2015 年度 森泰吉郎記念研究振興基金　研究者育成費

研究成果報告書

公衆 Wi-Fi のためのユーザプロビジョニングシステムの構築

政策・メディア研究科　延　優介

1. はじめに

来たる東京オリンピック開催に向け，様々な ICT 施策が検討されている．中でも無料公衆無線 LAN 環境の整備に対するニーズは極めて高い．観光庁の報告[1]によれば，外国人観光客が訪日中に一番困ったこととして，「無料公衆無線 LAN 環境」を挙げている．日本でも公衆無線 LAN サービス自体は普及が進んでいるものの，外国人観光客をはじめとして，各地を初めて訪れた利用者が容易に使えるものとはなっていない．

利用者によるインターネットアクセスの悪用や，逆に悪意のあるアクセスポイントが設置されることによる情報窃取などのリスクを踏まえれば，単に無認証のアクセスポイントを設置して使わせれば済むということにはならない．無線 LAN サービスの利用者と提供者が互いに信頼関係を構築した上，サービスが提供される形が望ましいと言えよう．しかしサービス利用者が安全なサービスを選択し，利用登録を経て利用に至るというプロセスは煩雑となるケースが多く，これを回避する形で安全性の低い無認証サービスが増加する傾向がある．

私は利用の開始時点において，公衆無線 LAN サービス提供者と利用者間の電子証明書の交換を行うことで安全性を担保するユーザプロビジョニングが，安全な公衆インターネットサービスの提供においては必須であると考える．それにより発生するコストを低減するために，NFC[2]を用いることによって簡便に行う手法を提案する．交換した電子証明書を用いて EAP-TLS 認証[3]を行うことにより，サービス提供者と利用者間の相互認証を実現する．

以下，2 章で関連研究，3 章でユーザプロビジョニング方式について整理したのち，4 章で解決手法の提案を行う．5 章で具体的な提案システムの実装と評価について解説し，最後に 6 章でまとめについて述べる．

2. 関連研究

サービス利用開始時の，利用申し込み，アカウント発行，システムへの登録などの一連の作業を，本稿では「ユーザプロビジョニング」と定義する．

公衆無線 LAN サービスのセキュリティについて数多くの危険性が指摘されており[4]，これらの問題を解決すべく京都を中心として運用されている公衆無線インターネット接続プロジェクトが，「みあこネット」である[5][6]．「みあこネット」は，悪意のあるアクセスポイントへの誤った接続の防止や課金のための利用記録の採取を行うため，サービス提供者と利用者間での「相互認証」が必要不可欠であるとの考えのもと，Virtual Private Network(VPN)プロトコルを用いることでこれを実現している．

安全な公衆無線インターネット接続を可能にした「みあこネット」であるが，この運用方式が今日の公衆無線 LAN サービスのスタンダード運用モデルになっていない点を考慮すると，いくつかの課題が考えられる．

実証実験段階での「みあこネット」プロジェクトでは，無線基地局から利用可能な PPTP(Point-to-Point Tunneling Protocol)[7]アカウントの発行について，京都駅などの無線基地局設置場所において，対面での本人認証に基づいた発行を行っていた．対面での本人確認はコストが高いだけでなく，書面での契約等やや繁雑なプロセスが必要となり，特に外国人観光客へのハードルは非常に高い．

これらの課題の多くはユーザプロビジョニングの複雑性に起因しており，そのコストの高さが普及へのネックとなっている．その結果，相互認証を伴わない片側認証，あるいはそもそも認証自体を省略した公衆無線 LAN サービスが展開されているのが現状である．そこで本稿では，ユーザプロビジョニングのコストを低減させ，相互認証を実現した安全かつ利用者にとって利便性の高い公衆無線 LAN サービスシステムの提案を行い，プロトタイプシステムの実装について述べる．

3. ユーザプロビジョニング方式

現状運用されている公衆無線 LAN サービスでのユーザプロビジョニング方式は大きく二種類に分けることができ，本稿ではそれぞれ事前登録型とオンサイト登録型と呼ぶ．

3.1 事前登録型

サービス提供者と利用者がサービス利用に先立って登録を行う形態を，本稿では事前登録型と呼ぶ．日本国内においては携帯電話事業者が，契約者向けに提供しているサービスが典型的である．

