# IPv6 対応ガイドライン

【中小通信事業者編】

２０１４年７月

# 目次


1. 目的 1
1.1 目的 1
1.2 本ガイドラインの対象者 1
1.3 本ガイドラインの使い方 1
2. 背景 6
2.1 インターネットを取り巻く動向 6
2.2 IPv6 化の進展状況 10
2.3 IPv6 対応を必要とする理由 12
3. 想定するシステム及びネットワークのモデル 15
3.1 一次プロバイダのモデル 16
3.2 二次プロバイダのモデル 17
3.3 ローミングサービスを利用する通信事業者のモデル 18
3.4 CATV 事業における通信事業者のモデル 19
3.5 IPv6 対応モデル 20
4. IPv6 対応に向けた基本計画づくり 21
4.1 IPv6 対応に向けたシナリオ 21
4.1.1 一次プロバイダとのトランジット接続 21
4.1.2 ユーザトラフィック中継のためのバックボーンネットワーク 21
4.1.3 ISP サービスのためのサービスセグメント 23
4.1.4 バックエンドセグメント 23
4.1.5 ユーザとのネットワーク接続 24
4.2 IPv6 対応の基本シナリオ 27
5. IP アドレス設計時の IPv6 対応方法 29
5.1 IPv6 アドレスの基本 29
5.1.1 IPv4 アドレスの表記について 29
5.1.2 IPv6 アドレスの表記について 29
5.1.3 IPv6 アドレスの種類 30
5.1.4 IPv6 アドレスの構造 30
5.1.5 IPv6 アドレスの集約 31
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 32
5.1.7 IPv6 アドレスの分割 32
5.1.8 IPv6 アドレスの調達 33
5.2 通信事業者における IPv6 アドレスの設計に関する留意点 33
5.2.1 ネットワークセグメントの切り分け 33
5.2.2 各セグメントにおけるアドレスサイズの考え方 34
5.2.3 サーバ類に割り当てる IPv6 アドレスの生成 34
6. ユーザに提供するインターネット接続部設計時の IPv6 対応方法 36
6.1 ユーザに提供するインターネット接続に関わる基本アーキテクチャ 36
6.2 IPv6 対応すべき機能 37

6.2.1 NGN をアクセス回線とするネイティブ方式を採用する場合 37
6.2.2 NGN をアクセス回線とするトンネル方式を採用する場合 37
6.3 機能毎の IPv6 対応方法 38
6.4 IPv6 対応に向けた事前準備 39
6.5 既存 IPv4 システムとの通信の確保 40
7. ISP サービス及びバックエンドサービス設計時の IPv6 対応方法 41
7.1 ISP サービス及びバックエンドサービスに関わる基本的アーキテクチャ 41
7.2 IPv6 対応すべき機能 42
7.2.1 セグメント共通 42
7.2.2 ISP サービスセグメント：セキュリティサービス 42
7.2.3 ISP サービスセグメント：ユーザサービス 43
7.2.4 ISP サービスセグメント：基盤サービス 43
7.2.5 バックエンドセグメント 44
7.3 機能毎の IPv6 対応方法 45
7.3.1 セグメント共通 45
7.3.2 ISP サービスセグメント：セキュリティサービス 46
7.3.3 ISP サービスセグメント：ユーザサービス 48
7.3.4 ISP サービスセグメント：基盤サービス 49
7.3.5 バックエンドセグメント 51
7.3.6 その他の機器やサービス 52
7.4 IPv6 対応に向けた事前準備 52
8. IPv6 環境におけるセキュリティ設計時の IPv6 対応方法 54
8.1 通信事業者にとってのセキュリティ課題の概要 54
8.2 機器に関するセキュリティ課題 54
8.3 運用に関するセキュリティ課題 55
8.4 システム環境に起因する予期せぬセキュリティ課題 55
8.5 セキュリティ課題への必要な対応策 55
9. 保守、運用及び監視に関する設計時の IPv6 対応方法 57
9.1 IPv6 設計時、導入時の考慮事項 57
9.2 IPv6 に対応した監視、管理の方法 57
9.2.1 監視ツールの IPv4/IPv6 対応 57
9.2.2 管理ツールの IPv4/IPv6 対応 58
9.3 IPv6 に対応した保守の方法 58
9.3.1 DNS サービスの正常稼動確認 58
9.3.2 ICMP を用いたサービスへの到達性確認 58
9.3.3 IPv4 経由でのサービスへの到達性確認 58
9.3.4 IPv6 経路上の障害点の確認 58
9.3.5 ネットワーク上で利用されているサービスの動作確認 58
10. IPv6 対応人材の確保 60
10.1 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 60
10.2 ハンズオンセミナー資料 60
10.3 Internet Week 等のネットワーク関連イベント時のハンズオン 60
10.4 その他、IPv6 に関するセミナー等 60
11. IPv6 対応に伴う調達及びコストについての考え方 61

11.1　コストに対する考え方の概要　61
11.2　機器のコスト　61
11.3　設計及び構築のコスト　61
11.4　運用のコスト　61
11.5　アドレス管理のコスト　61
12.　その他の留意事項　62
12.1　IPv6 対応手順の参考文献　62
12.2　通信事業者におけるフィルタリング設定　62
12.3　ユーザ問合せ対応の準備　62
13.　（参考）IPv6 対応チェックシート　63
14.　（参考）参考文献　65
用語集　67

# 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が、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 対応させるためのガイドライン及び調達仕様書モデルを提示することが重要であり、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、中小通信事業者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、インターネットとの接続点となる IX（Internet eXchange、用語集項番 3）やトランジットサービスを提供する通信事業者（一次プロバイダ等）との接続、ユーザ向けのインターネット接続サービス及びユーザ向けの DNS（用語集項番 4）やメールサービス等の ISP 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

中小通信事業者のシステムやネットワークは、その団体の規模やサービス提供地域、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。ユーザ数に応じて、また、提供するサービスの種類によって、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 の中小通信事業者があれば、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中小通信事業者によっては、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。

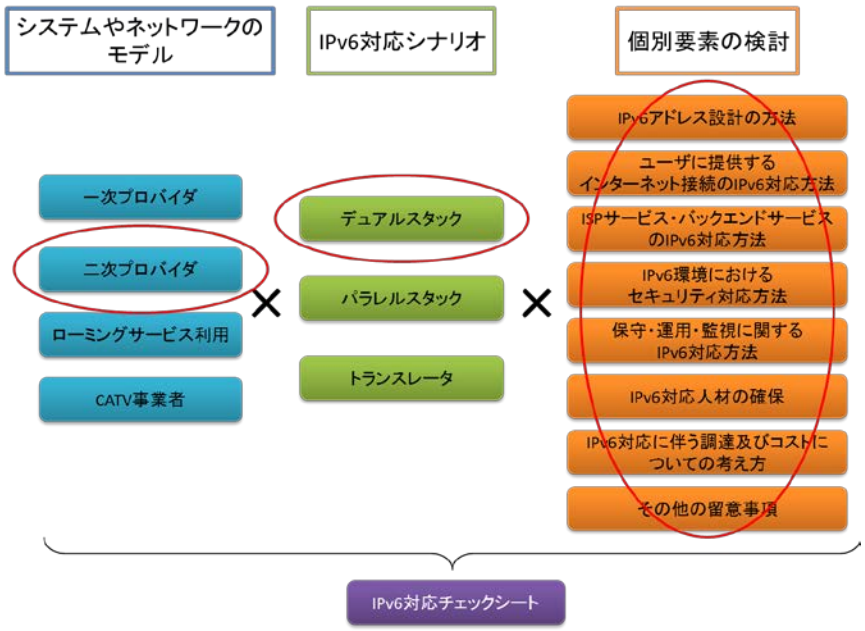


図 1-1　本ガイドラインの利用イメージ

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。

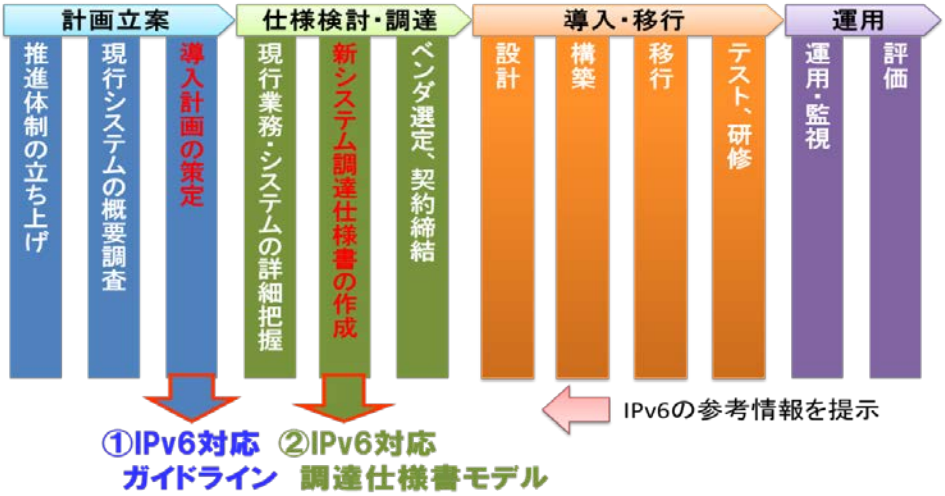


図 1-2　システム導入のフローと本ガイドラインの対象範囲
出典：自治体クラウド・情報連携推進のための研修教材（総務省）を参考に作成

(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、ベンダの評価・選定と契約を締結する。

(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、通信事業者としてなぜ 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

✓通信事業者の場合、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。一次プロバイダ、二次プロバイダ、ローミング（用語集項番 5）サービスの利用者及び CATV 事業者に分けて、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、基本パターンと自組織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、インターネットとの接続部分（IX、一次プロバイダとの接続）、ユーザ向けのインターネット接続サービス、ユーザが利用する外部向けサービスのそれぞれについて、IPv6 対応する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.ユーザに提供するインターネット接続部設計時の IPv6 対応方法

✓インターネット接続サービスとして、ユーザからの IPv6 トラフィックをインターネット上の IPv6 サービス等へと中継する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、既存の 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.ISP サービス及びバックエンドサービス設計時の IPv6 対応方法

✓中小通信事業者としてユーザに提供する ISP サービス（電子メールサービス、ウェブホスティング（用語集項番 6）、DNS サービス、中小通信事業者自身のポータルサイト等）や、バックエンドサービス（ユーザ管理システム、課金システム、ログ監視システム、サービス監視システム等）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。

8.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。

9.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。

10.IPv6 対応人材の確保

✓IPv6 対応にあたっては、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。

11.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。

12.その他の留意事項

✓11 章までに説明した IPv6 対応以外に留意すべき事項についての解説を行う。

13.（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。

14.（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 7）が存在する。

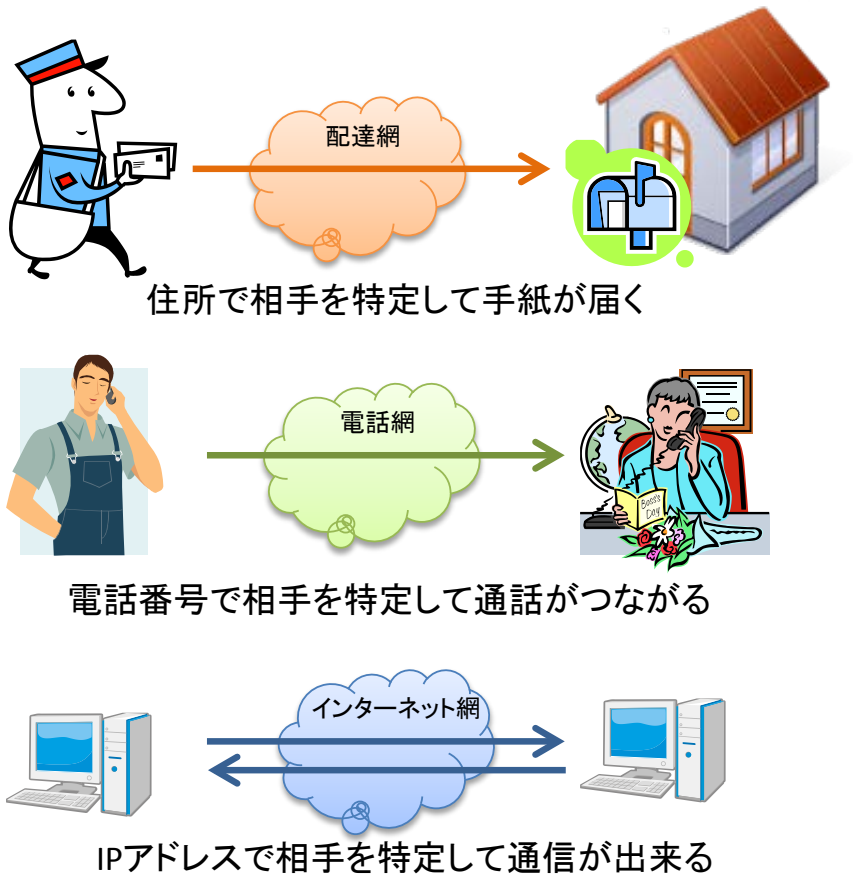


図 2-1　通信の際に相手を特定する情報

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。

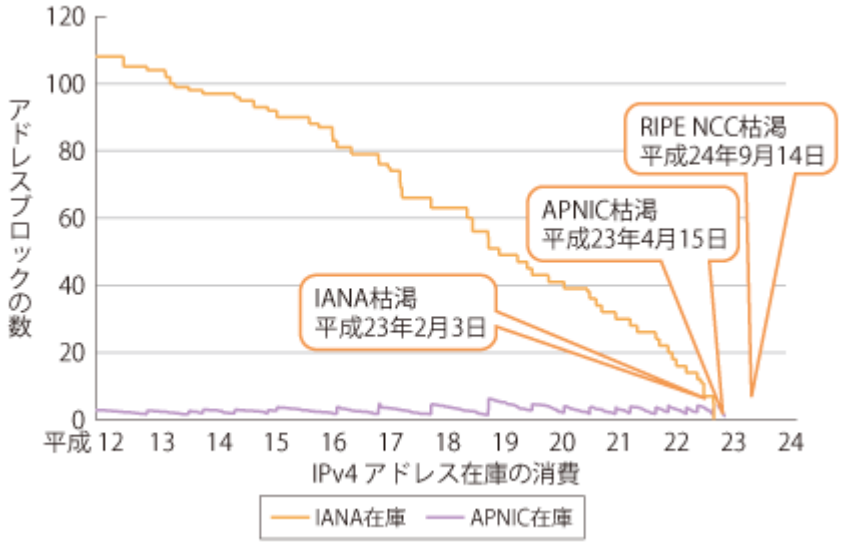


図 2-2　IPv4 アドレス在庫の消費グラフ
出典：総務省　平成 25 年度版　情報通信白書
（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc245350.html）

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 8）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。

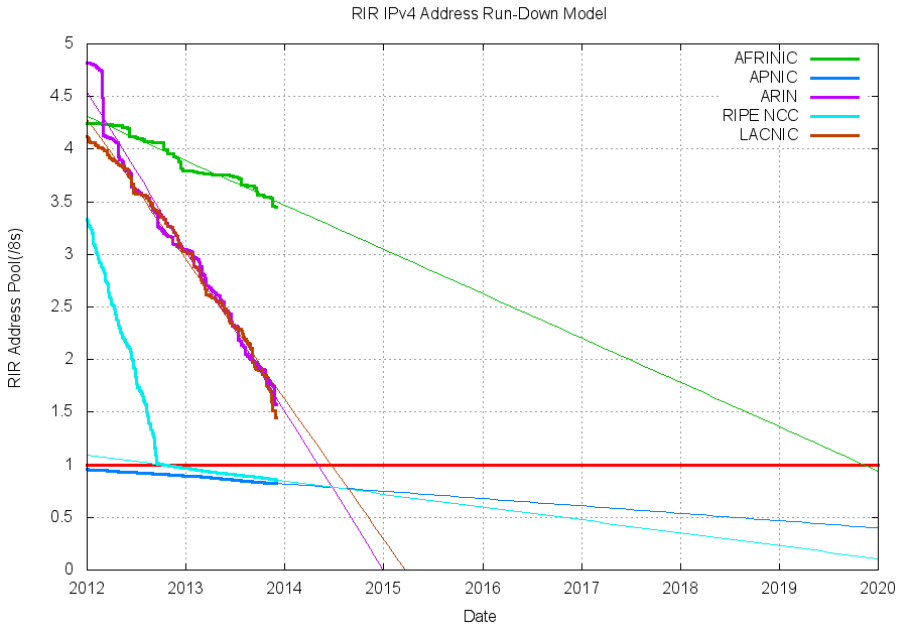


図 2-3　2013 年 12 月当初時点の IPv4 アドレス在庫の減少の推計グラフ
出典：Geoff Huston 氏の推計サイト（http://www.potaroo.net/tools/ipv4/index.html）

