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

2006－ＱＡ１－21（５）
2006／10／23

移動体通信の特性を考慮したゆるやかなアクセス認証方式

田島 浩一†, 藤田 貴大†, 岸場 清悟†, 西村 浩二†, 前田 香織‡, 相原 玲二†

†広島大学情報メディア教育研究センター 〒739-8511 広島県東広島市鏡山 1-4-2

‡広島市立大学総合情報処理センター 〒731-3194 広島市安佐南区大塚東 3-4-1

E-mail: †{ tashima, takfjt, kishiba ,kouji, ray}@hiroshima-u.ac.jp, ‡kaori@ipc.hiroshima-cu.ac.jp

あらまし セキュリティ対策として端末の IP ネットワーク接続には認証とその接続の許可設定を行う事が推奨される．しかし，音声通話やハンドオーバー時の情報更新などの通信を必要とするモバイル端末では，認証に要する時間の影響が通信断として現れる．本稿ではモバイル端末で行う通信特性を考慮し，認証していない状態でも短時間に限り一部の通信を許容するアクセス認証方式について提案を行う．

キーワード ネットワークサービス，アクセス認証，IP モビリティ

A Delayed Access Authentication Method for Mobile Communications

Kouichi TASHIMA† Takahiro FUJITA† Seigo KISHIBA† Kouji NISHIMURA† Kaori Maeda‡ and Reiji AIBARA†

† Information Media Center, Hiroshima University 4-1-2 Kagamiyama, Higashi-Hiroshima, Hiroshima, 839-8511 Japan

‡ Information Processing Center, Hiroshima City University 3-4-1 Ozuka-Higashi, Asaminami-ku, Hiroshima, 731-3194 japan

E-mail: †{ tashima, takfjt, kishiba ,kouji, ray}@hiroshima-u.ac.jp, ‡kaori@ipc.hiroshima-cu.ac.jp

Abstract For reasons of the network security, it is recommended that the terminals connecting to the IP network should use authentication. However, in the mobile terminal, as the communications such as the information update at the handover or the voice call are running, the influence of the time required for the authentication appears as interruption of the communications. In this paper, we propose a access authentic method that considers the communication characteristic with a mobile terminal. In the method, the terminal not authenticated allows a communication partially limiting in short seconds.

Keyword Network service, Access Authentication, IP Mobility

1. はじめに

近年，広帯域の無線 LAN ネットワーク接続サービスが広がり，端末の小型化とそこでのネットワーク通信を利用するためモバイル端末を常時持ち歩き可能な限りのネットワーク接続性を確保するための技術として Mobile IPv6[1], LIN6[2], MAT[3], Mobile PPC[4]などが提案されており，一部標準化や実証を目的とした実験も進められている．これらの技術は，端末が移動して接続しているネットワークに変更が生じ，利用する IP アドレス等が変更になっても連続した通信が継続できるようにする仕組みであり，移動により連続した音声通話やリアルタイムなストリーミング送受信が途切れないまたは途切れる時間を最小にする事が考慮されている．

他方，セキュリティ対策のために端末のネットワーク接続には認証による利用権限の確認とその許可設定が可能なものを用いる事が推奨されている．Mobile IPv6 においても，その仕様では端末のアクセス回線への接続時の認証およびアクセスの制御は，802.1X[5]を用いる事が示されている．

802.1X の動作の概要は 2.1 節に示すが，端末のネットワーク接続には認証が必要であり，かつ，認証に成功しない端末は，認証通信以外は DHCP などのアドレス設定に必要な通信も一切許可されず，ネットワークの利用開始にはある程度の待ち時間が生じる事になり，端末の接続性の維持には不利に働く．

そこで本論文では，ネットワークの利用には認証が原則として必要であることを前提として，これら移動する端末が行うリアルタイム通信という移動体通信の特性を考慮し，待ち時間の影響を少なくする端末のアクセス制御およびその認証方法についての仕組みについての提案およびその試作と評価について報告する．

