ユーザ認証機構を有する安全な無線LAN ・情報コンセント統合システムの構築

後藤英昭, 安西従道, 二階堂秀夫, 千田栄幸, 満保雅浩, 静谷啓樹
東北大学情報シナジーセンター情報教育研究部, 〒980–8576 仙台市青葉区川内
{hgot,anzai,nikaido,chida,mambo,shizuya}@icl.isc.tohoku.ac.jp

1 まえがき

近年の無線 LAN 機器の普及にともない，大学のキャンパスなどに無線 LAN アクセスポイントを設置する事例が増えている．このように公共の場に設置する無線 LAN では，情報コンセント (イーサネットジャック) と同様に，学内 LAN やそれに接続された計算機を守るためにユーザ認証とアクセス制御を行う必要がある [1, 2, 3] . 無線 LAN には，端末とアクセスポイントの相互の位置がわかりにくい，盗聴されやすい，端末のネットワーク切断を検出しにくいなどの性質がある．従来の情報コンセント用のアクセス制御方法は，無線 LAN に適用できなかったり，セキュリティ上の問題があった．無線 LAN に適した方法の開発が必要である．

無線 LAN や情報コンセントは初心者でも苦労せずに使える必要があり，多様な種類の端末が接続できる必要がある．特に教育機関では，管理者が計算機やネットワークにそれほど詳しくない場合が多いので，実装も非常に容易でなければならない．高価なスイッチが必要な方法 [1, 2] は予算面の制約により導入が非常に難しいことが多く，小規模なサイトでは特にこの傾向は強い．

本研究では，廉価な機器を使うことを前提として，ネットワークの高い安全性を確保しながら，導入の手間を著しく簡略化できるような方法の実現を目指した．本報告では，まず，情報コンセントについて従来検討されてきた様々な不正アクセスの問題に加えて，偽ポート/偽認証サーバの問題などを紹介する．続いて，本学情報シナジーセンター情報教育研究部で構築した，無線 LAN・情報コンセント統合システムを紹介する．

2 公共の無線LAN・情報コンセントの問題点

2.1 ユーザ認証・アクセス制御の必要性

無線 LAN アクセスポイントを学内 LAN に直結していると，SSID (Service Set Identification) と WEP (Wired Equivalent Privacy) の暗号化鍵さえ合わせれば誰でも自分の端末を学内 LAN に接続できる．キャンパス内で多数の学生に無線 LAN を利用させる場合，SSID などは公開する必要があるので，SSID と WEP はセキュリティ対策としては役に立たない．イーサネットの場合も，ハブやスイッチが学内 LAN に直結されていると，誰でも学内 LAN に接続することができる．利用者の故意あるいは不注意によって，学内 LAN やそれに接続された計算機に攻撃がなされる危険性がある．

また，学校の備品の端末でさえも，学内外のウェブ掲示板への荒し行為や，電子メールの悪用，電子ジャーナルなどの利用規定に反する利用なども起こることが知られている．このような行為を抑制することはもちろん，実行された場合は，利用者を特定して適切な指導を行うことが求められている．

無線 LAN アクセスポイントやスイッチの製品の中には，MAC アドレスを利用したセキュリティ機能を有するものがある．しかし，MAC アドレスによる認証では，数千 ~ 数万人規模での MAC アドレスの登録が困難である上に，盗難ハードウェアの使用によるなりすましなどに対処できない．

公共の場で利用される無線 LAN・情報コンセントでは，正規の利用者かどうかを調べる「ユーザ認証」と，正規の利用者に対してのみ学内 LAN への接続を許可する「アクセス制御」の機能が必要である．利用者認証では，どの利用者がいつ端末を接続したのかを記録する必要があり，できれば場所も把握できることが望ましい．なぜなら，ある利用者番号を使っている者が本人ではない可能性もあり，現場での本人確認が必要となる場合もあるからである．

学内 LAN の安全性を確保するためには，以下のすべての条件が満たされる必要がある．

1. 正規の利用者以外の者は，無線 LAN・情報コンセントから学内 LAN にアクセスできない．
2. 正規の利用者であっても，ユーザ認証に必要な他人の情報を知らなければ，身元を隠したり他人になりすまして学内 LAN にアクセスでき

