校内LANシステム更新

The Renewal of the Local Area Network System

和賀　宗仙・北村　早苗*・島村　浩**・小泉康一***・大槻　正伸***
福島工業高等専門学校モノづくり教育研究支援センター
*図書館スタッフ株式会社
**福島工業高等専門学校コミュニケーション情報学科
***福島工業高等専門学校電気工学科
Toshinori Waga, Sanae Kitamura, Hiroshi Shimamura*, Koichi Koizumi**, Masanobu Ohtsuki**
Fukushima National College of Technology , Manufacturing Support Center for Education and Research
*Fukushima National College of Technology, Department of Communication and Information Science
**Fukushima National College of Technology , Department of Electrical Engineering
（2013年9月17日受理）

FNCT Local Area Network (henceforth LAN) was replaced in October 2012. The replacement includes not only network switches and wireless access points but also several servers. The network servers are virtualized. iNetSec smart Finder was introduced so that all computers and devices are authenticated by MAC address. On the other hand, connecting wireless LAN has become more complicated compared to the old network. In this paper, we explain the explicit specification of the new network and the operational changes in the new network system.

Key words:　LAN, network

1. はじめに

福島高専では平成24年10月に校内ＬＡＮの機器更新を行った。各種サーバ類も更新対象である。これまで、サーバ群の管理に関しては以下にあげる問題点があった。

・１２台ものタワー側サーバが３段のラックに敷き詰められており、サーバ室内でもかなりのスペースを占めていた(Fig. 1)。

・www（WEBサーバー）はXOOPSのアップデート等重要な作業を行う際、仮想化していないので長時間かけてOS全体のバックアップをとる必要がある。

・メールサーバは本校で自力で構築したものであるが、トラブル時に頼れる保守業者がいない。メールは大変重要なサービスであるため、構築からトラブル対応までしてくれる保守業者が必要である。

・ＤＮＳ（これも自力で構築）、シスログサーバは小規模演習室である画像処理演習室にあったWindows 2000時代の古いＰＣを使いまわしたものであり、しばしばハードディスク故障をしてはAcronis True Imageで復旧をしていた。

これらの一般的なネットワークサーバは業者に構築を行ってもらい、安定動作を保障してもらうことが望ましい。仮想化による省スペース化、サーバリソースの効率利用も今回の機器更新の大きな目的である。

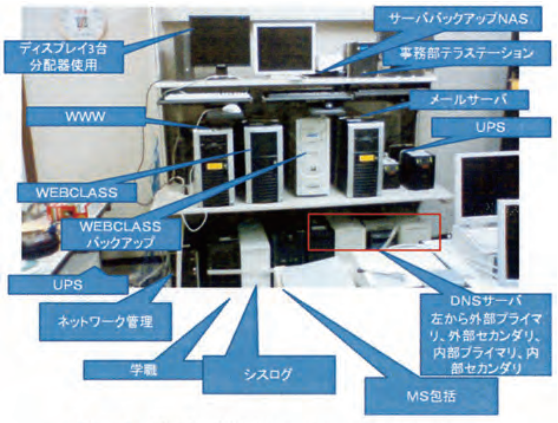


Fig. 1 機器更新前のサーバラック

この機器更新は各高専が仕様を決める個別調達によるものであるが、同時に一括調達（全国高専統一の機器が調達される）によるファイアウォールの入れ替えもされた。なお、認証サーバは既に平成２４年３月５日に一括調達により導入されている。

2. 更新仕様

2.1 ネットワークスイッチ

ネットワーク機器更新後のネットワーク構成図をAppendix.に示す。

更新後のネットワークスイッチは、コアスイッチ(L3)がCISCO Catalyst 3750X、エッジスイッチがFUJITSU SR-S348TC1に全て入れ替えられた。その中でも磐陽寮、モノづくり教育研究支援センター、第一体育館、第二体育館は更新前はSummitやアライドテレシス製の古いスイッチ類であり、各部屋との通信速度が100Mbpsあるいは10Mbpsのものであった。これ以外のエッジスイッチは更新以前はCISCO 2960で構成されており、1Gbpsであったが、平成２９年６月にサポート終了[1)]であるため入れ替えた。これでエッジスイッチの各ポートまでは1Gbpsの通信速度が保証されるが、第二体育館から熱実験室、寮スイッチからは同軸ケーブルで敷かれている箇所があり、そこの通信速度は10Mbpsである。また、コミュニケーション情報学科棟では、エッジスイッチから各部屋の情報コンセントへの配線が一部４芯になっており、100Mbpsまでしか通信速度を持てない。したがって、学内同士の通信において学内全体に1Gbpsを保証するまでには至っていない。

