初等教育機関におけるネットワーク分離の事例報告

松井　聰治 [1], 佐藤　隆士 [2]

1) 大阪教育大学　情報企画室
2) 大阪教育大学　情報処理センター

kmatsui@cc.osaka-kyoiku.ac.jp

Case reports of network separation in elementary school

Kikuji Matsui [1], Takashi Sato [2]

1) Information Planning Office, Osaka Kyoiku University
2) Information Processing Center, Osaka Kyoiku University

概要

初等中等教育機関において、情報セキュリティ対策から目的別にネットワーク分離が必要となっている。大阪教育大学附属学校においても、限られた予算の中でネットワーク分離を進めている。ネットワーク分離を実施する際の気づきや分離後の運用状況について報告する。

1　背景

初等中等教育機関では、最近の情報セキュリティ対策への対策のために教育情報セキュリティポリシーのためのガイドライン[1]を発出し、各学校及び学校を統括する機関に対してセキュリティ対策を呼び掛けた。

その中で、校務系ネットワークと学習系ネットワークについては完全に分離するとともに、校務系においてもインターネット接続可能なネットワークとインターネット接続が不可能なネットワークにわけるよう指針が示された。

本論文では、その指針に基づき、大阪教育大学附属天王寺小学校（以下，附属天王寺小学校と記す）において実際に構築して得た知見や今後に向けた課題をまとめたものを述べる。

2　着手前の状況

教員が使用するパソコンは、校務や授業指導のために一人一台所有している。端末の OS は Windows Home 版であるため一元管理はできていない。

職員室は、机が島状に構成され、各島にスイッチングハブがある。常勤教員の机には LAN コンセントがあり、ハブは机コンセントにつながっている。その他の 2 島（管理職、用務員及び共用 PC）及び複合機へはハブから直結している。

事務室には、VPN ルータがあり、事務職員は、大学本部から VPN 接続したパソコンを使用しており、ネットワークは、独立している。

ネットワークアドレスはグローバル IP アドレスを静的に付与している。過去には台帳管理が煩雑という声をいただいたこともある。学校内のラックには教材と校務資料が入った NAS があり、数 TB 程度のデータが存在する。

教室には 2012 年に無線 LAN を整備している。無線 LAN はプライベート IP アドレスが動的に配布され、天王寺地区の小中高で共通の管理をしている。

3　設計

校務支援システムのサーバ本体は、本学のメインキャンパスである柏原キャンパスに導入し

ており、附属天王寺小学校の利用者はキャンパス間ネットワーク経由で利用する。

3.1　サーバ及びルータ

サーバは次のとおり整備している。

（1）仮想化基盤システム

仮想化基盤システムの性能を表 1 に示す。

次項（2）～（4）についてを仮想マシンとして収容している。

（2）校務システム（DB サーバ・AP サーバ）

（3）HardLockey 管理サーバ

（4）Active Directory 兼 DNS サーバ

以下の（5）から（7）は、物理サーバで構築している。物理サーバの性能を表 2 に示す。

（5）WSUS 兼ウイルス対策ソフト管理サーバ

（6）学校 NAS 用ストレージサーバ

（7）バックアップサーバ（1 次・2 次用）

サーバのうち、（6）学校 NAS 用ストレージサーバ、（7）バックアップサーバ（1 次・2 次用）については FreeBSD で構築している。

ルータについては、ネットワークごとに設置している。

3.2　柏原キャンパスの接続構成

（1）校務系ネットワーク

校務系ネットワークは、外部からインターネット利用ができないネットワークである。附属学校の校務系ネットワークと相互に接続している。サーバのうち、（2）校務システム、（3）HardLockey 管理サーバ、（4）Active Directory 兼 DNS サーバ、（6）学校 NAS 用ストレージサーバが接続される。

（2）校務外部接続系ネットワーク

校務外部接続系ネットワークは、外部からインターネットが利用できるネットワークである。

校務システムのインターネット接続口や各学校からのメール等インターネット目的で利用する。サーバのうち、（5）WSUS 兼ウイルス対策ソフト管理サーバが接続される。

（3）管理系ネットワーク

管理系ネットワークは、バックアップや保守のためのネットワークである。

3.3　附属天王寺小学校の接続構成

（1）職員室ネットワーク

職員室は、原則校務系ネットワークである。ネットワーク分離のために、株式会社 JMC HardLockey を使用している。USB ドングルが接続されていなければ、校務系システムへは続できない。

（2）職員室パソコン

ネットワーク更新に際して、教員のパソコンを Microsoft Surface Laptop へ更新して Active Directory 及び USB デバイスによる多要素認証に対応している。

