Vol.2017-IOT-38 No.9
2017/6/24

IPv6ネットワークにおける利用者認証に関する一考察

近堂 徹[1,a)]　北口 善明[2]　鈴田 伊知郎[3]　小林 貴之[4]　前野 譲二[5]

概要：組織のネットワークでは，持ち込み端末等のネットワーク接続の際に利用者および端末を特定するための利用者認証を用いる場合が多い。利用者認証にはウェブ認証や MAC アドレス認証, IEEE 802.1X 認証などが存在し，有線 LAN, 無線 LAN を問わずこれらの認証方法が単一もしくは併用する形で運用されている。一方，組織内において，接続するデバイスの数の増加・多様化，および IPv6 が普及していくことを考えたとき，利用者認証のあり方そのものを考え直す必要が出てくる。本発表では，IPv6 ネットワークを前提とした，認証スイッチにおける従来のウェブ認証による利用者認証環境からの 802.1X 認証の活用と課題について議論する。

キーワード：IPv6, 利用者認証, 運用管理

Consideration of the User Authentication for IPv6 networks

Tohru Kondo[1,a)]　Yoshiaki Kitaguchi[2]　Ichiroh Suzuta[3]　Takayuki Kobayashi[4]　Joji Maeno[5]

Abstract: In the campus network, network authentication function for identifying users and terminals has been widely used. Network authentication includes web authentication, MAC address authentication, and 802.1X authentication. These authentication methods are operated in a single or combined use regardless of wired LAN or wireless LAN. On the other hand, when considering increase and diversification of the number of terminals and deployment of IPv6 network, it may be necessary to rethink the manner of network authentication itself. In this paper, we describe issues of conventional network authentications such as Web authentication and MAC address authentication by authentication switches for IPv6 network, discuss the utilization or combination of 802.1X authentication.

Keywords: IPv6, User Authentication, Operation and Management

1. はじめに

2011 年 2 月に IANA(Internet Assigned Numbers Authority) が管理する IPv4 アドレスが枯渇，同年 4 月には APNIC および JPNIC における IPv4 アドレスの新規割当が終了し，IPv6 の割当が徐々に拡大してきている [1]。データセンター，クラウド事業者やサービスプロバイダでの IPv6 対応も進みつつあり，特に Google や Facebook 等のハイパージャイアントを中心に IPv6 接続が可能な状況である。また，ほとんどのネットワーク機器や主要なクライアント OS およびサーバ OS でも IPv6 プロトコルスタックがすでに実装されており，接続ネットワークが IPv4 と IPv6 のデュアルスタック運用されている場合は IPv6 が優先して利用される状況になってきている。2017 年度には日本においてモバイルキャリアの IPv6 接続が標準的に提供される予定 [2] になっており，多くのサービスでの IPv6 導入が進むことが期待されている。

一方，IPv6 のトラフィックも徐々に増えてはいるものの，インターネットにおける通信の多くは未だ IPv4 である。組織において IPv6 導入が進まない原因としては，現時点では IPv4 での通信が必要不可欠であるため，結果的

[1] 広島大学情報メディア教育研究センター, Information Media Center, Hiroshima University, 739-8511, Japan
[2] 東京工業大学
[3] アラクサラネットワークス株式会社
[4] 日本大学 文理学部
[5] 早稲田大学 情報教育研究所
[a)] tkondo@hiroshima-u.ac.jp

に IPv4 と IPv6 のネットワークを二重に運用する必要があること，また IPv4 が存在する環境で IPv6 を積極的に利用するメリットがないことなどが挙げられる。しかし，世界的に IPv6 が普及が進むなか，重要インフラを支える技術として IPv6 への対応が無視できない状況になるのは想像に難しくない。近年では，NAT64/DNS64[3][4] に代表されるトランスレーション技術の確立により，組織内では IPv6 アドレスのみを利用した『IPv6 オンリーネットワーク』を提供し，IPv4 通信はネットワーク境界でアドレスに変換する手法も利用され始めている。今後は IPv4/IPv6 デュアルスタック運用のみならず，このようなアドレス変換技術を導入したネットワーク運用により，結果的に IPv6 アドレスの利用拡大に繋がることが期待される。

