IPv6 対応調達仕様書モデル

【地方自治体編】

２０１４年７月

目次

0. はじめに

0.1 はじめに

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

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

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

従って、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企業及び地方自治体が個別に確立し、実施することは極めて困難である。

このため、これらの関係者が、自らのネットワーク環境等を適切かつ円滑に IPv6 対応させることができるようにガイドライン及び調達仕様書モデルを取りまとめた。

0.2 本書の使い方（必ずお読みください）

本書は IPv6 対応ガイドラインとセットで利用することを想定している。ガイドラインでは、標準的なシステムやネットワークのモデル及び基本的な IPv6 対応シナリオをベースに、IPv6 対応の方法や検討上の留意点等を説明している。これを参考にすることで、IPv6 対応のための基本計画を作成することができるようになっている。

ガイドラインをベースに作成した IPv6 対応の基本計画にもとづき、IPv6 対応が必要な箇所について、調達上の要件等を整理することで、調達仕様書案を作成することができる。本書では、地方自治体における情報システム等を IPv6 対応させる際の基本的な調達仕様書のモデルを提示している。基本計画によって特定した IPv6 対応範囲や、基本計画に記載した対応上の留意点等を参考に、モデルの内容を適宜、抜粋、分割、修正等を行うことで、それぞれの地方自治体に応じた調達仕様書を作成できると考えている。

なお、本書の示す調達仕様書モデルは、基本的に IPv6 に対応した調達要件の記述に特化しており、通常のシステム調達仕様書に対する IPv6 対応のための追加要件として取り扱うことを前提としている。そのため、IPv6 対応以外のシステム要件（電源の冗長構成と通電障害時の切り替えが可能等）（冗長構成については用語集項番 3 参照）、機能以外の要件の内容（電話や電子メールでの 24 時間 365 日の障害対応専用窓口を持つこと等）、本モデルで取り扱う標準的なシステムやネットワークのモデル以外の要件（外部の Web アクセス統計分析サービスを利用すること等）を含めたシステム全体としての実現性を検討のうえ、最終的な調達仕様書として完成させることを想定している。

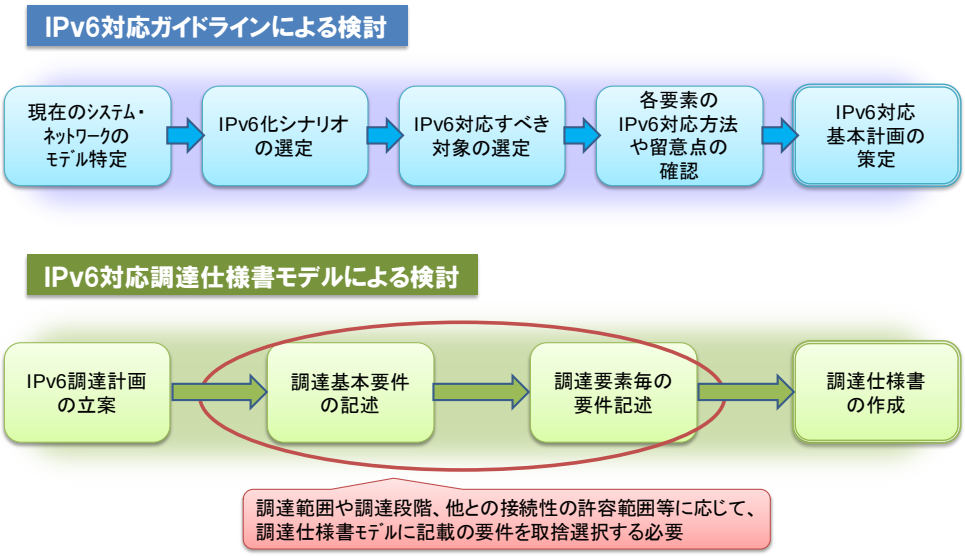

図 0-1　ガイドラインと仕様書モデルによる検討の流れ

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。このうち、本書は、調達仕様書の作成に向けた各種検討のうち、IPv6 機能の導入に係る参考となるものである。

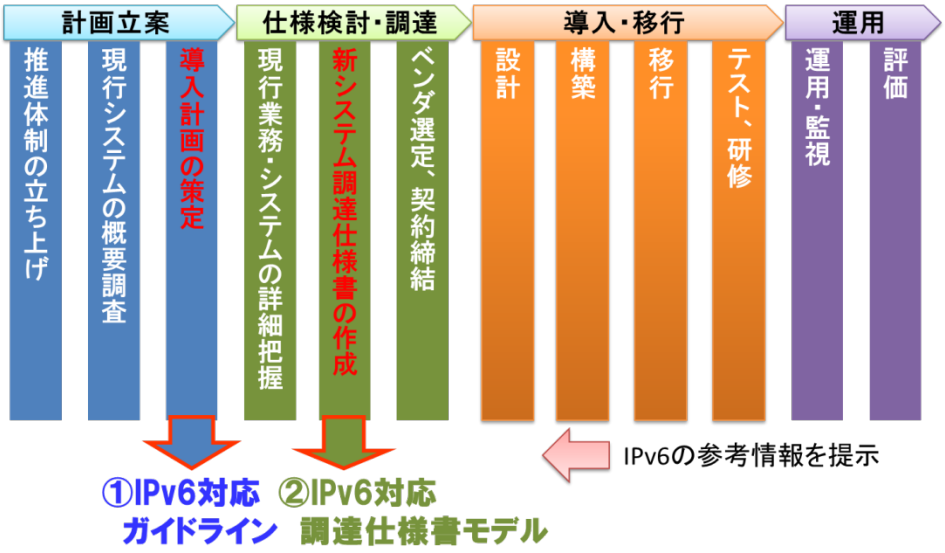

図 0-2　システム導入のフローと本調達仕様書モデルの対象範囲
出典：自治体クラウド・情報連携推進のための研修教材（総務省）を参考に作成

なお、本書における各調達要素は、物理的な機器等を想定したものではなく、機能を単位として記述している。これらの機能の実現方法としては、複数の機能を 1 つの機器で実現しているようなケースや、機器ではなく ASP やクラウド上のサービスとして展開しているケース等も考えられる。各自治体のシステム構築ポリシーや既存システム等の状況に応じて、本

