IPv6 対応ガイドライン

【地方自治体編】

２０１４年７月

目次

1. 目的

1.1 目的

これまでのインターネット経済の拡大を支えてきたインターネット上のアドレス体系である IPv4（用語集項番 1）アドレスは、2011 年 4 月 15 日にアジア太平洋地域及び我が国のアドレス管理組織において在庫枯渇の状態となった。

このため、IPv4 の後継規格である IPv6（用語集項番 2）を早期に導入することがこれまで以上に重要となってきている。一部の大手通信事業者を中心に IPv6 対応が進展しつつあるものの、特に中小通信事業者等においては、必ずしも IPv6 対応が進展していない。

また、ICT 系企業や一部の政府機関等を中心にウェブサイト等の外部向けサービスの IPv6 対応が進展しているのに対し、多くの企業や地方自治体のウェブサイト等の外部向けサービスについては、必ずしも IPv6 対応が進んでいない。このため、今後インターネットに IPv6 で接続する利用者の増加が見込まれる中、これら利用者がウェブサイトに接続できず、情報を得る事ができない等の不利益を被ることが懸念される。

従って、中小通信事業者、企業及び地方自治体の IPv6 対応を促進していくことが重要であるが、インターネットに関わるサービスは、多様な関係者を介して提供されるところから、IPv6 対応に伴うセキュリティ対策を含む様々な対応や対策を中小通信事業者、企業及び地方自治体が個別に確立し、実施することは極めて困難である。

このため、これらの関係者が、自らのネットワーク環境等を適切かつ円滑に IPv6 対応させることができるようにガイドライン及び調達仕様書モデルの形にまとめた。本ガイドラインは、IPv6 対応を考える際の全体像、IPv6 対応にあたっての基本的な考え方や方針、具体的に検討すべき箇所、検討の方法等について解説したガイドを提供することを目的としている。

1.2 本ガイドラインの対象者

本ガイドラインの対象者としては、地方自治体におけるネットワークの計画、調達、管理及び運用の担当者、並びに対応するベンダ側のネットワークの設計、構築、監視及び運用の担当者を想定している。

また取り扱う範囲としては、インターネットへの接続やインターネット向けのサービスに係る機能を想定している。

1.3 本ガイドラインの使い方

地方自治体のシステムやネットワークは、その団体の規模や立地、成り立ち等によって、様々なバリエーションが考えられる。政令指定都市やそれに準じる大規模自治体と、町村等の小規模自治体では、システムの規模はもちろん、その管理の仕方等も異なっている。また、IPv6 への対応方法も、全てを自前で IPv6 対応システムとして調達するのか、IPv6 に対応した外部のリソースを活用するのか、またその組合せの程度により、複数の IPv6 導入シナリオが考えられる。

100 の自治体があれば、組織体系やサービス方針によって、100 のシステムやネットワークが存在することになるが、大きく区分するとしても、数種類のパターンに分かれていくと考えられる。想定するシステムやネットワークのモデルと IPv6 導入シナリオの組合せで考えると更に数多くのバリエーションを考えることが必要となる。そこで本ガイドラインにおいては、それらのバリエーションを紹介した上で、その中で最も一般的な構成を基本パターンとして設定し、それ以降の説明を基本パターンに絞って行うこととしている（図 1-1）。

本ガイドラインを参照する自治体によっては、基本パターンとは異なるシステムやネット

ワーク構成を持つ団体もあると考えられるため、基本パターン以外の部分についても適宜補足説明を行うこととしており、補足とあわせてそれぞれの団体に合った形で活用できるように工夫をしている。

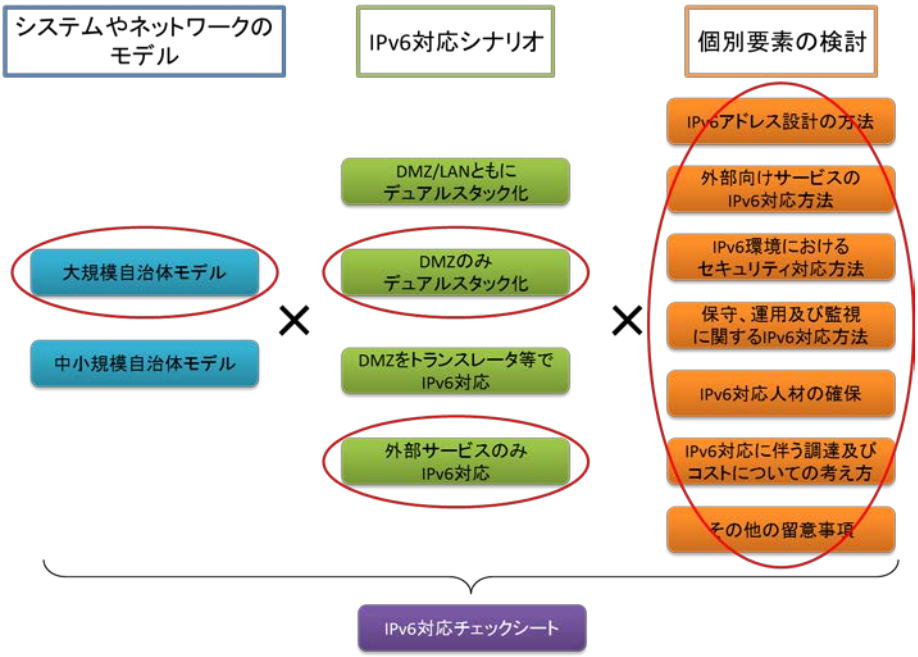

図 1-1　本ガイドラインの利用イメージ

一般に、組織がシステムやネットワークの入れ替えを行う際、またシステムやネットワークに新たな機能を導入する際には、下記に示すようなプロセスに従うと考えられる。

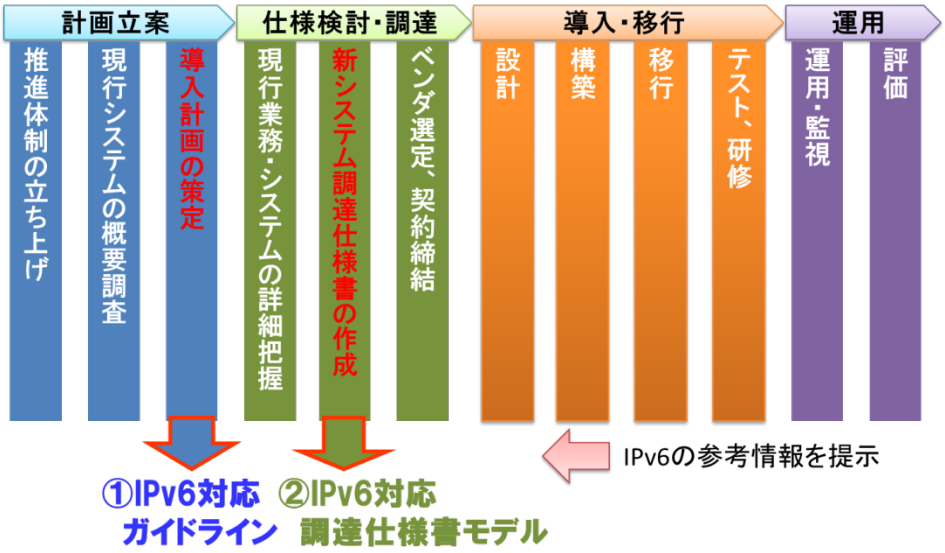

図 1-2　システム導入のフローと本ガイドラインの対象範囲
出典：自治体クラウド・情報連携推進のための研修教材（総務省）を参考に作成

(1)計画立案

①推進体制の立ち上げ（合意形成、推進組織の形態、規約等の整備、役割分担等）

組織内でシステムやネットワークの入れ替え、新たな機能の導入に向けた合意形成を行い、推進組織を設立するとともに、組織内での役割分担等を行う。

②現行システムの概要調査（機能概要、契約内容、費用、課題の調査等）

現行システムに関する概要を調査する。

③導入計画の策定

調査結果を踏まえ、本ガイドラインに示した各検討内容を整理し、IPv6 対応の基本計画を策定する。

(2)仕様検討、調達

①現行の業務、システムの整理

対象となる業務内容、業務に関連する部門及び業務に関連するシステムの機能やシステム構成等の整理を行う。

②新システム調達仕様書の作成

調達仕様書モデルを利用して調達仕様書を完成させる。

③ベンダ選定、契約締結（選定会議体の設置並びに評価基準、契約書及びサービスレベルの検討等）

調達に向け、評価基準に照らし適切なベンダの選定を行う。

(3)導入、移行

①設計（システム設計、検証、運用設計、研修計画等）

導入や移行に向けた詳細設計を行う。必要に応じて試験環境での検証を行い設計に反映する。

②構築（システム開発、インフラ基盤設置等）

設計に基づいた構築を行う。

③移行（移行計画策定、システム移行、データ移行、移行テスト実施等）

旧システムから新システムへの円滑な移行を行うための作業工程や作業内容の整理を行う。

④テスト、研修（運用テスト、研修の実施等）

導入に向けて運用テストや研修の計画を策定し、これを実施する。

(4)運用

①運用、監視（業務運用、インシデント管理、サービスレベル監視等）

運用のための作業項目や対応方法の整理を行い、運用を開始する。

②評価（契約書、サービスレベルの見直し等）

運用状況に関して定期的な評価を行う。

本ガイドラインは、導入計画の策定に向けた各種検討のうち、IPv6 機能の導入の参考とするものである。

具体的な検討としては、各章に記載した知識やノウハウを得て、IPv6 対応に向けた検討に利用することを想定している。各章の概要は以下の通りである。

2.背景

✓インターネットを取り巻く全体的な状況と、自治体としてなぜ IPv6 対応が必要なのかについて解説し、IPv6 対応の必要性について説明する。

3.想定するシステム及びネットワークのモデル

✓地方自治体の場合、その規模に応じて採用されるシステムやネットワークのモデルは異なる。大規模自治体と中小規模自治体に分けて、その典型的なシステムやネットワークのモデルパターンを示し、その上で、最も一般的な構成を基本パターンとして本ガイドラインにおいて採用する。従って、基本パターンと自団体の実際のシステムやネットワーク構成等の違いを確認することで、それ以降の説明を読むに当たっての前提条件を認識できるようにする。

4.IPv6 対応に向けた基本計画づくり

✓システムやネットワークのモデルの基本パターンをベースに、IPv6 に対応するための想定シナリオを示すが、これも IPv6 の採用範囲や対応方法等により複数のシナリオが考えられる。ここでは、DMZ（用語集項番 3）/LAN ともにフルデュアルスタック化（用語集項番 4）、DMZ のみデュアルスタック化、DMZ をトランスレータ等で IPv6 対応、サービス利用のみ IPv6 対応する各シナリオについて解説する。

✓これらシナリオを参考に、どのシナリオをベースに IPv6 対応をするかを決め、次章以降の項目に従って各要素についての具体的な検討を行うことで、IPv6 対応に向けた基本計画を得られるようにする。

5.IP アドレス設計時の IPv6 対応方法

✓IPv6 対応に向けて、その対応範囲や将来拡張を意識した上で、IPv6 のアドレス設計をどのようにすべきかを解説する。これに従って、IPv6 アドレスの設計プランについて検討を行い、IPv6 アドレス設計に関する基本計画を得られるようにする。

6.外部向けサービス設計時の IPv6 対応方法

✓外部向けサービスに関わる基本的アーキテクチャの知識、機器やサービス毎の IPv6 対応方法や留意点、既存 IPv4 環境との通信方法等について解説をする。これを参考に外部向けサービスの IPv6 対応方法について検討を行い、IPv6 対応に向けた基本計画を得られるようにする。

7.IPv6 環境におけるセキュリティ設計時の IPv6 対応方法

✓IPv6 対応に伴って考えられるセキュリティ上の課題や対応策について解説する。これを参考に IPv6 対応に向けたセキュリティ対策等についての基本計画を得られるようにする。

8.保守、運用及び監視に関する設計時の IPv6 対応方法

✓保守、運用及び監視に関して設計する際に IPv6 対応環境において留意すべき課題について解説する。これを参考に IPv6 対応に向けた保守等の基本計画を得られるようにする。

9.IPv6 対応人材の確保

✓IPv6 対応にあたっては、自治体の担当者自身も IPv6 の基本知識とともに、IPv6 に対応したシステムやネットワークを調達及び管理することが可能なレベルの知識を習得する

ことが必要になる。ここでは、技術者への IPv6 対応に必要な教育等に関する情報を提供する。

10.IPv6 対応に伴う調達及びコストについての考え方

✓実際に IPv6 対応を行うためには、基本計画の中で導入範囲や導入スケジュールを明らかにするとともに、必要な予算措置まで行うことが必要となる。ここでは、コスト算定に向けた方法論等について解説を行う。

11.その他の留意事項

✓例えば地方自治体であれば、LGWAN 等の自治体ネットワークに特有の存在等がある。これら自治体独自に考えるべきネットワークと IPv6 対応に向けた関係について解説を行う。

12.（参考）IPv6 対応チェックシート

✓IPv6 対応計画については IPv6 対応チェックシートに従って、対応に漏れが無いかのチェックを行う。

13.（参考）参考文献

✓各章における記述の参考文献を列挙し、各項目について読み解く際の参考とできるようにする。

2. 背景

2.1 インターネットを取り巻く動向

インターネットは世界中の特定の相手との通信を実現する仕組みの 1 つである。世界中に無数にいる通信相手を特定するための情報として郵便においては住所が、電話においては電話番号が存在する。これらと同様にインターネットの世界では、相手を特定するために用いられる情報として IP アドレス（用語集項番 5）が存在する。

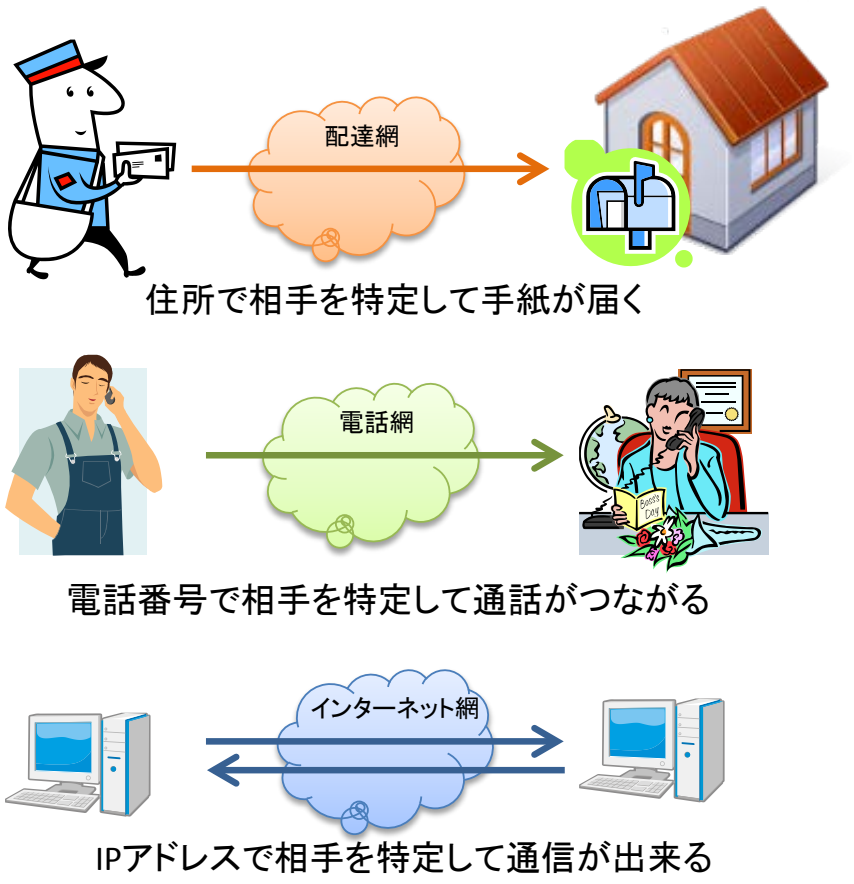

図 2-1　通信の際に相手を特定する情報

1990 年代半ばから利用が急拡大したインターネットを支えてきたのは、IPv4 と呼ばれるインターネット上での通信相手を特定する情報とその仕組みである。IPv4 では 2^{32}個（＝凡そ 43 億個）の IP アドレスが存在するため、約 43 億個の通信機器との間で通信することが可能である（実際には管理用の IP アドレスも必要となるため、利用可能な IP アドレスはこれよりも少ない）。しかしインターネットの利用拡大にともなって IP アドレスの需要が増大することにより、IPv4 における IP アドレス（IPv4 アドレス）の在庫は急速に少なくなり、2007 年頃には、IPv4 アドレスの在庫枯渇は目の前の課題として大きく取り上げられるようになった。このような流れの中で日本でも、インターネットの IPv4 から IPv6 への移行に関する研究会が、総務省主催で相次いで開催され、IPv4 アドレスの在庫枯渇の予測等が議題として取り上げられてきた。

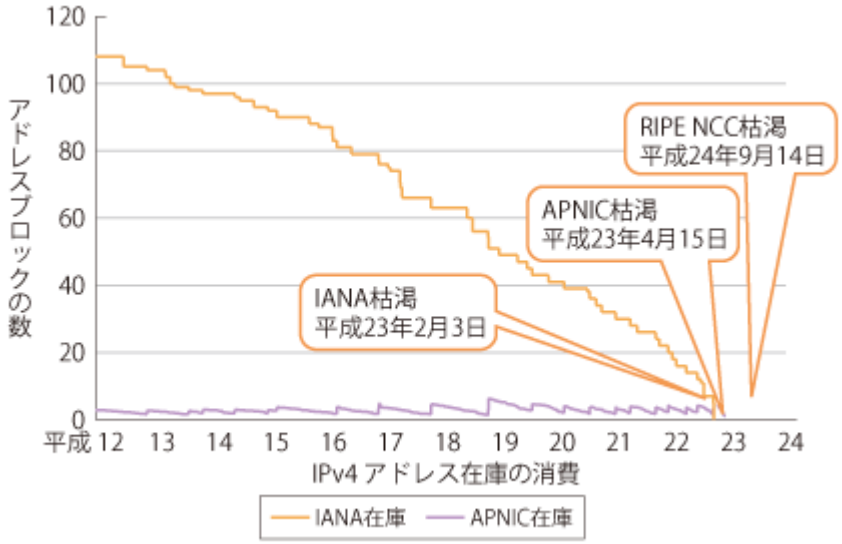

図 2-2　IPv4 アドレス在庫の消費グラフ
出典：総務省　平成 25 年度版　情報通信白書
（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc245350.html）

