2005 年 IPv6 移行ガイドライン

SOHO セグメント

2005 年 3 月

IPv6 普及･高度化推進協議会

移行 WG　SOHO SWG

目次

はじめに **3**

1.SOHOセグメントの特徴 **4**

SOHOの分類 4
現在のSOHOネットワーク 4
独立SOHO 4
ぶらさがりSOHO 5

2. 移行へのシナリオ **7**

移行のステップ 7
シナリオの関係 7
検討の軸 8

3.独立SOHOの移行 **10**

独立SOHOの概要 10
ネットワークの移行 11
アプリケーションの移行 14
セキュリティ管理の移行 21
独立SOHO 移行のまとめ 25

4. ぶらさがりSOHO の移行 **28**

ぶらさがりSOHO の概要 28
VPNの移行 30

5. 将来的な利用モデル **31**

将来的な利用イメージ 31
移行への課題 31

6. 要望・課題の整理 **32**

ネットワーク 32
その他の留意点 34
MTU Discovery 34
ホスト名登録 34
アプリケーションの対応 34

移行WG SOHOセグメント 検討メンバ 36
お問い合わせ先 36

はじめに

本ドキュメントは、SOHO の構築に携わる SIer およびシステム導入を検討する利用者/管理者を対象に、SOHO で今後 IPv6 を導入するにあたり、検討すべき一般的な項目、指針、方法について記述しています。

ここで記載される内容は、考え方の例を示すものであり、唯一の解ではありません。読者が、自らの指針により IPv6 の導入を検討する際、このドキュメントを参考に応用が図れるよう記述しました。

1.SOHOセグメントの特徴

SOHOの分類

SOHO と呼ばれる事業所には、以下のようなものがあります。

・個人商店
1 台の PC とインターネット接続回線によるシステム構成。家庭セグメント環境と類似。

・小規模事務所(独立 SOHO)
単一の小規模拠点のみで事業活動を行う企業。上記「1」に加えて、数台の PC と単一サブネット LAN によるシステム構成。

・小規模営業所(ぶら下がり SOHO)
より大規模な組織の小規模拠点。上記「2」に加えて、VPN 利用による外部ネットワーク（本社、ASP のセンター）接続。

・コンビニ店舗
構成機器に POS 端末や Non-PC 系の端末が含まれる。ネットワークも独自構成が多い。

この移行ガイドラインでは、小規模事業所（以下では「独立 SOHO」と呼びます）と小規模営業所（以下では「ぶらさがり SOHO」と呼びます）を対象とします。

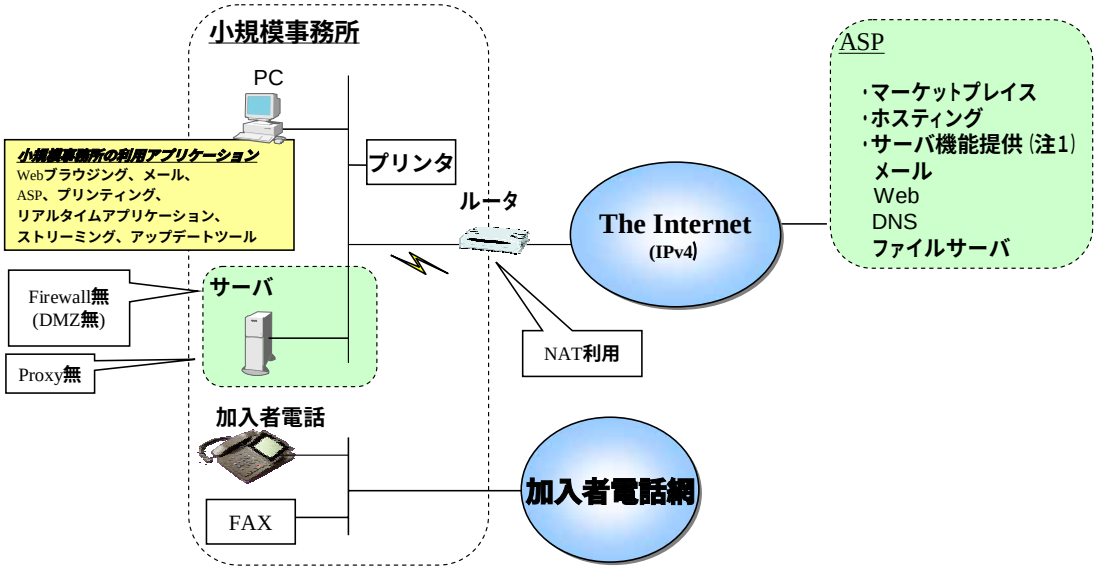
現在のSOHOネットワーク

独立 SOHO

独立 SOHO において、ネットワークはおもに社外とのメールのやり取りやインターネット経由での Web 閲覧に利用されています。また、ASP 利用や自前構築による販売用 Web サイト等にも用いられます。

独立SOHOイメージ

ネットワークは、社外とのメールのやり取り、インターネット経由でのWeb閲覧に利用されている。また、ASP利用や自前構築による販売用Webサイト等にも用いる。

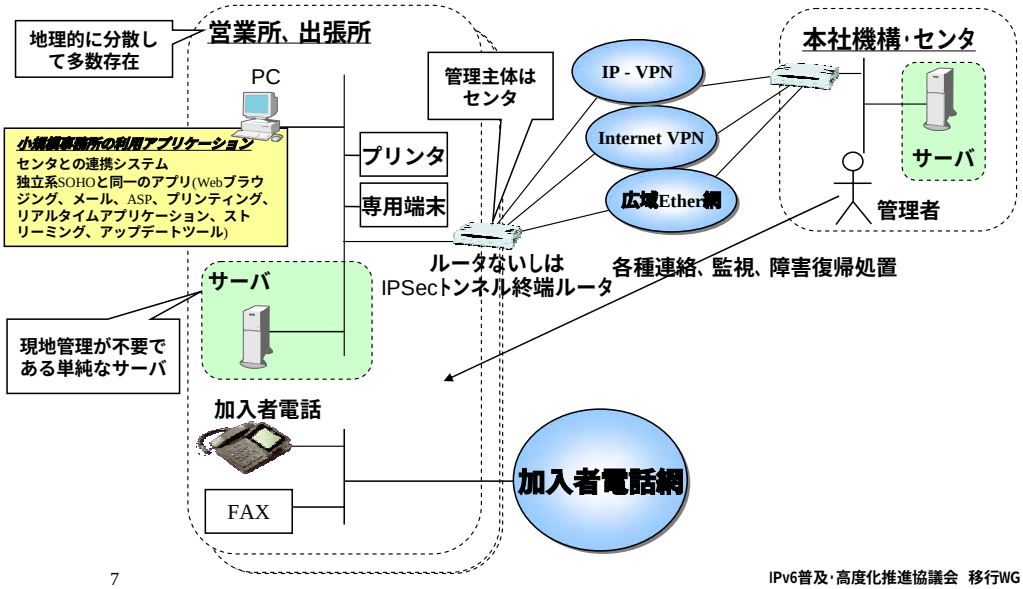


ぶらさがり SOHO

ぶらさがり SOHO の基本的な構成は独立型 SOHO と同じですが、IP-VPN、インターネット VPN、広域イーサネット網などによって管理者のいるセンターと接続しています。

ぶらさがりSOHOイメージ

基本的な構成は独立型SOHOと同じ。管理者の居るセンタとIP-VPN、InternetVPN、広域Ether網などと接続している。



2. 移行へのシナリオ

移行のステップ

ここでは、移行段階を現在の IPv4 利用段階、IPv6 の導入初期段階(IPv6:IPv4=1:9)、IPv6 の本格導入期(IPv6:IPv4=5:5) の 3 つのステップに分けて解説します。

導入初期での 2 つのシナリオ

IPv6 導入の初期には、導入目的によって 2 つのシナリオが考えられます。

①特定目的導入

これは、業務上の目的があり、IPv6 を利用したシステムを導入する場合です。IP 電話、インスタントメッセージなど、利用アプリケーションが IPv6 化されたり、商取引のセキュリティ強化、メンテナンスなどの理由から、取引先が IPv6 化されることがきっかけとなります。これは、現状の IPv4 ネットワークに基本的には手を入れないもので、保守的な IPv6 導入シナリオということができます。

②将来準備導入

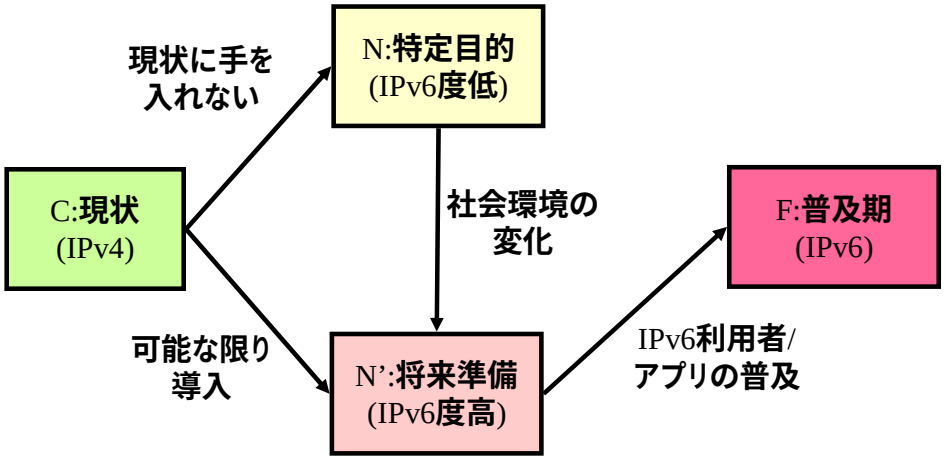
将来的に IPv6 になることを想定して、システムリプレースのタイミングで IPv6 を利用できるようにしておく場合です。これは、積極的な IPv6 導入と言えます。

