■3 群（コンピュータ -ソフトウェア）－ 3 編 ネットワーク層

2 章 IPv6（Internet Protocol version 6）

（執筆者：宮川　晋）［2015 年 4 月 受領］

■概要■

IPv6 とは，Internet Protocol version 6 の略であり，インターネットにおいてその通信プロトコルとして長らく使われてきている IPv4 に用いられるアドレスが枯渇してきていることから，その抜本的な対策として，インターネット技術の標準化機関 IETF（Internet Engineering Task Force）により規定された新しいインターネットプロトコルである．

■3 群 － 3 編 － 2 章

2-1 IPv6 誕生の背景と現在

（執筆者：宮川　晋）[2015 年 4 月 受領]

IETF が 1995 年に発行した RFC1752 “The Recommendation for the IP Next Generation Protocol” の Section 5.1 には, ALE WG の結論として “the Internet would exhaust the IPv4 address space between 2005 to 2011（インターネットは IPv4 アドレスを 2005 から 2011 の間に使い尽くすだろう）”と記述されている．この 20 年ほど前の予測は結果としてほぼ真実となり, 2013 年現在, インターネットでは IPv4 アドレスの新規ブロックはほぼその割当てを終了していることを背景に，実際のインターネットにおいての IPv6 の本格的な展開が進行している．具体的には，インターネットで用いられる通信機器であるルータやファイアウォールなどにおいてすでにデフォルトの機能として実装され，かつ，Windows や Mac，Linux や BSD といった OS では標準機能として搭載されるようになっており，また，世界中の ISP や携帯サービス各社から IPv6 接続サービスが提供されはじめているのと同時に，例えば Google や Facebook などのサービスが全面的に IPv6 対応になったこともあり, 着実にその利用も進んでいる状況である．最近では，IPv4 と IPv6 を同時に利用できるように端末のネットワークをコンフィギュレーションしておくと，v6 に高い優先順位があるために，ユーザがその利用を気が付かずに Google などのサービスを利用するかたちとなるため, 現代的なインターネット技術者としてはその理解，および，きちんとした使いこなしがセキュリティ確保のためにも重要なプロトコルである．なお，紙幅の関係から，IPv6 のプロトコルに関する詳細にわたる解説は，後述するリファレンスにあげる，その規定文書である RFC や参考文献，各種プレゼンテーションをご覧いただくこととして，本稿では，その規定方針の哲学（なぜそう決まったか）や，最新のアップデートにおける注意点など，既存の教科書やなどにない点を中心とする．

■3 群 － 3 編 － 2 章

2-2 IPv6 プロトコルの設計方針

（執筆者：宮川　晋）[2015 年 4 月 受領]

1990 年代当初に始まった IPv6 の設計作業の方針としては，元々の最大の目的であった

(1) アドレス空間を拡大すること，すなわち IPv4 の 32 ビット幅アドレスから 128 ビット幅アドレスへと拡大

という点のほかにも

(2) IPv4 のフォーマットを整理し，不要なフィールドや機能を削除

(3) 複数ヘッダを許容し拡張性を確保

(4) フローラベル機能とその活用

(5) IPsec による認証とセキュリティのデフォルト化

などがもたらされる計画であった．2014 年現在，実際に実装も計画通りに進行した部分も多いのだが，オリジナルの設計方針には，いくつかの課題があることが指摘されており，プロトコル自体の修正も行われているため，本稿では，現在進行中の議論も踏まえて記述する．

■3 群 － 3 編 － 2 章

2-3 IPv6 のアドレス体系

（執筆者：宮川　晋）[2015 年 4 月 受領]

IPv6 の最大の眼目は，IP アドレス空間の枯渇対策であったため，当然のこととしてアドレス空間が拡大された．議論はいろいろあったが結局，IPv4 の 32 ビット幅から 128 ビット幅へと拡張が行われた．すなわち IPv4 アドレス全体に比較してその 2 の 96 乗倍というまさに天文学的な大きさのアドレス空間がもたらされたことになる．また IPv6 では単なるアドレス幅の拡張のみならず，アドレスの考え方の整理，変更が行われている．

