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。

① 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。

6.1.2 要件定義

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。

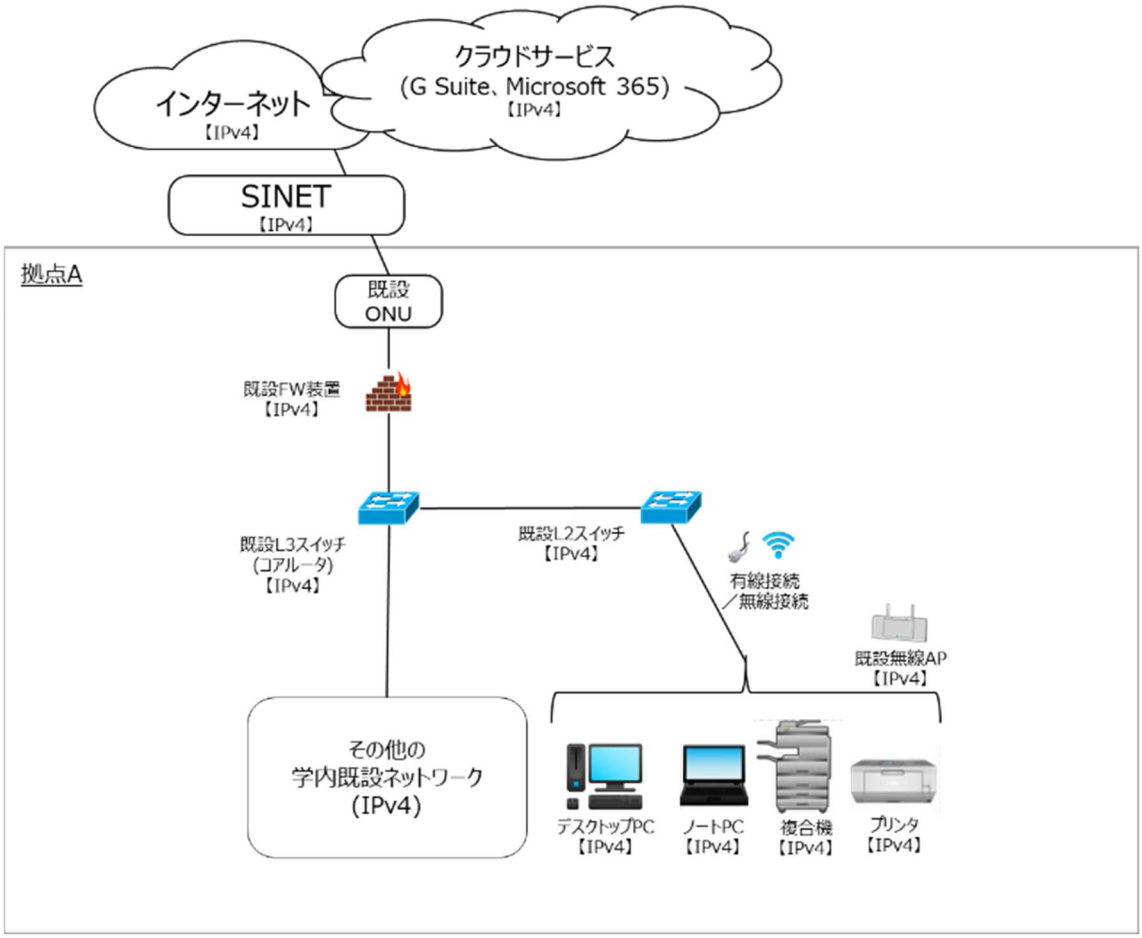


図 6.1.2-1 ネットワーク構成図イメージ

(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。

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	IPv6 対応状況確認	導入方針
新規	実証用 FW 装置	Fujitsu	IPCOM EX1300 SC	○	IPv6 対応	新規
新規	実証用 L3 スイッチ	Fujitsu	SR-S732TR1	○	IPv6 対応	新規
既存	既設 L3 スイッチ(コアルータ)	Fujitsu	SR-S732TR1	○	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	○	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	○	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	○	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	○	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	○	IPv6 対応	新規
既存	複合機	Fuji Xerox	Center-V C5575 T2	○	IPv6 対応	変更要
既存	プリンタ	EPSON	LP-S7160	-	対象外	変更不要

既存/新規	機器等	機器メーカ等	機器名等	移行対象	IPv6 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)	○	IPv6 対応	変更要
既存	G Suite	Gmail	Gmail	○	IPv6 対応	変更不要
既存	Microsoft 365	Exchange Online	Exchange Online	○	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。

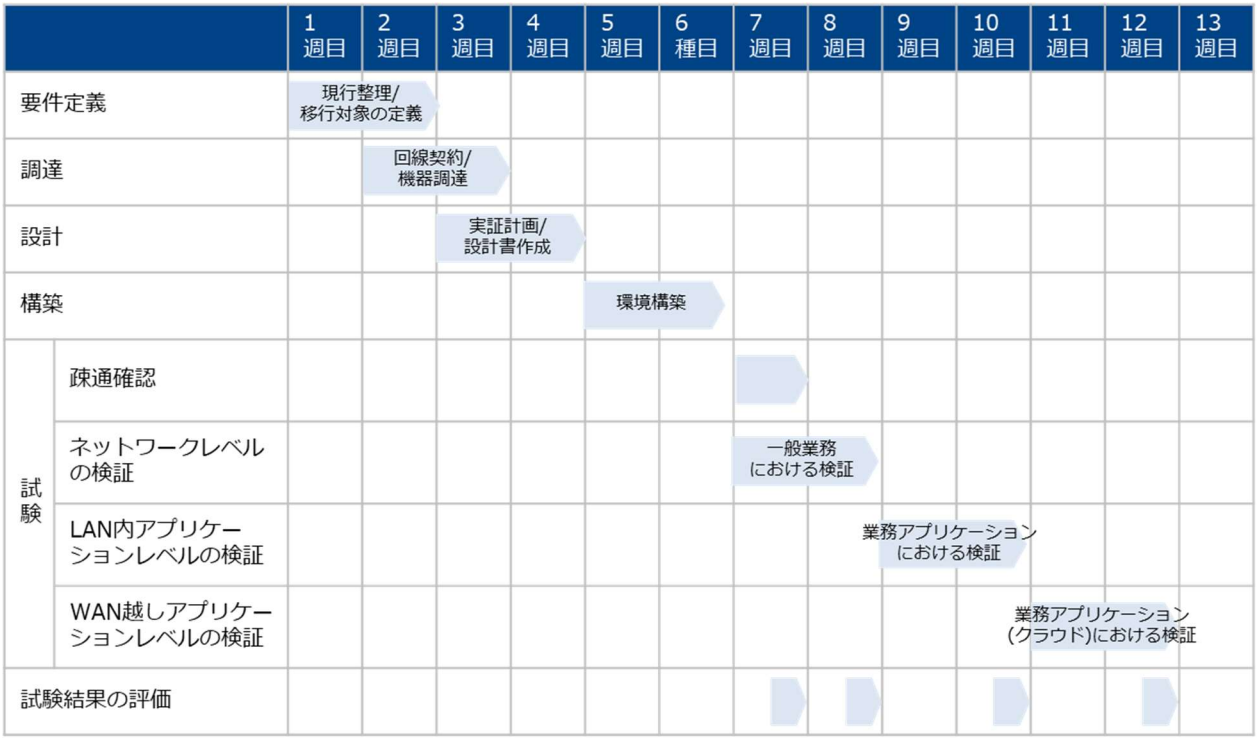


図 6.1.3-1 スケジュールイメージ(大学 A)

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 DHCPv6[65]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

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。

② 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

① 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

① 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。

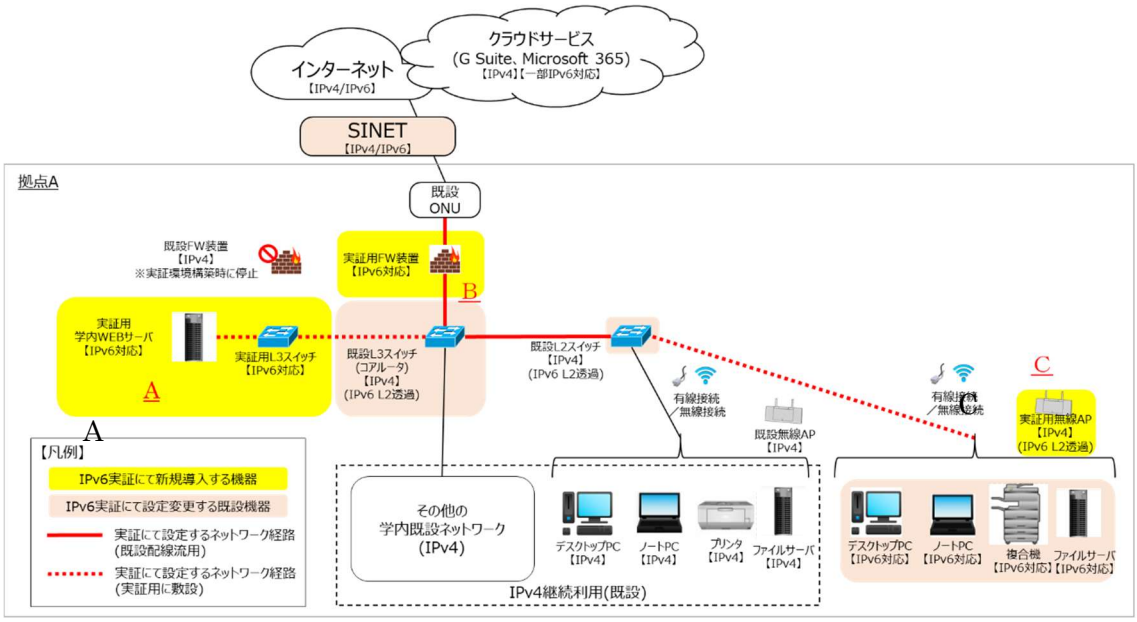


図 6.1.4-1 IPv6 対応後の A 大学のシステム構成図

【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。

つぎに、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。

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

設定	機器等	仕様例	備考
IPv4/ IPv6	実証用ファイルサーバ	Buffalo TeraStation/Windows Server IoT 2019 for Storage Workgroup(WS5220DN02W9)	・ファイルサーバ
IPv4/ IPv6	実証用学内 WEB サーバ	機種:仮想基盤上の仮想マシン OS:Windows Server 2016 Std CPU:仮想 CPU ×2 メモリ:8GB 仮想ディスク:100GB	・学内ポータルサイト用 WEB サービス
IPv4/ IPv6	実証用 FW 装置	Fujitsu IPCOM EX2-3200SC	・ルーティング ・ファイアウォール(FW)
IPv4/ IPv6	実証用 L3 スイッチ	Fujitsu SR-S732TR1	・ルーティング ・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 Fujitsu SR-S318TL3	・スイッチング
IPv4 (L2 透過)	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
IPv4 (L2 透過)	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
IPv4/ IPv6	SINET	インターネット接続(IPv4/IPv6 Dual) FW 装置から SINET までの接続速度は 1Gbps の専用回線	・インターネット接続
IPv4/ IPv6	G Suite	Gmail	・メール
IPv4/ IPv6	Microsoft 365	Exchange Online	・メール

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 [illegible]: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 [illegible] ipv6 route [illegible]:6051::/64 [illegible] ipv6 route [illegible]:6052::/64 [illegible]

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 !

項番	設定内容の詳細
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 通過設定 class-map match-all fil-from-huad-to-IPv4T 　　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 !
6-4	【パケットフィルタリング　リソース定義】EPSON プリンタ→実証用 NW 通過設定 class-map match-all fil-from-local-port-snmp-IPv4T 　　match class-map net-internal 　　match destination-address ipv4 172.16.19.163 　　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 ipv6 [redacted],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 ipv6 [redacted]:6050::/64 　　match source-address ipv6 [redacted]:6051::/64 　　match source-address ipv6 [redacted]: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	【実証用ネットワーク(ルーティング用:VLAN050) アドレス設定】 lan 50 ip address 172.16.50.253/24 3 lan 50 ip route 0 default 172.16.50.254 1 1 lan 50 ip6 use on lan 50 ip6 address 0 1:2f8:1 :6050::1/64 lan 50 ip6 route 0 default 1:2f8:1 :6050::2 1 1 lan 50 vlan 50 <<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
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 1,3-6,8,10-11,14-15,18-19,51,180-190 SR-S352TR1 向け VLAN51 追加 ether 8 vlan tag 1,3-6,8,10-11,14-15,18-19,51,180-190 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 1,3-6,8,10-11,14-15,18-19,51,180-190 既設 L3 向け VLAN 51 を追加 ether 26 vlan tag 1,3-6,8,10-11,14-15,18-19,51,180-190 既設 L3 向け VLAN 51 を追加 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）

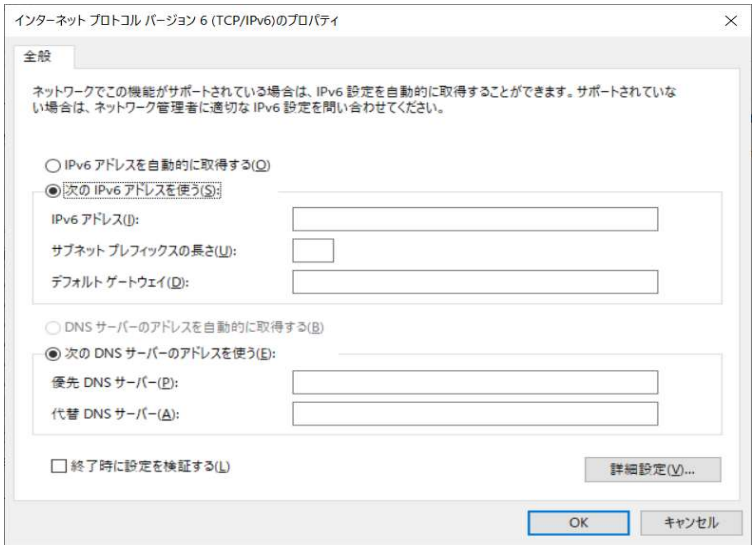
項番	設定内容の詳細
6	【IPv6 アドレスの手動設定】 ・親メニューに戻り、[TCP/IP− ネットワーク設定]を選び、[確認/変更]を押す ・[IPv6 − アドレス手動設定]を選択し、[確認/変更]を押す ・手動設定を「しない」→「する」に変更する ・「DHCP からアドレスを取得」のチェックを外す ・「手動設定アドレス」に複合機に割り当てる IPv6 アドレスを入力する。プレフィクス長は「64」を指定する ・「ゲートウェイアドレス」に実証環境のゲートウェイアドレス(IPv6)を入力する

(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

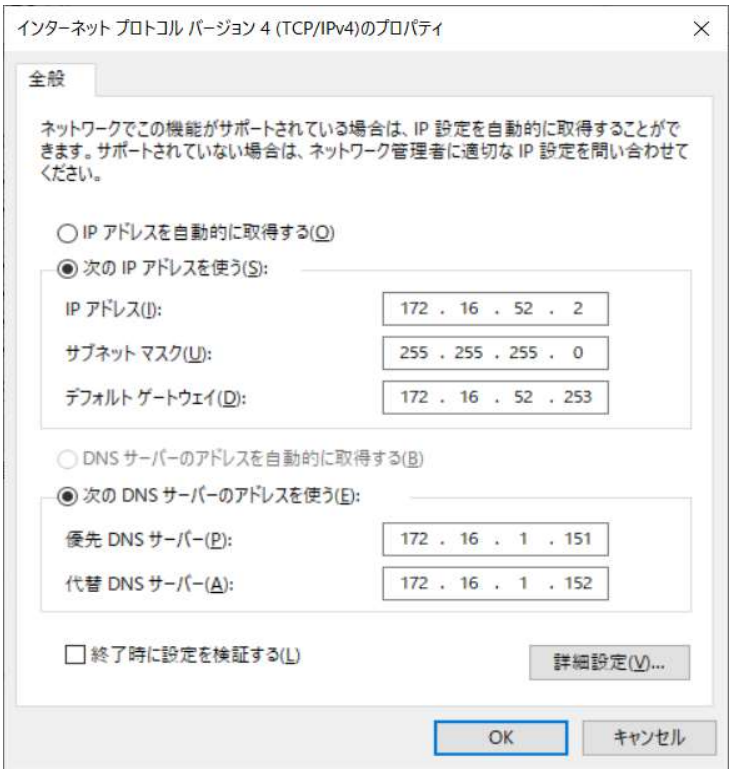
ファイルサーバ上で下記の設定を行い、IPv6 デュアルスタックに対応するファイルサーバを構築する。ファイルサーバのオペレーティングシステムが「Windows Server IoT 2019 for Storage」のため、設定方法は Windows サーバに準じる。 IPv6 実証環境ネットワークとの接続は別の LAN ポートに接続して実施する。

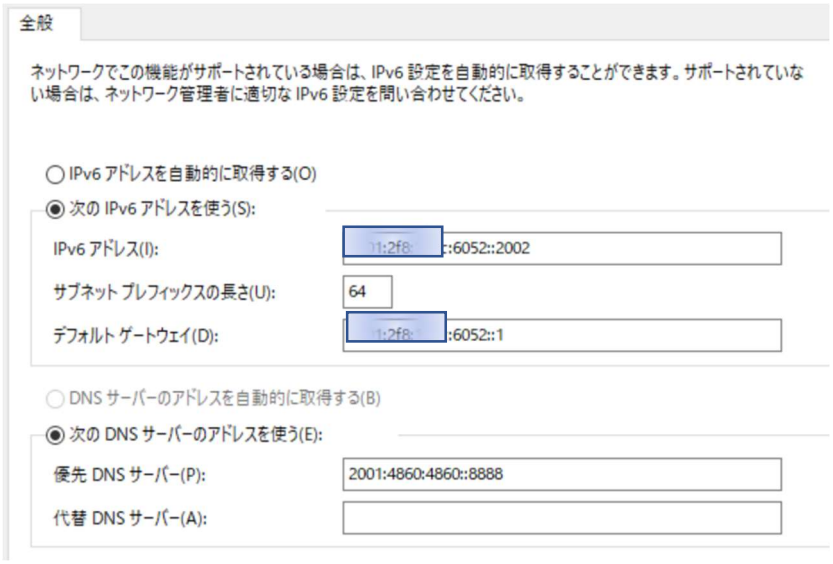
項番	設定内容の詳細
1	【IPv4 アドレスの設定】 既存ネットワークに接続したまま実施するため、変更しない
2	【IPv6 アドレスの設定】 IPv6 実証環境ネットワークと接続しているネットワークアダプタ(LAN)のプロパティを開き、IPv6 アドレスを手動で設定する 

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） 1:2F8:1(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。

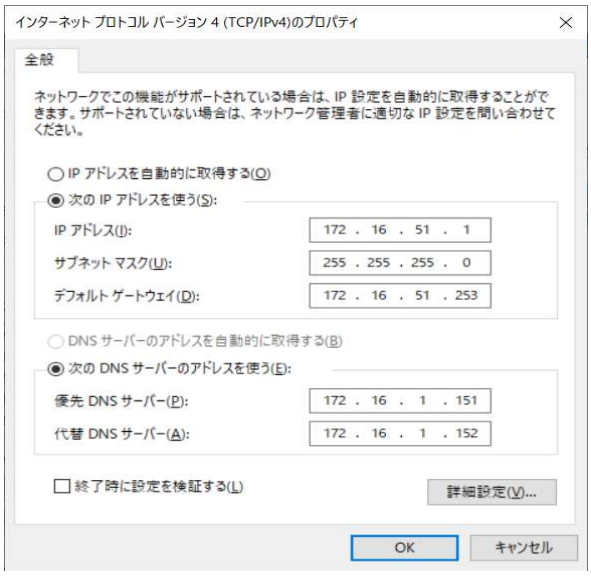
項番	設定内容の詳細
1	【IPv4 アドレスの設定】 接続しているネットワーク アダプタ（LAN or Wi-Fi）のプロパティから固定 IP を設定する。  ※IP アドレスは学内で管理している固定アドレスを設定する。 学外接続の検証を行う場合、優先 DNS サーバおよび代替 DNS サーバについては、パブリック DNS の IP アドレスを設定する（有線：8.8.8.8 代替：8.8.4.4）

