富山大学総合情報基盤センター広報　vol.7　（2010）　46-49頁.

研究ノート

学外者向け認証無線 LAN の構築

総合情報基盤センター　　助　教　沖野 浩二
総合情報基盤センター　技術職員　小林 大輔
総合情報基盤センター　　准教授　布村 紀男

第 70 回秋季応用物理学会が 2009 年 9 月 8 日-11 日に本学にて開催された。この会場にて学会参加者へのサービスとして高セキュリティ無線 LAN によるインターネット環境の提供を行った。本論文では、この無線 LAN アクセスサービスの概要とサービス結果を述べる。

1.はじめに

これまで、センターには、学内ネットワーク設備を本学で開催される学会参加者に提供したいとの要望が寄せられていた。この要望に対して今までは、臨時にネットワークの設定を変更して、有線 LAN コンセントが整備されている一室を学外利用者用として開放するなどにより対応していた。しかし、この方法では、利用時にセンター職員が基幹ネットワーク装置および各棟 HUB の設定を変更する必要があり、また誰が利用したか記録をとることができないなど管理・運用面で大きな問題を含んでいた。

2.セキュリティ項目検討

学内のセキュリティを確保しながら、学会参加者に対してネットワーク環境を提供するために、下記項目の検討を行った。

・利用者ごとの認証
・学内ネットワークとのトラフィック分離
・学内 LAN と同等の通信安全性
・現有機器での提供（CISCO 社製品）

これらを確保するために、初めに認証 HUB による有線 LAN の提供を検討したが、認証 HUB の利用には、ポート毎または機器毎にユーザ数の制限があるなど、今回のように多数のユーザが頻繁に入れ替わる状況では現有機器では難しいことが分かった。また、今回の学会では、ネットワークを提供する場所が、展示会会場である体育館が含まれていたために有線 LAN では配線が必要となり、この面からも断念した。

2 番目に学内無線 LAN を利用することを検討したが、既存システムでは、学会参加者を学内認証基盤に登録すれば利用できるが、これはセキュリティの面およびトラフィック分離ができないために、利用不可と判断した。

これらを踏まえて調査した所、既存無線 LAN 装置の firmware を update することにより、公衆無線 LAN アクセスサービス等も用いられるマルチ SSID による複数ネットワークの提供が可能であることが判明した。この機能を利用することで SSID 毎に利用する Radius サーバ指定および VLAN tag 設定ができ、利用者ごとの認証および学内トラフィックとの分離でできることが確認できた。また、SSID 毎に無線 LAN のセキュリティ設定が可能であり、高度なセキュリティの提供も可能であることが判明した。

3.機器の構成

本システムの概念図を図１に示す。

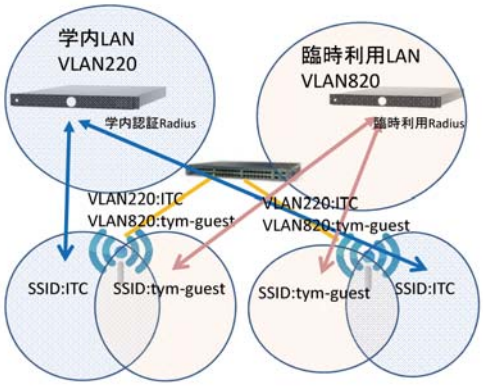

図１.概念図

各無線 LAN は学内用と学外者向けの SSID を配信し、SSID 毎に別の Radius サーバにて認証を行い、それぞれのトラフィックは別の tag を付けて送信する。無線 LAN を収容する HUB では VLAN tag を有効にし、それぞれの別 VLAN として認識する。

無線 LAN の設定

	学内向け	学外者向け
SSID	ITC	tym-guest
TagVLAN	220	820
暗号化/認証	WPA/PEAP	WPA2/PEAP

Radius サーバを 2 台設定し、dot11 ごとの ssid パラメータを指定して、それぞれの暗号化方式を指定する。さらに無線 LAN インタフェース(Dot11Radio0,1)において、利用する ssid と mbssid の設定を行うと、マルチ SSID のビーコンが発信される。また、VLAN ごとに仮想インタフェースにはループ防止のため、brige の設定を行うことが必要である。

実際の設定抜粋（VLAN220 の無線部分）

```
aaa group server radius local_eap
 server 160.26.XX.YY auth-port 1812 acct-port 1813
aaa group server radius guest_eap
 server 160.26.XX.ZZ auth-port 1812 acct-port 1813
aaa authentication login local_eap group local_eap
aaa authentication login guest_eap group guest_eap
!
dot11 ssid ITC
    vlan 220
    authentication open eap local_eap
    authentication network-eap local_eap
    authentication key-management wpa
    mbssid guest-mode
!
interface Dot11Radio0
 encryption vlan 220 mode ciphers tkip
 encryption vlan 820 mode ciphers aes-ccm
 ssid ITC
 ssid tym-guest
 mbssid
!
 encapsulation dot1Q 220
 no ip route-cache
 bridge-group 220
 bridge-group 220 subscriber-loop-control
 bridge-group 220 block-unknown-source
 no bridge-group 220 source-learning
 no bridge-group 220 unicast-flooding
 bridge-group 220 spanning-disabled
```

有線 LAN の設定

```
interface GigabitEthernet0/YY
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
```

