社会科学系大学における 認証付きアクセスポイントの構築と運用

奈古屋広昭
一橋大学情報処理センター

概要

今日では、社会科学分野での研究・教育においてもコンピュータネットワークへのアクセスが必須となっている。そのため本学のような社会科学系単科大学においても構成員へのキャンパスネットワークおよびインターネットへの自由なアクセスを提供する必要が生じてきてた。
本論文では、キャンパスネットワークへのアクセス提供方法のひとつとして、DHCP クライアントが接続可能な有線および無線のアクセスポイントと SSH による認証ゲートウェイの組み合わせによる、認証付きアクセスポイントの構築および運用をおこなった事例を報告する。

Making and operating of access points with authentication, on a university of the social science fields

Hiroaki Nagoya
Computer Center, Hitotsubashi university

Abstract

Today, it is necessity that network accessibility for everyone, even their fields of research or education are social sciences. Therefore, we must provide access service to campus network and Internet for member of our university, even fields of the university are only social sciences.
In this paper, we will show a case study of access service with authentication to campus network that is combination of wired/wireless access point for DHCP client and authentication gateway by SSH.

1 はじめに

インターネットの普及にともない、ネットワークアクセスの需要はあらゆる分野に広がっており、それは社会科学分野においても例外ではない。そのため本学[1] のような社会科学系の単科大学においても、キャンパスネットワークへのアクセスに対する需要が非常に高まっている。

その中でも近年とくに必要性が高まっているものとして、携帯型のパーソナルコンピュータを自由にキャンパスネットワークへ接続できるようなシステムがあげられる。これは以下のような本学の状況によるところが大きい。

- 大部分の学部生・大学院生に対しては学内での専用のスペースの割り当てがないため、パーソナルコンピュータなどを固定設置することができない構成員が多数存在する。
- 学内に設置されている一般利用可能なネットワーク接続されている共用端末の数が少ない (構成員 30 人あたり 1 台程度)。また利用時間にも制限がある (現在は平日の 9:30 - 20:00 で講義に使われていない時間帯のみ)。
- 講義室・ゼミ室や附属図書館内など、ネットワーク接続された共用端末が設置されていない場所での、ネットワークへのアクセスが研究・教育のために必要となってきている。

そこで本学では 2002 年度より学内に携帯型パーソナルコンピュータのキャンパスネットワー

[1] 一橋大学 (4 学部 6 研究科 1 研究所、学生数 約 6500 人、教職員数 約 500 人)

クへのアクセスポイントを構築・運用することにより

- 実際の需要の数値的な見極め
- 運用ノウハウの蓄積
- 実運用をおこなう上での問題点の洗い出し

といった点を評価する実験をおこなうこととなった。本稿では、この構築・運用実験についての報告をおこなう。

2　構築・運用・実装の方針

構築・運用については次のような方針にしたがった。

- 実験であるため構築と運用の手軽さを重視する。
- 携帯型パーソナルコンピュータのプラットホームへの依存性はなるべく減らす。
- 利用者認証によるアクセス制御をおこなうことにより、部外者の自由な利用を (ある程度) 妨ぐ。

上記の方針に沿って

- イーサネットおよび無線ネットワーク (IEEE 802.11b) での接続性を提供する。
- DHCP により IP アドレスの付与をする。
- ゲートウェイにより外部との通信を制御する形でのアクセス制御をおこなう。
- 情報処理センター発行の既存アカウントを利用した認証をおこなう。

という方針で実装をおこなった。

なお本稿では以下、本実験システム全体を「認証付きアクセスポイント」あるいは「本システム」、イーサネットおよび無線ネットワークの接続点を「アクセスポイント」、利用者認証によりアクセス制御をおこなうゲートウェイを「認証ゲートウェイ」、アクセスポイントに接続する携帯型パーソナルコンピュータを「クライアント」と呼ぶことにする。