ファイアウォールは一括調達によりFortigate 300Cに入れ替えられた。

2.2 サーバの仮想化

ネットワークサーバは仮想化され、Table.1のようにリソース配分されている。サーバ本体はFUJITSU PRIMEQUEST 1400S2であり、CPUは1.86GHzである。Fig.2は現在のサーバラックであり、左側が今回導入されたサーバラック、右側は情報演習室のものである。Fig.1に比べると省スペース化されていることがわかる。また、無停電電源装置(UPS)と連動し、停電時にはUPSに接続されているサーバのOSに指令を出し、自動で安全にシャットダウンしてくれる(以前はUPSのバッテリーが切れる前に我々が手動でOSをシャットダウンしなければならなかった)。

なお、WEBサーバはautomysqlbackupにより自動的にデータベースを定期バックアップし、rsyncコマンドにて毎日サイトのソースプログラムと一緒にバックアップサーバに同期している。これでOS障害によりサーバを起動できず、再構築することになっても、バックアップサーバからソースとデータベースを復旧でき、サイト復旧も迅速に行える。WEBサーバは学内限定サイト用のものをもう１台別に立て、卒業論文サイトはそこに置くようにした。メールサーバーは、DMZに転送専用のサーバー、内部にスプール用サーバーを立てることでセキュリティを確保した。また、内部メールサーバーにはWEBメール用に「ROUNDCUBE」と「squirrelmail」をインストールしてある。

ただし、WEBCLASSや学職サーバのようにマシン購入から構築まで業者が関わっているものは仮想化せずそのまま残した(Fig.3)。これらのサーバの電源コードは、差込口の手前で輪を結び、地震時に抜けにくくした(Fig.4)。

Table. 1 仮想化サーバのリソース配分

サーバ名	CPUコア数	メモリ(GB)	消費HDD(約GB)
外部WEB	2	8	200
外部DNSプライマリ	1	2	100
外部DNSセカンダリ	1	2	100
内部DNSプライマリ&内部WEB	1	2	200
内部DNSセカンダリ&メール	1	2	350
DHCP	1	4	150
syslog	1	2	100

Fig. 2 更新後のサーバラック

Fig. 3 仮想化しなかったサーバ

Fig. 4 電源コードの結び方

コミュニケーション情報学科棟では、エッジスイッチから部屋への配線が一部４芯になっており、100Mbpsまでしか出せない。平成30年度までには８芯になるよう工事が必要である。

2.3 無線ＬＡＮ

無線ＬＡＮアクセスポイントはFUJITSU SR-M20AP1にすべて入れ替えられ、全教室、各棟コモンスペース、大会議室、コミュニケーション情報学科棟５Ｆの共同教員室、視聴覚室、体育館、実験室で計47台配置された。

SSIDは教職員と学生用、ゲスト用のものがあり、教職員用はステルス(PC上にSSIDが一覧表示されない)になっている。

教職員用と学生用で用いられるセキュリティ方式はWPA2エンタープライズであり、IDパスワードは情報演習室のActive Directoryと連携している。学生用のSSIDで接続したときには、事務系VLAN上にあるサーバと高専共通システム（Web給与明細システム、旅費システム、KOALA・ザイトスシステム、財務会計システム）にはアクセスできないようにしている。

もう一つゲスト用のSSID（セキュリティ方式はWEP方式）があり、図書館、情報センター、体育館に設けてある。このSSIDで接続されたPCは学外上のPCと同じ扱いとなり、事務部サーバ、高専共通システムはもちろん、学内限定サーバには一切アクセスできない。

しかしながら、以前使っていたCISCO Aironet1000シリーズ、1130AGに比べ電波強度は著しく弱くなった。物理実験室、体育館、情報センター、サーバ室には外付けアンテナをつけて増幅している。

現在のアクセスポイントにはＬＡＮケーブルを差し込むポートが２つある。１つは部屋の情報コンセントにつなぐが、もう１つのポートを利用して部屋内に無線ＬＡＮと有線ＬＡＮを混在させることが可能である。ただし、有線と無線のVLANを混在させることになるので、エッジスイッチ側にはタグVLANによる特別な設定が必要である。

また、教職員用と学生用のWPA2エンタープライズ方式によるPCの接続設定は更新前のWEP方式と比べ難しくて覚えにくい。そこで、Windows 7,8では自動的にSSIDの設定をしてくれるexe形式のプログラムを作ったが、多くのセキュリティソフトで脅威としてみなされ、自動削除されてしまった。この問題は後にWindows 2008 ServerマシンにWindows SDKをインストールし[2)]、makecert,signtool signwizardによるファイル署名を施すことで解決された。学生用の設定プログラムは学内SNSからダウンロードできるようにしてある（Fig.5）。