2-3-1 IPv6 のアドレスの表記方法

IPv4 アドレスは，32 ビットの幅であり，それにはいくつかの表記法があるが，広く利用されている方法として，32 ビットを 8 ビットずつに区切り，その一つ一つを 0 から 255 までの 10 進数で表し，それを「.（ドット）」で区切る表記方法（例えば「127.0.0.1」は「01111111 00000000 00000000 00000001」を表す）が利用されているのに対し，IPv6 では，その 128 ビット幅のアドレスを 16 ビットずつに 8 分割し，それぞれの 16 ビットのフィールドを四つの 0 から f までの 16 進数字で表記してこれを「:（コロン）」で連結する方法がとられる．例えば，2001:0db8:0000:0000:0000:0000:0000:0001 というかたちとなる．IPv6 ではこのような表記方法を利用するときに特にサブネットプレフィックスに 0 が多数連続して並ぶことが多くなることから，（a）各 16 ビットフィールドに現れる先行する頭の 0 を省略してよい（ただし必ず一つは数字が必要）また（b）16 進数の数字における 0 あるいは連続する 0 を一か所だけ::で置き換えるという省略記法を利用できる．すなわち上記の例を（a）のルールに当てはめると 2001:db8:0:0:0:0:0:1 となり，（b）のルールも当てはめてみると，2001:db8::1 と書くこともできることになる．この省略記法ルールの適用次第で，一つのアドレスに複数の書き方が可能になることから，オペレーションの観点からエラーを減らすためにも一意に省略方法を決めるやり方があるとよいという考え方に基づき，RFC5952 が制定されている．

IPv6 で，サブネットを定義する際には，上位から連続したサブネットマスクのみを利用する CIDR 形式のみが許されることとなり，サブネットマスクという用語ではなく，特にサブネットプレフィックスと呼ぶこととなった（ちなみに IPv4 でも実用上は CIDR のみが運用されており，実際には規格上では利用できることになっていたビットが不連続のサブネットマスクが利用されることはない），アドレスの後に「/（スラッシュ）」と 10 進数によるプレフィックス長を付与してサブネットプレフィックスを明示することができる．例えば，2001:db8::/64　とは，2001:db8:0:0 の 64 ビットのプレフィックスを意味する．アドレス自体が 16 進数を利用して表記されるのに対して，同時に利用されるプレフィックス長は 10 進数で表されるために混乱しがちになることに注意する．例えば 2000:/3 とは，2 進数で表記したときに 0010 か 0011 のどちらかで始まるアドレスということになるが，これはすなわち 16 進数によるアドレス表記において“2”で始まるか“3”で始まるかのどちらかになる．

2-3-2 IPv6 のアドレスの考え方

IPv6 で非常に大事な整理として，IPv4 では時に曖昧であった，「アドレスは何に付与されているのか」ということが，はっきりと「アドレスはインタフェースに付与されるもの」と定義されたことがあげられる．バージョンに寄らず IP におけるサブネットモデルでは，アドレスを上位のサブネットプレフィックスと，それ以外の下位部を分離して考えるが，IPv4 では下位部を「ホスト部」(Host Number) と呼ぶのに対し，IPv6 では「インタフェース ID（Interface ID）」と呼ぶことになっており，明確にインタフェースにアドレスが付与されるものと意図されていることが理解できる（ホスト実装における Strong Host Model と Weak Host Model という議論と関係しているが，ここでは紙幅の関係からこれ以上は立ち入らない）．

IPv6 では（IPv4 でもいくつかの種類のアドレスが規定されているように），まず以下の二種類のアドレスが規定される．

・ユニキャスト（Unicast）

・マルチキャスト（Multicast）

IPv4 で用いられるブロードキャスト（Broadcast）は使用されない代わりに，いくつかのマルチキャスト，例えば，All Nodes Multicast や All Routers Multicast といったマルチキャストを使用する．初期の定義では，エニーキャスト（Anycast）アドレスの空間を独立に定義するとしていたが，その後の議論により，現在は（IPv4 と同様に）ユニキャストアドレスをエニーキャストに利用することを可能として専用のアドレス空間の規定は行われていない．