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 9）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。

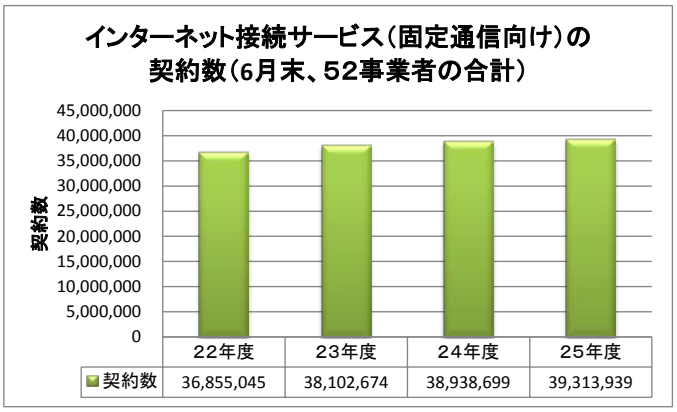


図 2-4 インターネット接続サービス（固定通信向け）の契約数（52 事業者の合計）
出典：総務省　ブロードバンドサービス等の契約数の推移
（http://www.soumu.go.jp/johotsusintokei/field/tsuushin01.html）

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 10）、WiMAX（用語集項番 11）等の BWA（用語集項番 12）、LTE（用語集項番 13）、公衆無線 LAN の合計）は急激に増加している。

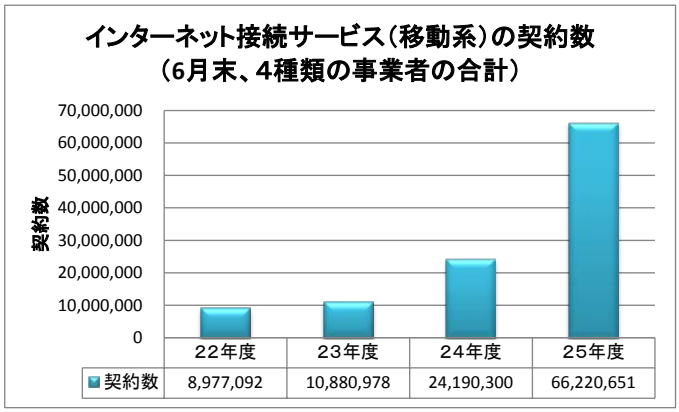


図 2-5　インターネット接続サービス（移動系）の契約数（4 方式の合計）
出典：総務省　ブロードバンドサービス等の契約数の推移
（http://www.soumu.go.jp/johotsusintokei/field/tsuushin01.html）

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。

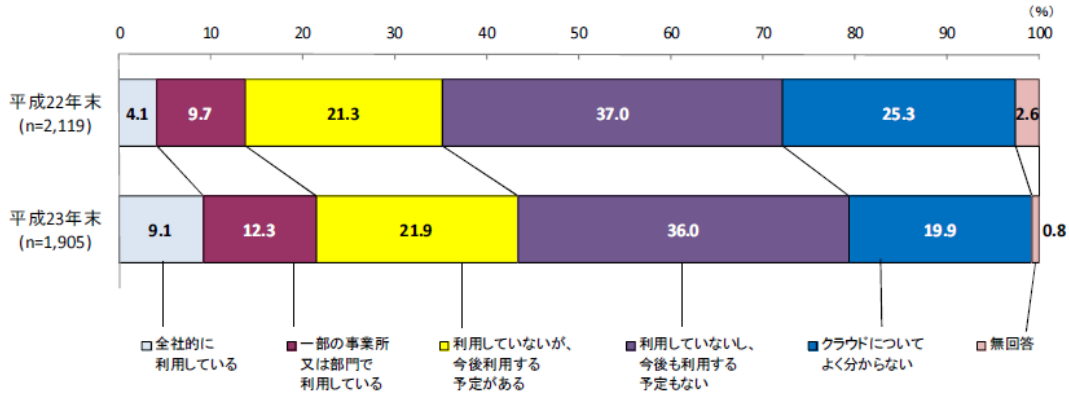


図 2-6　クラウドの利用状況
出典：総務省　平成23年通信利用動向調査（企業編）
（http://www.soumu.go.jp/johotsusintokei/statistics/statistics05b2.html）

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。

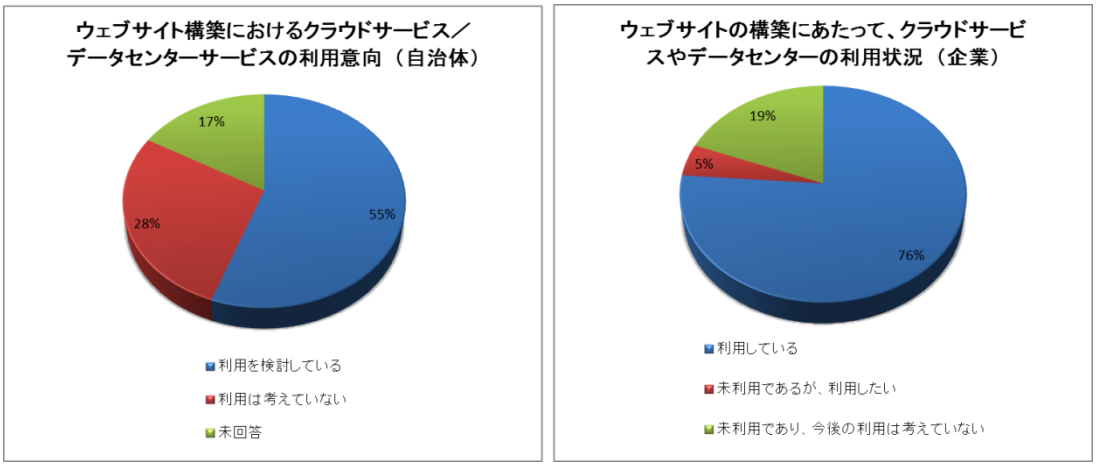


図 2-7　ウェブサイト構築にあたってのクラウドやデータセンターサービスの利用意向及び利用状況

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。

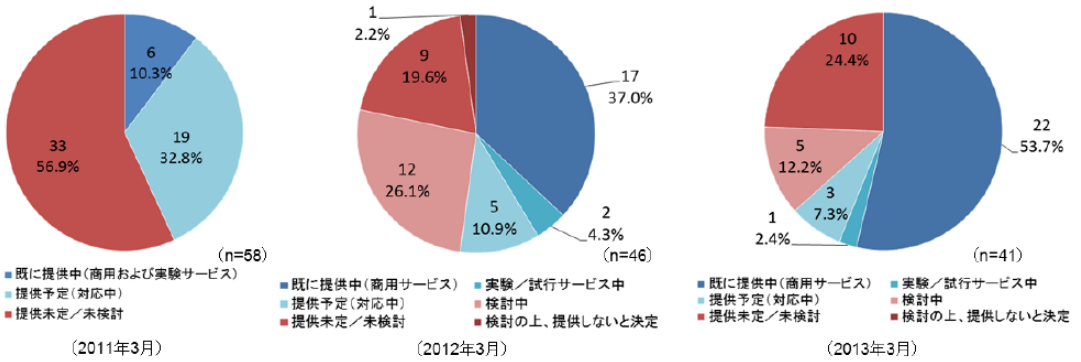


図 2-8　ISP の IPv6 対応状況推移（CATV 事業者を除く）

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

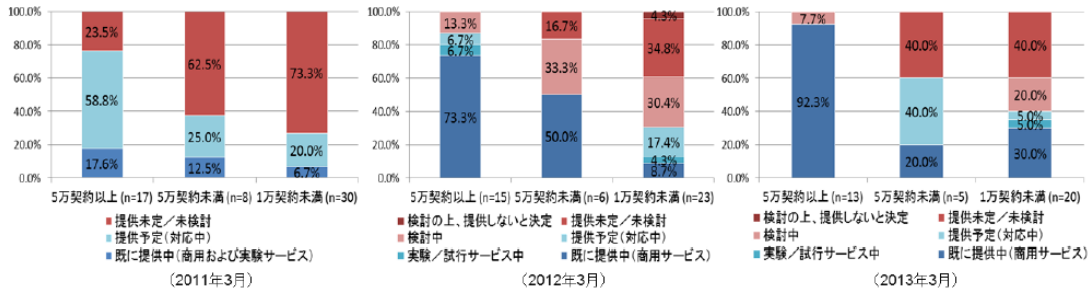


図 2-9　規模別の ISP の IPv6 対応状況推移（CATV 事業者を除く）

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。

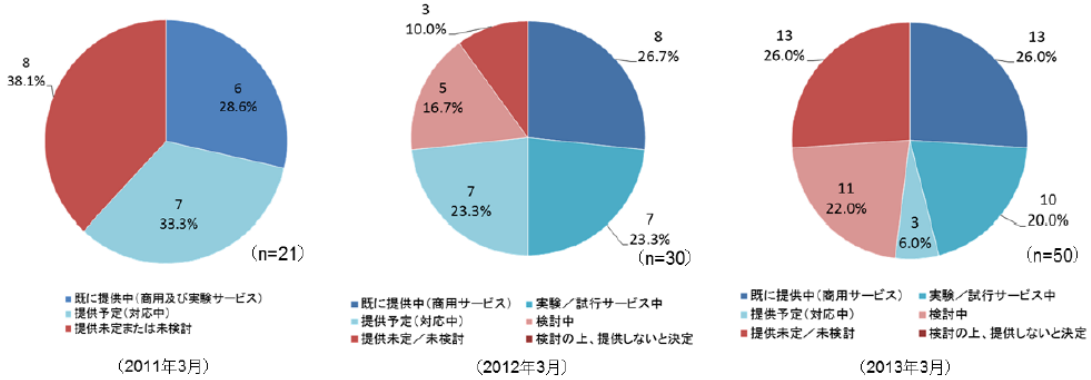


図 2-10　データセンタ事業者の IPv6 対応状況推移

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

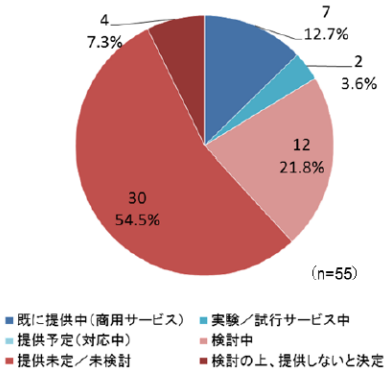


図 2-11　コンテンツ事業者の IPv6 対応状況

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

中小通信事業者の IPv6 対応を検討するには、IPv6 に関する最新の動向、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、IPv6 対応に向けて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<br>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<br>（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<br>（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<br>（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。

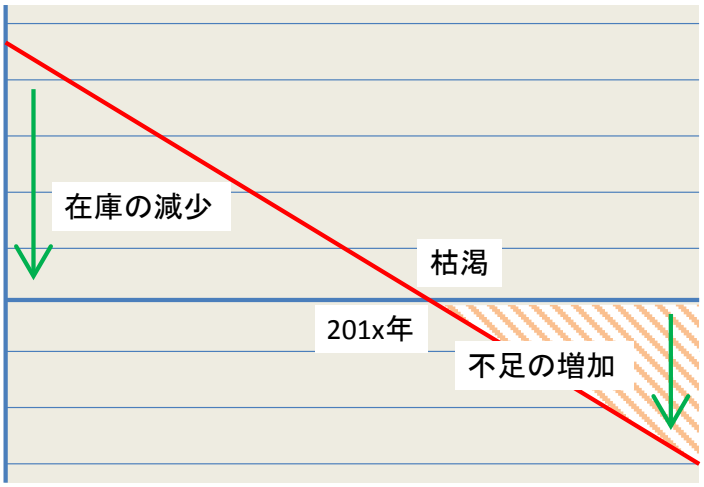


図 2-12　アドレス減少の時代からアドレス不足の時代へ

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 14）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、ベンダの努力もあり、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 15）を多数利用する基盤を調達する場合がある。この場合は、新規のグローバル IP アドレス（用語集項番 16）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。

中小通信事業者においては、ユーザに払い出す IP アドレス、ウェブホスティング等で提供する IP アドレス等、多くの IP アドレスを必要とすることから、IPv6 対応は必須といえる。

**(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。特に地方自治体の

ように全ての住民に対して公平にサービスを提供する必要がある場合や、ネット広告業界のように 1 人でも多くのユーザにリーチする必要がある場合は、IPv6 対応を実際に進める必要が出てくる。

中小通信事業者においては、ユーザの契約情報確認、新規申し込み受付サービスを提供するポータルサイト、ウェブホスティング等、インターネットを経由したサービスへのアクセスが多くあることから、これらのサービスを 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、自然に 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 17）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。

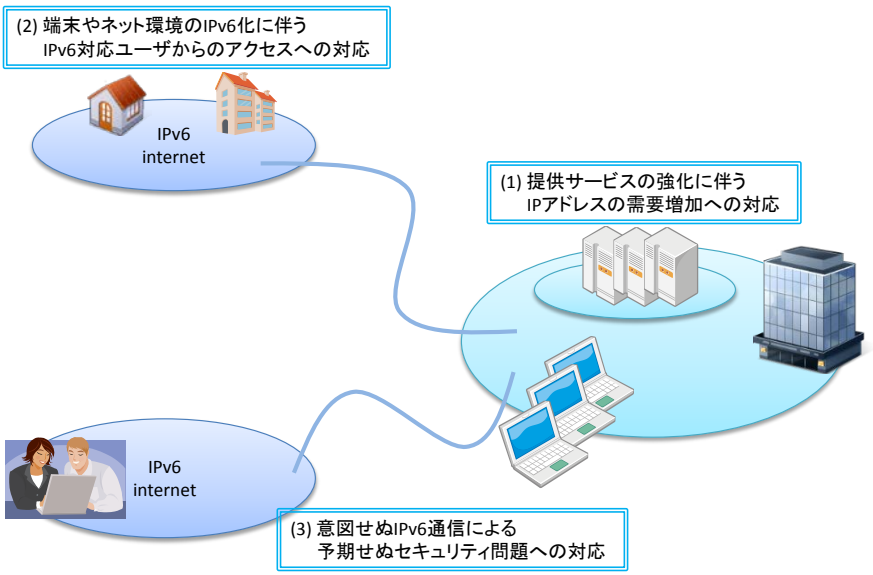


図 2-13　IPv6 対応を考えるべき 3 つの理由

## 3. 想定するシステム及びネットワークのモデル

通信事業者の場合、ユーザ回線数等の規模、電子メールサービスやホスティングサービス等のユーザに提供する ISP サービス、ユーザの利用するアクセス回線種別などによって、想定されるシステムやネットワークのモデルが異なる。

インターネットとの接続に関して、大規模な通信事業者ではインターネット相互接続点（IX）等との接続を持つネットワーク構成が想定され、中小通信事業者では別の通信事業者が提供するトランジット接続を利用するネットワーク構成が想定される。ユーザに対するインターネット接続サービスに関して、多くの通信事業者ではアクセス回線経由でユーザからのインターネットアクセスを収容するが、小規模通信事業者の場合には他の通信事業者の提供するローミングサービスを利用し、自社にはユーザからのインターネットアクセスを収容しないネットワーク構成が想定される。

