

## キャンパスネットワークにおける IPv6 の導入とその課題

佐藤 彰洋, 戸田 哲也, 福田 豊, 中村 豊

九州工業大学 情報科学センター

satoh@isc.kyutech.ac.jp

**概要:** IPv4 アドレスの枯渇を期に, IPv6 のサポートやサービスの提供の必要性が高まっている. キャンパスネットワークも例外ではなく, 学生への教育の観点から早期の対応が求められている. 効率的な IPv6 の導入及び IPv4 との共存を実現するためには, それに伴い発生する諸問題を広く共有することが重要となる. 本稿では, IPv4 で構築されたキャンパスネットワークに IPv6 を導入するにあたり, 実証実験から得られた知見や課題を報告する.

### 1 はじめに

IPv4 アドレスの枯渇を期に, IPv6 のサポートやサービスの提供の必要性が高まっている. キャンパスネットワークも例外ではなく, 学生への教育の観点から早期の IPv6 への対応が求められている. 多様なシステムが混在するキャンパスネットワークにおいて, その安定性を維持したまま IPv6 の導入を実現するためには, 段階的な対応による知見の蓄積と課題の解決が不可欠である.

本稿では, IPv4 で構築されたキャンパスネットワークの一部セグメントに IPv6 を導入するにあたり, 実証実験を通じて得られた知見や課題を述べる.

### 2 本学のネットワーク

本学のネットワークの概要を図1に示す. 本学は福岡県内にある3つのキャンパスからなる工学系総合大学である. 著者らが所属する情報科学センターは, 情報教育を行うために戸畑・飯塚の2キャンパスに設置された教育用計算機システムの運用を行っている.

教育用計算機システムの目的は, 情報処理教育を学ぶうえで必要不可欠な実習のための環境を学生に提供することである. 本システムは, ネットワーク起動型のディスクレス端末群と計算機室に設置してある各種サーバ群とを高速ネットワークで相互に接続することにより, 集中的な管理を実現している. それらの端末群は, 学生の利用を目的とした「利用者用端末」と, 職員の利用を目的とした「管理者用端末」に大別される. また, Windows Vista と KNOPPIX のデュアルブートを採用することで, 講義内容に応じた OS の選択が可能となっている.

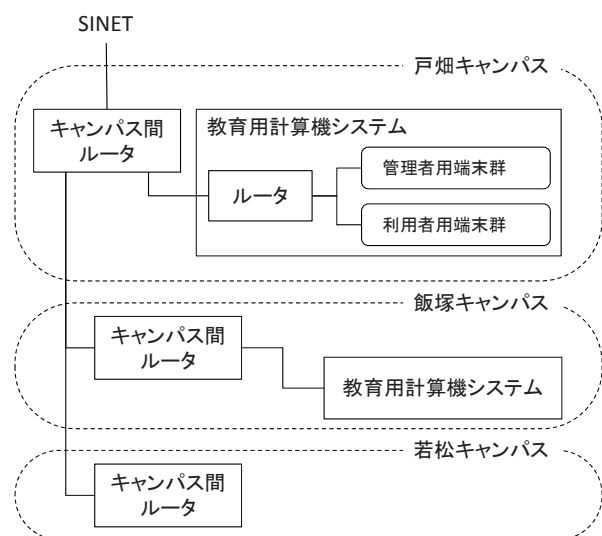


図1 本学のネットワークの概要

### 3 IPv6 ネットワークの導入

本節では, まず本学の教育用計算機システムに IPv6 を導入するための調査と設計を述べ, 次にそれにより得られた知見と課題をまとめる.

#### 3.1 調査と設計

Nii より本学に割当てられた IPv6 アドレスは, 約 65000 のネットワークに該当する, プレフィックス長が 48 の「2001:02F8:100F::」である. それに対して VLAN の tag は仕様上最大で 4000 程度であるため, 従来の IPv4 のように VLAN に依存したネットワークの構築は困難である.

