FMCv6 環境における課題（案）

IPv6 普及・高度化推進協議会
FMCv6 プラットフォーム WG
2013 年 2 月 15 日

目次

はじめに

IPv4 アドレスの枯渇を迎え、現在のインターネットは IPv6/IPv4 共存時代に入り、今後のインターネットの維持・発展のためには、そのインフラを支える重要な技術・資源である IPv6 の役割はますます重要なものとなってきた。

一方、利用環境に目を向けると、昨今のスマートフォンの普及に代表されるように、従来の固定環境において PC で利用する形態から、移動ネットワークや Wi-Fi を用いてさまざまなデバイスから利用する形態（マルチアクセス形態）へと大きく変わりつつある。

このような状況の中で、インターネット環境を提供するインフラ事業者及びその環境を利用して何らかのサービスを提供するプロバイダ、さらには端末ベンダー、その他関連する組織においては、従来の品質を維持しながら新しいインフラにも対応し、且つ新しい使い勝手に見合ったサービスを提供していくなど、この急激な変化に対応していく必要がある。

この IPv6 全体に関わるものやマルチアクセス環境における課題について、急ピッチでさまざまな団体などから報告がなされているが、両者共存を意識した内容については、まとまって言及されているものがなく、まだまだ深く浸透されてないものと思われる。

そこで、本 WG では、このマルチアクセスを前提とした環境において IPv6 を導入または利用する際に、どのような課題が存在するかを取りまとめることとした。

本報告書は、広く一般に公開することで、インターネットに関わるさまざまな方々の一助となることを期待する。

FMCv6 プラットフォーム WG

副査　吉井

課題1. IPv6/IPv4 品質差に関する課題

1.1. 本課題のターゲット

本課題はネットワーク、Web サービス、および端末メーカーなどのサービス提供者をターゲットとする。

1.2. 課題の解説

これまで IPv4 で問題なく利用できていた、FMC 環境でのネットワークサービスが、FMC オペレーターの固定ネットワーク側、あるいは移動ネットワーク側、あるいはその両方を IPv6 化もしくは IPv6/IPv4 デュアルスタック化した場合、サービスが利用できなくなったり、不安定になったりする場合がある。

1.3. 発生原因

IPv4 ネットワークサービスと IPv6 ネットワークサービスの品質差は、サービスが提供される区間に応じた原因、もしくはそれらが組み合わさったことから生じる。サービス区間は 3 つに大別できる。1 つ目は、サービスを提供しているアプリケーションサービスプロバイダの運用区間、2 つ目はネットワークサービスを提供しているネットワークサービスプロバイダの運用区間、3 つ目は端末を提供するベンダーである。以下、それぞれについて発生原因となりうる要因を述べる。

アプリケーションサービスプロバイダは、すでに FMC 環境で IPv4 によるサービスを提供しており、それらのサービスを IPv6 対応させることになる。すでに、アプリケーションサービス提供の基盤となるオペレーティングシステムや、ウェブサーバーなどの多くが IPv6 対応を完了しており、機能的には IPv6 サービスを構築できる状態にある。しかしながら、IPv6 での運用が始まったばかりである事、また、IPv4 のソフトウェアと比較して、IPv6 のソフトウェアがまだ未成熟であることなどの理由から、性能の最適化がなされていなかったり、また、バグなどが残っていたりといった問題が発生する場合がある。そのため、アプリケーションサービスが IPv6 に対応した場合に、利用者の視点から見て、サービスが不安定に感じられる、また、IPv4 のみを使っていたときと比較して体感できる性能が落ちていると感じられる場合がある。

ネットワークサービスプロバイダはアプリケーションサービスプロバイダとサービス利用者繋ぐインターネット回線を提供する部分であり、現在急速に IPv6 対応が進んでいる部分である。すでに、多くの大手ネットワークサービスプロバイダは IPv6 対応を完了させており、世界規模でのバックボーン回線の IPv6 化は完了していると考えてよい。ただし、アプリケーションサービスプロバイダの項で述べた通り、ネットワークサービスを提供するルーター機器の IPv6 実装に関しては、ベンダー毎の成熟度が異なる。たとえば、IPv4 と同じ機能を実装していても、あまり使われていない機能は IPv6 ではハードウェア処理がな

されていないなど、特定の場面で性能低下を引き起こす場合もある。また、IPv4 と IPv6 が異なるネットワークプロトコルであるため、ネットワークサービスプロバイダによっては、IPv4 を用いた場合の通信経路と、IPv6 を用いた場合の通信経路が異なる場合もある。この場合、一般的には IPv4 通信の方がよりよい性能を出す傾向にあるものの、過渡期では IPv6 の方がより良い性能がでていたり、また、IPv6 の通信経路が不安定だったりする場合もある。

端末の問題は、今後最もその影響が大きく現れてくる部分と考えられる。一般利用者の PC 用オペレーティングシステムに関しては、利用されているオペレーティングシステムが事実上マイクロソフトとアップルによって占められており、そのどちらもが積極的に IPv6 対応を進めているため、比較的問題が少ない。しかし、FMC 環境で主に利用されると考えられる小型移動端末については、IPv6 への対応状況がまちまちである状況である。これまで広く普及してきたクローズドな携帯電話などの機器は､そもそも IPv6 に対応していない､また今後も対応しない場合がほとんどと考えられるが、ここ数年急速に普及してきたスマートフォンに関しては、製品に採用されるオペレーティングシステムのバージョンや、インテグレートする端末ベンダーの開発力などに IPv6 機能、性能が大きく依存してしまう。これによって、サービスプロバイダやネットワークプロバイダが IPv6 対応していたとしても、端末によってはサービスが不安定であったり、性能がでなかったり、最悪の場合にはサービスそのものが利用できない事態が発生する。

