IPv6普及・高度化推進協議会　セキュリティWG
IPv6対応セキュリティガイドライン（第1.0版）

平成24年8月

変更履歴

版	改版日	摘要
0.5	2011年4月28日	企業ネットワーク（DMZ）を対象としたIPv6対応セキュリティガイドラインの中間報告書として0.5版を発行
1.0	2012年8月27日	0.5版の改訂

まえがき

本格的なIPv4/IPv6共存時代に突入し、何らかのサービスをインターネット上で提供している組織にとって、そのIPv6対応は喫緊の課題となった。このような状況の下で策定された本ガイドラインの主たる内容は、セキュリティガイドラインの考慮する範囲を広げ、セキュリティ確保とその運用の観点から企業DMZにおけるIPv4/IPv6共存のネットワークモデルを示すものとなっている。

IPv6対応に関するこれまでの取り組みは、ホストへの要求あるいはルータへの要求といった、機器(ホスト・ルータ)レベルでの議論が主であって、実際のネットワークを構築・運用する立場からの視点で行われたものは多くない。今回、セキュリティWGとしての最初のガイドラインを策定するにあたっても、この問題が表面化した。ガイドラインのあり方として無難な選択は、従来の機器レベルのセキュリティ対策を踏襲し更新する形であるが、その種のガイドラインであれば、すでに巷に溢れており、同種のガイドラインを策定する意義は小さいと考えた。われわれが選択したのは、もう一歩踏み込んで、実際の現場で役に立つ、セキュリティ運用の視点からの対策を示して行くことである。

では実際に構築運用されているIPv4ネットワークを、ありとあらゆる手法でIPv6対応させたネットワークの一つ一つにおいてセキュリティ対策を考えるのかということになるが、これは現実的には不可能である。そこで採用したのが、企業DMZにおけるいくつかのIPv4/IPv6共存モデルを示し、それらのモデルにおけるセキュリティ対策を確立していくというアプローチである。今回のガイドラインでは、セキュリティWGが議論すべき範囲を広げ、この先10年のオーダーで続くであろうIPv4/IPv6共存時代の間、いかに効率良く、いかに安全にセキュリティ運用を行っていくかという観点に立ち、そのためのネットワークモデルを提案することに注力したのである。

今後、セキュリティWGでは、関係諸団体・機関とも連携しながら、これらのモデルに基づいた各種の対策を示して行くと共に、モデルそのものの精査も行い、より有用なガイドラインとしていきたいと考えている。

2012年8月

IPv6普及・高度化推進協議会　セキュリティWG主査
北陸先端科学技術大学院大学　高信頼ネットワークイノベーションセンター長
篠田陽一

目次

1 はじめに

IPv4アドレスはIANA在庫に続いて、APNIC・JPNIC在庫も枯渇し、事実上、各ISP等の手持ち在庫しか余裕分がないという状況になっており、IPv4の後継プロトコルであるIPv6の本格的な利用が各方面で始まろうとしている。

IPv4は、これまで30年以上に渡って利用され、その間にセキュリティ問題への対応等を順次進めてきた歴史がある。一方、IPv6では、これまで大規模な利用や運用が行われた経験が十分にないため、IPv6におけるセキュリティ上の課題及びその対策は、実態ベースでは広く共有されていない部分が多い。間近に迫ったIPv6本格利用時代に向けて、IPv6を安心して使っていくことが出来るようにするためには、IPv6対応にあたってIPv4と同等のセキュリティを確保するための手法、各種セキュリティ機器のIPv6対応状況などについて調査・検討し、ノウハウを取りまとめ、関係方面間でその情報を共有することが重要である。

このため、IPv6普及・高度化推進協議会では、IPv6のセキュリティに関する検討を実施するセキュリティワーキンググループ（以下、セキュリティWG）において、関連団体と連携を行いながら、IPv6セキュリティにおける課題の特定、解決のためのノウハウの取りまとめの作業を本格化することにした。

本ガイドラインでは、セキュリティWGでの2012年6月末時点までの検討状況について報告する。

1.1 セキュリティWGの活動内容

セキュリティWGでは、以下の趣旨のもと、検討を実施している。

IPv4アドレス在庫枯渇をにらみ、IPv6の本格的な利用開始を前に、 IPv6ネットワークを安心して利用して行くことが出来るようにするため、 IPv6に係るセキュリティ課題の特定、課題解決ノウハウ等をガイドラインとしてまとめる。それに際しては、個別に具体的な脆弱性情報等の取扱いを考えるのではなく、 IPv6を利用する上で、セキュリティ上考慮すべき点等の一般化された情報の形で取りまとめることを主眼とし、幅広い利用者へのガイドラインとなることを目指す。

1.1.1 検討対象の整理

企業（DMZ、ホスティングを含むiDC利用）、キャリア（事業者、ISP）、個人を対象とし、そのIPv6利用／提供の典型的なネットワークモデルにおいて、セキュリティを考える上でのポイント、考えうるセキュリティ課題と対策の方法、推奨されるセキュリティモデル等について、ガイドラインの形で取りまとめを行い、広く公開する。

DMZは、企業等の社内ネットワークとインターネット等の外部ネットワークの中間に置かれるセグメントで、インターネットから社内ネットワークに直接に入ることができないような構成を取り、セキュリティ上の防衛機能等を持たせることにより、外部から社内ネットワークを守るための緩衝地帯としての役割を果たす。外部向けのWebサーバ等はDMZに置くことで、社内ネットワークを守りつつ、外部に対する情報発信を実現する役割も持っている。IPv4の枯渇によりインターネットがIPv6対応を進めつつある中で、外部のインターネットと直接つながる部分であるDMZのIPv6対応が重要であり、

そのセキュリティ確保策の検討が必要となっている。

ホスティングの利用に関しては、IPv6化に伴って提供者と利用者の間でのセキュリティ機能の分担等が複雑化する可能性があり、十分な検討が必要となることが予想される。

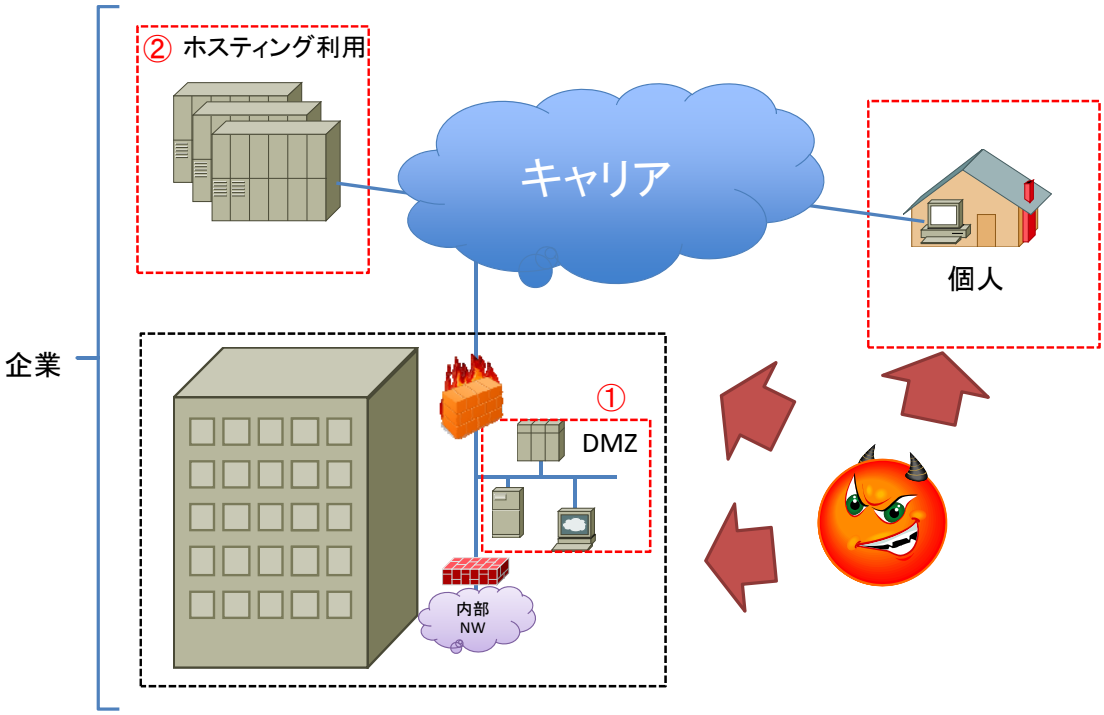

図 1.1.1-1 インターネットの構成主体

1.1.2 優先順位

対象のうち、企業ネットワーク、とりわけ、企業自身で主に設計・構築・運用等を行っており、企業自身による直接的な対応が必要となるDMZに関する需要がもっとも大きいと判断し、第一優先で検討を行った。また、DMZに関する検討より得られた知見等を参考に、iDC（ホスティングを含む、以下同じ）についても検討に加えていく。

なお、業界全体として技術力が高く、ベンダ対応が期待できる点も含めて、対策が進んでいるキャリア（事業者、ISP）に関しては、当面は優先順位を下げて考える。他と比べてネットワーク構成が単純な個人の利用環境に関しても同様に優先順位を下げる。

1.1.3 他の組織におけるIPv6セキュリティの議論

セキュリティWGでは、安全なIPv6ネットワークを構築するという観点から、モデル的なネットワークを意識した検討を行っている。そこで得られたIPv6セキュリティに関するノウハウは、実際のIPv6ネットワークの構築においても適用可能なものとなることを目指している。

一方、IPv6対応に際して注意の必要な、より一般的なIPv6セキュリティに関する議論が別の複数の組織においても行われており、これらについても参照していくことが望ましい。

