L-005

NFC を利用した公衆無線 LAN 相互認証
A Mutual Authentication Mechanism for Public Wireless LAN Based on Near Field Communication

延 優介† 八槇 博史‡
Yusuke Nobu Hirofumi Yamaki

1. はじめに

2020 年東京オリンピックの開催が決定するなど，外国人観光客の受け入れが目標となる一方で，観光庁の報告[1]によれば，外国人旅行者が滞在中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，それぞれの場所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，単純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 アクセスの利用者と提供者が互いに信頼関係を保った形でのサービスが提供されるのが望ましい．

本研究では，無線 LAN によるインターネットアクセスサービスに関して，利用の開始時点において提供者と利用者の間の電子証明書の交換を NFC[2]によって行う手法を提案し，その実装について述べる．それらの電子証明書を用いて EAP-TLS 認証[3]を行うことで，利用者と提供者の間で相互認証を行い，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．

2. 公衆無線 LAN における利用者登録方式

公衆無線 LAN のサービス形態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．以下では，それぞれの特徴について述べ，そこでの課題について説明する．

2.1 事前登録型

利用者と提供者がサービス利用に先立って登録を行う形態を本研究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，無線接続を行うだけでインターネット利用が可能となり，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もある．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使用された場合，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，外国人旅行者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行う必要があるが，国内利用者の場合と比べて契約に必要な手間が大きくなる問題が指摘されており，また使いたいときに即時利用することができないなどの問題がある．

2.2 オンサイト登録型

利用者が訪問した現地で利用登録を行い，サービス利用を開始する形態を本研究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．外国人旅行者に対する受入環境整備として，観光庁が推進している公衆無線 LAN サービスもこれに相当する．

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が簡単であるものの，悪意あるアクセスポイントに接続してしまうなどのリスクが同時に懸念される．たとえば観光地に上記のようなサービスが展開された場合，悪意ある攻撃者はそのサービスを装って，旅行者から個人情報を窃取しようとするかもしれない．

前節で述べたように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は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者にとっても，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，利便性の観点からは，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．

2.3 安全に信頼構築を可能とする機構の提案

以下では，観光地などの訪問者をサービス利用者，公衆無線 LAN を運営するサービス提供者，信頼できる団体，また攻撃者である偽サービス提供者の四者がいると想定する．ここでいう信頼できる団体とは，公的機関など運営者の信頼性が保障されている団体を指す．

本機構で提案する，安全に信頼構築を可能とする機構の例を図 1 に示す．本機構では，サービス提供者と信頼でき

†慶應義塾大学大学院政策・メディア研究科 Keio University, Graduate School of Media and Governance
‡東京電機大学情報環境学部 Tokyo Denki University, School of Information Environment

る団体は事前に契約を結んでいるとする．サービス利用者は利用したい公衆無線 LAN のアクセスポイントに接続するのだが，攻撃者が設置している偽アクセスポイントに誤って接続してしまう懸念がある．そこで利用者は信頼できる団体を直接訪問し，正しいサービス提供者の情報を得る．その後，サービス利用者はその情報を元に正しいサービスに接続を行う．サービス利用者はサービス提供者の証明書を，サービス提供者はサービス利用者の証明書の正当性を確認後，サービスの提供を開始する．