### 3.1 一次プロバイダのモデル

以下に、一次プロバイダと呼ばれる通信事業者の、システムやネットワークのモデル概念図を示す。このモデルは以下の要素から構成される。

（1） インターネットアクセスのため、IX において、他通信事業者等とのピアリング（peering、用語集項番 18）を行う。

（2） 主にユーザとインターネット間のトラフィックを中継するためのバックボーンネットワークを持つ。

（3） ISP サービスの基盤として、インターネット及びアクセス回線経由でユーザがアクセス可能なサービスセグメントを持つ。

（4） ユーザ管理等のバックエンドサービスを配置するバックエンドセグメントを持つ。

（5） ユーザとの間にアクセス回線経由でのネットワーク接続を持ち、ユーザとインターネット間のトラフィックを自社のバックボーンネットワーク上で流通させる。

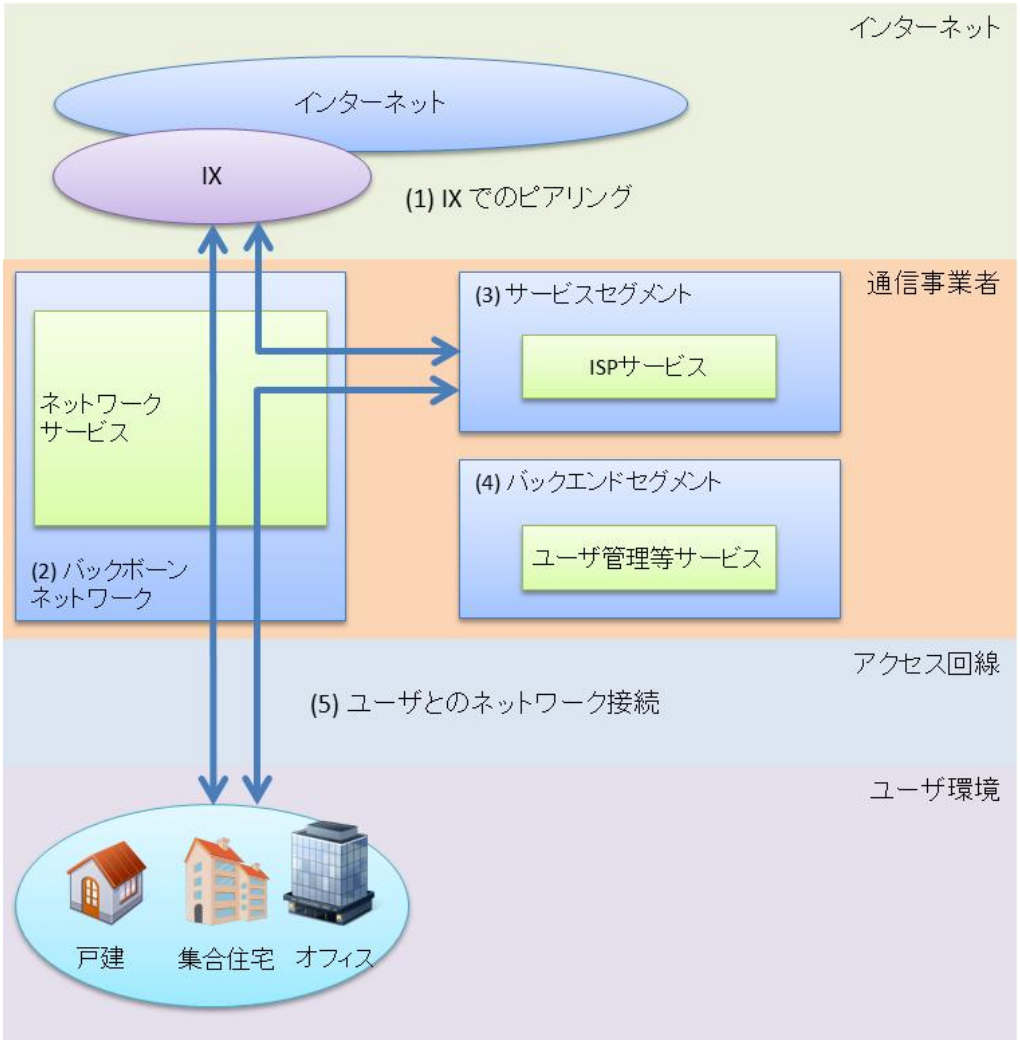


図 3-1　一次プロバイダにおけるシステム及びネットワークのモデル概念図

このモデルの場合、通信事業者は自身の AS（Autonomous System、用語集項番 19）に関する経路広告（用語集項番 20）を行う必要がある。

### 3.2 二次プロバイダのモデル

以下に、上流の通信事業者（一次プロバイダ）を介してインターネットとのアクセスを行う二次プロバイダと呼ばれる中小通信事業者の、システムやネットワークのモデル概念図を示す。

このモデルは以下の要素から構成される。

（1） 一次プロバイダとのトランジット接続を持ち、インターネットへのアクセスは、この一次プロバイダのネットワーク上を経由する。

（2） 主にユーザとインターネット間のトラフィックを中継するためのバックボーンネットワークを持つ。

（3） ISP サービスの基盤として、インターネット及びアクセス回線経由でユーザがアクセス可能なサービスセグメントを持つ。

（4） ユーザ管理等のバックエンドサービスを配置するバックエンドセグメントを持つ。

（5） ユーザとの間にアクセス回線経由でのネットワーク接続を持ち、ユーザとインターネット間のトラフィックを自社のバックボーンネットワーク上で流通させる。

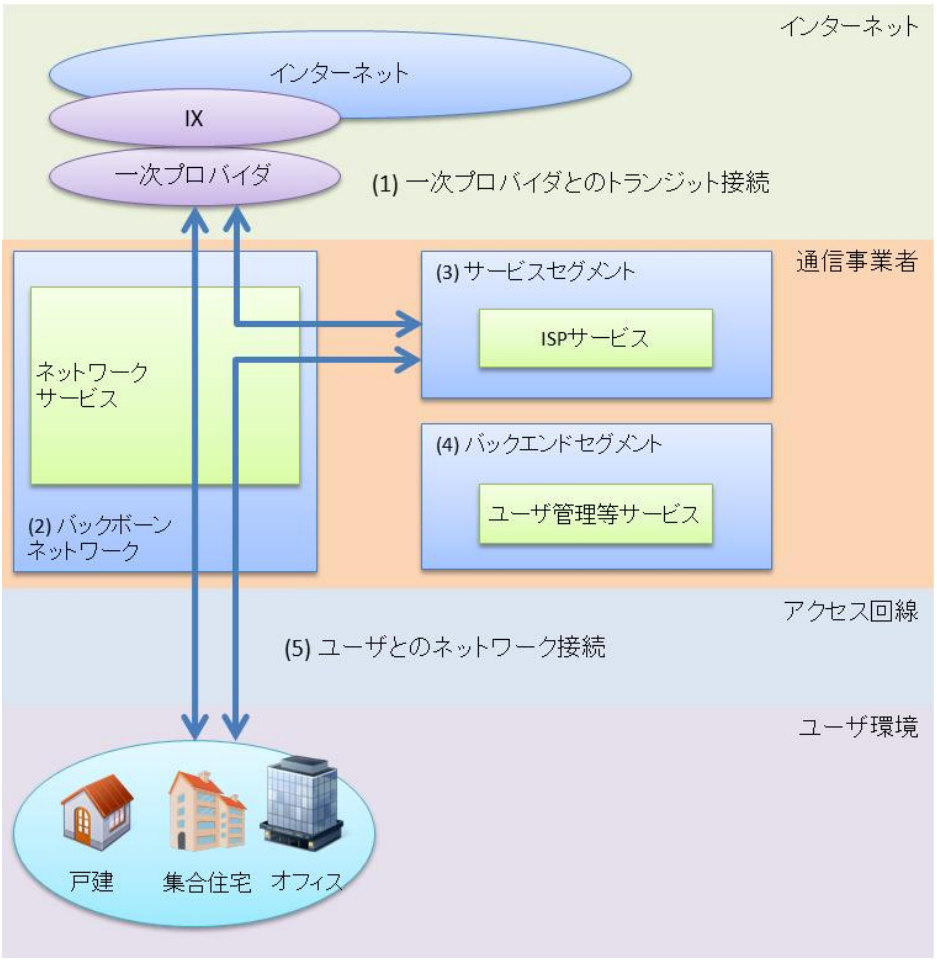


図 3-2　二次プロバイダのシステム及びネットワークのモデル概念図

このモデルの場合、中小通信事業者自身の AS に関する経路広告については一次プロバイダに依頼する。

### 3.3 ローミングサービスを利用する通信事業者のモデル

以下に、他通信事業者のローミングサービスを利用する中小通信事業者のシステムやネットワークのモデル概念図を示す。なお、ローミングサービスを提供する他通信事業者のことをローミングプロバイダという。このモデルは以下の要素から構成される。

(1) 一次プロバイダとのトランジット接続を持ち、サービスセグメントからインターネットへのアクセスは、この一次プロバイダとのネットワーク上を経由する。

(2) 主にサービスセグメントとインターネット間のトラフィックを中継するためのバックボーンネットワークを持つ。

(3) ISP サービスの基盤として、インターネットからアクセス可能なサービスセグメントを持つ。

(4) ユーザ管理等のバックエンドサービスを配置するバックエンドセグメントを持つ。

(5) ユーザとインターネット間のトラフィックは、他通信事業者のローミングサービスを利用して流通させる。

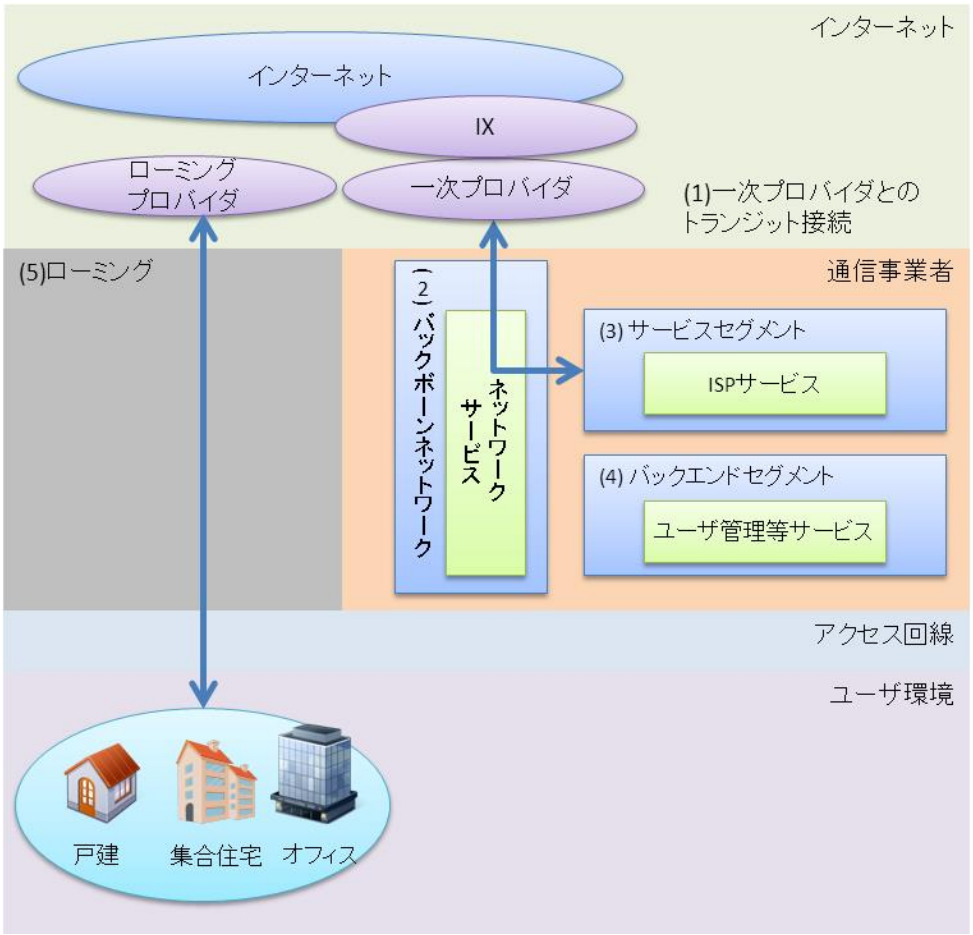


図 3-3 ローミングサービスを利用する通信事業者の
システム及びネットワークのモデル概念図

このモデルでは、アクセス回線を含めたユーザへのインターネットアクセス提供については、他通信事業者に委託する。また、中小通信事業者自身の AS に関する経路広告については一次プロバイダに依頼する。

### 3.4 CATV 事業における通信事業者のモデル

以下に、CATV 事業を行っている中小通信事業者のシステムやネットワークのモデル概念図を示す。このモデルは以下の要素から構成される。

（1） 一次プロバイダとのトランジット接続を持ち、インターネットへのアクセスは、この一次プロバイダとのネットワーク上を経由する。

（2） 主にユーザとインターネット間のトラフィックを中継するためのバックボーンネットワークを持つ。

（3） ISP サービスの基盤として、インターネット及びアクセス回線経由でユーザからアクセス可能なサービスセグメントを持つ。

（4） ユーザ管理等のバックエンドサービスを配置するバックエンドセグメントを持つ。

（5） ユーザとの間にアクセス回線（CATV 網）経由でのネットワーク接続を持ち、ユーザとインターネット間のトラフィックを自社のバックボーンネットワーク上で流通させる。

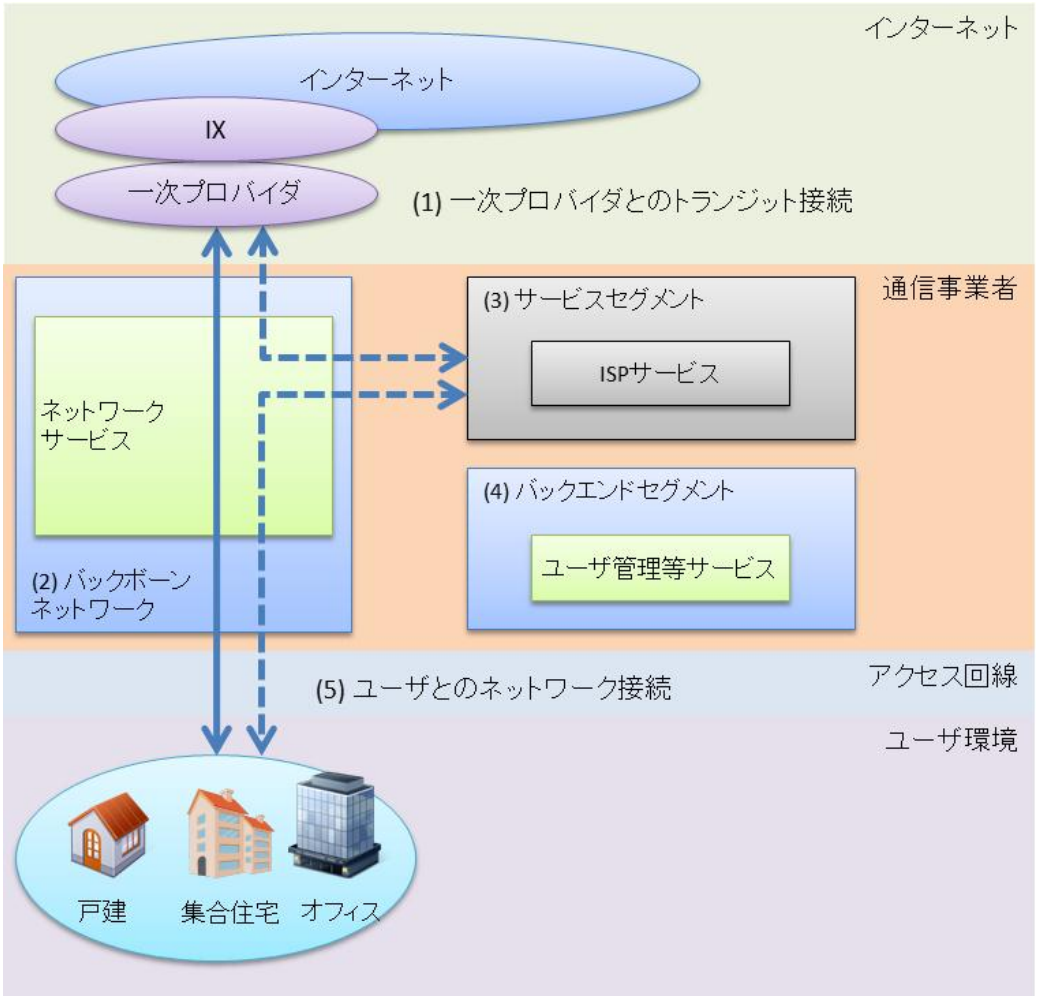


図 3-4　CATV 事業における通信事業者のシステム及びネットワークのモデル概念図

なお、CATV 事業者においては(3)サービスセグメントを自社で保有せず、一次プロバイダに委託しているケースもある。

### 3.5 IPv6 対応モデル

本ガイドラインでは、二次プロバイダのモデルが他モデルの構成要素を包含していることから、このモデルを基本パターンとして説明する。

# 4. IPv6 対応に向けた基本計画づくり

「3 想定するシステム及びネットワークのモデル」に示した中小通信事業者における典型的なシステムやネットワークのモデルに対して、モデルの構成要素ごとに IPv6 対応に向けた実行シナリオを想定する。

