富山大学総合情報基盤センター広報　vol.8　（2011）　8-11頁.

学内認証基盤の構築

総合情報基盤センター　助教　沖野 浩二

2006 年 2 月の情報システムの更新に合わせて、3 キャンパスのユーザ情報を一元管理する学内認証基盤の構築を行った。この認証基盤は、この 5 年の間に情報センターのシステムだけでなく、学務システム等にも連携され、学内の情報基盤にはなくてはならないものとなった。本稿では、5 年間で整備された学内認証基盤の概要とその効果、今後の課題について述べる。

１．はじめに

2005 年 10 月の 3 大学の統合時の課題として、3 キャンパスにおいて、どのキャンパスのユーザも同様に統一システムにアクセスすることが求められた。この課題に対応するために情報センターでは 2006 年の 2 月の情報システムの更新に合わせて、3 キャンパスのユーザ情報を一元管理するために学内認証基盤の整備を行った。この認証基盤の整備によりユーザはどのキャンパスにおいても同一のサービスを受けることが可能となった。

２．認証基盤要件

認証基盤には、物理デバイスのよる IC カードや WEB システムに特化した SSO(シングルサインオン)が代表的なものである。これらの導入には多大のコストが発生し、運用には多くのコストが発生する。また、情報センターのサービス基盤として考えた場合には、Windows 端末だけでなく、Mac や Linux など IC カードで適応できないものや WEB システム以外での ID 利用の場面が考えられた。そこで学内情報基盤として整備を行うための流れとして、3 キャンパスにおいて同一の ID・Password を利用できることを目的として、下記の順序で整備することとした。

a)センター内での ID 名（管理番号）の統一
b)ID 名をキーとした PasswordDB の整備
c)センター内のシステムを PasswordDB に接続

PasswordDB には、LDAP サーバを利用することとし、センターにある各システムが LDAP の認証情報を確認することで、ユーザ認証を行うこととした。これによりセンターの各システムは、ID 名を LDAP サーバに問い合わせを行うことにより認証されることになる。加えて、各キャンパスに存在するセンター管理の端末室(Windows および Mac)の認証も行うことも必要である。これらの要件を踏まえて、認証基盤の仕様を決定した。また、認証基盤は認証情報の一元管理を目的としており、最低限の認証情報および home パスなどのユーザ管理情報しか掲載しないこととした。

３．認証基盤構成

本学における認証基盤の概要を図１に示す。

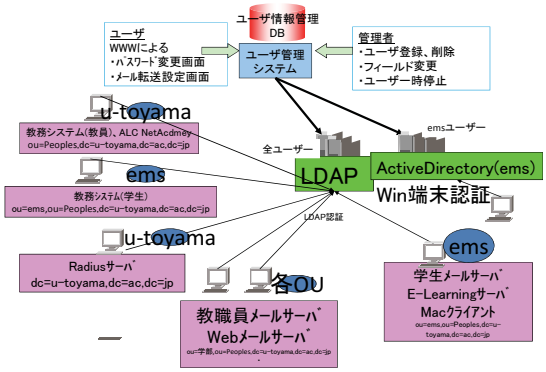

図１　認証基盤　構成図

認証基盤は、ユーザ情報管理 DB サーバ(umag)を中心として、配下に LDAP サーバとセンター端末室用の ActiveDirectory（以下 AD という）を有している。LDAP サーバは、五福キャンパスに 2 台、杉谷 1 台、高岡 1 台の配置とし、AD は、五福・杉谷 2 台、高岡 1 台の配置とした。Password の変更は、ユーザ情報管理 DB サーバの Web Interface を経由して行うことにより、3 キャンパスの LDAP および AD に自動的に反映されるシステムとした。

また、LDAP に記載される情報は、メールアドレスに合わせることとし、

・学部ごとのメールドメインに合わせて 15 個の ou（ドメイン）を設定

・cn に ID.domain を登録する。

という設計した。具体的には、sample@itc.u-toyama.ac.jp の LDIF（LDAP 情報）は表 2 の通りとなる。この場合 ou は itc となり、cn は sample.itc となる。ユーザは ID 名として cn を入力することにより、認証基盤を利用することが可能である。

表 2 サンプル LDIF

```
dn:
uid=sample,ou=itc,ou=Peoples,dc=u-toyama,dc=ac,d
c=jp
sn: itc
sambaAcctFlags: [UX]
loginshell: /bin/bash
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
objectClass: organizationalPerson
objectClass: sambaSamAccount
gidNumber: 501
mail: sample@itc.u-toyama.ac.jp
uid: sample
gecos: sample
uidNumber: 510
cn: sample.itc
homeDirectory: /home/g1/itc/sample
sambaLMPassword:
EDCE6E6AC4E1232936077A456CCDF409
sambaNTPassword:
123BE8084B4344BE33756632F3765F1C
userPassword: {crypt}aFt2JvErIo6R.
```

４．サービススケジュール

これらの認証基盤の整備を通じて、行った Password 連携は下記の通りである。

・2006 年 2 月更新時

-全学メールサービス

-端末室相互利用

-WebCT

・2006 年度中
　-学務システム
　-Call 教室、ALC
　-ECS system
・2007 年度
　-無線 LAN 認証
　-BlackBoard
・2009 年度
　-ファイル共有サービス
・2010 年度
　-有線 LAN 認証

