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 ―

第三分冊

第 26 版

東日本電信電話株式会社

本資料の内容は、機能追加などにより追加・変更されることがあります。
内容についての問い合わせは、下記宛にお願い致します。

東 日 本 電 信 電 話 株 式 会 社
ビジネス開発本部

ip-interface@ml.east.ntt.co.jp

目次

IP通信網サービスのインタフェース ― フレッツシリーズ ― 第三分冊 - 1 -
目次 1
まえがき 4
用語の定義 9
フレッツ 光ネクスト編 - 11 -
1 フレッツ 光ネクストの概要 - 12 -
1.1 サービスの概要 - 12 -
1.2 インタフェース規定点 - 12 -
1.3 端末設備と電気通信回線設備の分界点 - 13 -
1.4 施工・保守上の責任範囲 - 13 -
2 ユーザ・網インタフェース仕様 - 14 -
2.1 プロトコル構成 - 14 -
2.2 物理レイヤ（レイヤ1）仕様 - 15 -
2.3 データリンクレイヤ（レイヤ2）仕様 - 16 -
2.4 レイヤ3仕様 - 16 -
2.5 上位レイヤ（レイヤ4～7）仕様 - 23 -
3 PPPoE / PPPプロトコル - 30 -
3.1 PPP - 30 -
3.2 PPPoE - 32 -
4 付属資料 - 44 -
4.1 ONU（スロット式）の概要 - 44 -
フレッツ 光ライト編 - 45 -
1 フレッツ 光ライトの概要 - 46 -
1.1 サービスの概要 - 46 -
1.2 インタフェース規定点 - 46 -
1.3 端末設備と電気通信回線設備の分界点 - 47 -
1.4 施工・保守上の責任範囲 - 47 -
2 ユーザ・網インタフェース仕様 - 48 -
2.1 プロトコル構成 - 48 -
2.2 物理レイヤ（レイヤ1）仕様 - 49 -
2.3 データリンクレイヤ（レイヤ2）仕様 - 50 -
2.4 レイヤ3仕様 - 50 -
2.5 上位レイヤ（レイヤ4～7）仕様 - 53 -
3 PPPoE / PPPプロトコル - 60 -
3.1 PPP - 60 -
3.2 PPPoE - 62 -
4 付属資料 - 74 -
4.1 ONU（スロット式）の概要 - 74 -
フレッツ 光WiFiアクセス編 - 75 -
1 フレッツ 光WiFiアクセス概要 - 76 -
1.1 サービスの概要 - 76 -
1.2 インタフェース規定点 - 76 -
1.3 端末設備と電気通信回線設備の分界点 - 77 -
1.4 施工・保守上の責任範囲 - 77 -
2 ユーザ・網インタフェース仕様 - 78 -

2.1　プロトコル構成 - 78 -
2.2　物理レイヤ（レイヤ1）仕様 - 79 -
2.3　データリンクレイヤ（レイヤ2）仕様 - 80 -
2.4　ネットワークレイヤ（レイヤ3）仕様 - 80 -
2.5　上位レイヤ（レイヤ4～7）仕様 - 80 -
3　フレッツ 光WiFiアクセスの通信シーケンス - 82 -
3.1　接続シーケンス - 82 -
3.2　接続失敗シーケンス - 83 -
フレッツ・ＶＰＮ ゲート - 84 -
1　フレッツ・ＶＰＮ ゲートの概要 - 85 -
1.1　サービスの概要 - 85 -
1.2　サービス品目 - 86 -
1.3　インタフェース規定点 - 87 -
1.4　端末設備と電気通信回線設備の分界点 - 89 -
1.5　施工・保守上の責任範囲 - 90 -
2　Ethernet/FastEthernetタイプのユーザ・網インタフェース仕様 - 93 -
2.1　プロトコル構成 - 93 -
2.2　レイヤ1仕様 - 94 -
2.3　レイヤ2仕様 - 95 -
2.4　レイヤ3仕様 - 95 -
2.5　上位レイヤ（レイヤ4～7）仕様 - 97 -
3　GigabitEthernetタイプのユーザ・網インタフェース仕様 - 98 -
3.1　プロトコル構成 - 98 -
3.2　レイヤ1仕様 - 98 -
3.3　レイヤ2仕様 - 99 -
3.4　レイヤ3仕様 - 99 -
3.5　上位レイヤ（レイヤ4～7）仕様 - 99 -
3.6　デュアルクラスに関わる仕様 - 100 -
4　10 GigabitEthernetタイプのユーザ・網インタフェース仕様 - 102 -
4.1　プロトコル構成 - 102 -
4.2　レイヤ1仕様 - 102 -
4.3　レイヤ2仕様 - 103 -
4.4　レイヤ3仕様 - 103 -
4.5　上位レイヤ（レイヤ4～7）仕様 - 103 -
5　認証関連通信 - 104 -
5.1　パケットフォーマット - 105 -
5.2　通信シーケンス例 - 106 -
5.3　通信用タイマ - 114 -
フレッツ・ＶＰＮ ワイド センタ回線接続サービス - 115 -
1　フレッツ・ＶＰＮ ワイド　センタ回線接続サービスの概要 - 116 -
1.1　サービスの概要 - 116 -
1.2　サービス品目 - 116 -
1.3　インタフェース規定点 - 117 -
1.4　端末設備と電気通信回線設備の分界点 - 122 -
1.5　施工・保守上の責任範囲 - 124 -
2　ユーザ・網インタフェース仕様 - 127 -
2.1　プロトコル構成 - 127 -
2.2　レイヤ1仕様 - 128 -

2.3　レイヤ2仕様 - 130 -
2.4　レイヤ3仕様 - 130 -
2.5　上位レイヤ（レイヤ4～7）仕様 - 131 -
フレッツ・キャスト編 - 132 -
1　フレッツ・キャストの概要 - 133 -
1.1　サービスの概要 - 133 -
1.2　サービス品目 - 133 -
1.3　インタフェース規定点 - 133 -
1.4　端末設備と電気通信設備の分界点 - 135 -
1.5　施工・保守上の責任範囲 - 136 -
2　フレッツ・キャストのユーザ・網インタフェース仕様 - 137 -
2.1　プロトコル構成 - 137 -
2.2　レイヤ1仕様 - 138 -
2.3　レイヤ2仕様 - 138 -
2.4　レイヤ3仕様 - 139 -
2.5　上位レイヤ（レイヤ4～7）仕様 - 142 -
3　品質規定に係る仕様 - 144 -
3.1　制御信号における転送品質クラス指定方法 - 144 -
3.2　データパケットに設定する転送優先度識別子 - 144 -
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 - 144 -
4　エンド側端末機器の利用条件 - 145 -
4.1　MLDv2 - 145 -
4.2　SIP、SDP - 150 -
4.3　CDN構成情報の取得 - 150 -

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。東日本電信電話株式会社（以下、NTT東日本）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

第1版　2008年3月31日制定

第2版　2008年8月18日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ・ＶＰＮ ゲート	○10Mb/s 品目の追加 ○発信側利用回線として、フレッツ 光ネクストに加え、フレッツ・ＩＳＤＮ、フレッツ・ＡＤＳＬ、Ｂフレッツを新たに追加
	フレッツ・ＶＰＮ ワイド センタ回線接続サービス	○全体を新たに追加

第3版　2008年10月2日制定

分冊	サービス名等	変更内容
第一分冊	Ｂフレッツ	○上位レイヤ（レイヤ 4～7）仕様の記述内容を修正 ○付属資料の記述内容を修正
	FLET'S.NetEX	○レイヤ 3 仕様の記述内容を修正 ○IPTV フォーラム技術仕様公開に伴う記述内容修正
第三分冊	フレッツ 光ネクスト	○フレッツ 光ネクスト ビジネスタイプの追加 ○付属資料の記述内容を修正
	フレッツ・キャスト	○IPTV フォーラム技術仕様公開に伴う記述内容修正

第4版　2008年12月18日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ネクスト	○PPPoE セッション数の記述内容修正

第5版　2009年2月4日制定

分冊	サービス名等	変更内容
第一分冊	Ｂフレッツ	○DHCPv6 における DUID 生成方式の記述を追加
第二分冊	M フレッツ	○M フレッツサービスの提供終了に伴うインタフェース条件の削除
第三分冊	フレッツ 光ネクスト	○DHCPv6 における DUID 生成方式の記述を追加 ○MLDv2 の記述内容を修正
	フレッツ・キャスト	○100Mb/s 品目等の追加 ○MLDv2 の記述内容を修正

第6版　2009年4月20日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ・ＶＰＮ ゲート	○Ethernet/FastEthernet タイプ 局外接続型の記述を追加 ○10 GigabitEthernet タイプの記述を追加

第7版　2009年9月16日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ・キャスト	○回線情報通知機能の提供に伴い上位レイヤ（レイヤ 4～7）仕様に HTTP、SSL の記述を追加

第8版　2009年10月1日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ネクスト	○フレッツ 光ネクスト 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追加

第9版　2010年2月10日制定

分冊	サービス名等	変更内容
第一分冊	Ｂフレッツ	○ワイヤレスアクセスタイプの削除
	フレッツ・オフィス／ フレッツ・オフィス ワイド	○ゲートウェイ機能に関する認証関連通信の記述を削除
第二分冊	フレッツ・オフィス ゲートウェイ機能	○ゲートウェイ機能の提供終了に伴うインタフェース条件の削除

第10版　2010年4月26日制定

分冊	サービス名等	変更内容
第一分冊	フレッツ・ＩＳＤＮ フレッツ・ＡＤＳＬ Ｂフレッツ	○PADS パケットの記述内容の変更 ○最大転送単位(MTU)の記述を追加
第三分冊	フレッツ 光ネクスト	○PADS パケットの記述内容の変更 ○PADO パケットに関する記述を追加 ○MLDv2 の記述内容の変更 ○最大転送単位(MTU)の記述を追加
	フレッツ・ＶＰＮ ゲート	○１Ｇ品目におけるデュアルクラスに関する記載の追加
	フレッツ・キャスト	○MLDv2 の記述内容の変更 ○ICMPv6 に関する記述を追加

第11版　2010年7月1日制定

分冊	サービス名等	変更内容
第一分冊	Ｂフレッツ	○ファミリータイプの削除

第12版　2011年2月21日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ネクスト	○DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得に関する記述の変更

第13版　2011年5月16日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ライト	○フレッツ 光ライトの追加

第14版　2011年6月1日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ネクスト	○IPv6 仕様に関する記述の追加 ○PPPoE 接続での IPv6 通信に関する記述の追加 ○経路情報サーバに関する記述の追加
	フレッツ・キャスト	○IPv6 パケットフォーマットに関する記述の変更

第15版　2011年7月11日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ・ＶＰＮ ゲート	○ユーザ認証代行機能の追加に伴い、認証関連の記載を変更

第16版　2011年7月21日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ネクスト	○IPv6 仕様に関する記述の追加 ○経路情報提供サーバに関する記述の追加

第17版　2012年2月22日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ネクスト	○IPv6 仕様に関する記述の追加
	フレッツ 光ライト	○IPv6 仕様に関する記述の追加

第18版　2012年5月17日制定

分冊	サービス名等	変更内容
第一分冊	フレッツ・ＡＤＳＬ Ｂフレッツ	○PADO パケットに関する記述を追加

第19版　2012年6月26日制定

分冊	サービス名等	変更内容
第二分冊	フレッツ・アクセスポート	○フレッツ・アクセスポート提供終了に伴うインタフェース条件の削除

第20版　2012年11月1日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光 WiFi アクセス	○フレッツ 光 WiFi アクセスの追加

第21版　2013年1月7日制定

分冊	サービス名等	変更内容
第一分冊	フレッツ・オンデマンド	○フレッツ・オンデマンド提供終了に伴うフレッツ・オンデマンド（サーバ持込型）の削除
第三分冊	フレッツ・ＶＰＮ ゲート フレッツ・ＶＰＮ ワイド	○フレッツ・ＶＰＮ ゲートの認証パラメータの注意事項を追加 ○フレッツ・ＶＰＮ ゲートとフレッツ・ＶＰＮ ワイドの SAS（RFC6598）の非対応について

第22版　2013年4月1日制定

分冊	サービス名等	変更内容
第二分冊	FdN ナンバー	○FdN ナンバー提供終了に伴う FdN ナンバーに関する記載の削除

第23版　2013年10月1日制定

分冊	サービス名等	変更内容
第三分冊	フレッツ 光ライト	○IPv6 仕様に関する記述の追加

第24版　2014年1月6日制定

分冊	サービス名等	変更内容
第一分冊	FLETS'.Net EX	○FLET'S.Net EX の提供終了に伴う FLET'S.Net EX に関する記載の削除
第二分冊	FLET'S.Net	○FLET'S.Net の提供終了に伴う FLET'S.Net に関する記載の削除

第25版　2014年3月11日制定

分冊	サービス名等	変更内容
第二分冊	フレッツ・スポット	○提供役務の変更による仕様の変更

第26版　2014年3月24日制定

分冊	サービス名等	変更内容
第一分冊	Ｂフレッツ	○DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得に関する記述の変更 ○DNS に関する記述の変更 ○SNTP に関する記述の追加
第三分冊	フレッツ 光ネクスト	○IPv6 アドレス情報付与方法に関する記述の変更 ○帯域優先に関する記載の追加

「IP通信網サービスのインタフェース ―フレッツシリーズ―」は、以下の構成となっております。

技術参考資料名	分冊	掲載サービス名
IP 通信網サービスのインタフェース ― フレッツシリーズ ―	第一分冊	フレッツ・ＩＳＤＮ フレッツ・ＡＤＳＬ Ｂフレッツ フレッツ・オフィス／フレッツ・オフィス ワイド
	第二分冊	フレッツ・スポット
	第三分冊	フレッツ 光ネクスト フレッツ 光ライト フレッツ 光 WiFi アクセス 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 フレッツ・キャスト

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)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。

(9)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。

(10)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。

(11)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。

(12)IPパケット
IPで扱われるメッセージ転送単位です。

(13)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。

(14)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。

(15)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。

(16)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。

(17)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。

(18)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。

(19)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。

(20)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。

(21)SDP (Session Description Protocol)
端末ー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。

(22)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。

(23)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。

(24)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。

(25)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。

(26)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。

(27)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。

(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 光ネクスト編

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。

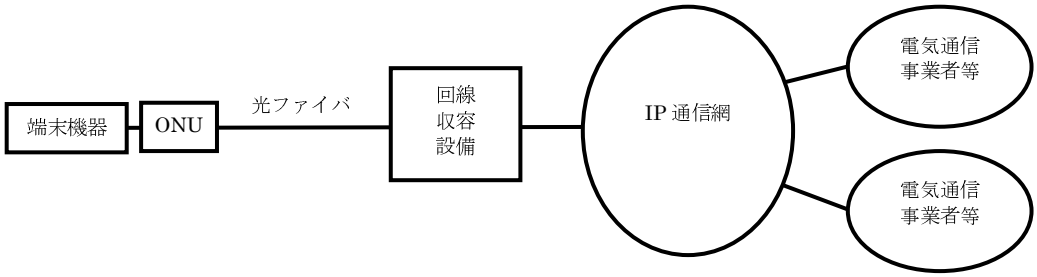


図 1-1 フレッツ 光ネクストの基本構成

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。

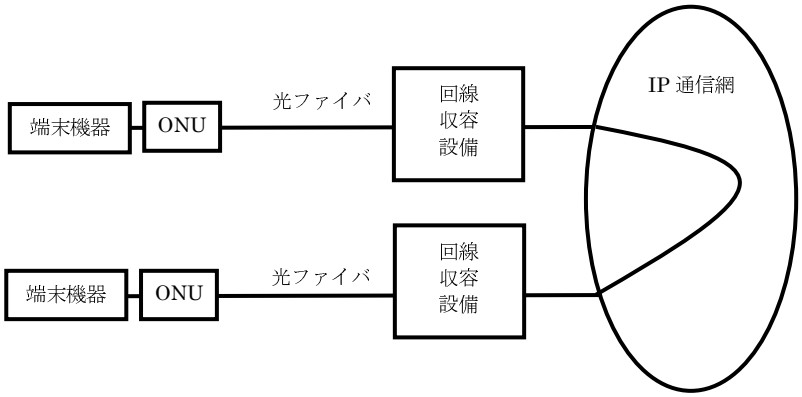


図 1-2 フレッツ・v6オプションの契約者同士の通信

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。

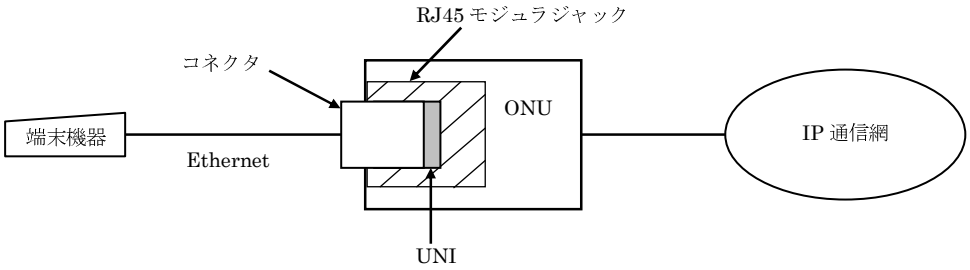


図 1-3 インタフェース規定点

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。

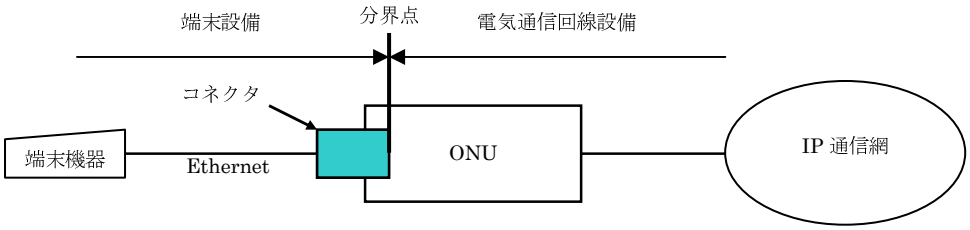


図 1-4 分界点

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。

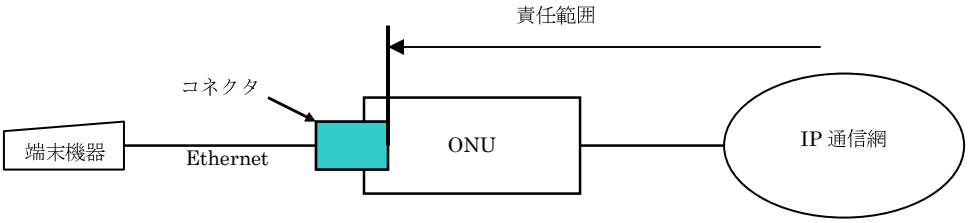


図 1-5 施工・保守上の責任範囲

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 プロトコル構成

レイヤ		使用するプロトコル		
		IPv6		IPv4
		IPoE 通信	PPPoE 接続	PPPoE 接続
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 DS Field : RFC2474	IPv6: RFC2460/ RFC3513 ICMPv6: RFC2463	IPv4: RFC791 ICMPv4: RFC792
2	データリンク	MAC: IEEE802.3-2005	PPPoE: 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
プライオ１０、プライオ１	10BASE-T、100BASE-TX または 1000BASE-T（Auto-MDI/MDI-X）(注)	自動折衝機能（Auto Negotiation）(注)
ビジネスタイプ		
ファミリー・ハイスピードタイプ	10BASE-T、100BASE-TX または 1000BASE-T（Auto-MDI/MDI-X）(注)	
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)	
マンションタイプ		

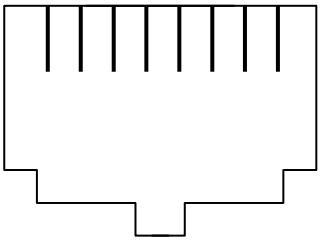
(注) インタフェースと通信モードはONUの自動折衝機能（Auto Negotiation）により決定します。

2.2.1 インタフェース条件

ユーザ・網インタフェースは、ISO8877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。

RJ-45ポート挿入面

ピン番号 1 2 3 4 5 6 7 8



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[3.1 PPP]と[3.2 PPPoE]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をサポートします。また、RFC2460に規定されているIPv6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。

PPPoE接続では、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。また、IPv6のサブセットとして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の一部、またはすべてをサポートします。

IPv6（IPoE）通信については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(IPoE)通信とPPPoE接続におけるIPv6通信の2つをサポートとしています。IPv6(IPoE)通信については[2.4.2.1 IPv6(IPoE)通信におけるIPv6仕様]を、PPPoE接続におけるIPv6通信については[2.4.2.2 PPPoE接続におけるIPv6仕様]をご参照下さい。

2.4.2.1 IPv6(IPoE)通信における IPv6 仕様

IPv6(IPoE)通信においては、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 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 IPv6(IPoE)通信における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 IPv6(IPoE)通信における 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は1が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、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グローバル・ユニキャストアドレス、またはDHCPv6-PDを使用してIP通信網から送信するメッセージに含まれる48bitまたは56bit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。