無線 LAN AP を収容する有線 LAN においては、上記のように、AP が利用する native vlan（今回の例では 100）の設定が必要である。

4.無線利用方法

無線 LAN サービスは、学内の 2 か所で 3 台の AP により提供した。（第一体育館（2 台），工学部 107 講義室（1 台））

無線 LAN のセキュリティには、WPA2 を利用し、PEAP によるユーザ認証を行う。

無線 LAN を利用するには、利用者は、

① 学会受付にて利用申請書を提出
　記載内容：氏名,所属,連絡先
② ID,Password,マニュアルを受取
③ PC に無線 LAN 設定

を行うことにより、利用が可能となる。

センター側の事前作業としては、

・利用者数の想定
・利用申請書の作成
　（ID,Password の作成）
・無線 LAN の提供箇所の確認
・マニュアルの作成
・学外向け Radius サーバへの登録

が必要となる。本無線 LAN の設定は、既存学内ネットワークとの共存が可能であり、本サービスの提供に従いネットワーク機器の設定変更の必要はない。

```
Radius -log
Thu Sep 10 09:25:56 2009：Auth: Login OK: [gutAAA/<via Auth-Type = EAP>] (from client edu1_1F-117Room port 1660 cli 0000.1234.WXYZ)
DHCP -log
Sep 10 09:25:56 dhcpsv dhcpd: DHCPACK on 160.26.YY.XXX to 00:00:12:34:WX:YZ(hoge) via 160.26.WW.VVV
```

Radius サーバと DHCP サーバには上記の記録が残り、利用申請書（gutAAA の申請者）と突き合わせを行うことにより本人特定が可能となる。

5.利用者数

無線 LAN の利用申請者は、総計 696 名であった。時間帯別申請者を図 2 に示す。

	2009/9/8	2009/9/9	2009/9/10	2009/9/11
～9:30	45	28	12	5
～10:30	50	21	20	4
～11:30	53	50	13	5
～12:30	51	41	30	4
～13:30	62	36	15	
～14:30	18	14	11	
～15:30	23	24	10	
～16:30	18	11	6	
～17:30	7	7	2	
合計	327	232	119	18

図 2.時間帯別申請者

利用申請者の OS は、下記の通りであった。

Windows XP	454
Winows Vista	163
MacOS	67
その他	12
合計	696
その他の内訳	
Linux	2
FreeBSD	1
iPod touch	4
Windows 98	1
スマートフォン	3
Windows 7	1

このうち、認証サーバに成功記録が残っているユーザは、446 名（64%）であった。

残り 36%のユーザに関しては、申請したが利用しなかったものや、利用している認証方式が最新であるために 98 や XP 初期の機器では対応できないものがあったこと、ユーザが設定をできなかった場合などが考えられる。

認証サーバにて 1 時間毎にアクセスしたユーザ数（重複の除く）は、図 3 に示す。

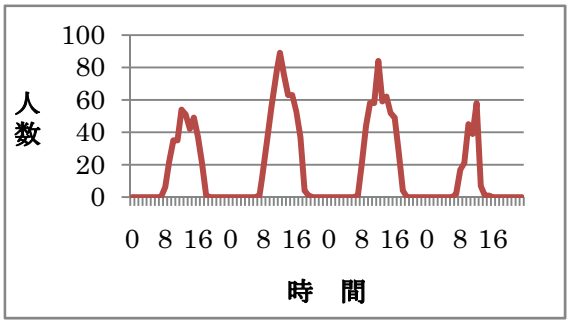

図 3.時間別の利用者

最高利用者数は、9/9 12:00-12:59 までの 89 名である。

4 日間でのトラフィック量を図 4 に示す。

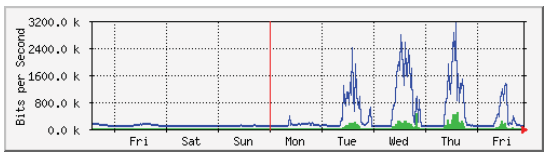

図 4　トラフィック量

今回のシステムにおいては、3 台の AP にて 90 名程度の利用者が問題なく利用できたことが分かる。この時の Network 利用率などはまだ余裕があり AP を増設することにより利用者数の最大を上げることは可能である。加えて、今回は、DHCP サーバでは、アドレス空間として 200 アドレスを準備し、リリース時間を 30 分とした。この設定においても、ピーク時には 180 程度まで割り当てをされており、今後の運用時にはリリース時間の短縮（10 分程度）が必要だと考えられる。

6.今後の課題

今回の学外者向け認証無線 LAN においては、学外向け Radius を別途準備することにより、

・利用者ごとの認証
・学内ネットワークとのトラフィック分離
・学内 LAN と同等の通信安全性
・現有機器での提供

を行うことができた。

今回のシステムにおいて、利用者からのクレームとして所有する機器が WPA2 に対応しておらず、利用できないユーザが少なからずいたことが上げられる。これに関しては、機材は WPA のサポートも可能であるが、セキュリティ面を検討して、今回は、採用を見送った経緯があるが、今後はこれらのユーザへの手当のために

・有線 LAN のサポート

の検討を行いたいと考える。また、学外者向け認証システムを常設化のために、

・学外向け Radius サーバの設置

を行いたい。これは、今回は、準備期間等の関係により Radius サーバの電子証明書は、自己証明書となってしまった。これは無線 LAN においては、致命的な問題となりうる。この問題の解決のためにも常設し、電子証明書を事前に導入することが必要だと考える。

今後、利用者からの要望を踏まえて、マニュアルの改訂や利用申請書のパスワード記載 font の変更などを行い、より使い易いシステムにしたい。