドレスは、接続時に動的に決定れる。
4．システムは、*C*から送られてきたIPアドレス要求パケットより*C*のMACアドレス*M*を取得し、ポート*P*からバックボーンに流入可能なパケットの送信元MACアドレスを*M*に、送信元IPアドレスを*I*に限定する。また、ポート*P*から利用者認証サーバへのアクセスを許可する。
5．*C*と利用者認証サーバとの間で利用者認証を行う。認証に成功すれば、利用者名、IPアドレス等を記録し、ポートPからバックボーンネットワークへのパケットの送出を許可する。

以上の動作により、\2.1で述べた機能を実現することが可能となる。

本方式の動作原理は、利用者の計算機を（IPアドレス、MACアドレス、ポート識別子）の3つ組に基づいて識別する点にある。本方式では、IPアドレスとMACアドレスの両者に加えて、ポート識別子という、利用者からは制御不可能な要素を利用してアクセス可能な計算機を限定しているため、送信者のIPアドレス・MACアドレスの偽造にも耐え得る不正アクセス防止を実現することができる。

しかも、本方式は（1）IPアドレスを動的に割り当てる、（2）MACアドレスを自動的に学習する、（3）利用者認証情報は既存のものを流用できる、などの特徴を有するため、本方式を導入することによって新たに管理上の負担が増加することはない。

3　システムの実現

本章では、前章で述べた方法を実現するシステム(LANA2と呼ぶ)の実装について述べる。

3.1　システム構成

LANA2は、LANAサーバ、LANAフィルタ、DHCPサーバ、RADIUS認証サーバ、VLAN機能付きスイッチングハブから構成される。

3.1.1　LANAサーバ

LANA2の中心となるサーバで、DHCPサーバやRADIUSサーバ、LANAクライアントと通信し、LANAフィルタやスイッチングハブを制御する。このサーバはマルチスレッドで実現されており、現在はSolaris 2.6およびFree BSD上で稼働するが、POSIX threadのあるOSならば移植は容易である。

LANA2では、基本部分がハブの持つ機能に依存しないよう、ハブを抽象化して扱っている。これによって、上位モジュールにとってハブの機種による設定コマンドの違いが隠蔽されているだけでなく、本稿で述べたVLANを利用した方法に加えて文献[17]で提案したフレームフィルタリング機能付ハブを使用する方法についても同一のサーバで扱うことが可能となっている。

3.1.2　LANAフィルタ

2つのネットワークインターフェースを持ち、一方をVLAN機能付きスイッチングハブに、他方をバックボーンネットワークに接続する。LANAフィルタは、2つのインターフェースの間でフレームを中継するものであり、フィルタリング機能とアクセス記録機能を持っている。今回は、FreeBSD 3.1上にBPF（Berkeley Packet Filter）を用いてユーザレベルプロセスの形で実装している。BPF機能を持つUNIX系OSへの移植は容易である。

フィルタリング機能

LANAフィルタは、指定された条件に基づいてフレームを通過させるべきか否かを決定し、許されたフレームのみを中継するフィルタリング機能を持つ。フィルタリングの条件として指定する要素には、（1）MACアドレス、（2）IPアドレス、（3）VLANタグ[2]、がある。また、（4）TCP/UDPポート番号、を条件に加えることにより、情報コンセントの利用者が使用できるサービスを限定することも可能である。我々の方式では、フレームはポート識別子、すなわち利用者の計算機と対応づけられているので、利用者ごとにサービスやアクセス先の限定が可能である。フィルタリングのための条件は、LANAサーバから設定される。

アクセス記録機能

LANAフィルタでは、通過するすべてのフレームをチェックすることが可能であるため、使用されたUDPのポート番号やTCPのポート番号を利用者ごとに記録したり、同時にTCPパケットのSYNビットやFINビットなどの情報をチェックすることによってTCPセッションの開始/終了時刻を記録するなど、利用者の各種の活動記録を取ることが可能である。

3.13　DHCPサーバ

図1におけるIPアドレス割り当てサーバに相当し、DHCPプロトコルによって利用者の計算機に対してIPアドレスを割り当てるサーバである。ISCのDHCPサーバをベースとして改造したものを使用している。

