IDENT 代理サーバによるリモートアクセスユーザ認証機構

中西 透[†] 山井成良[††] 安倍広多[†††]
石橋勇人[†††] 松浦敏雄[†††] 岡本卓爾[†]

IDENT プロトコルはアプリケーションレベルでのユーザ認証の手段として広く用いられている．しかしリモートアクセス環境では，ユーザの計算機がネットワーク管理者の管理外にあり，IDENT サーバが返すユーザ名が信頼できないために，IDENT プロトコルをそのまま適用することができない．本論文では，IDENT 代理サーバを導入し，ユーザの計算機に代わってネットワーク接続時の認証情報を返すことによりアプリケーションレベルでのユーザ認証を行う方法を提案する．また，本方法を実装した試作システムの試験運用および性能測定の結果からその有効性を示す．

An Authentication Mechanism for Remote Access Users with an IDENT Proxy Server

Toru Nakanishi,[†] Nariyoshi Yamai,[††] Kota Abe,[†††]
Hayato Ishibashi,[†††] Toshio Matsuura[†††] and Takuji Okamoto[†]

IDENT protocol is one of the most popular user identification methods on application layer. However, this protocol has not been used on remote access environment because an IDENT server on user's computer is not managed by the network manager and thus it is not trusted. In this paper, we propose a user identification method available even on remote access environment, by introducing an IDENT proxy which responds the user name authenticated on dial-up connection. Then, we show the usefulness of the method by empirical results of a trial system.

1. まえがき

近年，ネットワーク接続事業者の急速な増加や高速モデムなどの発達にともなって，ユーザが遠隔地から公衆電話網を経由して所属組織内のネットワークにアクセスするような利用形態（リモートアクセス）が急速に普及してきている．このような利用形態では，ユーザの計算機が組織内のネットワーク管理者ではなくユーザ自身の管理下に置かれており，また，ネットワーク管理者から離れた場所に設置されているために，様々な不正利用が発生している．なかでも特に，電子メールでのアドレス詐称や本来利用できないサービスでの偽のユーザ名を騙った利用などといったアプリケーションレベルでの不正利用が頻発している．このため，リモートアクセス環境におけるアプリケーションレベルでの不正利用を防止・抑制するための簡便な方法の開発が強く要求されている．

ネットワークにおける不正利用を防止・抑制するための有力な方法として，ユーザ認証が広く用いられている．リモートアクセス環境におけるユーザ認証には，PAP[1]，CHAP[2]などがあるが，これらはダイアルアップ接続時の認証を目的としたプロトコルであり，アプリケーションレベルでのユーザ認証には利用できない．他方，アプリケーションレベルでのユーザ認証の代表的な方法として，ディジタル署名[3),4)]や IDENT プロトコル[5)]を利用した方法が知られている．ディジタル署名による方法は厳密な認証が期待でき，原理的にリモートアクセス環境にも適用できるが，ユーザの計算機側での秘密鍵の管理のために負担が大きくなりすぎて，様々な種類の計算機が接続されるリモートアクセス環境に対して手軽に適用することはできない．それに対して，IDENT プロトコルによる方法は，TCP に基づいたアプリケーションのユーザ認証に限定されているものの，ユーザが秘密鍵などの秘密情報を管理

† 岡山大学工学部
Faculty of Engineering, Okayama University
†† 岡山大学総合情報処理センター
Computer Center, Okayama University
††† 大阪市立大学学術情報総合センター
Media Center, Osaka City University

する必要がないので，ユーザの計算機での負担は小さく，これまでに広く利用されている．しかし，ユーザの計算機がリモートアクセス環境にある場合には，これをリモートホストと見なしてIDENTサーバを実装したとしても，ネットワーク管理者の管理外にあるので，これが返すユーザ名は信頼できない．すなわち，この方法はそのままではリモートアクセス環境に適用できない．

本論文の目的は，リモートアクセス環境のもとで，ユーザの計算機に大きな負担を強いることなく，アプリケーションレベルでのユーザ認証を簡便に行う方法の開発にある．ここでは，この目的を達成するために，ダイアルアップ接続時の認証結果を保存しておき，これを利用して，ネットワーク管理者の管理下にある計算機上に導入したIDENT代理サーバにIDENTプロトコルによる問合せに対する応答をさせることにする．この場合，問合せに対してIDENT代理サーバが無条件にユーザ名を応答するようにすると，他のどの計算機からでも不正にユーザ名を取得できるようになってしまう．そこで，本論文では，IDENT代理サーバが問合せを受けたとき，TCPコネクションが実際に存在するか否かを確認し，存在した場合のみユーザ名を返すように配慮することにより，この問題を解決する．