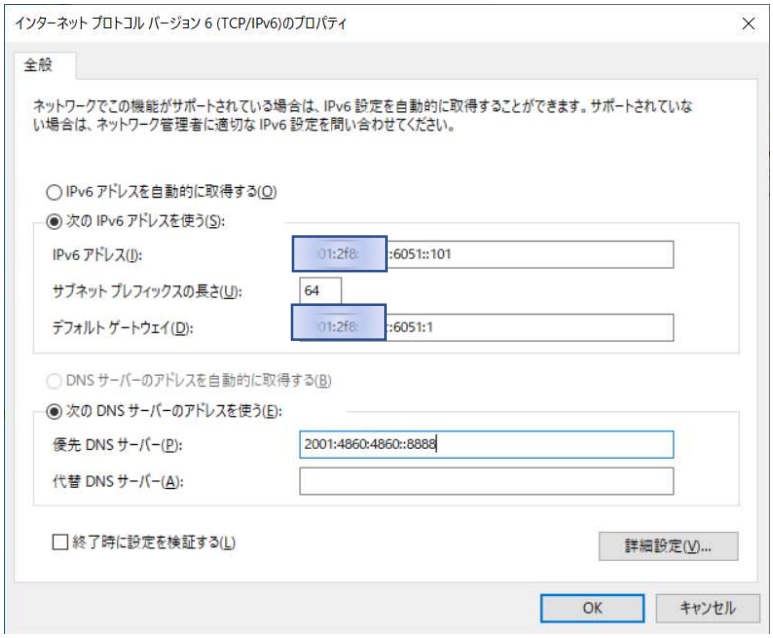
項番	設定内容の詳細
2	【IPv6 アドレスの設定】 接続しているネットワークアダプタ(LAN or wife)のプロパティから静的 IP が設定されるようにする。  ※学内向け検証を行う場合、優先 DNS サーバに設定しているパブリック DNS の IPv6 アドレスを消去する
3	【Hosts の設定追加】 Hosts ファイルに IPv6 の実証環境で利用するサーバのアドレスを追加する ¥Windows¥System32¥drivers¥etc¥hosts ===== ## IPv6 :6051::101 hunet-ipv6 :6052::1002 filesv-ipv6 ## IPv4 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 互換) 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 (既定値)→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 ESXi サーバは2台構成のため、二台とも設定を行う
3	【ゲスト OS 環境の構築】 VMware vSphere 上でゲスト OS（Windows Server）を構成する。 実証用学内 WEB サーバについては、既設の学内 WEB サーバを複製（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。  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。  ※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。

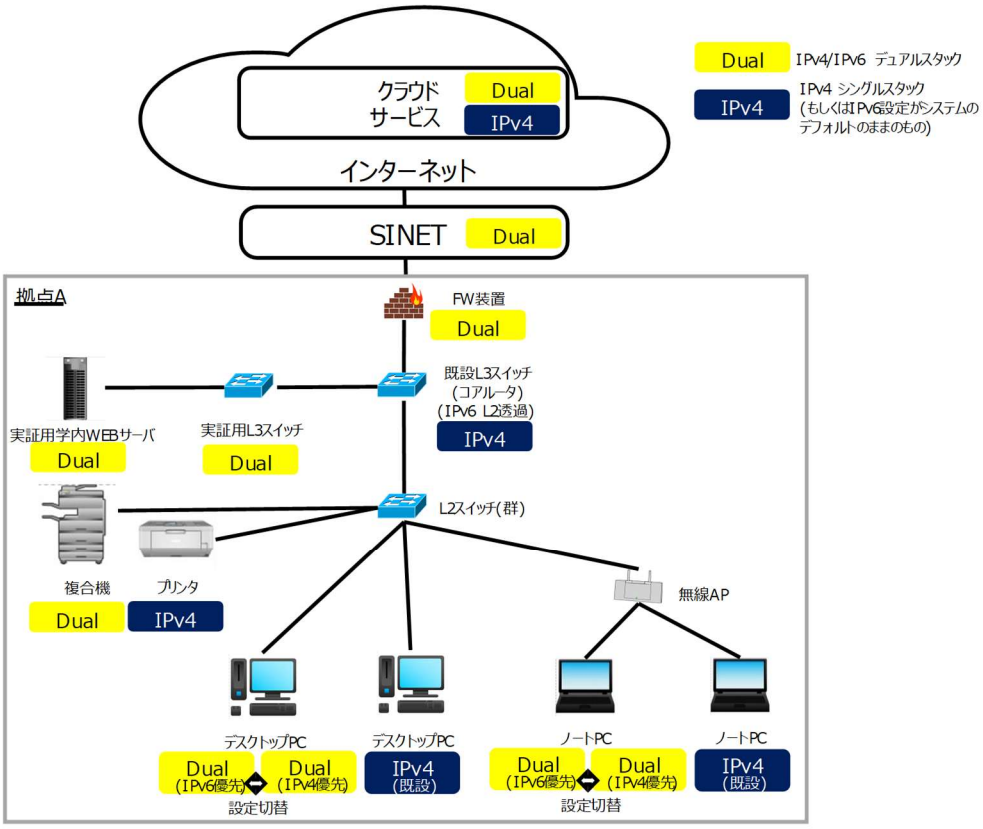


図 6.1.6-1 一般業務検証における接続イメージ

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。

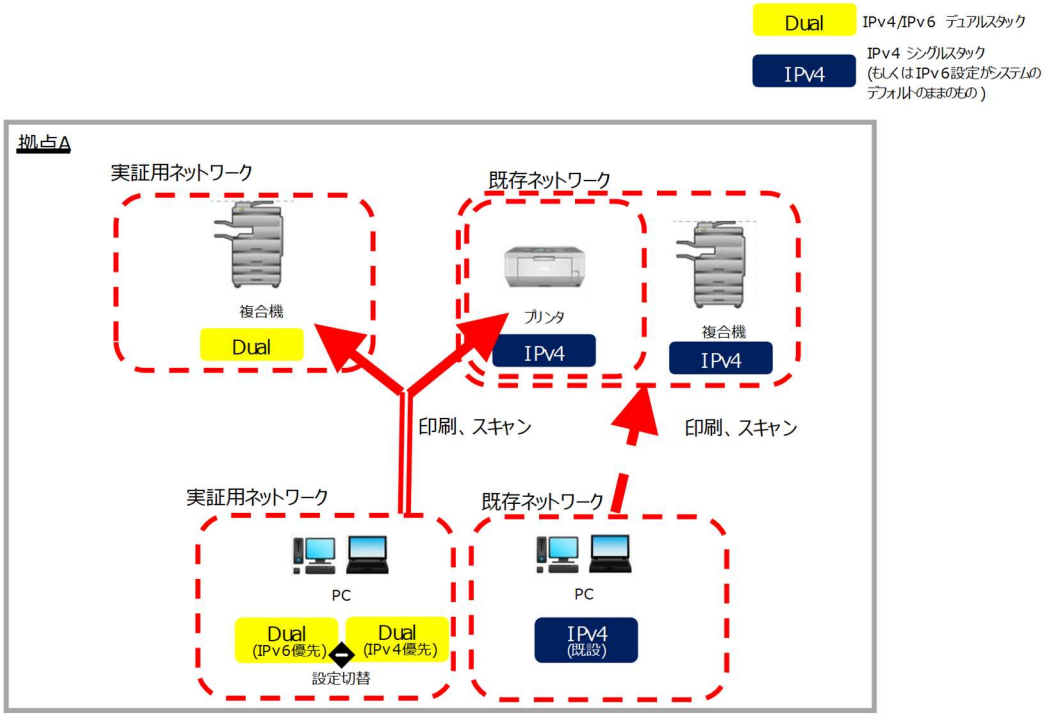


図 6.1.6-2 通常業務を想定した学内ネットワーク機器利用イメージ

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	実施結果
1	ノートPC	無線	IPv6優先	GW ルータ	IPv6	接続先に対し ping -6 をする	ping が通る	OK
2	ノートPC	無線	IPv6優先	外部 WEB サービス	IPv6	https:// kiriwake.jpne.co.jp/ へアクセスする	「IPv4/IPv6 接続判定ページ～」の後に「IPv6 でアクセス中です。」と IPv6 アドレスが表示される	OK
3	ノートPC	無線	IPv6優先	ファイルサーバ	IPv6	接続先に対し ping -6 をする（ping はホスト名で指定）	ping が通る	OK

【#1 の補足】

IPv6 で ping の応答を受信できることを確認した。

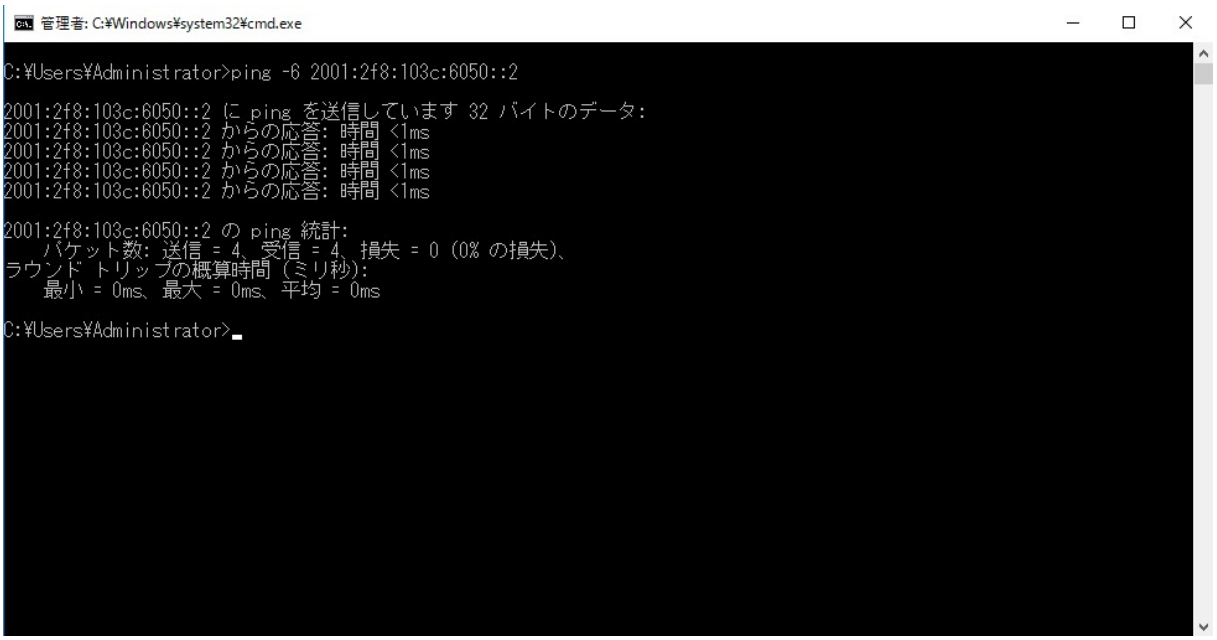


図 6.1.6-3 IPv6 で ping 応答あり

【#2 の補足】

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)

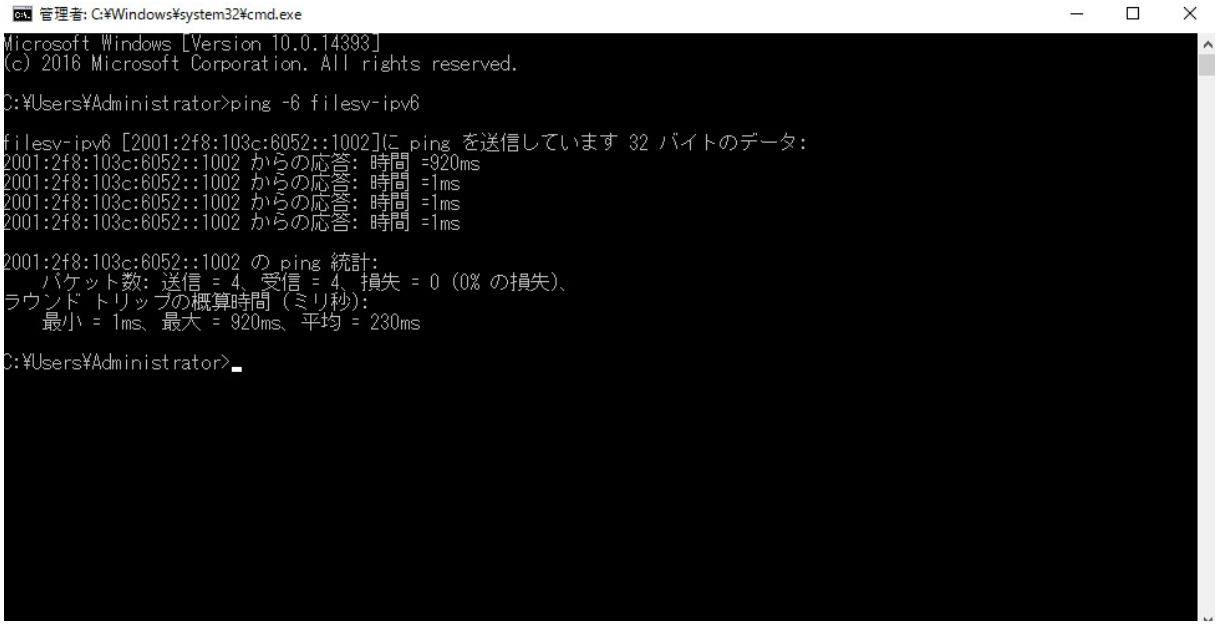


図 6.1.6-5 ホスト名でも ping 応答あり

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	実施結果
1	ノート PC	無線	IPv6 優先	インターネット（IPv6 対応サイト）	IPv6	WEB ブラウザで google へアクセスする	google 画面が表示される	OK
2	ノート PC	無線	IPv6 優先	インターネット（IPv6 未対応サイト）	IPv4	WEB ブラウザで yahoo.co.jp サイトへアクセスする	yahoo.co.jp 画面が表示される	OK
3	ノート PC	無線	IPv4 優先	インターネット(一般)	IPv4	WEB ブラウザで google へアクセスする	google 画面が表示される	OK

