次世代ネットワークインタフェース資料
（ＩＰ通信網）

― ユーザ・網インタフェース（UNI）―

本編

第 1.0 版

2007 年 10 月 25 日

東日本電信電話株式会社
西日本電信電話株式会社

まえがき

本資料は、次世代ネットワークとこれに接続する端末機器等とのインタフェース条件について説明したもので、端末機器等を設計、準備する際の参考となる技術的情報を提供するものです。

今後、本資料は、インタフェースの追加、変更などにより、予告無く変更される場合があります。

また、本機能の全てをサービスとして提供することを保証するものではありません。

目次

1 用語

(1) 端末
ホストおよび HGW の総称を指す。HGW は、家庭内の通信機器間を結ぶネットワーク(ホームネットワーク)と外部のネットワークを接続するゲートウェイまたはルータを指す。

(2) ホスト
IP 通信装置のうち、自分宛ではない IP パケットを、他の IP 通信装置へ転送しないものを指す。

(3) ルータ
IP 通信装置のうち、自分宛ではない IP パケットを、他の IP 通信装置へ転送するものを指す。

(4) ゲートウェイ
異なるプロトコルを使用するネットワーク／通信機器間を接続するために使用される通信装置。

(5) ユーザ・網インタフェース (UNI: User-Network Interface)
ユーザ（端末機器）とネットワークを接続するためのインタフェース。

(6) アプリケーションサーバ・網インタフェース (SNI: Application Server-Network Interface)
各種アプリケーションサーバ類とネットワークを接続するためのインタフェース。

(7) 網間インタフェース（Network-Network Interface）
ネットワーク間を接続するためのインタフェース。

(8) 3GPP (3rd Generation Partnership Project)
第 3 世代移動体通信のアーキテクチャなどの標準化を実施している団体。

(9) EIA (Electronic Industries Alliance)
米国電子工業会。電子産業に関する調査、統計の発表や、各種技術の標準化、政府への提言等を行う団体。

(10) Ethernet
CSMA／CD (Carrier Sense Multiple Access with Collision Detection)方式に従った信号の送受を行う方式。

(11) ETSI (European Telecommunications Standards Institute)
欧州電気通信標準化機構。TISPAN 技術委員会で次世代ネットワーク(NGN)の標準化を行っている。

(12) IEC (International Electrotechnical Commission)
国際電気標準会議。電気、電子、通信等の分野で各国の規格、標準の調整を行う国際的機関。1947 年以降から ISO の電気・電子部門を担当。

(13) IEEE（Institute of Electrical and Electronics Engineers）
米国電気・電子技術者協会。1884 年に設立された世界的な電気、電子情報分野の学会で、LAN 等の標準化を行う。

(14) IETF (Internet Engineering Task Force)
インターネット上で利用される各種プロトコルなどを標準化する組織。ここで標準化された仕様は RFC として公表される。

(15) IMS（IP Multimedia　Subsystem）
3GPP で移動体網への IP 通信用のために規定されたセッション制御サーバ群の仕様。現在、ITU-T、TISPAN 等で固定網への拡張を進めている。

(16) IP (Internet Protocol)
ネットワークレイヤにおけるインターネットの標準的な通信プロトコルで、IP データグラムのルート決定等を行う。バージョン 4 (IPv4)とバージョン 6 (IPv6)があるが、指定しない場合は両方を指す。

(17) IPv4 アドレス
32 ビットのバイナリデータで、IPv4 を用いて通信する必要がある機器に割り当てられる。

(18) IPv6 アドレス
128 ビットのバイナリデータで、IPv6 を用いて通信する必要がある機器に割り当てられる。

(19) IP アドレス
IPv4 アドレスまたは IPv6 アドレスを総称して指し示す場合、本資料では「IP アドレス」と記述する。

(20) IP データグラム／IP パケット
IP で扱われるメッセージ転送単位。

(21) ISO (International Organization for Standardization)
国際標準化機構。1946 年に設立された、商品に関する国際標準をつくることを目的とした国際的機関。

(22) ITU-T (International Telecommunication Union-Telecommunication standardization sector)
国際電気通信連合・電気通信標準化部門。国際間の電気通信を支障なく行うことを目的とした通信網所有者側の標準化委員会。

(23) ONU (Optical Network Unit)
ユーザ側に設置される光加入者線終端装置。

(24) OSI 参照モデル (Open Systems Interconnection)
データ通信を体系的に整理し、異機種相互間の接続を容易にするために ISO が共通する枠組みを定めたモデル。

(25) PPP (Point-to-Point Protocol)
2 地点間の通信に使用するプロトコルであり、専用線で接続を行うルータ間や、ダイヤルアップ接続を行う PC（パーソナル・コンピュータ）等で使用される。

(26) RFC (Request For Comments)
TCP／IP に関連するプロトコルや、オペレーションの手順等を定めた標準勧告文書。IETF が発行している。

(27) RTP (Real-time Transport Protocol)
音声や映像などのメディアを、IP によりリアルタイムに伝送するためのプロトコル。

(28) SDP (Session Description Protocol)
端末－端末間のセッションに関する情報を表現し、ビデオやオーディオ信号を送受信するために必要な情報をやりとりするためのプロトコル。

(29) SIP (Session Initiation Protocol)
IP に基づいた通信により、セッション制御を行うためのプロトコル。

(30) TIA (Telecommunications Industry Association)
米国電気通信工業会。USTSA(United States Telephone Suppliers Association)と EIA の情報通信グループが合併して発足した、データ転送に関する電気的標準を制定する団体。

(31) TCP (Transmission Control Protocol)
エラー検出と再送、フロー制御、順序制御等の機能を有するトランスポート層のプロトコル。コネクション型通信に用いられる。

(32) UDP (User Datagram Protocol)

エラー時の再送制御、フロー制御、順序制御等の機能を持たないトランスポート層のプロトコル。コネクションレス型通信に用いられる。

2　参照勧告類

本資料で参照する勧告類を下記に示します。

[1]　IETF RFC768 (08/1980): User Datagram Protocol
[2]　IETF RFC791 (09/1981): Internet Protocol
[3]　IETF RFC792 (09/1981): Internet Control Message Protocol
[4]　IETF RFC793 (09/1981): Transmission Control Protocol
[5]　IETF RFC826 (11/1982): An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48bit Ethernet Address for Transmission on Ethernet Hardware
[6]　IETF RFC1034 (11/1987): Domain Names – Concepts and Facilities
[7]　IETF RFC1035 (11/1987): Domain Names – Implementation and Specification
[8]　IETF RFC1123 (10/1989): Requirements for Internet Hosts – Application and Support
[9]　IETF RFC1700 (10/1994): Assigned Numbers
[10]　IETF RFC2131 (03/1997): Dynamic Host Configuration Protocol
[11]　IETF RFC2132 (03/1997): DHCP Options and BOOTP Vendor Extensions
[12]　IETF RFC2181 (07/1997): Clarifications to the DNS Specification
[13]　TTC JF-IETF-RFC2327 (06/2005) : SDP : セッション記述プロトコル
[14]　IETF RFC2460 (12/1998): Internet Protocol, Version 6 (IPv6) Specification
[15]　IETF RFC2461 (12/1998): Neighbor Discovery for IP Version 6 (IPv6)
[16]　IETF RFC2462 (12/1998): IPv6 Stateless Address Autoconfiguration
[17]　IETF RFC4443 (03/2006): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
[18]　IETF RFC2474 (12/1998): Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
[19]　IETF RFC2516 (02/1999): A Method for Transmitting PPP Over Ethernet （PPPoE）
[20]　IETF RFC2597 (06/1999): Assured Forwarding PHB Group
[21]　IETF RFC2671 (08/1999): Extension Mechanisms for DNS (EDNS0)
[22]　IETF RFC2711 (10/1999): IPv6 Router Alert Option
[23]　IETF RFC2782 (02/2000): A DNS RR for specifying the location of services (DNS SRV)
[24]　IETF RFC3246 (03/2002): An Expedited Forwarding PHB (Per-Hop Behavior)
[25]　TTC JF-IETF-RFC3261 (06/2005): SIP: セッション開始プロトコル
[26]　IETF RFC3315 (07/2003): Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[27]　IETF RFC3319 (07/2003): Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
[28]　IETF RFC3361 (08/2002): DHCPv4 Option for SIP Servers
[29]　IETF RFC3596 (10/2003): DNS Extensions to Support IP Version 6
[30]　IETF RFC3633 (12/2003): IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
[31]　IETF RFC3646 (12/2003): DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[32]　IETF RFC3810 (06/2004): Multicast Listener Discovery Version 2 (MLDv2) for IPv6
[33]　IETF RFC4075 (05/2005): SNTP Configuration Option for DHCPv6
[34]　IETF RFC4330 (01/2006): Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
[35]　ITU-T Recommendation Y.1221 (03/2002):Traffic control and congestion control in IP-based networks
[36]　ITU-T Recommendation Y.1540 (12/2002): Internet protocol data communication service - IP packet transfer and availability performance parameters

[37] ITU-T Recommendation Y.2001 (12/2004): General overview of NGN
[38] ETSI TR 180 001 (03/2006): Release1 Definition
[39] IEEE Std 802.3-2005 (12/2005): Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications - Media Access Control Parameters、 Physical Layers and Management Parameters for subscriber access networks
[40] ISO/IEC 8877:1992 (12/1992): Information technology - Telecommunications and information exchange between systems - Interface connector and contact assignments for ISDN Basic Access Interface located at reference points S and T
[41] IETF RFC3118 (06/2001): Authentication for DHCP Messages
[42] IETF RFC3203 (12/2001):DHCP reconfigure extension
[43] IETF RFC3396 (11/2002) :Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)
[44] IETF RFC3397 (11/2002):Dynamic Host Configuration Protocol (DHCP) Domain Search Option
[45] IETF RFC3442 (12/2002):The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version4
[46] IETF RFC3513 (04/2003):Internet Protocol Version 6 (IPv6) Addressing Architecture
[47] IETF RFC3925 (10/2004):Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)
[48] IETF RFC2308 (03/1998): Negative Caching of DNS Queries (DNS NCACHE)
[49] TTC TR-1014 (06/2006): NGN アーキテクチャの概要

3　機能の概要

本機能は、次世代ネットワーク 次世代 IP（以下、次世代ネットワークと呼ぶ）を利用する端末機器等（UNI）と電気通信事業者等（NNI）間、端末機器等（UNI）とアプリケーションサーバ機器等（SNI）間、および端末機器(UNI)相互の接続制御を行い、IP 通信を提供する機能です。

本機能では、図 3-1 に示す通り、下記の３つの通信及び接続制御機能をサポートします。

―インタラクティブ（ユニキャスト）通信機能

・双方向通信　　：IP 電話、TV 電話等

・片方向通信（受信）：映像配信（VoD）等

―マルチキャスト通信機能（受信）

・映像配信（IP 放送）等

―PPPoE 接続機能

・ISP 接続等

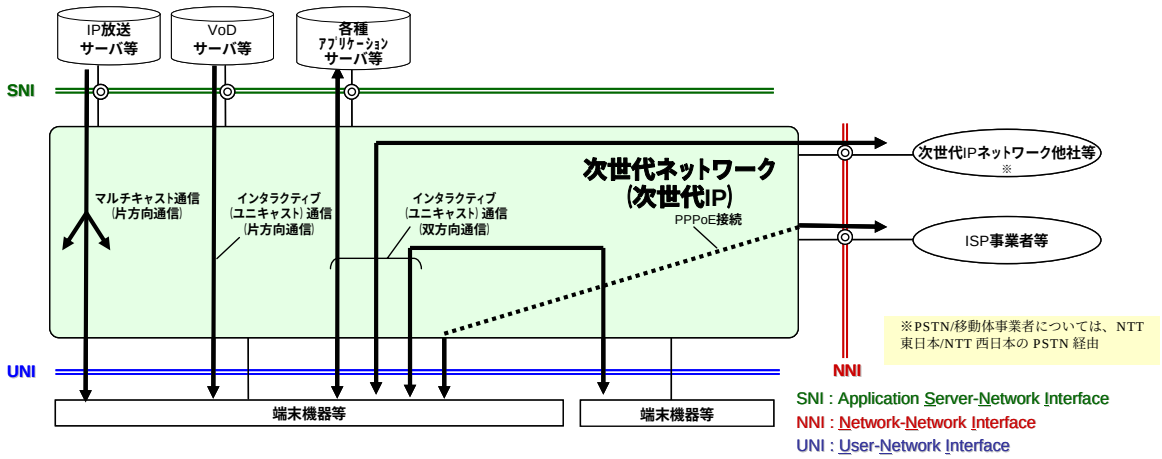


図 3-1：次世代ネットワークの基本構成

表 3-1 に次世代ネットワークにおける品質クラスと接続制御機能の対応について示します。インタラクティブ（ユニキャスト）通信機能では、次世代ネットワークのセッション制御機能を使用することにより、「最優先クラス」～「優先クラス」の複数の品質クラスを提供します。

表 3-1：次世代ネットワークにおける品質クラスと接続制御機能の対応

品質クラス		最優先クラス	高優先クラス	優先クラス	ﾍﾞｽﾄｴﾌｫｰﾄｸﾗｽ
優先制御クラス（Diffserv PHB[20][24][18]）との対応		EF	AF（高優先）	AF（優先）	Default
ｲﾝﾀﾗｸﾃｨﾌﾞ(ﾕﾆｷｬｽﾄ)通信機能	IPv4	○	○	○	―
	IPv6	○	○	○	○
マルチキャスト通信機能	IPv6	―	○	―	○
PPPoE接続機能	IPv4	―	―	―	○

○：次世代ネットワークにおいて提供予定

―：規定しない

本次世代ネットワークは、ITU-T で標準化が進められている次世代ネットワーク[37][49]に準拠しており、セッション制御機能は IMS に準拠しています。

4　規定範囲

本資料では、次世代ネットワークにおける、ユーザ・網インタフェース仕様を規定しており、主に IP トランスポート機能のインタフェース仕様について規定します。

4.1　ユーザ・網インタフェース規定点

本資料では、次世代ネットワークとこれに接続する端末間のインタフェースを規定します。

また、端末制御のインタフェースについては規定対象外です。

4.1.1　インタフェース規定点

次世代ネットワークと端末のユーザ･網インタフェース(UNI)規定点を図 4-1 に示します。

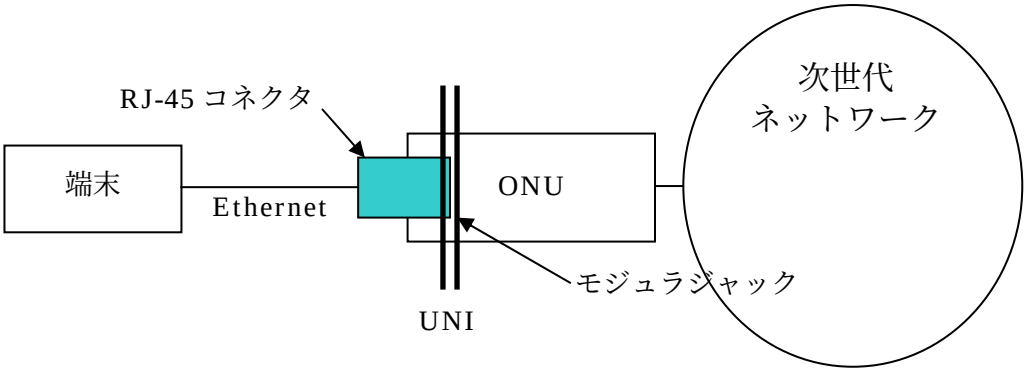


図 4-1：インタフェース規定点

4.1.2　端末設備と次世代ネットワーク側設備の分界点

端末設備と次世代ネットワーク側設備との分界点について図 4-2 に示します。

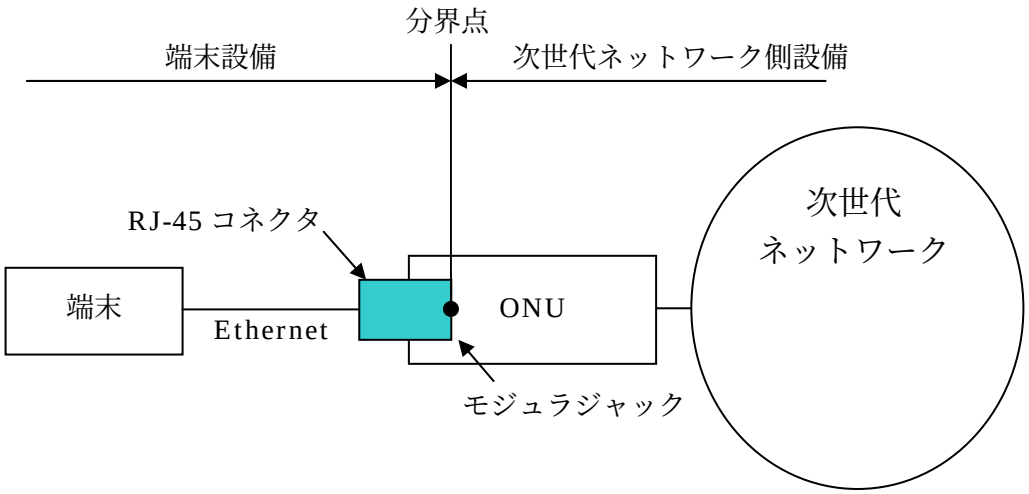


図 4-2：分界点

4.1.3　施工・保守上の責任範囲

施工・保守上の責任範囲について図 4-3 に示します。

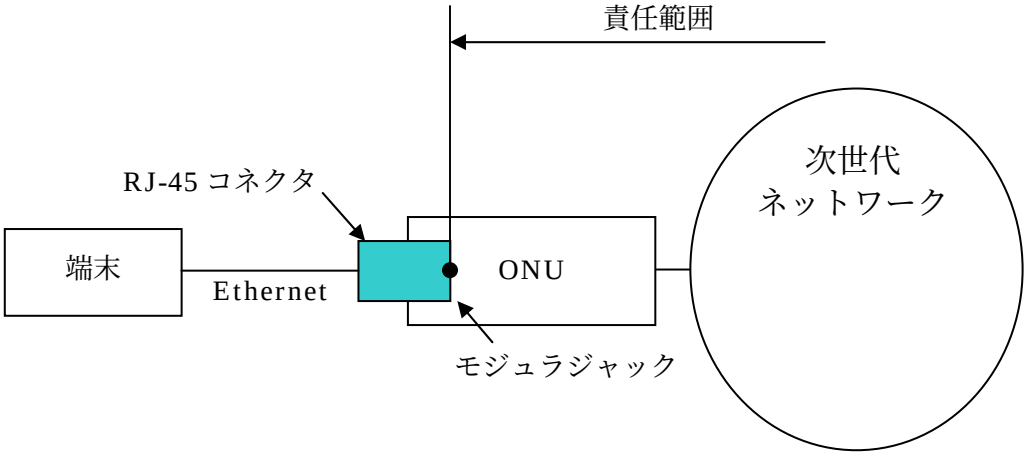


図 4-3：施工・保守上の責任範囲

4.2 ユーザ・網インタフェースプロトコル

ユーザ･網インタフェースのプロトコルの一覧を表 4-1 に示します。プロトコル構成は、OSI 参照モデルに則した階層構造となっています。

表 4-1：インタフェースのプロトコル一覧

<table>
<tr><th colspan="2" rowspan="3">レイヤ</th><th colspan="4">使用するプロトコル</th></tr>
<tr><th colspan="2">インタラクティブ（ユニキャスト）通信機能</th><th>マルチキャスト</th><th>PPPoE</th></tr>
<tr><th>IPv4</th><th>IPv6</th><th>通信機能</th><th>接続機能</th></tr>
<tr><td>7</td><td>アプリケーション</td><td rowspan="3">DHCPv4 :
RFC2131[10]
RFC2132[11]
RFC3118[41]
RFC3203[42]
RFC3396[43]
RFC3397[44]
RFC3442[45]
RFC3925[47]
RFC3361[28]</td><td rowspan="3">DHCPv6 :
RFC3315[26]/RFC3319[27]
RFC3646[31]/RFC4075[33]
RFC3513[46]
DHCPv6-PD :
RFC3633[30]
SNTP :
RFC4330[34]
DNS :
RFC1034[6]/RFC1035[7]
RFC1123[8]/RFC2181[12]
RFC2308[48]/RFC2671[21]
RFC2782[23]/RFC3596[29]</td><td rowspan="3">DHCPv6 :
RFC3315[26]
RFC3646[31]/RFC4075[33]
DHCPv6-PD :
RFC3633[30]</td><td rowspan="4">―</td></tr>
<tr><td>6</td><td>プレゼンテーション</td></tr>
<tr><td>5</td><td>セッション</td></tr>
<tr><td colspan="2"></td><td colspan="2">SIP、SDP、RTP、RTCP、RTSP、HTTP、FTP ※1</td><td>RTP ※2</td></tr>
<tr><td>4</td><td>トランスポート</td><td colspan="2">TCP : RFC793[4]
UDP :RFC768[1]</td><td>UDP : RFC768[1]</td></tr>
<tr><td>3</td><td>ネットワーク</td><td>IPv4 :
RFC791[2]
RFC2474[18]
ICMPv4 :
RFC792[3]</td><td>IPv6 :RFC2460[14]
RFC2474[18]
ICMPv6 :RFC4443[17]
NDP :RFC2461[15]</td><td>IPv6 :RFC2460[14]
RFC2474[18]
ICMPv6 :RFC4443[17]
NDP :RFC2461[15]
MLDv2 :
RFC2711[22]/RFC3810[32]</td><td>IPv4、
ICMPv4 ※3</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">データリンク</td><td>ARP:
RFC826[5]</td><td colspan="2" rowspan="2">―</td><td rowspan="2">IPCP、PAP、
CHAP、PPP
PPPoE:
※3　※４</td></tr>
<tr><td colspan="3">IEEE 802.3 (MAC)[39]</td></tr>
<tr><td>1</td><td>物理</td><td colspan="3">IEEE 802.3 (100BASE-TX/1000BASE-T) /RJ-45/IEEE 802.3/ISO8877[40]</td></tr>
</table>

※1　「次世代 IP　ユーザ・網インタフェース（UNI）　別表１　インタラクティブ（ユニキャスト）通信機能」に詳細を記載。

※2　「次世代 IP　ユーザ・網インタフェース（UNI）　別表２　マルチキャスト通信機能」に詳細を記載。

※3　「次世代 IP　ユーザ・網インタフェース（UNI）　別表３　PPPoE 接続機能（ISP 接続機能）」に詳細を記載。

※4　「次世代 IP　ユーザ・網インタフェース（UNI）　別表４　PPPoE 着信機能」に詳細を記載。

5　インタフェース仕様

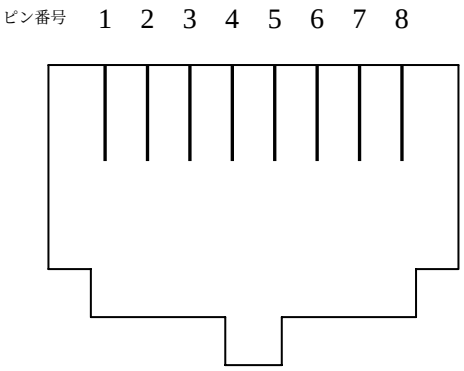
5.1　レイヤ 1 仕様

レイヤ 1 インタフェースとしては、IEEE 802.3[39]に規定される 100BASE-TX または、1000BASE-T を使用し、通信モードとしては自動折衝機能(Auto Negotiation)を使用し、全二重通信モードを使用します。これ以外のインタフェース、通信モードについては動作を保証しません。

5.1.1　インタフェース条件

ユーザ・網インタフェースは、ISO8877[40]準拠の 8 極モジュラジャックである RJ-45 ポートを用います。モジュラジャックの挿入面から見た RJ-45 ポートのピン配置を図 5-1 に示します。

RJ-45 ポート挿入面



ピン番号	100BASE-TX				1000BASE-T			
	方向	記号	信号方向		方向	記号	信号方向	
			端末側	網側			端末側	網側
1	受信	RD(+)	→		送受信	BI_DA+	⇔	
2	受信	RD(-)	→		送受信	BI_DA-	⇔	
3	送信	TD(+)	←		送受信	BI_DB+	⇔	
4					送受信	BI_DC+	⇔	
5					送受信	BI_DC-	⇔	
6	送信	TD(-)	←		送受信	BI_CB-	⇔	
7					送受信	BI_DD+	⇔	
8					送受信	BI_DD-	⇔	