その後 2011 年にはアジア・太平洋地域で、2012 年にはヨーロッパ地域で、各地域全体の IP アドレスを管轄する組織（RIR、用語集項番 6）における IPv4 アドレスの在庫が事実上の枯渇状態となった。そのためこれらの地域のインターネット事業者は、新たな IPv4 アドレスの割り振り及び割り当てを受けることが困難な状況になっている。

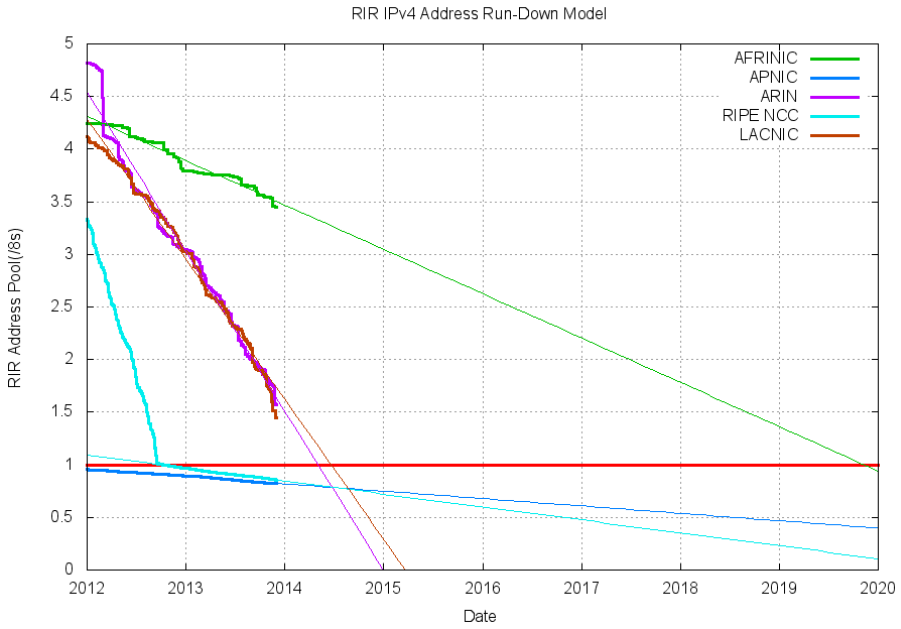

図 2-3　2013 年 12 月当初時点の IPv4 アドレス在庫の減少の推計グラフ
出典：Geoff Huston 氏の推計サイト（http://www.potaroo.net/tools/ipv4/index.html）

IPv4 アドレスの在庫はなおも減り続けている。アジア・太平洋地域の RIR である APNIC（用語集項番 7）のチーフ・サイエンティスト Geoff Huston 氏の予測では、2015 年初頭には図 2-3 のとおり、北米地域（紫色の線）及び南米地域（橙色の線）においても IPv4 アドレスの在庫が事実上の枯渇状態になると推計されている。なお、アフリカ地域（緑色の線）の枯渇は 2020 年以降と予想されているが、インターネットの利用量そのものが少ないため、全世界の枯渇状況にはほとんど影響しない。

このように、世界レベルにおいても IPv4 アドレスを新規に獲得することが困難な状況が、目の前に差し迫っている。

例えば日本の場合、下図にあるように、固定通信向けのインターネット接続サービスの契約数は、前年同期比で 1～3%程度の増加で推移しており、急激な契約数の増加はない。

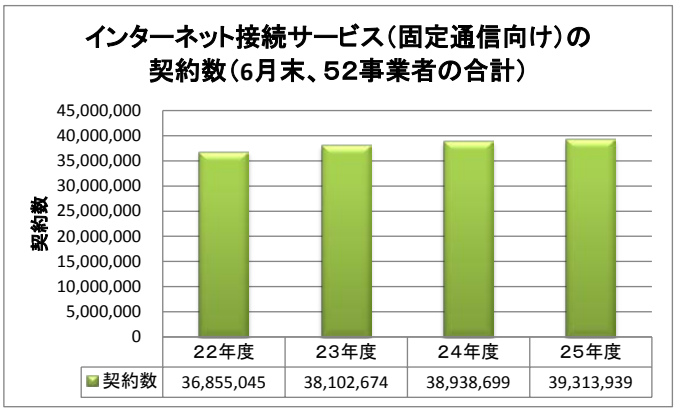

図 2-4 インターネット接続サービス（固定通信向け）の契約数（52 事業者の合計）
出典：総務省　ブロードバンドサービス等の契約数の推移
（http://www.soumu.go.jp/johotsusintokei/field/tsuushin01.html）

一方、移動系のインターネット接続サービスの契約数（FWA（用語集項番 8）、WiMAX（用語集項番 9）等の BWA（用語集項番 10）、LTE（用語集項番 11）、公衆無線 LAN の合計）は急激に増加している。

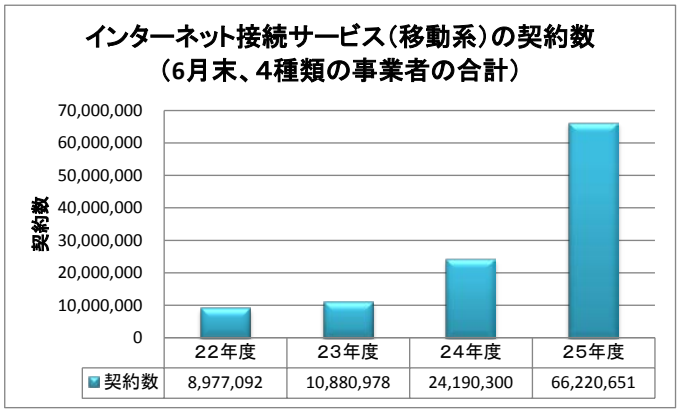

図 2-5　インターネット接続サービス（移動系）の契約数（4 方式の合計）
出典：総務省　ブロードバンドサービス等の契約数の推移
（http://www.soumu.go.jp/johotsusintokei/field/tsuushin01.html）

また、クラウドサービスの利用は堅調に増加しており、クラウドサービスを一部でも利用している企業(下図の灰色とえんじ色の部分)は、平成22年末から平成23年末にかけて13.8%から21.4%と7.6ポイント増加している。それでもクラウドに関して何らかの利用をしている企業は平成23年末で21.4%に留まっており、今後の利用増加の余地がまだ大きいということができる。

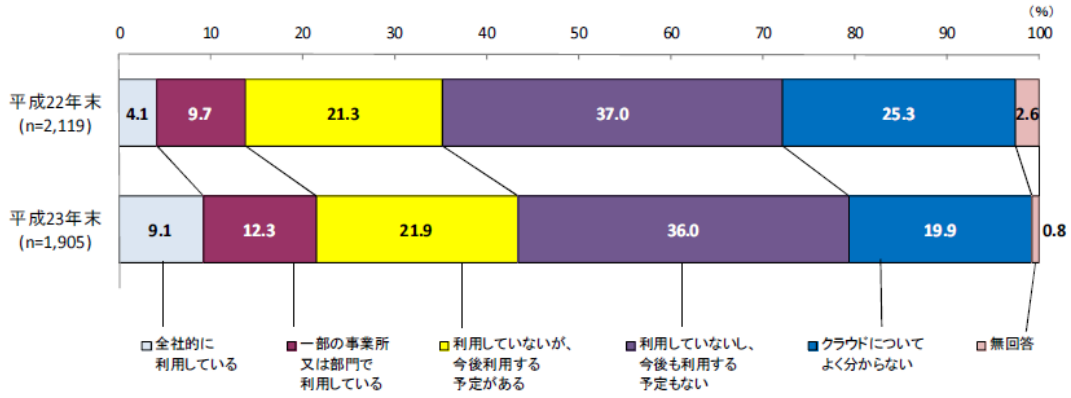

図 2-6　クラウドの利用状況
出典：総務省　平成23年通信利用動向調査（企業編）
（http://www.soumu.go.jp/johotsusintokei/statistics/statistics05b2.html）

今回、本ガイドラインの策定に先立って別途実施した地方自治体及び企業向けのクラウド利用に関するアンケートでも、下図に示すように、クラウドサービスの利用意向や利用状況は5割～7割を越えており、関心の高さを伺うことができる。

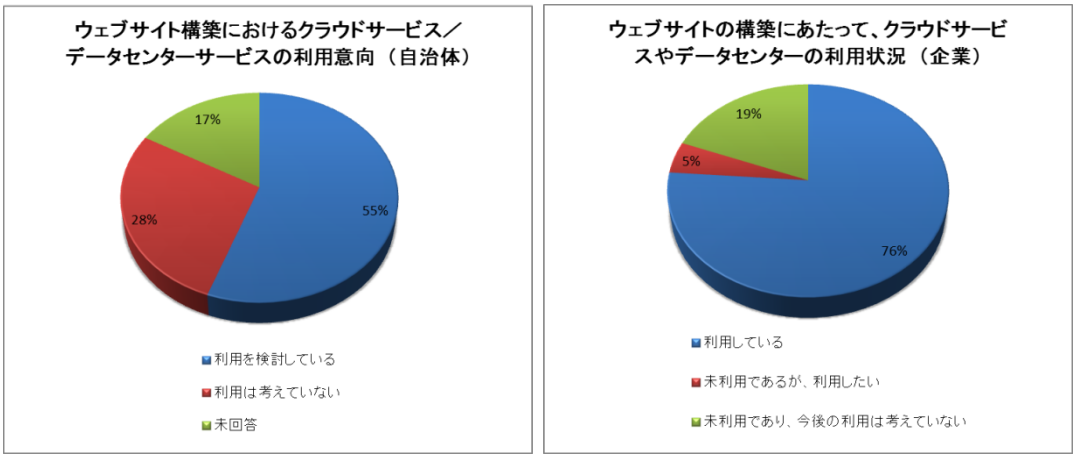

図 2-7　ウェブサイト構築にあたってのクラウドやデータセンターサービスの利用意向及び利用状況

このように、インターネットの利用全体で見た場合、固定通信向けのインターネット接続サービスの利用は横ばいながら、移動系のインターネット接続サービスやクラウド等のネット上のサービス利用は増加しており、その分、IPアドレスに対する新規需要も堅調であることが伺える。

多くのISPやデータセンタ事業者は、これまでに事業者が確保したIPv4アドレスを用いる

ことで、当面の間の事業の継続が可能である。しかし、いずれ IPv4 アドレスが足りなくなることが予想され、IP アドレスの需要が旺盛な成長性の高い事業分野、あるいはそういった事業を抱えている事業者ほど、IPv4 アドレスの不足は差し迫った問題となる。IPv4 アドレスが不足する事態への対応を放置すれば､将来の成長にブレーキを掛けることにもなりかねない。

このような IPv4 アドレスの枯渇に対応するため、IPv4 の後継規格として IPv6 が考案された。当初は研究者や技術者を中心に利用されてきた IPv6 も、今では実用レベルで利用できる時期を迎えており、大手の ISP を中心に、IPv6 に対応する ISP は年々増加している。

2.2 IPv6 化の進展状況

総務省では、インターネット関連事業者の IPv6 対応の状況を毎年調査している。これによると、ISP の半数以上が既に IPv6 対応サービスを提供しており、5 万契約以上の大手 ISP に至っては 9 割以上が IPv6 対応サービスを提供している。中小 ISP で IPv6 対応サービスを提供中のところは 2 割から 3 割に留まっているが、今後提供予定までを含めれば 5 割近い事業者が IPv6 対応サービスを提供することになる。

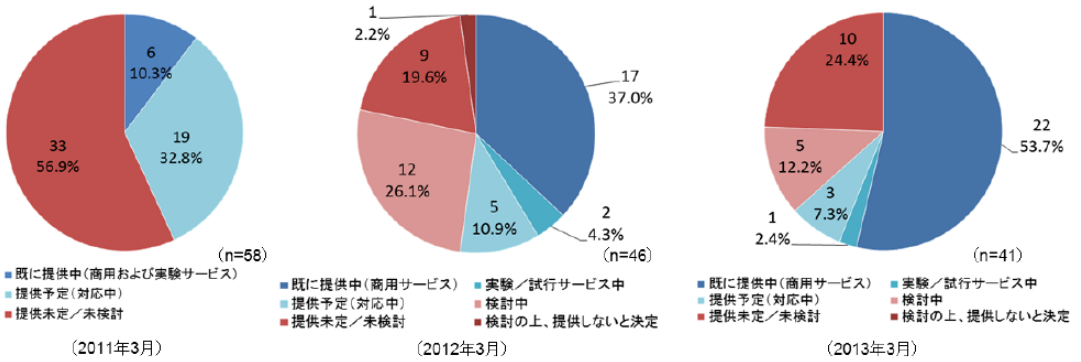

図 2-8　ISP の IPv6 対応状況推移（CATV 事業者を除く）

出典：IPv6 によるインターネットの利用高度化に関する研究会 第二次プログレスレポート（総務省　IPv6 によるインターネットの利用高度化に関する研究会）
http://www.soumu.go.jp/main_content/000239088.pdf

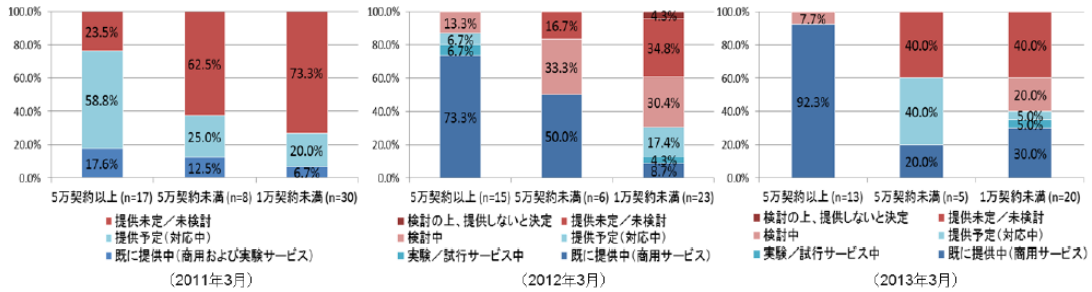

図 2-9　規模別の ISP の IPv6 対応状況推移（CATV 事業者を除く）

出典：IPv6 によるインターネットの利用高度化に関する研究会 第二次プログレスレポート（総務省　IPv6 によるインターネットの利用高度化に関する研究会）
http://www.soumu.go.jp/main_content/000239088.pdf

このことは、ユーザが複数の ISP から競争的環境のもとで IPv6 対応サービスを調達するこ

とが可能であることを示している。また回線サービスについては IPv6 対応が直ぐにでも実施可能な環境が整っていることも示している。

これに対しデータセンタの IPv6 対応は、データセンタ事業者全体の約 1/4 が IPv6 対応サービスを提供するに留まっている。コンテンツ事業者に至っては、IPv6 対応サービスを提供しているところは全体の約 1/8 という状況である。

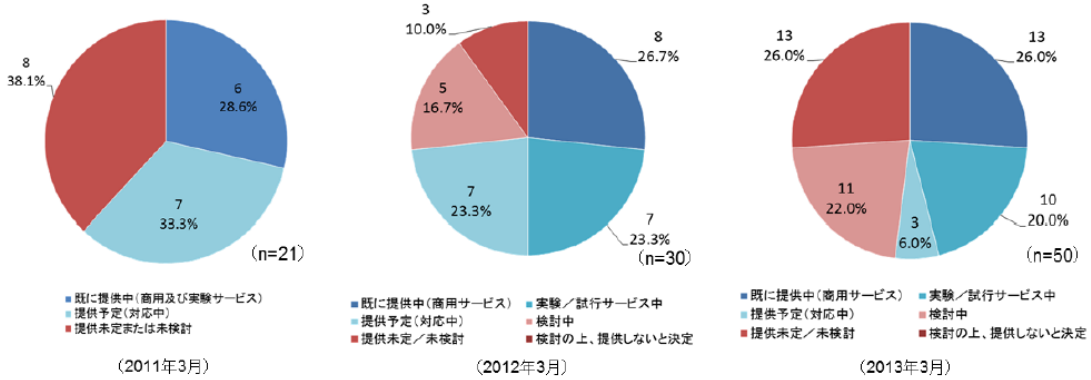

図 2-10　データセンタ事業者の IPv6 対応状況推移

出典：IPv6 によるインターネットの利用高度化に関する研究会 第二次プログレスレポート（総務省　IPv6 によるインターネットの利用高度化に関する研究会）
http://www.soumu.go.jp/main_content/000239088.pdf

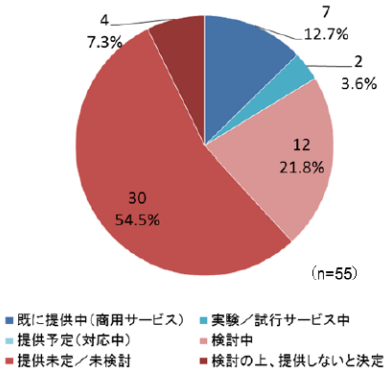

図 2-11　コンテンツ事業者の IPv6 対応状況

出典：IPv6 によるインターネットの利用高度化に関する研究会 第二次プログレスレポート（総務省　IPv6 によるインターネットの利用高度化に関する研究会）
http://www.soumu.go.jp/main_content/000239088.pdf

地方自治体では、自前で機器や通信環境を整えてシステムやネットワーク環境を構築しているケースが多いと考えられるが、一部にはデータセンタを借りて構築しているケースもある。また中小規模の地方自治体では、ASP やクラウドサービスを利用して外部向けサービスを展開しているケースもある。データセンタやコンテンツ事業者の IPv6 対応に関する現状は、これら地方自治体の IPv6 対応計画の立案にも影響を与えるものである。

地方自治体の IPv6 対応を検討するには、IPv6 に関する最新の動向や、機器やサービスの最新の IPv6 対応状況を把握しておく事が重要である。このため、参考情報として、地方自治体が IPv6 対応するために利用可能な機器やサービス、IPv6 に関する全般的な情報等の情報