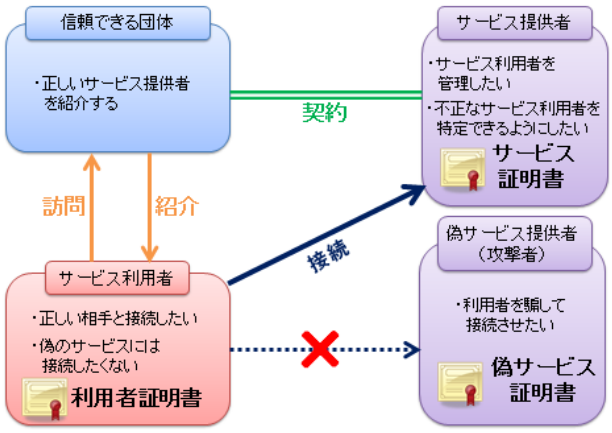

図 1　提案機構

この機構の目的は，サービス利用者が正しいサービスに安全に接続することができる環境整備である．

本機構では，サービス利用者は信頼できる団体に直接正式なサービスの情報を紹介してもらうので，サービス利用者が公衆無線 LAN サービスを利用し始める間に攻撃者が割り込む余地がなく，偽サービスに誤って接続しないメリットがある．一方でサービス利用者は信頼できる団体まで足を運ぶ必要があるが，そこでの手続きを単純なものにし，外国人旅行者にも直感的に理解できるものにすることでその煩わしさを解消する．

このように信頼できる団体を通して公衆無線 LAN サービスに接続する体制が整えば，正規のサービスに偽装した偽サービスに，誤って接続した利用者の個人情報が窃取されるような犯罪を防ぐことが期待される．

3. 公衆無線 LAN における相互認証

3.1 相互認証

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，サービス利用者とサービス提供者は互いに未知であり，お互いが信頼できるような相手であるかを確認する必要がある．サービス利用者は信頼できるサービス提供者にのみ接続し，サービス提供者は不正な利用をされないよう，信頼できる相手にのみ利用させたい．このように，サービスの利用あるいは提供以前にお互いが信頼できる相手であるかどうかを判断しなくてはならない．互いに信頼できる者であると判断することを相互認証という．安全なネットワークアクセスを実現するためには，アクセスポイントとクライアント端末の間での相互認証が必須である．

アクセスポイントとクライアント端末の間で相互認証を行う認証プロトコルとして EAP-TLS 方式があり，本機構でもこれを用いる．

3.1.1 EAP-TLS

EAP-TLS は，IEEE 802.1X[4]において定められた認証方式に対応した認証プロトコルの 1 つである．EAP-TLS では，認証サーバ，無線クライアント，認証局（CA）の三つの間で認証を行う．認証サーバと無線クライアントは認証局が発行したルート証明書の他，認証局が発行したサーバ証明書，クライアント証明書が必要である．

これらの証明書には認証局の電子署名が含まれており，サーバとクライアント間で交換し検証を行うことでお互いの正当性を確認する．これは公開鍵認証方式に基づいており，認証局の秘密鍵で暗号化された電子署名を認証局の公開鍵で複合し，電子署名に間違いがなければ正当性を保証できる仕組みである．

しかし，証明書の発行元が信頼されなければ証明書そのものが信頼できない問題があり，認証局の正当性は社会的信用によって担保されている．また，クライアントの秘密鍵と認証サーバの公開鍵を配置する手順が事前に必要となるが，これが一般には煩雑であり，導入・設定に手間がかかる問題もある．なお，一度導入を行えば次回以降は再度導入・設定の必要がなく，気軽に安全なネットワークアクセスを実現できるメリットもある．

3.1.2 EAP-TLS の認証手順

図 2 に EAP-TLS 方式の認証手順を示す．破線は EAPOL プロトコルでの通信であり，実線は RADIUS プロトコルでの通信である．EAP-TLS 方式を用いた EAP 認証のメッセージ交換は次のようになる．

1. アクセスポイントに接続したサプリカントは，EAPOL 開始フレームを送信する．
2. これを受信したアクセスポイントは EAP Request/ID を送信して，サプリカントのアイデンティティを要求する．
3. サプリカントは EAP Request/ID をアクセスポイントに送信し，アクセスポイントはそれを認証サーバに通知し，アクセス要求を行う．
4. 認証サーバはアクセスチャレンジとして送信し，アクセスポイントはそれをサプリカントに送信し，TLS 通信の開始を要求する．
5. サプリカントは TLS 通信を開始し，TLS バージョン，セッション ID などの通知を行う Client_hello メッセージを認証サーバに送信する．
6. 認証サーバは選択した TLS バージョンやセッション ID などの情報とサーバ証明書をサプリカントに送信する．
7. サプリカントは認証サーバにクライアント証明書の送付を行う．
8. 新たにネゴシエートされた暗号仕様を使用することを，サプリカントに通知する．
9. 鍵交換と認証処理が成功したことの通知を行い，実際の通信を開始する．