2. 関連する技術

2.1. 802.1X: Port Based Network Access Control

ネットワークに接続した端末が認証してネットワークを利用する事についての仕組みであり，基本的な動作は，IP 層を利用せずに Layer2 で認証に必要な通信を行い，端末のネットワーク接続時に認証サーバを同一リンク内より検出し，認証サーバとの間で認証を行う事でネットワークの利用が可能となる方式である．そのため接続した端末は，IP ネットワークへのアクセスのために，さらに IP アドレスの取得や設定などを経る必要があり，それらが完了するまで IP 層での通信が開始できない．

また，802.1X は，プロトコルの問題点や末端のアクセスポイントまでこの機能を持つ事が必要な事や対応している機器が限られている事，パケットロス時のタイムアウト処理に時間がかかる事で認証に要する時間が速くない事が指摘されている．

2.2. PANA: Protocol for Carrying Authentication for Network Access [7]

802.1X と同様にネットワーク接続およびその認証についての仕組みであり，認証を行う通信についての仕様およびアクセスの制御について定義されている．

PANA に対応したネットワークに接続した端末は，認証を UDP/IP で行う事としており，IP アドレスの設定に必要な DHCP 及び RA 等が利用できるようにアクセスの制御を行う箇所にてアドレス設定に必要な通信を制限しない様に構成する事が示されている．

PANA は，現在 IETF で標準化が進められており，IP 層で認証通信を行うためネットワークを構成するメディアの種類に依存しない点など 802.1X よりも優れている点があるものの，仕組みを提供するネットワーク側の機器や利用するクライアントの OS の対応はこれからという状況である．

2.3. 移動体通信の特性

移動する端末は，連続した通信を行っている最中にネットワークの接続を変更すると，新たに接続したネットワーク（切り替え後のネットワーク）を利用するために認証が必要になり，認証を行っている間の通信断が生じる．この通信断は，移動する端末での利用が想定される音声通話やストリーミング受信など接続しているネットワークに変更が生じても継続して利用し続けるようなアプリケーションに対して，通信の途切れとして不必要な影響を与える．

モバイルアーキテクチャによっては，移動する端末が接続しているネットワークを変更する際に，条件によっては複数インタフェースを利用して通信の途切れが生じないまたは最小となるようにネットワークを移動するハンドオーバーが実現されている．

それでも認証に必要な時間はそのままハンドオーバーの遅れにとして影響を与え，移動速度やオーバーラップ領域の広さによっては通信断の原因となる．

3. ゆるやかなアクセス認証方式

移動体通信に対して影響を与える認証時間による通信断への対策として，モバイルアーキテクチャのハンドオーバーの仕組みの改善によるアプローチ以外に，あらかじめ認証に必要な通信断を想定しこれに配慮した認証およびアクセス制御の方式を用いる事での改善というアプローチも考えられ，十分に検討の余地があると考えられる．本論文では，後者のアプローチにより移動する端末の認証時間の通信断へ配慮して，アクセス制限の設定方法を利用開始後の一定時間後（認証時間＋リトライ時間程度）とする事で移動体通信の連続性についての配慮を行った．この方法を本論文では「ゆるやかアクセス認証方式」と表す．

3.1. アクセス認証方式の基本方針

前章に挙げたスムーズなハンドオーバーや途切れなく連続したリアルタイム通信を行うために，端末が認証に成功していない状態であっても限られた許容時間の間，特定の通信のみを許可し，許容時間内に認証成功しなかったノードに対して通信制限を設定する仕組みを提供するものである．また，移動する端末の IP アドレスの設定については，移動先ネットワークにおいてそのネットワーク毎に割り当て済みのアドレスを既に取得しているという状況は考えにいため，接続するネットワークから毎回取得する事とした．

例として，VoIP/SIP 等を利用し音声通話中の端末が認証してネットワークを利用するクライアントとしてネットワークに移動してきた場合，許容時間内に利用できる特定の通信に音声通話で用いられる UDP ストリームを含めておく事で，端末が認証を行っている間も連続した通話を可能とする．

