IPv6 の新しいアドレス利用形態に関する報告書

IPv6 アドレスポリシー企画策定専門家チーム

1. 報告書の概要

「IPv6 アドレスポリシー企画策定専門家チーム」は、インターネットの今までにない新しい使い方をアドレスポリシーの観点からプロモートしていくことを目的とし、情報家電ベンダ、自動車メーカ関係者、IPv6 アドレスポリシー有識者、IPv6 技術者を招聘し設立された。IPv6 アドレスの利用形態として、製品のシリアル番号等識別子や自動車・交通システムでの利用、あらかじめ製品にアドレスを埋め込んでの利用を想定し、技術的課題とともに実現可能性を検討した。

検討結果として、

1. 新規のアドレス利用要望に対しては、現行の IPv6 アドレスポリシーの範囲で取得可能である場合が多く、製品埋め込み等を可能にするようなポリシーの提案は、現状可能な取得に対して影響することが考えられるため、ポリシーとしての明文化については慎重に状況を見極める必要がある
2. IPv6 を利用したビジネスの促進、及びインターネットのさらなる拡大を図るため、JPNIC として、従来の ISP 対象に限定しない、広範囲の IPv6 アドレス取得を可能にするような施策が必要。具体的には、IPv6 アドレス取得のために指定事業者になれるような仕組みを構築するべき

という結論が得られた。

1 に関しては、IPv6 普及・高度化推進協議会のリモコンノード SWG 主査との情報交換より、SWG が実施した APNIC とのミーティングにて APNIC ではかなり柔軟に IPv6 アドレス割り振りを捉えている模様である。JPNIC でも協議会と協調し、新サービス市場の動向把握とその立ち上げを支える活動を強化し、最も APNIC と近い日本を代表する組織として適切に APNIC のアドレス・マネージメントへフィードバックさせていくことが望まれる。2 についても今後 JPNIC にて実現検討を実施することを本専門家チームからの提言としたい。

2. はじめに

2.1. IPv6 における新たなアドレス利用形態検討の意義

IPv6 アドレスは、膨大なアドレス数を持つというその性質上、ISP を経由しないアドレス割り振りのニーズがあると考えられる。JPNIC IP 事業部で 2003 年初頭より、家電業界をはじめとする数社に対し、アドレスの割り振り、割り当てについて、どのようなニーズがあるのかのヒアリングを行った結果、各業界では実現時期の緊急性はないものの、IPv6 アドレスをシリアル番号等の製品識別子に利用したい、利用の際には製品にあらかじめアドレス（識別子）を付与しておきたい、といったニーズが強いことが確認できた。

また、2003 年 8 月には、センサー等の機器に対して IPv6 アドレスを割り当てるニーズがあることが IPv6 普及・推進協議会から報告されており、ISP を経由しないアドレスの取得が現実かつ緊急の課題として提起されている。

しかしながら現状のアドレスポリシーの範囲では、シリアル番号等の製品識別子等への利用といったニーズに対してアドレスを割り振ることは難しい状況であると考えられ、また、上記ニーズを満たすための割り振り、運用が技術的に実現できるかの検討も行う必要がある。ISP を経由しないアドレス割り振りを実現することができれば、従来の、PC 主導となっているインターネットの枠を超えた新たなネットワークの広がりを期待することができ、これにより、IPv6 の普及推進を図ることができる。

このような背景のもと、専門家チームを設立し、ISP を経由しないアドレス割り振りの技術的実現性の検討、ニーズの確認、調査、IPv6 アドレスポリシー改訂の要否検討を集中的に行うこととなった。本専門家チームは、IPv6 アドレス利用者の立場からのベンダ・メーカ、IPv6 アドレスポリシー有識者、IPv6 技術者のそれぞれを募り、現実に即した検討を実施した。専門家チームの構成メンバは以下である。

- 荒野 高志／株式会社インテック・ネットコア
- 伊藤 公祐／キヤノン株式会社
- 猪俣 彰浩／富士通株式会社
- 鈴木 史章／松下電器産業株式会社
- 丸田 徹 ／KDDI 株式会社
- 山本 信／トヨタ自動車株式会社
- 藤崎智宏／日本電信電話株式会社

また、メーリングリストでの議論の他、計 4 回の全体ミーティングを開催し、12 月の JPNIC Open Policy Meeting にて活動状況の報告を実施した。

2.2. 本検討の対象領域

本検討では、ベンダが製品にシリアル番号のような識別子として、IPv6 アドレスを出荷前に埋め込むといったアドレス利用方法を対象とする（このような割り振りを、「ISP を経由しないアドレス割り振り」と呼ぶ）。この際、IPv6 アドレスを割り振る対象を、インターネットへの接続の可能性を考え、以下のように分類した。

a) インターネットへ常時接続
b) インターネットへ間欠的に接続
c) 将来的にインターネットに接続する可能性がある
d) インターネットには接続しないが、他の IP ネットワークに接続する
e) インターネットにも他の IP ネットワークにも接続しない

ISP を経由しないアドレス割り振りでは、上記の分類の a)～d)において広域で一意なアドレスが必要と考えられるため、その検討の対象とする。また、アドレスの利用を考えた場合、その対象領域で、

- 必要なアドレスサイズ

- アドレス空間が連続していることの必要性
- 必要な一意性の度合い
- 広域で経路制御可能かどうか

といった項目についても検討する必要がある。

2.3. 報告書の構成

本報告書の構成を以下に述べる。

まず第 1 章にて、検討内容と検討の結果について概説する。第 2 章で、ISP を経由しない IPv6 アドレス割り振りに関する検討の意義と、検討対象領域について述べる。第 3 章では、新しいアドレス割り振り要求について、家電業界へのアンケート結果、自動車業界、携帯電話業界における“識別子”の利用という観点から概観する。第 4 章にて、“識別子”としての IPv6 アドレスと、インターネットにおける接続性という観点から技術的な実現手段について考察し、第 5 章にて、IPv6 アドレスを“識別子”として利用することに関連する、IPv6 普及高度化推進協議会や、IETF の標準化等の活動について述べる。第 6 章にて、ISP を経由しない、製品“識別子”としてのアドレス配布に関して、「アドレスポリシー」の観点からの考慮点を述べ、第 7 章にて本検討の結論を述べる。

3. 新しい IPv6 アドレスに対する要求

3.1. IPv6 アドレスを製品番号のような識別子に使う意味

従来、IPv6 アドレスの割り振り・割り当てポリシーは、APNIC などの RIR からアドレスの割り振りを受けた LIR/ISP が、その利用者に対して空間を割り当てることを想定して設定されている。

具体的に説明する。IPv6 アドレスの割り振り・割り当ては、APNIC、ARIN、RIPE NCC が共同で議論、策定したポリシー: “IPv6 Address Allocation and Assignment Policy”[1] に従って行われている。IPv6 アドレスの初期割り振りを受ける組織は、以下の 4 つの基準を満たすことが規定されている。

a) LIR であること
b) エンドサイトでないこと
c) /48 を割り当てた組織に対し、IPv6 の接続性を提供する計画があること。その際、経路広告は割り振られたアドレス一つに集成すること
d) 2 年以内に最低でも 200 の/48 の割り当てを行う計画があること

このポリシーは、ISP が RIR から直接 IPv6 アドレス空間の割り振りを受けるか、または ISP が RIR から IP アドレス割り振りを受けた LIR(=ISP)から間接的に IPv6 アドレス空間の割り振りを受ける一方、ISP はその利用者(=エンドサイト)に対して IPv6 アドレス空間を

[1] http://ftp.apnic.net/apnic/docs/ipv6-address-policy から入手可能

割り当てることを想定して設定されていた。

一方、IPv6 普及・高度化推進協議会のリモコンノード SWG の活動などを通じて、機器に対して、機器固有の IPv6 アドレスを固定的に付与し、それを ID として利用することのニーズが存在することがわかってきた。そこで、これらニーズとアドレス割り振り・割り当てポリシーへの反映について、関連業界(主に電機業界)に対し調査を実施した。

3.2. 調査結果

3.2.1. 家電業界における ID 利用

JPNIC では 2002 年度の TAO からの受託案件で、「世界標準として受け入れられる IPv6 アドレスポリシー」と題した調査報告を行った。この中では、現行の IPv6 アドレスポリシーの成り立ちの経緯、現状の割り振り状況、現在の IPv6 ポリシーの課題等についてとりあげ、中でも、IPv6 ポリシーの課題として、「家電への割り当て」に対するポリシーが未整備であることに触れている。そこで、2003 年 3 月から 6 月にかけ、IPv6 アドレスの利用に関するヒアリングを行った。

ヒアリングの結果、概要以下のような意見が得られた。

- IPv6 を使って何をしたいかという明確なニーズはまだないが、機器の ID 管理の負荷を軽減するひとつの方策として、IPv6 アドレス(128bit)を機器に焼き付けて出荷し、IPv6 アドレスを機器 ID として利用したいというニーズが一部のメーカにある
- IPv6 ネットワークへの移行状況の面などでまだ先が見えない部分があり、現段階での IPv6 利用の推進は難しい。
- IPv6 アドレスを機器 ID として共用する場合、固定の ID としつつルーティング可能とするためのモバイル IP のような仕組みが必要である。しかしコスト等を勘案し、モバイル IP 等の技術を使うことが本当に現実的かについては議論が必要と考えている
- 現段階では、メーカ側でポリシーに関しての具体的な要望は特にない

3.2.2. 自動車における固定 IPv6 アドレス付与

自動車はテレマティクスサービスの普及が進んでいるが、この中で IPv6 の果たしうる役割や、ISP に依存しない IPv6 アドレスの付与及び IPv6 アドレスを ID として利用できる可能性について、自動車業界での捉え方を調査した。その結果、以下のような現状認識にあることが判明した。

◆ 自動車への付与

将来、ネットワーク等を活用して、自動車に「安全」、「渋滞緩和」、「安心」、「快適」なサービスを提供する場合、自動車の移動性を考えると複数のプロバイダ、複数のネットワーク媒体を利用する事が想定される。その際、接続性、瞬時の切替え等の品質を保証する為には、ISP に依存しない IPv6 アドレスの付与の必要性が考えられる。

◆ 車内センサー等への付与

1) 車内 LAN の現状：従来クルマメーカ毎に別々の車内 LAN の方式を採用していたが、スモールカーの台頭や故障診断システムによる自動車監視の義務付けなどの規制への対応の必要から、仕様統一によるコスト・スペースの節約の方向にあり、ここ数年 CAN(Controller Area Network) 等への規格統一が検討されている
2) CAN は最大 1Mbps 程度の通信速度をもつレイヤ 1、2 の規格であるが、レイヤ 3 には言及していない。また、一般に CAN のレイヤ 3 には IP と異なる通信規格が用いられている
3) 自動車内で IP を用いている部分は通信ナビゲーションシステムが外部と通信する通信インタフェース部分のみである
4) 将来のクルマの高付加価値化を考えると、現状の CAN では速度的に十分ではなく（最大速度=1Mbps 程度)、5〜10 年の中長期レンジでは、高速化やタイムトリガ型による信頼性向上なども考慮した新しい車内 LAN 方式に置き換える事が考えられる
5) 車内 LAN に求められる要件は、「高速」「確実」「安価」であるが、現段階で TCP/IP がその要件を満たすことができるとはいいきれない

