研究計画書
移動体通信環境における AAA システムに関する研究

慶應義塾大学環境情報学部

自署：＿＿＿＿＿＿＿＿＿＿

学籍番号 79859316

平成 13 年 5 月 13 日

概要

IPv6 の導入により，利用者と共に移動する計算機にも通信機能が付加され，新たなサービスが生まれてくる．既存のインターネットアーキテクチャは移動しない計算機を前提に構築されているため，移動する計算機をインターネットに接続する際に様々な制約や問題が起こる．本研究では，特に認証，権限付与，課金に着目し，移動体通信環境に適した AAA システムの構築を行なう．本研究により，複数の ISP にまたがって利用可能な認証，権限付与，課金機構が実現され，移動する計算機は場所を選ばずインターネットに接続することが可能になる．

1 背景

Internet Protocol version 6(IPv6) の導入により，いわゆる計算機だけでなく，携帯電話，PDA(携帯情報端末)，自動車といった利用者と共に移動する機器がインターネットに接続されようとしている．

例えば，携帯電話をインターネットに接続すると，自宅のパソコンと携帯電話とでテレビ電話を行なったり，携帯電話から家電を操作することができる．また，自動車をインターネットに接続すると，スリップ情報を集めて道路の凍結状況を調べることができる．自動車の位置情報を取得して，先に行く友達の車と同じ道順をナビゲーションさせることができる．

利用者と共に移動する計算機をインターネットに接続し，あらゆる機器と双方向に情報をやりとりさせることで，前述のような今までにない新しいサービスが生まれてくる．

2 移動する計算機をインターネットに接続する際の問題点

既存のインターネットアーキテクチャは，移動しない計算機を前提に構築されている．そのため，携帯電話や自動車などの利用者と共に移動する計算機 (以後，移動体計算機) をインターネットに接続する際に様々な制約や問題が起こる．

例えば，移動体がインターネット接続業者 (Internet Services Provider, ISP) A のネットワークから ISP B のネットワークへ移動する場合を考える．利用者はインターネットに接続された携帯電話を利用して音楽ストリーミングを観賞しているとする (図 1)．ここでいう移動体とは，移動体計算機とその利用者を指す．

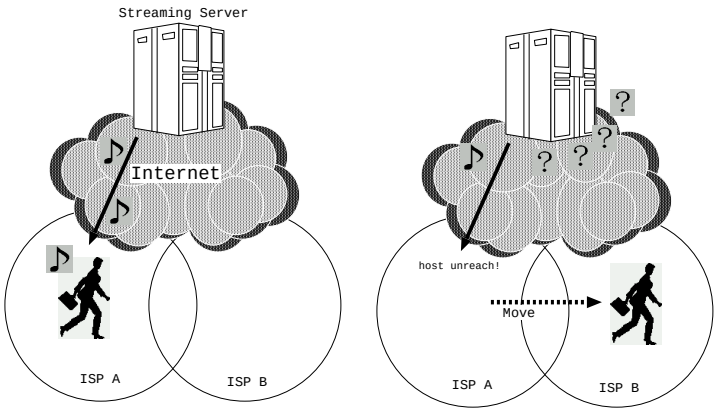

図 1: ストリーミングの例

移動体が ISP A から ISP B に移動することにより，携帯電話の識別子である IP アドレスが変化する．IP アドレスが変化することにより，通信が遮断され，音楽ストリーミングが中断されてしまう．ストリーミングサーバは携帯電話を特定で

きないため，音楽ストリーミングを再開することができない．通信を再開するためには，携帯電話の IP アドレスをストリーミングサーバに通知する必要がある．しかし，悪意を持った第 3 者になりすましが行なわれる危険性が高い．

また，移動体は複数のネットワークをまたがって移動するが，利用者がそのネットワークを常に利用できる権限を持っているとは限らない．移動体が ISP A，ISP B のネットワークを利用するためには，両方の ISP と契約をする必要がある．契約を結ぶことができたとしても，利用者は両方の ISP に接続料金を支払うことになる．また，ネットワークを移動する度にアカウントを切替える必要があり繁雑である．