【#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。

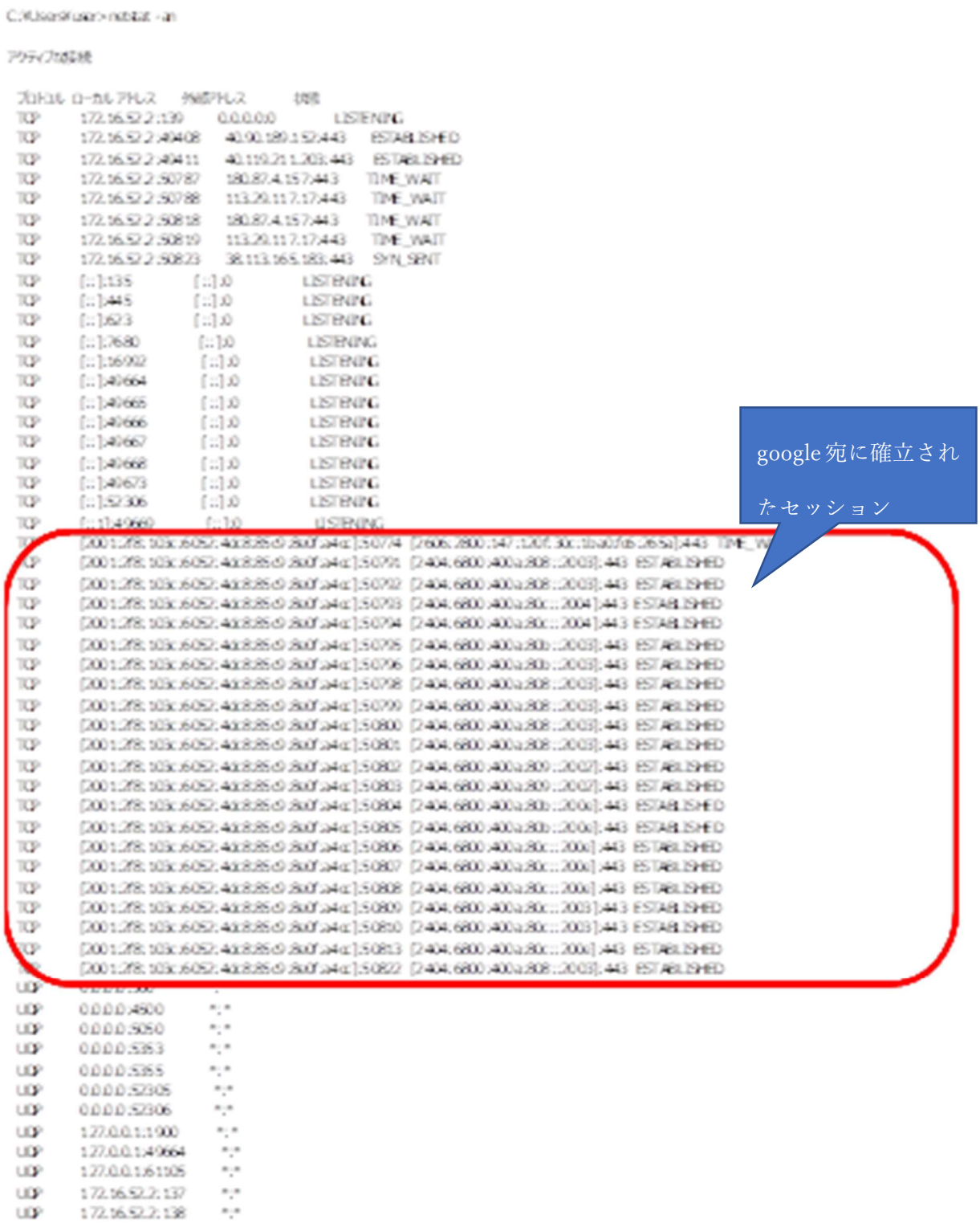


図 6.1.6-6 IPv6 優先接続端末で WEB アクセス時の「netstat -an」の実行結果

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。

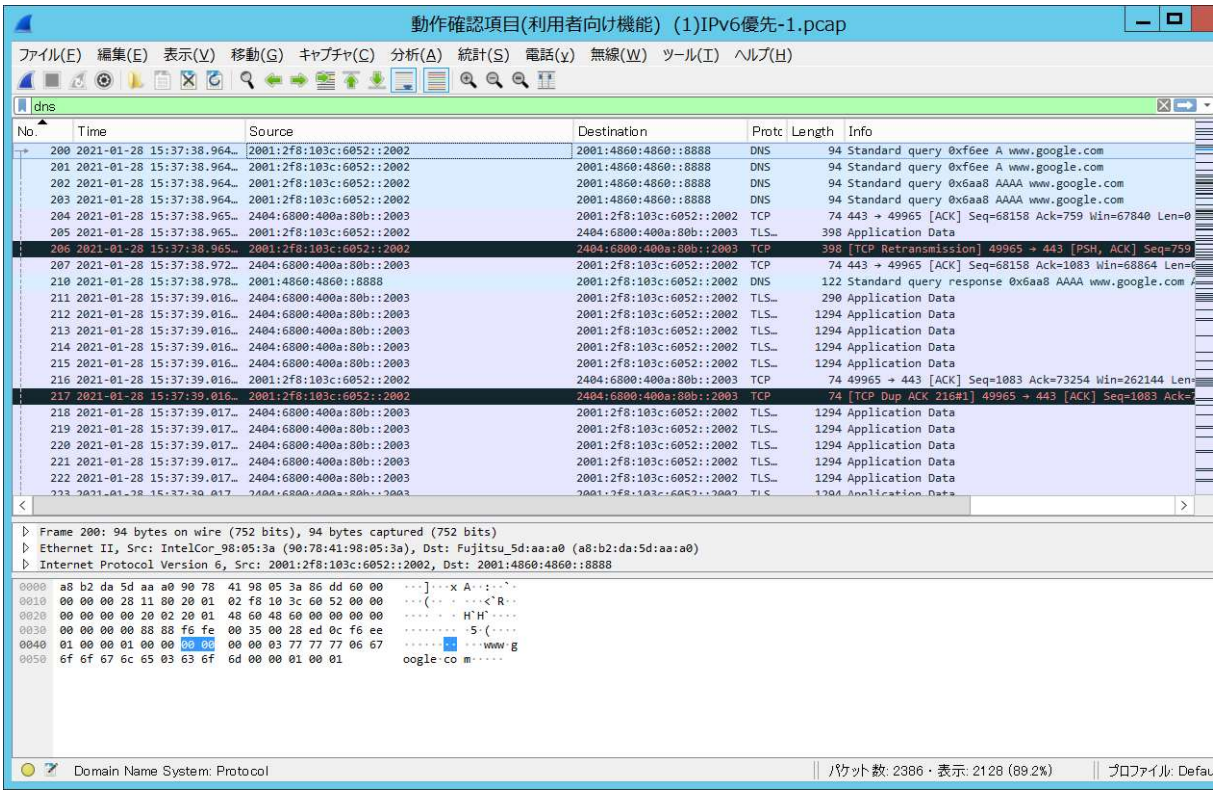


図 6.1.6-7 IPv6 優先接続端末で WEB アクセス時のネットワークキャプチャ結果

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。

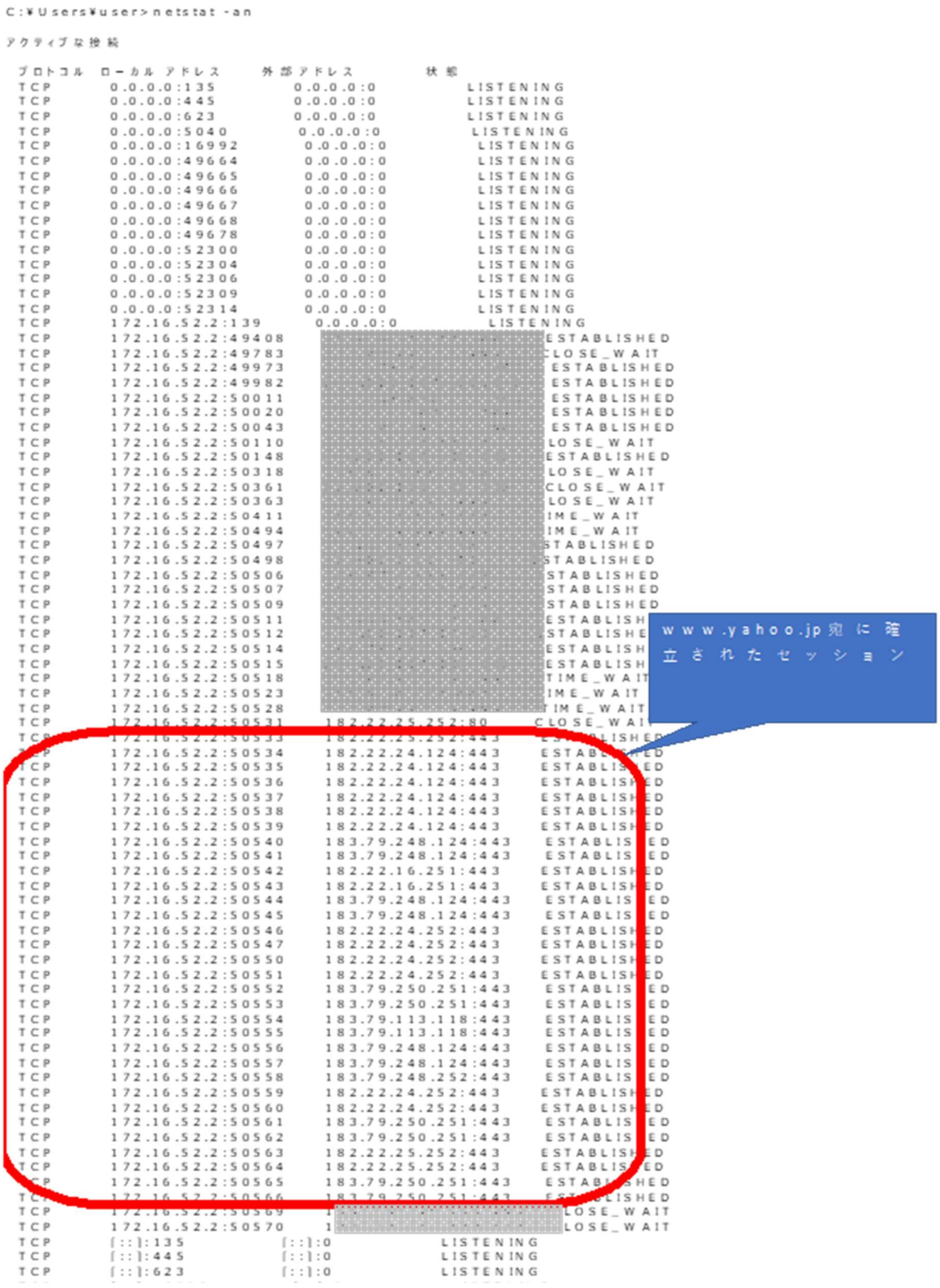


図 6.1.6-8 IPv6 未対応サイトを WEB アクセス時の「netstat -an」の実行結果

検証用PCで接続確認を行った際の 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。

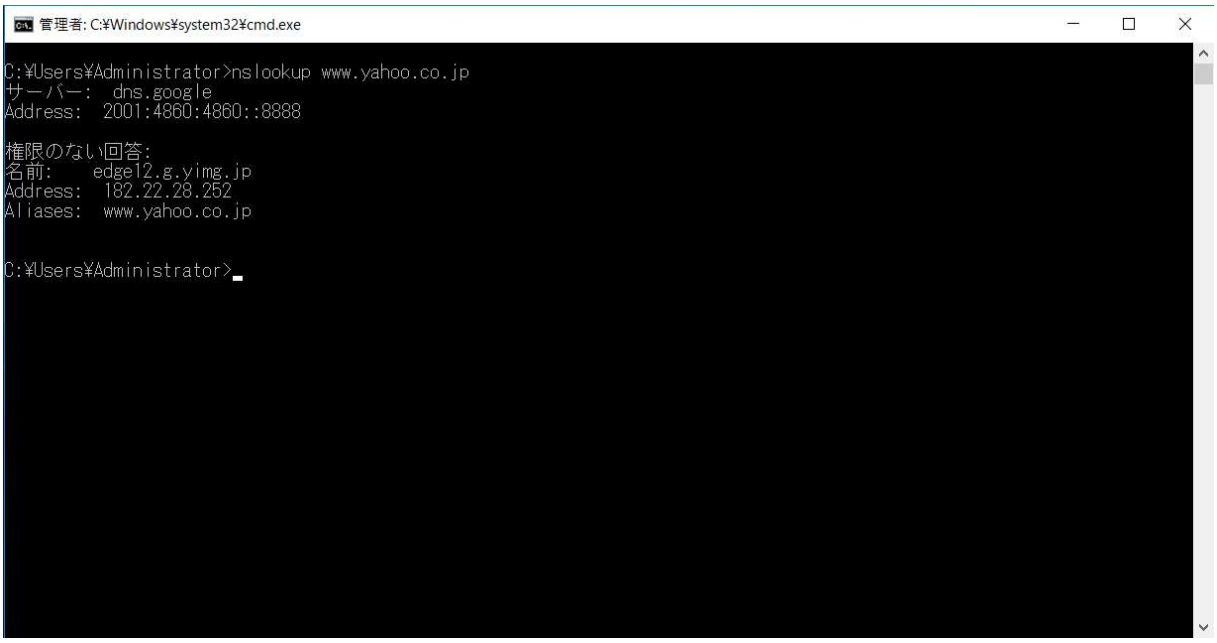


図 6.1.6-9 IPv6 未対応サイトの nslookup コマンド実行結果

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。

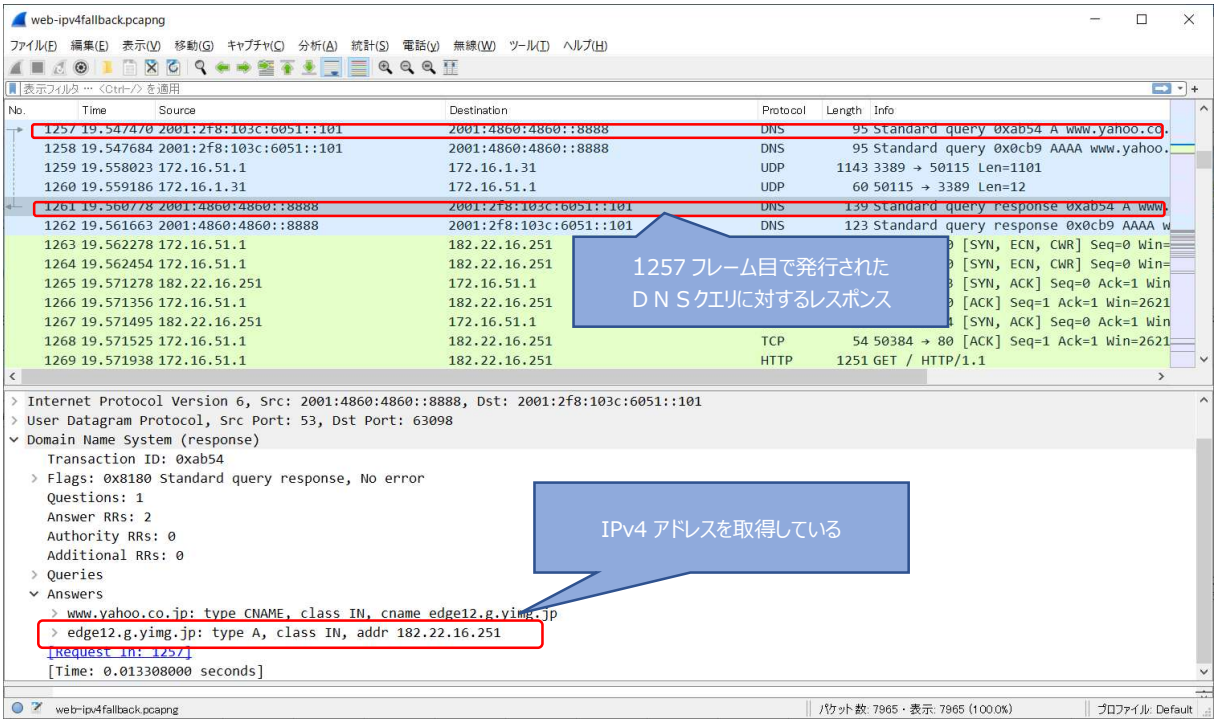


図　6.1.6-10　IPv6 未対応サイトのネットワークトレース結果(1)

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。

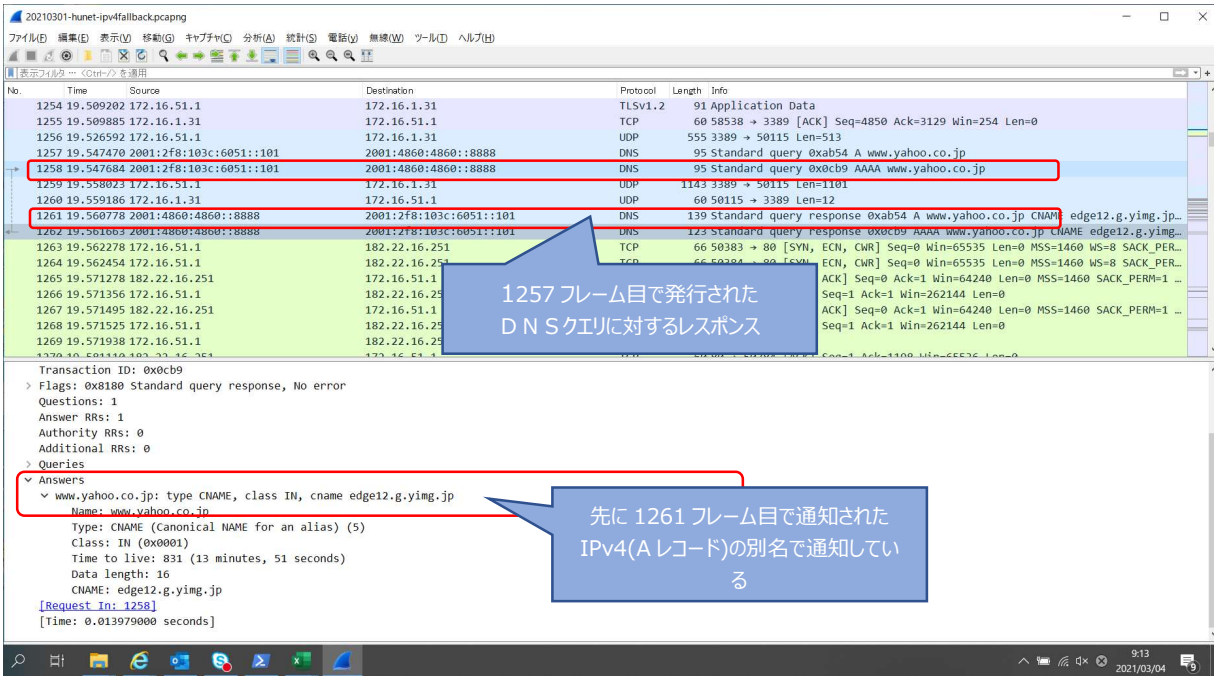


図　6.1.6-11　IPv6 未対応サイトのネットワークトレース結果(2)

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。

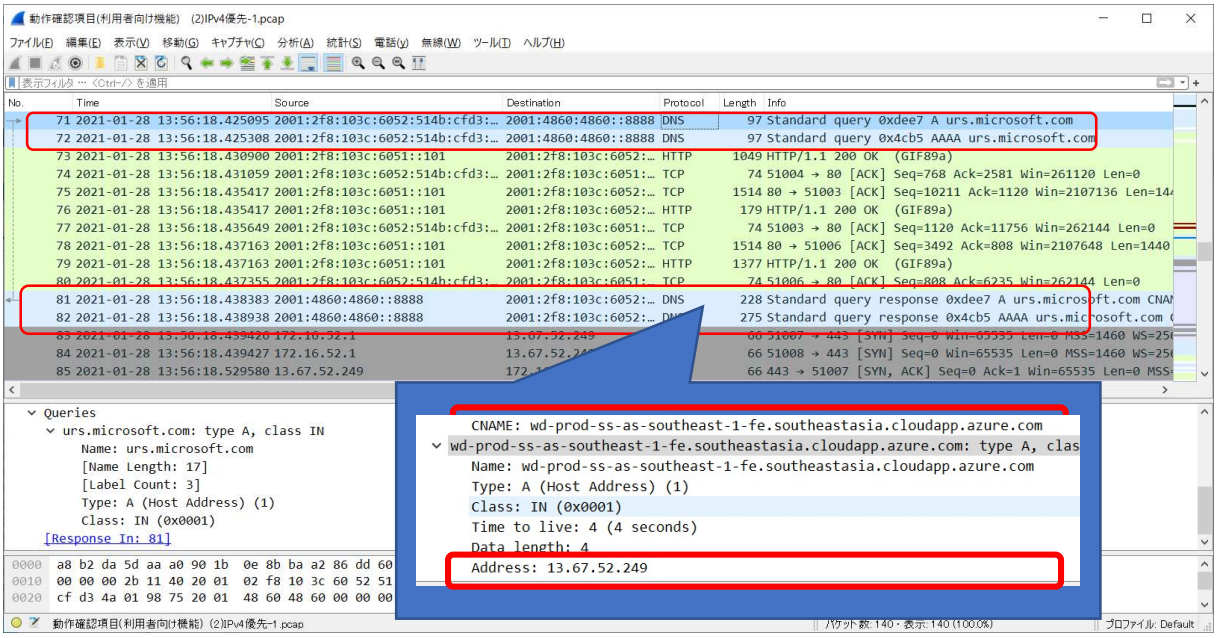


図 6.1.6-12 IPv4 優先端末で WEB アクセス時のネットワークキャプチャ実行結果(1)

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。

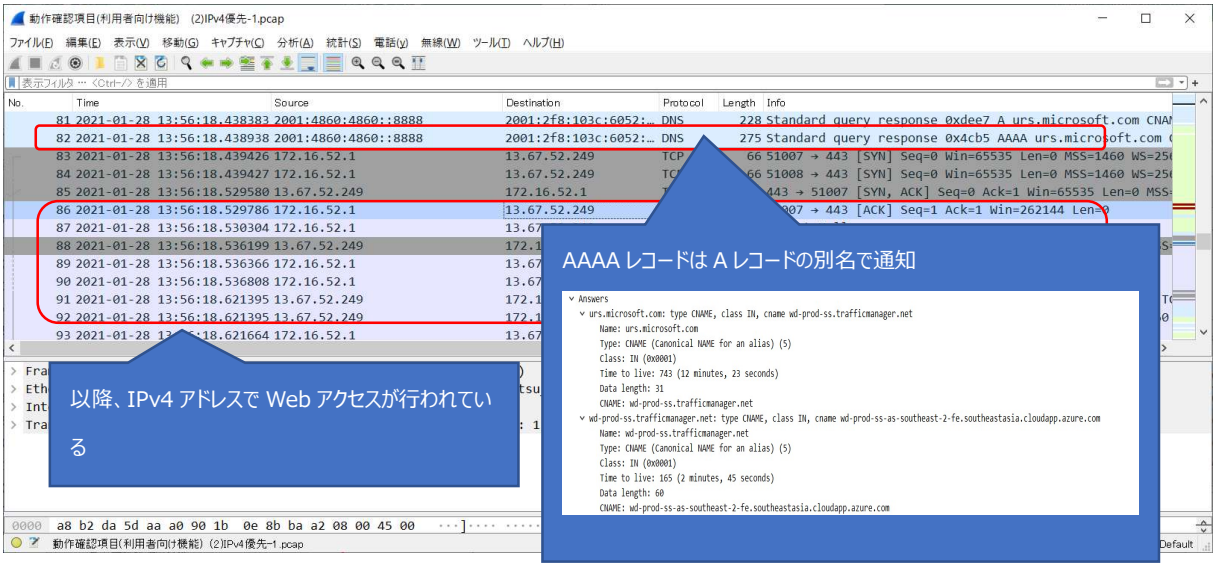


図 6.1.6-13 IPv4 優先端末で WEB アクセス時のネットワークキャプチャ実行結果(2)

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。

③ 通常業務を想定した学内ネットワーク機器の利用

#	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	実施結果
1	ノートPC	無線	IPv6優先	プリンタ	IPv4	印刷ジョブを送信する	印刷が実行される	OK ※
2	ノートPC	無線	IPv6優先	複合機(ﾃﾞｭｱﾙｽﾀｯｸ)	IPv6	印刷ジョブを送信する	印刷が実行される	OK
3	ノートPC	無線	IPv6優先	複合機(ﾃﾞｭｱﾙｽﾀｯｸ)	IPv4	複合機からスキャンを行い、スキャンデータを複合機からメール送信する	スキャンデータが指定されたメールアドレス宛に実行される	OK
4	ノートPC	無線	IPv6優先	複合機(ﾃﾞｭｱﾙｽﾀｯｸ)	IPv4	印刷ジョブを送信する	印刷が実行される	OK
5	ノートPC	無線	IPv6優先	複合機(IPv6シングルスタック)	IPv6	印刷ジョブを送信する	印刷が実行される	OK
6	ノートPC	無線	IPv6優先	複合機(IPv6シングルスタック)	IPv4	印刷ジョブを送信する	指定した宛先が見つからないため、印刷が実行されない	OK
7	ノートPC	無線	IPv6優先	複合機(IPv6シングルスタック)	IPv6	複合機からスキャンを行い、スキャンデータを複合機からメール送信する	スキャンデータが指定されたメールアドレス宛に実行されない	OK