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 DHCPv6 によるレイヤ 3 情報（網内サーバ）の自動取得

IPv6(IPoE)通信では端末機器は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 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 最大転送単位（MTU）

IP通信網におけるIPv6(IPoE)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。

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。

2.4.2.1.6.1　　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

2.4.2.1.6.2　　マルチキャスト受信継続確認シーケンス例

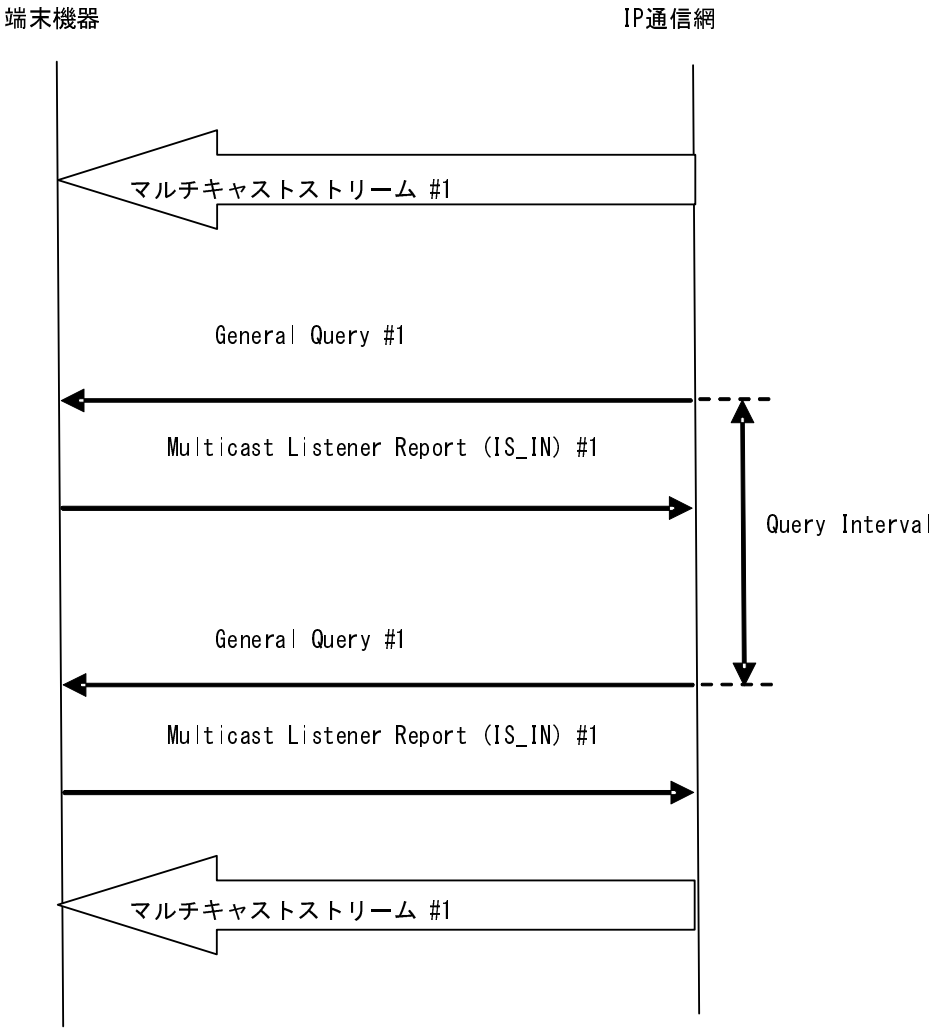


図 2-3 マルチキャスト受信継続確認シーケンス例

2.4.2.1.6.3　　チャネル切り替えシーケンス例

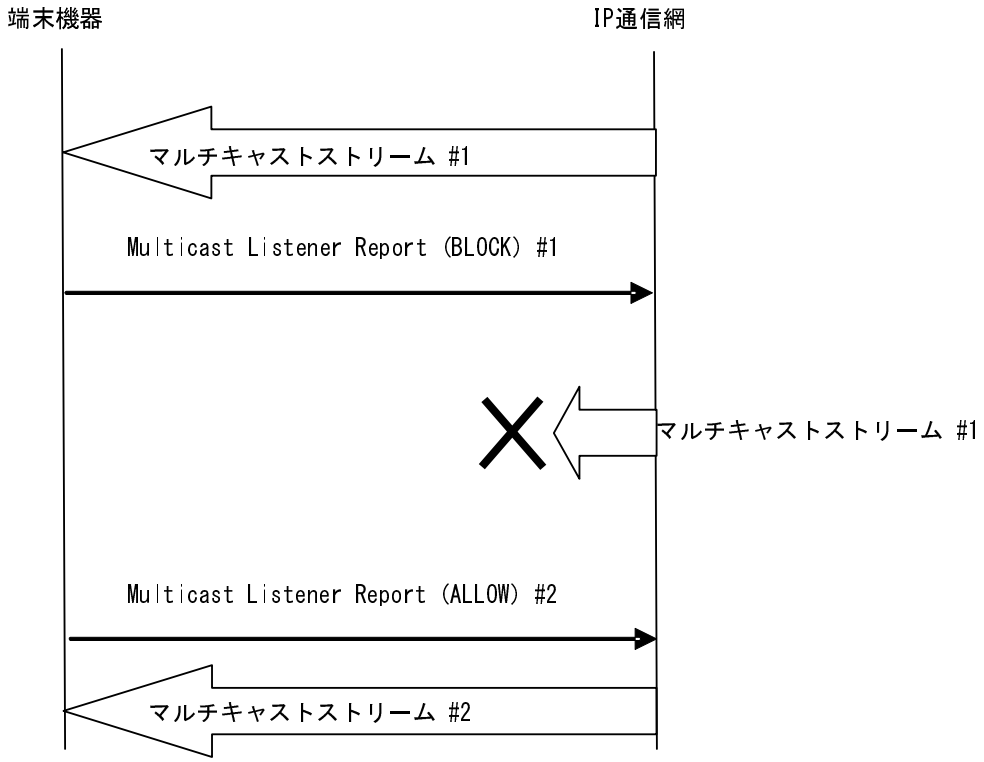


図 2-4 チャネル切り替えシーケンス例

2.4.2.1.6.4 マルチキャスト受信停止シーケンス例

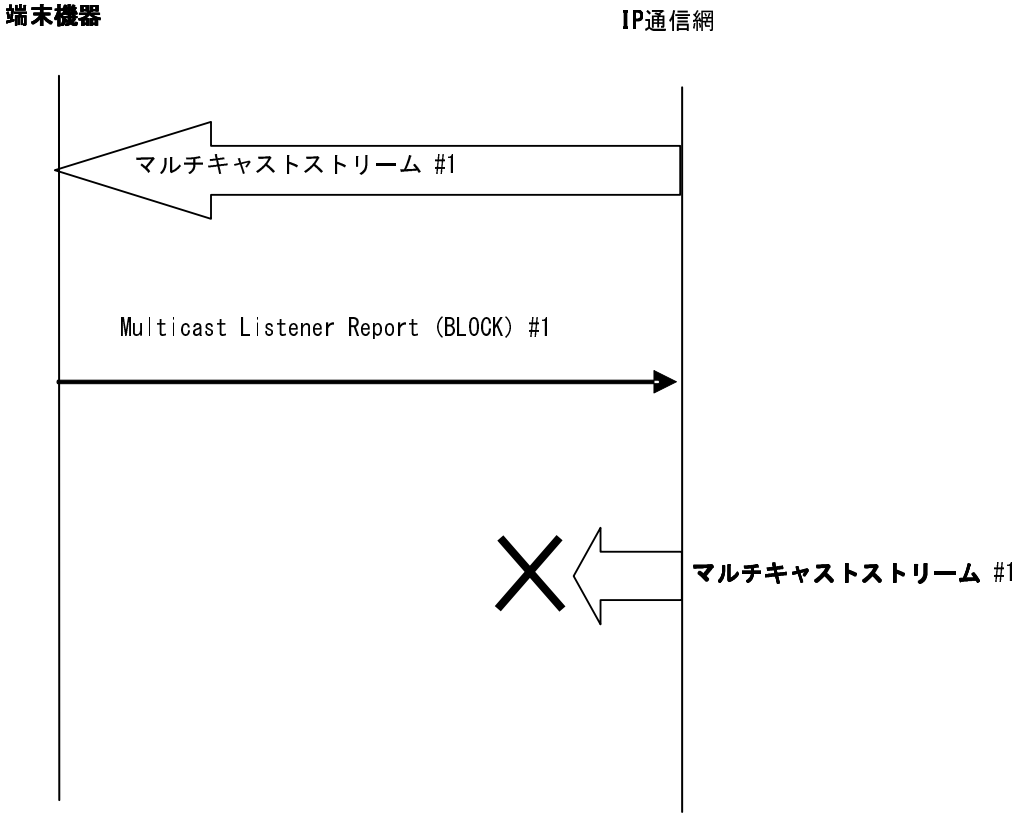


図 2-5 マルチキャスト受信停止シーケンス例

2.4.2.2 PPPoE 接続における IPv6 仕様

PPPoE接続においては、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 (IPv6Addressing 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通信網は転送を保障できない場合があります。

2.4.2.2.1 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接続における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 接続における IPv6 アドレス情報付与方法

IP通信網はRFC3315、RFC3633で規定されるDHCPv6-PDに基づき、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 接続におけるレイヤ 3 情報（網内サーバ）の自動取得

PPPoE接続では端末機器は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事が可能です。仕様に関する詳細はRFCを参照してください。

2.4.2.2.4 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 最大転送単位(MTU)

IP通信網におけるPPPoE接続でのIPv6 通信のMTU の値は1,454byte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。

2.4.4 帯域優先に関する仕様

契約帯域の範囲で優先クラスを利用したIPv6(IPoE)通信が可能となるサービスにて、当該サービス契約者の端末機器からIP通信網に送信されるIPv6パケットにおいて、RFC2474に規定される優先度の指定が可能です。当該サービス契約者の端末機器からIP通信網に送信されるIPv6パケット(IPoE方式）のトラヒッククラスフィールドの先頭6ビットに、DSCP値として8(001000)を指定することで、優先トラヒックとして転送します。
尚、指定された優先度以外が設定されたパケットの転送は保証しません。

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、DHCPv6、DHCPv6-PDのみ規定します。なお、IPv6(IPoE)通信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IPv6(IPoE)通信は[2.4.2.1.3 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 DHCPv6におけるDUID生成方式]を、PPPoE接続は[2.4.2.2.3 PPPoE接続におけるレイヤ3情報（網内サーバ）の自動取得]および[2.4.2.2.4 DHCPv6におけるDUID生成方式]を参照してください。DHCPv6-PDについてはIPv6(IPoE)通信は[2.4.2.1.2 IPv6(IPoE)通信におけるIPv6アドレス情報付与方法]を、PPPoE接続は[2.4.2.2.2 PPPoE接続における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 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通信網で利用できるHTTPサーバは、経路情報提供サーバがあります。経路情報提供サーバの利用条件は[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を参照してください。

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-east.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 メソッド	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フォーマットを表 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トコンテンツタイプ	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/省略可能	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）	I Pv6 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	東日本	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。

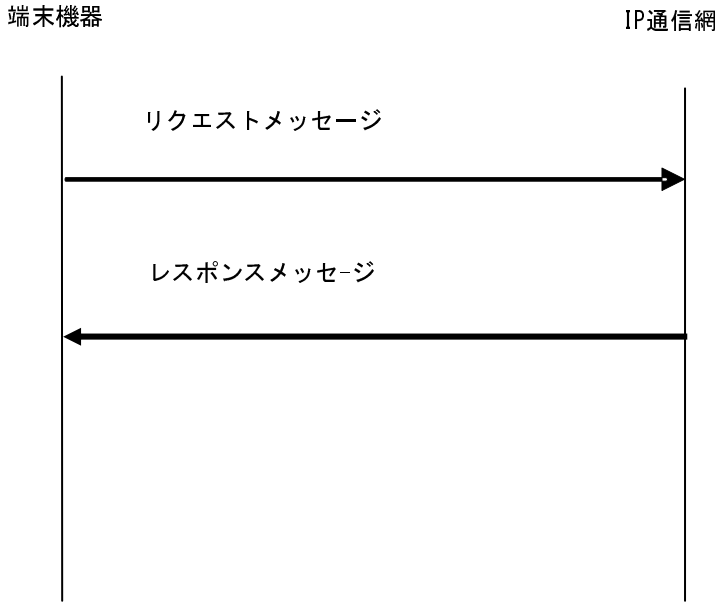


図 2-9経路情報提供サーバとの通信シーケンス

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
0x0057	Internet Protocol version6 （IPv6）	レイヤプロトコル

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 IPCPv6 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。

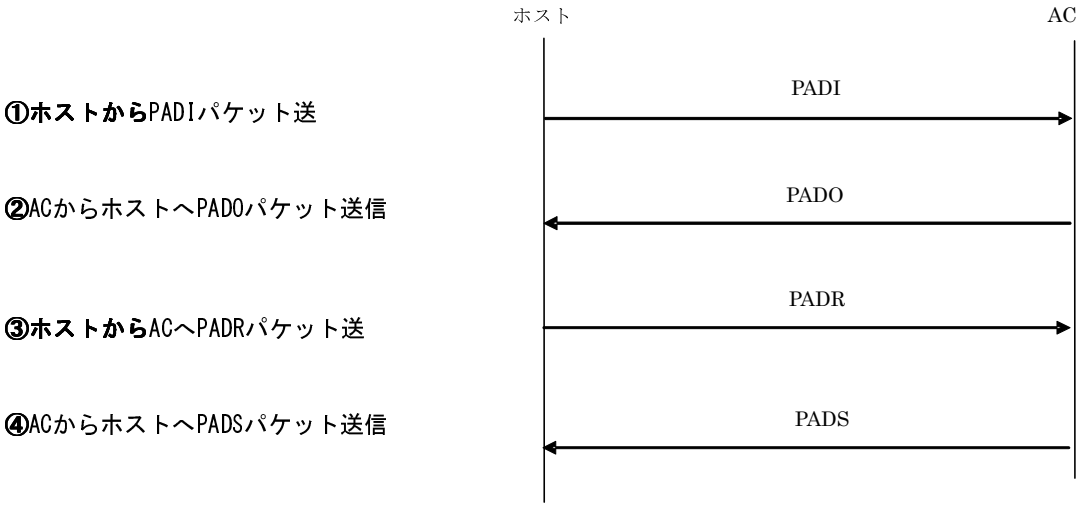


図 3-1 PPPoE セッション確立手順

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タグとと同一の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 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）
ビジネスタイプ	2 ／ 20
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）

