ソーシャルネットワークを用いた Wi-Fi ユーザー認証の提案・構築

小林 茉莉子[1]　鈴木 茂哉[2]

概要： Wi-Fi は人々の生活に必要不可欠なインフラの一部として整備が進んでいるが，Wi-Fi の認証における利便性は未だ乏しい．Wi-Fi のアクセスポイントを用いる際に，事前に共有鍵を一人一人が機器に入力する方法は，ユーザーにとって負担が大きい．また，アクセスポイントの共有鍵をユーザーに教えることは，ネットワークの管理者にとって，秘密の情報を他人に教えるという観点から不安に感じることが多い点があるだけでなく，運用上不便でもある．

そこで，本提案手法では Wi-Fi ユーザー認証の利便性向上を目的とし，これにより管理者とユーザー双方の問題の解決を計る．SNS の認証とソーシャルグラフを組み合わせた Wi-Fi ユーザー認証の手法を提案する．

A Design and Implementation of A Social Network Based Authentication Mechanism for Wireless LAN

MARIKO KOBAYASHI[1]　SHIGEYA SUZUKI[2]

1. はじめに

近年の Wi-Fi における認証手法は多岐多様に渡っているが，ユーザーにわかりやすく，かつ煩わしさを感じさせない手法は未だ少ない．Wi-Fi は今や万人が使うことができる重要なインフラの一つとなっており，認証における利便性の向上が近年さらに求められている．例えば，2014 年には総務省と観光庁により，無料講習無線 LAN 整備促進協議会が設立され，利用者が容易に利用できることが重要視されている [1].

現在主流の家庭内 Wi-Fi 認証手法では，アクセスポイントの SSID と事前共有鍵を用いる．しかし，事前共有鍵はランダムな数字やアルファベットの集合であることが多く，ユーザーにとって見慣れない文字列であり，入力が煩雑である．そして，複数の友人が家に訪れ，家庭内のアクセスポイントを利用する場合，各々が事前共有鍵を所有する機器に入力する必要があり，この手間は煩雑である．

また，トレンドマイクロによる調査 [2] によると，パスワードを使い回しているユーザーは 9 割以上である．このことからわかるように，ネットワークの管理者は自宅のネットワーク機器のパスワードと，事前共有鍵を似通った文字列にしてしまう傾向が否めない．いずれにせよ，一度事前共有鍵を友人に教えてしまった場合，事前共有鍵を変更するためには，全てのネットワーク機器の設定を変更する必要が生じるので，アクセスポイントの事前共有鍵を他人に教えることに抵抗がある．このように，Wi-Fi の利便性の向上が求められる中で，SNS の認証とソーシャルグラフを組み合わせ，ユーザーを認可し，利便性を向上させる手法を提案する．本提案手法によって，こうした Wi-Fi 認証におけるユーザーと管理者の双方が抱える問題点を解決することが可能である．

実際の問題点を図示したのが図 1 である．

図 1　現状の問題点

[1] 慶應義塾大学　環境情報学部
[2] 慶應義塾大学　政策・メディア研究科

2. 研究目的と提案手法

一つの場に複数の Wi-Fi 利用者が集まる環境下で Wi-Fi の認証を行う際に，煩わしさを最小限にする方法を提案・構築する．具体的なユースケースとして，複数の友人が家庭内のアクセスポイントに接続する際，ユーザー認証における煩雑さを減らす．

本提案手法では、Wi-Fi のアクセスポイントに接続するユーザーに対し，Facebook のソーシャルグラフから得られる友達リストを用いて，アクセスポイントの管理者の友人に対してのみインターネットへの接続を認可できる．

3. 実装

小型の Linux サーバー OpenBlocks IoT にアクセスポイントを構築し，このサーバー下に Captive Portal を実装した．Captive Portal とは，Wi-Fi のユーザー認証時に，特定の Web ページ (認証画面・同意画面) に強制的にリダイレクトさせる技術である．

3.1 実装・環境

表 1　実装に使用した環境・ツール

	用いた技術等	バージョン
実装環境	OpenBlocks IoT BX1	Kernel 3.10.17-13 対応 Ver.1.0.6
OS	汎用の Debian GNU/Linux	7.8
Captive Portal の OSS	Coova Chilli	1.2.9
認証サーバー	FreeRADIUS	3.0.11
認証ページフレームワーク	Ruby on Rails	4.2.5
PaaS	Heroku	
ライブラリ	Devise	3.5.3
	omniauth	1.2.2
	koala	2.2.0