1.1.3.1 政府機関の情報セキュリティ対策のための統一技術基準

内閣官房情報セキュリティセンターでは、政府機関の情報セキュリティ対策のための統一基準群を定めている。その中でも、政府機関が最低限実施するべき情報システム対策の技術的基準を示した「政府機関の情報セキュリティ対策のための統一技術基準（平成24年度版）」（平成24年4月18日情報セキュリティ対策推進会議（CISO等連絡会議）決定）においては、「2.4.1.1 情報システムへのIPv6技術の導入における対策」として、各府省庁の情報システムに対して遵守事項を定めている。政府機関以外の一般のIPv6ネットワークに対しては義務的なものではないが、指針としては必要に応じて参考となるだろう。

1.1.3.2 IPv6導入に起因する問題検討SWGにおける議論

IPv6普及・高度化推進協議会のIPv4/IPv6共存WG・IPv6導入に起因する問題検討SWGでは、IPv6導入後のIPv6/IPv4混在環境において発生が想定される問題の洗い出し、解法の検討、整理等を実施している。その中の一部には、IPv6セキュリティに係る課題も含まれており、例えば 不正RA問題、トンネルに起因する問題、ペアレンタルコントロールのすり抜け問題等が含まれている。

同SWGでは、2011年9月30日に「IPv6導入時に注意すべき課題」と題する報告書を公開している。この中では問題の解説、原因や症状の分析、問題の発見方法や対処方法についてまとめられており、必要に応じて参考とすることが望ましい。

公開ページ： http://www.v6pc.jp/jp/wg/coexistenceWG/v6fix-swg.phtml

1.1.3.3 海外政府関係の議論

海外では特に米国のNIST（USGv6）やDoD（jitc）によるガイドラインが有名である。これらについて、参照情報を記しておく。

NIST（USGv6）：

「A Profile for IPv6 in the U.S. Government Version 1.0」

http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf

「Guidelines for the Secure Deployment of IPv6」

http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

DoD（jitc）：

「DoD IPv6 Standard Profiles For IPv6 Capable Products Version 5.0」

http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf

「DoD IPv6 Generic Test Plan, Version 4」

http://jitc.fhu.disa.mil/adv_ip/register/docs/ipv6v4_may09.pdf

このうち、NIST（USGv6）の「Guidelines for the Secure Deployment of IPv6」については、参考となる部分も多いため、セキュリティWGではその一部を抜粋して、抄訳として公開を予定している。これについては、引き続きIPv6普及・高度化推進協議会のウェブサイト等でお知らせしていく。

1.2 セキュリティWGの検討ロードマップ

セキュリティWGの2011年度から2012年度にかけての検討ロードマップを下図に示す。1.1でも触

れているように、当初は企業ネットワークを主要対象に検討を行う。その中でも、まずはシステムの構成がシンプルであるDMZを対象として検討を行い、その経験を踏まえて、次にiDC（ホスティング利用を含む）を対象とした検討に進む予定である。

キャリアネットワークや個人のホームネットワークも検討の対象範囲に含めているが、現時点では具体的なプランについては未定である。

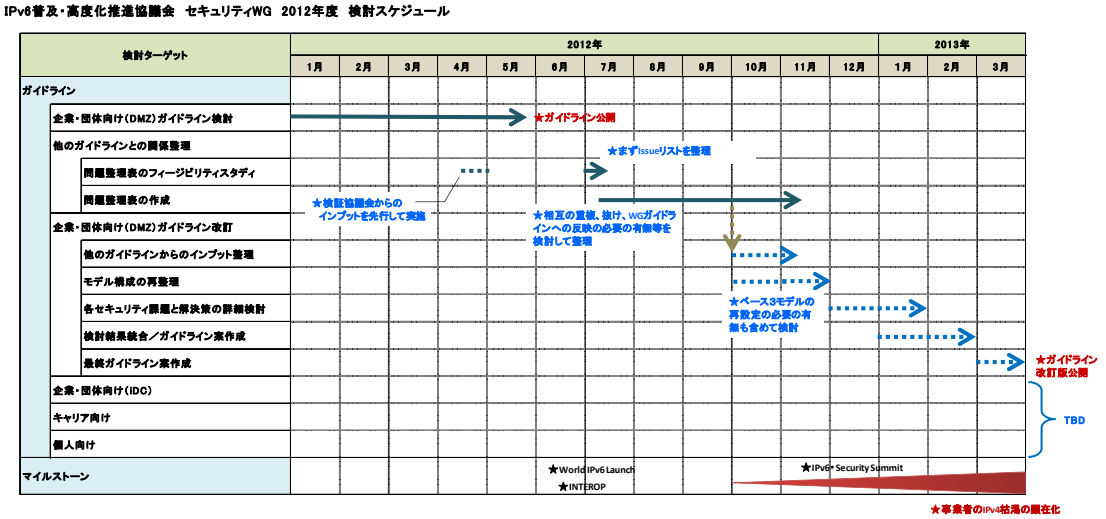

図　1.2-1　セキュリティWGの検討ロードマップ

1.3 他団体との連携関係

IPv6ネットワークのセキュリティについては、日本国内において他にも検討を進めている組織が存在する。個別にはベンダ等が社内にテストベッドを構築して検証を実施している例も見られるが、組織的に実施されている（実施予定の）主要なものとしては、IPv6技術検証協議会とNPO日本ネットワークセキュリティ協会（JNSA）がある。これらの組織は、実際の機材を用いてインシデントに対する脆弱性の検証を行ったり、運用に関する検証を行ったりしており、非常に秘匿性と個別性の高いノウハウを生産する活動を実施している。

セキュリティWGでは、IPv6技術検証協議会、JNSA調査研究部会との間で、役割分担と協調をしつつ、相互に連携することにしている。これらの組織での活動で得られたノウハウ等も取り込み、より多くの関係者が共有可能な一般化された知識の形で、ガイドラインへの組み込みを図り、一般へ公開することで、IPv6セキュリティの確立を目指している。

セキュリティWGおよびIPv6技術検証協議会、JNSA調査研究部会の相互連携について次図に紹介する。

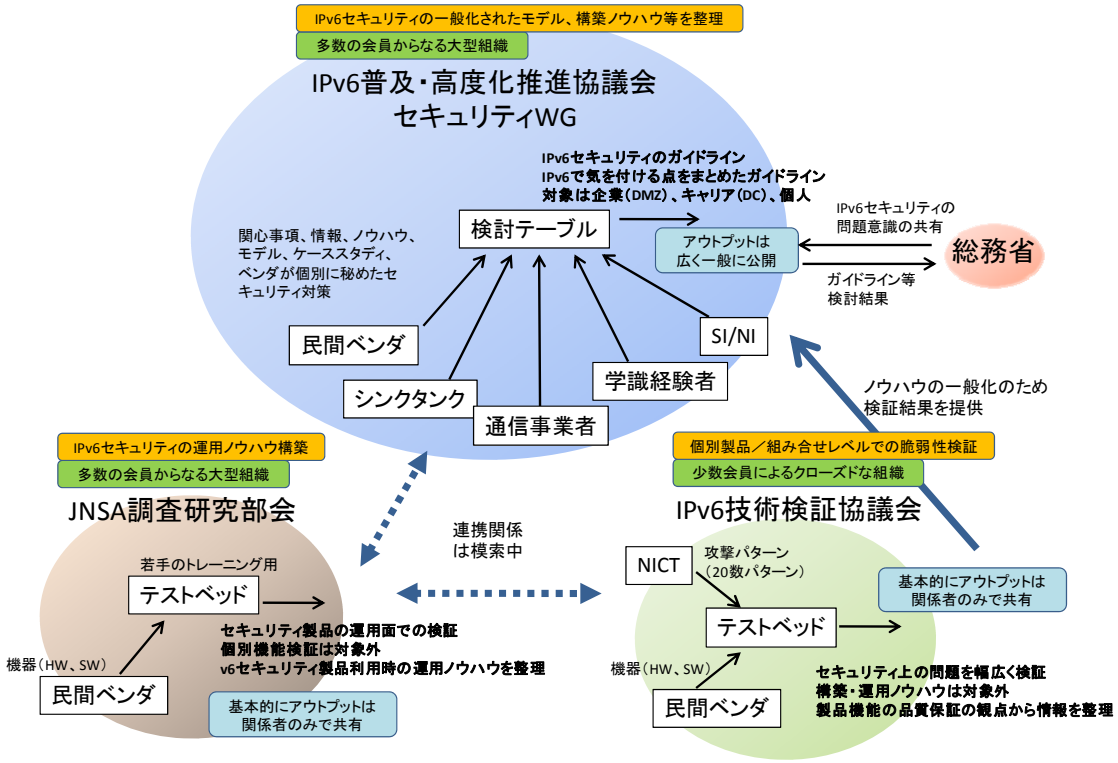

図 1.3-1 IPv6技術検証協議会、JNSA調査研究部会との連携関係

1.4 本書の内容

1.1節で述べた優先順位に従い、企業ネットワークのDMZをIPv6に対応させる際の構成方法について、セキュリティ確保の観点から取り得る形態、考慮点、懸念点、及び対策等について検討した。詳細については2章で解説する。

2 企業ネットワーク（DMZ）を対象とした検討

本章においては、今後広く利用されることが想定されるIPv6を利用したDMZモデルとして、3つのネットワーク・セキュリティモデルを検討した。各モデルには、それぞれ配置される物理コンポーネントや、要求される機能が異なるため、先ず、IPv6を考慮したDMZデザインにおけるセキュリティを鑑みた必要機能を洗い出し、それらを現時点で実現可能となるよう検討を行った。

