動的接続切替に対応する情報コンセントの認証方式

野村嘉洋 † 藤田貴大 † 岸場清悟 ‡ 西村浩二 ‡ 相原玲二 ‡
† 広島大学大学院工学研究科
‡ 広島大学情報メディア教育研究センター

あらまし

近年，ノートパソコンや PDA などの急速な普及により，モバイル端末を無線 LAN あるいは有線 LAN によりネットワークに接続するための情報コンセントが普及しつつある．これらのモバイル端末では頻繁にネットワーク接続と切断が繰り返されることがあるが，そのような状況では確実な認証機能を確保しつつ利用開始の高速化が要求される．本稿では動的な接続・切断が発生する情報コンセントでも利用可能な認証方式について提案する．本方式は，特に移動透過性を保証するモバイル IP 端末に対して適用すると効果的であり，筆者らが現在提案しているアドレス変換方式による移動透過インターネットアーキテクチャー MAT (Mobile IP with Address Translation) への適用についても述べる．

キーワード: 情報コンセント，利用者認証，移動体通信，モバイル IP

User Authentication Method for Information Outlet Systems Supporting Dynamic Connection

Yoshihiro NOMURA † Takahiro FUJITA † Seigo KISHIBA ‡ Kouji NISHIMURA ‡ Reiji AIBARA ‡
† Graduate School of Engineering, Hiroshima University
‡ Information Media Center, Hiroshima University

Abstract

In recent years, information outlet for connecting a mobile node to the network are spreading caused by the popularization of notebook PC, PDA, etc. These mobile nodes may frequently connect and disconnect. Such a situation requires secure authentication function and rapid start of use after connection. In this paper, we propose an authentication method which can be used for information outlet systems supporting dynamic connection, e.g., wireless LAN access. We also demonstrate the proposed method can be effectively applied to nodes with IP mobility support. We describe an application of the method to nodes supporting MAT (Mobile IP with Address Translation), that is one of IP mobility support architectures.

Keywords: Information Outlet System, User Authentication, Mobile Communications, Mobile IP

1 はじめに

近年，ノートパソコン・PDA (Personal Digital Assistant) などのモバイル端末や無線ネットワークの急速な普及により，キャンパスやカフェ，ホテルや空港のロビーなどに無線 LAN や有線 LAN の情報コンセントが設置されることもめずらしくなくなってきた．しかし，このような不特定多数の利用者が出入りするような環境で，誰でも自由にネットワークに接続できてしまうことは，セキュリティ上好ましくない．そこで，このような環境では，利用者の利用資格の有無に応じてネットワークサービスを提供する必要が生じてくる．このような背景から，筆者らは既に有線 LAN・無線 LAN に対応した認証に基づくアクセス制御を行う情報コンセントシステム PortGuard[1][2] の設計・開発を行い，現在広島大学内のネットワークで運用を行っており，在籍者であれ

ば誰でも利用できるようになっている．また，学内の宿泊施設では，学外者に対しても有効期限つきアカウントを発行し利用できるようなサービスも行っている．

一方，無線ネットワークの普及に伴い，自由に移動しながらネットワークサービスを利用したいという要望も高まってきた．しかし，キャンパスやビルなどで，施設や階ごとに別々のネットワークが存在するような環境では，PortGuard のようにアクセスポイントが変わるたびに新たにユーザ ID/パスフレーズ等を入力するオンデマンド認証は非常に面倒であり限界がある．このように，続接と切断が頻繁に発生するような情報コンセントにおいては，確実な認証機能を確保しつつネットワークの利用再開の高速性が要求される．

現在，認証に基づいてネットワークに接続する方式として，IEEE 802.1x や Mobile Internet Services Inc. (MIS)[3] が提案している方式がある．しかし，これらのアーキテクチャはいくつかの問題をかかえてえている．

そこで，筆者らは現在，これら既提案方式の問題を解決するため，頻繁にネットワークの接続･切断が発生する情報コンセントでも利用可能な新たな認証システムを提案し，実装を行った．本稿では，提案したシステムの概要と実装したシステムの評価実験を通して本システムが十分実用に耐えうる性能を有することを示していく．また，本方式は移動透過性を保証するモバイル IP 端末に対して適用すると効果的であり，筆者らが現行の移動透過性を実現するアーキテクチャの問題を解決するために提案しているアドレス変換方式による移動透過インターネットアーキテクチャ MAT (Mobile IP with Address Translation)[4] への適用についても述べ，ネットワークの切り替えが実用に耐えうるオーバヘッドで行えることを示す．