本ガイドラインでは、現状の IPv4 利用が、特定目的の IPv6 導入と将来準備のための IPv6 導入の 2 つに分かれて展開し、さらに特定目的の IPv6 導入はやがて将来準備のための積極的な IPv6 導入に進展し、これが本格導入期に進んでいくと仮定しています。

シナリオの関係

前記の 2 通りのシナリオを含め、現状(C)から IPv6 本格導入期(F)に至る道筋を図に示すと下図のようになります。特定目的(N)および将来準備(N’)は概ね 1 年後、本格導入期(F)は概ね 2〜4 年後と想定しています。

シナリオの関係



分類	C: Current	N: Next	N': Next'	F: Future
年代	現在	1年後	1年後	2～4年後
ネットワーク内容	移行前	簡易IPv6移行	本格的IPv6移行	完全IPv6移行
IPv4/IPv6の通信	IPv4のみ	トンネル、トランスレート	Dual Stack	IPv6ネィティブ /Dual Stack

検討の軸

本ガイドラインで検討する内容は以下の通りです。

①ネットワーク

・通信端末の分類

LAN 内部とのみ通信する端末

LAN 内部とインターネットの双方と通信する端末

インターネットとのみ通信する端末(例:内線機能のない電話など)

・利用するリンクの種類

・IP アドレス (配布、設定、通信)

②アプリケーション

・情報系通信:Web ブラウジング、メール、ASP

・リアルタイム通信:プリンティング、VoIP、ストリーミング

・管理系アプリ：UPnP，アップデートツール

③セキュリティ

・ネットワークセキュリティ

・端末セキュリティ

3.独立 SOHO の移行

独立SOHOの概要

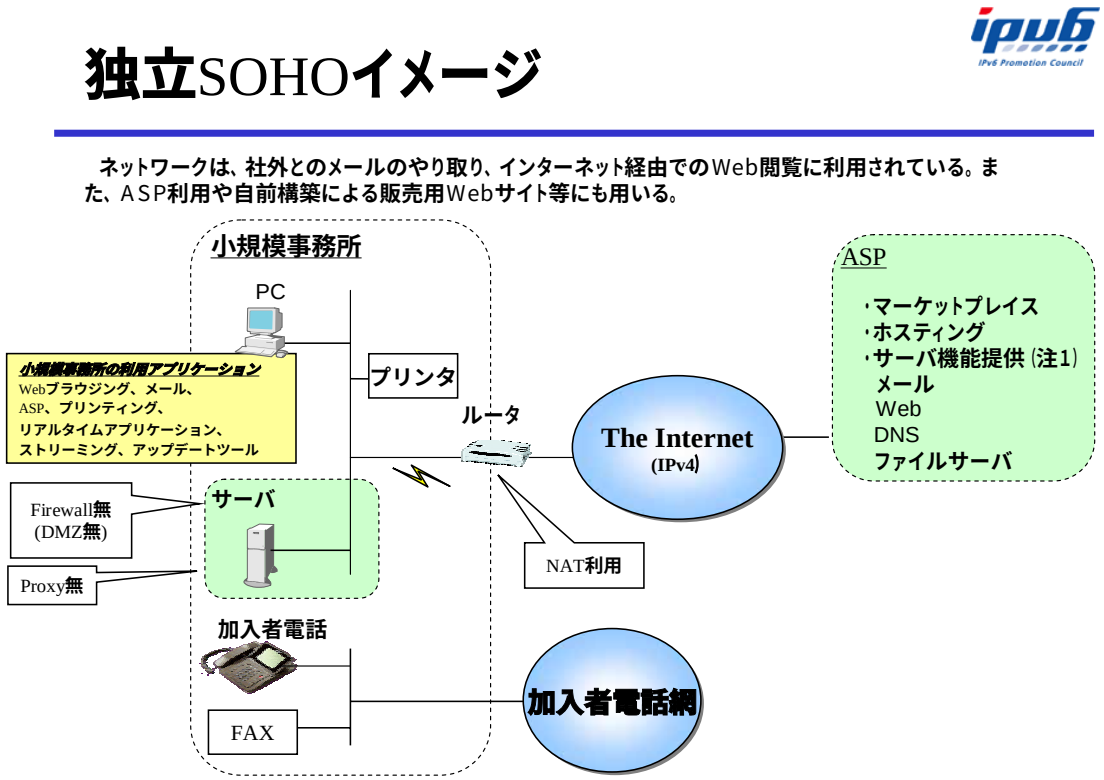
独立 SOHO としては、個人事務所などの小さな事務所を想定しています。税理士事務所、設計事務所などが典型的で、人数は 10 人程度の規模で、一般的には現地の IT スキルは高くありません。ただし、IT に詳しい人が 2、3 人いる場合があります。

場所は 1 箇所で、人は比較的いろいろな場所に移動します。コミュニケーションの対象は他社もしくは出張者、従業員の家庭などです。小規模のため、ネットにかけられるコストは小さく、複雑なサーバ類は現地にないのが一般的です。

独立 SOHO で利用する端末は、PC が中心で、ファイルサーバもあります。その他はプリンタ、電話、FAX などの事務機器です。

独立 SOHO イメージ

ネットワークは、社外とのメールのやり取り、インターネット経由での Web 閲覧に利用されています。また、ASP 利用や自前構築による販売用 Web サイト等にも用いられています。



ネットワークの移行

(1)ネットワーク

①利用する IP アドレス

分析

LAN 内部へグローバルアドレスを付与可能なため、グローバル環境との送受信が可能になります。LAN へ提供されるグローバルプレフィックス（動的/固定）と LAN 内へ配布されるプレフィックスは複数パターン（/64～/48）が考えられます。しかし、小規模企業のため、アドレス範囲は /48 以下になります。

この段階で利用されるアプリケーションには、一般的にソースアドレスセレクション機能は実装されていないため、複数プレフィックスを利用した通信は工夫が必要となります。

また、この規模の事業所では、複数セグメントにするとプリンタ接続やファイル共有などの通信管理が複雑になる可能性があるため、一般的には 1 セグメントのみの構成となります。

当面

上記のことから、利用するグローバルプレフィックスは/64 が一般的だろうと思われます。当面は 1 セグメント構成のため、それ以上のプレフィックスが必要になることはないからです。

課題

将来的に/64*n のグローバルプレフィックスを利用する場合の、アドレスの扱いについては検討が必要です。

②DNS 関連

分析

現状では、DHCPv6 の実装は Linux 等に限定され、Windows などの OS では実装されていません。ただし、IPv4 の DNS を用いて、IPv6 のホスト情報を参照することは可能となっています。また、一部ブロードバンドルータでは DNS のクエリ代行を実装済みです。

当面

したがって、現状では IPv4 の DNS を共用し、ルータによる DNS クエリの代行によって IPv6 上での名前解決を行うのが妥当と考えられます。

課題

この問題が将来的にどうなるか（DHCPv6 の利用方法など）については今後の課題となっています。

③リンク形態

分析

ISP との接続形態としては、現在トンネル接続、ネイティブ接続の 2 つがサービスされています。

当面

既存環境をそのまま利用するならトンネル接続を選択するのがよいですが、ルータに複雑な設定が必要となります。また、トンネルではネットワークアドレスの自動設定がサポートされていないケースが多くみられます。一方 SOHO で多く利用される ADSL のネイティブ接続サービスでは、アドレスの自動付与がサポートされています。設定を簡単にするならネイティブ接続をお勧めします。

