6 IPv6 対応ユースケース(大学)

国内には大学の内部環境を IPv6 化した実績が少ないことが考えられる。そこで、IPv6 対応に係る知見や ノウハウを蓄積するため、3.3 で選定したとおり、「モデル I」を対象とした IPv6 対応ユースケースを示す。

6.1 モデル I:大学 A

6.1.1 ユースケース大学の紹介

ユースケースを行った対象フィールドとシステム環境を紹介する。

(1) フィールド紹介

本ユースケースは、北陸地方に拠点を置く大学(以下、A大学と呼称)で行った。A大学は、県内に複数のキャンパスがあり、4学部体制を敷き、2,500人を超える学生に対して多様な学びが提供されている。また、多くの留学生が在学し、国際交流にも注力している大学である。

(2) 既存のシステム環境

本実証試験は、A 大学内で利用している一般業務システムだけでなく、A 大学で利用されている業務 アプリケーション相当のシステム、クラウドサービスに対して行った。A 大学のシステム環境の仕様を示 す。

- ネットワーク規模/インターネットとの接続方式 A大学のシステム環境内のノード数は50以上、サブネット数は10未満、2学部間を広域LAN接続している。インターネットとの接続は学術情報ネットワーク(SINET)を利用して接続している。
- ② 内部ネットワーク運営方法、およびサーバ運営方法/セキュリティ システム環境内の PC には IPv4 アドレス等を DHCP サーバで動的設定を行っているが、サーバ 機器および一部の PC は IPv4 アドレス等を静的に設定している。DNS サーバは学内に設置して いるが、メールについては外部のサービスを利用している。ファイアウォールは既設 FW 装置を用 いて実現している。

A 大学の内部環境を IPv6 対応するにあたり、要件定義の工程として 5 つのプロセスに沿って作業を行った。まず、1 つ目の「現状の把握」として既存環境で利用している機器やサービスを可視化し、現行システムを整理した。続いて、2 つ目の「移行方式の明確化」では IPv6 環境へ移行するための方式を定めた。そして 3 つ目の「移行対象の明確化」では現行システムの内、IPv6 対応する機器やサービスを明確にした。また 4 つ目の「IPv6 対応状況の確認」では移行対象の機器やサービスが IPv6 に対応しているか確認を行った。最 後に 5 つ目の「導入方針の策定」では機器やサービスの IPv6 対応状況に基づき、IPv6 化に向けた導入方 針を策定した。

(1) 現状の把握

現行システムを把握するため、ネットワーク構成図を作成し、システムの可視化を行った。ネットワーク構成図のアウトプットイメージを図 6.1.2-1 に示す。



図 6.1.2-1 ネットワーク構成図イメージ

(2)移行方式の明確化

本ユースケースにおいては IPv6 環境への移行を見据え、可能な範囲で既存システムを IPv6 対応する 方針とした。移行範囲を検討した結果、既存システムへの影響を最小限に抑えるため、既存システムの 一部を IPv6 対応することとした。そのため、IPv4 の既存学内ネットワークと IPv6 の実証試験ネットワーク を共存させる必要があることから移行方式としてデュアルスタック方式を採用した。

(3)~(5)移行対象の明確化、IPv6対応状況の確認、導入方針の策定

要件定義における作業プロセス(3)~(5)を実施するにあたり、機器等一覧を作成し、作業結果を記載した。機器等一覧のアウトプットイメージを表 6.1.2-1 に示す。

既存/ 新規	機器等	機器 メーカ等	機器名等	移行対象	IP∨6 対応 状況確認	導入方針
新規	実証用 FW 装置	Fujitsu	IPCOM EX1300 SC	0	IPv6 対応	新規
新規	実証用 L3 スイッチ	Fujitsu	SR-S732TR1	0	IPv6 対応	新規
既存	既設 L3 ス イッチ(コア ルータ)	Fujitsu	SR-S732TR1	0	対象外 (IPv6 ルーティ ング不要)	変更要 (IPv6 L2 透過)
既存	既設 L2 ス イッチ	Fujitsu	SR-S352TR1	0	対象外 (L2 機器のた め)	変更要 (IPv6 L2 透過)
新規	実証用無線 アクセスポ イント	Buffalo	WSR-2533DHPd3	0	対象外 (L2 機器のた め)	新規 (L2 透過)
既存	既設無線ア クセスポイ ント	Cisco	AIR-CAP1702I-Q- K9	0	対象外 (L2 機器のた め)	変更要 (L2 透過)
新規	実証用ファ イルサーバ	Buffalo	WS5220DN02W9	0	IPv6 対応	新規
新規	実証用学内 WEB サーバ	仮想基盤 上の仮想 マシン	Windows Server 2016 Std	0	IPv6 対応	新規
既存	複合機	Fuji Xerox	Center-V C5575 T2	0	IPv6 対応	変更要
既存	プリンタ	EPSON	LP-S7160	_	対象外	変更不要

表 6.1.2-1 機器等一覧イメージ

既存/ 新規	機器等	機器 メーカ等	機器名等	移行対象	IP∨6 対応 状況確認	導入方針
既存	SINET	インターネ ット接続 (IPv4/IPv6 Dual)	インターネット接続 (IPv4/IPv6 Dual)	0	IPv6 対応	変更要
既存	G Suite	Gmail	Gmail	0	IPv6 対応	変更不要
既存	Microsoft 365	Exchange Online	Exchange Online	0	IPv6 対応	変更不要

6.1.3 スケジュール計画

つぎに、IPv6 対応のスケジュールを計画する。本ユースケースで作成したスケジュールのイメージを図 6.1.3-1 に示す。ポイントは 3 点である。

1 点目は、環境構築において既存の SINET サービスの切り替えおよび学外接続用ファイアウォールの更 改は現行システムへの影響を最小限に抑えるため、休日作業として調整した。

2 点目は、IPv6 対応はレイヤー3(インターネットプロトコル)への影響が大きいため、ネットワークレベルの 検証とアプリケーションレベルの検証を分け、段階的に検証したことである。また、ネットワークレベルの検証 を「一般業務における検証」、アプリケーションレベルの検証を「業務アプリケーションにおける検証」と「業務 アプリケーション(クラウド)における検証」に分割した。段階的に検証することで、課題発生時の原因究明を 行いやすくなる。

3 点目は、試験結果の評価を検証ごとに行ったことである。検証ごとに課題を解決することができ、後続での手戻りが発生しにくくなる。

		1 週目	2 週目	3 週目	4 週目	5 週目	6 種目	7 週目	8 週目	9 週目	10 週目	11 週目	12 週目	13 週目
要作	沣定 義	現行 移行対象	整理/ 象の定義											
調道	5		回線調機器	22約/ 調達										
				実証: 設計書	計画/ 冒作成									
構築	ław					環境	冓築							
	疎通確認													
試験	ネットワークレベル の検証							一般調	業務 る検証					
	LAN内アプリケー ションレベルの検証								業	務アプリ? における	ケーション る検証	,		
	WAN越しアプリケー ションレベルの検証										業 (ク	務アプリ: ラウド)に	ケーション おける検	> 証
試験結果の評価														

図 6.1.3-1 スケジュールイメージ(大学 A)

6.1.4 設計

本ユースケースでは、内部環境に IPv4 環境を残す必要があるため、デュアルスタック環境の構築を目指 した。設計の方針を大きく4 つ定めた。

- ① 現行のシステム環境への影響(システム修正変更)は最小限に抑えること
- ② 今回の IPv6 実証のステップにおいて、実証にて定められた範囲にてIPv6の検証を行うことがで きること
- ③ 既存環境を可能な限りIPv6対応する環境とし、実証機器は本番環境と同等の設定を実装する。
- ④ 最終的な IPv6 シングルスタック構成に向けた、スコープとステップ策定を行うことができること

続いて IPv6 対応するための方式設計を行った。本ユースケースにおいて、現行の IPv4 シングルスタック 環境を構成する各要素に対する方式設計のポイントを以下に示す。

- (1) 無線接続のノート PC
 - ① 要素説明

インターネット(WEB サービス利用やメール等)、印刷やスキャン、ファイルサーバの利用を行うための 無線接続クライアント PC である。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

(a) IP アドレスについて

実証試験のため、IPv6 アドレスは固定 IPv6 アドレスと RA による IPv6 アドレス自動採番を採用する。ルータ仕様のため、プレフィックス部のみ DHCPv6⁶⁵で割り当てるステートレス方式とする。 ・IPv4 アドレス…静的アドレスによる手動設定 ・IPv6 アドレス…IPv6 アドレスは固定 IPv6 アドレスと RA による IPv6 アドレス自動採番を採用する

(b) DNS サーバ/デフォルトゲートウェイについて

DNS サーバについては、指定する IPv6 アドレスを RA で割り当てることが出来ないため、以下の 方式とする。

- ・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)
- ・IPv6アドレス…静的アドレスによる手動設定

(パブリック DNS の指定/hosts ファイルによる指定)

⁶⁵ DHCPv6 は管理が容易になるが、有事の追跡性に IP アドレスが使えなくなるため、ユーザ ID 等の追跡性確保の仕組みが別に必要である。

(c) ポリシーテーブルについて

IPv4アドレスおよび IPv6 アドレスを保有するため、利用するアドレスの優先順位を付ける。デフォルトは IPv6 アドレスが優先されるが、実証試験のため、IPv4 アドレスが優先される PC も用意し、通信経路の検証用として利用する。

・IPv4 優先 PC…IPv4 アドレスが優先されるよう設定

・IPv6 優先 PC…IPv6 アドレスが優先されるよう設定(デフォルト)

(d) hosts ファイルについて

実証試験用のファイルサーバが学内の1台あり、PC から実証用ファイルサーバへ接続する時に、 hosts ファイルで名前解決させる。既存設定はそのままで、IPv6 分の名前解決を hosts ファイル に追記する。

③ 特記事項

(c)ポリシーテーブルについて、IPv6 無効化は Microsoft 非推奨のため、優先設定としている。IPv4 優先 PC についてはレジストリ編集(TcpIP6の Parameters 配下の DisableComponents)により、IPv6を 無効化せず IPv4を優先するようポリシー設定を行った。

- (2) 有線接続のデスクトップ PC
 - 要素説明

インターネット(WEB サービス利用やメール等)、印刷やスキャン、ファイルサーバの利用を行うための有線接続クライアントPC である。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

(a) IP アドレスについて

実証試験のため、IPv6アドレスは固定 IPv6アドレスとRA による IPv6アドレス自動採番を採用する。ルータ仕様のため、プレフィックス部のみ DHCPv6 で割り当てるステートレス方式とする。 ・IPv4アドレス…静的アドレスによる手動設定(既存踏襲)

- ・IPv6 アドレス…固定 IPv6 アドレス 又は RA による IPv6 アドレス自動採番
- (b) DNS サーバ/デフォルトゲートウェイについて DNS サーバについては、指定する IPv6 アドレスを RA で割り当てることが出来ない ため、以下の方式とする。
 ・IPv4 アドレス…静的アドレスによる手動設定
 ・IPv6 アドレス…静的アドレスによる手動設定
 (パブリック DNS の指定/hosts ファイルによる指定

(c) ポリシーテーブルについて

IPv4アドレスおよび IPv6アドレスを保有するため、利用するアドレスの優先順位を付ける。デフォルトは IPv6アドレスが優先されるが、IPv4アドレスが優先される PC も用意し、通信経路の検証用として利用する。

・IPv4 優先 PC…IPv4 アドレスが優先されるよう設定

・IPv6 優先 PC…IPv6 アドレスが優先されるよう設定(デフォルト)

(d) hosts ファイルについて

実証試験用のファイルサーバが学内の1台あり、PCからファイルサーバへ接続する時に、既存同様 hosts ファイルで名前解決させる。既存設定はそのままで、IPv6分の名前解決を hosts ファイルに追記する。

③ 特記事項

(c)ポリシーテーブルについて、IPv6 無効化は Microsoft 非推奨のため、優先設定としている。IPv4 優先 PC についてはレジストリ編集(TcpIP6の Parameters 配下の DisableComponents)により、IPv6を 無効化せず IPv4を優先するようポリシー設定を行った。

- (3) 有線接続の OA 機器(プリンタ)
 - ① 要素説明

一般業務で使用する有線接続のプリンタである。

② 方式設計

実証用ネットワーク環境から既存ネットワーク環境に設置されているプリンタに印刷することを目的と するため、IPv4 シングルスタック方式のままとする。

(a) IP アドレスについて

特に変更なし。

- ・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)
- IPv6 アドレス…設定不可
- 3 特記事項

実証用ネットワーク環境から既存ネットワーク環境に設置されているプリンタに印刷を行う場合、実証用FW装置が介在した通信が行われるため、必要最低限のパケット通過許可設定を行う。

- (4) 有線接続の OA 機器(複合機)
 - ① 要素説明

一般業務で使用する有線接続の複合機である。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

(a) IP アドレスについて

実証試験のため、IPv6アドレスは固定 IPv6アドレスを設定する。

- ・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)
- ・IPv6 アドレス…固定 IPv6 アドレスを設定する
- ③ 特記事項

複合機から SMTP サーバ経由でスキャンデータのメール送信を行う場合、実証用 FW 装置が介在した通信が行われるため、実証用ネットワーク間に必要最低限のパケット通過許可設定を行う。

- (5) インターネット接続を制御する実証用 FW 装置
 - ① 要素説明 インターネット回線の接続、IPv4/IPv6 通信のルーティングやトラフィック制御を行うための機器である。
 - ⑦ 方式設計

方式設計の方針に従い、IPv4 シングルスタックの既設 FW 装置を実証試験開始時に IPv4/IPv6 デ ュアルスタックの実証用 FW 装置への切り替えを行う。

<IPv4/IPv6 デュアルスタックの実証用 FW 装置(実証時に置き換え)>

(a) IP アドレスについて

プレフィックス部は ISP から割り当てられ、インターフェース部はルータ側で生成する。また、ISP からルータへプレフィックスの委任を受けている。

- ・IPv4 アドレス… 静的アドレスによる手動設定(既存踏襲)
- ・IPv6 アドレス…固定 IPv6 アドレス 又は RA による IPv6 アドレス自動採番

(b) DNS サーバ/デフォルトゲートウェイについて

DNS サーバについては、指定する IPv6 アドレスを RA で割り当てることが出来ないため、以下の 方式とする。

- ・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)
- ・IPv6 アドレス

デフォルトゲートウェイ…静的アドレスによる手動設定又は RA による自動割当 DNS サーバ…静的アドレスによる手動設定

(パブリック DNS の指定/hosts ファイルによる指定)

(c) ファイアウォールについて

A大学内のセキュリティポリシーにしたがって設定する。

③ 特記事項

(c)ファイアウォールについて、IPv4とIPv6でプロトコルが異なるため⁶⁶、IPv4を流用ではなく、IPv6としてファイアウォールの設定内容を検討する必要がある。

- (6) 無線接続を制御する無線アクセスポイント
 - ① 要素説明 無線接続 PC から社内ネットワークに接続できるようにするための機器である。
 - ② 方式設計

レイヤー2の機器のため、IPv4/IPv6に依存した設定はなし。

③ 特記事項

特になし。

- (7) 実証用学内 WEB サーバ
 - 要素説明

業務アプリケーションに相当するシステムとして、実証用学内 WEB サーバの WEB コンテンツ提供を 検証対象とした。クライアント PC が利用する実証用学内 WEB サーバの動作環境を、仮想環境のゲ スト OS として構築する。

⁶⁶ 例えば、IPv4 では、ICMP、ARP、IGMP は別のプロトコルであるが、IPv6 では ICMPv6 に統合され た。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。学内ネットワーク配下で動作する利用者への影響を避けるため、既存の学内WEBサーバにシステム修正変更は行わず、実証試験用に、実証用学内WEBサーバを構築した。実証用学内WEBサーバを既存学内WEBサーバと同等設定(IPv4シングルスタック)した上で、IPv6 設定を追加する。

- (a) IP アドレスについて
 - ・IPv4 アドレス…静的アドレスによる手動設定(既存同等) ・IPv6 アドレス…静的アドレスによる手動設定
- (b) DNS サーバ/デフォルトゲートウェイについて
 ・IPv4 アドレス…静的アドレスによる手動設定(既存同等)
 ・IPv6 アドレス…静的アドレスによる手動設定
- (c) ポリシーテーブルについて AP/DB サーバにおいては、デフォルトの優先設定(IPv6 アドレスが優先)で検証を行う。
- (d) hosts ファイルについて
 実証用学内 WEB サーバは hosts ファイルでの名前解決を想定した通信を行わないため、追加
 設定を行わない。
- (e) ゲスト OS 環境(仮想サーバ)について ゲスト OS 環境は、ハイパーバイザー型のホスト OS(VMware vSphere)上で構築する。
- ③ 特記事項

ゲスト OS の静的アドレスには、グローバルユニキャストアドレス(GUA)を設定する。

- (8) 社内の情報資産を管理するファイルサーバ
 - 要素説明
 クライアント PC を Active Directory 認証し、ファイル共有を行うサーバ機器である。
 - ② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

- (a) IP アドレスについて
 - ・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)
 - ・IPv6 アドレス…静的アドレスによる手動設定

- (b) DNS サーバ/デフォルトゲートウェイについて
 ・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)
 ・IPv6 アドレス…静的アドレスによる手動設定
- (c) ポリシーテーブルについて ファイルサーバ(B 社製)については、IPv4/IPv6 デュアルスタック環境において、IPv4 と IPv6 の どちらが優先されるかの技術情報は非公開の状況である。実証試験については、実証用ファイ ルサーバのポリシー設定は既定値の状態、実証端末側で IPv6 優先端末と IPv4 優先端末の両 方で検証作業を行う。
- ③ 特記事項

ファイルサーバの静的アドレスには、グローバルユニキャストアドレス(GUA)を設定する。

- (9) 社外のクラウドサービス
 - ① 要素説明

A大学が開発し、ユーザサービスを提供しているクラウドサービスである。

② 方式設計

2 種類のクラウドサービスを利用している。G Suite および Microsoft 365 (Office 365)は IPv6 対応のため、IPv4/IPv6 デュアルスタック方式とする。

以上を踏まえ、IPv6対応後のシステム構成図を図 6.1.4-1 に示す。



図 6.1.4-1 IPv6 対応後の A 大学のシステム構成図

【補足説明】

IPv6 実証用ネットワーク A,C の IPv4 と、学外接続用ネットワークの IPv4 と、既存ネットワークの IPv4 の L3 中継 点は、実証用 FW 装置とする。 6.1.5 構築

本ユースケースでは IPv4/IPv6 デュアルスタック環境の構築にあたり、以下の前提の元、構成設計を行った。 ・既設ネットワークと相互乗り入れ可能な実証用ネットワークを準備する。

・既設ネットワークと実証用ネットワークのルーティング箇所は FW 装置とする。

実証用 L3 スイッチおよび実証用 FW 装置については、本前提要件を実現する必要最低限のスペックの機器を用意した。

また、既存ネットワーク環境(IPv4)でNAT/NAPT 対象コネクション数がピーク時にFW 装置のアドレス変換可能な最大数に達するトラブルがあったため、当面 IPv4 での運用を続ける場合、NAT/NAPT アドレス変換可能な最大数の上限が大きい上位機種を選定する必要があった。そのため、実証用 FW 装置については上位機種を選定した。

っぎに、設計内容を基に各機器に対してパラメータを設定し、環境を構築する。当ガイドラインでは、構築内容として、環境詳細を記載する。まず、本ユースケースで利用した各要素のスペックを表 6.1.5-1 に示す。

設定	機器等	仕様例	備考
IPv6	デスクトップ PC	Fujitsu ESPRIMO D586/M	・事務用
優先		OS Windows8.1 Pro	
/		CPU Core i7-6700 @3.40GHz	
IPv4		メモリ 8GB	
優先		HDD 512GB	
(適宜			
切り替え)			
IPv6	ノート PC	Panasonic Let's note LV8	・事務用
優先		OS Windows10 Pro	
/		CPU Core i7-8665U @1.90GHz	
IPv4		メモリ 16GB	
優先		SSD 512GB	
(適宜			
切り替え)			
IPv4/	複合機	Docu Center-V C5575 T2	・印刷やスキャン
IPv6			
IPv4	プリンタ	EPSON LP-S7160	・印刷

表 6.1.5-1 IPv4/IPv6 デュアルスタックを構築する各要素のスペック

設定	機器等	仕様例	備考
IPv4/	実証用ファイルサーバ	Buffalo TeraStation/Windows Server	・ファイルサーバ
IPv6		IoT 2019 for Storage	
		Workgroup(WS5220DN02W9)	
IPv4/	実証用学内 WEB サーバ	機種:仮想基盤上の仮想マシン	・学内ポータルサイト
IPv6		OS:Windows Server 2016 Std	用 WEB サービス
		CPU:仮想 CPU ×2	
		メモリ:8GB	
		仮想ディスク:100GB	
IPv4/	実証用 FW 装置	Fujitsu IPCOM EX2-3200SC	・ルーティング
IPv6			・ファイアウォール
			(FW)
IPv4/	実証用 L3 スイッチ	Fujitsu SR-S732TR1	・ルーティング
IPv6			・スイッチング
IPv4	既設 L3 スイッチ(コアルータ)	Fujitsu SR-S732TR1	・ルーティング
			・スイッチング
IPv4	既設 L2 スイッチ	Fujitsu SR-S352TR1	・スイッチング
		Fujitsu SR-S318TL3	
IPv4	実証用無線アクセスポイント	Buffalo WSR-2533DHPd3	・デバイスの無線中継
(L2 透過)			
IPv4	既設無線アクセスポイント	Cisco AIR-CAP1702I-Q-K9	・デバイスの無線中継
(L2 透過)			
IPv4/	SINET	インターネット接続(IPv4/IPv6 Dual)	・インターネット接続
IPv6		FW 装置から SINET までの接続速度	
		は 1Gbps の専用回線	
IPv4/	G Suite	Gmail	・メール
IPv6			
IPv4/	Microsoft 365	Exchange Online	・メール
IPv6			

