IPv6 対応ガイドライン

中小企業・大学のシステム担当者様へ

2022 年 5 月　総務省

目次

1 はじめに 1
1.1 読者の皆様へ 1
1.2 本ガイドラインの対象者 1
1.3 本ガイドラインの全体構成 2
1.4 本ガイドラインの活用方法 3
2 IPv6 の今 4
2.1 海外の動向 4
2.2 国内の動向 8
2.3 IPv6 未対応時の問題 9
2.4 IPv6 対応時の課題 10
3 ネットワーク構成のモデル化 11
3.1 モデルケースの整理 11
3.2 モデルごとの IPv6 対応プラン 13
3.2.1 モデル A 13
3.2.2 モデル B 14
3.2.3 モデル C 15
3.2.4 モデル D 16
3.2.5 モデル E 17
3.2.6 モデル F 18
3.2.7 モデル G 19
3.2.8 モデル H 20
3.2.9 モデル I 21
3.2.10 モデル J 22
3.3 ユースケースとしてのモデル選定 23
3.3.1 モデル選定理由 23
3.3.2 選定モデルとユースケースの概要 24
4 IPv6 対応シナリオの策定 25
4.1 要件定義 26
4.2 スケジュール計画 28
4.3 設計 29
4.4 構築 36
4.5 試験 38
4.6 運用・保守 40
5 IPv6 対応ユースケース(中小企業) 43
5.1 モデル G:中小企業 A 43

5.1.1 ユースケース企業の紹介 43
5.1.2 要件定義 44
5.1.3 スケジュール計画 46
5.1.4 設計 47
5.1.5 構築 57
5.1.6 試験 75
5.2 モデル I:中小企業 B 102
5.2.1 ユースケース企業の紹介 102
5.2.2 要件定義 103
5.2.3 スケジュール計画 106
5.2.4 設計 107
5.2.5 構築 116
5.2.6 試験 133
5.3 モデル G:中小企業 C 166
5.3.1 ユースケース企業の紹介 166
5.3.2 要件定義 167
5.3.3 スケジュール計画 170
5.3.4 設計 171
5.3.5 構築 181
5.3.6 試験 195
6 IPv6 対応ユースケース(大学) 212
6.1 モデル I:大学 A 212
6.1.1 ユースケース大学の紹介 212
6.1.2 要件定義 213
6.1.3 スケジュール計画 216
6.1.4 設計 217
6.1.5 構築 225
6.1.6 試験 241
7 IPv6 環境への移行に向けたコスト試算の考え方 297
7.1 システム開発におけるコストの構成要素 297
7.1.1 アプリケーション開発・運用に係るコスト 298
7.1.2 インフラ整備に係るコスト 298
7.1.3 調達に係るコスト 298
7.2 IPv6 対応におけるコスト試算の考え方 299
7.2.1 アプリケーションの IPv6 対応に係るコスト 300
7.2.2 インフラの IPv6 対応に係るコスト 301

7.2.3 IPv6 対応コストチェック表について 302
8 IPv6 対応チェックシートの活用 303
9 その他 IPv6 対応に向けて考慮すべき事項 304
10 参考資料 306
10.1 文献 306
10.2 サイト 306
11 付録 307

1　はじめに

1.1　読者の皆様へ

本ガイドラインは、中小企業および大学の皆様が IPv6 の今を知り、IPv6 対応の必要性を認識した上で、自身の情報システムを IPv6 対応するための知見やノウハウを紹介することを目的としたものである。

IPv4 アドレスの枯渇が謳われてから長らく経過したが、このまま何もしないことは企業および大学へ致命的な問題を招く可能性がある。インターネットサービスの利用者/提供者の立場で考えられる問題を以下に示す。

(1) インターネットサービス利用者の立場

商用機器やサービスの IPv6 対応が進むに連れて、IPv6 は IPv4 よりも優先されてきた。インターネットサービスを利用する際、IPv4 通信は IPv6 通信よりも遅い、あるいは一部機能を利用できなくなる可能性がある。また、商用機器やサービスの初期設定で IPv6 有効になっていることも多く、IPv6 に特化したサイバー攻撃の被害を受ける可能性もある。

(2) インターネットサービス提供者の立場

インターネットサービスを提供する際、サービスが IPv6 未対応だとエンドユーザに安定的な品質のサービスを提供できなくなる可能性がある。また、2016 年 6 月から、Apple による iOS アプリの審査基準として IPv4 に依存するコードの禁止が追加され、IPv6 対応が iOS アプリの義務となったように、IPv6 未対応のサービスは、提供する市場が次第に縮小する可能性もある。

1.2　本ガイドラインの対象者

本ガイドラインは、業者を問わず中小企業および大学を対象としており、その経営者と情報システム担当者を想定読者としている。

1.3　本ガイドラインの全体構成

本ガイドラインの目次、記載概要、要点を図 1.3-1 に示す。

目次	記載概要	要点
1 はじめに		
2 IPv6の今		
2.1 海外の動向	海外のIPv6対応状況を述べている。	・世界全体でIPv6普及率は約35%（増加傾向） ・iOSはアプリはIPv6対応必須 ・IPv4はサービス提供（as a Service）として定義
2.2 国内の動向	国内のIPv6対応状況を述べている。	・モバイル3キャリアが発売するスマホはIPv6対応 ・モバイルキャリアにてIPv6シングルスタックによるサービス提供を開始 ・NTT NGNにおけるIPv6普及率が80%に到達 ・企業等の内部環境はIPv6未対応が多いと推測
2.3 IPv6未対応時の問題	IPv6に対応しない場合の問題を述べている。	・IPv6未対応時の問題は「品質低下/国際競争力低下」
2.4 IPv6対応時の課題	IPv6対応する場合の課題を述べている。	・IPv6対応時の課題は「企業等のメリットが見えにくい/IPv6人材不足/IPv6セキュリティ情報不足/IPv6対応が不十分な製品/サービスの存在」の4つ
3 ネットワーク構成のモデル化		
3.1 モデルケースの整理	令和元年度事業でのヒアリング調査を基づいたネットワーク構成モデルを述べている。	・モデル化する際の観点は「ネットワーク規模/拠点間VPN/イントラネット内のエンドポイント管理」の3つ
3.2 モデルごとのIPv6対応プラン	モデルごとのIPv6対応プランを述べている。	・IPv6対応プランの項目は「対応範囲/セグメント設計/拠点間VPN/エンドポイント管理」の4つ
3.3 ユースケースとしてのモデル選定	モデルの選定とユースケースの概要を紹介している。	・中小企業及び大学を想定し、選定モデルは「モデルG/モデルI」 ・選定モデルに該当しない場合においてもユースケースで紹介される内容は他モデルへ横展開可能
4 IPv6対応シナリオの策定		
4.1 要件定義	IPv6対応するにあたり、要件定義の5つの作業プロセスを紹介している。	・要件定義の作業プロセスは「現状の把握/移行方式の明確化/移行対象の明確化/IPv6対応状況の確認/導入方針の策定」の5つ
4.2 スケジュール計画	IPv6対応するにあたり、スケジュール計画において考慮すべきポイントを紹介している。	・スケジュール計画のポイントは「各作業工程には余裕を持たせる/調達のリードタイムを考慮する/業務影響を考慮し作業タイミングに留意する」の3つ
4.3 設計	IPv6対応するにあたり、設計において考慮すべきポイントを紹介している。	・設計の区分はIPAの非機能要求グレードの6大項目に基づき、「可用性/性能・拡張性/運用・保守性/移行性/セキュリティ/システム環境・エコロジー」の6つ
4.4 構築	IPv6対応するにあたり、構築の基本的な作業内容と構築時のIPv6特有の留意事項を紹介している。	・構築の基本作業は「コンフィグレーション作成/機器セットアップ/機器設置・起動/機器間接続」の4つ ・構築時のIPv6特有の留意事項は「IPv6は表記が長いためプレフィックス設定の誤りに注意する/IPv6アドレスは特殊な記載するIPアドレスの記載誤りに注意する/ネットワーク機器の設定がIPv4とIPv6で類似しているため注意する」の3つ
4.5 試験	IPv6対応するにあたり、構築後の試験における実施順序を紹介している。	・試験は最初にネットワーク層の確認を行ってからアプリケーション層の試験を実施することを推奨
4.6 運用・保守	IPv6対応するにあたり、運用・保守において考慮すべきポイントを紹介している。	・IPv6対応後の運用・保守のポイントは「体制整備/ドキュメント整備/自動化ツールのIPv6対応/DNSを活用したホスト名での運用/ログ管理におけるIPv6アドレス表記の統一/アクティブなIPv6アドレスの管理」の6つ
5 IPv6対応ユースケース （中小企業）		
5.1 モデルG：中小企業A	中小企業におけるモデルGのユースケースを紹介している。	・作業工程として「要件定義/スケジュール計画/設計/構築/試験」のアプトプットイメージを例示
5.2 モデルI：中小企業B	中小企業におけるモデルIのユースケースを紹介している。	・作業工程として「要件定義/スケジュール計画/設計/構築/試験」のアプトプットイメージを例示
5.3 モデルG：中小企業C	中小企業におけるモデルGのユースケースを紹介している。	・作業工程として「要件定義/スケジュール計画/設計/構築/試験」のアプトプットイメージを例示
6 IPv6対応ユースケース （大学）		
6.1 モデルI：大学A	大学におけるモデルIのユースケースを紹介している。	・作業工程として「要件定義/スケジュール計画/設計/構築/試験」のアプトプットイメージを例示
7 IPv6環境への移行に向けたコスト試算の考え方		
7.1 システム開発におけるコストの構成要素	システム開発のコスト構成要素を紹介している。	・システム開発のコスト構成要素は「開発・運用/インフラ整備/調達」の3つ
7.2 IPv6対応におけるコスト試算の考え方	IPv6対応に係るコスト試算表を紹介している。	・IPv6環境へ移行するためには「機器」と「サービス」のIPv6対応が必要 ・コストチェック表を活用しIPv6対応に係るコスト算出を効率化
8 IPv6対応チェックシートの活用		
8 IPv6対応チェックシートの活用	IPv6対応を円滑に進めるためのチェックシートを紹介している。	・IPv6対応チェックシートは計画フェーズと実行フェーズで活用
9 その他IPv6対応に向けて考慮すべき事項		
9 その他IPv6対応に向けて考慮すべき事項	IPv6対応をその他考慮すべき事項を紹介している。	・IPv6対応でその他考慮すべき事項としては「IPv6移行の対象について/IPv4とIPv6のデュアルスタックについて/リンクローカルアドレスのゾーンID/一時アドレスの運用/プロバイダより提供されるプレフィックスについて」の5つ
10 参考資料		

図 1.3-1 本ガイドラインの全体構成

1.4　本ガイドラインの活用方法

本ガイドラインを参照し、図 1.4-1 の流れで IPv6 対応することを提案する。本ガイドラインでは、IPv6 仕様の詳細説明はユースケースに必要な範囲に留めている。ユースケースを参照し、IPv6 対応の具体的な作業イメージが湧いた後、必要に応じて IPv6 の仕様について詳細を確認することが望ましい。

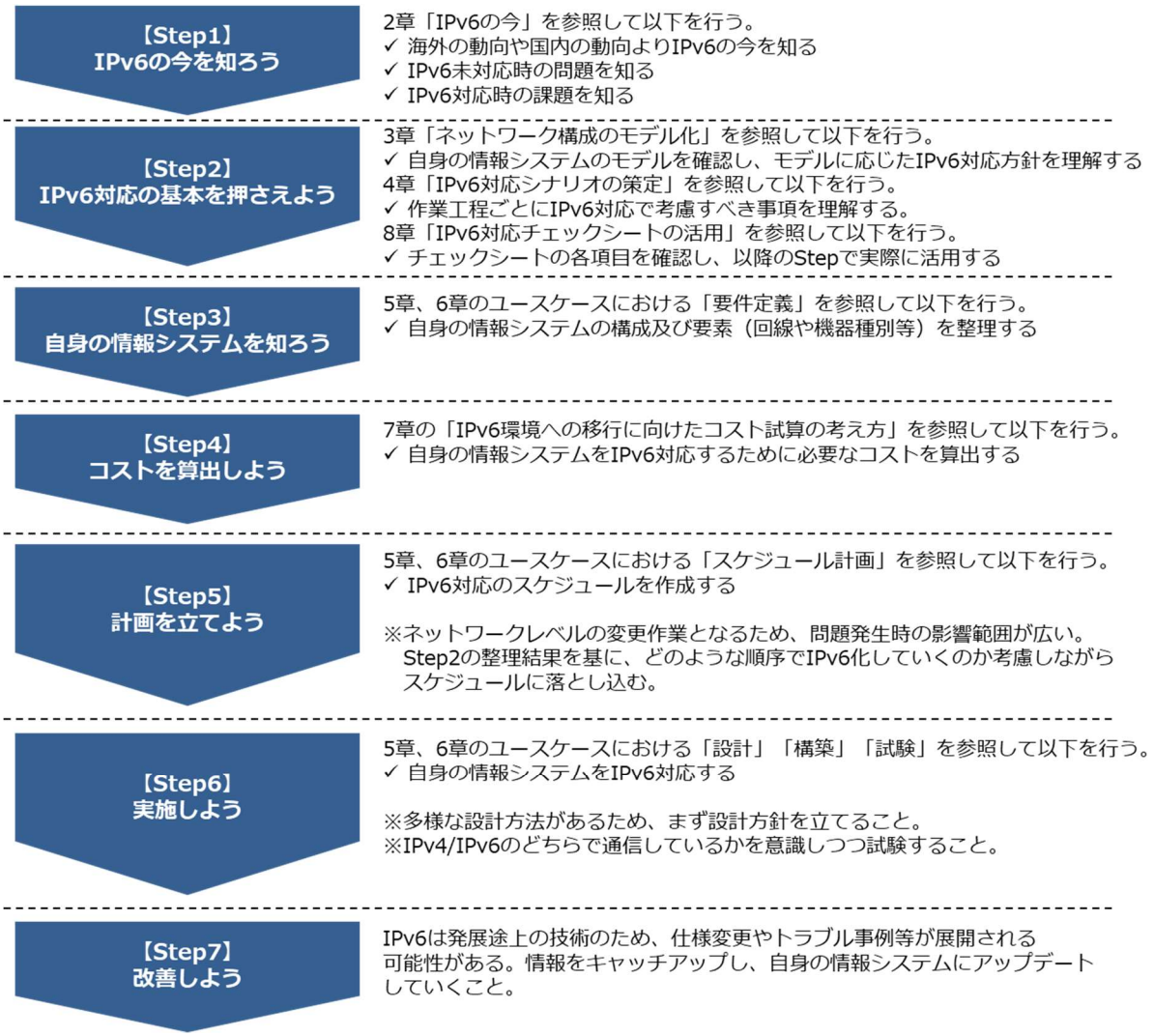


図 1.4-1 IPv6 対応の流れ

2　IPv6 の今

インターネットの飛躍的な発展とグローバルな普及は、世界的な IPv4 アドレスの枯渇という事態を招いた。2019 年 11 月に欧州地域の IP アドレスを管理している RIPE NCC は、最後となる IPv4 アドレスブロックの割り振りを行い、IPv4 アドレスを使いきったことを発表した 。しかし、IPv4 アドレスの枯渇は、新規 IPv4 アドレスを割り振ることができなくなっただけで、インターネットを利用できなくなるというわけではない。そのため、IPv6 対応の必要性を感じにくく、コンテンツ側の IPv6 対応が進まないと言われている。IPv6 の今を海外の動向と国内の動向に分けて以下に示す。

2.1　海外の動向

IPv6 普及率の高い諸外国において、政府指針が公開されている国の動向、Google および Apple における IPv6 に関するトピックについて記載する。また、IETF[1]が定義した IPv4 インターネットとの接続サービスの提供についても記載する。

(1) アメリカの動向

2003 年に国防総省が購入機器の IPv6 対応を義務付けた。2008 年には、国立標準技術研究所（NIST）が政府調達仕様で IPv6 対応を必須化した。2010 年には、連邦政府 CIO 発行の覚書により、2012 年度末までに外部向けシステム、2014 年度末までに内部システムの IPv6 対応を義務付けた。2020 年 3 月 2 日には、2025 年のおわりまでに、アメリカ政府のネットワークやサービスの最低 80%を IPv6 シングルスタックにする目標を公表した[2]。

(2) インドの動向

2010 年に「National IPv6 Deployment Roadmap ver 1.0」、2013 年には「National IPv6 Deployment Roadmap ver II」を公表した。その中で、2017 年度末までにすべての政府組織は IPv6 に完全移行する目標を策定した。2021 年 2 月に「National IPv6 Deployment Roadmap ver II」に対するリビジョンが行われ、政府組織は 2022 年 6 月 30 日に IPv6 移行を完了すべきであるとされた。政府目標のほかに、2013 年 6 月以降にインターネット接続する LTE ユーザは IPv6 対応すること、2014 年以降新たにインターネット接続するすべての企業および個人回線ユーザは IPv6 対応すること、2014 年 1 月以降に新たに利用が始まるすべての.in ドメイン[3]は IPv6 対応すること、2014 年 6 月以降に新たに提供されるすべてのコンテンツは IPv6 対応することも目標として策定している。

---

[1] The Internet Engineering Task Force

[2] https://www.federalregister.gov/documents/2020/03/02/2020-04202/request-for-comments-on-updated-guidance-for-completing-the-transition-to-the-next-generation

[3] 南アジアのインドに割り当てられた ccTLD（国別トップレベルドメイン）である。

上記リビジョンでは、2022 年 12 月 31 日までにサービスプロバイダによって現在提供されている CPE のうち IPv6 対応されていないものをリプレースすること、2020 年 12 月から有線によって提供される回線サービスを IPv6 対応することを目標としている。モバイルデバイス等に関しては、すべての機器が IPv6 対応済みであることが記述されている。コンテンツプロバイダ、データセンタ、クラウドコンピューティングに関しては、市場の自由競争によるとしている[4]。

(3) フランスの動向

2011 年に産業・エネルギー・デジタル経済省は、2015 年までに政府システムの IPv6 対応を完了し、2020 年までに民間企業の IPv6 利用を一般化する目標を設定した。2016 年に情報通信・郵政規制庁（ARCEP）が IPv6 対応状況の点検に関する最終報告書を公表し、今後の対応の方策の 1 つとして、政府自身が IPv6 対応を進め、事例を示すことを提言している。2016 年に、デジタル国家のための法律において、2018 年より、政府情報システムを構成する機器について、IPv6 対応機器へのマイグレーション促進を提唱している。他方で、2020 年の情報通信・郵政規制庁による報告書では、IPv6 対応が進んでいない分野として、モバイルオペレータ、企業等の組織内部の情報システム、PC やモバイルデバイスを除くネットワーク接続機器が指摘されている。また、メールや WEB ホスティングの IPv6 対応も進んでいないことが指摘されている。

(4) Google の統計情報

Google は、同社サービスに対する IPv6 での接続に関する統計情報を公開している 。そこで公開されている情報は、実際に同社サービスに対して IPv6 で通信が行われた割合である。この情報から、各国におけるおおよその IPv6 普及率を推測することができる。Google の統計情報によると、図 2.1-1 に示すとおり、IPv6 での接続は徐々に増加している。2022 年 3 月 12 日時点で世界全体での IPv6 普及率は約 35%、日本の普及率は約 45.27%であり、2021 年 3 月時点(約 38%)と比べると、約 7%増加し、世界的に見ても普及が進んでいる。世界全体で最も IPv6 普及率が高いのは、インドで約 65%である。IPv6 普及率が高い国を図 2.1-2 に示す。IPv6 普及率が増加する一方で、10%以下の国も非常に多く、IPv6 普及率は国ごとに大きな差があると言える。

[4] https://dot.gov.in/ipv6-transition

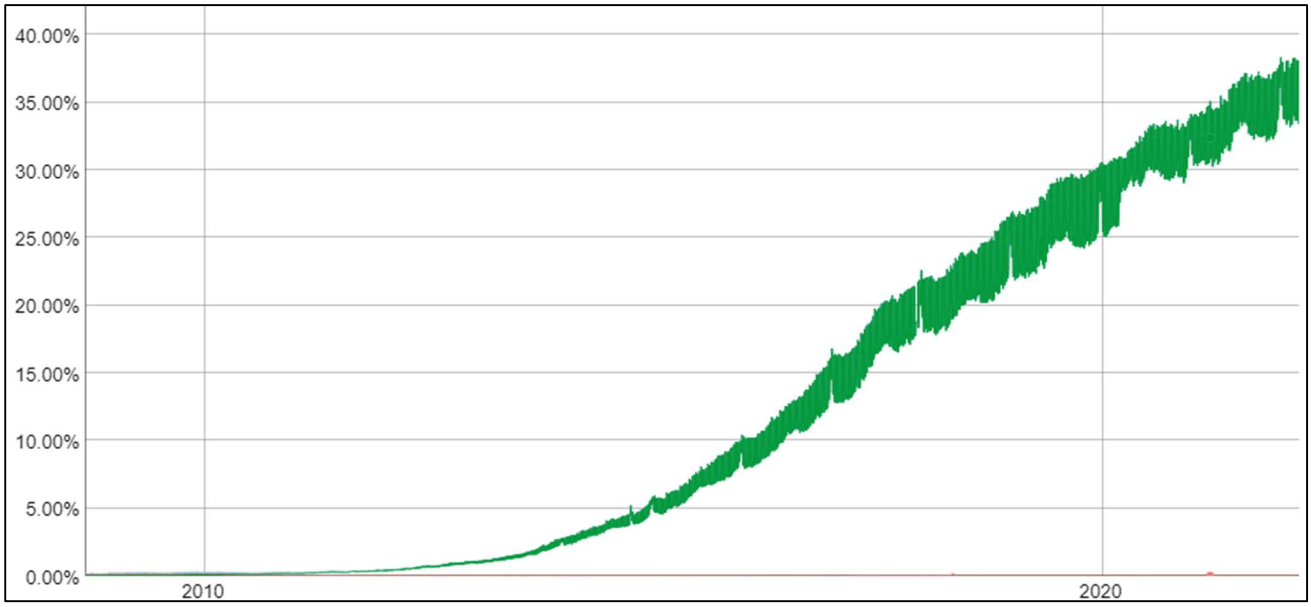


図 2.1-1 世界全体の IPv6 普及率
（「Google 統計情報」より引用）

国	普及率（%）
インド	64.73
マレーシア	56.85
サウジアラビア	55.90
ベルギー	55.54
ドイツ	55.49
フランス	53.64
ギリシャ	51.22
ベトナム	50.72
台湾	49.93
アメリカ	45.88
日本	45.27

図 2.1-2 IPv6 普及率が高い国
（「Google 統計情報」を参考に作成）

(5) Apple iOS の IPv6 必須化

2016 年 6 月から、Apple による iOS アプリの審査基準として IPv4 に依存するコードの禁止が追加された。IPv6 のみのシングルスタック環境で正しく動作することが求められるようになり、IPv6 対応が iOS アプリの義務となっている。また、Apple の iOS アプリ開発者は、IPv6 対応を行うとともに、NAT64 と DNS64 環境[5]でもアプリが正しく動作することを求められている。Apple のサイトでは、NAT64 と DNS64 は OS X 10.11 から標準搭載されるようになっているため、Mac を使って iOS アプリの動作確認をすることを推奨している[6]。

(6) IPv4 as a Service の必要性

IPv4 と IPv6 のデュアルスタック環境運用は、プラットフォーム提供者だけでなくコンテンツ提供者の運用コストも上昇する。しかし、2020 年現在、IPv4 インターネット上のコンテンツが数多くあるため、IPv6 シングルスタックの実現はまだ先になりそうである。そこで運用コスト上昇を防ぐため、提供者が構築する基幹ネットワークを IPv6 シングルスタックにしつつ、エンドユーザに対しては IPv4 インターネットからの接続性を実現する手法が提案されている。IETF では、SaaS、IaaS、PaaS のように、IPv4 との接続をサービスとして提供することを IPv4 as a Service と定義している。2019 年 5 月に、IPv4 as a Service を提供する CE ルータが満たすべき機能を紹介した RFC8585 が発行されている。その中で、IPv4 as a Service を実現する IPv6 移行技術として、464XLAT、DS-Lite、lw4o6、MAP-E、MAP-T が紹介されている。

---

[5] エンドユーザのネットワークが IPv6 シングルスタックで、IPv4 インターネット上のコンテンツを利用できるようにする変換技術である。例えば、IPv6 シングルスタックのスマートフォンで、IPv4 インターネット上の Web サーバからコンテンツを取得できるようになる。

[6] https://developer.apple.com/library/content/documentation/NetworkingInternetWeb/Conceptual/NetworkingOverview/UnderstandingandPreparingfortheIPv6Transition/UnderstandingandPreparingfortheIPv6Transition.html

2.2　国内の動向

(1) モバイルキャリアの対応

IPv4 アドレスの中央在庫(IANA 在庫)が枯渇した当時に比べると、日本国内において IPv6 を提供しているインターネット接続サービスは増加している。2017 年度から、モバイルキャリアである、NTT ドコモ、KDDI、ソフトバンクは、スマートフォンの IPv6 対応を開始した。モバイルキャリアから 2018 年度以降に発売されるスマートフォン全機種が、原則 IPv6 対応となっている[7]。また、2022 年 2 月より、NTT ドコモより IPv6 シングルスタック方式によるサービス提供を開始している。

(2) 個人向け MVNO サービスにおける IPv6 普及率

IIJ[8]は 2012 年から個人向けの MVNO サービスで IPv6 の提供を行っていたが、IPv6 普及率は 3%程度に留まっていた。しかし、2017 年 9 月以降から普及率は増加し、同年 10 月には普及率が 25%に達した。これは iOS 11 が配信されたためと推測される。iOS 11 では契約中の MVNO が IPv6 提供していれば、利用者が何も設定しなくても IPv6 で通信を行うためである[9]。

(3) NTT NGN における IPv6 IPoE 普及率

NTT NGN[10]における IPv6 IPoE 普及率は、2019 年 12 月時点で約 56%であった。これは前年同月比 134%であり、急激に増加している。また、NTT NGN での IPv6 トラフィックも急激に増加しており、同時点における全トラフィックの約 49%が、IPv6 IPoE によるものであった[11]。2021 年 3 月には、フレッツ光ネクスト[12]の IPv6 普及率が 80%に到達している。iOS11 配信やスマートフォン全機種が IPv6 対応したことが大きな要因の一つと推測される。

---

[7] https://www.soumu.go.jp/main_content/000517037.pdf
[8] Internet Initiative Japan Inc
[9] https://www.itmedia.co.jp/mobile/articles/1801/08/news008_2.html
[10] Next Generation Network
[11] https://www.janog.gr.jp/meeting/janog45/application/files/8215/7950/7604/025_nttngn_02-yamaguchi.pdf
[12] https://www.v6pc.jp/jp/spread/ipv6spread_03.phtml

2.3　IPv6 未対応時の問題

IPv6 未対応時の問題として考えられる点を 2 つ示す。

(1) 品質低下

IPv6 対応を行っていないことによって通信品質が低下する可能性がある。その結果、安定したサービスを提供することができなくなる。IPv6 が IPv4 よりも通信品質が高いと言われる理由はいくつかある。

- IPv6 は Happy Eyeballs の仕様として優先されるため
- IPv6 は通信経路上のフラグメント化やチェックサム計算によるオーバヘッドがなくなるため
- IPv4 は飽和状態で回線が混雑しているため
- IPv4 は CGN（大規模 NAT）によるオーバヘッドがあるため

(2) 国際競争力の懸念

2.1(4)で述べたとおり、IPv6 普及率は国別で大きな差があり、その差が将来的に何らかの国際競争力における優位性に繋がる可能性がある。

現時点では IPv4 で問題なくインターネット上のコンテンツを利用できるため、IPv6 を導入するモチベーションは低いと言える。しかし、時間の経過と共に、IPv6 普及率は増加し、相関して IPv6 対応の必要性も増加する可能性が高い。IPv6 対応が喫緊の課題となる前に、先んじて IPv6 対応する意義は十分あると言える。

2.4　IPv6 対応時の課題

先んじて IPv6 対応する意義はあるが、課題もある。

(1) 企業等のメリットが見えにくい

将来的に IPv6 の必要性が高くなることが推測される。しかし、現時点で、企業等は IPv6 対応することによる直接的なメリットを見いだせないことから導入に積極的ではないと言える。更に、IPv4 と IPv6 の並行運用に伴うコスト増加[13]や、IPv6 に関連する障害が発生するリスク増加等の問題があることから、本格導入に向けた決断が難しい。

(2) IPv6 人材不足

RFC7381 では、IPv6 のデプロイにおける最大の脅威は、IPv6 に関する運用経験の不足であるとし、IPv6 に関連する教育が非常に大事であるとも指摘している。ヒアリング結果としても、IPv6 対応未検討の理由として IPv6 人材不足が多く挙げられていた。IPv4 と IPv6 は互換性がなく、まったく別のプロトコルのため、IPv6 の知識を新たに習得する必要がある。しかし、IPv4 環境では、IPv6 に関する知識や経験を得ることはできない。IPv6 環境が少ないため、IPv6 人材が不足しており、IPv6 人材が不足しているため、IPv6 環境を増やしにくいという鶏と卵の関係になっている。このまま IPv6 普及率が増加し、IPv6 対応が必須になった場合、IPv6 対応の経験がない、あるいは少ない人材が無理な IPv6 対応を行うことになる。結果、非効率な設計を行い、セキュリティホールを生み出してしまう等の問題が発生する。

(3) IPv6 セキュリティ情報不足

IPv6 セキュリティ情報の不足もある。これは、中小企業等の内部環境の IPv6 対応と相関する。中小企業等の内部環境を IPv6 対応しないと、IPv6 に特化したサイバー攻撃は（IPv4 と比較して）発生しにくい。サイバー攻撃者は、攻撃手法を流用する傾向があるため、攻撃対象の母数が増えない限り、IPv6 はターゲットになりにくく、脆弱性が発見されない。IPv6 のセキュリティについて、「IPv6 普及・高度化推進協議会 IPv6 対応セキュリティガイドライン 」が公表されているが、当該ガイドラインは、主に外部向けサービスの IPv6 対応を対象としており、企業 LAN のデュアルスタック化に関しては対象外としている。

(4) IPv6 対応が不十分な機器/サービスの存在

IPv6 対応を謳う機器やサービスであっても、限定的な対応となっており、実際に使うと正常に動作しないことがある。IPv6 の利用者が少なく、IPv6 通信による利用がされない状況では、不具合が含まれていても発見されない。本実証試験でも IPv6 通信で複合機や IoT 機器、外部サービス等が利用できないという事象が発生した。

---

[13] 通常運用だけでなく、システム修正変更時の試験コストも含む。従来の IPv4 環境における試験だけでなく、IPv6 環境における試験も必要になる。

3　ネットワーク構成のモデル化

本ガイドラインにてIPv6対応ユースケースを紹介するにあたり、ユースケースの包括的な概念として、モデルケースを示す。モデルケースは総務省令和元年度事業にて実施したヒアリング調査に基づき、整理したネットワーク構成モデルを採用する。3.1にてモデルケースを整理する際の観点を示す。また3.2にてモデルごとのIPv6対応プランを示し、3.3にてモデルケースの事例となるユースケースの概要を示す。

3.1　モデルケースの整理

総務省令和元年度事業にて中小企業、学術機関、地方公共団体のそれぞれ 2 団体に対して現在運用中の情報システム等の状況についてヒアリング調査を実施した。

図 3.1-1 に示すとおり、ヒアリング結果を基に、ネットワーク構成をモデル化した。モデル化する際の観点は「ネットワーク規模」「拠点間 VPN」「イントラネット内のエンドポイント管理」の 3 つとした。

(1) ネットワーク規模

総務省が公表する「IPv6 対応ガイドライン（企業編）[14]」では、「中小企業の場合は、コスト削減や業務の効率化のために、DMZ をはじめとした多くの機能を ASP やクラウドサービス上に構築することが想定される。」としている。その上で、典型的な大企業のシステムやネットワークのモデルとして、DMZ を有した企業内ネットワークを紹介している。今回のヒアリングは、中小企業、大学、地方自治体を対象としており、大企業は範疇外であるが、DMZ 有無をネットワーク規模の 1 つの観点として考える。内部に DMZ（メールサーバや DNS サーバ等）が有る団体を大規模、無い団体を中規模と定義する。また、中規模については、サブネット数が 10 未満か 10 以上かでさらなる分類を行う。

(2) 拠点間イントラネット（VPN）

拠点間イントラネット（VPN）がある場合、通常のインターネットの経路とは別にトンネル化した経路を設計・構築する必要がある。ルーティングに関わる箇所であり、IPv6 独自の設計・構築が必要となるため、拠点間イントラネット（VPN）の有無を 1 つの観点として考える。

(3) イントラネット内のエンドポイント管理

IPv6 アドレスは NAT を用いずエンドポイントごとにグローバルアドレスを保有する。従来の境界防御ではなく、エンドポイント管理が更に求められる[15]。そのため、エンドポイント管理の有無を 1 つの観点として考える。

---

[14] https://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/index.html

[15] ゼロトラストという概念が登場したように、IPv6 普及とは別で境界防御の限界は提起されている。

IPv4 NAT、ASP/クラウドサービス、ファイアウォールの利用有無も IPv6 対応に伴う影響を受ける箇所であるが、ヒアリング結果のとおり、すべての団体が利用しているため、共通項目とする。

<table>
<tr><th>観点 ＼ モデル</th><th>モデルA</th><th>モデルB</th><th>モデルC</th><th>モデルD</th><th>モデルE</th><th>モデルF</th><th>モデルG</th><th>モデルH</th><th>モデルI</th><th>モデルJ</th></tr>
<tr><td>共通</td><td colspan="10">IPv4 NATあり
ASP/クラウドサービスあり
ファイアウォールあり</td></tr>
<tr><td>内部にDMZ（メールサーバやDNSサーバ等）があるか</td><td colspan="2">ある
（大規模）</td><td colspan="8">ない
（中規模）</td></tr>
<tr><td>サブネット数はいくつか</td><td colspan="2">10以上</td><td colspan="4">10以上</td><td colspan="4">10未満</td></tr>
<tr><td>拠点間イントラネット（VPN）はあるか</td><td>ある</td><td>ない</td><td>ある</td><td>ある</td><td>ない</td><td>ない</td><td>ある</td><td>ある</td><td>ない</td><td>ない</td></tr>
<tr><td>イントラネット内のエンドポイント管理はしているか</td><td colspan="2">ある</td><td>ある</td><td>ない</td><td>ある</td><td>ない</td><td>ある</td><td>ない</td><td>ある</td><td>ない</td></tr>
</table>

図 3.1-1 ヒアリング結果を基にしたネットワーク構成モデル

3.2　モデルごとの IPv6 対応プラン

3.1 にて整理したモデルごとの IPv6 対応プランを以下に示す。対応プランの項目はモデル化する際の観点に基づき、「対応範囲」「セグメント設計」「拠点間 VPN」「エンドポイント管理」の 4 つとし、その中からモデルの特性に応じた対応項目を示す。

3.2.1 モデル A

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を有し、メールサーバや DNS サーバ等が稼働しており、セグメントが 10 以上に分割された大規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装し、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは DMZ を有するネットワーク構成のため、機器の IPv6 対応として WAN 機器と LAN 機器に加えて、DMZ 内の機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434[16]にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

(4) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

---

16 RFC6434「IPv6 Node Requirements」

3.2.2 モデル B

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を有し、メールサーバや DNS サーバ等が稼働しており、セグメントが 10 以上に分割された大規模な環境である。尚、拠点間イントラネットを持たない構成であり、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは DMZ を有するネットワーク構成のため、機器の IPv6 対応として WAN 機器と LAN 機器に加えて、DMZ 内の機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.3 モデル C

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装し、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434[17]にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

(4) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

---

17 RFC6434「IPv6 Node Requirements」

3.2.4 モデル D

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装しているが、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434 にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

3.2.5 モデル E

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。尚、拠点間イントラネットを持たない構成であるが、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.6 モデル F

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。尚、拠点間イントラネットを持たない構成であり、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

3.2.7 モデル G

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装し、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434 にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

(4) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.8 モデル H

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装しているが、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434 にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

3.2.9 モデル I

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。尚、拠点間イントラネットを持たない構成であるが、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.10　モデル J

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。尚、拠点間イントラネットを持たない構成であり、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

3.3　ユースケースとしてのモデル選定

3.1 で整理したネットワーク構成モデルの内、ユースケースとして「モデル G」および「モデル I」を選定した。モデルの選定理由および選定モデルとユースケースの概要を以下に示す。

3.3.1 モデル選定理由

ユースケースとしてのモデルを選定するにあたり、選定項目はモデル化する際の観点に基づき、「ネットワーク規模」「サブネット数」「拠点間 VPN」「エンドポイント管理」の 4 つとした。

(1) ネットワーク規模

中小企業庁の「日本の中小企業・小規模事業者施策について」[18]によると、全事業者数の 99.7%が中小企業であると報告されている。中小企業が全事業者数の 9 割を占めることから選定モデルのネットワーク規模として中規模なモデルを対象とした。

(2) サブネット数

中小企業庁の「日本の中小企業・小規模事業者施策について」によると、事業者数では製造業が 11%にとどまり、卸・小売、サービス業が約 65%を占めている。同庁の中小企業基本法[19]の定義によると、事業者数の 6 割以上を占める卸・小売、サービス業の従業員数は 100～50 名以下とされている。また、IPA[20]による中小企業における情報セキュリティ対策の実態調査[21]によると、中小企業におけるサーバの利用台数は平均で 3.7 台と報告されている。これらの従業員数やサーバの平均利用台数を収容することを鑑み、選定モデルのサブネット数として 10 未満のモデルを対象とした。

(3) 拠点間 VPN

拠点間 VPN は IPsec による接続を行う際にトンネルの設計等、IPv6 独自の設計が必要となるためユースケースの蓄積として有効と考え、拠点間 VPN の有無を選定基準とした。

(4) エンドポイント管理

IPv6 対応により、エンドポイントにグローバルで通信可能なアドレスが付与されることになるため、セキュリティとしてエンドポイント管理がより一層求められることを踏まえ、エンドポイント管理を実施しているモデルを対象とした。

---

18 https://www.chusho.meti.go.jp/soshiki/180404seisaku.pdf

19 https://www.chusho.meti.go.jp/soshiki/teigi.html

20 Information-technology Promotion Agency, Japan(独立行政法人情報処理推進機構) https://www.ipa.go.jp/index.html

21 https://www.ipa.go.jp/files/000058502.pdf

3.3.2 選定モデルとユースケースの概要

選定モデルとユースケースの概要を表 3.3-1 に示す。尚、本ガイドラインの対象読者の内、選定モデルに該当しないケースも想定されるが、ユースケースで紹介する IPv6 対応の流れや各作業工程におけるアウトプットイメージ等はその他のモデルに横展開可能であるため、参考とすることを推奨する。

表 3.3-1 選定モデルとユースケース概要

ネットワーク構成モデル	ユースケース	移行方式	IPv6 対応方針	拠点間 VPN
モデル G	中小企業 A	デュアルスタック	・ 既存回線＋IPv6 回線新設 ・ IPv6 対応 GW ルータを新設し、IPv6 実証環境を既存環境と併設した構成にて構築 ・ IPv6 による拠点間 VPN を実装	有
モデル I	中小企業 B	デュアルスタック	・ 既存回線の IPv6 デュアル対応 ・ 回線切り替えに伴い IPoE 対応 GW ルータを増設 ・ 既存機器の IPv6 対応を実施し、IPv6 実証環境を既存環境と共存させて構築	無
モデル G	中小企業 C	デュアルスタック	・ 既存回線の IPv6 デュアル対応 ・ 複数拠点に対して回線切り替えに伴い IPoE 対応 GW ルータを増設 ・ 既存機器の IPv6 対応を実施し、IPv6 実証環境を既存環境と共存させて構築 ・ IPv6 による複数拠点間 VPN を実装	有
モデル I	大学 A	デュアルスタック	・ 既存回線(SINET[22])の IPv6 デュアル対応 ・ 回線切り替えに伴い GW となるファイアウォールを IPv6 対応機器へ更新するとともに、既存機器の IPv6 対応を実施し、IPv6 実証環境を既存環境と共存させて構築	無

[22] Science Information NETwork (学術情報ネットワーク)
https://www.sinet.ad.jp/

4　IPv6 対応シナリオの策定

システム開発における開発手法としてウォーターフォール型やプロトタイプ型、アジャイル型等が用いられている。ネットワーク構築においては要件が確定してからの対応となるためウォーターフォール型となる。これらの開発手法に共通した作業規定のガイドラインとして、IPA より「共通フレーム」[23]が発行されている。共通フレームはシステムライフサイクルの各工程における作業項目や役割を包括的に規定した共通の枠組みであり、共通フレームを参照することにより、システム開発に関わる人々が”同じ言葉を話す”ことができることを目的としている。

共通フレームはシステム開発の標準的なプロセスとして世の中に浸透しているため、大学および中小企業においてもシステム構築を検討する際は共通フレームを参考にすることを推奨する。

IPv6 対応においても共通フレームの標準的なプロセスに基づくことで効率的な移行が可能と考える。IPv6 対応シナリオでは共通フレームで紹介されているシステムライフサイクルに基づき、「要件定義、スケジュール計画、設計、構築、試験、運用・保守」を作業工程として定義する。IPv6 対応における移行プロセスの概要を図 4-1 に示す。尚、本章では全てのモデルケースに共通する指針として IPv6 対応シナリオの各工程において考慮すべき事項を以下に示す。

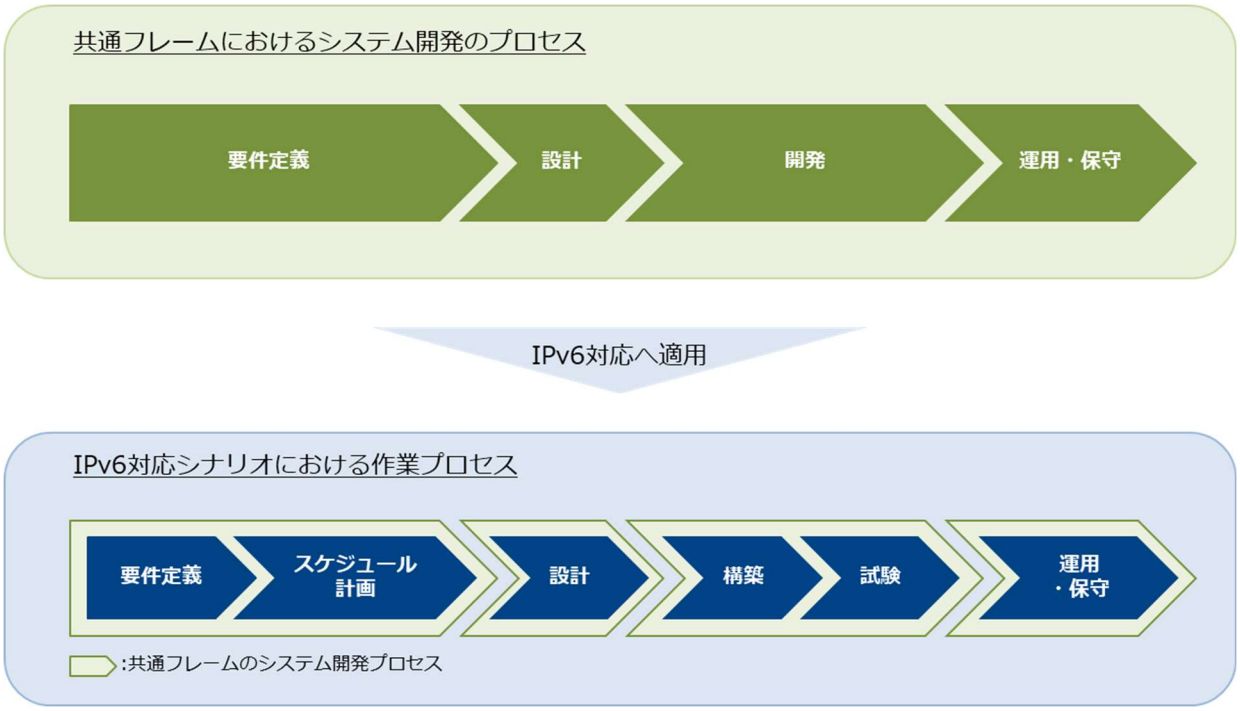


図 4-1 IPv6 対応における移行プロセスの概要

23 https://www.ipa.go.jp/sec/publish/tn12-006.html

4.1　要件定義

IPv6 対応するにあたり、要件定義の工程では 5 つのプロセスに分けて作業を行う。まず、1 つ目の「現状の把握」では既存環境で利用している機器やサービスを可視化し、現行システムを把握する。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る。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する。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い、IPv6 未対応の場合は機器やサービスの選定を行う。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する。

要件定義における 5 つのプロセスについて概要を図 4.1-1 に示す。

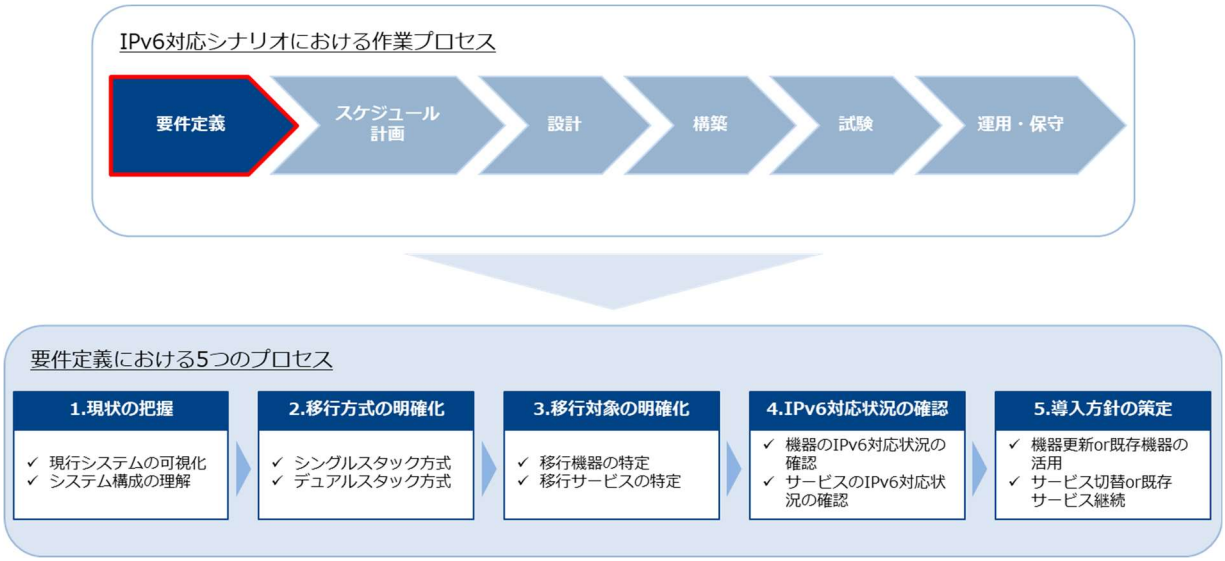


図 4.1-1 要件定義における 5 つのプロセス

（1）現状の把握

現行システムを正確に把握しない状態で IPv6 対応を進めることにより、本来 IPv6 対応すべき機器やサービスの対応を見落とす可能性がある。この見落としが業務影響に発展することになり得るため、現行システムの把握は IPv6 対応において重要な起点となる。現状利用している機器やサービスを把握するために可視化することを推奨する。可視化例としてシステム構成図や機器一覧表、利用サービス一覧表等が挙げられる。これらのドキュメントを必要に応じて作成および活用し、システム全体を俯瞰して理解することが重要である。

(2) 移行方式の明確化

IPv6 環境への移行方式はシングルスタックとデュアルスタックに分けられる。内部環境に合わせて、移行方式を明確にする必要があるが、IPv6 対応する環境が新規環境なのか既存環境なのかで移行の難易度が異なる。

新規環境の場合、根本的に IPv6 をネットワークの設計に取り込むことができるため、移行の難易度は下がる。そのため、新規環境ではまず IPv6 シングルスタックで移行できないか検討することが望ましい。

一方で、既存環境の場合、IPv6 未対応の機器やサービスが残存している可能性があるため、既存環境への影響を考慮し、デュアルスタックでの移行を検討することを推奨する。デュアルスタックでは IPv4 環境を維持しながら、IPv6 対応が可能となるため、IPv6 環境への移行がしやすくなるのが特徴である。

(3) 移行対象の明確化

(1)で整理した現行システムの内、IPv6 対応する機器やサービスを明確にする。機器の IPv6 対応においては有線機器/無線機器で同様に、GW ルータ、無線ルータ、L3 スイッチ、ファイアウォール、サーバ等の IP 通信を行う機器が対象となる。

サービスの IPv6 対応においては回線をはじめ、業務系や運用監視系の現行アプリケーションおよび外部サービスが対象となる。

情報システムは利便性を利用者へ提供するために機器やサービスが複合的に連携し構成されている。IPv6 対応はこのようなシステム基盤に対して適用するため、システム構成図等を活用し、システムの関連性を網羅的に把握した上で、移行対象を明確にすることが望ましい。

(4) IPv6 対応状況の確認

移行対象として定めた機器やサービスが IPv6 対応しているか確認を行う。IPv6 対応状況は事業者より公開されているカタログ等から確認することができるが、記載内容から明確に IPv6 対応していると判断できない場合はベンダやサポート窓口へ問い合わせを行うことを推奨する。問い合わせの結果、IPv6 に対応していない場合は内部環境に合わせて、機器やサービスの選定を行う必要がある。

(5) 導入方針の策定

機器やサービスの IPv6 対応状況に基づいて、IPv6 化に向けた導入方針を策定する。例えば、機器においては IPv6 未対応である場合は機器更新を行い、IPv6 対応の場合は既存機器の設定変更のみで対応するのが一例として挙げられる。サービスにおいては現行サービスが IPv6 対応である場合は切り替え不要とし、IPv6 未対応である場合はサービスを切り替えるか、もしくは事業者側で IPv6 対応の見通しが立っていることを確認できる場合は、切り替えを見送り、その時期まで現行サービスを継続する等の方針を策定することを推奨する。設計工程において移行計画の手戻りが発生しないよう移行対象の機器やサービスごとに導入方針を明確にすることが重要である。

4.2　スケジュール計画

IPv6 対応するにあたり、基本的なスケジュールイメージを図 4.2-1 に示すとともに、スケジュールを実現可能な計画にするために考慮すべきポイントを 3 点示す。

1 点目は、IPv6 対応する際は IPv6 独自で検討する事項が増えるため、各作業工程には余裕を持った作業期間を設定することを提案する。

2 点目は、回線や機器調達の際には対象ごとに調達に係るリードタイムを事前に確認し、スケジュールに沿って調達開始時期を調整することが重要である。

3 点目は、移行作業に伴う既存環境への業務影響を最小化できるよう、作業の実施タイミングを考慮することが重要である。

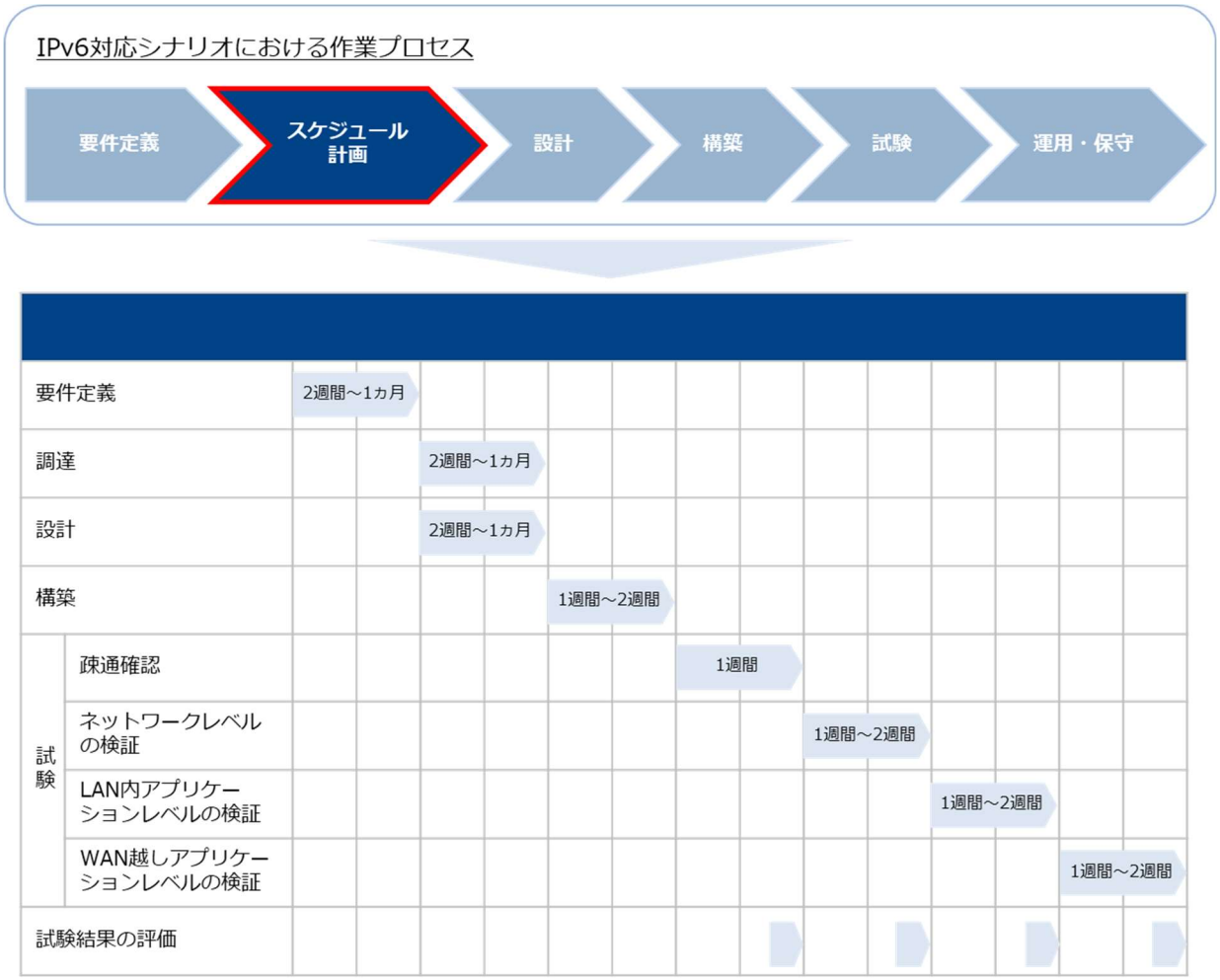


図 4.2-1 スケジュールイメージ

4.3　設計

情報システムにおける要求は大きく 2 つに分けられる。1 つは業務機能に対する要求を示す機能要求である。もう 1 つはシステム基盤に関する要求を示す非機能要求である。これらの要求を満たす情報システムを構築するためには、網羅的な観点で設計を行う必要がある。システム基盤はアプリケーションの土台であり、ハードウェア機器やネットワーク機器、OS やミドルウェア等で構成されている。IPv6 はシステム基盤における通信に関わるため非機能要求の要素に当てはまる。非機能要求は機能要求と比較し、不透明であるため、イメージし難い面があるため、システム基盤に関する非機能要求を明確化し、情報システムに関わる人々が共通認識を持つことで安定したサービスを提供できるようにすることを目的とし、IPA より「非機能要求グレード」[24]が公開されている。

IPv6 対応においても非機能要求グレードで定められている 6 大項目に基づくことで、網羅的な観点での設計が可能と考える。この 6 大項目と IPv6 対応の設計項目との関連を図 4.3-1 に示す。IPv6 の設計事項において考慮すべきポイントを以下に示す。

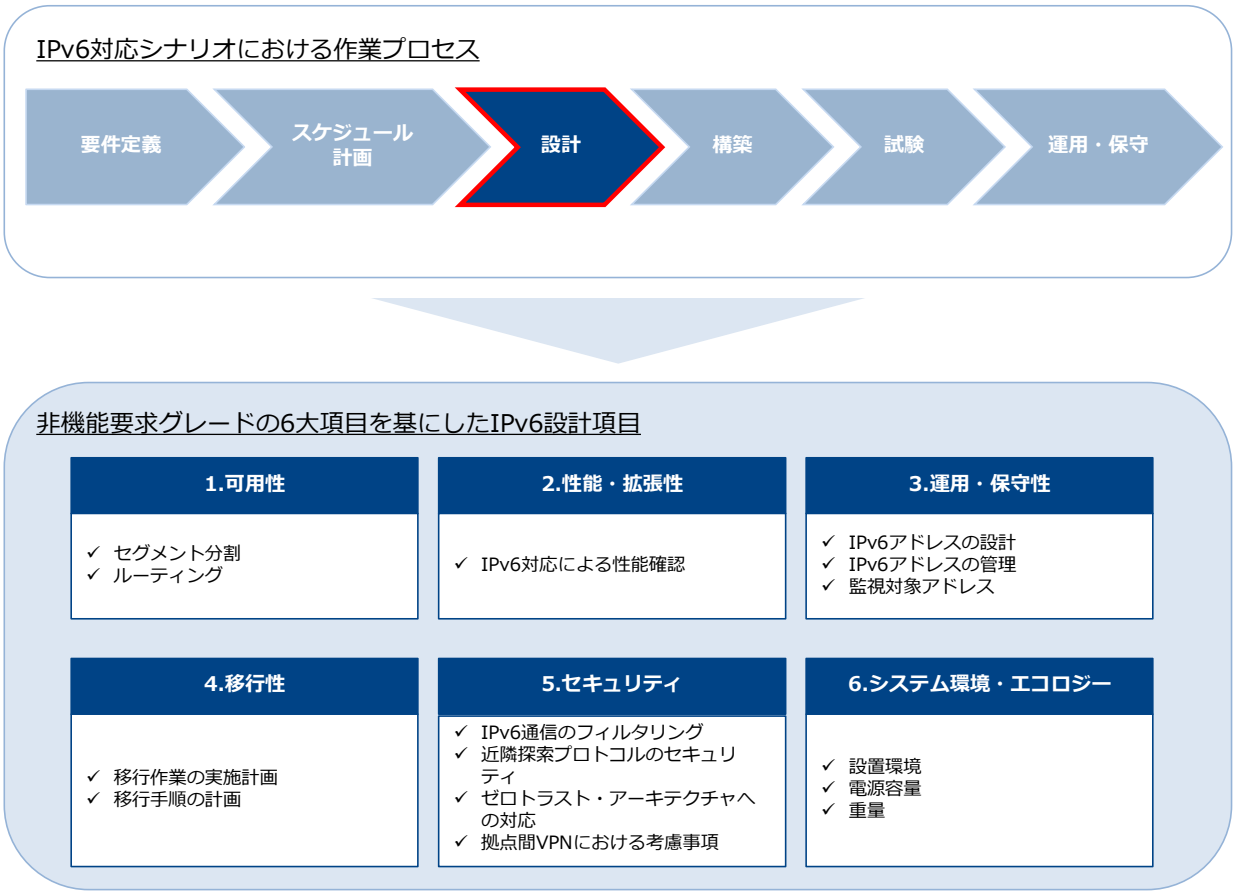


図 4.3-1 非機能要求グレードにおける 6 大項目と IPv6 設計項目との関連

[24] https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html

(1) 可用性

① セグメント分割

IPv6 はアドレス空間が広大であるため、1 つのセグメントで必要なアドレス数を十分に確保することが可能であるが、組織の通信要件に柔軟に対応していくためには IPv4 と同様に用途ごとにセグメントを分割し、管理することが望ましい。

