技術参考資料

IP通信網サービスのインタフェース
― フレッツシリーズ -
＜光ネクスト、光ライト、光WiFiアクセス編＞
第19版

2014.9.5

西日本電信電話株式会社

本資料の内容は、機能追加等により追加・変更されることがあります。

なお、内容についての問い合わせは、下記宛にお願い致します。

西日本電信電話株式会社

ビジネスデザイン部

flets-tech@ml.hq.west.ntt.co.jp

目次

まえがき

この技術参考資料は、IP 通信網とこれに接続する端末機器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。西日本電信電話株式会社（以下、NTT 西日本）は、この資料の内容によって通信の品質を保証するものではありません。

なお、IP 通信網に接続される端末設備が必ず適合しなければならない技術的条件は、「端末設備等の接続の技術的条件」または「端末等設備規則」（昭和 60 年郵政省令 31 号）に定められています。

今後、本資料は、インタフェースの追加、変更に合わせて、予告なく変更される場合があります。

改版履歴

版数	変更日付	変更内容
第1.0版	2008/3/31	制定
第 2 版	2008/8/18	フレッツ・ＶＰＮ ゲート 10Mb/s メニューの追加にともない、「フレッツ・ＶＰＮ ゲート」を改定 フレッツ・ＶＰＮ ワイド センタ回線接続サービスの提供にともない、「フレッツ・ＶＰＮ ワイド センタ回線接続サービス」を追加
第3版	2008/10/2	フレッツ 光ネクストビジネスタイプの追加にともない、「フレッツ 光ネクスト」を改定 「フレッツ 光ネクスト」付属資料の記述内容を修正 IPTV フォーラムによる標準運営規定の策定にともない、「フレッツ・キャスト」を改定
第4版	2008/12/18	フレッツ・セッションプラスの提供にともない、「フレッツ 光ネクスト」を改定
第5版	2009/2/4	100Mb/s 品目等の追加にともない、「フレッツ・キャスト」を改定 フレッツ・キャストの MLDv2 の記述内容を修正 フレッツ 光ネクストの DHCPv6 における DUID 生成方式について追記
第6版	2009/4/20	フレッツ・ＶＰＮ ゲート Ethernet/FastEthernet タイプにおける局外接続型の追加、及び 10 GigabitEthernet タイプの追加にともない、「フレッツ・ＶＰＮ　ゲート」を改定
第7版	2009/9/16	フレッツ・キャストにおける回線情報通知機能の追加にともない、「フレッツ・キャスト」等を改定
第8版	2009/12/1	フレッツ・ＶＰＮゲート、フレッツ・ＶＰＮワイドにおける、光ネクスト以外からの接続機能の提供にともない、「フレッツ・ＶＰＮ ゲート」「フレッツ・ＶＰＮワイド センタ回線接続サービス」を改定
第9版	2010/4/26	ファミリー・エクスプレスタイプ、マンション・エ

		クスプレスタイプ、ファミリー・ハイスピードタイプ、マンション・ハイスピードタイプの提供に伴い、「フレッツ 光ネクスト」の改訂 フレッツ 光ネクストの MTU に関する追記 フレッツ 光ネクストの PADO パケットの記述内容の追記 フレッツ 光ネクストの PADS パケットの記述内容の追記 フレッツ・ＶＰＮ ゲートにおける GigabitEthernet タイプのデュアルクラスの追加にともない、「フレッツ・ＶＰＮ ゲート」を改定 フレッツ・キャストにおけるプロトコル構成の更新、MLDv2 の記載内容の改定、ICMPv6 に関する記述を追加
第 10 版	2011/6/1	IPv6 通信 PPPoE 方式の記載追加にともない、「フレッツ 光ネクスト」を改定 IPv6 パケットフォーマットに関する記述の変更にともない「フレッツ・キャスト」を改定
第 11 版	2011/6/27	フレッツ・ＶＰＮ ゲート ユーザ認証代行機能の提供に伴い、「フレッツ・ＶＰＮ ゲート」を改定
第 12 版	2011/7/21	IPv6 通信 IPoE 方式の記載追加に伴い、「フレッツ・光ネクスト」を改定
第 13 版	2012/1/13	フレッツ 光ライトのサービス提供に伴い、「フレッツ 光ライト」を追加。 フレッツ 光ライトのサービス提供に伴い、表題を以下の通り変更 【変更前】IP 通信網サービスのインターフェースーフレッツシリーズー＜光ネクスト編＞ 【変更後】 IP 通信網サービスのインターフェースーフレッツシリーズー＜光ネクスト、光ライト編＞
第 14 版	2012/2/23	IPv6 通信 IPoE 方式の記載追加に伴い、「フレッツ 光ネクスト」を改定
第 15 版	2012/10/1	・スーパーハイスピードタイプ 隼の提供に伴う「フレッツ 光ネクスト」の改訂

第 16 版	2013/1/16	組織名変更に伴う改定 【変更前】サービスクリエーション部 【変更後】ビジネスデザイン部
第 17 版	2013/1/31	フレッツ 光 WiFi アクセスのサービス提供に伴い、「フレッツ 光 WiFi アクセス」を追加。 フレッツ 光 WiFi アクセスのサービス提供に伴い、表題を以下の通り変更 【変更前】IP 通信網サービスのインターフェースーフレッツシリーズー＜光ネクスト、光ライト編＞ 【変更後】IP 通信網サービスのインターフェースーフレッツシリーズー＜光ネクスト、光ライト、光 WiFi アクセス編＞
第 18 版	2013/8/30	IPv6 通信 IPoE 方式・PPPoE 方式の記載追加に伴い、「フレッツ 光ネクスト」および「フレッツ 光ライト」を改定
第 19 版	2014/9/5	フレッツ・スポット自社役務による Web 認証方式提供開始に伴い、「フレッツ・スポット」を追加。 フレッツ・スポット端末認証方式の廃止に伴い、「フレッツ・VPN ゲート」を改定

用語の定義

1.1 用語の定義

(1)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を指します。

(2)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、政府への提言などを行う団体です。

(3)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です。

(4)IEC (International Electrotechnical Commission)

国際電気標準会議。電気、電子、通信などの分野で各国の規格、標準の調整を行う国際的機関です。1947 年以降から ISO の電気・電子部門を担当しています。

(5)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 等の標準化を行っています。

(6)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です。ここで標準化された仕様は RFC として公表されています。

(7)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 パケットのルート決定等を行うものです。IP バージョン 4 と IP バージョン 6 が存在しますが、本書では IP バージョン 4 を指示する場合は「IPv4」、IP バージョン 6 を指示する場合は「IPv6」と表記します。IP と表記する場合は IP バージョン 4・IP バージョン 6 の両方を指示します。

(8)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」と記述します。

(9)IPv4 アドレス

IP 通信のために、通信の送信元と送信先を示すものです。アドレスは 32 ビットで構成され、IP 通信を行う機器に割り当てられている必要があります。

(10)IPv6 アドレス

IP 通信のために、通信の送信元と送信先を示すものです。アドレスは 128 ビットで構成され、IP 通信を行う機器に割り当てられている必要があります。

(11)IP パケット

IP で扱われるメッセージ転送単位です。

(12)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です。

(13)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です。

(14)JPNIC (Japan Network Information Center)

日本ネットワークインフォメーションセンタ。ドメイン名や IP アドレスなどの、日本のインターネットにおける共有資源の管理を行っている組織です。

(15)MRU (Maximum Receive Unit)

最大転送単位。所定のネットワークにて受信することができるパケットの最大量を示します。

(16)MTU (Maximum Transmission Unit)

最大転送単位。所定のネットワークに送信することができるパケットの最大量を示します。

(17)ONU (Optical Network Unit)

ユーザ側に設置される光加入者線終端装置です。

(18)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です。

(19)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などを定めた標準勧告文書です。IETF が管理、発行しています。

(20)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です。

(21)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です。

(22)SIP-UA(Session Initiation Protocol-User Agent)

SIP セッションの作成および管理に使用される論理的なプロセスです。

(23)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です。コネクション型通信に用いられます。

(24)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、電気通信に関する標準規格を制定する団体です。

(25)TTC (Telecommunication Technology Committee)

社団法人電信電話技術委員会。「日本における電気通信網の接続に関する標準」の作成と普及を図ることを目的として設立された民間組織です。

(26)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です。

(27) IPTV フォーラム

オープンな IPTV サービスを実現するために必要な技術仕様の策定・維持等を行っている国内の主要な通信事業者、家電メーカー、放送事業者の団体です。

(28)経路情報

IP 通信網で利用する IPv6 Prefix 等の詳細情報です。

フレッツ 光ネクスト

1　フレッツ 光ネクストの概要

1.1　サービスの概要

フレッツ 光ネクストは、ベストエフォート型の IP 通信サービスに加え、帯域確保型のアプリケーションサービスを利用可能なサービスです。フレッツ 光ネクストを利用する端末機器等（以下、端末機器）は、電気通信事業者等と IP 通信網を介して IP 通信を行います。フレッツ 光ネクストの基本構成を図 1.1 に示します。

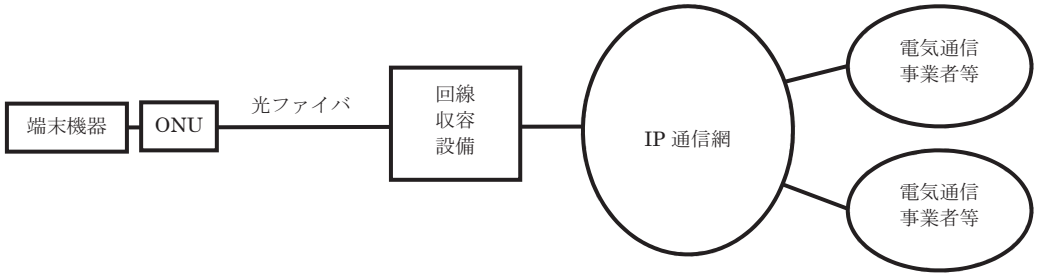


図 1.1 フレッツ 光ネクストの基本構成

なお、フレッツ・v6 オプションを契約することで、フレッツ光 ネクストおよびフレッツ光 ライトを利用する端末機器同士で図 1.2 に示す IP 通信網内で折り返した IPv6(IPoE)通信を行うことができます。

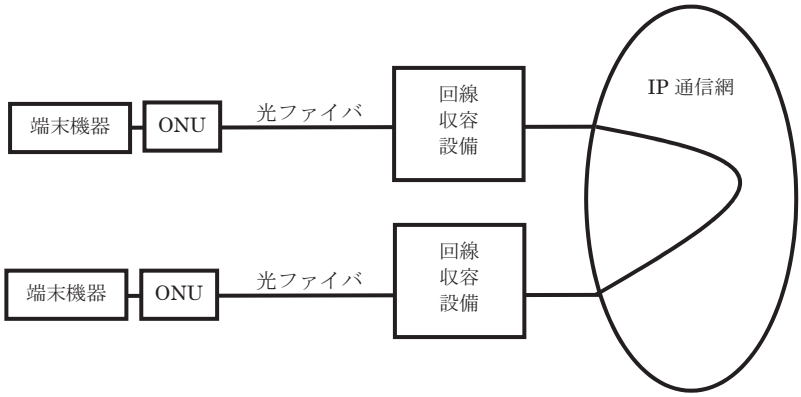


図 1.2 フレッツ・v6 オプションの契約者同士の通信

1.2 インタフェース規定点

フレッツ 光ネクストでは、図 1.3 に示すユーザ・網インタフェース（UNI）を規定します。

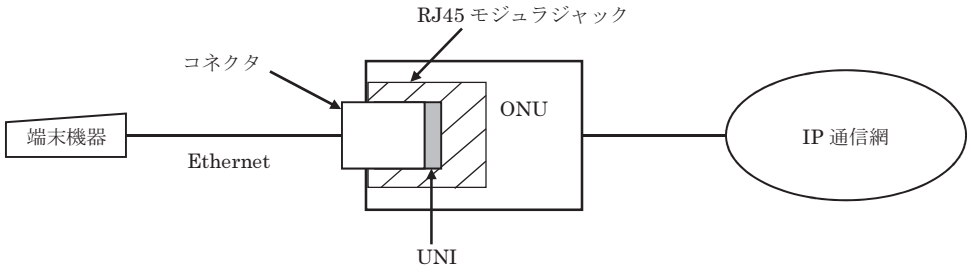


図 1.3 インタフェース規定点

1.3 端末設備と電気通信回線設備の分界点

端末設備と電気通信回線設備との分界点について図 1.4 に示します。また、端末設備が必ず適合しなければならない技術的条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

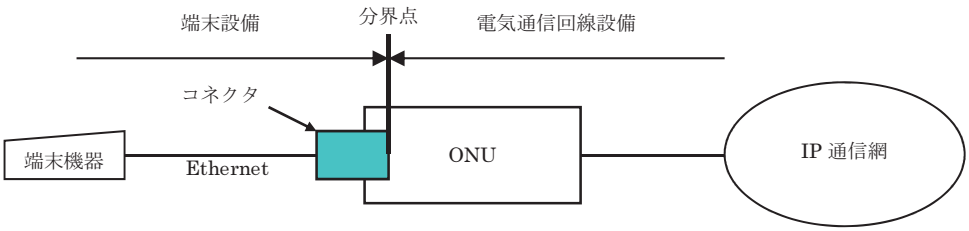


図 1.4 分界点

1.4 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 1.5 に示します。

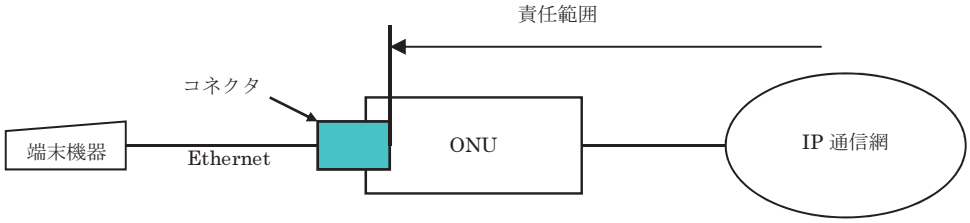


図 1.5 施工・保守上の責任範囲

2 ユーザ・網インタフェース仕様

2.1 プロトコル構成

プロトコル構成は、表 2.1 に示す OSI 参照モデルに則した階層構造となっています。

表 2.1 インタフェース条件

<table>
<tr><th colspan="2" rowspan="3">レイヤ</th><th colspan="3">使用するプロトコル</th></tr>
<tr><th colspan="2">IPv6 通信</th><th>IPv4 通信</th></tr>
<tr><th>IPoE 方式</th><th>PPPoE 方式</th><th>PPPoE 方式</th></tr>
<tr><td>7</td><td>アプリケーション</td><td rowspan="4">DHCPv6:
RFC3315 / RFC3513 /
RFC3646 / RFC4075
DHCPv6-PD:
RFC3633
DNS:
RFC1034 / RFC1035 /
RFC1123 / RFC2181 /
RFC2308 / RFC2671 /
RFC2782 / RFC3596
SNTP:
RFC4330
HTTP:
RFC2616</td><td rowspan="4">DHCPv6:
RFC3315 / RFC3513 /
RFC3646
DHCPv6-PD:
RFC3633</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>4</td><td>トランスポート</td></tr>
<tr><td>3</td><td>ネットワーク</td><td>IPv6:
RFC2460 / RFC2462 /
RFC3513
ICMPv6:
RFC4443
NDP:
RFC2461
MLDv2:
RFC2711 / RFC3810</td><td>IPv6:
RFC2460 /RFC3513
ICMPv6:
RFC2463</td><td>IPv4:
RFC791
ICMPv4:
RFC792</td></tr>
<tr><td>2</td><td>データリンク</td><td>MAC:
IEEE802.3-2005</td><td>PPPoE:
RFC1332 /
RFC2472(IPv6CP) /
RFC1334(PAP) /
RFC1994(CHAP) /
RFC1661(PPP) /
RFC2516(PPPoE)
MAC:
IEEE802.3-2005</td><td>PPPoE:
RFC1332 /
RFC1877(IPCP) /
RFC1334(PAP) /
RFC1994(CHAP) /
RFC1661(PPP) /
RFC2516(PPPoE)
MAC:
IEEE802.3-2005</td></tr>
<tr><td>1</td><td>物理</td><td colspan="3">IEEE 802.3-2005 1000BASE-T 準拠
IEEE 802.3-2005 100BASE-TX 準拠
IEEE 802.3-2005 10BASE-T 準拠</td></tr>
</table>

2.2 物理レイヤ（レイヤ 1）仕様

フレッツ 光ネクストがサポートするレイヤ 1 のインタフェース条件と通信モードを表 2.2 に示します。

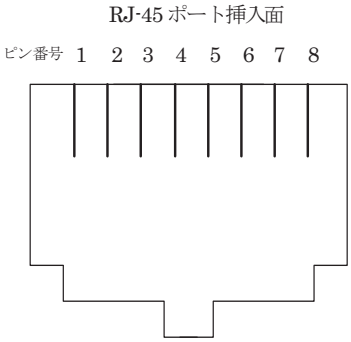
表 2.2 インタフェース条件

タイプ	インタフェース条件	通信モード
ビジネスタイプ	10BASE-T,100BASE-TX または 1000BASE-T（Auto-MDI/MDI-X）（注 1）	自動折衝機能（Auto Negotiation）（注 1）
ファミリー・ハイスピードタイプ 集		
マンション・ハイスピードタイプ 集		
ファミリー・ハイスピードタイプ		
マンション・ハイスピードタイプ		
ファミリータイプ	10BASE-T または 100BASE-TX（Auto-MDI/MDI-X）（注 1）	
マンションタイプ		

（注 1）インタフェースと通信モードは ONU の自動折衝機能（Auto Negotiation）により決定します。

2.2.1　　インタフェース条件

ユーザ・網インタフェースは、IS08877 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 2.1 に示します。



ピン番号	10BASE-T / 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_DB-	⇔	
7					送受信	BI_DD+	⇔	
8					送受信	BI_DD-	⇔	

図 2.1 挿入面から見た RJ-45 ポートのピン配置

2.3 データリンクレイヤ（レイヤ 2）仕様

レイヤ 2 では、IEEE 802.3-2005 に規定されている MAC、PPP、PAP、CHAP の一部、IPCP、IPv6CP、PPPoE を使用します。MAC の詳細については、IEEE 802.3-2005 を、PPP、PAP、CHAP、IPCP、IPv6CP、PPPoE の詳細については[3.1PPP]と[3.2PPPoE]を参照してください。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。

2.4 レイヤ 3 仕様

レイヤ 3 では、RFC791 に規定されている IPv4、RFC2460 に規定されている IPv6 の両方をサポートします。IP 通信網に接続された端末機器は使用用途、実装に応じ IPv4、IPv6 のどちらか一方、もしくは双方同時に使用することが可能です。

また IPv4 のサブセットとして RFC792 に規定されている ICMPv4 の一部についてもサポートします。

IPv6 通信（PPPoE 方式）については RFC3513 に規定されている IPv6 アドレッシング、RFC2463 に規定されている ICMPv6、RFC3315 に規定されている DHCPv6 等の一部、またはすべてをサポートします。

IPv6 通信(IPoE 方式)については RFC3513 に規定されている IPv6 アドレッシング､RFC2461 に規定されている NDP、RFC2462 に規定されている IPv6 アドレスオートコンフィグ、RFC4443 に規定されている ICMPv6、RFC3315 に規定されている DHCPv6、RFC3810 に規定されている MLDv2 等の一部、またはすべてをサポートします。ただし、IP 通信網内に存在しない宛先に送信されるパケットについては、IP 通信網において応答なくパケット破棄される場合や、RFC793 に規定される RST ビットをセットした TCP パケットを返信する場合があります。

それぞれのプロトコル適用範囲については[2.4.1 IPv4 仕様]、[2.4.2 IPv6 仕様]を参照してください。

各仕様に関する詳細は各 RFC を参照してください。

2.4.1 IPv4 仕様

RFC791 に規定されている IPv4 を使用します。また、IPv4 のサブセットとして RFC792 に規定されている ICMPv4 の一部についてもサポートします。

2.4.1.1 IPv4 アドレス

フレッツ 光ネクストでは、RFC1700 で規定されているクラス D、クラス E アドレスをサポートしません。また、端末機器のアドレスとして利用可能なアドレスは IP 通信網に接続する際に、IP 通信網または接続先から割り当てられたアドレスの範囲のみです。その他のアドレスを利用する場合、動作は保証しません。

2.4.1.2 最大転送単位 (MTU)

フレッツ 光ネクストではIP通信網におけるIPv4通信のMTU値は1454byte です。

IP通信網がMTU値を超えるパケットを受信した場合、IP通信網はパケットを分割転送、または破棄する場合があります。

2.4.2 IPv6仕様

IP通信網ではIPv6通信(IPoE方式)とIPv6通信(PPPoE方式)におけるIPv6通信の2つをサポートとしています。IPv6通信(IPoE方式)については[2.4.2.1 IPoE方式におけるIPv6仕様]を、IPv6通信(PPPoE方式)については[2.4.2.2 PPPoE方式におけるIPv6仕様]をご参照下さい。

2.4.2.1 IPoE方式におけるIPv6仕様

RFC2460 に規定されている IPv6 を使用します。また、IPv6 のサブセットとして RFC3513 (IPv6 Addressing Architecture)、RFC2461 (Neighbor Discovery for IPv6)、RFC2462 (IPv6 Stateless Address Autoconfiguration)、RFC4443 (ICMPv6)、 RFC3315 (DHCPv6)、RFC3810 (MLDv2) 等の一部、またはすべてをサポートします。

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 に規定するルータアラートオプション)、フラグメントヘッダ、認証ヘッダ、暗号化ペイロードヘッダを使用します。その他の拡張ヘッダを使用した場合は、IP通信網は転送を保証できない場合があります。

2.4.2.1.1 IPoE方式におけるIPv6アドレス

IPv6 アドレスは、RFC3513 で規定されている IPv6 のグローバル・ユニキャストアドレスを使用します。端末機器ではリンクローカルアドレスを除いて IP 通信網が割り当てる以外のアドレスは使用できません。また、端末機器はPreferred Lifetimeが0でないアドレスを所持している場合は、Preferred Lifetimeが0でないアドレスの利用を推奨します。IPv6アドレス情報の付与方法については[2.4.2.1.2 IPoE方式におけるIPv6アドレス情報付与方法]を参照してください。

2.4.2.1.2 IPoE方式におけるIPv6アドレス情報付与方法

IP 通信網は、RFC2461 に規定されている NDP (Neighbor Discovery Protocol) に基づき、ルータ広告 (Router Advertisement) メッセージを端末機器に送信します。なお、ルータ広告の Other stateful configuration flag 及び Managed address configuration flag が 1 に設定される場合があります。また、ルータ広告の Preferrd Lifetime は 0 に設定される場合があります。端末機器は Other stateful configuration flag が 1 に設定されたルータ広告を受信した際は、DHCPv6 機能を利用し付加情報を取得するため、Information-Request を送信することを推奨します。ル

ータ広告の Managed address configuration flag が 1 に設定されたルータ広告を受信した場合は RFC3315、RFC3633 に規定される DHCPv6-PD（DHCP による IPv6 Prefix Option）を使用し IPv6 Prefix を取得することを推奨します。なお、DHCPv6 を利用した 128bit の IPv6 アドレスの取得はできません。

端末機器のアドレスとして利用可能なアドレスは、このルータ広告メッセージに含まれる 64bit の IPv6 Prefix を利用して生成した IPv6 のグローバル・ユニキャストアドレスのみです。ただし、IP 通信網上で提供する音声利用 IP 通信網サービス等を利用する場合は、RFC3315、RFC3633 に規定される DHCPv6-PD のみを使用し、IP 通信網から 48bit または 56bit の IPv6 Prefix を含むメッセージを当該端末機器に送信します。

また、サービスの利用状況等により IP 通信網から送信される IPv6 Prefix の値は変更される場合があります。なお、IPv6 Prefix のサイズは IP 通信網より指定をして送信します。

2.4.2.1.3　IPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得

端末機器は DHCPv6 を用いて、DHCPv6 のオプションにより RFC3646 に規定される DNS サーバアドレスの情報及びドメインサーチリストの情報、RFC4075 に規定される SNTP サーバアドレスの情報を取得することが可能です。

また、IP 通信網上で提供する音声利用 IP 通信網サービスを利用する場合は、DHCPv6 のオプションにより取得可能な情報が追加される場合があります。詳細は該当するサービスの技術資料等を参照してください。

仕様に関する詳細は各 RFC を参照してください。

2.4.2.1.4　IPoE 方式における DHCPv6 における DUID 生成方式

IP 通信網の DUID 生成方式は RFC3315 に規定される DUID-LL 方式であり、MAC アドレスから DUID を生成します。端末側の DUID 生成方式は RFC3315 に規定される DUID-LL 方式に準拠する必要があります。端末機器も IP 通信網と同様に MAC アドレスから DUID を生成する必要があります。

2.4.2.1.5　IPoE 方式における最大転送単位（MTU）

IP 通信網における IPv6 通信の MTU の値は 1500byte です。

IP 通信網が MTU の値を超えるパケットを受信した場合、IP 通信網は、パケットを破棄します。

2.4.2.1.6　MLDv2

IP 通信網において端末機器とフレッツ・キャスト等側端末機器間でマルチキャストアドレスを利用した通信を行う場合、端末機器は RFC3810 で規定される MLDv2 に対応する必要があります。

Multicast Listener Report メッセージは、Version2 を使用します。この Multicast Listenner Report メッセージを端末機器から IP 通信網に送信する場合の ICMPv6 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、動作を保証しません。

RFC3810（MLDv2）では、マルチキャスト通信の受信要求方法として特定のマルチキャストアドレスを指定して要求する「インクルードモード（Include mode)」と、特定のマルチキャストアドレス以外を指定して要求する「エクスクルードモード（Exclude mode)」が定義されていますが、IP 通信網においてはインクルードモードにのみ対応しています。

表 2.3　設定可能な Multicast Address Record タイプ一覧を示します。なお、この値以外を設定した場合、動作を保証しません。

予め通信条件が設定されたマルチキャスト通信においては、設定された条件を満たさない受信要求（Multicast Address Record（RecordType=5）を含む Multicast Listener Report（以降 ALLOW））を破棄します。そのため IP 通信網に接続する端末が視聴チャネルを切り替える際にはマルチキャスト通信の受信要求を送信する前に、受信停止要求（Multicast Address Record（RecordType=6）を含む Multicast Listener Report（以降 BLOCK））を送信することが推奨されます。

図 2.2～図 2.5 に、それぞれマルチキャスト受信開始シーケンス例、マルチキャスト受信継続確認シーケンス例、チャネル切り替えシーケンス例及びマルチキャスト視聴停止シーケンス例を示します。

表 2.3　設定可能な Multicast Address Record タイプ一覧

種別	Record タイプ	値	用途
Current State Record	MODE_IS_ INCLUDE	1	クエリー応答において、インクルードモードを使用することを明示する。
Source List Change Record	ALLOW_NEW_ SOURCES	5	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に送信する。
	BLOCK_OLD_ SOURCES	6	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から離脱する場合に送信する。

2.4.2.1.7　マルチキャスト受信開始シーケンス例

図 2.2 マルチキャスト受信開始シーケンス例

2.4.2.1.8　マルチキャスト受信継続確認シーケンス例

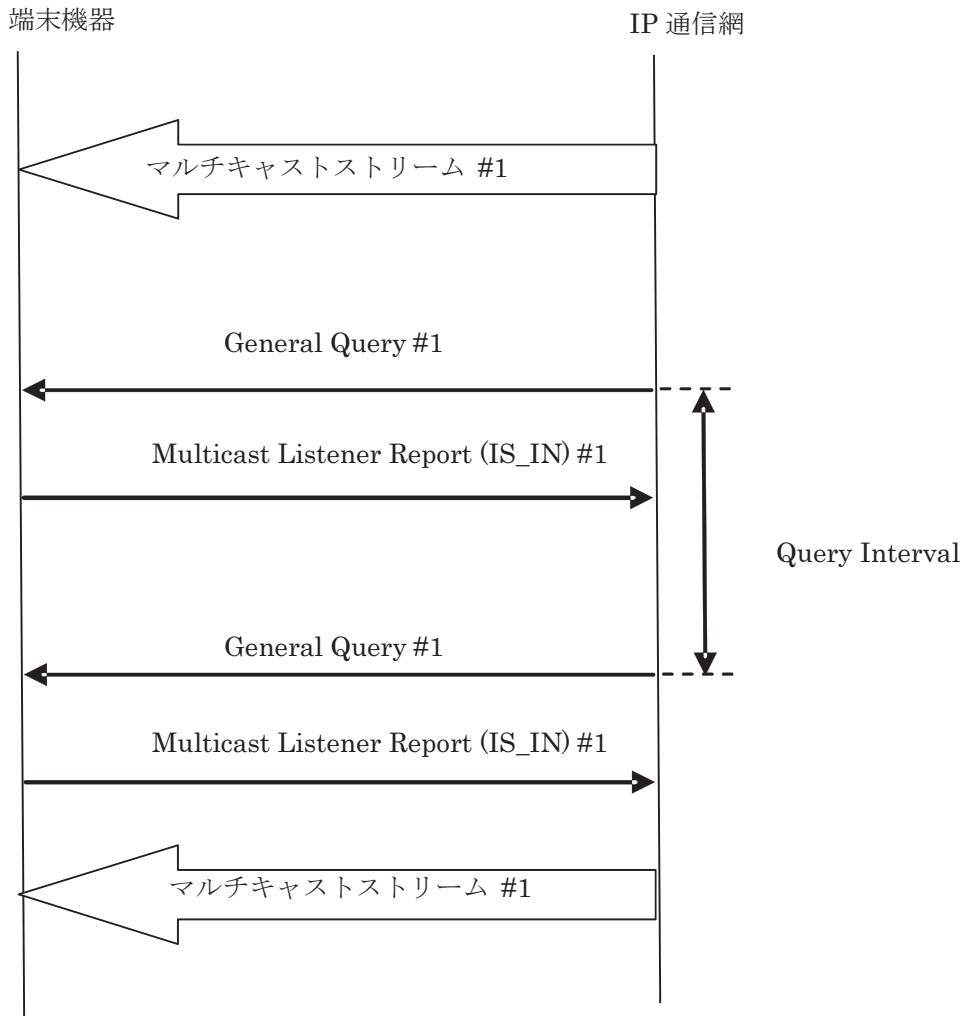


図 2.3 マルチキャスト受信継続確認シーケンス例

2.4.2.1.9　チャネル切り替えシーケンス例

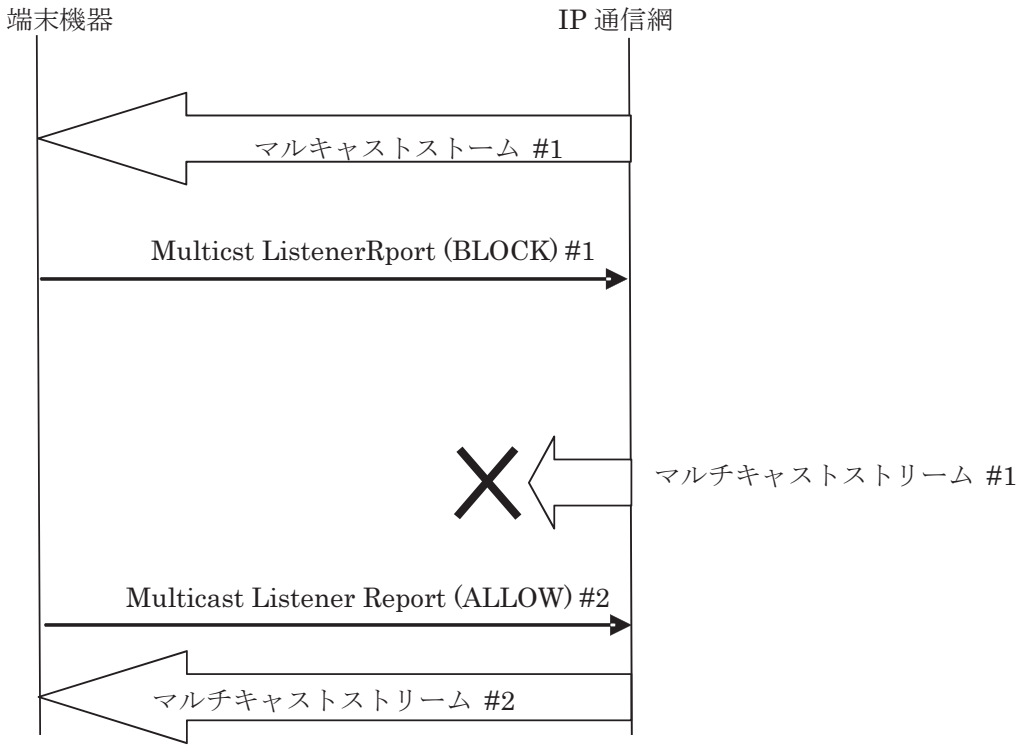


図 2.4 チャネル切り替えシーケンス例

2.4.2.1.10 マルチキャスト受信停止シーケンス例

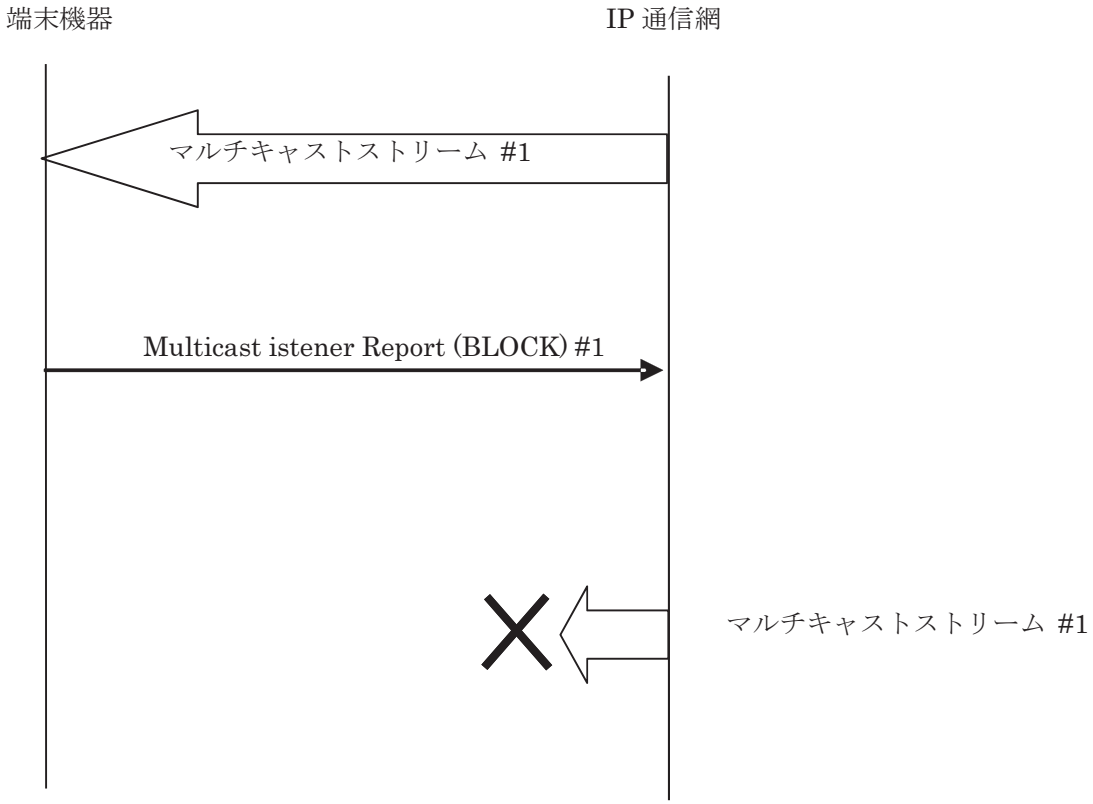


図 2.5 マルチキャスト受信停止シーケンス例

2.4.2.2 PPPoE 方式における IPv6 仕様

RFC2460 に規定されている IPv6 を使用します。また、IPv6 のサブセットとして RFC3513 （IPv6 Addressing Architecture)、RFC2463（ICMPv6)、 RFC3315（DHCPv6）等の一部、またはすべてをサポートします。

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、フラグメントヘッダ、認証ヘッダ、暗号化ペイロードヘッダを使用します。その他の拡張ヘッダを使用した場合は、IP 通信網は転送を保証できない場合があります。

2.4.2.2.1 PPPoE 方式における IPv6 アドレス

IPv6 アドレスは、RFC3513 で規定されている IPv6 のグローバル・ユニキャストアドレスを使用します。端末機器ではリンクローカルアドレスを除いて IP 通信網が割り当てる以外のアドレスは使用できません。IPv6 アドレス情報の付与方法については[2.4.2.2.2 PPPoE 方式における IPv6 アドレス情報付与方法]を参照してください。