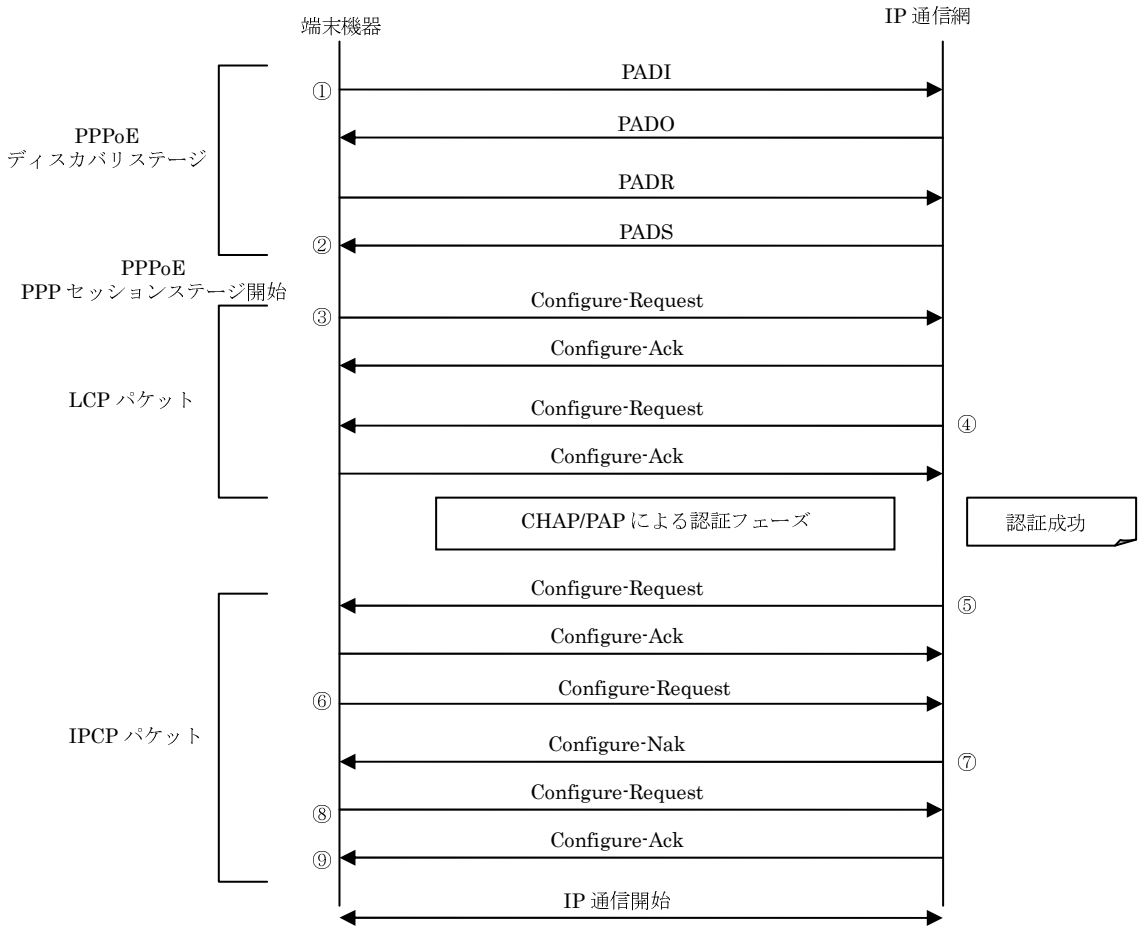


図 3-2　接続シーケンス（例）

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）

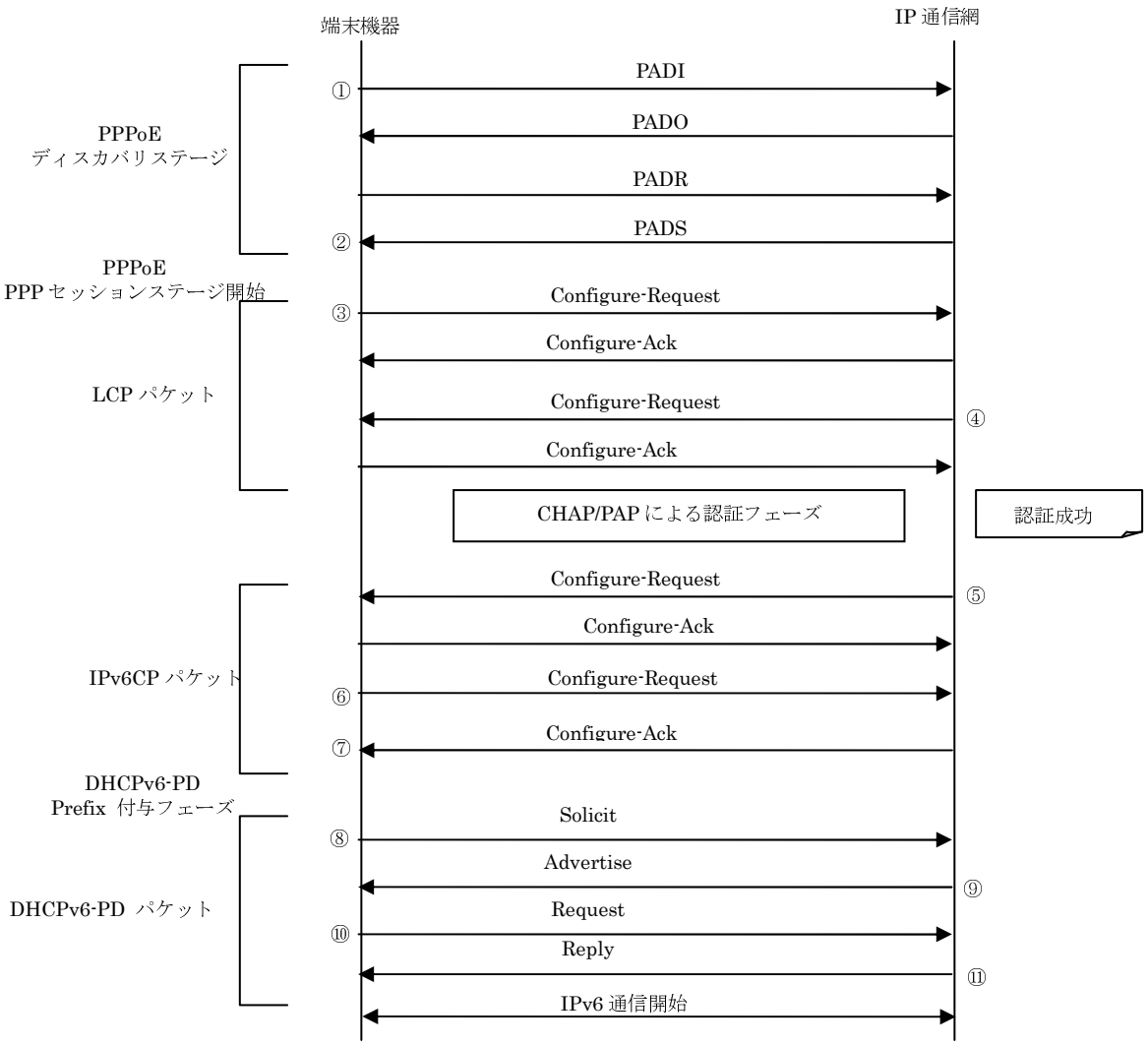


図 3-3　接続シーケンス（例）

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

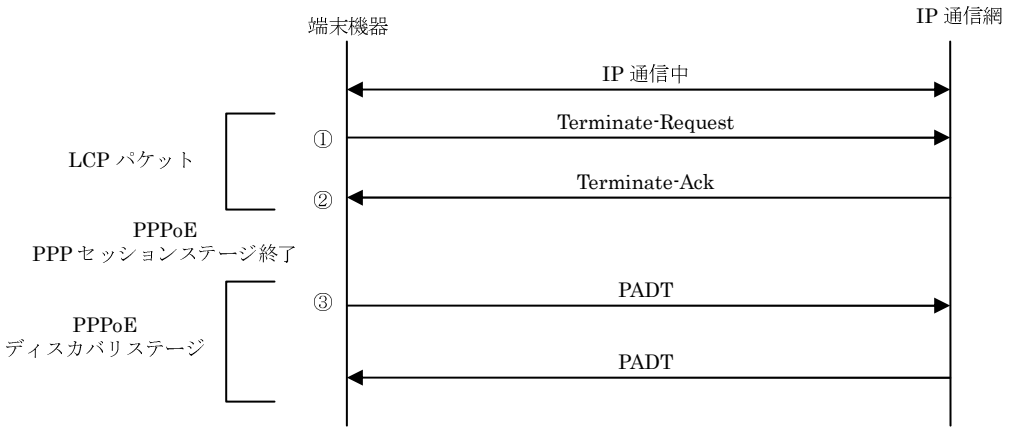


図 3-4　切断シーケンス（例）

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

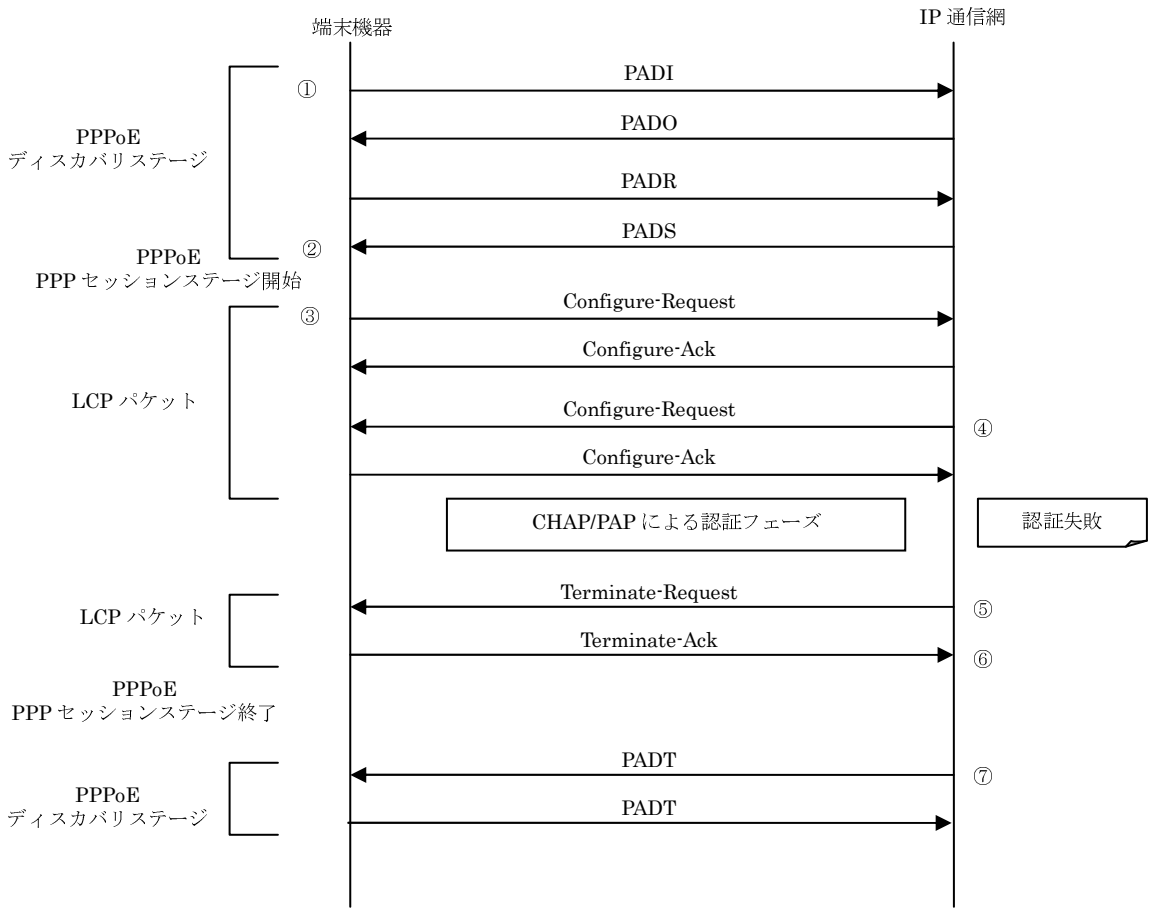


図 3-5　認証失敗シーケンス（例）

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

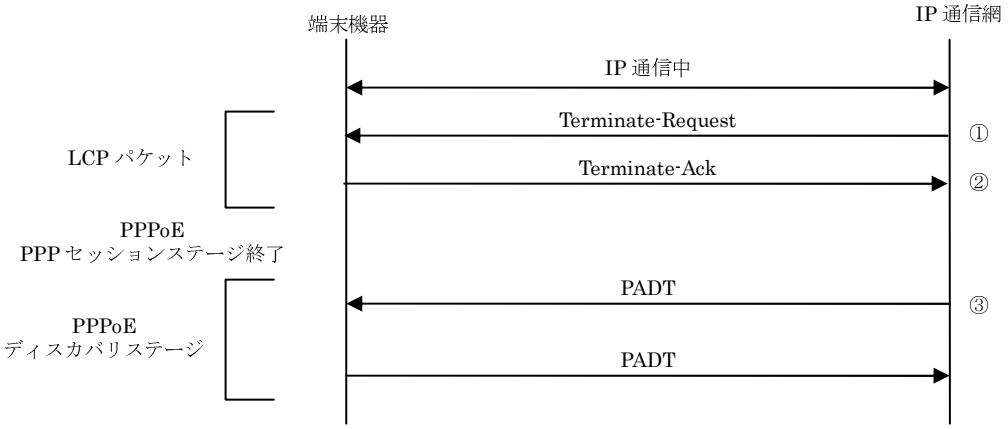


図 3-6　強制切断シーケンス（例）

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。

ONU（スロット式）

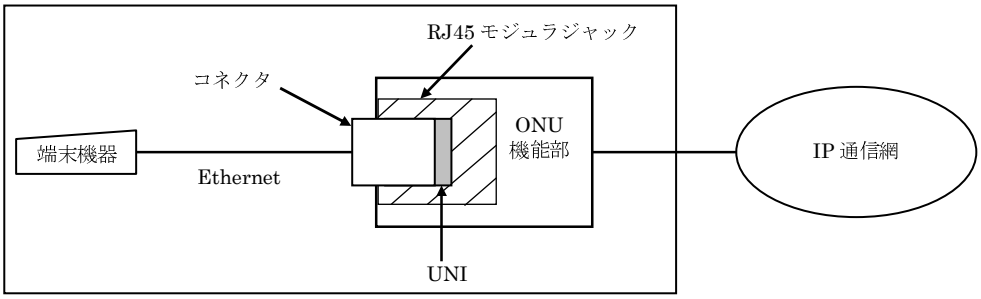


図 4-1 インタフェース規定点

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。

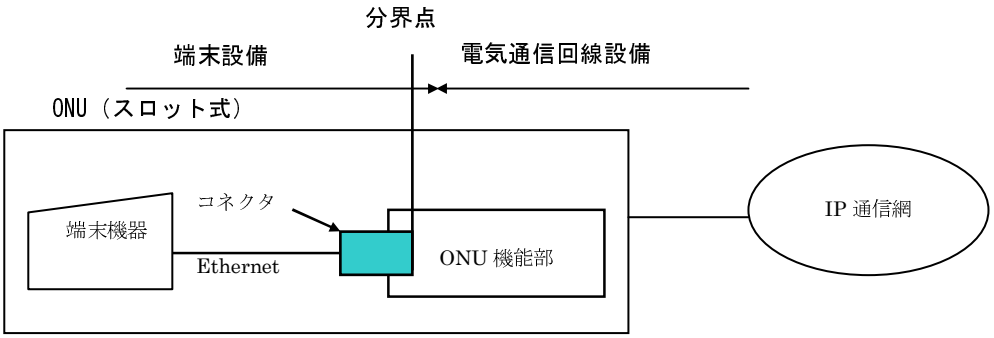


図 4-2 分界点

フレッツ 光ライト編

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。

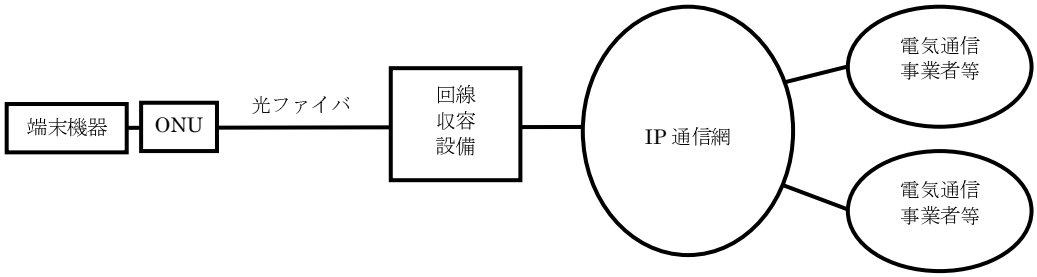


図 1-1 フレッツ 光ライトの基本構成

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。

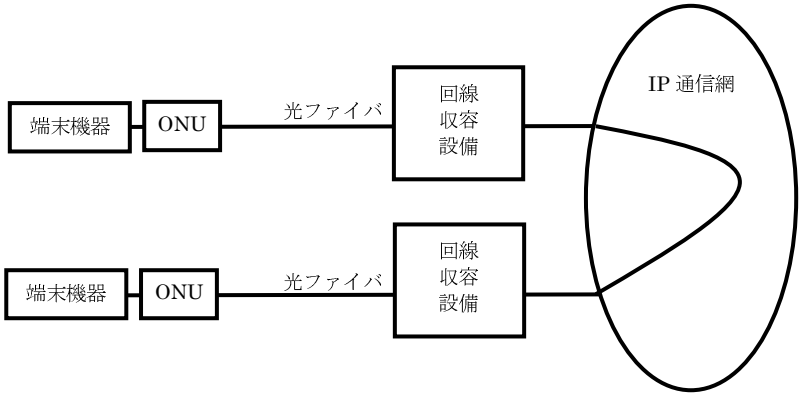


図 1-2 フレッツ・v6オプションの契約者同士の通信

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。

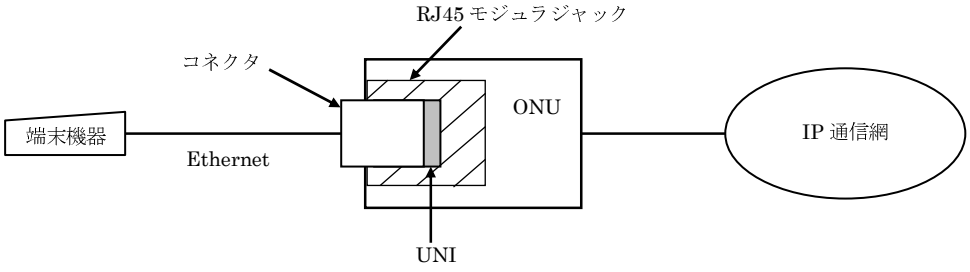


図 1-3 インタフェース規定点

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。

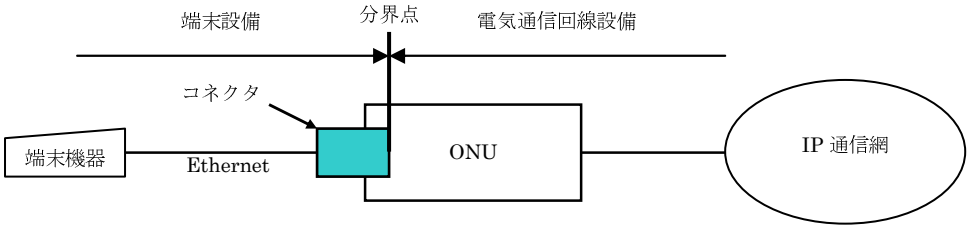


図 1-4 分界点

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。

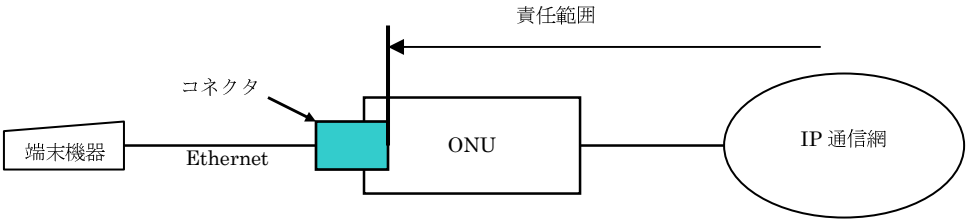


図 1-5 施工・保守上の責任範囲

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

<table>
<tr><td colspan="2" rowspan="3">レイヤ</td><td colspan="3">使用するプロトコル</td></tr>
<tr><td colspan="2">IPv6</td><td>IPv4</td></tr>
<tr><td>IPoE 通信</td><td>PPPoE 接続</td><td>PPPoE 接続</td></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</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:
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 マンションタイプ	10BASE-T または 100BASE-TX （Auto-MDI/MDI-X）(注)	自動折衝機能 （Auto Negotiation） (注)

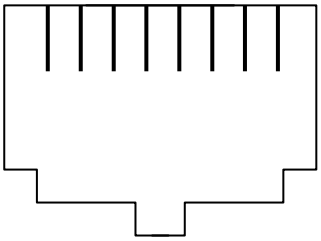
（注） インタフェースと通信モードはONUの自動折衝機能（Auto Negotiation）により決定します。

2.2.1 インタフェース条件

ユーザ・網インタフェースは、ISO8877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。

RJ-45ポート挿入

ピン番 1 2 3 4 5 6 7 8



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]、[2.4.12 IPv4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(IPoE)通信とPPPoE接続におけるIPv6通信の2つをサポートとしています。IPv6(IPoE)通信については[2.4.2.1 IPv6(IPoE)通信におけるIPv6仕様]を、PPPoE接続におけるIPv6通信については[2.4.2.2 PPPoE接続におけるIPv6仕様]をご参照下さい。

2.4.2.1 IPv6(IPoE)通信における IPv6 仕様

IPv6(IPoE)通信においては、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 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 IPv6(IPoE)通信における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 IPv6(IPoE)通信における 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は1が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、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グローバル・ユニキャストアドレス、またはDHCPv6-PDを使用してIP通信網から送信するメッセージに含まれる48bitまたは56bit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。

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 DHCPv6 によるレイヤ 3 情報 (網内サーバ) の自動取得

IPv6(IPoE)通信では端末機器は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 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 最大転送単位（MTU）

IP通信網におけるIPv6(IPoE)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 接続における IPv6 仕様

PPPoE接続においては、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 （IPv6Addressing 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通信網は転送を保障できない場合があります。

2.4.2.2.1 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接続における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 接続における IPv6 アドレス情報付与方法

IP通信網はRFC3315、RFC3633で規定されるDHCPv6-PDに基づき、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 接続におけるレイヤ 3 情報（網内サーバ）の自動取得

PPPoE接続では端末機器は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事が可能です。仕様に関する詳細はRFCを参照してください。

2.4.2.2.4 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 最大転送単位(MTU)

IP通信網におけるPPPoE接続でのIPv6 通信のMTU の値は1,454byte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。なお、IPv6(IPoE)通信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IPv6(IPoE)通信は[2.4.2.1.3　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 DHCPv6におけるDUID生成方式]を、PPPoE接続は[2.4.2.2.3 PPPoE接続におけるレイヤ3情報（網内サーバ）の自動取得]および[2.4.2.2.4 DHCPv6におけるDUID生成方式]を参照してください。DHCPv6-PDについてはIPv6(IPoE)通信は[2.4.2.1.2 IPv6(IPoE)通信におけるIPv6アドレス情報付与方法]を、PPPoE接続は[2.4.2.2.2 PPPoE接続における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通信網で利用できるHTTPサーバは、経路情報提供サーバがあります。経路情報提供サーバの利用条件は[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を参照してください。

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-east.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 2-62、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 2-2 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 メソッド	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 2-73に、ステータスラインおよびレスポンスヘッダのフォーマットを表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。

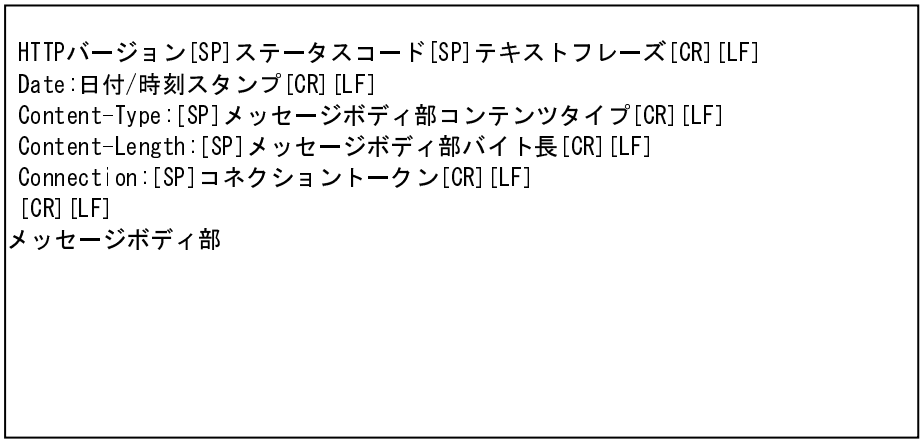


図 2-3 レスポンスメッセージのフォーマット

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トコンテンツタイプ	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を図 2-84に、構成要素を表 2-109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/省略可能	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）	I Pv6 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 2-110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	東日本	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 2-95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 2-121を参照してください。

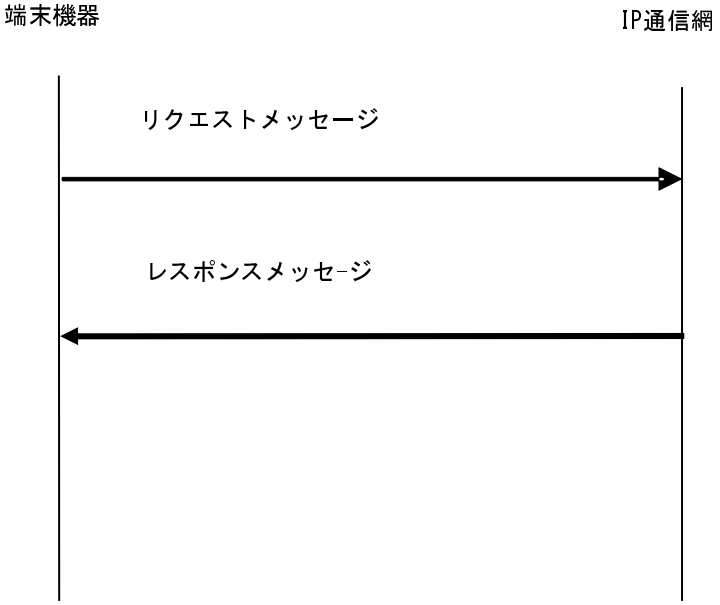


図 2-5経路情報提供サーバとの通信シーケンス

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
0x0021	Internet Protocol（IP）	ネットワーク レイヤプロトコル

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 IPCPv6 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。

