解説

非PC系ディジタル機器への適用に向けたIPv6最小要求仕様の検討

常時接続環境の普及に伴い，インターネットに接続するノードは，計算機だけではなく，センサ，白物家電，AV機器などが増えると考えられる．これらすべてをインターネットに収容するにはIPアドレスが多数必要になる．NAT技術を使ったとしても，双方向通信ができないので通信に制約がある．このためIPv6が必須になるが，非PC系ディジタル機器では，コスト，資源の制約が厳しく，IPv6の仕様をすべて実装することは困難であり，その仕様を選択しなくてはいけない．本稿では，このような要求に対するIPv6の仕様を検討した結果を報告する．

岡部宣夫　横河電機（株）
Nobuo_Okabe@yokogawa.co.jp
石山政浩　（株）東芝
masahiro@isl.rdc.toshiba.co.jp
井上　淳　（株）東芝
inoue@isl.rdc.toshiba.co.jp
筱島雅之　（株）ACCESS
osajima@access.co.jp
坂根昌一　横河電機（株）
sakane@kame.net
左治木次郎　横河電機（株）
Jirou_Sajiki@yokogawa.co.jp
野口　敬　（株）ACCESS
kay@v6.access.co.jp
宮田　宏　横河電機（株）
H_Miyata@yokogawa.co.jp

背景，研究の動機

インターネットは，すでに我々の産業活動や生活を支える基盤として利用されている．今後は，さらに高速，かつ高信頼性のある常時接続環境に向けた，ディジタル通信基盤の整備が国家的急務となっている．

常時接続環境では，従来の計算機（以降PCと記述する）はもちろん，センサや白物家電，AV機器など（以降非PC系ディジタル機器と記述する）をインターネット上で相互接続して新規サービスを提供することが期待されており，その場合，

- 収容される機器数が膨大であること．
- 電子機器の中には，さまざまな場所に持ち歩いてサービスを受けるものが多数存在するので，グローバルなIPアドレスによるエンド間通信を実現することによりサービスの構築，運用，管理が容易になること．
- 電子機器の中には，従来のクライアントPCと異なり，自ら情報を発信するサーバとなったり，ノード間でpeer-to-peerの通信を行う場合が出てくると予想される．この用途でもグローバルアドレスによるエンド間通信が有利であること．

などの理由により，従来使用されてきたIPv4ではなく，IPv6の使用が必須なことは明白である．

非PC系ディジタル機器では，利用できるメモリ量やCPU性能，コスト，物理的な仕様などの制約が厳しい．このため，IPv6仕様に定められている機能すべてを実装することは困難であると考えられる．また，実運用であまり使用されない機能を義務づけることは，そのままROMサイズなどのコスト増大を招き，IPv6ネットワーク機器の普及，発展に悪影響を与えることになる．

また，これらのノードがインターネットに常時接続されるようになると，プライバシーの漏洩，情報の改竄，犯罪の踏台にされるなどの危険が増大する．IPv6では通信の安全性を確保するためにIPSecが実装必須になっている．しかし，IPSecの仕様はさまざまなセキュリティ要求にかなうように設計されているため，非PC系ディジタル機器においては実装に必要な資源が確保できないことがある．

これに対し，IETFでは，IPv6の基本仕様は決まっているが[1]，非PC系ディジタル機器に関して特に考察はされていない．またIPSecについても同様である[2]．本稿では，限定された資源のもとでIPv6を使った通信を実現するための最小ホスト仕様，最小セキュリティ仕様を

検討した結果を報告する．

検討対象と仕様策定方法

現状，いくつかのIPv6をサポートする商用機器，スタックが発表されている[3),4)]．しかしIPv6搭載機器には，これら以外にもさまざまな構成，形態が考えられ，各々の設計方針，物理的形態などに応じ，実装における制約条件も大きく変わる．たとえば，現在のPCでは最低でも64MBのメモリエリアを保持するのが普通であるが，非PC系ディジタル機器では表-1に示すような非常に小さいエリアに，必須なIPv6/IPSec機能をいかに組み込むかが大きな技術課題となる．また，家電などのコンシューマ機器においては，通信機能を非常に厳しいコスト制約で実装しなければならず，その意味でも必須仕様の選定，実装のコンパクト化が重要になる．