1.4. FMCv6 環境に移行することによって新たに生じる課題であるか

本課題は、現在問題なく運用されている IPv4 での FMC 環境に、IPv6 サービスを追加した場合を述べているため、FMCv6 環境に移行することによって新たに生じた課題であると言える。

1.5. 確認方法

IPv6 を使うことによって発生する問題かどうかは、端末の IPv6 機能を有効/無効することによって確認できる。ただし、一般的には端末の通信プロトコルを制御できる機能は端末利用者には開放されていない事が多いため、確認は困難になると考えられる。

1.6. 対処方法

原因となる要因が、1.3 で述べたように 3 つの独立した部分に分かれているため、問題がどこにあるかを明確化し、対応する部分で対処する必要がある。

アプリケーションサービスプロバイダの問題の場合は、サーバーアプリケーションを運用しているオペレーティングシステムの IPv6 対応状況や、問題リストなどを検討し、適切なバージョンへアップグレード、あるいは独自に問題を修正するなどの対応を行う必要がある。また、サービスを構築しているソフトウェア（ウェブサービスソフトウェアなど）

に関しても、同様に IPv6 対応状況や問題リストを精査し、アップグレード、問題修正などの対応をすることになる。

ネットワークサービスプロバイダの場合は、対応部分が大きく 2 つにわかれると考えられる。ひとつはルーター機器などの IPv6 対応状況や問題リストなどの検討である。これらを調査し、サービスとして提供している部分をまかなうために十分な機能、性能が確保されているかどうかを確認し、必要に応じてアップグレードや機材の交換を検討しなければならない。もう一点は、ネットワーク構成の見直しである。もし IPv4 と IPv6 で大きく異なるネットワークトポロジーを構成している場合は、それらの間で性能の差が発生していることが考えられる。それが利用者に体感できるほどの差を生み出していたら、トポロジの再構築を含む、サービスネットワークの再設計が必要となる。

端末プロバイダの場合は、端末を設計するときの基本オペレーティングシステム選定の際に、IPv6 の対応状況や問題リストを調査し、端末が利用されるネットワークで提供されている IPv6 サービスの必要条件を満たしているかどうかを確認し、満たしていなければ、採用するオペレーティングシステムのバージョンを変更したり、場合によってはオペレーティングシステムそのものを別の物に差し替える必要もあると思われる。また、オペレーティングシステムがオープンソースで公開されている場合は、端末ベンダーの開発力にもよるが、独自の修正を加えて製品化する場合もあると思われる。

1.7. 現象

利用者から見ると、インターネットを通じて提供されているサービスにアクセスできない、一部機能が使えない、サービスの応答が遅い、サービスが不安定などの現象となって現れる。

課題2. 端末のインターフェイス優先度に関する課題

2.1. 本課題のターゲット

本課題は、ネットワーク、Web サービス、および端末メーカーなどのサービス提供者をターゲットとする。

2.2. 課題の解説

近年の無線通信デバイスの進歩により、小型移動端末が複数の通信デバイスを搭載することがめずらしいことではなくなった。一般的な端末の構成では、より広帯域な通信デバイスを用いて通信するようになっている。たとえば、3G ネットワークよりも Wi-Fi ネットワークを優先的に利用するといった実装が一般的である。しかしながら、理論的な通信速度と、利用者が実際に体感する通信速度は必ずしも一致しない。これに加えて、IPv4 と IPv6 のサービス品質の差も加わり、利用すべきインターフェイスの選択が困難な状況になっている。

2.3. 発生原因

現在提供されているデータ通信ネットワークは、そのほとんどがパケット交換による通信方式を採用しており、音声通信や以前のデータ通信で利用されていた回線交換方式と比較すると利用効率の高い運用が可能となっている。その反面、回線交換では保証されていたサービス帯域が、パケット交換では同時に利用する利用者の数や、利用者が送受信するデータ量に応じて共有されることになり、輻輳などによる品質低下が発生する。輻輳は回線交換方式でも発生するものの、回線交換の場合は輻輳時にはそもそも呼が成立しないため、実際のデータ通信に至る前に利用者が資源の枯渇に気付くことがほとんどである。これに対し、パケット交換の場合は、ネットワーク層での呼が存在しないため、接続できているように見える環境でも十分な品質を得られないという結果になる可能性がある。これは 3G など、運用者が限定されており、ある程度データ通信量の予測や制御ができる無線ネットワークでは、まだ相応の品質が保たれているものの、事業者免許不要で誰もが運用者となれる Wi-Fi ネットワークでは接続時間、接続場所、サービス運用会社によって品質に大きな差がでることになる。

2.1 項で述べた通り、一般的な端末は Wi-Fi を優先して接続するよう設定されているが、品質の悪い Wi-Fi ネットワークに接続してしまったために、逆に利用者の体感品質が悪くなってしまう場合が散見される。

さらに、「課題 1. IPv6/IPv4 品質差に関する課題」でも述べたように、利用するサービスが IPv6 対応することによって生じる品質の差も考えられるため、IPv4 では Wi-Fi ネットワークでよい体験が得られていたものの、サービスが IPv6 に対応したために Wi-Fi ネットワークが他のネットワークよりも悪い品質体験を提供するといった事態も発生する。

本来、よりよい通信品質（これは通信速度だけではなく、総合的には料金体系なども含んだものであるべきであるが）を得るために、多様な通信デバイスを用いて最適な通信路を選ぶべきところであるが、その選択が固定的かつ現実にそぐわない場合がでてきている。

2.4. FMCv6 環境に移行することによって新たに生じる課題であるか

ネットワークの輻輳による通信品質の劣化が原因で、理論的には広帯域の通信路であるにも関わらず期待通りの性能がでないという問題に関しては、IPv6 に限った話ではなく、すでに IPv4 によるサービスでも問題が発生している。しかしながら、これまで IPv4 で提供されていたサービスが IPv6 に対応したことにより、IPv4 でのインターフェイス優先度と IPv6 でのインターフェイス優先度の選択方法に差が出る可能性があり、後者の場合は IPv6 を導入したことによって発生した問題だと言える。