以下にその動作の実現に必要な機能は以下の 3 つにより構成する．

- **認証について**　認証を行う通信にはパスワードによる認証を考慮して暗号通信で行うこととし，今日のインターネットでも広く利用され，多くの端末に実装されている SSL/TLS（以下では便宜上 SSL と表記）を用いて認証情報をやり取りする事とした．
- **アクセス制御について**　一般的なアクセス認証方式では，認証に成功していない端末の通信を遮断して認証に成功した端末の通信を通過させる動作であり，認証成功と端末の離脱のみをイベントとしてそれぞれ通過，遮断の変更を行う事で実現されている．　しかし，本手法ではあらかじめ設定する一定時間（認証に要す

る時間程度）以内に認証に成功していない端末の通信を遮断する動作を行うため，ネットワークに接続している端末を検出してアクセス制御を行う必要がある．アクセス制限については，IP アドレス＋MAC アドレスによる制限を行う事とした．

o 端末の接続と接続した端末の検出について　ネットワークに接続した端末がそこでの利用に必要なアドレス等の取得については，一部認証に必要な拡張を行った他は，PANA と同様に DHCP 等により接続先から取得する事とした．接続した端末の検出には，端末の接続したネットワークスイッチによる接続の検出や IPv6 近隣キャッシュからの検出を行う事とした．

3.2. 端末の接続および端末の検出

ネットワークを経由して認証行う際には，端末が認証のためのアクセス先を検出する必要がある．端末に特定のホストの情報を取得する例として DHCPv6[8]を用いて DNS サーバアドレスの取得する方法がある．これは，ネットワークに接続した端末が RA/RS によりネットワークアドレスを取得しインタフェースにアドレスを生成して設定する際の RA には，別途にネットワークより DNS や NTP サーバのアドレス等を取得するための機能として用意されている other-flag（拡張情報フラグ）を設定して通知すされる．この DHCPv6 による DNS の取得と同時に認証アクセス先を取得できるように，「Auth-Server host:port, (複数繰り返し可)」のレコードを独自に追加し，DNS サーバとあわせて取得する事とした．

アクセス制御装置には，接続した端末の IP アドレス・MAC アドレス・接続ポート等の情報を検出できるエッジスイッチやルータおよび PC ルータ等を想定しており，それらにより接続の検出を行う事とした．PC ルータの場合には定期的なポーリングによる接続端末の検出が必要になる．

3.3. アクセス制御の動作

端末の接続後の動作概要を図 1 に示す．ネットワークに接続した端末に対して行うアクセス制御により，通信できる内容の違いによる状態は，以下の 3 つの状態として扱われそれぞれ状態の遷移を行う．ここで，端末がネットワークに新たに接続した時点では，認証前の状態である Pre-Auth の状態となる．

o Pre-Auth の状態（一部の通信のみ可能）

認証を行い成功した場合に①の OPEN 状態に遷移．一定時間内に認証が成功しなかった場合には④の CLOSE 状態に遷移を行う．

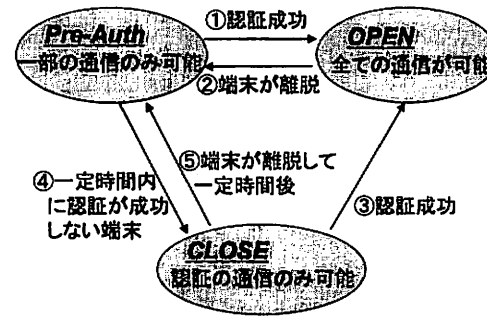

図１．基本動作

o OPEN の状態（全ての通信が可能）

端末が離脱またはログアウトにより利用を終了すると②の遷移を行う．

o CLOSE の状態（認証通信のみ可能）

認証を行い成功した場合に③の OPEN 状態に遷移．端末が離脱した場合には，一定時間後に④の Pre-Auth の状態に遷移を行う．

3.4. 認証方法

認証アクセスによりパスワードの様な認証情報を通信により送受信する場合には，今日の一般的なセキュリティ上の懸念より，以下について配慮されておく必要がある．

1) 認証に用いる通信経路の暗号化など盗聴への対策
2) 認証情報の送信先ホストの信頼性の検証
3) 認証に用いる情報の選択肢として ID/パスワードによる認証や，PKI に代用される公開鍵暗号化方式による証明書の利用