他方，大学などの高等教育機関におけるキャンパスネットワークは， 教育研究活動から管理運用業務に至る様々な活動を支える主要インフラとしての必要性が高まるばかりである。近年では，ICT を活用した授業支援や学外者も含めた BYOD(Bring Your Own Device)，基幹業務系での利用など，その利用形態は多種多様となっている。単にネットワーク接続性を提供するだけでなく，高いセキュリティと安定性を確保しつつユーザの利便性を損なわないことが求められる。また運用管理者側の要件としても，機器や利用者の的確な把握とセキュリティインシデント時等の迅速な対応が求められ，これらを背景としてネットワークにおける利用者認証を導入している学術機関も多い。現在，有線 LAN 接続ではウェブ認証や MAC アドレス認証，無線 LAN 接続では WPA2-EAP にて IEEE 802.1X 認証（以下，802.1X 認証）が利用されるケースが一般的となっている。

学術機関のキャンパスネットワークは未だ IPv4 が主流であり，利用者向けに IPv6 を提供している組織はまだ少ない。しかしながら今後 IPv6 導入が進んだ場合，従来の IPv4 を前提とした利用者認証機能では不十分なケースが出てくる可能性もある。したがって，実際に IPv6 ネットワークと利用者認証や機器認証等の認証ネットワークと組み合わせた場合の課題等について整理し，IPv4 ネットワークの場合と乖離のない状態で運用管理するための知識・経験を養っていく必要がある。これまでデュアルスタック環境における利用者認証システムに関する開発は行われてきているが [5][6]，認証スイッチを利用した場合の認証動作検証や複数認証方式を利用した際の課題について現状のクライアント OS や昨今の IPv6 実装状況を踏まえたうえで検討していく必要がある。

筆者らはこれまで大学等における IPv6 の利用状況の調査 [11] や実際のクライアント OS における IPv6 実装検証およびネットワーク運用における課題 [12] について整理してきた。そこで本稿では，IPv6 ネットワークにおける利用者認証に焦点を当てて既存の課題についてまとめるとともに，複数のネットワーク認証スイッチおよび各種クライアント OS を用いて行った動作検証についてまとめる。これらの内容をもとに，IPv6 ネットワークにおける利用者認証の在り方について考える。

2. IPv6 導入に関する動き

本章では，執筆時点における IPv6 導入に関する状況を簡単にまとめる。

2.1 通信事業者

通信事業者における IPv6 導入状況を推し量る情報として，BGP における経路情報がある。経路数に関しては，IPv4 の 70 万経路に対して IPv6 の経路数は 4 万程度であり 6%に満たないが [7]，これは，IPv4 におけるマルチホーミングの影響が大きいと考えられる。ネットワークの組織単位（AS: Autonomous System）で見るとトランジット AS における IPv6 導入比率は 30%を超えており [8]，インターネットのバックボーンにおける IPv6 導入は低くはない状況である。また，日本も同様にバックボーンの IPv6 対応は 30%を超えており，アクセス網の IPv6 対応も進んでいる。

モバイルネットワークに関しては，米国での取り組みが目立っている。Verizon Wireless と T-Mobile は，LTE 網整備において IPv6 を導入しており，IPv6 利用率は両社とも 80%を超える状況となっている [9]。また，日本でも総務省主導で大手の 3 モバイルキャリアにおける IPv6 導入が 2017 年度に予定されており，今後 IPv6 でアクセスする端末が増加してくることが予想される。

2.2 コンテンツ・クラウド事業者

ハイパージャイアントと呼ばれる米国の大手コンテンツ事業者（Google，Facebook など）は，早くから IPv6 対応を進めている。その他のコンテンツ事業者は IPv6 導入に消極的で，IPv6 の必要性がなくコスト増に直結するとの理由に因ると指摘されている [10]。

クラウド事業者に関しては，利用者からの需要がないため一部のクラウド事業者（さくらインターネットなど）でしか IPv6 利用が可能ではなかったが，2016 年に Microsoft Azure と Amazon EC2 が IPv6 対応し，IPv6 によるクラウドサービス利用が大きく前進したといえる。

2.3 コンシューマ・エンタープライズ

通信事業者やコンテンツ・クラウド事業者と比較すると，IPv6 導入が進んでいない。一般的な企業のネットワークでは，インターネットでの接続を有していたとしても，ウェブと電子メールの利用に限られている場合が多い。さらに，ウェブ接続にはプロキシサーバが用いられるため，利用者に対してグローバルアドレスを設定する必要性がないといえる。このため，IPv6 を導入する動機付けが全くない