サービス利用者（契約者）はサービス提供者（通信事業者）と事前に契約を結んでおり，サービス利用者はサービス提供者に個人情報を提示することにより，サービスの利用を許可される．サービス利用者は接続したいアクセスポイントを選択し，SIM カードを用いた無線接続を行うだけでインターネット接続が可能となり，認証にかかる時間を大幅に減らすことができるメリットがある．これは，無線接続の認証自体に契約者の個人情報を使用しており，サービスにアクセスしてくるユーザが正規のユーザであるかどうかの確認を接続と同時に行っているからである．サービス未契約者はサービスにアクセスすることはできない．

サービス提供者はサービス利用者の個人情報を管理することができ，サービスを犯罪行為等の不正利用に悪用された場合，サービス提供者は接続元ユーザの個人情報を追跡することが可能である．しかし，本サービス形態は事前に契約を行うことが前提となっているため，外国人観光客が本サービス形態を利用する場合にも日本国内の携帯電話事業者と契約を結ぶ必要があり，国内利用者の場合と比べて契約までのハードルは高い．また，使いたい時に即時利用開始することができないといった問題も挙げられる．

3.2　オンサイト登録型

サービス利用者が訪問した現地で初めて利用登録を行い，公衆無線 LAN サービスの利用を開始する形態を本稿ではオンサイト登録型と呼ぶ．地方自治体などが外来者，観光客向けに無料でインターネットアクセスを提供する事例などが典型的である．外国人観光客に対する受入環境整備として，観光庁が推進している「無料公衆無線 LAN 環境」もこれに当たる．即時利用が可能であり，利用開始までのプロセスが簡単であるといった特徴が挙げられる．

認証なしの無線 LAN サービスに利用者が端末を接続し Web のアクセスを行うと，利用申し込みサイトへと転送されるといった形態が典型的である．利用申し込みサイトにおいては，氏名や連絡先，支払い情報等の登録を行い，利用規約等への同意をとりつけた上でサービスを開始する．

利用者にとっては現地で初めてサービスを選択し接続することになるため，その場でサービスの信頼性を判断する必要がある．多くの場合利用開始のプロセスが簡単であるものの，サービス利用者が正式なサービスを正しく選択するのは難しく，悪意のあるアクセスポイントに誤って接続してしまうといったリスクが懸念される．

表 1 に，3.1，3.2 で説明したそれぞれの方式の特徴と課題を示す．

表 1 ：ユーザプロビジョニング方式の比較

	特徴	課題
事前登録型	○サービス利用に先立ってオフサイトで登録を行う形式 ○携帯電話事業者が契約者向けに提供しているサービスが典型的（SIM を利用） ○相互認証を実現している	○書面での手続きなど事前に重たいプロセスが必要となり，外国人観光客等には高いハードルとなっている ○使いたい時に即時利用開始することができない
オンサイト登録型	○ユーザが訪問した現地で利用者登録を行い，サービスの利用開始を行う形態 ○地方自治体などが外来者，観光客向けに無料でインターネットアクセスを提供するサービスが典型的 ○即時利用が可能，利用開始が簡単	○サービス利用者が正式なサービスを正しく選択するのは難しく，中間者攻撃のリスクがある

3.3 相互認証のためのユーザプロビジョニング

インターネットのようなオープンなネットワーク環境では，サービス利用者と提供者は互いに未知であり，お互いが信頼できる相手であるかどうかを確認する必要がある．相互認証のためのユーザプロビジョニングとして，実現されている代表的な方式を以下に示す．

3.3.1　EAP-SIM 方式

EAP-SIM 方式[8]は SIM カードを用いた相互認証方式であり，携帯電話事業者が提供する公衆無線 LAN サービスの大半は，本方式を用いて運用されている．SIM カード内にある契約者情報を用いるため，認証にかかる時間を大幅に短縮することができるが，事前手続きが必要であり即時利用開始できない他，物理的なハードウェアを必要とするため，コストが高くなる問題は残る．

3.3.2　EAP-TLS/TTLS/PEAP 方式

EAP-TLS/TTLS[9]/PEAP[10]方式は，サーバ側の認証に電子証明書を用い，ユーザ側の認証を電子証明書やパスワードを用いて実現する相互認証方式である．本方式を利用するには事前の認証情報の交換手続きや端末での設定手続きといったプロセスが必要となり，一般的にはこれらが煩雑であるとされ，公衆無線 LAN サービスにおいて用いられることは少ない．