## 4.1 IPv6 対応に向けたシナリオ

以下に、図 3-2 を構成する 5 種類の要素のそれぞれにおける IPv6 対応のシナリオを示す。最後に、これら 5 種類の要素における IPv6 対応のシナリオを組み合わせ、中小通信事業者における IPv6 対応の基本的なシナリオを設定する。

### 4.1.1 一次プロバイダとのトランジット接続

中小通信事業者（二次プロバイダ）の保有するネットワーク設備とインターネットの間を中継するサービスをトランジット接続サービスと呼ぶ（図 4-1）。

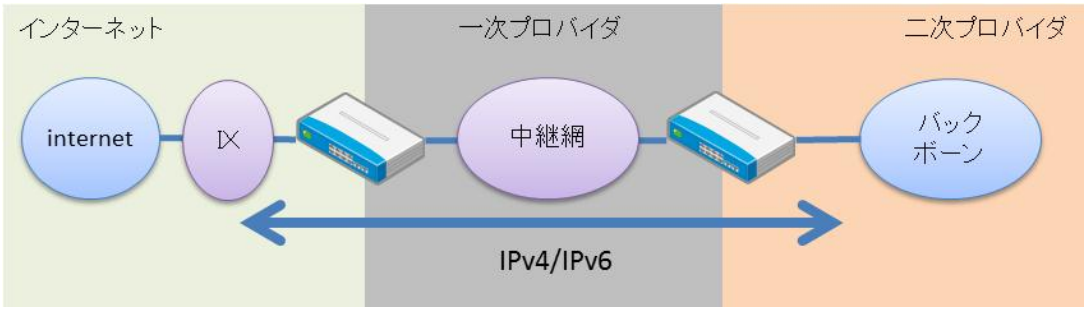


図 4-1　一次プロバイダとのトランジット接続

トランジット接続を用いた IPv6 対応については、以下の 2 種類のシナリオが想定される。

（1）　IPv6 接続サービス
（2）　IPv4/IPv6 デュアル接続サービス

IPv6 接続サービスは、IPv6 のみを中継するサービスである。既存のトランジット接続に影響を与えずに IPv6 接続を追加したい場合や、IPv4 は IX との直接接続を行っているが IPv6 はトランジット接続サービスで対応している場合など、IPv4 と IPv6 を別々に処理する場合に向いている。

IPv4/IPv6 デュアル接続サービスは、1 つのアクセス回線上で IPv4 及び IPv6 の双方を中継するサービスである。既存の IPv4 のトランジット接続を構成するルータに IPv6 接続も同時に収容したい場合に向いている。

### 4.1.2 ユーザトラフィック中継のためのバックボーンネットワーク

ユーザトラフィック中継のためのバックボーンネットワークは、中小通信事業者内のネットワーク設備で構成され、ユーザからのトラフィックの経路であるアクセス回線との接続点、インターネットへの接点となる一次プロバイダとの接続点、ISP サービスを提供するサービスセグメントとの接続点等を含む（図 4-2）。

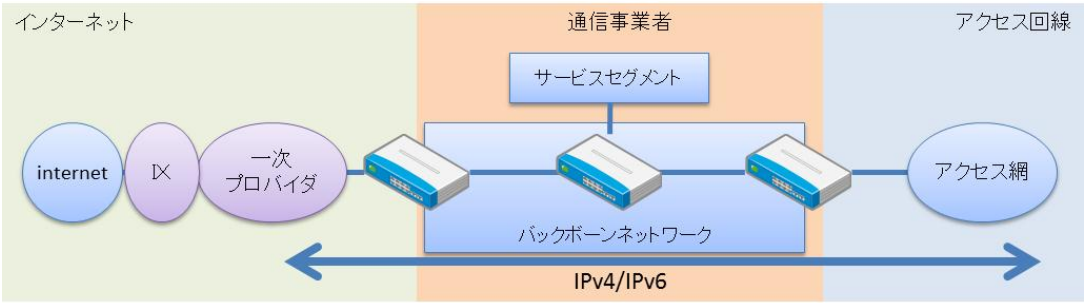


図 4-2　中小通信事業者のバックボーンネットワーク

バックボーンネットワークの IPv6 対応については、以下の 2 種類のシナリオが想定される。

（1）　通信機器のデュアルスタック（用語集項番 21）化
（2）　IPv4 対応機器に IPv6 対応機器を追加するパラレルスタック化

通信機器のデュアルスタック化においては、バックボーンネットワークを構成するルータ、L3 スイッチ（用語集項番 22）等、すべての通信機器を IPv4/IPv6 双方に対応するよう更新する。

IPv4 対応機器に IPv6 対応機器を追加するパラレルスタック化においては、IPv4 トラフィックを中継するネットワーク機器に加え、IPv6 トラフィックを中継するネットワーク機器を追加する。ただし、アクセス回線及び一次プロバイダとの接続が IPv4/IPv6 デュアル構成である場合、接続点となるルータは IPv4/IPv6 デュアルスタック対応とし、以降の IPv4 バックボーン（図 4-3 の赤点線）、IPv6 バックボーン（図 4-3 の青点線）に対してトラフィックの振り分け及び集約を行う構成とする（図 4-3）。

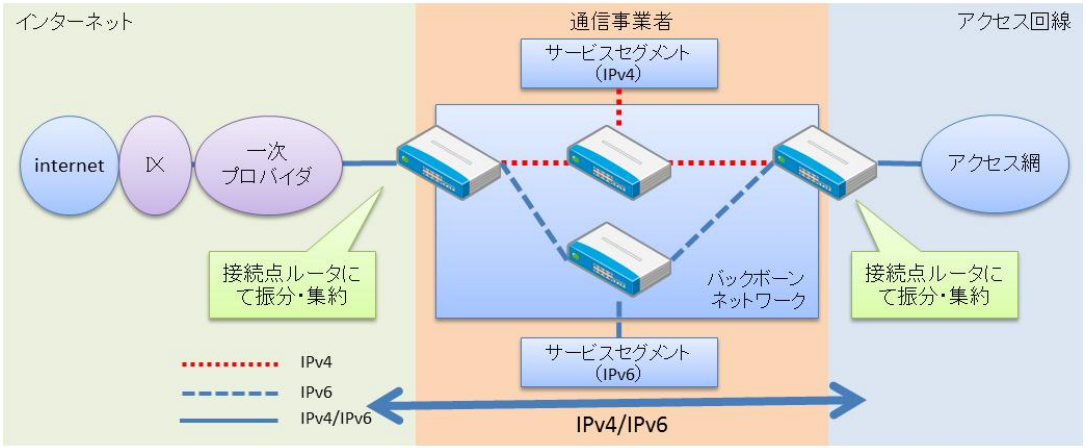


図 4-3　中小通信事業者のバックボーンネットワーク（パラレルスタック）

先に示したように、一次プロバイダとのトランジット接続において、IPv6 接続サービスを導入し、接続点を IPv4 及び IPv6 で独立としている場合には、バックボーンネットワーク全体を別構成とすることができる。

### 4.1.3 ISP サービスのためのサービスセグメント

中小通信事業者の ISP サービス（ポータルサイト、ユーザが利用する電子メールサービス、ウェブホスティング、DNS サービス等）を配置するサービスセグメントの IPv6 対応については、以下の 3 種類のシナリオが想定される。

（1） サービス提供機器のデュアルスタック化
（2） IPv4 対応機器に IPv6 対応機器を追加するパラレルスタック化
（3） トランスレータによる IPv6 対応化

サービス提供機器のデュアルスタック化においては、サービスを提供するサーバ機器等（ロードバランサー、SSL（用語集項番 23）アクセラレータを含む）及びサービスセグメントを構成するネットワーク機器等を IPv4/IPv6 双方に対応するように変更する。ネットワーク機器等については、バックボーンネットワークと同様に、全ての機器を同時期に IPv6 対応する必要がある。サーバ機器等については、一部のサービス（DNS サービス、メールサービス等）を先行的に IPv6 対応し、他のサービス（ホスティングサービス等）は IPv6 対応の時期を遅らせるといった、IPv6 への部分的な移行も可能である。

IPv4 対応機器に IPv6 対応機器を追加するパラレルスタック化においては、IPv4 でサービスを提供する機器に加え、IPv6 でサービスを提供する機器を追加するシナリオとなる。この場合も、サービスごとに IPv6 対応の時期を分けて移行することが可能である。

トランスレータによる IPv6 対応化においては、サービス提供機器自身で IPv6 対応を行わずとも、トランスレータ（IPv4 トラフィックと IPv6 トラフィックの相互変換を提供する機器）を導入することで IPv6 対応を実現することができる。なお、トランスレータの導入に際しては、サービスセグメントへの全トラフィックトランスレータを通過することから、このような場合でもトランスレータ導入による十分な性能が得られることを検証する必要がある。

### 4.1.4 バックエンドセグメント

ユーザとインターネット間のトラフィック中継や ISP サービス等に直接関与しない業務系システム（ユーザ管理システム、課金システム、ログ監視システム、監視システム等）をバックエンドサービスと呼ぶ。バックエンドサービスを収容するバックエンドセグメントについても、バックボーンネットワークに接続されると考えられる。

バックエンドセグメントについては、主なアクセスが中小通信事業者自身であることから、IPv4 での運用を当面維持することも現実的な選択といえる。ただし、IPv6 利用申請の有無、IPv6 利用状況、割り当てられた IPv6 プレフィックス（用語集項番 24）情報等のユーザの IPv6 関連情報は、ユーザからの問い合わせ対応や課金対応のために必要となるため、バックエンドサービスのうちユーザ管理システムや課金システムについては、IPv6 関連情報を取り扱うことができるよう更新する必要がある。

なお、バックエンドセグメントを IPv4 で運用とした場合でも、IPv6 に対応する ISP サービスやバックボーンネットワークに対する IPv6 の監視が必要となることから、監視システムについては IPv6 対応が必要である。このため、監視システムについてはバックエンドセグメントからサービスセグメントに移動したり、バックエンドセグメントの一部を IPv6 対応して監視システムを配置したりするなどの工夫が必要となる。

バックエンドセグメントを IPv6 対応する場合には、以下の 3 種類のシナリオが想定される。

（1） サービス提供機器のデュアルスタック化
（2） IPv4 対応機器に IPv6 対応機器を追加するパラレルスタック化
（3） トランスレータによる IPv6 対応化

サービス提供機器のデュアルスタック化においては、サービスセグメントと同様に、サービスを提供するサーバ機器等及びサービスセグメントを構成するネットワーク機器等を IPv4/IPv6 双方に対応するよう変更する。サービスセグメントと同様に、サービス提供機器については部分的な移行が可能である。

IPv4 対応機器に IPv6 対応機器を追加するパラレルスタック化及びトランスレータによる IPv6 対応化ついても、サービスセグメントと同様の対応となる。

### 4.1.5 ユーザとのネットワーク接続

ユーザとのネットワーク接続については様々なアクセス回線が利用されている。ここでは、代表的なアクセス回線を取り上げて、それぞれの IPv6 対応方法について説明する。

#### (1) NGN をアクセス回線とする場合

NTT 東日本及び NTT 西日本が展開する次世代ネットワーク網 NGN（用語集項番 25）をアクセス回線とする場合、ユーザからインターネットまでの経路を IPv6 対応とするネイティブ方式、アクセス回線の IPv6 ネットワーク上に別の通信事業者の IPv6 アドレスを持つ IPv6 ネットワークを設置するトンネル方式のいずれかを選択する。

ネイティブ方式では、NTT 東日本及び NTT 西日本が選定した接続事業者（VNE、用語集項番 26）と呼ばれる通信事業者が、ユーザとインターネット間の IPv6 トラフィックを中継する役割を持つ（図 4-4）。

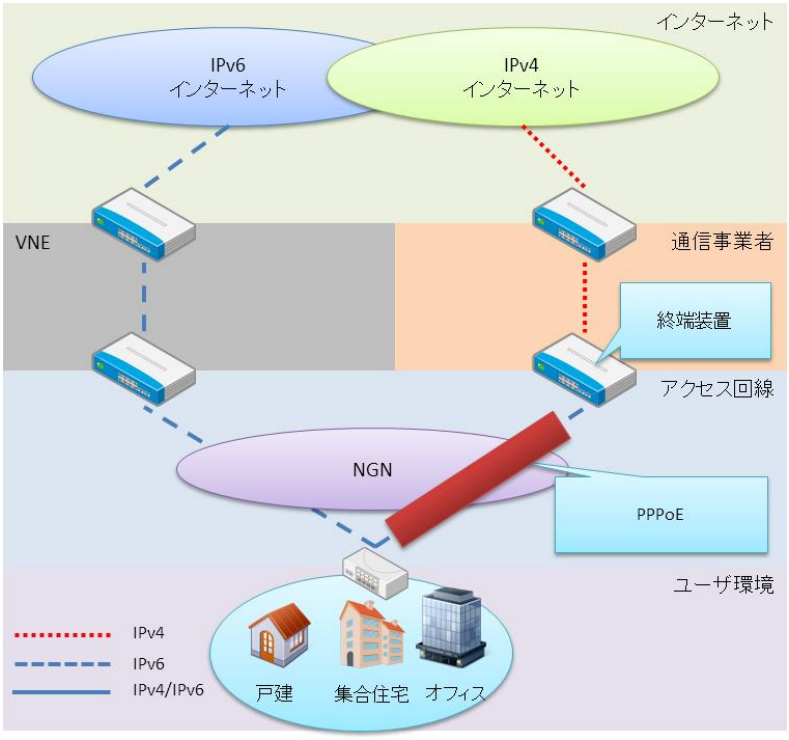


図 4-4 NGN におけるネイティブ方式

VNE としては、NTT 東日本及び NTT 西日本に選定された BBIX 株式会社、日本ネットワークイネイブラー株式会社及びインターネットマルチフィード株式会社の 3 社から選択することができる。ユーザからの IPv4 トラフィックについては、従来通り、PPPoE（用語集項番 27）を経由して中小通信事業者の設備に接続され、インターネット上の IPv4 サービスにアクセスを行う。

トンネル方式では、IPv4 トラフィックと同様に IPv6 トラフィックも PPPoE トンネルを経由して中小通信事業者に収容される。この際、それぞれの PPPoE セッションは別々に設置されることになる。また、トンネルの終端装置も別々になり、NGN 上に設置される集約用接続装置において IPv4 接続と IPv6 接続がまとめられる（図 4-5）。