【#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。

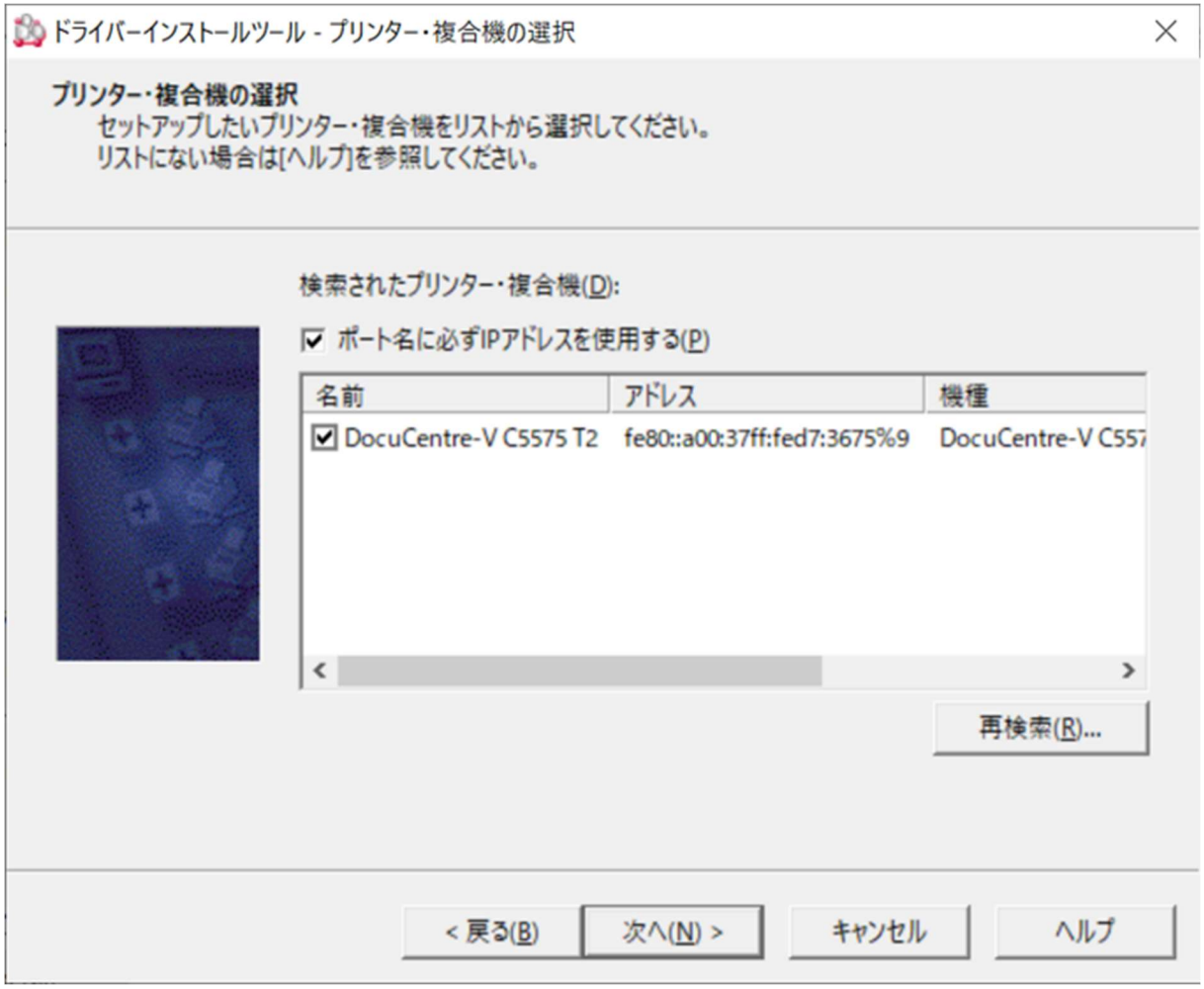


図 6.1.6-14 プリンタドライバインストール時にプリンタを自動検出した際の動作

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。

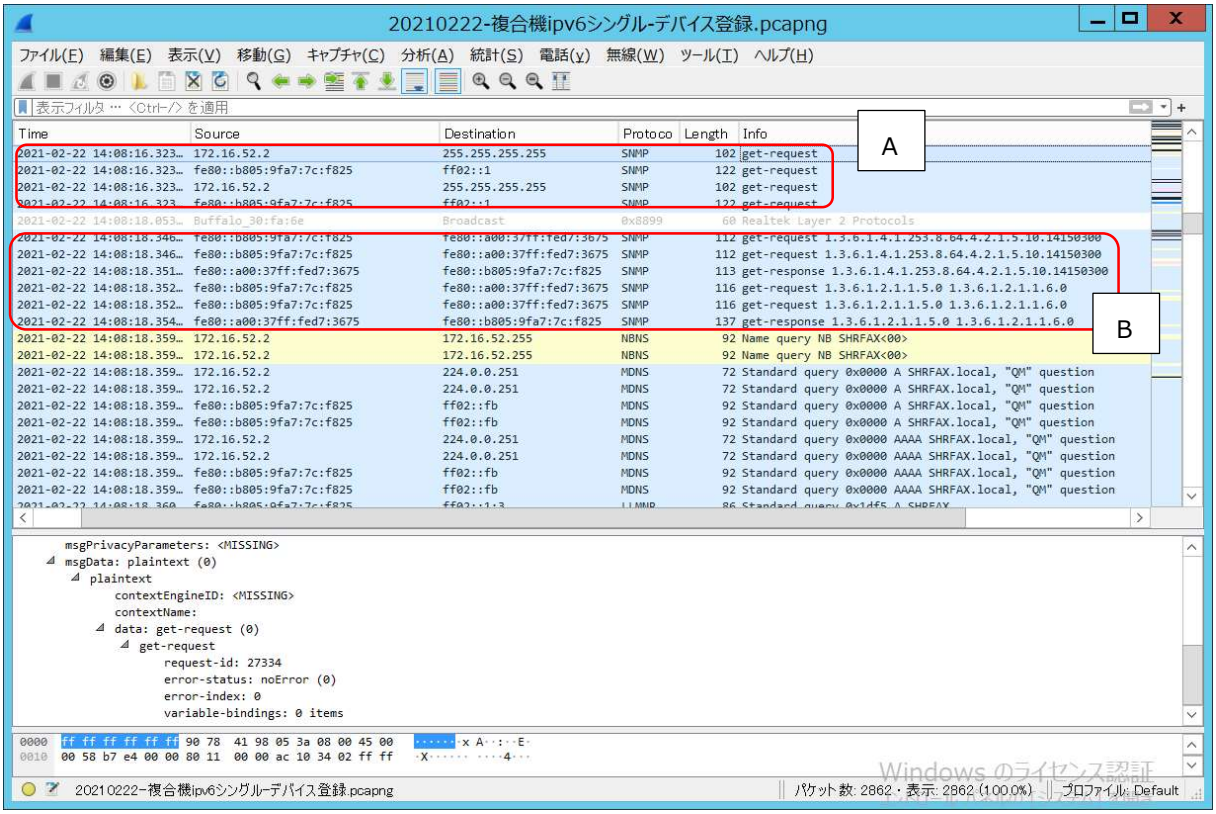


図 6.1.6-15 プリンタドライバインストール時のネットワークトレース結果

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。

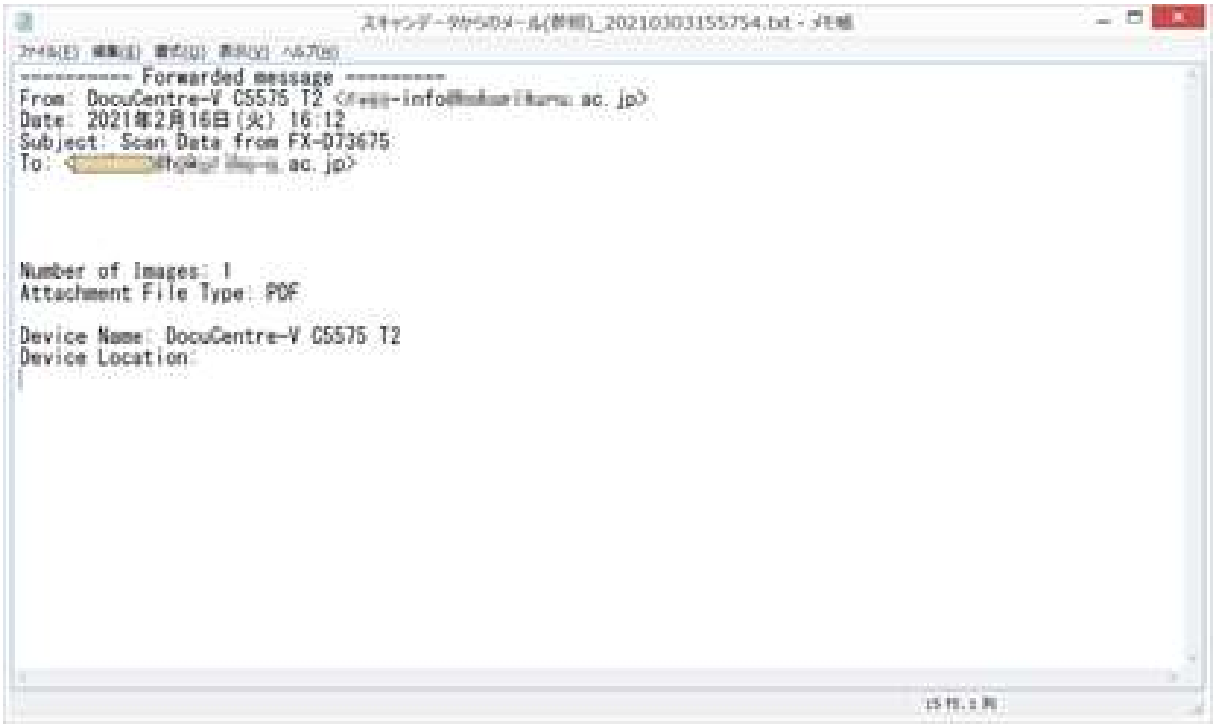


図 6.1.6-16 複合機からのスキャンデータ受信メール

【#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。

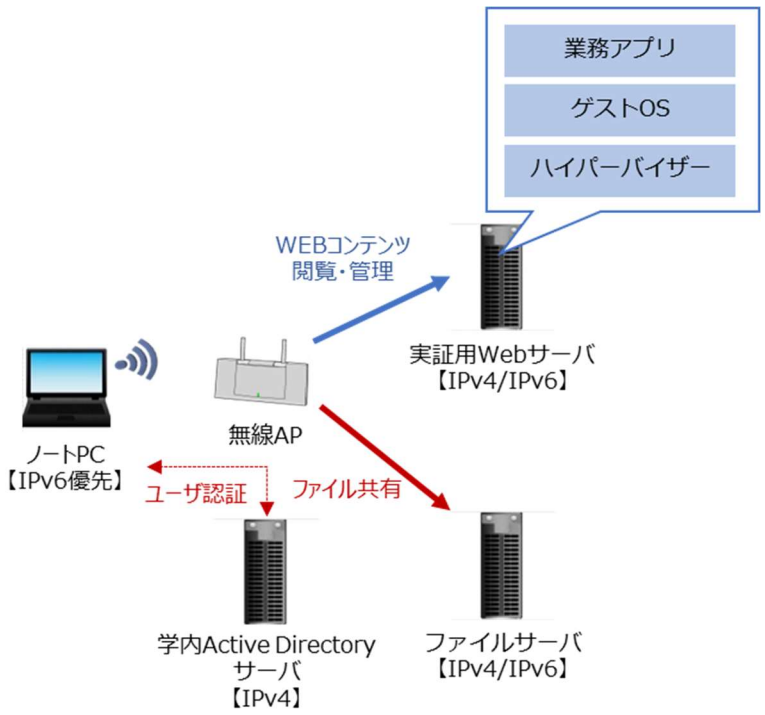


図 6.1.6-17 業務アプリケーションにおける検証範囲

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。

③ 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	実施結果
1	ノートPC	無線	IPv6 優先	実証用学内 WEB サーバ	IPv6	【一般利用者向け確認】 WEB ブラウザより学内 WEB サービス(IPv6 ｱﾄﾞﾚｽ)の WEB 表示を行う	学内 WEB コンテンツが正しく表示されること IPv6 アドレスで http セッションが確立されていること	OK
2	ノートPC	無線	IPv6 優先	実証用学内 WEB サーバ	IPv4	【一般利用者向け確認】 WEB ブラウザより学内 WEB サービス(IPv4 ｱﾄﾞﾚｽ)の WEB 表示を行う	学内 WEB コンテンツが正しく表示されること IPv4 アドレスで http セッションが確立されていること	OK
3	ノートPC	無線	IPv4 優先	実証用学内 WEB サーバ	IPv6	【一般利用者向け確認】 WEB ブラウザより学内 WEB サービス(IPv6 ｱﾄﾞﾚｽ)の WEB 表示を行う	学内 WEB コンテンツが正しく表示されること IPv6 アドレスで http セッションが確立されていること	OK
4	ノートPC	無線	IPv4 優先	実証用学内 WEB サーバ	IPv4	【一般利用者向け確認】 WEB ブラウザより学内 WEB サービス(IPv4 ｱﾄﾞﾚｽ)の WEB 表示を行う	学内 WEB コンテンツが正しく表示されること IPv4 アドレスで http セッションが確立されていること	NG ※1
5	ノートPC	無線	IPv6 優先	実証用学内 WEB サーバ	IPv6	【管理者向け確認】 ①学内 WEB サービスのハイパーリンク(CLBOX)をクリックする 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	CLBOX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できること	NG ※2

【#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。

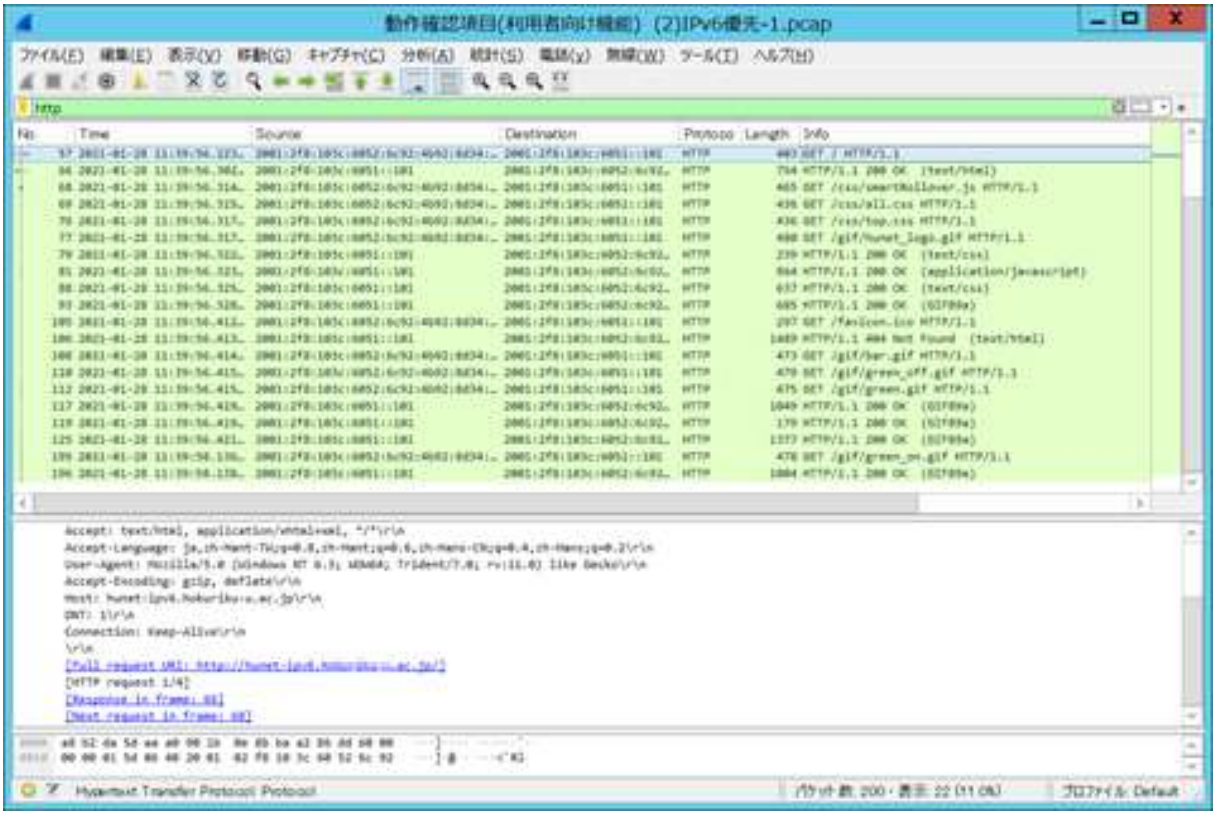


図 6.1.6-18 実証用学内 WEB サーバを WEB 表示した際のネットワークトレース結果(1)

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。

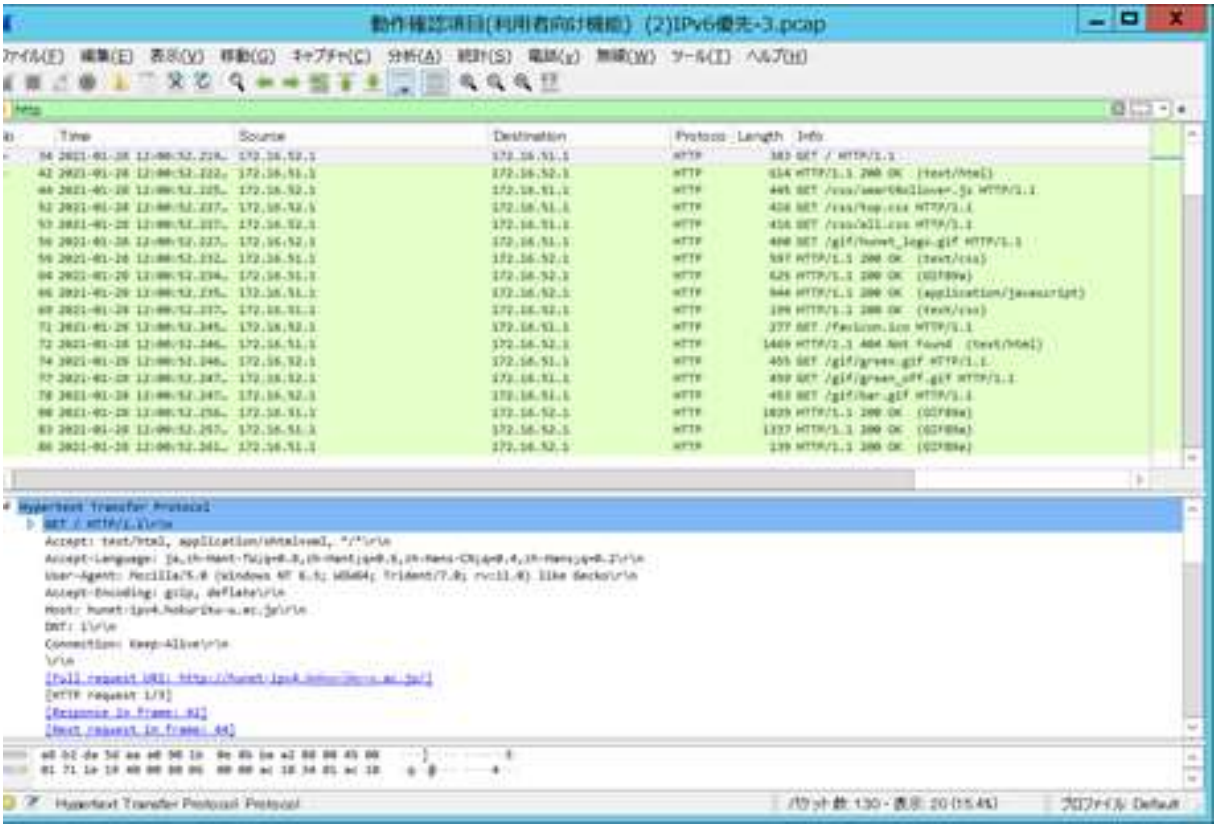


図 6.1.6-19 実証用学内 WEB サーバを WEB 表示した際のネットワークトレース結果(2)