図 5-1：挿入面から見た RJ-45 ポートのピン配置

5.1.2　適用ケーブル

モジュラジャックと接続する端末との配線は、100BASE-TX で接続する場合は、2 対(以上)の非シールドより対線(UTP)ケーブルを、1000BASE-T で接続する場合は、4 対の非シールドより対線(UTP)ケーブルを使用します。CAT5 以上の UTP ケーブルを使用します。

5.2　レイヤ 2 仕様

5.2.1　MAC プロトコル

IEEE 802.3[39]に規定されている MAC を使用します。図 5-2 に IEEE 802.3 に規定される MAC フレームフォーマットを示します。タイプ／フレーム長フィールドにフレーム長を指定した場合は、転送を保証できない場合があります。また、表 5-1 にタイプ／フレーム長フィールドの主な割り当てを示します。

ﾌﾟﾘｱﾝﾌﾞﾙ（7）	SFD（1）	宛先 MAC アドレス（6）	送信元 MAC アドレス（6）	タイプ／フレーム長（2）	データ（46～1500）	FCS（4）

各フィールド内の数値はフィールド長（単位：オクテット）を示します。

図 5-2： IEEE 802.3 MAC フレームフォーマット

表 5-1：タイプ／フレーム長フィールドの主な割り当て

タイプ／フレーム長の値(16 進数)		プロトコル
フレーム長	2E ～ 5DC	―※
タイプ	0800	Internet IP(IPv4)
	0806	Address Resolution Protocol(ARP)
	86DD	IP version 6(IPv6)
	8863	PPPoE Discovery Stage
	8864	PPPoE Session Stage

※フレーム長を指定した場合は、転送を保証できない場合があります。

5.2.2　ARP プロトコル

レイヤ 3 プロトコルとして IPv4 を使用する端末は、RFC 826[5]に規定されている ARP を使用する必要があります。図 5-3 に ARP のパケットフォーマットを示します。

HLEN：MAC アドレスの長さ＝6

PLEN：IPv4 アドレスの長さ　＝4

図 5-3：ARP のパケットフォーマット

5.2.3 PPP over Ethernet

PPPoE接続機能では、レイヤ２プロトコルとして、RFC2516[19]に規定されているPPPoEを使用します。図 5-4にPPPoEのフレームフォーマットを示します。詳細は「次世代IP　ユーザ・網インタフェース（UNI）　別表3　PPPoE接続機能（ISP接続機能）」を参照してください。

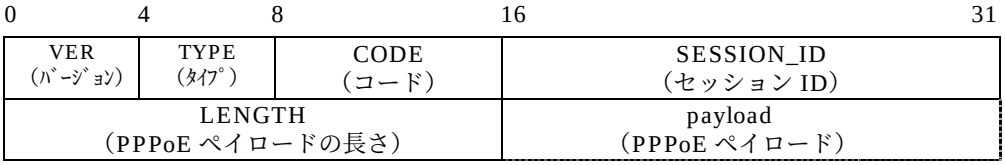


図 5-4：PPPoE フレームフォーマット

5.3 レイヤ 3 仕様

ネットワークレイヤ（レイヤ 3）としては、IPv4 と IPv6 のいずれかまたは両方をサポートします。

インタラクティブ（ユニキャスト）通信機能では、レイヤ 3 プロトコルとして IPv4 または IPv6 を使用します。マルチキャスト通信機能では、レイヤ 3 プロトコルとして IPv6 を使用します。

端末は IPv4 を使用する場合は ICMPv4 を、IPv6 を使用する場合は ICMPv6 を使用する必要があります。

5.3.1　IPv4 プロトコル

レイヤ 3 プロトコルの 1 つとして､網は IPv4 をサポートします｡サポートする IPv4 は、RFC791[2]の規定に従います。なお、IP ヘッダ情報（DSCP、パケット長、フラグ、フラグメントオフセット、TTL、ヘッダチェックサム、送信元 IPv4 アドレス、宛先 IPv4 アドレス）については、網内で書き換えて転送制御に利用することがあります。

5.3.1.1 IPv4 アドレス

IPv4 アドレスとしては、RFC791[2]に規定されている IPv4 アドレスをサポートすることとしますが､RFC1700[9]に規定されているクラス D（224.0.0.0/4）､クラス E（240.0.0.0/4）の IPv4 アドレスは使用しません。また、端末が利用可能な IPv4 アドレスは、網に接続する際に網から割り当てられた IPv4 アドレスの範囲のみで、その他の IPv4 アドレスを利用した場合の動作は保証されません。

5.3.1.2 IPv4 パケットフォーマット

図 5-5 に IPv4 パケットフォーマットを示します。図 5-6 に示す通り、IPv4 パケットフォーマット内のサービスタイプフィールド内に DSCP 値を指定します（RFC2474[18]に規定）。また、IPv4 パケットフォーマット内のプロトコルフィールドに設定可能な主な値を表 5-2 に示します。

また、フラグメントされた IPv4 パケットについては、ベストエフォートクラスとして扱われパケットが廃棄される場合があります。

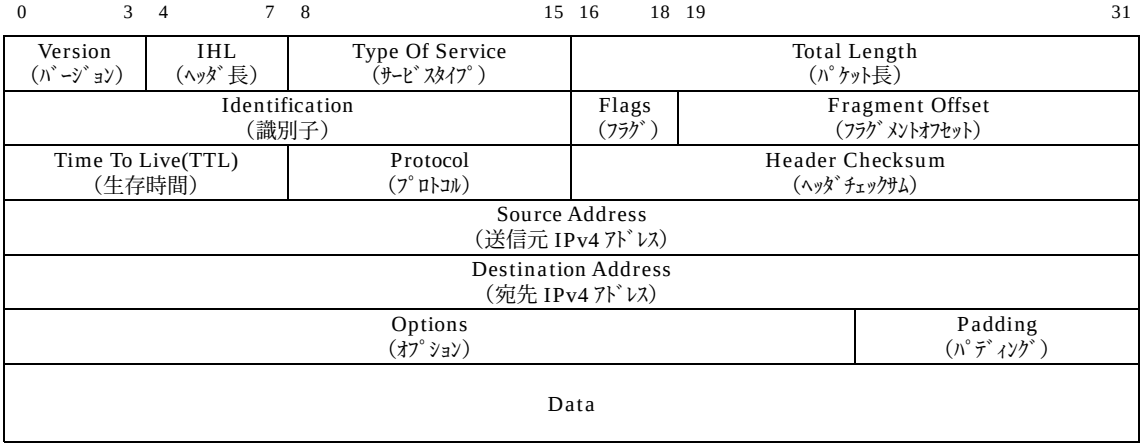


図 5-5：IPv4 パケットフォーマット

DSCP 値 （6 ﾋﾞｯﾄ）	未使用 （2 ﾋﾞｯﾄ）

図 5-6：DSCP 値の指定（サービスタイプフィールド）

表 5-2：プロトコルフィールドに設定可能な主な値

割り当て番号	略称	プロトコル名
1	ICMP	Internet Control Message Protocol
6	TCP	Transmission Control Protocol
17	UDP	User Datagram Protocol

5.3.1.3 ICMPv4 プロトコル

IPv4 を使用する端末は、RFC792[3]に規定される ICMPv4 をサポートする必要があります。

端末は、網から ICMPv4 エコー要求メッセージを受信した場合、ICMPv4 エコー応答メッセージで応答することとします。ただし、 ICMPv4 エコー要求メッセージは、端末と網との故障切り分けを行う場合を除いて、網側でフィルタリングされます。

図 5-7 に ICMPv4 のメッセージフォーマットを、表 5-3 に ICMPv4 の主なメッセージのタイプを示します。

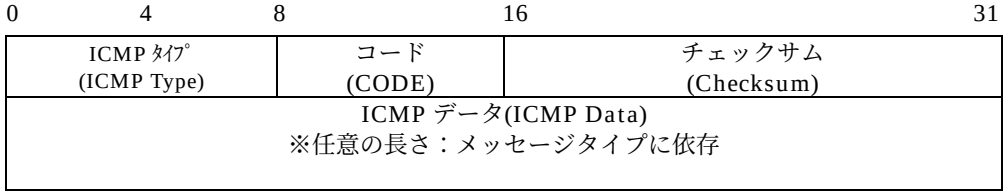


図 5-7：ICMPv4 のメッセージフォーマット

表 5-3：ICMPv4 の主なメッセージのタイプ

ICMP タイプ （１０進数）	内容
0	エコー応答（Echo Reply）
3	宛先到達不能（Destination　Unreachable）
4	発信抑制（Source Quench）
5	ルート変更（Redirect）
8	エコー要求（Echo　Request）
11	データグラムの時間超過（Time Exceeded for Datagram）
12	データグラムのパラメータ異常（Parameter Problem on　Datagram）

5.3.1.4 DHCPv4 プロトコル

IPv4 に対応した端末に対しては、RFC2131[10]に規定される DHCPv4 プロトコルを用いて、以下に示す各種アドレス等の情報を、DHCPv4 のオプションにより網から配布します。

- IPv4 アドレス　（RFC2132[11]）
- IPv4 サブネットマスク　（RFC2132[11]）
- ゲートウェイアドレス（IPv4）　（RFC2132[11]）
- SIP サーバアドレス（IPv4）※1　（RFC3361[28]）

※1　セッション制御用プロトコル(SIP)を送受信するための網側の IPv4 アドレス。

詳細については、付属資料 B を参照してください。

5.3.2　IPv6 プロトコル

レイヤ 3 プロトコルの 1 つとして、網は IPv6 をサポートします。サポートする IPv6 は RFC2460[14]の規定に従います。なお、IP ヘッダ情報（DSCP、ペイロード長、ホップリミット、送信元 IPv6 アドレス、宛先 IPv6 アドレス）については、網内で書き換えて転送制御に利用することがあります。

5.3.2.1 IPv6 アドレス

端末のアドレスとして利用可能な IPv6 アドレスは、RFC3315[26]に規定される DHCPv6 プロトコルを用い IPv6 プレフィックスを割り当てます。

リンクローカルアドレスを除き、網に接続する際に網から割り当てられた IPv6 アドレスプレフィックスの範囲外の IPv6 アドレスを利用する場合の動作は保証されません。

なお、RFC2462[16]に規定された IPv6 ステートレスアドレス自動設定（NDP を利用）についてもサポートします。

5.3.2.2 IPv6 パケットフォーマット

図 5-8 に IPv6 パケットフォーマットを、図 5-9 に IPv6 ヘッダを示します。図 5-10 に示す通り、IPv6 パケットフォーマット内のトラヒッククラスフィールドに DSCP 値を指定します（RFC2474[18]に規定）。また、IPv6 ヘッダ内の次ヘッダフィールドに規定される主な値を表 5-4 に示します。

IPv6 パケットフォーマットにおける拡張ヘッダについては、MLDv2 で使用するホップバイホップ拡張ヘッダ(RFC2711[22]に規定するルータアラートオプション)を使用します。

その他の拡張ヘッダを使用した場合は、網は転送を保証できない場合があります。

フラグメントされた IP パケットについては、ベストエフォートクラスとして扱われパケットが廃棄される場合があります。

IPv6 ヘッダ (40 ｵｸﾃｯﾄ)	拡張ヘッダ	ペイロード

図 5-8：IPv6 パケットフォーマット

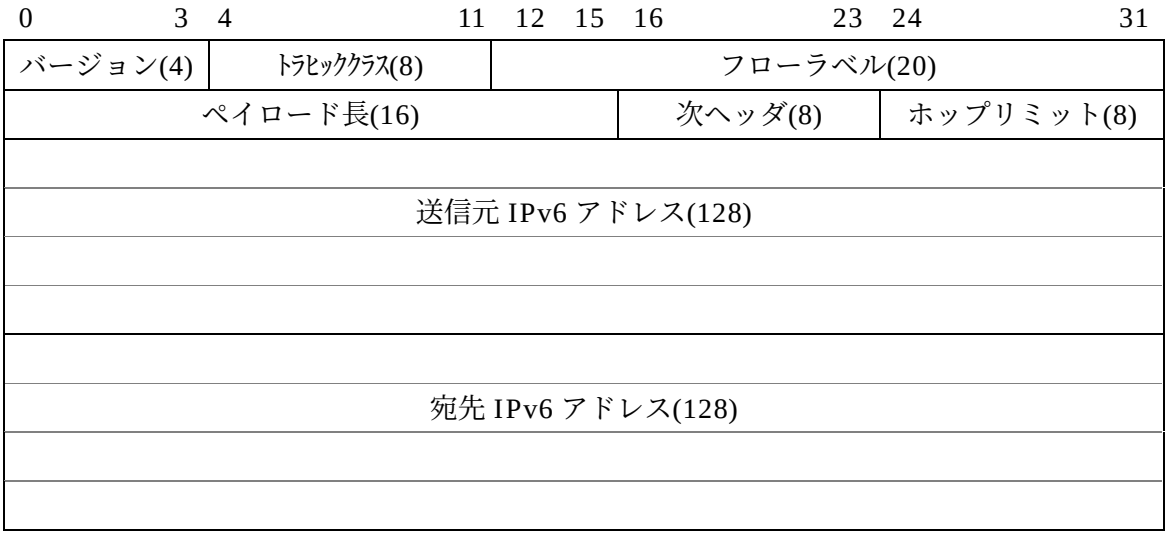


図 5-9：IPv6 ヘッダ

DSCP 値 （6 ﾋﾞｯﾄ）	未使用 （2 ﾋﾞｯﾄ）

図 5-10：DSCP 値の指定（トラヒッククラスフィールド）

表 5-4：次ヘッダフィールドの主な値

番号	プロトコル
0	IPv6 ホップバイホップオプション
6	TCP
17	UDP
58	ICMPv6

5.3.2.3 ICMPv6 プロトコル

IPv6 を使用する端末は、RFC4443[17]に規定される ICMPv6 をサポートする必要があります。

端末は、網から ICMPv6 エコー要求メッセージを受信した場合、ICMPv6 エコー応答メッセージで応答することとします。ただし、網からの ICMPv6 エコー要求メッセージは、端末と網との故障切り分けを行う場合を除いて、網側でフィルタリングされます。

図 5-11 に ICMPv6 のメッセージフォーマットを示します。また、表 5-5 と表 5-6 に、主な ICMP 情報メッセージとエラーメッセージのタイプを示します。

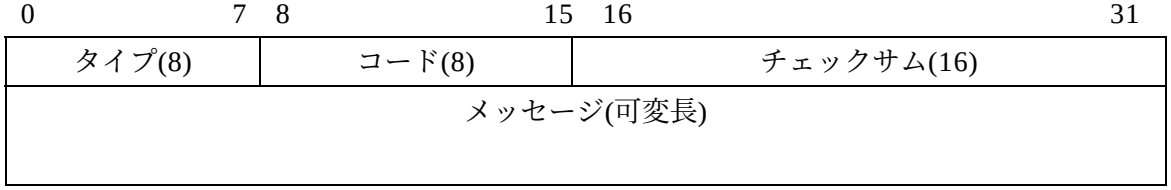


図 5-11：ICMPv6 のメッセージフォーマット

表 5-5：主な ICMPv6 情報メッセージのタイプ

タイプ	名称	
128	エコー要求（Echo Request）	
129	エコー応答（Echo Reply）	
130	マルチキャストリスナー照会（Multicast Listener Query）	MLDv2 関連
133	ルータ要請（Router Solicitation）	NDP 関連
134	ルータ広告（Router Advertisement）	
135	近隣要請（Neighbor Solicitation）	
136	近隣広告（Neighbor Advertisement）	
143	MLDv2 リスナー報告（Version 2 Multicast Listener Report）	MLDv2 関連

表 5-6：主な ICMPv6 エラーメッセージのタイプ

タイプ	名称
1	終点到達不能（Destination Unreachable）
2	パケットサイズ過大（Packet too Big）
3	時間超過（Time Exceeded）
4	パラメータ問題（Parameter Problem）

5.3.2.3.1 NDP プロトコル

IPv6 を使用する端末は、Neighbor Discovery 手順（NDP）をサポートする必要があります。NDP の仕様は RFC2461[15]に準拠します。

なお、 NDP に基づく IPv6 ステートレスアドレス自動生成についてもサポートします。

詳細については、付属資料 E を参照してください。

5.3.2.3.2 MLDv2 プロトコル

マルチキャスト通信機能では、マルチキャスト配信を受信する端末の登録・削除手順については、RFC3810[32]に規定される MLDv2 を用いることとします。なお、MLDv2 プロトコルの詳細については、「次世代 IP　ユーザ・網インタフェース（UNI）　別表２　マルチキャスト通信機能」を参照してください。

5.3.2.4 DHCPv6 プロトコル

IPv6 を使用する端末に対しては、RFC3315[26]に規定される DHCPv6 プロトコルを用いて、以下に示す各種アドレス等の情報を、 DHCPv6 のオプションにより網から配布します。

- IPv6 アドレスプレフィックス　（RFC3633[30]）
- DNS サーバアドレス（IPv6）　（RFC3646[31]）
- SIP サーバアドレス（IPv6）※1　（RFC3319[27]）
- SNTP サーバアドレス（IPv6）※2　（RFC4075[33]）

※1　セッション制御用プロトコル（SIP）を送受信するための網側の IPv6 アドレス

※2　時刻情報を提供する SNTP サーバの IPv6 アドレス

詳細については、付属資料 B を参照してください。

5.4 レイヤ 4 仕様

トランスポートレイヤ（レイヤ４）としては、RFC793[4]に規定される TCP と RFC768[1]に規定される UDP をサポートします。

インタラクティブ（ユニキャスト）通信機能では、レイヤ 4 プロトコルとして TCP または UDP を使用する必要があります。マルチキャスト通信機能では、レイヤ 4 プロトコルとして UDP を使用する必要があります。

なお、ヘッダ情報（ポート番号、チェックサム）については、網内で書き換えて転送制御に利用する場合があります。

5.5　レイヤ 5 以上の仕様

セッションレイヤ（レイヤ５）からアプリケーションレイヤ（レイヤ７）の主なプロトコルとしては、IPv4 に対応した端末に対して DHCPv4、また、IPv6 に対応した端末に対して DHCPv6、DNS、SNTP をサポートします。

DHCPv4 及び DHCPv6 については、5.3.1.4 及び 5.3.2.4 を参照してください。また、DNS については付属資料 C、SNTP については付属資料 D を参照してください。

6　品質規定条件

6.1　制御信号における転送品質クラス指定方法

次世代ネットワークでは、転送品質クラスは TTC JF-IETF-RFC2327[13]に規定される SDP を用いて指定されます。SDP による転送品質クラス指定の詳細については、「次世代 IP　ユーザ・網インタフェース（UNI）　別表１　インタラクティブ（ユニキャスト）通信機能」の 5.2 節を参照してください。

6.2　データパケットに設定する転送優先度識別子

データパケットにおいては、指定された転送品質クラスに対応する転送優先度識別子を設定の上、次世代ネットワークに対して送出する必要があります。

なお、呼の接続／切断に関わる制御信号（TTC JF-IETF-RFC3261[25]に規定される SIP）のパケットに対しては、一律、最優先クラスに対応する転送優先度識別子を設定の上、次世代ネットワークに対して送出する必要があります。

但し、制御信号における転送品質クラスの指定と、データパケットに設定する転送優先識別子に対応する品質クラスが一致しない場合は、転送を保証できない場合があります。

(1) IPv4 の場合

転送優先度識別子として、サービスタイプフィールドに DSCP 値を設定する必要があります。

DSCP 値と最優先クラス～優先クラス、ベストエフォートクラスとの対応を、表 6-1 に示します。

表 6-1：DSCP 値と転送品質クラスの対応(IPv4)

	最優先クラス	高優先クラス	優先クラス	ﾍﾞｽﾄｴﾌｫｰﾄｸﾗｽ
ｻｰﾋﾞｽﾀｲﾌﾟﾌｨｰﾙﾄﾞ（IPv4）に設定する DSCP 値	101110	100000	001000	000000

(2) IPv6 の場合

転送優先度識別子として、トラヒッククラスフィールド内に DSCP 値を設定する必要があります。

DSCP 値と最優先クラス～優先クラス、ベストエフォートクラスとの対応を、表 6-2 に

示します。

表 6-2：DSCP 値と転送品質クラスの対応(IPv6)

	最優先クラス	高優先クラス	優先クラス	ﾍﾞｽﾄｴﾌｫｰﾄｸﾗｽ
ﾄﾗﾋｯｸｸﾗｽﾌｨｰﾙﾄﾞ(IPv6)に設定する DSCP 値	101110	100000	001000	000000

6.3 UNI におけるトラヒック条件

次世代ネットワークの UNI におけるトラヒック条件を、以下のように規定します。

(1) 次世代ネットワークでは、UNI からの流入トラヒックをトークンバケットポリサー（ITU-T 勧告　Y.1221 [35] Appendix 1 参照）で監視します。ポリサーの監視条件を違反したパケットは、次世代ネットワーク内で廃棄されます。

(2) トークンバケットポリサーの監視パラメータは、レートと最大バケットサイズです。最大バケットサイズについては、各転送品質クラスに応じた値を次世代ネットワーク側で用意します。

6.4 端末側に期待する品質条件

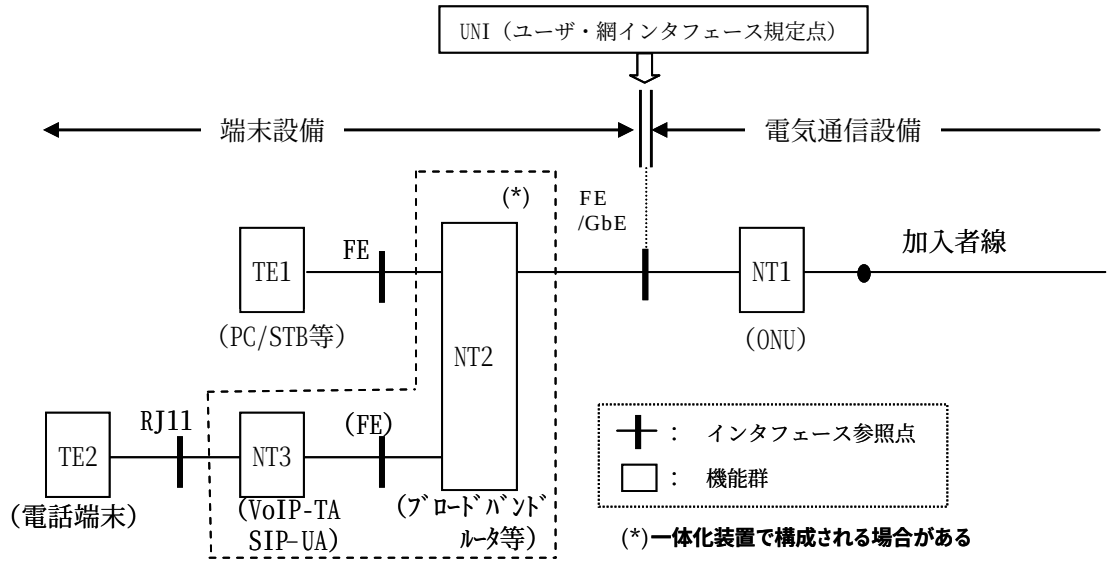
次世代ネットワークの UNI に接続される端末に期待する品質条件を、以下のように規定します。

(1) IP 電話サービスのように、総務省令等により品質基準が規定されているサービスにおいては、端末に対する一定の遅延品質配分を期待します。端末に期待する具体的な遅延品質配分については、「次世代 IP　ユーザ・網インタフェース（UNI）別表 1　インタラクティブ（ユニキャスト）通信機能」の付属資料 C を参照してください。

(2) 映像配信系のサービスにおいては、網側でのメンテナンス工事などに伴う一定のデータロス時間を規定し、それを前提にした能力を端末に期待します。

付属資料Ａ　ユーザ･網インタフェース規定点と端末設備の構成要素の具体例

次世代ネットワークにおけるユーザ・網インタフェース（UNI）規定点、及び UNI に接続される端末設備の構成要素、機能概要並びに、具体例を図 A-1 に示します。