ソースを以下に整理しておく。

表 2-1　IPv6 対応に関する参考情報

IPv6 全般に関する情報	
IPv6 普及・高度化推進協議会	http://www.v6pc.jp/
IPv4 アドレス枯渇対応タスクフォース	http://kokatsu.jp/
一般財団法人インターネット協会 IPv6 ディプロイメント委員会	https://www.iajapan.org/ipv6/
IPv6 地方 Summit	https://www.iajapan.org/ipv6/summit/index.html
Internet Week	https://www.nic.ad.jp/ja/materials/iw/
広島地域 IPv6 推進委員会	http://www.supercsi.jp/ipv6deploy/
総務省　IPv6 によるインターネットの利用高度化に関する研究会	http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/ipv6_internet/index.html
機器に関する情報	
IPv6 Ready Logo （IPv6 Forum）	http://www.ipv6ready.org/
IPv6 Ready Logo 認証 （一般財団法人 電気通信端末機器審査協会）	http://ipv6.jate.jp/
IPv6 対応ホームルータベンダリスト（World IPv6 Launch）	http://www.worldipv6launch.org/participants/?q=3
IPv6 セキュリティテスト検証済み製品リスト（JPCERT コーディネーションセンター）	http://www.jpcert.or.jp/pr/2013/ipv6project.html
接続サービスに関する情報	
IPv6 Enabled Logo （IPv6 Forum）	http://www.ipv6forum.com/ipv6_enabled/
IPv6 対応 ISP リスト（JAIPA）	http://www.jaipa.or.jp/ipv6/
IPv6 対応 ISP リスト（World IPv6 Launch）	http://www.worldipv6launch.org/participants/?q=2
ウェブ／サービスに関する情報	
IPv6 Enabled Logo （IPv6 Forum）	http://www.ipv6forum.com/ipv6_enabled/
IPv6 サービスリスト （IPv4 アドレス枯渇対応タスクフォース）	http://www.kokatsu.jp/blog/ipv4/data/ipv6service-list.html
IPv6 対応 Web サイトリスト （World IPv6 Launch）	http://www.worldipv6launch.org/participants/?q=1
IPv6 に関する情報通信政策、統計情報	
IPv6 の普及促進	http://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/

2.3 IPv6 対応を必要とする理由

「2.1 インターネットを取り巻く動向」でも説明したように、これまでインターネットの利用拡大を支えてきた IPv4 アドレスは、世界中で今まさに枯渇しつつある。ここで言う枯渇とは、新たな利用に供するための未利用在庫の枯渇であり、既に利用中のインターネットが直ぐに利用できなくなることを意味しない。しかし、在庫の枯渇により新たな利用に支障が出ることは容易に想像がつく。

図 2-2 や図 2-3 の IPv4 アドレスの在庫減少の推移を示すグラフは、見方を変えれば IP アドレスに対する新規需要の状況を示すグラフでもあり、仮に供給が途絶えたとしても新規需

要は無くならないと考えれば、それは即ち不足分が蓄積され、増加していくということである。

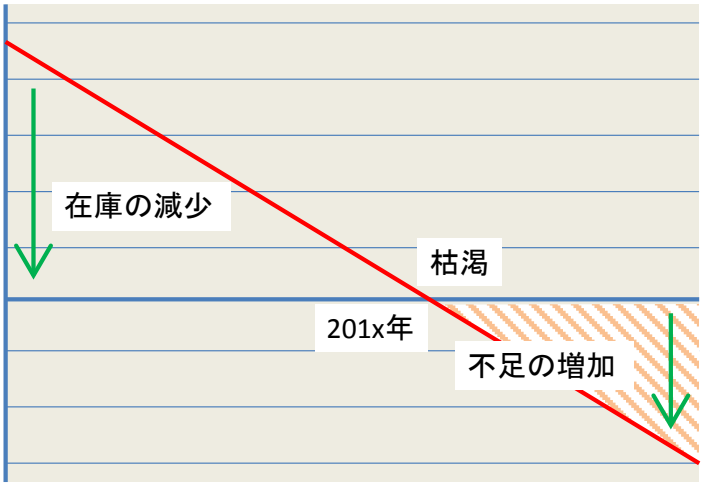

図 2-12　アドレス減少の時代からアドレス不足の時代へ

IPv4 アドレスの不足を補うため、IPv6 対応以外にも様々な方式が検討され、CGN（Carrier Grade NAT、用語集項番 12）のように一部では実際に利用されている方式もある。しかしこれらの方式は、IPv4 アドレスを効率的に使うための技術であり、本質的に IP アドレスの数を増加させるものではない。また外部向けサービスのようにグローバルアドレスを必要とするサービスでは CGN は使うことができないといった、利用方法による制約や制限がある。したがって、IP アドレスの不足を本質的に解決するには IPv6 への対応が必要となる。

多くの主要国において IPv6 対応に向けたロードマップ等が策定され、IPv6 普及策や支援策が展開されている。日本においても長年に渡って IPv6 推進策が展開されてきた結果、多くの大手 ISP が IPv6 対応サービスを提供するに至っている。また、政策による推進だけではなく、ベンダの努力により、ネットワーク機器や主要 OS の IPv6 対応はほぼ完了している。このため最近では、ほとんど意識せずに IPv6 を使っているユーザも出始めている。

このような状況を整理すると、主に 3 つの理由により、IPv6 への対応ないしはその検討が必要といえる。

(1) サービスの増強、新たな事業やサービスの展開に伴う IP アドレス需要増への対応

既存のサービスを継続するだけならば新たな IP アドレスは不要であり、IPv6 対応の必要性も少ない。しかしネット上のサービスを増強するために、また新たな事業やサービスを展開するために、サーバの導入やクラウドなど VM（仮想マシン、用語集項番 13）を多数利用する基盤を調達する場合がある。この場合には、新規のグローバル IP アドレス（用語集項番 14）が必要になる。IPv4 アドレスが枯渇した状態では新規の IP アドレスの獲得が困難になるため、IPv6 の利用を検討する必要が出てくる。

最近では国内外においてオープンデータの利活用が活発化しており、日本国内でもデータの提供元として地方自治体に多くの期待が寄せられている。地方自治体が保有し、オープンデータとして提供する情報には重要な基礎的情報が含まれており、その提供先は国内に留まらず、海外から参照されることも想定される。IPv6 を用いたインターネットが、アジアを中心とした新興国で今後普及が進んだ場合、オープンデータについても IPv4/IPv6 のデュアルスタックで提供されることが求められる。

(2) IPv6 でアクセスするユーザへの対応

インターネット経由でユーザ向けに様々なサービスを展開している場合には、ユーザ環境への配慮が必要となる。今後 IPv6 でアクセスしてくるユーザが増えてくると、これらのユーザへの対応として、外部向けサービスの最低限の IPv6 対応が求められる。特に地方自治体では、住民向けサービスなどは、そのサービスの利用を希望するすべての住民が利用できる必要がある。

住民が使用するインターネットアクセスの IPv6 対応や PC、スマートデバイス等の IPv6 デフォルト端末（IPv6 が標準で有効となっている OS や端末）の普及が進むと、住民向けサービスが IPv4 のみに対応したままでは、一部の住民に十分なサービスの提供ができなくなる可能性がある。また地方自治体が担っている災害発生時等における情報提供サービスは、確実に多くの住民が利用できる必要があるため、地方自治体の住民向けサービスは IPv6 に対応することが求められる。

(3) 意図せずに IPv6 による通信が行われることによる予期せぬ問題発生への対応

多くの端末 OS、ルータ等の通信機器は、既に IPv6 対応を行っている。このため、ユーザが意識することなく IPv6 が使われていることもある。ユーザに特段の負荷を求めることもなく、自然と IPv6 対応ができるという意味では良い面もあるが、例えば IPv6 に対応したセキュリティ監視の導入がなされていない環境で IPv6 が使われている場合には、知らぬ間にセキュリティ上の課題を抱えるようなことにもなりかねない。

また業務でモバイル PC を使っている場合、社内にいるときは IPv6 が遮断され、IPv4 の IPS（侵入抑止装置、用語集項番 15）によって確実に監視されていても、外部に持ち出して利用した際に、知らぬ間に IPv6 トンネル接続を確立され、IPv4 のセキュリティ監視を潜り抜けて IPv6 経由でのセキュリティ上の脅威にさらされる可能性がある。

このような意図せずに IPv6 による通信がなされた場合に発生するセキュリティ課題を整理し、必要に応じてセキュリティ対応のための IPv6 導入を検討する必要がある。

特に地方自治体では現在、WindowsXP の入れ替えが大きな問題となっているが、この問題の解決に向けて、一斉に端末や OS の入れ替えが進むと、地方自治体内部の端末はほとんど全てが IPv6 に対応したものになると考えられる。この際、ネットワークシステム全体をしっかりと管理するためには、IPv6 を意識したネットワーク管理の確立が必要となる。

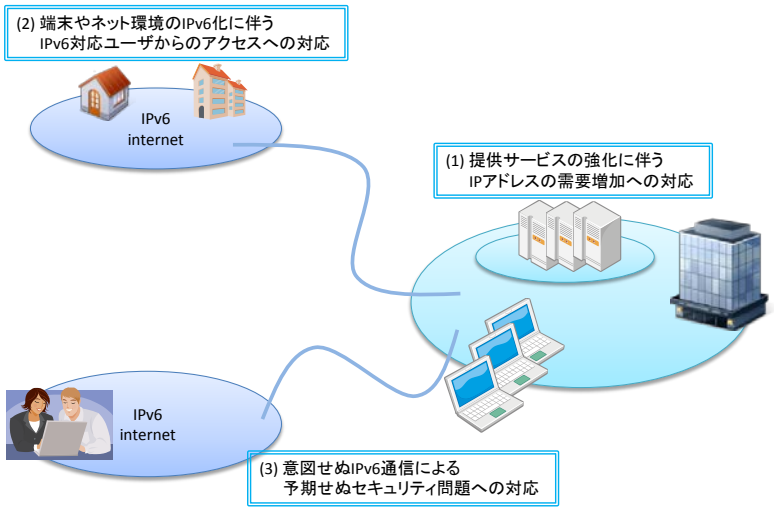

図 2-13　IPv6 対応を考えるべき 3 つの理由

3. 想定するシステム及びネットワークのモデル

地方自治体の場合、政令指定都市や中核都市、都道府県などの大規模自治体と、一般の市町村などの中小規模自治体では、想定されるシステムやネットワークのモデルが異なる。

大規模な自治体の場合は、一定規模の情報システムを保有することからすべてのネットワーク機器やサーバ等のハードウェアを調達するオンプレミスを中心とした従来型のシステムとなることが想定される。

一方、中小規模自治体の場合は、コスト削減や業務の効率化や共同化のために、自治体クラウドの取組と同様に、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。

3.1 大規模自治体のモデル

以下に、典型的な大規模自治体のシステムやネットワークのモデル概念図を示す。

自庁舎内のサーバ室やデータセンタにインターネット回線を引き込み、DMZ や LAN に必要なハードウェアを自ら運用する。本ガイドラインでは、ファイアウォールや DMZ 内の各種サービスの IPv4/IPv6 デュアルスタック化を想定する。

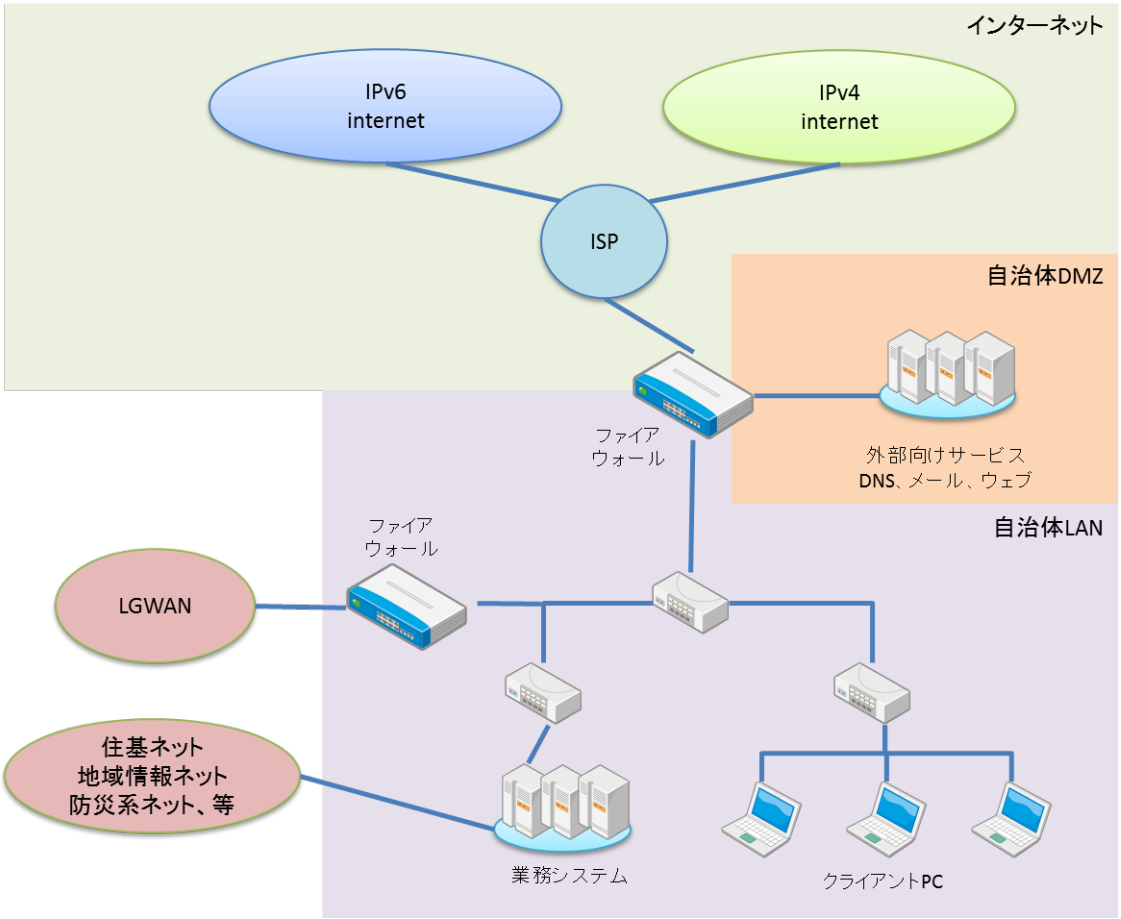

図 3-1　典型的な大規模自治体のシステム及びネットワークのモデル

3.2 中小規模自治体のモデル

以下に、典型的な中小規模自治体のシステムやネットワークのモデル概念図を示す。

DMZ 上で稼動させるサービスについては ASP やクラウドサービスを利用し、自前ではハードウェアを保有しない。LAN については、自庁舎にインターネット回線を引き込み、業務システムや職員の端末からインターネットが利用できるようにする。本ガイドラインでは、ASP やクラウドサービスにおける各種サービスの IPv4/IPv6 デュアルスタック化を想定する。

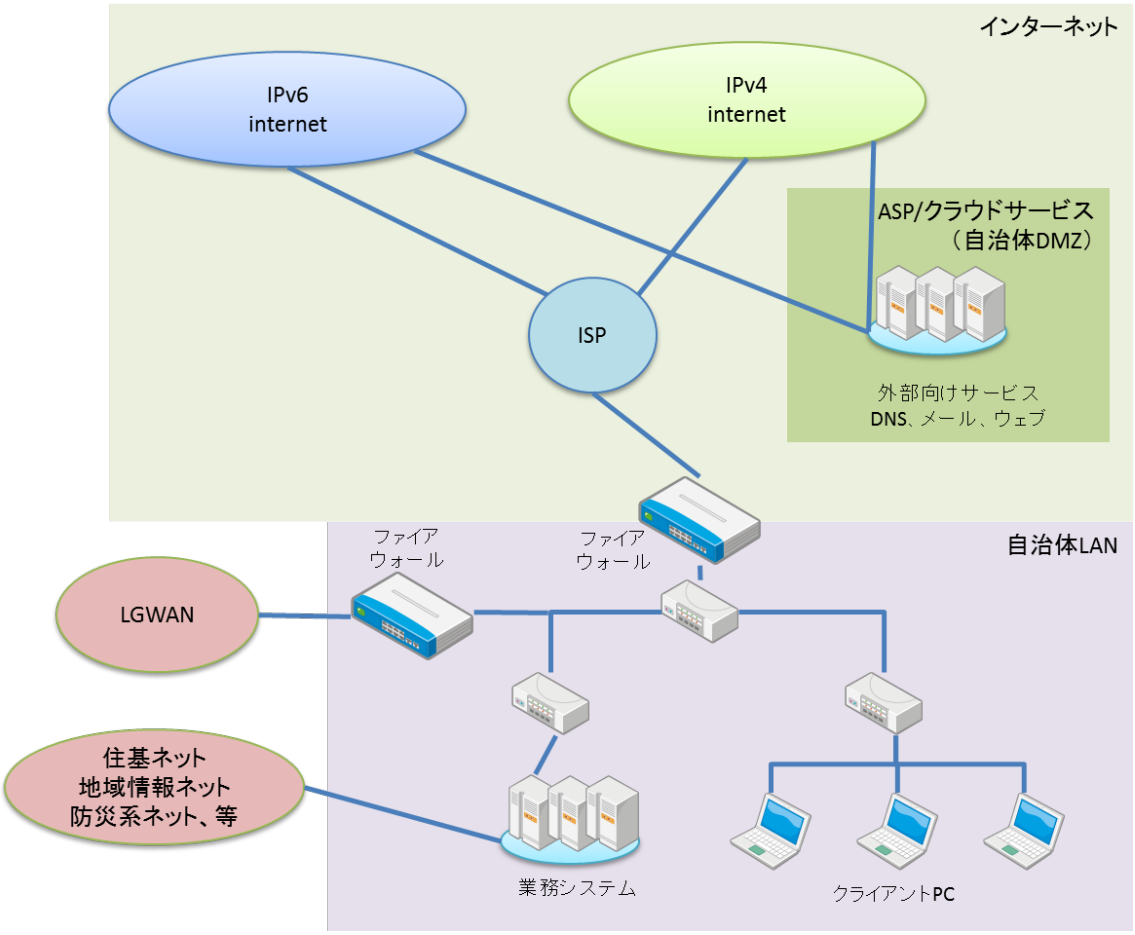

図 3-2　典型的な中小規模自治体のシステム及びネットワークのモデル

3.3 IPv6 対応モデル

本ガイドラインでは、大規模自治体及び中小規模自治体の 2 つのモデルのうち、大規模自治体のモデルを基本パターンとして説明する。大規模自治体のモデルでは、システムやネットワークを、ハードウェアを含めて調達し自ら運用をする想定となり、中小規模自治体のモデルにおいて考慮すべき内容をほとんど包含しているためである。ただし、中小規模自治体のモデルで示した ASP やサービスの調達において特に留意すべき点がある場合には、個別に解説を加えることとする。