これらの機能を満たす認証に適用可能な選択肢の 1 つに SSL があり，1)については SSL を用いる事による通信路の暗号化，2)については通信相手先ホストを，サーバ証明書を用いる事での信頼性の検証，3）についてパスワード認証は SSL による通信の確立後にその通信内でやり取り可能であり，また，クライアント側の証明書についても使用可能である．これら 3 つの機能を同時に満たす事ができるため，本提案手法で用いる事とした．なお，実際に認証に関する AAA（Authentication Authorization Accounting）は，RADIUS を用いる事とした．

3.5. 認証およびアクセス制御の動作

図 2 に認証して利用を開始した後に離脱して利用を終了する場合のフローを示す．認証クライアントはネットワークに接続してきた端末であり，フィルタ装置が接続を検出し認証サーバに通知を行う．認証サーバでは認証している/認証していない端末の監視を行う

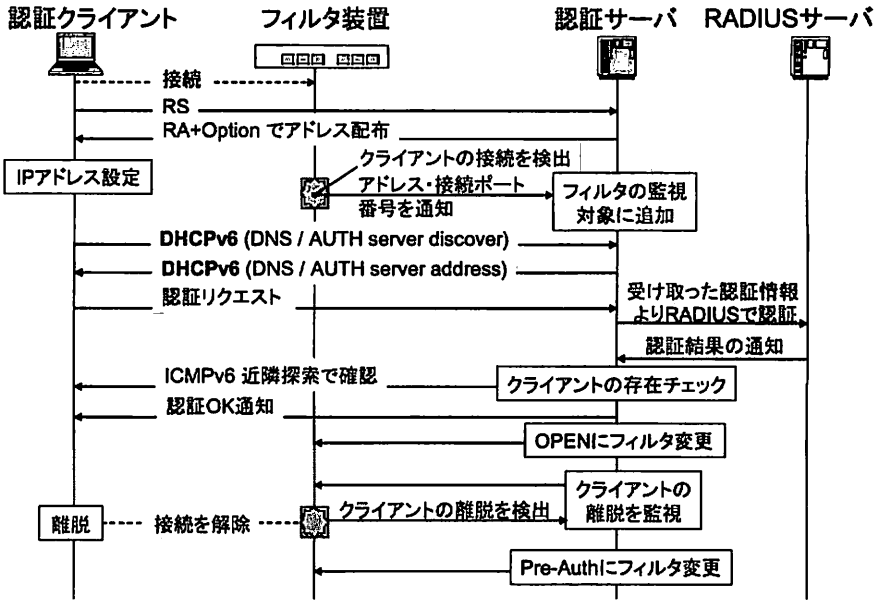

図2 認証およびアクセス制御のフロー

対象に接続してきた端末を追加する．

認証クライアントではそれと並行してアドレス設定や認証に必要な情報の取得を行い，それに基づき認証サーバに認証リクエストを送信する．認証サーバでは受け取った認証情報を RADIUS サーバに中継し認証可否の判断を行いクライアントに結果を通知する．認証に成功した場合には，クライアントが存在する事を確認した後にフィルタ装置に対してアクセス開放の設定変更を行い，認証が終了する．

認証成功後も認証サーバではクライアントの接続性を監視し，離脱した場合にはアクセス制御設定を元の Pre-Auth に変更する動作をする．

4. 実装と評価

4.1. 認証機能の実装

認証機能として，認証サーバ機能として Perl 言語により処理を行うサーバソフトを作成し，これには OpenSSL の簡易サーバ機能（特定 TCP ポートにて SSL 接続を受け付け，メッセージの送受信を行う機能）および FreeRADIUS による RADIUS プロトコルでの認証および同アカウンティングによる利用記録を合わせて利用する事とした．

認証クライアントにも同様に，Perl 言語により処理を行うクライアントソフトを作成し，SSL については同じく OpenSSL を利用した． なお認証用クライアントにはブラウザを用いる事も可能とした．