(2)ネットワーク移行に必要な機器

独立 SOHO におけるネットワーク移行に必要な機器としては、以下が挙げられます。

端末

IPv6 対応の OS を利用した PC、サーバ

一般的な最新 OS（Windows XP、MacOS, Solaris, Linux など）はすでに IPv6 対応しています。

ルータ

IPv6 対応したブロードバンドルータ

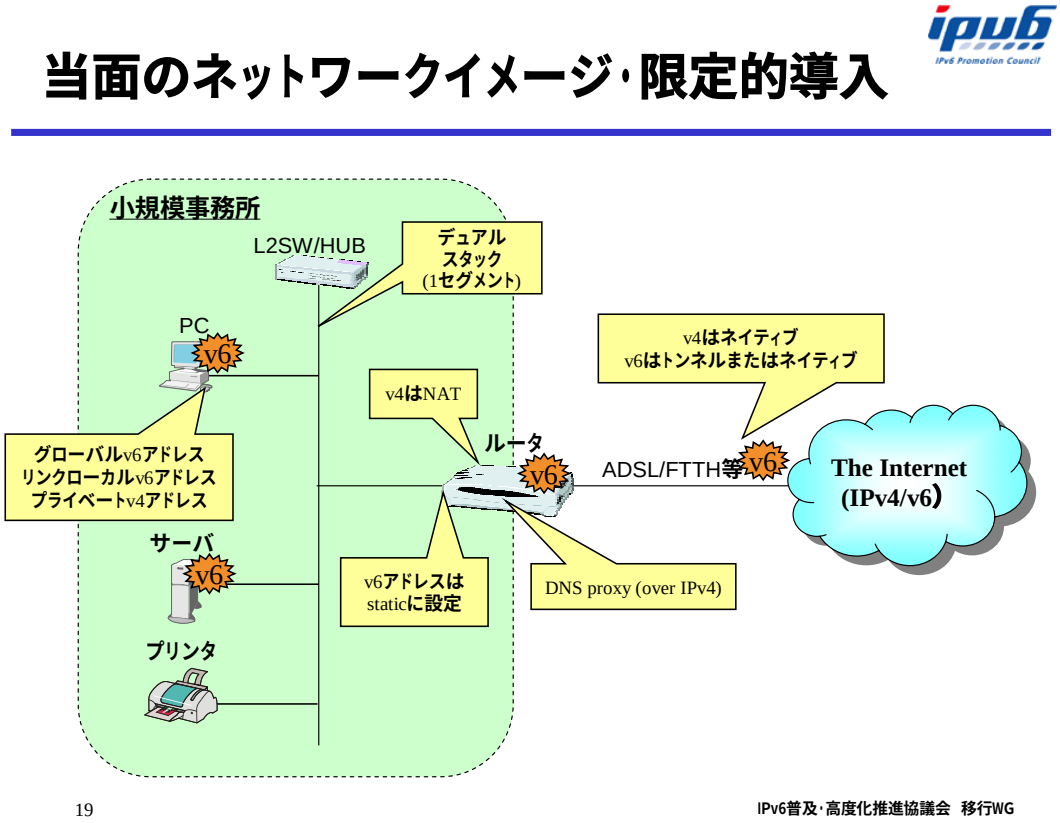
IPv6 での必要機能としては、Router Discovery への対応のほか、契約 ISP によっては、DHCP Prefix Delegation の仕組みを使っているため、この仕組みを実装する必要があります。さらに、トンネル接続を行う場合には、IPv6 over IPv4 トンネル機能が求められます。現状では IPv4 機能も必須です。

LANスイッチ/ハブ

レイヤ 3 スイッチ機能を使用しないなら、現在発売されている製品で特に問題はありません。ただし、レイヤ 2 スイッチ機能だけを使う場合でも、type 値をみて IPv4 以外を通さないものがあります。古いスイッチはチェックが必要です。

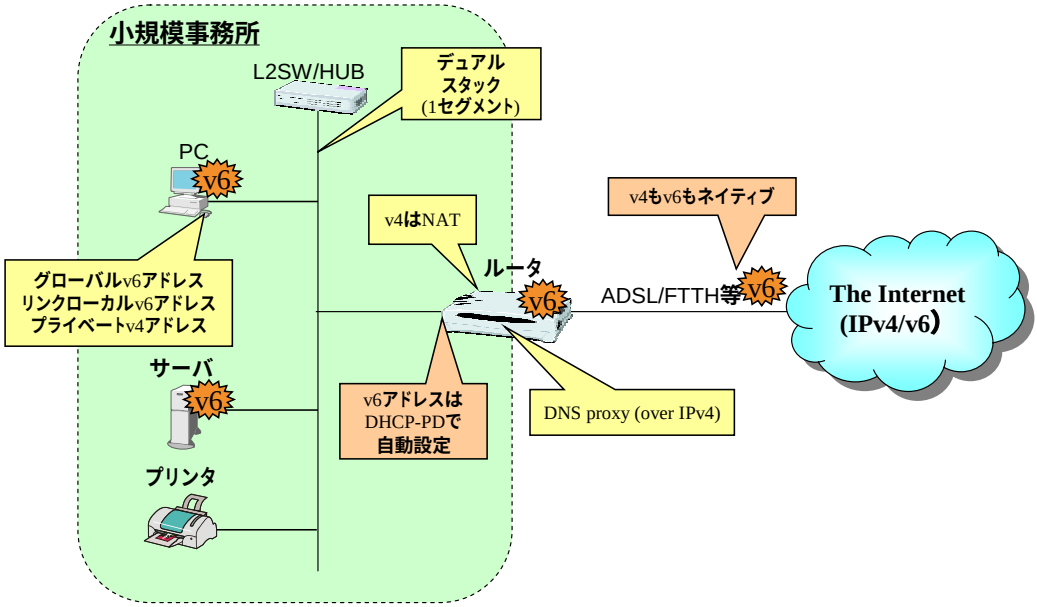
(3)当面のネットワークイメージ･限定的導入の場合

当面の特定目的導入（限定的導入）では、図のようなネットワーク形態になります。ISP との接続は、IPv4 とのデュアルスタック接続サービスを利用するか、IPv4 接続サービス上で IPv6 をトンネリングにより通す方法をとります。IPv6 のネットワークプレフィックスは、ルータに対してスタティックに設定されます。



(4)当面のネットワークイメージ･積極的導入の場合

積極的導入の場合、下図のように IPv4/IPv6 デュアル接続サービスを利用します。IPv6 のネットワークプレフィックスは、DHCP-PD により、ルータに対して自動設定されます。



(5)ネットワークの移行まとめ

独立 SOHO に割り当てられる IP アドレスは、当面は/64 のグローバルプレフィックス 1 つでよいと思われます。ネットワーク利用用途によっては、また ISP のサービスに広がりが出てきた場合には、複数のネットワークプレフィックス利用が有効になる可能性もあります。

ISP との接続は、ニーズに合わせてトンネルまたはネイティブ接続を選択します。

DNS については、当面は IPv4 トランスポートでの IPv6 アドレス解決を行います。これについては、ブロードバンドルータの IPv4 DNS プロキシ機能を使うと効率的です。

アプリケーションの移行

(1) アプリケーションの現状分析

独立 SOHO では、通常アプリケーション（メール、DNS、WWW 等）のためのサーバは、LAN 内に構築されているか、あるいは外部ネットワークからの提供を受けています。ASP やマーケット

プレイスを利用する場合もあります。プライベートアドレスと外部ネットワークとの通信を補助する仕組みとして、UPnP を利用するケースもあります（コミュニケーションツール等）。

PKI 連携や RAS(Remote Access Service)は利用数が少なく、証明書はブラウザのサーバ証明書のみの利用が一般的です。ただし今後、USB トークン等を利用したクライアント側証明書連携が増えると考えられます。独立 SOHO では、その他 LAN 内で閉じたアプリケーション（ファイル共有、プリンティングなど）が使われています。

(2) アプリケーションの移行

①Web ブラウジング

分析

セキュリティについて、Norton、Trend Micro などのウィルスチェックソフトが IPv6 対応していないという課題が存在します。また、通信相手である Web サーバに自分の IP アドレス情報を認識されてしまうというプライバシーの課題も指摘できます。

IPv4 との整合性は、デュアルスタック環境であれば確保されます。将来的に IPv6 のシングルスタックにしたときには、プロキシやトランスレータが必要となります。こうした機器の設置場所は ISP、サイト内の両方がありえます。

当面

ウィルス対策ソフトが IPv6 対応するまではデュアルスタック環境が必要となります。Web サーバ側についても、IPv6 のみによる提供が急速に進むとは考えにくいのが現状です。セキュリティの面から、通常のブラウジングは IPv4 で行うのが無難です。

②メール（メールクライアント～サーバ間）

分析

IPv6 対応のメールクライアントソフトはまだ少ないのが現状です。こうした状況もあり、Norton、Trend Micro などのウィルスチェックソフトは IPv6 対応していません。

メール利用において、クライアントサーバ･タイプは IPv4 と利用形態は変わりません。Web との違いとして、メールボックス(アクセス先)は自分が契約した場所にしかありません。一方、Web では多数の点に接続する利用形態になります。

デュアルスタック環境から IPv6 オンリーの環境に移行する際に気をつけなければならない点として、SPAM 増加の可能性や、特定の場所からのメール非到達の危険性が指摘できます。さらに、

IPv4 と IPv6 の対応リスト（3rd party relay のリストのような）が利用される可能性があります。クライアントサーバではなく、P2P メール利用の可能性も出てきます。

当面

セキュリティを考慮すると、メールクライアントが IPv6 対応していても、ウィルスチェックソフトが IPv6 未対応の場合、IPv6 を禁止する必要があります。メールについては Web ブラウジングと同様クライアントサーバ・モデルであり、IPv6 化するメリットが少ないため、当面は IPv4 のみで運用してもよいでしょう。現在見送ったとしても、他のアプリケーションの IPv6 移行状況を見て、IPv6 化対応すれば十分だと考えられます。

③ASP

分析

SOHO 向けの ASP サービスには E コマース、グループウェア、業種特化アプリなどさまざまなものがあり、大企業と比べると、ERP などのバックオフィス系よりも、情報サービスなどのフロントオフィス系へのニーズが高いという点が指摘できます。

プロトコル的観点からは「Web ベース ASP」と「独自プロトコル ASP」（Web 以外の通信（Notes など）に分類できます。

当面

Web ベース ASP に対しては、Web ブラウジングと同様の対応を行うのが妥当です。独自プロトコル ASP については、アプリケーションソフトの IPv6 対応が進んでくれば自然と移行可能になるでしょう。