2　システム概要

2.1　システム構成

本システムの構成を図 1 に示す．各構成要素の機能は以下のようになっている．

2.1.1　認証サーバ

利用者端末の認証を行い，その認証結果に基づき利用者端末に IP アドレスを割り当てる．利用者端末から送られてくる認証情報通知の一部は利用者端末の秘密鍵で暗号化されており，認証サーバは，この認証情報通知を受け取ると公開鍵サーバに対して予め登録されている利用者端末の公開鍵を要求し，受け取った公開鍵で正しく復元できた場合は認証成功として利用者端末に IP アドレスを割り当てる．利用者端末と認証サーバ間の通信は全てブロードキャスト通信で行われる．また，定期的にネットワーク情報の通知及び利用者の利用記録をとっている．利用者端末が送出する認証情報通知の暗号/復号化

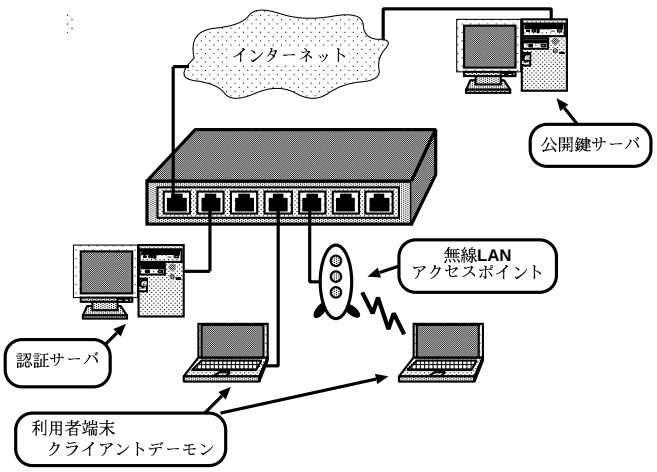

図 1: 本システムの構成

には OpenSSL 0.9.6c を使用した．現在認証サーバの動作確認ができている OS は，Linux 2.2/2.4 及び KAME スタックをのせた NetBSD 1.5.3 である．

2.1.2　公開鍵サーバ

要求に応じて予め登録しておいた公開鍵を提供する．公開鍵サーバには djbdns 1.05 をもとに DNS を拡張し新たに公開鍵問い合わせレコード (PKEY レコード) を追加することにより実装した．問い合わせには OS 付属のレゾルバ・ルーチンを用いて専用ライブラリを作成した．現在は Linux 2.2/2.4 で動作確認がとれている．

2.1.3　無線 LAN アクセスポイント

無線ネットワークと有線ネットワーク間のネットワーク接続機器．IEEE 802.11a 及び IEEE 802.11b 準拠の製品を使用した．実際には本システムは，有線・無線などネットワーク接続形態やネットワーク接続機器に依存すること無く使用可能であり，既存のネットワークに容易に設置することが可能である．

2.1.4　利用者端末

利用者が使用しながらネットワーク間を移動するモバイル端末．認証サーバからのネットワーク情報通知やネットワークインターフェースのリンク状態からネットワークが切り替わったと判断した際に，認証サーバに対して利用者端末の秘密鍵で暗号化した認証情報の通知を行う．認証が成功した場合は，サーバから割り当てられたアドレス情報を端末に設定し通信が行えるようになる．利用者端末と認証サーバ間の通信は全てブロードキャスト通信で行われる．

また，利用者端末内に格納している秘密鍵は，さらに別の鍵で暗号化して保存しておき，端末起動時にパスフレーズを入力することによりメモリに展開し安全に鍵管

理を行うことができる．現在利用者端末上で動作するクライアントデーモンプログラムは，Linux 2.2/2.4 及び KAME スタックをのせた NetBSD 1.5.3 で動作する．

