無線 LAN ホットスポット向け簡易個人認証システム

上原哲太郎[†*] 齋藤彰一[†] 満田成紀[†] 泉裕[†††*] 妻木祐介[‡] 西山秦史[‡*] 國枝義敏[†]
†：和歌山大学システム工学部 ††：和歌山大学システム情報学センター
‡：(有)サイプレス *：NPO 法人情報セキュリティ研究所

内容梗概

無償サービスとしての無線 LAN ホットスポットを運営するには，ユーザ登録制度をどうするかが問題となる．ユーザ認証を全く行わない状態では匿名ネットワーキングの入り口としてクラッカーの格好の標的になりかねないが，事前登録制にすると煩わしさにユーザが逃げかねない．そこで本研究では，電子メールと WWW ブラウズ機能を有した携帯電話を用いて，簡単にユーザ認証ができ，かつホットスポットの管理負担も軽減するシステムを提案する．システムの開発に当たっては，プリペイド式携帯など使用者個人が同定しにくい携帯電話の排除に留意した．

A simple user-authentication system for wireless LAN hotspot systems

Tetsutaro Uehara[†*] Shoichi Saito[†] Naruki Mitsuda[†] Yutaka Izumi[†††*]
Yusuke Tsumaki[‡] Yasufumi Nishiyama[‡*] Yoshitoshi Kunieda[†]

[†]Faculty of Systems Engineering, Wakayama University [††]Center for Information Science, Wakayama University
[‡]Cypress Ltd . [*]Research Institute of Information Security

Abstract

When offering wireless LAN hotspots for free of charge, the user-authentication system may often become the important issue. Without any user-authentication mechanism, the hotspot could be a fat target as the entrance of anonymous internetworking for crackers, but if we force the users to be registered in advance it is too cumbersome and causes the decrease of them. In this paper we propose a simple user-authentication system using mobile phones with e-mail and browsing services to make the authentication easy for the users and also to reduce the administration cost of the hotspot.

１．はじめに

近年，無線LAN技術は，ユビキタスコンピューティングに対する要求や，有線LANの新規敷設が難しいオフィス･家庭での代替策として急速に普及してきた．とりわけ，IEEE802.11b や 802.11a をはじめとする無線 Ethernet 技術は，価格の低下に伴って急速に普及率を高めている．特に無線 LAN に対するニーズが高いノートパソコンや PDA において，IEEE802.11b が広く使われるようになった．この動きに伴って，公共の場所で IEEE802.11b や 802.11a のアクセスポイントを有償または無償で提供する「ホットスポットサービス」が盛んになってきた．有償のサービスは，主にプロバイダなどが現在までの ISP 事業の延長として提供しており，アカウンティング機構を通してユーザを特定できるサービスとなっている例がほとんどである．

これに対し無償サービスは，喫茶店などの店舗やホテルロビーなどで顧客へのサービスとして行われる例が多い．このような無償サービスでは，ユーザ認証が行われず，事実上の匿名インターネットアクセスを提供するサービスとなっている場合がある．これはユーザの最大限の利便の確保と，サービス提供側の負荷軽減が目的と思われるが，インターネットに対する不正アクセスの土台などに使われると犯人特定の妨げになる危険性があり，インターネット全体にとってセキュリティ上好ましくない．しかし，利用前にユーザに窓口などでの登録やアカウント発行のような手続きを強いると，ユーザに敬遠され利用が減少し，ホットスポット設置の本来の目的を果たせなくなる恐れがある．

そこで本研究では，このようなサービスを無償サービスとして提供する場合に利用できる，ユーザに負担の少ない簡易個人認証システムを開発，実装した．開発にあたっては，(1)簡易な手続きで認証ができ，ユーザに過度の負担とならないこと，(2)無料サービス提供側の負担を最小限にとどめること，の 2 点を主な目標とした．この目標の中で，悪意あ

表1　携帯電話・PHS 各社の電子メール・WWW サービス

キャリア	サービス名	メールアドレス	WWW ブラウザ対応言語
NTT ドコモ	i モード	*@docomo.ne.jp	C-HTML
KDDI 等 TU-KA	EZweb	*@*.ezweb.ne.jp, *@*.ido.ne.jp	HDML, XHTML Basic
J フォン	J-SKY	*@jp-?.ne.jp (?は地域による 1 文字)	MML
DDI ポケット	H''LINK	*@*.pdx.ne.jp	P-mailDX 形式, HTML (一部のタグのみ)
NTT ドコモ (PHS)	パルディオ Eメール	*@*.nttpnet.ne.jp	C-HTML (ブラウザホンのみ対応)
アステル	MOZIO 又は ドットi	*@phone.ne.jp, *@*.mozio.ne.jp	C-HTML 拡張

るユーザによる匿名利用を可能な限り抑止するようなシステムを開発した.