② ルーティング

既存環境のルーティング方式に基づき、IPv6 環境におけるルーティング方式を静的または動的ルーティングとするか方針を策定する。動的ルーティングを行う際は IPv6 に対応したルーティングプロトコルを選定し、経路制御に関するパラメータを設計する必要がある。また、端末のデフォルトゲートウェイについてはルータの RA(Router Advertisement)による自動設定を活用することで、効率的なネットワーク設定が可能となるため、端末のアドレス設定を簡略化したい場合はルータ側で RA を有効にすることを推奨する。

(2) 性能・拡張性

① IPv6 対応による性能確認

IPv6 対応をすることにより、対応前よりも性能が劣化することなく、動作可能か確認する必要がある。IPv6 対応前後で性能比較ができるよう、既存環境にて性能を測定し、測定結果に基づいて IPv6 対応後の性能目標値を設定することを推奨する。

(3) 運用・保守性

① リンクローカルアドレスの設計

IPv6 対応機器にはリンクごとにリンクローカルアドレスが付与される。リンクローカルアドレスは EUI-64 形式により自動的に生成されるため、特別な設定は不要であるが、手動で設定することも可能である。例えば、リンクローカルアドレスはルーティング時のネクストホップとして利用されるため、デフォルトゲートウェイとなるルータ等ではリンクローカルアドレスを明示的に指定することでルーティング情報の把握がしやすくなる。したがって、ネットワーク機器ではリンクローカルアドレスを手動で設定することを推奨する。

② GUA（Global Unicast Address）[25]の設計

IPv6 ではインターネット接続の際に GUA が利用される。GUA を設定するにあたり、RFC3633[26]にて公開されている DHCPv6-PD(Prefix Delegation)[27]を利用することが可能である。プロバイダより取得したプレフィックスを LAN 側へ再配布することで LAN 機器のプレフィックス設定を効率化できる。インターフェース ID については EUI-64 形式で自動的に生成されるが、運用管理の面からネットワーク機器やサーバ等の基盤となる機器については手動で設定することを推奨する。

③ アドレス管理

IPv6 アドレスはアドレス空間が広大であるため、ホスト数を意識せずアドレスの割り当てが可能であるが、計画的に割り振らなければ、管理が行き届かなくなるため、IPv4 と同様に IP アドレス管理表を作成する等の管理は必要である。また、IPv6 アドレスは 1 つのインターフェースに複数のアドレスを持つことができるが、通信を行う際に送信元アドレスの選択誤りにより、フィルタリング等で通信できない問題が発生する可能性がある。したがって、利用する IPv6 アドレスは必要な分だけに絞ることが望ましい。

④ 監視対象アドレス

IPv6 でネットワーク機器やサーバ等の基盤となる機器の監視を行う際に監視対象の IPv6 アドレスは固定であることが望ましい。DHCPv6-PD にて設定した GUA を監視対象として登録した場合、プロバイダ側でプレフィックスが変更されると、LAN 側へ再配布するプレフィックスに変更が生じ、対象機器の GUA が変更されることで監視に支障をきたすことが想定される。したがって、IPv6 アドレスの固定化について、1 つのプレフィックスで運用可能なネットワーク構成においては、運用監視対象機器のリンクローカルアドレスを監視対象とし、複数のプレフィックスで運用するネットワーク構成においては、RFC4193[28]にて公開されている ULA（Unique Local Unicast Address）[29]を監視対象とする運用が有効である。

---

25 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。

26 RFC3633「IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6」

27 クライアントが RS 通信（プレフィックスとデフォルトゲートウェイ要求）を行い、ルータが RA 通信（プレフィックスとデフォルトゲートウェイ返答）を行う方式である。ルータではなく、ISP 側が RA 通信を行う RA プロキシという方式もある。ISP 種別によって採用方式が異なるため、ISP 事業者窓口に問い合わせを行うこと。

28 RFC4193「Unique Local IPv6 Unicast Addresses」

29 グローバルスコープであるが、サイト内での利用を想定されたアドレス。インターネットに公告されることは推奨されていない。

(4) 移行性

① 移行作業の実施計画

IPv6 環境へ移行する際に必要な作業項目を整理し、作業ステップを明確にした上で、移行作業のスケジュールを計画する必要がある。そして計画した作業スケジュールに基づいて、作業日時を調整する際は既存環境への影響を最小限にできるよう作業の実施タイミングを十分に考慮する必要がある。また移行作業においてはトラブルにより切り戻しを行うことも想定されるため、その際に冷静な対処ができるよう事前に切り戻しに要する作業時間を見込んだスケジュールを計画することが重要である。

② 移行手順の計画

移行作業を確実に行うために作業手順書やチェックリストを作成することが重要である。作業で使用するツールや実行するコマンド、想定される作業結果等を作業手順書やチェックリストへ明記することで作業品質が担保される。また、移行作業においてトラブルによる切り戻しを想定し、事前に切り戻し手順を作業手順書へ反映することを推奨する。

(5) セキュリティ

① IPv6 通信におけるフィルタリングの考慮事項

IPv4 ではインターネット接続の際に限られたグローバルアドレスを有効活用するために NAT を利用することが一般的である。NAT の特性上、アドレス変換により LAN 内の IP アドレスを秘匿することができるため、結果的に外部から内部への通信制限が可能となる点でセキュリティの利点として挙げられている。IPv6 ではグローバルスコープで通信可能なアドレスを広大に利用することができるため、インターネットを跨いだ End-To-End の通信が重視されているが、外部より内部へ不正に接続されないよう必要の無い通信に関してはファイアウォール等でフィルタリングを行い、IPv4 と同等のセキュリティレベルを確保する必要がある。尚、フィルタリングについて IPv4 環境においては DoS 攻撃の対策として外部からの ICMP パケットをフィルタしているケースがあるが、IPv6 環境では ICMPv6 でパス MTU 探索等、通信確立に不可欠なメッセージをやりとりしているため、IPv4 と同様に ICMPv6 を全てフィルタすることにより、通信に弊害が生じるため注意が必要である。フィルタすべきでない ICMPv6 メッセージについては RFC4890[30]にて紹介されているため、フィルタリングルール設計の際に参照することを推奨する。

30 RFC4890「Recommendations for Filtering ICMPv6 Messages in Firewalls」

② 近隣探索プロトコル(NDP：Neighbor Discovery Protocol)のセキュリティ

IPv4 と IPv6 の大きな違いとして、NDP の存在がある。IPv6 では NDP の機能である RA メッセージにより、端末のネットワーク設定を簡略化する仕組みがとられているが、RFC3756[31]で公開されている通り、RA にはデフォルトルータの情報が含まれているため、悪意ある者が組織内のネットワークに不正な RA を送信し、デフォルトルータになりすますことで通信内容が傍受されるリスクがある。また、故意ではなく設定誤りにより不正な RA を流してしまうことで端末に意図しないデフォルトルータが設定されることも考えられる。不正 RA の対策として RFC6105[32]で紹介されている RA Guard や RFC3971 [33]の SEND(SEcure Neighbor Discovery)等が存在するが、必ずしもこれらの機能がスイッチに実装されているわけではないため、広く普及していないのが現状である。ネットワークの運用形態にもよるが不正接続を防止するために、IPv6 通信が開始される前の段階での対策として、未使用ポートの無効化や認証 VLAN による 802.1x 認証等を検討することも有効である。

③ IPv6 によるゼロトラスト・アーキテクチャへの対応

従来のセキュリティ対策では、ネットワークを組織の外部・内部（例：インターネットと社内ローカルネットワーク）に分離して考えるのが一般的であった。守るべき情報資産はネットワーク境界内部にあり、一方で脅威は境界外部にあることを前提とした上で、セキュリティ対策はファイアウォールやプロキシなど「境界防御」を行うゲートウェイセキュリティが中心であった。しかし昨今、クラウドサービスの利活用やテレワークの普及等により、情報資産の格納場所やアクセス元が境界内部に限らないことから、これまでの境界が曖昧になり、境界防御の考え方では情報資産の保護が困難となっている。そのため、境界の外部・内部を問わず、信頼しないことを前提に、情報システムに対して適切にアクセスコントロールすることを目指す「ゼロトラスト・アーキテクチャ」[34]に基づいたセキュリティの考え方が求められている。

---

31 RFC3756「IPv6 Neighbor Discovery (ND) Trust Models and Threats」

32 RFC6105「IPv6 Router Advertisement Guard」

33 RFC3971「SEcure Neighbor Discovery (SEND)」

34 アメリカ国立標準技術研究所(NIST: National Institute of Standards and Technology)より、「ゼロトラスト・アーキテクチャ」について策定・公開されている。
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/assets/pdf/zero-trust-architecture-jp.pdf

「ゼロトラスト・アーキテクチャ」の代表的な技術要素として、以下が挙げられる。

- リソースへの認証・認可　　:IDaaS(Identity as a Service)[35]
- ネットワークのアクセス制御　:SASE(Secure Access Service Edge)[36]
- エンドポイントの制御　　:EDR(Endpoint Detection & Response)[37]

  など

「ゼロトラスト・アーキテクチャ」を検討する際には、これらの技術要素に該当する機器/サービスが IPv6 で実装可能かベンダ等へ確認することを推奨する。

④ 拠点間 VPN における考慮事項

IPv4 では拠点間接続をインターネット VPN で行う場合、論理的な VPN トンネルを構築することで、拠点内のプライベートアドレスにて通信可能である。一方で、RFC9099[38]に記載の通り、IPv6 ではアドレススコープがグローバルであるため、VPN が利用できない場合においても、インターネット経由で拠点間接続が行える可能性がある。そのため、暗号化されていないトラヒックがインターネットより拠点内へ流入することが考えられるため、拠点内で割り当てるプレフィックスをもとに、通信すべき送信元アドレス、宛先アドレスにてフィルタリングすることを推奨する。

35 クラウド経由で ID 認証ならび ID パスワード管理、シングルサインオン（SSO)、アクセス制御などを提供するサービス。

36 これまで個々に存在していたセキュリティサービスとネットワークサービスを一体にしたネットワークセキュリティの概念。

37 ユーザが利用するパソコンやサーバ（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するソリューション。

38 RFC9099「Operational Security Considerations for IPv6 Networks」

(6) システム環境・エコロジー

① 設置環境

IPv6 対応により機器を設置する際は放熱等を考慮し、できる限り機器間にスペースを確保できるよう収容設計することが望ましい。

② 電源容量

搭載予定のラックで提供される最大電源容量と余剰容量を確認し、IPv6 対応で機器を設置することで電源容量の上限を超過しないか確認する必要がある。もし上限を超過する場合は、別途電源工事の追加が発生する。

③ 重量

設置環境の耐荷重の上限を確認し、IPv6 対応で機器を設置することで耐荷重の上限を超過しないか確認する必要がある。もし上限を超過する場合は別のラックに搭載する等、収容設計を見直す必要がある。

4.4　構築

IPv6 対応するにあたり、まず(1)にて構築における基本的な作業工程を示す。つぎに(2)にて構築における IPv6 特有の留意点を示す。

(1) 構築における基本作業

構築作業の基本的な工程は IPv4 と同様となる。構築における作業工程のイメージを図 4.4-1 に示す。

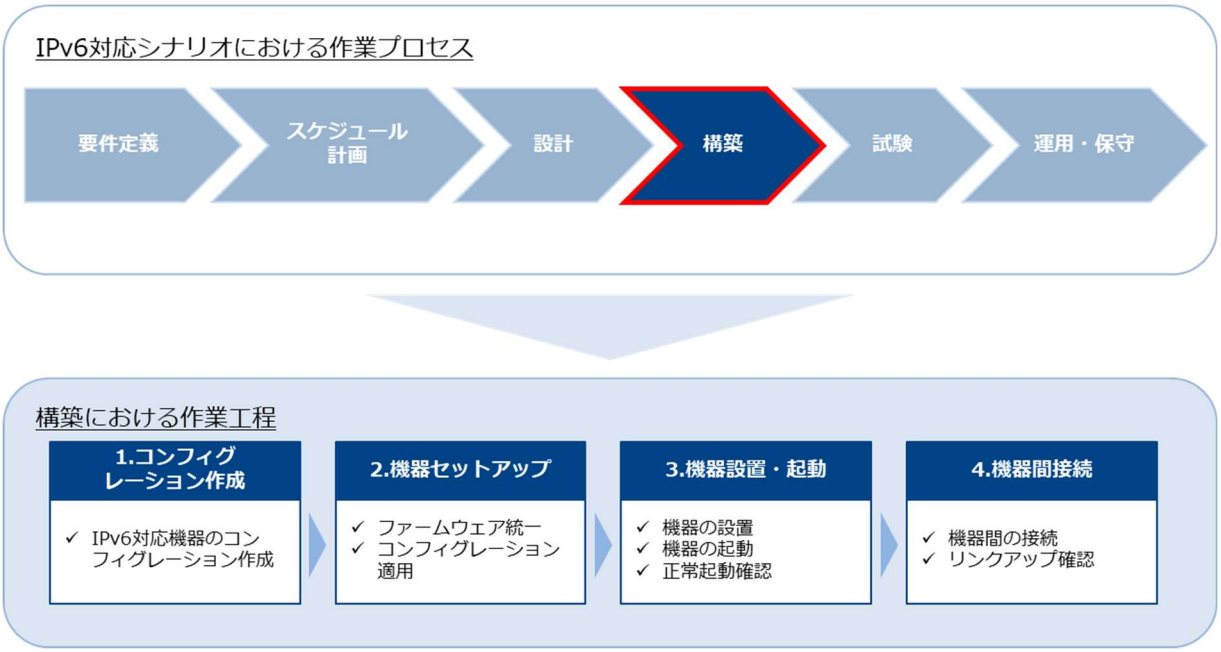


図 4.4-1 構築作業の工程イメージ

① コンフィグレーション作成

設計フェーズにて策定したパラメータ情報を基に、IPv6 対応機器のコンフィグレーションを作成する必要があるが、IPv6 アドレスは IPv4 アドレスより全体的に長い表記となるため、手入力ではアドレスの間違いが生じやすい。パラメータシートの表記をコピー&ペーストする等、できる限り手入力を避けることを推奨する。

② 機器セットアップ

セットアップにあたり、ファームウェアのバージョンが搭載予定のバージョンと異なると設定に差分が発生することがあるため、最初にファームウェアのバージョンを合わせることが重要である。つぎに作成したコンフィグレーションを対象の IPv6 対応機器へ投入し、設定が正常に反映されたか確認する。尚、設定保存の未実施により設定が初期化された場合に備えて、セットアップ後の設定ファイルはバックアップすることを推奨する。

③ 機器設置・起動

配線工事や電源工事の完了後に機器をラック等へ設置し、起動確認を行う。起動時には正常性確認としてハードウェア(パワーサプライ,ファン、モジュール等)の異常がないか確認することが重要である。

④ 機器間接続

機器の正常起動を確認後、機器間をケーブルで接続し、正常にリンクアップしているか確認する。また、接続後に CPU が継続して上昇していないか確認することも重要である。

(2) 構築における IPv6 特有の留意点

IPv6 対応するにあたり、構築において人為的な要因によるトラブルを最小限に抑えるために留意すべきポイントを 3 つ示す。

1 つ目は、IPv6 アドレスは表記が長く、省略表記が混在することからルーティング設定においてプレフィックスの設定誤りが発生しやすいため注意が必要である。

2 つ目は、IPv4 と異なり、IPv6 アドレスは hosts ファイル等において特殊な記載を行うため、IP アドレスの記載誤りが発生しやすいため注意が必要である。

3 つ目は、ネットワーク機器のコンフィグレーションが IPv4 と IPv6 で類似しているため、誤った設定とならないようプロトコルの違いを意識して設定することが重要である。以下に特定ベンダにおけるルータの設定例を示す。

IP アドレスの設定例 ※斜体は可変部を示す

(IPv4) ip *interface* address *ip_address/mask*

(IPv6) ipv6 *interface* address *ipv6_address/prefix_len*

4.5　試験

IPv6 対応するにあたり、構築後の試験について考慮すべき事項を以下に示す。試験は最初にネットワーク層に関する試験(疎通試験/一般業務)を行い、ネットワーク層に問題がないことを確認した後にアプリケーション層に関する試験(業務アプリケーション/外部システム・商用サービス等)を行うことで、問題発生時の切り分けが容易となるため、段階的に進めることを推奨する。また IPv6 環境へ移行後の運用・保守を想定し、運用監視システムに関する試験を実施することも必要である。試験の実施順序に関するイメージを図 4.5-1 に示す。

尚、デュアルスタック環境ではIPv4とIPv6が混在するため、どちらのプロトコルで通信しているかを意識して確認することが重要である。

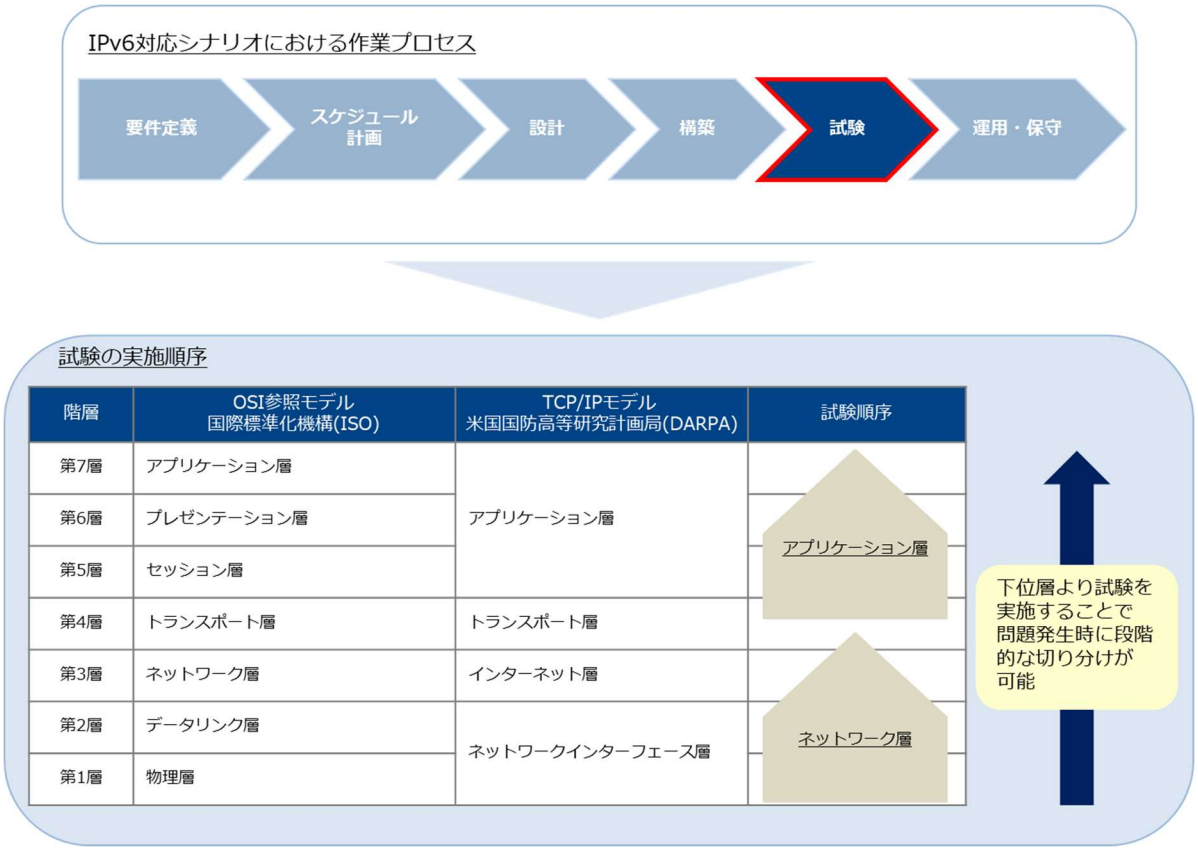


図 4.5-1 試験の実施順序

(1) ネットワーク層における試験

ネットワーク層における試験では、まず基本的な試験項目として各機器に対して疎通試験を実施する。また Traceroute 等を実行し、通信フローが設計通りとなっているか確認することも重要である。つぎに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、印刷やスキャン等の OA 機器利用といった通常業務が IPv6 通信で正常に行えるか検証することを目的としている。機器のカタログ等で IPv6 対応と記載があったとしても、実際には IPv6 未対応の場合があるため、動作確認することが重要である。

(2) アプリケーション層における試験

アプリケーション層における試験では、定常的に利用している業務アプリケーションや外部システム・商用サービス等が IPv6 通信で正常に利用可能か検証することを目的としている。検証項目については業務で利用する機能をベースに策定することが望ましい。アプリケーションやサービスの中には、一部の機能が IPv6 対応していない場合があるため、業務で利用する機能が IPv6 対応しているか実際に動作確認することが重要である。

(3) 運用監視システムにおける試験

運用監視システムにおける試験では、時刻同期や監視、バックアップ等の試験を想定する。時刻同期の試験では IPv6 通信で各機器が NTP サーバと正常に時刻同期できるか検証することを目的とし、監視の試験では監視ツールにて機器やサービスの稼働状況を IPv4 と同等に監視できるか検証することを目的としている。バックアップの試験では IPv6 通信でデータのバックアップが正常に行われるか検証することを目的としている。尚、これらは一例のため、検証項目については組織の運用監視システムにて定常的に利用する機能に基づいて、策定することが望ましい。

4.6　運用・保守

IPv6 対応後の運用・保守において考慮すべき事項を以下に示すとともに、その全体像を図 4.6-1 に示す。

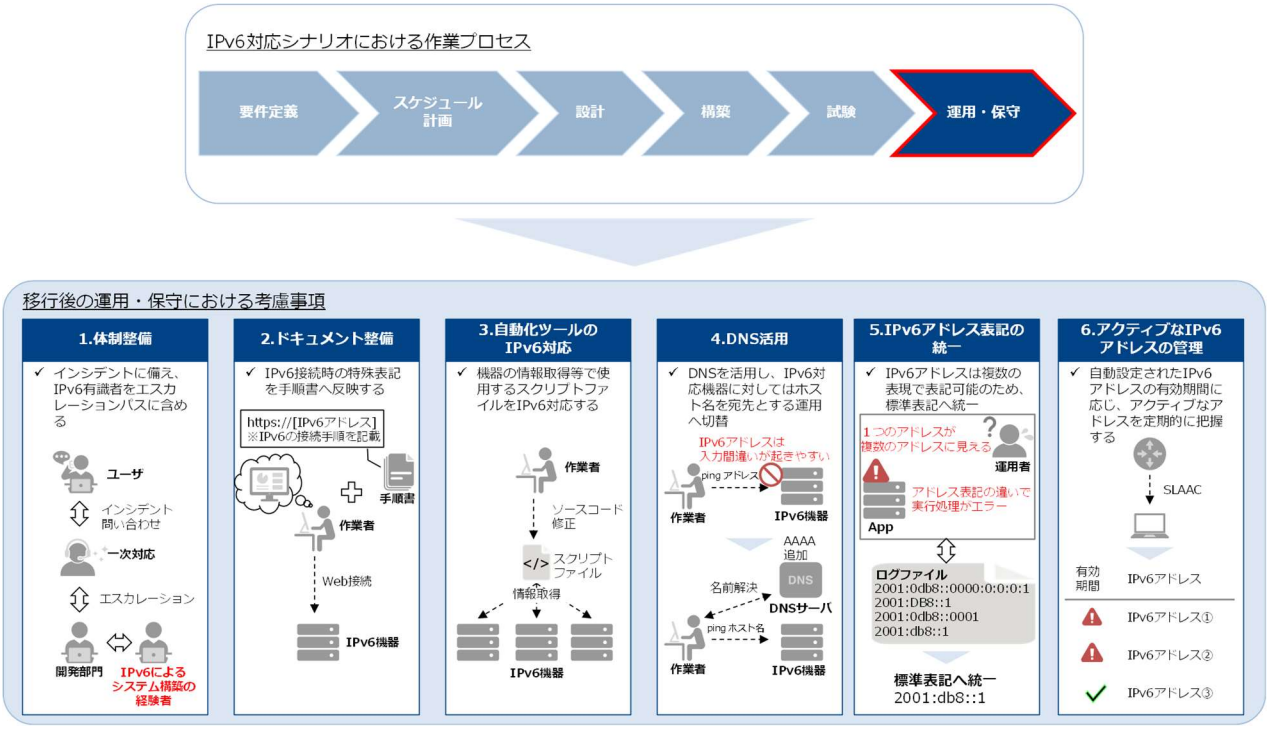


図 4.6-1 IPv6 対応後の運用・保守において考慮すべき事項

(1) 運用・保守の体制整備

機器やサービスのインシデント発生時において、適切に対応ができるよう IPv6 を活用したシステム構築の経験を有する者をエスカレーションパスに含める等、体制を整備することが重要である。

(2) ドキュメント整備

運用作業時に対象機器の管理画面へ WEB 接続するケースがあるが、IPv6 では RFC2732[39]で紹介されているとおり、URL に接続先を指定する際は IPv6 アドレス全体を角括弧[]で囲う表記となる。また、ファイルサーバへエクスプローラにて接続する際の UNC(Universal Naming Convention)表記においては IPv6 アドレスの「:」を「-」に置き換え、末尾に「.ipv6-literal.net」を付記する表記となる。接続の表記は作業時に影響するため、IPv6 対応によって変更となる点は運用作業手順書や保守マニュアルに反映することが重要である。

[39] RFC2732「Format for Literal IPv6 Addresses in URL's」

表記例(URL 接続)
http://[2010:836B:4179::836B:4179]:8080

表記例(エクスプローラ接続)
接続先が「2010:836B:4179::836B:4179」である場合、エクスプローラパスは以下となる。
¥¥2010-836B-4179--836B-4179.ipv6-literal.net

(3) 自動化ツールの IPv6 対応
運用・保守において機器の情報取得等をスクリプト等で自動化している場合は接続先が IPv6 アドレスに変更になることにより自動化ツールの動作に影響がないか確認し、必要に応じてスクリプト等を修正することを推奨する。

(4) DNS を活用したホスト名での運用
IPv6 アドレスは表記が長いため、疎通確認の宛先指定時に入力間違いが発生しやすい。そのため、DNS の AAAA レコード追加を十分に実施する必要があるが、宛先をホスト名とする運用へ切り替えることも有効である。

(5) ログ管理における IPv6 アドレス表記の統一
IPv6 環境において、情報システム等がログを出力する際に IPv6 アドレスを完全表記(省略表記をしない)にて出力する場合(<例> 2001:0db8:0000:0000:0000:0000:0000:0001)、IPv4 と比較して、運用者にとって可読性の低い出力となる。そのため、IPv6 アドレスは運用者が分析しやすい表記に加工することを推奨する。また、IPv6 は1つのアドレスを以下の通り、複数の表記で表現可能である。

- 2001:DB8::1 (大文字での表記例)
- 2001:0db8::0001 (先頭の 0 を含む表記例)
- 2001:db8::1 (RFC5952[40]に記載の標準表記例)

情報システム等における各種ログの管理が煩雑にならないように、IPv6 アドレスを標準表記に統一することを推奨する。尚、アドレス表記の統一については、可読性の観点だけでなく、アプリケーションの処理においてログ出力される IPv6 アドレスを参照し、プログラムを実行する場合、表記が統一されていないことでシステム連携等に支障をきたすことが考えられるため、アプリケーションの観点においても IPv6 アドレス表記の統一は重要である。

40 RFC5952「A Recommendation for IPv6 Address Text Representation」

(6) アクティブな IPv6 アドレスの管理

IPv6 の特徴として、1つのインターフェースに複数の IPv6 アドレスを設定する点が挙げられる。SLAAC(Stateless Address Auto Configuration)により、自動的に複数の IPv6 アドレスを設定することが可能であるが、そのアドレスが設定されてからの経過時間が記録されており、有効期間が切れた場合、アクティブなアドレスとして認識されず、通信できない可能性がある。IPv6 は無尽蔵なアドレス数を持つため、アドレス数の不足に悩むことはないが、自動設定により生成された IPv6 アドレスの有効性を定期的に把握することが必要である。

一方で昨今、通信キャリアやプロバイダ等の IPv6 対応により、IPv4 と同様に IPv6 においてもアドレススキャン攻撃が日常的に行われている。広大な IPv6 のアドレス空間の中からアクティブな IPv6 アドレスを検出することは困難とされているが、SLAAC で Modified EUI-64(Extended Unique Identifier 64-bit)[41]によるアドレス設定を行う際に 48 ビットの MAC アドレスに対して、OUI(Organizationally Unique Identifier)[42]と残りのビットの間に 0xfffe を挿入する等、これらの特性に着目することで、アドレススキャンの対象が絞り込まれる可能性がある。

IPv6 環境を運用する上で、アドレススキャンによりアラートを検知することが想定されるため、スキャンによる影響範囲を把握するために対象の IPv6 アドレスが自組織のアクティブ IPv6 アドレスなのか判断できるように管理する必要がある。

41 通信ネットワークなどで機器一台ごとに割り当てられる固有の識別番号の体系を定めた規格の一つ。IEEE が定めた EUI 規格の一つで、64 ビットの番号を与えるもの。

42 ネットワーク機器の物理アドレスである MAC アドレスの前半部にあたる、メーカごとに割り当てられる番号。標準化団体の IEEE が一元的に管理し、通信機器メーカなどに発行している。

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 のサーバは社内に立てず、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。

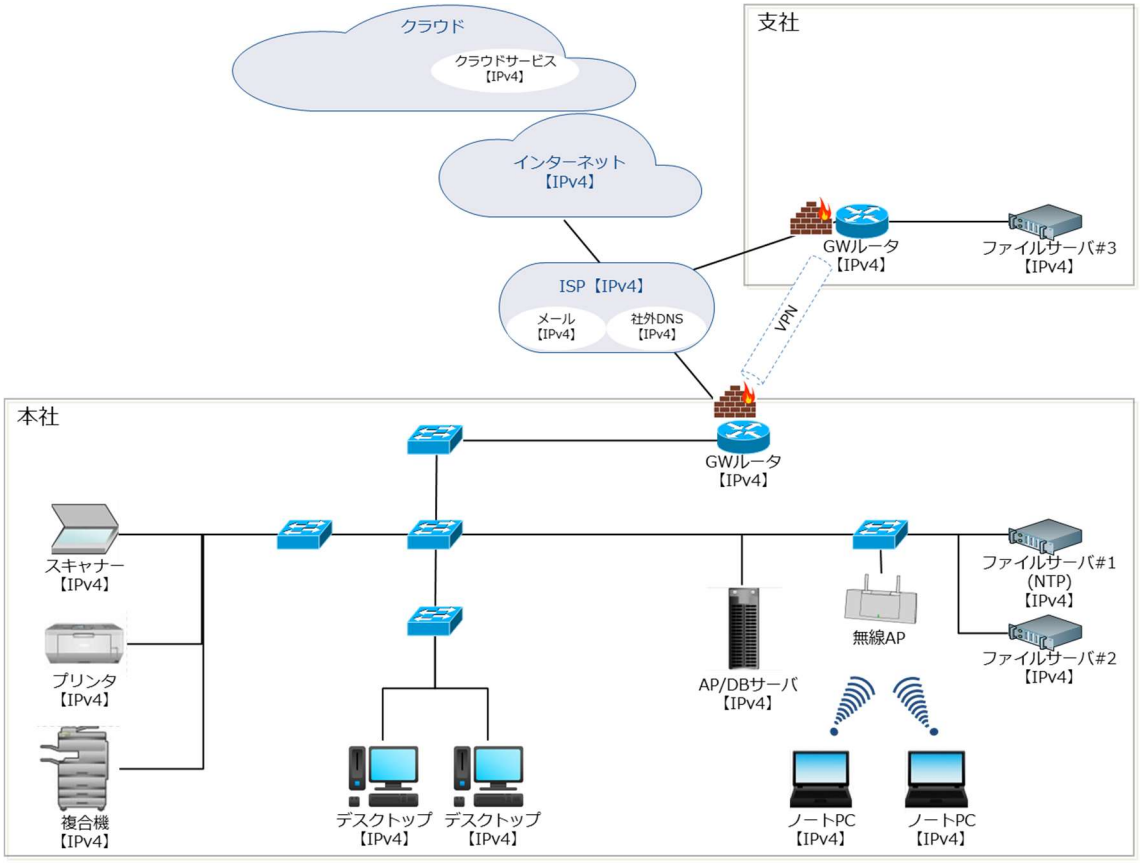


図 5.1.2-1 ネットワーク構成図イメージ

(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	imageRUNNER 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。

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。

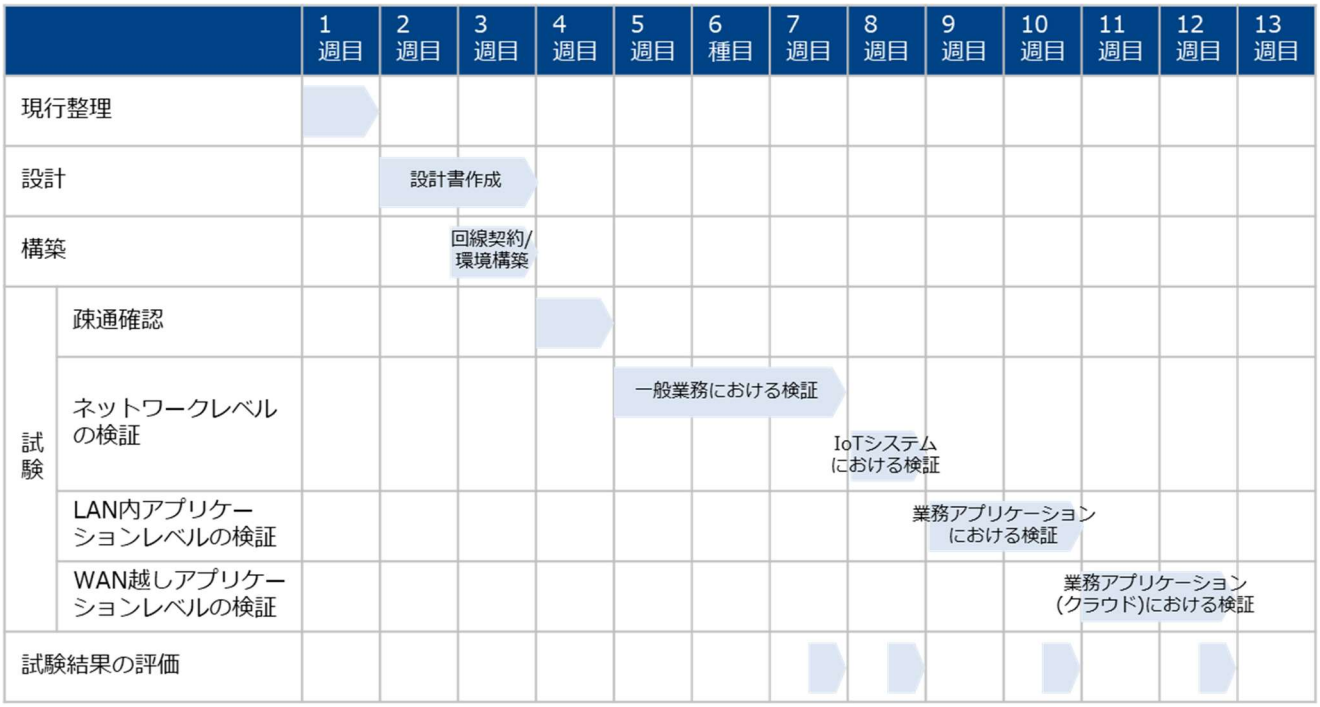


図 5.1.3-1 スケジュールイメージ(中小企業 A)

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で、IPv6 分の名前解決を hosts ファイルに追記する。

③ 特記事項

(c)ポリシーテーブルについて、IPv6 無効化は Microsoft 非推奨のため、優先設定としている。

(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で、IPv6 分の名前解決を hosts ファイルに追記する。

③ 特記事項

(c)ポリシーテーブルについて、IPv6 無効化は Microsoft 非推奨のため、優先設定としている。

(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。

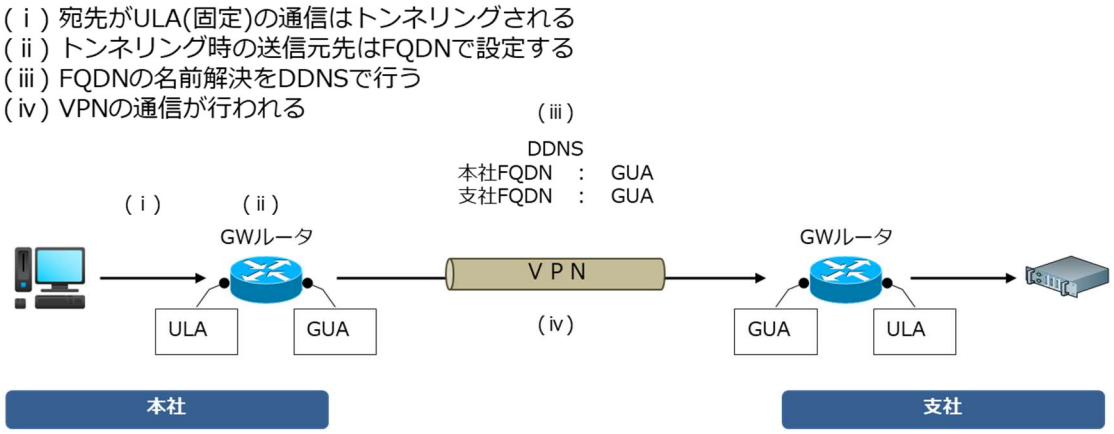


図 5.1.4-1 ULA および GUA を利用したインターネット VPN 通信の流れ

(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 優先の状態で、支社側のファイルサーバは IPv4 優先の状態で検証する。

(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。

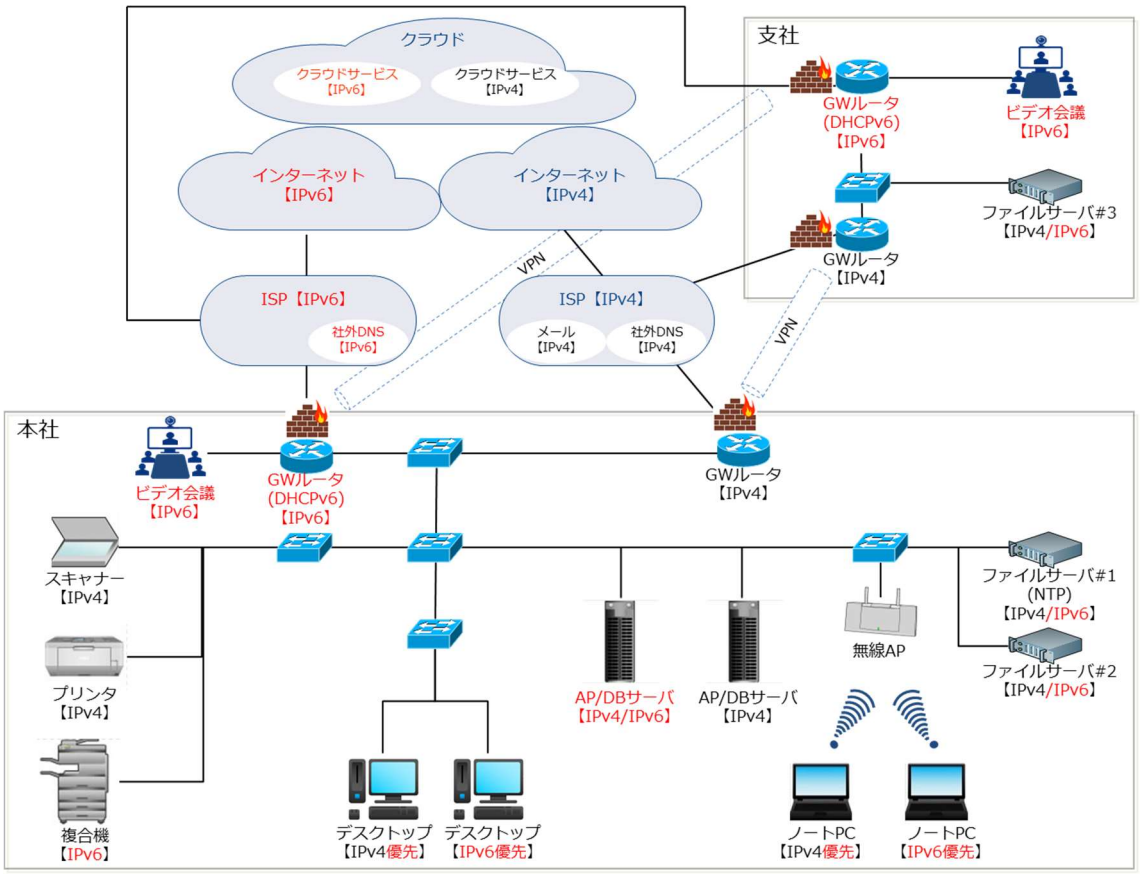


図 5.1.4-1 IPv6 対応後のネットワーク構成図

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 pppoe use lan2 pppoe 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	【拠点間の VPN 接続】 ※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。 [本社側] 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 [支社側] 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

項番	設定内容の詳細
4	【セキュリティ・ファイアウォール設定（パケットフィルタ）】 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

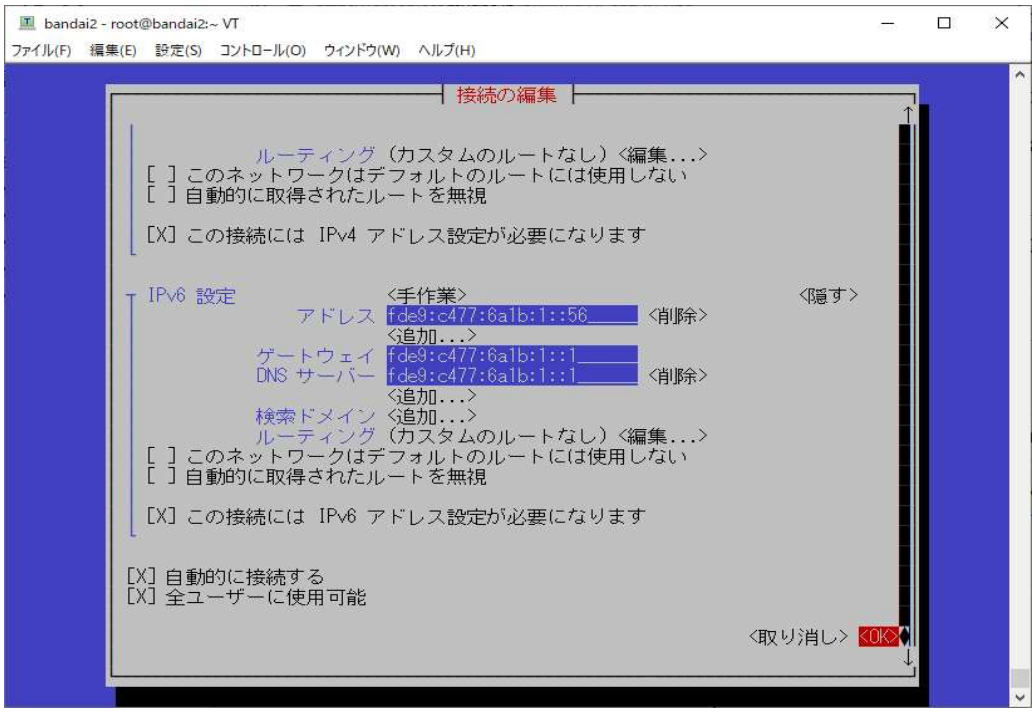
(2) 複合機の設定

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	【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
2	【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 ※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。

(3) ファイルサーバの設定

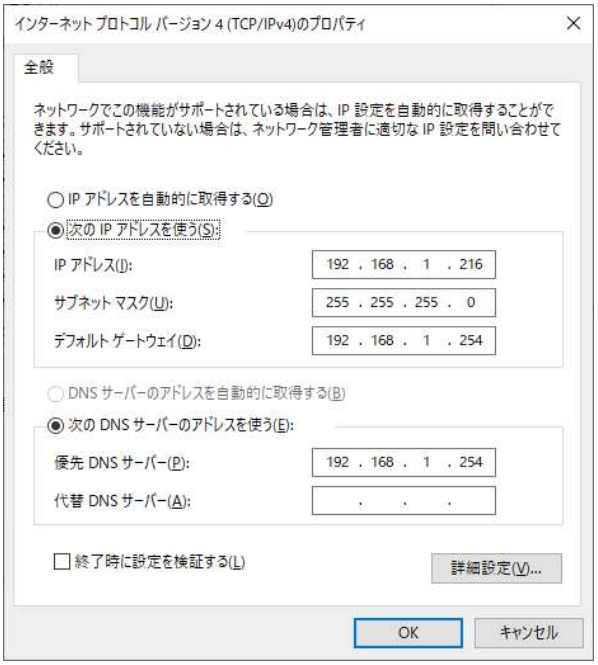
ファイルサーバ上で下記の設定を行い、IPv6 デュアルスタックに対応するファイルサーバを構築する。

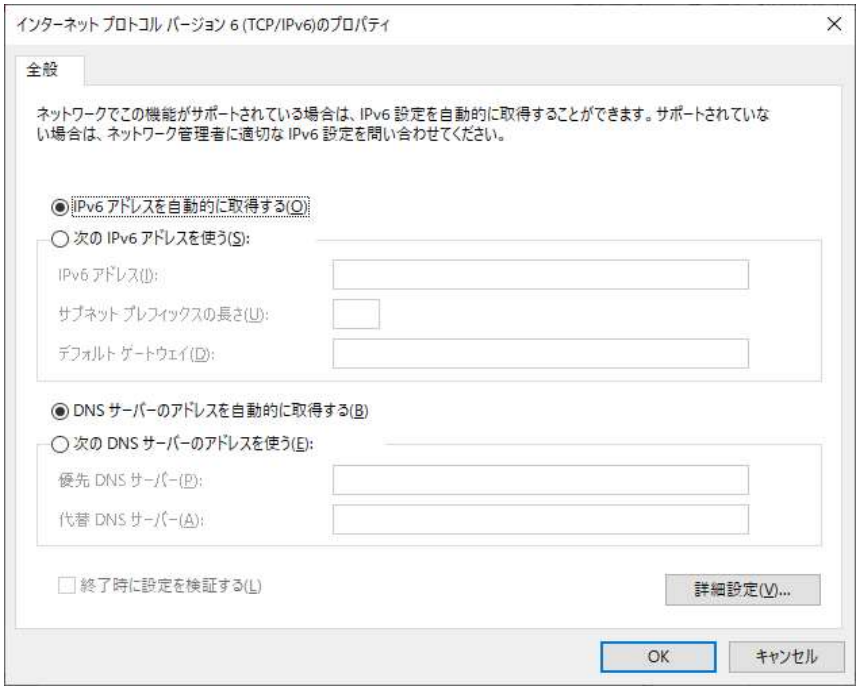
項番	設定内容の詳細
1	【本体のネットワーク設定】 各ファイルサーバ上で nmtui により、IPv6 アドレスの追加設定を行う。IPv6 アドレスは、社内で管理されているユニークローカルアドレスを設定する。 fde9:c477:6a1b:1::56/64 (bandai2) fde9:c477:6a1b:1::57/64 (yachiyo2) fde9:c477:6a1b:2::11/64 (park2) （設定画面の例） 
2	【hosts ファイルの設定】 /etc/hosts に IPv6 アドレスを追記する。 ===== fde9:c477:6a1b:1::56　　bandai2 bandai2v6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

項番	設定内容の詳細
3	【samba 設定】 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） [global] hosts allow =<既存の IPv4 アドレス> fde9:c477:6a1b:2::/64 fde9:c477:6a1b:1::/64 fe80::/64 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。 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)
4	【LDAP 設定】 LDAP の同期設定(ファイルサーバ 3（支社側）のみ) #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

(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。

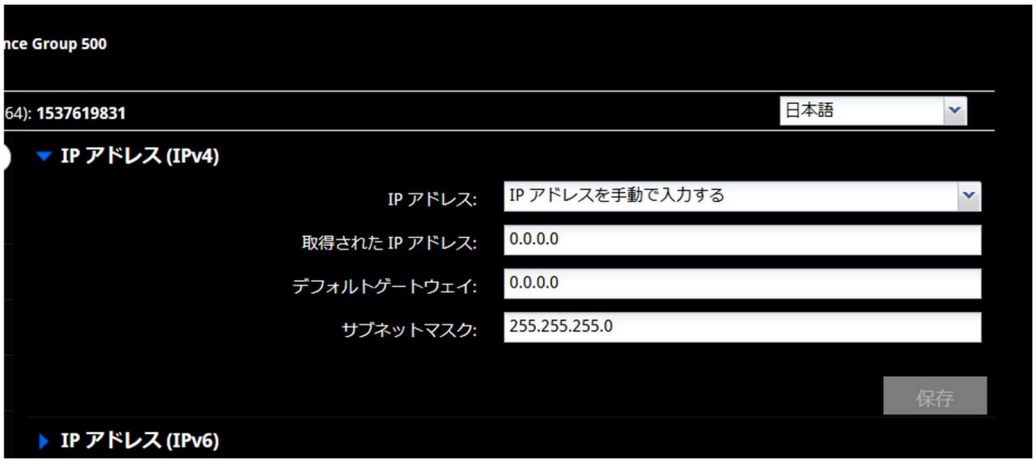
項番	設定内容の詳細
1	【IPv4 アドレスの設定】 接続しているネットワーク アダプタ（LAN or Wi-Fi）のプロパティから固定 IP を設定する。  ※IP アドレスは社内で管理している固定アドレスを設定する。

項番	設定内容の詳細
2	【IPv6 アドレスの設定】 接続しているネットワーク　アダプタ(LAN or 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) 
3	【Hosts の設定追加】 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) ¥Windows¥System32¥drivers¥etc¥hosts ===== ## IPv6 fde9:c477:6a1b:1::56 bandai2 fde9:c477:6a1b:1::57 yachiyo2 fde9:c477:6a1b:2::11 park2 =====

項番	設定内容の詳細
4	【IPv4 アドレスの優先設定】 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） netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0 netsh interface ipv6 set prefixpolicy ::1/128 40 1 netsh interface ipv6 set prefixpolicy ::/0 30 2 netsh interface ipv6 set prefixpolicy 2002::/16 20 3 netsh interface ipv6 set prefixpolicy ::/96 10 4 上記の設定を行ったら、PC を再起動する。
5	【IPv4/IPv6 優先設定を確認】 再起動後以下のコマンドを実行し、IPv4 が最優先になっていることを確認する。 netsh interface ipv6 show prefixpolicies （実行例） 優先順位　ラベル　プレフィックス ----------　-----　-------------------------------- 50　0　::ffff:0:0/96　(IPv4 マップ) 40　1　::1/128　(ループバック) 30　2　::/0　(IPv6 通信全般) 20　3　2002::/16　(6to4) 10　4　::/96　(IPv4 互換) 5　5　2001::/32　(Teredo)

(5) ビデオ会議の設定

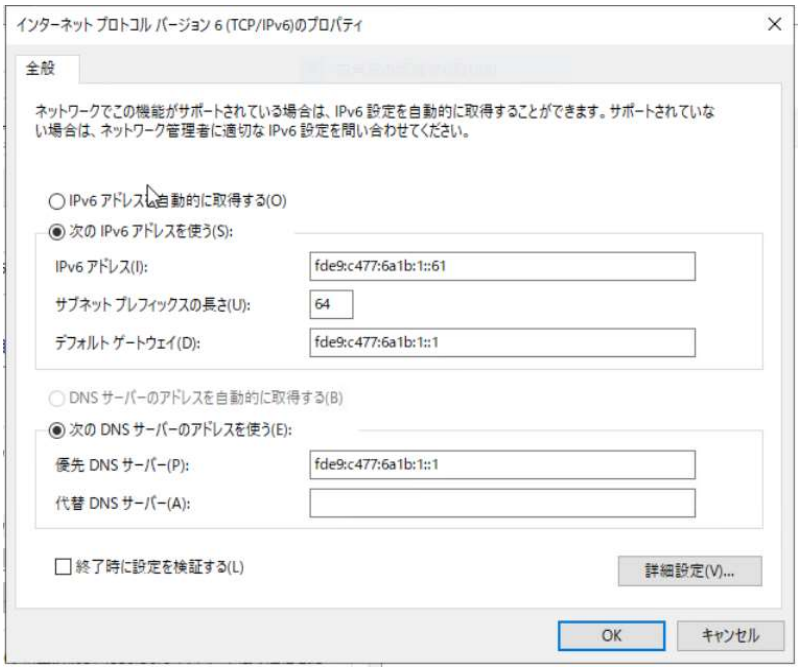
マニュアルに従ったシステムの初期セットアップ実施後、IPv6 に関連する以下の設定を実施した(本社側、支社側)

項番	設定内容の詳細
1	【IPv6 アドレス設定】 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。 
2	【IPv4 アドレス無効化設定】 IPv4 アドレスに「0.0.0.0」を設定して無効化する。 

(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)

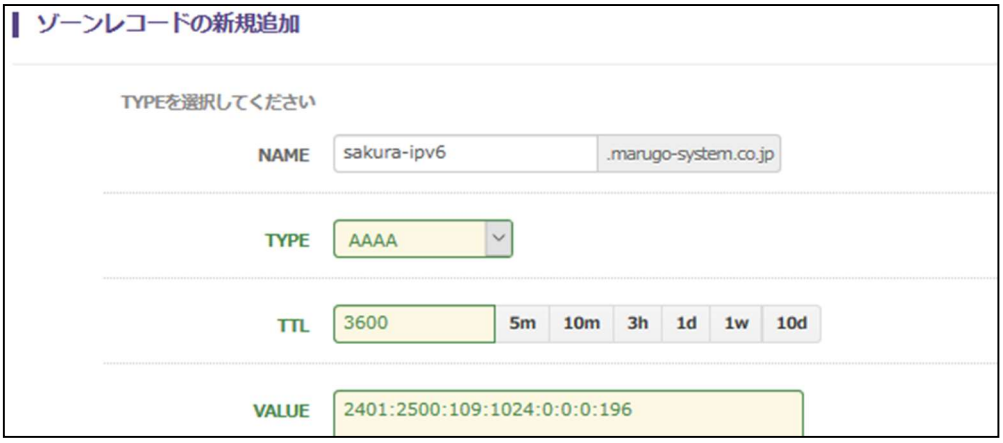
項番	設定内容の詳細
4	【ゲスト OS 環境の IPv6 設定】 ゲスト OS の IPv6 アドレスを以下のとおり設定する。 
5	【ゲスト OS 環境の DB 環境構築】 ゲスト OS で、DBMagic 付属の Pervasive.SQL をセットアップする。 （特記事項なし）
6	【クライアント環境のアプリケーション実行環境構築】 クライアント PC に、さんちょくアプリケーションの実行環境をセットアップする。 実行環境のセットアップ後、設定ファイル（Magic.ini）に IPv6 形式で DB の接続先（APDB サーバ）を指定する。 （設定例） [MAGIC_LOGICAL_NAMES] 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¥ クラインアント PC でアプリケーションの実行ファイルを起動し、さんちょくのメインメニューが起動するか確認する。

(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	【仮想サーバ環境のセットアップ】 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。 ※Windows Server のバージョンは 2016、プランは「for RDS」を指定
2	【IPv6 アドレスの有効化設定】 ネットワーク設定で IPv6 を利用可能にする。 「ルータ＋スイッチ」を作成する。 名前:任意の名称 ルータ:「はい」 IPv6 アドレス:「有効」 その他はデフォルトを指定する。 ※「IPv6 の逆引き設定」は必須ではないため、設定なし。 ※参考 https://manual.sakura.ad.jp/cloud/network/switch/ipv6.html ・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	【クラウド環境のファイアウォール設定】 ・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 **注意事項** • 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	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） ・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	・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	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。 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。 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。

項番	設定内容の詳細
7	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。 （設定例） 

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。

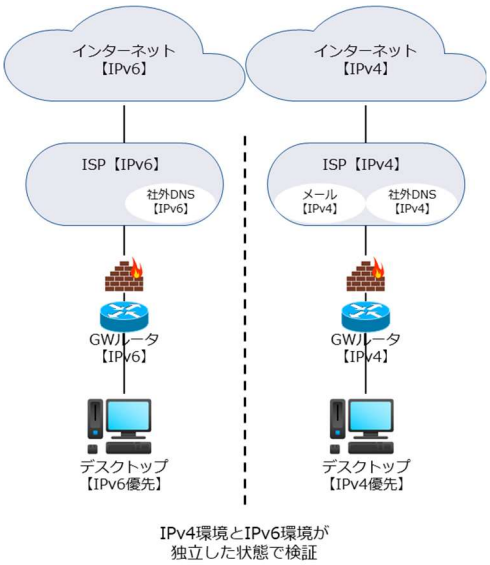


図 5.1.6-1 IPv4 経路と IPv6 経路を分離

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

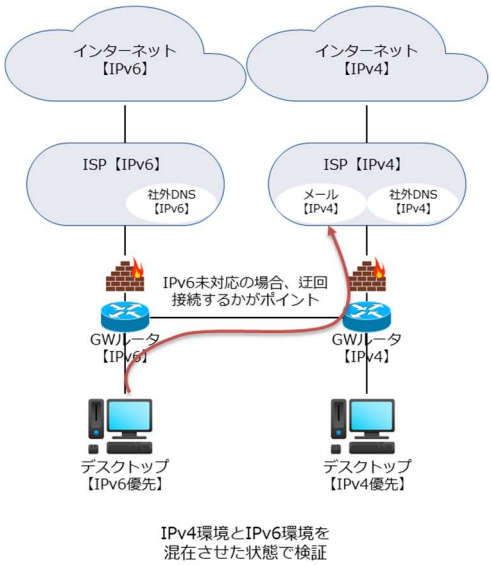


図 5.1.6-2 IPv4 経路と IPv6 経路を接続

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 経路を切り離し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。

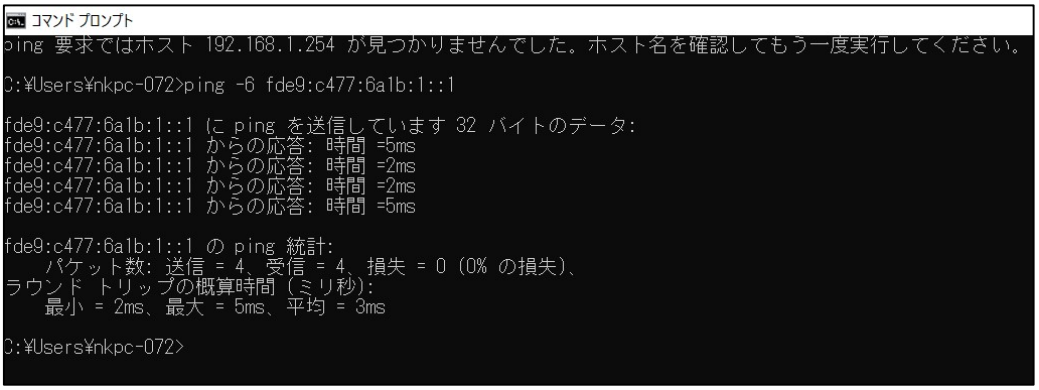


図 5.1.6-3 IPv6 で ping 応答あり

【#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)