しかしながら、車内にはプローブと呼ばれるセンサーが 100 近く搭載されており、それらを車外からモニターすることによる様々なアプリケーションが期待されている。したがって、中長期的に車内 LAN が IP に対応してくる場合、各々のセンサー等に ID を付与することのニーズが出てくることは想像に難くない。

3.2.3. 携帯電話における ID 利用

現在の携帯電話には一般にブラウザフォンなどのパケット通信機能が具備されていることから、IP アドレスを出荷時から付与するニーズや、IP アドレスを ID として利用するニーズがあることが想定される。よって、携帯電話の ID 管理手法の現状や、IPv6 を利用する場合に想定されるアドレス利用に関し、CDMA 方式について調査した。

CDMA 方式の携帯電話では、以下の ID を利用している。

(1) IMSI(International Mobile Station Identity)
CDMA の加入を識別する 15 桁の番号。MCC+MNC+MSIN という番号形態
- MCC: Mobile Country Code。3 桁固定であり、日本は 440、441 を使用。
- MNC: Mobile Network Code。2-3 桁であり、日本は 2 桁利用。
- MSIN: Mobile Station Identification Number。1-10 桁の加入者番号。

なお、IMSI は基本的にリサイクルされる

(2) MDN(Mobile Directory Number)
携帯電話に付与される電話番号。

(3) ESN(Electronic Serial Number)
CDMA 携帯電話を識別する番号であり、32bit(製造事業者識別コード 8bit＋シリアル 24bit)の番号空間を持つ。ESN は MAC アドレスと同様、メーカで設定を行う。

このように、携帯電話では複数の ID を持っており、端末を識別し、課金 ID としても用いられる IMSI、通話を接続するための論理的な ID である MDN、端末個体の識別子である ESN など、複数の ID がそれぞれの用途で用いられている。

また、携帯電話で IP 通信を行う場合、現在は RADIUS を用いて端末に動的な IPv4 アドレスを付与している。CDMA ベースの携帯電話に IPv6 アドレスを付与する方法は、第三世代携帯電話の標準化団体「3GPP2(3rd Generation Partnership Project 2)」で検討されている。ここで推奨されている IPv6 アドレスの付与方法は、端末に対して IPv6CP(IPv6 Control Protocol; RFC2472) により接続し、Stateless Address Autoconfiguration (RFC2462)に基づき/64 のプレフィックスを付与するよう規定されている。

これらのことから、出荷段階から携帯電話に IP アドレスを付与するという考え方は標準にはないことが判明した。したがって、IPv6 に対応した携帯電話の実装が存在しないことから断言は難しいが、IPv6 アドレスを機器 ID として携帯電話に付与することは、標準準拠の範囲では考えにくいといえる。

3.3. 具体的な利用イメージ　～自動車の場合～

本節では、具体的な利用イメージとして、自動車において ISP に依存しない IP アドレスの付与の必要性について詳説する。

3.3.1. 背景

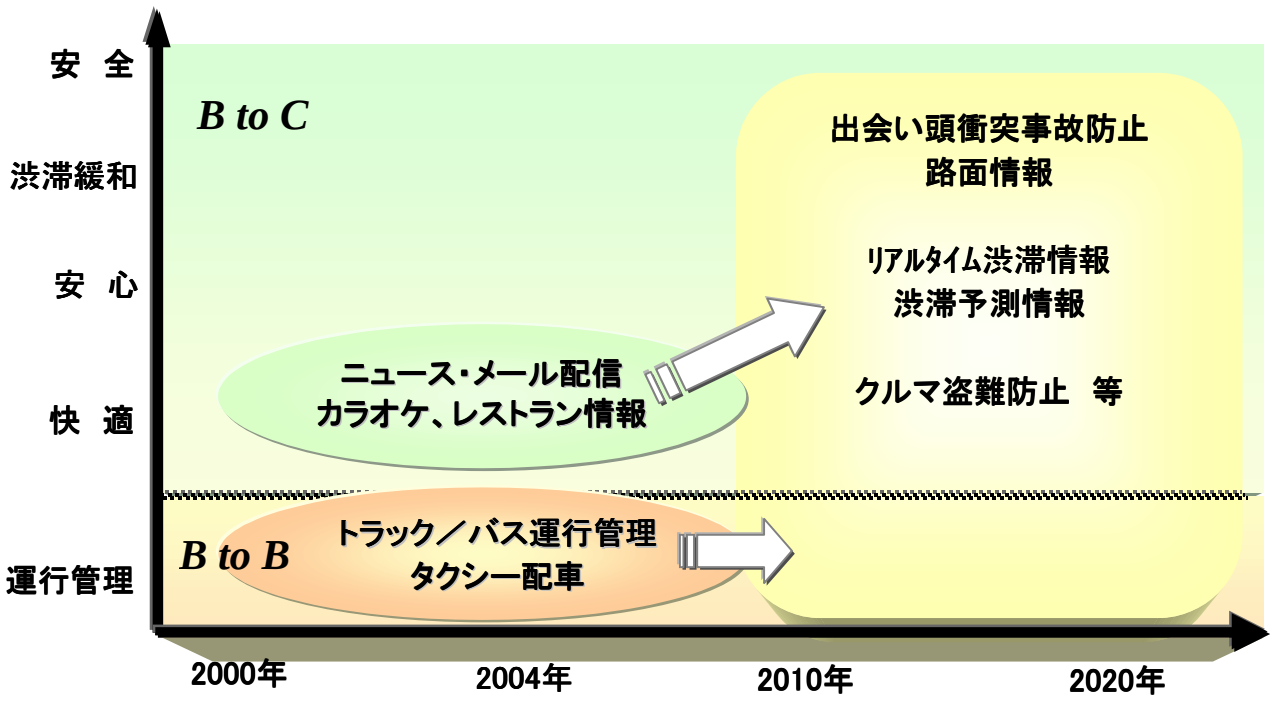
数年前より、自動車メーカ、ナビメーカを中心に、クルマ向け通信・ネットワークサービスが始まっている。現状は、メール/ニュース配信、カラオケ、レストラン情報等、「快適」というカテゴリーに属するサービスが主である。

また、ネットワークは携帯電話網（パケット通信）を利用しており、その特性から、

① 通信料金が高い
② 実効的な伝送速度が 100kbps 程度
③ 通信接続までに数秒程度の時間がかかる

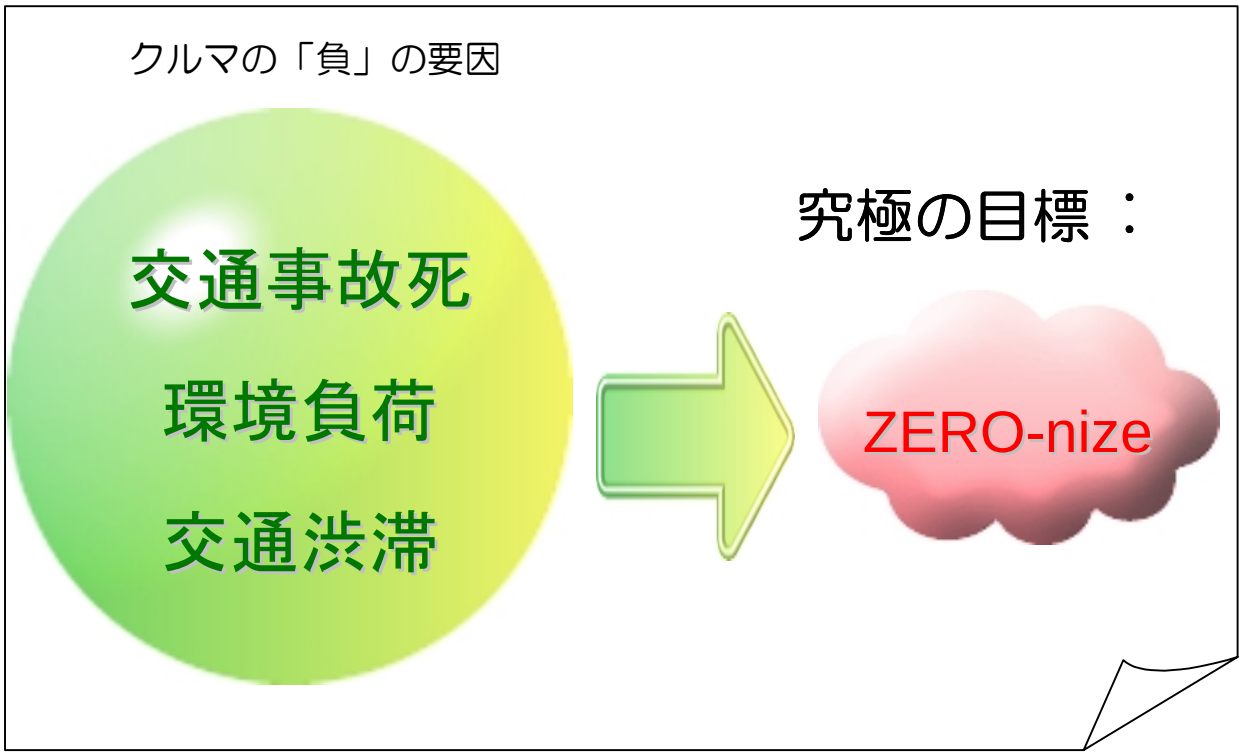
等、アプリ、コンテンツのレスポンスに時間を要す、サービスコストが高い等の課題があり、ユーザの真の利便性に答えきれていないのが実情である。

将来、インフラ・ネットワークを活用して、より「快適」や「安心」（クルマの状態管理や盗難防止/追跡）サービスの実現と共に、ITS（高度道路交通システム：Intelligent Transport Systems ）で目指す「安全」「渋滞緩和」なクルマ社会を目指すサービスを実現する為、ITS-Japan 等、官民学連携にて具体的検討が既に始まっている。



3.3.2. クルマ社会の究極の目標

クルマは、ヒト・モノの移動の道具として普及し、大きな利便性をもたらしたが、その反面、交通事故による死傷者の問題、渋滞による時間損失・環境への負荷という、負の要因も合せ持っている。