④プリンティング

分析

IPv6 対応のネットワーク直結プリンタが販売され始めました。現在 IPv4 に対応していないプリンタは、今後デュアルか IPv6 のみに対応するようになることが考えられます(クライアントでは、Windows の IPP の IPv6 対応等)。

また、IPv6 対応した端末(サーバ)をプリンタにつなげば、IPv6 でのプリントが可能になります。

IPv6 over IEEE1394 等が主流になれば、接続プロトコルが IPv6 のみになる可能性もあります。IPv4 のみのクライアントに対しては、IEEE1394 でプリンタと接続する PC がプリンタサーバとなり、IPv4 クエリを処理する機能を持てばよいことになります。

さらに、プリンタのヘルスチェックや消耗品消費状況などをリモートメンテナンスするために、IPv6 が普及していく可能性があります。ただし、プリンタとサーバの自動通信によるセキュリティホールの課題があります。

現在でも FAX の電話線を用いたヘルスチェックサービスがあり、こうしたサービスの発展が考えられます。

当面

当面の移行指針としては、プリンタが IPv6 対応しなくとも、ローカルプリンティングは可能です。しかし、リモートプリンティングのニーズについては IPv6 対応によって便利になる可能性があります。そして、プリンタの IPv6 対応が進めば、プリンティングを IPv6 に移行する契機となる可能性があります。

現状では、一部のプリンタは IPv6 ストリームがあるとダウンするケースがあります。

⑤P2P アプリケーション（VoIP 除く）

分析

P2P 通信の IPv6 対応は、アプリケーションが対応していれば可能です。P2P 通信は NAT の影響を受けやすく、柔軟な通信が阻害される可能性があるため、IPv6 が有利です。たとえば IP 電話機については、IPv4 に対して IPv6 では SIP-NAT が不要になるため導入しやすいと言えます。特に、通信相手が特定グループに属する場合には IPv6 のほうが利便性が高いと考えられます。

ただし、直接通信に関しては、セキュリティの検討が必要です。たとえば、IP アドレス情報が漏れることによるセキュリティ低下の危険性への対応が求められます。また、登録端末からのみ着信許可する機能などが必要です（アドレス変更更新などの高機能が要求されます）。

ネットワーク側では、通話パケットを経由するトランスレータの信用確認が必要（ISP が設置）です。

ユーザが直接通信可能な Voice Chat などでも、サーバ（課金連携）を利用する利点が考えられます。利点とは、たとえば電話帳機能による既存網の通信先特定やプレゼンス管理のスケーラビリティの確保です。

当面

当面、P2P 通信の移行については、アプリケーションが IPv6 対応しており、相手先が IPv6 対応していれば積極的に利用してよいと考えられます。また、サーバレス型 P2P 通信の導入も検討できます。

⑥VoIP

分析

・NATによる制限

IPv4 の場合、NAT を用いることが一般的であるため、ゲートウェイが VoIP を終端する際は問題ないものの、ハード IP フォンのように、LAN 内部で電話を終端する際 E2E 通信ができないため、VoIP の着信に問題が起こることが考えられます。ゲートウェイに特殊な NAT 機能を加えれば、対処可能ですが、ゲートウェイのコスト的に難しい面もあります。そのため、SOHO の VoIP 利用においては E2E 通信を容易に実現できる IPv6 が有利となります。

・IPv6-IPv4 間の通話

IPv6-IPv4 間で通話をしようとすると、NAT が必要になります。そのため、現在の一般公衆網での利用には不具合が出ます。

・ピアツーピア電話

SIP については、IPv4 では SIP サーバがほぼ必須ですが、IPv6 では SIP サーバを使わないモデルもあります。不特定多数への接続性を確保するなら、電話帳機能(LDAP のような DB 機能)が必要ですが、特定相手との通話であれば VoIP ゲートウェイに機能があれば良い（SIP サーバはなくてもよい）と言えます。また、3 名以上での音声通話は SIP サーバモデルでは困難で、端末間の直接通信が適しています。ただし、IPv6 でも、利用端末のコスト低下（低機能化）を目的とした SIP サーバ利用の可能性はあります。

・直接通信に関してセキュリティの検討が必要

IPv6 では、IP アドレス情報が漏れることによるセキュリティ低下の危険性があります。したがって、登録端末のみ着信を許可する機能などが必要（アドレス変更更新などの高機能が要求される）となります。

当面

IPv6 に対応した VoIP ソリューション（特にハードフォン）の利用がある場合は、IPv6 の適用は薦められます。しかし、IPv4 との通信には問題があるため、内線は IPv6、外線は IPv4 のような使い分けがあるとよいと思われます。

⑦ビデオストリーミング

分析

SOHO におけるビデオストリーミング利用は、送信コンテンツが少ないこともあり、IPv4 ではあまり行われていないのが現状で、当面インバウンド利用が中心と考えられます。しかし、同時視聴

やマルチキャストの点で、ストリーミングは IPv6 化のメリットがある分野と考えられます。IPv6 への移行については、Windows Media Player は対応済みです。

当面

技術的には移行における問題はありません。魅力的な IPv6 放送局が利用可能であれば IPv6 対応も検討できます。

⑦アップデートツール

分析

管理センターからのアップデート手法としては、pull 型と push 型が存在します。IPv6 対応下では、セキュアに端末個別の制御が可能となり、push 型がやりやすくなります。

要素機能として、制御端末検索機能、マルチキャスト機能、nonPC 制御機能があります。独立 SOHO で使われるアップデートツールはクライアントサーバ・モデルです。

当面

一般的なアップデートサービス（Windows Update、ウイルスパターンファイル更新機能など）は当面 IPv4 のみでの提供が継続されていくと思われます。

(3) アプリケーション移行に必要なクライアント

IPv6 で利用可能なクライアントとしては、以下のものが代表的です。

・Web ブラウザ：Microsoft IE、Firefox、OPERA など
・メールソフト：Win Biff、Edmax、Thunderbird
・ビデオストリーミング：Windows Media Player 9、10
・IP 電話：ソフトフォンで対応しているものあり。岩崎通信機のハードフォン

IPv6 化すると有利になるアプリケーションとしては、リアルタイム(P2P)系アプリ、ストリーミングアプリがあります。IPv6 では、NAT が必要ないという点が大きなメリットです。

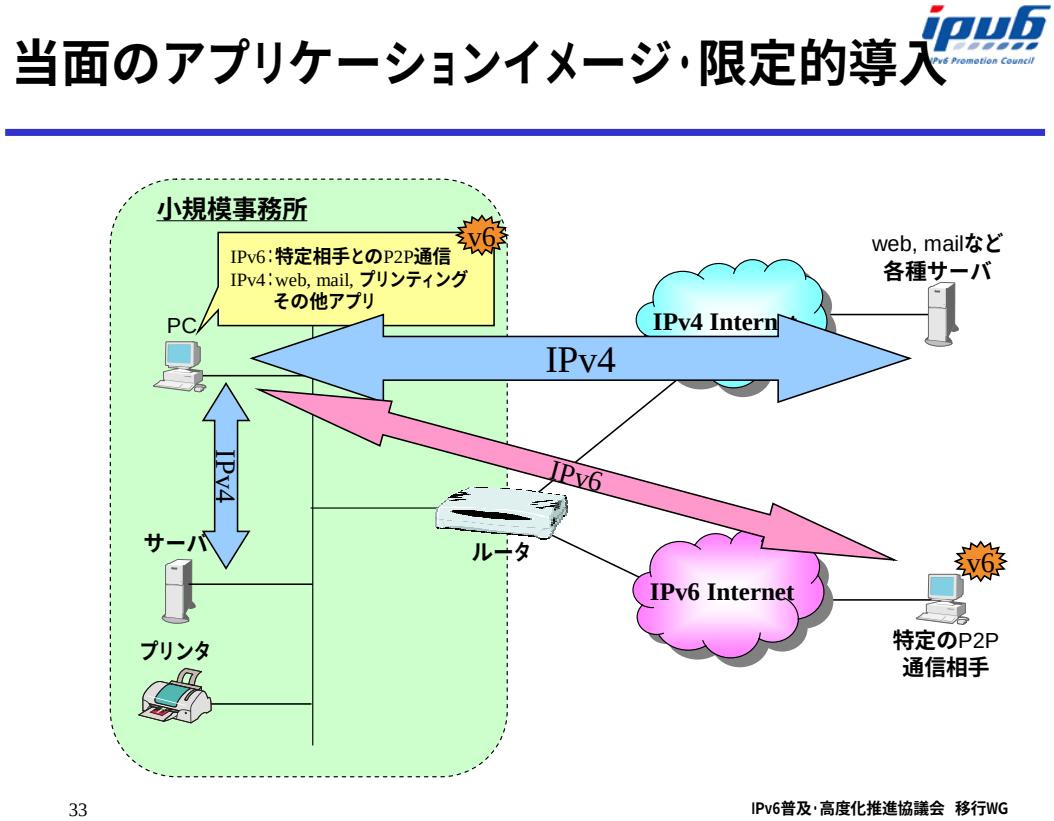
留意点としては、現状では Web や DNS の都合から、IPv4 のネットワークも必要となります。IPv6 化するアプリケーションは目的にあわせて選択するほうがよいと思われます。サーバまたは契約サービスの IPv6 対応も併せて確認する必要があります。

