4　IPv6 対応シナリオの策定

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

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

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

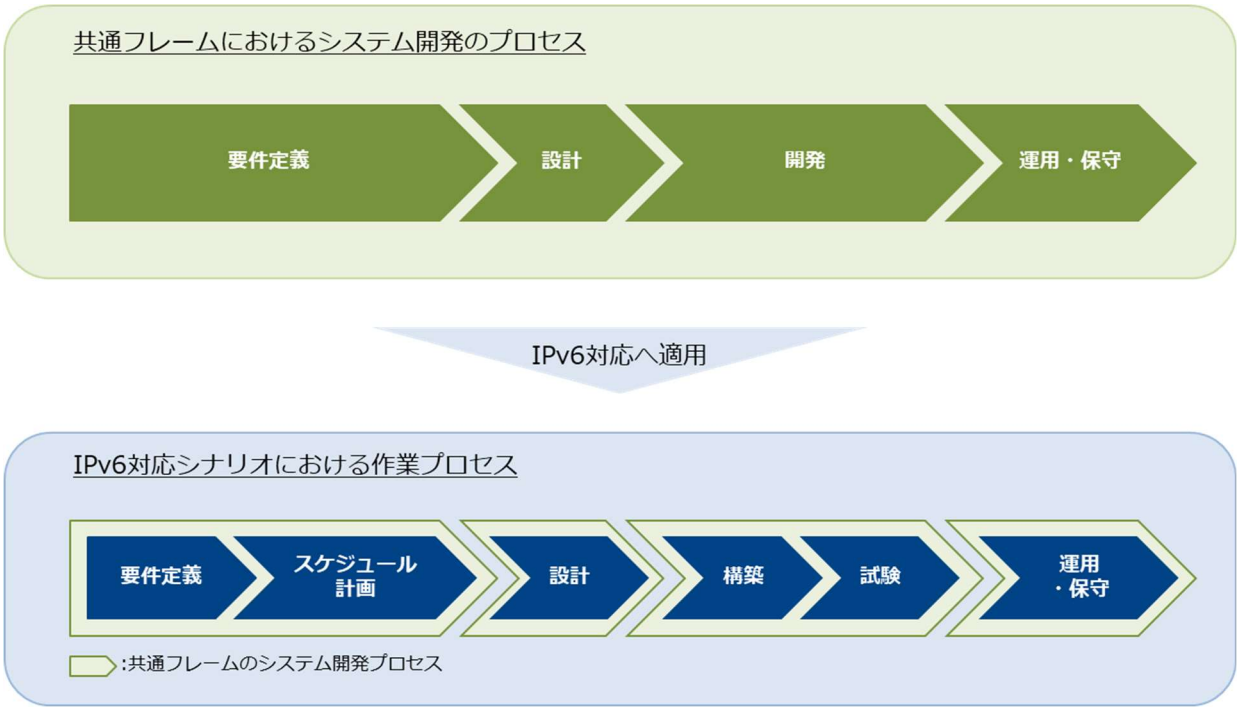

図 4-1 IPv6 対応における移行プロセスの概要

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

4.1　要件定義

IPv6 対応するにあたり、要件定義の工程では 5 つのプロセスに分けて作業を行う。まず、1 つ目の「現状の把握」では既存環境で利用している機器やサービスを可視化し、現行システムを把握する。続いて、2 つ目の「移行方式の明確化」では IPv6 環境へ移行するための方式を定める。そして 3 つ目の「移行対象の明確化」では現行システムの内、IPv6 対応する機器やサービスを明確にする。また 4 つ目の「IPv6 対応状況の確認」では移行対象の機器やサービスが IPv6 に対応しているか確認を行い、IPv6 未対応の場合は機器やサービスの選定を行う。最後に 5 つ目の「導入方針の策定」では機器やサービスの IPv6 対応状況に基づき、IPv6 化に向けた導入方針を策定する。