2. 携帯メールについて

本システムの基本的なアイデアは, 携帯電話や PHS の電子メール (以下, 総称して携帯メールと呼ぶ) のアドレスを利用して個人の同定を行うというものである. そこでまず, 現在国内で利用可能な携帯メールと, それぞれの端末サポートされている WWW ブラウズ機能についてまとめると表1のようになる.

日本国内では現在, NTT ドコモグループ各社[1], KDDI/沖縄セルラー各社[2], J-Phone[3], ツーカーグループ各社[4]の4グループによる携帯電話サービスと, DDI ポケット[5], NTT ドコモグループ各社, アステルグループ各社[6]の 3 グループによる PHS サービスが受けられる. これら全てのサービスにおいて, 端末固有のメールアドレスによるインターネットメールの送受信サービスが提供されている. よって, 少なくともメールアドレスから端末の同定ができ, 端末の所有者を同定できる.

表2　プリペイド式携帯電話・PHS 各社の電子メールサービス

キャリア	サービス名	メールアドレス
NTT ドコモ	ぷりコール	利用不可
KDDI 等	ぷりペイド	利用不可
TU-KA	プリティ, プリケー	*@sky.tu-ka.ne.jp, *@sky.tkc.ne.jp, *@sky.tkk.ne.jp
J フォン	プリカ, Pj	*@jp-?.ne.jp (?は地域による)
アステル東京	プチペイド	*@phone.ne.jp, *@*.mozio.ne.jp
アステル関西	プリペイド A	利用不可

注: 各社ともプリペイド式では WWW ブラウズはできない

ここで問題になるのは, 端末の同定が端末の所有者の同定にならない場合があることである. 具体的には, プリペイドカードを用いた携帯電話等が問題となる. これらは現在購入時に身分証明書の提示を受けることになっているが, 携帯電話各社がその制度を導入したのが 2000 年 7 月であり[7], それ以前に販売されたものについては確認ができない. また, 転売等で所有者が追跡できなくない場合もある. このようなプリペイド式携帯サービスの一覧を表2に示す. この中で特に問題となるのは, メールアドレスが見かけ上通常契約の携帯電話と変わらない J-Phone グループと, アステル東京のサービスである.

しかしこれらのいずれのサービスにおいても, プリペイド式携帯端末においては WWW サービスが利用できない. そこで本システムではこれを利用し, 携帯電話に送った電子メールにある URL を埋め込んでアクセスさせることで個人認証を行うことにした. よって, 電子メールと WWW サービスの両方が利用可能な携帯電話を持つユーザのみを対象として個人認証の対象とする.

3. システムの構成

本研究で提案するシステムの構成を図3に示す. 各ユーザは無線 LAN 端末となるノートパソコンや

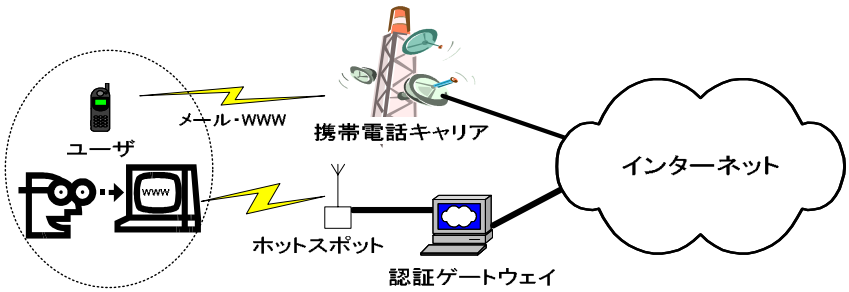

図３　システム全体の動作イメージ

PDA などと共に，WWW サービスへのアクセスが可能な携帯電話または PHS を持っている．無線 LAN ホットスポットとインターネットの間には，認証ゲートウェイがある．このゲートウェイは，ホットスポット側の LAN とインターネット側で IP のポートフィルタリングなどの機能を持ち，またホットスポット側，インターネット側双方に対して WWW サーバとして動作する．また，ホットスポット側 LAN を単一のネットワークで構成するなどして，ホットスポット側で動作している各端末の MAC アドレスを把握させる．