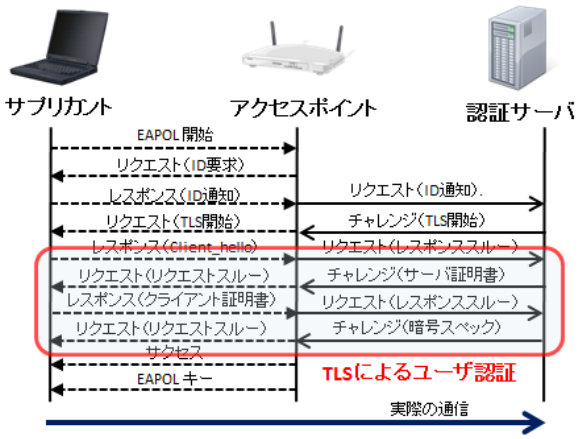

図 2　EAP-TLS 方式の認証手順

3.2　NFC を利用した公衆無線 LAN 相互認証

本研究では EAP-TLS 方式を用いて，アクセスポイントとクライアント端末の間での相互認証を行い，安全なネットワークアクセスを実現する．しかし先述した通り，EAP-TLS 通信を行うためにはクライアントの秘密鍵と認証サーバの公開鍵を配置する手順が事前に必要となり，この手順が一般には煩雑とされ，公衆無線 LAN で EAP-TLS 方式が用いられない大きな壁となっている．そこで，単純で分かりやすい方法でクライアント秘密鍵と認証サーバの公開鍵を端末に設定する方式を本機構において提案する．

3.2.1　NFC

NFC はデータ通信の国際標準規格 ISO/IEC 18092 であり，対応機器同士を 10cm 程度の近距離でかざすだけでデータ通信が可能である．NFC を使えばテキストだけでなく，画像等の様々なデータをかざすだけでやり取りすることができる．図 3 に NFC タグの例を示す．NFC リーダをこれらのタグにかざすことで，タグ内部に記録されたデータを読み出すことができる．

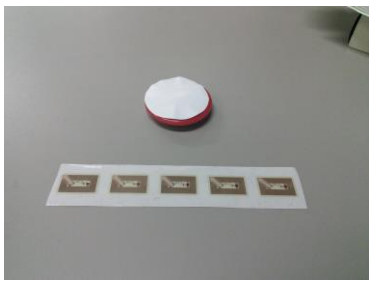

図 3　NFC タグ

本研究では，NFC を用いることで，かざすだけで通信を行うことができ，直感的で明示的な通信の確立が可能である．外国人旅行者や通信機器に詳しくない人でも，NFC を利用すれば煩雑な手続きを踏むことなく，得たい情報に簡単にアクセスし，それを手に入れることができる．また，NFC の通信距離は 10cm 程度に限定されているため，悪意のある攻撃者が間に割り込む余地を無くすことができ，通信の傍受や中間者攻撃等を防ぐことができる．

3.2.2　NFC タグの設置場所

NFC タグの設置場所として，安全が保障されたセキュアな場所に設置する必要がある．

攻撃者はいかなる手法を用いて，利用者を騙そうと試みる．例えば誰もが訪れることが可能で，監視の目が届かない場所に NFC タグを設置すると，攻撃者は誤った情報を与える偽 NFC タグをすりかえて設置し，悪意のある情報を流布することも懸念される．そこで NFC タグを設置する場として，市役所や駅の観光案内所などある程度の監視の目が行き届く場所に限定して設置する必要がある．また，これらの場所は外国人観光客にも直感的に安全な場であることが理解できると思われ，煩わしさを与えない．

3.2.3　提案機構の利用開始処理の流れ

本研究の提案機構の利用開始処理の流れを図 4 に示す．EAP-TLS 通信を行うため，クライアントの秘密鍵と認証サーバの公開鍵を端末に設定する必要がある．サービス利用者はサービス利用申込みの際に，これらの証明書データをまとめた相互認証用証明書データを端末にダウンロードし，インポートを行う．この過程は以下に示すとおりである．