そして、IPv6対応するために行った各機器への設定内容を示す。

(1) 実証用 FW 装置の設定

実証用 FW 装置の構成定義ファイルについては、旧機種(IPCOM EX-1300SC)の情報をインポートし、

IPv6 実証に関する追加設定を行う形態で実施した。具体的にはコマンドラインインタフェース(CLI)で構成管理モードに設定し、以下のカテゴリのコマンドを投入することで、インターフェース情報設定(SINET 側/実証環境側)のアドレス設定、スタティックルーティング情報追加設定、パケットフィルタリング設定を行った。

項番	設定内容の詳細							
1	【インターフェース情報設定(SINET 接続側インタフェース)】既存の vlan15 定義に追記							
	interface vlan15							
	ipv6 address link−local							
	ipv6 address SINET 接続用インターフェースに設定する IPv6 アドレス/64							
	ipv6-routing							
	!							
2	【インターフェース情報設定(実証環境側インタフェース)】 新規に VLAN 定義を追加							
	interface vlan50							
	ip address 172.16.50.254 255.255.255.0							
	description "IPv6-TEST internal-routing-lan"							
	ip-routing							
	vlan-link lan0.3 dot1q-tagged							
	ipv6 address link–local							
	ipv6 address 1:2f8:1 :6050::2/64							
	ipv6-routing							
	!							
3	【スタティックルーティング情報追加設定(IPv4 実証環境/IPv6】							
	ip route 172.16.0.0/12 172.16.1.254							
	ip route 172.16.51.0/24 172.16.50.253							
	ip route 172.16.52.0/24 172.16.50.253							
	ipv6 route ::/0 2f8:ff00:							
	ipv6 route 1:2f8:1 :6051::/64 2 :2f8:10 050::1							
	ipv6 route 1:2f8:1 :6052::/64 2 :2f8:10 :050::1							

項番	設定内容の詳細
4	【パケットフィルタリング定義(SINET 接続側インタフェース)】
	interface vlan15
	no rule access 210 in fil-to-hufw01-port-icmp accept …ICMP 応答対象変更
	rule access 210 in fil-from-R-to-hufw01-port-icmp4 accept
	rule access 1000 in fil-from-R-to-hufw01-port-icmp6 accept
	rule access 59998 in fil-from-any-IPv6TST drop audit-session-normal
	rule access 59999 in any drop audit-session-normal
	rule access 59999 out any accept audit-session-none
	!
5	【パケットフィルタリング定義(実証環境側インタフェース)】 新規
	interface vlan50
	rule access 10 in fil-from-local-port-https accept
	rule access 20 in fil-from-local-port-ftp accept
	rule access 30 in fil-from-local-port-etc-IPv4T accept
	rule access 40 in fil-to-local-port-ssh accept
	rule access 50 in fil-from-local-port-etc2-IPv4T accept
	rule access 60 in fil-from-huad-to-IPv4T accept
	rule access 70 in fil-from-local-port-snmp-IPv4T accept
	rule access 100 in fil-from-local-port-https-IPv6T accept
	rule access 200 in fil-from-local-port-ftp-IPv6T accept
	rule access 300 in fil-from-local-port-etc-IPv6T accept
	rule access 400 in fil-to-local-port-icmp accept
	rule access 500 in fil-to-local-port-ICMPv6 accept
	rule access 59999 in any drop
	rule access 59999 out any accept audit-session-none
	!
6	【パケットフィルタリング リソース定義】
6-1	【パケットフィルタリング リソース定義】 IPv6 ネットワーク全体
	class-map match-all fil-from-any-IPv6TST
	match source-address ipv6 ::/0
	!

6-2 【パケットフィルタリング リソース定義】学内 AD サーバ→実証用 NW 通過語	殳定
class-map match-all fil-from-huad-to-IPv4 I	
match destination-address ipv4 172.16.1.151,172.16.1.152	
match destination-port 389/tcp-udp,135/tcp,88/tcp	
!	
6-3 【パケットフィルタリング リソース定義】学内→実証用 NW 通過設定	
class-map match-all fil-from-local-port-etc-IPv4T	
match class-map net-internal	
match destination-port 123/tcp-udp,53/tcp-udp	
!	
class-map match-all fil-from-local-port-etc-IPv6T	
match class-map net-internal-IPv6TEST	
match destination-port 123/tcp-udp,53/tcp-udp	
class-map match-all fil-from-local-port-etc2-IPv4T	
match class-map net-internal	
match destination-port 3389/tcp-udp,137-138/udp,139/tcp,445/tcp,25	/tcp
!	
class-map match-all fil-from-local-port-ftp-IPv6T	
match destination-port ftp	
match class-map net-internal-IPv6TEST	
!	
class-map match-all fil-from-local-port-https-IPv6T	
match destination-port 80/tcp,443/tcp	
match class-map net-internal-IPv6TEST	
	۰.
6-4 【ハケットフィルタリンク リソース定義】 EPSON フリンタ→実証用 NW 通過語	定
class-map match-all fil-from-local-port-snmp-IPv41	
match class-map net-internal	
match destination-address $ipv4 1/2.16.19.163$	
match destination-port 161/udp,3289/udp,515/tcp	

項番	設定内容の詳細						
6-5	【パケットフィルタリング リソース定義】SINETルータからの WAN 側 ICMPv6 応答許可						
	設定						
	class-map match-all fil-from-R-to-hufw01-port-icmp6						
	match class-map ICMPv6						
	match source-address ipv(1:2f8:ff0(,fe80::/16						
	!						
6-6	【パケットフィルタリング リソース定義】学内からの ICMPv6 応答許可設定						
	class-map match-all fil-to-local-port-ICMPv6						
	match class-map net-internal-IPv6TEST						
	match class-map ICMPv6						
	!						
6-7	【パケットフィルタリング リソース定義】実証環境 IPv6 アドレス範囲設定						
	class-map match-any net-internal-IPv6TEST						
	match source-address ipv						
	match source-address ipv(;6051::/64						
	match source-address ipvention:6052::/64						
	!						

(2) 実証用 L3 スイッチの設定

実証用 L3 スイッチのコマンドラインインタフェース(CLI)より構成定義モードに変更し、以下のコマンドを実行することで、基本設定、VLAN 設定、ルーティング設定を行った。

項番	設定内容の詳細
1	【基本設定】
	password admin set 管理者パスワード
	ip routing enable
	ip6 routing enable
	stp mode disable
	sysname sr-s732tr1-11
	serverinfo sftp ip off
	serverinfo sftp ip6 off
	serverinfo telnet ip off
	serverinfo telnet ip6 off
	serverinfo http ip off
	serverinfo http ip6 off
	serverinfo dns ip off

項番	設定内容の詳細
	serverinfo dns ip6 off
	serverinfo sntp ip off
	serverinfo sntp ip6 off
	serverinfo time ip tcp off
	serverinfo time ip udp off
	serverinfo time ip6 tcp off
	serverinfo time ip6 udp off
2	【ether ポート設定】
	ether 1–28 eee off
	ether 1 vlan tag 50-52
	ether 15-16 vlan untag 50
	ether 17-18 vlan untag 51
	ether 19–20 vlan untag 52
	ether 21 vlan tag 50–52
3	【VLAN 設定】
	vlan 50 name LAN050
	vlan 51 name LAN051
	vlan 52 name LAN052
4	
4	【美証用ネットワーク(ルーナインク用:VLAN030) アトレス設定】
	Ian 50 ip address 172.10.50.253/24 3
	$ \lim_{n \to \infty} 50 $
	$\int dr = 50 \text{ in } 6 \text{ address } 0 \text{ address } 0$
	1211 30 100 address 0 1.210.1 0000.1704
	an 50 ylap 50
	・IPv6 アドレスの自動採番を考慮しないネットワークセグメントのため BA(Bouter
	Advertisement) \downarrow SEND/RECV $\not\models$ OFF
	・RIP は OFF とする
5	【実証用ネットワーク(実証環境(サーバ室)用:VLAN051) アドレス設定】
	lan 51 ip address 172.16.51.253/24 3
	lan 51 ip6 use on
	lan 51 ip6 address 0 1:2f8:1 :6051::1/64
	lan 51 vlan 51

項番	設定内容の詳細
	<<特記事項>>
	・IPv6 アドレスの自動採番を考慮しないネットワークセグメントのため、RA(Router
	Advertisement)はSEND/RECVともOFFにする
	・RIP は OFF とする
6	【実証用ネットワーク(実証環境(特定部局)用:VLAN052) アドレス設定】
	lan 52 ip address 172.16.52.253/24 3
	lan 52 ip6 use on
	lan 52 ip6 address 0 1:2f8:1 :6052::1/64
	lan 52 ip6 ra mode send
	lan 52 ip6 ra prefix 0 1:2f8:1 6052::/64 7d 1d c0
	lan 52 vlan 52
	<<特記事項>>
	・RA(Router Advertisement)によるステートレスな IPv6 アドレス自動採番の実証ができ
	る様、SEND は ON, RECV は OFF にする
	・RIP は OFF とする

(3) 既設 L3 スイッチ(コアルータ)の設定

既設L3スイッチ(コアルータ)のコマンドラインインタフェース(CLI)より構成定義モードに変更し、以下のコマンドを実行することで、実証環境で使用するイーサネットポート設定および VLAN 設定を行った。

項番	設定内容の詳細	
1	【イーサネットポート設定】	
	ether 1 vlan tag 1,3,50	実証用 FW 装置向け VLAN 50 を追加
	ether 7 vlan tag 1,3-6,8,10-11,14-15,18-19,5	1,180-190 SR-S352TR1 向け VLAN51
	追加	
	ether 8 vlan tag 1,3-6,8,10-11,14-15,18-19,5	1,180-190 SR-S352TR1 向け VLAN51
	追加	
	ether 21 vlan tag 50–52	実証用 L3 スイッチ向け VLAN 50-52 追
	加	
	ether 32 vlan tag 10,12,17,19,22,52,117,180	既設 L2 スイッチ向け VLAN 52 追加

項番	設定内容の詳細
2	【VLAN 追加設定】
	vlan 50 name LAN050
	vlan 51 name LAN051
	vlan 52 name LAN052

(4) 既設 L2 スイッチの設定

既設 L2 スイッチ(SR-XXXXTR1/SR-XXXXTL3) のコマンドラインインタフェース(CLI)より構成定義モード に変更し、以下のコマンドを実行することで、実証環境で使用するイーサネットポート設定および VLAN 設定 を行った。

項番	設定内容の詳細	
1	【SR-XXXXTR1:イーサネットポート設定】	
	ether 25 vlan tag 1,3-6,8,10-11,14-15,18-19,51,18	0-190 既設 L3 向け VLAN 51を追
	<u>לת</u>	
	ether 26 vlan tag 1,3-6,8,10-11,14-15,18-19,51,18	0-190 既設 L3 向け VLAN 51を追
	<u>ל</u> חם	
	ether 38 vlan tag 1,3,51	既設仮想基盤環境向け VLAN 51を
	追加	
	ether 40 vlan tag 1,3,51	既設仮想基盤環境向け VLAN 51 を
	追加	
	ether 42 vlan tag 1,3,51	既設仮想基盤環境向け VLAN 51 を
	追加	
	ether 44 vlan tag 1,3,51	既設仮想基盤環境向け VLAN 51 を
	追加	
2	【VLAN 追加設定】	
	vlan 51 name LAN051	

項番	設定内容の詳細	
1	【SR-XXXXTL3:イーサネットポート設定】	
	ether 16 eee off	空きポートを実証環境用に設定
	ether 16 vlan untag 52	特定部局 実証環境向け VLAN 52を
	設定	
	ether 18 vlan tag 10,12,17,19,22,52,117,180	既設 L3 向け VLAN 52 を追加
2	【VLAN 追加設定】	
	vlan 52 name LAN052	

(5) 複合機の設定

複合機上のパネル操作を行い、IPv4/IPv6 デュアルスタック設定および IPv6 のシングルスタック設定を 行った。

項番	設定内容の詳細
1	【複合機 機械管理者モードへの変更】
	・「認証」ボタンを押し、「認証」画面で機械管理者の ID を入力する
	・「確定」ボタンを押す
2	【プロトコル設定(デュアルスタック/IPv6 シングルスタック)】
	・メニュー画面の[仕様設定/登録]を押す
	・[仕様設定]>[ネットワーク設定]>[プロトコル設定]を押す
	・IP 動作モードを選択し、[確認/変更]を押す
	・IP モードを設定する
	デュアルスタックモード:[デュアルスタック]
	IPv6 シングルスタック:[IPv6]
3	【IPv4 アドレスの設定(変更)】
	・親メニューに戻り、[TCP/IP- ネットワーク設定]を選び、[確認/変更]を押す
	・[IPv4-IP アドレス]を選択し、[確認/変更]を押す
	・実証環境の IPv4 アドレスを設定する(IPv6 シングルスタック環境で利用する場合、
	「IPv4を使用」を「OFF」にする)
4	【IPv4 サブネットマスクの設定】
	・IPv6 デュアルスタック環境の場合は変更不要(既存設定流用)
	・IPv6 シングルスタック環境の場合は定義を削除する
5	【IPv4 デフォルトゲートウェイの設定】
	・親メニューに戻り、[TCP/IP- ネットワーク設定]を選び、[確認/変更]を押す
	・[IPv4-ゲートウェイアドレス]を選択し、[確認/変更]を押す
	・実証環境の IPv4 デフォルトゲートウェイアドレスを設定する
	(IPv6 シングルスタック環境の場合は定義を削除する)

項番	設定内容の詳細
6	【IPv6 アドレスの手動設定】
	・親メニューに戻り、[TCP/IP- ネットワーク設定]を選び、[確認/変更]を押す
	・[IPv6 - アドレス手動設定]を選択し、[確認/変更]を押す
	・手動設定を「しない」→「する」に変更する
	・「DHCP からアドレスを取得」のチェックを外す
	・「手動設定アドレス」に複合機に割り当てるIPv6アドレスを入力する。プレフィクス長は
	「64」を指定する
	・「ゲートウェイアドレス」に実証環境のゲートウェイアドレス(IPv6)を入力する

(6) プリンタの設定

既存ネットワークに設置された機器を使用するため、変更作業は行わない。

(7) ファイルサーバの設定

ファイルサーバ上で下記の設定を行い、IPv6 デュアルスタックに対応するファイルサーバを構築する。ファイルサーバのオペレーティングシステムが「Windows Server IoT 2019 for Storage」のため、設定方法はWindows サーバに準じる。 IPv6 実証環境ネットワークとの接続は別の LAN ポートに接続して実施する。

項番	設定内容の詳細
1	【IPv4 アドレスの設定】
	既存ネットワークに接続したまま実施するため、変更しない
2	【IPv6 アドレスの設定】
	 IPv6 実証環境ネットワークと接続しているネットワークアダプタ(LAN)のプロパティを開
l	き IPv6 アドレスを手動で設定する
	インターネット プロトコル パージョン 6 (TCP/IPv6)のプロパティ ×
	全般
	い場合は、ネットワーク管理者に適切な IPv6 設定を問い合わせてください。 ○ IPv6 アドレスを自動的に取得する(Q) ● 次の IPv6 アドレスを使う(<u>S)</u> :
	サブネット プレフィックスの長さ(山):
	デフォルト ゲートウェイ(<u>D</u>):
	 ○ DNS サーパーのアドレスを自動的に取得する(B) ● 次の DNS サーパーのアドレスを使う(E):
	優先 DNS サーバー(<u>P</u>):
	代替 DNS サーバー(<u>A</u>):
	○終了時に設定を検証する(L) 詳細設定(V)
	OK キャンセル

項番	設定内容の詳細
	・IPv6 アドレス:ファイルサーバに割り当てた IPv6 アドレス
	・サブネット プレフィックスの長さ:64
	・デフォルトゲートウェイ:実証用 L3 スイッチの IPv6 アドレス(特定部局向け IPv6 アドレ
	ス)
	1:2F8:10 6052::1
	・優先 DNS サーバ:指定しない

(8) クライアント PC の設定

Windows 上で以下の操作を行い、IPv6 優先設定を行った。

Ŧ	妾続しているネ	ネットワーク アダブタ(LAN 	N or Wi-Fi) のブロバティから ๚๛๚๛ゴロパティ	固定 IP を設定する。 ────
		全般		
		ネットワークでこの機能がサポートされて きます。サポートされていない場合は、 ください。	いる場合は、IP 設定を自動的に取得すること ネットワーク管理者に適切な IP 設定を問い合	:がで わせて
		○ IP アドレスを自動的に取得する()	<u>0</u>)	
		② 次の IP アドレスを使う(S):		
		IP アドレス(I):	172 . 16 . 52 . 2	
		サブネットマスク(U):	255 . 255 . 255 . 0	
		デフォルト ゲートウェイ(<u>D</u>):	172 . 16 . 52 . 253	
		○ DNS サーバーのアドレスを自動的)に取得する(<u>B</u>)	
		● 次の DNS サーバーのアドレスを使	ŧð(<u>E</u>):	
		優先 DNS サーバー(<u>P</u>):	172 . 16 . 1 . 151	
		代替 DNS サーバー(<u>A</u>):	172 . 16 . 1 . 152	
		□終了時に設定を検証する(<u>L</u>)	詳細設定()	D
			ОК + †	ンセル
			OK ‡t	ンセル

項番	設定内容の詳細		
2	【IPv6 アドレスの設定】		
	接続しているネットワークアダプタ(LAN or wife)のプロパティから静的 IP が設定されるよ		
	うにする。		
	全般		
	ネットワークでこの機能がサポートされている場合は、IPv6 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IPv6 設定を問い合わせてください。		
	○ IPv6 アドレスを自動的に取得する(O)		
	⑥ 次の IPv6 アドレスを使う(S):		
	IPv6 アドレス(I): ::6052::2002		
	サブネット プレフィックスの長さ(U): 64		
	デフォルト ゲートウェイ(D): :6052::1		
	○ DNS サーバーのアドレスを自動的に取得する(B)		
	● 次の DNS サーバーのアドレスを使う(E):		
	優先 DNS サーバー(P): 2001:4860:4860::8888		
	代替 DNS サーバー(A):		
	※学内向け検証を行う提合 原生 DNS サーバに設定しているパブリック DNS の IDv6 マ		
	※子内向け換証を117場合、優先 DNS サーバに設定しているパンサウサ DNS 00 IFV0 ア		
2	TUACAAS S		
5	Linetsの設定道加」		
	Hosts ファイルに IPV0 の 美証環境 C利用 9 る 9 一 八の アドレスを追加 9 る		
	¥Windows¥System32¥drivers¥etc¥hosts		
	## IPv6		
	1:2f8:1 :6051::101 hunet-ipv6		
	1:2f8:1 :6052::1002 filesv-ipv6		
	## IPv4		
	172.16.51.1 hunet-ipv4		
	172.16.19.203 filesv-ipv4		
	=====		

項番	設定内容の詳細		
4	【IPv4 アドレスの優先設定】		
	IPv4 優先 PC で IPv4 設定がループバックより優先されるように、バッチファイル(IPv4 優		
	先.bat)を実行する。IPv4(::ffff:0:0/96)が一番上になるように、優先順を振りなおす。		
	(実行例)		
	netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0		
	netsh interface ipv6 set prefixpolicy ::1/128 40 1		
	netsh interface ipv6 set prefixpolicy ::/0 30 2		
	netsh interface ipv6 set prefixpolicy 2002::/16 20 3		
	netsh interface ipv6 set prefixpolicy ::/96 10 4		
	上記の設定を行ったら、PC を再起動する。		
5	【IPv4/IPv6 優先設定を確認】		
	再起動後以下のコマンドを実行し、IPv4 が最優先になっていることを確認する。		
	netsh interface ipv6 show prefixpolicies		
	(実行例)		
	優先順位 ラベル プレフィックス		
	50 0 ::ffff:0:0/96 (IPv4 マップ)		
	40 1 ::1/128 (ループバック)		
	30 2 ::/0 (IPv6 通信全般)		
	20 3 2002::/16 (6to4)		
	10 4 ::/96 (IPv4 互换)		
	5 5 2001::/32 (Teredo)		
6	【レジストリでの IPv4 優先設定】		
	レジストリエディタを起動し、次のレジストリ キーを変更することで構成する。		
	場所:		
	HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip6¥Parameters¥		
	Name: DisabledComponents		
	型: REG_DWORD		
	値を 0x00 (跣定値)→0x20(IPv4 を優先する)に変更する		

(9) 実証用学内 WEB サーバの設定

既存仮想環境のホスト OS (VMWare Sphere 5.5) 上にゲスト OS である Windows Server2016 をセットアップする。既存の WEB サーバをクローン (複製)して構築する。