書記載の機能を分離又は結合する等の調整が必要となる。また、具体的な実装プランをベンダの提案余地とするなど、本書に示した各調達要素の使い方に自由度を与えている。

本書における各章では、調達仕様書のモデルとして、それぞれ以下の内容を記述している。

1.概要
✓地方自治体のシステムやネットワークを IPv6 対応させる背景、調達によって実現する目標及び調達仕様書として何を記しているのか等について記述する。

2.想定するシステム、ネットワークの全体像
✓調達対象、対象外を含めて、調達後に構築を目指すシステムやネットワークの全体像を説明する。

3.調達範囲
✓システムやネットワークの全体像に対する調達の範囲を示す。なお、調達仕様書モデルにおいては、システムやネットワークの標準モデル、IPv6 対応基本シナリオに従った調達しうる最大限の範囲を示す。

4.調達にあたっての基本的な考え方
✓調達にあたっての基本的な考え方（調達時期や設置場所等）、調達単位の分割の考え方、他の調達単位との関係性等について説明する。

5.回線サービス
✓調達対象である回線サービスに対する技術要件及び運用要件を具体的に記述する。また、回線サービスに付随して提供されることの多い DNS におけるセカンダリネームサーバについて、情報の格納や提供に関する条件等の IPv4/IPv6 共存環境に対する稼働条件を提示する。

6.リモートアクセス及びインターネット VPN
✓調達対象であるリモートアクセスやインターネット VPN サービスに対する技術要件及び運用要件を具体的に記述する。また、IPv6 に対応していないアプリケーションやサービスをリモートアクセスやインターネット VPN で利用する場合の条件等 IPv4/IPv6 共存環境に対する稼働条件を提示する。

7.機能及びサービス
✓調達対象である機能やサービスに対する技術要件及び運用要件を具体的に記述する。

8.運用及び保守要件
✓調達対象である保守作業に対する要件を具体的に記述する。特に、IPv4/IPv6 共存環境での留意すべき点等への言及を行う。

9.その他の留意事項
✓上記の他に付加すべき要件や、既存システムと接続する際の依頼事項等、留意すべき点について記載する。

10.（参考）IPv6 対応チェックシート

✓調達仕様書モデルに基づいて作成される調達仕様書は、1～9 までの抜粋や記述の修正によって構成されることを想定している。ここでは、各章の記述に対応づけて、調達範囲等を絞り込むためのチェックシートと、チェック結果に基づく対応フローを提示する。チェックシートに従ったチェックを行い、フローを追跡することで、全体システムにおける調達範囲や調達区分の考え方を反映した調達仕様書案を得ることができる。

11.（参考）参考文献

✓本文中の各記述に対応した参考文献を紹介する。

1. 概要

1.1 案件名

「外部向けサービスに関する IPv6 対応システム及びネットワークの調達」

1.2 目的

インターネット環境として各 ISP 事業者より IPv6 方式でのサービス提供が増えつつあるなか、今後、市の情報へのアクセスに IPv6 を利用する市民が増加することを見越し、ネットワークシステムの更新タイミングにあわせて、IPv6 方式に対応したネットワークシステム及び外部向けサービスシステムを調達することとした。

本調達により、市民がインターネットを経由して市のホームページや公開情報にアクセスする際に、新たに IPv6 方式でのアクセスを可能とすることにより、市民のインターネット環境によらず、公平に市の情報やサービスを提供することを実現する。また、市民以外のアクセスに対しても、より広範な情報提供の可能性を拓くことを実現する。

これらを実現するため、本調達仕様書では、外部向けサービス及びネットワークに関する調達対象を明らかにするとともに、要素毎の要求や要件、付帯条件等を明示するものである。

2. 想定するシステム及びネットワークの全体像

本調達範囲を含む本市が運用するシステム及びネットワークの全体像を下図に示す。なお、業務システム部分については今回の調達範囲外のため、模式化して示している。また点線の箇所は現状のシステム及びネットワークでは存在していない部分である。

