第三世代学内 LAN
（主として天久保地区について）

筑波技術大学　情報処理通信センター部局技術責任者

浅草肇

要旨：情報セキュリティ対策規程に適合する基盤機器への更新、SINET4 への接続変更など、第三世代と称すべき学内LANに更新されたので、天久保地区の状況を中心にその概況を報告する。
キーワード：情報セキュリティ，対外接続，SINET4，学内 LAN，更新

1．はじめに

既報 [1],[2] に示すように、本学学内 LAN（Local Area Network）は、次のように改良・運用されてきた。

【第一世代】平成6（1994）年3月運用開始
10BASE5（回線速度：10Mbps）
【第二世代】平成 13（2001）年 11 月運用開始
L3 及び L2 スイッチ使用
基幹 1000BASE-SX（回線速度：1Gbps）
末端 100BASE-TX（回線速度：100Mbps）

また、学外接続回線についても、64Kbps デジタル専用回線で運用が開始され、100Mbps まで通信速度の向上を図ってきた。

このような運用状態中、平成 17（2005）年7月にネットワーク基盤機器製造会社より、使用中の機器について平成 19（2007）年７月から平成 22（2010）年 3 月にかけて順次、故障時に修理対応不可になるとの通知があった。このことに対処するため、情報処理通信センターは、平成 18（2006）年1月に更新計画を立案し、次のように関連する更新作業等を完了させた。

（1）LAN 基盤機器等更新：平成 22（2010）年2月
（2）対外接続回線高速化：平成 22（2010）年3月
（3）SINET4 接続変更：平成 23（2011）年4月

学内 LAN は【第三世代】と称すべき新構成になったので、天久保地区の状況を中心に報告する。

2．学内 LAN 基盤機器更新

2.1　情報セキュリティ対策規程制定

平成 17（2005）年 12 月「政府機関の情報セキュリティ対策のための統一技術基準」が決定されたことを受けて、国立情報学研究所等においても、平成 19（2007）年 10 月「高等教育機関の情報セキュリティ対策のためのサンプル規程集」が公表された（平成 19 年2月一部先行公表）。

本学においては、平成 17（2005）年３月に「筑波技術短期大学セキュリティ基本方針」が制定されていたが、上記の統一基準・基本方針に対応させる改訂作業が、平成 19（2007）年３月より正式に開始された。

この結果、平成 20（2008）年２月、「情報システム運用基本方針」、「情報システム運用基本規程」が制定され、平成 21（2009）年3月「情報システム運用･管理規程」、「情報ネットワーク接続手順に関する規程」などの実運用に必要なセキュリティ関連規程が制定された。

また、平成 21 年度より、これらの規程に基づく「情報セキュリィティ監査」が実施されるようになった。

2.2　L3 スイッチ及び L2 スイッチ

情報セキュリティ対策規程に適合するためには、ネットワーク自体がセキュリティ保持機能を有することが必須事項となり、ネットワーク基盤機器にもそのことへの対応が必要となった。一方、通信回線に関しては、【第二世代】時代に敷設された通信ケーブルを継続使用することとし、主要幹線については通信帯域幅の確保及び冗長性の確保を兼ねて、複数の通信回線を同時使用することにした。この結果、スイッチ等主な調達仕様は次のように定められた。

（1）端末単位でネットワーク認証ができること。
（2）冗長性が確立していること。
（3）長期間の保守修理が可能であること。
（4）末端（情報コンセント）において、1Gbps であること。
（5）幹線においては 1Gbps、主要幹線においては、最大 1Gbps × 4 の帯域幅が確保できること。

学生寄宿舎については、平成 17（2005）年1月からネットワーク認証制度が実施されていることと、現行の設備状況が通信ケーブルの性能限界であることから、現行状態を継続することにした。ただし、L3 スイッチを介した完全分離型に変更した。

基盤機器更新時のネットワーク構成の概略を図1に示す。対外接続方法については、この後更新された。

2.3　情報セキュリティ体制

情報セキュリティを確保するために、天久保地区では、学外者を含む不特定の人が使用する可能性がある、若しくは、機器更新時に3ヶ月間利用実績のない情報コンセントに対して、端末単位で利用者本人の利用資格を確認する個人認証制度を平成 22(2010)年3月より導入した。認証には、全学共通情報基盤として平成 18(2006)年 11 月より運用開始した RADIUS 認証サービスを使用している。RADIUS 認証サービス用サーバは、天久保地区並びに春日地区にそれぞれ設置され、かつ、冗長化設定されているため、1地区のサーバが停止した状態であっても、利用者は常時そのサービスを享受できる安定した運用体制にある。

