2.　地方公共団体における緊急対策

2.1. 緊急対策の全体像

前章で述べたIPv4アドレス在庫枯渇について地方公共団体が対処することを考えたときに、最終的な解決策は、地方公共団体のシステム全体の IPv6 対応を実施することになる。しかし、IPv4 アドレス在庫枯渇が直前に迫っている今、即座にシステム全体を構築し直すことは難しいことから、最低限必要な対策を実施することと併せて、IPv6 移行のための方策について検討するのが、現実的な対応策となるであろう。

それでは緊急に対策する必要があることとして、下記の四つが挙げられる。なお、ここでいう「緊急」とは 2011 年（平成 23 年）から 2013 年度（平成 25 年度）までに対策が必要となるものである。

(1)　調達機器の IPv6 対応

今後実施する機器更新の際には、地方公共団体で調達する機器について IPv6 対応とすることが求められる。後述するように、IPv4 アドレス在庫枯渇への対応は機器の更新だけではなくシステムの改修が必要になる場合があるが、まずは機器を対応させるということが重要である。

(2)　フロントシステムの IPv6 対応

フロントシステムについて、IPv6 対応を実施することが求められる。この対策については、地方公共団体のシステム更新タイミングによっては、リース等の期限が来る前に対策を求められる時期が来る可能性がある。

(3)　セキュリティーについての検討

フロントシステムのIPv6対応に伴うセキュリティー課題について認識するとともに、内部システムのIPv6対応の手法について検討することが必要である。なお、内部システムの IPv6 対応の実施は、緊急対策の範囲外とする。

(4)　アドレス設計における最適化計画の検討

上記（1）～（3）の対策を行うことに併せて、システム更新タイミングを見極めつつ、IP アドレスを必要とする機器について、アドレス設計についての最適化の作業を実施することを推奨する。

上記四つの対策については、情報システムにかかる経費が現在と変わらないものもあるが、現在よりも高くなるものもある。しかし、これらの対策は、重点計画等でも地方公共団体に対応が求められているものであり、経費がかかるとしても、実施する必要がある。

また、上記の対策の期限を 2013 年度（平成 25 年度）としたのは次の理由による。

第 1 章にも記載されているように、2011 年（平成 23 年）4 月には ISP の IPv6 対応サービスが開始すること及び IPv4 アドレス在庫枯渇の時期が迫っていることを考慮すると、早ければ 2011 年（平成 23 年）中に IPv6 で地方公共団体にアクセスするユーザーが現れ、地方公共団体の提供する情報サービスを受けることに支障が生じるケースが起こり得る。このような事態を防ぐためには早期の IPv6 対応が求められるが、例えば来年までに対応する場合、情報機器のリース期限等によっては、違約金の発生等が起こり得る。また、システム更改の費用を予算に計上しているのかという問題もある。

以上より、地方公共団体が実施する住民に対するオンラインでの情報提供等について、一部の住民に対して提供できないという事態を防ぐためにも、早期のフロントシステムの IPv6 化を行うことは重要であるが、その時期は、現実的に予算措置等が必要なことをかんがみて、2012 年度（平成 24 年度）中、遅くとも 2013 年度（平成 25 年度）中を目処にすることが望ましい。また、調達機器の IPv6 対応は、今後短期間のうちに対応可能と考えられるが、セキュリティーについての検討やアドレス設計における最適化計画の検討については、検討のための一定の期間が必要と考えられ、2012 年度（平成 24 年度）までの検討を目途とすることが必要である。

さて、上記の対策を実施するに当たり、具体的に対処すべき内容について、表 2-1 に記載する。内容の詳細については、「参照」から該当ページを参照のこと。

表 2-1　緊急対策のポイント

（1）調達機器の IPv6 対応		参照
①	これから調達を行う機器については、IPv6 対応を要件として明記する。	p17
②	調達する機器については、IPv6 Ready Logo の Phase-2 の認証を受けた機器とする。	p20
③	調達の際の要求仕様には、参考資料 2 の調達仕様書案を参考にする。	p18 参考 p 4
④	機器の見積りを取る際には、複数社から取得して適正な価格を確認する。	p20

（2）フロントシステムの IPv6 対応		参照
－	フロントシステムについては、2012 年度（平成 24 年度）、遅くとも 2013 年度（平成 25 年度）までに IPv6 対応を行う必要がある。	P14
①	フロントシステムについてシステムチェック表に基づいてチェックを行い、IPv6 対応が必要なシステムを抽出する。 → 「不特定多数」欄に「○」がついたシステムが「対象システム」である。 → 「ASP」欄に「○」がついている場合、対応はサービスプロバイダーの対応に依存する。	p22
②	対象システムに利用している機器を特定して、機器対応状況リストに、必要な情報を入れる。 → ベンダーに各機器の IPv6 対応状況を確認する。	p25
③	対応方策について、システム調達時期に応じて場合分けをする。 2014 年（平成 26 年）以降のシステム更新 → トランスレーション方式による対応 2014 年（平成 26 年）より前のシステム更新 → IPv4/IPv6 デュアルスタック方式又はトランスレーション方式による対応	p28
④	ネットワーク回線の調達に当たっては、IPv4 アドレス枯渇対応タスクフォース「ISP サービスの IPv6 ガイドライン」の「必要条件」を満たしていることを要件として明記する。	p30
⑤	機器、ネットワーク回線、システム更新については、複数社から見積りを取得して適正な価格を確認する。	p30
⑥	2011 年（平成 23 年）、2012 年（平成 24 年）にシステム更新を検討しているが、IPv6 対応が含まれていない場合、一度計画を凍結して、IPv6 対応を含めた更新として再度計画を立てることを推奨する。	p34

（3）セキュリティーについての検討		参照
①	IPv6 対応を行う際のセキュリティー項目のチェックについては、IPv4 で実施しているものと同等のチェックを IPv6 でも実施する。	p37
②	現在の IPv4 のセキュリティーレベルが低い場合は、IPv6 についてもセキュリティーレベルが同様に低い状態になってしまうため、IPv4 と同等以上に注意を払う必要がある。	p37
③	IPv6 対応をした覚えが無くても、情報機器等が知らない間に IPv6 対応となっている場合もあり得るため、定期的にセキュリティー状態についてチェックをする。	p36
④	セキュリティー製品は、ネットワーク機器等と比べて IPv6 対応製品が少ないため、導入時には対応がなされているかどうかをチェックする必要がある。	p37

（4）アドレス設計における最適化計画の検討		参照
①	ネットワーク統合によるシステム最適化を実施するために、IPv6 アドレスによる設計を基盤とした到達像をあらかじめ想定する。	p39
②	政府や大手企業を含めた体制で、統合ネットワーク基盤の整備に基づいた最適化計画の検討と実行を図る。	p40

2.2. 調達機器の IPv6 対応

2.2.1. 対応策の概要

IPv4 アドレス在庫枯渇に備えて、まず地方公共団体が実施しなくてはならないことは、情報システムに関する調達について、IPv6 対応を必須とすることである。

住民が IPv6 を利用するようになると、住民からアクセスができるようにするために、地方公共団体のシステムは IPv6 対応を行うことが必要となる。早ければ 2011 年（平成 23 年）中にも IPv6 利用者が現れると予測されている。

さて、IPv6 からのアクセスに対応するためには、対象となるシステムを IPv6 対応にする必要がある。そしてそのためには、まず機器自体が IPv6 に対応していることが必要である。サービスそのものを提供しているサーバーについては、主要な OS がすべて IPv6 対応を終えているため、OS を最新にして IPv6 機能を使うように設定することで機器の IPv6 対応は可能である。しかしサーバーに行くまでの回線や、通信機器（ルーター、ロードバランサー等）については、IPv6 対応の機器が増えているとはいえ、すべてが対応しているわけではない。これらの機器・サービスすべてが IPv6 対応をしていない場合、サーバーを対応させたとしても IPv6 からのアクセスを受けられないので、住民向けのサービスに利用している通信機器や通信サービスについても併せて IPv6 対応を行う必要がある。

このような状況に対応するために、地方公共団体は調達仕様書に IPv6 対応を必須項目として入れることが必要である。既に日本政府の調達では、IPv6 が要件として入るようになっている。また、岡山県や倉敷市等、一部の地方公共団体でも同様の方法をとっており、機器レベルでの IPv6 機器の導入が進んでいる。

なお、機器の導入の際には、フロントシステムだけでなく、内部システムも含めたすべての機器について、IPv6 対応機器にしていく必要があることに注意する。第 3 章に記載しているように LGWAN の IPv6 対応が必要となる可能性が高いことから、内部システムについても、すぐにではなくても、近いうちに IPv6 化が必要になる可能性がある。それに対応して IPv6 での情報を受け取れるようにする際に、IPv4 にしか対応していない機器があると、その機器の入れ替えコストが発生することが予測される。

また、IPv4 のみに対応している通信機器は、世界市場の中では旧式の在庫として扱われているものが多くある。IPv6 対応を調達仕様で必須と指定していない場合、このような旧式の機器が導入される可能性もあり、それを回避するためにも、IPv6 対応を謳う必要がある。

なお、単に通信機器を IPv6 対応にするだけでは、IPv6 端末からのアクセスに対応できるようにはならない。実際には 2.3 に記載するようなシステム側の対応が必要になるが、それを行うためにも通信機器を IPv6 対応にする必要がある。

2.2.2. 調達仕様書案

具体的な調達仕様書の文例として、岡山県の事例を挙げる。岡山県では、システム調達の際に下記のようなネットワーク要件を定めており、IPv6 への対応を求めている。

X.X. ネットワーク要件

本システムは●●行政系ネットワークに接続することを前提とするため、同ネットワークに関する以下の通信規約等に従うこと。

（1） 通信規約／規格

表 X.X. 通信規約／規格

項番	OSI 階層	機能	通信規約
1	トランスポート層	プロセス間通信	TCP
2	ネットワーク層	ノード間通信	IP　　注 1
3	データリンク層	隣接ノード間通信	Ethernet

