

5 IPv6 対応ユースケース(中小企業)

国内には中小企業の内部環境を IPv6 対応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 G」および「モデル I」を対象とした IPv6 対応ユースケースを示す。

5.1 モデル G: 中小企業 A

5.1.1 ユースケース企業の紹介

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、新潟県に拠点を置く企業(以下、A 社と呼称)で行った。A 社は、新潟県内に本社と支社があり、約 50 人の従業員が所属している。

(2) 既存のシステム環境

本ユースケースは、A 社内で利用している一般業務システム(メールや OA 機器等)だけでなく、A 社が開発し、ユーザへ販売しているオンプレミス業務アプリケーション、クラウド(外部 IaaS)上の業務アプリケーションに対して行った。A 社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 社のシステム環境内のノード数は 50 以上、サブネット数は 2 つ、2 拠点間をインターネット VPN で接続しており、拠点ごとに OCN 光 PPPoE(光電話あり)の回線を引き込んでいる。

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 アドレス等を静的に設定しているが、一部の PC にはルータ上に構築している DHCP で動的設定を行っている。メールや DNS のサーバは社内を立てず、外部のサービスを利用している。ファイアウォールはルータの機能で実現している。

5.1.2 要件定義

A社の内部環境を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5.1.2-1に示す。

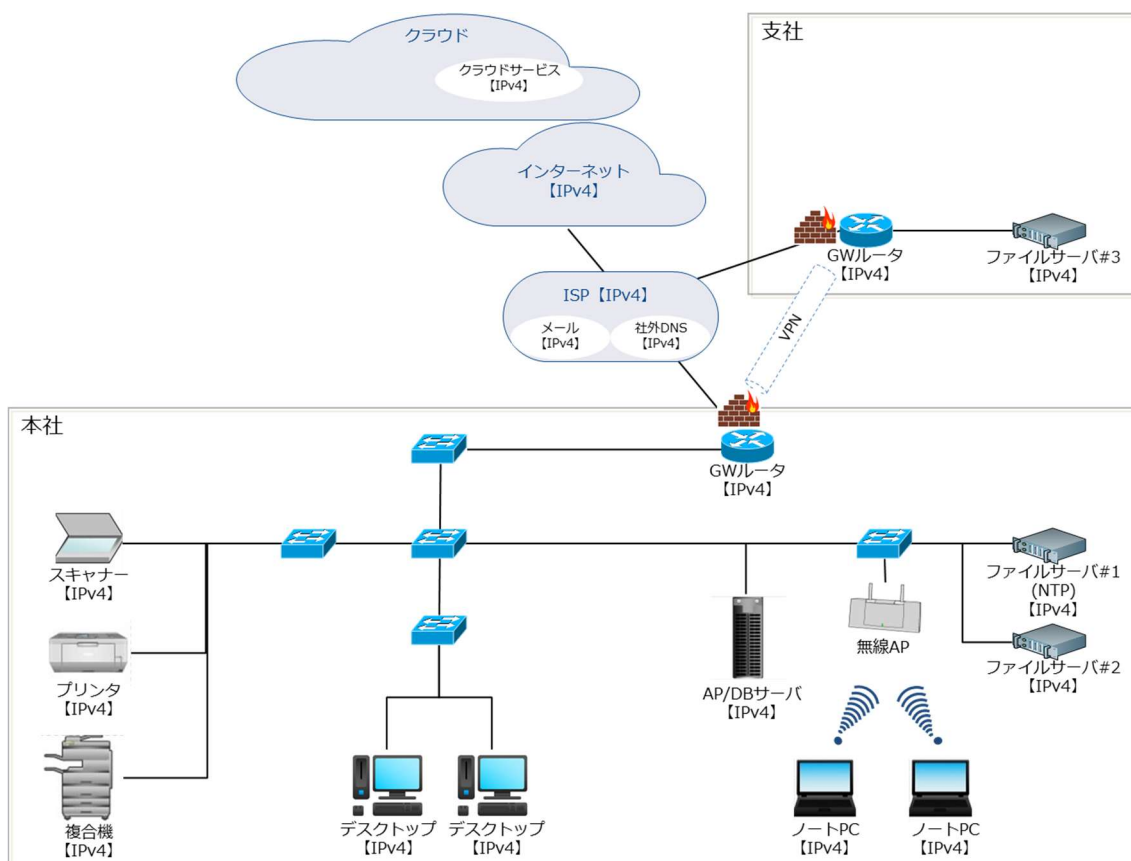


図 5.1.2-1 ネットワーク構成図イメージ

(2) 移行方式の明確化

本ユースケースにおいては、IPv6 対応の究極的な目標は IPv6 シングルスタックの実現であるが、世の中には IPv4 のみ対応の機器/サービスが残存していることから、IPv4/IPv6 デュアルスタック方式を採用した。既存環境への影響を最小限とするため、IPv6 回線を新設し、デュアルスタック方式にて IPv6 実証環境を既存環境と併設した構成で構築した。

(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 5.1.2-1 に示す。

表 5.1.2-1 機器等一覧イメージ

拠点	既存/ 新規	機器等	機器 メーカー等	機器名等	移行 対象	IPv6 対応 状況確認	導入方針
本社	既存	GW ルータ	YAMAHA	RTX830	-	対象外	変更不要
	新規	GW ルータ	YAMAHA	RTX830	○	IPv6 対応	新規
	既存	無線アクセス ポイント	BUFFALO	AirStation ProWAPM- 1266R	○	対象外 (L2 機器のため)	変更不要
	既存	ファイルサー バ	NEC	Express5800 T110i	○	IPv6 対応	変更要
	既存	複合機	Canon	imageRUNNE R ADVANCE C3520F III	○	IPv6 対応	変更要
	既存	プリンタ	Canon	LBP3980	○	IPv6 未対応	変更不要
	省略						
支社	既存	GW ルータ	YAMAHA	RTX830	-	対象外	変更不要
	新規	GW ルータ	YAMAHA	RTX830	○	IPv6 対応	新規
	既存	ファイルサー バ	NEC	Express5800 T110i	○	IPv6 対応	変更要
	省略						

5.1.3 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 5.1.3-1 に示す。ポイントは 2 点である。

1 点目は、IPv6 対応はレイヤー3(インターネットプロトコル)への影響が大きいので、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」と「IoT システムにおける検証」、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。

2 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
現行整理		[Bar chart showing current status]												
設計			設計書作成											
構築				回線契約/ 環境構築										
試験	疎通確認				[Bar chart]									
	ネットワークレベルの検証				一般業務における検証				IoTシステム における検証					
	LAN内アプリケーションレベルの検証								業務アプリケーション における検証					
	WAN越しアプリケーションレベルの検証										業務アプリケーション (クラウド)における検証			
試験結果の評価								[Bar chart]	[Bar chart]		[Bar chart]		[Bar chart]	

図 5.1.3-1 スケジュールイメージ(中小企業 A)

5.1.4 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2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 究極目標である IPv6 シングルスタックを意識し、IPv4 環境と IPv6 環境の分離(疎結合)を目指すこと

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

IPv6 アドレスは DHCPv6 を採用する⁴³。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(現行踏襲)
- ・IPv6 アドレス…DHCPv6 による自動設定

(b) DNS サーバ/デフォルトゲートウェイについて

指定する IPv6 アドレスは RA で割り当てる方式とする。

- ・IPv4 アドレス…静的アドレスによる手動設定(現行踏襲)
- ・IPv6 アドレス…RA による自動設定

(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、本ユースケースでは、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)

⁴³ 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。

(d) hosts ファイルについて

ファイルサーバが本社に 2 台、支社に 1 台あり、PC からファイルサーバへ接続する時に、現行同様 hosts ファイルで名前解決させる。現行設定はそのまま、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。

(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

IPv6 アドレスは DHCPv6 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(現行踏襲)
- IPv6 アドレス…DHCPv6 による自動設定

(b) DNS サーバ/デフォルトゲートウェイについて

指定する IPv6 アドレスは DHCPv6 で割り当てる方式とする。

- IPv4 アドレス…静的アドレスによる手動設定(現行踏襲)
- IPv6 アドレス…DHCPv6 による自動設定

(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、本ユースケースでは、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

ファイルサーバが本社に 2 台、支社に 1 台あり、PC からファイルサーバへ接続する時に、現行同様 hosts ファイルで名前解決させる。現行設定はそのまま、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。

(3) 有線接続の OA 機器 (スキャナー、プリンタ)

① 要素説明

一般業務で使用する有線接続のスキャナー、プリンタである。

② 方式設計

現行 OA 機器が IPv6 未対応のため、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(現行踏襲)
- IPv6 アドレス…設定不可

③ 特記事項

特になし。

(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

IPv6 シングルスタック方式とする。

(a) IP アドレスについて

IPv6 アドレスは DHCPv6 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…設定削除
- IPv6 アドレス…DHCPv6 による自動設定

③ 特記事項

複合機の仕様として、IPv6 シングルスタック方式でも対応可とあったが、IPv6 のみだと一部の機能が利用できなかった。最終的には方式設計を見直し、IPv4 アドレスの設定を戻し、デュアルスタック方式とした。

(5) インターネット接続や VPN 接続を制御する GateWay ルータ

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(ファイアウォール)、拠点間通信(インターネット VPN)を構築するための機器である。

② 方式設計

方式設計の方針に従い、既存の IPv4 シングルスタックのルータおよび回線とは別に、IPv6 シングルスタックのルータおよび回線を用意する。なお、現行 PPPoE で性能的な課題を抱えていないこと、相対コスト的に安いことより IPv6 回線も PPPoE(光電話なし)⁴⁴を採用した。

〈IPv4 シングルスタックのルータ(既存)〉

(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(現行踏襲)
- IPv6 アドレス…設定なし

(b) プロバイダ認証情報について

IPv4 用の PPPoE 認証情報のみ設定する(現行踏襲)。

(c) インターネット VPN について

アグレッシブモードを設定する(現行踏襲)。

(d) ファイアウォールについて

A 社内のセキュリティポリシーにしたがって設定する(現行踏襲)。

〈IPv6 シングルスタックのルータ(新規)〉

(e) 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(DHCPv6-PD)。

- IPv4 アドレス…設定なし(内部管理用のアドレスは手動設定)
- IPv6 アドレス…DHCPv6 による自動設定

(f) プロバイダ認証情報について

IPv6 用の PPPoE 認証情報のみ設定する。

⁴⁴ 現行に IPv4 回線は光電話ありのため、IPv6 の回線は光電話なしとした。

(g) インターネット VPN について

アグレッシブモードよりセキュアなメインモードを設定する。トンネル設定時に固定のグローバルアドレスが必要なため、ULA(Unique Local Unicast Address)を利用する。本社と支社間の通信は、ローカルではなくオープンなため、GUA(Global Unicast Address)での通信が必要である。GUA のプレフィックスは ISP から割り当てられており、変更される可能性があるため、FQDN で指定する。また、FQDN の名前解決に DDNS を利用する。通信の流れを図 5.1.4-1 に示す。

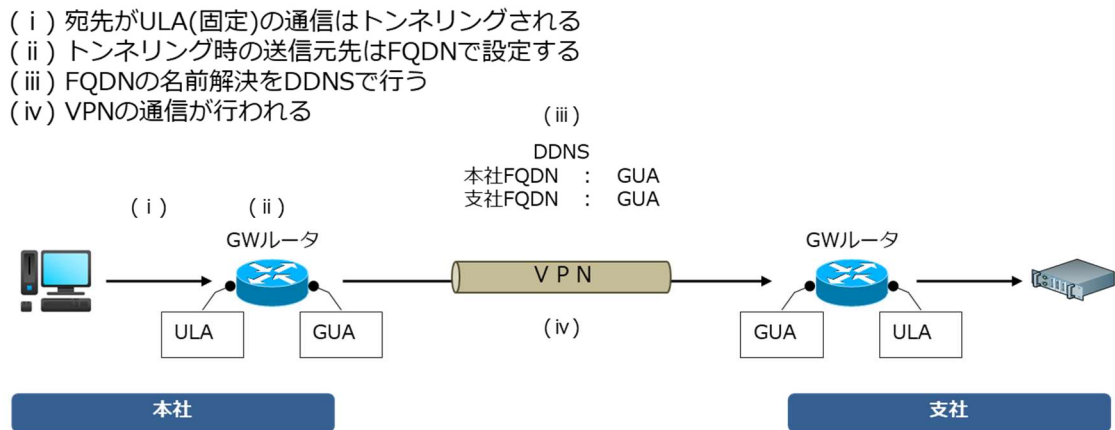


図 5.1.4-1 ULA および GUA を利用したインターネット VPN 通信の流れ

(h) ファイアウォールについて

A 社内で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

(g)インターネット VPN について、トンネル設定時に固定のグローバルアドレスが必要なため、ULA を利用した。しかし、RFC4193 で定義されているように ULA は、グローバルなスコープではあるが、サイト内でのローカルな通信で利用するといった用途での利用が想定されている。ULA は限られた範囲での通信に利用され、IPv6 インターネットとの通信を行うためには、別途 GUA が利用される。また、ULA は、万が一パケットが外に漏れた時を想定し、他のアドレスとの競合が発生しにくいランダム値を含ませる必要がある。そのため、本ユースケースでは、RFC4086 に準拠した生成方式で ULA を割り当てている。

(h)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⁴⁵、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。

⁴⁵ 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。

(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) 業務アプリケーションを処理する AP サーバや DB サーバ(WEB 機能含む)

① 要素説明

A 社が開発し、ユーザへ販売している業務アプリケーションを開発するサーバである。クライアント PC が利用する業務アプリケーションの動作環境(データベース含む)を、仮想環境のゲスト OS として構築する。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。A 社のユーザへの影響を避けるため、既存の AP/DB サーバにシステム修正変更は行わず、ユースケース用に、新規 AP/DB サーバを構築した。新規 AP/DB サーバを既存 AP/DB 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(現行同等)
- ・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(現行同等)
- ・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

AP/DB サーバは名前解決による通信を行わないため、追加設定なし。

(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、ULA 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 を認証し、ファイル共有を行うサーバ機器ある。

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(現行踏襲)
- 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(現行踏襲)
- 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(CentOS)においてもクライアント PC と同様に、IPv4 と IPv6 の優先設定が存在する。ユースケースのため、本社側のファイルサーバはデフォルトの IPv6 優先の状態、支社側のファイルサーバは IPv4 優先の状態を検証する。

(d) hosts ファイルについて

ファイルサーバ間で認証同期の通信を行っており、通信時に hosts ファイルで名前解決する。現行設定はそのままで、IPv6 分の名前解決を hosts ファイルに追記する。

(e) 認証同期設定について

A 社の社内環境における LDAP 認証は本社と支社のマルチマスターで構成されており、支社側のファイルサーバ 3 は本社側のファイルサーバ 1 の認証情報を一定間隔で取得し、同期している。IPv6 接続において認証情報が同期されるよう、ファイルサーバ 3 の LDAP 設定ファイルの接続先アドレスを IPv6 形式に変更する。

③ 特記事項

ファイルサーバの静的アドレスには、ULA を設定する。

(9) 上記以外のネットワーク接続デバイス(ビデオ会議)

① 要素説明

本社と支社間を接続し、双方向に映像および音声通話を行うビデオ会議システムである。

② 方式設計

IPv4 との通信が不要のため、IPv6 シングルスタック方式とする。IPv6 のインターネット VPN を利用する。

(a) IP アドレスについて

インターネット VPN を利用するため、ULA を設定する。

- ・IPv4 アドレス…設定不要
- ・IPv6 アドレス…静的アドレスによる手動設定

③ 特記事項

特になし。

(10)社外のメールサービス

① 要素説明

クライアント PC からメールの送受信(SMTP、POP)を行う外部メールサービス(MTA)である。

② 方式設計

現行メールサービスが IPv6 未対応のため、IPv4 シングルスタック方式のままとする。

(a) MUA 側の設定について

MTA の指定は FQDN で行っている。メールサービスが IPv6 未対応のため、社外の DNS では A レコードのみ応答され、IPv4 通信のみ可能となる。

③ 特記事項

(a)MUA 側の設定について、IPv6 優先 PC の場合、DNS で名前解決した後、IPv4 通信に自動で切り替わるため、利用上の問題は特になしと想定し、試験を行った。

(11)社外のクラウドサービス

① 要素説明

A 社が開発し、ユーザへ販売している業務アプリケーションを動作させるクラウド(IaaS)である。クライアント PC が利用する業務アプリケーションの動作環境(データベース含む)を、クラウドサービス上の仮想サーバ環境内に構築する。

② 方式設計

2 種類のクラウドサービスを利用している。さくらクラウド⁴⁶は IPv6 対応のため、IPv4/IPv6 デュアルスタック方式とする。IDC サービス⁴⁷は IPv6 未対応のため、IPv4 シングルスタック方式とする。A 社のユーザへの影響を避けるため、既存のさくらクラウドにシステム修正変更は行わず、ユースケース用に、新規さくらクラウド上に新規仮想サーバを構築した。新規さくらクラウド上の仮想サーバを既存さくらクラウドのものと同等設定(IPv4 シングルスタック)にした上で、IPv6 設定を追加する。

<さくらクラウド(IaaS)について>

(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
(サービス提供者から払い出されたグローバルアドレス)
- IPv6 アドレス…同上

<IDC サービス(IaaS)について>

(b) 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(現行踏襲)
- IPv6 アドレス…設定不可

③ 特記事項

特になし。

⁴⁶ さくらインターネット社のクラウドサービスである。

⁴⁷ NS・コンピュータサービス社のクラウドサービスである。

以上を踏まえ、IPv6 対応後のシステム構成図を図 5.1.4-1 に示す。

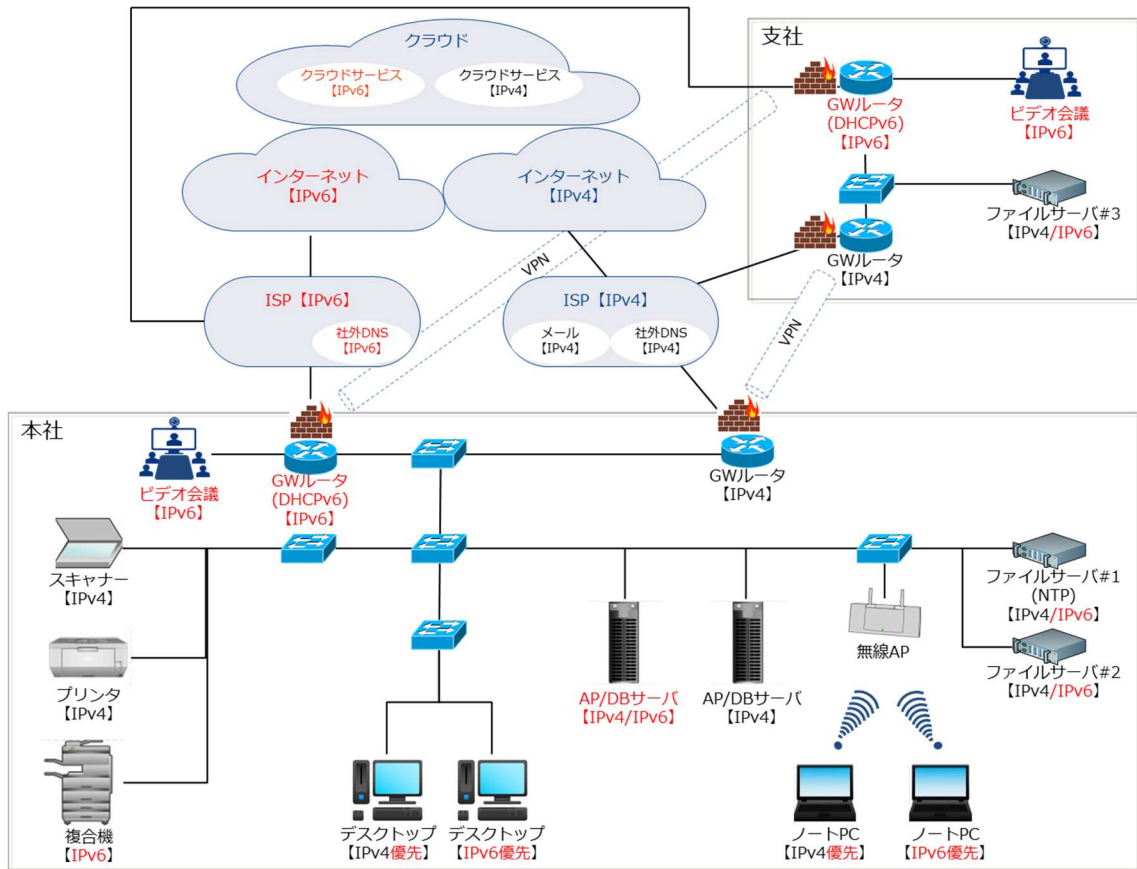


図 5.1.4-1 IPv6 対応後のネットワーク構成図

5.1.5 構築

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 5.1.5-1 に示す。

表 5.1.5-1 IPv4/IPv6 デュアルスタックを構築する各要素のスペック

拠点	設定	機器等	仕様例	備考
本社	IPv6 優先	デスクトップ PC	DELL vostro 2421 OS Windows10 Pro CPU Core i5-3337U @1.80GHz メモリ 8GB HDD 512GB	・一般業務や業務アプリケーション利用等
	IPv6 優先	ノート PC	thinkpad E580 OS Windows10 Pro CPU Core i5-8250U @1.60GHz メモリ 16GB HDD 256GB	・一般業務や業務アプリケーション利用等
	IPv4 優先	デスクトップ PC	CF-SV7HM9VS OS Windows10 Pro CPU Core i5-8250U @1.60GHz メモリ 16GB SSD 256GB	・一般業務や業務アプリケーション利用等
	IPv4 優先	ノート PC	CF-SV7HM9VS OS Windows10 Pro CPU Core i5-8250U @1.60GHz メモリ 16GB SSD 256GB	・一般業務や業務アプリケーション利用等
	IPv4/ IPv6	複合機	imageRUNNER ADVANCE C3520F III	・印刷やスキャン
	IPv4	スキャナー	Offirio ES-7000H	・スキャン
	IPv4	プリンタ	LBP3980	・印刷

拠点	設定	機器等	仕様例	備考
	IPv4/ IPv6	ファイルサーバ#1	OS CentOS CPU Intel Xeon CPU E3-1220 v5 メモリ 20.0GB HDD 465GB	・社内の情報資産管理や共有 ・NTP マネージャー
	IPv4/ IPv6	ファイルサーバ#2	OS CentOS CPU Intel Xeon CPU E3-1220 v5 メモリ 20.0GB HDD 465GB	・社内の情報資産管理や共有
	IPv4	AP サーバ/ DB サーバ	OS:Windows Server 2012 R2 CPU:Intel Core2 Duo CPU メモリ:8GB HDD:1TB OS:Windows Server 2008 R2 Standard CPU:Intel Xeon CPU E3-1220 v5 メモリ:20GB HDD:500GB	・業務アプリケーション動作
	IPv4/ IPv6	検証用 AP サーバ/ DB サーバ	OS Windows Server 2019 standard CPU Intel Xeon CPU E2124 メモリ 64.0GB HDD 1TB	・業務アプリケーション動作
	IPv4	GW ルータ	YAMAHA RTX-830	・ルーティング ・ファイアウォール(FW)
	IPv6	GW ルータ	YAMAHA RTX-830	・ルーティング ・ファイアウォール(FW)
	IPv4	無線 AP (アクセスポイント)	Air Station Pro WAPM-1266R	・デバイスの無線中継
	IPv6	ビデオ会議 デバイス	Polycom Group310/500-720p	・ビデオ会議

拠点	設定	機器等	仕様例	備考
支社	IPv4/ IPv6	ファイルサーバ#3	OS CentOS CPU Intel Xeon CPU E3-1220 v5 メモリ 20.0GB HDD 465GB	・社内の情報資産管理や共有
	IPv4	GW ルータ	YAMAHA RTX-830	・ルーティング ・ファイアウォール(FW)
	IPv6	GW ルータ	YAMAHA RTX-830	・ルーティング ・ファイアウォール(FW)
	IPv6	ビデオ会議 デバイス	Polycom Group310/500-720p	・ビデオ会議
共通	IPv4	ISP	光NEXTハイスピード データ送信 100Mbps データ受信 200Mbps マルチホームなし 光電話あり	・インターネットおよび VPN 接続
	IPv6	ISP	光NEXTギガライン データ送受信 1Gbps マルチホームなし 光電話なし	・インターネットおよび VPN 接続
	IPv4	メールサービス	WEBARENA	・メール
	IPv4	IaaS	さくらクラウド IDC サービス	・外部システム・商用サービス等動作
	IPv4/ IPv6	IaaS	さくらクラウド	・外部システム・商用サービス等動作

つぎに、IPv6 対応するために行った各機器への設定内容を示す⁴⁸。

⁴⁸ IPv6 に関するパラメータのみであり、IPv6 に無関係な構築パラメータは割愛する。

(1) ルータの設定

ルータの管理画面上で以下 1~4 のコマンドを実行し、基本設定、ネット接続、パケットフィルタ、VPN の設定を行った。

項番	設定内容の詳細
1	【ルータ基本設定(日付、管理パスワード、LAN 側の IP アドレス)】 login password * administrator password * ipv6 prefix 1 dhcp-prefix@pp1::/64 ipv6 prefix 2 fde9:c477:6a1b:1::/64(本社) ipv6 prefix 2 fde9:c477:6a1b:2::/64(支社) ipv6 lan1 address dhcp-prefix@pp1::1/64 ipv6 lan1 address fde9:c477:6a1b:1::1/64(本社) ipv6 lan1 address fde9:c477:6a1b:2::1/64(支社) ipv6 lan1 rtadv send 1 2 o_flag=on ipv6 lan1 dhcp service server
2	【IPv6 アドレスでのインターネット接続設定】 pp select 1 pp always-on on ppoe use lan2 ppoe auto disconnect off pp auth accept pap chap pp auth myname (ISP と接続する ID) (ISP と接続するパスワード) ppp lcp mru on 1454 ppp ccp type none ppp ipv6cp use on ipv6 pp rip send off ipv6 pp dhcp service client pp enable 1 ipv6 route default gateway pp 1 dns server pp 1

項番	設定内容の詳細
3	<p>【拠点間の VPN 接続】</p> <p>※本社側ルータには、支社側の ULA のプレフィックス(fde9:c477:6a1b:2)をトンネルするように設定し、支社側ルータには、本社側の ULA のプレフィックス(fde9:c477:6a1b:1)をトンネルするよう設定している。</p> <p>[本社側]</p> <pre> ipv6 route fde9:c477:6a1b:2::/64 gateway tunnel 1 tunnel select 1 tunnel name *** ipsec tunnel 1 ipsec sa policy 1 1 esp aes256-cbc sha256-hmac ipsec ike version 1 2 ipsec ike keepalive log 1 on ipsec ike keepalive use 1 on rfc4306 10 6 0 ipsec ike local name 1 ***.i.open.ad.jp fqdn ipsec ike pre-shared-key 1 text (PSK) ipsec ike remote name 1 ***.i.open.ad.jp fqdn ipv6 tunnel tcp mss limit auto tunnel enable 1 </pre> <p>[支社側]</p> <pre> ipv6 route fde9:c477:6a1b:1::/64 gateway tunnel 1 tunnel select 1 tunnel name *** ipsec tunnel 1 ipsec sa policy 1 1 esp aes256-cbc sha256-hmac ipsec ike version 1 2 ipsec ike keepalive log 1 on ipsec ike keepalive use 1 on rfc4306 10 6 0 ipsec ike local name 1 ***.i.open.ad.jp fqdn ipsec ike pre-shared-key 1 text (PSK) ipsec ike remote name 1 ***.i.open.ad.jp fqdn ipv6 tunnel tcp mss limit auto tunnel enable 1 </pre>

項番	設定内容の詳細
4	<p>【セキュリティ・ファイアウォール設定(パケットフィルタ)】</p> <pre> ipv6 filter 200000 pass * * icmp6 * * ipv6 filter 200001 pass * * tcp * ident ipv6 filter 200002 pass * * udp * 546 ipv6 filter 200110 pass fde9:c477:6a1b:2::/64 fde9:c477:6a1b:1::/64 * * * (本社) ipv6 filter 200110 pass fde9:c477:6a1b:1::/64 fde9:c477:6a1b:2::/64 * * * (支社) ipv6 filter 200098 reject * * * * * ipv6 filter 200099 pass * * * * * ipv6 filter dynamic 200080 * * ftp ipv6 filter dynamic 200081 * * domain ipv6 filter dynamic 200082 * * www ipv6 filter dynamic 200083 * * smtp ipv6 filter dynamic 200084 * * pop3 ipv6 filter dynamic 200085 * * submission ipv6 filter dynamic 200098 * * tcp ipv6 filter dynamic 200099 * * udp pp select 1 ipv6 pp secure filter in 200000 200001 200002 ipv6 pp secure filter out 200099 dynamic 200080 200081 200082 200083 200084 200085 200098 200099 pp enable 1 tunnel select 1 ipv6 tunnel secure filter in 200110 tunnel enable 1 </pre>

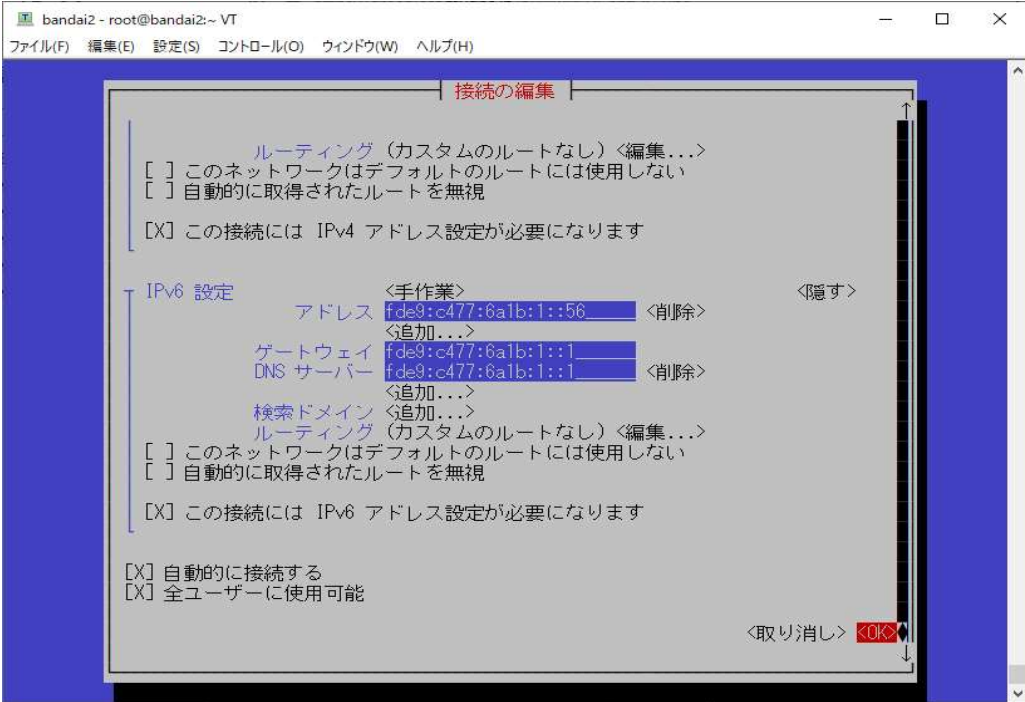
(2) 複合機の設定

複合機上のパネル操作を行い、IPv6 のシングルスタック(最終的にはデュアルスタック)設定を行った。

項番	設定内容の詳細
1	<p>【IPv6 アドレスの追加設定】 複合機のパネルから IPv6 アドレスの設定を行う。 「環境設定」→「ネットワーク」→「TCP/IP 設定」→「IPv6 設定」 ・「DHCPv6 を使用」を押下⇒「OK」を押下</p>
2	<p>【IPv4 アドレスの削除】(シングルスタック設定にする場合) 複合機のパネルから IPv4 アドレスの無効化を行う。 「環境設定」→「ネットワーク」→「TCP/IP 設定」→「IPv4 設定」 ・「IPv4 を使用」の「OFF」ボタンを押下⇒OK を押下</p> <p>※最終的に IPv6 シングルスタックからデュアルスタックでの運用を行うことにしたため、上記設定は「ON」に戻した。</p>

(3) ファイルサーバの設定

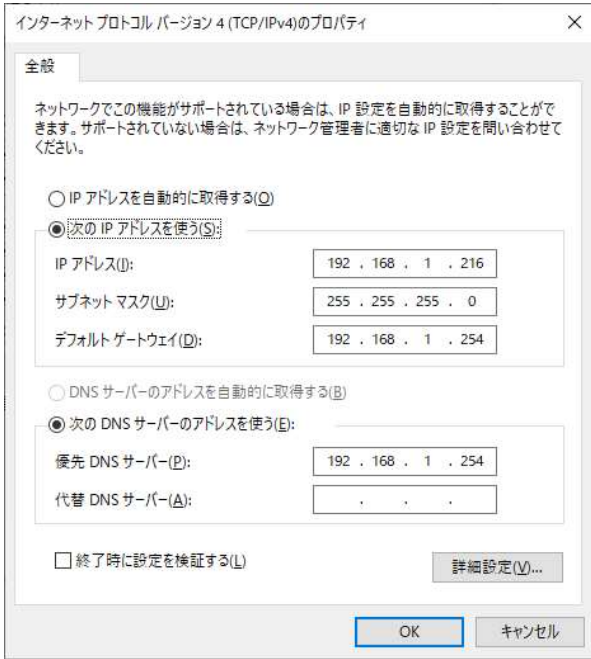
ファイルサーバ上で下記の設定を行い、IPv6 デュアルスタックに対応するファイルサーバを構築する。

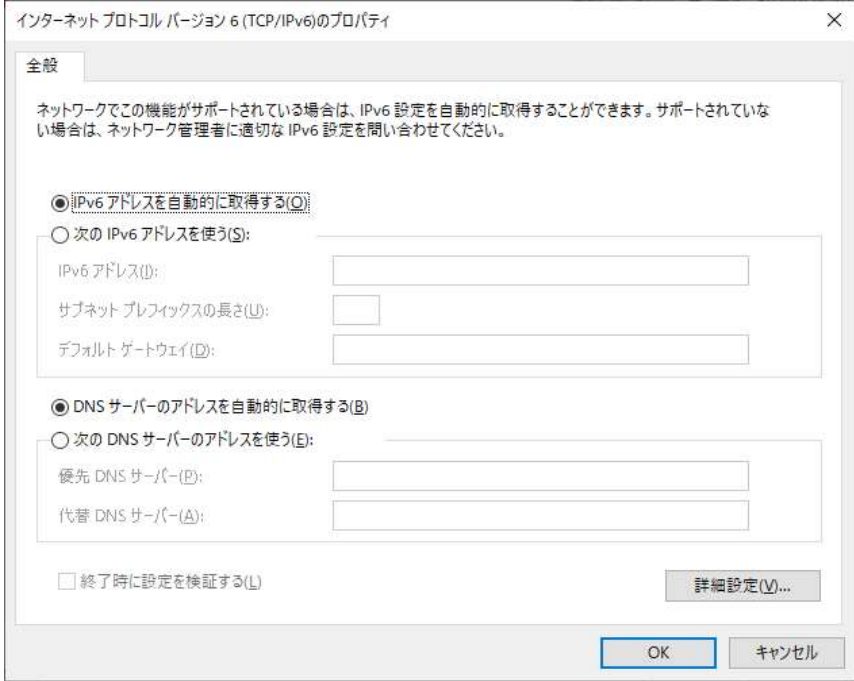
項番	設定内容の詳細
1	<p>【本体のネットワーク設定】</p> <p>各ファイルサーバ上で nmtui により、IPv6 アドレスの追加設定を行う。IPv6 アドレスは、社内で管理されているユニークローカルアドレスを設定する。</p> <p>fde9:c477:6a1b:1::56/64 (bandai2)</p> <p>fde9:c477:6a1b:1::57/64 (yachiyo2)</p> <p>fde9:c477:6a1b:2::11/64 (park2)</p> <p>(設定画面の例)</p> 
2	<p>【hosts ファイルの設定】</p> <p>/etc/hosts に IPv6 アドレスを追記する。</p> <p>===== fde9:c477:6a1b:1::56 bandai2 bandai2v6 fde9:c477:6a1b:1::57 yachiyo2 yachiyo2v6 fde9:c477:6a1b:2::11 park2 park2v6</p>

項番	設定内容の詳細
3	<p>【samba 設定】</p> <p>smb.conf の公開対象アドレスに IPv6 形式のアドレスを追加する(赤字部分)</p> <pre>[global] hosts allow =<既存の IPv4 アドレス> fde9:c477:6a1b:2::/64 fde9:c477:6a1b:1::/64 fe80::/64</pre> <p>また、参照先 LDAP サーバ設定(ldapsam 部分)を IPv6 アドレスに変更する。</p> <pre>passdb backend = ldapsam:"ldap://[:1] ldap://[fde9:c477:6a1b:2::11]" (bandai2) passdb backend = ldapsam:"ldap://[fde9:c477:6a1b:1::56] ldap://[fde9:c477:6a1b:2::11]" (yachiyo2) passdb backend = ldapsam:"ldap://[:1] ldap://[fde9:c477:6a1b:1::56]" (park2)</pre>
4	<p>【LDAP 設定】</p> <p>LDAP の同期設定(ファイルサーバ 3(支社側)のみ)</p> <pre>#vi syncrepl-modv6.ldif dn: olcDatabase={2}hdb,cn=config changetype: modify replace: olcSyncRepl olcSyncRepl: rid=001 provider=ldap://bandai2v6:389/ bindmethod=simple binddn="cn=Manager,dc=marugo-system,dc=co,dc=jp" credentials=***** searchbase="dc=marugo-system,dc=co,dc=jp" scope=sub schemachecking=on type=refreshOnly retry="60 10 300 10" interval=00:00:05:00 # ldapmodify -Y EXTERNAL -H ldapi:/// -f syncrepl-modv6.ldif</pre>

(4) 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。


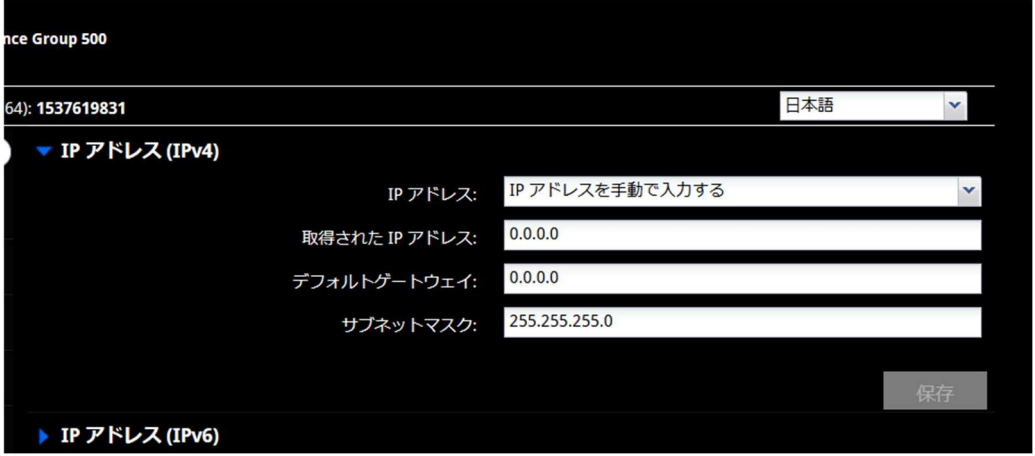
項番	設定内容の詳細
1	<p>【IPv4 アドレスの設定】</p> <p>接続しているネットワーク アダプタ(LAN or Wi-Fi)のプロパティから固定 IP を設定する。</p> <div data-bbox="544 488 1136 1144"></div> <p>※IP アドレスは社内で管理している固定アドレスを設定する。</p>

項番	設定内容の詳細
2	<p>【IPv6 アドレスの設定】</p> <p>接続しているネットワーク アダプタ(LAN or Wi-Fi)のプロパティから動的 IP が設定されるようにする。(※Windows のデフォルト設定であることを確認する)</p> 
3	<p>【Hosts の設定追加】</p> <p>Hosts ファイルに IPv6 の社内サーバのアドレスを追加する(ファイルサーバごとに割り当てたユニークローカルアドレスを設定する)</p> <p>¥Windows¥System32¥drivers¥etc¥hosts</p> <pre> ===== ## IPv6 fde9:c477:6a1b:1::56 bandai2 fde9:c477:6a1b:1::57 yachiyo2 fde9:c477:6a1b:2::11 park2 ===== </pre>

項番	設定内容の詳細																					
4	<p>【IPv4 アドレスの優先設定】</p> <p>IPv4 設定がループバックより優先されるように、コマンドを実行する。 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)</p> <pre>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</pre> <p>上記の設定を行ったら、PC を再起動する。</p>																					
5	<p>【IPv4/IPv6 優先設定を確認】</p> <p>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。</p> <pre>netsh interface ipv6 show prefixpolicies</pre> <p>(実行例)</p> <table border="1"> <thead> <tr> <th>優先順位</th> <th>ラベル</th> <th>プレフィックス</th> </tr> </thead> <tbody> <tr> <td>50</td> <td>0</td> <td>::ffff:0:0/96 (IPv4 マップ)</td> </tr> <tr> <td>40</td> <td>1</td> <td>::1/128 (ループバック)</td> </tr> <tr> <td>30</td> <td>2</td> <td>::/0 (IPv6 通信全般)</td> </tr> <tr> <td>20</td> <td>3</td> <td>2002::/16 (6to4)</td> </tr> <tr> <td>10</td> <td>4</td> <td>::/96 (IPv4 互換)</td> </tr> <tr> <td>5</td> <td>5</td> <td>2001::/32 (Teredo)</td> </tr> </tbody> </table>	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)
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)																				

(5) ビデオ会議の設定

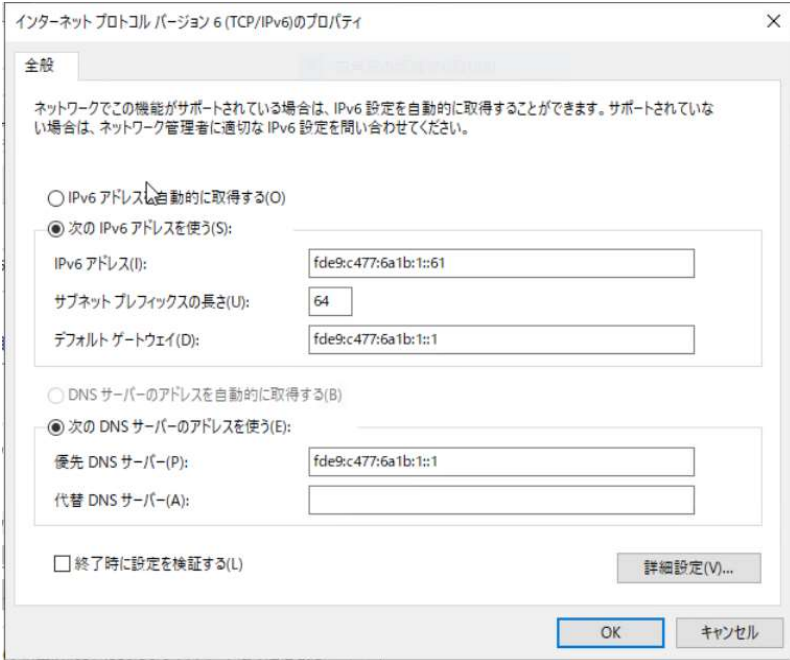
マニュアルに従ったシステムの初期セットアップ実施後、IPv6 に関連する以下の設定を実施した(本社側、支社側)

項番	設定内容の詳細
1	<p>【IPv6 アドレス設定】</p> <p>ビデオ会議用に割り当てた本社側、支社側の IPv6 アドレス(ULA)を、それぞれの拠点で手動設定する。</p>  <p>The screenshot shows a configuration page for 'ce Group 500'. It includes a language dropdown set to '日本語' and a sub-network ID '64): 1537619831'. Under the 'IP アドレス (IPv6)' section, the following settings are visible: 'IPv6 が有効:' is checked; 'IP アドレス:' is set to 'IP アドレスを手動で入力する'; 'リンク(ローカル):' is 'fe80::1/64'; 'サイト(ローカル):' is 'fde9:c477:6a1b:1::50/64'; 'グローバルアドレス:' is '::/128'; and 'デフォルトゲートウェイ:' is 'fde9:c477:6a1b:1::1'. A '保存' button is at the bottom right. A 'DNS サーバ' link is at the bottom left.</p>
2	<p>【IPv4 アドレス無効化設定】</p> <p>IPv4 アドレスに「0.0.0.0」を設定して無効化する。</p>  <p>The screenshot shows a configuration page for 'nce Group 500'. It includes a language dropdown set to '日本語' and a sub-network ID '64): 1537619831'. Under the 'IP アドレス (IPv4)' section, the following settings are visible: 'IP アドレス:' is set to 'IP アドレスを手動で入力する'; '取得された IP アドレス:' is '0.0.0.0'; 'デフォルトゲートウェイ:' is '0.0.0.0'; and 'サブネットマスク:' is '255.255.255.0'. A '保存' button is at the bottom right. A link for 'IP アドレス (IPv6)' is at the bottom left.</p>