2.4.2.2.2 PPPoE 方式における IPv6 アドレス情報付与方法

IP 通信網は、RFC3315、RFC3633 に規定される DHCPv6-PD（DHCP による IPv6 Prefix Option）のみを使用し、PPPoE によって確立したトンネルから通知される IPv6Prefix を含むメッセージを当該端末機器に送信します。端末機器のアドレスとして利用可能なアドレスは、このルータ広告メッセージに含まれる IPv6 Prefix を利用して生成した IPv6 のグローバル・ユニキャストアドレスのみです。

2.4.2.2.3 PPPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得

端末機器は DHCPv6 を用いて、DHCPv6 のオプションにより RFC3646 に規定される DNS サーバアドレスの情報を取得することが可能です。

仕様に関する詳細は RFC を参照してください。

2.4.2.2.4 PPPoE 方式における DHCPv6 における DUID 生成方式

IP 通信網の DUID 生成方式は RFC3315 に規定される DUID-LL 方式であり、MAC アドレスから DUID を生成します。端末側の DUID 生成方式は RFC3315 に規定される DUID-LL 方式に準拠する必要があります。端末機器も IP 通信網と同様に MAC アドレスから DUID を生成する必要があります。

2.4.2.2.5 PPPoE 方式における最大転送単位（MTU）

IP 通信網における IPv6 通信の MTU の値は 1454byte です。

IP 通信網が MTU の値を超えるパケットを受信した場合、IP 通信網は、パケットを破棄します。

2.4.3 転送優先度に関する仕様

端末機器等は、利用するサービスに応じて、パケットに転送優先度を指定することが可能です。転送優先度識別子として DSCP(Differentiated Services Code Point)値を使用します。DSCP の仕様については RFC2474 を、各サービスで利用可能な転送優先度に関する仕様については、各サービスの技術規定等を参照してください。

尚、各サービスにおいて許容されたプロトコルと転送優先度の組み合わせ以外のパケットに転送優先度を指定することは許容しません。

2.5 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、DHCPv6、DHCPv6-PD のみ規定します。IPv6 通信 IPoE 方式においては、前述に加え DNS、SNTP および HTTP を規定します。その他の通信においては、特に規定はありません。

DHCPv6 については[2.4.2.1.3 IPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得]および[2.4.2.1.4 IPoE 方式における DHCPv6 における DUID 生成方式]、または［2.4.2.2.3 PPPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得］および[2.4.2.2.4 PPPoE 方式における DHCPv6 における DUID 生成方式]を、DHCPv6-PD については[2.4.2.1.2 IPoE 方式における IPv6 アドレス情報付与方法]および［2.4.2.2.2 PPPoE 方式における IPv6 アドレス情報付与方法］を参照してください。

2.5.1 DNS

IPv6 に対応した端末機器は、IP 通信網経由でアクセス可能な DNS サーバ間で、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 2.4 に示します。各仕様に関する詳細は各 RFC を参照してください。

表 2.4 DNS 規定

参照文献	タイトル	備考
RFC1034	Domain names – concepts and facilities	DNS について規定
RFC1035	Domain names – implementation and specification	DNS について規定
RFC1123	Requirements for Internet Hosts – Application and Support	DNS の実装について規定
RFC2181	Clarifications to the DNS Specification	DNS について規定
RFC2308	Negative Caching of DNS Queries (DNS NCACHE)	ネガティブキャッシュについて規定
RFC2671	Extension Mechanisms	DNS において、ロング DNS ネーム

	for DNS (EDNS0)	問い合わせ・回答対応方法を規定
RFC2782	A DNS RR for specifying the location of services	SRV レコードを規定
RFC3596	DNS Extensions to Support IP Version 6	IPv6 対応を規定

2.5.2 SNTP

IPv6 に対応した端末は、利用するサービスに応じて、時刻取得のためのプロトコルとして SNTP を使用することが可能です。

SNTP を利用する場合に準拠する規定は RFC4330 となります。仕様に関する詳細は RFC4330 を参照してください。

2.5.3 HTTP

IPv6 に対応した端末は、通信するプロトコルとして HTTP を使用することが可能です。

HTTP を利用する場合に準拠する規程は RFC2616 となります。仕様に関する詳細は RFC2616 を参照してください。

IP 通信網内で利用できる HTTP サーバには、経路情報提供サーバがあり、経路情報提供サーバの利用条件については[2.5.3.1 経路情報提供サーバについて]、[2.5.3.2 経路情報提供サーバで利用するメッセージ]、[2.5.3.3 経路情報提供サーバとの通信シーケンス]を参照してください。

2.5.3.1 経路情報提供サーバについて

経路情報提供サーバは、端末機器に対して IP 通信網の IPv6 prefix 等の情報を提供します。経路情報提供サーバへの接続へは表 2.5 に示す条件でアクセスする事とします。

表 2.5 経路情報提供サーバへの接続条件

項番	項目名	内容
1	レイヤ 3	IPv6
2	上位レイヤ	HTTP
3	FQDN	route-info.flets-west.jp
4	ポート番号	49881

2.5.3.2 経路情報提供サーバで利用するメッセージ

2.5.3.2.1 リクエストメッセージ

経路情報提供サーバへリクエストメッセージを送信する際のフォーマットを図 2.6、リクエストライン、およびリクエストヘッダの構成要素を表 2.6 と表 2.7 に示します。表 2.7 で規定していないメッセージは動作保障対象外とします。

GET[SP]リクエスト URI[SP]HTTP プロトコル[CR][LF]
Host:[SP]ホスト名：ポート番号[CR][LF]
Accept:[SP]サポートコンテンツタイプ[CR][LF]
Accept-Charset:[SP]サポートエンコード種別[CR][LF]
Connection:[SP]コネクショントークン[CR][LF]
[CR][LF]

図 2.6 リクエストメッセージのフォーマット

表 2.6 リクエストライン

項番	項目名	必須／省略可能	内容
1	HTTP メゾット	必須	「GET」固定
2	リクエスト URI	必須	「/v6/route-info」固定
3	HTTP プロトコル	必須	「HTTP/1.1」固定

表 2.7 リクエストヘッダ

項番	ヘッダ名	項目名	必須／省略可能	内容
1	Host	ホスト名:ポート番号	必須	ホスト名に、経路情報提供サーバの URL を入力 ポート番号は「49881」固定
2	Accept	サポートコンテンツタイプ	必須	「*/*」固定
3	Accept-Charset	サポートエンコード種別	省略可能	指定可能な文字コードは「EUC-JP」、「Shift_JIS」、「UTF-8」とする 文字コードの指定が無い場合は「EUC-JP」として処理する
4	Connection	コネクショントークン	必須	「close」固定

2.5.3.2.2　レスポンスメッセージ

経路情報提供サーバからレスポンスメッセージを受信する際のフォーマットを図 2.7 に、ステータスラインおよびレスポンスヘッダの構成要素を表 2.8 と表 2.9 に示します。

レスポンスメッセージのステータスコードに 200 以外が指定される場合のレスポンスヘッダは定義しません。したがって、ステータスコード 408 または 503 が返却された場合、あるいはリクエストメッセージを送信後 10 秒以上無応答状態が発生した場合は再取得を行う必要があります。

なお、再取得はリクエストメッセージの送信契機につき 2 回までとします。

HTTP バージョン[SP]ステータスコード[SP]テキストフレーズ[CR][LF]
Date:日付/時刻スタンプ[CR][LF]
Content-Type:[SP]メッセージボディ部コンテンツタイプ[CR][LF]
Content-Length:[SP]メッセージボディ部バイト長[CR][LF]
Connection:[SP]コネクショントークン[CR][LF]
[CR][LF]
メッセージボディ部

図 2.7 レスポンスメッセージのフォーマット

表 2.8 ステータスライン

項番	項目名	必須／省略可能	内容
1	HTTP バージョン	必須	「HTTP/1.1」固定
2	ステータスコード	必須	経路情報提供サーバが正常に処理結果を送信できる場合、「200」を設定 リクエストメッセージのフォーマットエラー時は、「400」を設定 リクエストタイムアウトが発生した場合は「408」を設定 経路情報提供サーバが一時的にサービス停止状態である場合には「503」を設定
3	テキストフレーズ	必須	ステータスコードに応じたテキストフレーズを設定

表 2.9 レスポンスヘッダ

項番	ヘッダ名	項目名	必須／省略可能	内容
1	Date	日付/時刻スタンプ	必須	メッセージ生成の日付/日時
2	Content-Type	メッセージボディ部のコンテンツタイプとコンテンツタイプ	必須	「text/plain」固定
		メッセージボディ部の文字コード	必須	Accept-Charset で指定された文字コードを受信 未指定時は「EUC-JP」を設定
3	Content-Length	メッセージボディ部のバイト長	必須	HTTP メッセージボディ部バイト長の整数値
4	Connection	コネクショントークン	必須	「close」固定

2.5.3.2.3 メッセージボディ部

メッセージボディのフォーマットの構成要素を図 2.8 に、構成要素を表 2.10 に示します。

レスポンスメッセージのステータスコードに 200 以外が指定される場合のメッセージボディは定義しません。したがって、端末ではステータスコードが 200 以外の場合には、メッセージボディ部に指定された任意のパラメータを無視する必要があります。

タイプナンバー[1],経路情報の更新年月日[CR][LF]
タイプナンバー[2],IPv6 prefix/prefix 長[CR][LF]
・
・
・
タイプナンバー[n],IPv6 prefix/prefix 長[CR][LF]

図 2.8 メッセージボディのフォーマット

表 2.10 メッセージボディ

項番	パラメータ	必須/省略可	繰り返し可否 （最大数）	内容	許容文字種別	文字長 (byte)
1	タイプナンバー[n] n の最大数 :101	必須	可（101 回）	アドレス帯の識別情報 0000 は情報更新年月日時	0-9	4
2	経路情報の更新年月日	必須	否	経路情報提供サーバで保持する経路情報の更新年月日 YYYY/MM/DD[SP]hh:mm:ss の形式で表記	0-9 [/] [.] [:] [SP]	19
3	IPv6 prefix	必須	可（100 回）	経路情報を示すIPv6 prefix（完全表記）	0-9 a-f [:]	39
4	IPv6 prefix 長	必須	可（100 回）	IPv6 prefix 長	0-9	1 以上 3 以下の可変長

2.5.3.2.4 タイプナンバー

4 桁の数字で構成されるタイプナンバーにより、経路情報提供サーバから受信する経路情報の内容を把握することができます。1 桁目、2 桁目、3 桁目の数値は表 2.11 に示す内容を表し、4 桁目の数値は通番として利用しています。なお、タイプナンバー「0000」は情報更新年月日を意味します。

表 2.11 タイプナンバーの構成要素

1 桁		2 桁		3 桁		4 桁	
地域情報		アドレス帯の情報		利用用途		通番	
0	情報更新年月日時	0	情報更新年月日時	0	情報更新年月日時	0	情報更新年月日時
1	NTT 東日本エリア						
2	NTT 西日本エリア	1	IP 通信網	1	PPPoE 接続基盤		
		2	IP 通信網	1	IPoE 基盤		
		3	IP 通信網	1	網内折り返し基盤		
		4	接続事業者	1	IPv6 インターネット接続（IPoE）		

2.5.3.3 経路情報提供サーバとの通信シーケンス

経路情報提供サーバとの通信シーケンスは図 2.9 に示す通りです。なお、経路情報提供サーバは IP 通信網の状況により端末機器に対してレスポンスメッセージを返信しない場合がございます。端末機器からリクエストメッセージを送信する契機は表 2.12 を参照してください。

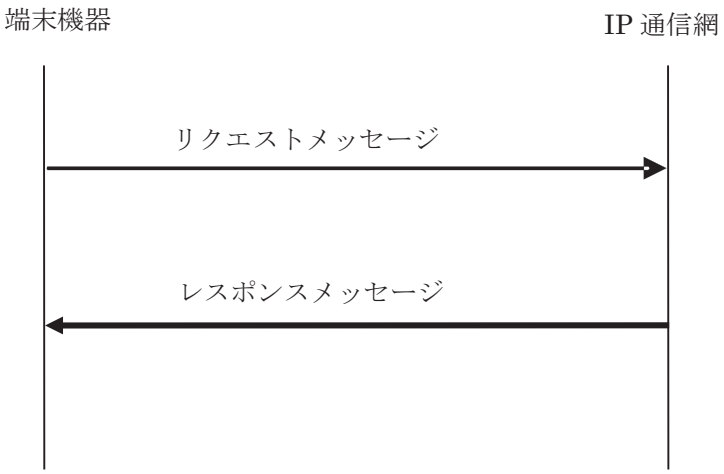


図 2.9 経路情報提供サーバとの通信シーケンス

表 2.12 リクエストメッセージの送信契機

送信契機	内容
初回送信	端末機器起動時から 0 秒～60 秒の間のランダムに設定した時間後に送信
定期送信(初回)	初回送信時から 86,400 秒～691,200 秒の間のランダムに設定した時間後に送信
定期送信	定期送信(初回)から 604,800 秒に 1 回の間隔で送信

3 PPPoE / PPP プロトコル

3.1 PPP

3.1.1 PPP の概要

PPP（Point-to-Point Protocol）は、非同期型（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ける複数のプロトコルのカプセル化と、LCP（Link Control Protocol）によるデータリンク回線の確立・設定・試験・開放、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・設定を行います。

使用する PPP の仕様の詳細は、以下に示す仕様を除き、RFC1661 を参照してください。

3.1.2 PPP パケット

PPP パケットのプロトコルフィールド（Protocol Field）に格納される値を表 3.1 プロトコル識別子に示します。表 3.1 で示す値以外のプロトコルについては動作を保証しません。

表 3.1 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
0x8057	IPv6 Control Protocol（IPv6CP）	
0x0021	Internet Protocol（IP）	ネットワーク レイヤプロトコル
0x0057	Internet Protocol Version 6（IPv6）	

3.1.3 LCP

LCP 通信設定オプション（LCP Configuration Option）のタイプ値を表 3.2 に示します。表 3.2 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。IP 通信網は Maximum-Receive-Unit（MRU）オプションの値を 1454 オクテットでネゴシエーションを要求します。MRU の詳細については RFC1661 を参照してください。

また、IP 通信網の要求する MRU 値より、小さな値で端末機器がネゴシエーションを要求した場合、接続や正常な通信ができない場合があります。 IP 通信網が MRU 値を超えるパケットを受信した場合、IP 通信網はパケットを分割転送、または破棄する場合があります。

表 3.2 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

3.1.4 PAP

PAP Authenticate-Request パケットの Peer-ID-Length フィールドに入る最大値は 0x3f です。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。

3.1.5 CHAP

CHAP Response パケットの Name フィールド長の最大長は 63 オクテットです。Name フィールド長がこの最大長を超えた場合は、動作は保証しません。

3.1.6 IPCP

IPCP 通信設定オプション（IPCP Configuration Option）のタイプ値を表 3.3 に示します。表 3.3 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 3.3 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

3.1.7 IPv6CP

IPv6CP 通信設定オプション（IPv6CP Configuration Option）のタイプ値を表 3.4 に示します。表 3.4 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 3.4 IPv6CP 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	Interface-ID	使用
2	IPv6-Compression-Protocol	使用不可

3.2 PPPoE

3.2.1 PPPoE の概要

PPPoE は、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 上の端末機器（以下、ホスト）と、IP 通信網の機能である Access Concentrator（以下、AC）間の PPP セッションの確立・設定・開放を行います。

PPPoE により PPP セッションを確立・設定・開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。

使用する PPPoE の仕様の詳細は、以下に示す仕様を除き、RFC2516 を参照してください。

3.2.2 ディスカバリステージ

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、開放を通知する動作が含まれます。

3.2.2.1 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 3.1 に示します。

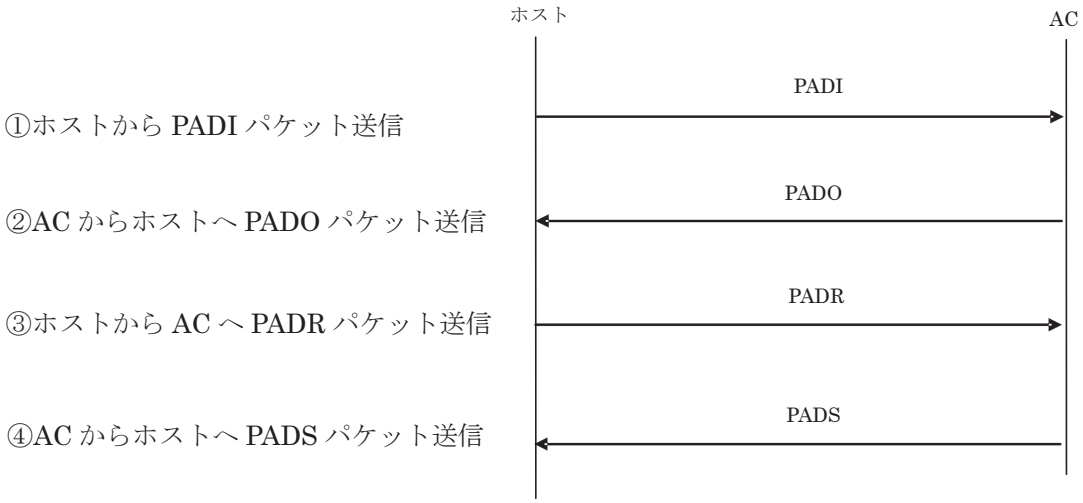


図 3.1 PPPoE セッション確立手順

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、ホストと AC 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。

3.2.2.2 PPPoE セッションの開放を通知する動作

PPPoE セッションの開放を通知する動作では、ホストまたは AC から PPPoE セッションが開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。

3.2.2.3 PADI パケット

ホストは要求するサービス名を含む PADI パケットを送信し、AC 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。ホスト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。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 オクテットを超えてはなりません。表 3.5 に PADI パケットのタグ設定値を示します。

表 3.5 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	-	-	使用不可
Service-Name	0x0101	0	-	使用
AC-Name	0x0102	-	-	使用不可
Host-Uniq	0x0103	可変長	-	使用可
AC-Cookie	0x0104	-	-	使用不可
Vendor-Specific	0x0105	-	-	使用不可
Relay-Session-Id	0x0110	-	-	使用不可
Service-Name-Error	0x0201	-	-	使用不可
AC-System-Error	0x0202	-	-	使用不可
Generic-Error	0x0203	-	-	使用不可

3.2.2.4 PADO パケット

PADI パケットを受信した AC は、送信元のホストに PADO パケットを送信し、AC がサポートするサービス名、AC 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 タグを含みます。AC 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 3.6 に PADO パケットのタグ設定値を示します。

なお、1 つの回線から 5 分間に 20 回を超える PADI パケットを受信した場合、一定期間、PADO パケットを送信しない場合があります。

表 3.6 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	-	-	未使用
Service-Name	0x0101	0	PADI 送信値	使用
AC-Name	0x0102	可変長	-	使用
Host-Uniq	0x0103	可変長	PADI 送信値	使用可
AC-Cookie	0x0104	可変長	-	使用可
Vendor-Specific	0x0105	-	-	未使用
Relay-Session-Id	0x0110	-	-	未使用
Service-Name-Error	0x0201	-	-	未使用
AC-System-Error	0x0202	-	-	未使用
Generic-Error	0x0203	可変長	-	使用可

3.2.2.5 PADR パケット

ホストは受信した 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 AC 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。ホスト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 3.7 に PADR パケットのタグ設定値を示します。

表 3.7 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	-	-	使用不可
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（注）
Vendor-Specific	0x0105	-	-	使用不可
Relay-Session-Id	0x0110	-	-	使用不可
Service-Name-Error	0x0201	-	-	使用不可
AC-System-Error	0x0202	-	-	使用不可
Generic-Error	0x0203	可変長	-	使用可

（注）PADO に AC-Cookie タグが含まれている場合は使用します。

3.2.2.6 PADS パケット

PADR パケットを受信した AC 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 パケットをホストへ送信します。

ホストが PADS パケットを受信すると、ホストと AC は固有の PPPoE セッション ID と相互の MAC アドレスを認識し、PPPoE セッションの確立が完了します。

AC 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 を設定します。表 3.8 に PADS パケットのタグ設定値を示します。

表 3.8 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（注 1）
AC-Name	0x0102	可変長	PADR 送信値	使用可（注 2）
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（注 2）
Vendor-Specific	0x0105	-	-	未使用
Relay-Session-Id	0x0110	-	-	未使用
Service-Name-Error	0x0201	可変長	-	使用（注 3）
AC-System-Error	0x0202	-	-	使用可
Generic-Error	0x0203	可変長	-	使用可

要求されたサービス名を受け入れる場合は使用します。

（注 2）PADR 送信値を送信しない場合があります。

（注 3）要求されたサービス名を拒否する場合は使用します。

3.2.2.7 PADT パケット

PPPoE セッション確立後、ホストまたは AC は PPPoE セッションが開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 フィールドには開放された PPPoE セッションのセッション ID を設定します。タグは使用しません。

3.2.3 PPP セッションステージ

PPPoE セッションが確立されると、PPP セッションステージへと進みます。PPP セッションステージでは、PPP セッションが確立され、IP 通信が開始します。PPP セッションの開放によって PPP セッションステージは終了します。

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ホストまたは 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。使用する PPP プロトコル識別子については 3.1 PPP を参照してください。

3.2.4 自動再接続間隔

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

3.2.5 PPPoE セッション数

同時に使用することが可能な PPPoE セッション数は制限されています。各品目において同時利用可能な最大 PPPoE セッション数について表 3.9 に示します。（基本セッション数を超える同時利用可能 PPPoE セッション数の設定は別途サービスの契約により変更可能です。）

表 3.9 同時利用可能 PPPoE セッション数

品目	同時利用可能 PPPoE セッション数 （基本セッション数／最大セッション数）
ビジネスタイプ	2 ／ 20
ファミリー・ハイスピードタイプ 隼	2 ／ 5
マンション・ハイスピードタイプ 隼	2 ／ 5
ファミリー・ハイスピードタイプ	2 ／ 5
マンション・ハイスピードタイプ	2 ／ 5
ファミリータイプ	2 ／ 5
マンションタイプ	2 ／ 5

3.2.6 通信シーケンス

端末機器と IP 通信網の間の通信シーケンスを図 3.2～図 3.6 に示します。

3.2.6.1　　接続シーケンス（IPv4 通信 PPPoE 方式）

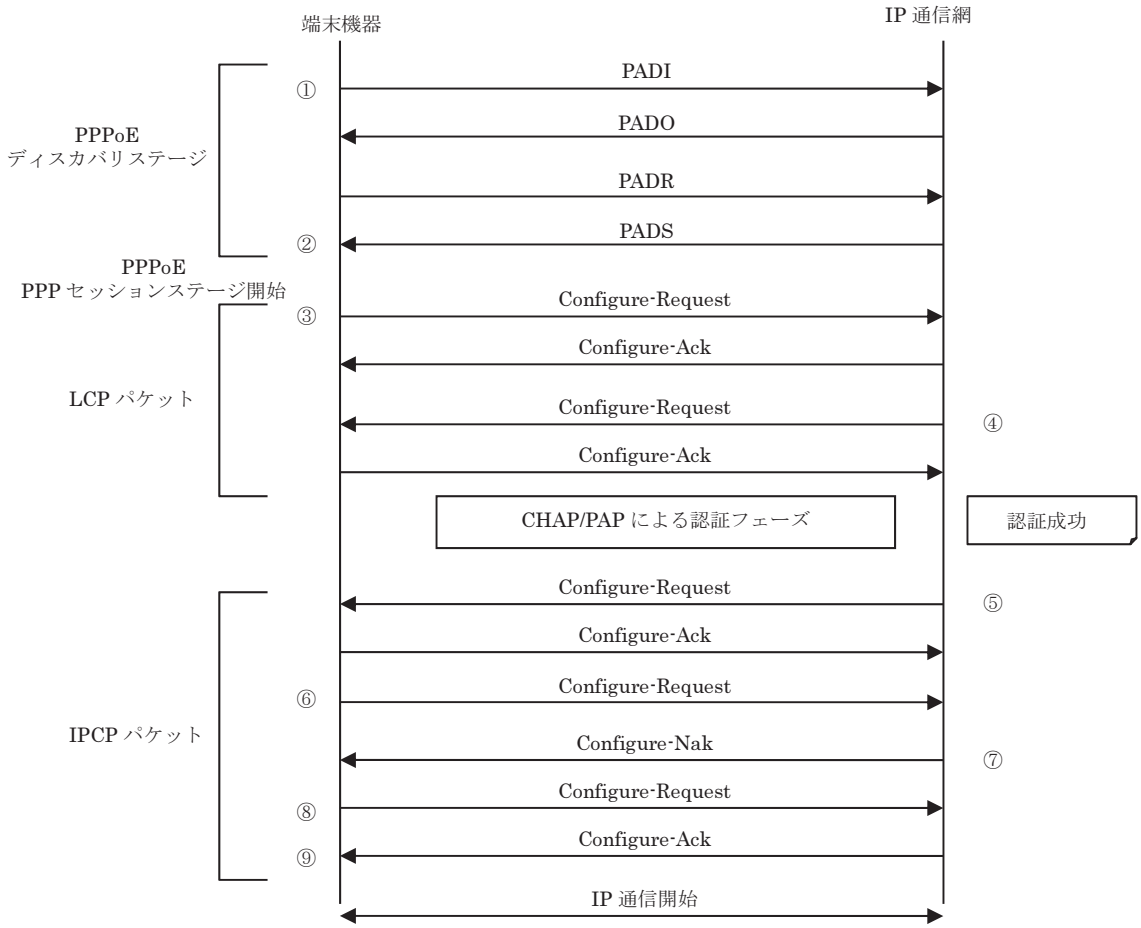


図 3.2　接続シーケンス（例）

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

3.2.6.2　　接続シーケンス（IPv6 通信 PPPoE 方式）

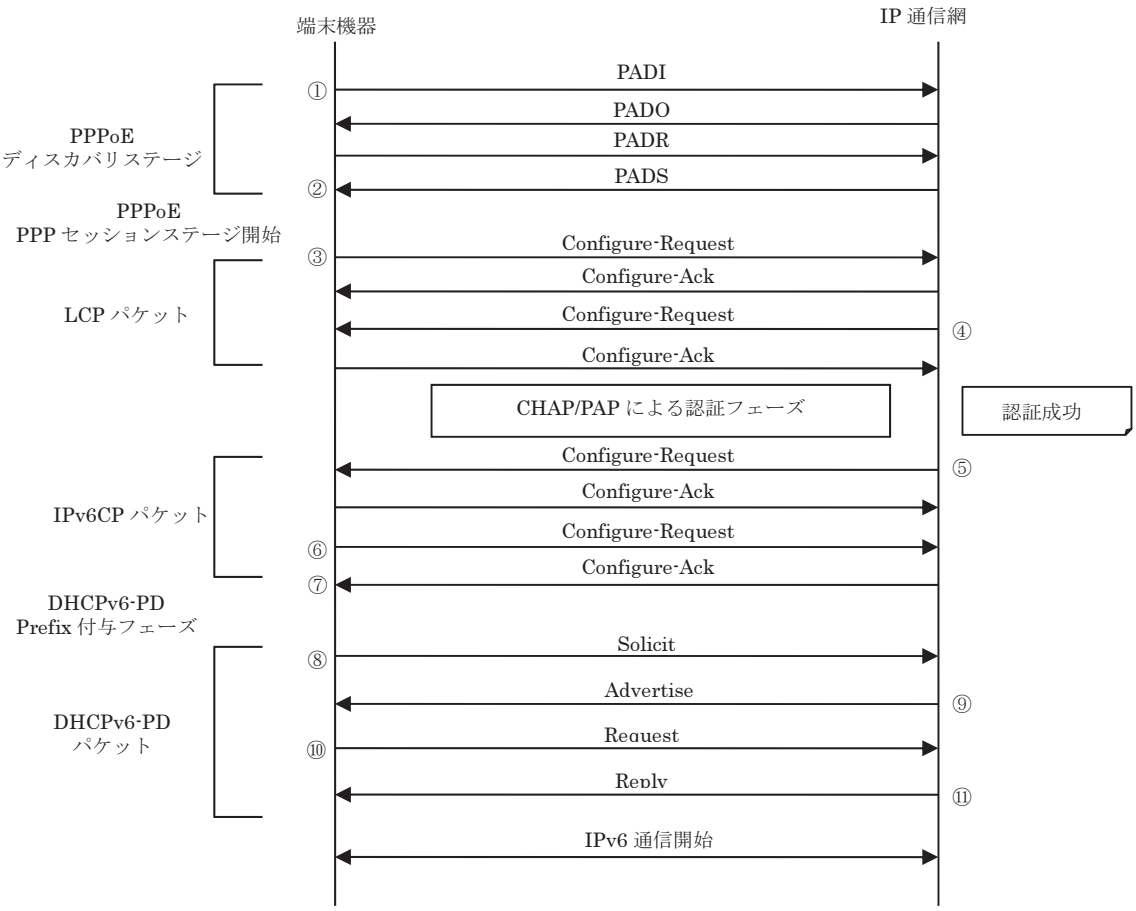


図 3.3　接続シーケンス（例）

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 網側が使用する Interface-ID を通知
⑥ 端末機器が使用する Interface-ID を通知
⑦ PPP セッションが確立
⑧ 端末機器が IP アドレス払出を要請
⑨ 網側が IP アドレスを広告
⑩ 端末機器が使用する IP アドレス払出を要求
⑪ 端末機器に割り当てる IP アドレスを返送

3.2.6.3 切断シーケンス

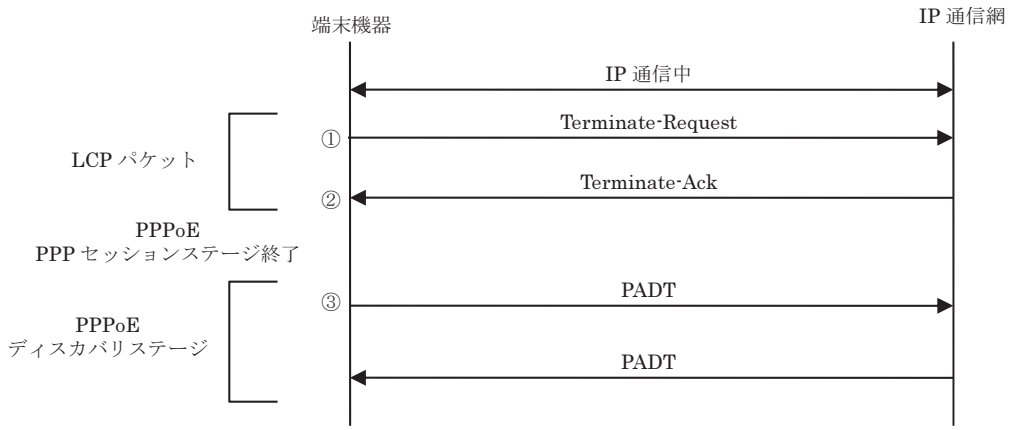


図 3.4 切断シーケンス（例）

① PPP セッションの開放を開始

② PPP セッションを開放

③ PPPoE セッションの開放を通知

3.2.6.4　　認証失敗シーケンス

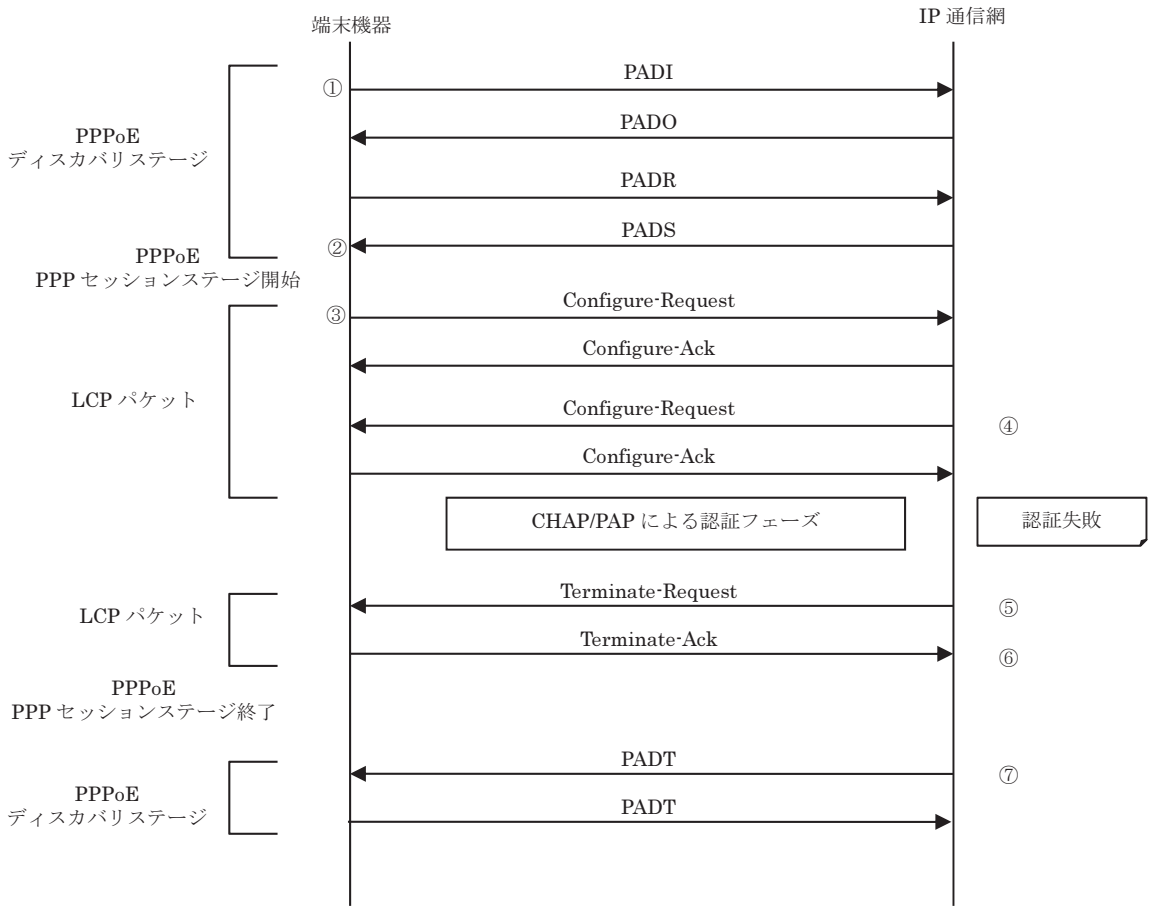


図 3.5　認証失敗シーケンス（例）

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 セッションの開放を開始

⑥ PPP セッションの開放

⑦ PPPoE セッションの開放を通知

3.2.6.5　　強制切断シーケンス

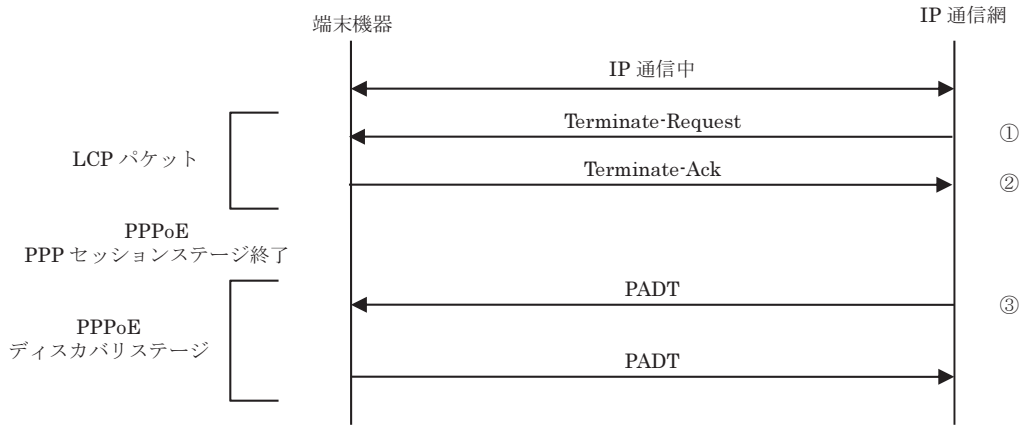


図 3.6　強制切断シーケンス（例）

① PPP セッションの開放を開始

② PPP セッションを開放

③ PPPoE セッションの開放を通知

4　付属資料

4.1　ONU（スロット式）の概要

本装置は、装置内部に端末機器を搭載することが可能なスロットを持った ONU です。装置内部の ONU 機能部と装置に搭載された端末機器は Ethernet により接続することが可能であり、装置に搭載された端末機器を動作させるための電源は本装置から供給することが可能です。以下に ONU(スロット式)の仕様および、端末機器に対する要求条件の概要を提示します。Enthernet により接続される ONU 機能部とのインタフェース仕様については、[2.2.1 インタフェース条件]に準じます。