要件定義における 5 つのプロセスについて概要を図 4.1-1 に示す。

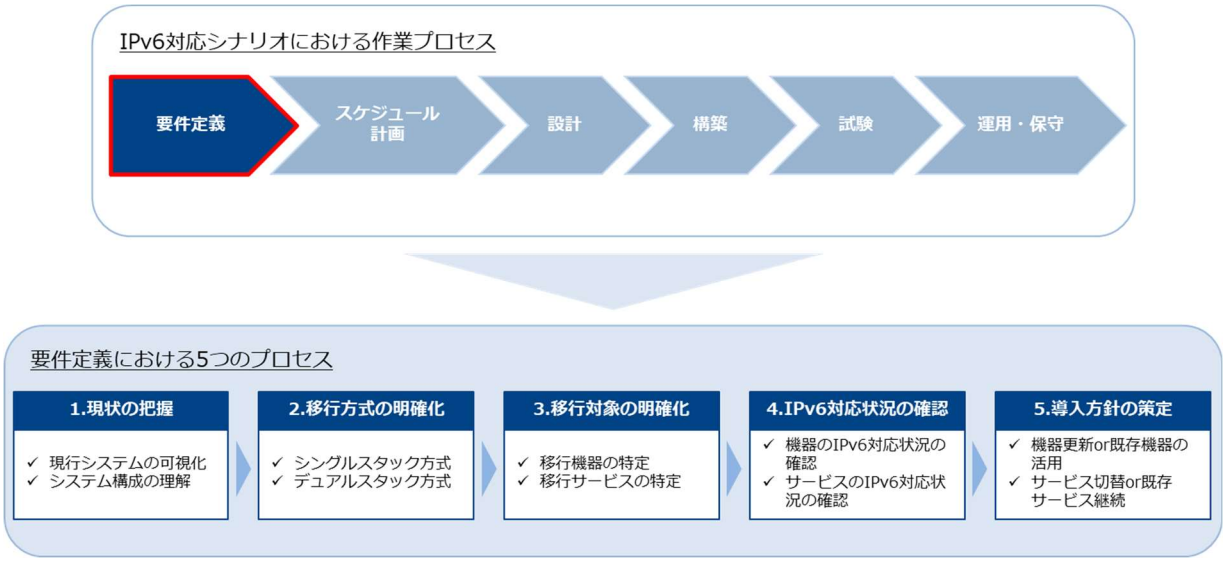

図 4.1-1 要件定義における 5 つのプロセス

（1）現状の把握

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

(2) 移行方式の明確化

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

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

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

(3) 移行対象の明確化

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

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

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

(4) IPv6 対応状況の確認

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

(5) 導入方針の策定

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

4.2　スケジュール計画

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

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

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

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

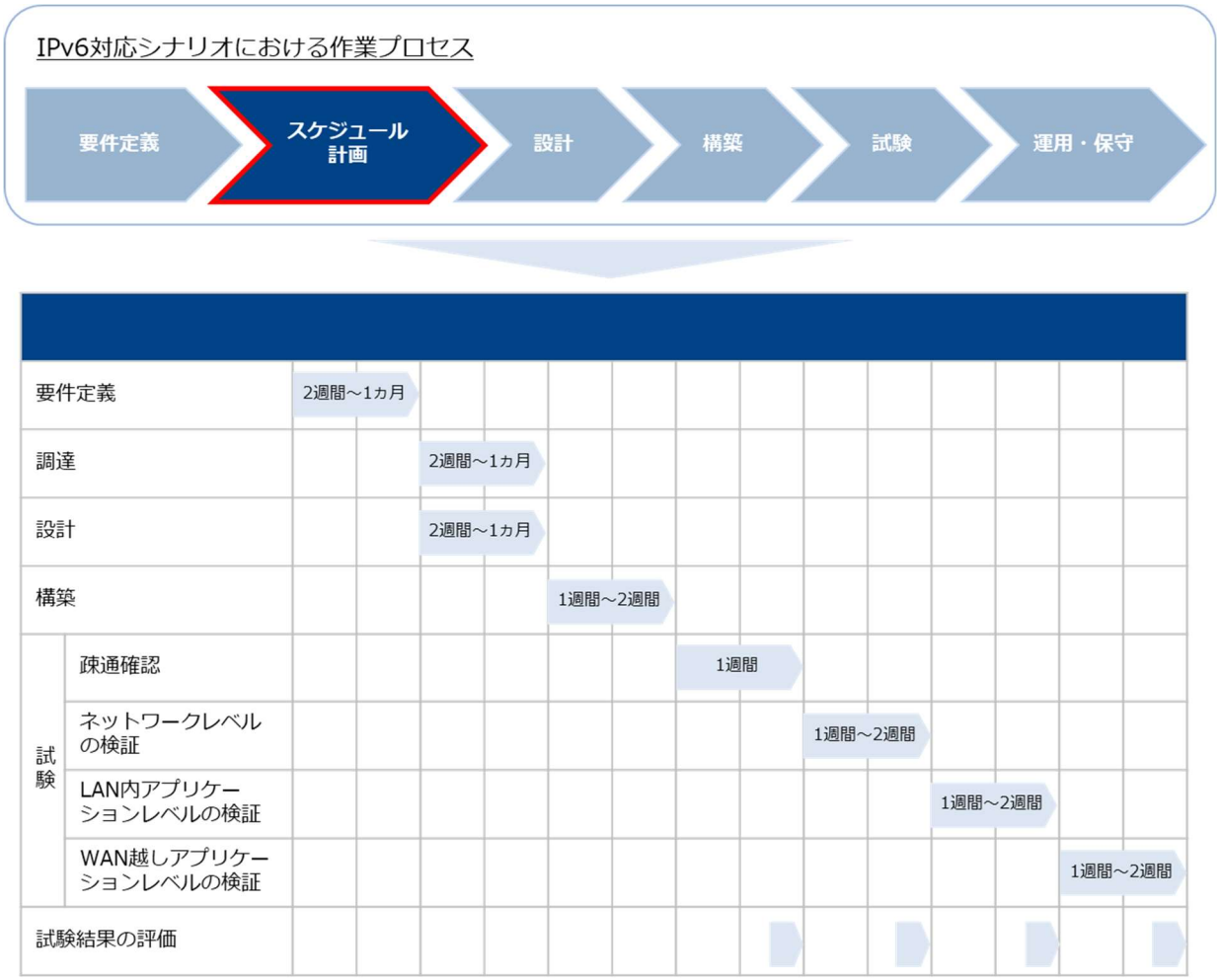

図 4.2-1 スケジュールイメージ

4.3　設計

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

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

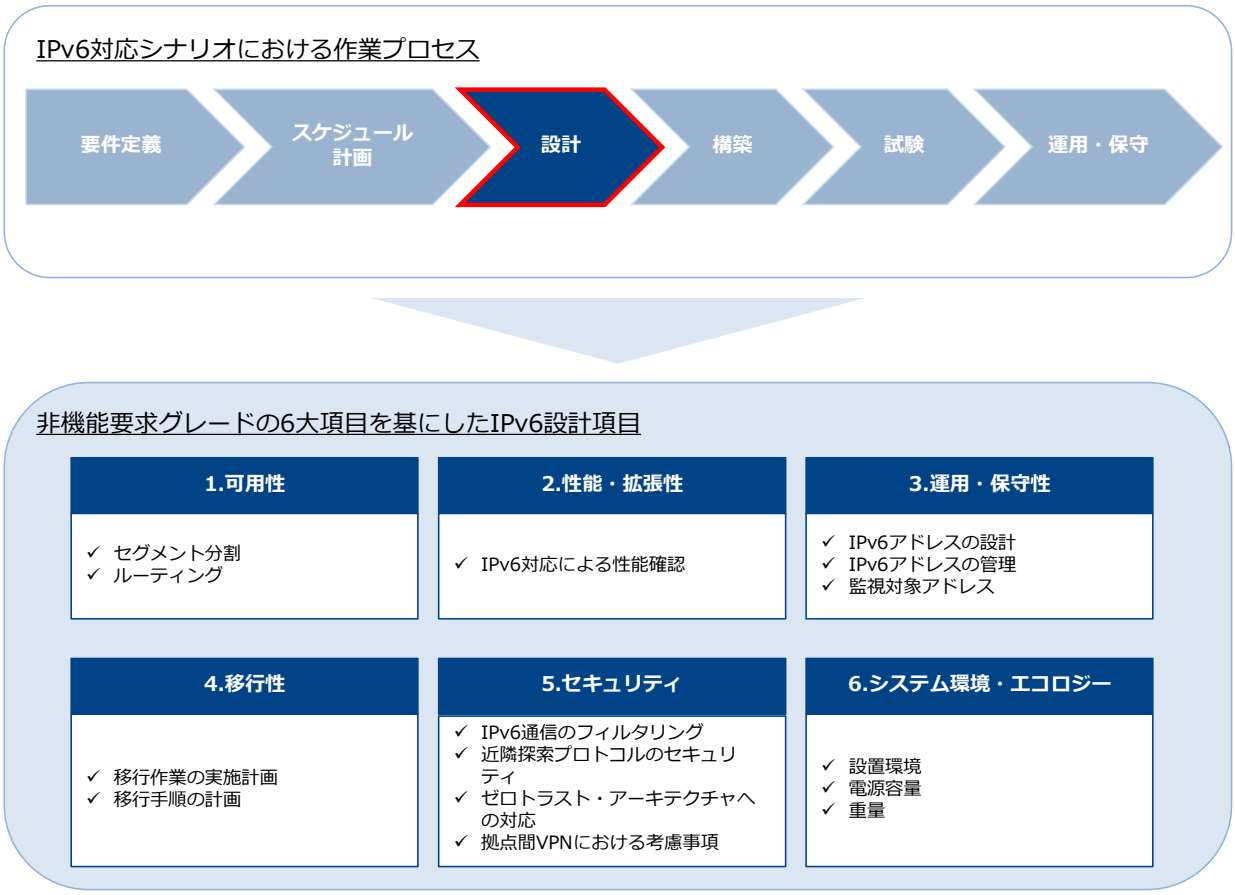

図 4.3-1 非機能要求グレードにおける 6 大項目と IPv6 設計項目との関連

