Vol.2010-IOT-8 No.53
2010/3/2

フェリス女学院大学 ネットワークシステムの構築

内田奈津子† 因幡哲男† 滝島繁則††

フェリス女学院大学では 2009 年 3 月に全面的なシステム更新を行った．その一環として，セキュリティと利便性の両立をめざして，トリプル認証（IEEE802.1X 認証/Web 認証/MAC 認証）を用いた統合認証システムを構築した．本報告では，本システム導入の経緯や，構築したシステムの評価について述べる．

On the Development of a Network System at Ferris University

Natsuko Uchida†, Tetsuo Inaba† and Shigenori Takishima††

Ferris University in Yokohama, Japan undertook a comprehensive system update in March 2009. In part this involved developing an integrated authentication system using triple authentication (IEEE802.1X authentication/Web authentication/MAC authentication) so as to balance the goals of security and user-friendliness. In this report, we will discuss the process of system introduction, as well as the review of system implementation.

1. はじめに

フェリス女学院は，1870（明治3）年に創立され，2010年には創立140周年を迎える日本初の近代女子教育機関であり，日本最古のミッション系女子大でもある．

本学は，「少人数教育」「語学教育」「国際理解」「主体的な学び」の四つを学びの特徴として，時代を拓くリベラルな女性を世に送り出してきた．学部は文学部，音楽学部，国際交流学部の3学部で学生数は約2600人．キャンパスは横浜市泉区の緑園キャンパスと同市中区の山手キャンパスの二箇所である．

2009 年 3 月末に教研系システムと事務系システムの更新時期が共に到来することになった．そこで，最新の技術を採用して，学内システムの全面的な刷新が行われることになった．本報告では，新システムのコンセプトと，認証を中心にしたシステムの実装について述べる．

2. 検討の経緯

2007 年に学内委員会において新システムの検討が開始され，基本方針として以下の三つが確認された．

第一が「安全性」である．マスコミ上で個人情報の漏洩であるとか情報の違法取得といったニュースで賑わっていたため，本学においても情報管理の強化と，不正な情報アクセスに対する対策が必要と認識された．

第二が「管理・利便性」である．本学ではICT教育および事務効率化のために，早くから全学ネットワークを構築し，サーバや端末を適宜配置してきた．しかし，それらを継ぎ足しして拡大してきたので，ひどく複雑な構成になっていた．サーバのセキュリティアップデートは何十台に及び，メールシステムやストレージサービスは登録内容の変更等のメンテナンスの工数が多く，運営側の負担になっていた．また，従来のシステムは事務系ネットワークと教育系ネットワークをポートベースVLANで分けていたため，柔軟性に乏しいものだった．運用側の管理・利便性をもとめ，ユーザ側の利便性も損なわないような提案を期待した．

第三が「環境配慮型システム」である．本学の特長の1つに「エコキャンパス」があり，2005年度には文部科学省の現代GPに本学の「地球温暖化抑制に向けた地域の環境教育拠点の形成」が採択されている．さらに2009年9月に実施された「第1回エコ大学ランキング（私立大学部門）」では本学が第1位となった．これは，エコ・リーグ（全国青年環境連盟）が主催した調査によるもので，調査に回答した全国109大学を対象として行われたものである．こうした経緯から，新システムにも「エコキャンパス」の一翼を担うことが期待された．

決定した基本方針を基にして，さらに具体的な構築指針が以下の通り策定された．

第一の「安全性」に関する構築指針は以下の通りである．

・有線 LAN および有線 LAN のセキュリティ強化
・Internet からの不正アクセスの防御とコンテンツの安全性確保

第二の「管理・利便性」に関する構築指針は以下の通りである．

・仮想化採用によるによるリソースの有効活用

† フェリス女学院大学
Ferris University
†† 伊藤忠テクノソリューションズ株式会社
IT OCHU Techno-Solutions Corporation