始めに検討すべき点は, IPv6 アドレスの割当て方針である. IPv4 と IPv6 の共存を考えた場合, IPv4 アドレスに加え, 膨大な量の IPv6 アドレスの管理が必要となるため, その作業は煩雑になることが懸念される. 本学では IPv6 アドレスでキャンパス及び IPv4 アドレスの情報を表現するこ

とにより、それらの対応関係を明確にした。

ネットワークの構成や規模に基づいて適切なプロトコルを選択することは、その性能を担保するうえで重要となる。実証実験で対象とするネットワークは、小規模でありルータの数は 10 に満たないことから、その数と設定の容易性を考慮して RIPng[1]を採用した。

教育用計算機システムで考慮すべき点は、端末の保護と管理である。潤沢なアドレス空間を持つ IPv6 では、従来のローカル・グローバルの分類を持たず、全ての端末に対する外部からの通信が可能となるため、端末に対するセキュリティ保護の対策が必要である。加えて、端末に自身のアドレス、デフォルトゲートウェイや DNS サーバのアドレスを自動設定する機能、それらを管理する機能が必要となる。

端末に対するセキュリティ保護の対策に関しては、教育用計算機システムに外部からの通信が必要となるサービスが存在しないことから、DNS を除く外部からの IPv6 による通信を全て遮断することにした。端末に対する自身のアドレスとデフォルトゲートウェイのアドレスの自動設定には RA[2]、DNS サーバのアドレスの自動設定には DHCPv6[3]を用いた。しかしながら、RA によるアドレスの自動設定は、ステートレスに行われるため、障害が発生した端末の特定が困難となる。その問題を解決するため、佐賀大学で開発が進められ、そのソースが一般に公開されている Opengate[4]による端末の認証を導入した。

### 3.2 知見と課題

前節で構築したネットワークにより、教育用計算機システムの端末で IPv6 による通信が可能となった。現状、多くの機器で IPv6 への対応が進み、その設定も容易となっている。本実証実験により得られた知見と課題は次の通りである。

**DNS :** ホスト名と IP アドレスの名前解決については、IPv4 の A と IPv6 の AAAA のように、利用するレコードがそれぞれ異なる。調査の結果、IPv4/IPv6 デュアルスタックでは、Windows、Linux 及び Mac OS において IPv6 の AAAA レコードを優先することが明らかになった。すなわち、IPv4 と IPv6 の両通信が可能な環境下では、多くの OS で IPv6 による通信を優先することになる。

**DHCPv6 :** 現在、DHCPv6 に初期設定で対応している OS は Windows 7 のみである。Linux や

Mac OS は DHCPv6 クライアントのインストール、Windows Vista は設定の変更が必要となる。DNS サーバのアドレスを端末に自動的に設定できる機構は、他に LLMNR や mDNS が開発されているが、これらも同様の課題を抱えている。近年、その自動設定に RA を利用する機構が標準化された[5]。しかしながら、未だ実装は無く、各社による一刻も早い製品化が期待されている。

**認証 :** Opengate は、不特定多数による利用が想定されるネットワークの為の、Captive Portal 型の認証ゲートウェイシステムである。IPv4/IPv6 デュアルスタックの端末に対して、IPv4 による最初の Web アクセスに割込みをかけ、認証ページを表示することによりユーザ ID とパスワードの入力を促す仕組みである。教育用計算機システムの端末は全て IPv4/IPv6 デュアルスタックに対応しているため、Opengate を使った認証で問題は発生していない。本格的な運用を想定した場合、IPv6 のみに対応した端末の認証が必要となるが、それに対応できる Web 認証システムは存在しないのが現状である。今後、802.1x などの利用について検討する必要がある。

## 4 おわりに

本稿では、IPv4 で構築されたキャンパスネットワークの一部セグメントに IPv6 を導入するにあたり、実証実験を通じて得られた知見や課題を述べた。実証実験の結果、現在 IPv6 の導入には端末に対する DNS サーバのアドレスの自動設定及び IPv6 のみに対応した端末の認証に課題があることが明らかになった。

今後も継続的な IPv6 の対応範囲の拡大と定期的な報告を行う予定である。

### 参考文献

- [1] G. Malkin et al., “RIPng for IPv6”, RFC 2080, 1997.
- [2] T. Narten et al., “Neighbor Discovery for IP Version 6 (IPv6)”, RFC 2461, 1998.
- [3] R. Droms et al., “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC 3315, 2003.
- [4] Opengate, <http://www.cc.saga-u.ac.jp/>
- [5] J. Jeong et al., “IPv6 Router Advertisement Option for DNS Configuration”, RFC 5006, 2007.