項番	設定内容の詳細		
1	【ESXi サーバ 仮想スイッチの設定】		
	vSphere Client より仮想スイッチの設定を行い、VLAN タグに「51」と紐づける設定を行う		
	IPv4、IPv6 アドレスに関しては追加および変更は行わない		
	 FSXi サーバは2台構成のため、二台とも設定を行う		
2			
3	L/AFOS 境現の構業】		
	VMware VSphere 上でケスト US (Windows Server)を構成する。		
	実証用字内 WEB サーハについては、既設の字内 WEB サーハを複製(クローン)したも		
	のを利用する		
4	【ゲスト OS ネットワーク設定】		
	vSphere Clientより既設 vCenter Server に接続し、複製 (クローン)した実証用学内 WEB		
	サーバの設定を編集する		
	仮想マシンの構成で「ネットワーク アダプタ」を選択し、「ネットワーク接続」の「ネットワ		
	ークラベル」のドロップダウンリストより「VLAN051」を選択する。		
5	【ゲスト OS 環境の IPv4 設定】		
	ゲスト OS の IPv4 アドレスを以下のとおり設定する。		
	インターネット プロトコル パージョン 4 (TCP/IPv4)のプロパティ ×		
	全般		
	ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することがで きます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせて ください。		
	○ IP アドレスを自動的に取得する(<u>○</u>)		
	● 次の IP アドレスを使う(S): IP アドレス(): 172.16.51.1		
	サブネットマスク(山): 255 . 255 . 0		
	デフォルトゲートウェイ(<u>D</u>): 172 . 16 . 51 . 253		
	○ DNS サーバーのアドレスを自動的に取得する(B) ○ なの DNS サーバーのアドレスを自動的に取得する(B)		
	後の DNS 9 - パーのパークスを使うし、 優先 DNS サーパー(P): 172 . 16 . 1 . 151		
	代替 DNS サー/(-(<u>A</u>): 172 . 16 . 1 . 152		
	□終了時に設定を検証する(上) 詳細設定(⊻)		
	OK キャンセル		
	学外接続の検証を行う場合、優先 DNS サーバおよび代替 DNS サーバについては、		
	パブリック DNS の IP アドレスを設定する(有線:8.8.8.8 代替:8.8.4.4)		

項番	設定内容の詳細									
6	 【ゲスト OS 環境の IPv6 設定】									
	ゲスト OS の IPv6 アドレスを以下のとおり設定する。									
	インターネット プロトコル パージョン 6 (TCP/IPv6)のプロパティ ×									
	全般									
	ネットワークでこの機能がサポートされている場合は、IPv6 設定を自動的に取得することができます。 サポートされていな い場合は、ネットワーク管理者に適切な IPv6 設定を問い合わせてください。									
	○ IPv6 アドレスを自動的に取得する(Q) ○ 次の IPv6 アドレスを有動的に取得する(Q)									
	● 次切 IPV6 アドレス(): IPv6 アドレス(): 01:2f8: :6051::101									
	サブネット ブレフィックスの長さ(U): 64									
	デフォルト ゲートウェイ(<u>D</u>): :6051:1									
	 DNS サーバーのアドレスを自動的に取得する(B) 									
	● 次の DNS サーバーのアドレスを使う(E):									
	優先 DNS サーバー(P): 2001:4860:4860:8888									
	代替 DNS サーバー(<u>A</u>):									
	□終了時に設定を検証する(L) 詳細設定(V)									
	OK キャンセル									
	※学内向け検証を行う場合、優先 DNS サーバに設定しているパブリック DNS の IPv6 アドレスを消去する									

6.1.6 試験

本ユースケースで実施した内容と結果を示す。

6.1.6.1 実証内容と結果

1. ネットワークレベルの検証

6.1.5 にしたがって構築した実証環境において、一般業務が無線および有線それぞれのネットワーク上で、 問題なく利用できるか検証した。

一般業務における検証では、WEB サービスやメール等のインターネット利用、複合機等の OA 機器の利用、 情報資産の管理/共有等のファイルサーバ利用といった一般的な業務について検証した。

結果として、IPv6の規格に起因した課題は発生しなかったが、機器/サービスの仕様に起因した課題が計1件、 IPv6対応における留意事項が1件発生した。

(1) 一般業務における検証について

6.1.4(5)の通り、学外向け接続は、SINET サービスを使用し、基本サービスである「インターネット接続(IPv4/IPv6 Dual)」を使用することで実現した。

IPv4とIPv6を共存させた状態で、①から③のシナリオをIPv4およびIPv6それぞれで検証した。接続した状態の イメージを図 6.1.6-1 に示す。



図 6.1.6-1 一般業務検証における接続イメージ

また、「図 6.1.4-1 IPv6 対応後の A 大学のシステム構成図」の【補足説明】で説明の通り、IPv6 実証用ネットワーク A,C の IPv4 と、学外接続用ネットワークの IPv4 と、既存ネットワークの IPv4 の L3 中継点は、実証用 FW 装置となるため、学内の既存機器への疎通確認時に実証用 FW 装置での通信ブロックが発生した場合、実証に必要な範囲内での通信許可設定を行いながら検証作業を進めた。

①疎通確認

各機器(実証用機器および学内の既存機器)に対して ping を実行し、通信経路に問題ないことを検証する。

- ② WEB サービスやメールサービス等のインターネット利用 WEB サービスやメール等へインターネット接続し、コンテンツが利用できることを検証する。IPv6 未対応の学 外コンテンツの場合、コンテンツが利用できないことを検証する。
- ③通常業務を想定した学内ネットワーク機器の利用

IPv4/IPv6 デュアルスタック環境において、IPv4 機器であるプリンタおよび IPv6 機器である複合機を正常に利用できるか検証する。



図 6.1.6-2 通常業務を想定した学内ネットワーク機器利用イメージ

上記①から③のシナリオを実施した結果の内、主要な結果を以下に示す。

① 疎通確認の検証結果

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
1	ノート	無線	IPv6	GW ルータ	IPv6	接続先に対し ping -6 をする	ping が通る	ок
	PC		優先					
2	ノート	無線	IPv6	外部 WEB	IPv6	https:// kiriwake.jpne.co.jp/	「IPv4/IPv6 接続判定ページ	ок
	PC		優先	サービス		ヘアクセスする	~」の後に「IPv6 でアクセス	
							中です。」と IPv6 アドレスが	
							表示される	
3	ノート	無線	IPv6	ファイルサ	IPv6	接続先に対し ping -6 をする	ping が通る	ОК
	PC		優先	- <i>i</i> ĭ		(ping はホスト名で指定)		

【#1 の補足】

IPv6で ping の応答を受信できることを確認した。



図 6.1.6-3 IPv6 で ping 応答あり

【#2の補足】

(Figure 1996) (F).jp/	ク・白 ぐ 「 ¹⁹⁶⁶ 」D. 41 (D. 6 任 法制1 デリール × アドレス バーオートコンプリートの表示
IPv4/IPv6接続判	定ページ	
IPV6 CF7T	判定開始	
1. 試験日時		
測定準備	完了	
 接続試験状況表示	ady ^{NS利用無)}	

IPv6 でインターネット接続できることを確認した。

図 6.1.6-4 IPv6 でインターネット接続可能

【#3の補足】

ファイルサーバへホスト名で ping 実行した場合も応答が返ってくることを確認した。

(filesv-ipv6 はファイルサーバのホスト名)

🔤 管理者: C:¥Windows¥system32¥cmd.exe



図 6.1.6-5 ホスト名でも ping 応答あり

② WEB サービス等のインターネット利用

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IP∨6	器名・サー	IP∨6			結果
				ビス名				
1	ノート	無線	IPv6	インターネ	IPv6	WEB ブラウザで google ヘア	google 画面が表示される	ок
	PC		優先	ット (IPv6		クセスする		
				対応サイ				
				Ь)				
2	ノート	無線	IPv6	インターネ	IPv4	WEB ブラウザで yahoo.co.jp	yahoo.co.jp 画面が表示され	ок
	PC		優先	ット (IPv6		サイトヘアクセスする	る	
				未対応サ				
				イト)				
3	ノート	無線	IPv4	インターネ	IPv4	WEB ブラウザで google ヘア	google 画面が表示される	ОК
	PC		優先	ット(一般)		クセスする		

【#1 の補足】

IPv6 優先接続設定を行った実証用PCが IPv6 で接続されていることを検証するため、「netstat -an」コマンドを実行し、WEB ブラウザが IPv6アドレス同士でセッションを確立しているかを確認した。

C//Users/user> netstat -an

アクティブは反映

70Hit	ローカル アドレス 外部	PHUX	125				
TOP	172.16.52.2:139	0.0.0.0	LIST	ENING			
TOP	172.16.52.2 ;40408	40.90.18	122443	ESTABLISHED	>		
TOP	172.16.52.2:49411	40,119,21	1,203:443	EST/BLISHE	0		
TOP	172.16.52.2:50787	180.87.4	157,443	TIME_WAT			
TOP	172.16.52.2:50788	113.29.11	17.17;443	TIME_WAIT			
TOP	172.16.52.2.50818	180.87.4	157:443	TIME_WAT			
TOP	172.16.52.2.50819	113.29.11	7.17;443	TIME_WAIT			
TOP	172.16.52.2 (50873	38,113,0	5.183:443	SYN_SENT			
TOP	[::]:135 [:	:1.0	LISTENIN	G			
TOP	(::):445 [:	:1:0	LISTENIN	G			
TOP	[::]x23 [:	:1:0	LISTENIN	G			
TOP	[::]:7680 [:	::]:0	LISTENIA	G			
TOP	[::]:16992 [::] x0	LISTER	G			
TOP	[::]:40664 [::]:0	LISTING	G			
TOP	(::):40665 (::]:0	LISTER	G			
TOP	[::]:40666 [1:130	LISTING	G			
TOP	[::]:40667 [::]:0	LISTER	G			1 (売)のでたことう
TOP	[::]:40668 [1:130	LISTING	G			google 宛に催立され
TOP	[::]:40673 [::]:0	LISTEN	G			
TOP	[::]:52306 [::]30	LISTEN	G			たわいション
TOP	f:::1049660	f::10	USIN	NG			
1	[2001:28:103:3605	2,418,855	30°240]3	50774 (2606:	2800:147:1206.30:18	N0563653]343 TM	
12	[2001;2/8;103:1605	2.418.856	80°a4¢]3	50791 (2404)	6800 (400)(808 : 2003	443 ESTABLISHED	
TOP	[2001:28:103:1605	2.418250	807540]3	50792 (2404)	6800 (400)(208): 2003	443 ESTABLISHED	
TOP	[2001;2/8;103::605	2,43,8353	30°a4¢]3	50793 (2404)	6800 (400 a 2011) 2004	3443 ESDABLISHED	
TOP	[2001:278.103:1605	2.428.856	80'240]3	50794 (2:404)	6800 (400 a 2011) 2004	3443 ESTABLISHED	
TOP	[2001:278:103:1605	2.418.850	80'240]3	50795 (2404)	6800 (400 a) 805 (120 03	443 ESTABLISHED	
TOP	[2001:278:103:1605	2.418250	201240]3	50796 (2:404)	6800 (400 a) 805 (120 03	443 ESTABLISHED	
TOP	[2001:278:103:1605	2,43,8256	2012403	50798 (2:404)	6800 (400): 808 (1200)	443 ESTABLISHED	
TOP	[2001:278:103:1605	2.438.856	(80°a4¢]3	50799 (2:404)	6800 (400): 808 2003	46 ESTABLISHED	
TOP	[2001:278:103:1605	2,428,856	807240]3	50800 (2:404)	6800 (400): 808 : 2003	443 ESTABLISHED	
TOP	[2001:2/8:103:1605	2.418250	801240]3	50801 (2:404)	6800 (400 a 208 : 2003	43 ESTABLISHED	
TOP	[2001:278:103:1605	2,428,856	807540]3	50802 (2:404)	6800 (400 a 200 : 20 02	:443 ESTABLISHED	
TOP	[2001:2/8:103:1605	2.418260	801240]3	50803 (2:404)	6800 (400 a 209 : 2002	443 ESTABLISHED	
TOP	[2001:28:103:1605	2.418250	30°a4¢]:	50804 (2:404)	6800 x400 x 200 x 200 x	:443 ESTABLISHED	
TOP	[2001:278:103:1605	2.418250	801240]3	50805 (2:404)	6800 (400 a 20) (120 0a	:443 ESTABLISHED	
TOP	(2001:2/8:103::605	2.418.850	80'240]3	50806 (2:404)	6800 x400 a 20c :: 200a	343 ESTRUMED	
TOP	[2001:298:103::605	2.418256	807240]3	50807 (2:404)	6800 x400 a 20c 200a	343 ESTABLISHED	
TOP	[2001;2/8;103::605	2.438856	80'240]3	50808 (2:404)	6800 x400 a 20c .: 200a	343 ESTRUMED	
TOP	[2001:28:103:1605	2.418,856	80'244]3	50809 (2404)	6800 ;400 a :80: : 2003	3443 ESTABLISHED	1
TOP	[2001:28:103:1605	2.418256	30°24¢]3	50850 (2:404)	6800 (400 a 2001: 2003	3443 ESDABLISHED	
702	[2001:278:103:1605	2.418.856	30°24¢]3	50813 (2404)	6800 x400 a 20c .: 200a	A43 ESTABLISHED	
	[2001:278:103:1605	2.438256	(80° a4 c]:	50822 [2:404:	6800 (400 a 208 : 20 03	43 ESTABLISHED	
UD?	VERN AVERAGE	+					
UDP -	0.024;0.0.0						
UDP:	0302:0000	*: *					
UDP -	£2£2:0000						
UDP -	2262:000						
UDP -	20622:0000						
UD2	0.0.0.0.52306						
UDP -	127.0.0.1:1900	*; *					
UDP.	127.0.0.1:49664						
UD22	127.0.0.1561505						
UDP:	172.16.52.2.137						
102	172.16.12.7.138						

図 6.1.6-6 IPv6 優先接続端末で WEB アクセス時の「netstat -an」の実行結果
検証用PCで接続確認を行った際のネットワークキャプチャ結果についても併せて記載する。

4	動作確認項目(利用者	皆向け機能) (1)IPv6	優先-1.pca	p 🗖 🗖
ファイル(F) 編集(E) 表示(V) 移動((G) キャプチャ(C) 分析(A) 統計(S) 電話(v) 無線(W) ツール(T) ^	Jレプ(H)	
	♦ ♥ ¥ ¥ ½ □ □ 0, 0, 0, 11			
I dns				× =
No. Time Sa	ource	Destination	Proto Length	Info
	01:2f8:103c:6052::2002	2001:4860:4860::8888	DNS 94	4 Standard query 0xf6ee A www.google.com
201 2021-01-28 15:37:38.964 20	01:2f8:103c:6052::2002	2001:4860:4860::8888	DNS 94	4 Standard query 0xf6ee A www.google.com
202 2021-01-28 15:37:38.964 20	01:2f8:103c:6052::2002	2001:4860:4860::8888	DNS 94	4 Standard query 0x6aa8 AAAA www.google.com
203 2021-01-28 15:37:38.964 20	01:2f8:103c:6052::2002	2001:4860:4860::8888	DNS 94	4 Standard query 0x6aa8 AAAA www.google.com
204 2021-01-28 15:37:38.965 244	04:6800:400a:80b::2003	2001:2f8:103c:6052::2002	TCP 74	4 443 → 49965 [ACK] Seq=68158 Ack=759 Win=67840 Len=
205 2021-01-28 15:37:38.965 20	01:2f8:103c:6052::2002	2404:6800:400a:80b::2003	TLS 39	B Application Data
206 2021-01-28 15:37:38.965 20	01:2f8:103c:6052::2002	2404:6800:400a:80b::2003	TCP 39	B [TCP Retransmission] 49965 → 443 [PSH, ACK] Seq=75
207 2021-01-28 15:37:38.972 24	04:6800:400a:80b::2003	2001;2f8:103c:6052::2002	TCP 7	4 443 → 49965 [ACK] Seq=68158 Ack=1083 Win=68864 Len
210 2021-01-28 15:37:38.978 20	01:4860:4860::8888	2001:2f8:103c:6052::2002	DNS 12	2 Standard query response 0x6aa8 AAAA www.google.com
211 2021-01-28 15:37:39.016 24	04:6800:400a:80b::2003	2001:2f8:103c:6052::2002	TLS 29	0 Application Data
212 2021-01-28 15:37:39.016 24	04:6800:400a:80b::2003	2001:2f8:103c:6052::2002	TLS 1294	4 Application Data
213 2021-01-28 15:37:39.016 24	04:6800:400a:80b::2003	2001:2f8:103c:6052::2002	TLS 1294	4 Application Data
214 2021-01-28 15:37:39.016 24	04:6800:400a:80b::2003	2001:2†8:103c:6052::2002	TLS 1294	4 Application Data
215 2021-01-28 15:37:39.016 244	04:6800:400a:80b::2003	2001:2f8:103c:6052::2002	TLS 1294	4 Application Data
216 2021-01-28 15:37:39.016 20	01:2†8:103c:6052::2002	2404:6800:400a:80b::2003	TCP 74	4 49965 → 443 [ACK] Seq=1083 Ack=73254 Win=262144 Le
217 2021-01-28 15:37:39.016 20	01:2f8:103c:6052::2002	2404:6800:400a:80b::2003	TCP 7	4 [TCP Dup ACK 216#1] 49965 → 443 [ACK] Seq=1083 Ack
218 2021-01-28 15:37:39.017 24	04:6800:400a:80b::2003	2001:2†8:103c:6052::2002	TLS 1294	4 Application Data
219 2021-01-28 15:37:39.017 24	04:6800:400a:80b::2003	2001:218:103c:6052::2002	TLS 1294	4 Application Data
220 2021-01-28 15:37:39.017 24	04:6800:400a:80b::2003	2001:218:103c:6052::2002	TLS 1294	4 Application Data
221 2021-01-28 15:37:39.017 24	04:6800:400a:80b::2003	2001:218:1030:6052::2002	TLS 1294	Application Data
222 2021-01-28 15:37:39.017 24	04:6800:400a:800::2003	2001:218:1030:6052::2002	TLS 1294	4 Application Data
<	47 · 6 204 · 7.045 · 205 · · 7.043	- JAG1 + JTS + 14 37 + 646 J + + JAG7	110 130	Application Data
 Frame 200: 94 bytes on wire (752 l Ethernet II, Src: IntelCor_98:05:: Internet Protocol Version 6, Src: 	<pre>bits), 94 bytes captured (752 bits) 3a (90:78:41:98:05:3a), Dst: Fujitsu_5d:aa:a0 2001:2f8:103c:6052::2002, Dst: 2001:4860:4860</pre>	(a8:b2:da:5d:aa:a0) ::8888		
0000 a8 b2 da 5d aa a0 90 78 41 98	05 3a 86 dd 60 00 ····]···x A··:··`·			
0010 00 00 00 28 11 80 20 01 02 f8	10 3c 60 52 00 00 ···(····························			
0028 00 00 00 00 20 02 20 01 48 60	48 60 00 00 00 00 ···· · H`H`····			
0030 00 00 00 00 88 88 f6 fe 00 35	00 28 ed 0c f6 ee			
0040 01 00 00 01 00 00 00 00 00 00 00	03 77 77 77 06 67			
	NA RI RA RI CORLECC M			
😑 🍸 Domain Name System: Protoco	1		<i>1</i> '	ひット教: 2386・表示: 2128 (89.2%)

図 6.1.6-7 IPv6 優先接続端末で WEB アクセス時のネットワークキャプチャ結果

図 6.1.6-7 に記載の通り、パブリック DNS に対して IPv6 アドレスでクエリの問い合わせを行い、返却され たクエリの応答結果に基づき、IPv6 アドレスで google のサイトに対する TLS 接続を行っていることを確認し た。

【#2の補足】

IPv6 優先接続設定を行った実証用PCを使用して IPv6 未対応サイトの WEB ブラウズを実行した場合、通信フォ ールバックによる IPv4 アドレスを使用した WEB ブラウズが行えることを確認した。

「netstat -an」コマンドを実行し、WEB ブラウザが IPv4 アドレス同士でセッションを確立しているかを確認した。

C:¥Users¥user>netstat -an

アクティブな 接続





検証用PCで接続確認を行った際の nslookup の結果および、ネットワークキャプチャ結果についても併せて記載する。



図 6.1.6-9 IPv6 未対応サイトの nslookup コマンド実行結果

nslookupを実行した所、WEBサイトのドメインは IPv4 アドレス(A レコード)のみ通知された。

ネットワークトレース結果より、1257 フレームおよび 1258 フレームでパブリック DNS に対して IPv4 アドレス(A レコード)および IPv6 アドレス(AAAA レコード)でクエリの問い合わせを行い、DNS クエリのレスポンスとして IPv4 アドレス(A レコード)が通知されていた。

