



キャンパスネットワークにおける IPv6 の導入

佐藤 彰洋¹

戸田 哲也²

福田 豊³

中村 豊⁴

1 はじめに

IPv4 (Internet Protocol, Version 4) [1] と共に発展してきたインターネットは、大きな過渡期に差し掛かっています。IPv4 アドレスの枯渇が懸念され、その延命処置として様々な対策が講じられてきましたが、2012 年 2 月 3 日に IANA (Internet Assigned Numbers Authority) [2] の管理するアドレスの在庫が無くなりました。そのため、RIR (Regional Internet Registry) が管理する在庫を割り振っているのが現状です。IPv4 アドレスの残数は、次のウェブサイトで確認することができます [3]。

IPv4 アドレス枯渇の根本的な解決策は IPv6 (Internet Protocol, Version 6) [4] にあり、各 ISP (Internet Services Provider) は次々と IPv6 を用いたサービスを発表しています。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ます。事務・教育・研究などに関連する多種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 に対応するためには、区間を限定した導入による知見の蓄積と課題の解決が不可欠です。

本稿では、既に IPv4 で構築済みの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について述べます。

2 本学のネットワーク

本学のネットワーク構成を図 1 に示します。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す。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ます。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す。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ます。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」に大別されます。また、Windows Vista と KNOPPIX [5] 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ます。

今回は、戸畑キャンパスの管理者用端末群において IPv6 を利用した通信の実現を目指します。具体的には、図 1 の灰色で示した範囲に IPv6 を導入します。

¹情報科学センター 助教 satoh@isc.kyutech.ac.jp

²情報科学センター 技術専門職員 toda@isc.kyutech.ac.jp

³情報科学センター 助教 fukuda@isc.kyutech.ac.jp

⁴情報科学センター 准教授 yutaka-n@isc.kyutech.ac.jp

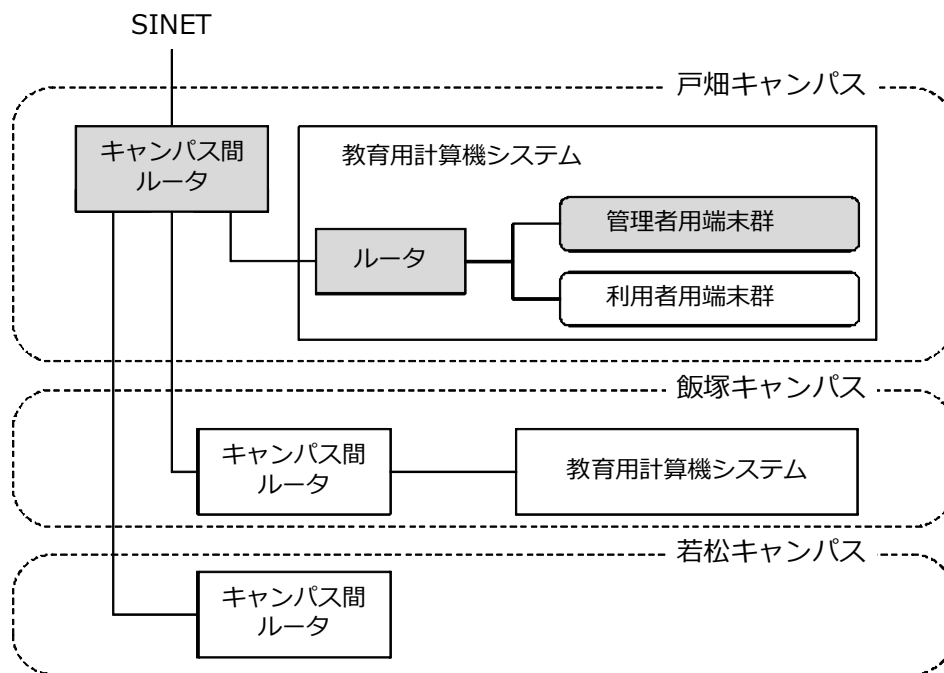


図 1: 本学のネットワーク構成.

3 IPv6 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ます。

3.1 調査と設計

IPv6 を導入するにあたり、特に検討したのは下記の点です。

アドレスの割り当て：

Nii (National Institute of Informatics) [6] 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::」です。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す。また、VLAN の代わりに SND (Software Defined Networking) を利用する案も考えられますが、費用面から見て現実的ではありません。始めに検討すべき点は、IPv6 アドレスの割当ての方針です。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ます。図 2 で示すように、IPv6 アドレス内にキャンパス及び IPv4 アドレスの情報を組み込むことで、それらの対応関係を明確にしました。

ルーティングプロトコル：

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ります。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 [7] を採用しました。

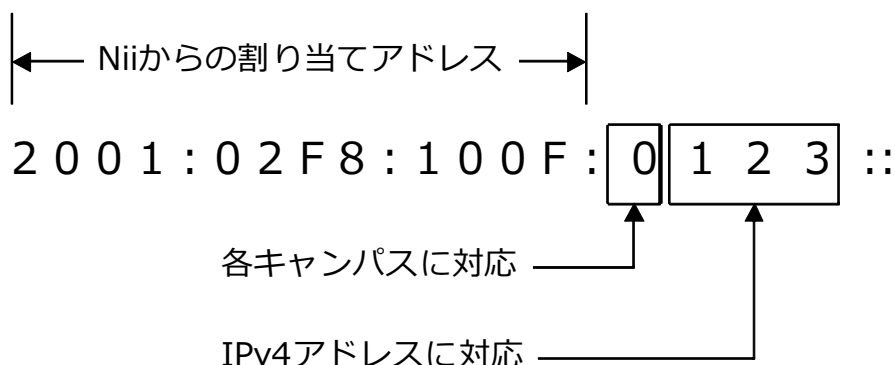


図 2: IPv4 と IPv6 の対応関係を考慮したアドレスの割当て。

端末の保護と管理：

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す。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の対策が必須となります。加えて、端末に自身のアドレス、デフォルトゲートウェイ、及び 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ります。

