

NSKプロトコル

日本新聞協会デジタル写真電送プロトコル

Revision 1.1

社団法人日本新聞協会

はじめに

日本新聞協会は、自由で責任ある新聞を維持発展させるという目的で新聞・通信・放送各社が1946年に創設した全国的な機関であり、編集倫理の向上とともに広告、販売、製作技術など新聞発行にかかわる各分野の共同研究・調査活動を行っている。

コンピューター技術の発展や電気通信分野の高度化は機器のダウンサイジングやオープン化をもたらし、新聞製作においても標準化を求める動きが活発化してきた。1992年には「日本新聞協会選挙FD標準フォーマット」、1993年には「人事FD標準フォーマット」が完成するなど、報道支援を中心としたソフトウェア分野での共有化が進み出した。

写真電送の分野では1991年8月、各社共通フォーマットの策定を行うことになった。画像電子学会などの下部機構として発足した写真電送ワーキンググループ(WG1)から新聞界に委員派遣依頼があり、新聞協会情報・通信部会(旧電気通信委員会)でも、カラーデジタル画像の標準化に向けて議論が始まった。

WG1では、1992年4月、新聞3社、通信1社、メーカー3社からなるフォーマット作業班を組織し、日本新聞協会デジタル写真フォーマット(NSK TIFF)を作成した。

NSK TIFFは1994年3月に英国ウインザーで開かれたIPTC春季全体会議にも報告し、同年5月、44回の会議を終え完成した。引き続きNSK TIFFの通信プロトコルを検討する作業班が発足して、本年5月末まで28回の審議を重ねNSKプロトコルの策定を進めてきた。初会合から勉強会を積極的に取り入れ、1994年12月までにZMODEMとTCP/IPの採用を決定した。NSKプロトコルは1995年3月のIPTC春季全体会議にも英語版ドラフトVer.0.7として報告した。その後、さらに技術的な検討を加えると共に、基本的な運用管理規定を定め今回の発表を迎えた。

本書作成にあたって、編集作業に参加していただいたメーカー関係者各位、ならびに新聞・通信各社委員に心から御礼申し上げます。そして、IPTCメンバー各位、特に本書の英語版の監修を引き受けていただいたIPTCマネージング・ディレクターのデビッド・アレン氏、NPDP議長としてアドバイスしていただいたAFPのステファン・ゲリオ氏、翻訳に関し協力していただいたAP東京支局写真技術部長の佐藤光彦氏に敬意を表します。

1995年5月

デジタル写真標準化ワーキンググループ
プロトコル作業班

「NSKプロトコル」改訂にあたって

この文書は、NSKプロトコル改訂版(Revision 1.1)を規定したものである。

NSKプロトコルはNSK TIFF(日本新聞協会デジタル写真フォーマット)を電送するためのプロトコルとして、1995年3月、デジタル写真標準化ワーキンググループプロトコル作業班により策定された。

今回、NSKプロトコルを改訂することになったのは、NSK TIFF(日本新聞協会デジタル写真フォーマット)Revision 1.1が97年11月、技術委員会の承認を受け、新たにリリースされたことによる。

NSKプロトコルそのものについては変更はなく、NSK TIFFフォーマットにおいて改訂された諸点との整合性を図るため、微調整を行う必要が生じたものである。

改訂にあたって留意すべきは次の点である。

NSK TIFFフォーマットでは、サービスIDおよび生成媒体の登録制を廃止した。また新聞協会の組織改編が行われ、担当セクションは開発部から技術部へと名称を変更している。プロトコルにおける改訂箇所は、これらに合わせた部分である。

このほか第5章における移動体通信サービスの動向等は、策定当初に比べ進歩の状況は著しいが、特に修正は加えていない。

写真電送の世界はオリンピック等さまざまな大舞台を経て、飛躍的に発展している。今回の改訂作業を担った情報・通信部会NSK TIFFサポートチームでは今後に向けた諸活動をすでにスタートしている。

これまでの活動を見守ってくれた上位部会(情報・通信部会)並びに技術委員会に謝意を表したい。

1998年5月

NSK TIFFサポートチーム

履 歴

1995年5月30日 Revision1.0発行
1998年5月15日 Revision1.1発行

第1章 NSKプロトコルの概要

1995年3月、このNSKプロトコルはデジタル写真標準化ワーキンググループプロトコル作業班により策定された。これは、1994年3月に日本新聞協会電気通信委員会(注1)で了承されたNSK T I F Fを電送するためのプロトコルとして、1995年5月、日本新聞協会技術委員会で承認された。

本書は英語版も作成され、ドラフトVer.0.7が1995年3月27日のI P T C(注2)春季全体会議のNews Photo Digitisation Working Partyで発表された。I P T Cとの意見交換や技術的な見直しを経て、5月30日に日本語版Revision 1.0を発行する運びとなった。6月中旬に発行される英語版Revision 1.0では、日本新聞協会内の規定は外国通信社などでは必要ないため省略した。

1.1.ではNSKプロトコルの目的と策定経緯について述べ、1.2.ではOSI基本参照モデルに沿ってNSK T I F Fを電送するためのアナログ、デジタル公衆回線における推奨プロトコルの概要を説明する。また、このNSKプロトコルの適用範囲と運用上の注意点について、基本的な考え方を示す。

第1章 目次

1.1.	NSKプロトコルの基本方針と策定経緯	
1.1.1.	基本方針	6
1.1.2.	策定経緯	6
1.1.3.	プロトコルの策定理由	7
1.1.4.	比較検討	7
1.2.	NSKプロトコルの概要	
1.2.1.	関係する国際標準化機関と活動	8
1.2.2.	OSI基本参照モデル	9
1.2.3.	アナログ公衆回線用プロトコルの概要	11
1.2.4.	デジタル公衆回線用プロトコルの概要	13
1.2.5.	適用範囲と運用上の注意点	14

注1) 1994年9月、日本新聞協会内の機構改革により電気通信委員会は、より大きな組織である技術委員会に改組された。詳しい組織図は付録を参照。

注2) International Press Telecommunications Councilの略。国際新聞電気通信評議会。

1.1. NSKプロトコルの基本方針と策定経緯

1.1.1. 基本方針

下記の基本方針に添って本プロトコルの検討を行なった。

- (1) NSK T I F Fのプロトコルは特殊な専用プロトコルとせず、汎用プロトコルの中から適したものを選択し採用する。
- (2) アナログとデジタルとに回線種別を分け、Point to Pointでの接続を考える。
- (3) 将来に向けて、同報送信、ネットワーク接続についても調査、研究する。

1.1.2. 策定経緯

デジタル写真の標準フォーマット策定作業を完了した後、1994年4月、17社25人(新聞・通信社9社14人、メーカー8社11人)で構成されるワーキンググループを発足させ、28回にわたる会合を持ち、研究、検討を重ねてきた。その間、電気通信事業者、メーカーを講師に勉強会を行った。主な内容はパソコン通信におけるプロトコル、高速モデム規格、国際標準プロトコル(G4FAX)、ISDNで利用されているプロトコルなどである。

アナログ公衆回線プロトコルは1994年9月21日に全会一致でZMODEMプロトコルに決定、1994年11月24日に上部団体の統括ワーキンググループに報告した。デジタル公衆回線プロトコルは1994年12月20日、ネットワーク接続とし、PPP(注3)+TCP/IP+FTPに全会一致で決定した。1995年1月12日の日本新聞協会技術委員会で報告、基本的な方向が了承された。

注3) Point to Point Protocol の略。インターネット通信におけるデータリンク層での標準プロトコル。異機種のルーター同士の接続が、このPPPにより容易になった。

1.1.3. プロトコルの策定理由

(1) ZMODEM

パソコン通信での広い普及
高速モデムでの高速通信
容易な操作性

(2) TCP/IP

世界的な業界標準でインターネットでの実績がある
各種のプラットフォームに共通なプロトコルで汎用性がある
代表取材の配信など各社間のシステムの対応が容易
記事系のシステムとの統合が容易になる

1.1.4. 比較検討

(1) アナログ公衆回線

BPLUS (注4): ホストプログラムが非公開で、ライセンスが必要である。

DIT (注5): AFPやAPなどIPTC加盟社の電送機で使用されている。

コダック社のDCSの電送にも利用されたが、日本国内ではパソコン上への移植がほとんどなくZMODEMに比べエラー訂正機能がやや複雑である。

(2) デジタル公衆回線

G4FAX: 国際標準だが全てに対して規格化されているため、ファイル転送だけの部分使用は難しい。

FTAM (注6): 国際標準だがプロトコル自体が複雑なため転送するためのマシン能力が必要である。

HDL C系独自プロトコル: プロトコルの上位層を独自に作成する必要がある。

注4) 米国のCompu Serveで開発されたセンター主導のファイル転送プロトコル。クライアントプログラムの仕様はオープンだが、センター側プログラムに関しては、ライセンスを受ける必要がある。

注5) Digital Information Transmissionの略。AFPとハッセルブラッド社が共同開発したデジタル画像電送プロトコル。現在のバージョンは3.2である。

注6) File Transfer, Access and Managementの略。ネットワークでのファイル転送と共有のためのITU標準。

1.2. NSKプロトコルの概要

従来の写真電送における通信プロトコルは、システムおよび端末装置固有の仕様に基づいていた。システムに要求される機能が多種多様化するなかで、新聞・通信各社独自の仕様でシステム構築することは不経済になってきた。標準化を積極的に取り入れて行くことが重要である。

このような背景から新聞・通信各社が共通に使用できる電送機と受信システムのネットワークアーキテクチャの確立が望まれている。NSK TIFFの策定に引き続き、デジタル写真標準化ワーキンググループがただちにNSKプロトコルに取り組んだのもこのためである。これからは、電送機は特殊なプロトコルを使用する専用機である必要性はなく、汎用のハードウェアとソフトウェアを採用すべきである。受信システムもパーソナルコンピュータやワークステーションなどの汎用コンピュータを使用したものが一般的になりつつある。日本新聞協会では、これらの電送機やシステム装置間の通信のための推奨プロトコルを制定した。

ここではアナログおよびデジタル公衆回線でのNSKプロトコルの概要を説明する。

1.2.1. 関係する国際標準化機関と活動

データ通信分野における国際標準化機関には、ISO(注7)とITU-TS(注8)がある。ISO規格は、各国の国家規格が準拠するべく定められたもので、ITU-T勧告は、実際に国際間、装置間の通信を支障なく行なうための標準である。

ISOでの情報処理分野の活動は、TC97で行なわれている。日本新聞協会が策定したNSK TIFFに影響を与えた印刷分野の標準TC130も、同じISOに母体がある。ITUではファクシミリ、テレックス、ビデオテックスなどのテレマティック端末を担当している。SG7ではデータ通信網を、SG8ではプロトコルを、SG17では電話網によるデータ通信を、SG18ではISDN関係をそれぞれ担当している。

注7) International Standards Organizationの略。国際標準化機構。工業関連分野の様々な標準化を行なう国際機関。

注8) International Telecommunication Union-Telecommunication Standardization Sectorの略。国際電気通信連合電気通信標準化セクター。電気通信関連の研究や勧告の策定を行なう。1993年にCCITTが組織改編されたこととともない改称された。

1.2.2. OSI基本参照モデル

様々な国際標準を開発してきたISOは、ハードウェアやネットワーク特性にとらわれない形での、システム間の通信および相互操作性を実現するための概念モデルとして、**OSI基本参照モデル**（注9）を発表した。これはISOではIS 7498、ITUではITU X.200として制定されている。OSI基本参照モデルは、図1.1の通り7層で構成されている。通信網に近い方を下位層、アプリケーション層に近い方を上位層と呼んでいる。ISOのなかでは、トランスポート層以下の下位層はSC6が、セッション層以上の上位層はSC21が担当している。

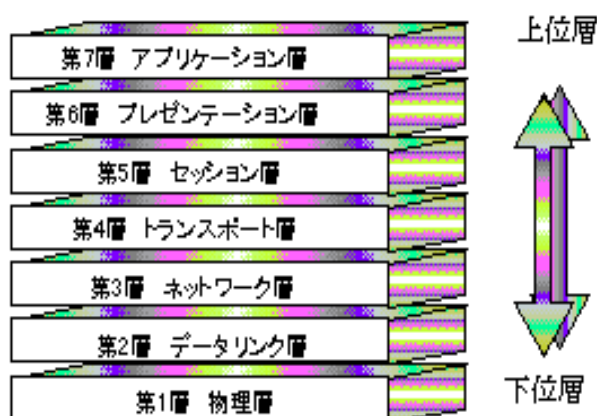


図1.1 OSI基本参照モデル図

第7層	アプリケーション層	アプリケーションで必要とされる通信サービスの提供、ファイル転送、メッセージ交換
第6層	プレゼンテーション層	データ表現形式の変換、マシンの種類に応じたデータの種類の形式の変換
第5層	セッション層	同期を取ったり、全半二重通信を行う、仮想通信回線の接続、切断、緊急通信
第4層	トランスポート層	透過的に送るデータ転送機能、通信網の品質が良くないときなどの訂正、補完
第3層	ネットワーク層	通信経路の選択やデータの中継を行う、複数のネットワークを介して接続する機能
第2層	データリンク層	同一ケーブル上で接続された装置間でのデータを交換する機能
第1層	物理層	コネクタの形状、ピン配置等の物理的な規定 モデム、DSUとのインターフェースの規定

表1.1 OSI基本参照モデルの意味

注9) Open System Interconnection Basic Reference Modelの略。7つの層から構成され、各層においてネットワーク機能を規定している。

表 1 . 1 に O S I 基本参照モデルの各層の意味を示す。このように通信プロトコルを 7 つの階層に分け細かく規定する理由は、技術革新によりある層が古くなっても、該当する層の改善だけで相互通信や装置対応に対処できるからである。

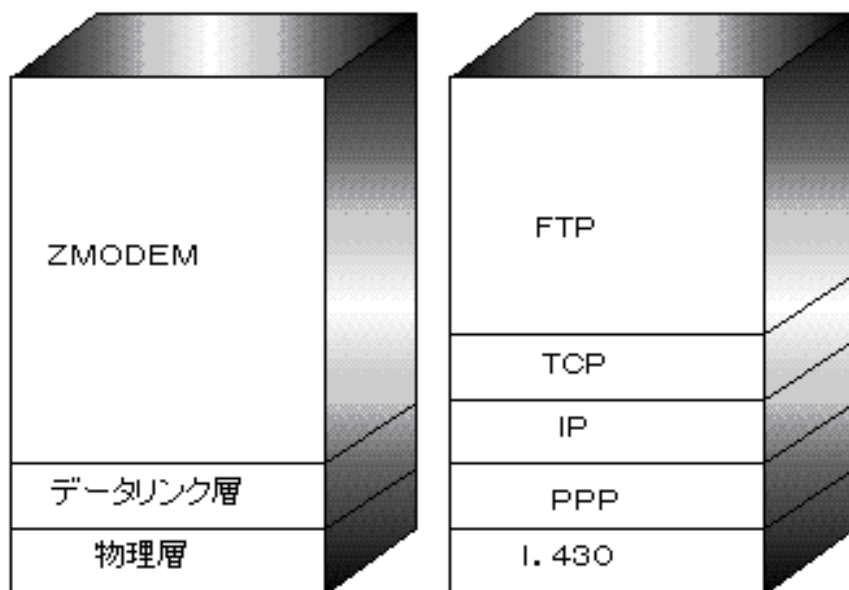


図 1 . 2 アナログ公衆回線およびデジタル公衆回線での日本新聞協会推奨プロトコルのイメージ

図 1 . 2 に日本新聞協会での N S K T I F F の電送のため定めた推奨プロトコルのイメージを示す。アナログ公衆回線でのプロトコルで Z M O D E M には、ネットワーク層の機能がないなど、厳密な意味では O S I モデルにあてはめることは妥当ではない。今回策定したプロトコルの概念としてこのように表現することが可能である。

1.2.3. アナログ公衆回線用プロトコルの概要

(1) 概要

アナログ公衆回線用プロトコルはZMODEMを採用している。ZMODEMは、アメリカのパソコンユーザーが開発したファイル転送のプロトコルをバイナリファイルも転送できるように、1987年にオーメンテクノロジー社が改善したものである。このZMODEMはほとんどのパソコン通信ソフトがサポートしている非同期通信プロトコルの標準的存在である。

(2) プロトコル要約

ZMODEMではユーザーデータを透過的に送信する。データは図1.3のようなフレームで構成されている。

(a) フレーム構成

データはヘッダーとデータサブパケットから構成される。ヘッダーは4種類、データサブパケットは2種類で用途に応じて使用される。データサブパケットはない場合と複数ある場合があり、可変長。

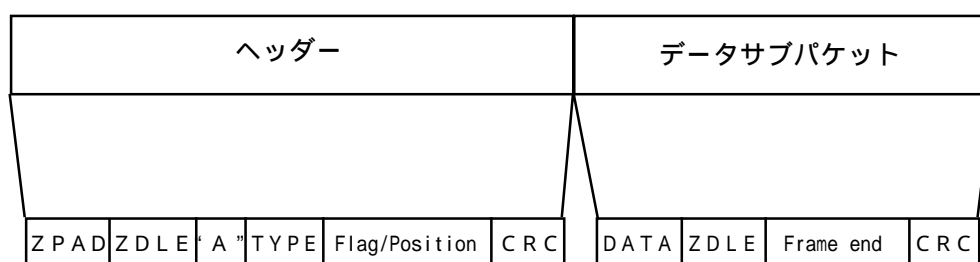


図1.3 ZMODEMのフレーム構成の一例

(b) 転送シーケンス

ZMODEMのファイル転送は送受信ともフレーム単位で行う。図1.4にZMODEM転送シーケンス例を示す。

送信側は再送要求が受信側より送られてこない限り送信データを送り続ける。受信側では送られてきたデータの整合性をチェックし、エラーが発生した場合はエラーの発生した場所の位置を送信する。送信側から指定されたデータを再送する。

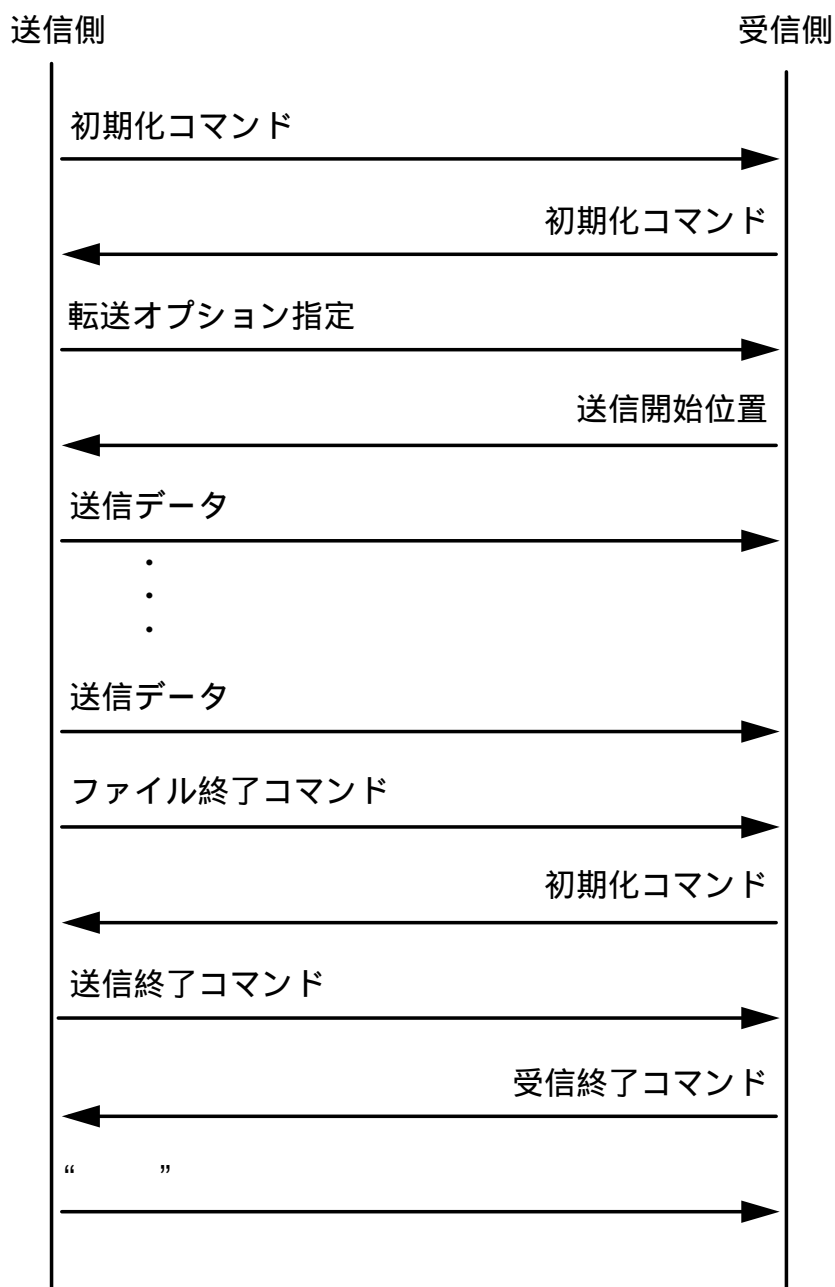


図1.4 ZMODEM転送シーケンス例

1.2.4. デジタル公衆回線用プロトコルの概要

(1) 概要

デジタル公衆回線用プロトコルとしては、TCP/IPを中心として、PPP、FTPを、関連プロトコルとして採用を決めた。TCP/IPは1960年代末に米国DARPA（国防総省高等研究計画局）の広域分散コンピューター・ネットワーク研究により誕生したプロトコル群であり、米国の大学、研究所を結ぶ研究者用ネットワークARPANETで採用された。また、BSD系UNIXが標準として採用したため全世界で急速に広まり、地球規模のネットワークであるインターネットでも、TCP/IPが使われ、実績の高さからUNIX以外の環境でも採用が進んでいる。

図1.5にデジタル公衆回線での推奨プロトコルの構成を示す。NSKプロトコルとしては、通信路の開設に必要なプロトコルとしてPPP、パケットの転送・経路制御のためにTCP/IP、ファイル転送のためにFTPを推奨とした。

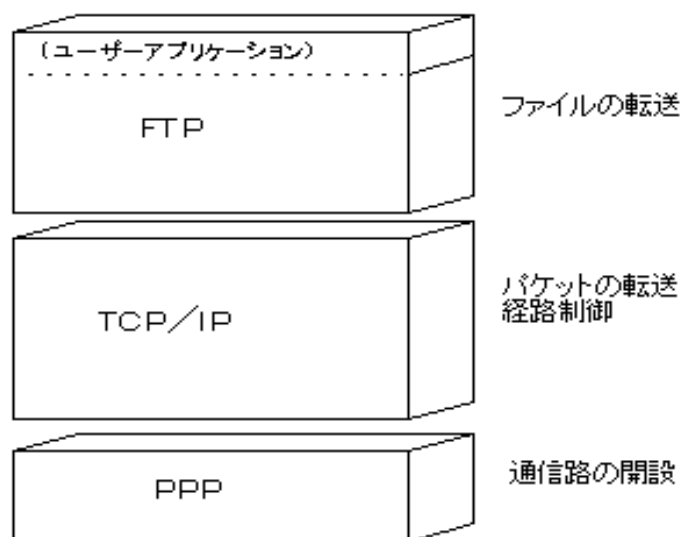


図1.5 デジタル公衆回線での推奨プロトコルの構成

(2) 各プロトコルの要約

NSKプロトコルは、デジタル公衆回線でのファイル転送に以下の各プロトコルが使用される。

(a) PPP

PPPは、回線に接続するインターフェース装置と、回線上でデータ伝送するためのプロトコルである。特徴は、複数の上位プロトコルに対応、認証、エラー検出、IPアドレスの情報交換、パケットヘッダー部の圧縮などの機能が利用できることである。

(b) T C P / I P

T C PとI Pはそれぞれのレイヤごとのプロトコル名称であるが、T C P / I Pと表現される場合には、実際に通信を行う上で利用されるプロトコル群全体を指す。

T C Pは、特定のサービスを提供するサーバー・プロセスにデータを送り届けるために用いられる。

I Pは、I Pアドレスを持つホスト間でパケット(データグラム)を送り届けるために用いられる。

(c) F T P

F T Pは、T C Pのトランスポートサービスを利用して、異なった仕様を持つコンピューター間においても、信頼性の高いファイル転送を実行する重要なプロトコルである。特徴は、クライアントとサーバーの認証、ファイル所有権、アクセス保護、データフォーマット変換などの機能が利用できることである。

1 . 2 . 5 . 適用範囲と運用上の注意点

N S Kプロトコルは、既存のプロトコルの中から業界内で共通に使用できるものを選定し規定した。

アナログ公衆回線用のZ M O D E Mは、一般に普及しているパソコン用通信ソフトとの互換性も狙っている。オプション機能の選択については、コンフォーマンステストの結果により、今後変更することがある。

デジタル公衆回線用のデータリンク層P P Pは、この層のネットワークプロトコルの中で現在は主流である。今後、新しい回線インフラの登場や見直しで大きな変更があったときは、O S Iモデルの主旨どおりN S Kプロトコルでも更新する必要がある。上位層のF T Pは、N S Kプロトコルのファイル転送プロトコルとして極めて基本的なものと位置付ける。実際の通信は、このF T Pの応用アプリケーションを利用して実現される。

通信においては、セキュリティーに配慮する必要がある。特にT C P / I Pでは十分に通信の安全性が保たれるよう工夫すべきである。

N S Kプロトコルの運用は、日本新聞協会が定めた運用管理規定に従わなければならない。N S Kプロトコルの運用管理規定を第4章に掲載した。これは基本的なガイドラインとしてまとめたものである。外国通信社など日本新聞協会加盟社以外に対して強制するものではない。日本における円滑なデジタル写真の交換のため、今後協会内の関係部会などでさらなる詳細規定の策定や審議を必要とする。

第2章 アナログ公衆回線での推奨プロトコル

アナログ公衆回線におけるNSK T I F Fの転送方式としてZMODEMプロトコルを採用した。モデムについてはITU-TのVシリーズ勧告を、ファイル転送のプロトコルはパソコン通信で広く使用されているZMODEMを採用した。

2.1.では現在主流になっているモデム伝送技術の概説、2.2.はファイル転送プロトコルであるZMODEMの概説、2.3.ではZMODEMのオプション規定を記述する。2.4.ではモデムプロトコルで規定されていない回線接続、切断のシーケンスの運用方法について規定している。

第2章 目次

2.1.	適応モデム技術	
2.1.1.	はじめに	16
2.1.2.	Vシリーズ勧告	16
2.1.3.	NSKプロトコルで適用するモデム勧告規格	17
2.1.4.	V.34/V.42技術解説	19
2.2.	ZMODEMプロトコルの機能	
2.2.1.	ZMODEMの概要	21
2.2.2.	ZMODEMの基本仕様	23
2.3.	オプション機能使用規定	
2.3.1.	オプション機能使用規定	29
2.4.	回線接続と運用方法	
2.4.1.	回線接続と切断のための推奨パラメーター	32
2.4.2.	回線接続	33

2.1. 適応モデム技術

2.1.1. はじめに

ここでは一般アナログ公衆回線を使用した伝送に必要なモデム技術を規定、解説している。モデムを使用した通信では相互接続できるかどうかの技術的問題はないものとする。モデムの基本的な機能についてはITU-TのVシリーズ勧告を技術標準としているためである。