・アカウント管理の統合による管理負荷の軽減
・外部フリーメールサービスの採用による管理効率の向上
・シームレスな接続環境

第三の「環境配慮型システム」に関する構築指針は以下の通りである

・省電力機器の積極的な採用
・仮想化によるサーバやストレージなどの集約化
・認証プリンタによる不要出力の削減

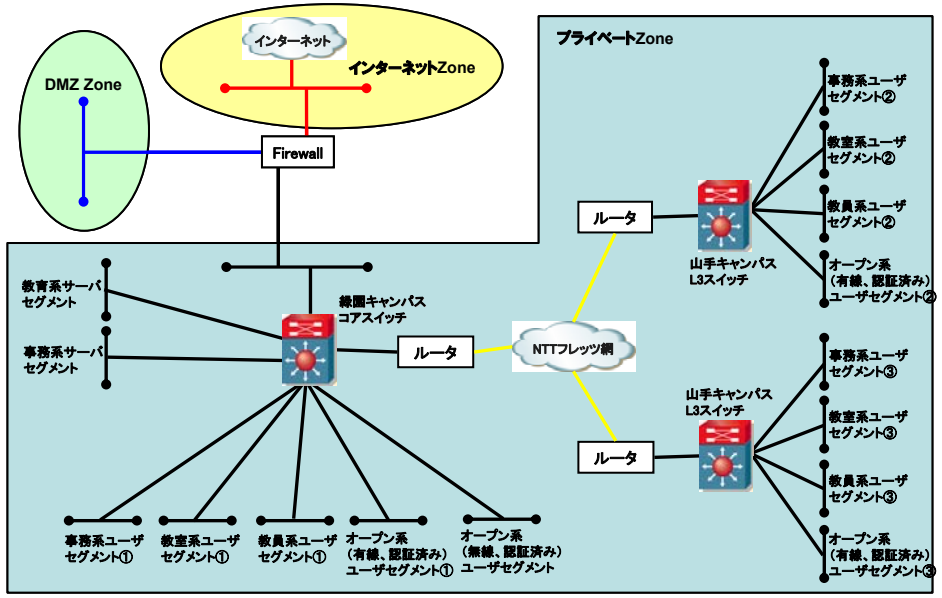

図１．フェリス女学院新ネットワークシステムの概要図

3. システムの構成

本項では，前項で示された構築指針にもとづいて構築された新システムについて述べる．

3.1 ネットワーク

新システムではコアスイッチには 10 ギガビットインターフェイスに対応したアラクサラネットワークス社のシャーシ型のスイッチである AX6304S を冗長構成にして配置し，エッジスイッチに同社の AX2430S を配置している．機種選定根拠として，次項以下で述べる IEEE802.1X 認証／Web 認証／MAC 認証の三種の認証方式の混在（以下，これをトリプル認証という）に対応していること，省電力であることがあげられる．本システムの概要を図 1 に示す．