(4) アプリケーションまとめ

特定相手の P2P 通信は IPv6 化する価値があります。NAT が必要ないため、アドレス管理コストやポート管理コストが削減できますし、パフォーマンス（遅延・スループット）の点でも有利です。Web、電子メールなど、現状 IPv4 で使われているアプリケーションについては、あえて IPv6 化するメリットは少なく、むしろ現状ではセキュリティ的リスクが高いと言えます。

(5) 当面のアプリケーションイメージ：限定的導入の場合

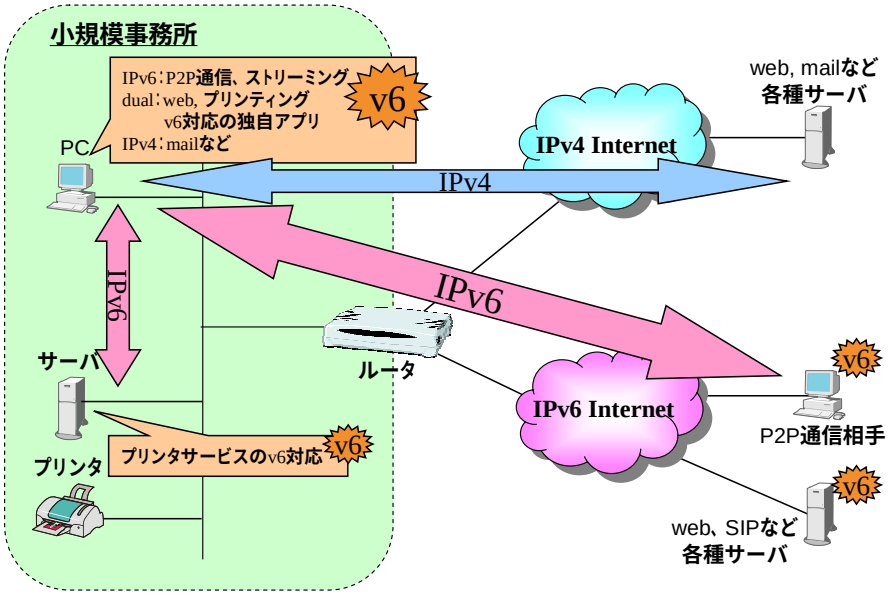
限定的導入では、Web、電子メール、印刷などについては IPv4 を使い、IPv6 は特定の相手との P2P 通信にのみ使われます。



(6) 当面のアプリケーションイメージ・積極的導入の場合

積極的導入では、P2P 通信やストリーミングを IPv6 に移行し、Web、印刷はデュアルプロトコルで利用、独自アプリケーションも IPv6 対応させます。電子メールなどは IPv4 のまま残します。

当面のアプリケーションイメージ･積極的導入



セキュリティ管理の移行

※セキュリティに関してはセキュリティ SWG 資料に詳細が記述されているので、そちらもご参照ください。

①ゲートウェイセキュリティ

分析

●暗号化

電話/FAX、社員のリモートアクセス、業務アウトソース、リモートメンテナンスでは、通信の暗号化が必要です。端末間で直接 IPsec 通信するほか、センサ等の機器を対象とした通信に関してはゲートウェイによる IPsec 通信を行います。この場合、暗号化通信をさまたげないように途中経由機器の標準化が必要となります。

●不正アクセス対策

IPv6 では、エンドツーエンド通信の実現に際し、UPnP のように勝手にポートを空ける仕組みは必要ありません。したがってこうしたポート空けのメカニズムが原因で引き起こされるセキュリティホールは考えなくてもいいことになります。しかし、事業所内の端末を公開 DNS に登録すると、アタック対象になりやすいという問題があります。

したがって、フィルタリングによる保護が必要となります。ステートフルパケットインスペクションを実施し、端末単位やポート単位でのトラフィック制御を行います。Windows XP では、IPv6 対応パーソナルファイアウォールが提供されていますので、これを利用することも考えられます。

●ウィルス対策

簡易 IDS を利用します。この場合、ファームウェアに攻撃パターンファイルを保持し、ファームウェアと攻撃パターンファイル双方の自動更新が可能なものが望まれます。IPv6 対応のウィルスチェック製品が提供開始されるまでは、IPv6 でのメール利用を禁止することをお勧めします。

●DoS 攻撃対策

IPv6 では、NAT による外部からの到達性喪失を改善できますが、各端末が DoS 攻撃を受ける可能性があります。対策としては、IDS の IPv6 対応が必要です。

●ファイアウォール

ファイアウォールについては、IPv4 の場合と同様、ステートフルパケットインスペクションを利用します。

●IPv4 との相違

ゲートウェイセキュリティに関しては、当面 IPv6 を導入したとしても、P2P 以外は IPv4 の場合とモデルは同じです。

当面

当面は、ステートフルパケットインスペクションの利用など、IPv4 と同様なモデルを踏襲します。P2P 通信を行う際は、アドレスが特定できる相手に限定してポートを空けるなどの通信がよいと考えられます。

課題

課題は、P2P 通信が関わった際のセキュリティポリシー設定の困難さにあります。通信先アドレスの設定など、専門知識のある人がいなくても正しく運用できる手段が提供できることが望まれます。

②端末セキュリティ

分析

P2P 通信を安全に行うためには、端末による IPsec 通信終端ができることが望まれます。ただし、公開 DNS 登録などにより、端末のホストアドレスが公開されるとセキュリティの低下につながる恐れがあります。

端末セキュリティ関連で、IPv6 対応がまだ十分に進んでいない要素としては、ホスト用のパケットフィルタ（パーソナルファイアウォールなど）、IDS、ウィルスチェッカなどがあります。また、ウィルス対策については、センターからのパターン Push による機能更新などでの IPv6 対応も望まれます。Windows 標準での PKI 機能については、ESP（暗号化など）の IPv6 対応も求められます。

一方、現状のままで IPv6 ネットワーク上でも利用できる機能としては、アプリケーションレベルでのチェック（ファイルの感染チェックなど）、ID/パスワードの利用、ブラウザでのサーバ証明書保持、専用クライアントでの PKI や IPsec の利用などがあります。

当面

IPv4 と同様なモデルは利用可能です。ID/パスワードのみ、Web サーバ証明書の利用については問題ありません。P2P 通信を行うためには、当面ゲートウェイで対応するのが一般的と考えられますが、一部製品で端末レベルでのセキュリティ確保が可能な製品もあります。

課題

課題としては、ウィルスチェッカやパーソナルファイアウォール製品の IPv6 対応が望まれます。また、端末レベルでのセキュリティ確保という考え方の一般化も望まれます。そのためには、こうしたツールの設定が簡単になる必要があります。

③セキュリティまとめ

独立 SOHO における当面の IPv6 移行では、セキュリティ対策として以下の点が指摘できます。

暗号化対応については、まず、一部のルータに搭載された IPsec トンネルモード機能、および専用クライアントを使った暗号化を利用します。SSL レベルでの暗号化は IPv6 でも有効です。

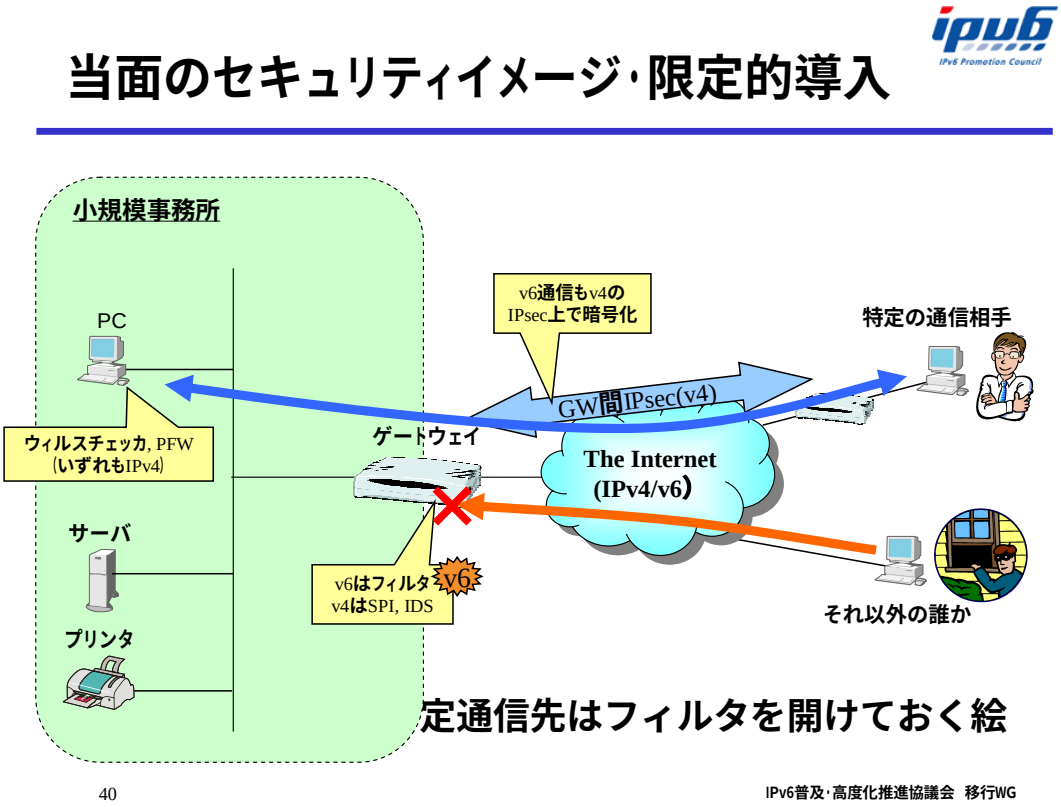
不正アクセス/DoS 対策に関しては、通常のクライアントサーバ型通信にはステートフルパケットインスペクションを利用し、P2P 通信にはフィルタによるセキュリティを適用します。フィルタによるセキュリティは、通信相手（アドレス）が固定の場合には有効です。ネットワーク内の端末アドレスは、できるだけ公開 DNS には登録しないほうがよいと言えます。