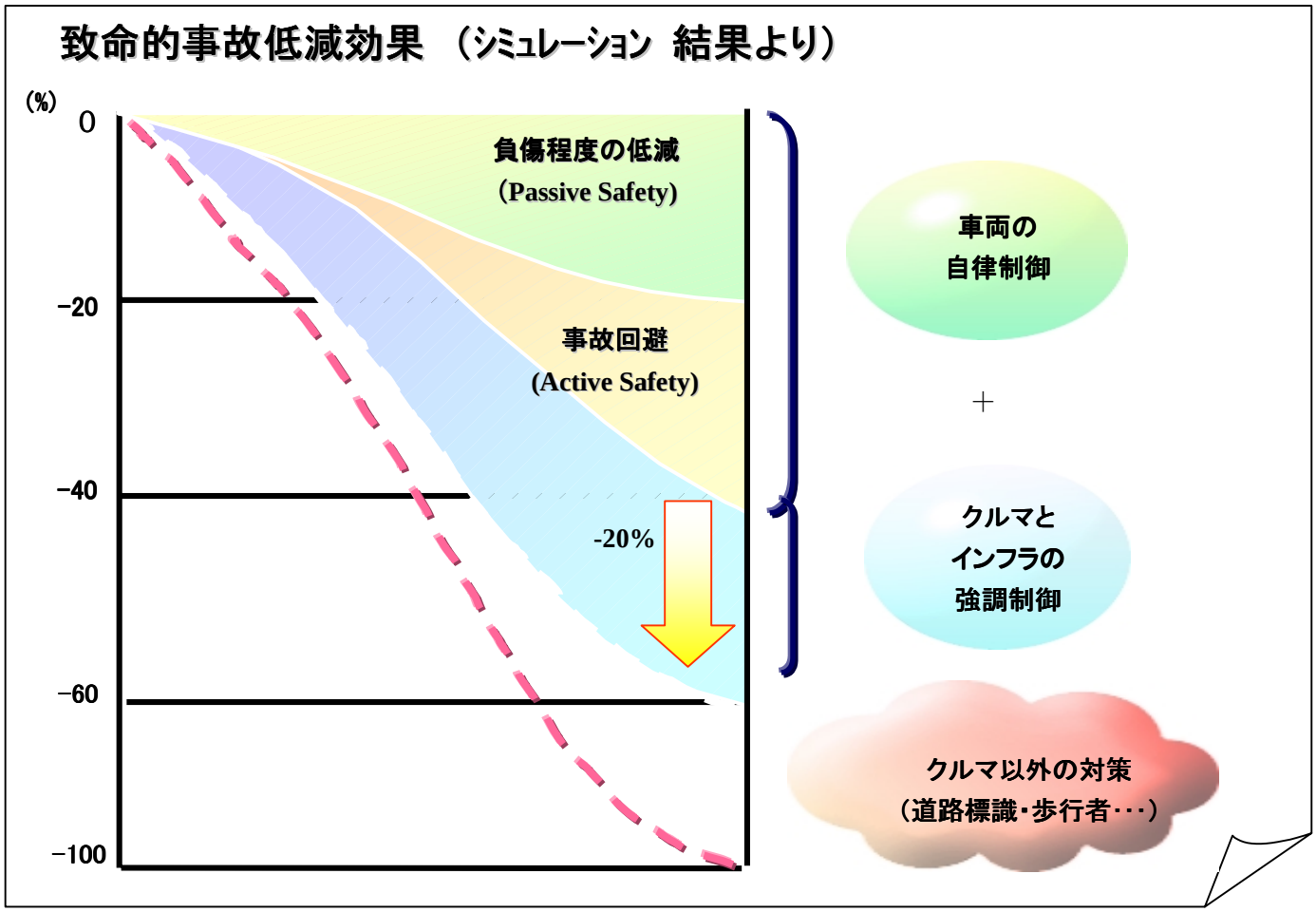
クルマ社会においては、「交通事故ゼロ」、「環境負荷ゼロ」、「交通渋滞ゼロ」が究極の目標となっている。

3.3.3. 致命的事故低減に向けたインフラ・ネットワークの活用

現在日本では、年間約 90 万件の事故があり、そのうち約 8 千人の方が亡くなっている。致命的事故低減に向けては、まずクルマ単体で検知、判断、制御を行う、自律系制御があり、次の２つに大別される。

① Passive Safety
クルマが事故を起こしても、ドライバー、同乗者の負傷の度合いを軽減する機能・技術（例. エアバッグ）

② Active Safety
クルマが事故を起こさないように、ドライバーに危険を予め通知、またはドライバーの操作を支援する機能・技術（例. ABS, VSC、プリクラッシュセーフティ）



これら①と②のような、車両自律系制御により交通事故の 40%は低減できると見られている。これらの他に、例えば「見通しのきかない交差点」、「見通しのきかないカーブの先にある路面凍結」における事故回避においては、クルマ、ヒト、自転車、バイク等がお互い

の存在や路面の状況等を把握する為に、インフラ・ネットワーク・センサー等の活用が有効と考えられる。このようなクルマとインフラとの通信による協調制御を行うことで、交通事故は更に、20%削減することが期待される。

環境負荷の現状と課題

（当社試算）

年度	世界の人口（億人）	クルマを利用している割合（％）				車両台数（億台）	影響 *注1）
		0	20	40	60		
2000	61					7.4	1.0
2050	89					32.4	4.4

影響度: ４～５倍

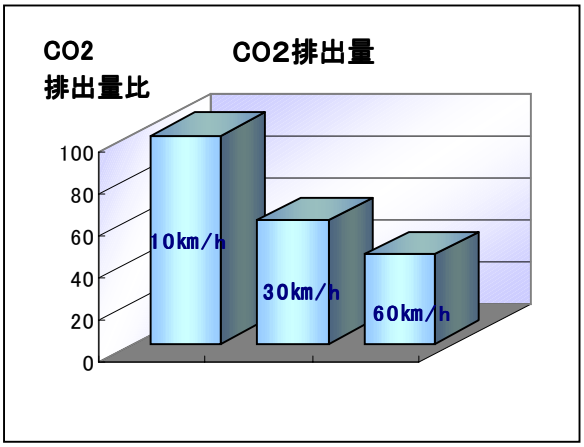
削減目標値　1/4 ～1/5

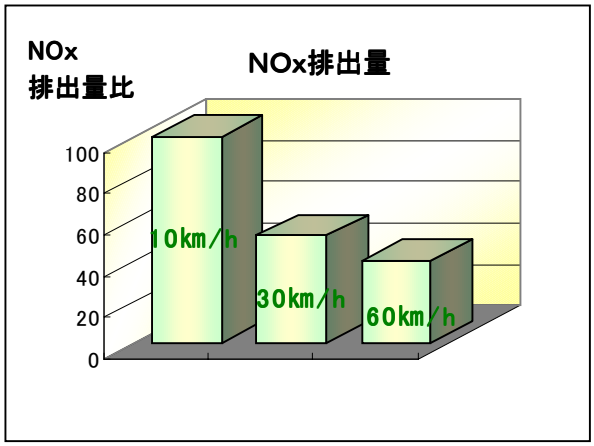
注1）2000年を基準にした場合の比率

交通渋滞の環境との関係

- 平均車速の改善により、CO2・NOxの排出量削減が可能

＜走行スピードとCO2・NOx排出量の関係（10km/hを100とした場合）





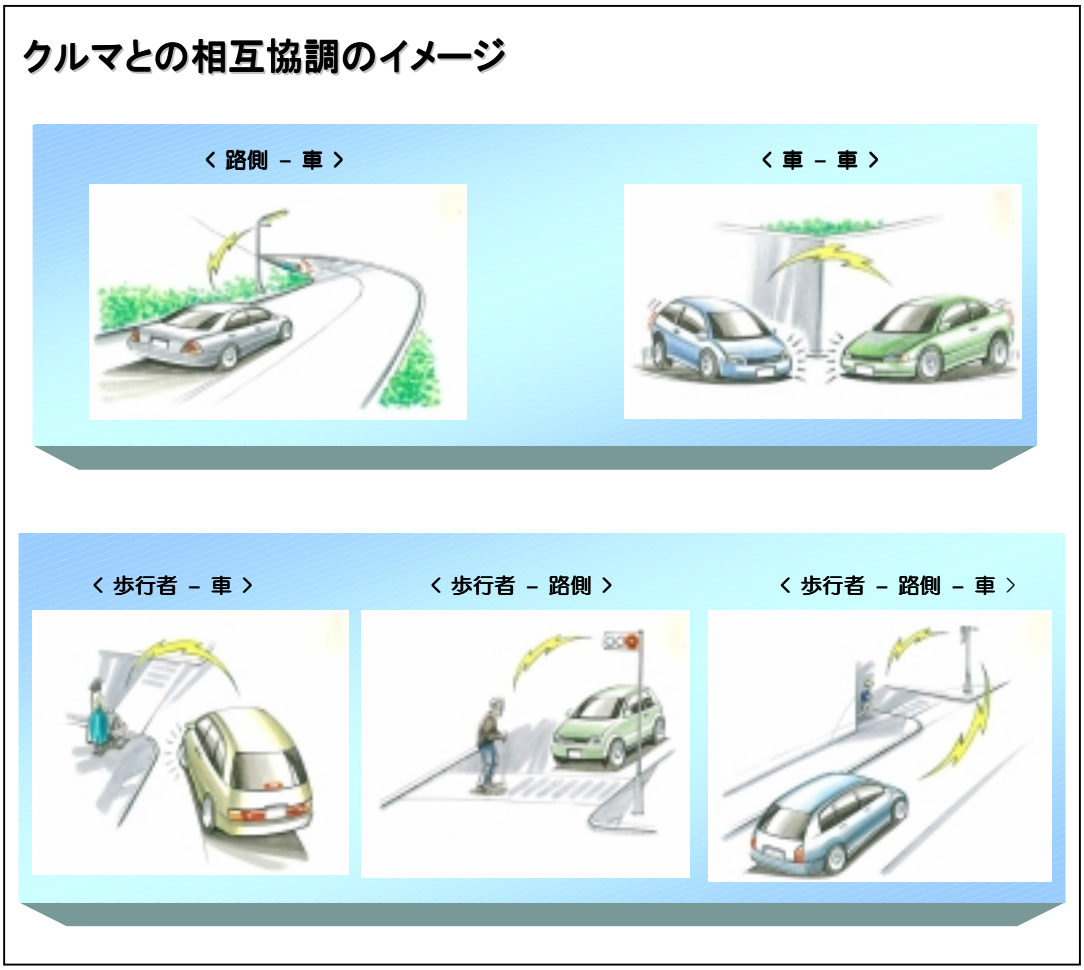
3.3.4. 渋滞緩和に向けたインフラ・ネットワークの活用

一方、渋滞に関しても、日本だけでも年間 53 億人･時間の時間損失があると言われている。時間の遅れによるビジネス・就労機会の損失、コスト増、燃費の悪化等を考えると、金額に換算して、年間 12 兆円の損失になる。

また、今後の世界人口の増加及びクルマの普及率増加から推定して、2050 年にはクルマの台数の増加に伴う環境負荷への影響度は、現在の 4～5 倍に達すると見られ、そのことを踏まえると、CO_2, NO_x の排出量削減等、環境負荷の削減目標値は１／４～１／５にする必要がある。このためには、ハイブリッド車、燃料電池車の開発・普及と同時に、交通渋滞の緩和・平均車速の改善により、 CO2, NO_x の排出量削減が望まれる。

3.3.5. クルマ・ヒトとインフラ・ネットワークとの協調イメージ

事故低減（安全）の為の、クルマ・ヒト、インフラ・ネットワークの協調イメージを下図に示す。下図のように、交差点・カーブとその周辺をカバレッジとした狭域通信が有効となると考えられる。このような、「安全」の為にインフラ・ネットワークを活用する場合、出来るだけ少ない遅延時間、瞬時でのセッションの確立等が必須となる。



また、「渋滞緩和」、「安心」、「快適」等のサービスも合せて考えた場合、上記の狭域通信に加え、携帯電話（パケット通信含む）、デジタル放送、無線 LAN、アドホック通信等、今後出てくる新しい通信方式を含め、様々なネットワークを組み合わせて、アプリ、コンテンツ、場面、場所に応じて、通信メディアを使い分けることが必要となる。