Captive Portal を利用し，アクセスポイントに接続したユーザーを認証ページに誘導する．そして，ユーザーが認証ページを経由して Facebook アカウントでログインした後，Facebook のソーシャルグラフの API である，Graph API を用いてユーザーの友達リストを取得し，そのユーザーが管理者と友人か否かを調べる．友人であればインターネットへの接続を認可し，友人でない場合は認証ページへのリダイレクトを繰り返し，インターネットへの接続を認可しない．

3.2 アクセスポイントと Captive Portal の構築

Open Blocks IoT 上において，無線インターフェース wlan0 をアクセスポイントとして動作するよう設定し，インターフェース eth0 に上流ネットワークを有線で接続した．そして，このアクセスポイントにユーザーが接続し，認証・認可が成功した際に，上流のネットワークへ接続する構成とした．今回は上流ネットワークとして研究室内のネットワークへ接続する．Captive Portal の実装には，オープンソースソフトウェアである，Coova Chilli を用いた．

3.3 認証ページの構築

認証ページは Ruby on Rails と Ruby を用いて作成した．なお，今回扱う SNS として Facebook に絞った理由は、Graph API の豊富なパラメーターの存在がある．Graph API には友人関係の情報だけでなく，ユーザーの所属するコミュニティや動向やステータスを表すパラメーターがあるため，多様な認証・認可システムの構築が可能である．Facebook アカウントによるソーシャルログイン実装部分に関しては，ライブラリである Devise と omniauth-facebook を用いた．また，認可時に Graph API を扱うためのライブラリである koala を用いた．

ユーザー認証の際に，ユーザーが自身の Facebook の友達リストに，ネットワーク管理者の識別 ID を保持している場合，Pass(認可成功) のページに飛ぶ．なお，認可されず，認証画面で Fail 画面 (認可失敗) へリダイレクトされた場合は，Coova Chilli 側に認証を通ったことは知らされないため，アクセスの許可は与えられず，その後も Wi-Fi を使うことはできず，認可されるまで認証ページにリダイレクトされ続ける．なお，この認証ページの公開には、PaaS である Heroku を用いた．

認証ページの動作を図 2 に，実際の認証画面を図 3 に示す．

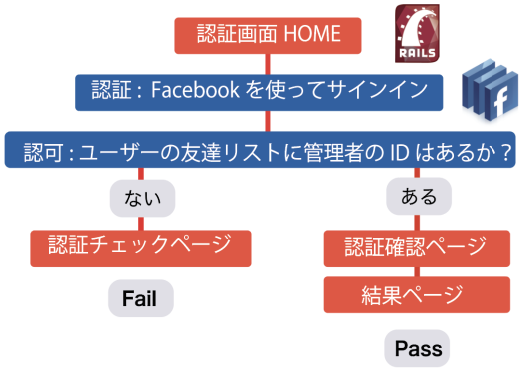

図 2　認証ページの動作

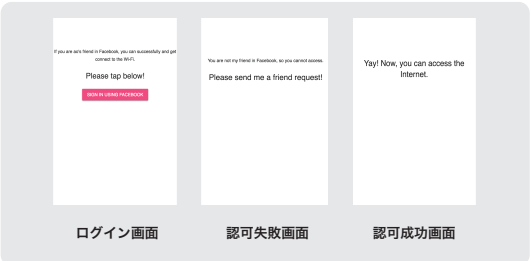

図 3　実際の認証画面

3.4 Captive Portal と認証ページ間のやりとり

各ユーザーが認証ページ管理者の識別 ID を Facebook の友達リストに保持している場合，認可成功画面にリダイレクトされる．この画面が読み込まれた際に，Coova Chilli の ChilliController が呼び出され，Captive Portal の IP アドレス 10.1.0.1，ポート番号 3990 に向けユーザーのログオン情報を渡す．RADIUS サーバーでは認可対象のユーザー設定を実験のため，All-Accept の状態にしたため，成功画面にユーザーがたどり着いた際，適当な ID とパスワードをブラウザを通して Coova Chilli 側へ送る．