🚄 web-ipv4fallback.pcapng				- 🗆 🗙	(
ファイル(E) 編集(E) 表示(Y) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(y)	無線(W) ツール(I) ヘルプ(H)				
▲ ■ 2 0 Ⅰ □ 🗙 ८ ९ ↔ 🛎 🖡 🖢 📃 🔍 ९ ९	Π				
【■表示フィルタ … 〈Ctrl-/〉を適用					+
No. Time Source	Destination	Protocol	Length Info		^
→ 1257 19.547470 2001:2†8:103c:6051::101	2001:4860:4860::8888	DNS	95 Standard query Øxab5	1 A www.yahoo.co.	
1258 19.547684 2001:2f8:103c:6051::101	2001:4860:4860::8888	DNS	95 Standard query 0x0cb	🤉 AAAA www.yahoo	1
1259 19.558023 172.16.51.1	172.16.1.31	UDP	1143 3389 → 50115 Len=110	L	
1260 19.559186 172.16.1.31	172.16.51.1	UDP	60 50115 → 3389 Len=12		
4- 1261 19,560778 2001:4860:4860::8888	2001:278:1030:6051::101	DNS	139 Standard query respo	nse Øxab54 A www <mark>.</mark>	
1262 19.561663 2001:4860:4860::8888	2001:2f8:103c:6051::101	DNS	123 Standard query respo	nse 0x0cb9 AAAA w	
1263 19.562278 172.16.51.1	182.22.16.251) [SYN, ECN	, CWR] Seq=0 Win=	
1264 19.562454 172.16.51.1	182.22.16.251 1257	フレーム目で発	行された 🦻 [SYN, ECN	, CWR] Seq=0 Win=	
1265 19.571278 182.22.16.251	172.16.51.1		B [SYN, ACK] Seq=0 Ack=1 Win	
1266 19.571356 172.16.51.1	182.22.16.251 DIN S	ックエリに刈りるい	ノ人爪ン人	=1 Ack=1 Win=2621	
1267 19.571495 182.22.16.251	172.16.51.1		t [SYN, ACK] Seq=0 Ack=1 Win	
1268 19.571525 172.16.51.1	182.22.16.251	TCP	54 50384 → 80 [ACK] Seq	=1 Ack=1 Win=2621	
1269 19.571938 172.16.51.1	182.22.16.251	HTTP	1251 GET / HTTP/1.1		~
<				>	
> Internet Protocol Version 6, Src: 2001:4860:4860::8	388, Dst: 2001:2f8:103c:6051::1	01			^
> User Datagram Protocol, Src Port: 53, Dst Port: 630	98				
✓ Domain Name System (response)					
Transaction ID: 0xab54					
> Flags: 0x8180 Standard query response, No error					
Questions: 1					
Answer RRs: 2		してを取得してい	13		
Authority RRs: 0			10		
Additional RRs: 0					
> Queries					
✓ Answers					
> www.yahoo.co.jp: type CNAME, class IN, cname e	ge12.g.yimg.jp				
> edge12.g.yimg.jp: type A, class IN, addr 182.2	2.16.251				
[Request In: 1257]					
[11me: 0.013308000 seconds]					~
• Web-ipv4fallback.pcapng			パケット数: 7965・表示: 7965 (100.0%)	プロファイル: Default	

図 6.1.6-10 IPv6 未対応サイトのネットワークトレース結果(1)

また、1258 フレーム目で発行した DNS クエリ(AAAA レコード)については、以下のように 1261 行目で得ら れた A レコードの別名(CNAME)で通知されている。



図 6.1.6-11 IPv6 未対応サイトのネットワークトレース結果(2)

以降の WEB ブラウザの通信はパブリック DNS サーバより得られた IPv4 アドレスによりで行われているこ とより、IPv6 から IPv4 への通信フォールバックが発生していないと推測できる。WEB ブラウザを利用してい る際のレスポンスは IPv4 サイトを利用していた場合と大差はなかった。仮に、IPv6 非対応サイトのコンテンツ 管理者が DNS に不用意に AAAA レコードを登録するようなことがない限り、IPv6 から IPv4 への通信フォー ルバックが発生しない可能性が高い。

【#3の補足】

IPv4 優先接続設定を行った実証用PCを使用して WEB ブラウズを実行した場合、IPv4 アドレスを使用した WEB ブラウズが行えることをネットワークキャプチャ結果より確認した。



図 6.1.6-12 IPv4 優先端末で WEB アクセス時のネットワークキャプチャ実行結果(1)

具体的には、71,72 フレーム目で IPv6 アドレスを使用してパブリック DNS に対して「urs.microsoft.com」の 名前解決クエリを発行し、81 フレーム目で名前解決した結果として A レコードを受け取っていることが判断 できる。また、82 フレーム目では AAAA レコードのレスポンスを受け取っているが、CNAME レコードで 81 フレーム目の A レコードの別名が通知され、以降 IPv4 アドレスで通信が行われていることを確認した。



図 6.1.6-13 IPv4 優先端末で WEB アクセス時のネットワークキャプチャ実行結果(2)

通常業務を想定した学内ネットワーク機器(複合機・既設プリンタ)の試験を示す。IPv4/IPv6 デュアルスタック環 境での実証試験に加えて、複合機の IPv6 シングルスタックでの動作について実施した。

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
1	ノート	無線	IPv6	プリンタ	IPv4	印刷ジョブを送信する	印刷が実行される	ок
	PC		優先					*
2	ノート	無線	IPv6	複合機	IPv6	印刷ジョブを送信する	印刷が実行される	ОК
	PC		優先	<mark>(テ^{゛゛}ュアル</mark>				
				<mark>スタック)</mark>				
3	ノート	無線	IPv6	複合機	IPv4	複合機からスキャンを行い、	スキャンデータが指定された	ок
	PC		優先	<mark>(テ^{゙゙}ュアル</mark>		スキャンデータを複合機から	メールアドレス宛に実行され	
				<mark>スタック)</mark>		メール送信する	3	
4	ノート	無線	IPv6	複合機	IPv4	印刷ジョブを送信する	印刷が実行される	ок
	PC		優先	<mark>(テ^{・・・}ュアル</mark>				
				<mark>スタック)</mark>				
5	ノート	無線	IPv6	複合機	IPv6	印刷ジョブを送信する	印刷が実行される	ок
	PC		優先	(IPv6				
				シングル				
				スタック)				
6	ノート	無線	IPv6	複合機	IPv4	印刷ジョブを送信する	指定した宛先が見つからな	ок
	PC		優先	(IPv6			いため、印刷が実行されな	
				シングル			い	
				スタック)				
7	ノートP	無線	IPv6	複合機	IPv6	複合機からスキャンを行い、	スキャンデータが指定された	ОК
	С		優先	(IPv6		スキャンデータを複合機から	メールアドレス宛に実行され	
				シングル		メール送信する	ない	
				スタック)				

③通常業務を想定した学内ネットワーク機器の利用

【#1の補足】※に関して

実証端末から IPv4 アドレスで既存ネットワーク配下のプリンタに印刷した際、帳票出力されない現象が発生した。実証端末からファイルサーバの共有フォルダアクセス時と同様に実証用 FW 装置のセッションログを確認した所、実証環境ネットワーク側のファイアウォールポリシーにより、学内既存ネットワーク上に設置されているプリンタからの状態確認を行う為のパケット(SNMP, ENPC(3289/udp), LPD(515/tcp))が drop されていることが判明した。対応策として、既存ネットワーク(IPv4)上にあるプリンタから、実証用ネットワーク(IPv4)上にあるプリンタへの通信許可をファイアウォールに設定した。

【#2、#5の補足】

複合機のデバイス登録を IPv6 で行おうとした場合、ベンダ提供のプリンタドライバインストーラからグロー バルユニキャストアドレス(GUA)で IPv6 アドレスを設定した複合機をネットワーク探索することができなかった。

🏠 ドライバーインストールツール - プリンター・複合機の選択									
プリンター・複合機の選択 セットアップしたいプリンター・複合機をリストから選択してください。 リストにない場合は[ヘルプ]を参照してください。									
	検索されたプリンター・複合機(<u>D</u>) ▼ ポート名に必ずIPアドレスを使): 5用する(<u>P</u>)							
	名前	アドレス	機種						
	▲前川 アドレス (被)(注) ✓ DocuCentre-V C5575 T2 fe80::a00:37ff:fed7:3675%9 DocuCentre-V C557								
and the second se	<		>						
			再検索(<u>R</u>)						
	< 戻る(<u>B</u>)	次へ(<u>N</u>) > キャンセル	ヘルプ						

図 6.1.6-14 プリンタドライバインストール時にプリンタを自動検出した際の動作

カスタムセットアップで標準 TCP/IP ポートを手動で作成し、IPv6 アドレスを追加することで IPv6 による印 刷を行えるようになったが、プリンタの状態取得を行うことができなかった。実証試験ではベンダ提供のプリ ンタドライバインストーラのネットワーク探索で得られたリンクローカルアドレスを使用してIPv6 印刷を行った。 プリンタデバイス登録時(IPv6 シングルスタック)のネットワークトレース結果を以下に記載する。

4 20	210222-複合機ipv6シン	/グル-デ/	「イス登録.pcapng			_ D X
ファイル(E) 編集(E) 表示(⊻) 移動(G) キャプチャ(C) 分)析(A) 統計(S) 電話(Y) 無	無線(⊻)	ツール(工) ヘルプ(日)			
🔬 🔳 🖉 😕 👗 🖺 🕱 🙆 🔍 👄 🛸 🖀 💆 💆	<u>.</u>					
【■ 表示フィルタ … 〈Ctrl-/〉を適用						
Time Source	Destination	Protoco	Length Info	- I . I		
2021-02-22 14:08:16.323 172.16.52.2	255.255.255.255	SNMP	102 get-request	A		
2021-02-22 14:08:16.323… fe80::b805:9fa7:7c:f825	ff02::1	SNMP	122 get-request			
2021-02-22 14:08:16.323 172.16.52.2	255.255.255.255 ff021	SNMP	102 get-request			
2021-02-22 14:08:18.053… Buffalo 30:fa:6e	Broadcast	0×8899	60 Realtek Layer 2	Protocols		
2021-02-22 14:08:18.346 te80::b805:9ta/:/c:t825	te80::a00:37tt:ted7:3675	SNMP	112 get-request 1.3	.6.1.4.1.253	.8.64.4.2.1.5.10.1415030	
2021-02-22 14:08:18.346 fe80::b805:9fa7:7c:f825	fe80::a00:37ff:fed7:3675	SNMP	112 get-request 1.3	.6.1.4.1.253	.8.64.4.2.1.5.10.1415030	0
2021-02-22 14:08:18:351 te80::a00:37tt:ted7:3675	te80::b805:9ta7:7c:t825	SNMP	113 get-response 1.	3.6.1.4.1.25	3.8.64.4.2.1.5.10.141503	00
2021-02-22 14:08:18:352 fe80::b805:9fa7:7c:f825	fe80::a00:37ff:fed7:3675	SNMP	116 get-request 1.3	.6.1.2.1.1.5	.0 1.3.6.1.2.1.1.6.0	
2021-02-22 14:08:18.354 fe80::a00:37ff:fed7:3675	fe80::b805:9fa7:7c:f825	SNMP	137 get-response 1.	3.6.1.2.1.1.	5.0 1.3.6.1.2.1.1.6.0	B
2021-02-22 14:08:18.359 172.16.52.2	172.16.52.255	NBNS	92 Name query NB S	HRFAX<00>		D
2021-02-22 14:08:18:359 172.16.52.2	172.16.52.255	NBNS	92 Name query NB Si	HRFAX<00>	CAN least "ON" success	
2021-02-22 14:00:10:359 172:10:32:2 2021-02-22 14:08:18:359 172:16:52:2	224.0.0.251	MDNS	72 Standard query 1	0x0000 A SHR	FAX.local, "OM" question	
2021-02-22 14:08:18.359 fe80::b805:9fa7:7c:f825	ff02::fb	MDNS	92 Standard query	0x0000 A SHR	FAX.local, "QM" question	
2021-02-22 14:08:18.359 fe80::b805:9fa7:7c:f825	ff02::fb	MDNS	92 Standard query	0x0000 A SHR	RFAX.local, "QM" question	
2021-02-22 14:08:18.359 172.16.52.2	224.0.0.251	MDNS	72 Standard query	0x0000 AAAA	SHRFAX.local, "QM" quest	ion
2021-02-22 14:08:18.359 172.16.52.2	224.0.0.251	MDNS	72 Standard query	0x0000 AAAA	SHRFAX.local, "QM" quest	ion
2021-02-22 14:00:10:359 1200:1005:9107:70:1025 2021-02-22 14:08:18:359 fe80::b805:9fa7:70:f825	ff02::fb	MDNS	92 Standard query 1	0x0000 AAAA	SHRFAX.local, "OM" quest	ion
2021-02-22 11.08.18 360 faso	ffa21.3	L.I. MNID	86 Standard query	AVINES A SHD	PEAX	×
5						2
msgPrivacyParameters: <missing></missing>						^
4 msgData: plaintext (0)						
contextEngineID: <missing></missing>						
contextName:						
▲ data: get-request (0)						
⊿ get-request						
error-status: noError (0)						
error-index: 0						
variable-bindings: 0 items						\sim
0000 ff ff ff ff ff ff 90 78 41 98 05 3a 08 00 45 00	······					
0010 00 58 b7 e4 00 00 80 11 00 00 ac 10 34 02 ff ff	·X·····4···			14/1	down m= /tax -	7 三天7 三丁
○ 20210222-複合様inv6シングルーデバイス 登録 ncanng			パケット表	yv100	T 2862 (100 0%)	7.1.1/2 Default
C KE Mapoo > > > > > > A Estimate			11 × 15 × 1 8			1 States and

図 6.1.6-15 プリンタドライバインストール時のネットワークトレース結果

上図のネットワークトレース結果より、SNMP プロトコルでマルチキャストアドレスやリンクローカルアドレス を使用してプリンタのネットワーク探索を行っていることが伺える。「A」で IPv4 および IPv6 のマルチキャスト アドレスに対して SNMP(GET-Request)を発行し、「B」で応答があったプリンタ(プリンタ製造元の MIB 情報を 持つ)のリンクローカルアドレスに対して「Get-request/Get-Response」でのやりとりが記録されている。

【#3の補足】

複合機でのスキャンデータの取り込みは実証用 PC 主導で行うのではなく、複合機の操作パネルよりスキャンデータを送信したい宛先を指定して実現する。複合機を IPv4/IPv6 デュアルスタック環境で動作させた 状態ではスキャンデータは IPv4 アドレスを使用して学内 SMTP サーバ経由でしてした宛先に送信されること を確認した。

_ 0 100 3 スキャンデータからのメール(参照)_20210303155754.bt・メモモ 2546(6) 編集(6) 業式(8) 業長(8) 小み7(6) From: DocuCentre-V CS575 12 <feet-infoffmalueThurs.ac.jp> Dute: 2021年2月16日(火) 16:12 Subject: Scan Data from FX-D73675 To: 《 新聞論書: May-a ac.jp> Number of Images: 1 Attachment File Type: PDF Device Name: DocuCentre-V 65575 12 Device Location: 15 11.1 11

図 6.1.6-16 複合機からのスキャンデータ受信メール

【#7 の補足】

複合機をIPv6シングルスタックモードで動作させた状態でスキャンデータのメール送信の実証 を行った所、未送信レポートが出力され、スキャンデータのメール送信を行うことはできなかった。 学内SMTPサーバはIPv4シングルスタックモードで稼働しており、複合機がIPv6シングルスタ ックモードで動作している場合、SMTPサーバとの間でIPv6通信を行うことができなかった。 2. LAN 内アプリケーションレベルの検証

6.1.5 にしたがって構築した実証環境において、業務アプリケーションに相当するシステムとして、実証用 学内 WEB サーバの WEB コンテンツ提供とファイルサーバによるユーザ認証とファイル共有を検証対象とした。

実証用学内WEBサーバにおける検証では、IPv4/IPv6デュアルスタックの実証用学内WEBサーバにてWEBサーバソフトウェアが正常に起動していることを確認した。次に、実証用学内WEBサーバに配置したWEBコンテンツをブラウザ経由で閲覧できるか確認した。また、WEBサーバの運用を想定し、WEBコンテンツの更新等の管理業務に影響がないか確認した。

ファイルサーバにおける検証では IPv4/IPv6 デュアルスタックのファイルサーバに対して、学内の Active Directory サーバによるユーザ認証を行うことで共有フォルダへ接続できるか確認した。

これらの確認をもとに IPv6 通信で業務アプリケーションに相当するシステムの利用が可能か検証した。また、デュアルスタック環境内で IPv4 通信でも同様のことが可能か検証した。

結果として、IPv6の規格に起因した課題は発生しなかったが、IPv6対応における留意事項が3件発生した。

IPv4 優先接続端末で実証用学内 WEB サーバの WEB コンテンツを開き、コンテンツ内のハイパーリンク をクリックした場合、TCP/IPv6 側の DNS 設定が行われていると、学内サーバの名前解決を行うことができず、 ページを表示することができなかった。その後、マイクロソフト社に問い合わせを行い、IPv6 の DNS サー バと IPv4 の DNS サーバにおいて、IPv6 の DNS サーバでレコードが存在しないことは Windows OS の 設計上想定された設定ではないと回答を頂いた。そして TCP/IPv6 側の DNS 設定を未設定状態にすること で回避した。

(3) 業務アプリケーションにおける検証について

6.1.4(7)の通り、実証試験用に新規構築した学内 WEB サーバ上で、WEB アプリケーションの IPv6 対応を行った。ここでは、①~③のシナリオを IPv6 通信で検証した。検証範囲を図 6.1.6-17 に示す。



図 6.1.6-17 業務アプリケーションにおける検証範囲

- ① WEB サーバソフトウェアの動作検証
- ②一般利用者向けの検証項目として IPv6 デュアルの実証用学内 WEB サーバに配置した WEB コンテンツが実証用 PC のブラウザ経由で閲覧できることを検証する。また WEB サーバの管理者 向けの検証項目として、実証用学内 WEB サーバにて WEB ページやコンテンツの変更が IPv4/IPv6 デ ュアルスタック環境下で利用できるか検証する。
- ファイルサーバの動作検証(ユーザ認証、ファイル共有) ファイルサーバのユーザ認証とファイル共有ができるか検証する。また、ユーザ認証が学内の Active Directory サーバとの間で IPv4 を使用して認証が行えることを検証する。

①WEBサーバソフトウェアの動作検証

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
1	ノート	無線	IPv6	実証用学	IPv6	【一般利用者向け確認】	学内 WEB コンテンツが正しく	ОК
	PC		優先	内 WEB サ		WEB ブラウザより学内 WEB	表示されること	
				— <i>/</i> ĭ		サービス(IPv6 アドレス)の WEB		
						表示を行う	IPv6 アドレスで http セッショ	
							ンが確立されていること	
2	ノート	無線	IPv6	実証用学	IPv4	【一般利用者向け確認】	学内 WEB コンテンツが正しく	ок
	PC		優先	内 WEB サ		WEB ブラウザより学内 WEB	表示されること	
				— <i>i</i> ĭ		サービス(IPv4 アドレス)の WEB		
						表示を行う	IPv4 アドレスで http セッショ	
							ンが確立されていること	
3	ノート	無線	IPv4	実証用学	IPv6	【一般利用者向け確認】	学内 WEB コンテンツが正しく	ок
	PC		優先	内 WEB サ		WEB ブラウザより学内 WEB	表示されること	
				— <i>.</i> , í		サービス(IPv6 アドレス)の WEB		
						表示を行う	IPv6 アドレスで http セッショ	
							ンが確立されていること	
4	ノート	無線	IPv4	実証用学	IPv4	【一般利用者向け確認】	学内 WEB コンテンツが正しく	NG
	PC		優先	内 WEB サ		WEB ブラウザより学内 WEB	表示されること	※ 1
				- <i>i</i> i		サービス(IPv4 アドレス)の WEB		
						表示を行う	IPv4 アドレスで http セッショ	
							ンが確立されていること	
5	ノート	無線	IPv6	実証用学	IPv6	【管理者向け確認】	CLBOXより教職員用フォル	NG
	PC		優先	内 WEB サ		①学内 WEB サービスのハイ	ダの作業用フォルダにコンテ	₩2
				—/Ň		パーリンク(CLBOX)をクリッ	ンツをアップロードできること	
						クする		
						②CLBOX より教職員用フォ		
						ルダの作業用フォルダにコ		
						ンテンツをアップロードする		

【#1、#2の補足】

実証用 PC から実証用学内 WEB サーバに IPv6 アドレスで WEB 表示した際のネットワークトレース結果 を以下に記載する。実証にあたり、実証用PCの hosts ファイルに実証用学内 WEB サーバのホスト名と IPv6 アドレスのペアを追記した状態で実施した。下図のネットワークトレース結果をhttpプロトコルに絞って表示 しているが、実証用 PC 実証用学内 WEB サーバとの WEB 表示が IPv6 アドレスで実施されていることが確 認した。レスポンスに関してもページの表示が約 0.2 秒で完了していることが下図のネットワークトレースより 確認した。

· 動作確認導	回(和用者向计输船)(2	JIPv64	EE-1.pcap		- 🗆 X
27/64(E) 編集(E) 表示(A) 時間(G) キャプチャ(G) 分析(A) 4	ଶ୍ୟାର୍ଯ୍ଯାର(x) ଅବସେ(x) ସ୍ସ୍ୟ୍ୟ	7-5(I) A\$7(H)		
Into	Contraction of the second s				4 · · ·
No. True Source 10 Juli - 42, Jii Li - 10, Mar. Ann. Jii Juli - 242, Jii - 10, Mar. Ann. Jii 14 Juli - 42, Jii Li - 10, Mar. Ann. Jii Juli - 242, Jii - 10, Mar. Ann. Jii 14 Juli - 42, Jii Li - 10, Mar. Ann. Jii Juli - 242, Jii - 10, Mar. Ann. Jii 16 Juli - 42, Jii Li - 10, Mar. Ann. Jii Juli - 242, Juli - 10, Mar. Ann. Jii 16 Juli - 42, Jii Li - 10, Mar. Ann. Jii Juli - 242, Juli - 243, Juli - 243, Juli - 244,	Construction 1	Provide color errors erors erors erors erorors erors erorors erors erorors e	Langth 340 443 867 / 8778/2.1 714 8779/3.1 349 06 445 877 / (14) 088708 446 877 / (14) 088708 448 877 / (14) 088708 448 877 / (14) 088708 448 877 / (14) 088708 448 877 / (14) 080 06 449 8779/1.1 348 08 449 8779/1.1 484 080 449 8779/1.1 484 080 449 8779/1.3 484 080 449 8779/1.3 348 08 479 877 / (14) 089 08 479 877 / (14) 089 08 479 877 / (14) 089 08 479 8779/1.3 348 08	11est/9661) Lleast_js_WTM72.3 wTM72.3 wTM72.3 wTM72.3 (Inst/cas) (set7/c	49
		THUE .		Contraction of the second s	i ki
<pre>Accept: test/med, splication/wendless1, f/"iris Accept: test/med, splication/wendless1, f/"iris Deer-Agent: multic/s.d (Mindex AT 0.5; Mindex Trideet/T.d) Accept-Decoding gifs, deflets/via must. Namet ipvi.Noberiarus.er.g/via growthread in the Acception of the Acception for the Accept Decoding acception for the Acception of the Acception for the Acception of Acception of the Acception for the Acception of Acception for the Acception of Acception of the Acception of the Decoder of Acception of Acception of the Decoder of Acception of Acception of the Acception of Acception for the Acception of Acception of Acception of Acception for the Acception of Acception of Acception of Acception Decoder of Acception of Acception of Acception of Acception for the Acception of Acception of Acception of Acception of Acception for the Acception of Acception of Acception of Acception of Acception of Acception for Acception of Acc</pre>	(h;qe0,4,c0-Han;qe0,2)/ris reill.0) like Beckelria				
all 52 da 52 da 40 00 30 da do 10 30 da 20 da 20 da 30 00					4
🗧 🗶 Hypertext Transfer Pirteast Poteast			パケット 数 200・数	E 22 (11 ON) 3	UTri & Default

