小山工業高等専門学校研究紀要
第　45　号（2012）　105－110

RADIUSとLDAPによるキャンパス無線LAN認証システム

南斉　清巳*1，山上　宇宙*2

Authentication System with RADIUS and LDAP for Campus Wireless LAN

Kiyomi NANSAI*1，　Uchu YAMAGAMI*2

With spread of tablet PCs and mobile devices, the needs to connect with wireless LAN freely and to access to the Internet are increasing.　A lot of wireless LAN access points are already installed in the classroom or the laboratory in the campus. However, some of those are low security level and we can also see interference of a channel. When these are neglected, there is a possibility of causing a serious security issue. We made a wireless LAN authentication system with a RADIUS server and a LDAP server, which can manage the authentication from many wireless LAN access points in a unified manner.

KEYWORDS : LDAP, RADIUS, Wireless LAN, Authentication

１．はじめに

タブレットPCや携帯端末の普及に伴い、学校内においても自由に無線LANに接続してインターネット等にアクセスしたいというニーズが高まっている。本校でも既に教室や研究室内にかなりの数の無線LANアクセスポイントが設置されている。しかし、それらの多くはセキュリティレベルが低くチャネルの干渉も見受けられる。これらを放置すると重大なセキュリティ問題を引き起こす恐れがある。本稿はRADIUSサーバとLDAPサーバを連携させ、ユーザが無線LANに接続するときにユーザ認証を行なうとともに、多数の無線LANアクセスポイントからの認証を一元管理できる無線LAN認証システムの構築例を報告する。

２．システムの構成

認証サーバにはアプライアンス製品の導入も考えられるが、できるだけ安価にしかも拡張性も考慮し、Linuxサーバ上にRAIUSとLDAPを導入し連携させることにした。Linuxのディストリビューションには RHELと互換性のある Sientific Linux6.1 を使用した。Scientific Linux はフェルミ国立加速器研究所（Fermilab）と欧州原子核研究機構（CERN）が開発するLinuxディストリビューションで、CentOSと同様にRHELと互換性を持つことが特徴である。学内の建屋全域で無線LANを利用可能とするためには、無線LANのアクセスポイント（以下、APという）は100台程度必要となる。これらのAPを効率よく管理運用するためにはAPの物理的な配置、利用するチャンネル設定や利用者認証方式など綿密な設計が必要となるが、ここでは主として利用者に対する認証方式について検討しシステム構築する。無線LANの運用においては有線LANに比較して利便

*1電子制御工学科(Dept. of Electronic Control Engineering) E-mail:nansai@oyama-ct.ac.jp
*2平成２４年３月電子制御工学科卒業、現茨城大学

性は高いが、無線の性質上盗聴やなりすましなどセキュリティの面で弱いという特徴がある。多くのAPがすでに設置されているが、それらの中にはSSIDとWEPによる暗号で運用されているものが見受けられる。WEPは脆弱性が指摘されておりツールを使えば簡単に盗聴できてしまうという危険性がある。

今回構築する認証システムではWPA2-EAPを使用する。EAP(Extensible Authentication Protocol)にはいくつかの種類がある。セキュリティ面でもっとも強固なのはサーバとクライアントの両者で電子証明書を用いるEAP-TLS方式であるが、すべてのクライアントに電子証明書をインストールする必要があるので運用の面で管理者の負担が大きい。ここではサーバ認証には電子証明書を用い、クライアント認証にはIDとパスワードで行うEAP-PEAP(Protected EAP)方式を採用した。この方式はWindowsの標準サプリカントをはじめ多くのデバイスが対応しているので特別なソフトをインストールする必要はない点で有利である。暗号化方式にはAES(Advanced EncryptionStandard)を用いる。AESは他の暗号方式に比べて安全性が高いと言われている。ただし、この方式で使用する無線LANのAPにはWPA2-EAPの認証方式に対応したものでなければならない。無線LAN認証システムの構成を図1に示す。