1. 公衆無線 LAN を利用したいサービス利用者は，サービス提供者と契約を結んでいる観光案内所等の安全が保障されている場所を訪れ，接続したい端末を設置してある NFC タグにタッチする．
2. NFC タグから端末に，サービス利用申込みサイトの URL が送られる．
3. 送られてきた URL に，3G 回線など無線 LAN 以外の通信方式による https でのアクセスをし，サービス利用申込みを行う．
4. サービス提供者はデータベースサーバに，サービス利用者が利用申込みサイトを通じて送信したユーザ情報の登録を行う．
5. サービス利用者は利用申込みサイトから相互認証用の証明書データをダウンロードし，端末で証明書の設定を行う．
6. 端末とアクセスポイントの間で 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. お互いの検証が完了し，正当性が確認できたら実際の通信を開始する．

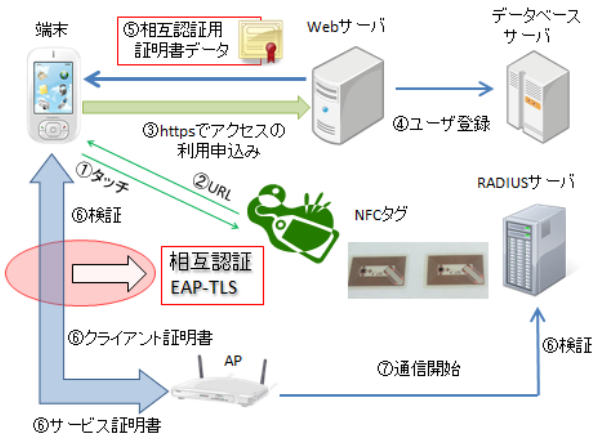

図 4　提案機構における利用開始処理の流れ

3.3 サービス利用申込みとユーザ登録

公衆無線 LAN サービス提供者は，提供するサービスを悪意のある者によって犯罪行為などに利用された場合に備えて，サービス利用者をある程度追跡できる体制を整えておく必要がある．本機構ではサービス利用申込みの際に，メールアドレスの入力と利用規約の同意を義務付けている．現在日本で展開されている公衆無線 LAN サービスのほとんどが，同じ利用申込み形態を採用している．

利用申込みが完了した後，相互認証用証明書データのダウンロードが可能となる．なお，本機構で EAP-TLS 通信に用いる相互認証用証明書データとは，表 1 で示す通り，ライアント秘密鍵，クライアント証明書および認証局（CA）証明書を指す．

表 1　EAP-TLS 通信に用いる相互認証用証明書データ

データ名	用途
クライアント秘密鍵	通信内容の秘匿
クライアント証明書	自己証明
認証局（CA）証明書	証明書の検証

サービス利用者は，画面の指示に従ってこれらのデータを端末にインポートする．この後は，接続したいアクセスポイントを選択し，目的のサービスに接続するだけで自動的に認証が行われる．また次回以降の接続時は，NFC タグにタッチしたり，利用申込みサイトにアクセスしユーザ登録を行ったりする必要は一切なく，相互認証によって正しい公衆無線 LAN サービスであることを保証されながら，直接接続することが可能となる．

4. 実装

4.1 実装の概要

本研究では提案機構の Web サーバ，データベースサーバ，RADIUS サーバの実装，また証明書発行のためプライベート CA，および NFC タグの実装を行った．Web サーバは公衆無線 LAN サービスの利用申込みサイトとダウンロードページの作成，データベースサーバはユーザ登録された利用者情報の蓄積，RADIUS サーバは EAP-TLS 認証の設定，プライベート CA は相互認証用証明書データの発行をそれぞれ行う．

以下に示す実装では，Dell PowerEdge R200 上に行った．

4.2 Web サーバ

Web サーバの構築にあたり，Apache/2.2.15 を利用した．HTML と PHP を用い，Web インタフェースを作成する．具体的には，公衆無線 LAN サービスの利用申込みページ，ダウンロードページの作成を行った．実際に作成した利用申込みページのスクリーンショットを図 5 に示す．

