寄 稿

新キャンパスネットワーク
―快適な利用環境とセキュリティの強化―

福井恵子，鵜川義弘，平井清巳，安藤明伸，小野元久
宮城教育大学 情報処理センター

1. はじめに

宮城教育大学のキャンパスネットワークは、メインの青葉山地区と附属校園のある上杉地区および学生寮のある水の森地区という３つのキャンパスネットワークで構成されている。そこには１日1600 台以上の機器が接続され、教員、事務職員、学生が 24 時間 365 日利用している。

青葉山キャンパスネットワークは平成 14 年、市販の回線使用料なしに利用できるよう東北大敷地まで光ファイバーを埋設することで自営線化し、TOPIC（東北学術研究インターネットコミュニティ）に 1 Gbps で接続した。SINET（学術情報ネットワーク）には TOPIC 経由で接続している。

平成 16 年に上杉地区、平成 19 年には水の森地区が市販の光通信により 100Mbps でインターネットに接続された。さらに VPN(仮想専用網) ルータを使い飛び地にもかかわらずあたかも学内ネットワークに接続されているよう運用されている。ただ、建屋内の配線や設備は、平成 11 年３月の補正予算により整備されたものであり、このとき導入された機器は旧型ゆえ保守部品も調達できずにいた。

基幹ネットワークが５年を経るころには、故障頻度が高まったため、重要な建物間のネットワーク接続については、リース機器により保守ができる体制にしたが、建物内の配線については、手がつけられない状態にあった。

また、平成 14 年３月の自営線化に伴い導入された無線ＬＡＮ設備は、必ずしも全キャンパスでの利用を計画したものではなく、昨今の利用要求の高まりに応えられない状況であった。

2. ネットワークの更新

そこで、平成 21 年度のキャンパスネットワーク更新は、老朽化した機器・配線を置き換え高速化するとともに、キャンパス全体での無線ＬＡＮの利用を可能とし、最新で高速な情報基盤を維持することを導入の目的とした。工事内容は建屋 HUB からの各フロア HUB の更改と老朽化した配線の張替、および無線 LAN のアクセスポイントの増強であった。また、管理面では、頻発するネットワークのトラブルに対応できるよう、ネットワーク管理システムを導入することであった。(図１)。

この更新契約時には政権交代があり政府調達が一時停止されたため、教授会でのアナウンスが遅れ、入室を伴う重要な工事の案内が紙でしか届けられなかった。工事期間中には、業者の入室に伴うクレームが数多くあがったが、これらは情報処理センターと利用者との情報共有が充分ではなかったことが要因であり、大きな反省となった。

3. 利用環境－ギガビット化－

新ネットワークは主な建物内のハブと屋内配線を Cat 6 の規格とし、メインスイッチ 33 台、フロアスイッチ 162 台を導入し、ギガビット化し

た。ただ従来より光ファイバを引いていない場所は、電話線を使った vDSL で接続を継続しているため、スピードは理論値最大で 100Mbps、ノイズ等の影響で、30 ～ 40Mbps 程度である。

