「家庭用ルータガイドライン 第0.9版」に対するパブリックコメントの一覧とその対応と回答

対象ページ	該当文言	意見	理由	対応	回答
全般	全般	その1) IPv4でしか通信できない機器(特に家電など)の対応についての不備が著しい。暗黙で家庭内LAN環境がIPv4/IPv6デュアルスタックネットワークあるいはIPv6で通信する機器しかない前提であるのであればそのことを明記すべき。もちろん私個人の意見としてはIPv4でしか通信できない機器(特に家電など)をIPv6経由で何らかの技術を用いて通信出きるような実装を当文書において推奨すべきであると考える。 その2) NAT(IPv6toIPv6 & IPv4toIPv6)の類がまったく触れられていない。 - IPv4ネットワークでのNATの効能にユーザの大多数がなれている - 特に現在では家庭内LANにおいてサーバの役割を行う機器(家庭内NASや家電等)も増えている 上記2点から"ISPが変わったら or ISPが配るアドレス変えたら宅内LANのアドレスも変わる"という"ポリシー" を全ての家庭内LANユーザが受け入れられるとは考えにくいと考える。また経済的理由で家庭内LAN環境をIPv4のまま留めておきたいユーザもいるだろう(現在のWindows9x/2000,Classic MAC ユーザの割合を想起せよ)。"ISPが変わっても"あるいは"ISPが配るアドレスが変わっても" 宅内LANのアドレス体系を固定できるような仕組みの実装(おそらくNATだと思うが)を当文書において奨すべきであると考える。		その1: 反映 その2: 課題	本ガイドラインでは対象環境をデュアルスタックでのサービス提供を前提としたものとしています。従って、IPv4しか利用できない家電などの機器は引き続きIPv4経由で接続可能な環境としています。この辺りの前提条件が明確になるように変更を行いました(**p.2**)。 また、トランスレータを含むNAT機能に関しては今後の課題とさせていただきます。
全般	全般	いわゆる家庭用ルータは、提供形態の観点で大きく分けて2つあり、 1. ユーザが市販品を購入し設置するもの。⇒インタフェースとしては 対ISP(WAN側)と対ユーザ(LAN側)の2つについて規定が必要。 2. ISPからユーザに提供されるもの。⇒ルータまでISPの責任区分であり、規定すべきものは対ユーザ側(LAN側)に限られる。 という状況ですが、ガイドラインではこの2つを区別していないように見えます。これにより、規定しなくてもいい場合においても規定してしまっている部分があります。 例えば、2. のような形態においては、ユーザのプリフィックスを割り当てる方法がDHCPv6-PDである必要は全くありませんが(ISP独自方式でも構わない)、ガイドラインでは DHCPv6-PD の実装をMUSTとしており規定としては過剰となってしまいます。 改定案1) BBルータの内部処理(ファイアウォール等)と、LAN側の規定のみとする。WAN側でどのようなことが行われるかはスコープ外とする。 改定案2) WAN側についても、対ISPのインターフェースとして規定をする。ただしBBルータがISP提供のものである場合は適用しないことを明記。		再検討 一部反映	本ガイドラインではISPを変更した場合においても利用可能な家庭用ルータを対象としていますので改定案1のような対応は難しいと考えます。また、このガイドライン自体が強制力を持つものではありませんし、ISPやルータベンダに対して仕様を強要するものでもありません。したがって、改定案2のようにISPにより提供されるものを区別するのではなく、強制力を持つものではないことを明確にしました(**p.1**)。 なお、必要度がMUSTであることに関しては引き続き議論したいと考えています。
全般	全般	従来の家庭用ルータ(IPv6非対応)についてはこういった文書はないんでしょうか。		-	本SWGにおいてもご指摘の文章は把握できておりません。
全般	全般	外部参照ドキュメントの概要が書かれていないものがある 参照だけでなにも書かれてないと読み辛いのと、いくつかの英文ドキュメントは翻訳か要約がついてるとわかりやすいでしょう。 特に draft-ietf-dnsext-dnsproxy はBCPになりそうですから、必ず実装しないといけないものになるので、要点列挙か参考訳があるとよいとおもいました。		今後検討	要約に関しては今後検討して判断したいと思います。
全般	全般	フラグメントについて書かれていない 特にDNSでは、EDNS0でpayload 4096octets程度までのUDPパケットを扱います。 フラグメントされたUDPパケットを捨てられるとDNSは終わります。(特にDNSSEC)		課題 一部反映	フラグメントとフィルタリングに関しては今後の課題とさせていただきます。なお、フィルタリングの個所においてフラグメントパケットに対しては再構成を考慮する必要がある旨を追記しました(**p.17**)。