3.2 認証サーバ

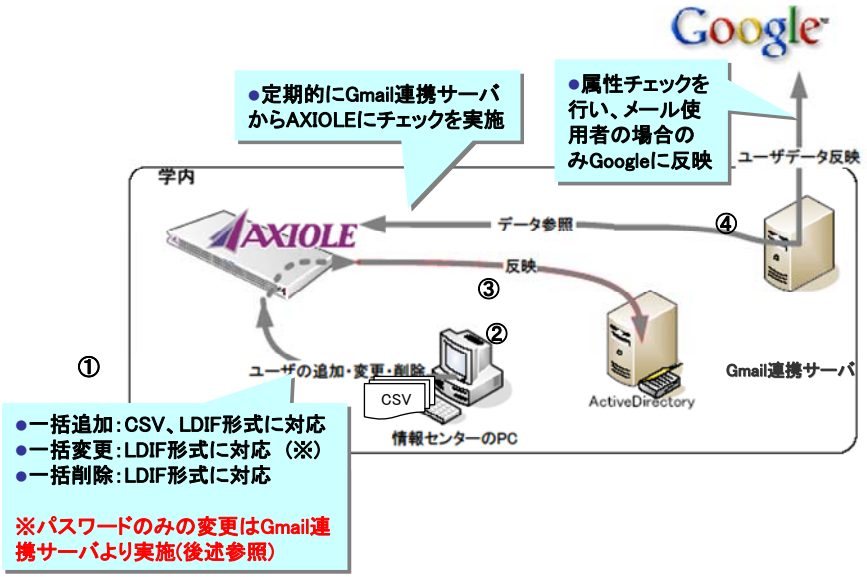

図 2．AXIOLE によるアカウント管理の一元化イメージ

本学の従来のシステムでは，教研系と事務系でそれぞれ別個の ActiveDirectory サーバが稼動していたが，相互連携していないため教研系ネットワークと事務系ネットワークは全く独立したネットワークであった．また個別のアプリケーションサーバが認証を行っており，ユーザは数個のパスワードを使い分けせざるを得ない状況であった．こうした環境はセキュリティ的にも好ましいものではなく，1 ユーザ 1 アカウントへの集約がセキュリティ的視点からも要請されていた

本学の新システムでは，認証用のサーバとしてネットスプリング社のAXIOLEを採用した．AXIOLEはLDAPとActiveDirectory，RADIUSを連携し，アカウントの一元管理を実現した．一元化の概要を図3に示す．

アカウントの一元化が実現すると認証サーバの重要性が増すため，AXIOLEは2台設置しホットスタンバイの冗長化構成を取っている．

AXIOLE は情報登録や管理作業が全て Web の GUI から行えるので管理工数が削減できた．

3.3 ネットワーク認証

従来のネットワークはポートベース VLAN を採用したものだったので，端末の設置場所（ポートの場所）によって利用者も制限される自由度の低いものだった．たとえば，学生は教室のパソコンにはログインできるが，アルバイト先の図書館の端末は図書館職員しかログインが許されていないため使用できないといった状況だった．そこで新システムではダイナミック VLAN を採用することが決まった．これにより，ユーザは端末の設置場所（スイッチポート）を意識することなく，ネットワーク上のリソースへアクセスさせることができるようになった．

こうした方針にもとづき，ユーザの区分，接続される VLAN の区分，接続可能なリソースの範囲が，表 1 の通り決定していった．

表 1　通信制御の概要

ユーザ区分	標準で接続される VLAN	サーバリソース			
		事務 A リソース	事務 B リソース	共有リソース	基盤リソース
大学教員	大学教員 VLAN	×	×	○	○
大学学生	大学学生 VLAN	×	×	×	○
職員 A	事務 A VLAN	○	○	○	○
職員 B	事務 B VLAN	○	×	×	×

○･･･アクセス許可，×アクセス拒否

ユーザのネットワークの使い勝手の問題と表裏の関係にあり，避けて通れないのがセキュリティの問題である．本学においてもセキュリティに対する意識が高まってきており，セキュリティを高める措置が要請されていた．そうした中で検討されたのが，最適な認証方式の選択と，学内でも場所によるセキュリティ強度に変化をつけることだった．

認証方式の検討にあたっては，端末の特性がまず注目された．学内に設置される端末は大学資産の端末だけではなく外部から持ち込まれる端末も数多く，利用されるOSもWindowsだけではなくMacOSなど複数のOSが混在する環境である．さらにプリンタのようにネットワークに接続される装置類も多くなってきている．このような端末群をキャンパスネットワークに収容するためには，それぞれの端末属性に応じた認証方法を検討する必要がある．単一の認証方式では，こうした端末群のセキュリティレベルを維持しつつ，洩れなく認証することが困難になってきているためである．