3.1.4 RADIUSサーバ

図1における認証サーバとして、ここでは、RADIUS[7]サーバを用いている。フリーの実装の1つであるDTC RADIUS[7]を使用した。RADIUSサーバでは、利用者の認証と、情報コンセント使用開始・終了の記録を行う。

[2] VALNタギングを利用する場合

3.1.5 VLAN機能付きスイッチングハブ

VLAN機能に加えて、MACアドレスフィルタリング機能ないしIEEE 802.1QVLANタギング機能を持つスイッチングハブであり、利用者の計算機が接続される。

ここでは、Cisco社製Catalyst 2912XLを使用した。ハブをコントロールするためには、LANAサーバからハブに対して制御用のtelnetセッションを開設し、これを利用してコマンドを実行させている。もちろん、SNMP(Simple Network Management Protocol)やシリアルラインによる制御としてもかまわない。

3.2 利用者認証

不正アクセス防止のためには、利用者の認証が必要である。LANA2では、認証のために利用者の計算機上で動作し、LANAサーバと通信して認証情報の交換を行うクライアントソフトウェア（LANAクライアント）を作成した。現在、Windows9x用にC++で記述したクライアントとJavaで記述したクライアントの2種類を用意している。

我々の提案する不正アクセス防止方式は、認証のために必ずしも専用クライアントを必要とするものではない。その代わりに、たとえばWWWやtelnetなどを用いてユーザ名とパスワードを入力させ、認証することも可能である。

3.3 動作の詳細

以下では、LANA2の具体的な動作について述べる。

1. 接続開始にあたって、利用者の計算機が接続されるポートをそれぞれ認証用のVLANに属するよう設定しておく。
2. 利用者は計算機を情報コンセント（ハブ）のポートPに接続し、DHCPシーケンスが開始される。この計算機（インターフェース）のMACアドレスをMとする。
3. DHCPサーバは、IPアドレス要求パケットからMACアドレスMを抽出し、これから利用者の計算機に与えようとするIPアドレスIとともにLANAサーバに通知する。
4. DHCPサーバはIPアドレスIを利用者の計算機に与える。
5. LANAサーバと（利用者の計算機で動作している）LANAクライアントの間で認証情報の交換を行う。LANAクライアントが存在しない（LANAクライアントからの応答がない）場合には、LANAサーバは利用者計算機が（WWW, telnetなどの手段によって）自発的に認証を行うまで待つ。
6. 認証に成功すると、LANAサーバは、利用者の計算機のMACアドレス、IPアドレスに加えて、ポートごとに定義されたVLAN（V_P）の情報を加えた（M, I, V_P）の組をLANAフィルタに伝え、これを充たすフレームがLANAフィルタを通過できるようにする。
7. ポートPの属するVLANを、V_Pに切り替える。

3.3.1 利用者計算機の切断検出

利用者が情報コンセントの利用を終了し、ネットワーク接続を切断する際には、LANAサーバはポートの設定を初期状態に戻し、RADIUS にログアウトを通知する。これは、以下の契機に行われる。

- LANAクライアント上で切断操作を行い, 切断通知がLANAサーバに送信された場合。
- ハブからSNMPトラップ（リンクダウントラップ）が送信された場合。これは利用者が情報コンセントからコネクタを引き抜く、あるいは利用者計算機の電源を切断することによって発生する。
- LANAサーバとLANAクライアント間のコネクションが切断された場合。
- LANAサーバからLANAクライアントへの存在確認要求に対して正しい応答がなかったとき。

4 電子メール送信時における認証機構

大学等の教育機関では、SPAM メールの中継拒否など他組織からの不正利用の防止も重要であるが、それにもまして自組織の利用者（主に学生）が不正利用を行わないようにすることが対外的な責務として重要である。そのためには、ユーザに対して電子メールの正しい利用法（ネットワークエチケット等）についての教育を徹底して行うことが必須であるが、それに加えて自組織の利用者による不正利用を抑制する仕組みを用意する必要がある。