2.5. 確認方法

複数のネットワークインターフェイスを持っている端末で、IPv6 を無効にする操作が可能であれば、IPv6 を無効にした状態でインターフェイス毎の通信品質を比較する。その後、IPv6 を有効にした状態で同様にインターフェイス毎の通信品質を比較し、それぞれの環境でどのインターフェイスが優先的に使われているのかを確認することで、IPv4 あるいは IPv6 で適切にインターフェイスが選択されているかを確認できる。

2.6. 対処方法

この課題の要因は 2 つある。1 つ目は、インターフェイスの優先度が静的に決められており、特定のネットワークインターフェイスの実際の品質に関わらず、事前に設定されたインターフェイスの序列にしたがって、単純に接続しているかいないかで利用するインターフェイスを決定してしまうことにある。よって対処方法としては、各インターフェイスでのサービス利用時の品質を動的に計測、あるいは、ネットワーク側から品質に関するヒントを与えることによって、実際の品質に即したインターフェイス優先度を端末側に設定する技術を導入する必要がある。

2 つ目は、「課題 1.IPv6/IPv4 品質差に関する課題」で取り上げた、IPv6 導入に伴うサービス、ネットワーク、端末の品質の差によるものである。こちらは、「課題 1.IPv6/IPv4 品質差に関する課題」で提案している対処方法がそのまま応用できると思われる。

2.7. 現象

端末が、より広帯域、あるいは高品質と考えられているネットワークインターフェイスを経由して通信しているにもかかわらず、それより狭帯域、低品質と考えられているネットワークインターフェイスを利用した場合よりも実効帯域が小さかったり、体感として品質が悪いと感じたりする（遅延、揺らぎ、パケットロスが大きいなど）現象が発生する。

課題3. 複数のネットワークから同一 IP アドレスが割り当てられる課題

3.1. 本課題のターゲット

本課題は、ネットワーク、端末メーカーなどのサービス提供者、およびネットワーク管理者をターゲットとする。

3.2. 課題の解説

FMCv6 環境において移動ネットワークおよび固定ネットワークから同時に割当を受けた IP アドレスが同一であった場合、端末が意図した通信ができない可能性がある。

3.3. 発生原因

異なるネットワークを同時に利用する際に、それぞれのネットワークで IP アドレスの管理者が異なることにより、同一 IP アドレスが割り当てられる可能性がある。特に、それぞれのネットワークでプライベート IP アドレスが用いられている場合などである。また、ネットワーク・コンフィギュレーションの誤りによっては、IP アドレスの種類に依らず同じ課題が発生し得る。但し、このことを逆に利用するような通信技術もあり、これについては 3.7 項において後述する。

3.4. FMCv6 環境に移行することによって新たに生じる課題であるか

IPv4 のプライベートアドレスを使用する環境において発生し得る課題であり、IP アドレスのユニークネス(唯一性)を特徴の 1 つとする IPv6 においては発生しにくい課題であると考えられる。

3.5. 確認方法

異なるネットワークに接続される各インターフェイスに割り当てられている IP アドレスに重複がないかを、コマンドやユーティリティ・ソフトウェア等で確認する。OS の作りによっては､割り当てられた IP アドレスの重複をユーザーや管理者に警告できるものもある。

3.6. 対処方法

IP アドレスを静的に設定するシステムにおいては、IP アドレスが重複しないようにネットワーク設計を行なう。IP アドレスが動的に割り当てられるシステムであって、コマンドなどで再割り当てを要求できる場合には、それを利用して異なる IP アドレスの割り当てを試みる。これらが不可能である場合には、IP アドレスが重複するインターフェイスからの接続を、重複が無くなるまで(つまり重複する中の最後の 1 本を残して)切断する。

3.7.　現象

IP アドレスが重複した場合、適切にルーティングされないことなどによって、期待するネットワークを経由した通信が行なわれない可能性がある。また、IP アドレスが重複したケースのみならず、IP アドレスが異なっていても同一サブネット内の IP アドレスが割り当てられた場合には、適切にルーティングされないなどの上記の課題が同様に発生し得る。

3.8.　課題の応用例

3GPP で規定される IFOM(IP Flow Mobility)仕様[1]においては、同じ端末のアプリケーションが異なるネットワークに対して、あえて同じ IP アドレスを「同時に」用いて通信することを規定している。これは、各種アプリケーションの IP フロー毎に、品質要件などにしたがって最適なネットワーク(例、移動ネットワーク、WLAN 経由の固定ネットワーク、など)を使い分けたり、トラヒックの混雑などに応じて他ネットワークへオフロードしたりすることができるようにするためである[図 3-1]。

これは具体的には DSMIPv6 (Dual Stack Mobile IPv6)を用い、同じ IP アドレスである HoA(Home Address)を異なる CoA(Care-of Address)に対しても同時に登録できるようにするなどの拡張[2]によって実現される。同じ HoA を用いながらも、実際にどのネットワークを介して通信するかは、Binding Cache[表 3-1]と呼ばれる IP フロー毎の CoA との紐付けを管理するテーブルによって決定される。