4. IPv6 対応に向けた基本計画づくり

前章に示した地方自治体における典型的なモデルに対して、IPv6 対応をするには、複数のシナリオが考えられる。インターネット接続サービスや利用者端末 OS の IPv6 対応状況などにより、どの範囲までを IPv6 対応するか、判断が必要となる。

以下では、IPv6 対応として考えられる 4 つのシナリオを示し、その中から本ガイドラインにおいて説明する基本的なシナリオを設定する。

① DMZ/LAN ともにフルデュアルスタック化
② DMZ のみデュアルスタック化
③ DMZ をトランスレータ等で IPv6 対応
④ サービス利用のみ IPv6 対応

4.1 DMZ/LAN ともにフルデュアルスタック化

本ガイドラインでは、外部向けサービスの IPv6 対応を対象とするため、本パターンは検討の対象外となる。本パターンにおいて IPv6 対応を実施する場合の留意点のみ、以下に記載しておく。

IPv6 対応として DMZ/LAN の段階的なフルデュアルスタック化を目指す場合、自組織内の業務や通信関連の機器、システムの調達や更新計画とあわせて検討する必要がある。自組織内の通信機器に IPv6 未対応の機器がある場合には、機器の調達や更新計画でハードウェアの IPv6 対応を考慮する必要がある。またそれと並行して、システムの調達や更新計画でソフトウェアの IPv6 対応を考慮し、システム面での IPv6 対応を実施することになる。

一方、IPv6 対応として最初から DMZ/LAN ともにフルデュアルスタック化を目指す場合、段階的な対応をする場合と比べて、すべてのネットワークを IPv6 対応するという最終的な目標を短期間で達成できる可能性がある。ただし、IPv6 対応としては難易度が高くなる。特に LAN のデュアルスタック化では、LAN 上で利用している業務システムの動作検証が必須となる。地方自治体では、ホストコンピュータを含めた旧来型のシステムを稼働させているケースも多く、それらのレガシーシステムが端末やネットワークの IPv6 対応により影響がないことを確認する必要がある。

また、地方自治体では、通常の LAN やインターネット接続とは別に、住基ネットや LGWAN 等との外部接続も行われている。これらの地方自治体独自の外部接続サービスにおける IPv6 対応計画との関係についても十分留意する必要がある。外部接続サービスの IPv6 対応計画よりも先行して LAN のデュアルスタック化を行う場合には、それらの外部接続サービスへの影響についても十分に確認する必要がある。

4.2 DMZ のみデュアルスタック化

IPv6 対応として、自らが所有するネットワーク機器やサーバ類の DMZ 部分のみをデュアルスタック化する場合、各機器のリプレース時期に IPv6 対応機器を順次導入しつつ、IPv6 に対応可能なサービスから順次デュアルスタック化する計画を立てることが、スムーズな IPv6 対応に繋がる。

たとえば、ルータやスイッチ等の DMZ を構成する基盤となるネットワーク機器のリプレース時に IPv6 対応機器を導入しておき、その後メールサーバ等のサーバ機器のリプレース時に、メールサービスの IPv6 対応を行うことなどが考えられる。

また、計画の策定時には、DMZ 部分のみならず、LAN 等の IPv6 対応を含めたロードマップを検討し、それらの将来の調達時期などを確認しておくことが望ましい。

4.3 DMZ をトランスレータ等で IPv6 対応

DMZ の IPv6 対応として、トランスレータ等を用いて DMZ 部分のみをデュアルスタック化する方法もある。この場合、トランスレータ等の必要な機器を調達するだけでよく、他のネットワーク機器やサーバ類の調達とは独立した調達ができるため、短期間に対応を終えることが可能となる。

ただし、トランスレータ等の機器に関するコストが発生する。また将来の各種ネットワーク機器やサーバ類の IPv6 対応により、トランスレータが不要となる時期が来ることも想定する必要がある。トランスレータ等を導入する場合には、導入計画のみならず、撤収計画についても検討しておくことが望ましい。

4.4 サービス利用のみ IPv6 対応

IPv6 対応として、ASP やクラウドサービス等のサービスを利用することで IPv6 に対応する方法もある。この場合、サービス調達時に IPv6 対応サービスを選択することで、サービス利用開始とともに IPv6 対応も完了する。

すでに ASP やクラウドサービスを使用中の場合、それらのサービスを中途で IPv6 に対応可能かどうか、また契約更新時に IPv6 対応サービスに移行可能かどうかを確認する必要がある。同サービスでの IPv6 対応が困難な場合には、他のサービスに移行することで IPv6 対応が可能か、あるいは同サービスが将来のロードマップに IPv6 対応を織り込んでいるかなどを確認する必要がある。

いずれの手段を用いても、サービスの調達時点で IPv6 対応が困難な場合には、契約期間を短く設定するなど、近い将来に再度 IPv6 対応を再検討できるようにすることが望ましい。

4.5 IPv6 対応の基本シナリオ

本ガイドラインでは、「DMZ のみデュアルスタック化」を基本シナリオとして説明する。ただし、ASP やクラウドサービスの利用においても IPv6 対応を進められるため、「サービス利用のみ IPv6 対応」のシナリオも組み合わせたシナリオを想定する。

5. IP アドレス設計時の IPv6 対応方法

外部向けのサービスを提供する DMZ セグメントの IPv6 対応に向けて、IPv6 アドレスの知識は必須である。本章では IPv6 アドレスの概要として、アドレスの種類、構造及び調達方法を紹介し、実際に DMZ に IPv6 アドレスを割り当てる際の留意点について説明する。

5.1 IPv6 アドレスの基本

始めに IPv6 アドレスの構造について紹介する。なお IPv6 アドレスの構造は、RFC4291（IP Version 6 Addressing Architecture）に規定されている

5.1.1 IPv4 アドレスの表記について

IPv4 の場合、IP アドレスは 32 ビットの長さを持ち、0 から 255 の十進数 4 個（例：192.168.100.64）又は、2 進数（例：前出の 192.168.100.64 は 11000000101010000110010001000000）で表記される。このアドレス長では 2^32（2 の 32 乗）、約 43 億個の IP アドレスを表記することが可能である。また、IPv4 アドレスは、ネットワークを示すネットワーク部とネットワーク内のホストを示すホスト部により構成されている（図 5-1）。IPv4 アドレス表記においては、ネットワークアドレスのビット長を示すため、IP アドレスの後ろに「/」を置き、ビット長を併記する記法が使われる（192.168.100.64/16 等）。

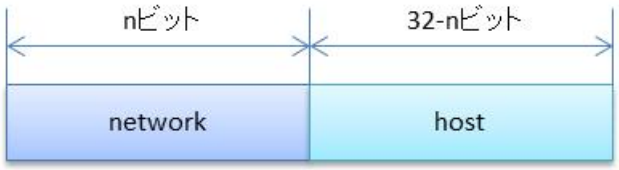

図 5-1　IPv4 アドレスの構造

5.1.2 IPv6 アドレスの表記について

IPv6 アドレスは、IPv4 アドレスの 4 倍となる 128 ビットの長さを持つ。IPv6 アドレスは、16 ビットを 1 つのグループ（16 ビットフィールド）とし、それぞれを 4 個の 16 進数で表記し、全体として 8 個の 16 ビットフィールドを「:」で連結した表記をする。RFC4291 に示される IPv6 アドレス表記の例を以下に示す。

2001:DB8:0:0:8:800:200C:417A

IPv6 アドレスのテキスト表記では、各 16 ビットフィールドにおける先頭の「0」を省略することが可能である（0123 を 123、0023 を 23 と表記）。また、すべて「0」である 16 ビットフィールドが連続する場合は 1 か所のみ「::」と省略することが可能である（前述の例を 2001:DB8::8:800:200C:417A と表記）。

IPv6 アドレスの表記によっては省略した結果が 1 つではないことがあり、IPv6 アドレス管理や運用上のトラブルの原因となる可能性がある。IPv6 アドレスについて推奨されるテキスト表記を規定した RFC5952（A Recommendation for IPv6 Address Text Representation）を参考に、組織内で IPv6 アドレスの表記を標準化することを推奨する。

5.1.3 IPv6 アドレスの種類

IPv6 では、グローバルに通信が可能な IPv6 アドレスとして、表 5-1 に示される 3 種類のアドレスが規定されている。

表 5-1　IPv6 アドレスの種類

種類	概要
ユニキャストアドレス	1 対 1 の通信に用いられる
マルチキャストアドレス	ネットワーク上に配置された複数のホストとの同時通信に用いられる
エニーキャストアドレス	複数のインタフェースで共有され、ネットワーク経路上、もっとも近いインタフェースに配信される

IPv4 では、ネットワーク上の全てのホストとの同時通信に用いられるブロードキャストアドレスが規定されている。IPv6 ではこれに該当するものが存在しないため、IPv4 におけるブロードキャストアドレスの代わりとしてマルチキャストアドレスが用いられることもある。

なお、IP アドレスの通信範囲をスコープと呼び、グローバルに通信可能な IP アドレスについてのスコープは「グローバル」と呼ばれる。この他に、インタフェースが接続されるリンク上でのみ有効なリンクローカルアドレスが規定され、こちらのスコープは「リンクローカル」と呼ばれる。リンクローカルアドレスは全てのインタフェースに自動的に付与されるため、グローバルに通信を行うインタフェースには複数の IP アドレスが付与されることになる。

5.1.4 IPv6 アドレスの構造

IPv6 インターネット上で利用されるユニキャストアドレスのことをグローバルユニキャストアドレスと呼ぶ。その構造は RFC3587（IPv6 Global Unicast Address Format）にて規定される。IPv6 アドレス全体の 128 ビットのうち上位の 64 ビットはサイト（組織）の識別やサイト内のネットワーク（サブネット）の識別に用いられる。このうち、サイト（組織）を識別する部分をグローバルルーティングプレフィックスと呼び、サイト内のネットワークに割り当てられる部分をサブネット ID と呼ぶ。下位の 64 ビットはインタフェース ID と呼ばれ、この部分が PC やサーバ、ネットワーク機器等の IPv6 インターネット上に存在する機器を示すことになる（図 5-2）。なお、先頭 3 ビットを「001」とすることでグローバルユニキャストアドレスとして識別される。

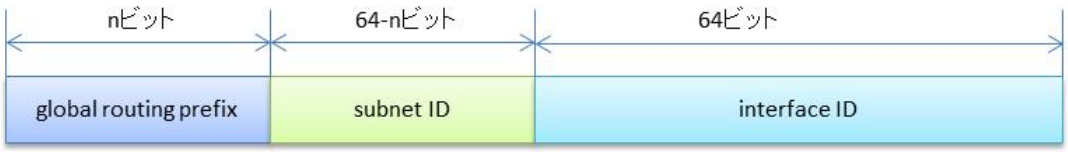

図 5-2　IPv6 グローバルユニキャストアドレスの構造

IPv4 で使われているプライベートアドレスのようにサイト内で閉じた通信用途のためにユニークローカル IPv6 ユニキャストアドレスが定義されている（図 5-3）。ここで「L」が「1」の場合は局所的な割り当てであることを示す。グローバル ID 部分について、乱数に基づいて生成することで、衝突の可能性は残るものの、サイト間での IPv6 アドレスの独立性を担保

することができる。

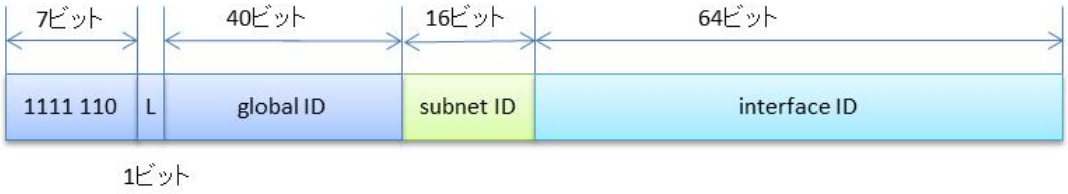

図 5-3 ユニークローカル IPv6 ユニキャストアドレスの構造

5.1.5 IPv6 アドレスの集約

インターネット上のホスト等を表記するグローバルユニキャストアドレスは、インターネット上の経路集約（アグリゲーション、用語集項番 16）を機能させるため、ネットワークトポロジーに基づいた階層的構造を維持することが求められている。RIR（地域インターネットレジストリ）及び NIR（国別インターネットレジストリ、用語集項番 17）から通信事業者に割り振りがなされ、通信事業者からエンドユーザへと割り当てを行うように管理体制が確立されている（図 5-4）。

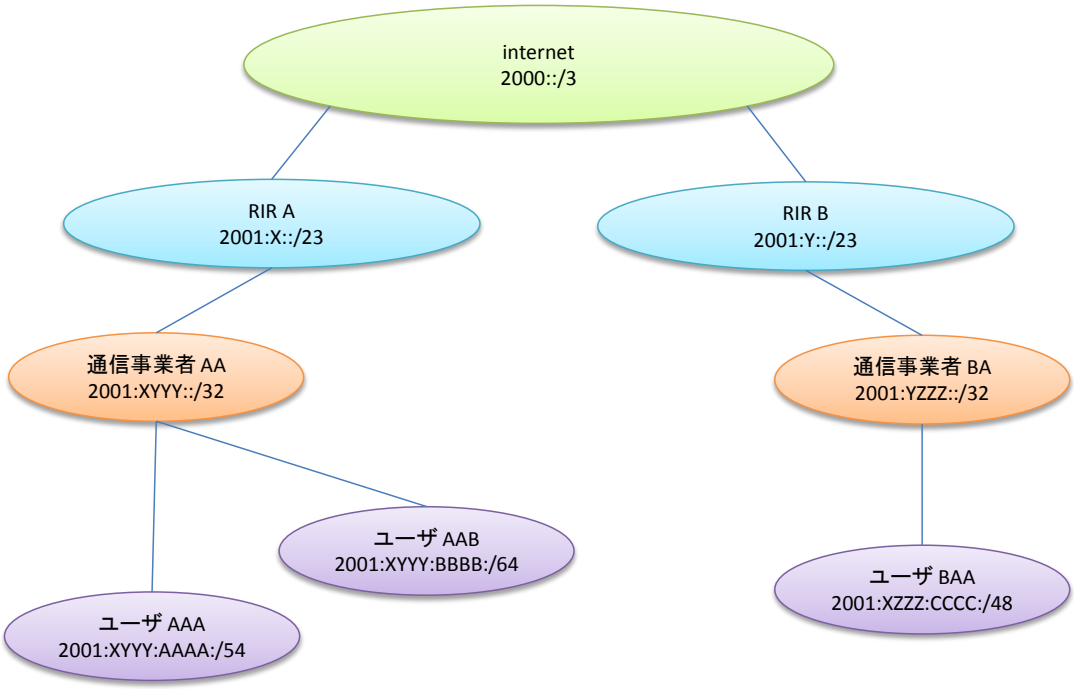

図 5-4　グローバルユニキャストアドレスの割り振りの例

この方針にもとづき、通信事業者が RIR 又は NIR からグローバルユニキャストアドレスの割り振りを受ける場合には 32 ビット長のプレフィックス（/32 と表記される。用語集項番 18）が割り振られることになる。なお、より多くのアドレスを収容する必要があれば、より短いビット長のプレフィックスを申請することも可能である。/32 が割り振られた場合、/64 までの 32 ビットをユーザ収容などの通信サービス事業に使うサブネット ID として通信事業者で管理を行う。

エンドユーザに払い出される IPv6 グローバルユニキャストアドレスは、一般的には、ユーザが管理できるサブネット ID が 16～32 ビットとなるように提供される。つまり/48（32+16）～/64（32+32）のプレフィックス割り当てが行われている（図 5-5）。

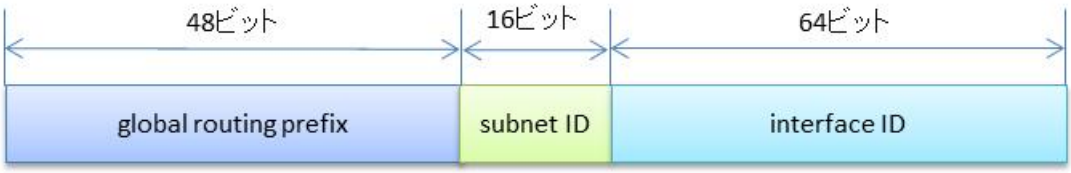

図 5-5　ユーザに割り当てられるグローバルユニキャストアドレスの構造（/48 の場合）

5.1.6 IPv6 アドレスサイズと収容可能なネットワーク数の関係

エンドユーザが IPv6 アドレスを調達する場合、一般的には /48、/56 又は/64 のいずれかのサイズ（領域）で割り当てを受けることになる。割り当てサイズが/48 の場合は、16（=64-48）ビットが自組織で利用可能なサブネット ID となり、/56 の場合は、8（=64-56）ビットが自組織で利用可能なサブネット ID である。なお、通信事業者からユーザが IPv6 アドレスの割当を受ける際には、アクセス回線の契約サービスの種類と接続形態（ネイティブ接続、トンネル接続等）により、プレフィックスサイズが固定されていることが多い。

IPv6 では、128 ビットのアドレス長のうち、半分の 64 ビットはインタフェース ID として利用されるため、ネットワークアドレスとして利用可能なアドレス長についても同じく 64 ビットとなる。このため、/64 という IPv6 プレフィックスが、それ以上分割することができない単一のネットワークを示すアドレスとなる。

図 5-6 に示すように、/48 のプレフィックスは、65,536 個の/64 ネットワークを収容可能である。/56 のプレフィックスの場合には、256 個の/64 ネットワークを収容可能である。