以下にVシリーズの中で必要な勧告の概要とアプリケーションからみた解説を行う。

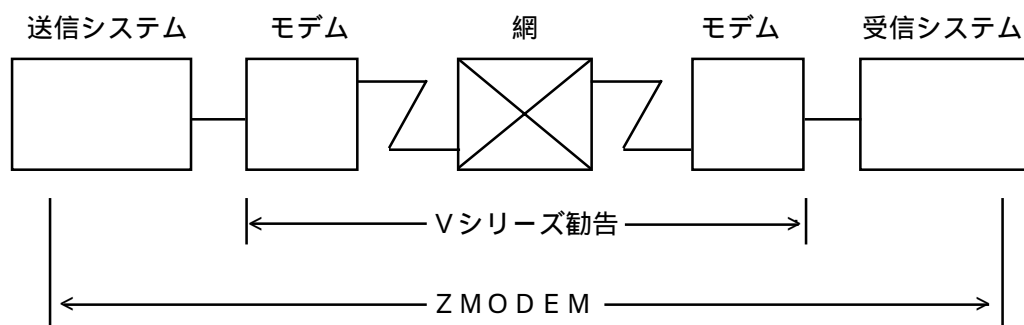


図2.1 第2章で規定している範囲

2.1.2. Vシリーズ勧告

ITU-TはITUの常設機関であり電気通信に関する技術運用面から研究勧告を行っている。これらはITU-T勧告と呼ばれA、B・・・、Zシリーズがある。

Vシリーズ勧告は有線通信の技術基準、運用規則を定め、電話網などにおいてデータ通信に使用される装置、伝送方式を定めた勧告である。その中でも今回のアナログ公衆回線伝送用のNSKプロトコルについて記述する。

なお詳細な規格等についてはITU-T発行の勧告書に基づくものとする。

2.1.3. NSKプロトコルで適用するモデム勧告規格

(1) NSKプロトコルで適用するモデム勧告

通信プロトコルはITU-T Vシリーズ勧告のV.32以上とする。アナログ公衆回線で一般に使用されているモデムは表2.1の通り。

Vシリーズ勧告	最大通信速度	主な特徴
V.21	300bps	全二重通信方式
V.22	1200bps	周波数分割による全二重通信 差動位相変調による同期伝送
V.22 bis	2400bps	V.22と互換性をとるために同じ周波数分割を採用した全二重通信
V.32	9600bps	エコーキャンセル技術によるチャンネル分割直交振幅変調方式の採用
V.32 bis	14.4Kbps	トレリス符号によるTCM変調方式の採用により、リトレインなしでダイナミックに通信速度が変えられる
V.34	28.8Kbps	4次元トレリスコーディング、プリエンファシス、プリコーディングを初めとするS/N向上技術の採用

表2.1 主なVシリーズモデム勧告

(2) MNPの取り扱いについて

MNPとはMicrocom Network Protocolの略で米国Microcom社が自社に使用したエラー訂正、圧縮方式である。

ホストに負荷をかけずに調歩同期伝送でエラー訂正、データ圧縮を実現したプロトコルである。機能によりMNPクラス1からクラス10までである。

MNPは多くのモデムに搭載されておりV.42シリーズのAnnex Aとしても制定されている。MNPの各クラスは基本的に上位互換性を持つ。このことがMNPが広く普及した原因のひとつと考えられる。現在主流になっているのはクラス4およびクラス5である。クラス4がエラー訂正機能、クラス5がデータ圧縮機能を規定している。MNPの最近の動向としてはMNPクラス10の設定が新たに追加、規定されている。これは移動体通信を利用したデータ伝送を想定した技術であり、これまでのMNPの内容とは異なる。悪条件の回線下でもリンクを保持し、その条件下で最高のスループットを確保することをねらったものである。

NSKプロトコルではMNPをオプションとして使用することを可能とする。ただし全てのクラスではなくクラス4、5、10の3種類。

MNPクラス	主な特徴
MNPクラス1	送られてきたデータに対し1回ごとにACKを返す、すなわちACKがこないと次のデータが送れないため高転送効率が望めない
MNPクラス2	エラー発生時にしかNAKを返さないためクラス1よりは効率がよい
MNPクラス3	モデム間が同期通信のためスタート、ストップビットを省略でき、ビット単位のフレームを採用して効率を上げている
MNPクラス4	伝送時のエラーを監視しており再送頻度が多くなるとパケットサイズを小さくして再送効率を上げる
MNPクラス5	伝送するデータを圧縮して転送効率を上げている
MNPクラス6	通信量の多い方向に対し、回線保有時間を多く与えて高速化している
MNPクラス7	クラス5の圧縮方式を採用
MNPクラス8	クラス6モデムにクラス7のデータ圧縮を採用、しかしクラス7、9と互換性がないため商品化が見送られた
MNPクラス9	ACKを送信時に一時的にデータ転送を中断していたがACKをデータパケットの中に埋め込み連続した伝送を行う
MNPクラス10	回線状態に合わせて適切なパケットサイズに切り替え、伝送スピードも高速側、低速側にもダイナミックにスピードを変え安定した通信をする

表2.2 MNPクラス一覧

(3) V.Fastモデムについて(V.FCモデム)

V.34勧告がまとまる以前にV.34規格のベースとなった技術を採用し、V.FastClassとして28.8Kbpsの通信速度をもつモデムが市販された。

このモデムはV.34のモデムと14.4Kbpsを超えるスピードでは互換性がなく通信ができないが、14.4Kbps以下ではV.34との間で相互通信が可能である。

2.1.4. V.34 / V.42 技術解説

これまでITU-TがV.Fastとして標準化作業を続けてきた超高速モデムの勧告がV.34として正式に国際標準となることが決まった。1994年2月ドラフト勧告を作成、6月に加速勧告化手続きを行い、10月には正式に国際勧告となった。V.34は従来のモデム技術とは大きく異なる部分が多い。

(1) V.34 モデム規格

V.22 bis までの2400 bps モデムの場合は帯域分割という方法で全二重通信を実現した。基本的には、アナログのバンド・スプリット・フィルタで1800 Hz以下とそれ以上にバンドを分け、それぞれ1200、2400 Hzのキャリアを用いて通信を行う。

それに対して、V.32 bis のモデムではともに1800 Hzのキャリアを使用して信号をぶつけ合い、エコーキャンセルフィルタを用いて、自己から出すキャリアの回り込みを除去しつつ通信を行う。通信開始時にはお互いのエコーキャンセルフィルタを学習させる。これにより伝送速度は14.4 Kbpsまで向上した。

V.34はV.32 bis で実現した14.4 Kbpsの伝送速度を上回る19.2 Kbpsとして開発され、最終的には28.8 Kbpsに対応した。

電話回線の帯域幅と伝送速度の間には密接な相関関係があり、シャノンの定理によれば28.8 Kbps モデムは音声帯域を使用するモデム原理として事実上境界の転送速度であると言われている。

V.34の高速化が可能になった技術背景には複数の変調速度およびキャリア周波数を使用したことが大きい。

以下にV.34 モデムで使用された新技術を紹介する。

(a) 4次元トレリスコーディング

複数の変調速度及びキャリアを用い、回線品質に応じてこれらの変調速度、キャリア周波数の組み合わせを変えている。また今までのモデムの伝送方法とは異なりV.34では伝送データをフレーム構造にしている。すなわち受信側と同期を取りながら送っており、このフレーム長は変調速度、キャリア周波数によって可変長となる。

(b) アダプティブパワー制御

送信側キャリアの出力レベルを回線によって調整する。このことによりPCM化による高調波歪を避けることが可能になる。

(c) プリコーディング

送信側でデータを符号化するときにはモジュロ演算を行い、符号化の片寄りを避けることによって受信側での複号化の際の判定をしやすくする。

(d) 非線形エンコーディング

回線品質によってある基準点となる信号の出力レベルが高い部分では互いに干渉し合わないよう信号の間隔を広げて通信する。

(e) アダプティブプリエンファレンス

従来固定であったイコライザーを送受信双方でダイナミックに調整して通信することによって最適値を決める。

(2) V.42 について

V.42 はフレーム同期で通信ができる V シリーズ全 2 重モデムに使用されるエラー訂正プロトコルである。

この規格は L A P M と呼ばれ H D L C をベースとするプロトコルである。また、M N P クラス 4 も A n n e x A として規定されている。I T U - T ではこの M N P クラス 4 のプロトコルはこのままで凍結し、今後の機能拡張は L A P M だけを対象にすることになっている。

2.2. ZMODEMプロトコルの機能

ZMODEMプロトコルは1990年頃に米国のオーメンテクノロジー社 (Omen Technology Inc.) が開発したアプリケーション間のファイル転送プロトコルである。このプロトコルはコンピューター上のファイルをアナログ公衆回線上でモデムを使用して非同期通信を行うことを目的としている。

2.2.1. ZMODEMの概要

ZMODEMはそれ以前に広く用いられていたXMODEM、YMODEMに比べて、高い効率と信頼性を考慮して設計されている。オーメンテクノロジー社では、以下のような点を考慮してこのプロトコルの設計を行った。詳細は「ZMODEM Inter Application File Transfer Protocol」に記載されている。なお、ZMODEMはパブリックドメインであり、ライセンス、トレードマーク、著作権に関する制限はない。ただし、ZMODEMのRLE圧縮はオーメンテクノロジー社が著作権を持っているので注意が必要である。

(1) 使用の容易性

- (a) 通信を行うどちらの側からも通信を開始することができる
- (b) バッチ処理中でのワイルドカードの使用が可能である
- (c) ZRQINITフレームを送信プログラムが送信することで自動ダウンロードが可能である。
- (d) タイムスタンプやその他の属性データを送信することができる

(2) スループット

ファイル転送プロトコルの設計ではスループットと信頼性という相反する事項のバランスが重要である。ZMODEMは次のような点について考慮をしている。低エラーレートの伝送路や、双方向で帯域をダイナミックに分割するモデムを使ったときの効率を上げるために、リバーチャンネルの通信量を減らす。高エラーレートで、遅延が大きいときにスループットを最適化するような動作は行わない。これにより、必要メモリ量を減らし、コードが複雑化しないようにしている。

(3) エラー訂正

ZMODEMのセッションが始まると、全ての処理は16 bit CRCあるいはオプションの32 bit CRC (注10)によって保護される。このデータの保護と情報の管理がZMODEMの信頼性を高くしている。32 bit CRCを使用するとエラーの見逃し率 10^{-5} の性能を発揮する。

(4) 幅広いシステムへの対応

ZMODEMは以下のような制限のあるコンピューターシステム上でも動作するように設計されている。

- (a) ディスクとシリアルI/Oが同時に動作しないようなシステム
- (b) シリアルポートの送受信が同時に動作しないようなシステム
- (c) XON/XOFFのフローコントロールが必要なコンピューターやネットワーク
- (d) データの受信完了を待たずに受信データをチェックできないコンピューター
- (e) エラーが発生したときの応答に時間がかかる場合があるタイムシェアリングシステム
- (f) X.25やMNPなどのエラー制御との重複使用

注10) 32 bit CRCはADCCP (ANSI X3.66 ITUT-T X.25) で決められている。

2.2.2. ZMODEMの基本仕様

(1) パケット化

ZMODEMフレームは、フレーム番号の上限が例えばXMODEMのように256に制限されない、可変長フレームへの対応などの特長を持つ。

(2) リンクエスケープコード化

ZMODEMはZDLEというエスケープシーケンスと拡張8bitキャラクターセットによってデータの透過性を保っている。

リンクエスケープコード化することにより、オーバーヘッドなしにデータサブパケットを可変長にできる。ZDLEキャラクターは重要な鍵であり、いくつかの種類のコントロールシーケンスを表現する。ZDLEの値は18 Hexである。これはアスキーコードのキャンセルキャラクターに相当し、YMODEMと同様に5個の連続したキャンセルキャラクターの送信でアボートできるように選択された。

ZDLEは通常の終了手順では使用しないため、相互のアプリケーションや通信プログラムはデータフローをモニターする事でZDLEを発見することができる。ZDLEに続くキャラクターはファイルやダウンロードコマンドを自動的に受信するためのZRQINITヘッダーを表すために使用される。

(3) ヘッダー

すべてのZMODEMフレームはバイナリヘッダーかHEXヘッダーのどちらかで始まる。ZMODEMヘッダーはある特定の場所を参照することによってヘッダーの種類を判定できる構造となっている。

(a) 16bitCRCバイナリヘッダー

バイナリヘッダーは送信側から受信側へ送信される。バイナリヘッダーはZPAD、ZDLE、ZBIN(アスキーコードのA)の順序で開始する。これに続き、タイプバイト、4バイトのポジション/フラグ、2バイトの16bitCRCが送信される。

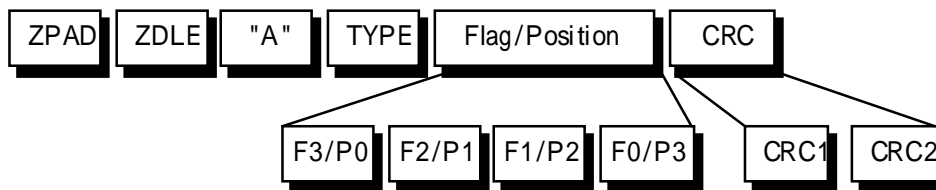


図2.2 16bitCRCバイナリヘッダー

(b) 32 bit CRC バイナリヘッダー

32 bit CRC バイナリヘッダーは16 bit CRC バイナリヘッダーと以下の点を除き同じである。ZBINキャラクターの代わりにZBIN32 (アスキーコードのC)が入る。最後に、4バイトの32 bit CRCが送信される。

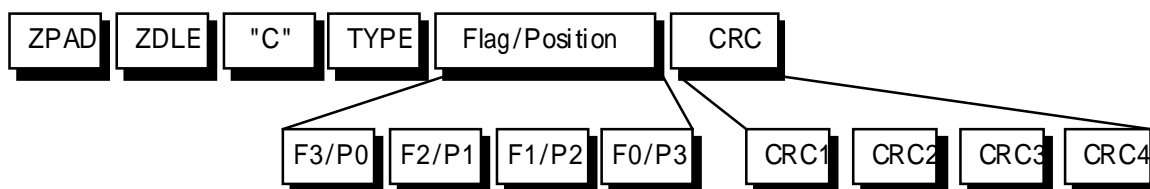


図2.3 32 bit CRC バイナリヘッダー

(c) 32 bit CRC - RLE バイナリヘッダー

32 bit CRC - RLE バイナリヘッダーは16 bit CRC バイナリヘッダーと以下の点を除き同じである。ZBINキャラクターの代わりにZBINR32 (アスキーコードのD)キャラクターが入る。最後に、4バイトの32 bit CRCが送信される。

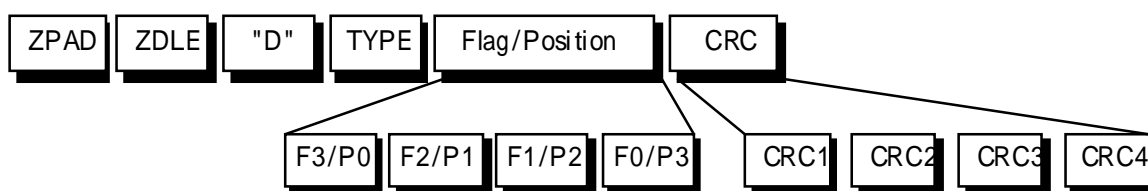


図2.4 32 bit CRC - RLE バイナリヘッダー

(d) HEXヘッダー

受信側はレスポンスとしてHEXヘッダーを送信する。HEXヘッダーはZPAD、ZPAD、ZDLE、ZHEX (アスキーコードのB)の順序で開始する。これに続き、2バイトのタイプバイト、8バイトのフラグ/ポジション、4バイトの16 bit CRC、CR、LF、XONの各キャラクターが送信される。タイプバイト、フラグ/ポジション、16 bit CRCはHEXコードで送信される。HEXヘッダーの32 bit CRC版は定義されていない。(図2.5 参照)

XON/XOFFフローコントロールを使用している場合は、XONキャラクターはZACKとZFINを除くすべてのHEXヘッダーに付加されるが、他のフローコントロールを使用する場合はXONキャラクターを送信しなくても良い。XONキャラクターはラインノイズなどによって誤って発生したXOFFキャラクターによる送信の停止を解除する。

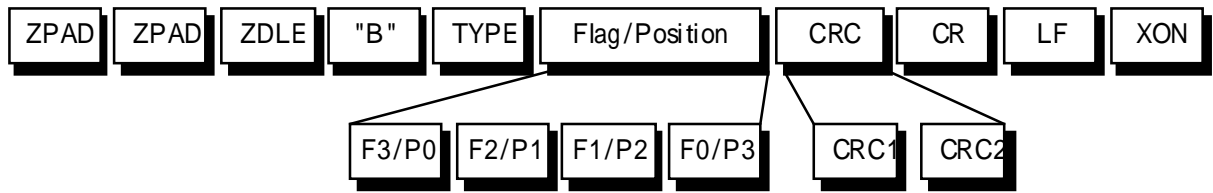


図 2 . 5 H E Xヘッダー

(4) データサブパケット

送信すべきデータの本体部分はデータサブパケットに収容され、以下の図のように、バイナリヘッダーのすぐ後に続いて送信される。

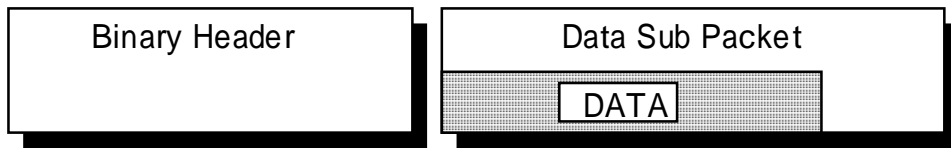


図 2 . 6 バイナリヘッダーとデータサブパケット

(a) バイナリデータサブパケット

一つのバイナリデータサブパケットは0から1024バイトのデータで構成される。推奨されているパケット長は2400 bps以下の時256バイト、2400 bpsで512バイト、4800 bps以上あるいは信頼性が高い回線では1024バイトである。

バイナリデータサブパケットでは余分なデータは付加されない。データはZDLEでリンクエスケープコード化され送信される。ZDLEコード化されたCRC(2/4バイト)が、一つのZDLEとフレームエンドに続いて送信される。CRCはデータバイトとフレームエンドが計算対象となる。(図2.7参照)

(b) R L Eバイナリデータサブパケット

送信しようとするファイルが圧縮に適しているときには、転送時間を短縮化するためにランレングス圧縮を行ってもよい。この場合は、ZBINR32に続いてRLEバイナリデータサブパケットを送信する。ZMODEMで使用するRLE圧縮はオーメンテクノロジー社が著作権を持っている。

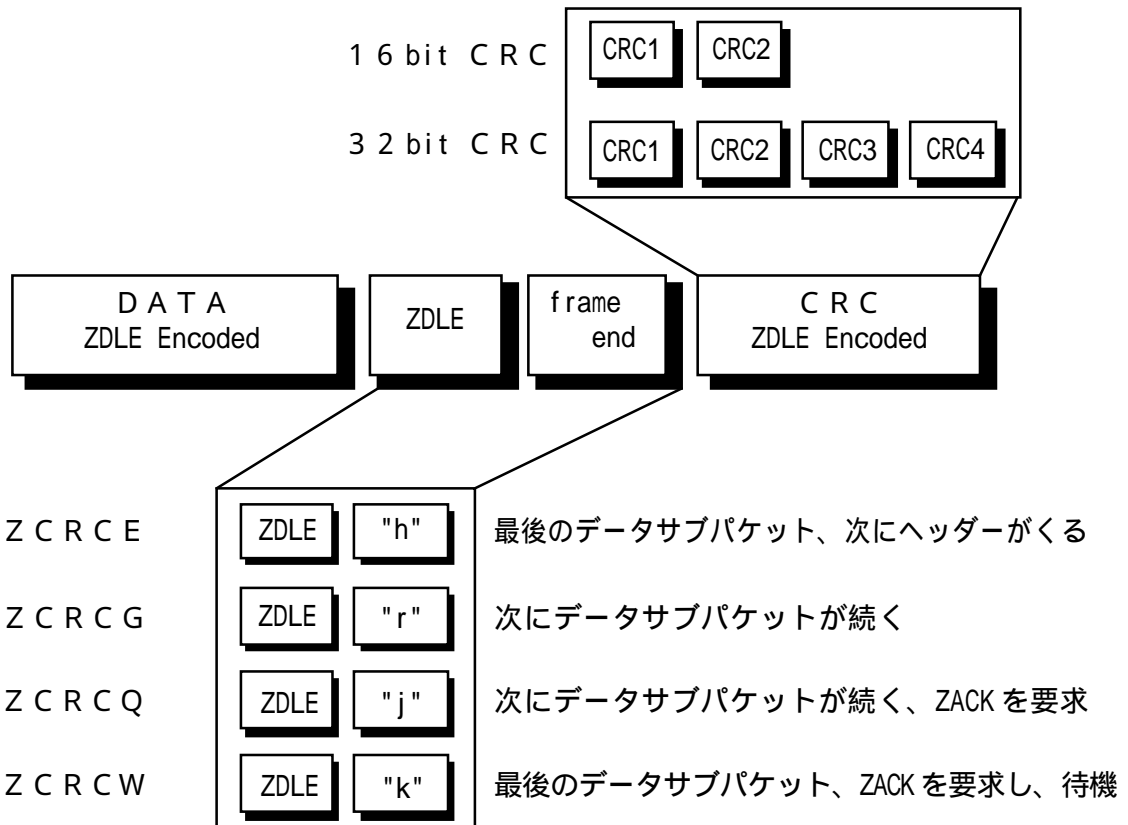


図 2 . 7 バイナリデータサブパケット

(5) プロトコル処理の概要

ZMODEMのタイミングは受信側が主導権を持つ。受信側が1分間何のヘッダーも受信できずにアボートする場合を除いて、送信側はいかなる時もタイムアウトを起こしてはならない。

送信側、受信側は、共に回線切断の際すぐにアボートができるように十分な頻度でキャリアあるいはそれに相当する信号の検出をしなければならない。ZMODEMは、エラー訂正の場合を除き、ファイルの転送中に送信側は受信側からのレスポンスも受け取らない。

以下にプロトコルの流れを説明する。(図 2 . 8 参照)

(a) セッションの開始

セッションを開始するには、送信プログラムを送信されるファイルのファイル名とオプションをパラメーターとして起動する。

送信側は受信側が現在コマンドモードにあるかどうかを確認するために、“ r z ¥ r ”を送信することができる。次に、送信側はZRQINITヘッダーを送信する。

一方、受信側はプログラムの起動後とZRQINITヘッダーを受信したときは、ZRINITヘッダーを送信する。最終的に送信側プログラムはZRINITヘッダーを受信する。

送信側は受信側からファイルの転送をスタートさせるためのコマンドがくるのを待つ。標準のZMODEMではここでYMODEM、XMODEMへの切り替えが可能であるが、本規定ではこのオプションを推奨しない。間違ったコマンドを受け取った場合、送信側プログラムはセッションが正常に開始されるまで何回でもコマンドを要求することができる。

(b) ファイル転送

送信側はZFILEヘッダーに続いて、ファイル名、ファイル長、変更日などの転送オプション情報を送信する。受信側は受信した転送オプションに対応できるかを判断する。転送オプションに答えられない場合はZRSKIPヘッダーなどで応答する。答えられる場合はZRPOSヘッダーで応答する。ZRPOSヘッダーには受信側が期待するファイルの送信開始位置を含む。通常は新規ファイルとなるのでファイルの先頭となる。レジューム機能が指定された場合は、ファイルの途中を送信開始位置とする。

送信側は、ZRPOSヘッダーで指定された位置からデータの本体部分をZDATAバイナリヘッダーを使って送信する。

受信側はZDATAバイナリヘッダーにあるファイルポジションと、正常に受信できたバイト数を比較する。もしエラーを検出したら、ZRPOSヘッダーをエラー応答として返し、送信側に再送を開始する位置を知らせ、再送信を要求する。

致命的なエラーが起こらなければ、送信側はいつかはファイルの最後に到達する。送信側はファイルの総バイト数の情報を含むZEOFヘッダーを送信する。受信側はこの数と受け取ったバイト数を比較する。この比較によって受信側がファイルをすべて受け取ったと認識すると、受信側はファイルをクローズする。ファイルのクローズができたら、受信側はZRINITを返す。異常の場合はZRPOSヘッダーをエラー応答として返す。この場合、新たにZDATAが来るため、ZEOFは無視する。受信側がファイルを適切にクローズできなかつたら、ZFERヘッダーを送信する。

(c) セッションのクリーンアップ

送信側は、セッションを閉じるためZFİNヘッダーを送信する。受信側は、これに対して同じくZFİNヘッダーを返す。

送信側はZFİNヘッダーを受信したら、“OO”(Over and Out)を返し、セッションを終了する。受信側は、“OO”を待ち、受信してもしなくてもセッションを終了する。

(d) セッションの中断

送信側、受信側は共に通信中にセッションを中断するときキャンセルシーケンスを送信する。キャンセルシーケンスでは8個のCANキャラクターと10個のバックスペースキャラクターを送信する。

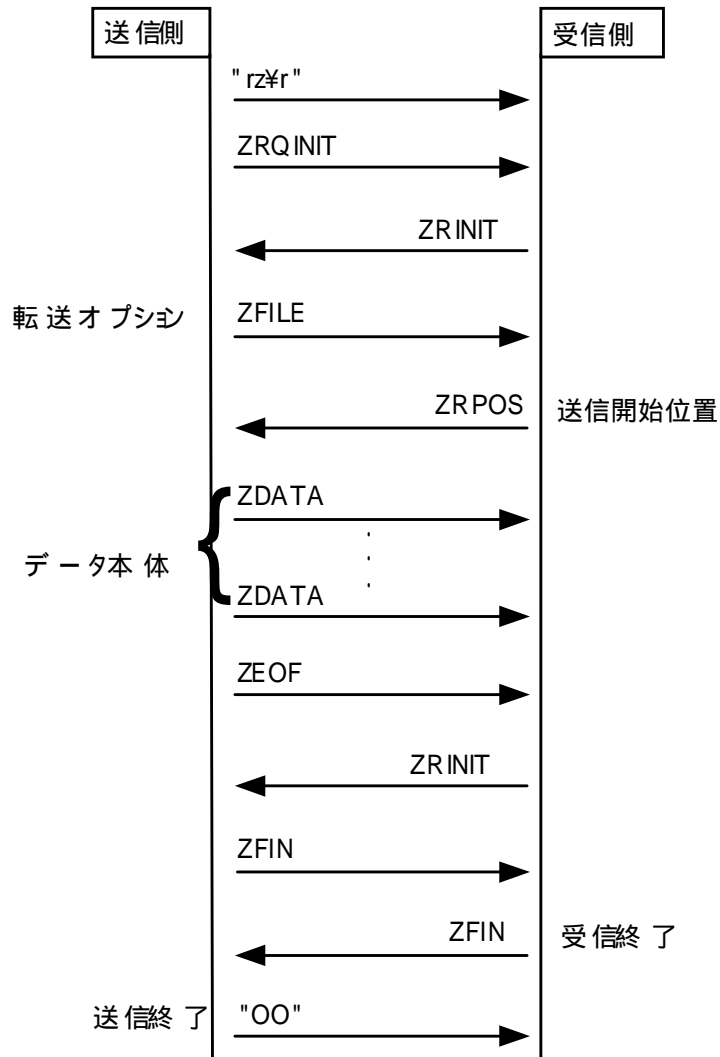


図 2 . 8 ZMODEMの通信例

2.3. オプション機能使用規定

2.3.1. オプション機能使用規定

ZMODEMプロトコルにはいくつかのオプション機能がある。本章では日本新聞協会が推奨するオプション機能の使用方法を規定する。

(1) YMODEM、XMODEMのサポート

ZMODEMでは相手方がZMODEMをサポートしない場合YMODEM、XMODEMを試みることができるとしている。本規定では信頼性などの点から、YMODEM、XMODEMを使用しないことを推奨する。