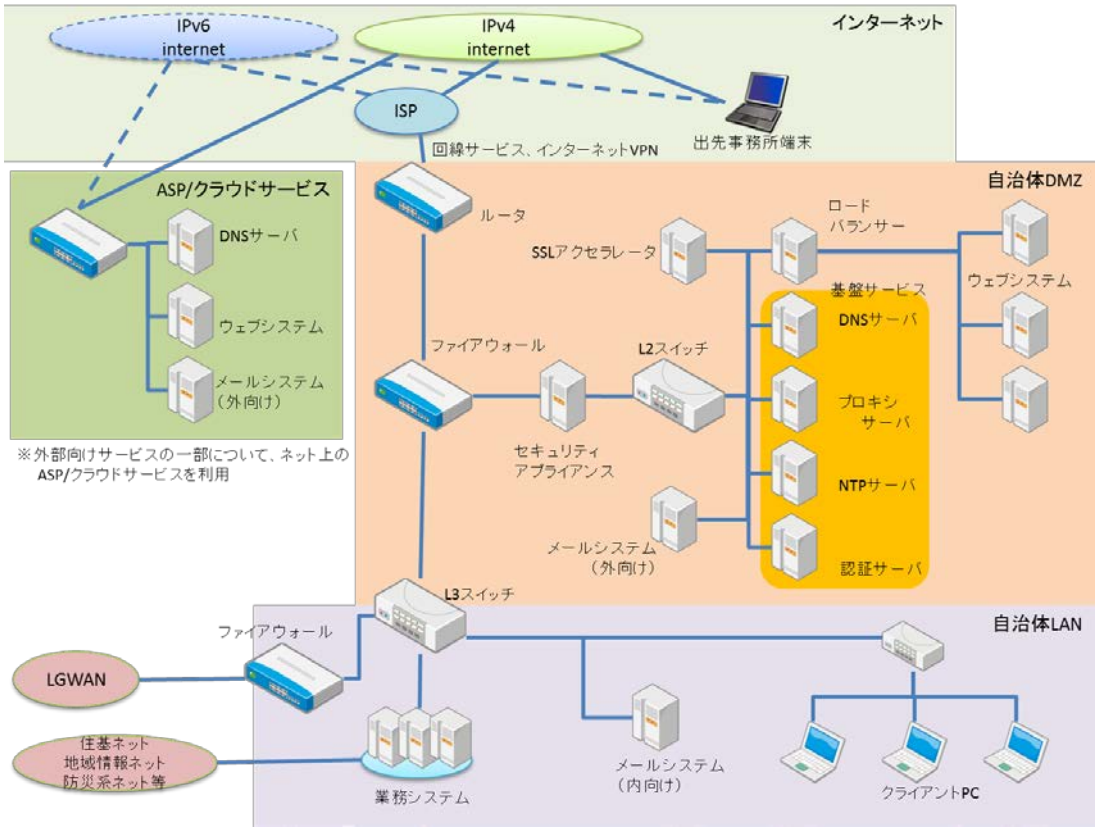

図 2-1　本市が運用するシステム及びネットワークの全体像

現状はいずれも IPv4 によって運用されており、個々の要素の概要は下表の通りである。

表 2-1　現在のシステム及びネットワークの構成要素の概要

機器、構成要素	概要
回線サービス	光回線経由で IPv4 固定アドレスによるインターネット接続をしている。自治体 DMZ（用語集項番 4）内におかれた外部向けサービスへのインターネットからのアクセスと、自治体 LAN 内のクライアントからのインターネットへのアクセスの両方に利用している。
リモートアクセス及びインターネット VPN	外部向けサービスの一部は ASP サービスを利用している。これらと自治体 DMZ 内の外部向けサービスの同期をとるためインターネット VPN サービスを利用している。また、少人数の出先事務所からはセキュリティを確保したリモートアクセスにより接続している。
ルータ	回線サービスの自治体側終端装置として自治体側に設置し、自治体ネットワークとインターネットとの接続に利用している。

機器、構成要素	概要
L3 スイッチ（用語集項番 5）	自治体 LAN を構成するコアスイッチとして利用している。
L2 スイッチ（用語集項番 6）	自治体 DMZ 内のスイッチや自治体 LAN 内のエッジスイッチとして利用している。
ファイアウォール	インターネットからの攻撃に対応するため、ファイアウォールを利用している。
セキュリティアプライアンス	インターネットからの攻撃及び侵入を検知し、不正な通信を遮断するため、侵入検知システム（IDS、用語集項番 7）、侵入防御システム（IPS、用語集項番 8）を利用している。
基盤サービス	ネットワークを運用するための基盤サービスとして、DNS（用語集項番 9）サーバ、プロキシサーバ、NTP（用語集項番 10）サーバ、認証サーバを利用している。
ロードバランサー	インターネットからウェブシステムへのアクセスの負荷分散を行うため、ウェブシステムの手前にロードバランサーを入れて利用している。
ウェブシステム	主に市民や市内の事業者／事業所向けの情報提供のためにウェブシステムを利用している。重要なお知らせやイベント時の負荷増に対応するため、複数台構成をとり、ロードバランサーにより負荷分散を行っている。
メールシステム	職員が業務用メールを利用できるよう、メールシステムを利用している。インターネットとの間でメールをやりとりする外向けメールシステムと、庁内で職員端末よりアクセスする内向けメールシステムからなる。
SSL（用語集項番 11）アクセラレータ	市民からの情報を守るため、ウェブ経由でのアクセスの一部（お問い合せ等）は暗号化通信を利用しており、この通信を高速に処理するために利用している。

