3　ネットワーク構成のモデル化

本ガイドラインにてIPv6対応ユースケースを紹介するにあたり、ユースケースの包括的な概念として、モデルケースを示す。モデルケースは総務省令和元年度事業にて実施したヒアリング調査に基づき、整理したネットワーク構成モデルを採用する。3.1にてモデルケースを整理する際の観点を示す。また3.2にてモデルごとのIPv6対応プランを示し、3.3にてモデルケースの事例となるユースケースの概要を示す。

3.1　モデルケースの整理

総務省令和元年度事業にて中小企業、学術機関、地方公共団体のそれぞれ 2 団体に対して現在運用中の情報システム等の状況についてヒアリング調査を実施した。

図 3.1-1 に示すとおり、ヒアリング結果を基に、ネットワーク構成をモデル化した。モデル化する際の観点は「ネットワーク規模」「拠点間 VPN」「イントラネット内のエンドポイント管理」の 3 つとした。

(1) ネットワーク規模

総務省が公表する「IPv6 対応ガイドライン（企業編）[14]」では、「中小企業の場合は、コスト削減や業務の効率化のために、DMZ をはじめとした多くの機能を ASP やクラウドサービス上に構築することが想定される。」としている。その上で、典型的な大企業のシステムやネットワークのモデルとして、DMZ を有した企業内ネットワークを紹介している。今回のヒアリングは、中小企業、大学、地方自治体を対象としており、大企業は範疇外であるが、DMZ 有無をネットワーク規模の 1 つの観点として考える。内部に DMZ（メールサーバや DNS サーバ等）が有る団体を大規模、無い団体を中規模と定義する。また、中規模については、サブネット数が 10 未満か 10 以上かでさらなる分類を行う。

(2) 拠点間イントラネット（VPN）

拠点間イントラネット（VPN）がある場合、通常のインターネットの経路とは別にトンネル化した経路を設計・構築する必要がある。ルーティングに関わる箇所であり、IPv6 独自の設計・構築が必要となるため、拠点間イントラネット（VPN）の有無を 1 つの観点として考える。

(3) イントラネット内のエンドポイント管理

IPv6 アドレスは NAT を用いずエンドポイントごとにグローバルアドレスを保有する。従来の境界防御ではなく、エンドポイント管理が更に求められる[15]。そのため、エンドポイント管理の有無を 1 つの観点として考える。

---

[14] https://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/index.html

[15] ゼロトラストという概念が登場したように、IPv6 普及とは別で境界防御の限界は提起されている。

IPv4 NAT、ASP/クラウドサービス、ファイアウォールの利用有無も IPv6 対応に伴う影響を受ける箇所であるが、ヒアリング結果のとおり、すべての団体が利用しているため、共通項目とする。

<table>
<tr><th>観点 ＼ モデル</th><th>モデルA</th><th>モデルB</th><th>モデルC</th><th>モデルD</th><th>モデルE</th><th>モデルF</th><th>モデルG</th><th>モデルH</th><th>モデルI</th><th>モデルJ</th></tr>
<tr><td>共通</td><td colspan="10">IPv4 NATあり
ASP/クラウドサービスあり
ファイアウォールあり</td></tr>
<tr><td>内部にDMZ（メールサーバやDNSサーバ等）があるか</td><td colspan="2">ある
（大規模）</td><td colspan="8">ない
（中規模）</td></tr>
<tr><td>サブネット数はいくつか</td><td colspan="2">10以上</td><td colspan="4">10以上</td><td colspan="4">10未満</td></tr>
<tr><td>拠点間イントラネット（VPN）はあるか</td><td>ある</td><td>ない</td><td>ある</td><td>ある</td><td>ない</td><td>ない</td><td>ある</td><td>ある</td><td>ない</td><td>ない</td></tr>
<tr><td>イントラネット内のエンドポイント管理はしているか</td><td colspan="2">ある</td><td>ある</td><td>ない</td><td>ある</td><td>ない</td><td>ある</td><td>ない</td><td>ある</td><td>ない</td></tr>
</table>