5	図 1-2 宅内ネットワークの設定概要 経路情報の配布 ・ISPは各ユーザの家庭用ルータに対して経路(デフォルトルート等)を配布する	「ISPから取得した経路情報(デフォルトルート等)を宅内機器に配布する」とすべき	図 1-1 のコピーとなっている	反映	ご指摘の通り誤りでしたので修正しました(**p.5**)。
5	1.4.2 宅内ネットワークの概略	宅内ネットワークがIPv6とIPv4のデュアルスタックとなる場合についての記述がない。	IPv6のサービスが本格化しても、当面の間、宅内ネットワークはIPv6とIPv4のデュアルスタック構成となるはずです。その場合、家庭用ルーターにも、IPv6とIPv4の間でトンネリングやトランスレートを行う機能が求められると思います。特に、将来IPv4アドレスが枯渇した後では、ISPから割り当てられるグローバルアドレスはIPv6のみ(IPv4アドレスはキャリアグレードNATでの割り当て)となるケースが出てくるでしょう。その場合、外部からグローバルIPアドレスで接続できることが求められる家電製品(宅外からのアクセス機能を持つHDDレコーダーなど)でIPv6に対応していないものは利用できなくなってしまいます。 そのため、家庭用ルータにも、ISPからのグローバルIPv6アドレスと宅内のプライベートIPv4アドレスとの間で行うNAT-PT機能や、IPv4 over IPv6トンネリング機能が必要ではないでしょうか。	反映	本ガイドラインでは対象環境をデュアルスタックでのサービス提供を前提としたものとして特にIPv6に関連する個所に特化して書いています。さらに、IPv4アドレス枯渇により登場すると想定されるLSNに関しては今回対象外としました。この辺りの前提条件が明確になるように変更を行いました(**p.2**)。
6	1.4.3 家庭用ルータに求められる機能	家庭用ルータに求められる機能として、IPv6とIPv4の間でのトンネリングやトランスレートの記述がない。		今後検討	トランスレータに関しては今後の課題とさせていただきます。

対象ページ	該当文言	意見	理由	対応	回答
7	推奨(SHOULD)、オプション(MAY)	RFC 2119に従った記述にすべき。 SHOULD → RECOMMENDED MAY → OPTIONAL	日本語と英語で受けるニュアンスが異なるので。 参考) "しなければならない(MUST)" "要求されている(REQUIRED)" "する必要がある(SHOULD)" "推奨される(RECOMMENDED)" "してもよい(MAY)" "選択できる(OPTIONAL)"	非対応	IETFにおける必要度のルールに準拠して記述しておりますのでこのままとさせていただきます。
8	「この章では、ルータに必要とされる機能定義は行っていない。また、各接続形態における認証技術に関しても今回は対象外としている。」	これだけではIPv6対応の家庭用ルータを作るための最小限のガイドラインとしては不十分に思います。3種類の接続方法が挙げられていますが、それぞれについて必要な技術・機能をもう少し詳細化できませんでしょうか？	家庭用ルータを実装する場合に重要である外部接続方法の技術詳細が不明なため。	今後検討	ISPにおけるサービスに依存した課題は、今後の課題とさせていただきます。
8	全体	ネイティブ接続にも2種類あるはずなので、その旨を追記したほうがよいかと思います。 a) ISPルータと1CPEをpoint-to-pointでネイティブ接続 (point-to-point mediaで; e.g. ダイアルアップPPP) b) ISPルータと複数CPEをpoint-to-multipointでネイティブ接続	a)はPPPoE/PPPoA/トンネルと同様に考えることも可能ですが、b)だともう少し考慮が必要になるかと思われます。(e.g.「ISP側がonlink-bit=OFFでRA広告」とか「ISP側のUnicast-RA実装+CPE側のRS定期送信が必須」とか、などなど)	今後検討	Point-to-Multipointは今後の課題とさせていただきます。
12	表3-1	IPv6の「非固定」にはこのような形もあるはずです - 接続中に自動的にアドレス更新される (一時的に端末が複数のIPアドレスを所有) 片方はPrefered-lifetime=0 -> 過去のTCP sessionなどの関係で古いアドレスを使い続けたい場合だけ使用 -> そのうちValid-lifetime=0になったときに、消滅 もう片方がPreferred-lifetime!=0 -> 新規 TCP sessionなどはこちらを使用 => 具体的なイメージ=新たな通信を行うと、新しいアドレスになる => 宅内のアドレスが徐々に変わるイメージ	IPv6ならではの非固定パターン(アドレス寿命が2種類あることに着目)であるため、特別な考慮が必要と考えます。	課題	非固定プレフィックス利用時のリナンバリングの挙動は整理が必要と考えています。今後の課題として今後反映したいと思います。
12	3.2節全体	「WAN側へのアドレス付与」に限定する意味はどのくらいありますか?	死活管理が目的ならば、ルータのloopback Interfaceへのアドレス付与でも実現できるはずかと思います。	課題	死活監視のみが目的でWAN側のアドレス設定を考えたわけではないのでSHOULDとしています。Loopback Interfaceに関する議論は今後の課題とさせていただきます。
