天久保地区における学内ネットワークの安全性・安定性の向上

筑波技術大学　情報処理通信センター（天久保地区）[1)]　副情報処理通信センター長[2)]

浅草肇[1)]　西岡知之[1)]　北川博[2)]

要旨：天久保地区学内 LAN について，平成 14 年度以降の主たる事業として，① 無線 LAN の敷設とネットワークセキュリティの向上，② サーバ機の増強、③ 対外接続回線の高速化などを行った結果，一層の安全・安定した高機動性のネットワークサービスが提供可能となったことの報告である。

キーワード：無線 LAN，ネットワークセキュリティ，認証，DNS，対外接続

1. はじめに

本学学内 LAN は，筑波技術短期大学当時の平成 6 年 3 月に 10Mbps の回線速度で運用が開始され，平成 13 年 11 月に基幹 1Gbps，末端 100Mbps の回線速度に改装され，運用されてきたものである。この間の変遷の詳細については，文献 [1] [2] に示されている。

その後，表 1，表 2 に示されるように，サーバの増強，安全性（ネットワークセキュリティー）の強化，無線 LAN の導入などがなされた。平成 17 年 10 月の筑波技術大学発足に伴い，学内 LAN についても，筑波技術大学情報処理通信センターがその運用主体となり，継続的に運用を行っているところである。

この報告では，この組織替えによる区別をせず，文献 [2] 以降から平成 18 年 10 月までの天久保地区での整備状況について一体的に述べる。

この期間，ネットワーク通信に関して新たな問題として提起されたものがネットワークセキュリティーである。平成 13 年 11 月から運用を開始した，現『新高速ネットワークシステム』は，DHCP（Dynamic Host Configuration Protocol）を導入し，「いつでも」，「どこでも」，「同じ環境で」を目標に 1990 年代半ばに設計されたものである。いわば「ユビキタス」環境を先取りした設計であった。設計当時，サーバ単体の安全性には充分な対処を行っていた。しかし，ネットワーク全体に対する安全性の概念はなく，導入当初のネットワークシステムは，当然，ネットワークセキュリティーに関しては，非常に脆弱な構造であった。

このため，導入後の情報処理通信センター（天久保地区）（以下，「センター」という。）の整備基本方針は，ネットワークセキュリティーの脆弱性の克服と，より一層の「ユビキタス」環境の構築と定められた。

2. 無線 LAN ネットワークシステムの整備

2.1 整備方針

平成 14 年頃から，無線 LAN アクセスポイント（以下，AP という）の低価格化に伴い，天久保地区内にも個人研究費等で設置された機器が散見されるようになり，将来的には，AP の学内普及が進むものと予想された。しかし，これらの中には，全く安全対策がなされていない AP が存在した。

AP が有線のネットワーク機器類と根本的に異なる点は，

表 1　学内 LAN の変遷（無線 LAN を除く）

平成14年3月	教員用メールサーバ運用開始
平成16年3月	副 DNS サーバシステム運用開始
平成16年6月	ネットワーク認証サーバ運用開始
平成17年1月	学生寄宿舎(天久保地区)に ネットワーク認証システム導入
平成17年10月	非常勤講師宿泊棟等に ネットワーク認証システム導入
平成18年2月	対外接続：100Mbps
平成18年4月	産業技術学部学生用メールサーバ 運用開始
平成18年5月	主 DNS サーバシステム運用開始

表 2　無線 LAN アクセスポイント設置歴

設置日	設置場所等	設置数	規格
平成15年3月	大会議室 多目的会議室(当時)	3台	802. 11b
平成15年12月	講堂，管理棟２階廊下	2台	802. 11g
平成16年2月	多目的会議室廃止に伴い 校舎棟5階講義室に移設	1台	802. 11b
平成16年7月	情報処理通信センター ネットワーク利用室	1台	802. 11g
平成17年1月	校舎棟北側1, 2, 3, 4, 6階	5台	802. 11g
平成17年1月	学生寄宿舎共用棟	1台	802. 11g
平成17年9月	校舎棟中央部，南側 4, 5, 6階	6台	802. 11g

無線であるがゆえに，その接続状況が目視により確認できないことである。充分な安全・管理対策がなされていないAPでは，学外者に無断で接続された上に，さらに，不正なネットワーク使用に利用される可能性を否定できない。また，電波傍受による通信内容漏洩の危険性も伴う。センターでは，これらの対策として，

