3X-01

NFC を用いた安全な公衆無線 LAN ユーザアカウントプロビジョニング

延 優介† 貫井 裕太‡ 原 正悟‡ 八槇 博史‡
慶應義塾大学† 東京電機大学‡

1 はじめに

2020 年の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．中でも外国人観光客への「おもてなし」として，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，外国人旅行者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，外国人旅行者をはじめとして，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．

我々は，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アカウント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人的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．その結果サービスの悪用や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，安全なインターネットアクセスが実現可能となる．

Secure User Account Provisioning of Public Wireless LAN Service Based on NFC
†Yusuke Nobu Keio University
‡Yuta Nukii, Syogo Hara, Hirofumi Yamaki
Tokyo Denki University

2 ユーザアカウントプロビジョニング方式

公衆無線 LAN サービスでのユーザアカウント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．表 1 に，それぞれの方式の特徴と課題を示す．

表 1: ユーザアカウント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	○書面での手続き等，重たいプロセスが必要となり，外国人旅行者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い ⇒ Man-in-the-Middle 攻撃のリスク

安全性の観点から見れば事前登録型は非常に有益であるが，事前登録が困難である利用者にとってはオンサイト登録型に大きなメリットがある．また，不特定多数の訪問者に対してサービスを提供するその性質からも，利用者一人一人とオフサイトで契約を行うことは効率が悪く，オンサイトでの利用者登録は何らかの形で行うことが望ましい．

サービス利用の最初の段階で，互いに未知である利用者と提供者の間に信頼関係を安全に構築することは，様々な主体が外来者にインターネットアクセスを提供する際に極めて重要である．また，利便性の観点から，信頼関係構築は簡単なプロセスにより実現されることが望ましい．

3 提案手法

本稿では公衆無線 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アカウント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」の実装を持ってこれを実現した．

提案手法全体の構成図を図 1 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，観光案内所等の安全が保証されている場所を訪れ，接続したい端末を設置してあるアカウント発行機にタッチする．
2. アカウント発行機は基幹サーバへ通信を行い，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. 端末へは相互認証用証明書データ（具体的にはクライアント秘密鍵，サービス側公開鍵，ユーザ ID 情報）が送られ，自動的に設定される．
5. サービス提供者が指定した SSID の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 RADIUS サーバのサーバ証明書，RADIUS サーバは端末が設定したクライアント証明書を互いに検証し，正当性を確認する．
7. 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．

本手法が安全に働くためにはアカウント発行機の信頼性が求められるが，これを観光案内所等に設置することでその信頼性を担保する．認証無し SSID にアクセスして登録する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

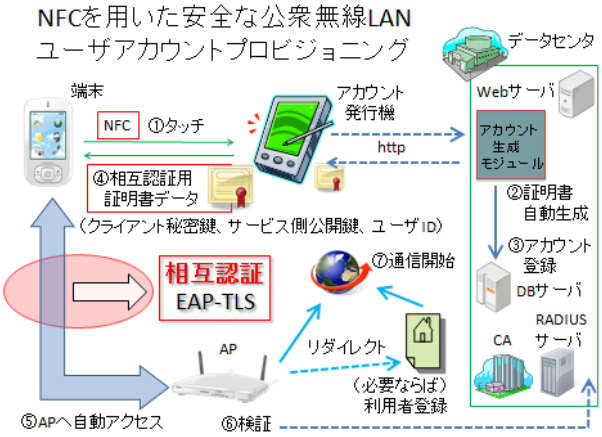

図 1: 提案手法全体の構成図

まで煩雑とされてきた相互認証のプロセスを実現することができ，安全なインターネットアクセスが可能となる．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，インターネットアクセスを犯罪行為等に悪用したユーザの追跡も可能となる．

4 おわりに

直感的な動作で，安全かつ簡単にユーザアカウント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や空港の到着口にアカウント発行機を設置しておけば，ユーザはスムーズにインターネットアクセスを実現することが可能となり，訪日外国人の満足度の向上は容易に見込まれる．また，一度証明書を端末に設定すれば，次回以降再度アカウント発行機を訪れる必要はない．証明書の有効期間を適切に設定することで，ユーザの利便性と管理の調整を行うことも可能となる．

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, March 2008.

[4] 延優介，八槇博史，“NFC を利用した公衆無線 LAN 相互認証”，FIT2014，2014.