4.1.1　インタフェース規定点

本装置では、図 4.1 に示すユーザ・網インタフェース（UNI）を規定します。

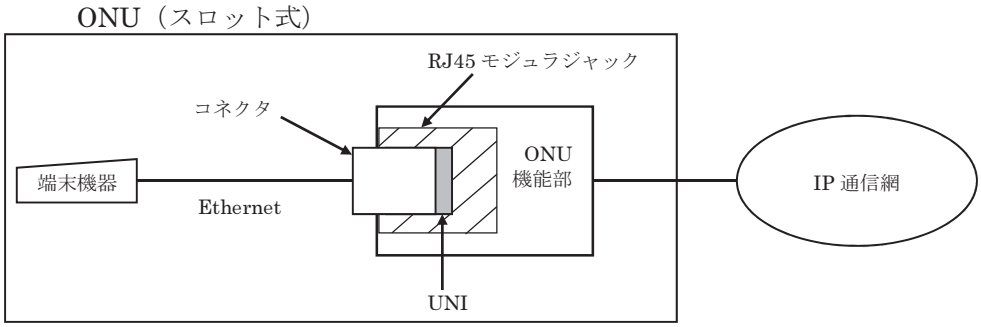


図 4.1　インタフェース規定点

4.1.2　端末設備と電気通信回線設備の分界点

本装置の端末設備と電気通信回線設備との分界点について図 4.2 に示します。また、端末設備が必ず適合しなければならない技術的条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

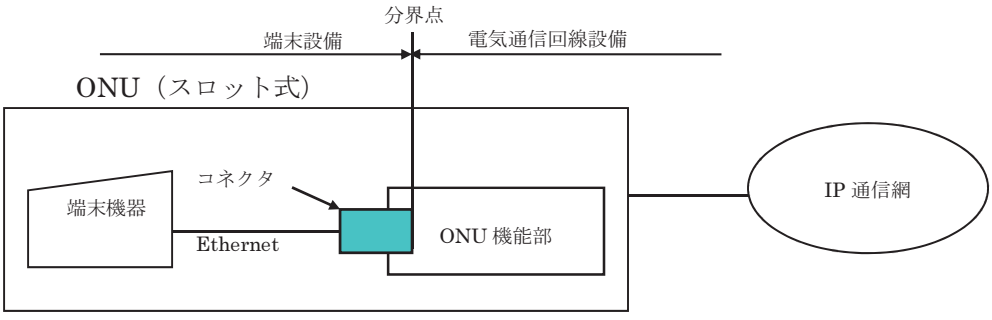


図 4.2　分界点

フレッツ 光ライト

1　フレッツ 光ライトの概要

1.1　サービスの概要

フレッツ 光ライトは、ベストエフォート型の IP 通信サービスに加え、帯域確保型のアプリケーションサービスを利用可能なサービスです。フレッツ 光ライトを利用する端末機器等（以下、端末機器）は、電気通信事業者等と IP 通信網を介して IP 通信を行います。フレッツ 光ライトの基本構成を図 1.1 に示します。

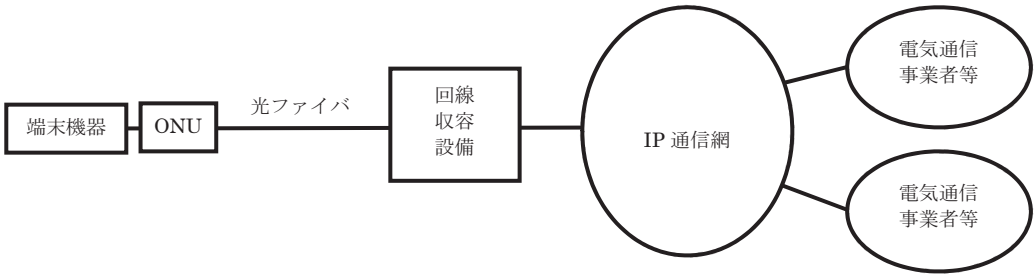


図 1.1 フレッツ 光ライトの基本構成

なお、フレッツ・v6 オプションを契約することで、フレッツ光 ネクストおよびフレッツ光 ライトを利用する端末機器同士で図 1.2 に示す IP 通信網内で折り返した IPv6(IPoE)通信を行うことができます。

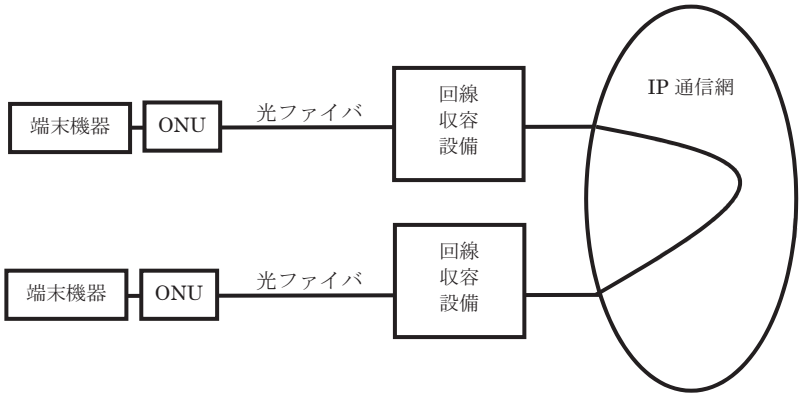


図 1.2 フレッツ・v6 オプションの契約者同士の通信

1.2 インタフェース規定点

フレッツ 光ライトでは、図 1.3 に示すユーザ・網インタフェース（UNI）を規定します。

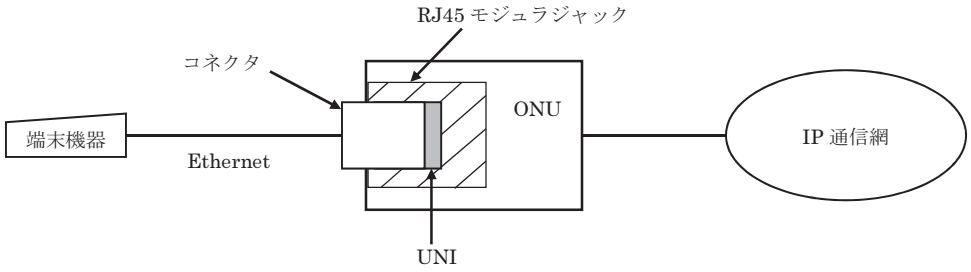


図 1.3 インタフェース規定点

1.3 端末設備と電気通信回線設備の分界点

端末設備と電気通信回線設備との分界点について図 1.4 に示します。また、端末設備が必ず適合しなければならない技術的条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

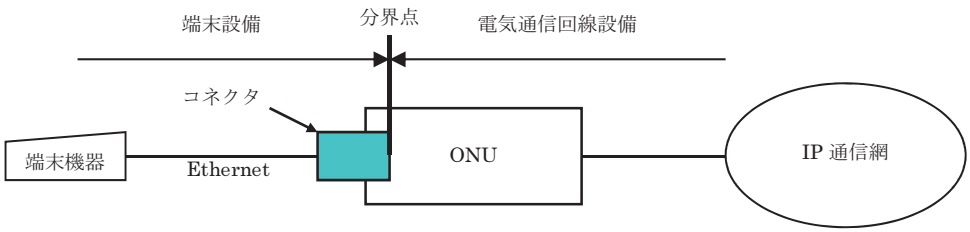


図 1.4 分界点

1.4 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 1.5 に示します。

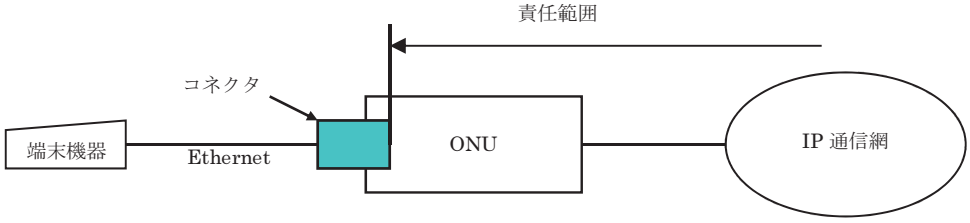


図 1.5 施工・保守上の責任範囲

2 ユーザ・網インタフェース仕様

2.1 プロトコル構成

プロトコル構成は、表 2.1 に示す OSI 参照モデルに則した階層構造となっています。

表 2.1 プロトコル構成

レイヤ		使用するプロトコル		
		IPv6 通信		IPv4 通信
		IPoE 方式	PPPoE 方式	PPPoE 方式
7	アプリケーション	DHCPv6: RFC3315 / RFC3513 / RFC3646 / RFC4075 DHCPv6-PD: RFC3633 DNS: RFC1034 / RFC1035 / RFC1123 / RFC2181 / RFC2308 / RFC2671 / RFC2782 / RFC3596 SNTP: RFC4330 HTTP: RFC2616	DHCPv6: RFC3315 / RFC3513 / RFC3646 DHCPv6-PD: RFC3633	
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	IPv6: RFC2460 / RFC2462 / RFC3513 ICMPv6: RFC4443 NDP: RFC2461 MLDv2: RFC2711 / RFC3810	IPv6: RFC2460 /RFC3513 ICMPv6: RFC2463	IPv4: RFC791 ICMPv4: RFC792
2	データリンク	MAC: IEEE802.3-2005	PPPoE: RFC1332 / RFC2472(IPv6CP) / RFC1334(PAP) / RFC1994(CHAP) / RFC1661(PPP) / RFC2516(PPPoE) MAC: IEEE802.3-2005	PPPoE: RFC1332 / RFC1877(IPCP) / RFC1334(PAP) / RFC1994(CHAP) / RFC1661(PPP) / RFC2516(PPPoE) MAC: IEEE802.3-2005
1	物理	IEEE 802.3-2005 1000BASE-T 準拠 IEEE 802.3-2005 100BASE-TX 準拠 IEEE 802.3-2005 10BASE-T 準拠		

2.2 物理レイヤ（レイヤ 1）仕様

フレッツ 光ライトがサポートするレイヤ 1 のインタフェース条件と通信モードを表 2.2 に示します。

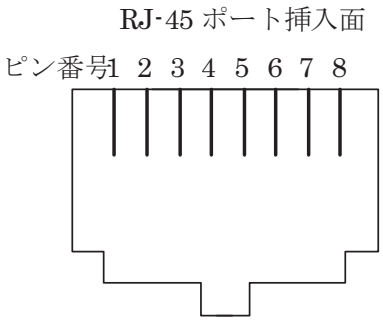
表 2.2 インタフェース条件

タイプ	インタフェース条件	通信モード
ファミリータイプ	10BASE-T または 100BASE-TX（Auto-MDI/MDI-X）(注)	自動折衝機能（Auto Negotiation）(注)
マンションタイプ		

（注） インタフェースと通信モードは ONU の自動折衝機能（Auto Negotiation）により決定します。

2.2.1 インタフェース条件

ユーザ・網インタフェースは、IS08877 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 2.1 に示します。



ピン番号	10BASE-T / 100BASE-TX			
	方向	記号	信号方向	
			端末側	網側
1	受信	RD(+)	→	
2	受信	RD(-)	→	
3	送信	TD(+)	←	
4				
5				
6	送信	TD(-)	←	
7				
8				

図 2.1 挿入面から見た RJ-45 ポートのピン配置

2.3 データリンクレイヤ（レイヤ 2）仕様

レイヤ 2 では、IEEE 802.3-2005 に規定されている MAC、PPP、PAP、CHAP の一部、IPCP、PPPoE を使用します。MAC の詳細については、IEEE 802.3-2005 を、PPP、PAP、CHAP、IPCP、PPPoE の詳細については[3.1PPP]と[3.2PPPoE]を参照してください。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。

2.4 レイヤ 3 仕様

レイヤ 3 では、RFC791 に規定されている IPv4、RFC2460 に規定されている IPv6 の両方をサポートします。IP 通信網に接続された端末機器は使用用途、実装に応じ IPv4、IPv6 のどちらか一方、もしくは双方同時に使用することが可能です。

また IPv4 のサブセットとして RFC792 に規定されている ICMPv4 の一部についてもサポートします。

IPv6 については RFC3513 に規定されている IPv6 アドレッシング、RFC2461 に規定されている NDP、RFC2462 に規定されている IPv6 アドレスオートコンフィグ、RFC4443 に規定されている ICMPv6、RFC3315 に規定されている DHCPv6 等の一部、またはすべてをサポートします。ただし、IP 通信網内に存在しない宛先に送信されるパケットについては、IP 通信網において応答なくパケット破棄される場合や、RFC793 に規定される RST ビットをセットした TCP パケットを返信する場合があります。

それぞれのプロトコル適用範囲については[2.4.1 IPv4 仕様]、[**エラー！ 参照元が見つかりません。 エラー！ 参照元が見つかりません。**]を参照してください。

各仕様に関する詳細は各 RFC を参照してください。

2.4.1 IPv4 仕様

RFC791 に規定されている IPv4 を使用します。また、IPv4 のサブセットとして RFC792 に規定されている ICMPv4 の一部についてもサポートします。

2.4.1.1 IPv4 アドレス

フレッツ 光ライトでは、RFC1700 で規定されているクラス D、クラス E アドレスをサポートしません。また、端末機器のアドレスとして利用可能なアドレスは IP 通信網に接続する際に、IP 通信網または接続先から割り当てられたアドレスの範囲のみです。その他のアドレスを利用する場合、動作は保証しません。

2.4.1.2 最大転送単位 (MTU)

フレッツ 光ライトでは IP 通信網における IPv4 通信の MTU 値は 1454byte です。IP 通信網が MTU 値を超えるパケットを受信した場合、IP 通信網はパケットを分割転送、または破棄する場合があります。

2.4.2 IPv6 仕様

IP 通信網では IPv6 通信(IPoE 方式)と IPv6 通信 (PPPoE 方式) における IPv6 通信の 2 つをサポートとしています。IPv6 通信(IPoE 方式)については[2.4.2.1 IPoE 方式における IPv6 仕様]を、IPv6 通信(PPPoE 方式)については[2.4.2.2 PPPoE 方式における IPv6 仕様]をご参照下さい。

2.4.2.1 IPoE 方式における IPv6 仕様

RFC2460 に規定されている IPv6 を使用します。また、IPv6 のサブセットとして RFC3513 (IPv6 Addressing Architecture)、RFC2461 (Neighbor Discovery for IPv6)、RFC2462 (IPv6 Stateless Address Autoconfiguration)、RFC4443 (ICMPv6)、 RFC3315 (DHCPv6)、RFC3810 (MLDv2) 等の一部、またはすべてをサポートします。

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 に規定するルータアラートオプション)、フラグメントヘッダ、認証ヘッダ、暗号化ペイロードヘッダを使用します。その他の拡張ヘッダを使用した場合は、IP 通信網は転送を保証できない場合があります。

2.4.2.1.1 IPoE 方式における IPv6 アドレス

IPv6 アドレスは、RFC3513 で規定されている IPv6 のグローバル・ユニキャストアドレスを使用します。端末機器ではリンクローカルアドレスを除いて IP 通信網が割り当てる以外のアドレスは使用できません。また、端末機器は Preferred Lifetime が 0 でないアドレスを所持している場合は、Preferred Lifetime が 0 でないアドレスの利用を推奨します。IPv6 アドレス情報の付与方法については[2.4.2.1.2 IPoE 方式における IPv6 アドレス情報付与方法]を参照してください。

2.4.2.1.2　IPoE 方式における IPv6 アドレス情報付与方法

IP 通信網は、RFC2461 に規定されている NDP（Neighbor Discovery Protocol）に基づき、ルータ広告（Router Advertisement）メッセージを端末機器に送信します。なお、ルータ広告の Other stateful configuration flag 及び Managed address configuration flag が 1 に設定される場合があります。また、ルータ広告の Preferrd Lifetime は 0 に設定される場合があります。端末機器は Other stateful configuration flag が 1 に設定されたルータ広告を受信した際は、DHCPv6 機能を利用し付加情報を取得するため、Information-Request を送信することを推奨します。ルータ広告の Managed address configuration flag が 1 に設定されたルータ広告を受信した場合は RFC3315、RFC3633 に規定される DHCPv6-PD（DHCP による IPv6 Prefix Option）を使用し IPv6 Prefix を取得することを推奨します。なお、DHCPv6 を利用した 128bit の IPv6 アドレスの取得はできません。

端末機器のアドレスとして利用可能なアドレスは、このルータ広告メッセージに含まれる 64bit の IPv6 Prefix を利用して生成した IPv6 のグローバル・ユニキャストアドレスのみです。ただし、IP 通信網上で提供する音声利用 IP 通信網サービス等を利用する場合は、RFC3315、RFC3633 に規定される DHCPv6-PD のみを使用し、IP 通信網から 48bit または 56bit の IPv6 Prefix を含むメッセージを当該端末機器に送信します。

また、サービスの利用状況等により IP 通信網から送信される IPv6 Prefix の値は変更される場合があります。なお、IPv6 Prefix のサイズは IP 通信網より指定をして送信します。

2.4.2.1.3　IPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得

端末機器は DHCPv6 を用いて、DHCPv6 のオプションにより RFC3646 に規定される DNS サーバアドレスの情報及びドメインサーチリストの情報、RFC4075 に規定される SNTP サーバアドレスの情報を取得することが可能です。

また、IP 通信網上で提供する音声利用 IP 通信網サービスを利用する場合は、DHCPv6 のオプションにより取得可能な情報が追加される場合があります。詳細は該当するサービスの技術資料等を参照してください。

仕様に関する詳細は各 RFC を参照してください。

2.4.2.1.4　IPoE 方式における DHCPv6 における DUID 生成方式

IP 通信網の DUID 生成方式は RFC3315 に規定される DUID-LL 方式であり、MAC アドレスから DUID を生成します。端末側の DUID 生成方式は RFC3315 に規定される DUID-LL 方式に準拠する必要があります。端末機器も IP 通信網と同様に MAC アドレスから DUID を生成する必要があります。

2.4.2.1.5　IPoE 方式における最大転送単位（MTU）

IP 通信網における IPv6 通信の MTU の値は 1500byte です。

IP 通信網が MTU の値を超えるパケットを受信した場合、IP 通信網は、パケットを破棄します。

2.4.2.2　PPPoE 方式における IPv6 仕様

RFC2460 に規定されている IPv6 を使用します。また、IPv6 のサブセットとして RFC3513 （IPv6 Addressing Architecture)、RFC2463（ICMPv6)、 RFC3315（DHCPv6）等の一部、またはすべてをサポートします。

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、フラグメントヘッダ、認証ヘッダ、暗号化ペイロードヘッダを使用します。その他の拡張ヘッダを使用した場合は、IP 通信網は転送を保証できない場合があります。

2.4.2.2.1　PPPoE 方式における IPv6 アドレス

IPv6 アドレスは、RFC3513 で規定されている IPv6 のグローバル・ユニキャストアドレスを使用します。端末機器ではリンクローカルアドレスを除いて IP 通信網が割り当てる以外のアドレスは使用できません。IPv6 アドレス情報の付与方法については[2.4.2.2.2 PPPoE 方式における IPv6 アドレス情報付与方法]を参照してください。

2.4.2.2.2　PPPoE 方式における IPv6 アドレス情報付与方法

IP 通信網は、RFC3315、RFC3633 に規定される DHCPv6-PD（DHCP による IPv6 Prefix Option）のみを使用し、PPPoE によって確立したトンネルから通知される IPv6Prefix を含むメッセージを当該端末機器に送信します。端末機器のアドレスとして利用可能なアドレスは、このルータ広告メッセージに含まれる IPv6 Prefix を利用して生成した IPv6 のグローバル・ユニキャストアドレスのみです。

2.4.2.2.3　PPPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得

端末機器は DHCPv6 を用いて、DHCPv6 のオプションにより RFC3646 に規定される DNS サーバアドレスの情報を取得することが可能です。

仕様に関する詳細は RFC を参照してください。

2.4.2.2.4　PPPoE 方式における DHCPv6 における DUID 生成方式

IP 通信網の DUID 生成方式は RFC3315 に規定される DUID-LL 方式であり、MAC アドレスから DUID を生成します。端末側の DUID 生成方式は RFC3315 に規定される DUID-LL 方式に準拠する必要があります。端末機器も IP 通信網と同様に MAC アドレスから DUID を生成する必要があります。

2.4.2.2.5　PPPoE 方式における最大転送単位（MTU）

IP 通信網における IPv6 通信の MTU の値は 1454byte です。

IP 通信網が MTU の値を超えるパケットを受信した場合、IP 通信網は、パケットを破棄します。

2.4.3　転送優先度に関する仕様

端末機器等は、利用するサービスに応じて、パケットに転送優先度を指定することが可能です。転送優先度識別子として DSCP(Differentiated Services Code Point)値を使用します。DSCP の仕様については RFC2474 を、各サービスで利用可能な転送優先度に関する仕様については、各サービスの技術規定等を参照してください。

尚、各サービスにおいて許容されたプロトコルと転送優先度の組み合わせ以外のパケットに転送優先度を指定することは許容しません。

2.5　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、DHCPv6、DHCPv6-PD のみ規定します。IPv6 通信 IPoE 方式においては、前述に加え DNS、SNTP および HTTP を規定します。その他の通信においては、特に規定はありません。

DHCPv6 については[2.4.2.1.3 IPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得]および[2.4.2.1.4 IPoE 方式における DHCPv6 における DUID 生成方式]、または [2.4.2.2.3 PPPoE 方式における DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得] および[2.4.2.2.4 PPPoE 方式における DHCPv6 における DUID 生成方式]を、DHCPv6-PD については[2.4.2.1.2 IPoE 方式における IPv6 アドレス情報付与方法]および [2.4.2.2.2 PPPoE 方式における IPv6 アドレス情報付与方法] を参照してください。

2.5.1 DNS

IPv6 に対応した端末機器は、IP 通信網経由でアクセス可能な DNS サーバ間で、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 2.3 に示します。各仕様に関する詳細は各 RFC を参照してください。

表 2.3 DNS 規定

参照文献	タイトル	備考
RFC1034	Domain names – concepts and facilities	DNS について規定
RFC1035	Domain names – implementation and specification	DNS について規定
RFC1123	Requirements for Internet Hosts – Application and Support	DNS の実装について規定
RFC2181	Clarifications to the DNS Specification	DNS について規定
RFC2308	Negative Caching of DNS Queries (DNS NCACHE)	ネガティブキャッシュについて規定
RFC2671	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	A DNS RR for specifying the location of services	SRV レコードを規定
RFC3596	DNS Extensions to Support IP Version 6	IPv6 対応を規定

2.5.2 SNTP

IPv6 に対応した端末は、利用するサービスに応じて、時刻取得のためのプロトコルとして SNTP を使用することが可能です。

SNTP を利用する場合に準拠する規定は RFC4330 となります。仕様に関する詳細は RFC4330 を参照してください。

2.5.3 HTTP

IPv6 に対応した端末は、通信するプロトコルとして HTTP を使用することが可能です。

HTTP を利用する場合に準拠する規程は RFC2616 となります。仕様に関する詳細は RFC2616 を参照してください。

IP 通信網内で利用できる HTTP サーバには、経路情報提供サーバがあり、経路情報提供サーバの利用条件については[2.5.3.1 経路情報提供サーバについて]、[2.5.3.2 経路情報提供サーバで利用するメッセージ]、[2.5.3.3 経路情報提供サーバとの通信シーケンス]を参照してください。

2.5.3.1 経路情報提供サーバについて

経路情報提供サーバは、端末機器に対して IP 通信網の IPv6 prefix 等の情報を提供します。経路情報提供サーバへの接続へは表 2.4 に示す条件でアクセスする事とします。

表 2.4 経路情報提供サーバへの接続条件

項番	項目名	内容
1	レイヤ 3	IPv6
2	上位レイヤ	HTTP
3	FQDN	route-info.flets-west.jp
4	ポート番号	49881

2.5.3.2 経路情報提供サーバで利用するメッセージ

2.5.3.2.1 リクエストメッセージ

経路情報提供サーバへリクエストメッセージを送信する際のフォーマットを図 2.2、リクエストライン、およびリクエストヘッダの構成要素を表 2.5 と表 2.6 に示します。表 2.6 で規定していないメッセージは動作保障対象外とします。

GET[SP]リクエスト URI[SP]HTTP プロトコル[CR][LF]
Host:[SP]ホスト名：ポート番号[CR][LF]
Accept:[SP]サポートコンテンツタイプ[CR][LF]
Accept-Charset:[SP]サポートエンコード種別[CR][LF]
Connection:[SP]コネクショントークン[CR][LF]
[CR][LF]

図 2.2 リクエストメッセージのフォーマット

表 2.5 リクエストライン

項番	項目名	必須／省略可能	内容
1	HTTP メゾット	必須	「GET」固定
2	リクエスト URI	必須	「/v6/route-info」固定
3	HTTP プロトコル	必須	「HTTP/1.1」固定

表 2.6 リクエストヘッダ

項番	ヘッダ名	項目名	必須／省略可能	内容
1	Host	ホスト名:ポート番号	必須	ホスト名に、経路情報提供サーバの URL を入力 ポート番号は「49881」固定
2	Accept	サポートコンテンツタイプ	必須	「*/*」固定
3	Accept-Charset	サポートエンコード種別	省略可能	指定可能な文字コードは「EUC-JP」、「Shift_JIS」、「UTF-8」とする 文字コードの指定が無い場合は「EUC-JP」として処理する
4	Connection	コネクショントークン	必須	「close」固定

2.5.3.2.2　レスポンスメッセージ

経路情報提供サーバからレスポンスメッセージを受信する際のフォーマットを図 2.3 に、ステータスラインおよびレスポンスヘッダの構成要素を表 2.7 と表 2.8 に示します。

レスポンスメッセージのステータスコードに 200 以外が指定される場合のレスポンスヘッダは定義しません。したがって、ステータスコード 408 または 503 が返却された場合、あるいはリクエストメッセージを送信後 10 秒以上無応答状態が発生した場合は再取得を行う必要があります。

なお、再取得はリクエストメッセージの送信契機につき 2 回までとします。

HTTP バージョン[SP]ステータスコード[SP]テキストフレーズ[CR][LF]
Date:日付/時刻スタンプ[CR][LF]
Content-Type:[SP]メッセージボディ部コンテンツタイプ[CR][LF]
Content-Length:[SP]メッセージボディ部バイト長[CR][LF]
Connection:[SP]コネクショントークン[CR][LF]
[CR][LF]
メッセージボディ部

図 2.3 レスポンスメッセージのフォーマット

表 2.7 ステータスライン

項番	項目名	必須／省略可能	内容
1	HTTP バージョン	必須	「HTTP/1.1」固定
2	ステータスコード	必須	経路情報提供サーバが正常に処理結果を送信できる場合、「200」を設定 リクエストメッセージのフォーマットエラー時は、「400」を設定 リクエストタイムアウトが発生した場合は「408」を設定 経路情報提供サーバが一時的にサービス停止状態である場合には「503」を設定
3	テキストフレーズ	必須	ステータスコードに応じたテキストフレーズを設定

表 2.8 レスポンスヘッダ

項番	ヘッダ名	項目名	必須／省略可能	内容
1	Date	日付/時刻スタンプ	必須	メッセージ生成の日付/日時
2	Content-Type	メッセージボディ部のコンテンツタイプとコンテンツタイプ	必須	「text/plain」固定
		メッセージボディ部の文字コード	必須	Accept-Charset で指定された文字コードを受信 未指定時は「EUC-JP」を設定
3	Content-Length	メッセージボディ部のバイト長	必須	HTTP メッセージボディ部バイト長の整数値
4	Connection	コネクショントークン	必須	「close」固定

2.5.3.2.3 メッセージボディ部

メッセージボディのフォーマットの構成要素を図 2.4 に、構成要素を表 2.9 に示します。

レスポンスメッセージのステータスコードに 200 以外が指定される場合のメッセージボディは定義しません。したがって、端末ではステータスコードが 200 以外の場合には、メッセージボディ部に指定された任意のパラメータを無視する必要があります。

タイプナンバー[1],経路情報の更新年月日[CR][LF]
タイプナンバー[2],IPv6 prefix/prefix 長[CR][LF]
・
・
・
タイプナンバー[n],IPv6 prefix/prefix 長[CR][LF]

図 2.4 メッセージボディのフォーマット

表 2.9 メッセージボディ

項番	パラメータ	必須/省略可	繰り返し可否 （最大数）	内容	許容文字種別	文字長 (byte)
1	タイプナンバー[n] n の最大数 :101	必須	可（101 回）	アドレス帯の識別情報 0000 は情報更新年月日時	0-9	4
2	経路情報の更新年月日	必須	否	経路情報提供サーバで保持する経路情報の更新年月日 YYYY/MM/DD[SP]hh:mm:ss の形式で表記	0-9 [/] [.] [:] [SP]	19
3	IPv6 prefix	必須	可（100 回）	経路情報を示すIPv6 prefix（完全表記）	0-9 a-f [:]	39
4	IPv6 prefix 長	必須	可（100 回）	IPv6 prefix 長	0-9	1 以上 3 以下の可変長

2.5.3.2.4 タイプナンバー

4 桁の数字で構成されるタイプナンバーにより、経路情報提供サーバから受信する経路情報の内容を把握することができます。1 桁目、2 桁目、3 桁目の数値は表 2.10 に示す内容を表し、4 桁目の数値は通番として利用しています。なお、タイプナンバー「0000」は情報更新年月日を意味します。

表 2.10 タイプナンバーの構成要素

1 桁		2 桁		3 桁		4 桁	
地域情報		アドレス帯の情報		利用用途		通番	
0	情報更新年月日時	0	情報更新年月日時	0	情報更新年月日時	0	情報更新年月日時
1	NTT 東日本エリア						
2	NTT 西日本エリア	1	IP 通信網	1	PPPoE 接続基盤		
		2	IP 通信網	1	IPoE 基盤		
		3	IP 通信網	1	網内折り返し基盤		
		4	接続事業者	1	IPv6 インターネット接続（IPoE）		

2.5.3.3 経路情報提供サーバとの通信シーケンス

経路情報提供サーバとの通信シーケンスは図 2.5 に示す通りです。なお、経路情報提供サーバは IP 通信網の状況により端末機器に対してレスポンスメッセージを返信しない場合がございます。端末機器からリクエストメッセージを送信する契機は表 2.11 を参照してください。

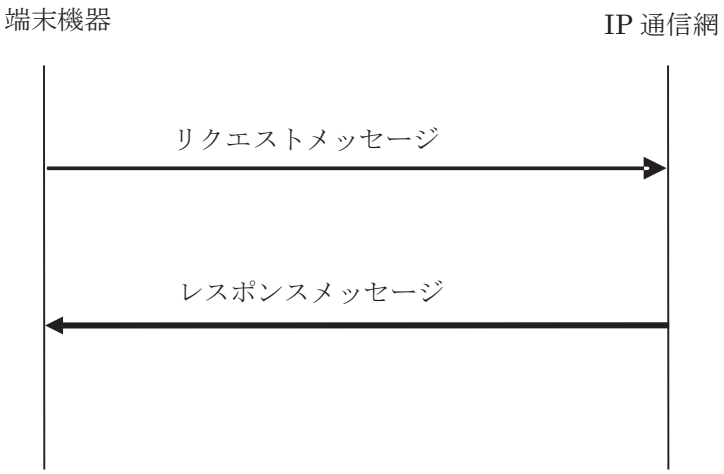


図 2.5 経路情報提供サーバとの通信シーケンス

表 2.11 リクエストメッセージの送信契機

送信契機	内容
初回送信	端末機器起動時から 0 秒～60 秒の間のランダムに設定した時間後に送信
定期送信(初回)	初回送信時から 86,400 秒～691,200 秒の間のランダムに設定した時間後に送信
定期送信	定期送信(初回)から 604,800 秒に 1 回の間隔で送信

3 PPPoE / PPP プロトコル

3.1 PPP

3.1.1 PPP の概要

PPP（Point-to-Point Protocol）は、非同期型（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ける複数のプロトコルのカプセル化と、LCP（Link Control Protocol）によるデータリンク回線の確立・設定・試験・開放、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・設定を行います。使用する PPP の仕様の詳細は、以下に示す仕様を除き、RFC1661 を参照してください。

3.1.2 PPP パケット

PPP パケットのプロトコルフィールド（Protocol Field）に格納される値を表 3.1 に示します。表 3.1 で示す値以外のプロトコルについては動作を保証しません。

表 3.1 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
0x8057	IPv6 Control Protocol（IPv6CP）	
0x0021	Internet Protocol（IP）	ネットワーク レイヤプロトコル
0x0057	Internet Protocol Version 6（IPv6）	

3.1.3 LCP

LCP 通信設定オプション（LCP Configuration Option）のタイプ値を表 3.2 に示します。表 3.2 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。IP 通信網は Maximum-Receive-Unit（MRU）オプションの値を 1454 オクテットでネゴシエーションを要求します。MRU の詳細については RFC1661 を参照してください。

また、IP 通信網の要求する MRU 値より、小さな値で端末機器がネゴシエーションを要求した場合、接続や正常な通信ができない場合があります。IP 通信網が MRU 値を超えるパケットを受信した場合、IP 通信網はパケットを分割転送、または破棄する場合があります。

表 3.2 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

3.1.4 PAP

PAP Authenticate-Request パケットの Peer-ID-Length フィールドに入る最大値は 0x3f です。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。

3.1.5 CHAP

CHAP Response パケットの Name フィールド長の最大長は 63 オクテットです。Name フィールド長がこの最大長を超えた場合は、動作は保証しません。

3.1.6 IPCP

IPCP 通信設定オプション（IPCP Configuration Option）のタイプ値を表 3.3 に示します。表 3.3 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 3.3 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

3.1.7 IPv6CP

IPv6CP 通信設定オプション（IPv6CP Configuration Option）のタイプ値を表 3.4 に示します。表 3.4 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 3.4 IPv6CP 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	Interface-ID	使用
2	IPv6-Compression-Protocol	使用不可

3.2 PPPoE

3.2.1 PPPoE の概要

PPPoE は、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 上の端末機器（以下、ホスト）と、IP 通信網の機能である Access Concentrator（以下、AC）間の PPP セッションの確立・設定・開放を行います。

PPPoE により PPP セッションを確立・設定・開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。

使用する PPPoE の仕様の詳細は、以下に示す仕様を除き、RFC2516 を参照してください。

3.2.2 ディスカバリステージ

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、開放を通知する動作が含まれます。

3.2.2.1 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 3.1 に示します。

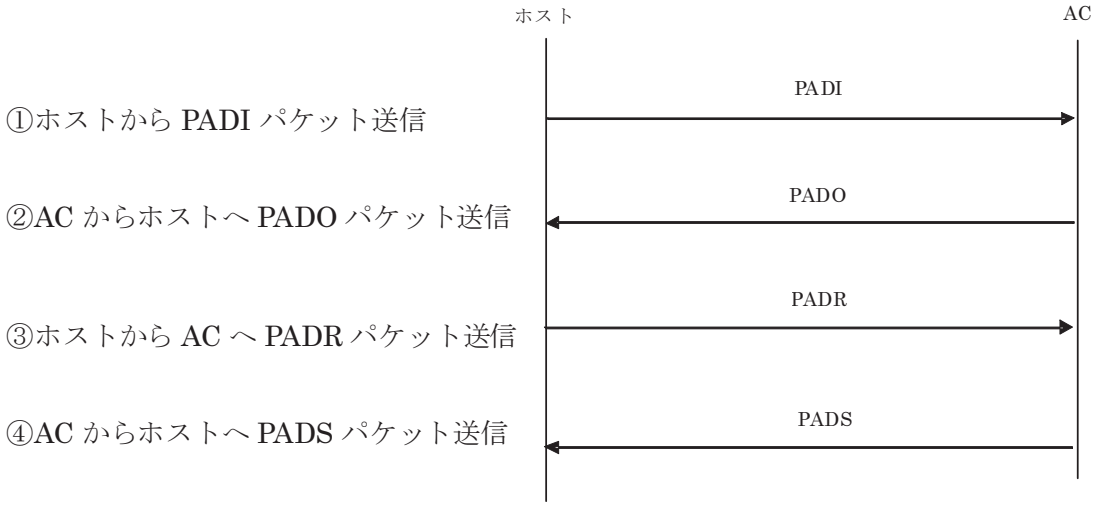


図 3.1 PPPoE セッション確立手順

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、ホストと AC 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。

3.2.2.2 PPPoE セッションの開放を通知する動作

PPPoE セッションの開放を通知する動作では、ホストまたは AC から PPPoE セッションが開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。

3.2.2.3 PADI パケット

ホストは要求するサービス名を含む PADI パケットを送信し、AC 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。ホスト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。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 オクテットを超えてはなりません。表 3.5 に PADI パケットのタグ設定値を示します。

表 3.5 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	-	-	使用不可
Service-Name	0x0101	0	-	使用
AC-Name	0x0102	-	-	使用不可
Host-Uniq	0x0103	可変長	-	使用可
AC-Cookie	0x0104	-	-	使用不可
Vendor-Specific	0x0105	-	-	使用不可
Relay-Session-Id	0x0110	-	-	使用不可
Service-Name-Error	0x0201	-	-	使用不可
AC-System-Error	0x0202	-	-	使用不可
Generic-Error	0x0203	-	-	使用不可