状況にある。

2.4 学術機関

学術機関である大学に関しては，一部の大学においてIPv6 導入がなされている状況で，その導入も一部のネットワークに限られている場合がある。国内の大学を例に挙げると，金沢大学では，サーバセグメントのデュアルスタック化は実施されているのみで，学内には試験的な IPv6 導入が数カ所行われている状況である。東京工業大学では，研究で要求された一部の研究室にのみ IPv6 の接続性を提供しているだけに留めている。これは，自組織でのネットワーク運用を行なっていることも関係しており，トラブルシュートの複雑さを回避するための措置でもある。日本大学では公開サーバの一部で IPv4/IPv6 デュアルスタック運用を行っている。ネットワークについては学部間基幹回線は IPv4/IPv6 デュアルスタック運用だが、学部内ネットワークは一部の学部でのみ IPv6 を運用している状況である。

広島大学では 2008 年 4 月より基幹ネットワークおよび支線ネットワークの一部で IPv4/IPv6 のデュアルスタック運用を進め，現時点でサーバ，クライアント全てのホストで IPv6 が利用可能である。クライアントに対しては SLAAC によるアドレス自動割当を行なっており，2015 年の調査では，全学無線 LAN ネットワークの接続端末の約 90%に IPv6 アドレスが付与されているデータが得られている [13]。これは，現在のクライアント OS が標準で IPv6 に対応し，ネットワーク側が対応できれば即時 IPv6 で通信可能になることを意味している。

なお学術組織における利用状況の調査については文献 [11] にもまとめているので，そちらも参照されたい。

3. IPv6 ネットワークにおける利用者認証の課題

本章では，主に学術機関のキャンパスネットワークにおける利用者認証の課題について述べる。

3.1 キャンパスネットワークにおける利用者認証の課題

広島大学を例にキャンパスネットワークにおける利用者認証について整理する。広島大学では，研究室向けに全学管理のネットワークを提供している [14]。教員に対して申請に基づき個別ファイアウォール配下のネットワーク (VLAN) を提供し，その VLAN を任意の情報コンセントに設定することで，研究室ネットワークの構築（管理者は申請教員，副管理者は管理者が指定する構成員）が可能になっている。各フロアに設置された認証スイッチでは，管理者・副管理者が登録した MAC アドレスによる端末認証かウェブ認証による利用者認証が必須となっている。

広島大学では上記の形態で 10 年運用してきているが，いくつか課題も出てきている。1 点目は未認証端末から外部への http/https 接続による認証スイッチの CPU 負荷の増大である。近年のパソコンはバックグラウンドで外部接続を行うプログラムが多数インストールされる。これらが全て認証スイッチでウェブ認証のリダイレクト対象となり，定常的に認証スイッチの資源を消費してしまう問題がある。

2 点目は複数の認証スイッチで相互に認証が発生するケースである。これは主に研究室内で無線 AP を運用する場合に発生する。例えば，同一 SSID を設定した無線 AP が複数の認証スイッチ配下に設置されていると，無線ローミングをしたタイミングで認証ポイントが変更となり，再認証が発生してしまうことになる。利用者からは，認証切断した形で見えるためユーザビリティの低下に繋がる。

3 点目は携帯端末（個人所有端末）との親和性である。もともとウェブ認証は共用端末での認証が行いやすいという面もあったが，近年では持込パソコン等の個人所有の端末が多くなり，毎回の入力が煩雑と感じる利用者が増えている。さらに，無線ローミングや端末がサスペンドした際の再認証も利便性を低下させる一因となっている。

3.2 IPv6 ネットワーク導入時の課題

IPv6 ネットワークにおける利用者認証の課題について，いくつかの観点から整理を行う。

1 点目は認証機能自体の IPv6 対応の必要性である。802.1X 認証や MAC アドレス認証の場合は，レイヤ 3 に依存しない形で認証を実現できる。一方，ウェブ認証の場合はウェブサーバや認証機構を IPv6 へ対応させる必要がある。端末の認証状態の管理等，IPv4 と IPv6 で併用するとなれば，その分のコスト増は避けられない。