端末のセキュリティに関しては、アプリケーションレベルのツール（ファイルのウィルスチェックなど）は IPv6 でも有効であり、継続して使用します。パーソナルセキュリティツールは、現状では

IPv6 では動作しない製品（メールウイルスチェックツールなど）もあるので、特に必要がないアプリケーションは IPv6 対応しないほうがよいと言えます。端末のみではなく、ゲートウェイと連携したセキュリティ設定を行うほうが簡単にできることから、端末フィルタとゲートウェイフィルタの併用をお勧めします。

④当面のセキュリティイメージ・限定的導入の場合

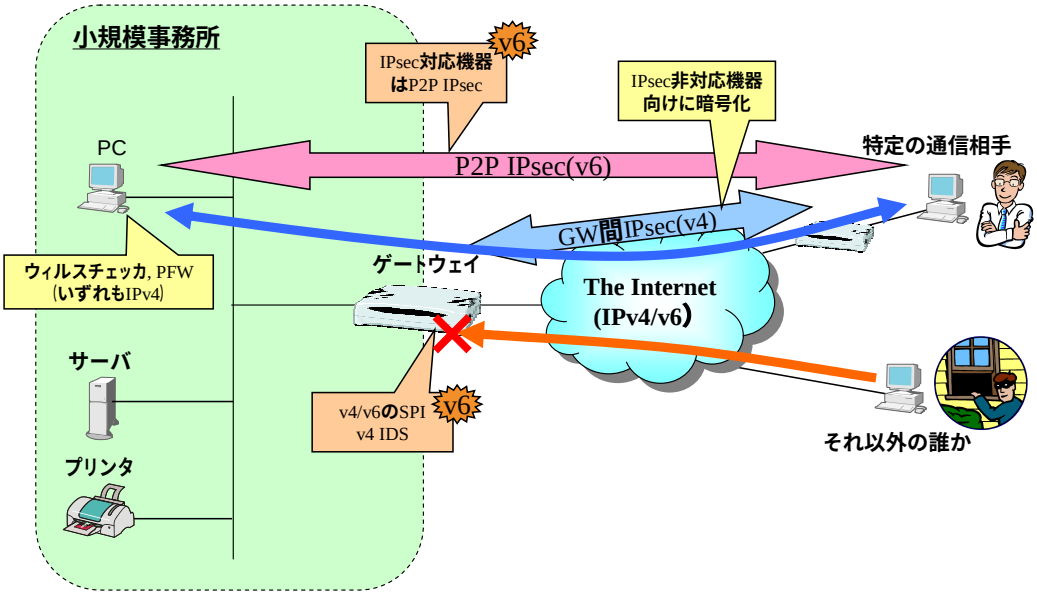
限定的導入では、特定の通信相手との暗号化通信については、ルータなどの IPsec 機能によるゲートウェイ間 IPsec を用います。IPv6 通信に関しても、暗号化を行いたい場合、IPv4 上での暗号化を行います。それ以外の相手と IPv6 通信したい場合は、ルータにこの通信のための穴を開けます。IPv6 に関する境界セキュリティは、フィルタリングによって対応します。



(5) 当面のセキュリティイメージ・積極的導入の場合

積極的導入では、特定の通信相手との通信はゲートウェイ間 IPsec で保護できるほか、IPsec 対応の IPv6 機器については、ピアツーピアでの暗号化を行います。それ以外の相手との IPv6 通信には、IPv6 対応のステートフルパケットインスペクションファイアウォールを適用します。

当面のセキュリティイメージ･積極的導入



独立SOHO 移行のまとめ

独立系 SOHO の IPv6 移行について、ネットワークの移行、アプリケーションの移行、セキュリティの移行は、それぞれ以下のようにまとめることができます。

ネットワークの移行の整理

項目	C: Current	N: Next	N': Next'	F: Future	課題
利用するリンク	PPP等	ルータ or 端末 からトンネル	Dual Stack	Native	
LANアドレス	プライベート アドレス	Dual Stack 単一の/64	Dual Stack 単一の/64	IPv6 Only 複数の/64	複数プレフィックス時の管理
ISPからユーザへのIPアドレス配布	PPP等	Static	自動割当 (DHCP PD利用)	自動割当 (DHCP PD利用)	
LANの通信端末へのIPアドレス配布	DHCP	RS/RA	RS/RA	RS/RA or DHCP(?)	
LANの通信端末へのDNSの設定	DHCP	IPv4を利用 (DNSクエリ代行)。		IPv6対応のDHCP or RA Extensionなど	標準化

ネットワークの移行の整理

項目	C: Current	N: Next	N': Next'	F: Future	課題
利用するリンク	PPP等	ルータ or 端末 からトンネル	Dual Stack	Native	
LANアドレス	プライベート アドレス	Dual Stack 単一の/64	Dual Stack 単一の/64	IPv6 Only 複数の/64	複数プレフィックス時の管理
ISPからユーザへのIPアドレス配布	PPP等	Static	自動割当 (DHCP PD利用)	自動割当 (DHCP PD利用)	
LANの通信端末へのIPアドレス配布	DHCP	RS/RA	RS/RA	RS/RA or DHCP(?)	
LANの通信端末へのDNSの設定	DHCP	IPv4を利用 (DNSクエリ代行)。		IPv6対応のDHCP or RA Extensionなど	標準化

43 IPv6普及・高度化推進協議会 移行WG

アプリケーションの移行の整理

項目	C: Current	N: Next	N': Next'	F:Future	課題
Webブラウジング (ASPのWebベース含む)	IPv4アクセス	IPv4アクセス 特別なサーバはIPv6化	Dual Stack アクセス	IPv6アクセス + Translator	セキュリティチェックツール
メール	IPv4アクセス	IPv4アクセス	IPv4アクセス (クラサバ)、IPv6アクセス(P2P)	IPv6アクセス (クラサバ、P2P)	セキュリティチェックツール(特にウィルス)
独自アプリ	IPv4アクセス	IPv4アクセス(※)	Dual Stackアクセス？(※)	IPv6アクセス？(※)	※：メーカ依存
プリンティング (ファイル共有等も含む)	IPv4アクセス	IPv4アクセス	Dual Stackアクセス(プリンタサーバのIPv6化)	IPv6アクセス	プリンタのIPv6対応
P2P(公衆)	IPv4アクセス (SIPサーバ経由+NAT)	IPv4アクセス (SIPサーバ経由+NAT)	IPv6アクセス (SIPサーバ経由とP2P)	IPv6アクセス (SIPサーバ経由とP2P)	P2Pで利用する枠組み
P2P(特定)		IPv6	IPv6	IPv6	
ストリーミング	IPv4アクセス	IPv4アクセス	IPv6アクセス (マルチキャスト含む)	IPv6アクセス (マルチキャスト含む)	
アップデートツール	IPv4アクセス (PULL型)	IPv4アクセス (PULL型)	IPv4アクセス (PULL型)	IPv6アクセス (PULL+PUSH型)	セキュリティチェックツール、制御端末検索

セキュリティの移行の整理

項目	C: Current	N: Next	N': Next'	F: Future	課題
暗号化	GatewayでIPsec	GatewayでIPsec	GatewayでIPsec or P2P IPsec 端末によって使分け	GatewayでIPsec or P2P IPsec 端末によって使分け	方式の標準化
ウィルス対策	IPv4 IDS	IPv4 IDS (IPv6メール禁止)	IPv4 IDS (IPv6メール禁止)	IPv6 IDS	ウィルスチェッカのIPv6対応遅れ
Dos攻撃防御	IPv4 SPI	IPv4 SPI	Dual Stack SPI	IPv6 IDS	名前解決とリソース遮断回避機能連携
GW Firewall	IPv4 SPI	IPv4 SPI + IPv6 Filter	Dual Stack SPI	IPv6双方向SPI	実装+Incoming制御
端末不正アクセス防御	IPv4 Personal-FW (PFW)	IPv4 PFW ※IPv6はGWで	IPv4 PFW ※IPv6はGWで	Dual Stack PFW	実装
端末のアクセス	ID/PW	ID/PW	ID/PW PKI(?)	ID/PW PKI(?)	設定の複雑化