なお、ギガビットの速度や安定性を享受するには次の環境が必要であるので、留意されたい。

［利用環境の留意点］----------

1. PC 本体のインターフェイスがギガビットに対応したものであること。
2. 壁コンセントから PC までの配線を Cat5e または、Cat6 にすること。
3. 途中にハブがある場合にはそのハブもギガビット化する必要があること。

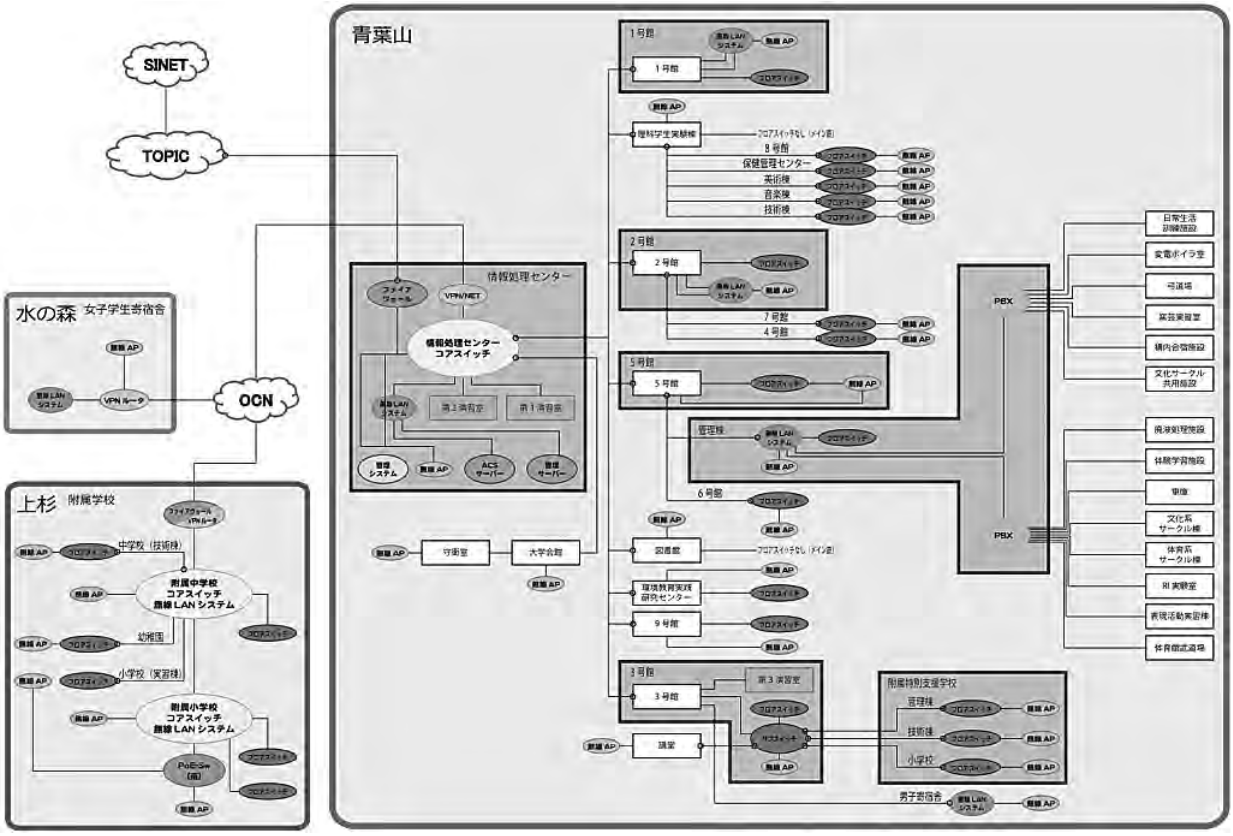

図１：新キャンパスネットワーク概念図

4. 利用環境－全学無線 LAN －

屋内全域をカバーできるよう無線 LAN アクセスポイント 202 台、集中コントローラ 8 台を導入し、WPA2-PSK と WPA2-Enterprise という２つの認証方法で提供している。

4.1 WPA2-PSK

学生や教職員が学内の様々なところで使うために WPA2-PSK の提供を開始した。これは今までの無線 LAN へ接続する時の認証方式より強力な WPA2 (Wi-Fi Protected Access2) を用い、PSK (Pre Shared Key= 事前に共通で使うよう周知したパスワード) で使う方法である。

PSK はユーザへの周知が必要なため急には変更できない。2010 年 4 月から 10 月の並行運用期間を設けて切り替えを行った。

無線 LAN アクセスポイントに接続後は、利用資格を持つ者であることを確認するため、従来どおり Internet Explorer 等の Web ブラウザを起動し Web ページで、認証を行ってから利用する方式である。

［利用手順］----------

1. SSID:miyakyo-u を選択する

2. AccessKey:＜センターへ問い合わせ＞を入力
3. 接続後は次の URL へアクセスする
　http://dhcp.miyakyo-u.ac.jp/
4. 本学でのユーザ名とパスワードにより認証を受ける

なお、今回の認証方法の変更により、旧型の無線 LAN アダプタの製品が WPA2 方式に対応しておらず、ドライバの更新が必要であった。

4.2 WPA2-Enterprise

今後提供するのは、主に教職員が使う接続で、使用開始時に Web 認証を行わずとも利用ができるよう学内の認証システムと連携するものである。

附属学校がある上杉地区では既に運用されている方法だが、青葉山地区においては、LDAP サーバ(ユーザパスワードを一元管理しているサーバ)との相性が悪く遅れていた。現在では LDAP サーバとのやり取りに、EAP-FAST という技術を用いることで解消できることが分かっているので、今後は早い時期に WPA2-Enterprise 専用の SSID を提供する予定である。

このネットワークへのアクセスは、MacOS や iOS の新バージョン OS ならば EAP-FAST が標準対応なので、すぐに利用できるが、Windows 端末は未対応のため、無線 LAN アダプタのメーカーが提供するサプリカントソフトまたは、フリーの Windows 用サプリカントを使うことになる。現在、この提供ソフトを模索･検証中である。