(6) AP/DB サーバの設定

AP/DB サーバ上に、仮想環境のホスト OS となる VMWare Sphere とゲスト OS である Windows Server をセットアップする。

項番	設定内容の詳細
1	【ハイパーバイザー環境のセットアップ】 AP/DB サーバに VMWare vSphere (ESXi) の仮想環境を構築する。 vSphere のマニュアルに従い、空き HDD 領域にセットアップする。
2	【IPv6 アドレスの設定 (ホスト OS、ESXi)】 インストールした ESXi に、静的な IPv6 アドレスを固定設定する。 (※上記アドレスは、WEB ブラウザから VMware vSphere の管理画面に接続する時に使用するためのもの) 設定値: fde9:c477:6a1b:1::60/64 ※プレフィックス部分(/64)は指定しないとエラーとなるため、指定必須。
3	【ゲスト OS 環境の構築】 VMware vSphere 上でゲスト OS (Windows Server) をインストールする。 (特記事項なし)

項番	設定内容の詳細
4	<p>【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。</p> 
5	<p>【ゲスト OS 環境の DB 環境構築】 ゲスト OS で、DBMagic 付属の Pervasive.SQL をセットアップする。 (特記事項なし)</p>
6	<p>【クライアント環境のアプリケーション実行環境構築】 クライアント PC に、さんちよくアプリケーションの実行環境をセットアップする。 実行環境のセットアップ後、設定ファイル(Magic.ini)に IPv6 形式で DB の接続先(APDB サーバ)を指定する。</p> <p>(設定例)</p> <pre>[MAGIC_LOGICAL_NAMES] HAMAS = ¥¥fde9-c477-6a1b-1--61.ipv6-literal.net¥sanchoku-xpa2.5¥HAMAS¥ HADAT = ¥¥fde9-c477-6a1b-1--61.ipv6-literal.net¥sanchoku-xpa2.5¥HADAT¥ CLIENT = ¥¥fde9-c477-6a1b-1--61.ipv6-literal.net¥sanchoku-xpa2.5¥CLIENT¥</pre> <p>クライアント PC でアプリケーションの実行ファイルを起動し、さんちよくのメインメニューが起動するか確認する。</p>

(7) クラウド環境の設定

外部クラウドサービス(さくらクラウド)に POS システムが動作する仮想サーバを作成し、クラウドの仮想環境で IPv6 の有効化設定を行う。その他、ドメイン指定で仮想環境に接続できるように、DNS サービスに仮想環境の IPv6 アドレスを正引き登録する。

項番	設定内容の詳細
1	<p>【仮想サーバ環境のセットアップ】</p> <p>さくらクラウドのマニュアルに従い、仮想サーバを追加する。</p> <p>※Windows Server のバージョンは 2016、プランは「for RDS」を指定</p>
2	<p>【IPv6 アドレスの有効化設定】</p> <p>ネットワーク設定で IPv6 を利用可能にする。</p> <p>「ルータ+スイッチ」を作成する。</p> <p>名前: 任意の名称</p> <p>ルータ: 「はい」</p> <p>IPv6 アドレス: 「有効」</p> <p>その他はデフォルトを指定する。</p> <p>※「IPv6 の逆引き設定」は必須ではないため、設定なし。</p> <p>※参考</p> <p>https://manual.sakura.ad.jp/cloud/network/switch/ipv6.html</p> <ul style="list-style-type: none">•IPv6 の使用を開始する•IPv6 アドレスに逆引き DNS を設定する

項番	設定内容の詳細
3	<p>【クラウド環境のファイアウォール設定】</p> <ul style="list-style-type: none"> ・IPv4 用のパケットフィルタ設定 →許可する送信元の指定で、A 社のグローバル IP を設定する。 ・IPv6 用のパケットフィルタ設定 →設定なし ※さくらクラウドでは IPv6 のパケットフィルタは利用不可 (2/21 現在) ※参考: https://manual.sakura.ad.jp/cloud/network/packet-filter.html <p>注意事項</p> <ul style="list-style-type: none"> ● ルール設定を変更した場合、該当のパケットフィルタを設定している NIC へのフィルタ設定もすぐに反映されます。 ● IPv6 には対応していません。 ● パケットフィルタによって破棄したパケットは、対象サーバに到達しないため、アクティビティにあるNICグラフ上に表示されません。
4	<p>仮想サーバで以下のセットアップを実施する(詳細は割愛)</p> <ul style="list-style-type: none"> ・ActiveDirectoryのインストール、設定 ・リモートデスクトップのインストール、設定 ・ネットワーク設定(ルータの設定内容に合わせる)
5	<ul style="list-style-type: none"> ・仮想サーバで業務用アプリケーションをセットアップする(特記事項なし) ・リモートデスクトップに接続する RDP ファイルを編集し、さくらクラウドの IPv6 アドレスを接続先に指定する(IPv6 アドレス指定で接続する場合) (設定例) full address:s:2401:2500:109:1024::196 ドメイン名指定で接続を行う場合は、上記にドメイン名を記載する。 (設定例) full address:s:<ドメイン名>
6	<p>クライアント PC でサーバ上のアプリケーションが起動できるよう、RemoteApp の設定を行う。</p> <p>リモートデスクトップサービス』→『QuickSessionCollection』→『RemoteApp プログラムの公開』で、『Magic xpa 2.5 Enterprise Client』をチェックする。</p> <p>クライアント PC で RDP ファイルを起動して、POSMARU のメインメニューが起動するか、確認する。</p>

項番	設定内容の詳細
7	<p>さくらクラウドの仮想サーバに割り振られた IPv6 アドレスを、DNS に正引き登録する。 正引き登録は marugo-system.co.jp ドメインを管理している、WEBArena の DNS サービスに接続して「ゾーンレコードの新規追加」で行う。</p> <p>(設定例)</p> <div data-bbox="325 506 1326 936" style="border: 1px solid black; padding: 10px;"> <p>ゾーンレコードの新規追加</p> <p>TYPEを選択してください</p> <p>NAME sakura-ipv6 .marugo-system.co.jp</p> <hr/> <p>TYPE AAAA</p> <hr/> <p>TTL 3600 5m 10m 3h 1d 1w 10d</p> <hr/> <p>VALUE 2401:2500:109:1024:0:0:0:196</p> </div>

5.1.6 試験

本ユースケースで実施した内容と結果を示す。

5.1.6.1 実証内容と結果

1. ネットワークレベルの検証

5.1.5 で構築したシステム環境において、無線ネットワークおよび有線ネットワークに問題ないことを、一般業務における検証、IoT システムにおける検証の 2 つの観点で検証した。

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加え、遠隔拠点にあるファイルサーバとユーザ認証情報(LDAP)を同期可能か検証した。IoT システムにおける検証では、本社と支社間のビデオ会議の通信を検証した。

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 4 件、IPv6 対応における留意事項が 6 件発生した。

実証結果に伴い設計を見直した点が 1 つある。複合機について、IPv6 シングルスタック方式だと一部の機能が利用できなかったため、対応として IPv4/IPv6 デュアルスタック方式とした。

(1) 一般業務における検証について

5.1.4 (5)の通り、IPv4 の経路(ルータおよび回線)と、IPv6 の経路(ルータおよび回線)を分離させ、接続先の IPv6 対応状況で、通過する経路が切り替わるような設計としている。まずは、通信経路を明確にするため、IPv4 経路側のルータと IPv6 経路側のルータを切り離した状態で、①から③のシナリオを IPv4 および IPv6 それぞれで検証した。切り離した状態のイメージを図 5.1.6-1 に示す。

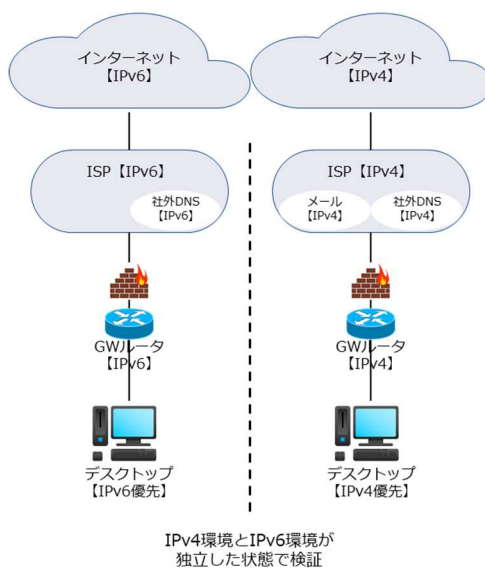


図 5.1.6-1 IPv4 経路と IPv6 経路を分離

① 疎通確認

各機器に対して 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 未対応のコンテンツ(A 社で現行利用しているメール等)の場合、利用できないことを検証する。

③ ファイルサーバの利用(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可能であることを検証する。また、変更した認証情報(パスワード)がファイルサーバ間で同期されることを検証する。

つぎに、IPv4 経路側のルータと IPv6 経路側のルータを接続し、IPv4 と IPv6 を共存させた状態で、④から⑤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 5.1.6-2 に示す

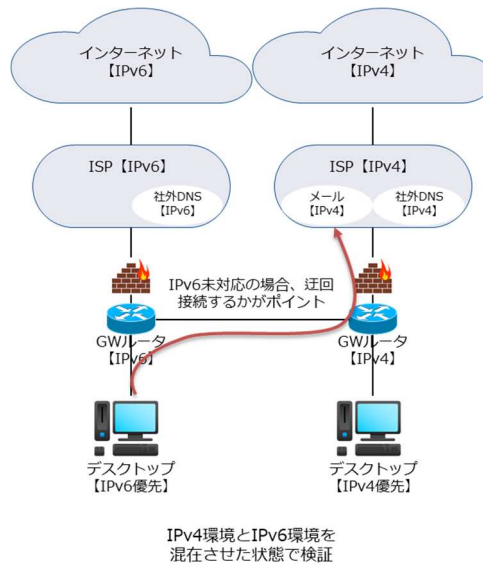


図 5.1.6-2 IPv4 経路と IPv6 経路を接続

④ 通常業務を想定した社内ネットワーク機器の利用

IPv4 と IPv6 を共存させた環境において、IPv4 デバイス(スキャナー、プリンタ)および IPv6 デバイス(複合機)を正常に利用できるか検証する。

⑤ 通常業務を想定した WEB サービスやメール等のインターネット利用

IPv4 と IPv6 を共存させた環境において、通常業務時間中に WEB サービスやメール等のインターネットを正常に利用できるか検証する。

上記①から⑤のシナリオを実施した結果の内、主要なサンプルを以下に示す。まずは IPv4 経路と IPv6 経路を切り離れた状態の試験を示す。

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://ipv6.test-ipv6.com/ へアクセスする	「あなたの IP アドレスは～」 の後に IPv6 アドレスが表示 されている	OK
3	ノート PC	無線	IPv6 優先	ファイルサ ーバ#3(支 社)	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】

図 5.1.6-3 の通り、IPv6 で ping の応答を受信できることを確認した。

```

C:\ コマンドプロンプト
ping 要求ではホスト 192.168.1.254 が見つかりませんでした。ホスト名を確認してもう一度実行してください。
C:\Users\%nkpc-072>ping -6 fde9:c477:6a1b:1::1

fde9:c477:6a1b:1::1 に ping を送信しています 32 バイトのデータ:
fde9:c477:6a1b:1::1 からの応答: 時間 =5ms
fde9:c477:6a1b:1::1 からの応答: 時間 =2ms
fde9:c477:6a1b:1::1 からの応答: 時間 =2ms
fde9:c477:6a1b:1::1 からの応答: 時間 =5ms

fde9:c477:6a1b:1::1 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンドトリップの概算時間 (ミリ秒):
    最小 = 2ms、最大 = 5ms、平均 = 3ms

C:\Users\%nkpc-072>

```

図 5.1.6-3 IPv6 で ping 応答あり

【#2の補足】

図 5.1.6-4 の通り、IPv6 でインターネット接続できることを確認した。



図 5.1.6-4 IPv6 でインターネット接続可能

【#3の補足】

図 5.1.6-5 の通り、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。(park2 は支社のファイルサーバのホスト名)

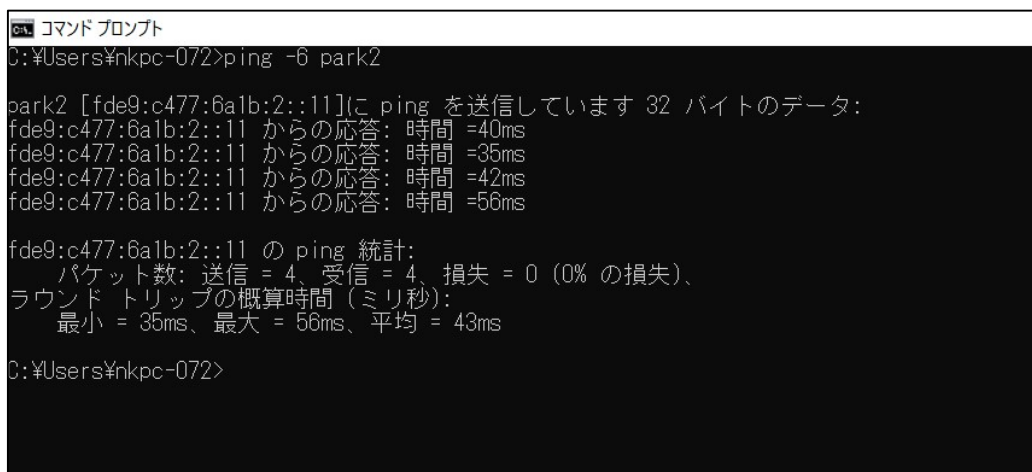


図 5.1.6-5 ホスト名でも ping 応答あり

② WEB サービスやメール等のインターネット利用

#	接続元機器名	有線 無線	IPv4 IPv6 優先	接続先機器名・サービス名	IPv4 IPv6 予想	検証内容	想定結果	実施結果
1	ノート PC	無線	IPv6 優先	IPv6 未対応メールサービス(送信)	IPv4	WEBArena (SMTP) 経由でメール送信を行う	メールが送信されない	OK
2	ノート PC	無線	IPv6 優先	IPv6 未対応メールサービス(受信)	IPv4	WEBArena (POP3) 経由でメール受信を行う	メールを受信できない	OK
3	ノート PC	無線	IPv6 優先	インターネット(一般)	IPv6 予想	WEB ブラウザで google へアクセスする	google 画面が表示される	OK
4	ノート PC	無線	IPv6 優先	インターネット(認証)	IPv6 予想	WEB ブラウザで Microsoft アカウントにログインする	アカウントページにログインできる	NG
5	デスクトップ PC	有線	IPv6 優先	Microsoft TEAMS	IPv6 予想	TEAMS を起動し、チャットを送信する	エラーが出ず使用できる	NG
6	ノート PC	無線	IPv6 優先	Microsoft TEAMS	IPv6 予想	TEAMS を起動し、チャットを送信する	エラーが出ず使用できる	NG

【#4 の補足】

Microsoft アカウントの認証ページ(<https://account.microsoft.com/>)に接続できなかった。Microsoft 認証サーバのドメインは、IPv4 アドレス(A レコード)のみが設定されているため、IPv6 シングルスタックでは、接続が行えないと推測される。「account.microsoft.com」に対して nslookup を実行した結果を図 5.1.6-6 に示す。

```
CA コマンドプロンプト
Microsoft Windows [Version 10.0.18362.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\%nkpc-071>nslookup account.microsoft.com
サーバー: UnKnown
Address: 2400:406a:2f0f:6b00::1

権限のない回答:
名前: e9412.b.akamaiedge.net
Address: 104.118.142.41
Aliases: account.microsoft.com
         account.microsoft.com.edgekey.net

C:\Users\%nkpc-071>
```

図 5.1.6-6 Microsoft アカウント認証ページは AAAA レコードなし

他方で、Google アカウントの認証ページ(<https://myaccount.google.com/>)は接続できた。認証サーバのドメインは、IPv4 アドレスおよび IPv6 アドレス(AAAA レコード)が設定されており、IPv6 シングルスタックでも、接続可能であった。「account.microsoft.com」に対して nslookup を実行した結果を図 5.1.6-7 に示す。

```
CA コマンドプロンプト
C:\Users\%nkpc-071>nslookup accounts.google.com
サーバー: UnKnown
Address: 2400:406a:2f0f:6b00::1

権限のない回答:
名前: accounts.google.com
Addresses: 2404:6800:4004:818::200d
          172.217.175.77

C:\Users\%nkpc-071>
```

図 5.1.6-7 Google アカウント認証ページは AAAA レコードあり

【#5、#6 の補足】

図 5.1.6-8 の通り、Microsoft Teams 起動時の Microsoft アカウントのログイン時にエラーとなり、認証が行えなかった。

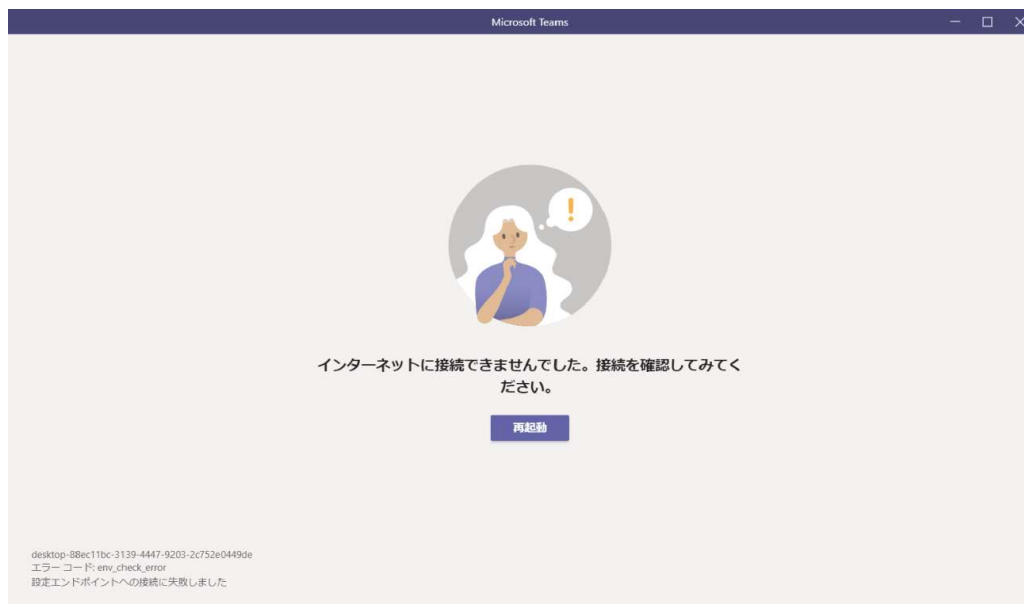


図 5.1.6-8 Microsoft Teams 起動不可

一時的に IPv4 経路側のルータと IPv6 経路側のルータを接続し、IPv4 と IPv6 を共存させる。IPv4 で一旦 Microsoft Teams 起動およびログインを行い、その後 IPv4 経路側のルータを切り離し、IPv6 シングルスタックに戻した状態でメッセージの送信を行うと、送信中にエラーとなり、チャットできなかった。

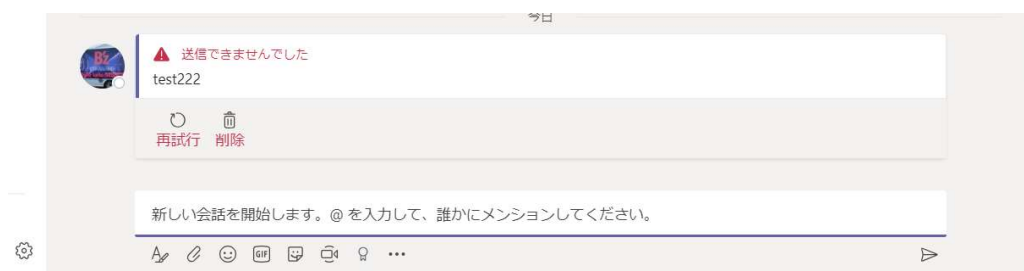


図 5.1.6-9 Microsoft Teams メッセージ送信不可

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#3(支社)	IPv6	IPv6 アドレスで接続しユーザ認証を行う	ユーザ認証が成功する	OK
2	ノート PC	無線	IPv6 優先	ファイルサーバ#3(支社)	IPv6	IPv6 アドレスで接続しファイルをアップロードする	ファイルが共有される	OK
3	ノート PC	無線	IPv6 優先	ファイルサーバ#3(支社)	IPv6	ホスト名で接続しユーザ認証を行う	ユーザ認証が成功する	OK
4	ノート PC	無線	IPv6 優先	ファイルサーバ#3(支社)	IPv6	ホスト名で接続しファイルをアップロードする	ファイルが共有される	OK
5	ファイルサーバ#1(本社)	無線	IPv6 優先	ファイルサーバ#3(支社)	IPv6	ホスト名で接続しファイルサーバ間で認証情報が同期されるかを確認する	変更後のパスワードでユーザ認証が成功する	OK

続いて、IPv4 経路と IPv6 経路を接続した状態の試験を示す。

④ 通常業務を想定した社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	スキャナ ー	IPv4	スキャナーを使用する	スキャンが実行される	OK
3	ノート PC	無線	IPv6 優先	複合機	IPv6	印刷ジョブを送信する	印刷が実行される	NG
4	ノート PC	無線	IPv6 優先	複合機	IPv6	スキャンを行う	スキャンが実行される	NG

【#3 の補足】

複合機が IPv6 シングルスタックの場合、ベンダ提供のプリンタドライバインストーラからネットワーク探索できなかった。カスタムセットアップで標準 TCP/IP ポートを手動作成し、IPv6 アドレスで手動追加することにより、IPv6 アドレスによる印刷処理が行えるようになった。サポートに問い合わせた結果、IPv6 シングルスタックでもネットワーク探索可能という回答であったが、機器仕様上、IPv6 シングルスタックに完全対応していないと判断する。最終的に複合機は、IPv4/IPv6 デュアルスタックとして試験を行った結果、デュアルスタックの場合では問題なく使用することができた。

【#4 の補足】

複合機が IPv6 シングルスタックの場合、Server Message Block プロトコルによる送信先の探索処理で PC が探索されず、スキャンデータの送信が行えなかった。サポートに問い合わせた結果、IPv6 シングルスタックでも探索可能という回答であったが、IPv6 シングルスタックに完全対応していないと判断する。最終的に複合機は、IPv4/IPv6 デュアルスタックとして試験を行った結果、デュアルスタックの場合では問題なく使用することができた。

⑤ 通常業務を想定した WEB サービスやメール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	IPv6 未対応メールサービス(送信)	IPv4	WEBArena (SMTP) 経由でメール送信を行う	メールが送信される	OK
2	ノート PC	無線	IPv6 優先	IPv6 未対応メールサービス(受信)	IPv4	WEBArena (POP3) 経由でメール受信を行う	メールを受信する	OK
3	ノート PC	無線	IPv6 優先	IPv6 未対応メールサービス	IPv4	メールサービスを 1 日通して使用してみる	問題なく使用できる	OK
4	ノート PC	無線	IPv6 優先	インターネット	IPv4 /IPv6	インターネットを 1 日通して使用してみる	問題なく使用できる	OK
5	ノート PC	無線	IPv6 優先	インターネット(認証)	IPv4 ⁴⁹	WEB ブラウザで Microsoft アカウントにログインする	Microsoft アカウントにログインできる。	OK

【#1、#2、#3 の補足】

IPv4 経路側のルータと IPv6 経路側のルータを接続した状態であるため、IPv6 未対応サービスであっても、問題なく利用することができた。当初、IPv6 優先 PC から IPv6 未対応サービスへ接続した場合、IPv4 通信に切り替わるまで(フォールバック)に一定時間を要すると推測していた。しかし、結果として、フォールバックによる遅延は体感せず、業務上支障をきたすことはなかった。PC 側のパケットログを解析したところ、IPv6 未対応のコンテンツへ接続する場合、DNS の名前解決で AAAA レコードを応答しない、あるいは IPv4 アドレスが応答されるように CNAME で回されていた。名前解決で IPv6 アドレスを取得できないため、すぐに IPv4 で通信しており、フォールバックが発生していない。この動きは、アプリの実装に依存するため、一概に断言できないが、コンテンツ提供者が、IPv6 未対応にもかかわらず不用意に IPv6 アドレス(AAAA レコード)を登録するようなことがない限り、IPv6 で TCP 接続(3way ハンドシェイク)を試みないため、フォールバックは発生しない可能性が高い。サンプルとして、IPv6 対応サービス(Google アカウント)と IPv6 未対応サービス(Microsoft アカウント)に接続を行った際の、パケットログの解析結果を図 5.1.6-10 および 5.1.6-11 に示す。

⁴⁹ シナリオ②「Web サービスやメール等のインターネット利用」におけるパケットログの解析結果より、部分的には IPv6 で通信しているが、IPv6 に完全対応していないことが判明した。

The screenshot shows a network traffic capture in Wireshark. The packet list pane shows several packets, with packet 16 being a DNS response. A blue callout box points to this packet with the text: "DNS クエリ(AAAA)のレスポンス後、IPv6 で通信を開始". The packet details pane for packet 16 shows the Domain Name System (response) section, including the transaction ID, flags, and answers. A blue callout box points to the AAAA record details with the text: "IPv6 アドレスを取得できている". Red dashed boxes highlight the packet list and details panes.

No.	Time	Source	Destination	Protocol	Length	Info
15	0.050845	2400:406a:2f0f:6b0...	2404:6800:4004:80...	TLSv1.2	278	Client Hello
16	0.051990	2400:406a:2f0f:6b0...	2400:406a:2f0f:6b...	DNS	156	Standard query response 0x3265 A
17	0.052557	2400:406a:2f0f:6b0...	2404:6800:4004:81...	TCP	86	51530 → 443 [SYN] Seq=0 Win=6553
18	0.053123	2400:406a:2f0f:6b0...	2400:406a:2f0f:6b...	DNS	156	Standard query response 0x3265 A
19	0.053574	2400:406a:2f0f:6b0...	2404:6800:4004:80...	TCP	86	51531 → 443 [SYN] Seq=0 Win=6553
20	0.059613	2404:6800:4004:809...	2400:406a:2f0f:6b...	TCP	86	51538 [ACK] Seq=1 Ack=200
21	0.062873	2404:6800:4004:801...	2400:406a:2f0f:6b...	TCP	86	51539 [ACK] Seq=1 Ack=200
22	0.063282	2400:406a:2f0f:6b0...	2404:6800:4004:80...	TCP	86	51540 [ACK] Seq=1 Ack=200
23	0.063371	2404:6800:4004:81c...	2400:406a:2f0f:6b...	TCP	86	51541 [ACK] Seq=1 Ack=200
24	0.063604	2400:406a:2f0f:6b0...	2404:6800:4004:80...	TCP	86	51542 [ACK] Seq=1 Ack=200
25	0.064501	2404:6800:4004:809...	2400:406a:2f0f:6b...	TCP	86	51543 [ACK] Seq=1 Ack=200

Packet 16 details:

```

> Frame 16: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface \Device\NPF_{2D265763-957-...}
> Ethernet II, Src: Yamaha_65:b5:5e (ac:44:f2:65:b5:5e), Dst: IntelCor_84:81:ae (dc:71:96:84:81:ae)
> Internet Protocol Version 6, Src: 2400:406a:2f0f:6b00::1, Dst: 2400:406a:2f0f:6b00:ccf4:d1f7:b578:b34b
> User Datagram Protocol, Src Port: 53, Dst Port: 49350
  Domain Name System (response)
    Transaction ID: 0x3265
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
      > accounts.youtube.com: type CNAME, class IN, cname www3.l.google.com
      > www3.l.google.com: type AAAA, class IN, addr 2404:6800:4004:81c::200e
        Name: www3.l.google.com
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 250 (4 minutes, 10 seconds)
        Data length: 16
        AAAA Address: 2404:6800:4004:81c::200e
  Request ID: 1
  
```

図 5.1.6-10 IPv6 対応サービスの場合、IPv6 アドレスを取得し IPv6 で通信

DNS クエリ(A, AAAA)のレスポンス後、IPv4 で通信している

No.	Time	Source	Destination	Protocol	Length	Info
67	1.379966	2400:406a:2f0f:6b0...	2400:406a:2f0f:6b00:ccf...	DNS	153	Standard query response 0xcafd A c.msn
68	1.384504	2400:406a:2f0f:6b0...	2400:406a:2f0f:6b00:ccf...	DNS	226	Standard query response 0x3b5 AAAA c.
69	1.385475	192.168.1.216	40.81.31.55	TCP	66	51511 → 443 [SYN] Seq=0 Win=65535 Len=
70	1.385476	192.168.1.216	40.81.31.55	TCP	66	51512 → 443 [SYN] Seq=0 Win=65535 Len=
88	1.443981	40.81.31.55	192.168.1.216	TCP	66	443 → 51512 [SYN, ACK] Seq=0 Ack=1 Win
89	1.444111	192.168.1.216	40.81.31.55	TCP	54	51512 → 443 [ACK] Seq=1 Ack=1 Win=2621
90	1.445078	192.168.1.216	40.81.31.55	TCP	54	51511 → 443 [ACK] Seq=1 Ack=1 Win=2621
91	1.445083	40.81.31.55	192.168.1.216	TCP	66	443 → 51511 [SYN, ACK] Seq=0 Ack=1 Win
92	1.445176	192.168.1.216	40.81.31.55	TCP	54	51512 → 443 [ACK] Seq=1 Ack=1 Win=2621

Transaction ID: 0xcafd
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 2
 Authority RRs: 0
 Additional RRs: 0
 Queries
 Answers
 c.msn.com: type CNAME, class IN, cname c.msn-com-nsatc.trafficmanager.net
 c.msn-com-nsatc.trafficmanager.net: type A, class IN, addr 40.81.31.55
 Name: c.msn-com-nsatc.trafficmanager.net
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Time to live: 7 (7 seconds)
 Data length: 4
 Address: 40.81.31.55
 [Request In: 65]
 [Time: 0.012516000 seconds]

A レコードのレスポンスで IPv4 アドレスを取得する

AAAA レコードのレスポンスでは、CNAME で IPv4 アドレスに回されている

No.	Time	Source	Destination	Protocol	Length	Info
67	1.379966	2400:406a:2f0f:6b0...	2400:406a:2f0f:6b00:ccf...	DNS	153	Standard query response 0xcafd A c.msn
68	1.384504	2400:406a:2f0f:6b0...	2400:406a:2f0f:6b00:ccf...	DNS	226	Standard query response 0x3b5a AAAA c.
69	1.385475	192.168.1.216	40.81.31.55	TCP	66	51511 → 443 [SYN] Seq=0 Win=65535 Len=
70	1.385476	192.168.1.216	40.81.31.55	TCP	66	51512 → 443 [SYN] Seq=0 Win=65535 Len=
88	1.443981	40.81.31.55	192.168.1.216	TCP	66	443 → 51512 [SYN, ACK] Seq=0 Ack=1 Win
89	1.444111	192.168.1.216	40.81.31.55	TCP	54	51512 → 443 [ACK] Seq=1 Ack=1 Win=2621
90	1.445078	192.168.1.216	40.81.31.55	TLSv1.2	252	Client Hello
91	1.445083	40.81.31.55	192.168.1.216	TCP	66	443 → 51511 [SYN, ACK] Seq=0 Ack=1 Win
92	1.445176	192.168.1.216	40.81.31.55	TCP	54	51512 → 443 [ACK] Seq=1 Ack=1 Win=2621

Transaction ID: 0x3b5a
 Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 2
 Authority RRs: 1
 Additional RRs: 0
 Queries
 Answers
 c.msn.com: type CNAME, class IN, cname c.msn.com
 Name: c.msn.com
 Type: CNAME (Canonical NAME for an
 Class: IN (0x0001)
 Time to live: 579 (9 minutes, 39 seconds)
 Data length: 36
 CNAME: c.msn-com-nsatc.trafficmanager.net
 c.msn-com-nsatc.trafficmanager.net: type CNAME, class IN, cname c.msn-com-asia-vip.trafficmanager.net
 Authoritative nameservers

図 5.1.6-11 IPv6 未対応サービスの場合、IPv6 アドレスを取得できず IPv4 で通信

(2) IoTシステムにおける検証について

5.1.4(9)のとおり、ビデオ会議システムはIPv6 シングルスタックである。

①ビデオ会議システムの利用

本社と支社間でビデオ通話を行い、正常にビデオ会議システムが利用できることを確認する。IPv6 側の経路を通過していることを確認するため、IPv6 側のルータのWAN 線を抜線した状態で接続し、ビデオ会議システムが利用できないことも確認する。シナリオを実施した結果を以下に示す。

①ビデオ会議システムの利用

#	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	ビデオ会議システム(本社)	有線	IPv6	ビデオ会議システム(支社)	IPv6	ビデオ会議システムで支社に接続する	ビデオ会議システムが利用できる(映像・音声途切れずに通話できる)	OK
2	ビデオ会議システム(本社)	有線	IPv6	ビデオ会議システム(支社)	IPv6	IPv6 側のルータの WAN 線を抜線し、ビデオ会議システムで支社に接続する	ビデオ会議システムが利用できない(支社のビデオ会議システムに接続できない)	OK

2. LAN 内アプリケーションレベルの検証

5.1.5にしたがって構築したシステム環境において、A社開発の業務アプリケーションをIPv6対応する際、どのような影響があるかを検証した。その他に、ユーザ向けにリモートの保守作業で使用している市販のパッケージソフトウェアにおいて、どのような影響が発生するかも検証した。

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2件発生した。

尚、実証結果に伴い設計を見直した点が1つある。Windows標準FTP(アクティブモード)について、SEP(Symantec Endpoint Protection)との相性が良くないため、対応としてFFFTP(パッシブモード)で代用した。

(1) 業務アプリケーションにおける検証について

5.1.4(7)のとおり、実証試験用に新規構築したAP/DBサーバ上で、A社が開発し、ユーザへ販売しているオンプレミス業務アプリケーションのIPv6対応を行った。①のシナリオをIPv6通信で検証した。検証範囲を図5.1.6-12に示す。

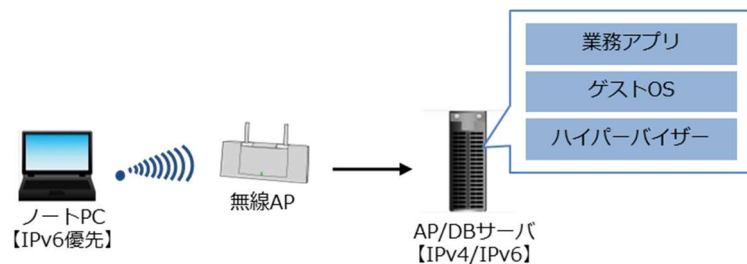


図 5.1.6-12 業務アプリケーションにおける検証範囲

① 直売所向け POS システムの動作検証

オンプレミス業務アプリケーションの内、「直売所向けの POS システム」を選定した。開発言語、DBMS、OS は以下のとおりであり、業務アプリケーションの利用(アプリ起動/FTP 接続等)に問題が発生しないかを検証した。

- ・ 開発言語 : Magic xpa(2.4)
- ・ DBMS : Pervasive.SQL(V11)
- ・ OS : Windows Server 2019

また、リモートの保守作業で使用している市販のパッケージソフトウェアに関する②のシナリオを IPv4 および IPv6 それぞれで検証した。検証範囲を図 5.1.6-13 に示す。

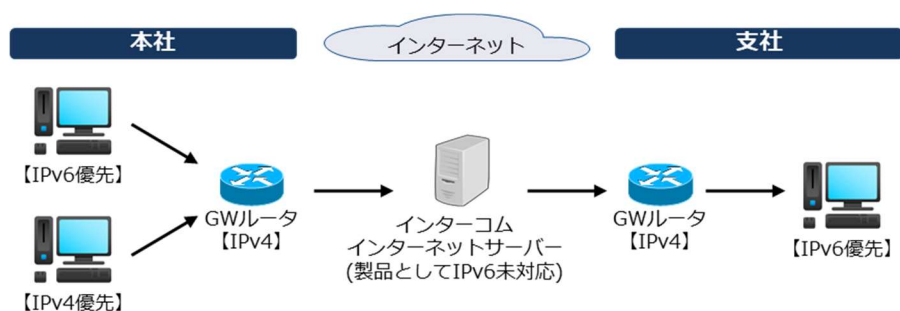


図 5.1.6-13 保守作業用ソフトにおける検証範囲

② その他の保守作業の検証

リモートの保守で使用しているソフトウェア「LAPLINK (version 14)⁵⁰」を本社、支社の 2 拠点の PC にインストールし、支社側をホスト PC、本社側をゲスト PC として、ホスト PC へのログイン、リモート操作に問題が発生しないかを検証した。

⁵⁰ 遠隔地の PC 画面を手元の PC 画面で共有し、マウス操作やキーボード入力、ファイル転送などを実現するリモートコントロールソフトである。

上記①②のシナリオを実施した結果の内、主要なサンプルを以下に示す。

① 直売所向け POS システムの動作検証

#	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	DB サーバ (PSQL V11)	IPv6 優先	直売所向け POS システムを起動し、データを登録する (データの DB 接続先は ¥¥[ホスト名]を設定する)	正常にデータ登録できる。	OK
2	ノート PC	無線	IPv6 優先	DB サーバ (PSQL V11)	IPv6 優先	直売所向け POS システムを起動し、データを登録する (データの DB 接続先は ¥¥[IPV6 アドレス]を設定する)	正常にデータ登録できる。	NG
3	ノート PC	無線	IPv6 優先	FTP サービス	IPv6 優先	コマンドプロンプトで、[ホスト名]を指定して FTP 接続する。	アクセス許可されたユーザー ID とパスワードを入力すると、接続成功する。接続成功した場合は get コマンド、put コマンドが成功するか確認する。	NG
4	ノート PC	無線	IPv6 優先	FTP サービス	IPv6 優先	コマンドプロンプトで、[IPV6 アドレス]を指定して FTP 接続する。	アクセス許可されたユーザー ID とパスワードを入力すると、接続成功する。接続成功した場合は get コマンド、put コマンドが成功するか確認する。	NG

【#2 の補足】

DBMS である PSQL (Pervasive.SQL) は、クライアント PC からサーバ上の共有フォルダに対してデータファイルを配置し、ファイルを更新することで、DB に対するデータ登録や更新を行う仕組みである。サーバ上の共有フォルダのパスは、クライアント PC の設定ファイル側に DB 接続先として記述して設定するが、IPv6 形式の UNC 指定 (¥¥[IPv6 アドレス].ipv6-literal.net) で記述した場合、直売所向け POS システムでデータベースの接続エラーが発生し、データを登録できなかった。サポートに確認した結果、「最新バージョン (V13) では IPv6 形式指定による動作確認ができています。動作確認対象外であるが、V11 でも IPv6 形式指定可能である」という回答を得た。サーバ側の PSQL を V11 から V13 にアップデートしたところ、データベースの接続エラーは解消し、データを登録できるようになった。サポートから IPv6 対応という回答を得ていたが、このように機器のバージョンによって、利用できない場合もあり得ることがわかった。

【#3、#4 の補足】

IPv6 アドレス指定で Windows 標準の FTP(アクティブモード)⁵¹を試みると、認証は可能だが、データ転送コマンド(put, get)が失敗する事象が発生した。調査の結果、IPv6 アドレス指定、あるいは対応するホスト名⁵²指定で FTP を行うと、PC にインストールしている SEP のファイアウォールで通信が遮断されていることがわかった。FTP で利用するポートを解放しても事象は解決しないが、試しに全ポートあるいは全 IP アドレスを解放すると事象は解決した(セキュリティ上 NG)。また、SEP をアンインストールし、Windows 標準のセキュリティソフトである Defender を有効化し、FTP で利用するポートを解放すると事象は解決した。事象の解析のため、検討した設定の組み合わせと FTP 通信結果の一部を図 5.1.6-14 に示す。

クライアント側の設定				サーバー側の設定		結果	
SEP		Windows Defender		Windows Defender		コントロール コネクション (Port21)	データ コネクション (Port20)
不一致IPトラフィックの設定	FWルール	受信/送信の規則	許可されたアプリ	受信/送信の規則	許可されたアプリ		
アプリケーション トラフィックのみ を許可	既定のルール			既定の規則	FTP:プライベート	○	×
アプリケーション トラフィックのみ を許可	サーバーIPv6アド レスに対し20,21 ポートを許可			受信・送信の規 制：20,21ポートを 許可	FTP:プライベート	○	×
アプリケーション トラフィックのみ を許可	サーバーIPv6アド レスに対し20,21 ポートを許可			受信・送信の規 制：全てのTCP ポートを許可	FTP:プライベート	○	×
アプリケーション トラフィックのみ を許可	サーバーIPv6アド レスに対し全ての TCPポートを許可			受信・送信の規 制：全てのTCP ポートを許可	FTP:プライベート	○	○
IPトラフィックを 許可	既定のルール			既定の規則	FTP:プライベート	○	○
		既定の規則	なし	既定の規則	なし	×	×
		既定の規則	なし	既定の規則	FTP:プライベート	○	×
		既定の規則	FTP:パブリック	既定の規則	FTP:プライベート	○	○

図 5.1.6-14 各設定とFTP 通信結果

FTP には「パッシブモード」と「アクティブモード」の2種類が存在しており、セキュリティ上「パッシブモード」が有効と言われることが多い。理由として、アクティブモードの場合、クライアントに対するインバウンド通信となり、ファイアウォールに穴あけが必要になるためである。今回、SEP にはインバウンド通信への特別な遮断設定がされていると推測した。そこで、「パッシブモード」を選択可能なフリーソフトである FFFTP で代用した。FFFTP では、問題なく通信可能であった。

⁵¹ FTP にはセッション制御用のコントロールコネクション(ポート 20)とデータ転送用のデータコネクション(ポート 21)がある。また、FTP にはパッシブモードとアクティブモードがあり、前者はクライアントからサーバにデータコネクションの確立を試みる。後者はサーバからクライアントにデータコネクションの確立を試みる。Windows 標準 FTP はアクティブモードのみである。

⁵² 前述のファイルサーバ等のホスト名は TCP/IP 系であり、host ファイルで名前解決しているものであるが、DB サーバのホスト名は NetBIOS 系を指している。

クライアント側の設定				サーバー側の設定		結果	
SEP		Windows Defender		Windows Defender		コントロール コネクション (Port21)	データ コネクション (Port20)
不一致IPトラ フィックの設定	FWルール	受信/送信の規則	許可されたアプリ	受信/送信の規則	許可されたアプリ		
アプリケーション トラフィックのみ を許可	既定のルール	-		既定の規則	FTP:プライベート	○	○

図 5.1.6-15 FFFTP での設定と通信結果

以上より、「アクティブモード」ではクライアントへのインバウンド通信が発生し、SEP がこれを遮断していたこと、「パッシブモード」ではクライアントからのアウトバウンド通信となるため、SEP の設定は変えず(穴あけせず)、問題なくデータ転送まで可能なことを検証した。

②その他の保守作業の検証

#	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	ノート PC	IPv6 優先	LAPLINK を使用して拠点 A (本社) から保守対象リモート PC (支社) の操作ができること	・LAPLINK でのログインできる ・リモート PC 側のアプリケーションが起動できる	OK
2	ノート PC	無線	IPv4 優先	ノート PC	IPv6 優先	LAPLINK を使用して拠点 A (本社) から保守対象リモート PC (支社) の操作ができること	・LAPLINK でのログインできる ・リモート PC 側のアプリケーションが起動できる	OK

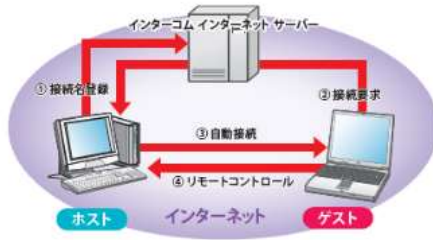
【#1、#2 の補足】

LAPLINK は、イントラネットでは IPv6 対応しているが、インターネット経由での IPv6 接続は未対応である。LAPLINK はインターネット経由でリモート接続を行う場合、リモート接続先 PC のアドレス情報を直接指定するのではなく、仲介サーバ(インターコム インターネットサーバ)にホスト PC 側から登録した「接続先名」をクライアント PC で指定して、仲介サーバから接続先の情報を取得するような動作となっている。LAPLINK の仕組みを図 5.1.6-16、図 5.1.6-17 に示す⁵³。