図 6.1.6-18 実証用学内 WEB サーバを WEB 表示した際のネットワークトレース結果(1)

次に実証用 PC から実証用学内 WEB サーバに IPv4 アドレスで WEB 表示した際のネットワークトレース 結果を以下に記載する。実証にあたり、実証用 PC の hosts ファイルに実証用学内 WEB サーバのホスト名と IPv4 アドレスのペアを追記した状態で実施した。

6	動作確認項目(利用者向は機能)	(2)IPv640	先-3.pcap		- 0 X
ヤイル(E) 編集(E) 表示(V) 年齢(G) キャプチャ(C) (単 二 単 二 又 乙 Q ★ ★ 雪 丁)	916(A) HE1(S) RA(y) MR()	W) 7-5(I)	~#JH)		
heta					01.2
a Time Source	Destination .	Protocol	Length 3-th		
M 2421-41.38 11-80-53.728. 172 187.13 42 2021-41.28 12/80-53.728. 172.15.51.1 43 2021-41.38 12/80-53.728. 172.15.51.1 44 2021-41.38 12/80-53.727. 172.15.51.1 45 2021-41.38 12/80-53.727. 172.15.51.1 46 2021-41.38 12/80-53.727. 172.15.51.1 47 2021-41.38 12/80-53.727. 172.15.51.1 47 2021-41.38 12/80-53.732. 172.15.51.1 47 2021-41.38 12/80-53.732. 172.15.51.1 47 2021-41.38 12/80-53.732. 172.15.51.1 48 2021-41.38 12/80-53.737. 172.15.51.1 49 2021-41.38 12/80-53.737. 172.15.51.1 49 212-41.28 12/80-53.747. 172.15.51.1 49 212-41.38 12/80-53.747. 172.15.51.1 49 12/80-53.718.51.8 172.15.51.21 172.15.51.21 49 12/80-53.728.11.9 12/80-53.74.1 172.15.51.1<	179, 56, 59, 5 179, 56, 59, 5 179, 56, 59, 5 179, 56, 51, 7 179, 56, 51, 7 179, 56, 51, 7 179, 56, 52, 7 179, 56, 52, 7 179, 56, 52, 7 179, 56, 52, 7 179, 56, 51, 7 179, 56, 50, 7	8775 8775 8775 8775 8775 8775 8775 8775	343-647 / 0017/1.3 200 00 445-617 /100/1000700 446-617 /100/1000700 446-617 /100/1000700 446-617 /100/100070 446-617 /100/100070 446-617 /100/100070 446-6170/1.3 200 00 346-6170/1.3 200 00 346-6170/1.3 200 00 346-6170/1.3 200 00 346-6170/1.3 200 00 347-6170/1.3 200 00	(1001/998)) Lines-(30.0719/3.1. 9739/3.4. 9739/3.4. 9739/3.4. (1001/998) (1001/998) (1001/998) 9739/3.1. food (1001/968)) fr.9739/3.1. 9739/3.1	6 3)
The sector of sector sector bits and	9(4)-99-96(-9		the second second	(An-mak)	14
Hyperinest Trensfer Protocol b Batt A stiff(1)/oran Accept test/from (.splication/arcsised, ''''' Accept testoneling (.splication/arcsised, '''''' test-Agent Periller's (.viotes for the stiff Accept testoneling (.splication or .gl/ste Most testo testo (.gl/steries) Most testo (.gl/steries) Most testo (.gl/steries) Most testo (.gl/steries) Most testo (.gl/steries) Most testo (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/steries) (.gl/sterie	rue de Suph-Hens-Oligiet (4,3%-Hensiget, 2)/// p Trident/7.ds ruch).(8) Like Secks/urin	12			
all bit de Sur an eff 50 10 50 50 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 50 51 50 50 50 50 50 50 50 50 50 50 50 50 50	1 .4				
2 Huterland Transfer Pestousi Protocol			/切片数 130-数	8 20-015-463 26	1774 (j): Default

図 6.1.6-19 実証用学内 WEB サーバを WEB 表示した際のネットワークトレース結果(2)

【#4の補足】 ※1に関して

実証用 PC (IPv4 優先端末)から実証用学内 WEB サーバに IPv4 アドレスで WEB 表示した際、コンテンツ 内のハイパーリンクをクリックした際に「ページが見つかりません」エラーになることが実証の過程で判明した。

トラブルシューティングを行った所、Windows 側で IPv4 優先を行う設定を行っても、TCP/IPv6 側で設定し たパブリック DNS に対して名前解決を行っていることをネットワークトレースで確認した。なお、URL に実証 用学内 WEB サーバの URL を直接入力した場合、学内 WEB ページが正しく表示された。

ファイル(E) 編集(E) 表示(⊻) 移動(⊆) キャブチャ(⊆) 分析(A	 約計(S) 電話(y) 無線(W) ● ● ● ● ● ● 	l) ツール(工) ヘルプ(H)	
■ 表示フィルタ … <ctrl-></ctrl-> を適用			
No. Time Source	Destination	Protoco Length Info	7
No. Time Source 1 165 2021-93-01 14:40:18.846. 2001:1450:1456:1603:16051:101 1 166 2021-93-01 14:40:18.846. 2001:1450:1460:18088 167 2021-93-01 14:40:18.846. 172.16.51.1 1 1 166 2021-93-01 14:40:18.846. 172.16.51.1 1 1 172 2021-93-01 14:40:18.891. 172.16.51.1 1 1 172 2021-93-01 14:40:18.891. 172.16.51.1 1 1 172 2021-93-01 14:40:18.891. 172.16.51.1 1 1 172 2021-93-01 14:40:18.891. 172.16.51.1 1 1 172 2021-93-01 14:40:18.891. 172.16.51.1 1 1 172 2021-93-01 14:40:18.891. 172.16.51.1 1 1 172 2021-93-01 14:40:18.892. 172.16.51.1 1 177 2021-93-01 14:40:18.892. 172.16.51.1 1 1 180 2021-93-01 14:40:18.892. 172.16.51.1 1 1 182 2021-93-01 14:40:18.892. 172.16.51.1 1 1 182 2021-93-01 14:40:18.892. 172.16.51.1 1 1 <t< td=""><td>Destination 2001:4660:4850::8888 2001:4600:4850::8888 172:16:1.151 172:16:1.151 172:16:1.1 172:16:3.1</td><td>Protoco Length Info DNS 104 Standard query 0x978e AAA inetsvr. ac.ji 11 DNS 152 Standard query response 0x f8e NAAA inetsvr. ac.ji DNS 132 Standard query 0x978e AAA inetsvr. ac.ji DNS 132 Standard query 0x978e AAAA inetsvr. ac.ji DNS 142 Standard query 0x9789 AAAA inetsvr. ac.ji TCP 66 52551 StW, 0KI, CKR, Seque AAckel Mine6230 Lene0 M TCP 66 30e + 52551 (StW, ACK) Seque Ackel Mine6244 Lene0 TCP</td><td></td></t<>	Destination 2001:4660:4850::8888 2001:4600:4850::8888 172:16:1.151 172:16:1.151 172:16:1.1 172:16:3.1	Protoco Length Info DNS 104 Standard query 0x978e AAA inetsvr. ac.ji 11 DNS 152 Standard query response 0x f8e NAAA inetsvr. ac.ji DNS 132 Standard query 0x978e AAA inetsvr. ac.ji DNS 132 Standard query 0x978e AAAA inetsvr. ac.ji DNS 142 Standard query 0x9789 AAAA inetsvr. ac.ji TCP 66 52551 StW, 0KI, CKR, Seque AAckel Mine6230 Lene0 M TCP 66 30e + 52551 (StW, ACK) Seque Ackel Mine6244 Lene0 TCP	
B:実証端未と実証月	月 Web サ−バ間は IPv	∨4 アドレスでセッションが確立されている	~
0010 00 00 00 32 11 80 20 01 02 f8 10 3c 60 51 00 00 ···2·	·····<`Q··	× * * * * * * * * * * * * * * * * * * *	7
◎ Z hunet-ok.pcapng		パケット数: 508/1表示: 508 (1.00.0%) / プロファイル Default	đ

図 6.1.6-20 IPv4 優先端末から WEB 表示した際のネットワークトレース結果(1)

ハイパーリンクをクリックした場合、図 6.1.6-20 の DNS 名前解決との挙動が異なり、IPv6 アドレスでの DNS での名前解決に失敗した後、IPv4 アドレスでの名前解決が行われていないが、ブラウザのセッションが IPv4 で行われていることをトレース結果より確認した。

ファイル(E) 編集(E) 表示(Y) 移動(G) キャプチャ(C) 分析(A) 統 ▲ ■ ② ③ ↓ ○ X ② ♀ ◆ ◆ 警 ▼ ↓ ↓ ● ④	(計(<u>S</u>)電話(¥)無線(₩) 、	ツール(工) ヘルプ(且)	
表示フィルタ … 〈Ctrl-/〉を適用			
No. Time Source	Destination	Protoco Length Info	~
<pre>19 2021-03-01 14:41:47.823. 172.16.51.1 142 2021-03-01 14:41:47.823. 172.16.1.31 141 2021-03-01 14:41:47.826. 172.16.1.31 142 2021-03-01 14:41:47.929. 172.16.1.31 143 2021-03-01 14:41:47.929. 172.16.51.1 144 2021-03-01 14:41:47.929. 172.16.51.1 145 2021-03-01 14:41:48.016. 172.16.51.1 146 2021-03-01 14:41:48.016. 172.16.51.1 147 2021-03-01 14:41:48.015. 172.16.51.1 148 2021-03-01 14:41:48.015. 172.16.51.1 149 2021-03-01 14:41:48.015. 172.16.51.1 149 2021-03-01 14:41:48.015. 172.16.51.1 150 2021-03-01 14:41:48.015. 172.16.51.1 151 2021-03-01 14:41:48.052. 2001:276:103:10551:1101 152 2021-03-01 14:41:48.052. 2001:276:103:10551:1101 152 2021-03-01 14:41:48.059. 172.16.51.1 153 2021-03-01 14:41:48.059. 172.16.51.1 154 2021-03-01 14:41:48.059. 172.16.51.1 155 2021-03-01 14:41:48.059. 172.16.51.1 154 2021-03-01 14:41:48.059. 172.16.51.1 155 2021-03-01 14:41:48.059. 172.16.51.1 154 2021-03-01 14:41:48.059. 172.16.51.1 155 2021-03-01 14:41:48.059. 172.16.51.1 154 2021-03-01 14:41:48.059. 172.16.51.1 155 2021-03-01 14:41:48.059. 172.16.51.1 154 2021-03-01 14:41:48.059. 172.16.51.1 155 2021-03-01 14:41:48.059. 172.16.51.1 155 2021-03-01 14:41:48.059. 172.16.51.1 154 2021-03-01 14:41:48.059. 172.16.51.1 154 2021-03-01 14:41:48.059. 172.16.51.1 155 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 157 2021-03-01 14:41:48.059. 172.16.51.1 159 2021-03-01 14:41:48.059. 172.16.51.1 159 2021-03-01 14:41:48.059. 172.16.51.1 159 2021-03-01 14:41:48.059. 172.16.51.1 159 2021-03-01 14:41:48.059. 172.16.51.1 159 2021-03-01 14:41:48.059. 172.16.51.1 159 2021-03-01 14:41:48.059. 172.16.51.1 159 2021-</pre>	172.16.1.31 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.1.31 172.16.1.31 172.16.5.1.1 172.16.1.31 172.16.1.31 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.1 172.16.5.1.31 172.16.1.31 17	TLSV1.2 105 Application Data TCP 60 52515 + 3389 [ACK] Seq=1763 UDP 60 53636 + 3389 Lon=12 TLSV1.2 92 Application Data UDP 222 3389 + 53630 Lon=12 TLSV1.2 92 Application Data UDP 222 3389 + 53630 Lon=120 TCP 54 3389 + 52515 [ACK] Seq=279 Å TLSV1.2 92 Application Data UDP 60 53630 + 3389 Lon=12 TLSV1.2 91 Application Data TCP 66 32551 + 3389 [ACK] Seq=1839 UDP 876 3389 + 59530 Lon=34 DNS 104 [Standard query 0xb108 AAAA 1 TLSV1.2 92 Application Data DNS 104 [Standard query response 0xb1 DNS 152 Standard query response 0xb1 UDP 349 3389 + 53538 Lon=327 UDP 349 3369 + 53538 Lon=327 UDP 69 53630 + 3389 Lon=12 TCF 54 3389 + 53538 Lon=327 UDP 349 3369 + 53538 Lon=327 UDP 69 53630 + 3389 Lon=12 TCF 54 3389 + 55515 [ACK] Seq=553 A UDP <t< td=""><td>Ack=279 Win=256 Len=0 ck=1801 Win=63043 Len= Ack=353 Win=256 Len= svr. the lineac. j instsvr.the lineac. j win=62967 Len=</td></t<>	Ack=279 Win=256 Len=0 ck=1801 Win=63043 Len= Ack=353 Win=256 Len= svr. the lineac. j instsvr.the lineac. j win=62967 Len=
▶ Frame 151: 194 bytes on wire (832 bits), 194 bytes captured (83 bits), 194 bytes capt	bits) on interface \Device リックする前は IPv4 〕 パブリック DNS への4 再問い合わせを行っ	^{wpp} (\$98882F7-89A1-4438-A4FF-80644896A3CB}, id アドレスで Web セッションが確立され 名前解決で否定応答を受け取り、 っていない	● れている IPv4 アドレ
😔 🌋 hunet-ng.pcapng		パケット数: 2082 / 表示: 2082 (1)	00.0%) プロファイル Default

図 6.1.6-21 IPv4 優先端末から WEB 表示した際のネットワークトレース結果(2)

本来の DNS 動作であるが、DNS サーバから否定応答のレスポンス(No such name)が通知されたら、以降 のクエリ問い合わせは行わない仕様のため、図 6.1.6-21 ケースについては仕様通りといえる。図 6.1.6-20 動作については、DNS サーバから否定応答を受け取っているが、OS やブラウザのキャッシュによりセッショ ンが継続されたことが考えられる。

本件で実証した環境についての考察として、IPv6 の DNS サーバと IPv4 の DNS サーバにおいて、 IPv6 の DNS サーバでレコードが存在しないことは Windows OS の設計上想定された設定ではないと考え る。デュアルスタック環境での DNS 設定は、IPv4 側(学内オンプレミス環境)と IPv6 側(パブリック DNS)のよ うに、異なる仕様の DNS サーバを指定してはいけないということである。学内の WEB サーバへのアクセス を目的とした実証検証については、IPv6 側の DNS サーバを未指定状態とし、IPv6 での実証機器向け名前 解決を hosts ファイルで実施すべきと考える。

【#5の補足】 ※2に関して

実証用学内WEBサーバのWEBページより「CLBOX」のハイパーリンクをクリックした際、「CLBOX」が稼働しているサーバの名前解決に失敗し、CLBOXを起動することができなかった。TCP/IPv6 側のパブリックDNS 側で学内ネットワーク内のサーバの名前解決ができないことが原因と判断し、CLBOX が稼働するサーバのIPv4 アドレスをWEBブラウザから直接入力することで実証を行った。本件に関しても、hosts ファイルでの名前解決が可能な実証環境であれば、正常動作したと推測する。

③ファイルサーバの利用(ユーザ認証、ファイル共有)

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
1	ノート	無線	IPv6	ファイルサ	IPv6	①検証用 PC から実証用ファ	Active Directory の認証が成	ОК
	PC		優先	- <i>i</i> ĭ		イルサーバの共有フォルダ	功し、共有フォルダの一覧表	
						を IPv6 アドレスで開く	示ができること	
						②認証画面で学内 AD ドメイ		
						ンの Windows アカウントを入		
						カする		
2	ノート	無線	IPv6	ファイルサ	IPv4	①検証用 PC から実証用ファ	Active Directory の認証が成	ок
	PC		優先	— <i>.</i>		イルサーバの共有フォルダ	功し、共有フォルダの一覧表	*
						を IPv4 アドレスで開く	示ができること	
						②認証画面で学内 AD ドメイ		
						ンの Windows アカウントを入		
						カする		
3	ノート	無線	IPv4	ファイルサ	IPv6	①検証用 PC から実証用ファ	Active Directory の認証が成	ОК
	PC		優先	- <i>i</i> ĭ		イルサーバの共有フォルダ	功し、共有フォルダの一覧表	
						を IPv6 アドレスで開く	示ができること(No.4 と同様	
						②認証画面で学内 AD ドメイ	の結果となること)	
						ンの Windows アカウントを入		
						カする		
4	ノート	無線	IPv4	ファイルサ	IPv4	①検証用 PC から実証用ファ	Active Directory の認証が成	ОК
	PC		優先	—/ĭ		イルサーバの共有フォルダ	功し、共有フォルダの一覧表	
						を IPv4 アドレスで開く	示ができること(No.4 と同様	
						②認証画面で学内 AD ドメイ	の結果となること)	
						ンの Windows アカウントを入		
						カする		

【#1 の補足】

ファイルサーバの共有フォルダにアクセスしたタイミングで Windows 認証が要求されたが、実証用 PC と ファイルサーバの間では、Active Directory サーバとの認証処理は記録されていませんでした。ネットワーク キャプチャ結果の 143 フレームで SMB2(Server Message Block プロトコル version 2)の「Session Setup Request」により、Active Directory のドメイン名(NETBIOS 名)とユーザ名でセッションリクエストが行われてい るが、145フレームに記録された「Session Setup Response」で「Success」が返答されるまでの間、Active Directory のドメインコントローラとの通信が介在していないことより、ファイルサーバとドメインコントローラの 間で IPv4 アドレスを使用した認証処理が行われたことが考えられる。



図 6.1.6-22 IPv6 優先端末でファイルサーバアクセス時のネットワークキャプチャ実行結果

【#2の補足】※に関して

実証端末からIPv4アドレスでファイルサーバにアクセスした際、「ネットワーク エラー」により共有フォルダ にアクセスできない現象が発生した。

ネットワーク エラー		×						
¥¥filesv-ipv4 にアクセスできません								
名前のスペルを確認しても問題がない場合 ります。ネットワークの問題を識別して解決す	は、ネットワークに問題が するには、[診断] をクリック	ある可能性があ りします。						
◇ 詳細を参照してください	診断(<u>D</u>)	キャンセル						

図 6.1.6-23 実証端末から IPv4 アドレスでファイルサーバアクセス時のエラーメッセージ

実証用 FW 装置のセッションログを確認した所、実証環境ネットワーク側のファイアウォールポリシーにより、学内既存ネットワーク上に設置されているファイルサーバからの SMB および SMB2 プロトコルが drop されていることが判明した。

				1 S					
ファイル(E) 編集(E) 設定(S)	コントロール(2) ウィンド	2(型) ヘルプ(日)							
Feb 12 17:01:06 hufw0	1/hufw02_IPCOMEX2	-3200_SC: firewall:	WARNING[40300011]: TCP connection	denied. src=172.16	.51.1 dst=172.16.1.	120 proto=tcp srcpor	rt=53048 dstpc	ort=22 in
terface=vlan50 dir=inl	bound action=drop	reason=filter rule	=59999						
[root@husv17 hufw01]#	more session-fwl	og-20210212 grep 1	72.16.51.1 grep	172.16.19.203					
Feb 12 17:18:28 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172.16.51.1 ds	t=172.16.19.203 pro	to=icmp icmp-type=8	icmp-code=0	icmp-id=1
icmp-sequence-no=45	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:18:28 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172.16.19.203	dst=172.16.51.1 pro	to=icmp icmp-type=0.	icmp-code=0	icmp-id=1
icmp-sequence-no=45	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:18:29 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172.16.51.1 ds	t=172.16.19.203 pro	to=icmp icmp-type=8	icmp-code=0	icmp-id=1
icmp-sequence-no=46	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:18:29 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172.16.19.203	dst=172.16.51.1 pro	to=icmp icmp-type=0	icmp-code=0	icmp-id=1
icmp-sequence-no=46	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:18:30 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172.16.51.1 ds	t=172.16.19.203 pro	to=icmp icmp-type=8	icmp-code=0	icmp-id=1
icmp-sequence-no=47	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:18:30 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172,16,19,203	dst=172.16.51.1 pro	to=icmp icmp-type=0	icmp-code=0	icmp-id=1
icmp-sequence-no=47	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:18:31 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172.16.51.1 ds	t= <mark>172.16.19.203</mark> pro	to=icmp icmp-type=8	icmp-code=0	icmp-id=1
icmp-sequence-no=48	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:18:31 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	INF0[00300005]:	IP packet passed.	src=172,16,19,203	dst=172.16.51.1 pro	to=icmp icmp-type=0	icmp-code=0	icmp-id=1
icmp-sequence-no=48	interface=vlan50	dir=inbound action=	accept rule=400						
Feb 12 17:19:17 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	WARNING[40300011]: TCP connection	denied. src=172.16	.51.1 dst=172.16.19	.203 proto=tcp srcpo	ort=53051 dstr	port=445
interface=vlan50 dir=	inbound action=dr	op reason=filter ru	ile=59999						
Feb 12 17:19:18 hufw0	1/hufw02 IPCOMEX2	-3200_SC: firewall:	WARNING[40300011]: TCP connection	denied. src=172.16	.51.1 dst=172.16.19	.203 proto=tcp srcpo	ort=53052 dstr	port=139
interface=vlan50 dir=	i <u>n</u> bound action=dr	op reason=filter ru	ile=59999						
Froot@husv17 hufw017#									