表 2　代表的な認証方式の比較

認証方式	端末対応		導入の容易さ	運用の容易さ	セキュリティレベル	概要
	Win	Mac Linux				
IEEE802.1X	○	△	△	△	◎	接続するパソコン上のサプリカントと呼ばれる認証クライアント･ソフトウェアと，802.1X 対応の LAN スイッチ，認証サーバで構成される．
Web 認証	○	○	◎	◎	○	Webページにアクセスするときに，ユーザ名とパスワードの入力を求め，入力された値がサーバでアクセスを許可しているユーザに一致すると，ページにアクセスすることができる．暗号化はSSLが使用可能だが，全ての環境で利用できるわけではない．
MAC 認証	○	○	◎	×	△	それぞれの Ethernet カードが持つ固有の ID 番号を認証システムに登録しておき，登録されたアドレス以外のアクセスを制限する方式．暗号化はできない．サプリカントや Web の稼動しない装置類でも認証可能．

表 2 に代表的な認証方式をしめすが，本学では Windows 端末以外にも，MacOS 端末の導入も必須とされており，さらにプリンタもあり，これら含めた認証システムを構築するためには，複数の認証方式の組合せをせざるを得ないと判断した．

ここで，三案の運用モデルを仮定し，それぞれのモデルについて管理性とセキュリティの両面から検討を行った．その検討内容を表 3 に示す．第 1 案は，セキュリティの最も高い 802.1X 認証を基本としている．Windows2000 以前の WindowsOS や MacOS は 802.1X 対応が限定的であるので，802.1X 認証に適用困難な端末については Web 認証を適用し，Web 認証も困難な端末については MAC 認証方式を適用するものとした．第 2 案は，大学では一般的な MAC 認証をメインとし，セキュリティリスクの高い持込端末には Web 認証を適用するものである．第 3 案は，貸出端末，持込端末のみに認証をかける方式である．

三案の中では，まず非認証端末が発生する第 3 案が否決された．最終判断としては管理性よりもセキュリティの高さを優先して，第 1 案のトリプル認証が選択されるこ

Vol.2010-IOT-8 No.53
2010/3/2

とになった.

表 3　認証方式の比較

検討案		第 1 案	第 2 案	第 3 案
検討案の条件		学内全ポートで 802.1X 認証，Web 認証，MAC 認証を実装	学内全ポートで Web 認証，MAC 認証を実装	事務室，教室は認証なし，情報コンセントはWeb認証，MAC認証を実行
認証方式	事務端末	802.1X 認証	MAC 認証	認証なし
	教室端末	802.1X 認証	MAC 認証	認証なし
	貸出端末	802.1X 認証	MAC 認証	MAC 認証
	持込端末	Web 認証	Web 認証	Web 認証
	プリンタ等	MAC 認証	MAC 認証	情コン⇒MAC 認証 他⇒認証なし
評価	管理性	△	○	◎
		・802.1X 認証端末にサプリカントの配布が必要 ・プライベート CA 局が必要 ・事務室，教室，情コンの展開自由度が高い ・事務系端末は，IP アドレス自動取得に切り変えの必要あり	・学内資産全端末の MAC アドレスを管理し，Radius サーバへ登録が必要 ・事務室，教室，情コンの展開自由度が高い ・事務系端末は，IP アドレス自動取得に切り変えの必要あり	・学内資産端末のうち，貸出端末の MAC アドレスを管理し，Radius サーバへ登録が必要 ・事務室，教室，情コン用でスイッチのポートを分ける必要あり ・事務系端末は，従来の固定 IP アドレスを継続資料可能
	セキュリティ	◎	△	×
		学内ネットワークに高レベルのセキュリティを提供可能	・Web 認証，MAC 認証は詐称可能性あり	事務室，教室は認証されないため，第三者の学内ネットワークへの侵入が可能

第 1 案を新システムに実装した運用イメージが、図 3 に示すものである.