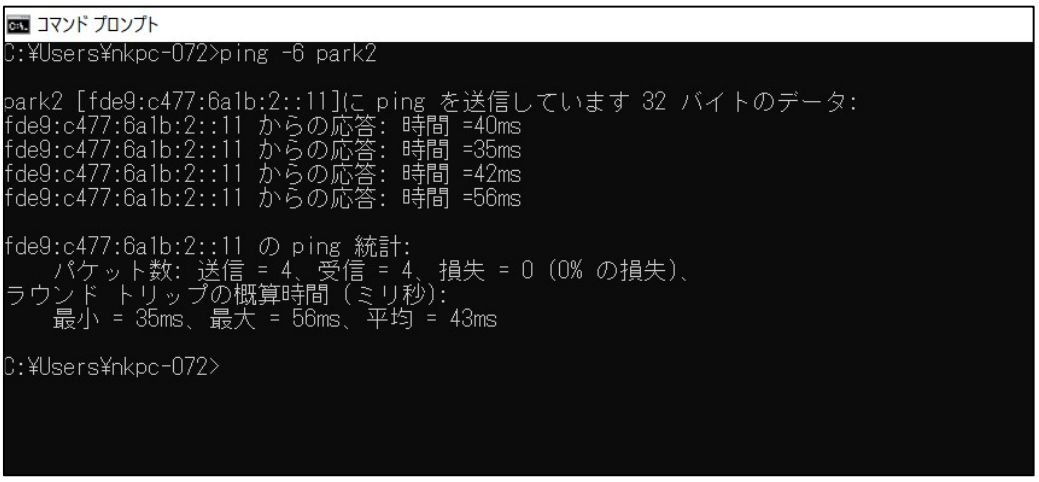


図 5.1.6-5 ホスト名でも ping 応答あり

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	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。

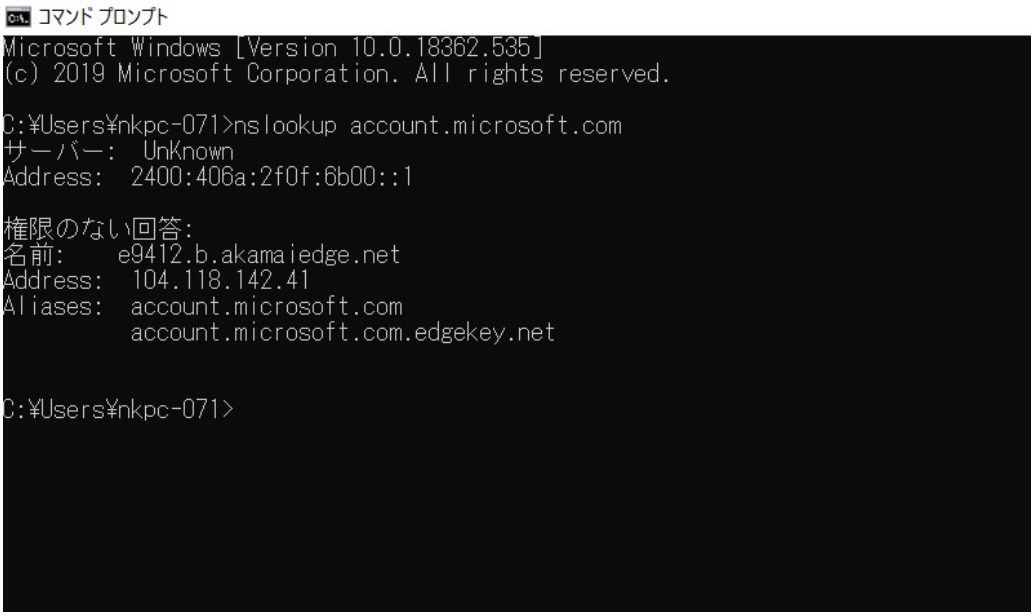


図 5.1.6-6 Microsoft アカウント認証ページは AAAA レコードなし

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。

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、MicrosoftTeams 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 MicrosoftTeams 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 MicrosoftTeams 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。

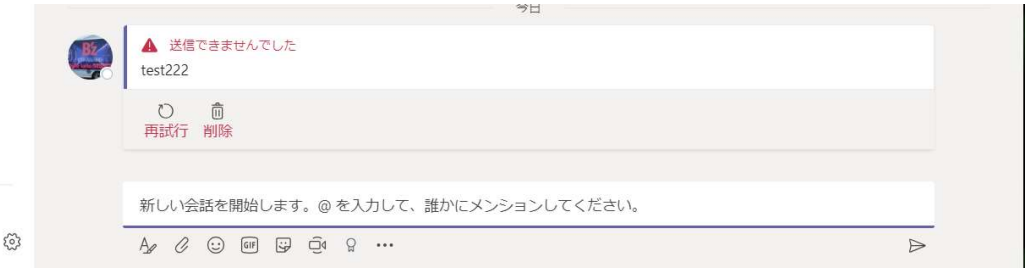


図 5.1.6-9 MicrosoftTeams メッセージ送信不可

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した結果、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した結果、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。

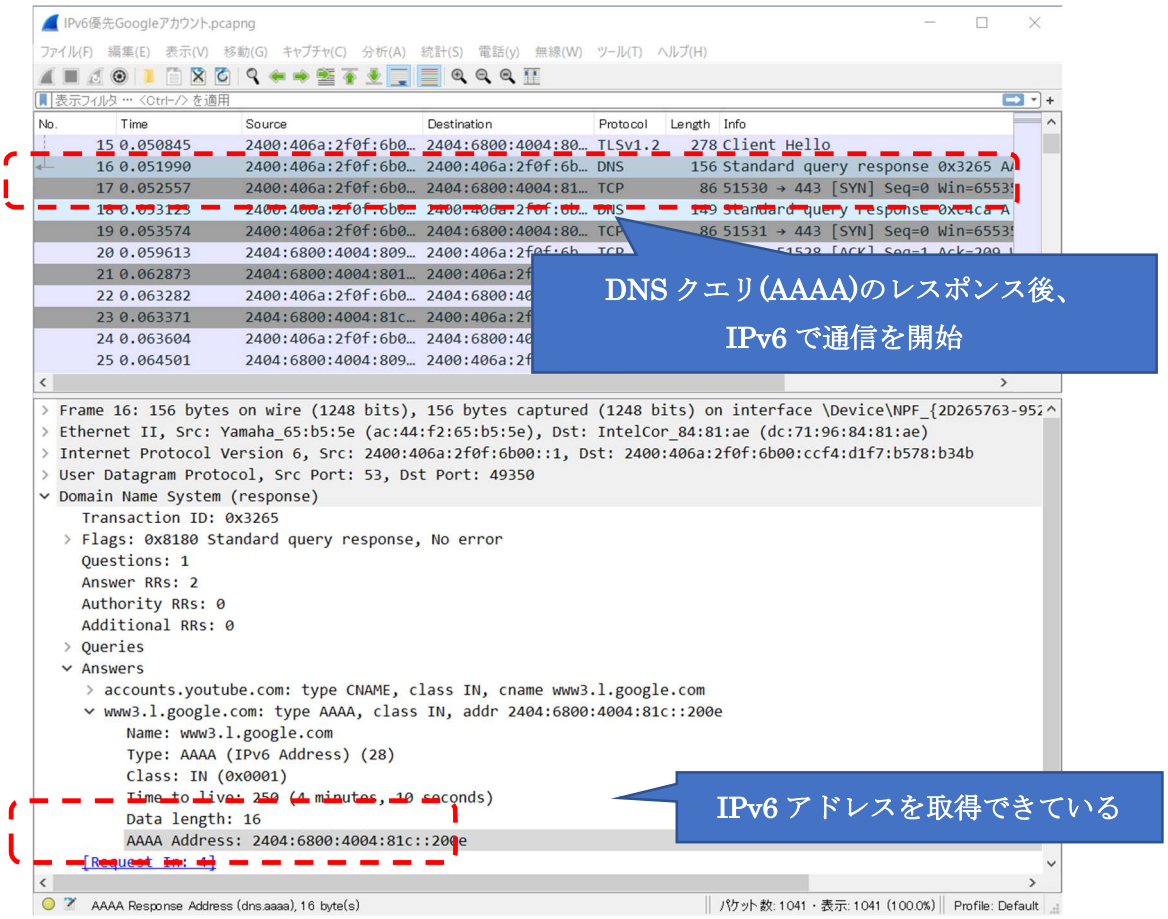


図 5.1.6-10 IPv6 対応サービスの場合、IPv6 アドレスを取得し IPv6 で通信

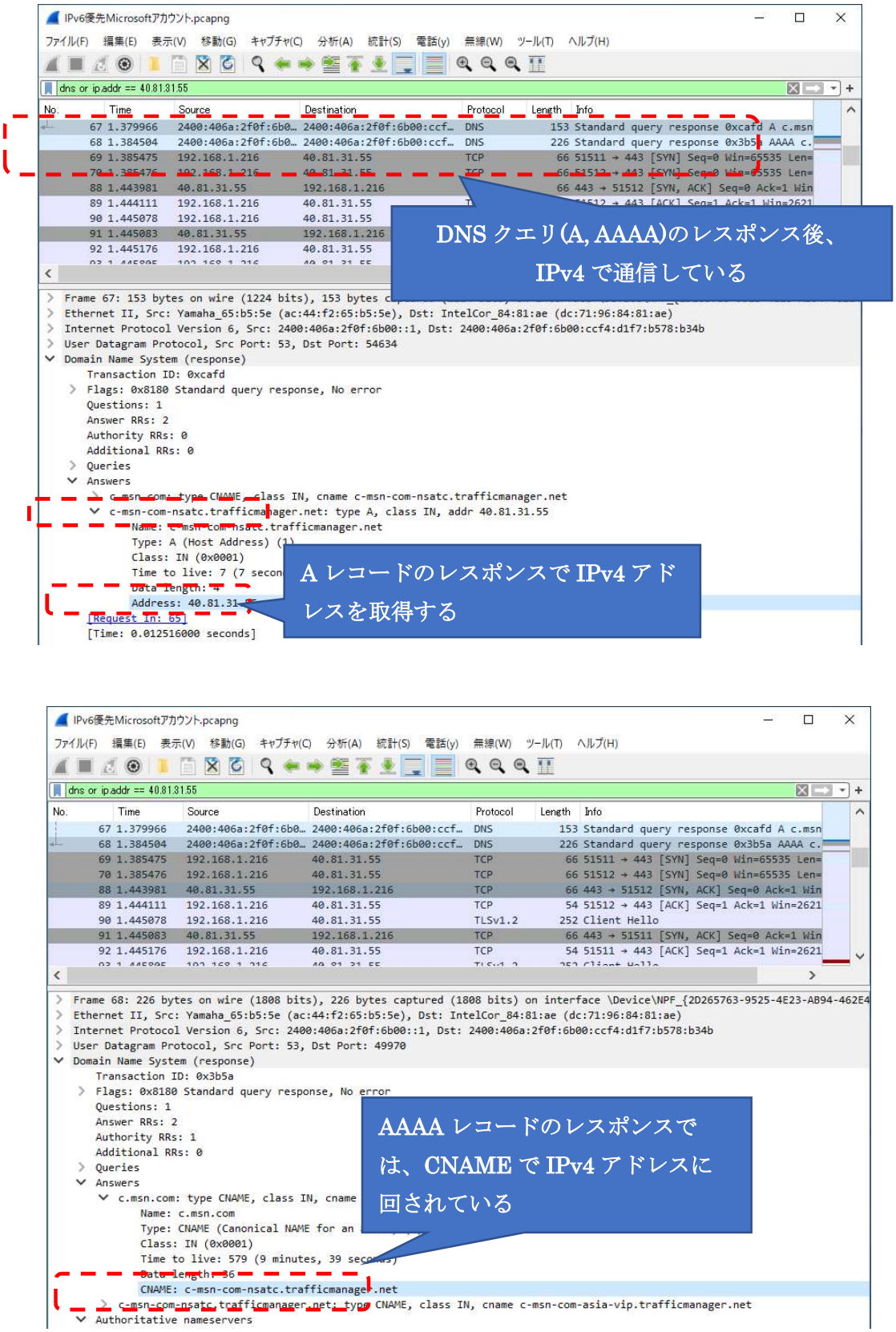


図 5.1.6-11 IPv6 未対応サービスの場合、IPv6 アドレスを取得できず IPv4 で通信

⑵ IoT システムにおける検証について

5.1.4⑼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・音声が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。

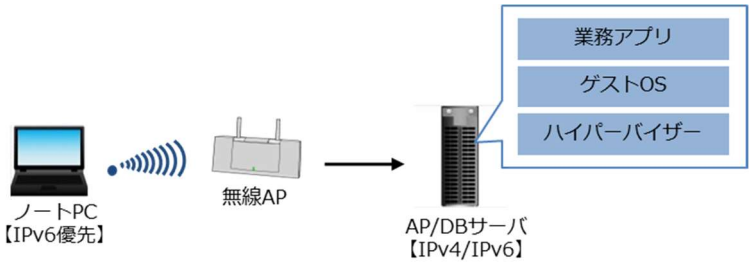


図 5.1.6-12 業務アプリケーションにおける検証範囲

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。

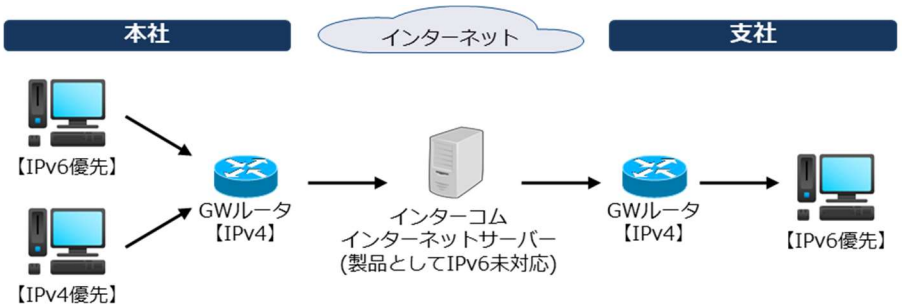


図 5.1.6-13 保守作業用ソフトにおける検証範囲

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 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 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る。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

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）

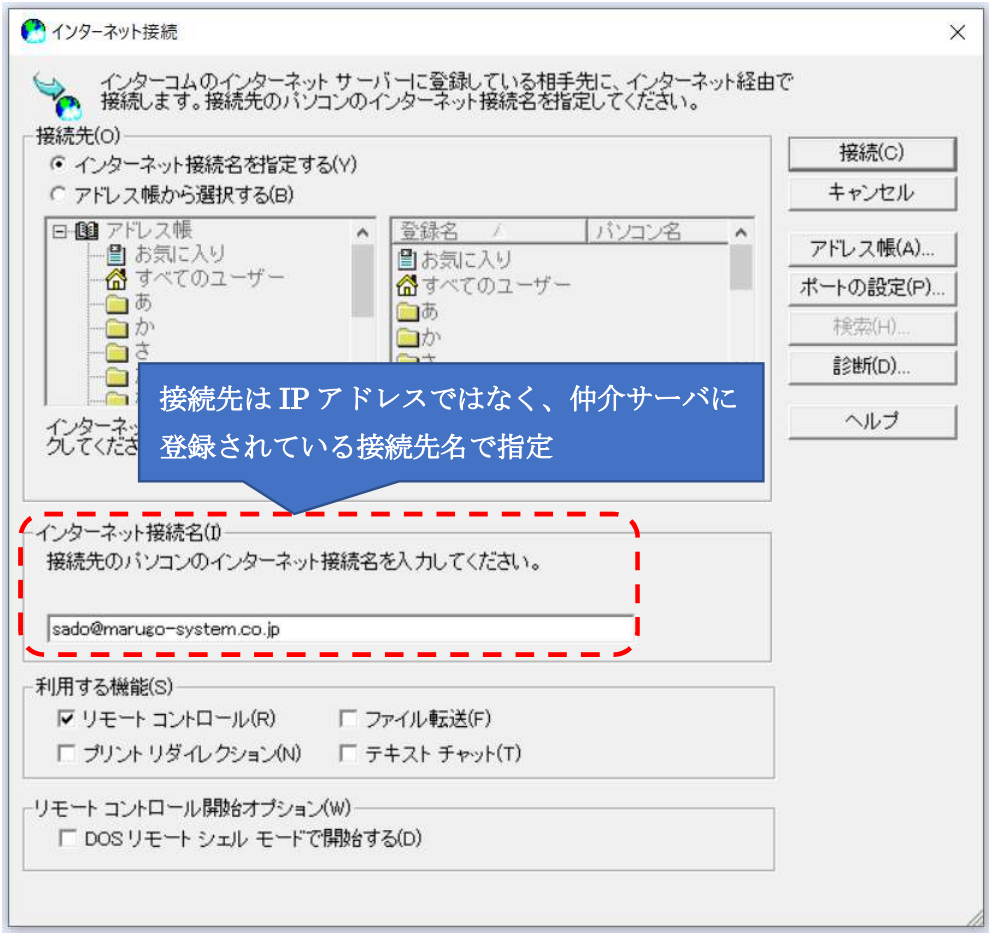


図 5.1.6-17 ゲスト PC 側の接続先指定画面

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。

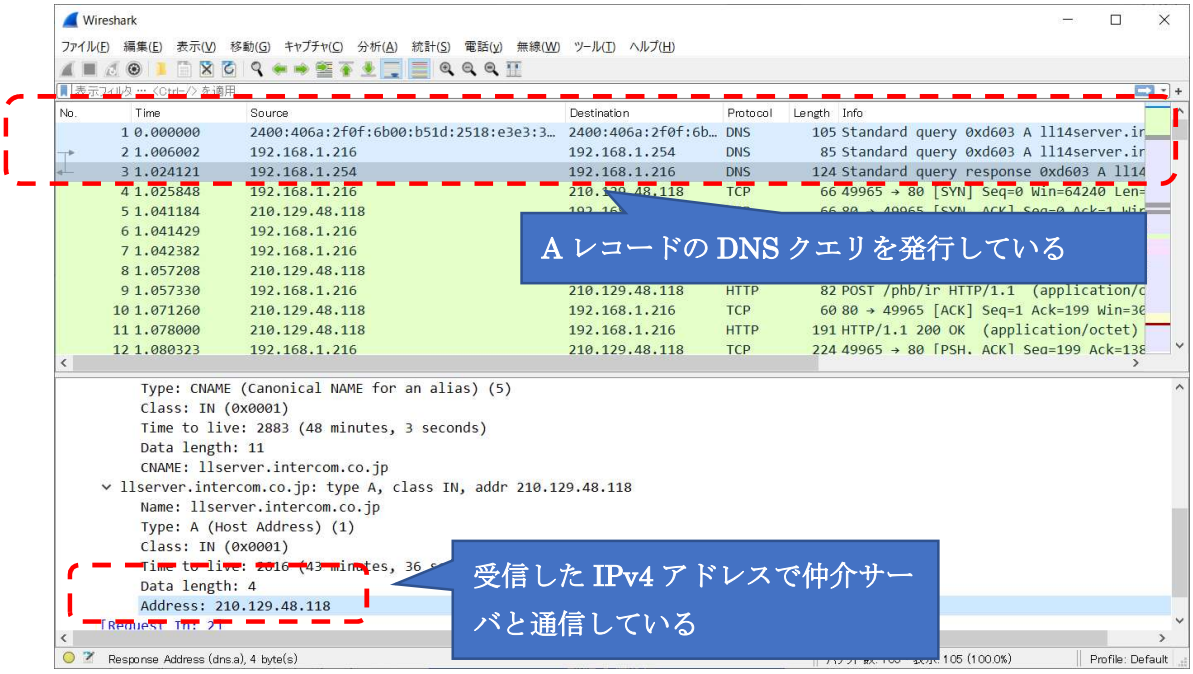


図 5.1.6-18 ゲスト PC と仲介サーバ間のパケットログ

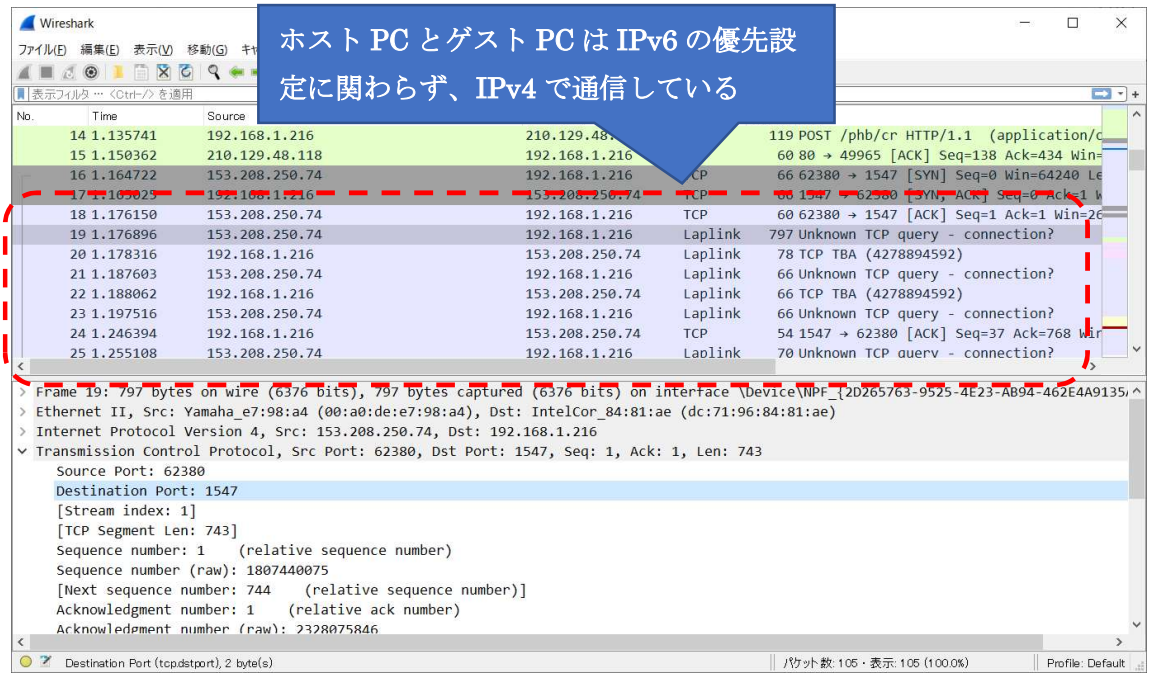


図 5.1.6-19 ゲスト PC とホスト PC 間のパケットログ

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。

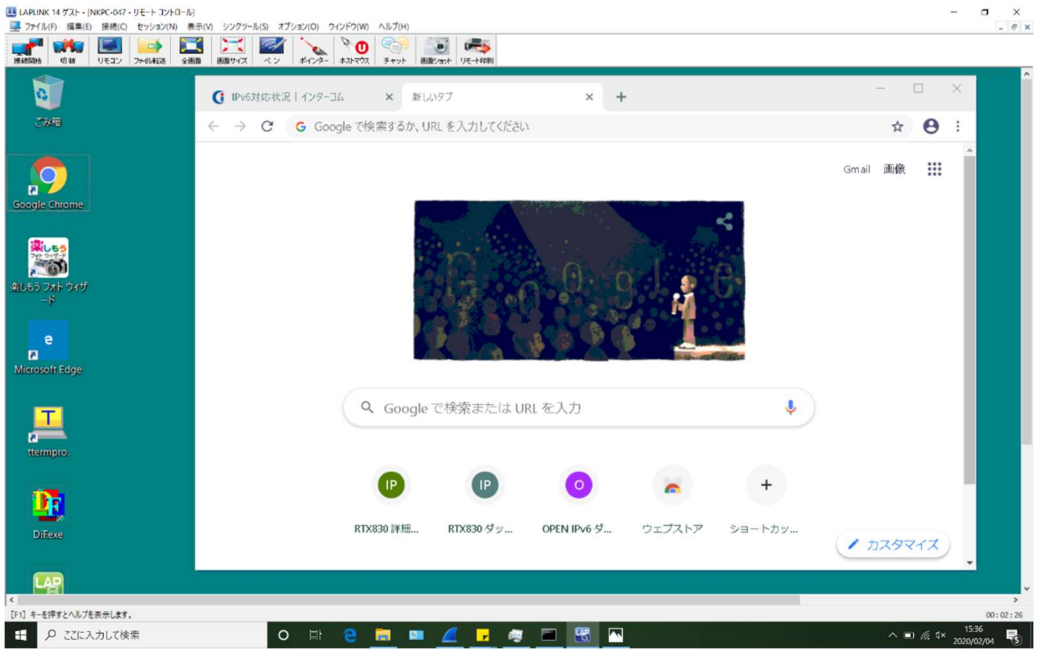


図 5.1.6-20 リモート接続成功時のスクリーンショット

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。

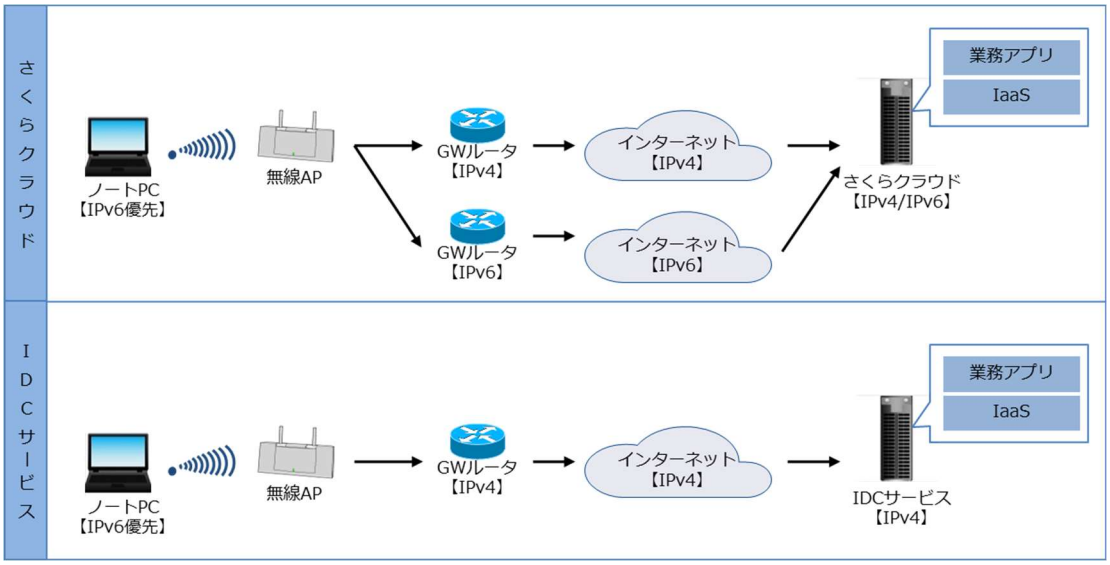


図 5.1.6-21　業務アプリケーションにおける検証（クラウド）範囲

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

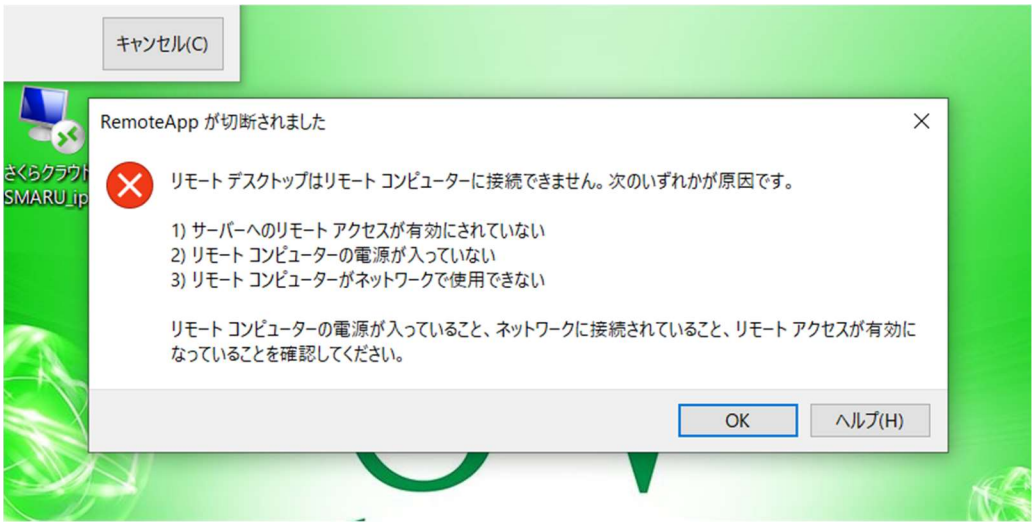


図　5.1.6-23　IaaS の IPv6 を無効にした場合、IPv6 通信できなくなる

#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、機器メーカのサポート等に確認した結果、IPv6 対応が十分でないことが判明した課題と対応の事例を示す。

(2) IPv6 対応における留意事項(構築時の Tips)

本検証において実際に発生した IPv6 関連のトラブルシュート事例をもとに、IPv6 対応において普遍的に留意すべき点を示す。

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 とくとく 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。

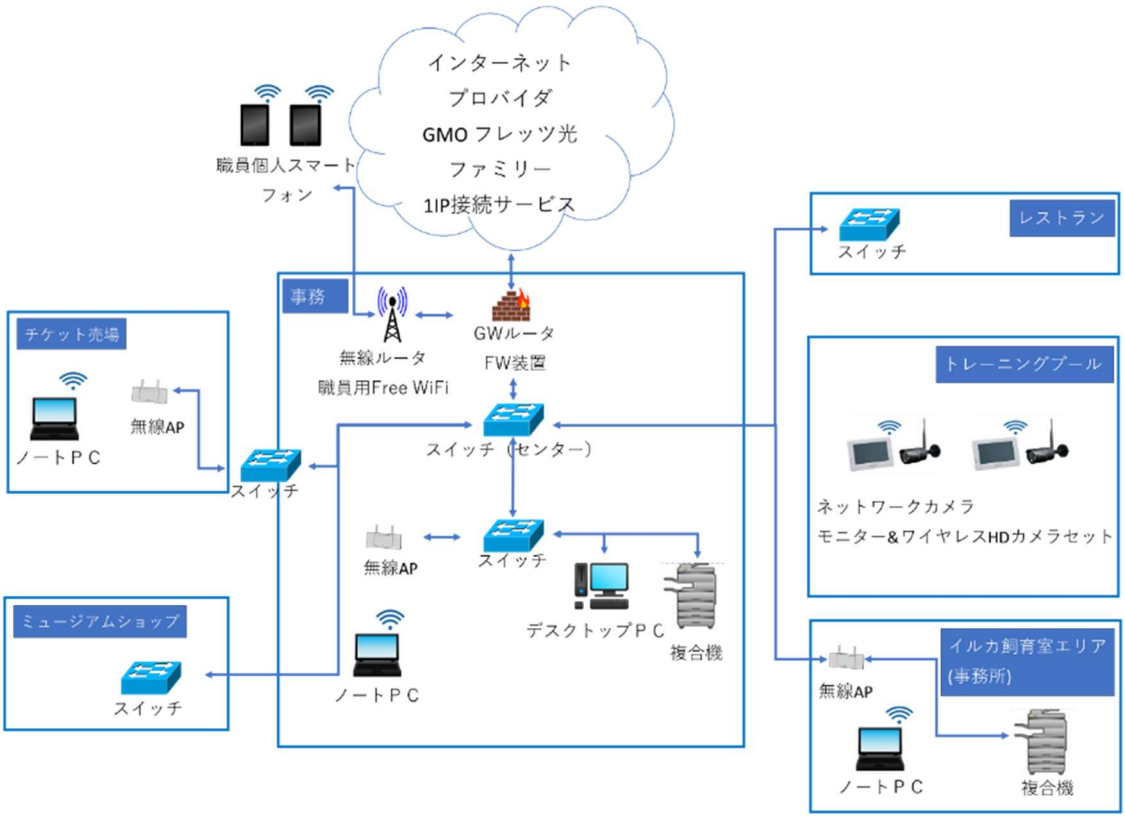


図 5.2.2-1 ネットワーク構成図イメージ

(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。

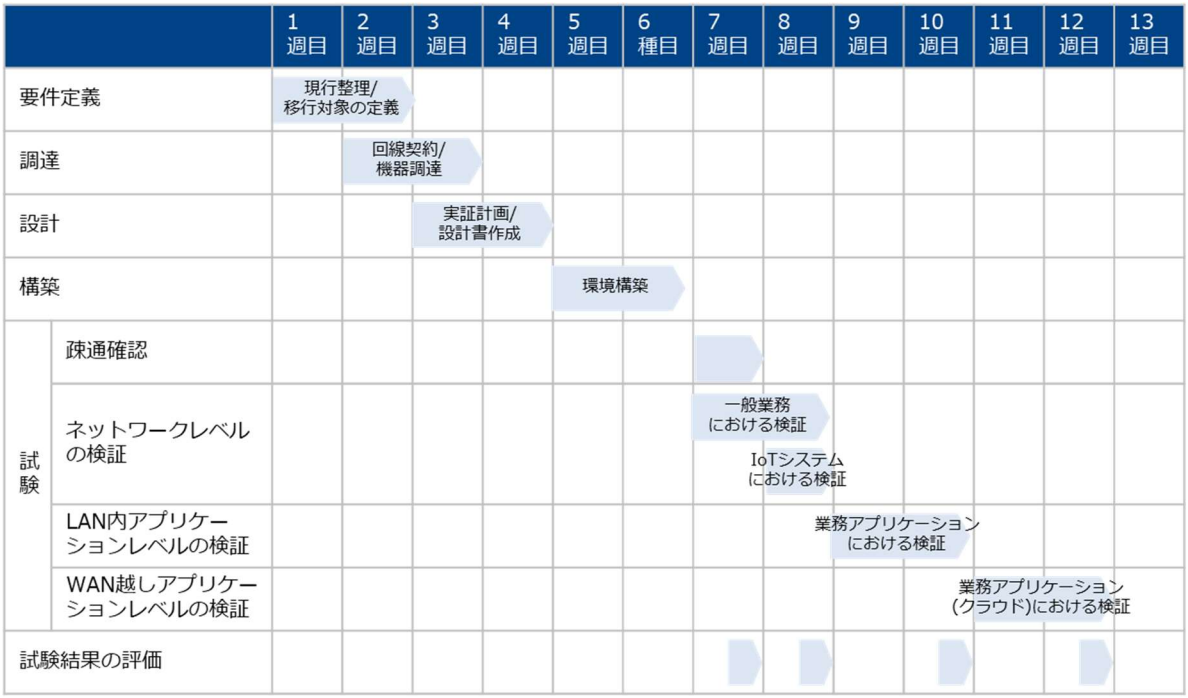


図 5.2.3-1 スケジュールイメージ(中小企業 B)

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、現存環境では 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、また現存機器は全て静的 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（NAS[54]、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、SMB[57]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 VPS[58]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。

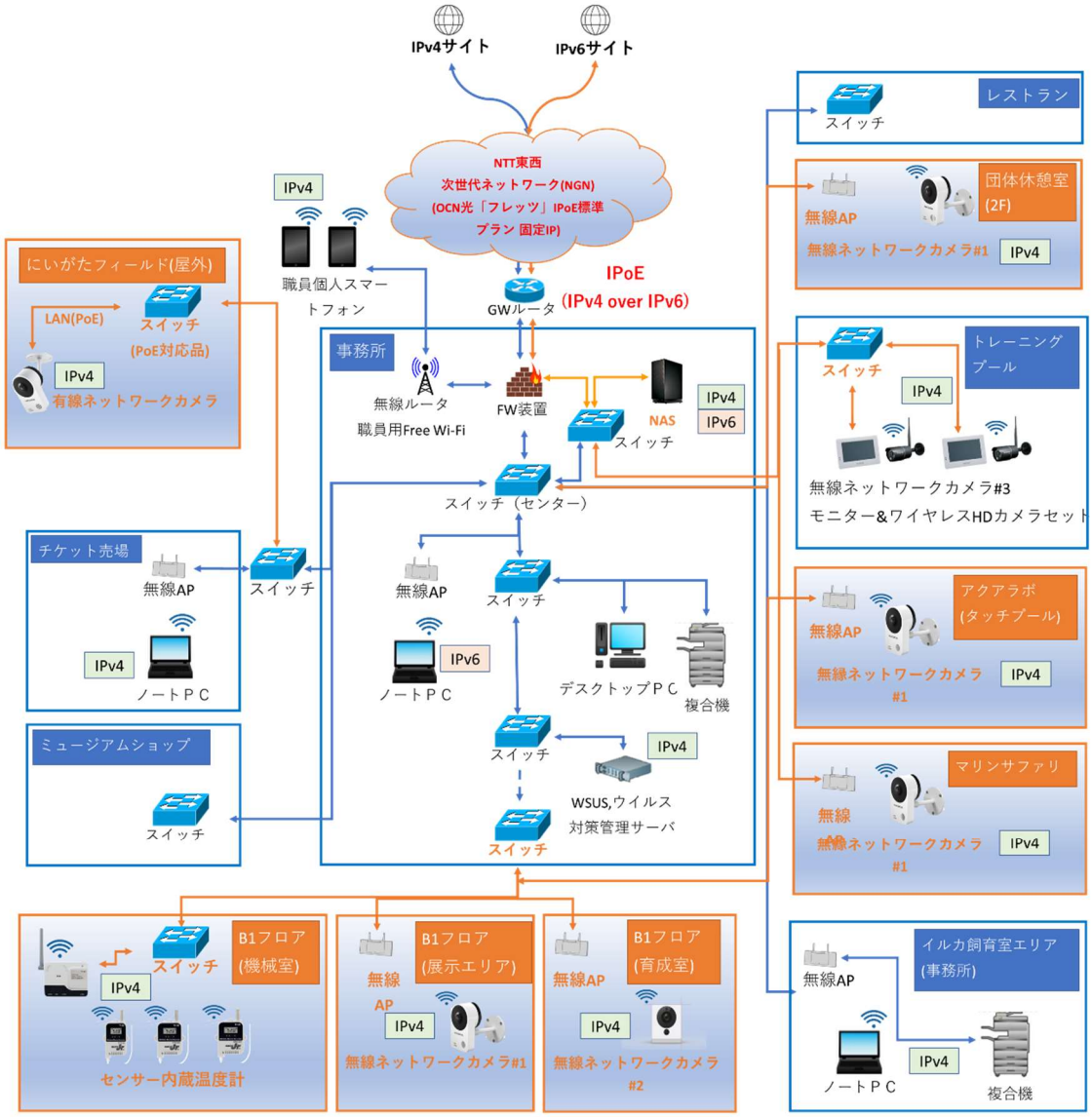


図 5.2.4-1 IPv6 対応後のネットワーク構成図

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った。

【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。

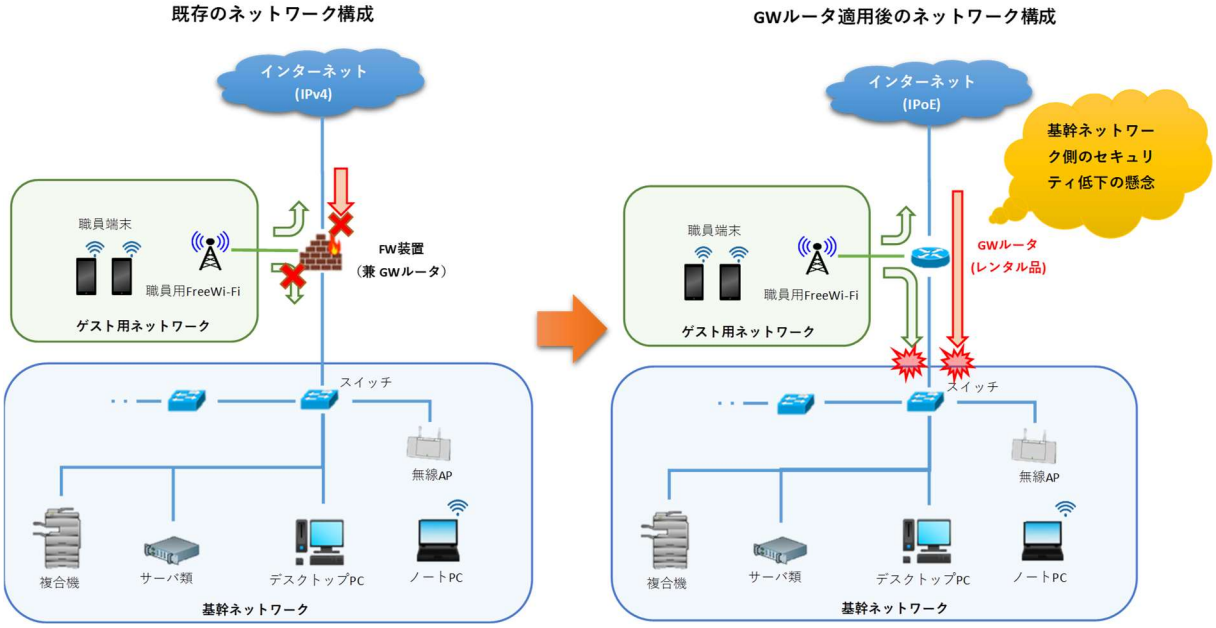


図 5.2.5-1 GW ルータ置き換えによるセキュリティ低下の懸念

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り、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かも課題となった。

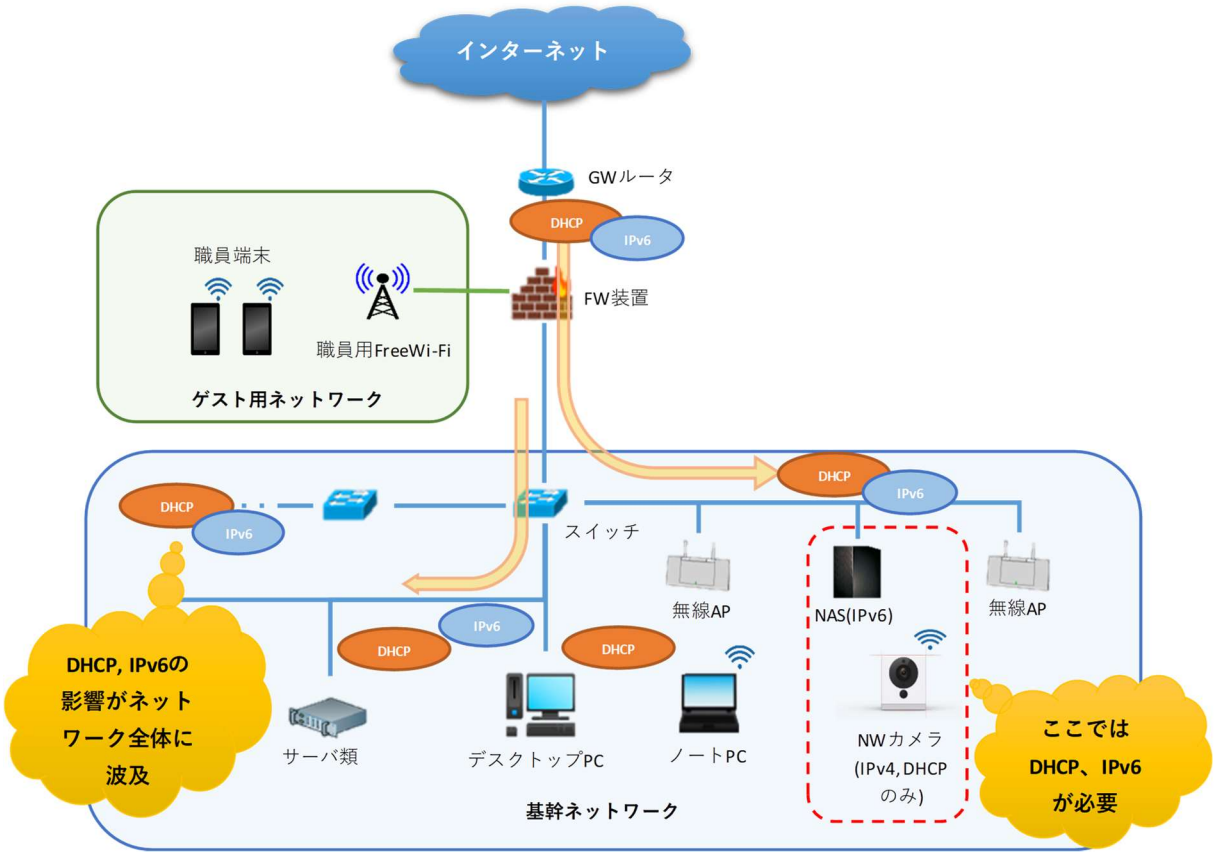


図 5.2.5-2 DHCP を有効化した場合のネットワーク全体への影響の懸念

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、機器自体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)。

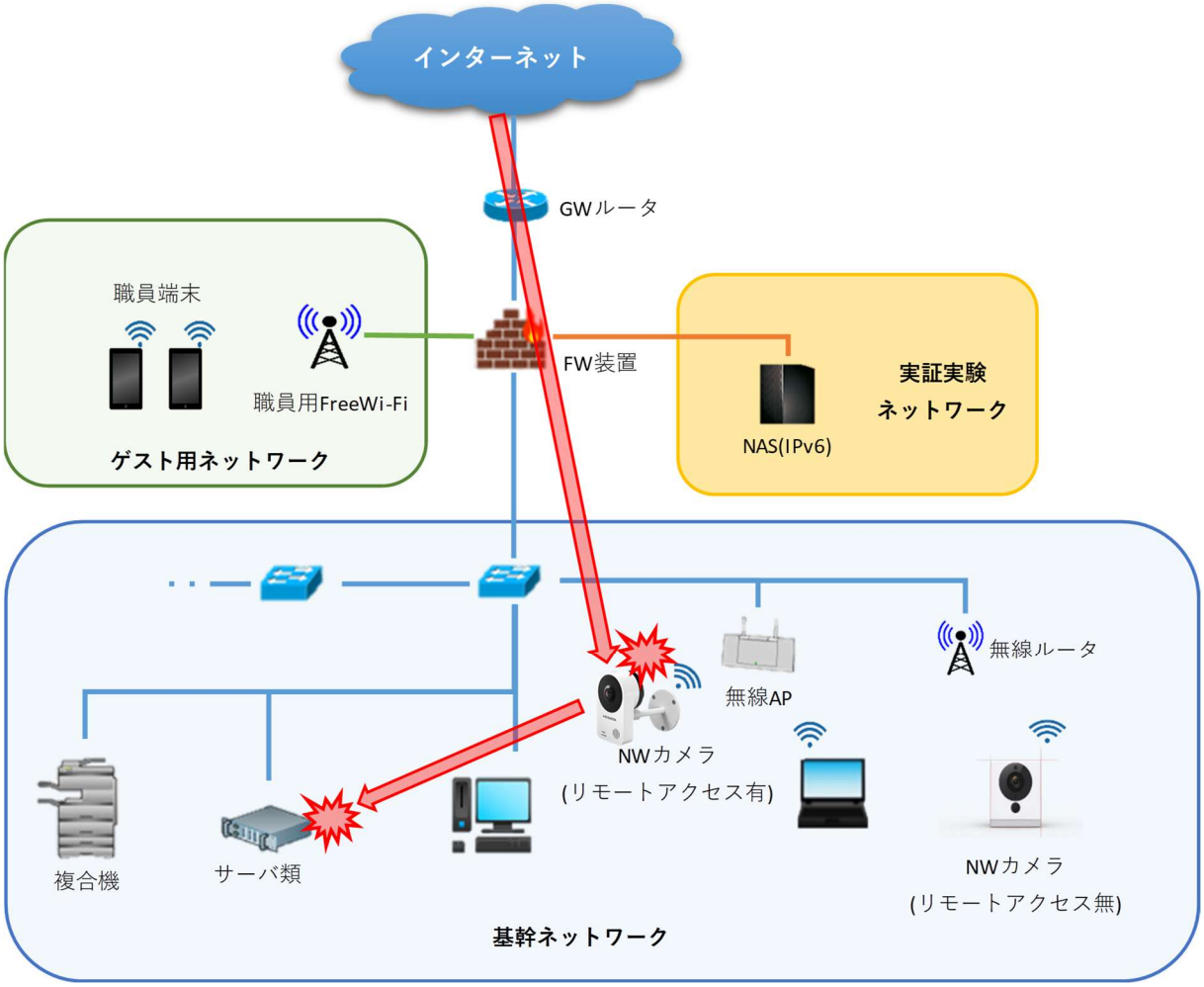


図 5.2.5-3 リモートアクセスによる、不正アクセスのリスク

(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。
選定の候補に挙がったものは 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。

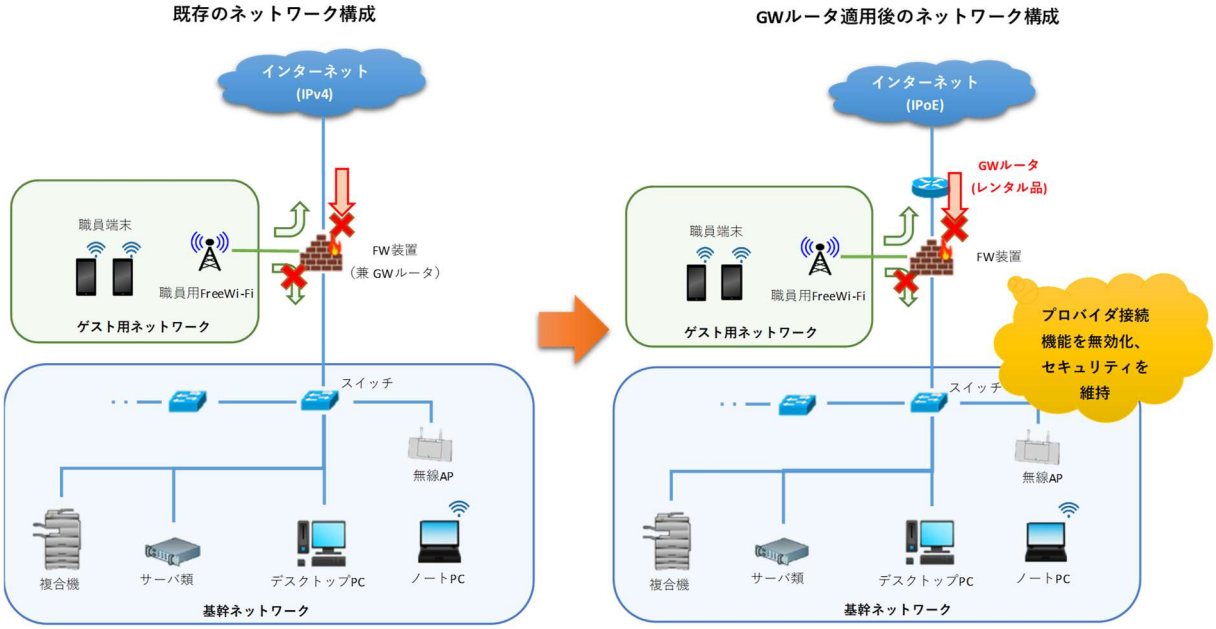


図 5.2.5-4 プロバイダ接続機能無効化によるによる FW 装置の運用

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。

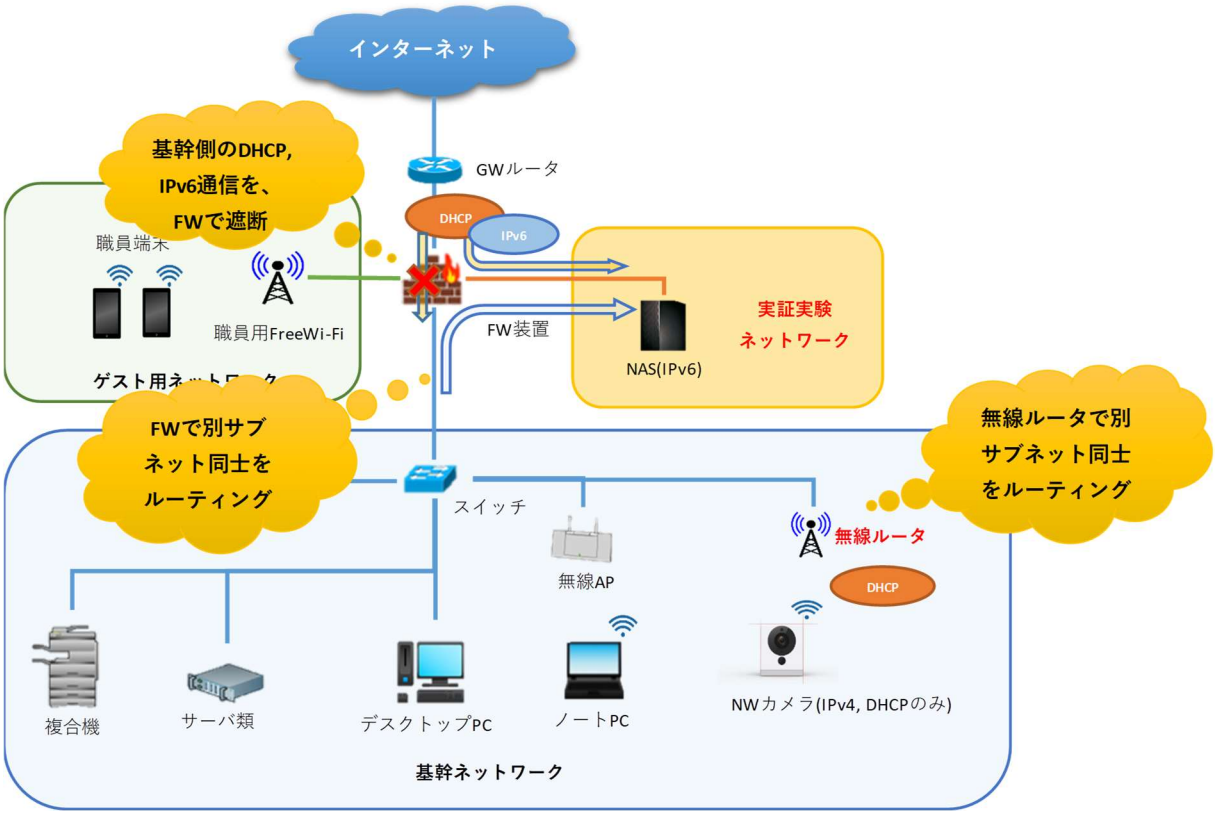


図 5.2.5-5 VLAN とルーティングを利用した DHCP, IPv6 の適用

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 として割り当てるだけで基幹ネットワークから分離は行える。