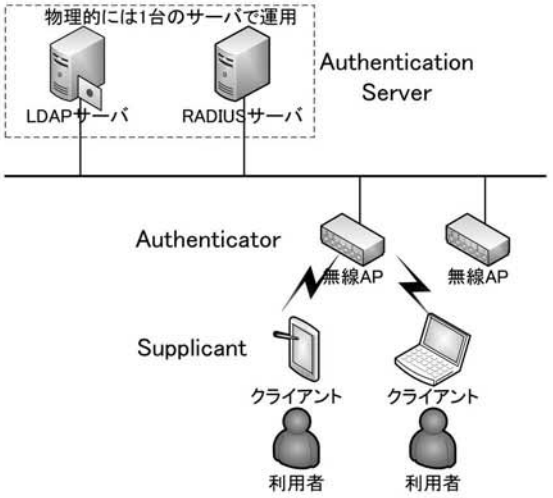

図1　無線LAN認証システムの構成

【使用機器およびソフトウェア】
○ Server: Intel Celeron 2.2GHz, 2GB
○ OS: Scientific Linux 6.1
○ RADIUS: FreeRadius 2
○ LDAP: OpenLDAP 2.4
○ アクセスポイント: Buffalo AirStationPro
○ LDAP管理ツール: LDAPadmin(Windows)

3．システムの仕組み

図2に動作原理を示す。ネットワークに接続したいクライアントは無線アクセスポイントのSSIDを選択し接続要求する。端末画面に認証画面が現れるので利用者は自分のIDとパスワードを入力する。端末はIDとパスワードをRADIUSサーバに送信する。このときパスワードはCHAPプロトコルを用いるのでパスワードそのものは流れない。IDとパスワードを受け取ったRADIUSサーバはLDAPサーバに問い合わせを行い、利用者の認証を行う。登録された正規のユーザであれば正しく認証され、ネットワークへの接続が完了する。RADIUSサーバの真正性はサーバの電子証明書で行うが、ここでは自己証明書を用いている。

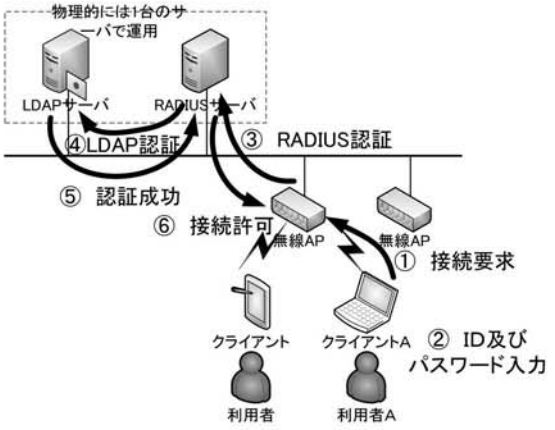

図2　認証の仕組み

4．インストールと設定

4．1　FreeRadiusのインストールと設定

Scientific Linuxの標準ツールからFreeRasiusのインストールを行う。メニューバーのシステム＞管理＞ソフトウェアの追加と削除を選択し、FreeRadius2をインストールする。LDAPサーバと連携するには「LDAP support for freeradius」のプラグインを追加でインストールする必要があ

るので注意しなければならない。

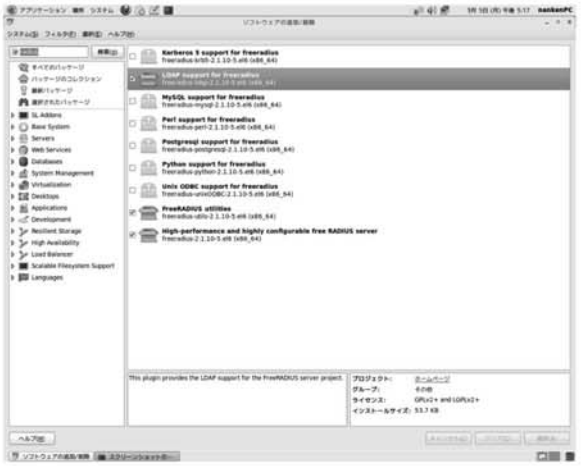

図３　FreeRADIUS のインストール画面

インストール終了後、次に示すように設定ファイル変更を行う。

(1) RADIUS サーバを停止させる。
　　# service radiusd stop
(2) /etc/raddb/radius.conf の修正
　　auth = no の行をコメントアウトし、
　　auth = yes を新しく追加する。
(3) exec、expiration、logintime をコメントアウトする。
(4) /etc/raddb/client.conf の修正
　　以下を追加してアクセスポイントを登録。
　　client 172.16.22.△△△{
　　　secret　　=　△△△△
　　　shortname　=　SouthLab
　　}
(5) RADIUS サーバを起動させる。
　　# service radiusd start