2 点目は端末のトレーサビリティへの課題である。IPv6 では IPv4 と異なり，インタフェースに対して複数の IPv6 アドレスが付与される仕様となっている。そのため，MAC アドレスに対応する IPv6 アドレスが複数存在することに留意する必要がある。現在の一般的な実装では，リンクローカルアドレスとグローバルアドレスが最低限設定され，グローバルアドレスもルータ広告による SLAAC（StatelLess Address AutoConfiguration）では，MAC アドレスなどを基にしたインターフェース毎に固定のアドレスに加え，セキュリティとプライバシを確保するためのプライバシ拡張アドレスが設定される。したがって，端末の IPv6 トレーサビリティを確保するためには，IPv4 の場合の 3 倍以上のリソースがデータベースに必要となる [12]。

4. 動作検証

本章では，IPv6 ネットワークにおける利用者認証の実装検証についてまとめる。今回は，有線 LAN における 802.1X 認証 (EAP) とウェブ認証の利用者認証機能と IPv6 ネットワークとの挙動を確認する目的で行ったものである。

4.1 検証構成

今回の動作検証で用いたネットワーク構成を図 1，ネットワーク機器諸元を表 1，検証に利用したクライアント OS のバージョンを表 2 に示す。本検証は認証スイッチおよびクライアント OS の動作確認を主目的としているため，インターネット接続性は提供せず，L3 スイッチにてクライアント端末とサーバ群をルーティングする構成としている。なお，図 1 における赤丸が認証ポイントとなる。

L3 スイッチでは，O フラグ付き RA(Router Advertisement) による IP アドレス自動設定とステートレス DHCPv6 による DNS 情報配布を行なっている。また，認証スイッチのアクセスポートは固定 VLAN による認証設定とし，53/udp および 67/udp を許可する認証前 ACL を適用している。なおクライアント OS のうち，Windows 系の OS では標準で有線 LAN での 802.1X 認証は無効化されているため，有線 LAN で利用する場合はあらかじめ Wired AutoConfig サービスを起動させておく必要がある。また，EAP 認証方式としては Windows 系 OS では PEAP 方式，macOS は TTLS 方式となっている。

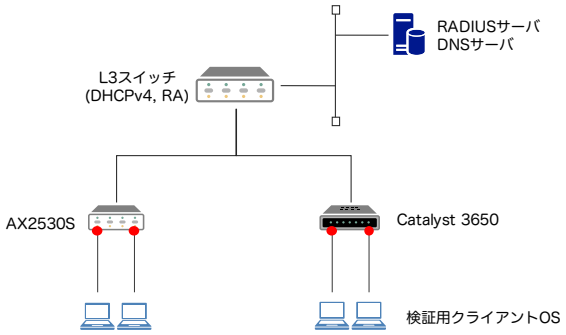

図 1 検証におけるネットワーク構成
Fig. 1 Network configuration of the verification

表 1 ネットワーク機器の仕様
Table 1 Specification of network equipments

用途	機器	バージョン等
L3 スイッチ	Alaxala AX3630	11.14.J
RADIUS サーバ	Ubuntu 16.04.1LTS	Free Radius 2.2.8
DNS サーバ		bind 9.10.3
認証スイッチ	Alaxala AX2530S	4.0.C
	Cisco Catalyst 3650	16.3

表 2 利用したクライアント OS のバージョン
Table 2 Version of client OS

OS	バージョン	認証方式
Windows 7 Pro	6.1 (build 7601 SP1)	PEAP
Windows 8.1 Pro	6.3 (build 9600)	PEAP
Windows 10 Pro	1607 (build 14393.1198)	PEAP
macOS	10.12	TTLS

4.2 検証項目

4.2.1 有線 LAN における 802.1X 認証の挙動検証

本検証の目的は，IPv4 接続が提供されない IPv6 オンリーネットワークにおいても 802.1X 認証により IPv6 接続性が確保できるかを確認するものである。そもそも 802.1X プロトコルはデータリンク層のプロトコルであるため IPv4/IPv6 に依存することなく動作可能と考えられるが，各種クライアント OS および複数認証スイッチの基本動作として検証を行う。