このように，Heroku 上のアプリケーションでの認証の可否を，Open Blocks IoT BX1 で稼働している Coova Chilli へ送ることで，Coova Chilli がユーザーのアクセスを許可し，その後ユーザーは Wi-Fi を使うことが可能となる．なお，認可が失敗し，認証失敗画面へリダイレクトされた場合は，Coova Chilli 側にユーザーが認証を通ったことは知らされないため，アクセスの許可は与えられず，その後も Wi-Fi を使うことはできない．そして，認可されるまで認証ページにリダイレクトされ続ける．

Captive Portal の動作を図 4 に示す．

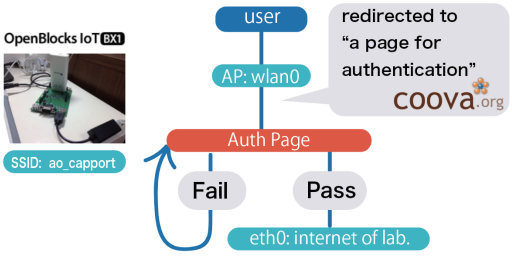

図 4　Captive Portal 動作の流れ

4. 関連研究・事例

本項では，ソーシャルネットワークを用いた Wi-Fi ユーザー認証を扱っている先行研究やサービスについて示す．

4.1 FOAF を用いた Wi-Fi ユーザー認証

Ynus Durns，Koen Langedong らは，Web ID を用いた Wi-Fi 認証の事例の提案・構築を行った [3]．Web ID とは URI を用いて，各ユーザーの名前や所属等が記載されたプロフィールページであり，ソーシャルネットワーキングを目的としている．2000 年に Dan Brickley や Tim Berners-Lee らによって作られた [4].

本手法では Web ID の組み込まれ FOAF(friend of a friend) という友人情報をもとに，direct trust，indirect trust，same-owner の 3 種類のステータスの場合，Wi-Fi 接続を認可する．direct trust は直接友人である場合を示し，indirect trust は間接的に友人である場合を示す．same-owner は機器がいくつかあり，それらのオーナーが同一である場合を示す．

この研究の問題点としては，ユーザー間のソーシャルネットワークを探索するアルゴリズムが非効率的で，Web ID の情報を取得するプロセスに時間がかかる点にある．結果として認証・認可における時間がかかってしまうため，ユーザーの感じる利便性の点から好ましくない．また，Web ID は HTTPS が必須ではないので，中間者攻撃に対して脆弱である．そして，Web ID は SNS として提唱されたものの，結果的として流行せずユーザー数は増えなかったため，FOAF を用いた Wi-Fi 認証手法は一般性に欠ける．

4.2 Wi-Fi コミュニティ FON

FON[5] は世界 150 ヶ国で展開されている，会員内で Wi-Fi のアクセスポイントを共有するサービスである．現在世界で約 1900 万箇所のアクセスポイントの共有が FON では可能となっている．FON は会員登録料金は必要ないが，対応ルーターの購入やプロバイダー契約は自己負担となる．Wi-Fi 接続における認証方式としては，FON 対応のアプリケーションをダウンロードし，FON の SSID を探し，FON アカウントのユーザー名とパスワードを入力することで，インターネット接続が可能となる．

FON のアクセスポイントからは 2 種類の SSID がブロードキャストされており，片方は FON 会員向けのネットワーク，片方はアクセスポイントの管理者の自宅向けのプライベートなネットワークであり，後者はパスワードで保護されている．しかし，このようにネットワークのセグメントを分けた場合においても，第三者がオープンなネットワーク経由でプライベートなネットワークへ侵入することが可能であることも報告されている．また，FON のユーザーが悪質な手口で，アクセスポイントの管理者になりすまし，不正アクセスを行う可能性も否定はできないという点もあり，セキュリティに関して課題が未だ残されている．

4.3 Facebook Wi-Fi

Facebook Wi-Fi[6] とは，Facebook が提供する Wi-Fi のユーザー認証サービスである．ユーザーが飲食店や小売店で，利用者が自身の位置情報を共有することによって，各店舗にて無料で Wi-Fi 接続を利用できるサービスである．店舗側で Facebook Wi-Fi を導入するためには，対応のルーターが必要であり，店舗の Facebook Page を作成・登録し，設定をした後，ユーザーに Facebook Wi-Fi としてサービスの提供が可能となる．

ユーザーが Facebook アカウントを用いて，サービスにログインすることで Wi-Fi を利用できる容易さは利点であるが，ユーザーが自身の位置情報を好まない場合を考慮する必要はある．また，店舗としては対応のルーターを設置する必要があり，導入にコストがかかるという欠点もある．