4. ぶらさがり SOHO の移行

ぶらさがりSOHO の概要

(1) ぶらさがり SOHO の想定

ぶらさがり SOHO とは、企業の営業所、出張所などを指します。保険代理店や旅行代理店なども含みますが、基本的には直営店が対象となります。人数は 10 人程度で、システム管理者は現地ではなく、センターに常駐しています。現地の IT スキルは高くありません。

こうした拠点は全国各地に点在しており、人員はローカルエリアでの活動が中心です。しかし、これらの拠点は、本部とシステム的、対話的なコミュニケーションが必要です。拠点の数が多く、1 箇所あたりのコストはかけられません。複雑なサーバ類は現地にないのが一般的です。

(2)ぶら下がり SOHO の現状分析

利用端末は PC が中心で、他にはプリンタ、ファイルサーバなどの事務機器や、ホスト端末などの業務専用端末、そして電話、FAX などがあります。利用アプリケーションとしてはメール、イントラ内やインターネットの Web ブラウジング、プリントやファイル共有によるローカル通信などがあります。ホスト（センター）連携では、トランザクション、ファイル交換などを行っています。プロトコルとしては、SNA などが利用されてきましたが、Web ベースに移行されていく傾向にあります。電話、FAX については、徐々に IP 電話化されてきています。

ネットワークは、センター中心のスター型 VPN を構成しています。これには、IP-VPN、広域イーサネット、インターネットVPN（ゲートウェイ IPsec ベース）が使われています。より小規模な拠点は ISDN や DA128 による接続が行われていますが、今後は ADSL が主流になっていくと思われます。これらはバックアップとして使われている場合や、音声・情報系と業務系で分ける場合があります。

アドレス構成としては、WAN 側アドレスを1個持ち、LAN 側は/24 のプライベートアドレスを構成しているのが一般的です。各拠点で NAT を利用しているか、VPN 内は固定アドレスを利用しています。プライベートアドレスは、全拠点が同じアドレスを使っている場合があります。また、インターネット向きとイントラネット向き、あるいはアプリケーション別にポリシールーティングが必要なケースもあります。

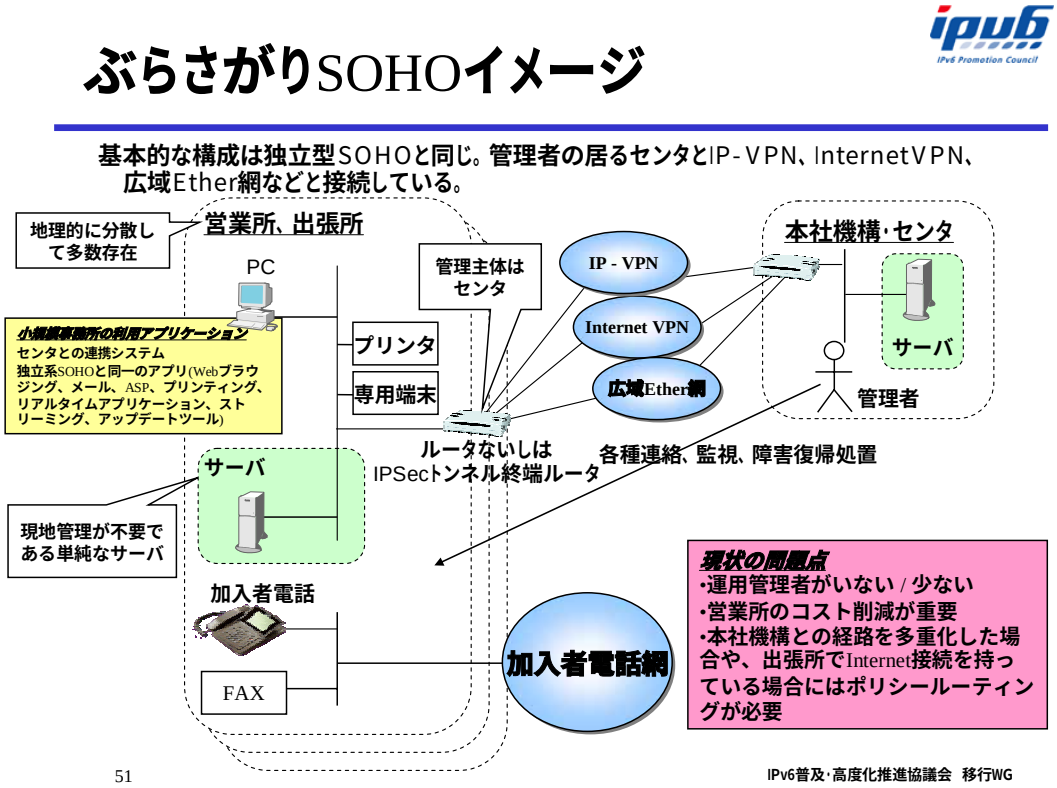
利用プロトコルは、ローカル通信では IPv4、NetBEUI、IPP、ファイル共有プロトコルなど、リモート通信では IPv4、SNA、http/SSL、POP3/SMTP、3217、H.323/SIP、RTP、DLSW などです。

セキュリティについては、本社で集中管理しています。各営業所では対応できないか、できてもほんの一部の対応に留まります。回線接続についてはゲートウェイで管理しています。インターネ

ットからの内部向通信は基本的にはありません。端末にはウイルスチェックツールをインストール済みです。場合によっては、インターネット通信は VPN を通り、本社ファイアウォール経由で行っています。

(3) ぶらさがり SOHO イメージ

ぶらさがり SOHO のネットワーク構成は、概ね独立系 SOHO と同様ですが、本社機構･センタと IP-VPN、インターネット VPN、広域イーサネット等で接続しています。



ぶらさがり SOHO 移行の分析

ぶらさがり SOHO の移行については、ほとんどは独立 SOHO と同じですが、相違項目として、VPN の IPv6 対応が必要になりますし、逆に IPv6 での VPN 構築が望まれます。また、QoS などポリシー通信のニーズが考えられます。マルチホーム等、外部向け経路が複数ある場合のルーティングについては Tips を参照してください。

アプリケーションについては、レガシーアプリを利用するところが、独立 SOHO とは異なります。アプリケーション利用については、大企業ガイドラインを参照してください。

セキュリティについては本社のゲートウェイで管理します。大企業ガイドラインを参照してください。ただし、大企業ガイドラインに含まれない要素として、営業所側のルータを遠隔管理する必要があります。

VPNの移行

分析

VPN に関しては、まずインターネット上の SSL サーバ利用は IPv6 でも影響を受けず、従来通り実行できます。IPv4 ではルータベースで IPsec のアグレッシブモードによるトンネルを利用するのが一般的です。

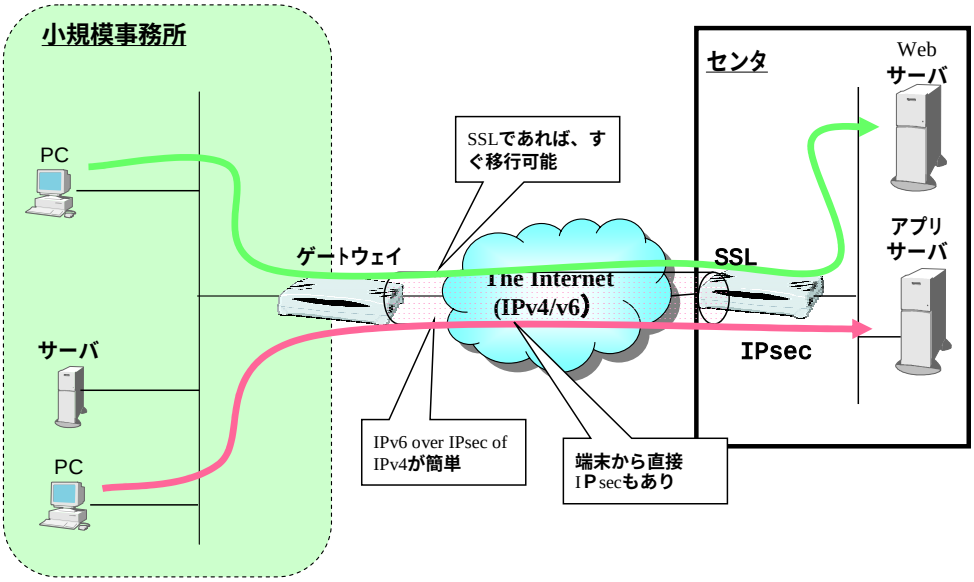
IPv6 の VPN 実現方式としては、IPv6 over IPv4 over IPsec、DTCP、IPv6 over IPsec IPv4、IPsec IPv6 + ネイティブサービスといった選択肢があります。

IPv6 over IPv4 over IPsec はフラグメント化の影響が大きいという問題があります。DTCP は暗号化機能がなく、フラグメント化につながります。IPv6 over IPsec IPv4 は比較的安価にできるソリューションです。IPsec IPv6 + ネイティブサービスは、性能面、拡張性から見ると優れています。

当面

では、当面の VPN 対策はどうしたらよいでしょうか。SSL ベースなら、スタックを IPv6 に変えるだけで、他に何もすることなく従来通り利用できます。IP レイヤでの VPN を軽く行うなら、IPv6 over IPsec IPv4 が適しています。拡張性を重視するなら、ネイティブ（デュアルスタックを含む）接続を利用します。