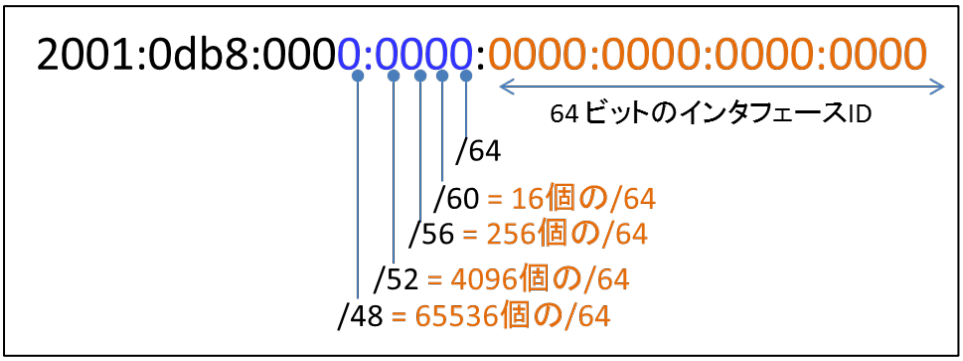

図 5-6　/48 アドレスに収容可能な/64 ネットワーク

また、1 つの/64 プレフィックスには、2 の 64 乗（= IPv4 アドレス空間全体となる 43 億の 2 乗）個のインタフェースが収容可能であり、事実上、ネットワークに接続するサーバ類に割り当てるアドレス数の制限がないと考えてよい。

5.1.7 IPv6 アドレスの分割

IPv6 ネットワークアドレスとして/48 又は/56 プレフィックスの割り当てを受けた場合、例えば、/48 プレフィックスを 16 個の/52 プレフィックス、256 個の/56 プレフィックスといっ

たように分割することができる（図 5-7）。

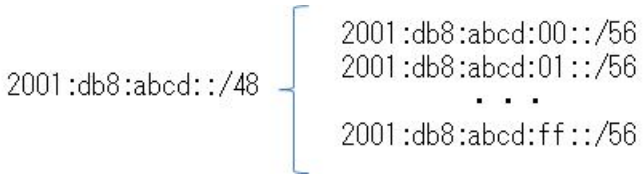

図 5-7　/48 アドレスに収容可能な/56 ネットワーク

/56 プレフィックスには 256 個の/64 プレフィックスを収容可能なため、256 個の/64 プレフィックスを収容可能な/56 プレフィックスを 256 個収容する/48 プレフィックスというように、階層的なネットワーク構成に応じて IPv6 アドレスを分割することができる（図 5-8）。

図 5-8　階層的なネットワーク構成

5.1.8 IPv6 アドレスの調達方法

IPv6 アドレスを調達する場合、インターネット接続を提供する回線サービス事業者からプロバイダ依存アドレス（PA アドレス）の割り当てを受ける方法の他に、日本における NIR である一般社団法人日本ネットワークインフォメーションセンター（JPNIC、用語集項番 19））から「特殊用途用プロバイダ非依存アドレス」（PI アドレス）の割り当てを受ける方法と、アジア太平洋地域の RIR である APNIC から PI アドレスの割り当てを受ける方法の 3 種類がある。一般的な組織であれば、PA アドレスの調達で十分であるが、回線サービス事業者を経由せずにインターネットに直接接続したネットワークを自ら運用する組織や、特殊なセンサーネットワークを運用する組織では、PI アドレスを調達する場合もある。

PA アドレスを調達する際には、DMZ において必要なサイズ（プレフィックス長）を算出し、回線サービスを調達する際の調達要件とする。ただし、IPv6 では利用可能なアドレス数が膨大であるため、それほど厳密に考えずに、ラフな設計でも十分に運用可能である。

5.2 DMZ における IPv6 アドレス割り当ての留意点と管理方法

前述のように IPv6 アドレスは大きく、グローバルルーティングプレフィックス、サブネット ID 及びインタフェース ID に分かれている。

5.2.1 必要なアドレスサイズの算出

DMZ セグメントに設置するサービスが多種多様で、サーバ台数も数十台というような大規

模な体制であれば、DMZ を複数のネットワークに分割して、ネットワークごとに役割分担や負荷分散を行う場合がある。このような DMZ では、複数の/64 を収容することになる。このとき、/64 のネットワークの数が 256 未満におさまれば/56 のネットワークを要求し、256 以上であれば/48 のネットワークを要求すればよい。

本ガイドラインで想定している外部向けの DNS（用語集項番 20）やメールサービス等を設置する DMZ セグメントは、ファイアウォールを介して、上流の通信事業者及び自治体 LAN セグメントに接続される。他ネットワークとのアクセス制御はファイアウォールで実施することとし、DNS サーバとしてプライマリサーバを 1 台（セカンダリサーバは通信事業者のサービスなど別ネットワークに配置）、メールサーバを数台、ウェブサーバを数台といった規模であれば、1 個の/64 ネットワークに十分収容可能である。

この場合においても、将来的に、自治体 LAN の IPv6 対応や、出先機関、関連組織の自組織の IPv6 ネットワーク配下への接続等、必要とする/64 ネットワークの増加が想定される場合には、/56 以上の大きさを持つアドレスを要求しておく必要がある。

5.2.2 サーバ類に割り当てる IPv6 アドレスの生成

IPv6 では、グローバルユニキャストアドレスを機器等に割り当てる方式として、機器の管理者が自らプレフィックスアドレス（グローバルルーティングプレフィックス＋サブネット ID）とインタフェース ID を管理し、設定ツール等を介して入力する手動設定方式と、機器をネットワークに接続するだけで自動的にアドレスが設置される自動設定方式を選択することができる。

他の機器から IPv6 アドレスを指定して選択されることがないユーザ端末では、自動設定方式とすることで、アドレス設定の手間を軽減するとともに、設定間違いを抑制することが可能である。

しかし、ホスト名と IPv6 アドレスどちらでも参照されることがあるサーバ機器については、自動設定ではなく、一定の基準に従って生成された固定のアドレスを手動で設定することが望ましい。なおルータ等では、自動設定方式がデフォルト状態では無効になっており、手動設定方式が前提として考えられている。

IPv6 アドレスは全体として長い表記となるため、手入力の際に間違いが生じやすい。IPv6 アドレスを入力しなければならない場合は、入力の間違いを検出するため、ツールを用いた検証手順等を整備することが望ましい。

6. 外部向けサービス設計時の IPv6 対応方法

「4. IPv6 対応に向けた基本計画づくり」で示した IPv6 対応の基本シナリオに基づき、本章では DMZ を中心とした外部向けサービスにおける IPv6 対応の方法について説明する。

外部向けサービスはウェブシステムやメールシステムが中心となるが、インターネットとの連携上必要となる DNS サーバやセキュリティ対策機器なども対象である。地方自治体の場合、対象となる外部向けサービスには、ウェブシステム（地方自治体のウェブサイト）、DNS サービス、メールシステム（職員向け）を想定する。

本章では、外部向けサービスの基本アーキテクチャを示し、IPv6 対応すべき機器やサービスの範囲と、それら機能の IPv6 対応方法について説明する。

6.1 外部向けサービスに関わるアーキテクチャ

6.1.1 基本的なアーキテクチャ

以下に、典型的な地方自治体における外部向けサービスの基本的アーキテクチャを示す。

自庁舎内のサーバ室やデータセンタにインターネット回線を引き込み、DMZ や LAN に必要なハードウェアを自ら運用する（図 6-1）。

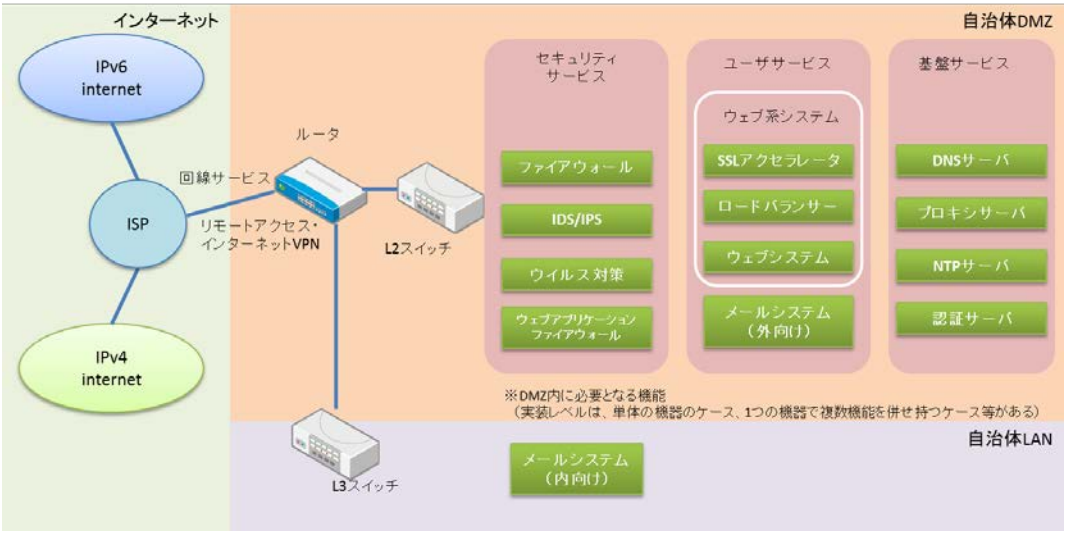

図 6-1　典型的な地方自治体の外部向けサービスの基本的アーキテクチャ

6.1.2 サービス利用におけるアーキテクチャ

地方自治体の外部向けサービスについて、ASP やクラウドなどのサービスを利用する場合のアーキテクチャを図 6-2 に示す。

DNS、メール、ウェブのいずれも ASP やクラウドなどのサービスを利用し、職員向けの POP や IMAP など内向けのメールシステムのみ、自庁舎内のサーバ室やデータセンタに設置する。

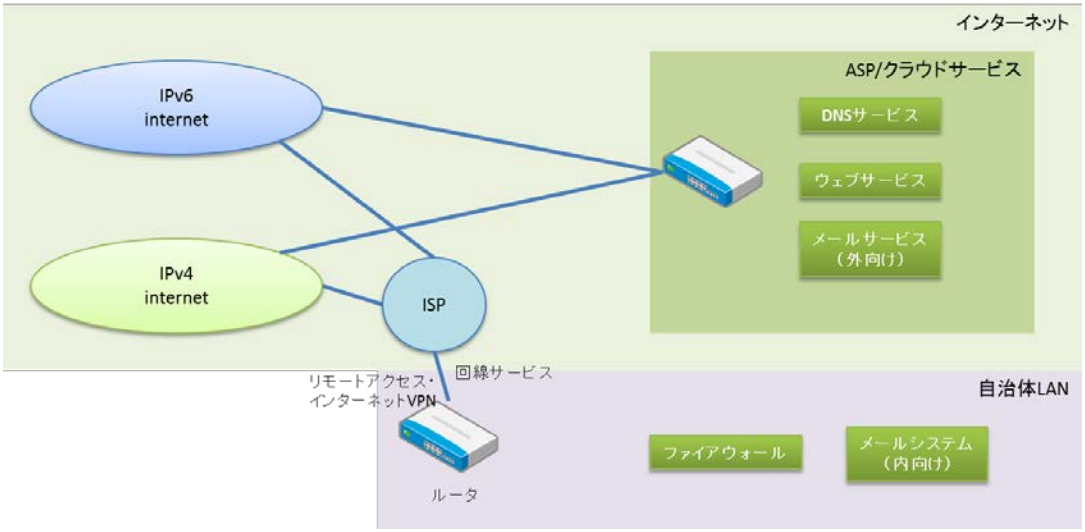

図 6-2　外部向けサービスに ASP/クラウドサービスを利用する場合

6.2 IPv6 対応すべき機能

地方自治体において、IPv6 対応すべき機器やサービスとして、以下の構成要素を想定する。

6.2.1 回線サービス

インターネットと自治体ネットワークとの間を接続するための回線サービスである。従来の IPv4 による接続に加えて、IPv6 による接続を併せて提供する必要がある。ISP 事業者から、同じ回線上で IPv4 と IPv6 を提供してもらう方式の他、IPv6 のみの回線サービスを追加で提供してもらう方式などがある。

6.2.2 リモートアクセス及びインターネット VPN

出先事務所のリモートアクセス端末や、インターネット上の ASP やクラウドサービスと自治体ネットワークを接続するためのリモートアクセスサービス及びインターネット VPN サービスである。従来の IPv4 による接続に加えて、IPv6 による接続を併せて提供することが必要である。自治体ネットワーク側にリモートアクセス終端装置やインターネット VPN 終端装置を設置することになる。

6.2.3 ルータ、スイッチ

インターネットとの接続点に設置するルータや、DMZ のネットワークを構成するための L3 スイッチ（用語集項番 21）や L2 スイッチ（用語集項番 22）等のスイッチがある。

ルータは、ISP との接続点に設置し、自治体ネットワーク（DMZ を含む）をインターネットに接続するために利用する。

L3 スイッチは、主に自治体ネットワークの LAN を構成するコアスイッチとして利用する。

L2 スイッチは、DMZ 内のスイッチや、LAN 内のエッジスイッチとして利用する。

6.2.4 セキュリティサービス機能

(1) ファイアウォール

インターネットからのサイバー攻撃などに対応するために、ファイアウォール機能やウェブアプリケーションファイアウォール（WAF、用語集項番 23）機能を備えるファイアウォー

ルがある。最近では、ウイルス対策などの高度な機能を備える UTM（統合脅威管理）装置も対象である。

ファイアウォールは、ISP と接続したルータと接続し、自治体 LAN、DMZ、インターネット間の通信を制御する。UTM 装置についても、位置づけはファイアウォールと同等である。

(2) IDS/IPS

インターネットからのサイバー攻撃を検知及び防御するための不正侵入検知システム（IDS、用語集項番 24）や IPS がある。

IDS 及び IPS は、インターネットと DMZ との間、あるいはインターネットと LAN との間に設置される。特に透過型の IDS 及び IPS では、ファイアウォールの DMZ ポート、あるいはファイアウォールの LAN ポートに設置する場合が多い。

(3) ウイルス対策

サーバ等に感染し機密性の高い情報を第三者に送信するコンピュータウイルスや、設定ファイルの破壊や CPU 負荷を異常にあげることでサーバの機能を妨害するコンピュータウイルスが存在する。これらコンピュータウイルスの感染活動の遮断や感染時の早期検出のためにウイルス対策を行う必要がある。サーバ等の個々の機器にインストールするタイプと、ファイアウォール等に統合されたセキュリティアプライアンス（複数のセキュリティ機能を統合した機器）として提供されるタイプがある。

(4) WAF

WAF は、ウェブアプリケーションで用いるプロトコルのトラフィックを監視し、必要に応じてトラフィックを遮断することで、攻撃によるリスクを低減する。データベースと連携するアプリーションに対する SQL インジェクション（不正な SQL コマンドを発行させる）、アカウント盗用（管理者アカウントでの不正ログインの試み）といった、ウェブアプリケーションに特有の脆弱性が悪用されることを防ぐために配置される。

6.2.5 ユーザサービス機能

(1) ウェブシステム

自治体のウェブサイトを構成するためのウェブシステムである。ウェブシステムを構成するソフトウェアとしては、HTTP（用語集項番 25）サーバ、CMS（コンテンツマネジメントシステム、用語集項番 26）、アクセス解析等がある。ASP やクラウドサービスでも、ウェブサービスとして同様の機能が提供される。

ウェブシステムは、通常は DMZ 上に配置するが、ロードバランサー等のリバースプロキシ（用語集項番 27）を介する場合には、LAN 上に配置することも可能である。

(2) メールシステム

地方自治体職員が利用する電子メールシステムである。インターネットとのメール送受信を行う外向けのメールサーバと､職員の端末からアクセスする内向けのメールサーバがある。

本ガイドラインでは、DMZ 上に設置した外向けのメールサーバを対象とする。LAN 上に設置する内向けのメールサーバは対象外とする。

ASP やクラウドサービスでも、外向けのメールサービスとして同様の機能が提供される。

(3) SSL アクセラレータ

ウェブサイトで SSL（用語集項番 28）を使用する場合、SSL の暗号化や復号処理の高速化が必要であれば、SSL アクセラレータが必要となる。

(4) ロードバランサー

ウェブシステムの負荷分散を行うためのロードバランサー（負荷分散装置）である。近年ではウェブシステムやデータベースなどをインターネットから隠蔽するためのリバースプロキシの機能として導入されることもある。

ロードバランサーは DMZ 内に設置し、インターネットからウェブシステムに対するアクセスを受け付け、適切なウェブシステムに振り分ける。

6.2.6 基盤サービス機能

インターネットを利用する際に必要となる基盤サービスとして、DNS サーバ、プロキシ サーバ、NTP サーバ（用語集項番 29）、認証サーバがある。DNS については、ASP やクラウドサービスで提供される DNS サービスもある。

(1) DNS サーバ

DNS サーバは、自治体 LAN 上のクライアント等がインターネットにアクセスする際の名前解決のために使われるキャッシュサーバと、自組織のドメイン名を管理する権威サーバがある。いずれも DMZ 上に設置される。ASP やクラウドサービスでも、DNS サービスとして権威サーバと同様の機能が提供される。

(2) プロキシサーバ

プロキシサーバは、自治体 LAN 上のクライアントがインターネットアクセスをする際に、インターネットに直接アクセスせずに、アクセスを中継する役割を果たす。同一コンテンツを複数ユーザが閲覧する際に効率を上げるキャッシュ機能と、アクセス管理やアクセス監視を行う機能を備える。

(3) NTP サーバ

NTP サーバは、自治体 LAN 上にあるクライアントの時刻同期をするために、DMZ 上に設置される。NTP サーバ自身の時刻同期は、インターネット上の NTP サーバを使って行われる場合が多い。

(4) 認証サーバ

認証サーバは、ウェブシステムを利用するユーザを識別するための認証機能を備える。

6.2.7 その他の機能やサービス

メールシステムにおいては、ウイルス対策機能を備える必要がある。メールサーバに搭載するウイルス対策ソフトや、SPAM メールやウイルスを遮断するウイルス対策アプライアンスなどがある。

ネットワーク機器やサーバ機器の監視ツールについても、IPv6 対応の機器やサービスを監視できる必要がある。

なお、ウェブシステムのバックエンドにあるアプリケーションサーバやデータベースサーバ、各サーバのデータをバックアップするバックアップシステムについては、LAN 側に配置

することを想定して、本ガイドラインでの IPv6 対応には含めないこととする。また、各サーバが共有して使用するストレージについては、FC（ファイバーチャネル）等で SAN（ストレージエリアネットワーク）を構成することとし、本ガイドラインでの IPv6 対応には含めないこととする。