2.4　冗長化と運用体制

基盤機器の冗長化については、末端では通信ケーブルが一経路しか敷設されていないので、完全自動冗長化は不可能である。したがって、幹線末端に設置する L2 スイッチについては、予備機を各地区ごとに1台用意する仕様設計とした。また、幹線中枢の L3 スイッチについては、シャーシ以外の全ての構成部品を冗長化する、若しくは、完全に同一機能・性能の予備機を各地区ごとに各1台を設置する仕様設計とした。

結果的には、L3 スイッチも予備機での対応となった。障害発生時には、静態保存予備機に切り替え、短時間で復旧できる。さらに、その際、春日地区に同一機能・性能の予備機が存在するので、障害発生機の修理等に十分な余裕を持って対応できる。運用の安定性と保守費用の低減に著しく貢献する運用体制が確立できた。

2.5　ファイアウォールゲートウェイ

平成 18(2006)年 11 月に最大通信速度 100Mbps の UTM（Unified Threat Management）型ファイアウォールゲートウェイを学内 LAN 最上位に設置していた。

今回の機器更新に際して、冗長性確保の観点からと SINET4 への接続を予測して、最大通信速度 1Gbps の UTM 型ゲートウェイに換装し、既設機器を予備機として静態保存することにした。

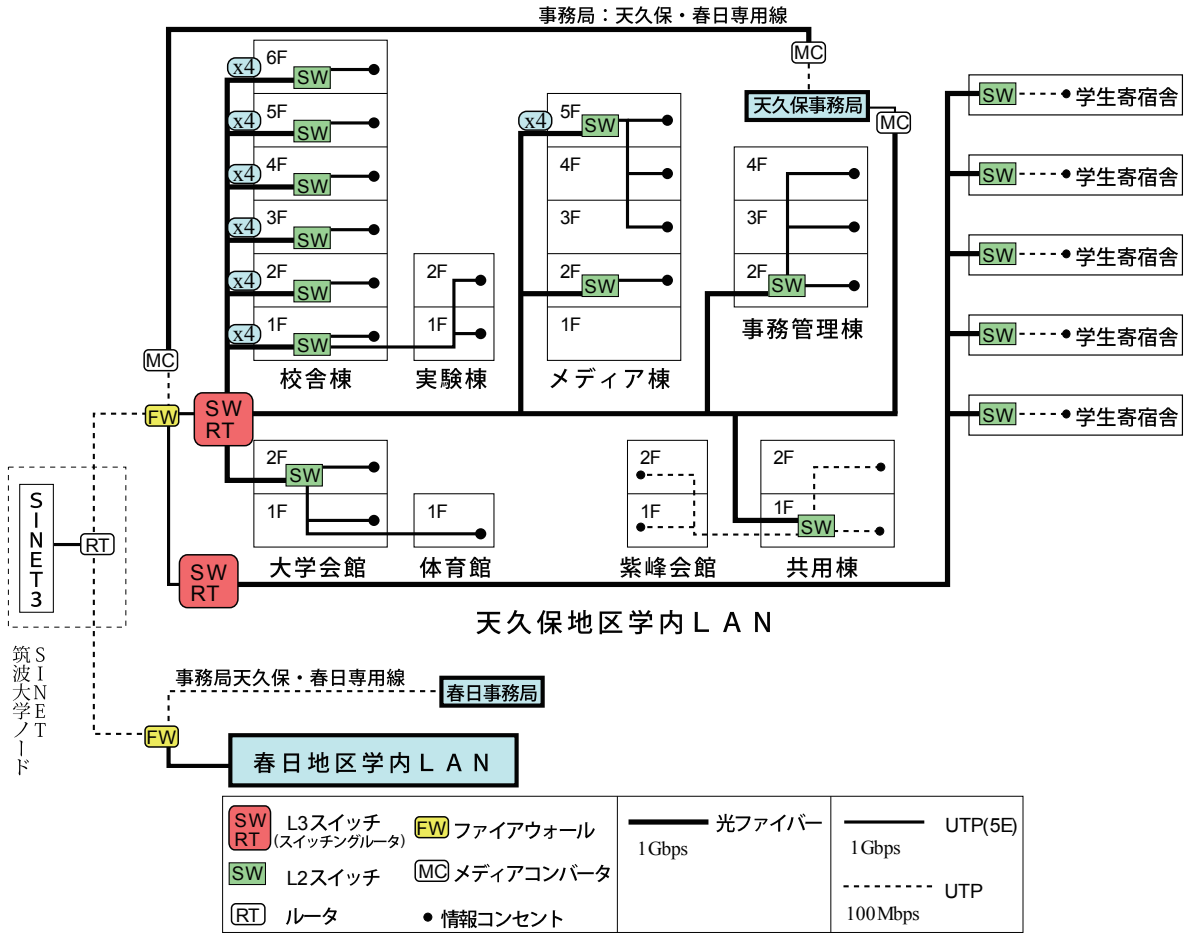

図1　情報ネットワーク構成の概要（基盤機器更新時）

2.6　学外からの安全な接続（SSL-VPN）

本学構成員が学外から学内 LAN に安全に接続し、学内資産をあたかも学内に居るかのごとく使用できる環境を提供するために SSL-VPN（Secure Sockets Layer Virtual Private Network）装置を設置した。最大通信速度 1Gbps、同時接続数 50 である。

この装置の利用には、RADIUS 認証サービスによる個人認証が必要である。教職員及び学外居住や帰省中の学生利用が確認できている。

3. 対外接続回線の改良

3.1　100Mbps 接続回線

平成 18（2006）年2月に、100Mbps 専用回線を用い、図2に示すような、SINET3 筑波大学ノード設置の本学所有 L3 スイッチを介し、天久保・春日地区相互間及び SINET3 へ接続する方式とした。しかし、後年、この構成に次の問題が発生した。

（1）L3 スイッチの通常の CPU 負荷最大限度は 50 ～ 60% であるとの製造会社の推奨値に対して、常時 90% 以上の高負荷を示し、その結果、スイッチの遠隔操作に支障を来す状態となった。