12	3.2.1 グローバルアドレスの付与	必要度はSHOULDでなく、MAYが妥当と考える	IPv6においてはNATを使用しない場合複数のネットワークインタフェース(以下、「NIC」とする)を持つノード(家庭用IPv6ルータを含む)それぞれにGlobalアドレスを付与して運用することも想定されるが、備考にも触れられている通りWAN側にGlobalアドレスを設定することが必ずしも必要ではないと考える。 IPv6ルータのWAN側にはNIC活性時に振られるLink Localアドレスが存在しており、WAN側NICにてパケット転送を有効にすればNDPが有効になることにより(NATが不要なため)シームレスにLAN側Globalアドレス-エクストラネットワーク間の通信も行える。 一方で、WAN側NICにもGlobalアドレスをDHCPv6、ICMPv6、手動により設定した場合、逆にDADによるアドレス決定までのタイムラグやMLDv2report、Globalアドレス設定後のルーティングテーブル管理など、管理コストが発生することすら想定される。 上記理由により、家庭用IPv6ルータのWAN側NICに関しては、IPv6Globalアドレスの付与に対する必要度はSHOULDではなく、MAYが妥当と考える。	再検討	必要度の再議論を今後の課題として対応したいと思います。

対象ページ	該当文言	意見	理由	対応	回答
13	3.2.1.1	SLAACはありえないと思います。	死活管理が目的である以上、ISP側がCPEの持つアドレスを学習する必要があるはずです。しかしSLAACではCPEが割り振ったアドレスをISP側が学習できません。 別プロトコルでCPEのアドレスなりinterface-idなりをISPへ通知するなら話が別ですが、それなら「SLAAC+何かしらのアドレス/interface-id通知プロトコル」と書くべきかと思います。	反映	備考としてアドレスを通知する仕組みが別途必要になる旨を追記しました(**p.13**)。
13	3.2.1.1 グローバルアドレスの付与方法(自動) 「下記のいずれかの方法を必須とする」	「下記のすべての方法を必須とする」に変更する。	SLAACとDHCPv6の片方だけだと製品として混乱するので、両方とも実装すべき。	再検討	必要度の再議論を今後の課題として対応したいと思います。
13	3.2.1.1 グローバルアドレスの付与方法(自動)	「推奨: デフォルトの挙動を自動判別設定とする」を追記する。	ユーザの負担とならないように、選択式ではなく自動判別とすべき。	今後検討	ISPサービスの自動判別機能は今後の課題とさせていただきます。
13	3.2.1.1の備考	「DHCPv6では/64固定であること」というのは、「現状、端末へ配布可能なプレフィックスは/64のみ」にすべきかと思います。	全般に事実認識が不正確です。 - DHCPv6でも、技術的には、/64以外のprefix長を学習可能です (RFC4861 4.6.2のPrefix長の定義やdraft-droms-dhc-dhcpv6-default-router-00を参照) ＊DHCPv6自体は、RAからprefix長を学習する仕様 ＊SLAACを使わなければ(=autonomous-bit OFF)、RAでもprefix長=64以外を広告可能 ※現実問題として/64を当て込んでいるDHCPv6実装があるかもしれませんが、それを「DHCPv6の技術の問題」と表現するのは不正確だと思います。 - 事の本質は、今日配布可能なIPv6アドレス空間(2000::/3やFC00::/7)ではprefix長が/64限定なこと(RFC3587や4291の3節)ではないでしょうか?	反映	ご指摘のように、表現が正しくありませんでいしたので修正しました(**p.13**)。
14	複数の上流がある環境は家庭用ルータとしては特殊であると考えられるため	マルチセッションPPPoEをサポートする場合には、マルチプレフィクスサポートを必須とするべき。また、デフォルトの挙動は決めておくべき。 推奨: デフォルトの挙動は全て再配布	マルチセッションPPPoEは多くのIPv4ブロードバンドルータに実装されているので、複数の上流がある場合は特殊と考えるのは間違っている。	今後議論	マルチプレフィックスに関しては今後の課題としていますので、マルチセッションに関しても今後の課題とさせていただきます。 なお、PPPoEのマルチセッションはIPv4では一般的だったがIPv6ではマルチプレフィックスを考えないといけないので「特殊」と書きました。