6.3 機能毎の IPv6 対応方法

機器やサービス毎の IPv6 対応方法として、ここでは特に IPv6 に関連する要件を示す。実際の機器やサービスの調達にあたっては、ここで示す対応方法に加えて、当該機器やサービスが本来持つべき機能や IPv4 通信に関する事項や、ハードウェアなどの物理的な諸元について要件を示す必要がある。

(1) 回線サービス

回線サービスの IPv6 対応では、以下の項目を含めることとする。

- インターネットとの IPv4/IPv6 通信が可能であること。
- 静的経路（デフォルトゲートウェイ）を提供すること。
- IPv6 アドレスに対応したセカンダリ DNS サーバを提供すること。
- 回線サービスで品質が保証される場合には、通信帯域（保証帯域、最大帯域等）及びサービス提供条件（最大遅延時間、利用時間に対する通信不能時間比率等）について IPv4/IPv6 間での差異がないこと。
- トンネル方式での IPv6 接続の場合には、利用者側に設置するトンネル終端装置についての障害対応、脆弱性対応等、必要な保守について速やかに対応すること。
- ISP 事業者から IPv6 アドレスを払い出す場合には、/48 又は /56 の IPv6 プレフィックスの払い出しが可能であること。
- ISP 事業者から IPv6 アドレスを払い出す場合には、必要に応じて IPv6 アドレスの追加払い出しが可能であること。
- ISP 事業者から IPv6 アドレスを払い出す場合には、IPv6 アドレスについて固定アドレスを払い出すこと。
- 地方自治体自身で IPv6 アドレスを取得する場合には、回線サービスへの IPv6 アドレスの持込みが可能であること。
- セカンダリ DNS サーバについては IPv4 アドレスに関するレコードも格納と情報提供が可能であること。
- IPv4 アドレスについても払い出しが可能であること。

(2) リモートアクセス及びインターネット VPN

リモートアクセスサービスやインターネット VPN サービスの IPv6 対応では、以下の項目を含めることとする。

- リモートアクセス終端装置及びインターネット VPN 終端装置のネットワークインタフェースの双方（インターネット側のクライアント接続、DMZ 又は LAN 側接続）で IPv4/IPv6 通信が可能であること。
- インターネット側のクライアント接続、DMZ 又は LAN 側の接続の双方で IPv4/IPv6 通信が可能であること。
- 外部認証装置を利用可能な場合、その装置との接続について IPv4/IPv6 通信が可能であ

ること。

- IPv4/IPv6 ともに同等のサービスレベルを提供すること。
- インターネット接続サービスにおいて、IPv4 又は IPv6 のいずれかの通信に障害が発生した場合において、利用可能なプロトコルを用いたサービス提供が可能であること。
- 不正アクセス等の監査の際に IPv6 アクセスを識別できること。
- アドレスベースのアクセスコントロール機能を有する場合には、IPv4/IPv6 どちらであっても制御対象とできること。
- 接続クライアントからのインターネットを介した接続について IPv4/IPv6 ともに待ち受け可能であること。
- 接続クライアントの認証について IPv4/IPv6 双方で可能であること。
- リモートアクセス又はインターネット VPN 接続を行って利用するアプリケーションやサービスが IPv6 に対応していない場合は、IPv6 接続に加え IPv4 接続を提供すること。

(3) **ルータ**

ルータの IPv6 対応では、以下の項目を含めることとする。

- ルータとして備えるべき基本機能を有すること。
- インターネットと IPv4/IPv6 通信が可能であること。
- ルータから ISP に接続する回線上に IPv4/IPv6 パケットを通過させること。
- IPv4/IPv6 のルーティング機能を有すること。
- IPv4/IPv6 のフィルタリング機能を有すること。
- IPv4/IPv6 のパケットシェーピング（用語集項番 30）機能を有すること。
- IPv4/IPv6 の優先制御機能を有すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成（用語集項番 31）を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 の MIB（用語集項番 32）に対応すること。
- MIB の設定や情報取得のための転送に IPv4/IPv6 通信が利用できること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(4) L3 **スイッチ**

L3 スイッチの IPv6 対応では、以下の項目を含めることとする。

- L3 スイッチとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4/IPv6 のルーティング機能を有すること。
- IPv4/IPv6 のフィルタリング機能を有すること。
- IPv4/IPv6 のパケットシェーピング機能を有すること。
- IPv4/IPv6 の優先制御機能を有すること。

- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 の MIB に対応すること。
- MIB の設定や情報取得のための転送に IPv4/IPv6 通信が利用できること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(5) L2 スイッチ

L2 スイッチの IPv6 対応では、以下の項目を含めることとする。

- L2 スイッチとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- MIB の設定や情報取得のための転送に IPv4/IPv6 通信が利用できること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(6) ファイアウォール

ファイアウォールの IPv6 対応では、以下の項目を含めることとする。

- ファイアウォールとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4/IPv6 のルーティング機能を有すること。
- IPv4/IPv6 のフィルタリング機能を有すること。
- IPv4/IPv6 の TCP/UDP が監視できること。
- IPv4/IPv6 のステートフルインスペクション機能を有すること。
- IPv4/IPv6 の IP ヘッダチェック機能を有すること。
- IPv4/IPv6 の DoS 攻撃防御機能を有すること。
- IPv4/IPv6 のフラグメンテーションアノマリ（異常検知、用語集項番 33）機能を有すること。
- IPv4/IPv6 の IP アドレスアノマリ機能を有すること。
- IPv4/IPv6 の TCP アノマリ機能を有すること。
- IPv4/IPv6 の UDP アノマリ機能を有すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。

- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(7) ウェブアプリケーションファイアウォール

ウェブアプリケーションファイアウォールの IPv6 対応では、以下の項目を含めることとする。

- ウェブアプリケーションファイアウォール（WAF）として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- アプリケーションレベル（L7）の検査が IPv4/IPv6 通信に対して可能であること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(8) IDS/IPS

IDS/IPS の IPv6 対応では、以下の項目を含めることとする。

- IDS/IPS として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- 電子メールのウイルス検出など、アプリケーションレベル（L7）の検査が IPv4/IPv6 通信に対して可能であること。
- パターンファイルは、スケジュールを設定してパターンファイル納入元のサーバに IPv4/IPv6 でインターネット等を経由してアクセスし、自動的に更新できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(9) SSL アクセラレータ

SSL アクセラレータの IPv6 対応では、以下の項目を含めることとする。

- SSL アクセラレータとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- サーバ証明書をインストールし、IPv4/IPv6 通信を SSL や TLS（用語集項番 34）プロトコルで暗号化できる機能を有すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(10) **ロードバランサー**

ロードバランサーの IPv6 対応では、以下の項目を含めることとする。

- ロードバランサーとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- 外部からの IPv4/IPv6 によるアクセスをウェブサーバに振り分ける際に、ウェブサーバに対する通信を IPv4 及び IPv6 のいずれかを選択できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- IPv4 通信と IPv6 通信が同等の TLS/SSL のアクセラレータの性能を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(11) **ウェブシステム**

ウェブシステムの IPv6 対応では、以下の項目を含めることとする。

- ウェブシステムとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- ウェブブラウザ等のクライアントからの IPv4/IPv6 通信による要求に対して、ウェブサーバ上に格納されたコンテンツを返送できること。
- サーバ証明書をインストールし、IPv4/IPv6 通信を SSL や TLS プロトコルで暗号化できる機能を有すること。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。
- ウェブシステムの CMS 等が備える外部との連携機能において、IPv4/IPv6 の双方に対応すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。

- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(12) **メールシステム**

メールシステムの IPv6 対応では、以下の項目を含めることとする。

- メールシステムとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- インターネットとの IPv4/IPv6 通信による送受信要求は SMTP（用語集項番 35）に対応すること。送信ドメイン認証が可能であること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(13) DNS **サーバ**

DNS サーバの IPv6 対応では、以下の項目を含めることとする。

- DNS サーバとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4/IPv6 通信による DNS の名前（アドレス）解決機能を有すること。
- IPv4/IPv6 通信による順引き及び逆引きに対応していること。
- 上位又は下位の DNS サーバと IPv4/IPv6 通信で連携する機能を有すること。
- IPv4 及び IPv6 に関連するレコードを保持できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(14) **プロキシサーバ**

プロキシサーバの IPv6 対応では、以下の項目を含めることとする。

- プロキシサーバとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4/IPv6 通信によるアクセスをプロキシサーバが中継できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(15)NTP サーバ

NTP サーバの IPv6 対応では、以下の項目を含めることとする。

- NTP サーバとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4/IPv6 通信による NTP の時刻同期リクエストを受け付けること。
- 上位又は下位の NTP サーバと IPv4/IPv6 通信により連携する機能を有すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(16)認証サーバ

認証サーバの IPv6 対応では、以下の項目を含めることとする。

- 認証サーバとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4/IPv6 通信を使用するウェブ アプリケーションに対して、指定された認証方式による認証と、URL をベースとしたアクセス制御の機能を提供すること。
- （外部の認証サーバと連携する場合）外部の認証サーバと IPv4/IPv6 通信で連携できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。

- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

(17) その他の機器やサービス

その他の機器やサービスとしては、「運用監視機能」「仮想化基盤」「トランスレータ」がある。

1) 運用監視機能

運用監視機能の IPv6 対応では、以下の項目を含めることとする。

- 運用監視機能として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- ネットワーク機器やサーバ機器の IPv4/IPv6 通信に関する死活監視ができること。
- 各種サービス（ウェブ、メール、DNS など）の IPv4/IPv6 通信に関するサービス監視（品質監視を含む）ができること。
- IPv4 通信と IPv6 通信を統合して監視できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 の MIB に対応すること。
- MIB の設定や情報取得のための転送に IPv4/IPv6 通信が利用できること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

2) 仮想化基盤

仮想化基盤の IPv6 対応では、以下の項目を含めることとする。

- 仮想化基盤として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
    - ゲスト OS に対して、IPv4/IPv6 通信が可能な仮想ネットワークインタフェース（NIC、用語集項番 36）を提供すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

3) トランスレータ

トランスレータの IPv6 対応では、以下の項目を含めることとする。

- トランスレータとして備えるべき基本機能を有すること。

- IPv4/IPv6 通信が可能であること。
- DMZ 上のネットワーク機器やサーバ等からインターネットに対する IPv4 通信を、IPv6 通信に変換すること。またその結果生じるインターネットから DMZ 上のネットワーク機器やサーバ等への IPv6 通信を、IPv4 通信に変換すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。

6.4 IPv6 対応に向けた事前準備

機器やサービスの IPv6 対応においては、IPv4 通信で備えるすべての機能及び性能を IPv6 で要求した場合、調達の時点では要件を満たす機器やサービスが存在しない可能性がある。IPv6 対応の範囲に加えて、要求する機能を満たす機器やサービスの有無について確認する必要がある。

また、IPv6 対応と表記されている製品の中には、IPv6 パススルー機能（IPv6 通信を透過する機能）のみを実装しているものもあるため、本ガイドラインで説明する IPv6 対応としては、機能不足であることに留意する必要がある。

地方自治体のウェブシステムについては、住民サービスとして多様な住民の端末を対象とする必要がある。このため、市場動向等を踏まえて可能な限り多くの端末をサポートできるように、導入時の試験対象端末の種類について、十分に配慮する必要がある。

IPv6 対応は、ネットワークレイヤからアプリケーションレイヤまで広範囲に及ぶため、IPv6 対応に伴い交換又は更新された機器、サービスソフトウェア及び監視・管理ツール等について、通常運用の範疇において変更点の把握を行うとともに、IPv6 対応の及ぼす影響について整理しておく必要がある。

IPv6 導入に伴う主な障害の発生要因として、以下の項目があげられる。

- アドレスの自動設定による IPv6 非対応機器の暗黙の IPv6 化
  - ルータ等で IP アドレスの自動設定が有効となっている場合、IPv6 に非対応とした機器においても、IPv6 アドレスが付与され、IPv6 通信が可能となることで様々な問題の要因となる。
  - 特にサービスを提供している機器において IPv6 アドレスが付与されたことで、IPv4 と同じように IPv6 によるサービス提供が行われてしまうことがある。IPv6 での設定を正しく行っていない状況のため、IPv4 では制限していたアクセスを IPv6 では許可してしまうという問題が生じる。
- セキュリティポリシーの不整合
  - IPv4/IPv6 双方に対応したサービスについては、セキュリティポリシーを同等に設定しなければならない。ただし、どちらか一方のプロトコルのみに対応したサービスが存在する場合には、対応しないプロトコルについてはアクセスを制限するセキュリティポリシーとしなければならない。
- 名前解決とサービス提供の不整合

- DNS 上、IPv6 アドレス（AAAA レコード、用語集項番 37）が登録されていても、実際のサービスが IPv6 上で提供されていないことがある。また IPv4/IPv6 双方が有効な環境では IPv6 での通信が優先される。これにより、DNS 上に IPv6 アドレスが見つかった場合には IPv6 アドレスでサービスに接続しようとするが、サービスが IPv6 上で提供されていないと、実際に通信可能な IPv4 への切り替え（フォールバック）が発生し、一定時間反応がないという状態になる。ただし、通信の可用性が高まるという点では一定のメリットもあるため、フォールバックを考慮の上で、DNS の管理を確実に実施することが望ましい。

IPv6 のネットワークやサービスの運用について知見を持つサービス事業者、機器ベンダ等から情報収集を密に行い、利用するサービス、機器、OS に応じて、IPv6 導入に伴う障害を調査し、障害発生時の迅速な切り分けが可能であるように対処しておくことが必要である。

6.5 既存 IPv4 システムとの通信の確保

IPv6 対応の範囲を限定することにより、IPv6 で通信できない既存の IPv4 システムが残されることが想定される。この場合、既存の IPv4 システムが IPv6 対応システムと通信できることが求められる。

特に DMZ を IPv6 対応した場合、LAN 上の既存の IPv4 システムとの通信を確保し、従来と比べて遅延などが発生しないことを確認する必要がある。

6.6 IPv6 対応環境への移行にあたっての留意点

IPv6 対応は、既存環境からの移行に当たるため、特にデータの移行及び管理、運用要員の教育及び習熟に留意する必要がある。

6.6.1 データの移行

- 既存システムから IPv6 対応システムへ移行することになったコンテンツについては、その全てを指定の期間内に IPv6 対応システムへと移行する必要がある。このデータには外部向けサービスに必要なデータ以外に、認証に必要なデータ、ログデータ等も含まれる。
- 移行すべきデータについては、IPv6 に対応したテスト環境を用いて検証を行う必要がある。特にログデータ等については既存データのみならず、IPv6 環境で生成されるデータが混在した場合でも、監視や監査が問題なく実施可能であることを検証する必要がある。
- 対象となるシステムやネットワークの規模、扱うデータ量にもよるが、データの移行は移行開始から概ね 1 か月程度で完了するように、予め移行計画を策定することが重要である。
- 移行期間中においても、既存システムが並行稼働可能で、利用上の障害が発生しないような方策が必要である。
- 次々期のシステム更改の際にシステム間のデータ移行を確実なものとするため、その際のデータアーカイブの出力までを確実に実施することを事業者に求めることが重要である。

6.6.2 要員の教育

- 新システムの稼働にあたって、関係者向けの説明会を実施する必要がある。

- 管理担当者が特別な教育訓練なしにシステムを管理することができるように、コンテンツ管理者向けのマニュアルやシステム管理者向けのマニュアルを用意する必要がある。
- IPv6 対応によって変更された運用手順などについて教育を行うと同時に、IPv6 全般の知識も習得できるように、教育用コンテンツの内容に配慮する必要がある。

7. IPv6 環境におけるセキュリティ設計時の IPv6 対応方法

IPv6 対応を進めるにあたり、IPv6 環境に起因する新たなセキュリティ上の脅威への対策を講じる必要がある。脅威としては、IPv6 対応の機器やサービスが導入されることによる技術的な課題に加えて、運用に関する課題についても想定される。

以下では、特に地方自治体における IPv6 対応における脅威と対策について説明する。

7.1 地方自治体にとってのセキュリティ課題の概要

地方自治体では、インターネット利用回線やそれが接続している庁内 LAN とは別に、個別業務システム専用の回線や独自 LAN が数多く導入されている場合がある。LGWAN が導入されている点も含めて、複雑なネットワーク構成となっている点に留意する必要がある。

加えて、情報システムやネットワークの構成情報が一元管理されておらず、所管部署が独自に導入した情報システムやネットワークを、情報システム管理部門が十分に把握できていない場合もある。この場合に、IPv6 対応による影響が既存の情報システム等に及ぼす影響を事前に予測できないことも想定される。IPv6 対応による既存の情報システム等に及ぼす影響を事前に確認する必要である。

IPv6 対応においては、地方自治体のセキュリティポリシーを特別に改訂する必要はないが、現状のセキュリティポリシーを維持するために、IPv6 対応による影響の範囲や程度については、自治体内部の関連部署を含めて詳細な調査が必要である。

7.2 機器に関するセキュリティ課題

IPv6 対応機器を導入する際には、IPv4 と同等のセキュリティが IPv6 でも確保できていることを確認する必要がある。特にネットワーク機器の場合、IPv4 に対して提供される機能や性能に比べて、IPv6 では機能や性能が劣る場合もあるため、導入時には注意が必要である。

7.3 運用に関するセキュリティ課題

メールシステムについて、IPv4 の利用時に送信者の真正性を確認する手段として、IPv4 アドレスの逆引きの可否を用いる場合がある。IPv6 の利用においては、IPv6 の逆引きが登録されているケースが少ないこともあるため、真正性の確認に逆引きを使用するか否かは、十分に配慮する必要がある。

中小規模の自治体では、運用に十分な要員を確保できないため、運用状況の監視や異常発見時の対応などの、IPv6 対応による変更の有無を十分に検討する必要がある。特に運用ツールが IPv4/IPv6 で統合されない場合、運用手順が煩雑になり作業量も増えるため、運用要員の負荷が高まり、特に IPv6 側の対応がおろそかになりかねない。IPv6 対応と同時に、運用作業の自動化や効率化を検討する必要がある。

7.4 システム環境に起因する予期せぬセキュリティ課題

自治体職員に対する IPv6 デフォルト端末の導入や、IPv6 対応のネットワーク機器の導入により、設計時には想定していなかった IPv6 通信や外部に対する IPv6 トンネルが発生する可能性がある。この場合、IPv4 を前提としたセキュリティ対策をすり抜けてしまうため、セキュリティ上の脅威となり得る。

