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 0.5 版）

（企業ネットワーク（DMZ）に関する中間報告書）

平成２３年４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	2011 年 5 月 31 日（予定）	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として 1.0 版を発行

目次

1 はじめに 1

1.1 セキュリティ WG の活動趣旨 1
1.1.1 目標とするスコープ 1
1.1.2 優先順位 1
1.1.3 その他の一般的な IPv6 セキュリティ問題 2
1.2 セキュリティ WG の検討ロードマップ 4
1.3 他団体との連携関係 4
1.4 本書の内容 5

2 企業ネットワーク（DMZ）を対象としたガイドライン（中間報告） 6

2.1 機能要件毎のセキュリティ要件 6
2.1.1 機能要素の説明 6
2.1.2 物理コンポーネントの説明 7
2.2 検討対象モデルの説明 10
2.2.1 機能要素と物理コンポーネントのマッピング 10
2.2.2 検討対象モデルの選択 11
2.2.3 パラレルスタックモデル 11
2.2.4 デュアルスタックモデル 13
2.2.5 トランスレータモデル 15

APPENDIX IPV6 時代のネットワークセキュリティの考え方 18

APPENDIX.A 現場の声 1 18
APPENDIX.B 現場の声 2 18
APPENDIX.C 現場の声 3 20

検討メンバ 22

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 への移行にあたって 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（0.5 版）では、セキュリティ WG での 2011 年 4 月時点の検討状況について報告する。

1.1 セキュリティ WG の活動趣旨

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り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 目標とするスコープ

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。

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 に関して、第一優先で検討を行う。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、比較的対策が進んでいるキャリア（事業者、ISP）、他と比べてネットワーク構成が単純であり、セキュリティを確保しやすい個人に関しては、当面は優先順位を下げて考える。

1.1.3 その他の一般的な IPv6 セキュリティ問題

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参考情報として展開的に適用可能なものとなることを目指している。

一方、IPv6 への移行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考情報として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 23 年 4 月 21 日情報セキュリティ政策会議決定）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以下の 3 点への遵守を求めている。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。

2.4.1.1 情報システムへの IPv6 技術の導入における対策

遵守事項

(1) IPv6 移行機構がもたらす脆弱性対策

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、情報システムに IPv6 技術を利用する通信（以下「IPv6 通信」という。）の機能を導入する場合には、IPv6 移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。

(2) 意図しない IPv6 通信の抑止と監視

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、IPv6 通信を想定していない通信回線に接続されるすべての電子計算機及び通信回線装置に対して、IPv6 通信を抑止するための措置を講ずること。

【強化遵守事項】

(b) 情報システムセキュリティ責任者は、IPv6 通信を想定していない通信回線を監視し、IPv6

通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講ずること。

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 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。

IPv6 導入に起因する問題検討 SWG では、現在報告書を取りまとめ中であり、パブリックコメント公開の上で、2011 年 5 月下旬には正式公開を予定している。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る予定となっており、必要に応じて参考とすることが望ましい。

公開予定先ページ： http://www.v6pc.jp/jp/wg/coexistenceWG/v6fix-swg.phtml

例：不正 RA 問題についての現在検討中の内容（抜粋） ※最終的には公開版を参照のこと。

問題名：

不正なルータ広告による通信不全の問題

問題の解説：

･想定していない機器による RA の広告で、同一リンク上の機器にディフォルト経路、（プレフィックス）が追加付与され、

1.通信が混乱する問題

2.OS の動作がおかしくなる問題

対処方法：

･スイッチなどによる RA のフィルタリング

･Router Preference(RFC4191)の利用

･意図的なものは排除できない

･モニタリングによる対策

･NDPMon： セグメント内の NDP パケットの異常を検知

･rafixd(KAME)： 不正 RA と同じ RA を Router Lifetime=0 で広告、不正 RA による機器内容をリセット

･SEND(Secure Neighbor Discovery)の導入

･設定アドレスの上限設定

･無制限に RA を受け付けず上限を実装において設ける

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 2010 年度およびその翌年度も見越した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比較的シンプルである DMZ を対象として検討を行い、その経験を踏まえて、次に iDC を対象とした検討に進む予定でいる。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は、INTEROP の開催時期を意識し、2011 年 5 月末を公開目標として作業を進めている。iDC に関するガイドラインの公開は 2011 年度の下半期を目指している。

