汎用端末での利用者認証を可能とした セキュアな教育支援用ネットワークの構築

新井　イスマイル[*1]，福嶋　徹[*2]，井谷　武史[*3]，中川　卓也[*3]，福田　豊[*3]，
佐村　敏治[*1]，渡部　守義[*4]，堤　保雄[*1]

Development of Secure Network for Education Support which Enables General Terminal to Authenticate Users

Ismail ARAI, Tohru Fukushima, Takeshi INANI, Takuya NAKAGAWA, Yutaka FUKUDA,
Toshiharu SAMURA, Moriyoshi WATANABE, and Yasuo TSUTSUMI

The conventional education support network in Akashi National College of Technology was physically and logically divided into Office LAN and Research LAN because of the security purpose. Furthermore, computer software in these LANs needs to be ready for proxy to reach the Internet. In short, these LAN are inconvenience for users. This paper describes a case study of introducing NAT (instead of the proxy servers) and concurrent use of Web authentication and MAC authentication instead of the conventional proxy server to meet the requirements for both security and convenience.

KEYWORDS : The Internet, Education Network System, Network Operation, BYOD(Bring Your Own Devices)

1. はじめに

高等専門学校（以下、高専）のネットワークは、学生への教育支援を主目的としており、教育支援の形態は、学生の学習・研究、教員の教育・研究、教職員の成績処理等の事務作業といったように、多岐にわたる。教職員の事務作業では教務・学生指導関係の機密データを取り扱うため、学生や校外者がそのようなデータにアクセスできないセキュアなネットワーク設計が求められる。一方で、学生・教員の学習・教育・研究活動においては、校内外を自由にアクセスできる利便性の高いネットワーク設計が求められる。

明石高専のネットワークは、人員の都合により極力メンテナンスが不要でセキュアであることが求められており、学習・教育・研究のための利便性を犠牲にしてきた背景がある。本校ネットワークは、学生と教員が学習・教育・研究目的で主に利用するもの（研究 LAN）と、教職員が事務作業を主目的として利用するもの（事務 LAN）の２つに、物理的・論理的に分離して、相互の通信を認めない構成にしている。各 LAN にそれぞれ設置したプロキシサーバを経由してのみ、インターネットへの接続性を各端末に提供していた。

しかし、各LANに１台ずつ設置したプロキシサーバに通信が集中し、通信のボトルネックになる問題が無視できなくなった。ログが一杯になりプロキシサーバが機能せずLAN内の全端末がインターネット接続性を失っ

*1 明石工業高等専門学校電気情報工学科(Dept. of Electrical and Computer Engineering, Akashi National College of Technology)
〒674-8501　兵庫県明石市魚住町西岡 679-3　E-mail: ismail@akashi.ac.jp
*2 明石工業高等専門学校事務部学生課(Student Affairs Division, Akashi National College of Technology)
*3 明石工業高等専門学校技術支援センター(Technical Education Support Center, Akashi National College of Technology)
*4 明石工業高等専門学校都市システム工学科(Dept. of Civil Engineering, Akashi National College of Technology)

た事例もある。また、学生教職員が利用するテレビ会議システムの導入や、研究目的での研究室内サーバ設置等、特定の部屋の特定の端末に対して外部からのアクセスを可能とする要求（すなわち新たなネットワーク敷設の要求）、あるいはネットワーク接続を前提とするが、プロキシサーバ経由での通信に未対応のアプリケーションが存在する等、現状のネットワークでは学生・教職員の要求に柔軟に応えられない。他にも、研究 LAN の接続端末数が多い中、研究室等に無線ルータを間違った方法で設置して校内全域にトラブルが波及してしまう事件が度々起こった。

そこで、平成 24 年のネットワーク機器共同調達を機に上記問題を解決するネットワークを再設計した。

第 1 に、範囲が広すぎた研究 LAN を分割して、LAN 内に問題が起きた際の影響範囲を狭くした。また、テレビ会議システム等、グローバル IP アドレスを必要とするサービスを利用するためのネットワークを別途敷設できるように VLAN を導入した。

第 2 にプロキシサーバへの通信集中およびプロキシ未対応のアプリケーションの問題を解決するためにプロキシサーバを撤廃し、各端末が直接インターネットに接続できる構成にした。ただし、プロキシサーバに割り当てていた利用者認証機能は運用上重要な機能のため、新規導入スイッチの Web 認証および MAC 認証機能を活用した。スイッチの標準機能では、複数のネットワークに対して個別の認証サーバを用いたポート認証が不可能であったため、それを可能とする独自の Web アプリケーションも作成し、要求を満たした。

