IPv6 移行ガイドライン

(SOHO セグメント)

2004 年 5 月

IPv6 普及･高度化推進協議会

移行 WG SOHO SWG

目　次

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。

■検討メンバ

SWG チェア

猪俣（富士通）

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）
金山（インテックネットコア）
川島（NEC アクセステクニカ）
尾崎（富士通）
加藤（富士通）
黒瀬（富士通）

（敬称略、あいうえお順）

■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を下さい。

IPv6 普及・高度化推進協議会 移行 WG／e-mail: wg-dp-comment@v6pc.jp

1. SOHO セグメントの特徴

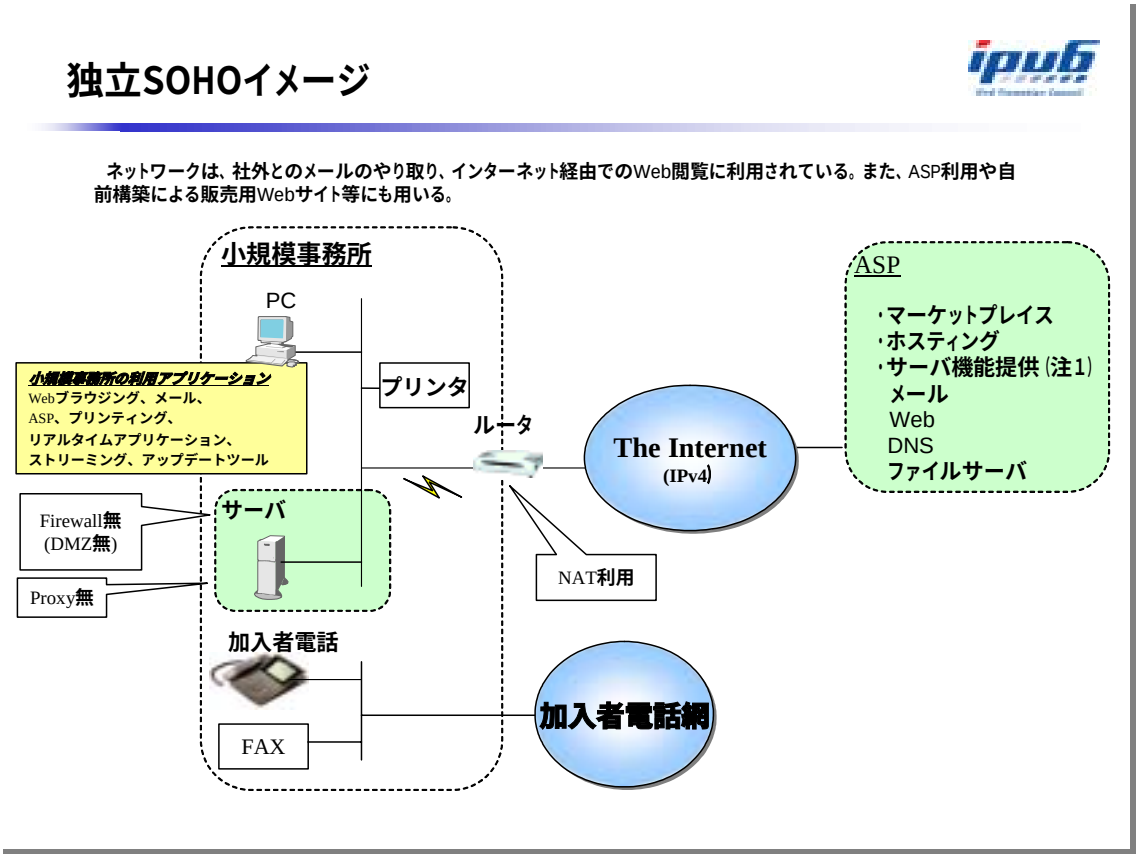
■SOHO の分類

SOHO と呼ばれる事業所には、以下のようなものがあります。

1. 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。
2. 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。
3. 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。
4. 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。

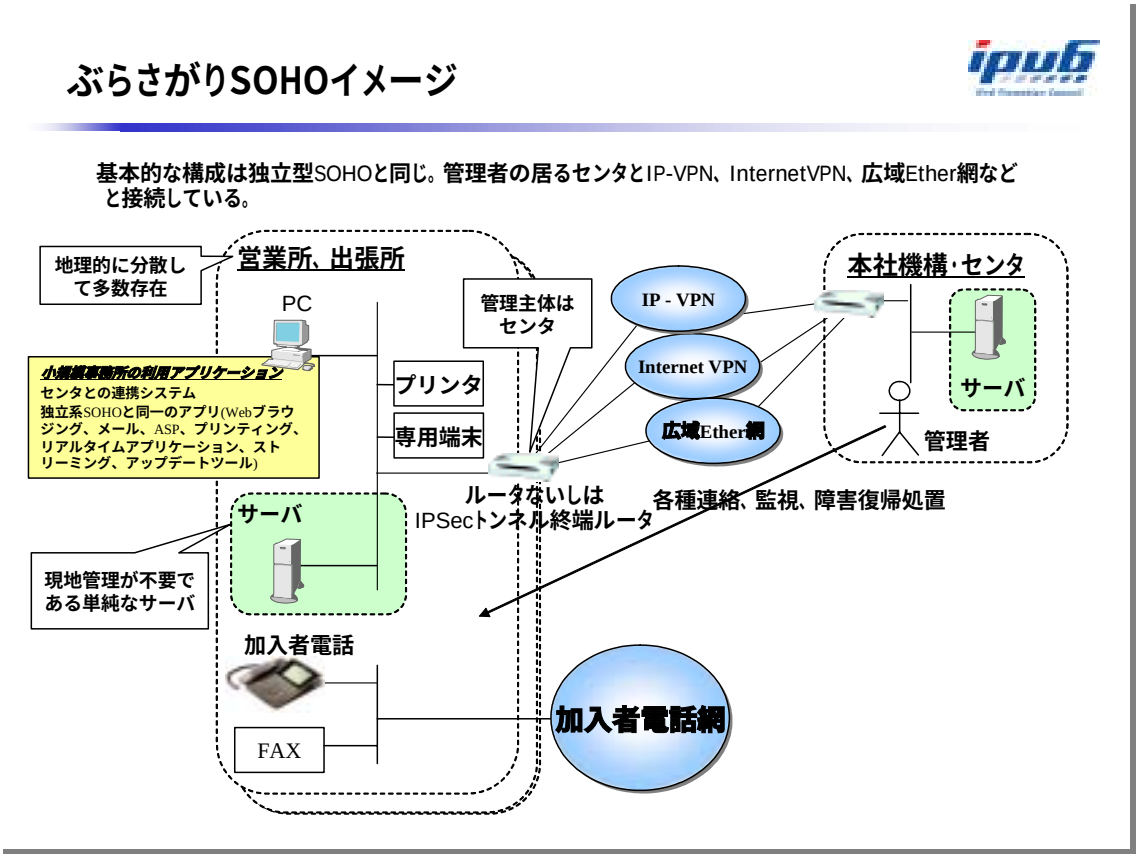
この移行ガイドラインでは、小規模事業所（以下では「独立 SOHO」と呼びます）と小規模営業所（以下では「ぶらさがり SOHO」と呼びます）を対象とします。

■独立 SOHO イメージ



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。

■ぶらさがり SOHO イメージ



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。

2. 移行へのシナリオ

■移行へのシナリオ

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)、Pv6 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。

(1)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

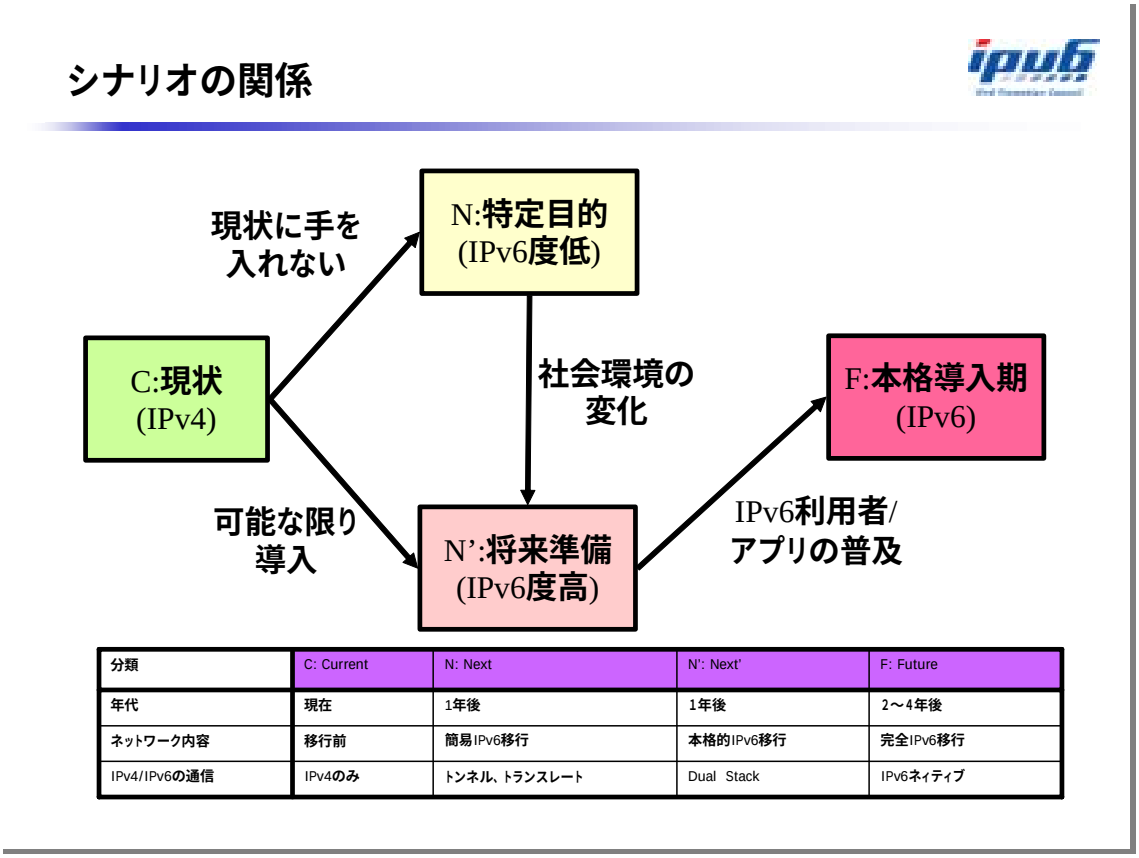
これは、業務上の目的があり、IPv6 を利用したシステムを導入する場合です。IP 電話、インスタントメッセージなど、利用アプリケーションが IPv6 化されたり、商取引のセキュリティ強化、メンテナンスなどの理由から、取引先が IPv6 化されることがきっかけとなります。これは、現状の IPv4 ネットワークに基本的には手を入れないもので、保守的な IPv6 導入シナリオということができます。