端末に対するセキュリティの対策に関しては、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ました。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 (Router Advertisement) [8]、DNS サーバのアドレスの自動設定には DHCPv6 [9] を用いました。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ります。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 [10] による端末の認証を導入しました。

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管理者用端末で IPv6 による通信が可能となりました。現状、多くの機器で IPv6 への対応が進み、その設定も容易になってきているようです。本実証実験により得られた知見と課題は次の通りです。

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ります。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りました。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ります。

DHCPv6：

DHCPv6 に初期設定で対応している OS は Windows 7 と Windows 8 のみです。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ります。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 (Link-Local Multicast Name

Resolution) [11] や mDNS (Multicast DNS) [12] が開発されていますが、これらも同様の課題を抱えているのが現状です。2011 年に、その自動設定に RA を利用する機構が標準化されました [13]。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ます。

認証：

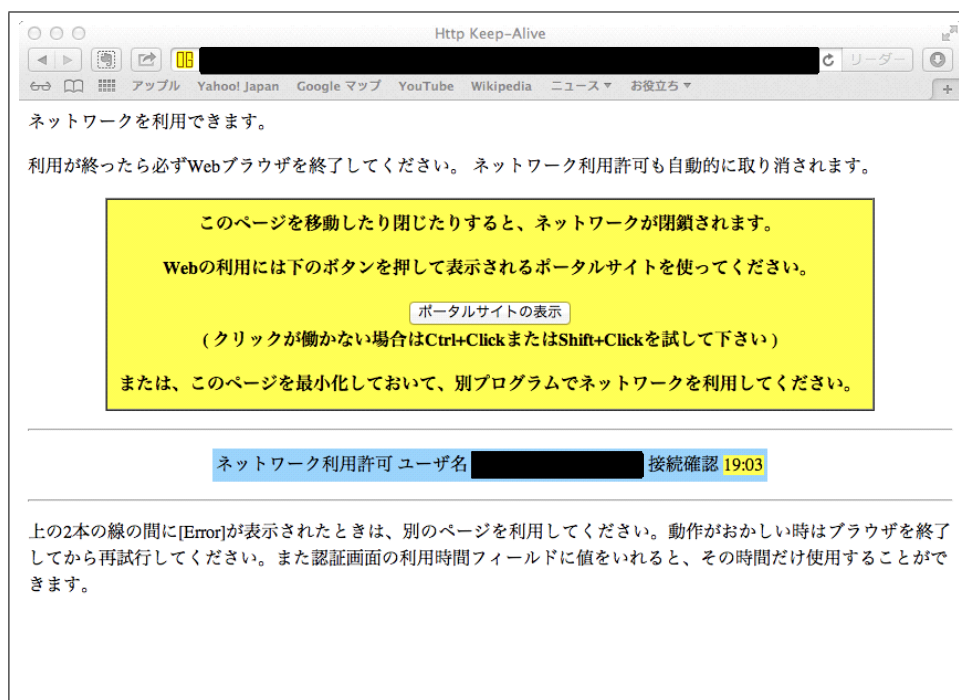
Opengate は、不特定多数による利用が想定されるネットワークの為に、Captive Portal 型の認証ゲートウェイシステムです。図 3 に、Opengate による認証の概要を示します。IPv4/IPv6 デュアルスタックの端末に対して、IPv4 による最初の Web アクセスに割込みをかけ、図 3(a) の認証ページを表示することによりユーザ ID とパスワードの入力を促す仕組みになっています。その認証が成功した場合、図 3(b) の認証成功ページが表示されると同時にネットワークの利用が許可されます。教育用計算機システムの端末は全て IPv4/IPv6 デュアルスタックに対応しているため、Opengate を使った認証で問題は発生していません。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りますが、その要求に対応できる Web 認証システムは存在しないのが現状です。今後、802.1x [14] などの利用について検討する必要があると言えます。

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ました。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りました。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す。



(a) 認証時の表示



(b) 認証後の表示

図 3: Opengate による認証.

参考文献

- [1] J. Postel. Internet Protocol Darpa Internet Program Protocol Specification. *RFC 791*, 1981.
- [2] Internet Assigned Numbers Authority. <http://www.iana.org/>.
- [3] IP アドレス枯渇問題を可視化：IPv4 枯渇時計.
<http://inetcore.com/project/ipv4ec/index.html>.
- [4] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. *RFC 2460*, 1998.
- [5] KNOPPIX Linux Live CD. <http://www.knoppix.org/>.
- [6] National Institute of Informatics. <http://www.nii.ac.jp/>.
- [7] G. Malkin and R. Minnear. RIPng for IPv6. *RFC 2080*, 1997.
- [8] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (IPv6). *RFC 2461*, 1998.
- [9] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). *RFC 3315*, 2003.
- [10] Opengate. <http://www.cc.saga-u.ac.jp/>.
- [11] B. Aboba, D. Thaler, and L. Esibov. Link-Local Multicast Name Resolution (LLMNR). *RFC 4795*, 2007.
- [12] Multicast DNS. <http://www.multicastdns.org/>.
- [13] J. Jeong, S. Park, L. Beloeil, and S. Madanapalli. IPv6 Router Advertisement Option for DNS Configuration. *RFC 5006*, 2007.
- [14] P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese. IEEE 802.1X Remote Authentication Dial in User Service (RADIUS) Usage Guidelines. *RFC 3580*, 2003.