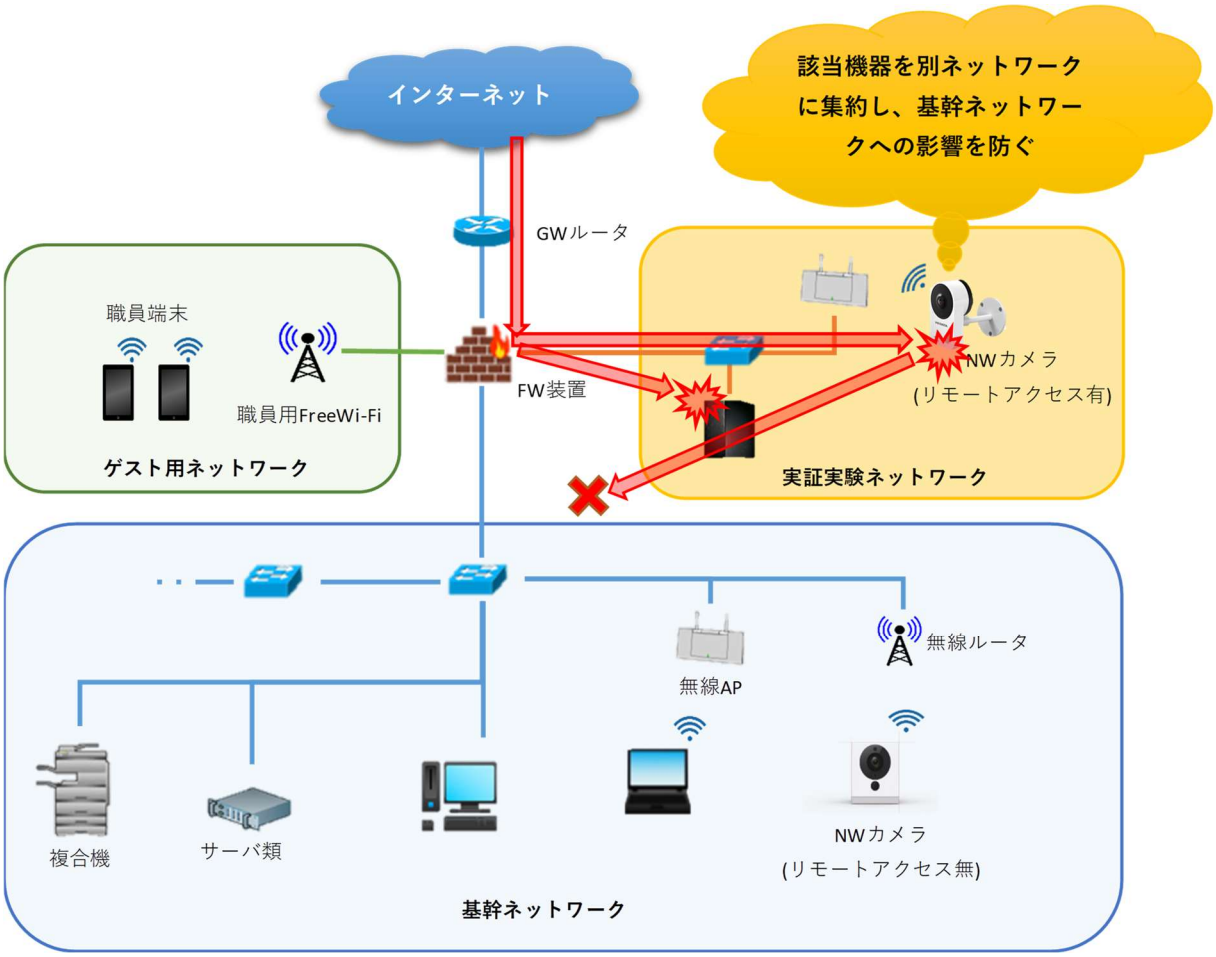


図 5.2.5-6 VLAN を用いた基幹・実証実験ネットワーク分離

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。

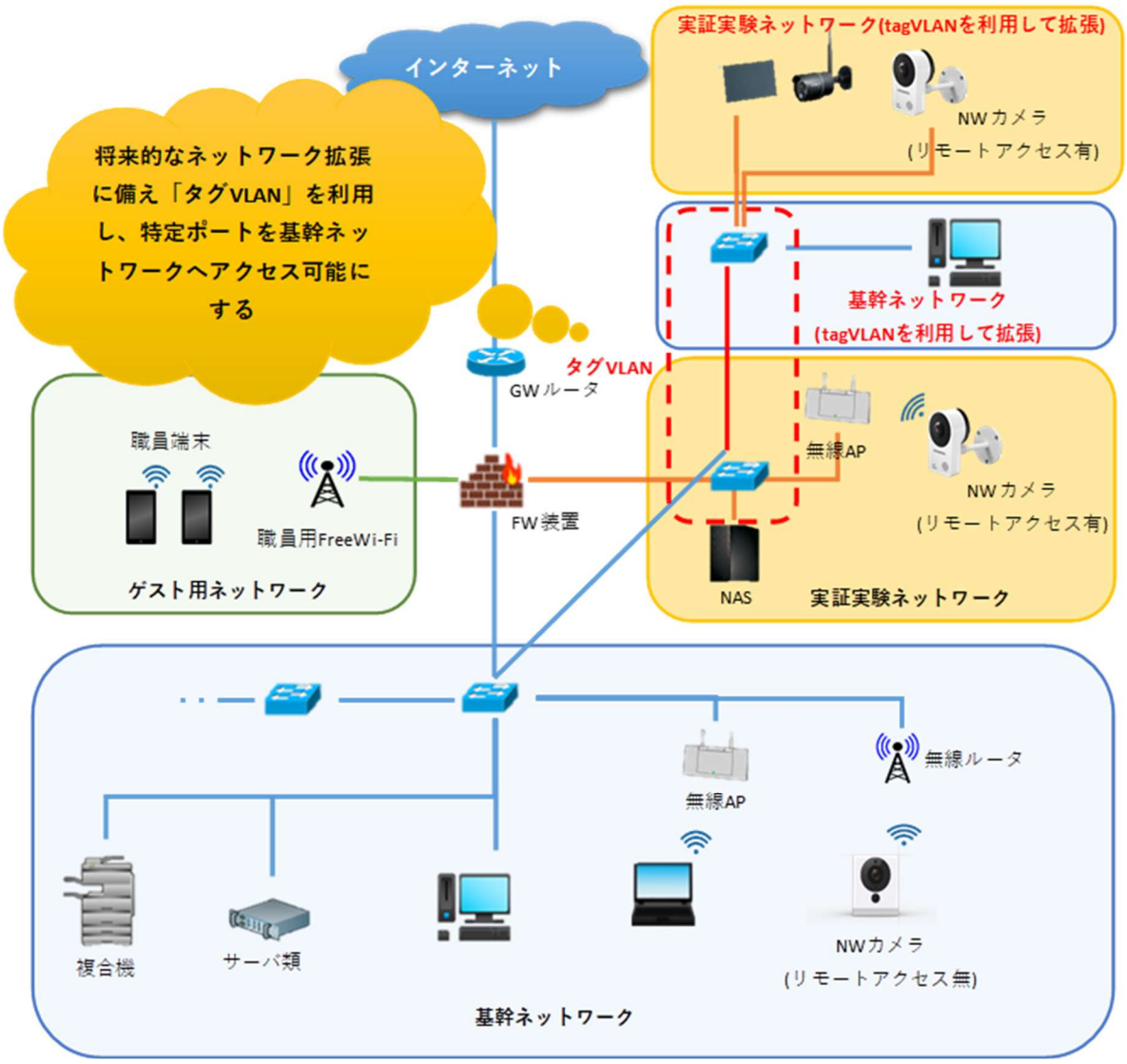


図 5.2.5-7 タグ VLAN を用いたネットワーク拡張のイメージ

【(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。

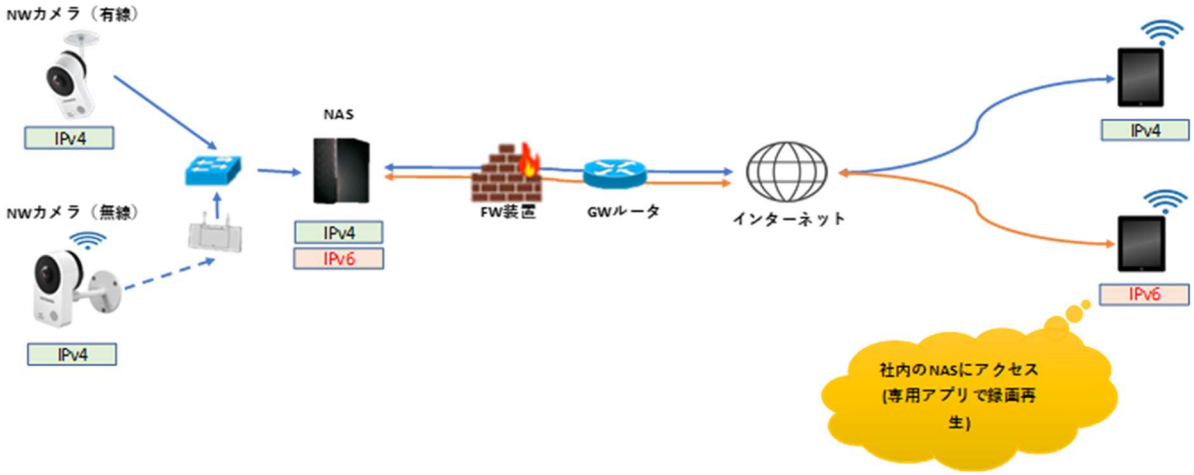


図 5.2.5-8 ネットワークカメラとNASの録画連携イメージ

【(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

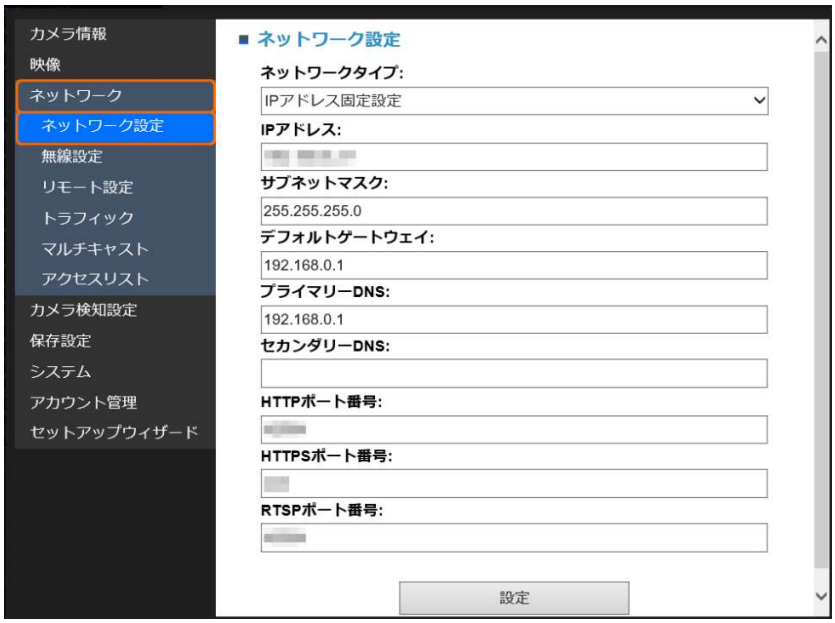
設定	機器等	仕様例	備考
IPv4	無線ルータ	BUFFALO WSR-2533DHP3-BK	・ネットワークカメラの無線接続
IPv4	無線アクセスポイント	BUFFALO WAPS-1266	・ネットワークカメラの無線接続
IPv4	有線ネットワークカメラ	I/O データ TS-NA220	・構内監視
IPv4	無線ネットワークカメラ#1	I/O データ TS-NA220W	・構内監視
IPv4	無線ネットワークカメラ#2	ATOM ATOM Cam	・映像記録撮影
IPv4	無線ネットワークカメラ#3	マスプロ WHC7M3/10M3	・映像記録撮影
IPv4	センサー内蔵温度計	T&D 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	【基幹ネットワークのファイアウォール設定】 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

(2) IoT 機器の設定

項番	設定内容の詳細
1	【ネットワークカメラ#1～3 の設定】 

項番	設定内容の詳細
2	【NAS の設定(IPv4)】  【NAS 設定(IPv6)】 

(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	【IPv6 アドレスの有効化設定】 ネットワーク設定で IPv6 を利用可能にする。 「ルータ＋スイッチ」を作成する。 名前:任意の名称 ルータ:「はい」 IPv6 アドレス:「有効」 その他はデフォルトを指定する。 ※「IPv6 の逆引き設定」は必須ではないため、設定なし。 ※参考 https://manual.sakura.ad.jp/cloud/network/switch/ipv6.html ・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	【クラウド環境のファイアウォール設定】 ・「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。 ※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) 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。
3	ConoHa VPS に割り振られた IPv6 アドレスを、DNS に正引き登録する。

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。

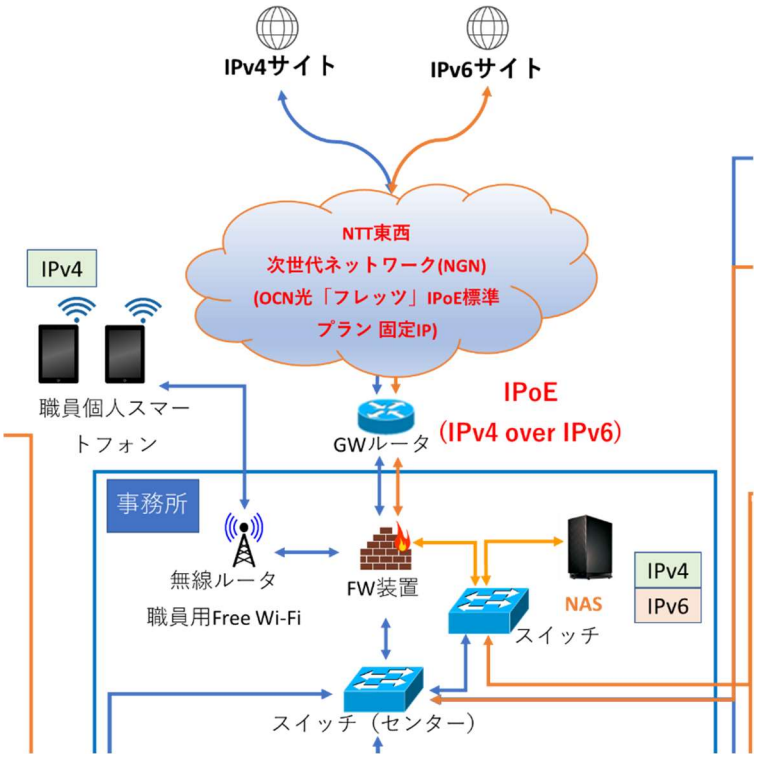


図 5.2.6-1 IPv4 経路と IPv6 経路

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。

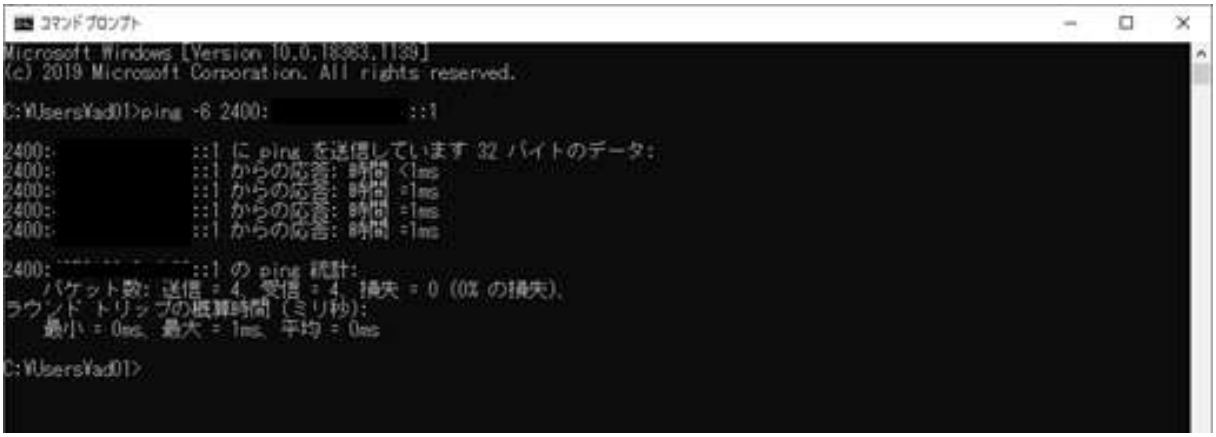


図 5.2.6-2 IPv6 で ping 応答あり(GW ルータ)

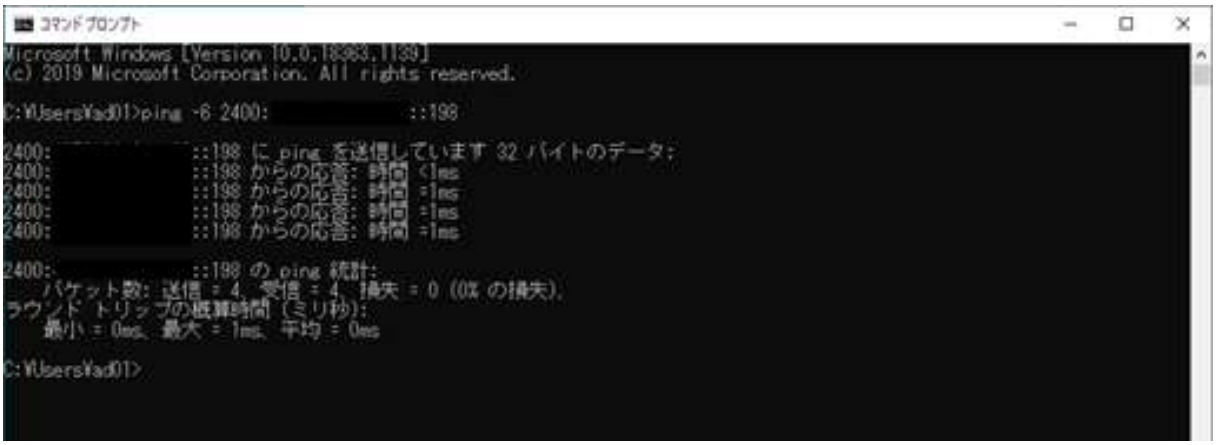


図 5.2.6-3 IPv6 で ping 応答あり(FW 装置)

【#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。

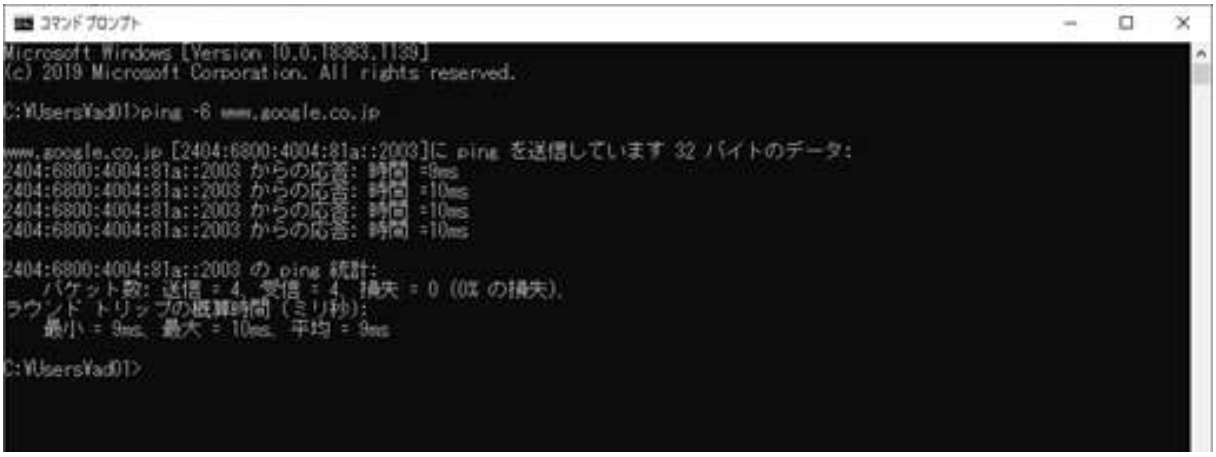


図 5.2.6-4 IPv6 で ping 応答あり(外部サイト)

【#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。

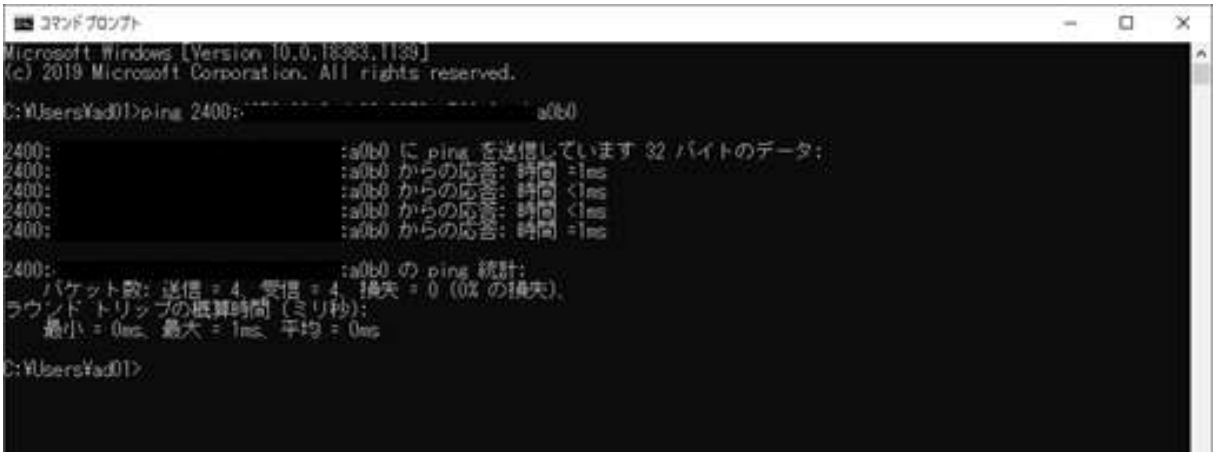


図 5.2.6-5 IPv6 で ping 応答あり(NAS)

【#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。

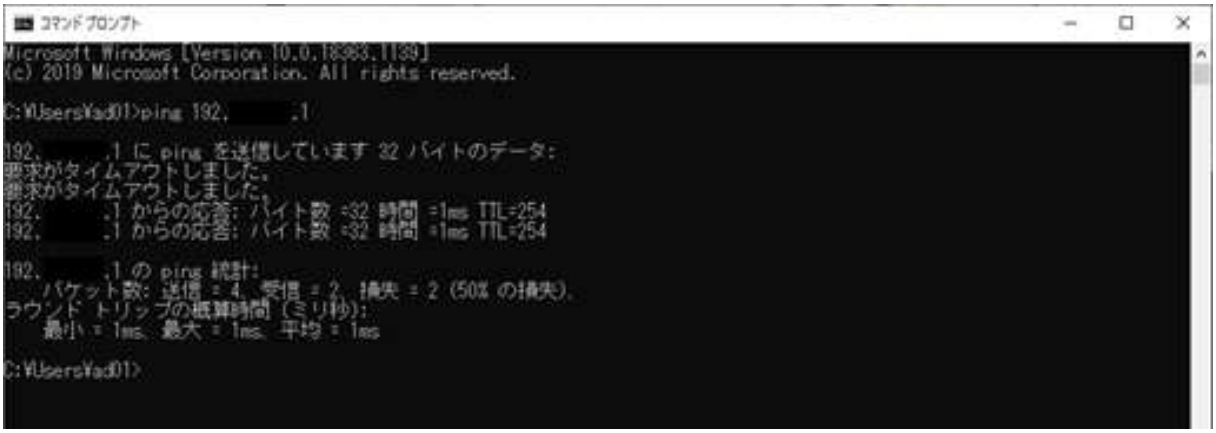


図 5.2.6-6 VLAN で IPv4 の ping 応答が不安定(2回タイムアウト後、2回応答あり)

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。

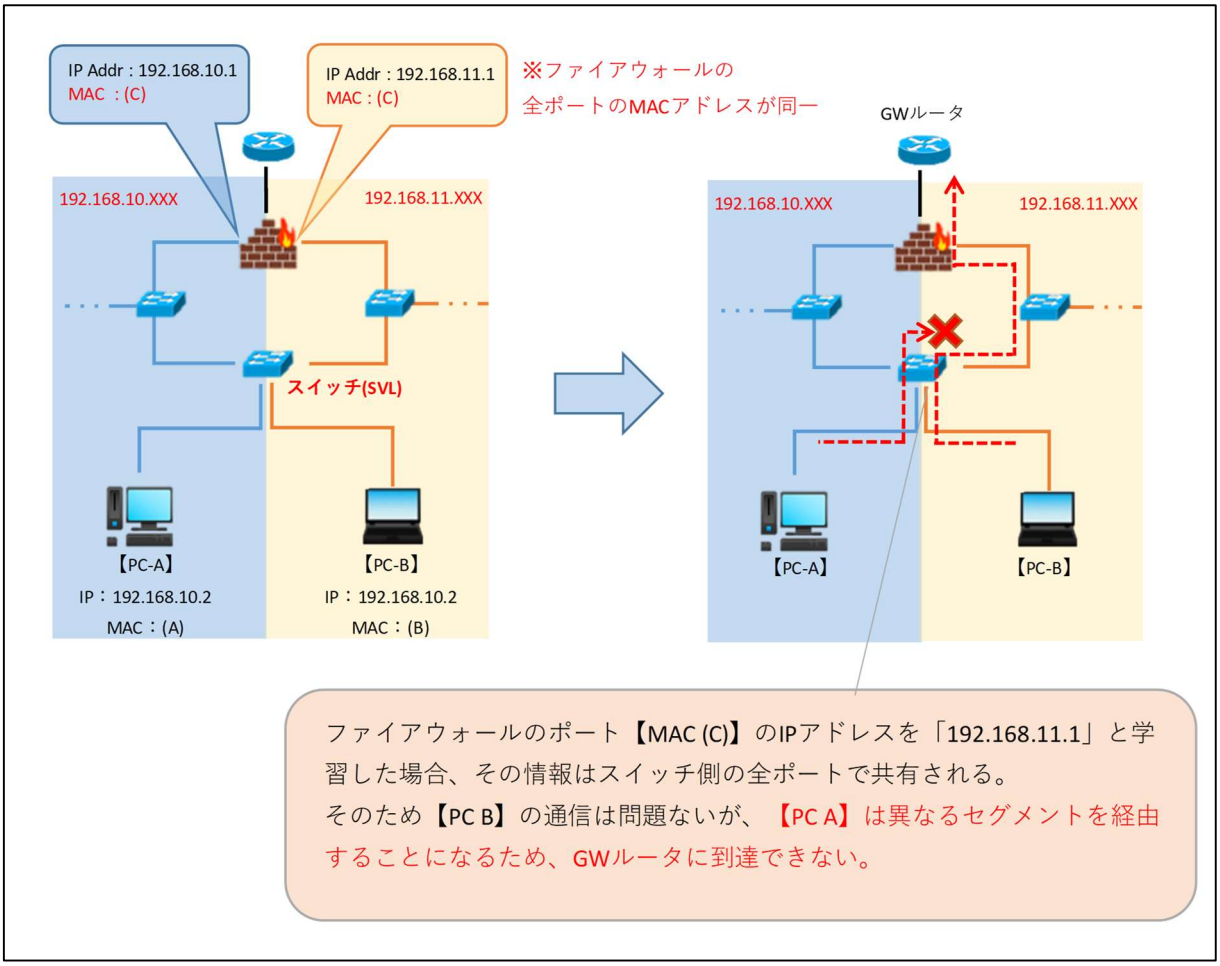


図 5.2.6-7 SVL 方式による MAC アドレス学習結果の例

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。

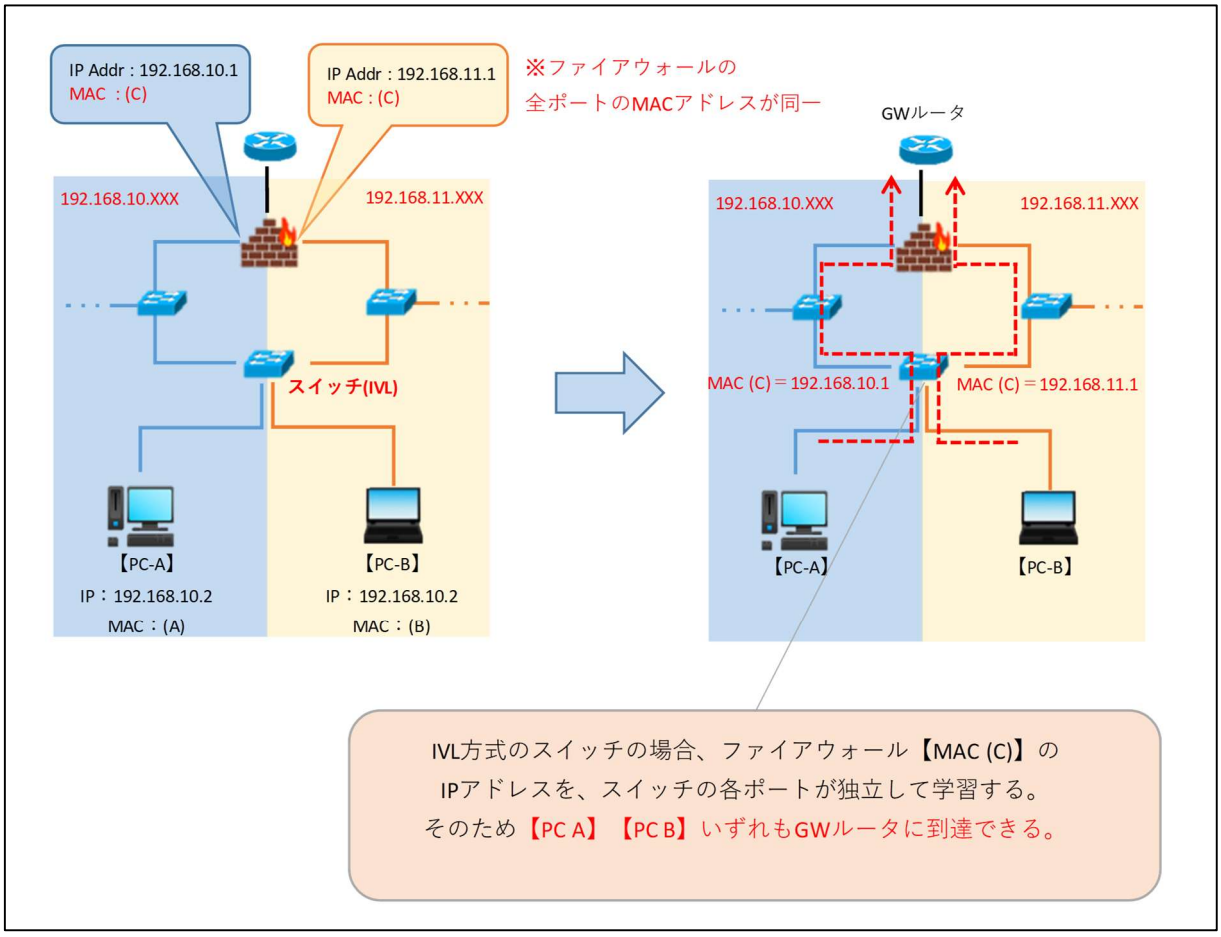


図 5.2.6-8 IVL 方式による MAC アドレス学習結果の例

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。

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。

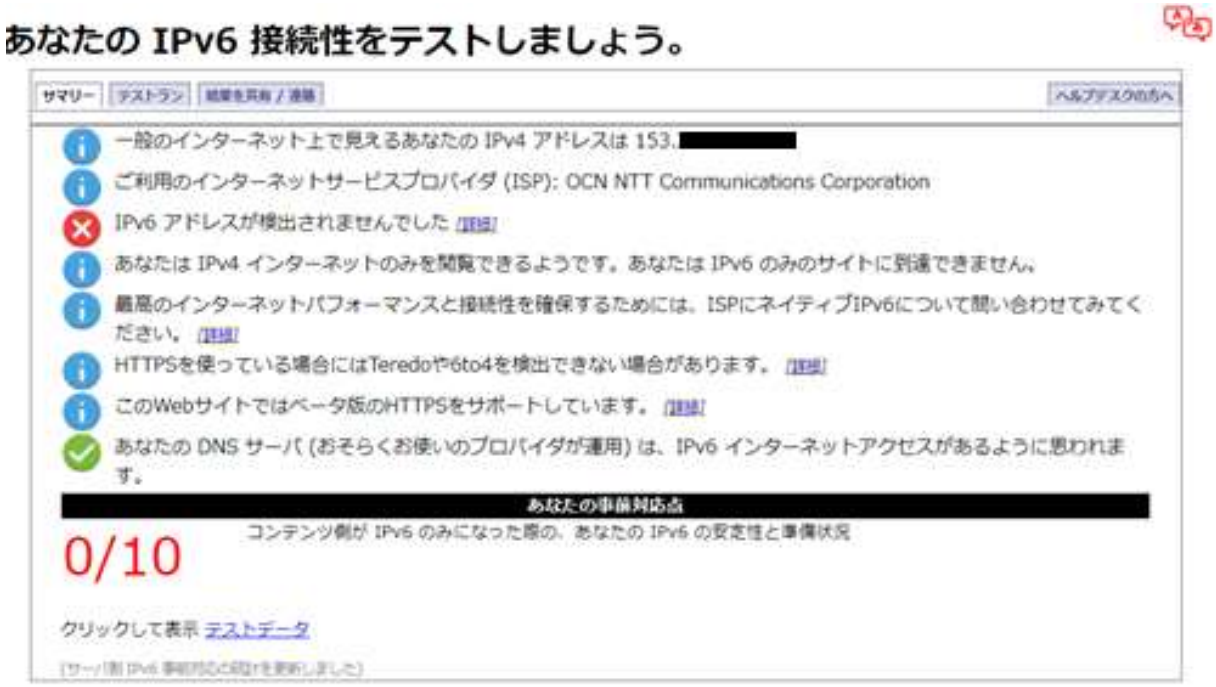


図 5.2.6-11 IPv4 でインターネット接続可能(VLAN 環境)

【#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。

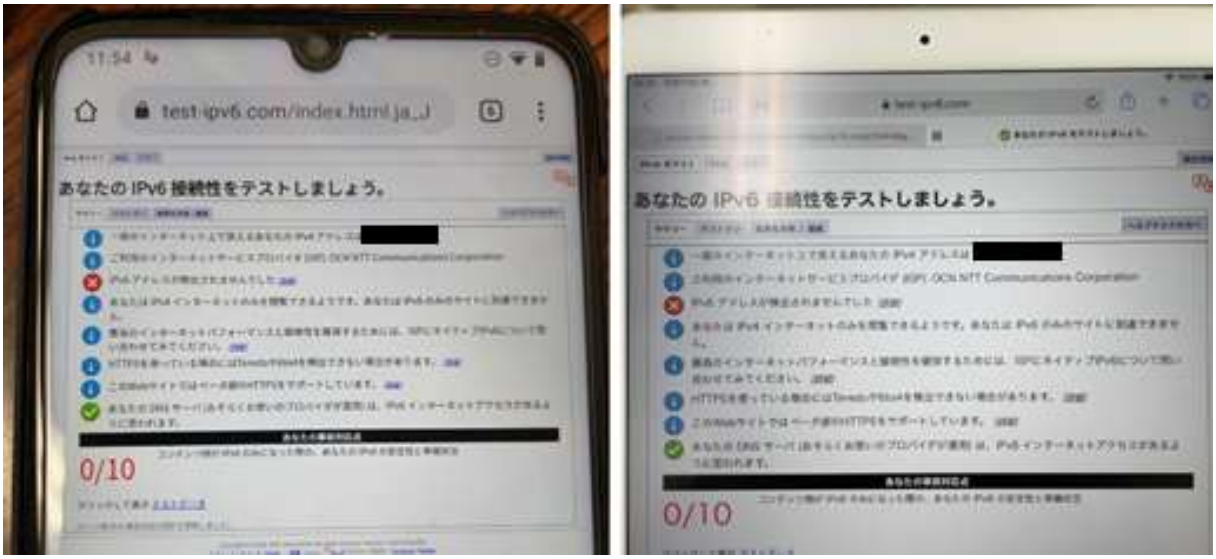


図 5.2.6-12 ゲスト用 Wi-Fi 環境でインターネット接続可能

(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。

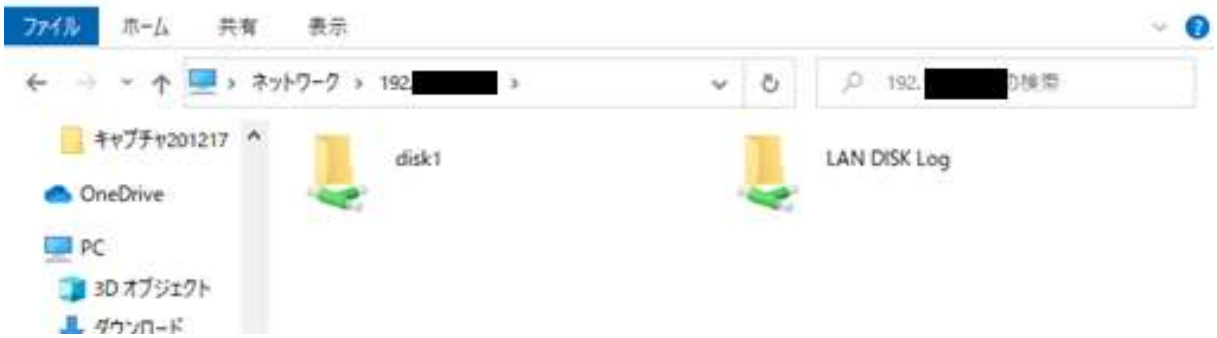


図 5.2.6-13 NAS のファイル参照(IPv4 アドレス指定)のイメージ

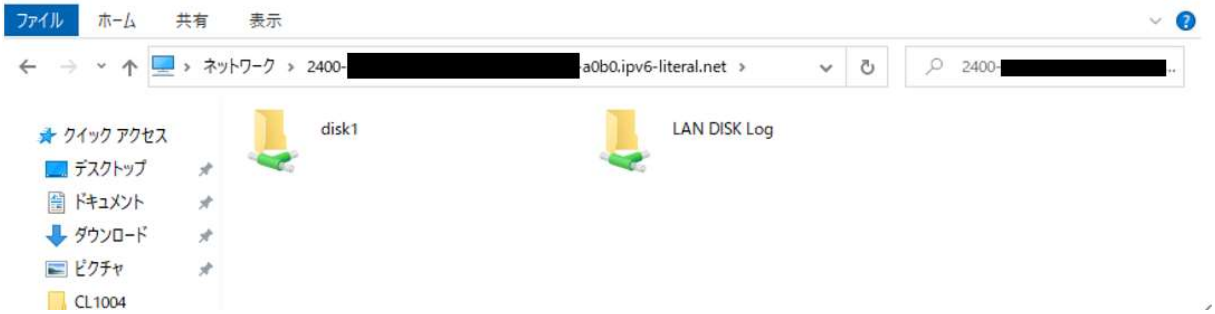


図 5.2.6-14 NAS のファイル参照(IPv6 アドレス指定)のイメージ

(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。

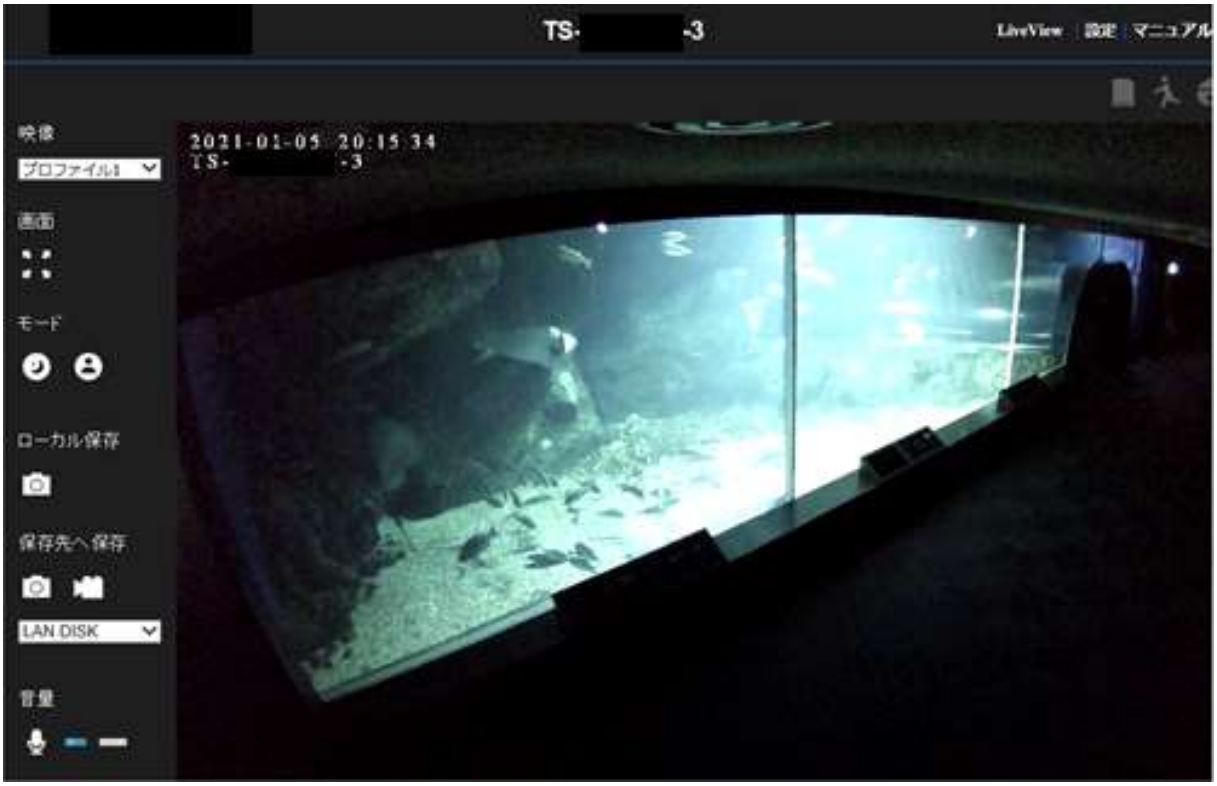


図 5.2.6-15 ネットワークカメラのライブ映像参照結果

【#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。

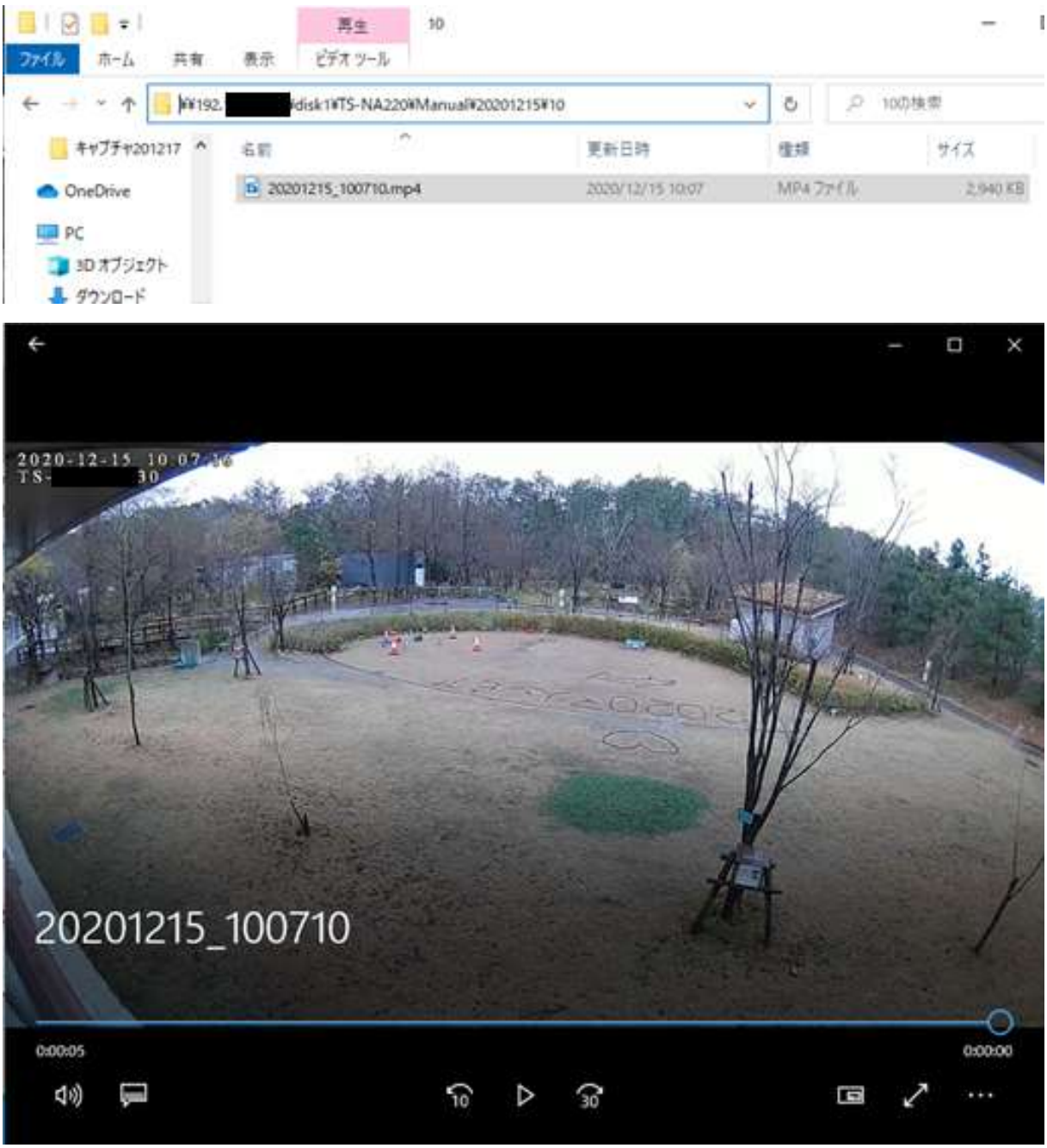


図 5.2.6-16 NAS 録画映像の再生結果

【#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。

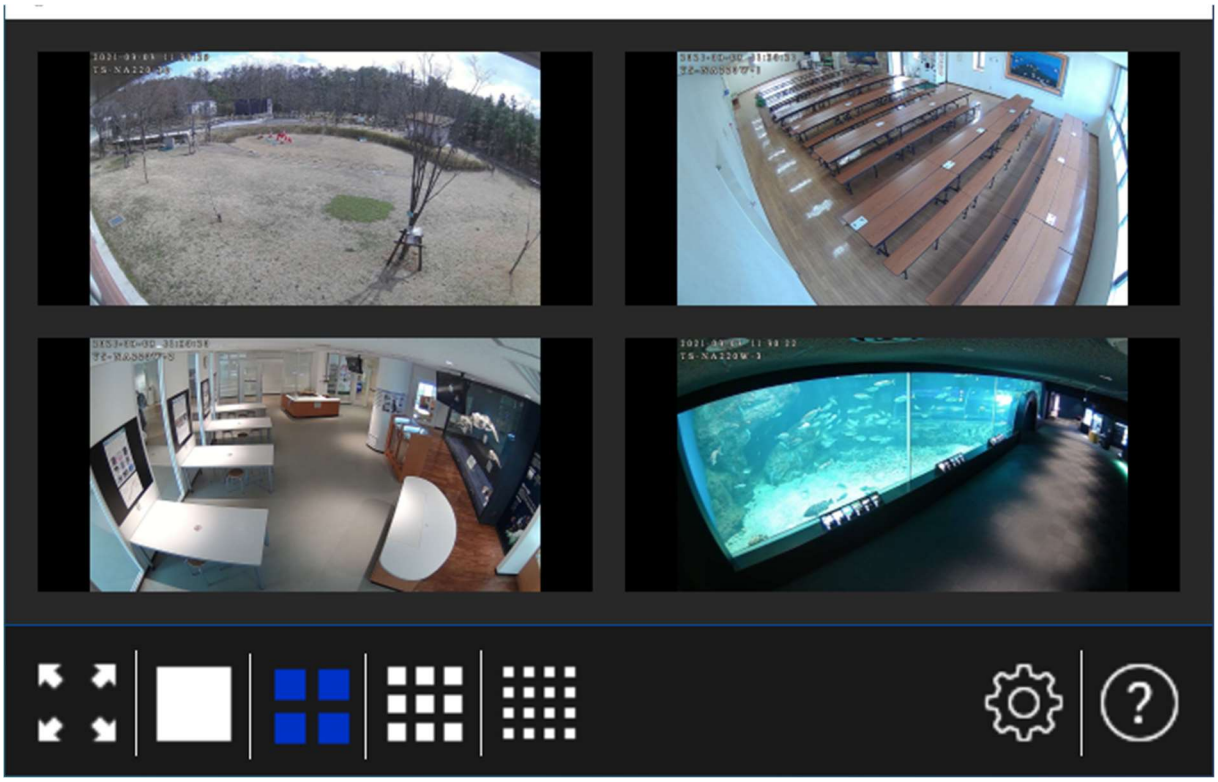


図 5.2.6-18 ビューワーアプリケーション実行結果(Qwatch Monitor)

【#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。

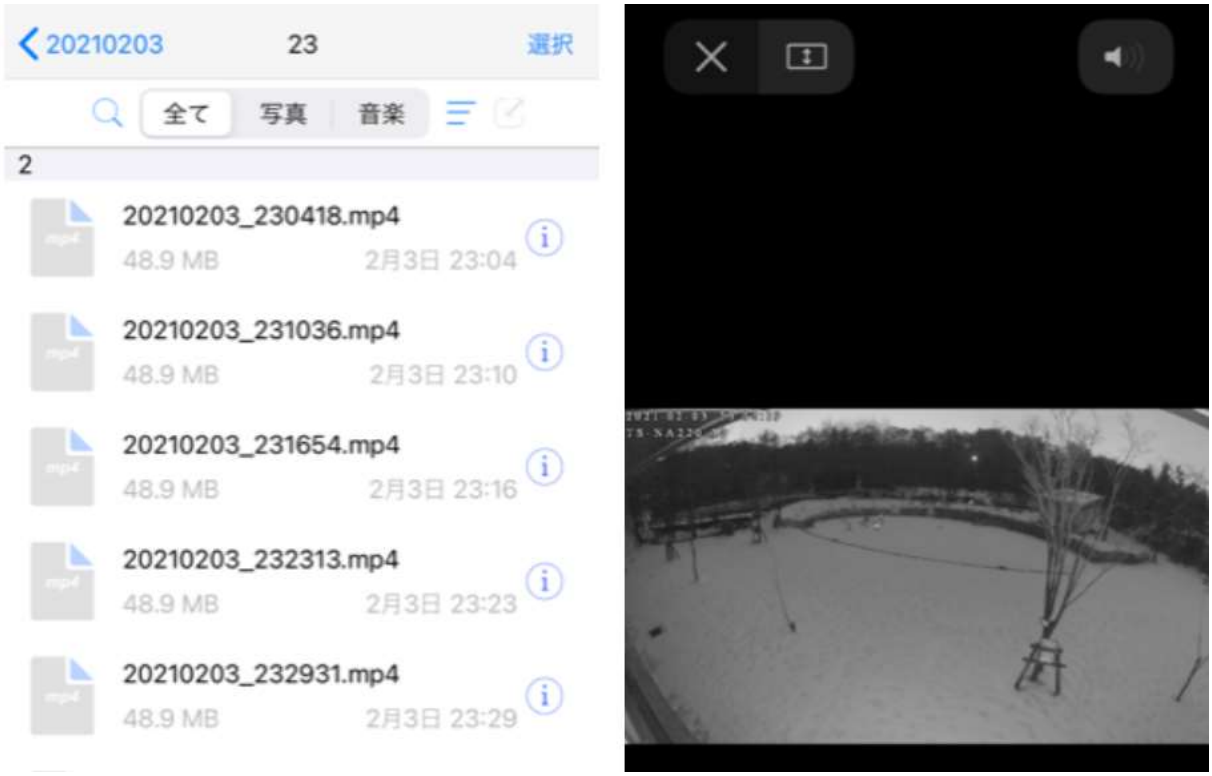


図 5.2.6-21 NAS のリモート接続結果 2(左:ファイル選択、右:動画ファイル再生)

スマートフォンから NAS へのリモート接続のおける 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。

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。

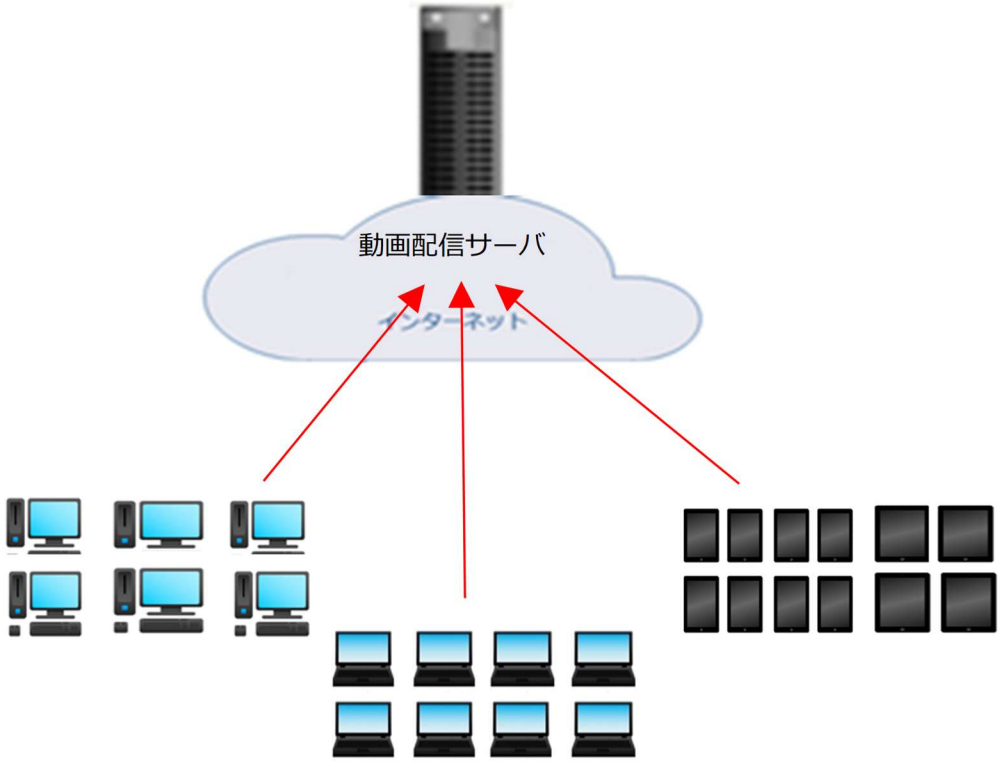


図 5.2.6-23　クラウドサービスの検証イメージ図

(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。

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。

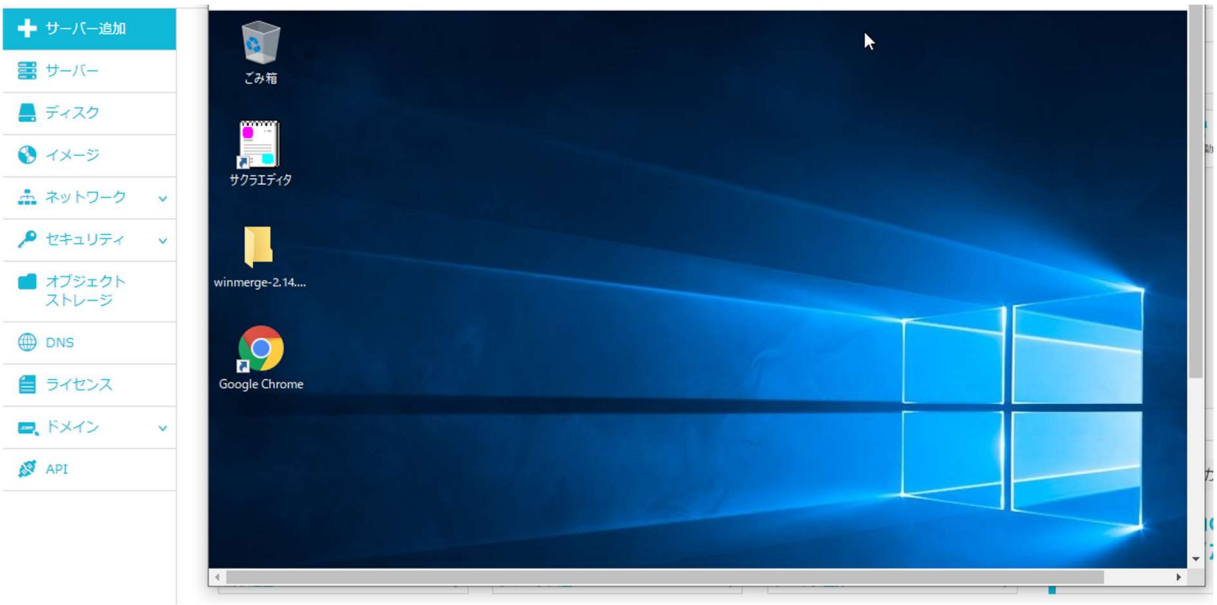


図 5.2.6-26 仮想環境のデスクトップ画面表示

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。

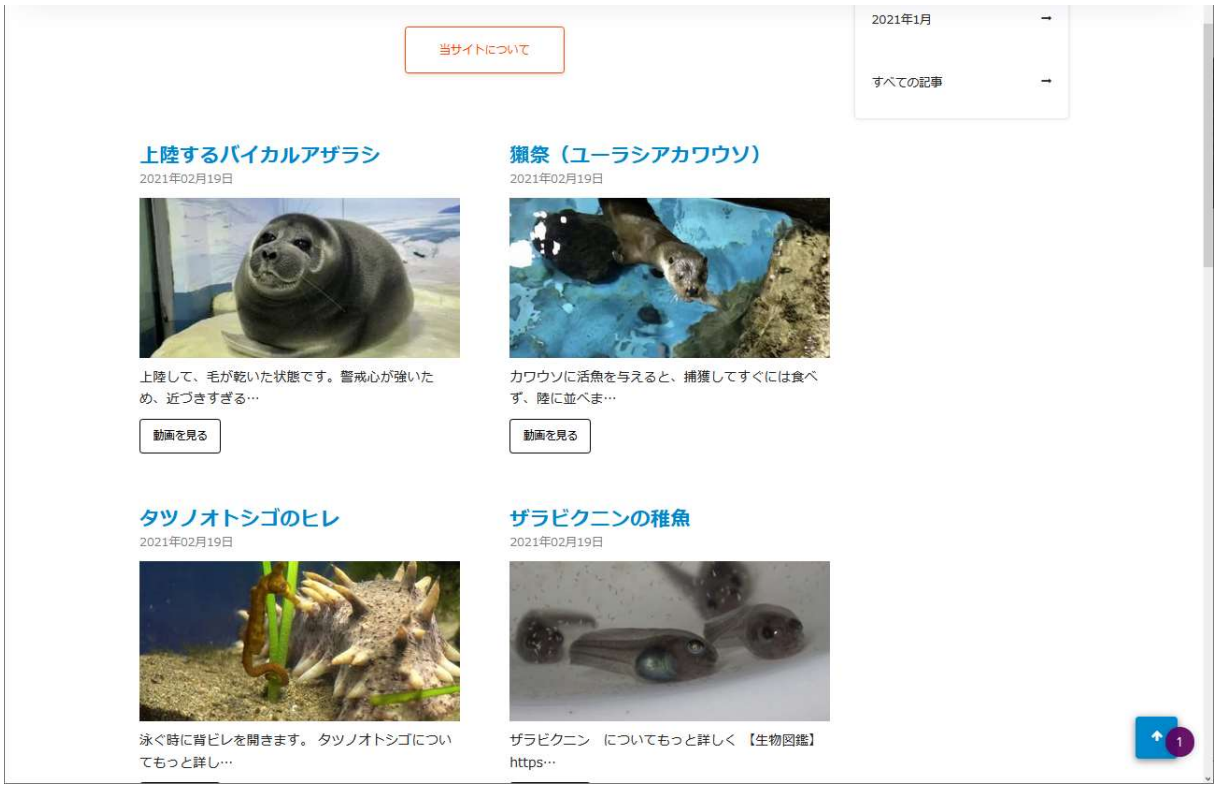


図 5.2.6-28 動画配信用クラウドサービスのアクセス結果

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しての集計結果を表 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、機器メーカのサポート等に確認した結果、IPv6 対応が十分でないことが判明した課題と対応の事例を示す。

(2) IPv6 対応における留意事項(構築時の Tips)

本検証において実際に発生した IPv6 関連のトラブルシュート事例をもとに、IPv6 対応において普遍的に留意すべき点を示す。

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。

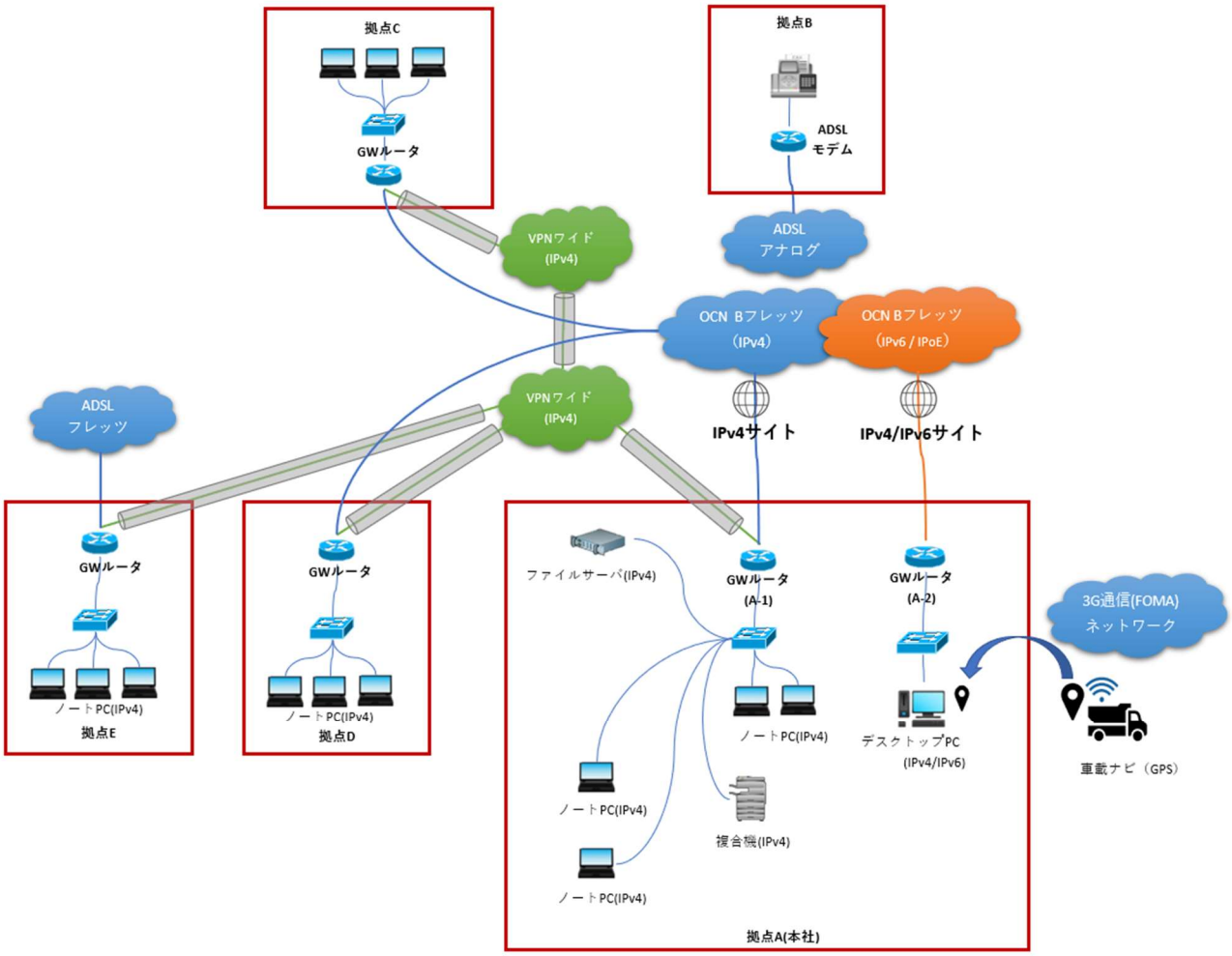


図 5.3.2-1 ネットワーク構成図イメージ

(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。

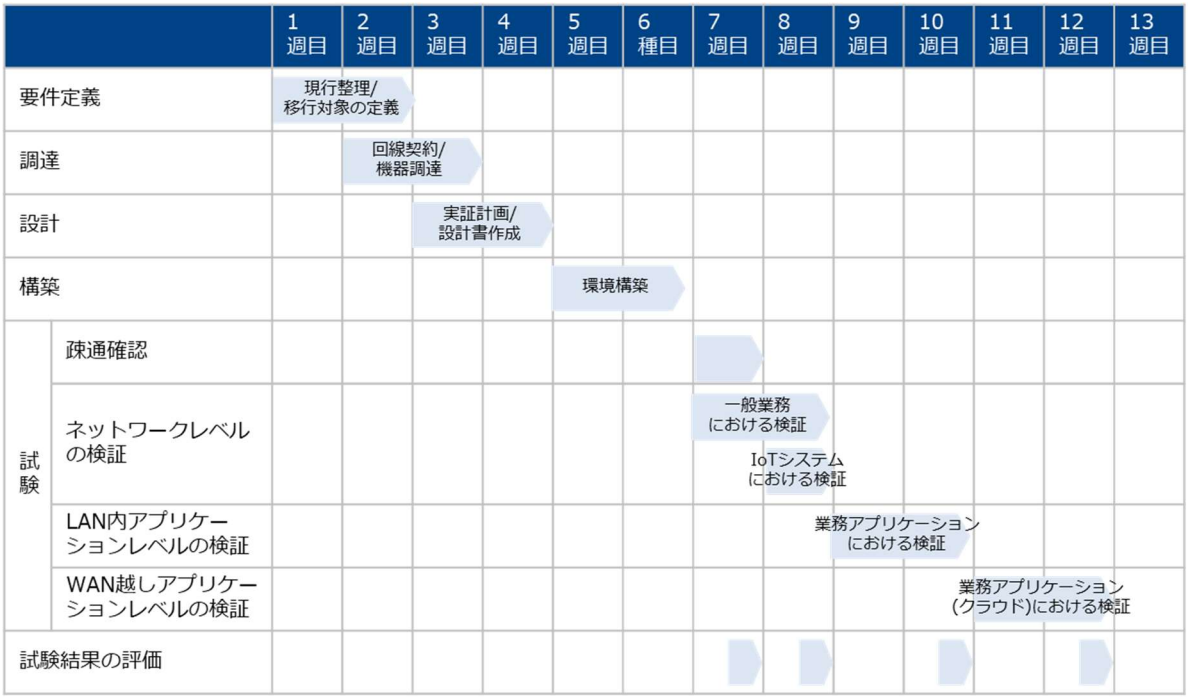


図 5.3.3-1 スケジュールイメージ(中小企業 C)