2.2 利用者認証の流れ

本システムにおける利用者認証の流れを図 2 に示す．利用者端末は，ネットワークが切り替わったと判断すると認証サーバーに対してブロードキャストでチャレンジを要求し，認証サーバからチャレンジを受け取ると，チャレンジと利用者端末の情報をその利用者端末の秘密鍵で暗号化して，これを認証情報として認証サーバに通知する．認証サーバは，認証情報通知を受け取ると公開鍵サーバに対してこの利用者端末の公開鍵を要求し，受け取った公開鍵で認証情報を復元し，その認証情報が正しいものであればこの利用者端末の認証成功とし，利用者端末に IP アドレス及び付随するアドレス情報を割り当てる．利用者端末はアドレス情報が割り当てられたらそれを端末に設定することにより通信を開始できるようになる．

2.3 利用者端末のセキュリティ

認証時，利用者端末は IP アドレスが割り当てられていないため認証サーバとの通信はブロードキャストで通信を行う．そのため他の利用者端末に認証情報を盗聴される可能性がある．本システムではまず，認証サーバが利用者端末に対してチャレンジを発行し，利用者端末は認証要求として認証情報を通知する際に，このチャレンジと利用者端末の MAC アドレスを利用者端末自身の秘密鍵で暗号化し，これを認証情報として認証サーバに通知する．認証サーバは，利用者端末の公開鍵でこの認証情報を復元し，正しく復元できた場合は，チャレンジの比較と認証情報通知に含まれる MAC アドレスとチャレンジ要求にきた際の MAC アドレス，及びイーサネットフレームに含まれる MAC アドレスが同一であることを確認し認証成功とすることにより，利用者端末の詐称を防止する．また，チャレンジは一度認証情報通知を受け取ると破棄され，また，十分長い周期で再利用するため，事実上同じチャレンジが使われることはない．

また，無線 LAN ネットワークの場合，利用者端末は互いに通信可能であり盗聴などが行われる危険性がある．そこで，無線 LAN アクセスポイントによっては WEP (Wired Equvalent Privacy) と呼ばれる暗号方式を用いることにより，外部からの盗聴に対してセキュリティを確保することができるが，WEP は共通鍵暗号方式であるため鍵の配布が非常に困難である．そこで本システムでは，認証サーバが利用者端末の認証成功時，アドレス情報を割り当てる際に，利用者端末の公開鍵で WEP のキーを暗号化し利用者端末に通知することより安全に WEP のキーを通知できる．これにより，無線区間の暗号化を安全に実現できるが，現在本提案システムでこの機能は実装していない．

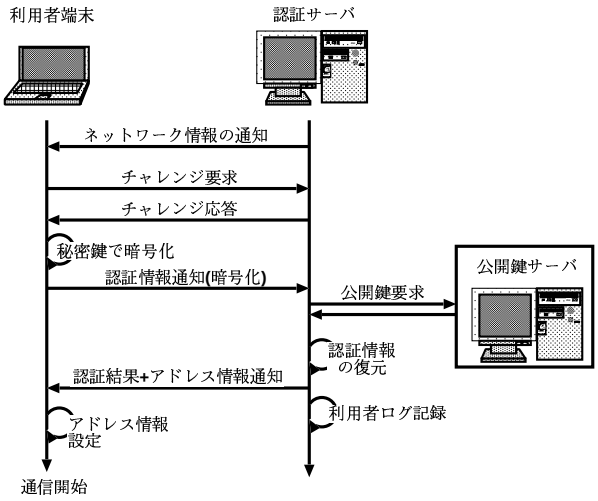

図 2: 利用者認証の流れ

2.4 他の方式との比較

DHCP (Dynamic Host Configuration Protocol)[5] ネットワークを利用する際に，その設定と管理を簡単にし，かつ，IP アドレス資源を有効に割り当てるために実現されたプロトコル．ただし，利用者認証機能はない．本提案システムのアドレス割り当てに関するプロトコルは，DHCP を基本に，認証機能を追加したとみなすことができる．処理手順の概要は以下のようになっている．