注 1)
IP は､現在 IPv4 を使用しているが､段階的に IPv6 への移行を予定していることから、本調達の対象となるハードウェア及びソフトウェアについては、IPv4、IPv6 双方（デュアルスタックを含む。）に対応したものとすること。

（2）以下省略

図 2-1　調達仕様書例(岡山県)

岡山県の場合は、既に県の情報ハイウェイを IPv6 対応にしていることからこのような表記となっている。そのため、まだ IPv6 対応をしていない地方公共団体の場合は、例えば図 2-2 のような表記とすることが考えられる。

X.X. ネットワーク要件

本システムについては以下の通信規約等に対応したものとすること。

（1） 通信規約／規格

表 X.X. 通信規約／規格

項番	OSI 階層	機能	通信規約
1	トランスポート層	プロセス間通信	TCP
2	ネットワーク層	ノード間通信	IP　　注 1
3	データリンク層	隣接ノード間通信	Ethernet

注 1)

IP については現在 IPv4 を使用しているが、IPv4 アドレス在庫枯渇に伴い、段階的に IPv6 への移行を予定していることから、本調達の対象となるハードウェア及びソフトウェアについては、IPv4、IPv6 双方に対応したものとすること（注 2)。なお、IPv6 への対応方法としては、IPv4/IPv6 デュアルスタック方式による対応が望ましい。

注 2)

機器の選定に当たっては、国際的な IPv6 に関する標準プログラムである IPv6 Forum Ready Logo Program で、Phase-2 の認証を受けている機器であること。

https://www.ipv6ready.org/db/index.php/public/

（2）ネットワーク回線

本件において調達を行うネットワーク回線については、当団体が指定する任意の時期に、IPv4 アドレス枯渇対応タスクフォース「ISP サービスの IPv6 対応ガイドライン」の要件を満たしたサービスに切り替え可能であること。

http://www.kokatsu.jp/blog/ipv4/data/isp-guideline.pdf

図 2-2　調達仕様書案

実際に調達を行う際には、機器だけでなく、ソフトウェアやネットワーク回線等を含めて、情報システムとしての調達が行われることが多いと考えられる。そのため、参考資料で調達仕様の案をそれぞれ記載している。

ここで挙げている調達仕様の例は、地方公共団体が情報システムの発注を行う際に、そ

のまま要求仕様に記載することを想定している。なお、システム、機器、ネットワーク回線のそれぞれについて、現在は IPv4 で利用するが、任意の時期（IPv6 利用者が現れた時など）に IPv6 に対応できるような構成にしておくことを求めている。

2.2.3. 対応機器の状況

以上のように調達仕様書に IPv6 に対応していることと書いていても、すぐに IPv6 を使うわけではない場合、納入された機器について IPv6 機能を利用しない状態で動かすことになるため、本当に IPv6 を使える機器なのかが分からない。

仕様上（カタログ上）IPv6 の通信を受けることができるとされていても、実際に使ってみるとうまく動かないということや、機器間の相互接続がうまくできないということが、まだ起こり得るというのが実情である。いざ使おうというときに結局使えなかった場合、改めて機器調達が必要となり、コストの減少が図れないため、IPv6 での相互接続性の確保等が証明されている機器を選ぶことが重要である。

そのため、今回の調達仕様書案では、IPv6 Ready Logo という IPv6 の相互接続性について審査・認証を与えている世界的なプログラムで Phase-2 の認証条件を満たしている機器であることを求めている。この認証を得ている機器同士であれば、一定水準以上の相互接続性が確保されている。

IPv6 Ready Logo Phase-2 の認定を受けた機器のリスト[4]は、財団法人電気通信端末機器審査協会（JATE）が運営する日本 IPv6 認証センター[5]のホームページでも閲覧することができる。またこのリストでは分からない場合は、上記の日本 IPv6 認証センターのウェブサイトから相談することも可能である。

2.2.4. コスト

調達の際に IPv6 対応を要件とすることによって、コストがどのように変わるかという点も重要である。機器の見積りを取る際には、複数社から取得して適正な価格を確認する。

結論から言うと、IPv6 に対応した通信機器を導入する場合、特に費用が高くなることはない。最近の通信機器は一部を除いて IPv6 対応しているものがほとんどであり、現在の IPv4 環境と同等のことを行うために機器の更新をする、ということであれば、大きな費用の違いは生じない。実際に既に IPv6 対応機器を導入している地方公共団体でも、特に調達費用が高くなってはいない。もし大きく調達コストが上がると示された場合、それは不必要な機能が搭載されていたり、元々の提案が相当に古い機器であったりすることが推測されるため、高額化の理由についてベンダーに確認を求めた方が良い。

---

[4] https://www.ipv6ready.org/db/index.php/public/
[5] http://ipv6.jate.jp/ready

2.2 の重要ポイント

- これから調達を行う機器については、IPv6 対応を要件として明記する必要がある。
- 調達する機器については、IPv6 Ready Logo の Phase-2 の認証を受けた機器とする。
- 調達の際に機器の IPv6 対応を求めても、調達コストが増えることはない。

2.3. フロントシステムの IPv6 対応

2.3.1. 緊急対策の対象となるシステム・サービスの抽出

IPv4 アドレス在庫枯渇に備えて、地方公共団体が緊急に対策をしなくてはならないシステムは、「近いうちに IPv6 でアクセスされる可能性があるシステム」である。

住民・企業等が利用している端末は、地方公共団体の意思とは関係なく、何らかのきっかけで IPv6 化が行われる。そして IPv6 化、特に IPv6 しか IP アドレスを持たない端末が現れると、地方公共団体のシステムに対しても IPv6 でアクセスしてくる。そして、そのアクセスに対して応答するためには IPv6 対応が必要である。

住民・企業等の端末が IPv6 化するタイミングは、IPv4 アドレスの在庫が枯渇した後、どのタイミングで起こるか予測できない。早ければ 2011 年（平成 23 年）中にも現れる。そのため、在庫枯渇後すぐに IPv6 からのアクセスが来ても問題が起こらないように、緊急の対策が必要である。

さて、具体的に住民・企業等からのアクセスがあるシステムとしては、下記が考えられる。まずはそれぞれの団体で、これらのシステムを利用しているかどうかをチェックすることからはじめる必要がある。

表 2-2　システムチェック表

カテゴリ	システム名	チェック項目			
		システムの有無	オンライン公開	不特定のアクセス	ASP 利用/独自提供
ウェブサイト	公式ウェブサイト				
電子申請	電子申請受付システム				
施設予約	公共施設予約システム				
	図書館の蔵書検索・予約システム				
電子調達	電子調達システム				
	電子入札システム				
その他	統合型 GIS				
	地域 SNS・ブログ・電子会議室等				

具体的には、各システムが存在しているかどうかをまずチェックする。システムがある場合は、そのシステムのサービスをオンライン上で提供しているかどうかをチェックする。この際、庁内からや特定の人からのみアクセス可能になっているのか、それとも、不特定の住民・企業等からもアクセスが可能なのかをチェックする。さらに、各システムのサー

ビス提供について、独自で提供しているのか、アプリケーションサービスプロバイダー（以下「ASP」と言う。）等を利用しているのかをチェックする必要がある。

このチェック表のうち、「不特定のアクセス」に「○」がついているものが、緊急対策の対象となるシステムである。

また、オンライン化しているが、特定の人・企業のみを対象としているシステムについては、その接続対象によっては緊急対策の対象となるので、対象としている人・企業に対して、IPv6 対応をいつまでに行うかを別途確認する必要がある。

2010 年（平成 22 年）11 月にすべての地方公共団体を対象に実施した「地方公共団体における IPv4 アドレス枯渇対応に関するアンケート調査」では、多くの地方公共団体で住民向けにオンラインサービスが可能になっていることが明らかになったが（図 2-3）、これらのシステムは優先的に対応する必要がある。