3.3.6. ネットワーク要件と ISP に依存しない IPv6 グローバルアドレスの必要性

以上より、インフラ・ネットワークを活用した「安全」、「渋滞緩和」、「安心」、「快適」サービスを実現する為のネットワークの要件は次の様になる。

① 移動するクルマは、コンテンツ・アプリ、場面、場所等に応じて、様々なプロバイダ/管理者が運営するインフラ・ネットワークを利用する
② 走行途中に他のネットワークに移動することが十分に想定され、アプリ、コンテンツによっては、セッション継続性や瞬時での切替えが求められる。

従って、将来は IP アドレスに関して、クルマ、ヒト、自転車、バイク等に

① グローバル且つユニークな IP アドレスが必要
② 様々なプロバイダ、管理者が運営するネットワークを使い分ける為、プロバイダ等に依存しない IP アドレスが必要

⇒ 将来、ネットワークが IPv6 ベースであることを仮定すると、プロバイダに依存しない IPv6 グローバルアドレスをクルマ、ヒト、自転車、バイク等に付与することが必要

3.3.7. Non-ISP の IPv6 グローバルアドレス取得必要性提言に向けた課題

前述のクルマ社会を実現する為には、以下の課題があり、実現には今しばらくの時間を要する為、現状においては、IPv6 グローバルアドレス取得の必要性を提言するには至らない。

① IPv6 ベースのネットワークの普及
② インフラの整備
③ 各種必要技術の開発
④ ビジネスモデルの確立　等

3.3.8. 車内 LAN の IP 化及び IPv6 グローバルアドレスの必要性について

車内 LAN は大きく次の 3 種類に大別される。

① 制御系
アクセル、ステアリング等
② ボディ系
パワーウィンドー等
③ マルチメディア系
ナビ、車載機、カーステレオ等

現状、全ての系において Non-IP であり、当面 IP 化する動きはない。特に制御系は、クルマの安全に関わる部分であり、接続保証型、高速、セキュアな通信方式が必要である。
但し、将来クルマへのユーザ持込み端末の利便性、持込み端末とクルマのマルチメディア系部品との連携を考えると、マルチメディア系は汎用技術である IP を採用し、マルチメディア系部品に IPv6 アドレスを付与する可能性は考えられる。
その際には、クルマにはネットワークのプロバイダに依存しない IPv6 グローバルアドレスが必要と述べた様に、マルチメディア系部品の IPv6 アドレスにも同様のアドレスが必要となる。

4. ID 割り振りと接続性　～技術的解法～

本章では、機器固有の ID を割り振り、その ID を用いて遠隔(インターネット上)から機器に接続する場合において、機器接続性を実現する複数の方法を技術的観点から検討し、その得失について論じる。

機器固有の ID 割り振りにおける機器接続性を検討するにあたり、機器接続のアプリケーションとして「リモートメンテナンス」を取り上げる。具体的なアプリケーションを想定することにより、機器接続性の得失がより明らかになると考えられるからである。

機器固有の ID として IPv6 アドレスを固定的に割り振る場合について、以下の 3 通りの実現方法を比較、検討する。

- /128 をインターネットに広告する
- Mobile IP を使用する
- VPN トンネリングを使用する

また比較のため、機器固有の ID として IPv6 アドレスを固定的に付与しない、以下の 2 つの実現方法についても検討する。

- DDNS を使用する
- 独自に ID を付与する

4.1. /128 の広告

端末に付与した/128 のアドレスを、そのままインターネット上に経路として広告する手法を検討する。

IPv4 では最大/32 の長さの経路広告が発生するが、その数が増えるとルーティングテーブルの肥大化を招き、ルータの性能に与える影響が大きい。したがって、一般的な IP 網の運用では一定の長さ以上の経路広告は廃棄することが多い。廃棄される経路広告のプレフィックス長はプロバイダの運用ポリシーによるので一概にはいえないが、/24 よりも長いプ

レフィックス長は廃棄（フィルタ）される可能性がある。

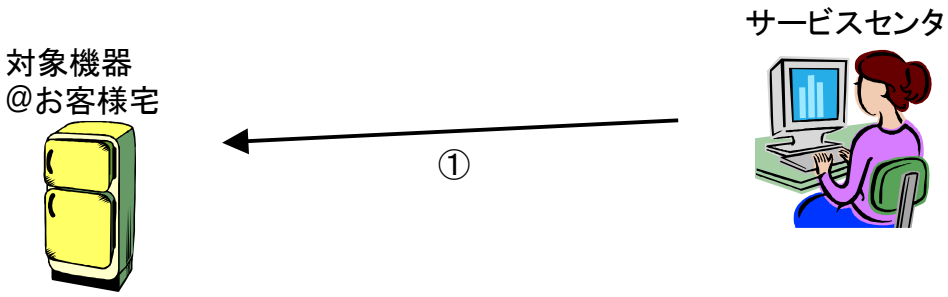


図 4.1 端末に付与した/128 アドレスを用いたリモートメンテナンスの実現

IPv6 では IPv4 におけるルーティングテーブルサイズの問題を踏まえ、経路集約可能なネットワーク設計としている。具体的には、アドレス割り振りのサイズを/32 単位とし、(初期に割り振られた/35 を除き)/32 よりも長い経路広告が BGP 等の広域ルーティングシステムに発生しないよう配慮している。したがって、もし仮に/35 よりも長いプレフィックスが広告された場合、プロバイダにより経路が廃棄される可能性がある。

/128 のアドレスを付与し、それがルーティング可能なのであれば、もっとも確実な方法であるといえる。しかしながら、128 ビットのプレフィックス長を広告することは現実的にはほぼ無限の IPv6 アドレス空間を端末単位で経路広告することを意味し、ルータの性能上不可能である。現実的には、アドレスのネットワーク部はその端末を接続するネットワークから付与するか、モバイル IP などの手段によりルーティング可能とすることが求められる。

[利点]

- 実装のコスト
  - ルーティング可能であるならば、本方式を用いるために IPv6 通信が可能であること以外の追加機能は不要である

[欠点]

- ルーティングの実現が困難
  - 現在のルータの性能では、/128 をルーティングすることが困難であり、本方式により IPv6 アドレスを機器 ID として用いることは現実的でない

4.2. Mobile IP

Mobile IP を用いて機器への接続性を実現する場合について検討する。

Mobile IP は、端末の移動性を IP レイヤで実現する。すなわち、端末が IP ネットワーク上でネットワーク間を移動した場合において、端末が移動する前の IP アドレスを用いた接続性を確保する。IP レイヤで実現されるため、アプリケーションレベルやユーザレベルで

は、端末の移動(移動先で付与される IP アドレスが変更されていること)は隠蔽される。

IPv4 版の Mobile IP は、RFC 3344 で規定されている。IPv6 版の Mobile IP は、IETF の mip6 WG (IPv6 版)で現在標準化が進められている[2]。本書では、今後主流となると思われる、IPv6 版の Mobile IP を例にとり、検討を行う。

Mobile IP を用い、遠隔から機器のリモートメンテナンスを行う場合の例を以下に示す。

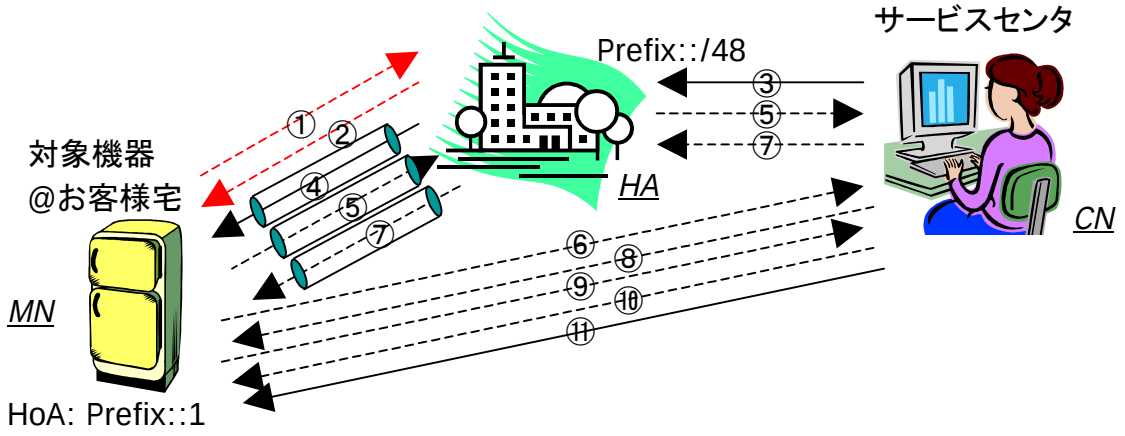


図 4.2 Mobile IP を用いたリモートメンテナンスの実現

リモートメンテナンスで制御対象となる対象機器が Mobile Node (MN)である。MN は、Home Address (HoA)のアドレス空間(Prefix::/48)の中にある IP アドレスの一つを固定的に付与されている。Home Agent(HA)は、インターネット上で HoA のアドレス空間に対してルーティングされている場所に設置されている。またサービスセンタの操作端末は、Mobile IP を用いて対象機器と通信を行い、Corresponding Node (CN)として振舞う。

なお、リモートメンテナンスを行うサービスセンタを運営する組織は、HA を持つ組織と同一である必要はない。

Mobile IP の場合、リモートメンテナンスを開始するまでの通信シーケンスは以下のようになる。

① 移動先のネットワークに設置され、新たに移動先の IP アドレス= Care of Address (CoA)を取得した対象機器 MN は、HA に対して移動通知(Binding Update: BU)メッセージを送信する。なお、Mobile IP のドラフトに準拠するのであれば、この BU メッセージは、IPsec によって保護されなければならない

② MN からの Binding Update を受信した HA は、MN に対して Binding Acknowledgement (BA)を送信する。Mobile IP のドラフトに準拠するのであれば、BA メッセージは、BU 同様 IPsec によって保護されなければならない

③ (リモートメンテナンスの必要性に伴い)操作端末 CN は MN に対して通信を開始する。

[2] 最新のドラフトは draft-ietf-mobileip-ipv6-24.txt であり、現在 RFC 文書の発行待ちとなっている。

CN は MN の移動先 IP アドレス CoA を知らないので、HoA 宛にパケットを送信する

④ HoA のアドレス空間上に設置された HA は、HoA 宛のパケットを MN に代わって受信する。HA は MN の移動先 IP アドレス CoA を知っているので、CN が送信したパケットを CoA 宛のパケットでカプセル化し、移動先の MN に送信する。これら一連の動作により、CN が MN に送信したパケットは、移動先の MN に到達する

⑤ HA によってカプセル化された、CN からのパケットを受け取った MN は、CN に対して HA 経由で Home Test Init (HoTI)メッセージを送信する。HA を経由させるために、MN→HA 間は HoTI メッセージをカプセル化して送信する