Fig. 5 無線LAN設定プログラムのアナウンス

2.4 MACアドレス認証の導入

これまでは各教職員に所定のエクセルファイル

に各自が管理しているコンピュータのＭＡＣアドレス、IPアドレス一覧を送ってもらい、情報センターで帳簿管理していたが、人事異動が頻繁にあるため最新のデータを保持することが難しかった。また、IPアドレスは各学科の情報センター運営委員に管理を任せているが、しばしばデータの食い違いが生じてIPアドレスの衝突が起こり、衝突相手を突き止めるのに苦労していた。

今回の機器更新でiNetSec Smart Finderという機器管理アプライアンスを導入した。はじめて本校ＬＡＮに接続する情報端末上では、IPアドレスやWi-Fiなどの適切なネットワーク設定が完了した後の初回ブラウザ起動時に、ブラウザ画面にＬＡＮ接続申請画面が現れる(Fig. 6)。そこに必要事項を記入して申請する。無銭ＬＡＮの場合は情報センター管理者が承認操作をすると該当端末がネットワークを利用できるようになる。有線の場合は申請と同時に自動承認される。ここで、iNetSec Smart Finderは可能な限り接続機器の種類判別も行い、PCやスマートフォン以外のブラウザを持たないネットワーク機器、例えばプリンタなどの場合は自動的に承認するようにしている。しかし、まれに判別のつかない機器もあるため、その場合には該当機器まで情報センタースタッフが行き、ＭＡＣアドレスを確かめる。許可が下りていない機器でも接続した機器のＭＡＣアドレスはiNetSec Smart Finder管理サイト上に表示されるので、これを手動で承認操作する。接続機器の一覧画面にはIPアドレスも表示されるので、IPアドレスの空き状況を把握しやすくなった。

Fig. 6に示すとおり、有線と無線では入力する項目内容が異なる。無線ＬＡＮではセキュリティソフトをきちんと導入しているかを重点的に見て承認を行う。Androidも必須とした。Macintosh, iOS端末は不要とした。Windows 8はMicrosoft Security Essentialsと同等のセキュリティ機能をもつと謳われているので必須でないとした。Windows 7以前に関しては個人PCにはMicrosoft Security Essentials、学校所有PCにはSystem Center Endpoint Protection(SCEP)を推奨しており、それ以外のフリーのセキュリティソフトは認めないこととしている。SCEPは2012年12月より、マイクロソフト包括ライセンスに含まれるようになった。これまで利用してきたMcAfee SaaS Endpoint Protectionは2013年9月末に契約満了となるまで、平成25年度後期までに学内のすべてのPCのセキュリティソフトを完全に切り替える。

有線の場合にはPC設置場所を入力してもらうことにしている。情報コンセントには番号シールがはっていない箇所もある場合や、施設管理係の所持する図面と番号が異なる場合があるので、これまではエッジスイッチのログだけでは場所を把握しにくかったが、今後はネットワークトラブル時には、iNetSec Smart Finderの管理画面からトラブル発生個所を特定しやすくなる。

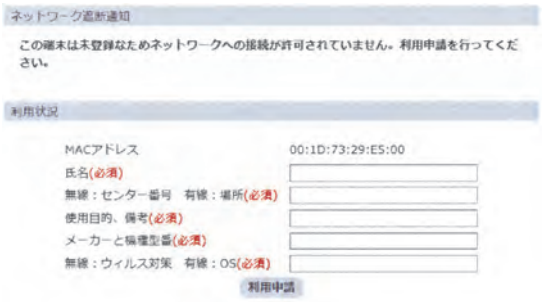


Fig. 6 iNetSec接続申請画面

2.5 VPN

一括調達で提供されているファイアウォールFortigate 300Cのほかにもう１台、下位機種のFortigate 100Dを個別調達にて導入している。300Cが故障したときの予備であるとともに、VPN機能[3)]を100Dで動作させようとしている。

現在でも、業者構築によるサーバには業者の事業所の固定IPから指定ポートによる接続をファイアウォールポリシーで許可しているが、固定IPアドレスを持たない業者には対応できない。固定IPでも、接続元の事業所の規模が大きい場合には、事業所内の誰もがサーバにアクセスできてしまうことも問題である。色々な場所から研究室のサーバに接続したい教員のために、任意のIPからのSSH接続を許可することはセキュリティ上大変危険である。また、学外からのwebmailを使わせるためには、任意のIPからのメールサーバへのHTTPSアクセスを許可せざるを得ず、セキュリティ上の観点から現実的に無理である。そのため、学外からメールを読みたい教職員は各自の設定によりフリーのウェブメールアド

