L-023

NFC を用いた公衆無線 LAN 接続環境の構築
Building of Public Wi-Fi Connecting Environment using NFC

宮下 悠生† 橋本 周平† 福井 千晶† 藤村 真生†
Yuki Miyashita Shuhei Hashimoto Chiaki Fukui Masao Fujimura

1. はじめに

外国人観光客の増加に伴って、無料で利用できる公衆無線 LAN の需要が年々高まってきている [1] [2] [3]。観光庁の報告 [4]によれば、外国人観光客が旅行中で最も困ったことに無料公衆無線 LAN 環境が挙げられる。加えて、誰もが無料で利用できる公衆無線 LAN を増やすことを目標としている。現在、日本で提供されている公衆無線 LAN は手軽に利用できることを重視している。そのため、これらの多くは暗号化や相互認証などのセキュリティ対策をしていない。そのため、暗号化されていない通信データを盗聴される危険性がある。また、アクセスポイントの正当性を検証することができない問題もある。この問題によって、なりすまされたアクセスポイントに接続して悪意のあるサイトへ接続する危険性も指摘されている。加えて、利用者にインターネットアクセスを悪用される可能性がある。そのために利用者を追跡する必要がある。

無線 LAN で相互認証する方法として PKI を利用した EAP 認証 [5]がある。これは利用者認証の際、事前に認証情報の交換が必要である。従来であれば観光案内所などで書類を書くことが必要であり、人員コストがかかっていた。本研究では、相互認証で使用する認証情報の交換手法としてかざすことで通信することができる NFC [6]を用いる。これによって公衆無線 LAN サービス提供者と利用者間の相互認証を安全かつ容易に実現するシステムを提案する。

本稿では第 2 章で、現在の無線 LAN 認証方式について述べる。第 3 章で、無線 LAN 接続システムの構成及びその認証情報の交換手法と利用者追跡情報について述べる。第 4 章では、提案手法の評価とその結果について述べる。

2. 無線 LAN 認証方式

無線 LAN では認証と暗号化はセットになっている。そのため、認証方式により暗号化方式が決定する。現在、無線 LAN での主な認証方式として以下の 3 方式がある。

- オープン認証方式
  無線 LAN への接続交渉をしてきたすべての機器を承認してネットワークに接続させる方式である。認証をしていないため無線 LAN と利用者間の通信は暗号化することができない。
- 共通鍵認証方式
  無線 LAN アクセスポイントに設定されているパスフレーズを知っている利用者を認証する方式である。利用者端末ごとに通信を暗号化することができる。しかし、パスフレーズを多人数で共有するためパスフレーズが漏洩する危険性がある。また、利用者の判別はできない。
- 公開鍵認証方式
  EAP 認証に基づいて利用者ごとに発行された認証情報を検証して双方向で認証する方式である。サーバ認証には電子証明書を用い、クライアント認証には電子証明書を用いる EAP-TLS 方式やユーザ ID/パスワードを用いる EAP-PEAP 方式/EAP-TTLS 方式などがある。

利用者ごとに適切な利用制限を与えるためには、利用者を個別に認証する必要があると考える。また、無線 LAN は SSID によって識別されるため、オープン認証方式と共通鍵認証方式では、悪意のある第三者が正規のアクセスポイントと同じ SSID を使った場合、そのアクセスポイントの正当性を検証することができない。よって本稿では、公開鍵認証方式によって利用者ごとに認証する方法について考える。

3. 公衆無線 LAN 接続システム

公衆無線 LAN 接続システムである WAACS [7]についての概要や基本的な機能について説明する。

3.1 概要

WAACS は、公衆無線 LAN 提供者と利用者間の相互認証を実現するため、NFC を用いた接続手法を提供するシステムである。利用者は接続したい利用者端末を機器にかざすだけで安全で容易にネットワークに接続させることができる。

WAACS は図 1 のように利用者端末、認証情報発行機、認証サーバ、アクセスポイントから構成されている。利用者端末は、認証情報発行機から認証情報を受け取り自動で無線 LAN に接続する。本来、OS の機能にて自動で無線 LAN 接続することが望ましいが現在のところ Android の機能としてそのような機能はない。したがって、本研究では事前に無線 LAN 自動接続アプリを利用者端末に実装することでこれを実現した。

WAACS 利用の流れを以下に示す。

1. 利用者端末を認証情報発行機にタッチする。
2. 証情報発行機は認証サーバに対して SSL 通信で、認証情報発行を要求する。
3. 認証サーバは利用者端末で使用する認証情報を生成して認証データベースに登録する。そして、認証情報発行機に認証情報を送信する。
4. 認証情報発行機は利用者端末に NFC を使って SSID などのアクセスポイント情報とともに認証情報を送信する。
5. 利用者端末は自動で無線 LAN 自動接続アプリを起動して認証情報で指定されたアクセスポイントに接続を試みる。
6. アクセスポイントは認証サーバに対して認証情報の検証をして問題なければインターネットへのアクセスを