モデルとしては、IPv4とIPv6が混在するモデル、独立するモデル等の検討を十分に行い、それらのメリット・デメリットを洗いだした。ここでは、セキュリティのみを考慮したモデルではなく、広く普及されることを意識し、費用対効果、管理運用の容易さ、IPv4からIPv6へ対応する際に発生する工数、障害発生時の対処方法等、様々な観点からの検討を加えている。

2.1 セキュリティ確保のための機能要素

本節では、IPv6においてIPv4と同等のセキュリティを確保するために必要となる機能を要素毎に分類し、それらを担う各物理コンポーネントについて精査した。これらを検討対象モデルにて考慮すべきセキュリティ要件とともに検討した。

2.1.1 考慮すべきセキュリティ機能要件

2.1.1.1 通信経路上の制御

セキュリティを考慮した「通信経路上の制御」とは、以下3点に分類できる。

（1）通信機器へのアクセスを制御

ネットワークに設置されている通信機器（ルータやスイッチ等）に対するアクセス制御を実施すること。例えば、ルータ等に対するping(ICMP Echo Request)やtracerouteなどに応答しないこと、機器自身に対するTCP SYN Flood等の攻撃を可能な限り回避すること、機器へのログインを認可したIPアドレスをもつホストからのみに制限することなどが含まれる。

本制御は、通信機器においてパケットフィルター機能などを用いて実装されることが多いが、それに限らない。

（2）セキュリティデバイスなどを用いた通信内容の制御

近年の攻撃通信は、OSI参照モデルにおける第3層（ネットワーク層/IP層）に対する攻撃よりも、第4層(トランスポート層/TCP,UDP層)及びそれよりも上位の層に対するものが多くなっている。このような状況に対応した制御を実施するためには、いわゆるIPS (Intrusion Prevention System)やWAF (Web Application Firewall)などを導入することが多い。

（3）通信方法(経路方式や分散方式など)の制御

ネットワーク通信において、経路情報は非常に重要な情報である。この経路情報には、ネットワーク層(IP層)における経路の他にデータリンク層(Ethernet層)における経路情報がある。例えば、ARP Spoofingなどはデータリンク層に対する攻撃である。この種の攻撃からネットワークを保護するために、経路情報の交換方式（ルーティングプロトコル等）を選択できるだけでなく、対向機器との認証、帯域を有効活用するためのパケットへの優先順位の付加、サーバの冗長化に対

する自由度の高い負荷分散などの機能を備えた制御を行うことが必要となる。

2.1.1.2 個別アプリケーションの対応

アプリケーションは、サービス提供の中心的存在である。したがって理想的には、アプリケーション側で十分にセキュリティが考慮され対応されていれば、究極的には通信経路上のネットワークでは、最小限のセキュリティ対策を実装すれば良くなる。したがって、アプリケーションセキュリティは十分に考慮されるべきである。その上で、通信経路上に十分なセキュリティデバイスを導入し、多段で防御することで、未知の脆弱性が発見された場合に、通信経路上のセキュリティデバイスによって一時的な保護を行うように運用すれば、サービス提供を行う「系としてのロバスト性」を高め、ソフトウェアの改修までの時間を稼ぐこともできるようになる。

既存のアプリケーションを修正し、アプリケーションをIPv6に対応させる場合に、特に注意する必要があるセキュリティ関連項目を以下に記載する。

- IPv6アドレスの取扱い
  - アプリケーション内部でのIPアドレスの処理がIPv4に依存している場合、IPv6アドレスの処理時にバッファオーバーラン等を引き起こす可能性がある。したがって、IPアドレスを取扱う部分に対して十分に注意を払う。
- Cookie等に記録される情報の取扱い
  - Cookie内に記載される情報の生成がIPv4アドレスを前提としている実装が散見される。このようなアプリケーションに関しては、生成ロジックを変更する必要がある。
  - Cookie内の情報としてIPv4アドレスを直接利用している実装がしばしば見られる。特に認証系システムなどでこの種の情報の取扱いがなされている場合が多い。このような実装では、利用者がIPv4/IPv6の両方の空間を利用しており、どちらを利用するかが一位に定まらない場合などに問題が発生する。このような実装の場合、単純にIPv4/IPv6両方に対応させることが困難である。
- 他システムとの連携
  - SSO(Single Sign On)等に代表される統合認証システムや、システム間連動を行うようなアプリケーションでは、IPv4/IPv6が混在した状況でシステム連携を行う必要がある。
    このようなシステムでは、IPアドレスに依存しない認証情報の保持や機器特定の方式などを実装する必要がある。

2.1.2 機能要件を有する物理コンポーネント

前節で述べた機能概要と、技術名称としての機能要素（機能モデル）、および実際に市販されている物理コンポーネントの関係を図 2.1.2-1 機能概要と機能要素と物理コンポーネントの関係に示す。

次節以降は本節で述べている機能要素を用いるものとする。つまり、「機器」としての取扱いではなく、「機能」としての要素を列記した。図に表した各用語は次のとおりである。

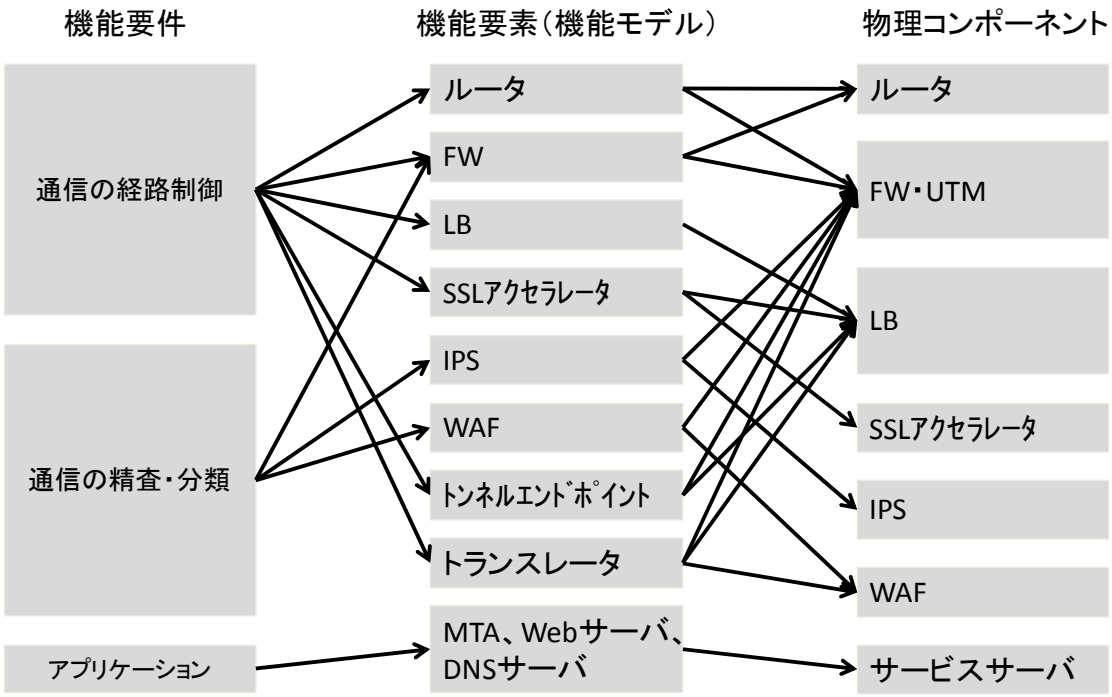

図 2.1.2-1 機能概要と機能要素と物理コンポーネントの関係

・ルータ

TCP/IP(v4/v6)通信において経路制御を行う機能。この機能によって、複数の異なるIPネットワークを繋ぐ役割を担う。

中小規模のネットワークにおいては、ファイアウォール機器に実装されているルータ機能を用いる場合も多い。

ルータは、本ガイドラインでは、対外接続ポイントに設置する経路制御機能として取扱う。

・ファイアウォール（FW）・UTM

ネットワークの経路上で、特定の通信の通過・遮断、および記録を取る機能。

この機能をもつ機器はネットワークの境界に設置されることが多く、多くのFW機器はルータ機能もあわせ持つ。

FWに加え、VPN終端機能やアンチウイルス機能、後述のIPS機能やWAF機能など、複数の機能を包含した機器を特にUTM (Unified Threat Management)と呼ぶことがある。

FW・UTMは、本ガイドラインでは、パケットフィルタリング（送信元・先のIPv4/IPv6アドレス、送信元・先のTCP/UDPポートを用いたフィルタリング機能）を行う機器として取扱う。

・SSLアクセラレータ

近年では、セキュリティ保護の観点から、メール（SMTP/POP3/IMAP4等）やWeb（HTTP等）などの通信を保護することが望まれており、SSL (Secure Socket Layer)やTLS (Transport Layer Security)が用いられている。このSSL・TLS処理における暗号を高速化するために用いられる機器をSSLアクセラレータという。SSLアクセラレータは機能というよりは機器であるが、セキュリティを考慮するに際して採り上げる必要があるため、敢えて記載する。

SSLやTLSにおける暗号処理は計算量が多いため、サービスシステム（特にサーバ）に大きな負荷をかける可能性がある。SSLアクセラレータはこの負荷の高い暗号処理を一手に担うことで、サービスシステム全体（特にサーバ）の負荷軽減を図る目的で利用されることが多い。

なお、SSL/TLSは通信内容を暗号化するため、後述のIPSやWAFを用いて通信の分析を行う場合は、先に何らかの方法で通信内容を復号しておく必要がある。そのために、SSLアクセラレータを利用することが増えてきている。

SSLアクセラレータは、SSLやTLSの暗号処理を行う機器として取扱う。

・ロードバランサ(LB)

