附属学校における ICT 活用のためのネットワーク再整備

佐々木 正人, 石黒 克也, 佐々 浩司

高知大学 総合情報センター

sasaki@kochi-u.ac.jp, ishiguro@kochi-u.ac.jp, sassa@kochi-u.ac.jp

概要：これまで附属学校では，校内ネットワークをそれぞれの校園で管理運用してきたが，ネットワーク配線や構成機器の維持管理や情報セキュリティ対策などが不十分である．また，今後の ICT を活用した授業への対応も遅れていることから，総合情報センターの管理運用ノウハウを活用して再設計・再構築を行った．

1　はじめに

高知大学教育学部には４つの附属学校（小学校，中学校，幼稚園，特別支援）があり，特別支援学校を除く３校園は小津地区（総合情報センターのある朝倉地区から約 5Km）にある．附属学校のネットワークは３校園それぞれが管理し，学内ネットワークとは小津地区設置の Firewall を経由して回線接続している（図１）．

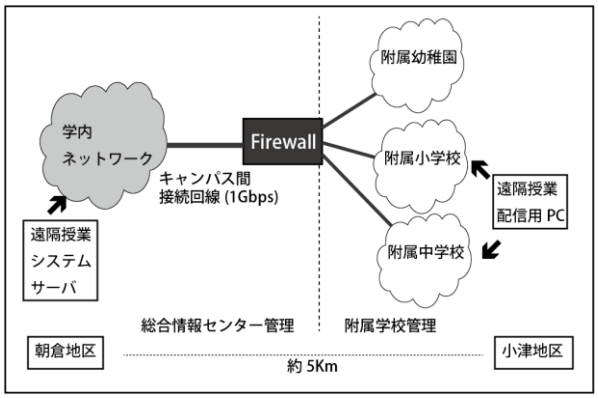

図１　附属学校（小津地区）ネットワーク概要

2015 年度，教育学部において附属学校での授業風景や児童・生徒が使用するタブレット端末の画面配信等を行う「遠隔授業システム」の導入が決まった．学内ネットワーク上のサーバと附属小学校・中学校のネットワーク上の配信用ノート PC の通信を実現するため，総合情報センターが附属小学校・中学校のネットワーク状況を担当者にヒヤリングして遠隔授業システムの設計およびネットワーク設定を行った．その作業の過程で，ネットワーク配線や機器構成などの管理が不適切であること，個人情報を含むデータの扱いや責任体制が曖昧であることなどの問題が明らかになった．これらの問題を解消するため，遠隔授業システムを接続する前に，本学セキュリティポリシーを踏まえ総務省作成のガイドラインを参考にして小津地区ネットワークの再設計を行い，可能な範囲で再構築した．同時に無線 LAN 環境の整備計画を策定し，今後授業でタブレットや電子黒板等 ICT 活用が可能な環境を整備することになった．

以下，総合情報センターの管理運用ノウハウを活用した附属学校のネットワーク再設計・再構築の取り組みについて報告する．

2　物理配線の調査・再構築

学内ネットワークの教室・研究室への配線（情報コンセント）は，施設課と連携し総合情報センターで図面とデータベースにより管理している．また各部局予算で配線する際は，あらかじめ総合情報センターに相談・接続申請してもらうことで情報コンセントを管理している．一方附属学校で整備した情報コンセントは附属学校で管理しているが，配線図面や構成図等がなく管理が不十分である．このため，附属学校内のすべてのネットワーク配線と構成機器（ハブなど）を現地で調査し，総合情報センターの配線方法(情報コンセント単位で VLAN 設定が可能)に沿って再構築した．

2.1 主な問題点・課題とその対応

現在情報コンセントは，総合情報センターが管理するフロアーSW のポートに CAT6 以上のケーブルにより接続し，1Gbps の通信サービスを提供している．附属学校内では一部 CAT5 ケーブルによる配線があること，10Mbps，100Mbps のハブ中継により通信速度が制限されていることが判明した．また，配線の無い建物間を無線により LAN 間接続していたり，一部に設置されている無線アクセスポイントではアクセス記録が収集さ

れていない等の問題点が明らかになった．物理配線の更新は建物改修工事等の際に行うこととし，中継ハブはすべて1Gbps対応の機器に置き換え，情報コンセント単位でVLAN設定可能になるよう一部配線を変更した．無線については今後の授業での利用を検討し，タブレット追加購入も含め年次計画を策定の上整備することとした．

