ネットワーク･プロトコルについて（入門）

≪ パソ救・勉強会資料の作成のための準備資料 ≫

2012(H24).8.2.　*T.Ogawa*

本資料は、2012(H24).9.23 に開催するパソ救・勉強会用の資料として作り始めたものであるが、43 ページと大きくなり過ぎたので自己学習用の資料とすることにした。

本資料を基にコンパクト化して、20 ページ前後の「ネットワーク・プロトコルの概要」として勉強会用資料を作成することとする。

目次

1.　ネットワークアーキテクチャ

コンピュータ、端末、通信ネットワークなどの要素からなる通信システムにおいて，各要素の接続条件や、要素間を通信する場合の約束（プロトコル）を体系的に定めたものを「ネットワークアーキテクチャ（Network Architecture）」と言いう。

1.1.　ネットワーク･アーキテクチャの乱立と OSI

筆者が 1971 年から 3 年間担当した全銀システム（都銀、上位地銀の為替交換システム）は各行の勘定系システムを接続する日本初の異機種コンピュータ間の相互接続システムであり、各行のコンピュータ間にミニコンピュータを置き個別のプロトコル変換ソフトを開発した。このように 1990 頃までは、各社が独自のネットワーク･アーキテクチャ（※1）（IBM の SNA、富士通の FNA、日立の HNA、日電の DINA、電電公社の DCNA 等）を構築していたので、異なるメーカのコンピュータを相互接続するのは困難であった。

これを解決するため、ISO（※1）と ITU-T（※2）が 1982（S57）に共同プロジェクトを立ち上げ、異なるメーカ間で相互接続を行うための OSI（※3）プロトコルの策定に取り組んだ。

（※１）ＩＳＯ（International Organization for Standardization：国際標準化機構）
なお ISO 電気分野を除いた国際規格を策定）

（※２）ＩＴＵ-Ｔ（International Telecommunication Union Telecommunication Standardization：国連にある国際電気通信連合の電気通信標準化部門）

（※３）ＯＳＩ（Open System Interconnection：開放型システム間相互接続）

1.2.　OSI 参照モデルについて

OSI の策定プロジェクトは 1996（H8）に解散したが、その中で OSI 参照モデル（※1）が策定され、1984（S59）に ITU-T で承認された。

しかし OSI 策定プロジェクトが自前主義であったため、ボランティア技術者がインターネット上で ＲＦＣ（※2）文書としてプロトコルを決めてゆく ＩＥＴＦ（※3）との間で論争が生じた。

こうした中で、IETF が推進する TCP/IP が 1983（S53）にはインターネットの起源である ARPANET（※4）の標準プロトコルに採用され、UNIX 系の LAN にも採用された。

TCP/IP は、1988（S63）の米国での商用インターネットの開始、Mac への搭載、1995（H7）の Windows 95 への搭載を経て、インターネットの標準プロトコルとなった。こうしてインターネットで不動の地位を得た TCP/IP プロトコルは、OSI の役目をも奪ってデファクトスタンダード（※5）のネットワークアーキテクチャになった。

OSI プロトコルは、TCP/IP プロトコルに押され色あせてしまったが、OSI プロジェクトで策定された「OSI 参照モデル」はネットワークアーキテクチャを体系的に説明／理解する標準的なモデルとして現在も使い続けられている。

（※１）OSI 参照モデルは、通信機能を 7 つの階層に分け定義したプロトコルの階層モデル

（※２）RFC（Request For Comment）は、TCP/IP の仕様・要件をメーリングリストで提案（Request）し、意見（Comment）を得ながらプロトコルを策定する方式を言い、その際に文書に付与される管理番号を RFC 番号と言う。

（※３）IETF（Internet Engineering Task Force）は、民間のインターネット技術標準化団体であり、メーリングリストに登録された個人ボランティアで構成され、テーマ毎の WG に分かれて論議している。

（※４）ARPANET は、米国防省・高等研究計画局がパケット通信実験用ネットとして開発した世界初の異機種コンピュータ･ネットワークであり、これがインターネットの母体となった。

（※５）デファクトスタンダード（de facto：ラテン語で「事実上の」）とは、国際機関や標準化機関による公的な標準ではなく、市場の実勢や学問上の評価などによって「結果として事実上の標準になった規格」のことを言う。例としては、VHS ビデオ、Blu-ray、SD メモリ、TCP/IP 等がある。

OSI 参照モデルにおけるプロトコルの階層

階層	階層（レイヤ）名	階層が分担する通信機能
第７層	アプリケーション層 （Application Layer）	ユーザが利用するアプリケーションソフトに関する取り決め。 ・送信元と宛先のアプリケーション間でのデータのやり取り（（サービス機能、動作手順、データ種類、データ構造等）を規定する。
第６層	プレゼンテーション層 （Presentation Layer）	アプリケーションで扱うデータ形式（文字コード、数値表現等）と通信が扱う共通のデータ形式を相互に変換するための取り決め。 ・相手コンピュータとの間でやりとりするデータの表現方法（文字コード変換、数値表現等）、符号化、暗号化等を規定する。
第５層	セッション層 （Session Layer）	アプリケーション間の通信において、相手コンピュータとの接続状態を制御し管理するための取り決め。 ・相手アプリケーションとの間で行う通信の開始から終了までの一連の手順（接続の確立／解放／切断、中断／再開、全二重通信／半二重通信等）を規定する。
第４層	トランスポート層 （Transport Layer）	ネットワーク層以下で伝送されるデータが確実に相手コンピュータに届いていることを保証するための取り決め。 ・上位層から渡されたたデータのセグメント分割、下位層から受け取った分割データの組み立て復元についてきていする ・コネクション制御、データエラー制御、データ欠落制御、フォロー制御等について規定する
第３層	ネットワーク層 （Network Layer）	送信元ノード（※6）から宛先ノードまでルータ（※7）を経由して、データを伝送するための取り決め。 ・複数種類のデータリンク層の仕様の違いを吸収し、送信元ノードと宛先ノードとの間にある複数のネットワークを経路選択して送信元ノードと宛先ノードとの間で行うパケット通信を規定する
第２層	データリンク層 （Datalink Layer）	通信媒体（電線、光ケーブル、無線等）で直接つながっているノード間でデータを伝送するための取り決め。 ・隣接するノード間のデータのパケット化、物理的ノードアドレス、パケットの送受信方法、接続形態等を規定する。

第１層	物理層 （Physical Layer）	通信媒体に応じた信号の種類・内容やデータの伝送方法に関する取り決め。 ・物理的な接続のための物理的な電気信号、符号の変調方法等を規定（例：コネクタ、ケーブル、電圧、変調等、周波数、波形、変調、電波強度、暗号化等）を規定する。通常は第２層のデータリンク層の仕様と共に既定する場合が多い。

（※６）ノード（Node）は、英語で節や集合点を意味し、通信ネットワークではネットワークを構成する一台一台の通信機器（コンピュータ、スイッチングハブ、ルータ等）を言う。

（※７）ルータ（Router）とは、複数の LAN 同士や LAN とインターネットを相互に接続して、ノード同士が通信できるように IP パケットのやりとりを可能にする中継装置を言う。

1.3. インターネット･プロトコル･スイート（TCP/IP）

インターネットの爆発的な普及に伴って､インターネットで使用されているインターネット･プロトコル･スイート（Internet protocol suite）は他の多くの商用ネットワークにも採用されるようになった。

インターネット･プロトコル･スイートは TCP と IP を中核とした通信プロトコルの一式であり、インターネットの初期から使われている TCP と IP にちなんで TCP/IP プロトコル･スイート（以下､TCP/ IP プロトコルという）とも呼ばれている。

次表に、OSI 参照モデルと TCP/IP プロトコルの階層を対比する。

【OSI 参照モデルの 7 階層と TCP/IP プロトコルの 4 階層の対応】

OSI 参照モデルの階層		TCP/IP プロトコルの階層	
第７層	アプリケーション層	第４層	アプリケーション層
第６層	プレゼンテーション層		
第５層	セッション層		
第４層	トランスポート層	第３層	トランスポート層
第３層	ネットワーク層	第２層	インターネット層
第２層	データリンク層	第１層	リンク層（ネットワークインタフェース層）
第１層	物理層		

TCP/IP プロトコルは、おおよそ次の 4 階層のプロトコル群に分類できるが、OSI 参照モデルのように明確に定義されたものではなく、例えば第１層の名称でさえも「リンク層」あるいは「ネットワーク・インタフェース層」と複数の呼び名がある。

OSI 参照モデルと TCP/IP プロトコルは、関連のない組織で別々に策定されたので説明者や筆者により異なった階層分類がなされることがある。

また、TCP/IP プロトコルを構成するプロトコルは必要の都度、提案され論議されて標準化されるので、プロトコルの階層と個々のプロトコルとの結びつきも厳格なものではない。

2.　プロトコル階層化とカプセル化

ネットワークアーキテクチャにおけるカプセル化（Encapsulation（インカプセレーション））とは、送信側の各階層で上位層から渡されたデータの前後に下位層のプロトコルで規定された情報（ヘッダ、トレーラ）を付加して包み込むことを言う。

逆に受信側の各階層は、付加された情報（ヘッダ、トレーラ）を参照し包み込まれたデータを取り出して上位層に渡して行き、最終的にアプリケーション層にデータを転送する。これをカプセル化解除（カ非プセル化、逆カプセル化等）という。

ここでは、TCP/IP プロトコルを例にしてカプセル化の流れを説明する。

2.1. カプセル化とカプセル化解除の流れ

１）送信元コンピュータでのカプセル化の流れ

① アプリケーション（第 4 層）は、アプリケーションデータを下位層（TCP）に渡す。

② TCP（第 3 層）は、上位層（アプリケーション）から受け取ったアプリケーションデータを経路 MTU 探索で得た MSS（最大セグメントサイズ）単位に分割した後、それぞれの分割データの前に TCP ヘッダを付加して TCP セグメントを編成し、TCP セグメント単位に下位層（IP）に渡す。

③ IP（第 2 層）は、上位層（TCP）から受け取った TCP セグメントの前に IP ヘッダを付加して IP パケットを編成し、下位層（イーサネット）に渡す。

④ イーサネット（第 1 層）は、上位層（IP）から受け取った IP パケットの前にイーサネットヘッダを付加し、後ろに FCS（Frame Check Sequence（フレーム チェック シーケンス）：伝送エラーチェック情報）を付加してイーサネットフレームとして下位層（通信ネットワーク）に送信する。

２）宛先コンピュータでのカプセル化解除の流れ

① イーサネット（第 1 層）は、下位層（通信ネットワーク）から受信したイーサネットフレームのイーサネットフヘッダを参照し、既定の処理を行った後、IP パケットを取り出して上位層（IP）に渡す。