	メモリ	CPU性能	OS
PC	256MB	Pentium 64bit (1GHz)	Windows
AV機器	512KB ROM 20～64KB RAM	RISC 32bit (20MHz)	組み込みOS
PDA	2～8MB	RISC 32bit (50MHz)	WindowsCE,Vxworks, PalmOS
センサ	1 MB	8～16bit マイコン (40MHz)	モニタ＋専用ROM
白物家電	512KB ROM 16～32KB RAM	8～16bit マイコン (40MHz)	モニタ＋専用ROM

表-1 典型的な非PC系ディジタル機器のリソース制約

以上の状況を考慮し，本稿では，以下の方針でIPv6/IPSec最小要求仕様を検討した．

- 本仕様はIPv6搭載機器が，最低限の安全性を保持して通信するためのベースライン仕様を定める．すなわち，本仕様に従っていれば，最低限IPv6で接続された他の機器群と通信が行えることを保証する．
- 特定用途の機器や，機器特有の使用形態を想定することはしない．
- 特定の機器間接続形態や，通信内容，機器の移動等の利用モデルに依存して必要な機能がある．それらについては，汎用的に考慮が必要か否かを評価し，必要なものは仕様に取り込み，そうでないものは特定利用形態における必須機能情報として明示するにとどめる．

なお，本仕様をより多様な機器の要求に合わせるためには，機器の利用形態，通信形態，通信内容，ネットワーク上の移動の有無，実際の利用モデルを分類，検討した上で，各々について最適な取捨選択を行うこ

	タイトル	検討対象外の理由
RFC1887	An Architecture for IPv6 Unicast Address Allocation	アドレス割り当ては検討対象外
RFC2374	An IPv6 Aggregatable Global Unicast Address Format	アドレス割り当ては検討対象外
RFC2450	Proposed TLA and NLA Assignment Rules	アドレス割り当ては検討対象外
RFC2471	IPv6 Testing Address Allocation	アドレス割り当ては検討対象外
RFC1981	Path MTU Discovery for IP version 6	対象ノードは Path MTU discovery をサポートしない
RFC2147	TCP and UDP over IPv6 Jumbograms	Jumbogramsはサポートしない
RFC2675	IPv6 Jumbograms	Jumbograms はサポートしない
RFC2375	IPv6 Multicast Address Assignments	Multicastは将来の検討アイテム
RFC2710	Multicast Listener Discovery (MLD) for IPv6	Multicastは将来の検討アイテム
RFC1888	OSI NSAPs and IPv6	OSIは検討対象外
RFC2292	Advanced Sockets API for IPv6	Socket APIの存在は必ずしも仮定しない
RFC2553	Basic Socket Interface Extensions for IPv6	Socket APIの存在は 必ずしも仮定しない
RFC2473	Generic Packet Tunneling in IPv6 Specification	トンネルはサポートしない
RFC2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels	トンネルはサポートしない
RFC2507	IP Header Compression	IPヘッダ圧縮はサポート外
RFC2526	Reserved IPv6 Subnet Anycast Addresses	Anycastアドレスはサポートしない
RFC2452	IP Version 6 Management Information Base for the Transmission Control Protocol	SNMP/MIBはサポートしない
RFC2454	IP Version 6 Management Information Base for the User Datagram Protocol	SNMP/MIBはサポートしない
RFC2465	Management Information Base for IP Version 6: Textual Conventions and General Group	SNMP/MIBはサポートしない
RFC2466	Management Information Base for IP Version 6: ICMPv6 Group	SNMP/MIBはサポートしない
RFC2467	Transmission of IPv6 Packets over FDDI Networks	Layer 2はEthernet/PPPのみ想定
RFC2470	Transmission of IPv6 Packets over Token Ring Networks	Layer 2はEthernet/PPPのみ想定
RFC2497	Transmission of IPv6 Packets over ARCnet Networks	Layer 2はEthernet/PPPのみ想定
RFC2711	IPv6 Router Alert Option	対象ノードはRouterではない