† 大阪工業大学大学院工学研究科, Graduate School of Engineering, Osaka Institute of Technology

開始する。この際、必要であれば初回アクセス時に利用規約同意や利用者情報登録画面を表示する。

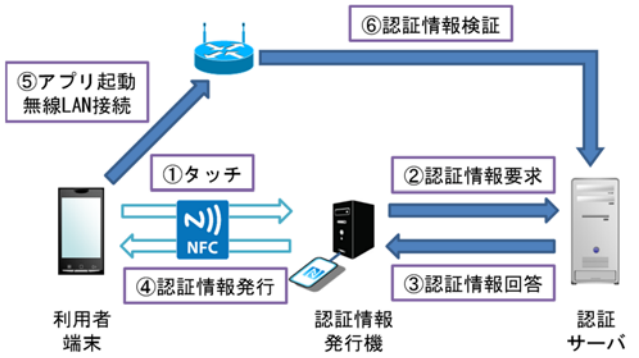

図 1 システム概要

3.2 認証情報とその交換方法

利用者端末・認証サーバ間の認証情報及びその交換方法について述べる。

本研究での無線 LAN 認証方式として EAP-PEAP 認証を使用する。これにより認証サーバはユーザ名とパスワードにより利用者端末の認証ができる。また、利用者端末は無線 LAN 接続交渉時に送られるサーバ証明書により認証サーバの認証ができる。サーバ証明書は、本来第三者の認証局により正当性を検証されてから発行する必要がある。しかし、第三者の認証局から発行してもらうにはコストがかかる。提案方式では、利用者端末が認証情報発行機へ物理的に接続することによってサーバ証明書を信頼したと考えることができる。したがって、図 2 に示すように 1 回のタッチで情報交換することができる。

認証情報発行機は、利用者端末のタッチを検知するとタッチされた時間と認証情報発行機情報を認証サーバに送信して認証情報を要求する。認証情報には、EAP-PEAP 認証で使用するユーザ名とパスワードの情報以外にもサーバ証明書が含まれている。これにより、利用者端末は無線 LAN 接続交渉時に認証サーバより取得したサーバ証明書と NFC によって取得したサーバ証明書が同じであることを確認することができる。それによりなりすましされた無線 LAN アクセスポイントに接続することを防ぐことができる。

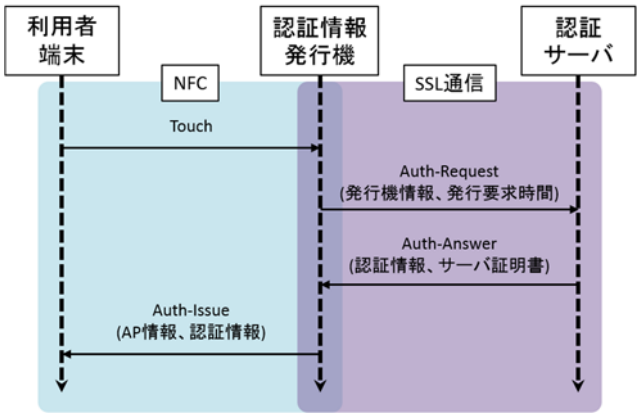

図 2 認証情報シーケンス

認証サーバ・認証情報発行機間の通信はネットワーク的に離れた場所にあるため、暗号化された方式で通信する必要がある。これは、SSL を使用してサーバ・クライアント証明書によって認証及び暗号化することで安全に通信することができる。

3.3 利用者追跡情報

公衆無線 LAN では、利用者が不正行為をした際に利用者を特定するための情報を保存しなければならない。提案方式では、無線 LAN 利用する際に認証情報発行機にタッチする必要がある。よって、認証情報発行機を監視カメラがある場所に置くことにより、いつどの認証情報発行機を使用したかが分かれば利用者の情報を取得することができる。

4. おわりに

利用したい公衆無線 LAN の認証情報発行機にタッチすることで、安全に公衆無線 LAN を利用することができる本方式は、非常に直感的であり、誰にでも利用できる方式であるといえる。さらに、EAP 認証方式による認証を使用することによって現状よりも細かい利用者制御が可能である。また、認証情報発行機をかざした際のカメラ映像を利用することで、公衆無線 LAN 不正利用時に利用者の特定をすることができる。今後、オリンピック会場の入場ゲートなどの人が多く通る場所に認証情報発行機を設置することが想定して多人数での実証実験をしていく必要があると考えられる。

参考文献

[1] 総務省 情報セキュリティ対策室. (2015, Mar.) 公衆無線 LAN 利用に関する情報セキュリティ意識調査結果. [Online]. http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000091.html

[2] 総務省 情報セキュリティ対策室. (2015, Mar.) WI-FI 利用に係る調査結果（詳細版）. [Online]. http://www.soumu.go.jp/main_content/000347144.pdf

[3] 矢野経済研究所. (2014, May) 平成 25 年度国内と諸外国における公衆無線ＬＡＮの提供状況及び国内と諸外国における公衆無線ＬＡＮの提供状況及び訪日外国人旅行者のＩＣＴサービスに関するニーズの調査研究. [Online]. http://www.soumu.go.jp/main_content/000292482.pdf

[4] 総務省・観光庁. (2016, Jan.)「訪日外国人旅行者の国内における受入環境整備に関する現状調査」結果. [Online]. http://www.mlit.go.jp/common/001115689.pdf

[5] Network Working Group, "RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs," 2005.

[6] ISO, "Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)," 2013.

[7] 宮下悠生, "NFC を用いたセキュアな公衆無線 LAN 接続システムの構築," *電子情報通信学会総合大会講演論文集*, vol. 2015, no. 2, p. 162, 2015.