15	前提条件として、IPv6 の家庭用ルータにおいても、IPv4 の場合に取られていたセキュリティ機能(NAT/NAPTにより外部ネットワークから直接宅内ネットワークへの到達性が失われていた点も含む)は必要とする。	IPv6ルータにおいてWAN側-LAN側のNAT/NAPTは行わない記述であるが、IPv6-IPv6によるNAT設定も選択肢に加えるべき(必要度はMAY)と考える。	該当項目に記載されている宅内セキュリティ確保の方法はNAPTであるように見受けられ、原則指定されない場合はIPv6Globalアドレスを使用してWAN側-LAN側で通信を行う方式である。対して、現在一般的になっているBBR経由でのインターネット接続の場合、WAN-LAN間でNAT/NAPTを行い、LAN側で使用するIPアドレスはWAN側からはわからないまま通信することとなっている。このことにより、特定のポートに対する攻撃を未然に防ぐことができ、結果的に(ユーザが負担する)コストが低く、セキュアなインターネット接続を行えている。 IPv6ルータ使用時でもIPv6-IPv6NATを行うことにより、完全にIPv4環境と同等なセキュアな接続も行えるようにすべきである。 ただし、必要度に関しては元々のIPv6使用時のメリットとして、SIP使用時の通信等でALG/B2BUAを経由する必要がない等、エンドツーエンドの接続性が挙げられていたため、これを尊重しMAYとすることを提案する。	再検討	必要度の再議論を今後の課題として対応したいと思います。
15	外部から内部への通信はデフォルトで遮断するアクセス制限が行えること。	当該規定をMUSTとしていますが、SHOULD レベルとすべきと考えます。	ISP/ユーザのセキュリティポリシの問題であるため。	反映	機能の話なのでMUSTとしています。今回は、「デフォルトで」とした個所の削除で対応としました(**p.16**)。
15	4.1.1 外部からのアクセスを制限する	以下の要件を追加すること。 要件:フラグメント化されたUDPパケットについても、フラグメントに対応した上でアクセス制限を行うこと。 必要度:必須(MUST)	DNSの通信はUDPの1パケットで行われる場合が多く、今後はDNSSECの普及等で応答サイズが増大し、パケットのサイズが大きくなることが見込まれる。ガイドラインにはパケットのフラグメントに関する明示的な記述がないが、フラグメントが発生しても、正常な通信が行われることが必要であり、それを明記する事が望ましい。	課題 一部反映	フラグメントとフィルタリングに関しては今後の課題とさせていただきます。なお、フィルタリングの個所においてフラグメントパケットに対しては再構成を考慮する必要がある旨を追記しました(**p.17**)。 また、ベンダに任せる項目とすると、単純なルータはすべて通す動作が必要と判断しています。
16	4.1.2 表	「ICMP番号」は、正確には「ICMP TypeとCode」です(参照されているRFC4890でも指摘されている通り)	今の記述を読むと、ICMP Typeだけフィルタできるような実装を作る人が出てきてしまう可能性があります。	反映	ご指摘の捉え方がなされると良くないですので、TypeとCodeによる制御ができることとしました(**p.18**)。

対象ページ	該当文言	意見	理由	対応	回答
16	4.1.2 表	「次ヘッダ(プロトコル)を認識できること」と「次ヘッダチェーンを辿ること」がMUSTになっていますが、何回辿れることをMUSTにしますか?	- ハードウェア実装の場合は,無限回辿ることはまず無理です。 - ソフトウェア実装でも、ある程度の回数以上は辿らない実装が普通かと思います（ヘッダチェーンを延々と辿らせるの攻撃で)という基準がないと、CPEを作る人も実装しきれないのではないでしょうか? (残念ながらRFCには明確な基準がないため、運用経験から語るしかないかと思われます)	今後検討 一部反映	推奨値を出すのはかなり難しいと考えています。今後の課題として議論して、その結果を反映したいと思います。 また、今回は、備考に補足事項として追記しました(**p.18**)。
16	4.1.1.2 アクセス制限の詳細設定	トランスポート層の静的フィルタ設定にて、TCPとUDPのみ設定対象としているが、SCTP・DCCPも対象とすべき。	TCP・UDP以外のトランスポート層プロトコルについて、特にSCTPはマルチホーミング、メッセージ指向などの特徴を持ち、近い将来に各OSにて利用可能となることが考えられるため、設定対象とすべきである。 具体的には、外部からSCTPアソシエーションを開始するためのINIT、INIT-ACKに対する応答であるCOOKIE-ECHOを破棄することでWAN側からの制御を抑える程度の設定は行えるようにすべきである。	今後検討	他のトランスポート層プロトコルに関しては今後の課題として対応したいと思います。
16	4.1.1.3 アクセス制限の拡張機能 推奨(SHOULD)	必須(MUST)へ変更する。	SPIは事実上必須である。	再検討	必要度の再議論を今後の課題として対応したいと思います。
16	4.1.1.3 アクセス制限の拡張機能 推奨(SHOULD)	アクセス制限の拡張機能が推奨(SHOULD)に対して なんでMUSTじゃないんだろう、、、 PCをそこにつないでWindowsをinstallしてもいいぐらいの安心感がほしいです		再検討	必要度の再議論を今後の課題として対応したいと思います。