複数のサービスシステムに、負荷を分散させるための機能。

TCP/IPの設計は負荷分散の考えは含まれておらず、DNS Round-Robinを用いたサーバの切り替えによるアクセスの分散しか負荷分散の方法が無かった。しかし、この方法では障害を起こしたサーバを切り離すためにはDNSの設定変更を行う以外に対応策はない。これは、運用上の負荷を上げることになり、また、DNSを外部に委託しているような場合には即時対応できないなどの問題が残る。

このような問題に対処するために、サーバの代わりにアクセスを受け取り、適切に通信や負荷を分散させるための機器がロードバランサである。

現在のサービスはWebを利用している例が多く、その通信を保護するためにSSL/TLSを利用していることが多いため、通信セッションの維持管理を行うLBとSSLアクセラレータの機能を実装し、集中的に管理できるコンポーネントをLB機器として提供している場合が多い。

LBは、本ガイドラインでは、負荷分散を行う機能として取扱う。

・侵入防御システム(Intrusion Prevention System/IPS)

通信内容を分析し、保護対象のシステムに対する攻撃を検知し、攻撃通信であると判断した場合に攻撃が来たことを報告し、その通信を遮断する機能。但し、一般にIPSはトランスポート層（OSI参照モデルにおける第4層）までを対象とし、更に上位の層の通信に関しては一部の物しか検出しないものが多い。

遮断を行わず、報告のみを行う機器（もしくはソフトウェア）は、侵入検知システム(Intrusion Detection System/IDS)と呼び、IPSとは区別される。一般にIPS・IDSといった場合、その機能をもつ機器を想定することが多いが、Host IPSやHost IDSと呼ばれるソフトウェアによる実装も存在する。

IPS・IDSは、その分析の特性上、暗号化されている通信を分析することはできない。したがって、何らかの形で復号された、生の通信が取得できる位置に設置する必要がある。

IPSは本ガイドラインでは、攻撃通信の検知・遮断を行う機器として取扱う。

・Webアプリケーションファイアウォール(WAF)

Webの通信に特化し、通信内容を分析して保護対象のWebアプリケーションに対する攻撃を検知し、攻撃通信であると判断した場合にその通信を遮断する機能。

Webを利用したサービスが増加するとともに、Webアプリケーションを狙った攻撃も急激に増え

ることとなった。これらの攻撃はネットワークやサーバに対する攻撃ではなく、アプリケーションの脆弱性やバグを突くものであるため、通信プロトコル上の異常はなく、通常の通信と同様に見える。また、Web通信における攻撃はその種類が多いため、FWやIPSでは防御が困難である。IPSでも技術的には対応できるはずだが、検出のためのパターンが多岐にわたり膨大になるため、現状IPSでWeb通信まで保護させることは難しい。そこでWebの通信に特化し、クライアントとサーバ間でやりとりされるデータの内容も含めて防御可能な機能としてWAFが開発された。

WAFは、本ガイドラインでは、Webの通信に特化した攻撃通信の検知・遮断を行う機能として取扱う。

・トランスレータ

IPv6からIPv4への変換、その逆など、異なる通信の間に入り、変換を行う機能。

この機能は、ルータ、FWやLBなどに含まれていることが多い。

トランスレータは、本ガイドラインでは、IPv6とIPv4の変換を行う機能として取扱う。

・サービスサーバ（MTA、Webサーバ、DNSサーバ）

一般にサーバといった場合、「物理的なサーバハードウェア」と「サーバアプリケーション」の両方を指すことが多い。サーバの中で、利用者に対しメールやWeb、DNS等のサービスを提供するものを特にサービスサーバと呼ぶものとする。

セキュリティ的には「保護の対象」であり、ネットワークで保護するだけではなく、サーバ自身の設定でも保護する必要がある。

サービスサーバは、本ガイドラインでは取扱わない。

2.2 セキュリティを考慮したDMZのIPv6ネットワークモデル

本節では、企業ネットワークのDMZにおけるIPv6対応の際に考慮すべきセキュリティモデルについて記載する。

一般に、通信プロトコルとしてのIPv6への対応に関しては、様々な文献、報告等が広く公開されており、これらを参照することでIPv4ネットワークからIPv4/IPv6の両方に対応したネットワークへの移行は比較的容易であると考えられる。しかしこれらの文献ではセキュリティについて触れられていないものも多く、現実のインターネットの状況を考慮すると、IPv6に対応させたとしても、利用者にセキュリティ上の不安が残ってしまうと考えられる。したがって、IPv6に対応する際のセキュリティ対応についての考慮が、必要となる。

本ガイドラインでは、ネットワークのIPv6対応に関して実装可能なモデルを定義し、そのモデル毎のイメージと説明、各々の注意事項を述べ、セキュリティの観点からそれぞれのメリットとデメリットを議論する。

2.2.1 セキュリティ確保のための物理コンポーネントの配置

物理コンポーネントの配置は機器が増える毎に加速度的に複雑化するため、機能を考慮した単

純なケースを考える。仮に、セキュリティを考慮しないでよいネットワークを構築するならば、図2.2.1-1の「最も単純な構造」に記載した非常に簡単な構造でサービスを提供することが可能である。この場合、IPv6への対応方策は、本質的には、各コンポーネントのIPv6対応（とIPv6アドレスの取得・割り当て）のみでよい。このレベルの知見は現時点でも十分に蓄積されており、IPv6インターネットに接続できる環境であれば、単純にIPv6対応が可能となる。

しかしながら現実のネットワークでは、大量に送られてくるSPAMとよばれるUCE(Unsolicited Commercial Email)やUBE(Unsolicited Bulk Email)、絶え間なく行われるポートスキャン等、様々な攻撃、探索が行われており、そのような迷惑行為からシステムを防御するための仕組みが導入されている。加えて、サービスの可用性確保のための冗長化やLB装置の投入などもなされているのが現実である。

このような状況に対応することのできる、概念的なネットワーク構造として当WGで検討したのが、図 2.2.1-1の「現実の構造（概念）」である。この構造はあくまで概念であり、利用している機材等の状況に応じて、各コンポーネントの有無、コンポーネントの統合等があり、また、コンポーネントが投入されている位置が異なる場合もある。

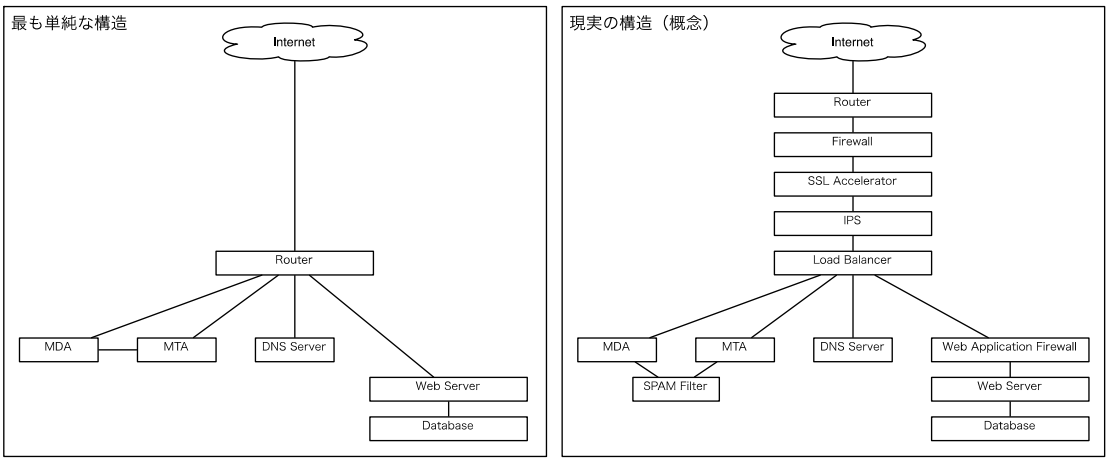

図 2.2.1-1 DMZのネットワークのモデル構造

2.2.2 典型的なIPv6導入モデル

本項では、検討対象モデルに関するメリット・デメリットを記載する。

インターネットに対して公開されているサービスを運用する上で重要なことは、サービスの可用性、安全性、機密性、いわゆるCIA（Confidentiality、Integrity、Availability）の確保である。サービスシステムを構築することは、その後長く続くサービスの提供、運用の第一歩であり、構築すること自体はゴールではない。サービスシステムを構築し、長期間に渡って安全に運用し、そのコストを回収するという流れこそが重要である。

この点を考慮し、サービスシステムのIPv6対応のために考えられる代表的な構成は、パラレルスタックモデル（Parallel Stack Model）、デュアルスタックモデル（Dual Stack Model）、トランスレータモデル（Translator Model）の3つがある。

(1) パラレルスタックモデルは、IPv4とIPv6を分離し、ネットワークとしてIPv4とIPv6を独立に構築、管理、運用する構成である。

(2) デュアルスタックモデルは、サービスシステムを構成するそれぞれの機器においてIPv4/IPv6の両方を取り扱えるように設定して動作させ、運用する構成である。

(3) トランスレータモデルは、サイトへの入口からサービスサーバへの入口までの間のどこかで、流入してくる全ての通信をIPv4（もしくはIPv6）に変換し、サービスシステムで取扱う通信プロトコルを1つにしてしまう構成である。

以下の各節に、それぞれの構成を説明する。

本ガイドラインでは、それぞれのモデル毎にメリットとデメリットを記載している。本ガイドラインの利用者は、各モデルの記述を参考に、それぞれの状況に合わせたメリット・デメリットの検討を行うべきである。また可能な限り、各モデルに記載されているコンポーネントを整備することが望ましい。

