学外からのアクセスについて

総合情報基盤センター　助手　沖野 浩二
okino@itc.u-toyama.ac.jp

はじめに

近年、安価なブロードバンド環境の整備･普及により､自宅でも ADSL や CATV, 光ファイバ等による Internet アクセスが一般的なものとなってきました。それに従って大学のダイアルアップ機材の利用者も減少し、現在では一部の人がメールの確認に利用する場合がほとんどとなっています。

このような中で、総合情報基盤センターには、自宅にあるブロードバンド環境から大学の設備を利用したいという要望が多く寄せられるようになりました。

今までも､ssh によるリモートアクセスやポートファワードによる mail サーバへのアクセス等を紹介してきましたが、残念ならば一般の人の簡単に利用できるものではないというのが現状でした。

そこで、平成１８年度稼動予定の新ネットワークシステムにおいて、外部からの利用を支援するアクセスシステムを導入することとしました。

アクセスシステム

外部からのアクセスシステムに関して利用の要望は大きく分けて下記に分類されることになると思います。

・電話回線によるアクセス
・ Internet 経由によるアクセス

つぎに、利用したいアプリケーションとしては、

・ メールサーバ
・ Web サーバ
・ その他サーバ

が挙げられると思われます。

そこで、これらの要望を満たすために、下記のシステムを導入することとなりました。

・ ダイアルアップサーバ
・ SSL-VPN 装置
・ WebMail システム

この三種類のサービスを提供することにより、ほぼ、前出の要望が満たすことができると思われます。

また、これらのサービスを導入するにあたり、下記の点をついて検討を行いました。

・ セキュリティの確保
・ 使いやすさ
・ 安定性
・ パスワードの同期

これらの問題に対応するために、基本的には、

・ OS 標準機能だけで新規のアプリケーションをインストールしないもの
・ 暗号化されていること
・ 新規に整備される認証基盤に接続されること

を選定の基準としました。

認証基盤

新システムではセンターの整備する機材の認証を一元的に管理するために、LDAP(Lighweight Directory access Protocol)を導入し、機器のアクセス情報を管理する Radisu(Remote Authentication Dail In User Service)はユーザ情報を LDAP に確認するように構築いたしました。このシステムにより、センターに利用申請をしていただくことにより、すべてのユーザは、hhhh.ddd(hhh はユーザ名,ddd はドメイン)という形式の ID とセンターのパスワードにより利用することが可能となりました。また、センターシステムのパスワードを変更すると同時にアクセスパスワードも変更となります。また、この形式で無線 LAN もアクセスすることが可能となります。

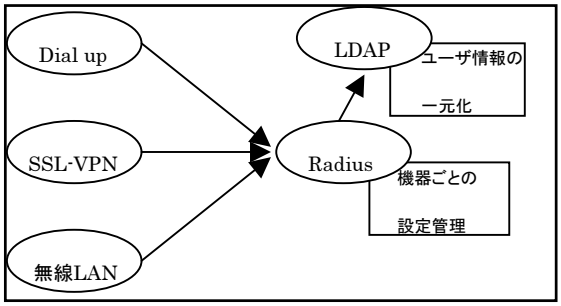

図１：認証基盤構成図

暗号化

新システムでは、Internet 経由にアクセスするために、パスワード等を暗号化により適切に扱うことが必要となりました。ダイヤルアップでは、通話盗聴がないために PAP と呼ばれる暗号化されないパスワードにより運用されていましたが、インターネット経由では盗聴の可能性があるためそのままでは危険です。そこで、chap と呼ばれる暗号化認証方式で運用することになるのですが、現在利用されている OS（windows XP や Mac OS X）では、よりセキュリティが強化されている ms-chap v2 と呼ばれるものが標準となっています。本システムではより安全性を求めるために最初から ms-chap v2 に対対応するように設計したしました。これによりユーザは最新の OS のセキュリティの設定を落とすことなく（設定を変更することなく：図２）利用することが可能になりました。また WEB メールに関しても公式な証明書を導入した https により運用し、安全性を確保しています。