3 インターネットにおける移動体支援に関する研究

これらの問題を解決するために，インターネットにおける移動体支援に関する研究が盛んに行なわれてきた．

3.1 解決された問題

これまでの研究の成果として，移動体が常時安定してインターネットに接続できること (常時接続性) アプリケーションから移動を隠蔽すること (移動透過性) 一意な識別子を用いて通信を開始できること (着信可能性) が挙げられる．

これにより，通信が遮断される問題，移動体計算機を特定することができない問題が解決した．

3.2 解決すべき問題

第 3 者によるなりすましの問題やネットワークを利用する権限の問題は解決されていない．今後，インターネットにおける移動体支援を実社会のインフラとして広く運用するためには，以下に挙げる項目の実現が重要になる．

- なりすましを防ぐための移動体計算機の認証
- 複数の ISP にまたがった利用者の認証
- 認証した利用者にネットワークを利用できる権限の割り当て
- 複数の ISP にまたがった課金情報の管理

課金を正しく行なうためには利用者を正しく認証できる必要があるなど，これらの項目は互いに密接な関係にある．したがって，これらの項目を統括的に解決できる枠組が望まれる．

4 研究の目的

本研究では，上記の問題を解決する移動体通信環境に適した認証 (Authentication)，権限付与 (Authorization)，課金 (Accounting) システム (以後，AAA システム) を構築する．

既存の AAA システムを移動体通信環境に当てはめた場合に起こる問題を整理し，移動体支援環境に適した AAA システムのモデルを提案し，実装する．また，そのモデルを構築する上で障害となる問題を解決する．

5 既存の AAA システム

既存の AAA システムを移動体通信環境に当てはめた場合に起こる問題を整理するために，既存の AAA システムについて述べる．

5.1 RADIUS

RADIUS[1] は，現在，ほとんどの ISP で利用されているダイヤルアップユーザの AAA システムである．IETF によって標準化されている．電話回線などを通じて接続したユーザの認証，IP アドレスの割り当て，課金情報の収集といった機能を提供する．

システムは，ユーザや属性を登録したデータベースを集中管理する「RADIUS サーバ」と、ダイヤルインアクセスを受け付けるサーバが「RADIUS クライアント」から構成される．両者は互いにユーザや属性の情報を交換する．

5.2 DIAMETER Mobile IP extension

IPv4 における移動体支援システムでは，IP Mobility Support(Mobile IPv4)[2] を拡張して AAA システムに対応した，Diameter Mobile IP Extension(以後，DIAMETER) [3] がある．DIAMETER AAA システムの特徴として，ISP をまたがったアカウント認証と権限付与機構，大規模 ISP でも利用可能な規模性をもつ Security Association(SA) の鍵配布機構，課金情報を管理する枠組が挙げられる．

6 既存の AAA システムの問題点

既存の AAA システムを移動体通信環境に当てはめた場合に起こる問題を挙げる．

6.1 アカウントの汎用性に関する問題

移動体は複数の ISP 間を移動する．ところが，現状 (RADIUS を用いたシステム) では ISP 毎に AAA システムを運用・管理しているため，利用者は複数の ISP と契約を結び，状況に応じてアカウントを切替える必要がある．

6.2 移動体計算機の認証に関する問題

移動体計算機は第 3 者によるなりすましが容易に行なわれる危険性が高い．RADIUS の認証は，利用者の特定つまりアカウントの認証であり，計算機自体を認証することはできない．通信相手が本当に自分の通信したい計算機であることを保証するためには，移動する計算機自体の認証できる枠組の実現が重要である．

6.3 プロトコル依存性に関する問題

DIAMETER は Mobile IPv4 の拡張であるため，Mobility Support in IPv6(Mobile IPv6)[4]，Location Independent Networking for IPv6(LIN6)[5] など，他の移動体支援プロトコルで利用できない．

7 問題点解決へのアプローチ

上記の問題を解決するために考慮すべき項目を以下の 6 点とする．

7.1 分散性を考慮した認証機構

認証サーバをすべての ISP で共有し，アカウント管理を集中して行なえば，単一のアカウントで複数の ISP を利用することができる．しかし，この方法は規模性に限界がある．各 ISP ごとに認証サーバを管理し，他の ISP は該当する ISP の認証サーバに問い合わせることにより，アカウントを認証できる機構が望ましい．