なお、本ネットワーク刷新に必要な機器は平成 24 年の全高専共同調達、および 3 高専共同調達によるものである。今後このような調達の増加が見込まれ、高専に共通のネットワーク機器が導入される可能性が以前より高まるため、本件で取り上げた問題に対する解決方法が他高専にも役立つことを期待して、以下に本校の新ネットワーク構築成果を詳述する。

2. 旧ネットワークの分析

平成 20 年に設計・構築され平成 24 年 9 月まで運用した旧ネットワーク [1]構成概要を**図 1** に示す。1 章でも述べた通り、教職員が教育支援の事務処理目的で利用する事務 LAN と、学生・教員が学習・教育・研究目的で利用する研究 LAN があり、両ネットワークはセキュリティ確保のため物理的・論理的に分離している。特に事務 LAN は成績資料等機密性の高いデータを取り扱うため、無線 LAN 基地局の設置を禁止し、情報コンセントは学生の立ち入れない箇所にのみ設置している。事務 LAN と研究 LAN にはそれぞれインターネット接続性を持つプロキシサーバが設置されており、両 LAN の端末はプロキシサーバに通信を依頼することでインターネット上の資源にアクセスできる。プロキシサーバ経由の対外通信はトラブル時に問題が特定できるようプロキシサーバ内に通信情報を記録している。また、トラブルが起こった際に、その原因となった端末および利用者を特定できるよう、プロキシサーバの利用に至るには認証を要する。事務 LAN は DHCP サーバによる MAC アドレス認証（機器認証）、研究 LAN はプロキシサーバによる ID・パスワード認証（ユーザ認証）によって対応している。尚、ログの保存先や形式がネットワークによって異なるため、管理コストが高い問題がある。他、詳細は後述するが MAC アドレス認証の方が利便性は高いが端末認証のみでユーザ認証はできない。事務 LAN では、端末とユーザがほぼ 1 対 1 対応しており端末の管理が行き届いていることと、ユーザは教職員のため規定を遵守でき分別が効くことから MAC アドレス認証を採用した。研究 LAN は演習室等端末を共有する機会が多く、また管理が行き届かない端末が接続されるため、ユーザ認証を採用している。

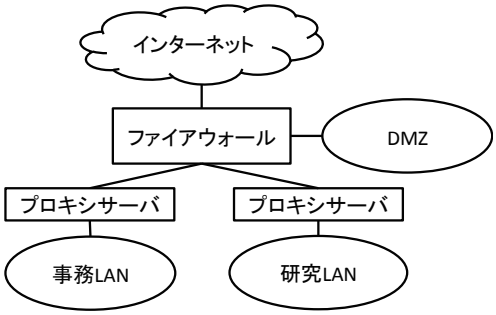

図 1 旧ネットワーク概要

上記ネットワーク構成により、セキュアな教育支援ネットワークが構築できているが、利便性を大きく損なうことを覚悟した設計となっている。以下に、ネットワーク設計時に想定できた問題と、想定外の問題を述べる。

2．1 想定内の問題

各 LAN の端末はプロキシサーバ経由のインターネット接続しか認められないため、プロキシ未対応のネットワークアプリケーションが利用できない。さらに研究 LAN ではアプリケーション毎のユーザ認証を必要とするが、これに対応しないネットワークアプリケーションがある。そのようなアプリケーションの接続先が分かっている場合は、プロキシサーバのホワイトリストに接続先情報を追加することで、例外的にユーザ認証を不要とする措置をとった

が、このホワイトリストの申請・管理労力はネットワークアプリケーションの増加に比例する。特に労力を要したのが、Java プログラムの開発環境である Eclipse のプラグインのインストール・更新である。Eclipse はオープンソースの開発環境で、その上で動作するプラグインもオープンソースであることから、プラグイン毎に開発者が異なり、全てのダウンロード先を列挙してネットワーク管理者に依頼する必要があった。当然ながら開発途中にさらにプラグインを追加することもあり、改めて管理者にホワイトリスト追加要求が必要となる。このような要求が学生からあった場合、教員を通してネットワーク運用者に伝える運用となっており、要求から反映までに時間がかかる。即時性を優先して自宅のネットワークで環境を整備したり、一時的に携帯電話網に接続して対処したりする学生が散見された。