これにあわせて，共用端末における 802.1X 認証の挙動についても確認する。キャンパスネットワークでは個人所有の持込端末が増加しているものの，研究室等では依然として共用端末で作業を行うケースも少なくない。この場合，利用者毎に正しく認証および認証解除させる必要がある。従来ウェブ認証では，認証解除のトリガーが認証スイッチからの ARP ポーリングによる死活監視か利用者による明示的にログアウト操作が必要であった。したがって，802.1X 認証時の認証解除方法も検討する必要がある。認証サプリカントは OS に標準装備されている機能であるため，端末のログオフ時にサプリカントによる制御が行われていることが期待される。本検証では利用者の操作に連動した認証状態の変化について確認する。

4.2.2 マルチプル認証利用時の動作検証

多くの認証スイッチでは，単一アクセスポートで複数の認証方式を選択もしくは併用した認証（本稿では，マルチプル認証とよぶ）が可能となっている。一方で認証方式の併用時の注意点として，認証の順序や異なる認証方式を組み合わせることによる不具合やクライアント OS への意図しない影響も予想される。そこで，今回はマルチプル認証利用時の動作検証として，802.1X 認証とウェブ認証の併用時の認証動作について確認する。

4.2.3 未認証端末に対するマルチキャスト/ブロードキャスト通信

IPv6 ネットワークと認証スイッチの組合せにおける課題のひとつとして，未認証端末に対する RA 等のマルチキャスト通信の制御が困難な点が挙げられる。典型的な例に，認証スイッチ配下に LAN スイッチを設置し，多数の端末を収容しつつ認証を行う例である。この場合，認証ポイントが認証スイッチのアクセスポート側となるため，通常は認証スイッチ上流から下流に対して転送されるパケットは制御することができない。また，アクセスポート側に認証済み端末が 1 台でも存在する場合，その端末に対するブロードキャストやマルチキャストパケットは，未認証端末にも到達する可能性がある。したがって，認証済端末と未認証端末が混在する環境でのアドレス付与の挙動について確認する。

4.3 検証結果

はじめに，IPv6 オンリーネットワークにおける 802.1X

認証の挙動について述べる。今回の検証では，いずれの認証スイッチおよびクライアント OS の組み合わせにおいても正しく 802.1X 認証に成功し，RA による IPv6 アドレスが付与されることが確認できた。また，OS のユーザーログオフ操作により認証スイッチでの認証解除も正しく動作することが確認できた。ただし，Windows と macOS では認証解除のトリガが異なっており，macOS ではプロトコル通り「EAPOL-Logoff」パケットによるログアウト処理が行われたものの，Windows 系ではログオフと同時にコンピューターの認証に切り替わることで認証スイッチ側で認証失敗し，認証状態が解除される動作となった。この点については，さらなる検証が必要になると思われるが，いずれにせよ従来ウェブ認証では共用端末におけるログアウト処理を別途考慮する必要があったが，802.1X 認証の場合は OS 標準のサプリカント機能でローカルユーザーのログイン/ログアウト処理に連動して認証状態を解除する運用が可能であることを確認した。

次に，マルチプル認証利用時の動作検証結果について述べる。本稿では AX2530S の認証スイッチを利用したマルチプル認証の挙動について示す。実際にクライアント OS にてキャプチャしたパケットフローを図 2 に示す。この挙動からわかるように，マルチプル認証利用時には，802.1X 認証と，ウェブ認証のための L3 動作が並行して動作している様子が確認できた。つまり，クライアント OS 側の挙動として 802.1X 認証より前に DHCP による IP アドレス取得動作が動き，またタイミングによっては上位 L3 スイッチからの RA による IPv6 アドレス付与される（が外部への通信はできない）結果となった。この挙動は Windows 系 OS,macOS の両 OS で確認できたが，Windows10 の場合は図 3 に示すフォールバック設定を行うことで 802.1X 認証を優先する制御が可能であることを確認した。

最後に未認証端末に対するマルチキャスト/ブロードキャスト通信について述べる。今回の検証では認証スイッチ配下の LAN スイッチに接続された 1 台の端末が 802.1X 認証し，NS(Neighbor Solicitation) に対する RA がマルチキャストされる際に他の未認証端末で IPv6 アドレスが付与されるか否かを確認した。その結果，Windows 系 OS, macOS ともに IPv6 アドレスが付与された。つまり，認証前であっても接続端末にアドレスが自動設定される可能性があることを確認した。