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 DNS[61]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、アドレス変更に即座に追随して 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。

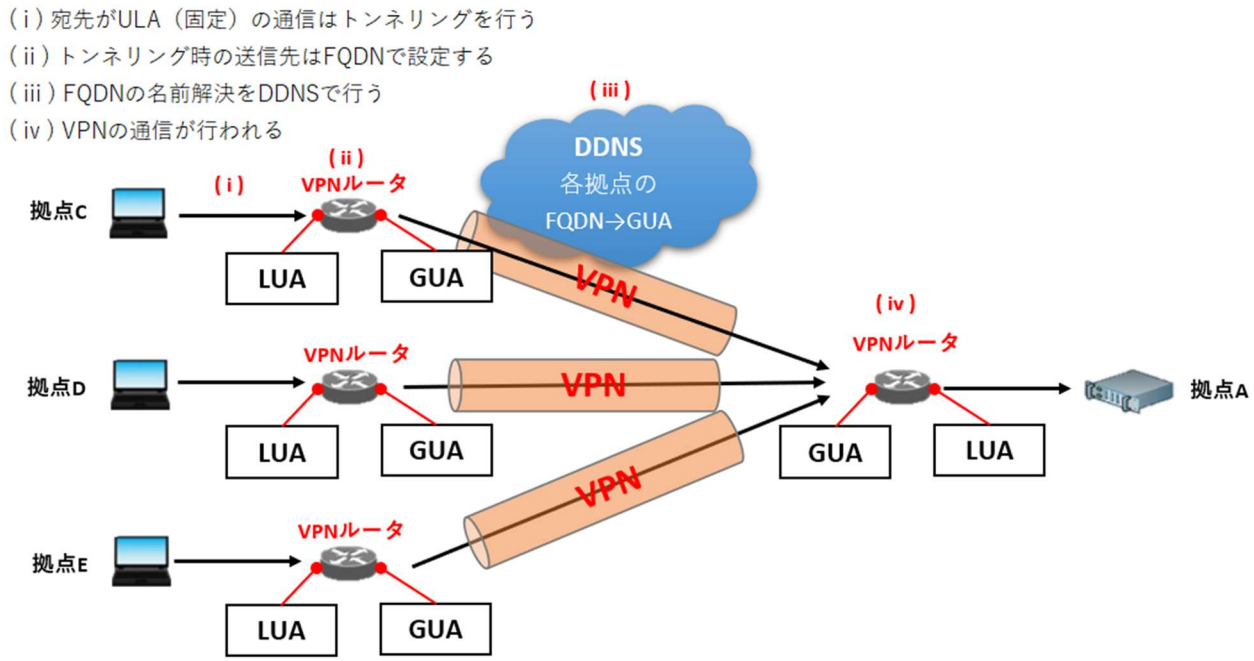


図 5.3.4-1 ULA および GUA を利用したインターネット VPN 通信の流れ

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、クライ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 種類を組み合わせて構築する。

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。

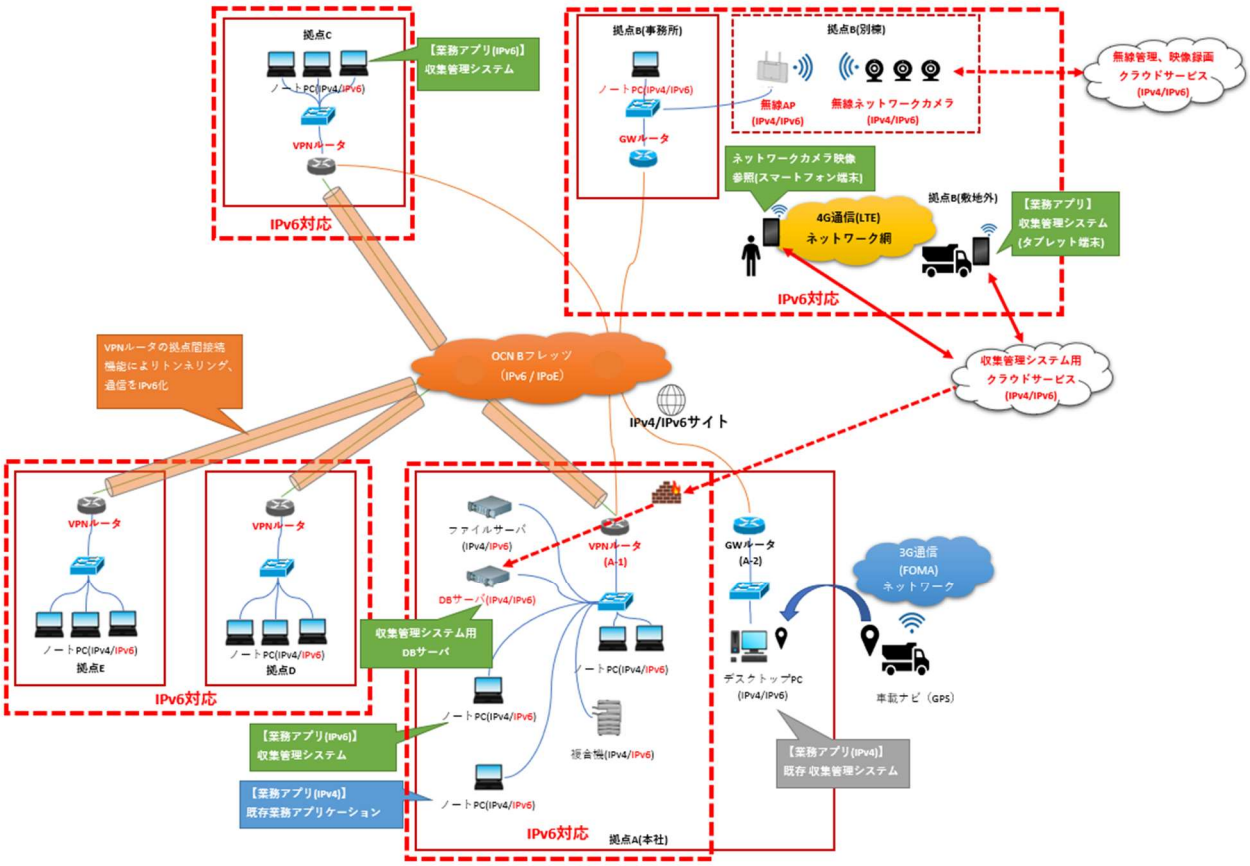


図 5.3.4-2 IPv6 対応後の C 社のシステム構成図

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	Buffallo	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 対応を謳ってはいないが、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経由して拠点内の 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）

・Safie（セーフィー株式会社）

・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。

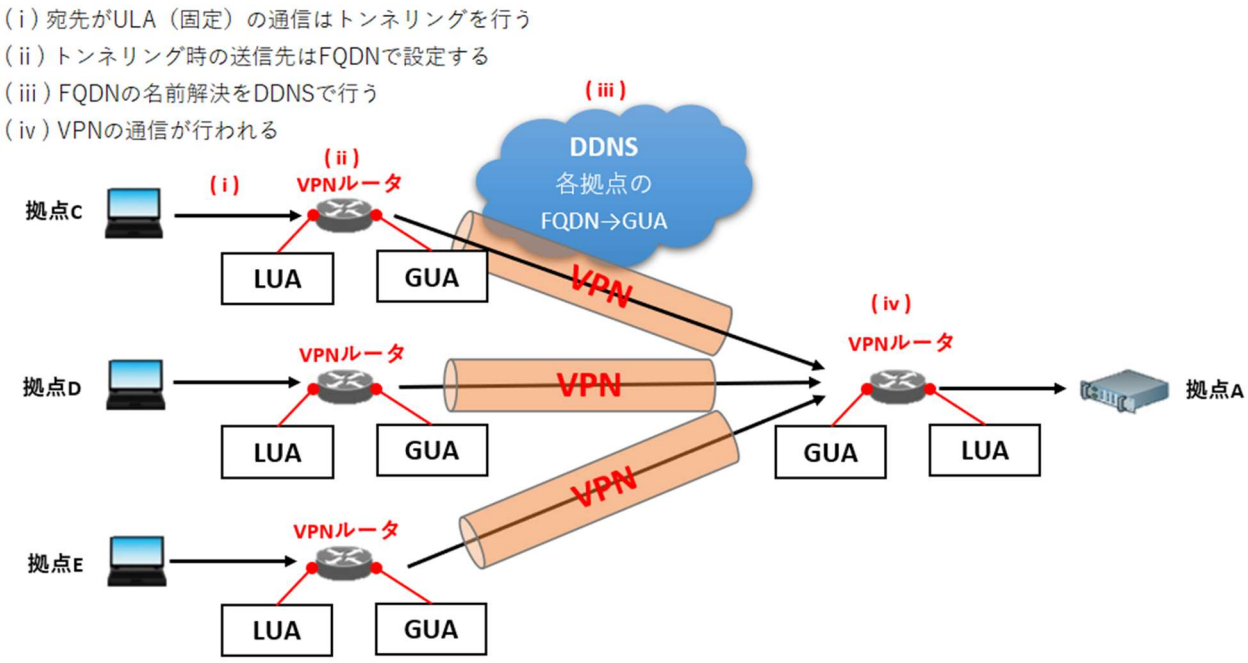


図 5.3.5-1 ULA および GUA を利用したインターネット VPN 通信の流れ(再掲)

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	【基本ルーティング設定】 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" 【VPN 設定】 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 ※上記を拠点 D、E も同様に設定

【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 .

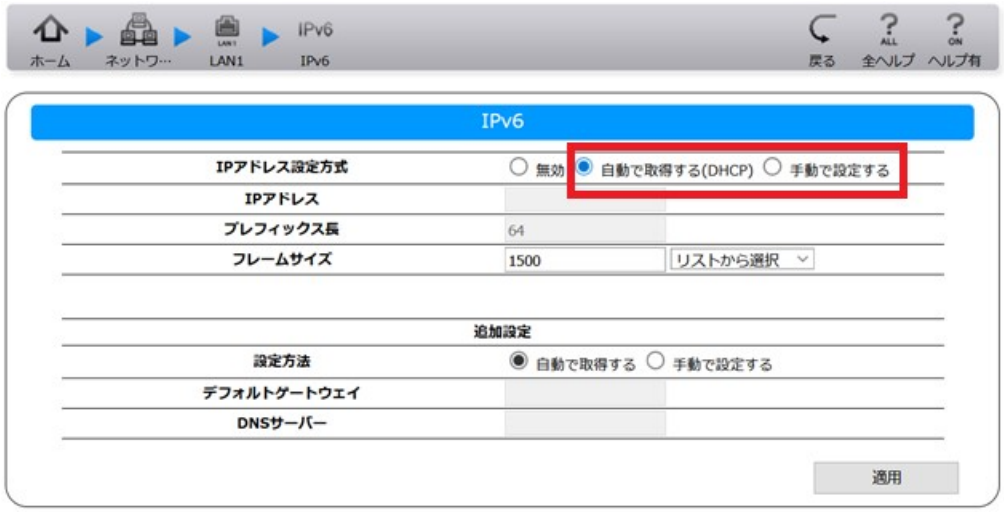
dns server select 500000 <既存 DNS サーバ IPv6 アドレス> aaaa .

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	【ネットワークカメラの設定（AXIS）】  【NAS 設定（IPv6）】 ※自動、または手動で設定する 

項番	設定内容の詳細
	【無線アクセスポイント設定（ブリッジモード）】 ※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。 

(3) クラウド環境の設定

項番	設定内容の詳細
1	【VPS＋Windows における、IPv6 の有効化設定】 PowerShell より、以下のコマンドを実行する # Enable-NetAdapterBinding -Name "Global" -ComponentID ms_tcpip6 ※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

※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。

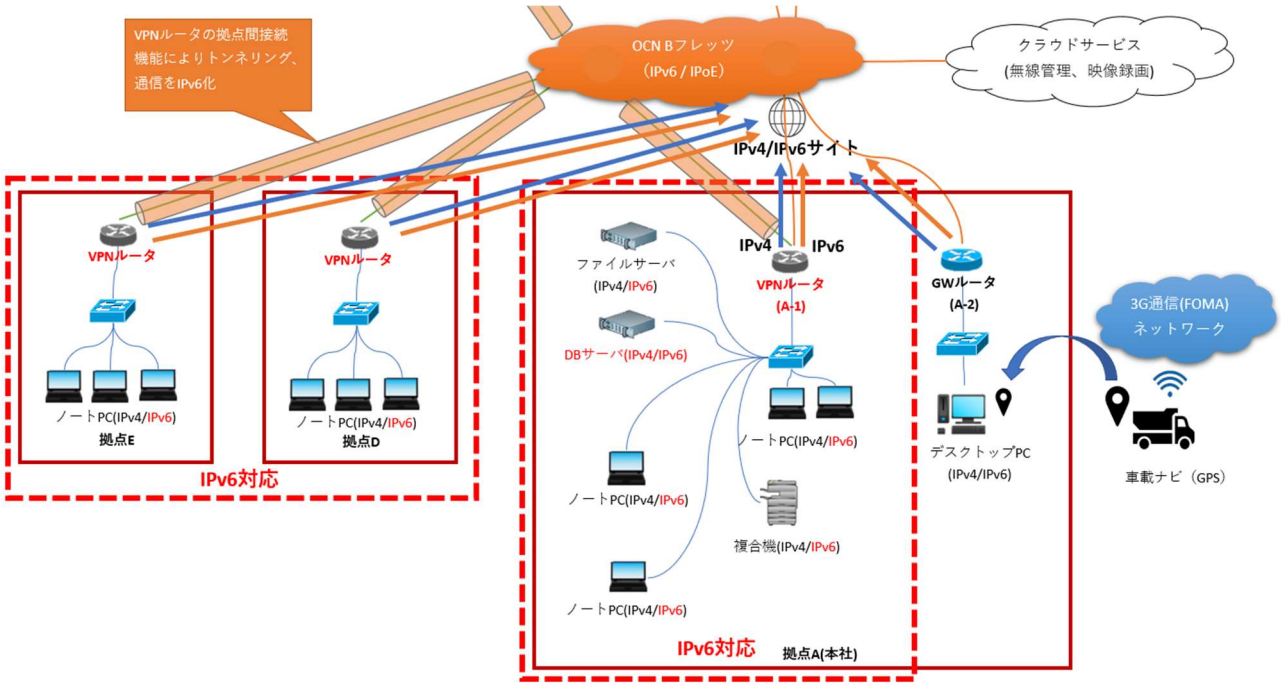


図 5.3.6-1　IPv4 経路と IPv6 経路

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。

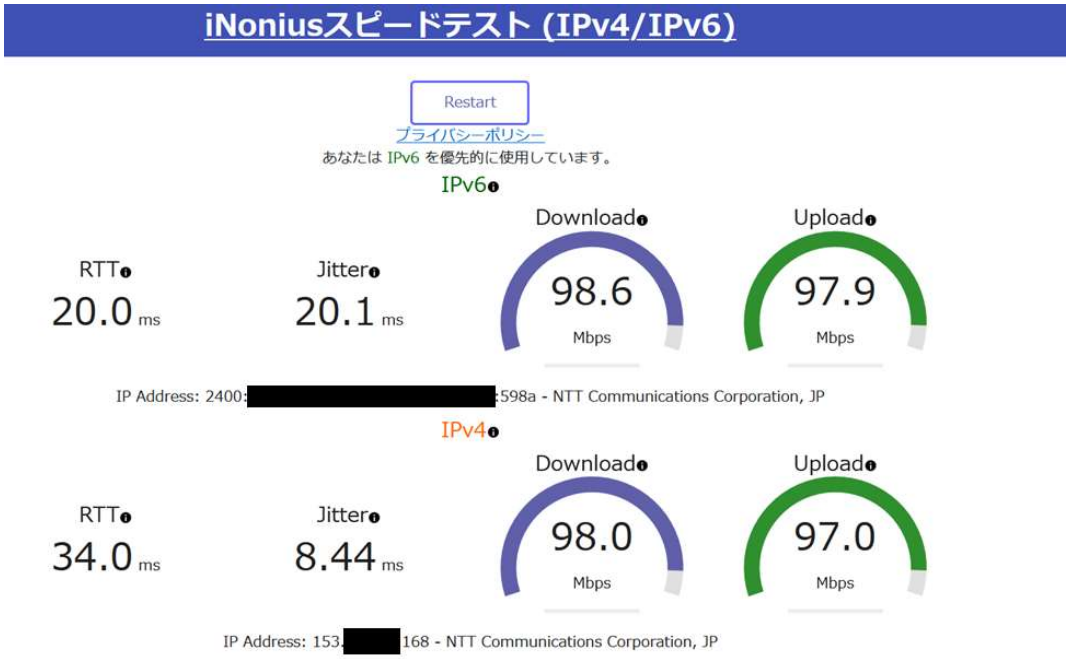


図 5.3.6-4 計測サイトによる IPv4/IPv6 速度計測の実行例

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。

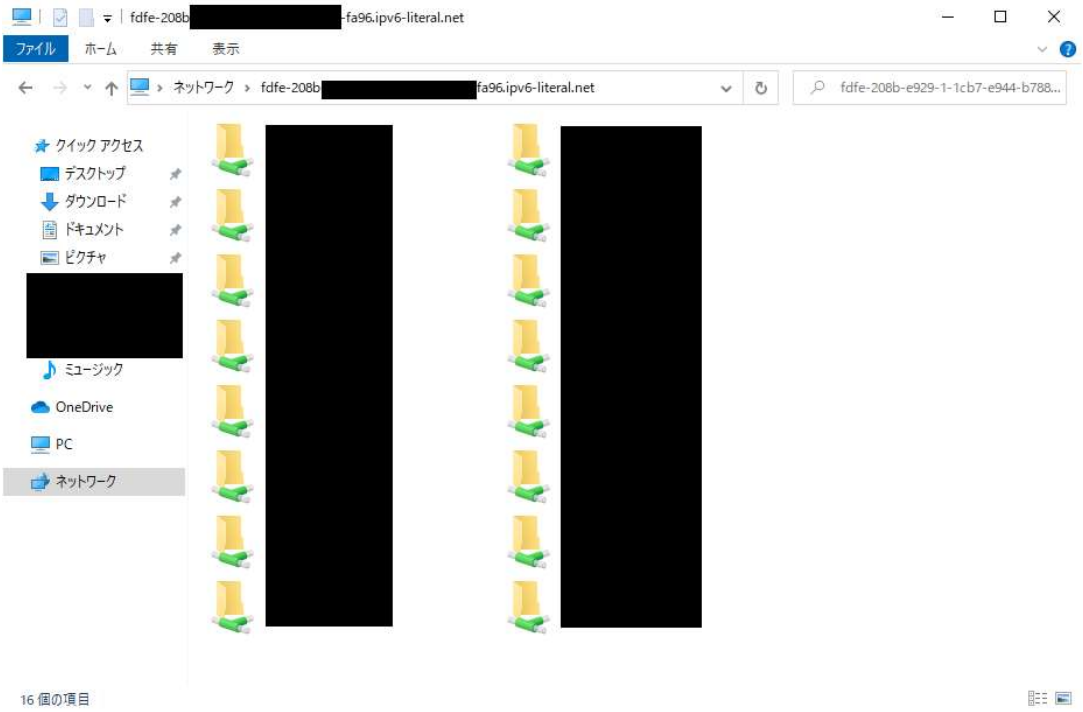


図 5.3-1 IPv6 の UNC 表記による共有フォルダのアクセス例

(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。

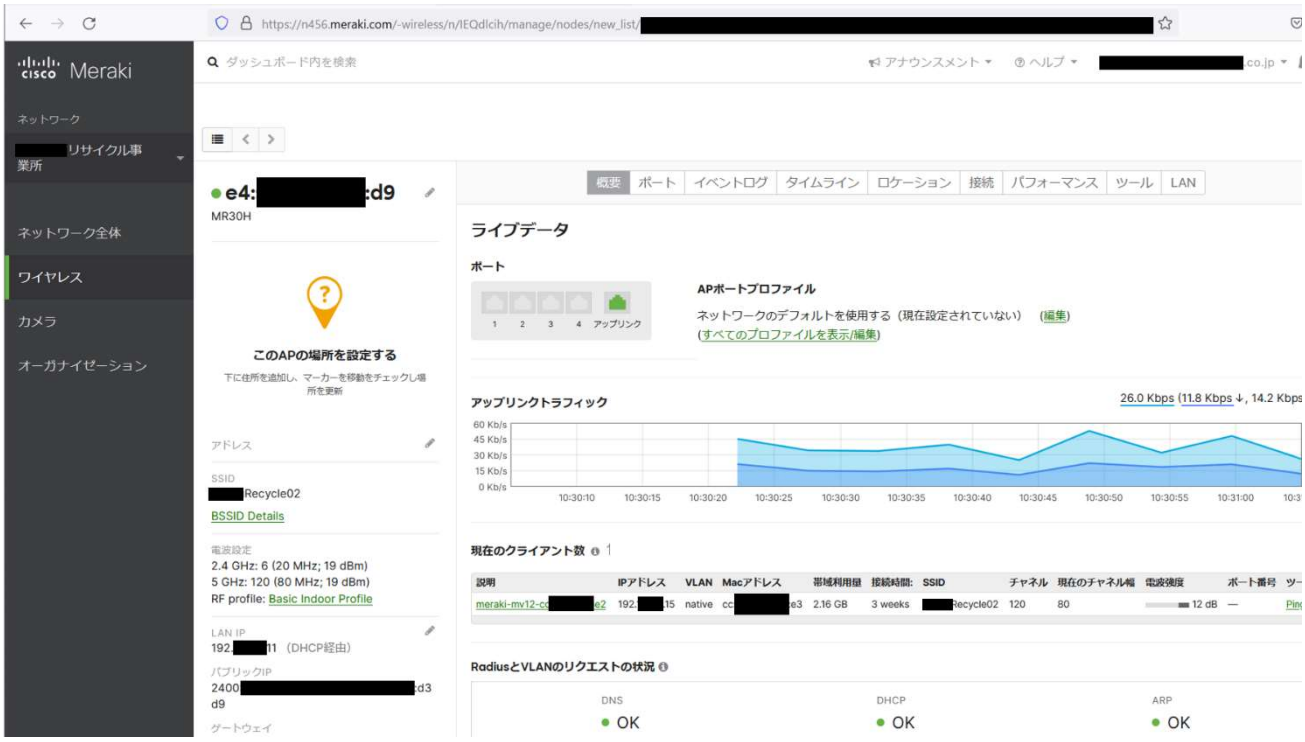


図 5.3.6-5 管理画面上で機器の状態参照の結果

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。

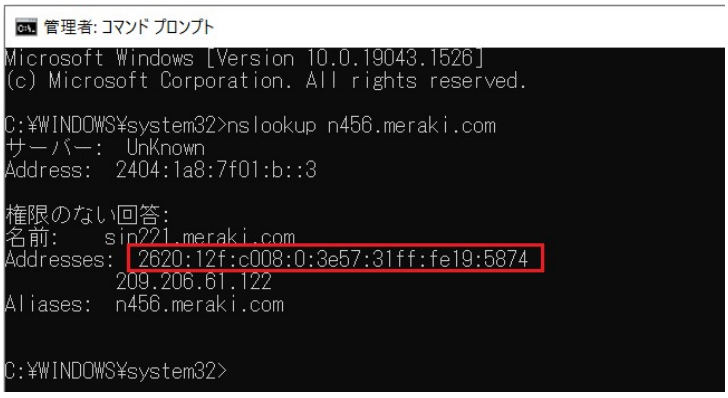


図 5.3.6-6 クラウドサービスの IPv6 アドレス取得結果

※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

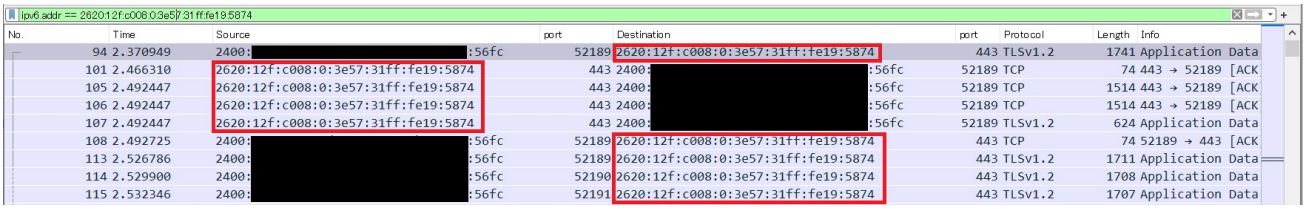


図 5.3.6-7　管理画面にアクセス中のパケットキャプチャの結果

【#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。

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

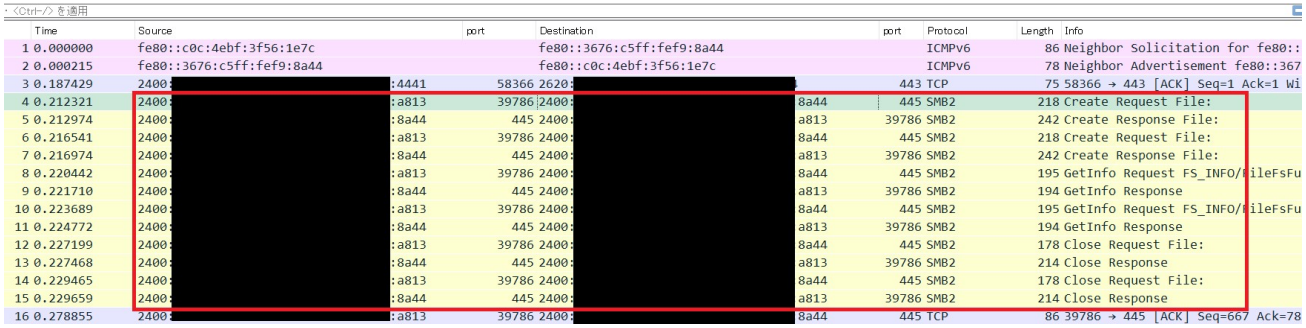


図 5.3.6-9　ネットワークカメラ録画中のパケットキャプチャ結果

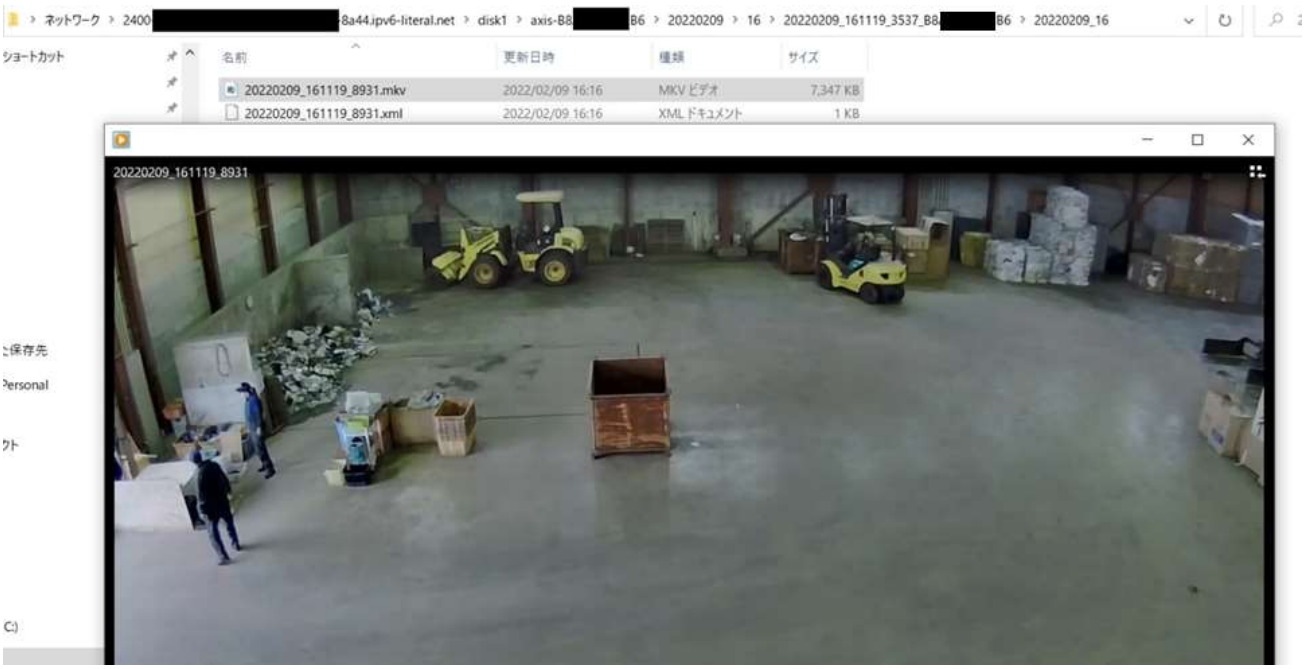


図 5.3.6-10　ネットワークカメラで NAS に録画した映像の参照結果

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

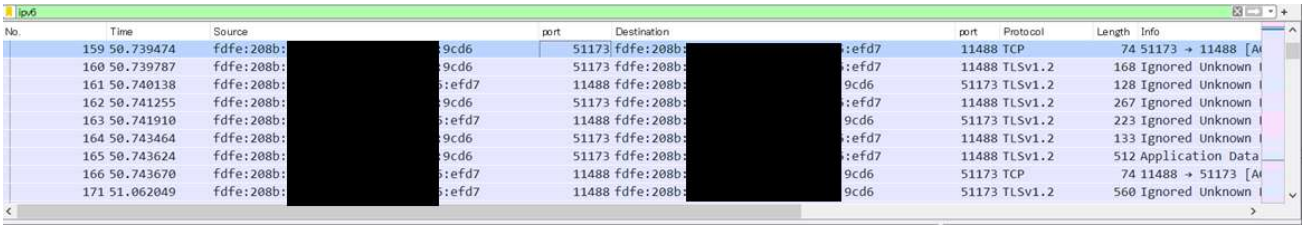


図 5.3.6-12　収集管理システム操作における DB サーバ間のパケットキャプチャ(同一拠点内)

【#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。

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

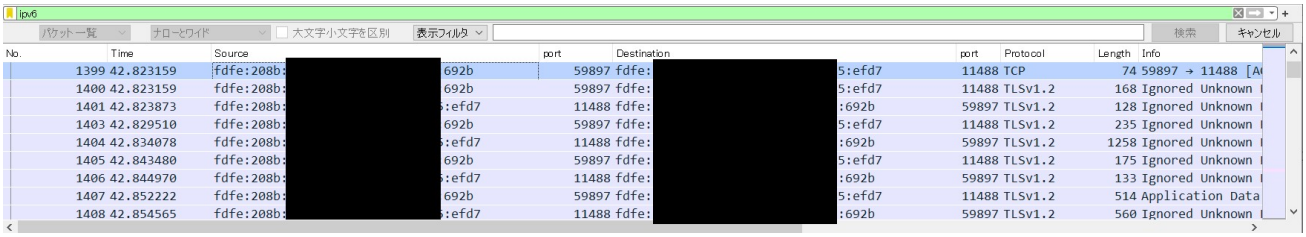


図 5.3.6-14　収集管理システム操作における DB サーバ間のパケットキャプチャ(拠点外から VPN を経由)

【#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。

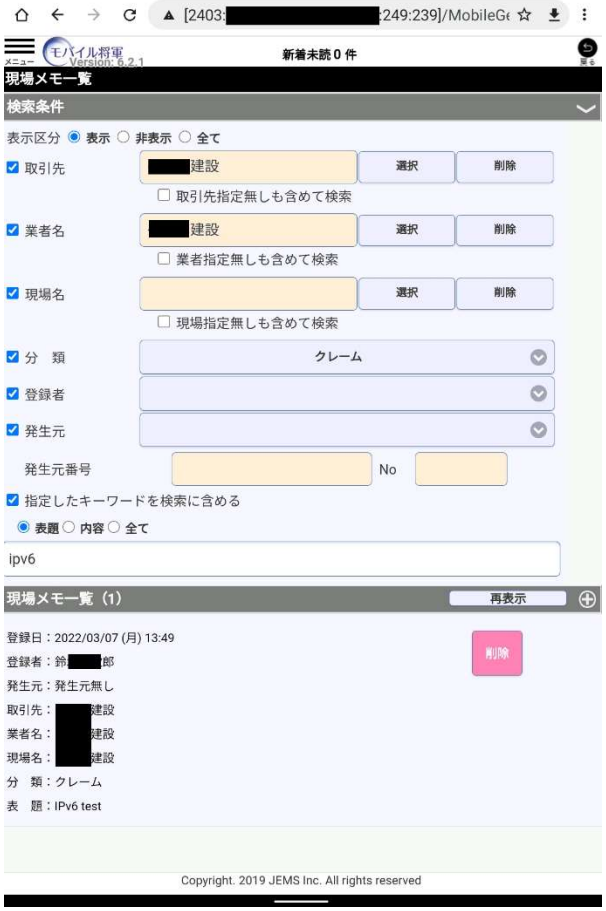


図 5.3.6-15 収集管理システム(モバイル版)の実行結果(インターネット接続)

※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

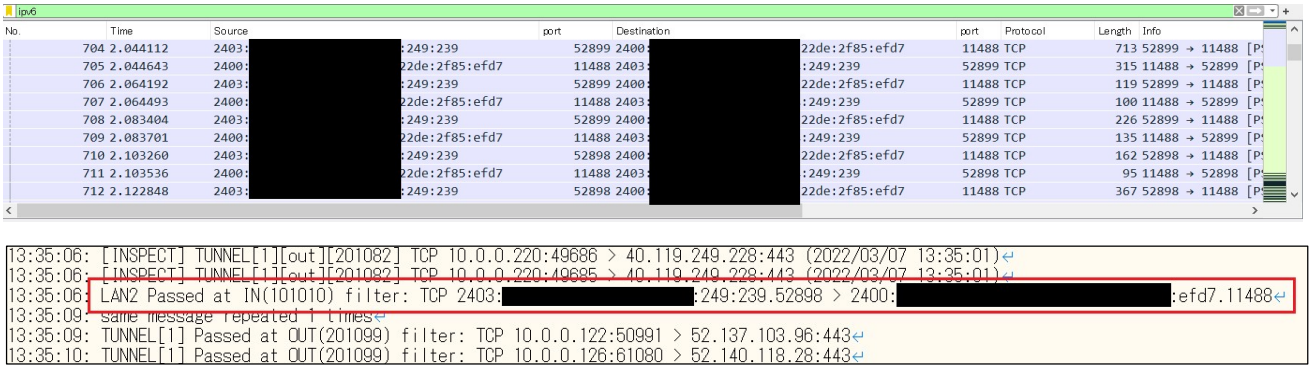


図 5.3.6-16 WEB サーバと本社拠点内 DB サーバ間のパケットキャプチャ、FW ログ

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。

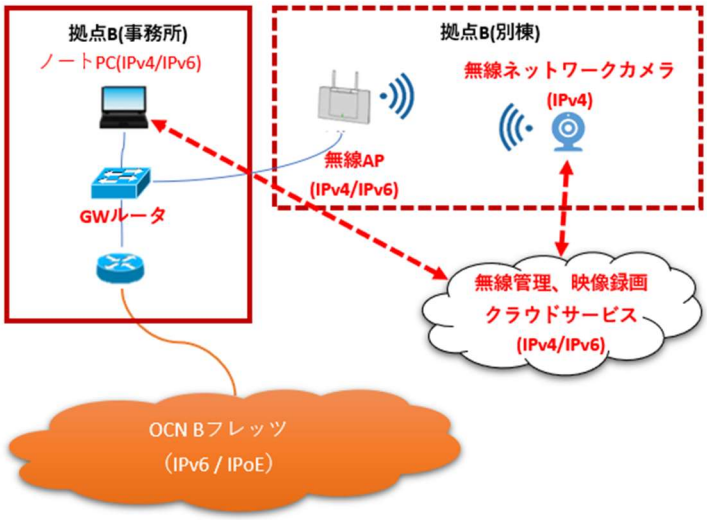


図 5.3.6-17　クラウドサービスの検証イメージ図

(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。

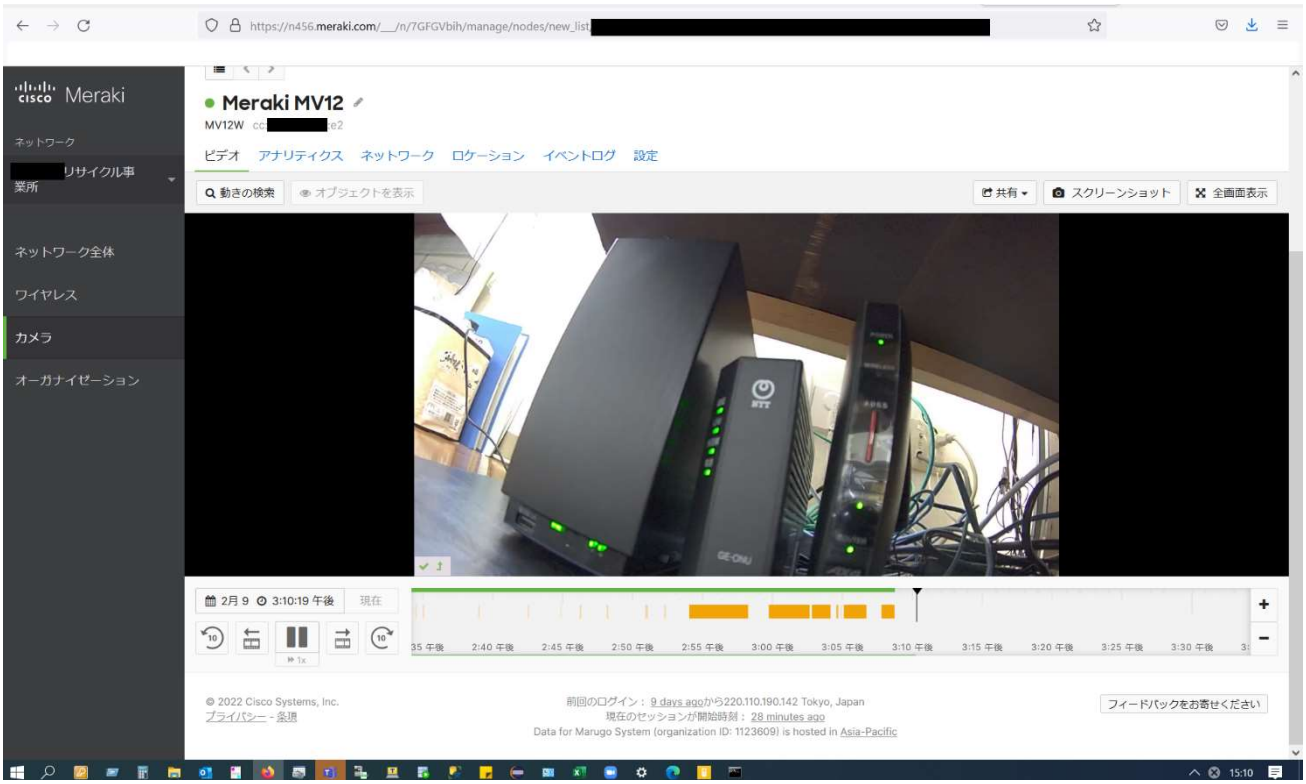


図 5.3.6-18 クラウドサービスの録画映像参照機能

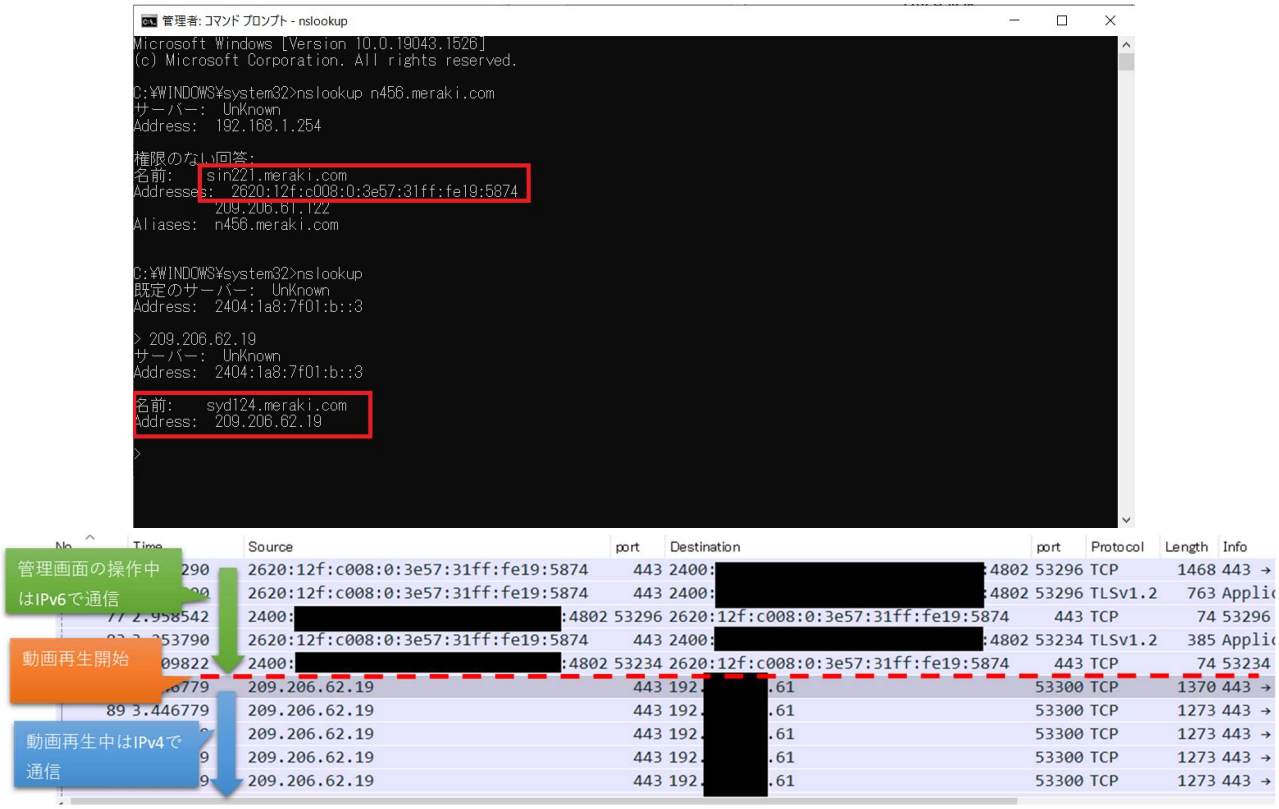


図 5.3.6-19 クラウドサービスの nslookup、動画再生時のパケットキャプチャ確認結果

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、機器メーカのサポート等に確認した結果、IPv6 対応が十分でないことが判明した課題と対応の事例を示す。

(2) IPv6 対応における留意事項(構築時の Tips)

本検証において実際に発生した IPv6 関連のトラブルシュート事例をもとに、IPv6 対応において普遍的に留意すべき点を示す。

6　IPv6 対応ユースケース(大学)

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

6.1　モデル I：大学 A

6.1.1 ユースケース大学の紹介

ユースケースを行った対象フィールドとシステム環境を紹介する。

(1) フィールド紹介

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

(2) 既存のシステム環境

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

① ネットワーク規模/インターネットとの接続方式

A 大学のシステム環境内のノード数は 50 以上、サブネット数は10未満、2 学部間を広域LAN接続している。インターネットとの接続は学術情報ネットワーク(SINET)を利用して接続している。

② 内部ネットワーク運営方法、およびサーバ運営方法/セキュリティ

システム環境内の PC には IPv4 アドレス等を DHCP サーバで動的設定を行っているが、サーバ機器および一部の PC は IPv4 アドレス等を静的に設定している。DNS サーバは学内に設置しているが、メールについては外部のサービスを利用している。ファイアウォールは既設 FW 装置を用いて実現している。

6.1.2 要件定義

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

(1) 現状の把握

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

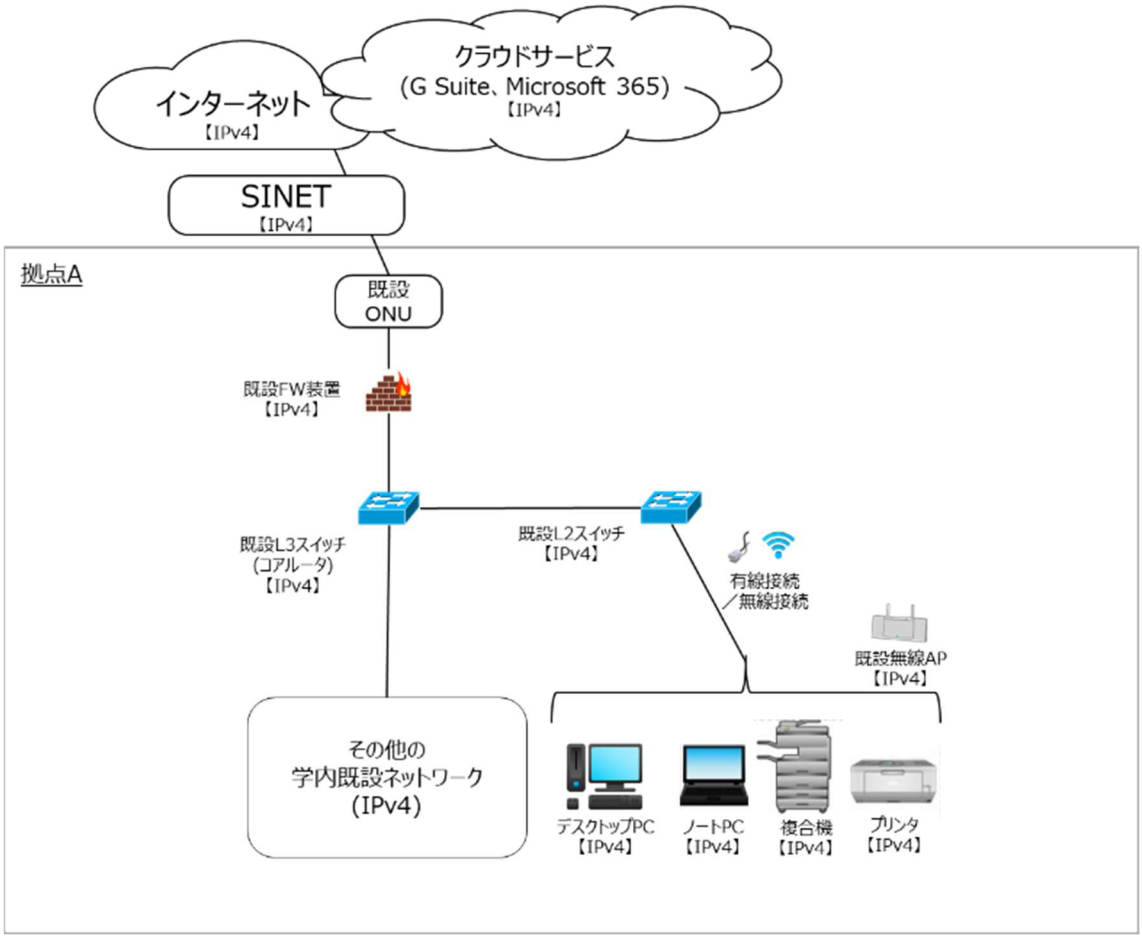


図 6.1.2-1 ネットワーク構成図イメージ

(2) 移行方式の明確化

本ユースケースにおいては IPv6 環境への移行を見据え、可能な範囲で既存システムを IPv6 対応する方針とした。移行範囲を検討した結果、既存システムへの影響を最小限に抑えるため、既存システムの一部を IPv6 対応することとした。そのため、IPv4 の既存学内ネットワークと IPv6 の実証試験ネットワークを共存させる必要があることから移行方式としてデュアルスタック方式を採用した。

(3)～(5) 移行対象の明確化、IPv6 対応状況の確認、導入方針の策定

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

表 6.1.2-1 機器等一覧イメージ

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

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

6.1.3 スケジュール計画

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

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

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

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

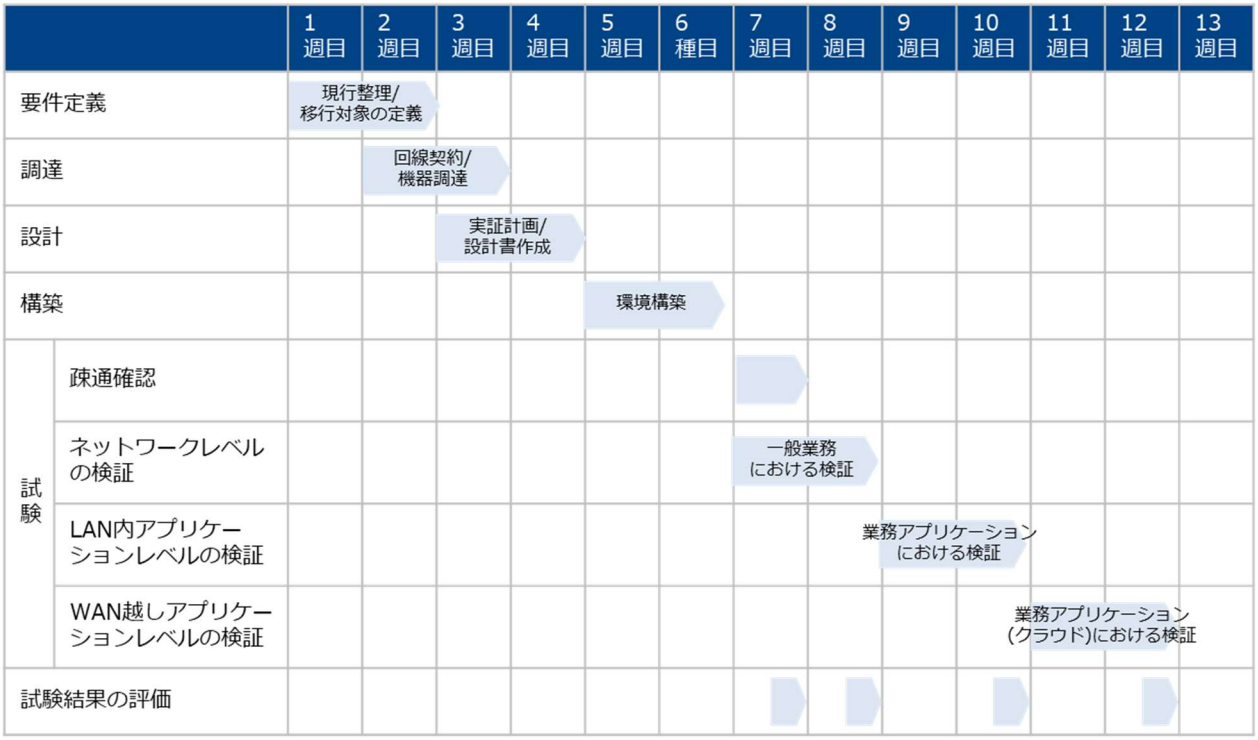


図 6.1.3-1 スケジュールイメージ(大学 A)

6.1.4 設計

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

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

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

(1) 無線接続のノート PC

① 要素説明

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

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

(a) IP アドレスについて

実証試験のため、IPv6 アドレスは固定 IPv6 アドレスと RA による IPv6 アドレス自動採番を採用する。ルータ仕様のため、プレフィックス部のみ DHCPv6[65]で割り当てるステートレス方式とする。

・IPv4 アドレス…静的アドレスによる手動設定
・IPv6 アドレス…IPv6 アドレスは固定 IPv6 アドレスと RA による IPv6 アドレス自動採番を採用する

(b) DNS サーバ/デフォルトゲートウェイについて

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

・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)
・IPv6 アドレス…静的アドレスによる手動設定
(パブリック DNS の指定/hosts ファイルによる指定)

---

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

(c) ポリシーテーブルについて

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

・IPv4 優先 PC…IPv4 アドレスが優先されるよう設定

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

(d) hosts ファイルについて

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

③ 特記事項

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

(2) 有線接続のデスクトップ PC

① 要素説明

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

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

(a) IP アドレスについて

実証試験のため、IPv6 アドレスは固定 IPv6 アドレスと RA による IPv6 アドレス自動採番を採用する。ルータ仕様のため、プレフィックス部のみ DHCPv6 で割り当てるステートレス方式とする。

・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)

・IPv6 アドレス…固定 IPv6 アドレス 又は RA による IPv6 アドレス自動採番

(b) DNS サーバ/デフォルトゲートウェイについて

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

・IPv4 アドレス…静的アドレスによる手動設定

・IPv6 アドレス…静的アドレスによる手動設定

(パブリック DNS の指定/hosts ファイルによる指定

(c) ポリシーテーブルについて

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

・IPv4 優先 PC…IPv4 アドレスが優先されるよう設定

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

(d) hosts ファイルについて

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

③ 特記事項

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

(3) 有線接続の OA 機器(プリンタ)

① 要素説明

一般業務で使用する有線接続のプリンタである。

② 方式設計

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

(a) IP アドレスについて

特に変更なし。

・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)

・IPv6 アドレス…設定不可

③ 特記事項

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

(4) 有線接続の OA 機器(複合機)

① 要素説明

一般業務で使用する有線接続の複合機である。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

(a) IP アドレスについて

実証試験のため、IPv6 アドレスは固定 IPv6 アドレスを設定する。

・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)

・IPv6 アドレス…固定 IPv6 アドレスを設定する

③ 特記事項

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

(5) インターネット接続を制御する実証用 FW 装置

① 要素説明

インターネット回線の接続、IPv4/IPv6 通信のルーティングやトラフィック制御を行うための機器である。

② 方式設計

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

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

(a) IP アドレスについて

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

・IPv4 アドレス… 静的アドレスによる手動設定(既存踏襲)

・IPv6 アドレス…固定 IPv6 アドレス 又は RA による IPv6 アドレス自動採番

(b) DNS サーバ/デフォルトゲートウェイについて

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

・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)

・IPv6 アドレス

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

DNS サーバ…静的アドレスによる手動設定

（パブリック DNS の指定/hosts ファイルによる指定）

(c) ファイアウォールについて

A 大学内のセキュリティポリシーにしたがって設定する。

③ 特記事項

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

(6) 無線接続を制御する無線アクセスポイント

① 要素説明

無線接続 PC から社内ネットワークに接続できるようにするための機器である。

② 方式設計

レイヤー2 の機器のため、IPv4/IPv6 に依存した設定はなし。

③ 特記事項

特になし。

(7) 実証用学内 WEB サーバ

① 要素説明

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

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

② 方式設計

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

(a) IP アドレスについて

・IPv4 アドレス…静的アドレスによる手動設定(既存同等)

・IPv6 アドレス…静的アドレスによる手動設定

(b) DNS サーバ/デフォルトゲートウェイについて

・IPv4 アドレス…静的アドレスによる手動設定(既存同等)

・IPv6 アドレス…静的アドレスによる手動設定

(c) ポリシーテーブルについて

AP/DB サーバにおいては、デフォルトの優先設定（IPv6 アドレスが優先）で検証を行う。

(d) hosts ファイルについて

実証用学内 WEB サーバは hosts ファイルでの名前解決を想定した通信を行わないため、追加設定を行わない。

(e) ゲスト OS 環境（仮想サーバ）について

ゲスト OS 環境は、ハイパーバイザー型のホスト OS（VMware vSphere）上で構築する。

③ 特記事項

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

(8) 社内の情報資産を管理するファイルサーバ

① 要素説明

クライアント PC を Active Directory 認証し、ファイル共有を行うサーバ機器である。

② 方式設計

IPv4/IPv6 デュアルスタック方式とする。

(a) IP アドレスについて

・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)

・IPv6 アドレス…静的アドレスによる手動設定

(b) DNS サーバ/デフォルトゲートウェイについて

・IPv4 アドレス…静的アドレスによる手動設定(既存踏襲)

・IPv6 アドレス…静的アドレスによる手動設定

(c) ポリシーテーブルについて

ファイルサーバ(B 社製)については、IPv4/IPv6 デュアルスタック環境において、IPv4 と IPv6 のどちらが優先されるかの技術情報は非公開の状況である。実証試験については、実証用ファイルサーバのポリシー設定は既定値の状態、実証端末側で IPv6 優先端末と IPv4 優先端末の両方で検証作業を行う。

③ 特記事項

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

(9) 社外のクラウドサービス

① 要素説明

A 大学が開発し、ユーザサービスを提供しているクラウドサービスである。

② 方式設計

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

以上を踏まえ、IPv6 対応後のシステム構成図を図 6.1.4-1 に示す。

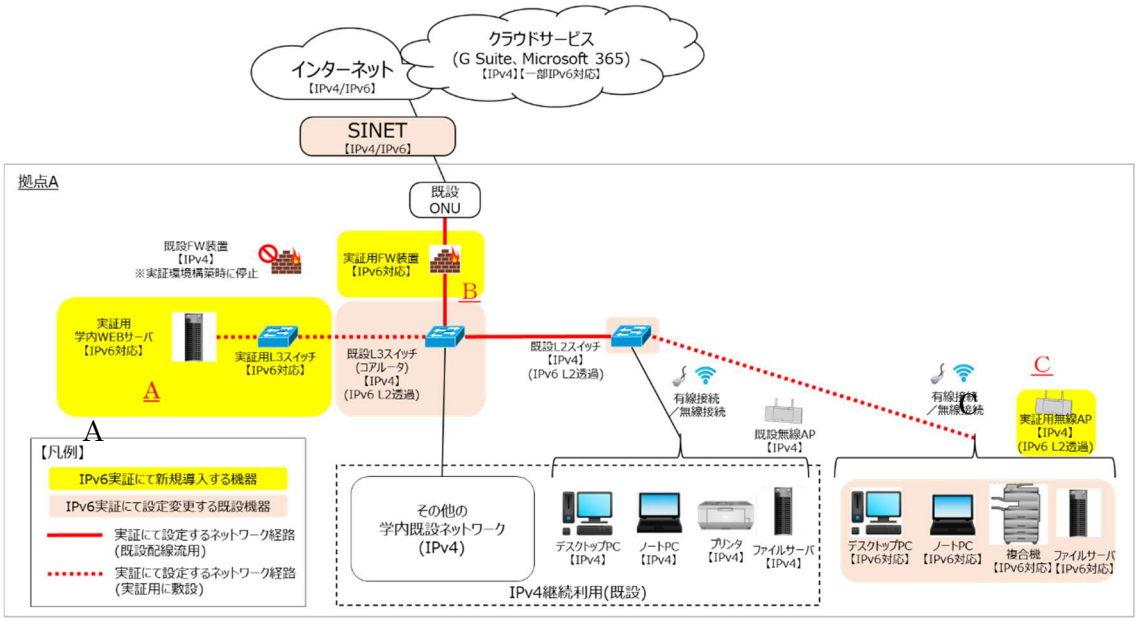


図 6.1.4-1 IPv6 対応後の A 大学のシステム構成図

【補足説明】

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

6.1.5 構築

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

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

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

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

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

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

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

そして、IPv6 対応するために行った各機器への設定内容を示す。

(1) 実証用 FW 装置の設定

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

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

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

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

項番	設定内容の詳細
6-2	【パケットフィルタリング　リソース定義】学内 AD サーバ→実証用 NW 通過設定 class-map match-all fil-from-huad-to-IPv4T 　　match destination-address ipv4 172.16.1.151,172.16.1.152 　　match destination-port 389/tcp-udp,135/tcp,88/tcp !
6-3	【パケットフィルタリング　リソース定義】学内→実証用 NW 通過設定 class-map match-all fil-from-local-port-etc-IPv4T 　　match class-map net-internal 　　match destination-port 123/tcp-udp,53/tcp-udp ! class-map match-all fil-from-local-port-etc-IPv6T 　　match class-map net-internal-IPv6TEST 　　match destination-port 123/tcp-udp,53/tcp-udp ! class-map match-all fil-from-local-port-etc2-IPv4T 　　match class-map net-internal 　　match destination-port 3389/tcp-udp,137-138/udp,139/tcp,445/tcp,25/tcp ! class-map match-all fil-from-local-port-ftp-IPv6T 　　match destination-port ftp 　　match class-map net-internal-IPv6TEST ! class-map match-all fil-from-local-port-https-IPv6T 　　match destination-port 80/tcp,443/tcp 　　match class-map net-internal-IPv6TEST !
6-4	【パケットフィルタリング　リソース定義】EPSON プリンタ→実証用 NW 通過設定 class-map match-all fil-from-local-port-snmp-IPv4T 　　match class-map net-internal 　　match destination-address ipv4 172.16.19.163 　　match destination-port 161/udp,3289/udp,515/tcp !