図 6.1.6-24 実証端末から IPv4 アドレスでファイルサーバアクセス時のファイアウォールログ

「図 6.1.4-1 IPv6 対応後の A 大学のシステム構成図」の【補足説明】で説明の通り、IPv6 実証用ネットワークの IPv4 と、既存ネットワークの IPv4 の L3 中継点は、実証用 FW 装置となるため、実証用 FW 装置による通信ブロックによるものと判断した。

対応として、既存ネットワーク(IPv4)→実証用ネットワーク(IPv4)のファイアウォール規則で SMB プロトコル (137-138/udp,139/tcp)および SMB2 プロトコル (445/tcp)の inbound に対する通信許可を与えることで対応 した。

3. WAN 越しアプリケーションレベルの検証

外部システム・商用サービスとして、複数のクラウドサービスによるメールの利用を検証対象とした。対象と したクラウドサービスは「G Suite」および「Exchange Online」(メールのみ)である。検証にあたり、IPv6 通信で SINET を経由してクラウドサービスへ正常に接続できるか検証した。次にクラウドサービスより提供されるメー ル機能を活用し、メールの送受信に影響がないか検証した。以上の確認をもとに、IPv6 通信でインターネッ トにあるクラウドサービスが利用できるか検証した。また、デュアルスタック環境内で IPv4 通信でも同様のこと が可能か検証した。

結果として、IPv6の規格に起因した課題は発生しなかったが、機器/サービスの仕様に起因した課題が計1件発生した。

(1) 業務アプリケーションにおける検証(クラウド)について

クラウド上で動作する業務アプリケーションの検証については、実証試験用の PC からクラウドサービス(G Suite および Exchange Online)に接続し、IPv6 でクラウドサービスに正常に接続できることを確認した。一般利 用者向け検証ではメールサービスが利用可能かどうか検証を行い、管理者向け検証では管理コンソールを 起動し、サービスの正常性確認が可能かどうか検証した。検証範囲を図 6.1.6-25 に示す。



図 6.1.6-25 業務アプリケーションにおける検証(クラウド)範囲

① G Suite の動作検証

クラウドサービス(G Suite)での一般利用者向けの動作検証として、Gmail が IPv6 および IPv4 の双 方で問題なく利用できるかどうか検証する。

管理者向けの動作検証として、「G Suite ステータス ダッシュボード」が IPv6 および IPv4 の双方で 問題なく利用できるかどうか検証する。

② Exchange Online の動作検証

クラウドサービス(Exchange Online)での一般利用者向けの動作検証として、WebMail 機能が IPv6 および IPv4の双方で問題なく利用できるかどうか検証する。

管理者向けの動作検証として、管理センタを起動し、サービス正常性を IPv6 および IPv4 の双方で 問題なく利用できるかどうか検証する。

上記①②のシナリオを実施した結果の内、主要な結果を以下に示す。

① G Suite の動作検証

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IP∨6			結果
				ビス名				
1	ノート	無線	IPv6	G suite	IPv6	①Gmail の URL を開く	Gmail が IPv6 で接続できるこ	ОК
	PC		優先	(WEB メー		②認証画面で ID、パスワー	ک	
				ル)		ドを入力する。		
				一般利用		③テストメールを送信する	テストメールの送受信が可	
				者向け			能であること	
2	ノート	無線	IPv4	G suite	IPv4	①Gmail の URL を開く	Gmail が IPv4 で接続できるこ	ок
	PC		優先	(WEB メー		②認証画面で ID、パスワー	ک	
				ル)		ドを入力する。		
				一般利用		③テストメールを送信する テストメールの送受信		
				者向け			能であること	
3	ノート	無線	IPv6	G Suite	IPv6	①G suite 管理者画面の URL	G suite 管理者画面が IPv6	ок
	PC		優先			を開く	で接続できること	
				管理者向		②管理コンソール画面右の		
				け		「ツール」のリストから「G	「G Suite ステータス ダッシ	
						Suite ステータス ダッシュボ	ュボード」画面の「現在のス	
						ード」をクリックする	テータス」の表から、Gmailの	
							ステータスを確認できること	
4	ノート	無線	IPv4	G Suite	IPv4	①G suite 管理者画面の URL	G suite 管理者画面が IPv4	ОК
	PC		優先			を開く	で接続できること	
				管理者向		②管理コンソール画面右の		
				け		「ツール」のリストから「G	「G Suite ステータス ダッシ	
						Suite ステータス ダッシュボ	ュボード」画面の「現在のス	
						ード」をクリックする	テータス」の表から、Gmailの	
							ステータスを確認できること	

【#1 の補足】

Gmail の実証にあたり、「(a)nslookup コマンドでの名前解決状況確認」、「(b)WEB メールが IPv6 で起動できているか」、「(c)メール送受信が IPv6 で正しく行えているか」について実証を行った。

(a) nslookup コマンドでの名前解決状況確認

Gmail 実証時の nslookup コマンド実行結果を以下に記載する。



図 6.1.6-26 「mail.google.com」に対する nslookup 結果

Gmail のアクセス先である「mail.google.com」に対する DNS クエリの結果として、IPv6 アドレス(AAAA レ コード)と IPv4 アドレス(A レコード)が通知されていることが確認した。

(b)WEBメールが IPv6 で起動できているか

WEBメールを起動し、利用者認証が行われたことを確認後、ネットワークトレース結果を確認した。

mixー) の tmlusrfi00	心確認用O(D1
177-5817		
□ パスワードを表示	します	
パスワードをお忘れの場	lê.	* ^

図 6.1.6-27 Gmail での利用者認証画面

ネットワークトレース結果より、実証用 PC と google 社のサイトが IPv6 アドレスでセッションが確立されていることを確認した。

民族	伝フィルタ…、	(Ctr⊢/> をji	阃用					+ 🕞
No.	Time			Source	Destination	Protocol	Length Info	^
	892 202	1-01-28	13:00:22.1401	0 2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50224 [AC	K] Seq=3827 Ack=3811 Win=7321
	893 202	1-01-28	13:00:22.14039	00 2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.3	654 Application Dat	a, Application Data
	894 202	1-01-28	13:00:22.1405	70 2001:2f8:103c:6052:	2404:6800:400a:809::200e	TLSv1.3	105 Application Dat	a
	895 202	1-01-28	13:00:22.1408	9 2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.3	105 Application Dat	a
	896 202	1-01-28	13:00:22.15119	06 2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50224 [AC	K] Seq=4438 Ack=3842 Win=7321
	897 202	1-01-28	13:00:22.1807	9 2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.3	441 Application Dat	a
	898 202	1-01-28	13:00:22.1808	3 2001:2f8:103c:6052:	2404:6800:400a:809::200e	TCP	74 50224 → 443 [AC	K] Seq=3842 Ack=4805 Win=6502
	899 202	1-01-28	13:00:22.18104	15 2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.3	665 Application Dat	a, Application Data
	900 202	1-01-28	13:00:22.18104	15 2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.3	113 Application Dat	a
	901 202	1-01-28	13:00:22.18110	08 2001:2f8:103c:6052:	2404:6800:400a:809::200e	TCP	74 50224 → 443 [AC	K] Seq=3842 Ack=5435 Win=6604 🗸
۲								>
▷ E ▷ D	thernet I ata (46 b 0 ff ff	I, Src: ytes) ff ff ff f	Buffalo_30:fa	6e (58:27:8c:30:fa:6e) 30 fa 6e 88 99 23 51	<pre>, Dst: Broadcast (ff:ff:ff:ff:ff)x.xave and ave a second second</pre>			
001 002	0 92 42 0 00 00	9d 41 e 00 00 0	9 58 27 8c 30 0 00 00 00 00	fa 6e 00 00 00 00 00 00 00 00 00 00 00 00 00	·B·A·X'· 0·n·····			
003	00 00	00 00 00	00 00 00 00	00 00 00				

図 6.1.6-28 Gmail での利用者認証画面表示時のネットワークトレース結果

(c)メール送受信が IPv6 で正しく行えているか

Gmail にログイン後テストメールを送信し、正しく処理できているかどうかを確認した。 以下のようにテストメールを作成し、「送信」ボタンを押した後にテストメールを受信できることを確認 いた。

E M Gmail	Q メールを模定			0 8		
作成	□- c :				1~50/293.87 ()
] 受信トレイ 11		🗶 ソーシャル 💊 プロ	モーション			
オ スター付き	📋 🚖 🐌 Google	セキュリティ通知・新しいデバイスでのログ	インマートで、「トルート」のなたの	Google アカウントに新しい	Window	12
) スヌーズ中	📋 🚖 D Google	セキュリティ通知・新しいデバイスでのログ	10x6 text			12
> 送信済み	🗆 🌣 🎽 inician Shiftmaren y	test - test	NH I may all 2012 PRO1 atminuted		_ K A	1/
下書き / もっと見る	🗌 🕁 🥭 自分	test-test	現代人 With A Land Construction	of the first floor (by a	uc boc	17
laat	🔲 🗄 🗇 Google	セキュリティ通知・新しいデバイスでのログ	· iPv6 test			1
 会議を新規作成 	□ ☆ ⊅ ₹213	mailtest0608 問い合わせNo.1向けテスト-04	IPv6高证用			16/
3 参加予定の会議	📋 👷 🗇 tmlgrpfj001	mailtest0608 問い合わせNo.1向けテスト-03	8			16/
ングアウト	二 合 D テスト3	mailtest0608 目い合わせNo.1向けテスト-02	i			16/
メール確認用な	+ 🗌 🕆 D 721-3	mailtest0608 問い合わせNo.1向けテスト-01	テスト-01			16
	🗍 🖞 🍺 Kobayashi.no(ilians.	mailtest0603 問い合わせNo.2#2向けテスト・				16/
	🗋 🕁 D bis, ku, ko, liebargestu	mailtest0603 目い合わせNo.2#2向けテスト・				16.
		mailtest0603 目い合わせNo.2#2向けテスト・				16/
最近のチャットはありません	🗋 🕁 🔉 kohayanlık neşi hçifa	mailtest0603 問い合わせNo.2#2向けテスト-				16,
	が トップ手切を有効にしてください OV 1	10603 貫い合わせNo.2向けテスト-04				16/
	STRACTOR CONTRACTOR	····································		801	: 🖬	16/1

図 6.1.6-29 Gmail でのテストメール作成画面

= 附 Gmail	Q、 又一儿应根索	· 0 @ II +4	852 😣
- 作成	□- ¢ :	1-50 / 294 77	з э
ロ 登録トレイ 112	Q X4>	ン ソーシャル	
★ スター付き	🗌 ☆ 笋 自分	IPv6 test - IPv6英証用	13:06
0 スヌーズ中	📋 🏫 🐌 Google	セキュリティ通知・新しいデバイスでのログイン	12:55
> 送信済み ▶ 工業★	🗌 🚖 D Google	セキュリティ通知・新しいデバイスでのログイン 「Particle Particle Part	12:48
■ 「日本 × もっと見る		test - test	2020/11/15
leat	🗌 🕸 🐌 自分	test-test.	2020/11/15
 会議を新規作成 	📋 💠 🗩 Google	セキュリティ通知・新しいデバイスでのログイン internation 1 graduation a so (p あなたの Google アカウントに新しい Windo	2020/11/15
) 参加予定の会議	🗋 쇼 D 77F3	nativities Buddutini, Althe 23-14	2020/06/08
ングアウト	🗇 oʻ to Maydilli	malmontan Blockstyne of the 2.5 Au	2020/06/08
メール確認用0(+	D 7213	national BAARPA REPORT AND A CONTRACT OF A C	2020/06/08
	□ ☆ Ɗ 7 2 ►3	automon By Augen, Miller A. 49 20.2 - 6.0 March 76 2005-7. (mapping, class, 20.4).	2020/06/08
	🗇 🛧 😕 kablesahi regihijiti	national Redaipin and REPAID an extension Representation (CD) in the REPAID and	2020/06/03
	🗍 🖈 2	national discharge (Add 131-D) constraints and the constraints of the	2020/06/03
厳近のチャットはありません		national disalation and details as managed in proprior difference in the pathward.	2020/06/03
メール水送信しました。 歌び)酒し、メッセージを表示 X	NUMBER OF ADDRESS OF ADDRESS ADDRESS OF ADDRESS OF ADDR	2020/06/03
	Chigospi	and a set of the set o	2020/06/03

図 6.1.6-30 Gmail でのテストメール受信画面

テストメールの受信を確認後、ネットワークトレース結果より実証用 PC と google 社のサイトが IPv6 アドレスでセッションが確立されていることを確認した。

		db/13				
	Time		Source	Destination	Protocol L	ength Info
165	5 2021-01-28	13:06:51.331136	Buffalo_30:fa:6e	Broadcast	0x8899	60 Realtek Layer 2 Protocols
166	6 2021-01-28	13:06:51.861602	Buffalo_f8:87:48	Broadcast	ARP	60 Who has 172.16.52.254? Tell 172.16.52.252
167	7 2021-01-28	13:06:52.209584	2001:2f8:103c:6052:	2404:6800:400a:809::200e	TLSv1.2	307 Application Data
168	8 2021-01-28	13:06:52.209678	2001:2f8:103c:6052:	2404:6800:400a:809::200e	TLSv1.2	837 Application Data
169	9 2021-01-28	13:06:52.215602	2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50224 [ACK] Seq=860 Ack=4061 Win=14
176	0 2021-01-28	13:06:52.215900	2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50224 [ACK] Seq=860 Ack=4824 Win=14
171	1 2021-01-28	13:06:52.256809	2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.2	457 Application Data
172	2 2021-01-28	13:06:52.256809	2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.2	436 Application Data, Application Data
173	3 2021-01-28	13:06:52.257006	2001:2f8:103c:6052:	2404:6800:400a:809::200e	TCP	74 50224 → 443 [ACK] Seq=4824 Ack=1605 Win=2
174	4 2021-01-28	13:06:52.257272	2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TLSv1.2	113 Application Data
175	5 2021-01-28	13:06:52.258930	2001:2f8:103c:6052:	2404:6800:400a:809::200e	TLSv1.2	113 Application Data
176	6 2021-01-28	13:06:52.264877	2404:6800:400a:809:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50224 [ACK] Seq=1644 Ack=4863 Win=1
17	7 2021-01-28	13:06:53.331037	Buffalo_30:fa:6e	Broadcast	0x8899	60 Realtek Layer 2 Protocols
178	8 2021-01-28	13:06:53.984666	2001:2f8:103c:6052:	2404:6800:400a:80b::200e	TCP	75 50223 → 443 [ACK] Seq=1 Ack=1 Win=256 Ler
179	9 2021-01-28	13:06:53.990619	2404:6800:400a:80b:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	86 443 → 50223 [ACK] Seq=1 Ack=2 Win=361 Ler
180	0 2021-01-28	13:06:54.243583	2001:2f8:103c:6052:	2404:6800:400a:80c::2005	TLSv1.2	2195 Application Data
181	1 2021-01-28	13:06:54.243650	2001:2f8:103c:6052:	2404:6800:400a:80c::2005	TLSv1.2	179 Application Data
182	2 2021-01-28	13:06:54.249617	2404:6800:400a:80c:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50222 [ACK] Seq=9062 Ack=10549 Win=
183	3 2021-01-28	13:06:54.249617	2404:6800:400a:80c:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50222 [ACK] Seq=9062 Ack=11230 Win=
184	4 2021-01-28	13:06:54.249617	2404:6800:400a:80c:	2001:2f8:103c:6052:f4ac:7f31:3947:76a5	TCP	74 443 → 50222 [ACK] Seq=9062 Ack=11335 Win=
18	5 2021-01-28	13.06.54 456617	2404 · 6800 · 400a · 80c ·	2001.2f8.103c.6052.fdac.7f31.3947.76a5	TI 5v1 2	466 Annlication Data
						•
Frame	1: 78 bytes	on wire (624 bi	ts), 78 bytes capture.	d (624 bits) on interface \Device\NPF_{F46BD	3AC-E983-47	711-81A1-4C46D0BBEEBB}, id 0
200 al	8 b2 da 5d a	a a0 90 1b 0e 8	3b ba a2 08 00 45 00	···]··················		
010 0	0 40 10 46 0	0 00 80 11 00 0	0 ac 10 34 01 ac 10	·@·F···· 4···		
820 04	0 cc 13 6d 1	.3 6c 00 2c 8d 2	b 48 57 24 00 00 00	····m·l·, ·+HW\$····		
	3 00 00 00 9	c b0 85 00 00 0	00 00 00 00 00 00 00			
930 0	5 00 00 00 5					

図 6.1.6-31 Gmail でのテストメール受信時のネットワークトレース結果

② Exchange Online の動作検証

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
1	ノート	無線	IPv6	Office365	IPv6	①マイクロソフトオンラインサ	Office365(WebMail) が IPv6	OK
	PC		優先	(WEB メー		ービスの URL を開く	で接続できること	
				ル)		②認証画面で ID、パスワー		
				一般利用		ドを入力する	テストメールの送受信が可	
				者向け		③テストメールを送信する	能であること	
2	ノート	無線	IPv4	Office365	IPv4	①マイクロソフトオンラインサ	Office365(WebMail) が IPv4	OK
	PC		優先	(WEB メー		ービスの URL を開く	で接続できること	
				ル)		②認証画面で ID、パスワー		
				一般利用		ドを入力する	テストメールの送受信が可	
				者向け		③テストメールを送信する	能であること	
3	ノート	無線	IPv6	Office365	IPv6	①マイクロソフトオンラインサ	Office365 管理センタ画面が	OK
	PC		優先			ービスの管理ポータル画面	IPv6 で接続できること	
				管理者向		の URL を開く		
				け		②管理センタのメニューから		
						「正常性」-「サービス正常	「サービス正常性」画面の	
						性」を選択する	「すべてのサービス」の表か	
							ら、Exchange Online の「状	
							態」列が	
							「正常」、もしくは運用に支障	
							が無いインシデント/アドバ	
							イザリ検知、であること	
4	ノート	無線	IPv4	Office365	IPv4	①マイクロソフトオンラインサ	Office365 管理センタ画面が	OK
	PC		優先			ービスの管理ポータル画面	IPv4 で接続できること	
				管理者向		の URL を開く		
				け		②管理センタのメニューから	「サービス正常性」画面の	
						「正常性」-「サービス正常	「すべてのサービス」の表か	
						性」を選択する	ら、Exchange Online の「状	
							態」列が	
							「正常」、もしくは運用に支障	
							が無いインシデント/アドバ	
							イザリ検知、であること	

【#1 の補足】

Office365(WEBメール)の確認に際し、Gmailと同様の確認を行った。

(a) nslookup コマンドでの名前解決状況確認

マイクロソフトオンラインサービスの URL「login.microsoftonline.com」起動に先立ち、nslookup コマンド実行結果を以下に記載する。

CIV.	管理者: C:¥Windows¥system32¥cmd.exe	-	×
バケッ ラウンド 最小 =	ト数: 送信 = 4、受信 = 4、損失 = 0(0% の損失)、 トリップの概算時間(ミリ秒): : 6ms、最大 = 6ms、平均 = 6ms		^
C:¥Users¥a サーバー: Address:	administrator>nslookup login.microsoftonline.com dns.google 2001:4860:4860::8888		
権限のない 名前: c Addresses:	回答: >sa.next.a.prd.aadg.trafficmanager.net 20.190.165.20 40.126.37.0 40.126.37.6 20.190.165.5 40.126.37.4 20.190.165.22 20.190.165.7 20.190.165.7 20.190.165.4		
Aliases:	login.microsoftonline.com a.privatelink.msidentity.com prda.aadg.msidentity.com www.tm.a.prd.aadg.trafficmanager.net		
C:¥Users¥a	administrator>_		~

図 6.1.6-32 マイクロソフトオンラインサービスの nslookup 確認結果

上図に記載の通り、マイクロソフトオンラインサービスのサインイン URL に関してはAレコードのみ 通知されるため、ログイン認証については IPv4 で通信されることが予測される。

引き続き、マイクロソフトオンラインサービスのサインイン認証完了後にリダイレクトされる「office.com」 についても同様の確認を行った。

CETTER C:¥Windows¥system32¥cmd.exe	- 🗆 🗙
名前: www.tm.a.prd.aadg.akadhs.net Addresses: 20.190.141.193 20.190.141.225 20.190.141.231 20.190.141.227 20.190.141.230 20.190.141.192 20.190.141.194 20.190.141.229	
Aliases: login.microsoftonline.com a.privatelink.msidentity.com prda.aadg.msidentity.com C:¥Users¥administrator>nslookup office.com サーバー: dns.google	
Address: 2001:4860:4860::8888 権限のない回答: 名前: office.com Addresses: 2620:1ec:a92::156 13.107.6.156	
C:¥Users¥administrator>_	~

図 6.1.6-33 「office.com」の nslookup 確認結果

上図に記載の通り、リダイレクト先「office.com」の URL に関してはAレコードと AAAA レコードが通知されるため、IPv4/IPv6 デュアルで通信できることが予測される。