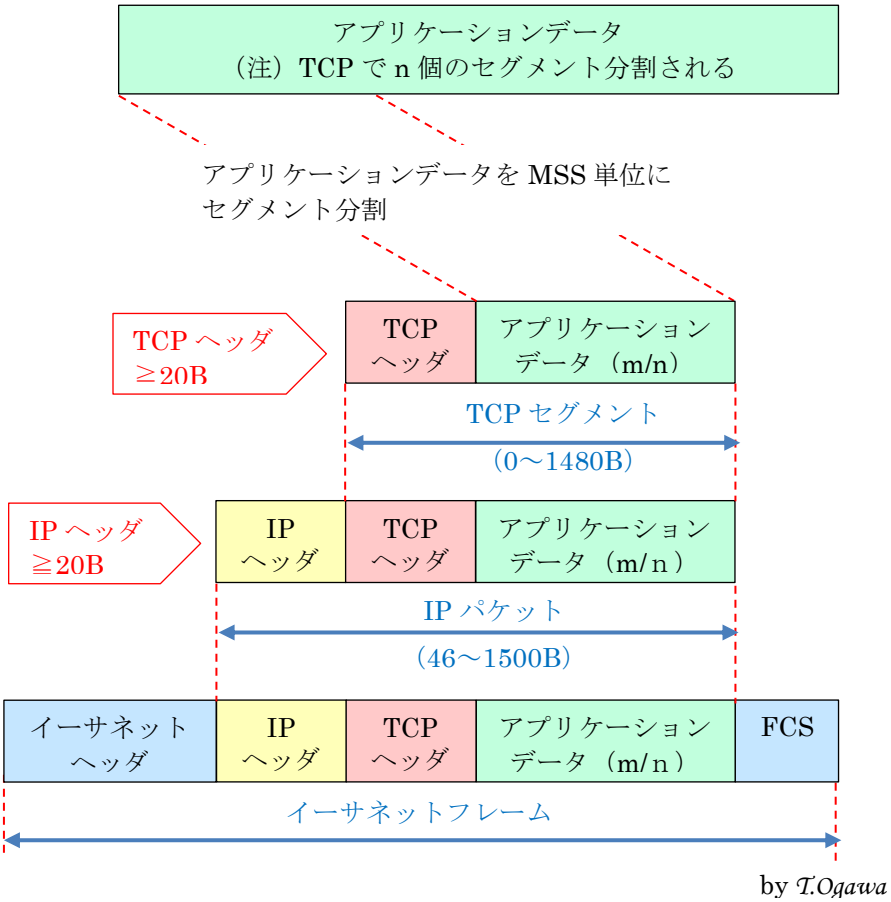
② IP（第 2 層）は、下位層（イーサネット）から受け取った IP パケットの IP ヘッダを参照し、既定の処理を行った後、TCP セグメントを取り出して上位層（TCP）に渡す。

③ TCP（第 3 層）は、下位層（IP）から受け取った TCP セグメントの TCP ヘッダを参照し、既定の処理を行った後、別々に届いた分割データを組み立て直し元のアプリケーションデータを復元して上位層（アプリケーション）に渡す。

④ アプリケーション（第 4 層）は、下位層（TCP）から受け取ったアプリケーションデータを処理する。

2.2. カプセル化のイメージ

TCP/IP プロトコルにおける各階層でのカプセル化のイメージは下図のとおりであり、各階層でプロトコルに規定した情報（ヘッダ、トレーラ）を付加して順次下位層に渡して行く。



by *T.Ogawa*

3. TCP/IP プロトコルの主なプロトコル

ここでは、TCP/IP プロトコルの各階層の主なプロトコルの内、次表に**赤字**で表示したプロトコルについて説明する。

【TCP/IP プロトコルの階層（4 階層）**】**

階層	階層（レイヤ）名	各階層の主なプロトコル
第４層	アプリケーション層	BGP、DHCP、DNS、FTP、HTTP、IMAP、IRC、LDAP、MGCP, NNTP、NTP、POP、RIP、RPC、RTP、SIP、SMTP、SNMP、SSH、Telnet、TFTP、TLS/SSL、XMPP
第３層	トランスポート層	TCP、UDP、DCCP、SCPT、RSVP、ECN
第２層	インターネット層	IP（IPv4、IPv6）、ICMP、ICMPv6、IGMP、IPsec
第１層	リンク層（ネットワーク・インタフェース層）	ARP、NDP、OSPF、L2TP（トンネリング）、PPP、MAC（イーサネット、IEEE802.11、DSL、ISDN、FDDI）

3.1. 各階層の主なプロトコル

1）第 4 層 アプリケーション層の主なプロトコル

TCP/IP プロトコルのアプリケーション層（第 4 層）は、おおよそ OSI 参照モデルの上位 3 層（第 7 層のアプリケーション層、第 6 層のプレゼンテーション層、第 5 層のセッション層）を一体化した階層である。

送信元コンピュータの第 4 層のアプリケーションは、転送するデータを下位のトランスポート（例：TCP）に渡して送信依頼し、宛先コンピュータの第 4 層のアプリケーションは下位層のトランスポート層（同）から受信データを受け取り既定の処理を行う。

【表の説明】次表の［備考］欄の上段はプロトコルの RFC 番号（公開仕様の管理番号）、中段の数字は対応アプリケーションのポート番号（複数ポートの場合がある）、下段はトランスポート層の対応プロトコル

名称	プロトコルのフルネイムと概要	備考
エッチティーティーピー H T T P	ハイパーテキスト トランスファー プロトコル Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル） HTTP は、クライアント（※1）とウェブ Web（※2）サーバ（※3）間でデータの転送を行うプロトコルであり、Web ページを閲覧する取り決めである。 インターネット全盛の現在、最もよく使われているアプリケーションであり、クライアントのアプリケーションを Web ブラウザと呼んでいる。 HTTP では、クライアントから Web サーバに「リクエスト」を送信し、Web サーバは「レスポンス」をクライアントに転送する ・ 「リクエスト」には、指定するデータの転送要求、指定宛先へのデータ送信等がある ・ 「レスポンス」で転送するデータには、ハイパーテキスト（※4）（HTML、XML）、画像、動画、音声等がある （参考）Web ブラウザには、Internet Explorer、Google Chrome 等があり、これらは Web メール機能として後述の SMPT、IMAP 等のプロトコルも実装している。	RFC2616 80 TCP
エスエムティーピー S M T P	シンプル メール トランスファー プロトコル Simple Mail Transfer Protocol（簡易メール転送プロトコル） SMPT は、クライアントから宛先メールサーバのメールボックスにメールを転送するプロトコルである。 クライアントは送信メールをメールサーバに転送し、メールを受け付けたメールサーバはそれを宛先メールサーバに転送する。 転送を受けた宛先メールサーバはメールをメールボックスに振り分ける。 ・ メール ユーザ エージェント Mail User Agentで、クライアントからサーバへメールを転送する ・ メール トランスファ エージェント Mail Transfer Agentで、メールサーバ間でメールを転送する ・ メール デリバリ エージェント Mail Delivery Agentで、メールボックスにメールを振り分ける （参考）SMPT の MUA を実装した身近なアプリケーションとして、Windows Live メール、Outlook Express 等がある	RFC5321 25 TCP

ポップスリー POP 3	ポスト オフィス プロトコル バージョン Post Office Protocol Version 3（メール受信プロトコル Ver.3 ） POP3 は、メールボックスに配信されたメールをクライアントが取り出して取り込むプロトコルである。 ・ クライアントがメールを取り出すと、該当メールはメールボックスから削除される （注）POP、POP2、POP3 があり、最新の POP3 を POP とも呼ぶ （参考）POP3 を実装した身近なアプリケーションとして、Windows Live メール、Outlook Express 等がある	RFC1939 110 TCP
アイマップ IMAP	インターネット メイル アクセス プロトコル Internet Mail Access Protocol（インターネットメッセージアクセスプロトコル） IMAP、は宛先メールボックスに振り分けられたメールに、クライアントがアクセスし操作するプロトコルである。 ・ メールボックスのメールを読み込んでクライアントにコピーを保存できる ・ メールボックスにあるメールの管理（削除、フラグ付加等）はクライアントが行う （注）最新版は IMAP4（IMAP バージョン 4）である	RFC3501 143 TCP
エフティーピー F T P	ファイル トランスポート プロトコル File Transport Protocol（ファイル転送プロトコル） FTP は、クライアントとサーバ間でファイルを転送するプロトコルである。 クライアントが制御用ポートを用いてログイン（ID、パスワード）した後、「コマンド」を送信して制御しながら、サーバのデータ用ポートを使用してテータを転送する ・ 複数ファイルを転送する場合は、ファイル毎にテータ転送用のコネクションを確立する ・ 「コマンド」には、ディレクトリ移動、データタイプ指定、ファイル取得、ファイル書き込み、ファイル削除、転送中断等がある （参考）身近なアプリケーションとして、フリーソフトの FFTP がある。	RFC959 20（データ） 21（制御） TCP
ディーエヌエス D N S	ドメイン ネーム システム Domain Name System（ドメイン名／IP アドレス変換プロトコル） DNS は、インターネットを用いた階層的な分散型データベースであり、ドメイン名と IP アドレスと (※5) の対応付けに使用する。 ・ ドメイン名→IP アドレス（正引き）、IP アドレス→ドメイン名（逆引き）の変換を行う DNS サーバ (※6) ・ DNS はオーバーヘッドの少ない UDP を使用できるように、問合せ／応答メッセージを 512B 以内に制限し 1 パケット伝送を実現している。	RFC1034、 RFC1035 53 UDP、TCP

ディーエッチシーピー D H C P	ダイナミック ホスト コンフィグレーション プロトコル Dynamic Host Configuration Protocol（接続情報割り当てプロトコル） DHCP は、一時的にネットワークに接続するコンピュータに対して、接続に必要な情報を自動的に割り当てるプロトコルである。 接続を希望する DHCP クライアントからの要求に DHCP サーバが設定情報を通知し、更に DHCP クライアントの設定要求に対して設定許可を与えて接続を可能にする ・ DHCP が割り当てる情報には、IP アドレス、サブネットマスク（※7）、デフォルトゲートウェイ（※8）IP アドレス、DNS サーバ IP アドレス等がある ・ ブロードバンドルータ（ADSL モデム、フレッツ光の CTU 等）、無線ルータ等は DHCP 機能を内蔵している ・ IPv6 用に DHCPv6（RFC3315）が規定されている	RFC2131 67（Server） 68（Client） UDP

（※１）クライアントとは、サーバが提供する機能やデータを利用するコンピュータを言う。

（※２）Web は、ワールド ワイド ウエブ World Wide Webの略であり、WWW または ダブリュスリー W 3 とも呼ばれる。インターネット上で提供されるハイパーテキスト･システムを言う。

（※３）サーバとは、クライアントに対して自分が持っている機能やデータを提供するコンピュータを言う。

（※４）ハイパーテキスト（Hypertext）とは、複数の文書（テキスト）を相互に関連付け、結びつける仕組みを言う。

（※５）IP アドレスは、ネットワーク上の機器を識別するためのネットワーク層における識別番号である。
グローバル IP アドレスは、世界的な管理の下で割り当てられるので同一番号がない。
所属 LAN 内だけで使用する IP アドレスをローカル IP アドレスと言い、168.192.0.0～192.255.225 を割り当てる。

（※６）DNS サーバは、ルート DNS サーバ、トップレベル DNS サーバ、第 2 レベル DNS サーバ、第 3 レベル DNS サーバに階層化されたツリー構造になっている。

（※７）サブネットマスク（サブネット マスク Subnet mask）は、IP アドレスからネットワークアドレス部とホストアドレス部を分離するための鍵になる値であり、IP アドレスとサブネットマスクとを AND 演算し、前 24bit（3B）がネットワークアドレス部、後 8bit（1B）がホストアドレス部である。そしてネットマスクの後部の連続した“0”の bit を“1”に読み替えた［2 進数－2］が最大の IP アドレス数である。