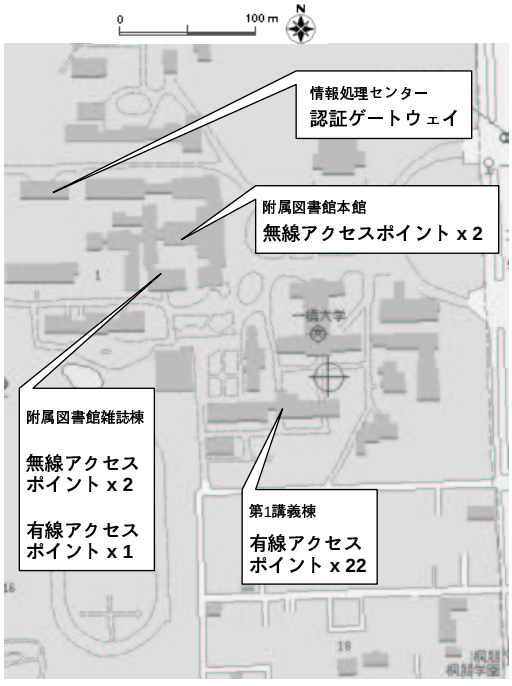
[2] http://www.cc.hit-u.ac.jp/monban/

3　具体的な実装の概略

以下、現時点での認証付きアクセスポイントの実装についての概略を述べる。詳細については本学情報処理センターの WWW サイト[2] にて公開しているので、必要があれば参照されたい。

3.1　アクセスポイント

本学では 2000 年度末の補正予算により IEEE 802.1q VLAN 対応のキャンパスネットワークが構築・運用されており、キャンパス内に約 1300 個の「情報コンセント」が設置されている。これらの情報コンセントは 802.1q VLAN 対応のスイッチングハブのイーサネットポートに (ほぼ)1 対 1 で直結している。本実験ではこの情報コンセントを利用して有線および無線のアクセスポイントを設置した。本稿執筆時点での、アクセスポイントのキャンパス内での配置については次図を参照されたい。



3.1.1 有線

講義室やゼミ室には、1〜2 個程度の情報コンセントが既に設置されているので、これをそのまま有線アクセスポイントとして提供している。

また、附属図書館内のように情報コンセントの数に比べて同時利用者がかなり多いと想定される場所では、小型のイーサネットスイッチングハブを情報コンセントにカスケード接続し、このハブのイーサネットポートをアクセスポイントとして提供している。

いずれも MAC アドレスによるフィルタなどは一切かけていない。

3.1.2 無線

IEEE 802.11b Wi-Fi 準拠の無線アクセスポイントをフロアごとに設置し、最寄りの情報コンセントに接続している。ESS-ID ANY による接続を許可するよう設定し、WEP や MAC アドレスフィルタリングなどは一切おこなっていない。

また附属図書館のカウンターにて、無線 LAN クライアント用の PC カードの貸し出しサービスをおこない、利用者の便宜を計っている。

3.1.3 VLAN

基本的には、情報コンセントごとに異なる VLAN を割り振っている。したがって異なるアクセスポイントは、異なる VLAN に属していることになる。本稿執筆時点では 10 個の異なる VLAN を本実験用に利用している。

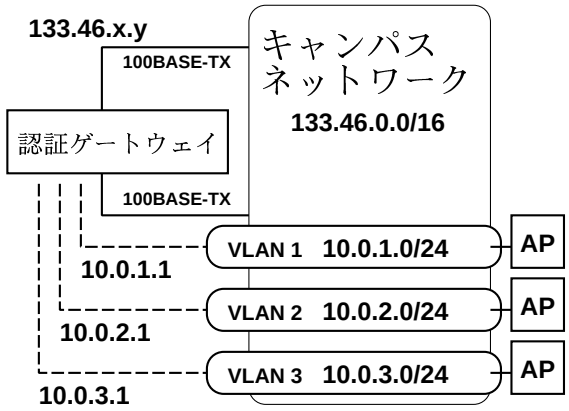
3.2 認証ゲートウェイ

認証ゲートウェイはキャンパスネットワークへ接続しているインターフェースと、各 VLAN へのインターフェース (物理的には 1 本のイーサネットインターフェース) を持つルータであり、以下の機能を有している。