⁵³ バージョン 13 の機器ガイドより抜粋している。旧バージョンであるが仕組みは同等である。
https://icdl.intercom.co.jp/unlimited/pdf/laplink13/internet_guide.pdf

② なぜリモート操作をする側のゲストパソコンで、ポートの開放やグローバル IP アドレスが必要なの？

リモート操作をされる側のホストパソコンで特別な設定を必要としないように、以下の仕組みで通信しているためです。



インターネット接続の仕組み

- ① ホストがサーバーにインターネット接続名を登録し、接続を待機します。
- ② ゲストが接続を開始しようとするときに、サーバーにグローバル IP アドレスを通知します (グローバル IP アドレスが必要)。
- ③ ホストは通知されたグローバル IP アドレスを使って、ゲストに自動接続し、通信が開始されます (ポートの開放が必要)。

図 5.1.6-16 LAPLINK の仕組み
(「インターネット接続ガイド」より引用)

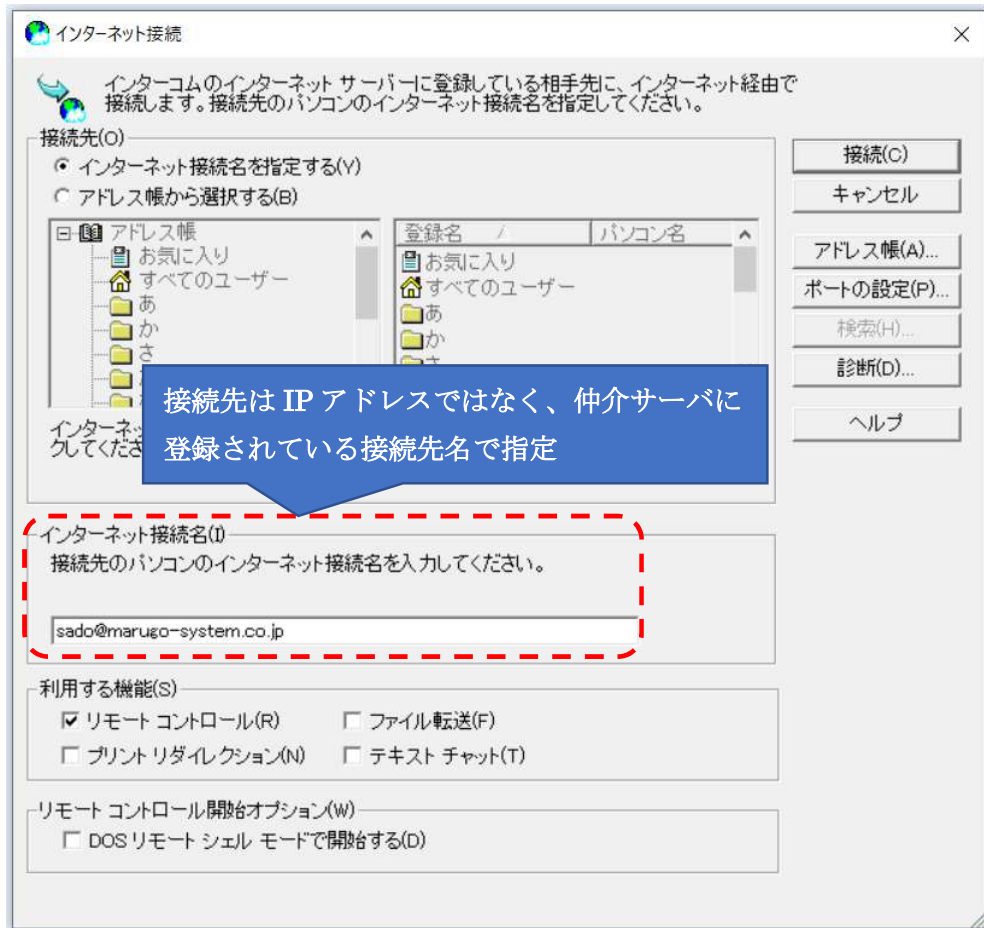


図 5.1.6-17 ゲスト PC 側の接続先指定画面

当初の想定では、IPv6 優先 PC では、一度 IPv6 接続でインターネットサーバに接続を試行した後、フォールバックで IPv4 接続に切り替わることを想定していた。結果として、フォールバックによる遅延はなかった。PC 側のパケットログを解析したところ、リモート接続を開始したタイミングで FQDN の名前解決で A レコードのみの名前解決を行っていた。仲介サーバは IPv6 アドレスを持たないため、IPv6 通信は発生しない。その後のゲスト PC とホスト PC 間についても、IPv4 のみで通信が行われていた。

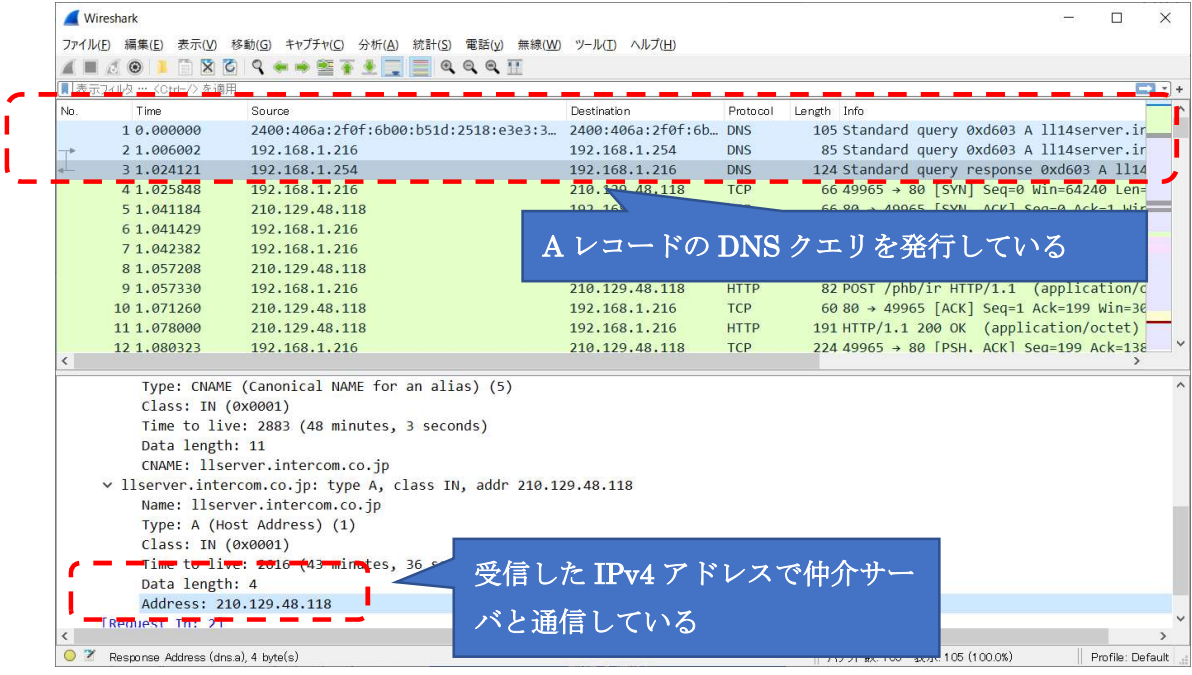


図 5.1.6-18 ゲスト PC と仲介サーバ間のパケットログ

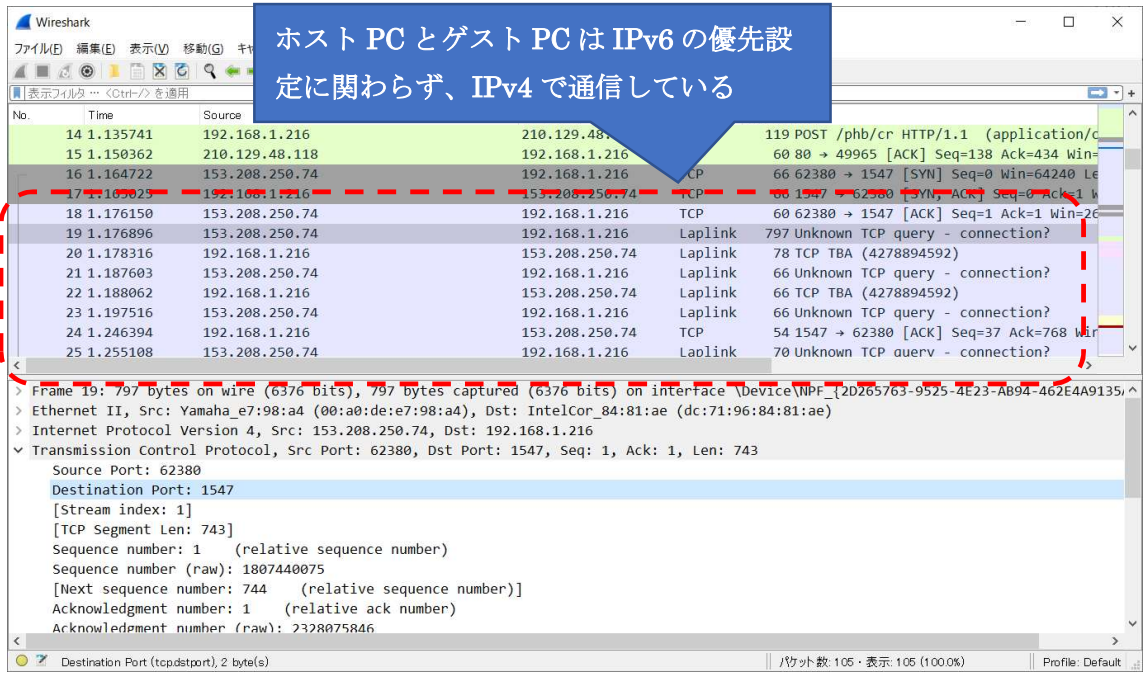


図 5.1.6-19 ゲスト PC とホスト PC 間のパケットログ

以上より、ソフトウェアの IPv6 対応有無に関わらず、不要なフォールバックを伴わずにソフトウェアを利用できることがわかった。

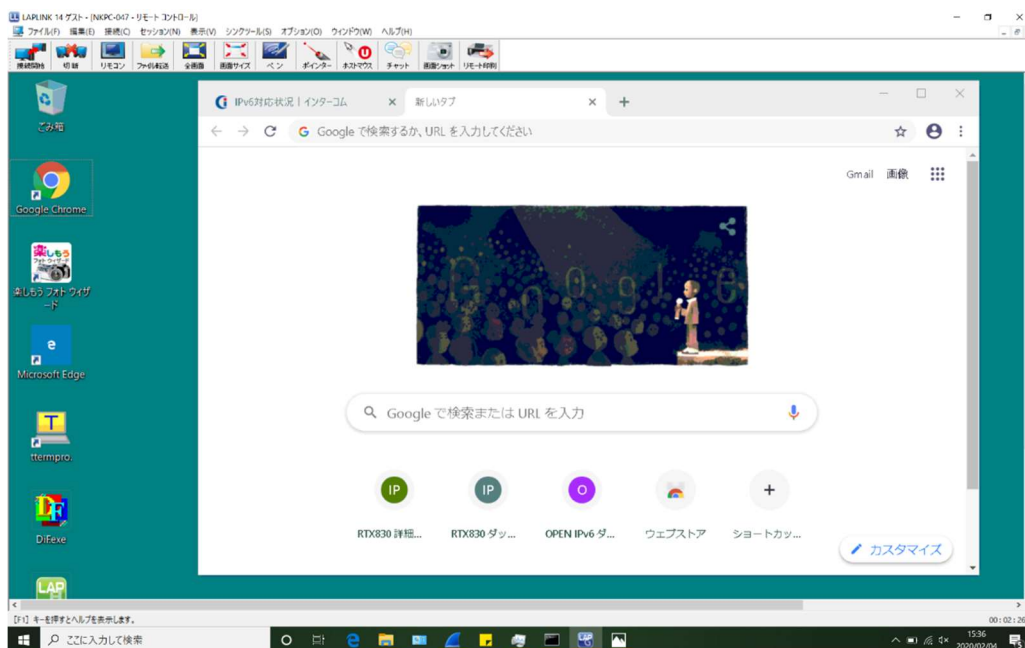


図 5.1.6-20 リモート接続成功時のスクリーンショット

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、提供されているクラウドサービス環境上 (IaaS) に構築した環境において、A 社開発の業務アプリケーションを IPv6 対応する際、どのような影響があるかを検証した。

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

(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

5.1.4(11)の通り、さくらクラウドについては、ユースケース用に新規構築した IaaS 上で、業務アプリケーションの IPv6 対応を行った。IDC サービスについては、IPv6 未対応のため、既存のクラウド環境 (IPv4) を利用する。①のシナリオで、インターネットにあるクラウドサービス (外部システム・商用サービス等) を IPv6 で利用可能か検証した。②のシナリオで、インターネットにあるクラウドサービスを IPv4 で利用可能か検証した。検証範囲を図 5.1.6-21 示す。

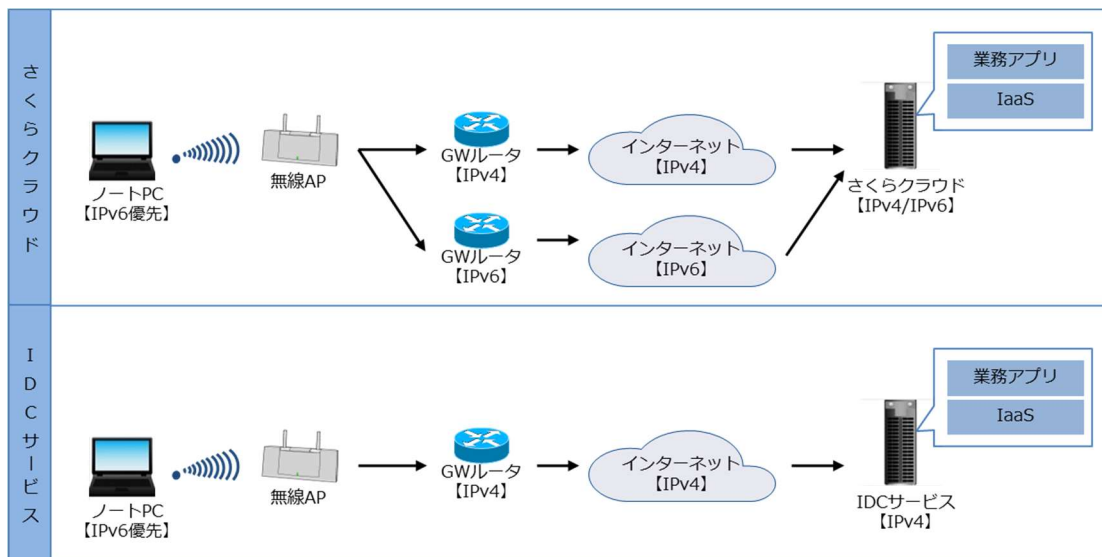


図 5.1.6-21 業務アプリケーションにおける検証(クラウド)範囲

① 小売店向け POS システムの動作検証

クラウド用業務アプリケーションの内、「小売店向け POS システム」を選定した。開発言語、DBMS、OS は以下のとおりであり、サービスの利用 (RDP 接続/アプリケーションの起動/FTP 接続) に問題が発生しないかを検証した。

- ・IaaS 環境 : さくらクラウド、IPv6 対応あり (IPv6 の無効化も可能)
- ・開発言語 : Magic xpa(2.5)
- ・DBMS : SQL Server2016
- ・動作環境 OS : Windows Server 2016

② 保育園栄養管理システムの動作検証

クラウド用業務アプリケーションの内、「保育園栄養管理システム」を選定した。開発言語、DBMS、OS は以下のとおりであり、サービスの利用 (WEB ブラウザ接続/SVNクライアントの接続) に問題が発生しないかを検証した。

- ・IaaS 環境 : NS コンピュータサービスの IDC サービス、IPv6 対応なし
- ・開発言語 : PHP(5.4.45)
- ・DBMS : MySQL(5.5.36)
- ・動作環境 OS : CentOS(6.5)

上記①②のシナリオを実施した結果の内、主要なサンプルを以下に示す。

① 小売店向け POS システムの動作検証

#	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	さくらクラウド RDP	IPv6 有効	Windows のリモートデスクトップ接続機能で権限のあるユーザで接続する(接続先は IPv6 アドレス指定)	RDP でクラウドサーバにログインできる。	OK
2	ノート PC	無線	IPv6 優先	さくらクラウドサーバ(FTP サービス)	IPv6 有効	コマンドプロンプトで、[IPv6 アドレス]を指定して FTP 接続する。	アクセス許可されたユーザ ID とパスワードを入力すると、接続成功する。接続成功した場合は get コマンド、put コマンドが成功するか確認する。	NG
3	ノート PC	無線	IPv6 優先	小売店向け POS システム (RDP)	IPv6 有効	クライアント PC から RDP 機能を使って小売店向け POS システムを起動する(接続先は IPv6 アドレス指定)	POS システムの画面が正常に起動する。	OK
4	ノート PC	無線	IPv6 優先	小売店向け POS システム (RDP)	IPv6 無効	クライアント PC から RDP 機能を使って小売店向け POS システムを起動する(接続先は IPv4 アドレス指定)	POS システムの画面が正常に起動する。	OK
5	ノート PC	無線	IPv6 優先	小売店向け POS システム (RDP)	IPv6 無効	クライアント PC から RDP 機能を使って小売店向け POS システムを起動する(接続先は IPv6 アドレス指定)	接続エラーになる。	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
6	ノート PC	無線	IPv6 優先	小売店向け POS システム (RDP)	IPv6 有効	クライアント PC から RDP 機能を使って小売店向け POS システムを起動する(接続先は IPv6 のドメイン指定)	POS システムの画面が正常に起動する。	OK
7	ノート PC	無線	IPv6 優先	小売店向け POS システム (RDP)	IPv6 無効	クライアント PC から RDP 機能を使って小売店向け POS システムを起動する(接続先は IPv6 のドメイン指定)	接続エラーになる。	OK
8	ノート PC	無線	IPv6 優先	小売店向け POS システム (RDP)	IPv6 無効	クライアント PC から RDP 機能を使って小売店向け POS システムを起動する(接続先はドメイン指定)	POS システムの画面が正常に起動する (IPv4 で接続される)	OK

【#2 の補足】

#①-3、#①-4 と事象および対応は同等である。

【#6、#7、#8 の補足】

外部 DNS サービス内で自社ドメインを管理している。#37 では、ドメインに対応する IPv6 アドレスを AAAA レコードとして正引き登録し、名前解決により IPv6 アドレスでの接続が行われることを検証した。結果、問題なくアプリケーションのメニュー画面がクライアント PC 上に表示されることを確認した。念のため、#38 では、名前解決が IPv6 で行われていることを確認するため、事前にクラウドサービスの IPv6 接続オプションを無効化した状態で実施した。想定通り、RDP 機能の接続が失敗した。

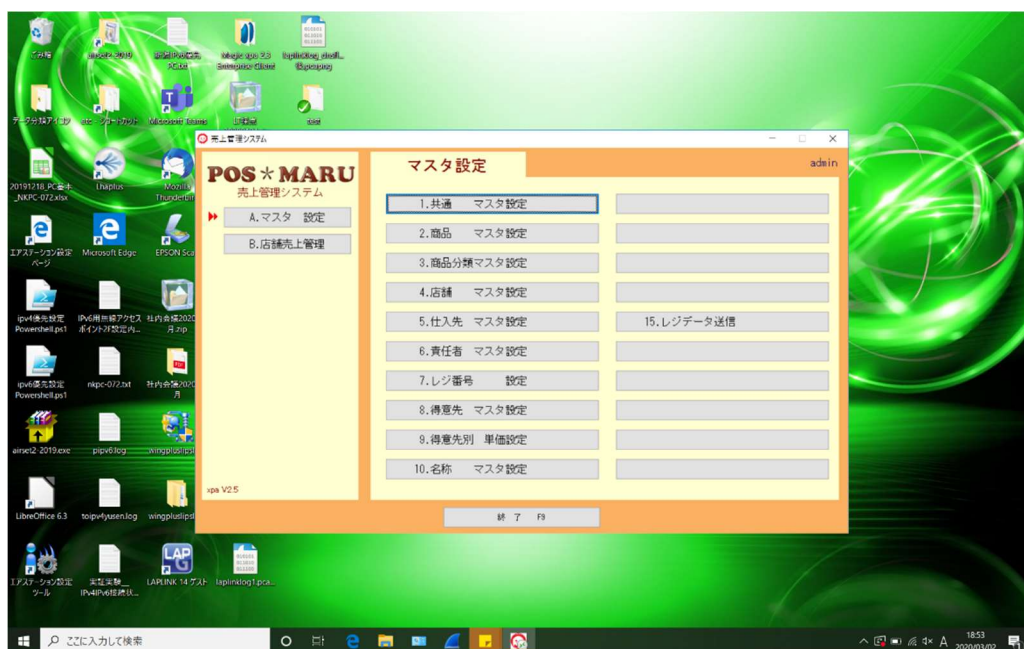


図 5.1.6-22 クラウドサービス利用成功時のスクリーンショット

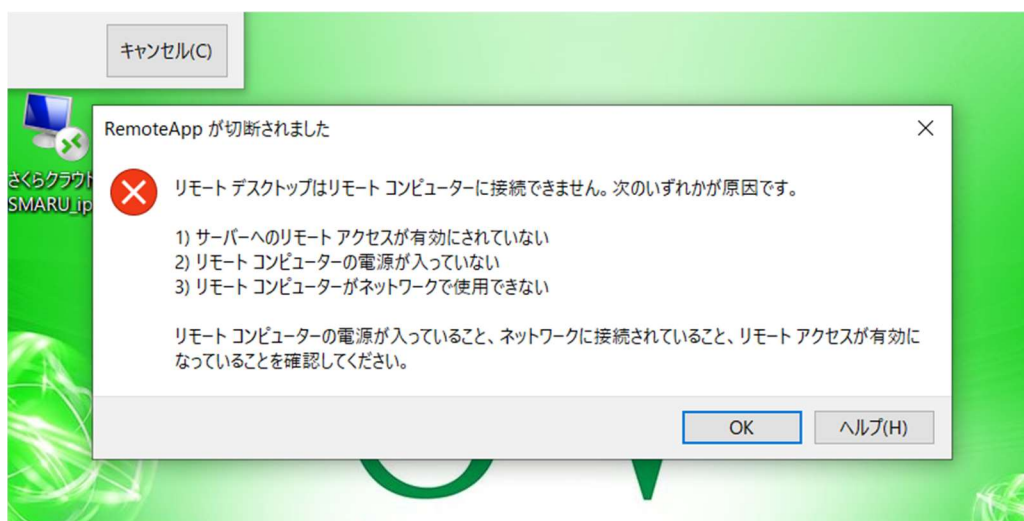


図 5.1.6-23 IaaS の IPv6 を無効にした場合、IPv6 通信できなくなる

#39 では、当ドメインに対応する IPv4 アドレスを追加で正引き登録し、IPv4 アドレス(A レコード)と IPv6 アドレス(AAAAレコード)の両方を取得できる状態にした。この状態で、IPv6 接続オプションを無効にし、IPv6 から IPv4 へのフォールバックが発生するか検証した。結果、AAAA レコードおよび A レコードの両方で DNS リクエストを行い、取得した IPv6 アドレスおよび IPv4 アドレス両方で TCP 接続を試みていた。IPv6 接続オプションを無効にした状態であったため、IPv4 のみ TCP レスポンス(ACK)を返す。TCP レスポンスが早いプロトコルで通信を開始しており、すぐに IPv4 通信が行われるため、フォールバックは発生しなかった。

② 保育園向け栄養管理システムの動作検証

#	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	保育園栄養管理システム	IPv4	IPv4 ドメイン指定で、クライアント PC から保育園栄養管理システムを起動する(ブラウザは IE を利用)	正常に起動する。	OK
2	ノート PC	無線	IPv6 優先	保育園栄養管理システム	IPv4	保育園栄養管理システムで献立を作成し、献立表をダウンロードする(ブラウザは IE を利用)	正常にダウンロードできる。	OK
3	ノート PC	無線	IPv6 優先	DB サーバ	IPv4	指定された接続先(ドメイン)に接続できるか確認する(ブラウザは IE を利用)	DB のメンテナンス画面が正常に起動する。	OK

【#1、#2、#3 の補足】

クラウド IaaS サービスが IPv6 未対応のため、IPv6 対応した LAN 環境(デュアルスタック環境)から従来通りクラウドサービスを利用できるか検証した。

5.1.6.2 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。

そこで、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: 中小企業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、機器メーカー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ティング事例をもとに、IPv6 対応において普遍的に留意すべき点を示す。

5.2 モデル I: 中小企業 B

5.2.1 ユースケース企業の紹介

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、新潟県の外郭団体である財団が運営する施設（以下、B社と呼称）で行った。B社は、新潟県内で施設型ビジネスを展開し、対外的な情報発信や施設運営に IoT システムを活用している環境である。

(2) 既存のシステム環境

本実証試験は、B社内で利用している一般業務システムだけでなく、B社で利用されている IoT システムや業務アプリケーション、クラウド上の動画配信サービスに対して行った。B社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

B社のシステム環境内のノード数は 50 以上、サブネット数は 1 つ、他拠点への VPN 接続はなく、GMO とくどく BB フレッツ光ファミリー(1 IP 接続サービス)による PPPoE(光電話なし)の回線を引き込んでいる。

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、サーバ、事務機器には、IPv4 アドレスを静的に設定している。インターネット回線と社内ネットワークの間には専用機器である FW 装置が設置されており、FW 装置側のプロバイダ接続機能によりインターネットに接続している。また、単体の GW ルータは設置せず、FW 装置が GW ルータを兼用する構成となる。

GW ルータ側で DHCP を無効化しており、社内機器に対しては IP アドレスの動的割り当てを許可しない運用としている。

職員の私用端末を接続するための無線ルータでは DHCP 接続を許可しているが、ゲストモード(内部ネットワークへの接続は不可)で運用している。

メールや DNS のサーバは社内に設置せず、外部のサービスを利用している。

5.2.2 要件定義

B社の内部環境を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5.2.2-1に示す。

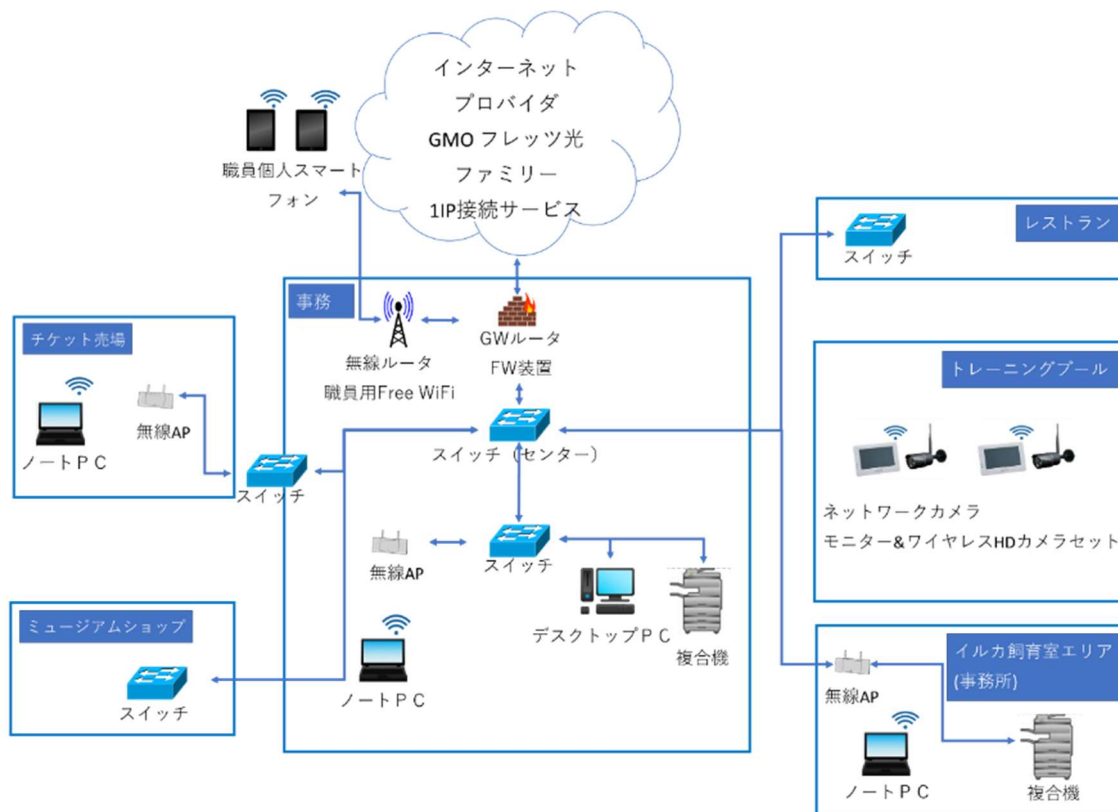


図 5.2.2-1 ネットワーク構成図イメージ

(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、IPv4 の基幹ネットワークは社内端末のセキュリティを維持するためのウイルス対策管理サーバ等が稼働しており、IPv6 の適用による影響リスクを避けるため、基幹ネットワークは現状のまま運用する方針とした。そのため、IPv4 の基幹ネットワークと 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 5.2.2-1 に示す。

表 5.2.2-1 機器等一覧イメージ

既存/ 新規	機器等	機器 メーカー等	機器名等	移行対象	IPv6 対応 状況確認	導入方針
新規	GW ルータ	YAMAHA	RTX830	○	IPv6 対応	新規
既存	FW 装置	YAMAHA	FWX-1201	○	IPv6 対応	変更要
新規	スイッチ	BUFFALO	BS-GS2008P	○	対象外 (L2 機器のため)	新規
新規	スイッチ	NETGEAR	GS108E	○	対象外 (L2 機器のため)	新規
既存	無線ルータ	Buffalo	WXR-1900DHP3	○	IPv6 対応	変更要
新規	無線ルータ	Buffalo	WSR-2533DHP3- BK	○	対象外 (無線クライアントが IPv6 未対応のため)	新規
新規	無線アクセ スポイント	Buffalo	WAPS-1266	○	対象外 (L2 機器のため)	新規 (L2 透過)
新規	有線ネットワ ークカメラ	I/O データ	TS-NA220	○	IPv6 未対応	新規
新規	無線ネットワ ークカメラ#1	I/O データ	TS-NA220W	○	IPv6 未対応	新規
新規	無線ネットワ ークカメラ#2	ATOM	ATOM Cam	○	IPv6 未対応	新規
新規	無線ネットワ ークカメラ#3	マスプロ	WHC7M3/10M3	○	IPv6 未対応	新規

既存/ 新規	機器等	機器 会社名等	機器名等	移行 対象	IPv6 対応 状況確認	導入方針
新規	センサー内 蔵温度計	T&D	RTR-500BW(親機) RTR-500BL(子機)	○	IPv6 未対応	新規
新規	NAS	I/O データ	HDL2-AAX16	○	IPv6 対応	新規
既存	複合機	RICOH	imagio MP C4002	-	対象外	変更不要
既存	ISP	OCN 光	フレッツ IPoE 標準 プラン 固定 IP	○	IPv6 対応	変更要
既存	メールサー ビス	GMO メール サービス	GMO メールサービ ス	-	対象外	変更不要
新規	ホスティング サービス	GMO 専用 サーバ	GMO 専用サーバ	○	IPv6 対応	変更不要

5.2.3 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 5.2.3-1 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 ISP の切り替えに伴う GW ルータの導入および既存ファイアウォールの構成変更はネットワークの不通による現存機器への影響を調査した上で、最も影響が少ない時間帯を選択して実施した。

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」と「IoT システムにおける検証」、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
要件定義		現行整理/ 移行対象の定義												
調達			回線契約/ 機器調達											
設計				実証計画/ 設計書作成										
構築					環境構築									
試験	疎通確認							疎通確認						
	ネットワークレベルの検証							一般業務 における検証						
	LAN内アプリケーションレベルの検証								IoTシステム における検証					
	WAN越しアプリケーションレベルの検証								業務アプリケーション における検証					
試験結果の評価														

図 5.2.3-1 スケジュールイメージ(中小企業 B)

5.2.4 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2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 既存環境を可能な範囲で IPv6 対応をすること

①について、既存環境では FW 装置側で IPv6 通信を遮断するポリシーで運用されており、また既存機器は全て静的 IP アドレスの設定により管理する運用となっているため、DHCP 自体が無効化されている。一般業務で使用する基幹ネットワークでは、社内端末のセキュリティを維持するためのウイルス対策管理サーバ等が稼働しており、IPv6 の適用による影響リスクを避けるため、基幹ネットワークは現状のまま運用する方針とした(IPv6、DHCP の無効化する)

【IPv6 に移行できない部分】

- ・基幹ネットワーク全体
- ・一般業務で利用する外部サービス(メールサービス、グループウェアサービス等)

上記を踏まえ、基幹ネットワークから切り離しが可能な部分を現環境から抽出した。

【IPv6 に移行できる部分】

- ・ゲスト用 Wi-Fi
- ・新規導入する IoT 機器(NAS⁵⁴、ネットワークカメラ、センサー内蔵温度計)
- ・新規構築する一般ユーザ向けのクラウドサービス

その他、プロバイダ、GW ルータ、FW 装置については、現環境では IPv6 への移行のため変更が必須であった。基幹ネットワークへ影響を与えないよう設定を行う必要があるため、設計時に十分に注意するポイントとなる。

②について、IPv6 対応可能な機器を選定して実施したが、実際のところ IoT 機器の IPv6 対応は芳しくない状況であった。

また、IoT 機器が連携するクラウドサービスについても、機器は IPv6 に対応しているが、クラウドサービス側は IPv6 非対応など、完全に IPv6 対応している機器を探すのは難しい状況であった。

【IPv6 に移行できない仕様の機器/サービス】

- ・IPv6 対応していない IoT 機器(ネットワークカメラ、センサー内蔵温度計)

これらの①、②に関する機器、サービスの選定において発生した課題、検討した内容の詳細については、5.2.5 に記載する。

⁵⁴ ネットワークに接続可能な外部記憶装置 (Network Attached Storage)

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

基幹ネットワーク、および実証実験ネットワークにおいて、インターネット(WEB サービス利用やメール等)、複合機での印刷等の一般業務を行うための無線接続クライアント PC (Windows) 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/デフォルトゲートウェイについて

実証試験のため IPv6 アドレスは DHCPv6 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…RA による自動設定

(b) DNS サーバについて

指定する IPv6 アドレスは DHCPv6 で割り当てる方式とする。

- 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…DHCPv6 による自動設定

③ 特記事項

特になし。

(2) 有線接続のデスクトップ PC

① 要素説明

実証実験ネットワークにおいて、インターネット(WEB サービス利用やメール等)、複合機での印刷等の一般業務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/デフォルトゲートウェイについて

ノートPC同様、IPv6 アドレスは DHCPv6 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…RA による自動設定

(b) DNS サーバについて

指定する IPv6 アドレスは DHCPv6 で割り当てる方式とする。

- 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…DHCPv6 による自動設定

③ 特記事項

実証実験を行う端末の OS は、Windows、および Mac 両方を対象とする。

(3) 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 シングルスタック方式とする(既存踏襲)。

(a) IP アドレスについて

既存の設定を踏襲し、IPv4 の静的アドレスと設定する。

- IPv4 アドレス…静的アドレスによる手動設定

③ 特記事項

特になし。

(4) インターネット接続を制御する GW ルータ

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を構築するための機器である。

② 方式設計

方式設計の方針に従い、FW 装置を残したまま新たな GW ルータを導入する。GW ルータは IPoE 接続に対応したレンタルルータを使用し、IPv4 と IPv6 のデュアルスタックの回線を用意する。

(a) IP アドレスについて

- IPv4 アドレス…設定なし(内部管理用のアドレスは手動設定)
- IPv6 アドレス…DHCPv6 による自動設定

(b) プロバイダ認証情報について

レンタルルータのため、特に設定なし。

(c) ファイアウォール機能について

設定なし(デフォルト設定で利用)。

※詳細なパケットフィルタ機能は、別途設置する FW 装置側の機能を利用する。

③ 特記事項

レンタルルータの性質上、ユーザが端末の設定を直接変更することができない。プロバイダ側にルーティング設定、ファイアウォール設定、LAN 側の IP アドレス設定などの情報を事前に連絡し、GW ルータ起動時にコンフィグレーションをダウンロードする方式で設定を適用している。

このため、GW ルータの実際のコンフィグレーションはユーザが参照することはできず、詳細な設定内容は確認することができない。

ファイアウォール機能に関しても、同様の方式で設定可能であるが、細かな設定を行うことが難しかった。そのため、既存の FW 装置を流用し、GW ルータと併用する構成とする。

(5) 外部からのネットワーク通信を制御する FW 装置

① 要素説明

GW ルータからのインターネット通信に対してパケットのフィルタリングを行うための機器である。

② 方式設計

5.2(1)項の方式設計の方針に従い、以下の通りとする。

- ・基幹ネットワーク側の接続ポート…IPv4 シングルスタック方式(既存踏襲)
- ・実証実験ネットワーク側の接続ポート…IPv4/IPv6 デュアルスタック方式
- ・ゲスト用 Wi-Fi ネットワークの接続ポート…IPv4/IPv6 デュアルスタック方式

(a) IP アドレスについて

- ・IPv4 アドレス…設定なし(内部管理用のアドレスは手動設定)
- ・IPv6 アドレス…RA による自動設定

(b) プロバイダ認証情報について

本機ではプロバイダ認証は行わない(既存の認証設定は削除する)。

(c) ファイアウォール機能について

インターネット接続に関するパケットフィルタ設定は、既存の設定内容を踏襲する。

ただし、実証実験ネットワーク内に新たに設置する IoT 機器に関して、リモート接続が必要な場合は、機器の IP アドレス、通信許可が必要なポートを確認した上で、ダイナミックフィルタの通過設定を追加する。

(d) ポートベース VLAN 機能について

既存環境では、ゲスト用 Wi-Fi ネットワークから基幹ネットワークへのアクセスを制限するため、FW 装置に接続されている各ポートに対して、ポート間のパケットフィルタ、ルーティングといった通信制御を行っている。

新たに実証実験ネットワークを FW 装置に接続する場合、基幹ネットワーク側から実証実験ネットワークにアクセス可能としなければならないが、その逆のアクセスに対しては制限する必要があるため、既存環境の設定内容に倣い、実証実験ネットワーク向けのポートベース VLAN の制御設定を追加する。

③ 特記事項

特になし。

(6) 無線接続を制御する無線アクセスポイント

① 方式設計

無線接続 PC、IoT 機器から社内の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 特記事項

特になし。

(7) 社内で運用している既存サーバ類

① 要素説明

B 社では、社内端末のセキュリティを維持するため、WSUS サーバ⁵⁵や、ウイルス対策管理サーバ⁵⁶を運用している。

② 方式設計

社内セキュリティへの影響を避けるため、IPv4 シングルスタック方式のまま、設定は変更しない。

③ 特記事項

特になし。

⁵⁵ ローカルネットワーク内で Windows Update を配信するサービス (Windows Server Update Services) が稼働しているサーバ。

⁵⁶ 各端末のウイルス対策ソフトの稼働状況を監視、管理するためのサーバ。

(8) 社内の情報資産を管理する NAS 機器

① 要素説明

クライアント PC を認証し、ファイル共有を行うネットワーク接続可能なストレージ機器である。

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) 認証設定について

認証の設定は NAS 側のユーザ管理機能を利用し、アカウント登録を行う。

本機器におけるユーザ認証とファイル転送機能は、SMB⁵⁷により実現している。NAS にアクセス可能なユーザ情報は、NAS 側の管理機能によりアクセス許可ユーザの情報登録を行う。

(d) リモート接続について

NAS をリモート接続可能とするため、リモート接続用の追加パッケージをインストールする(NAS の管理画面上から追加可能)。

③ 特記事項

NAS へのリモート接続は(c)で登録されたアカウント情報にて、スマートフォン用のアプリケーションを介して行う。

⁵⁷ Server Message Block の略称であり、主に Windows を中心とした環境で LAN を通じてファイル共有やプリンタ共有などに使用される通信プロトコルを指す。

(9) 上記以外のネットワーク接続デバイス(IoT 機器)

① 要素説明

社内の各所に設置するネットワークカメラ、センサー内蔵温度計等の IoT 機器である。

② 方式設計

IPv6 方式に対応していないため、IPv4 シング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

③ 特記事項

特になし。

(10) 社外のメールサービス

① 要素説明

クライアント PC からメールの送受信(SMTP、POP)を行う外部メールサービス(MTA)である。

② 方式設計

既存メールサービスが IPv6 未対応のため、IPv4 シングルスタック方式のままとする。

(a) MUA 側の設定について

MTA の指定は FQDN で行っている。メールサービスが IPv6 未対応のため、社外の DNS では A レコードのみ応答され、IPv4 通信のみ可能となる。

③ 特記事項

(a)MUA 側の設定について、IPv6 優先 PC の場合、DNS で名前解決した後、IPv4 通信に自動で切り替わるため、利用上の問題は特になしと想定し、試験を行った。

(11) 社外のクラウドサービス

① 要素説明

不特定多数の一般ユーザ向けに公開する動画配信サービスを動作させるクラウド(VPS)である。本動画配信サービスはクラウドサービス上の仮想サーバ環境を用いて構築する。

② 方式設計

クラウドサービスは、IPv6をサポートしている ConoHa VPS⁵⁸を利用する。IPv6 対応のため、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
(サービス提供者から払い出されたグローバルアドレス)
- IPv6 アドレス…同上

③ 特記事項

特になし。

以上を踏まえ、IPv6 対応後のシステム構成図を図 5.2.4-1 に示す。

⁵⁸ GMO Internet 社のクラウドサービスである。

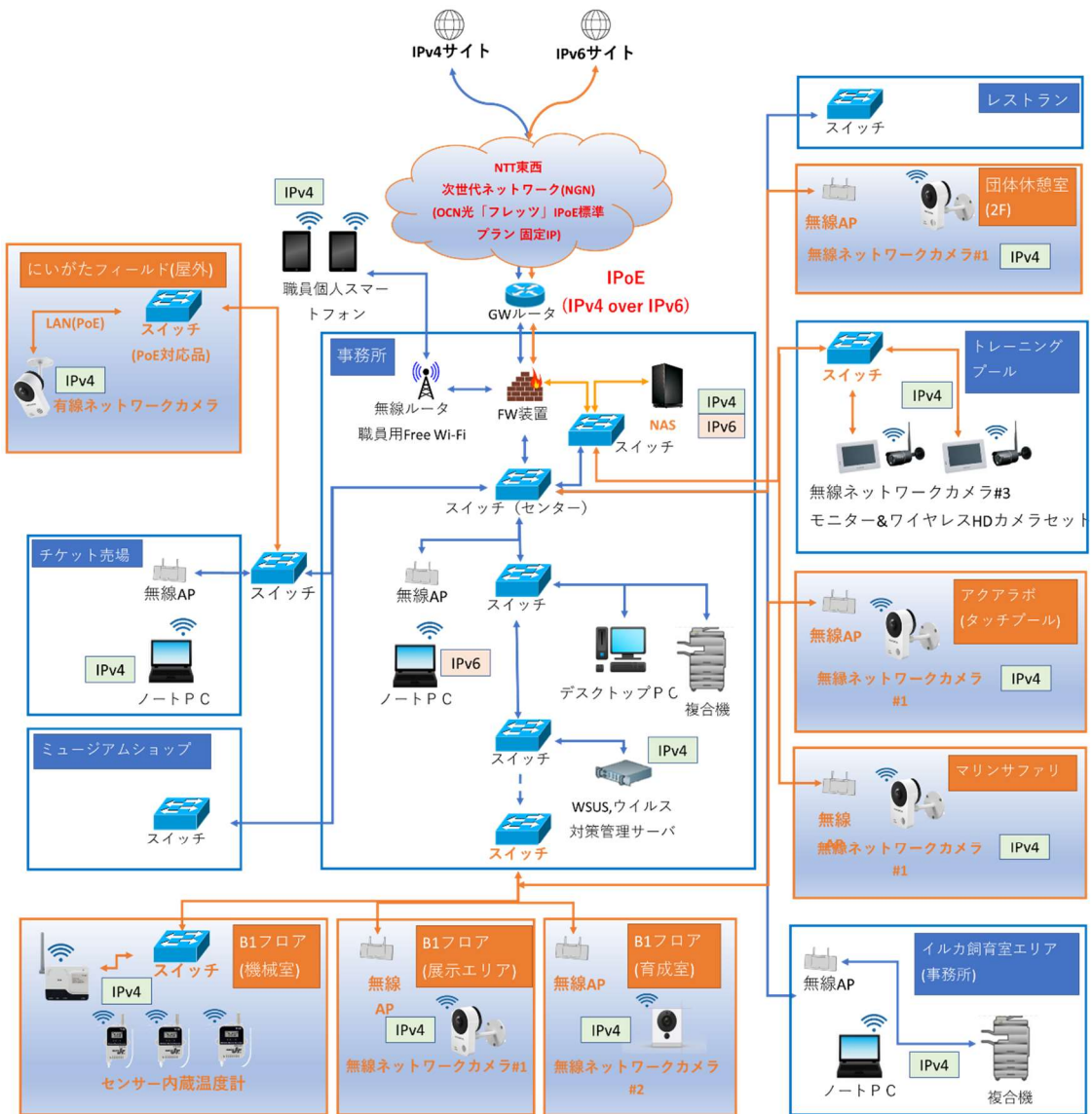


図 5.2.4-1 IPv6 対応後のネットワーク構成図

5.2.5 構築

本ユースケースでは検証環境構築において、以下の流れで機器や環境の検討を行った。(1)～(4)において各検討過程における課題を記載し、(5)にその解決策・対応方針を記載する。