また、プロキシサーバに全インターネット通信が集中するため通信ボトルネックが発生する。プロキシサーバではHTTP以外をサポートしなかったため、導入当初は帯域を消費する UDP 等を用いたストリーミング通信は仕様上利用できないことで無視できたが、Youtube や Skype 等、HTTP によってストリーミング通信するサービスが普及するにつれ、プロキシサーバの負荷が高くなった。

２．２　想定外の問題

H.323 や SIP(Session Initiation Protocol)によるテレビ会議システムは旧ネットワーク設計当初は非常に高価だったため、導入の可能性がなかったが、機器の価格が下がって教員が研究費で購入できるようになったり、法人化後に高専間連携が推進されたりといった背景で、対応せざるを得ない状況になった。テレビ会議システムはグローバルIPを必要とするため、旧ネットワーク構成では対応できず、テレビ会議システム用に個別のネットワークを敷設する必要が出た。

他、無線 LAN の普及により研究 LAN 内で想定外の問題が発生した。情報センター予算では校内を網羅する台数の無線 LAN 基地局を購入できないため、情報センターが状況を把握できない研究室や学寮居室に次々と設置され、現状校内に 100 台近くの無線 LAN 基地局が設置されている。この中で無線ルータの誤接続によるトラブルが度々起こっている。無線ルータはWANポート側から得たIPアドレスをNATして、LAN ポート側に新たなネットワークを作成し、一般的には LAN ポート側に接続された端末は無線ルータ内で稼働するDHCPサーバからIPアドレスを自動取得する。この WAN ポートと LAN ポートの向きを誤接続すると、研究 LAN 全体に非正規の DHCP サービスを行ってしまう。この非正規 DHCP サーバから得られるIPアドレスおよびネットワーク設定情報は研究 LAN のものと異なるため、プロキシサーバや他の重要な研究 LAN 上のサーバにアクセスができなくなり、通信障害をきたす。年に数回の頻度で非正規 DHCP サーバの問題が起こった。研究 LAN は校内全域にフラットに展開されているため、問題を起こしている端末を特定するには労力を要した。このフラット構成は平成 13 年度に設計されたもので当初の規模では妥当なものだった。平成 18 年度には、端末台数が増えたことから（上記問題は想定外）、ネットワーク分割が一度検討されていた。既存・新設機器の組み合わせにおいて DHCP リレーや既存 LAN 内専用サーバのネットワーク超え可否の検証が不十分で、導入時期の異なる L3 スイッチの保守費用が確保できなかったため見送られていた。

他にはスマートフォンの普及により無線 LAN 基地局の接続が増えているが、Android が公開され 5 年が経った現在においてもプロキシ経由の通信に満足に対応していない。Android が繋がらないことで通信ボトルネックの問題に対しては助かっているが、近年の背景を踏まえると著しくサービス性の低いネットワークとなりつつある。

２．３　新ネットワークへの要求

上記の問題を踏まえて、ネットワーク改善要求として以下の項目に整理した。

- **ネットワーク分割**

研究 LAN のような巨大な単一ネットワーク内に問題を持った端末が1台接続されるだけでネットワークが麻痺してしまう現状を鑑み、研究 LAN は学科単位等によって分割する。また、テレビ会議システム等、グローバル IP を必要とする端末が現れた場合、別途ネットワークを敷設する必要があるため、柔軟にネットワーク増に対応できる構成にする。なお、事務 LAN は機密性の高い情報を取り扱うため、今後も物理的には不可能としても論理的には単独のネットワークとして運用する。

- **プロキシサーバの廃止**

プロキシ通信に対応しないアプリケーションの増加を考慮する必要がある。また、通信ボトルネックも解消したい。

3. 新ネットワークの構築

平成 24 年に全高専にてファイアウォールと認証サーバの共同調達、および本校と宇部高専、呉高専でのネットワーク機器共同調達の機会を得たため、前章で挙げた要求を解決するネットワークに刷新した。要求を満たすにあたっては、機器の導入・設定だけでは対応できないものがあったため、一部独自にソフトウェアを開発することになった。