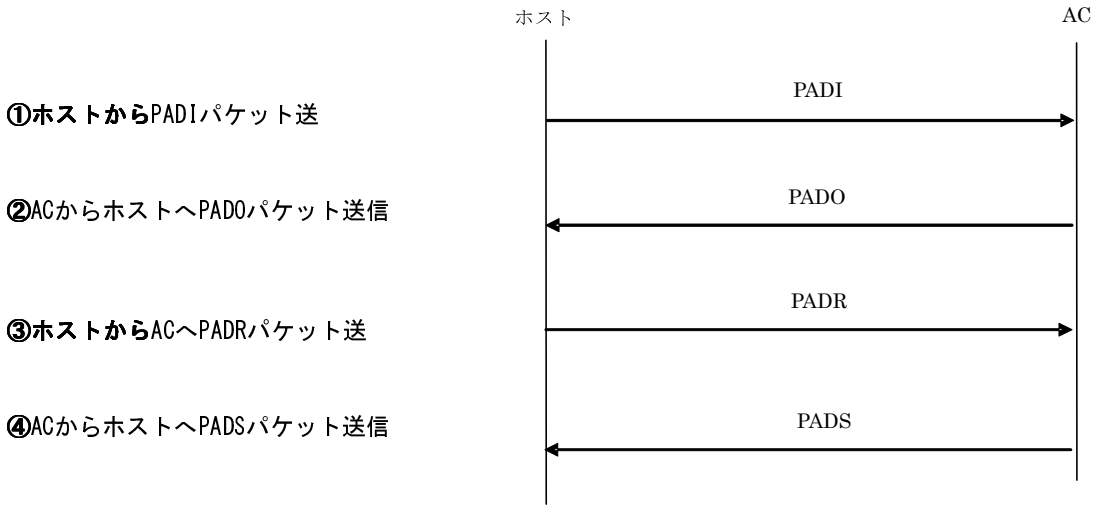


図 3-1 PPPoE セッション確立手順

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タグとと同一の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～図 3-6に示します。

3.2.6.1　　接続シーケンス（IPv4 通信）

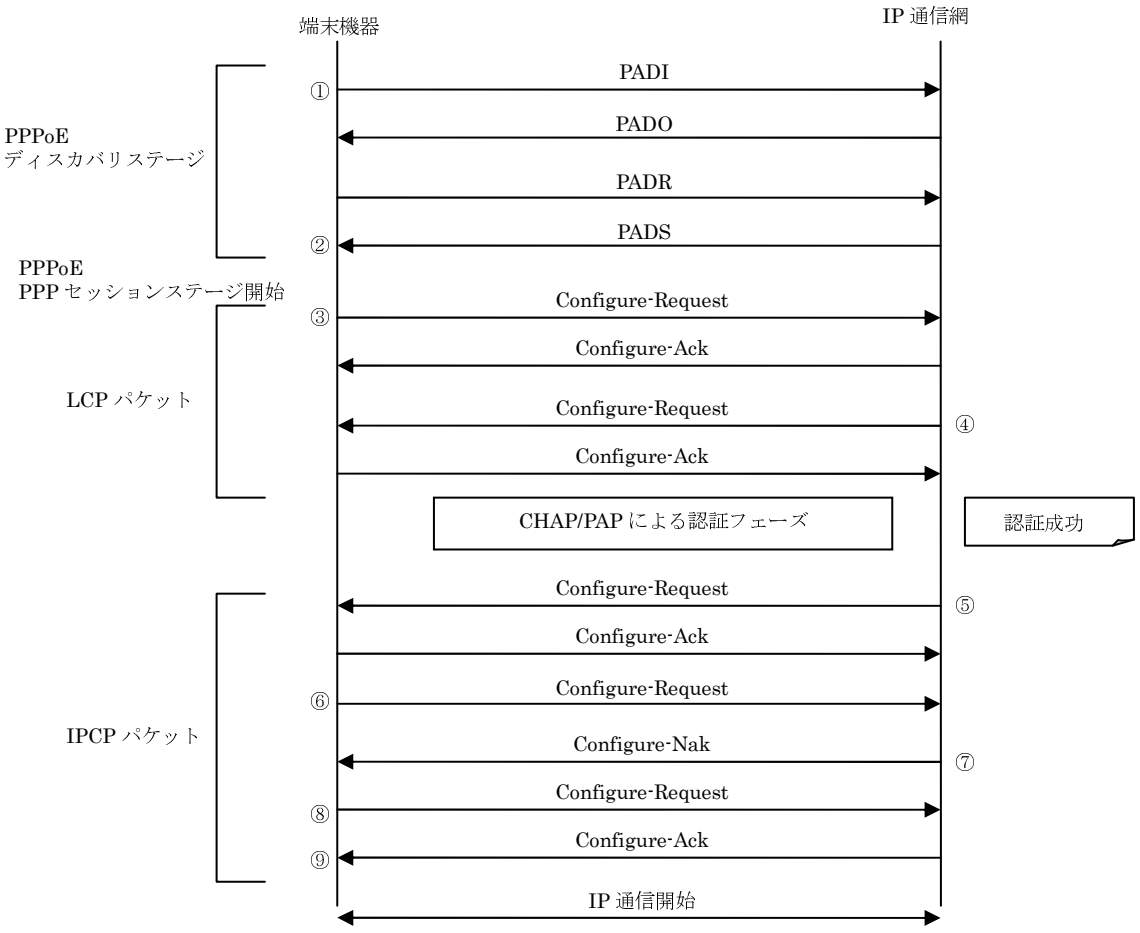


図 3-2　接続シーケンス（例）

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）

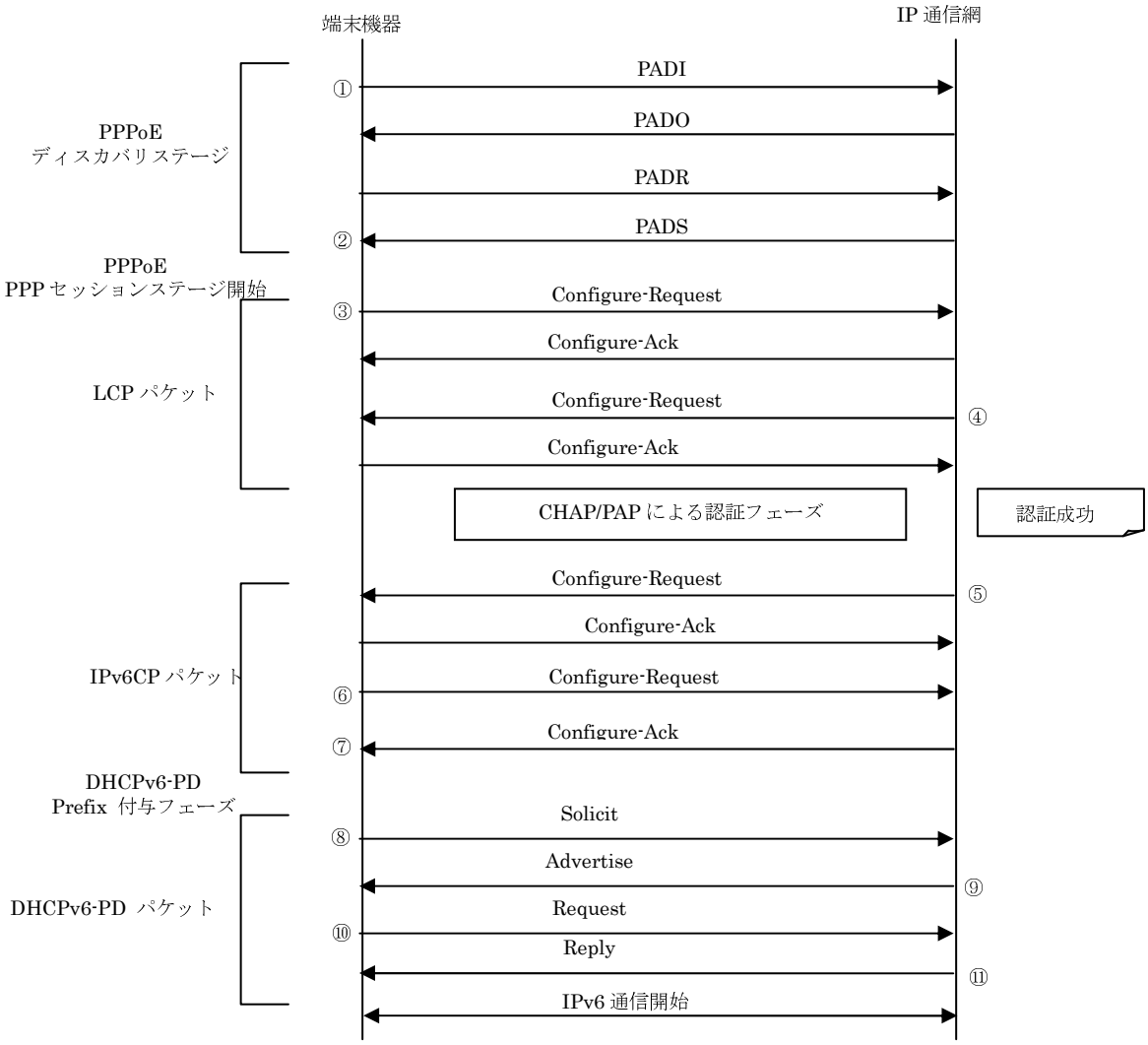


図 3-3　接続シーケンス（例）

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

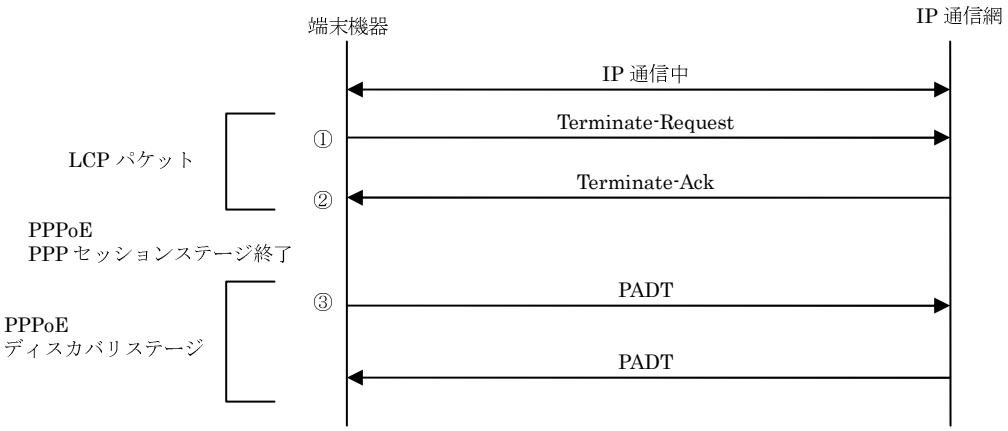


図 3-4　切断シーケンス（例）

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

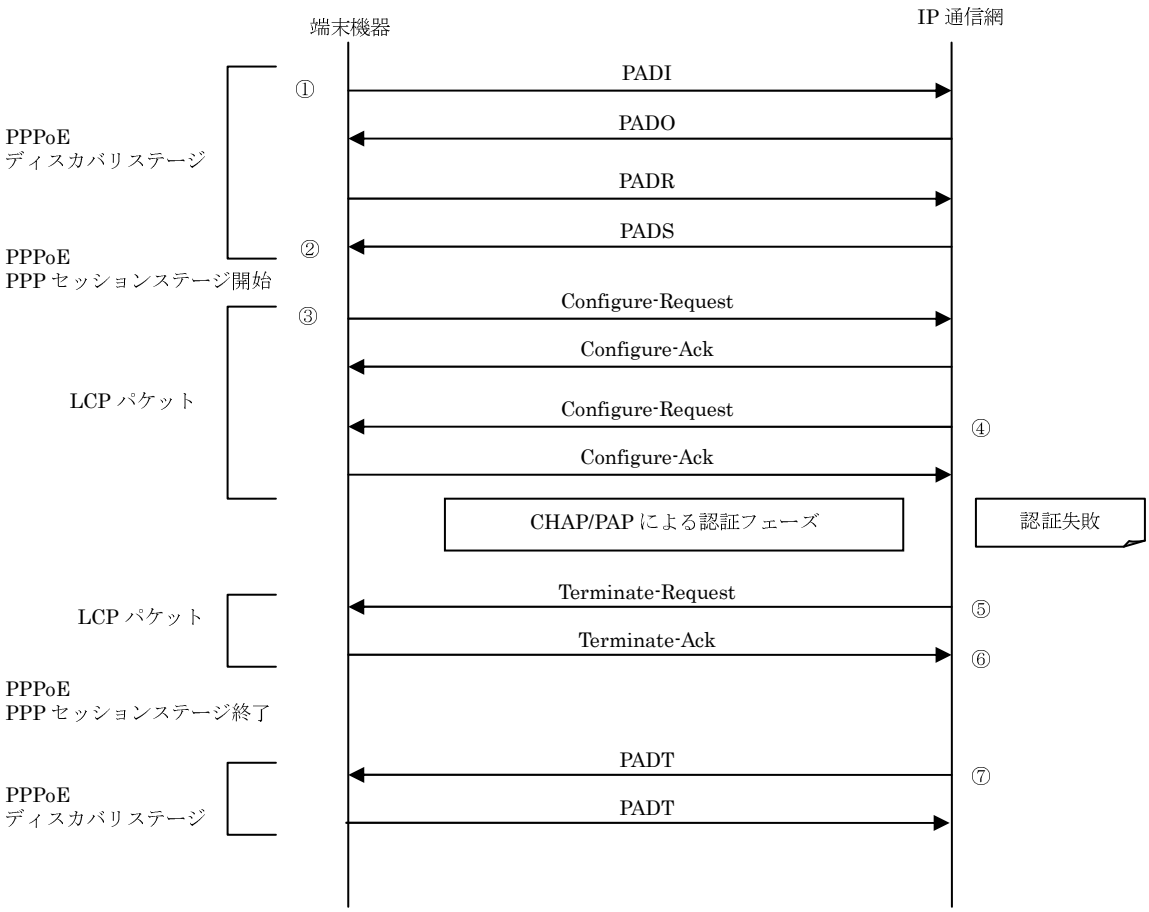


図 3-5 認証失敗シーケンス（例）

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

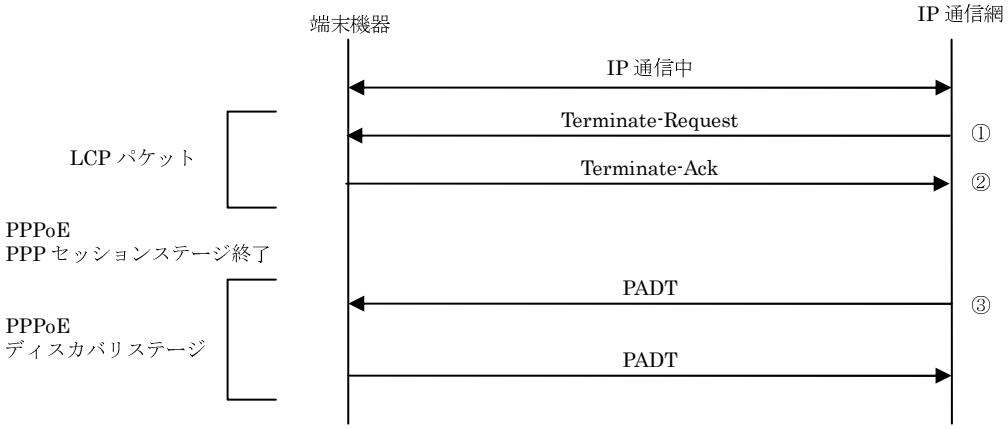


図 3-6　強制切断シーケンス（例）

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。

ONU（スロット式）

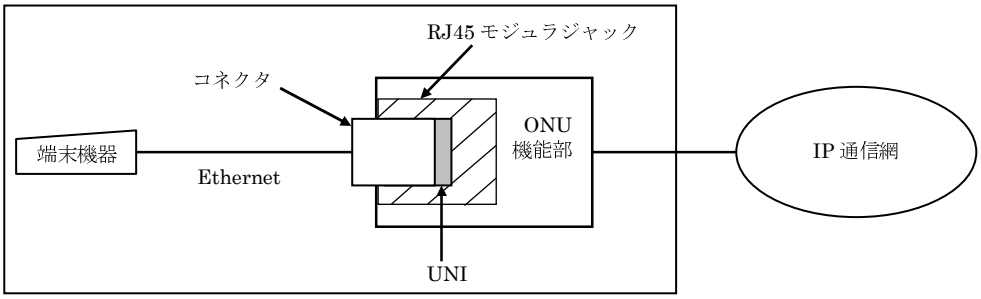


図 4-1 インタフェース規定点

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。

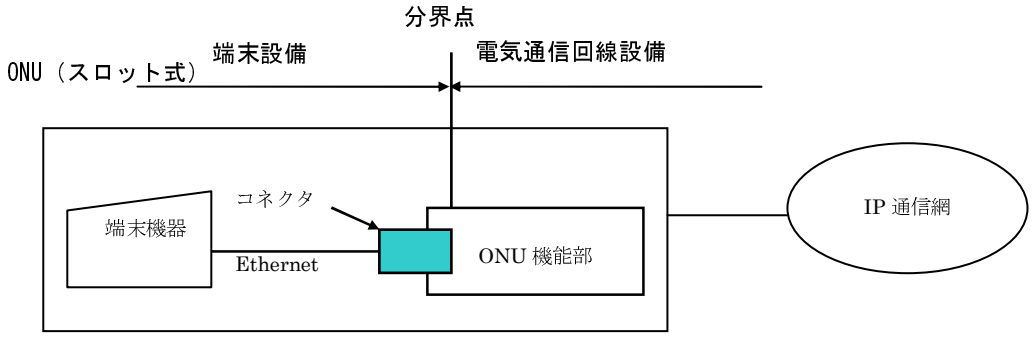


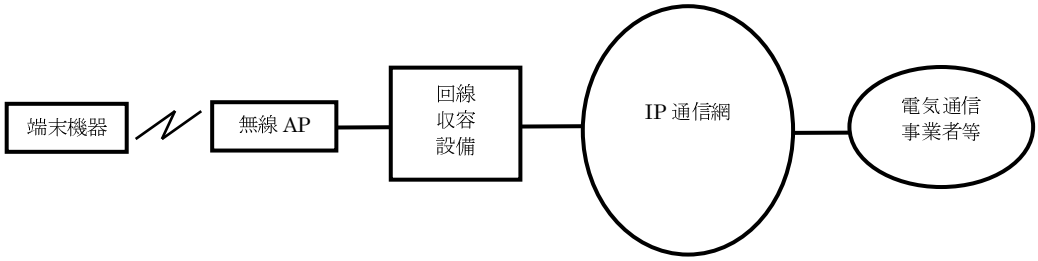
図 4-2 分界点

フレッツ 光 WiFi アクセス編

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、電気通信事業者等については、フレッツ 光WiFiアクセス装置ごとに、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。

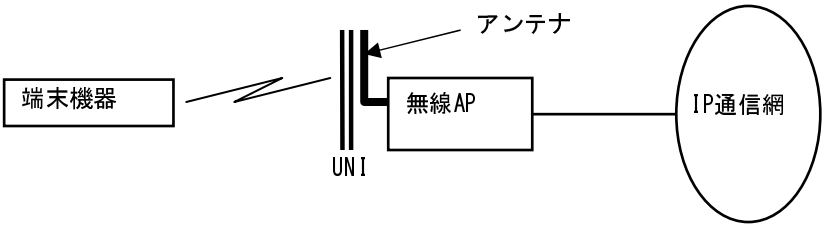


図 1-2 インタフェース規定点

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。

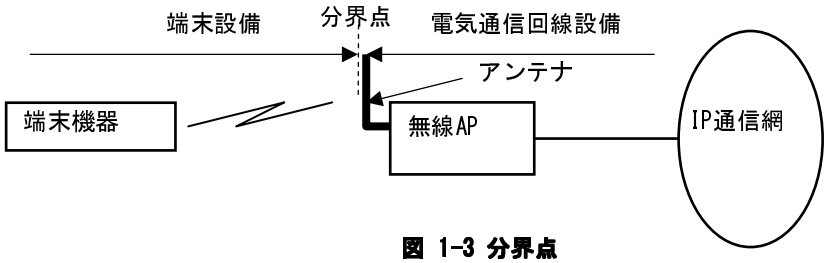


図 1-3 分界点

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。

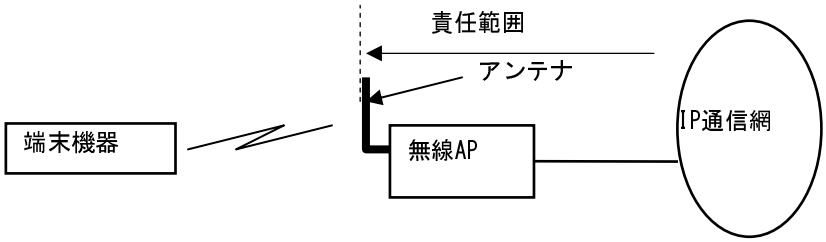


図 1-4 施工・保守上の責任範囲

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)
1	物理	IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n, ARIB STD-T71/STD-T66