名　称	概　　要	具　体　例
網終端（装置）１ （ＮＴ１）	伝送路終端等のレイヤ１機能をもつ	光加入者線終端装置 （ＯＮＵ）
網終端（装置）２ （ＮＴ２）	ＩＰレイヤ（レイヤ３）以下の集線・交換及びＩＰレイヤに付随する機能（ＮＡＰＴ等）をもつ	ブロードバンド ルータ等
端末装置１ （ＴＥ１）	ＵＮＩに接続可能な端末 （ＮＴ２非介在にて接続が可能な端末）	パソコン、 ＳＴＢ※1等
端末装置２ （ＴＥ２）	既存アナログ電話網に接続可能な端末	既存の端末装置等
網終端（装置）３ （ＮＴ３）	ＴＥ２を次世代ユーザ・網インタフェースに接続するためのアダプタ（併せて、ＳＩＰ－ＵＡとして機能し、既存端末の親電話機相当（ＮＴ２より下部側の端末に対して、内線接続、外線発信等を統括）を提供）	ＶｏＩＰ－ＴＡ※2／ ＳＩＰ－ＵＡ※3等

※1　STB : Set Top Box
※2　VoIP-TA : Voice over IP – Terminal Adapter
※3　SIP-UA : SIP-User Agent（「次世代 IP　ユーザ・網インタフェース（UNI）　別表１　インタラクティブ（ユニキャスト）通信機能」参照）

図 A-1：UNI 規定点及び端末設備の構成要素と機能概要の具体例

付属資料 B　DHCP プロトコル

B.1　DHCPv4 プロトコル

B.1.1　DHCPv4 手順

DHCPv4 は、端末と網間で動作し、網が端末の IPv4 アドレス及び各種設定パラメータを通知するために用いられます。DHCPv4 の動作は 2 フェーズ（4 メッセージ交換）で実行されます。

DHCPv4 による IPv4 アドレス情報払い出しのシーケンスを図 B-1 に示します。

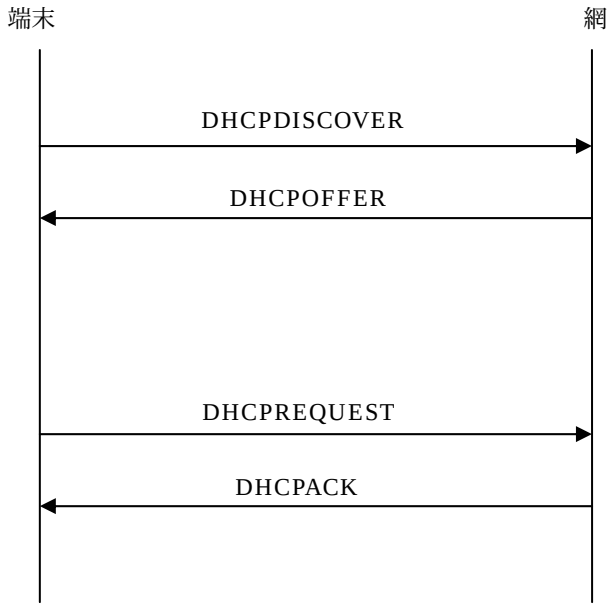


図 B-1：IPv4 アドレス情報払い出しシーケンス

端末は、IP アドレスの割当を希望する場合、第 1 フェーズとして DHCPDISCOVER メッセージを網へ送信します。DHCPDISCOVER を受信した網は、IP アドレス割当が可能と判断した場合、DHCPOFFER メッセージを端末に送信します。端末は、第 1 フェーズで網が IP アドレス割当可能と判断した場合、第 2 フェーズとして、DHCPREQUEST メッセージを送信します。この時に端末は、要望するオプションリストを含めて送信して下さい。網は、DHCPACK メッセージを用いて応答し、IP アドレスが決定します。また網は、この時に要望されたオプションに対する情報も含めて送信します。なお DHCPACK に配布した IP アドレスに対する有効期限が含まれる場合は、端末は、その有効期限を記憶しなければなりません。

網がサポートするメッセージ・オプションコードを表 B-1 と表 B-2 に示します。端末が規定外のメッセージを送信した場合、サーバは受信したメッセージを無視し、廃棄します。また、未規定のオプションコードが指定された場合は、未規定のオプションコードのみを無視して処理を継続します。

表 B-1：DHCPv4 サーバがサポートするメッセージタイプ

メッセージタイプ	値	説明
DHCPDISCOVER	1	クライアントがサーバを探索するためのメッセージ
DHCPOFFER	2	サーバが DHCPDISCOVER に対して応答する際に使用するメッセージ
DHCPREQUEST	3	IPv4 アドレス、設定パラメータを要求・更新する際に使用する
DHCPDECLINE	4	DHCPOFFER メッセージで通知された IPv4 アドレスの重複を検出した際に使用する
DHCPACK	5	サーバが DHCPREQUEST に対して応答し、各種情報を通知する際に使用する
DHCPNAK	6	サーバが DHCPREQUEST に対して拒否する際に使用する
DHCPRELEASE	7	クライアントが IPv4 アドレス、設定パラメータの解放を要求する際に使用する

表 B-2：DHCPv4 でサポートされるオプション一覧

オプション	Code	RFC	説明
Pad	0	RFC2132[11]	パディング用データ オプションデータを一定サイズに調整するために本オプションを使用してもよい
Subnet Mask	1		サブネットマスク
Router	3		ルータアドレス(IPv4)
Requested IP Address	50		端末がリクエストする IPv4 アドレス
Address Time	51		IPv4 アドレスリース期間
Option Overload	52		オプションフィールドの分割方法を指定します
DHCP Msg Type	53		DHCP メッセージタイプ
DHCP Server Id	54		DHCP サーバアドレス(IPv4)
Parameter List	55		端末からのパラメータ要求リスト
Maximum DHCP Message Size※2	57		DHCP メッセージサイズを変更する際に指定します
Renewal (T1) Time Value ※3	58		リース更新要求タイムアウト時間（T1） 網で端末によるリース期間延長要求時のタイムアウト時間（秒）を指定
Rebinding (T2) Time Value ※2	59		リース更新要求タイムアウト時間（T2） 網で端末による再割り当て要求時のタイムアウト時間（秒）を指定
Client-identifier ※4	61		網で端末をユニークな ID で識別する際に使用する
End Option	255		ベンダフィールドで正当なインフォメーションの終わりを記録する
Authentication Option	90	RFC3118[41]	DHCPFORCERENEW メッセージに認証情報を含める場合に使用します。
SIP Server DHCP Option	120	RFC3361[28]	セッション制御用の網側送受信アドレス(IPv4)
The Classless Static Route Option	121	RFC3442[45]	端末のルーティング設定情報を通知するために用いる
Vendor-Identifying Vendor class Option※1	124	RFC3925[47]	ベンダの識別情報 端末機器に設定するネットワーク関連情報等の通知を受けるための端末識別に使用する
Vendor-Identifying Vendor-Specific information Option※1	125		ベンダ特有の情報 端末機器に設定するネットワーク関連情報等の通知に使用する

※1　ネットワーク関連情報等の端末機器への設定の自動化のために使用する可能性があります。

※2　DHCP メッセージサイズを変更する際に、DHCPDISCOVER か DHCPREQUEST メッセージでサイズを指定する際に指定します。本仕様では、必須オプションとし、本オプションに指定するサイズは、888,1200 バイトの何れかを指定して下さい。それ以外の指定サイズは無視する可能性があります。

※3　Renewal (T1) Time Value・Rebinding (T2) Time Value が網より指定される場合は、端末は指定された値に従った動作をする必要があります。

※4　Client-identifier オプションを用いて網が端末を識別する場合は、端末は本オプションコードを送信可能とする必要があります。

B.1.2　SIP サーバアドレス取得

セッション制御用の IPv4 アドレスを、網から端末に配布する機能が提供される場合には、

RFC3361[28]の手順に従います。なお、RFC3361[28]によるドメイン名通知は未サポートとします。

B.1.3　DHCPv4 アドレス付与条件

DHCPv4 によるアドレス付与条件は、1 アクセスラインに対して、1IP アドレスを付与します。またアドレス払い出し時に、サブネットマスク及びゲートウェイアドレスも配布します。なお、サブネットマスク、ゲートウェイアドレス配布及びデータ設定方法は、RFC2132[11]手順に従います。

B.2　DHCPv6 プロトコル

B.2.1　アドレスプレフィックス取得

網から端末へは DHCPv6-PD を用いた IPv6 アドレスプレフィックス配布が行われます。

B.2.2　DHCPv6-PD 手順

DHCPv6-PD は、端末と網間で動作し、網が端末の IPv6 アドレスプレフィックス及び各種パラメータを通知するために用いられます。

DHCPv6-PD では、端末と網は、DUID を所持します。DUID は、端末及び網が互いを識別するために用います。

DHCPv6-PD の動作は、2 フェーズ（4 メッセージ交換）で実行されます。

DHCPv6-PD による IPv6 アドレスプレフィックス払い出しのシーケンスを図 B-2 に示します。

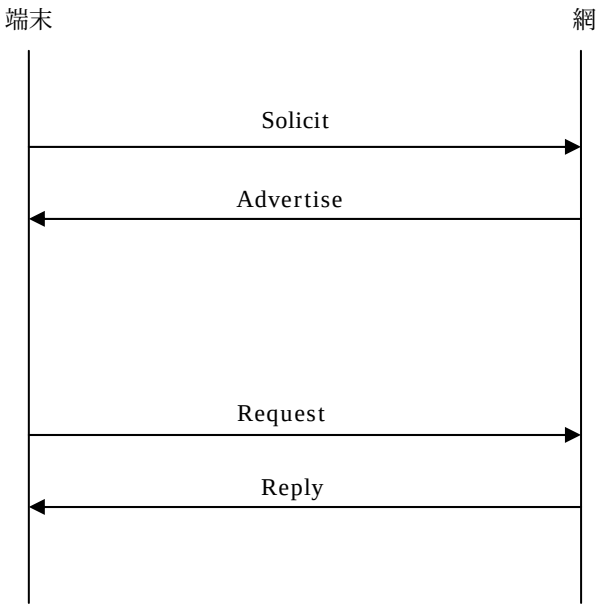


図 B-2：IPv6 アドレスプレフィックス払い出しシーケンス

端末は、IPv6 アドレスプレフィックスの割当を希望する場合、第 1 フェーズとして SOLICIT メッセージを網へ送信します。SOLICIT メッセージを受信した網は、IPv6 アドレスプレフィックス割当が可能な場合、ADVERTISE メッセージを用いて応答します。

網は、第 1 フェーズで IPv6 アドレスプレフィックス割当可能と判断した場合、第 2 フェーズとして、REQUEST メッセージを網に送信します。この時、端末は、要望するオプションリストを REQUEST メッセージに含めることが可能です。網は受信した REQUEST メッセージに対して、IPv6 アドレスプレフィックスと関連するオプションを含めて REPLY メッセージで応答します。また REPLY メッセージにその IPv6 アドレスプレフィックスに対する有効期限が含まれる場合は、端末は、その有効期限を記憶しなければいけません。

NDP に基づく IPv6 ステートレスアドレス自動生成端末が、DHCPv6 手順によりサーバアドレス情報取得のみを行う場合のシーケンスを図 B-3 に示します。

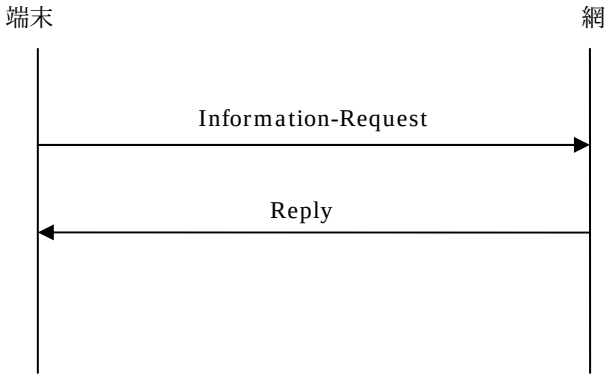


図 B-3：サーバアドレス情報通知シーケンス

網がサポートするメッセージを表 B-3 に示します。端末が規定外のメッセージを送信した場合、受信したサーバは無視し、廃棄を行います。

表 B-3：DHCPv6 サーバがサポートするメッセージタイプ

メッセージタイプ	値	説明
Solicit	1	クライアントがサーバの場所を検出するメッセージ
Advertise	2	サーバが DHCP サービスで利用可能であることを示すメッセージ
Request	3	設定パラメータを要求するメッセージ
Confirm	4	割り当てられた IPv6 アドレスが適切であるかを確認するメッセージ
Renew	5	IPv6 アドレスの寿命延長、他の設定パラメータの更新を行うメッセージ
Rebind	6	IPv6 アドレスの寿命延長、他の設定パラメータの更新を行うメッセージ（クライアントが Renew に対する Reply を受信できなかった場合）
Reply	7	サーバから割り当てた IPv6 アドレス、設定パラメータを通知するメッセージ メッセージの受領確認を示すメッセージ
Release	8	割り当てられた IPv6 アドレスを解放するメッセージ
Decline	9	割り当てられた IPv6 アドレスが他者により使用中であることを示すメッセージ
Reconfigure	10	サーバの設定パラメータが更新され、新しい情報の取得を促すメッセージ
Information-Request	11	IPv6 アドレス以外の情報を要求するメッセージ

B.2.2.1　DUID

全てのサーバ及びクライアントは、それぞれ相異なる DUID を用いて、互いを識別します。DUID は、可能な限り変更を行いません。サーバ及びクライアントは、受信メッセージの宛先確認のためのみに使用します。

クライアント側の DUID 生成方式は RFC3315 に準拠した方式のうち、リンクレイヤアドレスが含まれる方式（DUID-LL）を用いる必要があります。

クライアントの再設定を行う場合、Reconfigure メッセージのメッセージ認証方式として

Reconfigure Key Authentication Protocol を使用します。クライアントが再設定を行えるか否かは、クライアントが Solicit／Request／Information-Request メッセージのいずれかで Reconfigure Accept オプションを指定するか否かで判断を行います。

B.2.2.2　IA_PD

IA_PD を、IPv6 アドレスプレフィックスと、IPv6 アドレスプレフィックスを割り当てるインタフェースや設定情報などを関連づけて識別し、管理するために使用します。IA_PD はこのようなアソシエーションとアソシエーションに関する設定情報にて構成され、識別される IAID はユニークであることが必要です。つまり、クライアントにおいて、IA_PD と IAID の対応付けは、クライアントが再起動されても変更してはなりません。

特定の IA_PD に関する処理のステータスを表示する場合は、Status Code オプションを、対象となる IA_PD-options 構成に含める必要があります。

B.2.2.3　**オプション種別**

IANA により規定されるオプションコードを表 B-4 に示します。表 B-4 以外（IANA の規定外）の DHCP オプションを受信した場合は、受信側の動作は保証されません。なお、サーバは、各オプションを定義している RFC において、特定のメッセージでの使用が許可されないと規定されているオプションを含むメッセージを廃棄します。

表 B-4：DHCPv6 のオプション一覧

Option	code	RFC	説明
Client Identifier※1	1	RFC3315[26]	端末を識別する DUID
Server Identifier	2		網を識別する DUID
Identity Association for Non-temporary Address※2	3		IA_NA に関連する情報
Identity Association for Temporary Address※2	4		IA_TA に関連する情報
IA Address※2	5		IA アドレス
Option Request※1※3	6		要求するオプションのリスト
Preference※2	7		網側サーバの優先度
Elapsed Time	8		メッセージ交換の経過時間
Relay Message※2	9		リレー転送あるいはリレー応答メッセージで、DHCP メッセージを運ぶ
Authentication※3	11		メッセージ認証のための情報
Server Unicast※2	12		ユニキャストでのサーバアクセス可能
Status Code	13		状態表示
Rapid Commit※2	14		IPv6 アドレスプレフィックス割り当てで 2 メッセージ交換を使用
User Class※2	15		ユーザ／アプリケーションのタイプ／カテゴリを指定
Vendor Class※1※4	16		ベンダの識別情報 端末機器に設定するネットワーク関連情報等の通知を受けるための端末識別に使用する
Vendor-specific Information※4	17		ベンダ特有の情報 端末機器に設定するネットワーク関連情報等の通知に使用する
Interface-Id※2	18		リレーエージェントが端末のインタフェースを識別するために使用
Reconfigure Message※3	19		再設定メッセージで再設定すべき情報を指定
Reconfigure Accept※3	20		端末は再設定受け入れ可能なことを示し、網は Reconfigure メッセージ使用を通知します。また Reconfigure では認証情報を通知します。
SIP Servers Domain Name List※2	21	RFC3319[27]	SIP サーバのドメイン名
SIP Servers IPv6 Address List	22		SIP サーバのアドレス(IPv6)
DNS Recursive Name Server	23	RFC3646[31]	DNS サーバアドレス(IPv6)
Domain Search List	24		ドメインサーチリスト
Identity Association for Prefix Delegation (IA_PD) ※1	25	RFC3633[30]	IA_PD に関連する情報
IA_PD Prefix	26		IA_PD プレフィックス
NIS Servers※2	27	—	NIS サーバアドレス(IPv6)
NIS+ Servers※2	28		NIS+サーバアドレス(IPv6)
NIS Domain Name※2	29		端末の NIS ドメイン名
NIS+ domain name※2	30		端末の NIS+ドメイン名
SNTP Servers	31	RFC4075[33]	SNTP サーバアドレス(IPv6)

※1　端末から受信した値を網側で使用する項目。
※2　本インタフェース仕様では使用しません。
※3　再設定を使用する場合に使用する項目。
※4　ネットワーク関連情報等の端末機器への設定の自動化のために使用する可能性があります。

B.2.2.4　DNS サーバアドレス取得

網から端末に DNS サービスが提供される場合は、RFC3646[31]に従う手順で、DNS サーバの IPv6 アドレスが網から端末に配布されます。また DNS ドメインサーチリストも RFC3646[31]に従う手順で配布します。

B.2.2.5　SIP サーバアドレス取得

セッション制御用の IPv6 アドレスまたはホスト名を網から端末に配布するサービスを提供する場合には、RFC3319[27]の手順に従います。

B.2.2.6　SNTP サーバアドレス取得

網から端末に SNTP 機能が提供される場合は、RFC4075[33]に従う手順で、SNTP サーバの IPv6 アドレスが網から端末に配布されます。

B.2.2.7　DHCPv6-PD アドレスプレフィックス配布条件

DHCPv6-PD による IPv6 アドレスプレフィックス付与条件は、1 アクセスラインに対して、1IPv6 アドレスプレフィックスを付与します。なお、払い出し IPv6 アドレスプレフィックスを変更する機能も提供します。

付属資料 C　DNS

IPv6 に対応した端末は、インタラクティブ（ユニキャスト）通信時に、ホスト名解決のためのプロトコルとして DNS を使用することができます。

DNS プロトコル使用時に準拠する規定の一覧を表 C-1 に示します。

表 C-1：DNS 規定

レイヤ	参照文献	タイトル	備考
L5 以上	RFC1034[6]	Domain names – concepts and facilities	DNS について規定
	RFC1035[7]	Domain names – implementation and specification	DNS について規定
	RFC1123[8]	Requirements for Internet Hosts – Application and Support	DNS の実装について規定
	RFC2181[12]	Clarifications to the DNS Specification	DNS について規定
	RFC2308[48]	Negative Caching of DNS Queries (DNS NCACHE)	ネガティブキャッシュについて規定
	RFC2671[21]	Extension Mechanisms for DNS (EDNS0)	DNS において、ロング DNS ネーム問い合わせ･回答対応方法を規定
	RFC2782[23]	A DNS RR for specifying the location of services	SRV レコードを規定
	RFC3596[29]	DNS Extensions to Support IP Version 6	IPv6 対応を規定

付属資料 D　SNTP

IPv6 に対応した端末は、インタラクティブ（ユニキャスト）通信時に、時刻取得のためのプロトコルとして、SNTP を使用することができます。

SNTP 使用時に準拠する規定の一覧を表 D-1 に示します。

表 D-1：SNTP 規定

レイヤ	参照文献	タイトル	備考
L4 以上	RFC4330[34]	Simple Network Time Protocol (SNTP) Version 4 for IPv4、 IPv6 and OSI	SNTPv4 について規定

付属資料Ｅ　IPv6 ステートレスアドレス自動設定

端末のアドレスとして利用可能な IPv6 アドレスは、5.3.2.1 章に記載の通り、原則として、RFC3315 に規定される DHCPv6-PD を用い IPv6 アドレスプレフィックスを割り当てます。ただし、ユーザが DHCPv6-PD 非対応である１台の端末のみを UNI に接続する場合に限り、網は IPv6 ステートレスアドレス自動設定機能を提供します。

本付属資料は、IPv6 ステートレスアドレス自動設定シーケンスについて示すものであり、以下の２ステージから構成されます（図 E- １参照)。

(1) IPv6 ルーティング情報設定(NDP を利用)

(2) 各種サーバアドレスアドレス取得（DHCPv6 を利用）

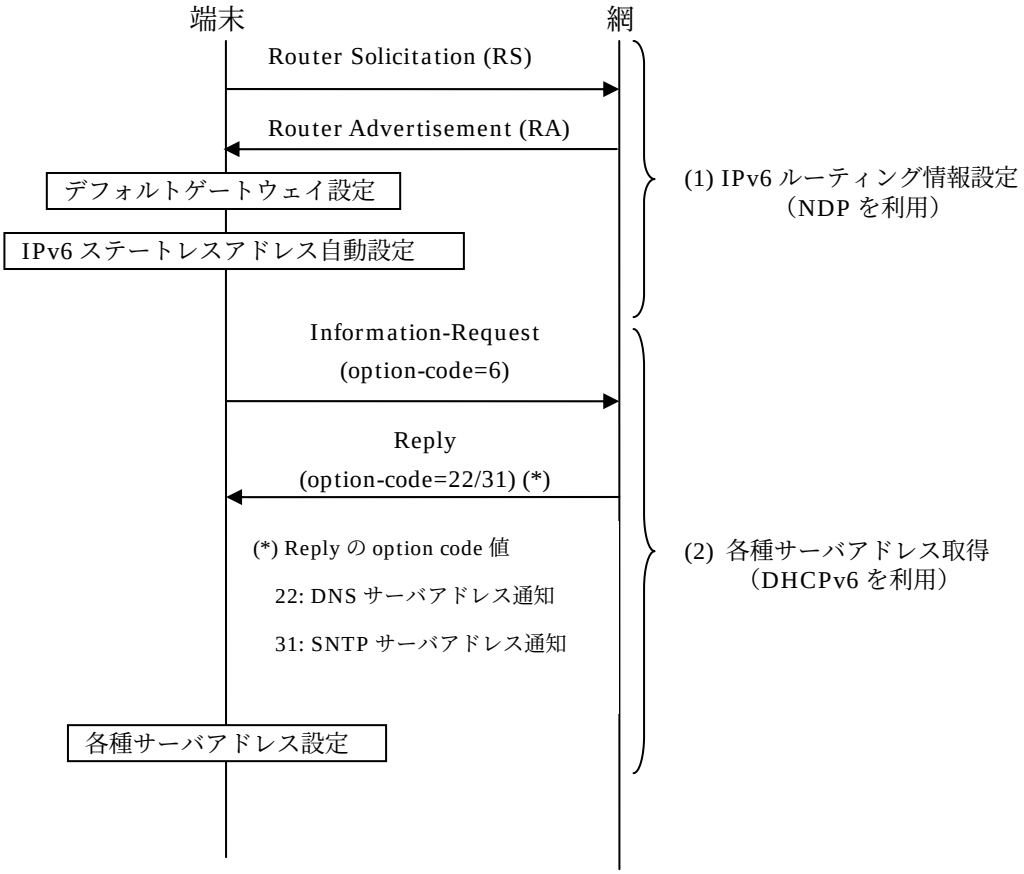


図 E- 1　IPv6 ステートレスアドレス自動設定シーケンス

(1) IPv6 ルーティング情報設定(NDP を利用)

網は、端末のアドレスとして利用可能な IPv6 アドレスに関し、RFC2461 に規定される Neighbor Discovery 手順(NDP)にて Router Advertisement (RA)メッセージによるアドレスプレフィックス（64 ビット長）を割り当てます。

端末は RFC2462 に規定された IPv6 ステートレスアドレス自動設定を行うと共に、デフォルトゲートウェイ設定も行うことが可能です。

(2) 各種サーバアドレスアドレス取得（DHCPv6 を利用）

網から端末への各種サーバアドレス通知については、RFC3736 に規定されるステートレス DHCPv6 機能を使用し、網が端末から受信する Information-Request メッセージに対する網からの Reply メッセージにて実現します。