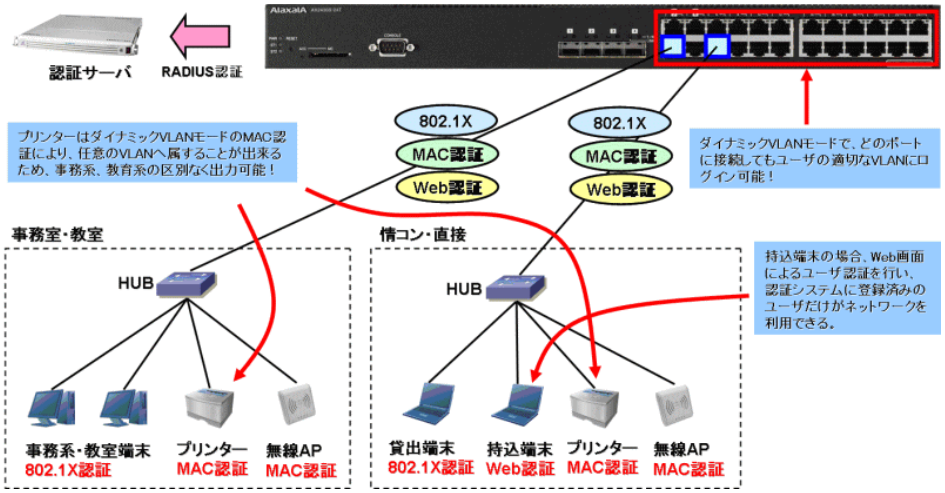

図3. トリプル認証方式の運用イメージ

次に，場所別にセキュリティ強度を変化させることを検討した．教室やオープンスペースなどの学生が自由に出入りできる場所についてはセキュリティを高くし，事務室や会議室など事務職員中心の利用が想定される場所については，セキュリティを緩やかにするという考え方である.

具体的には，人の出入りの多い教室では，認証された端末は固定VLANモードによる接続のみが許可され，大学学生VLANに接続される．その他の事務室，図書館事務室，会議室，研究室では，動的VLANにより，ユーザ種別に応じたVLANに接続されるようになっている.

端末の種別とネットワークポートの設置場所による認証方式とVLANモードの関係について，表4に示す.

また，新システムでは802.1X認証にWindows標準サプリカントを採用した．このため，端末への802.1X設定をActive Directoryサーバより配布することができるようになった．こうした方式がとれるため，商用サプリカント利用時のインストールや設定の作業と比べると，管理負荷を大幅に低減することができた.

表 4　認証方式及び VLAN モード

端末		認証方式及び接続 VLAN　注 1，注 2				
端末種別	端末台数	事務 A ポート	事務 B ポート	会議室 ポート	研究室 ポート	教室 ポート
事務端末	200	802.1X 動的	802.1X 動的	802.1X 動的	－	－
学生用 貸出端末	120	802.1X 動的	802.1X 動的	802.1X 動的	802.1X 動的	802.1X 固定
教員用 貸出端末	90	802.1X 動的	802.1X 動的	802.1X 動的	802.1X 動的	802.1X 固定
学生・教員等 持込端末	150	－	－	Web 動的	Web 動的	Web 固定
教室端末 (Windows)	150	－	－	－	802.1X 動的	802.1X 固定
教室端末 (MacOS)	20	－	－	－	－	MAC 固定

注 1.「認証方式及び接続 VLAN」の項目は，上段が認証方式，下段が接続 VLAN モードを示す．
注2.「認証方式及び接続VLAN」の項目の，動的は動的VLANモードを，固定は固定VLANモードを示す．

3.4　無線LAN

無線LANシステムとしてARUBA Networks社製品を採用した．アクセスポイントを教室と公共スペースを中心にした学内42箇所に設置している．

ARUBAは中央管理型を特徴とする製品で，認証・暗号・ポリシーは中央側の無線LANコントローラ上で管理されており，その内容をアクセスポイントがダウンロードする仕組みになっている．アクセスポイント単位の設定作業が不用になり，管理負荷が大幅に軽減されている．