図 3.1-1 ヒアリング結果を基にしたネットワーク構成モデル

3.2　モデルごとの IPv6 対応プラン

3.1 にて整理したモデルごとの IPv6 対応プランを以下に示す。対応プランの項目はモデル化する際の観点に基づき、「対応範囲」「セグメント設計」「拠点間 VPN」「エンドポイント管理」の 4 つとし、その中からモデルの特性に応じた対応項目を示す。

3.2.1 モデル A

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を有し、メールサーバや DNS サーバ等が稼働しており、セグメントが 10 以上に分割された大規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装し、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは DMZ を有するネットワーク構成のため、機器の IPv6 対応として WAN 機器と LAN 機器に加えて、DMZ 内の機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434[16]にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

(4) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

---

16 RFC6434「IPv6 Node Requirements」

3.2.2 モデル B

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を有し、メールサーバや DNS サーバ等が稼働しており、セグメントが 10 以上に分割された大規模な環境である。尚、拠点間イントラネットを持たない構成であり、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは DMZ を有するネットワーク構成のため、機器の IPv6 対応として WAN 機器と LAN 機器に加えて、DMZ 内の機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.3 モデル C

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装し、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434[17]にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

(4) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

---

17 RFC6434「IPv6 Node Requirements」

3.2.4 モデル D

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装しているが、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434 にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

3.2.5 モデル E

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。尚、拠点間イントラネットを持たない構成であるが、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.6 モデル F

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 以上に分割された中規模な環境である。尚、拠点間イントラネットを持たない構成であり、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

3.2.7 モデル G

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装し、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434 にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

(4) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.8 モデル H

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。また、複数拠点を有し、拠点間イントラネット接続として VPN を実装しているが、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。
当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) 拠点間 VPN

IPv6 は IPsec の実装が「必須」とされていたが、RFC6434 にて更新され、「必須」から「推奨」とされている。一般的に IPv6 はデフォルトで通信が暗号化されているため安全であると捉えがちであるが、誤った認識となる。したがって、拠点間 VPN 接続を行う当モデルでは IPv6 においてもグローバルで通信する場合はセキュリティ担保の面から IPsec による接続対応を検討する。

3.2.9 モデル I

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。尚、拠点間イントラネットを持たない構成であるが、イントラネット内のエンドポイント管理を実施している。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

(3) エンドポイント管理

エンドポイント管理を実施している当モデルでは管理システムの IPv6 対応を行う。エンドポイントの IP アドレスが IPv6 になることにより、アドレス検索等、システムの機能に影響がないか動作確認を行う。

3.2.10　モデル J

当モデルは WAN と LAN のネットワーク構成を前提とし、情報システム等に ASP やクラウドサービスを活用している。内部のネットワークには DMZ を持たない構成であり、セグメントが 10 未満の中規模な環境である。尚、拠点間イントラネットを持たない構成であり、イントラネット内のエンドポイント管理を実施していない。

(1) 対応範囲

IPv6 対応として機器の IPv6 対応とサービスの IPv6 対応を行う。

当モデルは WAN と LAN で構成されたネットワークのため、機器の IPv6 対応として WAN 機器と LAN 機器を対象とする。また、サービスにおいては現行アプリケーションや商用システム・外部サービス等の IPv6 対応を行う。

(2) セグメント設計

セグメントは IPv4 と同様に用途ごとに分割する前提とするが、IPv4 環境でホスト数の制約によりセグメントを分割している場合はアドレス空間が広大である IPv6 を利用することにより、1つのセグメントに集約して運用できないか検討する。但し、セグメントを集約することでセグメント単位でのアクセス制限が適用しづらくなるケースもあり得るため、セキュリティの観点からもセグメントの集約要否を検討する。

3.3　ユースケースとしてのモデル選定

3.1 で整理したネットワーク構成モデルの内、ユースケースとして「モデル G」および「モデル I」を選定した。モデルの選定理由および選定モデルとユースケースの概要を以下に示す。

