事務局ネットワークのプライベート IP アドレスへの移行

早坂 成人 [1)], 佐藤 之紀 [1),2)], 松本 浩明 [2)],小師 隆 [2)] ,三林 光 [2)]

1) 室蘭工業大学　情報メディア教育センター
2) 室蘭工業大学　技術部

hayasaka@mmm.muroran-it.ac.jp

Transition to Private IP Address of Administration Bureau Network

Narihito Hayasaka [1)], Yukinori Sato [1),2)], Hiroaki Matsumoto [2)], Takashi Komoro [2)]
, Hikaru Mitsubayashi [2)]

1) Center for Multimedia Aided Education, Muroran Institute of Technology.
2) Technical Division, Muroran Institute of Technology.

概要

学内には大学固有の重要情報があるが、それらの情報を集約して保管している部署は事務局である。これらのセキュリティを高めるために事務職員が利用している ICT 機器をプライベート IP アドレスへ移行することにした。事前に移行が可能な機器か棚卸を行ったり、移行時に必要な移行手順書を準備し移行を試みたが、棚卸作業が不十分であったり、学内限定のホームページを閲覧できないなどのトラブルがいくつか発生したが、重要情報や機器を安全なネットワークへ移行することが出来た。

1　はじめに

大学にネットワークが導入され、多くのサーバや PC がネットワークに接続されて久しい。本学は比較的早い時期にIPアドレスを取得し潤沢に保持しているため、どのネットワーク機器にもグローバルIPアドレスを設定して利用してきた。しかし情報セキュリティの向上のために情報メディア教育センターが中心となって近年導入したシステムは、プライベートIPアドレスを活用し出している。

学内には多くの個人情報や成績などの重要情報が集約されて保管している部署が事務局である。このため事務職員が利用している PC や NAS をプライベートIPアドレスへ移行して情報セキュリティの向上を図るべきと考え、本学の技術部と協力し移行を行うことにした。業務で活用している機器の一斉移行には事前に検討すべき事柄も多く、十分な事前準備が不可欠である。ただし移行予算を計上していなかったため、外部コンサルタントの協力を得ることなく、約半年をかけて計画立案から全て自前で移行を行った。本論では昨年実施した移行について事前準備内容や実施時に判明した問題点について報告する。

2　検討チームによる移行検討

検討がスムーズに進むように CISO（最高情報セキュリティ責任者）の下に検討チームを設置した。メンバーは情報メディア教育センター教員 2 名、事務職員 8 名（各課から 1 名）、技術部職員 1 名の 11 名である。

検討チームによる検討会は 8 月から 10 月にかけて 3 回開催して、初回は移行の必要性を説明した上で協力を要請し、次の内容について検討を行った。

(1) 移行先ネットワークの構成
(2) IP アドレスの管理方法
(3) 通信ポリシー

移行先ネットワークの構成は現状通りで良いか検討し、混乱をさけるためなるべく変更が無い構成とすることにした。また ICT 機器の登録時に割り当てるIPアドレスの管理が十分に出来ていない部署があったため、管理を技術部に委託することにした。最後にセキュリティ強化のための通信ポリシーを検討し、グローバル IP アドレスからプライベートIPアドレスへのアクセスは禁止とした。

2 回目と 3 回目は次節の移行機器の棚卸状況とヒアリング結果の確認および移行を 2 回に分けて実施することや学内スケジュールを考慮した上で

11 月に実施することを決定した。

3 事前準備

移行時のトラブルを未然に防止するため、必要となる事項を検討して次の事前準備を行った。

3.1 移行機器の棚卸

既存ICT機器の一覧表を作成して対象部局に配布し、対象機器について移行が可能か 9 月に棚卸を実施した。基本的に移行可能機器は全て移行を前提として洗出した。

多くの Web サーバは移行対象外のネットワークに接続されているが、たまたま事務職員用ネットワーク内に接続されていた一部業務用サーバとテレビ会議システムなどは対象外とした。また外部に接続元 IP アドレスを登録している PC も移行対象外とした。このほかにも接続元 IP アドレスを登録している PC があったが、本学のプロキシサーバの IP アドレスを登録していたため、それらは移行対象とした。

各課で実施した棚卸結果が適切な選定内容となっているか確認するため、情報メディア教育センターがヒアリングを行った。このヒアリングを実施しても移行可能か判断できない機器は、納入業者に再度確認を依頼し最終決定を行っている。

3.2 移行手順書の作成

移行時の問い合わせを最小限に抑えるために移行時に必要となる設定方法や設定内容を確認するための手順書として、次のものを事前に作成し対象部局に配付した。

(1) IP アドレスの確認方法
(2) プロキシの設定方法
(3) プリンタの設定方法
(4) NAS の設定方法
(5) 複合機のネットワーク設定の変更方法

手順書は職員自らが確認や設定変更が出来るように用意した(1)(2)(3)。また課内の管理者が必要となる手順書も別途用意した(4)(5)。

複合機は利用者毎の使用データを毎月学外のサーバへ自動転送する仕組みとなっているため、納入ベンダーに送信方法を確認し、手順書に反映した。

3.3 移行当時の役割分担確認

移行日は午前 8 時までに対象スイッチ内の MAC アドレステーブルなどの情報を削除する担当者。また問い合わせは情報メディア教育センタースタッフ 3 名と技術部職員 3 名で対応し、始業前の午前 8 時に情報メディア教育センターに集合することや、電話相談受付者と現地での設定対応者など、前日に役割分担を確認した。

4 移行時の問題点

移行時あるいは移行後に次の不具合があった。

(1) 移行リストから漏れていた機器が 11 台あり、プライベート IP アドレスが自動的に割り当てられなかった。
棚卸時には既に利用していない機器は削除フラグを、利用者や利用場所に変更があるものは修正をした上で、移行可能か移行フラグの選択を依頼していた。この一覧上では全機器の棚卸は完了していたが、実際には管理元の所属名が旧部署の機器が含まれていたため、棚卸結果に漏れがあった。

(2) 移行した PC で学内限定のホームページが閲覧できなくなったり、ホームページの更新作業が出来なくなったりした。
学内のみから閲覧を可能とするアクセス制限やホームページ更新作業の接続元制限に IP アドレスを使用していたが、プライベート IP アドレスを追加したり、グローバル IP アドレスからプライベート IP アドレスに変更し忘れたことが原因だった。

(3) NAS が利用できなくなった。
同一スイッチに接続されている PC と NAS は正常に利用できたが、異なるスイッチに接続している場合は利用することができなかった。
ネットワーク上部のスイッチの設定漏れが原因だった。

5 おわりに

移行は 2 回に分けて実施したので、前節で述べた不具合点は初回のみだけであり、その一週間後に行った移行 2 回目はトラブル無く実施することが出来た。

また移行時の棚卸作業で漏れが発生した根本原因は、ネットワークに接続している機器情報が一切更新されていなかったことにある。このため IP アドレスの管理者となった技術部と協力して、年 1 回管理者等の変更確認を実施している。

いくらかのトラブルはあったものの、学内の多くの重要情報やそれらを扱う ICT 機器を安全なネットワークへ移行することが出来た。