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。

(2)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

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上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。

■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 Internet の双方と通信する端末

・Internet とのみ通信する端末 (例:内線機能の無い電話など)

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

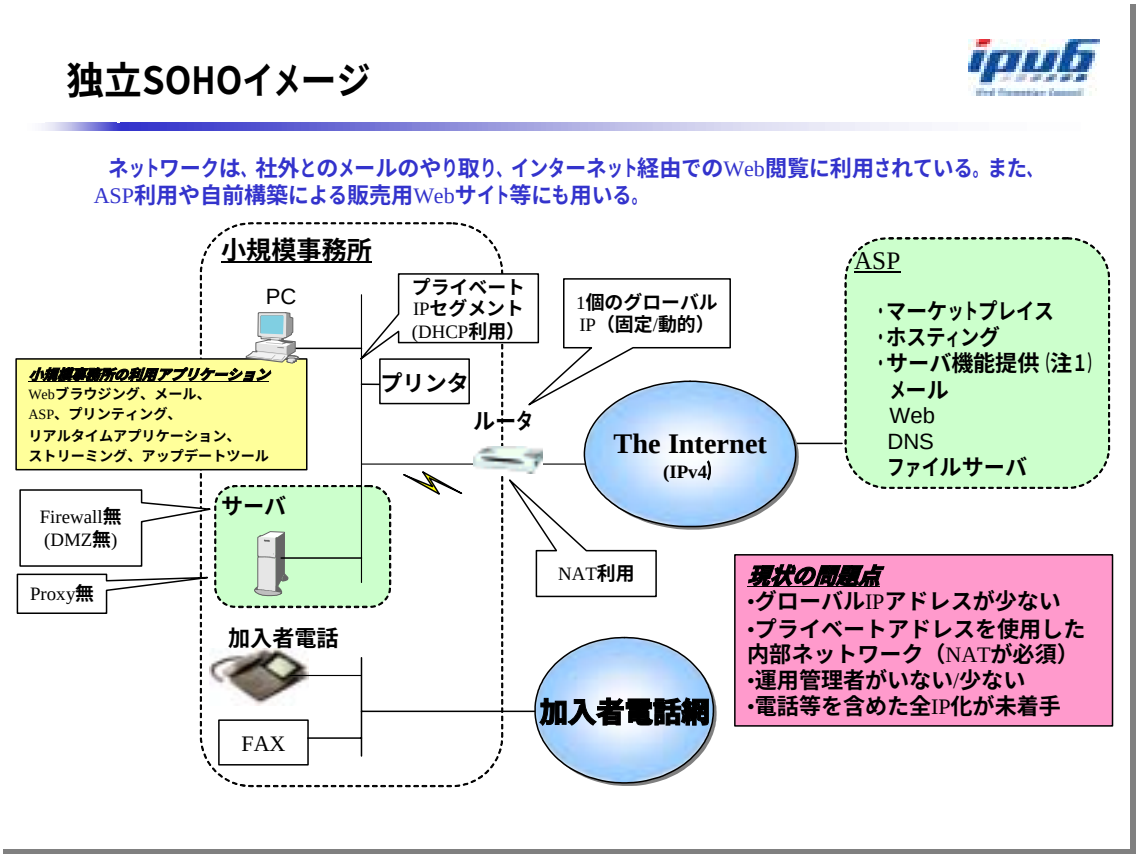
(1) 独立 SOHO の想定

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少なく、複雑なサーバ類は現地にないのが一般的です。

独立 SOHO に配置されている端末は、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。

(2) 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)ネットワークの移行

①利用する IP アドレス

分析

まず、IP アドレスに LAN 内の端末は、IPv6 を導入した場合、リンクローカルアドレスを必ず取得することになります。また、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）はアドレスポリシー的には/48 もしくは/64 です。また、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。

この段階で利用されるアプリケーションには、ソースアドレスセレクション機能は一般的に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、当面の IPv6 導入では、まずリンクローカルアドレスとグローバル IPv6 アドレスを利用します。これは P2P 通信などで有利なためです。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と考えられます。

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 IPv6 の DNS の自動設定機能については、Widows などの OS では実装がされていません。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 のクエリ代行は実装済みです。