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。

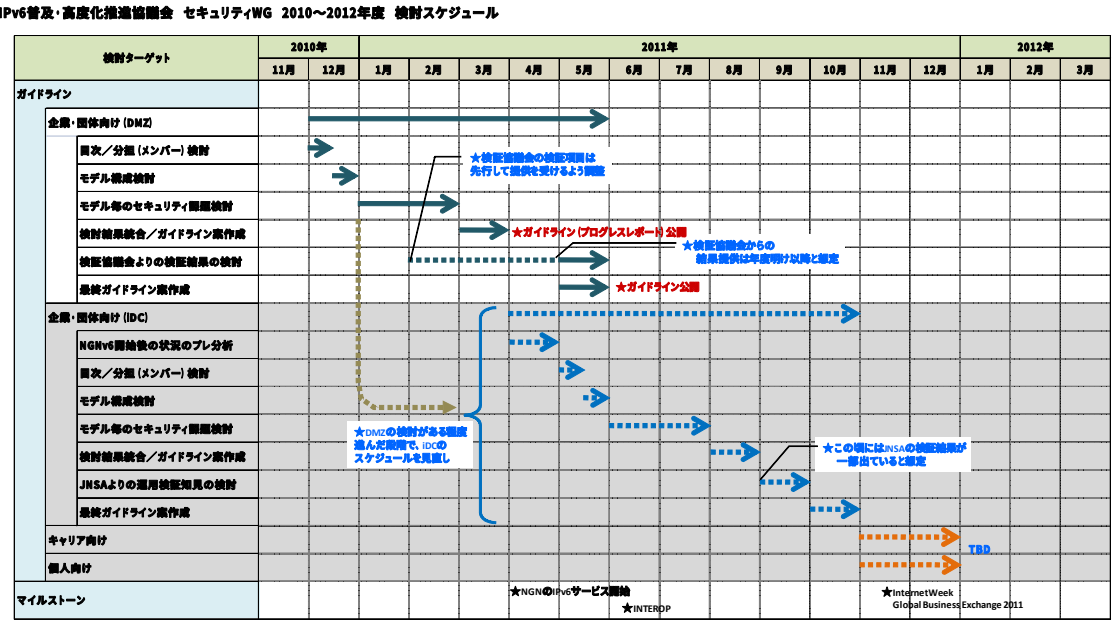

図 1.2-1 セキュリティ WG の検討ロードマップ

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 法人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。