(2) 複数ファイルのサポート

ZMODEMでは複数のファイルを1回のセッションの中で送信する方法を定義している。しかし、この機能が無くても送信側がセッション終了後、ZRINITから再度繰り返せば特に支障はない。通信効率に影響を与えるほどのものではないし、回線を切断せずに続けて送信が可能である。この理由から本規定では、複数ファイルのサポートを必須としない。

(3) ZRINITオプション

ZRINITに複数のオプションがある。以下にその使用方法のガイドラインを記述する。

- (a) 全二重、ディスクI/O中の受信、ブ레이크信号の送信機能は、必須としないが、ほとんどのシステムで無理なく実現できると思われるためサポートすることを推奨する。
- (b) RLEのサポート、LZW圧縮化データのサポートは本規定の使用法と合わないため、使用しないこととする。
- (c) 通信の信頼性の向上のため、CRCはCRC32の使用を推奨する。ZMODEMの規定ではCRC16が必須であり、CRC32はオプションとなっている。
- (d) 制御文字、8ビットコードのエスケープは本規定の使用法では必要ないため、使用しないこととする。
- (e) 可変長ヘッダーは扱えるようにすることを推奨する。

以下にZRINITオプションのフラグ位置と本規定での使用法をまとめる。

フラグ	ビット	内容	本規定での使用方法
ZF0	0	全二重	必須としないが、サポートすることを推奨する
ZF0	1	ディスクI/Oの中の受信	必須としないが、サポートすることを推奨する
ZF0	2	ブ레이크信号の送信	必須としないが、サポートすることを推奨する
ZF0	3	RLEのサポート	使用しない
ZF0	4	LZW圧縮データのサポート	使用しない
ZF0	5	CRC16/32	CRC32の使用を推奨する
ZF0	6	制御文字のエスケープ	使用しない
ZF0	7	8ビットコードのエスケープ	使用しない
ZF1	0	可変長ヘッダー	扱いができることを推奨する

表2.3 ZRINITオプション

(4) ZFILEオプション

ZFILEに複数のオプションがある。以下にその使用方法のガイドラインを記述する。

- (a) レジューム転送はオプションとする。
- (b) ZMNEWL、ZMAPND、ZMCLOB、ZMNEW、ZMDIFF、ZMPROT、ZMCHNGの各オプションはファイルを上書きしたり、受信側で混乱することがあるので、使用しないものとする。
- (c) LZW、RLE圧縮は、使用しないこととする。

以下にZFILEオプションのフラグ位置と本規定での使用方法をまとめる。

フラグ	名称	内容	本規定での使用方法
ZF0	ZRECOV	レジューム機能	必須としないが、送受信合意の上使用しても良い
ZF1	ZMNEWL	日付による制御	使用しない
ZF1	ZMCRC	サイズによる制御	使用しない
ZF1	ZMAPEND	追加	使用しない
ZF1	ZMCLOB	上書き	使用しない
ZF1	ZMNEW	日付による制御	使用しない
ZF1	ZMDIFF	サイズによる制御	使用しない
ZF1	ZMPROT	スキップ	使用しない
ZF1	ZMCHNG	ファイル名の変更	使用しない
ZF2	ZTLZW	LZW圧縮	使用しない
ZF2	ZTCRYPT	暗号化	使用しない
ZF2	ZTRLE	RLE圧縮	使用しない

表2.4 ZFILEオプション

(5) ファイル名オプション

ファイル名の決め方は規定しない。レジューム機能を使用する場合は、受信側ファイルのユニーク性を保つ必要があるので、注意を要する。

また、日付、パス名は使用しない。

(6) パケットサイズ

1024バイトを推奨値とする。ただし1024バイトを超えない範囲なら、特にサイズは規定しない。

2.4. 回線接続と運用方法

2.4.1. 回線接続と切断のための推奨パラメーター

実際の運用時にVシリーズの勧告の他にいろいろなモデムのパラメーター設定値を適切に決めることによって、より速い転送速度で安定に伝送することが可能になる。以下の一般公衆回線及びアナログ携帯電話使用時のモデム設定推奨値を基本とする。ただし、モデムの機種によっては設定方法が異なるものもあるので注意が必要である。

(1) 一般公衆回線使用時のモデム設定推奨値

項目	推奨値	設定内容詳細
自動フォールバック	使用	回線接続時、相手モデムのスピードに合わせる 回線品質が悪いときに自動的に通信速度を下げる
誤り訂正使用	使用	誤り訂正の有無の選択
誤り訂正方式選択	L A P M優先	誤り訂正方式の選択 L A P M / M N P 優先順位選択
M N P 最大ブロック長	2 5 6 Byte	M N P プロトコル使用時の最大ブロックの指定
動作モード	自動 リライアブル	モデムはエラー訂正モードを試みるがエラーリライアブル 訂正リンクモードが成功しなかった場合でもフォールバックし通信を行う
V . 4 2 bis	O F F	モデムによる圧縮使用の有無の選択
M N P 1 0 接続	選択	M N P クラス 1 0 誤り訂正機能の使用の有無 国際回線等回線品質の悪い時に O N にすると、より安定した通信が行える
オートリレーン	O N	モデムが回線品質を監視して、必要時には転送速度を落とす
発信時間	3 sec以上	ダイヤルトーンを検出してから実際に発信を開始する時間
キャリアー待ち時間	3 0 sec以上	相手モデムからのキャリアーを検出するまでの待ち時間、この時間内にキャリアーが検出できないとき、No Carrierとして回線を切断する
キャリアー検出時間	6 0 0 msec以上	相手モデムからのキャリアーが設定値より長い時間検出されなかった場合、回線を切断する

表 2.5 一般公衆回線使用時のモデム設定推奨値

(2) アナログ携帯電話使用時の設定

アナログ携帯電話を使用時の電送時には一般公衆回線のモデム設定に加えて表 2.6 の設定を行うとより安定した電送が可能になる。

項目	推奨値	設定内容詳細
MNP10 接続	ON	アナログ携帯電話を使用してモデムによる写真電送を行う場合は必ず有効にすること。また、国際回線を使用した通信時に有効とすれば、より安定した通信が行える。
回線速度	9600 bps	モデムどうしがネゴシエーション通信を開始する速度を設定。一般にアナログ電話は高速モデム通信にとっては回線品質が十分でなく、28.8 Kbpsからトレーニングを行うと実際に通信を開始するまでかなりの時間が必要となる。このため、あらかじめ開始通信速度を実際に通信できる速度に合わせるためのネゴシエーションを行う。

表 2 . 6 携帯電話使用時の追加設定

2 . 4 . 2 . 回線接続

ここでは実際にモデムを使用した伝送時における回線接続から ZMODEM 転送が始まるまで、および ZMODEM 転送終了後に実際に回線を切るまでのシーケンスの推奨手順を示す。

(1) 回線接続から ZMODEM 転送開始までの網制御シーケンス

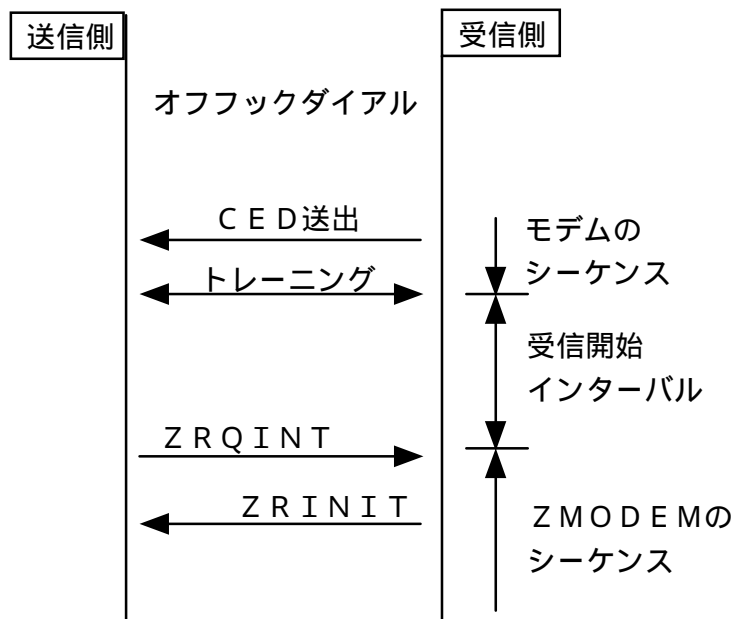


図 2 . 9 接続シーケンス

トレーニング終了時から ZRQINIT 信号が送受されるまでの最大時間推奨値 (受信開始インターバル) を 30 秒とする。この時間以内に ZRQINIT コマンドが受信できない場合は回線を切断するのが望ましい。

(2) リダイヤル時の注意事項

電気通信事業法の端末設備規則により、リダイヤル時の発信と発信の間隔には60秒以上の待ち時間が必要。

(3) ZMODEM終了後の回線切断の網制御シーケンス

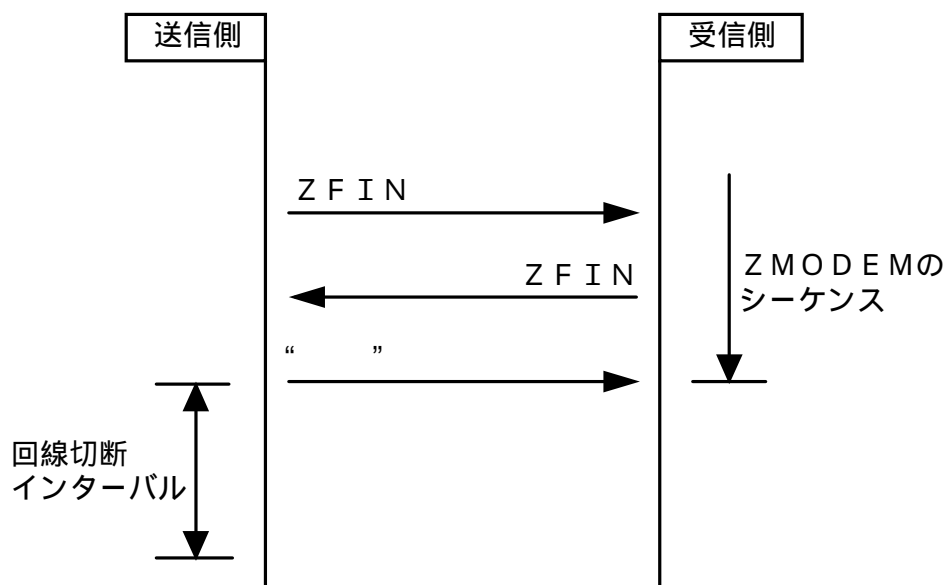


図2.10 切断シーケンス

ZMODEM正常終了時(“OO”送出時)から回線切断までの推奨時間(回線切断インターバル)を3秒以上とする。

第3章 デジタル公衆回線での推奨プロトコル

デジタル公衆回線における「NSK T I F F」の転送方式としてインターネットネットワーク技術を採用することとした。TCP/IPを中心としたインターネットネットワーク技術は、ネットワークに接続されたどの端末間でも容易にデータのやりとりができる標準的な方式で、拡張性も優れている。第3章では、このインターネットネットワーク技術に関する技術的要件を解説する。

3.1.ではISDNを利用したネットワーク接続技術について、3.2.では現在主流となっているデータリンク層プロトコルとしてPPPを、3.3.では推奨プロトコルとして採用したTCP/IP通信について、3.4.ではファイル転送プロトコルのFTPとその関連アプリケーションについて、3.5.ではネットワーク接続におけるセキュリティーについて記述する。

第3章 目次

3.1.	適用ハードウェア技術	
3.1.1.	ISDN(INSネットサービス)の概要	36
3.1.2.	ISDN利用技術と構成要素	39
3.1.3.	適用ルーター技術	45
3.2.	PPP	
3.2.1.	PPPの概要	48
3.2.2.	LCP	51
3.2.3.	NCP	54
3.3.	TCP/IP	
3.3.1.	TCP/IPの概要	56
3.3.2.	IP	58
3.3.3.	TCP	61
3.4.	FTPと関連アプリケーション	
3.4.1.	FTP	64
3.4.2.	関連アプリケーション	69
3.5.	セキュリティー技術	
3.5.1.	セキュリティーに対する基本的考え方	75
3.5.2.	アクセス制御	76
3.5.3.	パスワード	77
3.6.	関連するRFCの一覧	78

3.1. 適用ハードウェア技術

3.1.1. ISDN (INS ネットサービス) の概要

デジタル公衆回線におけるNSK T I F Fの転送方式として、TCP / IP (Transmission Control Protocol / Internet Protocol)を採用した。このTCP / IPをベースとして、例えばFTP (File Transfer Protocol)を利用して、T I F Fのファイルを転送する。

日本のISDNは、1995年現在、日本電信電話株式会社 (NTT) がTTC標準JTに規定されている勧告に準拠してインプリメントした交換網を構築し、INS ネットサービスとしてユーザーに提供している。ここではINS ネットサービスをベースに記述している。

(1) INS ネットサービスの特徴

(a) 高速転送

64 Kbps の高速でファイルの転送が可能となる。

例えば、1 MByte のファイル転送に要する時間と通信料をアナログ電話網 (通信速度を9600 bps とした場合) と比較すると、約6倍の違いとなる。

例) 東京 - - - 大阪間

INS ネット64	通信時間	約140秒	通信料	140円
アナログ電話網	通信時間	約930秒	通信料	930円

アナログ電話網はNTTを利用。いずれもダイヤル接続昼間帯10円 / 10秒伝送効率90%として計算。料金計算の基礎資料は、財団法人テレコム高度利用推進センター発行のテレコム・サービス料金便覧第18号1994年11月発行による。

(b) 発信者番号通知サービス

INS ネットでは、発信者の電話番号が着信端末に通知されるサービスがある。着信側であらかじめ登録した発信者の番号以外の接続を拒否するなどの手段により、不正なアクセスを防止し、セキュリティー機能を付加することができる。

(c) グループセキュリティーサービス

特定のグループ内での通信に限定する閉域接続サービス。あらかじめNTTに登録しておいた電話番号以外からの受信、あるいは登録以外の番号への発信を規制する。不正アクセス、誤発呼による情報の漏れを防止できる。

(2) サービスの種類

INSネットサービスにおける提供サービスのうち、本規定では回線交換の基本ベアラサービスである64 Kbps、非制限デジタル情報伝送とする。BチャンネルまたはDチャンネルパケット交換は使用しない。また回線交換のうち64 Kbps × 2のいわゆる128 Kbps バルク伝送機能は、ベアラサービスの上位層の規定とし、ここでは規定しない。

(3) プロトコルの規定

ユーザー・網インターフェースのプロトコル規定は、ISOやITU-Tで標準化されている開放形システム相互間接続(OSI)の7レイヤ(階層)モデルに準拠しており、網の制御に関する物理層、データリンク層およびネットワーク層の低位レイヤについて規定している。図3.1にユーザー・網インターフェースプロトコル階層構成を示す。

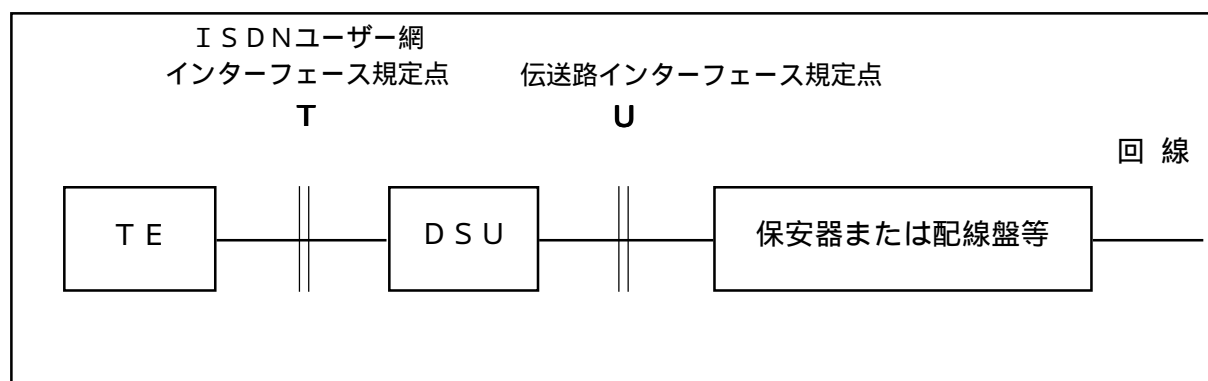
7	アプリケーション				
6	プレゼンテーション			FTP	
5	セッション				
4	トランスポート			TCP	
3	ネットワーク	情報チャンネル制御 手順(JT-Q931)		IP	
2	データリンク	LAPD(JT-Q921)		PPP	
1	物理	レイヤ1 プロトコル (JT-1430、JT-1431)			
レイヤ 適用対象		呼制御信号	パケット交換	回線交換	パケット交換
		Dチャンネル		Bチャンネル	

図3.1 ユーザー・網インターフェースプロトコル階層構成

(4) ユーザーインターフェースの規定点

INSネットサービスにおけるユーザーインターフェースの規定点を、図3.2に示す。図で示したT点は、TE(端末、ここでは写真電送装置またはパソコン等)とDSU(回線終端装置)の接続点であり、T点をユーザーインターフェースの規定点とする。

物理的なT点とは、具体的にはD S Uのバス接続のためのインターフェース接続点すなわち4線のネジ止め用品または8ピンのコネクターを規定する。



TE：パソコン等端末設備

図3.2 ユーザー・網インターフェース規定点

(5) レイヤ1 (物理層)

レイヤ1は、端末 (TE : Terminal Equipment) をDSU (回線終端装置) に接続するときの電氣的、物理的条件について規定するものである。具体的には、配線構成、フレーム構成、伝送符号、Dチャンネルアクセス制御、フレーム同期、電氣的特性および給電条件等が含まれる。

レイヤ1は、情報 (B) チャンネルと信号 (D) チャンネルの両方に対して共通に適用される。

レイヤ1プロトコルの規定は、ITU-T勧告のIシリーズに準拠し、電信電話技術委員会 (TTC : Telecommunication Technology Committee) が定めたTTC標準JT-I430に規定されている。日本のINSネットサービスは、日本電信電話株式会社 (NTT) がこの勧告に従ってインプリメントした交換網を構築し、ユーザーに提供しているものである。従ってINSネットサービスを利用するときは、NTTが発行しているレイヤ1の規定に従う必要がある。

(6) Dチャンネルアクセス制御手順 (レイヤ2、レイヤ3)

接続制御手順のためのDチャンネルアクセス制御手順の規定は、同じくTTC標準JT-Q921「ISDNユーザー・網インターフェース レイヤ2仕様」ならびにJT-Q931「ISDNユーザー・網インターフェース レイヤ3仕様」に準拠したNTT発行資料 (注11) に従う必要がある。

注11) 技術参考資料「INSネットサービスのインタフェース第2分冊 (レイヤ1編) 第3版」
 技術参考資料「INSネットサービスのインタフェース第2分冊 (レイヤ2編) 第5版」
 技術参考資料「INSネットサービスのインタフェース第3分冊 (レイヤ3回線交換編) 第4版」

3.1.2. ISDN利用技術と構成要素

デジタル公衆回線を利用した形態として、スタンドアロンのノード（注12）間同士を接続する基本的な形態（基本構成）と、ノード間に中継装置を介在させた形態（拡張構成）とに分けることができる。

(1) 基本構成

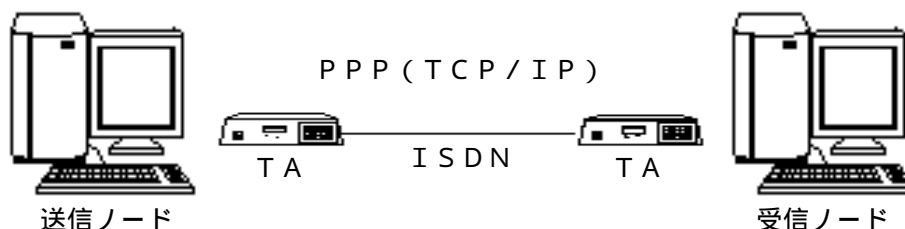


図3.3 基本構成

構成要素としては、次の通りである。

送受信ノード : NSK T I F F 電送機と受信装置

TA : TAは、TE 2（注13）タイプの端末を接続する時に必要。
TE 1（注14）タイプの端末は直接ISDN網に接続できるため不必要となるので、接続するノードの種類により選択する。

TAを使用する場合、送受信ノード～TA間のインターフェースについては、送受信ノード間の接続性に影響を与えないので任意とする。TA～ノード間のインターフェースには、X.21/V.35/RS-449/V.24などがある。

また、ワークステーション（以下WS）やパーソナルコンピュータ（以下PC）をISDN網に接続する場合、次の点を考慮しなければならない。

WSやPCは、基本的に同期通信はサポートされないため、そのままではISDNのBチャネルを使用した64 Kbpsでの伝送ができない。これを回避する方法として、次に述べる利用形態が考えられる。

注12) ネットワークに接続された端末など、ネットワークを構成する機器のこと。

注13) ISDN非標準端末のことで、Vインターフェース等を持っている端末を表す。

注14) ISDN標準端末のことである。

(a) Vシリーズ・インターフェース用T Aを使用する。

Vシリーズ・インターフェース用T A [勧告V . 1 1 0 (注15)] を、W S / P C のシリアルポートにR S - 2 3 2 C ケーブルで接続し使用する。V . 1 1 0 には、同期 / 非同期モードがあり、この場合は非同期モードで使用する事になるが、V . 1 1 0 勧告の中の非同期モードでサポートされている通信速度は、1 9 . 2 Kbps までである。ただし、T A の中には非同期モードで3 8 . 4 Kbps までサポートされているものもあり、そのT A 同士であれば3 8 . 4 Kbps での通信が可能である。この利用形態は、商用インターネット・プロバイダーのダイヤルアップ接続に使用されている方法である。

現在では、アナログ公衆回線においても高速モデムの出現により、同程度の通信速度が実現できるため、この形態ではI S D N を使用するメリットは以前より少なくなってきた。

(b) W S や P C に同期通信ボードを装着し、Vシリーズ・インターフェース用T Aを使用する。

これは、W S や P C に同期通信カード又は同期通信ドライバーを使用して、Vシリーズ・インターフェース用T A (勧告V . 1 1 0) を、同期モードの6 4 Kbps で通信する利用形態である。

この形態では、同期通信用のボードが必要でありコスト的に高くなる。また、同期通信用のボードを使用するためのA P I (注16) 等が、接続するノード間で統一されていないと相互接続性がなくなるため、使用上の注意が必要である。

(c) W S や P C にI S D N ボードを装着する。

W S や P C にI S D N ボードを装着し、直接I S D N に接続する方法が最も高速に伝送できる。

I S D N ボードの機能によるが、Bチャネルを同時に2本使用して1 2 8 Kbps の通信が可能な製品もある。しかし、現状ではボードメーカー独自の方式で行っており、相互接続を保証するには同一メーカーのボードを使用しなくてはならない。

なおI S D N ボードにおけるA P I の標準化作業は財団法人テレコム高度利用推進センターで行われている。

注15) この他に、V . 1 2 0 を使用したVシリーズ・インターフェース用T A があるが、多重化方式が異なるため相互接続はできない。V . 1 2 0 は主に米国で使用されている。

注16) アプリケーション・プログラム・インターフェースの略。

(2) 拡張構成

(a) 拡張構成 1 は、図 3 . 4 の通り受信ノードがローカルエリアネットワーク (以下 LAN) に接続されている形態であり、この場合 NSK T I F F データは送受信ノード間のみ P P P での伝送となる。

この形態の場合、使用するノードが U N I X の様にルーティングプロトコルを使用できる時は、**セキュリティ** (注 17) の問題からダイナミック (動的) ルーティングを行わないようにする必要がある。

構成要素としては、送信又は受信ノードが LAN とのインターフェースを持っている事を除けば、基本構成と同様である。

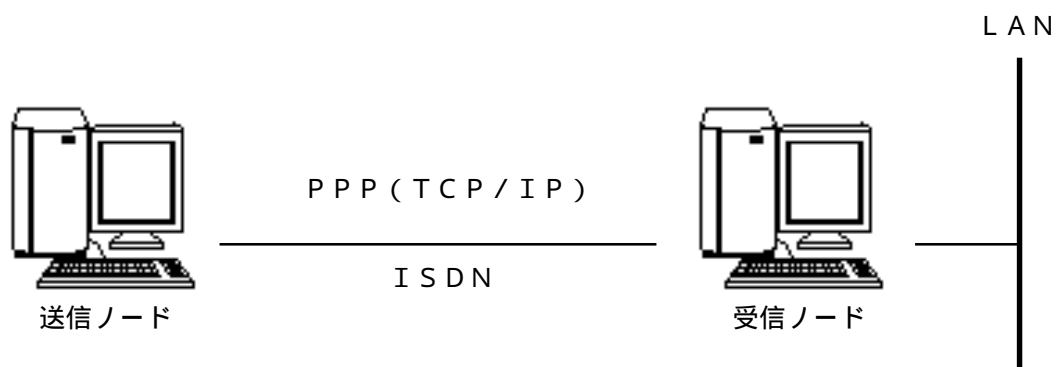


図 3 . 4 拡張構成 1

注 17) ルーティングプロトコルを読み取ることにより、接続相手のネットワークの構成、ネットワークアドレスのすべて (又は一部) が判ってしまうため、最悪の場合はネットワークに入り込まれたり、組織構成が分かってしまうといった問題が発生する。

(b) 拡張構成 2、拡張構成 3 の場合、片側または両側のノードが LAN に接続されている中継ノードを経由する形態であり、この場合、NSK T I F F データは、すべて中継ノードを経由して、送受信ノード間の伝送が行われる。

図 3 . 5 は、片側のノードが LAN に接続されている中継ノードを経由する形態で、図 3 . 6 が両側のノードが LAN に接続されている中継ノードを経由する形態である。

