情報処理学会論文誌 Vol. 49 No. 7 2614–2622 (July 2008)

IP パケット認証ゲートウェイシステム AIPS

安井浩之[†1] 松山実[†1]

PDA のような携帯端末の普及にともない，さまざまな場所でのネットワーク接続を可能とするため，無線 LAN のアクセスポイントや情報コンセントの設置が必要となる．このようなネットワーク環境の場合，ネットワーク内外に対するセキュリティの観点からも不特定者の利用を排除する必要があり，ユーザ認証の機能が不可欠となる．情報コンセントにおけるユーザ認証では，いったん認証が完了した携帯端末（ノートパソコンなど）の MAC アドレスや IP アドレスを偽装することによる第三者の通信を防ぐため，キープアライブのような仕組みが用いられているが，トラブルなどにより途切れると改めて認証が必要になるといった問題がある．我々はこのような問題が発生しない新たな認証システムとして，すべての IP パケットに認証情報を付加する認証システムを提案している．本論文では，この認証システムについて説明するとともに，実験環境での運用結果について報告する．

IP Packet Authentication Gateway System AIPS

Hiroyuki Yasui[†1] and Minoru Matsuyama[†1]

Along with the wide use of mobile computers, the installation of wireless LAN's access points or ethernet jacks is needed to enable network connection at various places. In such network environments, a user authentication function is indispensable to reject the connection by an unspecified third-party user for security of inside and outside of the network. As a user authentication function for the most ethernet jacks, a keep-alive mechanism is introduced to prevent the connection by an unspecified third-party user with a spoofed MAC or IP address of authenticated mobile computer. However, the keep-alive mechanism has a problem that the re-authentication is necessary if the keep-alive is suspended. We are proposing an authentication system which embeds authentication information into the header of all IP packets to avoid this problem. In this paper, described are the scheme of the authentication system and discussion on the operation result obtained in our experimental environment.

1. はじめに

ノートパソコンや PDA のような携帯型の端末機器（以下，携帯端末）の普及にともない，これらの機器のネットワーク接続を可能とするため，さまざまな場所に無線 LAN アクセスポイントや有線の情報コンセントが設置され始めているが，ネットワーク内外に対するセキュリティの観点からも不特定者の利用を排除する機能は必須である．

無線 LAN アクセスポイントの場合は，WEP や WPA，WPA2 といった比較的普及している機能によって利用者の制限を行うことが可能であり，IEEE802.1x のようなユーザ認証機能により，誰がネットワークを利用したかの記録を残すことも可能となっている．一方，有線の情報コンセントの場合も，IEEE802.1x のようなユーザ認証機能を有するネットワークスイッチや認証ゲートウェイのような製品[1)] で，接続ポート単位のユーザ認証を行い，IP アドレスや MAC アドレスに対するアクセス制御を行うことが一般的である．しかし，正規の接続終了手続きを行わずに携帯端末を取り外したり，ポートの先がハブなどで分岐されていたりすると，IP アドレスや MAC アドレスの偽装により第三者の通信が可能となってしまうため，その回避策として，認証を受けた携帯端末と認証用装置の間に接続確認コネクション（キープアライブ）を保持し，コネクション切断と同時に通信を遮断にする方法が提案・実装されている[2)–5)]．

これらのシステムにはキープアライブのために専用のプログラムをインストールして使用するものとブラウザ（Java Applet などを含む）や telnet のように一般的な PC に備わっているプログラムを用いるものとがある．前者は利用者に新たなプログラムをインストールさせる負担が生じることから，後者のようなシステム，特にブラウザを用いるシステムが有利であるという考え方が主流である．しかし，キープアライブ用のプログラム（ブラウザなど）を終了すると通信が遮断されるという点を考慮すると，後者が有利とはいいきれない．

情報コンセント環境の利用者の多くは，ブラウザによるインターネットアクセスを行っていると想定されるため，誤ってブラウザを終了してしまう可能性も高い．その結果，キープアライブ通信ができなくなり，通信が遮断，引き続きインターネットアクセスを行うためには，再度の認証が必要となる．ブラウザ以外の一般的なプログラム（telnet など）を使う場合でも，本来は別の用途に用いるプログラムではあるが，認証が終わった後も通信許可を維

†1 武蔵工業大学
Musashi Institute of Technology

持するために動作させ続けなければならない，というシステムの仕組みを利用者に意識させる必要がある．

このように考えると，新しいプログラムを導入する手間はないが，利用時にいつもキープアライブに気を使い続けなければならないシステムより，キープライブのための専用プログラムを導入するほうが，利用者にとっては分かりやすいシステムといえるだろう．