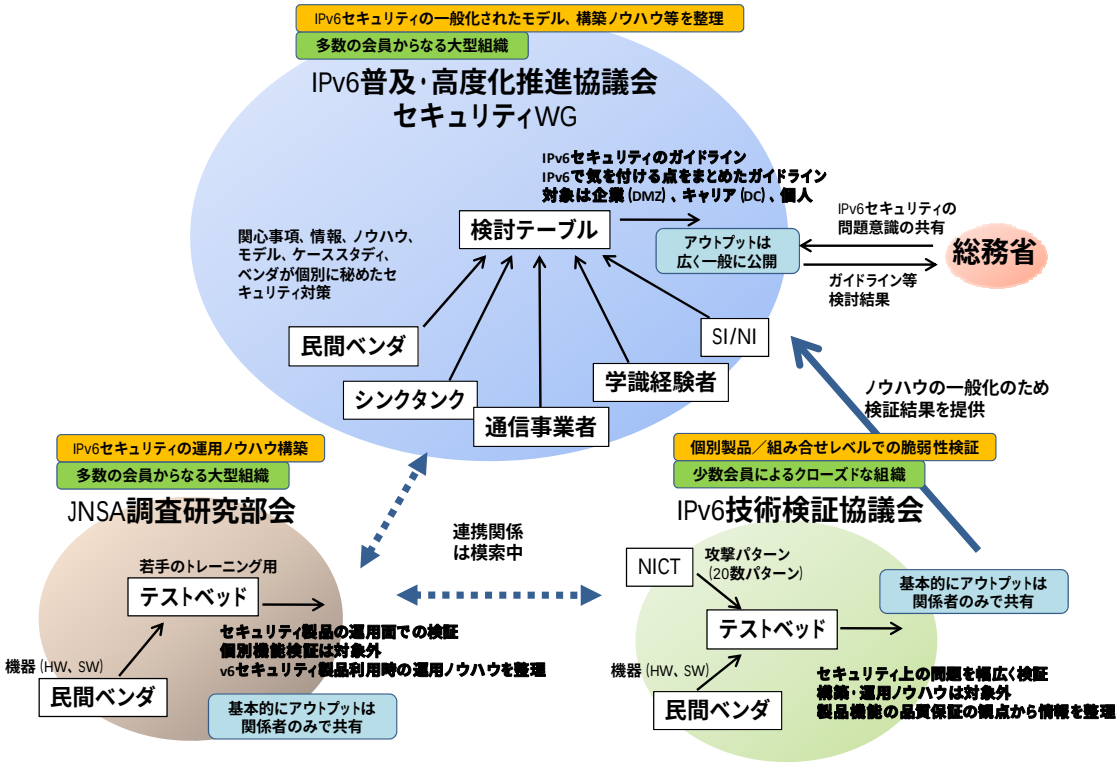

図 1.3-1 IPv6 技術検証協議会、JNSA 調査研究部会との連携関係

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 に移行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、及び懸念点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) を対象としたガイドライン (中間報告)

本章において、セキュリティ WG が推奨する IPv6 を利用した DMZ モデルとして今後広く利用されると想定できる 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する製品に落としこむ検討を行った。

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、それらの利点・不利点を洗いだした。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 へ移行する際に発生する工数、障害発生時の対処方法等、あらゆる観点から検討を行っている。

2.1 機能要件毎のセキュリティ要件

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する。

2.1.1 機能要素の説明

2.1.1.1 通信の経路制御

セキュリティを考慮した「通信の経路制御」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

存在が不明瞭な機器からのトレースルートや ICMP echo request などに応答しない、TCP Syn フラッド攻撃を可能なかぎり回避する、認可した宛先からのみアクセスを可能にする、などの機能を備える必要がある。

(2) 通信機器を流れる通信そのものを制御

外部と DMZ の間を流れる通信において、OSI 基本参照モデルの第 3 層および第 4 層を中心にフィルタリングを実装する機能、断片化された通信の再構築を行う機能などを備える必要がある。

(3) 通信方法(経路方式や分散方式など)

パケットの経路・転送方式を選択できるだけでなく、対向機器との相手認証、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る必要がある。

2.1.1.2 通信の精査・分類

OSI 基本参照モデルの第 2 層から第 7 層までをフィルタリングし、ポリシーに合致しない通信を

破棄する機能だけでなく、悪意のある攻撃に対し予めシグネチャを用意し、それに合致するようであれば通信を破棄する機能が必要となる。つまり、DDoS 攻撃のような低い階層を目標にした攻撃だけでなく、SQL インジェクションやクロスサイトスクリプティングなどのアプリケーション層（第7層）までの攻撃に対し、検知および防御する機能が必要となる。

2.1.1.3 アプリケーション

アプリケーションは、サービス提供の中心的存在である。従って理想的には、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 アドレスが取り扱えない、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。
    従って、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。

2.1.2 物理コンポーネントの説明

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 2.1-1 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。図に表した各用語は次のとおり。