レスや携帯アドレスに転送をかけているが、大変好ましくない。

したがって、webmail、サーバメンテナンスはVPN接続にて行わせるよう準備中である。準備には、

- VPNの利用を希望する教職員へのユーザアカウント発行
- ユーザアカウントごとのポリシー設定
- 各OSのVPNクライアントソフトの入手

をすることになる。多くのユーザはwebmailのみを使うことになるので、メールサーバへのHTTPS接続のみを許可するようユーザをグループ化する。サーバをメンテナンスしたいユーザはそのグループから外し、接続したいサーバへのSSH接続など、必要なプロトコル通信の許可をする。クライアントソフトのダウンロードはネットワーク保守業者が所持するCisco IDが必要であり、後日業者にダウンロードしたソフトを提供してもらう予定である。

なお、作成されたユーザのIDパスワードは、教職員に関しては一括調達による認証サーバに既に連動させている。メンテナンス業者に対しては認証サーバにそのユーザが存在しないので、高専機構本部の策定したパスワードポリシーを満たすようにFortigate 100D側にアカウントを作成する。

加えて、VPN接続でも高専共通システムへのアクセスは禁止する考えである。

3. 補足

3.1 メールセキュリティアプライアンス

平成１９年度にメールセキュリティアプライアンスCisco製IronPort[4]を導入してから、スパムメールはほぼ完全に届いてこなくなり、大変評判がよいため、現在も継続利用している。

IronPort、Fortigate（現在使っているファイアウォール）とも、AntiSPAMとAntiVirus機能をもっているが、FortigateのAntiSPAMはIronPortに比べると性能が悪いと聞き、IronPort側にAntiSPAMをさせ、Fortigate側にはAntiVirusのみをさせることにした。

3.2 ウェブフィルタ

Fortigate 300Cにはウェブフィルタの機能があり、現在は

- 違法性、犯罪性の高いサイト
- セキュリティ上問題のあるサイト
- 市民運動団体、ギャンブル、アルコール、タバコを除くアダルト成人コンテンツ

を学内ＬＡＮで見られないようブロックしている。「問題のないサイトなのに見られない」という苦情がきた場合には、技術職員の持つiPhone5で、3G回線で一度そのページをチェックし、問題がないと判断した場合にはホワイトリストとしてオーバーライドしている。また、行政機関の注意喚起等で、マルウェアのダウンロード元などのセキュリティ上危険なサイト情報が通達された場合にはブロックリストとしてそのURLを書き込んでいる。

3.3 アプリケーションコントロール

WinnyのようなP2P通信[5]を伴うファイル交換ソフトはウィルス感染の原因となる悪名高いソフトであり、利用を阻止しなければならない。Fortigate 300Cにはアプリケーションコントロール機能があり、校内で利用するアプリケーションに制限をかけることが可能である。ここではP2P通信を伴うアプリケーションをブロックしているが、例外設定としてSkypeとEzpeerは利用できるようにしている。Ezpeerは産学連携コーディネータ室で動いているWEB会議システムの内部で動作しているアプリケーションであり、これを禁止するとWEB会議ができなくなるためである。今後、スマートフォンの普及に伴い、Skype以外にも様々な通話ソフトが出現することから、このような例外設定をしつつ一般的なP2Pソフトはブロックしていくことになる。