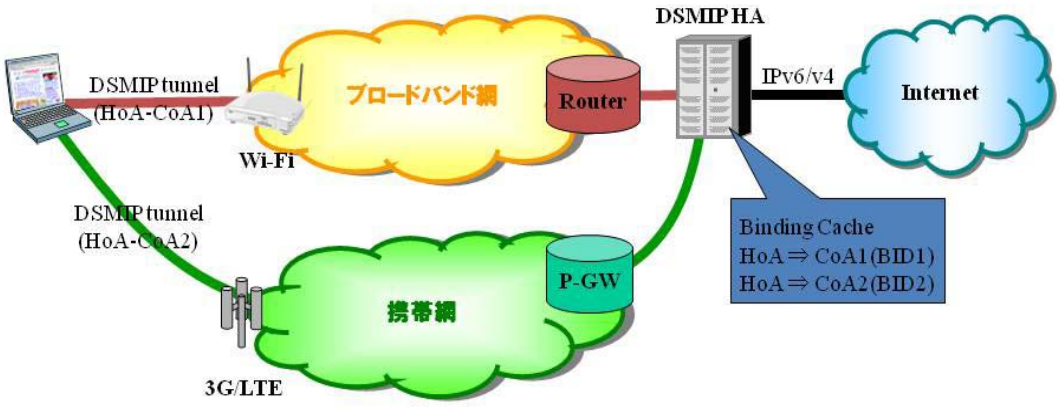

図 3-1. 異なるネットワークを介した同時通信の例

表 3-1. Binding Cache の例

Home Address	Routing Address	Binding ID	Flow ID	Routing Filter
HoA1	CoA1	BID1	FID1	Description of IP flows…
			FID2	Description of IP flows…
HoA1	CoA2	BID2	FID3	…

3.9. 参考文献

[1] 3GPP TS 23.261: “IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2”

[2] IETF RFC 5648 (October 2009): “Multiple Care-of Addresses Registration”

課題4. IPv6 のプッシュ通信に関する課題

4.1.　本課題のターゲット

本課題は、ネットワーク、Web サービス、および端末メーカーなどのサービス提供者をターゲットとする。

4.2.　課題の解説

IPv6 アドレスのグローバル性を利用して 1 端末に 1 つのグローバル IP を付与することで実現する、利用者端末への Push 型通信、Push 型アプリケーションは、中継ルーターや宅内ルーター等に IPv6 Firewall が適用されている場合には、経路途中で廃棄され正常に利用できない。

一方で同じ利用者端末を別の事業者（アクセス回線）に接続すると、IPv6 Firewall のポリシーの相違から正常に利用できる場合がある。

4.3.　発生原因・課題の分析

【宅内固定環境】

宅内ルーターや利用する端末において利用者が Firewall のポリシーを設定して所望のアプリケーションを Push 利用できるように設定することもできるが、通常の利用者は初期設定状態で利用することが多く、入力が困難な Firewall 設定を変える機会はまれであるため、その事象を解決し難い。

【移動環境】

スマートフォンやタブレット端末、モバイル PC の普及に伴い、異なる環境のアクセス回線や異なる事業者を利用していつでもどこでもネットワーク・コンテンツに接続できる環境となっているが、各アクセス回線、各事業者のセキュリティポリシーが異なるため、環境によって疎通する通信と遮断する通信が発生する。

4.4.　FMCv6 環境に移行することによって新たに生じる課題であるか

IPv4 の場合は、通常プライベートアドレスを利用する場合が多く、Push 型通信、Push 型アプリケーションは DDNS 等、多くは各サービス事業者主導で対策が施されている。

IPv6、および IPv6/IPv4 デュアルスタックにおいても同様に DDNS 等の手段を用い各サービス事業者主導で対策を施す必要があるという面では、IPv6 特有の事象ではない。

しかし、IPv6 ならではの世界観（IPv4 とは異なる）に立つと、IPv6 グローバルアドレスで唯一無二に識別できるものに対しても DDNS を使用する必要があるという観点では、IPv6 特有事象である。（IPv4 ではプライベートアドレスや動的に付与されるアドレスに直

接アクセスできないという問題を解決するための DDNS 等の利用であった）

4.5.　確認方法

アプリケーション、ISP、アクセスネットワーク、宅内ルーター、利用端末と、Firewall 等の利用制限を行いうる箇所は多岐多様にわたるため、事前に発見することはきわめて困難である。

また、Firewall の初期設定状態も技術に精通していない一般利用者から見るときわめて困難であり、初期状態で利用できないとすると、その状態が変更できないものと感じられる。

4.6.　対処方法

【固定環境】

①Push 通信を受けたいアプリケーションにたいして、ユーザー主導で簡易に利用できる仕組み（ワンクリックで該当通信の穴あけ等）

【移動環境】

②モバイル IP 等のようにアドレスが変更してもホームアドレスが変更しない仕組みの導入

・利用者はホームアドレスを管理する事業者のポリシーに従えばよい

【共通】

③IPv6（IPv4 デュアルスタックを含む）における Push 通信に対する考え方を業界横断的に整理する

・Push アクセス方法のデファクトスタンダート化

④準リアルタイム Pull 方式による Push 方式の代替

・Pull 間隔を短くすることによる擬似 Push（ただしネットワーク・サーバー負荷が増大）

⑤携帯端末との連動による解決

・携帯電話の Push 通信機能を利用して、利用者の携帯端末と利用者端末とを連動させることで解決

4.7.　現象

【固定環境】

IPv6、IPv4 を利用した Push 型のアプリケーション（たとえばリモートカメラやリモートデスクトップなど）を利用する場合、宅内ルーターや利用端末の IPv6 Firewall 設定によって利用できない。結果、IPv6 のグローバル性を活かしたサービスが創出されない。

【移動環境】

IPv6、IPv4 を利用した Push 型のアプリケーション（たとえば何らかのお知らせ通知など）を利用する場合、アクセス事業者などのセキュリティポリシーによって、サービスを

受けられる場所と受けられない場所が発生してしまう。利用端末は自動的にアクセス回線に接続する例が多いため、利用者が知らないうちにサービスが途中で利用できない状況が発生する。

課題5. 端末の挙動に関する課題

5.1. 本課題のターゲット

本課題は、ネットワーク、Web サービス、および端末メーカーなどのサービス提供者をターゲットとする。

5.2. 課題の解説

2010 年度の検証で確認したスマートフォンで名前解決とアクセスの通信が別のインターフェイスを使うといった特殊な挙動をする場合、ネットワーク事業者やコンテンツ事業者が意図しない通信となる可能性がある。