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

(1) 可用性

① セグメント分割

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

② ルーティング

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

(2) 性能・拡張性

① IPv6 対応による性能確認

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

(3) 運用・保守性

① リンクローカルアドレスの設計

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

② GUA（Global Unicast Address）[25]の設計

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

③ アドレス管理

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

④ 監視対象アドレス

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

---

25 グローバルスコープであり、インターネットでルーティングできる。

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

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

28 RFC4193「Unique Local IPv6 Unicast Addresses」

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

(4) 移行性

① 移行作業の実施計画

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

② 移行手順の計画

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

(5) セキュリティ

① IPv6 通信におけるフィルタリングの考慮事項

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

30 RFC4890「Recommendations for Filtering ICMPv6 Messages in Firewalls」

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

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

③ IPv6 によるゼロトラスト・アーキテクチャへの対応

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

---

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

32 RFC6105「IPv6 Router Advertisement Guard」

33 RFC3971「SEcure Neighbor Discovery (SEND)」

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

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

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

  など

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

④ 拠点間 VPN における考慮事項

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

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

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

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

38 RFC9099「Operational Security Considerations for IPv6 Networks」

(6) システム環境・エコロジー

① 設置環境

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

② 電源容量

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

③ 重量

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

4.4　構築

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

(1) 構築における基本作業

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

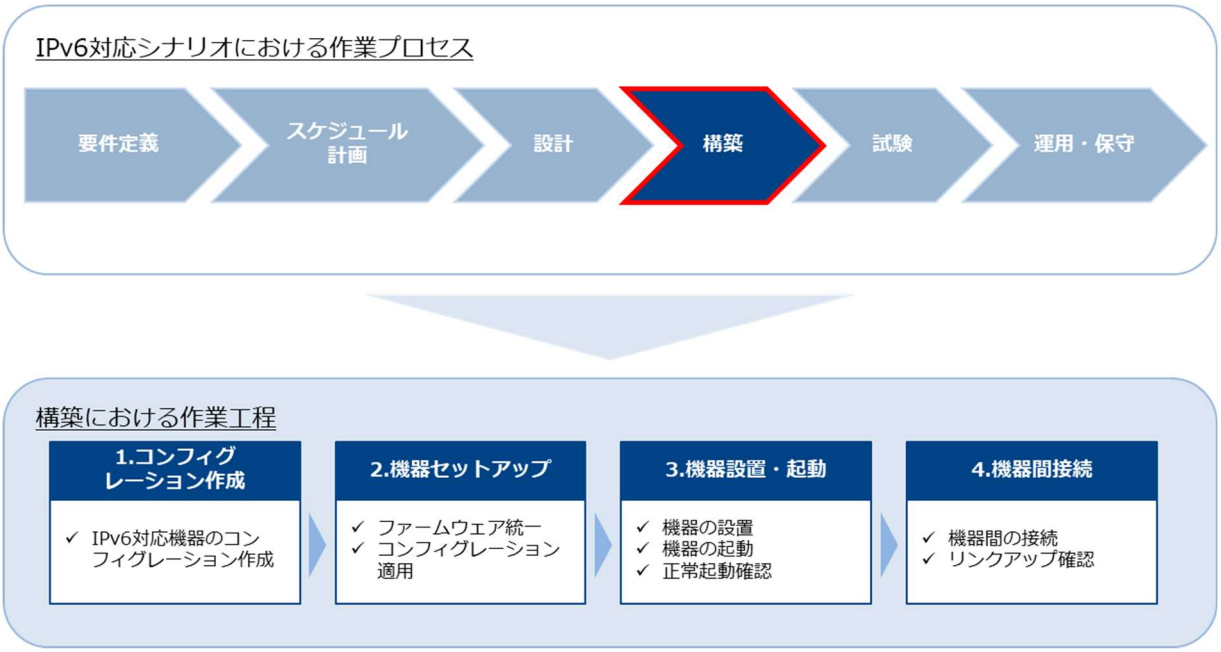