導入したネットワーク機器を**表 1** にまとめる。ファイアウォールには IP アドレスおよびポート単位の静的なフィルタリング機能に加えて、パケットや URL のパターンマッチングによって不正な通信を遮断する UTM と呼ばれる機能が備わっている。UTM 機能はこの他にも添付ファイルのスキャンや、アプリケーション毎の通信制御が可能等、多機能ではあるが、全ての機能を有効にすると 1Gbps のインタフェースにも関わらず 120Mbps 程度のスループットしか出ないことが事前に報告されていたため、本校ではパケットのシグネチャマッチング機能のみ有効にした。サーバ室に収容するコアスイッチには AX3650S を 2 台導入し冗長化によってフェイルオーバに対応する。エッジスイッチには APRESIA 13200 を予備機含めて 11 台導入した。以降、新ネットワークへの要求解決に対する議論と結果を述べる。

3．1　ネットワーク分割による研究 LAN のセキュリティ向上

旧ネットワークではコアスイッチとエッジスイッチの接続のために 4 本の光ファイバを配線し、事務 LAN と研究 LAN の 2 種類のネットワークを 2 本のファイバで冗長化する構成にしていたが、今後、テレビ会議等の要望に応じてネットワークを増やしたい時の配線費用を賄う予算はないことから、新ネットワークでは VLAN を導入した。新ネットワークの概要を**図 2** に示す。図中の JLAN が事務 LAN、KLAN が研究 LAN である。

研究 LAN での非正規 DHCP サーバ問題については、エッジスイッチの下流から上流に流れる DHCPOffer パケットを遮断するように ACL(Access Control List)を設定した。しかし、これは非正規 DHCP サーバ問題に対する個別の対応であり、今後その他の問題の通信によってネットワーク全体に悪影響を及ぼす可能性もあるため、万が一問題が起きた際に被害の範囲を最小限に留める目的

表 1　導入機器

メーカ	製品名	数
FortiGate	FortiGate-300C	1
富士通	UnifIDOne	1
アラクサラネットワークス	AX3650S	2
日立電線	APRESIA 13200	11

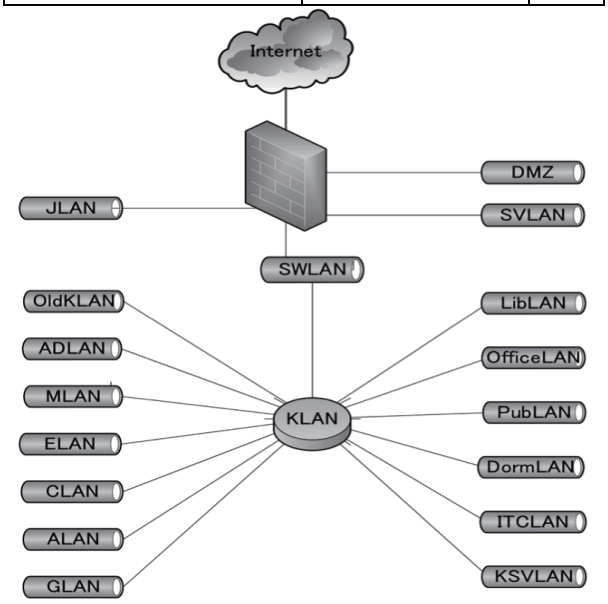

図 2　新ネットワーク概要

で、研究 LAN を 13 のネットワークに分割した。無駄に広範囲にブロードキャストパケットが届かない効果も期待できる。この他に、スイッチ間通信用のスイッチ LAN と、研究 LAN と事務 LAN のどちらからでもアクセスできる校内公開用サーバネットワークである、サーバ LAN を新たに作成した。

3．2　汎用端末での利用者認証

プロキシサーバは不要なインターネット接続性を排除する機能と、利用者を認証し有事の際にトレースバックできる機能を担っていた。

前者についてはセキュリティが十分確保される反面、利便性が著しく低下したため、各ネットワークの端末は NAT 接続することにした。NAT 接続は多くのネットワークアプリケーションで想定されているため利便性の向上が期待できる。ただし、ワームやウィルスに万が一感染した場合にはそれらのソフトウェアの通信も認めることになってしまうため、これらに多用される SMTP 通信についてはポートを遮断した。また、ファイアウォールのアンチウィルス機能を有効にして特定のシグネチャを含む通信もブロックして一定のネットワークセキュリティ性

能は確保している。

利用者認証についてはエッジスイッチのポート認証機能を利用することにした。導入したエッジスイッチは以下の3種類の認証手法に対応している。

・ 802.1X 認証

サプリカント（証明書・ID・パスワード等のサプリカント情報を暗号化通信する認証専用ソフトウェア）を利用して RADIUS によるユーザ認証を行う。Layer2 認証のためアプリケーションに対する汎用性が高く、また暗号化強度も要求に応じて選択できるため時代にあったセキュリティ性能が確保できる。ただし、サプリカントが用意されていない OS では利用できない。さらに、サプリカントとスイッチの相互運用性が実装依存のため、サプリカントが用意されている OS でも利用できない場合がある等、機種に対する汎用性に懸念がある。