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

ただし、IPv6 を利用した規格も標準化されつつあり(Well Known Address、DHCPv6 など)、将来的に解決されていくと考えられます。

③リンク形態

分析

ISP との接続形態としては、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。

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。

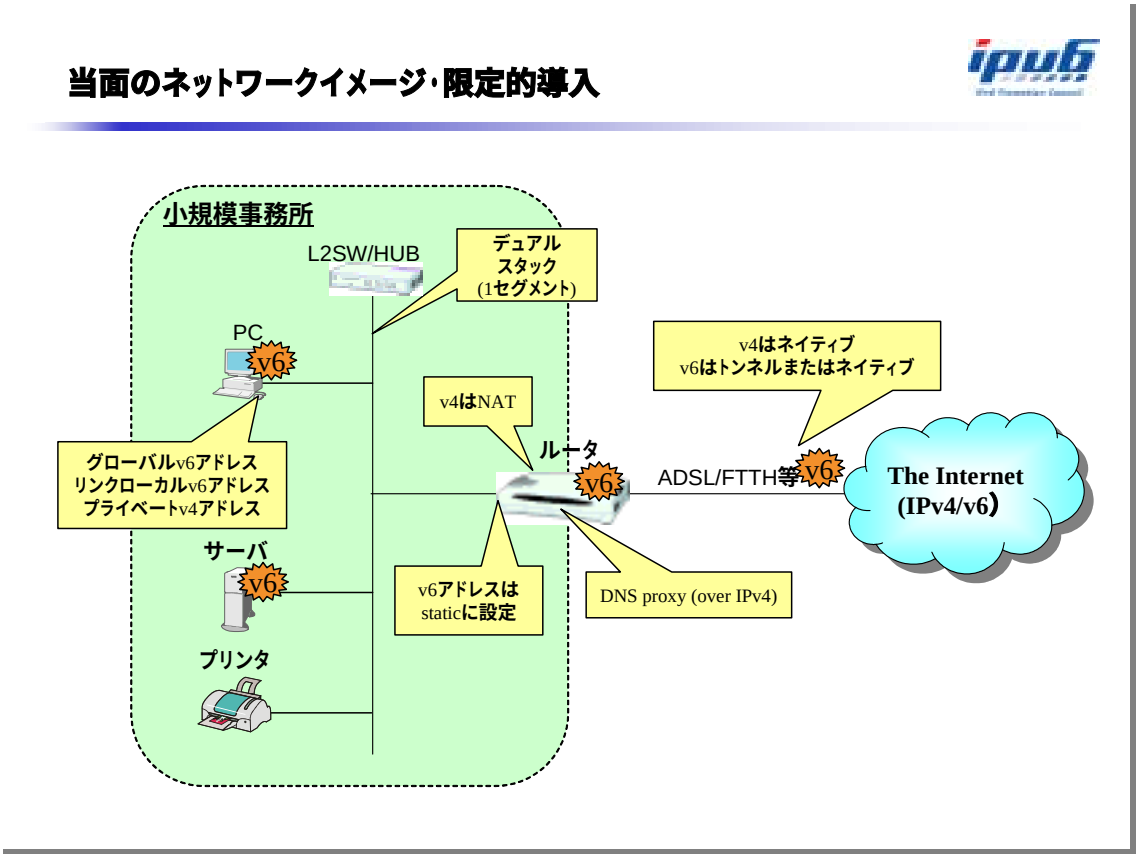
IPv6 対応したブロードバンドルータ

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

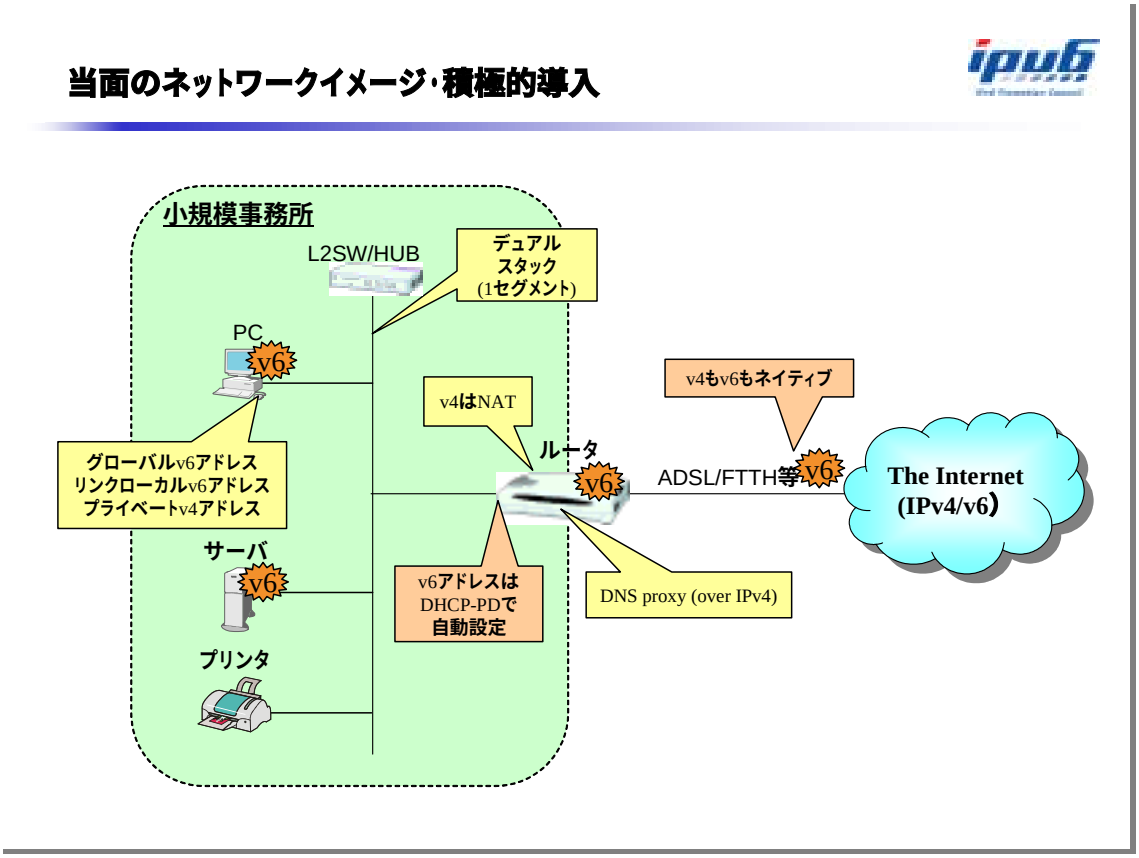
レイヤ 3 スイッチ機能を使用しないなら、現在発売されている製品で特に問題はありません。ただし、レイヤ 2 スイッチ機能だけを使う場合でも、type 値をみて IPv4 以外を通さないものがあります。古いスイッチはチェックが必要です。

(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、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

Web ブラウジングの移行においては Microsoft 社の IE をはじめ、多くのブラウザソフトが IPv6 対応となっています。また、サーバ側でも多くの IIS、Apache など多くの Web サーバソフトが IPv6 対応になっています。そのため、単にブラウジングを行うという点に限っては IPv4 と同様に利用することが可能です。

ただし、セキュリティについて、Norton、Trend 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。

デュアルスタック環境であれば、IPv4 との整合性が確保されます。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、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

いずれにしろ、Web サーバ側の IPv6 移行が急速に進むとは考えにくく、当面はデュアルスタック環境が必要となります。また、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。

課題

IPv6 オンリーの端末や環境から IPv4 の Web を閲覧するには、トランスレータかリバースプロキシが必要となります。

②メール（メールクライアント～サーバ間）

分析

クライアント・サーバタイプの IPv6 メールは、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。そのため、契約している ISP が IPv6 対応すれば、比較的容易に IPv6 対応できます。
しかし、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 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、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。

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、ウィルスチェックが IPv6 未対応の場合、IPv6 を禁止するのが妥当です。メールについては Web ブラウジングと同様クラサバモデルであり、IPv6 化するメリットが少ないため、IPv4 のみで運用しても IPv6 移行全体にたいする影響は少ないでしょう。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。

今後は、クライアント・サーバ型でなく、P2P メールが登場する可能性もあります。

課題

課題は、セキュリティチェックソフトの IPv6 対応です。

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。

プロトコル的観点では「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。

課題

独自プロトコルの ASP は、アプリケーションの改造が必要になる場合があります。

④プリンティング

分析

現状では、IPv6 対応のネットワーク直結プリンタは発売されていません。ただし、IPv6 対応した端末(サーバ)をプリンタにつなぐ使い方はできます。

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を満たすためには IPv6 対応が望まれます。

コンシューマ向けプリンタのように、USB や IEEE1394 経由の接続しかサポートされていない製品でも、今後これらのプロトコルの上で IP がサポートされる可能性もあります。その場合、IPv4 と IPv6 が両方使えるようになるか、IPv6 のみに対応するかは未知数です。また、Windows の IPP が IPv6 対応する可能性もあります。

課題

プリンタでの IPv6 利用に関しては、プリンティング機能の IPv6 対応というだけでなく、プリンタ機器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潜在的ニーズがあります。すでに電話線を用いた FAX 機のヘルスチェックサービスがあり、これを IPv6 経由で実施することが考えられます。ただし、こうしたサービスの際、プリンタとサービスサーバが自動的に通信をするわけですが、この通信パケットを許可する取り決めを、サービス業者とユーザ企業との間で行わなければなりません。

⑤P2P アプリケーション（VoIP 等）

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。

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 サーバを使わずに、直接やり取りをすることも可能です。不特定多数への接続性を確保するなら、電話帳機能（LDAP のようなデータベース機能）が必要となります。特定相手なら VoIP ゲートウェイにこの機能があれば通信できます。VoIP ゲートウェイの電話帳機能には、適宜電話帳エントリを追加する機能があれば効果的です。

IPv4 と IPv6 の IP 電話の相互接続するためには、通話パケットのトランスレータの設置が必要となります。コスト面、管理面などからみると、このようなサーバの運用は IPv6 移行へのネックとなります。SOHO サイト内で簡単に設置できるトランスレータや、トランスレーションサービスなどを ISP が提供するのが待たれます。

当面

当面 VoIP を中心とした 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。

課題

大規模なシステムにも適用できる拡張性の高いセキュリティ保護の仕組みが望まれます。IPv6 による IP 電話と IPv4 による IP 電話の相互接続についても、拡張性の高い仕組みが必要です。

⑥ビデオストリーミング

分析

SOHO の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が現状で、当面インバウンド利用が中心と考えられます。ただし、IPv6 への移行については、Windows Media Player は対応済みで、その利用に関しては技術的には問題ありません。

当面

IPv6 においては、マルチキャストが使いやすい環境を実現できることもあり、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。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。しかし、業務アプリなど特殊なアプリケーションでは、アップデートツールもサーバも特注となります。そのため、IPv6 対応も比較的一貫して行えます。IPv6 の特徴が生かせる PUSH 型モデルに変更することも検討できるでしょう。

(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、Mozilla など
メールソフト：Win Biff、Edmax
ビデオストリーミング：Windows Media Player 9

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

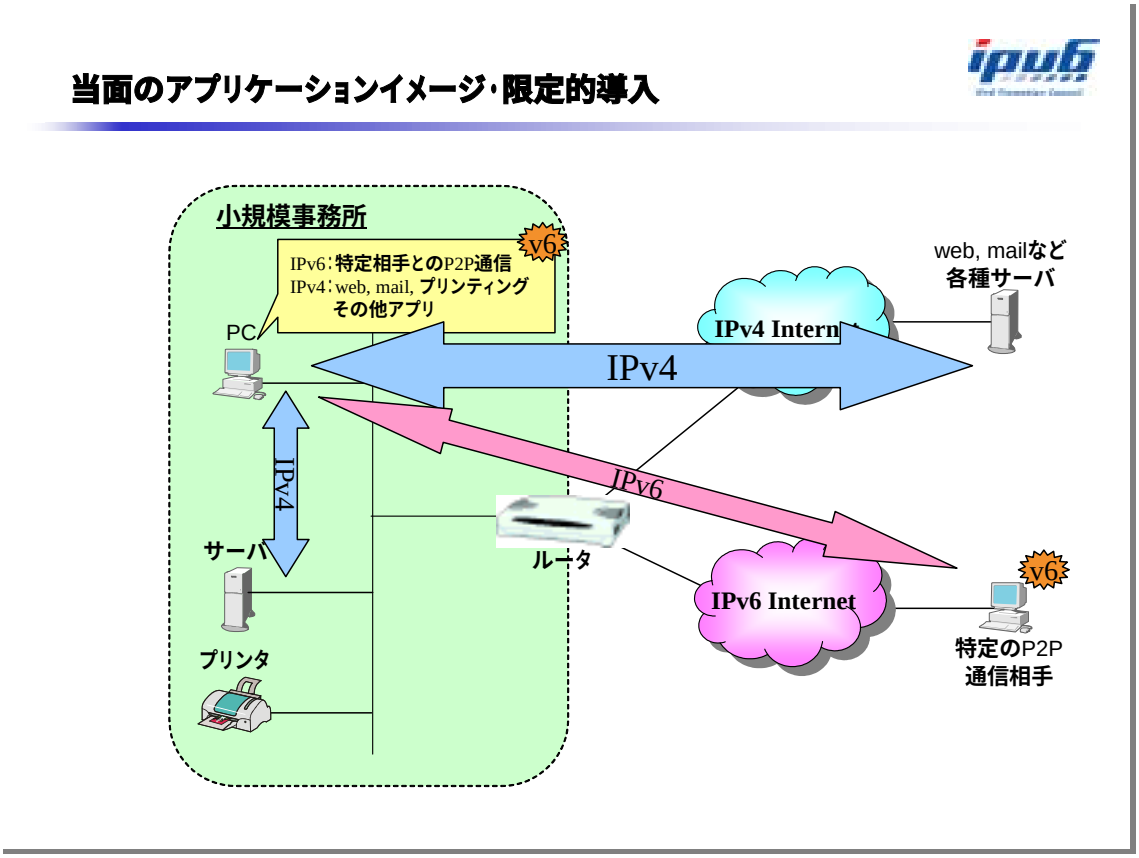
IPv6 化すると有利になるアプリケーションとしては、リアルタイム(P2P)系アプリ、ストリーミングアプリがあります。IPv6 では、NAT が必要ないという点が大きなメリットです。