① センター事業として，充分な安全・管理対策がなされたAPを積極的に設置する。

② 無線LANによるユビキタス環境を天久保地区に構築する。

以上のことを整備方針として定め，個人設置APよりも安全で利便性のある環境を構築することにより，結果的に，個人設置APが一掃されることを目標とした。

APの規格については，平成14年当時，IEEE802.11aとIEEE802.11bの2規格が候補として存在した。双方の規格に対して優劣を決定することが困難であったので，何れにも対応できるように，802.11aにも拡張可能な802.11b規格の機器を最初に選定した。その後，新規格の制定，普及状況等を勘案し，IEEE802.11g規格の機器に統一した。また，移動通信が可能であるように，ローミング（Roaming）機能も採用した。

2.2 整備状況

上述の整備方針に基づき，以下に示すように体系的にAPの設置事業を推進・継続中である（表2参照）。

(1) 平成14年度に試行として，3台のAPを大会議室他に先行設置した。安全対策としては，使用時のみの運用と，ESSID（Extended Service Set Identifier）を発信しないなど，極めて脆弱なものであった。

(2) 平成15年度に，教育研究基盤設備としてRADIUS（Remote Authentication Dial In User Service）サーバを導入し，ユーザIDとパスワードによるIEEE802.1xネットワーク認証とWEPによる暗号化を開始した。APから学内LANに接続するための安全な環境が確立できた。これに伴い，講堂などに2台のAPを増設し，共用空間における24時間運用を開始した。

(3) 平成16年度に，講義室前廊下にAPを増設し，校舎棟全講義室を無線LAN運用区域とした。また，学生寄宿舎共用棟にも設置し，無線LAN運用対象の共用空間を拡大した。

(4) 平成17年度に，校舎棟4～6階にそれぞれ2台ずつ，6台のAPを廊下に増設し，これらの階の全域を無線LAN運用区域とした。

規則面においては，平成16年3月に天久保地区を対象に「天久保地区無線LANアクセスポイント運用要領」を定め，平成18年3月には「国立大学法人筑波技術大学無線LANアクセスポイント運用要領」として，全学にその適用範囲を拡大した。これにより，APの設置には，安全対策の設定と届出が必要となった。また，運用・安全面での問題が発生した場合には，センターが当該APの学内LANからの切り離し等が行えることになり，一層の運用責任を担うこととなった。

2.3 成果及び問題点

天久保地区約44,000m^{2}の敷地面積の内，無線LANサービス対象地域と想定した約17,000m^{2}の地域内に，平成17年度末現在で合計18台のAPを設置した。

この結果，以下のような成果と問題点が判明した。

① 室内，室外を問わず，APが目視できる範囲内では，快適な接続環境が得られた。ガラス越しであっても特段の電波状況の減衰は見られない。

② 鉄筋コンクリート壁等がAPと端末の間に存在すると，電波の減衰は極めて著しい。このため，廊下等の共用空間にAPを設置し室内をその運用対象区域とする場合には，高密度にAPを設置する必要があるが，廊下等の共用空間では過密状態となる。

③ 802.11gで使用できる無線周波数の数は13である。これに対し，18台のセンター設置APに加えて，センター設置外のAPも多数存在しており，周波数の数は不足している。センター設置APは，電源投入時に電波状況を確認し，干渉が起こらないように自動的に周波数を選択後，起動する。しかし，センター設置外のAPが後から動作を始めた場合には，動作中のセンター設置APとの間に電波干渉が生じ，障害が発生している可能性がある。

④ 電波干渉等による障害を抑制するために，次期AP整備については，随時，周波数及び電波出力を統合的に制御する方式が不可欠である。

次期AP整備計画については，現在調査・策定中であり，平成19年度に事業を開始する計画である。

3. 学生寄宿舎のネットワークセキュリティ

3.1 ネットワーク障害

現『新高速ネットワークシステム』では，DHCP等の自動設定プロトコルの導入により，複雑な設定・手続きが不要な自動接続環境を実現している。誰でも，例え学外者であっても，自由に学内LANに自動接続できる環境である。しかし，この学内LAN自動接続環境が，障害等発生時の原因追及を困難にしている。実際，学生寄宿舎では，以下のような重大な事態が発生したが，その事態を発生させた

当事者は確定できなかった。

① 平成 13 年 11 月，割り当て外の IP アドレスが無断使用された。

② 平成 15 年 9 月，ウィルスによる広範囲なパソコン汚染が生じた。

③ 平成 16 年 6 月，不正な DHCP サーバが稼動して不正な IP アドレスが配付された結果，学生寄宿舎ネットワーク全体が半日近く利用不能となった。

このような事態に際して，原因機器と使用者の特定が早期にできなかったことが，被害の拡大を招いた。また，対処方法としても，入居学生数人の「ユニット」単位での学内 LAN 切断を行うことしかできず，関係のない学生が学内 LAN を利用できなくなる事態を招いた。