（※８）デフォルトゲートウェイとは、所属 LAN の外にあるコンピュータにアクセスする際に出入り口になるポートを言う。

2）第 3 層 トランスポート層の主なプロトコル

TCP/IP プロトコルのトランスポート層（第 3 層）は、OSI 参照モデルのトランスポート層（第 4 層）に相当する。

トランスポート層の主なプロトコルには､コネクション型の TCP とコネクションレス型の UDP がある。

名称	プロトコルのフルネイムと概要	備考
ティーシーピー T C P	トランスポート コントロール プロトコル Transport Control Protocol（伝送制御プルとコル） TCP は、信頼性を重視したコネクション型のデータ伝送プロトコルであり、TCP/IP プロトコルの中核となるプロトコルである。 宛先コンピュータとのコネクションの確立、データ到着の確認、フロー制御、データの重複や抜けの検出などを行うことで信頼性の高い通信を実現する。 ・ 通信相手とコネクションを確立（接続要求送信→確認応答＆接続要求受信→確認応答送信）してから通信を開始する。 ・ データ伝送が終了したらコネクションを開放（切断要求送信→切断応答受信）する ・ 送信側 TCP は、アプリケーションから渡されたデータを最大セグメントサイズ（※1）単位に分割し、分割されたデータの前に TCP ヘッダを付加して TCP セグメントとして下位の IP に渡す ・ 受信側 TCP は、下位の IP から渡された TCP セグメントの TCP ヘッダを基にして、重複／欠落の検査と再送制御、セグメント到着乱れの修正等の制御を行って、元のデータに組み立てた後、指定されたアプリケーションに渡す （参考）TCP を使用する主なアプリケーション層のプロトコルには、HTTP、FTP、SMTP、POP 等がある。	RFC793
ユーディーピー U D P	ユーザ データグラム プロトコル User Datagram Protocol（無手順型のデータ伝送プロトコル） UDP は、高速性を重視したコネクションレス型のデータ転送プロトコルである。コネクションの確立、データ到着の確認、データの再送等の機能がなく信頼性にやや難点がある。逆に、信頼性確保の機能がなく処理が速いため、データが僅かに欠けることよりも連続的なデータの取得が重視されるストリーミング・データ処理などでは、UDP が用いられる場合が多い。 （参考）UDP を使用する主なアプリケーション層のプロトコルには、DNS、DHCP、TFTP、NPT 等がある。	RFC768

（※1）最大セグメントサイズ（エムエスエス マクシマム セグメント サイズ ＭＳＳ＝Maximum Segment Size）とは、送信元～宛先の間にある全てのルータが、IP パットを分割せずに転送できる最大のセグメントサイズを言う。
この MSS はパス エムティユー ディスカバリ Path ＭＴＵ Discovery（経路 MTU 探索、RFC1191）機能を用いて経路 MTU（送信元～宛先の最小 MTU）を調べ、それを基に算出する。

3）第 2 層 インターネット層の主なプロトコル

TCP/IP プロトコルのインターネット層（第 2 層、ネットワーク層ともいう）は、OSI 参照モデルのネットワーク層（第 3 層）に相当する。

名称	プロトコルのフルネイムと概要	備考
アイピー ＩＰ	インターネット プロトコル Internet Protocol（インターネットプロトコル） IP は、End to End（送信元～宛先）をパケット単位でデータ交換するプロトコルであり、TCP/IP プロトコルの中核となるプロトコルである。 IP では、ルータを用いて異なる LAN（セグメント）同士を論理的に相互接続して WAN を構成し IP パケットをバケツリレー式に宛先まで伝送する。 ・ IP はコンピュータやルータ内で、次の役割を果たしている ✧ ルーティング（経路選択）機能で、IP アドレスを用いて IP パケットの転送先 (※1) を決める ✧ 生存時間（TTL）機能で、ルータの中継回数をカウントして、ループ状態と疑わしい IP パケットを検知し破棄 (※2) する ✧ フラグメント（パケット分割）機能で、必要に応じて IP パケットを分割 (※3) して次の経路を通過させる ✧ ヘッダ検査（Header Checksum）機能で、ヘッダが破損した IP パケットを破棄 (※4) する ✧ プロトコル番号 (※5) を基に、上位プロトコル（例：TCP）に受信パケットを引き渡す ・ IP には、IPv4、(※6) と IPv6 (※7) の 2 種類（3.2 節参照）があり、 IPv4 は 2011 年の春～初夏に IP アドレスをほぼ枯渇したと言われている。 【追記】本資料を執筆中の今日（2012/6/6）は、World IPv6 Launch（世界の IPv6 開始）と呼ばれる日であり、世界中の大手 Web サイトやプロバイダが一斉に IPv6 への対応を開始する日である。 対応が完了する日は予測できない（その間は IPv4 と IPv6 が共存）。	RFC791 （IPv4） RFC2460 （IPv6）
アイシーエムピー ＩＣＭＰ	インターネット コントロール メッセージ プロトコル Internet Control Message Protocol（インターネット制御メッセージプロトコル） ICMP は、IP アドレスで指定した宛先との間で制御メッセージやエラーメッセージを転送する IP の補助的なプロトコルである。 なお IMPC は、ICMP メッセージ（制御メッセージ、エラーメッセージ）を IP パケット化して転送するので、ネットワーク層で動作しているが、正確にはネットワーク層（IP）の上位のプロトコルともいえる。 ・ 制御メッセージには、エコー応答、エコー要求、経路変更通知等がある。 ・ エラーメッセージには、到達不能、パケット放棄、宛先不明、時間超過などがある。 ・ ICMP には、IPv4 用の ICMPv4 と IPv6 用の ICMPv6 がある。 （参考）DOS コマンドの ping コマンド、traceroute コマンド等が ICMP を利用している	RFC792 （ICMPv4） RFC4443 (ICMPv6)

（※１）宛先 IP アドレスが所属 LAN 内にある場合には直接転送し、所属 LAN 内にない場合はデフォルトゲートウェイとして設定されているポートに転送する。

なお、「宛先 IP アドレスが所属 LAN 内」にあるかどうかの判断は、サブネットマスク（例：255.255.255.0）と自 IP アドレス（例：192.168.24.51）との AND（例：192.168.24.0）を求め、宛先 IP アドレスが 192.168.0～192.168.255 の範囲にあれば所属 LAN 内と判断する。

（※２） IP パケットが無限ループに陥ってターネットがパンク状態になるのを回避する対策である。正常な場合には、ルータ間を 100 回以上中継されるケースはないらしい。

IP ヘッダの TTL にパケットが通過できるルータ数（例：255、128）を設定して送信し、ルータを通過するごとに減算して 0 になったらパケットを破棄すると共に、破棄を送信元に通知する。：

（※３） 従来は、経路上にある各ルータの IP は、次の経路の MTU（Maximum Transmission Unit：最大転送単位）に合わせて IP パケットを分割しながら中継していたためルータの負荷が増して転送効率が低下していた。

近年では、Path MTU Discovery（経路 MTU 探索、RFC1191）機能を用いて経路 MTU（送信元～宛先の最小 MTU）を調べ、MSS（Maximum Segment Size：最大セグメントサイズ）を算出して、TCP がデータをセグメント分割して IP に渡すのでパケット分割が減少した。

（※４）IP パケットのデータ部の検査は上位プロトコル（例：TCP）に任せて、IP の責任部分である IP ヘッダを検査し異常があれば IP パケットを破棄する。なお IP ヘッダ異常時には破棄通知は行わない。（Header Checksum、ヘッダ検査情報）

（※５）プロトコル番号には、TCP＝1 番、UDP＝17 番、ICMP=1 番等がある。

（※６）IPv4 は IP アドレスの表示に 4B（32bit）を用いて、約 43 億個の IP アドレス空間を管理できる。

なお、IPv4 の IP アドレスは 1B（8bit）毎に 4 分割し、10 進数（0～255）に変換してピリオド“ . ”で区切って表示する。（例：225.49.0.183）

（※７）IPv6 は IP アドレスの表示に 16B（128bit）を用いて、ほぼ無限（約 340 兆個の 1 兆倍の 1 兆倍）の IP アドレス空間を管理できる。

なお、IPv6 の IP アドレスは 2B（16bit）毎に 8 分割し、16 進数（0～FFFF）に変換して、コロン“ : ”で区切って表示する。（例：2001:0DB8:0:CD30:1F3:A56C:89AB:CFBE）

4）第１層 リンク（ネットワークインタフェース）層の主なプロトコル

TCP/IP プロトコルのリンク層（第 1 層、ネットワークインタフェース層ともいう）は、OSI 参照モデルのデータリンク層（第 2 層）に相当する。

名称	プロトコルのフルネイムと概要	備考
イーサネット	Ethernet（イーサネット）（※1）は、IEEE802.3 として標準化された LAN であり、物理層の CSMA/CD（シーエスエムエー シーディー）（※2）とリンク層の MAC（マック）（※3）フレームに関するプロトコルを規定している。 イーサネットは、TCP/IP が扱う MAC フレームを規定することから、最も普及したリンク層のプロトコルと言える。	IEEE 規格は RFC と無関係
PPP（ピーピーピー）	Point to Point Protocol（ポイント トゥ ポイント プロトコル）（2 点間通信プロトコル） PPP は、通信回線を挟んだ 2 つのコンピュータ間でデータ通信を行うためのデータリンク層（MAC 層）のプロトコルである。 PPP は、電話回線、ISDN 等のダイアルアップ接続で使用されている。 ・ LCP（エルシーピー）（※4）（リンク制御プロトコル）で、2 点間のリンクの確立、維持、解放を行う ✧ 最大受信単位（MRU）その他を調整・設定する ✧ LCP でのリンクの確立後に、オプションの PAP（パップ）（※5）、CHAP（チャップ）（※6）で、ユーザ認証（ユーザ名、パスワード）を行うことができる ・ NCP（エヌシーピー）（※7）（ネットワーク制御プロトコル）で、ネットワーク層のプロトコルを選択・設定する	RFC1661 他
PPPoE（ピーピーピーオーイー）	PPP over Ethernet（ピーピーピー オーヴァー イーサネット）（イータネット上の 2 点間通信プロトコル） PPPoE は、イーサネット環境上で PPP を使うためのプロトコルである。 PPPoE は、DSL（ディーエスエル）（※8）、FTTH（エフティーティーエイチ）（※9）、CATV（シーエーティーヴィ）（※10）等のブロードバンド･インターネットで使用されている。 ・ PPP が持つ PAP、CHAP のユーザ認証（ユーザ名、パスワード）機能を利用してイーサネット環境上で PPP を実現する ・ ユーザ認証は、IPS（プロバイダ）とユーザ宅のブロードバンドルータ（例：フレッツ光：CTU（回線終端装置）、フレッツ ADSL：ADSL モデム）との間で行う。	RFC2516
ARP（アープ）	Address Resolution Protocol（アドレス レソリューション プロトコル）（アドレス解決プロトコル） ARP は、IP アドレスから Ethernet の物理アドレス（MAC アドレス）を求めるためのプロトコルである。 逆に、物理アドレスから IP アドレスを求めるプロトコルを RARP（Reverse ARP）という。 ・ ARP は、インターネット層とリンク層の中間（IP の下、リンク層の上）で動作する。 （参考）コマンドプロンプトの arp コマンドを用いて、MAC アドレスを得ることができる。	RFC826

（※１）Ethernet は、Xerox（ゼロックス）、Intel（インテル）、DEC（デックス）（現 HP）が開発・公開した DIX 仕様（LAN の規格）を言う。これを元にして IEEE802（LAN 関係）委員会が、1983（S58）に IEEE802.3（ＣＳＭＡ/ＣＤ（シーエスエムエー／シーディー））として規格化した。
元来 Ethernet は 10Mbps の LAN 規格であったが、現在は Fast Ethernet（100Mbps）や Gigabit Ethernet（1Gbps）をも含んでいる。
DIX 仕様のヘッダ（イーサネット･ヘッダ）と IEEE802.3 仕様のヘッダ（IEEE802.3 ヘッダ）は若干異なるが、現在主流になっているインターネットではイーサネット･ヘッダが用いられている。

（※２）CSMA/CD（Carrier Sense Multiple Access with Collision Detection（キャリア センス マルティプル アクセス ウィズ コリジョン ディテクション））は、他のキャリアを検出した場合に送信を一旦休止して衝突を回避する媒体アクセス制御方式である。（IEEE802.3 の規格）。

（※３）MAC（Media Access Control（メディア アクセス コントロール））は、LAN などの通信媒体でデータ（フレーム）を伝送する際の既定（送受信方式、形式、誤り制御）をいう。

（※４）LCP（Link Control Protocol（リンク コントロール プロトコル）：リンク制御プロトコル）は、リンク相手を識別して受け入れ可否を決定、許容パケットサイズを決定、構成エラーを検出。(RFC1570)