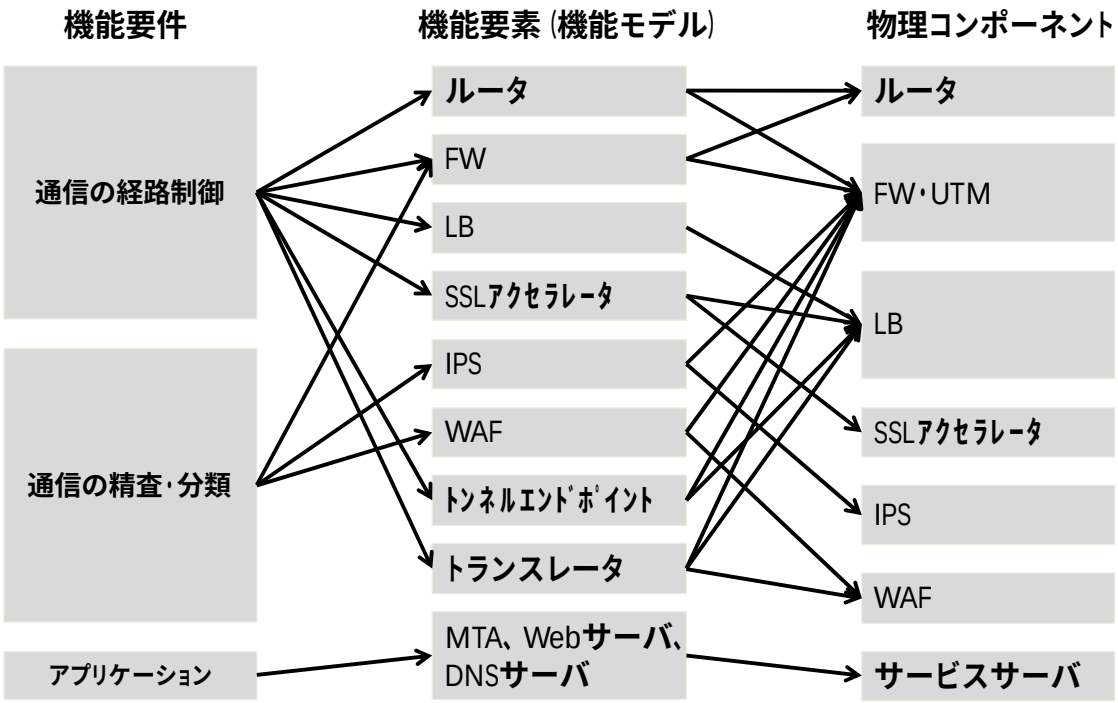

図 2.1-1 機能概要と機能要素と物理コンポーネントの関係

・ルータ

TCP/IP(v4/v6)通信において経路制御を行う機能であり、複数の異なる IP ネットワークを繋ぐ役割を持つ機器である。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を用いている場合も多い。

本報告書内では、対外接続ポイントに設置する経路制御機器として取り扱う。

・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器。ネットワークの境界に設置されることが多く、多くのファイアウォール機器はルータ機能をもあわせ持つ。ファイアウォール（以下、FW）に加え、VPN 終端機能やアンチウイルス機能、後述の IPS や WAF 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。

本報告書内では、パケットフィルタ FW（送信元・先の IPv4/v6 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）のこととして取り扱う。

・SSL アクセラレータ

メール通信（SMTP/POP3/IMAP4 等）や Web 通信（HTTP 等）における通信内容を保護するために用いられる SSL(Secure Socket Layer)や TLS(Transport Layer Security)を高速に処理するための機器。後述の LB（ロードバランサ）の機能の1つに含まれることがある。

SSL や TLS の暗号処理は、非常に多くの計算資源を利用するため、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 通信は通信を暗号化するため、後述の IPS や WAF を用いて通信の分析を行う場合は、これらの機器よりも Internet 側に設置する必要がある。

本報告書内では、SSL や TLS の暗号処理を行う機器として取り扱う。

・ロードバランサ(LB)

複数のサービスシステムに、通信を分散させるための機能を担った機器。

大量のアクセスを処理するためには、非常に大きな計算資源が必要となるが、そのような機器は高価であるため、なかなか導入することができない。また、サービス提供機器が極少数の場合、様々な理由でサービスシステムが停止してしまう可能性がある。例えば、定期メンテナンス、負荷の集中、予期せぬシステム内の障害などである。このような事態に対処するため、サービス提供システムを複数準備し、通信を分散する機能が要望された。この機能を提供するのが LB 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 を利用している例が多いため、通信セッションの維持管理を行う LB に SSL Accelerator の機能を実装し、集中的に管理できるコンポーネントとして提供されている場合が多い。