3.2.2.4 PADO パケット

PADI パケットを受信した AC は、送信元のホストに PADO パケットを送信し、AC がサポートするサービス名、AC 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 タグを含みます。AC 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 3.6 に PADO パケットのタグ設定値を示します。

なお、1 つの回線から 5 分間に 20 回を超える PADI パケットを受信した場合、一定期間、PADO パケットを送信しない場合があります。

表 3.6 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	-	-	未使用
Service-Name	0x0101	0	PADI 送信値	使用
AC-Name	0x0102	可変長	-	使用
Host-Uniq	0x0103	可変長	PADI 送信値	使用可
AC-Cookie	0x0104	可変長	-	使用可
Vendor-Specific	0x0105	-	-	未使用
Relay-Session-Id	0x0110	-	-	未使用
Service-Name-Error	0x0201	-	-	未使用
AC-System-Error	0x0202	-	-	未使用
Generic-Error	0x0203	可変長	-	使用可

3.2.2.5 PADR パケット

ホストは受信した 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 AC 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。ホスト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 3.7 に PADR パケットのタグ設定値を示します。

表 3.7 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	-	-	使用不可
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(注)
Vendor-Specific	0x0105	-	-	使用不可
Relay-Session-Id	0x0110	-	-	使用不可
Service-Name-Error	0x0201	-	-	使用不可
AC-System-Error	0x0202	-	-	使用不可
Generic-Error	0x0203	可変長	-	使用可

(注)PADO に AC-Cookie タグが含まれている場合は使用します。

3.2.2.6 PADS パケット

PADR パケットを受信した AC 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 パケットをホストへ送信します。

ホストが PADS パケットを受信すると、ホストと AC は固有の PPPoE セッション ID と相互の MAC アドレスを認識し、PPPoE セッションの確立が完了します。

AC 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 を設定します。表 3.8 に PADS パケットのタグ設定値を示します。

表 3.8 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(注 1)
AC-Name	0x0102	可変長	PADR 送信値	使用可(注 2)
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(注 2)
Vendor-Specific	0x0105	-	-	未使用
Relay-Session-Id	0x0110	-	-	未使用
Service-Name-Error	0x0201	可変長	-	使用(注 3)
AC-System-Error	0x0202	-	-	使用可
Generic-Error	0x0203	可変長	-	使用可

(注 1)要求されたサービス名を受け入れる場合は使用します。

(注 2)PADR 送信値を送信しない場合があります。

(注 3) 要求されたサービス名を拒否する場合は使用します。

3.2.2.7 PADT パケット

PPPoE セッション確立後、ホストまたは AC は PPPoE セッションが開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 フィールドには開放された PPPoE セッションのセッション ID を設定します。タグは使用しません。

3.2.3 PPP セッションステージ

PPPoE セッションが確立されると、PPP セッションステージへと進みます。PPP セッションステージでは、PPP セッションが確立され、IP 通信が開始します。PPP セッションの開放によって PPP セッションステージは終了します。

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ホストまたは 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。使用する PPP プロトコル識別子については 3.1[3.1 PPP]を参照してください。

3.2.4 自動再接続間隔

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

3.2.5 PPPoE セッション数

同時に利用することが可能な PPPoE セッション数は制限されています。各品目において同時利用可能なセッション数を表 3.9 に示します。（基本セッション数を超える同時利用可能 PPPoE セッション数の設定は別途サービスの契約により変更可能です。）

表 3.9 同時利用可能 PPPoE セッション数

品目	同時利用可能 PPPoE セッション数 （基本セッション数／最大セッション数）
ファミリータイプ	2 ／ 5
マンションタイプ	2 ／ 5

3.2.6 通信シーケンス

端末機器と IP 通信網の間の通信シーケンスを図 3.2 **エラー！参照元が見つかりません。**～図 3.6 **エラー！参照元が見つかりません。**に示します。

3.2.6.1　　接続シーケンス（IPv4 通信 PPPoE 方式）

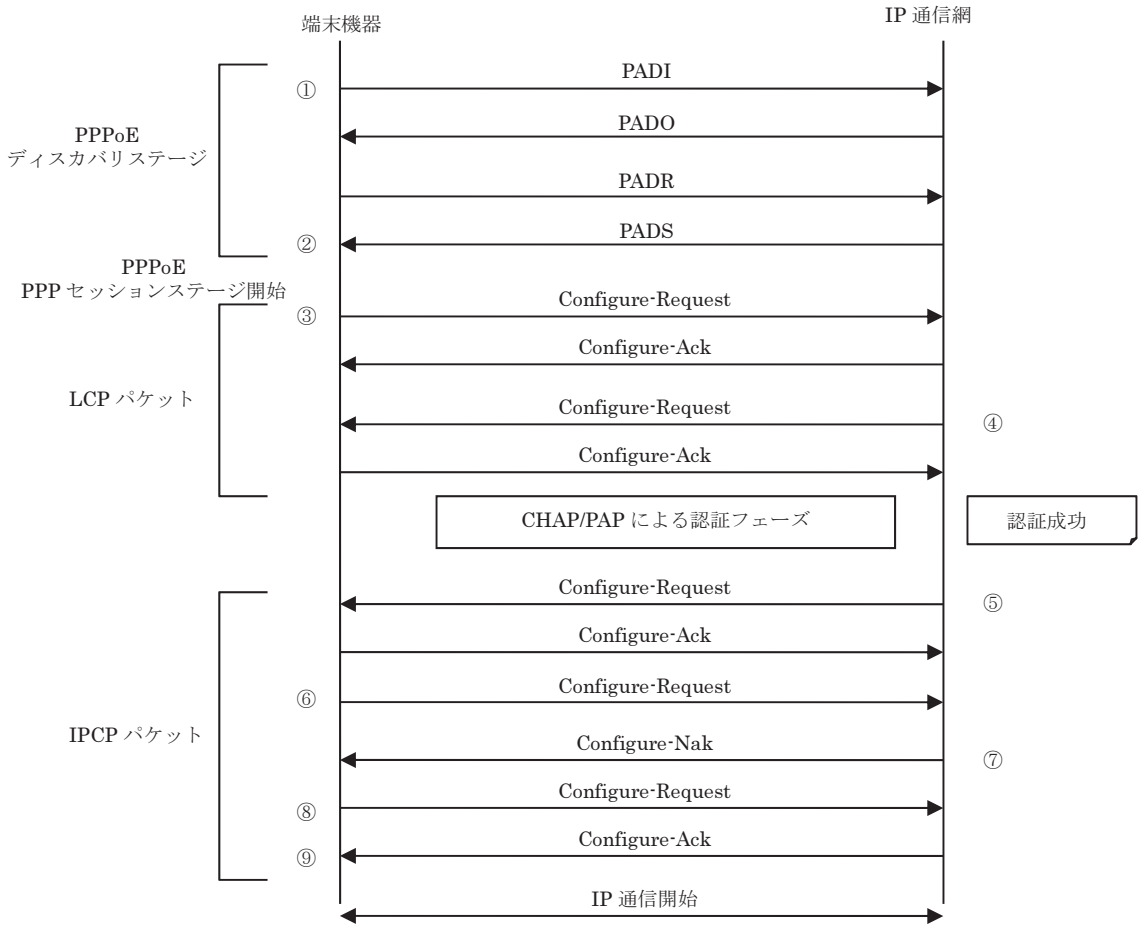


図 3.2　接続シーケンス（例）

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

3.2.6.2　　接続シーケンス（IPv6 通信 PPPoE 方式）

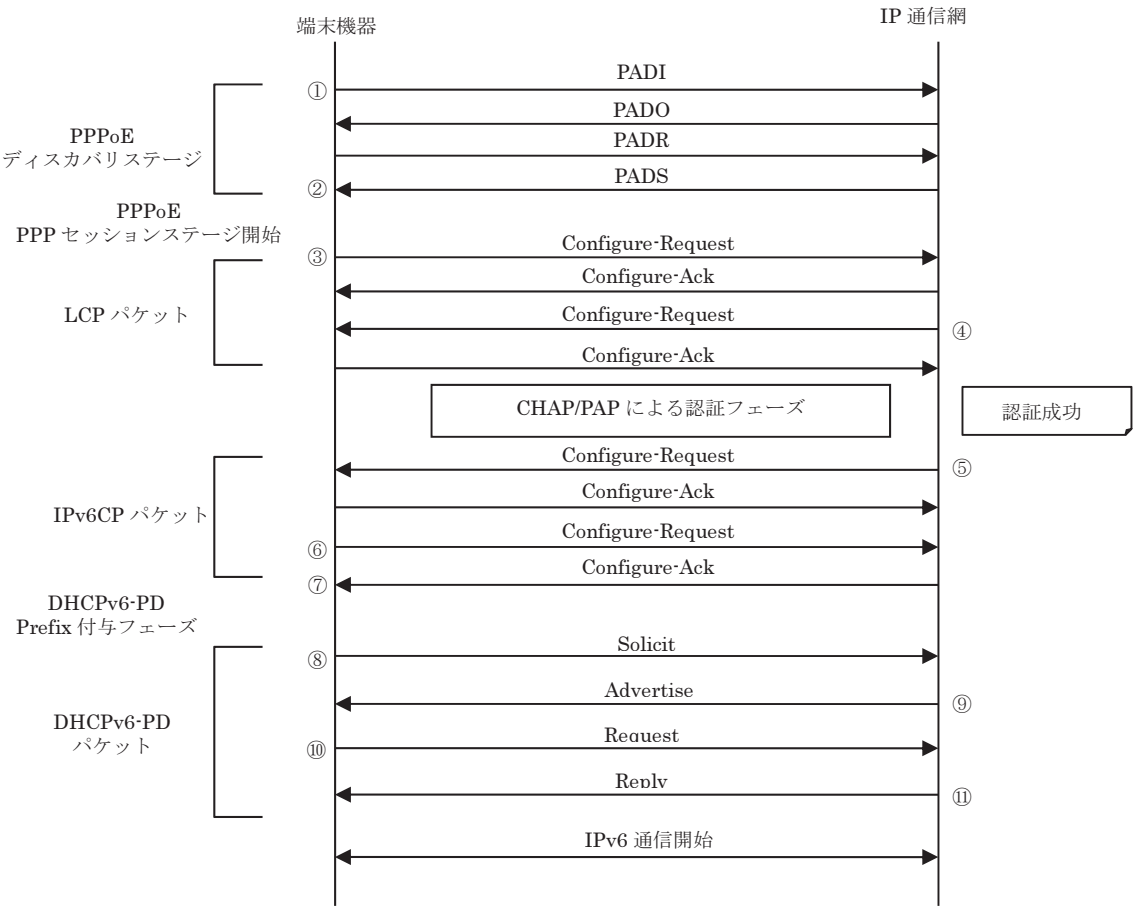


図 3.3　接続シーケンス（例）

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 網側が使用する Interface-ID を通知
⑥ 端末機器が使用する Interface-ID を通知
⑦ PPP セッションが確立
⑧ 端末機器が IP アドレス払出を要請
⑨ 網側が IP アドレスを広告
⑩ 端末機器が使用する IP アドレス払出を要求
⑪ 端末機器に割り当てる IP アドレスを返送

3.2.6.3 切断シーケンス

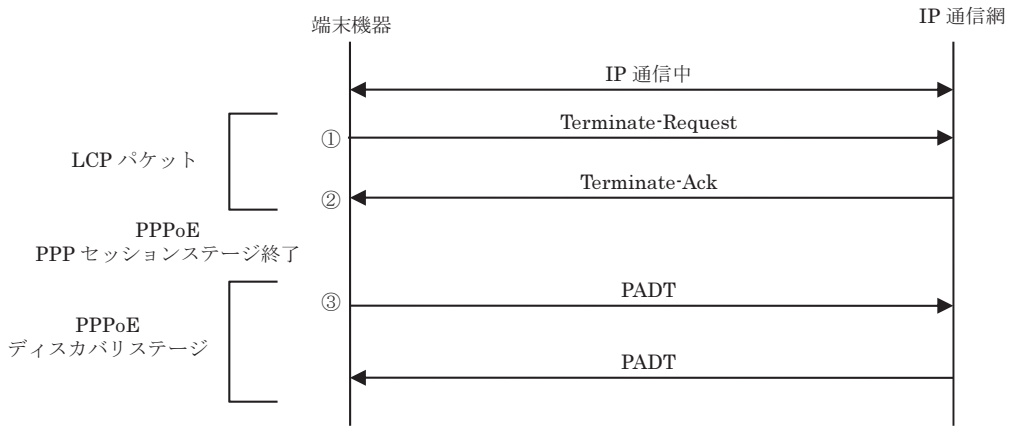


図 3.4 切断シーケンス（例）

① PPP セッションの開放を開始

② PPP セッションを開放

③ PPPoE セッションの開放を通知

3.2.6.4　　認証失敗シーケンス

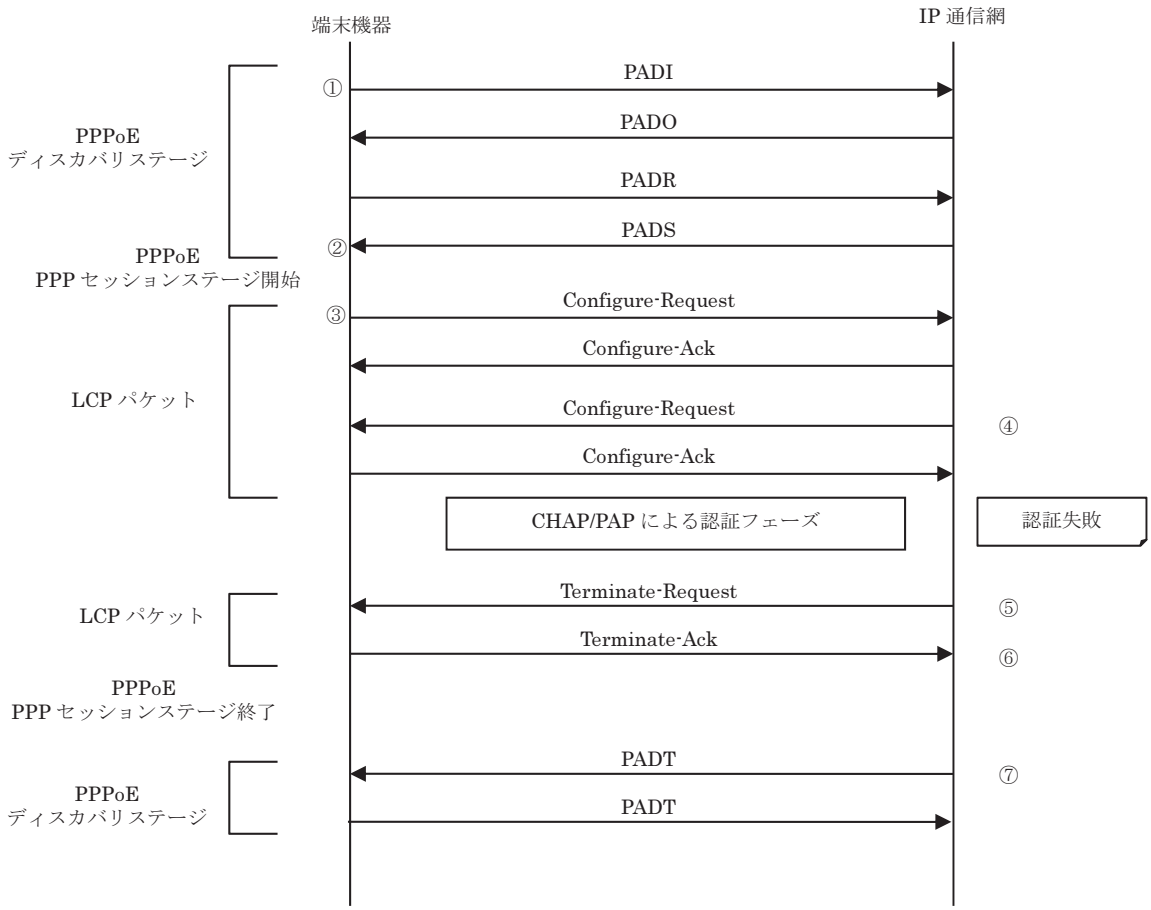


図 3.5　認証失敗シーケンス（例）

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 セッションの開放を開始

⑥ PPP セッションの開放

⑦ PPPoE セッションの開放を通知

3.2.6.5　　強制切断シーケンス

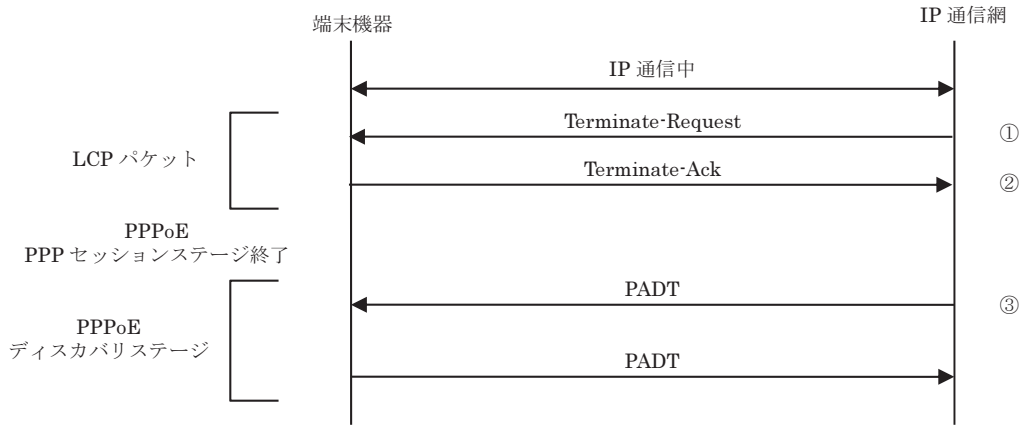


図 3.6　強制切断シーケンス（例）

① PPP セッションの開放を開始

② PPP セッションを開放

③ PPPoE セッションの開放を通知

4　付属資料

4.1　ONU（スロット式）の概要

本装置は、装置内部に端末機器を搭載することが可能なスロットを持った ONU です。装置内部の ONU 機能部と装置に搭載された端末機器は Ethernet により接続することが可能であり、装置に搭載された端末機器を動作させるための電源は本装置から供給することが可能です。以下に ONU(スロット式)の仕様および、端末機器に対する要求条件の概要を提示します。Enthernet により接続される ONU 機能部とのインタフェース仕様については、[2.2.1 インタフェース条件]に準じます。

4.1.1　インタフェース規定点

本装置では、図 4.1 に示すユーザ・網インタフェース（UNI）を規定します。

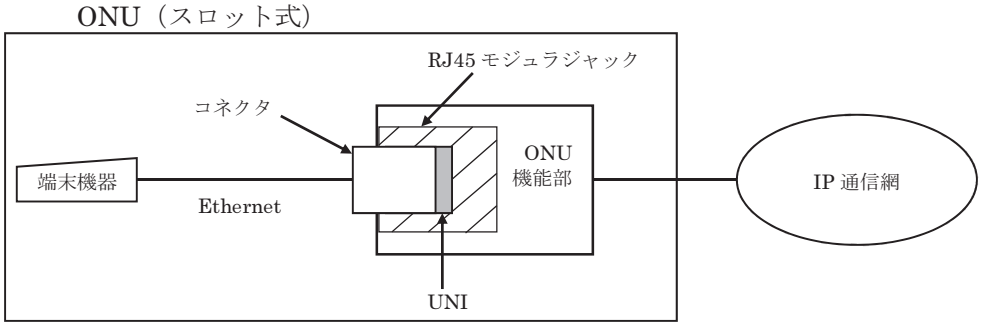


図 4.1　インタフェース規定点

4.1.2　　端末設備と電気通信回線設備の分界点

本装置の端末設備と電気通信回線設備との分界点について図 4.2 に示します。また、端末設備が必ず適合しなければならない技術的条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

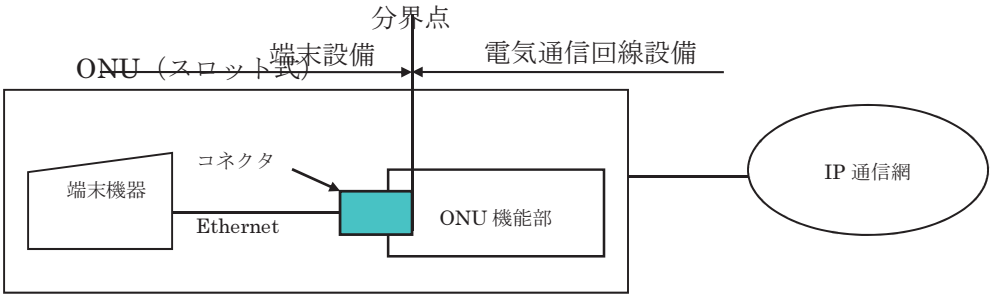


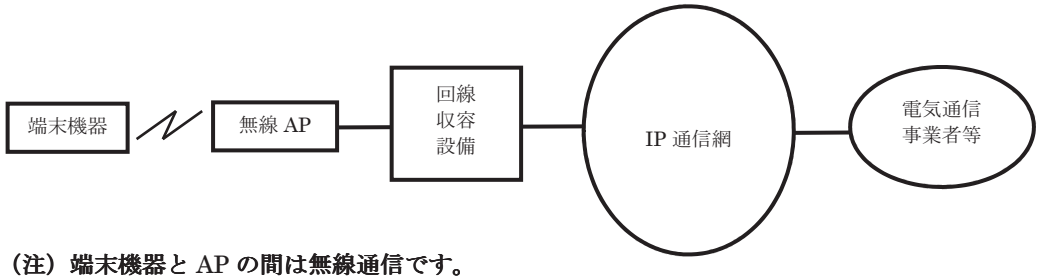
図 4.2　分界点

フレッツ 光 WiFi アクセス

1 フレッツ 光 WiFi アクセス概要

1.1 サービスの概要

フレッツ 光 WiFi アクセスは、ベストエフォート型の IP 通信サービスです。フレッツ 光 WiFi アクセスを利用する端末機器等（以下、端末機器）は、無線アクセスポイント（以下、無線 AP）に接続した後、電気通信事業者等と IP 通信網を介して IP 通信を行います。また、無線 AP ごとに、その装置を設置した共同住宅等における所有者等（その共同住宅等を所有又は管理等する者であって、当社が指定する者をいいます。）が指定する 1 つの電気通信事業者と接続が可能となります。フレッツ 光 WiFi アクセスの基本構成を図 1.1 に示します。



（注）端末機器と AP の間は無線通信です。

図 1.1 フレッツ 光 WiFi アクセスの基本構成

1.2 インタフェース規定点

フレッツ 光 WiFi アクセスでは、図 1.2 に示すユーザ・網インタフェース（UNI）を規定します。

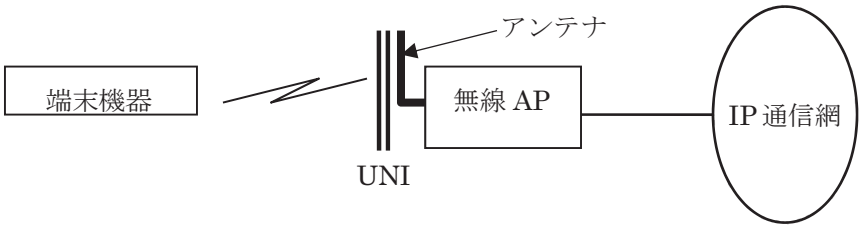


図 1.2 インタフェース規定点

1.3　端末設備と電気通信回線設備の分界点

端末設備と電気通信回線設備との分界点について図 1.3 に示します。

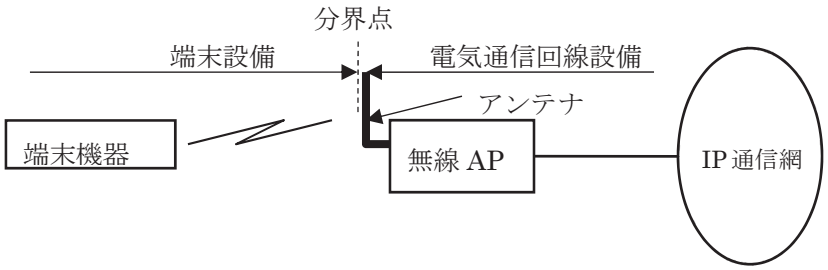


図 1.3 分界点

1.4　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 1.4 に示します。

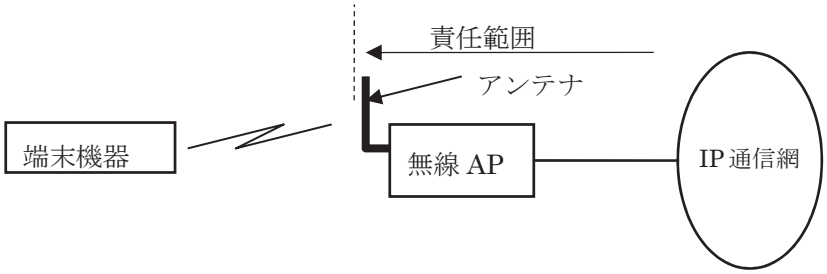


図 1.4 施工・保守上の責任範囲

2　ユーザ・網インタフェース仕様

2.1　プロトコル構成

プロトコル構成は、表 2.1 に示す OSI 参照モデルに則した階層構成となっています。

表 2.1　プロトコル構成

レイヤ		使用するプロトコル
7	アプリケーション	認証時の通信において以下のプロトコルを規定します。 DHCP： RFC2131 DNS： RFC1034,RFC1035,RFC1123,RFC2181,RFC2308,RFC2671,RFC2782 HTTP： RFC2616 TLS1.0： RFC2246 TLS1.2： RFC5246 ※その他通信においては、特に規定はありません。
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, RFC1918
2	データリンク	MAC： IEEE802.11 IEEE802.11i
1	物理	IEEE802.11b準拠 IEEE802.11g準拠 IEEE802.11n準拠 ARIB STD-T66（2.4GHz帯）

2.2 物理レイヤ（レイヤ 1）仕様

フレッツ 光 WiFi アクセスがサポートするレイヤ 1 インタフェース条件は、IEEE802.11b（Wi-Fi 認定）、IEEE802.11g（Wi-Fi 認定）及び IEEE802.11n（Wi-Fi 認定）とします。

表 2.2 レイヤ 1 仕様

項目		規格
周波数帯域	802.11b	2,400 ～ 2,483.5MHz
	802.11g	2,400 ～ 2,483.5MHz
	802.11n	2,400 ～ 2,483.5MHz
使用チャネル	802.11b	1 ～ 13CHのいずれかを使用
	802.11g	1 ～ 13CHのいずれかを使用
	802.11n	1 ～ 13CHのいずれかを使用（2.4GHz帯）
伝送速度［Mbps］(注)	802.11b	最大11Mbps
	802.11g	最大54Mbps
	802.11n	【20MHz】最大144.4Mbps（2ストリーム）、最大72.2Mbps（1ストリーム） 【40MHz】最大300Mbps（2ストリーム）、150Mbps（1ストリーム）
変調方式	802.11b	DSSS方式
	802.11g	OFDM方式
	802.11n	OFDM方式
メディアアクセス制御		CSMA/CA

（注）無線回線状況等により伝送速度が変化します。また、この伝送速度を保証するものではありません。

2.3 データリンクレイヤ（レイヤ 2）仕様

レイヤ 2 では、IEEE 802.11 に規定されている MAC を使用します。MAC の詳細については IEEE 802.11 を参照してください。また、SSID と WPA/WPA2-PSK キーの設定条件を表 2.3 に示します。

表 2.3 SSID と WPA/WPA2-PSK キーの設定条件

設定項目	設定条件	備考
SSID	使用します	設定値は契約者に個別通知
WPA/WPA2-PSKキー	使用します	設定値は契約者に個別通知

2.4 ネットワークレイヤ（レイヤ 3）仕様

レイヤ 3 では、RFC791 に規定されている IPv4 を使用します。IPv4 についての詳細は RFC791 を参照してください。

また、端末機器の IP アドレスとして利用可能な IPv4 アドレスは、IP 通信網に接続する際に、IP 通信網から割り当てられた RFC1918 で規定されているクラス A のプライベートの IP アドレスのみです。その他の IP アドレスを利用する場合、動作は保証しません。

2.5 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、DHCP、DNS 、HTTP、TLS1.0、TLS1.2 を認証時の通信において規定します。その他通信においては、特に規定はありません。

2.5.1 DNS

IPv4 に対応した端末機器は、IP 通信網経由でアクセス可能な DNS サーバ間で、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 2.4 に示します。各仕様に関する詳細は各 RFC を参照してください。

表 2.4　DNS 規定

参考文献	タイトル	備考
RFC1034	Domain names -Concepts and facilities	DNSについて規定
RFC1035	Domain names -implementation and specification	DNSについて規定
RFC1123	Requirements for Internet Hosts - Application and Support	DNSの実装について規定
RFC2181	Clarifications to the DNS Specification	DNSについて規定
RFC2308	Negative Caching of DNS Queries (DNS NCACHE)	ネガティブキャッシュについて規定
RFC2671	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	A DNS RR for specifying the location of services	SRV レコードを規定

2.5.2　HTTP

IPv4 に対応した端末機器は、通信するプロトコルとして HTTP を使用することが可能です。HTTP を利用する場合に準拠する規定は RFC2616 となります。TLS1.0 を利用する場合に準拠する規定は RFC2246 となります。TLS1.2 を利用する場合に準拠する規定は RFC5246 となります。各仕様に関する詳細は各 RFC を参照してください。

HTTP の通信先には、認証サーバがあり端末機器が電気通信事業者側への通信をするための認証を行います。

表 2.5 認証サーバへの接続条件

項番	項目名	内容
1	レイヤ３	IPv4
2	上位レイヤ	HTTP、TLS1.0、TLS1.2

2.5.3 制限事項

フレッツ 光 WiFi アクセスでは以下の制限事項があります。

(1) 端末機器の IP アドレスとして、IPv6 アドレスを利用した通信は利用できません。

(2) 端末機器から PPPoE 接続を行うことができません。

(3) 端末機器の IP アドレスは IP 通信網から払い出したプライベートアドレスとなるため、グローバルアドレスを用いて電気通信事業者を介する IP 通信では端末機器に接続ができません。

3 フレッツ 光 WiFi アクセスの通信シーケンス

フレッツ 光 WiFi アクセスを利用する場合の通信シーケンスについて、接続および切断手順等の具体的な例について説明します。

3.1 接続シーケンス

3.1.1 無線区間における接続シーケンス

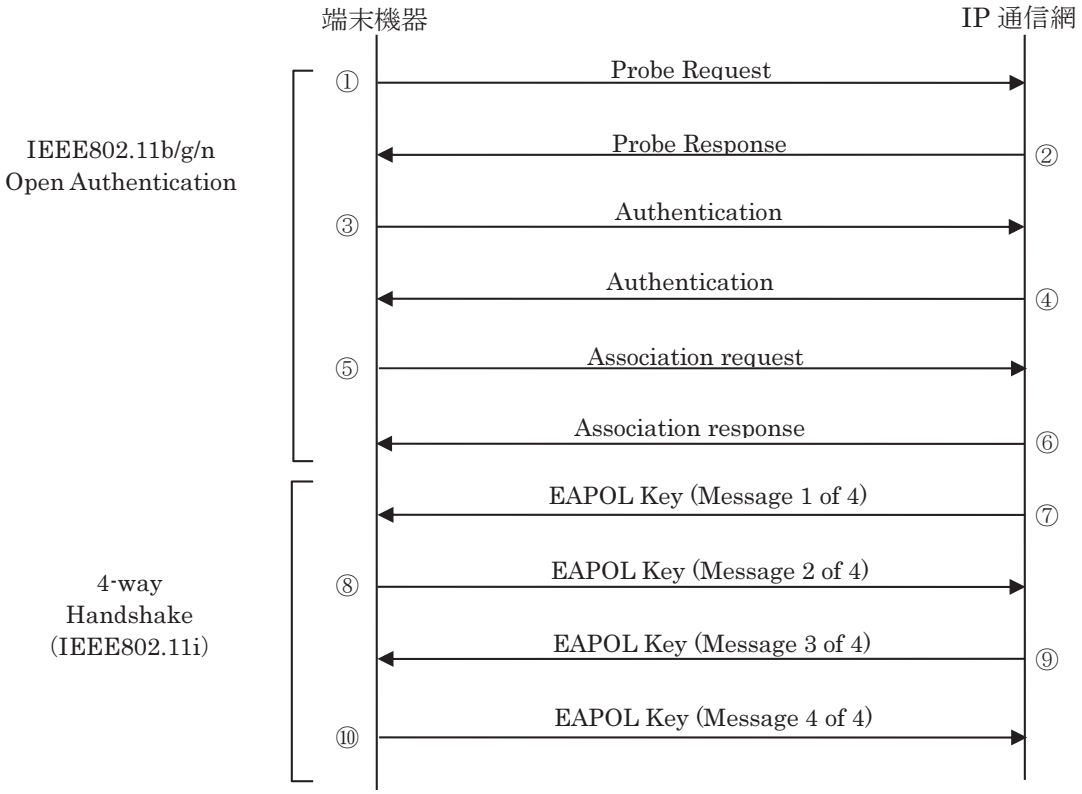


図 3.1 接続シーケンス（例）

［説明］

① 端末機器が接続する SSID とサポートするパラメータを無線 AP に送付します。

② 無線 AP がサポートするパラメータを、端末機器に送付します。

③ 端末機器がオープンシステム認証を要求します。

④ 無線 AP がオープンシステム認証要求に応答します。

⑤　端末機器がアソシエーション要求を送信します。

⑥　無線 AP がアソシエーション ID を応答します。

⑦　無線 AP がナンスを送信します。

⑧　端末機器がナンスを送信します。

⑨　無線 AP がペアキーの設定メッセージとグループキーを送信します。

⑩　端末機器が応答します。

3.2　接続失敗シーケンス

3.2.1　無線区間における接続失敗シーケンス

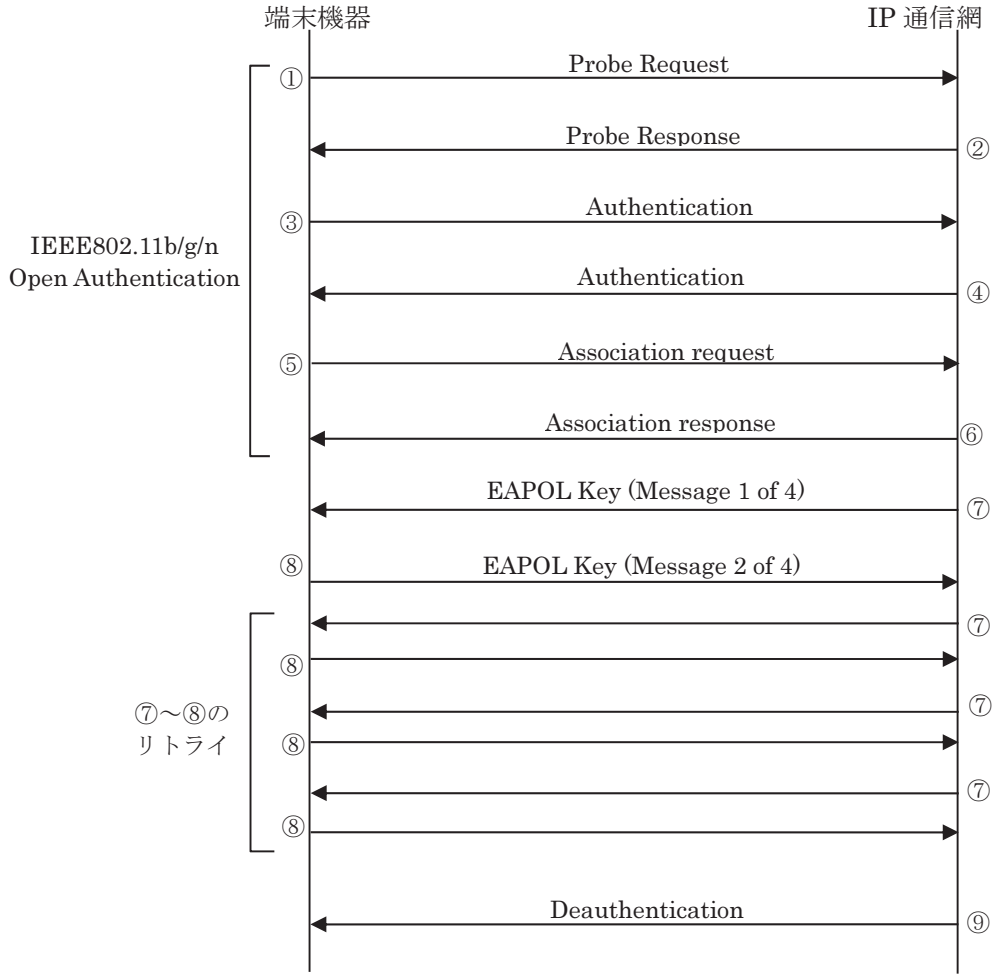


図 3.2　接続失敗シーケンス（例）

［説明］

① 端末機器が接続する SSID とサポートするパラメータを無線 AP に送付します。

② 無線 AP がサポートするパラメータを、端末機器に送付します。

③ 端末機器がオープンシステム認証を要求します。

④ 無線 AP がオープンシステム認証要求に応答します。

⑤ 端末機器がアソシエーション要求を送信します。

⑥ 無線 AP がアソシエーション ID を応答します。

⑦ 無線 AP がナンスを送信します。

⑧ 端末機器がナンスを送信します。(端末に設定された事前共有キーが誤っている場合、本ステップで失敗します)