項番	設定内容の詳細
6-5	【パケットフィルタリング　リソース定義】SINETルータからの WAN 側 ICMPv6 応答許可設定 class-map match-all fil-from-R-to-hufw01-port-icmp6 　　match class-map ICMPv6 　　match source-address ipv6 [redacted],fe80::/16 !
6-6	【パケットフィルタリング　リソース定義】学内からの ICMPv6 応答許可設定 class-map match-all fil-to-local-port-ICMPv6 　　match class-map net-internal-IPv6TEST 　　match class-map ICMPv6 !
6-7	【パケットフィルタリング　リソース定義】実証環境 IPv6 アドレス範囲設定 class-map match-any net-internal-IPv6TEST 　　match source-address ipv6 [redacted]:6050::/64 　　match source-address ipv6 [redacted]:6051::/64 　　match source-address ipv6 [redacted]:6052::/64 !

(2) 実証用 L3 スイッチの設定

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

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

項番	設定内容の詳細
	serverinfo dns ip6 off serverinfo sntp ip off serverinfo sntp ip6 off serverinfo time ip tcp off serverinfo time ip udp off serverinfo time ip6 tcp off serverinfo time ip6 udp off
2	【ether ポート設定】 ether 1-28 eee off ether 1 vlan tag 50-52 ether 15-16 vlan untag 50 ether 17-18 vlan untag 51 ether 19-20 vlan untag 52 ether 21 vlan tag 50-52
3	【VLAN 設定】 vlan 50 name LAN050 vlan 51 name LAN051 vlan 52 name LAN052
4	【実証用ネットワーク(ルーティング用:VLAN050) アドレス設定】 lan 50 ip address 172.16.50.253/24 3 lan 50 ip route 0 default 172.16.50.254 1 1 lan 50 ip6 use on lan 50 ip6 address 0 1:2f8:1 :6050::1/64 lan 50 ip6 route 0 default 1:2f8:1 :6050::2 1 1 lan 50 vlan 50 <<特記事項>> ・IPv6 アドレスの自動採番を考慮しないネットワークセグメントのため、RA(Router Advertisement)は SEND/RECV とも OFF にする ・RIP は OFF とする
5	【実証用ネットワーク(実証環境(サーバ室)用:VLAN051) アドレス設定】 lan 51 ip address 172.16.51.253/24 3 lan 51 ip6 use on lan 51 ip6 address 0 1:2f8:1 :6051::1/64 lan 51 vlan 51

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

(3) 既設 L3 スイッチ(コアルータ)の設定

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

項番	設定内容の詳細
1	【イーサネットポート設定】 ether 1 vlan tag 1,3,50 実証用 FW 装置向け VLAN 50 を追加 ether 7 vlan tag 1,3-6,8,10-11,14-15,18-19,51,180-190 SR-S352TR1 向け VLAN51 追加 ether 8 vlan tag 1,3-6,8,10-11,14-15,18-19,51,180-190 SR-S352TR1 向け VLAN51 追加 ether 21 vlan tag 50-52 実証用 L3 スイッチ向け VLAN 50-52 追加 ether 32 vlan tag 10,12,17,19,22,52,117,180 既設 L2 スイッチ向け VLAN 52 追加

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

(4) 既設 L2 スイッチの設定

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

項番	設定内容の詳細
1	【SR-XXXXTR1：イーサネットポート設定】 ether 25 vlan tag 1,3-6,8,10-11,14-15,18-19,51,180-190 既設 L3 向け VLAN 51 を追加 ether 26 vlan tag 1,3-6,8,10-11,14-15,18-19,51,180-190 既設 L3 向け VLAN 51 を追加 ether 38 vlan tag 1,3,51 既設仮想基盤環境向け VLAN 51 を追加 ether 40 vlan tag 1,3,51 既設仮想基盤環境向け VLAN 51 を追加 ether 42 vlan tag 1,3,51 既設仮想基盤環境向け VLAN 51 を追加 ether 44 vlan tag 1,3,51 既設仮想基盤環境向け VLAN 51 を追加
2	【VLAN 追加設定】 vlan 51 name LAN051

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

(5) 複合機の設定

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

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

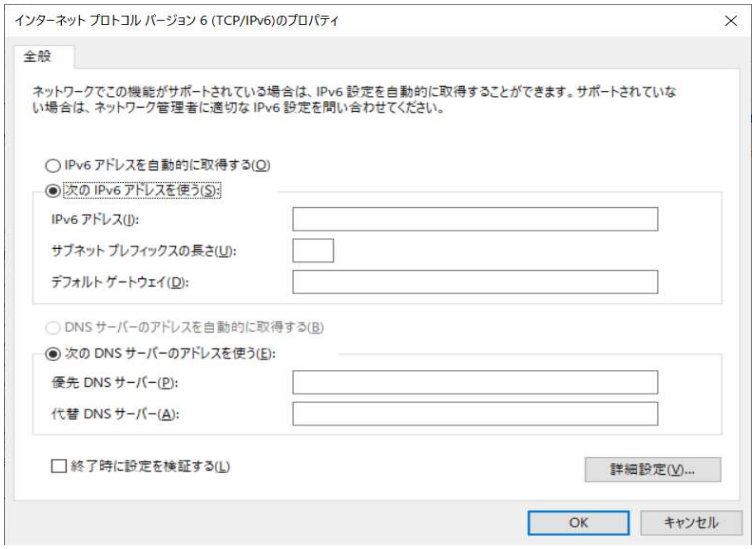
項番	設定内容の詳細
6	【IPv6 アドレスの手動設定】 ・親メニューに戻り、[TCP/IP− ネットワーク設定]を選び、[確認/変更]を押す ・[IPv6 − アドレス手動設定]を選択し、[確認/変更]を押す ・手動設定を「しない」→「する」に変更する ・「DHCP からアドレスを取得」のチェックを外す ・「手動設定アドレス」に複合機に割り当てる IPv6 アドレスを入力する。プレフィクス長は「64」を指定する ・「ゲートウェイアドレス」に実証環境のゲートウェイアドレス(IPv6)を入力する

(6) プリンタの設定

既存ネットワークに設置された機器を使用するため、変更作業は行わない。

(7) ファイルサーバの設定

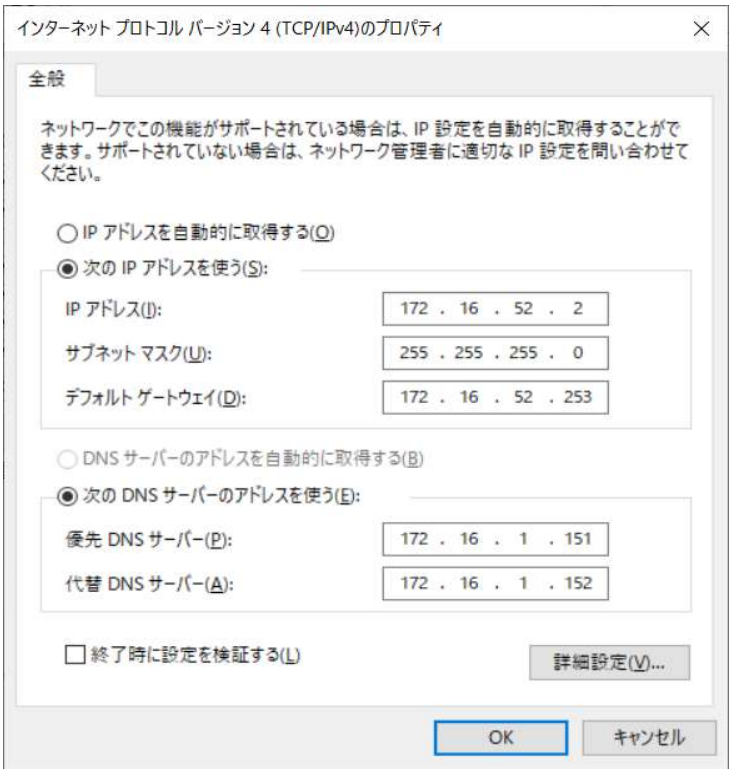
ファイルサーバ上で下記の設定を行い、IPv6 デュアルスタックに対応するファイルサーバを構築する。ファイルサーバのオペレーティングシステムが「Windows Server IoT 2019 for Storage」のため、設定方法は Windows サーバに準じる。 IPv6 実証環境ネットワークとの接続は別の LAN ポートに接続して実施する。

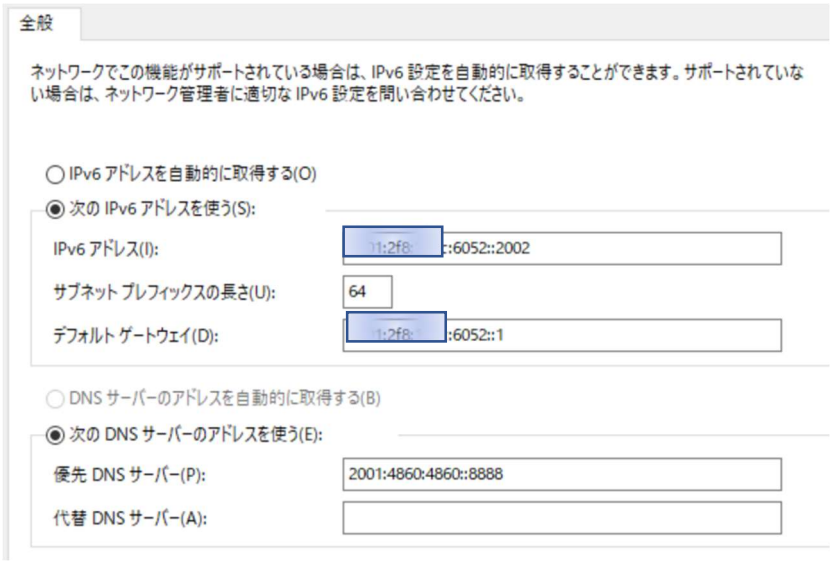
項番	設定内容の詳細
1	【IPv4 アドレスの設定】 既存ネットワークに接続したまま実施するため、変更しない
2	【IPv6 アドレスの設定】 IPv6 実証環境ネットワークと接続しているネットワークアダプタ(LAN)のプロパティを開き、IPv6 アドレスを手動で設定する 

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

(8) クライアント PC の設定

Windows 上で以下の操作を行い、IPv6 優先設定を行った。

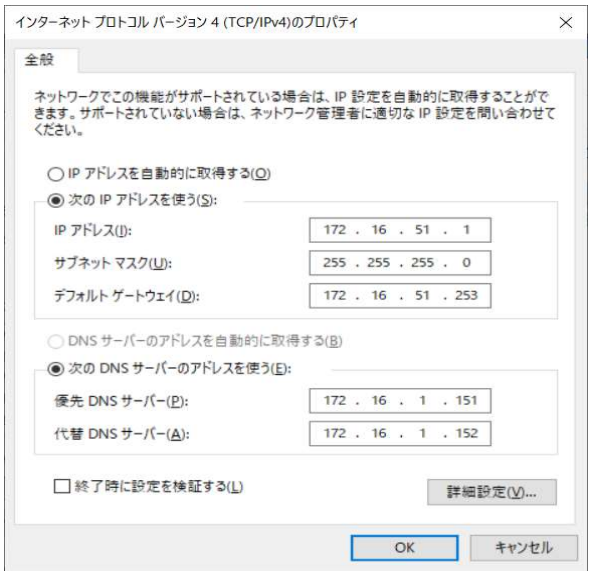
項番	設定内容の詳細
1	【IPv4 アドレスの設定】 接続しているネットワーク アダプタ（LAN or Wi-Fi）のプロパティから固定 IP を設定する。  ※IP アドレスは学内で管理している固定アドレスを設定する。 学外接続の検証を行う場合、優先 DNS サーバおよび代替 DNS サーバについては、パブリック DNS の IP アドレスを設定する（有線：8.8.8.8 代替：8.8.4.4）

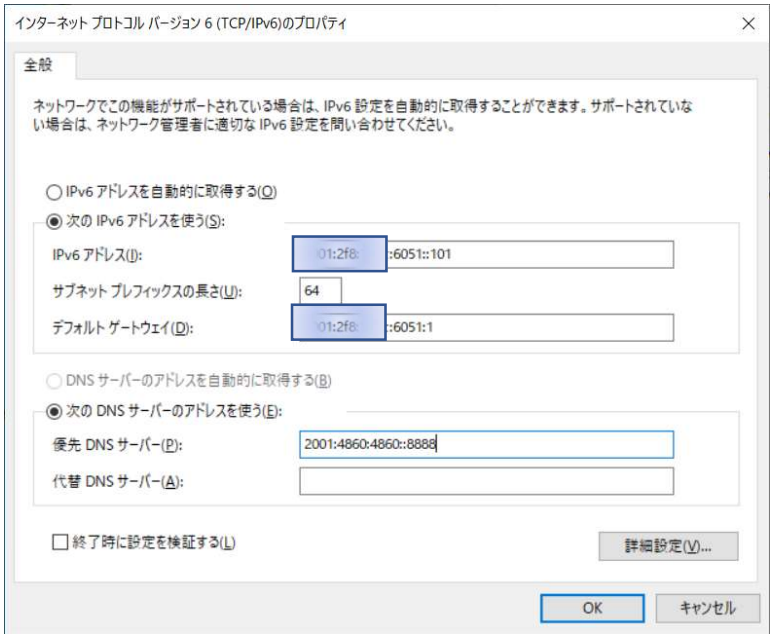
項番	設定内容の詳細
2	【IPv6 アドレスの設定】 接続しているネットワークアダプタ(LAN or wife)のプロパティから静的 IP が設定されるようにする。  ※学内向け検証を行う場合、優先 DNS サーバに設定しているパブリック DNS の IPv6 アドレスを消去する
3	【Hosts の設定追加】 Hosts ファイルに IPv6 の実証環境で利用するサーバのアドレスを追加する ¥Windows¥System32¥drivers¥etc¥hosts ===== ## IPv6 :6051::101 hunet-ipv6 :6052::1002 filesv-ipv6 ## IPv4 172.16.51.1 hunet-ipv4 172.16.19.203 filesv-ipv4 =====

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

(9) 実証用学内 WEB サーバの設定

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

項番	設定内容の詳細
1	【ESXi サーバ　仮想スイッチの設定】 vSphere Client より仮想スイッチの設定を行い、VLAN タグに「51」と紐づける設定を行う IPv4、IPv6 アドレスに関しては追加および変更は行わない ESXi サーバは2台構成のため、二台とも設定を行う
3	【ゲスト OS 環境の構築】 VMware vSphere 上でゲスト OS（Windows Server）を構成する。 実証用学内 WEB サーバについては、既設の学内 WEB サーバを複製（クローン）したものを利用する
4	【ゲスト OS　ネットワーク設定】 vSphere Client より既設 vCenter Server に接続し、複製（クローン）した実証用学内 WEB サーバの設定を編集する 仮想マシンの構成で「ネットワーク　アダプタ」を選択し、「ネットワーク接続」の「ネットワークラベル」のドロップダウンリストより「VLAN051」を選択する。
5	【ゲスト OS 環境の IPv4 設定】 ゲスト OS の IPv4 アドレスを以下のとおり設定する。  学外接続の検証を行う場合、優先 DNS サーバおよび代替 DNS サーバについては、パブリック DNS の IP アドレスを設定する（有線：8.8.8.8　代替：8.8.4.4）

項番	設定内容の詳細
6	【ゲスト OS 環境の IPv6 設定】 ゲスト OS の IPv6 アドレスを以下のとおり設定する。  ※学内向け検証を行う場合、優先 DNS サーバに設定しているパブリック DNS の IPv6 アドレスを消去する

6.1.6 試験

本ユースケースで実施した内容と結果を示す。

6.1.6.1 実証内容と結果

1. ネットワークレベルの検証

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

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

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

(1) 一般業務における検証について

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

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

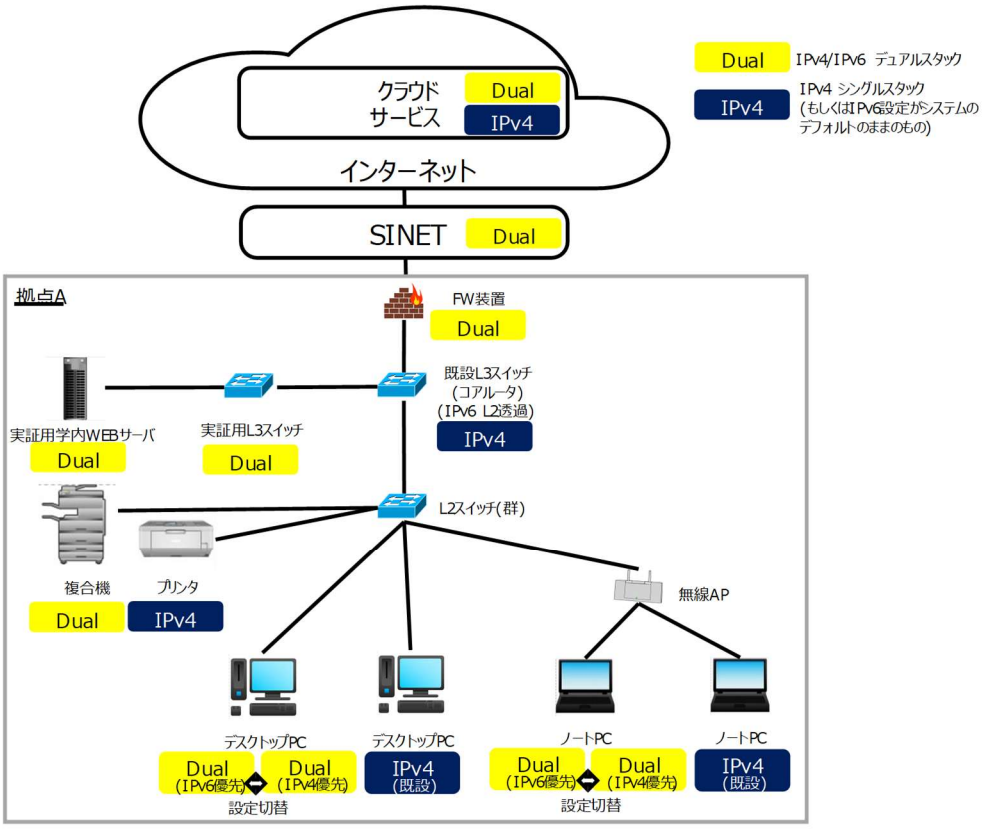


図 6.1.6-1 一般業務検証における接続イメージ

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

① 疎通確認

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

② WEB サービスやメールサービス等のインターネット利用

WEB サービスやメール等へインターネット接続し、コンテンツが利用できることを検証する。IPv6 未対応の学外コンテンツの場合、コンテンツが利用できないことを検証する。

③ 通常業務を想定した学内ネットワーク機器の利用

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

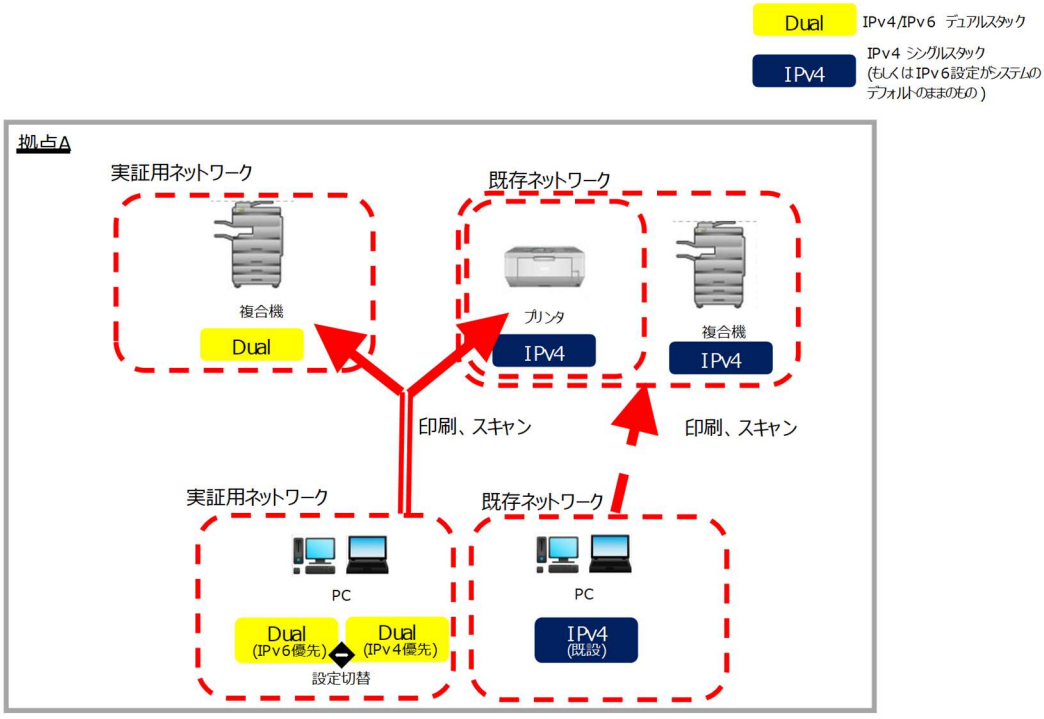


図 6.1.6-2 通常業務を想定した学内ネットワーク機器利用イメージ

上記①から③のシナリオを実施した結果の内、主要な結果を以下に示す。

① 疎通確認の検証結果

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

【#1 の補足】

IPv6 で ping の応答を受信できることを確認した。

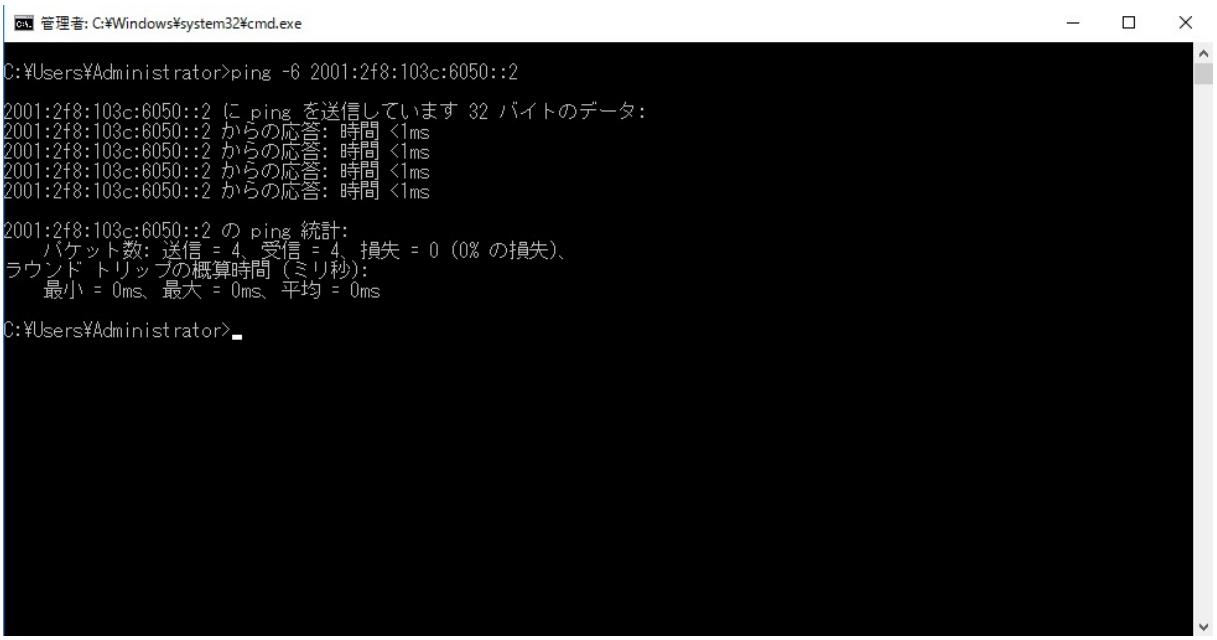


図 6.1.6-3 IPv6 で ping 応答あり

【#2 の補足】

IPv6 でインターネット接続できることを確認した。

図 6.1.6-4 IPv6 でインターネット接続可能

【#3 の補足】

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

(filesv-ipv6 はファイルサーバのホスト名)

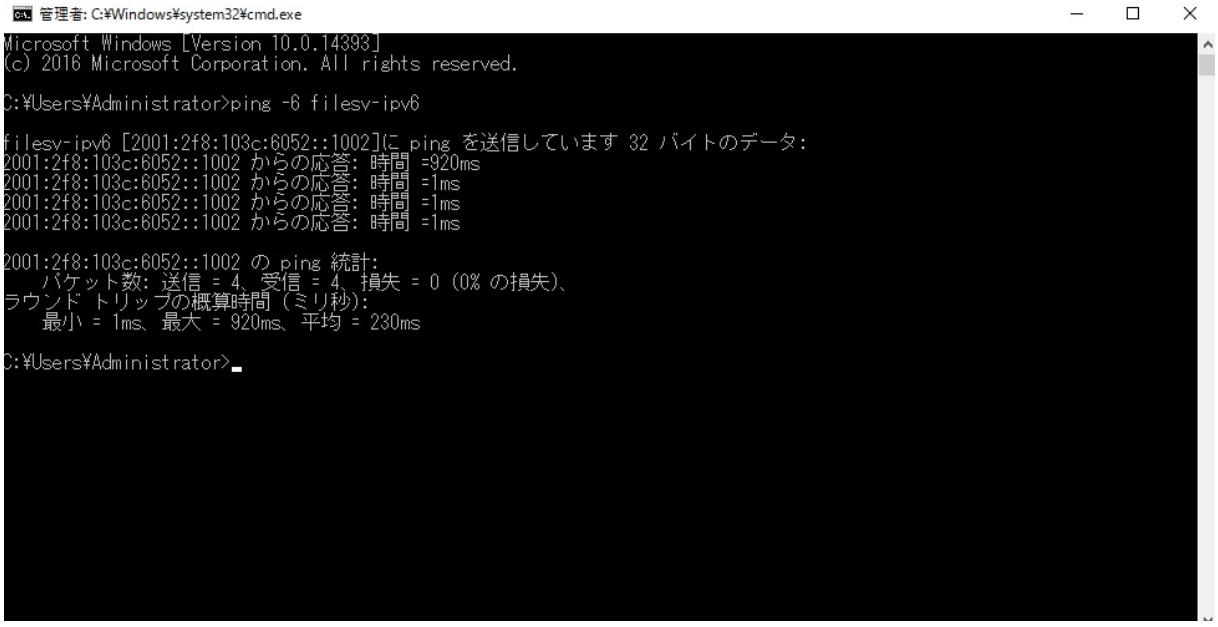


図 6.1.6-5 ホスト名でも ping 応答あり

② WEB サービス等のインターネット利用

#	接続元機器名	有線無線	IPv4 IPv6	接続先機器名・サービス名	IPv4 IPv6	検証内容	想定結果	実施結果
1	ノート PC	無線	IPv6 優先	インターネット（IPv6 対応サイト）	IPv6	WEB ブラウザで google へアクセスする	google 画面が表示される	OK
2	ノート PC	無線	IPv6 優先	インターネット（IPv6 未対応サイト）	IPv4	WEB ブラウザで yahoo.co.jp サイトへアクセスする	yahoo.co.jp 画面が表示される	OK
3	ノート PC	無線	IPv4 優先	インターネット(一般)	IPv4	WEB ブラウザで google へアクセスする	google 画面が表示される	OK

【#1 の補足】

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

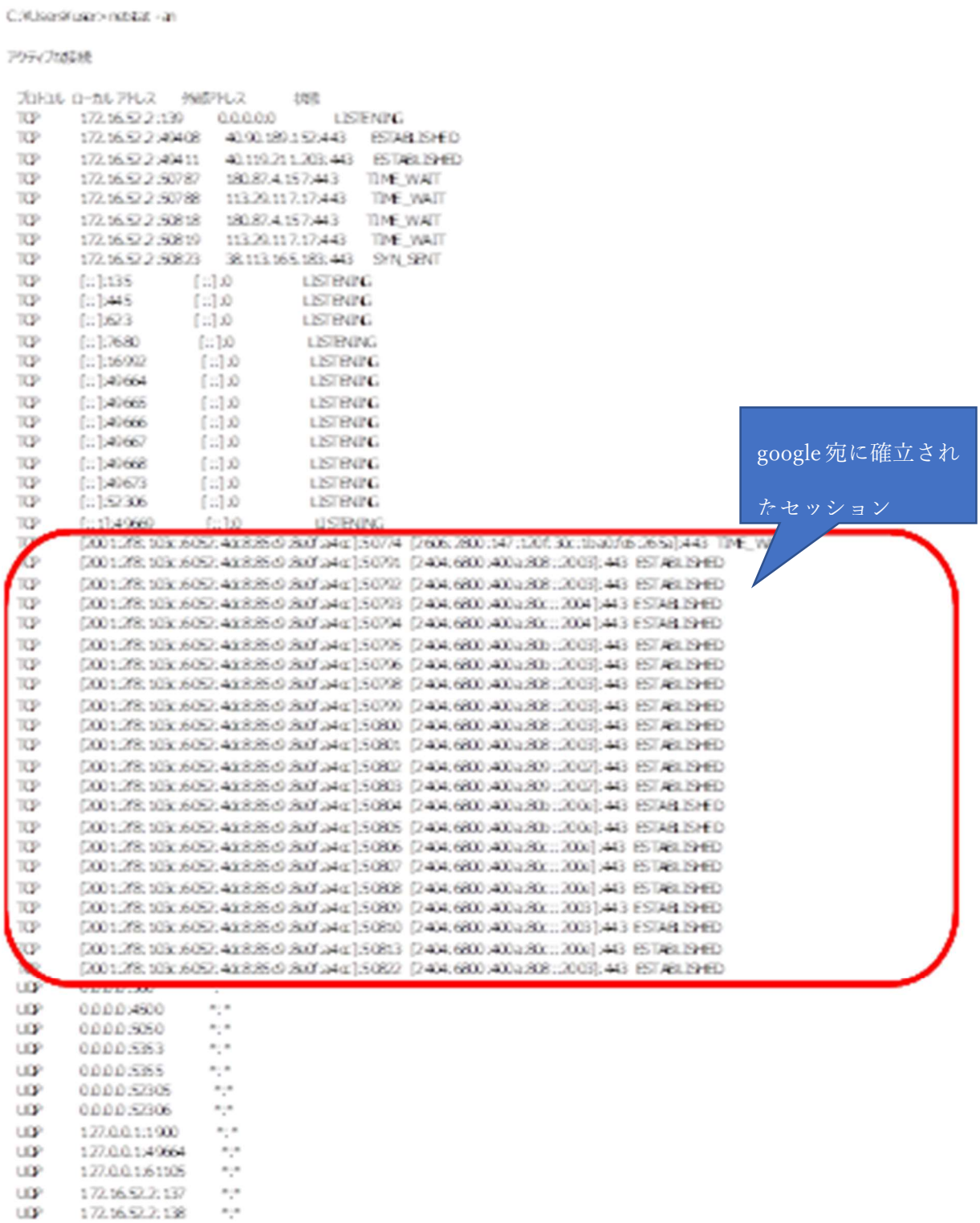


図 6.1.6-6 IPv6 優先接続端末で WEB アクセス時の「netstat -an」の実行結果

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

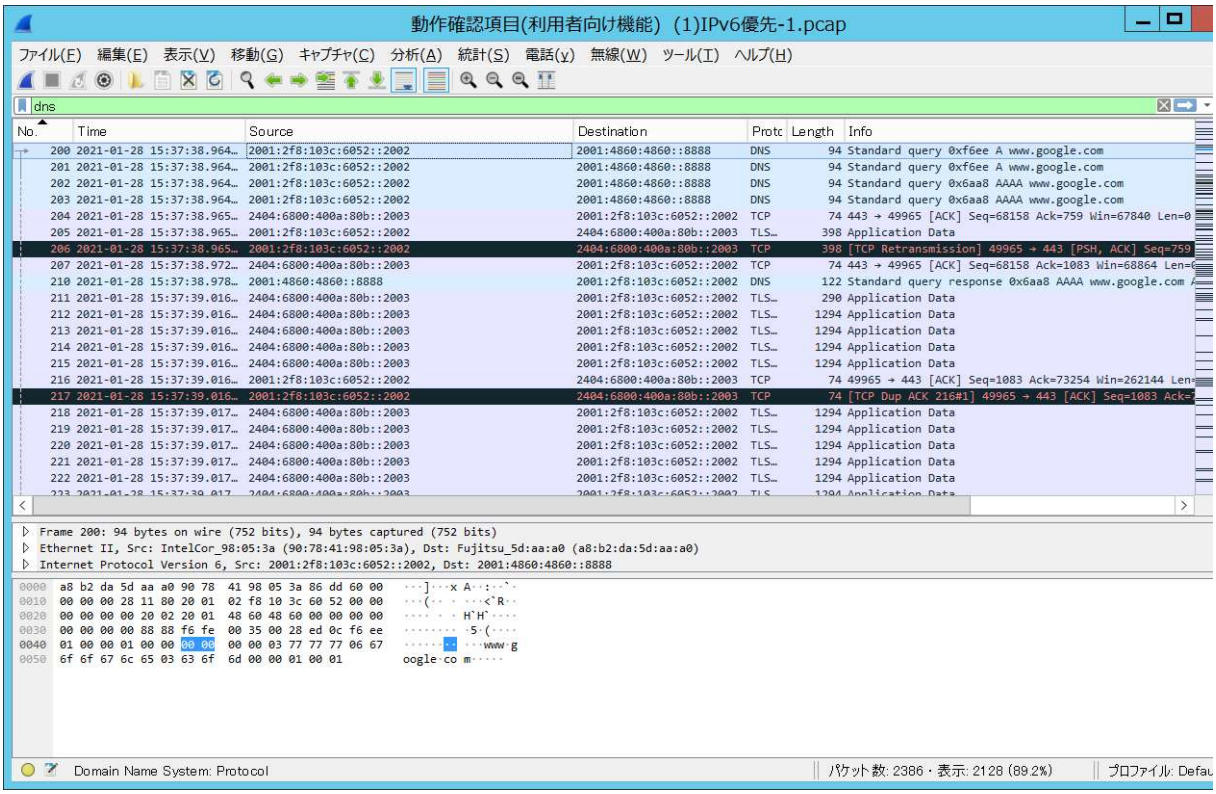


図 6.1.6-7 IPv6 優先接続端末で WEB アクセス時のネットワークキャプチャ結果

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

【#2 の補足】

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

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

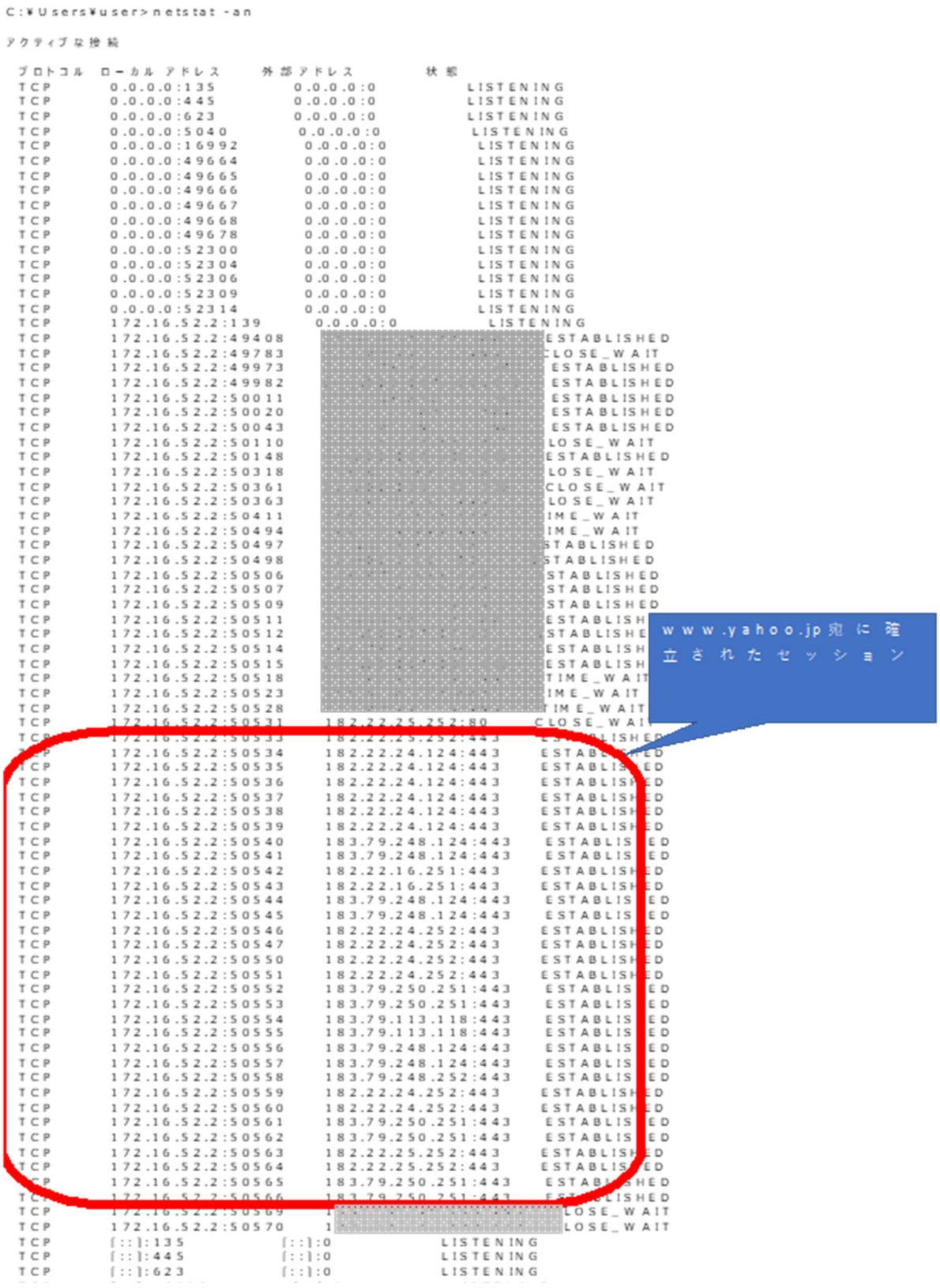


図 6.1.6-8 IPv6 未対応サイトを WEB アクセス時の「netstat -an」の実行結果

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

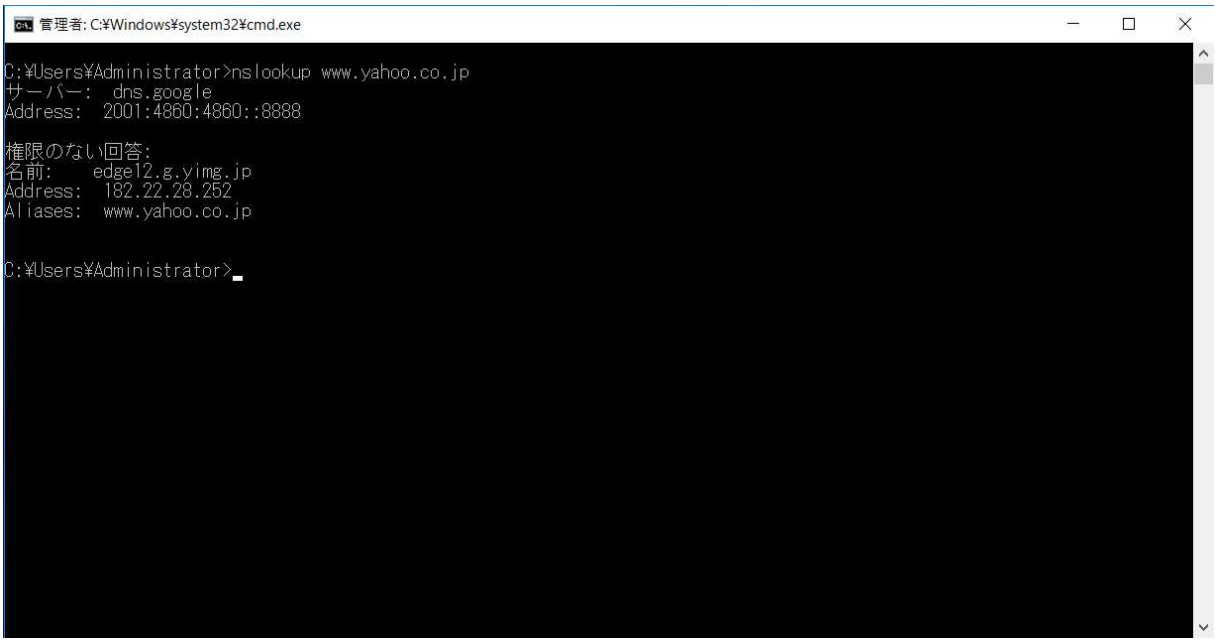


図 6.1.6-9 IPv6 未対応サイトの nslookup コマンド実行結果

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

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

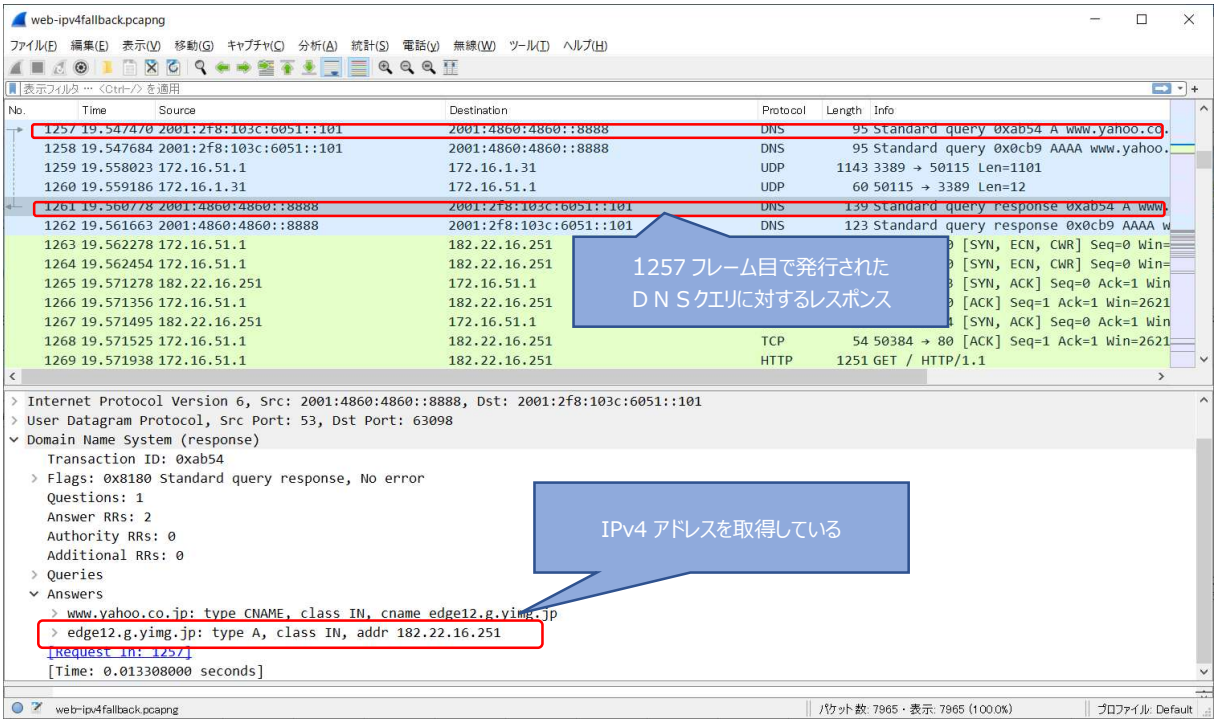


図　6.1.6-10　IPv6 未対応サイトのネットワークトレース結果(1)

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

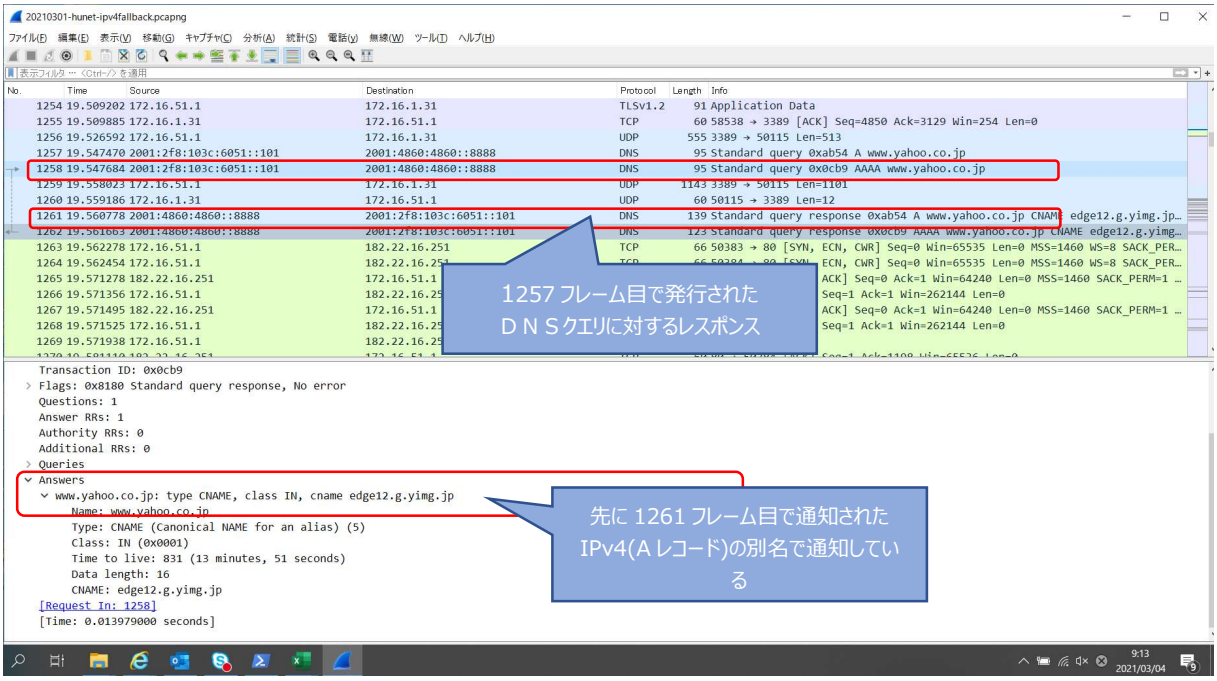


図　6.1.6-11　IPv6 未対応サイトのネットワークトレース結果(2)

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

【#3 の補足】

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

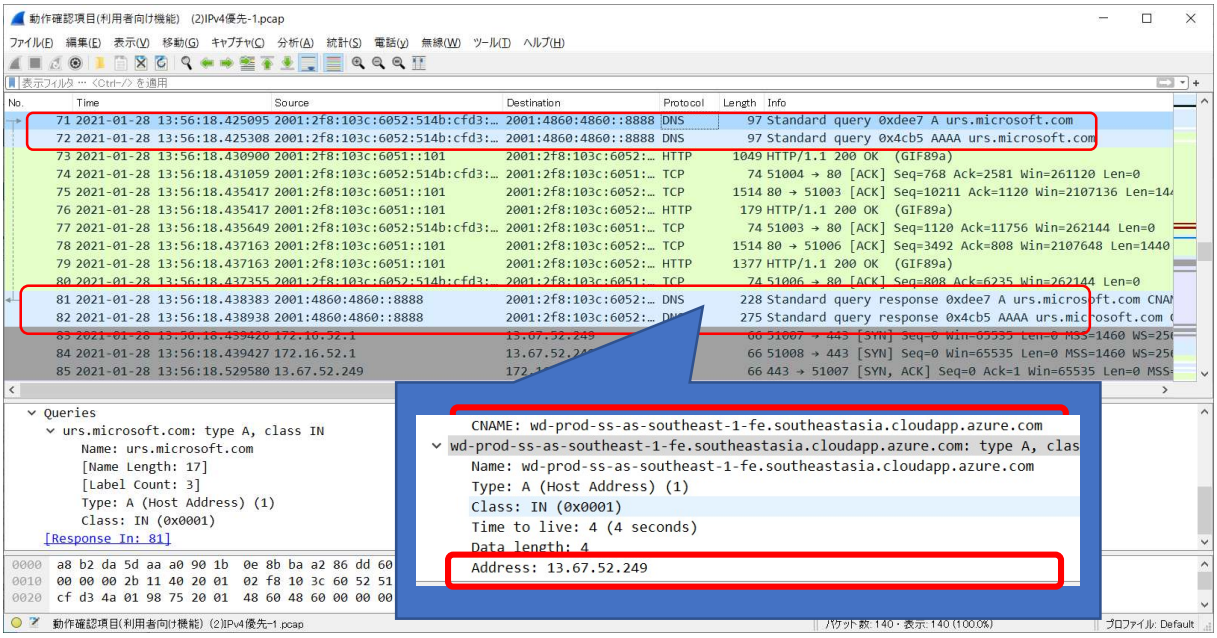


図 6.1.6-12 IPv4 優先端末で WEB アクセス時のネットワークキャプチャ実行結果(1)

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

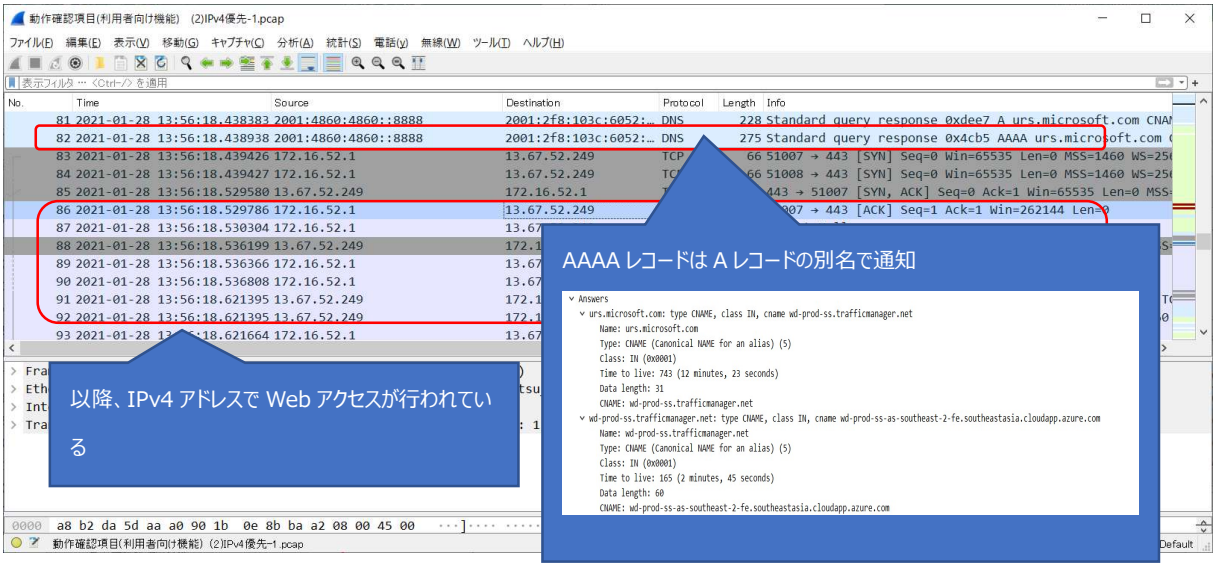


図 6.1.6-13 IPv4 優先端末で WEB アクセス時のネットワークキャプチャ実行結果(2)