1. 利用者端末が DHCP サーバに アドレス要求を送信
2. DHCP サーバが利用者端末にアドレスを割り当てる

IEEE 802.1x 方式 利用者端末とアクセスポイント間で IEEE 802.1x プロトコルを使い，RADIUS (Remote Authentication Dial-In User Service) サーバを利用することで，ネットワークの利用に認証機能を付加した方式．使いはじめには必ず認証が必要となり不正アクセスを排除でき，また，RADIUS システムを利用して，WEP のキーを定期的に変更することで安全性を高めることも可能である．しかし，認証は利用者がネットワークを使いはじめる際に ユーザ ID/パスフレーズを入力するオンデマンド方式であり，頻繁にネットワークが切り替わるような環境には適さない．また，ネットワーク内全てのアクセスポイントやスイッチが 802.1x 対応機器でなければならないため，新しく環境を構築する場合に，既存のネットワーク環境をそのまま用いることができない．本提案システムは，ネットワーク上に認証サーバを設置するだけでよく，既存のネットワークを有効利用できる．また，IEEE 802.1x は，既にセキュリティ上の脆弱性が指摘されている．

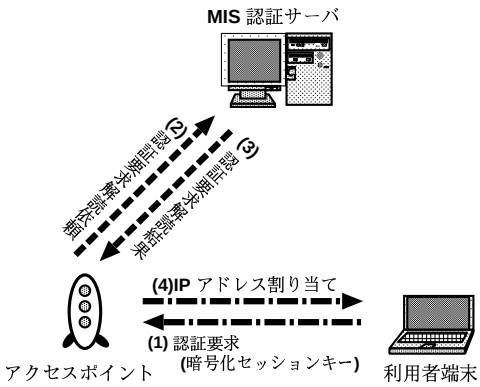

図 3: MIS 方式 利用者認証の流れ

MIS 方式 最近よく話題になり使われている「街角インターネット」を標榜し，無線 LAN インフラを進めている MIS の方式．この方式の処理手順の概要を図 3 に示す．

1. 利用者端末は認証要求として，利用者端末の共有鍵で暗号化したセッション鍵をアクセスポイントに送信
2. アクセスポイントは，認証要求パケットの暗号解読を MIS 認証サーバに依頼
3. MIS 認証サーバは，予め登録された利用者端末の共有鍵で復号化し，結果をアクセスポイントに通知
4. アクセスポイントは，認証結果に応じて利用者端末に IP アドレスを割り当てる
5. 以降，利用者端末とアクセスポイント間は，そのセッション鍵で通信を行う

ここで，アクセスポイントは，本提案システムで言う認証サーバと類似の機能を持ち，MIS 認証サーバは RADIUS サーバの拡張したものである．本提案システムは，認証サーバ (アクセスポイント) が公開鍵サーバから利用者端末の公開鍵を取得し，認証サーバ自身が端末認証を行う点が大きく異なる．MIS 方式は，MIS 認証サーバとアクセスポイント間で安全な通信 (RADIUS キーを利用) が必要となるため，複数の異なる IPS 等がアクセスポイントと MIS 認証サーバをそれぞれ管理する場合，スケーラビリティに問題が出ると考えられる．

3 MAT への適用

ネットワークアドレスが同一のネットワーク内の移動の場合，前節で説明した機能により認証を即座に行い，利用を開始 (再開) することができる．一方，異なるネットワーク間での移動の場合，各ノードが Mobile IP[6] など，IP レベルで移動透過性を持つ必要がある．本節では，本提案認証方式を Mobile IP の一種である MAT への適用例について述べる．

3.1 MAT の概要

MAT は既に提案されている移動透過インターネットアーキテクチャの問題を解決するように設計された，トランスポート層以上 (以下 上位層) において移動透過的な通信を保証するインターネットアーキテクチャである．Mobile IP と Mobile IPv6[7] の持つ一点障害やオーバヘッドの増加問題をなくし，最適経路による End-to-End の通信を保証する．また，LIN6[8] のように特殊なアドレスを使わず，通常のグローバルアドレスのみを用いて通信を行う．

移動透過性を実現するため，MAT では移動ノード (Mobile Node，以下 MN) はホームアドレス (Home Address) とモバイルアドレス (Mobile Address) という 2 種類のアドレスを持つ．ホームアドレスは上位層におけるノード識別子であり，MN が普段接続しているホームサブネット (Home Subnet) のアドレスプレフィックスを持つグローバル IP アドレスである．ホームアドレスは，MN がホームサブネット以外のサブネットに移動しても変わらないアドレスである．一方，モバイルアドレスはネットワーク上の位置を示すグローバル IP アドレスで，サブネットを移動するたびに DHCP や 本システムのようなアドレス割り当て機構により与えられるか，IPv6 であればステートレス機構により自動的に設定される．