表-2 検討対象外のIPv6関連RFC

RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
RFC 2461	Neighbor Discovery for IP Version 6 (IPv6)
RFC 2462	IPv6 Stateless Address Autoconfiguration
RFC 2463	Internet Control Message Protocol for the (ICMPv6) Internet Protocol Version 6 (IPv6) Specification
RFC 2373	IP Version 6 Addressing Architecture
RFC 1886	DNS Extensions to support IP version 6
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 2472	IP Version 6 over PPP
draft-ietf-ipngwg-icmp-name-lookups-05	IPv6 Node Information Queries
draft-ietf-ipngwg-scoping-arch-02.txt	IPv6 Scoped Address Architecture
RFC 2401	Security Architecture for the Internet Protocol
RFC 2402	IP Authentication Header
RFC 2406	IP Encapsulating Security Payload (ESP)
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2409	The Internet Key Exchange (IKE)

表-3（a） 検討対策のIPv6関連RFC，Internet Draft

RFC2002	IP Mobility Support
draft-ietf-mobileip-ipv6-13.txt	Mobility Support in IPv6
draft-ietf-ipngwg-default-addr-select-02.txt	Default Address Selection for IPv6
RFC2671	Extension Mechanisms for DNS (EDNSO)
draft-ietf-ipngwg-dns-discovery-01.txt	Analysis of DNS Server Discovery Mechanisms for IPv6
RFC2874	DNS Extensions to Support IPv6 Address Aggregation and Renumbering
draft-moskowitz-hip-03.txt	Host Identity Payload and Protocol
draft-bradner-pbk-frame-00.txt	A Framework for Purpose Built Keys (PBK)

表-3（b） 本検討で参照，考慮したIPv6関連RFC，Internet Draft

とが必要であり，これらについては今後の検討課題である．

■最小ホストの前提

本稿における最小ホストの定義は以下の通りである．

- ホストであり，ルータではない．
- 現時点の拡張ヘッダの仕様では，Mobile IPv6（以下，MIP6と略す）機能を除けば，ホストがこれらを積極的に使わねばならない機能は規定されていない．ゆえに，最小ホストは拡張ヘッダの付いたパケットを出す使い方を不要とする．
- 最小ホストはネットワークインタフェースを1つだけ持つ．もし複数のインタフェースを持つと，マルチホームホストになるので，以下を検討する必要が生じる．
  - 始点選択機能☆1の手続きが繁雑になる．
  - 経路情報を管理する機能が必要になる．
  - 近隣探索機能で利用する各種キャッシュ類（近隣キャッシュ，デフォルトルータリスト，プレフィックスリスト）のエントリ数が多くなる可能性がある．

☆1 Source Address Selection.

■検討対象外の機能／技術

表-2に示すRFC群の規定する仕様は，明らかに非PCディジタル機器の機能を逸脱しているので検討対象外とする．また，これら非PCディジタル機器の適用における（IPv4からの）移行技術は非常に重要なテーマであるが，議論が多岐に渡るため，今回は検討しない．したがって，純粋なIPv6ネットワークにおける通信のみを対象とする．

■仕様の策定方法

本節ではIPv6最小要求仕様，およびIPSec最小要求仕様検討における議論のポイントを説明する．各検討では，表-3（a）に示すRFC，インターネットドラフトをレビューし，最小限必要な機能を明確化する，というアプローチをとった．また表-3（b）には，各検討事項で仕様決定の際に検討・考慮したRFC，インターネットドラフトを示す．必要に応じ，参照されたい．