(1) プロバイダの選定

まず初めに、既存プロバイダは IPv6 未対応であったため、乗り換えが必要であった。

令和元年度の事業では IPv6 の PPPoE 接続による実証実験を実施していたため、今回は IPoE 接続によるデュアルスタック化に着目し、IPoE 対応を前提としたプロバイダの選定を実施した。

【プロバイダ選定における課題点】

今回の実験環境では、一般業務において WEB サービス上のグループウェアを利用している。ここでは市の情報を取り扱っていることや、職員が業務時間外に社外から業務に触れる機会を持たせないため、WEB サービス側で社外からの参照を禁止するよう、固定 IPv4 アドレスによるアクセス制限を行っている。しかし、グループウェアが IPv6 未対応であるため、固定 IP(v4)による制限を継続する必要がある。このため、IPoE に対応し、かつ IPv4 の固定 IP が利用可能であるプロバイダの選定が必須となる。

(2) ネットワーク設計の検討

プロバイダを選定した後は、IPoE 接続を前提としたネットワーク構成を検討した。

今回の実証実験環境に IPv6 を導入するためには、既存環境への影響を最低限とするため、以下の3つの課題を解決する必要がある。

【ネットワーク設計における課題点】

① GW ルータ変更によるセキュリティ低下への懸念

既存環境では FW 装置を GW ルータ兼 FW 装置として運用している。

しかし、上記の FW 装置は PPPoE での IPv6 接続は可能だが、IPoE 接続には対応していない仕様であった。

単純に GW ルータの置き換えを行ってしまうと FW を撤去することになってしまい、既存のセキュリティが維持できなくなってしまう。更に FW ではポートベース VLAN で基幹ネットワークとゲスト用 Wi-Fi との接続を分離しているため、この構成を新しい GW ルータを導入した環境でも実現する必要がある。

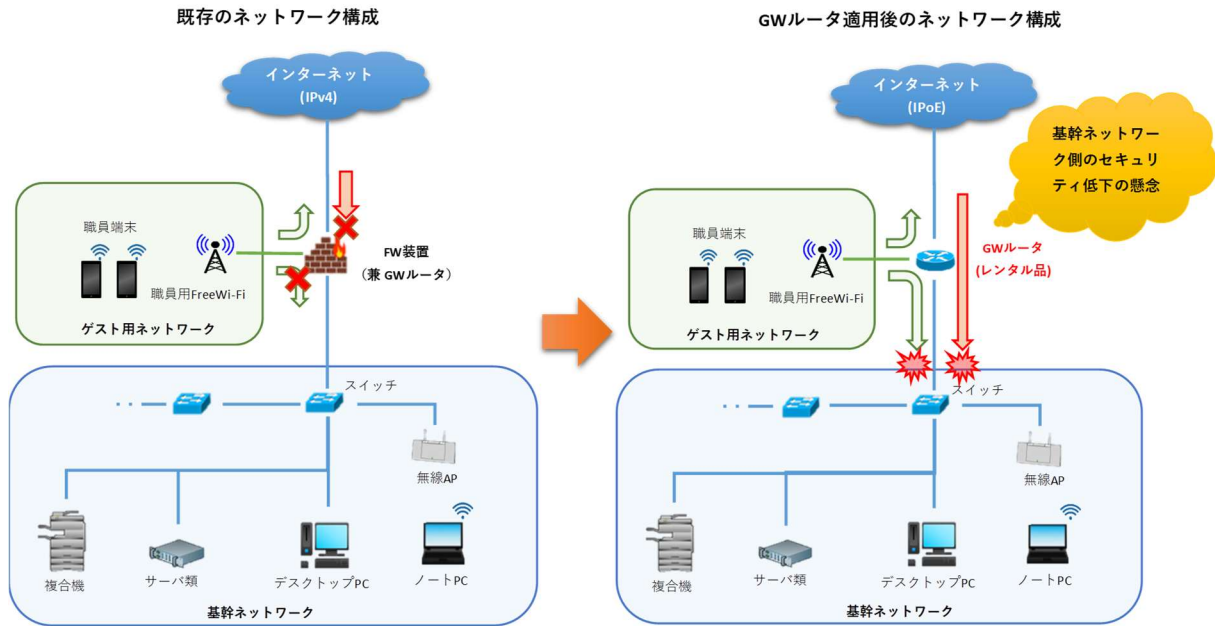


図 5.2.5-1 GW ルータ置き換えによるセキュリティ低下の懸念

② 基幹ネットワークに対する DHCP 有効化の影響

既存環境では端末管理のため GW ルータの DHCP 機能を無効化しており、機器は全て固定の IPv4 アドレスで運用している。本来、IPv6 対応機器はアドレスを自動割り当てすることが理想的であるため、IPv4 は DHCP 無効のまま、IPv6 のみ DHCP で運用したい。しかし、GW ルータによっては、IPv4 と IPv6 の DHCP 機能を個別で制御できない機器も存在している。既存機器に対して DHCP の影響を避けながら、IPv6 だけ DHCP を適用できるような方法を検討する必要がある。

また、一部のネットワークカメラにおいては、IPv6 非対応機器であるが、IP アドレスの設定手段が DHCP のみである。本機器は基幹ネットワーク上で運用する必要があるため、IPv4 の DHCP が無効化されている環境において、どのような手段で機器を導入するのも課題となった。

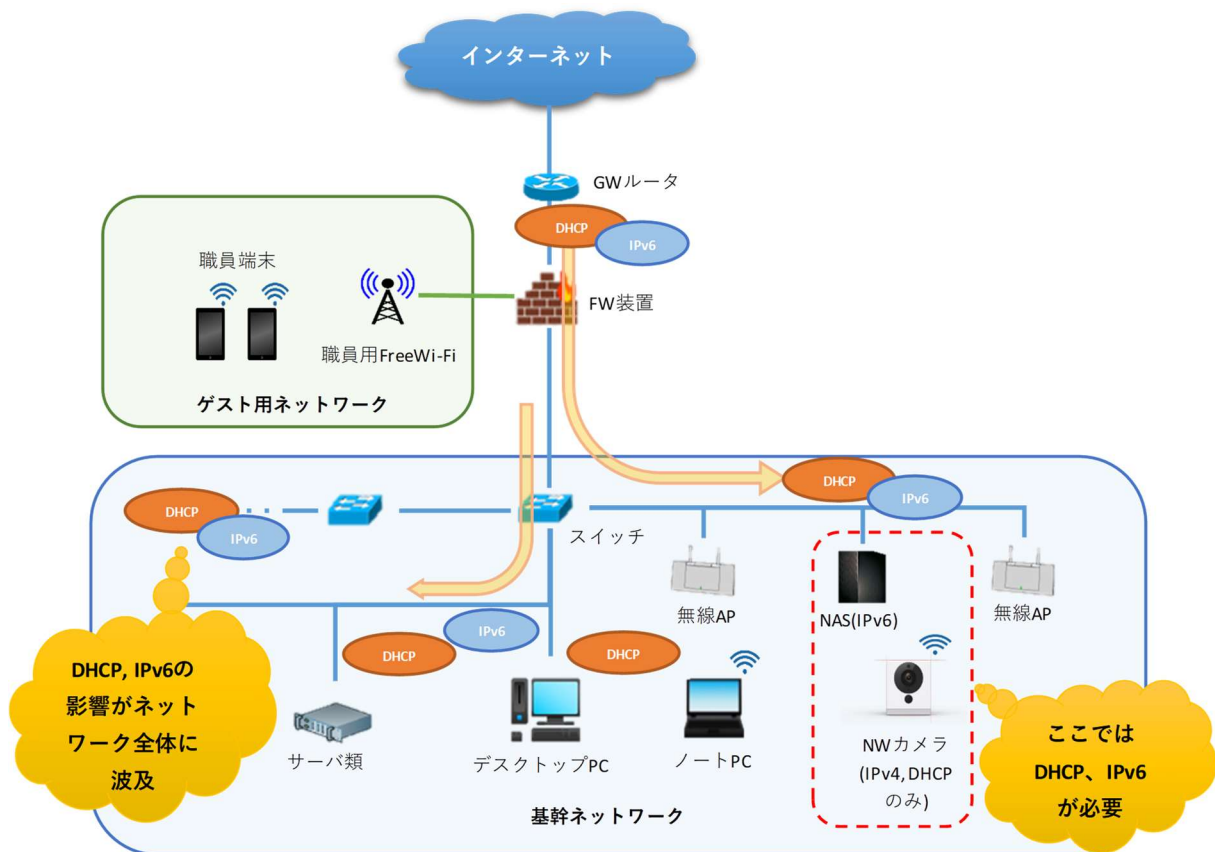


図 5.2.5-2 DHCPを有効化した場合のネットワーク全体への影響の懸念

③ IoT 機器を踏み台とした、不正アクセスの懸念

外部からのリモートアクセスが発生するIoT 機器に関しては、機器自身が不正アクセスに会うリスクが少ないとは言えず、更に踏み台となり基幹ネットワーク側に被害を及ぼすリスクを考慮する必要がある。

WEB サーバを外部公開する場合、緩衝地帯(DMZ)を構築して基幹ネットワーク側へ被害を避けるため隔離した領域を構築するのが一般的であると考えられるが、様々な個所に配置が必要なIoT 機器の場合においては適用しにくい(将来的にIoT 機器が接続されている場所から基幹ネットワークへのアクセスが必要となった場合、完全に独立するネットワークを新たに構築する必要が生じ、コスト増となるため)。

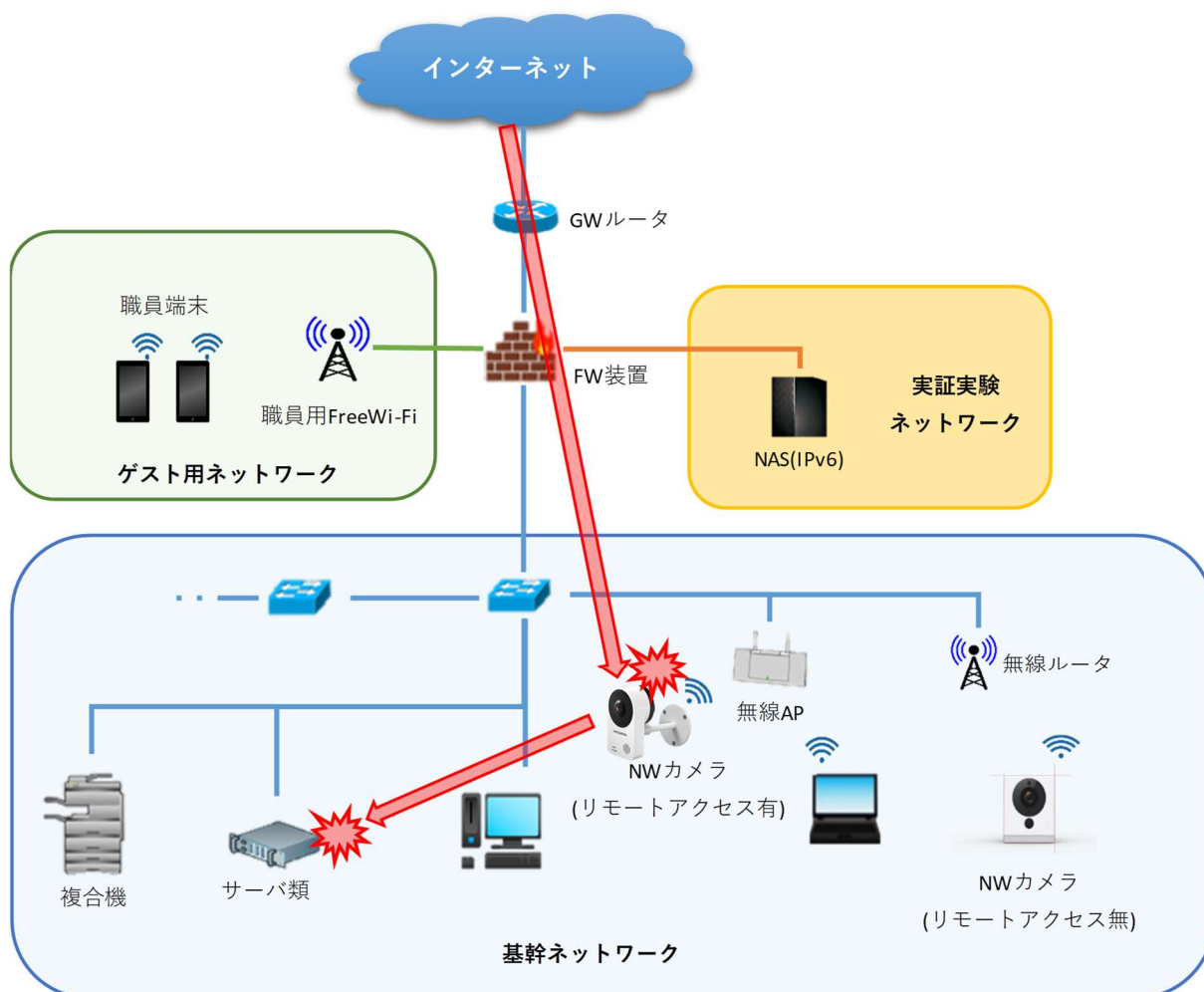


図 5.2.5-3 リモートアクセスによる、不正アクセスのリスク

(3) 実験機器の選定

既存機器を含めた、今回の実証試験シナリオに利用する選定機器の一覧を以下に示す。

表 5.2.5-1 選定機器の一覧

区分	概要	機器ベンダ	型番	IPv6 対応	リモート接続
新規	GW ルータ	YAMAHA	RTX830	○	—
既存	FW 装置	YAMAHA	FWX120	○	—
既存	ゲスト用 Wi-Fi	BUFFALO	WXR-1900DHP3	○	—
新規	NAS	I/O データ	HDL2-AAX16	○	○
新規	ネットワークカメラ	I/O データ	TS-NA220(W)	×	○
新規	ネットワークカメラ	ATOM	ATOM Cam	×	○
既存	ネットワークカメラ	マスプロ	WHC7M3/10M3	×	○
新規	ネットワークカメラ	Panasonic	BB-SC シリーズ	○	○
新規	センサー内蔵温度計	T&D	RTR-500BW	×	○

○:サポート、×:非サポート

ネットワークカメラにおける選定では、IPv6 対応していること、かつリモートから映像を参照できる機器を中心として選定を行った。

しかし、現状でも IPv6 の対応を謳う機器は少なく、仮に対応していたとしても、比較的高価な機器がほとんどであった。

選定の候補に挙げたものは Panasonic 製のネットワークカメラが、IPv6 対応かつクラウド上に録画データを保存できる機能を持っていたため、有力な候補であった。

外部から社内ネットワーク側へのアクセスを抑えることが可能なクラウド録画方式は、セキュリティ上望ましい。しかし、そのクラウドサービスである「みえますねっと」が IPv6 に対応していないことがマニュアル上に明記されていたため、選定対象から除外した。

【機器選定における課題点】

特にネットワークカメラにおいて、IPv6 対応している機器は高価なものが中心で、IPv6 対応機器の選択肢が少ない。

データ保存・参照がクラウド上で完結する機器はいくつかあったが、IPv6 対応・非対応を明示していない機器が多く、更にもその中でクラウドサービス含めて IPv6 にも対応している機器を見つけることは、困難な状況であった。

(4) クラウドサービスの選定

IPv6 環境における外部システム・商用サービス等への影響を検証するクラウドサービスの選定を行った。現環境のプロバイダ、メールサービスで GMO を利用しており、同社提供のサービスで利用可能なものがないかを検討した。その中で、環境構築の自由度が高く、保守性も優れている点で「WADAX」の「専用サーバプラン」を第一候補として検討した。

【クラウドサービスの選定における課題点】

「WADAX」にはいくつかのプランが存在しており、そのプランによって IPv6 の対応状況が異なっていた。当初候補としていた「専用サーバ」は IPv6 接続に未対応であることが、サポートへの問い合わせの結果判明した。

(5) (1)～(4)における課題解決

【(1)の課題解決の方針、実施内容】

IPv6 の環境適用において、この運用上の条件は必須であったため、プロバイダの選定においては、以下に注目して選定を行った。

- ・IPoE が利用できること
- ・固定 IPv4 アドレスが取得できること

IPoE が利用可能なプロバイダは多いが、固定 IPv4 も取得可能なプロバイダは少なく、選定対象に残ったプロバイダは以下の通りであった。

- ・OCN 提供の「フレッツ」IPoE 標準プラン 固定 IP」
- ・DiX 提供の「IPoE (IPv6) オプション」
- ・IPQ 提供の「IPoE 接続プラン」
- ・インターリンク提供の「ZOOT NATIVE」

DiX に関しては、1 つの固定 IPv4 アドレスを無料で利用できることを前面に出していたが、IPoE と固定 IPv4 アドレスの併用ができないことが問い合わせで分かったため、選定対象から除外した。残ったプロバイダからコスト面、導入のしやすさを見て吟味したが、GWルータがレンタル可能であること、法人向けプランとして提供されていることを鑑み、OCN「フレッツ IPoE 標準プラン 固定 IP」を最終的に選定した。

【(2)の課題解決の方針、実施内容】

① GW ルータ変更によるセキュリティ低下への懸念について

IPoE に対応した GW ルータを入手、またはレンタルを検討した結果、自営端末を用意して利用することもできたが、プロバイダからのサポートが利用できなくなる点などを考慮し、最終的にはレンタルルータを利用する構成で環境を構築した。

現状の FW をそのまま活かす方針とし、FW は GW ルータと内部ネットワークの中間に配置することで、内部ネットワークは今まで通りのセキュリティが維持されるようにした。

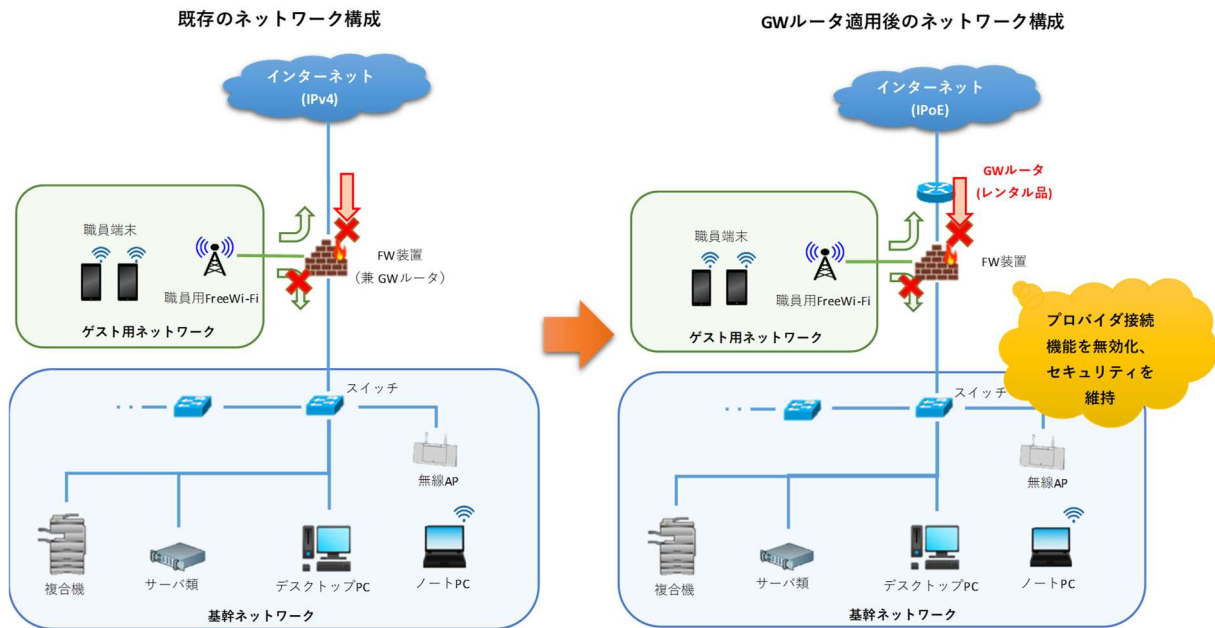


図 5.2.5-4 プロバイダ接続機能無効化によるFW 装置の運用

② 基幹ネットワークに対する DHCP 有効化の影響について

基幹ネットワークの機器に意図せず IP アドレスが振られてしまうことを防ぎ、かつ IPv6 接続を遮断するポリシーを踏襲するため、FW を以下のように設定する方針とした。

- GW ルータ側→基幹ネットワーク側への通信に対し、IPv4 パケットの DHCP を遮断する。
- GW ルータ側と基幹ネットワーク側、双方向の通信に対して、IPv6 パケットを全て遮断する。

また、基幹ネットワーク上の機器で DHCP が必須であるネットワークカメラに対しては、拡張したネットワーク上に DHCP サーバ機能を持つ無線ルータを新たに設置することで課題の解決を図った。本ルータに無線接続した機器に限定して DHCP を有効化し、更にルーティング機能により無線ルータのローカルネットワーク側と基幹ネットワーク側を双方向に接続することで、IoT 機器をインターネット接続可能とする設計とした。

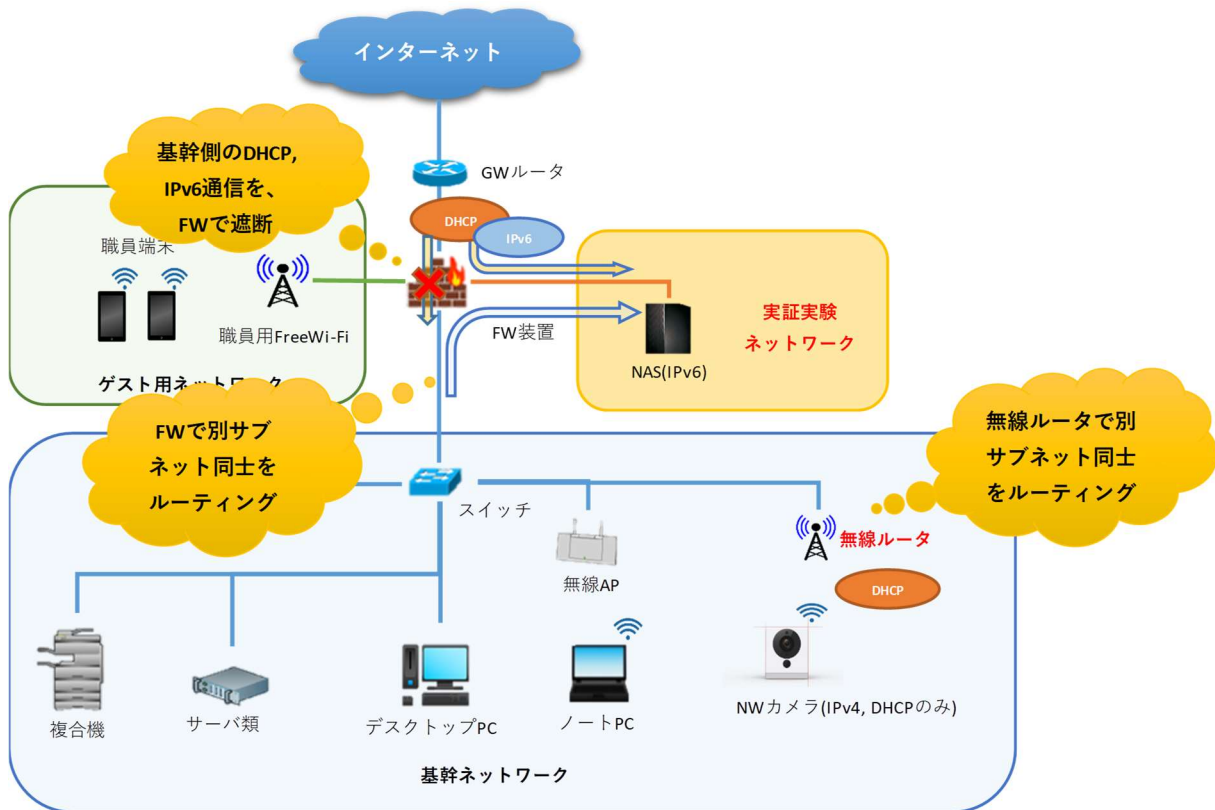


図 5.2.5-5 VLANとルーティングを利用した DHCP, IPv6 の適用

- ③ IoT 機器を踏み台とした、不正アクセスの懸念について
 基幹ネットワークと外部からアクセスが発生する実証実験ネットワークの分離は、元々FW がポートベース VLAN でアクセス分離していたため、FW 本体の未使用ポートを新たな VLAN として割り当てただけで基幹ネットワークから分離は行える。

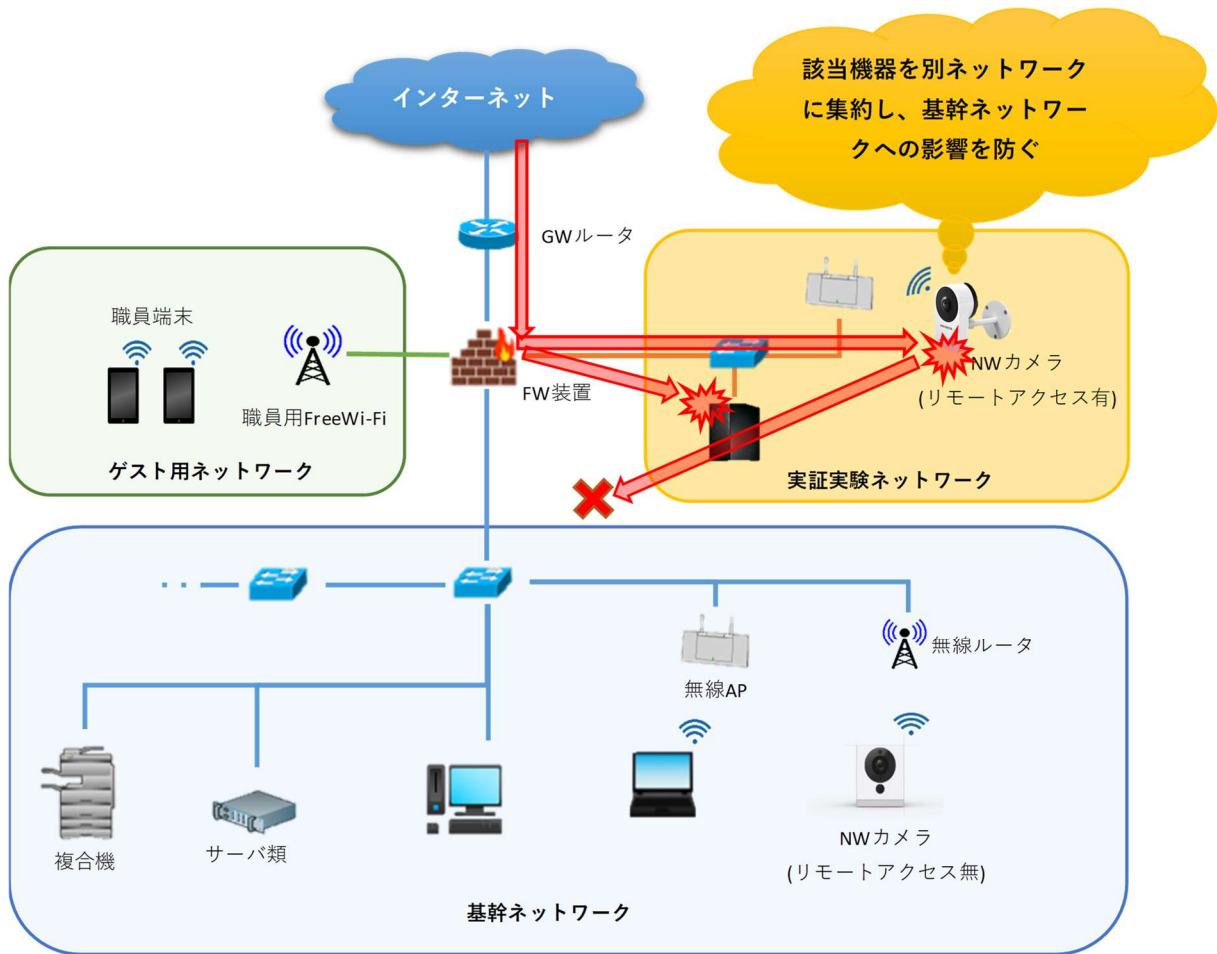


図 5.2.5-6 VLANを用いた基幹・実証実験ネットワーク分離

しかし、実証実験後の運用を検討した結果、同ネットワークからも基幹ネットワークへのアクセス可能となるような拡張性を持たせることが望ましかった。

将来的なネットワーク拡張時に機器導入のコストを抑えるため、基幹ネットワークと実証実験ネットワークを論理的に分離し、最終的にインテリジェントハブ側の設定により接続制御を行える方針とした。

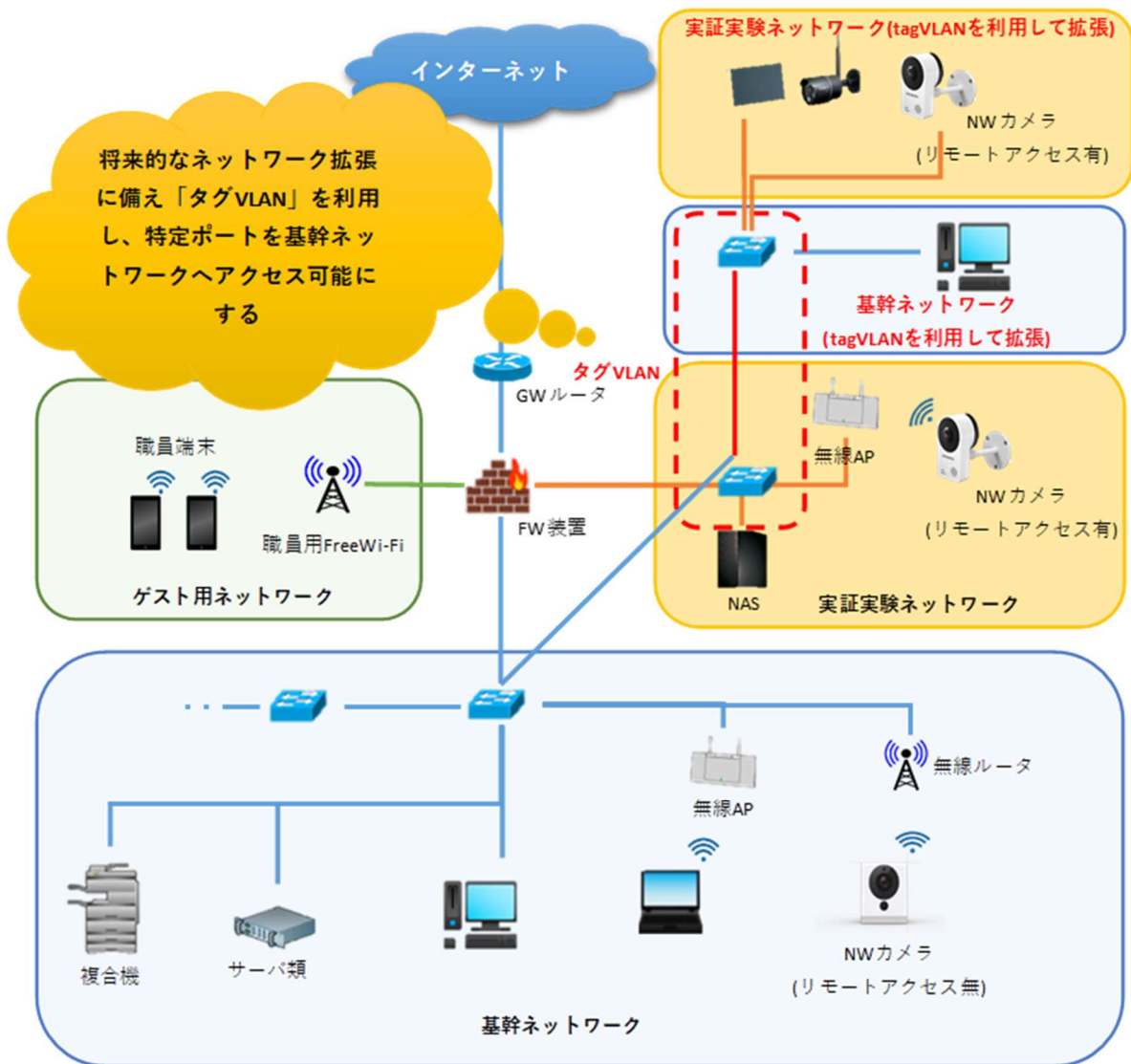


図 5.2.5-7 タグ VLAN を用いたネットワーク拡張のイメージ

【(3)の課題解決の方針、実施内容】

ネットワークカメラの構成については、IPv6 対応機器が高価であるため、IPv6 非対応であるが一般的な中小企業が入手しやすい価格帯の機器を中心に選定した。NAS 連携が可能な I/O データ製のネットワークカメラに関しては、録画した動画データを NAS 上に保存し、動画データの参照は NAS に対してリモート接続する構成とした。(イントラネット側は IPv4、リモート側は IPv6 で接続する想定)

センサー内蔵温度計については、IPv6 対応されている代替品が存在しなかったため、IPv4 対応の機器を選択し、IoT 機器と連携するクラウドサービス側にて IPv6 接続の検証を行う方針とした。

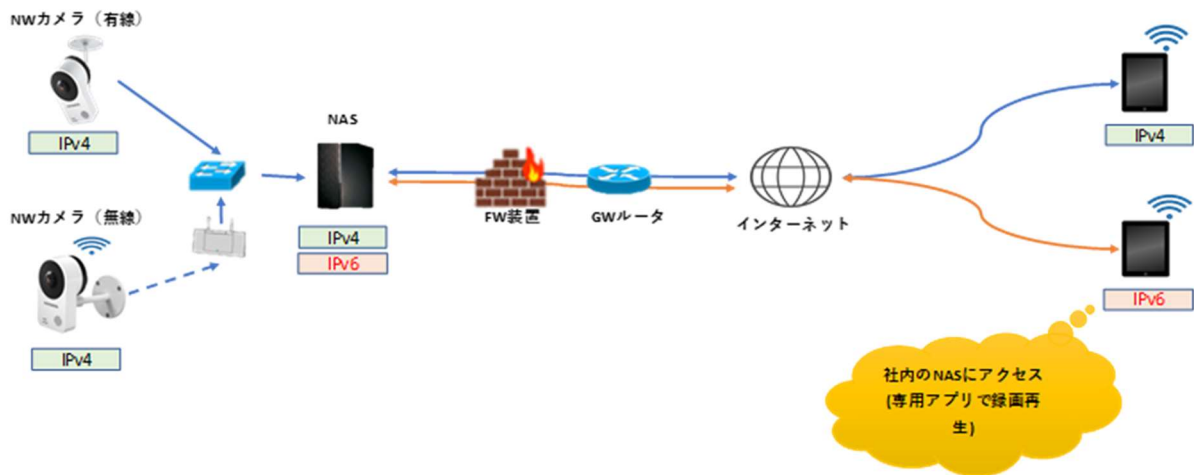


図 5.2.5-8 ネットワークカメラとNASの録画連携イメージ

【(4)の課題解決の方針、実施内容】

「WADAX」の「専用サーバ」は選定から外し、共用タイプのサーバにはなるが、同じ GMO が提供するクラウドサービスの中で、IPv6 接続の正式サポートが明確であった「ConoHa VPS」を最終的に選定した。

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 5.2.5-1 に示す。

表 5.2.5-2 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	デスクトップ PC	[Windows] HP prodesk400GS OS Windows10 Pro CPU Celeron® G4900 プロセッサー (3.1GHz) メモリ 8GB HDD 500GB [Mac] iMac OS OSX 10.13.4 CPU Intel Core i5(2.3GHz) メモリ 8GB HDD 1TB	・事務用
IPv4/ IPv6	ノート PC	[Windows] HP probook 450 G2 CPU Core™ i3-4030U プロセッサー (1.9GHz) メモリ 8GB SSD128GB	・事務用
IPv4	複合機	RICOH imagio MP C4002	・印刷
IPv4/ IPv6	無線ルータ (アクセスポイント)	BUFFALO WXR-1900DHP3	・ゲスト用 Wi-Fi
IPv4/ IPv6	タブレット、 スマートフォン	iPad Pro(10.5 インチ) Zenpad(Android) MOTOROLA moto g8(Android)	・事務用
IPv4/ IPv6	GW ルータ	YAMAHA RTX830	・ルーティング
IPv4/ IPv6	FW 装置	YAMAHA FWX-120	・ファイウォール
IPv4	スイッチ	BUFFALO BS-GS2008P	・スイッチング

設定	機器等	仕様例	備考
IPv4	無線ルータ	BUFFALO WSR-2533DHP3-BK	・ネットワークカメラの無線接続
IPv4	無線アクセスポイント	BUFFALO WAPS-1266	・ネットワークカメラの無線接続
IPv4	有線ネットワークカメラ	I/O データ TS-NA220	・構内監視
IPv4	無線ネットワークカメラ#1	I/O データ TS-NA220W	・構内監視
IPv4	無線ネットワークカメラ#2	ATOM ATOM Cam	・映像記録撮影
IPv4	無線ネットワークカメラ#3	マスプロ WHC7M3/10M3	・映像記録撮影
IPv4	センサー内蔵温度計	T&D RTR-500BW(親機) T&D RTR-500BL(子機)	・水温計 ・計測ログの収集
IPv4/ IPv6	NAS	I/O データ HDL2-AAX16	・構内監視映像の録画用
IPv4/ IPv6	ISP	・光NEXTギガライン データ送受信 1Gbps ・OCN 光「フレッツ」IPoE 標準プラン 固定 IP ・マルチホームなし	・インターネット接続
IPv4	メールサービス	GMO メールサービス	・メール
IPv4/ IPv6	ホスティングサービス	GMO 専用サーバ	・動画配信

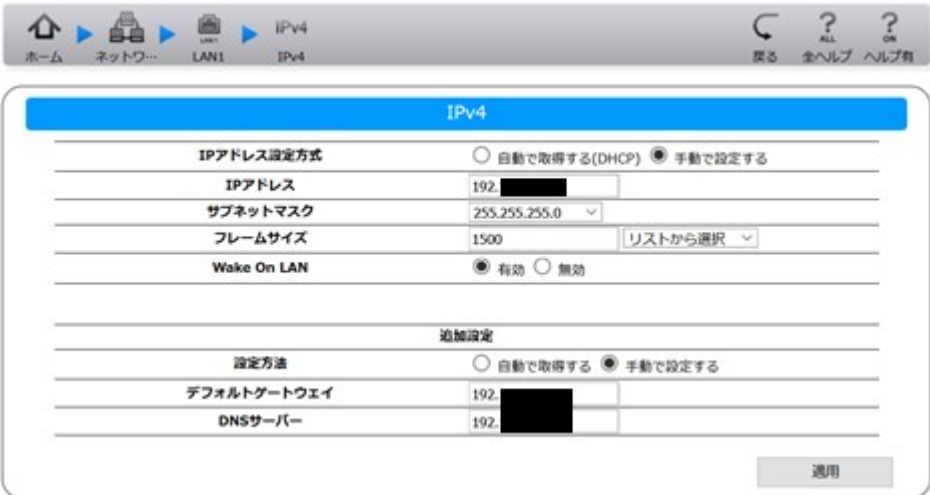

そして、IPv6 対応するために行った各機器への設定内容を示す。

(1) FW 装置の設定

項番	設定内容の詳細
1	<p>【基幹ネットワークのファイアウォール設定】</p> <pre>ipv6 filter 200000 pass * * icmp6 * * ipv6 filter 200001 pass * * tcp * ident ipv6 filter 200002 pass * * udp * 546 ipv6 filter 200098 reject * * * * * ipv6 filter 200099 pass * * * * * ipv6 filter dynamic 200080 * * ftp ipv6 filter dynamic 200081 * * domain ipv6 filter dynamic 200082 * * www ipv6 filter dynamic 200083 * * smtp ipv6 filter dynamic 200084 * * pop3 ipv6 filter dynamic 200085 * * submission ipv6 filter dynamic 200098 * * tcp ipv6 filter dynamic 200099 * * udp pp select 1 ipv6 pp secure filter in 200000 200001 200002 ipv6 pp secure filter out 200099 dynamic 200080 200081 200082 200083 200084 200085 200098 200099 pp enable 1 tunnel select 1 ipv6 tunnel secure filter in 200110 tunnel enable 1</pre>

(2) IoT 機器の設定

項番	設定内容の詳細
1	<p data-bbox="331 297 746 331">【ネットワークカメラ#1~3 の設定】</p> <div data-bbox="331 342 1161 958"><p data-bbox="355 365 435 387">カメラ情報</p><p data-bbox="355 398 387 421">映像</p><p data-bbox="355 432 451 454">ネットワーク</p><p data-bbox="355 465 499 488">ネットワーク設定</p><p data-bbox="355 499 435 521">無線設定</p><p data-bbox="355 533 467 555">リモート設定</p><p data-bbox="355 566 467 589">トラフィック</p><p data-bbox="355 600 483 622">マルチキャスト</p><p data-bbox="355 633 483 656">アクセスリスト</p><p data-bbox="355 667 467 689">カメラ検知設定</p><p data-bbox="355 701 419 723">保存設定</p><p data-bbox="355 734 419 757">システム</p><p data-bbox="355 768 467 790">アカウント管理</p><p data-bbox="355 801 531 824">セットアップウィザード</p><p data-bbox="563 365 738 387">■ ネットワーク設定</p><p data-bbox="587 409 738 432">ネットワークタイプ:</p><p data-bbox="587 432 1098 454">IPアドレス固定設定</p><p data-bbox="587 465 675 488">IPアドレス:</p><p data-bbox="587 510 1098 533">サブネットマスク:</p><p data-bbox="587 544 691 566">255.255.255.0</p><p data-bbox="587 577 770 600">デフォルトゲートウェイ:</p><p data-bbox="587 611 675 633">192.168.0.1</p><p data-bbox="587 645 722 667">プライマリDNS:</p><p data-bbox="587 678 675 701">192.168.0.1</p><p data-bbox="587 712 722 734">セカンダリDNS:</p><p data-bbox="587 745 1098 768">HTTPポート番号:</p><p data-bbox="587 790 1098 813">HTTPSポート番号:</p><p data-bbox="587 835 1098 857">RTSPポート番号:</p><p data-bbox="826 925 866 947">設定</p></div>

項番	設定内容の詳細
2	<p>【NAS の設定 (IPv4)】</p>  <p>IPv4</p> <p>IPアドレス設定方式 <input type="radio"/> 自動で取得する(DHCP) <input checked="" type="radio"/> 手で設定する</p> <p>IPアドレス 192. [REDACTED]</p> <p>サブネットマスク 255.255.255.0</p> <p>フレームサイズ 1500 [リストから選択]</p> <p>Wake On LAN <input checked="" type="radio"/> 有効 <input type="radio"/> 無効</p> <p>追加設定</p> <p>設定方法 <input type="radio"/> 自動で取得する <input checked="" type="radio"/> 手で設定する</p> <p>デフォルトゲートウェイ 192. [REDACTED]</p> <p>DNSサーバー 192. [REDACTED]</p> <p>適用</p> <p>【NAS 設定 (IPv6)】</p>  <p>IPv6</p> <p>IPアドレス設定方式 <input type="radio"/> 無効 <input checked="" type="radio"/> 自動で取得する(DHCP) <input type="radio"/> 手で設定する</p> <p>IPアドレス [REDACTED]</p> <p>プレフィックス長 64</p> <p>フレームサイズ 1500 [リストから選択]</p> <p>追加設定</p> <p>設定方法 <input checked="" type="radio"/> 自動で取得する <input type="radio"/> 手で設定する</p> <p>デフォルトゲートウェイ [REDACTED]</p> <p>DNSサーバー [REDACTED]</p> <p>適用</p>