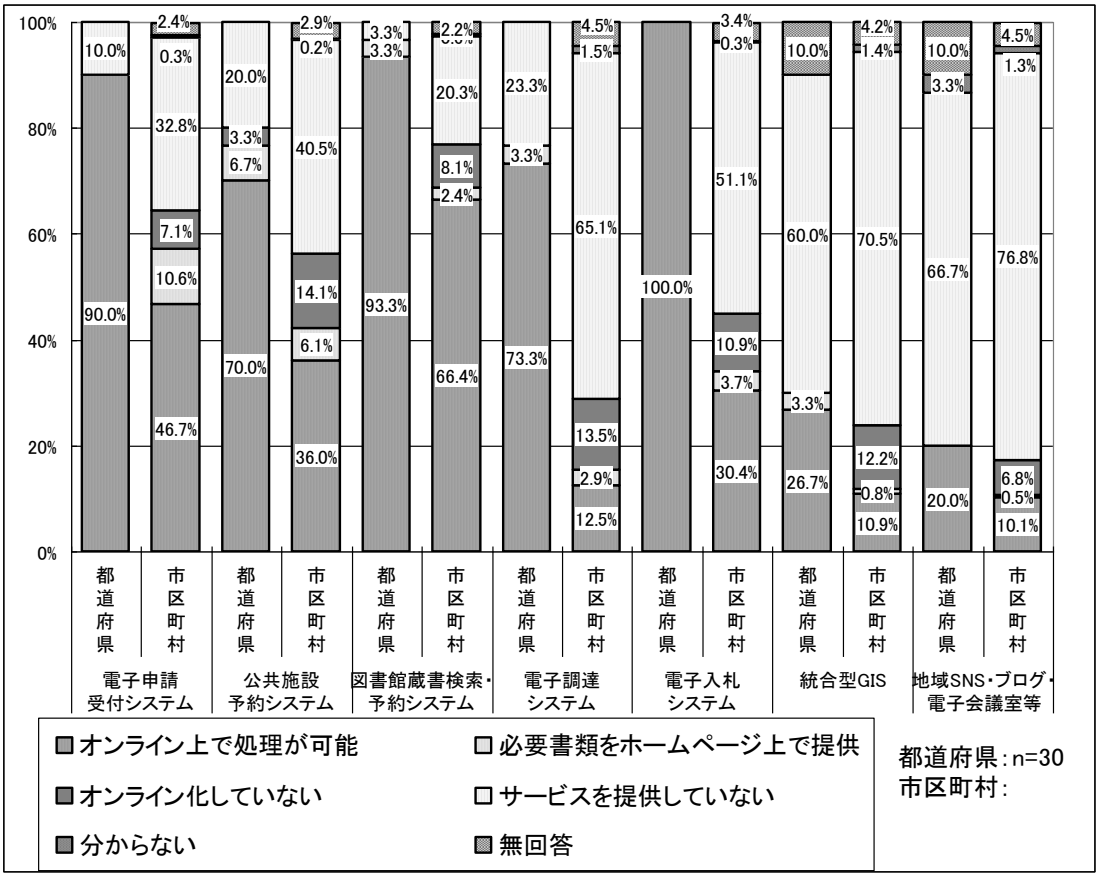

図 2-3　フロントシステムのオンライン化状況（市区町村）

なお、外部からのアクセスについては、内部向けの業務システムについても無関係というわけではない。「地方公共団体における IPv4 アドレス枯渇対応に関するアンケート調査」

では、0～20%程度の都道府県（図 2-4）、0.5～3.6%程度の市区町村（図 2-5）で、内部の業務システムについても、インターネットからの接続が可能であるとの回答があった。

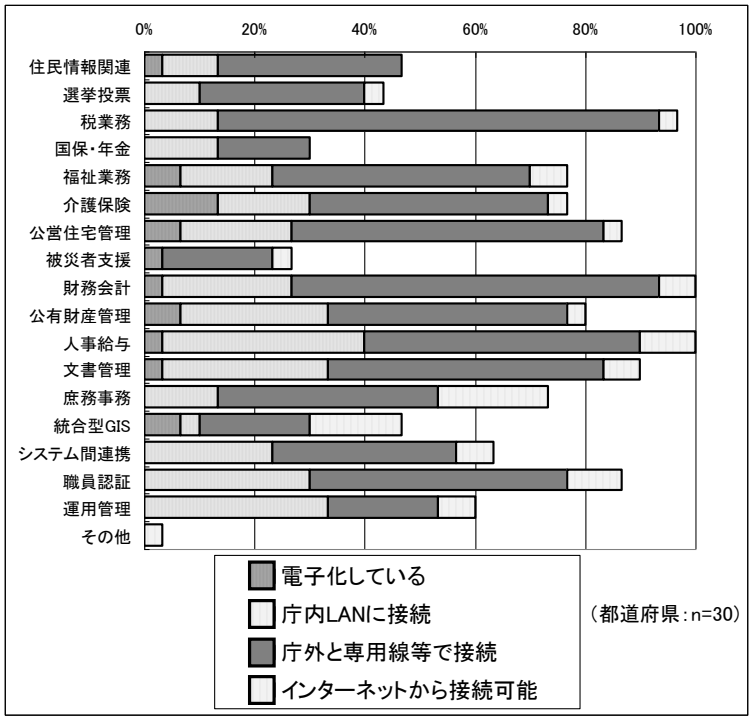

図 2-4　業務の電子化とネットワーク化（都道府県）

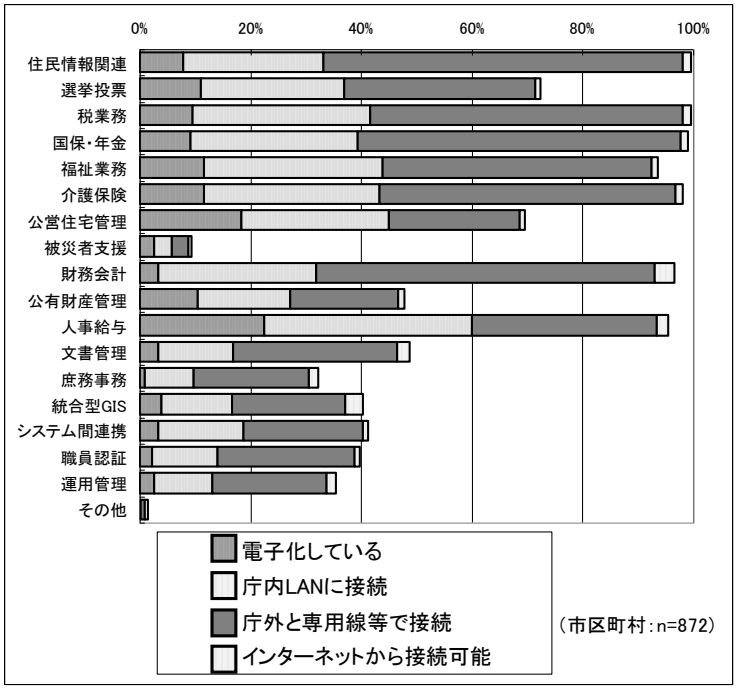

図 2-5　業務の電子化とネットワーク化（市区町村）

この「インターネットから接続可能」というのは、インターネット上に公開していて住民等がアクセスできるというものではなく、インターネット VPN 経由でのシステム構築業者によるメンテナンス用のアクセスや、在宅勤務や外出先から内部システムを利用する等の理由でのリモートアクセスを許可していたりするものである。

このような接続形態の場合、基本的にアクセス元が特定できるような形で運用されており、リモートアクセス元となる端末やネットワークが IPv6 化しない限り、緊急での対応は必要ないと考えられる。当面の間は、リモートアクセスをする端末は IPv4 でも対応できるようにしておくという条件を付けておくことも、移行期間の選択肢になり得るであろう。

ただし、外部からのアクセスを可能にしているということは、外的な要因によって当該システムの IPv6 対応実施を迫られる可能性が、リモートアクセス等を許可していないシステムよりも高いということでもある。そのため、業務システムについても、外部からの接続という要因によって IPv6 対応が求められる可能性があることを、考慮しておいた方が良い。

2.3.2. 対象となる機器の抽出

対象となるシステム・サービスの特定の次は、対応しなくてはいけない機器の特定が必要である。

その前に 2.3.1 で確認を行った、ASP を利用しているのか、独自で提供しているのかということによって対応が異なる。ASP を利用している場合、IPv6 対応を行うのは地方公共団体ではなく、そのサービスを提供している事業者である。

そのため、地方公共団体としては、目標とする時期までに IPv6 からのアクセスが可能になるように ASP 事業者に対して対応を求めるか、それが可能な事業者に切り替えることが必要になる。ASP の対応方法としては 2.3.3 で挙げているものと基本的に変わらないので、これを参考にして指示や発注を出す。

これに対して、独自でシステムを提供している場合は、自ら対応する必要がある。

まず、各システム・サービスを構成している機器について、以下の二つのどちらかに当てはまる機器かを特定する。

(1) インターネットからの通信を処理する機器

ウェブサーバー等、住民向けの電子自治体サービスを提供するために、インターネット側から来る通信を直接処理する機器。

(2) インターネットからの通信を中継する機器

インターネットから、住民向けの電子自治体サービスを実施しているサーバーまでの区間で、通信を中継する機器。

（1）は住民向けにサービスを実施している機器のうち、直接住民とのインターフェースになっている機器（主としてウェブサーバー）を指しており、（2）は（1）のウェブサーバーまでの経路で通信の中継を行っている機器（主としてルーター、スイッチ）を指している。これらの機器は、サービスの IPv6 化を実施する際に IPv6 対応が基本的に必須となる機器である。

なお、住民と直接やりとりをする必要がないシステムについては、IPv6 対応をしなくても基本的にはサービスの提供に問題はない。例えば、住民向けに公開しているサービスについて、情報を公開サーバーとは別のサーバーのデーターベースで管理し、住民からのリクエストに応じて公開サーバーからデーターベースサーバーにアクセスして情報を入手する、というような構成をとっている場合のデーターベースサーバー等があてはまる。これらの住民と直接通信をせず通信の中継もしないという機器については、サービスの提供上は困らないため、初期の時点では IPv6 化の対象外とする選択もあり得る。ただし 1 点気をつけなくてはいけない点として、これらの内側のシステムについても改修が必要な場合がある。それは、来訪者の IP アドレスを収集して利用しているようなシステムである。例えば認証キーとして来訪者の IP アドレスを利用しているようなシステムでは、そのキーとして IPv6 アドレスが通るようにする必要がある。そのため、更新機器の一つとしてリストアップしておく必要がある。

なお、IPv6 化の対象外とする場合も、機器更新のタイミングが来るようであれば、機器の IPv6 対応までは実施しておく必要があるであろう。

次に、IPv6 化対象として特定したサーバーやルーター、スイッチ、セキュリティー機器等について、下記の点を確認し表 2-3 のようなリストに記入する必要がある。

(1)　機器の種類
(2)　ホスト名
(3)　機種型番
(4)　シリアルナンバー（S/N）
(5)　OS バージョン
(6)　リース期間（購入の場合は減価償却期間）/更新予定日
(7)　IPv6 対応機器への切替の必要性

これらの情報のうち、（3）～（5）までの 3 項目を利用して、当該機器が IPv6 に対応しているかどうかについて調査を行う。ここ数年のうちに導入した機械であれば、IPv6 に対応している機器も多くあり、特に考慮していないうちに IPv6 対応の機器が入っていることもある。この調査の結果、IPv6 に対応していることが分かったものについては、（7）に「不要」を入れる。