システムの利用イメージの概要は以下のようになる（図4）．

① ユーザが無線 LAN 端末をホットスポットに持ち込むと，アクセスポイントの間でリンクが確立し，DHCP によって端末に適切なアドレスが割り当てられ，ルーティングも行われる．そこでユーザが任意の WWW ページを参照する．

② ゲートウェイはその端末の IP アドレスが未認証であることを検知して IP パケットを横取りし，自身が WWW サーバとして動作して認証用画面を端末に強制的に表示する．

③ ユーザは認証用画面に現れたフォームに自分が持つ携帯電話のメールアドレスを入力し，ゲートウェイに送る．

④ ゲートウェイは受け取ったメールアドレスが携帯電話向けメールアドレスであるかどうか確認した後，その端末が利用中の IP アドレス，MAC アドレス，ランダムに発生した文字列（パスワード），その有効期限を組にしてデータベースに登録し，そのパスワードを埋め込んだ URL を含むメールをそのメールアドレスに送信する．

⑤ ユーザは自分の携帯電話に送られてきたメールに含まれる URL に，その携帯電話からアクセスする．その URL はゲートウェイのインターネット側アドレスを指しており，CGI を通してメールに含まれるパスワードをゲートウェイに返信する．ゲートウェイでは受け取ったパスワードをデータベースから探して，対応する端末 IP アドレスやパスワードの有効期限などを探し出す．

⑥ パスワードが有効期限切れでないことを確認して，ゲートウェイにおいて当該 IP アドレスを認証済みとマークし，その IP アドレスを含むパケットを，IP アドレスの有効期限が来るまでゲートウェイを通過できるように設定する．