これらの方式から分かるように，相互認証を実現するには必ず事前に手続きやコストが生まれ，気軽に即時利用開始したいという，特に無料での公衆無線 LAN サービス利用者の需要と相反するプロセスを取る必要が生じる．このプロセスの煩雑さから，利便性を考慮しユーザ登録そのものを省略する傾向が起きており，相互認証を伴わない片側認証，ひいては認証行為自体を行わない公衆無線 LAN サービスが展開され続ける要因となっている．従ってこの問題を解決することができれば，利用者・提供者双方にとって，安全なサービスが利用可能になる．

4.　提案手法

4.1　NFC とユーザプロビジョニング

安全なユーザプロビジョニングを実現するには，中間者攻撃のリスクを考慮する必要がある．中間者攻撃の例を図 1 に示す．中間者攻撃とは認証情報の交換時に悪意ある攻撃者が認証情報の交換を行う二者の間に割り込み，交換する認証情報を用意した偽の認証情報とすり替えることにより，通信内容の盗聴や改ざんを可能とする行為である．無線区間は通信経路が直接確認できないため，悪意のある攻撃者が設置した偽のサービスを掴まされる危険性が高い．本稿では近距離無線通信規格である NFC の Peer-to-Peer モードを用いることで，この問題を克服した．

NFC Peer-to-Peer モードを用いた中間者攻撃対策を図 2 に示す．NFC の通信距離は 10cm 程度という非常に短い距離に限定されているため，悪意のある攻撃者が間に介在することが困難となり，中間者攻撃を物理的に防ぐことが期待できる．本稿では NFC とユーザプロビジョニングの親和性に着目し，NFC に基づく公衆無線 LAN サービスのユーザプロビジョニングを実現する．

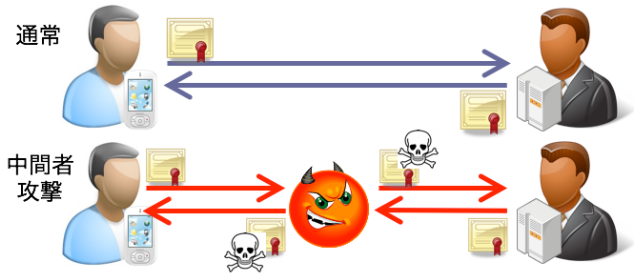

図１：中間者攻撃の例

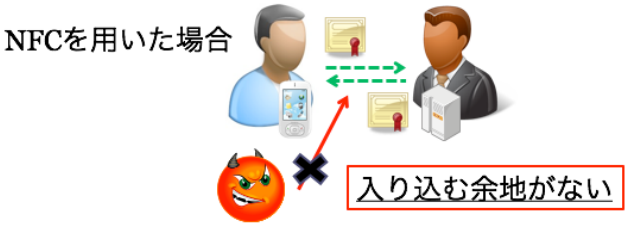

図２：NFC を用いた中間者攻撃対策

4.2　NFC を用いた安全な公衆無線 LAN ユーザプロビジョニング

公衆無線 LAN サービス提供者と利用者間の相互認証を実現するため，電子証明書を用いたユーザプロビジョニングを，NFC を用いた直感的で明示的なプロセスで実現する手法を提案する．利便性の観点で言えば OS の機能拡張等で対応されることが望ましいが，本研究では「証明書自動設定アプリ」を実装することでこれを実現した．

提案システム全体の構成図を図３に示す．公衆無線 LAN サービスを利用したいユーザは，予め端末に「証明書自動設定アプリ」を導入する．その後の過程は，以下に示す通りである．

1. 公衆無線 LAN サービスを利用したいユーザは駅の観光案内所等を訪れ，設置してあるアカウント発行機に，サービスに接続したい端末をタッチする．
2. アカウント発行機は基幹サーバへ https での通信を行い，アカウント生成モジュールが動的に動作し，証明書の自動生成が行われる．
3. 生成した証明書情報は，データベースサーバにアカウント登録される．
4. 端末へ相互認証用証明書データ（具体的にはクライアント証明書，SSID，ユーザ ID 情報）が送られ，適切な設定が端末で自動的に行われる．
5. サービス提供アクセスポイントへ自動接続を行う．
6. 電子証明書を用いた EAP-TLS 通信を行う．端末はサービス側のサーバ証明書，RADIUS サーバは端末が設定したクライアント証明書をお互いに検証し，正当性を確認する．
7. お互いの検証が完了し，正当性を確認できたらインターネットアクセスを開始する．なお，初回アクセス時は利用者登録ページへリダイレクトを行い，サービス提供ポリシーに則った利用者情報を登録させる．