⑨ 無線 AP が端末機器に切断を通知します。

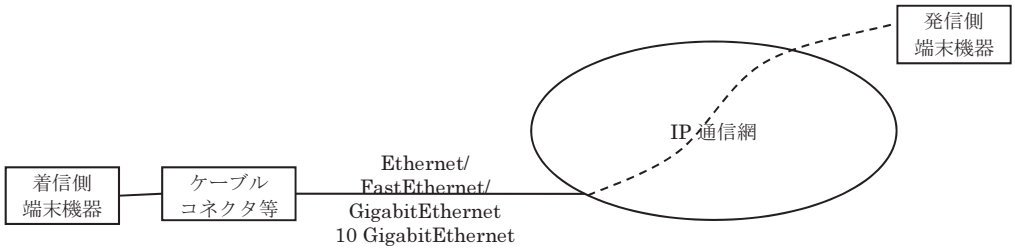
フレッツ・ＶＰＮ ゲート

1　フレッツ・ＶＰＮゲートの概要

1.1　サービスの概要

フレッツ・ＶＰＮ ゲートは、LAN やサーバ機器を IP 通信網に接続し、フレッツ・ISDN、フレッツ・ADSL、B フレッツ、フレッツ・光プレミアムおよびフレッツ 光ネクストを利用する端末機器との IPv4 通信を提供するサービスです。以下、本資料では、フレッツ・ＶＰＮ ゲートを利用する LAN やサーバ機器等を着信側端末機器、フレッツ・ISDN、フレッツ・ADSL、B フレッツ、フレッツ・光プレミアムおよびフレッツ 光ネクストを利用する端末機器等を発信側端末機器と呼びます。フレッツ・ＶＰＮ ゲートの基本構成の例を図 1.1 に示します。

図 1.1　フレッツ・ＶＰＮ ゲートの基本構成



端末機器間の通信を開始するためには、発信側端末機器が発信した接続要求を認証する必要があります。認証処理は着信側端末機器で行う方式と、IP 通信網内で行う方式があります。着信側端末機器には IPv4 パケットを交換する機能が必要です。また、着信側端末機器で認証を行う場合、着信側端末機器は、接続要求に対して認証処理を行う機能が必要です。以下に、着信側端末機器で認証処理を行う場合の、端末機器間通信の開始から終了までの概要を示します。

(1)　発信側端末機器は、目的とする着信側端末機器に対する接続要求を、認証処理に必要な認証情報と一緒に IP 通信網に送信します。

(2)　IP 通信網は発信側端末機器の認証情報を、該当する着信側端末機器へ送信します。

(3)　着信側端末機器は受信した認証情報をもとに発信側端末機器に対する認証を行い、その結果を認証結果として IP 通信網へ送信します。

(4)　認証結果が認証成功の場合、IP 通信網は接続要求を行った発信側端末機器と着信側端末機器を IPv4 通信が可能となるよう接続します。

(5)　発信側端末機器からの切断要求により、IP 通信網は着信側端末機器に発信側端末機器の切断情報を送信し、端末機器間の接続を切断します。

(6)　(4)で認証結果が認証失敗の場合、接続を要求した発信側端末機器に対し IP 通信網が接続要求を拒否し、端末機器間の IPv4 通信は開始しません。

以下、本資料では(2)、(3)及び(5)、(6)を認証関連通信と呼びます。

IP 通信網内で認証処理を行う場合は、着信側端末機器と IP 通信網間での認証関連通信は行われません。

認証関連通信についての詳細は[5 認証関連通信]を参照してください。また、発信側端末機器からの接続要求についての詳細は該当するサービスの技術参考資料を参照してください。

1.2 サービス品目

フレッツ・ＶＰＮ ゲートのサービス品目とサービス品目におけるインタフェースの条件を表 1.1 に示します。本資料では、フレッツ・ＶＰＮ ゲートのサービス品目を、インタフェース条件から表 1.1 に示す 4 つのタイプに分類して説明します。

表 1.1 フレッツ・ＶＰＮ ゲートのサービス品目とインタフェース条件

タイプ	サービス品目		インタフェース条件
Ethernet	10Mb/s	局内接続型	IEEE 802.3-2005 10BASE-T 準拠
		局外接続型	
FastEthernet	100Mb/s	局内接続型	IEEE 802.3-2005 100BASE-FX/TX 準拠
		局外接続型	IEEE 802.3-2005 100BASE-TX 準拠
Gigabit Ethernet	1Gb/s	局内接続型	IEEE 802.3-2005 1000BASE-LX 準拠
		収容エリア内接続型	
10 Gigabit Ethernet	10Gb/s	局内接続型	IEEE 802.3-2005 10GBASE-LR 準拠
		収容エリア内接続型	

1.3　インタフェース規定点

1.3.1　Ethernet/FastEthernet タイプのインタフェース規定点

Ethernet/FastEthernet タイプでは、図 1.2 に示す、ユーザ･網インタフェース（UNI）を規定します。

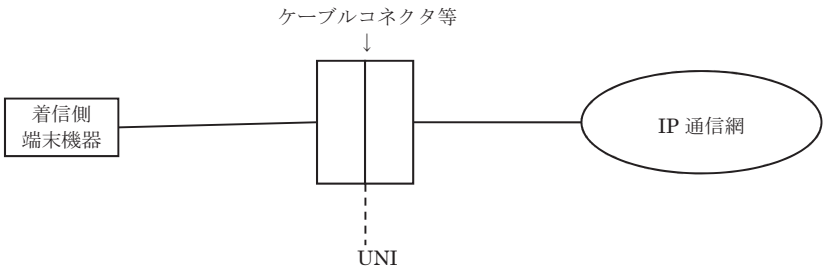


図 1.2　Ethernet/FastEthernet タイプのインタフェース規定点

1.3.1.1　　ユーザ･網インタフェース（UNI）

ユーザ･網インタフェース（UNI）の規定点を図 1.3、図 1.4 に示します。インタフェースの詳細については、[2 Ethernet/FastEthernet タイプのユーザ・網インタフェース仕様]を参照してください。

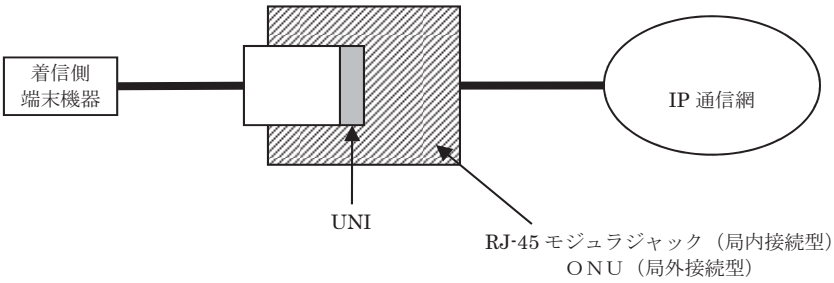


図 1.3　Ethernet/FastEthernet タイプのインタフェース規定点

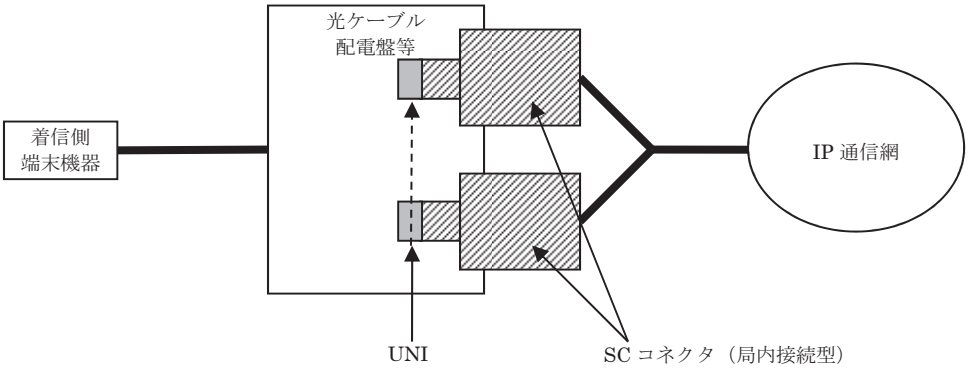


図 1.4　FastEthernet タイプのインタフェース規定点

1.3.2 GigabitEthernet/10 GigabitEthernet タイプのインタフェース規定点

GigabitEthernet/10 GigabitEthernet タイプでは、図 1.5 に示す、ユーザ･網インタフェース（UNI）を規定します。

インタフェースの詳細は、GigabitEthernet タイプについては[3 GigabitEthernet タイプのユーザ・網インタフェース仕様]を、10 GigabitEthernet タイプについては[4 10 GigabitEthernet タイプのユーザ・網インタフェース仕様]をそれぞれ参照してください。

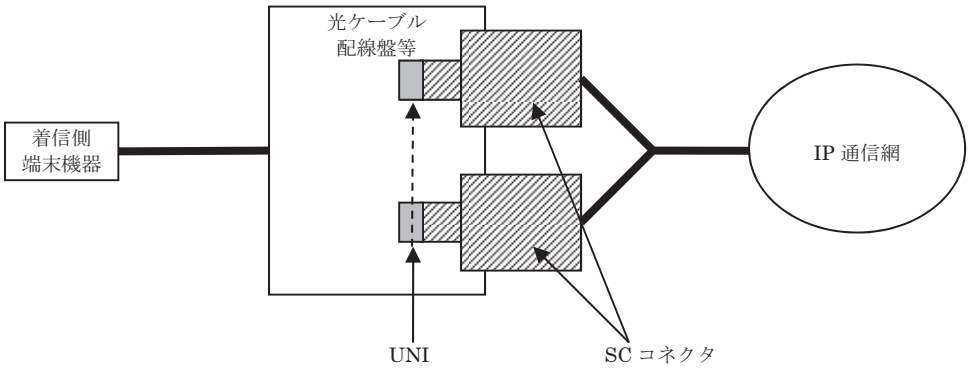


図 1.5 GigabitEthernet/10 GigabitEthernet タイプのインタフェース規定点

1.4　端末設備と電気通信回線設備の分界点

1.4.1　Ethernet/FastEthernet タイプの分界点

Ethernet/FastEthernet タイプにおける、端末設備と電気通信回線設備との分界点を図 1.6 に示します。

また、端末設備が必ず適合しなければならない技術的条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

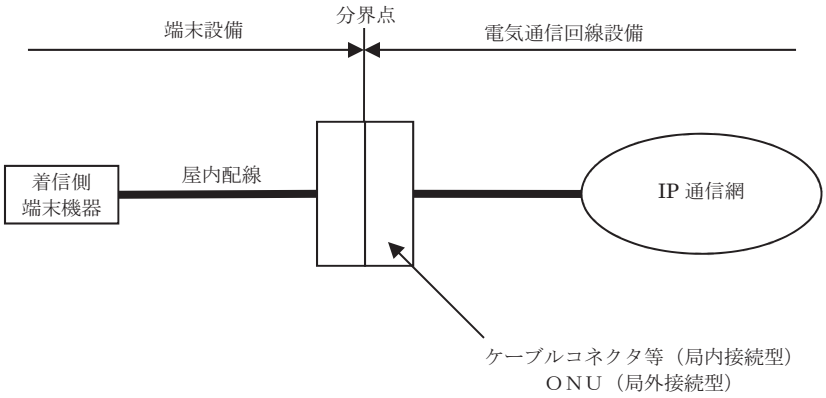


図 1.6　Ethernet/FastEthernet タイプの分界点

1.4.2　GigabitEthernet/10 GigabitEthernet タイプの分界点

GigabitEthernet/10 GigabitEthernet タイプにおける、端末設備と電気通信回線設備との分界点を図 1.7 に示します。

また、端末設備が必ず適合しなければならない技術的条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

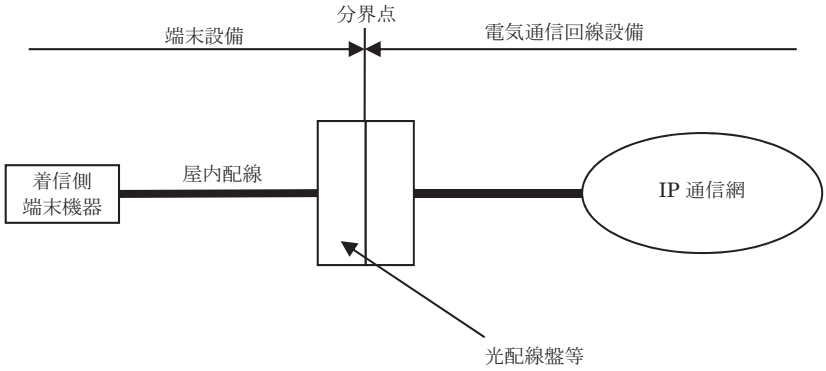


図 1.7　GigabitEthernet/10 GigabitEthernet タイプの分界点

1.5　施工・保守上の責任範囲

1.5.1　Ethernet/FastEthernet タイプの施工・保守上の責任範囲

Ethernet/FastEthernet タイプにおける施工・保守上の責任範囲を、図 1.8 に示します。

施工・保守上の責任範囲の分界点は図 1.9、図 1.10 に示すケーブルコネクタの接続点で、斜線部より IP 通信網側が責任範囲となります。

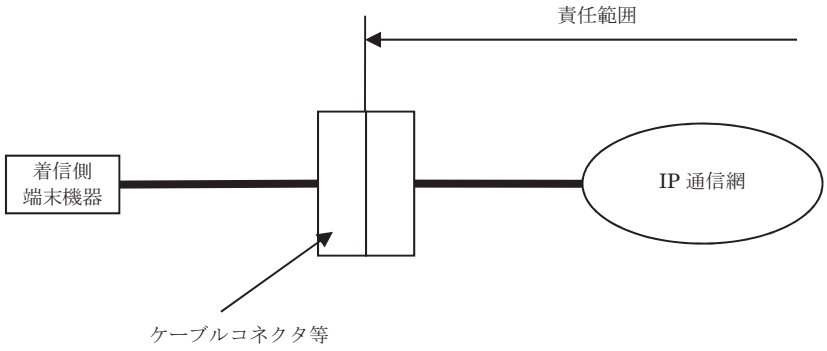


図 1.8　Ethernet/FastEthernet タイプにおける施工・保守上の責任範囲

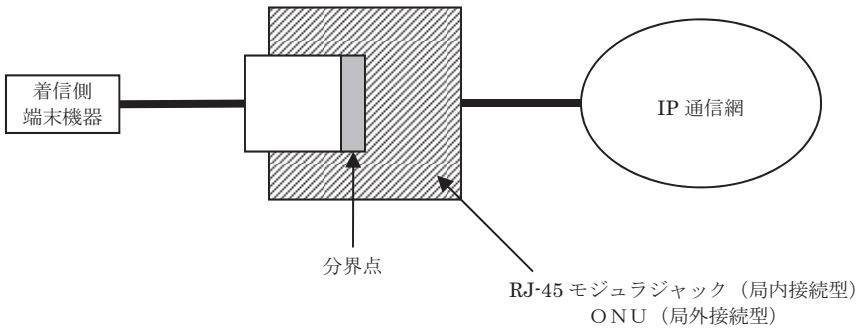


図 1.9　Ethernet/FastEthernet タイプにおける施工・保守上の責任範囲分界点

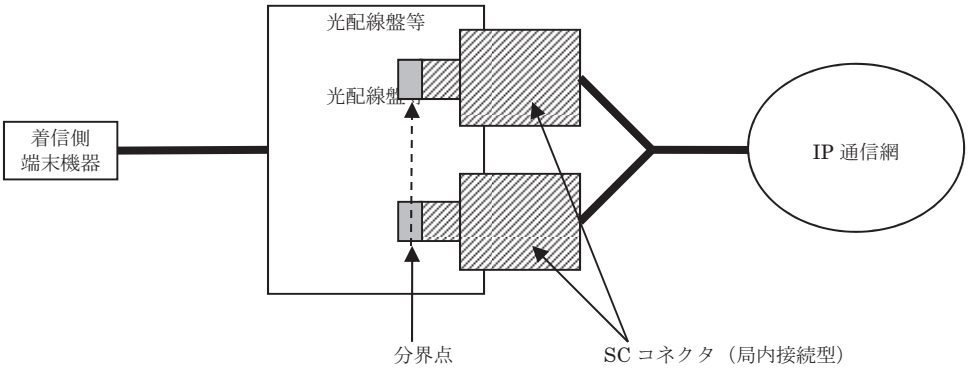


図 1.10　FastEthernet タイプにおける施工・保守上の責任範囲分界点

1.5.2　GigabitEthernet/10 GigabitEthernet タイプの施工・保守上の責任範囲

GigabitEthernet/10 GigabitEthernet タイプにおける施工・保守上の責任範囲を、図 1.11、図 1.13 に示します。

施工・保守上の責任範囲は契約条件によって異なります。

1.5.2.1　局内接続型の施工・保守上の責任範囲

局内接続型における施工・保守上の責任範囲を、図 1.11 に示します。

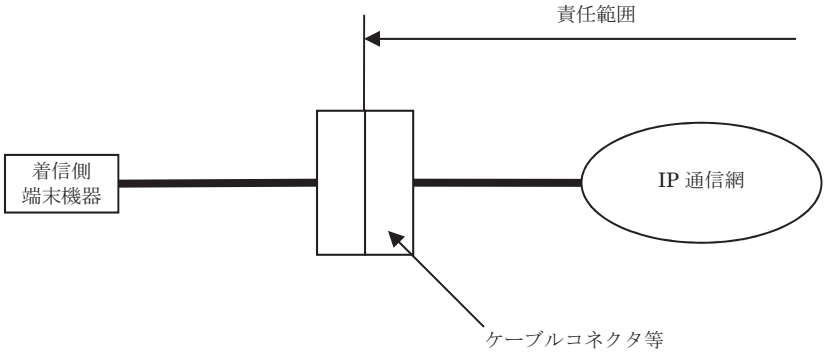


図 1.11　GigabitEthernet/10 GigabitEthernet タイプにおける施工・保守上の責任範囲

施工・保守上の責任範囲の分界点は図 1.12 に示す接続点で、斜線部より IP 通信網側が責任範囲となります。

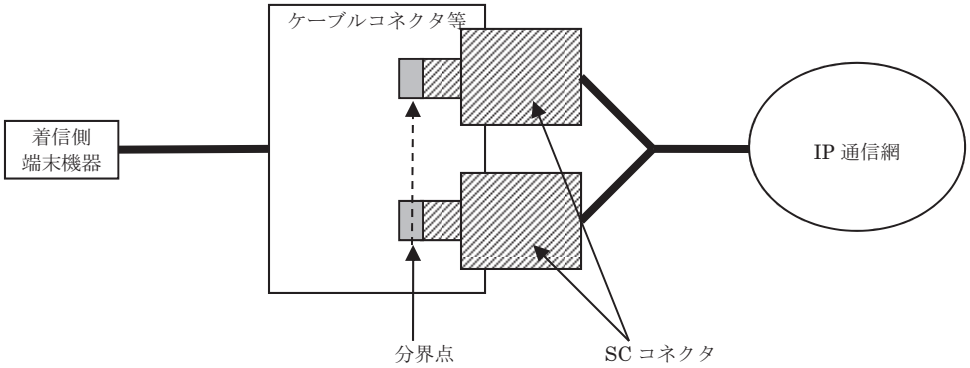
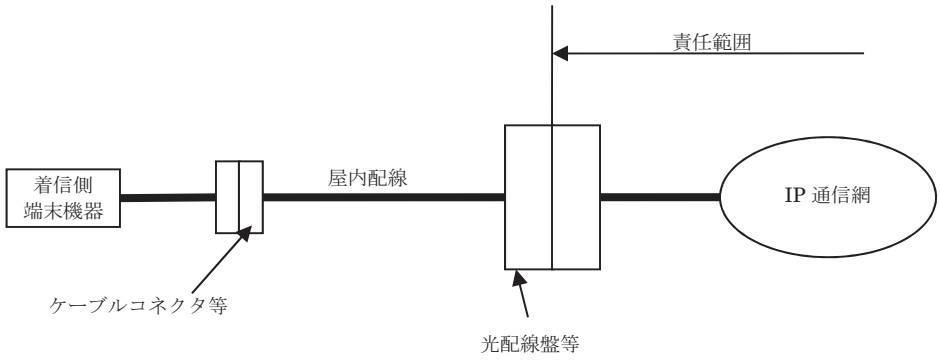


図 1.12　GigabitEthernet/10 GigabitEthernet タイプにおける施工・保守上の責任範囲分界点

1.5.2.2　収容エリア内接続型の施工・保守上の責任範囲

収容エリア内接続型における施工・保守上の責任範囲を、図 1.13 に示します。

(a) 弊社が光配線盤等までの光ファイバを提供する場合



(b) 弊社が屋内配線までを提供する場合

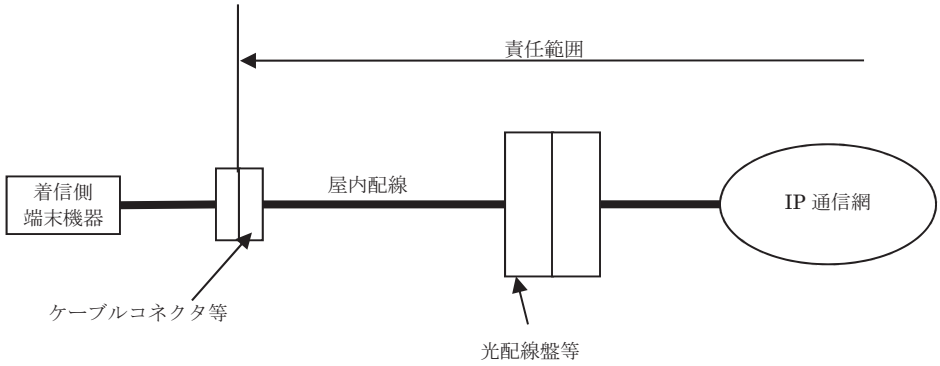


図 1.13　GigabitEthernet/10 GigabitEthernet タイプにおける施工・保守上の責任範囲

施工・保守上の責任範囲の分界点は図 1.14 に示す接続点で、斜線部より IP 通信網側が責任範囲となります。

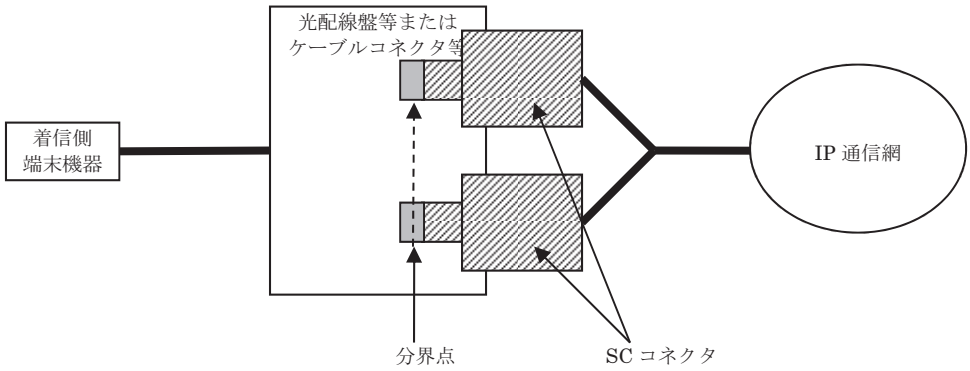


図 1.14　GigabitEthernet/10 GigabitEthernet タイプにおける施工・保守上の責任範囲分界点

2 Ethernet/FastEthernet タイプのユーザ・網インタフェース仕様

2.1 プロトコル構成

Ethernet/FastEthernet タイプのユーザ・網インタフェースのプロトコル構成を、OSI 参照モデルに則した階層構成で表 2.1 に示します。

IP 通信網と着信側端末機器との IPv4 通信については、レイヤ 1～3 のプロトコルについて規定します。また、着信側端末機器で認証処理を行う場合、IP 通信網と着信側端末機器との認証関連通信については、レイヤ 1～7 のプロトコルについて規定します。

表 2.1 プロトコル構成

レイヤ		規定するプロトコル	
7	アプリケーション	RFC2865（RADIUS） RFC2866（RADIUS Accounting）	
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	RFC791（IPv4） RFC792（ICMPv4）	
2	データリンク	RFC826（ARP） IEEE 802.3-2005 MAC 準拠	
1	物理	Ethernet	IEEE 802.3-2005 10BASE-T 準拠
		FastEthernet	IEEE 802.3-2005 100BASE-FX/TX 準拠

2.2　　レイヤ 1 仕様

レイヤ 1 では、IEEE 802.3-2005 に規定されている 10BASE-T または 100BASE-FX/TX を使用し、10Mb/s または 100Mb/s の伝送速度でベースバンド信号の全二重固定の通信を行います。

詳細については、IEEE 802.3-2005 を参照してください。

2.2.1　　10Mb/s 品目のレイヤ 1 仕様

10Mb/s 品目のレイヤ 1 では、IEEE 802.3-2005 に規定されている 10BASE-T を使用し、10Mb/s の伝送速度でベースバンド信号の全二重固定の通信を行います。

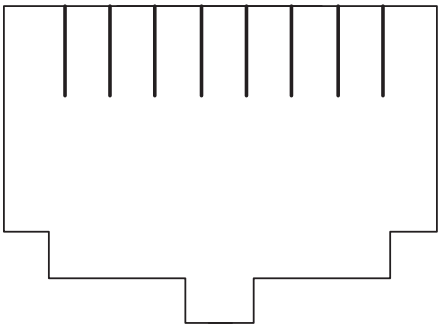
詳細については、IEEE 802.3-2005 を参照してください。

2.2.1.1　　インタフェース条件

10Mb/s 品目で提供するユーザ・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 2.1 に示します。

RJ-45 ポート挿入面

ピン番号　1　2　3　4　5　6　7　8



	記号	信号方向		ピン番号
		端末機器	IP 通信網	
受信	RD(+)	←		1
	RD(−)	←		2
送信	TD(+)	→		3
	TD(−)	→		6

※ピン番号 4、5、7、8 は使用しません

図 2.1　挿入面から見た RJ-45 ポートのピン配置

2.2.1.2 10BASE-T の適用ケーブル条件

モジュラジャックと接続する着信側端末機器等との配線は、2 対の非シールドより対線ケーブル（EIA/TIA-568 標準 UTP ケーブル カテゴリ 3 以上）を使用します。また、配線状況によりモジュラジャックと端末機器間のケーブルの最大長は、IEEE 802.3-2005 に規定されている 100m よりも短いものとなります。

2.2.2 100Mb/s 品目のレイヤ 1 仕様

100Mb/s 品目のレイヤ 1 では、IEEE 802.3-2005 に規定されている 100BASE-FX/TX を使用し、100Mb/s の伝送速度でベースバンド信号の全二重固定の通信を行います。

詳細については、IEEE 802.3-2005 を参照してください。

2.2.2.1 インタフェース条件

100Mb/s 品目で提供するユーザ･網インタフェースは､100BASE-FX については 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。(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。)

100BASE-TX については 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 2.1 に示します。

2.2.2.2 100BASE-TX の適応ケーブル条件

モジュラジャックと接続する着信側端末機器等との配線は、2 対の非シールドより対線ケーブル（EIA/TIA-568 標準 UTP ケーブル カテゴリ 5 以上）を使用します。また、配線状況によりモジュラジャックと端末機器間のケーブルの最大長は、IEEE 802.3-2005 に規定されている 100m よりも短いものとなります。

2.3 レイヤ 2 仕様

レイヤ 2 では、IEEE 802.3-2005 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。

MAC についての詳細は IEEE 802.3-2005 を、ARP についての詳細は RFC826 を参照してください。

2.4 レイヤ 3 仕様

レイヤ 3 では、RFC791 に規定されている IPv4 を使用します。IPv4 のサブセットとして RFC792 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 についての詳細は RFC791 を、ICMPv4 についての詳細は RFC792 を参照してください。

2.4.1 IP アドレス

フレッツ・ＶＰＮ ゲートでは、RFC1700 で規定されているクラス D、クラス E の IPv4 アドレスをサポートしません。RFC1918 で規定されているプライベートアドレスは使用可能です。

IPv4 アドレスについての詳細は RFC1700 を、プライベートアドレスについての詳細は RFC1918 を参照してください。

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り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。

2.4.2 接続用 IP アドレス

着信側端末機器と IP 通信網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。

着信側端末機器と IP 通信網間で IPv4 通信を行うために、着信側端末機器の IP 通信網を接続するインタフェース、及び IP 通信網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。

2.4.3 ルーティング

IP 通信網と着信側端末機器間のルーティング方式はスタティックルーティングです。

2.4.4 最大転送単位（MTU）

IP 通信網内の MTU の値は 1454byte (注) です。MTU の値を越えるパケットを IP 通信網が受信した場合、IP 通信網内で分割転送が発生する場合があります。

（注）フレッツ・光プレミアム利用端末との通信について、IP 通信網内の MTU の値は 1438byte です。

2.5 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。

着信側端末機器で認証処理を行う場合、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。 IP 通信網内で認証処理を行う場合、上位レイヤ（レイヤ 4～7）についての規定は特にありません。

3　GigabitEthernet タイプのユーザ・網インタフェース仕様

3.1　プロトコル構成

GigabitEthernet タイプのユーザ・網インタフェースのプロトコル構成を、OSI 参照モデルに則した階層構成で表 3.1 に示します。

IP 通信網と着信側端末機器との IPv4 通信については、レイヤ 1～3 のプロトコルとルーティングプロトコルについて規定します。また、IP 通信網と着信側端末機器との認証関連通信については、レイヤ 1～7 のプロトコルについて規定します。

表 3.1　プロトコル構成

レイヤ		規定するプロトコル
7	アプリケーション	RFC2865（RADIUS） RFC2866（RADIUS Accounting）
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	RFC791（IPv4） RFC792（ICMPv4） RFC2453（RIP Version 2）（注 1） RFC1771（BGP-4）（注 1）
2	データリンク	RFC826（ARP） IEEE 802.3-2005 MAC 準拠
1	物理	IEEE 802.3-2005 1000BASE-LX 準拠

（注１）契約形態によっては使用できません。

3.2　レイヤ 1 仕様

レイヤ 1 では、IEEE 802.3-2005 に規定されている 1000BASE-LX を使用し、1Gb/s の伝送速度でベースバンド信号の通信を行います。固定または自動折衝機能(Auto Negotiation 機能)により、全二重の通信モードを利用可能です。

詳細については、IEEE 802.3-2005 を参照してください。

3.2.1　インタフェース条件

GigabitEthernet タイプで提供するユーザ・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。

3.3 レイヤ 2 仕様

レイヤ 2 では、IEEE802.3-2005 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。

MAC についての詳細は IEEE802.3-2005 を、ARP についての詳細は RFC826 を参照してください。

3.4 レイヤ 3 仕様

レイヤ 3 では、RFC791 に規定されている IPv4 を使用します。IPv4 のサブセットとして RFC792 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 についての詳細は RFC791 を、ICMPv4 についての詳細は RFC792 を参照してください。

3.4.1 IP アドレス

フレッツ・ＶＰＮ ゲートでは、RFC1700 で規定されているクラス D、クラス E の IPv4 アドレスをサポートしません。RFC1918 で規定されているプライベートアドレスは使用可能です。

IPv4 アドレスについての詳細は RFC1700 を、プライベートアドレスについての詳細は RFC1918 を参照してください。

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り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。

3.4.2 接続用 IP アドレス

着信側端末機器と IP 通信網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。

着信側端末機器と IP 通信網間で IPv4 通信を行うために、着信側端末機器の IP 通信網を接続するインタフェース、及び IP 通信網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。

3.4.3 ルーティング

IP 通信網と着信側端末機器間のルーティング方式は契約形態により異なります。契約形態と利用可能なルーティング方式を表 3.2 に示します。

表 3.2 契約形態と利用可能なルーティング方式

契約形態	利用可能なルーティング方式
シングルクラス	・スタティックルーティング

デュアルクラス	・スタティックルーティング または ・ダイナミックルーティング －RIP Version 2（RFC2453） －BGP-4（RFC1771）

3.4.4 最大転送単位（MTU）

IP 通信網内の MTU の値は 1454byte (注) です。MTU の値を越えるパケットを IP 通信網が受信した場合、IP 通信網内で分割転送が発生する場合があります。

（注）フレッツ・光プレミアム利用端末との通信について、IP 通信網内の MTU の値は 1438byte です。

3.5 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。

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。

3.6 デュアルクラスに関わる仕様

3.6.1 トラフィック制御方式

IP 通信網から着信側端末機器向けの通信におけるトラフィック制御方式として、Act-Act 方式及び Act-Standby 方式があります。トラフィック制御方式の動作を表 3.3 に示します。

表 3.3 トラフィック制御方式の動作

トラフィック制御方式	動作
Act-Act 方式	・正常通信時は、両方の回線を利用して通信を行う。 ・一方の回線の回線障害発生時には、自動的にもう一方の回線に切り替え、通信を行う。 ・回線障害回復時には、自動的に回線の切り戻しを行い、正常通信時の動作に復旧する。
Act-Standby 方式	・正常通信時は、一方の回線（現用回線）のみを利用して通信を行う。 ・現用回線の回線障害発生時には、自動的にもう一方の回線（待機回線）に切り替え、通信を行う。 ・現用回線の回線障害回復時には、自動的に回線の切り戻しを行い、正常通信時の動作に復旧する。

3.6.2　　回線障害発生、回線障害回復検知方法

回線障害発生及び回線障害回復の検知を行う方式は、ルーティング方式により異なります。ルーティング方式と検知方式の関係を表 3.4 に示します。

なお、回線切り替え動作時、及び回線切り戻し動作時には、IP 通信網を介した通信ができない場合があります。

表 3.4　ルーティング方式と検知方式

ルーティング方式	検知方式
スタティックルーティング	・IP 通信網と着信側端末機器間のリンクダウンにより回線障害発生を検知。 ･IP 通信網と着信側端末機器間のリンクアップにより回線障害回復を検知。
ダイナミックルーティング	・IP 通信網と着信側端末機器間のリンクダウン、またはダイナミックルーティングの経路情報受信停止により回線障害発生を検知。 ・IP 通信網と着信側端末機器間のリンクアップ、且つ、ダイナミックルーティングの経路情報受信再開により回線障害回復を検知。

3.6.3　　ルーティングに関する主な条件

3.6.3.1　　RIP Version 2 (RFC2453) を利用する場合

ルーティング方式として表 3.2 における RIP Version 2 (RFC2453) を利用する場合の主な条件は以下のとおりです。

①着信側端末機器と IP 通信網の間のルーティング情報の交換時には、RFC4822 記載の RIP Version 2 MD5 Authentication を利用します。

②Authentication Type の値には、「Keyed Message Digest (3)」を利用します。

③着信側端末機器は IP 通信網に対して、デフォルトルートを通知する必要があります。

④IP 通信網から着信側端末機器向けに送信するルーティング情報のメトリック値は、トラフィック制御方式により異なります。Act-Act 方式の場合は、両方の回線を同値に設定し送信します。Act-Standby 方式の場合は、現用回線を優先した値に設定し送信します。

RIP Version 2 についての詳細は RFC2453 を参照してください。

3.6.3.2 BGP-4(RFC1771) を利用する場合

ルーティング方式として表 3.2 における BGP-4 (RFC1771) を利用する場合の主な条件は以下のとおりです。

①RFC1771 の 4.2 項における Option Parameters の項において Parameter Type の値に「1」を使用できません。

②RFC1771 の 4.2 項における Hold Time の推奨値は 180 秒です。

③RFC1771 の 4.4 項における KEEPALIVE Message の送信間隔の推奨値は 60 秒です。

④RFC1771 の 5 項における Optional attributes は使用できません。

⑤着信側端末機器において、RFC1771 の 5.1.2 項における AS_PATH は両方の回線を同値に設定する必要があります。

⑥IP 通信網から着信側端末機器向けに送信する RFC1771 の 5.1.4 項における MULTI_EXIT_DISC の値は、トラフィック制御方式により異なります。Act-Act 方式の場合は、両方の回線を同値に設定し送信します。Act-Standby 方式の場合は、現用回線を優先した値に設定し送信します。