本報告書内では、負荷分散を行う機器として取り扱う。

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

IPS とは、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装置である。なお、遮断を行わず、報告のみを行う装置の事を侵入検知システム(Intrusion Detection System/IDS)と呼び、IPS と区別する。

IPS は、その分析の特性上、暗号によって保護されている通信を分析することはできない。従って、何らかの形で暗号が解かれている、生の通信が取得できる位置に設置する必要がある。

・Web アプリケーションファイアウォール(WAF)

HTTP/Web を利用したサービスが増え、HTTP に対する攻撃が増えるにつれ、従来の IPS（侵入防御システム、後述）のみでは対応することが困難になってきた。この状況を改善するため、HTTP/Web 通信に特化した IPS のような機器が要望されるようになってきた。このような IPS が WAF である。

・トランスレータ

IPv6 と IPv4 の変換、その逆など、異なる通信の間に入り、変換を行う機器。単体として存在することは少なく、FW や LB、NAT などの機能に含まれることが多い。

・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。そのサーバの中で、利用者に対し、メールや Web、ネーム等のサービスを提供するサーバ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。

本報告書では取り扱わない。

2.2 検討対象モデルの説明

本節では、企業ネットワークのDMZについて、IPv6への移行におけるセキュリティモデルについて記載する。

一般に、IPv6 への移行に関しては、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、セキュリティの問題を避けて通ることはできないのが現状である。従って、IPv6 への移行に際しては、IPv6 環境におけるセキュリティ対応について考慮することが、どうしても必要となる。

以上より、本報告書では、ネットワークの IPv6 移行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、それぞれのメリットとデメリットを議論する。

なお、本書は中間報告書であり、それぞれのモデルに関する詳細等に関しては、未だ議論中であることから、

1) 各モデルの詳細は議論中であるため、現時点での検討を記載する。

2) 各モデル間のメリット・デメリットの比較については、本中間報告書には記載しない。

という方針で作成した。

2.2.1 機能要素と物理コンポーネントのマッピング

まず簡単なケースから考えてみる。仮に、セキュリティを考慮しないでよいネットワークであれば、図 2.2-1 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 への移行方策は、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、比較的単純に IPv6 への移行が可能となる。

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、探索が行われている。加えて、サービスの可用性確保のための冗長化や負荷分散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ネットワークの概念的な構造として当 WG で検討したのが、図 2.2-1 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。