4.4 eduroam

eduroam[7] は欧州の GËANT Association (旧 TERENA) にて開発された，教育機関間での無線 LAN ローミング基盤である．当該組織の参加機関を訪れ，他大学内の Wi-Fi のアカウントを持っていない場合において，自分の大学の ID とパスワードを使うことでローミングが可能となり，無線 LAN 環境を利用できる．そして，ユーザーは eduroam 参加機関で日本では eduroam JP としてサービスを利用することが可能である．

まず, 該当機関が認証サーバーや認証局を用意し, eduroam のユーザーに利用を許可することで，ユーザーは eduroam 参加機関で利用できる．ユーザー認証方式に関しては，IEEE802.1x を採用しており，WPA2/AES といった通信を暗号化する技術を用いることで，セキュリティの向上に努めている．また，ユーザーはの利用を用意し，機関しかし一方で，このようにユーザーや教育機関側にて行う手順が多いため，運用・管理面のコストは高いと言える．

4.5 Social WiFi

Zhen Cao，Panagiotis Papadimitriou，Jürgen Fitschen らは，異なるソーシャルネットワークサービス (以下 SNS) 間におけるソーシャルネットワークを用いて，Wi-Fi ホットスポットをオンライン上の友人と共有する，Wi-Fi ユーザー認証手法を提案・構築した [8].

論文内には「High penetration of online social networks(以下 OSNs)」という概念があり，これはあらゆるソーシャルネットワークサービス上のソーシャルネットワークを集約したソーシャルネットワークを指す．OSNs の API では，Facebook や Linkedln，Google+といった異なる SNS における，友人関係の情報を一括で管理している．つまりユーザーは，異なる SNS 上で関係をもつ人物と Wi-Fi ホットスポットを共有することが可能である．また，Social Wi-Fi における認証のプロセスにかかる時間は，EAP-TTLS を比べ，27ms 短縮することができたという．

5. 評価

評価は下記の 2 点の観点に分けた．

- 評価 1 : 既存の家庭内 Wi-Fi 認証手法との比較
- 評価 2 : 公共向け Wi-Fi 認証手法との比較

5.1 既存の家庭内 Wi-Fi 認証手法との比較

既存の家庭内 Wi-Fi 認証手法との比較を下記に示す．

表 2 に挙げた手法のうち，AOSS[9] と QR コード [10] の手法はユーザーにとって煩雑な手順が含まれる．iPhone で AOSS の認証を利用する場合，事前に Safari ブラウザに専用のプロファイルをインストールする必要があり，このプロファイルがない場合，警告が出てプロファイルのインストール画面へと促される．また，QR コード認証においては，専用のアプリケーションのダウンロードが必要である，という点に関してユーザーの負担を増やしている．SSID と PSK(事前共有鍵) の方式は本研究手法とステップ数が同値で，利便性における大差がないように感じられるが，SSID/PSK は初期設定の場合ランダムな英数で生成される場合が多く，手元のキーボードから打ち込む際も煩雑である．一方，本研究手法は Facebook でログインし認証を行うため，入力する ID やパスワードに本人のものを用いるため，煩雑さが少ない．よって、既存の家庭内 Wi-Fi の認証手法に比べ，少ない手順でインターネットへアクセスすることが可能なため，Wi-Fi 認証における使いやすさの向上を実現できる．

表 2 i Phone の HOME 画面からアクセス完了までに要するステップ数

家庭内 Wi-Fi 認証手法	ステップ数
AOSS	7 ステップ
QR コード	6 ステップ
SSID/PSK	5 ステップ
本研究手法	5 ステップ

5.2 公共向け Wi-Fi 認証手法との比較

各先行研究・事例との比較を下記の表 3 に示した．表 3 はユーザーの利便性観点からの比較と，運用・管理の観点からの比較の 2 つに分かれている．

表 3 公共向け Wi-Fi 認証手法との比較

	認証に必要なもの	アプローチ	一般性
FON	アプリ・ID・パスワード	FON 会員限定	×
eduroam	証明書	教育機関限定	×
Social Wi-Fi	ONS アカウント	ソーシャルグラフ	△
Facebook Wi-Fi	Facebook アカウント	位置情報共有	○
FOAF Wi-Fi	Web ID アカウント	ソーシャルグラフ	×
本研究手法	Facebook アカウント	ソーシャルグラフ	○