以下本論文では，まず，ユーザ認証システムを構成する際の議論を明確にするために，従来のIDENTプロトコルの動作とその認証能力について述べ，構成の対象となるリモートアクセス環境を定義する．次に，この環境のもとでIDENT代理サーバを導入したユーザ認証システムの構成法を示す．最後に，このユーザ認証システムの試作を行い，このシステムの有効性を確かめる．

2. 準　　備

2.1 IDENTプロトコル

本論文では，リモートアクセス環境でのアプリケーションレベルにおける認証を行うために，IDENTプロトコル[5]を利用する．IDENTプロトコルとは，TCPに基づいたアプリケーションにおいて，サーバプログラムがクライアントプログラムのユーザ名を取得するために利用されるプロトコルである．ここで，サーバプログラムおよびこれに対応したクライアントプログラムをそれぞれSPおよびCPとし，CPの実装された計算機上ではIDENTサーバISが動作しているものとする．ユーザがCPからSPのサービスを利用する場合，まず，SP–CP間にコネクションCが確立される．そして，SPによるCPのユーザ名取得は，IDENTプロトコルにより以下の手順で実行される．

(1) SPはCの相手側のIPアドレスとポート番号を取得し，このアドレスを用いてISとの間にコネクションを確立する．
(2) SPはISにCの両端のポート番号を送る．
(3) ISはSPの動作している計算機のIPアドレスを求め，このアドレスと自計算機のIPアドレスおよび(2)で受け取ったポート番号から特定されるCが存在するかどうか確認する．
(4) Cの存在が確認されれば，ISはコネクションCを確立したユーザの名前を応答し，さもなければ，エラーメッセージを応答する．

ここで，Cの両端のIPアドレスはSP–IS間のコネクションから求められるので，手順(2)ではISに両端のポート番号だけが送られることに注意する．

IDENTプロトコルをユーザ認証として利用するためには，クライアントプログラムの動作している計算機においてIDENTサーバが動作しており，さらにこれが信頼できるユーザ名を返すことが前提となる．リモートアクセス環境では，クライアントプログラムの動作しているリモートアクセス計算機はネットワーク管理者の管理外にあり，これが返すユーザ名は信頼できないため，IDENTプロトコルをそのまま用いてユーザ認証を行うことは危険である．そこで本論文では，ネットワーク管理者の管理下にある計算機上に導入したIDENT代理サーバにIDENTプロトコルによる問合せに対する応答をさせることにより，リモートアクセス環境におけるアプリケーションレベルでのユーザ認証を実現する．

2.2 リモートアクセス環境

リモートアクセス環境においては，多くの場合，ユーザがその組織内のネットワークに対するアクセス権を有するか否かを調べるために，すでに述べたダイアルアップ接続時の認証が行われる．そこで本論文では，このような状況に配慮し，ユーザ認証の対象とするリモートアクセス環境として，**図1**のようなネットワーク構成を想定する．破線で囲んだ部分は組織内のネットワークであり，その組織のネットワーク管理者の管理下にある．RASおよびASは，それぞれ，リモートアクセスサーバおよびダイアルアップ接続用の認証サーバである．また，LNはこれ以外の組織内のネットワークであり，種々のサービスを提供する計算機群が存在する．これらの中には，IDENTプロトコルを利用したサーバプログラムが実装されているものとし，これらの任意のものをSPで表す．他方，破線外にある $RC_1, RC_2, \ldots, RC_n$ は，遠隔地のユーザが利用す

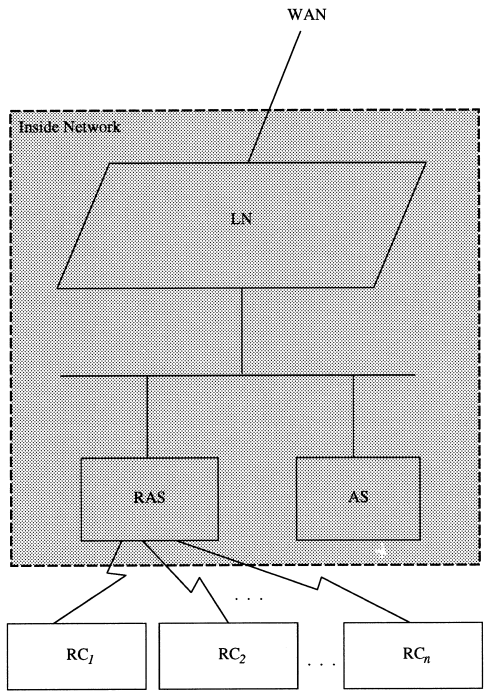

図 1 リモートアクセス環境におけるネットワーク構成
Fig. 1 Network structure on remote access environment.