IPv6 最小ホスト仕様☆2

■IPv6 基本仕様（RFC2460）

最小ホストは拡張ヘッダの付いたパケットを送信しないと規定する．これに対し，最小ホストが拡張ヘッダの付いたパケットを受信した場合，RFC2460に定められている最低限の処理は行わなければならない．以下に詳細を述べる．

- 未サポートの拡張ヘッダを受け取った場合，相手にICMP Parameter Problem Message（Type=1，Code=1）を返し，パケットを破棄する．
- 拡張ヘッダは認識できるが，そこに含まれるオプションが未サポートの場合，オプション番号に従ったエラー処理をしなくてはならない．

○拡張ヘッダの順序

RFC2460では，複数種類の拡張ヘッダとその順序を定義している．最小ホストが拡張ヘッダの機能を必要としないと仮定するならば，拡張ヘッダの順序チェックは省略できる．

○中継点オプションヘッダ

受信側：経路上に存在するすべてのノードは，本ヘッダを解釈できねばならないが，含まれるすべてのオプションを解釈できる必要はない．したがって，最小ホストは中継点オプションヘッダとして認識し，含まれるオプションとオプション番号に従った処理をすべきである．

○経路制御ヘッダ

受信側：ルータなどの中間ノードと終点ノードは本ヘッダを解釈せねばならない．RFCでは，本拡張ヘッダの中継点残数が非零の場合には，そのノードがホストでも，そのパケットを次の中間ノードへ転送せねばならないと規定しているが，最小ノードはこの転送をせず，未サポートの拡張ヘッダとして扱ってもよい．ただし，このノードがMIP6の移動ノード機能も実装する場合には，MIP6の規約の中で経路制御ヘッダを使用するため，このヘッダを正しく処理することが必要になる．

送信側：MIP6 の モビリティエージェントと通信するためにバインディングキャッシュ更新機能☆3を利用して最適経路でパケットを配送するためには，本拡張ヘッダ付きパケットを出力できなくてはならない．

○断片ヘッダ

受信側：もし最小ホストが，IPパケットの再構成を省略したいならば，本ヘッダを未サポート拡張ヘッダとみなし，ICMPを返し，そのパケットを破棄せねばならない．断片化されたパケットの再構成処理は，これらのパケットをメモリに保存し，1つのIPパケットへ再構成するので，より多くのメモリを必要とする処理である．最小ホストのメモリ領域は非常に制約されるので，断片化されたパケットの再構成処理は最も省きたい機能の1つであるといえる．

ICMPを返しパケットを破棄する処理は，通信のパフォーマンスの低下につながるため可能な限り回避するのが望ましい．IPv6では最小MTUが1280バイトと定められており，これ以下のパケットが断片化されることはない．TCPでは，広告するMSS（Max Segment Size）を小さくすることで，送信側ペイロードに利用できる最大のサイズを受信側が指定することができる．これを利用して，常にMSSを小さく広告すれば，断片化が起きる可能性を減らすことができる．たとえばMSSを1000で広告すれば，IPヘッダと拡張ヘッダの合計が280バイトを超えない限り断片化が起きることはない．

UDP の場合，TCP に備わっているパケットサイズ制御機構がないので，相手ノードの送信するパケットを IPv6 最小 MTU 未満に強制することができない．サイズの大きな UDP パケットを送信する可能性のある一般的なサービスとしては，DNS と NFS が考えられる．一般にDNSのペイロードは 512 バイト以下だが，EDNS0では証明書が付加されるので，IPv6最小 MTU を超える可能性が高い．しかし，この場合には，トランスポートプロトコルにTCPを使うと思われるので，本問題を回避できることが期待できる．典型的な NFS 用 UDPペイロードのサイズは数キロバイトである．もし最小ホストがNFS サービスを実装する場合には，IPパケットの再構成が必要となる．