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 対応も合わ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

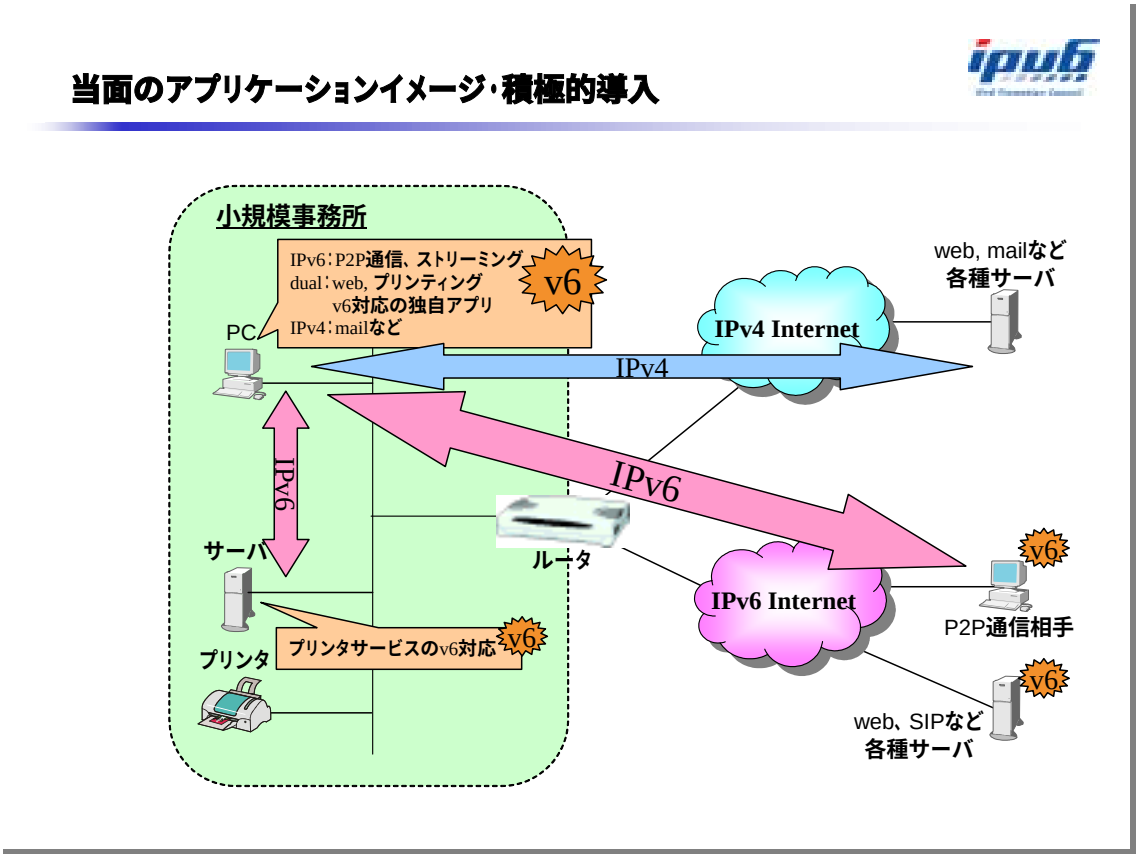
特定相手の P2P 通信は IPv6 化する価値があります。NAT が必要ないため、アドレス・ポート管理コストが削減できますし、パフォーマンス（遅延・スループット）にも有利です。Web、電子メールなど、現状 IPv4 で使われているアプリケーションはあえて IPv6 化のメリットは少なく、むしろ現状ではセキュリティ的リスクが高いと言えます。

(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。

■セキュリティ管理の移行

(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、途中機器が暗号化通信をさまたげないような設定が必要となります。

●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、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。

当面

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。ファイアウォールでは、ステートフルパケットインスペクションを利用します。P2P 通信を行う際は、アドレスが特定できる相手に限定し、ポートをあけるなどの通信がよいと思われます。

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を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

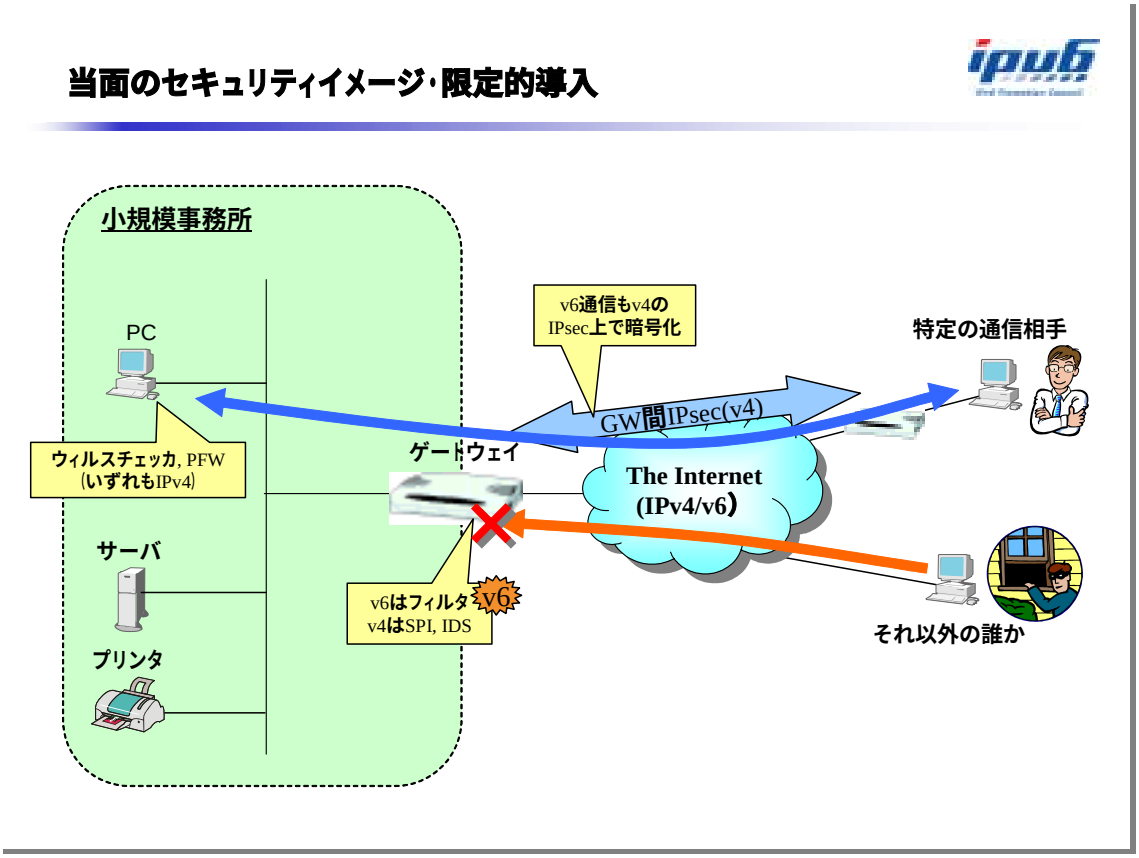
独立 SOHO における当面の IPv6 移行では、セキュリティ対策として以下の点が指摘できます。

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。

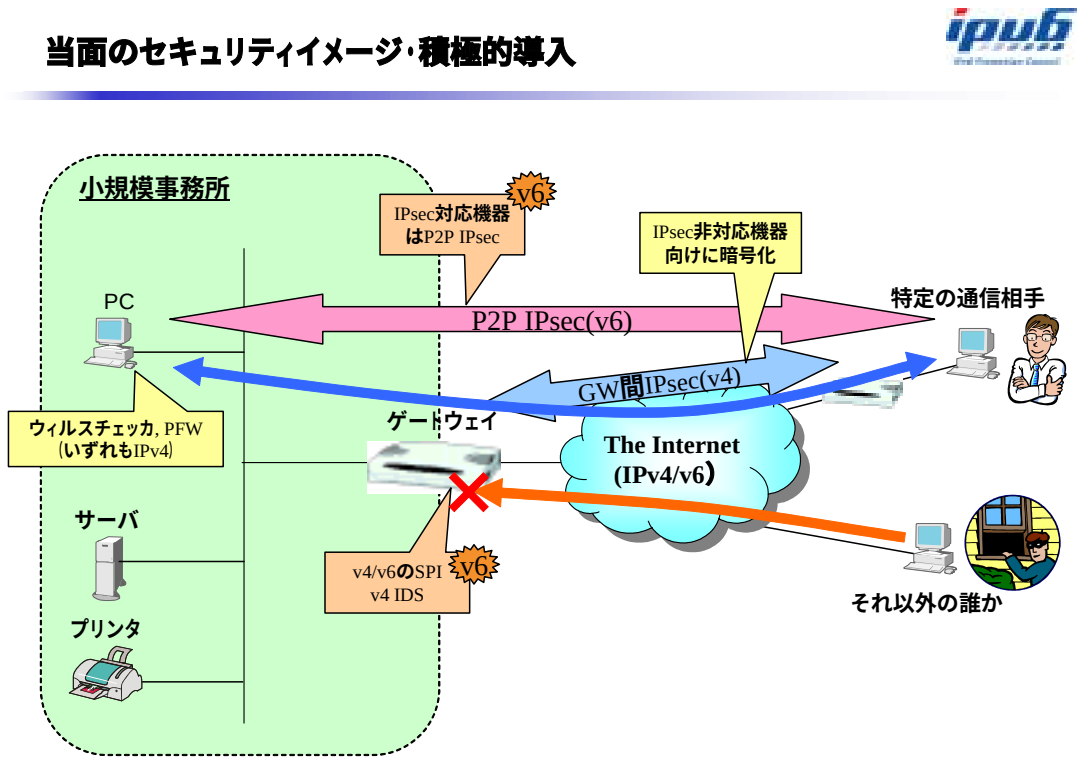
端末のセキュリティに関しては、アプリケーションレベルのツール（ファイルのウィルスチェックなど）は IPv6 でも有効であり、継続して使用します。パーソナルセキュリティツールは、現状では IPv6 では動作しない製品（メールウイルスチェックツールなど）もあるので、特に必要がないアプリケーションは IPv6 対応しないほうがよいと言えます。端末のみではなく、ゲートウェイと連携したセキュリティ設定を行うほうが簡単にできることから、端末フィルタとゲートウェイフィルタの併用をお勧めします。