る計算機（リモートアクセス計算機）であり，それぞれユーザ自身の管理下にある．RC_i $(1 \leq i \leq n)$ には上で述べたダイアルアップ接続時の認証のためのソフトウェアが実装されているが，その種類や搭載されている OS は任意である．なお，LN から組織のネットワーク外へ向かう実線は，広域ネットワークへの接続を示す．

ここでは，以降の議論を明確にするために，次の仮定を設ける．

(a) RC_i を利用するのは，ダイアルアップにより接続してからこれを切断するまでの間，同一のユーザである．

リモートアクセス環境では，ほとんどの場合において，リモートアクセス計算機のユーザはダイアルアップ接続でのみ外部と接続する．本論文では，より強めて，リモートアクセス計算機のユーザは必ずダイアルアップ接続でのみ外部と接続することを前提とする．この場合において，ダイアルアップにより接続してからこれを切断するまでの間，RC_i のユーザが同一でない状況が発生するのは，正規のユーザ A が別の者 B に対して自発的に A の計算機の使用を許す場合だけである．ゆえに，B の不正の責任は A の責任であり，仮定 (a) を設けてもさしつかえないといえる．

図 1 のネットワークにおいて RC_i を LN に接続してサービスを利用する場合，まずユーザは RC_i から RAS に接続要求を行う．その後，RAS が AS と通信を行い，RC_i のユーザを認証する．RC_i のユーザがこのネットワークへのアクセス権を有する者である場合のみ，RAS は RC_i に IP アドレスを割り当て，LN への接続を許可する．

3. リモートアクセス環境におけるユーザ認証

3.1 ユーザ認証システムの構成方針

本論文では 1 章で述べたように，RC_i のユーザ認証を行うために，2.2 節で述べたリモートアクセス環境のもとで，ネットワーク管理者の管理下にある計算機上に設けた IDENT 代理サーバが，接続時の認証結果を利用して IDENT プロトコルの問合せに応答するという方針をとる．

ここでは，このようなユーザ認証システムの構成にあたって，さらに以下の仮定を設ける．

(b) 組織内のネットワークにおいて不正行為が行われない．また，広域ネットワークおよびリモートアクセス計算機から組織内のネットワークに対して，IP アドレス・ポート番号の偽造などによる不正アクセスを行えない．

(c) ダイアルアップにより接続してからこれを切断するまでの間，RC_i を利用しているユーザの名前と RC_i に割り当てられた IP アドレスの組が，AS に保存されている．以下，このユーザ名を U_i，IP アドレスを AR_i と略記する．

仮定 (b) は，アプリケーションレベルでの認証に限らず，組織のネットワークの運用全般における前提条件である．これらは，組織内のネットワークを適切に管理し，さらにファイアウォールなどによりアクセス制御を行えば，高いレベルで達成できる．また，仮定 (c) については，たとえば RADIUS[6),7)] など，多くの AS ではダイアルアップ接続時の接続記録を残すことが可能であり，この記録を用いて U_i と AR_i の組を保存することは容易である．以上のことから，仮定 (b), (c) を設けたとしても実用上さしつかえないと考えられる．

仮定 (a), (b), (c) から，代理サーバが AS より RC_i のユーザ名を取得し，IDENT プロトコルの問合せに対する応答として送出することにより，RC_i のユーザ認証が行える．

前述した方針のもとでユーザ認証を行う場合，何らかの手段により，SP から RC_i の IDENT サーバに向けて発せられる問合せを，IDENT 代理サーバに向けて発せられるように変更することが必要である．しか