送信側：最小ホストが送信する IP パケットを 常にIPv6最小 MTU（1280バイト）以下にすれば，規約上最終ノードまで断片化されずに転送されるため送信側の断片ヘッダ処理コードは不要となる．副次的効果として，終点ごとの経路 MTUの管理も不要となり，消費メモリを軽減することができる．

○終点ヘッダ

受信側：すべての終点ノードは本ヘッダを認識せねばならないが，含まれるすべてのオプションを解釈できる必要はない．すなわち，最小ホストは本ヘッダを終点ヘッダとして認識し，含まれるオプションとオプ

☆2 以下の説明で，特に原文の用語の指示がない場合，IPv6関連の技術用語の日本語訳は，http://www.v6.wide.ad.jp/Documents/glossary.txtに準ずる．

☆3 Binding Update.

Destination Unreach Message (Type=1)	
code=0 no route to destination	不要
code=1 administratively prohibited	不要
code=3 address unreachable	不要
code=4 port unreachable	必要
Packet Too Big Message (Type=2)	
code=0	不要
Time Exceeded Message (Type=3)	
code=0 hop limit exceeded	不要
code=1 fragment reassembly time exceeded	不要
Parameter Problem Message (Type=4)	
code=0 erroneous header field	必要
code=1 unrecognized next header	必要
code=2 unrecognized IPv6 option	必要
Echo Request Message (Type=128)	
code=0	必要
Echo Reply Message (Type=129)	
code=0	必要

表-4　ICMPv6の実装に関する考察

ション番号に従った処理をすべきである．

送信側：最小ホストが，MIP6のバインディング更新機能を用いて，移動エージェントと通信する必要があるなら，受信パケットの本拡張ヘッダを解釈でき，本拡張ヘッダを含むパケットを送信できねばならない．さらに，上述した通り，バインディング更新機能を解釈できる最小ホストは，経路ヘッダを付けたパケットも出力できねばならない．

■IPv6 近隣探索（RFC2461）

IPv6 最小ホストの前提に従い，ルータ用機能を省略できる．

- ルータ通知メッセージの送信
- ルータ要請メッセージの受信
- 向け直しメッセージの送信

これ以外の機能は，ホストに必要なものなので，原則として実装すべきである．例外は向け直しメッセージ（Redirect Message）の受信である．もし，最小ホストが，経路表や終点キャッシュまたはそれに類似した経路情報を実装しないなら，そのホストは向け直しメッセージを受けても，その情報を記録できないので，無視することになる．

■IPv6 アドレス自動設定（RFC2462）

アドレス重複検出機能は，近隣探索機能を利用している．近隣探索機能は必須なので，必ず実装されているはずである．したがって，アドレス重複機能の実装のためにメモリサイズに与える影響はほとんどなく，原則としてすべてを実装すべきである．例外は，ネットワークからブートするホストである．この場合のブートコードは，非常に限られた容量の ROM上で動作するので，別の評価基準が必要かもしれない．今回の検討では，この部分の評価は行っていない．

■ICMPv6（RFC2463）

最小ホストでは，ルータでしか利用しないICMP は省略できる（**表-4**参照）．

■DNS に関して

現在の IPv6 の自動設定で欠けている機能はDNS サーバの自動的な検出である．これに関しては，現在 IETF IPNGWG で方式を検討中であり，仕様が決定すれば，最小ホスト仕様の必須項目となる可能性が高い．名前から IPv6 アドレスへの変換としてAAAA レコードが規定されており，これが現状での名前解決に関する最小ホストの必須仕様である．しかし，AAAA レコードの代案としてA6 レコードが提案され，その是非がIETF で議論さ