【#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。

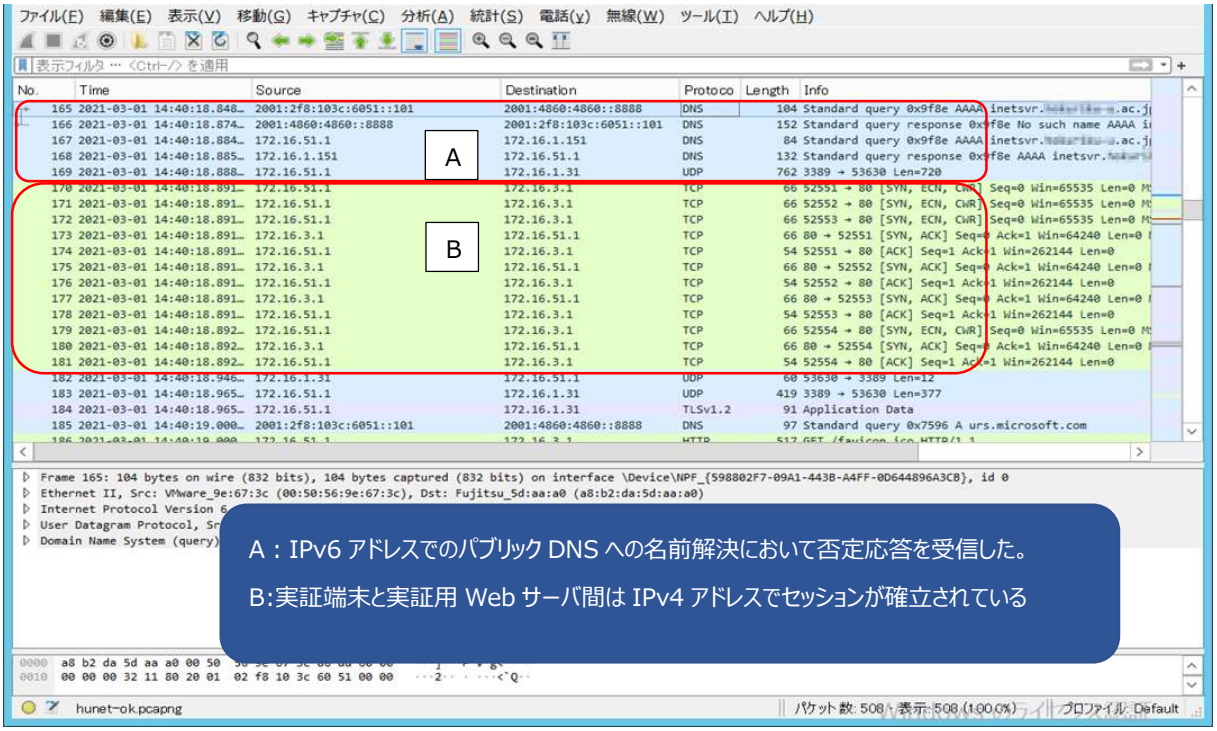


図 6.1.6-20 IPv4 優先端末から WEB 表示した際のネットワークトレース結果(1)

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。

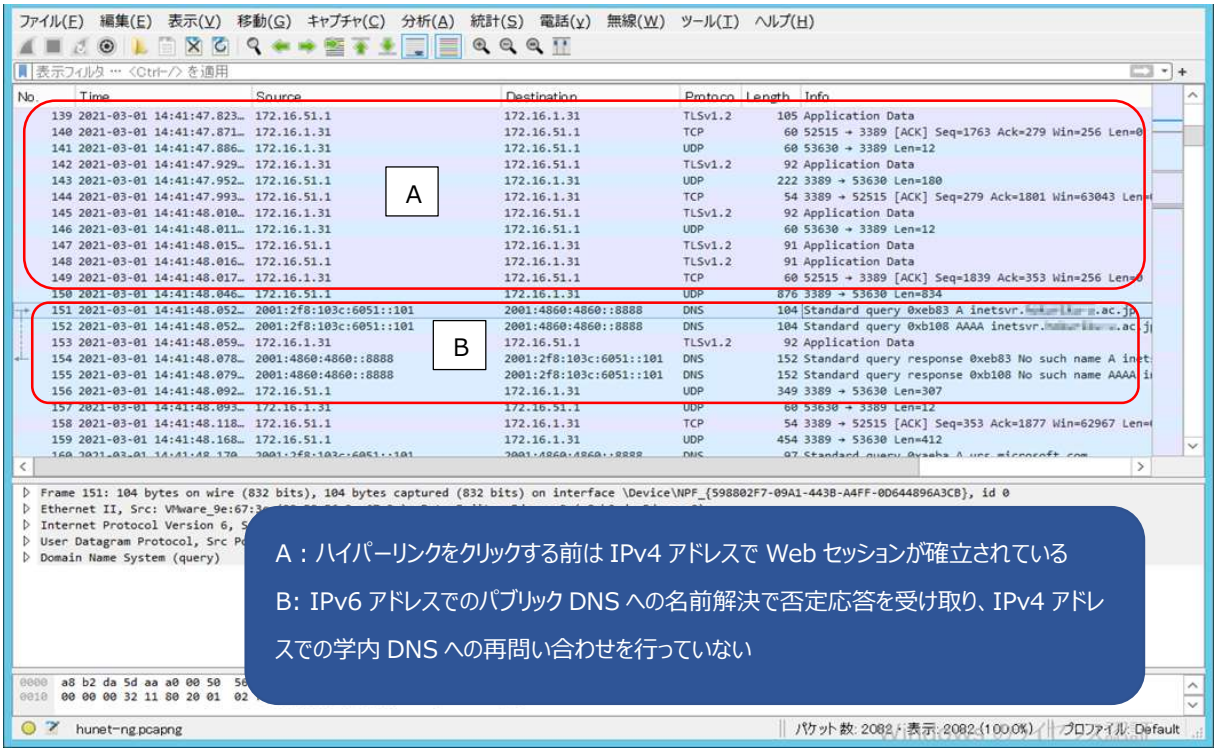


図 6.1.6-21 IPv4 優先端末から WEB 表示した際のネットワークトレース結果(2)

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	実施結果
1	ノートPC	無線	IPv6優先	ファイルサーバ	IPv6	①検証用PCから実証用ファイルサーバの共有フォルダをIPv6アドレスで開く ②認証画面で学内ADドメインのWindowsアカウントを入力する	Active Directoryの認証が成功し、共有フォルダの一覧表示ができること	OK
2	ノートPC	無線	IPv6優先	ファイルサーバ	IPv4	①検証用PCから実証用ファイルサーバの共有フォルダをIPv4アドレスで開く ②認証画面で学内ADドメインのWindowsアカウントを入力する	Active Directoryの認証が成功し、共有フォルダの一覧表示ができること	OK ※
3	ノートPC	無線	IPv4優先	ファイルサーバ	IPv6	①検証用PCから実証用ファイルサーバの共有フォルダをIPv6アドレスで開く ②認証画面で学内ADドメインのWindowsアカウントを入力する	Active Directoryの認証が成功し、共有フォルダの一覧表示ができること(No.4 と同様の結果となること)	OK
4	ノートPC	無線	IPv4優先	ファイルサーバ	IPv4	①検証用PCから実証用ファイルサーバの共有フォルダをIPv4アドレスで開く ②認証画面で学内ADドメインのWindowsアカウントを入力する	Active Directoryの認証が成功し、共有フォルダの一覧表示ができること(No.4 と同様の結果となること)	OK