具体的には、以下図のような環境下において観測された。

図 5-1. IPv6/IPv4 環境におけるスマートフォンの挙動例

図 5-1 は、3G ネットワーク側は IPv4 のみの接続環境で、Wi-Fi ネットワーク側が IPv6 のみの接続環境であることを示す。

この時スマートフォンは、名前解決時 3G ネットワーク側で名前解決を行い、AAAA レコードが返ってきた場合は、Wi-Fi ネットワーク側で通信を行うような挙動を示している。

このような事象が生じた場合、例えばインターネット側でコンテンツフィルターを実施した DNS を準備していたとしても、3G 回線側の DNS で期待したフィルターがなされていないようなケースでは、完全なフィルターが施せない結果となってしまう恐れがある。

また、インターネット側のオペレーターからは名前解決に関わる通信が見えないことから、画面上の一部のみ表示されないといった何らかの不具合発生時、DNS の問い合わせに失敗しているのか、それとも端末が受け取って動作しないだけなのか等、切り分けが困難になることが想定される。

5.3. 発生原因

これは、スマートフォンが複数のインターフェイスを同時にアクティブ状態で使用することができ、また、IPv4 と IPv6 を判別して、通信インターフェイスの優先度を決めるロジックがこの状態で併用されることで発生する可能性がある。

5.4. FMCv6 環境に移行することによって新たに生じる課題であるか

IPv6 が利用されるような環境になると、スマートフォンは、3G、Wi-Fi のどちらを利用すべきかを選択することに加え、IPv4 か IPv6 かを選択できることになり、新しくこのようなケースに気をつける必要がある。

5.5. 確認方法

① 図 5-1 のような環境を構築する。
② AAAA レコードを持つ URL へアクセスする。
③ ゾーンの DNS の履歴や Wi-Fi 側モニター結果を照らし合わせ、アクセスが存在したかチェックする。

5.6. 対処方法

3G 側とインターネット側のポリシーを出来る限り合わせる必要がある。

また、何らかの切り分け確認が必要なときは、Wi-Fi 側のモニターで DNS クエリパケットが存在するかを必ずチェックする。

課題6. サービスサイトにおいてIPv6とIPv4でコンテンツが異なる課題

6.1. 本課題のターゲット

本課題は、Webサービス提供者をターゲットとする。

6.2. 課題の解説

IPv6とIPv4の両方に対応するサービスとして提供されていても、IPv6アクセスとIPv4アクセスで得られる結果が異なる場合がある。

具体的には、IPアドレスのロケーション情報を利用しているサービスサイトや、Webアプリケーションのコンテキスト情報をサーバー側に保存するサービスサイトにおいて、ユーザーが利用するFMCv6環境に依存して表示されるコンテンツが異なる事象が挙げられる。

ただし、IPv6サービスまたはIPv6/IPv4サービスを既存のIPv4のみのサービスと別ドメインなどで提供している場合は、本課題には含まない。

6.3. 発生原因

① IPv6対応方法に起因する場合

サービスサイトのIPv6対応には大きく分けて3つの方法が考えられる。1つ目は、既存のIPv4コンテンツサーバーをIPv6/IPv4両方に対応するデュアルスタック化することである。2つ目は、既存のIPv4コンテンツサーバーはそのままで、IPv4とIPv6を変換するトランスレーターを追加することである。3つ目は、同じく既存のIPv4コンテンツサーバーはそのままで、新規にIPv6コンテンツサーバーを追加することである。

上記の3つ目の方法でIPv6対応しているサービスサイトでは、IPv6コンテンツとIPv4コンテンツを別の筐体やインフラで提供しており、このような環境でIPv6サーバーとIPv4サーバーのデータの連携やセッションの同期が適切に行われていない場合に発生する可能性がある。

② コンテンツ判定方法に起因する場合

サービスサイトによっては表示するコンテンツをIPアドレスでユーザー端末の所在地域を判定し変更することがある。しかしながら、IPv4とIPv6ではIPアドレスの割り当てポリシーが異なるため、このようなIPアドレスを利用しコンテンツ内容を変更するサービスサイトにおいて差異が発生する可能性がある。

6.4. FMCv6環境に移行することによって新たに生じる課題であるか

サービスサイトをIPv6対応する際に気をつけなければならないポイントとして一般的に

認識されている。特に FMCv6 環境では、固定環境と異なり Web サイトの次ページへ移動するまでのごく短い期間であっても同一端末で同一サービスを使用していてもサービスサイトへのアクセス環境が変化してしまうため、本課題が発生する可能性が高くなっていると考えられる。

6.5. 確認方法

複数のネットワークインターフェイスを持つ端末を、少なくとも一つは IPv6 に対応した 3G/WiMAX/LTE などの移動ネットワークと固定ネットワークに接続し、対象のサービスサイトを表示する。その後、最初に接続したネットワークから切断し別のネットワークに接続した後に、対象のサービスサイトを再度表示する。ここで表示されたコンテンツが同一であるか、同一でないかにより確認することができる。

6.6. 対処方法

サービスサイトの IPv6 対応において十分に対応方法を検討し、適切な方法を選択することが必要である。

具体的には 6.3 項に記載した 1 つ目のデュアルスタック化する方法、または 2 つ目のトランスレーターを追加する方法によりデータの連携やセッションの同期が容易になる。また、IPv6 コンテンツと IPv4 コンテンツを別のサーバーで提供しているサービスサイトにおいても、アクセス環境の変化に依存せず同じ IPv6 または IPv4 プロトコルを使い続けることが可能なコンテンツの構成にすることなどが考えられる。