このような仕組みの1つとして、メッセージの送信時に利用者を認証し、発信者の詐称を防止することが考えられる。これは SPAM メールの送付などの不正利用を直接防止するものではないが、不正利用が行われた場合でも発信者が特定できるため、不正利用を間接的に抑制する効果を持つ。

我々の提案している方式は、信頼できる認証サーバが存在する場合に、それを用いて発信者を確認し、発信者アドレスとの照合を行う。具体的には、PPP によるダイアルアップ環境や2章で述べた LANA システムを採用した情報コンセント環境などに適用が可能である。本方式では、利用者側には特別なプログラムを必要とせず、従来のクライアントプログラムをそのまま利用することができる。また、問題のあるメールを発見した際には柔軟なエラー処理が可能である。

4.1 設計方針

既存の方式の問題点を解決しつつ発信者詐称を防止するためには、電子メールシステムが次の各条件を満足する必要がある[19]。

1. 利用者が管理するクライアント計算機に特別なソフトウェアを必要とせずに利用者認証を行える
2. メッセージの送信にSMTPをそのまま利用できる
3. 認証した利用者と発信者アドレスを照合できる
4. 発信者詐称を検出した場合、柔軟な発信者詐称処理を行える

我々の方式では、既存のMTAと協調して動作するフロントエンドプログラムを導入する。このフロントエンドプログラムは SMTP によってMUAからメッセージを受け取るようになっており、利用者は従来のMUAをそのまま利用することができる。また、メッセージを受け取った際に、SMTPセッションを確立したままMUAの利用者を認証サーバに問い合わせ、メッセージ中の発信者アドレスと認証した利用者とを照合することができる。更に、照合の結果、発信者詐称を検出した場合には、SMTPセッション中に配送を拒否できるだけでなく、エラーメールとして本来の差出人に送り返したり、発信者を強制的に書き換えたりするなど、柔軟な発信者詐称処理が可能となる。

4.2 システム構成と動作

システム構成の例を2に示す。以下では、フロントエンドプログラムをauth-smtpdと呼ぶことにする。認証サーバにはRADIUSを使用しているが、利用者が設定を変更できないという条件が満たされればIDENTサーバ[4]などを使用することも可能である。

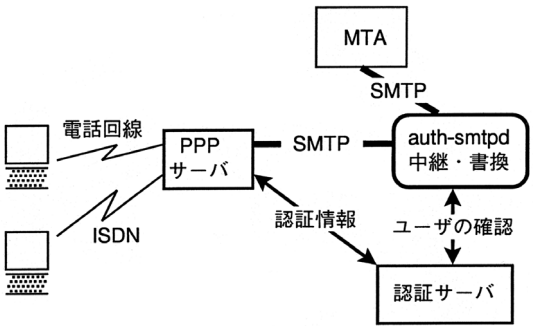

図2　電子メール発信者認証システム

次に、電話回線を使用してダイアルアップ接続した計算機からメッセージを発信する場合の動作を述べる。

1. 利用者は遠隔地から公衆電話回線などを介してクライアント計算機をリモートアクセスサーバに接続する。
2. リモートアクセスサーバは認証サーバと通信して利用者の認証を行い、正規の利用者であると認証すると、クライアント計算機からのネットワークアクセスを許可する。このとき、クライアント計算機の IP アドレスとユーザ名を記録する。
3. 利用者はクライアント計算機上の MUA を用いてメッセージを作成・発信する。MUA は電子メールサーバに SMTP で接続する。
4. 電子メールサーバでは、auth-smtpd が MUA からの SMTP 接続を受け付け、IPアドレスを基にクライアント計算機が監視対象であるかどうかを調べる。
5. クライアント計算機が監視対象であれば、auth-smtpd は認証サーバやリモートアクセスサーバと通信して、クライアント計算機のユーザ名を取得し、発信者詐称防止処理を行いながら MUA からの SMTP セッションをMTAに中継する。監視対象でなければ、MUA からの SMTP セッションを単に MTA に中継する。