【#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。

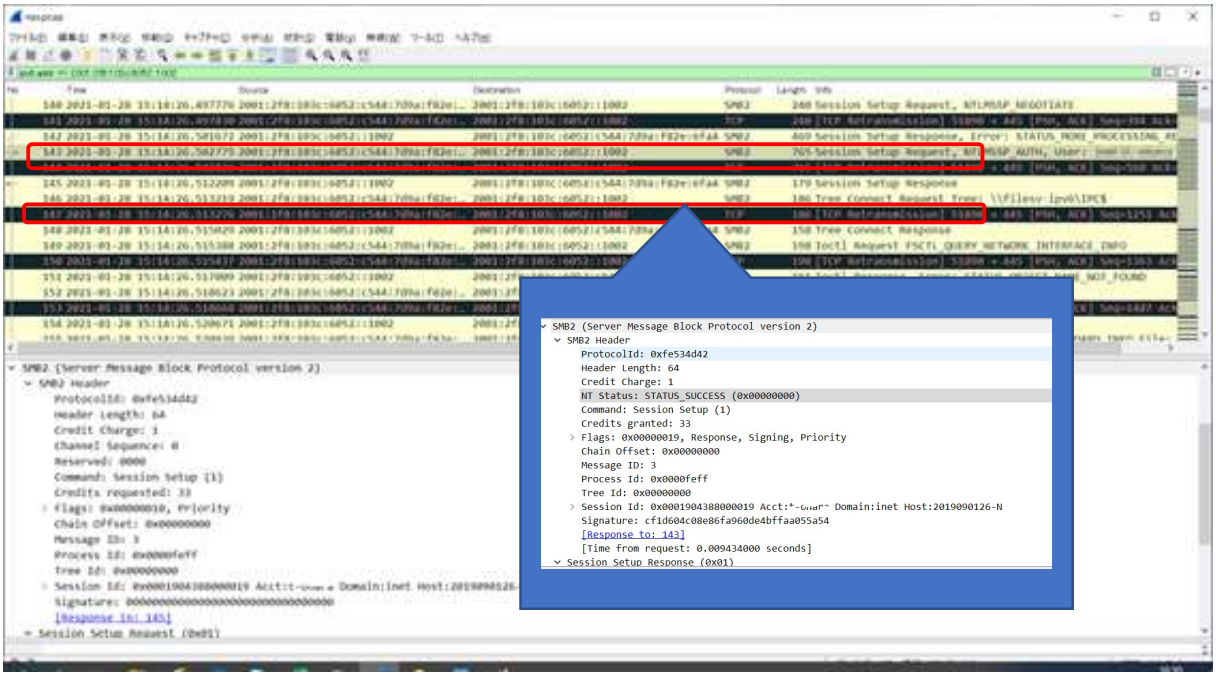


図 6.1.6-22 IPv6 優先端末でファイルサーバアクセス時のネットワークキャプチャ実行結果

【#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。

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。

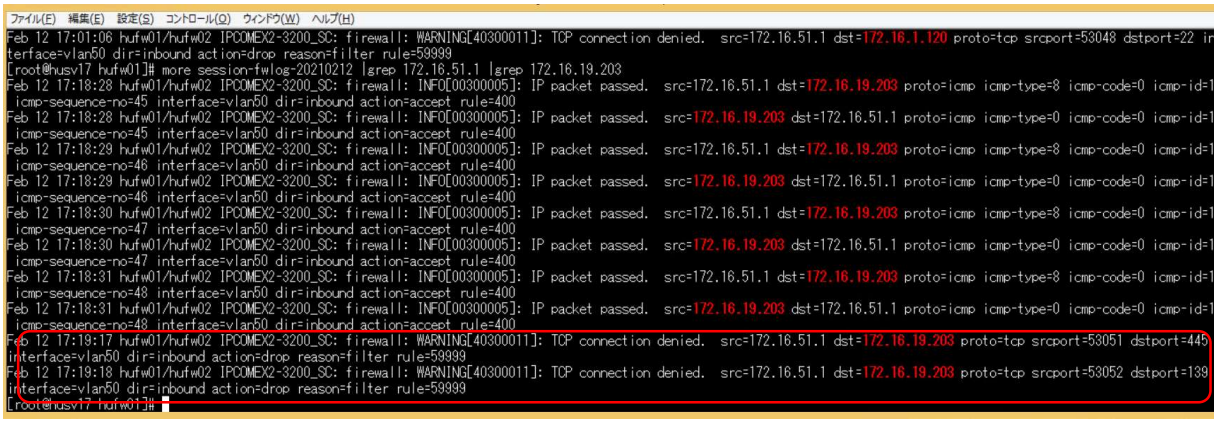


図 6.1.6-24 実証端末からIPv4アドレスでファイルサーバアクセス時のファイアウォールログ

「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。

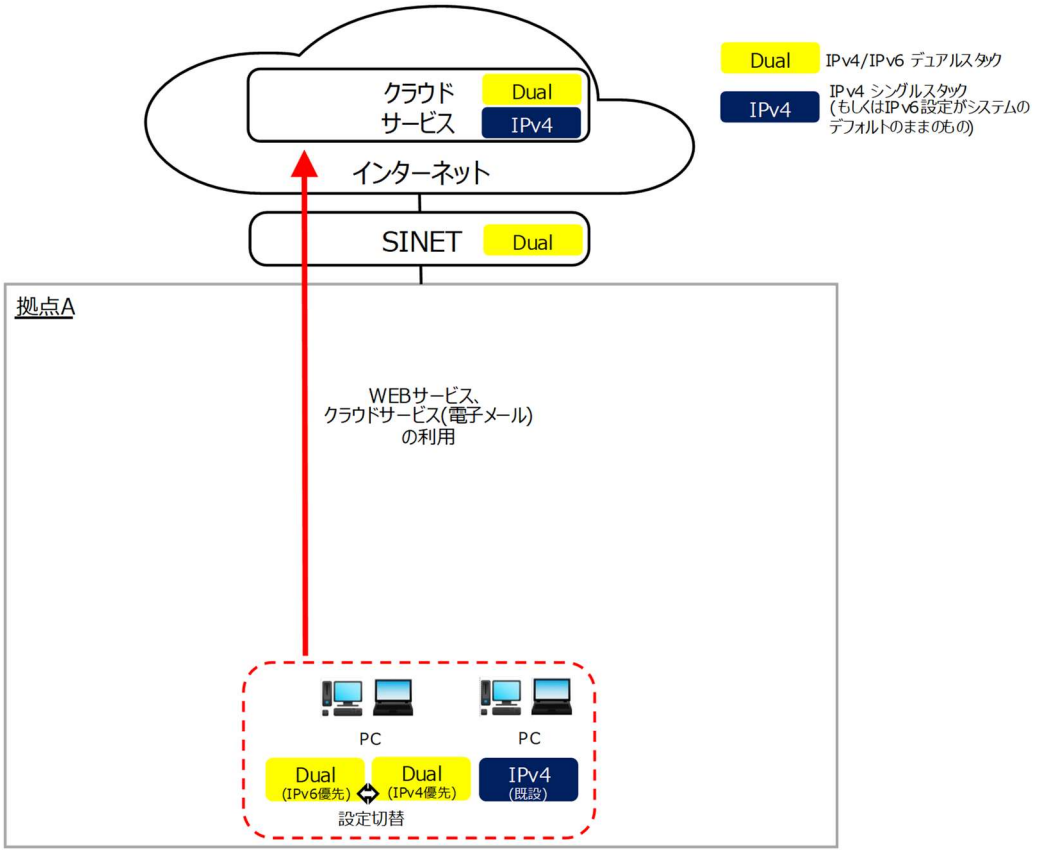


図　6.1.6-25　業務アプリケーションにおける検証(クラウド)範囲

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

【#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。

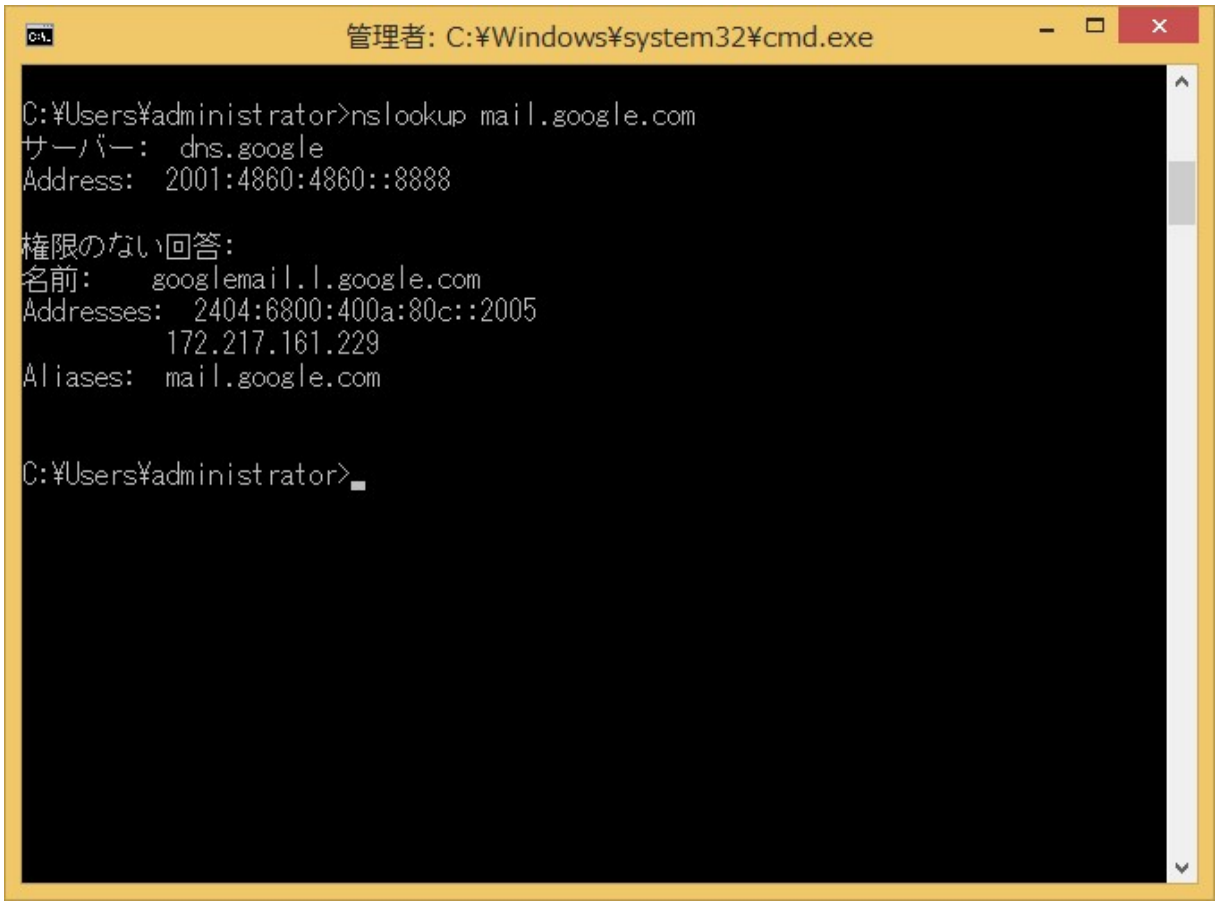


図 6.1.6-26 「mail.google.com」に対する nslookup 結果

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。

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。

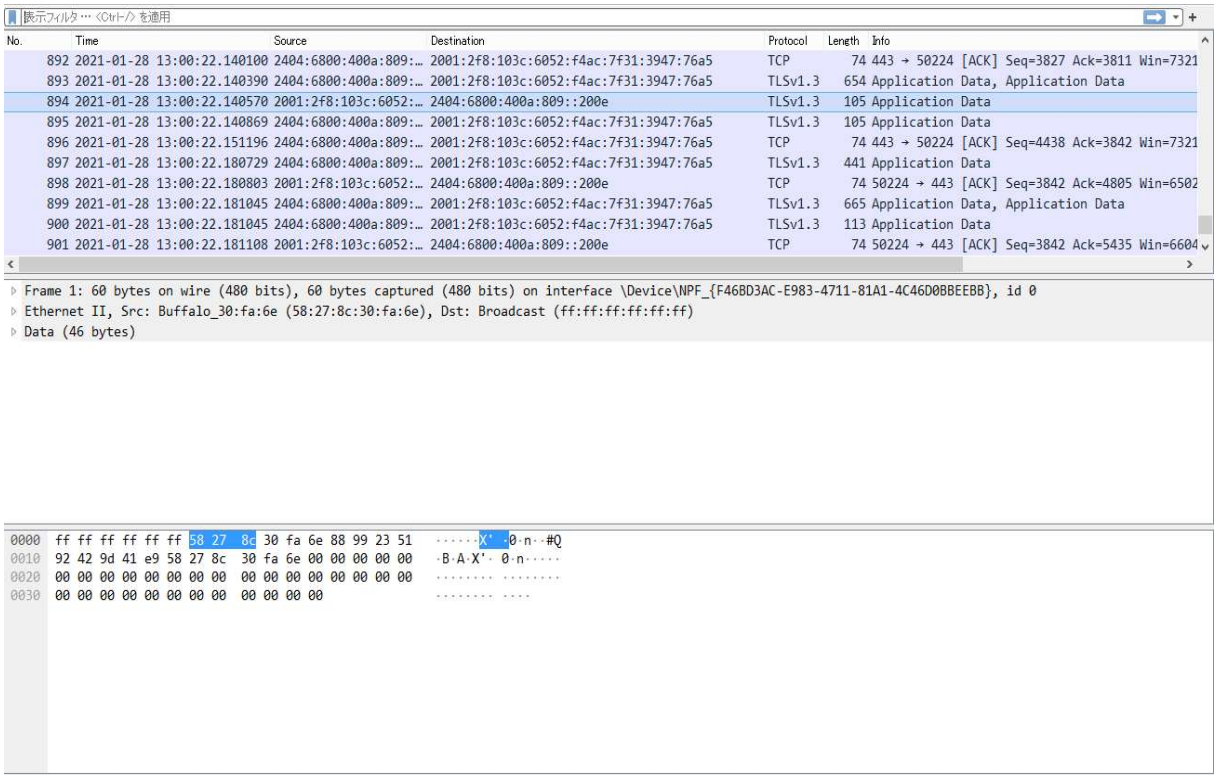


図 6.1.6-28 Gmail での利用者認証画面表示時のネットワークトレース結果

(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。

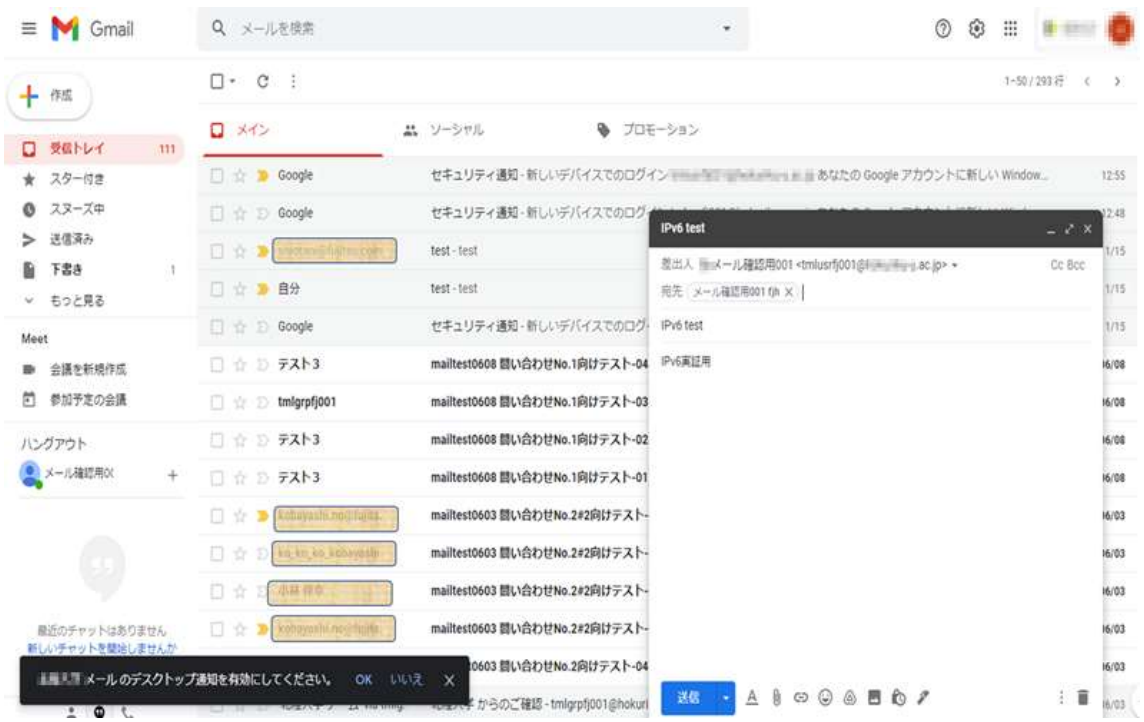


図 6.1.6-29 Gmail でのテストメール作成画面

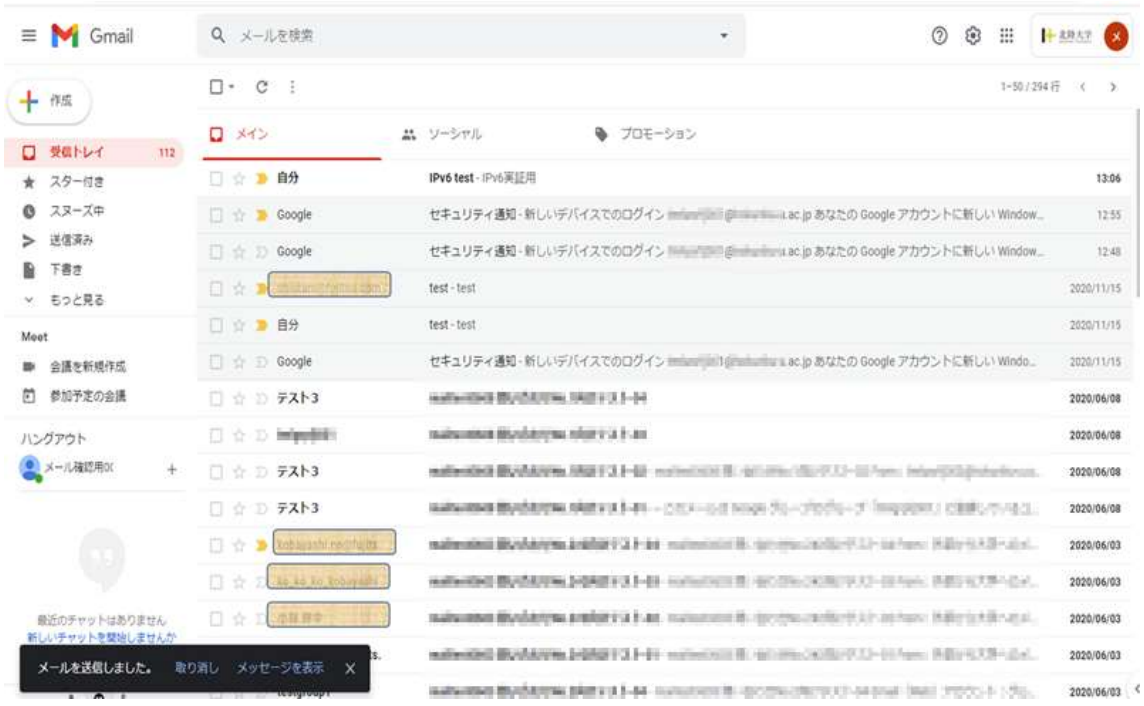


図 6.1.6-30 Gmail でのテストメール受信画面

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。

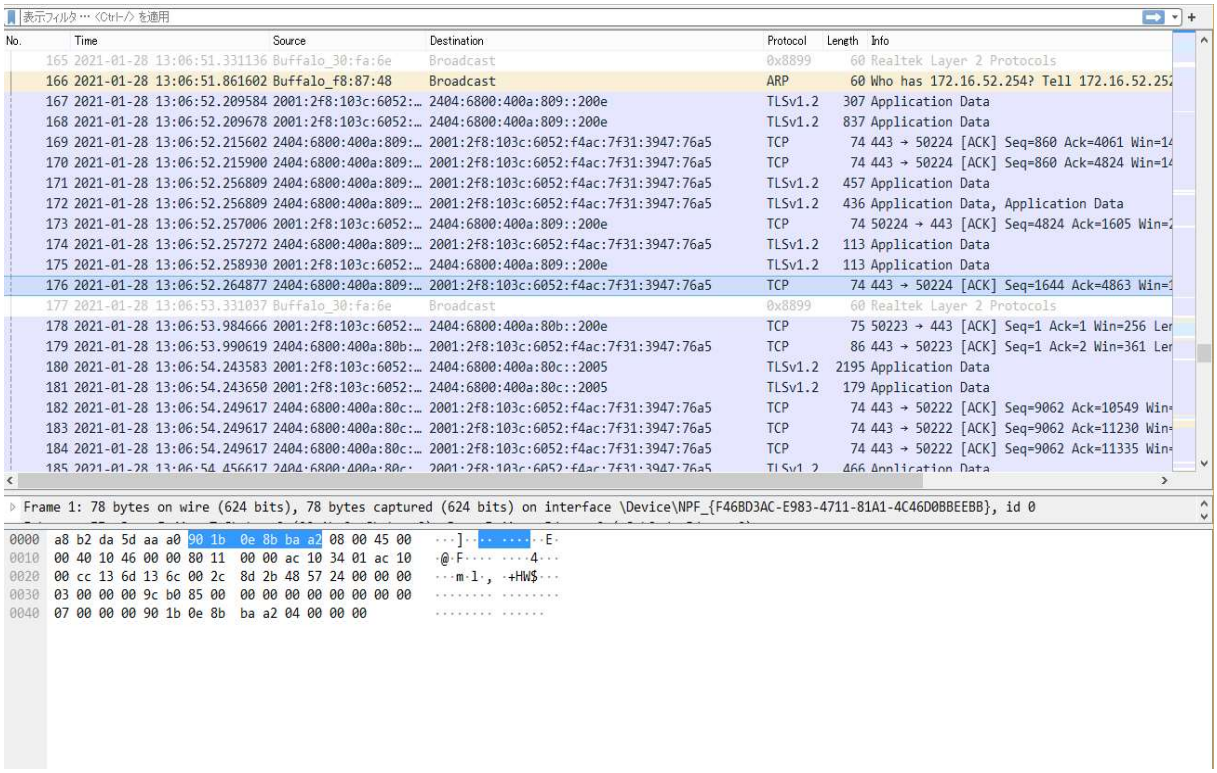


図 6.1.6-31 Gmail でのテストメール受信時のネットワークトレース結果

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	実施結果
1	ノートPC	無線	IPv6 優先	Office365 (WEB メール) 一般利用者向け	IPv6	①マイクロソフトオンラインサービスの URL を開く ②認証画面で ID、パスワードを入力する ③テストメールを送信する	Office365(WebMail) が IPv6 で接続できること テストメールの送受信が可能であること	OK
2	ノートPC	無線	IPv4 優先	Office365 (WEB メール) 一般利用者向け	IPv4	①マイクロソフトオンラインサービスの URL を開く ②認証画面で ID、パスワードを入力する ③テストメールを送信する	Office365(WebMail) が IPv4 で接続できること テストメールの送受信が可能であること	OK
3	ノートPC	無線	IPv6 優先	Office365 管理者向け	IPv6	①マイクロソフトオンラインサービスの管理ポータル画面の URL を開く ②管理センタのメニューから「正常性」－「サービス正常性」を選択する	Office365 管理センタ画面が IPv6 で接続できること 「サービス正常性」画面の「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	OK
4	ノートPC	無線	IPv4 優先	Office365 管理者向け	IPv4	①マイクロソフトオンラインサービスの管理ポータル画面の URL を開く ②管理センタのメニューから「正常性」－「サービス正常性」を選択する	Office365 管理センタ画面が IPv4 で接続できること 「サービス正常性」画面の「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	OK