3. 調達範囲

「2 想定するシステム及びネットワークの全体像」を踏まえた本調達の範囲を下図に示す。

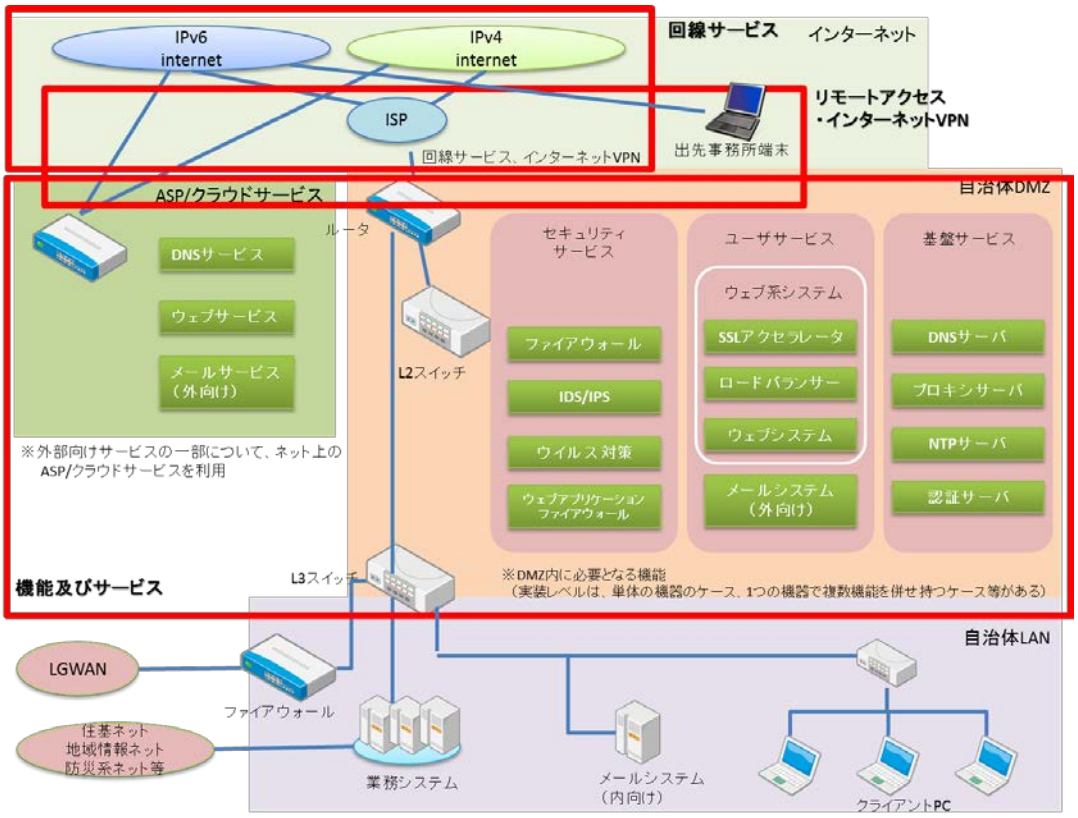

図 3-1　本調達範囲（赤囲い部分）

調達は「回線サービス」、「リモートアクセス及びインターネット VPN」、「機能及びサービス」の構築及びその「保守」からなっており、いずれも IPv4 と IPv6 の両方に対応したシステム及びサービスであることが基本となる。それぞれについて以下に記載する。

3.1 回線サービス

インターネットと自治体ネットワークとの間を接続するための回線サービスである。従来の IPv4 による接続に加えて、IPv6 による接続を併せて提供することが必要である。庁舎内に回線終端装置を設置し、回線終端装置までが責任範囲となる。またプライマリ DNS は自治体 DMZ 内に持ち、セカンダリ DNS は回線サービスを提供する ISP 事業者より提供を受けることを想定している。

3.2 リモートアクセス及びインターネット VPN

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

3.3 機能及びサービス

外部向けサービスの IPv6 対応を実現するため、自治体 DMZ 内の各機器（サーバ装置及びネットワーク関連機器）を IPv6 対応とする。なお、現在稼働する各機器が提供する機能をカバーするものであれば、統合型の機器やインターネット上での ASP やクラウドサービスの利用も検討範囲となる。そのためこれ以降は、機能及びサービスとして説明する。

3.4 保守

上記「回線サービス」、「リモートアクセス及びインターネット VPN」、「機能及びサービス」の保守を行う。それぞれが IPv4/IPv6 対応となることを前提としているため、保守においても IPv6 に対応した保守が必要となる。

4. 調達にあたっての基本的な考え方

本市では情報システム最適化基本計画を策定しており、業務プロセス及びシステムの標準化、共同化に向けた作業を継続的に実施している。今回、次期ネットワークシステムへの更新にあたって、IPv6 の全面的な導入を実現するため、本調達では、IPv4 に加えて IPv6 に対応した回線やネットワーク機器、外部向けサービスシステム等を導入するものである。

今後、ネットワーク以外の各業務システム等の更新にあたっても、IPv6 への対応が検討される可能性があるため、その際にもシステムに支障や制約を与えることがないよう、将来的な運用の継続性や拡張性に十分に留意したものである必要がある。

このため、まず、調達にあたっての全体要件を以下に示す。また、個々の要素単位での要件については、「5 回線サービス」以降に示す。

4.1 調達単位と調達スケジュール

4.1.1 調達単位

本調達の範囲は、「回線サービス」、「リモートアクセス及びインターネット VPN」、「機能及びサービス」及び「保守」とし、これらは一括して調達する。

また、機能及びサービスに関しては、「7 機能及びサービス」に示すような機能単位でその要件を提示するが、複数の機器の機能を備えた統合型機器による提案や、ASP やクラウドサービス等のネットワーク経由でのサービスの提案を妨げるものではない。なお、ネットワーク経由でのサービスを提案する際には、そのサービスの利用や運用に、本調達範囲の「リモートアクセス及びインターネット VPN」の利用を前提とする。

4.1.2 調達スケジュール

本調達の基本的な想定スケジュールを下表に示す。詳細な工程及び工程毎のスケジュールについては提案内容に含めることとする。

表 4-1　想定スケジュール（サンプル）

項目	時期、期間
設計	平成 26 年 7 月中旬～8 月下旬
構築	平成 26 年 9 月上旬～12 月下旬
システム試験	平成 27 年 1 月上旬～2 月中旬
ユーザ試験	平成 27 年 2 月中旬～3 月中旬
データ移行	平成 26 年 2 月中旬～3 月下旬
職員向け教育期間	平成 27 年 3 月上旬～3 月下旬
運用開始	平成 27 年 4 月