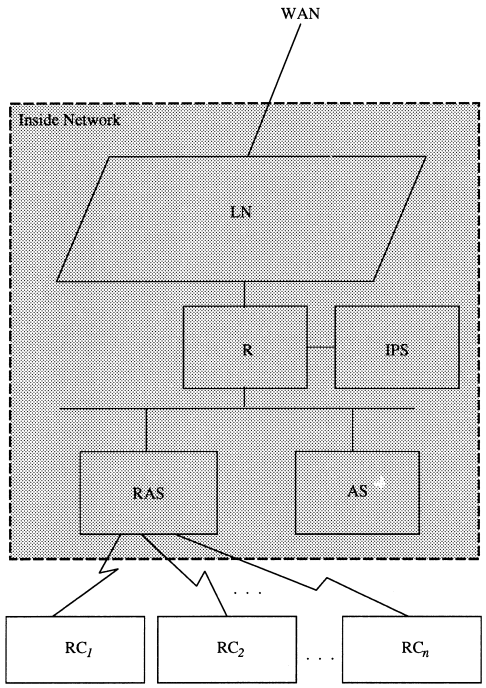

図 2 リモートアクセス環境におけるユーザ認証を行うためのネットワーク構成
Fig. 2 Network structure to authenticate users on remote access environment.

し，IDENT プロトコルを利用しているサーバプログラムが LN 内の計算機に数多く実装されていると想定する以上，これらのプログラムを改造することによりこの変更を実現することは望ましくない．そこで，**図 2** に示すように，RAS と LN の間に新たにルータ R を設け，RC_i に対する IDENT プロトコルの問合せを，IDENT 代理サーバ IPS に転送させるようにする．ここでは，このような転送を実現するための手法として，アドレス変換機構（Network Address Translator：以下，NAT と呼ぶ）[8] を採用し，SP から RC_i への問合せを IPS への問合せに置き換える．

3.2 代理応答にともなう問題点とその解決策

R 上の NAT によって SP と RC_i との通信を SP と IPS との通信に置き換える単純な方法として，RC_i の IP アドレス AR_i だけを IPS の IP アドレスに書き換えることが考えられる．しかし，この方法では，書き換えられる前のリモートアクセス計算機の IP アドレスの情報が失われてしまうにもかかわらずコネクションの両端のポート番号しか送られないため，IPS はどのリモートアクセス計算機への問合せであるかを特定できなくなってしまう．そこで，この問題を解決するために，各 AR_i と対応づけたポートを IPS 側に n 個用意し，R において IP アドレスだけでなくポート番号も変換するようにする．このときの R の動作は，IPS の IP アドレスを AI，RC_i に対する IPS 上のポート番号を PI_i とすると，以下のようになる．

(i) 送信先 IP アドレスおよび送信先ポート番号がそれぞれ AR_i および 113（IDENT のポート番号）であるパケットを受信すると，それぞれを AI および PI_i に変換して IPS に中継する．
(ii) 送信元 IP アドレスおよび送信元ポート番号がそれぞれ AI および PI_i であるパケットを受信すると，それぞれを AR_i および 113 に変換して SP に中継する．

次に，IPS が問い合わせられたコネクションの存在をいかにして確認するかについて述べる．図 2 の構成において RC_i のユーザが SP を利用する場合，RC_i 上のクライアントプログラムと SP との間に IPS を経由することなくコネクションが確立され，その後，(i) に基づいて SP から IPS への問合せが行われ，IDENT プロトコルによる認証が開始される．したがって，IPS 単独では SP と RC_i との間のコネクションの存在を判断できない．この場合，コネクションの存在を確認せずに，IPS へのすべての問合せに対して無条件に RC_i のユーザ名を応答する単純な方法も考えられるが，どの計算機に対しても同様にユーザ名を応答するために，ユーザ名が不正取得される危険性がある．そこで，本論文では，R で IP パケット中の SYN フラグ，RST フラグ，FIN フラグを監視してコネクションの状態を管理し，IPS からの問合せに対してコネクションの有無を応答するようにする．

コネクションの確立および解放を監視するための機能を持つルータは筆者らの知る限り市販されていないが，UNIX 系の OS を搭載した計算機上でこのような機能を持つプログラムを実装することは容易であると考えられる．

以上から，存在しないコネクションに対する問合せがあった場合でも，ISP はエラーを返すことができ，ユーザ名が不正取得される危険性を回避することができる．

3.3 ユーザ認証の手順

サーバプログラム SP に対する RC_i のユーザ U_i のクライアントプログラムを CP_i とし，CP_i が用いるポート番号を PR_i とする．このとき，本論文で提案するユーザ認証の手順を整理すると以下のようになる．

(1) U_i は RC_i で CP_i を起動する．CP_i は SP との間にコネクション C_i を確立する（**図 3** (a)）．このとき，R は C_i の確立を認識し，その両

