慶應義塾における eduroam の IPv6 接続提供

大橋 真 [1)], 細川 達己 [2)], 金子 康樹 [2)]

1) 慶應義塾三田インフォメーションテクノロジーセンター
2) 慶應義塾インフォメーションテクノロジーセンター本部

{makoto1d,hosokawa,yasuki.kaneko}@keio.jp

A Report of IPv6 Usage on eduroam at Keio University

Makoto Ohashi [1)], Tatsumi Hosokawa [2)], Yasuki Kaneko [2)]

1) Mita Information Technology Center, Keio University
2) Information Technology Center, Keio University

概要

慶應義塾では 2015 年に eduroam JP に参加、外部との接続には SINET の eduroam アクセスネットワーク収容サービスを活用している。IPv6 での接続については本学におけるサービス開始当初から提供している。本稿では、本学における eduroam 環境の紹介および IPv6 と IPv4 の利用状況と、IPv6 接続環境の導入効果について報告する。

1 はじめに

慶應義塾では 2015 年 6 月に eduroam JP に参加、2015 年 9 月から試験運用を開始、2015 年 12 月に正式なサービスとして運用を開始した。

学内においては既に IPv4 と IPv6 のデュアルスタックでのワイヤレスネットワーク接続環境を提供していたため、同様の接続環境をサービス開始当初から提供することが可能であった。

2 システム構成

学内で運用しているアクセスポイントは、キャンパス毎に集中管理されており、メーカーも異なっている。

主要 6 キャンパスにて運用しているアクセスポイントは、2018 年 3 月末時点で合計 2,100 台以上となっている。

表 1. アクセスポイント導入台数
(2018 年 3 月末現在)

キャンパス	台数
三田キャンパス	552
日吉キャンパス	483
信濃町キャンパス	233
矢上キャンパス	375
湘南藤沢キャンパス	438
芝共立キャンパス	70
合計	2,151

2.1 外部ネットワークとの接続

外部との接続には、SINET の eduroam アクセスネットワーク収容サービスを活用している。

このサービスでは、グローバルな IPv4 アドレスとしてネットマスク 30 ビットのアドレスブロックを 1 つ、IPv6 アドレスとして 64 ビットのアドレスブロックを 2 つ割り当てられる。

ただし、IPv4 は SINET との接続に用いるネットワークのみの割当てであり、クライアント用のネットワークは別途 NAT で用意する必要がある。IPv6 は SINET の接続用とクライアント用のネットワークの双方が割り当てられる。そのため、クライアントも IPv6 グローバルユニキャストアドレスを持つこととなるため、外部からの接続の制限など、適切なフィルターをルーターで用意する必要があることに注意が必要である。

2.2 学内ネットワークの構成

SINET との接続は SINET DC と直接接続しているキャンパスの 1 つである日吉キャンパスで行っており、eduroam 用ゲートウェイも日吉キャンパスに設置し、運用している。

それ以外のキャンパスに対しては、キャンパス間の VPLS（Virtual Private LAN Service）による L2 VPN を利用し、クライアント向けの内部ネットワークをレイヤー2 で供給している。（図 1 参照）

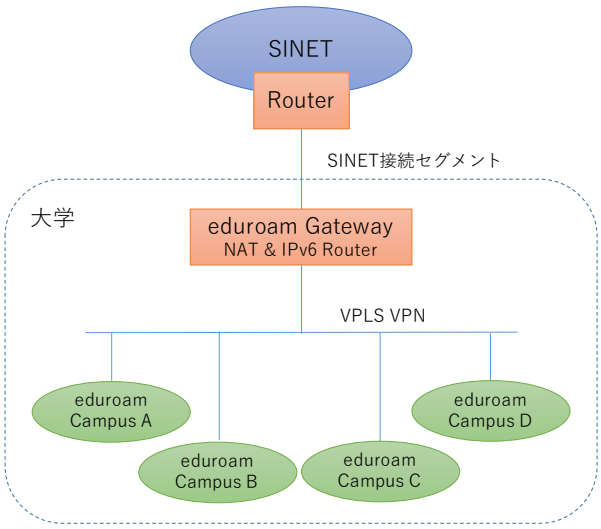

図 1. 本学におけるネットワーク構成

2.3 NAT ボックス兼 IPv6 ルーターについて

eduroam 用のゲートウェイとしては、Linux ディストリビューションの一つである CentOS を導入した PC サーバーを、NAT ボックス兼 IPv6 ルーターとして構築した。