外部向けサービスの IPv6 対応においても、各サービスの出力ログが IPv6 通信に十分対応できていない場合や、IPv4 と IPv6 のログが別々に出力され、管理される場合には、IPv6 部分の管理が不十分になることも想定されるため、留意が必要である。

7.5 セキュリティ課題への対応策

IPv6 デフォルト端末や IPv6 対応のネットワーク機器などが導入された場合、実際に IPv6 化する時期以前は確実に IPv6 通信を抑制することで、予期せぬセキュリティ違反を防ぐことが可能である。外部向けサービスについても、IPv6 対応を開始する時期以前は確実に IPv6 通信を抑制することで、IPv6 通信に関する管理不足を防ぐことが可能である。

その他、IPv6 に関するセキュリティ課題や対応策については、下記も合わせて参照することが望ましい。

(1) IPv6 対応セキュリティガイドライン（第 1.0 版）
http://www.v6pc.jp/jp/upload/pdf/swg-IPv6SecurityGuideline_v1.0.pdf

(2) IPv6 導入時に注意すべき課題
http://www.v6pc.jp/jp/upload/pdf/2011093001_v6fix.pdf

8. 保守、運用及び監視に関する設計時の IPv6 対応方法

本章では、外部向けのサービスを提供する DMZ セグメント及び外部事業者の提供するサービスを利用する場合の、保守、運用及び監視の IPv6 対応方法について説明する。

8.1 IPv6 設計時、導入時の考慮事項

IPv6 対応を行った直後は、機器やサービスの稼働状況の監視において、IPv4 のみで運用していた状況と比べ、特別な変化が表れていないか十分に注意する必要がある。IPv4 と IPv6 が相互に影響して想定外の変化が生じることもあるため、障害要因の切り分け手順を設計時から想定し、ドキュメント化しておくような配慮も必要となる。

また、IPv6 導入を原因として大規模な障害が発生することのないよう、IPv6 導入前の試験、検証を十分に行っておく必要がある。

8.2 IPv6 に対応した監視、管理の方法

外部向けサービスを IPv4 及び IPv6 で提供する際の機器やサービスの監視及び管理対応について説明する。

サービスを提供する機器は外部公開用のネットワークセグメントと、監視及び管理専用のネットワークセグメントの双方に接続されており、サービスの稼動状況を監視する監視サーバが設置されているモデルを想定する（図 8-1）。監視及び管理専用のネットワークセグメントが設置されている場合、各サービスの管理や監視サーバから各サービスの状態監視は、こちらのセグメントを経由して行われる。

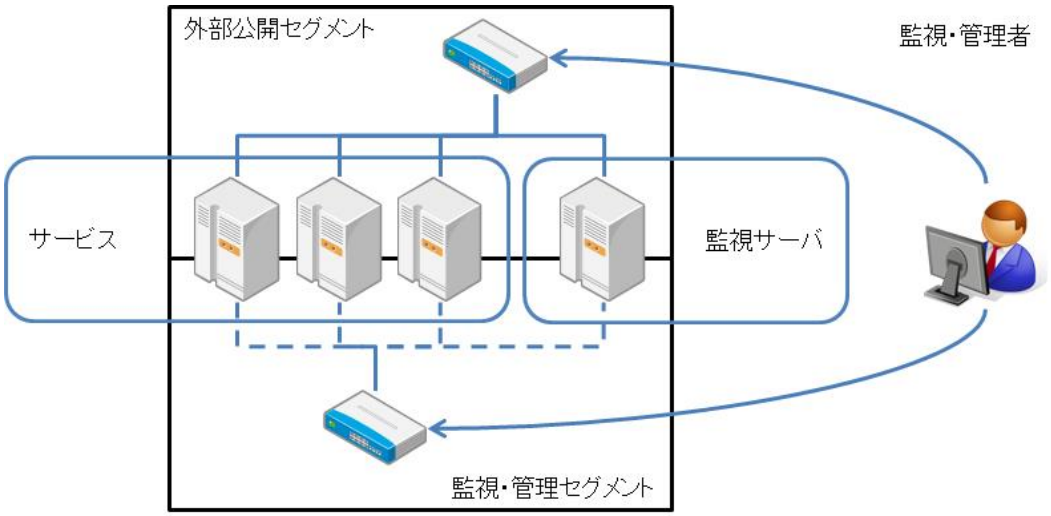

図 8-1　外部向けサービスの監視、管理方法のモデル

ここでの監視対象は、サービスの稼動又は停止状況（死活監視）、ネットワークレスポンスを含めた性能（トラフィック監視や性能監視）、メモリ等リソースの消費状況（キャパシティ管理）とする。

8.2.1 監視ツールの IPv4/IPv6 対応

一般にサービスの監視は、各機器上で稼動して情報を収集する監視エージェント（用語集項番 38）と、監視サーバ上で監視エージェントからの情報を集約する監視サービスから構成

される。このため、サービスの稼働状況監視や性能監視を IPv6 に対応する場合には、監視エージェントにおいて監視対象の取り扱いデータも含めた IPv4/IPv6 対応が必要となり、監視サービスとのデータのやりとりについても、IPv4/IPv6 で行うことが必要となる。

8.2.2 管理ツールの IPv4/IPv6 対応

管理ツールについては、IPv4 又は IPv6 どちらかのトランスポートに障害が発生した場合においても、利用可能なトランスポートを介して管理を行うことが求められるため、IPv4 及び IPv6 双方に対応することが必要である。

8.3 ASP、クラウドサービス利用時の留意事項

ASP やクラウド等のサービスでは､ユーザからのサービス状況の監視を可能とするために、サービスの稼働状況、負荷状況及び性能等の指標情報をモニターやレポートする Web 等のインタフェースが提供されることがある。これらのインタフェースにおいて、IPv6 上の指標情報が取得可能であることを提供事業者に確認することが必要である。

8.4 IPv6 に対応した保守の方法

ネットワークスタックとして IPv4 のみの環境から、IPv4/IPv6 対応のデュアルスタック環境に移行することで、障害が発生する要因が多くなると考えられる。

ここでは、IPv6 対応に伴い保守手順に追加が必要となるネットワークレベルでの障害発生要因の切り分け手順について例示する。

8.4.1 DNS サービスの正常稼動確認

問題の発生しているサービスの IP アドレスは、ホスト名をキーとして DNS サーバから取得する。その際、IPv4 アドレスを示す A レコードと IPv6 アドレスを示す AAAA レコードの双方に対して取得できることを確認する。また、DMZ 上のプライマリ DNS サーバ及びセカンダリ DNS サーバのすべてを確認する必要がある。

8.4.2 ICMP を用いたサービスへの到達性確認

DNS サービスに問題がなければ、例えば ping 又は ping6 コマンド等を用いて、当該サービスへの ICMPv6（用語集項番 39）パケットの到達性を確認する。同時に ICMP（用語集項番 40）パケットの到達性を確認し、レスポンスに要する時間の違いを確認する。ICMPv6 に対するレスポンスはあっても、ICMP よりも明らかに遅い場合には、IPv6 上のパケット転送に問題が生じている可能性がある。

8.4.3 IPv4 経由でのサービスへの到達性確認

ICMP 及び ICMPv6 がともに到達可能でレスポンス時間にも違いがなければ、当該サービスに IPv4 経由でアクセスを試みる。IPv4 においてもサービスにアクセスができない場合には、ネットワークの物理レイヤーで問題が生じている可能性がある。

8.4.4 IPv6 経路上の障害点の確認

IPv4 経由でアクセスが可能であった場合には、IPv6 対応に起因する問題が生じている可能性がある。例えば traceroute コマンドを使うなどしてネットワーク経路上の中継ルータを調査し、IPv6 アクセスが経路上のどのルータまで到達できているのかを調査する。

IPv6 通信にトンネルを用いている場合にはトンネル終端装置に障害が発生している可能

性があるため、確認を行うことが必要である。

8.4.5 ネットワーク上で利用されているサービスの動作確認

メールやウェブ等のネットワーク上で利用されているアプリケーションやサービスの動作においても、IPv4 に関する設定や動作と IPv6 に関する設定や動作のどこに障害の発生要因があるかを調べる手順等、保守手順全体にわたっての更新が必要となる。また、保守作業の実施前に関連する IPv4 及び IPv6 のサービスについて把握した上で保守の実作業を行うとともに、保守作業の実施後にはこれらサービスの正常性を確認することが必要である。

9. IPv6 対応人材の確保

IPv6 対応にあたり、設計や調達の担当者、あるいは運用の担当者自身も IPv6 に対する基本的な知識を習得しておく必要がある。これは担当者自身のスキル向上のみならず、外注業者等に求める IPv6 スキルの指定方法にも関係する知識である。

しかし、現時点では IPv6 によるネットワーク環境を構築しているのは、ネットワーク環境の提供側組織である ISP やデータセンタがほとんどで、利用側組織である地方自治体や企業等の事例は限られており、ノウハウの蓄積も少ない状況である。

ここでは、このような状況の中でまだ数は少ないながら展開されている IPv6 技術者向け教育プログラムについて紹介する。

9.1 ネットワーク技術者に求められる IPv6 関連技術習得に係る資格試験認定

IPv6 普及・高度化推進協議会と一般財団法人電気通信端末機器審査協会（JATE）が共同で運営する IPv6 対応技術者向け教育プログラムの認定制度である。認定された教育プログラムを受けることで、IPv6 に関する一定水準の技術知識が身につくことが期待されており、定期的かつ一般に広く提供されている教育プログラムとしては、現在唯一と言える。

参考 URL：

http://www.v6pc.jp/jp/entry/wg/2012/02/v6qualification.phtml

http://ipv6.jate.jp/cqv6op

9.2 ハンズオンセミナー資料

2012 年度まで実施された IPv4 アドレス枯渇対応タスクフォースのハンズオンセミナーの資料が公開されている。ISP、CATV、データセンタ等のネットワークのリファレンスモデルとともに公開されており、自習により知識を習得できるようになっている。

参考 URL：

http://www.kokatsu.jp/

9.3 Internet Week 等のネットワーク関連イベント時のハンズオン

Interop や Internet Week 等のインターネット関連のイベントにおいて、IPv6 に関するハンズオンセミナーが開かれることがある。プログラムの内容はイベントによって異なるので、早めに実施情報を入手することが重要である。

参考 URL：

http://www.interop.jp/

https://www.nic.ad.jp/ja/materials/iw/

https://internetweek.jp/

9.4 その他、IPv6 に関するセミナー等

ネットワークの機器ベンダや代理店、SIer 等が、機器の紹介を兼ねて定期又は不定期に IPv6 に関するセミナーを開くことがある。詳細については検索等により情報入手し、当該業者に問い合わせて欲しい。

10. IPv6 対応に伴う調達及びコストについての考え方

10.1 コストに対する考え方の概要

IPv6 対応に伴うコストには、機器コスト、設計及び構築コスト、運用コストを考える必要がある。各コストに関して、従来の IPv4 対応のコストに加えて、以下に示すような IPv6 対応に伴うコストの増減が想定される。

一方、IPv6 対応は、アプリケーションレベルでみると大きな違いはないが、基盤レベルでみると機器や機能の刷新を伴うものである。これを期にシステムの総合的な見直しを行い、ASP/クラウドサービスの導入や統合管理の導入を図るなどにより、全体的なコスト低減を検討することが望ましい。

10.2 機器のコスト

機器コストに関しては、初期コストと保守コストの両面を考える必要がある。

初期コストに関しては、特にルータやスイッチ、サーバ等の機器については標準で IPv6 対応機能が付属しているケースが増えてきているため、IPv6 対応における増分はあまり多くない。一方、セキュリティ関連の機能については、IPv6 対応に追加費用が必要となるケースもあるため、留意が必要である。調達時には、必要とする IPv6 機能が標準で対応可能か否か、確認が必要である。

保守コストに関しては、基本的には従来の IPv4 対応の場合と同様と考えられるが、調達時に IPv6 機能が標準で対応していない場合には、その分が保守費用にも追加されることになる。

10.3 設計及び構築のコスト

設計及び構築コストについては、事業者の IPv6 対応の実績や経験により差が出る場合がある。特に IPv6 対応の設計及び構築ができるエンジニアが限られている可能性があり、その場合に IPv6 対応の追加コストが発生する。

また、設計及び構築の工期についても留意が必要である。対応可能なエンジニアをアサインするために、IPv4 対応の場合よりも工期を長く設定する場合があり得る。また、構築時の試験項目も IPv6 対応の分が増えるため、コスト、工期ともに増加する可能性がある。

10.4 運用のコスト

運用コストについては、監視の目的などは IPv4 の場合と同様であっても、監視対象に IPv6 対応を加えることで、コスト増となる可能性がある。特に、監視ツールなどが IPv4/IPv6 を統一的に扱うことができず IPv6 を別のツールで監視する場合には、コスト増に加えて、監視が不十分になるなどのリスクがあることにも留意する必要がある。

障害発生時の対応についても、障害の原因切り分けを IPv4/IPv6 で実施するために、対応可能なエンジニアが限られるなどの理由から、標準的な対応時間が延びる可能性がある。従来と同様の対応時間を求める場合にコスト増となる場合もあるため、サービスレベルの設定には十分留意する必要がある。

一方で、1 つのサブネットが収容可能なホストの数が事実上無限大となるため、組織構成や物理的配置構成に合わせたアドレス設計が楽になるという利点もある。当面は IPv4 との共存になるため、従来かかっていたコストが減ることは考え難いが、将来的に IPv6 のみの運用なども組み合わせていくことで、アドレス管理コストを減らすことが期待される。

11. その他の留意事項

11.1 地方自治体の IPv6 対応におけるその他の留意点

地方自治体の IPv6 対応においては、通常のインターネット接続のみならず、業務システムで独自に利用している回線や LAN との関係に留意する必要がある。特に、LGWAN については導入が必須であることから、LGWAN の IPv6 対応計画との関係に留意し、そのスケジュールとの整合を図る必要がある。

11.2 LAN を IPv6 対応する場合の留意点

ここでは、LAN 環境を IPv6 に対応させる場合の留意点について説明する。

11.2.1 IPv6 アドレス自動設定に伴う留意点

ルータ広告（RA、Router Advertisement）を用いた自動アドレス割り当てを行っている場合、LAN に機器を接続するだけで通信可能となってしまうことがある。セキュリティ上の抜け穴となるため、DHCPv6 を用いて、登録された機器には事前に定められたアドレスが付与されるようにし、それ以外は自動で生成されたアドレスを拒否するような設定が必要である。

11.2.2 OS のアップデート等に伴う挙動の変化

OS のアップデート、アプリケーションのアップデートに伴い、IPv6 対応の挙動が変化し、正常な通信ができないといった事象が発生するリスクがある。ネットワークプロトコルスタックに関連するアップデート、サービスアプリケーション、クライアントアプリケーションのアップデートの際には、試験環境で十分に検証試験を行う必要がある。

11.2.3 端末管理システムの IPv6 対応

LAN に接続された端末等の機器の情報を管理するシステムにおいて、IP アドレスを管理するフィールドを IPv6 対応する必要がある。IPv6 アドレスにおいては、「0」の省略方法により、同じアドレスを何通りか表記することができるため、IP アドレスによるデータ検索、ソートといったアドレス表記に影響される機能の動作検証を十分に行う必要がある。

11.3 複数拠点間で IPv6 を利用する場合の留意点

組織の拠点間を専用回線で接続する場合における IPv6 対応について説明する。2 つの拠点 A と B があり、拠点間が専用回線等で接続されているモデルを考える（図 11-1）。

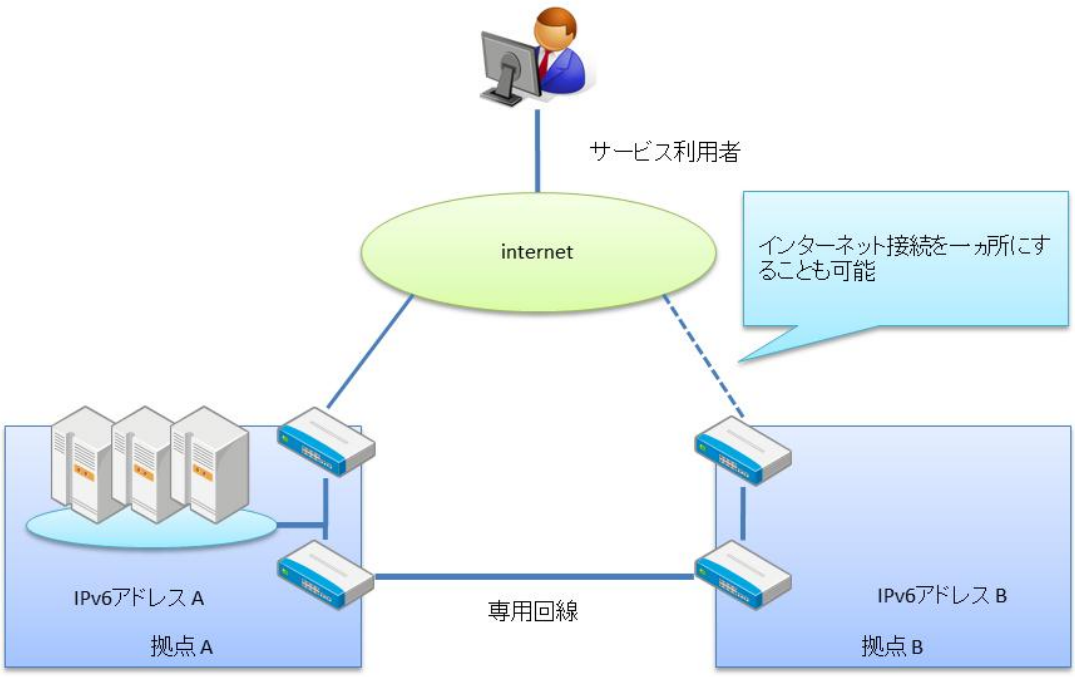

図 11-1　複数拠点間の IPv6 接続

拠点間を結ぶ回線上で IPv4、IPv6 のどちらか、あるいは双方を利用可能とするか否かの判断については、拠点間で利用するサービスの IPv6 対応状況に依存する。拠点間で LAN を共有する場合、LAN 内が IPv6 に完全に対応しているのであれば、拠点間接続は IPv6 のみとすることが可能である。IPv4 のみのサービスが存在している状況や、IPv6 対応は完了しているが実運用面で不安が残っている状況では、IPv4 及び IPv6 双方に対応することが望ましい。