(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 機能を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。

■独立系 SOHO 移行まとめ

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の 3 点は、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	Native	Native	MSR(Multi-Link Subnet Router)の扱い
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 Well-Known Address(?)	標準化

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。

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 電話化されていくことが予想されます。

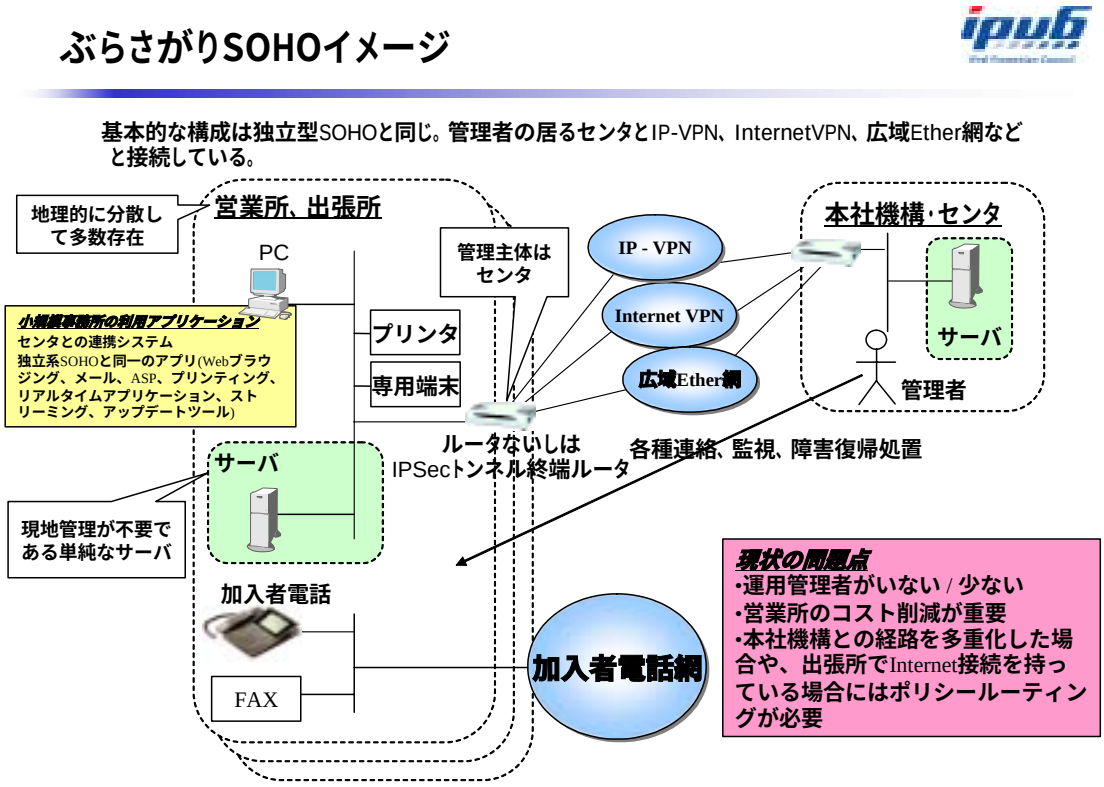
ネットワークは、センター中心のスター型 VPN を構成しています。これには、IP-VPN, 広域イーサネット, インターネット VPN（ゲートウェイ IPsec ベース）が使われています。より小規模な拠点は ISDN や DA128 による接続が行われていますが、今後は ADSL が主流になっていくと思われます。これらはバックアップとして使われている場合や、音声・情報系と業務系で分ける場合があります。

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 のネットワークは、概ね独立系 SOHO と同様ですが、本社機構・センタと VPN 等で接続していることが特徴です。

■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

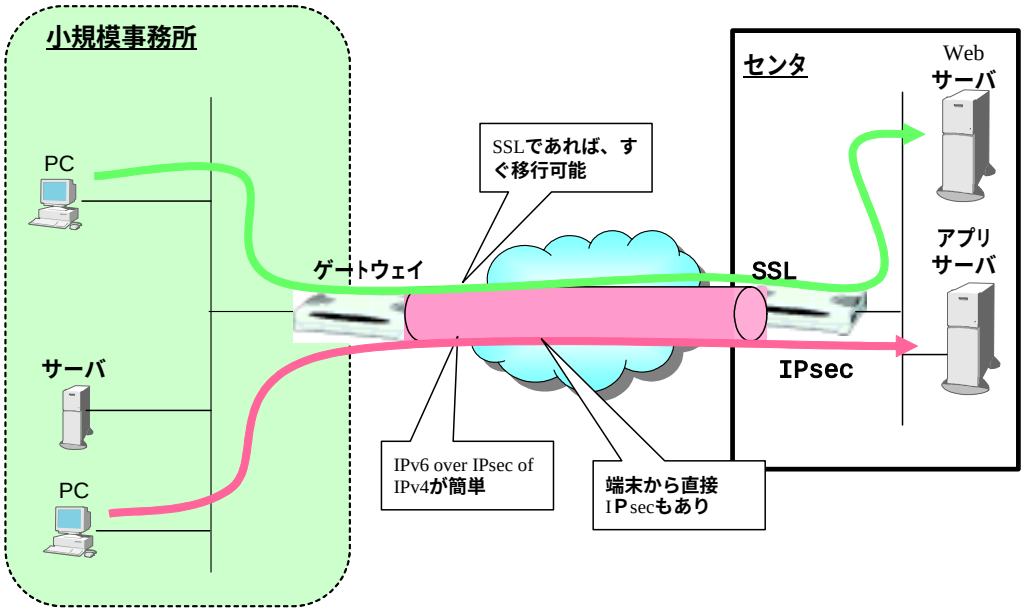
VPN に関しては、まずインターネット上の SSL サーバ利用は IPv6 でも影響を受けず、従来通り実行できます。IPv4 ではルータベースで IPsec のアグレッシブモードによるトンネルを利用するのが一般的です。

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 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

■全体イメージ

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、v6 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 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。

■技術課題

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

■ネットワークの課題

(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 prefix （1 セグメント分）配布タイプと、/48 prefix (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 prefix 割当でも 1 セグメントによる運用は可）。

/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 標準化が間近です（2003 年 12 月時点で 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です。

ASP での IPv6 対応に関しては、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 アプリケーションに関しては、IPv4 と IPv6 の間で通信する場合にトランスレーションをどこで行うべきかが 1 つの課題となります。

(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、設定が簡単になることとも関係します。

■その他の留意点

(1) 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。

(2) 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。しかし、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。

(3) 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。リゾルバの中身は IPv6 対応だが、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 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/v6 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。

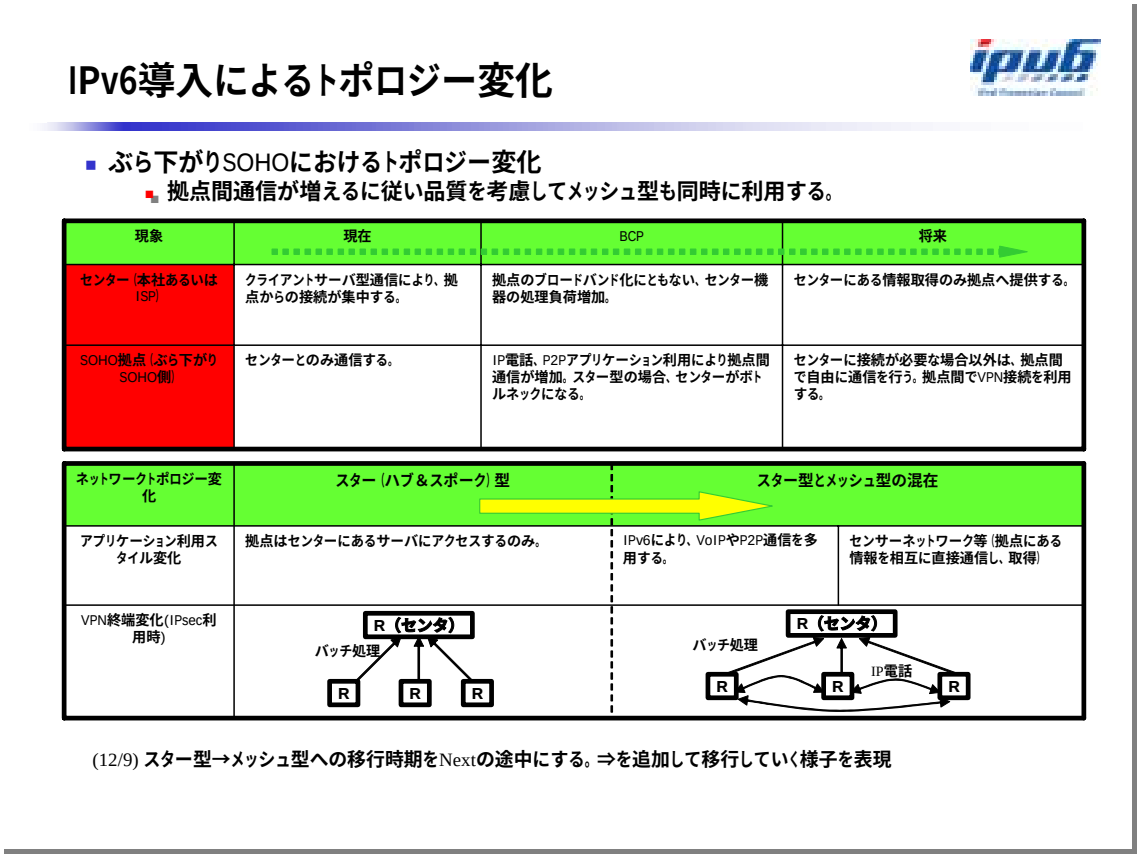
(4) QoS

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。しかしコスト的問題などにより、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。