16	4.1.1.3 アクセス制限の拡張機能	SPIの実装は、RFC 4787のフィルタリング部分に従うようにすべき。 フィルタリングの特性: エンドポイント非依存フィルタリング(EIF)推奨、等	IPv4ブロードバンドルータと同等にするため。 加えて以下の条件があると、アプリケーションが不慮のフィルタリングを防ぐことが可能となるので、なお良い。 UDPの返答パケットの転送を保証する期間: 30秒以上, 必須	今後検討 一部反映	RFC4787を参考資料に追加しました(**p.17**)。なお、フィルタリングの推奨値などは今後の課題とさせていただきます。
16	要件：動的フィルタ（SPI）によりアクセスを制限できること。 ・ 内部から外部へは、デフォルトで通過させる。 ・ 内部から外部への通信があったコネクションを記憶し、このコネクションについては外部から内部へ通過させる。	使用可能な具体的なアプリケーションを記載する。 以下候補。 ・DNS ・FTP（パッシブモード、アクディブモード） ・HTTP/SMTP/POP3等、常にTCPコネクションが内部から外部に向けて張られるもの(これは一つ前の項で通信可能としているものですが)	元々、ユーザやISPがルータに期待する最小限の機能を規定するというのがガイドラインの趣旨とのことですが、FWの機能として「デフォルト遮断」を宣言した以上、具体的にどのようなアプリケーションが利用可能となっているか明記すべきと思います。	今後検討	使用可能なアプリケーションに関してはその一覧の整理を今後の課題とさせていただきます。
17	4.2	フィルタによる実装がどこまで必然的でしょうか?	- privacy address extensionと自宛フィルタは非常に相性が悪いと思います(CPE向けの話をされていますが、CPEのホスト機能としてprivacy address extensionを実装されても、文句はあまり言えないかと思います。Kaminsky Attack対策とか考えるとむしろ筋が良いかも。) =>「装置自身への通信をフィルタ実装MUST」と規定されても実装しきれないのではないでしょうか? ※「外から内への通信を、装置自身も含めて、フィルタするのがMUST」とか「特定サービスのフローを一律rate-limitするのがMUST」とかなら、まだ理解できますが。	反映	フィルタを設定可能であるとしている個所をアクセス制御ができることに変更しました(**p.18**)。
18	[14]も参照のこと。	draft-ietf-dnsext-dnsproxy-05の内容を追加／反映すること。	本Internet Draftはガイドライン P.18の本文中で旧版(-03)が参照先として触れられているが、その内容には本章に反映させるべきものが多く含まれる。単なる参照としてではなく、ガイドラインに追加、反映させる事が望ましい。	今後検討	今回は03に関しての内容となっていますが、次の版では05版に対応したいと思います。
19	5.2.2 優先するトランスポート	以下の二項目に分ける。 ・トランスポート変換機能 DNS要求をIPv4でしか出せない端末が存在する可能性がある。 必須 ・IPv6/v4両方のトランスポートがある場合に優先するトランスポート要件を分割すれば、トランスポートを合わせることをオプションにする必要はない。 オプション→推奨	この小節は複数の要件が混ざっているようなので、分割すべき。	再検討	表現方法の整理や必要度の再検討を今後の検討課題とさせていただきます。
20	要件	グローバルアドレスで待ち受ける場合は、DNSオープンリゾルバとならないようアクセス制限を必須とすること。	DNSオープンリゾルバはDNS AMP攻撃の踏み台となり得るため、明白な危険性については言及しておくべきである。 4.1.1でアクセス制限について述べられているが、ルータ自身が提供するサービス（DNSプロキシ等）もアクセス制限（デフォルト禁止）の対象であることを明示しておくのがよいと考える。	反映	ご指摘の点を踏まえ、オープンリゾルバは禁止という文言を追記しました(**p.21**)。

対象ページ	該当文言	意見	理由	対応	回答
22	5.5 キャッシュ、5.6 リゾルバ機能	新しいサブセクションとして「5.5.x ソースポートランダマイゼーション」を追加し、以下を記述する。 要件：キャッシュを行うDNSプロキシは、インターネット側の問い合わせUDPソースポートを都度異なるポート番号とする（ソースポートランダマイゼーションする）こと。 必要度：必須（MUST） 理由：カミンスキーアタック[18]によるキャッシュ汚染を低減するため。 同様に、「5.6.x ソースポートランダマイゼーション」を追加し、以下を記述する。 要件：リゾルバ機能を持つDNSプロキシが内側からのDNS問い合わせをNATする場合は、インターネット側のUDP問い合わせソースポートを都度異なるポート番号とする（ソースポートランダマイゼーションする）こと。 必要度：必須（MUST） 理由：カミンスキーアタック[18]によるキャッシュ汚染を低減するため。 備考：端末側がキャッシュ機能を持つ場合、NATする側がソースポートを同一にしてしまうと端末側でのキャッシュ汚染の危険性が高まる。	カミンスキーアタックにより、ソースポートが固定されるとキャッシュ汚染が容易に行われるため、明白な危険性については言及しておくべきである。	今後検討	DNSプロキシを実装した場合にカミンスキーアタックに対するケアが必要と明記しております。ただ、頂いたような詳細なコメントを反映するかは今後検討して次の版以降で対応したいと思います。