3.2 学生寄宿舎ネットワークの改修計画

センターでは，この種の障害が発生する度に掲示等で入居学生に対応を求めていたが，誠実な対応がなされないまま事態は推移していた。その結果，3.1 ③にあるように学生寄宿舎における学内 LAN 全面停止という極めて重大な事態を招いた。この種の障害に対しては，ネットワーク利用モラルを徹底することが有効ではあるが，そのようなソフトウェア的対応だけでは限界がある。障害・問題発生を完全に防止・対処するためには，ハードウェア的対応も必要であると判断し，平成 16 年度教育研究基盤設備「聴覚部寄宿舎認証 LAN システム」として「認証スイッチ」を要求した。

この「認証スイッチ」システムは，ウェブブラウザ上でユーザ名とパスワードを用いたネットワーク認証実行後に，その端末を学内LANへ接続する。認証システムには，2.2 (2) の RADIUS サーバを兼用する設計である。導入の効果としては，

① 障害発生時に原因機器およびその利用者を直ちに特定でき，早期の対応・処理が可能となり，関係のない学生が不利益を被ることがなくなる。

② 学外者による不正利用を防止することができる。

③ 不正なサービス機能の防止が可能となる。

などの点が実現でき，学生寄宿舎ネットワークの安全かつ安定した運用が期待できる。

3.3 学生寄宿舎ネットワークの改修結果

平成 16 年 11 月 24 日に学生寄宿舎全 4 棟のスイッチを「認証スイッチ」に交換した。平成 17 年 1 月 11 日より各学科のネットワーク相談員により，全入居学生に対し，ユーザ名とパスワードの配付を開始した。

平成 17 年 1 月 19 日午後 1 時よりネットワーク認証の運用を開始した。学生寄宿舎からの学内 LAN の利用に際しては，少なくとも 1 日に 1 回のネットワーク認証が必要となった。十分な周知時間をかけ，計画的に作業を進めた結果，運用開始に伴う混乱は生じなかった。

この「認証スイッチ」とネットワーク認証を導入した結果，ユーザ名と端末機器の対応が確実できるようになった。ただし，幸いにもこの対応付けが必要となる事態は発生していない。

ネットワーク認証により個人が特定されているという意識のためか，あるいは，認証方法を含めたネットワーク利用教育をセンターが積極的に行った成果であるのか不明ではあるが，ネットワーク認証運用開始後，ウィルス汚染を含めた学生寄宿舎ネットワークでの重大な障害発生はなくなった。さらに，副次的効果として，認証システムを兼用する無線 LAN 利用も進んでいる。

4. 非常勤講師等宿泊施設へのネットワーク認証導入

非常勤講師等宿泊施設（以下，紫峰会館という）においても，DHCP 等を導入しているため，利用者はだれでも情報コンセントに UTP ケーブルを差し込むだけで快適に学内 LAN が利用できる状況にあった。このような環境下で，紫峰会館から学外に向けた通信が，数時間連続して発生していた記録が発見された。宿泊者の行為であろうと推測したが，行為者を特定する方法がなかった。

昨今のネットワーク事情から見て，紫峰会館を利用する学外者が自由に学内 LAN を利用でき，かつ，その利用者の特定が不可能である非常に危険な状態であると判断し，紫峰会館に対しても，学生寄宿舎と同等の「認証システム」を導入することとした。

これに伴い，平成 17 年 10 月「筑波技術大学非常勤講師等宿泊施設での学外者ネットワーク利用に関する申し合わせ」を定め，学外者にも学内規則他の遵守を誓約させた上で，一時利用のユーザ名とパスワードを発行し，学内 LAN を利用させている。

不測の事態が発生した場合に，その原因を直ちに特定できる管理体制が確立できた。認証システム導入後，幸いにも，未だ，そのような作業が必要となる事態は発生していない。

5. サーバの整備

基幹サーバについては，文献 [1] に示したとおりであり，大きな変更はない。その後，表 1 に示すように，一般学内利用者用メールサーバ，DNS (Domain Name System) サーバ，ネットワーク認証サーバ（2.2 項参照）の追加がなされた。

5.1　メールサーバ

従来メールサーバは短期大学部の各学科ごとに運用されてきたが，学科での保守・管理・運用の限界，学科に属さない教職員に対するサービスなどを考慮し，将来的に天久保地区全教員を収容する計画で，平成14年3月に情報処理通信センター（天久保地区）ドメインのメールサーバを運用開始した。平成14年12月には，このサーバ上でメーリングリストサービスも開始した。平成17年8月には，ウェブメールを導入し，利用者の利用環境の拡大を図った。天久保地区教員の半数近く，メーリングリストサービス利用者を含めればほぼ全員が利用していると言っても過言でない重要なサーバとなった。