ホームアドレスとモバイルアドレスはネットワーク層において変換することにより，上位層でのノード識別はホームアドレスで，経路設定にはモバイルアドレスをそれぞれ使う．このようにネットワーク層でホームアドレスとモバイルアドレスの変換を行うためには，MN の通信相手ノード (Correspondent Node，以下 CN) が MN のホームアドレスとモバイルアドレスの対応 (マッピング) を知っている必要がある．そこで MAT では MN のアドレスマッピング情報を管理するために IP Address Mapping Server (IMS) と呼ばれるサーバを導入する．IMS は複数の MN の最新のマッピング情報を管理するサーバであり，CN は，通信したい MN のマッピング情報を IMS に問い合わせる (図 4)．現在 IMS の実装は，Linux 上で djbdns 1.05 をもとに，DNS を拡張して新たに MA (Mobile Address) レコードを追加し，MN のホームアドレスをクエリとして問い合わせると，最新のモバイルアドレスを返すようになっている．

このような，アドレス変換方式を用いることにより，MAT では移動透過的な通信を可能としており，現在以下に示すプラットフォームで MAT の開発を行っている．

- FreeBSD-4.4RELEASE + KAME IPv6 スタック
- NetBSD-1.5.3RELEASE + KAME IPv6 スタック
- OpenBSD-3.0RELEASE + KAME IPv6 スタック
- Linux + USAGI 2.4 Kernel IPv6 スタック

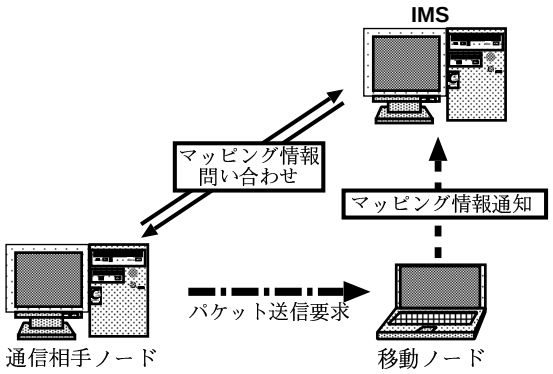

図 4: ホームアドレスからモバイルアドレス取得

3.2 本システムの MAT への適用概要

本システムの機能拡張による MAT への適用は，MN の新しいモバイルアドレスの IMS への通知機能である．ここでは，MN の新しいモバイルアドレスを IMS へ通知する方法について述べる．IMS に登録されているマッピング情報は常に最新で正しいものである必要がある．そこで，MN のモバイルアドレスが変わった際はすぐさま IMS のマッピング情報を更新する必要があり，さらに，アドレス詐称などが行われないように安全に更新しなければならない．

ネットワークが頻繁に変わるような環境であってもスムーズに認証を行いながら移動できるように，本システムでは公開鍵サーバを導入している．この公開鍵サーバを利用することにより，若干の機能拡張で IMS のマッピング情報を安全かつ容易に更新できるようになる．以下にその更新手順を示す (図 5).

MN は認証サーバから新しくモバイルアドレスを割り当てられたら，ホームアドレスと以前のモバイルアドレスと新しく割り当てられたモバイルアドレス及び現在のタイムスタンプを MN の秘密鍵で暗号化し IMS に更新通知を送る．IPv4 のモバイルアドレス更新通知パケットの構造を図 6 に示す．

現在 IMS は DNS に新しくレコードを追加して実装を行っているため，マッピング情報を更新する仕組みは用意されていない．そこで，IMS と同一ホスト上で動作し安全にマッピング情報を更新するためのデーモンプログラム (IMSd) を用意した．また，IMS と公開鍵サーバはともに djbdns 1.05 をもとに実装しているため，それぞれを別々のホストでも，同一のホストでも動作させることが可能である．