⑦RFC1771 の 5.1.5 項における LOCAL_PREF は IP 通信網では設定しません。

⑧着信側端末機器は IP 通信網に対して、デフォルトルートを通知する必要があります。

BGP-4 についての詳細は RFC1771 を参照してください。

4　10 GigabitEthernet タイプのユーザ・網インターフェース仕様

4.1　プロトコル構成

10 GigabitEthernet タイプのユーザ・網インタフェースのプロトコル構成を、OSI 参照モデルに則した階層構成で表 4.1 に示します。

IP 通信網と着信側端末機器との IPv4 通信については、レイヤ 1～3 のプロトコルとルーティングプロトコルについて規定します。また、IP 通信網と着信側端末機器との認証関連通信については、レイヤ 1～7 のプロトコルについて規定します。

表 4.1　プロトコル構成

レイヤ		規定するプロトコル
7	アプリケーション	RFC2865（RADIUS） RFC2866（RADIUS Accounting）
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	RFC791（IPv4） RFC792（ICMPv4） RFC1771（BGP-4）
2	データリンク	RFC826（ARP） IEEE 802.3-2005 MAC 準拠
1	物理	IEEE 802.3-2005 10GBASE-LR 準拠

4.2　レイヤ 1 仕様

レイヤ 1 では、IEEE 802.3-2005 に規定されている 10GBASE-LR を使用し、10Gb/s の伝送速度でベースバンド信号の全二重の通信を行います。

詳細については、IEEE 802.3-2005 を参照してください。

4.2.1　インタフェース条件

10 GigabitEthernet タイプで提供するユーザ・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。

4.3　レイヤ 2 仕様

レイヤ 2 では、IEEE802.3-2005 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。

MAC についての詳細は IEEE802.3-2005 を、ARP についての詳細は RFC826 を参照してください。

4.4 レイヤ 3 仕様

レイヤ 3 では、RFC1771 に規定されている BGP4、RFC791 に規定されている IPv4 を使用します。IPv4 のサブセットとして RFC792 に規定されている ICMPv4 の一部についてもサポートします。

BGP4 についての詳細は RFC1771 を、IPv4 についての詳細は RFC791 を、ICMPv4 についての詳細は RFC792 を参照してください。

4.4.1 IP アドレス

フレッツ・ＶＰＮ ゲートでは、RFC1700 で規定されているクラス D、クラス E の IPv4 アドレスをサポートしません。RFC1918 で規定されているプライベートアドレスは使用可能です。

IPv4 アドレスについての詳細は RFC1700 を、プライベートアドレスについての詳細は RFC1918 を参照してください。

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り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。

4.4.2 接続用 IP アドレス

着信側端末機器と IP 通信網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。

着信側端末機器と IP 通信網間で IPv4 通信を行うために、着信側端末機器の IP 通信網を接続するインタフェース、及び IP 通信網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。

4.4.3 ルーティング

IP 通信網と着信側端末機器間のルーティング方式はダイナミックルーティングです。RFC1771 で規定されている BGP4 を使用します。

BGP4 を使用する場合の主な条件は以下のとおりです。

①RFC1771 の 4.2 項における Option Parameters の項において、Parameter Type の値に「1」を使用できません。

②RFC1771 の 4.2 項における Hold Time の推奨値は 180 秒です。

③RFC1771 の 4.4 項における KEEPALIVE Message の送信間隔の推奨値は 60 秒です。

④RFC1771 の 5 項における Optional attributes は使用できません。

⑤着信側端末機器において、RFC1771 の 5.1.2 項における AS_PATH は両方の回線を同値に設定する必要があります。

⑥RFC1771 の 5.1.5 項における LOCAL_PREF は IP 通信網では設定しません。

⑦着信側端末機器は IP 通信網に対して、デフォルトルートを通知する必要があります。

BGP-4 についての詳細は RFC1771 を参照してください。

4.4.4 最大転送単位（MTU）

IP 通信網内の MTU の値は 1454byte です。MTU の値を越えるパケットを IP 通信網が受信した場合、IP 通信網内で分割転送が発生する場合があります。

4.5 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。

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

IP 通信網は RFC2865、及び RFC2866 に準拠した RADIUS クライアント（NAS）として動作します。発信側端末機器を認証するためには、着信側端末機器または端末設備において RFC2865(RADIUS)、RFC2866（RADIUS Accounting)に準拠した RADIUS サーバとしての機能が必要です。

RADIUS サーバ～RADIUS クライアント間の通信において、RADIUS サーバ側で用いるポート番号は、1645(RADIUS)、1646(RADIUS Accounting)または 1812(RADIUS)、1813(RADIUS Accounting)を使用します。

RADIUS サーバとしては、通常利用するプライマリサーバと、プライマリサーバが利用できないときに RADIUS サーバとして機能するセカンダリサーバを、それぞれに異なる IPv4 アドレスを付与して設置することができます。

（注 1）セカンダリサーバを設置した場合の、プライマリサーバからセカンダリサーバへの切り替え条件、並びにセカンダリサーバからプライマリサーバへの切り戻し条件については、[5.3 通信用タイマ] を参照してください。

（注 2）セカンダリサーバは最大 2 台まで設置できます。1 台目のセカンダリサーバから 2 台目のセカンダリサーバへの切り替え条件は、プライマリサーバから 1 台目のセカンダリサーバへの切り替え条件と同じです。

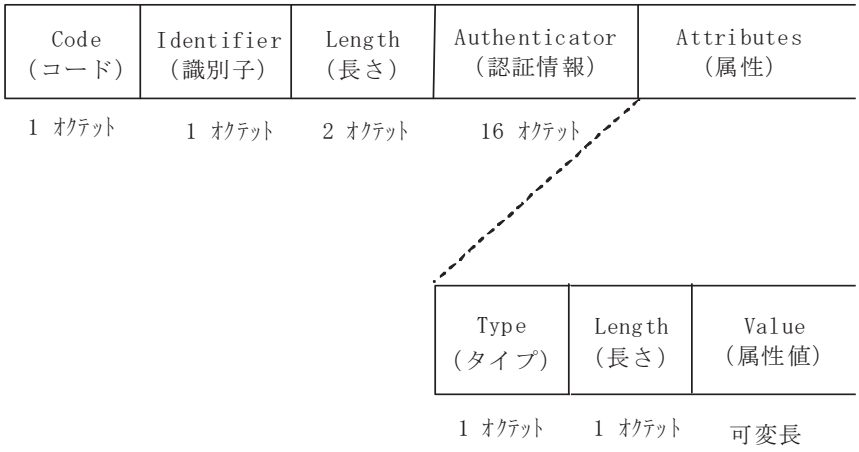
5.1　　パケットフォーマット

RADIUS サーバと IP 通信網の間で、送受信される認証関連通信のパケットフォーマットは RFC2865、及び RFC2866 に準拠します。以下、本資料では、これらの RFC に準拠した認証関連通信で用いられるパケットを認証関連通信パケットと呼びます。

パケットフォーマットを図 5.1 に示します。

使用する Attributes については、表 5.1 を参照してください。

表 5.1 に記述した以外の Attributes を使用した場合、IP 通信網での動作は保証しません。



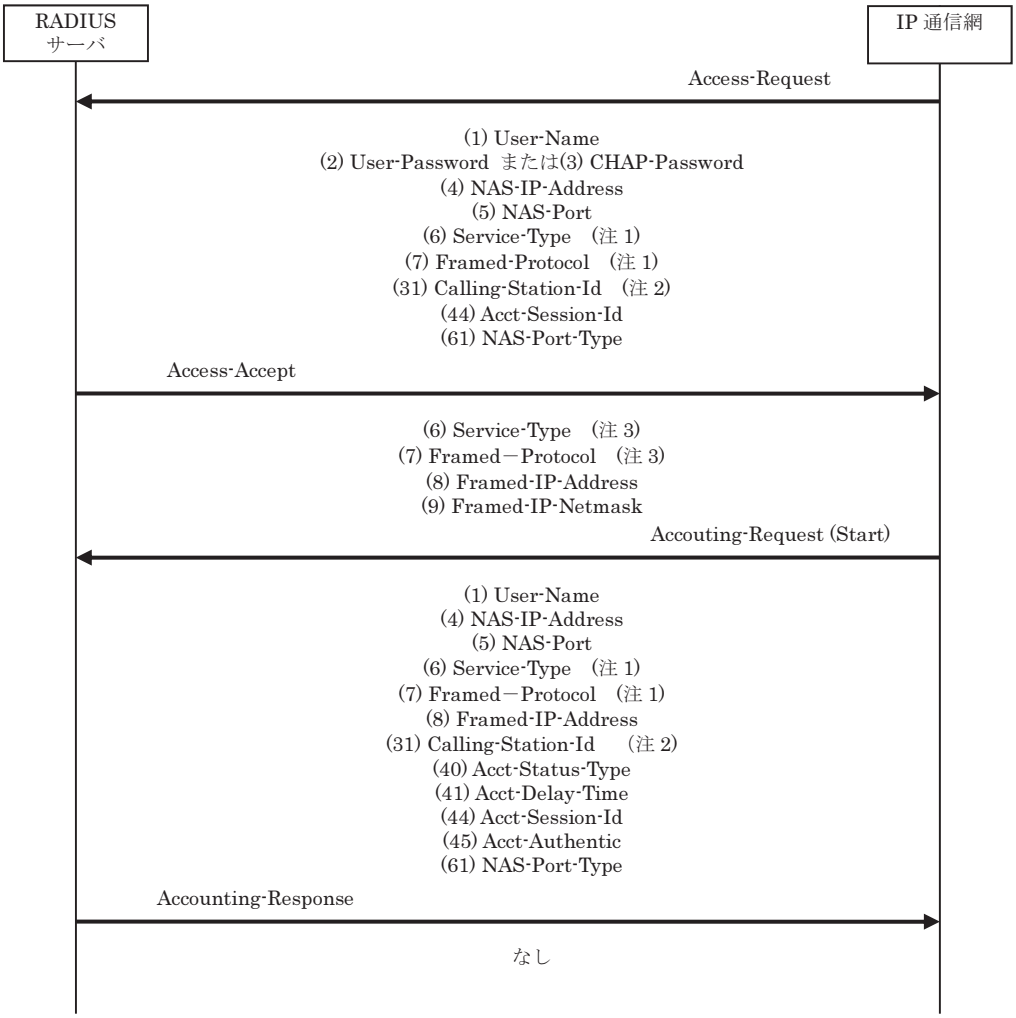
（注）パケットフォーマットについての詳細は RFC2865 及び、RFC2866 を参照してください。

図 5.1　認証関連通信パケットのパケットフォーマット

5.2　通信シーケンス例

IP 通信網と RADIUS サーバの間の通信シーケンス例を図 5.2～図 5.4 に示します。

5.2.1　　認証成功



（注 1）フレッツ・光プレミアム利用端末からの認証の場合は送出されません。

（注 2）回線情報転送機能を利用する場合において、フレッツ 光ネクスト及びフレッツ・ＩＳＤＮ利用端末からの認証の場合のみ IP 通信網から送出されます。ただし、フレッツ・ＩＳＤＮ利用端末からの認証の場合、発信者番号の非通知を設定している場合は送出されません。

（注 3）フレッツ・光プレミアム利用端末からの認証の場合は送出不要です。

() は Attributes の Type を示しています。

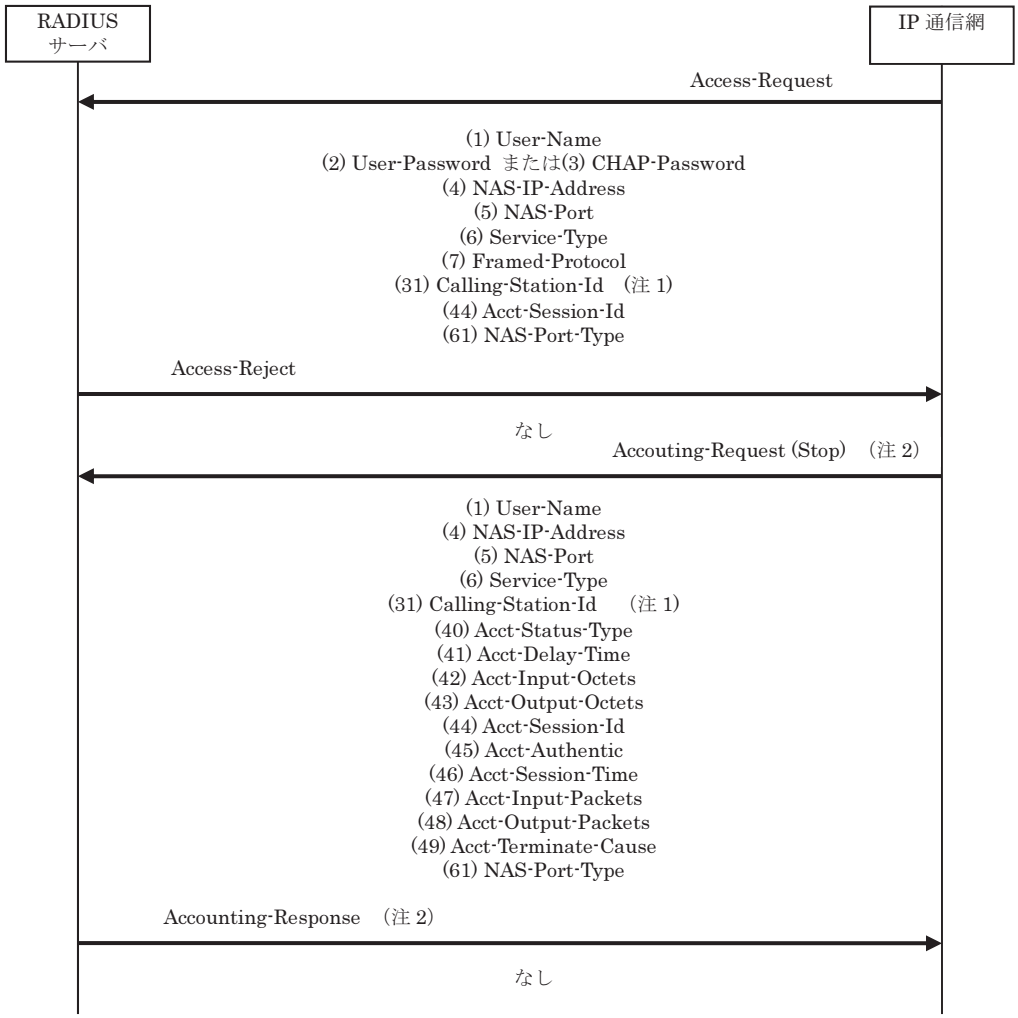
認証情報は図中 Access-Request で送信されます。

認証結果（認証成功）は図中 Access-Accept で送信します。

各 Attributes に関する詳細は表 5.1 を参照してください。

図 5.2　接続要求の通信シーケンス例（認証成功）

認証失敗



（注 1）回線情報転送機能を利用する場合において、フレッツ 光ネクスト及びフレッツ・ＩＳＤＮ利用端末からの認証の場合のみ IP 通信網から送出されます。ただし、フレッツ・ＩＳＤＮ利用端末からの認証の場合、発信者番号の非通知を設定している場合は送出されません。

（注 2）フレッツ・光プレミアム利用端末からの認証の場合は送出されません。

() は Attributes の Type を示しています。

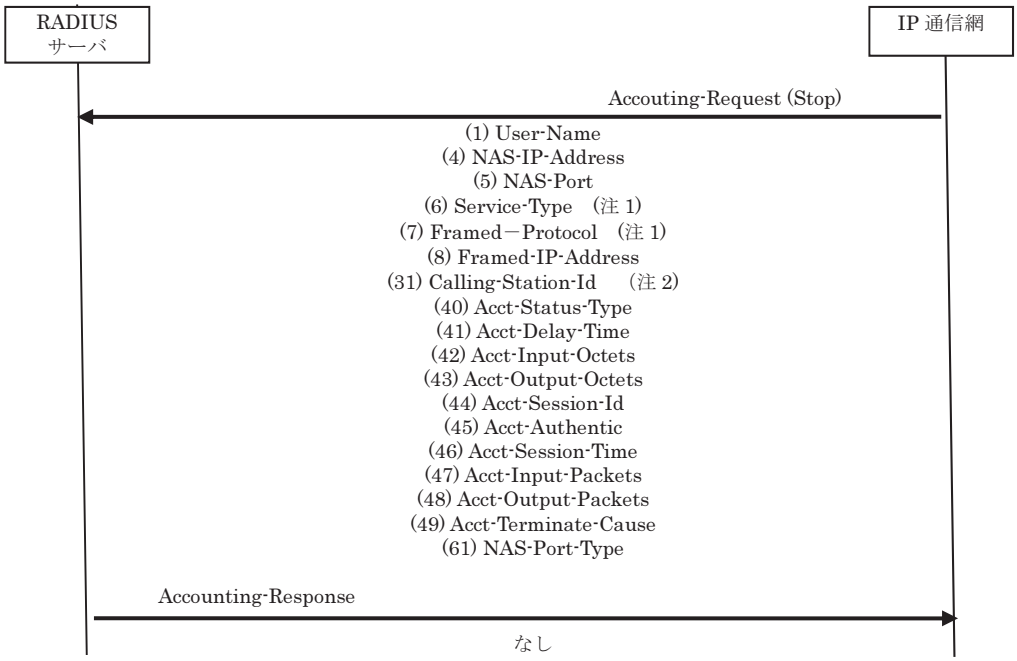
認証情報は図中 Access-Request で送信されます。

認証結果（認証失敗）は図中 Access-Reject で送信します。

各 Attributes に関する詳細は表 5.1 を参照してください。

図 5.3 接続要求の通信シーケンス例（認証失敗）

切断情報



（注 1）フレッツ・光プレミアム利用端末からの認証の場合は送出されません。

（注 2）回線情報転送機能を利用する場合において、フレッツ 光ネクスト及びフレッツ・ＩＳＤＮ利用端末からの認証の場合のみ IP 通信網から送出されます。ただし、フレッツ・ＩＳＤＮ利用端末からの認証の場合、発信者番号の非通知を設定している場合は送出されません。

() は Attributes の Type を示しています。

切断情報は図中 Accounting-Request(Stop)で送信されます。

各 Attributes に関する詳細は表 5.1 を参照してください。

図 5.4　切断情報の通信シーケンス例

5.2.2 利用可能な Attributes

フレッツ・ＶＰＮ ゲートで利用可能な Attributes 一覧を表 5.1 に示します。

表 5.1 フレッツ・ＶＰＮ ゲートで利用可能な Attributes 一覧

	Type	Value 形式	値	備考
<Access-Request>				
User-Name	1	文字列	(ユーザ名)	(ユーザ名)の長さは 63 オクテット以下です。(注 1)
User-Password	2	文字列	(パスワード)	(注 2)
CHAP-Password	3	文字列	(パスワード)	(注 2)
NAS-IP-Address	4	IPv4 アドレス	(IPv4 アドレス)	IP 通信網に設定した IPv4 アドレスとなります。
NAS-Port	5	整数	(ポート番号)	NAS-IP-Address と組み合わせて コネクションやユーザを 特定することはできません。
Service-Type	6	整数	2:Framed	(注 3)
Framed-Protocol	7	整数	1:PPP	(注 3)
Calling-Station-Id	31	文字列	(発信者回線情報)	回線情報転送機能を利用する場合において、フレッツ 光ネクスト及びフレッツ・ＩＳＤＮ利用端末からの認証の場合のみ、発信者回線情報が送出されます。(注 4)
Acct-Session-Id	44	文字列	(ID)	
NAS-Port-Type	61	整数	0～15	
<Access-Accept>				
Service-Type	6	整数	2:Framed	(注 3)
Framed-Protocol	7	整数	1:PPP	(注 3)
Framed-IP-Address	8	IPv4 アドレス	(IPv4 アドレス)	発信側端末機器に付与する IPv4 アドレスを設定します。 契約条件により IP 通信網から IPv4 アドレスを付与する場合は 255.255.255.254 を設定します。
Framed-IP-Netmask	9	IPv4 アドレス	(ネットマスク)	
<Accounting-Request(Start)>				
User-Name	1	文字列	(ユーザ名)	(ユーザ名) の長さは 63 オクテット以下です。(注 1)
NAS-IP-Address	4	IPv4 アドレス	(IPv4 アドレス)	IP 通信網に設定した IPv4 アドレスとなります。
NAS-Port	5	整数	(ポート番号)	NAS-IP-Address と組み合わせて コネクションやユーザを特定することは できません。
Service-Type	6	整数	2:Framed	(注 3)
Framed-Protocol	7	整数	1:PPP	(注 3)
Framed-IP-Address	8	IPv4 アドレス	(IPv4 アドレス)	
Calling-Station-Id	31	文字列	(発信者回線情報)	回線情報転送機能を利用する場合において、フレッツ 光ネクスト及びフレッツ・ＩＳＤＮ利用端末からの認証の場合のみ、発信者回線情報が送出されます。(注 4)

	Type	Value 形式	値	備考
Acct-Status-Type	40	整数	1:START	
Acct-Delay-Time	41	整数	(秒)	
Acct-Session-Id	44	文字列	(ID)	
Acct-Authentic	45	整数	1:RADIUS	
NAS-Port-Type	61	整数	0～15	
<Accounting-Request(Stop)>（注 3）				
User-Name	1	文字列	(ユーザ名)	（ユーザ名）の長さは 63 オクテット以下です。（注 1）
NAS-IP-Address	4	IPv4 アドレス	(IPv4 アドレス)	IP 通信網に設定した IPv4 アドレスとなります。
NAS-Port	5	整数	(ポート番号)	NAS-IP-Address と組み合わせて コネクションやユーザを特定することは できません。
Service-Type	6	整数	2:Framed	（注 3）
Framed-Protocol	7	整数	1:PPP	認証失敗時には設定されません。（注 3）
Framed-IP-Address	8	IPv4 アドレス	(IPv4 アドレス)	認証失敗時には設定されません。
Calling-Station-Id	31	文字列	(発信者回線情報)	回線情報転送機能を利用する場合において、フレッツ 光ネクスト及びフレッツ・ＩＳＤＮ利用端末からの認証の場合のみ、発信者回線情報が送出されます。（注 4）
Acct-Status-Type	40	整数	2:STOP	
Acct-Delay-Time	41	整数	(秒)	
Acct-Input-Octets	42	整数	(オクテット)	数値が設定されますが、 有意な値ではありません。
Acct-Output-Octets	43	整数	(オクテット)	
Acct-Session-Id	44	文字列	(ID)	
Acct-Authentic	45	整数	1:RADIUS	
Acct-Session-Time	46	整数	(秒)	
Acct-Input-Packets	47	整数	(パケット数)	数値が設定されますが、 有意な値ではありません。
Acct-Output-Packets	48	整数	(パケット数)	
Acct-Terminate-Cause	49	整数	1～18	
NAS-Port-Type	61	整数	0～15	
<Accounting-Request(Accounting-On)>　（注 5）				
NAS-IP-Address	4	IPv4 アドレス	(IPv4 アドレス)	IP 通信網に設定した IPv4 アドレスとなります。
Acct-Status-Type	40	整数	7:On	
Acct-Delay-Time	41	整数	(秒)	
Acct-Session-Id	44	文字列	(ID)	（注 3）
<Accounting-Request(Accounting-Off)>　（注 5）				
NAS-IP-Address	4	IPv4 アドレス	(IPv4 アドレス)	IP 通信網に設定した IPv4 アドレスとなります。
Acct-Status-Type	40	整数	8:Off	
Acct-Delay-Time	41	整数	(秒)	
Acct-Session-Id	44	文字列	(ID)	（注 3）
Acct-Terminate-Cause	49	整数	1～18	（注 3）（注 6）

（注 1） ユーザ名は、契約により選択された「ユーザ ID」もしくは「ユーザ ID@接続識別子」のいずれかが設定されます。接続識別子は契約の際、決定します。

（注 2） 「User-Password」、「CHAP-Password」の使用については、認証方式の契約（「CHAP/PAP 併用とする CHAP 優先使用」もしくは「PAP のみ使用」等）によります。

「User-Password」、「CHAP-Password」を暗号化するためのシークレットキーは、IP 通信網と RADIUS サーバで共有します。

（注 3） フレッツ・光プレミアム利用端末からの認証の場合は送出されません。

（注 4） フレッツ 光ネクスト利用端末からの認証の場合、発信側端末機器が接続されている回線において、発信者回線情報通知機能を利用の場合は発信者回線情報が設定され、発信者回線情報通知機能を利用していない場合は非通知相当文字列「NOINFO」が設定されます。フレッツ・ＩＳＤＮ利用端末からの認証の場合、発信側端末機器が接続されている回線において、発番号通知を実施している場合は発信電話番号が設定され、発番号通知を実施していない場合は送出されません。

（注 5） IP 通信網が異常となった場合、着信側端末機器に異常を通知するため、Accounting-Off を IP 通信網が送信する場合があります。また、異常により再起動した場合、再起動したことを着信側端末機器に通知するため Accounting-On を IP 通信網が送信します。

（注 6） Ｂフレッツ、フレッツ・ＡＤＳＬ、フレッツ・ＩＳＤＮ利用端末からの認証の場合は送出されない場合があります。

5.3　通信用タイマ

IP 通信網では、認証関連通信パケットの再送用タイマとして T1、T2 を、RADIUS サーバの切り戻し用タイマとして T3 を使用します。

タイマ T1、T2 は表 5.2 に示す起動条件で起動します。また、起動したタイマ T1、T2 は表 5.2 に示す正常停止条件で停止します。タイマ T3 については表 5.3 に示す起動条件で起動し、停止条件で停止します。タイマ T1 または T2 が正常停止条件を満たさず、タイマ値に達した場合、IP 通信網は起動条件である認証関連通信パケットを最大再送回数まで再送信します。

セカンダリサーバを設置していない場合、最大再送回数まで再送を行った後に、タイマ T1 または T2 が正常停止条件を満たさずタイマ値に達すると、認証失敗となり、認証関連通信は終了し、端末機器間の IPv4 通信は開始されません。

セカンダリサーバを設置している場合、最大再送回数まで再送を行った後に、タイマ T1 または T2 が正常停止条件を満たさずタイマ値に達すると、IP 通信網は認証関連通信の送信先をセカンダリサーバへ切り替え、再送回数を初期化した後に、再度、認証関連通信を開始します。

セカンダリサーバを使用している場合において、最大再送回数まで再送を行った後に、タイマ T1 または T2 がタイマ値に達すると認証失敗となり、認証関連通信は終了し、端末機器間の通信は開始されません。認証関連通信の送信先がセカンダリサーバに切り替わると、タイマ T3 が起動します。タイマ T3 が表 5.3 に示す停止条件を満たした場合、IP 通信網は表 5.3 に示す停止後の動作に従って、認証関連通信の送信先を切り替えます。

2 台目のセカンダリサーバを設置している場合、最大再送回数まで再送を行った後に、タイマ T1 または T2 が正常停止条件を満たさずタイマ値に達すると、IP 通信網は認証関連通信の送信先を 1 台目のセカンダリサーバから 2 台目のセカンダリサーバへ切り替え、再送回数を初期化した後に、再度、認証関連通信を開始します。2 台目のセカンダリサーバにおける、タイマ T1、T2、T3 の停止条件及び停止後の動作は 1 台目のセカンダリサーバと同じ動作を行います。

表 5.2　認証関連通信パケットの再送用タイマ

タイマ	タイマ値	起動条件	正常停止条件	最大再送回数
T1	3 秒	(1)Access-Request 送信	(2)Access-Accept または、 (3)Access-Reject 受信	2 回
T2	3 秒	(4)Accounting-Request 送信	(5)Accounting-Response 受信	2 回

() は RFC2865、及び RFC2866 で規定されているコード値を示します。

表 5.3　RADIUS サーバ切り戻し用タイマ

タイマ	タイマ値	起動条件	停止条件	停止後の動作
T3	15 分	プライマリサーバから セカンダリサーバへの 切り替え	タイマ値の満了	プライマリサーバへ 切り戻し
			最大再送回数後に タイマ T1、T2 が 正常停止条件を 満たせない場合	プライマリサーバへ 切り戻し
				セカンダリサーバ(2 台 目)へ切り替え（注 1）
		セカンダリサーバ(1 台 目)からセカンダリサーバ (2 台目)への切り替え	タイマ値の満了	プライマリサーバへ 切り戻し
			最大再送回数後に タイマ T1、T2 が 正常停止条件を 満たせない場合	

（注 1）2 台目のセカンダリサーバを設置している場合に動作します。

フレッツ・ＶＰＮ ワイド　センタ回線接続サービス

1　フレッツ・ＶＰＮ ワイド　センタ回線接続サービスの概要

1.1　サービスの概要

フレッツ・ＶＰＮ ワイド センタ回線接続サービス（以下、本サービスと呼びます）は、LAN やサーバ機器を IP 通信網に接続し、フレッツ・ISDN、フレッツ・ADSL、B フレッツ、フレッツ・光プレミアムおよびフレッツ 光ネクストを利用する端末機器との IPv4 通信を提供するフレッツＶＰＮ ワイドのサービスです。以下、本資料では、本サービスを利用する LAN やサーバ機器等を着信側端末機器、フレッツ・ISDN、フレッツ・ADSL、B フレッツ、フレッツ・光プレミアムおよびフレッツ 光ネクストを利用する端末機器等を発信側端末機器と呼びます。本サービスの基本構成の例を図 1.1 に示します。

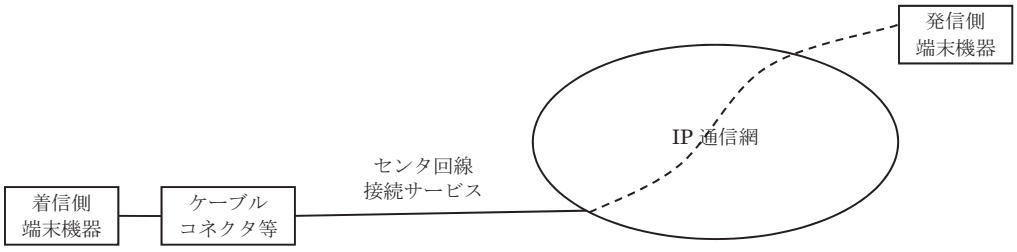


図 1.1　本サービスの基本構成

1.2　サービス品目

本サービスのサービス品目とサービス品目におけるインタフェースの条件を表 1.1 に示します。本資料では、本サービスのサービス品目を、インタフェース条件から表 1.1 に示す 3 つのタイプに分類して説明します。

表 1.1　本サービスのサービス品目とインタフェース条件

タイプ	メニュー	インタフェース条件
局内 接続タイプ	10Mb/s	IEEE 802.3-2005 10BASE-T 準拠
	100Mb/s	IEEE 802.3-2005 100BASE-FX/TX 準拠
		IEEE 802.3-2005 1000BASE-LX 準拠
収容エリア内 接続タイプ	100Mb/s	IEEE 802.3-2005 1000BASE-LX 準拠
ビジネスイーサ ワイド接続タイプ	10Mb/s	IEEE 802.3-2005 10BASE-T 準拠
	100Mb/s	IEEE 802.3-2005 100BASE-TX 準拠

1.3　　インタフェース規定点

1.3.1　　局内接続タイプのインタフェース規定点

局内接続タイプでは、図 1.2 に示す、ユーザ･網インタフェース（UNI）を規定します。

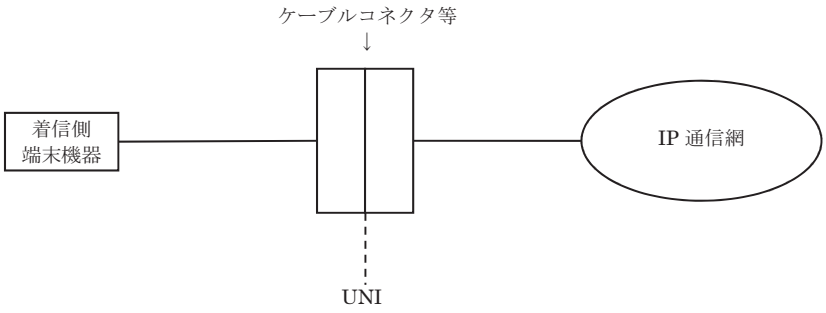


図 1.2　局内接続タイプのインタフェース規定点

各メニューにおけるインタフェース規定点は、図 1.3～図 1.5 を参照してください。インタフェースの詳細については、[2 ユーザ・網インタフェース仕様]を参照してください。

1.3.1.1　　10Mb/s メニューのユーザ･網インタフェース（UNI）

10Mb/s メニューにおけるユーザ･網インタフェース（UNI）の規定点を図 1.3 に示します。

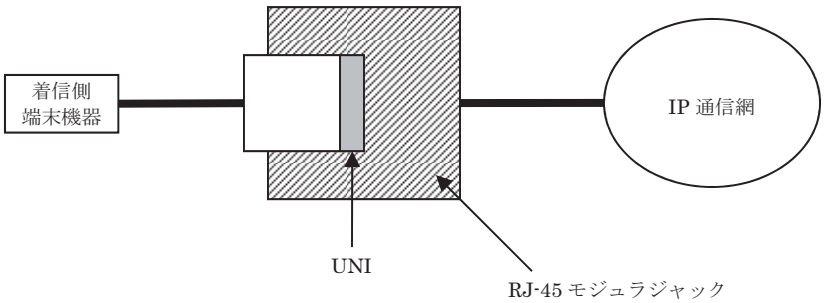


図 1.3　10Mb/s メニューのインタフェース規定点

1.3.1.2　　100Mb/s メニューのユーザ・網インタフェース（UNI）

100Mb/s メニューのユーザ・網インタフェース（UNI）の規定点を図 1.4 および図 1.5 に示します。

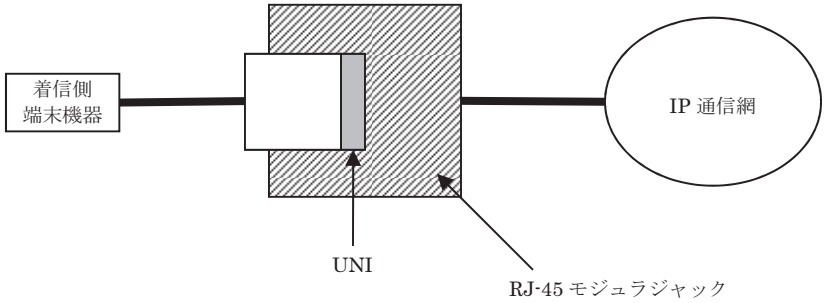


図 1.4　100Mb/s メニューのインタフェース規定点

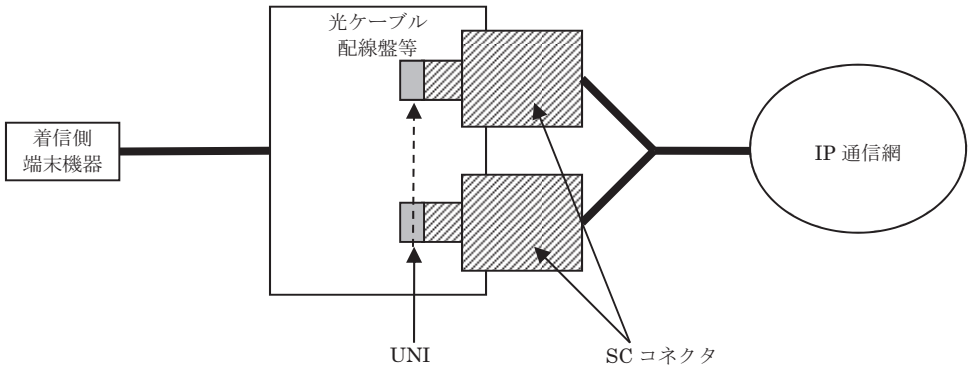


図 1.5　100Mb/s メニューのインタフェース規定点

1.3.2　　収容エリア内接続タイプのインタフェース規定点

収容エリア内接続タイプでは、図 1.6 に示す、ユーザ・網インタフェース（UNI）を規定します。

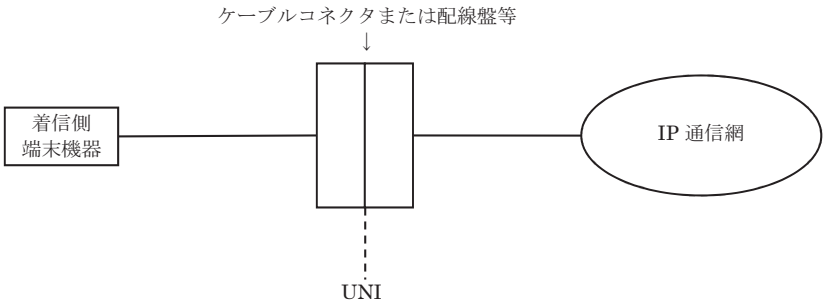


図 1.6　収容エリア内接続タイプのインタフェース規定点

インタフェースの詳細については、[2 ユーザ・網インタフェース仕様]を参照してください。

1.3.2.1　　100Mb/s メニューのユーザ・網インタフェース（UNI）

100Mb/s メニューにおけるユーザ・網インタフェース（UNI）の規定点を図 1.7 に示します。

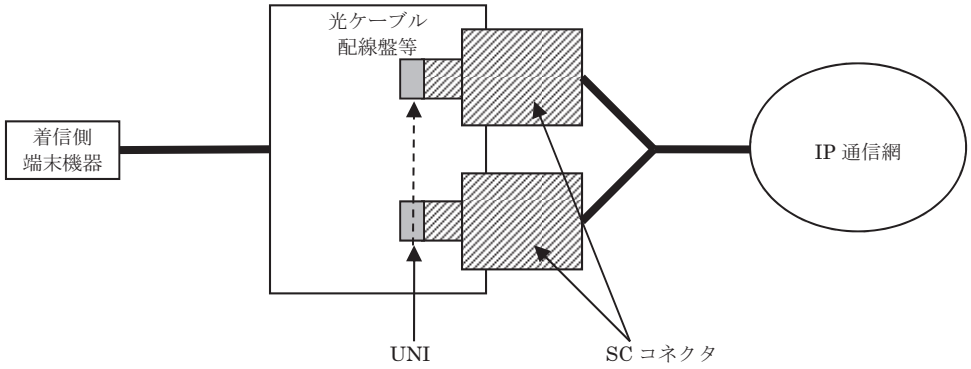


図 1.7　100Mb/s メニューのインタフェース規定点

1.3.3　　ビジネスイーサワイド接続タイプのインタフェース規定点

ビジネスイーサワイド接続タイプでは、図 1.8 に示す、ユーザ・網インタフェース（UNI）を規定します。

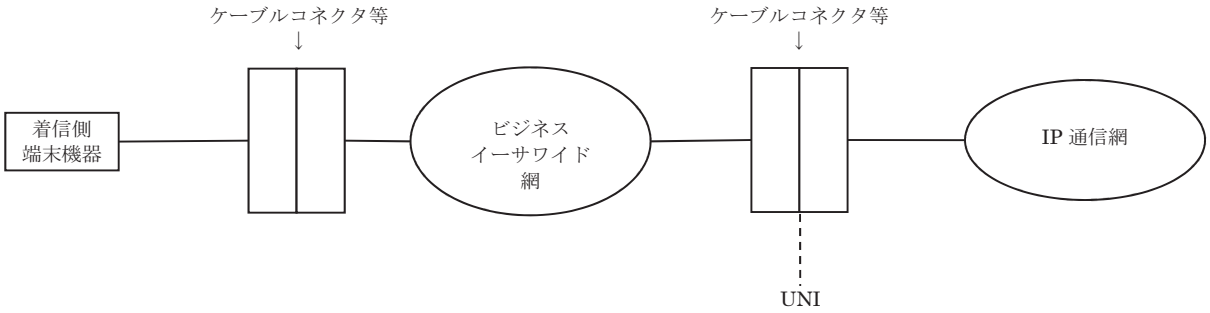


図 1.8　ビジネスイーサワイド接続タイプのインタフェース規定点

各メニューにおけるインタフェース規定点は、図 1.9 および図 1.10 を参照してください。
インタフェースの詳細については、[2 ユーザ・網インタフェース仕様]を参照してください。