IPv6 アドレスのアドレスには IPv4 ユニキャストでは用いないスコープ（Scope）の概念があり（ちなみに IPv4 マルチキャストにはスコープの概念がある），基本的なスコープとしてリンクローカルとグローバルの二つが存在している．それぞれの定義は以下のとおりである．

・リンクローカル（link-local）：そのインタフェースが接続しているリンク内のみで一意に定義されるアドレス：fe80::/10

・グローバル（global）：全世界で一意に定義されるアドレス：（現在のところ）2000::/3

ここで，グローバルは IPv4 と同じに考えればよいので明快だが，リンクローカルは IPv4 では用いられない概念なので注意が必要である．リンクとは，インターネットプロトコルの階層モデルにおける Layer3 層である IP 層の下に位置する Layer2 層におけるリンクの意味であり，例えば，そのインタフェースがイーサネットインタフェースであるときは，そのインタフェースが接続されているイーサネットのブロードキャストドメインであると考えてよい．ループバックインタフェースは，一つのインタフェースだけでリンクが完結する仮想的なリンクである．すなわちリンクとは，実際上はサブネットと同一視されると考えてよいが，厳密な定義によれば，マルチリンクサブネットという概念があり，複数のリンクから構成されるサブネットを考えることもでき，本稿ではこれ以上の記述は控えたいが，Layer2 であると考えてよいだろう．複雑な場合でも IPv4 でも Proxy ARP 技術を用いるなどして PPP リンクとイーサネットリンクを同一のサブネットに収めることが可能であることと同じように考えてみるとよい．

スコープとして，かつてはサイトローカル（site-local）も考えられていたが，詳細な実装検討が進み，その実装が意外と困難であることに加え，その運用上の懸念点も明らかになってきたことなどの理由により廃止されている．

また，最近，この二つの種別に加え，

・ユニークローカル（Unique Local Address）:fc00:/7

が IPv4 におけるプライベートアドレスと等価な利用が可能な空間として規定されている．ULA の利用に際しては，IPv4 と違い NAPT の利用は推奨されない．最近ではステートレスな NAT66 といわれる技術も想定されており，かつ，また推奨されていないはずの NAPT も，実際に運用されている例（例えば 2014 年現在，仮想化製品で有名な Oracle Virtual Box では NAPT66 が実装されている）もあるのだが，本稿ではこの件についてはこれ以上の議論は行わない．

IPv6 では，明快に一つのインタフェースに複数の種類のユニキャストアドレスを付与することができるとする．IPv4 では（もちろん例外の実装はあるが）基本的には一つのインタフェースには一つのユニキャストアドレスしか付与されないものと考えるのに対し，IPv6 では，インタフェースはかならずリンクローカルアドレスを持ち，そのうえで，グローバルアドレスやユニークローカルアドレスを運用する．これは IPv4 と IPv6 の明快な違いの一つであり，後述するアドレス解決方法の違いをはじめとして様々な局面でその違いが現れることに注意する必要がある．

特殊なユニキャストアドレスとしては，IPv4 における 0.0.0.0/32 に相当する，すべてが 0 のアドレス（::/128）である「未指定アドレス」，IPv4 における 127.0.0.1 に相当する::1 を「ループバックアドレス」として規定する．::ffff/96 のプレフィックスに 32 ビットの IPv4 アドレスを下位に連結する IPv4-Mapped IPv6 Address の規定もある．

マルチキャストでは，最上位 8 ビットを 1 とし（すなわちアドレスは ff で始まることとなる），その次の 4 ビットがフラグ，そしてその次の 4 ビットをスコープとしてそれに 112 ビットのグループ ID を接続してアドレスを構成する，すなわち

〔11111111〕〔4 ビットフラグ〕〔4 ビットスコープ〕〔112 ビットグループ ID〕

スコープが“2”（すなわち 0010）の場合リンクローカル，“e”（すなわち 1110）の場合グローバルとなる（ほかのスコープについては省略する）．

予約済みのマルチキャストアドレスとしては，ff02::1（All Nodes：そのリンク上のすべてのノード），ff02::2（All Routers：そのリンク上のすべてのルータ），ff02::5（All OSPF Routers），ff02::6（All OSPF Designated Routers），ff02::0（All RIP Routers），ff02::1:2（All DHCP Agents），ff02::1::3（LLMNR：Link Local Multicast Name Resolution）などが規定されており，また，アドレス解決のために，ff02::1:ff00:0/104：Solicited Node Address（要請ノードアドレス） がある．Solicited Node Address は，IPv4 での ARP によるアドレス解決に相当する ND（Neighbor Discovery：近隣発見）に使用されるマルチキャストプレフィックスである．