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

③ 通常業務を想定した学内ネットワーク機器の利用

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

【#1 の補足】 ※に関して

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

【#2、#5 の補足】

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

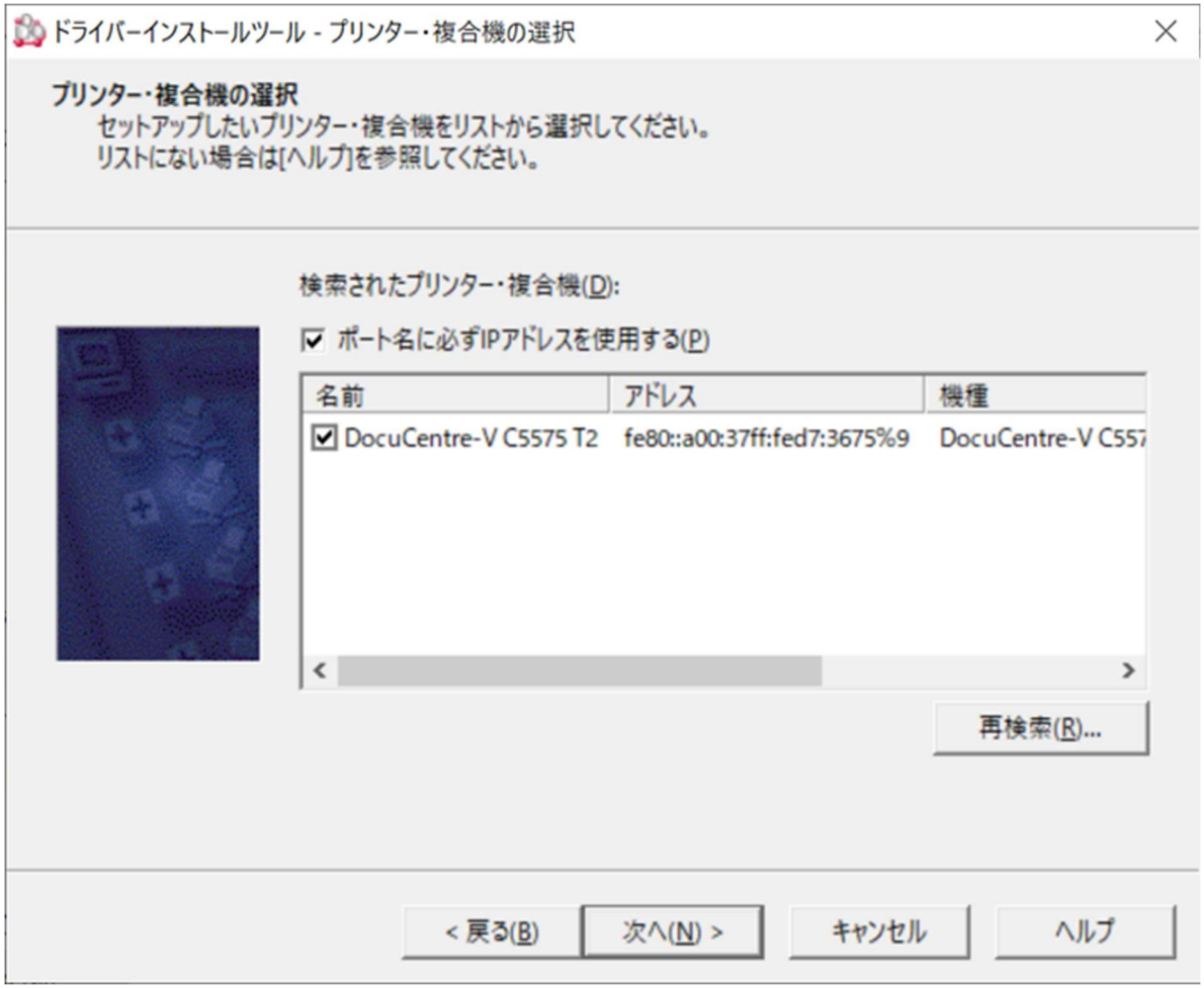


図 6.1.6-14 プリンタドライバインストール時にプリンタを自動検出した際の動作

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

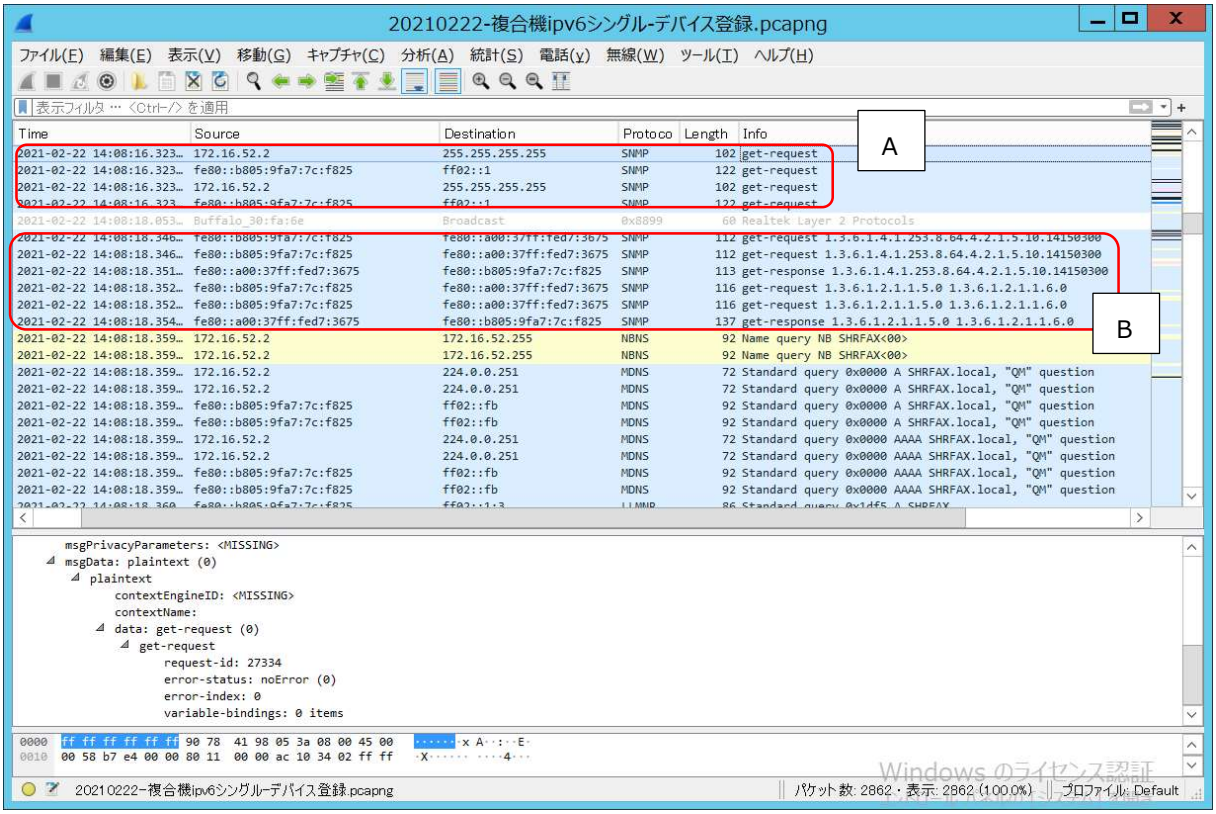


図 6.1.6-15 プリンタドライバインストール時のネットワークトレース結果

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

【#3 の補足】

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

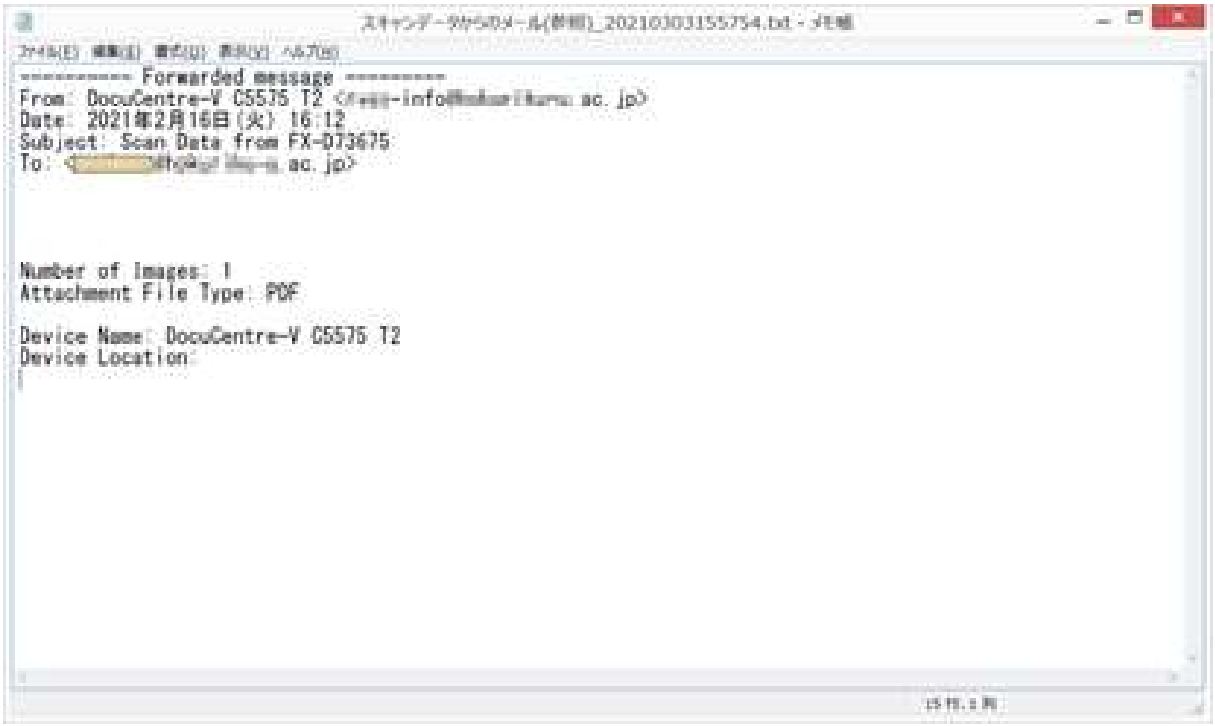


図 6.1.6-16 複合機からのスキャンデータ受信メール

【#7 の補足】

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

2. LAN 内アプリケーションレベルの検証

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

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

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

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

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

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

(3) 業務アプリケーションにおける検証について

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

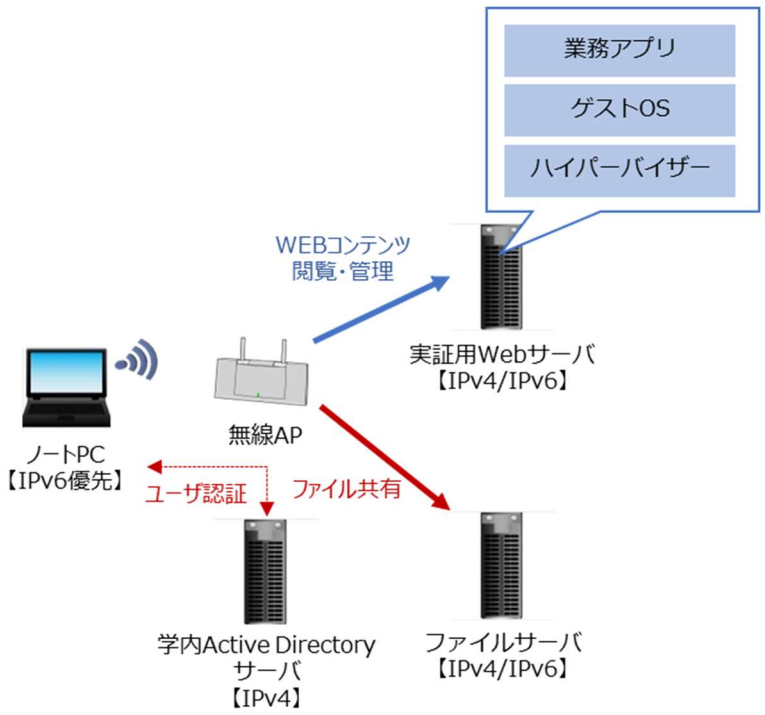


図 6.1.6-17 業務アプリケーションにおける検証範囲

① WEB サーバソフトウェアの動作検証

② 一般利用者向けの検証項目として IPv6 デュアルの実証用学内 WEB サーバに配置した WEB コンテンツが実証用 PC のブラウザ経由で閲覧できることを検証する。また WEB サーバの管理者向けの検証項目として、実証用学内 WEB サーバにて WEB ページやコンテンツの変更が IPv4/IPv6 デュアルスタック環境下で利用できるか検証する。

③ ファイルサーバの動作検証（ユーザ認証、ファイル共有）
ファイルサーバのユーザ認証とファイル共有ができるか検証する。また、ユーザ認証が学内の Active Directory サーバとの間で IPv4 を使用して認証が行えることを検証する。

①WEB サーバソフトウェアの動作検証

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

【#1、#2 の補足】

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

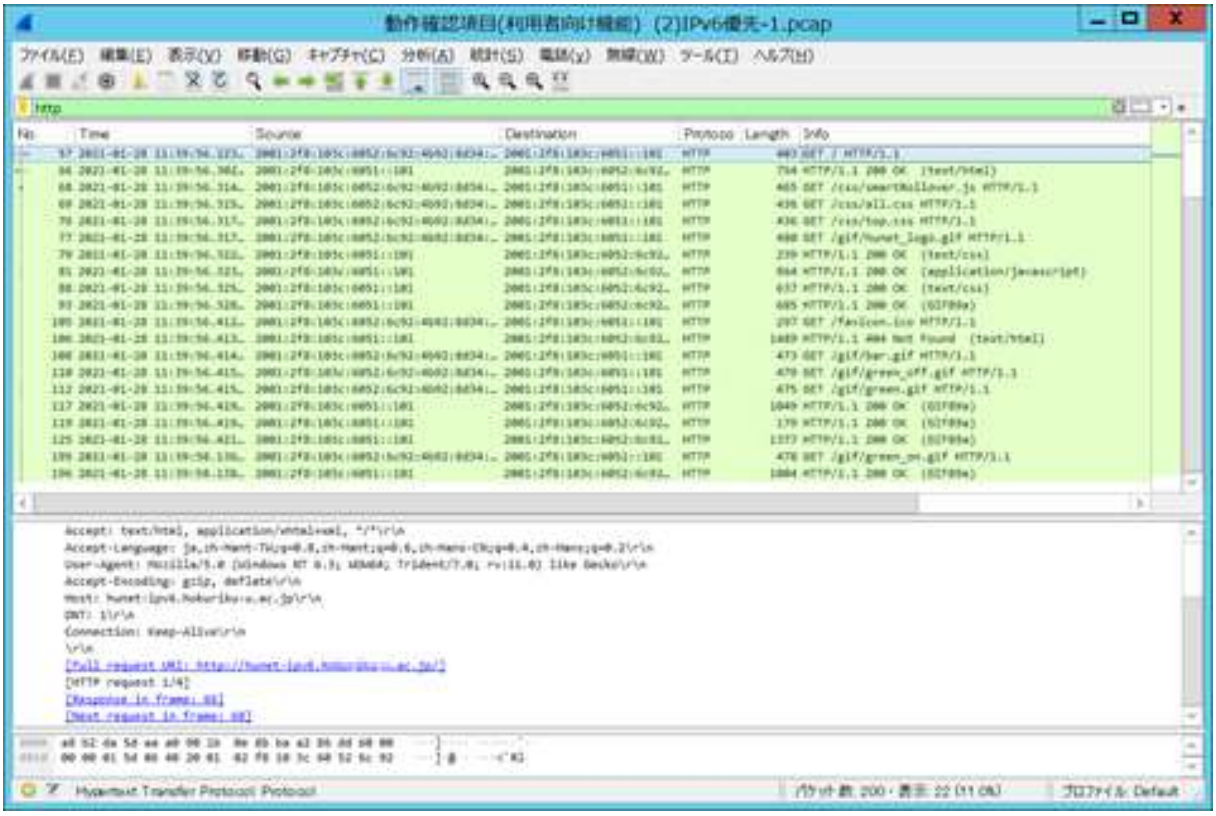


図 6.1.6-18 実証用学内 WEB サーバを WEB 表示した際のネットワークトレース結果(1)

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

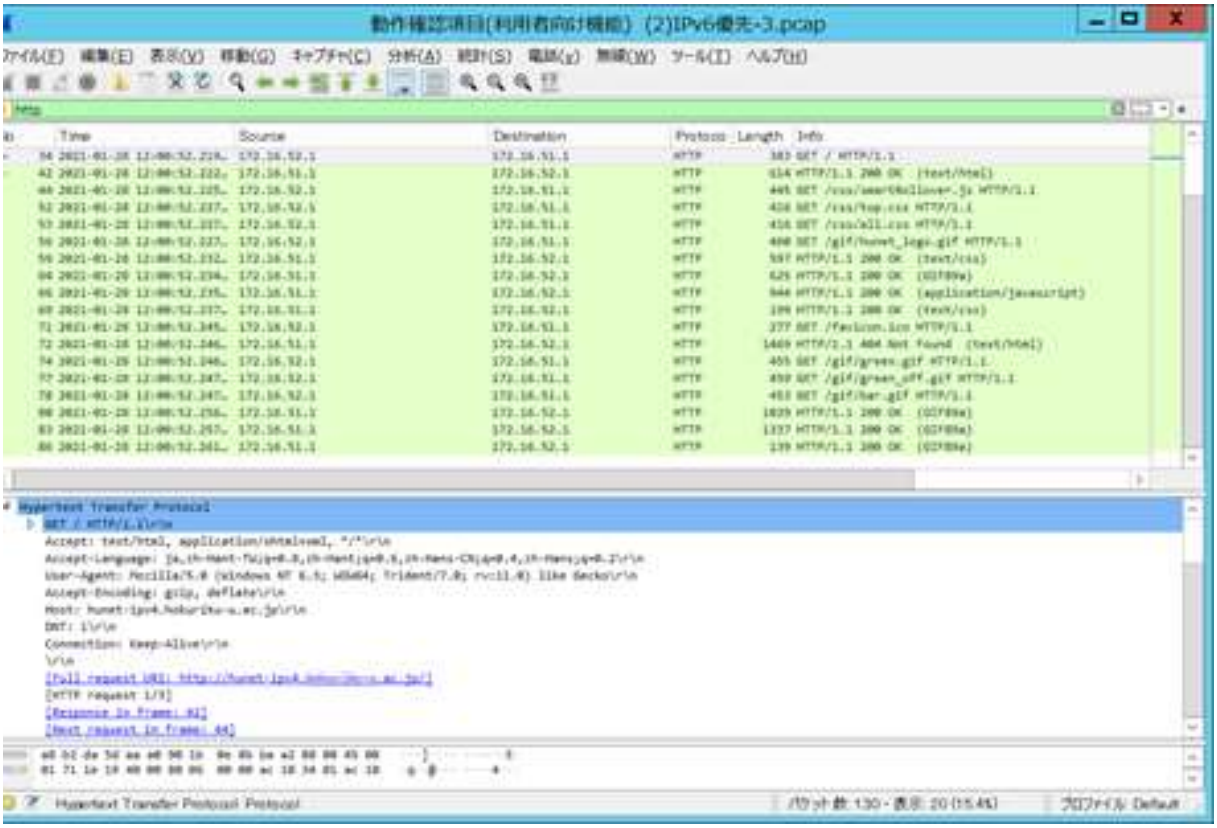


図 6.1.6-19 実証用学内 WEB サーバを WEB 表示した際のネットワークトレース結果(2)

【#4 の補足】 ※1に関して

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

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

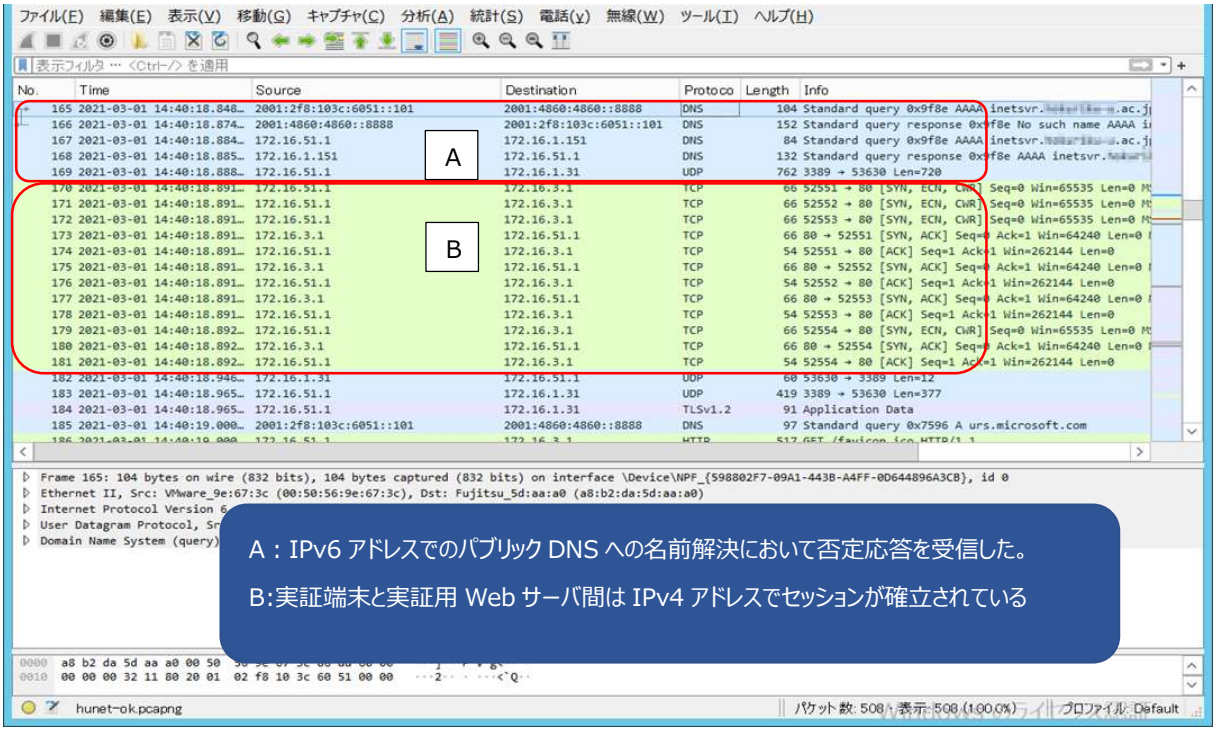


図 6.1.6-20 IPv4 優先端末から WEB 表示した際のネットワークトレース結果(1)

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

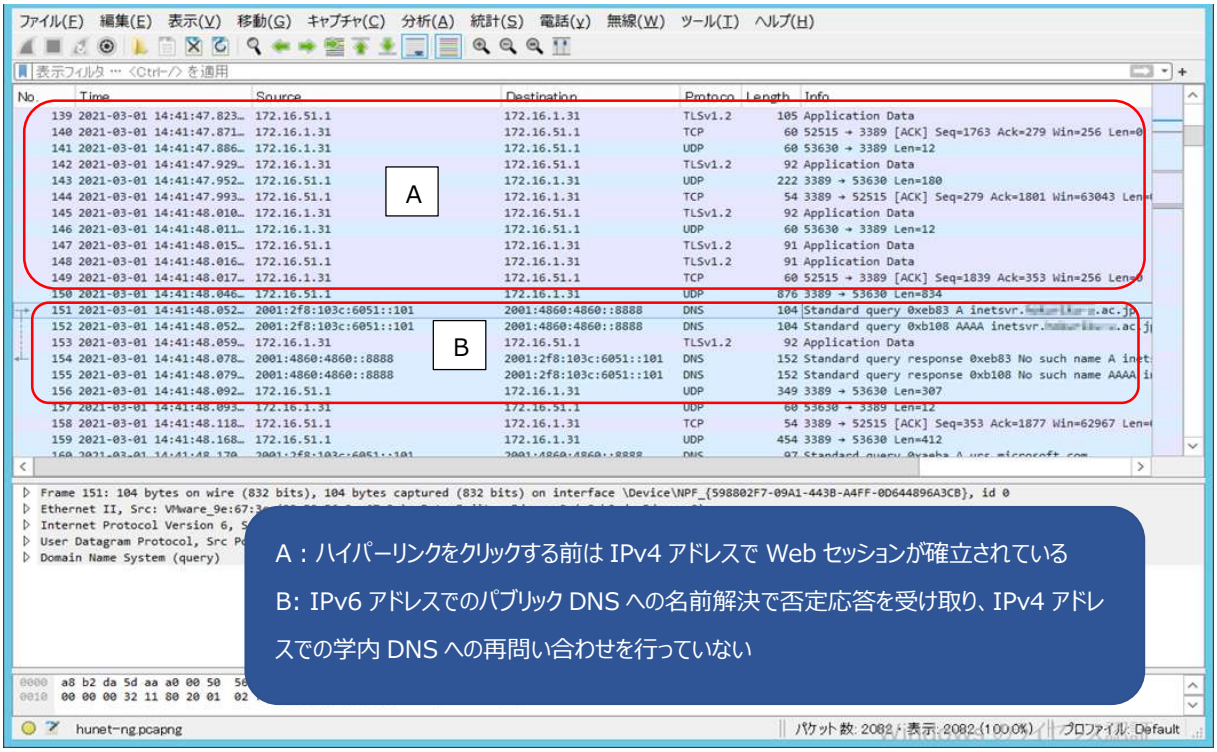


図 6.1.6-21 IPv4 優先端末から WEB 表示した際のネットワークトレース結果(2)

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

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

【#5 の補足】 ※2に関して

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

③ファイルサーバの利用(ユーザ認証、ファイル共有)

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

【#1の補足】

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

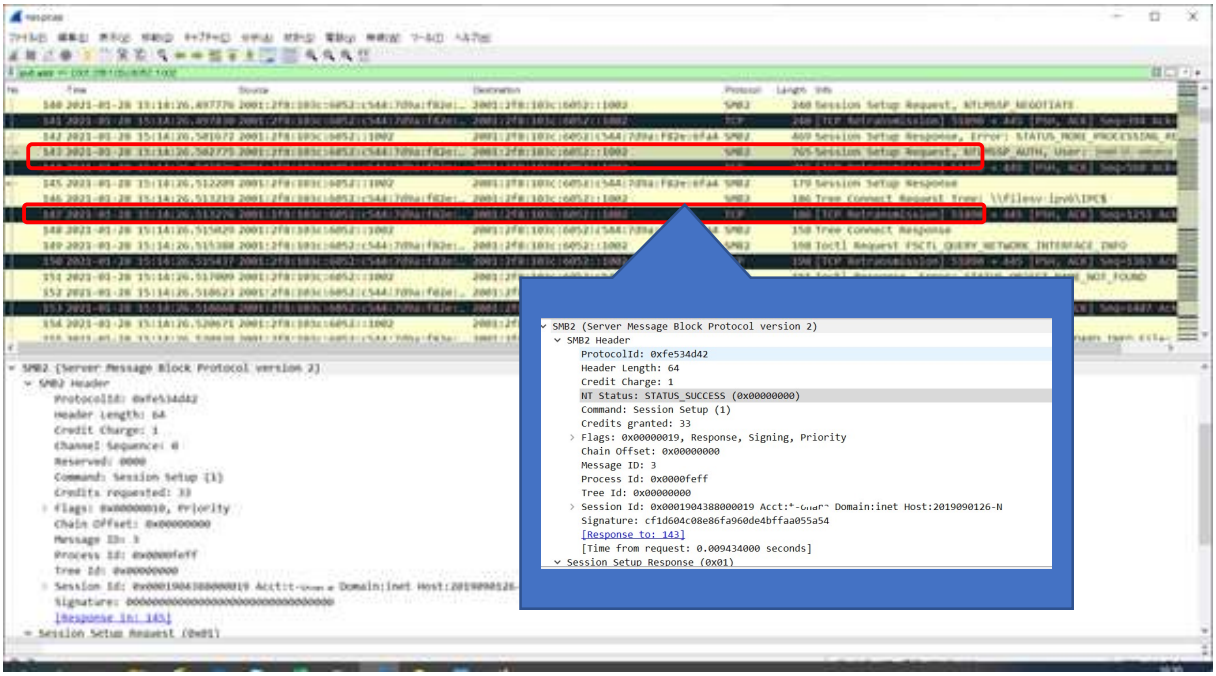


図 6.1.6-22 IPv6 優先端末でファイルサーバアクセス時のネットワークキャプチャ実行結果

【#2 の補足】 ※に関して

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

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

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

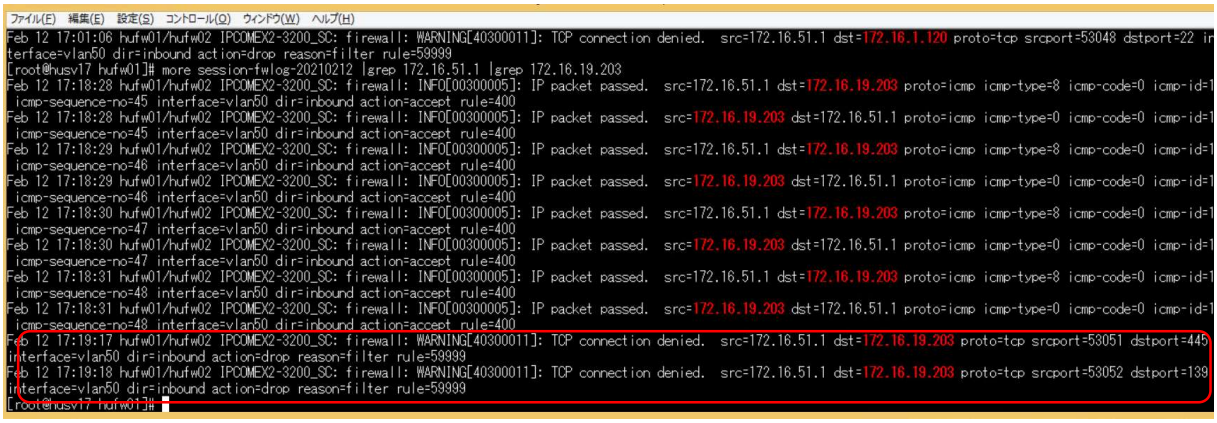


図 6.1.6-24 実証端末からIPv4アドレスでファイルサーバアクセス時のファイアウォールログ

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

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

3.　WAN 越しアプリケーションレベルの検証

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

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

(1)　業務アプリケーションにおける検証(クラウド)について

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

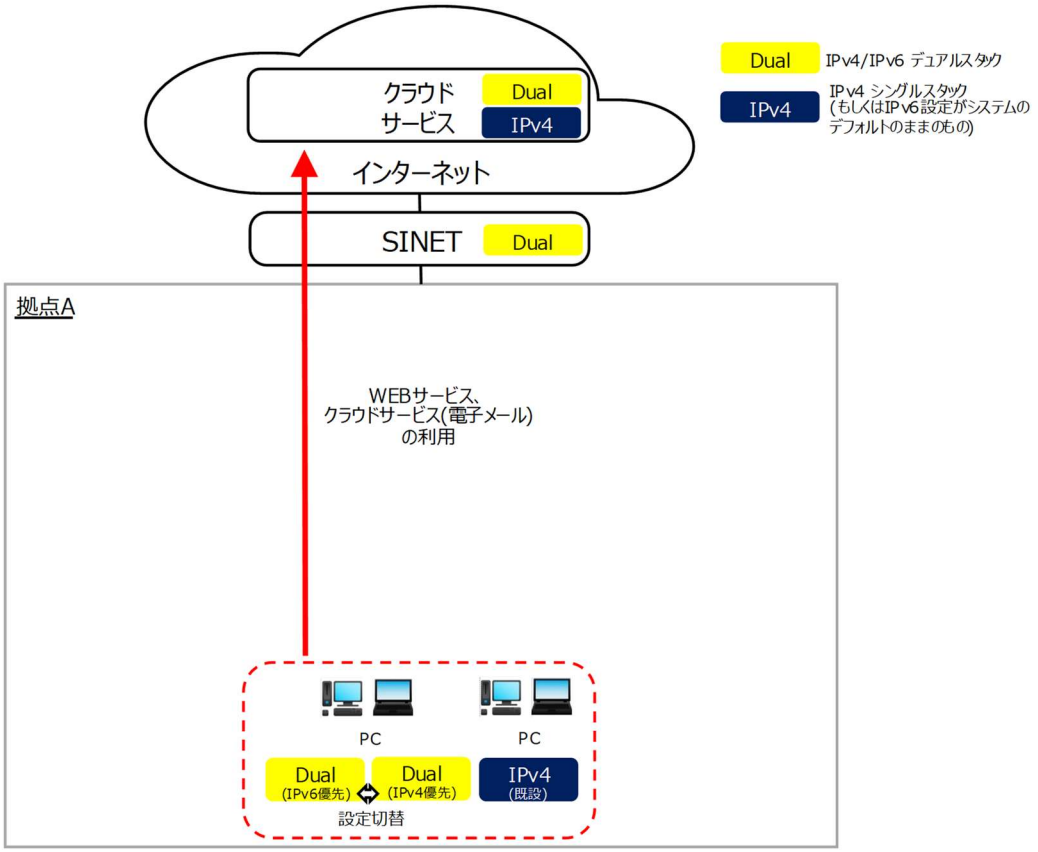


図　6.1.6-25　業務アプリケーションにおける検証(クラウド)範囲

① G Suite の動作検証

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

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

② Exchange Online の動作検証

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

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

上記①②のシナリオを実施した結果の内、主要な結果を以下に示す。

① G Suite の動作検証

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

【#1 の補足】

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

(a) nslookup コマンドでの名前解決状況確認

Gmail 実証時の nslookup コマンド実行結果を以下に記載する。

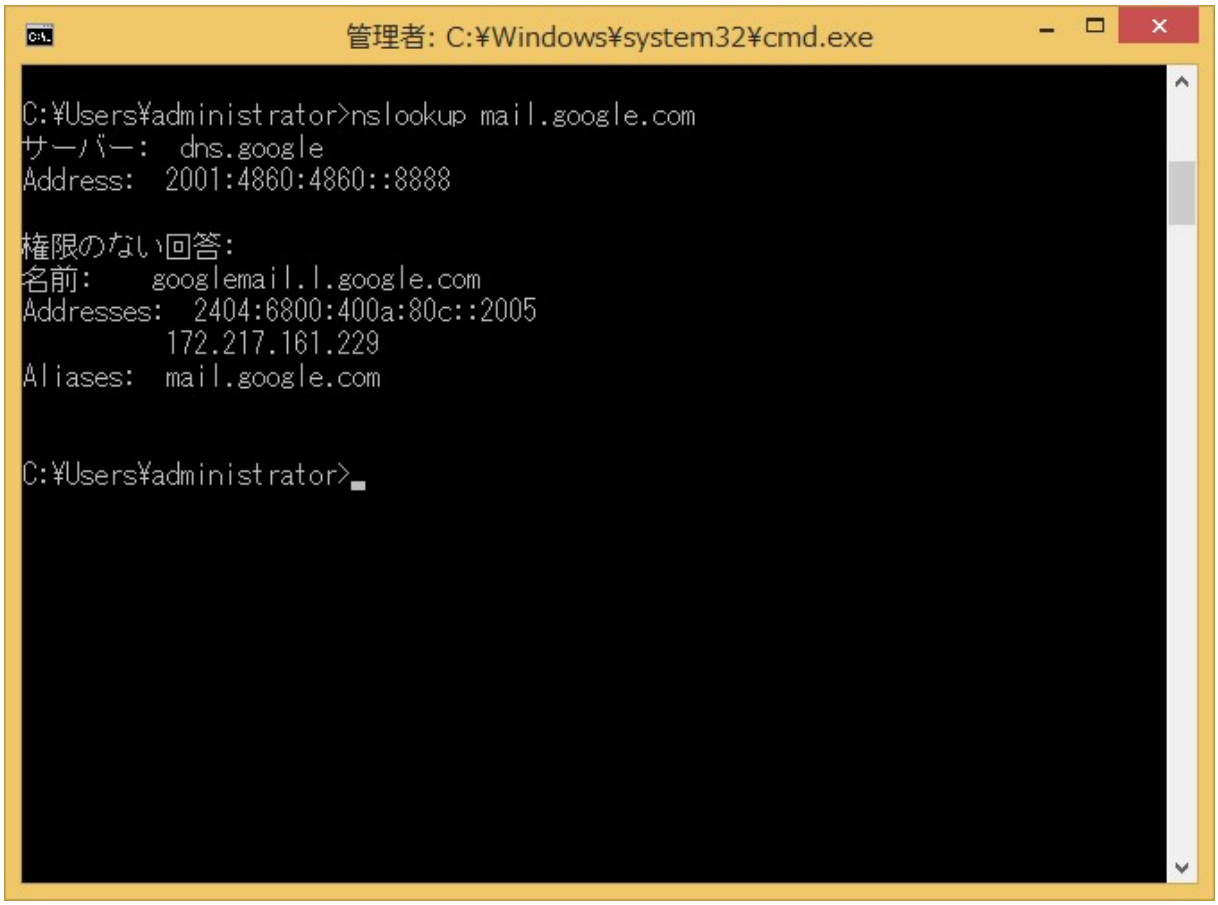


図 6.1.6-26 「mail.google.com」に対する nslookup 結果

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

(b)WEB メールが IPv6 で起動できているか

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

図 6.1.6-27 Gmail での利用者認証画面

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

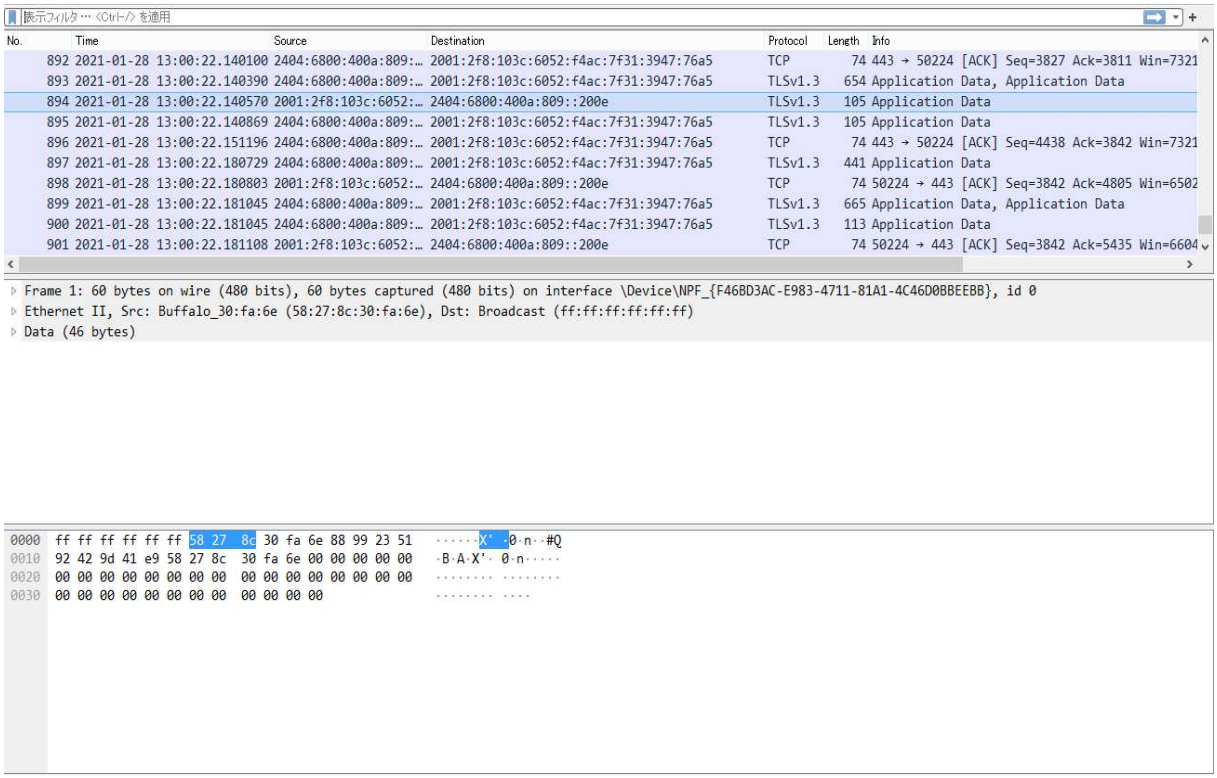


図 6.1.6-28 Gmail での利用者認証画面表示時のネットワークトレース結果

(c)メール送受信が IPv6 で正しく行えているか

Gmail にログイン後テストメールを送信し、正しく処理できているかどうかを確認した。

以下のようにテストメールを作成し、「送信」ボタンを押した後にテストメールを受信できることを確認いた。

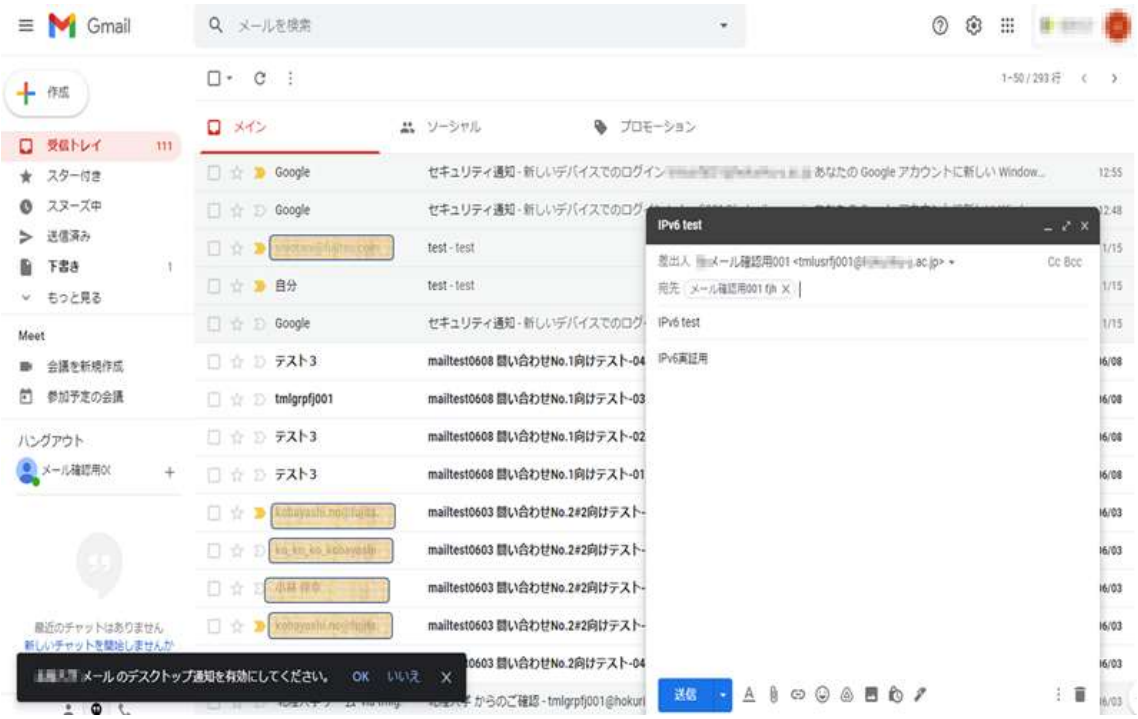


図 6.1.6-29 Gmail でのテストメール作成画面

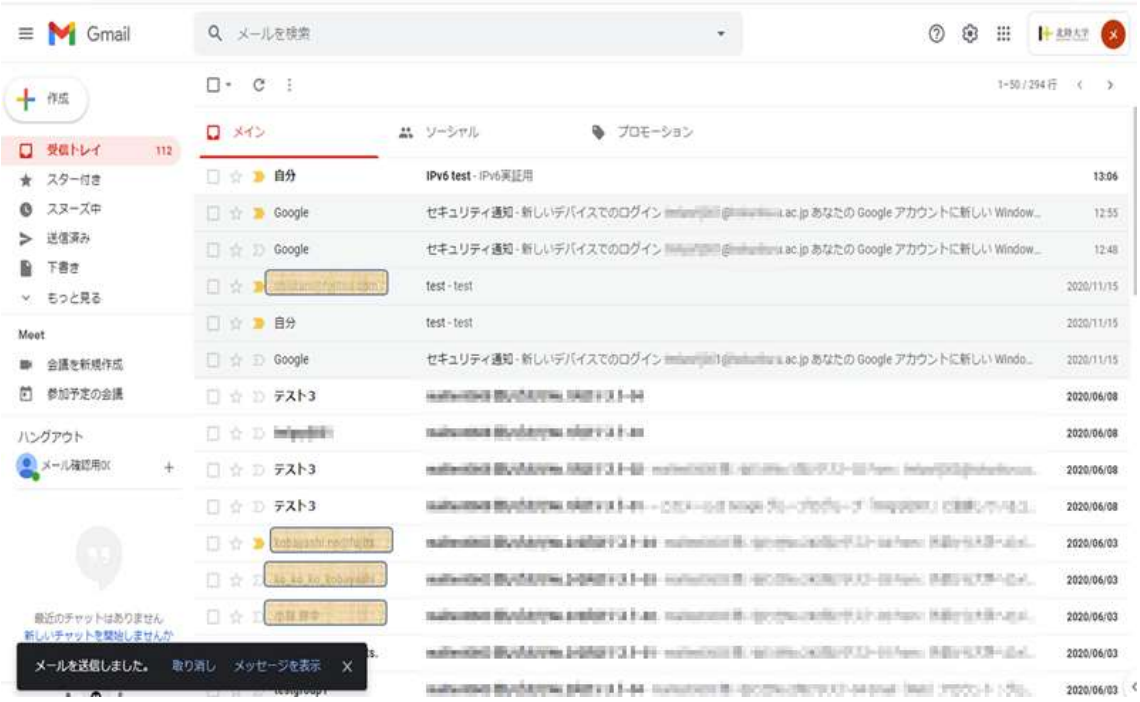


図 6.1.6-30 Gmail でのテストメール受信画面

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

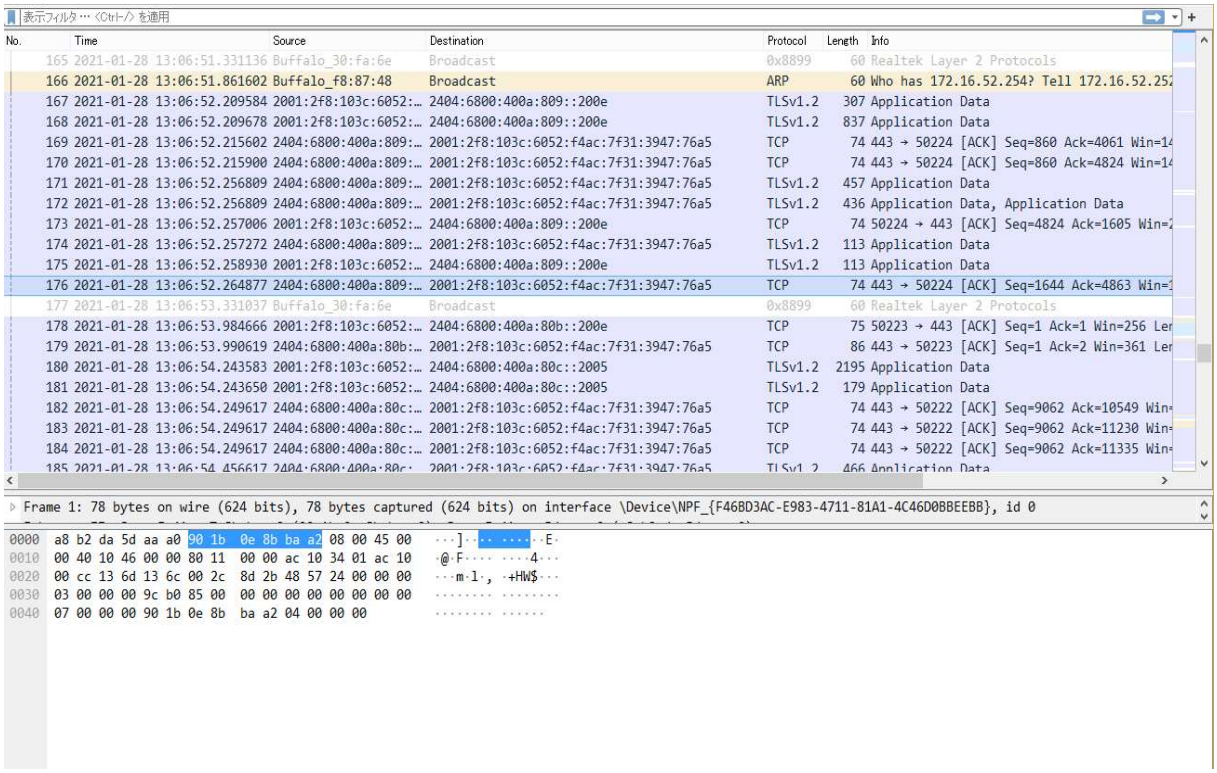


図 6.1.6-31 Gmail でのテストメール受信時のネットワークトレース結果

② Exchange Online の動作検証

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

【#1 の補足】

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

(a) nslookup コマンドでの名前解決状況確認

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

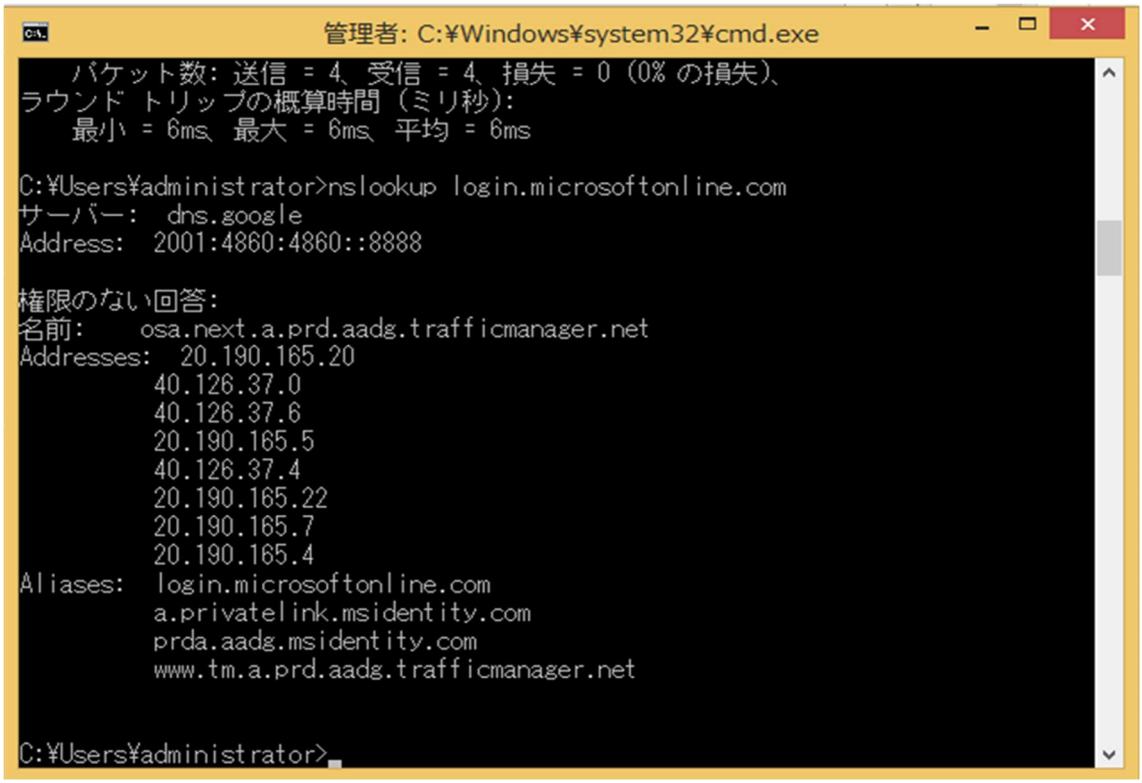


図 6.1.6-32 マイクロソフトオンラインサービスの nslookup 確認結果

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

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

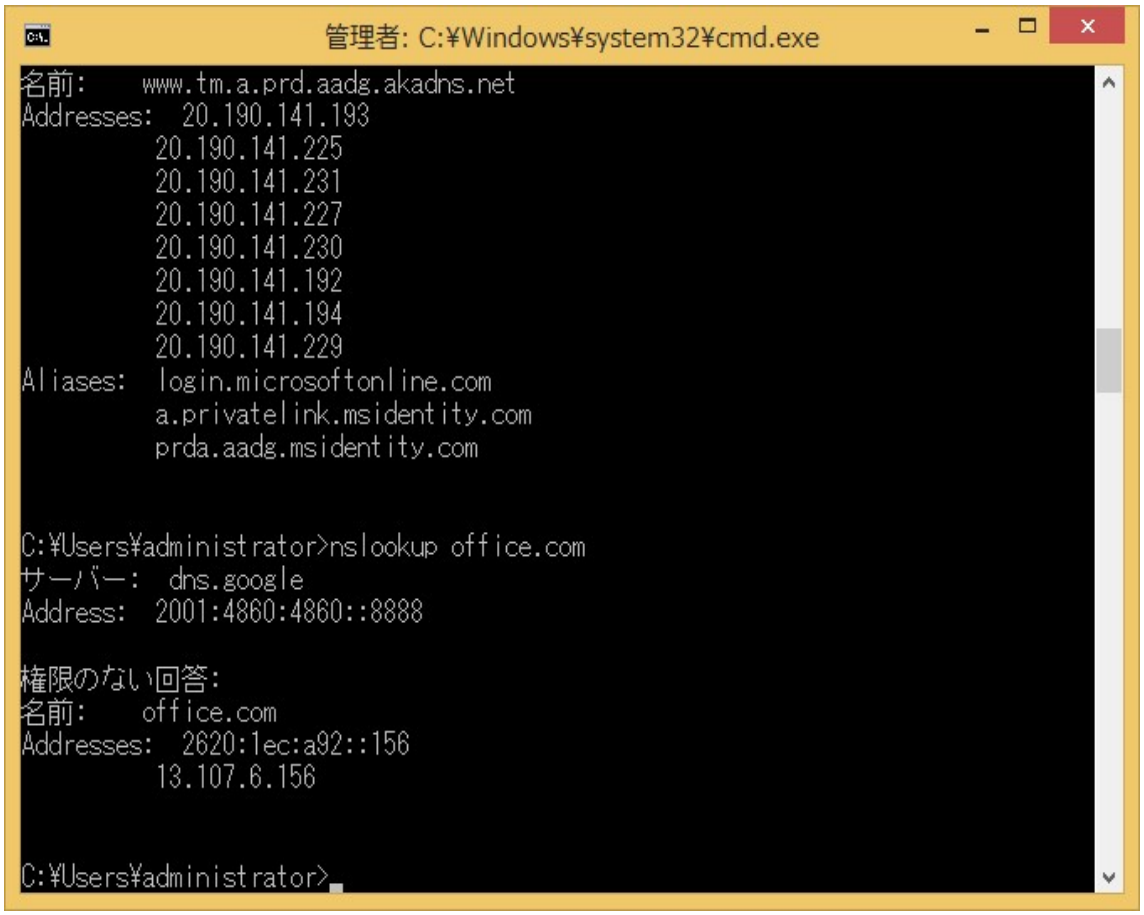


図 6.1.6-33 「office.com」の nslookup 確認結果

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

(b)WEB メールが IPv6 で起動できているか

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

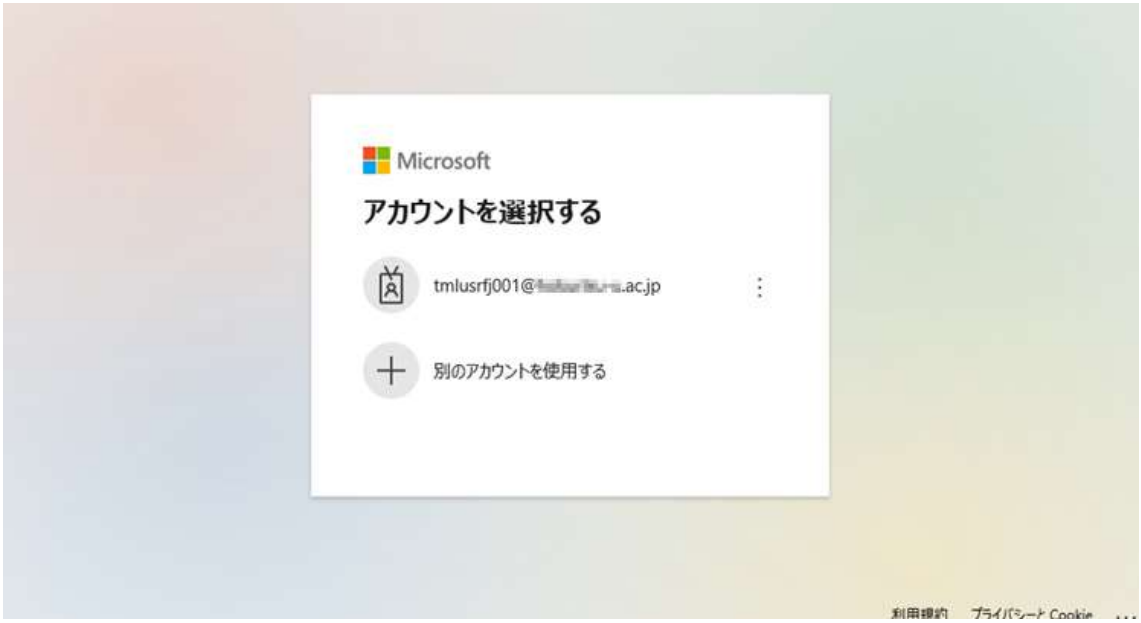


図 6.1.6-34 マイクロソフトオンラインサービスサインイン画面

上図の状態でのネットワークトレースを以下に記載する。

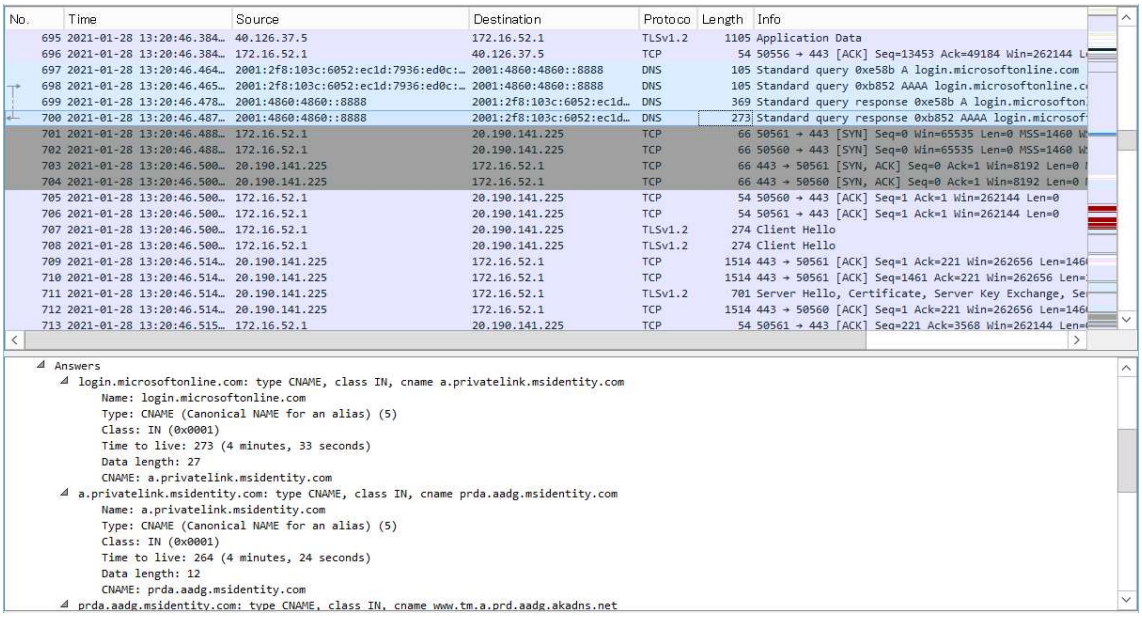


図 6.1.6-35 マイクロソフトオンラインサービスサインイン時のネットワークトレース結果

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

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

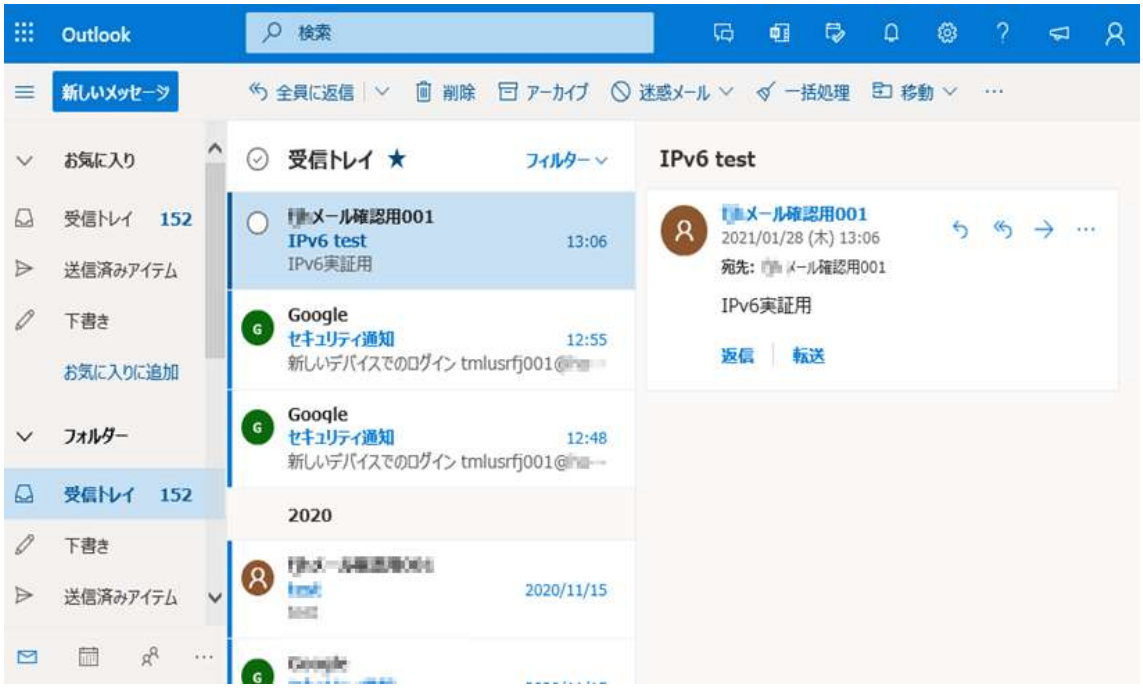


図 6.1.6-36 「office.com」から Outlook WEB メールを開いた状態

この状態でのネットワークトレースを以下に記載する。

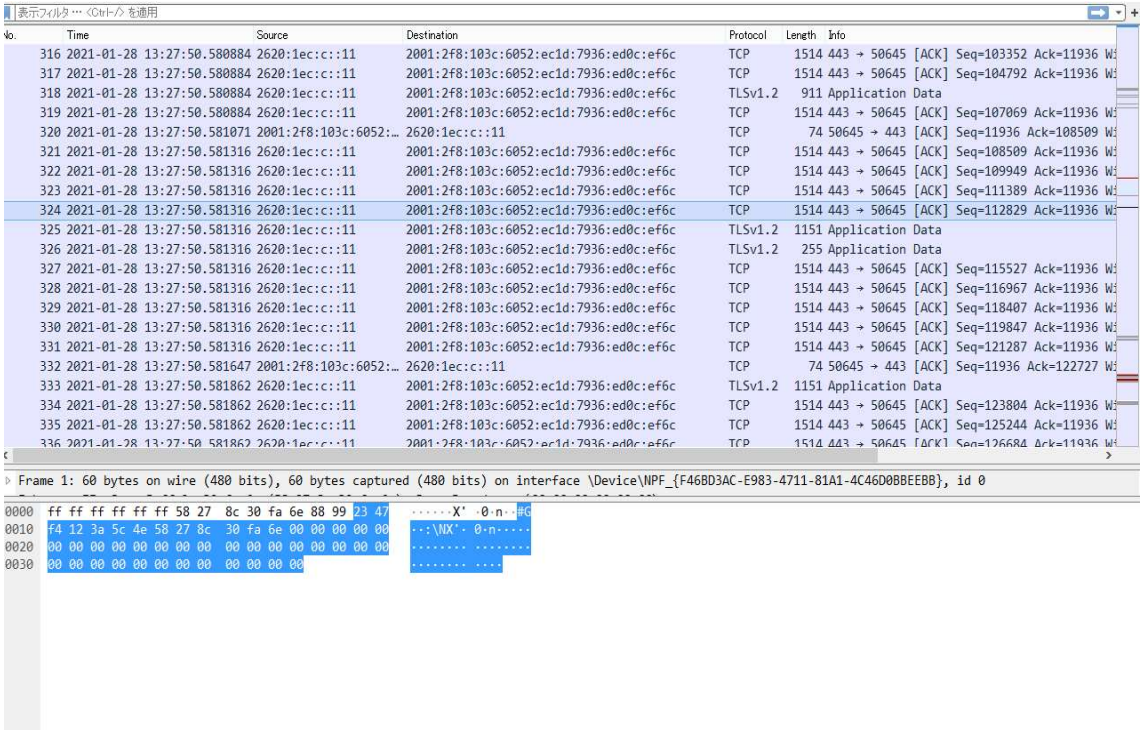


図 6.1.6-37 「office.com」から Outlook WEB メールを開いた状態でのネットワークトレース結果

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

(c)メール送受信が IPv6 で正しく行えているか

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

4. 運用性/保守性に関する検証

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

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

(1) IPv4/IPv6 デュアルスタックの基本的な設定の確認

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

① IPv6 アドレスの自動設定における検証

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

#	接続元機器名	有線無線	IPv4 IPv6	接続先機器名・サービス名	IPv4 IPv6	検証内容	想定結果	実施結果
2	デスクトップ PC	有線	IPv6 優先	実証用ネットワーク（LAN052） RA 送信有	IPv6（手動）	ipconfig /all を実行する	実行結果より以下の内容を確認する ・IPv6 アドレス：手動設定値 ・一時 IPv6 アドレス：自動設定 ・リンクローカル IPv6 アドレス：自動設定 ・以下、手動設定した値 – IPv4 アドレス – サブネット マスク – デフォルトゲートウェイ（IPv4） – デフォルトゲートウェイ（IPv6）	OK
3	ノート PC	無線	IPv6 優先	実証用ネットワーク（LAN052） RA 送信有	IPv6（手動）	ipconfig /all を実行する	実行結果より以下の内容を確認する ・IPv6 アドレス：手動設定値 ・一時 IPv6 アドレス：自動設定 ・リンクローカル IPv6 アドレス：自動設定 ・以下、手動設定した値 – IPv4 アドレス – サブネット マスク – デフォルトゲートウェイ（IPv4） – デフォルトゲートウェイ（IPv6）	OK