3.3.1 モデル選定理由

ユースケースとしてのモデルを選定するにあたり、選定項目はモデル化する際の観点に基づき、「ネットワーク規模」「サブネット数」「拠点間 VPN」「エンドポイント管理」の 4 つとした。

(1) ネットワーク規模

中小企業庁の「日本の中小企業・小規模事業者施策について」[18]によると、全事業者数の 99.7%が中小企業であると報告されている。中小企業が全事業者数の 9 割を占めることから選定モデルのネットワーク規模として中規模なモデルを対象とした。

(2) サブネット数

中小企業庁の「日本の中小企業・小規模事業者施策について」によると、事業者数では製造業が 11%にとどまり、卸・小売、サービス業が約 65%を占めている。同庁の中小企業基本法[19]の定義によると、事業者数の 6 割以上を占める卸・小売、サービス業の従業員数は 100～50 名以下とされている。また、IPA[20]による中小企業における情報セキュリティ対策の実態調査[21]によると、中小企業におけるサーバの利用台数は平均で 3.7 台と報告されている。これらの従業員数やサーバの平均利用台数を収容することを鑑み、選定モデルのサブネット数として 10 未満のモデルを対象とした。

(3) 拠点間 VPN

拠点間 VPN は IPsec による接続を行う際にトンネルの設計等、IPv6 独自の設計が必要となるためユースケースの蓄積として有効と考え、拠点間 VPN の有無を選定基準とした。

(4) エンドポイント管理

IPv6 対応により、エンドポイントにグローバルで通信可能なアドレスが付与されることになるため、セキュリティとしてエンドポイント管理がより一層求められることを踏まえ、エンドポイント管理を実施しているモデルを対象とした。

---

18 https://www.chusho.meti.go.jp/soshiki/180404seisaku.pdf

19 https://www.chusho.meti.go.jp/soshiki/teigi.html

20 Information-technology Promotion Agency, Japan(独立行政法人情報処理推進機構) https://www.ipa.go.jp/index.html

21 https://www.ipa.go.jp/files/000058502.pdf

3.3.2 選定モデルとユースケースの概要

選定モデルとユースケースの概要を表 3.3-1 に示す。尚、本ガイドラインの対象読者の内、選定モデルに該当しないケースも想定されるが、ユースケースで紹介する IPv6 対応の流れや各作業工程におけるアウトプットイメージ等はその他のモデルに横展開可能であるため、参考とすることを推奨する。

表 3.3-1 選定モデルとユースケース概要

ネットワーク構成モデル	ユースケース	移行方式	IPv6 対応方針	拠点間 VPN
モデル G	中小企業 A	デュアルスタック	・ 既存回線＋IPv6 回線新設 ・ IPv6 対応 GW ルータを新設し、IPv6 実証環境を既存環境と併設した構成にて構築 ・ IPv6 による拠点間 VPN を実装	有
モデル I	中小企業 B	デュアルスタック	・ 既存回線の IPv6 デュアル対応 ・ 回線切り替えに伴い IPoE 対応 GW ルータを増設 ・ 既存機器の IPv6 対応を実施し、IPv6 実証環境を既存環境と共存させて構築	無
モデル G	中小企業 C	デュアルスタック	・ 既存回線の IPv6 デュアル対応 ・ 複数拠点に対して回線切り替えに伴い IPoE 対応 GW ルータを増設 ・ 既存機器の IPv6 対応を実施し、IPv6 実証環境を既存環境と共存させて構築 ・ IPv6 による複数拠点間 VPN を実装	有
モデル I	大学 A	デュアルスタック	・ 既存回線(SINET[22])の IPv6 デュアル対応 ・ 回線切り替えに伴い GW となるファイアウォールを IPv6 対応機器へ更新するとともに、既存機器の IPv6 対応を実施し、IPv6 実証環境を既存環境と共存させて構築	無

[22] Science Information NETwork (学術情報ネットワーク)
https://www.sinet.ad.jp/