我々の提案している IP パケット認証ゲートウェイシステム AIPS（Authenticated IP System）[6)–9)] は，情報コンセントへの接続に対して認証を行うものではなく，携帯端末から送信される IP パケットに対して認証を行うものである．そのため，キープライブの仕組みが不要であり，IP アドレスや MAC アドレスの偽装にも十分な耐性を持っているうえ，コネクション（同時接続）数の増加による認証システムの負荷増加もほとんどないという特徴がある．また，利用者は専用プログラムを導入する必要があるが，ドライバレベルで認証処理を行うことから，パスワード入力時以外，システムの仕組みを意識する必要はない．

本論文では，まず AIPS の認証方式や認証手順について説明し，続いてシステムの実装について述べる．さらに，AIPS の動作実験の結果について示し，最後に今後の課題について述べる．

2. AIPS について

2.1 認証方式

AIPS では，IP パケットのヘッダ内に認証情報を埋め込み，IP レベルでの認証を行う．しかし，IPsec の AH（Authentication Header）のように IP ヘッダのオプションフィールドに認証情報を埋め込むのではなく，情報コンセント環境での利用という特徴を生かし，IP ヘッダ内の冗長部分を用いることで，IP ヘッダ長を増大させることなく，したがってパケットのフラグメンテーションを発生させることなく認証情報埋め込みを実現している．ここでは，AIPS における認証方式について説明する．

2.2 システム構成

AIPS では，**図 1** のような情報コンセント環境を想定している．

情報コンセント環境を利用するには，あらかじめ IP ヘッダに認証情報を埋め込むための認証クライアントを，携帯端末（図 1 の認証クライアント）に導入しておく．情報コンセント環境のゲートウェイは AIPS の認証サーバを兼ねており，認証クライアントが埋め込んだ認証情報が正規のものである場合には，埋め込まれた認証情報を削除し，本来の IP ヘッダに復元して，外部ネットワーク（インターネット）に送出する．

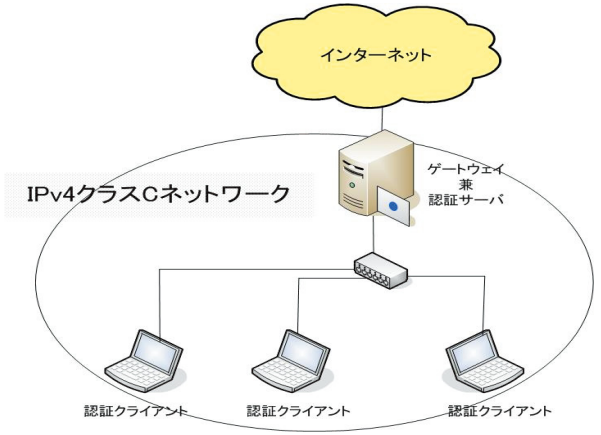

図 1　AIPS の構成例
Fig. 1　Example of AIPS network.

基本的には DHCP 環境での利用を想定しているが，プライベート IP を用いる NAT 環境でもグローバル IP 環境でも対応可能である．また，固定 IP での利用も可能である．

一般に 1 つの情報コンセント環境は，1 つのセグメントとして構成されており，その規模はクラス C 程度と仮定できる．Opengate [10)] のように大学規模で導入されている場合でも，実際は小規模の情報コンセント環境を統合的に管理しており，1 つ 1 つの情報コンセント環境がクラス C 以上の規模になることは，通常はない．つまり，情報コンセント環境で割り当てられる IP アドレスの上位 24 ビット目まではネットワークアドレス部であり，接続されるすべての携帯端末において同一である．AIPS では，情報コンセント環境で割り当てられる IP アドレスの上位 24 ビットを冗長部分と見なし，その部分に認証情報を埋め込むことで，IP ヘッダ長を変更せずに済むようにしている．

なお，現在の AIPS は 1 つの情報コンセント環境に閉じたシステムであるが，ユーザパスワードを一元管理し，各 AIPS の認証サーバにパスワードを通知するようなパスワード管理サーバを構築することで，前述した Opengate と同様に，複数の情報コンセント環境の統合が可能である．

2.3 認証情報

通常の IP ヘッダ（**図 2**）と比較し，AIPS の認証情報は**図 3** のように IP ヘッダに埋め

Version	IHL	TOS	パケット長
識別子		フラグ	フラグオフセット
TTL	プロトコル番号	ヘッダチェックサム	
送信元 IP アドレス			
宛先 IP アドレス			

図 2　通常の IP ヘッダ
Fig. 2　Normal IP header.