れているので，動向に注目する必要がある．

最小セキュリティ仕様

非PC系ディジタル機器の限られた資源を考慮し，RFC2401に定められたIPSecの仕様に制限を設けることで，最小セキュリティ仕様を検討した．

○ 通信形態の制限

RFC2401では，さまざまな通信形態を想定しているが，本稿ではホスト同士のトランスポート・モードを使った通信だけを対象とし，セキュリティ・ゲートウェイがかかわる通信は対象外とした．また，ノード同士が，少なくとも1回は安全に通信できる形態について検討した．これ以外の通信形態は，なんらかの方法で相手を認証する必要がある．このためのインフラとしてIETF PKIX WG[5]で議論されている技術もあるが，これを利用するための仕様や，IPSecとの連携に関する仕様がないので，対象外とする．マルチキャスト通信は，鍵交換に関する仕様策定がIETFにおいて始まったばかりなので対象外とする．エニキャスト通信は，その仕様が確定していないので対象外とする．IPSec MIBやIPSec固有のICMPは，いくつかの提案がされているが，いまだ標準化されていないので対象外とする．

○ 仕様の制限

RFC2401では，IPv4およびIPv6に対する共通の仕様を定めているが，本稿ではIPv6だけを対象とした．セキュリティ・プロトコルは，暗号化ペイロードを実装必須とする．ペイロードの内容を必要とするプロトコルに関しては，NULL暗号アルゴリズムを使用すればよい．また，IPv6最小ホスト仕様では，IPv6拡張ヘッダを制限しているので認証ヘッダの使用は最小セキュリティ仕様から省いた．セキュリティアソシエーション（以降SAと記述する）を構成するパラメータの最小構成は以下の通りとする．

(1) 宛先IPv6アドレス
(2) 送信元IPv6アドレス
(3) セキュリティ・パラメータ・インデクス（SPI）
(4) IPSecのプロトコル種別
(5) 暗号化アルゴリズム／鍵／初期ベクタ
(6) 認証アルゴリズム／鍵
(7) 32bitのシーケンス番号カウンタ
(8) 再送攻撃を防ぐための情報

これ以外の項目は，実装依存とする．暗号化アルゴリズムはAESを実装必須とし，鍵長は128ビットとする．認証アルゴリズムはHMAC-SHA2-256を実装必須とする．これ以外のアルゴリズムは実装依存とする．また，IPSecに関するAPIは実装に依存するので対象外とした．このためノードを使用するユーザの認証や，通信に参加しているユーザの認証は対象外とした．

○鍵管理について

手動鍵管理は実装必須だが，自動鍵管理は実装必須としない．また，APIは実装依存とする．自動鍵管理を実装した場合は，SAのパラメータとして時間と送受信バイト数による生存時間が必要になる．自動鍵管理のための鍵交換アルゴリズムとしては，IKEがあるが，これは汎用的に設計されており，非PC系ディジタル機器のような非力なノードには相応しくない．また，IPアドレスが不変なノード同士の通信を仮定しているので，移動ノードにおいて使用するには不向きである．さらには例外処理の規定が曖昧であり，IETFでは再検討しようとする動きもある．

これらの状況を考慮して，より軽量なアルゴリズムが現在が提案，検討されており，今後の仕様提示が期待される．さらに鍵配布センターモデルも，場合によっては有効に活用できると考えられる．

結語

情報家電機器やセンサなどの非PC系ディジタル機器にIPv6を搭載する際の最小IPv6仕様，最小セキュリティ仕様について検討した結果を報告した．

今後は，実際の機器ベンダを含めた公共性の高い中立的な組織の下で，オープンなプロセスで企業や研究機関からのフィードバックを得ながら仕様のブラッシュアップを行い，その成果をWEBなどを用いて広く公開していく．公開後も企業や研究機関からのフィードバックと協力を得て継続強化することにより，本仕様をデファクト標準として普及していく．

参考文献
1) IETF IPNG WG (現在IPv6 WG に改名中): http://www.ietf.org/html.charters/ipngwg-charter.html
2) IETF IPSEC WG : http://www.ietf.org/html.charters/ipsec-charter.html
3) インターネットノード株式会社 : http://www.i-node.co.jp/
4) 株式会社ACCESS : http://www.access.co.jp/
5) IETF PKIX WG : http://www.ietf.org/html.charters/pkix-charter.html

(平成13年7月11日受付)