認証については有線LANと同様で，貸出端末に対しては802.1X認証が行われ，持込端末に対してはWeb認証が行われる．いずれの場合でも，有線LANに比べるとセキュリティの不安があることから，認証が成功した端末は大学無線VLANに固定的に割り当てられる設定になっている．

また，貸出端末は802.1X認証を行っているため信頼性が高いと判断し大学無線VLANのサーバリソースへのアクセスに制限は設けていないが，持込端末はArubaのFirewall機能を利用してWebとメール利用のみに利用制限をかけている．

3.5　メールシステム

電子メールの管理負荷は，平常時のパスワード忘れや配信確認依頼等の対応をはじめ，年度更新作業まで含めると非常に大きなものがある．そうした対策として，教育機関を対象としたフリーメールサービスへのアウトソーシングを行った．このサービスは現在のところ3社が提供しているが，本学のフリーメール導入の主目的が管理負荷軽減であることから，以下2点を重視してGoogle Apps Education Editionを選択した．

①認証連携が可能である点
　学内に構築した認証システムと連携することにより，アカウント管理の負荷軽減を図りたい．

②不要なサービスを利用不能な設定が可能である点
　サービス提供会社は競争するようにサービスメニューを増やしている．サービスが増えれば問合せの増加も予想され，不要なサービスは利用不可にしたい．

認証連携の仕組みを構築し，学内システムと同一のパスワードでGmailを利用することを可能にした．Gmailへのログインは，GoogleApps Education Editionの用意するSAML準拠のAPIを利用することによって，パスワードが学外に流出しない仕組みを構築した．この接続手順を図4に示す．

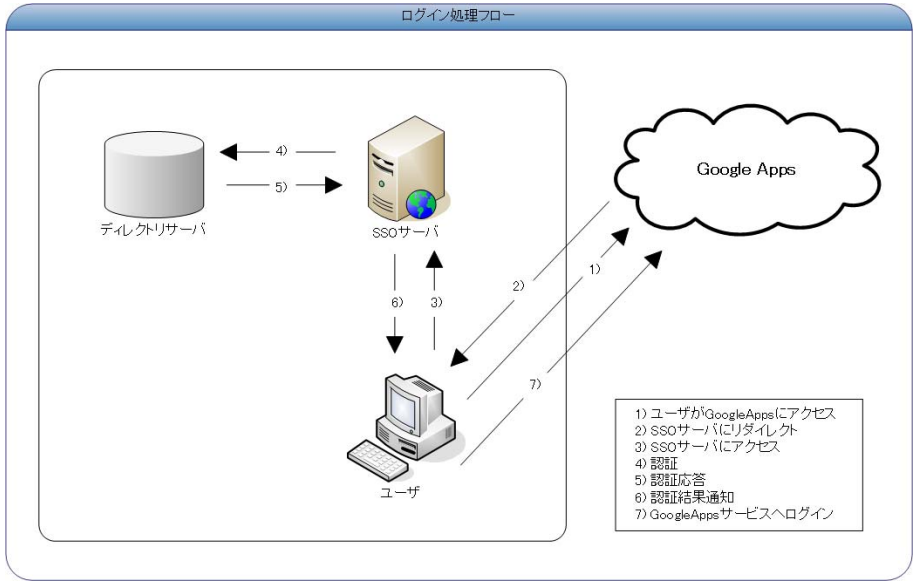

図 4.Gmail へのログインの流れ

また，ユーザはフリーメール使用中にパスワード変更を行うことが可能であるが，この状況を放置すると，学内の認証サーバとフリーメールのパスワードの整合性が取れなくなる．そこで，フリーメールでのパスワード変更を，本学の認証サーバに反映させるための仕組みを構築した．このフローを図 5 に示す．