(3) クラウド環境の設定

外部クラウドサービス(ConoHa VPS)に動画配信サービスを構築し、クラウドの仮想環境で IPv6 の有効化設定を行う。その他、ドメイン指定で仮想環境に接続できるように、DNS サービスに仮想環境の IPv6 アドレスを正引き登録する。

項番	設定内容の詳細
1	<p>【IPv6 アドレスの有効化設定】</p> <p>ネットワーク設定で IPv6 を利用可能にする。</p> <p>「ルータ+スイッチ」を作成する。</p> <p>名前: 任意の名称</p> <p>ルータ: 「はい」</p> <p>IPv6 アドレス: 「有効」</p> <p>その他はデフォルトを指定する。</p> <p>※「IPv6 の逆引き設定」は必須ではないため、設定なし。</p> <p>※参考</p> <p>https://manual.sakura.ad.jp/cloud/network/switch/ipv6.html</p> <ul style="list-style-type: none">・IPv6 の使用を開始する・IPv6 アドレスに逆引き DNS を設定する
2	<p>【クラウド環境のファイアウォール設定】</p> <ul style="list-style-type: none">・「WEB ポート」の IPv4 アクセスを有効化する。・「WEB ポート」の IPv6 アクセスを有効化する。 <p>※アクセス制御で指定できるポートは限定されている(Telnet、WEB、RDP 等)</p> <p>詳細なパケットフィルタを行う設定は、クラウドサービス上に存在していない。</p>
3	<p>ConoHa VPS に割り振られた IPv6 アドレスを、DNS に正引き登録する。</p>

5.2.6 試験

本ユースケースで実施した内容と結果を示す。

5.2.6.1 実証内容と結果

1. ネットワークレベルの検証

5.2.5にしたがって構築した実証環境において、一般業務とIoTシステム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、ネットワーク上に存在する情報資産(NAS)の利用といった一般的な業務について検証した。また、社内のセキュリティシステムの一部であるウイルス対策管理サーバや WSUS サーバ、勤怠管理に利用する静脈認証端末、および固定 IPv4 アドレスでアクセス制限を行っているクラウド上のグループウェアサービスに対しても、IPv6 を適用した環境で正常に利用できるか検証した。

IoT システムにおける検証では、社内ネットワーク上で稼働している IoT 機器に対する疎通性と動作の正常性を検証した。

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 2 件、IPv6 対応における留意事項が 2 件発生した。

(1) 一般業務における検証について

IPv4 の経路(ルータおよび回線)と、IPv6 の経路(ルータおよび回線)は IPoE 接続により1回線(1プロバイダ)に統合された状態でインターネットに接続し、接続先の IPv6 対応状況で、通過する経路が切り替わる設計である。

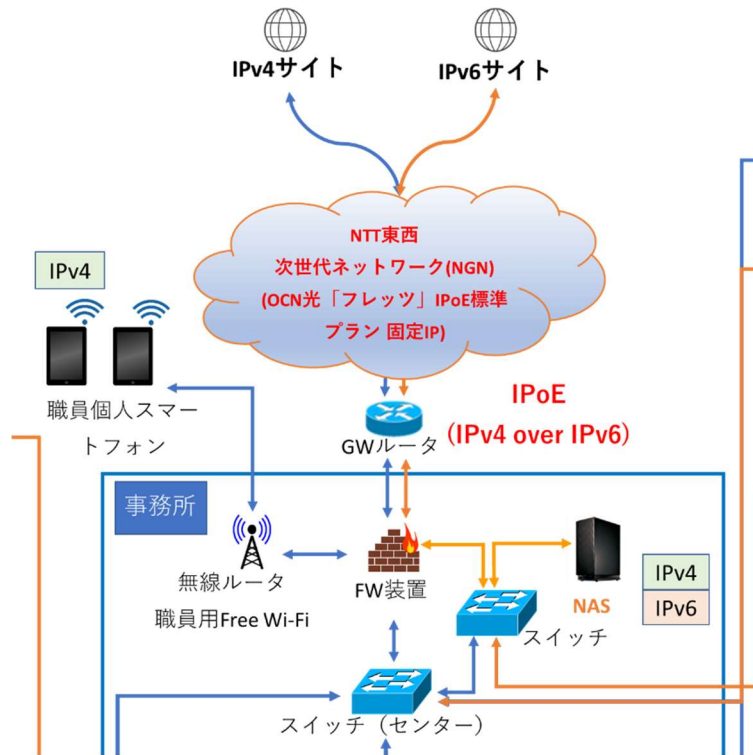


図 5.2.6-1 IPv4 経路と IPv6 経路

① 疎通確認

各機器に対して ping を実行し、通信経路に問題ないことを検証する。

また、IPv4/IPv6 が混在する「実証実験ネットワーク」末端のスイッチングハブより IPv4 のみの「基幹ネットワーク」にアクセスすることが可能か、ping を実行して VLAN の通信経路を検証する。

② 通常業務を想定した WEB サービスやメール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。

また、VLAN で切り分けられた基幹ネットワークからインターネット接続ができることを検証する。

③ 通常業務を想定した社内ネットワーク機器の利用

IPv4 と IPv6 を VLAN で分離させた環境において、IPv4 機器である複合機、ウイルス対策サーバ、静脈認証端末および IPv6 機器である NAS を正常に利用できるか検証する。

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、FW 装 置	IPv6	接続先に対し ping を実行す る	ping が通る	OK
2	ノート PC	無線	IPv6 優先	外部 IPv6 サーバ	IPv6	接続先に対し ping を実行す る	ping が通る	OK
3	ノート PC	無線	IPv6 優先	NAS	IPv6	接続先に対し ping を実行す る	ping が通る	OK
4	ノート PC	無線	IPv6 優先	GW ルー タ、FW 装 置	IPv4	基幹ネットワーク側のポート に接続した状態で、接続先 に対し ping を実行する	ping が通る	NG

【#1 の補足】

GW ルータ、FW 装置へ IPv6 で ping の応答を受信できることを確認した。

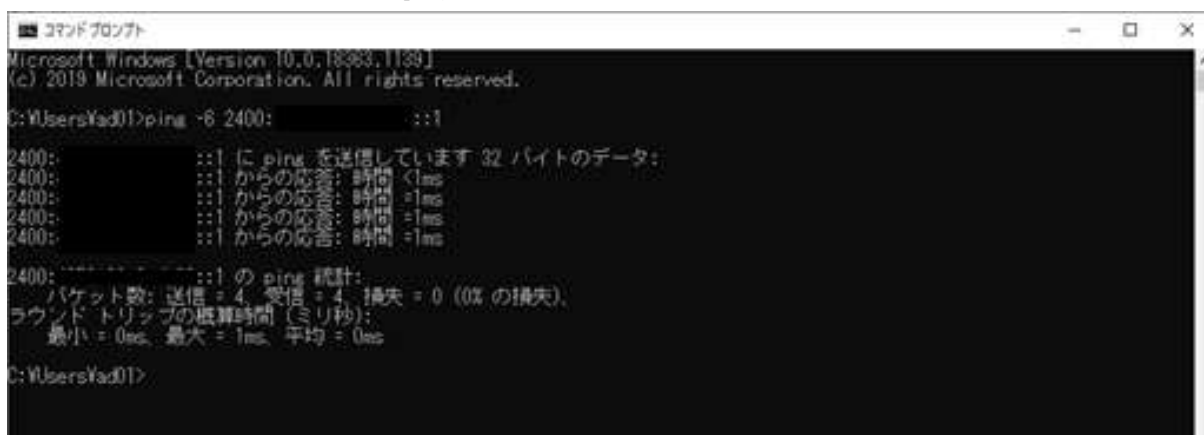


図 5.2.6-2 IPv6 で ping 応答あり(GW ルータ)

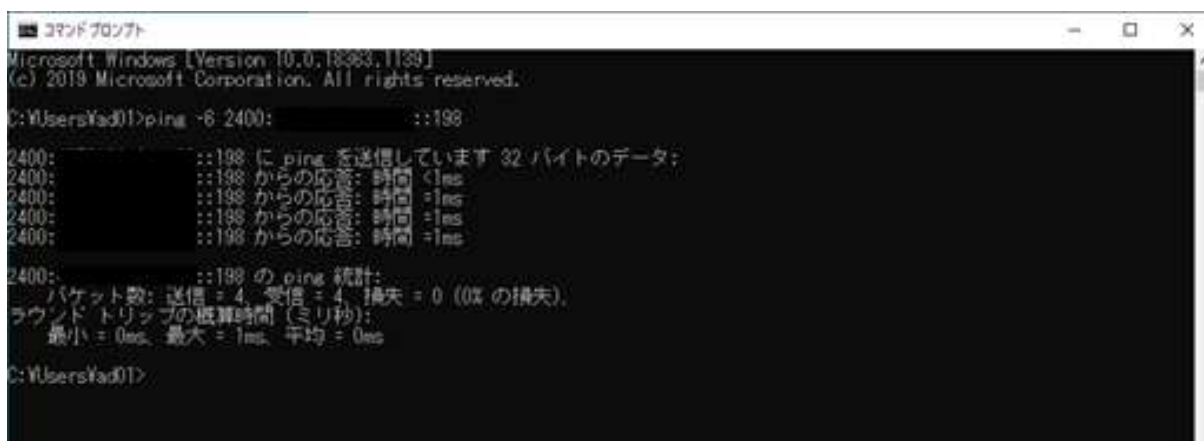
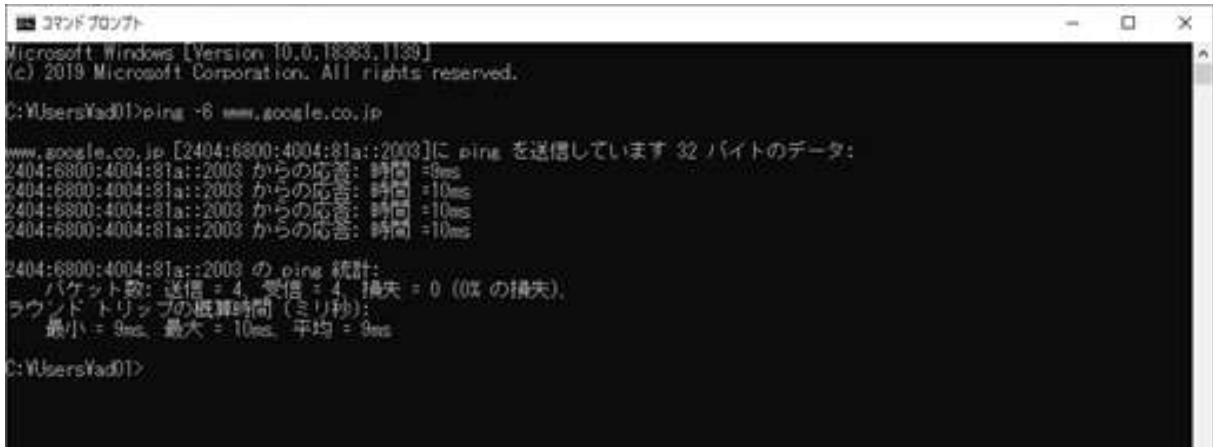


図 5.2.6-3 IPv6 で ping 応答あり(FW 装置)

【#2の補足】

外部サイト(www.google.com)へ ping 実行した場合も応答が返ってくることを確認した。



```
コマンドプロンプト
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Yad01>ping -6 www.google.co.jp

www.google.co.jp [2404:6800:4004:81a::2003]に ping を送信しています 32 バイトのデータ:
2404:6800:4004:81a::2003 からの応答: 時間 = 9ms
2404:6800:4004:81a::2003 からの応答: 時間 = 10ms
2404:6800:4004:81a::2003 からの応答: 時間 = 10ms
2404:6800:4004:81a::2003 からの応答: 時間 = 10ms

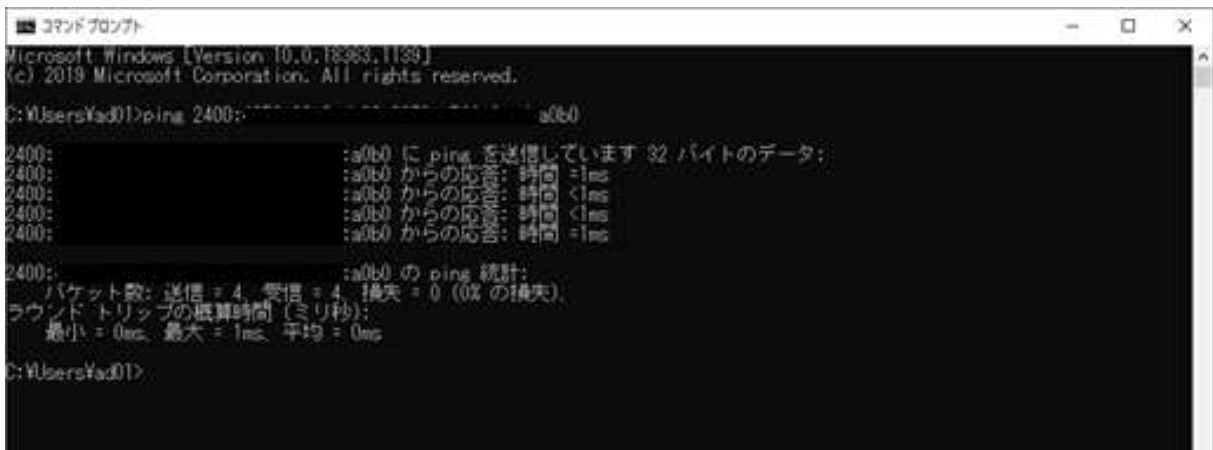
2404:6800:4004:81a::2003 の ping 統計:
    パケット数: 送信 = 4, 受信 = 4, 損失 = 0 (0% の損失),
    ラウンドトリップの概算時間 (ミリ秒):
        最小 = 9ms, 最大 = 10ms, 平均 = 9ms

C:\Users\Yad01>
```

図 5.2.6-4 IPv6 で ping 応答あり(外部サイト)

【#3の補足】

NAS へ ping 実行した場合も応答が返ってくることを確認した。



```
コマンドプロンプト
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Yad01>ping 2400:.....:a0b0

2400:.....:a0b0 に ping を送信しています 32 バイトのデータ:
2400:.....:a0b0 からの応答: 時間 = 1ms
2400:.....:a0b0 からの応答: 時間 <1ms
2400:.....:a0b0 からの応答: 時間 <1ms
2400:.....:a0b0 からの応答: 時間 = 1ms

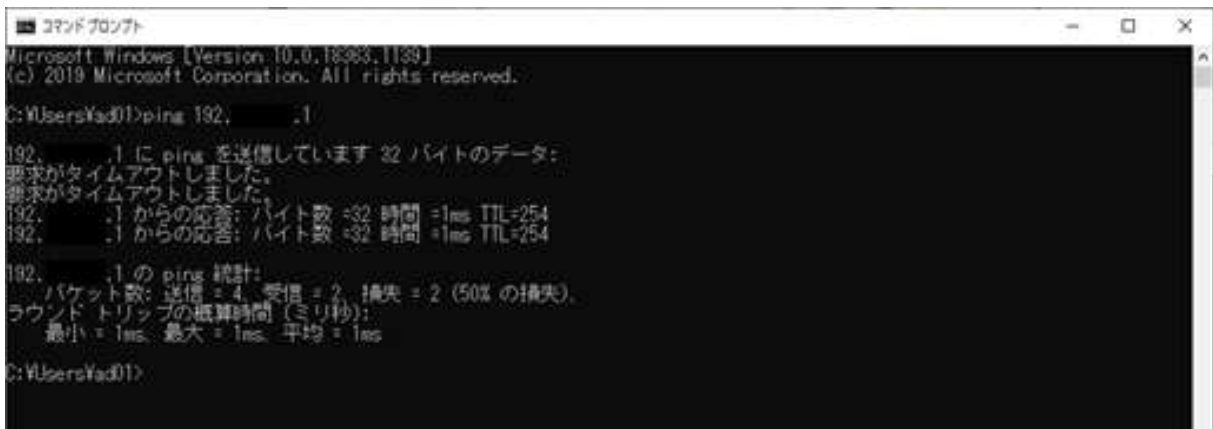
2400:.....:a0b0 の ping 統計:
    パケット数: 送信 = 4, 受信 = 4, 損失 = 0 (0% の損失),
    ラウンドトリップの概算時間 (ミリ秒):
        最小 = 0ms, 最大 = 1ms, 平均 = 0ms

C:\Users\Yad01>
```

図 5.2.6-5 IPv6 で ping 応答あり(NAS)

【#4の補足】

基幹ネットワークの GW ルータ、FW に対して ping を実行すると、タイムアウト発生の中、まれに応答が返るような実行結果が不安定になる現象が発生した。



```
コマンドプロンプト
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Yad01>ping 192.168.1.1

192.168.1.1 に ping を送信しています 32 バイトのデータ:
要求がタイムアウトしました。
要求がタイムアウトしました。
192.168.1.1 からの応答: バイト数 =32 時間 =1ms TTL=254
192.168.1.1 からの応答: バイト数 =32 時間 =1ms TTL=254

192.168.1.1 の ping 統計:
    パケット数: 送信 = 4, 受信 = 2, 損失 = 2 (50% の損失),
    ラウンドトリップの概算時間 (ミリ秒):
        最小 = 1ms、最大 = 1ms、平均 = 1ms

C:\Users\Yad01>
```

図 5.2.6-6 VLAN で IPv4 の ping 応答が不安定(2回タイムアウト後、2回応答あり)

本件は、実験ネットワークに VLAN を構築したスイッチの MAC アドレス学習方式(SVL 方式⁵⁹)が関係していた。FW 装置側はポートベース VLAN であり、LAN 側の4ポートが全て同一の MAC アドレスで構成されている。(機器仕様上、ポート毎に異なる MAC アドレスは設定できない)

実証実験ネットワークと FW 装置を接続していたスイッチは、MAC アドレスの学習方式が SVL であるため、LAN ポート間で同一の MAC アドレスをもつ FW 装置に対して、意図したポートにパケット送出できていなかった。

⁵⁹ Shared VLAN Learning。学習した MAC アドレスを、全ポートで共有する方式。

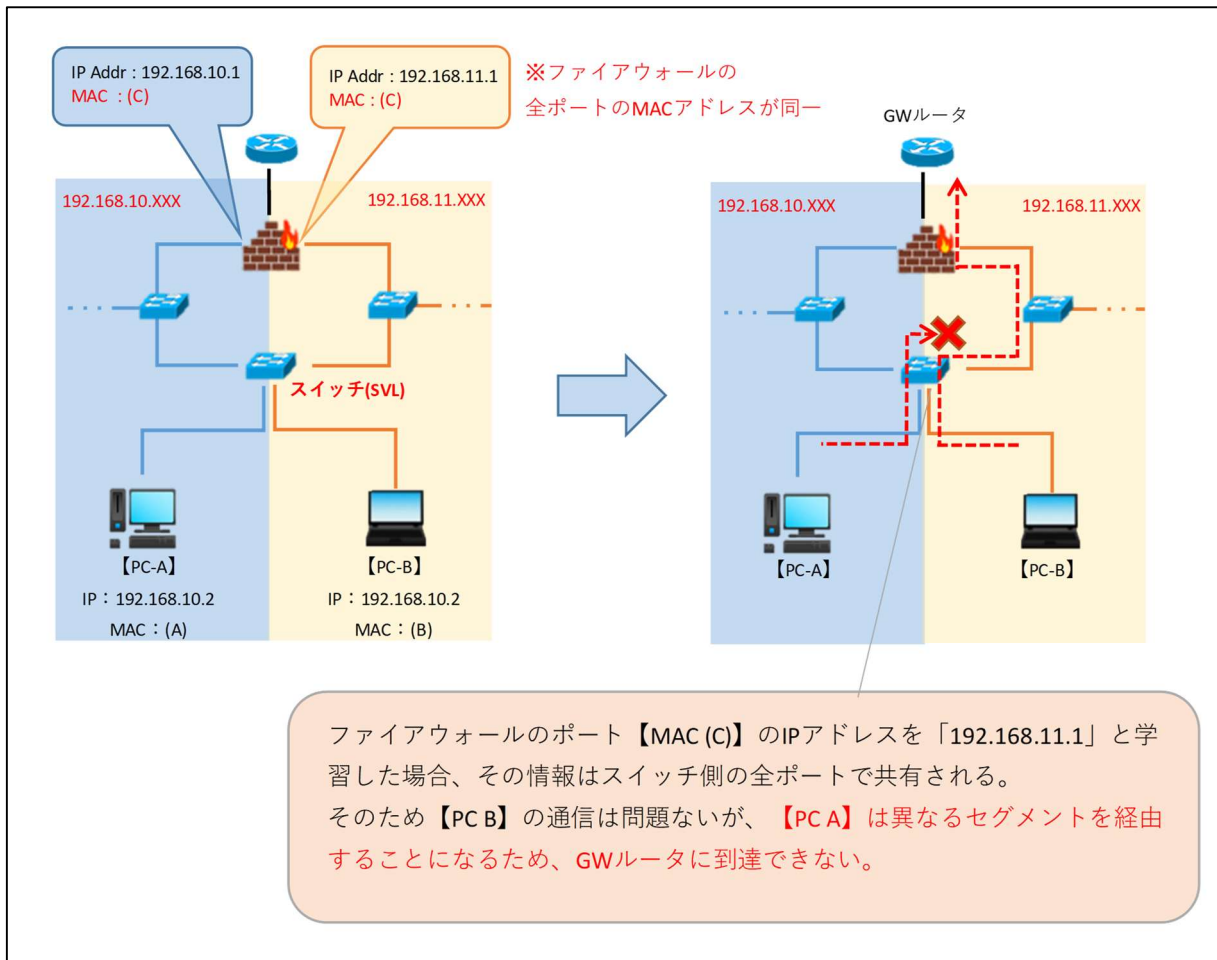


図 5.2.6-7 SVL 方式による MAC アドレス学習結果の例

この対策として、FW 装置と接続する該当のスイッチを、IVL 方式⁶⁰の機器に置き換えることにより、VLAN 間の通信が安定することを確認した。

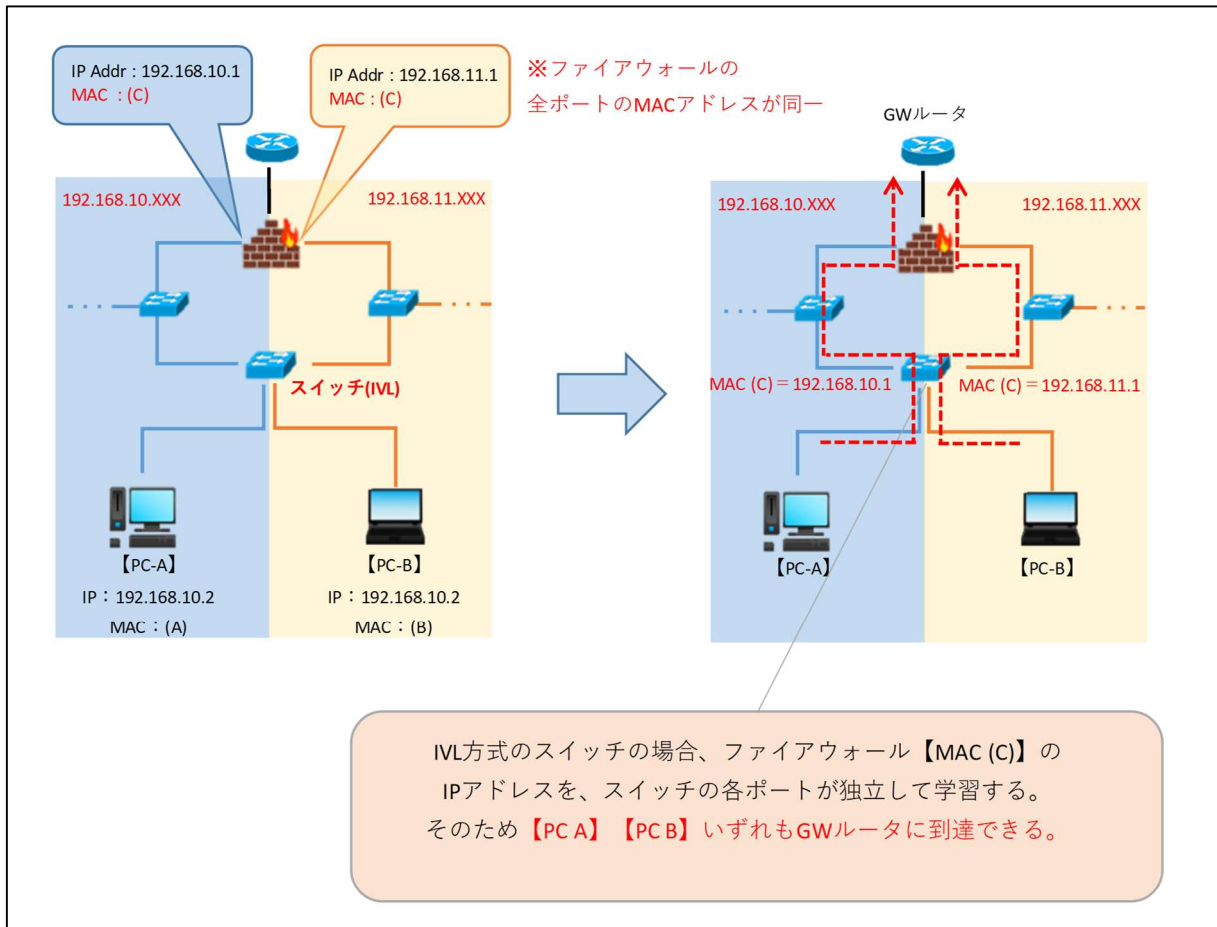


図 5.2.6-8 IVL 方式による MAC アドレス学習結果の例

⁶⁰ Independent VLAN learning. 学習した MAC アドレスを、各ポートで独立して記憶する方式。

② WEB サービスやメール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 (Windows)	無線	IPv6 優先	IPv6 未対応メールサービス	IPv4	実証実験ネットワークに接続した状態で、GMO メールサービス経由でメール送受信を行う	メールの送受信ができる	OK
2	デスクトップ PC (Mac)	有線	IPv6 優先	IPv6 未対応メールサービス	IPv4	実証実験ネットワークに接続した状態で、GMO メールサービス経由でメール送受信を行う	メールの送受信ができる	OK
3	ノート PC (Windows)	無線	IPv6 優先	インターネット	IPv6	実証実験ネットワークに接続した状態で、 https://ipv6.test-ipv6.com/ へアクセスする	WEB サイトへアクセスでき、かつ IPv4 アドレスと IPv6 アドレスが表示される	OK
4	デスクトップ PC (Mac)	有線	IPv6 優先	インターネット	IPv6	実証実験ネットワークに接続した状態で、 https://ipv6.test-ipv6.com/ へアクセスする	WEB サイトへアクセスでき、かつ IPv4 アドレスと IPv6 アドレスが表示される	OK
5	ノート PC (Windows)	無線	IPv6 優先	WEB サービス	IPv4	実証実験ネットワークに接続した状態で、WEB サービス(グループウェア)へアクセスする	正常にアクセスでき、提供機能が正常に利用できる	OK
6	ノート PC (Windows)	無線	IPv6 優先	インターネット	IPv4	VLAN(基幹ネットワーク)に接続した状態で、 https://ipv6.test-ipv6.com/ へアクセスする	WEB サイトへアクセスでき、かつ IPv4 アドレスのみが表示される	OK
7	スマートフォン (Android)	無線	IPv6 優先	インターネット	IPv4	ゲスト用 Wi-Fi に接続した状態で、 https://ipv6.test-ipv6.com/ へアクセスする	WEB サイトへアクセスでき、かつ IPv4 アドレスのみが表示される	OK
8	タブレット (iOS)	無線	IPv6 優先	インターネット	IPv4	ゲスト用 Wi-Fi に接続した状態で、 https://ipv6.test-ipv6.com/ へアクセスする	WEB サイトへアクセスでき、かつ IPv4 アドレスのみが表示される	OK

【#3,4の補足】

Windows および Mac 端末から IPv6 アドレスでアクセスできることを確認した。

あなたの IPv6 接続性をテストしましょう。



図 5.2.6-9 IPv6 でインターネット接続可能

【#5の補足】

IPoE接続においても、プロバイダから提供された固定 IPv4 アドレスを使用し、WEB サービスへアクセスできることを確認した。その後、異なるプロバイダからインターネット接続を行っている状態で WEB サービスに接続したとき、アクセス不可であることを確認した。



図 5.2.6-10 WEB サービスへアクセス不可

【#6 の補足】

VLAN 内の IPv6 アドレスが無効な環境においても、IPv4 アドレスのみでアクセスできることを確認した。

あなたの IPv6 接続性をテストしましょう。



図 5.2.6-11 IPv4 でインターネット接続可能(VLAN 環境)

【#7, 8 の補足】

IPv6 アドレスが無効なゲスト用 Wi-Fi 環境においても、モバイル端末が IPv4 アドレスのみでアクセスできることを確認した。

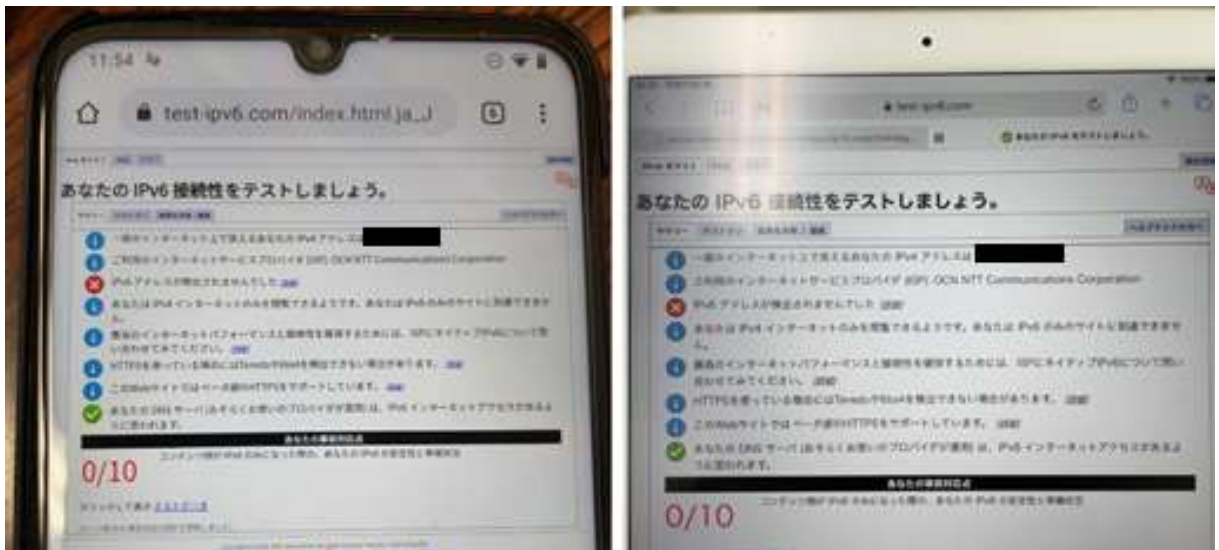


図 5.2.6-12 ゲスト用 Wi-Fi 環境でインターネット接続可能
(左:Android 端末、右:iOS 端末)

③ 社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 (Windows)	無線	IPv6 優先	複合機	IPv4	印刷処理を実行する	ネットワーク経由の印刷が正常に行える	OK
2	ノート PC (Windows)	無線	IPv6 優先	NAS	IPv6	ユーザ認証を実行し、ファイル参照する	ユーザ認証が正常に行われ、ファイル参照が行われる	OK
3	ノート PC (Windows)	無線	IPv6 優先	WSUS サービス	IPv4	WSUS 管理アプリケーションの画面を参照する	WSUS 管理アプリケーションが正常に稼働している	OK
4	ノート PC (Windows)	無線	IPv6 優先	ウイルス対策管理サービス	IPv4	ウイルス対策管理アプリケーション画面を参照する	ウイルス対策管理サービスが正常に稼働している	OK
5	デスクトップ PC (Windows)	有線	IPv6 優先	共同レジ精算システム	IPv4	専用アプリケーションを起動し、売上データのメール配信を実行する	メール配信が正常に実行できる	OK
6	デスクトップ PC (Windows)	無線	IPv6 優先	静脈認証端末	IPv4 想定	専用アプリケーションを起動し、勤怠データのバックアップ処理を実行する	勤怠データのエクスポート処理が正常に実行できる	OK
7	クレジットカード端末	有線	IPv4 想定	クレジットカードサービス	IPv4	クレジットカードの決済処理を行う	決済処理が正常に実行できる	OK

【#2の補足】

IPv4 アドレスと IPv6 アドレスをそれぞれ指定し、ユーザ認証とファイル参照が正常に行われることを確認した。

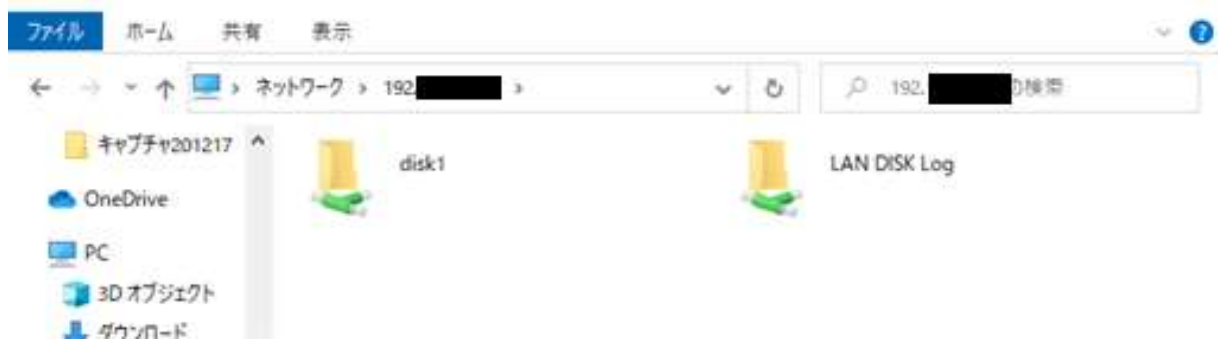


図 5.2.6-13 NAS のファイル参照 (IPv4 アドレス指定) のイメージ

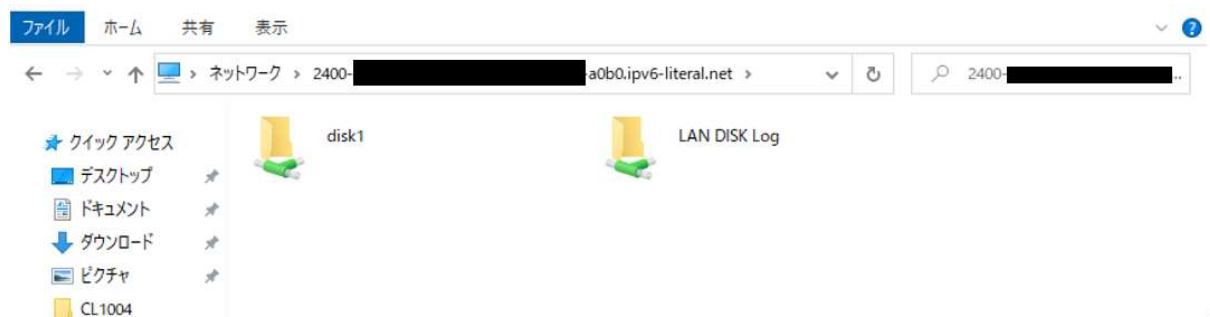


図 5.2.6-14 NAS のファイル参照 (IPv6 アドレス指定) のイメージ

(2) IoT システムにおける検証について

① IoT 機器の疎通、基本機能確認

基幹ネットワークおよび実証実験ネットワークに設置された IoT 機器の通信経路と基本機能の確認を行う。クライアント端末から各種 IoT 機器の管理画面へアクセスし、基本機能を正常に利用可能か検証する。管理画面を持たない IoT 機器については、ping を実行して通信経路を確認する。これらの試験結果を以下に示す。

①IoT 機器の疎通、基本機能確認の結果

#	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	有線	IPv6 優先	ネットワークカメラ	IPv4	WEB ブラウザで管理画面にアクセスし、ライブ配信映像を参照する	ライブ映像が管理画面上で参照できる(映像が途切れずに配信されている)	OK
2	ネットワークカメラ	有線	IPv4	NAS	IPv4	ネットワークカメラの NAS 録画機能を実行する	ネットワークカメラのライブ映像が NAS 上に録画保存される	OK
3	ノート PC	有線	IPv6 優先	センサー内蔵温度計親機	IPv4	接続先に対し ping を実行する	ping が通る	OK
4	既存ネットワークカメラ(親機)	有線	IPv4	アップデートサービス	IPv4	本体のソフトウェアアップデートを実行する	最新のアップデートが検出される	OK

【#1 の補足】

WEB ブラウザ上でネットワークカメラのライブ映像が正常に参照できることを確認した。

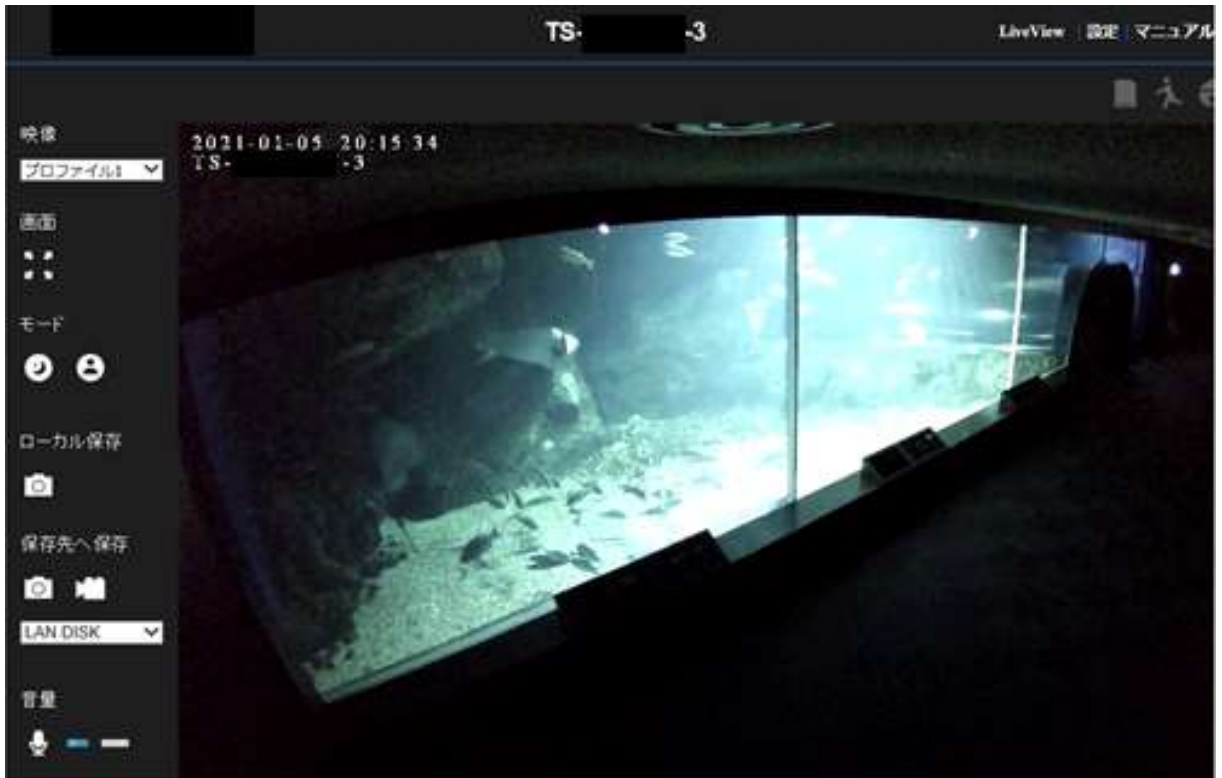


図 5.2.6-15 ネットワークカメラのライブ映像参照結果

【#2の補足】

ネットワークカメラのNAS録画機能が正常に参照できることを確認した。

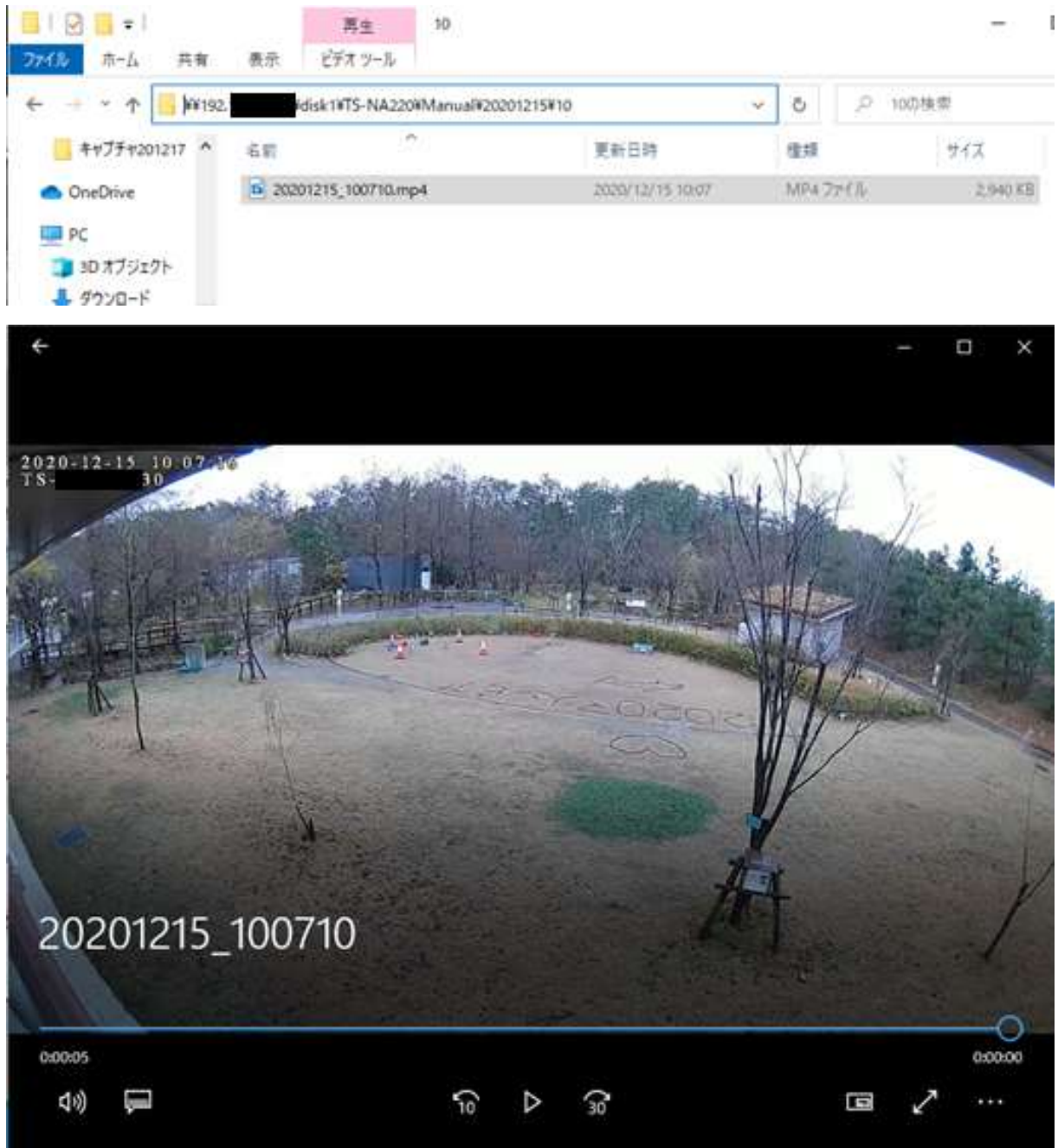


図 5.2.6-16 NAS録画映像の再生結果

【#4の補足】

既存ネットワークカメラ(親機)のソフトウェアアップデート機能が利用可能であることを確認した。



図 5.2.6-17 既存ネットワークカメラのソフトウェアアップデート
(左:ネットワーク未接続、右:ネットワーク接続後)