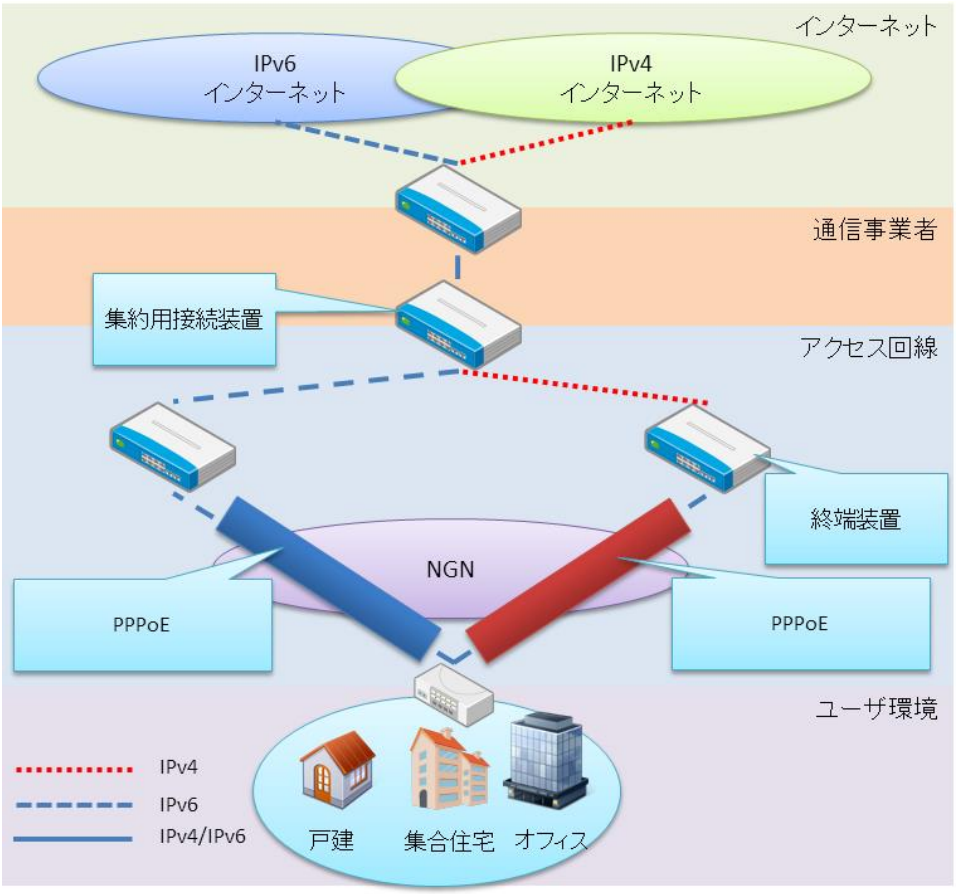


図 4-5　NGN におけるトンネル方式

トンネル方式の場合、ユーザ側に PPPoE トンネルを終端するための IPv6 トンネル対応アダプタが必要となる。

ネイティブ方式とトンネル方式における違いについて表 4-1 にまとめる。

表 4-1　NGN IPv6 対応方式の違い

| | ネイティブ方式 | トンネル方式 |
|---|---|---|
| **ユーザの申し込み** | 通信事業者への IPv6 利用申請に加え、NTT 東日本及び NTT 西日本への「フレッツ・v6 オプション」申請が必要（今後不要になる見込み） | 通信事業者への IPv6 利用申請が必要 |
| **ユーザ割り当てアドレス** | 接続事業者（VNE）保有のアドレスから割り当て | 通信事業者（ISP）保有のアドレスから割り当て |
| **PPPoE アカウント** | 特になし | IPv6 用のアカウントを追加 |
| **機器の追加** | 特になし | IPv6 対応トンネルアダプタが必要 |

ネイティブ方式とトンネル方式には、この他にも細かな技術的な違いがある。その違いがネットワーク設計やサービスに影響する可能性があるので、事前に十分な調査を行う必要がある。また、ユーザの IPv6 インターネットアクセスに関して、ネイティブ方式の場合は接続事業者、トンネル方式の場合は中小通信事業者がそれぞれ対応することになる。特にトンネル方式を利用する場合には、中小通信事業者の技術者に対する IPv6 運用技術の教育を十分に行う必要がある。

### (2) 地域 IP 網等をアクセス回線とする場合

NTT 東日本及び NTT 西日本が全国に設置する地域 IP 網や通信事業者の独自中継網サービスを用いたネットワーク（B フレッツ、ADSL 等を含む）をアクセス回線とする場合、これらのネットワークは IPv4 のみの対応（フレッツ光プレミアムは IPv6 対応）であるため、中小通信事業者は独自の工夫により IPv6 対応を行う必要がある。方式としては、IPv6 トラフィックを IPv4 ネットワーク上で中継するトンネル方式が適用可能である。トンネル方式の場合には、NGN と同じく、ユーザ側に IPv6 トンネルを終端する装置が必要となり、中小通信事業者側のトンネル終端は事業者自身で行う必要がある（図 4-6）。

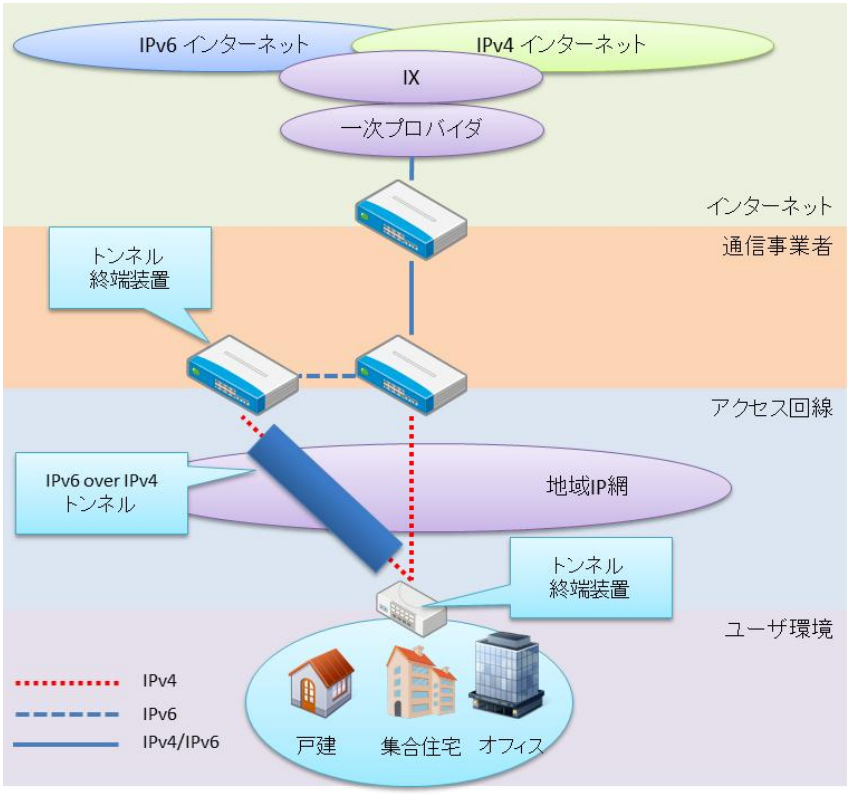


図 4-6　地域 IP 網上におけるトンネル方式

図 4-6 では、ユーザ側のホームゲートウェイ（用語集項番 28）が IPv6 のトンネル終端装置を兼用するイメージを示している。

### (3) 専用回線をアクセス回線とする場合

一部の法人ユーザのように、中小通信事業者との間を専用回線で接続している場合がある。この場合、IPv6 インターネット接続サービスとして、デュアルスタック接続（既存 IPv4 インターネット接続からの移行又は新規提供を想定）、あるいはトンネル接続（既存 IPv4 インターネット接続のオプションを想定）等を提供する。デュアルスタック接続においては、バックボーン側の収容ルータをデュアルスタック対応とする。トンネル接続においては、ユーザ側及び中小通信事業者側の双方に IPv6 トンネル終端装置を導入する。

## 4.2 IPv6 対応の基本シナリオ

前節までに、中小通信事業者において想定される IPv6 対応のシナリオを、典型的な中小通信事業者のシステムやネットワークのモデルを構成する 5 種類の要素ごとに示した。本ガイドラインでは、次の組み合わせを基本シナリオとする。

表 4-2　本ガイドラインで想定する IPv6 対応のシナリオ

| 構成要素 | IPv6 対応のシナリオ |
|---|---|
| **上流通信事業者とのトランジット接続** | IPv4/IPv6 デュアル接続サービス |
| **バックボーンネットワーク** | 通信機器のデュアルスタック化 |
| **サービスセグメント** | サービス提供機器のデュアルスタック化 |
| **バックエンドセグメント** | IPv6 対応しない（IPv4 を維持）<br>又は<br>サービス提供機器のデュアルスタック化 |
| **ユーザとのネットワーク接続** | NGN をアクセス回線とするネイティブ方式<br>又は<br>NGN をアクセス回線とするトンネル方式 |

バックエンドセグメントについては、ユーザ管理システムや課金システムのような IPv6 対応が必須ではないものもあるが、監視システムのように IPv6 対応が必要なものもあるため、部分的にデュアルスタック化で対応するシナリオとする。

ユーザとのネットワーク接続については、ネイティブ方式とトンネル方式のいずれも採用する中小通信事業者があることから、双方を基本シナリオとする。

# 5. IP アドレス設計時の IPv6 対応方法

本章では、IPv6 対応に向けた必須の知識である IPv6 アドレスの概要として、IPv6 アドレスの種類、構造及び調達方法を紹介し、IPv6 アドレスを割り当てる際の留意点についても説明する。

## 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）。

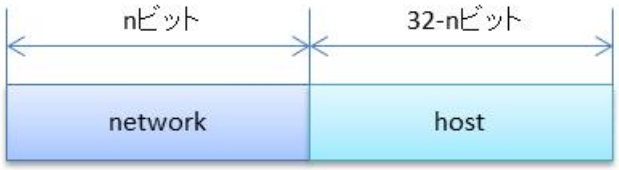


図 5-1　IPv4 アドレスの構造

### 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「:」で連結した表記とする。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。

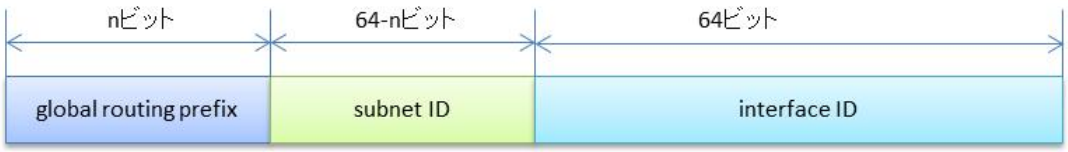


図 5-2　IPv6 グローバルユニキャストアドレスの構造

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。

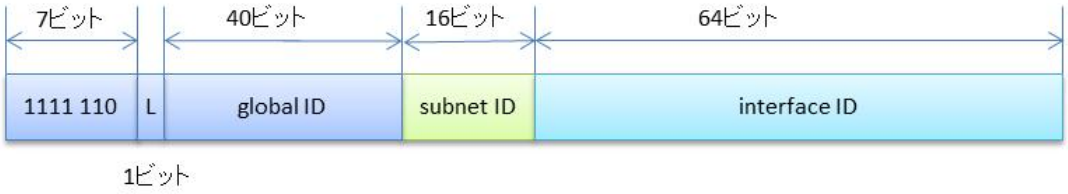


図 5-3　ユニークローカル IPv6 ユニキャストアドレスの構造

### 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 29）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な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 30）から通信事業者に割り振りがされ、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）。

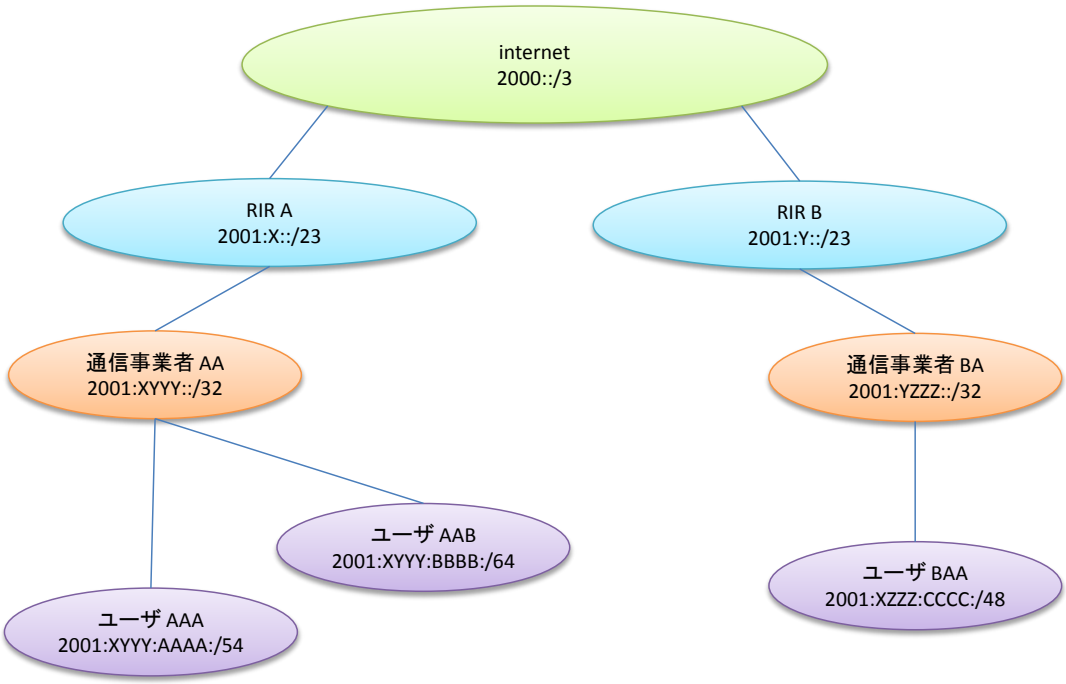


図 5-4　グローバルユニキャストアドレスの割り振りの例

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。）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）。

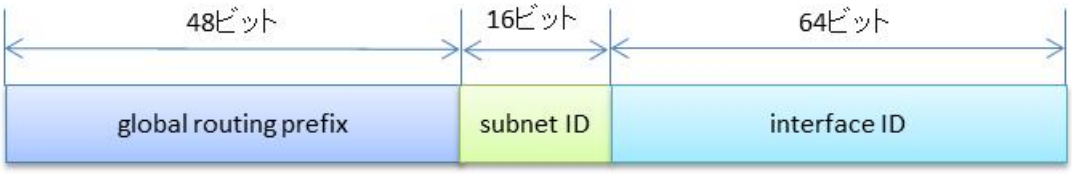


図 5-5　ユーザに割り当てられるグローバルユニキャストアドレスの構造（/48 の場合）

### 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 アドレスの割り当てを受ける際には、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。

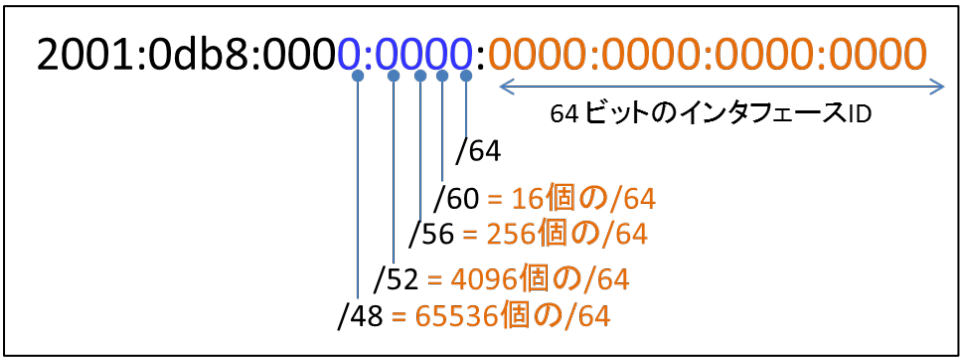


図 5-6　/48 アドレスに収容可能な/64 ネットワーク

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）。

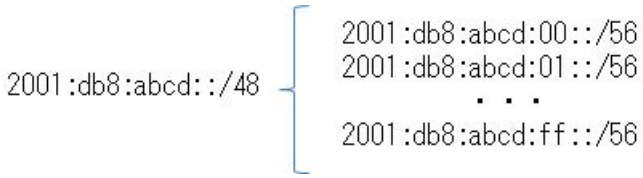


図 5-7　/48 アドレスに収容可能な/56 プレフィックス

/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）。

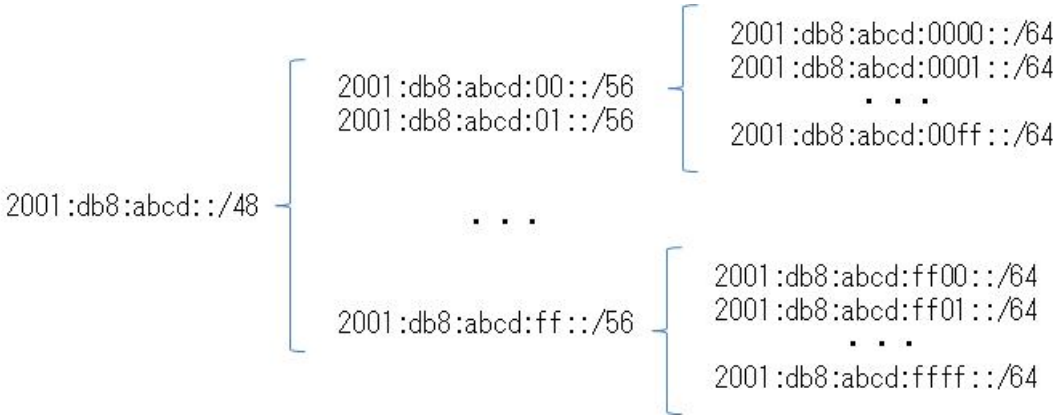


図 5-8　階層的なネットワーク構成

### 5.1.8 IPv6 アドレスの調達

IPv6 アドレスを調達する場合、日本国内における IPv6 アドレスの割り振りについては、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 31）の「IPv6 アドレスに関する申請手続きについて」（https://www.nic.ad.jp/doc/jpnic-01140.html）に従い申請手続きを行う。