表 2-3　機器対応状況リスト

機器種類	ホスト名	機種型番	S/N	OS バージョン	リース期間	IPv6対応機器への切替

以上のようにシステム・サービスと、機器の状況を整理することで、緊急対策として何を行う必要があるかを検討する材料が揃う。

なお、クライアント PC やサーバーの場合、OS のバージョンを確認することで IPv6 対応状況が分かる。しかし、ルーターやスイッチ等については、OS のバージョンだけでは分からないことがあるので、各ベンダーに問い合わせをして機種型番、S/N 等をもとに確認する方が望ましい。この際、古いルーター等には、IPv6 アドレスや IPv6 マルチキャスト（ネット上の特定グループへの放送型配信）アドレスを受け取るだけで不具合が発生するものがある。このような機器がもしあった場合は何よりも早期に対応する必要があるので、ベンダーへの確認を行う際には IPv6 パケットが来ても正常に動くかどうかという点を併せて確認する必要がある。

参考までに、クライアント PC 用の OS、サーバーOS についての対応は、表 2-4 のようになっている。

表 2-4　各 OS の IPv6 対応状況

	OS	IPv6 対応バージョン
クライアント PC	Windows	XP SP2 以降（完全対応ではない） VISTA 以降
	Macintosh OS	OS X 10.4 以降
	Linux	カーネル 2.2 以降
サーバー	Windows	Windows Server 2003 以降
	Linux	カーネル 2.2 以降
	Free BSD	4.0-RELEASE 以降

2.3.3. 対応方策の選択

前節までで収集した情報をもとに、IPv6 からのアクセスに対して、どのような方法で対応するかについて検討する。

先に記載したように、フロントシステムの IPv6 対応は 2013 年度（平成 25 年度）までの対応が求められているが、対応の方策については、各地方公共団体のシステムの構成や、この時期までのシステムの更新状況によって異なる。

まずシステムの更新時期が 2014 年（平成 26 年）以降の場合、既に導入している機器が IPv6 に対応していない限り、下記の三つの方策のうち、（3）トランスレーション方式を利用して当面の解決を行うことが望ましい。

これに対して、システムの更新時期が 2014 年（平成 26 年）より前の場合は、下記の三つの方策の何れも可能だと考えられる。

なお（1）IPv6 独立方式は、既存のシステムの移行ではコストもかかり、あまり望ましいとは言えないが、新たなサービスを提供しようとする場合、こちらの方がコストが低く効率の良いサービスを展開できることがある。

また（3）トランスレーション方式を採用する場合には、それで解決したと考えるのではなく、当面の対応であると考えて、その後、どのように IPv4/IPv6 デュアルスタック方式や、IPv6 独立方式等へと移行するかについて検討する必要があるであろう。

では、具体的な方策について、下記に記載する。

（1） IPv6 独立方式
（2） IPv4/IPv6 デュアルスタック方式
（3） トランスレーション方式

（1）IPv6 独立方式

既存の IPv4 のサービスの提供と並行して、IPv6 によるサービスを提供できるように新たにシステムを構築する方法である。既存のサービスに全く影響を与えることなく、IPv6 への対応をすることが可能だが、IPv6 ユーザーのためにわざわざシステムをもうひと揃い揃えることになり、機器の調達等でコストがかかる。

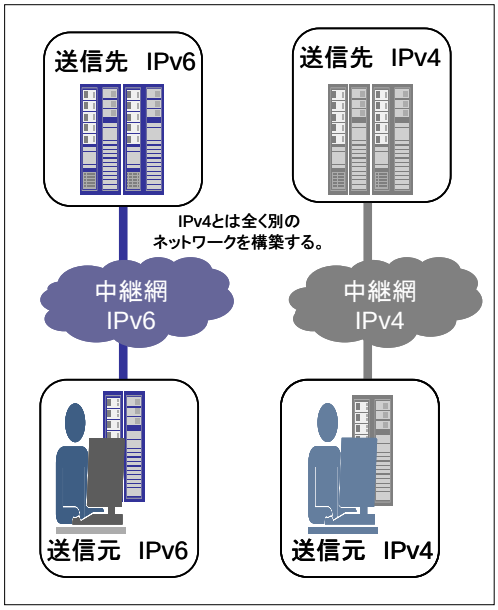

図 2-6 IPv6 独立方式

（２）IPv4/IPv6 デュアルスタック方式

住民向けに提供しているサービスについて、IPv4 でも IPv6 でも双方からアクセス可能な形にする（デュアルスタック）という対応である。既に機器が IPv6 に対応している場合には、IPv4 と IPv6 の双方で通信が可能なように設定を変更し、サービスについても、IPv6 からのリクエストを受け付けられるように変更する。また現在の機器が IPv6 に対応していない場合には、IPv6 に対応している新たな機器を導入して、IPv4 と IPv6 の双方で通信が可能なように設定する。これから当面の間は、IPv4 と IPv6 が共存して利用される時代になると考えられるため、両方からの通信を一つのシステムで対応できるようにすることは、コストとしても短期～中期的な対応としても望ましいであろう。

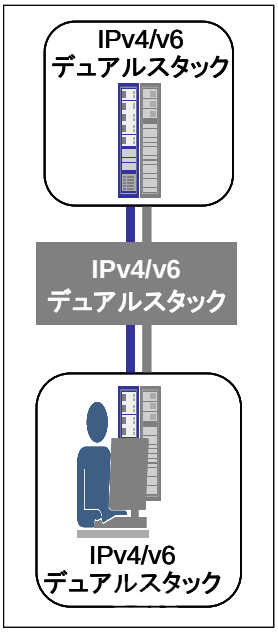

図 2-7　IPv4/IPv6 デュアルスタック方式

（３）トランスレーション方式

既存の IPv4 のサービスについては変更せずに、サービスにアクセスする入口の機器で、IPv6 のアクセスを IPv4 に変換する（トランスレーションする）という方法である。既存の機器については一切手を加えずに、トランスレーターの導入によって解決をするため、トランスレーターの導入費用のみで済むというメリットがある。ただし、大量にアクセスが来た場合にトランスレーターで通信を処理できるかという問題や、すべてのサービスについてトランスレーターの検証をしているわけではないことから、既存のサービスに対して、IPv6 からトランスレーターを介してアクセスが可能かどうか、ベンダーに確認する必要があるであろう。

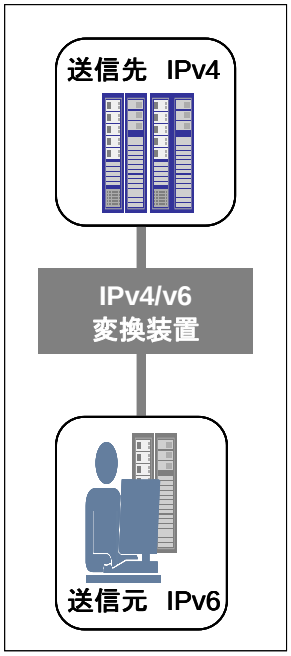

図 2-8　トランスレーション方式

2.3.4. システム更改方法と費用の見積もり

それではIPv4アドレス在庫枯渇についての緊急対策にかかるコストはどの程度になるのか。これは、各地方公共団体のシステムの現状によって大きく異なる。

基本的な前提として、IPv6 に対応した機器を導入する場合、一般的なルーターやスイッチなどの通信機器や、サーバーなどについては、特に IPv6 になったからといってコストはほとんど変わらない。

これに対して、外部と接続するインターネット回線については、利用している事業者や、サービスによって費用が異なる。多くの地方公共団体は、フロントシステムに対して住民が接続可能にするためのネットワークとして、民間の ISP か、地域情報ハイウェイを利用している。

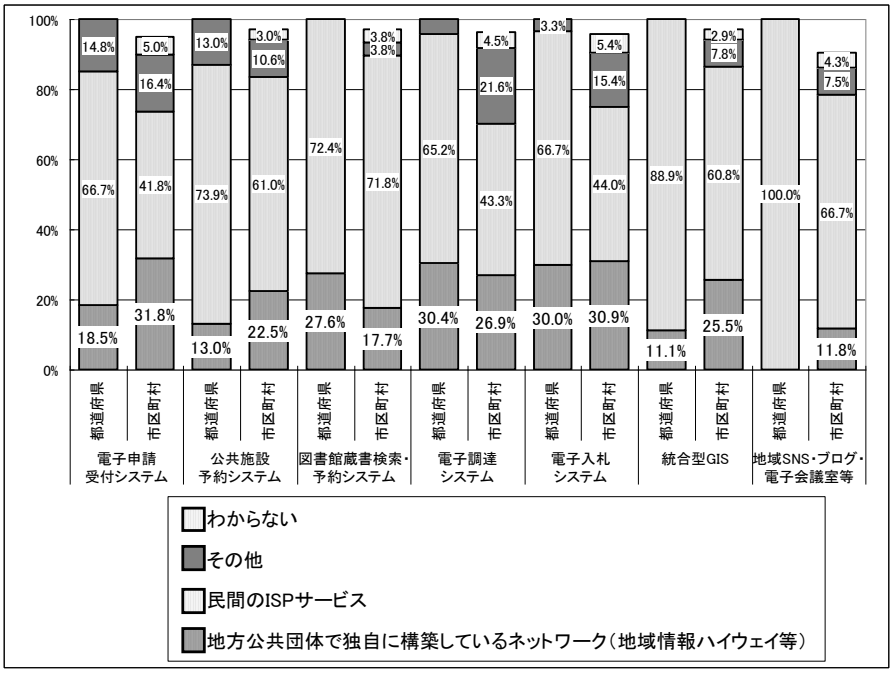

図 2-9　フロントシステムの接続ネットワーク

地域情報ハイウェイは、現状ほとんど IPv6 化が行われていないので、地域情報ハイウェイが IPv6 化をしない限り、民間の ISP が提供している IPv6 サービスを利用する必要がある。社団法人日本プロバイダー協会（JAIPA）が公開している「ISP の IPv6 対応について[6]」の「ISP 各社の IPv6 インターネット接続サービス提供に関する情報」や、IPv4 アドレス枯渇対応タスクフォースが公開している「IPv6 サービスリスト[7]」を見ると、大手の ISP では IPv6 に対応しているところが多くあることが分かる。また、地方の ISP でも対応している事業者が増えてきており、IPv4 アドレス在庫枯渇を見据えて、各事業者が対応を進めているので、このガイドがお手元に届く頃には、さらに IPv6 対応事業者が増えているので