■3 群 － 3 編 － 2 章

2-4 IPv6 のパケット構造

（執筆者：宮川　晋）[2015 年 4 月 受領]

IPv4 では，一つのパケットに対して一つのヘッダと一つのペイロード（Payload ：実際の情報が格納されるフィールド）しかないのに対して，IPv6 では，一つのペイロードに，複数の連鎖するヘッダを付与することでパケットを構成する．ヘッダの構造は IPv4 での運用から規定されてはいるが実際は利用されないフィールドを削除するなどして効率化を図っている（一方で引き続き，例えば Flowlabel は実用上の利用が進んでいない）．

以下に IPv6 の基本ヘッダの構造を示す．Next Header 値は，次のヘッダが何であるかの種類を示す．ペイロード長は，拡張ヘッダと実際のペイロードの長さの合計を示す．

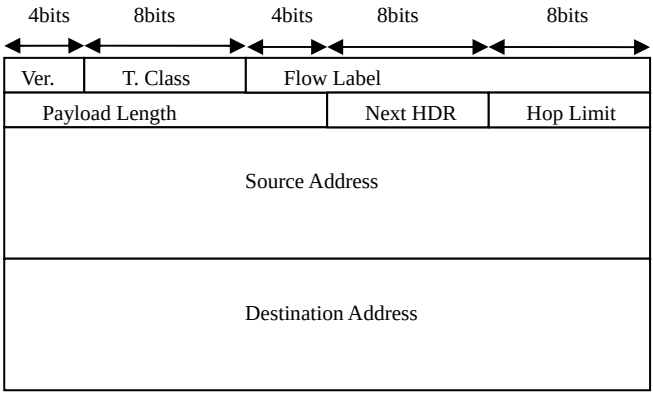

図 2・1　IPv6 の基本ヘッダ

IPv4 のヘッダと比較すると，一番違いがあるのはヘッダチェックサムがないことだと思われる．TTL の代わりに用いられる Hop Limit は，ルータでフォーワードされるたびにその値を一つ減ずることは同じで，IPv4 ではそのたびにチェックサムの再計算が必要だが，IPv6 ではチェックサムがないためにその処理は必要ない．すなわち高速な転送が可能となる．この変更は，なんらかの理由でビット誤りが起きたときには途中の中継ノードで廃棄する IPv4 の仕様と比較して,「ビット誤りが起きてデータが変化してしまっても途中のノードではなく，最終目的地のノードで廃棄すればよい」というように哲学に変化したことを意味している．

IPv6 ではこの基本ヘッダにチェーンのように拡張ヘッダを追加して目的とするパケットを構成する．例えば，UDP パケットは次のようになる．

基本ヘッダ	UDP ヘッダ	UDP ペイロード

拡張ヘッダは複数個指定することができ，仕様上はヘッダの数に制限はないが，実用的には，ネットワークオペレータが，主にセキュリティ上の理由からハンドリングすることを拒

否しないような推奨順と最大の長さがあるものと思った方がよい．

IPv4 ともう一つ根源的に異なるものとしてはフラグメントの扱いがあげられる．IPv6 では，Path MTU Discovery（PMTU）のサポートが必須とされており，IPv4 で可能であったリンクごとのフラグメントができなくなっている．ただし，同時に IPv6 ではリンクの MTU の最小値は 1280 であると規定されており 1280 より小さな MTU しかないリンクは独自の機構をもちいてでも 1280 の MTU を構成しなければならないとされる．

この仕様は現在でも守られてはいるのだが，2014 年現在，セキュリティ上の問題やパフォーマンスの問題から必ずしも良いものだとは限らないという考え方もあり，将来変更される可能性があることを指摘しておく．