なお IPv6 アドレスの初期割振りを受けるためには「JPNIC における IPv6 アドレス割り振り及び割り当てポリシー」（https://www.nic.ad.jp/doc/jpnic-01167.html）の「初期割り振り及び割り当て基準」に示される諸条件を満たす必要がある。

初期割振りサイズは/32 とされているが、「最小サイズを超える初期割り振り」に示される条件を満たすことができれば、より大きなサイズを要求することができる。

## 5.2 通信事業者における IPv6 アドレスの設計に関する留意点

中小通信事業者のシステムやネットワークを IPv6 対応する上で、IPv6 アドレスに関して留意すべき事項について説明する。

### 5.2.1 ネットワークセグメントの切り分け

上流通信事業者（一次プロバイダ）との接続から、バックボーンネットワーク、サービスセグメントについてデュアルスタックとして IPv6 対応を進める場合、IPv4 と IPv6 とで共通

したルータ及び L3 スイッチを用いることになる。IPv4 と IPv6 の設定上の混乱を避けるため、サブネットワークのプレフィックスサイズを統一する、又は IPv6 アドレスの集約上の上位ネットワークと下位ネットワークの関係を同じようにするなど、各セグメント内のサブネットワーク構成については同じような管理体系保つことが望ましい。

バックボーンネットワーク、サービスセグメントについてパラレルスタックとして IPv6 対応を進める場合には、ルータ及び L3 スイッチといったネットワークセグメント境界に設置する機器及びサービス用のサーバ機器等を IPv4 用の機器と別にすることができるので、ネットワークセグメント構成を異なるものにすることも可能である。

### 5.2.2 各セグメントにおけるアドレスサイズの考え方

中小通信事業者への割り振りとして /32 のプレフィックスを保有すると想定する。/32 のプレフィックスでは、/48 のプレフィックスを 65,536 個、/56 であれば約 1,678 万個を収容可能である。

この/32 の IPv6 アドレスを、サービスセグメントに割り当てるプレフィックス、バックエンドセグメントに割り当てるプレフィックス、ユーザに割り当てるプレフィックス等、必要なセグメントに分割する。

サービスセグメントにて、多数のグローバルアドレスを必要とするウェブホスティングやレンタルサーバ等のサービスを提供している場合には、将来にわたる提供予定サーバ数を算出し、サーバあたりの割り当てアドレス数を乗じて、必要なアドレスサイズを算出する。

電子メールサービスや DNS サービスなどは、それほど多くのアドレスを必要とすることはないため、/64 のプレフィックスをいくつか、又は /56 のプレフィックスを 1 つ確保する程度で十分と考えられる。

次にバックエンドセグメントを IPv6 対応する場合を想定する。セグメント内を多くの/64 に分けて運用及び管理する必要はあまりないが、扱う情報のセキュリティレベルに応じて、ネットワーク境界にセキュリティ機能を配置できるよう、細かくセグメントを分けることも考えられる。例としては、/56 のプレフィックスを 1 つ確保し、ユーザ情報、課金情報及びサーバ監視ログを扱うサーバ等の役割ごとに/64 のプレフィックスを割り当てるといった方針をあげることができる。

中小通信事業者の提供する ISP サービスの種類や規模次第であるが、サービスセグメント、バックエンドセグメントに必要なアドレスサイズを差し引いたとしても、/32 の多くはユーザに割り当てるプレフィックスとして利用可能と考えられる。仮に /32 をすべてユーザに対して割り当てるプレフィックスとした場合、/48 のプレフィックスが約 6 万 6 千個、/56 のプレフィックスが約 1,678 万個、/64 のプレフィックスが約 43 億個（IPv4 の全空間と同じ）提供可能である。

ユーザに割り当てるアドレス空間については、既存の IPv4 ユーザが全て IPv6 を利用すると想定し、将来的な変動を含めてアドレス割り当て対象となるユーザ数を算出する。そして、ユーザ数にアドレスサイズを乗じたアドレス空間がユーザに割り当て可能なアドレス空間に収まるよう、確保しておくアドレス空間の大きさを調整する。

なお、/48 以上の大きさを持つアドレスを割り当てたユーザについては、そのユーザの情報について JPNIC のデータベースに登録することが求められている。

### 5.2.3 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低減するとともに、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. ユーザに提供するインターネット接続部設計時の 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、一次プロバイダとのトランジット接続とバックボーンネットワーク（ユーザの IPv6 トラフィックをインターネットに流通させるための経路）を含めた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等の機能の範囲と、それら機能の IPv6 対応の方法について説明する。

## 6.1 ユーザに提供するインターネット接続に関わる基本アーキテクチャ

以下に、中小通信事業者（二次プロバイダ）がユーザに提供するインターネット接続の基本的アーキテクチャを示す。インターネットとの接続には一次プロバイダのトランジット接続を利用し、中小通信事業者保有のバックボーンネットワークとアクセス回線を経由して、ユーザの保有する機器をインターネットに接続する（図 6-1 の赤点線部分）。

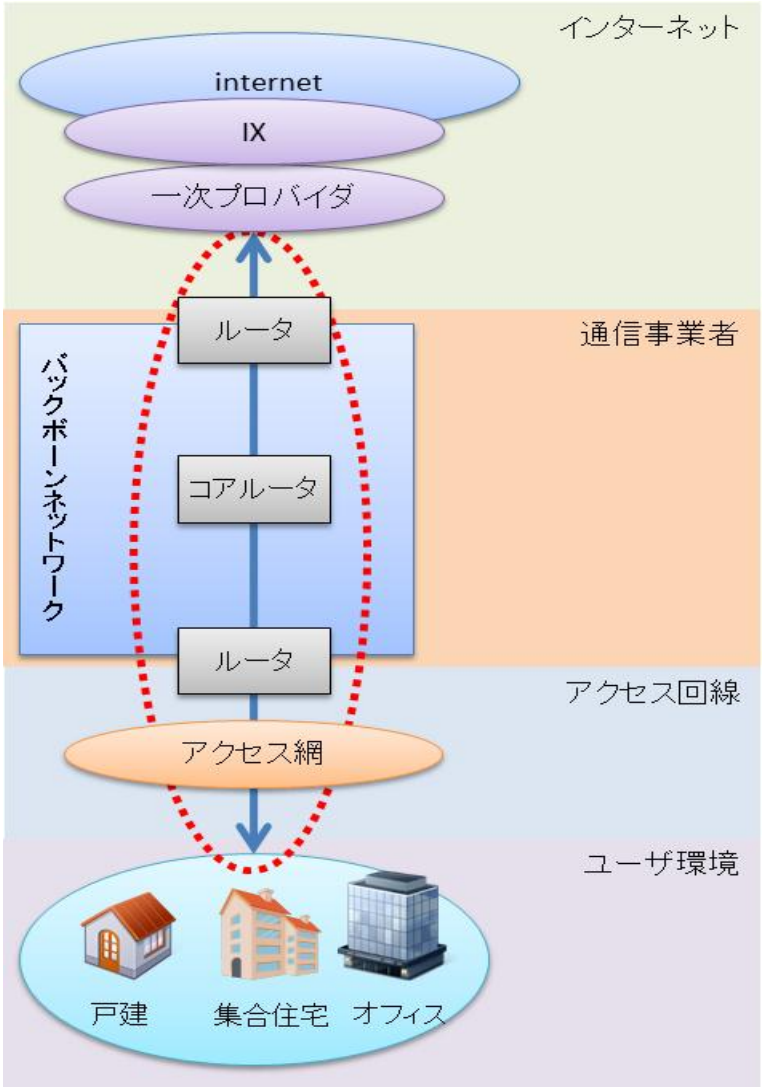


図 6-1　中小通信事業者がユーザに提供するインターネット接続の基本的アーキテクチャ

なお図 6-1 では、サービスセグメント、バックエンドセグメントについては示していない。それらセグメント上の機器に関しては次章にて説明する。

## 6.2 IPv6 対応すべき機能

前節で示した基本的アーキテクチャにおける IPv6 対応すべき機器やサービスとして、以下の構成要素が想定される。

インターネットとの接続点となる一次プロバイダのトランジット接続を収容するルータ、バックボーンネットワークを構成するコアルータ、アクセス回線との接続点となるルータの IPv6 対応が必要である。ルータと同様の機能を持つ L3 スイッチについても同様である。

イーサネット集約のために設置される L2 スイッチ（用語集項番 32）については、通信を転送する機能として IP レイヤーでの処理を行うものではないが、機器の管理及び監視については IP 通信を利用するものが多い。そのため、管理及び監視を IPv6 対応する際には、L2 スイッチについても IPv6 対応が必要である。

一次プロバイダとの接続点に用いるルータについては、その接続の形態に応じて必要となるルーティングプロトコル（BGP、 OSPF 等）の IPv6 対応が必要となる。

### 6.2.1 NGN をアクセス回線とするネイティブ方式を採用する場合

ユーザのアクセス回線を、NTT 東日本及び NTT 西日本が提供する NGN としてネイティブ方式による IPv6 対応を行う場合、ユーザとインターネット間の接続は、両事業者が承認する接続事業者の設備を経由する方式となる（図 4-4）。

この接続方式においては、ユーザの IPv6 トラフィックが中小通信事業者の設備を経由することが無いので、ユーザに提供するインターネット接続に関して IPv6 対応すべき機器やサービスは存在しない。ただし、バックエンドサービス（ユーザ管理システム、課金システム等）では、ユーザ対応のために、ユーザの IPv6 関連情報（IPv6 利用申請の有無、IPv6 利用状況、割り当てられた IPv6 プレフィックス情報等）を取り扱うことができるように更新する必要がある。

### 6.2.2 NGN をアクセス回線とするトンネル方式を採用する場合

ユーザのアクセス回線を、NTT 東日本及び NTT 西日本が提供する NGN を用いたトンネル方式によって IPv6 対応を行う場合、IPv6 対応が必要となる機器やサービスについて以下に示す。

#### (1) 認証サーバ

NGN をアクセス回線とするトンネル方式を採用した場合、ユーザ認証時に IPv6 アドレスを払い出す必要がある。このため、中小通信事業者の認証サーバを IPv6 アドレス払い出しに対応させる必要がある。

#### (2) トンネルアダプタ

NGN をアクセス回線とするトンネル方式を採用した場合、IPv6 トラフィック用の PPPoE トンネルを終端するための装置として、IPv6 対応トンネルアダプタをユーザ環境に設置する必要がある（図 6-2）。

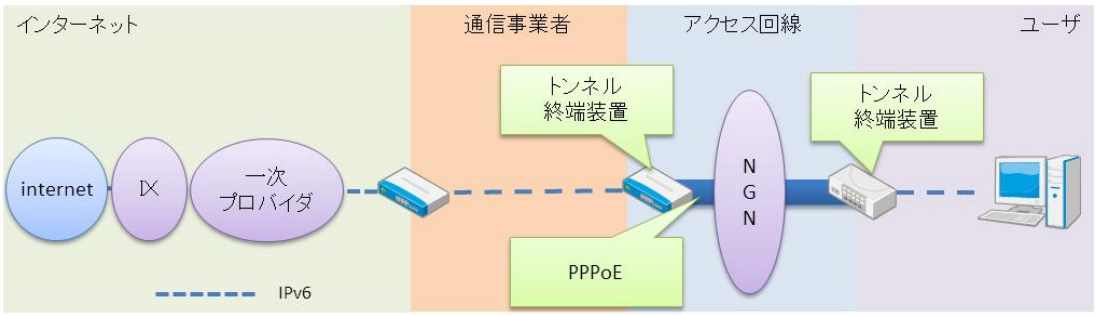


図 6-2　NGN トンネル方式の概要

この IPv6 対応トンネルアダプタについては、ユーザ負担による導入となるが、今後は、ホームゲートウェイに機能として追加される見通しである。

### 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、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) 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。なお、ユーザとの接続回線を収容するルータとバックボーンセグメントの中心に配置するコアルータでは、性能要件のほかにも、ユーザとの接続回線を収容するルータにはユーザの新規追加や設定変更等の構成変更をシステム的に行う機能が求められるなど、要件が異なる場合があることを考慮する必要がある。

- 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 33）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 34）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 35）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) 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。

(3) 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。

### 6.4 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 36）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

デュアルスタック構成での IPv6 対応の場合、IPv4 での通信に影響を与えずに IPv6 対応を行う必要がある。特に、本章での説明対象としている一次プロバイダとの接続点となるルータやアクセス網との接続点となるルータについては、他の事業者が使用する機器との相性が問題となるケースがあることから、検証済みの機器リスト、IPv6 対応にあたっての注意事項等を事業者から事前に入手し、機器調達、設定作業等に活用することが望ましい。

また、バックエンドセグメントについて IPv4 を当面維持する選択をした場合、バックエンドセグメント、サービスセグメント等との通信を IPv4 のみで行うことに支障が出ないよう、それらセグメントの IPv6 対応を進める必要がある。

## 7. ISP サービス及びバックエンドサービス設計時の 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、ISP サービス（中小通信事業者のポータルサイト、ユーザが利用する電子メールサービス、ウェブホスティング、DNS サービス等）及びバックエンドサービス（ユーザ管理システム、課金システム、ログ監視システム、サービス監視システム等）における IPv6 対応の方法について説明する。

### 7.1 ISP サービス及びバックエンドサービスに関わる基本的アーキテクチャ

以下に、中小通信事業者（二次プロバイダ）における ISP サービス、バックエンドサービスの基本的アーキテクチャを示す（図 7-1）。サービスセグメントは、ファイアウォール等のセキュリティサービス経由でコアルータに接続される。

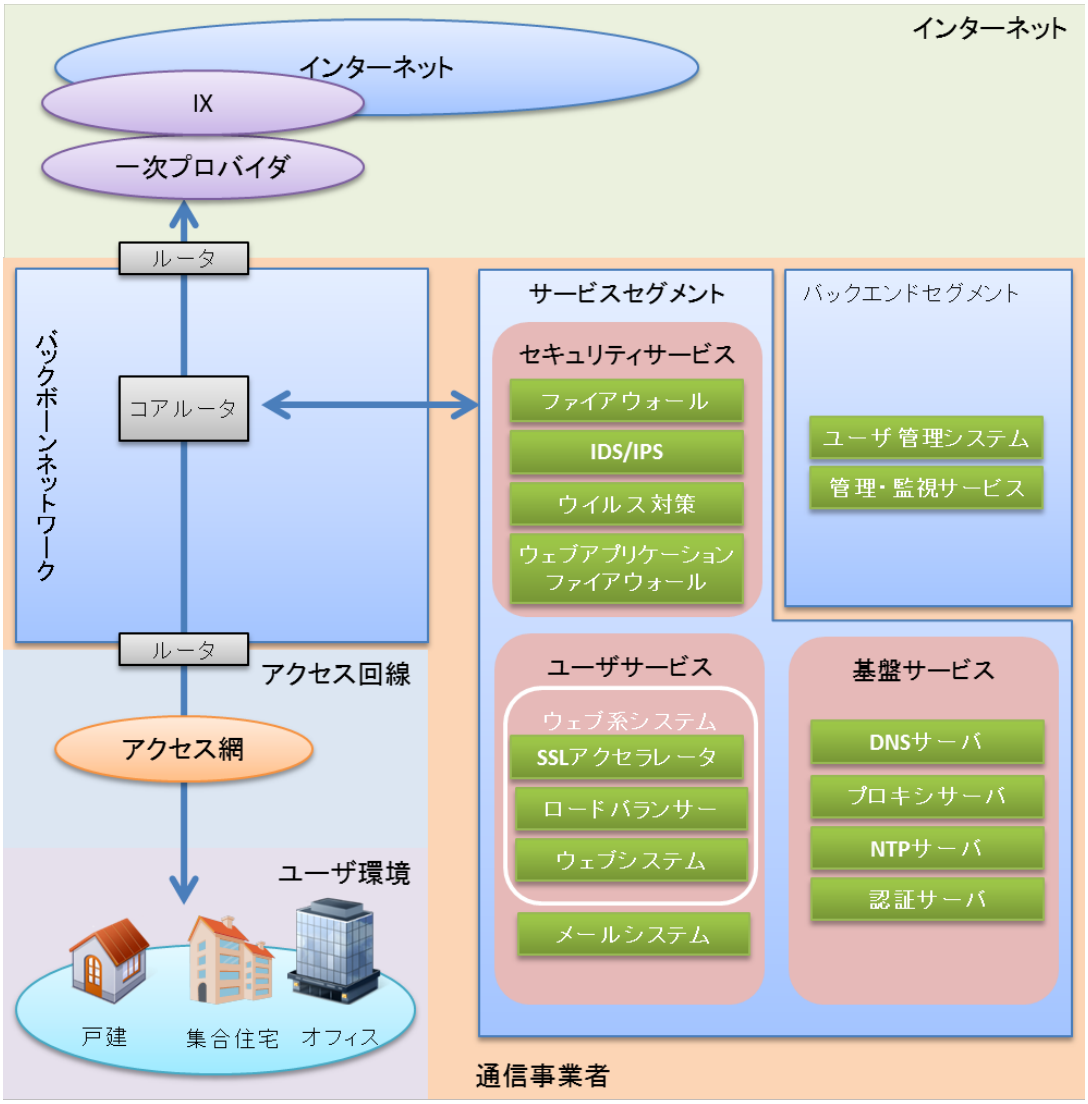


図 7-1　中小通信事業者の ISP サービス、バックエンドサービスの基本的アーキテクチャ

### 7.2 IPv6 対応すべき機能

中小通信事業者の ISP サービス及びバックエンドサービスにおいて、IPv6 対応すべき機器やサービスには、以下の構成要素が想定される。

#### 7.2.1 セグメント共通

(1) ルータ、スイッチ

バックボーンセグメントと、サービスセグメント（ISP サービスを配置）及びバックエンドセグメント（バックエンドサービスを配置）の境界に設置するルータや L3 スイッチ等について IPv6 対応の必要がある。