網から端末に DNS サービスが提供される場合は、RFC3646 に従う手順で、DNS サーバの IPv6 アドレスが網から端末に配布されます。

網から端末に SNTP 機能が提供される場合は、RFC4075 に従う手順で、SNTP サーバの IPv6 アドレスが網から端末に配布されます。

なお、端末は Information-Request メッセージの Option Request Option (option-code=6) において、取得が必要な各種サーバアドレスに対応する option-code を全て記述することにより、DNS サーバアドレス取得・SNTP サーバアドレス取得を一括して要求し、Reply 受信にてそれらを一括して取得することが可能です。

次世代ネットワークインタフェース資料
（ＩＰ通信網）

― ユーザ・網インタフェース（UNI）―

別表１　インタラクティブ（ユニキャスト）通信機能

第 1.0 版

2007 年 10 月 25 日

目次

1. インタラクティブ（ユニキャスト）通信機能の概要

1.1. 機能の概要

本機能は、次世代ネットワークを利用する端末機器等（UNI）と電気通信事業者等（NNI）間、端末設備等（UNI）とアプリケーションサーバ機器等（SNI）間、及び端末機器等（UNI）相互の双方向及び片方向の IP 通信を提供します。

本機能では、次世代ネットワークのセッション制御機能を使用することにより、従来の固定系の電話番号（0AB～J）を接続先情報とする IP 電話機能（G.711μ-law）に加えて、多様なメディア（音声、映像等）での多様な通信形態（双方向、片方向）を提供します。

図 1-1 に次世代ネットワークにおけるインタラクティブ（ユニキャスト）通信の形態を示します。

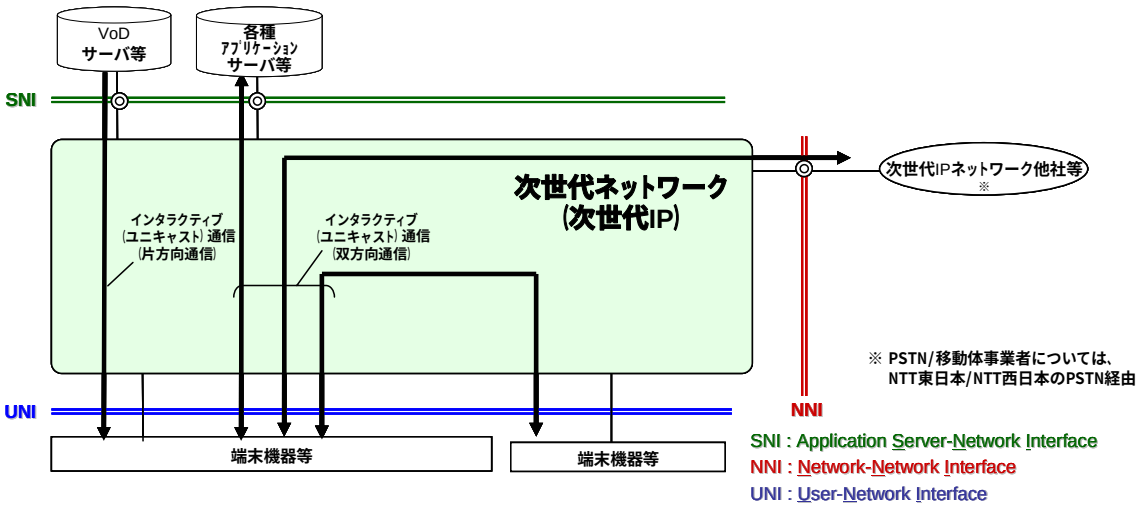


図 1-1：インタラクティブ（ユニキャスト）通信の形態

1.2. 提供機能

次世代ネットワーク インタラクティブ（ユニキャスト）通信機能の UNI で提供される転送品質クラスは、下記の 4 クラスです。

（1）　転送品質クラス　　最優先クラス
　　アドレス種別　　IPv4（UDP）/IPv6（UDP）
　　帯域　　セッション制御機能を利用して SDP の b=行の内容等で指定される

（2）　転送品質クラス　　高優先クラス
　　アドレス種別　　IPv4（TCP/UDP）/IPv6（TCP/UDP）
　　帯域　　セッション制御機能を利用して SDP の b=行の内容等で指定される

（3）	転送品質クラス	優先クラス
	アドレス種別	IPv4（TCP/UDP）/IPv6（TCP/UDP）
	帯域	セッション制御機能を利用して SDP の b=行の内容等で指定される
（4）	転送品質クラス	ベストエフォートクラス
	アドレス種別	IPv6（TCP/UDP）
	帯域	網による帯域制御機能は提供されない

提供機能及び品質クラスに関する詳細は、「次世代 IP　ユーザ・網インタフェース（UNI）本編」を参照してください。

2. 参照勧告類

本書が参照する勧告類を下記に示します。

[1] ITU-T Recommendation G.711 (11/1988): PULSE CODE MODULATION (PCM) OF VOICE FREQUENCIES
[2] TTC JT-G711v4 (04/2001): 音声周波数帯域信号の PCM 符号化方式
[3] TTC TS-1008 v1 (06/2005): 事業者 SIP 網における着サブアドレス情報転送サービスに関する技術仕様
[4] TTC TS-1009 v1.0 (08/2005): 事業者 SIP 網における SDP メディア能力交換に関するインタフェース技術仕様（MPEG4-Visual）
[5] TTC TR-9022 v2.0 (12/2006): NGN における網付与ユーザ ID 情報転送に関する技術レポート
[6] TTC TR-9024 v2.0 (12/2006): NGN に接続する SIP 端末基本接続インタフェース技術レポート
[7] IETF RFC768 (08/1980): User Datagram Protocol
[8] IETF RFC793 (09/1981): Transmission Control Protocol
[9] IETF RFC2326 (04/1998): Real Time Streaming Protocol (RTSP)
[10] IETF RFC2616 (06/1999): Hypertext Transfer Protocol – HTTP/1.1
[11] IETF RFC4733 (12/2006): RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
[12] IETF RFC3016 (11/2000): RTP Payload Format for MPEG-4 Audio/Visual Streams
[13] TTC JF-IETF-RFC3261 (06/2005): SIP: セッション開始プロトコル
[14] TTC JF-IETF-RFC3262 (06/2005): セッション開始プロトコル（SIP）における暫定レスポンスの信頼性
[15] TTC JF-IETF-RFC3264 (06/2005): セッション記述プロトコル（SDP）を使ったオファー／アンサーモデル
[16] TTC JF-IETF-RFC3311 (06/2005): セッション開始プロトコル（SIP）UPDATE メソッド
[17] TTC JF-IETF-RFC3323 (06/2005): セッション開始プロトコル（SIP）のためのプライバシー機構
[18] TTC JF-IETF-RFC3324 (06/2005): 網付与 ID 情報のための短期的な要求条件
[19] TTC JF-IETF-RFC3325 (06/2005): トラストドメイン内の網付与 ID 情報のためのセッション開始プロトコル（SIP）へのプライベート拡張
[20] TTC JF-IETF-RFC3327 (03/2007): 隣接していないコンタクトを登録するためのセッション開始プロトコル（SIP）の拡張ヘッダフィールド
[21] TTC JF-IETF-RFC3428 (09/2006): インスタントメッセージのためのセッション開始プロトコル（SIP）拡張
[22] TTC JF-IETF-RFC3455 (03/2007): 3GPP のためのセッション開始プロトコル（SIP）のプライベートヘッダ（P-Header）拡張
[23] TTC JF-IETF-STD64 (06/2005): RTP: リアルタイムアプリケーションのためのトランスポートプロトコル
[24] TTC JF-IETF-STD65 (06/2005): 最小限の制御による音声とビデオ会議のための RTP プロファイル
[25] TTC JF-IETF-RFC3608 (03/2007): 登録時のサービスルート検出のためのセッション開始プロトコル（SIP）拡張ヘッダフィールド
[26] TTC JF-IETF-RFC3966 (06/2005): 電話番号のための tel URI
[27] IETF RFC3984 (02/2005): RTP Payload Format for H.264 Video
[28] TTC JF-IETF-RFC4028 (08/2005): セッション開始プロトコル（SIP）におけるセッションタイマ
[29] TTC JF-IETF-RFC4145 (03/2007): セッション記述プロトコル（SDP）における TCP ベースのメディアトランスポート
[30] TTC JF-IETF-RFC4566 (03/2007): SDP: セッション記述プロトコル
[31] 3GPP TS 24.229 V7.2.0 (12/2005): IP multimedia control protocol based on Session Initiation

Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 7)
[32] 3GPP TS 29.208 V6.7.0 (06/2007): End-to-end Quality of Service (QoS) Signalling flows (Release 6)
[33] JT-G722v2.2 (06/2004): 64kbit/s 以下の 7kHz オーディオ符号化方式
[34] TTC JT-H264v2 (08/2006): オーディオビジュアルサービス全般のための高度ビデオ符号化方式
[35] TTC JF-IETF-RFC4715 (03/2007): tel URI のための ISDN サブアドレスエンコード形式
[36] IETF draft-ietf-sipping-race-examples-04 (08/2007): Examples call flow in race condition on Session Initiation Protocol
[37] IETF draft-ietf-sip-acr-code-05 (07/2007): Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)
[38] ISO 14496-2 (06/2004): Information technology – Coding of audio-visual objects – Part 2: Visual
[39] ISO 14496-3 (12/2005): Information technology – Coding of audio-visual objects – Part 3: Audio
[40] ITU-T Recommendation H.281 (11/1994): A FAR END CAMERA CONTROL PROTOCOL FOR VIDEOCONFERENCES USING H.224
[41] IETF RFC4573 (07/2006): MIME Type Registration for RTP Payload Format for H.224
[42] IETF draft-ietf-avt-rtp-uemclip-00 (05/2007): RTP payload format for UEMCLIP speech codec
[43] IPTV フォーラム IPTV サービス運用規定 第 1.0 版 (04/2007): 第六編 IPTV サービス通信運用規定

3. 規定範囲

3.1. 規定点

規定点については、「次世代 IP　ユーザ・網インタフェース（UNI）　本編」の 4.1.1 節を参照してください。

3.2. プロトコル一覧

プロトコル構成について、表 3-1 に示します。OSI 参照モデルに準拠した階層構成となっています。なお、使用するプロトコルについては、予告なく変更される場合があります。

表 3-1：インタラクティブ（ユニキャスト）通信機能のプロトコル構成

レイヤ		使用するプロトコル（ユーザ・網インタフェース）(※1)		
		セッション制御	メディア	その他
7	アプリケーション	SIP： TTC JF-IETF-RFC3261[13], TTC JF-IETF-RFC3262[14], TTC JF-IETF-RFC3311[16], TTC JF-IETF-RFC3323[17], TTC JF-IETF-RFC3324[18], TTC JF-IETF-RFC3325[19], TTC JF-IETF-RFC3327[20], TTC JF-IETF-RFC3428[21], TTC JF-IETF-RFC3455[22], TTC JF-IETF-RFC3608[25], TTC JF-IETF-RFC3966[26], TTC JF-IETF-RFC4028[28], TTC JF-IETF-RFC4715[35], TTC TS-1008[3], TTC TS-1009[4], TTC TR-9022[5], TTC TR-9024[6], 3GPP TS24.229[31], draft-ietf-sipping-race-examples-04[36], draft-ietf-sip-acr-code-05[37] SDP： TTC JF-IETF-RFC4566[30], TTC JF-IETF-RFC3264[15], TTC JF-IETF-RFC4145[29], 3GPP TS29.208[32]	RTP（ペイロード）： G.711 μ-law[1][2], DTMF[11], G.722[33], MPEG4-visual[4][12][38], H.264[27][34], UEMCLIP[42], MP4A-LATM[12][39], TTS[43], 1Dparityfec[43], FECC[40][41] RTP・RTCP： TTC JF-IETF-STD64[23], TTC JF-IETF-STD65[24], RTSP： RFC2326[9]	（端末・ｱﾌﾟﾘｹｰｼｮﾝｻｰﾊﾞ間通信） HTTP： RFC2616[10]
6	プレゼンテーション			
5	セッション			
4	トランスポート	UDP： RFC768[7]	UDP： RFC768[7] TCP： RFC793[8]	UDP： RFC768[7] TCP： RFC793[8]

注）「次世代 IP　ユーザ・網インタフェース（UNI）　本編」 表 4-1 に記載のあるプロトコルについては省略しています。

（※1）：本資料に記載のない内容については未サポートの場合があります。

4. インタフェース仕様

4.1. レイヤ 1～3 の仕様

レイヤ 1～3 のプロトコルについては「次世代 IP　ユーザ･網インタフェース（UNI）　本編」 5.1～5.3 節を参照してください。

4.2. レイヤ 4 仕様

レイヤ 4 プロトコルについては、次世代ネットワークのセッション制御機能を使用する場合は、セッション制御については UDP[7]を、メディアについては上位プロトコルに応じて UDP[7]または TCP[8]、またはその両方を使用します。

レイヤ 4 ヘッダ情報については、その一部（ポート番号、チェックサム）を網内で書き換えて転送制御に用いることがあります。

4.3. レイヤ 5 以上の仕様

レイヤ 5～7 のプロトコルについては、表 3-1 に従うものとします。SIP 及び SDP に関しては第 5 章・第 7 章と付属資料 A を、RTP・RTCP に関しては第 6 章と付属資料 B を参照してください。

5. セッション制御

5.1. セッション制御用プロトコル（SIP）

次世代ネットワークのセッション制御機能を使用する端末機器等は、セッション制御用ユーザエージェント（SIP-UA）を実装し、SIP-UA と網との間のセッション制御を許容するための登録手順とセッションの起動、停止を行うためのセッション制御手順が必要となります。

本章では、SIP-UA と網とのセッション制御で規定すべき内容について記載します。以下、本資料では、インタラクティブ（ユニキャスト）通信機能を利用する端末機器等を端末と呼びます。特に、網に対して、セッションを起動する側の端末を発端末、網からセッションを起動される端末を着端末と呼びます。

なお、本資料で規定しない内容に関しては、TTC TR-9024[6]をはじめ表 3-1 に示す参照勧告類に準拠してください。

5.1.1. セッション制御用ユーザエージェント（SIP-UA）の登録

5.1.1.1. SIP-UA 登録手順

SIP-UA の登録手順は以下の通りです。

(1) SIP-UA は登録要求を網に送信します。

(2) 網は SIP-UA に登録が完了したことを通知します。

(3) 網側の登録が完了すると、発着信が可能となります。

5.1.1.2. SIP-UA 登録の制限

契約者電話番号一つにつき、IPv4 一つ、または IPv4 と IPv6 それぞれ一つずつの IP アドレスの登録を許容します。追加電話番号及びサブアドレスについて追加の登録は不要です。なお、登録時には IPv4 を用いて SIP 信号の送受信を行ってください。

契約者電話番号一つに対して IPv4 と IPv6 の両アドレスを同時に使用する場合は、登録時に両アドレスを Contact に設定してください。

5.1.1.3. 登録失敗時の SIP-UA 登録再送条件

SIP-UA 登録時、網が REGISTER リクエストを受け付けることができず、登録が失敗となる場合があります。本事象が発生した場合、SIP-UA は、一定時間経過後に再送を行う必要があります。

5.1.2. セッション制御手順

SIP-UA のセッション制御手順は以下の通りです。

(1) SIP-UA は登録したアドレスから接続要求を網に送信します。
(2) 網は発着 SIP-UA の状態を確認し通信可能であれば、着 SIP-UA へ通知します。
(3) 着 SIP-UA は、網から通知された接続要求に対し、応答して SIP-UA 間の通信を開始します。
(4) 通信中の SIP-UA のどちらかが網に切断要求を送信すると、網は相手 SIP-UA に対し、切断要求を送信し SIP-UA 間の通信を終了します。

5.1.3. 同時通信可能数

セッション接続数（通話数）およびメディアストリーム（SDP の m=行で指定）数については、別途規定します。

5.2. SDP

SDP 仕様は、TTC JF-IETF-RFC4566[30]、TTC JF-IETF-RFC4145[29]で規定される SDP 仕様に従います。SDP ネゴシエーションは TTC JF-IETF-RFC3264[15]に従います。

5.2.1. メディア、コーデック（メディア・フォーマット）種別

メディア種別については、音声（m=audio）、映像（m=video）、その他（m=application）を許容します。

音声通信（m=audio）については G.711μ-law を基本とし、表 5-1 の音声コーデック種別での通信を許容します。b=行を指定する場合は、TTC JF-IETF-RFC4566[30]の規定に従ってください。

映像通信（m=video）については、表 5-1 の映像コーデック種別での通信を許容します。b=行を指定する場合は、TTC JF-IETF-RFC4566[30]の規定に従ってください。

その他のメディア通信（m=application）を行う場合は、b=行を指定することを推奨します。b=行の指定がない場合は、網で規定する値が設定されたものとします。また、m=行のトランスポートプロトコル（proto）として TCP の指定[29]も許容します。

なお、b=行で指定する帯域は、TTC JF-IETF-RFC4566[30]で参照される RFC4566 の 5.8 節に従い、b=AS 行を用いてレイヤ 4 及びレイヤ 3 プロトコルのオーバーヘッドを含む値を指定してください。

表 5-1：メディア、コーデック種別

	主なコーデック
音声通信 (m=audio)	G.711μ-law[1][2]
	G.722[33], DTMF[11], MP4A-LATM[12][39], UEMCLIP[42]
映像通信 (m=video)	MPEG4-visual[4][12][38], H.264[27][34], TTS[43], 1Dparityfec[43]

※）コーデックについては、変更されることがあります

端末は G.711μ-law のパケット化周期として、20ms のサポートを必須とします。

また、DTMF 送受信のため、RFC4733[11]に規定される telephone-event 形式の RTP メディアフォーマットをサポートします。

5.2.2. 制御信号における転送品質クラス指定方法

次世代ネットワークでは、表 5-2 の SDP の m=行の media-type と a=行の組み合わせでメディア（m=行）毎に転送品質クラスを指定します。（3GPP TS 29.208[32]参照）

転送品質クラスは SDP のオファー／アンサーの結果、メディア（m=行）の新規設定時に決定されます。メディア変更によって a=行によるメディア送受信モードが変更された場合も、転送品質クラスは変更されません。

なお、RTCP パケットの転送品質クラスは、表 5-2 に基づき指定される RTP パケットの転送品質クラスと同じとします。（3GPP TS 29.208[32]参照）

表 5-2：SDP による転送品質クラス指定方法

	最優先クラス	高優先クラス	優先クラス
SDP の m 行/a 行	以下の(1)～(2)のいずれかの場合： (1)media-type=video かつ a=sendrecv (2)media-type=audio かつ a=sendrecv	以下の(1)～(4)のいずれかの場合： (1)media-type=video かつ a=sendonly (2)media-type=video かつ a=recvonly (3)media-type=audio かつ a=sendonly (4)media-type=audio かつ a=recvonly	media-type=application

5.2.3. SDP のネゴシエーション手順

SIP-UA によるメディア確立のためのネゴシエーションは、オファー＆アンサー手順（TTC JF-IETF-RFC3264[15]）および 488 Not Acceptable Here レスポンスを受けた後のフォールバック（再発信）を組み合わせて実現されます。

5.2.3.1. ネットワークプロトコルの不一致

SIP-UA は、送信した INVITE リクエストに対して Warning コード 300 (Incompatible network protocol) もしくは 301（Incompatible network address formats）を含む 488 Not Acceptable Here レスポンスを受信する場合があります。

発側の SIP-UA が IPv6 をプロトコルとして用いていた場合、発側の SIP-UA は着側の SIP-UA が IPv4 しか利用できないために SDP のオファーに含まれる IPv6 アドレスを利用できないと解釈して、IPv4 によるフォールバックを試みることが可能です。

但し、フォールバックした呼に対し、上記レスポンスを受信してもさらなる再発信は許容されません。

また、INVITE リクエストを受信した SIP-UA は、SDP のオファーに含まれる IPv6 アドレスを利用できない場合で、IPv4 によるフォールバックを望む場合は、発側の SIP-UA に対して Warning コード 300 (Incompatible network protocol) を含む 488 Not Acceptable Here レスポンスを送信します。なお、ネットワークプロトコルの不一致の判定は、次節で記述するメディア、コーデック（メディア・フォーマット）の不一致の判定より先に処理することとします。

5.2.3.2. メディア、コーデック（メディア・フォーマット）の不一致

SIP-UA は、送信した SDP のオファーに対して 488 Not Acceptable Here レスポンス（Warning コード 304(Media type not available)または 305(Incompatible media format) が設定される場合もある）を受信する場合があります。

SDP のオファー側の SIP-UA は受信側の SIP-UA が SDP のオファーに含まれるメディアもしくはコーデック（メディア・フォーマット）が利用できないと解釈して、異なる内容の SDP のオファーに変更してフォールバックを試みることができます。また、488　Not Acceptable Here レスポンスの Message-Body 部に SDP が設定されている場合は、その中から利用可能なメディアおよびコーデック（メディア・フォーマット）を選択して、フォールバックを行うことができます。

但し、G.711 μ-law のみを含めた SDP のオファーを行ったにもかかわらず、488　Not Acceptable Here レスポンスを受けた場合は、それ以降のフォールバックを行わないこととします。

また、SDP のオファーを受信した SIP-UA は、SDP のオファーに含まれるメディアもしくはコーデック（メディア・フォーマット）を利用できない場合で、異なるメディアもしくはコーデック（メディア・フォーマット）によるフォールバックを望む場合は、SDP のオファーを送信した SIP-UA に対して、488 Not Acceptable Here レスポンスを送信することが可能です。なお、488 Not Acceptable Here レスポンスに Warning コード 304(Media

type not available)または 305(Incompatible media format)を付与することが可能です。

6. メディア条件

本章では、次世代ネットワークのセッション制御機能を使用した場合におけるメディア条件等について示します。

6.1. パケット送受信契機

端末がメディア通信を行うための RTP 等のパケット送受信契機を表 6-1 に記載します。

表 6-1：メディアパケットの送受信契機

端末条件	パケット送信条件	パケット受信条件	記事
メディアの新規設定要求の送信側	・オファーに対するアンサー受信時にメディア確立後送信開始	・オファー送信後に受信開始	
メディアの新規設定要求の受信側	・オファーに対するアンサー送信後に送信開始	・オファーに対するアンサー送信後に受信開始	
セッション切断／メディア削除要求の送信側	・送信停止後セッション切断(BYE または CANCEL 送信) ・Confirmed Dialog 確立前のエラーレスポンス送信時に送信停止 ・送信停止後にメディア削除要求の送信	・BYE（または CANCEL）送信時に受信停止 ・Confirmed Dialog 確立前のエラーレスポンス送信時に受信停止 ・メディア削除要求の送信時に受信停止	
セッション切断／メディア削除要求の受信側	・BYE（または CANCEL）受信時に送信停止 ・Confirmed Dialog 確立前のエラーレスポンス受信時に送信停止 ・メディア削除要求の受信時に送信停止	・BYE（または CANCEL）受信時に受信停止 ・Confirmed Dialog 確立前のエラーレスポンス受信時に受信停止 ・メディア削除要求の受信時に受信停止	・エラーレスポンスは、3xx～6xx が対象

注)　メディア変更時は、メディアストリーム毎に表 6-1 の規定が適用されます。

6.2. 音声利用における網サポート音源

音声メディアの双方向通信（IP 電話機能）における接続不可能時の音声トーキなどの可聴音等については網側でサポートしますが、状況によっては音源を提供できない場合もあります。なお、音源については、IPv4 での音声メディアの双方向通信で、かつ、コーデックが G.711μ-law の場合に提供されます。

網側サポートのトーキについては、網側から SDP 情報を設定した 18x レスポンス、またはその後の SDP 情報を含む UPDATE リクエストを SIP-UA 側へ送信することを契機に、

網から端末へ音声メディアストリームを提供します。また、網側トーキの完了時には呼を切断するため、SIP-UA 側にエラーレスポンスを送信します。

6.3. 音声利用における付加機能

現在、音声利用 IP 通信網で提供されている着信転送機能、発信電話番号通知要請機能、迷惑電話おことわり機能等の付加機能については、音声メディアの双方向通信で、かつ、コーデックが G.711μ-law の場合は提供可能です。その他のコーデック（メディア・フォーマット）利用時における付加機能については、サービス条件により規定されます。