■3群 － 3編 － 2章

2-5 IPv6のアドレス設計方法

（執筆者：宮川　晋）[2015年4月 受領]

IPv6 でも IPv4 と同様にアドレスを静的に設定するか，動的に設定するかを選択することができる．

2-5-1 Static設定

IPv6 のアドレスは，そのホストあるいはルータの設定を行うオペレータを静的に設定することができる．特に（ホームルータを除く）ルータの場合は，アドレス設定を静的に行うことが推奨される．

動的な設定方法には SLAAC（State-Less Address Auto-Configuration）と呼ばれる IPv6 特有のやり方と，IPv4 と基本的には同一の DHCP を用いる方法がある．

2-5-2 SLAAC

SLAAC とは，IPv6 の 128 ビットアドレスを上位 64 ビットのプレフィックスと，下位 64 ビットのインタフェース ID に分離し，上位 64 ビットのプレフィクスを RA（Router Advertisement：ルータ広告）と呼ばれる ICMP メッセージに乗せて流し，ホスト側では RA を受信して得られるその上位 64 ビットのプレフィクスと,インタフェースカードに割り当てられている MAC アドレスから生成した 64 ビットのインタフェース ID を組み合わせて 128 ビットのアドレスを作り出すものである．RA には，そのリンクが SLLAC をつかうか DHCP をアドレス指定につかうか，あるいは，その他のパラメータを受領するために使うかのビットがあり（M 及び O），それらのビットによって DHCP を利用するかどうかが決まる．

MAC アドレスからの計算ルールは参考文献を参照されたい．

2-5-3 DHCP

DHCP は IPv4 のそれと基本的に同じなのだが，DHCPv6 では，DHCP Lite として 2Way のパラメータ伝達も認められている．これによりアドレスは SLAAC で設定しつつ，DNS サーバの位置や NTP の情報など，運用に必要なパラメータを同時に DHCP で伝達するという利用が可能となっている．

■3 群 － 3 編 － 2 章

2-6 IPv4・v6 デュアルスタック運用と Happy Eye Ball

（執筆者：宮川　晋）[2015 年 4 月 受領]

2014 年現在，IPv6 だけのネットワークを運用することは，まだ実用的ではない．

Google 社の（ほぼ）すべてのサービス，Facebook，Akamai のコンテンツデリバリーシステムの一部が IPv6 に対応しているおかげで，インターネット回線を IPv4 だけでなく IPv6 にも対応させるいわゆるデュアルスタックとすると，ほぼ 40%近くのトラフィックが IPv6 によって運ばれる状況となる．とはいえ，いまだ多くのサイトが IPv4 にだけ対応しており，IPv6 での名前解決さえできないことも多い．このため，例えば多くのサイトへのリンクから構成される現代的なウェブページを IPv6 だけの環境で表示させようとすると，画面に欠損が生じたり，機能が利用できないということが起こりうる．

すなわち IPv6 を導入するには IPv4 への疎通性も何らかのかたちで（例えば CGN：Carrier Grade NAT を利用するなどして）導入することが現実的であり，多くの IPv6 導入事例において IPv6 単独導入でなく，デュアルスタックとしての IPv6・IPv4 同時存在環境が現出することとなる．

このとき，先にあげたような IPv6 対応サイトは，当然 IPv4 にもそのまま対応していることが多いため，そのようなサイトへ，デュアルスタック環境からアクセスしようとすると，IPv6，IPv4 のいずれでも疎通が可能となるということになる．このとき，現在の多くのオペレーティングシステムでは，IPv6 を優先的に扱うポリシーをもつものが多いのだが，いまだ IPv6 はオプション的なサービスであることがあるので，例えば，IPv6 は IPv4 の上のトンネルで提供されている状況や，IPv6 が IPv4 とは異なる経路を通ってしまい遠回りするような場合などには，却ってサービスへのアクセスが遅くなってしまうという事態になることがある．このため，“Happy Eye Ball”と呼ばれるテクニックがある．これは，「IPv4，IPv6 に優先順位をつけず，アプリケーションが通信を開始しようとする前に DNS を参照してアドレスを取得し，ソケットを空ける試行を v4 と v6 で並行して行い，先に開通した通信路を利用して通信を行う」という技術である．リソースは無駄になるが，アプリケーションを利用しようとするユーザからみれば，アプリケーションが利用できさえすればトランスポートはどちらでも構わないので，合理的な技術であるということができる．