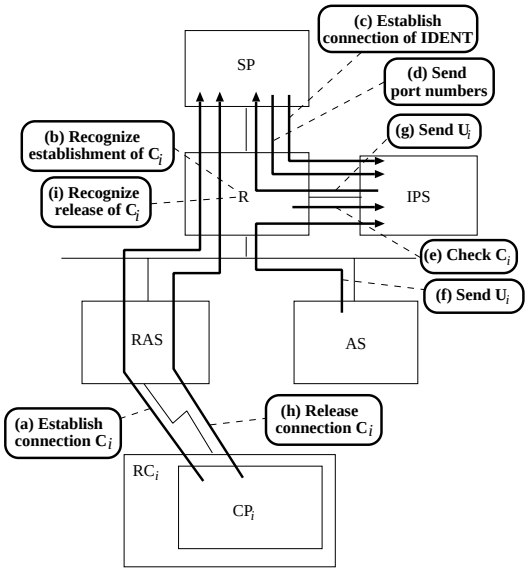

図 3 ユーザ認証の手順
Fig. 3 Process to authenticate users.

端の IP アドレスおよびポート番号を記録する（図 3 (b)）.

(2) SP は C_i の相手側の IP アドレス AR_i およびポート番号 PR_i を取得する.

(3) SP は IP アドレス AR_i・ポート番号 113 との間に IDENT プロトコルのコネクションを確立しようとする．R はこのコネクションを用いる通信に関して，SP の通信相手の IP アドレス・ポート番号を，AR_i・113 から AI・PI_i になるように変換して中継する．この結果，IDENT プロトコルのコネクションは，SP と IPS との間に確立される（図 3 (c)）.

(4) SP は IPS にコネクション C_i の両端のポート番号を送る（図 3 (d)）.

(5) IPS は受信したポート番号から AR_i を取得し，SP との間のコネクションの情報より SP の動作している計算機の IP アドレスを得る.

(6) IPS は (5) で得られた C_i の両端の IP アドレスおよび (4) で得られた C_i の両端のポート番号を R に渡し，C_i の有無を問い合わせる．R は現在確立されているコネクションの記録を調べ，C_i の有無を IPS に返す（図 3 (e)）.

(7) IPS は C_i の存在が確認できなかった場合には SP にその旨を伝え，処理を終了する．C_i の存在を確認した場合には，AS に AR_i を渡し，RC_i のユーザ名を問い合わせる．AS は問合せに対して U_i を返す（図 3 (f)）.

(8) IPS は SP に U_i を返す（図 3 (g)）．SP は CP_i のユーザが U_i であることを確認し，処理を続ける.

(9) SP は処理を完了し，コネクション C_i を解放する（図 3 (h)）．R はこの解放を検出し，C_i に関する記録を削除する（図 3 (i)）.

前述した手順の本システム上での流れを図 3 に示す．各矢印あるいは R に付した処理内容 (a)〜(i) は，各手続きの括弧内に記した (a)〜(i) に対応している.

前記の手順から明らかなように，本論文の方法では，RC_i に新たにソフトウェアを導入する必要がないので，ユーザに負担をかけずにユーザ認証が行える．また，SP を改造する必要がないため，管理者の負担も小さい.

4. ユーザ認証システムの実装

4.1 試作システムの構成

これまでに述べた方式の有効性を確認するために，ユーザ認証システムの試作を行った．試作したシステムの構成を**図 4** に示す．この図から分かるように，このシステムでは 1 台の計算機にリモートアクセスサーバ（pppd），IDENT 代理サーバ（ident proxy），ルータ（natd）のすべての機能を持たせている．この構成では，ユーザ認証のための情報がこの計算機自身で管理されているため，認証サーバは不要となっている.

この計算機はいわゆる AT 互換機で，OS として FreeBSD-2.2.7 を搭載している．リモートアクセスサーバとしては IIJ-PPP を用いている．仮定 (c) におけるユーザ名と IP アドレスの対応の記録は，IIJ-PPP により wtmp ファイルに記録される．また，3.3 節の (7) におけるユーザ名の取得は，IDENT 代理サーバが last コマンドを用いて wtmp ファイルから取得するようにしている．ルータの機能は OS 自身が有しているが，コネクション管理機能ならびにアドレス変換機能は natd プログラムを一部修正したものを用いて実現している．主な修正点は，アドレス変換を必要としない通信についてもコネクションを管理するようにした点と，コネクションの確立・解放をファイル（connection log）に記録するようにした点である．3.3 節の (6) におけるコネクションの存在の確認は，ファイルに残されたコネクションの確立・解放の記録を分析するプログラムを新たに作成し，このプログラムに担当させている．また，IDENT 代理サーバも新たに作成したプログラムであり，RC_1 および RC_2 に対応したポートで問合せを待つ inetd により起動される.