（2）平成 21（2009）年８月以降に天久保・春日地区において、それぞれ少なくとも3回、最大帯域幅の 100Mbps（5分平均値）の通信量が計測された。特に、天久保地区においては、業務時間内に発生した。

いずれも、直接原因は通信量の増大に基づくが、特に（1）については、事務局を含めた天久保・春日間通信数の著しい増大が原因ではないかと推測された。

これらのことから、対外接続回線の容量拡大を図るとともに、天久保・春日間通信方法については、基本設計から改めることとした。

3.2　改良接続回線網

平成 22（2010）年３月に図３に示すように 1Gbps 専用回線を用いたスター型 L2 接続専用回線網に変更された。この回線網の特徴は、これまで本学が設置していた SINET3 ノード設置の L3 スイッチ機能が通信事業者により提供されたこと。また、L2 回線網なので、天久保・春日間通信が直通となったことである。さらに、通信事業者が、専用回線終端装置であるメディアコンバータとして L2 スイッチを天久保地区、春日地区にそれぞれ設置したことである。この L2 スイッチの設置により、天久保・春日間には独立した複数の直通 VLAN を設定することが可能となった。この直通 VLAN により事務局天久保・春日間通信は革新的に変化した。

3.3　事務局天久保・春日間接続

従来、事務局天久保･春日間通信は、学内 LAN のデータと混合して同一経路を流れていること、さらに、学外の SINET ノードを経由しているために、セキュリティ確保の観点から暗号化が必要であった。これらのことから、天久保及び春日事務局ネットワークと学内 LAN 接続地点には、そ

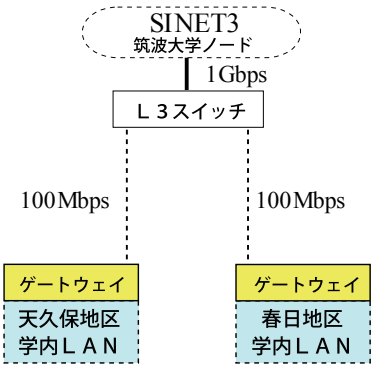

図2　対外接続概略図1
平成 18（2006）年2月

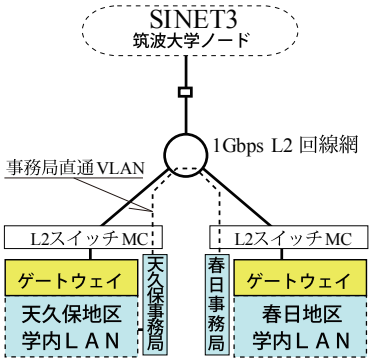

図3　対外接続概略図2
平成 22（2010）年3月

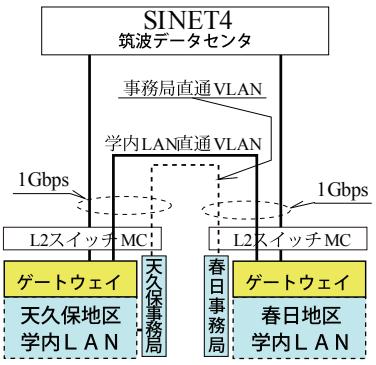

図4　対外接続概略図3
平成 23（2011）年4月

れぞれ UTM 型のゲートウェイを設置し事務局ネットワークを学内 LAN から隔離していた。次に、この両ゲートウェイ間を VPN（Virtual Private Network）により接続し、事務局間通信のセキュリティを確保していた。