図 5　利用申込みページ

公衆無線 LAN サービスを利用したいサービス利用者は，サービス提供者と契約を結んでいる観光案内所等の安全が保障された場所に出向き，接続したい端末を NFC タグにタッチすることにより，端末に利用申込みページの URL が送られてくる．サービス利用者はこの利用申込みページにアクセスし，ユーザ登録を行う．本機構では，サービス利用者は個人情報としてメールアドレスを入力する必要がある．また，利用規約に同意する必要があり，メールアドレスの入力と利用規約の同意をもってユーザ登録の完了となる．

次に，相互認証用証明書データのダウンロードページのスクリーンショットを図 6 に示す．

図 6　ダウンロードページ

図 5 の利用申込みページにて，メールアドレスの入力と利用規約の同意を行い，ユーザ情報の送信を行うことで図 6 のダウンロードページに移動する．ここではクライアント秘密鍵，クライアント証明書，認証局（CA）証明書から成る相互認証用証明書データのダウンロードを行う．ここでダウンロードした相互認証用証明書データを適切に端末にインポートすることにより，アクセスポイント間での EAP-TLS 通信を可能とする．

また，利用申込みページから送られてきたメールアドレスは，PHP スクリプトによってデータベースサーバに送信される．データベースサーバについては 4.3 項にて説明を行う．

4.3 データベースサーバ

データベースサーバの構築にあたり，MySQL/14.14 を利用した．利用申込みサイトで入力された情報が PHP スクリプトによって，データベース内に蓄積される．

データベースサーバには，発行番号としての識別 ID とメールアドレスが対応される形で蓄積される．本機構を悪意のある者によって犯罪行為などに利用された場合に備え，蓄積されたメールアドレスよりサービス利用者を追跡できる体制をとっている．

4.4 RADIUS サーバ

RADIUS サーバの構築にあたり，FreeRADIUS/2.1.12 を利用した．EAP-TLS 通信に対応させるため，設定ファイルの編集を行った．

4.5 プライベート認証局と証明書

証明書を発行するためのプライベート認証局の構築にあたり，OpenSSL 1.0.1e-fips を利用した．

まず初めに，プライベート認証局の CA 証明書と鍵の作成を行う．証明書データには国名，都道府県名，市町村名，会社名やメールアドレスといった情報を組み込むことができる．

次にサーバ証明書の作成を行い，認証局の署名を入れる．また，クライアント証明書と鍵の作成も行い，同じく認証局の署名を入れる．作成したクライアント秘密鍵，クライアント証明書，CA 証明書をまとめて PKCS#12 方式に変換する．PKCS#12 方式は複数の証明書を格納することができるフォーマットであり，多くの Android 端末に対応している．また，まとめることでダウンロードの手間を 1 回に抑えるメリットもある．

今回作成した相互認証用証明書データは，サイズが 3.53KB となった．

4.6 NFC タグ

本機構で用いるタグとして，NFC タグに公衆無線 LAN サービスの利用申込みサイトの URL を書き込んだ．公衆無線 LAN サービスの利用者は，サービス提供者と契約を結んでいる観光案内所等の安全が保障された場所を訪れ，接続したい端末を本 NFC タグにタッチすることにより，公衆無線 LAN サービスの利用申込みサイトに自動的にアクセスすることができる．

4.7 提案機構のデータの流れ

実装した本機構のデータの流れを図 7 に示す．クライアントとなる端末は，NFC と EAP-TLS 通信に対応している必要がある．

以下に本機構のデータの流れを説明する．NFC により利用申込みページの URL が与えられると，端末はまず 3G 回線など無線 LAN 以外の通信方式により Web サーバにアクセスする．この際 https 通信を利用し，Web サーバと Web ブラウザの間の通信の暗号化を行い，通信経路上での盗聴や第三者によるなりすましを防止する．申し込みのための Web アプリケーションは PHP により記述されており，登録結果はデータベースに蓄積される．端末には相互認証用証明書データとして，クライアント秘密鍵，クライアント証明書および認証局（CA）証明書が送られる．サービス利用者は，画面の指示に従ってこれらの鍵を端末にインポートする．この後は目的のサービスに接続するだけで，自動的に認証が行われる．