Version	IHL	TOS	パケット長
識別子		フラグ	フラグオフセット
TTL	**AIPS Proto**	ヘッダチェックサム	
プロトコル番号	認証情報		送信ホスト部
宛先 IP アドレス			

図 3　AIPS の IP ヘッダ
Fig. 3　IP header of AIPS.

込まれる．

送信元 IP アドレス上位 24 ビットのうち，上位 8 ビットには本来の IP ヘッダのプロトコル番号を退避させ，プロトコル番号として AIPS 用のプロトコル番号（**AIPS Proto**）を割り当てる．残る 16 ビットには，後述する計算方法で求めた認証情報を埋め込む．なお，下位 8 ビットはクラス C において，ホストアドレス部であり，携帯端末ごとに異なるため，そのまま保持しておく．

認証サーバ（ゲートウェイ）は，AIPS 用のプロトコル番号の IP パケットに対して，認証情報を確認し，正しい場合はプロトコル番号部を送信元 IP アドレスの上位 8 ビットに退避させてあった元のプロトコル番号に，送信元 IP アドレスの上位 24 ビットを元のネットワークアドレスにそれぞれ復元し，外部に送出する．このとき，AIPS 用のプロトコル番号以外の IP パケットはすべて破棄することで未認証の通信を遮断する．

認証情報の計算には，IP パケットのペイロードとユーザパスワード，さらにワンタイムパスワードを使い，1 方向ハッシュ関数を用いている．

2.4　認 証 手 順

次に AIPS における認証手順の概略を示す．詳細は 3 章で述べる．

1.　ワンタイムパスワード発行

情報コンセント環境に接続すると，認証クライアントから利用者のユーザ名が認証サーバに送信され，認証サーバからワンタイムパスワードが認証クライアントに返信される．その際，認証サーバはユーザの使用している携帯端末の IP アドレスを取得し，そのホスト部とユーザパスワード，ワンタイムパスワードを関連付ける．

2.　認証情報確認

認証クライアントは，ワンタイムパスワード取得後に送出するすべての IP ヘッダに，IP ペイロード，ユーザパスワード，ワンタイムパスワードから算出される認証情報を埋め込む．認証サーバ兼ゲートウェイは，保持している送信元 IP アドレスのホスト部に対応するユーザパスワード，ワンタイムパスワードを用い，プロトコル番号フィールドが **AIPS Proto** の IP パケットから認証情報を算出して，IP ヘッダ内の認証情報と比較することで，正しいかどうかを判定する．その他のプロトコル番号を持つ IP パケットはここで遮断する．

3.　IP ヘッダ復元

正しい認証情報を持つ IP ヘッダは，本来のプロトコル番号と送信元 IP アドレスに復元され，外部ネットワークへ送出される．また，認証情報が誤っている場合は破棄される．

なお，AIPS では，携帯端末から送信される IP パケットに対してのみ，認証情報を埋め込んでおり，外部ネットワークから携帯端末へ届く IP パケットに対しては認証情報の埋め込みを行わない．なぜなら，AIPS は携帯端末を認証するためのシステムであり，認証サーバ側で埋め込んだ情報を認証クライアント側で判定する意味がないためである．万一，認証されていない携帯端末に外部から通信があったとしても，携帯端末からのレスポンスはゲートウェイで破棄されることから，通信は成立しない．

特に，携帯端末はほとんどの場合クライアントとして利用されるため，情報コンセント環境内部から外部への通信量よりも，外部から内部への通信量のほうが多いと予想される．よって，逆方向の認証を行わないことで，認証情報の埋め込みと復元にともなう負荷増大を防ぐことができる．

2.5　認証情報の強度

認証情報が 16 ビット長ではたかだか 65,536 通りにすぎないことから，その強度を補うための対策が必要である．そのため，2.4 節で説明したとおり，認証情報の生成にはワンタイムパスワードを採用しており，リプレイアタックを回避し，長期に通信内容を監視，記録さ

れても認証情報の偽造を困難にしている．また，あらゆるハッシュ関数に有効とされるバースデーアタック[11] を用いると，256 とおりのランダムな認証情報を試せば，約 50%の確率で認証情報を当てられてしまうことが分かっているが，これに対しては，認証に複数回失敗した時点でその携帯端末（IP アドレス）からの通信を遮断するような実装を行う．これにより，ブルートフォース型の偽装アタックに対しても十分な耐性を持たせることができる．