PPP による通信は、中継ノードから中継ノード、送信ノードから中継ノード、受信ノードから中継ノード間で行われる。

拡張構成 1 と同様にルーティングプロトコルを使用して、ダイナミック・ルーティングを行わない様にする必要がある。

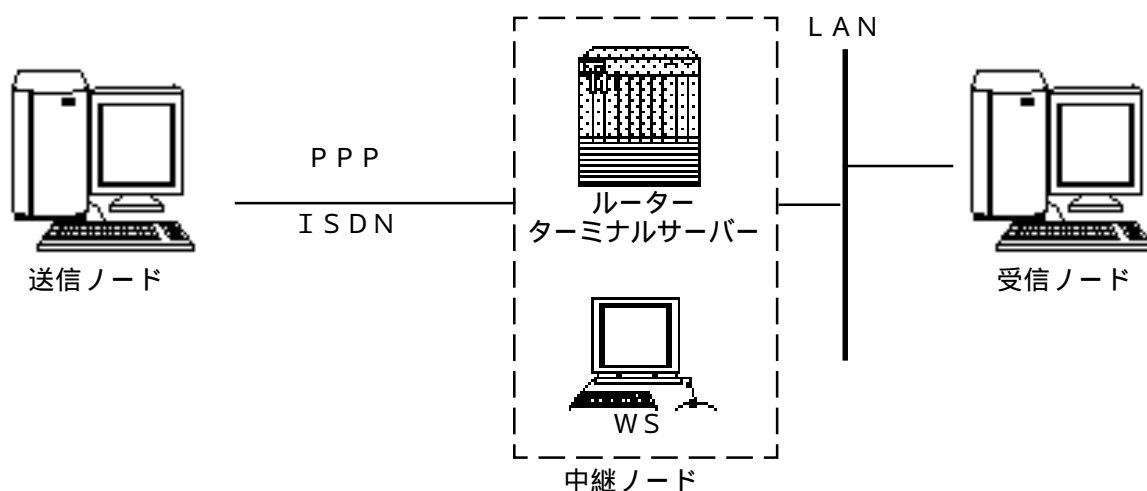


図 3 . 5 拡張構成 2

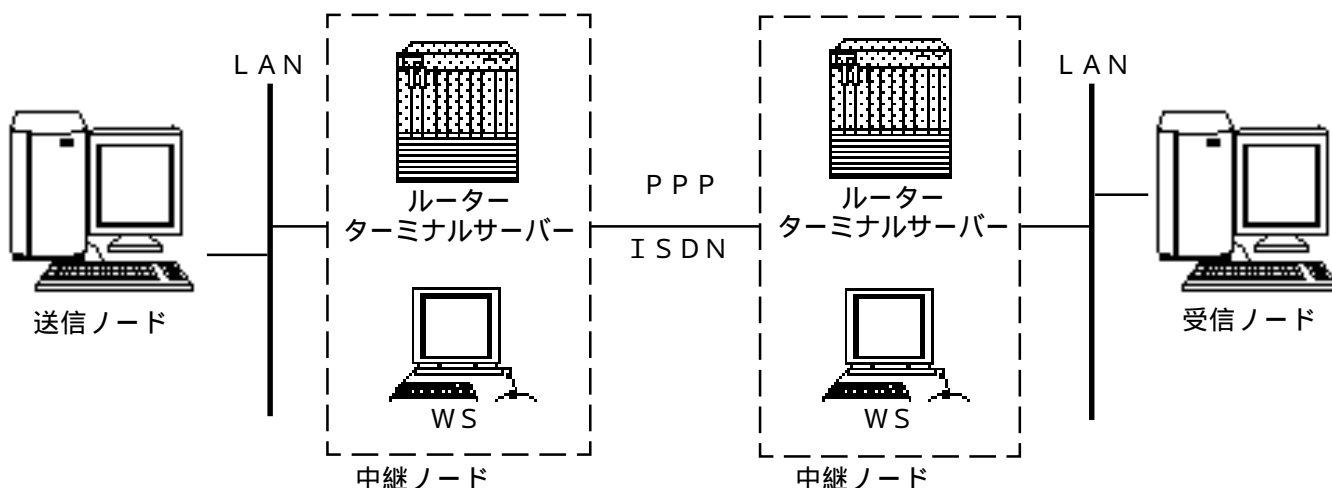


図 3 . 6 拡張構成 3

(3) 中継ノードの種類

(a) ルーター

最低限の機能として、LAN用インターフェース、WAN用インターフェース、TCP/IP、PPPをサポートしている必要があり、TAを必要とするものとISDNインターフェースを装備しているものがある。

なお、ISDNインターフェースを装備しているものには、Bチャンネルを2つ使用して128 Kbpsで接続できるものもある。

(b) ターミナルサーバー

ターミナルサーバーは非同期端末をLANに接続するための機器であるが、非同期回線用ルーターとしても使用することができる。ISDN網を使用する場合は、V.110非同期モードをサポートしているTAが、1ポートにつき1台必要となり最大回線速度は38.4 Kbpsとなる。

(c) ワークステーション

ルーターの代わりにUNIXワークステーションを中継ノードとして使用することができる。

(4) トポロジー

基本的に、専用線ではないので明確なトポロジーはないが、運用面から次の2つが考えられる。

(a) メッシュ型 (任意の接続先に接続を許可)

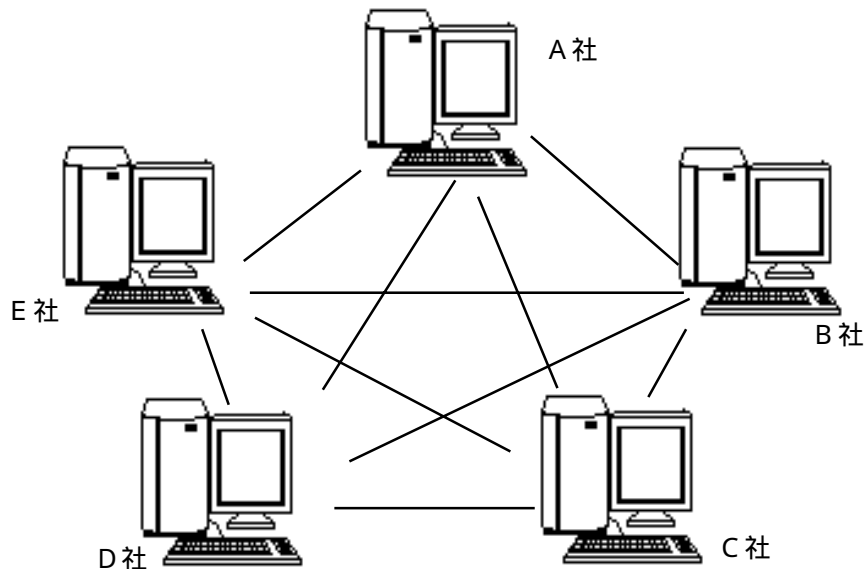


図3.7 メッシュ型

任意の拠点と接続するタイプであり、IPアドレスの運用について各拠点間で同一アドレスを使用しないように明確な運用方法を決めておく必要がある。

(b) スター型 (接続先は特定の1拠点)

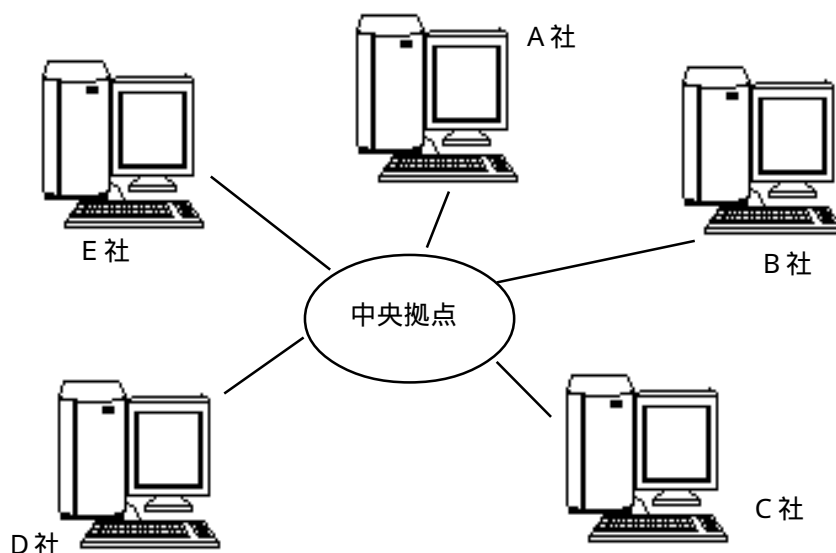


図3.8 スター型

IPアドレスを中央拠点にて一元管理する事ができ、各拠点は使用するアドレスを接続するときにダイナミックに割り当てることが可能である。

3.1.3. 適用ルーター技術

(1) ルーター概説と最新事情

一般にルーターとはネットワーク同士を接続し、異なるネットワーク上に接続されるホスト間の通信を、OSI参照モデルにおけるネットワーク層のアドレスに基づいて中継する機器を言う。したがってルーターは少なくとも2つ以上の物理インターフェースを装備しているが、その種類は接続されるネットワークにより様々である。

ルーターの典型的な利用形態としては、イーサネットのようなLAN同士を1台のルーターによって接続する場合や、回線によって接続されたLAN同士を2台のルーターによって接続する場合がある。前者で用いられるルーターをローカル・ルーター、後者で用いられるルーターをリモート・ルーターと呼ぶことがある。ルーターをハードウェアの面から見ると、専用ルーターとワークステーション上にルーティング機能を搭載したものとに分類することができる。後者を選択した場合には、ルーターとしての機能以外にそれ自身をエンド・ノードとしても利用することが可能であるが、ルーティング性能や管理機能においては専用ルーターが優っている。

デジタル公衆網によってLAN間接続を行う場合、ターミナルアダプターを介してルーターを網に接続する形態と、ルーターを網に直接接続する形態が考えられる。ルーターとターミナルアダプターとの接続には、V.35やX.21のインターフェースが主に用いられている。近年になりターミナルアダプターを内蔵したISDN対応ルーターが各社から提供されており、ルーターを網に直接接続する形態が今後の主流になりそうである。

(2) NSK T I F Fの転送に必要とされるルーターの機能

(a) インターフェース

ルーターの回線側のインターフェースは、I.430に対応したISDNインターフェースまたは、ターミナルアダプターと接続するためのX.21/V.35/RS-449等のインターフェースが必要となる。

(b) データリンク層のサポート

回線側のデータリンク層プロトコルとしてPPPをサポートする。認証機能としてPPPで規定されているCHAPをサポートすることがセキュリティ上は望ましい。

(c) I P ルーティング機能

受信した I P パケットをルーティング・テーブルを参照することにより、経路を選択し転送する。パケットを中継する際に I P ヘッダー中の必要な箇所を書き換える。ルーティング・テーブルの維持 / 更新のしくみとしては、静的な方法 (スタティック・ルーティング) および動的な方法 (ダイナミック・ルーティング) とがある。ただし I S D N 回線を利用する場合、ダイナミック・ルーティングでは回線を接続し続けなければならない、回線料金の面から現実的ではない。回線側をスタティック・ルーティング、L A N 側をダイナミック・ルーティングとし、スタティック・ルーティングで設定したルーティング情報をルーティング・プロトコルで L A N 側に知らせるしくみが必要である。

以降に N S K T I F F 転送で必須ではないが、I S D N 対応ルーターとして便利な機能を掲げておく。

(d) ダイヤルオンデマンド機能

ルーターが I P パケットを回線側に転送する時に、自動的に発呼する機能である。ターミナルアダプターと接続する場合には、V . 2 5 b i s 規格を用いることが多い。ダイヤルオンデマンド機能を用いる場合には、タイマー監視によるアイドル時の自動切断機能が必要であり、またそのためには不要なパケットを回線上に流さないためのフィルタリング機能や切断タイマーの対象となるパケットを識別する機能が不可欠となる。

(e) バルク伝送機能

同時に 2 つの B チャンネルを使用してほぼ 128Kbps の速度で通信する機能である。

(f) 発信者番号確認機能

あらかじめいくつかの発信者番号を登録しておき、それ以外からの着呼を拒否する機能。セキュリティー上有効な手段である。

(g) I S D N サブアドレス対応

ルーター側でサブアドレスを認識させることにより、1 本の回線に複数のルーターを接続することを可能にする。

一般的な I P ルーターでは、この他にコントロール・メッセージ、管理プロトコルの送受信、一部のアプリケーション層の中継など、数多くの機能が備わっている。I P ルーターの機能要件については R F C 1 7 1 6 に記されている。

(3) ルーティング・プロトコル

T C P / I Pのルーティング・プロトコルとしては様々なものが用いられており、現在最も利用されているのはR I P（注18）であるが、近年ではO S P F（注19）が脚光を浴びている。また、R I Pを拡張したR I P Version 2も検討されている。

ルーティング・プロトコルに求められる要件は、ネットワーク・トポロジーの変化に素早く応答できること、ルーティング・プロトコルによる回線上の負荷が小さいこと、複数の同一コストの経路に対して負荷を分散する機能が備わっていることなどである。

それぞれのルーティング・プロトコルには一長一短があり、現時点ではどれが最良とは言い難いが、ネットワーク規模や回線速度、ルーター間の相互接続性などを考慮して選択する必要がある。

(4) セキュリティー

I Pルーターの多くはパケットフィルタリングの機能を有しており、特定のパケットのみを転送・廃棄する処理が可能である。特に異なる組織間のL A Nを公衆回線で接続する場合は、この機能が重要となってくる。N S K T I F Fの転送時には、I Pのソース/デスティネーションアドレスやT C P / U D Pポート番号によるフィルタリングを行うことが望ましい。

また、このふたつを併用することも有効な手段である。

注18) Routing Information Protocolの略。ディスタンスベクター型のルーティングプロトコルに属する。ホップ数（ルーターを通過する数）によって経路選択を行うが、ホップ数が15を越えることができない、という制限がある。

注19) Open Shortest Path Firstの略。リンクステート型のルーティングプロトコルに属する。サブネットマスクやT O S (Type Of Service)をサポートしている。

3.2. PPP

3.2.1. PPPの概要

(1) 成立の経過と特徴

回線を利用してコンピューター通信を実現するには、回線に接続するためのインターフェース装置と回線上でデータ伝送するためのプロトコルが必要になる。インターネットワーキング用に業界標準としてはじめて登場したプロトコルはSLIP (Serial Line IP) である。IPパケットを1200～19200 bpsの専用線または加入電話回線で転送することを目的としている。高速回線向きにはHDLC (High-level Data Link Control) が用いられてきた。

これはIPパケットをHDLCのデータ部 (Iフレーム) に乗せて (カプセル化という) 転送する。一般的にはリンクの確立、フロー制御、再送制御は行わない。フレームのビット化けをチェックして、フレームが破損していれば破棄するだけである。しかしHDLCのフレームフォーマットは機器のメーカーが独自に決めたため、異なるベンダー間での相互接続が不可能であった。この問題を解決するために、PPPプロトコルとして標準化が図られた。

PPPプロトコルは1989年にRFC 1134として提案されたのが始まりで、現在までいくつかの改良が加えられ、最新はRFC 1661となっている。

PPPプロトコルの特徴は以下の4点に要約できる。

- (a) 複数のネットワーク層プロトコルのパケットを伝送できる。これはフレーム内にプロトコル種別を示すフィールドをもっているためである。
- (b) エラー検出：フレーム内にFCS (Frame Check Sequence) フィールドを持つ。
- (c) アドレッシング：IPアドレス情報を交換するメカニズムをオプションで用意している。
- (d) TCPとIPのヘッダー圧縮：Van Jacobsonの圧縮技術の利用をネゴシエートでき (オプション)、圧縮したパケットであることをプロトコルフィールドで示すことができる。

この他、PPPは接続相手を認証する機能をオプションで用意する。この機能は、加入電話網やISDN公衆網を利用するときに効果を発揮する。

(2) 動作概要

PPPでは、リンク確立から切断までを図3.9に示すフェーズに分けて動作する。

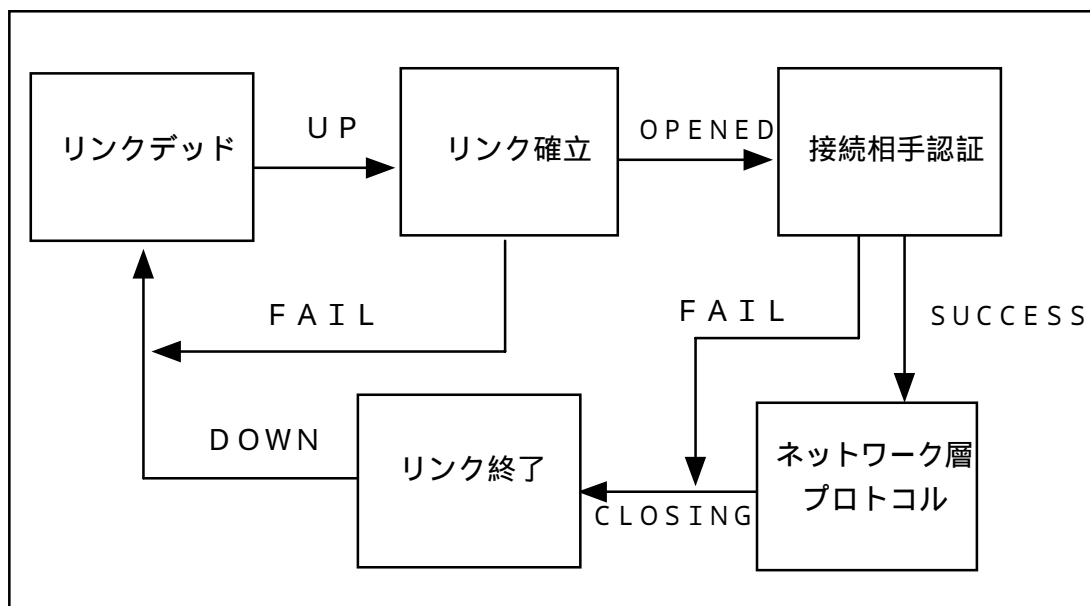


図3.9 PPPのフェーズダイアグラム

- (a) 最初は、PPPはリンクデッドという状態におかれている。物理的な通信路が利用可能になると、次のリンク確立フェーズに移る。
- (b) リンク確立フェーズでは、使用するネットワーク層のプロトコルに依存しない接続のための情報を互いに交換することにより、2点間のリンクを確立する作業を行う。実際の作業にはLCP (Link Control Protocol) を用いる。
- (c) リンクを確立すると、認証フェーズに入る。リンク確立時に交換した情報に基づいて、必要に応じて互いに相手を認証する作業を行う。PAPまたはCHAPプロトコルが利用される。
- (d) 認証が完了すると、ネットワーク層のプロトコルであるIPパケットを転送するフェーズに入る。このフェーズではまず利用するネットワーク層のプロトコルごとにNCP (Network Control Protocol) を使って必要な情報を交換する。

TCP/IPではIPに対応するNCPはIPCP (IP Control Protocol) である。IPCPでの接続が完了すると、IPパケットが運べるようになる。
- (e) リンク切断フェーズはPPPリンクを切断する。実際にはLCPがリンクを切断するための情報を交換することにより切断する。

(3) PPPのフレームフォーマット

PPPで使用するフレームフォーマットを図3.10に示す。

各フィールドは左のものから順に送出される。

(数字はオクテット数を示す)

1	1	1	2	0 ~ 1500	2	1
フラグ 7EH	アドレス FFH	制御 03H	プロトコル (表3.1)	情報フィールド	FCS	フラグ 7EH

図3.10 データリンク層のフレームフォーマット

(a) フラグフィールド:

1オクテット。常に01111110("7EH"と示す)である。フレームの始めと終わりを示す。フレーム間には最低1つのフラグが必要である。

(b) アドレスフィールド:

1オクテット。PPPで使用するアドレスは、常に全ステーションを示す11111111("FFH")である。

(c) 制御フィールド:

1オクテット。常に00000011("03H")である。すなわち、HDLCのポール/ファイナルビット(P/Fビット)を0に設定したUI(Unnumbered Information: 非番号情報)フレームであることを意味する。

(d) プロトコルフィールド:

2オクテット。カプセル化する情報のプロトコル種別を示す。"0XXXH ~ 3XXXH"の範囲はネットワーク層プロトコルのパケット伝送、"8XXXH ~ BXXXH"の範囲はNCPの伝送、"CXXXH ~ FXXXH"の範囲はLCPの伝送を意味する。

IPプロトコルで使用するプロトコルフィールドの値を表3.1に示す。

値	プロトコル名
0021H	IP (Internet Protocol)
8021H	IPCP (Internet Protocol Control Protocol)
C021H	LCP (Link Control Protocol)
C023H	PAP (Password Authentication Protocol)
C223H	CHAP (Challenge Handshake Authentication Protocol)

表3.1 プロトコルフィールドの規定

(e) 情報フィールド:

0オクテット以上。プロトコルフィールドで定義したプロトコルのパケットをのせるフィールド。デフォルトの最大値は1500オクテットである。

(f) FCSフィールド:

2オクテット。アドレス、制御、プロトコル、情報の各フィールドを対象にCRC演算した結果を入れる。

3.2.2. LCP

(1) リンク確立のためのLCPの動作

LCPはリンクを確立するための各種のパケットを交換し、オプションの指定などについて双方で確認作業を行う。この手続きの中には接続相手認証機能を使うかどうか、使うとしたらどの方式を使うかも含まれる。

これらの動作はイベント、アクション、ステートの3つで定義する。コマンドの受信やリスタートタイマーなどのイベントに従って、あるステートからあるステートに遷移する。そのときコマンドの発信など指定されたアクションを実行する。

状態は最初クローズドであるが、前述のようにこの状態遷移について、詳細は煩雑になるのでここでは触れない。厳密な定義についてはRFC 1661の中の状態遷移テーブルを参照すべきである。

(2) LCPのフォーマット

LCPパケットは、データリンク層フレームフォーマットの情報フィールドに図3.11に示す情報要素を格納したものである。

このときデータリンク層フレームフォーマット内のプロトコルフィールドは、"C021H" にセットする。

(数字はオクテット数を示す)

1	1	2	0 ~
コード (表3.2)	識別子	長さ	データフィールド

図3.11 LCPパケットのフォーマット

L C P パケットとして追加された情報要素は以下のフィールドからなる。

(a) コードフィールド :

1 オクテット。L C P パケットの種類を示す。L C P パケットを表 3 . 2 に示す。

1 ~ 4 はリンクを確立するためのパケット、5 と 6 はリンクを終了するためのパケット、7 ~ 1 1 はリンクを管理、デバッグするための保守パケットである。

コード	パケット
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack
7	Code-Reject
8	Protocol-Reject
9	Echo-Request
10	Echo-Reply
11	Discard-Request
12	予約済み

表 3 . 2 L C P パケットの種類

(b) 識別子フィールド :

1 オクテット。ポイント・ツー・ポイント接続するエンドノードが要求パケットを送出するとき、識別子フィールドに数値を入れる。
その要求パケットに対するレスポンスをこの数値で確認する。

(c) 長さフィールド :

2 オクテット。コード、識別子、長さ、データの全フィールド長を表す。

(d) データフィールド :

0 オクテット以上。データフィールドのフォーマットはコードによって定義される。特に L C P 設定オプションは、このフィールドに含まれる。

(3) LCP設定オプション

LCP設定オプションは、エンド・ノード間で標準のリンク設定を変更するネゴシエーションを行うために用いる。ネゴシエーションの結果で変更できる項目は、受信可能な最大データユニット長、非同期通信制御文字マッピング、接続相手認証機能などである。

これらのオプションは、一方のノードがLCPの Configure-Request パケット(コード1)の中で指定し、受け取ったノードが Configure-Ack パケット(コード2)を返送することで有効となる。

LCP設定オプションのフォーマットを図3.12に示す。

(数字はオクテット数を示す)

1	1	2	1	2	0 ~
コード	識別子	長さ	タイプ (表3.3)	オプション長	データフィールド

図3.12 LCP設定オプションのパケットフォーマット

(a) タイプフィールド:

1オクテット。LCPの設定オプションを指定する。
現在割り当てられている番号を表3.3に示す。

タイプ	設定オプション
1	Maximum-Receive-Unit
2	Async-Control-Character-Map
3	Authentication-Protocol
4	Quality-Protocol
5	Magic-Number
6	予約済み
7	Protocol-Field-Compression
8	Address-and-Control-Field-Compression

表3.3 LCP設定オプション

例えば、接続相手認証機能のタイプは3である。

(b) オプション長フィールド:

2オクテット。タイプ、長さ、データの各フィールドを含んだ設定オプションの長さを示す。

(c) データフィールド:

設定オプションのデータフィールドの内容は、そのタイプによって決まる。

(4) 接続相手認証機能のPAPとCHAP

接続相手認証機能には、PAPとCHAPがあり、ここでは概略を説明する。PAPよりCHAPのほうがセキュリティーの機能が高い。詳細はRFC1334を参照されたい。

LCPのConfigure-Request パケットでどちらかを指定する。

PAPでは、LCPのConfigure-Request 送信に対して、Configure-Ack を受信すると、認証フェーズに入る。IDとパスワードを送信してACKを受信すると確認が完了するいわゆる2ウェイハンドシェイクである。IDもパスワードもテキストで伝送されるのでセキュリティー機能としては高くない。

CHAPは3ウェイハンドシェイクを用い、PAPに比較してかなり複雑な手続きをとる。リンクが確立して認証フェーズになると、チャレンジメッセージ、すなわち返答要求メッセージを接続相手に送信する。接続相手はハッシュ・アルゴリズム(MD5)で計算した数値を送り返す。送信元では自分でもハッシュ値を計算しておき、返ってきた数値が一致すればACKを接続相手に送って認証作業が終了する。CHAPは直接パスワードをテキストで交換しないので、セキュリティー機能として優れている。

3.2.3. NCP

LCPによってリンクが確立し、オプションのネゴシエーションが完了すると、PPPはNCPを使ってネットワーク層プロトコルのネゴシエートを行う。これによって通信可能となったネットワーク層プロトコルは、そのパケットをリンク上へ転送できるようになる。

NCPは各ネットワーク層プロトコルごとに用意されている。IPに対応するNCPはIPCP(IP Control Protocol)とよばれ、詳細はRFC1332に規定されている。

(1) IPCP

IPCPの役割は、接続を行う双方が互いに使用するIPアドレスと、TCPのヘッダー圧縮を行うかどうかネゴシエートすることにある。IPCPのパケットフォーマットを図3.13に示す。

(数字はオクテット数を示す)

1	1	1	2	1	1	2	0~	2	1
フラグ 7EH	アドレス FFH	制御 03H	プロトコル 8021H	コード (表3.4)	識別子	長さ	データ	FCS	フラグ

図3.13 IPCPのフォーマット

L C P パケットと同じフォーマットであるが、L C P とは以下の点が異なる。

(a) プロトコルフィールド :

データリンク層フレーム内のプロトコルフィールドは I P C P を示す "8021H" がセットされる。

(b) コードフィールド :

パケット内のコードフィールドには I P C P パケットの種類を示す値 (表 3 . 4) が入る。

コード	パケット
1	Configure-Request
2	Configure-Ack
3	Configure-Nak
4	Configure-Reject
5	Terminate-Request
6	Terminate-Ack
7	Code-Reject

表 3 . 4 I P C P パケットの種類

I P C P も L C P と同様のフォーマットで、データフィールドを使った設定オプションがある。設定オプションとしては、

コード 1 : IP Addresses

コード 2 : IP Compression-Protocol

コード 3 : IP Address

の 3 種類がある。

(2) 動作の概要

手順としては、互いに自分の使用したい I P アドレスを Configure-Request パケットで相手に通知する。受信した側は、受け取った I P アドレスを認めるときは Configure-Ack を返送するが、認められないときは Configure-Nak と共に使用するべき I P アドレスを返送する。こうして互いに相手からの Configure-Ack を受け取るとネゴシエートは完了する。ヘッダー圧縮についても同様に、ヘッダー圧縮されたパケットを受信できることを Configure-Request によって相手に通知する。

この様にして、ネゴシエートが完了し、I P C P が Open 状態に遷移すると、I P パケットの転送を開始する。I P パケットは図 3 . 1 4 に示すフォーマットで、データリンク層フレームの情報フィールドにカプセル化されて転送される。このときプロトコルフィールドに I P パケットを示す "0021H" をセットして転送する。

(数字はオクテット数を示す)

1	1	1	2	0 ~ 1 5 0 0	2	1
フラグ 7 E H	アドレス F F H	制御 0 3 H	プロトコル 0 0 2 1 H	I P パケット	F C S	フラグ 7 E H

図 3 . 1 4 I P パケットの転送時のフォーマット

3.3. TCP/IP

3.3.1. TCP/IPの概要

TCP/IPは、米国の代表的な研究開発用ネットワークであり、長距離ネットワークの草分けといわれるARPANET用に開発されたネットワークアーキテクチャーである。

ARPANETは、米国国防総省(DOD: Department of Defense)の一機関であるDARPA(Defense Advanced Research Project Agency)の支援のもとに発展した。現在では多くの大学、政府機関、軍関係施設、企業をつなぎ、「DARPA Internet」または単に「The Internet」と呼ばれる。このネットワークは、TCP/IPプロトコルを使い、ひとつの協調的な仮想ネットワークとして機能する。

TCP/IPは、BSD系のUNIXがプロトコルとして採用したことから、UNIXにおいては実質上の標準プロトコルとなっている。また、インターネットプロトコルとしての実績の高さから、UNIX以外でも普及が進んでいる。