⑦ 有効期限が来ればその端末 IP アドレスを未認証状態に戻す．ただし期限になる前に⑤が再び実行されれば，IP アドレスの有効期限を延長する．

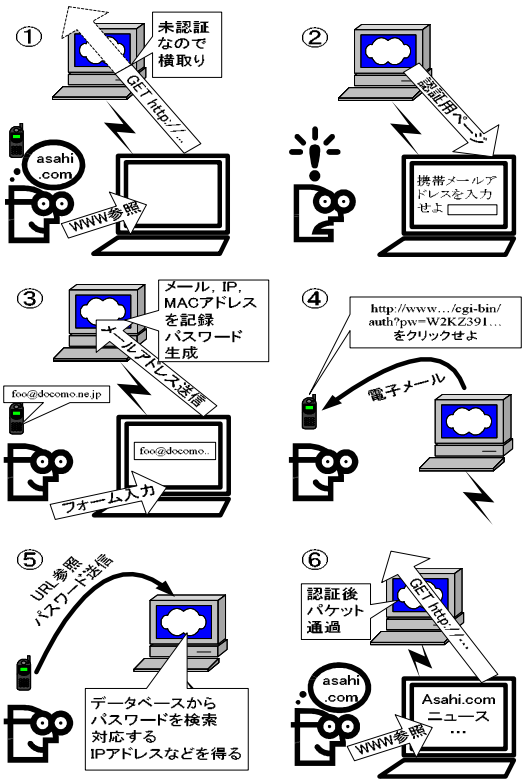

図４　システム利用イメージ概要

この手順を踏むことで，手順③の時点での端末 IP アドレスの利用者が，そこで入力されたメールアドレスを持つ携帯電話等の所有者であることが同

定できる．よって，何らかのセキュリティインシデントが発生した際には，このメールアドレスを手がかりに利用者の特定が可能である．

４． ユーザ同定の精度の向上

この手法は簡易な方法であり，ユーザ同定の保証できない場合がいくつか存在する．我々が想定しているセキュリティホールと対応策を以下に述べる．

● パスワードが漏洩する危険性

パスワードとなるランダム文字列を携帯電話に送る際，携帯電話のメールの仕様上平文で送るしかないため，ゲートウェイから携帯電話キャリアのメールサーバまでの間に盗聴可能な部分があれば漏洩する危険性がないとはいえない．しかし実際には，ゲートウェイと上流 ISP との間のネットワークを盗聴しにくい構成にすれば実害はほとんどないと考えられる．また，このパスワードは全て手順④の時点でその都度生成されて使い捨てられるので，安全性は高い．さらに手順⑦において延長する際も最大延長回数などを定めておくことにより，パスワード漏洩における被害を小さくすることができる．

● 送信したメールアドレスが プリペイド式携帯電話である危険性

前述のとおり，J-Phone の携帯電話メールアドレスに送付した場合，アドレスだけでは受取人がプリペイド式携帯かそうでないか区別がつかない．プリペイド式携帯の場合，メールで送付した URL にその携帯からアクセスはできないが，ほかの携帯電話やパソコン，PDA などに URL を転記してアクセスすることによって認証を通過してしまう可能性がある．

この問題への対処としては，ユーザ認証のために送付したメールアドレスが J-Phone であった場合には，パスワードを返送するために行われたブラウザでのアクセスの際の IP アドレス（の FQDN）が J-Phone ドメインである場合にのみ認証を通過させるようにすればよい．J-Phone ドメインが発信元であるようなアクセスは，J-Phone の端末の WWW ブラウズ機能または J-Phone 自身が提供するインターネットプロバイダサービスでアクセスした場合にのみであると考えられる上，後者はプリペイド式携帯電話からは利用できないので，これにより少なくともプリペイド式でない携帯電話からのアクセスであることが保証でき，個人同定の手がかりになる．

なおアステルグループの PHS に関しては，電話機による WWW ブラウズの際も ISP を選択できるなどの理由により，プリペイド式でない場合も IP アドレスのドメイン名が固定しない．そのため，今回のシステムではアステルグループのメールアドレスを個人同定に使うことを断念し，除外した．

● IP アドレスを横取りされる危険性

今回のシステムではホットスポットを利用する端末が使用の終了を宣言する機構を設けていないため，IP アドレスの利用期限が残っている間なら，あるユーザがホットスポットから去った隙を狙い，同じ IP アドレスを使用してホットスポットを認証なしに利用することができる．これを防ぐため，一定時間トラフィックがない IP アドレスについては使用期限が残っていても未認証状態に戻す処理を加える． また，各 IP アドレスと MAC アドレスの対応を調べ，対応が変化した場合は即座に当該 IP アドレスを未認証状態に戻す処理を加える．しかし MAC アドレスの改変が可能な NIC を用いた攻撃にはこれだけでは対処できないため，パスワードが漏れていなくともその時点の有効期限が切れるまでは他人に使用される可能性がある．これを防ぐためには，ユーザから明示的にホットスポットの使用終了を宣言させる機構を設けるべきである．

● 携帯電話そのものの盗難などの危険性

このシステムでは携帯電話固有の情報であるはずのメールアドレスを個人同定の根拠としているため，盗難や貸借などによってその電話の所有者が利用していない場合までは想定していない．

５． 実装について

本研究で提案したシステムを実装し，和歌山市ぶらくり丁商店街のホットスポットで運用実験を行っている．その実装の概略をここで述べる．同商店街では現在，アーケードに沿って既に無線 LAN アクセスポイントが設置され，それらは有線で商店街事務局内に引き込まれ，ADSL 経由で対外接続されている．今回 ADSL ルータと無線 LAN の間に設置したゲートウェイは CPU: Pentium-III 500MHz, Memory: 128MB, HDD: 10GB の PC で，これに FreeBSD 4.6R を導入し，ソフトウェアとして Apache2, ISC-dhcp などを導入した．データベースはそれほど大規模なものではないので今回は DBMS を導入せず，OS 標準の dbm ライブラリだけで実現している．