また、LAN 内の IPv6 対応時期が未定という場合には、暫定措置として IPv4 のみの対応とし、拠点間接続の IPv6 対応については、IPv6 移行計画上の検討事項としておく選択も考えられる。

11.3.1 インターネット接続を全拠点で共有する場合の留意点

組織全体としてインターネット接続を 1 つの拠点のみとし、他の拠点からはインターネット接続を持つ他拠点を経由してインターネットアクセスを行う構成とする場合、拠点間接続を IPv6 のみとすると、インターネット上の IPv4 サービスにアクセスすることができなくなる。このような場合には、IPv4 と IPv6 をプロトコルレベルで変換、転送するトランスレータを設置して、インターネット上の IPv4 サービスを利用可能とする。

なお､インターネット接続を 1 ヵ所のみとした場合､その拠点に障害が発生した場合には､他拠点も障害の影響を受け、インターネットアクセスが不可能となってしまう。インターネットアクセスの可用性を維持するためには、拠点ごとにインターネット接続を持つことになる。

11.3.2 インターネット接続を拠点ごとに持つ場合の留意点

2 つの拠点 A と B があり、それぞれがインターネットと接続され、別々の IPv6 アドレスを割り当てられている場合、インターネット上の利用者が拠点 A に配置されたサービスを利用する際の経路が 2 通り存在する（図 11-2)。

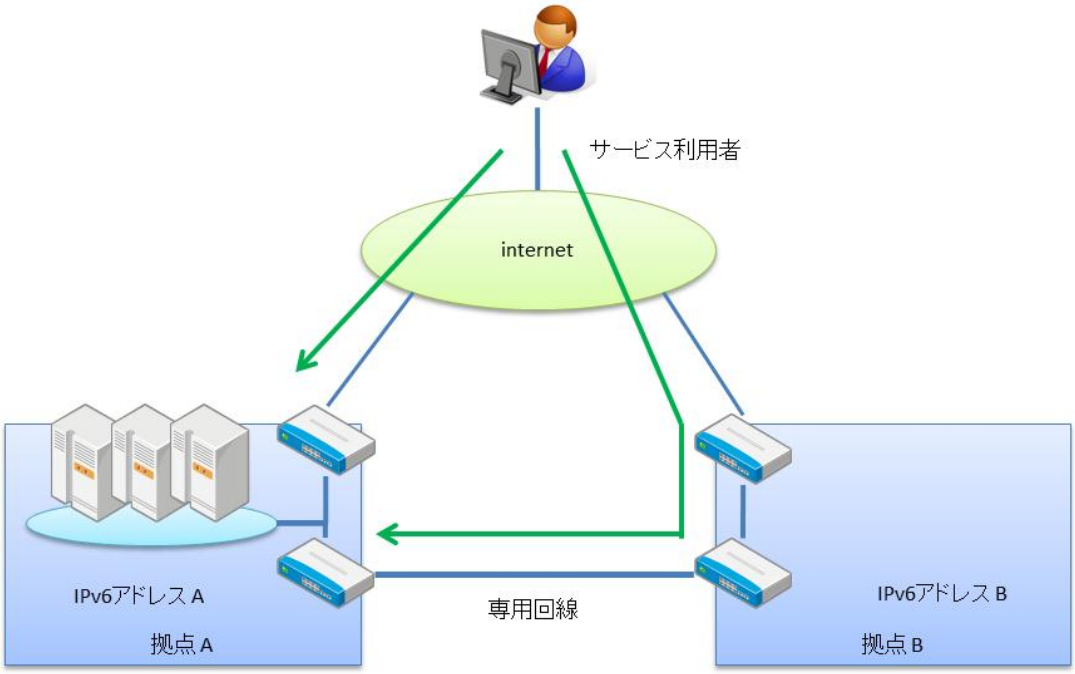

図 11-2　拠点間の経路によりマルチホームとなる場合

拠点 A には IPv6 アドレス A が割り当てられ、拠点 B には異なる IPv6 アドレス B が割り当てられる。このような場合、拠点上のサーバ等には IPv6 アドレス A 及び IPv6 アドレス B をともに割り当て、通信先となるインターネット上のサービスの IPv6 アドレスに応じて、2 つの経路を使い分けることが可能である。

複数の通信事業者から割り当てられた IPv6 アドレスをサーバ等に割り当てる環境をマルチホーム（又はマルチプレフィックス）と呼ぶ。マルチホーム環境は上記のように IPv6 アドレスに応じた経路の使い分けが可能となる一方で、マルチホーム環境に特有なアドレスの誤選択や設定ミス等により意図した通信ができないといった問題が発生する可能性がある。

マルチホーム環境を構成する際には、その問題点を十分に理解し、運用に支障を来さない構成を立案することが求められる。

12. （参考）IPv6 対応チェックシート

表 12-1　IPv6 対応チェックシート

分類	チェック内容	補問／回答例	チェック欄
IPv6対応に向けた基本計画			
	IPv6対応する範囲を検討しましたか。次のシナリオのいずれかに該当しますか。	DMZ/LANともにフルデュアルスタック化	□
		DMZのみデュアルスタック化	□
		DMZをトランスレータ等でIPv6対応	□
		サービス利用のみをIPv6対応	□
	段階的にIPv6対応する場合に、移行計画を含めた複数年に渡るスケジュールを策定しましたか。関連する他のシステムの更新計画との整合性を確認しましたか。		□
IPv6アドレスの設計			
	自組織に必要なIPv6アドレスサイズを確認しましたか。	/64を選択する場合、IPv6対応する範囲を将来拡張した場合に問題ないか確認しましたか。	□
	IPv6アドレスの調達先の回線サービス事業者を選定しましたか。		□
	将来、回線サービス事業者を変更して割り当てられるIPv6アドレスが変わっても大丈夫なように設計してありますか。		□
IPv6対応すべき機器やサービスの確認			
	IPv6対応する範囲に含まれる機器やサービスを、自組織のネットワーク構成図などで確認しましたか。		□
	IPv6対応すべき機器やサービス、回線について、IPv6対応が可能か否か事業者等に確認しましたか。		□
	IPv6対応する範囲に含まれるソフトウェア（パッケージソフト、自主開発ソフト等）がIPv6対応しても問題ないことを確認しましたか。		□
	IPv6対応すべき機器やサービスに要求する機能要件、非機能要件を定めましたか。		□
	IPv6対応しない既存の機器やサービスとのIPv4による通信は担保できていますか。		□
セキュリティ対応			
	IPv6対応によって、現状のセキュリティポリシーが保たれることを確認しましたか。		□
	IPv6対応によって、システムのレスポンスなどが著しく低下しないことを確認しましたか。		□
	IPv6対応によって、運用手順が煩雑になるなど、運用要員の負荷が高まらないことを確認しましたか。		□
	想定しないIPv6トンネルがLANとインターネットとの間で作られることを抑制していますか。		□
保守、運用及び監視の体制			
	IPv6対応する機器やサービスについて、IPv4とIPv6の運用が統一的に実施できますか。必要とする人員のスキルや体制が従来と同様ですか。		□
	機器やサービスの障害時の保守体制は、IPv4とIPv6で同様ですか。		□
	IPv6対応する機器やサービスについて、IPv6の稼働状況がIPv4と同様に監視できますか。		□

分類	チェック内容	補問／回答例	チェック欄
人材の確保			
	IPv6対応に関して、設計及び調達の担当者や運用の担当者の知識及びスキルに問題はありませんか。外部事業者の知識及びスキルに問題はありませんか。		□
	要員のIPv6対応に向けた教育計画を策定しましたか。		□
調達コスト			
	IPv6対応に必要なコストを試算し、予算化しましたか。		□
	機器やサービスのコストについて、初期コストと保守コストの両面を確認しましたか。		□
	設計及び構築のコストについて、IPv6対応によって追加コストが発生しないことを確認しましたか。工期が長くならないことを確認しましたか。		□
	運用のコストについて、IPv6対応によって追加コストが発生しないことを確認しましたか。障害発生時などにサービスレベルが低下しないことを確認しましたか。		□
その他の留意点			
	その他の留意事項に該当する事項があるかどうかを確認し、内容把握と対象方法を決定しましたか。		□

13. （参考）参考文献

[1]

「IPv4 アドレス在庫枯渇緊急対策ガイド　ハンドブック」平成 23 年 2 月
財団法人地方自治情報センター

[2]

「財団法人地方自治情報センター（LASDEC）における IPv6 対応方針書【公開版】」
平成 23 年 6 月」
財団法人地方自治情報センター

[3]

「情報システム調達のための技術参照モデル（TRM）平成 24 年度版」平成 25 年 4 月
経済産業省

[4]

IPv6 によるインターネットの利用高度化に関する研究会第二次中間報告書参考資料
総務省　IPv6 によるインターネットの利用高度化に関する研究会

[5]

Geoff Huston 氏の推計サイト
http://www.potaroo.net/tools/ipv4/index.html

[6]

ブロードバンドサービス等の契約数の推移
総務省
http://www.soumu.go.jp/johotsusintokei/field/tsuushin01.html

[7]

平成 23 年通信利用動向調査（企業編）
総務省
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05b2.html

[8]

IPv6 によるインターネットの利用高度化に関する研究会 第二次プログレスレポート
総務省　IPv6 によるインターネットの利用高度化に関する研究会
http://www.soumu.go.jp/main_content/000239088.pdf

[9] [RFC4291]

RFC4291（IP Version 6 Addressing Architecture）
IETF（Internet Engineering Task Force）
http://datatracker.ietf.org/doc/rfc4291/

[10] [RFC5952]
RFC5952（A Recommendation for IPv6 Address Text Representation）
IETF
http://datatracker.ietf.org/doc/rfc5952/

[11] [RFC3587]
RFC3587（IPv6 Global Unicast Address Format）
IETF
http://datatracker.ietf.org/doc/rfc3587

[12]
IPv6 Address Allocation and Assignment Policy
RIPE
http://www.ripe.net/ripe/docs/ripe-589

用語集

項番	用語	読み・別名	意味
1	IPv4	アイピーブイフォー	Internet Protocol version 4、インターネットを構成するネットワーク層のプロトコル。
2	IPv6	アイピーブイシックス	Internet Protocol version 6、IPv4 と同じく、インターネットを構成するネットワーク層のプロトコル。IPv4 との互換性は持たない。
3	DMZ	ディーエムゼット、非武装地帯	DeMilitalized Zone、インターネット向けサービス等を配置するネットワークセグメントのこと。万一、DMZ 上のサーバ等が不正な第三者の侵入を許した場合においても、LAN への侵入を防ぐため、DMZ から LAN への接続を制限される。
4	デュアルスタック		Dual Stack、IP によるネットワーク通信を提供するソフトウェアをネットワークプロトコルスタックと呼ぶ。一つの機器等に IPv4 及び IPv6 二つのプロトコルスタックを共存させることをデュアルスタックと呼ぶ。
5	IP アドレス	アイピーアドレス	IPv4 及び IPv6 を用いて通信を行う際、個々の通信者に付与される識別子の一種。IPv4 では 32 ビット長、IPv6 では 128 ビット長を持つ。
6	RIR	アールアイアール	Regional Internet Registry、地域レベルで設置された IR を RIR、地域別レジストリと呼ぶ。北アメリカを管轄する ARIN、ヨーロッパ・中東・中央アジアを管轄する RIPE、アジア太平洋地域を管轄する APNIC、ラテンアメリカを管轄する LACNIC、アフリカを担当する AfriNIC が設置されている。
7	APNIC	エーピーニック	アジア・太平洋地域を管轄する IR。
8	FWA	エフダブリューエー、固定無線アクセス	Fixed Wireless Access、通信事業者とその加入者間を無線で接続して通信を行うサービスにおいて、基地局及び加入者端末が固定されているもののこと。
9	WiMAX	ワイマックス	Worldwide Interoperability for Microwave Access、中長距離向け無線規格の一つ。
10	BWA	ビーダブリューエー	Broadband Wireless Access、ブロードバンドインターネット接続を提供する無線アクセスサービスのこと。
11	LTE	エルティーイー	Long Term Evolution、第 3.9 世代携帯電話と呼ばれる携帯電話用の通信規格。

項番	用語	読み・別名	意味
12	CGN	キャリアグレードナット	事業者側で使用可能な大規模な NAT のこと。1 つのアドレスに複数のアドレスを割り当て、変換を行うことで、アドレスを節約する仕組を提供している。
13	VM	ブイエム、仮想マシン	Virtual Machine、クラウドサービス等で、1 つの物理的なマシンを仮想的に複数のマシンに見せて、様々なプログラムを同時に走らせるための仕組み。
14	グローバル IP アドレス		Global IP Address、インターネット上でアクセス可能な IP アドレスのこと。反対にインターネットにはアクセスできない IP アドレスを、IPv4 ではプライベートアドレス、IPv6 ではリンクローカルアドレスと呼ぶ。
15	IPS	アイピーエス、侵入抑制システム	Intrusion Prevention System、不正な第三者による侵入の試みを抑制するためのシステム。侵入抑制システム、侵入遮断システムと呼ばれる。IDS と対として提供される場合には、IDS/IPS とまとめて称される。
16	経路集約		Route Aggregation、ルータ等の持つ経路は、経路表（ルーティングテーブル）に保持される。経路表上の各エントリを調べ、同じ配送先のゲートウェイアドレスを持つエントリについて、ネットワークアドレスに共通部分を持つエントリを一つのエントリにまとめることを経路集約と呼ぶ。ネットワーク構築の際、階層型 IP アドレス（プレフィックス）構造とすることで、効率的に経路集約を行い、経路表のサイズを小さくすることができる。
17	NIR	エヌアイアール	National Internet Registry、国レベルで設置された IR を NIR、国別レジストリと呼ぶ。
18	prefix	プレフィックス	IPv6 アドレスのネットワーク部。
19	JPNIC	ジェイピーニック	Japan Network Information Center、わが国における国別インターネットレジストリ（NIR）として、インターネット上のリソースである IP アドレスや AS 番号等を管理する組織。アジア・太平洋地域を管轄する地域インターネットレジストリである APNIC に加盟している。

項番	用語	読み・別名	意味
20	DNS	ディーエヌエス	Domain Name System、ホストネームと IP アドレスの対応関係等をデータとして保有し、ホストネームに対応する IP アドレス又は IP アドレスに対応するホストネーム検索といった問い合わせに対して、データを持っていれば、そのデータを、持っていなければ持っていないことを答えるシステム。
21	L3 スイッチ	エルスリースイッチ	OSI 参照モデルの第 3 レイヤー、ネットワークレイヤにて、通信の中継を行う機器。
22	L2 スイッチ	エルツースイッチ	OSI 参照モデルの第 2 レイヤー、データリンクレイヤにて、通信の中継を行う機器。
23	WAF	ワフ	Web Application Firewall、ウェブアプリケーションを保護するため、ウェブアプリケーション特有の脆弱性である SQL インジェクション、アカウント推測攻撃等の攻撃を検知、遮断する仕組み。
24	IDS	アイディーエス、侵入検知システム	Intrusion Detection System、不正な第三者による侵入の試みを検出するためのシステム。侵入検知システムと呼ばれる。
25	HTTP	エイチティーティーピー	HyperText Transfer Protocol、HTML（HyperText Markup Language）ファイル、画像ファイル、動画ファイル等、ウェブコンテンツをやりとりするためのプロトコル。
26	CMS	シーエムエス	Contents Management System、ウェブアプリケーションの一つで、ウェブインタフェース上からウェブサイトのコンテンツを管理できるようなシステムのこと。
27	リバースプロキシ		Web サーバなど特定の用途のサーバの代理として、そのサーバへの要求を中継するプロキシサーバ。通常の「内部から外部へのアクセスを中継する」(フォワード）プロキシの動作と反対であることが、「リバース」の由来と言われている。
28	SSL	エスエスエル	Secure Sockets Layer、通信を安全性に行うため、通信相手の認証、通信内容の秘匿、通信内容の改ざん検出機能を提供するプロトコル。
29	NTP	エヌティーピー	Network Time Protocol、ネットワーク上で時刻を同期するためのプロトコル。
30	パケットシェーピング		通信量を一定の水準に抑える帯域制御の方式の一つで、規定の通信容量を超えるデータを通信機器内部に保存し、容量に空きができたときに送信する方式。

項番	用語	読み・別名	意味
31	冗長構成		機器等を複数台用意し、一台に障害が発生しても、残りの機器で機能提供を継続できるように、あらかじめ機器を構成すること。
32	MIB	エムアイビー	Management Information Base、通信デバイスの設定情報、状態情報などをオブジェクトの集合として表現するための規格。SNMP によりデバイスを管理する際に利用される。
33	アノマリ		セキュリティ検知の方式の１つ。正常な状態を定義し、それを外れた状態を観測したら異常と判断する。RFC に準拠していない通信、通常よりあきらかに多いトラフィック、通常は使用しないポートへの接続などを検知する。
34	TLS	ティーエルエス	Transport Layer Security、SSL が私企業の独自プロトコルであったことから、SSL の第三版である SSL 3.0 を元に標準化されたプロトコル。HTTPS にて利用される。
35	SMTP	エスエムティーピー	Simple Mail Transfer Protocol、いわゆる電子メールの配送を規定するプロトコル。
36	NIC	ニック	Network Interface Controller 又は Card、サーバ等でイーサネットケーブル等、ネットワークとの物理的な接続を提供するために設置される拡張デバイスのこと。LAN カード、ネットワークアダプタとも呼ばれる。
37	AAAA レコード	クワッドエーレコード	ホスト名と IPv6 アドレスを対応づけるための DNS レコード。
38	監視エージェント		一般にサービスの監視は、各機器上で稼動して情報を収集する監視エージェントと、監視サーバ上に設置され、監視エージェントと通信を行って情報を集約する監視サービスから構成される。監視エージェントはサービスプロセスと同じ機器上で稼動しているので、サービスプロセスの稼動状況、ディスク I/O 等のネットワークに関わらない性能、メモリ、ネットワークインタフェースごとの使用帯域等の情報について、OS を介して取得可能である。
39	ICMPv6	アイシーエムピーブイシックス	IPv6 のための ICMP。
40	ICMP	アイシーエムピー	Internet Control Message Protocol、IP 通信において、障害の検知、通信に関する情報の要請・取得等に利用されるプロトコル。