4.2 構築要件

4.2.1 庁舎内設置機器について

本調達範囲の「機能及びサービス」のうち、自治体 DMZ を構成する以下の各機器については、自治体 LAN へのネットワークサービス提供上必須の機器であるため、庁舎内サーバ室に設置することとする。

- ルータ
- L3 スイッチ
- L2 スイッチ

- ファイアウォール
- IDS/IPS
- 基盤サービス

上記以外の機能については、庁舎内サーバ室に機器として設置する方法、ASP やクラウドサービスによりネットワーク上のサービスとして提供する方法のいずれも可とする。

4.2.2 設置場所要件

庁舎内サーバ室には、システムの構築に十分な空きラックスペース、空き電源容量、空調能力が用意されている。また十分な配管スペースがあり、任意の回線を引き込み可能である。

提案にあたっては、システムの構築や設置に必要となるサーバ室への要求事項や要求される能力を見積もって提示すること。

4.2.3 ネットワーク上のサービスを利用する場合の要件

本調達範囲の「機能及びサービス」のうち、「4.2.1 庁舎内設置機器について」で指定した機器以外は、ASP やクラウドサービス等のネットワーク上のサービスを提供する提案も可能である。ただし、その場合には以下の要件を満たすこととする。

- 当該 ASP やクラウドサービスの利用や運用は、「6 リモートアクセス及びインターネット VPN」に示すインターネット VPN の利用を前提とすること。
- 構築費用と運用費用の比率が変わる可能性があるため、運用年数分の費用の一括支払等、調達者の要求する料金メニューに柔軟に対応すること。

4.3 全体として確保すべき非機能要件

現在のシステムはそれぞれ次項以降に示す各要件を満たす形で運用されている。本調達システムにおいても、IPv4/IPv6 いずれからのアクセスかに関わらず、以降の各要件を満足すること。

4.3.1 規模要件

表 4-2　規模に対する要求要件（サンプル）

要求項目	内容
データ検索回数	1,000 件／時
データ閲覧回数	1,000 件／時
ログデータ保管期間	5 年間
登録利用者数	300,000 人

4.3.2 性能要件

表 4-3　性能に対する要求要件（サンプル）

要求項目	内容
オンラインレスポンス	最大で 5 秒程度
オンラインスループット	1,000 件／時

4.3.3 信頼性要件

表 4-4　信頼性に対する要求要件（サンプル）

要求項目	内容
運用スケジュール	24 時間稼働
	故障時には 24 時間以内に要員を派遣できる体制を確保すること
稼働率	全体として 98%以上の稼働率を実現すること
拡張性	標準的なパーツを使用し、容易にシステムを拡張可能であること
事業継続性	故障時には代替機器／代替サービスを用いることで 24 時間以内に再開可能であること
	バックアップにより障害発生時にもデータやログを回復可能であること

4.3.4 セキュリティ要件

表 4-5　セキュリティに対する要求要件（サンプル）

要求項目	内容
利用者の権限	システム管理者、登録利用者、一般利用者を区別して権限管理できること
利用制限	システム管理者は、システムの全ての機能及びデータにアクセスできること
	登録利用者は、一般利用者が利用可能なコンテンツ及び登録利用者向けに制限された機能及びデータにアクセスできること
認証	ID/パスワードによる認証機能を備えること
	登録利用者が自ら、ID/パスワードの登録、変更、削除が可能なこと
権限管理	認証情報には、システム管理者のみがアクセス可能であること
	認証情報は、毎日完全なバックアップを取得すること

4.4 移行要件

本調達による新システムへの移行に際しては、下記に示すデータの移行に係る要件と利用者の教育に係る要件を満足すること。

4.4.1 移行に係る要件

- 既存システムから次期システムへ移行すべきと指定されたコンテンツについては、その全てを指定の期間内に次期システムへと移行すること。このデータには外部向けサービスに必要なデータ以外に、認証に必要なデータ、ログデータ等も含むものとする。
- 移行すべきデータについては、IPv6 に対応したテスト環境を用いて検証を行うこと。特にログデータ等については既存データのみならず、IPv6 環境で生成されるデータが混在した場合でも、監視や監査が問題なく実施可能であることを検証すること。
- IPv4 に関係するシステムの場合、システム移行時及び移行後に IPv4 サービスに問題がないことを事前に検証で確認すること。

- 移行開始から概ね 1 か月程度で完了する移行計画を策定すること。(数値はサンプル)
- 移行期間中においても、既存システムが並行稼働可能で、利用上の障害が発生しないような方策を手当すること。
- 次々期のシステム更改に際して、システム間のデータ移行を確実なものとするため、その際のデータアーカイブの出力までを確実に実施すること。

4.4.2 教育に係る要件

- 新システムの稼働にあたって、事前に関係者説明会を実施すること。
- コンテンツ管理者向けのマニュアルを用意し、特別な教育訓練なしに利用可能とすること。
- システム管理者向けのマニュアルを用意し、特別な教育訓練なしに利用可能とすること。
- IPv6 対応によって変更された運用手順などについて教育を行うと同時に、IPv6 全般の知識も獲得できるように、教育用コンテンツの内容に配慮すること。