4.2. アクセス制御機能の実装

アクセス制御装置で行う制限は，OS に Linux を用いた PC を用意し，ip6tables によりフィルタのルールを追加変更する事で行った．なお，Pre-Auth 状態で利用できる通信内容には以下を設定した．

o Permit Dest-Port = 500（UDP） MIPv6 を利用するモバイルノードは，MIPv6 ではアクセス回線への接続や変更による接続情報の更新には，IPsec/IKE を用いた更新アクセスを行っており，認証前の一部許可設定に含めておく事でより更新に要する時間の短縮が可能になる．

o Permit Protocol = ICMP MAT を利用するモバイルノードは，接続切り替え後に利用するアクセス回線のメディアの品質についての測定等を行い，帯域やパケット間隔の違いに対して適切なバッファリングを行う試みがあり，接続回線の品質の影響を吸収する仕組みについて検討中である[6]．この測定には UDP の他に ICMP を用いて行っており，認証前の一部許可設定に含めておく事でよりスムーズなネットワークの移動が可能になる．

o Permit Port = 5004（UDP） ITU-T H323 による音声通信によりデフォルトで利用開始されるポート

o Permit Port = 554（UDP） Real Time Stream Control Protocol として IANA により"WELL KNOWN PORT NUMBERS"として割り当て済み．

4.3. 性能評価

図4に示す構成で各測定を行った．ここでは認証サーバが1台のサーバでアクセス制御装置を兼ねる構成とした．各ホスト間の通信遅延はホスト間の数値として図中に示すとおりである．各ホストのスペックは表1の機器を用いた．

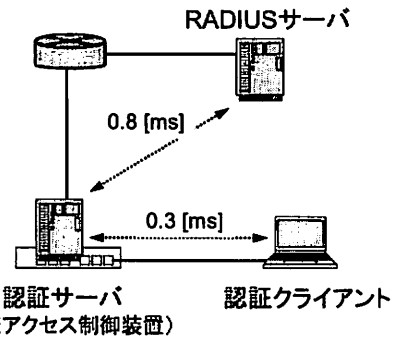

図3．テスト環境の構成

表1．テスト環境のスペック

認証クライアント	Celeron 2.2 GHz Debian 3.1
認証サーバ	Pentium4 2.4GHz VineLinux 3
RADIUS サーバ	UltraSPARCIII 900MHz Solaris8

認証クライアントは認証を行いネットワークへアクセスする端末であり，DHCP による認証サーバの取得から認証サーバとの間で認証を行う時間を認証時間として測定した結果を図4に示す．RADIUS 認証の結果は，RADIUS サーバで認証クライアントから認証サーバに送信された認証情報で認証を行う場合であり，比較のために RADIUS 認証を用いない場合をローカル認証として示した．RADIUS をもちいる本手法では，認証に要する約 150[ms]であるが，約 80%が RADIUS 認証部分であり，認証サーバで行っている DHCP による通知および認証情報の中継によるオーバーヘッドはローカル認証の場合の約 30[ms]との比較から約 20%となり，全体の認証時間から十分許容可能な範囲であると考えている．また，フィルタ設定に要する時間は，文献[9]で PC サーバによるアクセスリストの設定数による通信への遅延等について評価を行っているが，接続ホスト数が 1000 以下の場合には誤差程度の影響しかない事が得られている．設定の変更に必要な時間はおよそ約 100[ms]であり，認証時間とあわせると約 250[ms]になり，これが認証クライアントが認証を行いアクセスが開放されるまでの時間であり，許容できる範囲内であると考えている．