(b)WEBメールが IPv6 で起動できているか

マイクロソフトオンラインサービスが IPv4 で認証が行われ、office.com が IPv6 通信で行われるかど うかを確認するため、マイクロソフトオンラインサービスでのサインイン認証を行った時点、および WEBメール起動完了時点でのネットワークトレース結果を確認した。



図 6.1.6-34 マイクロソフトオンラインサービスサインイン画面

上図の状態でのネットワークトレースを以下に記載する。

No.	Time	Source	Destination	Protoco	Length Info
69	5 2021-01-28 13:20:46.384	40.126.37.5	172.16.52.1	TLSv1.2	1105 Application Data
69	6 2021-01-28 13:20:46.384	172.16.52.1	40.126.37.5	TCP	54 50556 → 443 [ACK] Seg=13453 Ack=49184 Win=262144 L
69	7 2021-01-28 13:20:46.464	2001:2f8:103c:6052:ec1d:7936:ed0c:	2001:4860:4860::8888	DNS	105 Standard query 0xe58b A login.microsoftonline.com
69	8 2021-01-28 13:20:46.465	2001:2f8:103c:6052:ec1d:7936:ed0c:_	2001:4860:4860::8888	DNS	105 Standard query 0xb852 AAAA login.microsoftonline.c
69	9 2021-01-28 13:20:46.478	2001:4860:4860::8888	2001:2f8:103c:6052:ec1d	DNS	369 Standard query response 0xe58b A login.microsofton
70	00 2021-01-28 13:20:46.487	2001:4860:4860::8888	2001:2f8:103c:6052:ec1d	DNS	273 Standard query response 0xb852 AAAA login.microsof
70	1 2021-01-28 13:20:46.488	172.16.52.1	20.190.141.225	TCP	66 50561 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W
78	2 2021-01-28 13:20:46.488	172.16.52.1	20.190.141.225	TCP	66 50560 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W
78	3 2021-01-28 13:20:46.500	20.190.141.225	172.16.52.1	TCP	66 443 → 50561 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 /
70	4 2021-01-28 13:20:46.500	20.190.141.225	172.16.52.1	TCP	66 443 + 50560 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 /
70	5 2021-01-28 13:20:46.500	172.16.52.1	20.190.141.225	TCP	54 50560 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
70	6 2021-01-28 13:20:46.500	172.16.52.1	20.190.141.225	TCP	54 50561 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
70	7 2021-01-28 13:20:46.500	172.16.52.1	20.190.141.225	TLSv1.2	274 Client Hello
70	8 2021-01-28 13:20:46.500	172.16.52.1	20.190.141.225	TLSv1.2	274 Client Hello
78	9 2021-01-28 13:20:46.514	20.190.141.225	172.16.52.1	TCP	1514 443 → 50561 [ACK] Seq=1 Ack=221 Win=262656 Len=146
71	0 2021-01-28 13:20:46.514	20.190.141.225	172.16.52.1	TCP	1514 443 → 50561 [ACK] Seq=1461 Ack=221 Win=262656 Len=
71	1 2021-01-28 13:20:46.514	20.190.141.225	172.16.52.1	TLSv1.2	701 Server Hello, Certificate, Server Key Exchange, Se
71	2 2021-01-28 13:20:46.514	20.190.141.225	172.16.52.1	TCP	1514 443 → 50560 [ACK] Seq=1 Ack=221 Win=262656 Len=146
71	3 2021-01-28 13:20:46.515	172.16.52.1	20.190.141.225	TCP	54 50561 → 443 [ACK] Seq=221 Ack=3568 Win=262144 Len=
					>
⊿	Answers				
	⊿ login.microsoftonline.c	com: type CNAME, class IN, cname a.pr	ivatelink.msidentity.com		
	Name: login.microso	ftonline.com			
	Type: CNAME (Canoni	cal NAME for an alias) (5)			
	Class: IN (0x0001)				
	Time to live: 273 (4 minutes, 33 seconds)			
	Data length: 27				
	CNAME: a.privatelin	k.msidentity.com			
	▲ a.privatelink.msidentit	ty.com: type CNAME, class IN, cname p	rda.aadg.msidentity.com		
	Name: a.privatelink	.msidentity.com			
	Type: CNAME (Canoni	cal NAME for an alias) (5)			
	Class: IN (0x0001)				
	Time to live: 264 (4 minutes, 24 seconds)			
	Data length: 12				
	CNAME: prda.aadg.ms	identity.com			
	4 prda.aadg.msidentity.co	om: type CNAME, class IN, cname www.t	m.a.prd.aadg.akadns.net		

図 6.1.6-35 マイクロソフトオンラインサービスサインイン時のネットワークトレース結果

上図のネットワークトレース結果より、nslookupコマンドで得られたマイクロソフトオンラインサービスの IPv4 アドレスとの間で TCP 通信が行われていることを確認した。

引き続き、マイクロソフトオンラインサービスから「office.com」 ヘリダイレクトされた後の通信状況の確認を行った。



図 6.1.6-36 「office.com」から Outlook WEB メールを開いた状態

この状態でのネットワークトレースを以下に記載する。

	表示フィルタ … 〈Ctrl-/〉を適用			
٩o.	Time Source	Destination	Protocol L	ength Info
	316 2021-01-28 13:27:50.580884 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=103352 Ack=11936 Wi
	317 2021-01-28 13:27:50.580884 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=104792 Ack=11936 Wi
	318 2021-01-28 13:27:50.580884 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TLSv1.2	911 Application Data
	319 2021-01-28 13:27:50.580884 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=107069 Ack=11936 Wi
	320 2021-01-28 13:27:50.581071 2001:2f8:103c:6052:.	. 2620:1ec:c::11	TCP	74 50645 → 443 [ACK] Seq=11936 Ack=108509 Wi
	321 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=108509 Ack=11936 Wi
	322 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=109949 Ack=11936 Wi
	323 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=111389 Ack=11936 Wi
	324 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=112829 Ack=11936 Wi
	325 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TLSv1.2	1151 Application Data
	326 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TLSv1.2	255 Application Data
	327 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=115527 Ack=11936 Wi
	328 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=116967 Ack=11936 Wi
	329 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=118407 Ack=11936 Wi
	330 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=119847 Ack=11936 W
	331 2021-01-28 13:27:50.581316 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=121287 Ack=11936 W
	332 2021-01-28 13:27:50.581647 2001:2f8:103c:6052:.	. 2620:1ec:c::11	TCP	74 50645 → 443 [ACK] Seq=11936 Ack=122727 Wi
	333 2021-01-28 13:27:50.581862 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TLSv1.2	1151 Application Data
	334 2021-01-28 13:27:50.581862 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=123804 Ack=11936 W
	335 2021-01-28 13:27:50.581862 2620:1ec:c::11	2001:2f8:103c:6052:ec1d:7936:ed0c:ef6c	TCP	1514 443 → 50645 [ACK] Seq=125244 Ack=11936 Wi
¢	336 2021-01-28 13+27+50 581862 2620+1ec+c++11	2001.248.103c.602.er14.2036.ed0c.ef6c	тср	1514 443 → 50645 [ACK] Sen=126684 Ark=11936 W
Þ	rame 1: 60 bytes on wire (480 bits), 60 bytes captur	ed (480 bits) on interface \Device\NPF_{F46	BD3AC-E983-4	711-81A1-4C46D0BBEEBB}, id 0
00	30 ff ff ff ff ff ff 58 27 8c 30 fa 6e 88 99 23 47	·····X* ·0·n·· <mark>#G</mark>		
00	10 f4 12 3a 5c 4e 58 27 8c 30 fa 6e 00 00 00 00 00	••:\NX'• 0•n••••		
00	20	· · · · · · · · · · · · · · · · · · ·		
00	30 00 00 00 00 00 00 00 00 00 00 00			

図 6.1.6-37 「office.com」から Outlook WEB メールを開いた状態でのネットワークトレース結果

上記ネットワークトレース結果より Office365 WEB サービスとの間で IPv6 通信を行えていることを確認した。

(c)メール送受信が IPv6 で正しく行えているか

Office365(WEBメール)よりテストメールを送信し、正しく処理できているかどうかを確認した。

4. 運用性/保守性に関する検証

IPv6 環境における保守作業に関する影響の確認について、運用性/保守性(ログ管理、トラブルシュート 方式、端末追跡等)の確認および実証に使用する各種機器の基本的な設定確認を行うことで、既存の IPv4 ネットワーク環境との間で運用・保守に関して留意すべき内容が発生しないか検証した。また、実証に使用 する各種機器の基本的な設定確認については、IPv6 ホストに付与される IPv6 アドレスが RA を使用した IP アドレスやゲートウェイの自動設定を行う場合とそうでない場合に分けて検証した。

結果として、IPv6の規格に起因した課題は発生しなかったが、IPv6対応における留意事項が1件発生した。

(1) IPv4/IPv6 デュアルスタックの基本的な設定の確認

実証対象のサーバおよび PC について、IPv6 ホストに付与される IPv6 アドレスがどのように割り当てられるか 検証した。本実証環境では、特定部局向けネットワークセグメントについて、(Router Advertisement: ルータ広 告)による IPv6 アドレス自動取得可能な環境を構成し、ネットワークトレースを行いながら RA を構成しないネ ットワーク環境との差異について検証した。実証結果を以下に記載する。

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
1	実証用	有線	IPv6	実証用ネ	IPv6	ipconfig /all を実行する	実行結果より以下の内容を	ОК
	WEB		優先	ットワーク	(手動)		確認する	
	サーバ			(LAN051)			・IPv6 アドレス:手動設定値	
							・一時 IPv6 アドレス:未割	
				RA 送信無			当	
							・リンクローカル IPv6 アドレ	
							ス:自動設定	
							・以下、手動設定した値	
							- IPv4 アドレス	
							- サブネット マスク	
							- デフォルトゲートウェイ	
							(IPv4)	
							- デフォルトゲートウェイ	
							(IPv6)	

① IPv6 アドレスの自動設定における検証

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
2	デスクト	有線	IPv6	実証用ネ	IPv6	ipconfig /all を実行する	実行結果より以下の内容を	ОК
	ップ PC		優先	ットワーク	(手動)		確認する	
				(LAN052)			・IPv6 アドレス:手動設定値	
							・一時 IPv6 アドレス:自動	
				RA 送信有			設定	
							・リンクローカル IPv6 アドレ	
							ス:自動設定	
							・以下、手動設定した値	
							- IPv4 アドレス	
							- サブネット マスク	
							- デフォルトゲートウェイ	
							(IPv4)	
							- デフォルトゲートウェイ	
							(IPv6)	
3	ノート	無線	IPv6	実証用ネ	IPv6	ipconfig /all を実行する	実行結果より以下の内容を	ОК
	PC		優先	ットワーク	(手動)		確認する	
				(LAN052)			・IPv6 アドレス:手動設定値	
							・一時 IPv6 アドレス:自動	
				RA 送信有			設定	
							・リンクローカル IPv6 アドレ	
							ス:自動設定	
							・以下、手動設定した値	
							- IPv4 アドレス	
							- サブネット マスク	
							- デフォルトゲートウェイ	
							(IPv4)	
							- デフォルトゲートウェイ	
							(IPv6)	
#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実施
---	-----	----	------	----------	------	----------------------	---------------------	----
	機器名	無線	IPv6	器名・サー	IPv6			結果
				ビス名				
4	ノート	無線	IPv6	実証用ネ	IPv6	①「インターネット プロトコル	実行結果より以下の内容を	ОК
	PC		優先	ットワーク	(自動)	バージョン 6(TCP/IPv6)」の	確認する	
				(LAN052)		プロパティより「IPv6 アドレス	・IPv6 アドレス:自動設定値	
						を自動的に取得する」を選択	・一時 IPv6 アドレス:自動	
				RA 送信有		し、「OK」を押して設定を反	設定	
						映する。	・リンクローカル IPv6 アドレ	
						②ipconfig /all を実行する	ス:自動設定	
							・デフォルトゲートウェイ	
							(IPv6)	
							実証用 L3 スイッチの	
							(LAN052)の IPv6 アドレス	
							・以下、手動設定した値	
							- IPv4 アドレス	
							- サブネット マスク	
							- デフォルトゲートウェイ	
							(IPv4)	
							- デフォルトゲートウェイ	
							(IPv6)	

【#1の補足】

(a) IP アドレス割り当て状況の確認

実証用 L3 スイッチから RA 送信が行われないネットワークアドレスで IPv6 設定を確認した結果を 下図に記載する。



図 6.1.6-38 「ipconfig /all」実行結果(RA 未送信セグメント)

以上のように、手動で設定した IPv6 アドレスおよびデフォルトゲートウェイを確認した。リンクローカ ルアドレスについては、「fe80::」のプレフィックス以降、ユニークな情報が設定され、「%」以降にネッ トワーク アダプタのインターフェース番号が付与されていることを確認した。L3 スイッチから RA 送 信が行われないネットワークセグメントについては、一時(匿名) IPv6 アドレスが付与されないことに ついても確認した。

(b) ネットワークトレースに関する考察

TCP/IPv6 を利用するネットワーク アダプタについて、TCP/IPv6 の無効→有効を行った際のネットワークフローを確認する目的で採取したネットワークトレースを以下に記載する。

A	20210217-hunet rsra	a.pcapng
ファイル(E) 編集(E) 表示(Y) 移動(G) キャプチャ(C) 分析(A)	紀け(S)電話(x)無線(W) Q、Q、Q、 <u>計</u>) ツール(工) ヘルプ(出)
II icmpv6		Q
No. Time Source 1728 2921-02-17 14:11:29.200 fe80:17ca0:d600:560c:a528 1723 2021-02-17 14:11:29.200 fe80:17ca0:d600:560c:a528 1725 2021-02-17 14:11:29.200 fe80:17ca0:d600:560c:a528 1725 2021-02-17 14:11:29.210 fe80:17ca0:d600:560c:a528 1729 2021-02-17 14:11:29.210 fe80:17ca0:d600:560c:a528 1737 2021-02-17 14:11:29.210 fe80:17ca0:d600:560c:a528 1737 2021-02-17 14:11:29.341 fe80:17ca0:d600:560c:a528 1742 2021-02-17 14:11:29.341 fe80:17ca0:d600:560c:a528 1745 2021-02-17 14:11:29.341 fe80:17ca0:d600:560c:a528 1745 2021-02-17 14:11:29.341 fe80:17ca0:d600:560c:a528 1745 2021-02-17 14:11:29.341 fe80:17ca0:d600:560c:a528 1745 2021-02-17 14:11:29.341 fe80:17ca0:d600:560c:a528 1746 2021-02-17 14:11:37.341 fe80:17ca0:d600:560c:a528 1746 2021-02-17 14	Destination ff02:116 ff02:116 ff02:116 ff02:116 ff02:126 ff02:12 ff02:12 ff02:12 ff02:11 ff02:12 ff02:12 ff02:12	Protoco Length Info ICMP+6 90 Multicast Listener Report Message v2 ICMP+6 150 Multicast Listener Report Message v2 ICMP+6 160 Multicast Listener Report Message v2 ICMP+6 170 Router Solicitation from 00:50:56:10:10:10:10:10:10:10:10:10:10:10:1
<		>
D Frame 1771: 86 bytes on wire (688 bits), 86 bytes captured (68 D Ethernet II, Src: Whare, 9e:67.3c (00:50:56:9e:67.3c), Dat: IP D Internet Protocol Version 6, Src: feB0::7ca0:6600:560c:a528, D d Internet Control Nessage Protocol v6 Type: Neighbor Advertisement (136) Code: 0 Checksum: 0xffb6 [correct] [Checksum: 0xffb6 [correct] [Checksum: 0xffb6 [correct] [Checksum: 0xffb6] b Flags: 0c20000000, Override Target Address: feB0::7ca0:6600:560c:a528 d IOPv6 Option (Target Link-layer address : 00:50:56:9e:67:11 Type: Target Link-layer address (2) Length: 1 (8 bytes) Link-Layer address: Vhare_9e:67:12 (00:50:56:9e:67:12)	i bits) on interface \Device (decast_01 (33:33:00:00:00:00:0) it: ff02::1 c)	VNPF_{598002F7-09A1-4438-AAFF-00644896A3C8}, 1d 0 1)
0010 00 00 00 20 3a ff fe 80 00 00 00 00 00 7c a0 1		
Q 2 Internet Control Message Protocol v6: Protocol		/竹ット数: 2948 · 表示: 12 (0.4%) プロファイル: Default

図 6.1.6-39 ネットワークトレースの状態(RA 未送信セグメント)

1742 フレーム目で実証用 PC から近隣のルータ宛にマルチキャストで RS(Router Solicitation)が発行していることを確認した。本セグメントはルータ(実証用 L3 スイッチ)から RA (Router Advertisement)が送信されていないため、1741 フレームで発行した NS(Neighbor Solicitation)に対する応答として、自側のリンクローカルアドレスをマルチキャストで NA(Neighbor Advertisement)を送信していることを確認した。

【#2の補足】

(a) IP アドレス割り当て状況の確認

実証用 L3 スイッチから RA 送信が行われるネットワークアドレスで IPv6 設定を確認した結果を図 6.1.6-40 に記載する。

C:¥WINDOWS¥system32¥cmd.exe —		×
Microsoft Windows [Version 10.0.18363.1016] (c) 2019 Microsoft Corporation. All rights reserved.	最大化	^
C:¥Users¥user>ipconfig /all		
Windows IP 構成		
ホスト名		
Wireless LAN adapter Wi-Fi:		^
接続固有の DNS サフィックス : 説明. : Intel (R) Wireless-AC 9560 160MHz 物理アドレス. : 90-78-41-98-05-3A DHCP 有効. : いいえ 自動構成有効 : (+1) IPv6 アドレス. : 2001:278:103c:6052::2002(優先) 時 IPv6 アドレス. : 2001:278:103c:6052:e509.8513.07e.9d04(優先) リンクローカル IPv6 アドレス. : 2001:278:103c:6052:e509.8513.07e.9d04(優先) IPv4 アドレス. : 172:16.52.2(優先) サブネット マスク. : : 2001:278:103c:6052::1 : 172:16.52.255.255.0 : デフォルト ゲートウェイ : 2001:278:103c:6052::1 : 172:16.52.253 : DHCPv6 IAID : 160462913 DHCPv6 クライアント DUID. : 00-01-00-01-24-01-F9-31-4C-36-4E-3E-F6-57 DNS サーバー : 8.8.8 NetBIOS over TCP/IP : 有効		
イーサネット アダプター Bluetooth ネットワーク接続:		
メディアの状態メディアは接続されていません 接続固有の DNS サフィックス 説明		
C:¥Users¥user>_		

図 6.1.6-40 「ipconfig /all」実行結果(RA 送信セグメント)

以上のように、手動で設定した IPv6 アドレスおよびデフォルトゲートウェイを確認した。併せてルータからの RA 送信が有効なネットワークセグメントの場合、IPv6 アドレス・一時 IPv6 アドレスも併せて 設定されていることを確認した。

新たに設定されたIPv6アドレスについては、ルータからアドバタイズされたルート情報に基づいて、 新しく割り当てられた IPv6 アドレスが自動設定されている。

一時 IPv6 アドレスについては、本実証パターンのように IPv6 アドレスの自動設定を行った場合に 自動的に作成されることを確認した。

(b) ネットワークトレースに関する考察

TCP/IPv6 を利用するネットワーク アダプタについて、TCP/IPv6 の無効→有効を行った際のネットワークフローを確認する目的で採取したネットワークトレースを以下に記載する。

	201101261310-IPv6RSRA.pcapng	
	ファイル(E) 編集(E) 表示(Y) 移動(G) キャブチャ(C) 分析(A) 統計(S) 電話(Y) 無線(W) ツール(I) ヘルプ(H)	
	No. Time Source Destination Protoco Length Info	~
В	20 2021-01-26 13:10:45.665 fe30::72b6:2405:e423:488d ff02::2 ICMPv6 62 Router Solicitation 21 2021-01-26 13:10:45.865 fe30::72b6:2405:e423:488d ff02::16 ICMPv6 110 Multicast Listener Report Message v2 22 2021-01-26 13:10:45.865 fe30::72b6:2405:e423:488d ff02::16 ICMPv6 110 Multicast Listener Report Message v2	
	23 2021-01-26 13:10:45.866. fc80::aab2:daff;fc3d:aaa0 ff02::11 ICMPv6 110 Router Advertisement from a8:b2:da:5d:aa:a0 34 2021-01-26 13:10:46.364 fc80::7cb6:2405:e423:488d ff02::16 ICMPv6 110 Multicast Listener Report Message v2 35 2021-01-26 13:10:46.364 fc80::7cb6:2405:e423:488d ff02::16 ICMPv6 110 Multicast Listener Report Message v2 44 2021-01-26 13:10:46.864 fc80::7cb6:2405:e423:488d ff02::11 ICMPv6 86 Neighbor Advertisement fc80::7cb6:2405:e423:488d ff02::11	
	45 2021-01-26 13:10:46.864+ re30::72b6:2405:re423:483d ff02::1 ICMPv6 86 Neighbor Advertisement fe80::72b6:2405:e423:483d (14) 46 2021-01-26 13:10:46.864 2001:2f8:103::6052:72b6:2405:e423: ff02::1 ICMPv6 86 Neighbor Advertisement 2001:2f8:103::6052:72b6:2405:e423: 82 47 2021-01-26 13:10:46.864 2001:2f8:103::6052::72b6:2405:e423: ff02::1 ICMPv6 86 Neighbor Advertisement 2001:2f8:103::6052::72b6:240 48 2021-01-26 13:10:46.864 2001:2f8:103::6052::302f:ff06::9058:f ff02::1 ICMPv6 86 Neighbor Advertisement 2001:2f8:103::6052::302f:ff06::9058:f 49 2021-01-26 13:10:46.864 2001:2f8:103::6052::302f:ff06::9058:f ff02::1 ICMPv6 86 Neighbor Advertisement 2001:2f8:103::6052::302f:ff06	
	50 2021-01-26 13:10:46.872. re80::/c06:2405:e423:488d TT02::16 1LMPvb 110 Multicast Listener Report Message v2 51 2021-01-26 13:10:46.872. re80::/c06:2405:e423:488d ff02::16 ICMPvb 110 Multicast Listener Report Message v2 64 2021-01-26 13:10:46.878. re80::/c06:2405:e423:488d ff02::16 ICMPvb 90 Multicast Listener Report Message v2 66 2021-01-26 13:10:46.878. re80::/c06:2405:e423:488d ff02::16 ICMPvb 90 Multicast Listener Report Message v2 66 2021-01-26 13:10:46.878. re80::/c06:2405:e423:488d ff02::16 ICMPvb 90 Multicast Listener Report Message v2 68 2021-01-26 13:10:46.878. re80::/c06:2405:e423:488d ff02::16 ICMPvb 90 Multicast Listener Report Message v2	
	69 2021-01-26 13:10:46.888 fe80::7cb6:2405:e423:488d ff02::16 ICMPv6 90 Multicast Listener Report Message v2 > >	~
	Retrans timer (ms): 0 ////////////////////////////////////	× .
	Length: 4 (32 bytes) Prefix Length: 64 Valid Lifetime: 604800 Valid Lifetime: 604800	
	Reserved Prefix: 2001:2f8:103c:6052:: 0000 33 33 00 00 00 aa b2 da da	~
	0010 00 00 00 38 3a ff fe 80 00 00 00 00 00 aa b2 🖪 8:	7
	● Z Internet Control Message Protocol v6: Protocol プロファイル: Default / パット数: 647・表示: 63 (9.7%) プロファイル: Default	4