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IEEE802.11a（Wi-Fi認定）、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	802.11a	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
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
伝送速度[Mbps](注)	802.11a	最大54Mbps
	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	802.11a	OFDM
	802.11b	DSSS
	802.11g	OFDM
	802.11n	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2-5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2-5 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 equirements for Internet	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サーバは、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2-6 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
3	FQDN	wifi.e-flets.jp

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

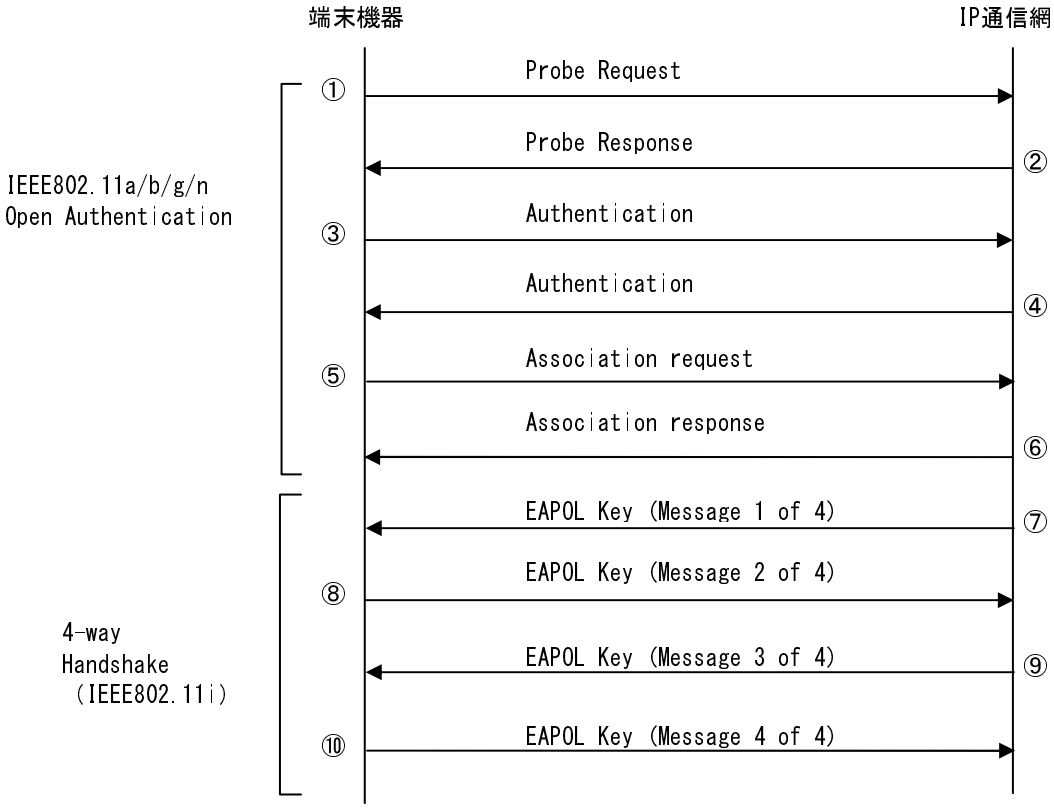


図3-1 接続シーケンス（例）

［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

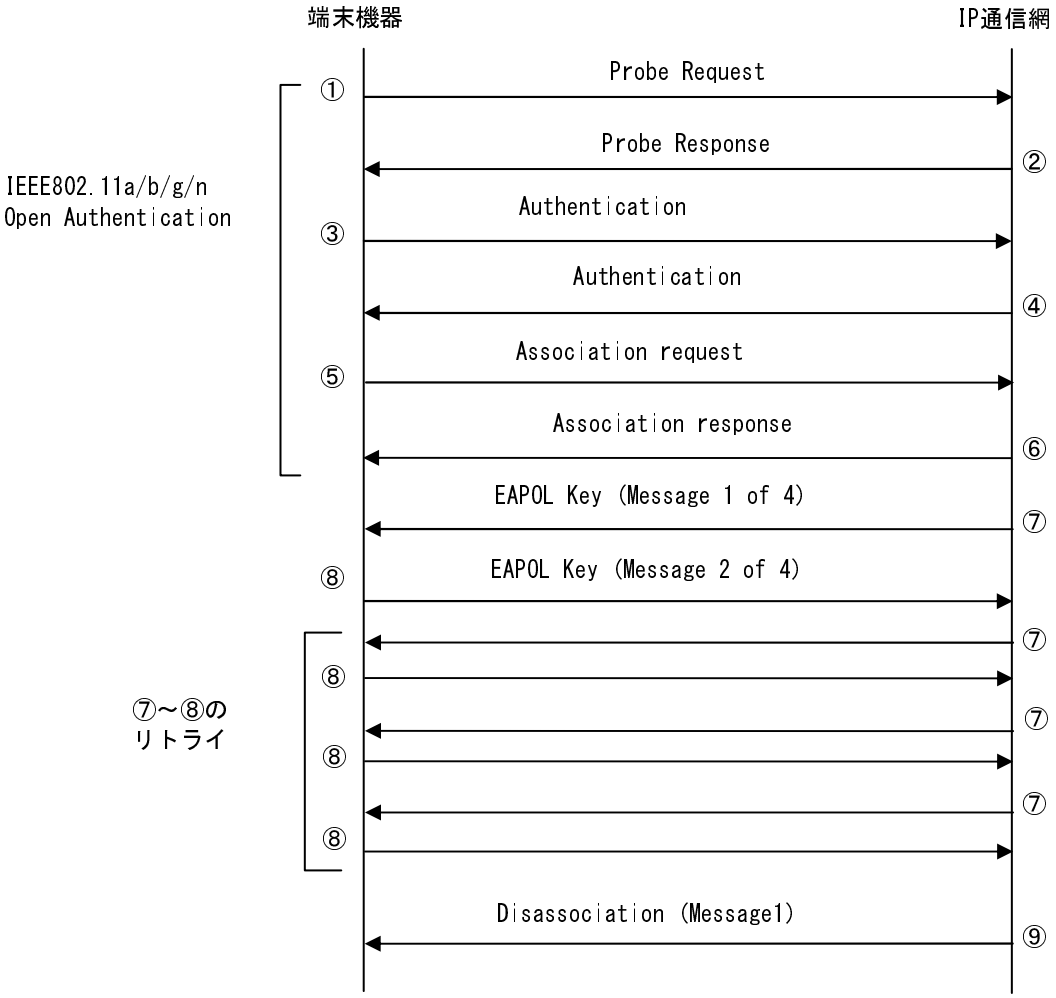


図 3-2 接続失敗シーケンス（例）

［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。

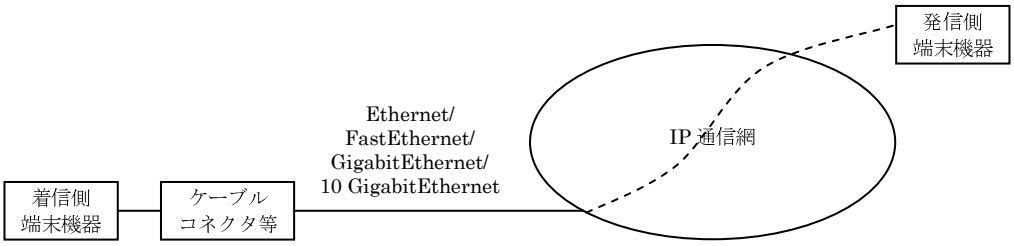


図 1-1　フレッツ・ＶＰＮ ゲートの基本構成

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。認証処理に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。

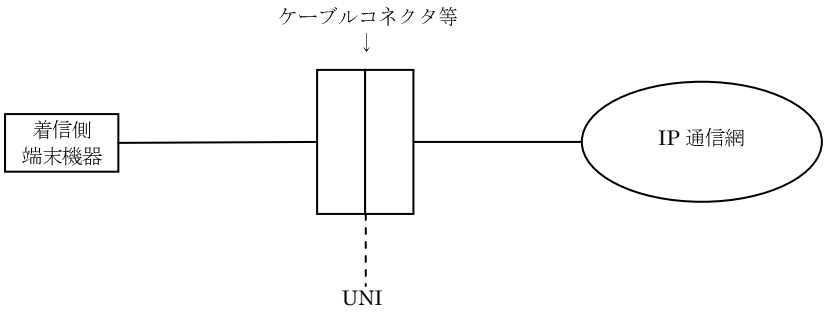


図 1-2　Ethernet/FastEthernetタイプのインタフェース規定点

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。

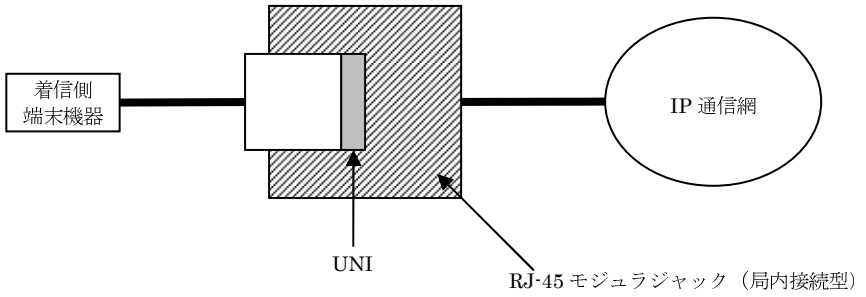


図 1-3　Ethernet/FastEthernetタイプのインタフェース規定点

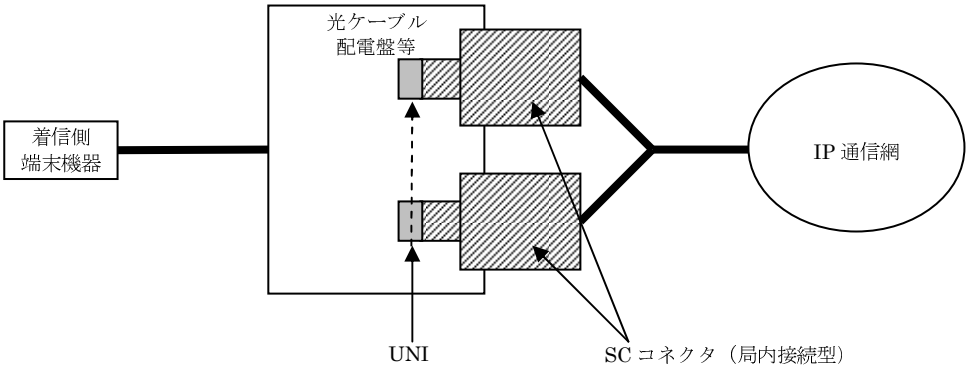


図 1-4　FastEthernetタイプのインタフェース規定点

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。
GigabitEthernetタイプのインタフェースの詳細については、[3 GigabitEthernetタイプのユーザ・網インタフェース仕様]を参照してください。10 GigabitEthernetタイプのインタフェースの詳細については、[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。

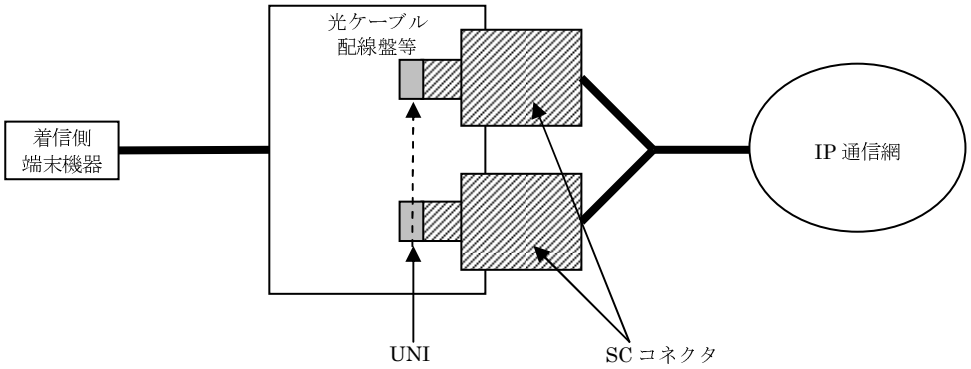
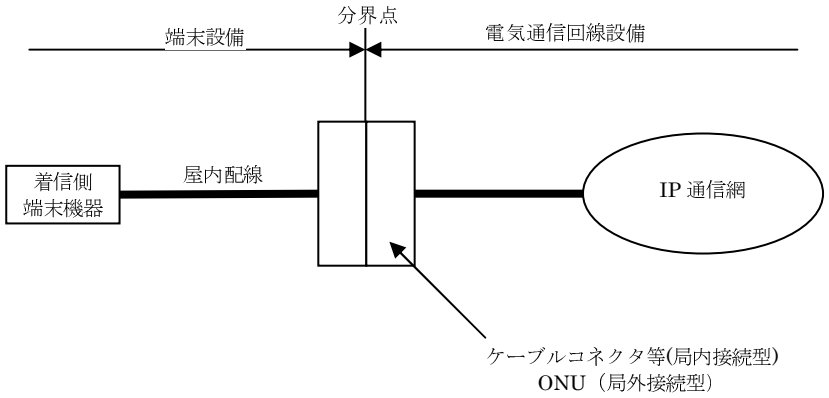


図 1-5　GigabitEthernet/10 GigabitEthernet タイプのインタフェース規定点

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。

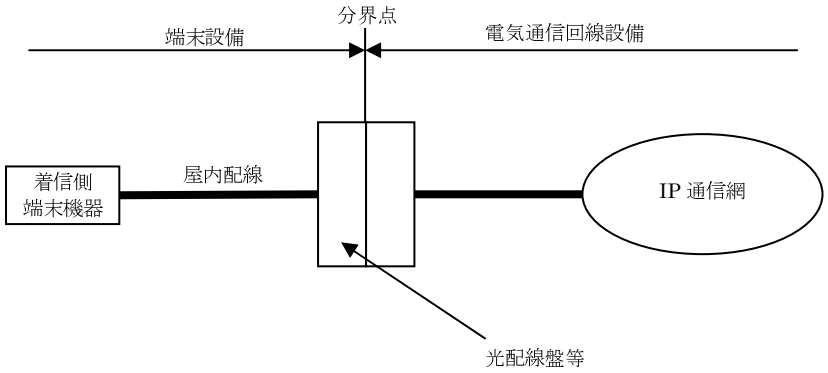


図 1-7　GigabitEthernet/10 GigabitEthernetタイプの分界点

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。

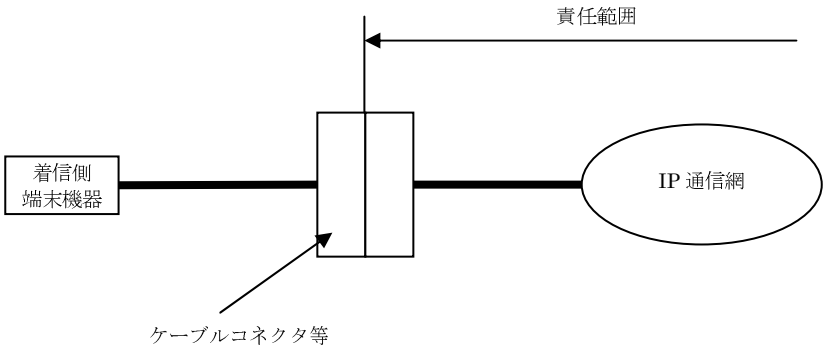


図 1-8　Ethernet/FastEthernetタイプにおける施工・保守上の責任範囲

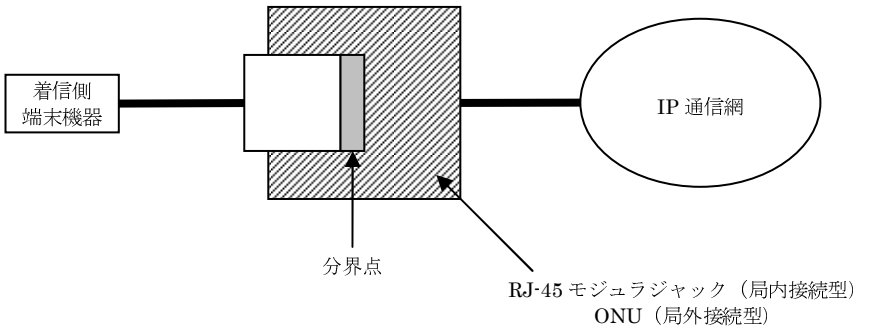


図 1-9　Ethernet/FastEthernetタイプにおける施工・保守上の責任範囲分界点

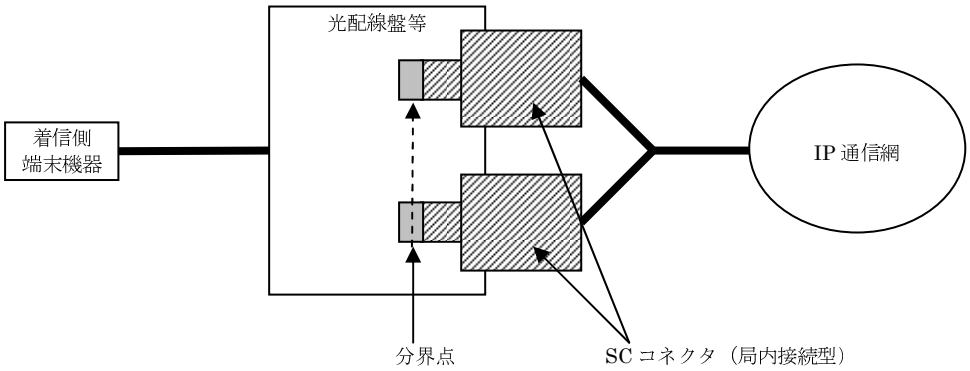


図 1-10　FastEthernetタイプにおける施工・保守上の責任範囲分界点

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。

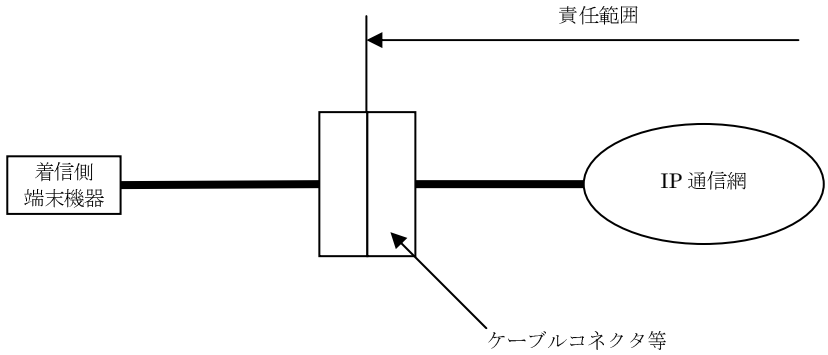


図 1-11　GigabitEthernet/10 GigabitEthernetタイプにおける施工・保守上の責任範囲

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。

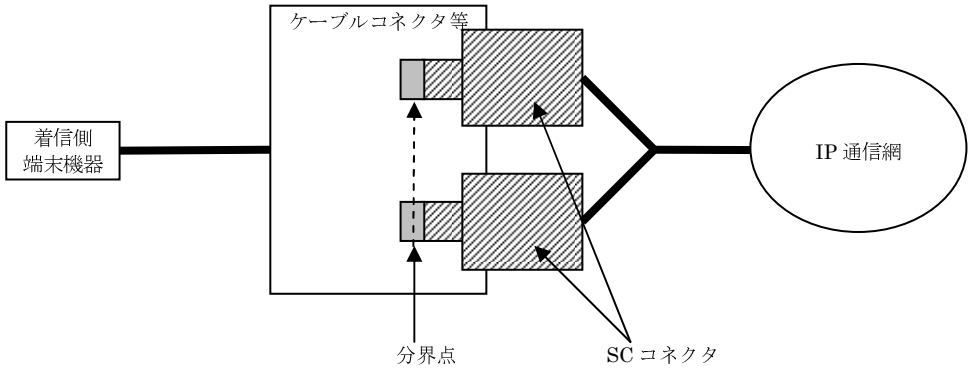
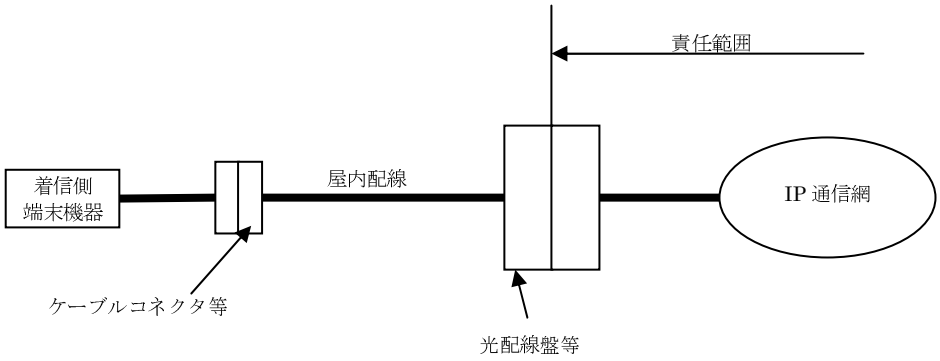