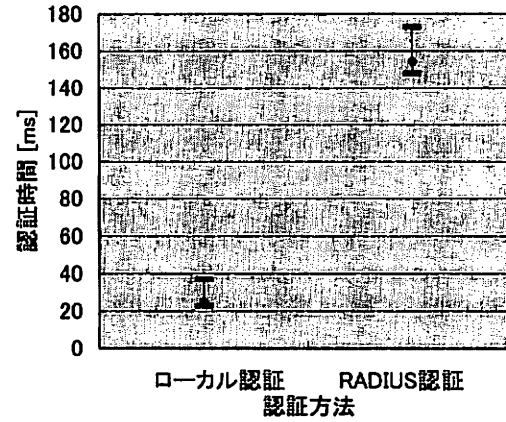

図4．認証時間

4.4. セキュリティについての考察

本提案手法のセキュリティ上の懸案として以下の2点についての考察を行う．

認証前利用の影響について　認証前に利用可能な通信としては，音声通話などの特定ポート番号の UDP パケットおよび特定の ICMP パケットのみを通過させる事を想定している．一定時間後（デフォルトで8秒後には全通信が遮断される事，および端末をネットワークから切断して 180 秒間，この制限された端末からの通信の再度の利用ができない事から，影響は少ないと考えている．

アクセス制御装置の機能の影響　許容時間内に認証が成功しなかった端末が多数存在する場合，それらを制限する際には，アクセス回線に設定できる制限の数の限界が影響する．本論文では PC ルータで構成する場合には問題にならない事を示しているが，スイッチ等で設定を行う場合には，機種によって異なるが 200 台前後が限界となる．

5. まとめ

本論文では，端末のネットワーク接続時における認証とアクセス制御について，モバイルノードの通信特性を考慮し，特定の通信を一定時間に限って許可できる方式についての提案と実装評価を行った．本提案手法をモバイルノードのアクセス回線への接続に用いる事で，関連する研究での測定等で得られている通信を「許可設定」にしておく事でハンドオーバーの特性に配慮した技術をそのまま利用する事が可能になる．

今後の課題としては，複数のアクセス認証環境を用意して実際にモバイルア端末によるハンドオーバーを行い，連続した通信を行うアプリケーションへの実機での影響についての評価やそれに伴う認証前に利用可

能な通信の内容についての検討を行う．

その他，評価に用いた構成よりフィルタ装置と認証サーバは実装に必要な Linux が動作する同一のホスト上で動作可能であり，認証クライアントを Linux で構成する事で，比較的容易にその配下に対して同様のアクセス認証が提供可能である．この状況は移動する認証クライアントを乗り物に例えると，そこに乗り込んで接続する端末がさらにそのクライアントとなる場合であり，これに対応するため２段以上の階層化接続された場合の認証サーバが行うクライアントからの認証情報の中継やその方法について検討中である．

謝辞

本研究の遂行にあたり御助力を頂きました，ネットワンシステムズ株式会社赤座正樹氏，杉本康則氏，岸田崇志氏に深く感謝致します．また，本研究の一部は日本学術振興会科学研究費補助金(17300019，17500037)，広島市立大学平成 17，18 年度特定研究費(5111) の支援を受けて実施しています．ここに記して謝意を表します．

文　献

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF, RFC 3775, Jun. 2004.

[2] Ishiyama, M., Kunishi, M., Uehara, K., Esaki, H. and Teraoka, F.: LINA: A New Approach to Mobility Support in Wide Area Networks, IEICE Transaction on Communication, Vol.E84-B, No.8, pp.2076-2086 2001.

[3] 相原，藤田，前田，野村，"アドレス変換方式による移動透過性インターネットアーキテクチャ，" 情報処理学会論文誌，Vol.43, No.12, pp.3889-3897, Dec. 2002.

[4] 竹内，鈴木，渡邊，"エンドエンドで移動透過性を実現する Mobile PPC の実装と評価，" DICOMO2005, pp.125-128, Jul. 2005.

[5] IEEE 802.1X　http://www.ieee802.org/.

[6] ネットワーク遅延の変化を制御するシームレスハンドオーバ手法の提案と評価」,情報処理学会研究会報告，Vol.2005, No.101, pp.55-60, 2005 -DSM-39(9).

[7] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, "Protocol for Carrying Authenti- cation and Network Access (PANA)", IETF, Internet-Draft, 2006

[8] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) ", IETF (Standards Track), RFC3315, 2003

[9] 西村，秋成，野村，相原，"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.662-630, 2002