2.6　類似方式との比較

1 章において紹介した文献 2)–5) の各システムは，IP アドレスや MAC アドレスの偽装を防ぐために，何らかの方法で携帯端末と認証用機器の間でキープライブを維持し，そのコネクションが切れると同時に認証情報を破棄して，通信をできなくする方法を採用している．そのため，携帯端末の数が増えるとキープアライブ確認の負荷が増大することになる．一方，本方式では，すべての IP パケットに認証情報を埋め込むため，同時に利用する携帯端末の台数が増えてもキープアライブ確認の負荷が増大することはない．また，認証後のコネクションの維持が不要であるうえ，ドライバレベルで認証クライアントが動作していることから，利用者は認証時以外に認証システムを意識する必要はない．

次に，2.1 節でも触れた IPsec の AH を用いれば，送信元の認証や改ざんの確認が可能であることから，本方式と同様に IP パケット単位の認証を行うことが可能である．しかし，IPsec はホスト（IP アドレス）単位での認証を行い，ユーザ単位での認証はできない．よって，不正利用が発生してもその利用者を特定することが困難である．また，外部からの IP パケットに対しても同様の認証処理が必要であることからオーバヘッドが大きくなることは避けられない．一方，本方式ではユーザ単位での認証を行うことから，携帯端末の共有利用が行われたとしても，利用者を特定できるという利点がある．また，外部からの通信には認証情報が付加されないため，オーバヘッドの増大が防げる．

最後に，ADSL 接続などで広く用いられる PPPoE を利用して情報コンセント環境を構築する場合[12] と比較する．PPPoE を用いた情報コンセント環境は，一般的な Linux のゲートウェイがあれば，比較的簡単に構築が可能であるうえ，ユーザ単位での認証も可能である．しかし，PPPoE を用いることでのオーバヘッドによるスループット低下や MTU 値のチューニングなどの手間が生じるなどの問題があるといえる．実際に AIPS と PPPoE（rp-pppoe3.7[13]）を同一のゲートウェイ（CPU: 733 MHz，Mem: 512 MB）に実装して実験を行った結果，認証を行わない場合と比較して，AIPS が 2%の速度低下だったのに対し，PPPoE では 38%もの速度低下となっている．

3.　システム実装

ここでは AIPS の実装について述べる．AIPS は，認証サーバ兼ゲートウェイを Linux，認証クライアントを Windows および Linux で実装している．

3.1　認証サーバ兼ゲートウェイ

認証サーバ兼ゲートウェイは，AIPS の認証処理と情報コンセントのゲートウェイの役割も果たす．認証サーバプログラムは一般的なサーバプログラムと同様にデーモンとして実装されており，Linux の標準的 IP 通信監視ツールである tcpdump でも用いられている IP パケット捕捉ライブラリ libpcap[14]（以下，pcap）を用いて実装している．

情報コンセント環境の内側からゲートウェイ経由で外側に向かう，認証情報を含んだ IP パケットを pcap で捕捉し認証情報を確認する．正しい認証情報であれば認証情報の部分を，正規の IP ヘッダの情報に復元して外側へ送り出すが，pcap は本来 IP パケットを複製するためのものなので，**図 4** のように，認証情報が埋め込まれたままの IP パケットや認証情報の埋め込まれていない IP パケットはファイアウォールで遮断する必要がある．なお，ゲートウェイ機能やファイアウォール機能は Linux の標準的な機能やプログラムをそのまま用いている．

情報コンセント環境で DHCP を用いる場合は DHCP サーバ，DNS を用いる場合は DNS サーバの役割も，認証サーバ兼ゲートウェイが同時に果たす必要がある．なぜなら，AIPS では IP ヘッダ内に認証情報を埋め込むため，認証サーバ兼ゲートウェイ以外にこれらのサー

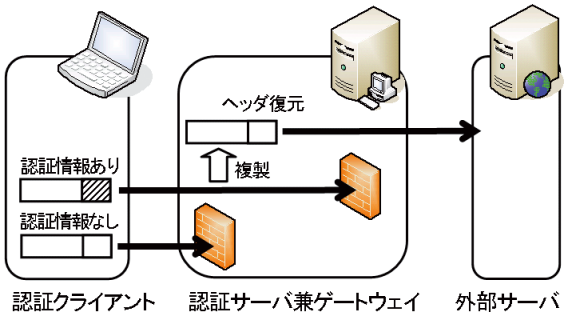

図 4　認証サーバ上での処理
Fig. 4　Processing on authentication server.