7. Tips & Topics

■IPv6 導入によるトポロジー変化



ぶら下がり SOHO では、従来個々の拠点はセンターと通信するのみであり、このためネットワークトポロジーも一般的にはセンターを中心としたスター型に構成されてきましたが、IPv6 の普及とともに拠点間通信が増えていくことが考えられます。すると、通信品質を考慮し、スター型と併せてメッシュ型も同時に利用するようになっていくと想定されます。

具体的には、IPv6 移行に伴い、全通信を IP 網に頼る SOHO において従来のクライアント・サーバ型のアプリケーションだけでなく、IP 電話のような P2P アプリケーションの利用増加も考えられます。P2P アプリケーションを利用する際は、従来のスター型接続では一箇所に通信が集中してしまい、通信品質劣化の危険性があります。このため、拠点間との P2P 接続が可能なメッシュ型接続が必要となります。したがって、同時にスター型とメッシュ型が利用出来る接続形態が求められるようになっていきます。

■マルチホーミング

(1) マルチホーミングの目的

マルチホーミングの主な目的の 1 つは、用途別の回線使い分けにあります。たとえば SNA 系は専用線、Web やメールは ADSL 回線を利用する、などが考えられます。もう 1 つの目的はバックアップ通信路の確保です。このような目的に使われる回線の候補としては ADSL 、ISDN などが挙げられます。その他のマルチホーミングの目的としては、負荷分散やパフォーマンス最適化も考えられます。

(2) 目的ごとの要件

用途別の回線使い分けのためにマルチホーミングを行う場合、用途（アプリ）で異なる回線を選べるのが利点です。PULL でも PUSH でも、同じ用途であれば、行きと帰りで同じ回線を利用するようにしたいというニーズがあります。

バックアップ通信路の確保のためのマルチホーミングでは、ある回線が利用できなくなった時点で初めて他の回線を使う、メイン回線が使えるときは他の回線を通さない（双方向）、回線切り替え時にセッションが切れないといったことが求められます。

(3) マルチホーミング技術・手法【outbound】

外向きのトラフィックに対するマルチホーミングの実現手法としては、以下のものが挙げられます。

端末ごとに異なるゲートウェイを設定

これは、端末によって使う回線を分けるというやり方です。

端末が振り分ける

これには、端末が宛先アドレスよって自分で振り分ける（デフォルト以外の経路も持つ）、端末でポリシールーティングを行う（アプリで振り分ける）、の 2 通りが考えられます。

ゲートウェイ（ルータ、負荷分散装置）が振り分ける

これには、宛先アドレスを基にして振り分ける、ポリシールーティング（アプリケーションあるいは送信元アドレスで分ける）、ECMP などランダム的負荷分散を行う、といった手法が考えられます。

内向き DNS

これは、用途（アクセス先の FQDN）によって答えるアドレスを変える（特にぶらさがり SOHO で適用）というものです。バックアップや負荷分散目的で複数アドレスを設定します。

VRRP、HSRP、ESRP など

バックアップ目的で使われます。回線落ちが発生すると、ルータが擬似的にダウンしたように見せる拡張機能が実装されたルータがあります。

(4) マルチホーミング技術・手法【inbound】

BGP

BGP によるマルチホーミングは、経路が増えるので大規模なネットワークの場合しか許されません。

個別的 ISP 対応

これは、ISP 間でローカルに経路を流し合うといったことを想定しています。

ネットワークの途中でアドレスを変更する技術

NAT、プロキシ、トンネリングといった手法を使って、アドレスを変更する技術があります。

外向き DNS

用途（FQDN）で答えるアドレスを変えるというものです。バックアップや負荷分散を目的として、複数アドレスを設定します。

Multi prefix

同一リンク（インタフェース）に対して複数のネットワークプレフィックスを設定します。IPv6 では複数アドレスが前提となるため、広く利用することのできる仕組みです。PULL 型のアプリケーションでは、用途に応じて端末がソースアドレスを選択できます。

Mobile IP

Care-of address（気付アドレス）を使い分けるというものです。

(5) IPv6 のマルチホーミング

現在の IPv4 の世界においては、SOHO で利用できるマルチホームは NAT しかありません。SOHO で AS をもらうのは無理ですし、パンチングホールは問題視されています。また、同一端末に対して複数アドレスを設定するのは一般的でなく、複雑です。そもそもマルチホーミングでなくても NAT をしているわけですが、これでは P2P アプリケーションの利用が困難という問題があります。

一方、IPv6 ではマルチプレフィックスが手段として有効と考えられます。RFC3178（secondary link を使う）という方法もありますが、これはコスト高になります。特にぶらさがり SOHO では、マルチプレフィックスを使ってサービス毎にアドレスを分けることで、うまく運用できそうです。PULL 型アプリではソースアドレス選択の機能が重要です。この手法については IETF の multi6 WG において検討中で、全体的な考え方だけは RFC 化済み（RFC3582）です。

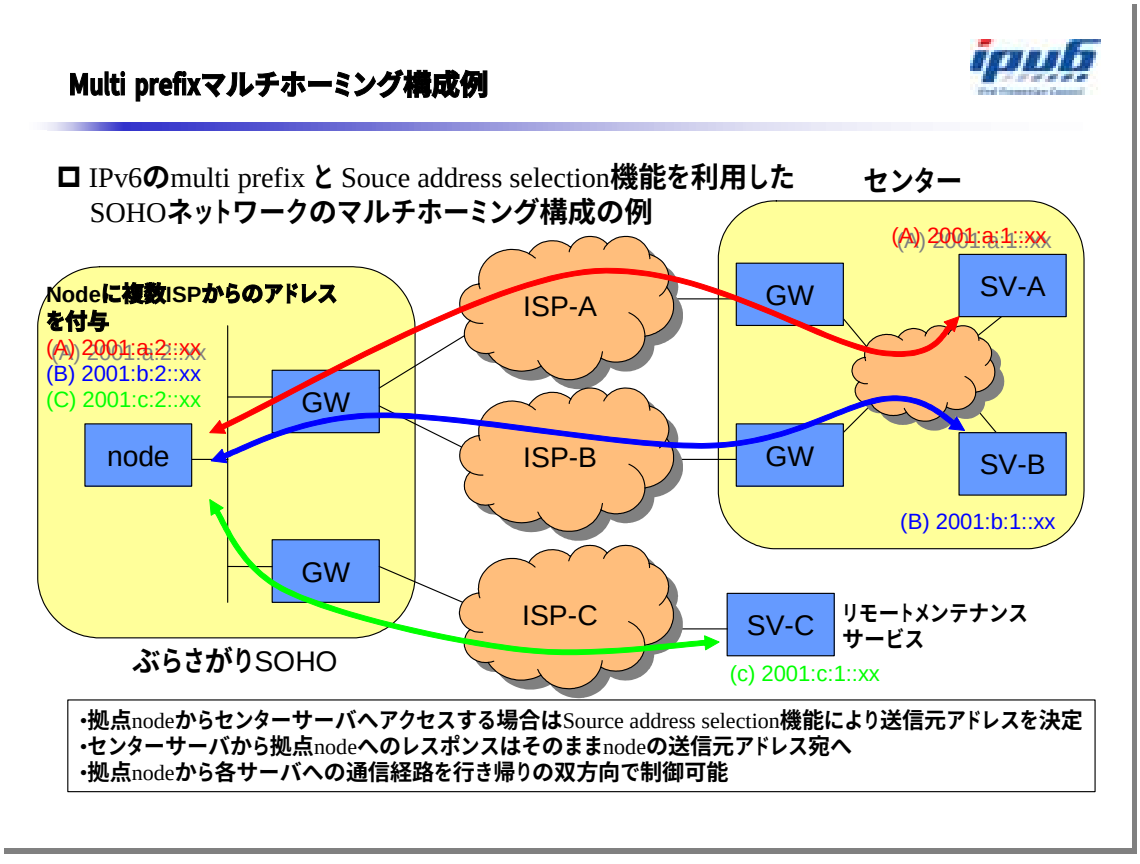
(6) IPv6 のソースアドレス選択

ソースアドレス選択は、RFC3484 Default Address Selection for Internet Protocol version 6 (IPv6)に規定されています。この RFC では、送信元アドレスを選ぶ 8 つのルールを定義しています。

1. 宛先と同じアドレスを優先
2. 宛先とスコープ的に近いアドレスを優先
3. deprecated でないアドレスを優先
4. care-of address（気付アドレス）より home address（ホームアドレス）を優先（※ アプリで逆転できるメカニズムを提供するべき(SHOULD)）
5. そのパケットを送信するインタフェースのアドレスを優先
6. ポリシーテーブル上でラベルが宛先と同じアドレスを優先
7. 一時的アドレスよりパブリックアドレスを優先（※ アプリで逆転できるメカニズムを提供しなければならない(MUST)）
8. 宛先と一致部分が長いアドレスを優先（longest match と呼ばれる）

アプリで使い分けるには、現状では 8.のルールが利用できます。ただし、計画的なアドレス設計が必要となります。6.のルールは全端末に設定が必要な点が難点として挙げられます。