図 1-12 GigabitEthernet/10 GigabitEthernetタイプにおける施工・保守上の責任範囲分界点

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

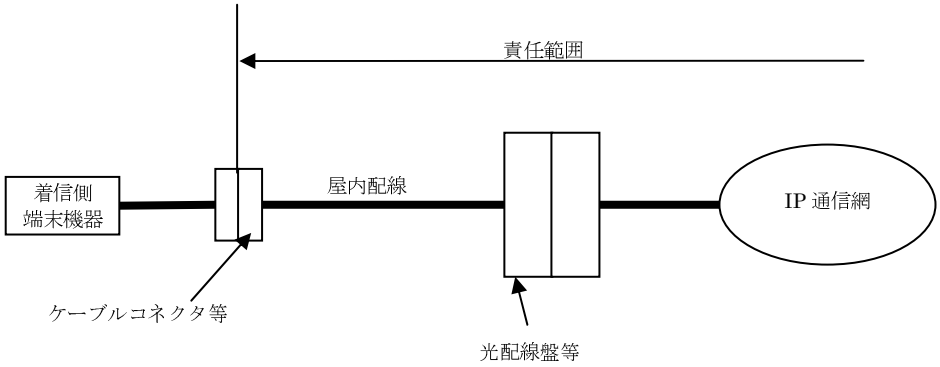


図 1-13　GigabitEthernet/10 GigabitEthernetタイプにおける施工・保守上の責任範囲

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。

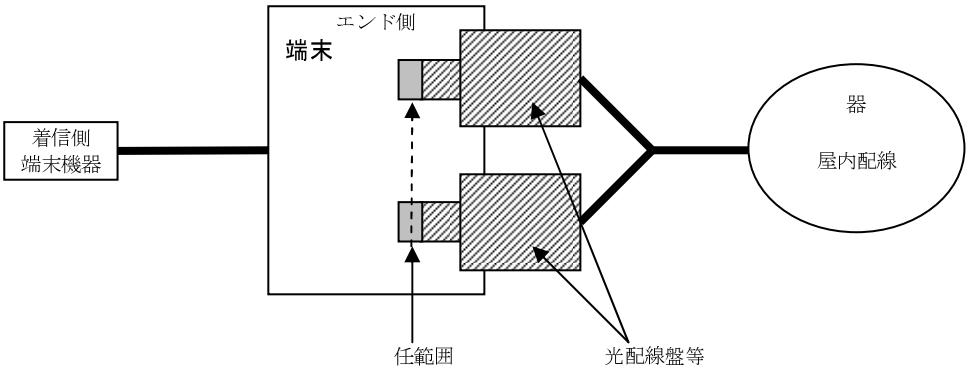


図 1-14　GigabitEthernet/10 GigabitEthernetタイプにおける施工・保守上の責任範囲分界点

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

<table>
<tr><th colspan="2">レイヤ</th><th colspan="2">規定するプロトコル</th></tr>
<tr><td>7</td><td>アプリケーション</td><td rowspan="4" colspan="2">RFC2865（RADIUS）
RFC2866（RADIUS Accounting）</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 colspan="2">RFC791（IPv4）
RFC792（ICMPv4）
RFC1918 (Private Address Space)</td></tr>
<tr><td>2</td><td>データリンク</td><td colspan="2">RFC826（ARP）
IEEE 802.3-2005 MAC 準拠</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2">物理</td><td>Ethernet</td><td>IEEE 802.3-2005 10BASE-T 準拠</td></tr>
<tr><td>FastEthernet</td><td>IEEE 802.3-2005 100BASE-FX/TX 準拠</td></tr>
</table>

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

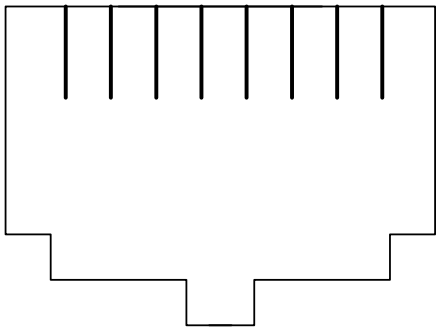
10Mb/s品目のレイヤ1では、IEEE 802.3-2005に規定されている10BASE-Tを使用し、10Mb/sの伝送速度でベースバンド信号の全二重固定の通信を行います。
詳細については、IEEE 802.3-2005を参照してください。

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。プライベートアドレスについては、RFC1918で規定されているアドレスは使用可能ですが、RFC6598で規定されているShared Address Spaceは利用できません。

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およびRFC6598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。

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) RFC1771（BGP-4）(注) RFC1918（Private Address Space）
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)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。プライベートアドレスについては、RFC1918で規定されているアドレスは使用可能ですが、RFC6598で規定されているShared Address Spaceは利用できません。
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およびRFC6598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。

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 Parameter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） RFC3576（Dynamic Authorization Extensions to RADIUS）
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） RFC1918(Private Address Space)
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。プライベートアドレスについては、RFC1918で規定されているアドレスは使用可能ですが、RFC6598で規定されているShared Address Spaceは利用できません。
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およびRFC6598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BGP-4を使用します。

BGP-4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。また、10 GigabitEthernetタイプにおいて、セッション解除を行うためには、RFC3576（Dynamic Authorization Extensions to RADIUS）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。また、セッション解除を行う場合のRADIUSクライアント側で用いるポート番号は、3799（Dynamic Authorization Extensions to RADIUS）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。

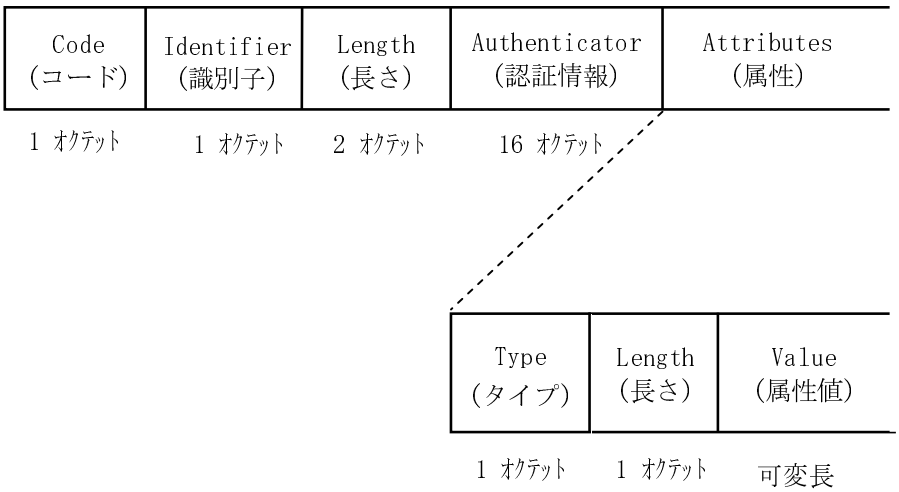
（注1） セカンダリサーバを設置した場合の、プライマリサーバからセカンダリサーバへの切り替え条件、並びにセカンダリサーバからプライマリサーバへの切り戻し条件については、[5.3通信用タイマ] を参照してください。

（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、RFC2866、及びRFC3576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。



（注）パケットフォーマットについての詳細は RFC2865、RFC2866、及び RFC3576 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

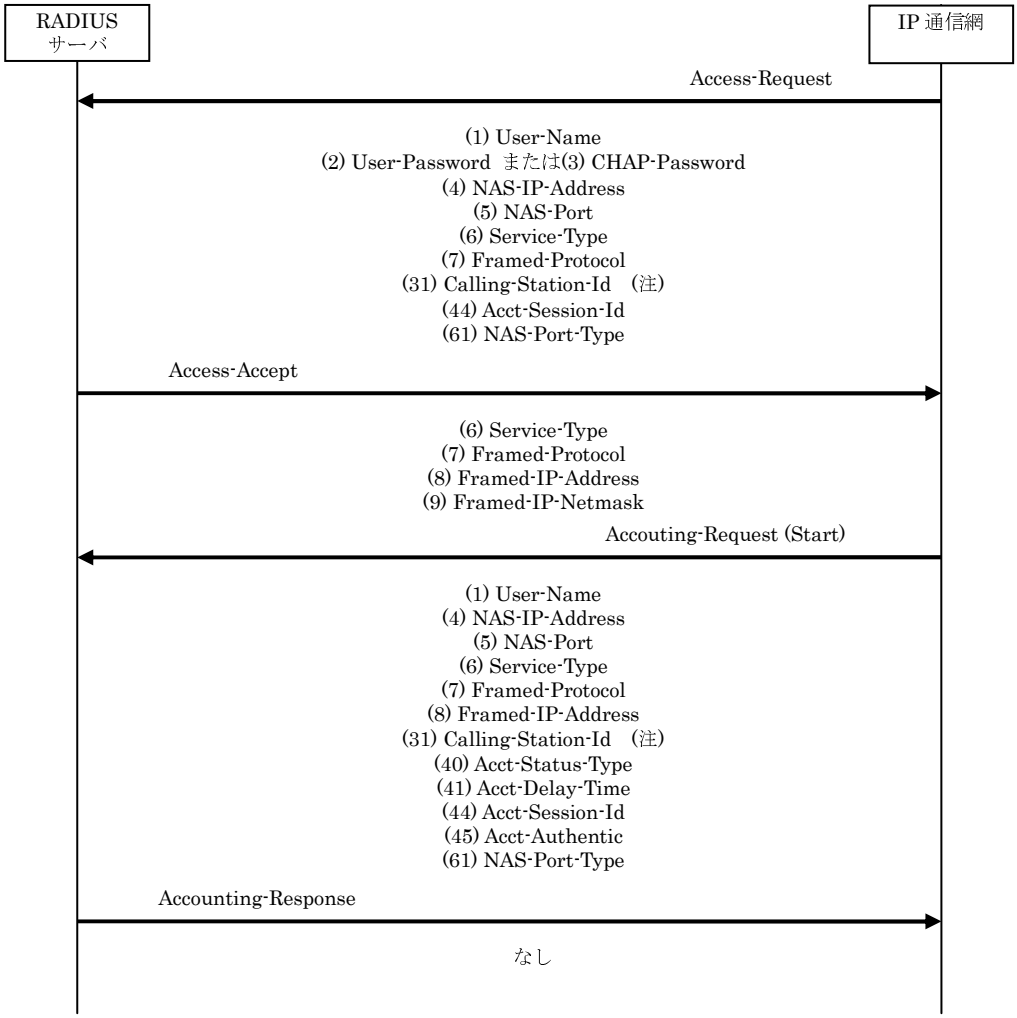
利用可能なAttributesを表5-1に示します。詳細は、5.2.6を参照ください。

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**エラー！ 参照元が見つかりません。**～図 5-6に示します。

5.2.1　認証成功

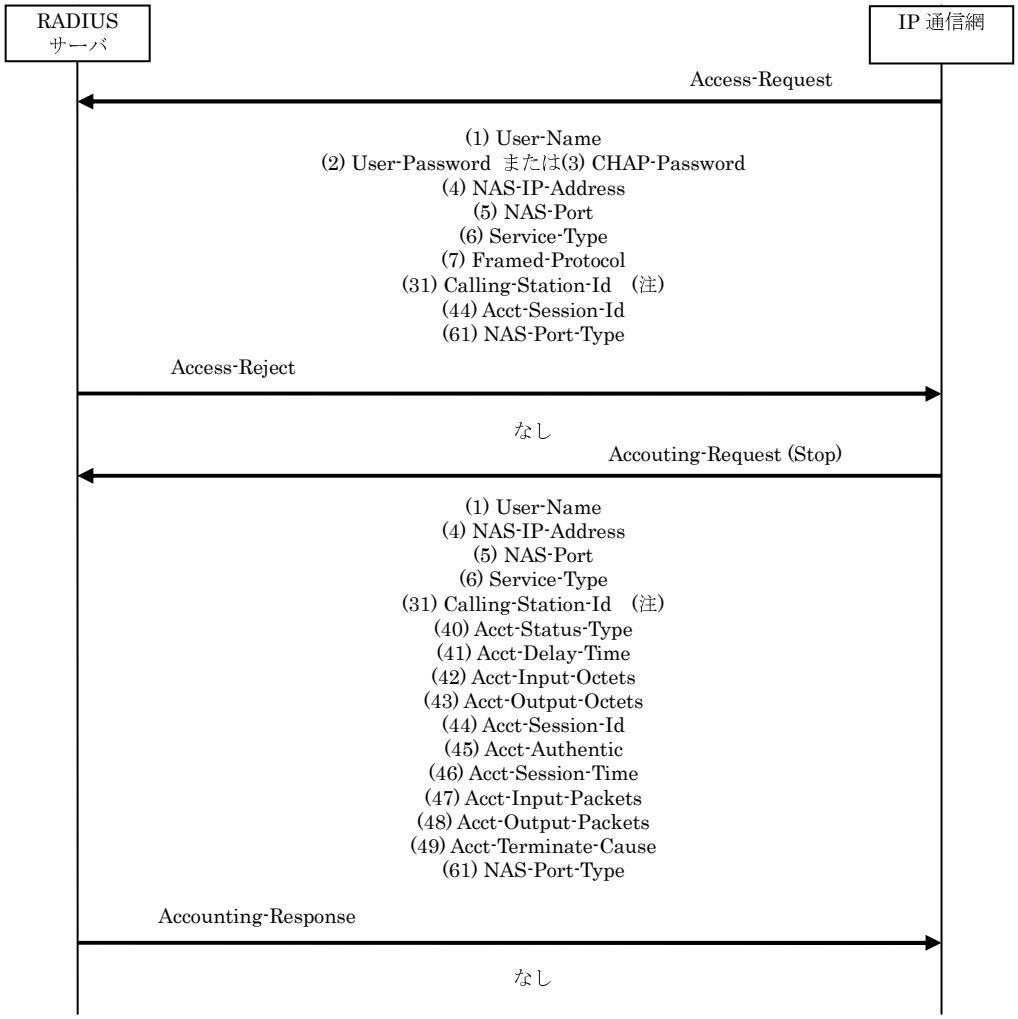
(注)回線情報転送機能を利用する場合のみIP通信網から送出されます。



（ ）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、5.2.6を参照ください。

図 5-2　接続要求の通信シーケンス例（認証成功）

5.2.2　認証失敗

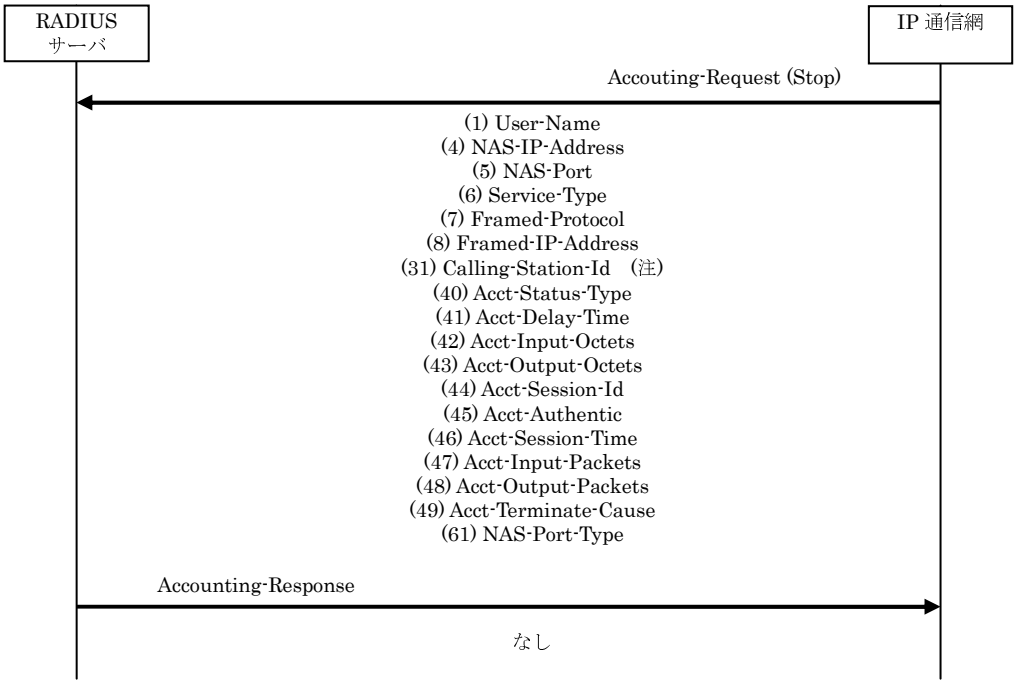


（注）回線情報転送機能を利用する場合のみIP通信網から送出されます。
（　）はAttributesのTypeを示しています。
認証情報は図中Access-Requestで送信されます。
認証結果（認証失敗）は図中Access-Rejectで送信します。
各Attributesに関する詳細は、5.2.6を参照ください。

図 5-3　接続要求の通信シーケンス例（認証失敗）

5.2.3　切断情報

(注)回線情報転送機能を利用する場合のみIP通信網から送出されます。

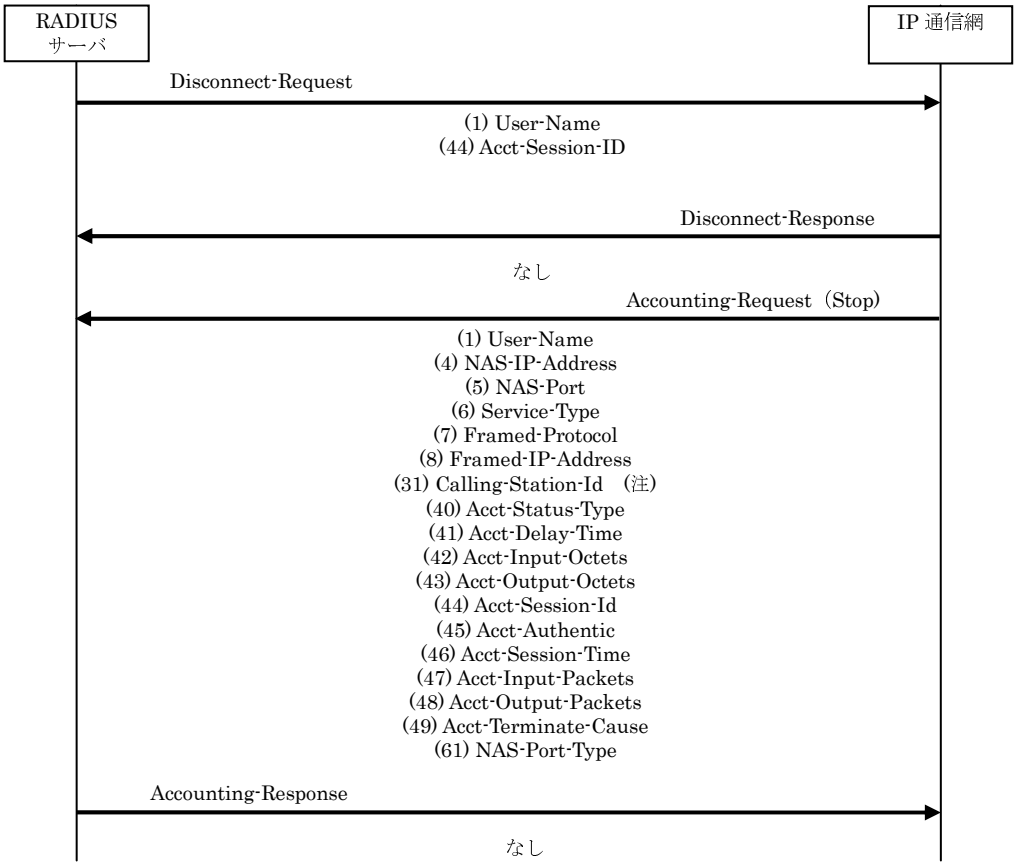


（ ）はAttributesのTypeを示しています。
切断情報は図中Accounting-Request(Stop)で送信されます。
各Attributesに関する詳細は、5.2.6を参照ください。