バを設置しても，正常な通信ができないためである．

3.2　認証クライアント

認証クライアントプログラムは，いずれもドライバレベルでの実装となっている．

Linux 版については Linux の標準的なファイアウォール機能である iptable で利用されている netfilter [15] を用いてカーネルモジュールとして実装しており，OUTPUT chain で IP パケットの捕捉と認証情報の埋め込みを行っている．認証クライアントの起動時および停止時には，このモジュールの導入および削除を行うために root 権限が必要となる．

Windows 版は TCP/IP 用のフィルタフックドライバ[16] として実装しており，IP パケットが NIC に渡される前に捕捉し，認証情報の埋め込みを行っている．認証クライアントの起動時および停止時には，このパケットフィルタドライバが着脱される．

現時点では Windows 2000 および XP に対応しているが，ドライバの構造が大幅に変更されている Vista には対応していない．

3.3　動作の流れ

認証の各段階における具体的な動作について**図 5** を用いて説明する．ここでは，DHCP 環境での利用を想定する．

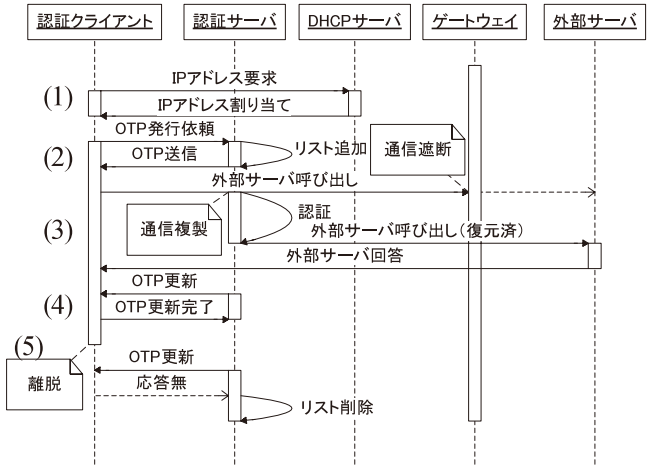

図 5　認証のシーケンス
Fig. 5　Authentication sequence.

（1）　情報コンセント環境への接続

AIPS の情報コンセント環境に携帯端末を接続すると，まず DHCP による通常の IP アドレス割当てが行われる．この時点では，まだ認証クライアントの機能は有効になっておらず，認証情報が埋め込まれていないため，情報コンセント環境の外側への通信はすべて認証サーバ兼ゲートウェイのファイアウォール機能で遮断される．

（2）　ワンタイムパスワード発行

DHCP による IP アドレスの割当てが完了すると，利用者は認証クライアントを起動し，ユーザ名とパスワードを入力する．すると，認証クライアントがワンタイムパスワードの発行依頼を認証サーバに対して行う．このときにユーザ名の通知も同時に行う．

発行依頼を受けた認証サーバは，ワンタイムパスワードを認証クライアントに送信し，受け取ったユーザ名と IP アドレスの送信ホスト部，さらに発行したワンタイムパスワードで構成されるレコードを接続中リストに追加する．

これ以降，携帯端末からの通信はすべて認証情報の埋め込みが行われる．

（3）　認証通信

認証サーバは，ゲートウェイを内側から外側に通過する IP パケットの送信ホスト部に対応するレコードを接続中リストから検索し，そのユーザ名と使用中のワンタイムパスワードを特定，認証情報が正しいかどうかを検査する．

認証情報が正しいものについては，認証情報を除去し，IP ヘッダを正規のものに復元したうえで外部へ送出する．一方，認証情報が正しくない場合は，そのまま破棄し，認証失敗の記録を行う．同一の携帯端末（接続中リストの同一レコード）に対して複数回，認証失敗が記録されると，セキュリティのため，接続中リストから当該レコードを削除し，以後の通信を破棄する．

なお，pcap を用いて認証情報の確認を行っているため，認証情報が埋め込まれたままの複製元の IP パケットも残っているが，これらは外側に出る前にファイアウォール機能で遮断される．また，認証情報が埋め込まれていない通信も，(1) で述べたとおり遮断される．

（4）　ワンタイムパスワード更新

ワンタイムパスワードには有効期間を設け，一定時間が経過すると更新が行われる．

更新通知は認証サーバ側から認証クライアントに対して行われ，新しいワンタイムパスワードを受け取った認証クライアントは，更新完了通知を返信し，以後は新しいワンタイムパスワードを使用する．