現在、センターが運用しているシステムは、すべて学内認証基盤により認証がおこなわれるようになっている。また、学生は普通利用するすべてのシステムにおいて、教員は事務系を除いて認証基盤を利用することとなっている。（図 3,4）

図 3　学生向け Password 関係図

図 4　教員向け Password 関係図

5．導入効果

認証基盤は、センターだけでなく、学内のシステムへ拡張されてきた。実際の利用者数も大きく増えており、導入効果は高いと言える。実際の導入効果の一部として、大きく変化したものを示す。

<u>無線 LAN 利用者の変化</u>

認証基盤を利用している代表的なサービスとして全学による PEAP 認証付きの無線 LAN サービス（図 5：利用者数）があげられる。現在 3 キャンパスで、100 台の AP が稼働している。この認証サービスは、キャンパス内のユーザだけでなく、キャンパス間を移動する教員が多く利用しており、今後も増えること予想される。

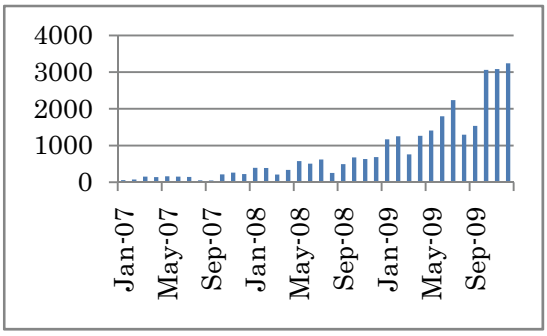

図 5　無線 LAN 利用者数

<u>Password の再発行回数の変化</u>

認証基盤整備により大きく変化したものが図 6 に示すユーザ Password 再発行回数の変化である。

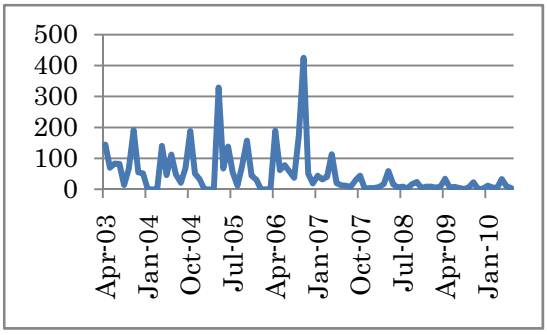

図 6　Password 再発行回数の変化

2006 年 2 月に認証基盤の稼働が開始され、同年 9 月に学務情報システムとの連携が行われ、このときに 425 名の再発行が行われた。しかし、その後再発行件数は大きく減少することとなる。実際に、Password 発行業務は、認証基盤導入前の 2005 年度の 927 回から 2009 年度の 106 回へと 89%もの業務低減となった。再発行減少の理由は、認証基盤の ID/Password を利用するシステムが増加したため、ユーザの利用機会が増えたためと考えられる。

６．課題

5 年間の認証基盤運用を行った結果、改善すべき課題は以下の通りである。

性能上の問題

年数を重ねるごとに認証基盤の利用範囲が広がり、初期の想定より、多くのアクセスが発生している。加えて、認証を利用するシステムの多くが、五福キャンパスに設定しているために、五福キャンパス設置の LDAP サーバの負荷が高い状態が続いている。負荷に応じたサーバの増強・分散が必要となった。

認証基盤に格納する情報

認証基盤には、最低限のユーザ情報しか格納しなかった。しかし、この 5 年間の間に LDAP システムが認証情報 DB の標準として確立され、多くの WEB システムなどで標準的に利用できるようになった。加えて Shibboleth 等に代表される SSO に於いて LDAP 上にユーザ氏名や所属等の情報を格納していることが必携となってきている。

認証情報の安全性

LDAP 上には、安全性の確保のため平文は格納せず、hash 化されたパスワードをその目的に応じて 3 種類格納されている。

・sambaNTPassword
・smbaLMPassword
・userpassword

これら 3 種類のうち sambaLMPassword は利用されている hash 能力が低く脆弱性が指摘されている。また、userpassword に関しては、暗号化関数が DES-Base であるために、これも hash 能力が低く脆弱である。加えて、暗号化の文字数が 8 文字までに制限されるため現在のコンピュータ能力では全数攻撃が可能である。

安定性の確保

認証基盤が学内システムにおける中心となったために、認証基盤の停止がシステムの停止へ直結することとなった。

７．今後の予定

2011 年 2 月の情報システムの更新では前述の問題を解決するために、

・五福キャンパスに設置する LDAP を、2 台から 3 台へ増設（全体で 4 台から 5 台へ増強）
・WEB システムに氏名等を表示するために格納情報を追加（氏名、所属等）
・脆弱な暗号システムから暗号システムを更新し、文字数を 16 文字まで拡張

を行った。

今後の課題として Shibboleth 対応などの新しいユーザサービスを検討していきたい。

[1] 沖野浩二,布村紀男,”富山大学における認証基盤の整備による業務軽減評価”,学術情報処理研究 No14,2010

[2] 江藤博文,渡辺健次,只木進一,渡辺義明,"全学的な共通情報アクセス環境のための統合認証システム",2002-95 IOT 研究会 IPSJ,pp31-36 ,2002