VPNの構成イメージ



5. 将来的な利用モデル

将来的な利用イメージ

将来は、IPv6 によって様々なものがネットワークにつながることになります。

アドレスが豊富で、自動設定が充実しているということから、PC、プリンタ、IP 電話、PDA だけでなく、コピー機、FAX、ホワイトボード、プロジェクタといった事務機器、さらには PC 周辺機器、防犯カメラ、タイムカードなどがネットワークインタフェースを持つことによって、使いやすくなっていきます。

IPv6 の普及によって、外部ノードとの連携が多くなるということも言えます。これは、P2P 通信やセキュリティのインフラが整備されていくことによって、外部連携しやすい環境が整うためであり、結果として機能のアウトソーシングが進むと考えられます。

連携の例としては、注文・予約システムの構築(Web ベースは現在もある)、問い合わせ・サポート受付、電話や TV 電話があります、また、IPv6 化で社外とのコラボレーションが広く見られるようになっていきます。こうした進展に伴って、IPv6 オンリーのノードが出てくることが予想されます。

外出時に SOHO へアクセスして動的な名前解決をし、P2P による情報交換をするなど、モバイル性も高まり、情報のリアルタイム性が高くなっていきます。

移行への課題

本格的な普及に向けた技術課題としては、ネーミング、セキュリティ、QoS、信頼性確保（マルチホーミング）、トランスレータ（誰が用意するか）などが考えられます。

6. 要望・課題の整理

ネットワーク

(1) ネットワーク

・SOHOネットワーク内のセグメント数について

ユーザ組織に対して、どの大きさの IPv6 アドレスを提供するかについては、ISP の裁量にまかされています。現在の ISP からの IPv6 アドレス配布の種類には、/64 プレフィックス（1 セグメント分）配布タイプと、/48 プレフィックス（複数セグメント分）配布タイプがあります。

/64 の 1 セグメントによる運用は、アドレスの自動割当機能などにより構築やユーザの利用が楽だというメリットがあります（当然、/48 のプレフィックス割当でも 1 セグメントによる運用は可）。

一方、/48（/64 複数セグメント）による運用は、セグメントごとのポリシー分けが柔軟に行える利点があります。一方、ポリシー管理や運用など管理の複雑さが増し、管理者不在の SOHO では管理が難しくなる可能性があります。

・Prefix Delegation について

管理者のいない SOHO における設定を簡素化するためには、ISP からのネットワークプレフィックスの自動設定機能（Prefix Delegation と呼ばれます）が必要となります。現在考案されている Prefix Delegation 手法には、以下のようなものがあります。

●MSR(Multi-link Subnet Router)モデル

これは CPE（Customer Premise Equipment：ADSL モデムなど）－PE（Provider Edge Device）間リンクと CPE の LAN 側リンクを同一リンクとして扱うというものです。単一の/64 プレフィックスが LAN 側端末に割り当てられます。これは、形態としてはありうるが、実際のサービスは当面登場しないことが考えられます。ISP へ向けて ICMP ルータ要請（Router Solicitation）パケットの大量送信が考えられるためです。

●レイヤ3ルータ型のモデル

CPE となるレイヤ3ルータが ISP からのネットワークプレフィックス割当をいったん終端し、この割当プレフィックスの中から再度 LAN 側へ配布するスタイルです。このモデルは、/48 あるいは /64 のプレフィックスを割当対象とすることができます。このスタイルに基づく技術としては DHCPv6-PD がメジャーで、RFC としての承認は完了しています。

・DNS Discovery について

IPv4 では、DHCP により、最低限必要なネットワーク情報（IP アドレス、デフォルトルータ、DNS サーバアドレス）をすべて自動的に取得することができ、実際にこれが一般的に利用されています。

では、IPv6 でのネットワーク情報自動設定はどうなるでしょうか。IPv6 では、ネットワークプレフィックスやデフォルトルータアドレスを、ルータからの RA（Router Advertisement）により取得する仕組みが用意されています。しかし、現在のところ、DNS サーバアドレスについては RA では配布されません。このため、現在、IETF で DNS サーバアドレスの配布方法について議論中です。

候補としては、well-known な固定アドレスを利用する方法、RA の拡張、DHCPv6 の拡張（Stateless DHCPv6）などが挙げられています。

(2) アプリケーションの留意事項

IPv6 シングルスタックの端末/環境が広まっていった場合、IPv4 オンリーの Web にアクセスするために、トランスレータあるいはリバースプロキシが必要となります。これらは ISP で設置することもあるでしょうが、ホームゲートウェイ等における実装を利用する可能性もあります。

メールソフトにおける IPv6 移行については、現在の時点で、既存のセキュリティチェックソフトはまだ IPv6 対応していないものがほとんどだという状況があります。

ASP での IPv6 対応に関して、独自プロトコル ASP はアプリケーションの改造が必要になる可能性があります。

P2P アプリケーションの通信を v4 端末から v6 端末に行う場合、v4-v6 NAT 装置が必要です。しかしアドレス領域サイズの違いから、v6 端末を固定的にマッピングするのは困難です。そのため、v4 端末側は NAT 装置と何らかのネゴシエーションをし、マッピング情報を取得する必要があります。これは、UPnP や DNS 連携などによる実装が考えられます。

(3) セキュリティの留意事項

セキュリティに関しては、通信形態の多様化にしたがって、ポリシー設定が困難になっていくことが指摘できます。通信先アドレスの設定などについて、専門知識のある人がいなくても正しく運用できる手段が求められていくことなります。

ウィルスチェッカ、パーソナルファイアウォール製品といった、必要不可欠なインフラ製品が IPv6 対応する必要もあります。端末レベルでのセキュリティがどれだけ一般化するかは、設定がどれだけ簡単になるかにも関係します。

その他の留意点

MTU Discovery

IPv4 では、パケット配送の途中経路でも Fragment が可能で、ICMPv6 Type2 のような ICMP の利用はありません。ISP などにおいて、ICMP パケットをフィルタリングするケースもあります。

一方、IPv6 ではパケット配送における経路途中では Fragment が実施されません。経路途中のあるルータでパケットサイズが Too Big となった場合、そのルータが ICMPv6 の Type2「Packet Too Big Message」を送信元に返します。そして送信元はそのメッセージを受け取り、再度適切なサイズにパケットを収めて送信することになっています。このため、IPv6 インターネット上では ICMPv6 メッセージ（少なくとも Type2）がエンドノードまで配送されないと、通信性がそこなわれる場合があるので注意が必要です。ISP を含めて、ICMPv6 Type2 メッセージはフィルタリングしない運用を徹底する必要があります。

ホスト名登録

ネットワークに直結できる Non-PC 機器（カメラ、プリンタなど）が今後増加すると、手軽にネットワークに接続して使いたいというニーズも増大します。また管理者不在の SOHO では、PC についても、IPv6 のアドレス（128bit）を毎回手動登録したくないものです。このため、端末の名前とアドレスをマッチングさせる機能が求められてきます。

標準的なホスト名の自動登録手法については、現在はまだ検討段階といえます。利用可能な技術としては、Dynamic DNS、UPnP（Universal Plug and Play）、SIP があります。また、逆引きには ICMPv6 の Node Information Query という手もあります。これは、Node Information Query（ICMPv6 の Type139）を宛先に送信すると Node Information（ホスト名など）を含んだ Reply（ICMPv6 の Type140）が返答されるというものです。現在のところ対応プラットフォームは、UNIX 系の FreeBSD、Linux などです。

アプリケーションの対応

現在 IPv6 対応待ちのアプリケーションとしては、まず DNS リゾルバがあります。現在、

Windows の DNS リゾルバは、情報の中身については IPv6 対応ですが、通信自体が IPv6 化されていないという状況です。

セキュリティツールに関しては、アプリケーションゲートウェイ型ウィルスチェックソフト（Web 、メールなど）がまだ IPv6 に未対応です。ただし、OS のファイル I/O チェック型のソフトは、IPv4 か IPv6 かに依存しないため問題ありません。また、Windows Update などのアップデートツール、Windows Messenger などのメッセンジャーアプリケーションなども IPv6 対応が望まれます。

(4) QoS

ブロードバンド化によりリアルタイムアプリケーションが増加しつつありますが、さらに IPv6 が普及することにより P2P 通信性が向上し、将来は QoS の必要性が増加することが予想できます。

PE-CPE 間の QoS の課題としては、上り方向 QoS 制御は技術的にある程度可能です。しかしコスト的な問題などから、現実にはあまり実施されていません。下り方向については、基本的に末端側からの QoS が困難です。ただし、ブロードバンドルータのパケットシェーピング機能でもある程度の QoS は実現可能です。これについては、ISP 側、機器ベンダーへのサービス、機能要求につながっていくと考えられます。

移行WG SOHOセグメント 検討メンバ

（敬称略）

SWG チェア

猪俣（富士通）
阪内（NEC）
月岡（日立）

メンバ

荒野（インテックネットコア）
中井（NTT コミュニケーションズ）
中原（NEC）
金海（NEC）
大平（リコー）
伊藤（キヤノン）
山本（清水建設）
吉岡（トヨタ）
尾崎（富士通）

お問い合わせ先

本ガイドラインに関するお問い合わせは、以下のアドレスまでメールでご連絡下さい。
IPv6 普及・高度化推進協議会移行WG／e-mail: wg-dp-comment@v6pc.jp