6 http://www.jaipa.or.jp/ipv6/
7 http://www.kokatsu.jp/blog/ipv4/data/ipv6service-list.html

はないかと考えられる。

なお、調達の際には、ISP に対して、IPv4 アドレス枯渇対応タスクフォース「ISP サービスの IPv6 対応ガイドライン」[8]の「必要条件」を満たしているかどうか確認する必要がある。このガイドラインは総務省発行の「インターネットサービス等の IPv6 対応に係る基本指針」に準拠しており、IPv6 接続サービスについて最低限求めていることを記載している。これが満たされていないサービスについては、採用しない方が望ましいであろう。

通信機器やネットワーク回線については上記のようであるが、IPv6 対応をする際には、システムそのものの改修が必要になる可能性がある。ホームページでの情報提供等、情報公開に利用しているだけの場合は、あまり大きな改修作業は必要ではないが、電子入札システムをはじめとした認証を必要とするシステムやアプリケーション等によりサービスを住民・企業等に提供している場合には、そのシステムの内容次第で、IPv6 対応のための開発コストがかかる場合がある。

それでは、IPv6 対応に必要なコストについて検討する。

（1）機器調達のコスト

機器調達については、現時点で利用している機器が IPv6 対応であるかどうかによって異なる。現時点で IPv6 対応の機器が導入されている場合、基本的に新規のコストはかからない。ただし、IPv6 対応の方法としてトランスレーション方式を利用する場合には、その機器（トランスレーター）の導入コストが別途かかる。

それに対して、現時点の機器が IPv6 対応をしていない場合には、IPv6 対応の機器に入れ替えるコストが発生する。機器の値段としては IPv4 対応のものとほとんど変わらない値段で入手することが可能であるため、更新時期に合わせて調達した場合にはコストは同等で済む。しかし、レンタル／リース期限が 2014 年（平成 26 年）以降である場合等に、レンタル／リース期限前に更新をする場合には違約金等のコストが別途かかる可能性がある。

なおトランスレーション方式を利用する場合は、現行の機器の入れ替えは必要ないが、トランスレーターを導入するコストが別途かかる。実際の価格についてはシステムの構成や規模によって大きく異なるため、ベンダーに見積りを依頼する必要がある。なお、比較的新しい技術への対応になるので、見積りに際しては複数の事業者に依頼して、適正な値段を把握する必要がある。

（2）ネットワーク回線調達のコスト

現在地方公共団体で利用しているネットワーク回線は、基本的に IPv6 に対応した契約にはなっていないと考えられる。そのため、IPv6 に対応した契約に切り替える必要がある。

民間の ISP を利用している場合、利用している ISP が IPv6 サービスを提供しているか

[8] http://www.kokatsu.jp/blog/ipv4/data/isp-guideline.pdf

どうかを確認する。先述した「ISP の IPv6 対応について[9]」にも記載されているように、大手の ISP では対応が進んでいるが、中小の ISP では対応していないところが多くある。ただし、現時点でホームページ上に情報が無くても、対応を予定している事業者はあるので、現在契約中の ISP 担当者等に確認をする必要があるであろう。なお、コストは利用したい回線容量等によって大きく変わる上、まだ始まったばかりのサービスが多くて価格も異なることから、これを機会に複数社から見積りを取得して検討した方が良いであろう。一般的に、現在利用している回線料金よりも高額になると考えられる。

次に地方公共団体の提供する地域情報ハイウェイを利用して外部と接続している場合、地域情報ハイウェイそのものが IPv6 化しているか、もしくは IPv6 対応を予定しているかを確認する必要がある。

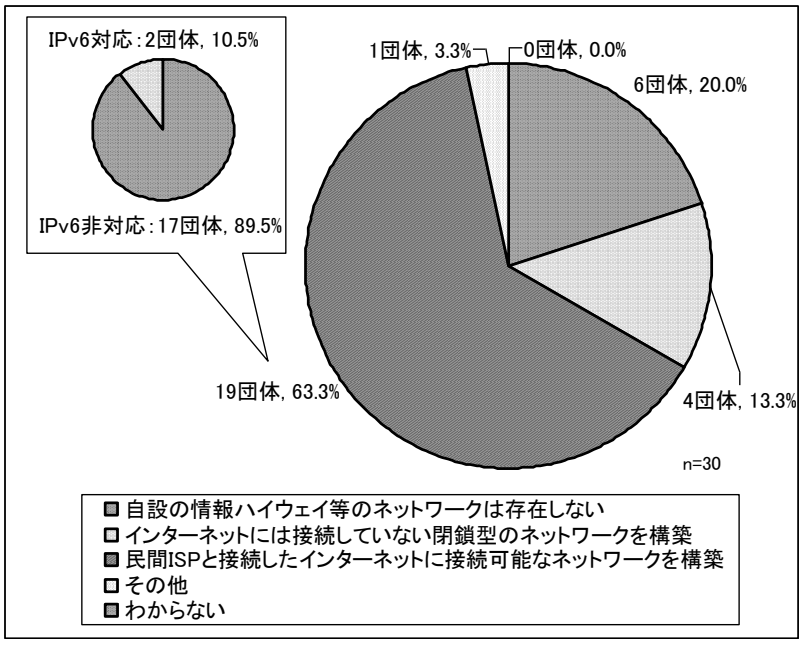

図 2-10　独自ネットワークの構築状況（都道府県）

現時点で IPv6 サービスを提供しているのは、前述のアンケート結果によれば 2 団体しかないので、その他の都道府県の市区町村では、地域情報ハイウェイの IPv6 化予定を確認する必要がある。地域情報ハイウェイが早々に IPv6 化を予定していればそれを待つという選択肢があるが、当面 IPv6 化の予定がない場合、新たに民間 ISP と契約することを検討する必要がある。民間 ISP と契約を行う場合、その回線費用が新たにかかるコストである。

地域情報ハイウェイを提供している都道府県については、地域情報ハイウェイそのものを IPv6 化することを検討する必要がある。今後は IPv6 によるアクセスに対応しなくては

[9] http://www.jaipa.or.jp/ipv6/

ならないため、市区町村としても地域情報ハイウェイに IPv6 化を求めることになるであろう。それに対応できない場合、市区町村は地域情報ハイウェイとは別に民間 ISP とも契約することになり、結果的に地域情報ハイウェイが使われなくなることが懸念される。なお、地域情報ハイウェイの IPv6 化にかかるコストについては、本節でとりあげている機器調達のコスト、ネットワーク回線の調達または対応のコスト、サービスを IPv6 化するコストが考えられる。つまり、機器調達については更新時期に調達すればコストは同等、ネットワーク回線については増額、サービスの IPv6 対応についてはサービス次第だが基本的にコストがかかる。

（3）システムの IPv6 化にかかるコスト

システムの IPv6 化については、幾つかパターンを分けて考える必要がある。

まず IPv6 アドレスに対応したシステムを構築しているかどうかの確認が必要になる。これは構築を担当したベンダーに問い合わせることになるが、例えば認証時やデーターベースの処理などに IP アドレスを利用している場合、そこで IPv6 アドレスを受け入れられないようになっていたり、利用しているソフトウェアが IPv6 対応をしていなかったりする場合は、IPv6 には対応していない。それに対して、通常は IPv4 アドレスで利用するが、必要な処理（設定の変更、ソフトウェアの再構築等）を行うことで IPv6 に対応することができるという回答が返ってきたシステムの場合は、対応していると考えて良いであろう。

システムが IPv6 に対応している場合は機器も対応していると考えられるので、ネットワーク回線を対応させて、IPv6 用の設定を行うだけである。そのため、システムとして大きなコストがかかることはないであろう。

また、公式ホームページ等のうち、情報提供にのみに使われているウェブサイトは、サーバーの設定変更だけで IPv6 に対応できる場合が多いため、あまりコストをかけずに IPv6 化ができると考えられる。

次に、システムが IPv6 に対応していない場合は、機器とネットワーク回線を対応させた上で、システムを IPv6 対応させるための開発コストがかかる。このコストはシステムの規模によって異なるが、相当のコストがかかる可能性があるため、既存システムの改修を実施するか、新たに IPv6 対応のシステムを発注するかを比較検討する必要があるであろう。なお、IPv6 対応は地方公共団体共通の課題のため、既に複数の地方公共団体で同じシステムを共同利用しているような場合には、IPv6 対応を協力して実施することで、1 団体当たりの負担コストを低く抑えることも可能であろう。

IPv6 対応としてトランスレーション方式を利用する場合は、システム開発のコストは基本的にかからない。しかし、来訪者のログ解析等、来訪者の IP アドレスを必要としている場合は、トランスレーターを介すとその情報が別の形でくることになるため（拡張ヘッダ等に元 IP アドレスが記載された状態でアクセスが来る。）、対応が必要になる。また、トランスレーションが可能なシステムかどうかということは、トランスレーターとして利用す