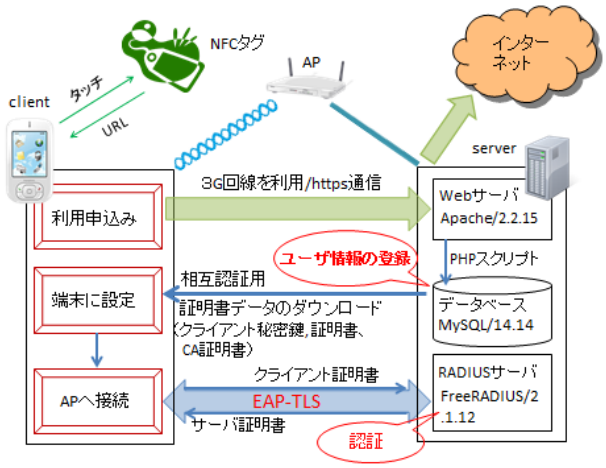

図 7　提案機構のデータの流れ

5. 運用試験と考察

5.1 運用試験

運用試験は，NFC と EAP-TLS 通信に対応しているクライアント端末 2 つで行う．使用した端末の仕様を以下の表 2 に示す．

表 2　実行端末の仕様

	GoogleNexus 7	Google Galaxy Nexus
OS	Android4.4.2	Android4.3
CPU	Qualcomm Snapdragon S4 Pro, 1.5GHz	Texas Instruments OMAP4460 1.2GHz
メモリ	2GB	1GB
ストレージ	16GB	16GB

本研究における運用試験は，公衆無線 LAN サービスに接続したい端末を NFC タグにタッチし，利用申込みを経て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．

5.2 試験結果と考察

5.2.1 試験結果の評価

特に大きな負荷がかかる処理もなく，実用的なレスポンスで動作することがわかった．今回の運用試験は 2 種類の端末を用いて行ったが，端末の性能差はほとんど影響を与えないことが分かった．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，その後のサービスへの接続時に再び設定を行う必要がなく，必要となる労力は最初に信頼できる場所を訪れる 1 回のみであるといえる．複雑な操作

を必要とせずに，正式なサービス提供者に安全に接続することを可能とし，外国人旅行者や通信機器に詳しくない人にも気軽に利用されることが期待できる．

5.2.2 本機構の実用性について

本機構は相互認証用証明書データを簡単な操作で端末にダウンロードすることを可能にしているが，その一方，鍵の端末への配置や接続すべき ESSID の選択などは利用者のマニュアル操作に委ねられている． このため，証明書の配置の仕方，EAP-TLS 通信の開始の手順がまだ難しいと感じる利用者も少なくないと予想される．よって，ユーザビリティのさらなる改善を図る必要がある．具体的には証明書自動設定アプリの開発や，OS の機能拡張を行うなどの対策が必要になると考える．

サービス利用者は証明書自動設定アプリをあらかじめ端末にインストールしておくことにより，サービス利用申込みサイトからダウンロードした相互認証用証明書データが自動的に端末に設定され，接続すべき ESSID の選択まで自動的に行い，マニュアルでの設定が一切不要で実際の通信を行うことができる．

また，本機構では公衆無線 LAN サービスの利用申込みサイトへのアクセスを，携帯事業者の 3G 回線を利用し，アクセスを行っている．しかし，日本で通信を行うために国際ローミングを用いることを嫌う外国人旅行者の存在が懸念される．よって，外国人旅行者には更なる考慮が必要であると考える．

本機構の前提となっている，NFC と EAP-TLS 通信が利用可能なクライアント端末は近年増加しているが，販売されている全ての端末にこれらの機能が内蔵されているわけではなく，これらの機能を有した端末の普及も本機構稼働の課題となる．