（※５）PAP（Password Authentication Protocol（パスワード オーセンティケーション プロトコル）：パスワード認証プロトコル）は、2 ウエイ･ハンドシェーク方式の単純な認証プロトコルである。（RFC1334）

（※６）CHAP（PPP Challenge Handshake Authentication Protocol（チャレンジ ハンドシェーク オーセンティケーション プロトコル）：チャレンジハンドシェイク認証プロトコル）は、3 ウエイ･ハンドシェーク方式の安全性の高い認証プロトコルである。（RFC1994）

（※７）NCP（Network Control Protocol（ネットワーク コントロール プロトコル）：ネットワーク制御プロトコル）は、ネットワーク層（IPCP で IP、IPV6CP で IPv6、IPXCP で IPX、ATALKCP で Apple Talk）の設定を行うプロトコルである。(RFC1570)

（※８）DSL（Digital Subscriber Line（ディジタル サブスクライバー ライン））は、加入者線（電話回線）を用いて高速データ通信を行う技術を言い、ADSL（Asymmetric ＤＳＬ（アシンメトリック ディーエスエル）：非対称加入者線、下りが高速で上りが低速なので非対称と言う）、VDSL（Very high bitrate ＤＳＬ（ベリー ハイ ビットレート ディーエスエル）：超高速デジタル加入者線）等がある。

（※９）FTTH（Fiber To The Home（ファイバー トゥ ザ ホーム））は、光ファイバーを加入者線に使用する通信サービス。

（※10）CATV（Cable Television（ケーブル テレビジョン））は、同軸ケーブル、光ケーブル等を用いてテレビジョン放送、インターネット接続、電話などのサービスを提供する有線放送。

3.2. IPv4 のアドレスと IPv6 のアドレス（おまけで追記した項目です）

くしくも本資料を執筆中の 2012 年 6 月 6 日（水）午前 9 時（日本時間）に、『World IPv6 Launch（ワールド ランチ）（世界の IPv6 開始）』イベントが催され IP v 6 への本格的な対応がスタートした。
これは、世界中の大手 Web サイトやプロバイダが一斉に IPv6 への対応を開始する日であり、インターネットが産声を上げた 1980 年代初頭から使われてきた IP がバージョン 4（IPv4）からバージョン 6（IPv6 ）への移行を始める日である。
しかし 43 億個の IP アドレスが枯渇するほど普及しているインターネットを IPv4 から IPv6 に移行するには予測不能の期間が必要であり、その間は IPv4 と IPv6 が共存することになる。

（参考）米ガートナー社の 2008/6/23 の発表では、世界のパソコン台数が 2014 年前半に 20 億台を突破すると試算している。これに急増中のスマートフォン、タブレット端末等を加えると膨大な IP アドレスの需要が見込まれる。
また国連の 2011 年版「世界人口白書」によると、世界人口が 70 億人に到達したと推定されている。

1）IPv4 アドレスの枯渇と IPv6 への移行について

IPv4 は 32bit（4 B）のアドレス空間を用いて最大 43 億個の IP アドレスを管理できるが、インターネットの想定外の普及により 2011 年にはプールされていた IP アドレスが枯渇したと言われ、新たな IP アドレスを割り振ることができなくなってしまった。

（補足）B（Byte）は「Bite（＝一噛み）」をもじった造語であり 1 文字の情報量を言い bit 数はマシンにより異なっていた。筆者がコンピュータに接した 1970 年前後には 1B＝7～9bit のマシンもあった。このため 8bit の塊を 8octed（「オクタ」はギリシャ語で「8」の意）と呼ぶこともあった。

この IP アドレスの枯渇を見越して、IETF（前述のインターネット技術の標準化組織）が 1991 年から調査を開始し、1998 年に IPv6（RFC2460）の仕様が確定して 1999 年 7 月から IPv6 アドレスの割り振りが開始された。

IPv6 の準備が整うまでの間、IPv4 アドレスの枯渇を先延ばしする当面の対策として、プライベートアドレス（RFC1918、1996 年）、NAT（RFC2663、1999 年）、CIDR（Classless Inter-Domain Routing、RFC4632、2006 年）等により IPv4 アドレスの節約と有効活用が図られたのが現状であった。

新しいい規格の IPv6（同 Ver.6）は、これまでの 4 倍の長さの 128bit（16B）のアドレス空間を用いて最大 340 兆個の 1 兆倍の 1 兆倍の IP アドレス持っていて、無限のアドレス空間を持つと言われている。

2）IPv4 アドレスについて

IPv4 アドレスは単に IP アドレスと呼ばれていて、32bit（4B）のアドレス空間を持っている。
32bit で 43 億個のアドレスが使用可能であるが 2011 年に枯渇した。

（A） IPv4 アドレスの表記方法

- アドレスの 32bit を 8bit（1B）ずつ 4 ブロックに分割してドット（“ . ”）で区切り、それぞれを 10 進数（0～255）で表記する
- 2 進数（00000000～11111111）から 10 進数（0～255）への変換

00000000～11111111（$=1\times2^7+1\times2^6+1\times2^5+1\times2^4+1\times2^3+1\times2^2+1\times2^1+1\times2^0$
$=128+64+32+16+8+4+2+1$
$=255$）

（例）1100000.10101000.00011000.00111001＝192.168.24.57
1100000.10101000.00000011.00011000＝192.168.3.24
10101100.00010000.11111110.00000001＝172.16.254.1

(B) IPv4 の構造

IPv4 アドレス（32bit）は、前半のネットワークアドレスと後半のホストアドレスからなり、下図に示すように RFC791 でクラス毎の境界位置を定めている。

IP アドレス（IPv4：32bit）	
ネットワークアドレス IP ルータで境界を区切られた同一の物理ネットワークに付与されたネットワーク ID	ホストアドレス ネットワーク内のサーバ、ルータ、パソコン等に付与されたホスト ID
・ クラス A：0 で始まる 8it ・ クラス B：10 で始まる 16bit ・ クラス C：110 で始まる 24bit ・ 拡張アドレスモード：111 で始まる 32bit	・ クラス A：24bit（16,777,215 個） ・ クラス B：16bit（65,535 個） ・ クラス C：8bit（256 個） ・ 拡張アドレスモード：0bit（無し）

- IP アドレスの前半のネットワークアドレスはレジストリと呼ばれる階層化された国際組織が割り振りを行っていて、
  総括レジストリ（IANA（アイアナ）、Internet（インターネット） Assigned（アサインド） Numbers（ナンバーズ） Authority（オーソリティ））が世界を 5 ブロックの分けた地域レジストリ（例： APNIC、Asia-Pacific（アジアーパシフィック） Network（ネットワーク） Information（インフォメーション） Centre（センター）=アジア・太平洋地域等）にアドレス範囲を割り振り、
  地域レジストリが地域内の国別レジストリ（例：JPNIC、Japan（ジャパン） Network（ネットワーク） Information（インフォメーション） Center（センター））にアドレス範囲を割り振っている
- 国別レジストリが国内のプロバイダ、企業、研究機関等に個々のネットワークアドレスを割り当てている

(C) 「アドレスマスク」によるネットワークの分割

クラス A では 16,777,225 個ものホストアドレス、クラス B でも 65,535 個ものホストアドレスが使えるが、このように膨大なネットワークは一般に存在せず、アドレス利用に無駄が生まれアドレス不足の一因になった。このアドレス不足を補う対策としてアドレスマスク（例：255.255.255.000）を用いてホストアドレスの一部をサブネットとしてネットワーク分割（RFC950）するようになった。

(D) 「グローバル IP アドレス」と「プライベート IP アドレス」

グローバル IP アドレスはインターネットにアクセスするために使用する IP アドレス

- 世界中で同じアドレスは存在しない
- 世界で IP アドレスの割り振りが決まっている

プライベート IP アドレスはローカル IP アドレスとも呼ばれ、組織内（家庭内、企業内等）でのみ使用できる IP アドレス

- 組織内では IP アドレスを重複できない
- プライベートアドレスの範囲は規定（RFC1918）されている
  192.168.0.0/16・・・192.168.0.0～192.168.255.255

【重要】 IP アドレスに続く「 /16 」は前半の 16bit が固定されていることを指す

3）IPv6 アドレスについて

IPv6 アドレスは 2012 年 6 月 6 日から使用が開始された新しい IP アドレスであり、128bit（16B）のアドレス空間を持っている。

(A) IPv 6 アドレスの表記方法

・ アドレスの 128bit を 16bit（2B）ずつ 8 ブロックに分割してコロン（“ : ”）で区切り、それぞれを 16 進数（0、1、2、…、8、9、A、B、…E、F）で表記する

（補足）10 進数とは、0、1、…、9 の 10 個の数があり 9 から 10 になると桁上りする数を言い、16 進数とは、0、1、…、9、A、B、…、F の 16 個の数があり 15 から 16 になると桁上りする数を言う。同様に 2 進数は 0、1 の 2 個の数があり 1 から 2 になると桁上りする。

10 進数	0	1	2	3	4	5	6	7	8	9
2 進数	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001
16 進数	0	1	2	3	4	5	6	7	8	9

10 進数	10	11	12	13	14	15
2 進数	1010	1011	1100	1101	1110	1111
16 進数	A	B	C	D	E	F

10、11 …15 に相当する 1 桁の文字が無いので、A、B …F を使用

・ あるブロックが“ 0 ”で始まる場合は、先行する“ 0 ”を省略できる（ゼロサプレス）

（例） 3ffe:2002:0000:0000:0000: 03ab:0000: ff01

⇒ 3ffe:2002: 0: 0:0:3ab: 0: ff01

・ 値が 0 のブロックが連続しているところは、連続した 0 のブロックをまとめて“ :: ”と表記して省略できる。ただし “ :: ”は可変長なので、一番長く 0 が続くところで、1 ヶ所だけ“ :: ”を使用すること

（例） 3ffe:2002:0000:0000:0000: 03ab:0000: ff01

⇒ 3ffe:2002: 0: 0:0: 3ab: 0: ff01

⇒ 3ffe:2002:: 3ab: 0: ff01

0 が少ない（1 個だけ）ので残す

0 が一番多く続く（3 個）ので、これを“ :: ”で省略する

・ Web ブラウザの［アドレスバー］欄に IPv6 アドレスを入力する場合は、半角大カッコ“ [”と“] ”で囲む（RFC3936）

（例） [3ffe:2002: : 3ab: 0: ff01]

(B) IPv6 の構造

IPv6 アドレス（128bit）は、前半 64bit のネットワークプレフィックスと後半 64bit のインタフェース ID からなり、下図に示すように RFC791 でクラス毎の境界位置を定めている。

<table>
<tr><td colspan="3">IPv6 アドレス（128bit）</td></tr>
<tr><td colspan="2">ネットワークプレフィックス（64bit）
IPv6 グローバルユニキャストアドレス形式
（RFC3587、2003/8）
（注）旧プロトコル（RFC2374、1998/7）は廃止</td><td rowspan="2">インタフェース ID（64bit）
IPv4 の「ホストアドレス」に相当するが、固定長である。
・ 自動的に MAC アドレスを元に EUI-64 (※2) アドレスを得て、さらに bit＃6 を反転してインタフェース ID を設定
・ 自動的に履歴データを元にしたランダムな匿名（一時的な）インタフェース ID を生成する
・ 手動設定
・ DHCPv6（RFC3315、「OCN ユーザ網インタフェース仕様書〔第 1.0 版 H17.12.5〕」では DHCPv6 プロトコルの適用を明記）</td></tr>
<tr><td>グローバルルーティングプレフィックス（またはグローバル ID）
（参考）2006/1 の配布ポリシーでは 48bit
・ レジストリ (※1) が ISP 等に割り振る</td><td>サブネット ID
（64-n bit）
・ ISP が企業、組織等に割り振る</td></tr>
</table>