1.3.3.1　　10Mb/s メニューのユーザ・網インタフェース（UNI）

10Mb/s メニューにおけるユーザ・網インタフェース（UNI）の規定点を図 1.9 に示します。

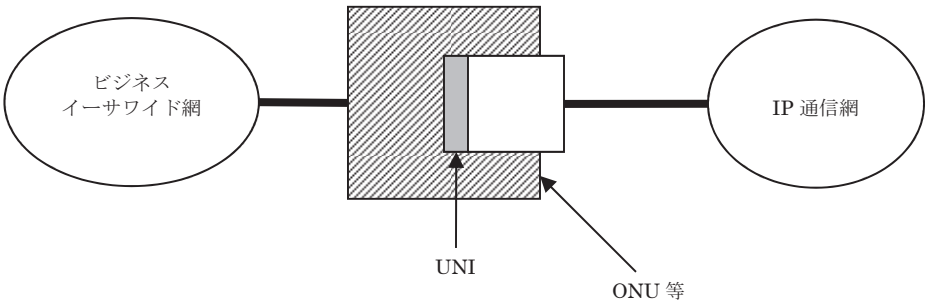


図 1.9　10Mb/s メニューにおけるインタフェース規定点

1.3.3.2　　100Mb/s メニューのユーザ・網インタフェース（UNI）

100Mb/s メニューにおけるユーザ・網インタフェース（UNI）の規定点を図 1.10 に示します。

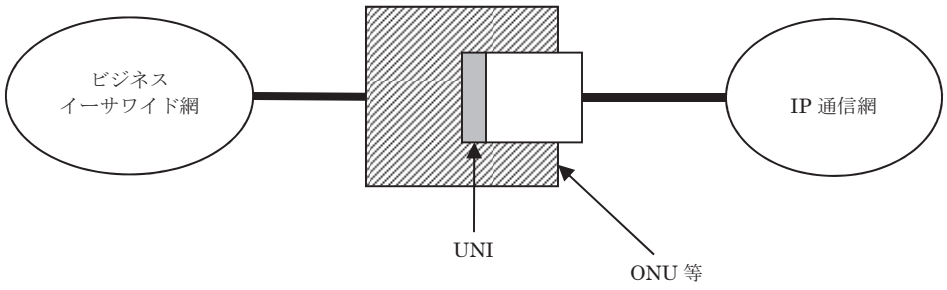


図 1.10　100Mb/s メニューのインタフェース規定点

1.4　　端末設備と電気通信回線設備の分界点

端末設備と電気通信回線設備との分界点は以下の通りです。

また、端末設備が必ず適合しなければならない技術的条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

1.4.1　　局内接続タイプの分界点

局内接続タイプの分界点を図 1.11 に示します。

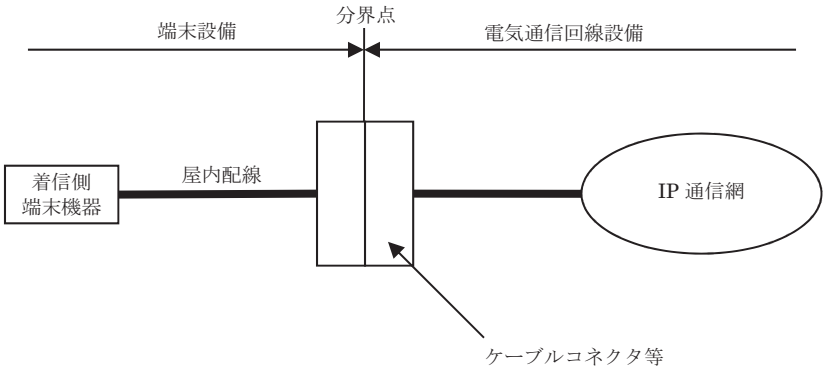
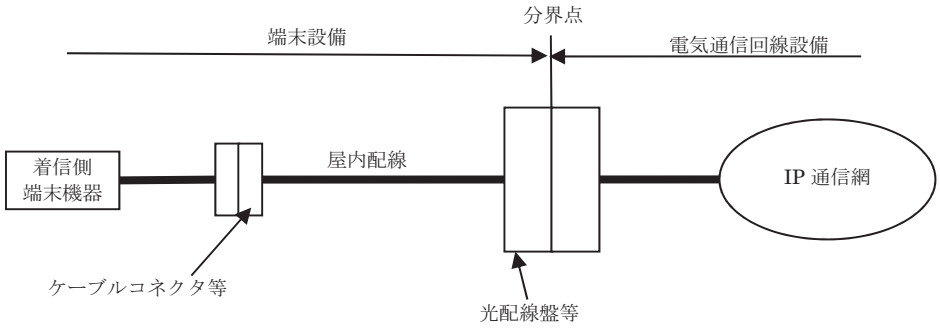


図 1.11　局内接続タイプの分界点

1.4.2　　収容エリア内接続タイプの分界点

収容エリア内接続タイプの分界点を図 1.12 に示します。

(a) 弊社が光配線盤等までの光ファイバを提供する場合



(b) 弊社が屋内配線までを提供する場合

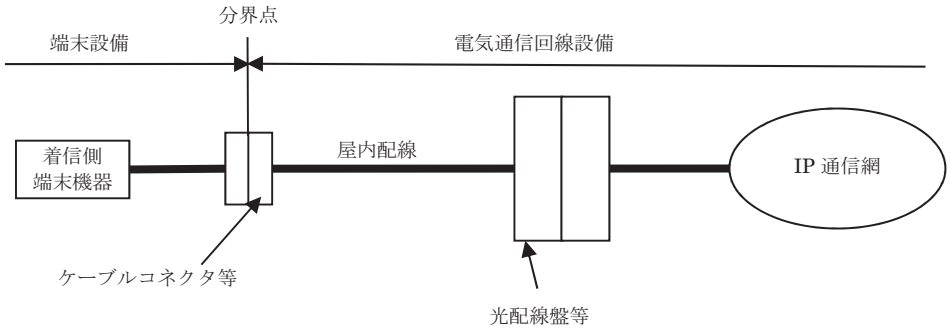


図 1.12　収容エリア内接続タイプの分界点

1.4.3　　ビジネスイーサワイド接続タイプの分界点

ビジネスイーサワイド接続タイプの分界点を図 1.13 に示します。

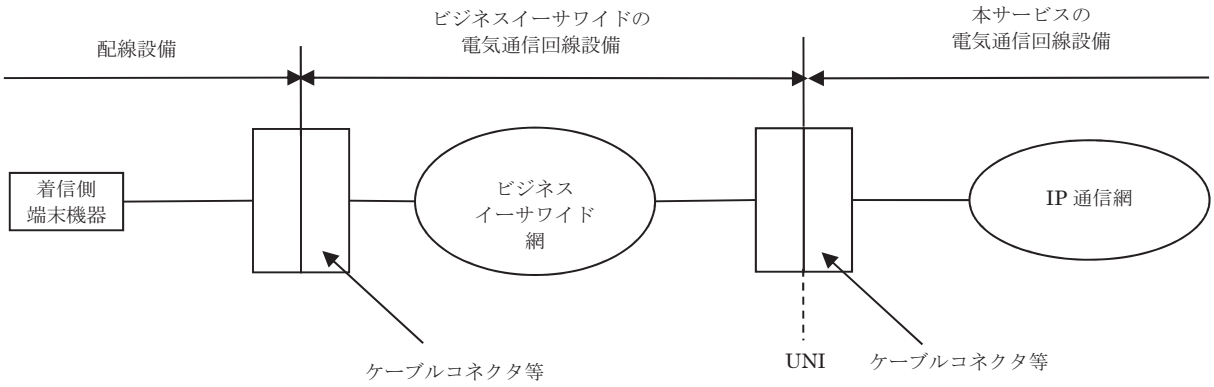


図 1.13　ビジネスイーサワイド接続タイプの分界点

1.5　　施工・保守上の責任範囲

本付加機能の施工・保守上の責任範囲については、以下の通りです。

1.5.1　　局内接続タイプの施工・保守上の責任範囲

局内接続タイプの施工・保守上の責任範囲を図 1.14 に示します。

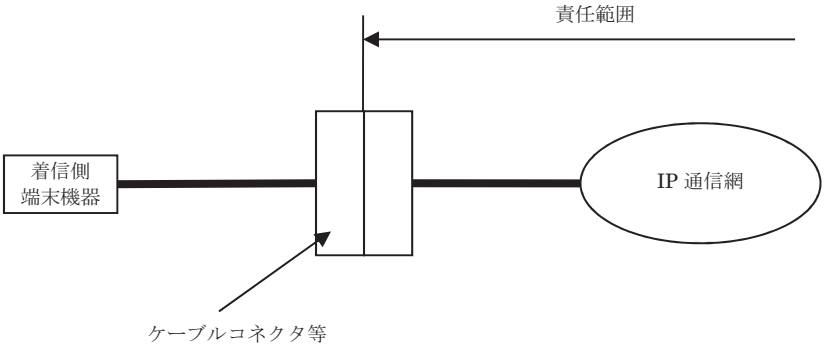
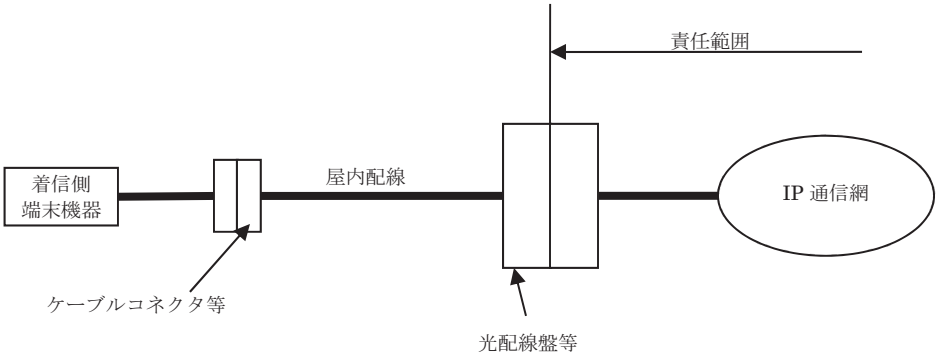


図 1.14　局内接続タイプの施工・保守上の責任範囲

1.5.2　　収容エリア内接続タイプの施工・保守上の責任範囲

収容エリア内接続タイプの施工・保守上の責任範囲を図 1.15 に示します。

(a) 弊社が光配線盤等までの光ファイバを提供する場合



(b) 弊社が屋内配線までを提供する場合

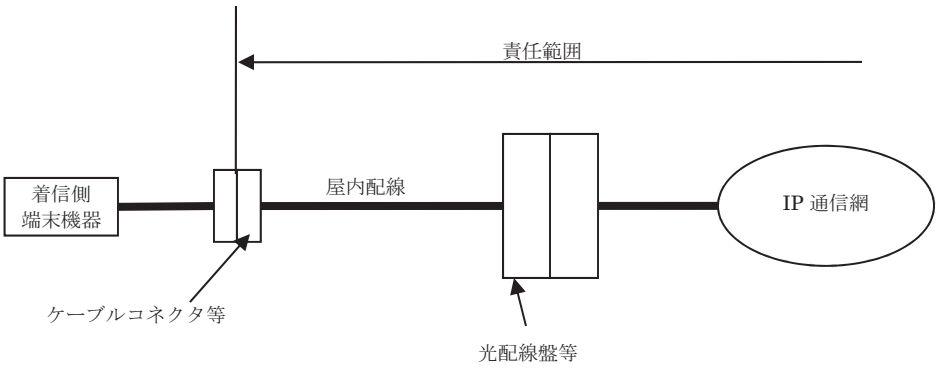


図 1.15　収容エリア内接続タイプにおける施工・保守上の責任範囲

1.5.3　　ビジネスイーサワイド接続タイプの施工・保守上の責任範囲

ビジネスイーサワイド接続タイプの施工・保守上の責任範囲を図 1.16 に示します。

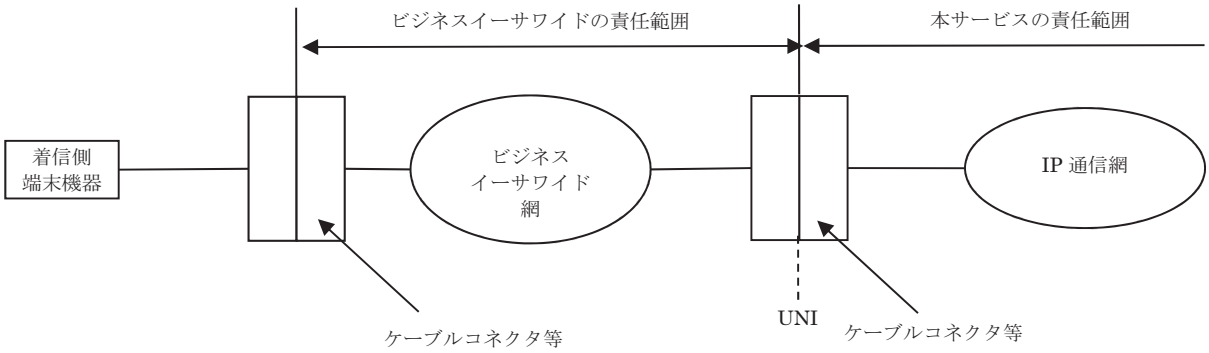


図 1.16　ビジネスイーサワイド接続タイプの施工・保守上の責任範囲

2　ユーザ・網インタフェース仕様

2.1　プロトコル構成

ユーザ・網インタフェースのプロトコル構成を、OSI 参照モデルに則した階層構成で表 2.1 に示します。

IP 通信網と着信側端末機器との IPv4 通信については、レイヤ 1～3 のプロトコルについて規定します。

表 2.1　プロトコル構成

レイヤ		規定するプロトコル
7	アプリケーション	規定しない
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	RFC791（IPv4） RFC792（ICMPv4）
2	データリンク	RFC826（ARP） IEEE 802.3-2005 MAC 準拠
1	物理	IEEE 802.3-2005 10BASE-T IEEE 802.3-2005 100BASE-FX/TX IEEE 802.3-2005 1000BASE-LX 準拠

2.2　　レイヤ 1 仕様

レイヤ 1 では、IEEE 802.3-2005 に規定されている 10BASE-T、100BASE-FX/TX または 1000BASE-LX を使用し、10Mb/s、100Mb/s の伝送速度でベースバンド信号の全二重の通信を行います。

詳細については、IEEE 802.3-2005 を参照してください。

2.2.1　　10Mb/s メニューのレイヤ 1 仕様

10Mb/s メニューのレイヤ 1 では、IEEE802.3-2005 に規定されている 10BASE-T を使用し、10Mb/s の伝送速度でベースバンド信号の全二重固定の通信を行います。

詳細については、IEEE802.3-2005 を参照してください。

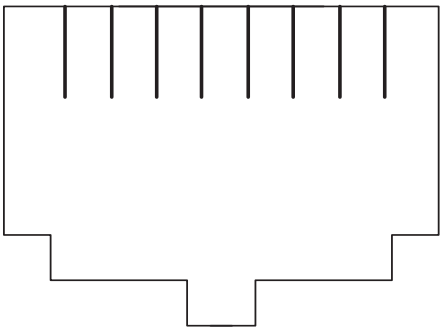
2.2.1.1　　インタフェース条件

局内接続タイプの 10Mb/s メニューで提供するユーザ・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 2.1 に示します。

ビジネスイーサ ワイド接続タイプの 10Mb/s メニューで提供するユーザ・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 コネクタ（1 コネクタ）です。コネクタの先端面から見た RJ-45 コネクタのピン配置を図 2.2 に示します。

RJ-45 ポート挿入面

ピン番号　1　2　3　4　5　6　7　8

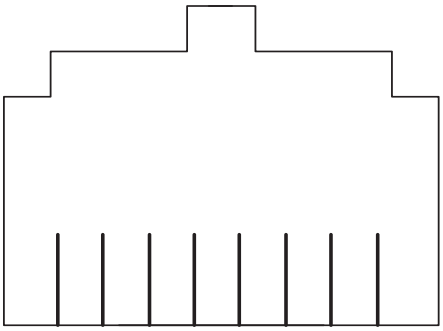


	記号	信号方向		ピン番号
		端末機器	IP 通信網	
受信	RD (+)		→	1
	RD (−)		→	2
送信	TD (+)	←		3
	TD (−)	←		6

※ピン番号 4、5、7、8 は使用しません

図 2.1　挿入面から見た RJ-45 ポートのピン配置

RJ-45 コネクタ先端面



ピン番号 1 2 3 4 5 6 7 8

	記号	信号方向		ピン番号
		端末機器	IP 通信網	
送信	TD(+)	←		1
	TD(−)	←		2
受信	RD(+)		→	3
	RD(−)		→	6

※ピン番号 4、5、7、8 は使用しません

図 2.2　コネクタ先端面から見た RJ-45 コネクタのピン配置

2.2.1.2　10BASE-T の適用ケーブル条件

モジュラジャックと接続する着信側端末機器等との配線は、2 対の非シールドより対線ケーブル（EIA/TIA-568 標準 UTP ケーブル カテゴリ 3 以上）を使用します。また、配線状況によりモジュラジャックと端末機器間のケーブルの最大長は、IEEE802.3-2005 に規定されている 100m よりも短いものとなります。

2.2.2　100Mb/s メニューのレイヤ 1 仕様

100Mb/s メニューのレイヤ 1 では、IEEE802.3-2005 に規定されている 100BASE-FX/TX または 1000BASE-LX を使用します。100BASE-FX/TX の場合、100Mb/s の伝送速度で全二重固定の通信を行います。1000BASE-LX の場合、100Mb/s の伝送速度で、固定または自動折衝機能（Auto Negotiation 機能）により、全二重の通信モードを利用可能です。

詳細については、IEEE802.3-2005 を参照してください。

2.2.2.1　インタフェース条件

局内接続タイプの 100Mb/s メニューで提供するユーザ・網インタフェースは、100BASE-FX については 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。（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。）

100BASE-TX については 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 2.1 に示します。

収容エリア内接続タイプの 100Mb/s メニューで提供するユーザ・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-TG.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。

ビジネスイーサ ワイド接続タイプの 100Mb/s メニューで提供するユーザ・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 コネクタ（1 コネクタ）です。コネクタの先端面から見た RJ-45 コネクタのピン配置を図 2.2 に示します。

2.2.2.2　100BASE-TX の適応ケーブル条件

モジュラジャックと接続する着信側端末機器等との配線は、2 対の非シールドより対線ケーブル（EIA/TIA-568 標準 UTP ケーブル カテゴリ 5 以上）を使用します。また、配線状況によりモジュラジャックと端末機器間のケーブルの最大長は、IEEE802.3-2005 に規定されている 100m よりも短いものとなります。

2.3　　レイヤ 2 仕様

レイヤ 2 では、IEEE802.3-2005 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。

MAC についての詳細は IEEE802.3-2005 を、ARP についての詳細は RFC826 を参照してください。

2.4　　レイヤ 3 仕様

レイヤ 3 では、RFC791 に規定されている IPv4 を使用します。IPv4 のサブセットとして RFC792 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 についての詳細は RFC791 を、ICMPv4 についての詳細は RFC792 を参照してください。

2.4.1　　IP アドレス

本付加機能では、RFC1700 で規定されているクラス D、クラス E の IPv4 アドレスをサポートしません。RFC1918 で規定されているプライベートアドレスは使用可能です。

IPv4 アドレスについての詳細は RFC1700 を、プライベートアドレスについての詳細は RFC1918 を参照してください。

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り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。

2.4.2　　接続用 IP アドレス

着信側端末機器と IP 通信網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。

着信側端末機器と IP 通信網間で IPv4 通信を行うために、着信側端末機器の IP 通信網を接続するインタフェース、及び IP 通信網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。

なお、接続用 IP アドレスには、一部利用できないアドレス領域があります。

2.4.3　　ルーティング

IP 通信網と着信側端末機器間のルーティング方式はスタティックルーティングです。

2.4.4　　最大転送単位（MTU）

IP 通信網内の MTU の値は 1454byte (注) です。MTU の値を越えるパケットを IP 通信網が受信した場合、IP 通信網内で分割転送が発生する場合があります。

（注）フレッツ・光プレミアム利用端末との通信について、IP 通信網内の MTU の値は 1438byte です。

2.5　　上位レイヤ（レイヤ 4～7）仕様

上位レイヤ（レイヤ 4～7）については規定しません。

フレッツ・キャスト

1　フレッツ・キャストの概要

1.1　サービスの概要

フレッツ・キャストは、LAN やサーバ機器を IP 通信網に接続し、フレッツ 光ネクストを利用する端末機器との IP 通信を提供するサービスです。

以下、本資料では、フレッツ・キャストを利用する LAN やサーバ機器等をセンタ側端末機器、フレッツ 光ネクストを利用する端末機器等をエンド側端末機器と呼びます。

フレッツ・キャストの基本構成の例を図 1.1 に示します。

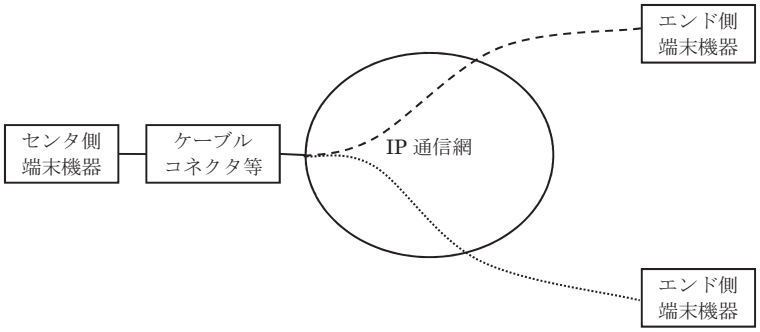


図 1.1　フレッツ・キャストの基本構成

1.2 サービス品目

フレッツ・キャストのサービス品目とサービス品目におけるインタフェースの条件を表 1.1 に示します。

表 1.1 フレッツ・キャストのサービス品目とインタフェース条件

<table>
<tr><th>サービス品目</th><th>マルチキャスト機能</th><th colspan="2">インタフェース条件</th></tr>
<tr><td rowspan="2">ベストエフォート型 100Mb/s
シングルクラス</td><td>なし</td><td rowspan="4">IEEE 802.3-2005
100BASE-TX 準拠</td><td rowspan="4">IEEE 802.3-2005
1000BASE－SX 準拠
1000BASE－LX 準拠</td></tr>
<tr><td>あり</td></tr>
<tr><td rowspan="2">ベストエフォート型 100Mb/s
デュアルクラス</td><td>なし</td></tr>
<tr><td>あり</td></tr>
<tr><td rowspan="2">ベストエフォート型 200Mb/s
シングルクラス</td><td>なし</td><td rowspan="12" colspan="2">IEEE 802.3-2005
1000BASE－SX 準拠
1000BASE－LX 準拠</td></tr>
<tr><td>あり</td></tr>
<tr><td rowspan="2">ベストエフォート型 200Mb/s
デュアルクラス</td><td>なし</td></tr>
<tr><td>あり</td></tr>
<tr><td rowspan="2">ベストエフォート型 300Mb/s
シングルクラス</td><td>なし</td></tr>
<tr><td>あり</td></tr>
<tr><td rowspan="2">ベストエフォート型 300Mb/s
デュアルクラス</td><td>なし</td></tr>
<tr><td>あり</td></tr>
<tr><td rowspan="2">ベストエフォート型 1Gb/s
シングルクラス</td><td>なし</td></tr>
<tr><td>あり</td></tr>
<tr><td rowspan="2">ベストエフォート型 1Gb/s
デュアルクラス</td><td>なし</td></tr>
<tr><td>あり</td></tr>
<tr><td>帯域確保型 1Gb/s
シングルクラス</td><td>なし</td></tr>
</table>

1.3　インタフェース規定点

規定するユーザ･網インタフェース（UNI）を図 1.2 に示します。

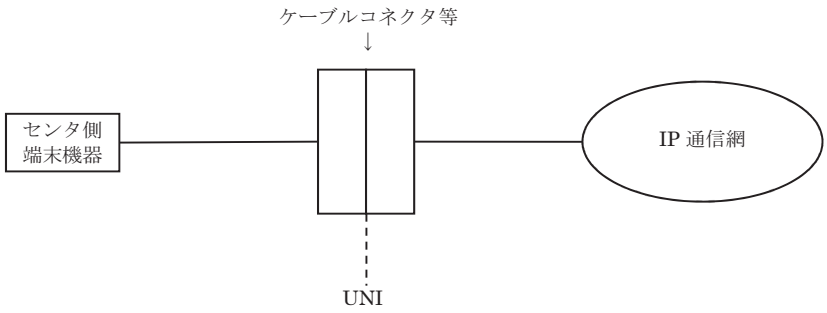


図 1.2　フレッツ・キャストのインタフェース規定点

1.3.1　　ユーザ･網インタフェース（UNI）

ユーザ･網インタフェース（UNI）の規定点を図 1.3 に示します。インタフェースの詳細については、[2 フレッツ・キャストのユーザ・網インタフェース仕様]を参照してください。

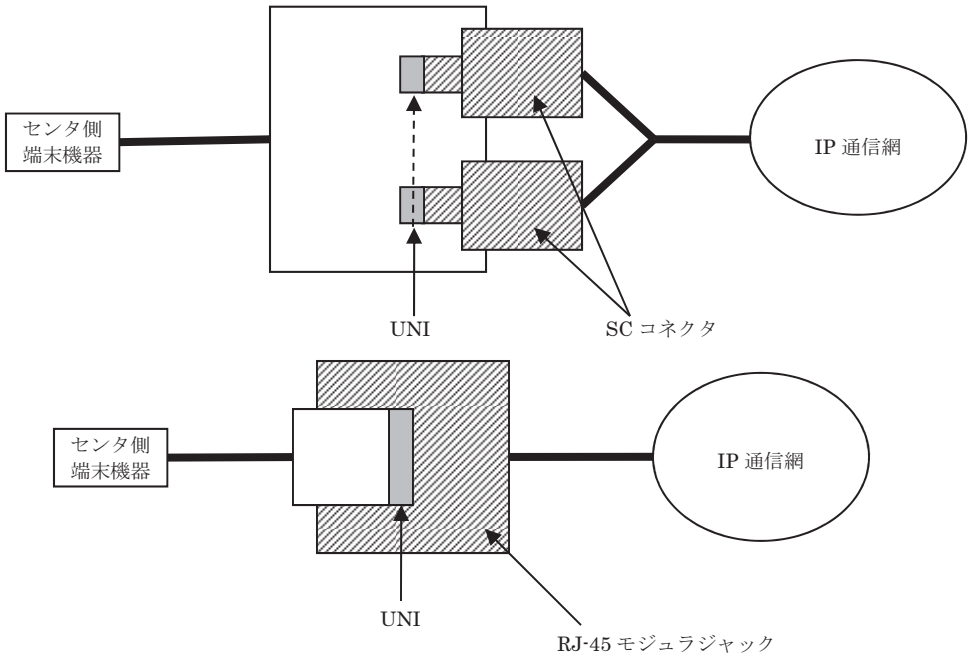


図 1.3　フレッツ・キャストのインタフェース規定点

1.4　　端末設備と電気通信設備の分界点

端末設備と電気通信設備との分界点を図 1.4 に示します。

また、端末設備が必ず適合しなければならない技術条件は、「端末設備等規則」（昭和 60 年郵政省令 31 号）を参照してください。

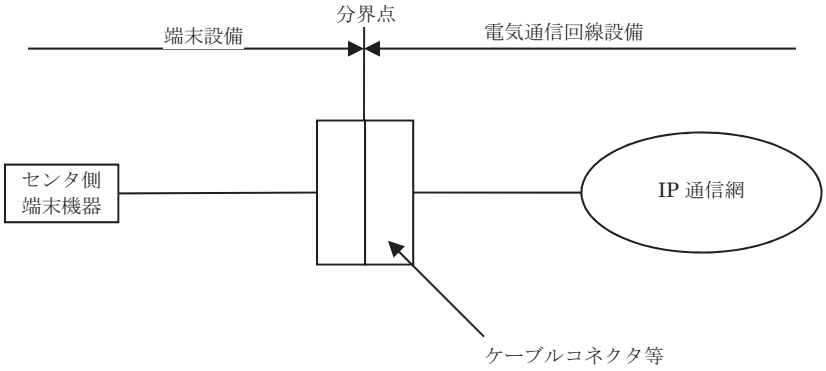


図 1.4　フレッツ・キャストの分界点

1.5　施工・保守上の責任範囲

フレッツ・キャストにおける施工・保守上の責任範囲を、図 1.5 に示します。

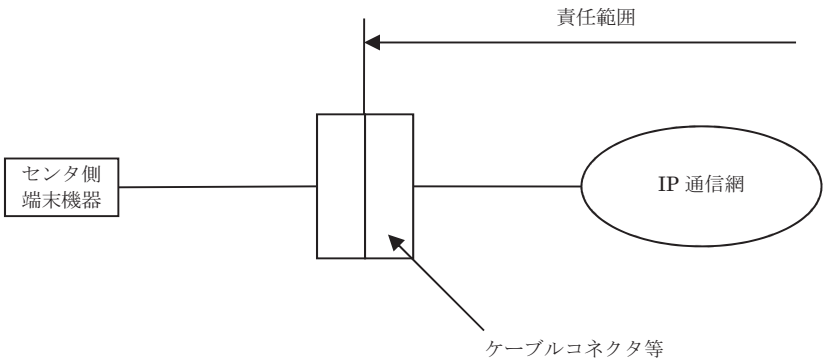


図 1.5　フレッツ・キャストにおける施工・保守上の責任範囲

施工・保守上の責任範囲の分界点を図 1.6 **に示します。接続点で、斜線部より IP 通信網側が責任範囲となります。**

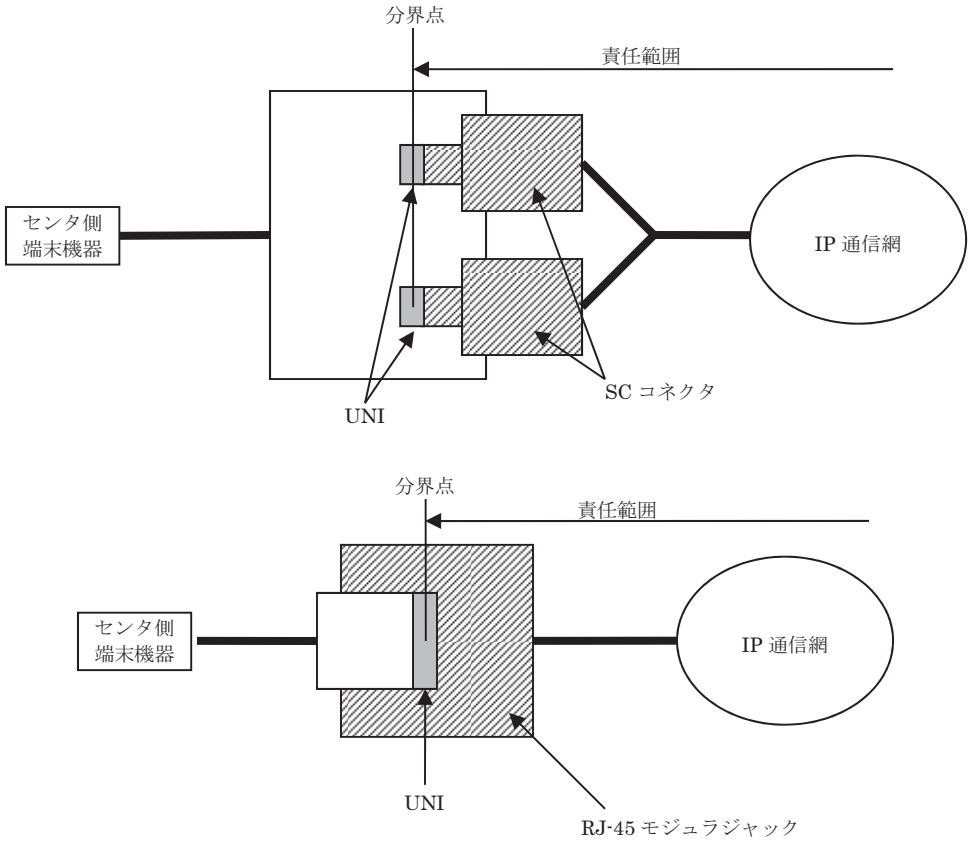


図 1.6　フレッツ・キャストにおける施工・保守上の責任範囲分界点

2　フレッツ・キャストのユーザ・網インタフェース仕様

2.1　プロトコル構成

ユーザ・網インタフェースのプロトコル構成を、OSI 参照モデルに則した階層構成で表 2.1 に示します。

表 2.1　フレッツ・キャストのプロトコル構成

<table>
<tr><th colspan="2" rowspan="2">レイヤ</th><th colspan="2">規定するプロトコル</th></tr>
<tr><th>ベストエフォート型のもの</th><th>帯域確保型のもの</th></tr>
<tr><td>7</td><td>アプリケーション</td><td colspan="2" rowspan="4">DNS(注 1)：
RFC1034 / RFC1035 / RFC1123 / RFC2181/ RFC2308 /
RFC2671/ RFC2782 / RFC3596
RTP/RTCP(注 2)：
TTC JF-IETF-STD64 / TTC JF-IETF-STD65
RTSP(注 2)：
RFC2326
SNTP(注 3):
RFC4330
SIP(注 4) ：
RFC3261 / RFC3262 / RFC3311 / RFC3323 / RFC3324 /
RFC3325 / RFC3327 / RFC3428 / RFC3455 / RFC3608 /
RFC3966 / RFC4028 / RFC4715 /
TTC TS-1008 / TTC TS-1009 / TTC TR-9022 / TTC TR-9024 /
3GPP TS24.229 / RFC5407
RFC5079
SDP(注 4)：
RFC4566 / RFC3264 / RFC4145 / 3GPP TS29.208
HTTP（注 6）
RFC2616
SSL Version3.0（注 6）</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>4</td><td>トランスポート</td></tr>
<tr><td>3</td><td>ネットワーク</td><td>IPv6:
RFC3513 / RFC2460 / RFC2474 /
RFC3306(注 5) / RFC3307(注 5)
ICMPv6：
RFC4443
NDP:
RFC2461
BGP4+:
RFC1771 / RFC2545 / RFC2858</td><td>IPv6:
RFC3513 / RFC2460 /
RFC2474
ICMPv6：
RFC4443
NDP:
RFC2461</td></tr>
<tr><td>2</td><td>データリンク</td><td colspan="2">IEEE 802.3-2005(MAC)</td></tr>
<tr><td>1</td><td>物理</td><td colspan="2">IEEE 802.3-2005 (100BASE-TX、1000BASE-SX、1000BASE-LX)準拠</td></tr>
</table>