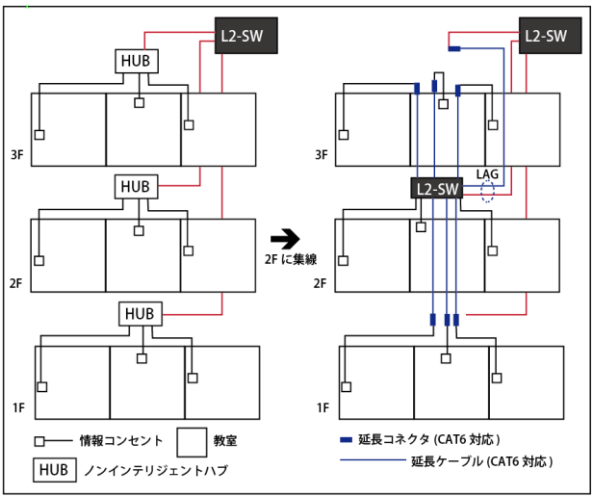

図２　パッチケーブルによる集線

2.2 パッチケーブルによる集線と今後の管理

ノンインテリジェントハブをカスケードすることで単一VLANによる接続を行っている箇所に，総合情報センターのフロアーSW を新設し，原則情報コンセント単位でVLAN設定可能となるようパッチケーブルにより配線変更した（図２）．これにより，附属学校の情報コンセントの 95%以上の情報コンセントで VLAN 設定可能となり，総合情報センターの管理方法に合わせた管理が可能となった．今後附属学校で増設・更新工事を行う場合は事前に申請してもらい（学内ネットワークでのルール適用），他学内ネットワークと同様に管理することとした．

3　情報セキュリティを考慮したネットワークの再設計・再構築

附属学校の物理配線を把握し，情報コンセント単位での VLAN 設定がほぼ可能となった．附属学校のネットワークにおいて，情報セキュリティも考慮しながら今後の授業での ICT 活用が可能となるよう，３校園で統一した考え方にもとづいて再設計・再構築した（図３）．

3.1 利用用途別ネットワークの定義

接続する端末の用途や求められるセキュリティ・レベルから以下の６つのネットワークを定義し，既存の端末をその利用目的に応じたネットワークに移行することとした．

[net1] **児童・生徒用ネットワーク１**　：パソコン室設置のデスクトップ PC 接続用…有線のみ(Mac アドレス認証)

[net2] **児童・生徒用ネットワーク２**　：タブレット端末やノート PC 接続用…有線・無線(利用時認証)

[net3] **教員用ネットワーク１**：教材研究など児童・生徒の個人情報を扱わない端末接続用(IP アドレス制限)

[net4] **教員用ネットワーク２**：児童・生徒の個人情報を扱う職員室等の端末接続用(IP アドレス制限, NAT)

[net5] **全学共通無線ネットワーク**：他地区でも利用可能な教育研究用無線ネットワーク(教員，教育学部教育実習生のみ，利用時認証)

[net6] **事務用ネットワーク**：事務業務端末接続用(教育研究用および附属学校内ネットワークとは分離)