サーバーのスペックは CPU が Intel Xeon E3120（3.16GHz、2 コア）、メモリーが 5GB、ディスクは 73.4GB である。

NIC は 3 つ利用しており、外部ネットワーク接続用、内部ネットワーク接続用 NIC の他に RADIUS プロキシ・アカウンティング用サーバーへの接続用 NIC を持つ。

3 利用履歴の収集方法

eduroam 向けに用意した RADIUS プロキシのログは、RADIUS プロキシ・アカウンティング用サーバーで稼働している PostgreSQL のデータベースに保存している。これは FreeRADIUS の SQL バックエンド機能を用いて実現している。

3.1 アカウンティングログについて

本学では異なる WLC（Wireless LAN Controller）によって制御される複数キャンパスの Wi-Fi システム間でクライアント向け内部ネットワークを共有しており、また全ての WLC が IPv6 アドレスのログ記録に対応しているわけではないため、RADIUS プロキシと eduroam 用ゲートウェイの利用状況のログを保管することで一元管理を行っている。

一方、アクセスポイントの全てが同一の WLC で管理されており、それが IPv6 アドレスのログ記録にも対応しているような環境であれば、WLC のログを参照するだけで十分であると考えられる。

3.2 IPv4/IPv6 アドレスのログについて

eduroam 用ゲートウェイでは定期的に MAC アドレスと IPv4/IPv6 アドレスの対応関係を収集し、RADIUS プロキシ・アカウンティング用サーバーの同じデータベースに保存している。（図 2 参照）

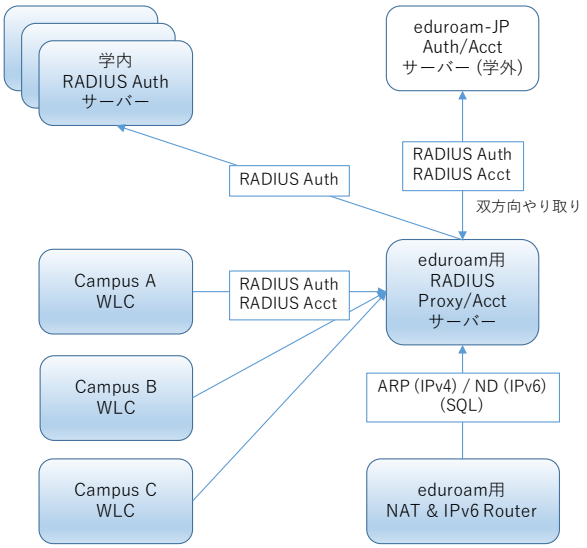

図 2. 本学における利用履歴収集方法

特に IPv6 アドレスに関しては、デバイス 1 台に対し複数のアドレスを同時に保持することが普通に行われるため、これを考慮した仕組みでログが記録される（図 6）。具体的な手順を次に示す。

1. eduroam 用ゲートウェイにて、内部ネットワーク側のインターフェースで認識されている有効な IPv4/IPv6 アドレスと MAC アドレスの対応を ip コマンドで取得する
2. 得られた MAC アドレスをキーにデータベースを検索し、RADIUS アカウンティング用のログ記録を行っているテーブル上のユニークな ID（radacctid）を取得する。
3. このセッション ID を外部キーとして、MAC アドレスに対応する IPv4 アドレスと IPv6 アドレス（前述のように通常は複数である）を IP アドレス用のログ記録を行っているテーブルに書き込む。

図 6 には表していないが、接続開始時刻、切断時刻などを含む多くの情報が、RADIUS アカウンティングログのテーブルに含まれている。

インシデント発生時など調査が必要となった場合にはこのデータベースを検索することで、利

用していた日時とIPアドレスから利用していたユーザーIDを特定することが可能である（ただしここで取得できるIDはouter tunnel用のユーザーIDのため、匿名IDの利用を想定すれば、信用できるのはレルム名のみである）。

3.3 セッションログについて

通信のセッションログに関しては、netfilterのログ出力機能を利用し、ローカルのストレージにそのまま記録している。

本学ではCentOSを利用し、NATボックス兼IPv6ルーターとして構成しているが、NetFlowなどfull flowを収集可能かつIPv6対応のレイヤー3スイッチなどで構成することも考えられる。この場合はFlow Collectorが必要となり、SNMPでMACアドレスとIPv4/IPv6アドレスのテーブルを収集できるレイヤー3スイッチである事も条件となる。