ない．

3. 正規の利用手続きにおいて，ユーザ認証に必要な情報がシステムを介して他人に盗まれることがない．

特に 3. に関して，利用者のパスワードなどの重要な情報が容易に盗み出せるようなシステムではいけない．

2.2 解決すべき問題点

2.2.1 ネットワーク切断の検出

無線 LAN や情報コンセントでは，利用者が正規の手続きによるログアウトなどを行わずにネットワークが物理的に切断されることがしばしば起こる．正規の利用者に対して開かれた接続チャネルが他人に利用されたりしないように，ネットワークが切断されたらすみやかに，当該チャネルを閉じる必要がある．

廉価なスイッチや無線 LAN アクセスポイントは，リンクダウンをハードウェア的に検出して制御用の計算機に伝えるような機能はもっていない．TCP socket のタイムアウトを利用する方法もあるが [2]，数秒の精度で確実にネットワーク切断を検出することが困難である．

2.2.2 カスケードハブ問題と盗聴

イーサネットでは，ケーブルを延長したりポート数を増やすために，ハブをカスケード接続することが一般的に行われている．教室などの情報コンセントでも，ハブが安易に接続されることは避けられない．スイッチのリンクダウン検出機能を利用する方法では，ハブがカスケード接続されると，ネットワーク切断の検出ができなくなるという問題がある [1]．

また，同じハブにつながれた端末から，ユーザ認証のデータなどを盗聴できるようになる．無線 LAN は盗聴されやすいと言われている．認証情報を暗号化するなどして，ネットワークが盗聴されても認証情報が保護されるようにしておく必要がある．

2.2.3 偽ポート/偽認証サーバ問題

ユーザ認証を行うサーバを認証サーバと呼ぶ．無線 LAN・情報コンセントでは次のような攻撃が可能である．

1. 認証サーバと同じ IP アドレスを付けた端末を接続し，他の端末に対して，あたかも認証サーバであるかのように見せる．
2. 正規の情報コンセントのスイッチのそばや，今まで情報コンセントが無かった所に偽物のスイッチ (または接続口) を設置することで，それに接続された偽の認証サーバに，正規の利用者の端末を接続させる．無線 LAN の場合は，偽のアクセスポイントを設置する．

telnet のように安全ではない認証機能を用いている場合，偽の認証サーバで正規の利用者から利用者番号とパスワードを聞き出すのは容易である．これを偽ポート/偽認証サーバ問題と呼ぶ．

注意すべきは，システムの改良によって 1. の対策は可能なのに対して，2. の対策は直接的には不可能だということである．telnet や Web ベースの認証方式を採用する限り，偽ポート/偽認証サーバ問題は解決できない．認証サーバからみて利用者を認証するという従来のセキュリティ対策に加えて，利用者が認証サーバ側を認証できるような仕組みが必要である．

3 無線LAN・情報コンセント統合システム

3.1 システムの構成

前章に挙げた様々な問題を解決できるような新しいユーザ認証・アクセス制御方法を開発した．この方法に基づくシステムを，SecAP-i (Secure Access Ports with Inexpensive Switches) と呼ぶ．評価用のシステムを本学情報シナジーセンター情報教育棟に設置して，2001 年 3 月から試験運用を行っている．

システムの構成を図 1 に示した．無線 LAN・情報コンセントとスイッチを一つのサブネットに収容し，ネットワークインタフェースを複数有する計算機をゲートウェイとして，このサブネットと学内 LAN を接続する．この計算機はユーザ認証機能も備えるので，以下では認証サーバと呼ぶ．評価用システムでは，Pentium Pro 200MHz を搭載し，2 個のネットワークインタフェース (100Base-TX) を有するパーソナルコンピュータ (PC) を用いた．OS には，導入や管理の容易さや，導入コスト，標準添付のソフトウェア (DHCP, Firewall) などを考慮して，Vine Linux 2.1CR [1] (RedHat Linux 6.2 ベース) を用い