なお、発信者 ID 受信機能については、G.711μ-law に限らず提供可能です。

7. SIP メッセージ定義

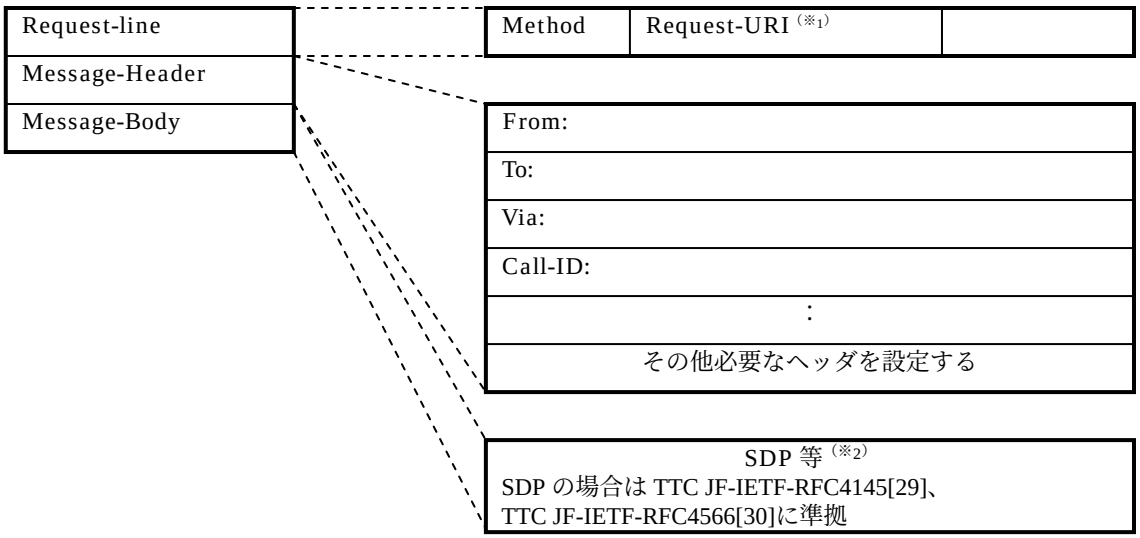
本章では、セッション制御に関する SIP-UA と網側の通信に必要なメッセージについて示します。

7.1. 基本フォーマット

SIP メッセージには、リクエストメッセージ及びレスポンスメッセージの 2 つのフォーマットが存在します。それぞれのフォーマット概要を下記に示します。なお、詳細な内容については、TTC JF-IETF-RFC3261[13]を参照してください。

7.1.1. リクエストメッセージ

リクエストメッセージについて図 7-1 に記載します。

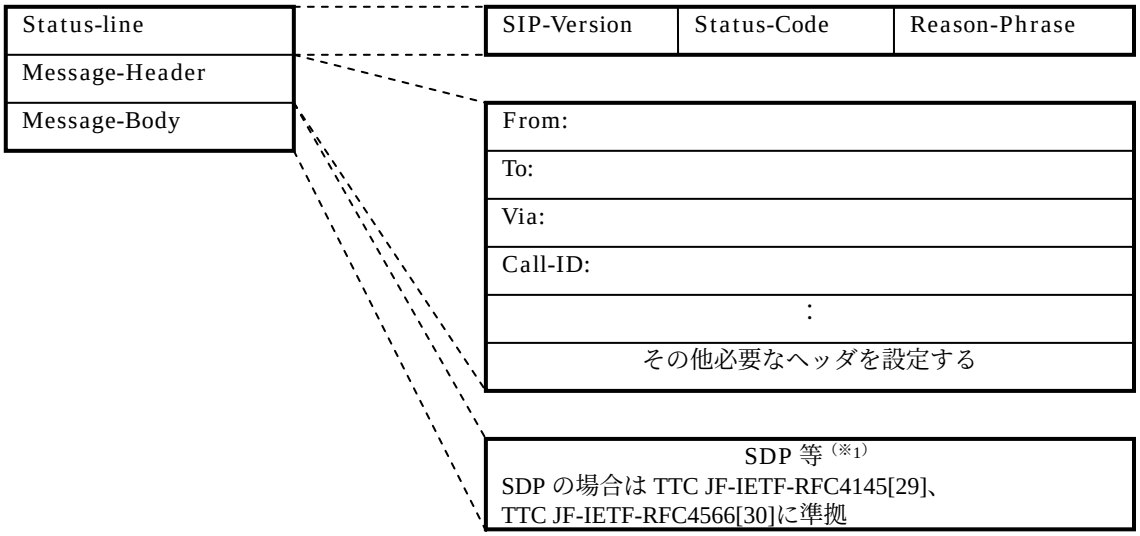


(※1) userinfo 部は電話番号に限定されない
（※2）MIME-Multipart は非許容

図 7-1：リクエストメッセージのフォーマット

7.1.2. レスポンスメッセージ

レスポンスメッセージについて図 7-2 に記載します。



（※1）MIME-Multipart は非許容

図 7-2：レスポンスメッセージのフォーマット

付属資料A　TTC TR-9024 に対するオプション選択

A.1　TR-9024 オプション選択

本付属資料では、TR-9024 付録 ii のオプション表について、本仕様における選択を示します。選択結果は下表の網掛け部分です。なお、下表中に記述されている「本文」は TR-9024 を、節に関する記述は TR-9024 の当該節を指します。

付表 ii-1／TR-9024　フォーマット例

項番	項目（本文該当箇所）	選択肢		備考
		網	ユーザ	
1	Supported ヘッダの設定	timer を提供	timer を設定する	
			timer を設定しない	
		100rel を提供	100rel を設定する	
			100rel を設定しない	
		提供しない	timer,100rel を設定する	
			timer,100rel を設定しない	

付表 ii-2／TR-9024　リクエスト信号

項番	項目（本文該当箇所）	選択肢		備考
		網	ユーザ	
1	ダイアログ外リクエストにおける Request-URI への SIP URI の設定（5.1.2）	許容する	利用する	
			利用しない	
		許容しない	利用しない	
2	ダイアログ外リクエストにおける Request-URI への TEL URI の設定（5.1.2）	許容する	利用する	
			利用しない	
		許容しない	利用しない	
3	セッション変更時の re-INVITE の送出（10.2.3）	許容する	利用する	網が許容する場合でも、要求内容や接続相手等により必ずしも変更要求が受け入れられるわけではない
			利用しない	
		禁止する	利用しない	
4	REGISTER の送出（13.1.1）	提供する	利用する	
			利用しない	
		提供しない	利用しない	
5	REGISTER の更新間隔（4.1.6）	指定する	指定値を設定する	網が指定する場合は、設定値を変更できる必要がある
		指定しない	任意値を設定する	
6	セッション変更時の UPDATE の送出（10.2.3）	許容する	利用する	網が提供していても Initial INVITE のネゴシエーションで利用できない場合あり
			利用しない	
		禁止する	利用しない	

項番	項目 （本文該当箇所）	選択肢		備考
		網	ユーザ	
7	ダイアログ外での MESSAGE の送出（13.1.1）	許容する	利用する	
			利用しない	
		許容しない	利用しない	
8	ダイアログ内での MESSAGE の送出（13.1.1）	許容する	利用する	
			利用しない	
		許容しない	利用しない	
9	ダイアログ外での REFER の送出（13.1.1）	許容する	利用する	
			利用しない	
		許容しない	利用しない	
10	ダイアログ内での REFER の送出（13.1.1）	許容する	利用する	
			利用しない	
		許容しない	利用しない	
11	SUBSCRIBE メソッドの送出(13.1.1)	提供する	利用する	
			利用しない	
		提供しない	利用しない	
12	NOTFY メソッドの送出（13.1.1）	提供する	利用する	
			利用しない	
		提供しない	利用しない	
13	PUBLISH メソッドの送出（13.1.1）	提供する	利用する	
			利用しない	
		提供しない	利用しない	
14	規定外のヘッダまたはパラメータの利用（13.3）	利用する	利用する	
			利用しない	
		利用しない	利用しない	

付表 ii-3／TR-9024　レスポンス信号

項番	項目	選択肢		備考
		網	ユーザ	
1	INVITE で 3xx レスポンスに対する転送（5.4.1）	3xx レスポンスを送信する可能性がある	利用する	転送は網からのものであることが確認され、且つセキュリティ上のリスクがないことが確認された場合のみ可能とする
			利用しない	
		送信しないことを保証する	利用しない	
2	REGISTER のレスポンス中の P-Associated-URI ヘッダの利用（13.4.6）	P-Associated-URI ヘッダを設定する可能性がある	利用する	
			利用しない	
		設定しないことを保証する	利用しない	
3	REGISTER の 200 レスポンス中の Service-Route ヘッダの利用（13.4.6）	Service-Route ヘッダを設定する可能性がある	利用する	
			利用しない	
		設定しないことを保証する	利用しない	
4	規定外のヘッダまたはパラメータの利用（13.4）	利用する	利用する	
			利用しない	
		利用しない	利用しない	

付表 ii-4／TR-9024　SDP

項番	項目	選択肢		備考
		網	ユーザ	
1	m=の fmt list に複数のコーデック設定（10.1）	許容する	複数コーデックを設定する	複数のコーデック設定時は優先順位を変更できる
			単一コーデックのみ設定する	
		許容しない	単一コーデックのみ設定する	
2	a=の ptime の設定（10.2）	許容する	設定する	設定時は値の変更が必要な可能性がある
			設定しない	
		許容しない	設定しない	
3	オファーに設定できるコーデックの数（10.2）	指定する	指定数以内で設定する	
		指定しない	任意の数を設定する	
4	リクエストの m=行の優先順位を指定（10.2）	指定する	指定する	
		指定しない	指定する	
			指定しない	
5	レスポンスの m=行の優先順位を指定（10.2）	指定する	指定する	
		指定しない	指定する	
			指定しない	
6	レスポンスの m=行のダイナミックペイロードタイプの設定（10.2）	オファーと同一値のみ許容	オファーと同一値を設定	
		オファーと異なる値を許容	オファーと同一値を設定	
			オファーと異なる値を設定	
7	レスポンスの a=行の設定（10.2）	オファーと同一値のみ許容	オファーと同一値を設定	
		オファーと異なる値を許容	オファーと同一値を設定	
			オファーと異なる値を設定	
8	G．711 μ-law 以外のコーデックの設定（10.2）	許容する	設定する	
			設定しない	
		許容しない	設定しない	

付表 ii-5／TR-9024　REGISTER

項番	項目	選択肢		備考
		網	ユーザ	
1	Request-URI の port 設定（4.1.2）	デフォルト値を提供する	設定する	デフォルト値を提供しない場合は値が変更できる必要がある
			設定しない	
		デフォルト値を提供しない	設定する	
			設定しない	
2	Contact の q パラメータの設定（4.1.3.2）	許容する	設定する	設定時は値が変更できる必要がある
			設定しない	
		禁止する	設定しない	
3	Contact の expires パラメータ値／Expires ヘッダの設定値（4.1.3.2）	固定値を指定する	指定値を設定する	設定時は値が変更できる必要がある 423 Interval Too Brief レスポンスを受けた場合の Expires に従う必要がある
		固定値を指定しない	任意値を設定する	
			設定しない	
4	From の設定（4.1.3.1）	To と異なる値を許容	To と異なる値を設定する	To と異なる値を設定する場合は値が変更できる必要がある
			To と同値を設定する	
		To と同値のみ許容	To と同値を設定する	
5	Contact の transport パラメータの設定（4.1.3.2）	UDP のみ許容する	UDP を設定する	
			設定しない	
		UDP または TCP を許容する	UDP を設定する	
			TCP を設定する	
			設定しない	
6	Allow ヘッダ設定（13.3.8）	設定を許容する	設定する	［以下 NTT 東日本/NTT 西日本追記］ ダイアログ外 MESSAGE を使用する場合は Allow ヘッダに記述する
			設定しない	
		設定を禁止する	設定しない	
7	Supported の path の設定（4.1.1）	path の設定を許容する	path を設定する	
			path を設定しない	
		path の設定を禁止する	path を設定しない	
8	登録状態変更通知予約の提供（4.6）	提供する	利用する	
			利用しない	
		提供しない	利用しない	

付表 ii-6／TR-9024　Initial INVITE

項番	項目	選択肢		備考
		網	ユーザ	
1	着側端末が Request-URI と REGISTER の Contact と検証する機能（6.1.2）	一致を保証する	検証する	
			一致による検証を行わない	
		一致を保証しない	一致による検証を行わない	
2	Request-URI の port 設定（5.1.2）	デフォルト値を提供する	設定する	デフォルト値を提供しない場合は値が変更できる必要がある
			設定しない	
		デフォルト値を提供しない	設定する	
3	Allow の PRACK の設定（13.3.5）	PRACK の設定を許容する	PRACK を設定する	［以下 NTT 東日本/NTT 西日本追記］ 100 Trying 以外の暫定応答を介在しない通信であることが明確である場合、PRACK を設定しなくてもよい
			PRACK を設定しない	
		PRACK の設定を許容しない	PRACK を設定しない	
4	Allow の UPDATE の設定（13.3.5）	UPDATE の設定を許容する	UPDATE を設定する	
			UPDATE を設定しない	
		UPDATE の設定を許容しない	UPDATE を設定しない (注)	
5	Allow に本書では規定外のメソッドの設定（13.3.5）	設定を許容する	規定外のメソッドを設定する	
			規定外のメソッドを設定しない	
		設定を禁止する	規定外のメソッドを設定しない	
6	From の userinfo 部の設定（5.1.3）	telephone-subscriber を提供する	telephone-subscriber を設定する	設定時は値が変更できる必要がある
		文字列を提供する	文字列を設定する	
7	Min-SE の設定（13.3.5）	指定する	設定する	設定時は値が変更できる必要がある
			設定しない	
		指定しない	設定しない	
8	Session-Expires の設定（13.3.5）	設定を許容する	設定する	設定時は値が変更できる必要がある
			設定しない	
		設定を禁止する	設定しない	
9	Supported の timer の設定（13.3.5）	timer の設定を許容する	timer を設定する	
			timer を設定しない	
		timer の設定を禁止する	timer を設定しない	
10	Supported の 100rel の設定（13.3.5）	100rel の設定を許容する	100rel を設定する	［以下 NTT 東日本/NTT 西日本追記］ 100 Trying 以外の暫定応答を介在しない通信であることが明確である場合、100rel を設定しなくてもよい
			100rel を設定しない	
		100rel の設定を禁止する	100rel を設定しない	

項番	項目	選択肢		備考
		網	ユーザ	
11	Supported に本書では規定外の Option-tag の設定（13.3.5）	設定を許容する	規定外の Option-tag を設定する	
			規定外の Option-tag を設定しない	
		設定を禁止する	規定外の Option-tag を設定しない	
12	Pre-existing ルートの設定（7.2.1）	許容する	利用する	
			利用しない	
		許容しない	利用しない	

注）　TR-9024 では「UPDATE を設定する」と記載しているが、誤記のため修正した。

付表 ii-7／TR-9024　re-INVITE

項番	項目	選択肢		備考
		網	ユーザ	
1	Allow の UPDATE の設定（13.3.7）	UPDATE を許容する	UPDATE を設定する	
			UPDATE を設定しない	
		UPDATE 設定を禁止する	UPDATE を設定しない	
2	Min-SE の設定（13.3.7）	指定する	設定する	設定時は値が変更できる必要がある
			設定しない	
		指定しない	設定しない	
3	Session-Expires の設定（13.3.7）	設定を許容する	設定する	設定時は値が変更できる必要がある
			設定しない	
		設定を禁止する	設定しない	
4	Supported の timer を設定（13.3.7）	timer の設定を許容する	timer を設定する	
			timer を設定しない	
		timer の設定を禁止する	timer を設定しない	

付表 ii-8／TR-9024　UPDATE

項番	項目	選択肢		備考
		網	ユーザ	
1	Min-SE の設定（13.3.9）	指定する	設定する	設定時は値が変更できる必要がある
			設定しない	
		指定しない	設定しない	
2	Session-Expires の設定（13.3.9）	設定を許容する	設定する	設定時は値が変更できる必要がある
			設定しない	
		設定を禁止する	設定しない	
3	Supported の timer の設定（13.3.9）	timer の設定を許容する	timer を設定する	
			timer を設定しない	
		timer の設定を禁止する	timer を設定しない	

付表 ii-9／TR-9024　MESSAGE

項番	項目	選択肢		備考
		網	ユーザ	
1	Pre-existing ルートの設定（13.1.1）	許容する	利用する	
			利用しない	
		許容しない	利用しない	

付表 ii-10／TR-9024　Initial INVITE リクエストに対するレスポンス設定

項番	項目	選択肢		備考
		網	ユーザ	
1	1xx,2xx レスポンスでの Allow で PRACK の設定（13.4.3）	PRACK を許容する	PRACK を設定する	［以下 NTT 東日本/NTT 西日本追記］ 100 Trying 以外の暫定応答を介在しない通信であることが明確である場合、PRACK を設定しなくてもよい
			PRACK を設定しない	
		PRACK を禁止する	PRACK を設定しない	
2	1xx,2xx レスポンスでの Allow で UPDATE の設定（13.4.3）	UPDATE を許容する	UPDATE を設定する	
			UPDATE を設定しない	
		UPDATE を禁止する	UPDATE を設定しない	
3	1xx,2xx レスポンスの Allow に本書では規定外のメソッドの設定（13.3.5）	設定を許容する	規定外のメソッドを設定する	
			規定外のメソッドを設定しない	
		設定を禁止する	規定外のメソッドを設定しない	
4	1xx レスポンスでの Require で 100rel の設定（13.4.3）	100rel を許容する	100rel を設定する	設定時は受信 INVITE の Supported に 100rel が設定されている場合が対象となる
			100rel を設定しない	
		100rel を禁止する	100rel を設定しない	
5	2xx レスポンスでの Require で timer の設定（13.4.3）	timer を許容する	timer を設定する	設定時は受信 INVITE の Supported に timer が設定されている場合が対象となる
			timer を設定しない	
		timer を禁止する	timer を設定しない	
6	1xx レスポンスでの RSeq の設定（13.4.3）	設定を許容する	設定する	設定時は受信 INVITE の Supported に 100rel が設定されている場合が対象となる
			設定しない	
		設定を禁止する	設定しない	
7	2xx レスポンスでの Session-Expires の設定（13.4.3）	設定を許容する	設定する	設定時は受信 INVITE の Supported に timer が設定されている場合が対象となる
			設定しない	
		設定を禁止する	設定しない	
8	2xx レスポンスでの Supported で timer の設定（13.4.3）	timer を許容する	timer を設定する	
			timer を設定しない	
		timer を禁止する	timer を設定しない	

付表 ii-11／TR-9024　re-INVITE リクエストに対するレスポンス設定

項番	項目	選択肢		備考
		網	ユーザ	
1	2xx レスポンスでの Allow で UPDATE の設定（13.4.5）	UPDATE を許容する	UPDATE を設定する	
			UPDATE を設定しない	
		UPDATE を禁止する	UPDATE を設定する	
			UPDATE を設定しない	
2	2xx レスポンスでの Require で timer の設定（13.4.5）	timer を許容する	timer を設定する	設定時は受信 INVITE の Supported に timer が設定されている場合が対象となる
			timer を設定しない	
		timer を禁止する	timer を設定しない	
3	2xx レスポンスでの Session-Expires の設定（13.4.5）	設定を許容する	利用する	利用時は受信 INVITE の Supported に timer が設定されている場合が対象となる
			利用しない	
		設定を禁止する	利用しない	
4	2xx レスポンスでの Supported で timer の設定（13.4.5）	timer を許容する	timer を設定する	
			timer を設定しない	
		timer を禁止する	timer を設定しない	

付表 ii-12／TR-9024　UPDATE リクエストに対するレスポンス設定

項番	項目	選択肢		備考
		網	ユーザ	
1	2xx レスポンスでの Require で timer の設定（13.4.7）	timer を許容する	timer を設定する	設定時は受信 UPDATE の Supported に timer が設定されている場合が対象となる
			timer を設定しない	
		timer を禁止する	timer を設定しない	
2	2xx レスポンスでの Session-Expires の設定（13.4.7）	設定を許容する	設定する	設定時は受信 UPDATE の Supported に timer が設定されている場合が対象となる
			設定しない	
		設定を禁止する	設定しない	
3	2xx レスポンスでの Supported で timer の設定（13.4.7）	timer を許容する	timer を設定する	
			timer を設定しない	
		timer を禁止する	timer を設定しない	

付表 ii-13／TR-9024　SIP メッセージの下位レイヤ

項番	項目	選択肢		備考
		網	ユーザ	
1	SIP メッセージの送受信に用いる下位レイヤ（3）	UDP/IPv4 以外を許容する	利用する	［以下 NTT 東日本/NTT 西日本追記］ UDP/IPv4 と UDP/IPv6 が利用可能である
			利用しない	
		UDP/IPv4 以外を許容しない	利用しない	

付表ii-14／TR-9024　サブアドレス

項番	項目	選択肢		備考
		網	ユーザ	
1	発サブアドレスの利用（付属資料 a）	許容する	利用する	
			利用しない	
		許容しない	利用しない	
2	着サブアドレスの利用（付属資料 a）	許容する	利用する	
			利用しない	
		許容しない	利用しない	

付属資料B　RTP・RTCP

インタラクティブ（ユニキャスト）通信機能（UNI）においては、メディア通信のプロトコルとして RTP 及び RTCP をサポートします。

B.1　RTP プロトコル

本節では、端末～網間における音声及び映像等のリアルタイムデータの通信に用いるプロトコルである RTP について規定します。

RTP 仕様としては、TTC JF-IETF-STD64[23]・TTC JF-IETF-STD65[24]と、本節にて参照される各勧告に準拠することとします。本節では、各勧告に加えてインタラクティブ（ユニキャスト）通信機能（UNI）における RTP 仕様として規定すべき事項について記述しており、本節で規定されていない事項については上述の各勧告を参照してください。

B.1.1　RTP ヘッダの定義

RTP ヘッダのフォーマットを図 B-1 に示します。

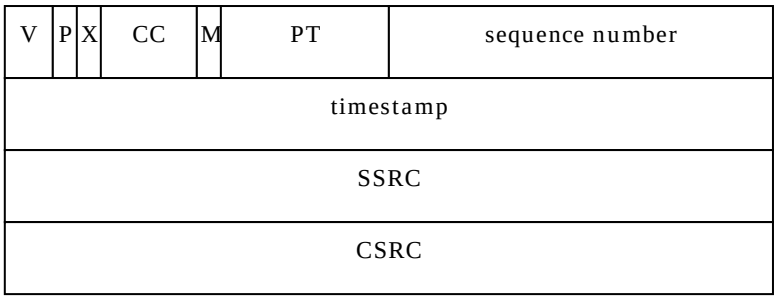


図 B-1：RTP ヘッダのフォーマット

（凡例）

V	バージョン番号
P	パディング
X	拡張ビット
CC	CSRC カウント
M	マーカビット
PT	ペイロードタイプ
sequence number	シーケンス番号
timestamp	タイムスタンプ
SSRC	同期ソース識別子
CSRC	貢献ソース識別子

B.1.1.1　バージョン番号

RTP パケットのバージョン番号を識別するために使用します。本書で定義しているバー

ジョンは 2 です。

B.1.1.2 マーカビット

マーカビットは通常 0 とします。ただし、表 B-1 に示すサービスの特定パケットについては、1 とします。

表 B-1：マーカビットを使用するパケット

サービス	対象パケット
DTMF（RFC4733[11]）	RFC4733 パケットのうち先頭パケット
映像(※1)	映像フレームの最後の RTP パケット

(※1) 双方向通信の場合

B.1.1.3 ペイロードタイプ

ペイロードタイプは、RTP のペイロードで送受信されるメディアの識別に使用します。その値としては、SIP 信号によりネゴシエーションされた値を使用します。

網は、あらかじめネゴシエーションされたペイロードタイプと異なるペイロードタイプ値のパケットを受信した場合は、転送を保証しません。

以下に音声及び映像で用いられるペイロードタイプを表 B-2 に示します。なお、その他のペイロードタイプは TTC JF-IETF-STD65[24]を参照してください。

表 B-2：ペイロードタイプの定義

Payload Type	Encoding Name	Codec 名	Media Type
0	PCMU	G.711 μ-law	音声
9	G722	G.722	音声
96～127	telephone-event	DTMF	音声
96～127	MP4A-LATM	MP4A-LATM	音声
96～127	UEMCLIP	UEMCLIP	音声
96～127	MP4V-ES	MPEG4-Visual Elementary Stream	映像
96～127	H264	H.264	映像
96～127	vnd.iptvforum.ttsavc	TTS	映像
96～127	vnd.iptvforum.1dparityfec_1010	1Dparityfec	映像
96～127	h224	FECC	データ

