端末接続ネットワーク用認証サーバの構成例

Authentication Server Configuration for a Terminal Netowork

檜垣 泰彦[1]　阿由葉 努[1]　全 へい東[2]　土屋 俊[3]

Yasuhiko Higaki　Tsutomu Ayuha　Heitoh Zen　Syun Tutiya

千葉大学 (工学部[1] / 総合メディア基盤センター[2] / 文学部[3])

Chiba University (Faculty of Engineering / Institute of Media and Information Technology)

1　まえがき

本稿では本学における端末接続ネットワークの構成と工学部におけるその運用について，認証サーバの構築と運用を中心に述べる．

無線 LAN の WEP だけによる運用は危険であることが知られており，また，情報コンセントについても利用者認証を行うことがセキュリティ上好ましい．そのため，本学でも“端末接続ネットワーク”なるものを導入した．工学部では学生数も多く，端末接続ネットワーク専用の ID とパスワードをひとつの担当係が配布・管理することは困難な状況であった．そこで，学生については，既に運用中の別システムから各自で利用登録を行う方式をとり，職員については，階層的な管理権限を設けて，管理・運用を分散させる方式をとった．

2　端末接続ネットワーク

図 1 に本学総合メディア基盤センターが提供している端末説接続ネットワークの構成を示す．アクセスマネージャ(AM)，コントロールサーバ (CS) としては Vernier の AM6500・CS6500[1] を使用している．AM はクライアントからの認証要求を CS へ取次ぎ，CS の指示でクライアントのアクセスを制御する．CS は認証サーバに問合わせることで認証要求を処理する．

本学では，AM・CS までを総合メディア基盤センターが管理運用し，情報コンセントや無線のアクセスポイント，認証サーバは各部局で準備，運用する方式をとっている．工学部ではこれを Safe (Secure Internet Access @ Faculty of Engineering) と名付け，教育委員会・計算機ネットワーク委員会により構築・運用している．Safe で設置されている情報コンセント数は 5 つの OA 教室を中心に，全 23 教室に合計約 500 個，アクセスポイント数は約 30 である．

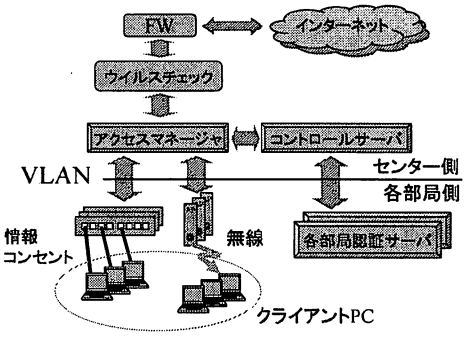

図 1　端末接続ネットワーク構成

表 1　Safe の権限一覧

権限	説明
safe0	管理者．登録権限のある第 1 種スタッフ (safe1) の登録・削除権限のみあり．管理者 1 人あたり数 10 人程度のユーザを管理．
safe1	第 1 種スタッフ．常勤スタッフ等．ユーザ (safe2, safe3, safe9) の登録・削除権限あり．1 人あたり高々10 人程度のユーザを管理．
safe2	第 2 種スタッフ．非常勤スタッフ等．safe1 権限のユーザにより登録される．ユーザの登録・削除権限はない．
safe3	大学院生・研究生等．safe1 権限のユーザにより登録される．
safe9	有効期限付の一時利用 ID．safe1 権限のユーザにより登録される．

3　認証サーバの構成

工学部の認証サーバは OpenLDAP[2] を利用して構成した．FreeBSD[3] に ports から www/apache13-modssl, net/openldap21, www/mod_auth_pam, security/pam_ldap, net/p5-perl-ldap をインストールして認証サーバと管理用 Web サーバを構築した．3,253 人の学部学生については既に運用中の学生用サーバ s4s[4] のユーザ認証済みのページ内に Safe ユーザ登録ページを設けた．パスワードは s4s 認証用のものとは別のパスワードを新たに設定し登録するようにした．

s4s に登録されていない大学院学生や研究生，及び職員については表 1 に示すような権限を設定し，分散管理する方法をとった．各学科ごとに safe0 権限をもつ管理者を数名置き，具体的な運用はそれぞれの学科に任せた．スタッフを追加登録ができる権限 (safe1) とできない権限 (safe2) に分類した．各研究室所属の大学院生・研究生については，その研究室内の safe1 権限の職員が管理を行う．全員が利用すると仮定した場合，safe0 の管理者 12 人が 252 人の常勤職員 (safe1) を管理し，その safe1 が 244 人の非常勤 (safe2)，1,179 人の大学院生等 (safe3) を管理すると，各 safe0 は 12 人の safe1 を担当，safe1 は合わせて 5.6 人の safe2・safe3 を担当する計算となる．s4s で管理する学部学生も合わせると，総数 4,928 人をこの人数分担で管理できる計算となる．

4　あとがき

重要度がそれほど高くない ID・パスワードについて，従来のシステムと連携をとり，管理単位を適切な規模に分割することでスムーズな運用を実現できた．それぞれの権限保有者が継続してそれぞれの責任範囲を認識し，適正な管理・運用を続けていくことが可能かどうかが今後の課題である．

参考文献・URL

[1] http://www.verniernetworks.com/AMCS6500.html
[2] http://www.OpenLDAP.org/
[3] The FreeBSD Project, http://www.FreeBSD.org/
[4] 檜垣, 阿由葉, 土屋:履修登録システムの構築と運用, 電子情報通信学会技術研究報告 OIS2003-10, Vol.103, No.45, pp.13-18(2003-5)

Copyright © 2004 IEICE