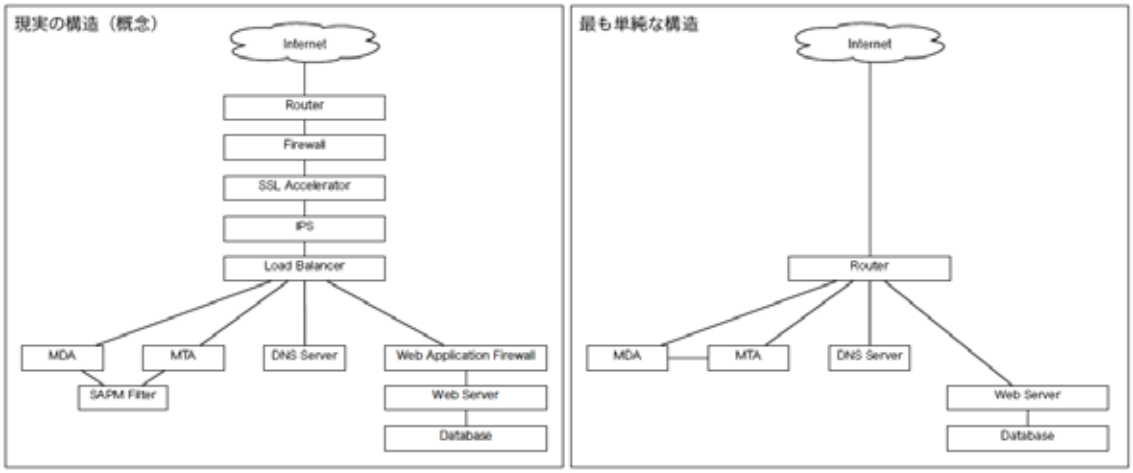

図 2.2-1 DMZ のネットワークのモデル構造

2.2.2 検討対象モデルの選択

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事は、サービスの可用性、安全性、機密性（いわゆる CIA（Availability、Integrity、Confidentiality））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 への移行のためにすぐに考えられる構成は 3 つある。それが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）である。

- パラレルスタックモデル（Parallel Stack Model）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。
- デュアルスタックモデル（Dual Stack Model）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。
- トランスレータモデル（Translator Model）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り扱う通信プロトコルを 1 つにしてしまう構成である。

以下に、それぞれの構成を説明する。

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（Parallel Stack Model）とは、IPv4 と IPv6 を分離して制御するモデルである。このモデルの例を図 2.2-2 に示す。

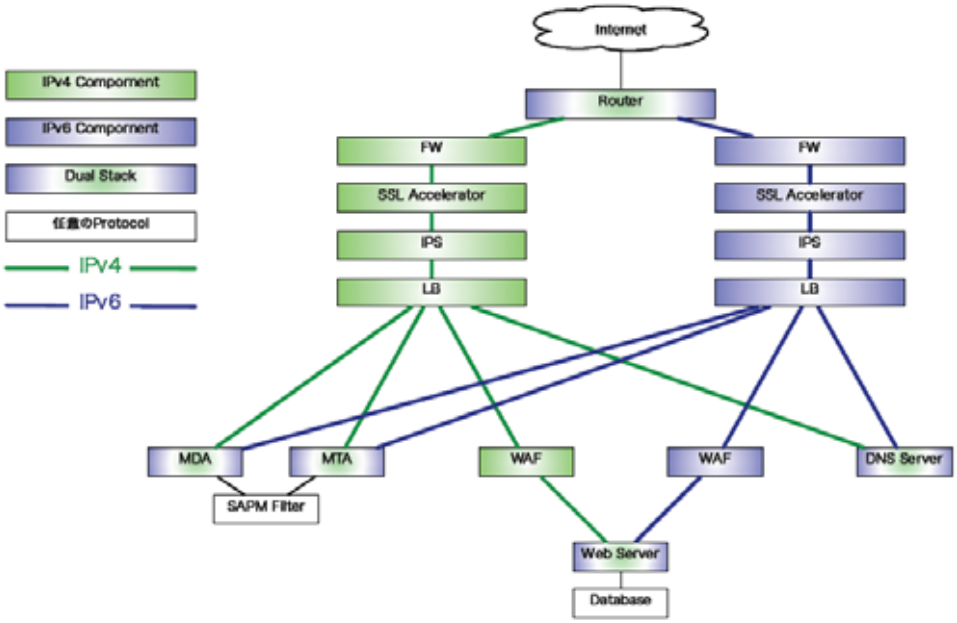

図 2.2-2 パラレルスタックモデルの例

2.2.3.1 モデルの説明

サービスシステムを IPv6 に移行するにあたって、簡単に思いつく手法は、IPv6 専用のサービスシステムを構築することである。しかしながら、現在のサービスネットワークでは、各種のサービス機能が複雑に連動していることが多く、サービス提供システム（いわゆるサーバー群）を完全に分離し、新たに構築することは難しいことが多い。それに加えて、2011 年 3 月現在、ほとんどのサービスアプリケーションは IPv6 に対応していると言える状況にある。

このため、サービス提供システムの最前面に立つサービスシステムについてはデュアルスタック（Dual Stack）にし、サービスネットワークのバックエンド（データベース等）はデュアルスタック化しないという手法をとることが可能となる。