2. LAN 内アプリケーションレベルの検証

5.2.5 にしたがって構築した実証環境において、B 社の職員がリモートワーク等で外部から IoT 機器の利用を想定した場合、IPv6 環境を適用したネットワークでどのような影響を受けるかを検証した。検証には、モバイル端末で利用可能なベンダ提供のアプリケーションを使用した。

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 2 件発生した。

(1) 業務アプリケーションにおける検証について

① ネットワークカメラの動作検証

各種ネットワークカメラに対して、イントラネット向けのビューワーアプリケーション (Windows 端末で動作)、インターネット経由でアクセス可能なビューワーアプリケーション (Android, iOS 端末で動作)、それぞれを用いてアプリケーションの動作を検証した。

まずイントラネット用のビューワーアプリケーションでライブ配信映像が参照できることを確認し、その後、インターネット経由でライブ配信映像を参照できるか検証した。

② NAS のリモートアクセス検証

NAS に対して、インターネット経由でアクセス可能なビューワーアプリケーション (Android, iOS 端末で動作) を用い、IPv6 環境におけるアプリケーションの動作を検証した。

③ センサー内蔵温度計のクラウドサービス連携の検証

センサー内蔵温度計がインターネットを経由して送信している計測データを、IPv6 環境の PC からクラウドサービスにアクセスし、問題なく参照できるか検証した。

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 ネットワークカメラの動作検証の結果

#	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	有線ネットワークカメラ、無線ネットワークカメラ#1	IPv4	ビューワーアプリケーション「Qwatch Monitor」を実行する	ライブ映像が正常に参照できる	OK
2	スマートフォン	無線	IPv6 優先	無線ネットワークカメラ#1	IPv4	ビューワーアプリケーション「Qwatch View」を実行する	ライブ映像が正常に参照できる	OK
3	スマートフォン	無線	IPv6 優先	無線ネットワークカメラ#3	IPv4	ビューワーアプリケーション「iHomeCam」を実行する	ライブ映像が正常に参照できる	OK
4	スマートフォン	無線	IPv6 優先	無線ネットワークカメラ#2	IPv4	ビューワーアプリケーション「ATOM」を実行する	ライブ映像が正常に参照できる	OK

【#1の補足】

ノートPCでネットワークカメラのライブ映像が参照できることを確認した。

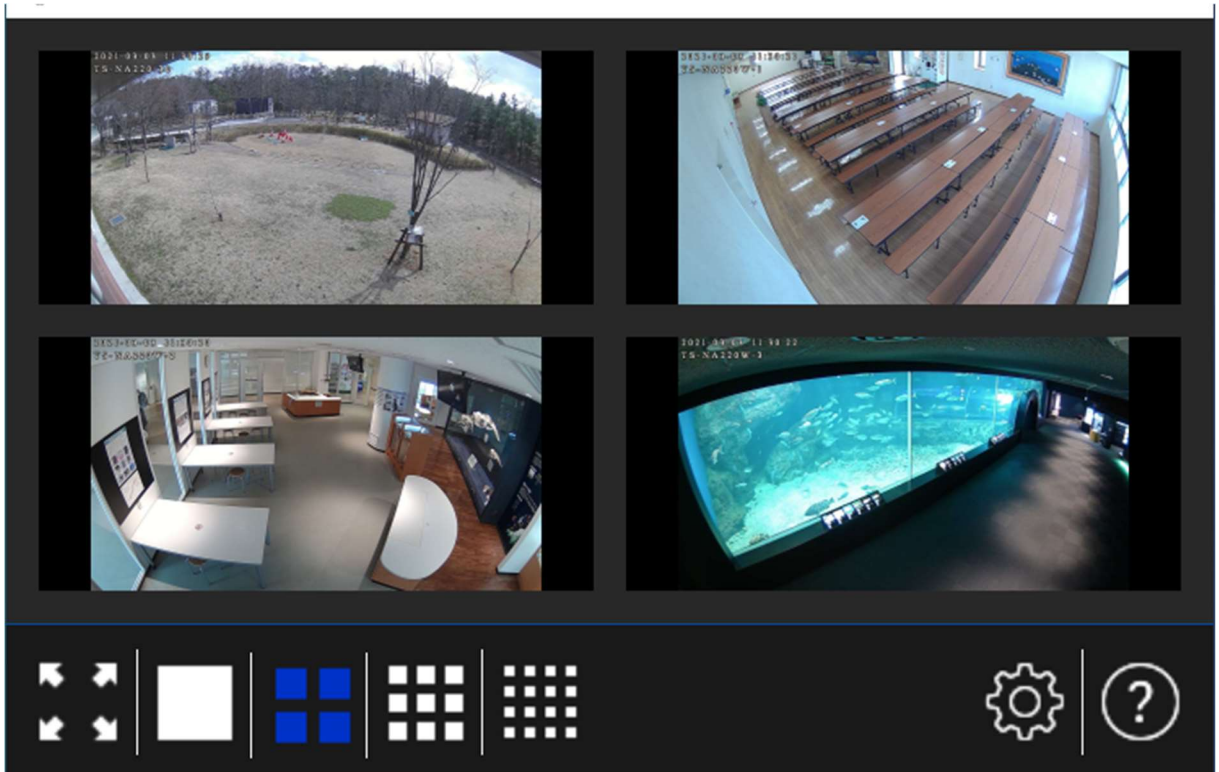


図 5.2.6-18 ビューワーアプリケーション実行結果(Qwatch Monitor)

【#2~4の補足】

スマートフォンで各種ネットワークカメラのライブ映像が参照できることを確認した。



図 5.2.6-19 ビューワーアプリケーション実行結果
(左:Qwatch View、中:iHomeCam、右:ATOM)

② NAS の動作検証の結果

#	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	スマート フォン	無線	IPv6 優先	NAS	IPv6 想定	ビューワーアプリケーション 「RFFiles」を実行する。	ストレージ内の動画ファイル が正常に参照できる。	NG

【#1 の補足】

スマートフォンから NAS へのリモート接続が可能であることを確認した。

下図の左から、リモート接続前の状態、接続中の状態、接続完了の状態となる。



図 5.2.6-20 NAS のリモート接続結果 1(左:接続前、中:接続中、右:接続完了)

更にフォルダツリーを展開し、ファイル一覧より選択した動画ファイルが再生可能であることを確認した。

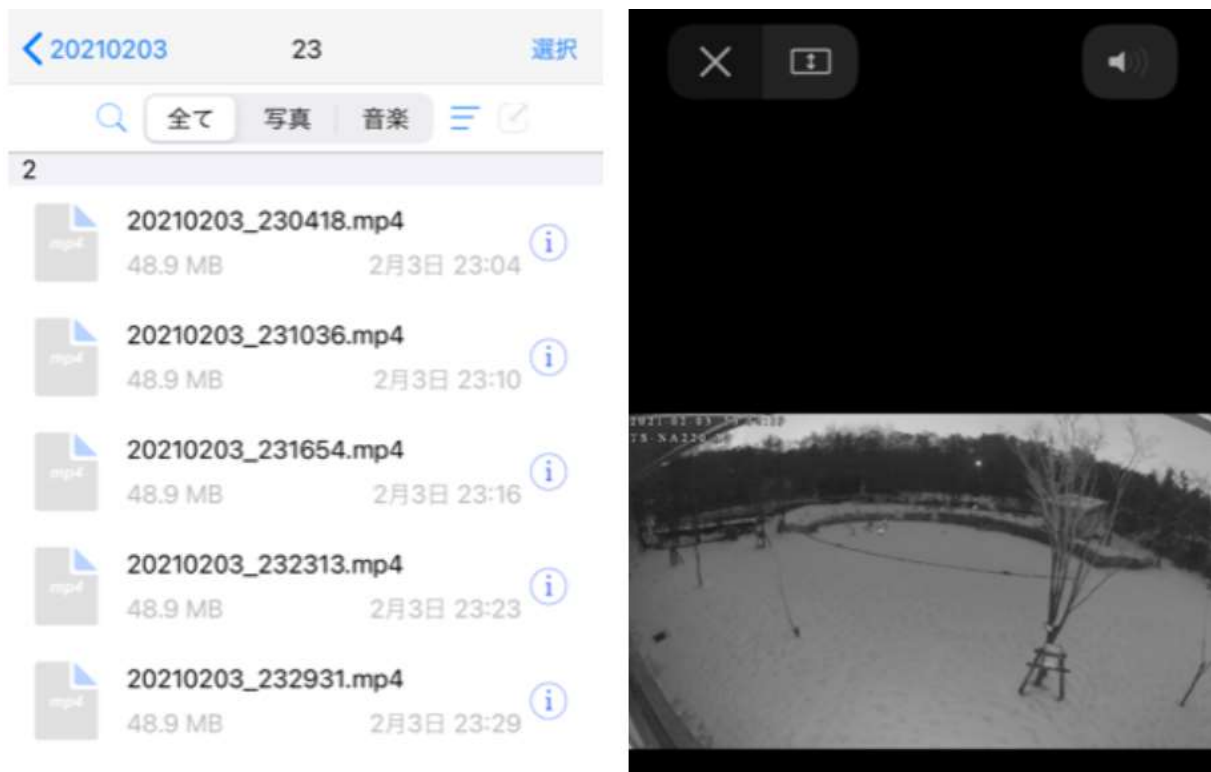


図 5.2.6-21 NAS のリモート接続結果 2(左:ファイル選択、右:動画ファイル再生)

スマートフォンからNAS へのリモート接続におけるFW 装置の通信ログを確認した結果、IPv6 想定であったが、IPv4 で通信されていることがわかった。そのため、サポートへ問い合わせを行ったところ、NAS のビューワーアプリケーションは IPv6 に対応していないことがわかった。

③センサー内蔵温度計のクラウドサービス連携の検証

#	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	センサー内蔵温度計クラウドサービス	IPv4	センサー内蔵温度計のクラウドサービス 「おんどとり WEB Storage」にアクセスする。 https://ondotori.webstorage.jp/	ログデータが正常に参照できる。	OK

【#1 の補足】

センサー内蔵温度計の計測データをクラウドより参照できることを確認した。

親機名	グループ名	機器名	測定値	更新日	詳細
	Group1		chl 27.0 C	8 分前	
	Group1		chl 14.2 C	12 分前	
	Group1		chl 26.1 C	10 分前	
	Group1		chl 20.4 C	17 分前	

図 5.2.6-22 クラウドサービスのログ参照結果

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提供されているクラウドサービス上に構築した環境において、自社サービスの IPv6 対応する際、どのような影響があるかを検証した。

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。

今回の実証実験で利用したクラウドサーバ、「ConoHa VPS」については、実証試験用に新規構築した仮想環境で、Windows Server が動作している。本環境に環境構築を行い、一般ユーザ向けの動画配信サービスの IPv6 対応を行った。①のシナリオでは、VPS の管理機能を IPv6 で利用できるか検証した。②のシナリオでは、インターネットにあるクラウドサービスを IPv6 で利用できるか検証した。③のシナリオでは、アクセス解析ツールを利用して、一般ユーザの IPv6 利用状況の分析を行った。検証範囲を図 5.2.6-23 に示す。

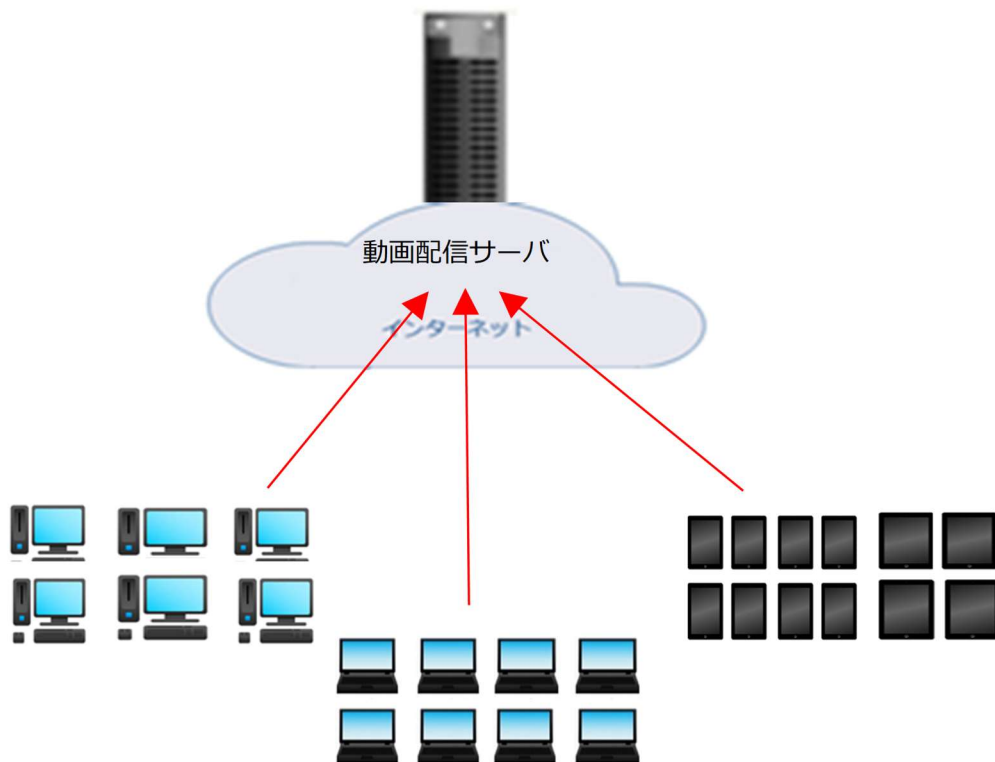


図 5.2.6-23 クラウドサービスの検証イメージ図

(2) 業務アプリケーションにおける検証(クラウド)について

① クラウドサービス管理機能の検証

クラウドサーバ上の管理機能が問題なく利用できるか検証する。実験の結果、クラウドサーバ自体はIPv6対応していたが、管理機能についてはIPv4接続のみであることが分かった。そのため、本項目の検証はIPv6環境において、IPv4接続で正常に動作するかという観点とした。

② 一般ユーザによるクラウドサービス利用の検証

一般ユーザの端末からクラウドサーバにアクセスし、クラウドサーバ上に構築した動画配信サービスが問題なく利用できるか検証する。

③ 一般ユーザの端末におけるIPv6利用状況の確認

②の検証において、一般ユーザにおけるIPv6適用状況を確認するため、アクセス解析ツールである「Google Analytics」を用いて情報を収集する。IPv4とIPv6それぞれのユーザ数、ブラウザ、OS等、プラットフォームの分布傾向や、コンテンツの取得速度による性能差など、プロトコルによる違いがどの程度あるのか、アクセスログを参照して傾向を調査する。

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 クラウドサービス管理機能の検証結果

#	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	ConoHa VPS	IPv6 想定	コマンドプロンプトで、 nslookup manage.conoha.jp を実行する	IPv6 アドレスが表示される	NG
2	ノートPC	無線	IPv6 優先	ConoHa VPS	IPv4	コントロールパネルのログイン画面を表示する	認証情報を入力後、ログインできる	OK
3	ノートPC	無線	IPv6 優先	ConoHa VPS	IPv4	IPv4 の接続可能ポートを変更する	仮想環境が IPv4 のみ接続可能になる	OK
4	ノートPC	無線	IPv6 優先	ConoHa VPS	IPv4	IPv6 の接続可能ポートを変更する	仮想環境が IPv6 のみ接続可能になる	OK
5	ノートPC	無線	IPv6 優先	ConoHa VPS	IPv4	VPS を起動する	仮想環境が起動する	OK
6	ノートPC	無線	IPv6 優先	ConoHa VPS	IPv4	コンソールを表示する	仮想環境のデスクトップがコンソール上に表示される	OK
7	ノートPC	無線	IPv6 優先	ConoHa VPS	IPv4	VPS をシャットダウンする	仮想環境がシャットダウンする	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
8	ノート PC	無線	IPv6 優先	ConoHa VPS	IPv4	バックアップを実行する	バックアップ一覧に保存イメージが表示される	OK
9	ノート PC	無線	IPv6 優先	ConoHa VPS	IPv4	イメージ(バックアップ)をリストアする	バックアップ実行時の状態に復元される	OK

【#1 の補足】

クラウドサーバ管理機能の接続先ドメインに対して nslookup を実行したが、IPv6 のアドレスは取得されなかった。つまり、クラウドサーバ自体は IPv6 に対応しているが、管理機能は IPv6 に対応していないことが考えられる。

```

C:\> 選択コマンドプロンプト
Microsoft Windows [Version 10.0.18363.1139]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ad01>nslookup manage.conoha.jp
サーバー:  one.one.one.one
Address:  1.1.1.1

権限のない回答:
名前:     manage.conoha.jp
Address:  150.95.236.31

C:\Users\ad01>

```

図 5.2.6-24 クラウドサーバ管理機能への nslookup 実行結果

また、Windows のネットワーク設定のプロパティから、IPv6 接続を有効化した状態で IPv4 接続を無効化した場合、想定通り管理機能へアクセスすることはできなかった。



図 5.2.6-25 管理機能へ IPv6 のみでアクセスした場合の実行結果

【#6 の補足】

クラウドサーバ上の VPS を起動後、仮想環境のデスクトップ画面が管理コンソール上に表示されることを確認した。



図 5.2.6-26 仮想環境のデスクトップ画面表示

② 一般ユーザによるクラウドサービス利用の検証

#	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	ConoHa VPS	IPv6	動画配信サービスに動画をアップロードする	正常にアップロードできる	OK
2	スマートフォン、タブレット	無線	IPv6 優先	ConoHa VPS	IPv4 IPv6	動画配信サービスにアクセスし、動画を再生する	実験用端末で再生できる	OK
3	ノート PC	無線	IPv6 優先	ConoHa VPS	IPv4 IPv6	Google Analytics のアクセスログを確認する	IPv4、IPv6 別にアクセス情報（アクセス数、環境、アクセス速度）が集計される	OK

【#1 の補足】

IPv6 環境においても、正常に動画をアップロードできることを確認した。



図 5.2.6-27 クラウドサービスにおける動画アップロード結果

【#2 の補足】

IPv6 環境においても、正常に動画配信サービスにアクセスし、動画が再生可能であることを確認した。

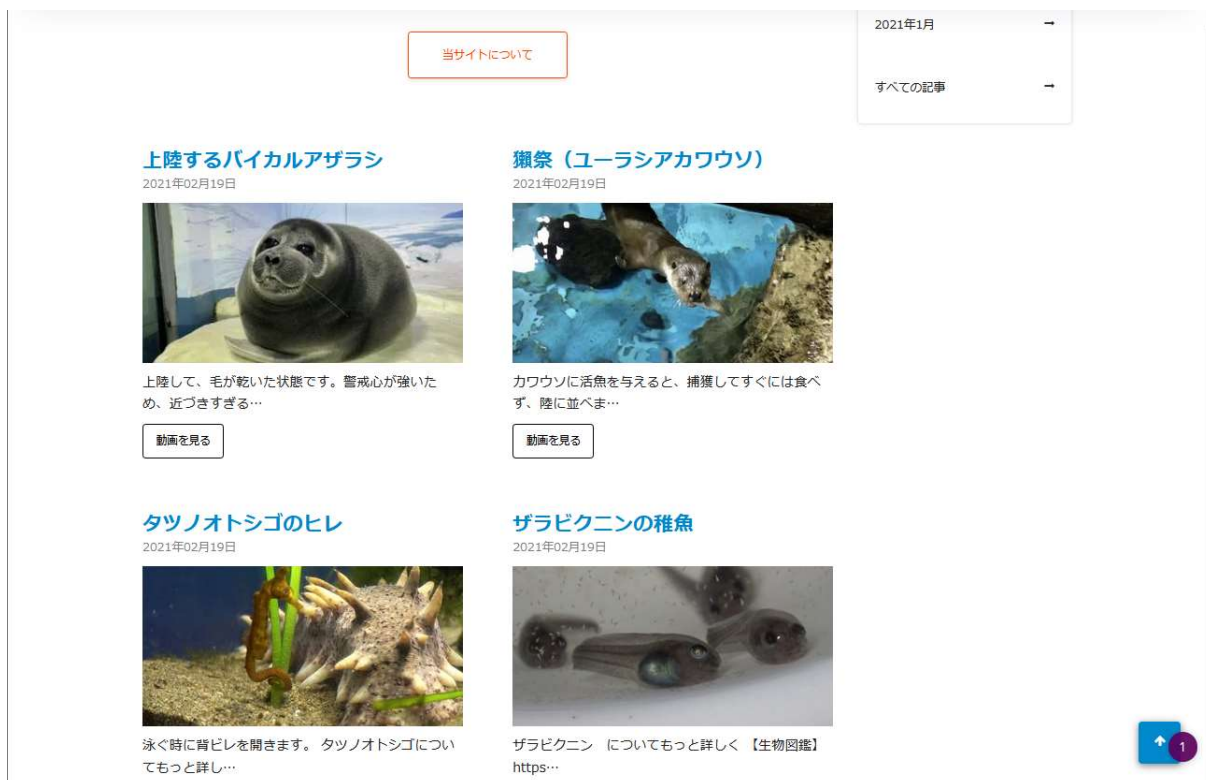


図 5.2.6-28 動画配信クラウドサービスのアクセス結果



図 5.2.6-29 動画再生画面の表示結果

【#3の補足】

IPv4とIPv6別にアクセス情報が集計されることを確認した(以下はアクセス数、アクセス速度で抽出した例)



図 5.2.6-30 Google Analytics アクセスログ確認結果

③ 一般ユーザの端末における IPv6 利用状況の確認

②の実験により収集した一般ユーザのアクセス記録から以下の観点で分析を行った。

1. ユーザ数
2. アクセス速度
3. 端末(OS)の割合

クラウドサービス上に構築した動画配信サービスでは、クラウドサービスの検証期間中に計 3 回のコンテンツ更新を実施し、一般ユーザ向けに SNS 等を通じて新着動画の公開を通知することでユーザにアクセスを促した。そして、最もアクセスが集中する更新日当日のアクセス状況を取得し、分析を実施した。

【1. ユーザ数の分析結果】

本項目においては、ユニークなユーザ数とアクセス時の IP アドレスを分析した結果、およそ 4 割前後のユーザが IPv6 を利用していることが分かった。分析の結果を表 5.2.6-1 に示す。

表 5.2.6-1 ユーザ数の分析結果

ユーザ数の分析結果		ユニークユーザー数	IPv4/IPv6 の割合
1 回目の動画公開時	IPv4	184	55.93 %
	IPv6	145	44.07 %
2 回目の動画公開時	IPv4	262	62.68 %
	IPv6	156	37.32 %
3 回目の動画公開時	IPv4	161	58.33 %
	IPv6	115	41.67 %

【2. アクセス速度の分析結果】

本項目においては、コンテンツページの「平均ダウンロード時間」を集計、分析した。Google Analytics ではアクセス速度を測る指標として、「平均読み込み時間」と「平均ダウンロード時間」が存在しているが、「平均読み込み時間」ではクライアント端末でのページをレンダリングする時間等が含まれているため、端末の性能差による影響を受け難くするため、「平均ページダウンロード速度」に着目して分析を行った。

結果として、本実験環境におけるアクセス速度については、1 回目こそ差が出ているが、2、3 回目は顕著な差は現れなかった。これは、1 回目の公開において極端にダウンロード速度の遅い端末が 1 台存在しており、全体の平均値を押し上げていた。このような極端値による集計上の影響を緩和するため、平均値の他に中央値も算出し、IPv4 と IPv6 それぞれの傾向を確認した。その詳細を表 5.2.6-2 に示す。

表 5.2.6-2 アクセス速度の分析結果

アクセス速度の分析結果		ページダウンロード 時間 (平均値)	ページダウンロード 時間 (中央値)	総ページアクセス 数
1 回目の動画公開時	IPv4	62.4 ms	16.8 ms	625
	IPv6	129.1 ms	16.5 ms	493
2 回目の動画公開時	IPv4	59.9 ms	21.1 ms	733
	IPv6	55.8 ms	24.0 ms	408
3 回目の動画公開時	IPv4	54.4 ms	18.1 ms	492
	IPv6	45.7 ms	24.6 ms	366

中央値に着目した場合、IPv4 と IPv6 の差はほぼ無いという結果となった。3 回目の計測結果では、それぞれの中央値に若干の開きが見えるものの、時間単位を考慮すると、動画コンテンツの閲覧といった一般的な利用方法において、体感上の差異は感じられないレベルだと言える。

【3. 端末(OS)の割合】

本項目においては、「1. ユーザ数の分析結果」の補足情報として、一般ユーザの端末種別に関する集計結果を表 5.2.6-3 に示す。

今回の検証の性質上、クライアント側の端末はモバイル端末である Android、iOS が中心となっている。この中でも、IPv4/IPv6 プロトコル毎でのプラットフォームの偏りは、特に認められない。

表 5.2.6-3 端末の割合の分析結果

端末の割合の分析結果		OS	ユーザ数	IPv4/IPv6 の割合
1 回目の動画公開時	IPv4	Android	84	25.53 %
		iOS	94	28.57 %
		Windows	6	1.82 %
		Mac	0	---
		Linux	0	---
	IPv6	Android	70	21.28 %
		iOS	67	20.36 %
		Windows	8	2.43 %
		Mac	0	---
		Linux	0	---
2 回目の動画公開時	IPv4	Android	101	24.16 %
		iOS	127	30.38 %
		Windows	27	6.46 %
		Mac	6	1.44 %
		Linux	1	0.24 %
	IPv6	Android	63	15.07 %
		iOS	76	18.18 %
		Windows	11	2.63 %
		Mac	6	1.44 %
		Linux	0	---
3 回目の動画公開時	IPv4	Android	64	23.19 %
		iOS	81	29.35 %
		Windows	14	5.07 %
		Mac	2	0.72 %
		Linux	0	---
	IPv6	Android	51	18.48 %
		iOS	57	20.65 %
		Windows	2	0.72 %
		Mac	2	0.72 %
		Linux	0	---

これらの分析結果より、IPv4 と IPv6 で通信されていることが記録されていることから一般ユーザーにおいて IPv6 が浸透してきていることがわかった。また、ページダウンロード時間の観点では IPv4 と IPv6 の速度差はミリ秒単位であるため、体感での違いはなかった。IPv6 はオーバーヘッドの懸念があったが、IPv4 と同等の品質で通信できることを確認した。

5.2.6.2 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:中小企業B」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、機器メーカー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ティング事例をもとに、IPv6 対応において普遍的に留意すべき点を示す。

5.3 モデル G: 中小企業 C

5.3.1 ユースケース企業の紹介

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

本実証試験は、新潟県にて廃棄物の収集・処理等の環境保全をはじめとした公共事業を展開している中小企業(以下、C 社)で行った。A 社は複数の拠点を持ち、VPN で接続されたネットワーク構成である。また、廃棄物の回収業務等において、データ連携するための収集管理システムや遠隔監視を行うための IoT システムを活用している環境である。

(2) 既存のシステム環境

本実証試験は、C 社内で利用している一般業務システムだけでなく、C 社で利用されている IoT システムや業務アプリケーション、クラウド上の動画録画サービスに対して行った。C 社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

C 社の全拠点のノード数は約 50 台、サブネット数は 4 つのネットワーク構成である。全 5 拠点中 4 拠点については回線事業者が提供している VPN サービスで拠点間の基幹ネットワークを接続している。また、VPN サービスが接続されている拠点のうちの 1 つは、ADSL 回線を利用しており、光回線と混在している状態である。プロバイダは全拠点で OCN を利用し、光回線には全て IPv6 オプションが付加されている。

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

システム環境のルータ、複合機の事務機器には静的な IPv4 アドレスを設定して運用している。PC については、拠点によりポリシーが異なり、20 台以上の PC が存在する拠点では DHCP で設定、10 台未満の拠点では静的設定としている。インターネット接続には GW ルータを設置、同ルータのファイアウォール(以降 FW)機能により、外部からのトラフィックを制御している。FW 機能の設定ポリシーは、デフォルトで適用されるセキュリティレベルであり、一般業務で利用される WEB (HTTP、HTTPS、DNS) やメール (POP3、SMTP) の利用に必要な通信を許可している。また、メールサーバは外部サービス (OCN) を利用している。

5.3.2 要件定義

C社の内部環境を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5.3.2-1に示す。

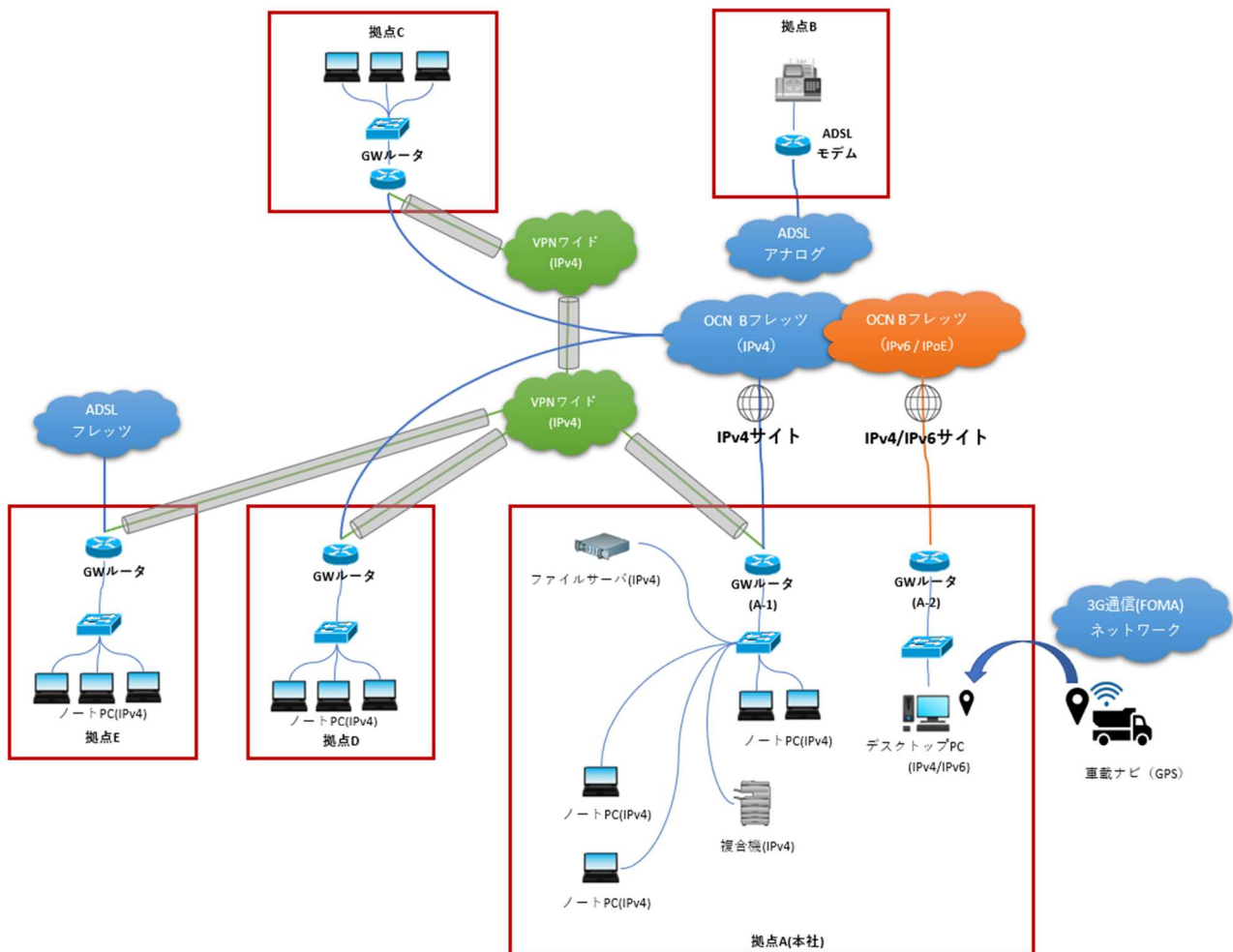


図 5.3.2-1 ネットワーク構成図イメージ

(2) 移行方式の明確化

本ユースケースにおいては基幹ネットワーク内の機器全般に IPv6 を適用するため、何らかの制約で IPv6 に移行できない機器/サービスについて、既存環境へ影響を与えない範囲で移行する方針とした。尚、既存の収集管理システムが稼働する基幹ネットワークから独立したネットワークについてはユーザの業務へ影響が大きいため、本実証試験では移行の対象外とし、実験用に IPv6 に対応した収集管理システムを拠点 A に新たに構築し、各拠点からこの収集管理システムと連携することを前提とした。

基幹ネットワークの IPv6 対応をするにあたり、IPoE 非対応であるルータ、回線事業者提供の VPN サービス、収集管理システム等、これらを IPv6 に対応している機器/サービスへ移行した上で、社内ネットワーク全体の IPv6 対応を実施することとした。

VPN サービスについては、回線事業者が提供している上位サービスで IPoE 接続に対応しているものが存在したが、拠点内では IPv6 が利用できないことを確認したため(詳細は後述の 5.3.5(2)に記載)、自営ルータの VPN 機能を利用して拠点間を接続する方針とした。

また、既存環境で利用しているメールサービスや、売上管理や電子入札といった既存の業務アプリケーションについては、事前調査の結果、IPv4 のみの対応であることを確認したため、これら既存のシステムについては現行運用を可能とする必要があるため、IPv4/IPv6 の両方が利用可能な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 5.3.2-1 に示す。

表 5.3.2-1 機器等一覧イメージ

既存/ 新規	機器等	機器 メーカー等	機器名等	移行対象	IPv6 対応 状況確認	導入方針
既存	GW ルータ	NEC	PR-300NE (拠点 A:A-2)	-	対象外	変更不要
新規	GW ルータ	BUFFALO	WSR-3200AX4S- BK (拠点 B)	○	IPv6 対応	新規
新規	VPN ルータ	YAMAHA	RTX830 (拠点 A:A-1、拠 点 C～E)	○	IPv6 対応	新規
既存	スイッチ	Cisco	SG110-16	○	対象外 (L2 機器のため)	変更要
新規	無線アクセ スポイント	Cisco	Meraki GR60	○	IPv6 未対応	新規 (L2 透過)
新規	無線アクセ スポイント	Cisco	Meraki HW30H	○	IPv6 対応	新規 (L2 透過)

既存/ 新規	機器等	機器 メーカー等	機器名等	移行対象	IPv6 対応 状況確認	導入方針
既存	複合機	Brother	HL-L2375DW	○	IPv6 対応	変更要
既存	ファイルサーバ	Fujitsu	TX1320 M4	○	IPv6 対応	変更要
新規	DB サーバ	Fujitsu	TX1310 M3	○	IPv6 対応	新規
新規	無線ネットワークカメラ	Cisco	Meraki MV12WE	○	IPv6 未対応	新規
新規	無線ネットワークカメラ	AXIS	M1045-LW	○	IPv6 対応	新規
新規	NAS	IO-DATA	HDL2-AAX2	○	IPv6 対応	新規
既存	ISP	OCN 光	フレッツ IPoE 標準プラン	○	IPv6 対応	変更要
新規	LTE 通信 SIM	NTT ドコモ	Docomo Xi ギガライトプラン	○	IPv6 対応	新規
新規	収集管理システム	JEMS	環境将軍 R	○	IPv6 対応	新規
既存	メールサービス	NTT コミュニケーションズ	Biz メール&WEB	○	IPv6 未対応	変更不要
新規	クラウドサービス	Cisco	Meraki Dashboard	○	IPv6 対応	変更不要

5.3.3 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 5.3.3-1 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 ISP の切り替えおよび拠点 VPN の構築に伴う VPN ルータの導入はネットワークの不通による現存機器への影響を調査した上で、最も影響が少ない時間帯を選択して実施した。

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」と「IoT システムにおける検証」、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
要件定義		現行整理/ 移行対象の定義												
調達			回線契約/ 機器調達											
設計				実証計画/ 設計書作成										
構築						環境構築								
試験	疎通確認							疎通確認						
	ネットワークレベル の検証							一般業務 における検証						
	LAN内アプリケー ションレベルの検証								IoTシステム における検証					
	WAN越しアプリケー ションレベルの検証									業務アプリケーション における検証				
試験結果の評価														

図 5.3.3-1 スケジュールイメージ(中小企業 C)

5.3.4 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3つ定めた。

- ① 複数拠点に対して IPv6 対応を展開すること
- ② 拠点間 VPN の IPv6 対応を行うこと
- ③ IoT システム、業務アプリケーションの IPv6 対応を行うこと

①について、各拠点の基幹ネットワークの機器全体に対して、可能な範囲で IPv6 対応を実施した。具体的には、新規に導入するルータ機器の DHCP により、基幹ネットワークに接続されている PC 端末、一般業務でファイル共有を行うための既存ファイルサーバ、複合機など一般業務で使用する機器全般に IPv6 を適用する方針とした。

但し、その中でも IPv6 に移行できない機器、外部サービス等が存在しており、移行できる部分と移行できない部分を以下の通り、整理した。

【IPv6 に移行できない部分】

- ・ 一般業務で利用する外部サービス(メールサービス等)
- ・ IPv4 のみ対応の一部機器(既存の Network Attached Storage (以下、NAS))
- ・ 拠点間を接続する既存の VPN サービス

【IPv6 に移行できる部分】

- ・ 基幹ネットワーク、ファイルサーバ、複合機等の事務機器
- ・ 新規導入する IoT システム(NAS、ネットワークカメラ)
- ・ 新規導入する業務アプリケーション(収集管理システム)
- ・ 新規構築する IoT システム向けクラウドサービス

②について、既存の VPN サービスが IPv4 のみの対応であること、また拠点間を IPoE で接続する上位のサービスに移行した場合においても、IPv6 の適用は回線事業者が提供する拠点間接続用の専用回線網内に限定され、拠点内部での通信は IPv4 のみに制限されるサービス仕様であった。このため、拠点間の VPN 接続を、回線事業者が提供する VPN サービスから、自営ルータの VPN 機能を利用したインターネット VPN を行う方式とし、既存サービスに依存しない形で VPN 接続を実現する方針とした。

インターネット VPN への移行では、拠点間を IPv6 で接続するために必要な設定を自営ルータに施す必要があった。

一例として、IPv6 のグローバルユニキャストアドレスを用いて接続する場合、プロバイダから配布されるグローバルユニキャストアドレスはプレフィックスが半固定である。そのため、IPv6 アドレスのプレフィックス変化時にも追従できるようにダイナミック DNS⁶¹を利用するための設定を行う必要があった。その他、IPv6 接続の拠点間ルーティング設定、IPv6 におけるインターネット接続においてセキュリティを維持するためのパケットフィルタ設定等が必要であったため、VPN ルータは信頼性の高い機器を選定した上で、VPN 接続による拠点間ネットワークを構築した。

③について、カタログにて IPv6 対応と明記されたネットワークカメラ等の IoT システムを新たに選定し、IoT システムの通信が IPv6 で行われる環境を構築する方針とした。

一部 IPv4 のみ対応の機器（ネットワークカメラ）もあったが、連携するクラウドサービスが IPv6 対応していたため、クラウドサービスを介すことで、IPv6 対応の範囲を拡張することが可能か検証する方針とした。

【IPv6 に移行できない仕様の機器/サービス】

業務アプリケーション（収集管理システム）についてはクラウド版とオンプレミス版の選択肢があり、導入および保守といった運用面の利便性から、当初はクラウド版を選定する方針としたが、クラウド版のクラウドサーバが IPv4 のみ対応であることが判明したため、クラウド版の導入は見送ることとした。

オンプレミス版では IPv6 環境で利用可能であったため、オンプレミス版の収集管理システムを導入する方針とした。

これらの①～③に関する機器/サービスの選定において発生した課題、検討した内容の詳細については、5.3.5 に記載する。

⁶¹ IP アドレスが頻繁に変わるホストに固定的にドメイン名を割り当て、アドレス変更在即座に追従して DNS 情報を更新するシステム。また、その仕組みを利用して提供される動的な DNS サービス。

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) 有線接続のノート PC

① 要素説明

基幹ネットワークにおいて、インターネットの利用(WEB サービス利用やメール等)、複合機での印刷等の一般業務を行うための有線接続クライアント PC (Windows) 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/デフォルトゲートウェイについて

IPv6 アドレスは DHCPv6 を採用する。ルータの仕様により、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…拠点毎に DHCP または静的アドレスによる手動設定いずれかで統一(既存踏襲)
- IPv6 アドレス…RA による自動設定

(b) DNS サーバについて

指定する IPv6 アドレスは DHCPv6 で割り当てる方式とする。

- 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…DHCPv6 による自動設定

③ 特記事項

特になし。

(2) 有線接続のデスクトップ PC

既存の収集管理システムを利用するための有線接続クライアント PC である。

別回線のネットワークに接続されており、基幹ネットワークからは切り離されているため、今回の実証実験では本デスクトップ PC は検証の対象外とする。

(3) 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

既存の設定を踏襲し、IPv4 の静的アドレスと設定する。

- IPv4 アドレス…静的アドレスによる手動設定
- IPv6 アドレス…DHCPv6 による自動設定

③ 特記事項

特になし。

(4) インターネット接続を制御する GW ルータ

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を構築するための機器である。

② 方式設計

方式設計の方針に従い、既存の GW ルータに代わり、かつルータ側でインターネット VPN を構築可能な新たな GW ルータ (VPN ルータ) を導入する。VPN ルータは IPoE 接続に対応した機器を選定し、IPv4 と IPv6 のデュアルスタックの回線を用意する。

(a) IP アドレスについて

- IPv4 アドレス…設定なし(内部管理用のアドレスは手動設定)
- IPv6 アドレス…DHCPv6 による自動設定

(b) プロバイダ認証情報について

IPoE 接続のためルータ側でのユーザ認証は不要である。但し、ルータ設定は MAP-E で接続可能な設定に変更する。

(c) ファイアウォール機能について

既存のネットワーク環境と同様に、ルータ側のファイアウォール機能を利用する方式とする。ファイアウォールのセキュリティポリシーについては、既存ルータの設定内容を踏襲する。

(d) インターネット VPN について

アグレッシブモードよりセキュアであるメインモードを設定する。トンネル設定時に固定のグローバルアドレスが必要なため、ULA (Unique Local Unicast Address)⁶²を利用する。本社である拠点 A と拠点 C～E 間の通信は、ローカルではなくオープンなため、GUA (Global Unicast Address)⁶³での通信が必要である。GUA のプレフィックスは ISP から割り当てられており、変更される可能性があるため、FQDN で指定する。また、FQDN の名前解決に DDNS (Dynamic DNS) を利用する。通信の流れを図 5.3.4-1 に示す。

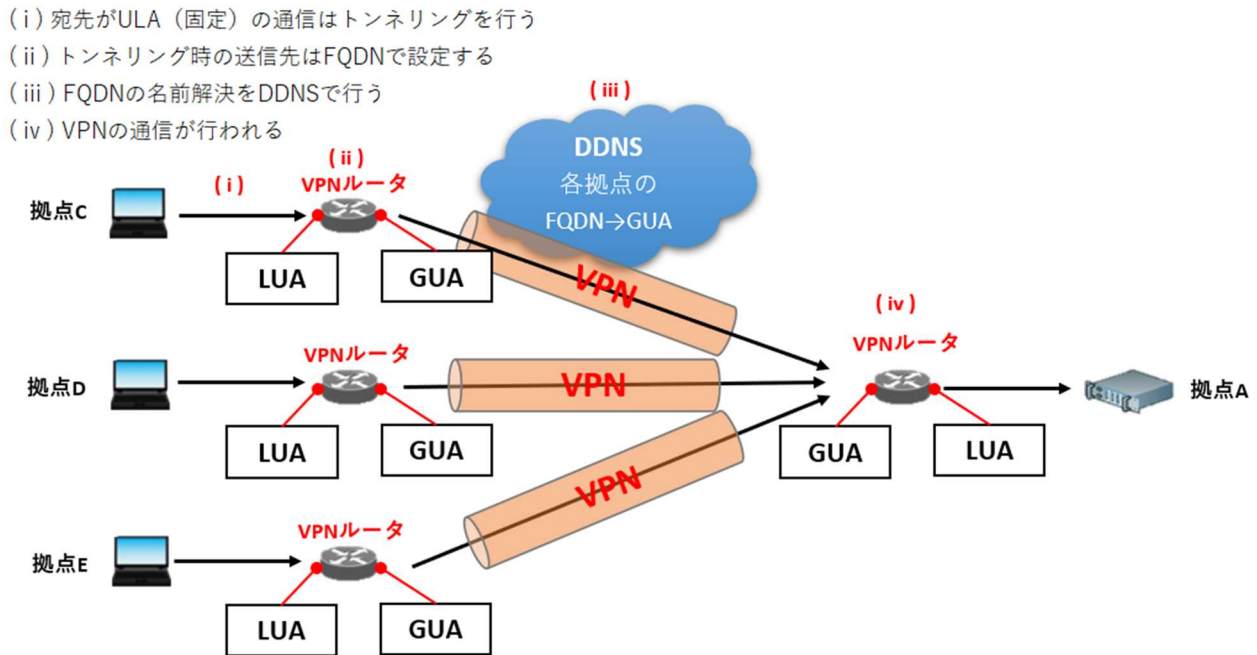


図 5.3.4-1 ULA および GUA を利用したインターネット VPN 通信の流れ

③ 特記事項

収集管理システムでは、クラウドサーバからの通信を基幹ネットワーク側に設置するデータベースサーバへの通信を許可する設定が必要となる。この設定は、ルータ側のポートフォワード機能、パケットフィルタ機能を使用して実現する。