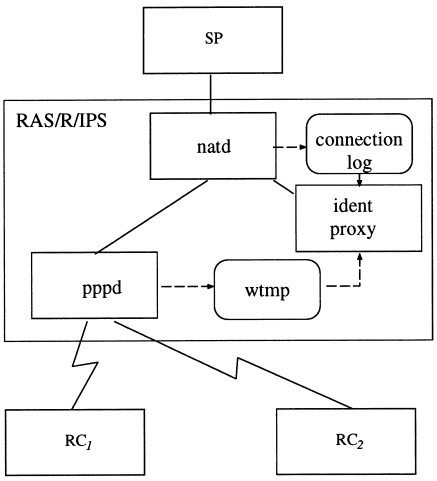

図 4 試作システムの構成
Fig. 4 Structure of trial system.

4.2 動作確認

図 4 の構成において，IDENT 代理サーバが正しく機能するか否かを確認するために，試験運用を行った．以下その結果を述べる．

まず，IDENT プロトコルによりユーザ情報を得るためのプログラムの代表として sendmail を取り上げ，試験した．sendmail は標準で IDENT プロトコルによる発信者情報の取得を行い，ヘッダに付加する機能を有している．そこで試験では sendmail をサーバ計算機上で動作させ，リモートアクセス計算機からメッセージを送信した．その結果得られたヘッダの一部を**図 5** に示す．リモートアクセス計算機はユーザ kenya が利用しており，IP アドレスとして 150.46.254.3 が割り当てられている．ユーザ kenya はメッセージをサーバ計算機 ruin に発信する際，その From アドレスを 1 行めに示すように yamai@cc.okayama-u.ac.jp と偽ったが，2 行めに示すように Received ヘッダには (kenya@[150.46.254.3]) のようにリモートアクセス計算機のユーザ名と IP アドレスが記録されている．これにより，IDENT 代理サーバは正しく動作していることが分かる．

次に，IDENT プロトコルを用いてアクセス制御を行うプログラムとして tcpd を取り上げ，試験を行った．tcpd は TCP による種々のサービスへの接続要求を監視し，アクセスを制御したり通信記録をとったりするためのプログラムであり，その中には，IDENT プロトコルによりクライアントのユーザ名を求め，得られたユーザ名とクライアントの IP アドレスの組に基づいてアクセス制御を行う機能が含まれている．

試験では，サーバ計算機 ruin 上で tcpd を動作させ，tcpd の設定ファイルに対してユーザ kenya からのアクセスだけを許可するように設定して，shima と kenya の 2 通りのユーザ名でリモートアクセス計算機を接続し，finger コマンドでサーバ計算機にアクセスした．その結果，kenya からのアクセスだけが許可されることが確認された．また，このとき tcpd が出力したログを**図 6** に示す．これらにより，IDENT 代理サーバは正しく動作し，tcpd がユーザ kenya からのアクセスだけを許すように機能していることが分かる．

以上の 2 例から，IDENT 代理サーバはリモートアクセス計算機のユーザを認証でき，IDENT プロトコルを用いる既存のプログラムと組み合わせて用いることができることが確認された．

4.3 評価

本論文で述べたユーザ認証システムの有効性を示すために，同時にリモートアクセスしているユーザの数 n が 1 の場合に限定して，図 4 の構成のもとで，以下の測定を行った．このときの pppd とリモートアクセス計算機との間の通信速度は 33600 bps であった．

まず，サーバプログラムが IDENT プロトコルのコネクションを確立し，認証終了後にこのコネクションを解放するまでの時間を測定した．また，従来の IDENT プロトコルを用いた方法と比較するために，図 4 において IDENT 代理サーバの代わりに IDENT サーバを動作させ，これに対して IDENT プロトコルを行った場合について，同様の測定を行った．その結果，100 回の測定における平均処理時間は，本システムの場合は 27 ms であり，従来の方法の場合は 4.7 ms であった．従来の方法と比較すると，本システムの処理時間は増加しているが，IDENT プロトコルを利用するプログラムの全体の処理時間（sendmail においては数秒程度）を考慮すると，十分小さいといえる．