24	5.6.4 DNSSEC（参考）	要件中にあるDNSSEC関連のRRとして、記載されている4つ（RRSIG、DNSKEY、DS、NSEC）の他に、NSEC3、NSEC3PARAMを追加する。 DNSSEC関連RRおよびフラグを透過的もしくは適切に処理することは極めて重要であるため、必要度を以下とする。 必要度：推奨（SHOULD） 備考の「現状～高くないと考えられる。」の部分は、以下で置き換える。 必要度が推奨（SHOULD）の理由は、他国（スウェーデン）においてDNSSECに対応していない家庭用ブロードバンドルータにより問題が発生した経緯があるため。この問題を ICANNの諮問機関であるSSACが認識し、Nominet UKと協力の上、ブロードバンドルータ実装の調査を行ったところ、IPv6やDNSSECで規定されている新しいDNSプロトコルへの 準拠状況においてさまざまな問題点が確認された[参考文献]。 参考文献: <http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf>	DNSセキュリティの向上を目的とするDNSSECは、プロトコルの策定が完了し、昨今のDNSに関連するセキュリティ問題への対応策として、TLDを中心に導入が行われ始めるなど、世界的な普及段階に入りつつある。その状況においてプロトコルに準拠していないネットワーク機器が存在するのは、インターネットセキュリティの向上を阻害する要因となりかねない。ただし、現在は普及の初期段階であるため必要度は推奨（SHOULD）とした。	今後検討 一部反映	ご指摘いただいたRRのもれは追記しました（**p.25**）。 なお、ご指摘の項目の追加に関しては今後の課題として議論を行い、反映したいと考えています。
25	6 宅内ネットワークへの情報配布機能	DHCPv6サーバのStateful設定とStateles設定に関する記述がない. それぞれの場合における，RAのMビット/Oビットの設定も合わせて明確に記述してほしい.	ルータに接続される端末機器との接続性を高めるため	今後検討	RAのOフラグ/Mフラグに関しては、現状の仕様から外されており、検討段階になっていることから、今後の課題として検討後反映したいと考えています。
28	6.2.2 備考	draft-ietf-ntp-dhcpv6-ntp-opt-03.txtは削除してほしいです	このdraftはNTPサーバアドレスだけではなく、その他の情報（FQDN,NTP用のマルチキャストアドレス）も流せるようにする拡張です。サーバアドレス広告という観点ではちょっとずれていると思います	反映	NTPサーバアドレスに関しては、ご指摘のように観点が異なるものが含まれ、また、RFCとなっていない理由から削除することにしました（**p.28**）。
29	6.2.2 図	端末が学習するサーバアドレスからprefix長を消してほしい	DHCPv6 optionでは、サーバアドレスは広告できますが、サーバのprefix長までは広告できません。	反映	ご指摘の誤りを修正しました（**p.29**）。

対象ページ	該当文言	意見	理由	対応	回答
29	6.2.3 備考	per-I/Fでの排他制御を想定していますか? per-装置での排他制御を想定していますか?	文章からはどちらなのか読み取れませんでした。(理論上は前者ですが、実用性からは後者でも十分な気もしなくはないです) CPE実装者の方は「どちらなのかを明確にしてもらわないと実装できない」と思われるのではないでしょうか?	反映	Per-装置で考えておりましたので、その旨が明確になるように変更しました(**p.29**)。
31	7.1の後半の前提	Numbered-Linkを定義するか、別の単語で説明してください(非リンクローカルアドレスを割り振ったリンク、ということ?)	文書全体を通じて、ここにしか出てこない単語です。初出の概念なので、読者が理解できません。	反映	ご指摘の通りここにしか登場しない単語でありましたので、Unnumbered-Linkの表現を用いない表現に変更しました(**p.30**)。
31	7.1の後半の前提	要件のところに「point-to-pointのリンクで」と書いてありますが、これは要件ではなく前提に書くべき事項ではないのでしょうか?	point-to-pointではない回線では、これがなくてもping-pongしません(最初にNDP解決に失敗しておしまいなので)	反映	ご指摘の通り前提項目に記載することに変更しました(**p.30**)。