図 4.4-1 構築作業の工程イメージ

① コンフィグレーション作成

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

② 機器セットアップ

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

③ 機器設置・起動

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

④ 機器間接続

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

(2) 構築における IPv6 特有の留意点

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

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

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

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

IP アドレスの設定例 ※斜体は可変部を示す

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

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

4.5　試験

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

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

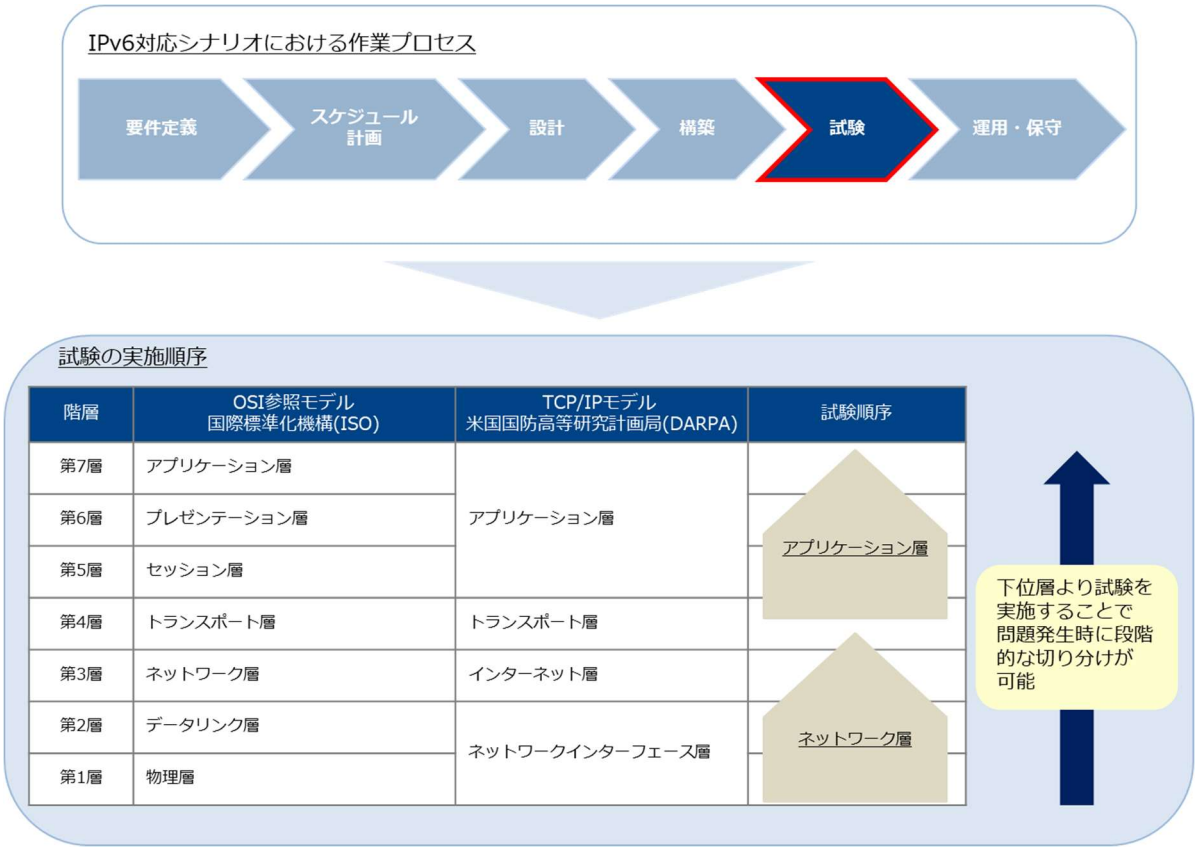

図 4.5-1 試験の実施順序

(1) ネットワーク層における試験

ネットワーク層における試験では、まず基本的な試験項目として各機器に対して疎通試験を実施する。また Traceroute 等を実行し、通信フローが設計通りとなっているか確認することも重要である。つぎに一般業務における検証では、WEB サービスやメール等のインターネット利用、印刷やスキャン等の OA 機器利用といった通常業務が IPv6 通信で正常に行えるか検証することを目的としている。機器のカタログ等で IPv6 対応と記載があったとしても、実際には IPv6 未対応の場合があるため、動作確認することが重要である。

(2) アプリケーション層における試験

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