7.2 認証情報の保護

認証用のユーザ ID やパスワードなどの情報は，第 3 者に知られてはならない．したがって，認証される移動体と認証サーバ間で認証情報を暗号化し，セキュリティを高める機構が必要である．

7.3 利用制限

利用者が正しく認証され利用権限が得られるまでは，必要以上にネットワーク資源を利用できないようにするべきである．しかし，認証のために通信を行なう必要があるため，認証情報を移動体から認証サーバまで転送するサーバを設置し，移動体がネットワークに接続された時にそのサーバが特定できる仕組みが必要である．

7.4 切断検出

移動先の ISP をどのくらい利用したかを正しく記録するために，移動体がネットワークから切断されたことを検出できる仕組みが必要である．しかし，なんらかのアクシデントで突然切断される可能性があるため，移動体からの切断要求を利用することは難しい．

7.5 自動鍵交換

すべての通信相手となる計算機との SA をあらかじめ保持しておくことは不可能に近い．したがって，移動体計算機を認証するための鍵を自動的に交換する機構が必要である．

7.6 プロトコル非依存

システム自体の汎用性を考えると，移動体支援プロトコルに依存しない機構が必要である．

8 システム概要

8.1 私が提案するシステム

上記のアプローチを基に，問題点を解決するモデルを提案する．

図 2 に，システムの概要を示す．移動体 (Mobile Node) に対して，移動先のネットワークを Visited ISP，契約関係にある ISP を Home ISP とする．

(1) 移動体は Visited ISP のネットワークに接続されると，なんらかの方法を用い，はじめに通信をするべき相手 (Attendant Server) を知る．途中経路における情報の改竄やなりすましを防止するため，認証情報を暗号化する．なお，移動体と Home ISP の AAA サーバ (Home AAA Server) は，あらかじめ契約関係にあるため，暗号化のための鍵を保持できる．

(2) 移動体は，Attendant Server に認証情報を送信し，ネットワークの利用許可を待つ．

(3)Attendant Server はローカルの AAA サーバ (Local AAA Server) に対し，認証情報の確認を行なう．

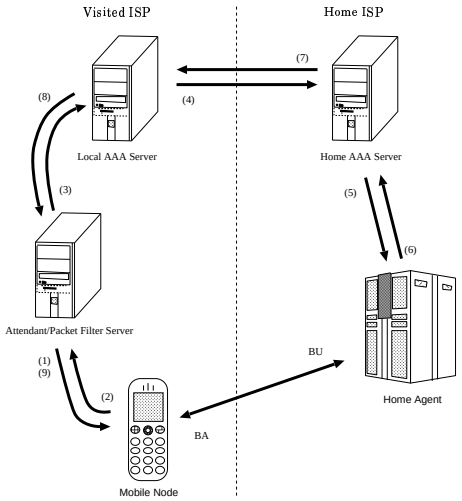

図 2: システム概要

(4)Local AAA Server は，Home AAA Server 対して認証情報の確認を行なう．ここで，AAA サーバを Visited ISP と Home ISP に設置した理由は，AAA 情報のバックアップさせるためである．

(5)(6)Home AAA Server は，認証情報の確認を行なう．また，移動に影響を受けない固定の IP アドレスと実際に利用可能な IP アドレスの対応を行なうサーバ (Home Agent) に対して，計算機を認証するための SA 用の鍵を要求する．

(7)(8)Home AAA Server は，認証が成功したことを Attendant Server に伝える．

(9)Attendant Server は，移動体にネットワークの利用許可を通知し，SA 用の鍵を受け渡す．

なお，認証に有効期限をつけることで切断検知を行なう．通信をつづけたい場合は，移動体は有効期限が切れる前に上記のやりとりを繰返し行なう．

8.2 検討すべき課題

上記のシステムを実現するために，今後検討すべき課題を挙げる．

- どのように移動体が Attendant Server を知るか
- どのパラメータを利用者の認証情報とするか
- どの技術を移動体と Home AAA Server との鍵に用いるか
- 適切な Attendant Server の設置場所はどこか
- 適切な有効期限とは