課題7.セキュリティに関する課題

7.1.　本課題のターゲット

本課題は、ネットワーク提供者をターゲットとする。

7.2.　課題の解説

FMCv6 環境では悪意あるユーザーが、多数の送信元アドレスを渡り歩けることで、フィルタリング（ACL など）や迷惑メール対策（グレイリスティングなど）が有効に機能しない可能性がある。以下 ACL、DNSBL、グレイリスティングについて検討した。

機能の整理

①ACL

ユーザー毎にアクセス出来るサーバーやネットワーク、ファイルなどの IP アドレスを登録しアクセス制限をする。

②DNSBL

迷惑メール送信メールの IP アドレスをブラックリスト化、DNS を利用して参照する。

③グレイリスティング

Bot からの迷惑メールは再送されない前提で、初めてメールを受けるホストからの受信を一度拒否。IP アドレスをグレイリストに登録。再送してきた場合は正規のメールサーバとして受信。IP アドレスをホワイトリストに登録。

今後の記載において、共通に適用できる項目は上記３機能の区別をしていないが、特有の注意事項がある場合は、その旨記載するようにしている。

これらの機能において、IPv4、IPv6、固定環境、移動環境といった形でアドレス環境が変化し、それぞれに対して IP アドレスが付与される事を想定すると、処理すべきアドレス数が飛躍的に増大する事が想定され、このことにより種々の課題が発生する。

IP アドレスの増大を考える際に以下のような簡単な想定をした。

【想定】

グローバル IP アドレスを考慮した場合、IPv4 アドレスに加え、アドレス長が（例えば）４倍になる IPv6 アドレスが加わる。また、これに固定端末で割り当てられるアドレス、移動端末に割り当てられるアドレスがあるため、ブラックリスト化する IP アドレスの量が多大になる。現状使用している IPv4 固定アドレスのデータ量の指標を１００とすると次のように想定される。（固定 IPv4：１００、固定 IPv6：４００、移動 IPv4：１００、移動 IPv6：４００）

単純に仮定するとデータ量は、IPv4 固定ネットワークだけの場合の１００に対して１，０

００と１０倍になる。この結果、DB 拡張、処理能力の確認が必要となる。

7.3. 発生原因

単一ネットワークの場合は、IP アドレスも単一であるが、FMCv6 環境においては、考慮すべきネットワークが複数になる事、端末が複数のアドレスを持ちうる事などから、管理すべき IP アドレスが増加する。IP アドレスの増加に伴い、悪意のあるユーザーは複数の IP アドレスを渡り歩くことが出来るため、セキュリティ上の脅威は増大する。ユーザーにとっては、悪意のあるユーザーからの攻撃を防御する必要があるため、制限する IP アドレスの管理に関わる工数の増加や管理すべきアドレスの領域が不足する事が想定される。

7.4. FMCv6 環境に移行することによって新たに生じる課題であるか

本件は、アドレス管理の問題で IPv4 と IPv6 の環境となった事により発生する課題ではない。また、固定、移動の異なる環境になる事によって発生する課題でもない。このような、アドレスの管理は IPv6 でも発生するが、IPv4 と IPv6 両方に対して制限が必要な為、問題が複雑化する。

7.5. 確認方法

制限する IP アドレスの個数をシミュレーションする。運用時には IPv6 の制限リストがどの程度あるか想定する事が難しい為余裕を持った設計が必要となる。

グレイリスティングにおいては、新規のアドレスについてのグレイリスト登録が発生するため、トラヒック増についてもシミュレーションする必要がある。

7.6. 対処方法

- アドレス空間の確保

  アクセス制限を行うためのアドレス空間の領域の増加を考慮する必要がある。十分な領域を確保している場合は問題ないが、少ない領域で運用している場合には、新たな領域の確保が必要となる。また、制限するアドレス数が増加するため、処理能力に課題が出る可能性もある。必要に応じて処理能力の増強も考慮する。

- 回線増強についての検討

  グレイリスティングにおいては、上記に加えて場合によっては回線増強が必要となる。

- 管理の自動化

  IPv6 アドレスについては登録作業を人手により作業している事が殆どと思われる。ツールの問題ではあるが登録・管理のツールが早急に整備される事が望ましい。

- アドレス集約化の工夫

  今まで述べてきた内容は全ての端末にグローバルアドレスを配布した事例であるが、アドレスの集約化などにより、管理 IP アドレスの増大を抑制する事も有効な方法である。

7.7. 現象

悪意あるユーザーが多数の送信元アドレスを渡り歩くため、IP アドレスのフィルタリングが間に合わず迷惑メールが送りつけられる、禁止されているサイトへのアクセスが可能となるなどの現象が現れる。また、処理能力、メモリ容量オーバーの場合は通信が不可能、悪意のあるユーザーに対する防御が出来ない状態が、装置の改修まで継続する事もある。

7.8. 参考文献

[1] IPv6 時代の迷惑メール対策（2011 年 5 月 27 日）
迷惑メール対策委員会委員長／IPv6 ディプロイメント委員会委員

課題8. アドレス割当/フォールバックの実装が統一されていないため発生する課題

8.1. 本課題のターゲット

本課題は、ネットワーク、および端末メーカーなどのサービス提供者をターゲットとする。

8.2. 課題の解説

スマートフォンなどで IPv6 に関連する必須仕様や拡張仕様などの要求仕様がないため、アドレス自動設定やフォールバックなどの動作が異なる。このためネットワーク事業者やサービス事業者が意図しない通信とならないようにするため、多数の仕様の組み合わせに対応したサービスを提供する必要がある。

8.3. 発生原因

スマートフォンなどの一部の OS の IPv6 アドレス自動設定では、ステートレスな設定方法のみが実装されている。このような OS を使用している端末を IPv6 の接続性のみが提供されているネットワークに接続した場合、ステートレス DHCPv6 でネームサーバーの設定ができないため名前解決を行うことができなくなる。また同様に、ステートフル DHCPv6 でアドレス割り当てができないため、相手の IPv6 アドレスが分かっており名前解決が不要だとしても通信することができなくなる。