産業技術学部学生については，短期大学部学科メールサーバが利用できないために，新たにセンターの管理下に専用メールサーバを構築することにした。平成18年度入学生（1期生）から「産業技術学部学生用メールサーバ」の運用を開始した。このサーバには安全性の観点からLDAP（Lightweight Directory Access Protocol）認証を採用したことが特徴的である。将来的には，このサーバに学部学生，200人を収容する計画である。

5.2　DNSサーバ

従来のDNSサービスは，他のサービスも提供する汎用サーバ機上で提供されていた。このため，他サービス保守作業上の必要性からサーバ機を停止させた場合などに，DNSサービスも停止するため，冗長化構成であっても通信に遅延が生じるなどの障害が発生していた。

この遅延障害などを解消するために，図1に示すDNSサービスのみを提供する単機能サーバ機を導入した。図中，左端が主（Primary）DNSサーバ，中央と右端が副（Secondary）DNSサーバである。主1台，副2台の3台構成とし，処理の分散と冗長化構成を強化した。大きさを判別するために，3.5インチフロッピーディスクを右側に置いている。従来のサーバ機の概念を打ち破る非常に小さな筐体であるが，LINUXで動作している。

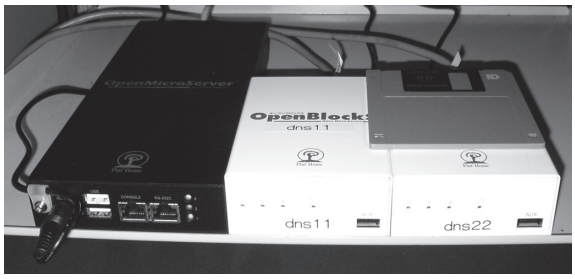

図1　DNS単機能サーバ機

このサーバ機の特徴は，大きさではなく，ハードディスクなどの機械的駆動装置を持たないことである。このため，停電・振動対策などが不要であり，極めて簡便な環境で運用でき，既に3年間以上無障害で動作している。

このサーバ運用開始後，DNSサーバが原因の通信障害は発生せず，設置目的を果たしている。また，DNSサーバのIPアドレスが固定できたことにより，他のサーバ構成の変更が機動的に行えるようになり，この効果は非常に大きい。

6. 対外接続の改善

対外接続としては，平成14年2月よりSINET筑波大学ノードとの間に10Mbpsの専用回線を使用していたが，平成17年4～5月に回線容量不足による通信障害が発生した。また，この時期に，SINETが「地域IP網」や「広域LAN接続サービス」を利用した新たな接続形態を発表したこともあり，情報処理通信センターでも新たな対外接続方法の調査を開始した。

この結果，通信の安定性，安全性などを考慮して，平成18年2月より100Mbpsの専用回線による接続方法に更新した。これにより，高速化が実現でき，余裕のある対外接続状況が維持されている。

7. おわりに

平成15年度以降，①無線LANの敷設とネットワークセキュリティの向上，②サーバ機の増強，③対外接続回線の高速化などの改善事業を行った結果，以前に比較して，より安全・安定した機動性の高いネットワークサービスを提供することが可能となった。

平成18年度には，特別教育研究経費「障害学生支援情報統合運用管理システム」の構築が計画され，より一層，利便性の高い学内ネットワーク環境の構築を目指すものである。

参考文献

[1]　浅草 肇, 西岡 知之, 清水 豊：情報処理通信センター（聴覚部）における新サーバシステム．筑波技術短期大学テクノレポート9（1）：47-52，2002.

[2]　浅草 肇，西岡 知之，内野權次，清水 豊：聴覚部における新高速ネットワークシステム．筑波技術短期大学テクノレポート9（2）：31-36，2002.

Improvement of Security and Stability of a Campus Network System in Amakubo

ASAKUSA Hajime[1)] NISHIOKA Tomoyuki[1)] and KITAGAWA Hiroshi[2)]

[1)] Information Processing and Networking Center (Amakubo)

[2)] Vice Director of Information Processing and Networking Center

Abstract: This report introduces the following improvement on the Amakubo campus network system since 2002. (1) Secure LAN system for wire and wireless was established. (2) Additional server system was designed and installed. (3) Leased line between SINET was changed more fast line.

Keywords: wireless, security, authentication, additional server, line speed