TCPとIPはそれぞれプロトコルの名称であるが、TCP/IPという時には、ネットワークアーキテクチャーを構成するプロトコル群全体を指している。TCPはRFC 793、IPはRFC 791で規定されている。

図3.15に代表的なTCP/IPの関連プロトコル構成図を示す。

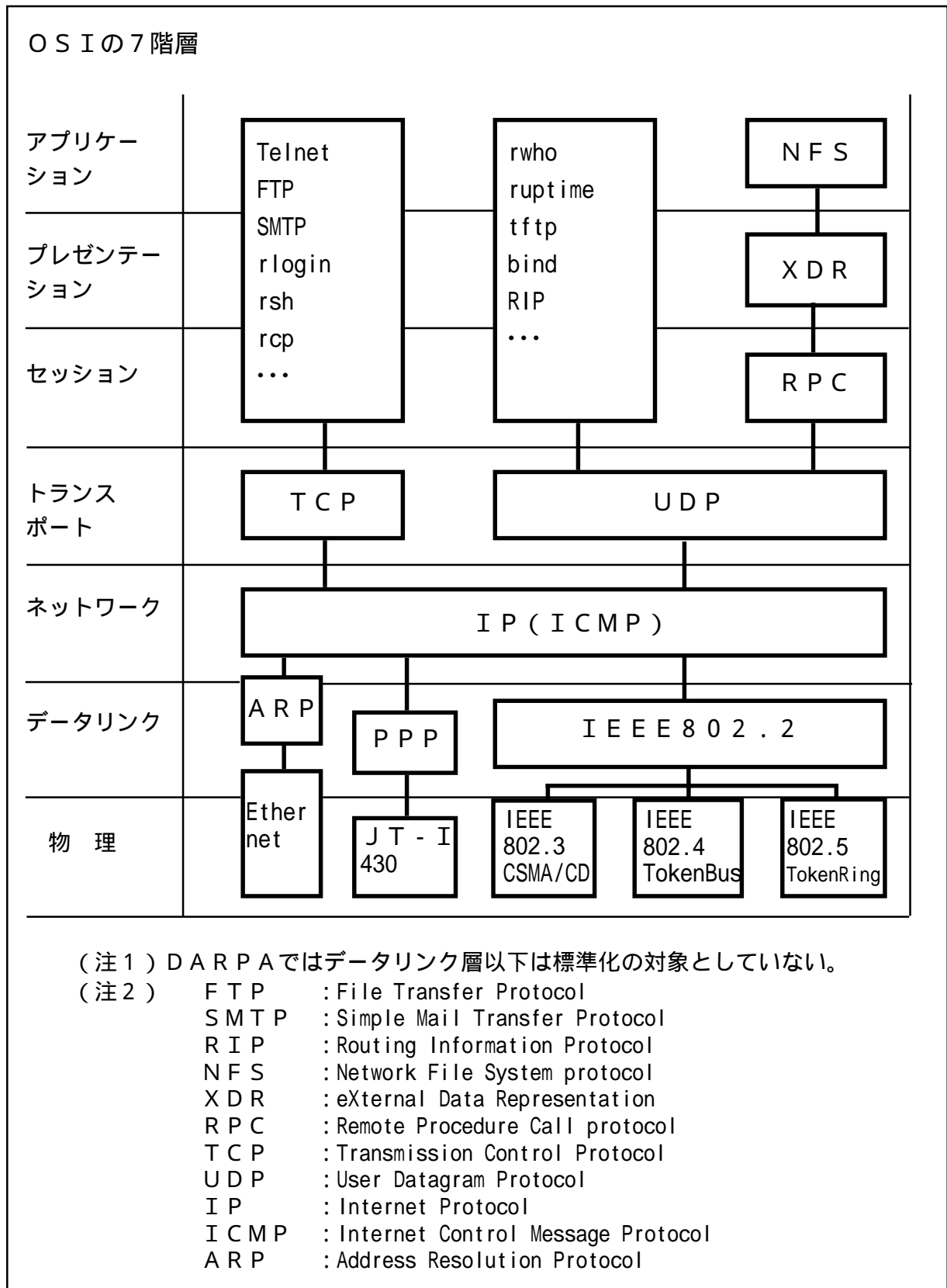
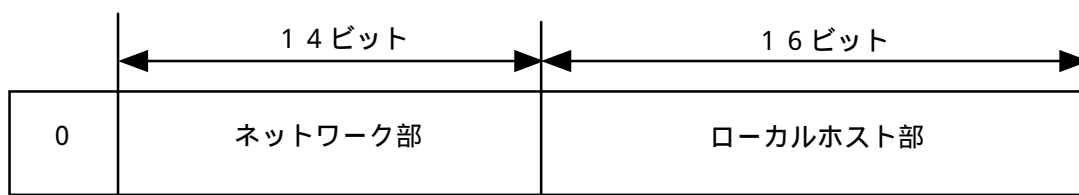
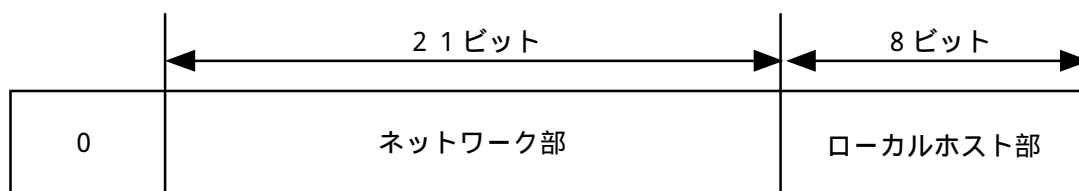


図3.15 代表的なTCP/IP関連プロトコル構成図

- ・クラス B (128.0.X.X ~ 191.255.X.X) ネットワーク数 : 16,384
ローカルホスト数 : 65,534



- ・クラス C (192.0.0.X ~ 223.255.255.X) ネットワーク数 : 2,097,150
ローカルホスト数 : 254



アドレスは、C C I R N (Cordinating Comittee for Intercontinental Research Networking : インターネットワーキングの研究、開発の国際協力の調整を助ける国際団体) が決めた統一手続きにより地域ごとに分散管理する。米国では、G S I (Government System Inc) / N I C (Network Information Center)、日本では J P N I C が割り当てを管理する。

(3) I P パケットフォーマット

I P 転送の単位であるパケットの形式を図 3 . 1 6 に示す。

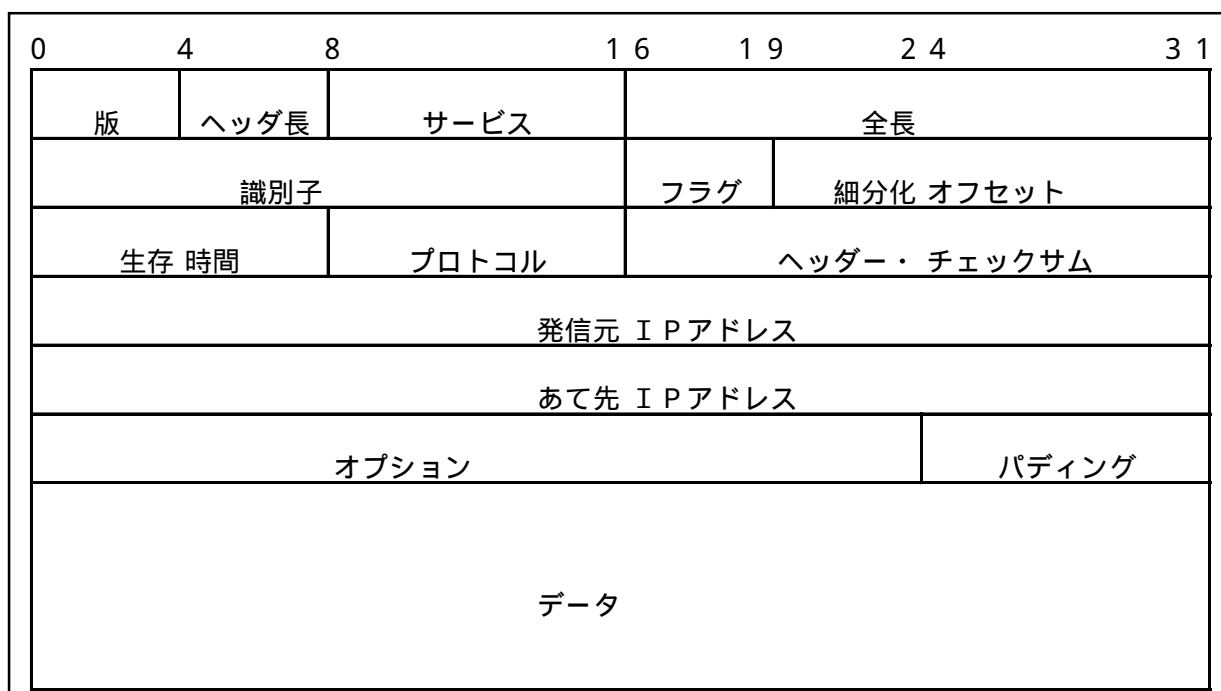


図 3 . 1 6 I P パケットフォーマット

- (a) 版 (4 ビット)
I P ヘッダーのバージョン (現在は 4)
- (b) ヘッダー長 (4 ビット)
3 2 ビットを 1 単位とした、I P ヘッダーの長さ。
- (c) サービス (8 ビット)
要求されたサービスの品質。通常遅延 / 低遅延フラグ、通常転送 / 高速転送フラグ、通常信頼性 / 高信頼性フラグなど。
- (d) 全長 (16 ビット)
ヘッダー + データのバイト数。
1 6 ビット長なので許せる最大長は 65535 バイト。すべてのホストは最小でも 576 バイトのパケットを受け取れなければならない。
- (e) 識別子 (16 ビット)
細分化されたデータグラムの再組み立てのために発信元で付けるシーケンス番号。
- (f) フラグ (3 ビット)
細分化 (フラグメンテーション) の制御フィールド。
ビット 0 : 将来のため未定義。必ず 0。
ビット 1 : D F (Don't Fragment) フラグ。細分化許可 = 0 / 禁止 = 1。
ビット 2 : M F (More Fragment) フラグ。最後のフラグメント = 0 / 続きのフラグメント有り = 1。
- (g) 細分化オフセット (13 ビット)
分割されたフラグメントが元のデータグラムのどこに位置していたかを 8 バイト単位のオフセットで示す。
- (h) 生存時間 (8 ビット)
その I P パケットがネットワーク上に存在できる時間。 (TTL : Time To Live) (秒単位) 送信側で、受信ホストに達するまでの時間を予測して設定する。
途中のゲートウェイは、処理に費やした時間分 (1 秒以下のときにも必ず 1) T T L の値を減らして送り出す。T T L が 0 のパケットを検出した I P モジュールはそれを破棄する。これは、永遠に配達されずにネットワーク上を浮遊するパケットが存在しないようにするための処置である。T T L の最大値は 2 5 5 秒。
- (i) プロトコル (8 ビット)
このデータグラムを使用する上位のプロトコル (TCP=6 , UDP=17)
- (j) ヘッダー・チェックサム (16 ビット)
I P ヘッダー部分のみのチェックサム。高速性を重視してデータ部分のチェックサムは行わない。計算は、ヘッダーを 1 6 ビットワードの並びとみなし、先頭のワードから加算して途中でキャリーが立ったら (桁あふれ) 1 を加える。その加算結果の 1 の補数をチェックサムとする。
ヘッダー部しかチェックしないことや簡易な計算方法を採用しているのは、ゲートウエーでの処理の軽減をねらいとしたものである。
- (k) 発信元 I P アドレス、宛先 I P アドレス (各 32 ビット)

(1) オプション

セキュリティー、経路記録など。

(m) パディング

ヘッダー長を4バイトの整数倍とするために0を付加する。

(4) 細分化と再組み立て

IPの主要な機能にデータグラムの細分化とその再組み立てがある。上位から渡されたデータグラムを下位のデータリンク層の制限によって細分化する。パケット交換網が相互に接続された環境では、それぞれのローカル網で許される最大パケットサイズ (MTU : Maximum Transmission Unit) がまちまちであるが、これに合わせるわけである。

3 . 3 . 3 . TCP

TCPとUDPは、OSIのトランスポート層に位置するプロトコルであるが、異なった特徴を持つ。信頼性を求めるアプリケーションはTCPのサービスを、高速性を求めるアプリケーションはUDPのサービスを受ける。

ユーザーに対し、TCP/IPネットワークを介したファイル転送や電子メールのやりとりのサービスを提供しているのは、様々なアプリケーションプログラムである。アプリケーションプログラムは、下位のTCPやUDPにトランスポートサービスを要求し、そのサービスを受けてリモートホスト上の対応するアプリケーションと通信する。ソケットインターフェースはBSD系UNIXで実装されたプロセス間通信用インターフェースである。TELNETやrwhoなど多くのアプリケーションが、ソケットを用いてTCP/IPのサービスを利用している。

(1) 機能と特徴

(a) TCP

[機能] プロセス間のバイトデータ (ストリーム) の通信
ポート番号による通信端点の多重化
再送処理
重複データの排除と順序制御
フローコントロール (ウィンドウ制御)

[特徴] コネクション型のバイトストリーム通信
再送処理、順序制御などによる信頼性の高い通信が可能

(b) U D P

- [機能] プロセス間のデータグラム通信
ポート番号による通信端点の多重化
- [特徴] コネクションレス型のデータグラム通信
信頼性は低いが高速な通信が可能
(データの信頼性の保証はアプリケーションレベルで行う)

(2) ヘッダー

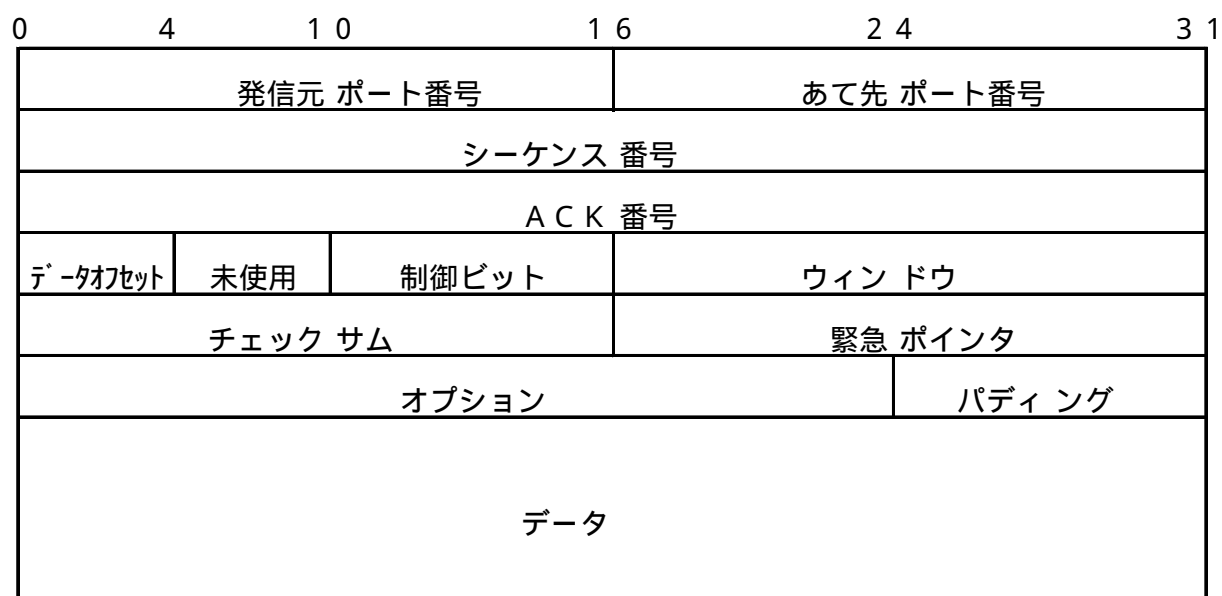


図 3 . 1 7 T C Pヘッダー

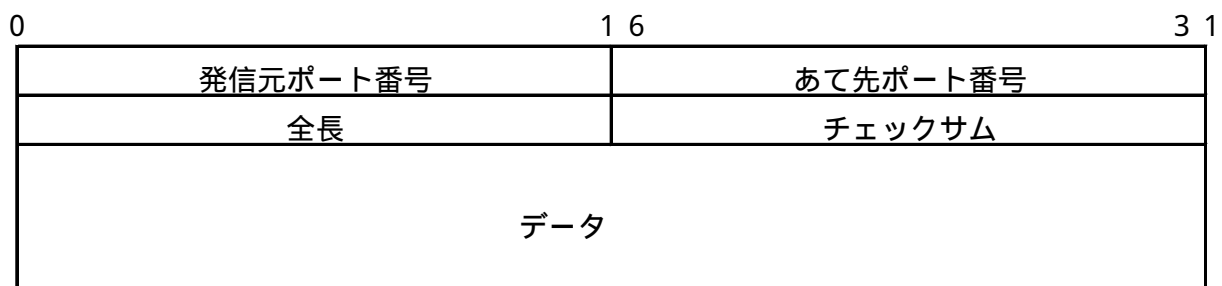


図 3 . 1 8 U D Pヘッダー

(a) 発信元、宛先ポート番号 (各 16 ビット)

発信元と宛先の T C P (または U D P) モジュール間の通信端点をポートという。アプリケーションは通信相手を、 I P アドレスとポート番号を組み合わせで指定する。

(b) シーケンス番号 (32 ビット)

上位プロトコルから渡されたバイトストリームの各バイトに与えられたシーケンス番号。今回の送信データが、そのバイトストリームの何バイト目からなのかを示す。

(c) A C K 番号 (32 ビット)

次に受信することを期待しているデータのシーケンス番号。

(d) データオフセット

T C P ヘッダーの長さ (4 バイト単位)。データの開始位置を示す。

(e) 制御ビット (6 ビット)

F I N (0x01) : 送信終了

P S H (0x08) : P U S H 要求

S Y N (0x02) : 接続要求

A C K (0x10) : A C K 番号セットフラグ

R S T (0x04) : 接続リセット

U R G (0x20) : 緊急ポインター有

(f) ウィンドウ (16 ビット)

受信側が次に受け取ることができるバイト数。

(g) チェックサム (16 ビット)

ヘッダー部、データ部、仮想ヘッダーを併せたチェックサム。

仮想ヘッダーは発信元と宛先の I P アドレスを含む 9 6 ビット長で、T C P や U D P は、下位の I P の持つ情報をのぞきこむことで値を作成する。仮想ヘッダーを含むことにより、受信誤りを検出するとともに、本当に自分宛なのかの確認がなされる。

計算方法は I P と同じ。

(h) 緊急ポインター

緊急データの末尾を指す。U R G ビットオンのときのみ有効。

(i) パディング

ヘッダー長を 4 バイトの整数倍とするために 0 を付加する。

(3) コネクションの確立と切断

T C P はコネクション型通信である。T C P ヘッダーの制御ビットの立ったセグメントをやりとりすることにより、コネクションの確立、切断を制御する。

(4) ウィンドウ

T C P ではウィンドウを用いたフローコントロールを行う。

3.4. FTPと関連アプリケーション

3.4.1. FTP

(1) FTPの概要

FTP (File Transfer Protocol : ファイル転送プロトコル) はファイルの共有を促進し、リモートコンピューターの間接的使用を助ける。また、ユーザーをホスト間のファイル記憶システムの相違から開放し、データを高信頼度でかつ効率良く転送するために考案された、ネットワークプロトコルである。開発当初ARPANETで使用されていたが、現在はTCP/IP上はもちろん、事実上のコンピューター間のファイル転送標準プロトコルとして、広く使われている。

FTPは、信頼性のある通信サービスを必要とするため、TCPのトランスポートサービスを使用している(注20)。

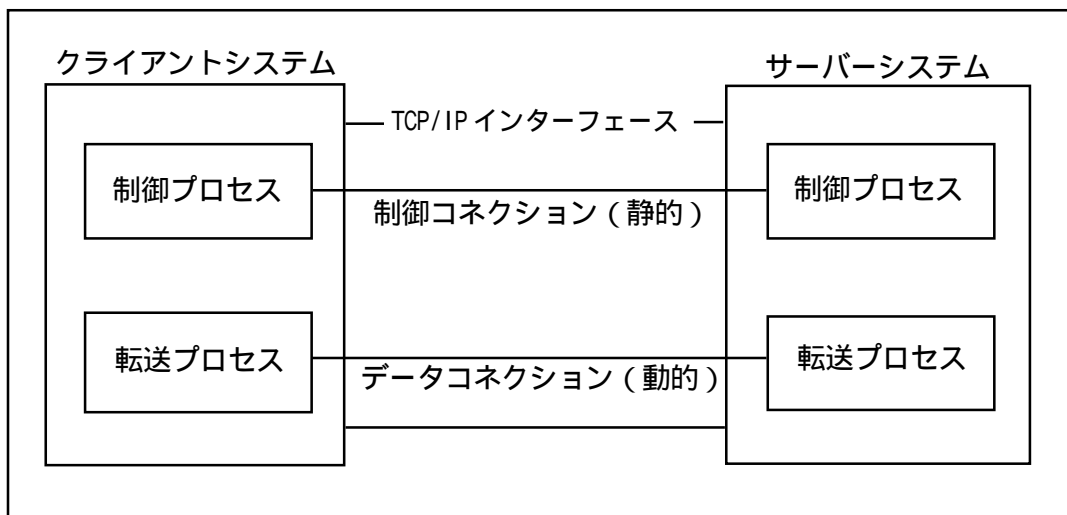


図3.19 FTPのコネクション

制御コネクションはセッションを通じて持続しているが、データコネクションは動的に生成される。制御コネクションが消滅するとセッションは終了し、データ転送プロセスは終了する。

注20) TCP/IPアプリケーションサービスでは、コネクションの発信者・サービスの依頼者をクライアント、コネクションの受信者・サービスの提供者をサーバーと定義している。

F T Pは、異なった仕様を持つコンピューター間のファイル転送を行うため、クライアントとサーバーの認証、ファイルの所有権、アクセス保護、データフォーマットに関する合意を容易に解決している。そのためファイル転送機能だけではなく以下の機能も提供する。

(a) インタラクティブ (会話的) アクセス :

F T Pはプログラムによって使われるよう設計されているが、大部分の実装では人間が簡単にリモートのサーバーと相互作用できるようにするインタラクティブなインターフェースを提供している。

(b) フォーマット (表現形式) 仕様 :

F T Pはクライアントが蓄積されたデータの型やフォーマットを規定できるようにしている。

(c) 認証制御 :

F T Pはクライアントがファイル転送を要求する前にログイン名とパスワードを送り、自分自身を認証するように要求している。サーバーは正当なログイン名とパスワードを設定できないクライアントのアクセスを拒否する。

(2) プロトコル概要

F T PプロトコルはT C Pのトランスポートサービスを利用し、クライアントとサーバー間でやりとりを行う。標準F T Pコマンドは、T C Pセグメントのデータフィールドに格納され、送信される。代表的なコマンドを次ページに示す。

コマンド	オペランド	パラメーター	説明
USER	USER(username) <crif>	username ユーザーID	ログインユーザーのIDを送る
PASS	PASS(password) <crif>	password パスワード	ユーザーのパスワードを送る
ACCT	ACCT <crif>	なし	アカウント情報を送る
QUIT	QUIT <crif>	なし	現在実行中のデータ転送終了後、 コネクションを開放する
PORT	PORT(Host-port) <crif>	Host-port ホスト番号 ポート番号	サーバーに対して、データコネクション 確立のために“listen”を出している データポートを伝える
TYPE	TYPE(type code) <crif>	type code データ型	データ表現タイプを伝える (ASCII、EBCDICなど)
CMD	CMD(pathname) <crif>	pathname ディレクトリパス名	ワーキングディレクトリを変更する
RETR	RETR(pathname) <crif>	pathname ファイルのパス名	ファイル受信
STOR	STOR(pathname) <crif>	pathname ファイルのパス名	ファイル送信
DELE	DELE(pathname) <crif>	pathname ファイルのパス名	ファイル削除
RMD	RMD(pathname) <crif>	pathname ディレクトリパス名	ディレクトリの削除
MKD	MKD(pathname) <crif>	pathname ディレクトリパス名	ディレクトリの作成
LIST	LIST [(pathname)] <crif>	pathname ディレクトリパス名	引数がディレクトリの時は、直下の ファイルの時はファイル情報を通知 するように依頼する
NLST	NLST [(pathname)] <crif>	pathname ファイルのパス名	ファイル名リストを通知するように 依頼する
STAT	STAT [(pathname)] <crif>	pathname ファイルのパス名	状態通知要求
HELP	HELP [(pathname)] <crif>	string コマンド	ヘルプ情報要求

表 3 . 5 F T P プロトコルの代表的コマンド

以上のコマンドはF T Pのクライアントソフトウェアとサーバーソフトウェア
が相互に通信する場合のみ使用され、直接ユーザーが使用することはない。しか

しネットワークアナライザーを使用、またはFTP動作がトレースモードやデバッグモードであれば、送信されたままのテキストとして実際に確認することが可能である。FTPサーバーはこれらのコマンドに対する独自の応答方法を持っている。

以下に応答コマンドを示す。なお、サーバー応答の数字列と文字列は常に対で用いられる。

サーバー応答	説明
220 Server ready	サービス準備完了
331 User name OK. need password	ユーザー名了解。パスワードが必要
230 User Logged in. proceed	ユーザーはログイン完了。続行可能
150 File status OK. about to open data connection	データコネクションをオープンするためのファイルの状態了解
226 Closing data connection	データコネクションをクローズ
200 Command OK.	コマンド了解
550 Access denied	アクセスが拒否された

表3.6 FTPプロトコル上の代表的なサーバー応答コマンド

以下は代表的なFTPトランザクションの流れである。

```
leia($HOME)% ftp -d inter.uwf.co.jp
Connected to inter.uwf.co.jp
220 inter.uwf.co.jp FTP server ready.
Name (inter.uwf.co.jp:nobu):Username
---> USER Username
331 Guest login ok.
Password:
---> PASS Password
230 User Username logged in.
ftp> get Filename
---> PORT 199,5,60,51,6,4
200 PORT command successful.
---> RETR Filename
150 Opening ASCII mode data connection
226 Transfer complete
```