ただし，[net6]はすでに構築済み．

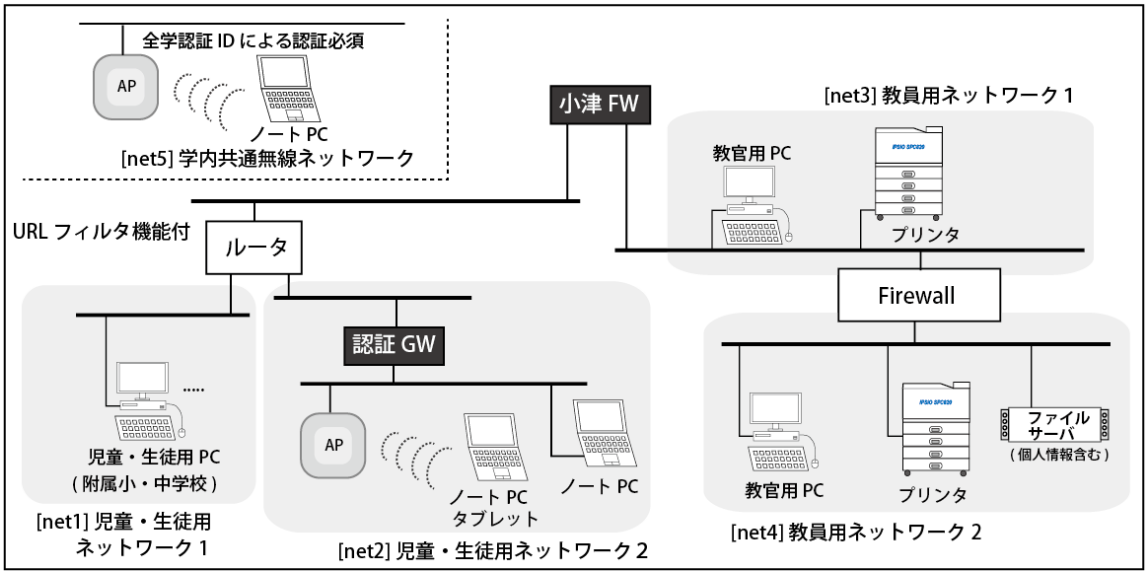

図３　附属学校新ネットワーク構成図

3.2 ネットワークの再構築

教員用 PC を[net3], [net4]に分類し接続するために必要な Firewall や，[net1], [net2]からインターネットにアクセスする際に必要な URL フィルタリング機能付ルータ等を附属学校（教育学部）が購入し，ユーザ ID による認証のための認証ゲートウェイは総合情報センターで準備してネットワークの再構築を行った．予算の関係で，[net1],[net2]は附属学校共通とし，今後利用状況に応じてネットワークを分ける予定である．また，新ネットワークへの移行により通常の授業や校務にできるだけ支障をきたさないよう新ネットワーク環境を構築（新旧ネットワークを異なる VLAN で同時に構築）した上で順次移行できるよう配慮した．

接続機器の管理台帳(識別番号, 購入年度, 購入先, 設置場所・情報コンセント番号, 目的, 利用責任者等)の整備は３校園担当者が行った．この際，既に総合情報センターのフロアーSW に各情報コンセントが直接接続されているため，フロアーSW にて収集した Mac アドレス情報にもとづいて接続機器リストを作成して，管理台帳と突合することで接続機器に漏れがないよう配慮した．

3.3 IP アドレスや情報コンセントの管理

これまでは台帳により３校園それぞれで IP アドレスを管理してきた．教員の異動や機器の入れ替え等の際に多くの管理漏れが見られるため，今後は登録・返却・変更の際は総合情報センターに申請し総合情報センターで IP アドレスを管理することとした．

なお，[net4]についてはプライベートアドレスを使用するが，新設 Firewall にて 1:1 NAT(グローバルアドレスへ)し IP アドレスの４オクテット目を同じにすることで管理する．

3.4 接続端末の認証・利用制限

[net1]については，デスクトップ PC での利用認証(ログイン認証)はもちろん MAC アドレス認証を行って不正な機器が接続されないよう配慮している．[net2]については，タブレットやノート PC などのモバイル機器を接続しネット利用を開始する際に，認証ゲートウェイで全学認証システムと連携して利用者認証を行う．

なお，[net1]，[net2]については，URL フィルタリング機能付ルータ(YAHAMA ルータ＋Standard Web security)・学内プロキシサーバーを経由してインターネットに接続している．また，[net4]は[net3]と FireWall で接続し外部との通信が必要無いファイルサーバ等については通信を完全に遮断(NAT しない)している．

3.5 全学共通無線ネットワーク

本学では全地区において共通に利用できる教育研究用無線 LAN を整備している．附属学校教員や教育学部学生（教育実習時など）が附属学校でも利用できるよう[net5]用無線アクセスポイントを新設した．この無線システムでも，利用開始時に全学認証システムと連携して個人認証を実施している．

3.6 新ネットワークへの端末の移行

情報コンセント単位で，台帳により確認が完了した端末から順次移行作業を行っている．移行作業は，総合情報センターで作成した資料を見ながら利用者に設定変更してもらう方式で実施し，学生スタッフ等による支援も行っている．

3.3 ICT を活用した授業のための無線 LAN 整備

今回の再構築により各教室でノート PC が接続（有線）できる環境は整ったが，無線 LAN の環境は一部を除き整備されていない．このため，全教室で無線接続できるよう無線アクセスポイントを整備する予定である．[net5]の無線アクセスポイントに[net2]に接続できる設定を行い，総合情報センターで一元的に管理する方式を考えている．2015 年度は，ほぼすべての教室で無線接続可能な[net2]環境を整備し，多人数同時にタブレット等を接続する場合は，移動式無線アクセスポイントを利用する．さらに，全教室で児童・生徒全員が同時に無線接続できる環境をタブレットの整備と合わせて計画中であり，今後順次整備する予定である．

4 教員へのセキュリティ研修

今回の取り組みでは，附属学校の担当者と打ち合わせを何度も実施した．また，ネットワーク調査や接続機器の調査を通じて教員へのセキュリティ教育が必要であると考えている．また，教員からもセキュリティ講習を受けたいとの希望もある．このため，総合情報センターが全学教職員や学生を対象として実施しているセキュリティ講習会を附属学校でも開催している（図４）．これを契機に，情報セキュリティに対する意識を高め，それぞれの校園の教員が講師になって定期的にセキュリティ講習が開催できるよう総合情報センターで教育支援する予定である．特に職員会議等において，短時間での啓蒙活動を期待している．さらに，現在は附属学校のセキュリティポリシーの整備が不十分である．公立学校でのセキュリティポリシー雛型を元に総合情報センターが作成した案を，３校園のネットワーク担当者が検討し 2015 年度中に再整備する予定である．