る機器やソフトウェアにも依存するため、トランスレーション方式で対応可能なシステムであるかどうかを確認する必要がある。この方式で対応可能な場合、コストとしてはトランスレーターの導入費用と、必要な場合はIPアドレス周りのシステム改修をする費用以外にはかからない。

2.3.5. 移行スケジュール

2.3.5.1. 現行のシステムに関する期間の整理

移行スケジュールの検討に当たっては、まず現行のシステムの保守期間等を整理する必要がある。

2.3.2で機器のリース期間等を把握することを求めているが、併せて、対象となるシステムについても、保守期間がいつまでか、システム更新予定時期はいつか等について整理して、一覧表にまとめる必要がある。

2.3.5.2. 移行スケジュールの策定

地方公共団体のシステム、情報機器の更新時期について整理ができたら、それをもとに移行スケジュールを確定する。

情報機器については、2.2で述べたとおり、IPv6対応を要件に入れて、粛々と対応させることが望ましいと考えられる。先も述べたとおりコストが大きく変わるわけではないため、通常の予算どおりで機器レベルでのIPv6化を行うことが可能である。

ただし、フロントシステムと、フロントシステムに関連する情報機器については、先述のとおり、遅くとも2013年度（平成25年度）、可能であれば2012年度（平成24年度）中にIPv6対応ができるように計画を組む必要がある。検討期間と予算措置を考えると、最速でも2年後に構築となることから、2011年（平成23年）初頭から検討を開始して、更新ができるようにすることになるであろう。

なお、2011年（平成23年）、2012年（平成24年）にシステム更新を検討している場合、その更新にIPv6対応が含まれていなければ、一度計画を凍結して、IPv6対応のシステムへの更新として再度計画を立てる方が望ましいと考えられる。

2.3 の重要ポイント

- フロントシステムについては、2012 年度（平成 24 年度)、遅くとも 2013 年度（平成 25 年度）までに IPv6 化を行う必要がある。
- ASP を利用してサービスを行っている場合は、ASP 事業者に対して IPv6 対応を求めることで対策ができる。
- 独自で提供している場合は、機器、ネットワーク、システムのそれぞれについて対応が必要となる。
- 対応方法は複数あるため、現在の各地方公共団体のシステム構成と、IPv6 対応にかかるコストをもとに、最適な手法を選択する必要がある。

2.4. セキュリティーについての検討

2.4.1. セキュリティー課題の内容

IPv4 アドレス在庫枯渇に伴う緊急的な IPv6 対応は、2.3 で記載したとおり、基本的にはフロントシステムの対応となる。方法としては 2.3 で記載したように、（1）独立方式、（2）デュアルスタック方式、（3）トランスレーション方式があるが、それぞれセキュリティー上の課題が生じることがある。ここで生じるセキュリティー上の課題は解決可能なものであり、必要な対応を行うことで解決できるが、IPv6 においてもセキュリティーは重要な課題であり、IPv4 と同等以上に注意を払う必要がある。

まず（1）と（2）の場合だが、既存のシステムでは、住民向け等に提供しているサービスについて、ウェブサーバーまではアクセス可能にするが、内部のシステムと繋がっている部分にはファイアーウォール等を入れて、セキュリティーを確保している。ここで、内部システムとのやりとりを IPv4 で行っているのであれば、既存のセキュリティー製品で対応できる。それに対して、内部システムとの間も IPv6 でやりとりするように構成する場合、IPv6 に対応したファイアーウォール等をいれることで、セキュリティーを担保しなくてはならない。この際に、IPv6 に対応したファイアーウォール製品が少ないということが一つのネックとなる。

また外側を IPv6 対応にした場合、アクセス制御リスト（Access Control List: 以下「ACL」と言う。）の設定に気をつける必要がある。ACL の設定は IPv4、IPv6 の双方について設定する必要があるため、IPv4 についてはきちんと設定されているが、IPv6 についてはアクセス制限が無くなっていて、外からのアクセスを無制限に受け付けているという状態になっている可能性がある。これは自ら外側の機器について IPv6 に対応したのではなくても、OS のアップグレードやファームウェア（機器に内蔵された基本ソフト）のアップグレードによってユーザーの知らないうちに機器が IPv6 対応になっている可能性もあるため、注意して確認する必要がある。

次に（3）トランスレーション方式の場合は、これは基本的に今までどおりのセキュリティーで可能だ。ただし、IP アドレスをキーにしたシステムがある場合、トランスレーターを通り抜けたアクセスの IP がトランスレーターの持っている IPv4 アドレスになってしまうので、利用ができなくなることに注意する必要がある。また、セキュリティー等の目的で通常各システムはアクセスログを取得しているが、その場合も単に IP アドレスを記録しているだけではトランスレーターにより変換されたアドレスしか残らない。トランスレーター製品は元の IP アドレスを拡張ヘッダ等に記録して通信を行うので、その拡張ヘッダに残っているアドレスをログに記載するようにシステムを改修する必要がある。

また（1）～（3）のすべてに共通する課題として、アクセスログの保管方法がある。IPv6

アドレスはMACアドレス（ネットワーク上の機器に固有の物理的アドレス）を元に生成されるため、利用者の特定がIPv4アドレス以上に容易になる。そのため、ログが漏洩しないように、ログの保管体制については改めて検討しておく必要があるであろう。

またIPv6特有の課題としては、ビッグパケット問題がある。これはトンネル接続という方法（IPv6パケットにIPv4パケットのヘッダをかぶせて、IPv4パケットとして途中経路を通し、目的地でIPv6に戻す。）で接続されたときに起きる問題で、パケットサイズが大きくなりすぎて、途中の通信機器を通れなくなるという問題である。これが起きると、住民が地方公共団体のホームページにアクセスした際に、アクセスしてから反応が返ってくるまで数十秒以上かかったり、アクセスできなかったりする。

この問題はサービス提供者が利用している回線と、住民の利用している回線の双方で発生する可能性があるため、少なくとも提供側では問題が起きないように、地方公共団体はISPを選ぶ必要がある。2.3フロントシステムのIPv6対応でも記載しているように、「ISPサービスのIPv6対応ガイドライン」の条件を満たしたISPを採用することが望ましいであろう。

2.4.2. セキュリティー課題への対応

上述のセキュリティー課題については、IPv4とIPv6は基本的に同じIPというプロトコルなので、IPv6について気をつける場所はIPv4と同じである。そのため、IPv4で実施しているものと同等のセキュリティーチェックを行うことで解決可能になるが、現在のセキュリティーレベルが低い場合は、IPv6についてもセキュリティーレベルが同様に低い状態になってしまうので、IPv4と同等以上に注意を払う必要がある。

なおセキュリティー製品については、完全にIPv6に対応している機器は少なく導入時には対応の有無を確認する必要があるが、IPv6に対応している機器は基本的にIPv4アドレスについて提供されているものと、価格がほとんど変わらない。そのため情報機器の更新の際に対応製品に入れ替えるのであれば、コストはかからない。現在は対応製品が少ないところだが、各ベンダーはIPv4アドレス在庫枯渇を見据えて対応を進めているし、世界的に需要が伸びており対応は加速している。

2.4.3. 内部システムの対応方針についての検討

当面はフロントシステムのみをIPv6化することで対応が可能だが、今後、LGWANのIPv6化等が起き得ると考えると、LGWANに直結して利用している内部システムについてもIPv6対応を行うことを検討する必要がある。

この点については緊急対策ガイドの範囲を超えるため詳細には記載しないが、下記のようなことには気をつけておく必要があるであろう。

・ 内部システムの IPv6 化を行うと、IPv4 のようにプライベートアドレスではなく、グローバルアドレスの体系で内部システムが構成されることになる。
⇒ACL の設定等を適切にしておかないと、情報漏洩が起きることに繋がる。
・ LGWAN と情報系のネットワークのそれぞれに一つの端末から繋いでいる場合、アクセス制御を IPv4/IPv6 双方について実施する必要がある。マルチプレフィックス問題[10]への対応。
・ IPv4 を完全に捨てるわけにはいかないので、共存することになり、コストは高くなる。ただし、IPv6 に完全に切り替えられるのであれば、コスト削減の可能性はある。

2.4 の重要ポイント

● フロントシステムを IPv6 化することで、セキュリティー上の課題が発生するが、IPv4 で実施しているものと同等のセキュリティー項目についてチェックをすることで、このセキュリティー課題については解決可能である。ただし全体的なセキュリティー向上のため、IPv4 以上の注意を払うことが必要である。
● トランスレーターを利用する場合、IP アドレスをキーとして利用しているシステムが無いかを確認して、ある場合にはそのための対応を取る必要がある。

[10] IPv6 では端末等は複数のアドレスグループに属することが可能ある。片方のアドレスグループが閉域網の場合には、インターネット宛ての通信が間違って閉域網に取り込まれてしまい、インターネットと通信出来ないことが発生する場合がある。

2.5. アドレス設計における最適化計画の検討

2.5.1. アドレス設計の最適化の必要性

インターネットやリモートアクセスネットワーク等の外部向けのシステムをIPv6対応する際、内部ネットワークと連携するシステムが存在する場合には、IPv6 と IPv4 の両方を管理する必要性が同時に生じる。また、既に、Windows Vista 以降の OS 搭載の PC 等、IPv6 対応の機器の導入が内部のネットワークで始まっている場合、そこが物理的に孤立したネットワークとなっていない限り、外部向けシステムの IPv6 対応との関連で、当該機器に対する管理も同様に IPv6 と IPv4 の両方が必要となる。