[1] http://vinelinux.org/

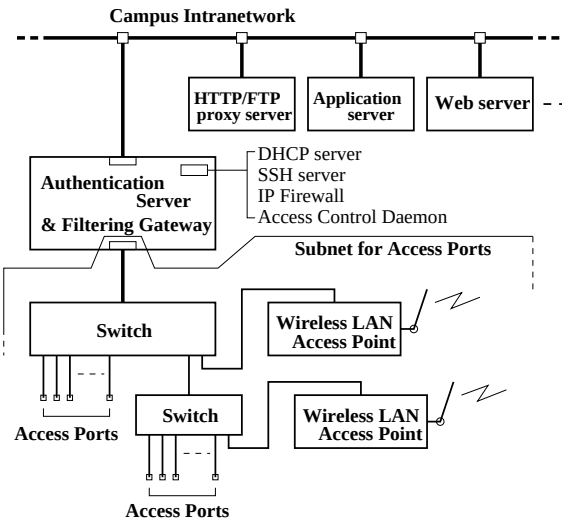

図 1: ユーザ認証・アクセス制御システム — SecAP-i

た．端末への IP アドレスの割り当てには，付属の DHCP サーバを用いた．

スイッチには特にモード切替え機能も持たないような廉価なものを用いた（corega FSW-8L など）．本方法ではスイッチがカスケード接続されていても問題はない．また，本システムでは IEEE 802.11b に対応した 2 台の無線 LAN アクセスポイント（Allied Telesis WR211AP）を接続している．情報コンセントと無線 LAN を合わせて，同時接続可能な端末数は 18 台に設定して運用している．

本システムでは廉価なスイッチを用いているので，文献 [1] の方法と違って，利用者が使用しているポートは特定できない．また，不正利用者は，端末をネットワークに接続しただけで，情報コンセントが収容されているサブネットに対しては様々な攻撃を仕掛けることが可能である．不正利用があった場合に不正利用者の位置を絞り込むことができるように，同じテーブルや部屋といった，非常に狭い範囲で小さなサブネットを割り当てるようにすることが望ましい．無線 LAN アクセスポイントには，到達範囲の狭い小電力のものを用いる．小さなサブネットを利用することにより，不正利用者は自分の近傍の利用者に対してしか攻撃ができなくなるので，不正利用を心理的に抑制する効果が期待できる．

ユーザ認証は，利用者が認証サーバにログインすることで行われる．本システムでは telnet の使用を禁止し，代わりに Secure Shell [4] を使うことによって，認証情報の盗聴の問題を解決している．Ylönen によって開発された Secure Shell（SSH）は，暗号化による安全なリモートログインなどの手段を提供し，インターネット上の暗号通信手法の事実上の標準となっている．

Secure Shell の採用により，偽ポート/偽認証サーバ問題も自然に解決されている．Secure Shell では，ユーザ認証に先立って，RSA 公開鍵暗号方式などによるホスト認証が行われる．Secure Shell サーバは自分の公開鍵を利用者に公開し，秘密鍵を秘密に保持する．利用者が認証サーバの公開鍵をもっていれば，もし偽の認証サーバに接続した場合は警告が発せられ，ユーザ認証が行われない．真の認証サーバの秘密鍵を入手できない限り，偽の認証サーバは本物になりすますことができない．

Secure Shell の実装の一つである OpenSSH[2] にタイムアウト機能を付けることによって，ネットワーク切断の問題を解決した．利用者が認証サーバにログインすると，Secure Shell クライアントは heartbeat（または keepalive null packet）を定期的に Secure Shell サーバに送る．Secure Shell サーバは，heartbeat が一定時間以上届かなくなった時点でネットワークが切断されたとみなし，利用者のログインシェルを強制的に終了させる．この方法は，セッションの乗っ取りに対しても安全である．

heartbeat の送出間隔と Secure Shell サーバのタイムアウト時間は，通常の利用においてタイムアウトを起こさないように決める必要がある．現システムでは，それぞれ 5 秒と 20 秒に設定している．

OpenSSH にタイムアウト機能を追加するためのパッチは，既にフリーソフトウェアとして公開済みである[3]．管理者はパッチ付きの OpenSSH をコンパイルするだけで，容易に導入が可能である．

この方法では，heartbeat を送出する機能を持った，やや特殊な Secure Shell クライアントが必要になる．しかし，他の目的のために同様の機能が追加されたクライアントがあり，MS-Windows 用，Java 用，UNIX 用などが既に幾つか出回っている．本システムでは MS-Windows や MacOS，UNIX などの様々な環境の端末が利用でき，無線 LAN・情報コンセント専用のプログラムは不要である．