このことが、図1に示すように事務局間通信手順・経路が複雑化することの原因であった。さらに、事務局天久保・春日間通信が途絶すると事務局業務に支障が生じる。この業務支障を防ぐためには学内 LAN を停止させてはならない。このことが、学内 LAN 管理・運用の立場に立脚すると、非常な重圧となっていた。

図3の改良回線網では、天久保事務局からの回線を直ちに専用回線終端装置：L2 スイッチに接続し、天久保・春日間直通事務専用 VLANを経由して春日事務局に直結した。この直通 VLAN におけるセキュリティは、電気通信事業法の定めるところによる電気通信事業者の責任において確保することとし、VPN 通信を廃止した。また、学内 LAN との結合も天久保地区1地点のみとした単純・安全なネットワーク構成となった。

この接続方法改良により、データの転送時間がほぼ半減したとの報告を受けている。また、不要となった UTM を予備機として静態保存し、冗長性を向上させた。さらに、学内 LAN に障害が発生しても、事務局天久保・春日間通信は影響を受けず、安定性が大きく向上し、学内 LAN 運用の重圧も解消した。

4. SINET4 への接続変更

平成 23（2011）年4月より SINET4 での運用が開始された。SINET3 との主な相違点は次のようである。

（1）SINET への接続拠点が民間の筑波データセンタに変更されたこと。

（2）接続通信速度が 1Gbps 以上に限定されたこと。

SINET4 への接続変更に際しては、図4に示すように各地区ごとに直結する形態を SINET より指定された。この接続形態変更により、各地区ごとに 1Gbps の帯域幅が確保できた。また、学内 LAN 用：最大 1Gbps、事務局用：最大 100Mbps の天久保・春日間直通 VLAN を設定した。これにより、図3のスター型 L2 接続専用回線網と同一機能となった。

5. 無線 LAN アクセスポイントの更新

平成 15（2003）年3月より無線 LAN アクセスポイント（AP）の設置を開始し平成 20（2008）年5月に天久保地区公共空間（研究室、実験室などを除く不特定の人間が利用できる空間）全域に対して、約 20 基の AP で IEEE 802.11g 規格による接続サービス体制が完成した [2]。

しかし、同規格で使用できる無線周波数のチャンネル数（13）以上の AP の存在よる電波障害発生が確認されたこと。また、新規格 802.11n が実用に供される状態になったこと。などの状況から常時、無線周波数並びに出力を中央にて統合的に制御する方式の機器に更新した。

新制御方式機器の導入により、複数の SSID（Service Set Identifier）の使用と、それぞれに異なるサブネットワークを割り当てること、並びに、異なる認証方式を設定することが可能となった。これにより、eduroam[3] の導入が可能となった。

6. おわりに

学内 LAN は第三世代に更新されたことにより、情報コンセント（研究室等）から SINET に至るまで、1Gbps の帯域幅が確保された。また、全基盤機器について予備機器が静態保存されているので、異常時にも素早く対応できる安定した運用体制が確立できた。

ネットワーク基盤機器の仕様は、全学情報システム運用委員会部局技術責任者により構成された仕様策定委員会（委員長:浅草肇）が「情報ネットワークシステム仕様書（平成 21 年7月）」として定めた。回線並びに無線 LAN AP の仕様は情報処理通信センターにて定めた。

参考文献

[1] 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.

[2] 浅草 肇, 西岡 知之, 北川 博：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, 筑波技術大学テクノレポート Vol.14：119-122, Mar 2007

[3] 例えば, http://www.eduroam.jp/docs.html

The Third-Generation Campus Network in Amakubo

ASAKUSA Hajime

Information Processing and Networking Center, Tsukuba University of Technology

Abstract: This report introduces the following third-generation improvements to the network system of the Amakubo campus: (1) Information equipment is upgraded to a new secure system that is compliant with information security rules. (2) Communication lines connect the campus to the outside world the campus through the SINET4.

Keywords: Information security, Outside communication line, SINET4, upgrade