電子行政の推進により、業務や部局ごとに固有だったシステムが統合される方向にあり、多くの地方公共団体では、システム更新タイミングを見極めつつ、これらの、IP アドレスを必要とする機器による最適化の作業も進めているところと思われる。最適化に当たっては、これまで個別ばらばらだったシステムをハード、ソフト、運用、保守、更新等の全体で総コストが最小化するように見直しを図り、システムの性能向上の時期を適確に判断しながら必要な統合化の手順を明らかにする。

この最適化の際には、個別のシステムで使用していたプライベート IPv4 アドレスが各々で重複していたり、管理の纏まりや方法が異なっていたりしていて、ネットワークの統合が困難になってしまう例が少なくない。特に、IP 電話の導入が伴う場合には、大量のアドレスを必要とするので、ネットワークの設計がより難しくなる。

ネットワーク統合によるシステム最適化に関しては、IPv6 アドレスによる設計を基盤として到達像をあらかじめ想定しておくことで、これらの困難を低減することが可能である。最適化の推進過程では、各々のシステムやそれを構成する端末等を、順次、接続していくことになるが、IPv6 の豊富なアドレス数を使えば、端末数の増大や変更、さらに、管理単位の柔軟な設定や変更に余裕をもって対応できる。すべてを統合化しなければならないというわけではなく、個別システムのまま改修して利用し続けるという場合もあるはずだが、こうしたケースでも、将来的に接続する場合のアドレス設計を行っておくことで、長期的な視野の中に含めて考えていくことができる。

以上のように、IPv6 による設計で到達像をあらかじめ想定しておくことで、様々なシステムが統合されて大規模化するネットワーク上の大量の機器やその動作の状況に対しても統合的な管理を行うことが可能となる。

特に、今後の調達では、ほとんどの機器がIPv6対応となっていることが予想されるので、システムの更新時期と合わせた新規導入であれば、IPv6 によるコスト増は無いに等しいと言える。それよりもむしろ、余裕のあるアドレス数で管理できる IPv6 を優先し、IPv4 での管理を最小化していく事で、トータルな面での管理運用コストを低減させる効果も期待できる。

これまでの地方公共団体のシステムに関しては、統合ネットワークによってシステムを接続していく構成を前提にしていない場合が大半であったことから、IPv4 アドレスの設計も十分には行われていないものと考えられる。これ以降は、もはや、IPv4 アドレスではなく IPv6 アドレスによる設計を基本とした方が、最適化を進める上でもより望ましい成果を期待できる。

2.5.2. 対応方針の検討例

都道府県や大都市の場合は、システムの種類も多く規模も大きいことはもちろん、共通基盤等もある程度整備されているものと考えられる。しかしながら、統合されたネットワーク基盤ですべてを網羅している例はまだ少なく、各システムが個別に外部ネットワークと接続しているケースの方が多いのが実情と言える。支局や区役所等の地域拠点が存在するとともに、部局の中には独立性の高いシステムを導入して、独自に地域拠点を有して専用に接続している例もあるものと考えられる。

こうした大規模モデルの場合は、国の電子政府システムとの接続も考慮する必要があり、都道府県の場合は市町村との接続も必要となる。地方公共団体とはいえ、政府や大手企業を含めた体制で、統合ネットワーク基盤の整備に基づいた最適化計画の検討と実行を図ることが求められる。

（1）最も多い状況

外部とのネットワークも住民向けホームページ程度で、庁内には個別のシステムが各々稼働しており、職員の端末も一部にインターネットを利用できないという状況は、多くの中小市町村に当てはまるものと考えられる。また、アプリケーションのカスタマイズ度合いにも留意し、IPv4 アドレスを直接プログラムに書き込んでしまっているような場合については注意が必要だが、こうした状況は、該当する地方公共団体も多く、対応方法については、ソフト開発に係る業界団体等での報告や事例整理による情報を活用することで、効率的に導入できるようになるものと期待される。これらの対応方法を踏まえ、統合ネットワークの活用を契機とした最適化について、幾つかのオプションを有するパターンで作成することが求められる。

（2）ネットワーク統合が進行中のケース

外部のネットワークと個別に接続されているものの、一部のネットワーク統合が進みつつある場合には、既に導入された機器の IPv6 対応度の確認も含めて、最初から IPv6 対応の最適化を図るよりも難易度の高い最適化の作業となると考えられる。整備が進みつつあるネットワークの共通化の状況を、各地方公共団体で詳細に共有しながら、複数のソリューションを想定し、企業等にベストな提供方法を提案してもらう検討体制を整えて作業す

る必要がある。

（3）ネットワーク統合が終了している場合

ネットワークの共通化等によって統合的に接続が管理されているモデルで、ほとんど、すべてのシステムが繋がっている場合は、IPv4 段階でも統合管理の仕組みが進んでいるものと考えられる。IPv6 への対応について、機器の状況を確認しつつも、LGWAN や外部ネットワークとの IPv6 接続状況を判断しながら、最適化計画を進める。特に、この状況は、IPv6 に対応した最適化のあるべき姿としての性格も有するので、その実現のため、他の地方公共団体での適用実例を関係団体によって収集蓄積する事で、有効な共有知を形成できる。

（4）クラウドサービスの導入を進めている場合

ネットワーク経由で外部のサービスを使う SaaS 型への移行を目指す場合、外部とのネットワーク接続の管理運用に焦点を絞り、内部は端末の管理を主に実施していれば済むようになるという想定が可能である。管理運用のための自職員の育成と配置を行うか、アウトソースを活用し、自職員としては判断と指示だけをすれば良いように体制を移行させるかが考えられる。この場合、地域のネットワーク技術者との連携を軸に検討するとともに、その人材育成の面において、同じように外部サービスを利用する地方公共団体同士でユーザー会等の関係団体の活用や協議の場の確保によって協働できるようにすることが重要である。

（5）人材育成に関する検討

特に、IPv6 ネットワークの管理運用ができる人材や企業サービスは、まだ限られているのが現状であり、政府の人材育成支援等を要請しながら、地方公共団体の発注力を活用した取組も重要である。企業に複数の地方公共団体の管理運用のアウトソースを受けられる体制ができていけば、これまでのシステム管理運用のコストと比較しても低減させていくことが可能である。

2.6. 緊急対策実施のための参考情報について

2.6.1. 全般的な情報の提供

2.6.1.1. 財団法人地方自治情報センター

財団法人地方自治情報センター（以下「LASDEC」と言う。）では、本ガイドを IPv4 アドレス在庫枯渇及びその対策についての地方公共団体向けの総括的な情報源の一つとして提供したところである。また IPv4 アドレス在庫枯渇に関連して、事業者やベンダー、一般ユーザー等の対応状況は時期に応じて変化していくため、最新の関連情報の提供を継続的に行っていくことが必要である。このため、IPv4 アドレス枯渇対応タスクフォースに引き続き参加し、周辺動向の情報を収集しつつ、ホームページやメールマガジン等を通じて継続的な情報提供に努めていく。

そのほかに、地方公共団体が実際に IPv6 対応を進めるに当たって、それぞれの既存システムの状況に合わせて具体的な対応方法を相談できる窓口や他の先行事例の情報を参照できる窓口なども必要になってくると考えている。これらの相談は主に地方公共団体のシステムを手掛けるベンダーやシステムインテグレータ、コンサルティング等が担うことになると考えられるが、特定のベンダーやシステム構築ソリューションに依存しない中立的な一次相談窓口の存在も重要になると考えられる。IT コーディネーターや一部の ICT 系業界団体等がその役割を担っていく可能性があるが、そのような環境整備が進んでいくことは重要である。

2.6.1.2. 総務省

総務省は、IPv6 の普及を政策の一つとして、そのための各種施策を実施している。特に IPv4 アドレスの在庫の枯渇が間近に迫るなか、様々な研究会での検討を通じて、在庫枯渇の時期やその影響の検討を行い、その対策として下記に示すような各種ガイドラインや指針等を策定し、IPv6 移行に向けて広く参照される情報を提供してきた。

（1）「電子政府システムの IPv6 対応に向けたガイドライン」
（2）「インターネットサービス等の IPv6 対応及び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基本指針」
（3）「ISP の IPv4 アドレス在庫枯渇対応に関する情報開示ガイドライン」

また、ISP やデータセンターの IPv6 対応について、2006 年度（平成 18 年度）より年次調査を実施し、IPv6 の普及動向をモニタリングしている。これによりユーザーが IPv6 を利用できる度合いがどの程度増加しつつあるかを把握し、次の IPv6 普及施策へと活かしている。

総務省による「IPv6 の普及促進」に係る情報全般については、総務省のホームページ（下記 URL）を参照のこと。

http://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/index.html

2.6.1.3. IPv4 アドレス枯渇対応タスクフォース

IPv4 アドレス枯渇対応タスクフォースは、IPv4 アドレスの在庫の枯渇が間近に迫る中、情報通信やインターネットに係る団体が相互に情報を共有し、共同で対応を調整する組織として発足した。現在、総務省及び 22 の団体が参加し、その中には、電気通信事業者の団体、ISP の団体、CATV ネットワークの団体、データセンターの団体、機器ベンダーの団体、インターネットやシステムに係る団体、そして地方公共団体の情報化に係る団体等が広く参加している。

そして、IPv4 アドレス在庫枯渇に関する最新情報の展開、枯渇対策のためのマスタープラン（アクションプラン）の策定、ISP 等が IPv6 に対応する際の要求仕様の策定、IPv6 技術者の教育活動支援等を実施している。