(7) マルチプレフィックス・マルチホーミングの構成例



図は、アクセスするサーバのアドレスに応じて、別の送信元アドレスを利用している例です。これにより、用途に応じて通信経路を双方向で制御することが可能となります。

(8) マルチプレフィックス・マルチホーミングの課題

マルチプレフィックスを使ったマルチホーミングの 1 つの課題は、デフォルトルータ選択にあります。回線毎にデフォルトルータが分かれている場合、どれに送るか分からないという問題です。これに関して、RFC2461 (Neighbor Discovery)では特に基準が設けられていません。ルータがそのまま不適切なパケットを回線に転送してしまうと、用途が合わない可能性があるほか、ISP の ingress filter にひっかかる可能性があります。

端末の実装に改良を加え、対応する送信元アドレスを見て、対応する RA 送出元ルータに送る、あるいは draft-ietf-ipv6-router-selection-02.txt（RA で経路を流す拡張）を利用するといった手が考えられます。しかし、これらの手法が利用できるようになるまでは、とりあえずルータ側でリダイレクトすることで対応するしかありません。

もう 1 つの課題は、回線切り替え時の挙動です。即座にアドレスを切り替えられないと、別回線のアドレスで ingress filter にひっかかることにより通信が途絶える可能性があります。ルータで回線断を検出した場合に、RA に反映できればいいのですが、エンドツーエンド通信では、セッション切れが発生します。これは NAT ベース IPv4 でも同じです。回線の切り替えが起こるとアドレスが変わるのだと、セッションは切れるため、たとえば Mobile IP などの、セッションを維持する仕組みが必要となります。

■QoS

(1) IP 網の通信品質保証

IP 網の特徴として、競合時のパケット廃棄を容認することで資源を共有化している点があげられます。このため、IP 網は安価な網を構築可能です。

IP 網を実現している物理的な網構成（ATM、Ethernet 等）により、品質保証技術は異なります。また VoIP や VPN などの使用目的によって品質の閾値が異なります。

品質保証には、QoS と CoS の２種類があります。QoS は帯域等を絶対的に確保するものです。CoS はパケット転送やパケット廃棄の順番に優先度を付けて処理し、相対的な通信品質を保証する技術です。QoS を保証する技術として、QoS シグナリング（RSVP 等）、パケットマーキング、パケットクラシファイング、パケットメータリング、パケットポリシング、スケジューリング（WFQ 等）、キュー長管理（WRED、CAR 等）があります。

(2) SOHO の通信品質保証

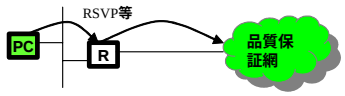
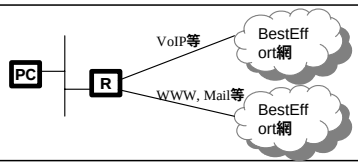
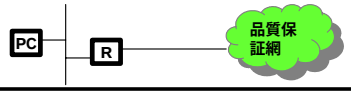
SOHO では、容易に Gigabit Ethernet ネットワークが構築出来るため、LAN 内において品質保証を行う必要はありません。ただし、SOHO 内に高付加なサーバがあるデザイン事務所などは例外です。

また、WAN は、LAN と比較すると帯域が小さいため、品質劣化原因の１つであり、SOHO における品質保証では、主に WAN を検討することが重要です。

(3) SOHO の通信品質保証パターン

SOHO においては、通信品質保証は以下の 4 パターンが考えられます。これらを単独で、または組み合わせて実現します。

SOHOの通信品質保証パターン

項目	内容	概要図
端末	端末主導の通信品質保証システムを利用する。	
接続回線	Routerにて品質保証設定（優先転送やパケット廃棄）を行う。接続回線帯域増加も含む。	
複数接続回線	複数の接続回線を利用し、負荷を分散させる。	
通信品質保証網	キャリアが通信品質を保証した網を用意する。	

上記パターンを単独あるいは組み合わせて利用する。

(4) IPv6 の品質保証に関する特徴

IPv6 の品質保証は、既存の IP 網の構成機器による品質保証機能に依存しており、IPv4 と比較して通信品質保証機能に何か優位点があるわけではありません。ただし、ヘッダフォーマットの QoS 対応による粒度細分化やパケット分割の無いことによる通信経路上機器の負荷低減における効果はあると思われます。

IPv6 では、ヘッダに Traffic Class フィールド（8bit）が設けられており、優先制御等のクラス分類に使用することができます。IPv4 でこれにあたるのは、ToS(Type of Service)（8bit）です。また、Flow Label フィールド（20bit）と呼ばれるフィールドも用意されています。これは、送信元がフロー単位の処理方法を指定するのに使用することができます。

通信品質保証に関連して、IPv6 では、通信経路上の機器によるパケット分割が行われない点には注意が必要です。送信端末が、廃棄されないサイズのパケットを送信するためには、より小さい MTU が設定された経路上の機器から、送信元へ ICMP の「Packet Too Big Message」が到達する必要があります。このため、経路の機器を管理する ISP 等が該当メッセージを遮断しないことや、遮断しないことによるセキュリティ低下について検討する必要があります。

(5) IPv6 の事象別特徴

IPv6の事象別特徴

項目	IPv4	IPv6
アプリケーションの通信品質保証	IPレイヤにて8bit (ToS) 種類が制御可能	IPレイヤにて8+24bit (Traffic ClassとFlow Label) 種類が制御可能
端末単位の通信品質保証 (VoIP, リモートメンテナンス等)	NAT利用のアドレス隠蔽により、E2EのQoS保証は困難	グローバルアドレス利用によりE2EのQoS保証が容易
端末自身による資源誘導	予め、資源へ経路設定を行う静的な資源誘導あるいはRSVP等のシグナリングを利用。	マルチプレフィックスによるソースアドレスセレクションを用いた動的な資源誘導
パケット分割による処理遅延回避	通信経路上でパケット分割や再構築が行われるため、処理遅延増加	送信元以外ではパケット分割をしないため、経路上での処理遅延低減

- IPv6は、QoS保証の粒度がより細分化でき、自由度の高い設定 (E2EのQoSのマッピング等) が可能である

表に示されているように、IPv6 では、きめ細かな設定を可能にする QoS、CoS の仕組みが用意されており、保証の粒度がより細分化でき、柔軟な運用ができます。

(6) 通信品質保証まとめ

IP の通信品質保証は、構成される物理網に大きく依存します。IPv4 から IPv6 へ移行する際に物理網が変化することはないため、品質保証技術そのものに差異はないと考えられます。しかし、IPv6 は、IPv4 と比較すると、品質保証に関して粒度細分化や E2EQoS、資源誘導、パケット分割に関して優位性があります。IPv6 を用いることで、特に VoIP やリモートメンテナンスといった E2E を対象とした品質保証実現が容易になります。このため、E2E 上の全構成要素を連携した品質保証も可能となります。ただし、SOHO では、品質保証を設計/設定/運用を行う管理者がいないことが課題です。

(7) 通信品質ガイドライン

IPv6 移行に伴い、全通信を IP 網に頼る SOHO においてミッションクリティカルな通信とその他通信を差別化し品質保証を行うことは必須となります。IPv6 により品質保証の細分化が向上しますが、管理者不在の SOHO では、LAN での品質保証は比較的容易である一方、WAN の品質保証は困難です。そのため、SOHO に対して、自動化された通信品質保証が提供される必要があります（注：品質保証サービスが従量課金か定量課金かのどちらになるかは、利用方法により異なる）。

■機器監視・遠隔制御

(1) 機器監視・遠隔制御の需要

遠隔的な機器の監視や制御に関する需要は、管理をアウトソースするニーズから生まれてきます。小規模な集合体が業務をアウトソースするもっとも良い例は、エレベータの遠隔監視でしょう。通常の中・小規模ビルでは「警備・防災センター」のような 24 時間人が常駐する集中監視所を設置できないため、エレベータの監視システムが稼働しています。

また、ネットワーク内の機器を監視する例としてはプリンタヘルスチェックシステム(カウンタ量チェックや、トナー&用紙使用料をチェックして、自動的にトナーや用紙を発送したり、定期メンテナンスをするシステム)があり、ビジネスとして成立しています。

SOHO は管理業務をアウトソースしやすいという側面があります。これは、アウトソースしなければならないケースが多いということでもありますし、アウトソースすることで管理レベルが向上することがはっきりしやすいという事情があります。遠隔監視・制御サービスを実現するには、LAN 内部の機器と外部の機器の通信が必要になります。