IMSd は MN からのモバイルアドレス更新通知を受け取ると，公開鍵サーバに MN の公開鍵を要求し，パケットの暗号化を解く．そして，暗号化されていたホームアドレスと比較し端末が詐称されていないことを確認する．また，更新通知パケットの順序が入れ換わって届くことの考慮と更新通知パケットを奪い以前のモバイルアドレスに更新しようとするといった攻撃を防ぐために，タイムスタンプを確認し逆行しないようにする．その後，モバイルアドレスのデータベースと MN のタイムスタンプ情報を更新し， MN に更新完了通知を送る．MN は，更新完了通知を受け取り通信を再開することができる．

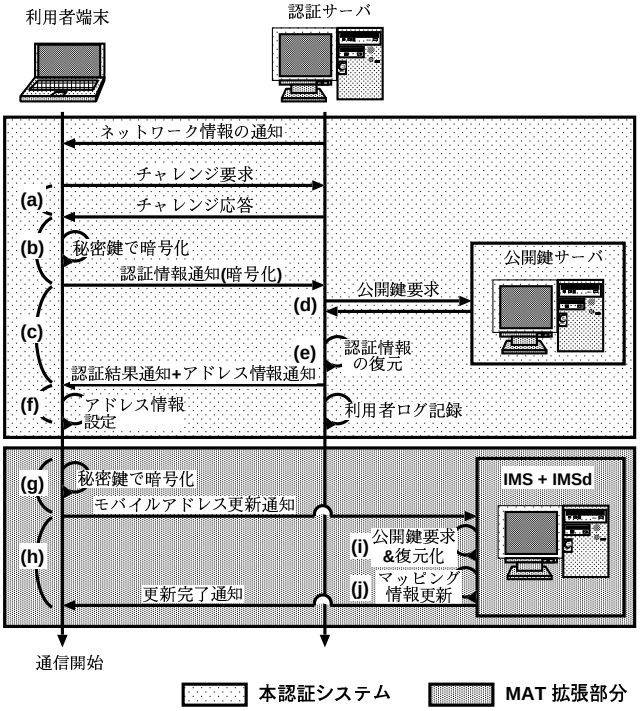

図 5: モバイルアドレス更新処理の流れ

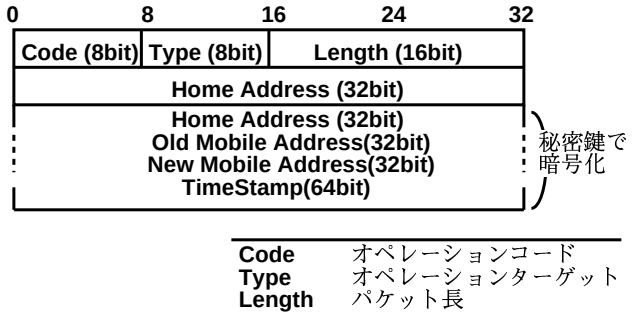

図 6: モバイルアドレス更新通知パケット

このような一連の動作により，安全かつスムーズなハンドオフが可能になると予想される．次節では，どの程度のオーバヘッドでこれらの処理が行われるかを測定し，本システムの評価を行う．

4 評価

4.1 実験環境

本システムの性能評価を行うために，利用者端末がネットワークを移動して，図 5 の流れに従いチャレンジ要求を出してから実際にネットワークが利用できるよう

表 1: マシン仕様

	利用者端末	認証サーバ	IMS + IMSd + 公開鍵サーバ
CPU	Mobile Pentium III 750MHz	Pentium III 866MHz	Pentium II 300MHz
memory	256MB	128MB	192MB
OS	Red Hat Linux 7.3	Vine Linux 2.1	Red Hat Linux 7.3
kernel	2.4.18	2.2.17	2.4.18

になり，さらに，IMS に新しいモバイルアドレスを通知するまでの時間を 10 区間 (図 5 中 (a)〜(j)) で計測した．測定は図 7 に示す環境の下で行い，各マシンの仕様は表 1 に示すようになっている．一連の認証処理と IMS への更新処理を 1000 回行い，平均した結果を表 2 に示す．