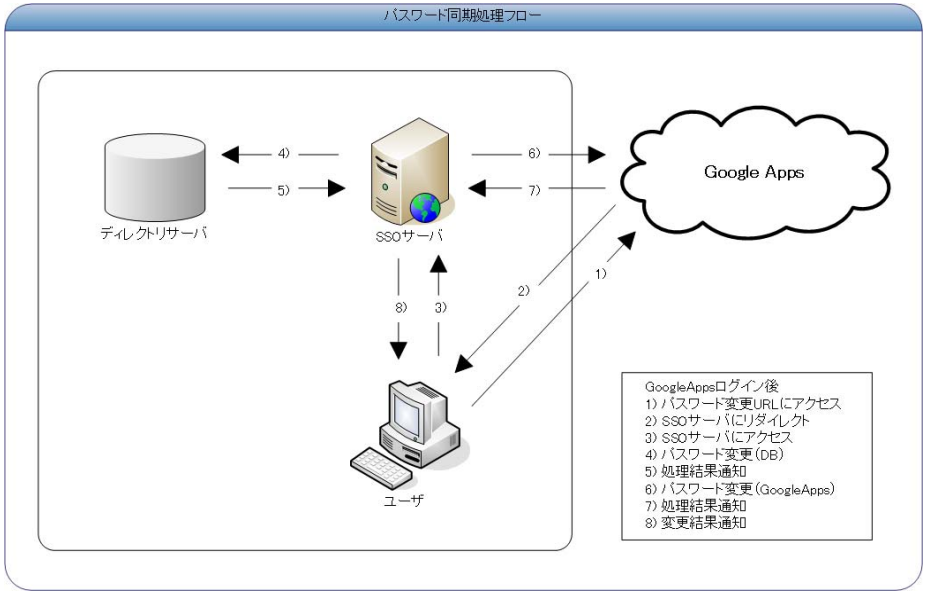

図 5　パスワード変更の流れ

4.　おわりに

新ネットワークシステムは2009年2月のフリーメールのリリースに始まり，段階的なリリースを経て，予定通り2009年4月から正式稼動に入り現在に至っている．

アカウントを統合したことによるメリットは大きかった．特に，同一アカウント/パスワードで学内システム及びフリーメールを利用できる効果は大きく，学生から情報センターへの問い合わせが激減した．従来は，履修登録時にアカウント忘れの学生が多く，そのための専用窓口を設置するほどだったが，新システムに移行しその必要がなくなった．さらに新システムでは，アカウント管理が簡素化されタイムリーな運用が可能となった．

しかし，学内には依然として個別認証のシステムもいくつか残っているが，これらも随時，システムの更新時に新しい認証システムに組み込んでいく予定である．既に2010年度に稼働する学務システムとは，認証連携がとれ試験稼働を始めたところである．

今回の更新で，事務系と教育系のネットワークが統合管理でき，認証システムの見直しを行ったことで，管理がしやすくなった．大学のように，様々な端末やユーザが利用する環境に適した，ネットワークのトリプル認証とダイナミックVLANの連携は，メーカー初の実装例であった．

授業の合間やレポート提出前には，オープンスペースや教室で，貸出用のノートPCを無線LANに接続して利用する学生が増えてきている．また，個人のPCの持込みも徐々に増えてきている．このような状況から現在の課題として，回線の帯域確保が問題となっている．現在，キャンパス間は，Bフレッツの公衆100Mbpsの回線である．インターネットへの接続も同様の公衆100Mbpsであり，内外ともに回線の遅さを感じている．

費用の問題もあり簡単には解決できないが，学生がITに触れる機会を増やし，学生の興味を引き出していくような環境を目指していきたいと考えている．

参考文献

1)　アラクサラネットワークス株式会社　http://www.alaxala.com/jp/
2)　株式会社ネットスプリング　http://www.axiole.jp/
3)　アルバネットワークス株式会社　http://www.arubanetworks.co.jp/