5. 回線サービス

本章では、調達対象である回線サービスに対する技術／運用要件を具体的に記述する。また、IPv4/IPv6 共存環境に対する稼働条件等を提示する。なお、回線サービスとしてはインターネット接続サービスを対象とし、IPv4 と IPv6 双方に対応した回線を ISP 事業者より調達することを想定する。

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

6. リモートアクセス及びインターネット VPN

本章では、調達対象であるリモートアクセス及びインターネット VPN サービスに対する技術／運用要件を具体的に記述する。また、IPv4/IPv6 共存環境に対する稼働条件等を提示する。

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

7. 機能及びサービス

調達の範囲に示した各機能及びサービスの具体的な仕様を以下に示す。

なお、【OP】の記号をつけた項目はオプションであり、条件に合致する場合のみ記載する項目である。

7.1 ルータ及びスイッチ

7.1.1 ルータ

- 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 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 12）に対応すること。
- 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。
- 【OP】IPv4/IPv6 のパケットシェーピング機能（用語集項番 13）を有すること。
  - 利用者やアプリケーションによって帯域を制限する必要がある場合。
- 【OP】IPv4/IPv6 の優先制御機能を有すること。
  - 利用者やアプリケーションによって優先制御を行う必要がある場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.1.2 L3 スイッチ

- 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 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。

- 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。
- 【OP】IPv4/IPv6 の優先制御機能を有すること。
  - 利用者やアプリケーションによって優先制御を行う必要がある場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.1.3 L2 スイッチ

- 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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.2 セキュリティサービス

7.2.1 ファイアウォール

- 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 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。

- 【OP】IPv4/IPv6 の DoS 攻撃防御機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】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 14）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】IPv4/IPv6 の IP アドレスアノマリ（異常検知）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】IPv4/IPv6 の TCP アノマリ（異常検知）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】IPv4/IPv6 の UDP アノマリ（異常検知）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.2.2 ウェブアプリケーションファイアウォール

- ウェブアプリケーションファイアウォール（WAF、用語集項番 15）として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- アプリケーションレベル（L7）の検査が IPv4/IPv6 通信に対して可能なこと。
- 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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.2.3 セキュリティアプライアンス（IDS/IPS）

- IDS/IPS として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- 電子メールのウイルス検出など、アプリケーションレベル（L7）の検査が IPv4/IPv6 通信に対して可能なこと。
- 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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.2.4 UTM

ファイアウォールや IDS/IPS の機能を統合的に備える UTM（Unified Threat Management、統合脅威管理）装置として提案する場合には、以下の要件を満たすこと。

- UTM 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。
- 電子メールのウイルス検出など、アプリケーションレベル（L7）の検査が IPv4/IPv6 通信に対して可能なこと。
- 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。
- 【OP】IPv4/IPv6 の DoS 攻撃防御機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】IPv4/IPv6 のフラグメンテーションアノマリ（異常検知）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】IPv4/IPv6 の IP アドレスアノマリ（異常検知）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】IPv4/IPv6 の TCP アノマリ（異常検知）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】IPv4/IPv6 の UDP アノマリ（異常検知）機能を有すること。
  - 高度なセキュリティ機能が必要な場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.3 ユーザサービス

7.3.1 SSL アクセラレータ

- SSL アクセラレータとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- サーバ証明書をインストールし、IPv4/IPv6 通信を SSL や TLS （用語集項番 16）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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.3.2 ロードバランサー

- ロードバランサーとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- 外部からの IPv4/IPv6 によるアクセスをウェブサーバに振り分ける際に、ウェブサーバに対する通信を IPv4 及び IPv6 のいずれかを選択できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- IPv4 通信と IPv6 通信が同等の TLS/SSL のアクセラレータの性能を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.3.3 ウェブシステム

- ウェブシステムとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- ウェブブラウザ等のクライアントからの IPv4/IPv6 通信による要求に対して、ウェブサーバ上に格納されたコンテンツを返送できること。
- サーバ証明書をインストールし、IPv4/IPv6 通信を SSL や TLS プロトコルで暗号化できる機能を有すること。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。

- 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。
- 【OP】ウェブシステムの CMS（コンテンツマネジメントシステム、用語集項番 17）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。
  - CMS 機能に外部連携機能を備える場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.3.4 メールシステム

- 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 18）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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.4 基盤サービス（DNS、プロキシ、NTP、認証）

7.4.1 DNS サーバ

- DNS サーバとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- IPv4/IPv6 通信による DNS の名前（アドレス）解決機能を有すること。
- IPv4/IPv6 通信による順引き及び逆引きに対応していること。
- 上位又は下位の DNS サーバと IPv4/IPv6 通信で連携する機能を有すること。
- IPv4 及び IPv6 に関連するレコードを保持できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。

- IPv4/IPv6 通信による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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.4.2 プロキシサーバ

- 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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.4.3 NTP サーバ

- 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。
- 上位または下位の 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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.4.4 認証サーバ

- 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。
- 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。
- 【OP】外部の認証サーバと IPv4/IPv6 通信で連携できること。
  - 外部の認証サーバと連携する場合。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.5 その他の必要な機能及びサービス

その他に必要となる可能性のある機能やサービスとしては、「運用監視機能」「仮想化基盤」「トランスレータ」がある。

7.5.1 運用監視機能

- 運用監視機能として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- ネットワーク機器やサーバ機器の IPv4/IPv6 通信に関する死活監視ができること。
- 各種サービス（ウェブ、メール、DNS 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 通信と IPv6 通信を統合して監視できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.5.2 仮想化基盤

- 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 19）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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