図3.20 コマンドラインにおける -d オプションで起動したFTPクライアント

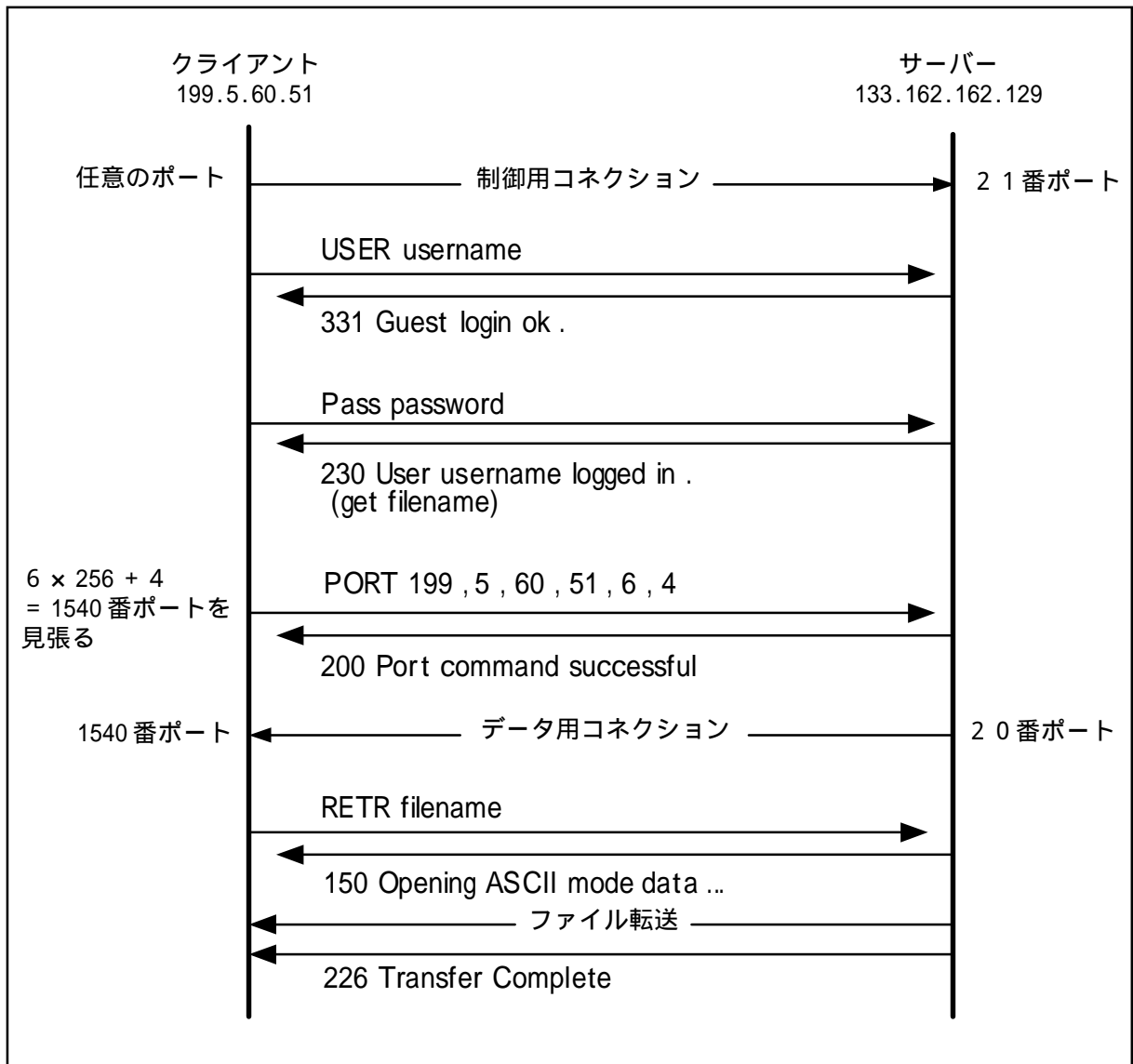


図3.21 FTPサーバーとクライアントのやりとり

なお、詳細はRFC959 (File Transfer Protocol) を参照されたい。

3.4.2. 関連アプリケーション

(1) FTPクライアントソフトのGUI対応

FTPに代表されるTCP/IPインターフェースソフトを利用するユーザーは最近まで、比較的曖昧で不自由なコマンドを学ばなければならなかった。しかし、現在ではGUI（グラフィカル・ユーザー・インターフェース）の普及により、コマンドの構文自体が効果的に隠され、操作がより簡単になっている。

以下に Microsoft Windows™ Version 3.1 上で動作するTCP/IPインターフェースソフトを使用したFTPの使用例を示す。

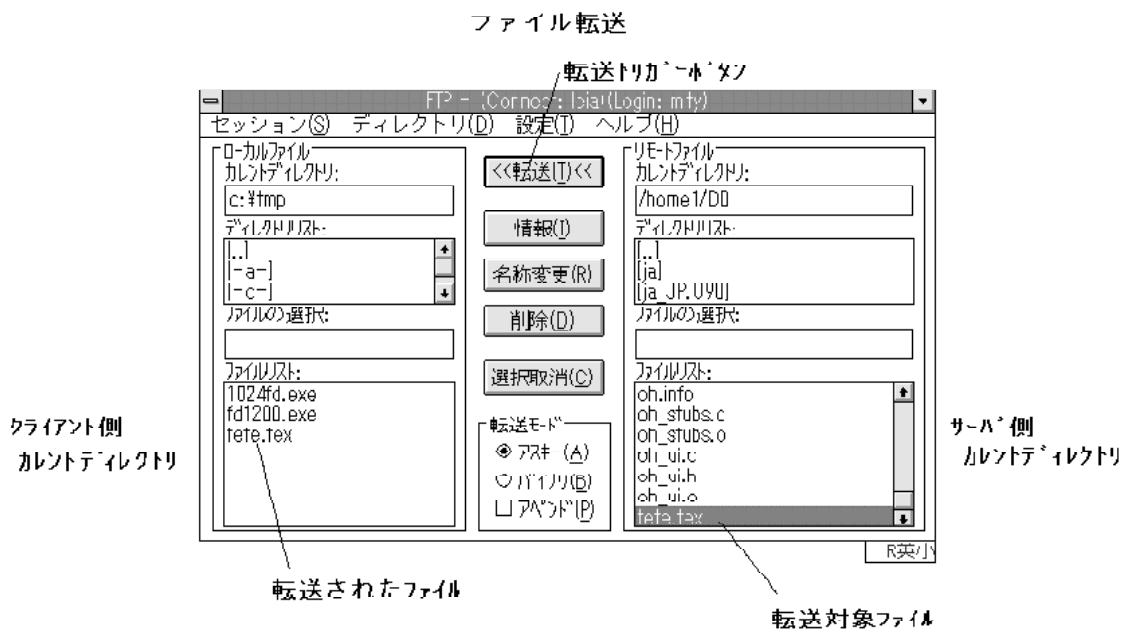


図3.22 GUI化されたFTPアプリケーションの使用例

(2) ネットワークブラウザのGUI対応

現在インターネット上では、FTPをはじめ様々なアプリケーションが使用されている。そこで以下に代表的な情報検索ソフトウェアである、WWW/Mosaicを中心に関連アプリケーションを概観する。



図3.23 WWWサーバーにアクセスしたMosaicの画面例

WWW (World Wide Web) はスイスのCERN (注21) において物理学者たちの研究活動を支援する目的で開発された、ソフトウェアである。インターネット上に散在する情報をハイパーテキスト (注22) 化して、統一されたユーザーインターフェースで提供する。

注21) Organisation (旧 Conseil) Européenne la Recherche Nucleaire の略。欧州合同原子核研究機関。

注22) テキストの文字や絵の一部などから関連したテキストや絵を呼び出すことのできるデータベース。

CERNが開発したWWWサーバーソフトウェアとクライアントソフトウェアは、WWWを普及させる目的で、パブリックドメインソフトとしてソースコードが無料公開された。それ以降ほとんどのWWW関連ソフトウェアは何らかのかたちでこのCERNのソースコードを利用している。

WWWサーバーは、米国イリノイ大学のNCSA (National Center for Supercomputing Applications)が開発したNCSA Mosaicの出現により、急速に普及した。

Mosaicとは、インターネットで利用可能な多数のサービスが統合されているネットワークブラウザソフトの1つである。WWWはHTTPと呼ばれる固有の通信プロトコルを持っているが、その他の概念のサービスを統合するために、HTTP以外にも様々なプロトコルに対応している。クライアントの種類やバージョンによって多少異なるが、具体的には次ページのようなサービス(アクセスプロトコル)が組み込まれている。

WWW : HTTP

ファイル転送 : FTP

メニュー型情報サービス : Gopher (注23)

テキストデータベース : WAIS (注24)

ネットニュース : NNTP (注25)

電子メール : SMTP (注26) 、ただし送信のみ

リモート端末 : TELNET (注27)

これらのサービスは、できるだけ画面表示や操作性が同一になるように工夫されており、ユーザーがサービスの違いを特に意識せずに利用できるようになっている。

Mosaicというひとつのクライアントソフトだけを使えば、従来はそれぞれのサービスごとに独立提供されていたクライアントソフト(FTPクライアント、Gopherクライアントなど)を使う必要がない。このため、ユーザーは自分が欲しい情報によって異なるクライアントを起動し、それぞれのクライアントに固有の操作によって情報をアクセスするという作業から開放される。

注23) メニュー形式でインターネットに分散して蓄積された情報に対するアクセス手段をテキストベースで提供するシステム。

注24) World Area Information Serversの略。インターネットに分散的に蓄積された情報に対するアクセス手段を提供するシステム。

注25) Network News Transfer Protocolの略。Network Newsの記事を読み書きするプロトコル。

注26) Simple Mail Transfer Protocolの略。より単純化されたメール転送プロトコル。

注27) 仮想端末プロトコル。ネットワークを介したリモートホストにログインする。

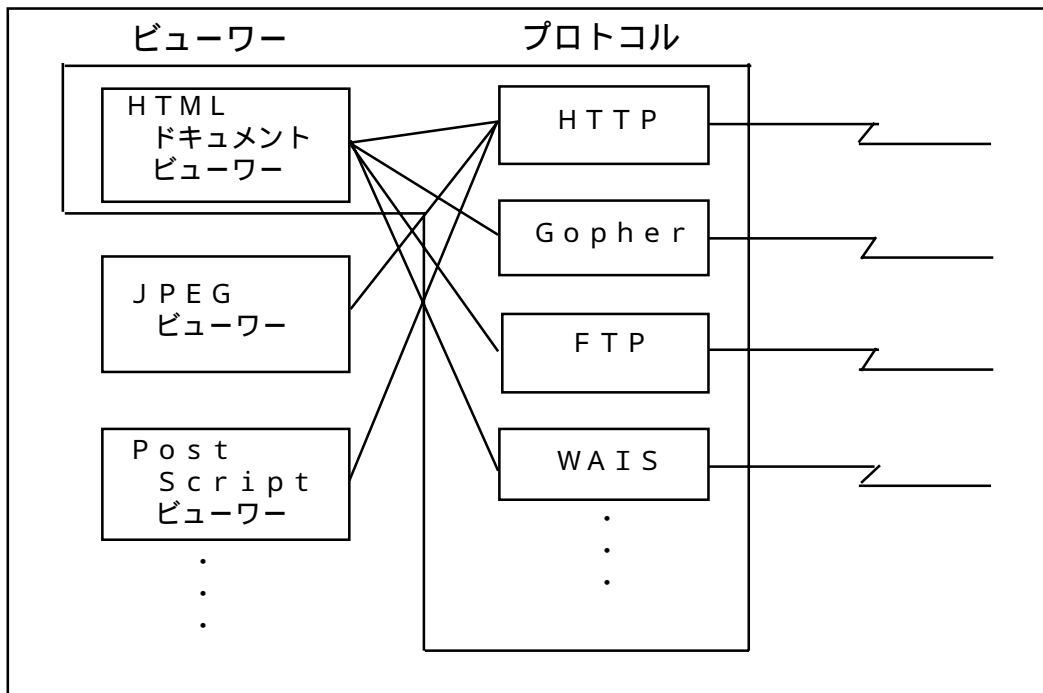


図3.24 WWW/Mosaicのクライアント構成

HTTPは、基本的にはクライアントがサーバーへリクエストを送信し、それに対してサーバーがクライアントへレスポンスを返信するという形式になっている。リクエストは一般に以下のシーケンスである。

メソッド
 URL (注28)
 HTTPバージョン
 リクエストヘッダー
 データ

メソッドは対象となる情報に対して行われる処理を示す。具体的には、GET、HEAD、PUT、POST、DELETEなどであるが、実装の度合いはサーバーにより異なるのが現状である。リクエストヘッダーはRFC 822 (SMTP) およびRFC 1521 (MIME) のフォーマットに従ったいくつかのフィールドからなり、From:、Accept: など数種類が規定されている。

サーバーがクライアントに返すレスポンスは、一般に次のシーケンスからなる。

HTTPバージョン
 ステータスコード
 リーズンライン

注28) Uniform Resource Locator の略でインターネット上の資源を統一的に記述するための記法。

ステータスコードはリクエストを解釈した結果を10進数3桁で表現したもの、リーズンラインは人間に説明を与えるための文字列である。この一連の文字列をステータスラインと呼ぶことがある。

リクエストを解釈した結果が正常であれば、ステータスラインの後にクライアントテキストが続く。ステータスラインがエラーの場合には、エラーであることおよびエラーを通知する何らかの情報がステータスラインの後に続いて返送される。いずれの場合もHTML（注29）のタグによりマークアップされた形式で返送されるため、クライアントは受け取った文字列をそのままHTMLテキストとして表示することが可能である。クライアントとサーバーの応答例を以下に示す。

例1：クライアントのリクエストが成功した場合

クライアントの要求

```
GET /index.html HTTP/1.0
```

サーバーの返答

```
HTTP/1.0 200 Document follows
```

```
MIME-Version:1.0
```

```
Server: CERN/3.0pre6
```

```
Data: Friday, 04-Nov-94 11:25:26 GMT
```

```
Content-Type: text/html
```

```
Content-Length: 1808
```

```
<HTML>
```

```
<HEAD>
```

```
<TITLE>index.html</TITLE>
```

```
</HEAD>
```

```
<BODY>
```

```
．．．(中略)．．．
```

```
</BODY>
```

```
</HTML>
```

注29) Hyper Text Markup Languageの略。ハイパーテキストを記述するための言語

例2：リクエストが失敗した場合（存在しないファイルを要求したとき）
クライアントの要求

```
GET /not-exist.html HTTP/1.0
```

サーバーの返答

```
HTTP/1.0 404 Not found - file does't exist or read  
protected [even tried multi]
```

```
MIME-Version: 1.0
```

```
Server: CERN/3.0pre6
```

```
Date: Friday, 04-Nov-94 11:25:26 GMT
```

```
Content-Type: text/html
```

```
Content-Length: 248
```

```
<HTML>
```

```
<HEAD>
```

```
<TITLE>ERROR<TITLE>
```

```
</HEAD>
```

```
<BODY>
```

```
<H1>Error 404</H1>
```

・・・(中略)・・・

```
</BODY>
```

```
</HTML>
```

以下はHTML、URL、HTTPの関係を図にしたものである。

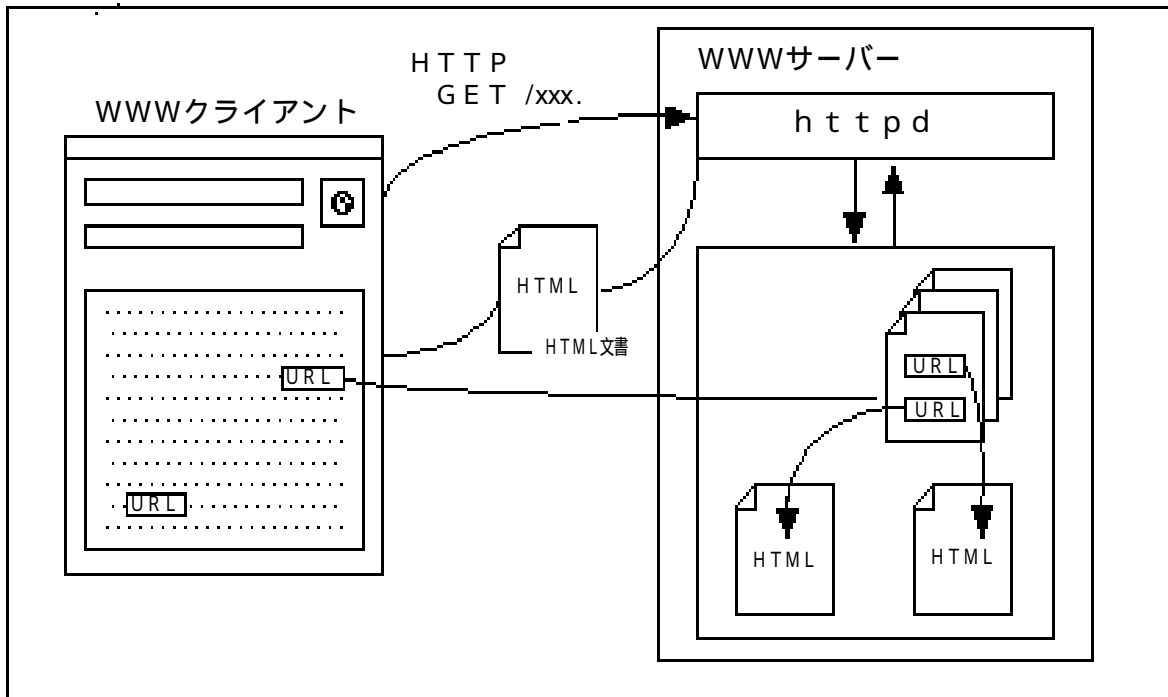


図3.25 動作図

3.5. セキュリティー技術

TCP/IPを使ったネットワーク環境で留意しなくてはならない点として「セキュリティー問題」がある。インターネットの世界的進化やオープンシステム化の急速な広まりで、TCP/IP通信は、多くの企業内システムですでに利用されており、ネットワークに接続されているパソコンやワークステーションは膨大な数となっている。したがって、セキュリティーの全く考慮されていないインターネットや公衆網のアクセスポイントを持つようなネットワークは、「世界中から家の中がすべて見えてしまう」ようなものである。セキュリティーを十分に考慮した、ネットワークの構築および運用は必須である。

3.5.1. セキュリティーに対する基本的考え方

LAN環境でセキュリティーを確保するためには、Firewall（防火壁）と呼ばれる手法を用いることが一般的である。これは、バリアセグメント（または、ボーダーセグメント）と呼ばれるLAN支線を用意して、組織内ネットワークと外部を接続するポイントを1個所に集めることにより、管理を容易にすることを基本とする。外部からのアクセスに必要なホストやマシンはバリアセグメントに配置し、組織内ネットワークとはアクセス制御で外部からの不正なアクセスを防止する。アクセス制御は、その内側のルーターやワークステーションで行う。

ネットワーク構成やアクセス制御の方法についてはいくつかの方法がある。使用形態や規模、目的に合った方法を選択、併用する。

また、安全性と利便性は相反する関係にあることもネットワーク設計をおこなう上で重要である。

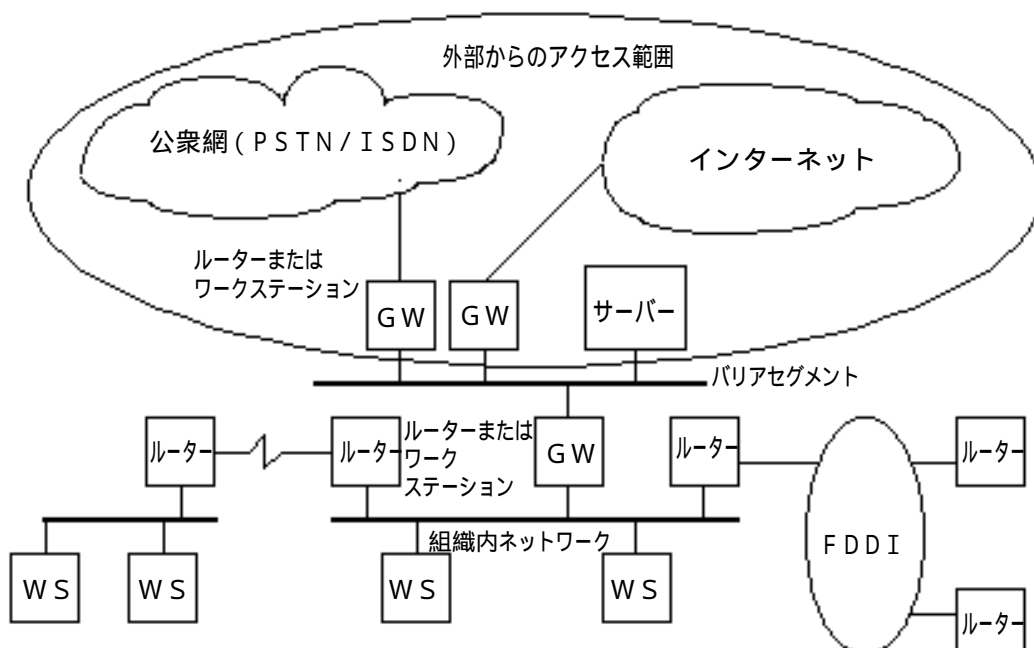


図3.26 Firewallの概念

3.5.2. アクセス制御

代表的なアクセス制御には、次の3つの方法がある。

(1) IPパケットの中継を禁止する

これは最も厳しい制限で、IPパケットの中継をバリアセグメントと内部ネットワーク間で禁止するものである。そのため、バリアセグメントと内部ネットワークを区切るゲートウエーは、ワークステーションとなり、アプリケーションだけで外と内とのやり取りが行われる。

バリアセグメントにサブネットの1つを割り当てる際には安全だが、外と内のゲートウエーとなるマシン上で扱えるアプリケーションしか使えないといった欠点がある。これを避けるため、特定のプロトコルだけを中継するプログラムを動かすことによって、実際の処理を組織内にあるマシンにリレーする手段もある。しかし、大変な方式であることは否めない。

(2) ルーティング情報を流通させない

これには、2つのケースが考えられる。1つは、バリアセグメントと内側のネットワークとが別のネットワーク・アドレスを使い、バリアセグメントのアドレスだけが外からのアクセスで認識される方法である。この場合、内側のネットワークには外からのアクセスはできない。しかし、バリアセグメント上にあるワークステーションと内側のマシンとの間では自由に通信できる。バリアセグメント上に必要に応じて何台ものマシンを配置してサービスをおこなうことが容易になる。

次が、内部のアドレスは外から認識できないが、外から内部のホストまたはマシンと通信したい場合、ネームサーバーをバリアセグメント上に置き、特定のマシンからのアクセスのみ許可する方法である。しかし、マシンの台数が極端に多くなると、ネームサーバーの管理が大変になる。いずれも、アクセス回線上にパスワードなどが流れる可能性が高く、CHAP (PPPの認証機能) などを利用して、回線上にパスワードを流さない工夫が必要である。

(3) ルーターによるフィルタリングをおこなう

ルーターのなかにはかなり強力なフィルタリング機能が実装されているものがある。ルーターのフィルタリング機能としては、ソース (送信元) アドレスでの制御、デスティネーション (送信先) アドレスでの制御、アプリケーションプロトコルごとの制御の3つがある。

IPアドレスでのフィルタリングは、Aというネットワークアドレスは通してもBは通さないといった使い方や、ある特定のアドレスだけ通すか、通さないかといった使い方である。

アプリケーション・プロトコルでの制御とは、SMTPは通すが、TELNETや、FTPは通さないといったものである。注意点としては、アプリケーションプロトコルでの制御をおこなうとオーバーヘッドになることや、機種によっては、これらを組み合わせて使う場合に制約が発生することである。

3.5.3. パスワード

ネットワーク機器、ワークステーションなどのログインパスワードなどの管理は、外部からの不正アクセス対策として極めて重要であり、安易なパスワードは絶対使ってはならない。特にユーザー名や会社名から推測されるパスワードは最も危険である。

また、不必要なサーバーは動作させないことも有効な手段である。技術的には外部から接続し容易にログインしているユーザー名が見えてしまうため、それを足がかりに狙われることも考えられる。パスワードを定期的に変えるなどの運用が必要である。

回線接続	着信制限	電話番号を公表しない 発信者番号通知サービス、グループ セキュリティーサービスの利用
	接続制限	PPPの認証機能(CHAPなど)
ファイアウォール	アクセス制御	IPパケットの中継禁止 ルーティング情報の流通禁止 ルーターによるフィルタリング アドレスによる制御 プロトコルによる制御
運用	ロギング	ログ情報の取得および定期的な ログ情報のチェック
	端末ログイン制限	見抜かれにくいパスワードの使用 定期的なパスワード変更 端末稼働時間の制限

表 3.7 デジタル公衆回線におけるセキュリティー確保のための方法

3.6. 関連するRFCの一覧

以下は、本書に関連するRFCのインデックスである。

- 1 7 2 1 G. Malkin, "RIP Version 2 Protocol Analysis", 11/15/1994.
- 1 7 1 6 P. Almquist, F. Kastenholz, "Towards Requirements for IP Routers", 11/04/1994.
- 1 6 6 1 W. Simpson, "The Point-to-Point Protocol (PPP)", 07/21/1994.
- 1 5 9 7 Y. Rekhter, R. Moskowitz, D. Karrenberg, G. deGroot, "Address Allocation for Private Internets", 03/17/1994.
- 1 5 8 3 J. Moy, "OSPF Version 2", 03/23/1994.
- 1 5 2 1 N. Borenstein, N. Freed, "MIME(Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", 09/23/1993.
- 1 4 6 6 E. Gerich, "Guidelines for Management of IP Address Space", 05/26/1993.
- 1 3 3 4 B. Lloyd, W. Simpson, "PPP Authentication Protocols", 10/20/1992.
- 1 3 3 2 G. McGregor, "The PPP Internet Protocol Control Protocol (IPCP)", 05/26/1992.
- 1 1 4 4 V. Jacobson, "Compressing TCP/IP headers for low-speed serial links", 02/01/1990.
- 1 0 5 8 C. Hedrick, "Routing Information Protocol", 06/01/1988.
- 0 9 5 9 J. Postel, J. Reynolds, "File Transfer Protocol", 10/01/1985.
- 0 8 2 2 D. Crocker, "Standard for the format of ARPA Internet text messages", 08/13/1982.
- 0 7 9 3 J. Postel, "Transmission Control Protocol", 09/01/1981.
- 0 7 9 1 J. Postel, "Internet Protocol", 09/01/1981.