- DHCP サーバ: IP アドレスの割り当てをおこなう。
- WWW サーバ: 利用者手引の公開と SSH2 クライアントの提供をおこなう。
- PAM (Pluggable Authentication Modules): 利用者認証の方式制御をおこなう。
- SSH2 サーバ: 利用者認証およびクライアントのヘルスチェックをおこなう。
- パケットフィルタ: 各 VLAN と外部の間のアクセス制御および NA(P)T をおこなう。

3.2.1 プラットホーム

イーサネット (100BASE-TX) インターフェースを 2 口持つ PC/AT 互換機上で実装をおこなった。OS には Debian GNU/Linux[3](以下、Debian と略す) と (`CONFIG_VLAN_8021Q` および Netfiter を有効にした) Linux kernel 2.4.18 を利用している。



3.2.2 DHCP サーバ

Debian にパッケージングされている ISC DHCP [4] を利用している。DHCP サーバは各 VLAN インターフェースからの DHCP リクエストに対して対応するプライベートネットワークアドレスの IP アドレスを割当てる。MAC アドレスによる利用制限などはおこなっていない。

[3] `http://www.debian.org/`
[4] `http://www.isc.org/`

3.2.3 WWW サーバ

Debian にパッケージングされている Boa [5] を利用している。本運用実験についての利用者手引などを掲載している。また SSH2 Client のひとつである Mindterm [6] を Java Applet として提供している。これにより、Java インタプリタ内蔵の WWW ブラウザ[7]が利用できるクライアントであれば、特別な設定をおこなわなくても後述の認証ゲートウェイへの接続と認証が可能である。

3.2.4 PAM (Pluggable Authentication Modules)

Debian にパッケージングされている、Linux-PAM および pam_radius_auth モジュール[8] を使い、情報処理センターに既存の RADIUS サーバによる利用者認証をおこなっている。

3.2.5 SSH2 サーバ

前項の PAM による RADIUS 認証に対応させるために若干のコード修正をおこなった上で OpenSSH [9] を利用している。

利用者認証 SSH2 クライアントからの接続が確立後、利用者からのアカウントとパスワードの入力を受けて PAM による RADIUS 認証をおこなう。認証に成功した場合は (利用者のアカウントに依存しないある特定の) 擬似ユーザの権限で、この擬似ユーザのログインシェルが起動する。ログインシェルは setuid-root perl スクリプトで、以下の機能を有する。

- 起動時に次項のパケットフィルタと連動して、クライアントの VLAN 外への通信を許可する処理をおこなう。
- 利用者に対して、利用時間などの情報を送信する。
- 終了時に次項のパケットフィルタと連動して、クライアントの VLAN 外への通信許可を取り消す処理をおこなう。