管理及び監視を IPv6 対応する際には、L2 スイッチについても IPv6 対応が必要である。

#### 7.2.2 ISP サービスセグメント：セキュリティサービス

(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、バックボーンセグメントとサービスセグメントの境界にはファイアウォールを配置して、不正な通信等を抑制する必要がある。IPv4 トラフィックに対する動作及び機能と同等の動作及び機能を、IPv6 トラフィックに対しても提供する必要がある。

ファイアウォール製品としては、電子メールやウェブトラフィック等のアプリケーションレイヤまで対応するアプリケーションファイアウォールも存在する。

(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 37）や IPS がある。

IDS 及び IPS は、インターネットと DMZ（用語集項番 38）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

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 39）は、ウェブアプリケーションで用いるプロトコルレベルにおいて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の悪用を防ぐために配置される。

### 7.2.3 ISP サービスセグメント：ユーザサービス

#### (1) ウェブシステム

中小通信事業者のポータルサイトや、ウェブホスティング、ブログサービス等ユーザ向けのサービスを提供するためのシステムは、HTTP（用語集項番 40）サーバ、CMS（コンテンツマネジメントシステム、用語集項番 41）、アクセスログ解析機能等から構成される。

通常ウェブシステムは、インターネットから直接アクセスできるようにするためサービスセグメント上に配置されるが、ロードバランサー等のリバースプロキシ（用語集項番 42）を介する場合には、サービスセグメントとは異なるセグメント上に配置することも可能である。

#### (2) メールシステム

中小通信事業者自身が利用するメールシステムとユーザが利用するメールシステムについて IPv6 対応が必要である。サーバとしては別々の機器で構成することが多いと思われるが、IPv6 対応に関する方法や要件については、ほぼ共通である。

#### (3) SSL アクセラレータ

ウェブシステムで HTTPS（用語集項番 43）接続を提供する場合、コンテンツの暗号化、コンテンツの改ざん検知及びサーバやクライアントの認証機能を提供するため、SSL（Secure Socket Layer）を使用することになる（SSL を標準化したプロトコルを TLS（Transport Layer Security、用語集項番 44）と呼ぶ）。一般に暗号処理はサーバに負荷をかけるため、大量の HTTPS 接続に対応する場合には、ハードウェアで暗号処理を行う SSL アクセラレータが必要となる。

#### (4) ロードバランサー

中小通信事業者のポータルサイトは、ユーザ会員に対する情報提供の窓口であるほか、非ユーザ会員からの情報照会の役割も担うことから、多くのアクセスが想定される。このような場合、ウェブシステムの負荷分散を行うため、ロードバランサー（負荷分散装置）を設置することがある。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として導入されることもある。

さらには、IPv4 上でのアクセスを IPv6 サービスに、反対に IPv6 上でのアクセスを IPv4 サービスにそれぞれ仲介するトランスレータ機能を合わせ持つロードバランサーも存在する。

### 7.2.4 ISP サービスセグメント：基盤サービス

サービスセグメント上の各機器やサービスの稼動のために、基盤サービスとして、DNS サーバ、プロキシ（用語集項番 45）サーバ、NTP（用語集項番 46）サーバ、認証サーバ等が必要になる。また、ユーザが参照するためのサービスとしても、DNS キャッシュサーバ、NTP サーバ等が必要である。

#### (1) DNS サーバ

DNS サーバには、インターネット上のホスト名を IP アドレスに変換するために使われるキャッシュサーバと、中小通信事業者が保有するドメインに関する名前解決やアドレス解決を提供する権威サーバがある。IPv6 対応する場合には、双方とも IPv6 対応する必要がある。ウェブホスティング等ユーザが保有するドメインを持つサーバを提供する場合には、セカンダリ DNS サービスについても IPv6 対応の必要がある。

#### (2) プロキシサーバ

各サービスが OS やサーバソフトウェアを更新するためにベンダ提供のアップデートサービスを利用する際に、サービスセグメント上の機器やサービスがインターネット上のアップデートサービス等にアクセスすることがある。各機器から直接 HTTP 又は HTTPS でそれらサービスにアクセスさせてもよいが、OS の更新時には同じパッケージファイルを何台もの機器がダウンロードすることになるため、プロキシサーバによるコンテンツキャッシュ機能を活用することで、トラフィックの削減を図ることができる。

また、コンテンツのウイルス検査などのセキュリティ対策を行いたい場合には、プロキシサーバを介することで、コンテンツキャッシュ機能を利用しつつ、アクセス管理やアクセス監視を行う機能を実現することができる。プロキシサーバは、HTTP 及び HTTPS トラフィックをアプリケーションレイヤで中継するため、IPv4 と IPv6 の相互変換を行うトランスレータとして利用することも可能である。

#### (3) NTP サーバ

サービスセグメント上の機器やサービスの中には、時刻が標準時刻に同期していることが重要となるものがある。NTP サーバは、正確な時刻を生成するハードウェアや、インターネット上の NTP サーバを利用して取得した標準時刻を、サービスセグメント上の機器やサービスに対して提供する。この標準時刻の提供について IPv6 上で実行できることが求められる。

#### (4) 認証サーバ

中小通信事業者のポータルサイトでは、ユーザ向けに、契約状況の確認、利用サービスの変更、契約の更新等の事務手続きや、ウェブメールやブログ等のウェブサービスを提供することがある。このような場合には、利用者のサービスアクセスにおける認証機能が必要となり、バックエンドサービスであるアカウント管理機能と連携する認証サーバが必要となる。認証サーバについては、バックエンドセグメントに配置してもよい。

### 7.2.5 バックエンドセグメント

#### (1) ユーザ管理サービス

ユーザの IPv6 利用申請状況、現在の利用状況、割り当てられた IPv6 アドレス情報等、問い合わせ時や課金時に必要となる情報について扱うことができるよう、ユーザ管理サービスを更新する必要がある。

また、ユーザからの接続サービス申請を受け付けるポータルサイト上のウェブサービス等については、IPv6 利用を選択可能とするように更新する必要がある。NGN をアクセス回線とするトンネル方式を採用する場合には、IPv6 対応トンネルアダプタの必要性について検討する必要がある。

ユーザ管理サービスについては、IPv6 に関するデータを取り扱うことができるよう更新することが主な IPv6 対応であり、通信に関しては IPv4 での運用を当面維持することも現実的な選択といえる。

#### (2) 管理、監視サービス

ネットワーク機器やサーバ機器の稼動状況を監視するシステムや統合的な運用管理システム等についても、IPv6 上での状況を確認及び監視するために、IPv6 対応が必要となる。管理及び監視サービスについては、ユーザに提供するインターネット接続に関わる機器やサービスだけでなく、ISP サービス及びバックエンドサービスに関わる機器やサービスについても、IPv6 上での状況を確認及び監視する必要がある。

また、サービスに障害が発生し、管理サービスが障害を感知した際に、運用担当者及び影響を被るユーザへの通知を行うシステムについても、IPv6 での通知を可能とする必要がある。

### 7.3 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。

#### 7.3.1 セグメント共通

(1) 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。

(2) 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。

(3) 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。

### 7.3.2 ISP サービスセグメント：セキュリティサービス

(1) 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 47）機能を有すること。
- IPv4/IPv6 の IP アドレスアノマリ（異常検知）機能を有すること。
- IPv4/IPv6 の TCP アノマリ（異常検知）機能を有すること。
- IPv4/IPv6 の UDP アノマリ（異常検知）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。

(2) 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(レイヤ 7)の検査が IPv4/IPv6 通信に対して可能なこと。
- 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。

(3) ウイルス対策

ウイルス対策の IPv6 対応では、以下の項目を含めることとする。

- ウイルス対策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の検査が IPv4/IPv6 通信に対して可能なこと。
- 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。

(4) WAF

ウェブアプリケーションファイアウォール（WAF）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の検査が IPv4/IPv6 通信に対して可能なこと。
- 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。

### 7.3.3 ISP サービスセグメント：ユーザサービス

#### (1) 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 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。

#### (2) 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。
- 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 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。
- 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) **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。
- 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。

(4) **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 48）に対応すること。送信ドメイン認証が可能なこと。
- 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。

### 7.3.4 ISP **サービスセグメント**：**基盤サービス**

(1) 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 に関連するリソース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。

(2) **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。

(3) 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。

(4) **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。

### 7.3.5 バックエンドセグメント

#### (1) ユーザ管理システム

ユーザ管理システムの IPv6 対応では、以下の項目を含めることとする。なお、ここでは通信自体は IPv4 での運用を継続することとし、データとして IPv6 を扱うことができることを要件として考える。

- IP アドレスに関するデータとして IPv4/IPv6 を扱うことができること。
- ユーザの IPv6 利用申請状況、利用状況をデータとして保持することができること。
- ユーザに割り当てた IPv6 アドレスをデータとして保持することができること。
- データのエクスポート時に IPv6 アドレスを出力できること。
- データのインポート時に IPv6 アドレスを入力データと扱うことができること。
- IPv4/IPv6 通信の情報をログ出力できること。

#### (2) 管理及び監視サービス

管理及び監視サービスの IPv6 対応では、以下の項目を含めることとする。

- 管理及び監視サービスとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能なこと。
- 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（ウェブシステム、メールシステム、DNS サーバ等）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/IPv6 通信を統合して管理及び監視ができること、
- 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。

#### 7.3.6 その他の機器やサービス

基本的アーキテクチャには示していないが、IPv6 対応時に用いるその他の機器やサービスとしては、「トランスレータ」及び「仮想化基盤」がある。

##### (1) 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。
- インターネットから IPv4 環境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。また、その結果生じる IPv4 環境からインターネットへの IPv4 通信を、IPv6 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。

##### (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 49）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。

### 7.4 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。

中小通信事業者のウェブシステムについては、ユーザが利用する端末に依存せずできるアクセシビリティを確保するため、多様な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配慮する必要がある。

またサービスセグメント及びバックエンドセグメント上の機器やサービスについては、中小通信事業者の職員が利用するものもある。本ガイドラインでは、中小通信事業者の LAN の IPv6 対応については扱わないが、LAN 内が IPv4 のみである場合、IPv6 対応されるサービスセグメント及びバックエンドセグメント上の機器やサービスと LAN 上の既存 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。

これらのほかに、「6.4IPv6 対応に向けた事前準備」で示した内容も考慮する必要がある。

# 8. 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、中小通信事業者における IPv6 対応における脅威と対策について説明する。

## 8.1 通信事業者にとってのセキュリティ課題の概要

通信事業者が確保すべきセキュリティの基準を示した「電気通信分野における情報セキュリティ確保に係る安全基準（第 2 版)」（安全・信頼性協議会）によれば、通信事業者が配慮すべき脅威は、次の 4 種類の要因から発生する。

（1） サイバー攻撃
（2） ネットワーク輻そう
（3） 故障、災害等
（4） 重要情報漏えい

このうち、サイバー攻撃と故障（設計や開発の不備、操作や設定ミス、バグ等）については、IPv6 対応にともない、セキュリティ上の問題が大きくなる可能性が考えられる。

IPv6 対応に際し、サイバー攻撃対策や故障対策として導入及び更新された機器について、IPv6 対応に伴う変更作業が漏れなく、また正しく行われるように、運用手順や対象機器リスト等を更新することが不可欠である。

サイバー攻撃対策については、ファイアウォール、IDS/IPS といったネットワークレイヤに設置される機器について、IPv4 と同等以上のセキュリティ対策機能を持つ機器を導入する必要がある。ファイアウォールのポリシーのように IP プロトコルに依存した設定については、IPv4 に対してかけていた制限を IPv6 に対してもかけることを原則とする。IPv6 特有の機能に影響を受ける部分については、制限を追加する等の検討を行う必要がある。

故障によるシステム停止の可能性を抑制するためにデュアルスタック構成とする場合には、IPv4 と IPv6 でネットワーク構成を揃える必要がある。また、メールシステムやウェブシステムについては、ネットワークレイヤに関する設定を IPv4 と IPv6 とで同じように行う必要がある。

また、IPv6 の設定を行う上では、通信相手が IPv6 に対応していない場合に、IPv4 での通信に切り替えるフォールバック動作に配慮する必要がある。サービス毎、機器及びソフトウェア毎に、どのような状況でフォールバック動作を行うのかについて確認し、想定外の挙動が存在しないことを確認する必要がある。

## 8.2 機器に関するセキュリティ課題

「6 ユーザに提供するインターネット接続部設計時の IPv6 対応方法」及び「7 ISP サービス及びバックエンドサービス設計時の IPv6 対応方法」それぞれの「機能毎の IPv6 対応方法」（6.3 及び 7.3）に示したように、IPv6 対応時には、IPv4 と IPv6 とで、機能や性能が同等であることが不可欠である。IPv4 では安全であった機器が IPv6 対応を有効にしたことで危険になることがあってはならない。機器の提供ベンダが IPv4 のみの運用、IPv4/IPv6 併用での運用及び IPv6 のみの運用のいずれにおいても安全性が同等であることを検証しているかどうか、調達時に十分確認することが必要である。

特にセキュリティ機能を提供する機器については、IPv4 トラフィックに対して抑制している脅威のうち、IPv6 上でも脅威となるものを同じように抑制できていることが重要である。

加えて、IPv6 特有の脅威に対する防護手段を提供していることを確認し、リスクを低減できるよう設定を行う必要がある。また、機器に対して脆弱性検査を行う際には、IPv6 上の問題を検出できるツールやシステムを利用する必要がある。

機器のファームウェア等のアップデートがネットワーク経由で提供される場合、アップデートサーバが IPv6 上で提供されているかどうかを、機器の導入検討時に確認する必要がある。また、アップデートサーバのホスト名を DNS 経由でアドレス変換した場合 IPv6 アドレス（AAAA レコード）が提供されているか、その IPv6 アドレスに到達可能かどうかも検証しておく必要がある。IPv6 アドレスだけが提供され、実際には IPv6 経由で到達できない場合、アップデートに失敗するか、アップデートにかかる時間が増大し、セキュリティリスクが増大する恐れがある。

### 8.3 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、スパムメールの送信を識別するため、送信者の真正性を確認する手段として、接続してきた SMTP クライアントの IPv4 アドレスを DNS 経由で逆引き（IP アドレスをホスト名に変換）が可能であるかどうか調べる方法が用いられていることがある。

このような対策を行っている状態でメールシステムを IPv6 対応すると、IPv6 対応された外部のメールサーバは IPv6 で通信を行ってくるが、IPv6 アドレスの逆引きを設定していない、あるいは設定が間違っていることが少なくないため、メールを受信拒否するケースが増えることがある。メール送信元の正当性の確認に IP アドレスの逆引きの可否を利用するか否かは、十分に配慮する必要がある。

