IPv4 学内ネットワークにおけるプライベート IP アドレスへの移行

松井　聴治 [1)], 尾崎　拓郎 [2)], 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

IPv4 Intranet Change Over from Global IP Address to Private IP Address

Kikuji Matsui [1)], Takuro Ozaki [2)], Takashi Sato [2)]

1) Information Planning Office, Osaka Kyoiku Univ.
2) Information Processing Center, Osaka Kyoiku Univ.

概要

大阪教育大学では、2017 年 2 月のシステム更新に合わせて、IPv4 ネットワークをプライベート IP アドレス中心のネットワークに変更した。変更に当たって、留意した既存ネットワークとの継続性や変更内容について報告する。

1　背景

大阪教育大学では、1991 年 7 月に class B を 1 セグメント分のグローバル IP アドレスを取得した。情報処理センターでは、取得したグローバル IP アドレスを管理しており、利用者に対して原則としてグローバル IP アドレスを付与するとともに、大阪教育大学キャンパスネットワーク「GRAPES」としてレイヤ 3 スイッチやルーターといったネットワーク機器でグローバル IP アドレスのルーティング環境を提供している。また、学内規程により、IP アドレス変換やルーティングを行うブロードバンドルーターのような機器の利用者による接続を禁止している。これにより、ネットワークを単純化することができ、ログの把握及び到達性の確保を重視してネットワーク整備を行ってきた。

管理体制に転機が訪れたのは、2013 年 11 月の学術関係機関で起こった情報漏えい事件である[1]。短期的には、複合機を含む既存端末が組織外からのアウトバウンド通信が遮断されていることを確認した。しかし、そもそもプライベート IP アドレスを利用していれば、IP マスカレードにより組織外からの直接攻撃を受けることは無かったということになり、グローバル IP アドレスの管理状況把握を確実に実施し、グローバル IP アドレスが真に必要となる端末以外のプライベート IP アドレスへの付け替えについて検討が始まった。

本稿では、2017 年 3 月稼働の新ネットワーク(GRAPES)及び教室系システムでのプライベート IP アドレスの実装事例紹介と全学展開への取り組み状況を紹介する。

2　実装内容

2.1 ハードウェア構成

本学のハードウェアは、全学ファイアウォール(PaloAlto PA-3020)及び、当該機の下流にコアスイッチ(Cisco Catalyst 4506-E ,4500-X)により構成されている。構成を図 1 に示す。他キャンパスへの通信についても、コアスイッチを経由しキャンパス間の L2-VPN 網によりルーティングしている。

2.2 アドレス構成

利用者端末に配布するアドレスは、グローバル IP アドレス（150.86.X.Y、以下「現アドレス」という。）を使用しているが、これをプライベート IP アドレス（10.86.X.Y、以下「新アドレス」という。）へ移行する。

学内については、利用者端末は現アドレス及び新アドレスのいずれの通信も区別なく対応し、アドレス変換を行うことなくサーバと通信を行う。

学外については、アドレス変換を行い、新アドレス（10.86.X.Y）をグローバル IP アドレス（150.86.0.X、以下「外部用アドレス」という。）に変換して通信する。

2.3 コアスイッチの設定

コアスイッチは、ルーティングが有効な VLAN ごとに VLAN Interface が存在する。移行期間は同一 VLAN 上で現アドレスと新アドレスが混在できる環境を用意できる環境設定にしている。具体的

には、コアスイッチにある VLAN Interface の Secondary Address 機能により、単一 VLAN 上で複数ネットワークのゲートウェイ IP を設定した。設定を図 2 に示す。コアスイッチでは、現アドレス・新アドレスの区別なくルーティング処理ができるようになり、上位ネットワークへデータ転送が可能となっている。

2.4 ファイアウォールの設定

イントラネットから組織外のグローバルなインターネットへ接続するにあたっては、ネットワークアドレス変換が必要となる。設定を図 3 に示す。アドレス変換については、ファイアウォールで発信元プライベート IP アドレスのサブネットごとにグローバル IP アドレスに IP マスカレードを行っている。

3 移行手順

移行の順序としては、以下のとおり実施する。

ファイアウォール、コアスイッチについては現アドレス及び新アドレスが共存できるように設定を実施する。

パソコン教室については、新システムの設計に含め実施する。利用者端末のうち DHCP 管理のネットワークは、サーバ側の設定変更のみで変更可能であるので行事などを加味して変更作業を実施する。

利用者端末のうち静的 IP アドレス設定により管理しているネットワークは、移行期間を設け、期間中は現アドレス及び新アドレスの両方が利用できるようにした。また、移行期間内で利用者自身により新アドレスに設定変更作業を実施する。

4 まとめ

本学のプライベート IP アドレス化に関する取り組みと紹介した。既存 VLAN 構成を保持しつつ移行することにメリットがある。本実装により、パソコン教室などの新規設備については新アドレスで安定稼働している。利用者への新アドレス移行は緩やかに進めているところである。現アドレスが急に使えなくなるわけではないため、サポート負荷も現状では重くはなっていない。今後も着実にプライベート IP 化を進めていく。

また、プライベート IP 化が完了したときには、本学の利用者向けグローバル IP アドレスはクラス C 程度に圧縮できる見込みであり、余剰空間を活用した研究などが実施できる見込みである。

参考文献

[1] プレス発表　複合機等のオフィス機器をインターネットに接続する際の注意点 <https://www.ipa.go.jp/about/press/20131108.html> 2017 年 10 月 2 日アクセス.

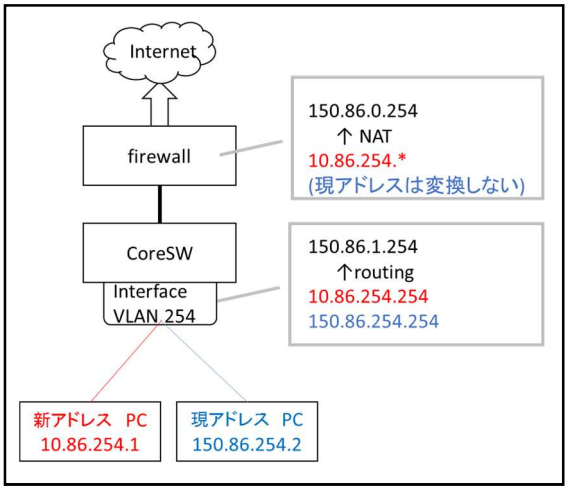

図 1　本学のネットワーク構成

```
#show running-config

!
interface Vlan254
 ip address 150.86.254.251 255.255.255.0
secondary
 ip address 10.86.254.251 255.255.255.0
 standby version 2
 standby 254 ip 10.86.254.254
 standby 254 priority 150
 standby 254 preempt
 standby 1254 ip 150.86.254.254
 standby 1254 priority 150
 standby 1254 preempt
!
```

図 2　コアスイッチにおける設定(抜粋)

```
> show running nat-policy
nat254 {
        nat-type ipv4;
        from inside;
        source 10.86.254.0/24;
        to outside;
        to-interface;
        destination any;
        service  any/any/any;
        translate-to "src: 150.86.0.254
(dynamic-ip-and-port) (pool idx: 1)";
        terminal no;
}
```

図 3　ファイアウォールにおける設定(抜粋)