（※１）レジストリ（Registry）とは、IP アドレス空間を割り振り／割り当てする組織を言い、総括レジストリ（IANA（アイアナ））→地域レジストリ（例：APNIC（エーピーニック））→国別レジストリ（例：JPNIC（ジェイピーニック））と階層化されている

（※２）EUI -64（Extended Unique Identifier-64（エクステンディッド ユニーク アイデンティファイア））は IEEE が標準化したデバイス識別のための 64bit の識別子を言う。EUI-64 の上位 24bit（3B）は IEEE が割り当てた製造業者番号であり、下位 40bit は製造業者の管理下で重複なく付与する番号である。

なお、MAC（Media Access Control（マック メディア アクセス コントロール））アドレスは IEEE802 アドレスとも呼ばれていて、48bit の前半 24bit（8B）が企業 ID、後半 24bit が企業内 ID であり、ネットワークアダプタに記録されている。企業 ID の bit＃6 が 0 の場合はユニバーサルで 1 の場合はローカルであり、bit＃7 が 0 の場合はユニキャストで 1 の場合はマルチキャストである。

(C) IPv6 アドレスの種類とアドレス範囲

IPv6 アドレスの種類		IPv6 の表記	概要
ユニキャストアドレス	グローバル	2000::/3	・ IPv6 インターネット用の IPv6 アドレス （注）2012/7 現在の割り振り範囲は、2001::/16
		2002::/16	・ 6to4 トンネリング用のユニキャスト 6to4 アドレス ・ アドレス構造は、 2002(16bit):IPv4 アドレス(32bit):サイトレベル集約 ID(16bit):インタフェース ID(64bit)
		2003::/16 ~3ffd::/16	・ 未割当
		3ffe::/16	・ IPv6 の研究開発用
	リンクローカル	fe80::/10	・ 同一サブネット上での通信に使う IPv6 アドレス ・ IPv6 ノードは 1 個以上のリンクローカルユニキャストアドレスを持つ
マルチキャストアドレス		ff00::/8	・ 指定範囲（リンクローカル、サブネット、グローバル等）内の指定通信機器（ノード、ルータ等）に対して同報（1 対 n）通信する IPv6 アドレス ・ IPv4 のブロードキャストアドレスに相当
エニーキャストアドレス			・ 複数ホストに同じエニーキャストアドレスの付与を許した環境で、ルートが一番近いホストと通信する IPv6 アドレス ・ 電話でたとえると 110 番、119 番あるいは代表電話番号のようなもの
未指定(Unspecified)		::/128	・ 重複アドレス検出の際に、パケットの始点アドレスとして利用される。
ループバックアドレス		::1/128	・ ローカルホスト（自デバイス）と通信する IPv6 亜でレス（EFC4291） ・ TCP/IP が必要に応じて自身との通信で使用する

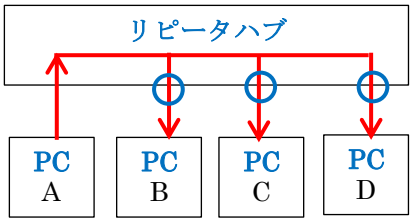
4.　ネットワーク機器と通信媒体について

4.1.　ネットワーク機器

インターネットの普及と技術進歩により、ネットワーク機器の発展は目覚ましく世代交代が激しい。
例えば同軸ケーブルの IEEE 10BASE2、同 100BASE5 を知る人が少なくなり、リピータ、リピータハブ（ハブ）が店頭から姿を消してしまった。
ここでは、現在主流になっているすイッチングハブ、ルータおよびブロードバンドルータについて説明し、参考までに過去の遺産となったリピータハブについて説明する。

1）リピータハブ（ハブ）

リピータハブ（※1）はシェアードハブあるいは単にハブとも呼ばれ、OSI 参照モデルの第 1 層（物理層）に対応するネットワーク機器であり、LAN 内にある複数の通信端末を相互に接続する時に用いる機器である。
右図に示すように、リピータハブは通信端末をケーブル接続する複数のポートを持っている。
リピータハブは、ポートに入力された電気信号を整形・増幅した後、他のすべてのポートに送信する。

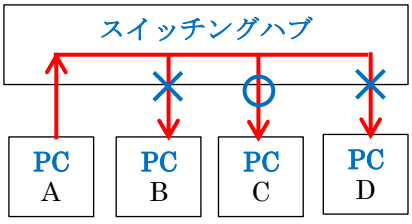


- リピータハブは、劣化（減衰、歪、ノイズ）した電気信号を補正するため、信号の波形を整形し増幅した後、全てのポートに送信する
- 受信信号を補正した後の信号を全てのポートに送信する
- 信号をすべてのポートに送信するため、衝突（コリジョン Collision）が発生する確率が高くネットワークの利用効率が低下する
- 遅延により衝突検出が困難になることから、リピータハブの多段接続は、10BASE-T で 2 段、100BASE-TX で 4 段と制限されている。

（※1）スイッチングハブの低価格化（5～6 ポートで 4,000 円前後）に伴って安価だけが特長のリピータハブは市場から姿を消している。

2）スイッチングハブ（L2 スイッチ）

スイッチングハブは L2 スイッチとも呼ばれ、OSI 参照モデルの第 1 層～2 層（物理層、データリンク層）に対応するネットワーク機器であり、自身の LAN 内にある複数の通信端末を相互に接続する時に用いる機器である。
右図に示すように、スイッチングタハブは通信端末をケーブル接続する複数のポートを持っている。
スイッチングハブは、ポートに入力された電気信号を整形・増幅した後、電気信号の中にある宛先 MAC アドレスを解釈して該当する通信端末が接続されたポートのだけに送信する。

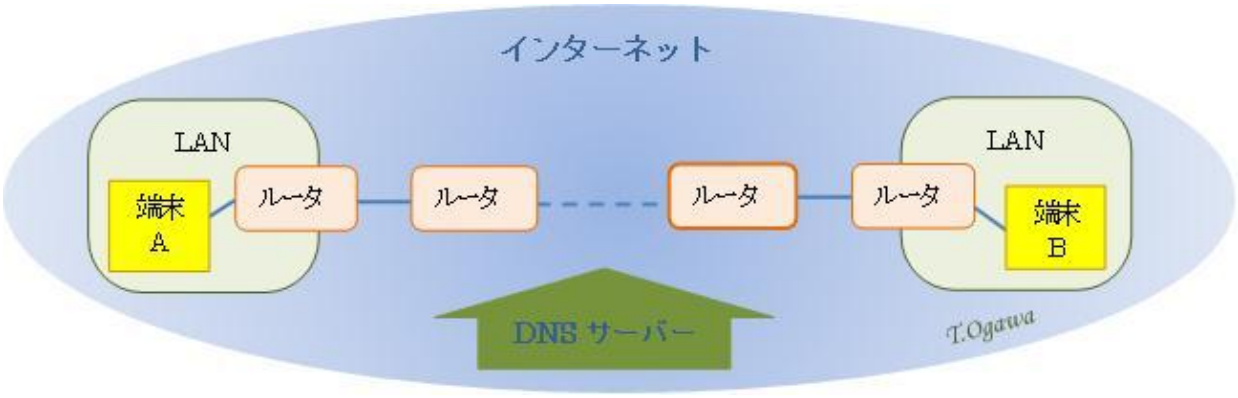


- スイッチングハブは、ポートに接続された通信機器の MAC アドレスを取り込んで MAC テーブルを作成する

・ スイッチングハブは、劣化（減衰、歪、ノイズ）した電気信号を補正するため、信号の波形を整形し増幅する
・ 作成した MAC テーブルを参照して、受信信号を補正した後の信号を宛先 MAC アドレスで指定された通信機器が接続されたポートに送信する
・ 信号を指定されたポートだけに送信するため、衝突（Collision（コリジョン））が発生する確率が低い
・ スイッチングハブの多段接続は 7 段程度が理想的（理論上は無制限）とされている。

3）ルータ

ルータは OSI 参照モデルの第 1 層～3 層（物理層、データリンク層、ネットワーク層）に対応するネットワーク機器であり、自身の LAN 内にある複数の通信端末を相互に接続する時、自身の LAN と外部の LAN を接続する時、LAN 同士を接続する時等に用いる中継機器である。



なおルータは、規模や使用位置により次表のように分類されている。

種類	規模	用途
コア･ルータ	数千万円～	基幹ネットワークを構成（IPS 相互間、IPS 拠点間を接続）
センター･ルータ	百万～数千万	IPS～企業間、WAN を介した企業ネットワークを接続
L3 スイッチ（※2）	百万～数千万	同上（以前ローカル･ルータと呼んだもの発展した）
エッジ･ルータ	数万～百万円	基幹ネットワークの端に設置（本店、支店等を WAN に接続）
リモート･ルータ	数万円～	WAN を介して LAN 同士を接続
ブロードバンド･ルータ	数千～数万円	家庭や小規模企業で ADRL や FTTH 等を介して IPS に接続 NAPT 機能（IP マスカレード）で 1 個のグローバル IP アドレスを複数端末で共用する

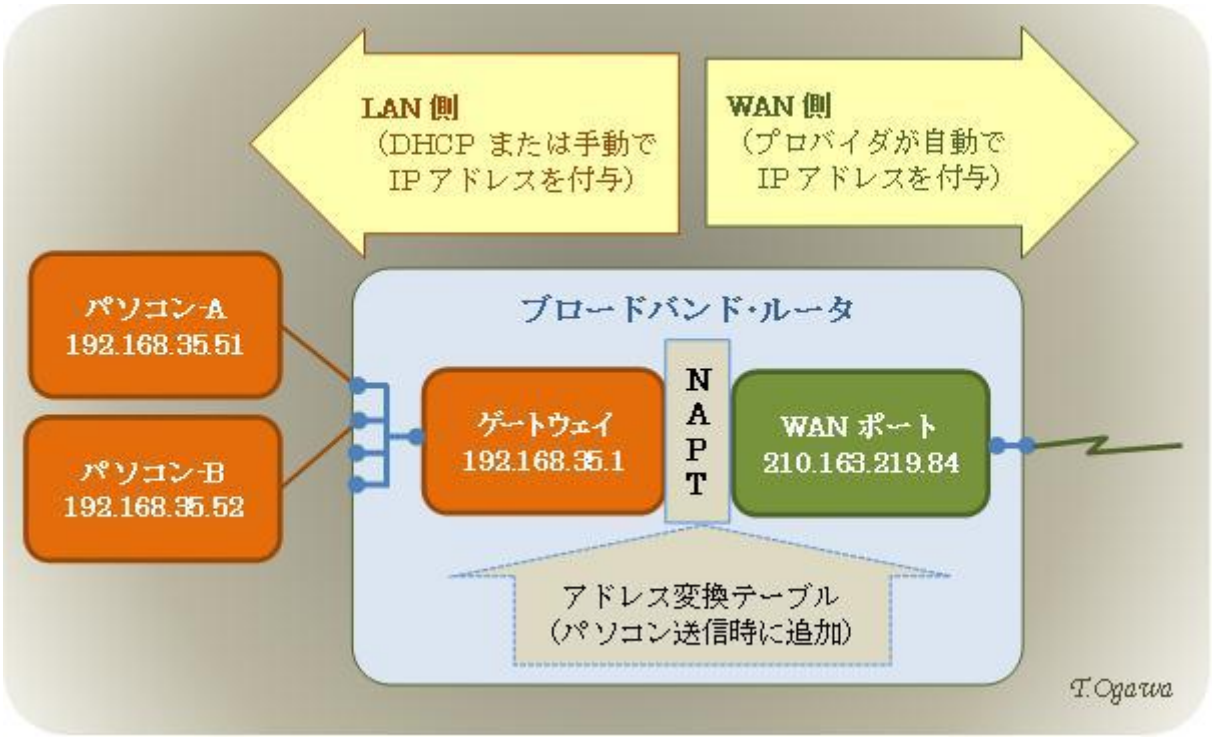
ルータの主な機能・役割は次のとおりである。

・ インタフェース･ユニットの追加･交換により、複数の回線種類（イーサネット、ATM、FDDI、ISDN 等）に接続できる
・ パケット単位で End To End（送信元端末～宛先端末）のデータを中継する
・ 宛先 IP アドレスが自身の LAN 内の場合は直接転送する
・ 宛先 IP アドレスが自身の LAN 外の場合は、次の処理を行い転送する
  - 送信伝送路に合わせて MAC フレームを生成し、それに IP パケットをいれて転送フレームを生成する
  - IP パケットを転送する際に、IP ヘッダの生存期間（TTL）を減算し書き換える
  - ルーティングテーブルを参照し、相互接続しているルータから適切なルータを選択しテータを転送する
・ 相互接続した他のルータとの通信によってルーティングテーブルを常に最新状態に保つ