2.2.3 パラレルスタックモデル

パラレルスタックモデルとは、IPv4とIPv6のネットワークを分離して構築・運用するモデルである。このモデルの例を図 2.2.3-1に示す。

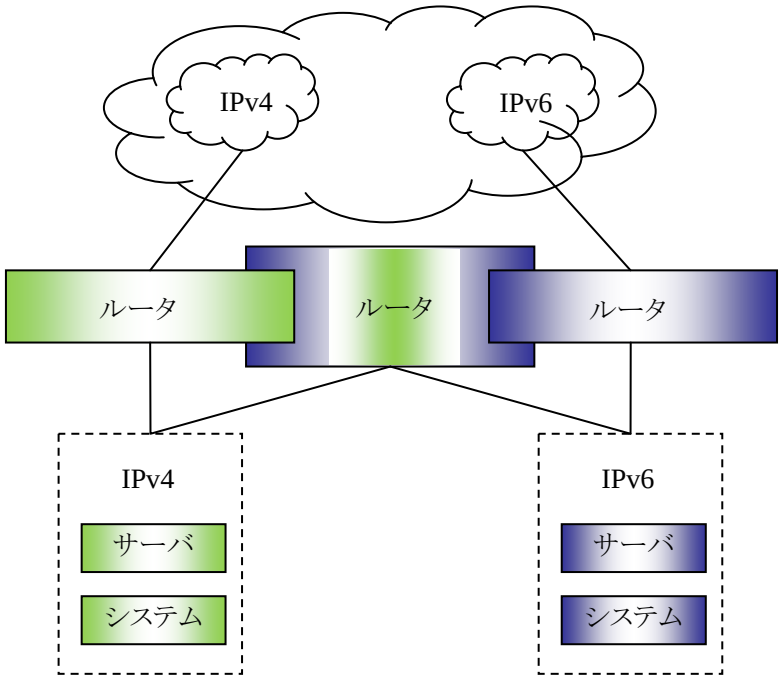

図 2.2.3-1 パラレルスタック構成

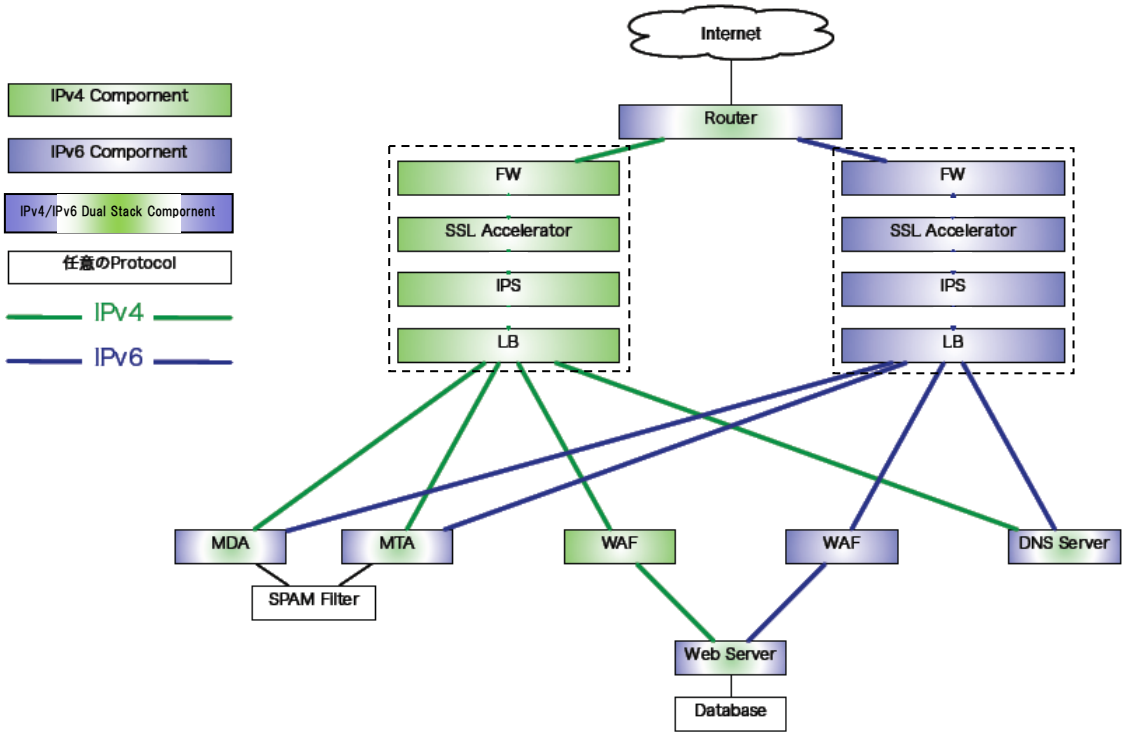

図 2.2.3-2 現実的なパラレルスタックモデルの例

2.2.3.1 モデルの概要

サービスシステム（いわゆるサーバ）をIPv6対応するにあたって最も単純に考えられる手法は、既存のIPv4ネットワーク上に構築されたIPv4用サービスシステムとは別に、IPv6のネットワーク上にIPv6用サービスシステムを構築するパラレルスタックモデルである。しかしながら、現実のサービスシステムにおいては、各種のサービス機能が複雑に連動していることが多く、既存のIPv4用サービスシステムと完全に分離されたサービスシステム（特にサーバシステム）を、IPv6用に新たに構築した別のサービスシステムで提供することは難しいことが多い。一方、本ガイドライン執筆時点において、Web サーバやメールサーバなどのほとんどのサービスサーバアプリケーションは既にIPv6に対応していると言える状況にある。

このため、ネットワークはIPv4用とIPv6用に分けて構築するが、サービスシステムの最前面に立つWebサーバやメールサーバなどは、IPv4用とIPv6用に分けずにデュアルスタックにして通信を集約し、サービスシステムのバックエンド（データベース等）は現状のIPv4のままで、デュアルスタック化しないという手法をとることで、パラレルスタックモデルを実現することが可能となる。

図 2.2.3-2は、このような現実的なパラレルスタックモデルを示している。

2.2.3.2 モデルの特徴

パラレルスタックモデルを用いたIPv6対応におけるメリットとデメリットを記載する。

（1）パラレルスタックモデルのメリット

パラレルスタックモデルでは、IPv4ネットワークとIPv6ネットワークが分離されているために以下のようなメリットがある。

・分界点が明確になる

セキュリティ上の問題（セキュリティイベント）が発生した時に、そのセキュリティイベントが「IPv4で起こったもの」なのか「IPv6で起こったもの」なのかが明確に分離される。そのため、分析や対策の検討が容易になる。

また、IPv4、IPv6のうち一方のネットワークでセキュリティ上の問題が生じても、その影響が他方のネットワークには波及しないという効果も期待できる。

・ネットワークの安定的な運用の確保

本ガイドライン執筆時点では、いわゆるセキュリティデバイス（FW/IPS/WAF等）は、IPv6での運用実績が少なく、安定性を十分に担保できない懸念がある。パラレルスタックモデルでは、運用が確立しているIPv4ネットワークと、新しく構築されるIPv6ネットワークが分離されているため、少なくともIPv4サービスに関しては安定して運用することが可能になる。

・概念が単純

IPv4とIPv6を分離しているため、ネットワークの構成などの全体的な概念が単純になる。

また、IPv4のみのサービスネットワークからIPv6にも対応したネットワークに移行する際に、IPv6ネットワーク部分のみを試験し、サービスに付加することが可能になる。

このため、セキュリティ上の考慮点（FWのポリシー等）の検討や、各セキュリティデバイスの設定などが比較的簡単になる。

（2）パラレルスタックモデルのデメリット

・コスト高

このモデルは、少なくともネットワーク部分を新たに構築する必要があるため、初期投資としての機器費用が必要になる。また、必要に応じて保守費用が付加される。

加えて、電力消費量が増加し、場所を必要とするため、ラック費用や追加電源が必要になり、このコストは定常的に必要となる。

・管理対象が増える

機材が増えるため、当然管理・監視しなければならない機器が増加する。したがって、運用上の工数が増加する。

2.2.4 デュアルスタックモデル

デュアルスタックモデルとは、それぞれのコンポーネントにおいて、IPv4/IPv6を同列に扱い処理させることでサービスを提供するモデルである。このモデルの例を図 2.2.4-1に示す。

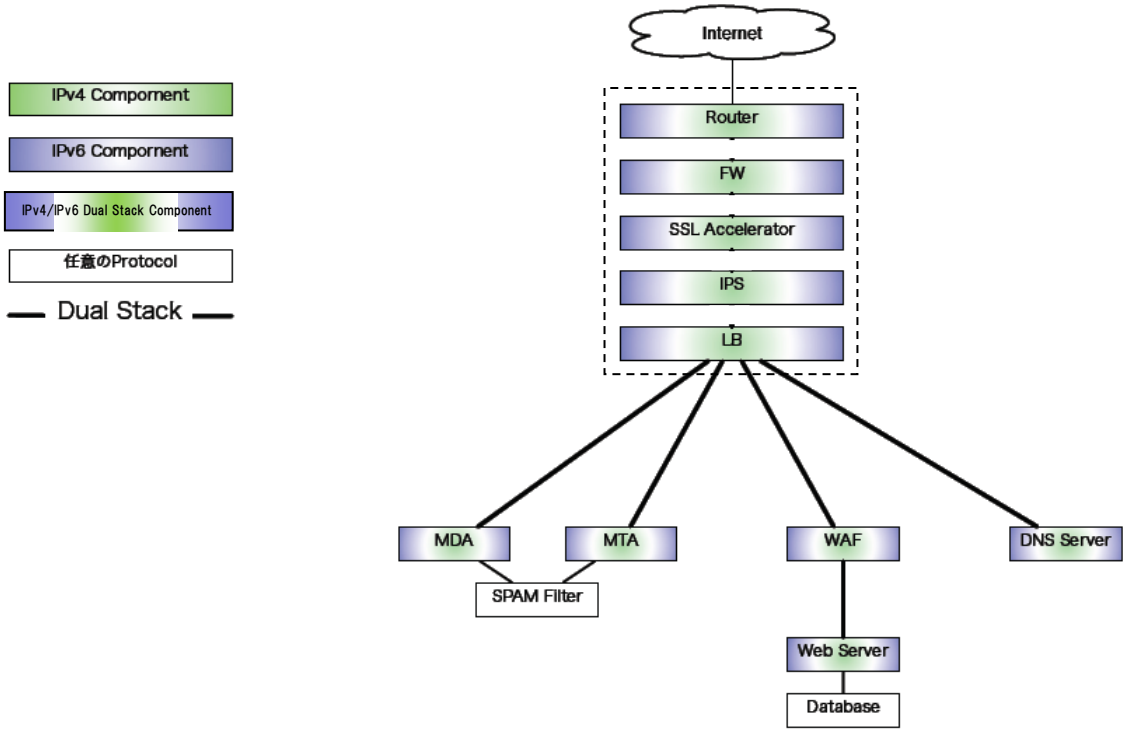

図 2.2.4-1デュアルスタックモデルの例

2.2.4.1 モデルの概要

IPv6対応が議論され始めた当初から、各種機器のIPv6対応に関しては、デュアルスタックによる利用が行えるように検討されてきた。本ガイドライン執筆時点において一般に流通しているネットワーク機器においては、多くの場合、基本的にはIPv4/IPv6デュアルスタックに対応していると考えられる。