無線 LAN は 192.168/16 のプライベートアドレスで運用しており，WEP 暗号化などは施していない．ゲートウェイは無線 LAN 側には DHCP サーバ，WWW サーバ，DNS サーバおよび NAPT サーバとして動作している．インターネット側のインターフェースでは認証用に WWW サーバとして，また認証用メールの送出のために sendmail と，各種ログのタイムスタンプを正確にするため NTP クライアントが動作しているが，ほかの各種 TCP ポートは閉じられており，NAPT とあわせてファイアウォールとして機能している．

本システムで最も重要な，各 IP パケットの認証に

基づく通過･拒否の制御には，FreeBSD の ipfw 機能および ipforward 機能を利用した．システム自体は，ユーザ認証画面で用いるメール送信のためと，携帯電話から送られてきたパスワードの確認のための 2 つの CGI プログラム，さらに毎分ごとに cron で起動される IP アドレスなどの有効期限チェックのためのスクリプトから構成される．

システムの動作の概要は以下の通りである．ホットスポット内に端末を持ち込むと，ゲートウェイから DHCP で IP アドレス等が設定され，端末は一見すぐに利用可能な状態になる．しかし初期状態では，無線 LAN 側からの全てのパケットは ipforward を用いてゲートウェイの localhost に転送される．これにより，端末からの任意の WWW アクセスはゲートウェイの WWW サーバに転送され，強制的にユーザ認証用ページが表示される（図5）．

認証ページでのメールアドレスの入力によって起動された CGI では，その CGI を起動した IP アドレス，MAC アドレス，ランダムに生成したパスワード，パスワードの有効期限(30 分後)をデータベースに記録し，図5にあるようなメールを携帯電話等に送信する．

ユーザがメール内の URL をクリックすると，ゲートウェイの WWW サーバを経由して別の CGI スクリプトにパスワードが伝えられる．CGI ではパスワードが有効であるかどうかチェックして，有効であればデータベースに IP アドレスの有効期限として 1 時間後の時刻を設定し，ipfw 機能を用いてその IP アドレスのゲートウェイの通過を許可する．以降，ユーザがメール中の URL をクリックするたびに，最初の認証時から 24 時間までの間，IP アドレスの有効期限を延長し続けることができる．

パスワード，IP アドレスの有効期限のチェックやトラフィック状態の監視のためには別のスクリプトが cron によって 1 分ごとに起動されている．このスクリプト内では，有効期限の切れたエントリ，長時間トラフィックのない IP アドレス，IP アドレスと MAC アドレスの対応が登録時と現状で異なるものなどに対し，データベースからのエントリ削除や当該 IP アドレスの利用不可の設定などを行う．

ユーザ認証用ページ

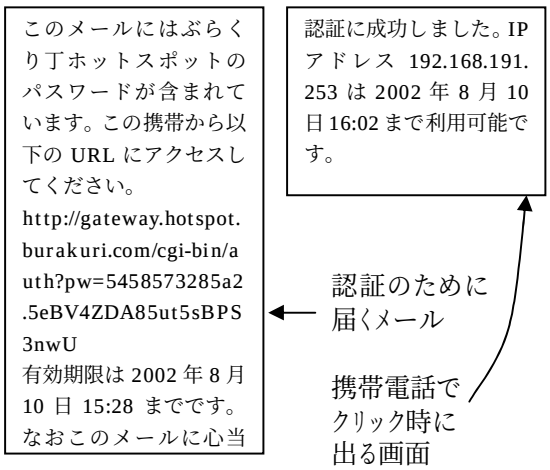

図５　システムの実行例

６．評価と考察

今回実装したシステムの利点は以下のようにまとめられる．

- ユーザにとっては，認証用に必要なのは通常利用している携帯電話のみであり，無線 LAN 端末には特殊なソフトウェアの導入や機器の接続は一切必要ない．
- ユーザは認証や登録作業がほとんどオンラインで可能であり，例えば商店街事務所などに出向いて登録を行うなどの煩わしい手続きが不要である．
- システム管理者側にとってもユーザ認証手続きが完全に自動になっているためインシデントが発生しない限りメンテナンスフリーであり，管理負担が軽減できる．