9 まとめ

IPv6 の導入により，利用者と共に移動する計算機にも通信機能が付加される．既存のインターネットアーキテクチャは，移動しない計算機を前提に構築しているため移動する計算機をインターネットに接続する際に様々な制約や問題が起こる．本研究では，特に認証，権限付与，課金に着目し，移動体通信環境に適した AAA システムの構築を行なう．本研究により，複数の ISP にまたがって利用可能な認証，権限付与，課金機構が実現され，移動する計算機は場所を選ばずインターネットに接続することができる．

10 実現される世界

本研究の成果を利用することにより，次に挙げるような世界が実現される．

10.1 複数の ISP をまたがって利用可能なアカウント

キャンパスでは慶應義塾が提供するネットワーク，成田エクスプレスの中では JR 東日本が提供するネットワーク，飛行機の中では航空会社が提供するネットワークを利用したい．既存の AAA システムでは，慶應義塾，JR，航空会社それぞれと契約しなければ，それぞれのネットワークを利用することができない．本研究の成果である AAA システムを利用すれば，ひとつの ISP とさえ契約すれば世界中のネットワークを利用できる．

10.2 インターネット接続性の開放

直接契約関係になくても，自分のネットワークを利用したアカウントに対して正しく課金できるため，小規模 ISP が増加する．例えば，自分の家が常時インターネットに接続されている場合に，昼間は不在なので無線 LAN を用いてネットワークを軒先に開放する．この無線 LAN を介してインターネットに接続した利用者に対して，その利用に対して課金できる．

11 これまでの研究活動

未踏ソフトウェア創造事業

本研究の基礎となる IPv6 による移動体支援プロトコルは,「次世代移動体通信支援システムの構

築」として，平成 12 年度未踏ソフトウェア創造事業 [6] に採択された．本プロジェクトでは，移動体支援プロトコルである Mobile IPv6 の開発および VoIP を用いたインターネット携帯電話システムを構築を行ない，私は全般に携わった．

このシステムは，電話番号として IP アドレスを用いたが，やはり第 3 者によるなりすましなどの危険性が明らかになった．

Mobile IPv6 相互接続実験

Sun Microsystems が主催する相互接続テスト「Connectathon 2001」に参加し，Mobile IPv6 相互接続実験を行なった．

Mobile IPv6 の基本的な相互接続が確認できたが，IPSec の SA を確立する際に不都合が生じ，改善の必要性が実証された．

12 政策・メディア研究科に進学を希望する理由

慶應義塾大学 政策・メディア研究科は，IPv6 をはじめとする次世代のインターネット技術の研究に積極的に取り組んでいる．また，インターネット自動車などの計算機以外のものに IP を組み込むという研究も非常に活発に行なっている．私の研究を行なう上で，これらの研究をしている方々からの意見は必要不可欠であり，また上記の研究から生み出されたものを実際に運用する上で私の研究は非常に有用なものであると考えている．

また，政策・メディア研究科では私が研究を希望するコンピュータサイエンスの分野ばかりでなく，政策系、情報系ともに広範な研究が行われ、実社会と関連した実際のイベントやプロジェクトが進められており，その先進の研究と関連プロジェクトの体験を本研究に役立てることができる．

これらの理由から，私は政策・メディア研究科への入学を強く希望する．

参考文献

[1] C. Rigney, A. Rubens, W. Simpson, S. Willens, “Remote Authentication Dial In User Service (RADIUS)”, Request for Comments, April 1997.

[2] C. Perkins, “IP Mobility Support”, Request for Comments, October 1996.

[3] Pat R. Calhoun, Charles E. Perkins, “Diameter Mobile IP Extensions”, Internet-Draft, April 2001.

[4] David B. Johnson, Charles E. Perkins, “Mobility Support in IPv6”, Internet-Draft, 17 November 2000.

[5] Fumio Teraoka, Masahiro Ishiyama, Keisuke Uehara, Mitsunobu Kunishi, Hiroshi Esaki, “LIN6: Mobility Support in IPv6 based on End-to-End Communication Model”, Internet-Draft, 8 December 2000.

[6] 平成 12 年度未踏ソフトウェア創造事業, http://www.ipa.go.jp/NBP/12nendo/12mito/.