【#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。

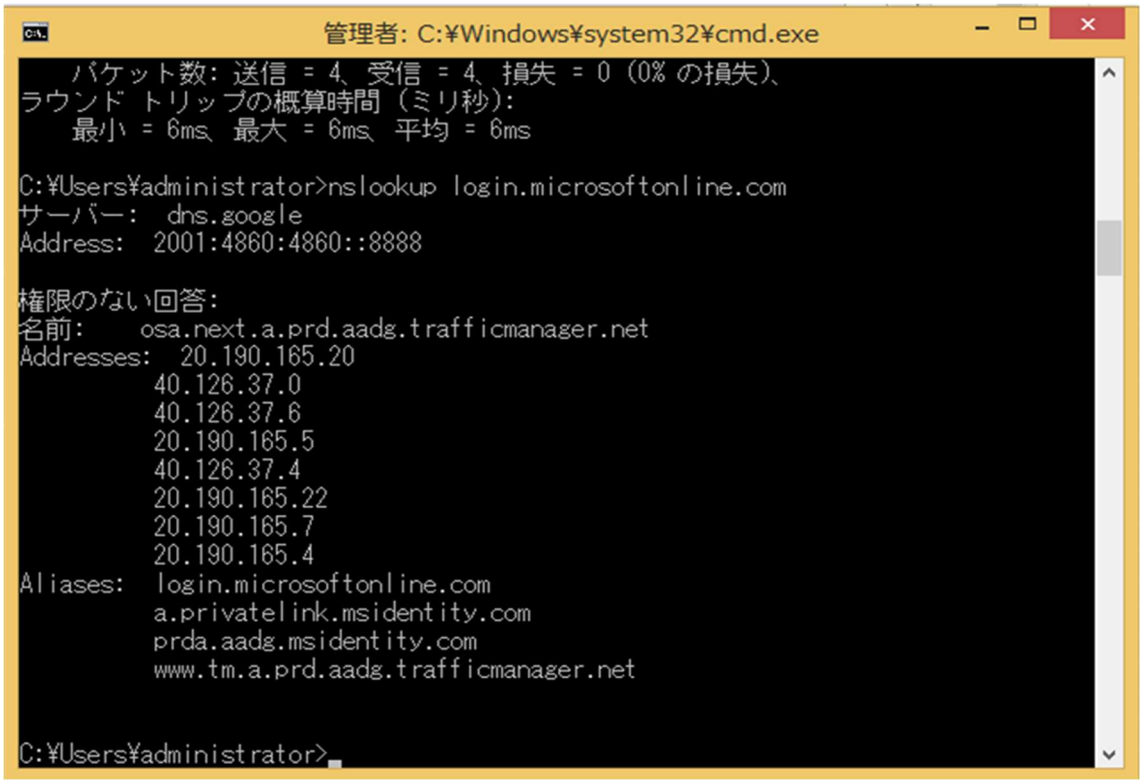


図 6.1.6-32 マイクロソフトオンラインサービスの nslookup 確認結果

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。

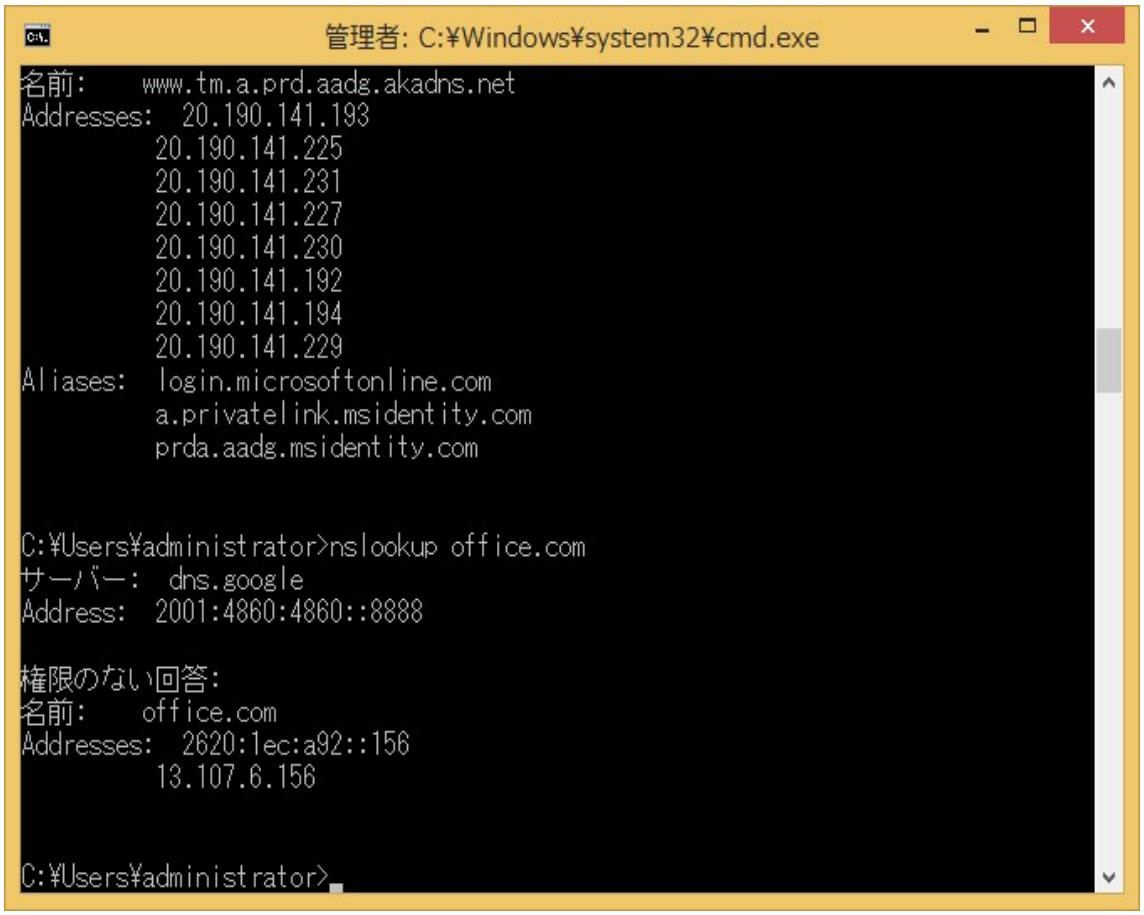


図 6.1.6-33 「office.com」の nslookup 確認結果

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。

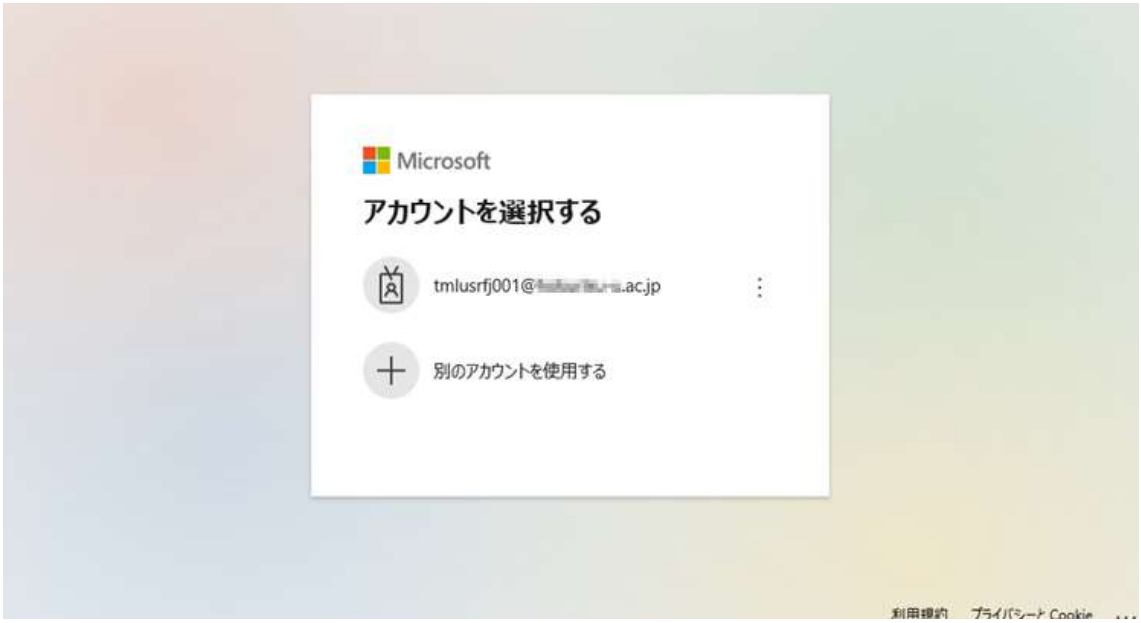


図 6.1.6-34 マイクロソフトオンラインサービスサインイン画面

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。

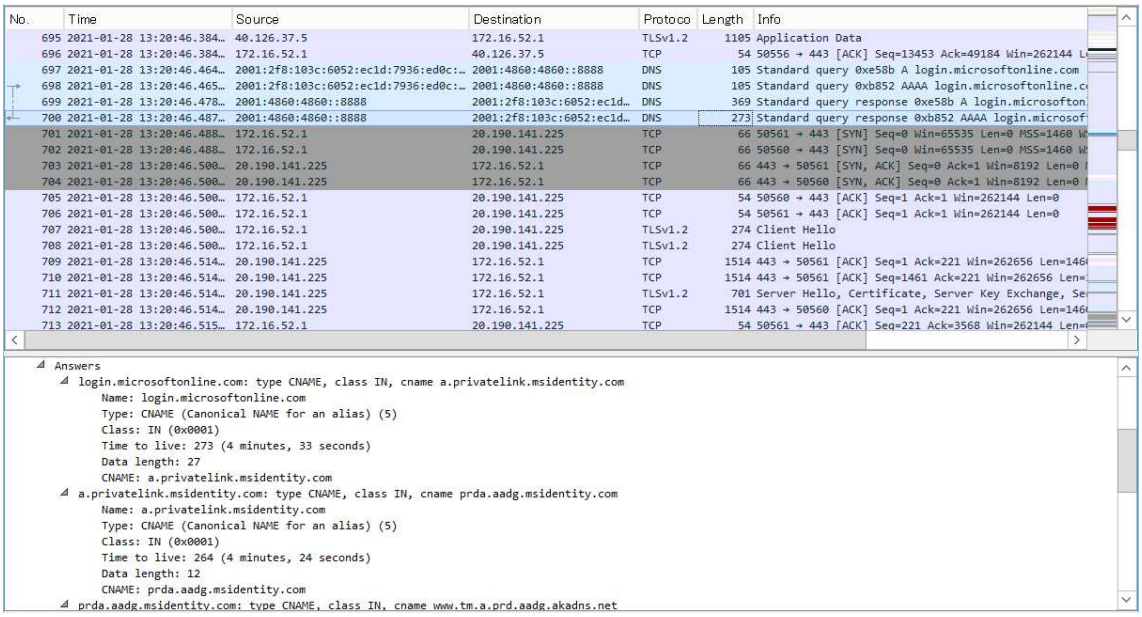


図 6.1.6-35 マイクロソフトオンラインサービスサインイン時のネットワークトレース結果

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」へリダイレクトされた後の通信状況の確認を行った。

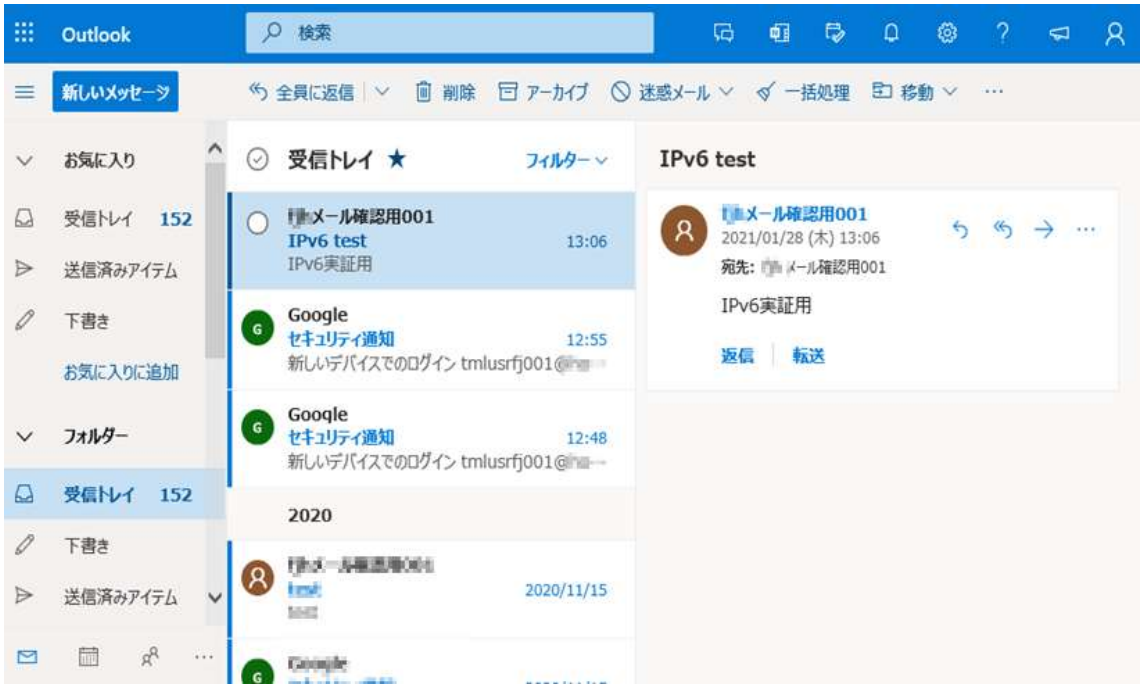


図 6.1.6-36 「office.com」から Outlook WEB メールを開いた状態

この状態でのネットワークトレースを以下に記載する。

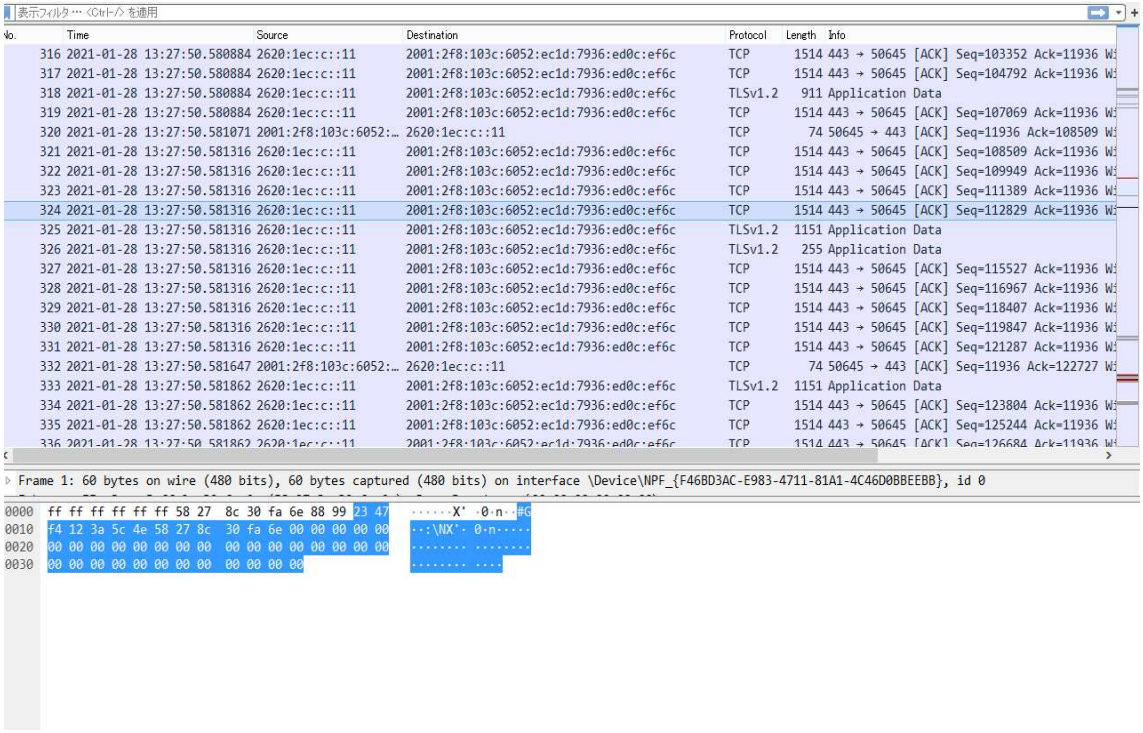


図 6.1.6-37 「office.com」から Outlook WEB メールを開いた状態でのネットワークトレース結果

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。

① IPv6 アドレスの自動設定における検証

#	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	実施結果
1	実証用 WEB サーバ	有線	IPv6 優先	実証用ネットワーク (LAN051) RA 送信無	IPv6 (手動)	ipconfig /all を実行する	実行結果より以下の内容を確認する ・IPv6 アドレス:手動設定値 ・一時 IPv6 アドレス:未割当 ・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)	OK

#	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	実施結果
2	デスクトップ PC	有線	IPv6 優先	実証用ネットワーク（LAN052） RA 送信有	IPv6（手動）	ipconfig /all を実行する	実行結果より以下の内容を確認する ・IPv6 アドレス：手動設定値 ・一時 IPv6 アドレス：自動設定 ・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）	OK
3	ノート PC	無線	IPv6 優先	実証用ネットワーク（LAN052） RA 送信有	IPv6（手動）	ipconfig /all を実行する	実行結果より以下の内容を確認する ・IPv6 アドレス：手動設定値 ・一時 IPv6 アドレス：自動設定 ・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）	OK

#	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	実施結果
4	ノートPC	無線	IPv6優先	実証用ネットワーク（LAN052） RA送信有	IPv6（自動）	①「インターネット プロトコル バージョン 6(TCP/IPv6)」のプロパティより「IPv6 アドレスを自動的に取得する」を選択し、「OK」を押して設定を反映する。 ②ipconfig /all を実行する	実行結果より以下の内容を確認する ・IPv6 アドレス：自動設定値 ・一時 IPv6 アドレス：自動設定 ・リンクローカル IPv6 アドレス：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)	OK

【#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。

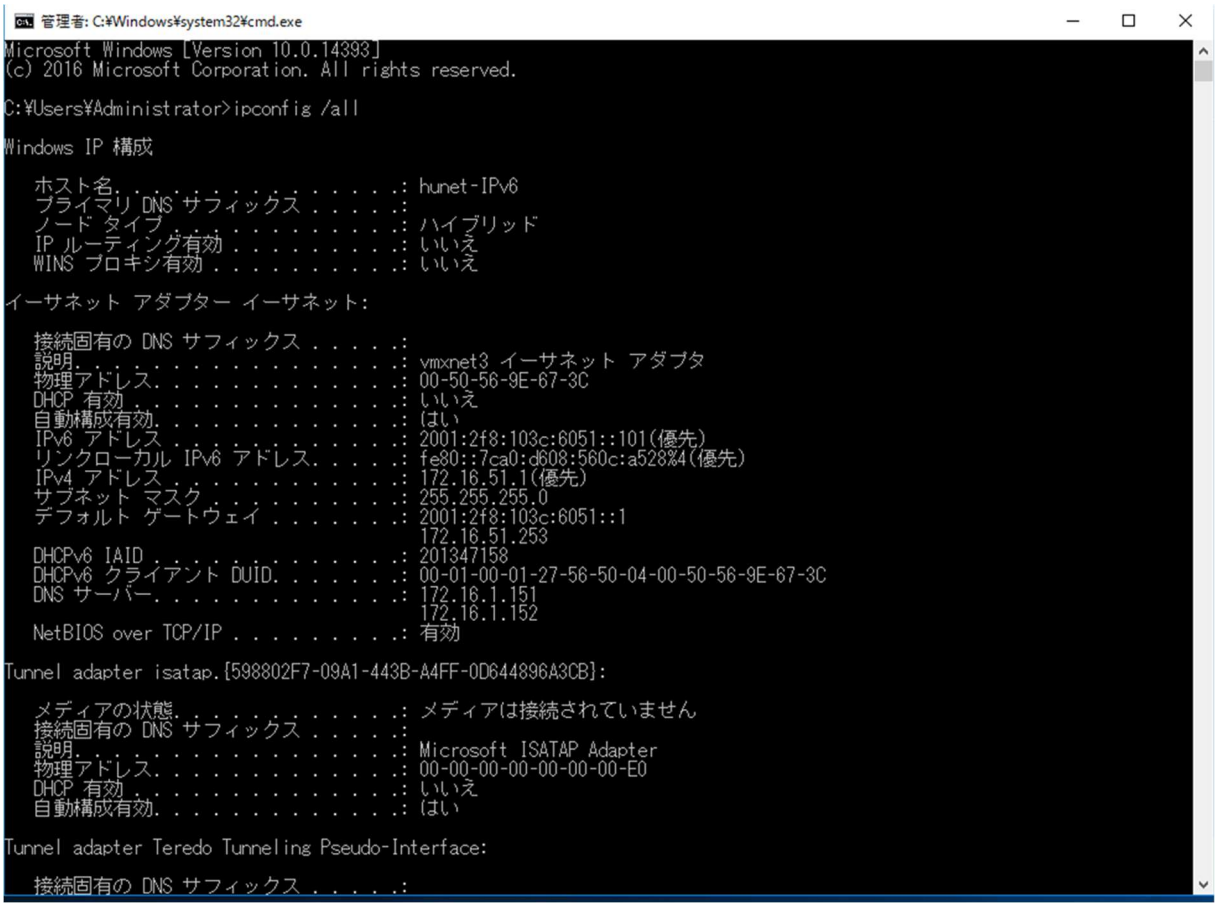


図 6.1.6-38 「ipconfig /all」実行結果(RA 未送信セグメント)

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。

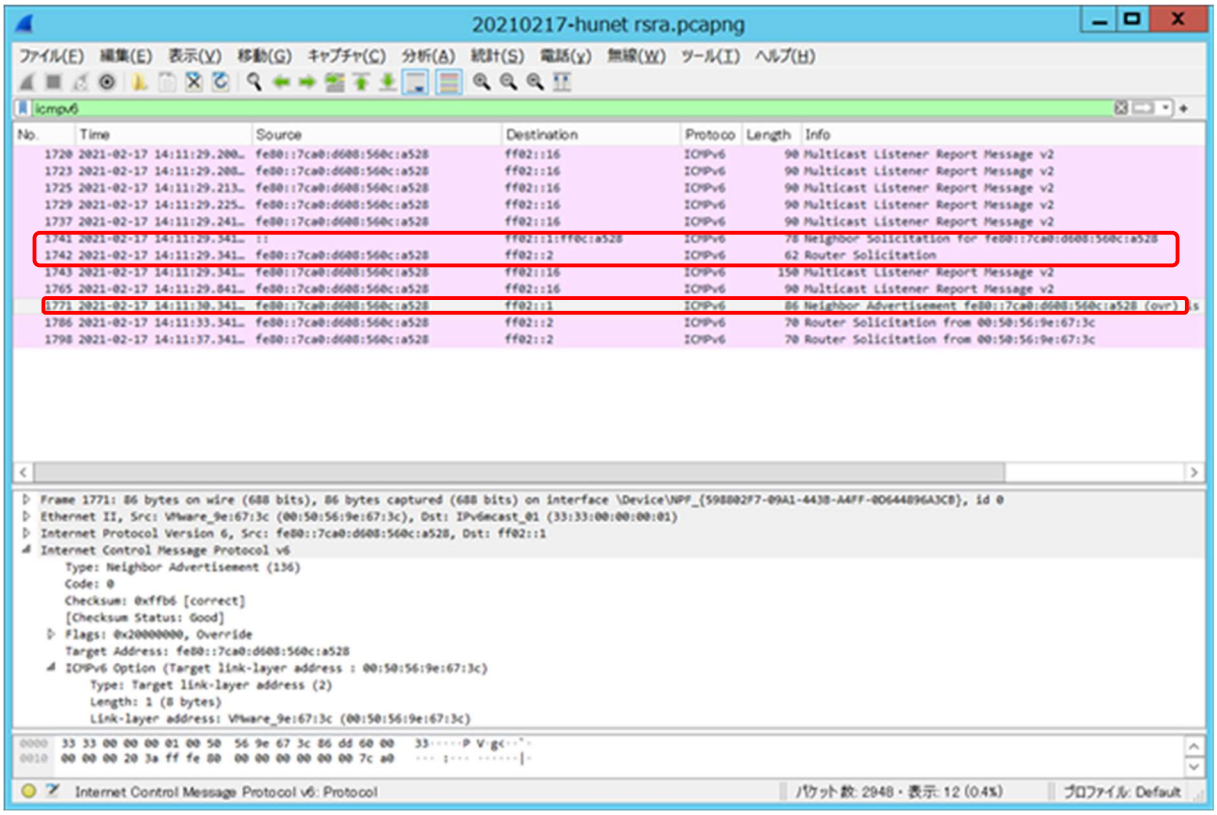


図 6.1.6-39 ネットワークトレースの状態(RA 未送信セグメント)

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。

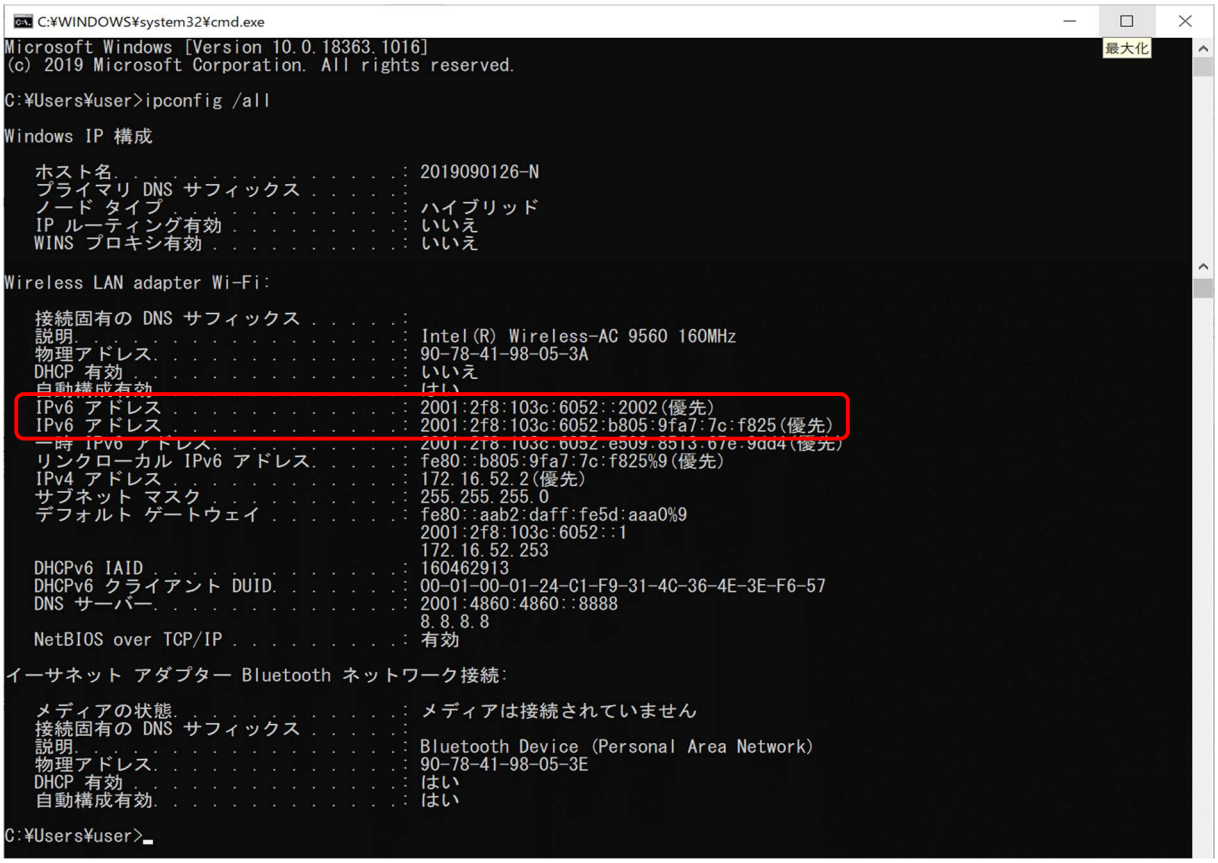


図 6.1.6-40 「ipconfig /all」実行結果(RA 送信セグメント)

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。

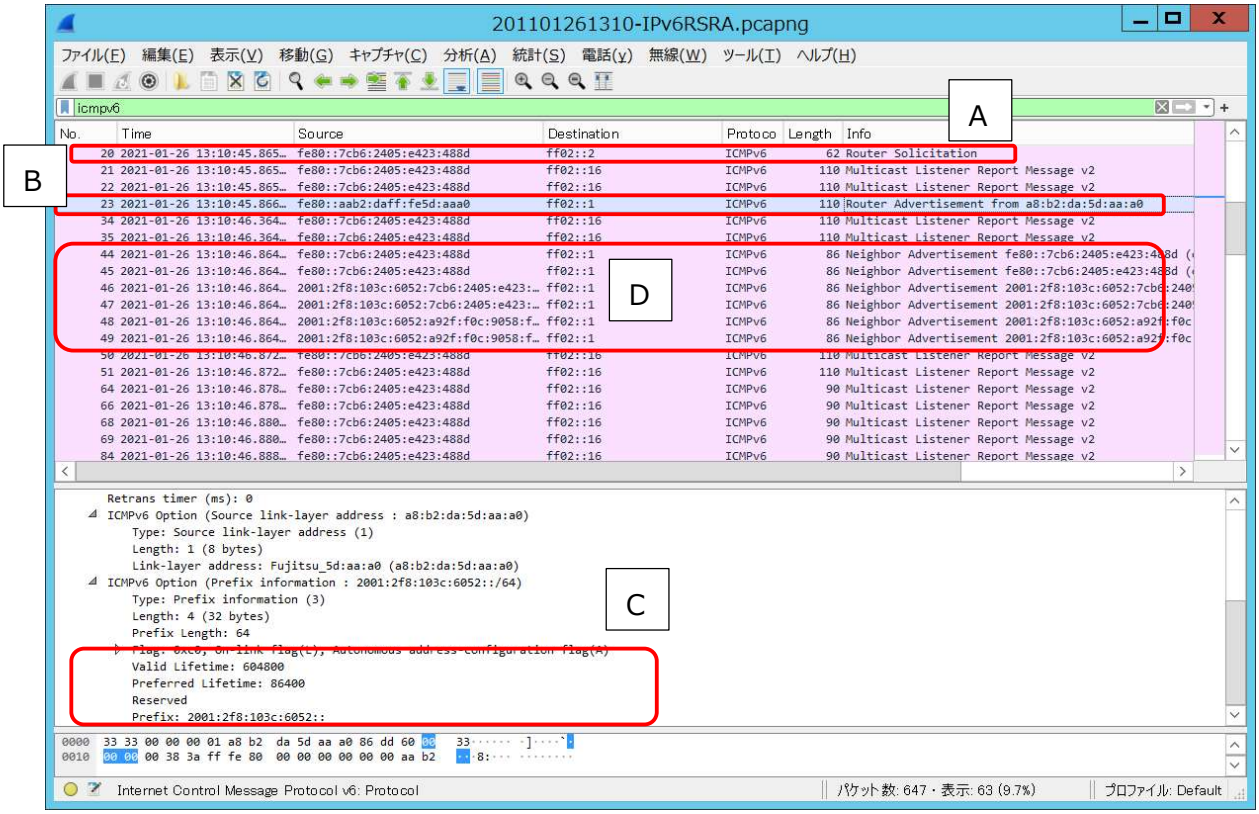


図 6.1.6-41 ネットワークトレースの状態(RA 送信セグメント)