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

【#1の補足】

(a) IP アドレス割り当て状況の確認

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

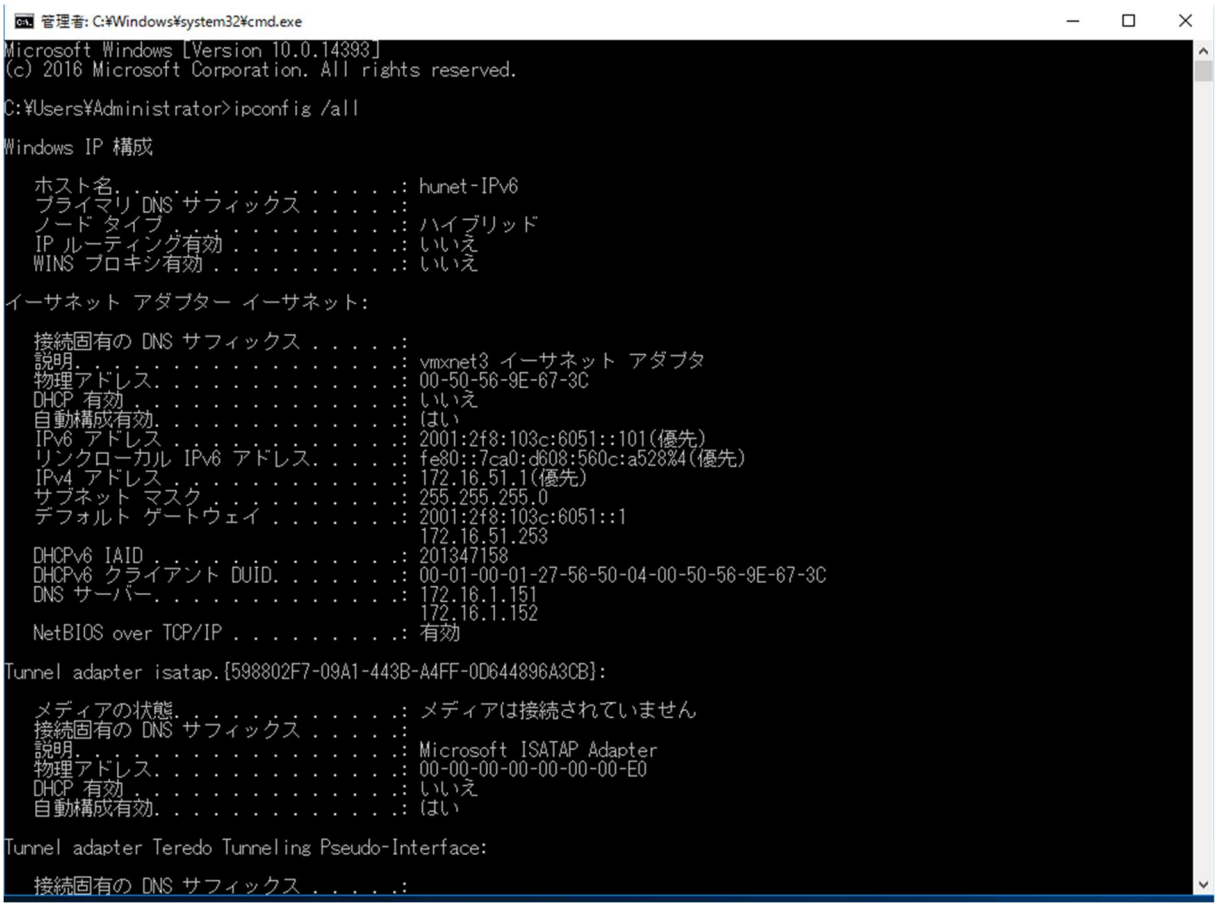


図 6.1.6-38 「ipconfig /all」実行結果(RA 未送信セグメント)

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

(b) ネットワークトレースに関する考察

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

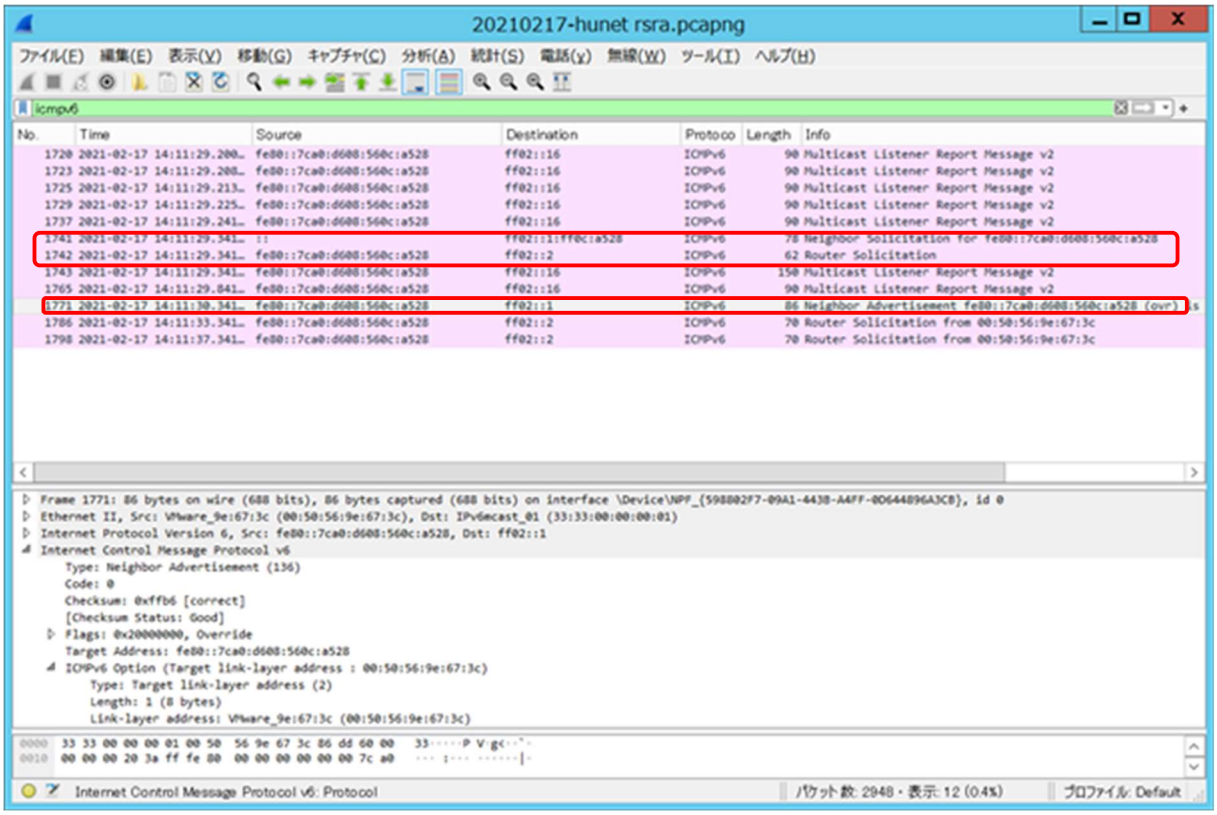


図 6.1.6-39 ネットワークトレースの状態(RA 未送信セグメント)

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

【#2 の補足】

(a) IP アドレス割り当て状況の確認

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

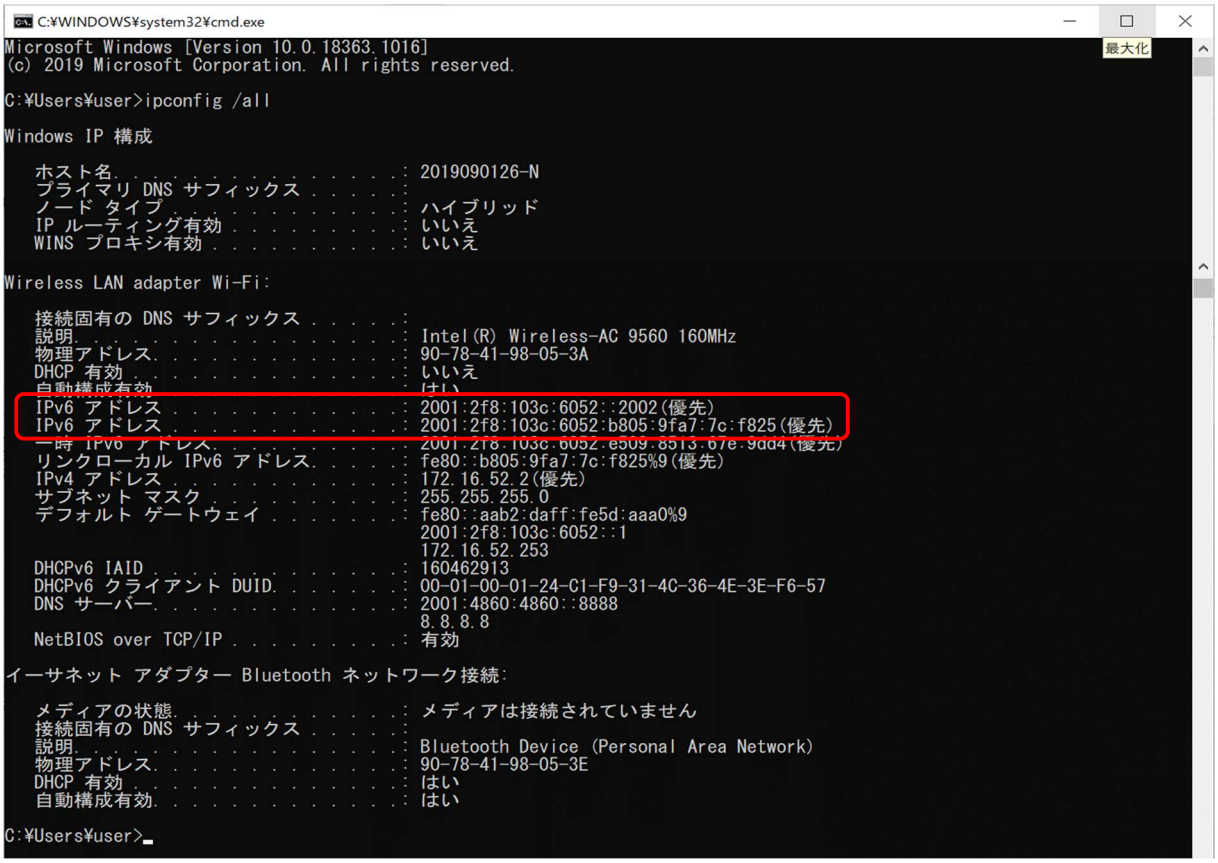


図 6.1.6-40 「ipconfig /all」実行結果(RA 送信セグメント)

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

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

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

(b) ネットワークトレースに関する考察

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

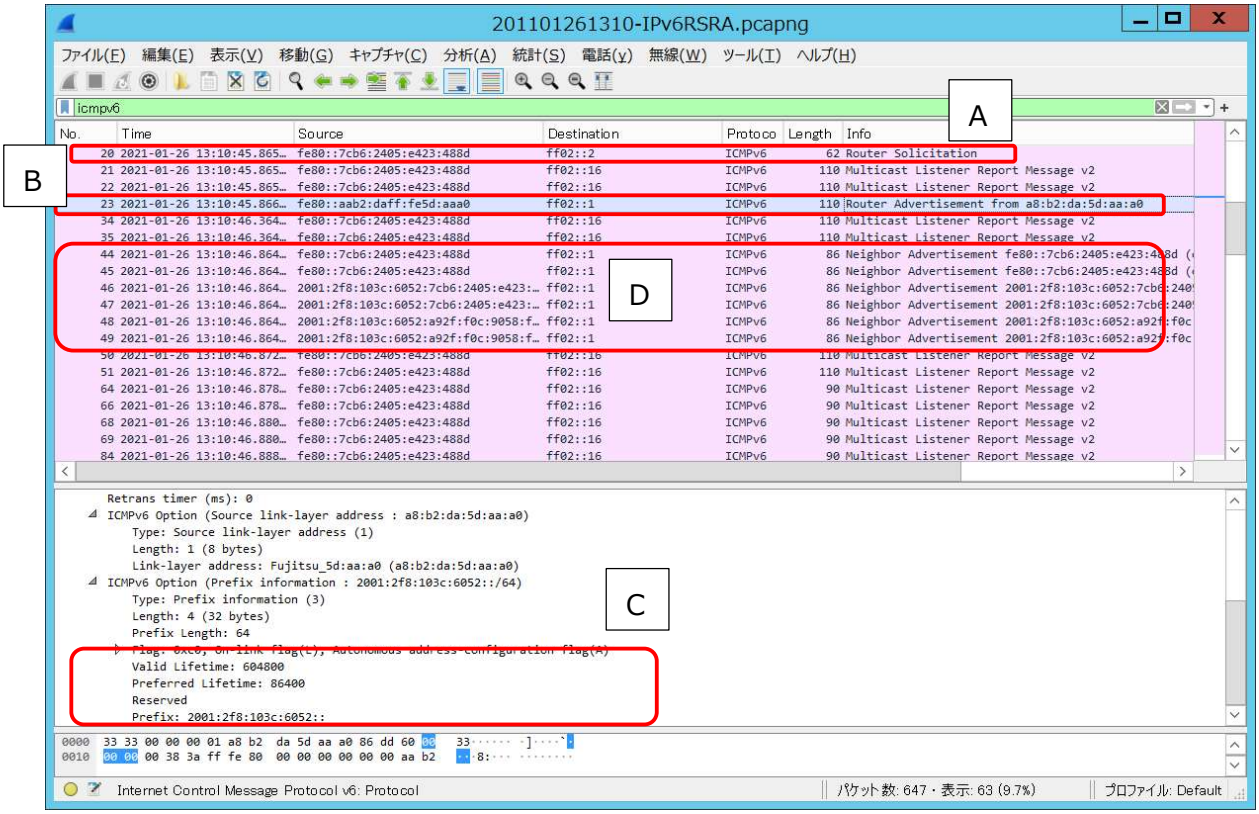


図 6.1.6-41 ネットワークトレースの状態(RA 送信セグメント)

20 フレーム目(A)で実証用 PC から近隣のルータ宛にマルチキャストで RS(Router Solicitation)が発行し、23 フレーム(B)ではルータ(実証用 L3 スイッチ)からマルチキャストで RA(Router Advertisement)が送信されていることを確認した。
ルータから送信された RA のフレームをネットワークトレース結果の詳細情報欄(C)に記載しているが、プレフィックス、デフォルトゲートウェイ、有効期限が通知されていることを確認した。

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

【#3 の補足】

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

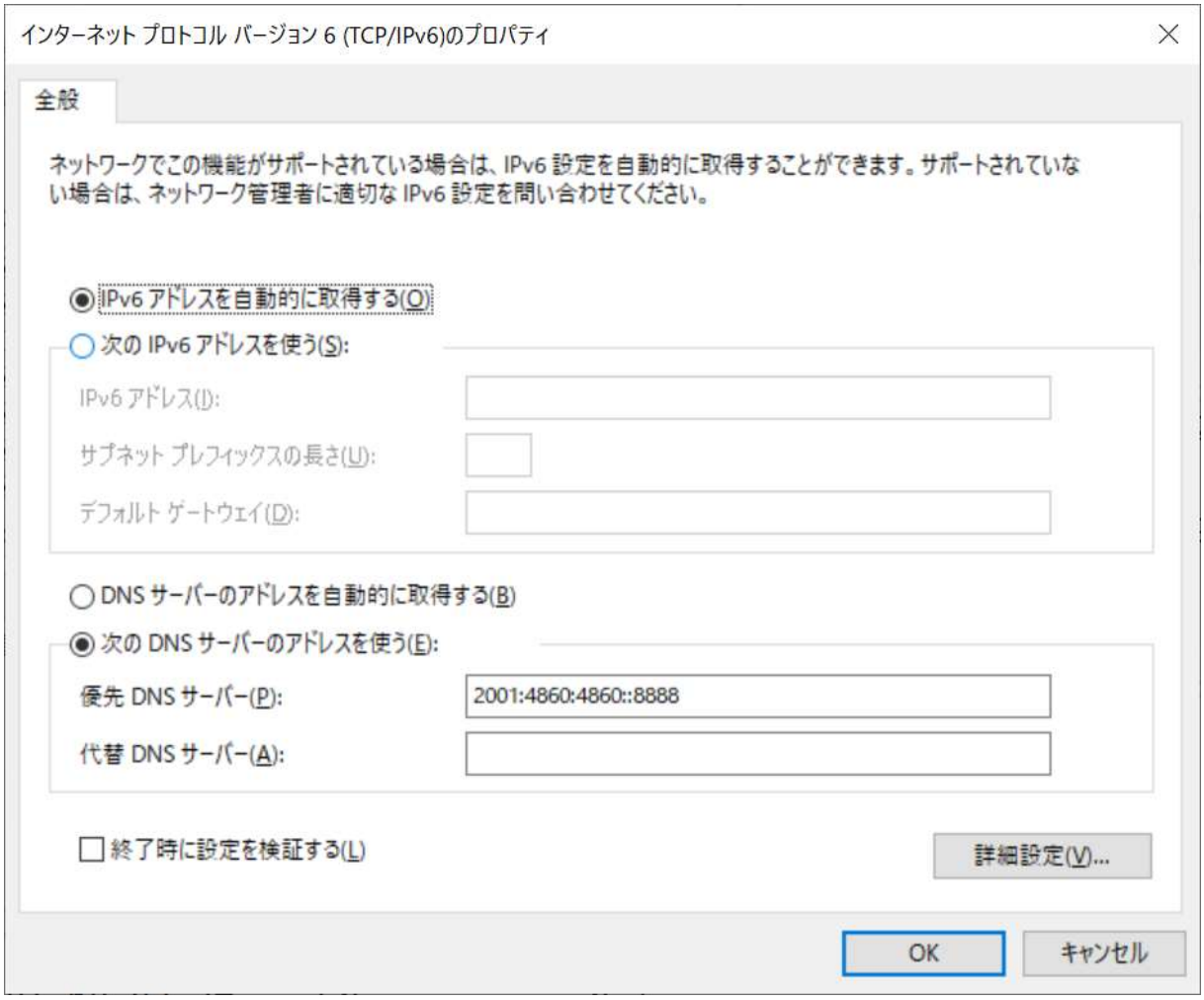


図 6.1.6-42 IPv6 アドレス自動構成を行う為の設定

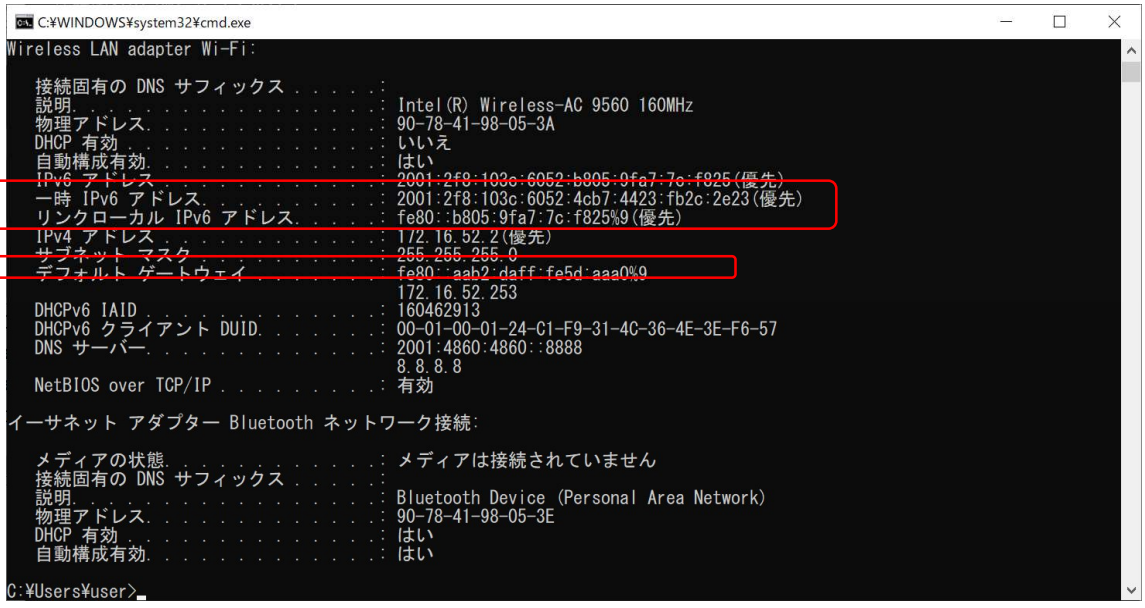


図 6.1.6-43 「ipconfig /all」実行結果(RA 送信セグメント:IPv6 アドレス自動構成)

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

(2) 運用性/保守性(ログ管理、トラブルシュート方式、端末追跡等)

IPv6 で通信を行う機器に関して、ログファイルや端末の IPv6 アドレスと MAC アドレスの関連付けについて、IPv4 実装時との運用的な違いについて実証を行った。

② 運用性/保守性における検証

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

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

【#1,#2 の補足】

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

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


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

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

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

```
# show ndp
IPv6 Address                              MAC Address        S F   Rest   Interface Port
----------------------------------------- ------------------ - --- ------ --------- ----
2001:2f8:103c:6050::1                     a8:b2:da:5d:aa:a0  R P   perm   lan50
2001:2f8:103c:6050::2                     00:80:17:ef:6d:43  R     00010  lan50      1
2001:2f8:103c:6051::1                     a8:b2:da:5d:aa:a0  R P   perm   lan51
2001:2f8:103c:6052::1                     a8:b2:da:5d:aa:a0  R P   perm   lan52
2001:2f8:103c:6052:3960:5cb5:a585:b6f3    90:1b:0e:8b:ba:a2  S     00721  lan52      19
fe80::280:17ff:feef:6d43%lan50            00:80:17:ef:6d:43  S     01179  lan50      1
fe80::aab2:daff:fe5d:aaa0%lan50           a8:b2:da:5d:aa:a0  R P   perm   lan50
fe80::aab2:daff:fe5d:aaa0%lan51           a8:                   erm    lan51
fe80::aab2:daff:fe5d:aaa0%lan52           a8:                   erm    lan52
    Entry:9
```


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

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

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

【#2 の補足】

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

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

```
[root@sv17 fw01]# ls
command-fwlog-20210105  message-fwlog-20181205  message-fwlog-20200704  session-fwlog-20180128.gz  session-fwlog-20190326.gz  session-fwlog-20200521
command-fwlog-20210106  message-fwlog-20181206  message-fwlog-20200706  session-fwlog-20180129.gz  session-fwlog-20190327.gz  session-fwlog-20200522
command-fwlog-20210107  message-fwlog-20181208  message-fwlog-20200707  session-fwlog-20180130.gz  session-fwlog-20190328.gz  session-fwlog-20200523
command-fwlog-20210108  message-fwlog-20181210  message-fwlog-20200708  session-fwlog-20180131.gz  session-fwlog-20190329.gz  session-fwlog-20200524
command-fwlog-20210112  message-fwlog-20181211  message-fwlog-20200709  session-fwlog-20180201.gz  session-fwlog-20190330.gz  session-fwlog-20200525
command-fwlog-20210127  message-fwlog-20181212  message-fwlog-20200710  session-fwlog-20180202.gz  session-fwlog-20190331.gz  session-fwlog-20200526
command-fwlog-20210212  message-fwlog-20181213  message-fwlog-20200712  session-fwlog-20180203.gz  session-fwlog-20190401.gz  session-fwlog-20200527
command-fwlog-20210216  message-fwlog-20181218  message-fwlog-20200713  session-fwlog-20180204.gz  session-fwlog-20190402.gz  session-fwlog-20200528
error-fwlog-20170601    message-fwlog-20181219  message-fwlog-20200714  session-fwlog-20180205.gz  session-fwlog-20190403.gz  session-fwlog-20200529
error-fwlog-20170615    message-fwlog-20181220  message-fwlog-20200715  session-fwlog-20180206.gz  session-fwlog-20190404.gz  session-fwlog-20200530
error-fwlog-20170629    message-fwlog-20181221  message-fwlog-20200716  session-fwlog-20180207.gz  session-fwlog-20190405.gz  session-fwlog-20200531
error-fwlog-20170713    message-fwlog-20181225  message-fw                                                                    session-fwlog-20200601
error-fwlog-20170727    message-fwlog-20181227  message-fw                                                                    session-fwlog-20200602
message-fwlog-20171107  message-fwlog-20191107  session-fw                                                                    session-fwlog-20201231
message-fwlog-20171108  message-fwlog-20191108  session-fw                                                                    session-fwlog-20210101
message-fwlog-20171109  message-fwlog-20191111  session-fw                                                                    session-fwlog-20210102
message-fwlog-20171112  message-fwlog-20191112  session-fw                                                                    session-fwlog-20210103
message-fwlog-20171113  message-fwlog-20191113  session-fw                                                                    session-fwlog-20210104
message-fwlog-20171115  message-fwlog-20191114  session-fwlog-20170719.gz  session-fwlog-20180914.gz  session-fwlog-20191110.gz  session-fwlog-20210105
message-fwlog-20171119  message-fwlog-20191115  session-fwlog-20170720.gz  session-fwlog-20180915.gz  session-fwlog-20191111.gz  session-fwlog-20210106
message-fwlog-20171121  message-fwlog-20191118  session-fwlog-20170721.gz  session-fwlog-20180916.gz  session-fwlog-20191112.gz  session-fwlog-20210107
message-fwlog-20171122  message-fwlog-20191119  session-fwlog-20170722.gz  session-fwlog-20180917.gz  session-fwlog-20191113.gz  session-fwlog-20210108
message-fwlog-20171124  message-fwlog-20191120  session-fwlog-20170723.gz  session-fwlog-20180918.gz  session-fwlog-20191114.gz  session-fwlog-20210109
message-fwlog-20171127  message-fwlog-20191121  session-fwlog-20170724.gz  session-fwlog-20180919.gz  session-fwlog-20191115.gz  session-fwlog-20210110
message-fwlog-20171128  message-fwlog-20191122  session-fwlog-20170725.gz  session-fwlog-20180920.gz  session-fwlog-20191116.gz  session-fwlog-20210111
message-fwlog-20171130  message-fwlog-20191125  session-fwlog-20170726.gz  session-fwlog-20180921.gz  session-fwlog-20191117.gz  session-fwlog-20210112
message-fwlog-20171201  message-fwlog-20191126  session-fwlog-20170727.gz  session-fwlog-20180922.gz  session-fwlog-20191118.gz  session-fwlog-20210113
message-fwlog-20171203  message-fwlog-20191127  session-fwlog-20170728.gz  session-fwlog-20180923.gz  session-fwlog-20191119.gz  session-fwlog-20210114
message-fwlog-20171204  message-fwlog-20191128  session-fwlog-20170729.gz  session-fwlog-20180924.gz  session-fwlog-20191120.gz  session-fwlog-20210115
message-fwlog-20171205  message-fwlog-20191129  session-fwlog-20170730.gz  session-fwlog-20180925.gz  session-fwlog-20191121.gz  session-fwlog-20210116
message-fwlog-20171206  message-fwlog-20191201  session-fwlog-20170731.gz  session-fwlog-20180926.gz  session-fwlog-20191122.gz  session-fwlog-20210117
message-fwlog-20171207  message-fwlog-20191202  session-fwlog-20170801.gz  session-fwlog-20180927.gz  session-fwlog-20191123.gz  session-fwlog-20210118
message-fwlog-20171208  message-fwlog-20191203  session-fwlog-20170802.gz  session-fwlog-20180928.gz  session-fwlog-20191124.gz  session-fwlog-20210119
message-fwlog-20171209  message-fwlog-20191204  session-fwlog-20170803.gz  session-fwlog-20180929.gz  session-fwlog-20191125.gz  session-fwlog-20210120
message-fwlog-20171211  message-fwlog-20191205  session-fwlog-20170804.gz  session-fwlog-20180930.gz  session-fwlog-20191126.gz  session-fwlog-20210121
message-fwlog-20171212  message-fwlog-20191206  session-fwlog-20170805.gz  session-fwlog-20181001.gz  session-fwlog-20191127.gz  session-fwlog-20210122
message-fwlog-20171213  message-fwlog-20191209  session-fwlog-20170806.gz  session-fwlog-20181002.gz  session-fwlog-20191128.gz  session-fwlog-20210123
message-fwlog-20171214  message-fwlog-20191210  session-fwlog-20170807.gz  session-fwlog-20181003.gz  session-fwlog-20191129.gz  session-fwlog-20210124
message-fwlog-20171215  message-fwlog-20191211  session-fwlog-20170808.gz  session-fwlog-20181004.gz  session-fwlog-20191130.gz  session-fwlog-20210125
message-fwlog-20171216  message-fwlog-20191212  session-fwlog-20170809.gz  session-fwlog-20181005.gz  session-fwlog-20191201.gz  session-fwlog-20210126
message-fwlog-20171219  message-fwlog-20191213  session-fwlog-20170810.gz  session-fwlog-20181006.gz  session-fwlog-20191202.gz  session-fwlog-20210127
message-fwlog-20171220  message-fwlog-20191214  session-fwlog-20170811.gz  session-fwlog-20181007.gz  session-fwlog-20191203.gz  session-fwlog-20210128
message-fwlog-20171221  message-fwlog-20191215  session-fwlog-20170812.gz  session-fwlog-20181008.gz  session-fwlog-20191204.gz  session-fwlog-20210129
message-fwlog-20171222  message-fwlog-20191216  session-fwlog-20170813.gz  session-fwlog-20181009.gz  session-fwlog-20191205.gz  session-fwlog-20210130
message-fwlog-20171224  message-fwlog-20191217  session-fwlog-20170814.gz  session-fwlog-20181010.gz  session-fwlog-20191206.gz  session-fwlog-20210131
message-fwlog-20171226  message-fwlog-20191218  session-fwlog-20170815.gz  session-fwlog-20181011.gz  session-fwlog-20191207.gz  session-fwlog-20210201
message-fwlog-20171227  message-fwlog-20191219  session-fwlog-20170816.gz  session-fwlog-20181012.gz  session-fwlog-20191208.gz  session-fwlog-20210202
message-fwlog-20171230  message-fwlog-20191220  session-fwlog-20170817.gz  session-fwlog-20181013.gz  session-fwlog-20191209.gz  session-fwlog-20210203
message-fwlog-20180102  message-fwlog-20191222  session-fwlog-20170818.gz  session-fwlog-20181014.gz  session-fwlog-20191210.gz  session-fwlog-20210204
message-fwlog-20180104  message-fwlog-20191223  session-fwlog-20170819.gz  session-fwlog-20181015.gz  session-fwlog-20191211.gz  session-fwlog-20210205
message-fwlog-20180105  message-fwlog-20191224  session-fwlog-20170820.gz  session-fwlog-20181016.gz  session-fwlog-20191212.gz  session-fwlog-20210206
message-fwlog-20180109  message-fwlog-20191226  session-fwlog-20170821.gz  session-fwlog-20181017.gz  session-fwlog-20191213.gz  session-fwlog-20210207
message-fwlog-20180110  message-fwlog-20191227  session-fwlog-20170822.gz  session-fwlog-20181018.gz  session-fwlog-20191214.gz  session-fwlog-20210208
message-fwlog-20180111  message-fwlog-20191228  session-fwlog-20170823.gz  session-fwlog-20181019.gz  session-fwlog-20191215.gz  session-fwlog-20210209
message-fwlog-20180113  message-fwlog-20191229  session-fwlog-20170824.gz  session-fwlog-20181020.gz  session-fwlog-20191216.gz  session-fwlog-20210210
message-fwlog-20180114  message-fwlog-20191230  session-fwlog-20170825.gz  session-fwlog-20181021.gz  session-fwlog-20191217.gz  session-fwlog-20210211
message-fwlog-20180115  message-fwlog-20200104  session-fwlog-20170826.gz  session-fwlog-20181022.gz  session-fwlog-20191218.gz  session-fwlog-20210212
message-fwlog-20180116  message-fwlog-20200106  session-fwlog-20170827.gz  session-fwlog-20181023.gz  session-fwlog-20191219.gz  session-fwlog-20210213
message-fwlog-20180117  message-fwlog-20200107  session-fwlog-20170828.gz  session-fwlog-20181024.gz  session-fwlog-20191220.gz  session-fwlog-20210214
message-fwlog-20180118  message-fwlog-20200108  session-fwlog-20170829.gz  session-fwlog-20181025.gz  session-fwlog-20191221.gz  session-fwlog-20210215
message-fwlog-20180122  message-fwlog-20200109  session-fwlog-20170830.gz  session-fwlog-20181026.gz  session-fwlog-20191222.gz  session-fwlog-20210216
message-fwlog-20180123  message-fwlog-20200110  session-fwlog-20170831.gz  session-fwlog-20181027.gz  session-fwlog-20191223.gz  session-fwlog-20210217
message-fwlog-20180124  message-fwlog-20200112  session-fwlog-20170901.gz  session-fwlog-20181028.gz  session-fwlog-20191224.gz
message-fwlog-20180125  message-fwlog-20200114  session-fwlog-20170902.gz  session-fwlog-20181029.gz  session-fwlog-20191225.gz
```

実証用 FW 装置のセッションログ

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

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

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

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

図 6.1.6-47 ファイアウォールルールで破棄された場合のログ

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

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

本事例では、実証用PCからGoogle社のサイトにアクセスした際、実証用 FW 装置の実証用ネットワークインターフェース(vlan50)で 5228/tcp（Google Playstore）からの応答を拒否し、パケットを破棄したケースとなる。

次に実証用 FW 装置のルールにより通過許可を行った場合の実例を説明する。

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

図 6.1.6-48 ファイアウォールルールで通過許可された場合のログ

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

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

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

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

6.1.6.2　課題と対応

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

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

(1) 機器/サービス仕様における課題

本検証において導入しようとした IPv6 対応を謳う機器/サービスの内、本検証では、IPv6 の利用可否が確認できず、機器メーカのサポート等に確認した結果、IPv6 対応が十分でないことが判明した課題と対応の事例を示す。

(2) IPv6 対応における留意事項(構築時の Tips)

本検証において実際に発生した IPv6 関連のトラブルシュート事例をもとに、IPv6 対応において普遍的に留意すべき点を示す。

7　IPv6 環境への移行に向けたコスト試算の考え方

7.1　システム開発におけるコストの構成要素

システム開発におけるコストは一般的に 3 つの要素で構成されている。まず 1 つ目は「アプリケーション」の開発・運用である。つぎに 2 つ目はアプリケーションの基盤となる「インフラ」の整備である。そして 3 つ目は機器やサービスの「調達」である。

この 3 つの構成要素はシステム開発に係るコストを算出する際の指針として活用できる。また、別軸としてシステム開発に係るコストを初期コストと運用コストに分けて算出することで、システム開発に必要となる総コスト(システム導入から運用および維持・管理までを含めた総額)の把握がしやすくなる。システム開発におけるコストの構成要素についてイメージを図 7.1-1 に示す。

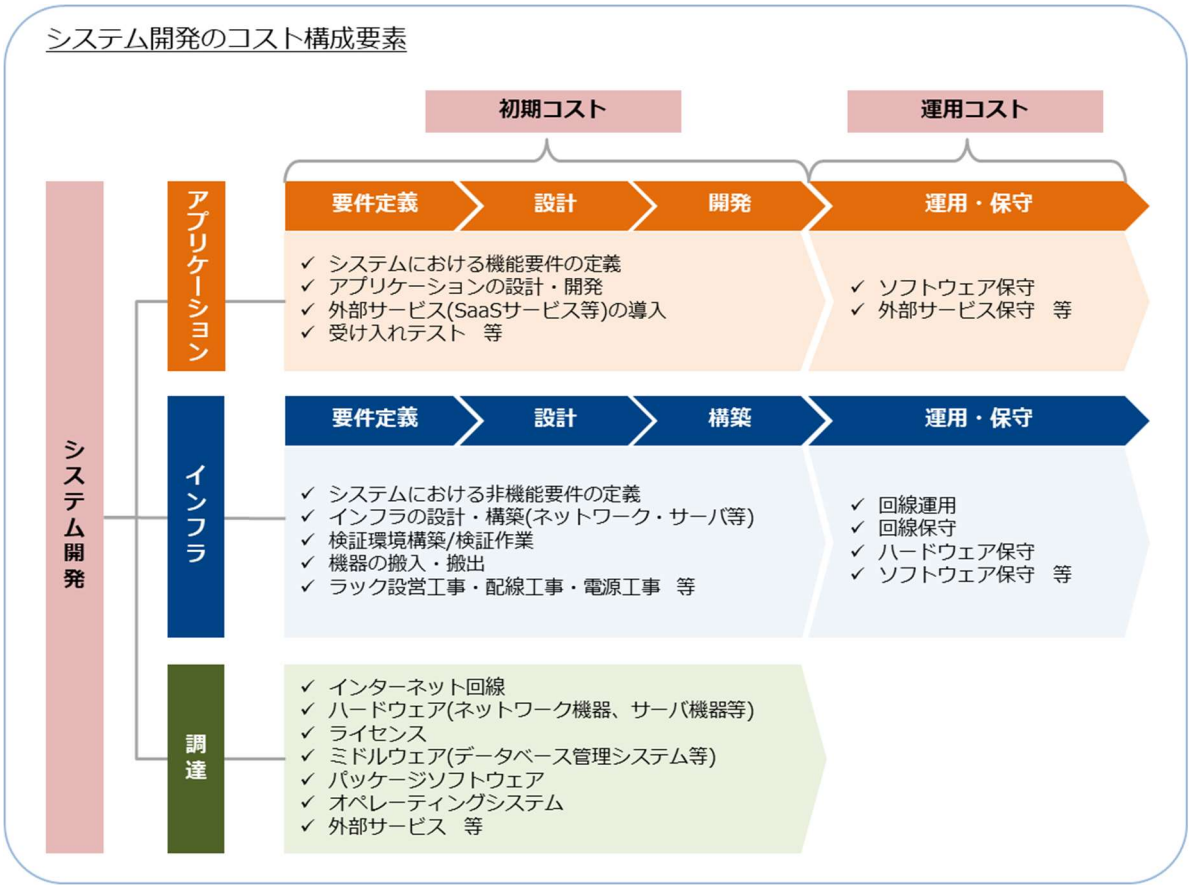


図 7.1-1 システム開発のコスト構成要素

7.1.1 アプリケーション開発・運用に係るコスト

アプリケーション開発は要件定義、設計、開発のプロセスに沿って行われる。この一連のプロセスに係る作業がコスト対象となる。またアプリケーションとして SaaS サービス等の外部サービスを導入する組織が増加している。その場合、アプリケーションの開発コストは抑えられる一方で、外部サービスの仕様確認や導入するための機能設定およびリリースに向けた受け入れテスト等の作業が発生する。そのため、これらの作業に係るコストについても算出する必要がある。

アプリケーションの運用においてはバグや欠陥による動作不良の改修等、ソフトウェア保守がコストの比重を占める。また外部サービスの保守においてはサービス事業者に一任できるが、サービスによっては保守サポートについて別途、有償契約となる場合もあるため、コスト面で注意が必要である。

7.1.2 インフラ整備に係るコスト

インフラはハードウェア(ネットワーク機器やサーバ等)を導入し、アプリケーションの安定稼働を支える基盤を指す。インフラの整備ではシステムの安定稼働に対する要求に基づき、要件定義、設計、構築のプロセスに沿って行われる。この一連のプロセスに係る作業がコスト対象となる。また、付帯作業として配線工事や電源工事等が発生するため、これらの作業に係るコストについても算出が必要である。

インフラの運用においては機器のハードウェア故障やソフトウェアの不具合等が発生する可能性があるため、ハードウェアおよびソフトウェアの両面で保守に係るコストの算出が必要である。

7.1.3 調達に係るコスト

システムはアプリケーションとインフラで構成されているため、システム開発を行うためには要件に適合した機器等を調達する必要がある。調達には購入コストが大きな比重を占める。また、事業が拡大するにつれてシステム増強を検討する必要が出てくるため、調達する際は要件に定めたスペックだけではなく、将来的な拡張性にも考慮した選定が必要である。

7.2　IPv6 対応におけるコスト試算の考え方

IPv6 環境への移行を促進する背景には IoT 社会の到来が関係している。IoT 技術の進展・普及により、広範な産業分野で IoT を活用したシステムが創出されている。

総務省の令和 2 年情報通信白書[67]にて公表されている通り、世界の IoT デバイスの数は 2022 年には 345 億台を超えるといわれている。IoT 社会において、スマートフォンや PC だけでなく、ウェアラブル機器、ネット家電、ドローン、自動車、ロボット等、大量のデバイスが無線でインターネットに接続するようになる。これらの大量のデバイス間を円滑に通信するためには事実上無限である IPv6 アドレスが不可欠である。IoT デバイスは右肩上がりに増加傾向にあるため、IoT 社会の実現は IPv6 環境への移行を後押しする契機になると考える。

一方で、IPv6 環境へ移行するにあたり、移行に係るコストの検討も必要である。IoT 社会により、IPv6 の時代へシフトしていくことが予想される。IPv6 通信がデフォルトとなってから内部環境の IPv6 対応を検討し始める段階ではシステムの IPv6 対応に伴い、全面的な更改が必要となる可能性がある。システムの刷新には大幅なコスト増が見込まれるため、システムライフサイクル等のタイミングを活かし、計画的に移行していくことが望ましい。

移行には一定のコストが発生するが、コストの大小は移行範囲によって異なる。そのため、計画的に移行を進めることで大幅なコスト増とならないよう調整することが重要である。

本節では IPv6 対応におけるコストの考え方を 7.1 のシステム開発におけるコストの構成要素に基づき、「アプリケーション」と「インフラ(調達を含む)」の観点から示す。

---

67 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nb000000.html

7.2.1 アプリケーションの IPv6 対応に係るコスト

アプリケーションはオンプレミスで開発されたものと SaaS サービス等の外部サービスに分類することができる。これらの IPv6 対応に係るコストの考え方を以下に示す。

(1) アプリケーション(オンプレミス)の IPv6 対応

アプリケーションを IPv6 対応する際には、初期コストとしてまず、アプリケーションの仕様調査を行い、IPv4 に依存している要素の洗い出し等に作業コストが発生する。つぎに IPv6 を正しく解釈し、処理を実行できるように改修するための設計・開発コストが発生する。そして改修後のアプリケーションをリリースするための導入に係るコストも算出する必要がある。

運用コストについてはバグや欠陥による動作不良の改修等、ソフトウェア保守のコストが発生するが、リリース判定にて IPv6 起因での動作影響がないことが確認されている場合、不具合に対する改修は従来通りのソフトウェア保守として賄える想定のため、IPv6 対応前後で大幅なコスト増にはなりにくいと考える。

一方でアプリケーション単体だけでなく、基盤となるインフラにも目を向ける必要がある。アプリケーションのみの IPv6 対応を計画していたとしても、ネットワーク機器やサーバ等が IPv6 対応していない場合には、7.2.2 に示す通り、インフラの IPv6 対応として追加コストが発生する。アプリケーションの IPv6 対応に係るコスト比較イメージを図 7.2-1 に示す。

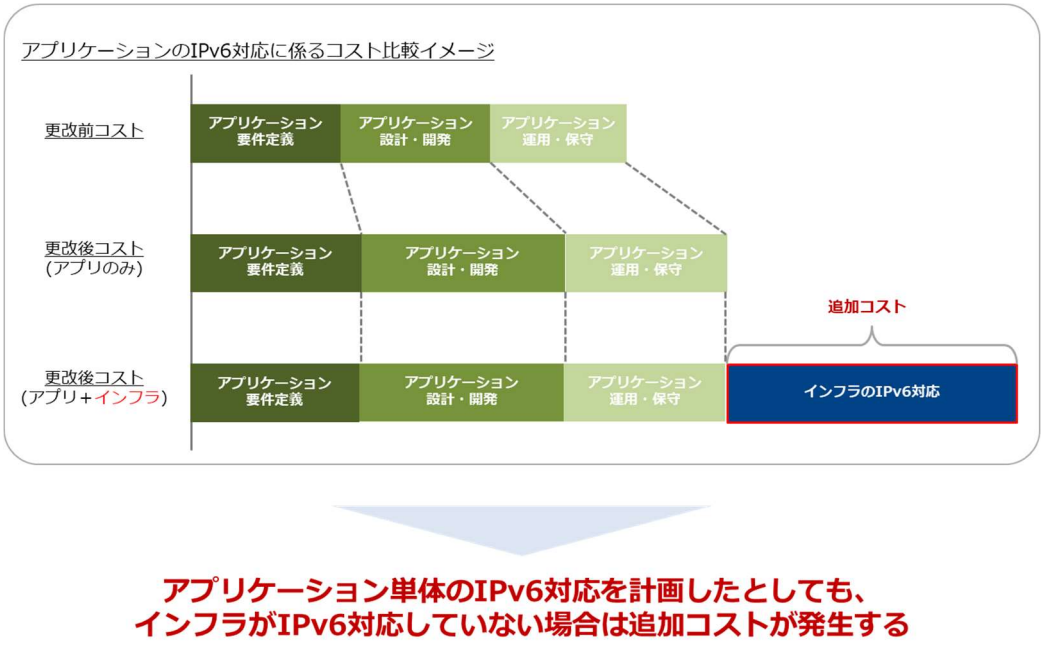


図 7.2-1 アプリケーションの IPv6 対応に係るコスト比較イメージ

(2) 外部サービスの IPv6 対応

IPv6 対応として外部サービスを切り替える際には、まず初期コストとして代替サービスの調査や切り替えに伴う初期設定、データ移行、受け入れテスト等のコストが発生する。つぎに運用コストとしてサービス利用費が大きな比重を占める。サービスプランによってコストが変動するケースが考えられるため、サービス事業者へプラン内容を確認し、サービス利用費が現行サービスより増加しないかコスト差には注意が必要である。

7.2.2 インフラの IPv6 対応に係るコスト

インフラはネットワーク機器やサーバ等のシステム基盤とインターネット接続で必要となる回線に分類することができる。これらの IPv6 対応に係るコストの考え方を以下に示す。

(1) インフラの IPv6 対応

インフラ(ネットワーク機器やサーバ等)が IPv6 に対応していない場合は機器更改が必要となる。IT 資産の管理としてライフサイクルの視点から考えていることが多いため、機器更改についてはライフサイクルに合わせて実施するケースが一般的である。

機器更改するにあたり、まず初期コストとして機器の調達コストが発生する。IPv6 対応が進んでいる通信事業者側でも利用されている通り、ネットワーク機器やサーバ等は IPv6 対応している機器が主流である。そのため、機器については現行機器と同価格帯での調達が想定される。

一方で要件定義、設計・構築および運用・保守においては IPv6 に関わる部分で一定の追加コストが想定される。しかし、機器ベンダより IPv6 の設定事例やトラブルシューティング事例等が公開されてきているため、それらを参照することで作業コストの縮減につながる。また、機器更改は拠点単位やシステム単位で段階的に実施するケースが一般的であるため、機器更改を進めていく中で IPv6 に関するノウハウを蓄積されていくと想定する。その結果、IPv6 に習熟していくことで設計・構築および運用・保守に係るコストを比較的抑えられると考える。

インフラの IPv6 対応においては従来通りのライフサイクルに沿って、機器更改していくことで同価格帯の機器に対して IPv6 の設定を付け足すイメージで実施することできると考える。そのため、IPv6 対応が起因して大幅なコスト増にはなりにくいと考える。機器の IPv6 対応に係るコスト比較イメージを図 7.2-2 に示す。

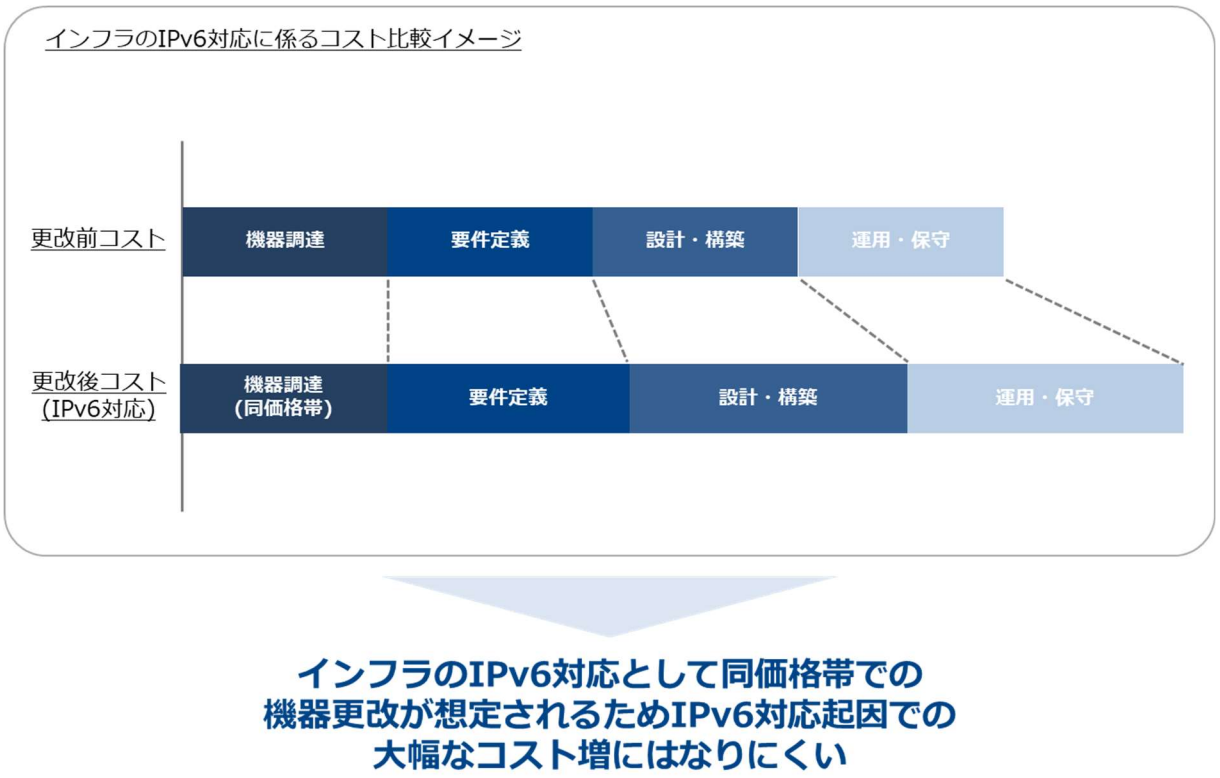


図 7.2-2 機器の IPv6 対応に係るコスト比較イメージ

(2) 回線の IPv6 対応

IPv6 対応として回線を切り替える際には、まず初期コストとして現行回線における利用形態(固定 IP アドレスの利用等)の調査、回線事業者の選定および回線工事等にコストが発生する。つぎに運用コストとして回線利用費が大きな比重を占める。運用変更に係るコストを抑える目的から現行回線の利用形態(固定 IP アドレスの提供等)を維持することを優先事項とするのは一般的である。しかし、その利用形態の維持に関わるサービスが回線事業者によって標準プランに含まれている場合とオプションサービスとなる場合に分かれる。そのため、回線事業者へオプションの利用要否を確認するとともに、回線利用費が現行回線より増加しないかコスト差には注意が必要である。

7.2.3 IPv6 対応コストチェック表について

IPv6 対応に係るコストは対応範囲によって異なるため、作業項目を明確にすることが重要である。そして、作業項目を実施する際に発生し得るコストを整理する必要がある。しかし、コストは付帯作業等も含めて算出する必要があるため、網羅的に算出するにはハードルが高い。そのため、IPv6 対応で想定される作業項目のパターンとそれに対応する費用項目との相関を「【付録 2】IPv6 対応コストチェック表」にまとめている。IPv6 対応に必要なコスト算出を効率的に実施することを目的にコストチェック表を活用することを推奨する。

8　IPv6 対応チェックシートの活用

IPv6 対応を円滑に進めるために各作業工程(要件定義、調達、スケジュール計画、設計・構築、運用・保守)にて確認すべき項目を「【付録 3】IPv6 対応チェックシート」にまとめている。

IPv6 の知見が十分でない場合においても、本チェックシートを活用することで、大きく立ち止まることなく、IPv6 対応が進められることを目的としている。

まずはチェックシート全体を一読することを推奨する。一読を通して、自組織における IPv6 化の全体像をイメージすることが重要である。イメージを持つことでスムーズに実作業へ入ることができる。そして、各工程において本チェックシートの項目を注意深く確認することで、手戻りを少なくし、効率的に IPv6 対応が実施できると考える。

9　その他 IPv6 対応に向けて考慮すべき事項

IPv6 対応するにあたり、その他考慮すべき事項を以下に示す。

(1) IPv6 移行の対象について

IPv6 はネットワーク層に関係するため、IPv6 移行はネットワーク機器だけでなく、サーバや OA 機器等、IP アドレスを持つ機器は移行対象となる。また、ネットワーク層だけでなく、アプリケーション層においても IPv6 を正しく扱えるよう考慮が必要である。

(2) IPv4 と IPv6 のデュアルスタックについて

IPv4 と IPv6 は互換性のないプロトコルである。そのため、基本的に IPv4 と IPv6 は相互に通信することはできない。相互に通信可能とするためにはゲートウェイ装置等の導入を検討する必要があるため、IPv4 と IPv6 は互換性のないプロトコルである前提でデュアルスタック方式にて移行を検討することを推奨する。デュアルスタック環境においては IPv4 ネットワークと IPv6 ネットワークが別々に存在することを認識し、運用していくことが重要である。

(3) リンクローカルアドレスにおけるゾーン ID について

RFC4007[68]にてリンクローカルアドレスの識別としてゾーン ID について紹介されている。複数のインターフェースを持つ機器で宛先にリンクローカルアドレスを指定する場合、どのインターフェースから送信するか識別するためにゾーン ID を付加する必要がある。尚、ゾーン ID の表記は OS によって異なる。[69]

(4) 一時アドレス(Temporary Addresses)の運用について

IPv6 のインターフェース ID は EUI-64 形式により自動生成されるが、MAC アドレスに基づいて生成されるため、送信元が特定されやすい面がある。それに対して、送信元の秘匿性を高める手法として RFC4941[70]で一定期間ごとに生成した乱数でインターフェース ID を生成する「一時アドレス(Temporary Addresses)」が紹介されている。一時アドレスは Windows 等の端末で有効化されている。乱数での生成により、送信元の特定は困難となるが、インターフェース ID がランダムに変更されることで端末管理やサーバとの通信に弊害が生じる可能性があるため運用時は注意が必要である。

---

68 RFC4007「IPv6 Scoped Address Architecture」

69 Windows では「アドレス%+番号」(例、fe80::1%1)、Linux では「アドレス%+インターフェース名」(例、fe80::1%eth0)となっている。

70 RFC4941「Privacy Extensions for Stateless Address Autoconfiguration in IPv6」

(5) プロバイダより提供されるプレフィックスについて

プロバイダのサービス仕様として、提供される IPv6 のプレフィックス情報が半固定である場合がある。プレフィックスの変動により運用に弊害が生じることが想定される場合は、回線選定時にプレフィックスが固定で提供されるかプロバイダのサービス仕様を確認することを推奨する。

(6) IPv6 対応機器またはサービスについて

IPv6 対応を明示している機器やサービスが少ない状況であるため、IPv6 対応を前提に選定する場合は、十分な事前確認が必要である。また、選定を行う場合においても、IPv6 対応状況が判断し難く、ユーザサポートに問い合わせをした場合においても、ユーザサポート側の IPv6 対応の適合基準に対する理解度により、ユーザサポートの回答と実際の IPv6 対応状況に乖離が発生することがあるため、事前調査は慎重に進める必要がある。IPv6 の認定プログラムである「IPv6 Ready Logo」認証を取得した機器を中心に選定することが、有効な手段の一つである。

10　参考資料

本ガイドラインを作成する上で参考にした資料を以下に示す。

10.1　文献

プロフェッショナル IPv6 第 2 版（小川晃通 著）https://www.lambdanote.com/products/ipv6-2

マスタリング TCP/IP IPv6 編 第 2 版(志田智 著、小林直行 著、鈴木暢 著、井上博之 著、黒木秀和 著、矢野ミチル 著) https://www.ohmsha.co.jp/book/9784274069192/

10.2　サイト

本文の注釈のとおり。

11　付録

本ガイドラインの付録資料を以下に示す。

- 【付録 1】課題管理表
- 【付録 2】IPv6 対応コストチェック表
- 【付録 3】IPv6 対応チェックシート