図 5-4　切断情報の通信シーケンス例

5.2.4　セッション解除成功

(注)回線情報転送機能を利用する場合のみIP通信網から送出されます。

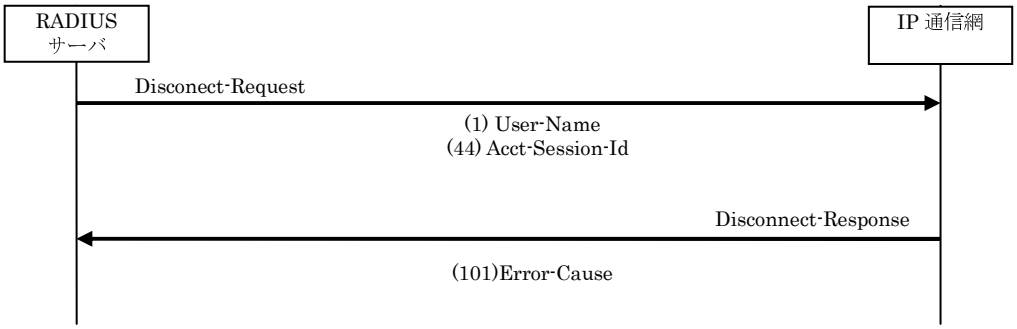


（ ）はAttributesのTypeを示しています。
切断情報は図中Accounting-Request(Stop)で送信されます。
各Attributesに関する詳細は、5.2.6を参照ください。

図 5-5　セッション解除成功時の通信シーケンス例

5.2.5　セッション解除失敗

() はAttributesのTypeを示しています。



各Attributesに関する詳細は、5.2.6を参照ください。

図 5-6　セッション解除失敗時の通信シーケンス例

5.2.6　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。
認証パラメータとして利用可能なAttributesは、「User-Name」、「User-Password」または「CHAP-Password」、「Calling-Station-Id」です。
上記Attributes以外を利用の場合には、認証が正常に行われなくなる可能性があります。

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	
Framed-Protocol	7	整数	1:PPP	
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のみ、 発信者回線情報が送出されます。(注 3)
Acct-Session-Id	44	文字列	(ID)	
NAS-Port-Type	61	整数	0～5	
<Access-Accept>				
Service-Type	6	整数	2:Framed	
Framed-Protocol	7	整数	1:PPP	
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	
Framed-Protocol	7	整数	1:PPP	
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のみ、 発信者回線情報が送出されます。(注 3)
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	

	Type	Value 形式	値	備考
NAS-Port-Type	61	整数	0～5	
<Accounting-Request(Stop)>				
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	
Framed-Protocol	7	整数	1:PPP	認証失敗時には設定されません。
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のみ、 発信者回線情報が送出されます。(注 3)
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	0～5	
<Accounting-Request(Accounting-On)> (注 4)				
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)	
<Accounting-Request(Accounting-Off)> (注 4)				
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)	
Acct-Terminate-Cause	49	整数	1～18	
<Disconnect-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)
Acct-Session-Id	44	文字列	(ID)	
<Disconnect-Response>				
Error-Cause (注 5)	101	整数	402 または 503	402：送信すべき Attribute が不足しています。 503：送信した Attribute の内容に誤りがあります

(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・ＡＤＳＬ、Ｂフレッツおよびフレッツ 光ネクストを利用する回線において、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（フレッツ・ナンバー）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。また、フレッツ・ＩＳＤＮを利用する回線において、発信者側で発番号通知を実施している場合は発信者番号（電話番号）が設定され、発信者側で発番号通知を実施していない場合（非通知の場合）は、本Attribute自体が設定されません。

(注4) 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5)セッション解除に失敗した場合にのみ含まれます。

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)
		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) 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。

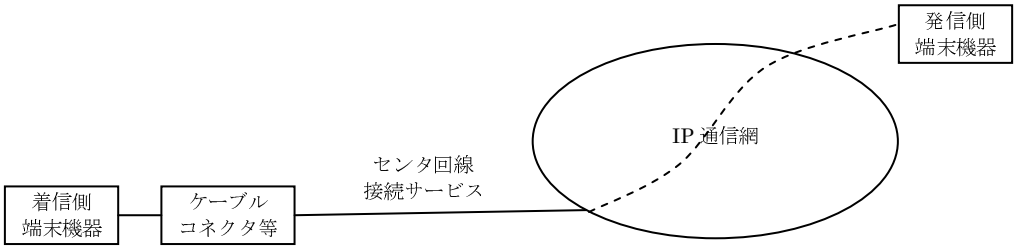


図 1-1　本サービスの基本サービス

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。

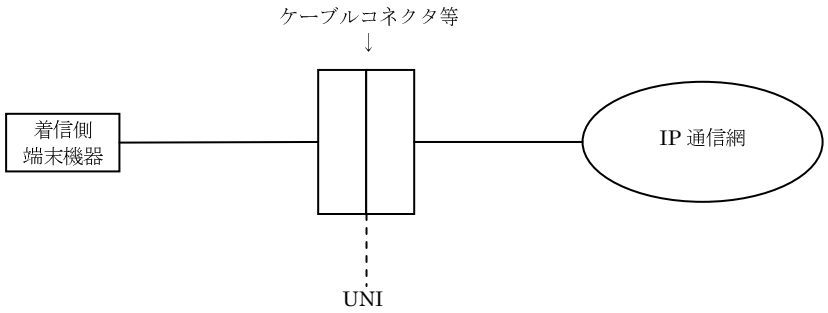


図 1-2　局内接続タイプのインタフェース規定点

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。

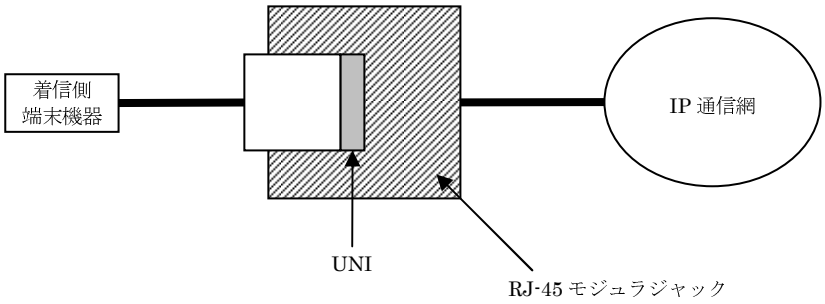


図 1-3　10Mb/sメニューのインタフェース規定点

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。

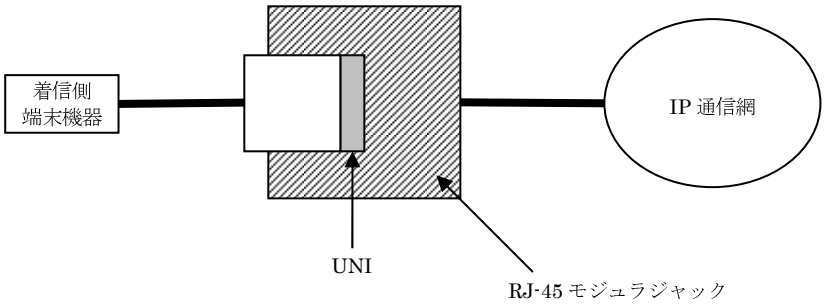


図 1-4 100Mb/sメニューのインタフェース規定点

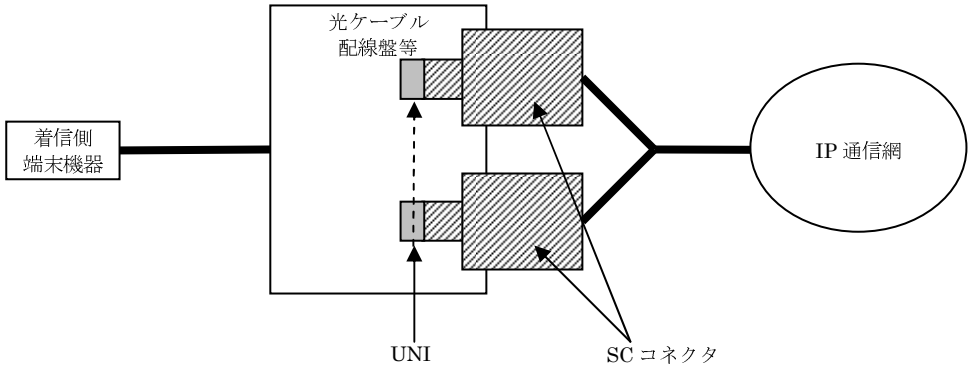


図 1-5 100Mb/sメニューのインタフェース規定点

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。

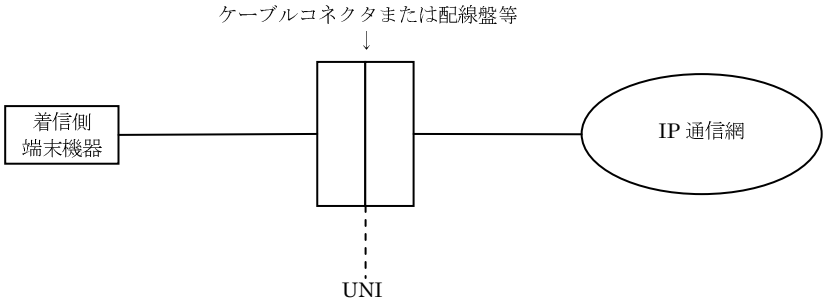


図 1-6　収容エリア内接続タイプのインタフェース規定点

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。

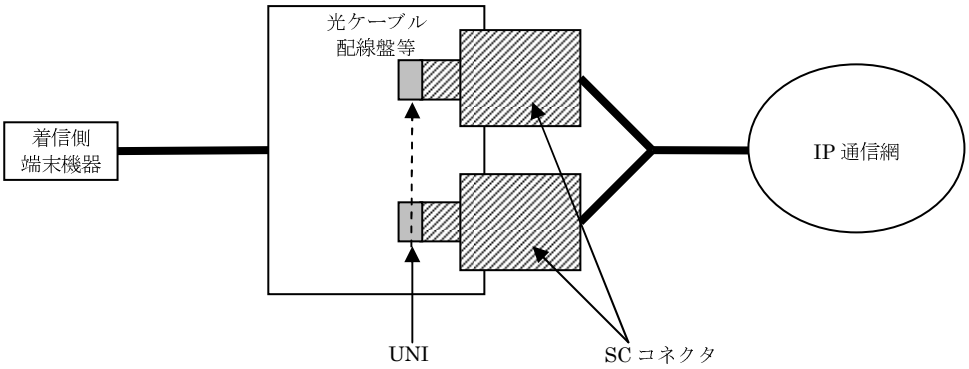


図 1-7　100Mb/sメニューのインタフェース規定点

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。

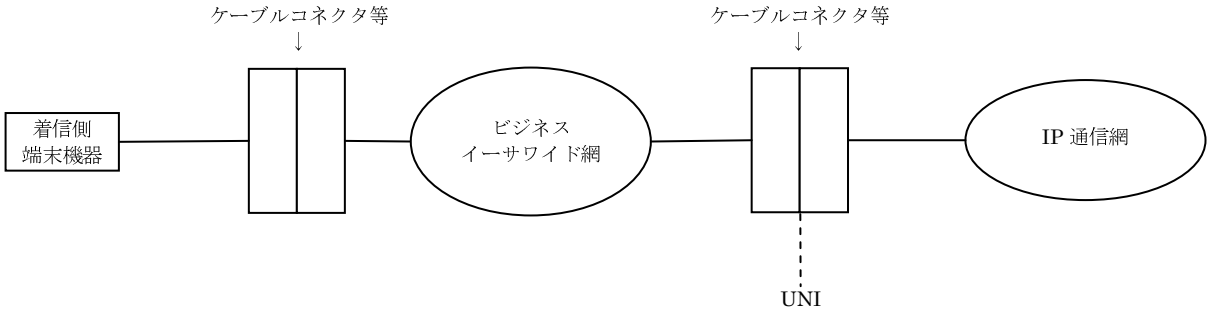


図 1-8　ビジネスイーサワイド接続タイプのインタフェース規定点

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。

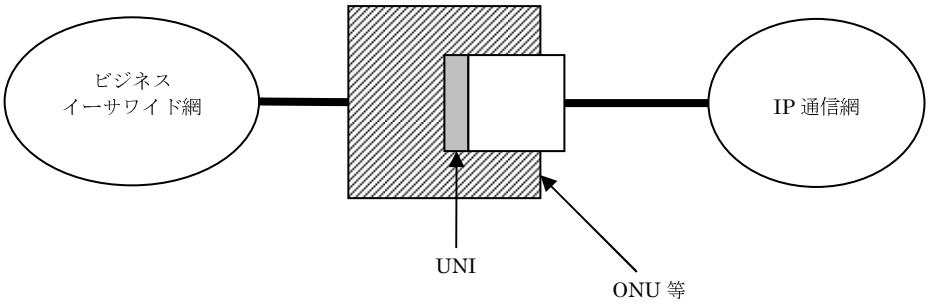


図 1-9 10Mb/sメニューにおけるインタフェース規定点

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。

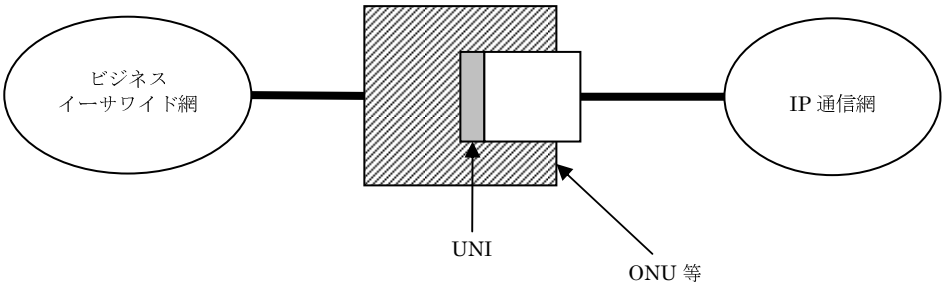


図 1-10 100Mb/sメニューのインタフェース規定点

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。

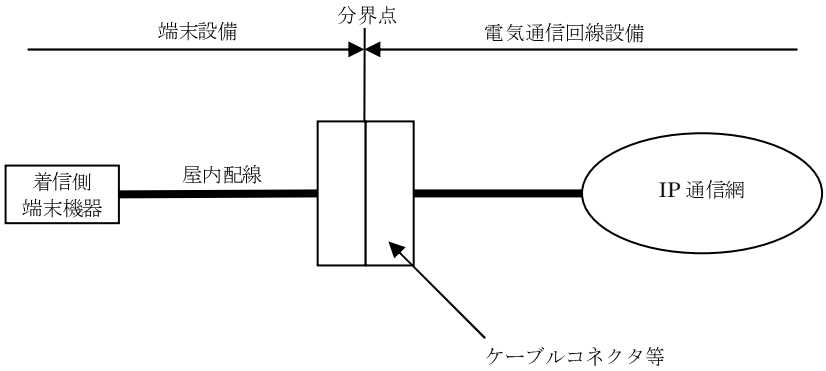
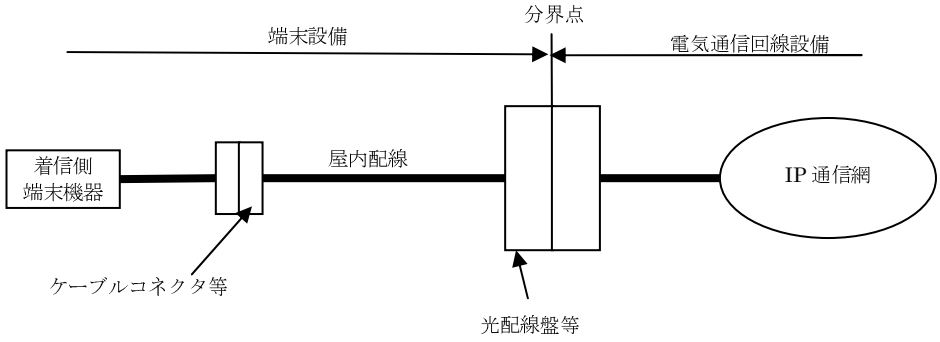


図 1-11　局内接続タイプの分界点

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

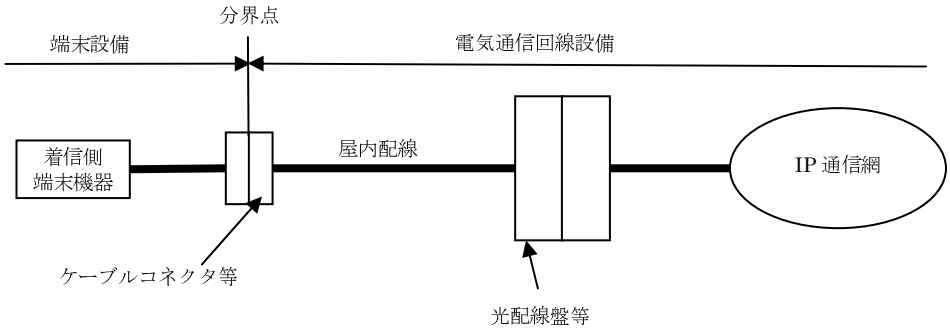
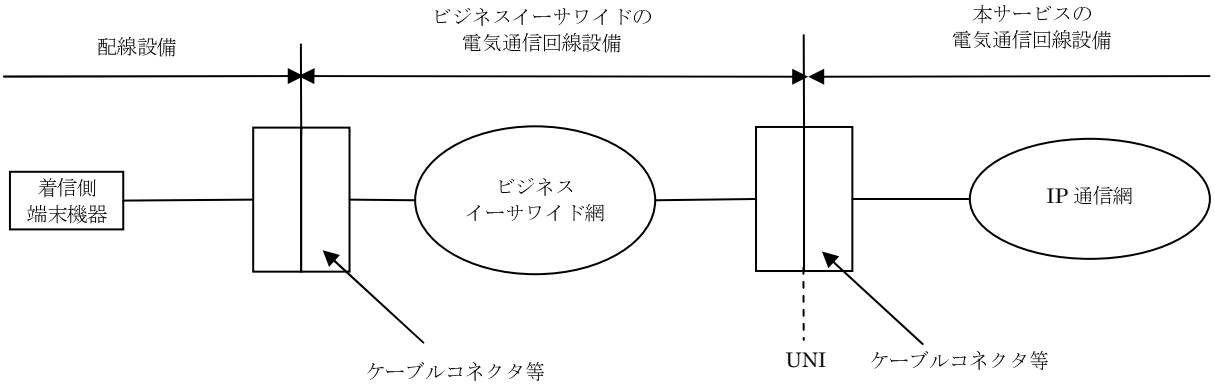


図 1-12　収容エリア内接続タイプの分界点

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

本サービスの施工・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。

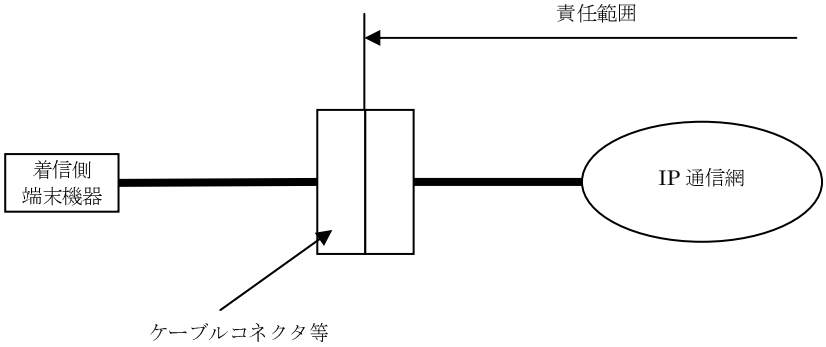
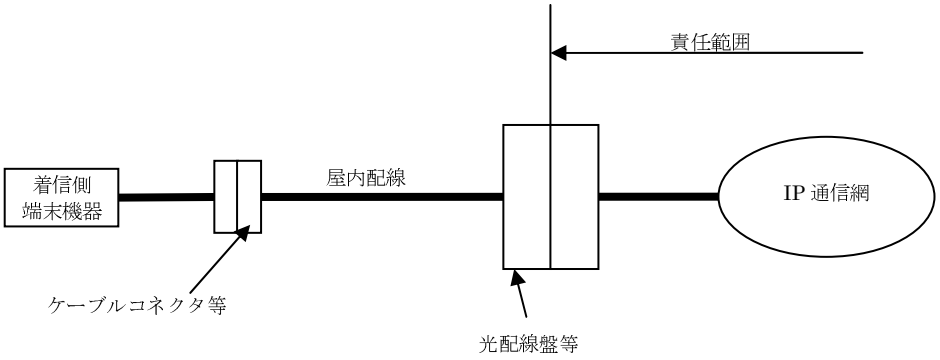