パラレルスタックモデル（Parallel Stack Model）とは、このような構成を取ったサービスネットワークモデルである。

2.2.3.2 モデル特有の注意事項

パラレ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）パラレルスタックモデルのメリット

・分界点が明確になる

障害発生時に、その障害が「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。従って、初期の障害対応が容易になる。

また、片側で起こった障害が逆側に波及しないという効果も期待できる。

・実績があるネットワークと実績が少ないネットワークが分離できる

2011 年 3 月現在、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、安定性を十分に証明できない場合が多い。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。

･移行が容易

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ため、移行が容易である。

･概念が単純

技術的に異なるものを分離しているため、ネットワークの構造などの全体概念が単純になる。

(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る。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。従って、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（Dual Stack Model）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 2.2-3 に示す。

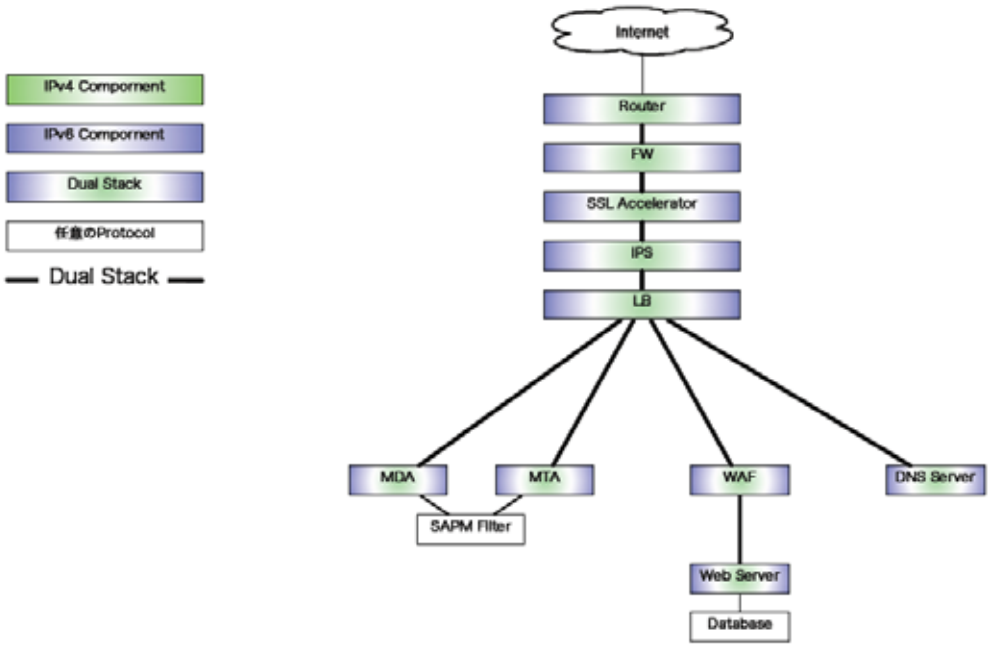

図 2.2-3 デュアルスタックモデルの例

2.2.4.1 モデルの説明

IPv6 への移行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（Dual Stack）による利用が行えるように検討されてきた。2011 年 3 月現在、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（Dual Stack Model）である。

2.2.4.2 モデル特有の注意事項

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一般に 5 年程度（減価償却期間が一般に 5 年以下）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。従って、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。従って、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非常に高いと考えられる。

（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

2011 年 3 月現在、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。従って、運用・管理も含め、製品として 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高く、また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がある。

・ネットワーク構造を変更する必要がある場合がある

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、そのネットワーク構造を単純に IPv4/IPv6 デュアルスタック構成に変更できるとは限らない。

・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ようだが、実際には、以下のような通信が発生する可能性がある。

・端末→(IPv4)→サービスネットワーク

・端末→(IPv4)→Translator→(IPv6)→サービスネットワーク

・端末→(IPv6)→Translator→(IPv4)→サービスネットワーク

・端末→(IPv6)→サービスネットワーク

従って、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 コンパチブルアドレス（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 両方を取り扱うことになる。従って、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。