RFCの入手方法

RFCは、日本ではftp.nic.ad.jpや他のおもなAnonymous FTPサーバから入手できる。mail-server@nic.ad.jpのサービスを利用し電子メールで入手することも可能であるし、他のインターネットの情報、ソフトウェアとともにCD-ROMとして販売されている。

第4章 NSK TIFF と NSK プロトコルの運用管理方法

NSK TIFF、およびNSKプロトコルは日本新聞協会（以下、協会）デジタル写真フォーマット、ならびに推奨プロトコル（以下フォーマット、ならびにプロトコル）として今後引き続き、国内の新聞・通信社などで使用される。

フォーマット、プロトコルの運用管理は、他社との交信性や他メディアとの画像データの交換について最低限の機能を確保するために必要であり、協会当該部会がこれらの主旨に適さないと判断する場合は、当該社に運用形態の変更要請、ならびに関連メーカーに対し、該当装置の改修などについて技術的諮問が行える。

協会技術部は、これまでに登録された新聞・通信各社のサービスIDなどの基本情報と協会に登録したメーカーが発売するNSK TIFFをサポートする装置の基本仕様を把握する。

第4章 目次

4.1.	運用管理組織と規定	
4.1.1.	運用管理組織	80
4.1.2.	代表取材の配信	80
4.2.	NSKプロトコル運用の参考例	
4.2.1.	アナログ公衆回線での電送手順例	81
4.2.2.	デジタル公衆回線での電送手順例	82
4.2.3.	運用する上での留意点	82
4.3.	NSK写真電送の応用例	
4.3.1.	商用パソコンネットの利用	83
4.3.2.	LAN間接続	83
4.3.3.	WWWサーバーの利用	83

4.1. 運用管理組織と規定

4.1.1. 運用管理組織

- (1) フォーマット、プロトコルの運用管理に関する協会の窓口は技術委員会情報・通信部会が当たる。

連絡先

〒100-8543
東京都千代田区内幸町二丁目二番一号
(日本プレスセンタービル7階)
日本新聞協会 技術部 技術・通信担当
電話 03(3591)6806(直通)
FAX 03(3591)6149

- (a) フォーマット、プロトコルについて、他社との交信性、他のメディアとの画像データ交換に関する問題などが発生した場合、その対応を協議する。
- (b) フォーマット、プロトコルについて、調査・分析・対応策など、必要に応じてメーカー各社の支援・協力を求める。

4.1.2. 代表取材の配信

代表取材による他社への配信は、これらのフォーマット、プロトコルを適用できるものとする。

4.2. NSKプロトコル運用の参考例

この節では運用する上でヒントになるように、NSK TIFFデータをNSKプロトコルで電送する例を示す。これはあくまで例であり、運用を規定するものではない。

4.2.1. アナログ公衆回線での電送手順例

アナログ公衆回線での電送形態例を図4.1に示す。図の(a)「電送端末または写真送受信システム」を送り側、(b)「写真送受信システム」を受け側とする。NSK TIFFおよびNSKプロトコルは、図の矢印で示す範囲での規定であり、各社内のシステム間通信のフォーマットやプロトコルにおよぶものではない。

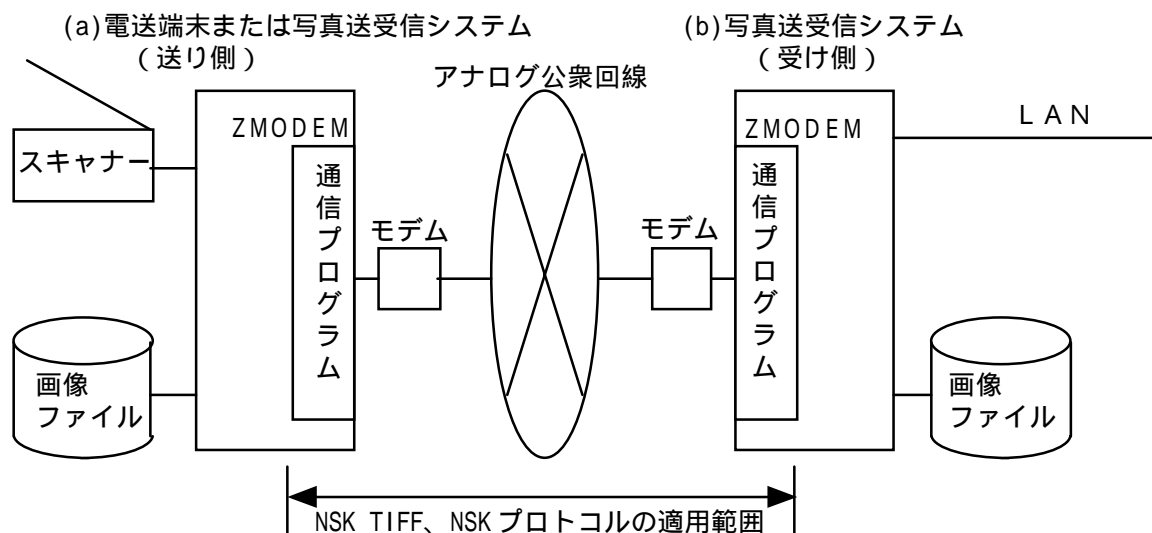


図4.1 アナログ公衆回線での電送形態例

(1) 回線の接続とデータリンクの確立

送り側から発呼する。受け側は常に受信可能とする。発呼からデータリンク確立までは、通信プログラムにより一連の流れで行われる。

(2) ファイル転送

ZMODEMプロトコルでファイルを転送する。オプションでレジューム機能、複数ファイル指定を使用できる。受信側は送信側のオプションに従って動作する。

ファイル名は自由だが、DOS形式(8.3)でエクステンション部がNSKであることを推奨する。

1回のファイル転送が終了した後、回線を接続したまま別のファイルを連続して転送することができる。

(3) データリンクの解放と回線の切断

送り側からリンクの終了と回線の切断を指示する。

4.2.2. デジタル公衆回線での電送手順例

デジタル公衆回線での電送形態例を図4.2に示す。図の(a)「電送端末または写真送受信システム」を送り側、(b)「写真送受信システム」を受け側とする。

NSK TIFFおよびNSKプロトコルは、図の矢印で示す範囲での規定であり、各社内のシステム間通信のフォーマットやプロトコルにおよぶものではない。

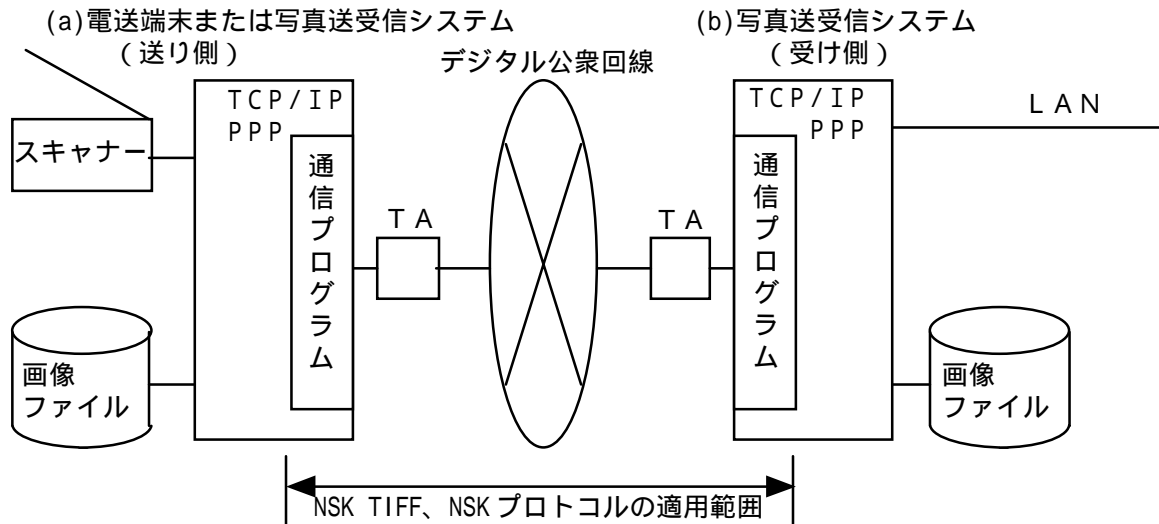


図4.2 デジタル公衆回線での電送形態例

(1) 回線の接続とデータリンクの確立

送り側から発呼する。PPPを使ったダイヤルアップIP接続とする。受け側は常に着信可能であり、着信と同時にPPPが動作する。受信側は、プールしているIPアドレスからひとつ選んで送信側に通知し、送信側は受信側から通知されたIPアドレスを使用する。このアドレスは、受信側システムに依存する。JPNICに登録していないアドレスを使用する場合は、プライベートアドレスを使用する。

(2) ファイル転送

FTPのputを使用する。ファイル名は自由。

(3) データリンクの解放と回線の切断

送り側から切断する。

4.2.3. 運用する上での留意点

(1) 回線番号の通知

回線番号を事前に通知する方法は、セキュリティー問題もあり、実際の運用する相手などとの検討が必要である。

(2) 認証のパスワード管理

デジタル公衆回線でPPPによるダイヤルアップIP接続でCHAPによる認証を使う時、およびFTPでloginする時のパスワードをいかに管理するか、セキュリティーと操作性の両面から検討する必要がある。

4.3. NSK写真電送の応用例

デジタルデータのファイル転送で写真を電送するため、上記プロトコルの他に、発展形態を考えることができる。今後の検討が望まれる。

4.3.1. 商用パソコンネットの利用

インターネットのような地球規模ネットワークや、パソコン通信会社同士の国際的な業務提携、またはパソコン通信会社のインターネット接続を利用すれば、プライベートネットワークの自社開発に比べ設備投資費や運用サポート費用などを軽減することができる。特に海外など遠隔地からの電送においては、ネットワークプロバイダーやパソコン通信サービスの提供するアクセスポイントを利用すると、品質の安定しない国際公衆サービスを利用するより、確実に高品質のデータ伝送が行え、時差も吸収できる。

4.3.2. デジタル回線でのLAN間接続

今回推奨する基本形態はPPPによるダイヤルアップIP接続だが、各社のLAN環境が進むにつれてLAN同士を接続（インターネット接続を含む）する形態（3章で解説）が増えることが予想される。

4.3.3. WWWサーバーの利用

インターネット上、またはプライベートに構築されるWWWサーバー（3章で解説）を利用して写真データの転送に応用することも考えられる。

コラム 取材無線とデジタル写真電送

各社で活用している無線写真電送はいまだ「アナログ電送」が定番だ。しかも、取材無線は新聞・通信各社間での通信が電波法上許可されないため標準化作業では対象とならなかった。

「写真電送は携帯電話や衛星回線に完全移行する予定・・・」といった無線担当者にとって寂しい話しも聞かれ、「デジタル」全盛時代の到来で「無線写真電送」も歴史的使命を終えたかと思われた。ところが、阪神大震災で取材無線が大活躍、「取材無線でのデジタル写真電送の実現話し」が急浮上することになる。

そこで、アイデアとして出されるのは、回線モデムを使ったタレ流し電送やFAXモデム利用だが、困ったことにデジタル写真電送はアナログ電送とは勝手が違いノイズ混入などがあればまず使い物にはならない。エラー訂正ができなければ要件を満たせない

次の手は、アマチュア無線や産業用で利用されているTNC（ターミナル・ノード・コントローラ）を使った無線パケット通信によるファイル転送が思い浮かぶ。しかし、画像データを短時間で送るにはプロトコルが重い。残念ながら、現状では容易に接続できる高速TNCは売られておらず開発されることを待つしかない。究極的な解決方法は、無線システムのデジタル化だ。警察庁が盗聴防止などのために採用した方式だけにセキュリティの点でもメリットは大きい。送受データを半分に圧縮すれば全二重通信が可能で、データ伝送との親和性も高い。嬉しいことに、郵政省も電波の有効利用からデジタル化には好意的と聞く。しかし、この話には莫大な費用がかかるといった決定的な欠点があった。台所事情が許せば是非検討頂きたい。

これまで述べたように、現段階では取材無線でのデジタル写真電送を実現するための決定打はなかなか見えてこない、原因を整理すると

- ・送受信制御が必要なため既存プロトコル利用が難しい。
- ・デジタルポートとのインタフェース装置が無い。

の2点に集約されそうである。

結論としては、「プロトコルとインタフェース装置を開発」すれば簡単に解決する問題ではあるのだが！？

(み)

第5章 NSK TIFFとNSKプロトコルの展望

デジタル写真標準フォーマットならびに推奨プロトコルの完成に伴い、今後、取り組まなければならない課題としてグラフィックスを含めたマルチメディアへの対応や、記事系システムと画像系システムとの統合など、次世代新聞制作システムの構築にあたって懸案とされてきた諸テーマへの対応があげられる。新聞・通信各社がマルチメディア時代に対応するシステム構築を行なう過程で、どのような技術の標準化・規格化をはかるべきかを十分検討する必要がある。

5.1. ではフォーマットのマルチメディアへの対応について、5.2. ではプロトコルをめぐり技術動向について、5.3. では協会の対応を含む今後の課題について述べる。

第5章 目次

5.1.	NSK TIFFとマルチメディア	
5.1.1.	グラフィックス	86
5.1.2.	動画、音声	86
5.2.	NSKプロトコルをめぐり技術動向	
5.2.1.	アナログ公衆網の利用動向	87
5.2.2.	デジタル回線サービスの動向	87
5.2.3.	移動体通信サービスの動向	88
5.3.	今後の課題	
5.3.1.	代表取材への対応	89
5.3.2.	保存メディアの選択	89
5.3.3.	記事系と画像系システムの統合	90
5.3.4.	協会での取り組み	90

5.1. NSK TIFFとマルチメディア

5.1.1. グラフィックス

NSK TIFFでは多値画像データが対象となっており、ポストスクリプトデータや二値圧縮のJBIGデータなどのグラフィックスの取り扱い規定はない。

共同通信社は加盟社への写真配信には、ポストスクリプトデータを内部に包括できる新共同フォーマットを採用した。またAP通信社では米国内のグラフィックス配信にPDF（注30）の採用を検討している。

ポストスクリプトデータは、新聞業界だけでなく一般にも事実上の標準であり、新聞協会としても早急な対応が望まれている。

グラフィックスを扱う方法としては、NSK TIFFにポストスクリプトデータを包括する形でのバージョンアップのほか、写真やグラフィックスなど、様々なデータを包括する新フォーマットの策定が考えられる。

このように様々なデータを統一的に扱え、しかもOSやアプリケーションを超えて使用できるフォーマットの研究は、これからの大きなテーマのひとつである。

5.1.2. 動画、音声

新聞業界では、これまで素材として記事、写真、グラフィックスなどが使われてきた。新聞が印刷物という形態をとる限り、これ以外の素材を扱うことはできない。

米国では情報スーパーハイウエー構想がスタートし、多くの新聞社がパソコン通信やインターネットを利用した電子新聞を事業化しつつある。

日本では通信網の整備が不十分であり、またパソコンの普及率も低いため、すぐに電子新聞を事業化できる環境にはない。しかし、インフラの整備により、近い将来、動画や音声を取り込んだ電子新聞が出現する可能性は非常に高い。

欧米ではこのような時代を想定し、新聞・通信社による共同研究もスタートしている。マルチメディアにかかわるフォーマットの研究は重要になるだろう。

注30) Portable Document Format の略。テキスト、写真、グラフィックスなどすべてのデータを包括できると言われているアドビシステムズ社が開発したフォーマット。

5.2. NSKプロトコルをめぐる動向

5.2.1. アナログ公衆網の利用動向

今後、技術進歩によりアナログ回線用モデムは、高速性、信頼性がより求められ、現在の方式とは異なったものが登場してくる可能性はある。しかし、ZMODEMは、アプリケーションによるファイル転送方式であるため、基本的にはその場合でも利用が可能であろう。

また、インターネットサービスを、エンドユーザーがアナログ公衆網からアクセスできるような、PPP・TCP/IP通信が一般に行われ出した。これは伝送メディアがアナログ回線ということだけで、3章で述べたデジタル回線での、NSK TIFFを転送するFTPプロトコルや、リモートアクセス、セキュリティー技術の考え方などは、そのまま利用が可能である。

5.2.2. デジタル回線サービスの動向

LAN間をより高速に接続しようと発展してきたWAN（注31）技術の一つに、フレームリレー技術がある。これは光ファイバーなど信頼性の高い伝送メディアをもとに、誤り制御や再送制御を上位層に委ねることで、2 Mbpsまでのパフォーマンスを発揮するデータ交換サービスである。バースト的に発生するLANのトラフィックと相性が良く、網内で輻輳制御が働くまで可変長フレームにより帯域を有効に利用する。

今後、マルチメディア対応できるサービスにB-ISDN（注32）がある。このサービスではATM（注33）技術を駆使し、6～156 Mbpsのシームレスなネットワークサービスが提供される。

注31) Wide Area Networkの略。LAN間をデジタル回線などで接続した広域LAN。

注32) Broadband-ISDNの略。ITUが提唱する超高速デジタル伝送サービス。網内の伝送技術としてATM技術が使われる。

注33) Asynchronous Transfer Modeの略。非同期転送モード。軽量のヘッダーとデータを固定長のセルにすることで、ハードウェアスイッチング技術により高速伝送を可能としている。

5.2.3. 移動体通信サービスの動向

自動車・携帯電話をはじめとする移動体通信サービスは、今後著しい発展を遂げることは間違いない。現在、ファイル転送などで利用されている移動体通信媒体の主流は自動車・携帯電話である。特にデジタル携帯電話サービスはアダプターやアプリケーションも用意されており、まさにデータ伝送向きのサービスといえる。NTTドコモでは1995年4月から9600 bpsの高速伝送サービスを開始しておりNSKプロトコル利用も容易である。

また、1995年7月からサービスが開始されるPHS（注34）は32 KbpsのADPCM（注35）で音声サービスをおこなうことから、高速データ伝送利用に期待が持たれている。データ伝送利用では誤り制御などのため実質的なスループットは28.8 Kbps程度と予測されるが、2回線を同時利用する57.6 Kbpsのサービスの可能性もある。

通信衛星サービスの関連では、インマルサット（注36）の国内利用の可能性やN-STAR（注37）衛星を利用した電話サービス、1998年にサービスが予定されているイリジウム計画（注38）などが注目されるところである。他にも、国際衛星移動通信計画（非静止衛星）としてプロジェクト21（INMARSAT）、グローバルスター（Loral Qualcomm Satellite Services Inc）、テレデシック（Teledesic Corp）などの計画がある。いずれも1997年から2001年までにサービス開始を予定している。しかし、現段階では64 Kbpsで高速デジタルサービスを始めたインマルサットA・HSDサービス以外は高速データ伝送利用の可能性についてはっきりしていない。

注34) Personal Handyphone Systemの略。簡易携帯電話システム。

注35) Adaptive Differential Pulse Code Modulationの略。音声符号化方式の一つ。

注36) 国際海事衛星機構の衛星サービス。日本ではKDDだけがサービスしている。電話、FAX、データなどの利用が可能だが国内利用は原則的に認められていない。

注37) NTTが中心となり1995年秋に打ち上げを予定している大型の通信衛星。NTTドコモがトランスポンダーの一部を使用して移動体通信サービスをおこなう予定。

注38) 米モトローラ社の国際衛星移動通信計画。66個の低地球軌道衛星で全世界をサービスエリアとする。

5.3. 今後の課題

5.3.1. 代表取材への対応

これまでの代表取材写真の配信は、幹事社が受信した写真を印画紙で配布する方法が一般的であった。しかし各社が写真集配信システムを構築したことや、カラー化が進んだことにより、蓄積データでの配信の要求が高まった。最近では在京各社が、NTT電話会議サービスを利用した配信を試みている。

新聞協会でフォーマットやプロトコルを策定した理由のひとつは、加盟各社間での写真データ送受信を効率的に行うためである。

今回のプロトコル決定によりこの目的は達成されたが、Point to Point を前提にしているため完全な同送は困難である。代表取材の写真配信で同送を実現するには、今後も研究を重ねていく必要がある。

5.3.2. 保存メディアの選択

NSKプロトコルによる通信でのデータ配布方法は、大量のデータを多くの社に渡す場合には時間差、手間、通信コストなどが問題となる。このことから、データを保存したメディアの配布方法も検討しなければならない。

保存メディアに求められるものは、大容量であること、汎用性が高いこと、十分なアクセス速度を持っていることである。現状では、光磁気ディスクが一般的だが、互換性、速度についてはまだ十分とはいえない。

5.3.3. 記事系と画像系システムの統合

新聞業界のシステムは、これまで記事系、画像系それぞれが独立して考えられ、構築されてきた。これは記事系、画像系が技術的に重なる部分が少なく、それぞれ独自に進化してきたことが原因となっている。しかし、オープン化やダウンサイジングにより使用されるコンピューター、OS、データベースなどが共通となってきた現在では、記事系と画像系を分ける理由は希薄で、むしろ別システムであることの欠点が指摘されるようになってきた。支局からのデータ集信から本社内の編集処理までの運用能率向上、コスト低減など記事、画像連携の利点は多い。

これからのシステム開発は、トータルシステムとして考えていく必要がある。

5.3.4. 協会での取り組み

新聞協会は1994年9月、電気通信委員会と工務委員会を統合し、新たに技術委員会を発足させた。新委員会発足にあたり、「情報サービスや通信政策など、特にマルチメディア時代をにらみ、各種技術の標準化・規格化などに対応できる委員会構成とする」とうたわれた経緯もあり、委員会のもとに設置された情報・通信部会、制作部会はこれらのテーマに取り組む姿勢を整えつつある。従来、旧電気通信委員会を中心に対応してきた各種標準化に関する課題も今後は、情報・通信部会、制作部会が連携し、取り組む必要がでてくると思われる。

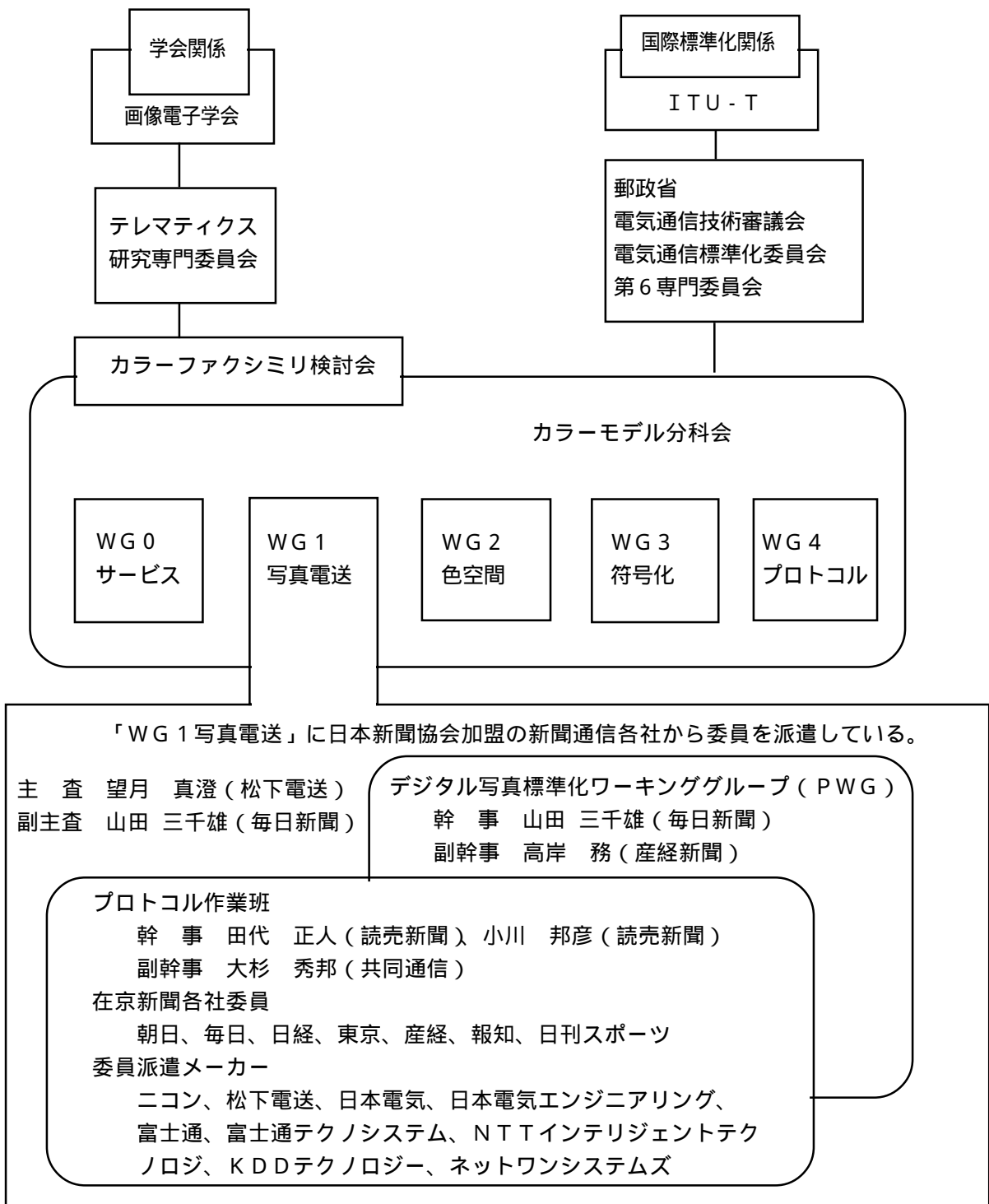
デジタル写真標準化ワーキンググループは、英国・ウインザーで開催されたIPTC春季全体会議に二度にわたり代表を派遣し、NSK T I F FとNSKプロトコルの策定経緯の報告を行ない、有意義な意見交換を行なうことができた。今後の標準化策定作業は日本国内のみならず、世界の標準化動向を把握しながら進めていかなければならない。

NSK T I F FとNSKプロトコルの策定に際しては、郵政省電気通信標準化委員会ならびに画像電子学会に当協会から委員を派遣する形で検討作業を進めてきたが、今後、業界の各種標準化研究に着手するにあたっては、I F R A（国際新聞印刷技術研究協会）やN A A（米国新聞協会）のように新聞協会もメーカーとの合同研究部会を発足させ、検討する必要もあるだろう。

付録A . 策定組織とメンバー

1 . 策定組織と関係組織

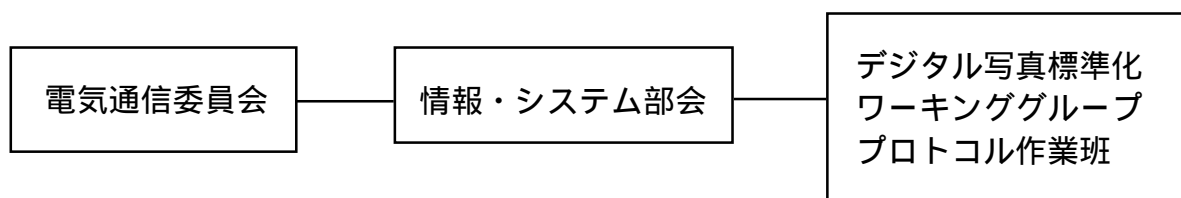
(WG 1、PWG、プロトコル作業班などの関係組織図)



2. 社団法人日本新聞協会 技術委員会組織図

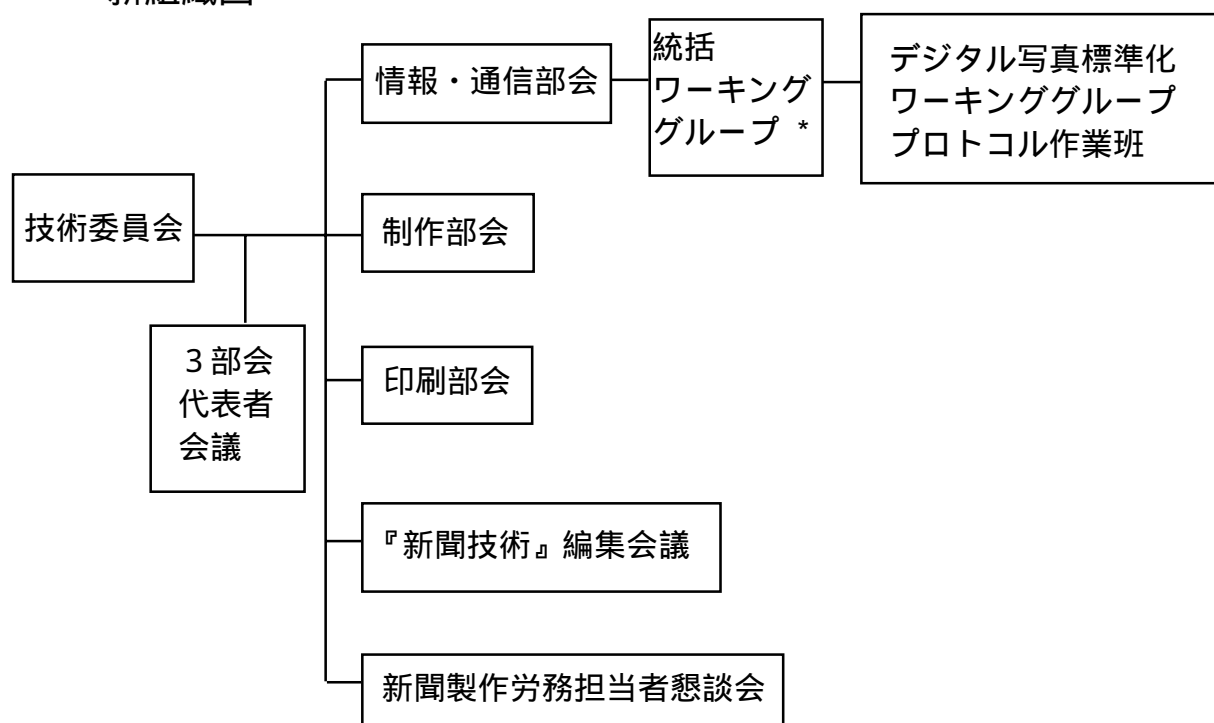
(日本新聞協会と本書を作成したワーキンググループとの関連組織図)