⁶² グローバルスコープであるが、インターネットでルーティングできない。詳細は 8 章に記載する。

⁶³ グローバルスコープであり、インターネットでルーティングできる。

(5) 社内で運用しているファイルサーバ

① 要素説明

C 社では、社内の情報共有のためのファイルサーバを運用している。また、同サーバは DHCP サーバ、DNS サーバ、ActiveDirectory の認証管理サーバも兼ねている。

② 方式設計

ファイル共有を IPv6 方式で可能とするため、IPv4/IPv6 デュアルスタック方式に変更する。

③ 特記事項

現行の運用への影響を限定するため、本サーバにおける DHCP サーバ機能は IPv4 に限定し、IPv6 についてはルータ側の DHCP 機能を利用する。

また、ActiveDirectory 管理機能については、クライアント PC が管理ドメインに参加する際に、クライアント PC からドメインコントローラとなる ActiveDirectory の認証管理サーバのドメイン名を名前解決するため、パブリック DNS で名前解決できない場合は DNS サーバとして本サーバを参照できるよう、ルータ側での設定も必要となる。

(6) 収集管理システム用のデータベースサーバ(DB サーバ)

① 要素説明

C 社が利用する収集管理システム用のデータベースとして、新規に構築するサーバである。

② 方式設計

収集管理システムのアプリケーションとの通信を IPv4/IPv6 の両方で可能とするため、IPv4/IPv6 デュアルスタック方式で設定する。

③ 特記事項

収集管理システムは、オンプレミス環境で利用する PC 版、クラウドサービスを介したモバイル版、どちらにおいても、システムの利用時はこの DB サーバを参照する必要がある。このため、他拠点から収集管理システムを利用するケースでは、VPN を経由して DB サーバへアクセス可能とするルーティング設定が必要となる。また、モバイル版の利用にあたっては、クラウドサービスと DB サーバ間の通信を通過させるためのファイアウォール設定が必要となる。

(7) 収集管理システム用のタブレット端末

① 要素説明

収集管理システムのモバイル版を利用するための Android OS を搭載したタブレット機器である。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

③ 特記事項

インターネットとの接続は、SIM カードによる LTE 通信環境下で利用する。キャリア側で IPv6 の利用が可能な場合、自動的に IPv4/IPv6 デュアルスタック構成で設定される。

(8) ネットワークカメラの映像を保存する NAS 機器

① 要素説明

ネットワークカメラの録画データを、ファイル共有を通じて保存するためのネットワーク接続可能なストレージ機器である。

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

③ 特記事項

特になし。

(9) クラウド管理機能を持つ無線アクセスポイント

① 要素説明

IoT 機器を無線接続するための、クラウド管理機能が可能なアクセスポイント機器である。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

③ 特記事項

Cisco 社が提供するクラウドサービス(Meraki DashBoard)と連携し、WEB ブラウザで機器の稼働状態の確認、および設定変更が可能な機器である。

(10) 上記以外の IoT システム

① 要素説明

社内の各所に設置するネットワークカメラ等の IoT システムである。

② 方式設計

ネットワークカメラは AXIS 製と Cisco 製の 2 種類を組み合わせで構築する。

AXIS 製のネットワークカメラは IPv6 方式に対応しているため、IPv4/IPv6 デュアルスタック方式とする。Cisco 製のネットワークカメラは IPv6 方式に対応していないため、IPv4 シング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…DHCP による自動設定 (AXIS、Cisco 製ネットワークカメラ)
- IPv6 アドレス…DHCPv6 による自動設定 (AXIS 製ネットワークカメラのみ)

③ 特記事項

Cisco 製ネットワークカメラは初期状態では静的アドレスの設定が出来ない仕様であり、DHCP を前提とした機器設計になっていることから、ネットワークカメラ全般は DHCP による自動設定に統一した。

(11) 社外のメールサービス

① 要素説明

クライアント PC からメールの送受信 (SMTP、POP) を行う外部メールサービス (MTA) である。

② 方式設計

既存メールサービスが IPv4 のみ対応のため、IPv4 シングルスタック方式のままとする。

(a) MUA(Mail User Agent)側の設定について

MTA(Mail Transfer Agent)の指定は FQDN で行っている。メールサービスが IPv4 のみ対応のため、社外の DNS では A レコードのみ応答され、IPv4 通信のみ可能となる。

③ 特記事項

(a)MUA 側の設定について、IPv6 優先 PC の場合、DNS で名前解決した後、IPv4 通信に自動で切り替わるため、正常に利用可能であると想定し、試験を行うこととした。

(12) 映像録画サービス

① 要素説明

C 社が利用している、ネットワークカメラの映像を録画するクラウドサービスである。

② 方式設計

利用するクラウドサービスは、IPv6 をサポートしている通信機器の管理ポータル(Meraki DashBoard)である。IPv6 対応のため、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
(サービス提供者が払い出しているグローバルユニキャストアドレス)
- IPv6 アドレス…同上

(13) 収集管理システム用のクラウドサービス

① 要素説明

C 社が利用している、収集管理システムをタブレット端末等のモバイル端末から利用するためのクラウドサービスである。

② 方式設計

タブレット端末から WEB ブラウザ経由で利用する。IPv6 対応のため、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
(サービス提供者から払い出されたグローバルユニキャストアドレス)
- IPv6 アドレス…同上

③ 特記事項

特になし。

以上を踏まえて構築した、IPv6 対応後のシステム構成図を図 5.3.4-2 に示す。

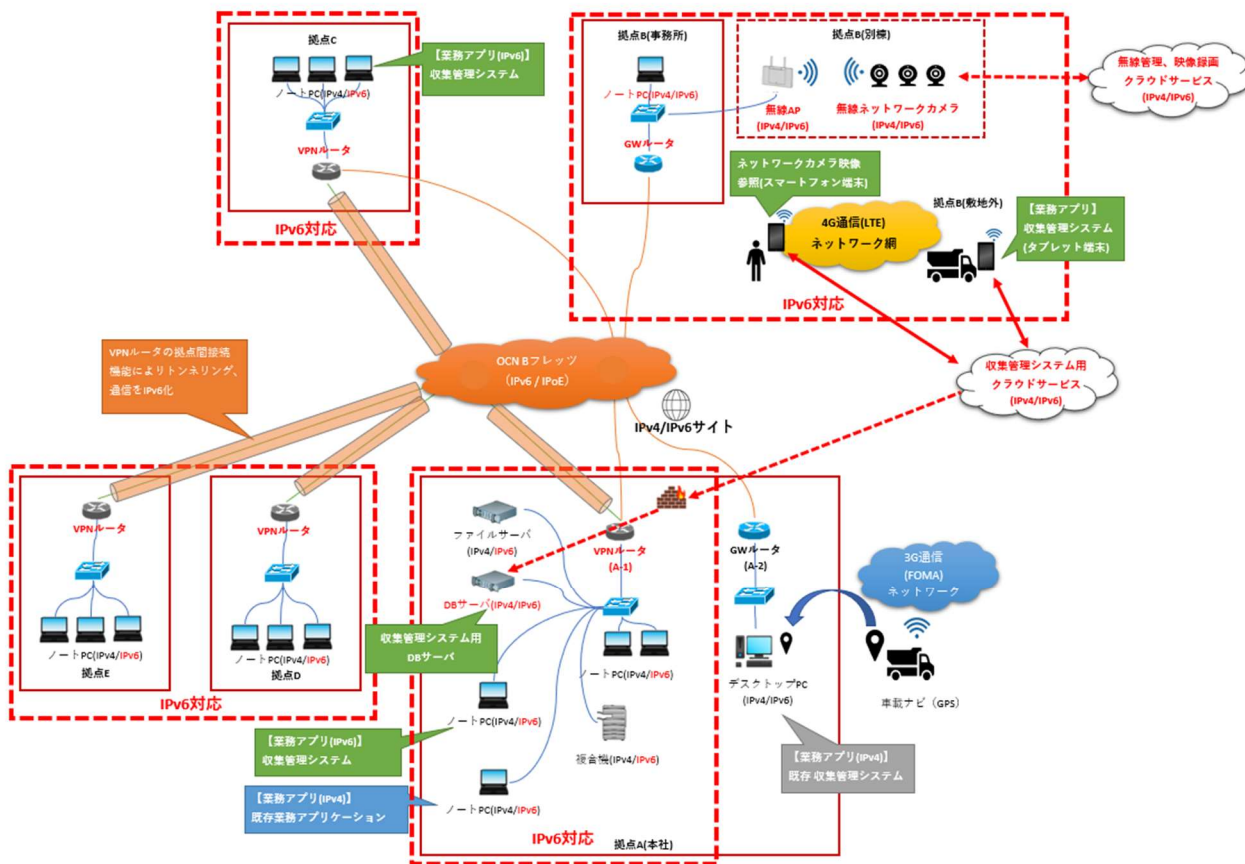


図 5.3.4-2 IPv6 対応後の C 社のシステム構成図

5.3.5 構築

本ユースケースでは検証環境構築において、以下の流れで機器や環境の検討を行った。(1)～(5)において各検討過程における課題を記載し、(6)にその解決策・対応方針を記載する。

(1) プロバイダの選定

プロバイダ選定においては、PPPoE 接続より通信速度、輻輳といった面で性能の優位性がある、IPoE 接続に対応しているプロバイダを前提に検討した。

【プロバイダ選定における課題点】

プロバイダ選定においては、IPv6 に対応しているかどうかに加え、利用する業務システムの仕様により固定 IP 契約が必要になった場合においても、プロバイダを移行せずに対応できることを見据えて選定を行うことが望ましい。

但し、プロバイダによっては固定 IP 契約をする際に現在利用中のプランを継続できず、新たなプランに切り替えるといった移行作業が必要となるケースもあるため、契約の移行可否はプロバイダ選定時に確認すべきポイントである。

(2) ネットワーク設計の検討

プロバイダを選定した後は、IPoE 接続を前提としたネットワーク構成を検討した。

今回の実証実験環境に IPv6 を導入するためには、既存環境への影響を最小限とするため、以下の 2 つの課題を解決する必要があった。

【ネットワーク設計における課題点】

① VPN 接続の IPv6 適用に関する課題

回線事業者側が提供している既存 VPN サービスが IPv4 のみの対応であったため、拠点間の VPN 接続を IPv6 対応するために VPN サービスの切り替えを検討した。

同 VPN サービスには上位版が存在しており、拠点間を IPoE で結ぶ IPv6 対応のサービスであったが、事前調査の結果、IPv6 対応は専用ルータ (CPE) と拠点間の専用回線網内に限定されており、ユーザが利用するイントラネット側の通信、およびインターネット接続は IPv4 対応のみとなる制約があったため、VPN サービスの移行だけでは解決できない課題が生じた。

② 本社拠点内の ActiveDirectory 運用に関する課題

既存ファイルサーバは ActiveDirectory のドメインコントローラ機能を持ち、既存 DNS サーバ機能も兼ねている。

PC からドメインコントローラに接続する際、ドメインコントローラの名前解決を行う必要があるが、インターネット上のパブリックな DNS サーバには、社内で運用されている ActiveDirectory のドメイン名を名前解決する能力がない。

このため、本社拠点内で ActiveDirectory を正常に運用するためには、IPv4/IPv6 のいずれにお

いても、名前解決時に既存 DNS サーバを参照可能とする必要がある。

また、既存 DNS サーバは名前解決を GW ルータ側にフォワードしている設計であった。IPv4/IPv6 の名前解決において、DNS のリクエストがループしてしまわないよう、新規ルータ側においても DNS 参照順序を考慮する必要がある。

(3) 実験機器の選定

既存機器を含めた、今回の実証試験シナリオに利用する選定機器の一覧を以下に示す。

表 5.3.5-1 選定機器の一覧

区分	概要	機器ベンダ	型番	機器本体の IPv6 対応	クラウドサービスの IPv6 対応
新規	VPN ルータ	YAMAHA	RTX830	○	—
新規	GW ルータ	Buffalo	WSR-3200AX4S	○	—
既存	ファイルサーバ	Fujitsu	TX1320 M4	○	—
新規	DB サーバ	Fujitsu	TX1310 M3	○	—
既存	NAS	Buffalo	LS220D0202G	×	—
既存	複合機	Fujitsu	XL-9321	○	—
既存	複合機	Brother	HL-L2375DW	○	—
新規	無線アクセスポイント	Cisco	Meraki HW30H	○	○
新規	ネットワークカメラ	Cisco	Meraki MV12	×	○
新規	無線アクセスポイント	Cisco	Meraki Go GR60	×	×
新規	ネットワークカメラ	AXIS	M1045-LW	○	×
新規	NAS	I/O Data	HDL2-AAX2	○	×
新規	タブレット	Lenovo	M10 FHD Plus	○	—

○: サポート、×: 非サポート

IPv6 通信による VPN の拠点間接続を構築するため、VPN ルータは IPoE に対応し、VPN 構築において実績がある機器を選定した。

一般業務で使用している既存のファイルサーバ、複合機においては、設定変更により IPv6 対応を実施した。

その他、IoT デバイスのネットワーク構築のため新規に導入する無線アクセスポイント、ネットワークカメラ、NAS は可能な限り IPv6 対応機器を導入した。

IPv4 のみ対応の機器に関しても、連携するクラウドサービス側が IPv6 対応している場合は、機器の選定対象に含めた。

その他、IPv4 のみの対応であるが、IPv6 の通信が行える可能性がある機器についても選定対象に含める方針とした。例えば、IPv4 のみ対応の無線アクセスポイントについては、メーカ側のスペックとしては IPv6 対応を謳っていないが、IPv4/IPv6 のトラフィック透過に問題がないことを検証するため選定した。

【機器選定における課題点】

IoT システムに関しては、メーカが IPv6 対応を公表している機器、例えば「IPv6 Ready Logo」認証を取得している機器、カタログ等で IPv6 対応を明記している機器を中心に選定を行うことが確実な方法であるが、その場合はハイエンドモデルが中心となり、選択肢が少ない状況である。

(4) 業務アプリケーションの選定

C 社の環境で検証に使用した収集管理システムは、クラウド版とオンプレミス版の選択肢があり、導入および保守といった運用面の利便性から、クラウド版を選定する方針で進めた。

【業務アプリケーションの選定における課題点】

業務アプリケーションの選定当初、事前にユーザサポートに問い合わせを行った結果、クラウド版が IPv6 対応しているとの回答を得ていたため、クラウド版の導入を前提として導入を進めていた。しかし、契約に際して直接開発元に調査を依頼した結果、クラウドサービスのデータセンタ側が IPv4 のみ対応であることが判明した。

また、オンプレミス版で環境構築する場合において、タブレット端末からモバイル版の収集管理システムを利用するにあたり、サービスの仕様上、メーカ提供のクラウドサービスを經由して拠点内の DB サーバへ接続する通信経路となるため、クラウドサービスから DB サーバへ通信を許可する設定を FW へ適用する必要があることも確認した。

(5) クラウドサービスの選定

ネットワークカメラと連携し、クラウドにて録画可能なサービスを中心に選定を行った。

IPv6 に対応するネットワークカメラとそのカメラと連携できるクラウドサービスを多くの機器/サービスから見つけ出すことは大変困難である。そこで、クラウドにて録画映像の参照を行う利用形態を想定し、ネットワークカメラは IPv4 のみの対応であるが、録画を行うためのクラウドサービスが IPv6 対応している Cisco 社のクラウドサービス(Meraki DashBoard)を選定した。

【クラウドサービスの選定における課題点】

ネットワークカメラの録画サービスという観点において、データ連携の仕様面からネットワークカメラと同一のメーカーより提供されているクラウドサービスを前提としたが、メーカーによってクラウドサービスが付属サービスとして、提供されていないケースがある。他メーカーのクラウドサービスと連携する方法があるが、選定範囲が多岐にわたる中で、対象とするネットワークカメラと連携可能、かつ IPv6 対応という条件に充足するクラウドサービスを選定することは困難であった。

今回、他メーカー提供のクラウドサービスのうち、対象とするネットワークカメラでサポートされているサービスが複数あることを確認したが、全て IPv4 のみの対応であった。

- アロバビュークラウド (iDATEN)
- Safe (セーフイー株式会社)
- VisualStage Type-S (キヤノンマーケティングジャパン)

(6) (1)～(5)における課題解決

【(1)の課題解決の方針、実施内容】

実証実験の検証環境下において、IPv6 の環境適用のための必須条件を以下に示す。

- IPoE が利用できること
- 固定 IPv4 アドレスが取得できること

上記の前提において、C 社で利用している収集管理システムの運用を考慮した選定を行った。具体的には、収集管理システムにはオンプレミス版とクラウド版の 2 種類が存在し、当初は導入の容易さ、保守性の高さからクラウド版を導入する計画であったが、クラウド版は IPv4 のみ対応している状況であったため、IPv6 対応のオンプレミス版を選択した。

オンプレミス版では、タブレット等のモバイル端末から収集管理システムを利用するためのクラウドサービスが存在し、そのクラウドサービスが C 社の拠点 A 内で稼働する DB サーバと連携するため、クラウドサービスから拠点内のネットワークに対する外部接続が必要になる。

システム仕様として、この外部接続を行うためには、拠点 A において固定 IP の利用が必要となるため、IPoE 対応かつ、固定 IP アドレスの利用が可能であることを前提としたプロバイダ選定を行った。現行環境で利用している OCN が上記の条件を満たしていたため、OCN が提供する「フレッツ IPoE 標準プラン 固定 IP」を選定した。

【(2)の課題解決の方針、実施内容】

① VPN 接続の IPv6 適用に関する課題について

回線事業者が提供する VPN サービスでは課題が解決できないため、自営ルータを利用したインターネット VPN を構築することで、IPv6 に対応する方針とした。しかしその際、以下の点に留意しながらネットワーク設計を進める必要があった。

(ア) IPv6 での拠点間通信を行うためには、固定のプレフィクスが必要となるため、拠点間の接続とインターネット接続において、ネットワークアドレスの設定方式を検討する必要がある。

(イ) 既存環境において、拠点間のファイル共有を NAT で実現している。各拠点から拠点 A の既存ファイルサーバを参照する際の IPv4 アドレスは変更せず、現行の運用を変更せずに、ファイルサーバに接続可能な方式を検討する必要がある。

(ア)を解決するための方針として、インターネット側は GUA で通信し、VPN による拠点間通信は ULA で通信する設計とすることとした。これにより、VPN ルータ間の認証方式を「アグレッシブモード」よりもセキュアである「メインモード」が採用できるようになり、更に DDNS で FQDN の名前解決を行う設計とすることで、VPN ルータ同士を IPv6 アドレスで接続し、プロバイダより VPN ルータに割り振られる GUA が変更された場合においても、ルータの設定変更なく運用が継続できるようになる。

- (i) 宛先が ULA (固定) の通信はトンネリングを行う
- (ii) トンネリング時の送信先は FQDN で設定する
- (iii) FQDN の名前解決を DDNS で行う
- (iv) VPN の通信が行われる

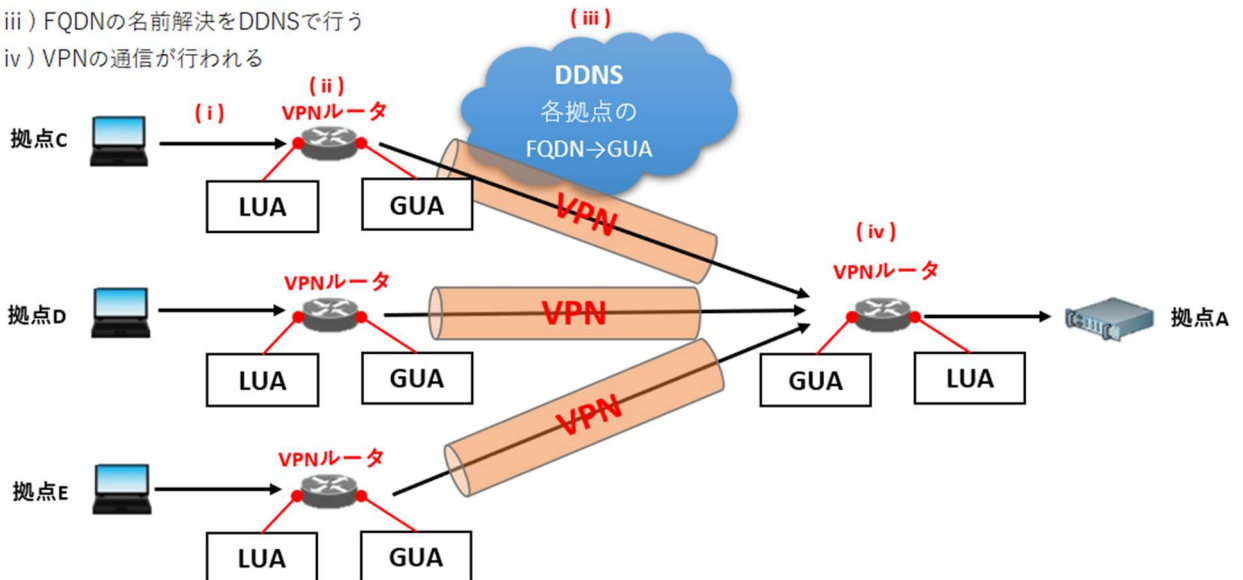


図 5.3.5-1 ULA および GUA を利用したインターネット VPN 通信の流れ(再掲)

尚、固定プレフィックスの算出方法には、無償公開されているツール (IPv6GlobalIdGenerator) を利用し、RFC 4193 (一意なローカル IPv6 アドレス) の算出アルゴリズムに基づいた ULA を算出した。次に、(イ)を解決するための方針として、拠点 A の既存ファイルサーバに他拠点から現行の運用を変更せずに、ファイル共有を可能とするため、NAT 機能を利用して現行通りの運用方法でファイルサーバへ接続できるよう、FW 機能の NAT 設定により、ファイル共有が可能となる設計とした。

※実際の設定内容は、5.3.5 (1) 【NAT 設定】に記載する。

② 拠点 A 内の ActiveDirectory 運用に関する課題

既存 DNS サーバは、IPv4 の名前解決は GW ルータ側にフォワードするが、IPv6 の名前解決はフォワードしない挙動であった。GW ルータ側で挙動の違いを吸収するため、新規 VPN ルータに DNS の参照設定を追加し、一般業務で利用することが多いインターネット側の通信を最優先に設定し、ドメインコントローラの名前解決が必要な場合に既存 DNS サーバを IPv4 が第 2 優先、IPv6 が第 3 優先の順で参照できるよう、問い合わせの優先順位を以下の通りに設定した。

1. インターネット DNS (IPv4/IPv6 の名前解決)
2. 既存 DNS サーバ (IPv4 でのドメインコントローラの名前解決)
3. 既存 DNS サーバ (IPv6 でのドメインコントローラの名前解決)

※実際の設定内容は、5.3.5(1) 【DNS 設定】に記載する。

【(3)の課題解決の方針、実施内容】

VPN ルータにおいては、過去に VPN 構築の実績がある機器を選定したため、ネットワークの構築自体に課題は発生しなかった。過去に導入実績がない VPN ルータ機器を選定する場合は、機器のリファレンスといった一般公開されている情報を元に、IPv6 設定に関する知見を入手しやすいメジャーな機器を選定することが機器選定において意識すべきポイントである。

IoT デバイスに関しては、課題で述べた通り IPv6 対応のネットワークカメラの選択肢が少ない状況であったが、その中で今回選定した AXIS 社のネットワークカメラはグローバルな機器であると共に、中小企業で導入しやすい価格帯であり、日本語対応、ユーザサポートも十分に展開されている。海外メーカーの機器を選定する方法も、1つの手段である。

しかし、本機器と連携可能なクラウドサービスが IPv4 のみの対応であったため、代替として、NAS との連携を証する方針とした。録画した動画データを NAS 上に保存し、イントラネット経由で NAS に接続し、動画データを参照する方針とした。

また、その他の機器については、機器自体が IPv6 対応していない場合においても、クラウドサービス側が IPv6 対応しているサービスを選定することや、無線アクセスポイントにおいて IPv6 通信を透過する設定に変更することで、IPv6 環境において利用可能となることを想定し、構築した。

【(4)の課題解決の方針、実施内容】

収集管理システムについて、クラウド版の導入は見送り、IPv6 対応が行われているオンプレミス版の収集管理システムを導入する方針とした。

事前調査として、IPv6 の対応状況をユーザサポートに問い合わせる際に、サポート担当者と開発担当者によって、IPv6 対応とする基準が異なる場合があるため、注意が必要である。

次に、タブレットで利用するモバイル版の収集管理システムについては、拠点内の DB サーバをインターネット経由で外部参照を可能とするため、拠点 A の VPN ルータにて、FW 機能を設定し、クラウドサービス側からの IPv4/IPv6 における外部参照を、オンプレミス環境内の DB サーバへ許可する設定を実施した。

※実際の設定内容は 5.3.5 (1) **【ファイアウォール設定】**に記載する。

【(5)の課題解決の方針、実施内容】

(3)の課題解決と同様に、機器側が IPv6 対応していない場合においても、クラウドサービス側が IPv6 対応しているサービスを選定することで、クラウドサービス側とクライアント端末側がインターネットを介して IPv6 によるサービス利用が可能な環境を構築した。

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 5.3.5-1 に示す。

表 5.3.5-2 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/ IPv6	デスクトップ PC	[Windows] Fujitsu ESPRIMO B532/G OS Windows10 Pro CPU Core™ i5-3470T プロセッサー (2.90GHz) メモリ 4GB HDD 500GB	・事務用
IPv4/ IPv6	ノート PC	[Windows] Fujitsu LIFEBOOK A5510/DOS OS Windows10 Pro CPU Core™ i5-10210U プロセッサー (1.60GHz) メモリ 4GB HDD 500GB	・事務用
IPv4/ IPv6	複合機	FUJITSU XL-9321 Brother HL-L2375DW	・印刷
IPv4/ IPv6	ファイルサーバ	[Windows] FUJITSU Server PRIMERGY TX1320 M4 OS Windows Server 2019 CPU Xeon E-2124 プロセッサー (3.3GHz) メモリ 8GB HDD 300GB	・ファイル共有
IPv4/ IPv6	DB サーバ	[Windows] FUJITSU Server PRIMERGY TX1310 M3 OS Windows Server 2016 CPU Pentium プロセッサー G4400 (3.3GHz) メモリ 16GB HDD 500GB	・収集管理システムのデータ管理

設定	機器等	仕様例	備考
IPv4	NAS(既設)	Buffalo LS220D0202G	・データバックアップ
IPv4/ IPv6	タブレット	Android:Lenovo Tab	・収集管理システム用の端末 ・ネットワークカメラの映像参照
IPv4/ IPv6	GW ルータ(既設)	拠点 A(A-2):NEC PR-300NE	・ルーティング ・FW
IPv4/ IPv6	GW ルータ(新規)	拠点 B:Buffalo WSR-3200AX4S-BK ※拠点 A(A-1)、および拠点 C～E は 下記 VPN ルータに置き換え。	・ルーティング ・FW
IPv4/ IPv6	VPN ルータ (新規)	YAMAHA RTX830	・ルーティング ・FW ・拠点間の VPN 通信
IPv4 /IPv6	スイッチ	Cisco SG110-16	・スイッチング
IPv4 /IPv6	NAS(新規)	IO-DATA HDL2-AAX2	・ネットワークカメラの映像録画
IPv4 /IPv6	無線アクセスポイント	Cisco Meraki GR60 Cisco Meraki HW30H	・ネットワークカメラの無線接続
IPv4 /IPv6	無線ネットワークカメラ	Cisco Meraki MV12WE AXIS M1045-LW	・構内監視
IPv4/ IPv6	ISP	フレッツ光ネクストファミリーハイスピード (IPv6 オプションあり) OCN 光 フレッツ マルチホームなし	・インターネット接続、拠点間 VPN 接続 ※拠点 A のみ 1 固定 IP を付 加。
IPv4/ IPv6	LTE 通信 SIM	Docomo Xi ギガライトプラン	・インターネット接続
IPv4/ IPv6	アプリケーションパッケージ	JEMS 環境将軍 R	・収集管理システムのアプリケーション
IPv4	メールサービス	NTT コミュニケーションズ Active! Mail(Biz メール&WEB)	・メール
IPv4/ IPv6	クラウドサービス	Cisco Meraki Dashboard	・無線管理機能 ・監視映像録画

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) VPN ルータの設定 (本社拠点である拠点 A を例として挙げる)

項番	設定内容の詳細
1	<p>【基本ルーティング設定】</p> <pre> ip route default gateway tunnel 1 ip route <拠点 C の IPv4 アドレス> gateway tunnel 2 ip route <拠点 D の IPv4 アドレス> gateway tunnel 3 ip route <拠点 E の IPv4 アドレス> gateway tunnel 4 ipv6 route <拠点 C の ULA>::/64 gateway tunnel 2 ipv6 route <拠点 D の ULA>:/64 gateway tunnel 3 ipv6 route <拠点 E の ULA>:/64 gateway tunnel 4 ip lan1 address <拠点 A の IPv4 アドレス(内向け)>/24 ip lan1 secondary address <拠点 A の IPv4 アドレス(外向け)>/24 ipv6 prefix 1 ra-prefix@lan2::/64 ipv6 prefix 2 <拠点 A の ULA>::/64 ipv6 lan1 address <拠点 A の ULA>::1/64 ipv6 lan1 address ra-prefix@lan2::1/64 ipv6 lan1 rtadv send 1 2 o_flag=on ipv6 lan1 dhcp service server ipv6 lan2 dhcp service client ir=on ngn type lan2 ntt description lan2 "OCN IPoE" </pre> <p>【VPN 設定】</p> <pre> tunnel select 2 tunnel name <拠点 C の FQDN> ip tunnel nat descriptor 2 ipsec tunnel 3 : (IKE のデフォルトパラメータのため省略) ipsec ike local name 2 【拠点 A の FQDN(i.open.ad.jp)】 fqdn ipsec ike pre-shared-key 2 text 【認証キー】 ipsec ike remote name 2 【拠点 C の FQDN(i.open.ad.jp)】 fqdn : (IKE のデフォルトパラメータのため省略) tunnel enable 2 </pre> <p>※上記を拠点 D、E も同様に設定</p>

【BRに対する IPIP の設定】

```
tunnel select 1
description tunnel "OCN IPoE Static IPv4"
tunnel encapsulation map-e
tunnel map-e type ocn
ip tunnel mtu 1460
ip tunnel nat descriptor 1
ip tunnel intrusion detection in on
ip tunnel tcp mss limit auto
tunnel enable 1
```

【NAT 設定】

```
nat descriptor type 1 masquerade
nat descriptor address outer 1 map-e
nat descriptor type 2 nat
nat descriptor address outer 2 <ファイルサーバの外向け IPv4 アドレス> <DB サーバの外向け IPv4 アドレス>
nat descriptor address inner 2 <ファイルサーバの内向け IPv4 アドレス> <DB サーバの内向け IPv4 アドレス>
nat descriptor static 2 1 <ファイルサーバの外向け IPv4 アドレス>=<ファイルサーバの内向け IPv4 アドレス> 1
nat descriptor static 2 2 <DB の外向け IPv4 アドレス>=<DB の内向け IPv4 アドレス> 1
nat descriptor masquerade static 1 1 10.0.0.220 tcp 1433
```

【DNS 設定】

```
dns host lan1
dns service recursive
dns service fallback on
dns server <既存 DNS サーバ IPv4 アドレス> <既存 DNS サーバ IPv6 アドレス>
dns server select 50000 dhcp lan2 any .
dns server select 100000 <既存 DNS サーバ IPv4 アドレス> a .
dns server select 500000 <既存 DNS サーバ IPv6 アドレス> aaaa .
dns private address spoof on
```

【ファイアウォール設定】

※DB サーバの外部参照用フィルタ設定は赤字部分を参照

nat descriptor masquerade static 1 1 <DB サーバの IPv4 アドレス> tcp <ポート番号>

:(中略)

ip filter dynamic 201101 * <DB サーバの IPv4 アドレス> <ポート番号>

:(中略)

ip filter 201030 pass * 10.0.0.0/24 icmp **

ip filter 201031 pass * 10.0.0.0/24 established **

ip filter 201032 pass * 10.0.0.0/24 tcp * ident

ip filter 201033 pass * 10.0.0.0/24 tcp ftpdata *

ip filter 201034 pass * 10.0.0.0/24 tcp,udp * domain

ip filter 201035 pass * 10.0.0.0/24 udp domain *

ip filter 201036 pass * 10.0.0.0/24 udp * ntp

ip filter 201037 pass * 10.0.0.0/24 udp ntp *

ip filter 201050 pass-log * <DB サーバの IPv4 アドレス> tcp * <ポート番号>

:(中略)

ipv6 filter 101000 pass ** icmp6 **

ipv6 filter 101001 pass ** tcp * ident

ipv6 filter 101002 pass ** udp * 546

ipv6 filter 101010 pass-log * <DB サーバの IPv6 アドレス> tcp * <ポート番号>

ipv6 filter 101099 pass * * * * *

ipv6 filter 200199 pass-log * * * * *

ipv6 filter dynamic 101080 ** ftp

ipv6 filter dynamic 101081 ** domain

ipv6 filter dynamic 101082 ** www

ipv6 filter dynamic 101083 ** smtp

ipv6 filter dynamic 101084 ** pop3

ipv6 filter dynamic 101085 ** submission

ipv6 filter dynamic 101098 ** tcp

ipv6 filter dynamic 101099 ** udp

(2) IoT システムの設定

項番	設定内容の詳細																
1	<p>【ネットワークカメラの設定 (AXIS)】</p> <p>TCP/IP</p> <div style="display: flex; justify-content: space-between;"><div style="width: 48%;"><p>IPv4</p><p>自動IP (DHCP) および DNS (DHCP) ▼</p><p style="text-align: right;">保存</p></div><div style="width: 48%;"><p>IPv4 - 無線</p><p>自動IP (DHCP) ▼</p><p style="text-align: right;">保存</p></div></div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"><div style="width: 48%;"><p>IPv6</p><p>自動割り当て (DHCP) <input checked="" type="checkbox"/></p></div><div style="width: 48%;"><p>フレンドリ名</p><p>Bonjour™を使用 <input checked="" type="checkbox"/></p><p>Bonjour名</p><p>UPnP®を使用 <input type="checkbox"/></p><p>UPnP名</p></div></div> <p>【NAS 設定 (IPv6)】</p> <p>※自動、または手動で設定する</p> <div style="border: 1px solid #ccc; padding: 10px;"><p>ホーム ネットワ… LAN1 IPv6 戻る 全ヘルプ ヘルプ有</p><p style="text-align: center;">IPv6</p><table border="1" style="width: 100%;"><tr><td>IPアドレス設定方式</td><td><input type="radio"/> 無効 <input checked="" type="radio"/> 自動で取得する(DHCP) <input type="radio"/> 手動で設定する</td></tr><tr><td>IPアドレス</td><td></td></tr><tr><td>プレフィックス長</td><td>64</td></tr><tr><td>フレームサイズ</td><td>1500 リストから選択 ▼</td></tr><tr><td colspan="2" style="text-align: center;">追加設定</td></tr><tr><td>設定方法</td><td><input checked="" type="radio"/> 自動で取得する <input type="radio"/> 手動で設定する</td></tr><tr><td>デフォルトゲートウェイ</td><td></td></tr><tr><td>DNSサーバー</td><td></td></tr></table><p style="text-align: right;">適用</p></div>	IPアドレス設定方式	<input type="radio"/> 無効 <input checked="" type="radio"/> 自動で取得する(DHCP) <input type="radio"/> 手動で設定する	IPアドレス		プレフィックス長	64	フレームサイズ	1500 リストから選択 ▼	追加設定		設定方法	<input checked="" type="radio"/> 自動で取得する <input type="radio"/> 手動で設定する	デフォルトゲートウェイ		DNSサーバー	
IPアドレス設定方式	<input type="radio"/> 無効 <input checked="" type="radio"/> 自動で取得する(DHCP) <input type="radio"/> 手動で設定する																
IPアドレス																	
プレフィックス長	64																
フレームサイズ	1500 リストから選択 ▼																
追加設定																	
設定方法	<input checked="" type="radio"/> 自動で取得する <input type="radio"/> 手動で設定する																
デフォルトゲートウェイ																	
DNSサーバー																	

項番	設定内容の詳細
	<p>【無線アクセスポイント設定(ブリッジモード)】</p> <p>※IPv6 通信を透過させるため NAT モードからブリッジモードの変更が必要。</p>  <p>IPアドレスとトラフィック</p> <p>クライアントへのIP割り当て</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> NATモード: Meraki DHCPを利用 クライアントは隔離された10.0.0.0/8 ネットワーク内のIPアドレスを受け取ります。無 で許可すれば有線LAN上のデバイスと通信できます。 <input type="radio"/> ブリッジモード: 無線クライアントネットワークを有線LANの一部とします Merakiデバイスは透過的に動作します (NATまたはDHCPはありません)。ワイヤレ スネットワークIPを使用します。これは、シームレスなローミング、共有プリンター、ファイ アウォールに使用します。 <input type="radio"/> レイヤ3ローミング クライアントは、ブリッジモードと同様に、LANからDHCPリースを受信するが、静的 IPアドレスの場合、クライアントは静的IPアドレスを受け取ります。

(3) クラウド環境の設定

項番	設定内容の詳細
1	<p>【VPS+Windows における、IPv6 の有効化設定】</p> <p>PowerShell より、以下のコマンドを実行する</p> <pre># Enable-NetAdapterBinding -Name "Global" -ComponentID ms_tcpip6</pre> <p>※上記は「さくらクラウド」で Windows Server を使用した時の例 参考「IPv6 有効化手順」 https://manual.sakura.ad.jp/vps/network/ipv6/windows.html#id11</p>

※今回の検証において、収集管理システムで使用しているクラウドサービスの構築は提供元ベンダによ
って行われたが、仮想環境(VPS)で環境の構築時に IPv6 の有効化に必要であった設定の情報を得た
ため、上記を参考情報として記載する。

5.3.6 試験

本ユースケースで実施した内容と結果を示す。

5.3.6.1 実証内容と結果

1. ネットワークレベルの検証

5.3.5にしたがって構築した実証環境において、一般業務とIoTシステム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、社内ネットワークに保存された情報資産(ファイルサーバ)の利用といった一般的な業務について検証した。

IoT システムにおける検証では、社内ネットワーク上で稼働している無線接続の IoT システムに対する疎通性と動作の正常性を検証した。

その結果、IPv6 の規格に起因した課題が 1 件発生し、IPv6 対応における留意事項が 2 件発生した。

(1) 一般業務における検証について

IPv4 の経路(ルータおよび回線)と、IPv6 の経路(ルータおよび回線)は IPoE 接続により1回線(1プロバイダ)に統合された状態でインターネットに接続し、接続先の IPv6 対応状況により、通過する経路が切り替わる設計である。

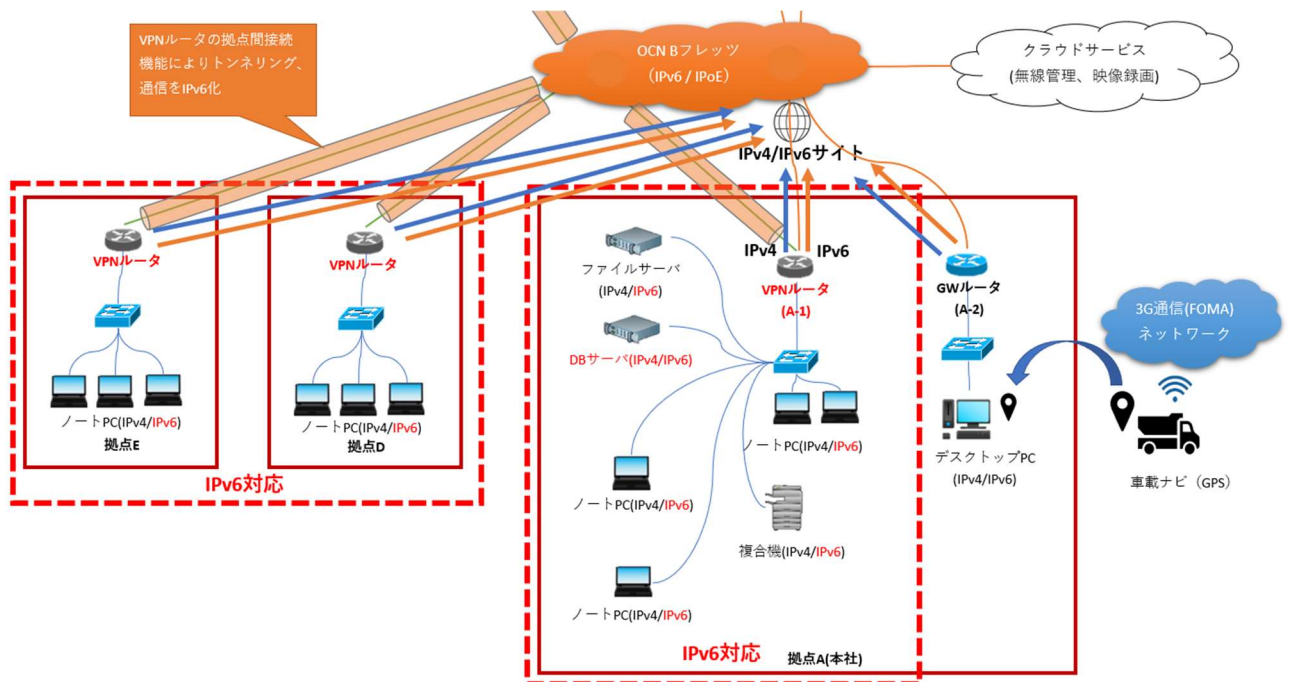


図 5.3.6-1 IPv4 経路と IPv6 経路

① 疎通確認

各機器に対して ping を実行し、通信経路に問題ないことを検証する。

また、VPN 経由で遠隔地の拠点から本社ネットワーク内部のファイルサーバ、DB サーバにアクセスすることが可能か、ping を実行して通信経路を検証する。

また、IPv4/IPv6 のデュアルスタックに対応した速度計測サイトを利用し、IPv6 接続の正常性および応答性、回線の速度を計測する。

② 通常業務を想定した WEB サービスやメール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。

③ 通常業務を想定した社内ネットワーク機器の利用

IPv4 と IPv6 が混在した環境において、IPv4 のシングルスタックから IPv4/IPv6 のデュアルスタック設定に変更した複合機、ファイルサーバが正常に利用できるか検証する。

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	拠点	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	有線	拠点 A (本社)	IPv6 優先	ルータ	IPv6	接続先に対し ping を実行する	ping が通る	OK
2	ノート PC	有線	拠点 A (本社)	IPv6 優先	DB サーバ	IPv6	接続先に対し ping を実行する	ping が通る	OK
3	ノート PC	有線	拠点 C~E	IPv6 優先	本社ルータ(VPN 経由)	IPv6	接続先に対し ping を実行する	ping が通る	OK
4	ノート PC	有線	拠点 C~E	IPv6 優先	DB サーバ (VPN 経由)	IPv6	接続先に対し ping を実行する	ping が通る	OK
5	ノート PC	有線	全拠点	IPv6 優先	速度計測サイト	IPv6	速度計測サイトにアクセスし、IPv4とIPv6の回線速度を計測する。 https://inonius.net/	IPv6 が検出され、正常に速度計測が行われる	OK

【#3の補足】

VPNを経由し、本社のGW ルータへ IPv6 で ping の応答を受信できることを確認した。

```
C:¥WINDOWS¥system32>ping -6 fdfe:208b: [REDACTED]:1::1

fdfe:208b: [REDACTED]:1::1 に ping を送信しています 32 バイトのデータ:
fdfe:208b: [REDACTED]:1::1 からの応答: 時間 =4ms
fdfe:208b: [REDACTED]:1::1 からの応答: 時間 =5ms
fdfe:208b: [REDACTED]:1::1 からの応答: 時間 =4ms
fdfe:208b: [REDACTED]:1::1 からの応答: 時間 =4ms
```