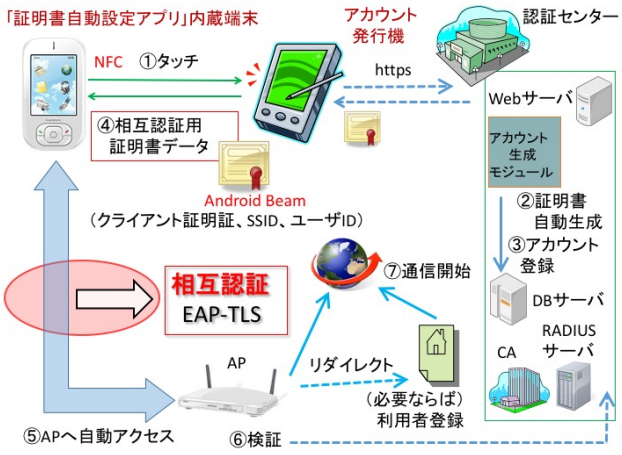

図３：ユーザプロビジョニングシステムの構成

本手法が安全に働くためにはアカウント発行機自体の信頼性が求められるが，これを駅の観光案内所等，利用者がその安全性を「容易に認識・確認できる場所」へ設置することで，その信頼性を担保する．認証無し SSID にアクセスして利用者登録を行うというよく採用される方式に比べて，偽のアクセスポイントに接続させられる危険性が低く，物理的な施設が介在することで信頼性の評価が容易に行えるメリットがある．

公衆無線 LAN サービスを利用したいユーザは，「アカウント発行機に接続したい端末をタッチする」という直感的な動作をとるだけで，これまで煩雑とされてきた相互認証のプロセスを達成することができ，安全なインターネットアクセスが可能となる．外国人観光客やセキュリティについて詳しくない人でも，取るべき行動が直感的に理解でき，その利便性は高い．相互認証を行っているため，偽アクセスポイントによる情報窃取等の攻撃を防止することができるのはもちろん，通信内容は暗号化されるため，通信の傍受に対しても耐性がある．また，データベースサーバと照合することで，インターネットアクセスを犯罪行為等に悪用した利用者の追跡を行うこともでき，サービス提供者・利用者共に，安全なサービス利用を行うことができる．

「NFC を用いてアカウント設定の手間を省く」というアプローチは，これまでも数多く提案されてきた．モバイル決済システムという領域において，ユーザがより単純に，簡単に決済を行うことを目的として，NFC を用いた決済システムが提案されている[11]．また，公衆無線 LAN の領域においても，NFC を用いたアカウント発行を行い，利用開始までのプロセスを簡便にすることを目指している類似研究がある[12]．これらは，NFC を用いて端末をタッチするだけで簡単に接続することができるという，NFC の特性に基づく「簡便さ」に着目し，ユーザの利便性向上に貢献したものである．我々のアプローチは，「単にアカウント情報を簡便に配布するだけではユーザは安全にならない」という考えのもと，サービス提供側の認証情報を端末側に送ることで，相互認証を実現させることにある．「NFC を用いてタッチする」というシンプルなプロセスにおいて実現されるのは簡便さだけではなく，信頼すべき相手を直感的な方法で指定し，かつその通信距離の短さから中間者攻撃を排除することができるという，重要な特性

も持ち合わせている．この特性に着目した安全な認証情報の交換を行うことで，EAP-TLS 通信を用いた相互認証に基づく，安全かつ簡便な公衆無線 LAN サービスを利用できるという点に，本研究の独自性がある．

5. 実装と評価

前章で提案したモデルの有効性を評価するため，実験システムの構築を行った．大きくクライアント側とサービス側の二つに分けることができ，本章ではそれぞれの実装と機能について述べる．

5.1 証明書自動設定アプリ

クライアント端末に予め入れておく，証明書自動設定アプリの実装を行った．Android アプリケーションとして構築し，以下の機能を実装した．

①端末とアカウント発行機間で通信する機能
②受け取った証明書を端末に自動設定する機能
③サービス提供アクセスポイントに自動接続する機能

本アプリを導入した端末をアカウント発行機にタッチすることを契機に，ユーザアカウント自動発行システムが動作し，端末に相互認証用証明書データが Android Beam で送られる．送られてきた証明書データを適切にインポートし，サービスが提供しているアクセスポイントに自動接続を行う．その後 EAP-TLS 通信を行い，双方の検証が認められたのち，実際のインターネットアクセスを開始する．