< 旧組織図 >



1994年9月9日、上記の電気通信委員会は工務委員会と統合、現在の技術委員会となり、同委員会の下部組織の構成は下記のとおり変更になった。

< 新組織図 >



* 統括ワーキンググループは、1998年5月15日開催の技術委員会において、その活動終了が承認された。

3 . 策定方法ならびに N S K プロトコル策定メンバー

策定方法

本規格は、日本新聞協会技術委員会情報・通信部会の下部組織であるデジタル写真標準化ワーキンググループにより作成された。下記メンバーにより構成されるデジタル写真標準化ワーキンググループは、カラーファクシミリの標準化を目的として組織された、郵政省電気通信標準化委員会・第6専門委員会・カラーモデル分科会と連携して、カラー写真電送部門の標準化を行い、平成6年4月、日本新聞協会デジタル写真フォーマット（NSK T I F F）を策定した。本規格は、NSK T I F F策定後、下記のメンバーにより策定されたNSK T I F F電送の推奨通信プロトコルである。

NSKプロトコル策定メンバー

（W；WG委員、P；プロトコル検討作業班委員）

《日本新聞協会デジタル写真標準化ワーキンググループ》

新聞・通信社各委員

神保 修	朝日新聞東京本社（W、P）
南村 幸弘	朝日新聞東京本社（W、Pそれぞれ1995年3月まで）
山田三千雄	毎日新聞東京本社（W副主査、P）
田代 正人	読売新聞社（W、P幹事）
小川 邦彦	読売新聞社（W、P幹事）
佐治 俊一	日本経済新聞社（W）
佐藤 博之	日本経済新聞社（P）
三菅 道夫	日本経済新聞社（P）
橋村 清三	東京新聞（W、Pそれぞれ1994年12月まで）
杉本 雅昭	東京新聞（W：1994年12月から、P）
上 学	東京新聞（P：1994年12月から）
高岸 務	産経新聞東京本社（W）
石川 勉	産経新聞東京本社（P）
増田 善功	報知新聞社（W、P）
米村 讓	日刊スポーツ新聞社（W）
新村 良孝	日刊スポーツ新聞社（P）
大杉 秀邦	共同通信社（W、P副幹事）
本多 浩	時事通信社（W）

《カラーファクシミリ検討会WG1》

外国通信社各委員

- 大澤 雄一 A P 通信社東京支局 (W : 1994 年 12 月まで)
佐藤 光彦 A P 通信社東京支局 (W : 1994 年 12 月から)
田島 学 A P 通信社東京支局 (W)
浜口 徹 ロイタージャパン (W)
田中 久恵 ロイタージャパン (W)
青山 亨 A F P 通信社東京支局 (W : 1994 年 12 月から)

電気通信事業者、メーカー各委員

- 安藤 大 NTT (W、P それぞれ 1994 年 11 月まで)
矢谷 正 NTT インテリジェントテクノロジー (W、P それぞれ 1994 年 11 月から)
斉藤 雅弘 KDD テクノロジー (W、P それぞれ 1995 年 2 月まで)
柳原 広昌 KDD テクノロジー (W、P それぞれ 1995 年 2 月まで)
河野 健男 KDD テクノロジー (W、P それぞれ 1995 年 2 月から)
鶴本 啓三 KDD テクノロジー (W、P それぞれ 1995 年 2 月から)
北村 義男 ソニー (W)
白柳 彰彦 東芝 (W)
豊田 堅二 ニコン (W : 1994 年 12 月まで)
原 俊郎 ニコン (W : 1994 年 12 月から)
中山 正 ニコン (W、P)
中川 博之 日本コダック (W)
橋口 祥一 日本電気 (W、P)
荒川 徳夫 日本電気エンジニアリング (W、P)
川北 修 ネットワンシステムズ (P : 1995 年 1 月から)
安藤 卓哉 ネットワンシステムズ (P : 1995 年 1 月から)
山口 誠吾 富士通 (W、P)
木村 誠 富士通テクノシステム (W、P)
長沼 泰宏 富士通 (P)
石川 茂雄 松下電送 (P)
寒澤 剛 松下電送 (P)
望月 真澄 松下電送 (W 主査)
梶 光雄 東京工芸大学、ITU - T、カラーモデル分科会委員 (W)

付録 B . 参考文献一覧

参考文献一覧

- [1] F T P、UNIX MAGAZINE 1995年1月号、山本 和彦、アスキー、1995年
- [2] H D L Cを使いこなす - H D L C時代の通信技術、インターフェース1991年2月号、高見 豊、高見 則子、CQ出版、1991年
- [3] I Pアドレスを取得する、Internet User Vol.1 No.5、1995年5月号、関 功、1995年
- [4] N S K T I F F、日本新聞協会デジタル写真フォーマット、デジタル写真標準化ワーキンググループ フォーマット作業班、(社)日本新聞協会、1994年
- [5] P C - 9 8 0 1通信プロトコルスーパーテクニク、山本 和信、佐川 顕、北原 静香、宮本 恒弘、宮下 好夫、アスキー
- [6] P P PとダイヤルアップI P接続、UNIX MAGAZINE 1995年2月号、大野 俊治、アスキー、1995年
- [7] P P Pによる廉価なI P接続、UNIX MAGAZINE 1993年3月号、Robert A. Sutterfield、アスキー、1993年
- [8] T C P / I Pによるネットワーク構築Vol.1、Douglas Comer、村井 純、楠本 博之、共立出版
- [9] T C P / I Pバイブル、Kevin Wahburn、Jim Evans、油井 尊、ソフトバンク
- [10] The Digital Information Transmission Protocol (DIT), Stephane Guerillot (AFP), France, 1991,Version 3.0
- [11] The ZMODEM Inter Application File Transfer Protocol,Chuck Forsberg, Omen Technology Inc, 1990
- [12] 異機種接続とT C P / I P絵とき読本、道下宣博、本間泰則、オーム社、1990年
- [13] インターネット参加の手引き 1994年度版、bit別冊、WIDE Project 編、共立出版、1994年
- [14] 新プロトコルハンドブック、朝日新聞社、1994年
- [15] 特集T C P / I Pの動作原理とトラブル対策、インターフェース1993年8月号、CQ出版編集部、CQ出版社、1993年
- [16] 特集：通信プロトコル研究、C Magazine、1993年
- [17] 日経データプロデータ通信標準、日経データプロ、日経データプロ編集者、日経B P社、1994年
- [18] マスタリングT C P / I P 入門編、竹下 隆史、他、オーム社

付録 C . 関連用語一覧

五十音順関連用語一覧

イーサネット

Ethernet。10Mbps 程度の速度を持つ LAN のメディアおよびプロトコル。バス型のトポロジーを持つ 10BASE5、10BASE2、スター型のトポロジーとなる 10BASE-T、10BASE-F がある。近年、より対線 (U T P) を用い配線・管理が容易な 10BASE-T が多く導入されている。

インターネット

広義の意味で用いる場合は、LAN 同士を広域回線を介して接続した状態をインターネット、インターネットワークという。また、これとは少し異なる意味で「インターネット」という語を使う場合も多い。TCP / IP 通信の世界 (IP アドレスの世界) は、現在全世界と接続されている。この全世界的なネットワークの固有名詞としてインターネット (The Internet) と呼ぶ。

エンドノード

Endnode。通信での最終目的のノードをいう。

オーバーヘッド

実際に通信を行う場合に、実データ以外に必要な制御のための処理部分。

オクテット

Octet。8 ビットを表す単位 (情報転送単位) 。

クライアント

Client。コンピューターネットワークでサービスを受ける側の機器、サービスを要求する側の機器。

ゲートウエー

Gateway。OS I 参照モデルの 7 階層までに渡って変換を行う装置。UNIX や IP ネットワークでは、ルーターのことをゲートウエーと表現する場合がある。

公衆回線

遠隔地間を接続する回線で、不特定多数の人が共有できる回線。電話網、X.25、ISDN などがこれにあたる。

コネクション

コネクション型の通信の場合、データを送信する時に、送信する端末と受信する端末間、つまりエンドノード間で通信を行うための「論理的な通信路 = コネクション」を設定する。データは必ずこのコネクション上を流れていき、データの到着や順序が保証される。

サーバー

Server。コンピューターネットワークでサービスを提供する側の機器。

サブネット

IPアドレスは、主にIPネットワークアドレス部とIPホストアドレス部からなるが、このIPホストアドレス部をさらにネットワークアドレスとして分割したものをIPサブネットワークという。このIPサブネットワークを定義するのがサブネットマスクとなる。

垂直分散

ホストコンピューターを中心に縦方向に機器を展開する方式。汎用コンピューターに複数の専用回線を介してノンインテリジェント端末が接続する場合などがこれにあたる。

水平分散

接続される機器同士が同等の力関係で通信を行い、横方向に発展していく方式。垂直分散のようにホストコンピューターに処理が集中する形でなく、コンピューターネットワークにつながる各コンピューターに処理が分散される形となる。

スタンドアロン

Stand Alone。ワークステーションやパソコンなどを1台のみで使用すること。コンピューターをネットワークに接続せず使用することの総称。

スループット

1秒間にどの程度のパケット処理能力があるかを表す言葉。単位はPPS (Packets Per Second) など。

専用回線

遠隔地間を接続する回線で、契約者のみがバンド幅を専有できる回線。専用回線には9600bpsなどの低速なものと、より高速なスーパーデジタル回線などがあり、コンピューターネットワークを接続する媒体として用いる。

ダウンサイジング

Downsizing。1980年代後半、パソコンやワークステーションの性能が飛躍的に向上し、価格も低下してきた。同時にTCP/IPの普及・発展や、OSの進化によりこれらのコンピューターをネットワークで接続することも一般的になってきた。この結果、ホストコンピューター（メインフレーム）で行っていた企業の業務を、パソコンやワークステーションのシステムに置き換える動きがでてきた。これをダウンサイジングという。

多重化

一本の回線（通信路）を複数のユーザー、サービスで共用すること。

データグラム

データのかたまり、もしくはデータを表す単位。パケット、フレームと同様な意味。

デーモン

デーモンとは、常時起動されていて特定の処理を行うプロセスのことをいう。

電子メール

ネットワーク上で特定の相手に対して、メッセージ（ファイル）を送り届けるサービス。紙に書かれた手紙をネットワーク上で実現しているイメージとなる。

ト・クンリング

Token Ring。リング形式のLAN。伝送速度には4Mbpsと16Mbpsのものが存在する。信頼性、転送効率はイーサネットより高い。見かけ上はスター型のネットワーク構成をとるものも多いが、論理的な接続形態はリング型となる。トークンというパケットがリング上を回っており、データを転送したいノードはこのトークンの後ろにデータをつけて送り出すことになる。標準化はIEEE802.5による。

ドメイン

DNSで階層化された名前的一部分で、組織部分を表す場合が多い。通常、同一組織であれば同一ドメインを使う。

トラフィック

ネットワーク上を流れるデータ量を意味する。

ネットワークアーキテクチャ

Network Architecture。コンピューター通信を実現するための考え方や体系を示したものの。つまり、コンピューター通信を行うための、全体構成（技術、データの流れなど）を提示したものといえる。SNA（IBM社）、FNA（富士通）、HNA（日立製作所）、XNS（ゼロックス社）など各社それぞれのものがあるが、各社ともTCP/IPとOSIに対応するようになりつつある。

ノード

Node。ワークステーション、ルーター、その他各種のコンピューターなどネットワークに接続されている機器の総称。

パケット

Packet。データのかたまり、もしくはデータの単位の呼び方。ネットワーク層以上で使う表現。

パケット交換

大きなデータを、小さなデータのかたまり（パケット）に分割し転送する方法。パケットには発信元、宛先、元データの位置などの情報を含むヘッダーが付く。これによりひとつの通信路を複数のユーザーで共用することが可能になる。

フィルター

ブリッジ、ルーターなどのインターネットワーク機器が、フレーム（パケット）をアドレス、その他の情報、基準に基づいて、その機器を通過させるさせないの判断をすること。

ブリッジ

Bridge。2つ以上のネットワークを接続する時に使用され、相互のデータを中継する。ブリッジはデータリンク層での中継機器に位置する。

ブルーター

対応するプロトコルについてはルーターとして機能し、非対応のプロトコルについてはブリッジとして機能する。マルチプロトコルルーターの多くは、ブリッジの機能を元から持っていたり、付加することが可能。これらもブルーターの種類といえる。ブリッジルーター、ブリッジ/ルーターなどと表現する場合もある。

フレーム

Frame。データのかたまり、もしくはデータの単位の呼び方。データリンク層レベルではフレームという単位で表す。

ブロードキャストパケット

同一ネットワーク内の全ノードに対して、同時に送るパケットのこと。同報パケットともいう。

プロトコル

Protocol。コンピューター通信を行うために必要な約束事をいう。コンピューター同士で通信を行う場合はプロトコルが一致している必要がある。

ホスト

Host。TCP/IP通信では、IPホストアドレスを持つコンピューターや接続装置などを指す。UNIXでは、ネームサーバーやTELNETの接続先のサーバー、データベースサーバーなどを慣用的に指す場合もある。また、汎用大型コンピューター（メインフレーム）やミニコンの世界では、その大型コンピューター、ミニコン自体を指す言葉として使われる場合もある。

ユニキャスト

ユニキャストは相手先をひとつに特定したパケットを指す。ブロードキャストやマルチキャストは複数の相手先をターゲットにするのに対して、ユニキャストはひとつの相手先がターゲットになる。

より対線

Twisted Pair Cable ツイステッドペアケーブル（ツイストペアケーブル）。シールドをされているSTP(Shielded Twisted Pair Cable)とシールドをされていないUTP(Unshielded Twisted Pair Cable)がある。

ルーター

Router。2つ以上の物理的なネットワークを接続する時に使用され、相互のデータを中継する。その際、経路情報を参照し、ルートを決めてデータを中継する。ネットワーク層での中継機器に位置する。

ルーティングプロトコル

Routing Protocol。経路情報を伝達もしくは取得するために使用するプロトコル。TCP/IP通信ではRIP、OSPFなどが使用されている。

アルファベット順関連用語一覧

anonymous F T P

インターネット上に数多く存在する、誰でも利用することのできるサーバー。便利な各種の P D S (パブリックドメインソフトウェア) や、いろいろなデータベースサービスなどが用意されている。

A N S I

American National Standard Institute 米国規格協会。アメリカ国内の標準化機関。

A P I

Application Program Interface。

A R P

Address Resolution Protocol。I P アドレスからハードウェアアドレスを得るためのプロトコル。

A R P A N E T

Advanced Research Projects Agency Network。米国国防総省 (DOD) がパケットやプロトコルの実験をするために開始したネットワーク。

A T M

Asynchronous Transfer Mode 非同期転送モード。B-ISDN を実現するための回線交換とデータ伝送の技術。

B - I S D N

Broadband-ISDN の略。ITU が提唱する超高速デジタル伝送サービス。網内の伝送技術として ATM 技術が使われる。

B P L U S

米国の CompuServe で開発されたセンター主導のファイル転送プロトコル。クライアントプログラムの仕様はオープンだが、センター側のプログラムに関しては、ライセンスを受ける必要がある。

C C I T T

International Telegraph and Telephone Consultative Committee 国際電信電話諮問委員会。通信関連の工業規格を作成していた委員会で ITU (International Telecommunication Union 国際電気通信連合) の付属機関。ITU の組織組み替えにより ITU-T (Telecommunication Standardization Sector) と名称変更された。

C E R N

Conseil Europeenne la Recherche Nucleaire 欧州合同原子核研究機関。

C H A P

Challenge Handshake Authentication Protocol。P P Pにおける接続相手認証機能。

C R C

Cyclic Redundancy Check 巡回冗長性検査。エラー検出方式で、16ビット方式と32ビット方式がある。

D A R P A

Defence Advanced Research Projects Agency 米国国防総省高等研究計画局。

D I T

Digital Information Transmission。AFPとハッセルブラッド社が共同開発したデジタル画像電送プロトコル。現在のバージョンは3.2である。

D N S

Domain Name System。ネットワーク上の資源を統合管理するためのシステム。

D O D

Department of Defence 米国国防総省。

D S U

Digital Service Unit の略。回線終端装置。ISDN伝送路の終端。

E T Y P E

イーサネットヘッダー内にある上位プロトコルを識別するためのフィールド。

F C S

Frame Check Sequence。フレーム内のフィールドで、エラーを検出するために使用される。

F D D I

Fiber Distributed Data Interface。ANSIのX3T9.5で規格標準化が行われている通信の規格。光ファイバーを使用した100MbpsのLAN。

Firewall

防火壁。LAN環境でセキュリティーを確保するための手法。

F T P

File Transfer Protocol。T C P / I P 通信でのファイル転送のために使用するプロトコル。コマンドも同様に ftp となる。

F T A M

File Transfer, Access and Management。ネットワークでのファイル転送と共有のための I T U - T 標準。

Gopher

インターネットの情報にアクセスする手段をテキストのメニュー形式で提供するシステム。

H D L C

High level Data Link Control。従来から使用されているデータリンク層のプロトコル。高速回線用として使用されてきた。

H T M L

Hyper Text Markup Language。WWW で使用されているハイパーテキストを記述するための言語。

H T T P

Hyper Text Transfer Protocol。WWW で使用されるハイパーテキストを通信するためのプロトコル。

I C M P

Internet Control Message Protocol。I P レベルで発生した障害を繰り返し発生させないような情報通知や診断を行うプロトコル。

I E T F

Internet Engineering Task Force。インターネットに関する短期間の技術的問題を解決するためのグループ。

I N S

Information Network System 高度情報通信システム。N T T の I S D N サービス名。

I P

Internet Protocol。インターネットプロトコルの略。T C P / I P 通信でのネットワーク層に位置するプロトコル。

I P アドレス

32ビットからなるIP層でのアドレス。IPネットワークアドレスとIPホストアドレスからなる。32ビットをこの2つに配分する方法などにより、A、B、C、Dなどのクラスに分類される。

I P C P

Internet Protocol Control Protocol。PPPにおいて、IPパケットを転送する前にIPアドレス等のネゴシエーションを行う。

I P T C

International Press Telecommunication Council 国際新聞電気通信評議会。

I S D N

Integrated Services Digital Network サービス総合デジタル網。音声通信とデータ通信が混在可能な回線。G4ファックス、データ通信、テレビ会議など多様な用途に使われている。

I S O

International Standards Organization 国際標準化機構。工業関連分野の様々な標準化を行う国際機関。

I T U - T S

International Telecommunication Union-Telecommunication standardization Sector 国際電気通信連合電気通信標準化セクター。電気通信関連の研究や勧告の策定を行う。1993年にCCITTが組織改編されたことに伴い改称された。

J P N I C

Japan Network Information Center。日本におけるIPアドレスの割り当て管理機関。東京大学内に設置。

L A N

Local Area Network。1つ建物の中やキャンパスの敷地内など比較的狭い地域でのネットワーク。10～100Mbpsの伝送速度が一般的。

L A P D

Link Access Procedure on the D-channel。ISDN-Dチャンネル用データリンク層アクセスプロトコル。

TTC標準ではJT-Q921で規定。

L A P M

Link Access Procedure for Modems。C C I T T (現 I T U - T) 勧告 V . 4 2 で定義されているエラー訂正プロトコル。

L C P

Link Control Protocol。P P P で 2 点間のリンクを確立する作業を行う。

L Z W

Lempel-Ziv 法を Welch が改良した画像圧縮方法。ZMODEM で使用される他、U N I X で多く使われている。

M A C アドレス

L A N のハードウェアアドレスのこと。データリンク層で定義される機器自体の物理アドレス。

M N P

Microcom Network Protocol。米国 Microcom 社が開発したエラー訂正、圧縮方式。

Mosaic

インターネットで利用されている H T M L を簡便に利用できるブラウザソフトウェア。

N C P

Network Control Protocol。P P P で I P パケットを転送するためのプロトコル。

Net Ware

ノベル社のパソコン用のネットワーク O S。Net Ware 自体も I P X / S P X などの各種の packets 交換プロトコルからなるプロトコル体系、またはネットワーク体系とみることもできる。

N F S

サン・マイクロシステムズ社が開発した、ネットワーク上の資源 (ハードディスクなど) を共有するためのサービス。多くのメーカーがサポートしている。

N N T P

Network News Transfer Protocol。インターネットの Network News 記事を読み書きするプロトコル。

O S I

Open Systems Interconnection 開放型システム間相互接続。異機種間接続を実現する国際標準のプロトコル。T C P / I P に比べ普及が遅れている。

O S P F

Open Shortest Path First。リンクステート型のルーティングプロトコル。

P A P

Password Authentication Protocol。P P P における接続相手認証機能。

P D F

Portable Document Format。テキスト、写真、グラフィックスなどすべてのデータを包括できると言われているアドビシステムズ社が開発したフォーマット。

P D S

Public Domain Software。PDS は、皆が無料で自由に利用できるソフトウェア。インターネット上にはたくさんの anonymous FTP が動いており、そこに有益なソフトウェアが PDS として存在している。

P H S

Personal Handyphone System。1995 年 7 月からサービスが開始される簡易携帯電話システム。

P P P

Point to Point Protocol。インターネット通信におけるデータリンク層での二点間のリンク確立、切断に関する標準プロトコル。異機種同士の接続が、この P P P により容易になった。

Proxy A R P

I P ルーターを認識できないノードも通信に参加させるため、I P ルーターが A R P リクエストに対して代理でレスポンスを返送するためのプロトコル（サービス）。

P S T N

Public Switched Telephone Network 公衆電話網。

R A R P

Reverse ARP。ARP と逆でハードウェアアドレスから、I P アドレスを知るためのプロトコル。

R F C

Request for Comments。T C P / I P 通信でのさまざまな取り決めやアイデアを、広く公表するためのもの。T C P / I P 通信プロトコルの仕様などが記述されている。

R I P

Routing Information Protocol。ディスタンスベクター型のルーティングプロトコル。

R L E

Run Length Encoding。米国オーメンテクノロジー社が著作権を持っているランレングス圧縮方式。送信するファイルを圧縮し、転送時間を短縮する。

S L I P

Serial Line IP。インターネットワーキング用に業界標準として広まったデータリンク層のプロトコル。現在では、P P P に取ってかわられている。

S M T P

Simple Mail Transfer Protocol。T C P / I P 通信上で電子メールを受け渡しするプロトコル。

S N M P

Simple Network Management Protocol。T C P / I P 上でのネットワーク管理プロトコル。

T A

Terminal Adapter ターミナルアダプター。コンピューターを ISDN 回線に接続するためにプロトコルを変換する装置。

T E

Terminal Equipment。ISDN 網に接続するユーザー装置。ISDN 標準端末が TE1、非標準端末が TE2。

T C P

Transmission Control Protocol。I P の上位に位置するトランスポート層プロトコル。コネクション型のプロトコルで、送達確認など信頼性が考慮されている。

T C P / I P

Transmission Control Protocol / Internet Protocol。T C P / I P と表記した場合、T C P と I P という2つのプロトコルのみでなく、I P プロトコル上で実現する全てのプロトコル群、通信サービスを指す。

T E L N E T

T C P / I P 通信での仮想端末プロトコル。コマンドも同様に telnet になる。

T O S

Type of Service。I P ヘッダー内の T O S フィールド。サービスタイプに情報を組み込むことにより、パケットの優先順位などが判断できるようになる。

T T C

Telecommunication Technology Committee の略。日本国内の電気通信関連の標準化委員会

U D P

User Datagram Protocol。トランスポート層に相当する機能を持つプロトコル。コネクションレスでの通信を行う。

U R L

Uniform Resource Locator。インターネット上の資源を統一的に記述するための記法。

V シリーズ勧告

ITU-T が有線通信の技術基準、運用規則の標準を定め、電話網などにおいてデータ通信に使用される装置、伝送方式を標準化した勧告。

W A I S

World Area Information Servers。インターネットの情報にアクセスする手段を提供するシステム。

W A N

Wide Area Network。L A N に比べて広い地域をカバーするネットワーク。離れた地点にある L A N 同士を、電話回線、専用回線、I S D N などを利用して接続する。

W W W

World Wide Web。インターネット上の情報をハイパーテキスト化して提供するソフトウェア。

X . 2 5

パケット交換網と端末とのインターフェースに関する C C I T T 勧告 (I T U - T 勧告)。論理的な手順、論理的な構造をいう。

X M O D E M

ファイル転送プロトコル。標準的には 128 バイトのデータを送る度に誤り訂正を行う。

Y M O D E M

ファイル転送プロトコル。1024 バイト単位に CRC チェックを行う。ファイル名や作成日付などのデータも転送する。

Z M O D E M

米国オーメンテクノロジー社が開発したファイル転送プロトコル。XMODEM、YMODEM を改良したもので、アナログ公衆回線上でモデムを使用して効率良くファイルを転送する。

あとがき

4年にわたる標準化作業は、日本新聞協会加盟の新聞・通信社が、相互に写真データを送受信できる共通のフォーマットとプロトコルの作成を目的として、現在まで継続してきた。1994年5月のNSK T I F F策定に続き、今回の推奨プロトコルで初期の目的は達成された。

技術開発分野で、新聞・通信各社は独自の路線を進めてきた。今回の標準化作業はその意味で画期的と言える。新聞・通信社側委員とメーカー技術者による調査、研究、調整には多大の時間と労力が費やされた。細部の決定では各社のデータを公開しあって検討を進めた。

プロトコルの決定にあたっては、H D L C系かT C P / I P系かの選択肢があったが、協会加盟各社の粘り強い話し合いや実現への熱意、参加メーカー各社の枠を越えた協力により問題点を解決してきた。マルチメディア時代を迎え、標準化への強い要求がユーザー、メーカーという異なる立場の障害を越えた協力を生み出したと言える。

標準化の第一歩は踏み出した。今後は、NSK T I F FとNSKプロトコルの新聞協会加盟各社での普及と安定した運用を図ることが急務である。編集サイドからの要望の強い代表取材での同報送信の実現が望まれる。同時に、新しい通信メディアの登場やハード・ソフトウェア技術の急速な展開を見据えた次世代のフォーマット、プロトコルへの取り組みも必要となろう。

インターネット、情報スーパーハイウエー、フレームリレーサービス、A T Mサービスなどマルチメディアを巡る話題は尽きない。動画と音声を含む電子新聞の研究も急ピッチで進んでいる。グラフィックスの対応も急がれるが、米国ではニュースグラフィックスの配信にP D Fの採用が具体化している。

街中で使用するP H S、さらに、世界の何処からでもアクセスできる低高度衛星計画など移動体通信の実現も近い。

新しい技術やサービスへの早い対応が、NSK T I F FとNSKプロトコルの普及、発展への重要な要素となろう。

目 次

はじめに	2
「NSKプロトコル」改訂にあたって	3
履 歴	4
第1章 NSKプロトコルの概要	5
1.1. NSKプロトコルの基本方針と策定経緯	6
1.2. NSKプロトコルの概要	8
第2章 アナログ公衆回線での推奨プロトコル	15
2.1. 適応モデム技術	16
2.2. ZMODEMプロトコルの機能	21
2.3. オプション機能使用規定	29
2.4. 回線接続と運用方法	32
第3章 デジタル公衆回線での推奨プロトコル	35
3.1. 適用ハードウェア技術	36
3.2. PPP	48
3.3. TCP/IP	56
3.4. FTPと関連アプリケーション	64
3.5. セキュリティー技術	75
3.6. 関連するRFCの一覧	78
第4章 NSK TIFFとNSKプロトコルの運用管理方法	79
4.1. 運用管理組織と規定	80
4.2. NSKプロトコル運用の参考例	81
4.3. NSK写真電送の応用例	83
コラム 取材無線とデジタル写真電送	84
第5章 NSK TIFFとNSKプロトコルの展望	85
5.1. NSK TIFFとマルチメディア	86
5.2. NSKプロトコルをめぐる動向	87
5.3. 今後の課題	89
付録A. 策定組織とメンバー	91
1. 策定組織と関係組織	91
2. 社団法人日本新聞協会 技術委員会組織図	92
3. 策定方法ならびにNSKプロトコル策定メンバー	93
付録B. 参考文献一覧	95
付録C. 関連用語一覧	96
五十音順関連用語一覧	96
アルファベット順関連用語一覧	101
あとがき	110