さらに、IPv6 と IPv4 のどちらを優先して使用するか、優先して使用されるプロトコルの接続性に問題があったときのフォールバックの挙動についても、現在は端末の実装に依存している。このためコンテンツが表示できるかできないか、表示されるまでの遅延時間など品質がバラバラとなってしまっている。

8.4. FMCv6 環境に移行することによって新たに生じる課題であるか

IPv4 のみの環境ではアドレス、デフォルトルートおよびネームサーバーなどの自動設定に使用される技術は DHCP のみであったが、IPv6 対応の環境ではアドレスとデフォルトルートの自動設定で使用される技術は RA が、アドレスとネームサーバーの自動設定で使用される技術は DHCPv6 がある。また、IPv6 の自動設定に関する技術は近年でも新しい標準の策定が進められており、RA にネームサーバーの通知オプションが追加されるなど複雑さは増していると言える。このことより IPv6 を使うことで新たに生じた課題であると言える。

さらに、FMCv6 環境では固定ネットワークおよびモバイルネットワークをユーザーの状態に合わせて頻繁に変更することが想定される。例えば、歩行移動中に様々な Wi-Fi が使用できたり、LTE/WiMAX/3G の中で使用可能なネットワークを使用したりする。このため、

FMCv6 に移行することにより発生が顕著になる課題と言える。

8.5. 確認方法

FMCv6 環境で主に使用されるスマートフォンを以下の①～④のネットワークで使用することにより確認できる。

① RA によるステートレスアドレス自動設定のネットワーク
② ステートレス DHCPv6 のネットワーク
③ ステートフル DHCPv6 のネットワーク
④ RA によるステートレスアドレス自動設定とネームサーバーが通知されるネットワーク

例として、一部のスマートフォン OS ではステートレス DHCPv6 に対応していることが確認できる。また、他のスマートフォン OS ではステートレスアドレス自動設定に対応していることが確認できる。

8.6. 対処方法

現在は、IPv6 対応のネットワーク事業者は提供するネットワークサービスに応じた端末をエンドユーザーに提供することで対処している。IPv6 対応の各端末メーカーはネットワーク側の仕様を想定し実装を行っている。

今後は、複数のネットワーク事業者および複数の端末メーカーが一体となり端末の必須仕様および拡張仕様を決めることで、FMCv6 環境での動作を保証することに加え開発・検証時間の短縮を実現することが可能になる。

8.7. 現象

IPv6 に対応した端末 A であっても、IPv6 対応ネットワーク B では IPv6 で使用できていたサービスが IPv6 対応ネットワーク C では IPv6 で使用できなくなることがある。

例えば、端末 A とネットワーク B ではステートレスアドレス自動設定とステートレス DHCPv6 のみの対応で、ネットワーク C ではステートフル DHCPv6 のみの対応で合った場合に発生する。

課題9. 管理系の課題

9.1. 本課題のターゲット

本課題は、ネットワーク提供者をターゲットとする。

9.2. 課題の解説

これまで IPv4 で構築してきたネットワーク環境、サービス環境において、構築作業や運用作業の簡素化、省力化、自動化を目的に、IPv4 アドレス体系を前提としたスクリプトツールや外部から制御を行うソフトウェアを作成、活用した運用が主体となっている。

IPv6 化に伴い、ネットワーク機器やサービスを提供するサーバー群のみならず、これら運用作業のためのツールや外部から制御を行うソフトウェアの IPv6 対応も避けられない。また IPv6 移行期においては、IPv6/IPv4 混在の環境も存在し、両方の IP バージョンに対応したツールや制御ソフトウェアの整備が必要となる。

この課題は通信事業者、サービスプロバイダ、企業ネットワークなど IPv6 化を行ううえで共通の課題であり、IPv4 と同等レベルの品質、コストで「管理」「運用」するためには、考慮すべき課題である。

IP アドレスをベースとした制御系の具体例としては以下のようなものがある。

① IP ACL

今日では、IP アドレスを用いた ACL はアクセス制御のみならず、ポリシーベースルーティング（PBR）、フィルターベースフォワーディング（FBF）とネットワーク内の基本的な経路制御でも一般的に使われている。

【IPv6 化による課題】

従来、IPv4 ベースで構築したネットワークにおいて、これらの PBR や FBF は経路設定も複雑化してしまい、access-list 内の IP アドレスをスクリプトやコンフィグレーションを事前または自動で生成し、対象となる機器へ設定する運用が行われる。特に企業間接続や複数のネットワークを集約する基幹ルーターなど、経路が多く且つサービス断による影響が多い接続ポイントは PBR、FBF を活用した経路設定を多く用いた運用、管理を行う。

IPv6 化に伴い、対象となる機器のバージョンアップのみならず、これらの運用で使用するスクリプトツールやコンフィグレーションも IPv6 化作業を行う必要が生じる。

② 再帰 ACL(Reflexive ACL)、コンテキスト ACL

再帰 ACL やコンテキスト ACL は上位層のセッション情報に基づいて IP レベルの制御（フィルタリング）する手法で、主にネットワーク内部から発生する IP トラヒックに対して上位層のアプリケーションを意識した下りトラヒックを制御（フィルタリング）に

用いられる。

これらは、ネットワーク内部から発信する端末の IP アドレスをベースに利用するアプリケーションに応じた制御を実現している。

【IPv6 化による課題】

上位層のセッション情報を基にした制御であり、アプリケーションレベルで使用する IP アドレスをキーとした動的制御が中心となる。これらの運用を自動化するツールでは、外部のデータベースやアプリケーションサーバーとの連携をスクリプトなどを用いて自動化し運用の簡素化を図っている。