32	7.2.1	「next-hopアドレスをリンクローカルアドレスでも指定できること」はMUSTにすべきかと思います	これができないと、static経路でICMPv6 Redirectが動作しません。IPv4ルータのつもりで安直にIPv6 CPE実装すると忘れがちな部分ですので、明記した方がよいかと思います。	反映	ご指摘の点を備考に追記しました(**p.31**)。
32	7.2.1	RAでのdefault route学習をMUSTにしていますが、 - 1I/Fだけで有効にすることを想定していますか? - 複数のI/Fで有効にすることも想定していますか?	RFC4862的には後者ですが、後者だと「どっちのdefaultrouteを優先するのか」をCPE側で解決する必要があり、それなりにハードルが高いはずです。 後者をMUSTと言って強制するのも、CPEの用途を考えるとちょっとしのびない気がしますが。。。	課題 一部反映	備考への追記を行い(**p.32**)、デフォルトルートの優先順位に関しては今後の課題とさせていただきます。
33	7.2.2 LAN側への経路制御	推奨に格上げする	IIJの現行サービスでRIPngが必須であるため。	非対応	こちらは、確認したところ現行サービスで必須のものはありませんでした。本ガイドラインにおいてはRIPngはLAN側に対する要求事項として記載しております。
35	7.3.2	この章は削除すべきだと思います。	PIM-SM/SSMの仕様の中には、optionalな機能/MUSTな機能がいろいろ混在しています。一口に「PIM-SM/SSMを実装」と言っても、その辺の実装具合によっては相互接続不能です。 と思うと、今のレベルの中途半端な記述があってもCPE側は結局何も実装できないように思えます。だとすると、そもそも「CPEの実装ガイドライン」になっていないのではないでしょうか? ※そもそも、エンドユーザがISPのPIM domainに参加できること自体が、ISP見地から見ると大きなリスクなので(e.g.RPを乗っ取る攻撃が可能)、エンドユーザにPIMで接続させるというサービス自体あまり考えられないような気もしますが。。。(Broadband Forum TR-101でも、ISP-CPE間のプロトコルはIGMP/MLDを想定しているように読めます)	課題 一部反映	PIMの実装に関しては、相互接続の考慮が必要と追加しました(**p.34**)。また、サービスに踏み込んでいないことも合わせて明記しました(**p.34上部**)。 なお、機能の詳細に関しては、今後の課題とさせていただきます。
35	7.3.4の本文	「無線LAN機能を持つ場合」の言及は不要ではないでしょうか?	端末1が無線LAN上でマルチキャスト1に参加した場合、仮に無線ルータ側でsnooping相当の処理をしたとしても、同じ無線LAN上の端末2は結局端末1向けの電波を聞いてしまうかと思います。なのでsnoopingをやっても余り意味がないのではないでしょうか? 無線ルータがスイッチング機能を持っていて有線・無線にまたがったVLANを持っているなら話は別ですが、そうだとしても「スイッチング機能があるならsnoopingはほしい」という結論にしかならないはずです。	反映	無線LANに対して不必要なマルチキャストのトラフィックを流さないように、無線LAN側への制限と考えて記載しておりました。 無線LANに不必要なトラフィックが流れないようにするという意図が伝わるような文章に変更しました(**p.35**)。
39	8.1 設定方式 概要: サービス提供者から家庭用ルータに対して必要な設定の投入を行うための機能を、家庭用ルータが具備すること 必要度: 必須(MUST)	ユーザが接続サービスを変更した場合に、以前のサービス提供者からの設定投入を禁止する機能を、家庭用ルータが具備するべき(MUST)である。	特に TR-069 や手動設定などインターネットを介して設定が可能な方式の場合、契約していないサービス提供者から設定の変更が可能であってはならない	今後検討	ISPにおけるサービスに依存した課題は、今後の課題とさせていただきます。
39	8.1 設定方式 概要: サービス提供者から家庭用ルータに対して必要な設定の投入を行うための機能を、家庭用ルータが具備すること 必要度: 必須(MUST)	この機能を推奨(SHOULD)とするか、あるいは前提としてサービス提供者が配布する家庭用ルータに限定するべきである	具体的な設定方式が例示のみであり、いずれか一つでも具備していれば要件をみたすものと考えられる。しかし、機能自体は具備していても接続サービス提供者との間で方式があわなければ有効とならないため、MUST である意味がない。	今後検討	ISPにおけるサービスに依存した課題は、今後の課題とさせていただきます。
39	8.1 設定方式	必須にするなら方式名を指定すべき。指定できないのであれば、必要度を推奨に落とすのが良い。	実装がばらついてしまい、ISPを変更したらルータが使用できなくなる等で、ユーザが混乱するので。	今後検討	ISPにおけるサービスに依存した課題は、今後の課題とさせていただきます。