B.1.1.4 シーケンス番号

シーケンス番号はパケットロスの検出及び順序制御に使用します。

1 つの音声ストリームまたは映像ストリーム（同一 SSRC 値のストリーム）において、シーケンス番号の初期値はランダムな値から開始し、送信パケット毎にシーケンス番号の連続性を確保しなければなりません。

SSRC の値が変更された RTP パケットを受信した場合は、送信側のソースが変わったものとし、シーケンス番号は不連続となったと認識するべきです。この場合、シーケンス番

号の不連続はパケットロスとは見なしません。

宛先 IP アドレスおよび宛先 UDP ポート番号、もしくは送信元 IP アドレスおよび送信元 UDP ポート番号が変更となる場合、別セッション、別ストリームとして処理します。

B.1.1.5 タイムスタンプ

1 つの音声ストリーム（同一 SSRC 値のストリーム）において、タイムスタンプの初期値はランダムな値から開始し、サンプリング周期毎に単調かつ線形に増加した値とし、タイムスタンプの連続性を確保しなければなりません。

また、映像ストリームにおいては、1 つの映像フレームを分割し、複数の RTP で送信する場合、RTP ヘッダに同一のタイムスタンプを付加し送信することが許容されます。

SSRC の値が変更された RTP パケットを受信した場合は、送信側のソースが変わったものとし、タイムスタンプの値は不連続となったと認識すべきです。

宛先 IP アドレスおよび宛先 UDP ポート番号、もしくは送信元 IP アドレスおよび送信元 UDP ポート番号が変更となる場合、別セッション、別ストリームとして処理します。

B.1.1.6 SSRC

SSRC は、RTP ストリームの識別に使用します。

トランスポートアドレス（宛先 IP アドレスおよび宛先 UDP ポート番号、もしくは送信元 IP アドレスおよび送信元 UDP ポート番号）が変更となる場合、SSRC の値を変更しなければなりません。送信側においてトランスポートアドレスの変更はなくメディアソースが切り替わった場合、SSRC の値を変更するか否かはインプリメントに依存します。

SSRC の値が変更された RTP パケットを受信した場合は、送信側のソースが変わったものとし、シーケンス番号、およびタイムスタンプの値は不連続となったと認識すべきです。

B.1.1.7 パケットロスの検出

連続して受信される RTP パケットのシーケンス番号が欠落した場合は、パケットロスとして扱います。

ただし、SSRC の値の変更に伴いシーケンス番号が変更された場合は、パケットロスとは扱いません。

B.1.1.8 パケット送信可能期間

RTP パケットは、SIP 信号によるセッション確立とセッション切断の間に送出することとし、セッション確立前やセッション切断後に送出するべきではありません。

B.1.1.9 UDP ポート番号

RTP パケットの宛先 UDP ポート番号については、SIP 信号によりネゴシエーションされた宛先ポート番号を使用します。

使用可能な UDP ポート番号は 1024～65534 の偶数とします。

B.1.2　RTP パケット送信上の留意事項

SDP を用いたメディアのネゴシエーションにおいて、最新の SDP アンサーの内容が下記の条件を全て満たす場合、SIP-UA は RTP のメディアストリームを網に対して送信し続けて下さい。

- Media Description は 1 つのみ記述されていること。
- 音声の RTP メディア（m=行の media は audio で、proto は RTP/AVP）であること。
- 記述されているコーデックは、G.711 μ-law のみであること。ただし、DTMF（telephone-event）が併記されていてもよい。
- メディアは双方向（a=sendrecv）の送受信モードで新規設定されていること。

RTP パケットが一定期間送受信されていない場合、網は通信状態が異常であると見なし、対応する SIP セッションを強制的に解放して通信を切断する可能性があります。

なお、通信中のメディア変更により、SDP に a=sendonly/recvonly を含むオファー／アンサーが行われた場合、SIP-UA は RTP が送出される方向に対してのみ RTP パケットを送信し続けてください。同様に、a=inactive を含むオファー／アンサーが行われた場合、SIP-UA は RTP パケットを送信する必要はありません。

SDP に関する詳細は、5.2 節 SDP を参照してください。

B.2　RTCP プロトコル

本節では、サービス品質のモニタリングや通信者の情報の伝達等に使用されるプロトコルである RTCP について規定します。

B.2.1　RTCP ヘッダの定義

RTCP ヘッダのフォーマットは TTC JF-IETF-STD64[23]を参照してください。

B.2.2　RTCP 制御パケット種別

RTCP 制御パケット種別を表 B-3 に示します。

網はいずれの種別のパケットを受信しても内部に記述されている情報を参照することはありません。

表 B-3：RTCP 制御パケット種別

パケットタイプ	タイプ値	内容
SR	200	RTP 送出状態にある端末の送出データに関する情報、及び受信したデータに関する統計情報を通知
RR	201	RTP 非送出状態にある端末の受信データに関する統計情報、または RTP 送出状態にある端末において 31 個以上のソースからデータを受信している場合、SR と組み合わせて受信したデータに関する統計情報を通知
SDES	202	RTP 送信ソースに関するユーザ情報を通知
BYE	203	通信の終了を通知

B.2.3　RTCP パケットの送受信

網は RTCP パケットを送信可能な状態となった場合、RTCP パケットの送信を開始します。また、網が RTCP パケットを受信した場合、フォーマット等の正当性を確認します。

なお、RTCP パケットは、SIP 信号によるセッション確立とセッション切断の間に送出することとし、セッション確立前やセッション切断後に送出するべきではありません。

B.2.4　UDP ポート番号

RTCP パケットの宛先 UDP ポート番号については、対となる音声・映像フローの RTP パケットの宛先 UDP ポート番号に 1 を加えた値とし、使用可能な範囲は 1025～65535 とします。

B.2.5　RTCP パケット送信上の留意事項

(1) 網は、正当な RTCP パケットを受信した時点以降、一定時間 RTCP パケットを受信できない場合、通信が異常であると見なし、対応する SIP セッションを強制的に解放して通信を切断する可能性があります。従って端末は、RTCP パケットを定期的に送

信し続けてください。

(2) RTCP パケットを送出する場合、TTC JF-IETF-STD64[23]の 6.2 節と 6.3 節に記述される以下の条件に従ってください。

- RTCP パケット送信帯域が RTP パケット送信帯域の 5%以下であること

付属資料C　端末に期待する遅延品質配分

G.711μ-law における音声通信においては、遅延品質の配分として、発着端末合計での遅延時間が 80msec 以下であることを期待します。

次世代ネットワークインタフェース資料
（ＩＰ通信網）

― ユーザ・網インタフェース（UNI）―

別表２　マルチキャスト通信機能

第 1.0 版

2007 年 10 月 25 日

目次

1　マルチキャスト通信機能の概要

1.1　機能の概要

本機能は端末機器等からの要求に基づき、アプリケーションサーバ機器類から次世代ネットワークを介して IP マルチキャストによる映像配信等を行うものです。具体的には、IP 放送、および映像配信に伴う番組情報配信等の機能を提供します。

次世代ネットワークにおけるマルチキャスト通信の形態を示します。

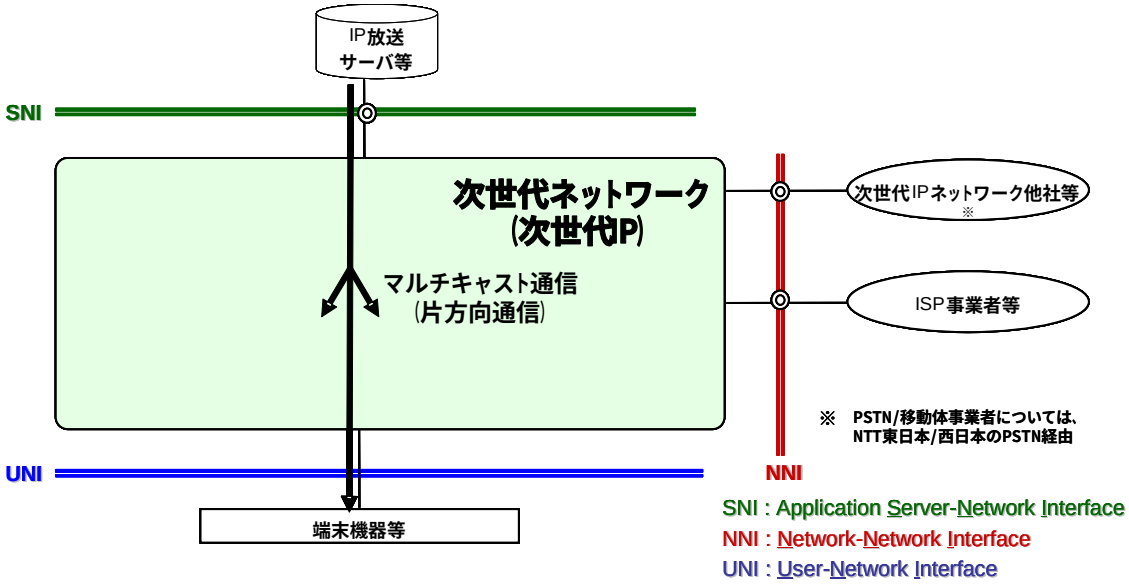


図 1-1：マルチキャスト通信の形態

1.2　提供機能

マルチキャスト通信の UNI において提供する転送品質クラスを以下に示します。

（１）転送品質クラス　　高優先クラス
　　アドレス種別　　IPv6

（２）転送品質クラス　　ベストエフォートクラス
　　アドレス種別　　IPv6

提供機能および品質クラスに関する詳細は、「次世代 IP ユーザ・網インタフェース（UNI）本編」を参照してください。

2　参照勧告類

本資料で参照する勧告類を下記に示します。

[1]　IETF RFC768 (08/1980): User Datagram Protocol
[2]　IETF RFC2460 (12/1998): Internet Protocol, Version 6 (IPv6) Specification
[3]　IETF RFC2461 (12/1998): Neighbor Discovery for IP Version 6 (IPv6)
[4]　IETF RFC4443 (3/2006): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
[5]　IETF RFC2711 (10/1999): IPv6 Router Alert Option
[6]　IETF RFC3315 (07/2003): Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[7]　TTC JF-IETF-STD64(06/2005):RTP:リアルタイムアプリケーションのためのトランスポートプロトコル
[8]　IETF RFC3633 (12/2002): IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
[9]　IETF RFC3646 (12/2003): DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[10]　IETF RFC3810 (06/2004): Multicast Listener Discovery Version 2 (MLDv2) for IPv6
[11]　IETF RFC4075(05/2005)　SNTP Configuration Option for DHCPv6

3　規定範囲

インタフェース規定点、端末設備と次世代ネットワーク側設備の分界点ならびに、施工・保守上の責任範囲については、「次世代 IP　ユーザ・網インタフェース（UNI）　本編」を参照してください。

3.1　プロトコル一覧

本資料で規定するインタフェースプロトコルの一覧を表 3-1 に示します。プロトコル構成は OSI 参照モデルに則した階層構造となっています。

表 3-1：規定するプロトコル一覧

レイヤ		使用するプロトコル	
7	アプリケーション	RTP:	TTC JF-IETF-STD64[7]
		DHCPv6:	RFC3315[6]*,RFC3646[9]*,RFC4075[11]*
6	プレゼンテーション	DHCPv6-PD:	RFC3633[8]*
5	セッション		
4	トランスポート	UDP:	RFC768[1]
3	ネットワーク	MLDv2:	RFC2711[5],RFC3810[10]
		IPv6:	RFC2460[2]*
		NDP:	RFC2461[3]*
		ICMPv6:	RFC4443[4]*

（注）*の記載があるプロトコルについては、「次世代 IP　ユーザ・網インタフェース（UNI）　本編」に規定しているため、本資料では、詳細な記述は省略してあります。

4　インタフェース仕様

4.1　レイヤ 1～2 の仕様

レイヤ 1 ～2 のインタフェース仕様については、「次世代 IP　ユーザ・網インタフェース（UNI）　本編」を参照してください。

4.2　レイヤ 3 仕様

マルチキャスト通信機能では、マルチキャスト配信を受信する端末の登録、削除手順については、RFC3810[10]に規定されている MLDv2 を用いることとします。MLDv2 の詳細については、第５章を参照してください。

なお、レイヤ３プロトコル（IPv6[2],ICMPv6[4],NDP[3]）については、「次世代 IP　ユーザ・網インタフェース（UNI）　本編」についても併せて参照してください。

4.3　レイヤ 4 仕様

4.3.1　UDP プロトコル

レイヤ 4 プロトコルとして、RFC768[1]に規定されている UDP を使用します。

UDP の詳細に関しては RFC768 を参照してください。

4.3.1.1　UDP ポート番号

表 3-1 に規定するレイヤ 5 以上のプロトコルのうち RTP プロトコルを使用する場合において使用可能な UDP ポート番号は 1024～65535 とします。

4.4　レイヤ 5 以上の仕様

端末機器類～次世代ネットワーク間における音声及び映像等のリアルタイムデータの通信には TTC JF-IETF-STD64[7]に規定されている RTP を用います。RTP 詳細に関しては、TTC JF-IETF-STD64 を参照してください。

なお、RTP 以外のプロトコルを用いる場合には、アプリケーションサーバ機器類等と端末機器等との間で別途規定する必要があります。

5　MLDv2 プロトコル

5.1　MLDv2 手順

マルチキャスト配信を受信する端末の登録・削除手順については、MLDv2 を用いることとします。

Multicast Listener Report メッセージを端末側から次世代ネットワークに送信する場合の ICMPv6[2]パケットのタイプ値は 143 を使用します。この値以外を設定した場合は、網は動作を保証しません。

MLDv2 は端末と次世代ネットワークの間で動作し、次世代ネットワーク側のルータがリスナーの存在を学習するために使用されます。ここで、リスナーとは、マルチキャストデータの受信を希望する端末であり、ルータはマルチキャストデータを端末に送信する次世代ネットワーク側のルータです。RFC3810[10]では、ルータがリスナーとしても動作することを許容していますが、本仕様では、次世代ネットワーク側のルータがリスナーとして動作することはしません。

MLDv2 によるマルチキャスト視聴要求のシーケンスを図 5-1 に示します。

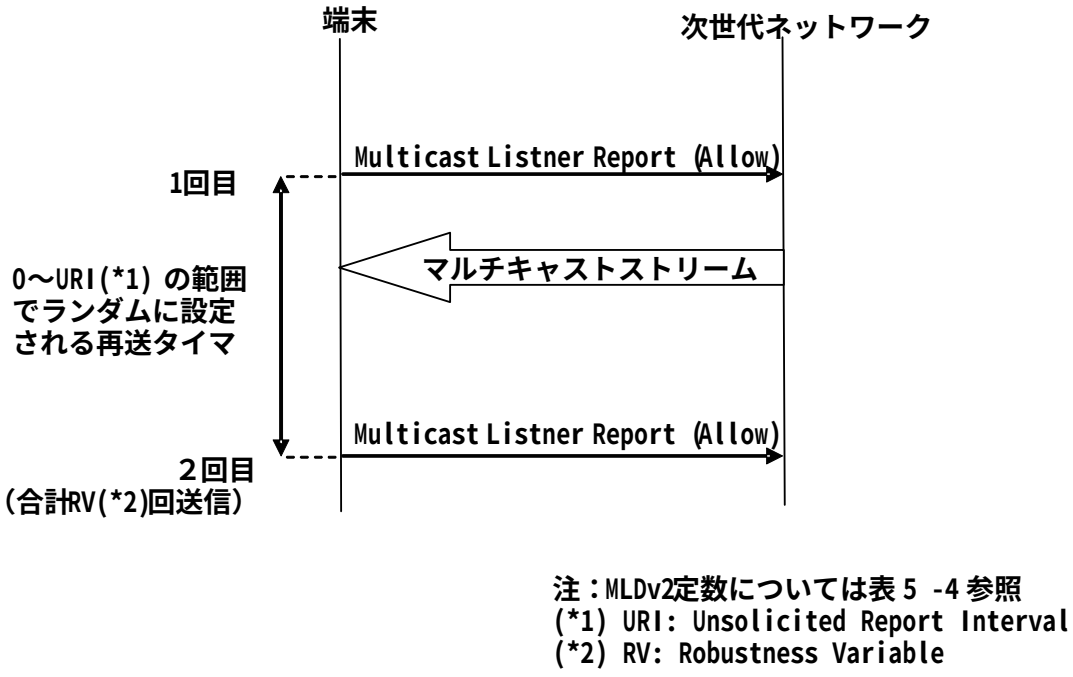


図 5-1：マルチキャスト視聴要求シーケンス

端末は、送信元アドレスが Unspecified Address (::)である MLD メッセージを送信してもよいが、次世代ネットワークは当該メッセージを受信した場合、廃棄します。

link-scope address (ff02::/16)のリスナーであることを通知するメッセージを受信した次世代ネットワークは、これを無視します。

MLDv2 では、受信を希望するマルチキャストアドレスについて、受信を希望するソースを指定する INCLUDE モードと、受信を拒否するソースを指定する EXCLUDE モードの 2 方式が動作可能ですが、本仕様では、INCLUDE モード動作のみを規定し、EXCLUDE モードでの次世代ネットワーク側動作は保証されません。

Multicast Listener Report メッセージ内において、Multicast Address Record に設定したマルチキャストアドレスを利用する通信に参加する場合は、その Record Type の値は 5(ALLOW_NEW_SOURCES)を使用します。

また、Multicast Listener Report に設定したマルチキャストアドレスを利用する通信から離脱する場合は、その Record Type の値は 6(BLOCK_OLD_SOURCES)を使用します。

なお、これらの値以外を Record Type に設定した場合は、1(MODE_IS_INCLUDE)を除き、動作を保証しません。図 5-2 に Multicast Address Record フォーマットを、表 5-1 にフィールド定義を示す。表 5-2 に MLDv2 の Record Type を示します。

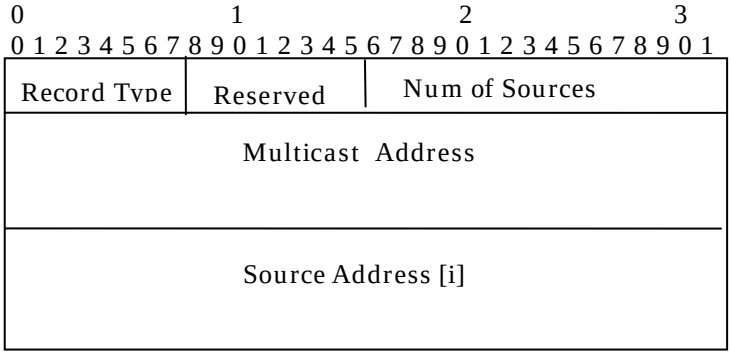


図 5-2：Multicast Address Record フォーマット

表 5-1：Multicast Address Record フィールド定義

No.	Field	Length	Definition
1	Record Type	8bits	表 5-2：Record Type 一覧 参照
2	Number of Sources	16bits	1 以上かつ 32 以下
3	Multicast Address	128bits	IPv6 マルチキャストアドレス(MA)
4	Source Address [i]	128bits	IPv6 グローバルアドレス i は１～32

表 5-2：Record Type 一覧

種別	Record　Type	略称	値	用途	備考
Current State Record	MODE_IS_ INCLUDE	IS_IN	1	Query 応答として送信する。MA に対するモードが INCLUDE であることを示す。	―
	MODE_IS_ EXCLUDE	IS_EX	-	Query 応答として送信する。MA に対するモードが EXCLUDE であることを示す。	Note
Filter Mode Change Record	CHANGE_TO_ INCLUDE_MODE	TO_IN	-	MA に対するモードが INCLUDE に変更された場合に送信する	Note
	CHANGE_TO_ EXCLUDE_MODE	TO_EX	-	MA に対するモードが EXCLUDE に変更された場合に送信する	Note
Source List Change Record	ALLOW_NEW_ SOURCES (ALLOW)	ALLOW	5	モード変更なしで、ソースリストのみが追加された場合に送信する。	―
	BLOCK_OLD_ SOURCES (BLOCK)	BLOCK	6	モード変更なしで、ソースリストのみが削除された場合に送信する。	―
Note:本仕様では使用しない Record Type。本メッセージを受信した場合の次世代ネットワーク側の動作は保証されない。					

5.2　メッセージ種別

MLDv2 インタフェースで使用するメッセージ種別を表 5-3 に示します。本項に示す以外の MLDv2 メッセージを受信した場合は次世代ネットワーク側の動作は保証されません。

表 5-3：MLDv2 のメッセージ一覧

No.	Message	Type	方向	備考
1	General Query	130	ネットワーク→端末 (Note1)	再送有
2	Multicast Address and Source Specific Query			
3	Multicast Address Specific Query			
4	Version2 Multicast Listener Report(Current State report)	143	ネットワーク←端末	再送有
5	Version2 Multicast Listener Report(State Change Report)			
6	Version1 Multicast Listener Report	―	―	Note2
7	Version1 Multicast Listener Done	―	―	Note2
Note1:端末は Query メッセージを送信してはならない。 Note2:本仕様では使用しない。本メッセージを受信した場合の次世代ネットワーク側動作は保証されません。				

General Query (GQ)は、リスナーの視聴を確認するために、次世代ネットワークより端末へ周期的に送信されます。

General Query (GQ)は、リスナーの視聴を確認するために、次世代ネットワークより端末へ周期的に送信されます。また、RFC3810[10]に規定するファーストリーブモードで動作します。

5.3 MLDv2 定数

MLDv2 定数一覧を表 5-4 に示します。

表 5-4：MLDv2 定数

No.	パラメータ	略称	定義	端末設定値
1	Robustness Variable	RV	パケット損失を想定したメッセージ送信回数	2
2	Multicast Address Listening Interval	MALI	次世代ネットワーク側ルータにてリスナーが存在しなくなったことを判断する時間	—
3	Query Response Interval	QRI	General Query に対する応答時間の最大値	Note1
4	Query Interval	QI	General Query の送信周期	—
5	Unsolicited Report Interval	URI	State Change Report の送信周期	1 秒
6	Last Listener Query Interval	LLQI	Multicast Address Specific Query 及び Multicast Address and Source Specific Query に対する応答時間の最大値	Note2 Note3
7	Last Listener Query Count	LLQC	Multicast Address Specific Query 及び Multicast Address and Source Specific Query の送信回数	Note3
8	Last Listener Query Timer	LLQT	次世代ネットワーク側ルータがリスナーが存在しなくなったことを確認する時間	Note3

Note1：　次世代ネットワーク側ルータにて 10000(10 秒)を端末に指示。
Note2：　次世代ネットワーク側ルータにて 1000(1 秒)を端末に指示。
Note3：　ファーストリーブの場合は使用しない。

次世代ネットワークインタフェース資料
（ＩＰ通信網）

― ユーザ・網インタフェース（UNI）―

別表３ PPPoE 接続機能（ISP 接続機能）

第 1.0 版

2007 年 10 月 25 日

目次

1　PPPoE 接続機能の概要

1.1　機能の概要

本機能は次世代ネットワークを利用する端末機器等(UNI)と ISP 事業者等(NNI)の接続制御機能を提供します。次世代ネットワークにおける PPPoE 接続機能の形態を図**１-1** に示します。