IPv6 化に伴い、対象となる機器のバージョンアップやアプリケーションサーバーの対応のみならず、これらの運用で使用するスクリプトツールやコンフィグレーションも IPv6 化作業を行う必要が生じる。

③ SLA

IP ACL を用いた PBR、FBF や再帰 ACL、コンテキスト ACL など、IP アドレスに依存するサービス制御が一般化している現状で、サービスレベル管理や障害検知、障害時の経路変更を行おうとすると、必然的に上位レイヤの情報を基に制御、管理を行うこととなる。

この場合、ルーターの IP SLA やサービスレベルを監視する外部のツールを用いたサービストラッキングが重要となり、その多くがサービスを確認するロジックを組み込んだスクリプトで障害を検出し、障害時の経路変更を自動的に行っている。

【IPv6 化による課題】

このようにアプリケーションレベルで使用する IP アドレスを用いたサービスレベルの正常性を確認するスクリプトや外部のソフトウェアも IPv6 化する際には変更する作業が生じる。

④ 障害ログ解析

障害時のサービス影響を最小限にとどめるため、IP アドレスを用いたサービストラッキングや自動発報による障害検知や、影響範囲を即座に知るため、影響範囲の情報（セグメント情報や IP アドレスレンジなど）を含んだログ情報を基に解析を行う。

【IPv6 化による課題】

これらのスクリプトやコンフィグレーションも IPv6 化に伴い変更作業が生じる。また固定 IP アドレスでアクセス先を固定している運用も多数あるなか、IPv6 を手作業で設定する場合の運用コストは膨大になるだけでなく、設定ミスなどによるサービス品質の低下は免れない。

⑤ アクセス情報、課金情報

不正アクセス時のアクセスログ解析や、第三者機関からの照会などサービスを提供するうえで必要なアクセス解析も IP アドレスをベースとした解析が発生する。

また、課金情報も IP アドレスをベースとしたセッション情報をもとに記録、課金情報と

して利用する場合もある。

【IPv6 化による課題】

障害解析や課金情報の取得など、日々の運用、管理のなかで迅速かつ確実に作業を行う必要がある業務において、IPv6 化は作業の煩雑化だけでなく、IPv6 化による複雑化という課題も生じる。

特に障害解析では、原因の特定や影響範囲が直感的わかりやすい IPv4 での運用に対して、IPv6 アドレス体系では、直感的な判定は不可能に近く、管理表などを用いた運用が必須となり、運用方法そのものに影響を与えてしまう。

9.3. 発生原因

IPv6 化に伴うスクリプトツール、ソフトウェア、さらにはオペレーションそのものの見直しは、直接的な技術課題として発生するものではない。

9.4. FMCv6 環境に移行することによって新たに生じる課題であるか

通信事業者、サービスプロバイダ、企業ネットワークの管理者は、これまで IPv4 で構築してきたネットワーク環境、サービス環境において、構築作業や運用作業の簡素化、省力化、自動化を目的に、IPv4 アドレス体系を前提としたスクリプトツールや外部から制御を行うソフトウェアを作成、活用し、安定したオペレーションを確立してきた。

「IPv4 既存サービスの継承」という目標からすると、IPv6 を使ううえで避けられない課題であり、過去から蓄積したツールやノウハウという運用資産に対して新たに生じる課題である。

9.5. 確認方法

課題の解説に記載した IP アドレスをベースとした制御系の具体例については、IPv6 化のネットワーク設計段階で変更箇所を、事前に確認することが可能である。

しかしながら、スクリプトツールや外部からの制御に頼るソフトウェアなどサービスレベルで総合的な対処が必要となり、これらを網羅し事前確認するには膨大な時間と労力を要する。

9.6. 対処方法

以下のような手法が考えられる。

- IPv6/IPv4 トランスレータを最大限活用し、IPv6 サービスに直接関与しないネットワーク機器、サーバー群は極力、既存 IPv4 環境のまま利用する。
- IPv6 への移行期に、デュアルスタックを前提としたネットワークを構築し移行期間中は IPv4 運用方法をそのまま利用。IPv4 運用方法をそのまま継承した確実なツールの整備などを平行して行い、運用レベルの統一、サービス品質を確保する。

9.7. 現象

IPv6 への移行において、IPv4 の運用ツールや運用方法を継承できなければ、サービス品質の低下を招くこととなる。

また、スクリプトなどのツールやソフトウェアの変更には膨大な作業が伴い、また、障害時のログ解析など運用が定着するまでには膨大な時間と労力を要する。

あとがき

FMCv6 プラットフォーム WG では今年度 FMCv6 に特化した環境における課題を取り上げ、既に実環境で起こっている事象および今後発生すると見込まれる事象について、より具体的な例を示しながら、課題の解説、原因、確認、対処、現象といった観点で本レポートに纏めた。

課題解決に向けて、アプリケーション、ネットワーク、端末といった分野で個々に対処するのみならず、業界横断的に解決の道しるべを示すことが益々重要となり、タイムリーに検討結果を公開することの意義を感じている。

FMC や IPv6 に携わる皆さんが初期段階からこれらの課題を認識し、その解決に向けてトライアンドエラーを繰り返しながらノウハウを蓄積することにより、世界に先駆けて FMCv6 プラットフォームの構築を実現する一助になれば望外の幸せである。

FMCv6 プラットフォーム WG

主査　野寺

検討メンバー

	氏名	所属
主査	野寺 義彦	ソフトバンクモバイル株式会社
副査	吉井 裕重	ソフトバンクテレコム株式会社
会員	島　慶一	株式会社インターネットイニシアティブ
	酒井 琢夫	ソフトバンクテレコム株式会社
	早田 叔弘	ソフトバンクテレコム株式会社
	黒川 英貴	ソフトバンクモバイル株式会社
	横田 大輔	ソフトバンクモバイル株式会社
	藤城 誠士	株式会社日立製作所

敬称略、主査、副査および会員の社名順にて記載