5. 考察

本章では，3 章および 4 章の結果から，IPv6 ネットワーク環境における利用者認証とネットワーク運用に与える影響について考察する。

デュアルスタック環境で認証スイッチによる利用者認証を行う場合，多くの場合は IPv4 でのウェブ認証で利用できる。しかしながら，3 章でも示した通り，IPv4 における

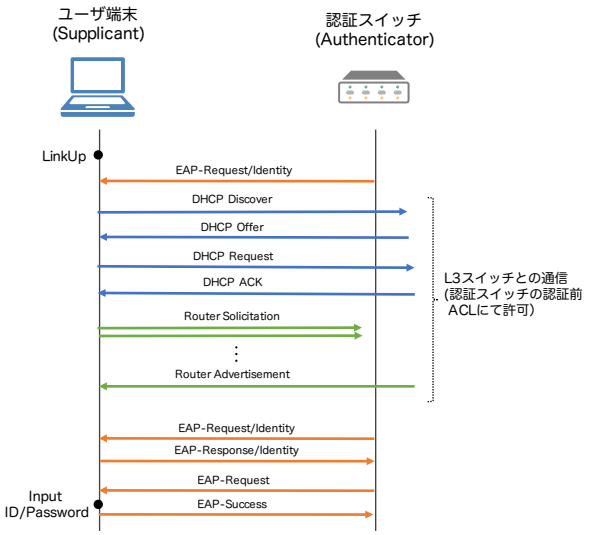

図 2 マルチプル認証時のパケットフロー（クライアント OS: macOS, 認証スイッチ: AX2530S の場合）

Fig. 2 Packet flow in multiple authentication mode (Client OS: macOS, Authentication switch: AX2530S)

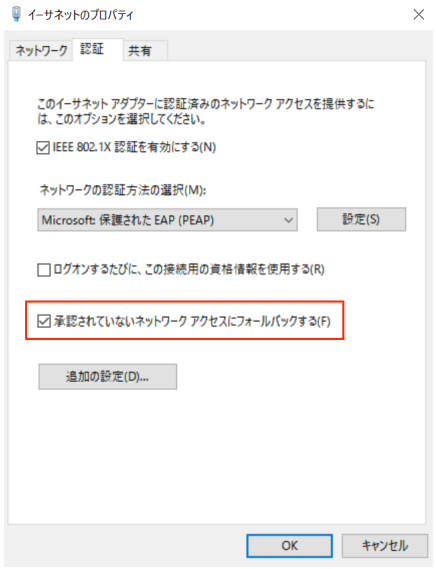

図 3 Windows10 における 802.1X 認証のフォールバック設定

Fig. 3 Fallback configuration for 802.1X authentication on Windows 10

ウェブ認証ではリダイレクトによる負荷増大等の課題もあり，できる限り 802.1X 認証へシフトしていく形が妥当であろう。その場合は，既存環境を考慮してマルチプル認証の利用が前提となる。しかしながら，今回の検証結果から，クライアント OS の実装によっては 802.1X 認証プロセスと IP アドレス付与処理が同時に動くことで，利用者が意図しない認証方式を利用せざるを得ない場合が出てくることも予想される。802.1X 認証を優先させるような動作が可能かどうかはさらに検証が必要である。

一方，IPv6 オンリーネットワークでは現時点では MAC アドレス認証か 802.1X 認証を利用せざるを得ない状況で

ある。ウェブ認証を実現するためには，認証機能の IPv6 対応が必須となり，従来 IPv4 のウェブ認証における ARP ポーリングに相当する死活監視が必要となる。この場合リンクローカルアドレスに対する ND(Neighbor Discovery) / NA(Neighbor Advertisement) の利用が想定されるが，IPv4 と IPv6 の併用も考慮した認証処理の複雑化やメモリ資源の制約が懸念点として挙げられる。

IPv6 固有の課題としては，RA に対する対応が挙げられる。端末に対する IPv6 アドレス設定には RA が必須となり，それが認証前であっても端末に到達することによる影響も考えておかなければならない。IPv4 の DHCP では接続に必要なパラメータを設定することが可能であったが，IPv6 のステートフル DHCPv6 ではプレフィックス情報は含まれずデフォルトルートを設定する機能もない。したがって，クライアント OS の実装によっては未認証状態で RA が到達したタイミングで一部の設定が端末側で行われることが予想される。この点は，認証スイッチにおける認証前フィルタの機能（Ingress/Egress の指定や詳細なプロトコル指定など）に依存するが，運用時の影響について今後検証していく必要がある。