また，本システムでは，認証サーバ上に Web サーバを立ち上げ，Java 用 Secure Shell クライアント[4] の署名付きアプレットを提供している．利用者は Web ブラウザを利用して Secure Shell クライアントを起動し，認証サーバにログインできる．この場合，端末側には Secure Shell クライアントすら導入

[2] http://www.openssh.com/
[3] http://www.icl.isc.tohoku.ac.jp/~hgot/
[4] MindTerm, http://www.appgate.com/

する必要がない．ただし，署名の妥当性の確認が難しいので，偽の認証サーバで偽のアプレットによって認証情報を盗まれる危険性があり，運用には注意が必要である．

3.2 アクセス制御の動作

Linux kernel 2.2 以降に組み込まれているパケットフィルタを利用して，IP パケット中継の制御を行う．フィルタのルールは ipchains コマンドで容易に，かつ動的に変更が可能である．次のようなポリシーを適用して，初期状態ではどの端末に対してもパケット転送を禁止するように設定しておく．

```
ipchains -P forward DENY
```

利用者のログイン状態に応じて，パケットフィルタのルールを変更する．この処理を行うプログラム“アクセス制御デーモン”を認証サーバ上で動かしておく．アクセス制御デーモンは，数秒ごと（我々の実装では 2 秒ごと）に utmp ファイルの内容を調べて，新規にログインした利用者が見つかった場合は，次のようにパケット転送を許可するコマンドを発行する．PC1 は端末のアドレスを表す．

```
ipchains -A forward -j ACCEPT -d PC1
ipchains -A forward -j ACCEPT -s PC1
```

利用者がログアウトした場合は，次のようにパケット転送を禁止する．

```
ipchains -D forward -j ACCEPT -s PC1
ipchains -D forward -j ACCEPT -d PC1
```

アクセス制御デーモンは，C 言語で作成された 200 行程度の非常に小さなプログラムである．

3.3 性能評価

本稿の執筆の時点（2001 年 8 月）まで，評価用システムに特に問題はみつかっていない．今日では低性能といえる計算機を使用しているものの，アクセス制御デーモンやネットワークの負荷に対しては性能的に余裕がある．しかし，登録アカウント数が多い（約 15,000 人分）のでログインに 10 秒前後の時間がかかっており，より高性能な PC の利用が望ましい．

認証サーバの限界を調べるために，同時にログインできるユーザ数の最大数を調べた．使用している Linux kernel 2.2 では，約 110 ユーザがログインしたところでファイルハンドルの不足が発生した．カーネルパラメータの変更でこれ以上のユーザも扱えるものと思われるが，ネットワークの帯域幅を考慮すると，1 台のサーバでは十分な数であると思われる．

上記のように大量のユーザがログインしている状態で，1 台の計算機から認証サーバの情報コンセント側のポートに対して ping flood による攻撃を仕掛けて様子を見た．実験の結果，いずれのセッションの heartbeat も規定時間内に認証サーバに届いており，強制切断は生じなかった．ただしこの実験では，設備と人手の制約により，各端末はほとんどデータ転送を行っていない．

4 むすび

本報告では，ユーザ認証機構を有する無線 LAN・情報コンセント統合システムを紹介した．新しいユーザ認証・アクセス制御方法は，偽ポート/偽認証サーバによる攻撃や盗聴，セッションの乗っ取りにも強く，ネットワーク切断の確実な検出が可能であり，従来の方法と比べて安全性が向上している．廉価な機器を利用できること，実装が非常に容易なこと，端末側に専用クライアントが不要であることなどが，本方法の特長である．大規模なシステムの構成とその評価が今後の課題である．

参考文献

[1] 石橋勇人, 山井成良, 安倍広多, 阪本 晃, 松浦敏雄, “利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式,” 情報処理学会論文誌, vol.42, no.1, pp.79–88, 2001.

[2] R. Beck, “Dealing with Public Ethernet Jacks — Switches, Gateways, and Authentication,” Proceedings of the 13th System Administration Conference (LISA’99), pp.149–154, 1999.

[3] 松澤智史, 山崎 誠, 武田正之, “DHCP 環境におけるネットワーク情報更新手法,” 電子情報通信学会論文誌 (B), vol.J83–B, no.6, pp.800–807, 2000.

[4] T. Ylönen, “SSH — Secure Login Connections over the Internet,” Proceedings of the Sixth USENIX Security Symposium, pp.37–42, 1996.