以上で基本的な設定は完了となる。次にテスト用ユーザを作成し、テストコマンドを用いてサーバが正しく動作しているか確認を行う。確認の手順は次に示す通りである。

最初に RADIUS サーバの動作を確認するため、RAIDUS サーバ自身でユーザ認証を行うように、ユーザ設定ファイル/etc/raddb/users にテストユーザを追加する。

(1) テストユーザ nanken を追加登録する。
　　“testuser” Cleartext-Password := “nanken”
(2) RADIUS サーバをデバックモードで起動する。一度サーバを停止させてからでないとデバッグモードで起動することはできないので注意すること。
　　# service radiusd stop
　　# radiusd -X
(3) 別のターミナルを立ち上げ、テスト用コマンドを入力する。
　　# radtest testuser nanken　172.16.22.△△△ 1812 △△△△
　　認証に成功すると Access-Accept と表示される。

以上でアクセスポイントを介した RADIUS サーバによる認証の設定が終了し、RADIUS サーバの動作が確認できる。

４．２　OpenLDAP のインストールと設定

システム＞管理＞ソフトウェアの追加と削除より OpenLDAP をインストールする。このときサーバ・クライアントの両方をインストールする必要がある。インストール時にサポートライブラリなどが自動でインストールされる。図４にインストール画面を示す。

図４　OpenLDAP のインストール画面

インストール終了後は設定ファイルを修正する。このとき root 権限でないとファイルの内容の書き換えが行えないので、注意する必要がある。
修正は次の手順で行う。

(1) LDAP サーバを停止させる。
　　# service slapd stop
(2) /usr/share/openldap-servers/DB_CONFIG.example を DB_CONFIG にリネームし

/var/lib/ldap にコピーする。

(3) slappasswd コマンドを使用してパスワードを暗号化して作成する。

```
# slappasswd
New password://暗号化したいパスワード入力
Re-enter new password: //もう一度入力
{SSHA}v4zq+lbUEhnORE1PiWhVgH
wUQQ0iLDgy　//暗号化されたパスワードが生成される
```

(4) /etc/openldap/slapd.conf　の修正

suffix　“dc=example,dc=com”　に修正

rootdn “cn=Manager,dc=example,dc=com” に修正する。

rootpw には slappasswd コマンドを用いて作成した暗号化されたパスワードをコピー・ペーストする。

(5) 設定データベースを再構築する。

```
# rm -rf /etc/openldap/slapd.d/*
#sudo -u ldap slaptest -f
/etc/openldap/slapd.conf -F
/etc/openldap/slapd.d
```

(6) LDAP サーバを起動させる。

```
#service slapd start
```

以上で基本的な設定は完了となる。このとき、設定データベースを再構築しないと slapd.conf で修正した内容が反映されず、デフォルトのままとなってしまうため注意する必要がある。

4．3　LDAP 管理ツール

次に LDAP の管理ツールである LDAPAdmin を用いてユーザの登録を行う。コマンドラインからの操作も可能であるが管理ツールを使用した方が操作性がよい。LDAPAdmin はダウンロードしたファイルを任意の場所に解凍し、実行ファイルを起動すればすぐに使用することができる。

今回は同じネットワーク内にある Windows マシンに導入し、そこから登録を行った。

LDAPadmin を起動後、Connect ボタンを押すと接続先一覧が表示される。設定画面を図５に示す。Host には LDAP サーバの IP アドレスを入力する。Base、Username、Password には slapd.conf で設定した suffix、rootdn、rootpw の値をそれぞれ入力する。

設定完了後、Test conection ボタンで接続の確認ができる。

図５　接続設定画面

接続が完了したら次はユーザの登録を行う。ディレクトリの右クリックメニューから

New>User を選択すると、図６のような画面が表示される。最低限入力する必要がある項目は Second name、Username、Home Directory の３つであるが、Username 以外の項目は今回使用しないので分かりやすい値を入力しておく。