⑥ 同時に MN は、CN に対して直接 Care-of Test Init (CoTI)メッセージを送信する

これから先の振る舞いは、CN が Mobile IP 対応である場合と、そうでない場合で異なる。

CN が Mobile IP 対応でない場合、CN は HoTI、 CoTI の受信に対し ICMP Parameter Problem メッセージを送信するか、または何も送信しない。この場合、MN は CN との通信を常に HA 経由で行う。HA と MN の間は、MN←→CN 間のパケットをカプセル化する。

以下は、CN が Mobile IP 対応である場合である。

⑦ HoTI と CoTI メッセージを受信した CN は HA 経由で Home Test (HoT)メッセージを送信する

⑧ 同時に CN は、MN に対して直接 Care-of Test (CoT)メッセージを送信する

⑨ 正しい HoT メッセージと CoT メッセージを受信した MN は CN に対して BU を送信する。HA へ BU を送信する場合と異なり、IPsec によるメッセージの保護は必要ない

⑩ MN からの BU を受信した CN は、MN に対して BA を送信する。HA が BA を送信する場合と異なり、IPsec によるメッセージの保護は必要ない

⑪ HoTI+CoTI、 HoT+CoT のやり取りが終了すると、MN と CN は HA を介さず直接通信を開始する

Mobile IP を用い接続性を確保する場合の利点と欠点を述べる。

[利点]

- 新たな独自プロトコルの規定が不要
  - 端末の移動は Mobile IP のみで隠蔽されている
- セキュリティを標準で提供
  - 十分議論されており、脆弱性のリスクが低い

[欠点]

- Mobile IP 実装のコスト
  - フットプリント
  - パフォーマンス
- IPsec の処理負荷
  - MN←→HA 間の BU、 BA(①、 ②)は、IPsec の使用が必須→実装の負荷
  - IKE を使った鍵交換は必須ではないが、使用する場合、鍵交換プロセスのフット

プリントや、べき乗剰余演算の計算量は無視できない

- セキュリティ
  - 明示的に制限しない限り、HoA を指定すれば誰でも MN に接続可能
- HA のスケーラビリティ
  - 特に、CN が Mobile IP 対応でない場合が課題

4.3. VPN トンネリング

VPN トンネリングを用いて機器への接続性を実現する場合について検討する。

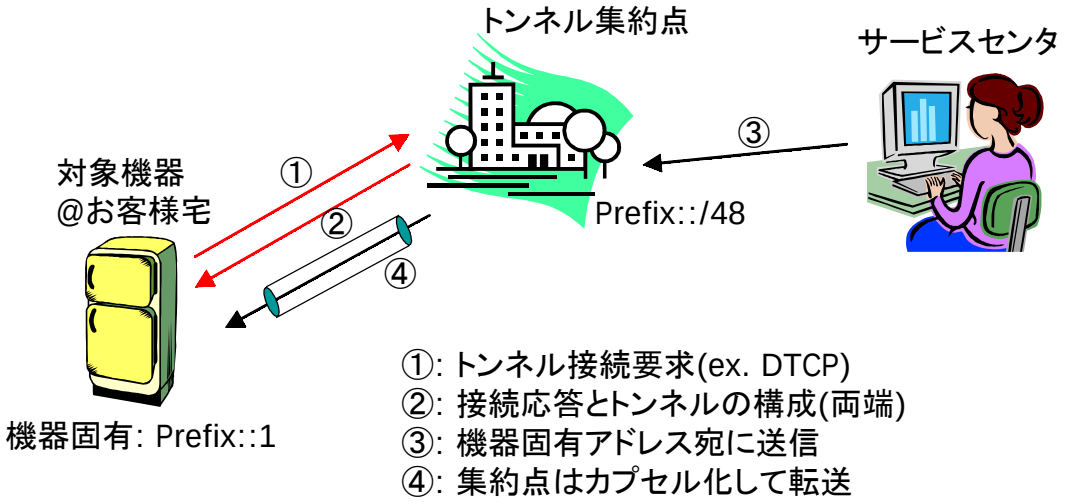


図 4.3 VPN トンネリングを用いたリモートメンテナンスの実現

このケースの場合、対象機器には、アドレス集約点が持つ特定のアドレス空間(ここでは Prefix::/48)の中にある IP アドレスの一つ Addr_equip が固定的に付与されている。またアドレス集約点は、インターネット上で Prefix::/48 のアドレス空間に対してルーティングされている場所に設置されている。

移動先に設置された対象機器は、まず IPv6 の標準的手法(NDP 等)で、移動先で使用するアドレス Addr_local を取得する。アドレスを取得した機器は、VPN トンネルを設定する何らかのプロトコルを用い、トンネル集約点に対して VPN トンネルの接続要求を送信する(①)。トンネル集約点はこの要求の是非を判断し、応答する。接続可能である場合は、対象機器とトンネル集約点の両側で設定を行い、トンネルの端点を構成する(②)。なお VPN トンネルの接続プロトコルとしては、例えば DTCP（dynamic tunnel configuration protocol）[3]が使用できる。

対象機器に対してメンテナンスを行うサービスセンタのオペレータは、機器固有のアドレス Addr_equip 宛にパケットを送信し、メンテナンスを実施する(③)。トンネル集約点は、このパケットをカプセル化し、Addr_local 宛に送信する(④)。

[3] DTCP は、Trumpet Software 社(http://www.trumpet.com.au/)が提案している、動的にトンネルを構成するためのプロトコルである。IETF に提出された Internet Draft は既に expire されているが、http://jazz-1.trumpet.com.au/ipv6-draft/dtcp-draft-prt-13-may-1999.htm から入手できる

VPN トンネルを用い接続性を確保する場合の利点と欠点を述べる。

[利点]

- Mobile IP と比較して、実装が軽い
- 機器に付与した IPv6 アドレスに対し、IPv4 ネットワークを経由して接続できる
  - IPv6 ネットワーク・インフラの普及を待たずに、IPv6 アドレスを ID として使用できる

[欠点]

- トンネルを動的に構成するための、一般的なプロトコルがない
  - 例えば、DTCP は RFC になっていない
  - 通信のためのシーケンスを別途定義、実装する必要あり
- セキュリティ
  - 明示的に制限しない限り、機器固有のアドレスを指定すれば誰でも対象機器に接続可能
- トンネル集約点のスケーラビリティ
  - すべての通信がトンネル集約点を通過する

4.4. DDNS

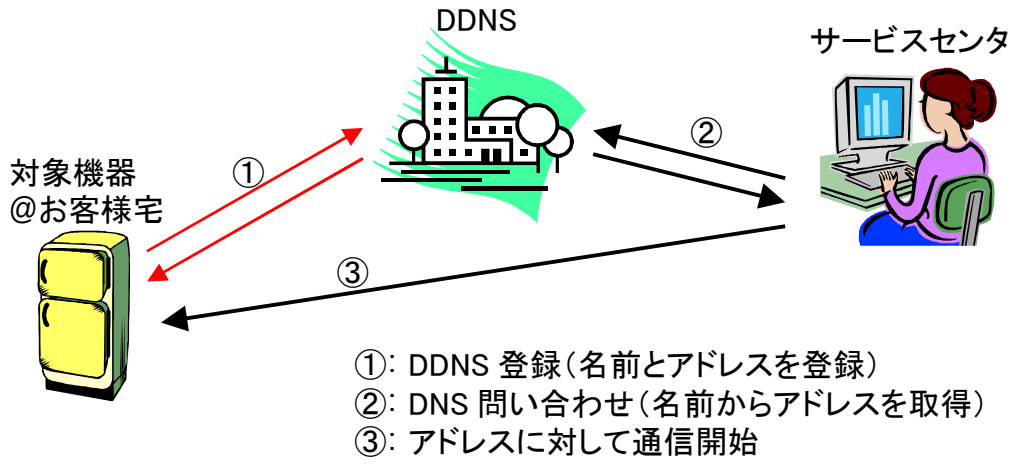


図 4.4 DDNS を用いたリモートメンテナンスの実現

機器に固有 ID を付与しない方法のひとつとして、DDNS(Dynamic DNS)を用いる方法がある。DDNS は RFC2136 に記述されており、DNS に対して動的にレコード登録を行う方法を規定する。DDNS を用いることにより、機器に固有 ID を付与することなく、以下のような手順により外部から機器に対してアクセスできるようにすることが可能である。

1) 機器出荷時に、機器が登録を行う DDNS サーバの所在と、機器がサーバに登録すべきネーム情報（Resource Record Set）を事前登録する
2) 機器がネットワークに接続された際に IP アドレスを自動取得する。自動取得の手順は、

RFC2462 などにより可能である

3) 機器は取得した IP アドレスとネーム情報を、あらかじめ指定された DDNS サーバに登録する
4) 外部から機器にアクセスする場合、あらかじめ設定したネーム情報をもとに DDNS サーバから機器が取得した IP アドレスを知ることができ、それによりアクセスが可能となる

上記のとおり、DDNS により機器へのアクセスを可能とするためには DDNS サーバを構築・運用することが前提となる。

DDNS を用い接続性を確保する場合の利点と欠点を述べる。

[利点]

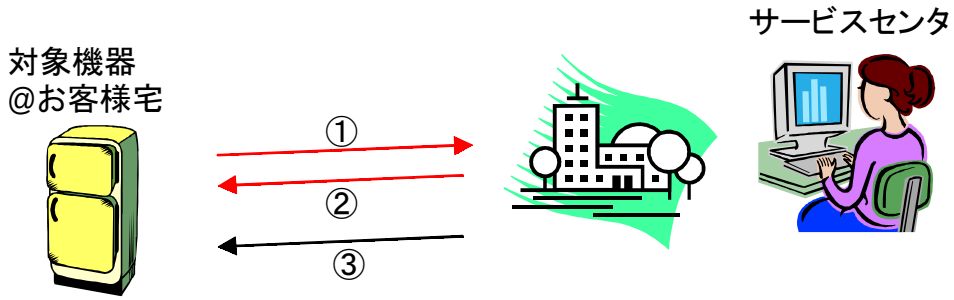
- 標準プロトコルの利用
  - DDNS は IETF にて RFC として標準化され、インターネットサービスとしても広く用いられている技術であることから、安定動作や相互接続の容易さが期待できる

[欠点]

- アドレスの代わりに名前管理が必要
  - アドレスを機器 ID として用いる当初の目的を満たしていない
- セキュリティについて詳細検討が必要
  - DNS はインターネットに公開されるサービスであることから、セキュリティやプライバシーが求められる場合には対応策の検討が必要である

4.5. 独自 ID

機器に独自の ID を付与し、その ID を用いて機器への接続性を実現する場合について検討する。



①: 現在のアドレスの登録(独自プロトコル)
②: 登録完了確認(独自プロトコル)
③: 機器制御 (Out of Scope)

図 4.5 独自 ID を用いたリモートメンテナンスの実現

このケースの場合、移動先に設置された対象機器は、まず IPv6 の標準的手法(NDP 等)

でアドレスを取得する。アドレスを取得した対象機器は、独自のプロトコルを用い、登録センタに取得したアドレスを登録する(①、 ②)。

対象機器に対してメンテナンスを行うサービスセンタのオペレータは、ID をキーとして登録センタに対象機器のアドレスを問い合わせる。アドレス取得後、オペレータは対象機器に接続し、メンテナンスを実施する(③)。