(2) 機器監視・遠隔制御の形態

遠隔監視・制御には、PULL 型と PUSH 型が考えられます。

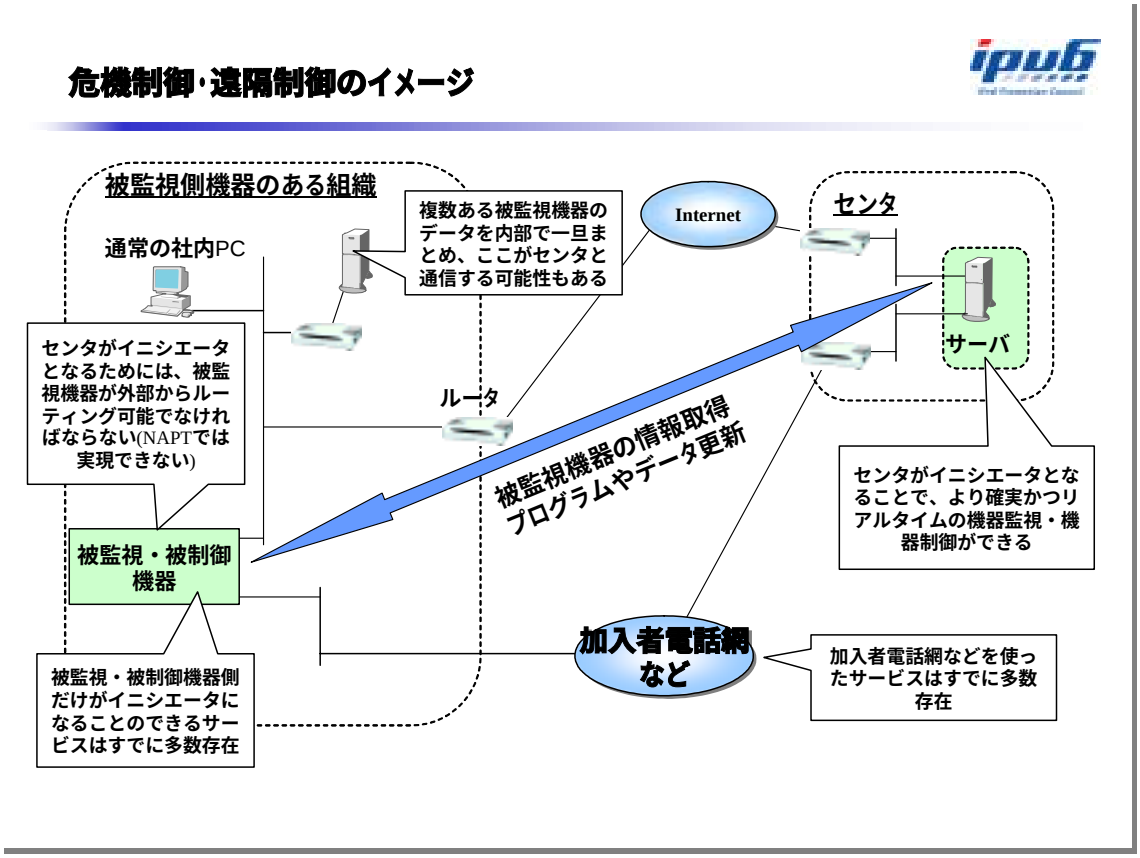
PULL 型は、LAN 内部にある機器のみイニシエータになれるという形態で、従来のセキュリティの枠組みで実現しやすいと言えます。しかし、通信に遅れが発生する、無駄に帯域を消費する、といった欠点があります。

一方、PUSH 型は、LAN 内部の機器だけでなく、外部の機器もイニシエータになれるというものです。この形態は、外部からのルーティングが可能な IPv6 でこそ実現可能性が高いもので、様々な新ビジネスの可能性があります。

PULL 型の悪い例が Windows Update です。これはユーザ主導による半自動方式であるため、ユーザが気づかずセキュリティホールが埋められないことが頻発しています。これに対して PUSH 型は外部から機器を直接コントロールする手法です。PULL 型でも擬似的に実現が可能ですが、その場合は帯域を浪費します。

(3) 機器監視・遠隔制御のイメージ

SOHO における、機器の遠隔監視・遠隔制御のイメージは、以下の図のようになります。



(4) PULL 型の欠点と PUSH 型の利点

PULL 型の欠点は、現在の Windows Update を例として説明することができます。PULL 型では、ユーザの対応行動に依存するため、対策が遅れることや、結局対策されないことがあり、未だに Blaster や Nimda などがなくならないのは、その証拠であるとも言えます。もし、Windows Update が PUSH 型だったとしたら、遅滞なく相手に通信し、センター側でアップデートされていないものを管理できます。そして、アップデートできなかった環境にだけ、アップデート CD を無料送付するなどの対策も可能です。特に、サーバ管理のアウトソース（外部からサーバに telnet する）など、リアルタイムのコントロールサービスを実現しようとするなら、外部がイニシエータにならざるをえません。

(5) 監視に利用するネットワーク

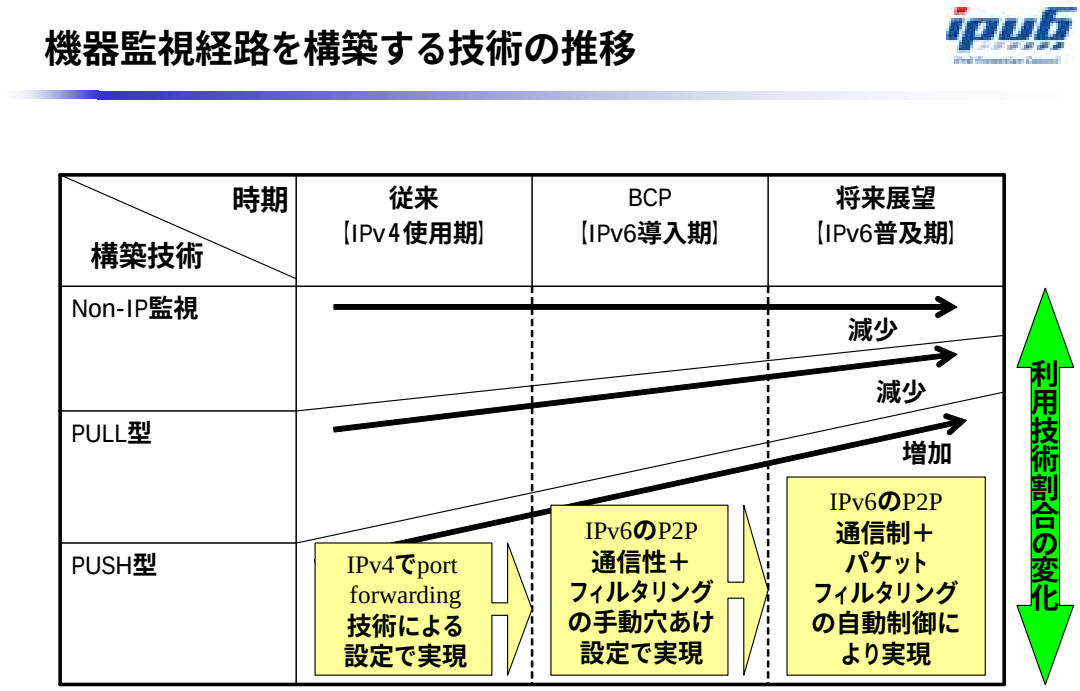
監視のためのネットワークとしては、次のような選択肢があります。

1. 非 IP 網(電話など)
   価格が高い、IP による透過的な通信が行いにくい
2. 専用線・広域イーサネット網・IP-VPN 網など
   大規模でないと費用対効果が悪い、管理が面倒
3. インターネット VPN 網
   価格が安い、トンネリングの欠点、機器のコストが必要
4. IPSec トランスポートモードによる監視通信
   特に価格が安い、PUSH 型通信が必要、エンドツーエンドの通信路さえあれば、管理しやすい

コストや使い勝手の面から、将来に向けて 1.から 4.へのシフトは進んでいくと考えられます。

(6) 機器監視経路を構築する技術の推移

現在の IPv4 使用期から将来展望の IPv6 普及期まで、機器監視経路を構築する技術を段階ごとに示すと、下記のようになるものと考えられます。



(7) IPv4 を利用した従来技術

IPv4 環境における PULL 型サービスは、イニシエータが常に LAN 内部のみであり、実現が容易です。一方、IPv4 において PUSH 型を実現するには、非 IP 回線、専用線、IP-VPN 網を利用する必要があります。つまり、端末を監視するだけのために異ネットワークを接続していることになります。これは、高コストであり、大規模な監視システムによる環境でなければ利用できません(SOHO では用いられにくい)。

ポートマッピングによる PUSH も考えられます。該当する内部ノードに対してポートフォワードを行うものですが、スケーラビリティを考慮する必要があり、ネットの管理にはある程度以上のスキルが必要です。

(8) IPv6 化による従来技術の変化（BCP）

IPv6 への当面の移行が起こった場合、遠隔監視・制御にどのような変化をもたらすでしょうか。

まず、PULL 型に関しては、IPv4 利用の場合と変化はありません。PUSH 型に関しても、非 IP 回線や専用線、IP-VPN 網などを経由した PUSH に限っては、IPv4 利用の場合と変化がありません。しかし、IPv6 の P2P 通信性を生かすことにより、非 IP 回線だけでなく、インターネット上でも特別な設定なしに同じことを実現できるようになります。

なおパケットフィルタ設定等のセキュリティ配慮は必要で、外部からの到達性を限定的に持たせる設定が要求されます。この設定はスケーラビリティが低く、管理にはある程度以上の技術が必要となります。 エンドツーエンド通信による IPSec トランスポートモード通信も適用可能です。

(9) 将来望まれる技術

将来は、自由度の高い PUSH により、BCP において手作業で行っていた限定的な到達性実現を自動化することが望まれます。 具体的には、相手の認証やフィルタへの穴あけ、利用完了後に穴を戻すような処理を自動的に実現することが求められます。

相手に応じた(認証結果に応じた) 制御や通信状況に応じた制御を実現したいわけで、そのためには SIP に似たプロトコルが使われるようになると思われます。こうした仕組みについては、手順を標準化する必要があります。標準化しないと、各メーカの独自規格が乱立し、メーカ、ユーザ共にコスト増となってしまいます。逆にこの仕組みが実現すれば、他の方式の必要性が低下します。

(11) セキュリティの課題

セキュリティに関しては、外部から内部へのルーティングを可能にすることに関する課題が生じますが、フィルタの設定をきちんと行う、という当然のことを行えばよいとも言えます。外から内への限定的アクセス許可を与えるには、従来のフィルタで静的に設定する方法に加え、端末からのリクエストを受け取り、必要に応じてその場で通信を許可するフィルタなど、条件に応じた動的フィルタの利用ができることが望まれます。

また、通信秘匿の必要性が増してきます。これにより、従来のレイヤ 4 以上によるセキュリティだけでなく、レイヤ 3 の IPSec も視野に入れられることになります。

内部に設置した機器から外部への情報漏えいの懸念については、内部の機器にセキュリティホールがあることから起こる漏えいの対策として、自動自己更新とその継続的サポートを必須とするなどの対策をとります。機器そのものに悪意のある実装がなされていることを防ぐためには、企業間の契約、法律による禁止が必要です。

IPv6 移行ガイドライン（SOHO セグメント）

平成 16 年 5 月発行

発　行　IPv6 普及・高度化推進協議会
連絡先　wg-dp-comment@v6pc.jp
URL　http://www.v6pc.jp/