図 5.3.6-2 IPv6 で ping 応答あり(GW ルータ)

【#4の補足】

VPNを経由し、本社のDB サーバへ IPv6 で ping の応答を受信できることを確認した。

```
C:¥WINDOWS¥system32>ping -6 fdfe:208b: [REDACTED]:efd7

fdfe:208b: [REDACTED]:efd7 に ping を送信しています 32 バイトのデータ:
fdfe:208b: [REDACTED]:efd7 からの応答: 時間 =5ms
fdfe:208b: [REDACTED]:efd7 からの応答: 時間 =5ms
fdfe:208b: [REDACTED]:efd7 からの応答: 時間 =5ms
fdfe:208b: [REDACTED]:efd7 からの応答: 時間 =5ms
```

図 5.3.6-3 IPv6 で ping 応答あり(DB サーバ)

【#5の補足】

速度計測が正常に実行され、回線速度についてIPv4とIPv6で概ね差異がないことを確認した。

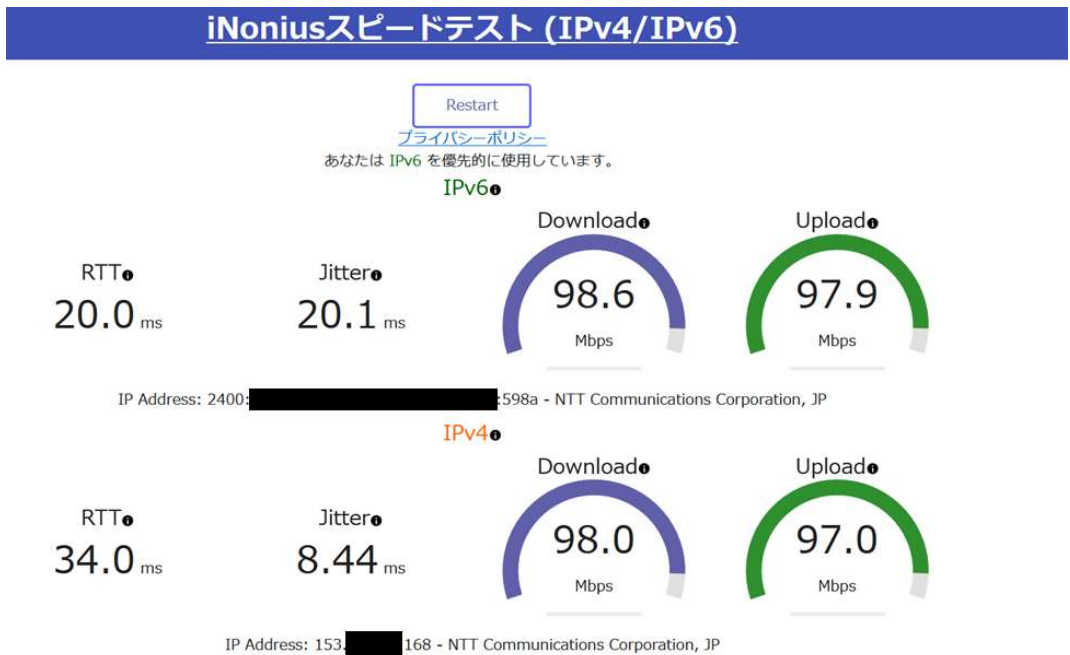


図 5.3.6-4 計測サイトによる IPv4/IPv6 速度計測の実行例

表 5.3.6-1 各拠点における IPv6 回線の速度計測結果(日中の参考値)

IPv6	RTT (ms)	Jitter (ms)	ダウンロード速度 (Mbps)	アップロード速度 (Mbps)
拠点 A	20.62	20.094	94.62	73.92
拠点 B	28.2	3.332	436.8	251.0
拠点 C	23.3	0.874	96.84	100.8
拠点 D	22.42	1.286	98.76	100.0
拠点 E	20.74	0.574	303.4	226.8

表 5.3.6-2 各拠点における IPv4 回線の速度計測結果(日中の参考値)

IPv4	RTT (ms)	Jitter (ms)	ダウンロード速度 (Mbps)	アップロード速度 (Mbps)
拠点 A	16.96	1.356	95.78	89.3
拠点 B	22.0	19.222	348.8	608.6
拠点 C	17.18	0.982	98.3	102.1
拠点 D	16.2	0.9	100.5	100.14
拠点 E	14.56	0.494	328.6	300.0

② メールや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 (Windows)	有線	IPv6 優先	IPv6 未対応メールサービス	IPv4	実証実験ネットワークに接続した状態で、OCN メールサービス経由でメール送受信を行う	メールの送受信ができる	OK
2	ノート PC (Windows)	有線	IPv6 優先	インターネット	IPv6	Google 等、一般業務で使用するサイトに接続	インターネットの検索サイトの利用、サイト閲覧に問題が発生しないこと	OK

③ 社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 (Windows)	有線	IPv6 優先	複合機	IPv6	IPv6 の標準 TCP/IP ポートで印刷処理を実行する	ネットワーク経由の印刷が正常に行える	OK
2	ノート PC (Windows)	有線	IPv6 優先	ファイルサーバ	IPv6	ドメイン参加した PC から、IPv6 の UNC ⁶⁴ 表記で共有フォルダにアクセスする	認証が正常に行われ、ファイル共有が可能である	OK

⁶⁴ UNC : Universal Naming Convention の略称であり、Windows ネットワーク上で共有されている様々な資源（ファイルやフォルダ、プリンタなど）の位置を表記する標準的な記法である。

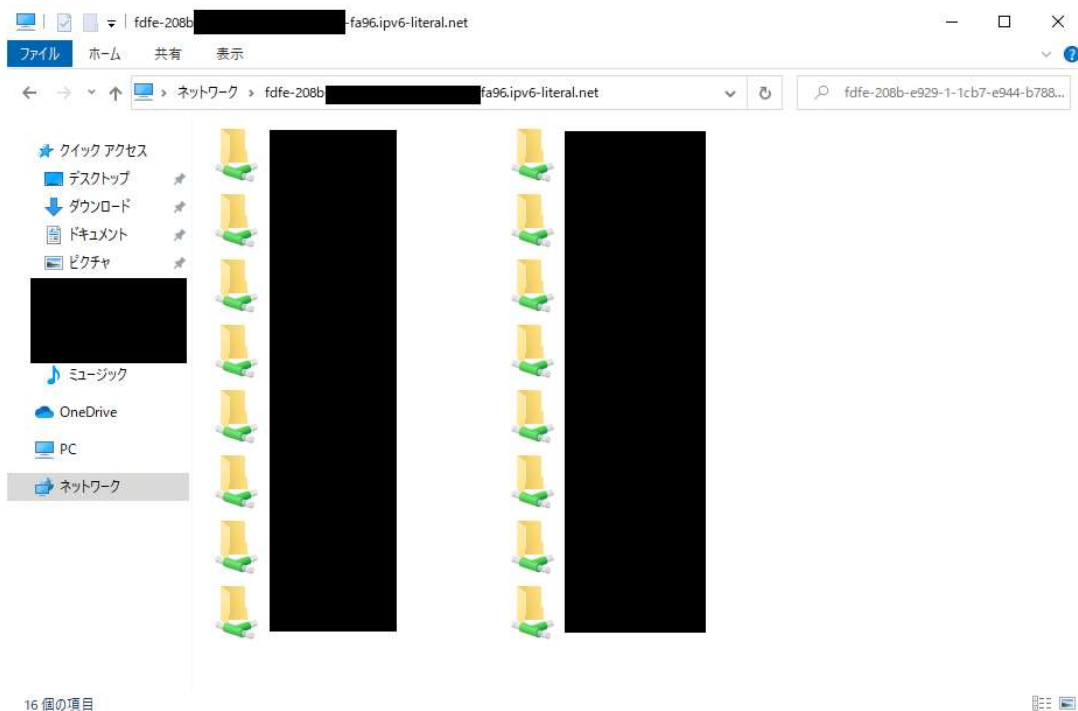


図 5.3-1 IPv6 の UNC 表記による共有フォルダのアクセス例

(2) IoT システムにおける検証について

① IoT システムの疎通、基本機能確認

基幹ネットワークに設置された IoT システムの通信経路と基本機能の確認を行う。クライアント端末から無線アクセスポイントをリモート制御するクラウドサービスへ接続し、基本的な管理機能が正常に利用可能か検証する。次に、ネットワークカメラに対して IPv4/IPv6 のデュアルスタック設定を行い、IPv6 アドレスが設定されたネットワークカメラが NAS に接続し、IPv6 通信で録画した映像が保存可能であるか検証する。これらの試験結果を以下に示す。

①IoT システムの疎通、基本機能確認の結果

#	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	無線 アクセスポイント	IPv6	WEB ブラウザで管理画面にアクセスし、無線アクセスポイントがオンライン状態であることを確認する	クラウド管理機能上でオンライン状態になっており、機器の状態が参照できる	OK
2	ネットワークカメラ	無線	IPv4 IPv6	NAS	IPv6	ネットワークカメラから NAS に IPv6 アドレスで接続し、録画機能を実行する	ネットワークカメラのライブ映像が NAS 上に録画保存される	OK

【#1の補足】

WEB ブラウザの管理画面上で、無線アクセスポイントがオンライン状態になっており、無線アクセスポイントの状態や、同アクセスポイントに接続しているネットワークカメラの状態が参照できることを確認した。

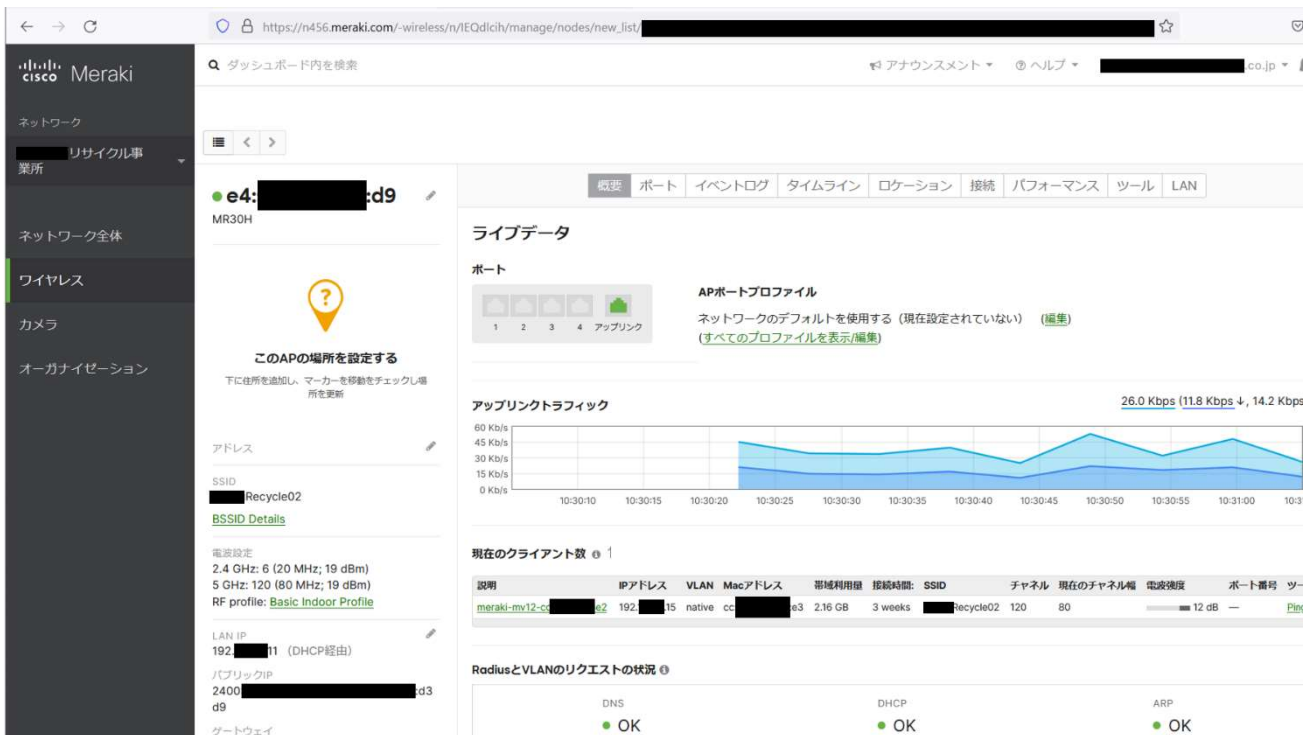


図 5.3.6-5 管理画面上で機器の状態参照の結果

次に管理画面の操作中、クラウドサービスの通信がIPv6で行われていることを確認した。クラウドサービスのIPv6アドレスをnslookupから取得し、実際に取得したIPv6アドレスで通信が行われていることをパケットキャプチャで確認した。

```
CA: 管理者: コマンド プロンプト
Microsoft Windows [Version 10.0.19043.1526]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>nslookup n456.meraki.com
サーバー: UnKnown
Address: 2404:1a8:7f01:b::3

権限のない回答:
名前: sin221.meraki.com
Addresses: 2620:12f:c008:0:3e57:31ff:fe19:5874
          209.206.61.122
Aliases: n456.meraki.com

C:\WINDOWS\system32>
```

図 5.3.6-6 クラウドサービスの IPv6 アドレス取得結果

※クライアント PC … 先頭が 2400、末尾が 56fc のグローバルユニキャストアドレス

※クラウドサービス … 2620:12f:c008:0:3e57:31ff:fe19:5874 のグローバルユニキャストアドレス

No.	Time	Source	port	Destination	port	Protocol	Length	Info
94	2.370949	2400: [redacted] :56fc		2620:12f:c008:0:3e57:31ff:fe19:5874	443	TLSv1.2	1741	Application Data
101	2.466310	2620:12f:c008:0:3e57:31ff:fe19:5874	443	2400: [redacted] :56fc	52189	TCP	74	443 → 52189 [ACK]
105	2.492447	2620:12f:c008:0:3e57:31ff:fe19:5874	443	2400: [redacted] :56fc	52189	TCP	1514	443 → 52189 [ACK]
106	2.492447	2620:12f:c008:0:3e57:31ff:fe19:5874	443	2400: [redacted] :56fc	52189	TCP	1514	443 → 52189 [ACK]
107	2.492447	2620:12f:c008:0:3e57:31ff:fe19:5874	443	2400: [redacted] :56fc	52189	TLSv1.2	624	Application Data
108	2.492725	2400: [redacted] :56fc	52189	2620:12f:c008:0:3e57:31ff:fe19:5874	443	TCP	74	52189 → 443 [ACK]
113	2.526786	2400: [redacted] :56fc	52189	2620:12f:c008:0:3e57:31ff:fe19:5874	443	TLSv1.2	1711	Application Data
114	2.529900	2400: [redacted] :56fc	52190	2620:12f:c008:0:3e57:31ff:fe19:5874	443	TLSv1.2	1708	Application Data
115	2.532346	2400: [redacted] :56fc	52191	2620:12f:c008:0:3e57:31ff:fe19:5874	443	TLSv1.2	1707	Application Data

図 5.3.6-7 管理画面にアクセス中のパケットキャプチャの結果

【#2 の補足】

ネットワークカメラを NAS に接続する際、NAS の IPv6 アドレスで指定し、正常に接続できるかを確認後、録画機能を実行した。



AXIS M1045-LW



ストレージ

ネットワークストレージ



サーバー (926.4 GB)

ホスト:

2400 [redacted] :8a4

4

共有: disk1

フリー: 924.4 GB

ステータス: OK

図 5.3.6-8 ネットワークカメラと NAS の IPv6 指定接続結果

※クライアント PC … 先頭が 2400、末尾が a813 の IPv6 グローバルユニキャストアドレス

※ネットワークカメラ … 先頭が 2400、末尾が 8a44 の IPv6 グローバルユニキャストアドレス

Time	Source	port	Destination	port	Protocol	Length	Info
1 0.000000	fe80::c0c:4ebf:3f56:1e7c		fe80::3676:c5ff:fef9:8a44		ICMPv6	86	Neighbor Solicitation for fe80::
2 0.000215	fe80::3676:c5ff:fef9:8a44		fe80::c0c:4ebf:3f56:1e7c		ICMPv6	78	Neighbor Advertisement fe80::367
3 0.187429	2400: [redacted] :4441	58366	2620: [redacted] :8a44	443	TCP	75	58366 → 443 [ACK] Seq=1 Ack=1 Wi
4 0.212321	2400: [redacted] :a813	39786	2400: [redacted] :8a44	445	SMB2	218	Create Request File:
5 0.212974	2400: [redacted] :8a44	445	2400: [redacted] :a813	39786	SMB2	242	Create Response File:
6 0.216541	2400: [redacted] :a813	39786	2400: [redacted] :8a44	445	SMB2	218	Create Request File:
7 0.216974	2400: [redacted] :8a44	445	2400: [redacted] :a813	39786	SMB2	242	Create Response File:
8 0.220442	2400: [redacted] :a813	39786	2400: [redacted] :8a44	445	SMB2	195	GetInfo Request FS_INFO/fileFsFu
9 0.221710	2400: [redacted] :8a44	445	2400: [redacted] :a813	39786	SMB2	194	GetInfo Response
10 0.223689	2400: [redacted] :a813	39786	2400: [redacted] :8a44	445	SMB2	195	GetInfo Request FS_INFO/fileFsFu
11 0.224772	2400: [redacted] :8a44	445	2400: [redacted] :a813	39786	SMB2	194	GetInfo Response
12 0.227199	2400: [redacted] :a813	39786	2400: [redacted] :8a44	445	SMB2	178	Close Request File:
13 0.227468	2400: [redacted] :8a44	445	2400: [redacted] :a813	39786	SMB2	214	Close Response
14 0.229465	2400: [redacted] :a813	39786	2400: [redacted] :8a44	445	SMB2	178	Close Request File:
15 0.229659	2400: [redacted] :8a44	445	2400: [redacted] :a813	39786	SMB2	214	Close Response
16 0.278855	2400: [redacted] :a813	39786	2400: [redacted] :8a44	445	TCP	86	39786 → 445 [ACK] Seq=667 Ack=78

図 5.3.6-9 ネットワークカメラ録画中のパケットキャプチャ結果

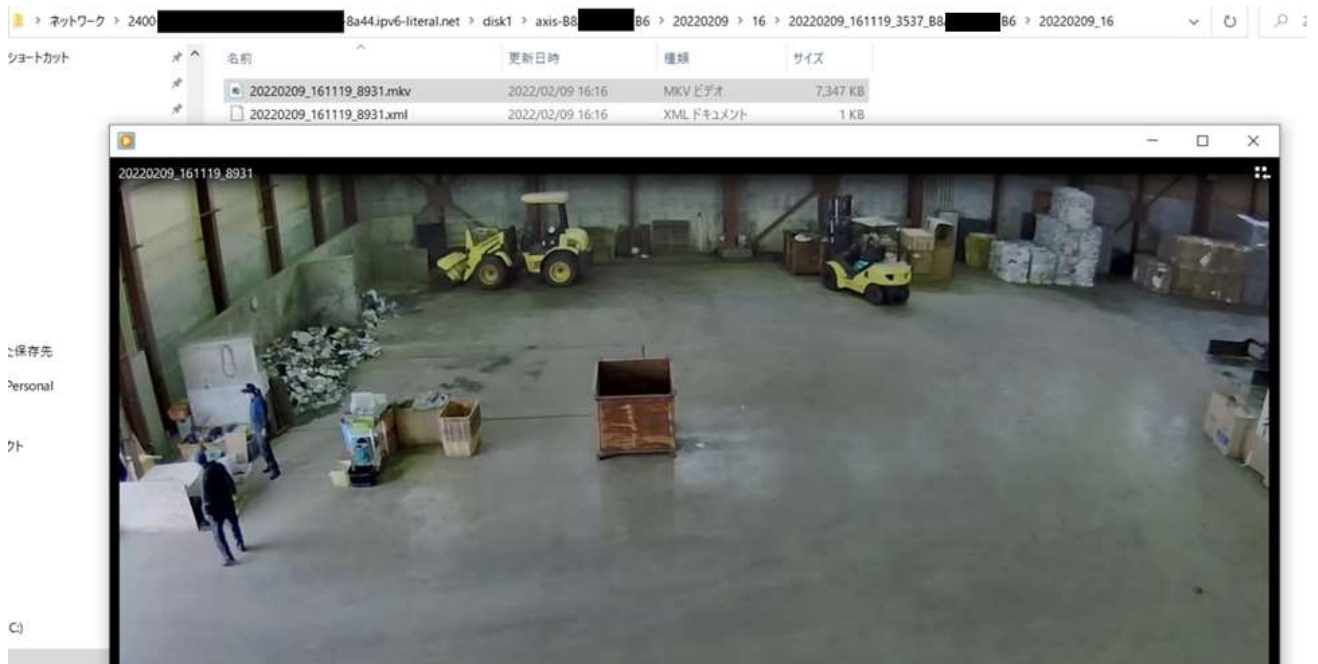


図 5.3.6-10 ネットワークカメラでNASに録画した映像の参照結果

2. LAN 内アプリケーションレベルの検証

5.3.5 にしたがって構築した実証環境において、C 社が行っている収集業務で使用する収集管理システムを IPv6 のネットワーク上で利用したときの影響を検証した。検証には、オンプレミス環境で利用する PC 向けのアプリケーションと、モバイル端末向けのアプリケーションを使用した。

その結果、PC 版アプリケーション、モバイル版アプリケーションいずれにおいても、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 2 件発生した。

(1) 業務アプリケーションにおける検証について

① 収集管理システムの動作検証

収集管理システムは以下のネットワーク構成で検証を行った。

(ア) オンプレミス環境のイントラネット接続における検証

(イ) VPN を経由した拠点間のイントラネット接続における検証

(ウ) LTE ネットワークを介したインターネット接続における検証

(ア)、(イ)では、PC 版アプリケーションを使用し、オンプレミス環境、または VPN を経由したイントラネット接続のネットワークにおいて、DB サーバが収集管理システムのデータ登録、データ参照操作を IPv4/IPv6 を使用して正常に行えることを検証した。

(ウ)では、LTE 通信が可能なモバイル端末を検証のために用意したが、通信基地局側の制限により IPv4 シングルスタック動作となることが判明した。このため、モバイル端末向けのアプリケーションの検証については IPv4/IPv6 デュアルスタックに対応した拠点外の Wi-Fi ネットワークに接続し、IPv4/IPv6 いずれにおいても利用可能か検証した。

① 収集管理システムの動作検証の結果

#	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	有線	IPv6 優先	収集管理 システム (PC 版)	IPv6	オンプレミス環境(PC 端末と DB サーバが同一拠点)において、データ入力、参照操作を実行する	データ入力、参照が正常に参照できる	OK
2	ノート PC	有線	IPv6 優先	収集管理 システム (PC 版)	IPv6	VPN 接続による環境(PC 端末と DB サーバが別拠点)において、データ入力、参照操作を実行する	データ入力、参照が正常に参照できる	OK
3	タブレット	無線	IPv6 優先	収集管理 システム (モバイル 版)	IPv6	IPv6 で通信可能な拠点外のインターネット接続環境において、データ入力、参照操作を実行する	データ入力、参照が正常に参照できる	OK

【#1 の補足】

DB サーバと同一拠点内のノート PC から収集管理システムを操作し、システムの基本操作が可能であることを確認した。

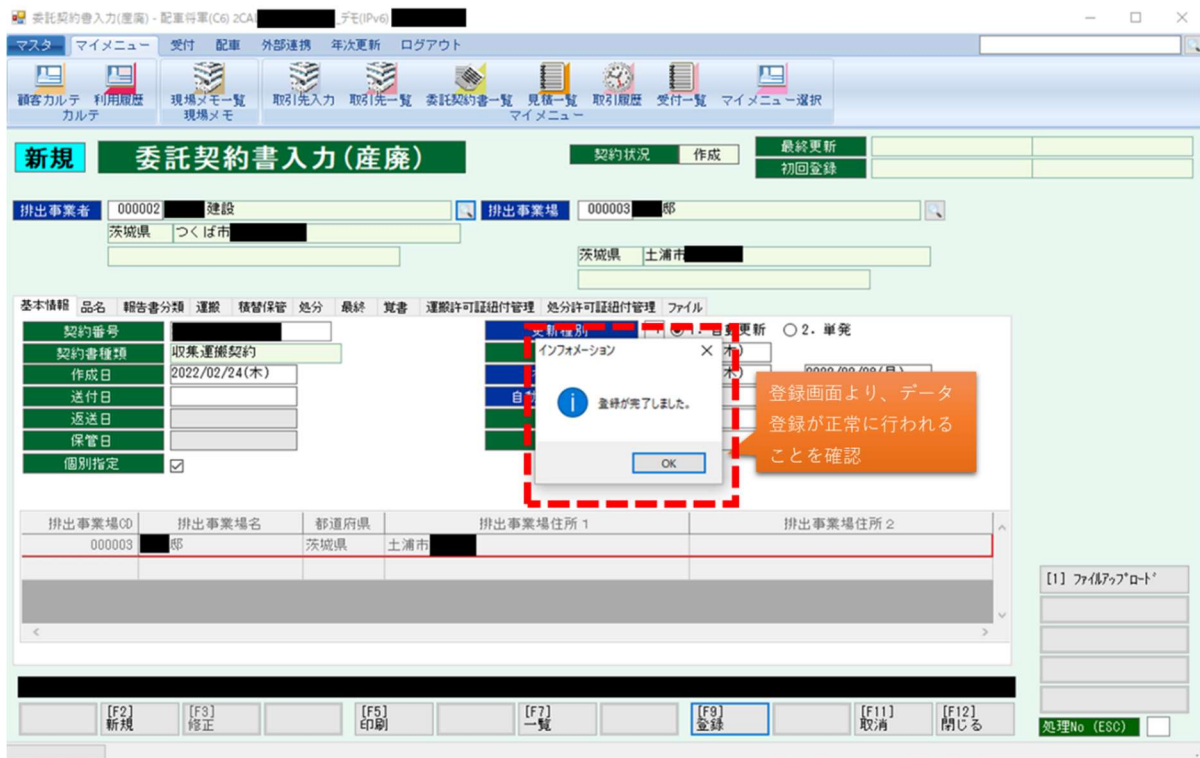


図 5.3.6-11 収集管理システム(PC 版)の実行結果例(登録処理)

- ※同一拠点内 PC の ULA … 先頭が fdfe、末尾が 9cd6 のユニークローカルアドレス
- ※DB サーバの ULA … 先頭が fdfe、末尾が efd7 のユニークローカルアドレス

No.	Time	Source	port	Destination	port	Protocol	Length	Info
159	50.739474	fdfe:208b:...	9cd6	51173 fdfe:208b:...	:efd7	11488 TCP	74	51173 → 11488 [AI
160	50.739787	fdfe:208b:...	9cd6	51173 fdfe:208b:...	:efd7	11488 TLSv1.2	168	Ignored Unknown I
161	50.740138	fdfe:208b:...	:efd7	11488 fdfe:208b:...	9cd6	51173 TLSv1.2	128	Ignored Unknown I
162	50.741255	fdfe:208b:...	9cd6	51173 fdfe:208b:...	:efd7	11488 TLSv1.2	267	Ignored Unknown I
163	50.741910	fdfe:208b:...	:efd7	11488 fdfe:208b:...	9cd6	51173 TLSv1.2	223	Ignored Unknown I
164	50.743464	fdfe:208b:...	9cd6	51173 fdfe:208b:...	:efd7	11488 TLSv1.2	133	Ignored Unknown I
165	50.743624	fdfe:208b:...	9cd6	51173 fdfe:208b:...	:efd7	11488 TLSv1.2	512	Application Data
166	50.743670	fdfe:208b:...	:efd7	11488 fdfe:208b:...	9cd6	51173 TCP	74	11488 → 51173 [AI
171	51.062049	fdfe:208b:...	:efd7	11488 fdfe:208b:...	9cd6	51173 TLSv1.2	560	Ignored Unknown I

図 5.3.6-12 収集管理システム操作における DB サーバ間のパケットキャプチャ(同一拠点内)

【#2 の補足】

DB サーバと他拠点に存在するノート PC から収集管理システムを操作し、システムの基本操作が可能であることを確認した。

委託契約書一覧

アラート件数: 300
読込データ件数: 74

委託契約番号	契約書種類	契約状況	表示条件
作成	収集運搬契約	産廃	2022/02/24(木)
作成	収集運搬契約	産廃	2022/02/24(木)
作成	収集運搬契約	産廃	2022/03/01(火)
作成	収集運搬契約	産廃	2022/03/01(火)
作成	収集運搬契約	産廃	2021/07/07(水)

自拠点と他拠点で登録したデータが、一覧画面上で参照できることを確認

図 5.3.6-13 収集管理システム(PC 版)の実行結果例(本社拠点へ VPN 経由で利用)

- ※拠点外 PC (VPN 接続) の ULA … 先頭が fdfe、末尾が 692b のユニークローカルアドレス
- ※DB サーバの ULA … 先頭が fdfe、末尾が efd7 のユニークローカルアドレス

No.	Time	Source	port	Destination	port	Protocol	Length	Info
1399	42.823159	fdfe:208b:...	692b	59897 fdfe:...	5:efd7	11488 TCP	74	59897 → 11488 [AI
1400	42.823159	fdfe:208b:...	692b	59897 fdfe:...	5:efd7	11488 TLSv1.2	168	Ignored Unknown I
1401	42.823873	fdfe:208b:...	:efd7	11488 fdfe:...	692b	59897 TLSv1.2	128	Ignored Unknown I
1403	42.829510	fdfe:208b:...	692b	59897 fdfe:...	5:efd7	11488 TLSv1.2	235	Ignored Unknown I
1404	42.834078	fdfe:208b:...	:efd7	11488 fdfe:...	692b	59897 TLSv1.2	1258	Ignored Unknown I
1405	42.843480	fdfe:208b:...	692b	59897 fdfe:...	5:efd7	11488 TLSv1.2	175	Ignored Unknown I
1406	42.844970	fdfe:208b:...	:efd7	11488 fdfe:...	692b	59897 TLSv1.2	133	Ignored Unknown I
1407	42.852222	fdfe:208b:...	692b	59897 fdfe:...	5:efd7	11488 TLSv1.2	514	Application Data
1408	42.854565	fdfe:208b:...	:efd7	11488 fdfe:...	692b	59897 TLSv1.2	560	Ignored Unknown I

図 5.3.6-14 収集管理システム操作における DB サーバ間のパケットキャプチャ(拠点外から VPN を経由)

【#3 の補足】

タブレット端末からインターネット経由で収集管理システム用クラウドサービスの WEB サーバにアクセスし、データ入力等の基本操作が可能であることを確認した。

また、タブレット端末の操作時に、収集管理システム用クラウドサービスの WEB サーバが本社拠点のファイアウォールを通過して、オンプレミス環境の DB サーバに外部から正常に接続できることを確認した。

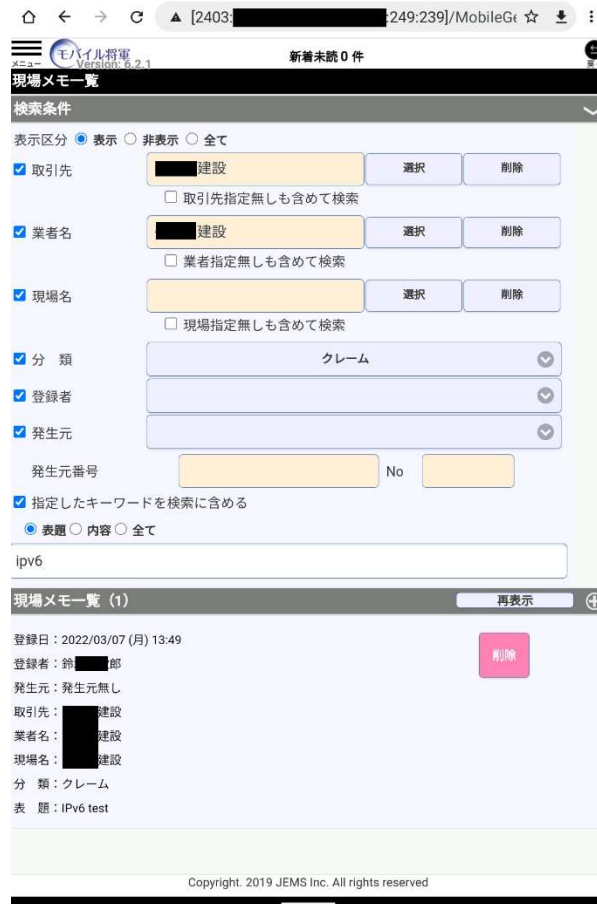


図 5.3.6-15 収集管理システム(モバイル版)の実行結果(インターネット接続)

※収集管理システム用クラウドサービスの WEB サーバ … 先頭が 2403、末尾が 239 の IPv6 グローバルユニキャストアドレス

※本社拠点内の DB サーバ … 先頭が 2400、末尾が efd7 の IPv6 グローバルユニキャストアドレス

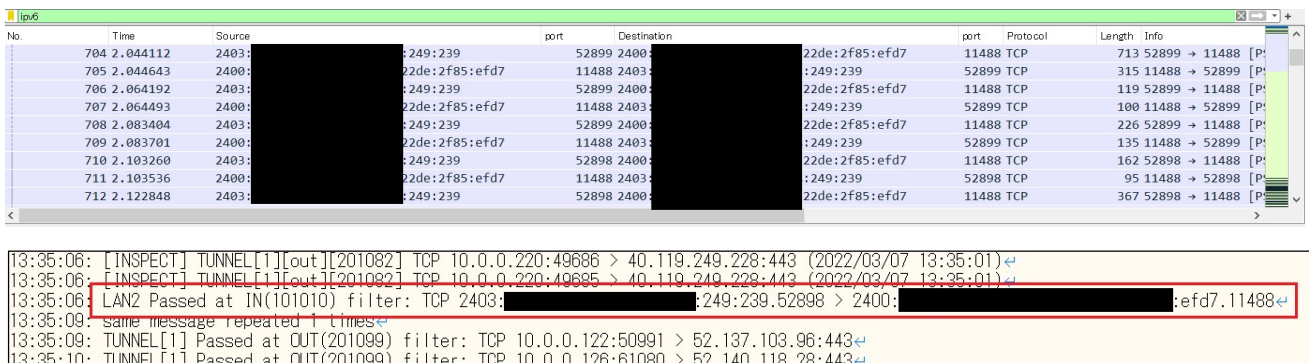


図 5.3.6-16 WEB サーバと本社拠点内 DB サーバ間のパケットキャプチャ、FW ログ

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 IoT システムのメーカー側が提供しているクラウドサービスを利用して、ネットワークカメラの映像の録画および参照ができるか検証した。

その結果、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。

今回の実証実験で利用したクラウドサービス「Meraki Dashboard」については、Cisco 製の無線機器、ネットワークカメラ等の IoT デバイスをクラウドで一括管理するための WEB サービスであり、サービスのフロントエンドとなる WEB サーバは IPv6 に対応している。

クラウドサービスに接続するネットワークカメラは IPv4 のみ対応の機器であるが、本サービスが提供しているクラウド録画機能、およびライブ映像参照機能を利用することで、ネットワークカメラの映像が IPv4/IPv6 のデュアルスタック環境で参照できるか検証した。検証範囲を図 5.3.6-1 に示す。

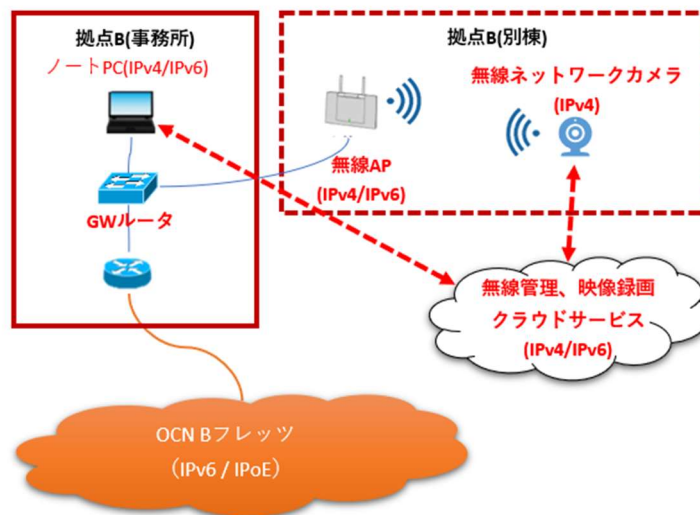


図 5.3.6-17 クラウドサービスの検証イメージ図

(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

① クラウド録画参照機能およびライブ映像参照機能の検証

クラウドサーバ上のネットワークカメラの録画映像の参照機能およびライブ映像の参照機能が問題なく利用できるか検証する。検証の結果、クラウドサービスから配信される録画映像の参照機能が IPv4 のみ対応であり、クラウドサービスに IPv6 で接続している場合も、動画のライブ映像は IPv4 でストリーミング再生されることを確認した。

上記①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 クラウド録画参照機能の検証結果

#	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	Meraki DashBoard	IPv6 想定	クラウド上に録画されたネットワークカメラの映像を、ノート PC で再生する	録画データが IPv6 でストリーミング再生される	NG
2	ノート PC	無線	IPv6 優先	Meraki DashBoard	IPv6 想定	ネットワークカメラのライブ映像を、クラウドサービスを介してノート PC で参照する	ライブ映像データが IPv6 でストリーミング再生される	NG

【#1、2の補足】

本検証シナリオで利用したクラウドサービスは 4.4.1(2)、「IoT システムにおける検証」で利用したものと同一クラウドサービスであるため、nslookup にて IPv6 対応されていることを確認した。

しかし、ネットワークカメラのライブ映像参照機能は、動画のストリーミング再生中の通信が全て IPv4 で行われていた。取得したパケットキャプチャを参照したところ、動画のストリーミング再生時に IPv4 で通信が行われることを確認した。

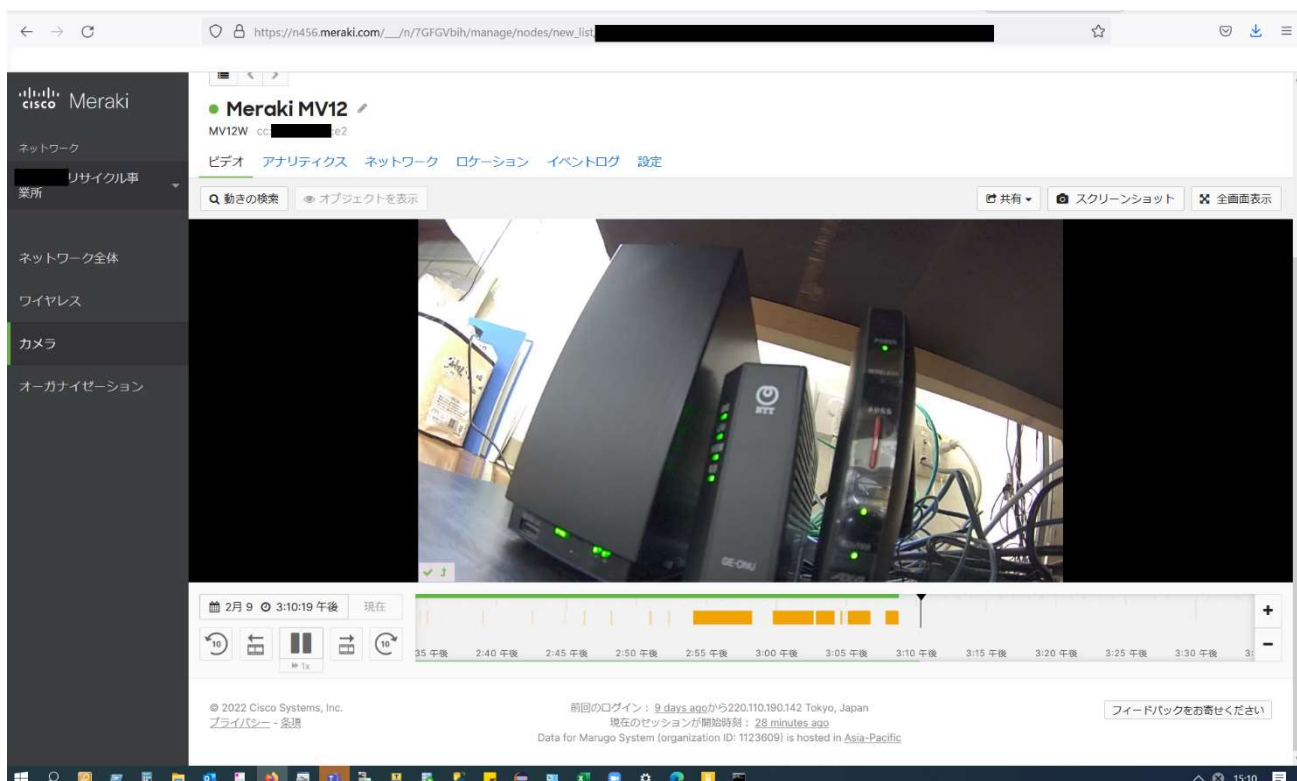


図 5.3.6-18 クラウドサービスの録画映像参照機能

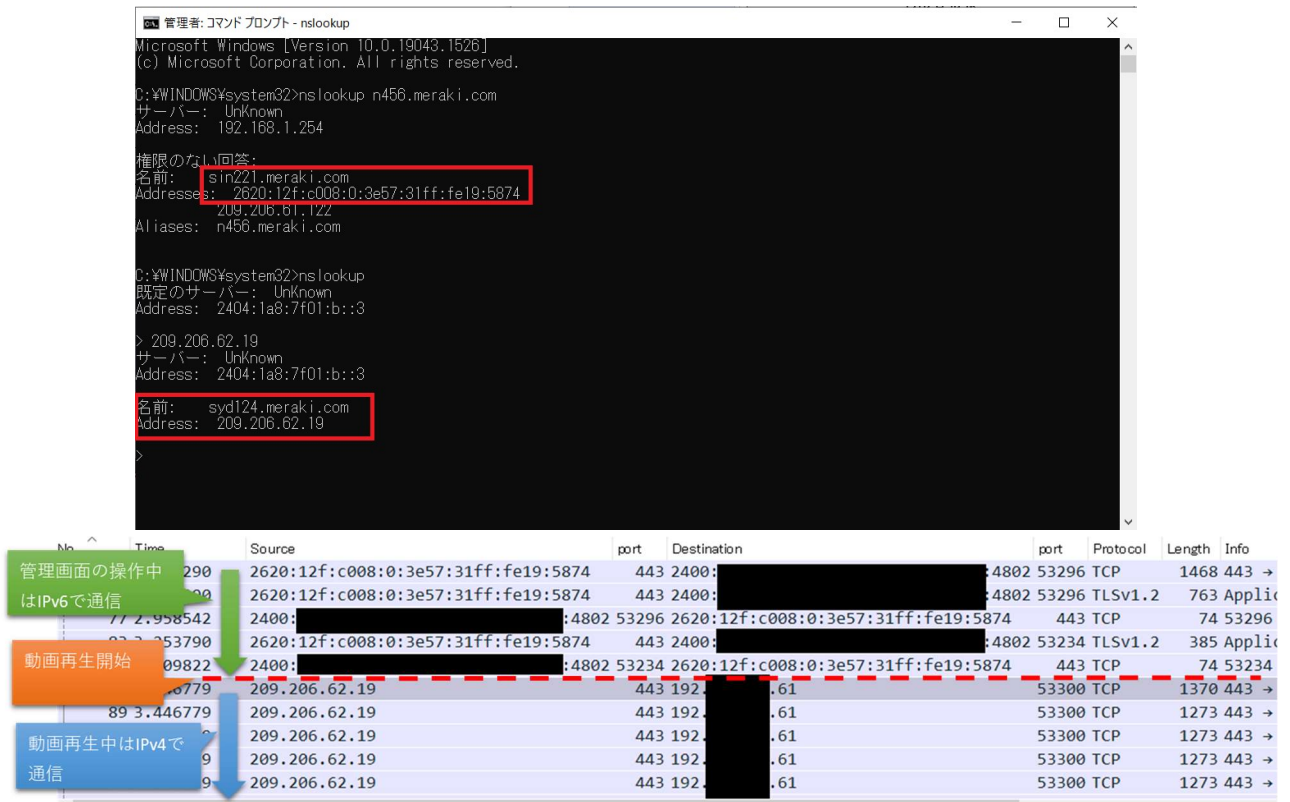


図 5.3.6-19 クラウドサービスの nslookup、動画再生時のパケットキャプチャ確認結果

5.3.6.2 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:中小企業C」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、機器メーカー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ティング事例をもとに、IPv6 対応において普遍的に留意すべき点を示す。