図２：セキュリティレベルの変更

ダイアルアップサーバ

今までも運用していた Dailup サーバを更新し、最新のサーバを導入いたしました。これによりアナログ(56k bps モデム),ISDN,携帯電話，32/64kbpsPIAFS V2.0,V2.1(第三世代携帯、PHS)というほとんどのアクセスに対応いたしました。

SSL-VPN 装置

SSL-VPN 装置には大きく分けて

- 専用 VPN 装置
- WEB-VPN
- PPTP 装置

に分けられます。

それぞれ特徴があり、専用 VPN 装置は、VPN 装置初期に出てきた機器で、利用者が利用する PC に専用ソフトを導入することが必要になります。そのため、導入するには手間が大きいと言えます。しかし、昔からあるために専用ソフトが対応している OS の範囲が多いということも言えます。

WEB－VPN は、その後出てきたもので、WEB インターフェースを利用することで、ユーザはソフトウェアをインストールする必要がないというものです。しかし、利用できるアプリケーションが WEB と指定されたメールサーバのみという制限やメールソフトウェアの設定を変更する必要があります。

最後の PPTP 装置は、最近注目されているもので、windows2000 以降や MacOS X で標準サポートされている機能です。OS 標準なので、ユーザは特殊な設定を行う必要がない、動作も安定しているという特徴があります。だた、最新の OS しかサポートしていないということがいえます。

本システムでは、安定性等の観点から PPTP をサポートするハードウェア SSL-VPN 装置を導入いたしました。

図３：PPTP 設定アイコン

PPTP の設定には、Windows の場合、OS 標準の新しい接続ウイザードにより設定でき、設定後は図３のアイコンをクリックすることで学内ネットワークに接続すると同様な環境を実現できます。

PPTP の利用時の注意点

PPTP を利用している時の通信は、すべて大学を経由しての通信となります。また、一部のソフトウェアに関しては、PPTP を利用した場合、接続が切れる場合があります。このときは PPTP を切断後、ソフトウェアの再起動を行ってください。

ホテルや空港などの FreeSPOT を利用してアクセスする場合、制限があることがあります。この場合には、以下の手順を試してみてください。

1.FreeSPOT 接続、2.web 起動、

3.どっかのサイト確認後、4.pptp 接続

これにより PPTP が利用可能となる場合があります。また、セキュリティ上 VPN を一切許していない FreeSPOT があります。この場合には利用できません。

WebMail システム

自宅からのメール確認のために、WEB 経由でメールを確認できる WEBMail システムを導入したしました。これにより自宅の PC から大学のメールを読むことが可能になりました。

図４：WEBMail 画面

このシステムでは、センターが準備するすべてのドメインのメールを読むことが可能で、多言語にも対応しています。その上、SPAM フィルター等も搭載していますので、ぜひご利用ください。利用時の注意点として、セッション管理のため Cookie を有効にする必要があります。

図５：WebMail の証明書

また、サーバに搭載している電子証明書は公式なものであるため、証明書等のインストール等のセキュリティ上懸念（オレオレ証明書等のインストール）のある行為を行わずに利用することが可能です。

まとめ

今回の整備により大学の認証基盤が整備され、これにより電子証明書等を利用した安全な認証を行う基盤が整備されました。今までのシステムごとの認証データから統一された認証データを利用することによるユーザの利便性の向上と ms-chapv2 等の安全な認証プロトコルによる本人確認が可能となりました。これにより OS のセキュリティを低減することのない運用が可能となり、盗聴等対応するセキュリティの向上を図ることが可能となりました。

参考文献

・PPTP マニュアル：センターWEB 掲載予定
・WebMail マニュアル：センターWEB 掲載予定
・RADIUS―ユーザ認証セキュリティプロトコル,Jonathan Hassell (著), アクセンス・テクノロジー(訳),オライリー・ジャパン,2003
・LDAP ハンドブック―ディレクトリ・サービス標準プロトコル,河津, 山形ら(著), ソフトリサーチセンター,2002
・LDAP -設定・管理・プログラミング- Gerald Carter, でびあんぐる（著),オーム社,2003