この状況を利用し、サービスにおける各コンポーネント(機器)を全てデュアルスタックとして運用するのがデュアルスタックモデルである。

2.2.4.2 モデルの特徴

デュアルスタックモデルにおけるメリットとデメリットを記載する。

(1)デュアルスタックモデルのメリット

・新規投資が少ない

ネットワーク機器の寿命は9～10年程度(減価償却期間が一般に9～10年)と考えられており、現在サービスネットワークに利用されている機材は概ねここ10年以内に調達されているものと考えられる。実際には機器の減価償却期間を5年以内に設定している組織が多いと考えられる。したがって、現在サービスに供されている大半のネットワーク機器は、多くの場合デュアルスタックに対応していると考えられる。以上より、最悪の場合でもファームウェアの更新でデュアルスタックに対応できる可能性が高いと考えられる。

(2) デュアルスタックモデルのデメリット

・セキュリティ機器の実績

本ガイドライン執筆時点において、各種セキュリティ機器はIPv6環境もしくはIPv4/IPv6デュアルスタック環境で稼動した実績が少ない。したがって、運用・管理も含めると、製品としてはIPv6対応環境における十分な知見が蓄積されていないと考えざるを得ない。このような状況では、何か障害があった場合に問題の切り分け、分析に時間がかかり、結果としてサービスの停止期間が長期化する可能性があり、緊急時の初期対応が複雑化する可能性がある。また、現時点でIPv6に対応していないセキュリティ機器も存在しており、必要に応じて機材の置き換えが必要となる可能性もある。

また、セキュリティ監視システムを導入している場合、セキュリティデバイスがIPv6に対応しているにもかかわらず、監視システムがIPv6に対応していないことによる運用上の問題が発生する可能性がある。特に、監視システムがIPv6のログを分析できないためにIPv6通信を監視できないという問題は見落としやすいため、十分に調査しておく必要がある。

・ネットワーク構造の変更が必要な場合がある

コストの問題等、様々な事情でNATを駆使したネットワークを構成している場合、IPv6を対象とするNAT機能が利用できない等の理由により、単純にIPv4/IPv6デュアルスタック構成を取ることができず、ネットワーク構造の変更が必要な場合がある。

このような変更を行う場合、セキュリティポリシーや設定の内容などを再度検討しなおす必要が生まれることになる。この対応の過程において、IPv4/IPv6の差異の部分を設定し忘れる、あるいは設定ミスに気づかずセキュリティ的に穴をあけてしまうなど、人為的ミスが発生する可能性がある。

・分析・運用工数が増加する

デュアルスタックで運用する場合、通信の分析・解釈のための工数が増加する。一般にはIPv4のみの場合と比べて倍になると認識されているが、実際には、以下のような通信が発生する可能性があり、その全ての通信パターンを追跡・分析する必要が生じる。

・端末(IPv4)→サービスネットワーク(IPv4)

・端末(IPv4)→トランスレーション機能(IPv4→IPv6)→サービスネットワーク(IPv6)

・端末(IPv6)→トランスレーション機能(IPv6→IPv4)→サービスネットワーク(IPv4)

・端末(IPv6)→サービスネットワーク(IPv6)

したがって、デュアルスタックモデルにおいては、分析・運用工数が最悪4倍になる可能性がある。

さらに、機器によって、IPv4アドレスをIPv4アドレスとして扱うもの、IPv4マップドアドレス(IPv4射影アドレス)として扱うもの、(非常に少数ではあるが)IPv4互換アドレスとして扱うものがあるため、それらを何らかの形で正規化するといった作業が発生する可能性もある。

・障害の影響範囲が広い

デュアルスタックモデルでは、各コンポーネントがIPv4/IPv6両方を取扱うことになる。したがっ

て、あるコンポーネントに障害が発生した場合、その影響がIPv4/IPv6両方に影響してしまう可能性がある。その結果として、IPv4/IPv6プロトコルに起因する障害が、本来は障害に関係ない側にまで影響を与え、サービスが完全に停止してしまう可能性がある。

同様に、セキュリティイベントを検知した際の対応に関しても、対応策の影響範囲を十分に見極めて、イベントが発生したプロトコルでは無い方に影響が出ないよう注意する必要がある。

2.2.5 トランスレータモデル

トランスレータモデルとは、現状保持しているIPv4ネットワークを変更することなく、IPv6をIPv4に変換することでIPv4/IPv6両方に対応するというモデルである。

このトランスレータモデルでは、トランスレータをどこに投入するかで複数の構造が考えられる。図 2.2.5-1 トランスレータモデルの例は、インターネットとの接続点でIPv6をIPv4に変換するモデルを示しているが、逆にLBの位置にトランスレータを設置し、サーバのみをIPv4で動かすといった構造も可能である。本ガイドラインでは、詳細な内容を検討中ということもあり、前者の場合を取り上げることとする。

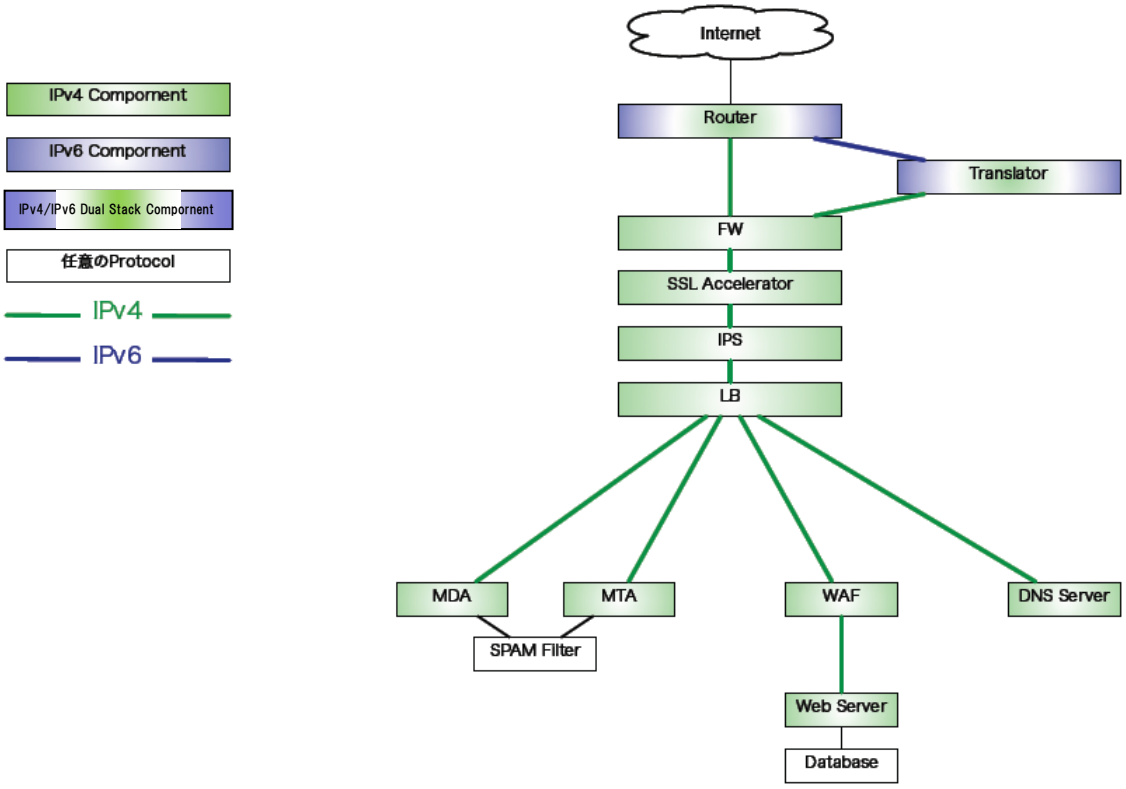

図 2.2.5-1 トランスレータモデルの例

2.2.5.1 モデルの概要

IPv6への移行における過渡期の手法として、全てのIPv6通信をIPv4に変換し、既存システムを変更せずにIPv6に対応させるモデルである。

2.2.5.2 モデルの特徴

本モデルは、IPv6によるサービス通信を、サービスの出入り口において、全てIPv4に変換するものである。したがって、IPv4におけるNATを使用したサービスモデルと同様の問題が生じる。