・ Web 認証

ブラウザで任意の Web ページにアクセスを試みると、認証 Web アプリケーションにリダイレクトされフォームに入力した ID・パスワードによって RADIUS のユーザ認証をする。802.11X 認証のサプリカントよりもブラウザの方が普及しているため汎用性が高いが、スイッチ毎に実装が異なるため、スイッチの機種あるいは OS を揃えないとインフラ構築コストが高くなる可能性がある。また、プリンタ等のネットワーク周辺機器にはブラウザが搭載されていないため、対応できない。

・ MAC 認証

48 ビットで表現される MAC アドレスが実質グローバルにユニークであることを利用して、MAC アドレスエントリを RADIUS サーバに登録しておくことで、端末の通信開始時に送信元 MAC アドレスを参照して RADIUS 認証する。汎用性が最も高いが、MAC アドレスを書き換えられる機器があるため、認証を通過する MAC アドレスを攻撃者に特定されると認証システムが機能しなくなる。また、あくまで端末を認証するため、共用 PC を利用する場合にはユーザを特定できない問題がある。

本校では汎用性を重視して、利用者認証が可能で汎用性の高い Web 認証を基本としつつも、Web 認証できない端末については MAC 認証を用いることにした。幸い Web 認証できない端末はプリンタや無線 LAN 基地局等、それ自身を操作して問題が起こる可能性が低い端末のため利用者認証が不要だった。事務 LAN を全て MAC 認証にするか、原則 Web 認証にするかを導入間際まで悩んだため、どちらでも対応できる設計とした。従来から MAC 認証は利用終了申請忘れによりエントリが単調増加していたため、導入時には原則 Web 認証を試行したが、苦情が出たため、利便性とセキュリティのバランスを取り、1 人 1MAC アドレスは MAC 認証を認めることにした。

一般的なネットワーク運用では RADIUS サーバは拠点に 1 台の構成となっており、スイッチが収容するどのポート（VLAN 構成のためポートによってネットワークが異なる）に対しても同一の ID/パスワードで利用者認証を行う。しかし、本校では事務 LAN と研究 LAN を物理的・論理的に分離していた背景から、各 LAN に 1 台ずつ認証サーバが存在しており、用途を棲み分けている。

全高専で共同調達した認証サーバ UnifIDOne（LDAP, RADIUS に対応）を、本校では事務 LAN に設置している。研究 LAN の認証サーバは本校で独自に調達した LDAP サーバのため、これを機に全校アカウントの認証サーバを UnifIDOne に統一する案も出たが、事務 LAN を他のネットワークから独立する要求を遵守するとファイアウォールを股がった通信が必要となり、全校の認証に関わる通信が全てファイアウォールを経由することでファイアウォールの負荷が高まることを懸念し、研究 LAN 用の認証サーバに RADIUS サーバ機能を追加した。

導入したスイッチは最大 4 つの認証サーバ情報（認証サーバと認証方法の組み合わせ）を登録することができ、登録した順序でポート認証を試みる。これは本校の要求を満たすにあたって重大な問題となった。事務 LAN を分離したいため、ポート単位で利用する認証サーバ情報を限定したいところだが、スイッチ単位でしか利用する認証サーバ情報が設定できない。従って、事務 LAN のポート認証を行いたいにも関わらず、認証サーバ情報の利用順序の設定によっては研究 LAN の認証サーバに対して認証を試みてしまい、研究 LAN にしかアクセス権を持たないユーザ（主に学生）に対して事務 LAN の利用認証を通してしまう恐れがある。Web 認証ではスイッチに保存できる認証用静的 Web ページによって、どの認証サーバ情報を利用するかをフォームによって選択する（例えば研究 LAN と事務 LAN のどちらを利用するかをラジオボタンやプルダウンメニューで選択する）ことができるが、研究 LAN にしかアクセス権を持たないユーザに事務 LAN の存在を不必要に伝えてしまう結果となる。導入スイッチはこの認証用静的 Web ページの代わりにリダイレクト先として別サーバの URL を設定することができる。すなわち別サーバであれば動的 Web ページによって Web 認証を行えるため、クライアントのソース IP アドレスから適切な利用認証サーバに接続す