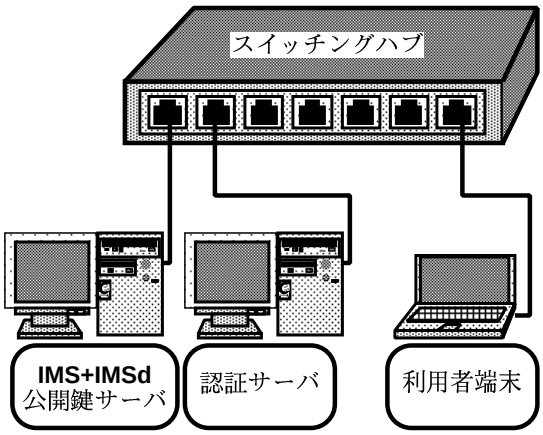

図 7: 測定環境

表 2: 各区間に要する時間の測定結果

区間	処理の概要	時間 (ミリ秒)
(a)	チャレンジ要求〜チャレンジ応答	0.405
(b)	チャレンジ応答〜認証情報通知	72.133
(c)	認証情報通知〜認証結果通知	3.239
(d)	公開鍵要求 (対 公開鍵サーバ)	0.810
(e)	認証情報復元〜認証情報確認	1.667
(f)	認証結果通知〜端末設定変更	1.885
(g)	端末設定変更〜アドレス更新通知	72.145
(h)	アドレス更新通知〜更新完了通知	66.245
(i)	公開鍵要求〜情報復元	7.560
(j)	マッピング情報更新	57.953

図 5・表 2 の区間 (b) と区間 (g) では，利用者端末の秘密鍵で送出するパケットの一部を暗号化しているため，その処理に若干時間がかかっている．また，区間 (j) では，利用者端末のホームアドレスとモバイルアドレスのマッピング情報を更新するため，DNS のデータベースファイルの書き換えるに時間を要してしまっている．しかし，これは IMS のホストのスペックアップと，管理する利用者端末の台数を適切に割り当て分散させることにより影響の無い時間まで減らすことが可能であろう．

表 2 の結果から，ネットワークが切り替わり利用者端末がチャレンジ要求を出してから，実際に通信が行えるようになるまでの時間 (区間 (a)+(b)+(c)+(f)) が約 77.7(ミリ秒)，IMS へ新しいアドレスを通知するのに要する時間 (区間 (g)+(h)) が約 138.4(ミリ秒) となり，合計 216.1(ミリ秒) 程度の時間で，認証・アドレス割り当て，マッピング情報の更新を行うことができる．

5 おわりに

本稿では，キャンパスなどに設置された情報コンセントで，動的な接続・切断が行われるような環境であっても，認証機能を確保しつつ高速に通信を開始できる認証方式の概要を示した．また，システムの実装と評価を行い許容できるオーバヘッドで認証を行うことが可能であることを示し，本システムが高速な移動が行われるような環境でも十分に耐えうる性能を有することを示した．今後は，MAT のみならず他の移動透過アーキテクチャに対する適用を検討する．

参考文献

[1] 西村浩二，秋成秀紀，野村嘉洋，相原玲二: 遠隔機器制御プロトコルを用いた有線/無線 LAN 用情報コンセントシステム，情報処理学会論文誌, Vol.43, No.2, pp.662-670 (2002).

[2] 広島大学情報メディア教育研究センター (情報通信基盤系): PortGuard on-line available at http://www.portguard.org.

[3] http://www.miserv.net/

[4] 藤田貴大，野村嘉洋，岸場清悟，河野英太郎，西村浩二，前田香織，相原玲二: MAT(Mobile IP with Address Translation) の設計とそのプロトタイプの実装, DICOMO シンポジウム 2002, 2002 年 7 月, Vol.2002, No.9, pp.397-400 (2002).

[5] R. Droms: Dynamic Host Configuration Protocol, RFC 2131 (1997)

[6] Perkins, C.: IP Mobility support, IETF (1996). RFC 2002

[7] Johnson, D. B. and Perkins, C.: Mobility Support in IPv6, IETF (2001). draft-ietf-mobileip-ipv6-14.txt, Internet-draft(Work in progress).

[8] Teraoka, F., Ishiyama, M., Uehara, K., Kunishi, M. and Esaki, H.: A Soution to Mobility and Multi-Homing in IPv6, IETF (2001). draft-teraoka-ipng-lin6-1.txt, Internet-draft.