機器やサービスに関する運用状態の監視や異常の発見について、IPv4 と同等であることも十分に検証する必要がある。IPv6 での状態を監視しているつもりで IPv4 の状態を監視している状況を避けるため、どちらのプロトコル上で監視しているのかをわかりやすく表示するような対応が必要となる。

また IP プロトコルが 2 つになることで運用時のコストが倍にならないよう、運用作業の自動化や効率化を検討する必要がある。

### 8.4 システム環境に起因する予期せぬセキュリティ課題

運用要員に対する 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。

ファイアウォール等で IPv4 トラフィックを制限していても、IPv6 トラフィックのセキュリティポリシーが設定されていない場合には、深刻な問題が発生する可能性がある。

ISP 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。

### 8.5 セキュリティ課題への必要な対応策

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。

デュアルスタック構成を採用する場合、導入の都合上、一部の機器のみ IPv6 対応とすることが想定される。機器の IPv6 設定に先立ち、セグメントを越えて影響が波及しないよう、ネ

ットワーク境界に設置するルータ、L3 スイッチ、セキュリティ機器等での IPv6 対応を先行して行い、トラフィック転送を制限できるよう設定するなどの工夫を行う必要がある。

また、IPv6 トラフィックの発生状況を確認できるよう、監視及び管理システムの IPv6 対応についても先行的に行い、IPv6 通信の監視や管理の漏れを防ぐことが必要である。

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

(3) IPv4 アドレスの枯渇時に生じる諸課題に適切に対処するための手順書
http://www.v6pc.jp/pdf/20131015newtech000240919.pdf

# 9. 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、中小通信事業者の典型的なシステムやネットワークのモデルにおける保守、運用及び監視の IPv6 対応方法について説明する。

## 9.1 IPv6 設計時、導入時の考慮事項

IPv6 対応を行った直後は、バックボーンセグメント、サービスセグメント、バックエンドセグメントの各セグメントにおける機器やサービスの稼動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。

バックボーンセグメントについては、IPv6 対応後に IPv4 のみの運用に戻すことは困難なため、IPv6 導入前の試験や検証を十分に行った上で、段階的な導入や対応が必要である。

## 9.2 IPv6 に対応した監視、管理の方法

ISP 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方法について説明する。

サービスを提供する機器は ISP サービスセグメントのネットワークと、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 9-1）。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、このセグメントを経由して行われる。

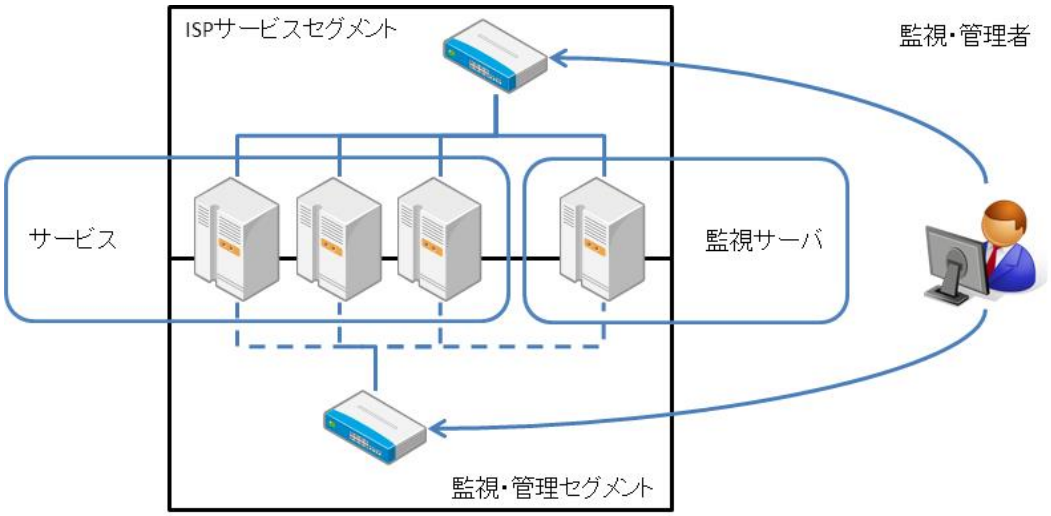


図 9-1　ISP サービスの監視、管理方法のモデル

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。

### 9.2.1 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 50）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。

#### 9.2.2 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。

### 9.3 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の発生要因の切り分け手順について例示する。

#### 9.3.1 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。

#### 9.3.2 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、当該サービスへの ICMPv6（用語集項番 51）パケットの到達性を確認する。同時に ICMP（用語集項番 52）パケットの到達性も確認し、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 よりもレスポンスが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。

#### 9.3.3 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。

#### 9.3.4 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、これの確認を行うことが必要である。

#### 9.3.5 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。

## 10. 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。

通信事業者の IPv6 対応に関しては、ネットワーク構築ベンダを中心として一定のノウハウが蓄積されている。IPv6 対応を検討する上で、機器ベンダ、ネットワーク構築ベンダ、また先行的に IPv6 対応を進めている通信事業者におけるノウハウを活用していくことで、合理的かつ安全な移行を実現できると考えられる。

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。

### 10.1 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

### 10.2 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/

### 10.3 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/

### 10.4 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。

# 11. IPv6 対応に伴う調達及びコストについての考え方

## 11.1 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。

## 11.2 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。

## 11.3 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。

## 11.4 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。

## 11.5 アドレス管理のコスト

通信事業者の場合には、新規 IPv4 アドレスの減少に伴い、ユーザに払い出す IPv4 アドレスの管理コストが上昇している。IPv6 アドレスについては、IPv4 と比較して大きなアドレス空間が割り振られるため、余裕を持った払い出しが可能であり、管理コストを抑えることが可能である。

また、IP アドレスの管理システムや運用体制を IPv4 と IPv6 とで共有化及び統合化することで、IPv6 対応に伴うコスト増を抑えることができる。

## 12. その他の留意事項

### 12.1 IPv6 対応手順の参考文献

IPv6 対応を進めるに際して、通信事業者においては、ユーザトラフィックの中継や各種サービスを可能な限り停止せずに実施する必要がある。設計、試験、移行といった対応手順について、十分な考察、慎重な手順化が求められる。

このような確実な IPv6 対応手順の策定に関する参考文献として、ユーザに提供するインターネット接続の IPv6 対応については IPv6 普及・高度化推進協議会の移行 WG によりまとめられた「2005 年 IPv6 移行ガイドライン ISP セグメント」、ISP サービスやバックエンドサービスの IPv6 対応については「2005 年 IPv6 移行ガイドライン 大企業・自治体編」、全体の構成については IPv4 アドレス枯渇対応タスクフォースによりまとめられた「IPv6 対応リファレンスモデル」を、それぞれ推奨する。

### 12.2 通信事業者におけるフィルタリング設定

IPv6 では、伝送経路上で IP パケットを物理レイヤーの最大パケットサイズ（MTU、Maximum Transmission）に合わせて分割及び再構成するフラグメンテーションを行わないこととされている。このため、通信に先立って経路上の各ルータの MTU を確認し、分割されないパケットサイズを設定する。この動作を Path MTU Discovery（用語集項番 53）という。このような IPv6 通信に必要なメッセージ類を経路途中でのフィルタリングによって制限してしまうと、通信に支障を来すことがある。

通信事業者におけるフィルタリング設定については、JANOG（JApan Network Operators' Group）によりまとめられた「xSP のルータにおいて設定を推奨するフィルタの項目について （IPv6 版）」において推奨設定が示されているので、こちらを参照して適切な設定を行う必要がある。

### 12.3 ユーザ問合せ対応の準備

IPv6 接続を提供するに際して、想定されるユーザからの問い合わせ事項とその回答、対応手順等について準備しておく必要がある。ユーザに生じるトラブル例については、IPv6 普及・高度化推進協議会の IPv4/IPv6 共存 WG　IPv6 導入に起因する問題検討 SWG によりまとめられた「IPv6 導入時に注意すべき課題」等を推奨する。

## 13. （参考）IPv6 対応チェックシート

表 13-1　IPv6 対応チェックシート

| 分類 | 確認項目 | チェック内容 | 補問／回答 | 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。 | 一次プロバイダとのトランジット接続 | □ |
| | | | バックボーンネットワーク | □ |
| | | | サービスセグメント | □ |
| | | | バックエンドセグメント | □ |
| | | IPv6対応するセグメントはシナリオのいずれかに該当しますか。 | デュアルスタック化 | □ |
| | | | パラレルスタック化 | □ |
| | | | トランスレータ等で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** | | | | |
| | | 以下のセグメントについて必要なIPv6アドレスサイズを確認しましたか。 | 一次プロバイダとのトランジット接続 | □ |
| | | | バックボーンネットワーク | □ |
| | | | サービスセグメント | □ |
| | | | バックエンドセグメント（IPv6対応の場合） | □ |
| | | 初期割振りプリフィクスとして/32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。 | | □ |
| | | 初期割振りを受けるための条件（5.1.8参照）を満たしていることを確認しましたか。 | | □ |
| **IPv6対応すべき機器やサービスの確認** | | | | |
| | **一次プロバイダとのトランジット接続** | | | |
| | | 接続点となるルータについて必要となるルーティングプロトコル（BGP, OSPF等）に対応していることを確認しましたか。 | | □ |
| | | ルータ等の相性問題等の存在を一次プロバイダ等に確認しましたか。 | | □ |
| | **バックボーンネットワーク** | | | |
| | | IPv6対応する範囲に含まれる機器やサービスを、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。 | | □ |
| | | NTT-NGNをアクセス回線とする際のIPv6対応方式を決定しましたか。 | トンネル方式を選択した場合、認証サーバはIPv6アドレス払い出しに対応していることを確認しましたか。 | □ |
| | | | ユーザに対してIPv6対応トンネルアダプタが必要になることを説明するよう、ポータルサイト上の申し込みページやパンフレット等を更新しましたか。（※アダプタ不要方式の検討が進んでいるので、常に最新状況の確認が必要です） | □ |

| 分類 | 確認項目 | チェック内容 | 補間／回答 | チェック欄 |
|---|---|---|---|---|
| | サービスセグメント | | | |
| | | IPv6対応する範囲に含まれる機器やサービスを、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。 | | □ |
| | バックエンドセグメント（IPv6対応の場合） | | | |
| | | IPv6対応する範囲に含まれる機器やサービスを、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。 | | □ |
| | | （バックエンドセグメントをIPv6対応しない場合）、想定しないIPv6トンネルが他セグメン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。 | | □ |
| 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。 | | □ |

## 14. （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

[5] 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

[6] 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

[7] 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

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

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

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

[11] RFC3484 （Default Address Selection for Internet Protocol version 6（IPv6））
IETF
http://datatracker.ietf.org/doc/rfc3484/

[12] RFC5220 （Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules））
IETF
http://datatracker.ietf.org/doc/rfc5220/

[13] [RFC6724]
RFC6724 （Default Address Selection for Internet Protocol Version 6（IPv6））
IETF
http://datatracker.ietf.org/doc/rfc6724/

[14] 電気通信分野における情報セキュリティ確保に係る安全基準（第 2 版）
安全・信頼性協議会

[15] 2005 年 IPv6 移行ガイドライン ISP セグメント
IPv6 普及・高度化推進協議会
http://www.v6pc.jp/pdf/ja-08-v6trans-ISP.pdf

[16] IPv6 対応リファレンスモデル
IPv4 アドレス枯渇対応タスクフォース
http://www.kokatsu.jp/blog/ipv4/data/isp.html

[17] xSP のルータにおいて設定を推奨するフィルタの項目について （IPv6 版）
JANOG、日本ネットワーク・オペレーターズ・グループ
http://www.janog.gr.jp/doc/janog-comment/jc1006.txt

[18] IPv6 普及・高度化推進協議会 IPv6 導入に起因する問題検討 SWG
IPv6 普及・高度化推進協議会
http://www.v6pc.jp/jp/upload/pdf/2011093001_v6fix.pdf

## 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 | IX | アイエックス | Internet exchange、インターネットサービスプロバイダやインターネットデータセンター同士を接続するポイントインターネット相互接続点と呼ばれる。 |
| 4 | 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。 |
| 5 | ローミング | | Roaming、ユーザが契約している通信事業者のサービスを、その通信事業者が本来はサービスを提供できない領域においても、提携する他通信事業者の設備を介して、サービスを提供できるようにすること。 |
| 6 | ウェブホスティング | | Web Hosting、ユーザ向けサービスの一つで、サービス提供事業者により管理されたウェブサーバ上にコンテンツを配置することでウェブサイトが構築、公開できるサービス。 |
| 7 | 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。 |
| 8 | 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。 |
| 9 | APNIC | エーピーニック | アジア・太平洋地域を管轄する IR。 |
| 10 | 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。 |

| 項番 | 用語 | 読み・別名 | 意味 |
|---|---|---|---|
| 11 | 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。 |
| 12 | 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。 |
| 13 | 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。 |
| 14 | 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。 |
| 15 | 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。 |
| 16 | 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。 |
| 17 | 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。 |
| 18 | peering | ピアリング | IX 等において、インターネットサービスプロバイダ同士が相互にネットワーク接続を行い、トラフィックを交換することをさす。IX を介さず、1 対 1 でピアリングを行うことをプライベートピアリングと呼ぶ。 |
| 19 | AS | エーエス、自律システム | Autonomous System、インターネットにおいて、あるルーティングポリシーに従うネットワークのことをさす。 |
| 20 | 経路広告 | | Route Advertisement、通信を行う際、IP アドレス等で示される宛先に対する通信パケットを、どの経路（ルート）で送ればよいのか、通信パケットを転送する機器であるゲートウェイ（ルータ等）に伝えること。 |

| 項番 | 用語 | 読み・別名 | 意味 |
|---|---|---|---|
| 21 | 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。 |
| 22 | 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。 |
| 23 | 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。 |
| 24 | prefix | プレフィックス | IPv6 アドレスのネットワーク部。 |
| 25 | NGN | エヌジーエヌ | New Generation Network、NTT 東日本、西日本が展開する次世代ネットワーク網。 |
| 26 | VNE | ブイエヌイー、接続事業者 | Virtual Network Enabler、NGN に接続し、IPv6 ネイティブ方式によるユーザ通信の転送を許された通信事業者。他通信事業者向けにローミングサービスを提供する。 |
| 27 | PPPoE | ピーピーピーオーイー | Point-to-Point Protocol over Ethernet、ユーザ認証をともなうポイント間接続プロトコルである PPP をイーサネット上で用いるためのトンネリングプロトコル。 |
| 28 | ホームゲートウェイ | | Home Gateway、固定回線サービスにおいて、公衆通信網と宅内ネットワークを接続するために宅内に設置される機器の総称。回線終端装置、ブロードバンドルータ機能、光電話等 VoIP ゲートウェイ機能等を持つ。 |
| 29 | 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。 |
| 30 | 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。 |

| 項番 | 用語 | 読み・別名 | 意味 |
|---|---|---|---|
| 31 | 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。 |
| 32 | 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。 |
| 33 | 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。 |
| 34 | 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。 |
| 35 | 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。 |
| 36 | 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。 |
| 37 | 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。 |
| 38 | 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。 |
| 39 | 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。 |
| 40 | 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。 |

| 項番 | 用語 | 読み・別名 | 意味 |
|---|---|---|---|
| 41 | 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。 |
| 42 | 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。 |
| 43 | HTTPS | エイチティーティーピーエス | HyperText Transfer Protocol Secure、HTTP にもとづく通信を安全に行うためのプロトコル。通信を保護するために、SSSL/TLS プロトコルが利用される。 |
| 44 | 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。 |
| 45 | | プロキシ | 主にウェブサービス（HTTP、HTTPS）を中継するサービス。 |
| 46 | 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。 |
| 47 | 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。 |
| 48 | 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。 |
| 49 | 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。 |

| 項番 | 用語 | 読み・別名 | 意味 |
|---|---|---|---|
| 50 | 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。 |
| 51 | ICMPv6 | アイシーエムピーブイシックス | IPv6 のための ICMP。 |
| 52 | 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や取得等に利用されるプロトコル。 |
| 53 | Path MTU Discovery | パスエムティーユーディスカバリー | 伝送経路上で IP パケットを物理レイヤーの最大パケットサイズ（MTU、Maximum Transmission）を検索する仕組み。 |