逆に今回実装したシステムは以下の点が不利であると考えられる．

- 結果として携帯電話のメールアドレスを収集するシステムであるため，ユーザの利用に一定の抵抗感があると考えられる．メールアドレスの転用はしないなど個人情報の扱いに関するユーザへの説明が十分でないと誤解を招きかねない．
- 認証はユーザが全てWWWページを利用するという前提で設計されているため，例えばメールだけを利用したいユーザなどにとっては認証のためにわざわざWWWブラウザを起動せねばならず，煩わしさは残る．

- インシデント発生時に，個人を同定し追跡するために利用できる情報はメールアドレス，端末の MAC アドレス，認証時の携帯電話からのアクセス時の IP アドレスと相手側 TCP ポート番号のみであり，個人を直接特定できるわけではない．これらの情報から個人を特定するには携帯電話キャリアの協力が不可欠であるが，簡単には情報が提供されない可能性がある．
- 既に述べたとおり MAC アドレスの詐称をされると認証されてないユーザでもホットスポットを利用可能な場合があるなど，簡易さを求めたためセキュリティ上は万全とはいえない．

しかし全体として，ユーザにとっても管理者にとっても負担を軽く保ったまま，適度な精度での個人認証が実現できたと考えられる．

なお，本システムはぶらくり丁商店街で実際に運用中である．本稿執筆時点では運用を開始して 1 週間程度であり，認知度が低いためまだ利用は数名と少ないが，現時点でログの解析から判明した問題を以下にまとめる．

- 認証前のユーザが，期待していない WWW ページ（つまり認証ページ）がいきなり表示された時点で，それをよく読まずに reload を繰り返したり，すぐにあきらめる等の行動がしばしば見られる．また携帯電話以外のアドレスを入力するなど，認証ページの記述だけでは認証システムの意図がよく伝わっていないと考えられるため，文章やデザインの工夫が必要と考えられる．
- POP3 のみのユーザがおり，しかも WWW にアクセスしないため認証システムに気づかない例が見られる．認証システムの十分な広報が必要であると考えられる．
- システム自体は商店街の客をターゲットに設計されているが，実際の利用には商店主なども多い．このような固定的なユーザのために携帯電話以外の一般的な認証方法も併用できるシステムにするべきである．

7． 終わりに

本研究では，無償で提供される無線 LAN ホットスポット向けに，携帯電話を用いた簡易個人認証システムを構築した．ユーザにとっても管理者にとっても負担の軽いシステムが実現できたと考えられる．現在は運用を開始したところだが，今後は長期間の運用を通して問題点を洗い出し，システムの改善につなげたい．

今後の課題としては以下のようなものが挙げられる．

- 本システムでもっとも問題になっている MAC アドレスの詐称を含む IP アドレスの横取り問題に対処する方法の開発．特にユーザに使用終了を明示的に宣言させる方法が有望と思われるが，ユーザに能動的に終了処理を行ってもらう手段を提供するか，文献[9]にあるような Java などのプログラムを WWW 経由で送り込んで終了を検知させる方法を検討している．
- POP3 のみのユーザなど，WWW を利用しないユーザのための適切な認証ページへの誘導方法の開発．POP に関しては，認証ページに誘導するようなダミーのメールを常に送付するサーバをゲートウェイに置くことを検討したが，ユーザの ID とパスワードを収集するプログラムとして働きかねずセキュリティ上問題が大きいので採用しなかった．より適切な手法の開発が課題である．

謝辞

運用実験にご協力いただいている㈱ぶらくりの方々に感謝いたします．

参考文献

[1] NTT Docomo Net: http://www.nttdocomo.co.jp/
[2] au ホームページ: http://www.au.kddi.com/
[3] J-フォン株式会社: http://www.j-phone.com/
[4] TU-KA: http://www.tu-ka.co.jp/
[5] DDI ポケット: http://www.ddipocket.co.jp/
[6] ASTEL GROUP: http://www.astel.ne.jp/
[7] “プリペイド式携帯電話ご利用の際のご本人確認手続きの実施について”NTT ドコモ報道資料, 2000.7.10
[8] P. Srisuresh and M. Holdrege, “IP Network Address Translator (NAT) Terminology and Considerations”, RFC 2663 (1999).
[9] 渡辺義明，渡辺健次，江藤博文，只木進一:“利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発”，情報処理学会論文誌,Vol.42，No.12，pp.2802-2809, 2001.