表 3 に挙げた手法はいずれも，公共向けの Wi-Fi 認証可手法である．

まず，FON や eduroam はサービスを利用できるユーザーの範囲に制約があり，対象のユーザーが限られてしまうため，一般性に欠ける．また，本研究手法と Facebook Wi-Fi との差別化に関しては，Facebook Wi-Fi は特定の場所で情報をシェアすることでインターネットに接続できるが，本研究手法はソーシャルグラフを用いるという観点にある．そして，一見酷似しているように見える手法である Social Wi-Fi に関しては，Facebook，Linkedln，Google+における友人関係のみの API を用いる．一方で，本研究手法は，現段階では友人関係のみであるが，実装において，柔軟に認可の条件を書き換えることが可能である．よって，友人関係のみでなく，ユーザーの所属や参加するイベント等に

よって，多様なソーシャルネットワークを認可に組み込める可能性を秘めている．

また，運用・管理のコストの面からも比較する．eduroamは事前の団体登録が必要かつ認証サーバーや認証局を運用・管理する必要があり，運用者にとって負担になる．FONやFacebook Wi-Fi，及び本認証方式は専用のルーターを設置する必要がある．

このように，公共性のあるWi-Fi認証の事例と比べ，本研究手法はユーザーにとって馴染み深いFacebookアカウントを認証に用いるため，一般性があり，かつ運用・管理コストが低く，また認可の条件を柔軟に変更することが可能である．

6. 今後の展望

本研究手法においては，Facebookにおける友人関係にあるユーザーを許可の基準としたが，Facebook Graph APIには，その他使用可能なパラメーターが多くある．例えば，中小規模の勉強会やイベントを行う際，Wi-Fiのユーザー認証に「eventパラメーター」を用いることで，特定のイベント参加者を対象とした認証が可能となる．また，同じ誕生日月の仲間で集まる際は，「birthdayパラメーター」を用いることで，認可の対象を，特定の月に生まれたユーザーに絞ることが可能である．

よって，本研究手法を応用することで，その日の条件や客層に合致する認可条件へ毎回カスタマイズすることが可能である．本研究手法はこうした認証・認可の条件において柔軟性がある点に，将来性があるといえる．

また，本研究手法はユーザーの友人関係のみでなく，様々なユーザー情報を認可に扱うことが可能である反面，ユーザーのプライバシーをいかに守り，ユーザーに納得して使ってもらうのか，今後考えていくことが課題となる．

参考文献

[1] 訪日外国人旅行者向けの無料公衆無線LAN環境の周知・広報の強化に取り組みます-共通シンボルマーク（Japan. Free Wi-Fi）を決定-
http://www.mlit.go.jp/kankocho/news03_000118.html（参照 2016-05-06）.

[2] -パスワードの利用実態調査 2014-
約7割が自分のパスワード管理にセキュリティ上リスクがあると認識
4割以上がパスワードを手帳やノートにメモして管理
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20140609010140.html
（参照 2016-05-08）.

[3] Durms, Y., Langendoen, K. Durm WiFiAuthentication through Social Networks ー a Decentralized and Context-Aware Approach ー (2014)
doi: 10.1109/Per-ComW.2014.6815263
http://www.es.ewi.tudelft.nl/papers/2014-Durmus-SocialAP.pdf（参照 2016-05-04）.

[4] Web ID
https://www.w3.org/wiki/WebID（参照 2016-05-11）.

[5] FON
http://fon.ne.jp/（参照 2016-05-01）.

[6] Facebook Wi-Fi
https://www.facebook.com/business/facebook-wifi（参照 2016-04-27）.

[7] eduroam
http://www.eduroam.jp/docs/eduroam-JP-flyer.pdf（参照 2016-05-03）.

[8] Cao, Z., Fitschen, J., Papadimitriou, P Social Wi-Fi: Hotspot sharing with online friends(2015)
https://www.ikt.uni-hannover.de/fileadmin/institut/Publikationen/pimrc_2015.pdf（参照 2016-05-02）.

[9] AOSS
http://buffalo.jp/aoss/（参照 2016-05-04）.

[10] Aterm らくらく QR スタート
https://121ware.com/product/atermstation/special/rakuraku_qr/（参照 2016-05-04）.