■3 群 － 3 編 － 2 章

2-7 プライバシーエクステンション

（執筆者：宮川　晋）[2015 年 4 月 受領]

前述した IPv6 で利用されることの多い SLAAC によるアドレス自動生成では，アドレスの下 64 ビットは MAC アドレスを基に EUI-64 準拠形式に拡張する．NAPT を基本的に仮定しない IPv6 の場合，上位 64 ビットのプレフィックスが変化しても下位 64 ビットは固定されるということになる．すると，例えば，ノートパソコンを自宅で接続して，どこかのサイトにアクセスしたのち，職場に移動して同じサイトにアクセスするとする．すると，そのサイトのログを検証すると，下位 64 ビットが同じものは同じ端末のアドレスであると推定できるので，その端末が上位 64 ビットのプレフィックスから「どのネットワークからアクセスしてきたか」が判明してしまう，という問題が指摘されている．これを解決するために「外にアクセスするときには下位 64 ビットをランダムに生成して利用する」という拡張が考えられた．これをプライバシー拡張と呼ぶ．Windows OS ではデフォルトで実装されており，実際に時々下位 64 ビットがランダムに生成されて使用される．

■3 群 － 3 編 － 2 章

2-8 モバイル対応と IPSEC 対応について

（執筆者：宮川　晋）[2015 年 4 月 受領]

IPv6 では IPSec 対応が必須とされていた．また MobileIP にも対応することが推奨されてきた．しかしながら現実には，IPSEC は IPv4 と同程度の利用，すなわち VPN 用途で多少の利用がある，という程度である．MobileIP も IPv4 と同程度，すなわちほとんど利用されていない，というのが実態といってよいだろう．セキュリティ確保には，TLS に代表されるトランスポート層でのセキュリティ確保方式の方が利用しやすいこともあり，IPSEC が当初の構想のように利用されることはこれからもあまり考えにくい．また，MobileIP は，v6 のバージョンは v4 のそれよりも非常に使いやすく，また効率的なのだが，残念ながら利用は進んでおらず，最新の Host Requirement では遂に IPSec も MobileIP ともども必須実装ではないとされることとなっている．

■3群 － 3編 － 2章

2-9 おわりに

（執筆者：宮川　晋）[2015年4月 受領]

以上，少ない紙面ながら駆け足でIPv6について解説してきた．ビットパターンの解説をはじめとする通常の教科書的な記述を，あえてほかの文書やインターネット上の情報に譲ることとし，筆者が実際にIETFなどに参加し，標準化策定にかかわった方々から聞いたエピソードなどを参考に，ほかの文献にない情報に拘って記述を行った．

■参考文献

1) 標準化文書　（各RFCは，http://www.ietf.org/ より入手可能）
RFC1752　The Recommendation for the IP Next Generation Protocol
RFC2460　Internet Protocol, Version 6 (IPv6) Specification
RFC4443　Internet Control Message Protocol Version 6 (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC4861　Neighbor Discovery for IP version 6 (IPv6)
RFC4862　IPv6 Stateless Address Autoconfiguration
RFC3315 DHCPv6
RFC3736 DHCPv6 lite
RFC4941　SLLAC Privacy Extension
RFC6434 IPv6 node Requirement
RFC5952 A Recommendation for IPv6 Address Text Representation
RFC3587 IPv6 Global Unicast Address Format
RFC4193 Unique Local Ipv6 Unicast Addresses
http://www.iana.org/assignments/ipv6-multicast-addresses

・IPv6に関する解説

2) クリスチャン・ウイテマ，村井純監修/WIDEプロジェクトIPv6分科会監訳/松島栄樹訳，“IPv6次世代インターネット・プロトコル”，プレンティスホール出版，ISBN 4-88735-010-4，1996年12月初版．
3) 江崎 浩（監修，監修），“IPv6教科書（インプレス標準教科書シリーズ）”，2007.