7.5.3 トランスレータ

- トランスレータとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- DMZ 上のネットワーク機器、サーバ等からインターネットに対する IPv4 通信を IPv6 通信に変換すること。またその結果生じるインターネットから DMZ 上のネットワーク機器、サーバ等への IPv6 通信を IPv4 通信に変換すること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6 通信による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。
- 【OP】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。
  - 運用管理を行うネットワークで IPv6 対応を行う場合。

8. 運用要件及び保守要件

本調達の対象となるシステム及びネットワークの保守に関する要件を示す。具体的には、以下に示す運用要件及び保守要件に関し、IPv4/IPv6 のいずれにおいても同等品質のサービスを提供することとする。

8.1 運用要件

- システムは原則として 24 時間 365 日運用とする。（数値はサンプル）
- システム障害の予防と早期発見のため、IPv4 及び IPv6 に対応した監視ツールを使用し、集中管理及び監視を 24 時間 365 日行うこと。（数値はサンプル）
- プログラム、データ、各種ログ等の特性に応じ、定期的にバックアップを行うこと。
- バックアップは、システムを停止しないオンラインバックアップにて行うこと。
- 監視及び運用に用いるシステムは庁舎内サーバ室に設置すること。なおその一部は、ASP やクラウドサービスにより提供するものでも可とする。
- システム運用体制、障害時の対応体制、連絡窓口、ヘルプデスク、保証品質について明示した運用計画書を予め提出し、承認を得ること。

8.2 保守要件

- システムの機能的な不具合の修正及び設定の変更等を保守の対象とする。
- 不具合発生時の早急な修正を可能とする計画を用意すること。
- 設計情報、定義情報等のドキュメントを整備し、障害や改訂の際に対象箇所を容易に識別できるようにすること。
- バージョン管理を適切に行える仕組を提供すること。
- 保守対応時間は、平日 9 時から 17 時までとする。なお、これ以外の対応時間においても、緊急度の高い不具合に対して臨時の対応を可能とする仕組を提供すること。（数値はサンプル）

9. その他の留意事項

本調達の対象となるシステム及びネットワークは、自治体 DMZ の構成に係る要素であるだけでなく、自治体 LAN とインターネットとの通信にも利用される基盤部分である。このため、自治体 LAN との間で以下の IPv4 通信を通過させる必要がある。

- 自治体 LAN 上の端末からプロキシサーバ経由でインターネット上のウェブシステム等へアクセスする通信
- 内向けメールシステムと外向けメールシステムとの間で相互に電子メールを転送する通信
- 自治体 LAN 上の端末から CMS 経由でウェブシステム上のコンテンツを管理するための通信
- ウェブシステム上で動作するウェブ アプリケーションが参照するバックエンドデータベースシステムとの通信（データベースが自治体 LAN 上にある場合）

10. （参考）IPv6 対応チェックシート

本書は地方自治体における IPv6 対応調達仕様書のモデルを示すものとして作成している。

本書のベースは同時に策定している「IPv6 対応ガイドライン」であり、ガイドラインによって採用している標準的なシステムやネットワークのモデル及び基本的な IPv6 対応シナリオをベースとして、インターネット接続に係るネットワーク及び外部向けサービスを IPv6 対応する際に調達が必要となる各要素について、IPv6 に対応するための要件を整理したものである。

個々の地方自治体はそれぞれ異なるネットワークを有しているため、この IPv6 対応調達仕様書モデルをそのまま採用できる地方自治体は限られるが、それぞれの状況に応じてモデルの内容を適宜、抜粋、分割、修正等を行うことで、多くの地方自治体に対して、それぞれに応じた調達仕様書を作成できると考えている。

ここでは、「2.想定するシステム及びネットワークの全体像」から「9.その他の留意事項」に解説した各事項について、チェックシートを提示する。このチェックシートに基づいて順次確認を行い、必要な修正を行うことで、各地方自治体の調達範囲や調達区分の考え方を反映した調達仕様書を作成することができる。

表 10-1　IPv6 対応チェックシート

分類	確認項目	チェック内容	回答例	確認方法及び対応方法	チェック欄
既存ネットワークシステムの確認					
	想定するシステム及びネットワークのモデルとの違い				
		現状のシステム及びネットワークと想定モデル（論理構成）との違いはどの程度ですか。	個別に違う部分があるが概ね同じである。	概ね同じ部分について同じである要素をチェックして下さい。	□
			概ね同じ部分と全く異なる部分がある。	全く異なる部分は別途検討が必要です。概ね同じ部分について同じである要素をチェックして下さい。	□
			ごく一部に同様な部分があるが概ね異なる。	モデルを前提としたネットワーク更新が可能か検討して下さい。可能な場合には、適用可能な範囲である要素をチェックして下さい。	□
調達範囲の確認					
	モデルの調達範囲との違い				
		概ね同じ部分／提供可能な要素のチェック結果をもとに、今回の調達範囲を確認して下さい。	チェック結果の対応範囲は、今回の調達対象として検討可能である。	調達範囲とするか検討の上、調達範囲とする要素をチェックして下さい。	□
			チェック結果の対応範囲でも、中期計画等に従って今回の調達対象外となる部分がある。	今回の調達対象にしうる範囲について、調達範囲とするか検討の上、調達範囲とする要素をチェックして下さい。	□
基本要件の確認					
	調達単位の確認				
		調達範囲とする要素の決定、チェック結果に基づき、調達単位の分割について検討して下さい。	全体を一括して調達する。	調達仕様書は全部で1冊になります。このまま検討を進めて下さい。	□
			全体を複数の単位に分割して調達する。	調達仕様書は分割単位の個数に分冊されます。以下では、分冊毎に対応する調達単位についてのみ検討を進めて下さい。	□
	スケジュールの確認				
		予算の執行時期、システムの規模等に応じて、全体スケジュールを調整して下さい。	ー	マイルストーンとなる日程を含めて、全体スケジュールを調整して下さい。	□