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。

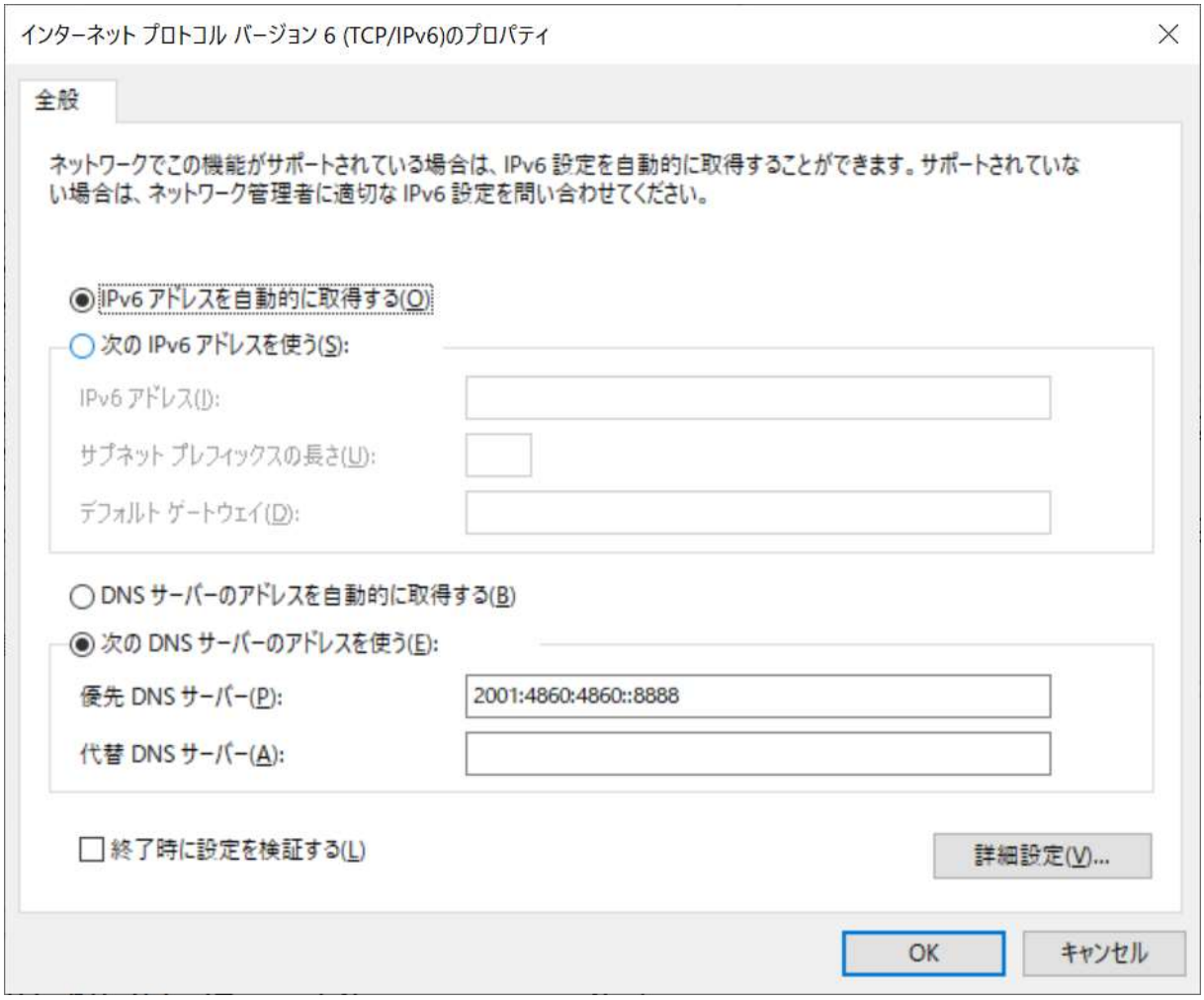


図 6.1.6-42 IPv6 アドレス自動構成を行う為の設定

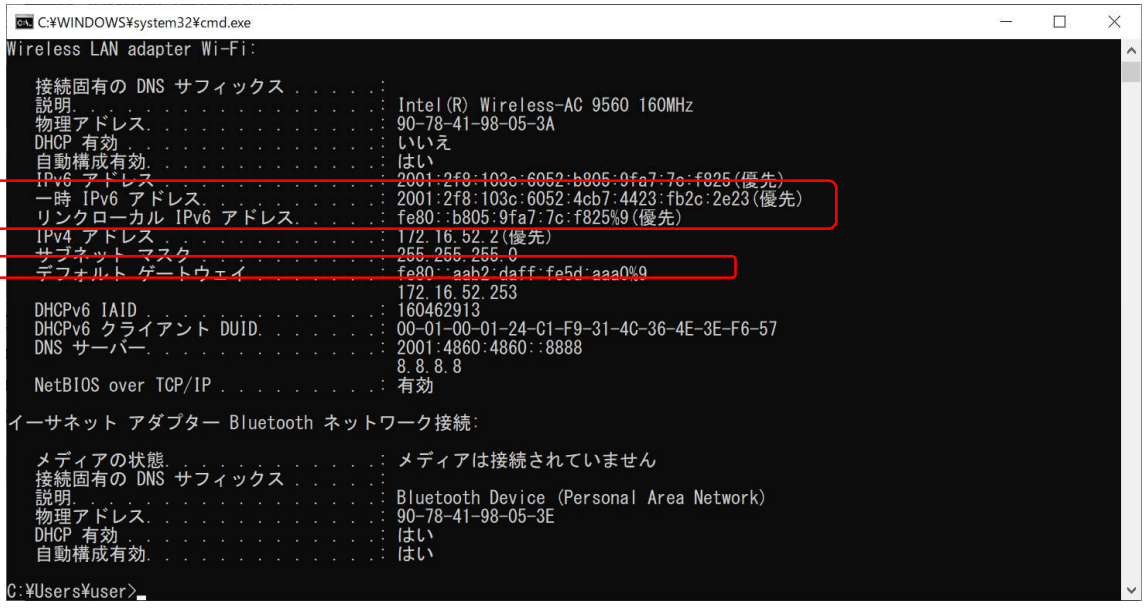


図 6.1.6-43 「ipconfig /all」実行結果(RA 送信セグメント:IPv6 アドレス自動構成)

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。

② 運用性/保守性における検証

#	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	実施結果
1	実証用L３スイッチ	有線	ー	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	ー	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	OK

#	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	実施結果
3	実証用FW装置	有線	ー	ログ管理サーバ	IPv4 /IPv6	ログ管理サーバに SSH でログインし、実証用 FW 装置からのログ転送先に生成されたセッションログを確認する	実証用 IPv6 アドレス(XXXX:YYY:*)で grep し、以下の情報が記録されていることを確認する ・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	OK

【#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。

```
# show arp
IP Address       MAC Address        F   Rest   Interface Port
---------------- ------------------ --- ------ --------- ----
172.16.50.254    00:80:17:ef:6d:43      00434  lan50      1
172.16.50.255    ff:ff:ff:ff:ff:ff  P   perm   lan50
172.16.51.1      00:50:56:9e:67:3c      00694  lan51      1
172.16.51.253    a8:b2:da:5d:aa:a0  P   perm   lan51
172.16.51.255    ff:ff:ff:ff:ff:ff  P   perm   lan51
172.16.52.1      90:1b:0e:8b:ba:a2      01173  lan52      19
172.16.52.252    84:af:ec:f8:87:48      01124  lan52      1
172.16.52.253    a8:b2:da               m      lan52
172.16.52.255    ff:ff:ff               rm     lan52
    Entry:9
```


図 6.1.6-44 ルータ(実証用 L3 スイッチ)での arp テーブルの確認結果

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※。

```
# show ndp
IPv6 Address                              MAC Address        S F   Rest   Interface Port
----------------------------------------- ------------------ - --- ------ --------- ----
2001:2f8:103c:6050::1                     a8:b2:da:5d:aa:a0  R P   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  R P   perm   lan51
2001:2f8:103c:6052::1                     a8:b2:da:5d:aa:a0  R P   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  R P   perm   lan50
fe80::aab2:daff:fe5d:aaa0%lan51           a8:                   erm    lan51
fe80::aab2:daff:fe5d:aaa0%lan52           a8:                   erm    lan52
    Entry:9
```


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]# ls
command-fwlog-20210105  message-fwlog-20181205  message-fwlog-20200704  session-fwlog-20180128.gz  session-fwlog-20190326.gz  session-fwlog-20200521
command-fwlog-20210106  message-fwlog-20181206  message-fwlog-20200706  session-fwlog-20180129.gz  session-fwlog-20190327.gz  session-fwlog-20200522
command-fwlog-20210107  message-fwlog-20181208  message-fwlog-20200707  session-fwlog-20180130.gz  session-fwlog-20190328.gz  session-fwlog-20200523
command-fwlog-20210108  message-fwlog-20181210  message-fwlog-20200708  session-fwlog-20180131.gz  session-fwlog-20190329.gz  session-fwlog-20200524
command-fwlog-20210112  message-fwlog-20181211  message-fwlog-20200709  session-fwlog-20180201.gz  session-fwlog-20190330.gz  session-fwlog-20200525
command-fwlog-20210127  message-fwlog-20181212  message-fwlog-20200710  session-fwlog-20180202.gz  session-fwlog-20190331.gz  session-fwlog-20200526
command-fwlog-20210212  message-fwlog-20181213  message-fwlog-20200712  session-fwlog-20180203.gz  session-fwlog-20190401.gz  session-fwlog-20200527
command-fwlog-20210216  message-fwlog-20181218  message-fwlog-20200713  session-fwlog-20180204.gz  session-fwlog-20190402.gz  session-fwlog-20200528
error-fwlog-20170601    message-fwlog-20181219  message-fwlog-20200714  session-fwlog-20180205.gz  session-fwlog-20190403.gz  session-fwlog-20200529
error-fwlog-20170615    message-fwlog-20181220  message-fwlog-20200715  session-fwlog-20180206.gz  session-fwlog-20190404.gz  session-fwlog-20200530
error-fwlog-20170629    message-fwlog-20181221  message-fwlog-20200716  session-fwlog-20180207.gz  session-fwlog-20190405.gz  session-fwlog-20200531
error-fwlog-20170713    message-fwlog-20181225  message-fw                                                                    session-fwlog-20200601
error-fwlog-20170727    message-fwlog-20181227  message-fw                                                                    session-fwlog-20200602
message-fwlog-20171107  message-fwlog-20191107  session-fw                                                                    session-fwlog-20201231
message-fwlog-20171108  message-fwlog-20191108  session-fw                                                                    session-fwlog-20210101
message-fwlog-20171109  message-fwlog-20191111  session-fw                                                                    session-fwlog-20210102
message-fwlog-20171112  message-fwlog-20191112  session-fw                                                                    session-fwlog-20210103
message-fwlog-20171113  message-fwlog-20191113  session-fw                                                                    session-fwlog-20210104
message-fwlog-20171115  message-fwlog-20191114  session-fwlog-20170719.gz  session-fwlog-20180914.gz  session-fwlog-20191110.gz  session-fwlog-20210105
message-fwlog-20171119  message-fwlog-20191115  session-fwlog-20170720.gz  session-fwlog-20180915.gz  session-fwlog-20191111.gz  session-fwlog-20210106
message-fwlog-20171121  message-fwlog-20191118  session-fwlog-20170721.gz  session-fwlog-20180916.gz  session-fwlog-20191112.gz  session-fwlog-20210107
message-fwlog-20171122  message-fwlog-20191119  session-fwlog-20170722.gz  session-fwlog-20180917.gz  session-fwlog-20191113.gz  session-fwlog-20210108
message-fwlog-20171124  message-fwlog-20191120  session-fwlog-20170723.gz  session-fwlog-20180918.gz  session-fwlog-20191114.gz  session-fwlog-20210109
message-fwlog-20171127  message-fwlog-20191121  session-fwlog-20170724.gz  session-fwlog-20180919.gz  session-fwlog-20191115.gz  session-fwlog-20210110
message-fwlog-20171128  message-fwlog-20191122  session-fwlog-20170725.gz  session-fwlog-20180920.gz  session-fwlog-20191116.gz  session-fwlog-20210111
message-fwlog-20171130  message-fwlog-20191125  session-fwlog-20170726.gz  session-fwlog-20180921.gz  session-fwlog-20191117.gz  session-fwlog-20210112
message-fwlog-20171201  message-fwlog-20191126  session-fwlog-20170727.gz  session-fwlog-20180922.gz  session-fwlog-20191118.gz  session-fwlog-20210113
message-fwlog-20171203  message-fwlog-20191127  session-fwlog-20170728.gz  session-fwlog-20180923.gz  session-fwlog-20191119.gz  session-fwlog-20210114
message-fwlog-20171204  message-fwlog-20191128  session-fwlog-20170729.gz  session-fwlog-20180924.gz  session-fwlog-20191120.gz  session-fwlog-20210115
message-fwlog-20171205  message-fwlog-20191129  session-fwlog-20170730.gz  session-fwlog-20180925.gz  session-fwlog-20191121.gz  session-fwlog-20210116
message-fwlog-20171206  message-fwlog-20191201  session-fwlog-20170731.gz  session-fwlog-20180926.gz  session-fwlog-20191122.gz  session-fwlog-20210117
message-fwlog-20171207  message-fwlog-20191202  session-fwlog-20170801.gz  session-fwlog-20180927.gz  session-fwlog-20191123.gz  session-fwlog-20210118
message-fwlog-20171208  message-fwlog-20191203  session-fwlog-20170802.gz  session-fwlog-20180928.gz  session-fwlog-20191124.gz  session-fwlog-20210119
message-fwlog-20171209  message-fwlog-20191204  session-fwlog-20170803.gz  session-fwlog-20180929.gz  session-fwlog-20191125.gz  session-fwlog-20210120
message-fwlog-20171211  message-fwlog-20191205  session-fwlog-20170804.gz  session-fwlog-20180930.gz  session-fwlog-20191126.gz  session-fwlog-20210121
message-fwlog-20171212  message-fwlog-20191206  session-fwlog-20170805.gz  session-fwlog-20181001.gz  session-fwlog-20191127.gz  session-fwlog-20210122
message-fwlog-20171213  message-fwlog-20191209  session-fwlog-20170806.gz  session-fwlog-20181002.gz  session-fwlog-20191128.gz  session-fwlog-20210123
message-fwlog-20171214  message-fwlog-20191210  session-fwlog-20170807.gz  session-fwlog-20181003.gz  session-fwlog-20191129.gz  session-fwlog-20210124
message-fwlog-20171215  message-fwlog-20191211  session-fwlog-20170808.gz  session-fwlog-20181004.gz  session-fwlog-20191130.gz  session-fwlog-20210125
message-fwlog-20171216  message-fwlog-20191212  session-fwlog-20170809.gz  session-fwlog-20181005.gz  session-fwlog-20191201.gz  session-fwlog-20210126
message-fwlog-20171219  message-fwlog-20191213  session-fwlog-20170810.gz  session-fwlog-20181006.gz  session-fwlog-20191202.gz  session-fwlog-20210127
message-fwlog-20171220  message-fwlog-20191214  session-fwlog-20170811.gz  session-fwlog-20181007.gz  session-fwlog-20191203.gz  session-fwlog-20210128
message-fwlog-20171221  message-fwlog-20191215  session-fwlog-20170812.gz  session-fwlog-20181008.gz  session-fwlog-20191204.gz  session-fwlog-20210129
message-fwlog-20171222  message-fwlog-20191216  session-fwlog-20170813.gz  session-fwlog-20181009.gz  session-fwlog-20191205.gz  session-fwlog-20210130
message-fwlog-20171224  message-fwlog-20191217  session-fwlog-20170814.gz  session-fwlog-20181010.gz  session-fwlog-20191206.gz  session-fwlog-20210131
message-fwlog-20171226  message-fwlog-20191218  session-fwlog-20170815.gz  session-fwlog-20181011.gz  session-fwlog-20191207.gz  session-fwlog-20210201
message-fwlog-20171227  message-fwlog-20191219  session-fwlog-20170816.gz  session-fwlog-20181012.gz  session-fwlog-20191208.gz  session-fwlog-20210202
message-fwlog-20171230  message-fwlog-20191220  session-fwlog-20170817.gz  session-fwlog-20181013.gz  session-fwlog-20191209.gz  session-fwlog-20210203
message-fwlog-20180102  message-fwlog-20191222  session-fwlog-20170818.gz  session-fwlog-20181014.gz  session-fwlog-20191210.gz  session-fwlog-20210204
message-fwlog-20180104  message-fwlog-20191223  session-fwlog-20170819.gz  session-fwlog-20181015.gz  session-fwlog-20191211.gz  session-fwlog-20210205
message-fwlog-20180105  message-fwlog-20191224  session-fwlog-20170820.gz  session-fwlog-20181016.gz  session-fwlog-20191212.gz  session-fwlog-20210206
message-fwlog-20180109  message-fwlog-20191226  session-fwlog-20170821.gz  session-fwlog-20181017.gz  session-fwlog-20191213.gz  session-fwlog-20210207
message-fwlog-20180110  message-fwlog-20191227  session-fwlog-20170822.gz  session-fwlog-20181018.gz  session-fwlog-20191214.gz  session-fwlog-20210208
message-fwlog-20180111  message-fwlog-20191228  session-fwlog-20170823.gz  session-fwlog-20181019.gz  session-fwlog-20191215.gz  session-fwlog-20210209
message-fwlog-20180113  message-fwlog-20191229  session-fwlog-20170824.gz  session-fwlog-20181020.gz  session-fwlog-20191216.gz  session-fwlog-20210210
message-fwlog-20180114  message-fwlog-20191230  session-fwlog-20170825.gz  session-fwlog-20181021.gz  session-fwlog-20191217.gz  session-fwlog-20210211
message-fwlog-20180115  message-fwlog-20200104  session-fwlog-20170826.gz  session-fwlog-20181022.gz  session-fwlog-20191218.gz  session-fwlog-20210212
message-fwlog-20180116  message-fwlog-20200106  session-fwlog-20170827.gz  session-fwlog-20181023.gz  session-fwlog-20191219.gz  session-fwlog-20210213
message-fwlog-20180117  message-fwlog-20200107  session-fwlog-20170828.gz  session-fwlog-20181024.gz  session-fwlog-20191220.gz  session-fwlog-20210214
message-fwlog-20180118  message-fwlog-20200108  session-fwlog-20170829.gz  session-fwlog-20181025.gz  session-fwlog-20191221.gz  session-fwlog-20210215
message-fwlog-20180122  message-fwlog-20200109  session-fwlog-20170830.gz  session-fwlog-20181026.gz  session-fwlog-20191222.gz  session-fwlog-20210216
message-fwlog-20180123  message-fwlog-20200110  session-fwlog-20170831.gz  session-fwlog-20181027.gz  session-fwlog-20191223.gz  session-fwlog-20210217
message-fwlog-20180124  message-fwlog-20200112  session-fwlog-20170901.gz  session-fwlog-20181028.gz  session-fwlog-20191224.gz
message-fwlog-20180125  message-fwlog-20200114  session-fwlog-20170902.gz  session-fwlog-20181029.gz  session-fwlog-20191225.gz
```

実証用 FW 装置のセッションログ

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 connection denied. src= :6052::2002 dst=2404:6800:4008:C00::BC proto=tcp srcport=49830 dstport=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 session
initiated.  src=                    :6052:CC33:5D4C:9EAC:EC9D dst=2001:4860:4860::8888 proto=udp
srcport=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。