将来的には、UPKI（大学間連携のための全国共同電子認証基盤）により職員や学生にユーザー証明書が発行されれば、証明書を利用した EAP-TLS（通信の暗号化のもと、相互認証するもの）による認証が利用可能となり、さらなるセキュリティの向上が望める。

5. セキュリティ強化－侵入防御システム－

ファイアウォール(IPS 付き) 3 台、VPN ルータ 3 台，認証用ルータ 1 台を導入し、侵入防御システム（Intrusion Prevention System）を含むシステムを導入することで、悪意のある通信を検知し必要な場合には自動的に遮断するなど、きめ細かな防御が可能となった。現在は次のような脅威を想定のうえ設定し、防御している。(図 2)

- 辞書にある単語を使って次々とログインを試みる攻撃。
- ウイルスに感染したパソコンが指令をもらうのに使う IRC 通信。
- Web ページの改ざんを目的とした SQL 注入攻撃。
- Web ページからのパスワード等のシステム情報を搾取する攻撃。
- 違法なファイル転送に用いられる P2P 通信。

誤検知防止のため学内から学外向けの場合は通知のみとし、管理者が精査してポリシーチューニングの参考としている。教室や寮などからの学生利用については、例外扱いとし自動で遮断 30 分後に再開を繰り返す設定になっており、このような通信があった場合には、管理者に電子メールで通知が届くようになっている。

図 2 ：IPS グラフィカル管理画面

6. セキュリティ強化－端末管理システム－

本学で学内全体の管理システムとして導入した NetSkateKoban はネットワークに接続された端

末を MAC Address ベースで識別し現在と過去の端末接続履歴を管理できる端末管理システムである。(図３)

このシステムは、不正利用や IP アドレスの競合があった場合に現在だけでなく過去にさかのぼって利用者を特定したり、事案の発生状況を確認するためのものである。

また、無線 LAN 管理システム (Wireless Control System) と連携させることで、端末がどの無線アクセスポイントに接続されているか特定できるようにもなり、先の侵入防御システムからの情報と合わせてより詳しい情報が取得可能となった（図４)。

IPS および NetSkateKoban と WCS、各システムの利点を連携させたことでセキュリティ強化につながった。

図３：NetskateKoban セキュリティ管理システム

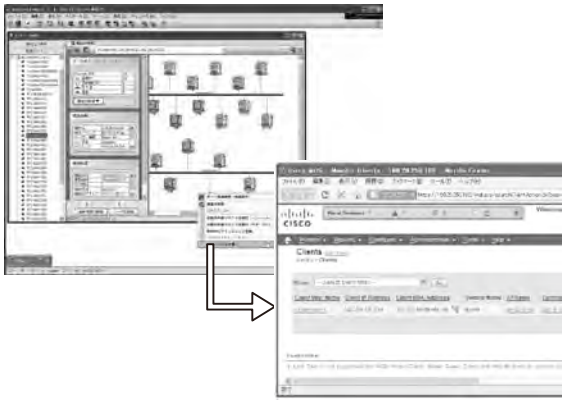

図４：NetskateKoban と
WirelessControlSystem との連携

7. 今後の課題

今後は、WPA2-Enterprise の早急な運用開始とともに、整備されたキャンパス無線 LAN を国内外の他機関の無線 LAN と接続して相互利用できるようにすることである。

このため、SINET の直接接続組織として加入し、国立情報学研究所と UPKI 構築事業による国際無線 LAN ローミング基盤 eduroamJP に参加した。Eduroam とは教育機関ごとの無線 LAN システムを相互接続し、認証連携技術により、利用者が所属機関のアカウントを使って他機関の無線 LAN インフラを利用できる国際的な仕組みである[3]。最近では商用無線 LAN サービスとの連携も進められており、キャンパスの垣根を超えた利用の可能性が広がる。この Eduroam を活かして教職員や学生が他の教育・研究機関間を移動しても現地で自由なネットワークが利用できるよう、本学での手続きなど早急に整備して利用者に提供することを目指したい。

参考文献

[1] Cisco IPS
http://www.cisco.com/web/JP/solution/netsol/security/literature/ipssol_ds.html

[2] NetSkateKoban http://www.cysol.co.jp/products/netskatekoban/

[3] 後藤英昭、曽根秀昭「eduroam による大学間無線 LAN 連携と国内外の動向」
http://www.eduroam.jp/docs/eduroam-JP-flyer10.pdf

[4] 後藤英昭、曽根秀昭「大学間無線 LAN ローミング基盤 eduroam の動向と容易な導入方法」情報処理教育研究集会 (2010)

[5] 福井恵子、鵜川義弘、平井清巳、安藤明伸、小野元久「全学 LAN 張替＆全学無線 LAN ＆端末監視」情報処理教育研究集会 (2010)