4 IPv6の利用状況

eduroam用ゲートウェイで収集しているセッションログから、全セッション数におけるIPv6の割合、最大同時接続デバイス数、一日ごとの平均セッション数（IPv4/IPv6）について、2017年8月分から2018年7月分のデータを月別に集計してみた。（図3、図4および図5参照）

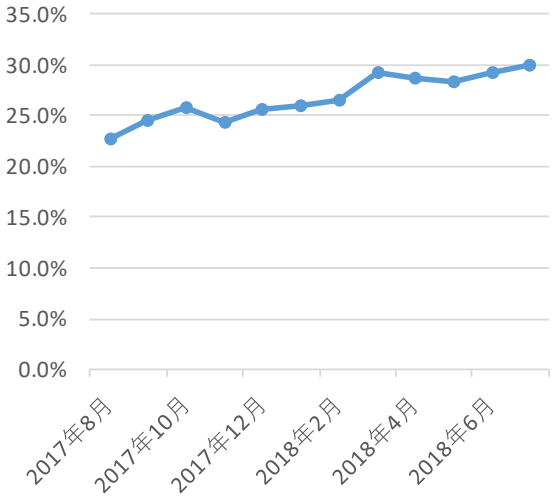

図3. 全セッション数におけるIPv6の割合
(2017年8月から2018年7月)

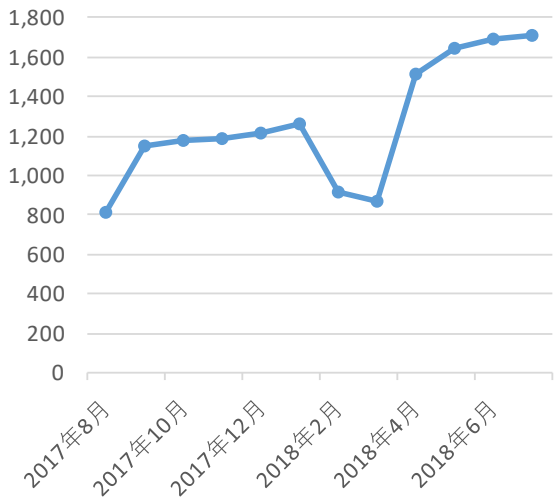

図4. 最大同時接続デバイス数
(2017年8月から2018年7月)

2017年8月のIPv6セッション数はセッション数全体の2割強であったが徐々に増加し、2018年3月以降は約3割まで増えている。

最大同時接続デバイス数は、2017年8月と2018年7月を比較すると2倍以上となっている。

2018年7月のIPv6セッション数の平均値は、2017年8月のIPv4セッション数の平均値とIPv6セッション数の平均値の合計を超えており、これは利用デバイス数の増加もさることながらIPv6の利用率増加も影響していると思われる。

5 IPv6接続環境提供のメリット

プロトコル毎のNATテーブルの上限値は、技術的にポート数の65,536を超える事は不可能であり、実際の限界はwell-knownポートの個数である1,024を除外した64,512よりも少ないのが現状である。IPv6のコネクションではこれを気にする必要はない。GoogleやMicrosoft、Facebookが提供しているオンラインサービスは既にIPv6でも提供されており、IPv6を積極的に利用促進すべきであると考える。

本学と同様にLinuxを利用してNAT機能を実現している環境にてIPv6を有効化する場合、IPv4とIPv6のセッションテーブルはnetfilterのconntrackにて一緒に管理されるため、カーネルパラメーターのnf_conntrack_maxの数値を増やしたり、メモリーを増設したりといった対応が必要になるケースが考えられる。

もしくは、単純に別の機器としてIPv6専用ルーターを追加する事で、NATテーブルの利用率を減

少させる事が可能だと思われる。

また、何かしらのインシデントが発生し、サービス提供者側にて観測・記録された IP アドレスからユーザーID を特定する必要が生じた場合、報告された IP アドレスが IPv4 の場合には、まずセッションログを調査、時刻と通信先から NAT ボックス内で利用されていたプライベート IP アドレスを特定し、更に時刻とプライベート IP アドレスを基に、ログからユーザーID を特定する必要があるが、IPv6 の場合には、時刻と報告された IPv6 アドレスを基に、ログからユーザーID を特定するだけとなる。調査の手間は IPv4 と比べると少なくて済む。