分類	確認項目	チェック内容	回答例	確認方法及び対応方法	チェック欄
	庁舎内設置機器の確認				
		調達対象としての機器やサービスの許容の考え方を整理して下さい。	ー	モデルでは、自治体LANへの接続の確保を考えた最低限必要な機器を明示しています。これ以外に庁舎内設置を求める機器などを特定して下さい。	□
	設置場所の確認				
		現在のサーバ室をそのまま使うのか、新しい部屋へ移動するのか、データセンター等外部に移すのか方針を整理して下さい。	ー	新たな部屋への移動やデータセンター等外部へ移動する場合には、設置場所としての要件を確認し、記載して下さい。	□
	ネットワーク上のサービスを利用する場合の要件の確認				
		予算執行の制約等を特に確認して下さい。	補助金等の利用により構築費は出るが運用費があまりない。	ASP/クラウドサービスの利用は難しい可能性があります。事前一括払いの料金プランを求める方法もあります。	□
			一般予算から確保するので、年あたりの支払を平準化したい。	ASP/クラウドサービスを利用する方が有利となる可能性があります。	□
	規模要件の確認				
		規模として求める具体的数字を確認して下さい。	ー	確認した具体的数字を記載して下さい。	□
	性能要件の確認				
		性能として求める具体的数字を確認して下さい。	ー	確認した具体的数字を記載して下さい。	□
	信頼性要件の確認				
		信頼性として求める具体的数字を確認して下さい。	ー	確認した具体的数字を記載して下さい。	□
	セキュリティ要件の確認				
		セキュリティ要件の内容を確認して下さい。	ー	必要に応じて修正、追記をして下さい。	□
	移行要件の確認				
		移行要件の内容を確認して下さい。	ー	必要に応じて修正、追記をして下さい。	□
	教育要件の確認				
		教育要件の内容を確認して下さい。	ー	必要に応じて修正、追記をして下さい。	□
回線サービスへの要求内容の確認					
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
リモートアクセス及びインターネットVPNの要求内容の確認					
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
機器及びサービスの要求内容の確認					
	ルータの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□

分類	確認項目	チェック内容	回答例	確認方法及び対応方法	チェック欄
	L3スイッチの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	L2スイッチの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	ファイアウォールの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	ウェブアプリケーションファイアウォールの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	セキュリティアプライアンスの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	UTMの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	SSLアクセラレータの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	ロードバランサーの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	ウェブシステムの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	メールシステムの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	DNSサーバの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	Proxyサーバの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□

分類	確認項目	チェック内容	回答例	確認方法及び対応方法	チェック欄
	NTPサーバの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	認証サーバの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	トランスレータの確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	仮想化基盤の確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
	運用監視機能の確認				
		調達範囲か確認して下さい。	調達範囲である。	記載内容をIPv6対応に必要な調達要件として仕様書に記載して下さい。	□
			調達範囲外である。	仕様書からは項目記載を削除して下さい。	□
保守要件の要求内容の確認					
	運用要件の確認				
		運用要件の内容を確認して下さい。	ー	必要に応じて修正、追記をして下さい。	□
	保守要件の確認				
		保守要件の内容を確認して下さい。	ー	必要に応じて修正、追記をして下さい。	□
その他留意事項の確認					
		調達範囲外のシステムとの関係を確認して下さい。	ー	調達範囲外のシステムとの通信等、必要に応じて修正、追記をして下さい。	□
		その他、記載すべき留意事項があれば記載して下さい。	ー	その他、記載すべき留意事項があれば記載して下さい。	□
IPv6以外の要件や機能以外の要件の追加等の確認					
	IPv6以外の要件の確認				
		IPv6以外の要件の内容を確認して下さい。	ー	必要に応じて追記して下さい。	□
	機能以外の要件の確認				
		機能以外の要件の内容を確認して下さい。	ー	必要に応じて追記して下さい。	□
	モデル以外の要件の確認				
		モデル以外の要件の内容を確認して下さい。	ー	必要に応じて追記して下さい。	□
	RFI等による実現性の評価と修正の確認				
		実現性の評価と修正内容を確認して下さい。	ー	必要に応じて追記して下さい。	□

11. （参考）参考文献

[1] 「電子政府システムの IPv6 対応に向けたガイドライン」平成 19 年 3 月
総務省

[2] 「電子自治体推進における IPv4 アドレスの枯渇への対応に関する調査研究『IPv4 アドレス在庫枯渇緊急対策ガイド』」平成 23 年 2 月
財団法人地方自治情報センター

[3] 「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

[4] 「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

[5] 「IPv4 サーバ環境への IPv6 ガイドライン」2009 年 11 月
IPv6 普及・高度化推進協議会

[6] 「IPv6 移行ガイドライン（大企業・自治体セグメント）」2004 年 5 月
IPv6 普及・高度化推進協議会

[7] 「2005 年 IPv6 移行ガイドライン（大企業・自治体編）」2005 年 3 月
IPv6 普及・高度化推進協議会

[8] 「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

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	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。
4	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。
5	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。
6	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。
7	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。
8	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。
9	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。
10	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。
11	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。

項番	用語	読み・別名	意味
12	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。
13	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。
14	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。
15	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。
16	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。
17	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。
18	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。
19	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。LAN カード、ネットワークアダプタとも呼ばれる。