情報セキュリティ研修会　チェックシート　　総合情報センター

場面１

(01) ログインパスワード　□設定している　□設定していない　□分からない
(02) スクリーンロック　□設定している　□設定していない　□分からない
(03) PC 上のファイル　□常に全ファイルを保存　□最小限のファイルのみ保存

場面２

(04) ウイルス対策ソフト　□導入している　□導入していない　□分からない
(05) ウイルス定義ファイル更新日時　□毎日確認　□時々確認　□確認していない
(06) Windows Update　□実施している　□実施していない　□分からない
(07) ファイヤーウォール機能　□設定している　□設定していない　□分からない
(08) フリーソフトのインストール　□気を付けている　□気にしていない　□インストールしない
(09) 怪しいサイト　□気を付けている　□気にしていない　□学内サイトのみ

場面３

(10) 送信前に宛先アドレス　□必ず確認している　□重要なメールのみ確認　□確認していない
(11) 添付ファイルの暗号化　□頻繁に　□時々　□暗号化をしたことがない
(12) Cc: と Bcc: の使い分け　□使い分けている　□気にしたことがない　□Cc: Bcc: 知らなかった
(13) 外部にメール転送　□自動転送　□手動転送　□していない

場面４

(14) フィッシング手口　□知っていた　□知らなかった
(15) 届いたメール　□必ず送信元 / 者を確認　□送信者のみ確認　□全く確認しない
(16) メール本文にリンク　□注意している　□気にしない　□クリックしない
(17) 本文が怪しいメール　□迷わずゴミ箱へ　□特に疑わない
(18) メール通知の大切な事項　□グループウェアで確認　□メールを信じる　□無視
(19) ログイン履歴　□頻繁に確認　□時々確認　□していない
(20) パスワード変更　□３ヶ月に１回程度　□年１回程度変更　□全く変更していない
(21) 全学認証 ID のパスワード　□学外では未使用　□学外でも使用　□分からない
(22) 学外システムの ID/ パスワード　□確実に把握　□ほぼ把握　□必要な時思い出す

場面５

(23) 学外への重要情報の持ち出し　□一度も無い　□時々ある　□頻繁にある
(24) USB の利用頻度　□一度も無い　□時々ある　□頻繁にある

その他

(25) 重要情報を含むファイル　□名前で区別　□フォルダを分ける　□意識したことが無い
(26) 作成過程のファイル　□確実に削除　□すべて残している　□意識したことが無い
(27) ゴミ箱　□毎日空に　□時々空に　□意識したことが無い
(28) セキュリティ関連情報（グループウェアの掲示）　□すべて確認　□読んでいない　□意識したことが無い

図４　情報セキュリティ講習会でのチェックシート

5 まとめ

ネットワークシステムを安全で安定して利用するためには，全体像を正確に把握し管理対象を明確にしておくことが重要である．今回の再設計・再構築の取り組みを通じて附属学校ネットワーク全体を把握すると同時に，セキュリティポリシーの策定，それにもとづいた管理運用体制の確立など最低限の環境は整った．附属学校でセキュリティ対策の実施，構成員へのセキュリティ教育，運用管理，利用支援が担える人材の育成が急務であることは言うまでもない．今後タブレットや電子黒板など ICT を活用した授業が急増すると考えられ，益々安全で安定したネットワーク環境を維持することが重要となる．このため，総合情報センターでの管理運用ノウハウや監視・管理システムを活用すると同時に，新しい技術に関する情報を共有することが必要であると考えている．

また，本学が 2014 年度から実施している上位ネットワーク回線を実際に切断した「ネットワーク防災訓練」において，現場教職員と総合情報センタースタッフが連携して，回線トラブルや停電発生時の対応訓練を実施する予定である．さらに，災害時避難場所となる附属小学校・中学校において，避難住民に対して無線サービスを提供することを朝倉地区も含め検討している．

参考文献

[1] 総務省，教育分野における ICT 利活用推進のための情報通信技術面に関するガイドライン（手引書）2013 [小学校版]

[2] 総務省，教育分野における ICT 利活用推進のための情報通信技術面に関するガイドライン(手引書) 2014 [中学校・特別支援学校版]

[3] 佐々木正人，豊永昌彦, 回線切断を含むネットワーク防災訓練に関する報告，大学 ICT 推進協議会 2014 年度年次大会（宮城県仙台市），2014