以下にトランスレータモデルにおけるメリットとデメリットを記載する。

(1)トランスレータモデルのメリット

・トランスレータを投入するのみでその他の部分をほとんど変更する必要が無い

ネットワークの変更点はトランスレータを投入することのみであり、コストが低い。

(2)トランスレータモデルのデメリット

・実績が非常に少ない

このモデルを実現するには、高性能(高機能ではない)なトランスレータを導入する必要がある。しかし、このような高性能なトランスレータは非常に新しい実装であり、十分な運用実績があるとは言えない。

・障害発生時の対応が難しい

トランスレータはNATと同様、通信における接続の状態を保持し、管理するといった制御を行う必要がある。これは、送信元の各種情報と受信先の各種情報に関する対応表をそれぞれの接続毎に持ち、管理する必要があるためである。このような実装においては、障害発生時に障害の起きている通信を特定し、その原因を追及することが困難であり、障害対応が遅れることになる可能性が高まる。

また、セキュリティイベントを検知した場合に、そのイベントが「IPv6通信によって発生した」のか「IPv4通信によって発生したのか」を区別することが困難になる。これは、緊急対応などを行う際に、問題になる可能性がある。

・セキュリティ機器の通信制御が難しくなる

セキュリティ機器は、一般的には、攻撃を検知した際の通信遮断方法として、送信元IPアドレスからの通信を遮断するといった手法を利用する場合が多い。これは、送信元ポートは通常ランダムであり、あらかじめ特定できないことによる。しかし、トランスレータを利用する場合、トランスレータによって変換される送信元IPアドレスのレンジは非常に狭く(トランスレータが持つアドレス空間のみ)、複数の通信が同一の送信元IPアドレスに割り当てられやすくなる。したがって、本来遮断すべきでない通信まで遮断されてしまう可能性がある。

2.3 今後の検討

今後の検討予定を含む2012年度の計画を図2.3-1セキュリティWGの検討ロードマップ(再掲)に示す。

今後は、

(1)共存モデルを示す

(2)共存状態におけるセキュリティ対策

を2本柱とした議論が重要になると考えており、両者とも業界全体として考えなければならない課題である。また、オペレーションの観点への言及も必要となるだろう。

このため、IPv6に関するセキュリティを含む課題について言及している他の活動成果との関係整理を進める中で、業界全体としての問題整理表を作成し、特に共存環境を意識する形で、議論を更に深めていく予定である。

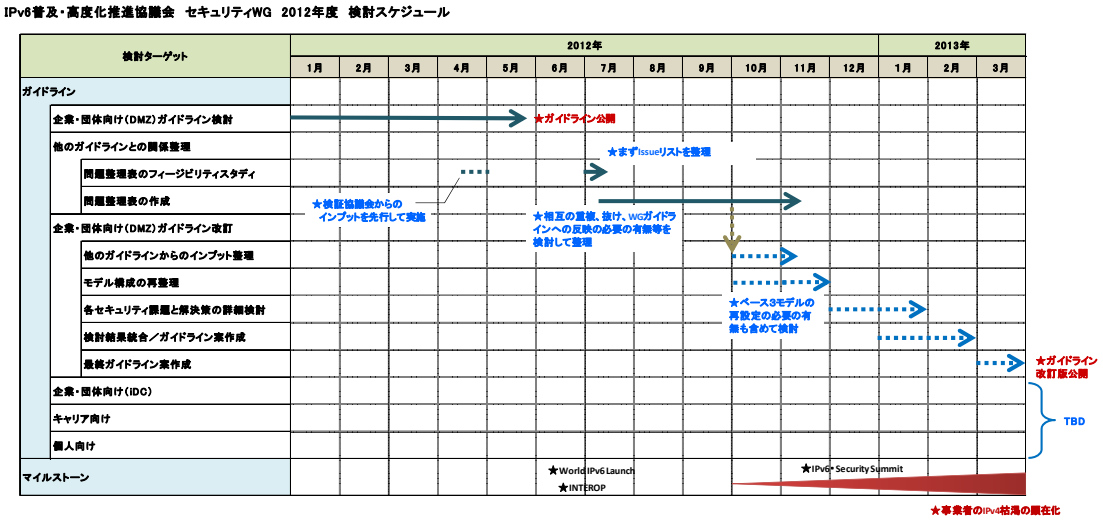

図2.3-1セキュリティWGの検討ロードマップ（再掲）

APPENDIX　IPv6時代のネットワークセキュリティの考え方

APPENDIX.A　各機能要素において考慮すべきセキュリティ要件について

ここでは、各機能要素において考慮すべきセキュリティ要件を列挙する。この要件は、各検討対象モデルについて議論を実施した際にIPv6に特化した要件としてリストアップしたものである。また、個々の機能要素については、必要な要件であるが、現状、十分な要件とはなっていない。

今後、IPv6導入に起因する問題検討SWGと連携し、それぞれの視点から提起された要件と共に、整理・分担し、相互に解決策を提供していく必要がある。

- 全機能要素対象の要件
  - すべての機能要素について、機能要素を実装している機器自身を守ることが必要である。機能要素が実装されている機器が乗っ取られたり、内部に保有する情報が漏洩したりすることのないようにすることが必要である（2.1.1.1 (1)も参照）。

- ルータ
  - 仕様上、禁止された機能を含むパケットを転送しないようにすることが必要である（RH0等）。
  - 自分宛の ICMP への対応が必要。返答するかどうかはサイトのポリシーに依存する。
  - IPv6 PAアドレス（プロバイダ集約可能アドレス）を利用してマルチホームをする際には始点アドレスに基づく経路制御（ISP選択）が必要である（マルチプレフィックス問題）。
  - DDoS に対する対策が必要である。

- ファイアウォール
  - IPv6拡張ヘッダについて、検査する階層数、及び、種別によるフィルタの考慮が必要である（数珠つなぎのヘッダへの対応）。
  - 断片化されたIPv6パケットについて、フィルタ等の目的のため、再構成が必要である。
  - IPv6では、プロトコル動作上通過させるべきICMPv6メッセージが存在することへの考慮が必要である（IPv4でのICMP全フィルタ的ポリシーをIPv6に演繹しないようにすることが必要）。特に、DDoS対策目的でのフィルタに注意する。
  - 特にIPv6導入期では、トンネルされたIPv6パケットへの注意が必要である。ペイロードに含まれるIPv6パケットについて、チェックが必要な場合がある。

- 中間デバイス（LB、IPS、SSLアクセラレータ等）
  - 特にIPv6導入期では、トンネルされたIPv6パケットへの注意が必要である。ペイロードに含ま

れるIPv6パケットについて、チェックが必要な場合がある。

- アプリケーション（2.1.1.2より再掲）

アプリケーションは、サービス提供の中心的存在である。したがって理想的には、アプリケーション側で十分にセキュリティが考慮され対応されていれば、中間段階でのセキュリティ対応が楽になる。その意味で、アプリケーションセキュリティは十分に考慮されるべきである。

アプリケーション側で考慮すべきセキュリティ対応の中で、特にIPv6において注意する必要がある項目を以下に記載する。

- IPv6アドレスの取扱い
  - システム内部でのIPアドレスの取扱いがIPv4に依存している場合、IPv6アドレスが取扱えない、もしくはバッファオーバーラン等を引き起こす可能性がある。
- Cookie等に記録される情報の取扱い
  - Cookie内に記載される情報の生成にIPv4アドレスを利用している実装がしばしば散見される。このようなアプリケーションに関しては、情報生成ロジックを変更する必要がある。
- 他システムとの連携
  - SSO(Single Sign On)等に代表される統合認証システムや、システム間連動を行うようなアプリケーションでは、IPv4/IPv6が混在した状況でシステム連携を行う必要がある。したがって、複数のシステムをまたがったアプリケーションシステムでは、アドレスの取扱いを含め、複数のプロトコルを同時に利用することが可能になるような実装を行う必要がある。

APPENDIX.B 現場の声

インターネットやセキュリティの第一線に関わる技術者のIPv6セキュリティに関する見解を「現場の声」として紹介する。まず、それらの声から言えるIPv6セキュリティに対応するための要件について整理した。

要件: 変化に対応する

- どのようなサービスを誰にどのように提供し、どう守るかを見直す。

要件: IPv6 only ホストの登場

- APNICのIPv4アドレスはすでに事実上枯渇した。
- 特にモバイルでは、1～2年のうちにもIPv6だけでインターネットを利用するホストが登場する。

要件: あなたも狙われている

- 攻撃はインターネット全域でコンピュータによって自動化されて実行されており、「自分のサイトだけは別、狙われない」ということはない。

要件: インフラ、ソフトウェアの更改タイミングを活用する

- 今のところIPv6対応だけでは新たな価値を生み出しにくいため、システムの更新、見直しタイミングでIPv6対応を検討する。しかしIPv6化の波が来るときは一度に来るかもしれない。

要件: 「知らないうちにつながっていた」を避ける

- IPv4 onlyで運用するサイトはIPv6を遮断することを忘れないように。
- Windows 7、Android、iPhoneなど、新しいソフトは標準状態でIPv6対応しているため「知らないうちにIPv6でインターネットに直結していた」ことになる。

B-1 現場の声1

セキュリティというものは、悪人との追いかけっこである。そのため、常に100%安全ということはない。また新しい攻撃手法が開発されたりして脅威が増えるために、時間とともに安全度は低下していく。

これまでセキュリティ業界は、「これを入れれば大丈夫」という安易なキャッチフレーズで次々と新しい製品を発売してきた。これは一時的に新しい脅威に対する機能を追加し対策をしたように見えるが、その箱のメンテナンスがなされなかったり、新たなボトルネックを作ってしまい、システム的な対応がとれなくなったりするといったことがおこっている。