対象機器は、登録センタに登録されたアドレスが常に最新となるよう、定期的にアドレスをセンタに登録する。またアドレスの変更を検出した場合も、登録を実施する。

悪意を持つユーザにより、実際に対象機器が取得したアドレスとは異なるアドレスが、登録センタに登録されることを防ぐため、登録のシーケンスは何らかの方法で保護されなければならない。

例えば、不正な登録を防ぐ比較的単純な方法は、①で送信し登録される ID および IP アドレスは、対象機器が持つ秘密鍵によって署名することである。①のパケットが再送されることによる攻撃を考慮するのであれば、nonce のやりとりや、challenge and response による認証の使用などを検討すべきである。

また、登録センタとサービスセンタの運営者が異なるのであれば、その間のセキュリティについても考慮する必要がある。

独自 ID を用い接続性を確保する場合の利点と欠点を述べる。

[利点]

- 実装のコスト
  - 必要最小限の機能のみを実装すればよく、一般にフットプリントは小さくなることが期待できる

[欠点]

- 新たな独自プロトコルの規定が必要
  - プロトコルを標準化できなかった場合、登録センタをプロトコル別にそれぞれ設置する必要がある
- セキュリティについて独自の検討が必要
  - 十分議論がなされず、これが脆弱性の要因となる可能性がある

5. 関連する活動

本章では、「ISP を経由しない IPv6 アドレス割り振り」検討にあたり、関連した活動として、IPv6 普及・高度化推進協議会での活動、IETF にて議論されている、IP アドレスの製品への組み込み非推奨議論、閉域ネットワークで自由に利用できる IPv6 アドレス「ユニークローカル IPv6 ユニキャストアドレス」、APNIC での IPv6 アドレス割り振り・割り当てに関するガイドラインの作成について報告する。

5.1. IPv6 普及・高度化推進協議会リモートコントロールノードアドレス SWG の活動状況

インターネット接続事業者から割り当てられたアドレスとは独立なアドレス領域を持っ

てサービス展開をしたいという足回りを持たないアプリケーションサービス事業者のニーズを吸い上げ、そのサービスが実現するよう地域インターネットレジストリ（RIR）から直接アドレスブロックの割り振りを受けられる環境を整備していくことを目的に昨年夏にスタートした「リモートコントロールノードアドレスＳWG」は、これまで４回の会合を重ねてきた。当初は、各種センサーや家電などのネット接続端末を遠隔でモニタリング、制御する分野を 1 つの先駆的な例に取り上げ、そのようなサービスが独立アドレスブロックを取得するに値するか、といったことをサービスの要求仕様や技術的な側面から検討した。また、センサー系の事例のほか、地方自治体系で検討されている緊急用アドホックネットワークのサービスや、自動車通信向けのアドホック通信サービス、さらには e!で取り上げられたトレーサビリティサービスなども議論に取り上げ、技術的フィジビリティや独立アドレスブロックをどういう組織に与えるべきか、同様なサービスを提供する組織がどの程度の規模として存在しそうか、といった点を検討した。一方、ＳWG運営陣は、アジア太平洋地域の RIR である APNIC とも情報交換を行い、ＳWGでの議論内容の紹介や APNIC の割り振り審議に対する見解について双方の理解を深めた。今後も新サービスの立ち上がり動向などについて情報交換を続ける予定である。ＳWGは、今後、これまでの議論を踏まえて、独立アドレス領域の取得による新サービスの提供に当たり、その際にサービス事業者が考慮しておくべきポイントなどを整理する予定である。またアドレス取得とそれによる新サービスの展開が加速する様に、これまでアドレス申請を行ったことのない組織を対象に、アドレス申請の手解きとなるようなものも用意する予定である。当初、３月までの活動予定であったが、参加メンバの要望により、近未来に想定できるサービス形態を題材に議論を続けることにしている。

5.2. IETF における IP アドレスの組み込みに関する議論

IETF GROW WG (Global Routing Operations WG)において、広域でルーティング可能なアドレスを組み込み用途に利用することに対する問題点[4]が提案されている。これは、コンシューマエレクトロニクスやネットワーク機器が、広域でルーティング可能な IP アドレスを製品のファームウェアに組み込んで出荷されている現状に対して、このような IP アドレスの組み込みは、インターネットの運用やアドレス空間管理に大きな影響をもたらすため実施すべきではない、というものである。この提案に対しては特に反論はなく、近々 Informational RFC 化されると思われる。

上記の提案は、主に（NTP サーバなどの）インターネット上でサービスを提供しているノードの IP アドレスを埋め込むことに関するものであり、また、アドレス枯渇が心配されている IPv4 に関しての提案で、広大な空間を持つ IPv6 には当てはまらない部分もあ。しかしながら、アドレスを識別子として組み込んだ場合、アドレスブロックの再利用が困難になってしまうこと、IP アドレスは「貸与」されるものであり、特定組織の持ち物ではない、という概念に反することなどは識別子としての利用にも共通するものであるため、識別子として利用する際には検討が必要である。なお、本提案に関するインターネットドラフトの邦訳を付録 1 に添付する。

[4] D. Plonka , “Embedding Globally Routable Internet Addresses Considered Harmful”, Internet Draft <draft-ietf-grow-embed-addr-00.txt> , work in progress

5.3. ユニークローカル IPv6 ユニキャストアドレス

本章では、ISP に接続しないサイトで使用できる IPv6 アドレスである、ユニークローカル IPv6 アドレス[5]について説明する。識別子としての IPv6 アドレス利用においては、当該アドレスの利用も検討対象になると思われる。ユニークローカル IPv6 アドレスは、現在 IETF ipv6 WG で、標準化に向けた議論が進められている。

5.3.1. 標準化の背景

従来、ISP に接続しないサイトで使用できる IPv6 アドレスとしては、RFC3513 で規定されたサイトローカルアドレスがあった。サイトローカルアドレスは、ネットワーク管理者が規定した範囲=「サイト」の中で、一意に割り当てられるアドレスである。しかしながらその定義から、いくつかの問題を抱えていた。

- サイト間では一意性が保証されず、このためサイトの外にアドレスが漏洩した場合、想定外の相手と通信できてしまうなど、セキュリティ上の問題を引き起こす可能性がある
- サイトは管理者のポリシーにより規定されるものであり、その境界は管理者が明示的に、手動で設定しなければならない
- DNS サーバは、サイトを意識しなければならない。すなわち、内部向けと外部向けのサーバを別に設置する、問い合わせたクライアントがどのサイトに属するかによって、応答を変えるなどの必要がある
- BGP4+/OSFPv6/RIPng などのルーティングプロトコルでは、サイトスコープが考慮されていない。このため、サイトの境界でのルータで複雑な設定を行わなければならないなど、運用に困難が伴う
- アプリケーションは、アドレススコープを意識しないかもしれない。この場合、SIP、FTP など、アプリケーションのプロトコル上で IP アドレスが通知される場合に、サイトローカルアドレスが漏洩する可能性がある
- 同様に、IPsec や MobileIP でサイトをまたぐような運用がされる場合にも、問題が発生する可能性がある

このような問題点から、ipv6 WG 内でサイトローカルアドレスの扱いについて議論がなされ、サイトローカルアドレスを廃止することで合意(ラフ・コンセンサス)が得られた。この合意を踏まえ、関連する RFC からのサイトローカルアドレスの削除、および従来サイトローカルアドレスが果たしてきた役割～ISP に接続しないサイトで使用できる IPv6 アドレス～を代替するアドレスの標準化に向けた議論が開始された。サイトローカルアドレスの代替として議論されているのが、ユニークローカル IPv6 ユニキャストアドレスである。

---

[5] Hinden. R., Haberman. B “Unique Local IPv6 Unicast Address”、 Internet Draft、<draft-ietf-ipv6-unique-local-addr-03.txt>

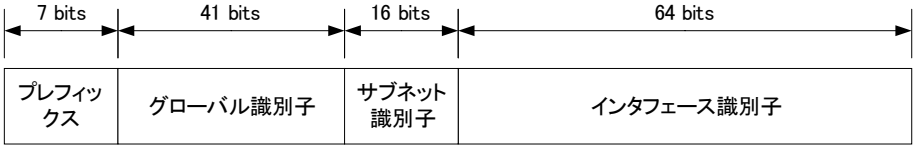
5.3.2. 特徴

ユニークローカル IPv6 ユニキャストアドレスが持つ性質を以下に示す。

- グローバルで一意のプレフィックス[6]
- サイトの境界で容易にフィルタリング可能な、よく知られたプレフィックス
- これらのプレフィックスを使いつつ、サイト同士を結合する、またはインターネットを介さずに相互に接続する場合、アドレスの競合や、リナンバリングの必要性が生じない
- 経路制御や DNS の設定/運用誤りによりアドレスがサイトの外に漏洩した場合でも、他のアドレスとの競合が生じない
- アプリケーションは、これらアドレスをグローバルスコープのアドレスと同様に扱うことができる

5.3.3. フォーマット

ユニークローカル IPv6 ユニキャストアドレスのフォーマットを以下に示す。



プレフィックス: FC00::/7 のプレフィックス
グローバル識別子: グローバルで一意のプレフィックスを作るための識別子。詳細は後述
サブネット識別子: サイト内で使用するサブネットの識別子
インタフェース識別子: RFC3513 で規定されたインタフェース識別子

5.3.3.1. グローバル識別子

41 ビットのグローバル識別子の空間は、異なる割り当て方法を持つ 2 つの空間に分割されている。2 つの空間は、それぞれ FC00::/8 と、FD00::/8 のプレフィックスで始まる。

FC00::/8	中央の組織が割り当てる空間 (Centrally Assigned Global IDs)
FD00::/8	各組織が個別に割り当てる空間 (Locally Assigned Global IDs)

また残りの 40 ビットは、擬似乱数を使い生成する。先頭から順番に割り当てたり、よく知られた番号(well known numbers)を割り当てたりしてはならない。生成方法の例は後述する。

[6] ただし後述する FD00::/8 の空間では、競合の可能性は低いものの必ずしも一意とはならない。したがって、アドレスの競合も、確率としては十分低いものの、起こらないわけではない。

5.3.3.2. **中央の組織が割り当てる空間** (FC00::/8)

単一の割り当て組織が ID を割り当てる空間。管理された、ある程度の規模を持つサイトでの使用を想定している。ユニークローカル IPv6 ユニキャストアドレスを持つサイトを相互接続する場合、またはその可能性がある場合には、この空間の使用が推奨される。

ID の割り当てに関して、以下の要件が提案されている。

- 公平なやりかたで、誰にでも割り当て可能なこと
- 恒久的に割り当てられ、定期的な使用料の支払いが不要であること
- 世界のさまざまなエンドユーザにとって手ごろな値段であり、割り当ての際にのみ必要とされる、返金不能な「割り当て料金」の制度
- ID が独占的に確保されることのない仕組み
- ID の所有権(所有者)は非公開にされつつ、第三者(割り当て機関)はその所有を管理できること(ID の重複割り当てを防ぐため)

5.3.3.3. **各組織が個別に割り当てる空間** (FD00::/8)

各組織が個別に ID を割り当てる空間。小規模や、他のサイトと接続しないサイトでの使用を想定している。割り当て組織にコンタクトする必要がなく、容易にプレフィックスを割り当てることができる。この空間では、他の組織が割り当てたプレフィックスとの競合が起こり得るが、その可能性は小さい。