また，仮に認証ログから利用者の ID と MAC アドレスの対応関係が記録できたとしても，IPv6 アドレスの場合，リンクローカルアドレスとグローバルアドレス，さらにはプライバシ拡張アドレスが割り当てられるため，これらの IPv6 アドレスと MAC アドレスの関係性を管理しなければ，セキュリティインシデント時の迅速性を低下させてしまう恐れがある。ステートレスな DHCPv6 のみで運用できることが望ましいが，現在のクライアント OS 実装状況では不十分な状況であるため [12]，この点についても継続的に検討していく必要がある。

6. まとめ

本稿では，IPv6 ネットワーク導入に伴う利用者認証のあり方について整理し，IPv6 オンリーネットワークにおける IEEE802.1X 認証の動作やウェブ認証/802.1X のマルチプル認証の動作検証について報告した。また，それらの結果を IPv6 ネットワークにおける利用者認証の課題について考察した。今回は，特定機種の認証スイッチや環境での検証となっているため，今後はさらに他機種での検証等が必要になる。また実運用を通した課題の抽出も今後行う予定である。

謝辞 本研究は，科学研究費助成金（15K00118）の助成を一部受けたものである。

参考文献

[1] RIPE NCC. IPv6 Enabled Networks. http://v6asns.ripe.net/v/6/ (参考: 2017-05-25).
[2] 携帯キャリアにおける IPv6 対応最新状況, IPv6 Summit in Tokyo 2016, http://www.jp.ipv6forum.com/timetable/program.html (参照: 2017-05-25).
[3] M. Bagnulo, P. Matthews, and I. van Beijnum. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. RFC 6146 (Proposed Standard), April 2011.
[4] M. Bagnulo, A. Sullivan, P. Matthews, and I. van Beijnum. DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers. RFC 6147 (Proposed Standard), April 2011.
[5] 大谷誠, 江口勝彦, 渡辺 健次. IPv4/IPv6 デュアルスタックネットワークに対応したネットワーク利用者認証システムの開発, 情報処理学会論文誌 Vol.47, No.4, pp.1146-1156, 2006.
[6] 永井勢一, 安井浩之, 吉野邦生, IPv6/IPv4 混在環境におけるユーザ認証システムの開発, 情報処理学会第 75 回全国大会論文集, pp.3-589 - 3-590, 2013.
[7] Geoff Huston, BGP Analysis Reports, http://bgp.potaroo.net/index-bgp.html (参照] 2017-05-27).
[8] CISCO, 6lab - The place to monitor IPv6 adoption (World Charts, Transit AS Data), http://6lab.cisco.com/stats/cible.php?country=world&option=network (参照: 2017-05-27).
[9] World IPv6 Launch, Measurements. http://www.worldipv6launch.org/measurements/ (参照: 2017-05-27).
[10] 馬渡将隆 ほか. なぜ，IPv6 対応したくないか, JANOG35 Meeting, 2015. https://www.janog.gr.jp/meeting/janog35/program/ipv6/ (参照: 2017-05-27)
[11] 小林貴之, 鈴田伊知郎, 前野譲二, 近堂徹. 2016 年度における IPv6 の大学等における利用状況, 大学 ICT 推進協議会 2016 年度年次大会予稿集, 2016.
[12] 北口善明, 近堂徹, 鈴田伊知郎, 小林貴之, 前野譲二. クライアント OS の IPv6 実装検証とネットワーク運用における課題, 情報処理学会研究報告, 2017-IOT-36(13) pp.1-8, 2017.
[13] 前田香織, 新谷隆文, 近堂徹, 相原玲二. IPv6 無線 LAN におけるマルチキャストパケットの実態とその影響分析, 情報処理学会論文誌,57(3), pp.989-997, 2016.
[14] 近堂徹, 田島浩一, 岸場清悟, 吉田朋彦, 岩田則和, 大東俊博, 西村浩二, 相原玲二. クラウドコンピューティング活用のための大規模キャンパスネットワーク, 情報処理学会インターネットと運用技術シンポジウム (IOTS)2014 論文集, pp.101-108, 2014.