ヘルスチェック OpenSSH のヘルスチェック機能[10]を有効にすることにより、クライアントのアクセスポイントからの切り離しをチェックしている。

その他 ポートフォワーディング機能は無効にしている。

3.2.6 パケットフィルタ

Linux 2.4.x に標準搭載されている Netfilter[11] を用いている。

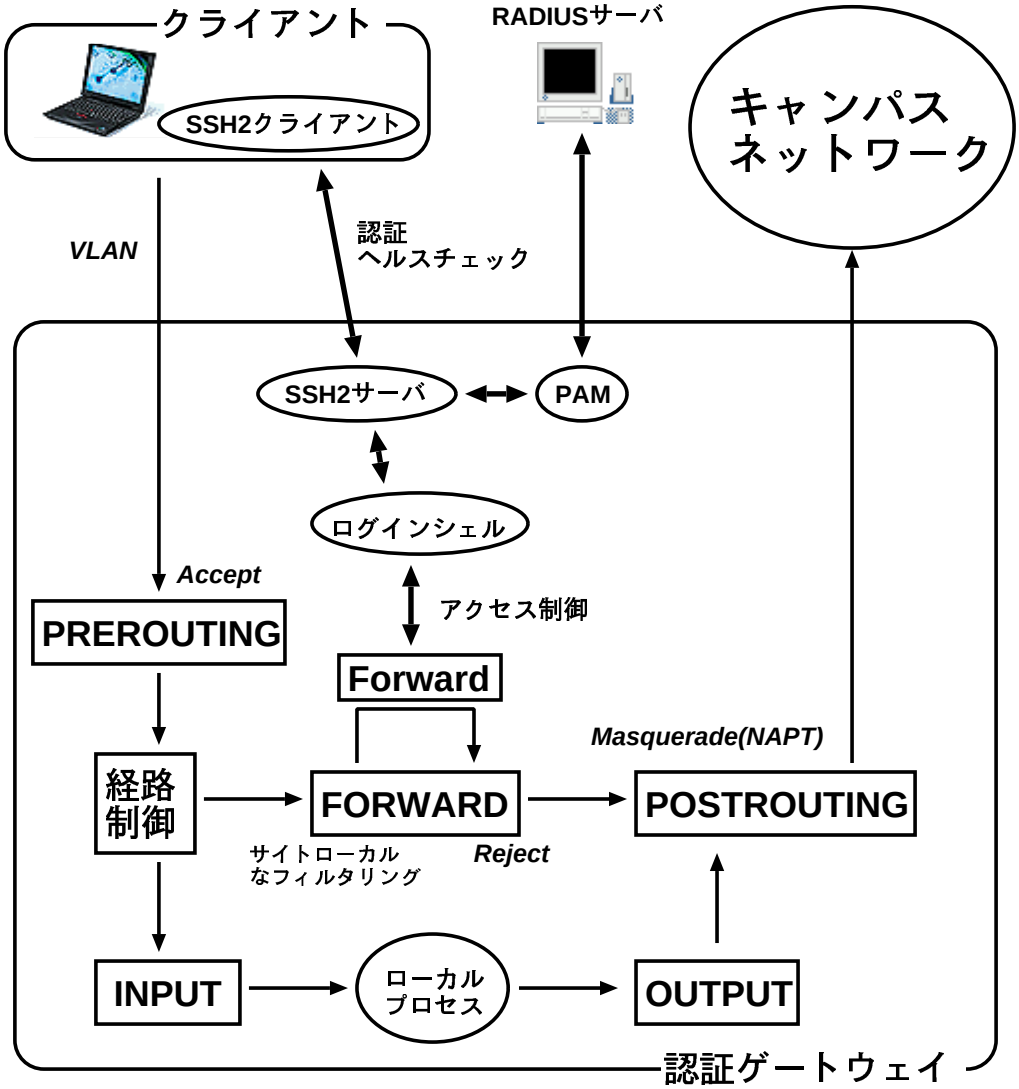
初期状態 各 VLAN から入ってくるパケットに対しての IP フォワーディングはすべて拒否する設定となっている。

利用者認証成功 ログインシェルからクライアントの IP アドレスと MAC アドレスの対を受け取り、VLAN 内から入ってくる、送信元が該当クライアントと一致するパケットに対しての IP フォワーディングを受理するよう設定を変更する。

クライアントの切り離し ログインシェルの終了時 (SSH のセッション終了) に、クライアントの IP アドレスと MAC アドレスの対を受け取り、送信元が該当クライアントと一致するパケットに対しての IP フォワーディングを拒否するよう設定を変更する。

---

[5] http://www.boa.org/
[6] http://www.appgate.com/
[7] Internet Exproler 5.x/6.x や Netscape Navigator 4.x/6.x など。
[8] http://www.freeradius.org/
[9] http://www.openssh.org/
[10] sshd の設定ファイル内で ClientAliveInterval と ClientAliveCountMax キーワードにより制御される
[11] http://www.netfilter.org/