る旨、ラジオボタンやプルダウンメニューではなく隠しパラメータ（hidden 値）をスイッチに伝えることによって、研究 LAN から接続された場合には研究 LAN 用の Web 認証フォームを、事務 LAN から接続された場合には事務 LAN 用の Web 認証フォームを動的に作成した。以下にエッジスイッチに設定した認証サーバ情報の利用順序を示す。

1. 事務 LAN 認証サーバによる MAC 認証
2. 研究 LAN 認証サーバによる MAC 認証
3. Web 認証（認証サーバは開発した Web アプリにより自動選択）

研究 LAN に接続した場合も、まず事務 LAN の MAC 認証を試みてしまうが、MAC 認証は MAC アドレスをキーとして RADIUS サーバから通信許可される VLAN ID を受け取り、スイッチに接続されているポートの VLAN ID が一致（実装は事務 LAN であるか否かの判定に簡略化）した場合のみポート認証を通過するため、他のネットワークの MAC 認証は必ず失敗するので、意図しない認証通過は発生しない。その代わり研究 LAN で MAC 認証する端末は事務 LAN の MAC 認証失敗のタイムアウト時間だけ認証に遅延が発生する仕様となっている。

4. 考察と今後の課題

2012 年 9 月から現在まで 1 年弱の運用期間において、2.2 節で取り上げた非正規 DHCP サーバ問題のような、他のノードに悪影響を与える様なトラブルは発生していない。現状、非正規 DHCP サーバのみが起こりえるトラブルのところ、ACL により通信をブロックした効果が出ていると考えられる。また、分割したネットワークも他に干渉することなく運用できている。本校と同様に導入スイッチのポート認証機能を複数ネットワークにて活用する場合には、本稿の報告事項が役立てば幸いである。

また、プロキシを廃止したことで利用できるネットワークアプリケーションの数が増え、学生が積極的に本校のネットワークを利用して学習・研究している様子が確認されている。幸いファイアウォールのウィルス検知機能が反応しない状況が続いているが、利用 PC へのアンチウィルスソフトウェアインストールの徹底により、プロキシを撤廃してもある程度セキュアであることが確認された。特にこれまでトラブルがなかったため、認証ログは活躍していないが、認証ログ自体は適切に蓄積されている。

他、新規ネットワークを VLAN で敷設できるようにした結果、教員が個別所有するテレビ会議システムが現状 2 台、各教員室で稼働しており、支障なく利用できている。

研究 LAN と事務 LAN の利用認証をスイッチのポート認証で統合することの導入コストは高かったが、ログが認証サーバに統一形式で保存されるため、ログの管理コストは軽減した。とはいえ、2 台の認証サーバを運用している点について改善の余地がある。ファイアウォールの統計を見る限り輻輳が発生しておらず帯域に余裕があるため、認証パケットがファイアウォールを通過しても通信のボトルネックになる可能性は低い。今後、全国高専にて国立情報学研究所（NII）が推進している学認[注 1)]への積極的参加が見込まれており、その際には校内の認証サーバを Shibboleth IdP に対応させる必要性が出てくる。UnifIDOne は Shibboleth IdP 対応方法がマニュアル化されておりほぼ追加コストなしに導入が可能である。本校においても UnifIDOne の 1 台のみで校内の認証機能を賄うか、2 台の認証サーバのどちらにも問い合わせをする Shibboleth IdP ラッパを設置するかについて今後検討する必要がある。

5. おわりに

教育支援を主目的とする明石高専のネットワークは、従来においてはセキュリティ性能を重視し、事務 LAN と研究 LAN を物理的・論理的に分離していた。それらネットワーク下の端末はプロキシサーバ経由のみのインターネット接続が提供されており、利用できるネットワークアプリケーションの種類に大きな制約があった。利便性を向上させるために、平成 24 年度のネットワーク機器刷新に伴いプロキシサーバを廃止しつつも Web 認証と MAC 認証の併用により、従来と比べてセキュリティ性能の低下を最小限に抑えたネットワークの構築を達成した。今後は本校の認証サーバに Shibboleth IdP 機能を追加するにあたって、複数の手法を提案し、それらの長短を整理し導入を進めたい。

参考文献

1) 佐村敏治他：セキュリティを考慮した教育支援ネットワークサーバーシステム，論文集「高専教育」，第 32 号，pp.871-876(2009)

注記

注1) 学認： http://www.gakunin.jp/ (2013/5/31)