認証サーバは更新完了通知を受け取った時点で，接続中リストを更新し，以後は新しいワ

ンタイムパスワードを使用する．

（5） 情報コンセント環境からの離脱

ワンタイムパスワードの更新が行われるかどうかで離脱の確認を行うため，携帯端末を情報コンセント環境から離脱させるための手続きは不要である．ただし，ワンタイムパスワードの更新間隔が長すぎると，離脱後に第三者によるリプレイアタックを許してしまう危険性があるため，1〜2 分程度としている．

更新通知後，認証クライアントからの更新完了通知が届かない場合，1 度だけ更新通知を再送する．それでも更新完了通知が届かない場合は，携帯端末がネットワークを離脱したものと判断し，接続中リストから該当するユーザを削除する．その後，正しい認証情報が埋め込まれた IP パケットが届いても，通信は遮断される．

更新通知の再送間隔については，情報コンセント環境内は同一セグメントということもあるため，ワンタイムパスワードの更新間隔と比べても十分短い時間とし，離脱判定に遅延が生じないようにする．

3.4 偽装認証情報による DoS 攻撃への対応

認証サーバ兼ゲートウェイでは，接続中リストの同一の携帯端末で認証情報の正しくないパケットが複数回検出されると，その携帯端末からの通信を遮断するようになっているため，第三者が認証情報の正しくないパケットを偽装することで，その携帯端末の通信を妨害する DoS 攻撃が可能である．

認証情報が誤っている通信だけ遮断することも可能であるが，2.5 節でも述べたとおり認証情報が 16 ビットと短いことから，セキュリティ上の問題がある．認証ネットワークの目的は，外部に脅威となるような第三者の利用を排除することであるという観点からは，この DoS 攻撃を避けることは難しい．

そこで，本質的な解決策ではないが，正規の利用者に対して誤った認証情報の通信が行われていることと，パスワードの誤入力か第三者による DoS 攻撃が行われている可能性があることを通知することにした．

3.5 ワンタイムパスワード更新偽装への対策

ワンタイムパスワード更新は，認証サーバから認証クライアントに対して行われるため，第三者による偽装が可能な場合，認証クライアントのワンタイムパスワードが故意に誤ったものに更新されてしまう DoS 攻撃が可能である．

ワンタイムパスワードを公開鍵暗号方式で暗号化して引き渡すという厳密な方法もあるが，復号するためのオーバヘッドやプログラムの複雑化を招くことから，ユーザのパスワードと更新前のワンタイムパスワード，さらに新しいワンタイムパスワードを IP ペイロードの代わりに用いて，AIPS の認証情報と同じ方法で計算した結果（OTP 署名情報）を，偽装防止に用いることにした．OTP 署名情報は，ワンタイムパスワードの更新通知で認証クライアントに送付され，認証クライアントは，OTP 署名情報が正しいことを確認してから，ワンタイムパスワードの更新を行う．

3.6 認証クライアントを未導入の場合への対応

AIPS の情報コンセントに，認証クライアントを持っていない利用者が携帯端末を接続した場合への対応として，その端末からの http 通信を認証サーバ兼ゲートウェイが，認証クライアント配布サーバへ転送し，認証クライアントプログラムの配布とインストール手順の説明を行うことができるように実装している．この際用いる認証クライアント配布サーバは，認証ネットワーク内に認証サーバ兼ゲートウェイとは別に用意することが可能である．

なお，現在の実装では，ユーザ登録は事前に行うことを前提としているが，認証クライアントプログラムの配布時にユーザ登録を行うような実装も可能である．

4. 実験と評価

3 章で示したシステムの実装で，Linux および Windows の携帯端末での正常な動作を確認している．ここでは，AIPS の特徴を確認するための実験とその評価について述べる．

AIPS の特徴の 1 つは，他の認証ネットワークシステムの多くで必要となっている，携帯端末が接続を維持しているかどうかを確認するためのキープアライブの管理が不要という点である．このことは，接続台数の増加によって生じる認証システムの負荷の増加がないことを意味している．ここでは実装した AIPS を用い，同時接続数の増加による認証サーバの負荷計測実験を行うことで，上記の特徴を実証する．

実験では，クライアントと外部サーバとの通信速度を，認証機能を有効にした場合とそうでない場合で測定した．通信速度の測定には netperf[17] を用い，それぞれ 10 回実施し，クライアント台数分の平均を求めた結果である．なお，実験環境は**図 6** ならびに**表 1** のとおりである．図 6 のように認証ネットワークと外部サーバ以外に通常利用のネットワークが接続されており，実験用ではあるが実環境に近いものとなっている．