6 今後の課題

現在，本学の環境は比較的安定稼働していると思われるが、更なる安定化と利便性の向上を目指し、以下の項目を検討している。

- NAT ボックス兼 IPv6 ルーターの冗長構成化
  - Active/Standby の冗長構成ではなく、Active/Active の冗長構成を検討
- 認証 VLAN 化の検討
  - ユーザーサイドの設定の手間を減らす事が可能となるため
- 一貫教育校（小学校から高等学校）への展開
  - 本学の大学教員は、一貫教育校にて授業を行う事もあるため

参考文献

[1] 細川達己, “慶應義塾における eduroam 提供”, https://www.nii.ac.jp/csi/openforum2017/track/pdf/20170607AM_G_04_Keio.pdf

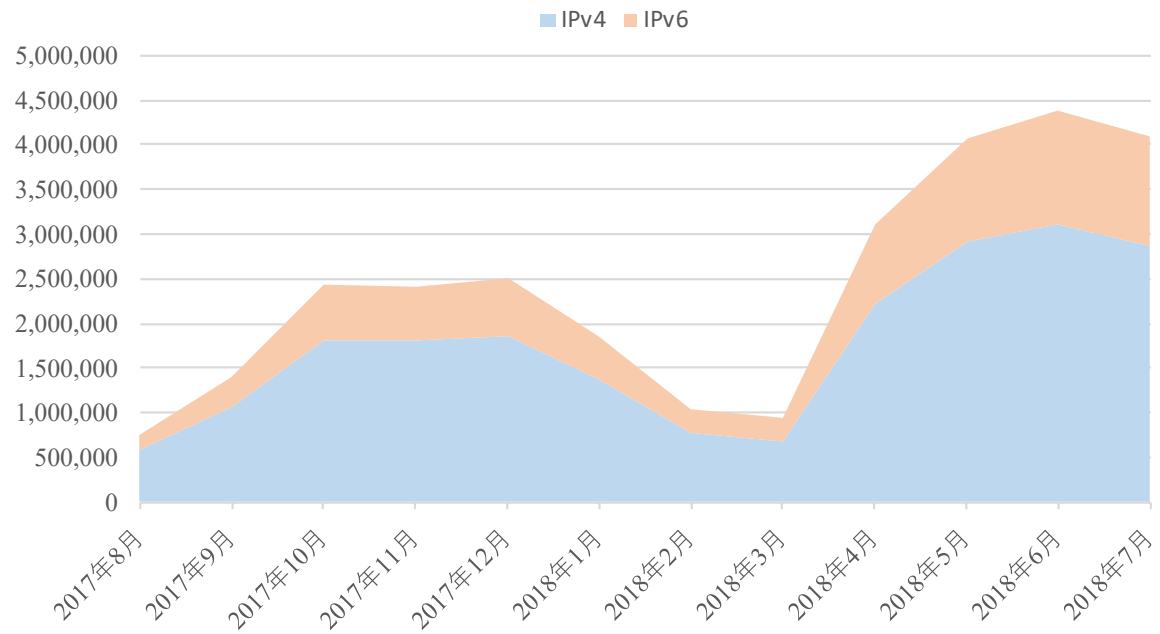

図 5. 一日ごとの平均セッション数（IPv4/IPv6）
(2017 年 8 月から 2018 年 7 月)

RADIUS アカウンティング ログのテーブル

radacctid	username (ユーザーID)	callingstationid (MACアドレス)
17702024	bbbb@sfc.keio.ac.jp	22-22-22-22-22-22
17702025	ccccccc@user.keio.ac.jp	33-33-33-33-33-33
17702026	dddddddd@keio.jp	44-44-44-44-44-44

IPアドレス ログのテーブル

radacctid	ipv4addr	ipv6addr
17702025	192.168.223.240	
17702025		fe80::1111:2222:3333:4444
17702025		2001:db8:aa:bb:cccc:dddd:eeee:ffff
17702025		2001:db8:aa:bb:1111:2222:3333:4444

図 6. データベースに格納されている
RADIUS アカウンティング ログと IP アドレスのログ