5.3.3.4. **グローバル識別子生成アルゴリズムの例**

グローバル識別子の生成アルゴリズムとして、以下の方法が提案されている。

1. 64 bit の NTP のフォーマット[7]で現在の日時表記を得る
2. このアルゴリズムを実行するシステムから、EUI-64 識別子を得る。EUI-64 がない場合には、RFC 3513 に規定された方法で、48 bit の MAC アドレスから生成してもよい。いずれも不可能な場合は、ノード固有の適切な識別子(シリアル番号など)を使用する
3. 上記、日時とシステム固有の識別を結合し文字列を生成する
4. 文字列の MD5 ダイジェストを計算する[8]
5. ダイジェストの末尾 40 bit をグローバル識別子として使用する

このアルゴリズムにより、グローバル ID のフィールドは十分一意となり、「グローバル ID」として使用することができるようになる。なお、この空間においてアドレスの一意性が保証される確率についての議論は、Internet Draft を参照のこと。

5.3.4. **本節のまとめ**

ISP に接続しないサイトで使用できる IPv6 アドレスである、ユニークローカル IPv6 ア

---

[7] Mills, David L., “Network Time Protocol (Version 3) Specification、 Implementation and Analysis”, RFC 1305, March 1992

[8] Rivest, R. “The MD5 Message-Digest Algorithm”, RFC 1321, April 1992

ドレスについて説明した。最後に、ユニークローカル IPv6 ユニキャストアドレスの利点と欠点についてまとめる。

[利点]

- プロバイダに依存しない IPv6 アドレスを提供する。インターネットに接続しないサイトや、通信をサイトの中に閉じ込めたいサイトでは、このようなアドレスは有用である
- アプリケーションは、これらアドレスをグローバルアドレスと同様に扱うことができる
- リナンバリングすることなく、これらアドレスを使う複数のサイトをマージすることができる
- これらアドレスを使った通信であれば、通信を中断することなく、プロバイダが提供するアドレスを変更することができる
- サイトの境界で、これらアドレスを容易にフィルタリングできる
- サイト間の VPN に使用できる
- これらアドレスが万一サイトの外に漏洩しても、他のアドレスとの競合することはない

[欠点]

- インターネットで、これらアドレスをルーティングすることはできない
- 「各組織が個別に割り当てる空間」では、非常に低い確率ではあるものの、一意性が保てない可能性がある。この危険性は現実には問題にならないと思われるが、理論上は起こりうる

5.4. APNIC IPv6 ガイドライン

5.4.1. 概要

現行の IPv6 アドレスポリシーは、2002 年 7 月から全世界共通のポリシーとして施行されているが、ポリシー運用の経験を経るにつれ、いくつかの問題点が指摘されるようになってきており、実際にポリシーの変更の提案がなされるに至っている地域もある。

そのため、JPNIC では現行の IPv6 アドレスポリシーを解説、補完する文書として「IPv6 ガイドライン文書」を APNIC 地域において策定することを JPNIC オープンポリシーミーティングにおいて提案した。この提案は同ミーティングにおいてコンセンサスを得るに至り、APNIC オープンポリシーミーティングで同様の提案を行なったところ、ここでもコンセンサスを得ることができた。

これを受け、ドラフトの作成が 2003 年 11 月から開始された。2004 年 3 月現在、APNIC にて「IPv6 ガイドライン文書」は正式文書化に向け作業が行なわれている状況である。

5.4.2. 策定に至った経緯

現行の IPv6 アドレスポリシーにおいて指摘されている問題点は以下のようなものがある。

- 200 × /48 という初期割り振り基準に対する心理的負担
- 主にオペレーションに関する事項についての記述不足
  - 求められる書類についての規定がない
- PI アドレスやプライベートアドレスの規定がない
- 基準そのものの妥当性
  - 初期割り振りの判断基準となる 200 × /48 という値
  - 追加割り振りの判断基準となる HD-ratio の値
- 家電等への IPv6 アドレス割り当てのような形態が、ポリシー上想定されていない

ポリシーそのものの見直しも中長期的には必要ではあるが、まずはガイドライン文書を策定して上記で挙げたようなオペレーションに必要な情報の提供を行なう方向で解決を目指すのが妥当と JPNIC では判断した。

ガイドライン文書の策定は、2003 年 7 月の JPNIC オープンポリシーミーティングで JPNIC により提案がなされ、会場の賛同を得た。この後、2003 年 8 月の APNIC ミーティングでガイドライン文書の策定が提案された。

APNIC ミーティングの結果、ガイドライン文書の策定はコンセンサスを得て、コミュニティからボランティアを募ってドラフト作成に着手することとなった。実際のドラフト策定は 2003 年 11 月から作業が始まり、2004 年 2 月の APNIC ミーティングでドラフトの報告が行なわれるに至った。2004 年 3 月現在、APNIC において正式文書化に向け、ガイドライン文書の編集が行われている段階である。今後、APNIC のメーリングリスト上で最終ドラフトが提示され、コメント期間を経た後実装にいたることとなる。

5.4.3. ドラフトとその内容

ドラフトを作成するワーキンググループは 2003 年 11 月に募集が行なわれ、3 人の共同チェアを含む 10 数名により、メーリングリスト上でのドラフト作成作業が行なわれた。2004 年 2 月の APNIC ミーティングで行なわれたドラフト報告時点の内容は、以下の通りである。

http://www.apnic.net/mailing-lists/wg-ipv6-guide/archive/2004/03/msg00000.html

（ガイドライン目次）

1. Introduction
2. Scope
3. Additional guidance

4. Goals of address space management
5. Application of guidelines
6. Definition of a 'site'
   ① Assignment address space size
7. Initial allocation criteria
   ① Use of existing IPv4 infrastructure
   ② Documentation required
      1. Supplementary Document
   ③ Closed networks
8. Second opinion requests
   ① Sub-Allocations and Second Opinion Request
   ② Documentation required
9. Subsequent allocations
10. Requesting a reverse delegation
11. Database registrations

「7.3 closed networks」は、本専門家チームの活動内容に関わってくる個所だと思われる。APNIC では、グローバル IPv6 インターネットに接続しないネットワークについても、割り振り基準を満たす限り IPv6 アドレスの割り振りを認めることを表明している。このことをレジストリ側が認める意義は決して小さくなく、今後の IPv6 アドレスの利用の広がりに期待が持てる決定ではないかと思われる。

http://www.apnic.net/docs/policy/discussions/prop-015-v001.txt

5.4.4. 今後の動き

現在は APNIC において正式文書化を待っている段階であるが、正式文書となった時点で JPNIC としては本文書の翻訳を行なったうえで、JPNIC オープンポリシーミーティング上での紹介等含め、広くコミュニティへの周知を図っていきたいと考えている。また、本専門家チームで検討したような割り当てのケースについては、今後の利用の経験を積んだ上で、ポリシー自体の改変提案をするのか、このガイドラインに盛り込むのか、ニーズを見極めて判断していくことになると思われる。

6. 識別子としての IPv6 アドレス配布ポリシーの考慮点

本節では、製品等の識別子として IPv6 アドレスを利用可能とするアドレスポリシーを提案する際に考慮すべき点について述べる。

1. アドレス取得資格

アドレスを取得できる組織の資格を明確化する必要がある。現状の ISP ベースの割り振

りポリシーでは、3.1 節で述べたとおり、アドレスを取得可能な組織に

a) LIR であること
b) エンドサイトでないこと
c) /48 を割り当てた組織に対し、IPv6 の接続性を提供する計画があること。その際、経路広告は割り振られたアドレス一つに集成すること
d) 2 年以内に最低でも 200 の/48 の割り当てを行う計画があること

といった条件を設けている。製品の出荷予定数や、ID としての利用計画を明示することが必要であると考える。また、5.3 章で述べた閉域アドレスでは対応できないこと、広域での一意性が必須なこと等も考慮すべきであると考える。

2. アドレス利用プラン（アドレス再利用への考慮）
取得資格にも関連するが、IP アドレスを使い捨てとしないための方策について、再利用の考え方の明示が必要であると考える。

3. インターネットへの接続（ルーティング手段等）
広域で利用できる IP アドレスを割り振る用件として、ID を付与した機器がインターネットにつながること、およびつながった場合に、技術的に実現可能な通信手段（モバイル IP を利用する等）の明示が必要であると考える。

4. アドレスブロック追加申請
取得したアドレスブロックを使い切りそうになった場合に、アドレスの追加申請を行うことになるが、ID としての利用形態に合致した追加申請基準の設定が必要である（現在の ISP ベースの割り振りでは、HD-Ratio をもとにした判定になるが、このような明確な基準を決める必要がある）。

7. まとめ

インターネットの今までにない新しい使い方をアドレスポリシーの観点からプロモートしていくことを目的とし、IPv6 アドレスの利用形態として、製品のシリアル番号等識別子や自動車・交通システムで利用、あらかじめ製品にアドレスを埋め込んでの利用を想定し、技術的課題とともに実現可能性を検討した。製品の識別子等、機器固有の ID として IPv6 アドレスを固定的に割り当てて利用した場合でも、MobileIP や VPN トンネリング等の技術を用いることにより、接続性を提供することは可能であると考えられる（現実に実装する場合には、コストやセキュリティの面での課題が考えられる）。

アドレスポリシーの観点からは、現状、考えられる新規の IPv6 アドレス利用要望に対しては、取得を希望する組織がサービスプロバイダとなるモデルであれば、現行の IPv6 アドレスポリシーの範囲で取得可能と考えられる。製品埋め込み等を可能にするようなポリシ

ーの提案は、現状可能な取得に対して影響することが考えられるため、ポリシーとしての明文化については慎重に状況を見極める必要があると思われる。アドレスポリシーに関しては、IPv6 普及・高度化推進協議会のリモコンノード SWG 主査との情報交換より、SWG が実施した APNIC とのミーティングにて APNIC ではかなり柔軟に IPv6 アドレス割り振りを捉えている模様である。JPNIC でも協議会と協調し、新サービス市場の動向把握とその立ち上げを支える活動を強化し、最も APNIC と近い日本を代表する組織として適切に APNIC のアドレス・マネージメントへフィードバックさせていくことが望まれる。

また、IPv6 を利用したビジネスの促進、及びインターネットのさらなる拡大を図るため、JPNIC として、従来の ISP 対象に限定しない、広範囲の IPv6 アドレス取得を可能にするような施策が必要である。具体的には、IPv6 アドレス取得のために指定事業者になれるような仕組みを構築するべきである。

参考

「IP アドレスの機器への組み込み不許可ドラフト」要約版

（Embedding Globally Routable Internet Addresses Considered Harmful）

著作者：D. Plonka(University of Wisconsin)
ステータス：IETF の個人ドラフト、 2003 年 11 月発行　2004 年 5 月１日期限
文書番号：draft-ietf-grow-embed-addr-00

■主旨

次の2つの理由から、消費向けの電気機器及びネットワーク機器に、固有のグローバル IP アドレスをデフォルト設定と組み込むべきではない。

① 消費者は設定を変えるだけの十分なスキル・経験を持っている事は期待できない為、誤った設定をしていた場合、リモートから修正することが出来ず、インターネットの運用に多大な問題を生じる。
② IP アドレスの再割当が不可能なため、アドレス空間の管理に著しい問題が生じる