4 評価

構築・運用の手軽さ コード修正・スクリプト作成・各種設定ファイル・スイッチングハブの設定変更などの作業を合計しても数百行程度の手間でシステム構築ができた。また複数の VLAN に対してひとつの認証ゲートウェイでアクセス制御ができるためゲートウェイの運用管理の手間は 1 台分で済む。

クライアントのプラットホーム依存性 Java Applet の利用さえできれば、Windows, Macintosh, UNIX(like) といった各種プラットホームのクライアントで本システムの利用が可能である。

セキュリティ 利用者認証に SSH2 を用いることにより、パスワードの盗聴やセッション乗っ取りといった攻撃にはある程度の耐性を確保できたと思われる。同一 VLAN 内でのクライアント間通信にはまったく制限がかかっておらず、IP アドレスや MAC アドレスの偽造についても無防備であるが、これについては VLAN を細かく設定することにより、危険をある程度は減少させられると考えている。

以上から、当初の方針の最低線は確保できたと考えられる。今後、数ヶ月程度は本システムの運用実験を継続し、実運用のための各種データの収集に努める予定である。

5 課題

5.1 技術的な検討事項

- RADIUS 以外の利用者認証への対応。
- アクセス制御をログインシェルではなく PAM の内部でおこなう [1]。
- IPv6 への対応。

5.2 他システムへの乗り換え

ネットワークへのアクセスを認証付きで提供するというシステムの研究は、過去に多数の事例がある (国内では、東北大学 [4], 東京大学 [telnet], 東京農工大学 [PPTP], 慶応大学 [5], 京都大学・立命館大学 [FreeBSD + Catalyst], 大阪市立大学・岡山大学 [6], 広島大学 [7], 佐賀大学 [8] など。海外での事例も WWW などで多数公開されている)。

いずれも十分な機能と実績を有しており、非常に寛容なライセンスでシステムを公開しているものも多い。したがって、実運用に当っては、これらのシステムの採用を検討するべきと考えられる。

また PPTP や IEEE 802.1x といった普及している (あるいはしつつある) 規格の利用、各社から販売されている商用製品 ([9] など) の導入といった方向も考慮すべきであろう。

5.3 運用サポート体制の確立

本システム運用開始後の利用者のトラブルの大半はネットワークドライバのインストールや DHCP クライアントの設定といった、クライアントをネットワークに接続するための基本的な部分で生じている。

この種のトラブルは前項に述べた各種システムのどれにに乗り換えても生じるものであると考えられるので、実運用をおこなうためには、利用者サポート体制の充実が必須であろう。

参考資料

[1] Nathan Zorn, “Authentication Gateway HOWTO”, http://www.itlab.musc.edu/~nathan/authentication_gateway/

[2] Rusty Russell, “Linux 2.4 Packet Filtering HOWTO”, http://www.netfilter.org/documentation/HOWTO//packet-filtering-HOWTO.html

[3] Rusty Russell, “Linux 2.4 NAT HOWTO”, http://www.netfilter.org/documentation/HOWTO//NAT-HOWTO.html

[4] 後藤英明 他 : “公共利用の無線 LAN/イーサネット・ジャックのセキュリティ対策”, http://www.sc.isc.tohoku.ac.jp/~hgot/secap.html

[5] ほそかわたつみ : xfw – オープンスペース用 IP 認証システム –, http://members.itc.keio.ac.jp/~hosokawa/xfw/

[6] LANA プロジェクト, “LANA(LAN Authentication)”, http://lana.media.osaka-cu.ac.jp/

[7] 広島大学情報メディアセンター : “PortGuard”, http://www.portguard.org/

[8] 佐賀大学学術情報処理センター : “OpenGate”, http://www.cc.saga-u.ac.jp/opengate/

[9] 日立製作所 : “ハイセキュリティLAN システム”, http://www.hitachi.co.jp/Prod/comp/network/security_lan/