42	8.2.2	この要件ですが、「ただし、ユーザ側の意思でdisableできること」というのがセットでないとまずいかと思います。	そのようなサービスを「セキュリティホール」と思うユーザさんもいらっしゃると思います。そうしたユーザさんに対してサービスをOFFにできないとなると、「IPv6ルータは穴だらけ」と誤解されかねないと思います。	反映	サービスに依存する個所であることを明記し、ユーザ側の意思で無効化も必要である点を追記しました(**p.40**)。

対象ページ	該当文言	意見	理由	対応	回答
42	8.2.2 セキュリティ関連設定	第一要件全体について、リンクローカルでのアクセスに限る等、具体的な例を提示してあると良い。	WAN側からのアクセス制御設定機構はセキュリティホールに繋がる可能性があるので。	反映	サービスに依存する個所であることを明記し、ユーザ側の意思で無効化も必要である点を追記しました（**p.40**）。
42	8.2.3.1 DNSプロキシ機能のためのDNSサーバアドレス 要件: DHCPv6にて取得したDNSサーバ情報を使用できること 必要度: 必須(MUST)	前提として DHCPv6 クライアント機能を有する場合とするか、推奨(SHOULD)とすべき	8.1 設定方式において、DHCPv6 クライアント機能以外の設定方式のみを持っている場合は、本機能については持つことができない	反映	本項目にてDHCPv6に限定するわけではありませんでしたので、DHCPv6などの手段で取得したと項目内容を変更しました（**p.40**）。
43	8.2.4.3 理由	厳密には「DHCPv6サーバの自動検出のためにはIPv6マルチキャストルーティングが必須だが、必ずしも提供されていないため」という説明になるかと思います。	RFC3315 5.1節をご参照ください。	反映	手法がないためという表現を改め、手法が必ずしも提供されていないために変更しました。またマルチキャストルーティングができれば自動設定が可能である点を備考に記しました（**p.41**）。
（記載がないことの対する指摘）	（記載がないことに対する指摘）	Subnet Router Anycastに関しては何かしらの形(フィルタなり機能無効化なり)でdisableしておくことが望ましい、とか書きませんか?	RFC4291 2.6.1節では、サポート必須(MUST)になっている機能です(IPv6 Ready Logoプログラムでも試験されています)。一方、Subnet Router Anycastの具体的な用途がないのも現実かと思います (RFC4942 2.1.6節でも、「外部からのSubnetRouter Anycastへのアクセスを止めたくなることもあるだろうが、その場合はフィルタして」と書いてある位)。 上記標準化動向に対して、運用見地からCPEではどう実装しておくべきとお考えでしょうか?(直観的には「defaultで有効にしておくことが望ましい機能」とは余り思えませんが、何も言わないと、IPv6 ReadyLogoプログラムの関係上、CPEにてSubnet Router Anycastはdefaultで有効になるかと思います) ※IPv6 Ready Logo委員会の方とも本件は議論しましたが、「立場上、RFCにMUSTと書いてあれば、どんな機能でもMUSTとせざるをえない」というのが同委員会の見解でした。 今更RFCやLogo規格を変えるわけにもいかないので、何か言うとしたら本ガイドラインで軽くコメントする位のことしかできないかなと思っています。	課題	サブネット・ルータ・エニーキャストに関しては今後の課題とさせていただきます。
（記載がないことの対する指摘）	（記載がないことに対する指摘）	IETFのCPE Router Recommendationを参照すべきかと思います(draft-ietf-v6ops-cpe-router-00)	まだ標準化途中ですが、議論漏れのチェック用には非常に役に立つかと思います。(裏では参照されているのかもしれませんが、9.4節には記載なし)	課題	今度の動向は注視していきたいと思います。また、関連動向を次の版において記載することとさせていただきます。
（記載がないことの対する指摘）	（記載がないことに対する指摘）	マルチセッションPPPoEへの考慮が欠けている。マルチセッションPPPoEをサポートする場合は、マルチプレフィックスのサポートは必須となるだろう。	多くのIPv4ブロードバンドルータがマルチセッションPPPoEをサポートしているので。	課題	マルチプレフィックスに関しては今後の課題としていますので、マルチセッションに関しても今後の課題とさせていただきます。
（記載がないことの対する指摘）	（記載がないことに対する指摘）	設定画面(UI)の用語を統一出来ると良い。	IPv4ブロードバンドルータで、同じ機能なのに複数の用語があり、ユーザが混乱しているため、IPv6では統一して欲しいので。 例）静的ポートフォワーディング ・別名もしくは似た機能の名称 ヴァーチャルサーバ DMZ	今後検討	ご指摘の点は必要性が高いと考えています。今後の課題とするか検討させていただきます。