6．MTA は auth-smtpd が中継した SMTP セッションを処理し、メッセージの配送を行う。

4.3 発信者詐称検出時の対応方法

本節では発信者詐称時の対応方法について議論する。

発信者の詐称行為として考えられるのは、SMTPセッション中のMAILコマンドに含まれる発信者アドレスとメッセージに含まれる From : ヘッダの発信者アドレスを詐称することである。

このうち、前者(reverse-path、一般にEnvelope Fromと呼ばれる)については、エラーメッセージを返す際に使用される情報であり, 確実に発信者のところへ戻る経路を提供する必要がある[1]ため、本来あるべきアドレス(ユーザ名とシステムのドメイン名から生成される電子メールアドレス)に強制的に書き換えを行う。この書き換えによって、不正行為によってユーザ名を偽った形でネットワーク接続を行わない限り、reverse-pathの詐称は不可能となる。また、reverse-pathは一般にシステムの動作記録の対象となるため、この強制書き換えにより動作記録の信頼性が増し、何らかの問題が生じた場合でも原因調査が容易になる効果も期待できる。

一方、後者の詐称を検出した場合の対応としては、次のような対応方法が考えられる。

1．SMTPセッション中にエラーとして配送を拒否する
2．エラーメールとして本来の発信者に送り返す
3．強制的に正しいアドレスに書き換える
4．From : には手を加えず、別途に発信者を示すヘッダ(Sender :)を付加する[3]
5．単に破棄する

我々の設計では、これらはいずれも実現可能であり、運用ポリシーによって選択することができるが、大阪市立大学学術情報総合センターの教育用システムにおけるダイアルアップサービスを対象とした設定では 4. を採用している。

[3] Sender : が既にあればその内容はX-Original-Sender : に、X-Original-Sender : があればさらにその前にX-Original-を付加することにより、元のヘッダを全て保存する。

5 おわりに

本稿では、教育用計算機システム環境において求められる認証のうち、特に情報コンセント利用における認証方法、ならびに、電子メール送信における認証方法について新しい方式を考案し、その実現について述べた。

前者の情報コンセントシステムに関しては、大阪市立大学学術情報総合センター内に設置された情報コンセントにおいて、実験運用を開始しており、後者については、同センターの教育用ダイアルアップ接続システムにおいて実際に運用している。また、岡山大学総合情報処理センターでもセンター内に設置されたパソコン端末のための電子メールサーバに導入され、稼働中である。

参考文献

[1] Postel, J.B.: Simple Mail Transfer Protocol, RFC 821, 1982
[2] Crocker, D.H.: Standard for the Format of ARPA Internet Text Messages, RFC 822, 1982.
[3] Rose, M.: Post Office Protocol - Version 3 Extended Service Offerings, RFC 1082, 1988.
[4] StJohns, M.: Identification Protocol, RFC 1413,1993.
[5] Myers, J., Rose, M.: Post Office Protocol - Version3, RFC1939, 1996.
[6] Crispin, M.: Internet Message Access Protocol -Version 4rev1, RFC 2060, 1996.
[7] Rigney, C. et. al.: Remote Authentication Dial In User Service (RADIUS), RFC 2138, 1997.
[8] http://www.sendmail.org/
[9] http://www.iecc.com/pop-before-smtp.html
[10] 松浦 敏雄、石橋 勇人、安倍 広多、藤川 和利 : “ 多人数教育用計算機システムの運用,” 第43回システム制御情報学会研究発表論文集、pp.71-72 (1999-05).
[11] 石橋勇人、阪本 晃、山井成良、安倍広多、大西克実、松浦敏雄 : “ 情報コンセントにおける認証とアドレス偽造防止をVLAN機能により実現するシステム LANA2 ”情報処理学会分散システム/インターネット運用技術研報、99-DSM-14, Vol.99, No.56, pp.137-142, (1999-07).
[12] 山井成良、中西 透、 安倍広多、石橋勇人、松浦敏雄、岡本卓爾 :“ IDENT代理サーバによるリモートアクセスユーザ認証機構,” 情報処理学会 分散システム/インターネット運用技術研報、99-DSM-15, Vol.99, No.77, pp.49-54 (1999-09).