IPv6に関しては、IPv4だけで作られたシステムに新たなプロトコル・機能を追加するため、システムとしても根本的な見直しが必要となってくる。また、各種セキュリティに関する装置の実装状況も発展途上なところもあるため、何を想定し、何をどのような方法で守るかを考えることが必要である。

この報告に書いてある内容は、現在のセキュリティに関する基本的な機能は何か、それを今、実

装すればこうなるという例を示している。それはベストなシステム構成でもなければ、将来的にも安全だといっているわけではない。ただし、この報告のように必要な機能を整理し、それをシステム的に実装するというアプローチは今後も有効であり、そのアプローチはIPv4、IPv6といったプロトコルに関わらず必要である。

IPv6の導入というタイミングで、これまで作られたセキュリティシステムもこの機会に見直しを行い、再設計をすべきである。

B-2 現場の声2

サービスネットワークにおいて、セキュリティは本質的に確保されなければならないものである。インターネットがまだ善意の人の利用するものであった牧歌的な時代においては、そもそも利用者が少なく、利用者の顔も見えており、また他のシステムを攻撃することにあまり意味が無かった。しかし、現代ではそのような仮定は危険である。

しかしながら現状を鑑みるに、サービスネットワークを提供している事業者の大半は

「うちなんか攻撃しても意味ないだろう」

「うちなんかに攻撃してくることはないだろう」

といった根拠のない思い込みや

「そうは言っても金が無い（からやれない）」

といった、ある種の「甘えの構図」があったと云わざるを得ない部分がある。また、セキュリティを確保しようという意志のある事業者でも、

「何を選べばいいか判らないから、出入りの業者の勧めるものを使う」

「これを導入すれば大丈夫と業者が言ったからそれを」

といった、自身で考えることをせずに外部に丸投げをしてしまうような例もしばしば見掛ける。

このような事態の根底には

「水と空気と安全と情報は無料」

「金が無いんだからしかたがないじゃないか」

といった甘えや、

「何を、誰から、幾らかけて、どのように護り、何を諦めるのか」

といった定義を自ら考えることをしない発注者側の問題と

「機器の詳細なんか判らないが、カタログに丸がついているから大丈夫だろう」

「売れてしまって保守代をもらえれば、後は野となれ山となれだ」

といった営業・販売側の勝手な事情や

「トラブったらその時に考えよう。どうせそんなに攻撃なんか受けないだろう」

といった、販売側の勝手な思い込み等によって増幅された、販売側の傲慢と購入側の怠慢ではないかと考えたくなるような事例がいくつも見られる。

IPv6対応に関しても同様の事が云える。

- 本当にアドレス割り当てが受けられなくなりそうになってから慌ててIPv6対応を考え、
- 考え始めたら実は「何がIPv6に対応しているのか」わからなくなり
- 慌ててベンダに確認したが自社のシステムに適用できるのかどうかも判らず、

- 判らないが故に必要なものの選別ができず、
- 結果的に必要以上に高価な機材を購入してみたり、実は問題のある機材を購入してしまったりする上に
- セキュリティ的には実は大穴が空いている

といった事態が発生する可能性があることが容易に想像される。この流れは大げさな例かもしれないが、実際に十分に起こり得るシナリオであると考えざるを得ない。

そもそもセキュリティの問題を考える場合、「絶対安全」や「100%大丈夫」等ということは、それこそ絶対にありえない。唯一考えられるとしたら、誰も利用しないシステムをインターネットに繋がないという「そもそも無意味」な状況でしかないだろう。広い目で見れば、ネットワークに接続され、誰かが利用するシステムは必ずセキュリティ上の問題を持っていると考えなければならない。そのリスクを最小限に押さえるのがセキュリティと言うものの本質であろう。

現時点で、IPv6ネットワークを、セキュリティを（ある程度以上）確保してサービスを提供することは非常に難しいと言わざるを得ない。それは、IPv6に対応しているセキュリティデバイスといえど、実績がほぼ無いに等しい状況であることや、IPv6を用いた攻撃に対する知見が溜まっていないこと等に起因する。

細かな例を言えば、ログの分析にあたって、省略記法と正式な128bit分を全て表示する記法のどちらを採用するべきかといった議論から、大きな部分では、そもそものネットワーク構造をどう構築するかといった議論まで、IPv4とIPv6が混在する環境に移行し、そのセキュリティを確保することの難しさ、事例の少なさを実感せざるを得ない。

この機会に、サービスネットワークと言うものを足元から見直し、どのようにセキュリティを確保するのか、セキュリティ運用を自前で行う事が可能なのか、今の機器でどこまでのセキュリティを確保することができるのかを問い直すことを奨めたい。

B-3 現場の声3

IANAのIPv4アドレスプールに続き、APNIC/JPNICの在庫も枯渇した状況であるが、IPv6への対応は本当に必要なのだろうか。確かに、大手のISPなどは今後の事業継続のためにはIPv6対応を真剣に考えなければいけないだろう。しかし、一般の企業などにとっては、IPv4アドレス枯渇からどのような影響を受けるのか、今ひとつ実感できないのではないだろうか。そこで、一般の企業ネットワークでIPv6対応がどの程度真剣に求められるのか、改めて考えてみる。

・イントラネット内をIPv6対応すべきか

中長期的にはその必要もあるだろうが、当面はIPv4のままでも問題ない。現状のイントラ内で使用されているソフトウェアのIPv6への対応可否を検証することがなかなか難しい。特に自社向けにカスタマイズしているアプリケーションを使用している場合、検証には大きなコストがかかる場合がある。それに対して今すぐにIPv6対応した場合のメリットを（少なくとも定量的には）見出しづらい。ただし、今後のイントラネット内の機器やソフトウェアの更改のタイミングでは、IPv6対応のものに変えていくべきである。

・DMZをIPv6対応すべきか

今後は「IPv6でしかアクセスできないユーザが現れるので、公開Webサーバなどインターネットとの接続を前提としたシステムはIPv6対応する必要がある」と言われている。これも中長期的には正しいだろうが、実際にこういうユーザはいつ頃現れるのだろうか。少なくとも国内では、ISPは何とかIPv4アドレスを調達または捻出して、IPv4グローバスアドレスを配れないユーザを作りたくはないはずだ。そういうユーザにはIPv6アドレスとCGN（Carrier Grade NAT）配下のIPv4プライベートアドレスを配布するのだろうが、運用コストが上がるのに対して利用料金を上げるわけにはいかないからだ。企業ネットワークの運用者ががんばってDMZをIPv6対応したが、実際には「IPv6でのアクセスなど、どこからも来ない」となるのだろうか？

国内の一部のISPは既にIPv6サービスを開始しており、KDDIのau光サービスではユーザが意識しなくてもIPv6/IPv4デュアルスタックでのサービスが開始されている。2011年6月以降にはNTT東西のNGNによるIPv6接続サービス（いわゆる「PPPoE方式」と「IPoE方式」）も始まり、次第にIPv6でアクセスするユーザは増えて行くはずだ。さらに、アジアなどインターネットが急激に発展している地域では、早い時期（2012年中にも？）にIPv6でしかアクセスできないユーザが出現するかもしれない。また、上記のNGNや通信キャリア各社が整備中のLTEでもIPv6をベースとしたサービスが登場する可能性がある。企業ネットワークで、今後これらのNGNやLTEのIPv6サービスを活用することは十分にありうると考えられる。このように、グローバルの環境や今後登場が期待される新サービスを考えると、企業ネットワークの管理者が早い時期からIPv6に親しんでおくことは無駄にはならないだろう。確かに、特にセキュリティの面から考えると、IPv6に関する運用については、本資料でまとめられているようにまだまだ課題が多いことも事実である。つまり、企業のネットワーク管理者は、今まさに

- 将来の本格的なIPv6対応に向けて、まずDMZのIPv6化からスタートする
- 本当にIPv6が必要とされる時まで待ち、今は何もしない

のどちらの対応とするか、判断が求められているのである。どちらの判断が正しいのか、現時点では正直なところわからない。ただし、IPv6対応は始めてすぐに完了するわけではなく、運用ノウハウの蓄積が必要であることを考えると、早い時期からネットワークの一部だけでもIPv6での運用を試行していくのがいいだろう。企業ネットワークの管理者の方々には、アンテナを高くして情報収集に励み、適切な判断を下されることを望みます。

検討メンバー

下記に検討メンバーを示す。会務担当者以外のメンバーは、所属の50音順に従っている。

氏名	所属
篠田 陽一（WG主査）	北陸先端科学技術大学院大学
藤崎 智宏（副査）	日本電信電話株式会社
津国 剛（事務局）	株式会社三菱総合研究所
新 善文	アラクサラネットワークス株式会社
佐藤 友治	財団法人インターネット協会／株式会社ブロードバンドセキュリティ
北口 善明	金沢大学 総合メディア基盤センター
小野寺 好広	シスコシステムズ合同会社
坂根 昌一	シスコシステムズ合同会社
西原 敏夫	シスコシステムズ合同会社
服部 亜紀子	シスコシステムズ合同会社
平賀 十志男	ソニーグローバルソリューションズ株式会社
今井 恵一	日本電気株式会社
宮永 直樹	日本電気株式会社
山形 昌也	日本電気株式会社
加藤 雅彦	NPO 日本ネットワークセキュリティ協会 調査研究部会長
林 憲明	日本ネットワークセキュリティ協会 調査研究部会 IPv6セキュリティ検証WG／トレンドマイクロ株式会社
花山 寛	ネットワンシステムズ株式会社
小野 一志	パナソニック株式会社
志田 智	株式会社ユビテック カスタマーサービスタスク
許 先明	株式会社ラック／日本セキュリティオペレーション事業者協議会（ISOG-J）
鵜飼 拓男	総務省データ通信課
田邉 大	総務省データ通信課