（※２）L3 スイッチは、IP 以外のプロトコル（IPX、トークンリング、Apple Talk、DLSw 等）には対応しない点、ルーティングに特化して高速な点、対応 VLAN が多い点等がルータと異なり、主に企業の基幹ネットワークなど、複数のサブネットを連結する大規模なシステムのルータとして使用されている。

４）ブロードバンドルータ

ブロードバンドルータ（BB ルータ：broadband（ブロードバンド） router（ルータ））とは、家庭や小規模事業所等で ADSL 、FTTH（光接続）等のブロードバンド回線を用いてインターネット接続にする際に使うルータを言う。



ブロードバンドルータには、ルーティング（経路選択）に特化した一般のルータに無い次の機能がある。

- NAPT（ナプト）（※3）機能で、プロバイダから付与された 1 個のグローバル IP アドレスを複数のプライベート IP アドレスに対応させることができる。これにより複数の通信端末から同時にインターネットに接続できる。
- NAPT のアドレス変換テーブルに送信記録がない外部（WAN 側）から始まる通信は、LAN 内で使用されるプライベート IP アドレスに変換できないので、データが破棄される。このため NAPT には簡易ファイアウォールとしての機能がある
- ポートフォワーディング（※6）機能を有効にすると、アドレス変換テーブルに手動で登録されている IP アドレス／ポート番号の通信端末を指定した外部（WAN 側）からの通信を登録した通信端末に接続することができる
- DMZ（※6）ホスト機能を有効にすると、アドレス変換テーブルに手動で登録あるいは自動で記録されている以外の IP アドレス／ポート番号等の通信端末を指定した外部（WAN 側）からの通信を特定の通信端末に接続することができる
- DHCP サーバ機能により、ポートに接続された通信端末に対してネットワーク接続情報（IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバ）を通知して自動設定させることができる

・ PPPoE クライアント機能により、クライアントに代わって PPPoE による認証を行い、プロバイダから 1 個のグローバル IP アドレスを得ることができる

（※３）NAPT（Network Address Port Translation（ネットワーク アドレス ポート トランスレーション）、RFC2663 で規定）は単に NAT あるいは Linux での実装名の IP マスカレードと呼ばれることが多い。

NAPT は IP v 4 の枯渇を先送りする技術であり、無限に近い IP 空間がある IPv6 では不要である。

NAPT 機能は、次によりプライベート IP アドレスとグローバル IP アドレスとの変換を行う。

・ **送信時（LAN→WAN）**は、IP ヘッダの送信元 IP アドレスをプライベート IP アドレスからブロードバンドルータ出口（WAN 側＝ゲートウェイ）にプロバイダが付与したグローバル IP アドレスに変換し、更に TCP（or UDP）ヘッダの送信元ポート番号を TU ポート番号（一般的に 1024～65535 を使用）に変換し、変換前後の送信元 IP アドレスと送信元ポート番号等を変換レコードとしてアドレス変換テーブルに記録した後、インターネットに転送する。

・ **受信時（WAN→LAN）**は、アドレス変換テーブルの変換レコードを検索・参照して、TCP ヘッダの宛先ポート番号（変換後の送信元ポート番号）を変換前の送信元ポート番号に戻し、更に IP ヘッダの宛先 IP アドレス（変換後の送信元グローバル IP）を変換前の送信元プライベート IP アドレスに戻した後、内部の通信端末に転送する。

LAN からの送信データに対する WAN からの返信データを受信したら、アドレス変換テーブルの該当レコードを削除する。このため、外部（WAN 側）から始まる通信では、アドレス変換テーブルに変換レコードがないので内部（LAN 内）の通信端末に接続できないのでデータは破棄され簡易ファイアウォールの役目を果たす。

（※４）ポートフォワーディング（port forwarding）機能は「ローカルサーバ」、「仮想（バーチャル）サーバ」、「静的 NAT」、「SUA（Single User Account）」、「アドレス変換テーブルの追加」等とも呼ばれている。

ポートフォワーディングは、NAPT 機能により不可能になっている外部（WAN 側）の通信端末から内部（LAN 内）の通信端末にアクセスを可能にする技術の一つであり、この機能を持つブロードバンドルータは多い。

（※５）DMZ（DeMilitarized Zone（ディミリタライズド ゾーン）：非武装地帯）ホスト機能は、「バーチャルコンピュータ」、「バーチャルサーバ」とも呼ばれている。

ポートフォワーディングは、NAPT 機能により不可能になっている外部（WAN 側）の通信端末から内部（LAN 内）の通信端末にアクセスを可能にする技術の一つであるが、この機能を持つブロードバンドルータは少ない。

4.2.　無線 LAN

無線 LAN の規格はＩＥＥＥ（アイトリプルイー）(※1) 802.11（無線 LAN）で策定されている。

１）無線 LAN の種類

現在使用されている無線 LAN、2012 年末以降に出荷予定の無線 LAN の種類と概要を以下に示す。

IEEE802.11（無線 LAN）の種類

規格	策定	周波数帯	公称速度	ストリーム	チャネル幅	備考
IEEE802.11a	1999.10	5GHz	54Mbps	1	20MHz (0.4GHz/ch)	19ch（同時使用 19ch）
IEEE802.11b	1999.10	2.4GHz	11Mbps 22Mbps	1	22MHz (0.1GHz/ch)	14ch（同時使用 4ch）
IEEE802.11g	2003.06	2.4GHz	54Mbps	1	20MHz	13ch（同時使用 3ch）
IEEE802.11n	2009.09	2.4GHz 、 5GHz	65Mbps 600Mbps	1 4	20/40MHz	14ch（同時使用 2ch） 19ch（同時使用 9ch） チャネルボンディング MIMO
IEEE802.11ac	2012.2 ドラフト 2.0	5GHz	433Mbps 6.93Gbps	1 8	80/160MHz	80m（100Mbps）？ MU-MIMO
IEEE802.11ad	2012.5 ドラフト 7.0	60GHz (57～ 66)	4.6Gbps 6.8Gbps	1	9GHz (2.16GHz/ch)	10m 程度

（参考）ドラフト 2.0 が 2012(H24).5 に公開されたばかりであるが BUFFALO が 2012(H24).7.上旬に、IEEE802.11ac の親機（WZR-D1100H）と子機（WLI-H4-D600）を発売した。

（※１）IEEE の LAN に関する規格を策定するために 1980 年 2 月に活動を開始したので 802 委員会と呼ばれている。802 委員会は OSI 参照モデルの第 1 層（物理層）と第 2 層（データリンク層）の標準規格を策定している。

なお IEEE802 委員会はテーマ毎に独立した WG で検討し、よく知られた WG に IEEE802.2（LLC：論理リンク制御プロトコル＝データリンク層の上位層）、IEEE802.3（CSMA/CD：イーサネット）、IEEE802.11（WLAN：無線 LAN）、IEEE802.15.1（Bluetooth:ブルートゥース）がある。

２）Wi-Fi とは

Wi-Fi（ワイファイ）（Wireless Fidelity（ワイアレス フィデリティ）、Fidelity＝忠実）は、IEEE802.11n の無線 LAN と同じものを指していると誤解されることが非常に多いが、全く定義が異なるものである。

Wi-Fi は、その製品が無線 LAN の相互接続を保証するための認定試験に合格した製品であることを指すブランド名である。無線 LAN が出始めた 2000 年（H12）前後は、親機と子機のメーカが異なる場合は当然のこととして、親機と子機が同じメーカでも製品の系列が異なる場合には相互接続が保障されず、無線 LAN の普及を妨げる一因であった。

こうした問題を解決するため、1999 年に無線 LAN の相互接続を保証する認定業務を行う業界団体としてWECA（Wireless Ethernet Compatibility Alliance：直訳で無線イーサネット適合同盟）が発足して認定業務を始めた。その後 Wi-Fi の知名度が高まってきたので団体名を 2002 年 10 月にWi-Fi Allianceに改名し、「Wi-Fi」ブランドを作った。

Wi-Fi Alliance は、相互接続を保証する認定試験に合格した製品に、下図に示す「Wi-Fi CERTIFIDE（Wi-Fi 保証）」ロゴを表示することを認めている。

なお、国内の主要な無線 LAN 機器メーカの Web ページで「Wi-Fi CERTIFIDE」認証取得について調べたところ、意外にも親機の認証取得の機種が少なかった（コレガ社のみ全機種で取得）。

（下衆の勘ぐり）NEC は通信機器メーカの自信と誇りで認証試験を必要としないのか？

【無線 LAN メーカの 「Wi-Fi CERTIFIDE」認証の状況】

メーカ	無線 LAN 親機の認証取得	無線 LAN 子機の認証取得
NEC	記述無し（取得無し？）	記述無し（取得無し？）
BUFFALO	450Mbps 対応の 2 機種のみ取得	全機種取得
I-O DATA	取得無し	USB の超小型×1 機種を除き取得
コレガ	全機種取得	全機種取得

3）IEEE802.11n の最高通信速度と MIMO、チャネルボンディング

IEEE802.11n は、2006 年 3 月にドラフト版 1.0、2007 年 6 月にドラフト版 2.0 が策定され、2009 年 9 月に正式規格が認定された。

周辺機器メーカの Web ページ（BAFFALO、I-O DATA 等）で調べると、IEEE802.11n 対応の無線 LAN 親機の最高通信速度が 150Mbps、300Mbps、450Mbps と製品によりまちまちである。一方、パソコンメーカの Web ページ（NEC、富士通等）で調べると IEEE802.11n 対応の内蔵無線 LAN 子機の最高通信速度が 150Mbps、300Mbps とまちまちである。

このような製品毎の違いは 11b、11a、11g には無かったことである。これは 11n が通信速度を向上させるための「MIMO」と「チャネルボンディング」と呼ばれる技術を採用しているためである。

【IEEE802.11n の最高通速度】

帯域幅 / データ分割（MIMO）	20MHz	40MHz チャネルボンディング
1 ストリーム	72.2Mbps	150Mbps
2 ストリーム	144.4Mbps	300Mbps
3 ストリーム	216.8Mbps	450Mbps
4 ストリーム	288.9Mbps	600Mbps

＊＊ MIMO ＊＊

MIMO（Multiple Input Multiple Output 、多入力多出力）とは、複数のアンテナを使ってデータを振り分けて同時に転送することで通信速度を高める技術を言い、送信側はデータをストリーム

単位に分割し別々のアンテナで送信し、受信側は別々のアンテナで受信したストリーム単位の分割データを合成して元のデータに復元する。IEEE802.11n ではアンテナ数を 4 本以下に制限し 4 ストリームまでと規定している。

＊＊ チャネルボンディング ＊＊

チャネルボンディング（channel bonding（チャネル ボンディング）、チャネル結束）とは、無線 LAN の隣り合った 2 つのチャンネルを束ねて通信する技術を言い、IEEE802.11n では 1 チャンネル分の 20MHz 幅で通信するところを 2 チャンネル分の 40MHz で通信することで通信速度を 2 倍強に高速化している。