[13] 阪本 晃、石橋 勇人、 山井 成良、安倍 広多、大西 克実、松浦 敏雄 :“ 情報コンセントにおける認証とアドレス偽造防止機構 の実現とその評価、” 情報処理学会第59回全国大会(平成11年後期)、5T5, 分冊3, pp.419-420 (1999-09)。
[14] 松浦 敏雄、石橋 勇人、安倍 広多 : “ 情報教育のための計算機環境、” 情処 コンピュータと教育研資、Vol.99, No.53, pp.41-47 (1999-10)。
[15] Hayato Ishibashi, Nariyoshi Yamai, Kota Abe, Katsumi Ohnishi and Toshio Matsuura : “ A Protection Method against Sender Spoofing in Email by Introducing an Authentication Server ”, Proc. of International Conference on Software in Telecommunications and Computer Networks, Vol. 7, pp. 259--268, FESB-Split, (Oct. 1999).
[16] 阪本晃、石橋勇人、安倍広多、山井成良、大西克実、松浦敏雄 : “ 教育用計算機環境における認証機構, ” 電子情報通信学会技術研究報告 FACE99-35, Vol. 99, No. 489, pp. 1--6 (1999-12).
[17] 石橋勇人、山井成良、安倍広多、大西克実、松浦敏雄 : “ IPアドレス/MACアドレス偽造に対応した情報コンセント不正アクセス防止方式 ”、情報処理学会論文誌, Vol.40, No. 12, pp.4353-4361 (1999-12).
[18] 中西 透、山井成良、安倍広多、 石橋勇人、松浦敏雄、岡本卓爾 : “ IDENT代理サーバによるリモートアクセスユーザ認証機構、” 情報処理学会論文誌(条件付き採録)。
[19] 石橋 勇人、 山井 成良、安倍 広多、大西 克実、松浦 敏雄 : “ 認証サーバを用いた電子メールの発信者詐称防止の一手法 ”,情報処理学会論文誌, (条件付き採録)。
[20] 石橋 勇人、 阪本 晃、山井 成良、安倍 広多、大西 克実、松浦 敏雄 : “ 情報コンセントにおける認証とアドレス偽造防止をVLAN機能により実現するシステムLANA2 ”、情報処理学会論文誌, (条件付き採録)。

＜発 表 資 料＞

題　　名	掲載誌・学会名等	発表年月
“ 多人数教育用計算機システムの運用 ”,	第43回システム制御情報学会研究発表論文集, pp.71-72	1999年5月
“ 情報コンセントにおける認証とアドレス偽造防止をVLAN機能により実現するシステムLANA2 ”,	情報処理学会分散システム/インターネット運用技術研報, 99-DSM-14, Vol.99, No56, pp.137-142	1999年7月
“ IDENT代理サーバによるリモートアクセスユーザ認証機構 ”,	情報処理学会分散システム/インターネット運用技術研報, 99-DSM-15, Vol.99, No77, pp.49-54	1999年9月
“ 情報コンセントにおける認証とアドレス偽造防止機構の実現とその評価 ”,	情報処理学会第59回全国大会（平成11年後期), 5T5, 分冊3, pp.419-420	1999年9月
“ A Protection Method against Sender Spoofing in Email by Introducing an Authentication Server ”,	Proc. of Int 'l Conf. on Software in Telecomm. and Computer Networks, Vol.7 pp.259--268, FESB-S	1999年10月
“ 教育用計算機環境における認証機構 ”,	電子情報通信学会技術研究報告 FACE99-35, Vol.99, No.489, pp.1-6	1999年12月
“ IPアドレス/MACアドレス偽造に対応した情報コンセント不正アクセス防止方式 ”,	情報処理学会論文誌,Vol.40, No.12, pp.4353-4361	1999年12月
“ IDENT代理サーバによるリモートアクセスユーザ認証機構 ”	情報処理学会論文誌,	条件付採録
“ 認証サーバを用いた電子メールの発案者詐称防止の一手段 ”	情報処理学会論文誌,	条件付採録
“ 情報コンセントにおける認証とアドレス偽造防止をVLAN機構により実現するシステム LANA2 ”,	情報処理学会論文誌,	条件付採録