4.1 実 験 結 果

Linux の認証クライアントを用いて行った実験の結果を**表 2** に示す．なお，クライアントの OS が Windows の場合や OS を混在させた場合の実験でも同様の結果が得られているが，手作業で実験を行う必要からばらつきの大きい結果となったため，割愛した．

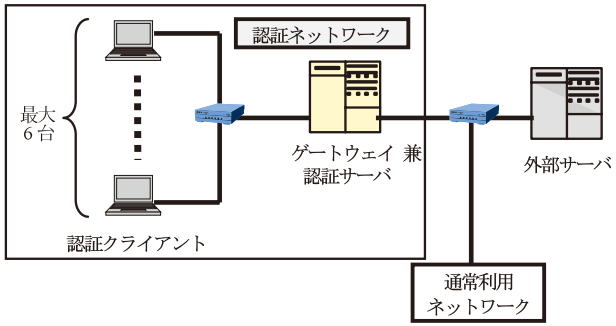

図 6　実験環境
Fig. 6　Experimental environment.

表 1　使用機器
Table 1　Specification of experimental equipments.

	CPU	メモリ	NIC	OS
認証 クライアント	2.0GHz	1024MB	100Mbps	KNOPPIX/Xen3.0.3-0
認証サーバ	2.8GHz	256MB	内外： 100Mbps	Debian/GNU Linux 3.1
外部サーバ	3.4GHz	1024MB	1000Mbps	Turbolinux 8.0 Server

表 2　Linux 認証クライアントの通信速度
Table 2　Traffic rate of Linux clients.

台数[台]	認証なし [KB/s]	認証あり [KB/s]	低下率[%]	認証あり総量 [KB/s]
1	11487	11487	0	11487
2	5750	5747	0	11494
3	3853	3902	0	11706
4	2899	2883	1	11532
5	2304	2316	0	11580
6	1924	1985	0	11910

4.2 考　　察

4.1 節の結果より，認証なしに対する認証ありの低下率は最高でも 1%程度というものであった．

続いて，台数による影響について分かりやすく示すために，認証ありの場合の台数 × 通信速度で求めた認証サーバを通過する通信速度（表 2 認証あり総量）に注目しても，台数による影響は見られないことが分かる．また，台数増加による低下の傾向を確認するため，一次近似を行ったが，正の傾きになっており，台数増加による低下の傾向は確認されなかった（**図 7**）．

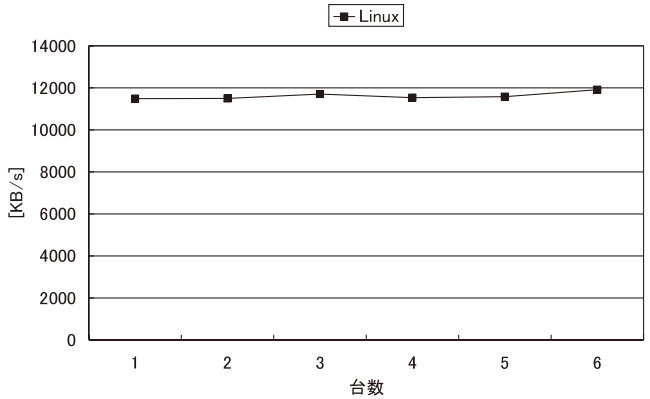

図 7　認証ありの総量
Fig. 7　Total traffic rate of AIPS.

なお，表 2 認証あり総量の値は，認証サーバ機の NIC の通信性能（100 Mbps）のほぼ 100%に達していることから，認証サーバ機には余力があるものと思われる．そのため，台数による影響を厳密に確認するためには，認証サーバ機の処理性能を下げるなどして，負荷が十分高い状態を作り出したうえで，実験を行う必要があるかもしれないが，提案方式の原理から考えれば，IP パケットの流量が変わらない限り，同様の結果が得られるものと推測できる．

以上の結果から，今回の実験環境においては，AIPS が接続台数に影響を受けていないことが確認できたといえる．

5. おわりに

現在，認証サーバは pcap ライブラリを使って実装されているため，認証クライアントから届いた IP パケットの複製を認証に用いている．そのため，認証サーバ内では認証情報を含んだ IP パケットと復元済みの IP パケットを処理しており，認証サーバの性能が低いと，大幅な速度低下が生じる恐れがある．そのため，現在，認証クライアントと同様に netfilter

を用いたデバイスドライバレベルでの実装を行っている．

また，2.2 節で触れたように，パスワード管理サーバを用意し，複数の情報コンセント環境を統合できるようにすることも検討していく．特に，安全にパスワードを AIPS の認証サーバに通知する機構が課題である．