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、サービスを完全に停止してしまう可能性がある。

2.2.5 トランスレータモデル

トランスレータモデル（Translator Model）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（Translator）をどこに投入するかで複数の構造が考えられる。図 2.2-4 トランスレータモデルの例では、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取り扱ったが、逆にロードバランサ（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考え得る。本報告書では、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。このモデルの例を図 2.2-4 トランスレータモデルの例に示す。

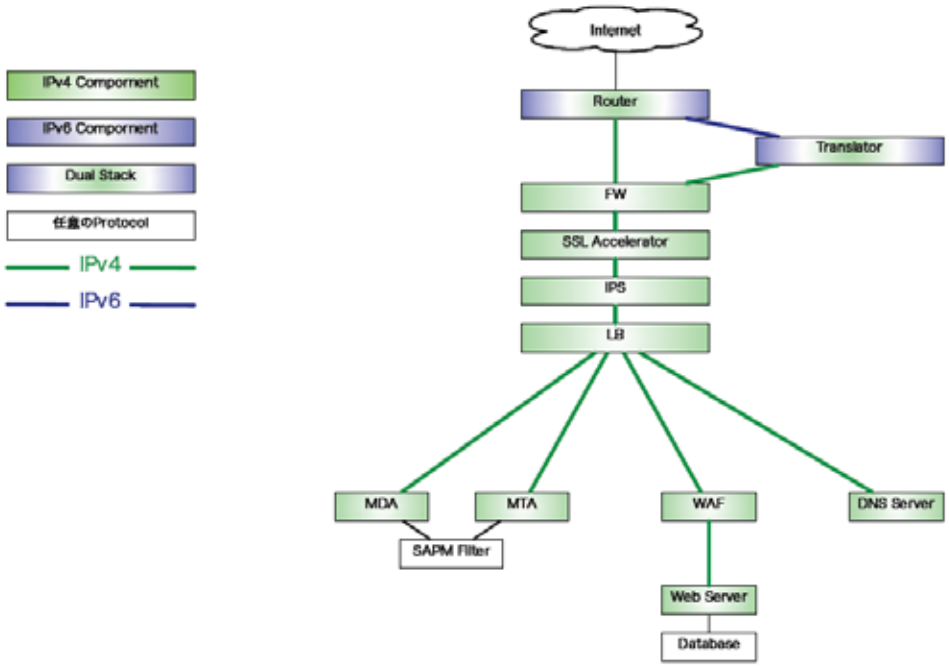

図 2.2-4 トランスレータモデルの例

なお, トランスレータの位置に関しては, セキュリティ WG で別途議論をしており, 今回はネットワーク構成が最も単純になる位置にトランスレータを導入した例のみ議論する。

2.2.5.1 モデルの説明

IPv6 への移行の過渡期の手法として、全ての IPv6 通信を IPv4 に変換して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。

本モデルでは、外部との全ての IPv6 通信を一度 IPv4 に変換し、その上で既存システムに処理させるという手法を用いる。

2.2.5.2 モデル特有の注意事項

本モデルは、サービスの出入り口における通信を全て IPv6 から IPv4 に変換するものである。従って、NAT を利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) Translator Model 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、比較的高性能（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比較的難しい

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原因となっている通信を取り出し、特定することが困難となり、障害対応が遅れること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、決め打ち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。従って、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。

APPENDIX　IPv6 時代のネットワークセキュリティの考え方

APPENDIX.A　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」といって新たな製品を次々に売りつけてきた。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。

APPENDIX.B　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にあるのは

「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をいくつも見てきた。

IPv6 への移行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、
- 考え始めたらじつは「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、
- 結果無意味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。

APPENDIX.C 現場の声3

IANA の IPv4 アドレスプールが枯渇し、まもなく RIR の在庫もなくなろうとしている状況であるが、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 への移行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 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 LSN 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？

短期的には、DMZ の IPv6 対応に関して上記の通りかもしれない。ただし、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（2011 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、2011 年 4 月以降には NTT 東西の NGN による IPv6 接続サービス（いわゆる 「トンネル方式」と「ネイティブ方式」）が始まり、また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。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

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