4.3. LAN ケーブルの種類

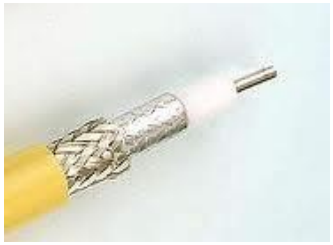
1）イサ―ネット用の LAN ケーブルの種類と特徴

イーサネットで使用される LAN ケーブルには、同軸ケーブル、ツイストペアケーブル、光ファイバーケーブルがあるが、2000 年前後の主流であった同軸ケーブルは目に触れることがなくなり、家庭や小規模事業所ではツイストペアケーブルが主流になっている。

【LAN ケーブルの種類と特徴】

同軸ケーブル

- ○ 磁気ノイズに強い
- × 伝送速度が遅い
- △ 伝送距離がやや長い
- △ ケーブルがやや高価
- △ 敷設が少し難しい

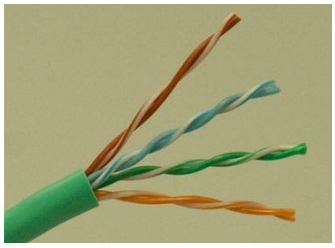


10Base5（φ10mm）

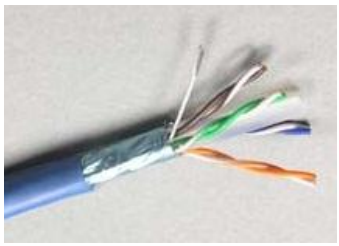
10Base2（φ5mm）

ツイストペアケーブル

- △ 磁気ノイズにやや弱い
- ○ 伝送速度がやや早い
- × 伝送距離が短い
- ◎ ケーブルが安価
- ◎ 敷設が易しい



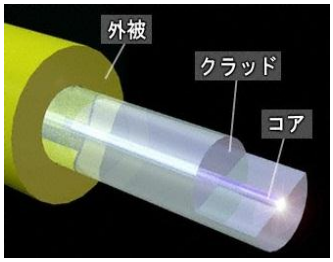
UTP（非シールド撚り対線）



STP（シールド付撚り対線）

光ファイバーケーブル

- ◎ 磁気ノイズの影響なし
- ◎ 伝送速度が速い
- ○ 伝送距離が長い
- × ケーブルが高価
- × 敷設が難しい

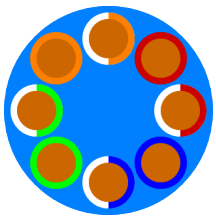
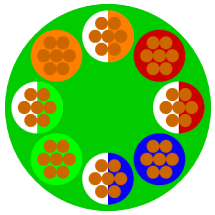


- SMF（シングルモードファイバ）コアが細く、長距離・高速伝送に向く
- MMF（マルチモードファイバ）はコアが太く、複数モードで伝送して情報量は多いが短距離向き

2）ツイストペアケーブルの銅線の種類

ツイストペアケーブルで使用している導体（銅線）には、単線仕様のものと撚り線仕様のものがあるので、使用場所に応じて使い分ける必要がある。

なお、フラット型のツイストペアケーブルは撚り線仕様である。

単線仕様 導体が 1 本の太い銅線でなっている ・電気抵抗が小さく、長いケーブルが使える ・極端な曲げに弱い 	**撚り線仕様** 導体が複数本の細い銅線でなっている ・電気抵抗が大きく、10m 以下の短いケーブルに適する ・柔軟性が高く、狭いスペースでの敗戦に適する 

3）フラット型のツイストペアケーブル

一般のツイストペアケーブルは、2 本の絶縁銅線を撚って（ツイスト）1 対として電気ノイズに強くし、それを 4 対まとめて全体を被覆しているので断面は円形である。

フラット型のツイストペアケーブルは、2 本の絶縁銅線を撚って 1 対として電気ノイズに強くし、それを 4 対横に並べて全体を被覆しているので断面は平型になっている。

このためフラット型のツイストケーブルは幅 5mm×厚さ 1mm となり、隙間やカーペットの下に配線する時に便利である。

4）イサーネット用の LAN ケーブルの規格

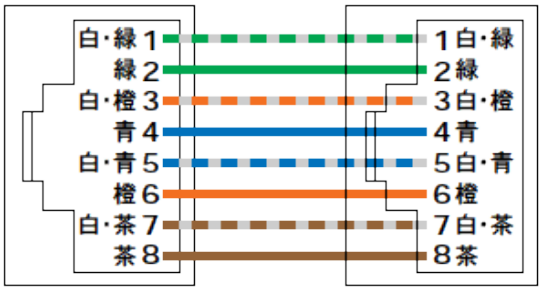
イーサネットで使用する LAL ケーブルの規格は、IEEE802.3 ワーキンググループで制定されている。

次表で、　　で塗りつぶした行が現在主流となっているツイストペアケーブルである。

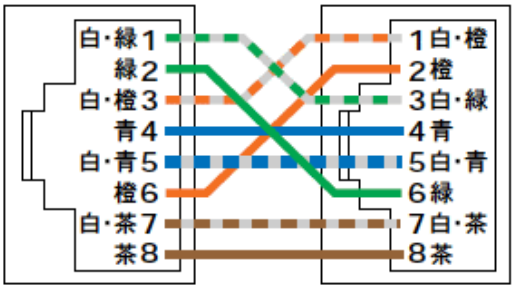
ケーブル	ケーブルの名称		伝送速度	最大長	備考	
	タスクフォース	ケーブル名称				
同軸	IEEE802.3	10BASE5	10Mbps	500m	直径 10mm	バス型接続
	IEEE802.3a	10BASE2	〃	185m	直径 5mm	
ツイストペア	IEEE802.3i	10BASE-T	〃	100m	UTP 2 対 CAT3 以上、RJ-45	
	IEEE802.3u	100BASE-TX	100Mbps	〃	UTP 2 対 CAT5 以上、RJ-45	
	IEEE802.3ab	1000BASE-T	1Gbps	〃	UTP 4 対 CAT5/5e、RJ-45	
	IEEE8023an	10GBase-T	10Gbps	〃	UTP 4 対 CAT6/6a/7、RJ-45	
光ファイバー	IEEE802.3u	100BASE-FX	100Mbps	400m	MMF	
	IEEE802.3z	1000BASE-SX	1Gbps	550m	〃	
		1000BASE-LX	〃	〃	〃	
			〃	10Km	SMF	
	IEEE802.3ae	10GBASE-LX4	10GBbps	240m	MMF	
			〃	10Km	SMF	
		10GBASE-SR	〃	300m	MMF	
		10GBASE-LR	〃	10Km	SMF	
		10GBASE-ER	〃	40Km	〃	
		10GBASE-SW	〃	300m	MMF	
		10GBASE-LW	〃	10Km	SMF	
		10GBASE-EW	〃	40Km	〃	

5）ストレートケーブルとクロスケーブル

同軸ケーブル、光ファイバーケーブルには無いが、ツイストペアケーブルには 2 台のパソコンの LAN 端子（RJ-45）同士を LAN ケーブルで接続するためのクロスケーブルがある。



ストレートケーブル（一般の接続用）



クロスケーブル（PC×2 台の相互接続用）

5.　コマンドプロンプトについて

コマンドプロンプトとは、キーボードを用いた C U I（Character User Interface）によるコマンドインタプリタにおいて、「命令の入力を促す」ための文字列をいう。

特に Windows NT 系 OS（2000/XP/Vista/7）において、は CUI 環境からアプリケーションを実行させるための機能をいう。

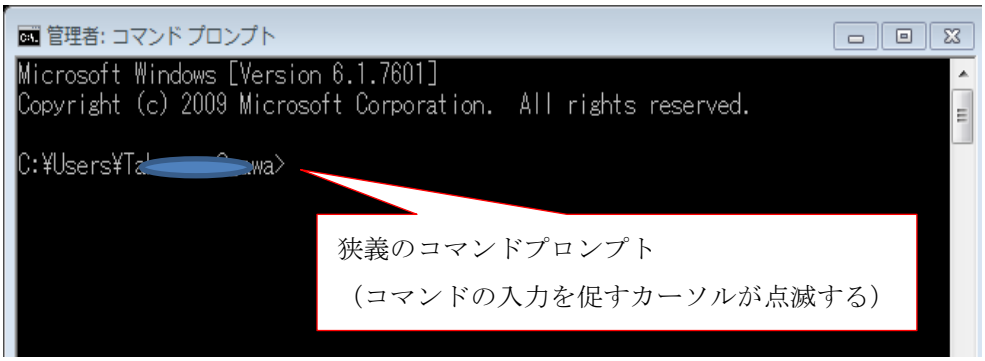
（参考）Windows 9.x 系 OS（95/98/Me）以前は、DOS コマンドと呼んでいた。

5.1.　コマンドプロンプトの操作方法

1）コマンドプロンプトの起動

コマンドプロンプトの起動は次の手順で行う。

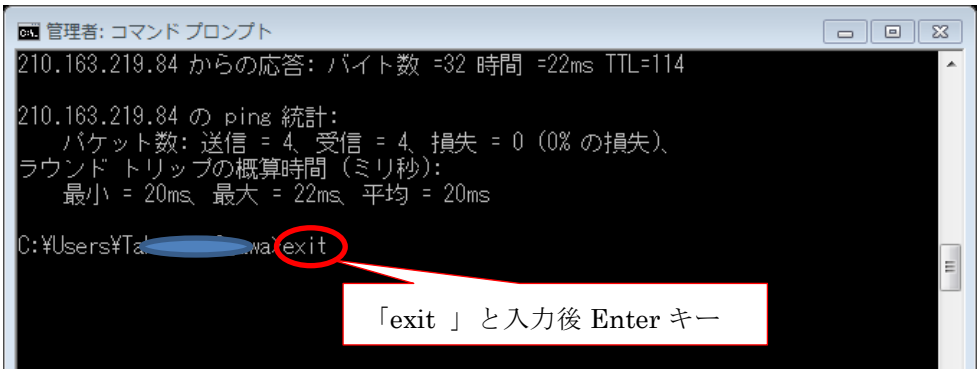
①　［スタート］→［すべてのプログラム］
　→［アクセサリ］→［コマンドプロンプト］