■背景

ウィスコンシン大学では、出荷した NetGear70 万台が、 時刻合わせをするのに、大学で運用されている NTP server の IP アドレスを見るように、予めハード・コーディングされていた。この為、学内に大規模なインターネット・トラヒックが発生し、運用上重大な問題となった。

■提案

① インターネットホストのメーカやベンダは、消費者向けの組込み IP アドレス機器の提供は避けるべきである。
② オペレータは、問題が発生した時に、いつでも対応策がとれるよう、不要な IP トラヒックを生み出す機能をデフォルトで無効にしておく、或いはそれらのインタフェースを公開しておくべきである。
③ インターネットサービスの信頼性、拡張性、性能を維持するためには、DNS を利用し、IP アドレスを機器に組み込まず、IP アドレスを再割当して利用すべきである。
④ インターネットホストのデフォルト設定、文書化、用例設定には、可能な限り常に、プライベート IP アドレスを使用するべきである。
⑤ サービスプロバイダや企業のネットワークオペレータは、適切なローカルサービスのアイデンティティを通知しなくてはならない。例えば、RFC 2132 [5]に規定されている DHCP プロトコルは、問合せを要求したクライアントに対して利用できるサーバについて回答できるように、サーバを設定することができる。
⑥ 例えば NTP コミュニティのように、グローバル・インターネット上で公共サービスを提供するオペレータは、サービスの IP アドレスの外部通知をすべきでない。これらのアドレスは短命であり、公共サービスのインデックスの中で広く引用されると、想像を越えて増えた負荷に対処するのに必要なサービスの再構成をすることができなくなってしまう。

「IP アドレスの機器への組み込み不許可ドラフト」

（Embedding Globally Routable Internet Addresses Considered Harmful）

著作者：D. Plonka(University of Wisconsin)
ステータス：IETF の個人ドラフト、 2003 年 11 月発行　2004 年 5 月１日期限
文書番号：draft-ietf-grow-embed-addr-00

0. 概要

消費向けの電気機器及びネットワーク機器のファームウェアにグローバル IP アドレスを組み込んでいる。これらの製品は、すでに世界中で利用されており、個人や家庭向けの低価格ルータやミドルボックスに限定していない。グローバル IP アドレスを、ホストのファームウェア内に ID として“ハード・コーディング”することは、インターネットの運用やアドレス空間の管理に著しい問題がある。特に、固定設定（fixed configuration）では使用すべきではない。

1. 背景

2003 年６月、ウィスコンシン大学では、大学の NTP サーバのひとつに、128.105.39.11 というIP アドレスをハード・コーディングしたリファレンスを組み込んだファームウェア付きのルータ、NetGear 製のネットワーク製品、70 万台を出荷したところ、組込み固定設定と導入時にバグがあったため、（壊れた）NetGear SNTP クライアントが 128.105.39.11 アドレスに向けて毎秒１回問合せした。数十万ものソースアドレスから大学ネットワークに向けて大規模なインターネット・トラヒックを発生させた。その結果、重大な運用上の問題を発生した。
これら（壊れた：flawed）ルータは、インターネットで広く導入されており、何年も利用されていく。ウィスコンシン大学は NetGear との協力（NetGear の負担？）のもとで、ダメージを緩和するため、新規の anycast time service を構築していく。

2. 課題

IP アドレスの組込みにより、単一の中央集中型インターネットサービスに依存するインターネット製品において、さまざまな問題が生じてきている。これは、全体の負荷が特定サービスの負荷を上回ったときに、そのサービスが停止するという事態に陥ってしまうこともある。ますます多くのクライアントの IP ホストに固定アドレスが組み込まれるようになると、それは階層的に展開されているサービスの設計意図とちょうど矛盾することになる。

さまざまなインターネットサービスにおいて、信頼性・拡張性・性能を維持するためには、ユーザが IP アドレスによってサービスに直接アクセスしないことが必要だ。代わりに彼らは Domain Name System、 RFC 2219 [1]によってもたらされる indirection（問い合わせ結果の回り道的な配信）のレベルに依存する。DNS はサービス事業者に、ユーザが関与することなく、メンテナンスと負荷均衡のためのリソースを再設定することを認めている。例えば、ある共通の負荷均衡技術は同じ名前の DNS レコードを複数採用しており、それを Berkley Internet Name Daemon (BIND) やその他の

DNS 実装サーバから戻ってきた、問合せ結果を、ラウンドロビン（総当り方式）方式で順番にあたる。そのような問合せへのレスポンスを受けて、resolver は通常、一連のレスポンスのうち、最初の有効問合せ結果を使用する。それにより、オペレータはユーザの問合せによる発生する負荷を、いくつものサーバを介して、一般的にユーザには知られていない別々の IP アドレスで配信することができる。

世界でひとつの IP アドレスを組み込めば、その属する IP アドレスブロックを汚染してしまい、それらの有用性・携帯性を減少させ、逆に運用コストが増えてしまう。また、IP アドレスやブロックが配置転換され、すでに該当サービスをホストしていない状態であっても、迷惑トラヒックが組込みアドレスに配信されることもあるかもしれない。Circa 1997、 RFC 2101 [3] の著者は以下のような観測を示している。

> 動的なアドレス割当てと、ますます頻繁に行われるネットワークの再ナンバリングによって、IPv4 アドレスの一時的独立性はもはや世界的に保証されているとはいえず、これらを識別子として利用することは、大いに疑問である。

このように、たくさんのインターネットホストの設定に組み込まれたアドレスを含んでいる IP アドレスブロックは、その従来の用法により負荷がかかりつつある。これにより、IP アドレスブロックを有効に再割当てするための、Internet Assigned Numbers Authority (IANA) および Internet Registry (IR) ヒエラルキーの機能が妨げられるかもしれない。この問題は、IPv4 アドレスのスペースが飽和状態に近づく中で、特に懸念される。RFC 2050 [2] は、IP アドレスの再利用を促進するために、Internet Service Provider (ISP) がアドレス割当てを「貸し出し」扱いにするよう促していることにも留意しておきたい。

必ずしもすべての消費者が能力や経験をもってインターネットホストを運用できるとは限らないので、もし問題が起こったとしても、その修正実行は期待できない。つまり、インターネットホストのメーカやベンダには、組込み IP アドレスを避けるという大きな責任があるといえる。

3. 提案

インターネットホストやルータの設計者（ネットワーク製品メーカーも含む）は、自社の製品が単一の global internet のみで展開されるだろうと考えてはいけないし、今日たまたまそのように見えるだけのことを当然と思ってはいけない。無数の private internet でこれらの製品が使われれば、ホストが global internet 上の任意のホストとエンド・ツー・エンドの通信を確立することが頻繁にできなくなるだろう。

ベンダは、製品に含まれる不必要な機能をデフォルトで無効にしておくべきである。これは特に、迷惑な IP トラヒックを生むような機能についていえる。このようにすれば、これらのホストは、自身の生み出す迷惑なインターネット・トラヒックに関して気をつけることになるだろう。例えば、組込み IP アドレスのもっとも一般的な用法は、よく知られた一般の Simple Network Time Protocol (SNTP RFC 2030 [4])サーバのアドレスのハード・コーディングだった。しかし、（現在の日時の概念をもち

ながらも）、これらの製品の利益を享受するのは、ほんの一部のユーザにすぎなかった。

ベンダは、迷惑な IP トラヒックを生み出すすべての機能について、オペレーター・インターフェースを提供しなければならない。その典型例として、Domain Name System の resolver は、オペレータが選択したサーバを確実に設定するとか、もしくは RFC 2132 [5]によって定義されている DHCP のような、標準自動設定プロトコルの利用か、どちらかが可能なインタフェースをもつべきだろう。オペレータのインタフェースとしては、これらの機能はデフォルトで無効とされるべきである。これらの機能を有効にしてしまうと、オペレータがその機能の存在を認識してしまうからである。つまり、問題が発生したときに、製品所有者もしくはオペレータが、問題特定やそれを緩和するという行動をとることができるからである。

インターネットホストは、要求するインターネットサービスのルータブル・IP アドレスを決定するのに、Domain Name System を使用するべきだ。しかし、IP アドレスではなく、DNS の Name を単純にハード・コーディングするだけでは万全ではない、ということに注意しなくてはならない。Domain Name Space への登録は短命でもあり、買収や訴訟といった様々な理由により、所有者を変えることができる。特定のベンダが、特定のゾーンを無期限に支配できると思ってはいけない。

インターネットホストのデフォルト設定、文書化、用例設定には、可能な限り常に、単一のグローバル･ルータブル･IP アドレスではなく、RFC 1918 [6]に規定される Private Internet アドレスを使用するべきである。

サービスプロバイダや企業のネットワークオペレータは、適切なローカルサービスのアイデンティティを通知しなくてはならない。例えば、RFC 2132 [5]に規定されている DHCP プロトコルは、問合せを要求したクライアントに対して利用できるサーバについて回答できるように、サーバを設定することができる。ローカルサービスの通知がユビキタスでなければ、設計者はセントラルサービスに頼るアドホック・メカニズムという手段をとることになるかもしれない。

例えば NTP コミュニティのように、グローバル･インターネット上で公共サービスを提供するオペレータは、サービスの IP アドレスの外部通知を廃止すべきである。これらのアドレスは短命である。従って、公共サービスのインデックスの中で広く引用されると、想像を越えて増えた負荷に対処するのに必要な、サービスの再構成をすることができなくなってしまう。

4.セキュリティ面での配慮

ホストの設定の中に、IP アドレスが組み込まれたり“ハード・コーディング”されたりしていれば、たいていは何らかのホストベースの信頼性モデルが導入されていると考えられる。また、特定のアドレスを持つインターネットホストがある意味信頼されているということでもある。ルータブル IP アドレスの役割が短命であるために、それらを製品のファームウェアやデフォルト設定に組み込むという操作は、セキュリティのリスクを引き起こす。

インターネットホスト設計者は、製品内に何らかの遠隔操作メカニズムを実装する可能性がある。

それによって、オペレータやユーザに依存することも接触することもなく、さらにはそれらを知らないままでも、インターネットホスト設定を変えることができる。これは、独自のセキュリティ問題を生む。このようなスキームが実装された場合、通知後の決定（informed decision）が行われるために、顧客やオペレーター、ユーザに対し、ローカルセキュリティやプライバシーポリシーに従って全面的に公開すべきだろう。さらに、悪意ある相手方がそのような遠隔操作メカニズムを利用して、遠隔操作スキームの潜在的利点を打ち消してしまう可能性も大きい。

5.結論

ますます多くの同じタイプのホストが導入されていくにつれて、設計者やその他のインターネットコミュニティメンバーの双方が、ホスト実装の質や再設定可能性について評価が特に重要になってくる。固有のグローバル・ルータブル IP アドレスは、ホストの固定設定の中に組み込まれるべきではない。なぜなら、そうすることで、それらの生み出した迷惑な IP トラヒックが、IP アドレス送信先の運用に問題を起こしたときに、遠隔からホストを修正することができないからである。