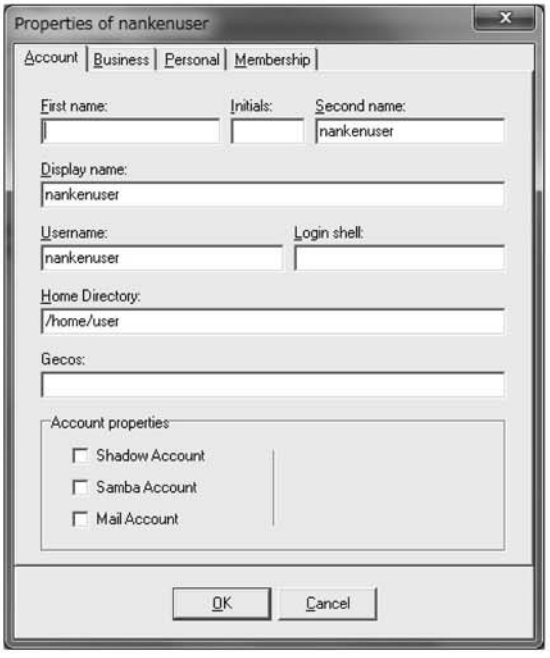

図６　ユーザ登録画面

次にユーザのパスワードを設定する。右クリックメニューから Set Password を選択し、設定したいパスワードを入力する。これでユーザ名とパスワードの登録が完了となる。ユーザ情報の設

定完了後の画面を図７に示す。

図７　ユーザ情報画面

以上で基本的なユーザ情報は登録できたので、LDAP サーバの構築が完了となる。ユーザ情報に新たな属性を付与したりする場合は、右クリックメニューからの Edit Entory から行う。

４．４　AP の設定

つぎに無線 LAN アクセスポイントの設定を行う。設定には本体（AirStationPro）に付属している AirStationAdminTools で行う。AirStationAdminTools を起動し、無線 LAN アクセスポイントの設定を編集する。TOP ページにある、『無線 LAN の暗号化を設定する(RADIUS サーバを使う)』から設定ページにいくことができる。ここでは暗号化方式と RADIUS サーバの IP アドレス、共有パスワードを設定する。

暗号化方式	: WPA2-EAP(AES)
RADIUS サーバの IP アドレス	: 172.16.22.△△△
共有パスワード	: △△△△
AP の IP アドレス	: 172.16.22.△△△

４．５　クライアントの設定

クライアントからの接続テストを行うため、ノート PC（Windows 7）上でワイヤレスネットワークの設定を行う。ネットワーク名には SSID 名を入力する。セキュリティの種類は「WPA2-エンタープライズ」を選択し、暗号化の種類は「AES」を選択する。ネットワークの認証方法の選択では「Microsoft 保護された EAP(PEAP)」を選択する。つぎに保護された EAP のプロパティ画面で「セキュリティで保護されたパスワード（EAP-MSCHAP v2)」を選択する。さらに構成ボタンを押し、「Windows のログオン名とパスワード・・・」のチェックを外しておく。以上で PC のワイヤレスネットワーク設定は終了である。ネットワークに接続されると図８に示すような認証画面が現れるので登録されたユーザ名とパスワードを入力する。

図８　端末から接続したときの認証画面

５．まとめ

RADIUS サーバと LDAP サーバを連携させた無線ＬＡＮ認証システムを構成し、動作を確認することができた。無線ＬＡＮ接続時に利用者ＩＤとパスワードによる認証を行うことで、無線ＬＡＮのセキュリティを保ち、運用の一元化ができる。さらにセキュリティを高めるためには、利用者が学生であるか教職員であるかの情報を LDAP サーバに登録しておき、ユーザ認証時にその情報を参照しそれぞれ異なる VLAN に接続されるようにすることが考えられる。また、本校においては全学生が教育計算機を利用するためのユーザ登録をアクティブディレクトリサーバ（ＡＤサーバ）に行っている。無線ＬＡＮ認証用の LDAP サーバと教育用計算機のＡＤサーバを連携させてユーザ情報を一元管理することによって運用管理が軽減できると考えられる。

参考文献

1）デージーネット著：入門 LDAP/OpenLDAP　ディレクトリサービス導入・運用ガイド、秀和システムズ 2007 年
2）　Jonathan Hassell：RADIUS―ユーザ認証セキュリティプロトコル、オライリージャパン 2003 年
3）中井悦司：プロのための Linux システム・ネットワーク管理技術、技術評論社 2011 年

【受理年月日　2012年 9月28日】