（3）変更対象外の機器

事務職員及び教室系ネットワークについては現状維持で今回は変更を行わなかった。

表 1　仮想化基盤システムの性能

型番	HP ML350 Gen10
CPU	Intel Xeon Bronze 3106
RAM	32GB(PC4-2666V-R 16GB*2)
HDD	2TB(SATA 2TB*2,RAID1構成)
OS	Vmware vSphere 6.7

表 2　物理サーバの性能

型番	組み立てのためなし
CPU	Intel Core i3-8100
M/B	Asus B360M-A
RAM	16GB (PC4-28800)
SSD	500GB(M.2)
HDD	6TB(バックアップサーバは12TB)
OS	Windows Server 2019 又は FreeBSD 12

4　実装

本実装は、2019 年 2 月から 3 月にかけて構築をおこなった。構築にあたり複数の課題が出てきたので列挙する。

4.1 DNS サーバ

Active Directory を設置するため、基本的にはドメインコントローラに DNS 機能が統合されておりクライアントは利用するが、ドメインコントローラは、校務系ネットワークに所属するため、外部情報を参照できない。Forwarder についても、ネットワーク分離していると上位 DNS に直接アクセスできないために代理応答の DNS が必要となり、今回はルータ機能で実現している。

4.2 複合機

所属が異なるネットワークから複合機への印刷やスキャンデータの取り出しが要望としてあるが、ネットワーク分離を徹底した場合利用できなくなる。

今回は、HardLockey により複合機やルータ側でなくクライアント側でネットワーク制御ができることで対応している。

4.3 ネットワーク回線帯域不足

運用を開始して、ネットワーク帯域が不足していることが顕著化した。次項以降の様々な症状の根本原因といえる。根本的な解決としては回線契約の更新を待っている状況である。

4.4 Active Directory 冗長化

ネットワークが遅い事象に悩まされたなか、様々な対応をした中の一つである。当初、サーバはセンターである柏原のみで運用していたが遠隔地の遅延も考え、附属学校にも設置している。設置後は、遅延状況のモニタにも利用できるようになり、利便性が向上している。

4.5 既設 NAS のデータ移行

附属学校には、6 年間の児童の活動について蓄積データがあり、大量のデータがある。新たなストレージサーバに集約するためにネットワーク経由でコピーを実施したが、大容量のため移行に 1 週間程度を要した。附属学校が使用する回線のスループットなどを予め把握しなかったため、理論値に近い値が出ると錯覚したことが原因である。

4.6 ユーザプロファイル

教員用パソコンにデータを置くのを最低限にとどめて、利便性と安全性を確保するためにユーザプロファイルはフォルダーリダイレクトを多用している。

実運用を始めたのち、ユーザプロファイルを運用すると非常に端末のレスポンスが遅いことがわかり、調査を行った結果、複数の点で課題が出てきたため対応している。

一点目は、IME 辞書がフォルダーリダイレクトの対象となっていたことである。文字入力の際に遅延が発生しており実用に耐えられなくなっていたため、フォルダーリダイレクトの範囲を変更して改善している。

二点目は、ネットワーク利用前提のソフトウェアが、校務用ネットワーク内でネットワーク探索を続けている事象である。グループポリシー等でソフトウェアや機能を無効にするなどにして改善している。

4.7 ハードウェアトラブル

最近のノートパソコンには有線 LAN 端子がついていない機種も多く、今回導入した教員用パソコンについても、有線 LAN 端子がついていない端末であったため別売の純正 Dock を購入して有線接続を可能にしている。Windows 起動直後に、LAN によるネットワーク接続がきちんと認識しないことがまれに発生し、ログイン障害などになっている。

4.8 既存端末

今までの教員のパソコンは、リース調達ではないため、引き続き学校内にある。今後は学習用パソコンの教材研究用として再利用している。

5 まとめと今後の展望

本稿では、附属学校での移行事例をもとに対応した課題について事例報告を行った。情報セキュリティ対策のためにはネットワーク分離が

必須であり、利便性を損ねない中での取り組みがより重要となっている。

本学では、附属学校が所在する地区とSINETを直結する準備を進めており、その背景も含め、附属天王寺小学校での事例をもとに本学の他の附属学校園においても、課題を昇華しながら対応を進めていく。

謝辞

校務支援システム及びHardLockeyの環境を構築頂いた株式会社ライオン事務器に感謝する。

年度末及び年度初めの多忙な中、移行作業に協力頂き、問題解決に協力頂いた大阪教育大学附属天王寺小学校に感謝する。

参考文献

[1] 「教育情報セキュリティポリシーに関するガイドライン」公表について <http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm> 2019年9月20日アクセス.