(注 1) DNS を用いて名前解決を行なう場合に適用されます。

(注 2) 音声および映像等のリアルタイムデータの通信を行う場合に適用されます。

（注 3） IP 通信網の SNTP サーバを利用する場合に使用します。

（注 4） 帯域確保型ユニキャスト通信を行う場合に適用されます。

（注 5） 「マルチキャスト機能あり」の場合に適用されます。

（注 6）「回線情報通知機能あり」の場合に使用します。

2.2 レイヤ 1 仕様

レイヤ 1 では、IEEE802.3-2005 に規定されている 100BASE-TX、または IEEE 802.3-2005 に規定されている 1000BASE-SX もしくは 1000BASE-LX を使用し、サービス品目が 100Mb/s(100BASE-TX)の場合は 100Mb/s、サービス品目が 100Mb/s、200Mb/s、300Mb/s、1Gb/s(1000BASE-SX もしくは 1000BASE-LX)の場合は 1Gb/s の伝送速度でベースバンド信号の通信を行います。固定または自動折衝機能(Auto Negotiation 機能)により、全二重の通信モードを利用可能です。

ただし、IP 通信網への流入トラヒックが契約帯域を超えるデータパケットを受信した場合には、IP 通信網内で廃棄されます。したがって、IP 通信網に送出するトラヒックについては、シェーピング機能等により転送制御することを推奨します。

1000BASE-SX もしくは 1000BASE-LX の詳細については、IEEE 802.3-2005 を参照してください。

2.2.1 インタフェース条件

フレッツ・キャストで使用するユーザ・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（100BASE-TX）、もしくは IEC60874-14 に規定される SC コネクタ（オス）（1000BASE-SX、1000BASE-LX）です。

また、IEEE802.3-2005 に規定されている 1000BASE－SX で提供するユーザ・網インタフェースの配線は、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。IEEE802.3-2005 に規定されている 1000BASE－LX で提供するユーザ・網インタフェースの配線は、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。

2.3 レイヤ 2 仕様

レイヤ 2 では、IEEE802.3-2005 に規定されている MAC を使用します。MAC についての詳細は IEEE802.3-2005 を参照してください。

2.4 レイヤ 3 仕様

レイヤ 3 では RFC 2460 に規定されている IPv6 を使用します。また、RFC3513 に規定されている IPv6 アドレッシングをサポートします。

IPv6 マルチキャスト機能として、RFC3306、RFC3307 に規定されている機能をサポートします。BGP4+によるルーティング機能として、RFC1771、RFC2545 および RFC2858 に規定されている機能をサポートします。

なお、IP 通信網に接続する機器類は、RFC4443 に規定されている ICMPv6 、RFC2461 に規定されている NDP をサポートする必要があります。

各仕様に関する詳細は各 RFC を参照してください。

2.4.1 IPv6 アドレス

RFC3513 で規定されている IPv6 のグローバル・ユニキャストアドレスを使用します。

加えて、配信方式が「マルチキャスト機能あり」のサービスを利用する場合、前記アドレスとは別にマルチキャスト通信用のアドレスとして IPv6 のマルチキャストアドレスも使用します。

フレッツ・キャストでは、リンクローカルアドレスを除き、弊社から割り当てられた以外の IPv6 アドレスを利用する場合の動作は保証しません。

IPv6 アドレスの詳細については、RFC3513 を参照してください。

2.4.2 IPv6 パケットフォーマット

RFC2474 に則り、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。

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、フラグメントヘッダ、認証ヘッダ、暗号化ペイロードヘッダを使用します。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。

また、フラグメントされたデータ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。

2.4.3 ICMPv6

センタ側端末機器は、RFC4443 に規定される ICMPv6 をサポートする必要があります。

センタ側端末機器は、IP 通信網から 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。IP 通信網からの ICMPv6 エコー要求メッセージは、センタ側端末機器と IP 通信網との故障切り分けを行う場合等に送出されます。また IP 通信網はセンタ側端末機器とエンド側端末機器の間での ICMPv6 エコー要求メッセージと ICMPv6 エコー応答メッセージの送受信を可能とします。

2.4.4 NDP

センタ側端末機器は、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 に準拠します。

2.4.5　ルーティング

IP 通信網とセンタ側端末機器間のルーティングは、利用するサービス品目により異なり、表 2.2 に示す通りとなります。なお、弊社より割り当てられた IP アドレス以外へのルーティングは行いません。

各仕様に関する詳細は、各 RFC を参照してください。

表 2.2　サービス品目とルーティング方式

サービス品目	ルーティング方式
ベストエフォート型 100Mb/s シングルクラス	スタティックルーティング ダイナミックルーティング(BGP4+) (RFC1771 / RFC2545 / RFC2858)
ベストエフォート型 200Mb/s シングルクラス	
ベストエフォート型 300Mb/s シングルクラス	
ベストエフォート型 1Gb/s シングルクラス	
帯域確保型 1Gb/s シングルクラス	スタティックルーティング
ベストエフォート型 100Mb/s デュアルクラス	ダイナミックルーティング(BGP4+) (RFC1771 / RFC2545 / RFC2858)
ベストエフォート型 200Mb/s デュアルクラス	
ベストエフォート型 300Mb/s デュアルクラス	
ベストエフォート型 1Gb/s デュアルクラス	

2.4.5.1　ルーティングに関する主な条件

ルーティング方式としてダイナミックルーティング（BGP4+）を利用するにあたり、RFC1771、RFC2545 及び RFC2858 に記載されているアトリビュートのうち、AS-PATH、NEXT-HOP、Origin、MP_REACH_NLRI、MP_UNREACH_NLRI が使用可能です。

これ以外のアトリビュートを設定した場合、動作を保証しません。

2.4.6　最大転送単位（MTU）

MTU の値は 1500byte です。MTU の値を越えるデータパケットを受信した場合、IP 通信網内で正常な通信ができない場合があります。

2.5 上位レイヤ（レイヤ 4～7）仕様

上位レイヤ（レイヤ 4～7）では、DNS、SNTP、RTP/RTCP、RTSP、SIP、SDP、HTTP、SSL をサポートします。

2.5.1 DNS

IP 通信網は、センタ側端末機器に対して、弊社が定める 1 以上のドメインを管理する DNS 機能を有します。また、センタ側端末機器に設定される弊社が割り当てた当該ドメインのサブドメインを管理する DNS サーバに対して権限を委譲します。

仕様に関する詳細は表 2.1 に示す参照勧告類に準拠してください。

2.5.2 SNTP

IP 通信網は、センタ側端末機器に対して、時刻取得のため IP 通信網の SNTP サーバを利用することができます。IP 通信網の SNTP サーバは、RFC4330 に準拠します。

2.5.3 RTP/RTCP、RTSP

IP 通信網とセンタ側端末機器間の音声・映像等のリアルタイムデータの通信には、RTP、RTCP および RTSP をサポートします。なお、RTSP にて記載の Interleaved 方式は許容されません。

仕様に関する詳細は表 2.1 に示す参照勧告類に準拠してください。

2.5.4 SIP、SDP

IP 通信網では、センタ側端末機器がセッション制御用ユーザエージェント（SIP-UA）を実装することで、SIP-UA と IP 通信網との間で帯域を確保したユニキャスト通信（帯域確保型ユニキャスト通信）を行うことが可能です。帯域を確保したマルチキャスト通信は行えません。

なお、セッションのネゴシエーションには SDP を使用します。SDP による転送品質クラス指定方法は[3.1 制御信号における転送品質クラス指定方法]を参照してください。また、本資料で指定しない仕様に関する詳細は表 2.1 に示す参照勧告類に準拠してください。

2.5.4.1　セッション制御用ユーザエージェント（SIP-UA）の登録手順

REGISTER 信号を用いたセッション制御用ユーザエージェント（SIP-UA）の登録は不要です。

2.5.4.2　SIP-UA の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 は接続要求を IP 通信網に送信します。

(2) IP 通信網は発着 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、IP 通信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 IP 通信網に切断要求を送信すると、IP 通信網は相手 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。

なお、SIP-UA は発 ID としてユーザ登録 ID を利用します。ユーザ登録 ID はエンド側端末機器が契約電話番号と SIP ドメインから構成される SIP-URI となり、センタ側端末機器が契約時に決定する SIP-URI となります。

契約電話番号から構成されないセンタ側端末機器の場合、SIP-UA は IP 通信網から接続要求が通知された場合のみ通信が可能であり、IP 通信網への接続要求送信は許容されません。

2.5.4.3　同時通信可能数

同時通信可能数については、制限があります。

2.5.5　HTTP、SSL

IP 通信網は、回線情報通知機能利用時に HTTP、SSL を用いて、エンド側端末機器の回線情報をセンタ側端末機器へ通知します。回線情報通知機能は、ベストエフォート型のみ利用可能です。回線情報通知機能に関する仕様については、当該サービスの技術規定等を参照してください。

3　品質規定に係る仕様

3.1　制御信号における転送品質クラス指定方法

IP 通信網では、転送品質クラスは RFC4566 に規定される SDP を用いた、セッションのネゴシエーションによって指定されます。

SDP による転送品質クラスは、SDP の m=行（Media Types）と a=行（Attributes）の組み合わせで、m=行毎に転送品質クラスを指定します。転送品質クラスは SDP オファー/アンサーの結果、m=行の新規設定時に決定されます。m=行の変更によって 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。m=行の種別については、音声（m=audio）、映像（m=video）、その他（m=application）を許容します。

3.2　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、IP 通信網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（RFC3261 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、IP 通信網に対して送出する必要があります。ただし、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。

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。

3.3　トークンバケットポリサーによる流入トラヒックの監視

フレッツ・キャストでは、IP 通信網へ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 Appendix 1 参照）で監視します。トークンバケットポリサーの監視条件を違反したデータパケットは、IP 通信網内で廃棄されます。したがって、IP 通信網に送出するトラヒックについては、シェーピング機能等により転送制御することを推奨します。

4　エンド側端末機器の利用条件

4.1　MLDv2

IP 通信網においてエンド側端末機器とセンタ側端末機器間でマルチキャストアドレスを利用した通信を行う場合、エンド側端末機器は RFC3810 で規定される MLDv2 に対応する必要があります。

Multicast Listener Report メッセージは、Version2 を使用します。この Multicast Listener Report メッセージをエンド側端末機器から IP 通信網に送信する場合の ICMPv6 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、動作を保証しません。

RFC3810（MLDv2）では、マルチキャスト通信の受信要求方法として特定のマルチキャストアドレスを指定して要求する「インクルードモード（Include mode）」と、特定のマルチキャストアドレス以外を指定して要求する「エクスクルードモード（Exclude mode）」が定義されていますが、IP 通信網においてはインクルードモードにのみ対応しています。

表 4.1 に設定可能な Multicast Address Record タイプの一覧を示します。なお、この値以外を設定した場合、動作を保証しません。

図 4.1～図 4.4 に、それぞれマルチキャスト受信開始シーケンス例、マルチキャスト受信継続確認シーケンス例、チャネル切り替えシーケンス例及びマルチキャスト受信停止シーケンス例を示します。

表 4.1　設定可能な Multicast Address Record タイプ一覧

種別	タイプ	値	用途
Current State Record	MODE_IS_ INCLUDE	1	クエリー応答において、 インクルードモードを使用すること を明示する。
State Change Record	ALLOW_NEW_ SOURCES	5	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に 送信する。
	BLOCK_OLD_ SOURCES	6	Multicast Address Record に 設定したマルチキャストアドレスを 利用する通信から離脱する場合に 送信する。

4.1.1 マルチキャスト受信開始シーケンス例

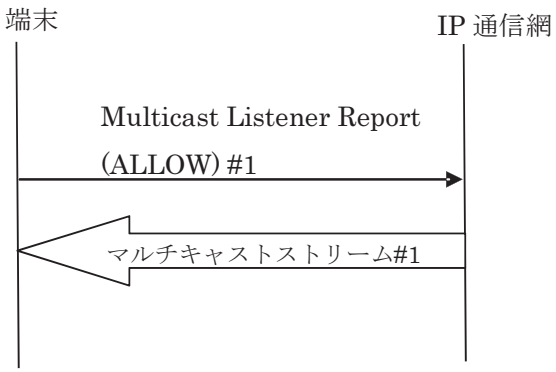


図 4.1 マルチキャスト受信開始シーケンス例

4.1.2　マルチキャスト受信継続確認シーケンス例

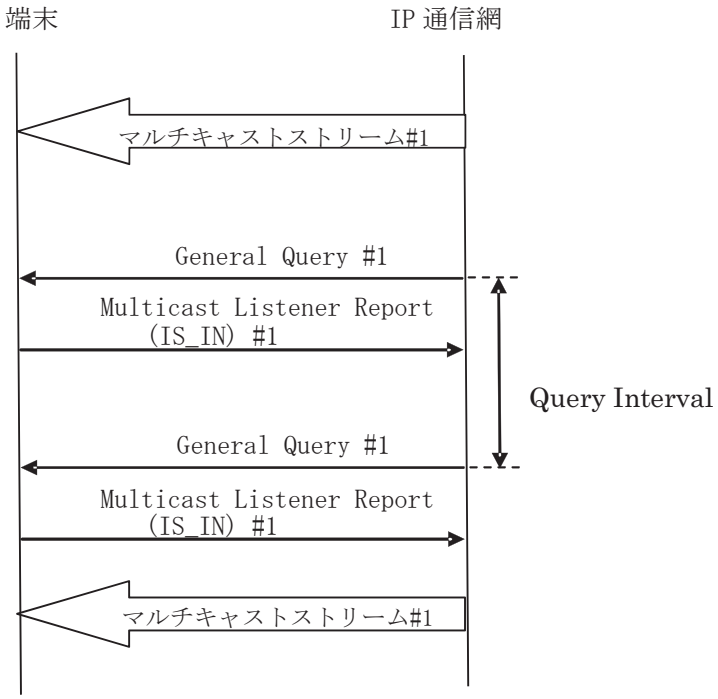


図 4.2 マルチキャスト受信継続確認シーケンス例

4.1.3　　チャネル切り替えシーケンス例

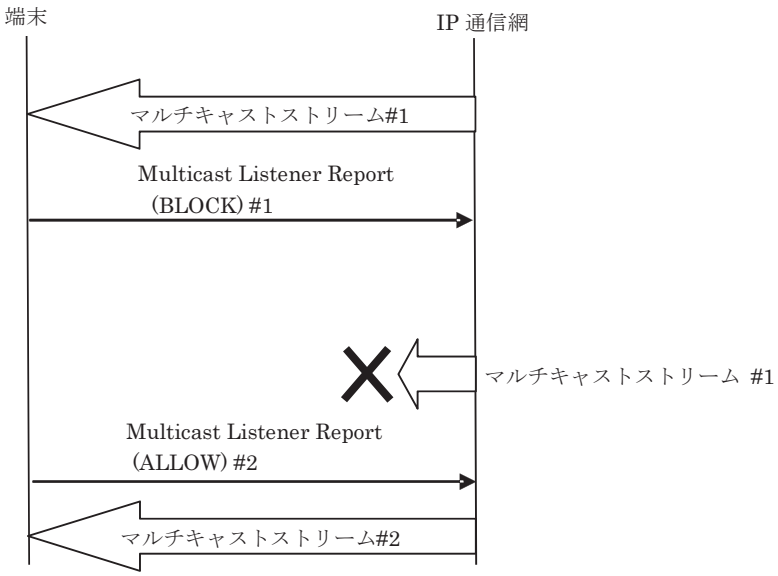


図 4.3 チャネル切り替えシーケンス例

4.1.4 マルチキャスト受信停止シーケンス例

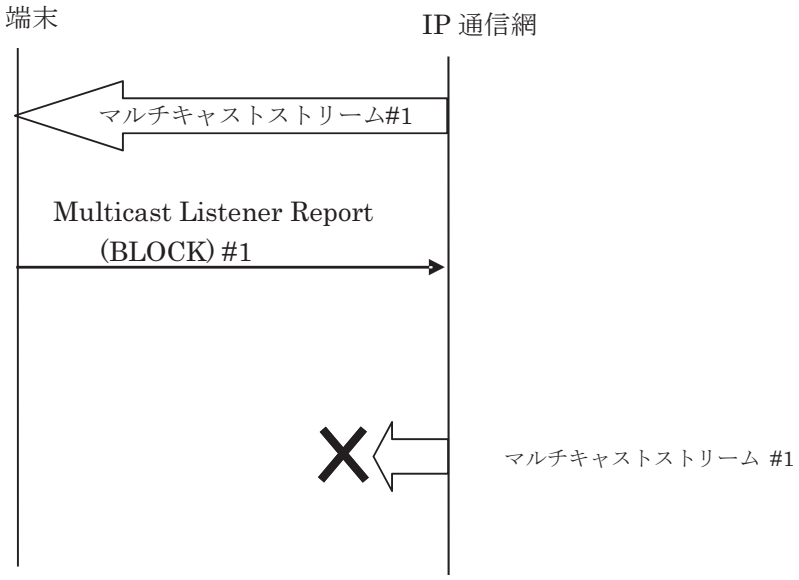


図 4.4 マルチキャスト受信停止シーケンス例

4.2 SIP、SDP

IP 通 信網では、エンド側端末機器がセッション制御用ユーザエージェント（SIP-UA）を実装することで、SIP-UA と IP 通信網との間で帯域を確保したユニキャスト通信（帯域確保型ユニキャスト通信）を行うことが可能です。帯域を確保したマルチキャスト通信は行えません。

なお、セッションのネゴシエーションには SDP を使用します。SDP による転送品質クラス指定方法の詳細は[3.1 制御信号における転送品質クラス指定方法]を参照してください。また、本資料で指定しない仕様に関する詳細は表 2.1 に示す参照勧告類に準拠してください。

4.2.1 セッション制御用ユーザエージェント（SIP-UA）の登録手順

SIP-UA の登録手順は以下の通りです。

(1) SIP-UA は登録要求を IP 通信網に送信します。

(2) IP 通信網は、SIP-UA に登録が完了したことを通知します。

(3) IP 通信網の登録が完了すると、発着信が可能となります。

4.2.2 SIP-UA の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 IP 通信網に送信します。

(2) IP 通信網は発着 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、IP 通信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 IP 通信網に切断要求を送信すると、IP 通信網は相手 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。

なお、SIP-UA は発 ID としてユーザ登録 ID を利用します。ユーザ登録 ID はエンド側端末機器が契約電話番号と SIP ドメインから構成される SIP-URI となり、センタ側端末機器が契約時に決定する SIP-URI となります。

契約電話番号から構成されないセンタ側端末機器の場合、SIP-UA は IP 通信網から接続要求が通知された場合のみ通信が可能であり、IP 通信網への接続要求送信は許容されません。

4.2.3 同時通信可能数

同時通信可能数については、制限があります。

4.3 CDN 構成情報の通知

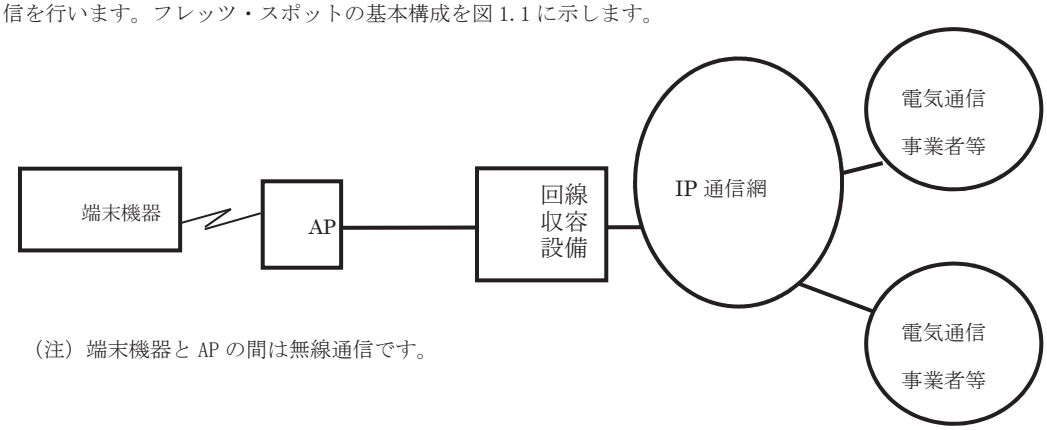
IP 通信網は、IPTV フォーラムが策定する IPTV 規定に準拠し IPv6 に対応した IPTV サービス対応受信機による CDN 構成情報の取得とその情報による各種サーバへのアクセスを可能とします。CDN 構成情報の提供と各種サーバへのアクセスに関する規定は IPTV フォーラム『IPTV 規定 CDN スコープ サービスアプローチ仕様 IPTVFJ STD-0006』に従います。

フレッツ・スポット

1　フレッツ・スポットサービス概要

1.1　サービスの概要

フレッツ・スポットはベストエフォート型の IP 通信サービスです。フレッツ・スポットを利用する端末機器等（以下、端末機器）は、無線アクセスポイント（以下、AP）に接続した後、電気通信事業者等と IP 通信網を介して IP 通信を行います。フレッツ・スポットの基本構成を図 1.1 に示します。



（注）端末機器と AP の間は無線通信です。

図 1.1　フレッツ・スポットの基本構成

1.2　インタフェース規定点

フレッツ・スポットでは、図 1.2 に示すユーザ・網インタフェース（UNI）を規定します。

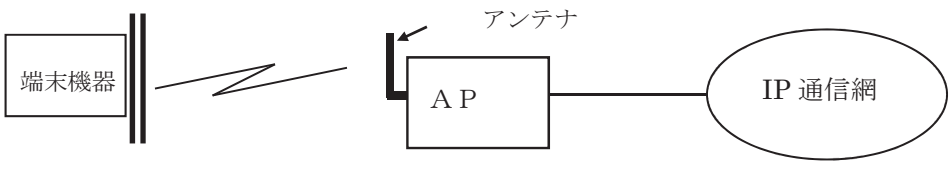


図 1.2　インタフェース規定点

1.3　端末設備と電気通信回線設備の分界点

端末設備と電気通信回線設備との分界点について図 1.3 に示します。

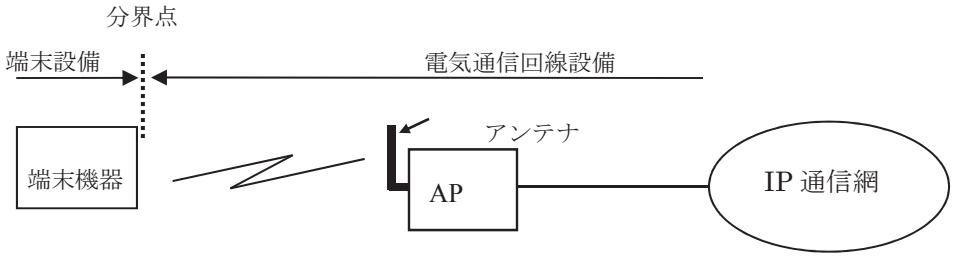


図 1.3　分界点

1.4　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 1.4 に示します。

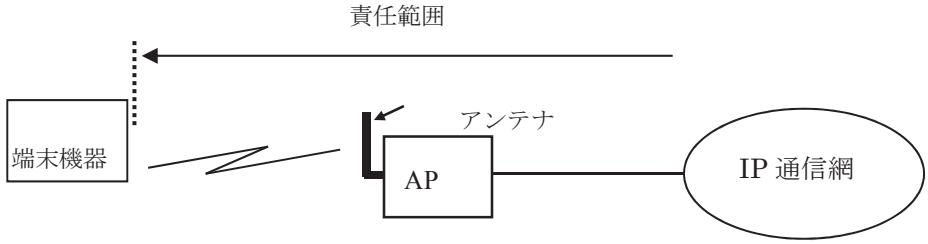


図 1.4　施工・保守上の責任範囲

2　ユーザ・網インタフェース仕様

2.1　プロトコル構成

プロトコル構成は、表 2.1 に示す OSI 参照モデルに則した階層構成となっています。

表 2.1　プロトコル構成

レイヤ		使用するプロトコル
7	アプリケーション	認証時の通信において以下プロトコルを規定します。 RFC2131(DHCP) RFC1034,RFC1035,RFC1123,RFC2181,RFC2308,RFC2671,RFC2782(DNS) RFC2616(HTTP) RFC2246(TLS1.0) RFC5246(TLS1.2) ※その他通信においては、特に規定はありません。
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	RFC791, RFC1918(IPv4)
2	データリンク	IEEE802.11(MAC) ,IEEE802.11i
1	物理	IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.11ac ARIB STD-T71/STD-T66

2.2　物理レイヤ（レイヤ 1）仕様

フレッツ・スポットがサポートするレイヤ 1 のインタフェース条件は IEEE802.11a、IEEE802.11bIEEE802.11g、IEEE802.11n、又は IEEE802.11ac とします。

表 2.2　無線インタフェースの条件

項目		規格
周波数帯域	802.11a	5,470 ～ 5,725MHz
	802.11b	2,400 ～ 2,483.5MHz
	802.11g	2,400 ～ 2,483.5MHz
	802.11n	5,470 ～ 5,725MHz、2,400 ～ 2,483.5MHz
	802.11ac	5,470 ～ 5,725MHz
使用チャネル	802.11a	100～140CHのいずれかを使用
	802.11b	1 ～ 13CHのいずれかを使用
	802.11g	1 ～ 13CHのいずれかを使用
	802.11n	2.4GHz: 1～13CHのいずれかを使用 5GHz:100～140CHのいずれかを使用
	802.11ac	100～140CHのいずれかを使用
伝送速度	802.11a	最大54Mbps
	802.11b	最大11Mbps
	802.11g	最大54Mbps
	802.11n	最大450Mbps
	802.11ac	最大1.3Gbps
変調方式	802.11a	OFDM
	802.11b	DSSS
	802.11g	OFDM
	802.11n	OFDM
	802.11ac	OFDM
メディアアクセス制御		CSMA/CA

（注）無線回線状況等により伝送速度が変動します。また、この伝送速度を保証するものではありません。

2.3　データリンクレイヤ（レイヤ 2）仕様

レイヤ 2 では、IEEE 802.11 に規定されている MAC を使用します。MAC の詳細については IEEE 802.11 を参照してください。また、SSID と WPA2-PSK キーの設定条件を表 2.3 に示します。

表 2.3　SSID と WPA2-PSK キーの設定条件

設定項目	設定条件	備考
SSID	使用します	設定値は契約者に個別通知
WPA2-PSKキー	使用します	設定値は契約者に個別通知

2.4　ネットワークレイヤ（レイヤ 3）仕様

レイヤ 3 では、RFC791 に規定されている IPv4 を使用します。IPv4 についての詳細は RFC791 を参照してください。

また、端末機器の IP アドレスとして利用可能な IPv4 アドレスは、IP 通信網に接続する際に、IP 通信網から割り当てられた RFC1918 で規定されているクラス A のプライベートの IP アドレスのみです。その他の IP アドレスを利用する場合、動作は保証しません。

2.5　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、DHCP、DNS 、HTTP、TLS1.0、TLS1.2 を認証時の通信において規定します。その他通信においては、特に規定はありません。

2.5.1　DNS

IPv4 に対応した端末機器は、IP 通信網経由でアクセス可能な DNS サーバ間で、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 2.4 に示します。各仕様に関する詳細は各 RFC を参照してください。

表 2.4　DNS 規定

参考文献	タイトル	備考
RFC1034	Domain names -Concepts and facilities	DNSについて規定
RFC1035	Domain names -implementation and specification	DNSについて規定
RFC1123	Requirements for Internet Hosts - Application and Support	DNSの実装について規定
RFC2181	Clarifications to the DNS Specification	DNSについて規定
RFC2308	Negative Caching of DNS Queries (DNS NCACHE)	ネガティブキャッシュについて規定
RFC2671	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	A DNS RR for specifying the location of services	SRV レコードを規定

2.5.2　HTTP

IPv4 に対応した端末機器は、通信するプロトコルとして HTTP を使用することが可能です。HTTP を利用する場合に準拠する規定は RFC2616 となります。仕様に関する詳細は RFC2616 を参照してください。TLS1.0 を利用する場合に準拠する規定は RFC2246 となります。仕様に関する詳細は RFC2246 を参照してください。TLS1.2 を利用する場合に準拠する規定は RFC5246 となります。仕様に関する詳細は RFC5246 を参照してください。

HTTP の通信先には認証サーバがあり、端末機器が電気通信事業者側への通信をするための認証を行います。

表 2.5 認証サーバへの接続条件

項番	項目名	内容
1	レイヤ3	IPv4
2	上位レイヤ	HTTP、TLS1.0、TLS1.2

2.5.3 制限事項

フレッツ・スポットでは以下の制限事項があります。

(1) 端末機器の IP アドレスとして、IPv6 アドレスを利用した通信は利用できません。

(2) 端末機器から PPPoE 接続を行うことができません。

(3) 端末機器の IP アドレスは IP 通信網から払い出したプライベートアドレスとなるため、グローバルアドレスを用いて電気通信事業者を介する IP 通信では端末機器に接続ができません。

3　フレッツ・スポットの通信シーケンス

フレッツ・スポットを利用する場合の通信シーケンスについて、接続及び切断手順等の具体例について説明します。

3.1　無線区間における接続シーケンス

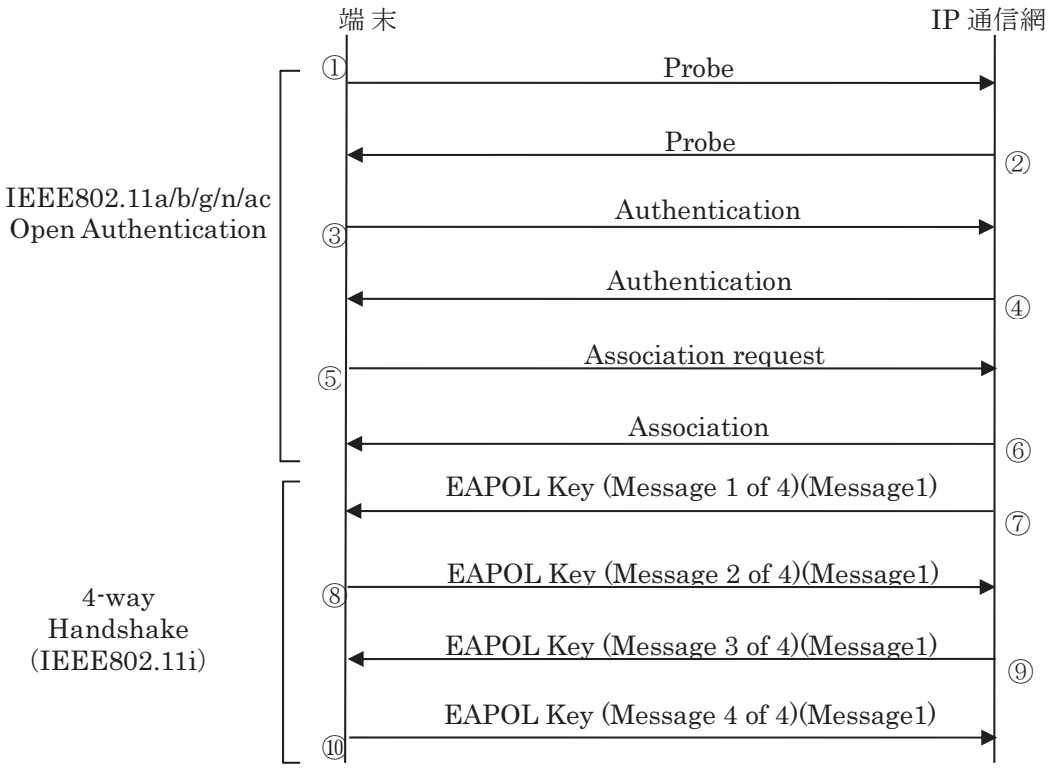


図 3-1 接続シーケンス（例）

［説明］

(1)　端末機器が接続する SSID とサポートするパラメータを無線 AP に送付します。

(2)　無線 AP がサポートするパラメータを、端末機器に送付します。

(3)　端末機器がオープンシステム認証を要求します。

(4)　無線 AP がオープンシステム認証要求に応答します。

(5)　端末機器がアソシエーション要求を送信します。

(6)　無線 AP がアソシエーション ID を応答します。

(7)　無線 AP がナンスを送信します。

(8)　端末機器がナンスを送信します。

(9)　無線 AP がペアキーの設定メッセージとグループキーを送信します。

(10)　端末機器が応答します。

3.2　無線区間における接続失敗シーケンス

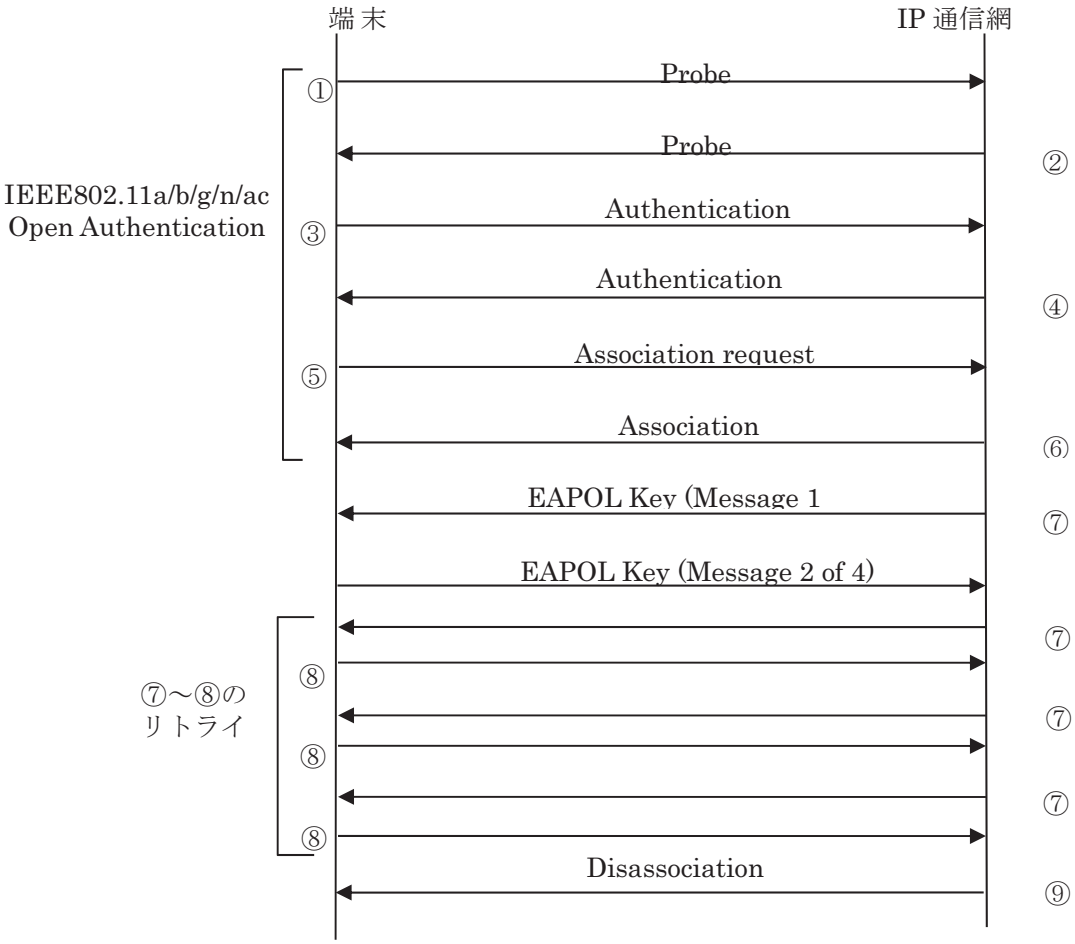


図 3-2　接続失敗シーケンス（例）

［説明］

(1) 端末機器が接続する SSID とサポートするパラメータを無線 AP に送付します。

(2) 無線 AP がサポートするパラメータを、端末機器に送付します。

(3) 端末機器がオープンシステム認証を要求します。

(4) 無線 AP がオープンシステム認証要求に応答します。

(5) 端末機器がアソシエーション要求を送信します。

(6) 無線 AP がアソシエーション ID を応答します。

(7) 無線 AP がナンスを送信します。

(8) 端末機器がナンスを送信します。(端末に設定された事前共有キーが誤っている場合、本ステップ で失敗します)

(9) 無線 AP が端末機器に切断を通知します。