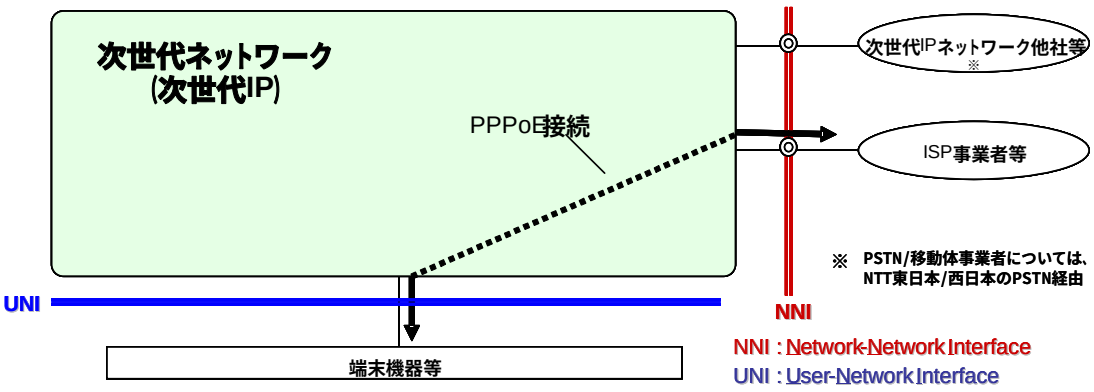


図 1-1：PPPoE 接続機能の形態

1.2　提供機能

PPPoE 接続機能において提供する転送品質クラスは、以下の通りです。

（１）転送品質クラス　　ベストエフォートクラス

提供機能および品質クラスに関する詳細は、「次世代ＩＰ　ユーザ・網インタフェース（ＵＮＩ）　本編」を参照してください。

2　参照勧告類

本資料で参照する勧告類を下記に示します。

[1]　IETF RFC791 (09/1980):Internet Protocol(IPv4)
[2]　IETF TFC792 (09/1981):Internet Control Message Protocol(ICMPv4)
[3]　IETF RFC1332 (05/1992): The PPP Internet Protocol Control Protocol (IPCP)
[4]　IETF RFC1334 (10/1992): PPP Authentication Protocols (PAP)
[5]　IETF RFC1661 (07/1994): The Point-to-Point Protocol (PPP)
[6]　IETF RFC1700(10/1994): Assigned Numbers
[7]　IETF RFC1877 (12/1995): PPP Internet Protocol Control Protocol Extensions for Name Server Addresses (IPCP)
[8]　IETF RFC1994 (08/1996): PPP Challenge Handshake Authentication Protocol (CHAP)
[9]　IETF RFC2516 (02/1999): A Method for Transmitting PPP Over Ethernet （PPPoE）
[10]　IEEE Std 802.3-2005 (12/2005): Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications - Media Access Control Parameters, Physical Layers and Management Parameters for subscriber access networks

3　規定範囲

インタフェース規定点、端末設備と次世代ネットワーク側設備の分界点ならびに、施工・保守上の責任範囲については、「次世代ＩＰ　ユーザ・網インタフェース（ＵＮＩ）　本編」を参照してください。

3.1　ユーザ・網インタフェースプロトコル

PPPoE 接続機能におけるユーザ・網インタフェースプロトコルの一覧を表 3-1 に示します。プロトコル構成は、OSI 参照モデルに則した階層構造となっています。

表 3-1：インタフェースのプロトコル一覧

レイヤ		使用するプロトコル
7	アプリケーション	
6	プレゼンテーション	
5	セッション	
4	トランスポート	
3	ネットワーク	IPv4: RFC791 [1] ICMPv4: RFC792 [2]
2	データリンク	IPCP: RFC1332[3], RFC1877 [7] PAP: RFC1334 [4] CHAP: RFC1994 [8] PPP: RFC1661 [5] PPPoE: RFC2516 [9] MAC: IEEE 802.3 [10]

4　インタフェース仕様

4.1　レイヤ１仕様

レイヤ１仕様については、「次世代ＩＰ　ユーザ・網インタフェース（ＵＮＩ）　本編」を参照してください。

4.2　レイヤ２仕様

レイヤ２では、IEEE.802.3[10]で規定されている MAC、及び PPP[5]、PAP[4]、CHAP[8]の一部、IPCP[3][7]、PPPoE[9]を使用します。MAC の詳細については、「次世代ＩＰ　ユーザ・網インタフェース（ＵＮＩ）　本編」を参照してください。また、PPP、PAP、CHAP、IPCP、PPPoE の詳細については、「第 5 章 PPPoE/PPP プロトコル」を参照してください。

4.3　レイヤ３仕様

レイヤ３プロトコルとして RFC791[1]に規定されている IPv4 を使用します。また、IP のサブセットとして、RFC792[2]に規定されている ICMPv4 の一部についてもサポートします。IPv4 の詳細については、RFC791 を、ICMPv4 の詳細については、RFC792 を参照してください。

4.3.1　IPv4 アドレス

PPPoE 接続機能においては、RFC1700[6]に規定されているクラス D（224.0.0.0/4）、クラス E（240.0.0.0/4）の IPv4 アドレスはサポートしません。また、端末機器の IPv4 アドレスとして利用可能な IPv4 アドレスは、網に接続する際に網または、接続先から割り当てられた IPv4 アドレスの範囲のみです。その他の IPv4 アドレスを利用した場合の動作は保証されません。

5　PPPoE/PPP プロトコル

5.1　PPP

PPP（Point-to-Point Protocol）[5]は、非同期（調歩同期:未提供）、同期型（ビット同期）両方の全二重回線上において、LCP（Link ControlProtocol）によるデータリンク回線の確立・設定・試験・解放、NCP（Network Control Protocol）によるネットワークレイヤのプロトコルの確立・設定を、RFC1661[5]の規定に従って行います。

PPPパケットのプロトコルフィールドに格納される値は表 5-1の通りです。

表 5-1：プロトコル識別子

値	プロトコル	用途
0xc021	Link Control Protocol (LCP)	LCP
0xc023	Password Authentication Protocol (PAP)	認証
0xc223	Challenge Handshake Authentication Protocol (CHAP)	
0x8021	Internet Protocol Control Protocol (IPCP)	NCP
0x0021	Internet Protocol (IP)	ネットワークレイヤプロトコル

5.1.1　LCP

LCP 通信設定オプション（LCP Configuration Option）のタイプ値を表 5-2 に示す。表 5-2 で示すタイプ値以外のオプションについては動作を保証しません。次世代ネットワークはMRU オプション(Maximum-Receive-Unit Option)の値を 1454 オクテットでネゴシエーション要求します。次世代ネットワークが要求する MRU 値より、小さな値で端末機器がネゴシエーション要求した場合、接続や正常な通信ができない場合があり、また、次世代ネットワークから要求する MRU 値を越えたパケットを次世代ネットワークが受信した場合においては、次世代ネットワーク内での分割転送が発生します。MRU の詳細についてはRFC1661[5]を参照してください。

表 5-2： LCP 通信設定オプションのタイプ値

タイプ値	オプション	設定条件
1	Maximum-Receive-Unit	使用
2	Asyncronous-Control-Character-Map	使用不可
3	Authentication-protocol	使用
4	Quality-Protocol	使用不可
5	Magic-Number	使用
7	Protocol-Field-Compression	使用不可
8	Address-and-Control-Field-Compression	使用不可
9	FCS-Alternative	使用不可

5.1.2 PAP

PAP[4]パケットの Peer-ID-Length フィールドに入る最大値は 0x3f であり、この最大値を超えた値を設定した場合、動作は保証しません。

5.1.3 CHAP

CHAP Response[8]パケットの Name フィールド長の最大長は 63 オクテットである。Name フィールド長がこの最大長を超えた場合については動作を保証しません。

5.1.4 IPCP

IPCP[7]通信設定オプション（IPCP Configuration Option）のタイプ値を表 5-3 に示す。表 5-3 で示すタイプ値以外のオプションについては動作を保証しません。

表 5-3：IPCP 通信設定オプションのタイプ値

タイプ値	オプション	設定条件
1	IP-Addresses	使用不可
2	IP-Compression-Protocol	使用不可
3	IP-Address	使用
129	Primary-DNS-Server-Address	使用可
130	Primary-NBNS-Server-Address	使用不可
131	Secondary-DNS-Server-Address	使用可
132	Secondary-NBNS-Server-Address	使用不可

5.2　PPPoE

PPPoEは、RFC2516[9]に規定の仕様に従って、Ethernet上でPPPを利用するためのPPPパケットのフレーム化と、Ethernet上の端末と次世代ネットワークとの間のPPPセッションの確立・設定・解放を行います。

PPPoEによりPPPセッションを確立・設定・解放するためのプロセスとして、ディスカバリステージ（Discovery stage）とPPPセッションステージ（PPP Session Stage）の２つのステージがあります。

PPPoEで利用するEthernetフレームおよびEthernetペイロードフィールドのフォーマットについてはRFC2516の規定に従います。パケット種別を示すコード値を設定するコードフィールド設定値について表 5-4に示します。

表 5-4：コードフィールドに設定する値

パケット種別	コード値
PPPoE Active Discovery Initiation（PADI）	0x09
PPPoE Active Discovery Offer（PADO）	0x07
PPPoE Active Discovery Request（PADR）	0x19
PPPoE Active Discovery Session-confirmation（PADS）	0x65
PPPoE Active Discovery Terminate（PADT）	0xa7
PPP セッションステージ	0x00

5.2.1　ディスカバリーステージ

PPPセッションを確立する相手のMACアドレスを特定し、PPPoEセッションIDの設定を行い、PPPoEセッションの確立を行うステージです。

ディスカバリステージには、PPPoEセッションの開始から確立までの動作と、解放を通知する動作が含まれます。

5.2.1.1　PPPoE セッションの開始から確立までの動作

PPPoEセッションの開始から確立までの手順を図 5-4に示します。

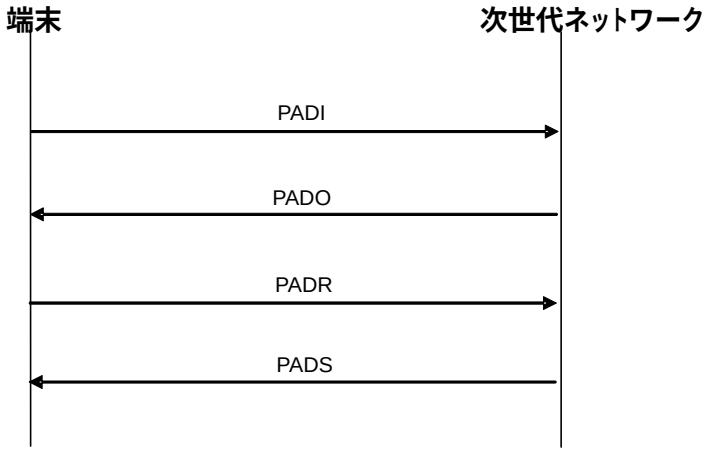


図 5-4：PPPoE セッション確立手順

本手順により、PPPoEセッションの開始から確立までの動作の各段階が完了すると、PPPoEセッションが確立され、端末と次世代ネットワークは固有のPPPoEセッションIDと相互のMACアドレスを認識します。PPPoEセッションの確立後、PPPセッションステージへ進みます。

5.2.1.2　PPPoE セッションの解放を通知する動作

PPPoEセッションの解放を通知する動作では、端末または次世代ネットワークからPPPoEセッションが解放されたことを通知するためにPADTパケットを送信します。

なお、ディスカバリステージにおいてPPPoEペイロードは、０個あるいは複数個のタグを含みます。

5.2.1.3　PADI パケット

端末は要求するサービス名を含むPADIパケットを送信し、次世代ネットワークにPPPoEセッションの開始を通知します。要求するサービス名を指定しない場合は、どのサービスでも受け入れられることを示します。あて先アドレスフィールドにブロードキャストアドレス0xffffffffffff、コードフィールドに0x09、セッションIDフィールドに0x0000 を設定します。端末が要求しているサービス名を示すService-Nameタグを含むことが必須です。Service-Nameタグのタグ値の長さフィールドに0x00を設定します。また、中間エージェントがRelay-Session-IDタグを追加することを考慮して、PADIパケットのサイズはPPPoEヘッダを含めて1484オクテットを超えることは許容できません。表 5-5にPADIパケットのタグ設定値を示します。

表 5-5：PADI パケットのタグ設定

タグタイプ	タイプ値	タグ値の長さ	タグ値	設定条件
End-Of-List	0x0000	ー	ー	未使用
Service-Name	0x0101	0	ー	使用
AC-Name	0x0102	ー	ー	未使用
Host-Uniq	0x0103	可変長	ー	使用可
AC-Cookie	0x0104	ー	ー	未使用
Vendor-Specific	0x0105	ー	ー	未使用
Relay-Session-Id	0x0110	ー	ー	未使用
Service-Name-Error	0x0201	ー	ー	未使用
AC-System-Error	0x0202	ー	ー	未使用
Generic-Error	0x0203	ー	ー	未使用

5.2.1.4　PADO パケット

PADIパケットを受信した次世代ネットワークは、送信元の端末にPADOパケットを送信し、次世代ネットワークがサポートするサービス名、網側装置(AC: Access Concentrator)名を通知します。コードフィールドには0x07、セッションIDフィールドには0x0000を設定します。ACの名前を示すAC-NameタグとPADIパケットと同一のService-Nameタグを含み、次世代ネットワークが他のサービス名もサポートする場合はそのService-Nameタグを含みます。表 5-6にPADOパケットのタグ設定値を示します。

表 5-6：PADO パケットのタグ設定

タグタイプ	タイプ値	タグ値の長さ	タグ値	設定条件
End-Of-List	0x0000	ー	ー	未使用
Service-Name	0x0101	0	PADI 送信値	使用
AC-Name	0x0102	可変長	ー	使用
Host-Uniq	0x0103	可変長	PADI 送信値	使用可
AC-Cookie	0x0104	可変長	ー	使用可
Vendor-Specific	0x0105	ー	ー	未使用
Relay-Session-Id	0x0110	ー	ー	未使用
Service-Name-Error	0x0201	ー	ー	未使用
AC-System-Error	0x0202	ー	ー	未使用
Generic-Error	0x0203	可変長	ー	使用可

5.2.1.5　PADR パケット

端末は受信したPADOパケットに含まれるAC名やサービス名をPADRパケットに設定し次世代ネットワークに送信します。コードフィールドには0x19、セッションIDフィールドには0x0000を設定します。端末が要求するサービス名を示すService-Nameタグを含むことが必須です。また、PADOパケットでAC-Cookieタグを受信した場合は、AC-Cookieタグを含むことが必須です。表 5-7にPADRパケットのタグ設定値を示します。

表 5-7：PADR パケットのタグ設定

タグタイプ	タイプ値	タグ値の長さ	タグ値	設定条件
End-Of-List	0x0000	ー	ー	未使用
Service-Name	0x0101	0	PADO 受信値	使用
AC-Name	0x0102	可変長	PADO 受信値	使用可
Host-Uniq	0x0103	可変長	PADO 受信値	使用可
AC-Cookie	0x0104	可変長	PADO 受信値	使用可*1
Vendor-Specific	0x0105	ー	ー	未使用
Relay-Session-Id	0x0110	ー	ー	未使用
Service-Name-Error	0x0201	ー	ー	未使用
AC-System-Error	0x0202	ー	ー	未使用
Generic-Error	0x0203	可変長	ー	使用可

*1：　PADOにAC-Cookieタグが含まれている場合は使用する。

5.2.1.6　PADS パケット

PADRパケットを受信した次世代ネットワークは、要求されたサービス名を受け入れる場合、PPPoEセッションの識別のために固有のセッションIDを生成し、セッションIDを含むPADSパケットを端末へ送信します。端末がPADSパケットを受信すると、端末と次世代ネットワークは固有のPPPoEセッションIDと相互のM ACアドレスを認識し、PPPoEセッションの確立が完了します。

次世代ネットワークは、要求されたサービスを拒否する場合、エラー内容を含むPADSパケットを送信しPPPoEセッションの確立を拒否します。コードフィールドには0x65、セッションIDフィールドにはこのとき生成した固有の値を設定します。要求を受け入れる場合、サービス名を示すService-Nameタグを含みます。

要求を拒否する場合、エラー内容を設定したService-Name-Errorタグを含めて、セッションIDには0x0000を設定する。表 5-8にPADSパケットのタグ設定値を示します。

表 5-8：PADS パケットのタグ設定

タグタイプ	タイプ値	タグ値の長さ	タグ値	設定条件
End-Of-List	0x0000	―	―	未使用
Service-Name	0x0101	0	PADR 送信値	使用*1
AC-Name	0x0102	可変長	PADR 送信値	使用可
Host-Uniq	0x0103	可変長	PADR 送信値	使用可
AC-Cookie	0x0104	可変長	PADR 送信値	使用可
Vendor-Specific	0x0105	―	―	未使用
Relay-Session-Id	0x0110	―	―	未使用
Service-Name-Error	0x0201	可変長	―	使用*2
AC-System-Error	0x0202	―	―	使用可
Generic-Error	0x0203	可変長	―	使用可

*1：要求されたサービス名を受け入れる場合に使用

*2：要求されたサービス名を拒否する場合に使用

5.2.1.7　PADT パケット

PPPoEセッション確立後、端末または次世代ネットワークはPPPoEセッションが解放されたことを通知するためPADTパケットを送信します。PADTパケットを受信すると、その後いかなるPPPトラフィックもこのPPPoEセッションを使用することは許可されません。コードフィールドには0xa7、セッションIDフィールドには解放されたPPPoEセッションのセッションIDを設定する。タグは不要とします。

5.2.2　　PPP セッションステージ

PPPセッションステージとは、PPPセッションを確立し、IP通信を行なうステージです。PPPセッションの解放によってPPPセッションステージは終了となります。

あて先アドレスフィールドおよび送信元アドレスフィールドには端末またはACのMACアドレス、コードフィールドには0x00、セッションIDフィールドにはディスカバリステージで割り当てられた固有の値を設定します。

PPPoEペイロードフィールドにはPPPフレームが格納され、そのフレームはPPPプロトコル識別子から設定します。

5.3　自動再接続間隔

自動再接続（網より端末機器へPADTが送出された後に、その端末機器が自動的に網へPADIを送出すること）の間隔は5秒以上でなければなりません。

5.4　PPPoE セッション数

PPPoE 接続機能おいては、同時に複数（最大２）の PPPoE セッションが利用可能です。

（注）セッション数の最大数は、今後変更される場合があります。

5.5　通信シーケンス

端末機器と次世代ネットワークの間の通信シーケンスを図4-5～図4-8に示します。

5.5.1　接続シーケンス

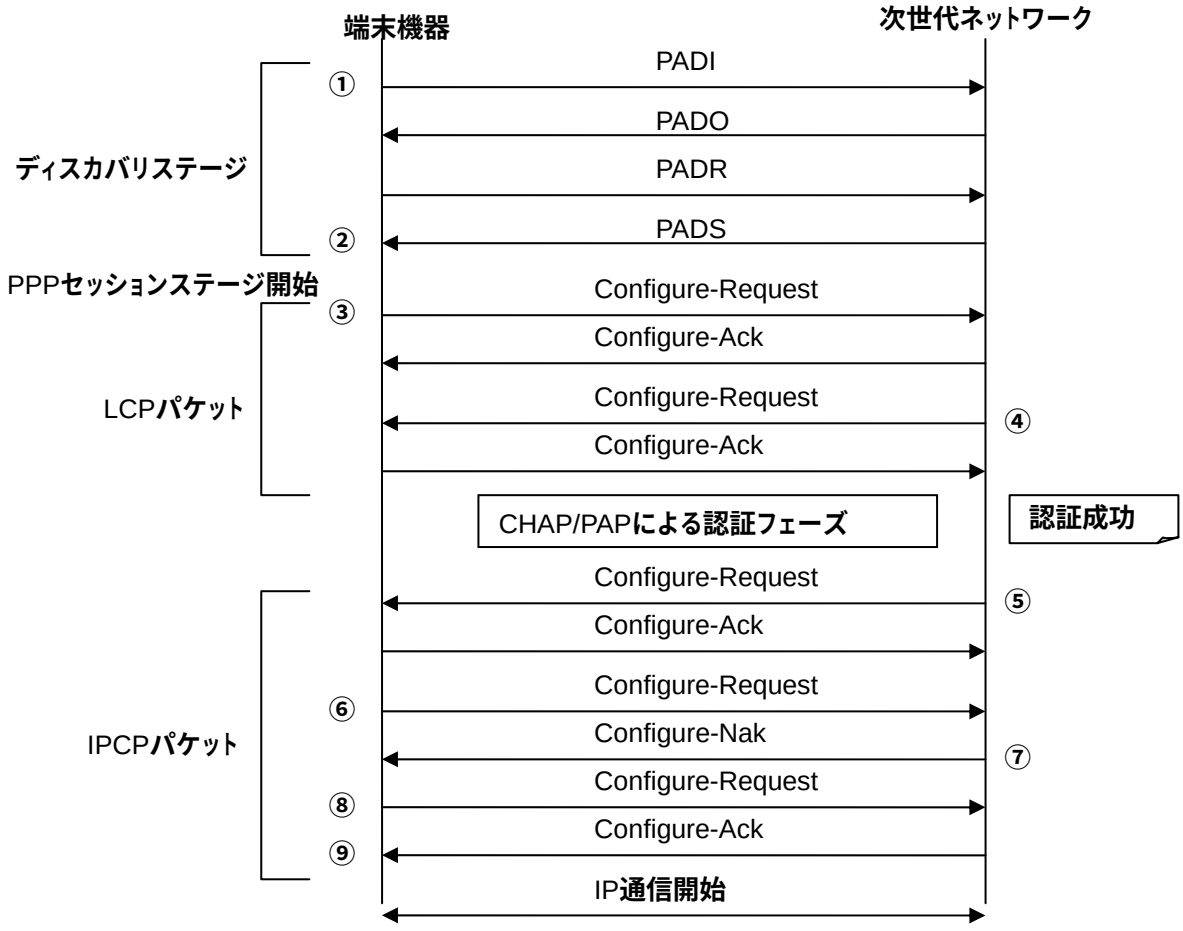


図4-5：接続シーケンス（例）

① PPPoE セッションの確立を開始
② PPPoE セッションが確立
③ PPP セッションの確立を開始
④ 認証プロトコルを要求
⑤ 網側の IP アドレスを通知
⑥ 端末機器が使用する IP アドレスを要求
⑦ 端末機器に割り当てる IP アドレス情報を返送
⑧ 端末機器が受信した IP アドレスを通知
⑨ PPP セッションが確立

5.5.2　切断シーケンス

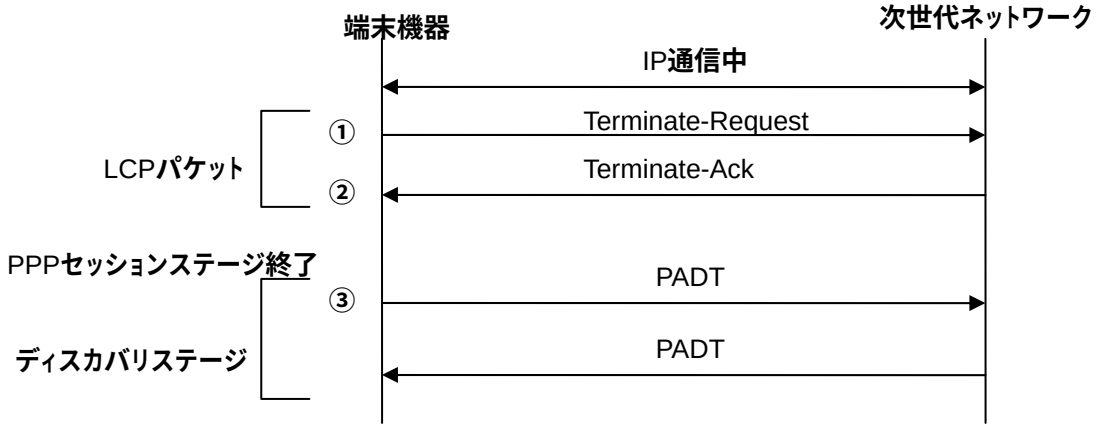


図4-6：切断シーケンス（例）

① PPP セッションの解放を開始
② PPP セッションを解放
③ PPPoE セッションの解放を通知

5.5.3　認証失敗シーケンス

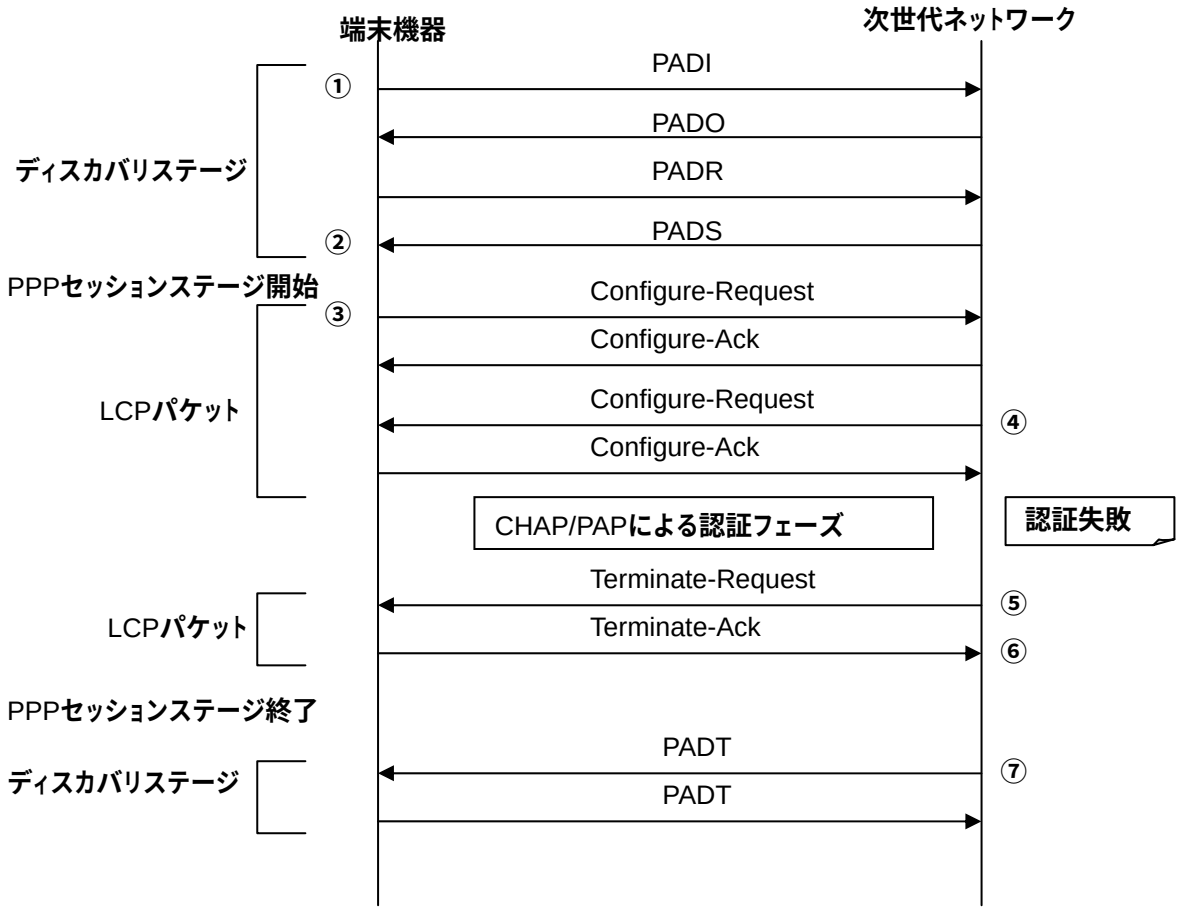


図4-7：認証失敗シーケンス（例）

① PPPoE セッションの確立を開始
② PPPoE セッションが確立
③ PPP セッションの確立を開始
④ 認証プロトコルを要求
⑤ PPP セッションの解放を開始
⑥ PPP セッションの解放
⑦ PPPoE セッションの解放を通知