次に，リモートアクセス計算機とサーバ計算機との間での，コネクション確立・解放時間および伝送速度の測定を行った．このうち，コネクション確立・解放時間については，リモートアクセス計算機上で，コネクション確立を行い，確立後ただちにこれを解放するというプログラムの実行時間を 100 回測定し，その平均値を求めた．また，伝送速度については，リモートアクセス計算機とサーバ計算機との間で ftp を用いて 387189 bytes のデータを伝送し，その速度を 10 回測定して，その平均値を求めた．なお，本システムを導入しない場合と比較するために，図 4 において natd を経由しないようにシステムを構成し，同様の測定を行った．これらの結果を**表 1** に示す．この表より，natd を経由する場合としない場合との間には差がな

```
From yamai@cc.okayama-u.ac.jp Fri Jan 22 22:09:01 1999
Received: from cc.okayama-u.ac.jp (kenya@[150.46.254.3])
        by ruin.cc.okayama-u.ac.jp (8.8.8/8.8.8) with ESMTP id WAA02023
        for <kenya@ruin.cc.okayama-u.ac.jp>; Fri, 22 Jan 1999 22:11:52 +0900 (JST)
        (envelope-from yamai@cc.okayama-u.ac.jp)
```

図 5 sendmail における認証例
Fig. 5 Authentication example on sendmail.

```
Feb  6 18:24:07 ruin fingerd[1044]: refused connect from shima@150.46.254.3
Feb  6 18:24:22 ruin fingerd[1045]: connect from kenya@150.46.254.3
```

図 6 tcpd における認証例
Fig. 6 Authentication example on tcpd.

表 1 リモートアクセス計算機とサーバ計算機との間の通信特性
Table 1 Communication characteristic between remote access computer and server computer.

	natd を経由する場合	natd を経由しない場合
コネクション確立・解放時間	0.13 ms	0.13 ms
伝送速度	6.7 KB/s	6.7 KB/s

いといえる．

ここでは，同時にリモートアクセスを行っているユーザの数 n が 1 の場合の測定を行ったが，1 つの組織のネットワークでは，n は数百程度まで増大しうる．そこで次に，n が 1 の場合の測定結果をもとに，n が数百程度まで増大した場合の認証時間の考察を行う．n が 1 の場合における 27 ms という認証時間は，前記のように，IDENT プロトコルを利用するプログラムの全体の処理時間に比べて十分小さい．このため，n の値が数百程度まで増大しても，同時に複数の IDENT プロトコルによる認証が行われる状況は稀である．そこで，以下，同時に複数の認証はないものとして検討する．

3.3 節に記述した提案システムの手順において，(3) の IDNET プロトコルのコネクションの確立から (8) のユーザ名の取得までが認証の処理である．これらの各手順の中で n の増大が処理時間に影響を及ぼす可能性があるのは，(3) の IP アドレス，ポート番号の変換のための検索，(6) のコネクション存在確認のための検索および (7) のユーザ名取得のための検索である．まず，IP アドレス，ポート番号の変換のための検索については，実装に用いた natd では，ハッシュ表を利用しているため，n の増大は検索時間にほとんど影響を与えない．また，コネクション存在確認のための検索でも，実装した ident proxy は connection log からコネクションの存在を示すハッシュ表を生成し，その表を利用して検索しているため，n の増大は検索時間にほとんど影響を与えない．これに対して，ユーザ名の取得は，その実装において，リモートアクセス計算機から接続されるポートに対応した端末で限定して last コマンドを実行しユーザ名を取得している．このとき last コマンドは現時点から当該ユーザがダイアルアップ接続した時刻までの間の wtmp ファイル中のアクセス記録を線形探索するため，n が増大すると，この間のアクセス記録が増加して last コマンドの実行時間増加につながると考えられる．この問題は次のように実装を変更することで解決できる．ident proxy において，ポートに対応した端末とリモートアクセス計算機に割り当てる IP アドレスの対応をあらかじめハッシュ表として保持させておく．そして，wtmp ファイルを監視し，ダイアルアップ接続しているユーザとその端末の対応を取得して，その対応をハッシュ表として保持させる．これら 2 つの表を利用すれば，ident proxy は IP アドレスからそのリモートアクセス計算機を利用している者のユーザ名を知ることができる．このようにすれば，ハッシュ表を用いるため，n の増大は検索時間にほとんど影響を与えない．また，この変更によるオーバヘッドもほとんどないと考えられる．以上から，n の値が増大した場合においても，認証時間の増大はほとんどないといえる．

また，natd による IP アドレス，ポート番号の変換に要する時間は n の増大の影響を受けないことから，通信特性に関しても，n の増大の影響を受けないと考えられる．