(3) 運用監視システムにおける試験

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

4.6　運用・保守

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

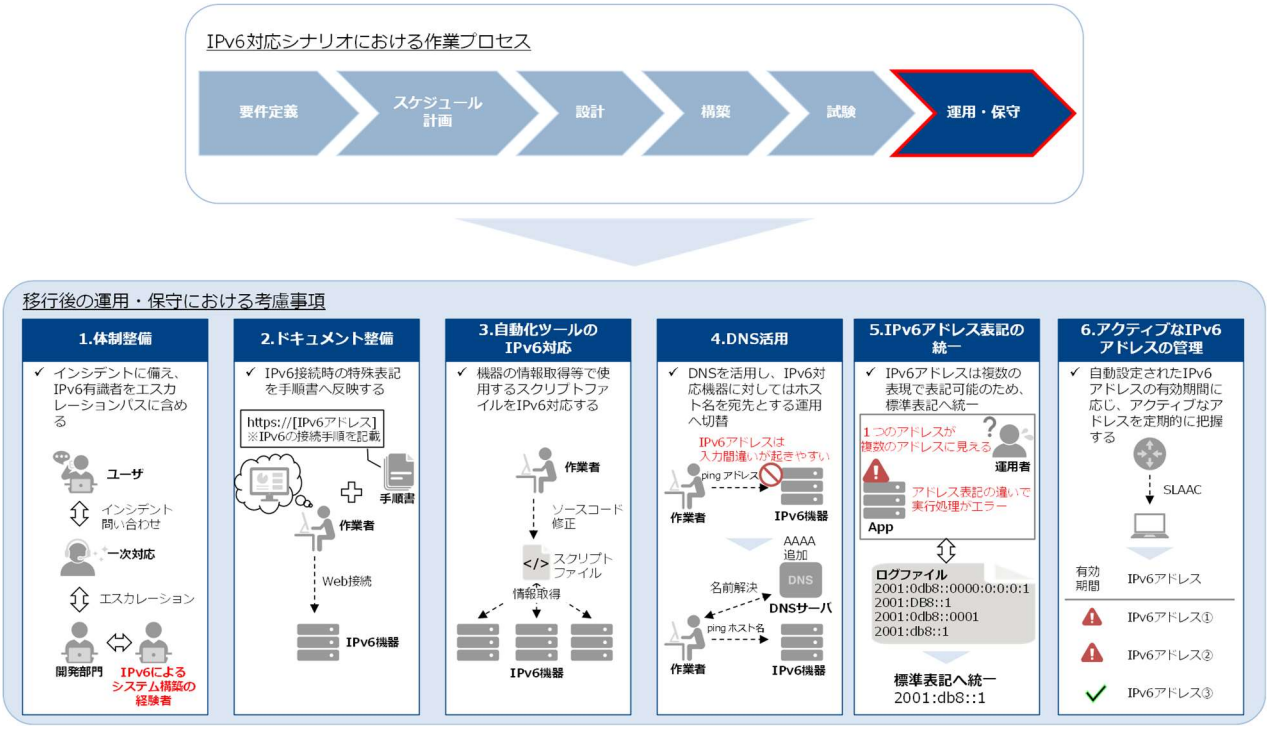

図 4.6-1 IPv6 対応後の運用・保守において考慮すべき事項

(1) 運用・保守の体制整備

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

(2) ドキュメント整備

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

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

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

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

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

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

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

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

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

40 RFC5952「A Recommendation for IPv6 Address Text Representation」

(6) アクティブな IPv6 アドレスの管理

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

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

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

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

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