IPv4 アドレス枯渇対応タスクフォースより提供される各種情報については、同団体のホームページ（下記 URL）を参照のこと。

http://www.kokatsu.jp/

2.6.1.4. IPv6 普及･高度化推進協議会

IPv6 普及･高度化推進協議会は、政府による e-Japan 戦略の開始に合わせて 2001 年（平成 13 年）に発足し、IPv6 に関する普及・啓発活動、技術研究開発活動、実証実験活動、政策立案活動、国際交流活動、さらに各種ガイドラインの策定等の活動を実施してきた。具体的には、IPv6 の普及・高度化に係る各種課題に合わせて、IPv6 対応機器の仕様適合／相互接続に関する検討、ステークホルダーごとの IPv6 移行のガイドラインの検討、さらに最近では、家庭用ルーターが備えるべき IPv6 機能の検討、ISP 等の技術者が実践的な検証を行い、運用経験を積むための IPv6 テストベッドの運営、総務省の指針に対応した IPv6 人材育成カリキュラムの認定等の活動を実施している。特定の業界分野を問わず、あらゆる法人、個人を対象とした会員制度となっており、会員向けに様々な情報を提供している。

IPv6 普及・高度化推進協議会より提供される各種情報については、同団体のホームページ（下記 URL）を参照のこと。

http://www.v6pc.jp/jp/index.phtml

2.6.1.5. 各種事業者やベンダー等の窓口

LASDEC として特定の事業者を推薦することはできないが、IPv6 に対応した事業者について、リスト化された既知の情報を以下に紹介する。

（1）IPv4 アドレス枯渇対応タスクフォースによる IPv6 サービスリスト
http://www.kokatsu.jp/blog/ipv4/data/ipv6service-list.html

（2）総務省による「IPv6 接続サービスの提供状況に関する調査」の結果（事業者リストを含む）

http://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/pdf/100421_1_i1.pdf
http://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/pdf/100421_1_a1.pdf

（3）IPv6 Forum Enabled Logo Program による IPv6 対応 ISP のリスト
http://www.ipv6forum.com/ipv6_enabled/isp/approval_list.php

（4）IPv6 Forum Ready Logo Program による IPv6 対応機器のリスト
https://www.ipv6ready.org/db/index.php/public/

2.6.2. 調達仕様の書き方･ポイント等

フロントシステムを IPv6 に対応させたり、システムのリプレース等に伴う調達機器について IPv6 対応を条件づけるためには、調達仕様において IPv6 対応であることを記述することが必要である。本ガイドにおいても「2.2.2 調達仕様書案」や「参考資料 調達仕様書（案)」で具体的な記載例を紹介しているが、ここでは IPv6 対応であることを概略的に述べるにとどまっている。その時点での本格的な IPv6 利用を目的とはせず、将来的な IPv6 移行の容易性の担保を目的として IPv6 対応を記述する場合、ネットワークシステムの姿をきちんと設計し､IPv6 の利用範囲や機能的な対応のレベルを定めた上で調達･構築するわけではないため、概略的な記述にならざるを得ないのは仕方のないところである。

一方で、いずれ本格的に IPv6 への移行を開始する際には、IPv6 のどの機能にどこまで対応する必要があるのか具体的に検討･定義したうえで、調達仕様を記述する必要が出てくる。IPv6 は現実には幾つかの仕様の集合によって成り立っており、IPv6 によるネットワークシステムをきちんと動くものとして構築するためには、それらの仕様の集合のうち、必要なものを必要なレベルで指定しておく必要がある。また既存の IPv4 システムとの共存の方法にも幾つかの方法があり、採用する方法ごとに、技術的な中身に踏み込んで調達仕様を検討する必要が出てくる。

ただし、これらについて都度、1 から検討する必要はなく、複数の IPv6 推進組織が、仕様の技術的な中身に踏み込んで検討したうえで、製品やサービスの一定レベル以上の品質を確保し、相互間の接続性を担保するための仕様の集合体を策定し、広く公表している。したがってこれらを必要なレベルで引用することで、調達仕様の記述を不必要に細かくすることを避けることが可能である。以下この項では、これらの参照可能な仕様について紹介する。

2.6.2.1. サーバーシステムの IPv6 化のポイント

IPv6 普及・高度化推進協議会 IPv4/IPv6 共存 WG サービス移行 SWG
「IPv4 サーバ環境への IPv6 導入ガイドライン」
http://www.v6pc.jp/jp/upload/pdf/IPv6ServiceDeployment_Guideline.pdf

調達仕様にそのまま流用可能なスタイルの記述ではないが、サーバーシステムを IPv6 対応させる場合の設計パターンや留意点がまとめられている。どのようなネットワークスタ

イルを採用するかによって、調達仕様として考慮すべきパーツを知ることができる。

2.6.2.2. ルーター機器の IPv6 化のポイント

IPv6 普及・高度化推進協議会 IPv4/IPv6 共存 WG IPv6 家庭用ルータ SWG
「IPv6 家庭用ルータガイドライン」

http://www.v6pc.jp/jp/upload/pdf/v6hgw_Guideline_2.0.pdf

家庭用ルーターを対象とした仕様書であるため、そのまま地方公共団体のシステムに流用可能とは言えない。しかしながら、ISP からの接続先である企業や地方公共団体は、同じく ISP からの接続先である家庭と同様な点も多く、記載されている技術は非常に参考になる記述である。

2.6.2.3. 端末等の機器全般の IPv6 化のポイント

IPv6 Forum IPv6 Ready Logo Phase-2

http://www.ipv6ready.org/

実用レベルで IPv6 対応機器が満たすべき仕様についてまとめられている。また、テストと認証制度を伴って運用されているため、仕様の中身に触れることなく、認証取得製品を調達条件とすることで、機器の IPv6 対応品質を確保することが可能である。必要とする製品機能により、IPv6 Core Protocols、IPsec、IKEv2、MIPv6、NEMO、DHCPv6、SIP、SNMP、MLDv2 の技術カテゴリに分けて運用されているが、最低限、IPv6 Ready Logo Phase-2 の IPv6 Core Protocols の取得を条件とすることが必要である。また IPv6 Core Protocols は Host と Router に分かれており、ルーター機器については Router の認証を求めることも有効な手段となる。

2.6.2.4. ISP/iDC(インターネットデーターセンター)の IPv6 化のポイント

IPv4 アドレス枯渇対応タスクフォース サービスロゴ WG 技術検討 SWG
「ISP サービスの IPv6 対応ガイドライン」

http://www.kokatsu.jp/blog/ipv4/data/isp-guideline.pdf

IPv6 に対応した ISP が必要とされる機能と品質を定義しているものである。総務省の策定した「インターネットサービス等の IPv6 対応及び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基本指針」にも沿うものとして作られている。IPv6 インターネットへの接続性だけでなく、ISP サービスとして IPv6 対応が求められるものを整理し、必要要件を定義している。要件の要求度に応じて、「必須」「推奨」「その他」に分けられているため、「必須」を満たすことを調達条件とすることで、必要最低限の品質確保が可能である。

IPv4 アドレス枯渇対応タスクフォース サービスロゴ WG 技術検討 SWG

「iDC サービスの IPv6 対応ガイドライン」

http://www.kokatsu.jp/blog/ipv4/data/iDC-logo-step1-rev0.2-20110111.pdf

IPv6 に対応した iDC が必要とされる機能と品質を定義しているものである。総務省の策定した「インターネットサービス等の IPv6 対応及び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基本指針」を受けて、iDC が最低限満たすべき要求条件について整理すると共に、iDC の運用条件等も加味した各 iDC に共通する要求条件を整理した拡張仕様となっている。要件の要求度に応じて、「必須」「推奨」「その他」とに分けられているため、「必須」を満たすことを調達条件とすることで、必要最低限の品質確保が可能である。

2.6.3. システムの IPv6 対応に向けての検証環境

既存のシステムをリプレースしたり、新たなシステムを導入しようとする場合、新しいシステム環境が設計どおりに不具合なく動作するか、既存のシステムに悪影響を与えないか、想定外の問題を起こさないか等について、事前に検証することが重要である。特に IPv6 のように、現時点では導入事例が少なく、ベンダーやシステムインテグレーターの経験が浅い分野においては、この点はより重要である。

システムの IPv6 対応に向けた検証環境として、特定のベンダーによらず幅広いユーザーが利用可能なものとしては、2011 年（平成 23 年）2 月現在において、IPv6 普及･高度化推進協議会が運営する IPv6 検証環境（テストベッド）が、東京（新川崎）と大阪（西梅田）の 2 ヶ所にある。こちらは ISP 等の事業者が主な対象であるが、機器ベンダーやワールドワイドなイントラネット網を持つグローバルカンパニー等も検証のために利用している。

IPv6 検証環境（テストベッド）については、IPv6 普及・高度化推進協議会のホームページ（下記 URL）を参照のこと。

http://www.v6pc.jp/jp/entry/wg/2010/05/v4exh-testbed.phtml

また、実際のネットワーク機器を使って、IPv6 利用のための設定や運用技術を学べる場として、IPv4 アドレス枯渇対応タスクフォースが、IPv6 ハンズオンセミナーを実施している。こちらも主な対象は ISP 等の事業者のオペレーター（システム運用担当者）だが、企業等の情報システム担当者も受講をしている。

IPv6 ハンズオンセミナーについては、IPv4 アドレス枯渇対応タスクフォースのホームページ（下記 URL）を参照のこと。

http://www.kokatsu.jp/blog/ipv4/event/2011/03/ipv6-handsonseminar.html

この他に、一部のベンダーでは、自社機器向けの検証環境や、自社機器を取り扱うシステムインテグレーター、自社機器を導入した顧客向けの検証環境を持つところもあるようだ。

地方公共団体のシステムの IPv6 対応に当たって利用可能な検証環境としては、IPv6 普及･高度化推進協議会の IPv6 検証環境が考えられるが、現在の予定では、2010 年度（平成 22 年度）末で終了する予定となっている。また、基本的には事業者向けの検証環境であるという点もあるため、地方公共団体のようなシステムの利用者の立場で、利用するシステムを IPv6 に対応させたときの動作を事前に検証できる環境が求められていると言える。