5.2 ユーザアカウント自動発行システム

本システムの基幹サーバとなるユーザアカウント自動発行システムの実装を行った．具体的にはアカウント生成モジュール，RADIUS サーバ，Web サーバ，データベースサーバから構成されており，以下の機能を実装した．

①相互認証用証明書データを生成し，生成したユーザ ID と証明書情報をデータベースへ動的に登録する機能
②接続元証明書データの検証を行い，検証が認められたのち，実際のインターネットアクセスを許可する機能

アカウント発行機からの https リクエストに応じ，アカウント生成モジュールが動的に証明書データの自動生成を行う．生成された証明書データはデータベースサーバにアカウント登録されるのと同時に，アカウント発行機にレスポンスとして送信する．また，サービス利用者の正当性検証を，データベースサーバと照合することにより行う．

5.3 評価

本稿における評価は，公衆無線 LAN サービスに接続したい端末をアカウント発行機にタッチし，実際の通信を開始するまでの過程を対象とし，実用的なレスポンスでの動作が可能であるかを検証するものとする．

検証の結果，タッチを行ってから 1 秒以内で実際の通信が開始されることを確認できた．これは，「タッチした端末を Wi-Fi につないでインターネットアクセスを行う」というユースケースにおいて，問題のないパフォーマンスである．また，一度端末に相互認証用証明書データの設定を行うと，その後のサービス接続時に再び設定を行う必要はなく，必要となる労力は，最初に「アカウント発行機を訪れてタッチする」という行為のみである点も，加えて評価できる．

6. まとめ

直感的な動作で，安全かつ簡単にユーザプロビジョニングを実現した本方式は極めて有益であり，今後様々な運用形式で普及が進むべきである．例えば駅の自動改札機の様に，オリンピック会場の入場ゲートにアカウント発行機の設置を行う．スタジアムを訪れた観客は入場ゲートを通る際に，公衆無線 LAN サービスに接続したい端末を入場ゲートにタッチを行うだけで，安全な公衆無線インターネットアクセスを実現させることができる．また，今後普及が見込まれる電子チケットとの親和性も高い．

活動報告として、複数の国内外の学会にて研究発表を行った。また、これらで頂いたコメントを元に本研究を発展させ、評価検証を主に行い、修士論文の執筆を行った。

参考文献

[1] 国土交通省観光庁，“【資料 1】外国人旅行者の日本の受入環境に対する不便・不満”，http://www.mlit.go.jp/common/000205584.pdf，平成 23 年度第 3 回訪日外国人旅行者の受入環境整備に関する検討会（平成 24 年 3 月 14 日），2012.
[2] “ Information technology. Telecommunications and information exchange between systems. Near Field Communication. Interface and Protocol (NFCIP-1)”, ISO/IEC 18092:2013 ED2, 2013.
[3] D. Simon, B. Aboba, and R. Hurst, “The EAP-TLS Authentication Protocol”, RFC5216，2008.
[4] 清水 渉, 小林 稔幸，“無線ホットスポットサービスのセキュリティ”，情処学研報，2002-DPS-107，2002.
[5] 大平 健司,隅岡 敦史,北岡 有喜,古村 隆明,藤川 賢治,岡部 寿男，“公衆無線インターネット接続サービス「みあこネット」の設計と運用”，電子情報通信学会論文誌 B Vol.J93-B No.5 pp.759-768，2010.
[6] http://www.miako.net/
[7] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn，“Point-to-Point Tunneling Protocol (PPTP)”，RFC2637，1999.
[8] H. Haverinen and J. Salowey，“Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”，RFC4186，2006.
[9] P. Funk and S. Blake-Wilson，“Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)”，RFC5281，2008.
[10] H. Andersson, S. Josefsson, G. Zorn and B. Aboba，“Protected Extensible Authentication Protocol (PEAP)”，RFC2026，2001.
[11] John Bauer, Glenn Curtiss McMillen, Eric Crozier, Christine Ann Schuetz and Garry Lloyd，“Secure account provisioning”，US 20120078735 A1，2012.
[12] 宮下 悠生, 明石 雄太, 橋本 周平, 福井 千晶, 藤村 真生，“NFC を用いたセキュアな公衆無線 LAN 接続システムの構築”，2015 年電子情報通信学会総合大会，2015.