6. おわりに

本研究では，公衆無線 LAN サービスに安全かつ簡単に接続する方式が求められているその解決案として，NFC を利用した公衆無線 LAN 相互認証機構の開発を行い，運用試験を行った．運用試験では，実用的なレスポンスで動作することが分かった．

安全なネットワークアクセスを実現するためには，アクセスポイントとクライアント端末の間での相互認証が必須である．そのため本機構では，EAP-TLS 方式を用い相互認証を行うことにした．EAP-TLS 方式を用いるにはクライアントの秘密鍵と認証サーバの公開鍵を端末に設定する手順が必要であり，一般にはこれが煩雑であるとされ，導入に時間がかかる問題がある．そこで，単純で分かりやすい方法でクライアント秘密鍵と認証サーバの公開鍵を端末に設置する方法が必要であり，NFC を用いることにした．NFC を選んだ理由として，かざすだけで通信が開始され，直感的で明示的な通信の確立を行うことが可能である点が挙げられる．

提案機構では，観光地に訪れた観光客が現地の公衆無線 LAN サービスに，安全かつ簡単に接続することを目的としている．サービス利用者は，観光案内所等の安全が保障されたサービス提供者と契約を結んでいる場所を訪れ，接続したい端末を NFC タグにタッチする．その後，NFC タグからサービス利用申込みページの URL が送られ，3G 回線など無線 LAN 以外の通信方式による https でのアクセスをし，サービス利用申込みを行う．サービス提供者はデータベースサーバに，サービス利用者が利用申込みサイトを通じて送信したユーザ情報の蓄積を行う．サービス利用者は利用申込みサイトから相互認証用の証明書データをダウンロードし，適切に端末にインポートし証明書の設定を行う．その後 EAP-TLS 通信を開始し，お互いの証明書の検証を行い，正当性が確認されれば実際の通信を開始する．

実装は Web サーバ，データベースサーバ，RADIUS サーバからなる相互認証システムの構築を行った．また，証明書発行のためのプライベート CA，および NFC タグの実装を行った．運用試験では比較的負荷のかかる処理も少なく，実用的な時間での運用が可能であることが分かった．しかし証明書の設定等，依然としてユーザにとってハードルの高い箇所も残されている．

NFC が至近距離との通信のみを行うという性質を用い，機器間の安全なペアリングを簡易に行うという方式は，Bluetooth 機器においては以前より手案されており[5]，標準化も進んでいる．本研究では，同様の仕組みを街中などオープンな環境でのサービス利用者と提供者の間のトラストの確立に応用している．NFC を用いたペアリングには，端末外部からの通信に応じてアプリケーションを立ち上げることによるセキュリティリスクが指摘されている[6]が，このような問題についても今後対処していく必要がある．

今後の課題として，証明書自動設定アプリの開発や，OS の機能拡張を行うなどの対策を行い，ユーザビリティの改善を図る．また，NFC を用いた多要素認証技術や，Bluetooth 通信による多様な通信の実現などを通じて，安全かつ簡単に接続することができる公衆無線 LAN サービス機構を目指す．

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] “IEEE Std. 802.1X-2004 IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control. Technical report”, Institute of Electrical and Electronic Engineers, Inc., 2004.

[5] C. Y. Leong, Ong, K. C., K. K. Tan and O. P. Gan, “Near field communication and bluetooth bridge system for mobile commerce. In International Conference on Industrial Informatics”, pp. 50-55, 2006.

[6] R. Verdult and F. Kooman, “Practical Attacks on NFC Enabled Cell Phones,” 2011 3rd International Workshop on Near Field Communication (NFC), pp.77-82, 2011

[7] “IEEE Std. 802.11i-2004 IEEE Standard for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. Technical report”, Institute of Electronic Engineers, Inc., 2004.

[8] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, “Extensible Authentication Protocol (EAP)”, RFC3748, June 2004.

[9] T. Dierks and C. Allen., “The TLS Protocol Version 1.0”, RFC2246, January 1999.

[10] A. DeKok, FreeRADIUS, http://freeradius.org/, 2008.