さらに，AIPS では認証クライアントを導入する必要があることから，それを生かした AIPS ベースの検疫システムの開発を始めている．検疫システムでは，持ち込まれた携帯端末内のセキュリティパッチ適用情報やウィルス対策ソフトの有無，パターンファイルのバージョンなどの情報取得が必要となるが，認証クライアントに検疫エージェントとしての機能を持たせることで，比較的容易にこれらの情報を得ることができる．

AIPS では，今後，この検疫機能とパスワード管理サーバによる統合を中心に実装を進めていく予定である．

参　考　文　献

1) 日立電線：Apresia シリーズ（オンライン），(参照 2008-01-29). http://www.apresia.jp/
2) 石橋勇人，山井成良，安部広多，阪本　晃，松浦敏雄：利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方法，情報処理学会論文誌，Vol.42, No.1, pp.79–88 (2001).
3) 渡辺義明，渡辺健次，江藤博文，只木進一：利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発，情報処理学会論文誌，Vol.42, No.12, pp.2802–2809 (2001).
4) 丸山　伸，浅野善男，辻　斉，藤井康雄，中村順一：既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築，情報処理学会研究報告 DSM-14，pp.131–136 (1999).
5) 福田浩章，山本喜一：XFW：アドレス偽造に対応したオープンスペース用ネットワークアクセスサービスの実装と導入，情報処理学会誌，Vol.47, No.8, pp.2352–2361 (2006).
6) 川内拓行，安井浩之，松山　実：IP ヘッダへの利用者認証フィールド埋め込みによる認証システム，情報処理学会第 64 回全国大会講演論文集，第 3 分冊，pp.405–406 (2002).
7) 倉内　努，安井浩之，松山　実：IP ヘッダへの利用者情報埋め込み型認証システムの構築，情報処理学会第 66 回全国大会講演論文集，第 3 分冊，pp.485–486 (2004).
8) 中西康夫，安井浩之，松山　実：情報コンセントにおけるユーザ認証システムの構築と改良—認証情報の強化とトラフィック量の低減，情報科学技術フォーラム講演論文集，pp.221–222 (2005).
9) 中西康夫，安井浩之，松山　実：IP ヘッダへの利用者情報埋め込み型認証システムの構築—実験と評価，情報処理学会第 68 回全国大会講演論文集，第 3 分冊，pp.689–690 (2006).
10) 只木進一，江藤博文，渡辺健次，渡辺義明：利用者移動端末に対応した大規模ネットワークの Opengate による構築と運用，情報処理学会誌，Vol.46, No.4, pp.922–929 (2005).
11) H. デルフス，H. クネーブル（著），林　芳樹（訳）：暗号と確率的アルゴリズム入門，シュプリンガー・フェアラーク東京，pp.59–60 (2003).
12) 桝田秀夫，鈴木未央，中西通雄：PPPoE を利用した認証付き情報コンセントの実装と評価，情報処理学会研究報告 DSM-21，pp.19–24 (2001).
13) Roaring Penguin Software: RP-PPPOE（オンライン），(参照 2008-01-29). http://www.roaringpenguin.com/products/pppoe/
14) tcpdump/libpcap: TCPDUMP public repository（オンライン），(参照 2007-08-24). http://www.tcpdump.org/
15) The netfilter.org Project: netfilter/iptables project homepage（オンライン），(参照 2007-08-24). http://www.netfilter.org/
16) Microsoft Tech net: TCP/IP パケット処理パス（オンライン），(参照 2007-08-24). http://www.microsoft.com/japan/technet/community/columns/cableguy/cg0605.mspx
17) Rich Jones: Netperf Homepage（オンライン），(参照 2007-08-24). http://www.netperf.org/netperf/

(平成 19 年 8 月 31 日受付)
(平成 20 年 4 月　8　日採録)

安井　浩之（正会員）

昭和 43 年生．平成 8 年明治大学大学院博士課程修了．平成 9 年武蔵工業大学工学部情報処理センター講師（現在，知識工学部）．博士（理学）．著書『ファジィとソフトコンピューティングハンドブック』（共立出版）等．主にネットワークセキュリティに関する研究・開発に従事．日本知能情報ファジィ学会会員．

松山　　実（正会員）

昭和 19 年生．昭和 51 年ウィンザー大学大学院博士課程修了．武蔵工業大学情報処理センター講師，助教授を経て平成 6 年教授（現在，知識工学部）．Ph.D. 主に教育用情報処理システムに関する研究・開発に従事．著書『基礎数値解析』（昭晃堂）．日本産業技術教育学会，IEEE 各会員．