参 考 文 献

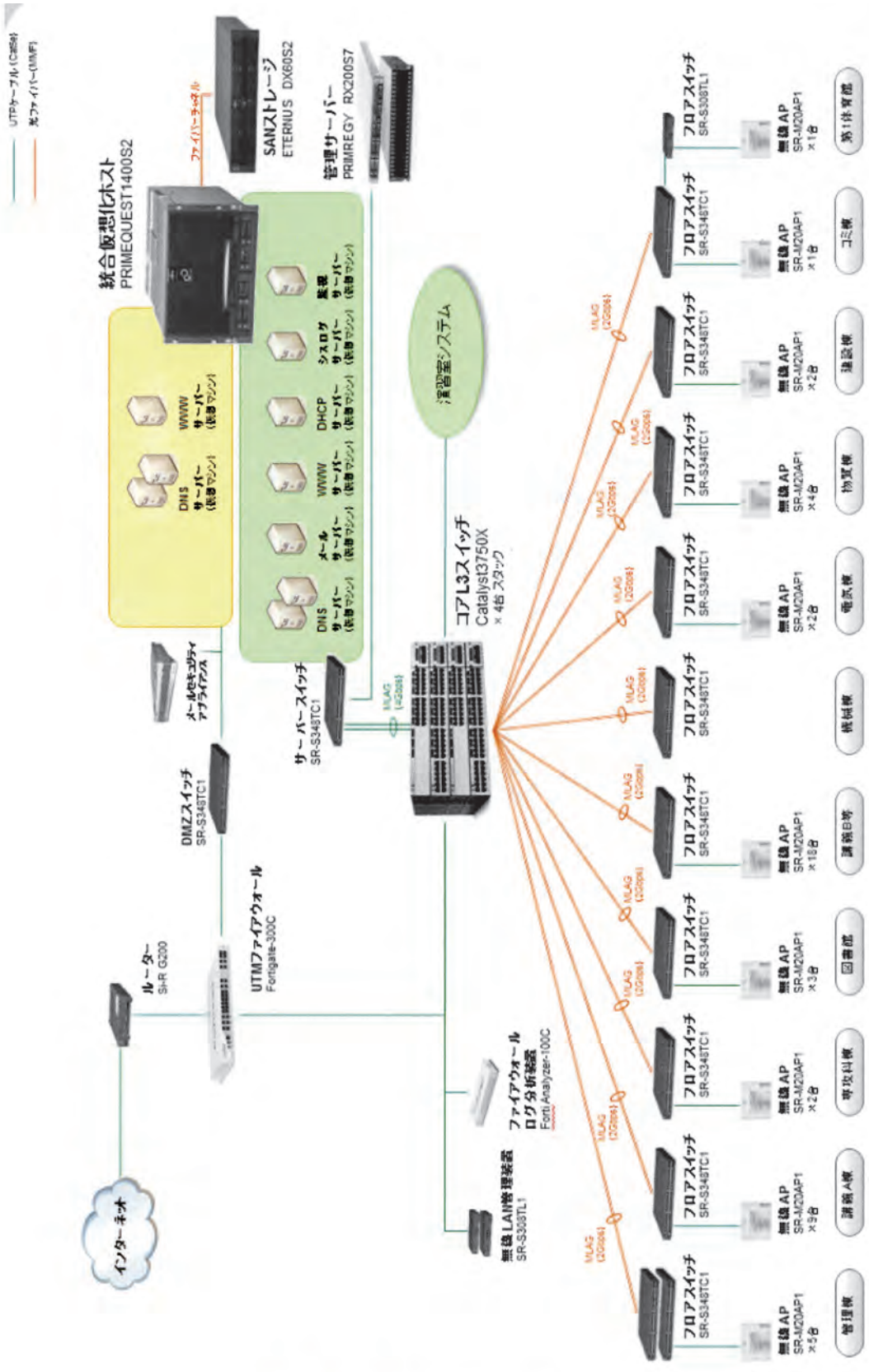
1) http://www.technovan.co.jp/products/switch/eos_sw.html

2) http://www.microsoft.com/en-us/download/details.aspx?id=11310

3) http://www.furukawa.co.jp/network/vpn/about_vpn/about_vpn_top.html#08

4) http://www.cisco.com/web/JP/product/hs/security/IPmail/prodlit/pdf/data_sheet_c78-694035.pdf

5) http://e-words.jp/w/E38395E382A1E382A4E383ABE4BAA4E68F9BE382BDE38395E38388.html



Appendix. ネットワーク構成図

福島高専研究紀要第54号「校内LANシステム更新」についての訂正

昨年発行の「福島高専研究紀要第54号」に掲載の論文「校内LANシステム更新（和賀宗仙・北村早苗・島村浩・小泉康一・大槻正伸著）」に誤りがありましたので、下記の通り訂正します。

p155　右の段　上から7行目

（誤）

現在のアクセスポイントにはＬＡＮケーブルを差し込むポートが２つある。１つは部屋の情報コンセントにつなぐが、もう１つのポートを利用して部屋内に無線ＬＡＮと有線ＬＡＮを混在させることが可能である。ただし、有線と無線のVLANを混在させることになるので、エッジスイッチ側にはタグVLANによる特別な設定が必要である。

（正）

アクセスポイントにはパケット中継機能がないことがわかり、ＬＡＮケーブルを差し込むポートが２つあるのは、エッジスイッチとの接続を２重化できるようにするためでした。実際には片方だけのポートが使われており、エッジスイッチとの接続は２重化しておりません。ただし、エッジスイッチ側にタグVLAN設定をし、アクセスポイントの前段にハブを仲介させることにより、アクセスポイントを置いている部屋で有線と無線を混在させることが可能です。