5.5.4　強制切断シーケンス

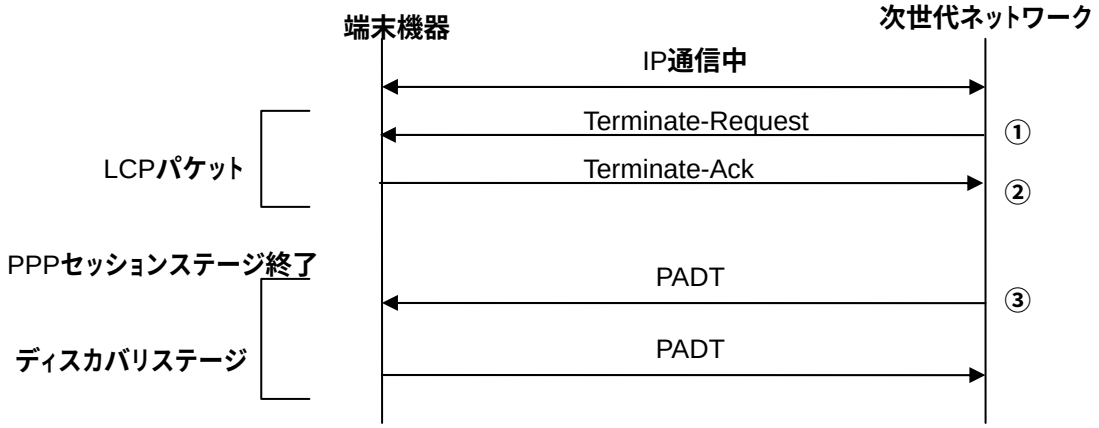


図4-8：強制切断シーケンス（例）

① PPP セッションの解放を開始
② PPP セッションを解放
③ PPPoE セッションの解放を通知

次世代ネットワークインタフェース資料
（ＩＰ通信網）

―　ユーザ・網インタフェース（UNI）―

別表４ PPPoE 着信機能

第 1.0 版

2007 年 10 月 25 日

目次

1　PPPoE 着信機能の概要

1.1　機能の概要

PPPoE 着信機能は、LAN やサーバ機器を次世代ネットワークに接続し、端末機器との IP 通信を提供するサービスです。

以下、本資料では、PPPoE 着信機能を利用する LAN やサーバ機器等をセンタ側端末機器、対向側の端末機器等をエンド側端末機器と呼びます。PPPoE 着信機能の基本構成の例を図 1-1 に示します。

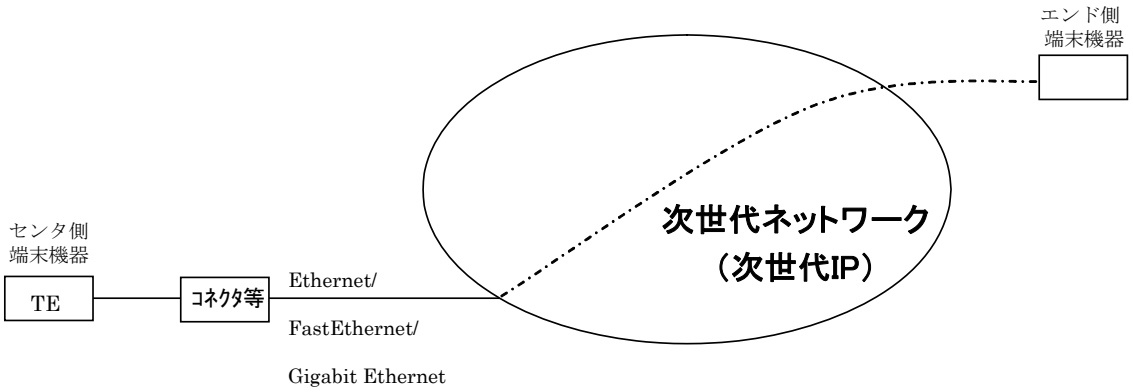


図 1-1：PPPoE 着信機能の基本構成

2　参照勧告類

本資料で参照する勧告類を下記に示します。

[1] IEEE Std 802.3-2005: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
[2] IETF RFC2865 (Remote Authentication Dial In User Service　2000.6)
[3] IETF RFC2866 (RADIUS Accounting　2000.6)
[4] IETF RFC791（Internet Protocol　1981.9）
[5] IETF RFC792（Internet Control Message Protocol　1981.9）
[6] IETF RFC826（An Ethernet Address Resolution Protocol:Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware　1982.11）
[7] IEEE Std 802.3 (Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part3:Carrier sense multiple access with collision detection(CSMA/CD) access method and physical layer specifications　1998 Edition)
[8] ISO IS 8877: 情報技術－システム間の電気通信及び情報交換－基準点 S 及び T に置かれた ISDN 基本アクセスインタフェース用のインタフェースコネクタ及び外部端子割当
Information technology－Telecommunications and information exchange between systems－Interface connector and contact assignments for ISDN Basic Access Interface located at reference points S and T
[9] IEC 60874-14(Connectors for optical fibres and cables　1997.6)
[10] ISO 9314-3(Information processing systems -- Fibre distributed Data Interface (FDDI) -- Part 3: Physical Layer Medium Dependent (PMD)　1990.10)
[11] ITU-T G.652 (Characteristics of a single-mode optical fibre and cable　2005.6)
[12] IETF RFC1700 (ASSIGNED NUMBERS　1994.8)
[13] IETF RFC1918 (Address Allocation for Private Internets　1996.2)

3　規定範囲

本資料では、次世代ネットワークとこれに接続する PPPoE 着信機能センタ側端末機器間のインタフェースを規定します。

3.1　インタフェース仕様

PPPoE 着信機能センタ回線のインタフェース仕様とインタフェース仕様を表 3-1 に示します。

表 3-1：PPPoE 着信機能センタ回線のインタフェース仕様

IF 仕様	IF 速度
10BASE-T	10M
100BASE-TX	100M
100BASE-FX	100M
1000BASE-LX	1G

3.2　規定点

ユーザ・網インタフェース規定点を、図 3-1 に示します。

規定点は、当社の施工・保守上の責任範囲の境界を定めています。

物理的には、10BASE-T、100BASE-TX の場合は UTP ケーブルのコネクタ部分,

100BASE-FX、 1000BASE-LX の場合は光ファイバケーブルのコネクタ部分が規定点となります。

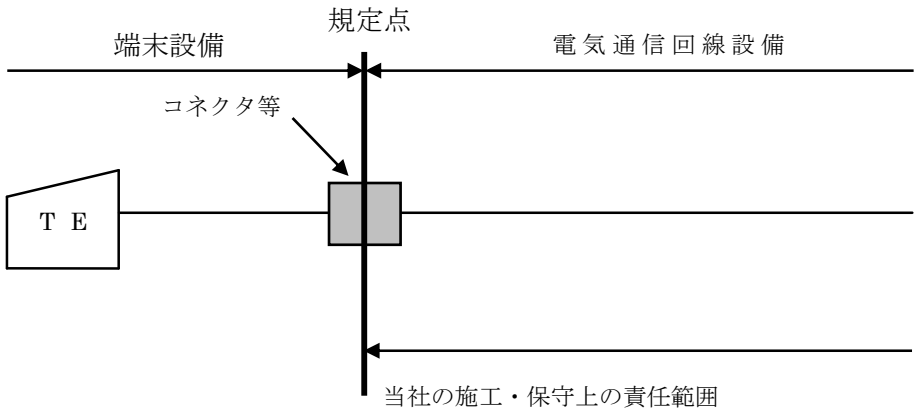


図　：3-1 規定点

3.3　プロトコル一覧

次世代ネットワークとこれに接続するセンタ側端末機器間で規定するインタフェースプロトコルの一覧を表 3-2 に示します。

表 3-2：OSI レイヤの関連規格

OSI レイヤ	内容と関連規格
7　アプリケーション層	RFC2865（RADIUS） RFC2866（RADIUS Accounting）
6　プレゼンテーション層	
5　セッション層	
4　トランスポート層	
3　ネットワーク層	RFC791（IP） RFC792（ICMP）
2　データリンク層	RFC826（ARP） IEEE 802.3（MAC）（注 1）
1　物理層	IEEE 802.3　10BASE-T IEEE 802.3　100BASE-TX IEEE 802.3　100BASE-FX IEEE 802.3　1000BASE-LX

（注 1）フレームフォーマットについては、DIX 規格の Ethernet Ver.2 のフォーマットも使用します。

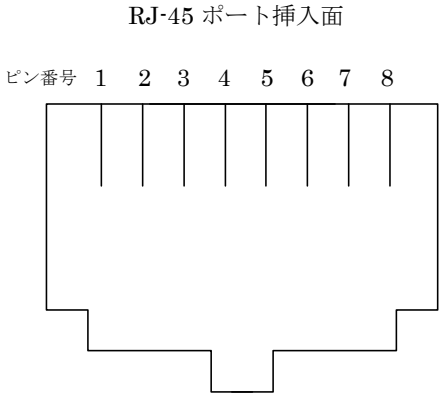
4　インタフェース仕様

4.1　レイヤ１仕様

レイヤ 1 のインタフェース条件は、10Mbit/s の場合は IEEE802.3 標準の 10BASE-T、100Mbitb/s の場合は IEEE802.3 標準の 100BASE-TX、100BASE-FX、1Gbit/s の場合は IEEE802.3 標準の 1000BASE-LX に準拠し、それぞれの伝送速度でベースバンド信号の転送を行います。利用可能な通信モードは全二重固定です。

4.1.1　　インタフェース条件（10BASE-T，100BASE-TX）

提供するユーザ・網インタフェースは、ISO8877 準拠の 8 極モジュラジャックである RJ-45 ポート（1 ポート）です。モジュラジャックの挿入面から見た RJ-45 ポートのピン配置を図 4-1 に示します。



	記号	信号方向		ピン番号
		TE	次世代ﾈｯﾄﾜｰｸ	
送信	TD(+)	←		3
	TD(-)	←		6
受信	RD(+)	→		1
	RD(-)	→		2

※ピン番号 4、5、7、8 は使用しません

図 4-1：挿入面から見た RJ-45 ポートのピン配置

4.1.2　　インタフェース条件（100BASE-FX）

提供するユーザ・網インタフェースは、IEC60874-14 準拠した SC コネクタ（オス）です。SC コネクタの数は、送信受信各 1 です。

また、光ファイバは、ISO9314-3 で規定されたコア径/クラッド径が 62.5μm/125μm のマルチモードを使用します。

4.1.3　インタフェース条件（1000BASE-LX）

提供するユーザ・網インタフェースは、IEC60874-14 準拠した SC コネクタ（オス）です。 また、光ファイバは、ITU-T G.652 で規定されたコア径/クラッド径が 9～10μm/125μm のシングルモードを使用します。

4.2　レイヤ２仕様

レイヤ２では、IEEE802.3 に規定されている MAC 及び、RFC826 に規定されている ARP を使用します。また、DIX 規格 Ethernet Ver.2 に規定されているフレームフォーマットも使用します。

MAC についての詳細は IEEE802.3 を、ARP についての詳細は RFC826 を、フレームフォーマットについての詳細は DIX 規格 Ethernet Ver.2 を参照してください。

4.3　レイヤ３仕様

レイヤ 3 では、IPv4 をサポートします。

4.3.1　IPv4 プロトコル

レイヤ 3 プロトコルとして、網は IPv4 をサポートします。サポートする IPv4 は、RFC791 の規定に従います。なお、IP ヘッダ情報（DSCP、パケット長、フラグ、フラグメントオフセット、TTL、ヘッダチェックサム、送信元 IPv4 アドレス、宛先 IPv4 アドレス）については、網内で書き換えて転送制御に利用することがあります。

4.3.2　IPv4 アドレス

IPv4 アドレスとしては、RFC791 に規定されている IPv4 アドレスをサポートすることとしますが、RFC1700 に規定されているクラス D（224.0.0.0/4）、クラス E（240.0.0.0/4）の IPv4 アドレスは使用しません。また、端末が利用可能な IPv4 アドレスは、網に接続する際に網から割り当てられた IPv4 アドレスの範囲のみで、その他の IPv4 アドレスを利用した場合の動作は保証されません。

グローバルアドレスを使用する場合は、JPNIC 等のインターネットレジストリから割当てられているグローバルアドレスを使用する必要があります。

4.3.3　接続用 IPv4 アドレス

センタ側端末機器と次世代ネットワークの接続には独立したサブネットを使用します。

独立した接続用のサブネットには、ネットワークアドレス、ブロードキャストアドレス、2 つ以上のホストアドレスが必要です。

センタ側端末機器と次世代ネットワーク間で IP 通信を行うために、センタ側端末機器の次世代ネットワークを接続するインタフェース及び、次世代ネットワークに対し接続用のサブネットのホストアドレスを付与します。

4.3.4　ルーティング

次世代ネットワークとセンタ側端末機器間のルーティングはスタティックルーティングです。

4.3.5　最大転送単位（MTU）

次世代ネットワーク内の MTU の値は 1454byte です。MTU の値を越えるデータグラムを次世代ネットワークが受信した場合、次世代ネットワーク内で分割転送が発生する場合があります。

4.4　上位レイヤ（レイヤ４～７）仕様

上位レイヤ（レイヤ 4～7）については、認証関連通信のプロトコルのみ規定します。

また、認証関連通信のプロトコルの詳細は、[5. 認証関連通信]を参照してください。

5　認証関連通信

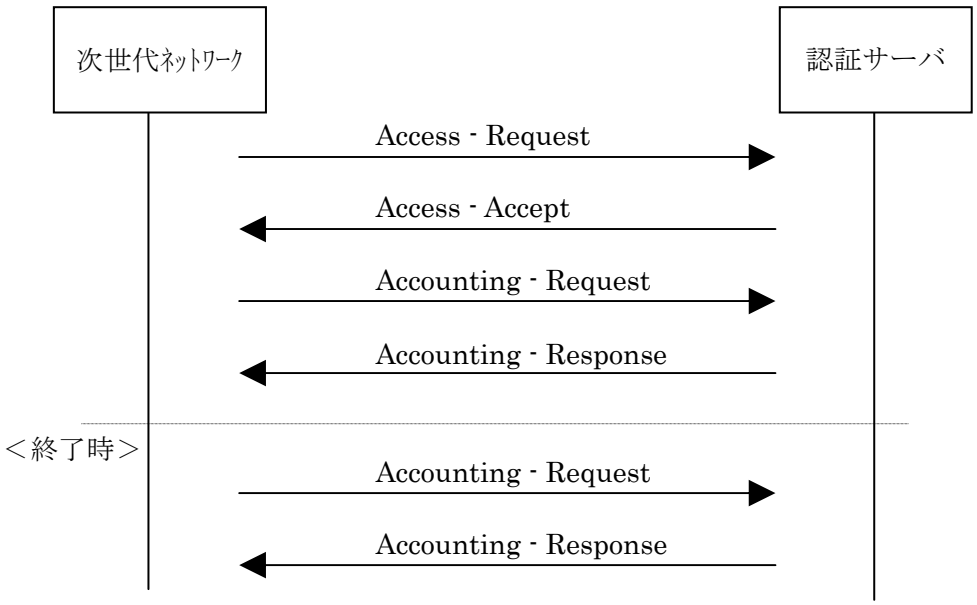
5.1　制御情報交換方式

次世代ネットワークと認証サーバ間の制御情報交換は IETF RFC2865 および IETF RFC2866 に準拠した RADIUS プロトコルにより行う。このとき、IETF RFC2865 および IETF RFC2866 の中で記述されている RADIUS サーバおよび RADIUS 課金サーバは認証サーバを、RADIUS クライアントについては次世代ネットワークを、それぞれ示すものとする。

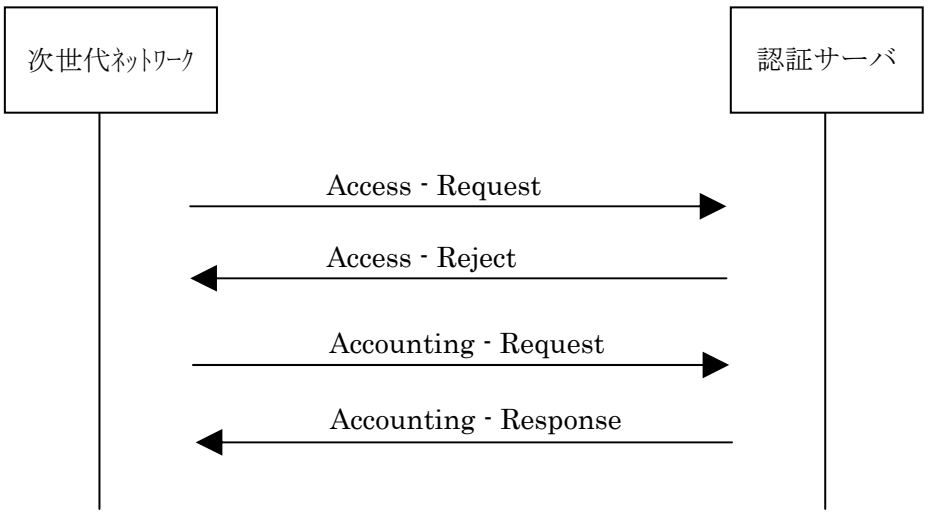
5.1.1　RADIUS シーケンス

次世代ネットワークと認証サーバ間のシーケンスは以下のとおり。

（１）正常時のシーケンス



（２）誤ユーザ名、もしくは、誤パスワード時のシーケンス

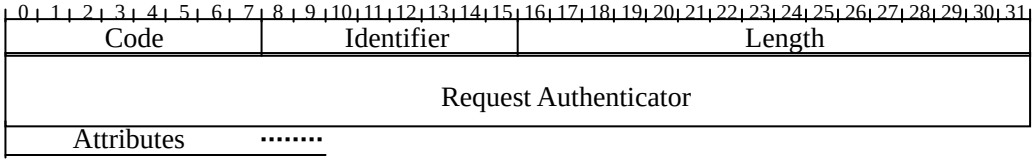


5.1.2　パケットフォーマット

次世代ネットワークと認証サーバ間で用いる制御情報パケットのフォーマットを以下に示す。なお、図中の各フィールドは左から右への順で送られる。

(1) アクセス要求（Access-Request）

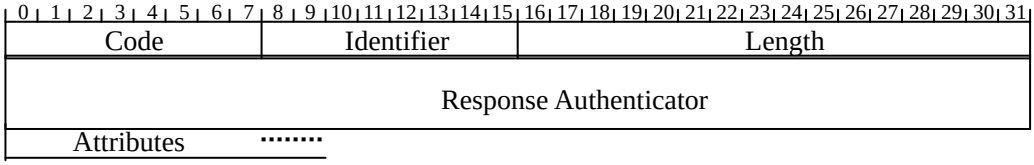
エンド･ユーザの次世代ネットワークへの接続の可否を決定するために使われる情報を、次世代ネットワークから認証サーバへ送出するパケット。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	1
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	(属性情報)

(2) アクセス応答（Access-Accept）

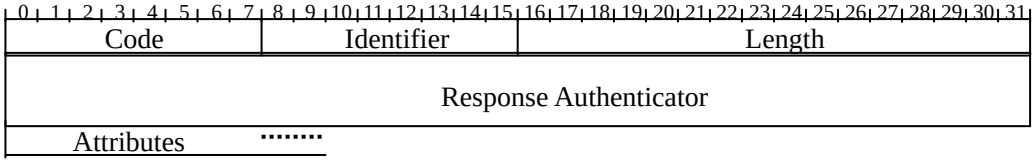
ユーザに対して、サービスを始めるために必要となる情報を提供するパケットで、認証サーバから次世代ネットワークへ送られる。Access-Request の属性が受け入れられた時に、認証サーバはコードフィールドに「２」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	2
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	(属性情報)

(3) アクセス拒否（Access-Reject）

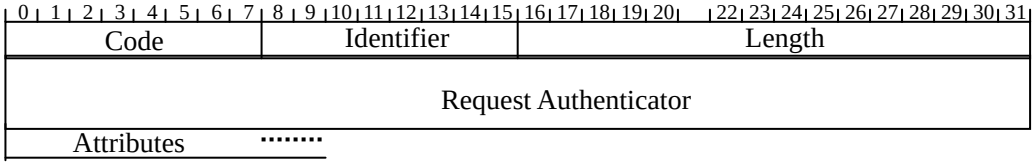
Access-Request の属性が受け入れられない時に、認証サーバはコードフィールドに「３」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	3
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	(属性情報)

(4) アカウント要求（Accounting-Request）

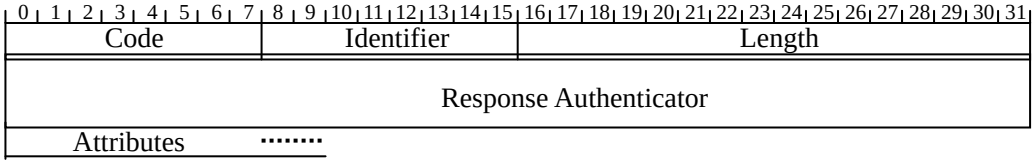
次世代ネットワークから認証サーバに送られるパケットで、ユーザに提供されるサービスに対するアカウンティング情報を含んでいる。次世代ネットワークはコードフィールドに「４」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	4
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	(属性情報)

(5) アカウント応答（Accounting-Response）

認証サーバから次世代ネットワークに送られるパケットで、Accounting-Request が正しく受け取られ、記録されたことを示す。このとき、認証サーバはコードフィールドに「５」を入れて送出する。



フィールド名		ﾌｨｰﾙﾄﾞ長(octet)	値
Code	コード	1	5
Identifier	識別子	1	
Length	パケット長	2	
Authenticator	認証者	１６	
Attributes	属性	可変	（属性情報）