図 1-14　局内接続タイプの施工・保守上の責任範囲

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

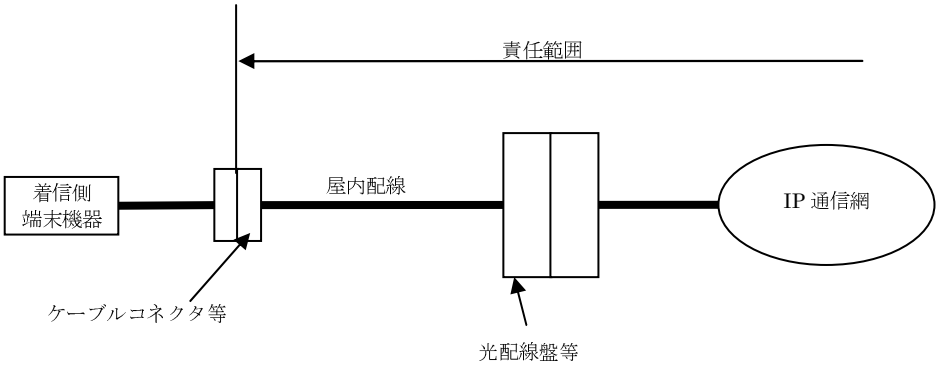


図 1-15　収容エリア内接続タイプにおける施工・保守上の責任範囲

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。

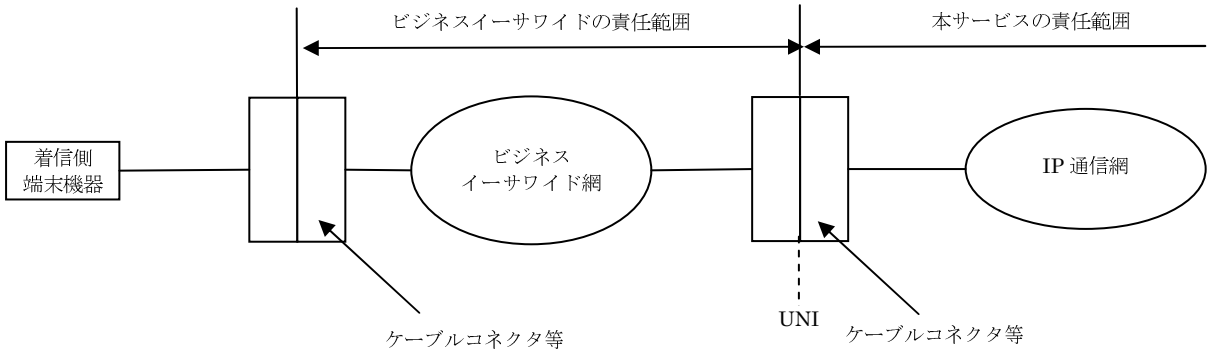


図 1-16　ビジネスイーサワイド接続タイプの施工・保守上の責任範囲

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） RFC1918 (Private Address Space)
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。

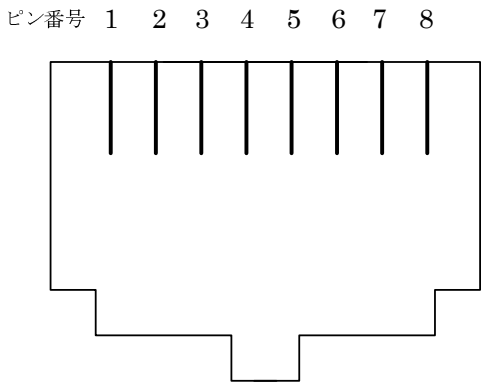
2.2.1　　10Mb/s メニューのレイヤ 1 仕様

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

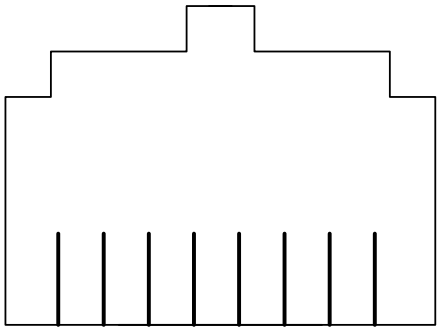


	記号	信号方向		ピン番号
		端末機器	IP 通信網	
受信	RD(+)	→		1
	RD(-)	→		2
送信	TD(+)	←		3
	TD(-)	←		6

※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

2.2.1.3　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の場合、IEC60874-14準拠の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の場合、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。

1000BASE-LXの場合、IEC60874-14準拠のSCコネクタ（オス）です。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。

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-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。

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

本サービスでは、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。プライベートアドレスについては、RFC1918で規定されているアドレスは使用可能ですが、RFC6598で規定されている Shared Address Spaceは利用できません。
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およびRFC6598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。

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・キャスト編

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。

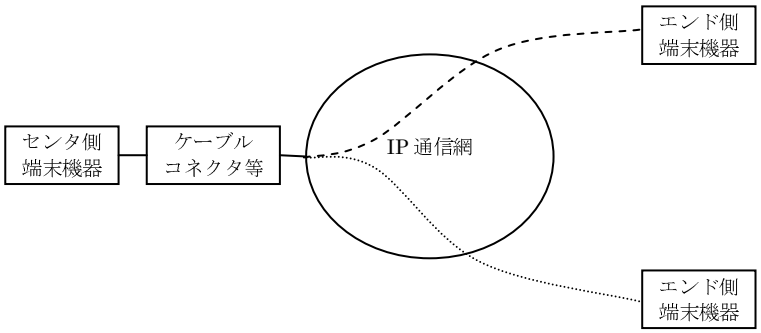


図 1-1 フレッツ・キャストの基本構成

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

サービス品目	マルチキャスト機能	インタフェース条件
ベストエフォート型 100Mb/s シングルクラス	なし	IEEE 802.3-2005 1000BASE-LX 準拠
	あり	
ベストエフォート型 100Mb/s デュアルクラス	なし	
	あり	
ベストエフォート型 200Mb/s シングルクラス	なし	
	あり	
ベストエフォート型 200Mb/s デュアルクラス	なし	
	あり	
ベストエフォート型 300Mb/s シングルクラス	なし	
	あり	
ベストエフォート型 300Mb/s デュアルクラス	なし	
	あり	
ベストエフォート型 1Gb/s シングルクラス	なし	
	あり	
ベストエフォート型 1Gb/s デュアルクラス	なし	
	あり	
帯域確保型 1Gb/s シングルクラス	なし	

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。

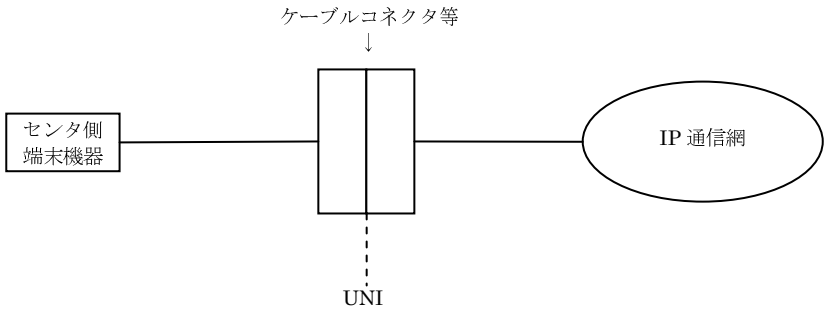
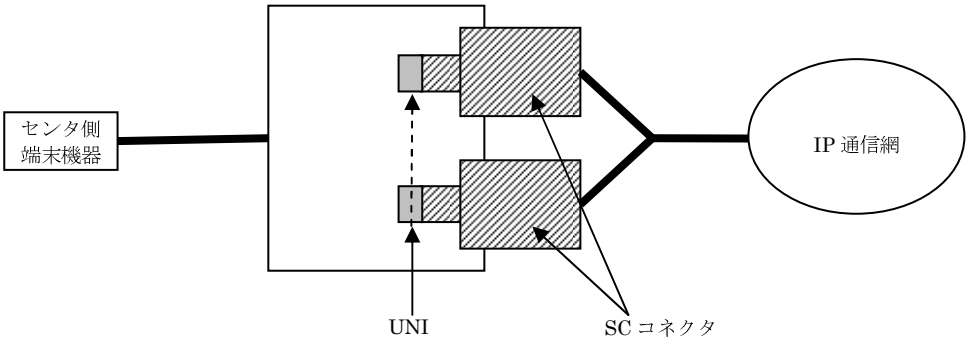


図 1-2　フレッツ・キャストのインタフェース規定点

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。

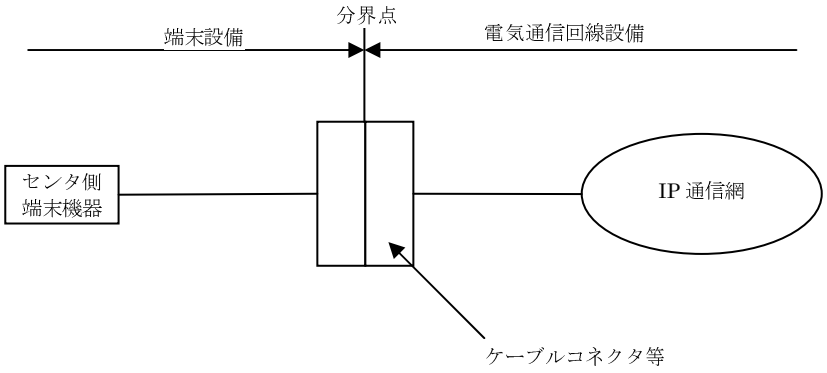


図 1-4　フレッツ・キャストの分界点

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。

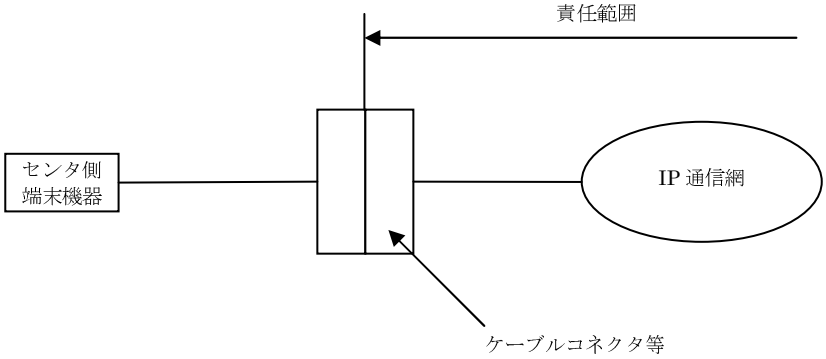


図 1-5　フレッツ・キャストにおける施工・保守上の責任範囲

施工・保守上の責任範囲の分界点は図 1-6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。

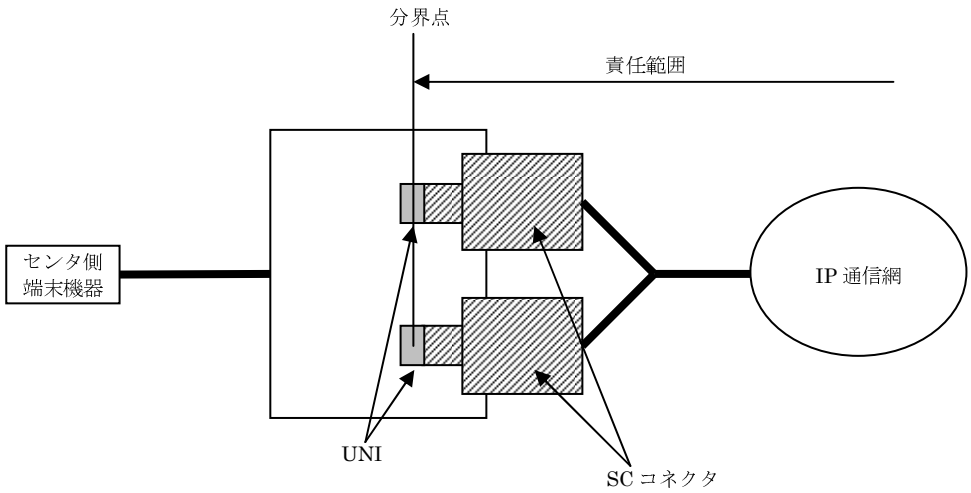


図 1-6　フレッツ・キャストにおける施工・保守上の責任範囲分界点

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

レイヤ		規定するプロトコル	
		ベストエフォート型のもの	帯域確保型のもの
7	アプリケーション	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)	
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: RFC3513 / RFC2460 / RFC2474 / RFC3306(注 5) / RFC3307(注 5) ICMPv6: RFC4443 NDP: RFC2461 BGP4+: RFC1771 / RFC2545 / RFC2858	IPv6: RFC3513 / RFC2460 / RFC2474 ICMPv6: RFC4443 NDP: RFC2461
2	データリンク	IEEE 802.3-2005(MAC)	
1	物理	IEEE 802.3-2005(1000BASE-LX)準拠	

(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、IEEE 802.3-2005に規定されている1000BASE-LXを使用し、サービス品目が1Gb/s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。

また、サービス品目が100Mb/s、200Mb/s、300Mb/s品目の場合は、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100Mb/s、200Mb/s、300Mb/s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。

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、IEC60874-14に規定されるSCコネクタ（オス）です。

また、IEEE802.3-2005に規定されている1000BASEー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・キャスト帯域確保型の品目では、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 I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 Listenner 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視聴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

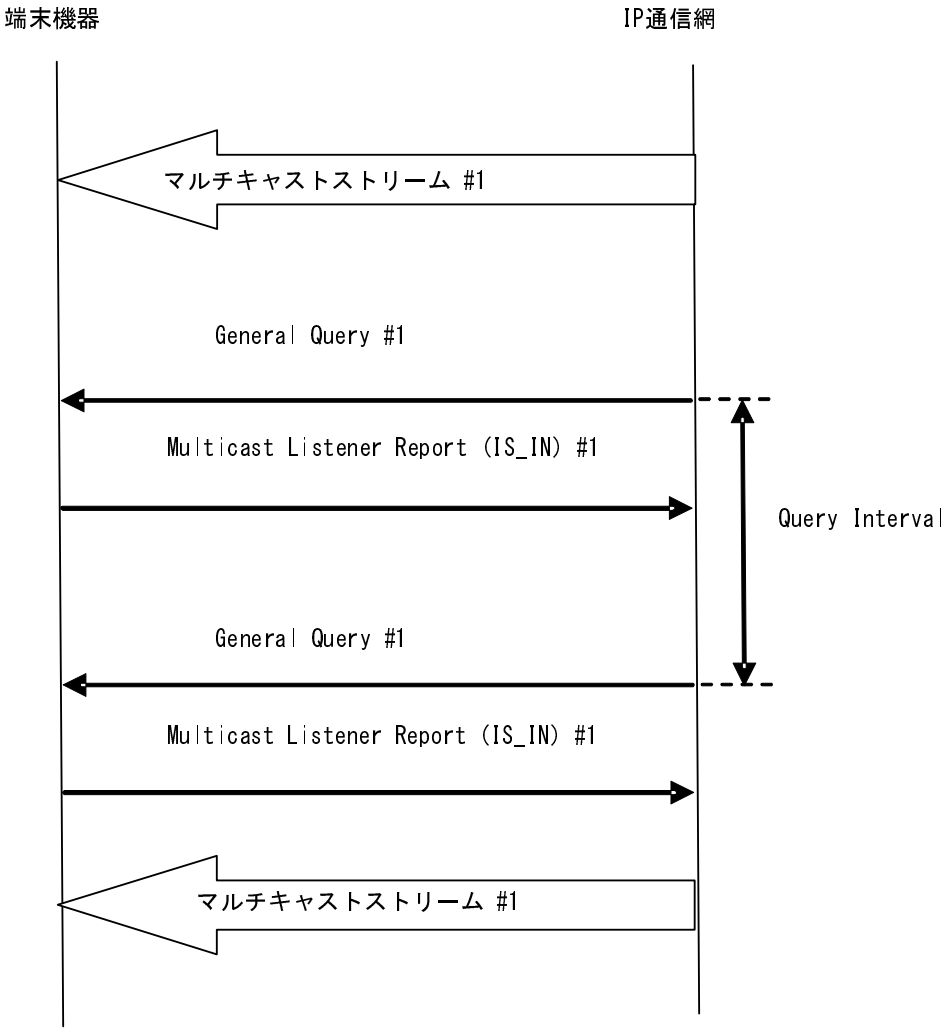


図 4-2　マルチキャスト受信継続確認シーケンス例

4.1.3　チャネル切り替えシーケンス例

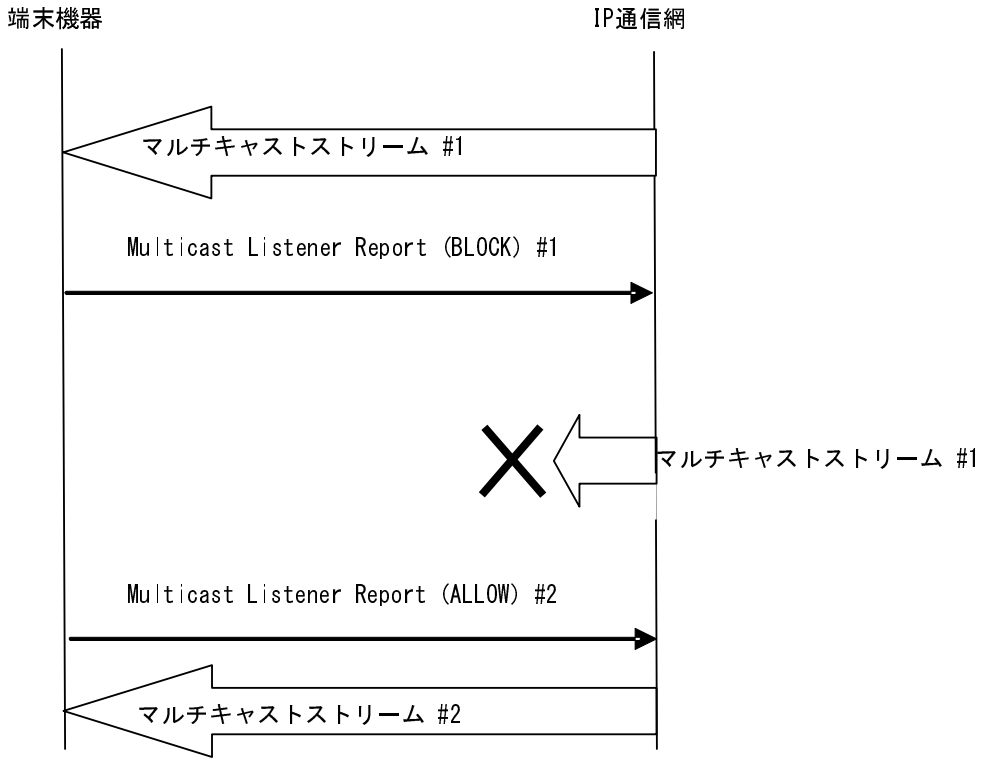


図 4-3　チャネル切り替えシーケンス例

4.1.4　マルチキャスト受信停止シーケンス例

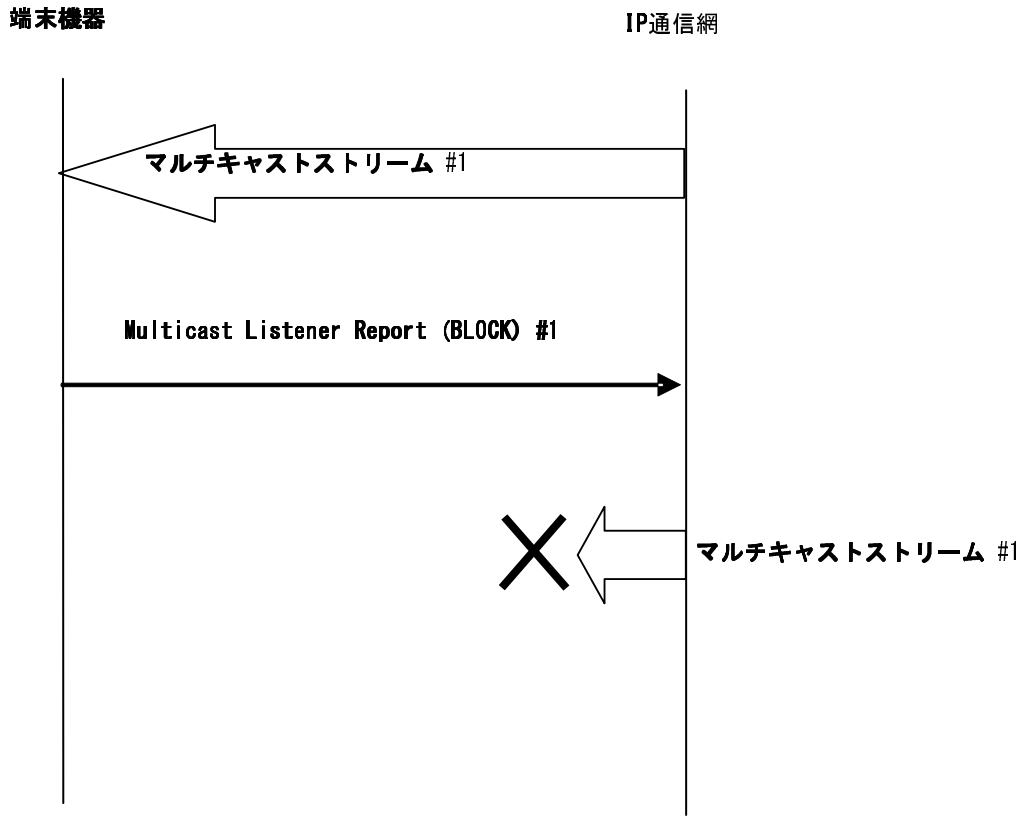


図 4-4　マルチキャスト受信停止シーケンス例

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 構成情報の取得

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。