図 6.1.6-41 ネットワークトレースの状態(RA 送信セグメント)

20 フレーム目(A)で実証用 PC から近隣のルータ宛にマルチキャストで RS(Router Solicitation)が 発行し、23 フレーム(B)ではルータ(実証用 L3 スイッチ)からマルチキャストで RA(Router Advertisement)が送信されていることを確認した。

ルータから送信された RA のフレームをネットワークトレース結果の詳細情報欄(C)に記載しているが、プレフィックス、デフォルトゲートウェイ、有効期限が通知されていることを確認した。

IPv6 アドレスの自動設定が完了すると、マルチキャストで自動設定した IPv6 アドレス(RA により払い出された IPv6 アドレス、一時 IPv6 アドレス)とリンクローカルアドレスについて NA(Neighbor Advertisement)を44~49 フレーム(D)で送信していることを確認した。

【#3の補足】

#3 では IPv6 アドレスの手動設定を解除し、IPv6 アドレスとデフォルトゲートウェイが自動設定される かどうかの確認を行った。

インターネット プロトコル バージョン 6 (TCP/IPv6)のプロパティ	Х
全般	
ネットワークでこの機能がサポートされている場合は、IPv6 設定を自動的に取得することができます。サポートされていな い場合は、ネットワーク管理者に適切な IPv6 設定を問い合わせてください。	
 IPv6 アドレスを自動的に取得する(Q) 	
○次の IPv6 アドレスを使う(<u>S</u>):	
IPv6 アドレス(D:	
サプネット プレフィックスの長さ(<u>U</u>):	
デフォルト ゲートウェイ(<u>D</u>):	
○ DNS サーバーのアドレスを自動的に取得する(B)	
● 次の DNS サーバーのアドレスを使う(E):	
優先 DNS サーバー(P): 2001:4860:4860::8888	
代替 DNS サーバー(<u>A</u>):	
□終了時に設定を検証する(上) 詳細設定(⊻)	l
OK キャンセル	

図 6.1.6-42 IPv6 アドレス自動構成を行う為の設定

	C ¥WINDOWS¥system32¥cmd.exe	-	\times
	Wireless LAN adapter Wi-Fi:		^
(c	接続固有の DNS サフィックス : 説明. 前理アドレス. : 90-78-41-98-05-3A DHOP 有効 自動構成有効 : Livx : PV6 アドレス. : 2001:2f8:103c:6052:b805:9fa7:7c:f825(優先) -時 IPv6 アドレス. : 2001:2f8:103c:6052:b805:9fa7:7c:f825(優先) リンクローカル IPv6 アドレス. : 1Pv4 アドレス. : 1Pv4 アドレス. : 1Pv4 アドレス. : 1Pv4 アドレス. : 2001:2f8:103c:6052:b805:9fa7:7c:f825(優先) リンクローカル IPv6 アドレス. : 1Pv4 アドレス. : 1Pv4 アドレス. : 1Pv5:b825:955.9 : デフォルト ゲートウェイ : 172:16:52:253 : DHCPv6 IAID : 160462913 : DHCPv6 クライアント DUID. : 00-01-00-01-24-C1-F9-31-4C-36-4E-3E-F6-57 DNS サーバー : 8.8.8 NetBIOS over TCP/IP :		
	イーサネット アダプター Bluetooth ネットワーク接続:		
	メディアの状態メディアは接続されていません 接続固有の DNS サフィックス 説明Bluetooth Device (Personal Area Network) 物理アドレス		
	C:¥Users¥user>_		~

図 6.1.6-43 「ipconfig /all」実行結果(RA 送信セグメント: IPv6 アドレス自動構成)

IPv6 アドレスおよび一時 IPv6 アドレスについては、#33 と同様に自動構成されているが、デフォル トゲートウェイについては RA を発行したルータ(実証用 L3 スイッチ)のリンクローカルアドレスが設 定されていることを確認した。

(2)運用性/保守性(ログ管理、トラブルシュート方式、端末追跡等) IPv6 で通信を行う機器に関して、ログファイルや端末の IPv6 アドレスと MAC アドレスの関連付けについて、 IPv4 実装時との運用的な違いについて実証を行った。

#	接続元 機器名	有線 無線	IPv4 IPv6	接続先機 器名・サー ビス名	IPv4 IPv6	検証内容	想定結果	実施結里
1	実証用 L3スイ ッ チ	有線	-	実証用 L3スイッ チ	IPv4	「show arp」コマンドを実行 し、IPv4 アドレスと MAC アド レスのペアを確認する	以下の情報が記録されてい ることを確認する ・IP Address ・MAC Address ・ARP エントリのインターフェ ース ・送信時に利用される ether ポート番号	OK
2	実 証 用 L3スイ ッチ	有線	-	実証用 L3スイッ チ	IPv6	「show ndp」コマンドを実行 し、IPv6 アドレスと MAC アド レスのペアを確認する	表示結果に以下の情報が記 録されていることを確認する ・IPv6 Address ・MAC Address ・Neighbor Cache エントリの 状態 ・Neighbor Cache エントリの インターフェース ・送信時に利用される ether ポート番号	ОК

② 運用性/保守性における検証

#	接続元	有線	IPv4	接続先機	IPv4	検証内容	想定結果	実
	機器名	無線	IPv6	器名・サー	IPv6			施
				ビス名				結
								果
3	実証用	有線	-	ログ管理	IPv4	ログ管理サーバに SSH でロ	実証用 IPv6 アドレス	ок
	FW 装			サーバ	/IPv6	グインし、実証用 FW 装置か	(XXXX:YYY:.*)で grep し、以	
	置					らのログ転送先に生成され	下の情報が記録されている	
						たセッションログを確認する	ことを確認する	
							・日付・時刻	
							・送信元・送信先 IPv6 アドレ	
							ス(※)	
							・使用したインターフェース名	
							・アクセス許可ルールの番号	
							・通信の記録(pass/drop)	
							(※)送信元•送信先 IPv6 ア	
							ドレスについては以下の観	
							点で確認する	
							・グローバルアドレス(実ア	
							ドレス)	
							・グローバルアドレス(匿名/	
							一時)	
							・リンクローカルアドレス	

【#1,#2 の補足】

#1 ではルータ(実証用 L3 スイッチ)側で arp テーブルを確認することにより、ルータ経由で接続を 行った機器の IP アドレス、MAC アドレス他の確認を行った。



以上のように、隣接機器やルータ経由で接続を行った機器の IP アドレス、MAC アドレスに加えて、 接続インターフェース名(VLAN 名)、接続先ポート番号を確認した。

IPv4 ではデータリンク層のアドレス(MAC アドレス)を解決するために、ARP ブロードキャストにより アドレスを解決していたが、IPv6 では Neighbor Discovery (ND)機能を使用しアドレスを解決してい る。IPv4 での「show arp」コマンドに対応する IPv6 でのコマンドとして「show ndp」コマンドで確認し た※。

#	s	hov	v n	db
	~			

IPv6 Address	MAC Address	S F	Rest	Interface	Port
2001:2f8:103c:6050::1	a8:b2:da:5d:aa:a0		perm	lan50	
2001:2f8:103c:6050::2	00:80:17:ef:6d:43	R	00010	lan50	1
2001:2f8:103c:6051::1	a8∶b2∶da∶5d∶aa∶a0	RΡ	perm	lan51	
2001:2f8:103c:6052::1	a8∶b2∶da∶5d∶aa∶a0	RΡ	perm	lan52	
2001:2f8:103c:6052:3960:5cb5:a585:b6f3	90:1b:0e:8b:ba:a2	S	00721	lan52	19
fe80::280:17ff:feef:6d43%lan50	00:80:17:ef:6d:43	S	01179	lan50	1
fe80::aab2:daff:fe5d:aaa0%lan50	a8∶b2∶da∶5d∶aa∶a0	RΡ	perm	lan50	
fe80::aab2:daff:fe5d:aaa0%lan51	a8:t		e.	lan51	
fe80::aab2:daff:fe5d:aaa0%lan52	a8:1 接続インターフ:	r−ス名	erm	lan52	ч
Entry:9				括	続先ポート

図 6.1.6-45 ルータ(実証用L3スイッチ)での Neighbor Discovery テーブルの確認結果

確認結果については、IPv4 アドレスが IPv6 アドレスに置き換えられたイメージとなる。

※Windows が搭載されている PC/サーバでは、「netsh interface ipv6 show neighbors」コマンドで Neighbor Discovery(ND)テーブルの確認が可能である。

【#2 の補足】

#2 では実証用 FW 装置からログ管理サーバに転送されたセッションログを IPv6 アドレスで絞り込ん で表示させることで、接続許可・拒否された端末の情報を確認した。

ログ管理サーバでは実証用 FW 装置ら転送されたログファイルが所定の形式で格納されている(対象:アカウントログ、メッセージログ、セッションログ、エラーログ)

[root@sv17 fw01]# is command-fwlog-20210105 command-fwlog-20210106 command-fwlog-20210107 command-fwlog-20210102 command-fwlog-20210112 command-fwlog-20210127 command-fwlog-20210216 error-fwlog-20170615 error-fwlog-20170615 error-fwlog-20170619 error-fwlog-20170713 error-fwlog-20170717 message-fwlog-20171109 message-fwlog-20171109 message-fwlog-20171113 message-fwlog-20171113	$\begin{array}{l} message-fwlog-20181205\\ message-fwlog-20181206\\ message-fwlog-20181208\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-20181221\\ message-fwlog-20181221\\ message-fwlog-20181221\\ message-fwlog-20181221\\ message-fwlog-20181221\\ message-fwlog-20181221\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018121\\ message-fwlog-2018113\\ message-fwlog-20191113\\ message-fwlog-20191113\\ message-fwlog-20191113\\ message-fwlog-20191114\\ \end{array}$	message-fwlog-20200704 message-fwlog-20200706 message-fwlog-20200707 message-fwlog-20200709 message-fwlog-20200719 message-fwlog-20200713 message-fwlog-20200713 message-fwlog-20200715 message-fwlog-20200716 message-fwlog-20200716 message-fwlog-20200716 message-fwlog-20200716 message-fwlog-20200716 message-fwlog-20200716 message-fwlog-20200716 message-fwlog-20200716 message-fwlog-20200718 message-fwlog-20170719.gz	session-fwlog-20180128, gz session-fwlog-20180129, gz session-fwlog-20180130, gz session-fwlog-20180130, gz session-fwlog-20180201, gz session-fwlog-20180202, gz session-fwlog-20180204, gz session-fwlog-20180206, gz session-fwlog-20180207, gz FW 装置のセッン	session-fwlog-20190326, gz session-fwlog-20190327, gz session-fwlog-20190328, gz session-fwlog-20190328, gz session-fwlog-2019031, gz session-fwlog-2019031, gz session-fwlog-20190401, gz session-fwlog-20190402, gz session-fwlog-20190404, gz session-fwlog-20190405, gz y ヨンログ , gz session-fwlog-20190405, gz session-fwlog-20190405, gz session-fwlog-20190405, gz	$\begin{array}{c} session-fw \log -2020052 \\ session-fw \log -20201010 \\ session-fw \log -2021010 \\ session-fw \log -202100 \\ session-fw \log -202100 \\ session-fw \log -202100 \\ session-fw \log -202100 \\ session-fw \log -202000 \\ session-fw \log -20000 \\ sessi$
message-fwlog-20171119 message-fwlog-20171121 message-fwlog-20171122 message-fwlog-20171127 message-fwlog-20171127 message-fwlog-20171120 message-fwlog-20171201 message-fwlog-20171203 message-fwlog-20171204 message-fwlog-20171204 message-fwlog-20171207 message-fwlog-20171208 message-fwlog-20171208 message-fwlog-20171208 message-fwlog-20171208 message-fwlog-20171208 message-fwlog-20171208 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-20171218 message-fwlog-201712218 message-fwlog-20171228 message-fwlog-20171228 message-fwlog-20171228 message-fwlog-20171228 message-fwlog-20171228 message-fwlog-20171228 message-fwlog-20171228 message-fwlog-20171280 message-fwlog-20180104 message-fwlog-20180104 message-fwlog-20180119 message-fwlog-20180119 message-fwlog-20180119 message-fwlog-20180119 message-fwlog-20180119	$\begin{split} message-fwl og-20191115\\ message-fwl og-20191118\\ message-fwl og-20191121\\ message-fwl og-20191121\\ message-fwl og-20191125\\ message-fwl og-20191125\\ message-fwl og-20191125\\ message-fwl og-20191125\\ message-fwl og-20191126\\ message-fwl og-2019120\\ message-fwl og-2019121\\ message-fwl og-2019122\\ message-fwl og-20$	session-fwlog-20170720. gz session-fwlog-20170721. gz session-fwlog-20170721. gz session-fwlog-20170722. gz session-fwlog-20170724. gz session-fwlog-20170725. gz session-fwlog-20170726. gz session-fwlog-20170726. gz session-fwlog-20170727. gz session-fwlog-20170730. gz session-fwlog-20170731. gz session-fwlog-20170801. gz session-fwlog-20170803. gz session-fwlog-20170805. gz session-fwlog-20170813. gz session-fwlog-20170813. gz session-fwlog-20170813. gz session-fwlog-20170813. gz session-fwlog-20170815. gz session-fwlog-20170815. gz session-fwlog-20170825. gz session-fwlog-20170822. gz session-fwlog-20170822. gz session-fwlog-20170822. gz session-fwlog-20170822. gz session-fwlog-20170822. gz session-fwlog-20170822. gz session-fwlog-20170822. gz session-fwlog-20170822. gz session-fwlog-20170825. gz session-fwlog-20170824. gz session-fwlog-20170824. gz	$session-fw \log -20180915. gz session-fw \log -20180916. gz session-fw \log -20180919. gz session-fw \log -20180919. gz session-fw \log -20180921. gz session-fw \log -20180921. gz session-fw \log -20180922. gz session-fw \log -20180924. gz session-fw \log -20180925. gz session-fw \log -20180926. gz session-fw \log -20180926. gz session-fw \log -20180926. gz session-fw \log -20180927. gz session-fw \log -20180092. gz session-fw \log -20181001. gz session-fw \log -20181005. gz session-fw \log -20181005. gz session-fw \log -20181017. gz session-fw \log -20181011. gz session-fw \log -20181012. gz session-fw \log -20181020. gz session-fw \log -20181$	$session-fw \log_2 20191111, gz session-fw \log_2 20191112, gz session-fw \log_2 20191113, gz session-fw \log_2 20191113, gz session-fw \log_2 20191116, gz session-fw \log_2 20191116, gz session-fw \log_2 20191118, gz session-fw \log_2 20191120, gz session-fw \log_2 20191122, gz session-fw \log_2 20191122, gz session-fw \log_2 20191124, gz session-fw \log_2 20191126, gz session-fw \log_2 20191126, gz session-fw \log_2 20191126, gz session-fw \log_2 20191126, gz session-fw \log_2 20191204, gz session-fw \log_2 20191214, gz session-fw \log_2 20191216, gz $	session-fwlog-20210106 session-fwlog-20210107 session-fwlog-20210107 session-fwlog-2021010 session-fwlog-20210110 session-fwlog-20210113 session-fwlog-20210113 session-fwlog-20210113 session-fwlog-20210115 session-fwlog-20210115 session-fwlog-20210115 session-fwlog-20210117 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-20210120 session-fwlog-2021020 session-fwlog-2021020 session-fwlog-20210203 session-fwlog-20210203 session-fwlog-20210205

図 6.1.6-46 ログ管理サーバに格納されている実証用 FW 装置のログ

セッションログを例に説明すると、「session-fwlog-」で始まるファイル名の後ろに日付情報が付与されたファイル名となっている。

セッションログには実証用 FW 装置で記録対象となっているファイアウォールルールがすべて記録 されているため、grep コマンドなどを使用して IPv6 アドレスや日時で絞り込んで確認する。 ファイアウォールルールによって通過許可した場合と破棄された場合の記録形式について、実例 を用いて説明する

Feb 16 15:52:39 **fw01/**fw02 IPCOMEX2-3200_SC: firewall: WARNING[40300011]: TCP connectiondenied.src=:6052::2002dst=2404:6800:4008:C00::BCproto=tcpsrcport=49830dstport=5228 interface=vlan50 dir=inbound action=drop reason=filter rule=59999

図 6.1.6-47 ファイアウォールルールで破棄された場合のログ

上記メッセージより「TCP connection denied」で始まるメッセージテキストが記録され、以降、以下の 情報が出力される。

・src:転送元 IPv4/IPv6 アドレス

- ・dst:転送先 IPv4/IPv6 アドレス
- ・proto:プロトコル情報(tcp/udpなど)
- ・srcport:転送元ポート番号
- ・dstport:転送先ポート番号
- ・interface:使用したインターフェース名
- •dir:通信方向(inbound/outbound)
- •action:破棄(drop)
- •rule:フィルタルールの番号

本事例では、実証用PCからGoogle社のサイトにアクセスした際、実証用 FW 装置の実証用ネット ワークインターフェース(vlan50)で 5228/tcp(Google Playstore)からの応答を拒否し、パケットを破 棄したケースとなる。 次に実証用 FW 装置のルールにより通過許可を行った場合の実例を説明する。

Feb 16 15:56:11 **fw01/**fw02 IPCOMEX2-3200_SC: firewall: INFO[00300003]: UDP sessioninitiated. src=:6052:CC33:5D4C:9EAC:EC9D dst=2001:4860:4860::8888 proto=udpsrcport=55920 dstport=53 interface=vlan50 dir=inbound action=accept rule=300

図 6.1.6-48 ファイアウォールルールで通過許可された場合のログ

上記メッセージより「TCP connection initiated(terminated)」で始まるメッセージテキストが記録され、 以降、以下の情報が出力される。

・src:転送元 IPv4/IPv6 アドレス

- ・dst:転送先 IPv4/IPv6 アドレス
- ・proto:プロトコル情報(tcp/udp など)
- ・srcport:転送元ポート番号
- ・dstport:転送先ポート番号
- ・interface:使用したインターフェース名
- •dir:通信方向(inbound/outbound)
- •action:破棄(drop)
- ・rule:フィルタルールの番号

本事例では、実証用 PC から Google 社のパブリック DNS サーバに対して名前解決を行った際、実証用 FW 装置の実証用ネットワークインタフェース(vlan50)で 53/udp(dns)からの応答を許可し、パケットを通過させたケースとなる。

尚、図 6.1.6-48 に記録された実証端末の IPv6 アドレスについて補足説明がある。記録されている IPv6 ア ドレスが固定 IPv6 アドレスでないことを結果より確認した。Windows が搭載されている機種については、IPv6 自動構成が有効になっている。この場合、ルータから RA による IPv6 アドレス自動構成を行った場合、ランダ ム アドレスと、匿名アドレスの両方が自動構成される。クライアント PC からのアウトバウンド通信をする際は、 送信元 IPv6 アドレスに一時(匿名)アドレスを使用する仕様のため、ランダムな IPv6 アドレスが記録されたも のと考える。 6.1.6.2 課題と対応

本検証にて発生した課題を整理した結果、機器やサービスが仕様により IPv6 に対応していない課題、IPv6 対応 を進める中で考慮不足が起因して発生した課題(構築時の Tips)に分かれることを確認した。

そのため、以下に示す2つの観点から本検証にて発生した課題と対応の事例を「【付録1】課題管理表:大学A」 に示す。

- (1) 機器/サービス仕様における課題 本検証において導入しようとした IPv6 対応を謳う機器/サービスの内、本検証では、IPv6 の利用可否が確認で きず、機器メーカのサポート等に確認した結果、IPv6 対応が十分でないことが判明した課題と対応の事例を示 す。
- (2) IPv6 対応における留意事項(構築時の Tips) 本検証において実際に発生した IPv6 関連のトラブルシュート事例をもとに、IPv6 対応において普遍的に留意 すべき点を示す。