5. ま と め

本論文では，リモートアクセス環境の下でアプリケーションレベルでのユーザ認証を簡便に行う方法として，IDENT 代理サーバを導入し，これにダイアルアップ接続時に認証したユーザ名を応答させる方法を提案した．また，この方法を実装し，既存のアプリケーションプログラムから IDENT プロトコルによりユーザ認証が行えることを運用試験により確認した．さらに，この実装されたシステムに対して，認証の処理速度およびシステム導入による通信への影響度を測

定し，このシステムが実用的な性能を有することを確認した．

この方法は既存のアプリケーションプログラムに何ら変更を加える必要がないため，多くのリモートアクセス環境に適用できると思われる．しかし，現在の構成では組織外で動作しているアプリケーションから見るとIDENT代理サーバが信用できるかどうか分からないため，本方法はIDENT代理サーバと同一組織内で動作しているサーバプログラムから認証を行う場合にしか適用できない．今後の課題としては，他組織のIDENT代理サーバが信頼できるか否かを認証できる機構を導入し，前記の問題点を解決することがあげられる．

参 考 文 献

1) Lloyd, B. and Simpson, W.: PPP Authentication Protocols, RFC 1334, IETF (1992).
2) Simpson, W.: PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, IETF (1996).
3) Atkins, D., Stallings, W. and Zimmermann, P.: PGP Message Exchange Formats, RFC 1991, IETF (1996).
4) Netscape Communications Corporation: Introduction to SSL. http://developer.netscape.com/docs/manuals/security/sslin/contents.htm (1998).
5) Johns, M.S.: Identification Protocol, RFC 1413, IETF (1993).
6) Rigney, C., Rubens, A., Simpson, W. and Willens, S.: Remote Authentication Dial In User Service (RADIUS), RFC 2138, IETF (1997).
7) Rigney, C.: RADIUS Accounting, RFC 2139, IETF (1997).
8) Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC 1631, IETF (1994).

(平成11年11月11日受付)
(平成12年 9 月 7 日採録)

中西　透

平成7年大阪大学大学院基礎工学研究科（物理系専攻情報工学分野）博士前期課程修了．平成10年同博士後期課程退学．同年岡山大学工学部情報工学科助手．平成12年同大学通信ネットワーク工学科助手．情報セキュリティ，ネットワークセキュリティに関する研究に従事．電子情報通信学会会員．

山井　成良（正会員）

昭和61年大阪大学大学院工学研究科（電子工学専攻）博士前期課程修了．昭和63年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程中退．同年奈良工業高等専門学校情報工学科助手．平成2年同講師．平成6年大阪大学情報処理教育センター助手．平成7年同大学大型計算機センター講師．平成9年岡山大学総合情報処理センター助教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．博士（工学）．IEEE，電子情報通信学会各会員．

安倍　広多（正会員）

平成4年大阪大学基礎工学部情報工学科卒業．平成6年同大学大学院博士前期課程修了．同年NTT入社．平成8年大阪市立大学助手．マルチスレッド機構の実装，オペレーティングシステムの設計等に興味を持つ．博士（工学）．電子情報通信学会会員．

石橋　勇人（正会員）

昭和62年京都大学大学院工学研究科修士課程情報工学専攻修了．平成元年同博士後期課程情報工学専攻退学．同年京都大学大型計算機センター助手．平成10年より大阪市立大学学術情報総合センター講師．高速ネットワーク，ネットワーク管理システム等に関する研究に従事．人工知能学会，電子情報通信学会，IEEE，ACM各会員．

松浦 敏雄（正会員）

昭和 50 年大阪大学基礎工学部情報工学科卒業． 昭和 54 年同大学大学院基礎工学研究科（情報工学専攻）後期博士課程退学後，同大学基礎工学部助手．平成 4 年同大学情報処理教育センター助教授，平成 7 年大阪市立大学教授．ユーザインタフェース，マルチメディア，情報教育等に興味を持つ．工学博士．ACM，IEEE，電子情報通信学会各会員．

岡本 卓爾（正会員）

昭和 33 年大阪大学工学部通信工学科卒業．同年川崎重工業（株）入社．昭和 35 年三井造船（株）転社．昭和 42 年岡山大学工学部奉職．現在，同大学通信ネットワーク工学科教授．平成 9 年より同大学総合情報処理センター長併任．主に論理回路を中心とした計算機ハードウェアの研究に従事．工学博士．電子情報通信学会，電気学会，IEEE 各会員．