2）コマンドプロンプトの終了

コマンドプロンプトの終了は次の手順で行う。

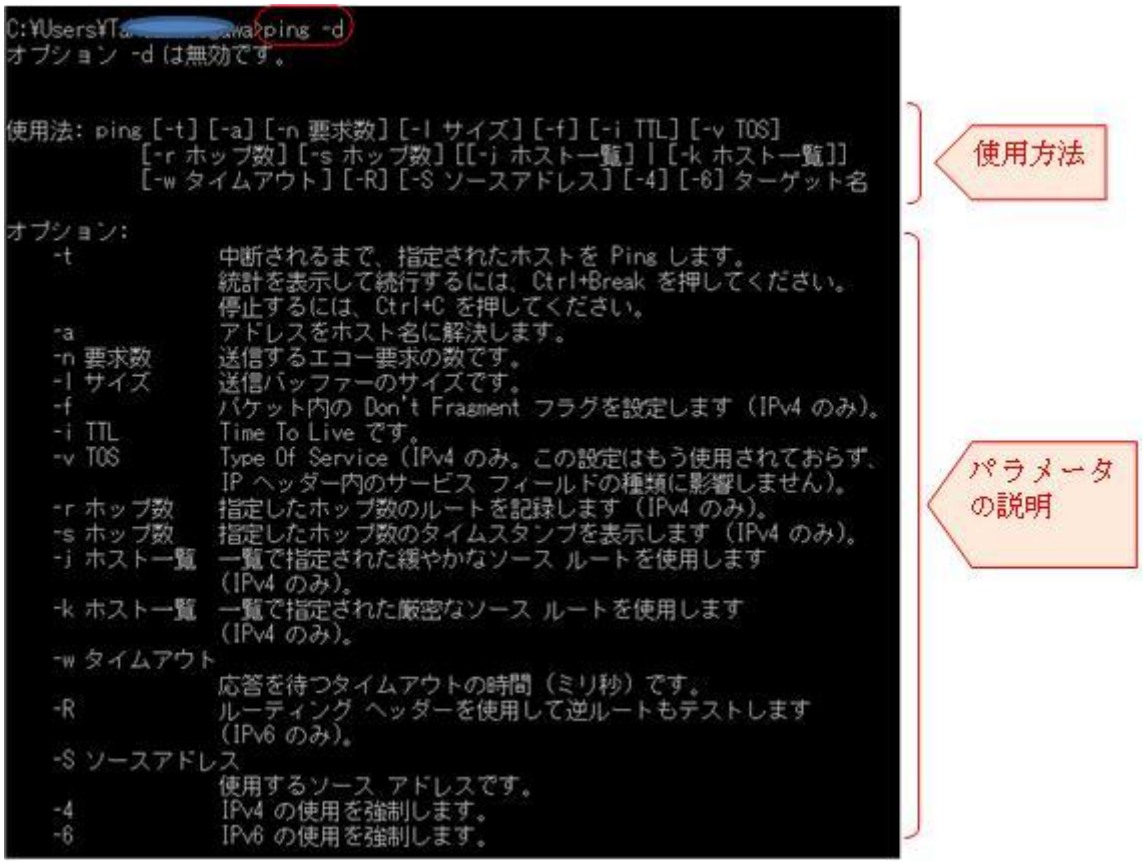
① コマンドプロンプトのカーソル位置に「exit 」と入力し Enter キーを押す



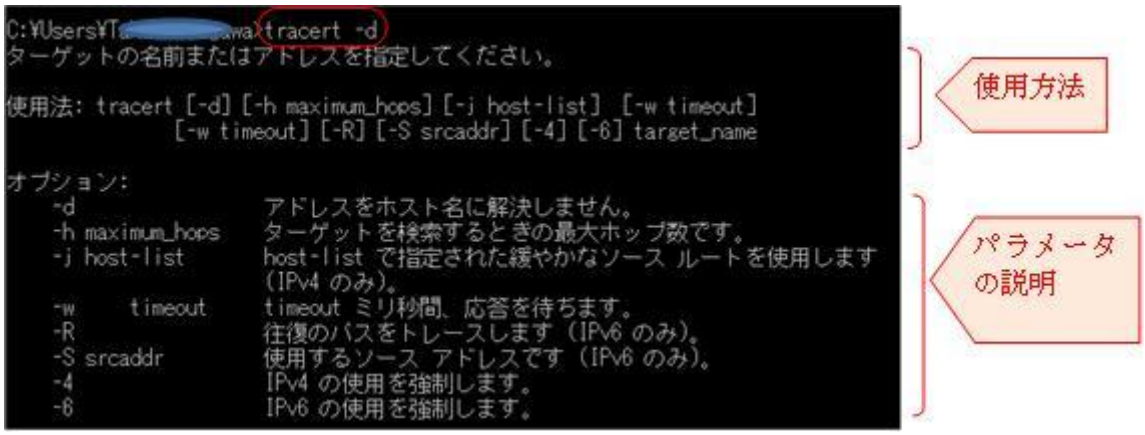
3）コマンドの使用方法を調べる

コマンドプロンプトのカーソル位置に、「**コマンド名 /?**」を入力し Enter キーを押す

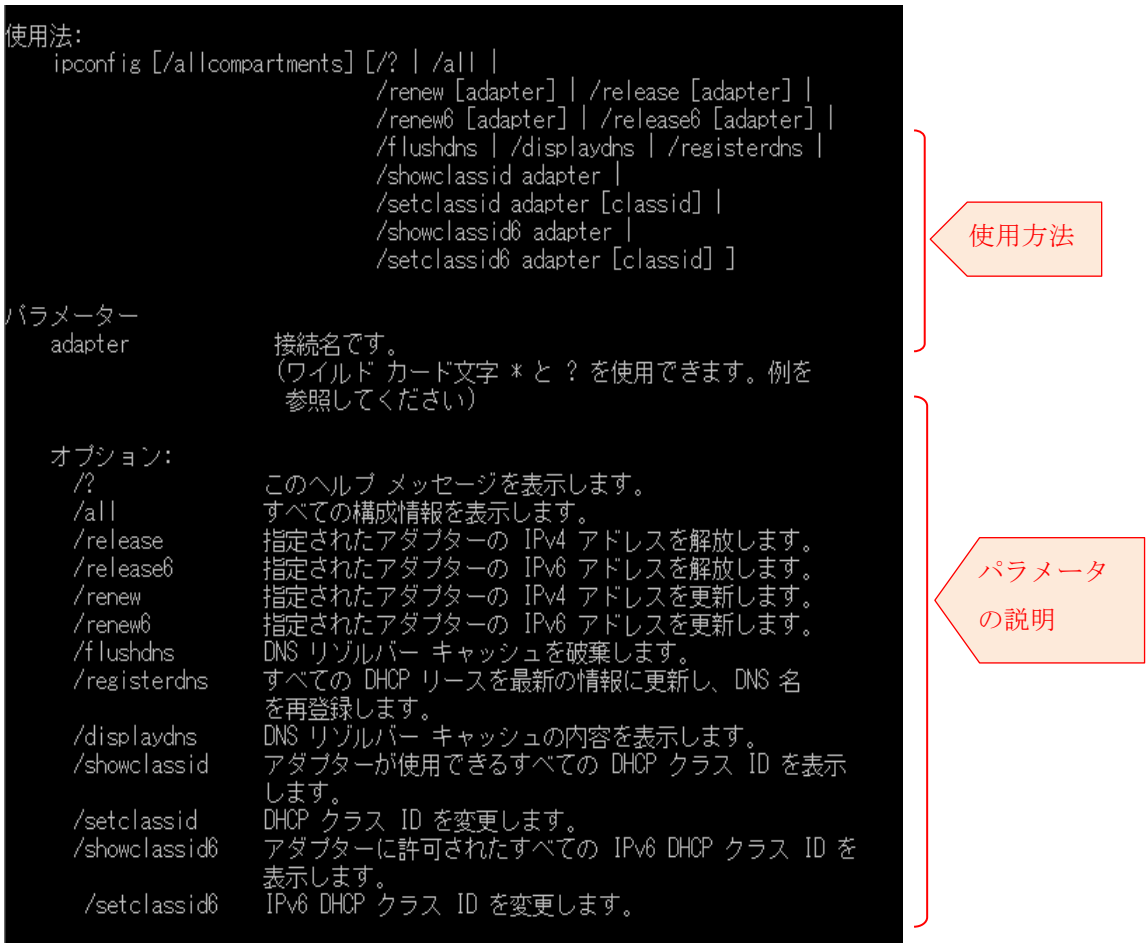
【使用例１】 「ping –d 」と入力する



【使用例２】　「tracert /? 」と入力する



【使用例３】　「ipconfig /？ 」と入力する



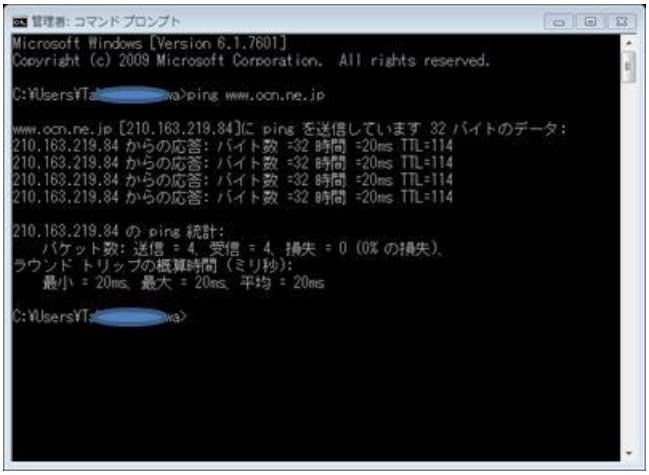
5.2.　コマンドプロンプトのコピーと貼り付け

コマンドプロンプトについての各種の資料を見ると、多くの資料が黒地に白文字のコマンドプロンプト画面を［Print Screen］でコピーした後に貼り付けるか、あるいは Word 2010 の［挿入］→［スクリーンショット］で取り込む方法を採っている。

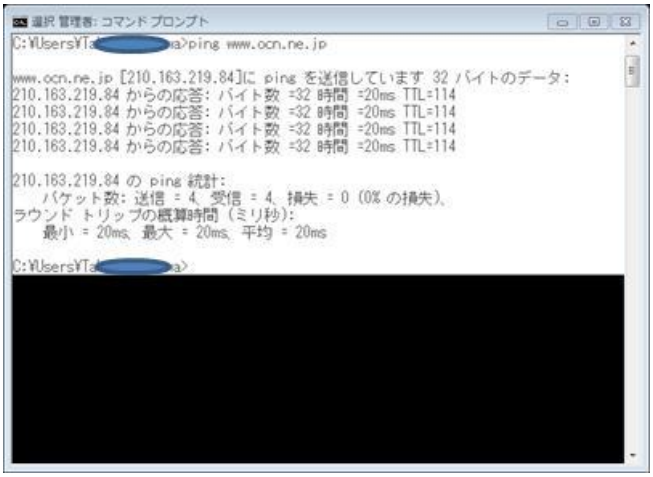
ここでは、コマンドプロンプト画面のテキストを黒文字の文字として［クリップボード］にコピーした後に貼り付ける方法について説明する。

1）コマンドプロンプトのすべての文字をコピーする方法

① コマンドプロンプト画面内を右クリックして、メニューを表示する



② ［すべて選択］をクリックすると、テキストがある領域全体が白黒反転する



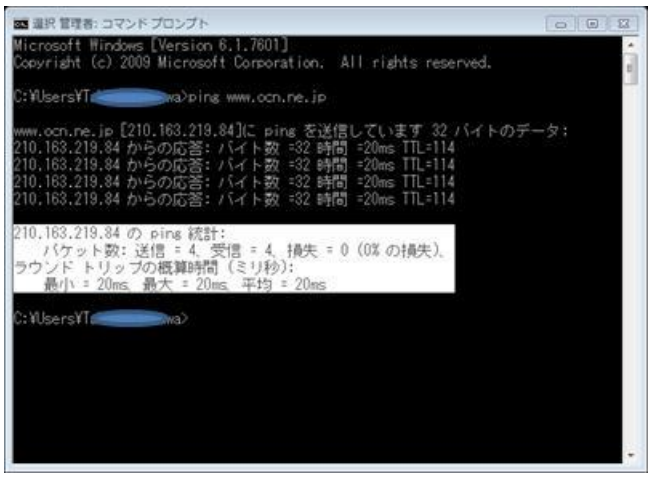
③ Enter キーを押すと、白黒反転した領域のテキストを［クリップボード］にコピーすると共に、白黒反転が元に戻る。

④ ［クリップボード］のテキストを Word 等に貼り付ける。

2）コマンドプロンプトの選択範囲のテキストをコピーする方法

① コマンドプロンプト画面内を右クリックして、メニューを表示する

② ［範囲選択］をクリック



③ 選択するテキストをドラッグして範囲選択すると、選択した範囲のテキストが白黒反転する

④ Enter キーを押すと、白黒反転した領域のテキストを［クリップボード］にコピーすると共に、白黒反転が元に戻る

⑤ ［クリップボード］のテキストを Word 等に貼り付ける。

5.3.　ネットワーク系コマンドの使用例

ここでは、よく知られているネットワーク系のコマンドについて、その使用例を説明する。

１）pingコマンド

ping コマンドは、URL で指定したホストに接続できるかどうかを確認し、併せて指定ホストとの間の回線の状況を知る。

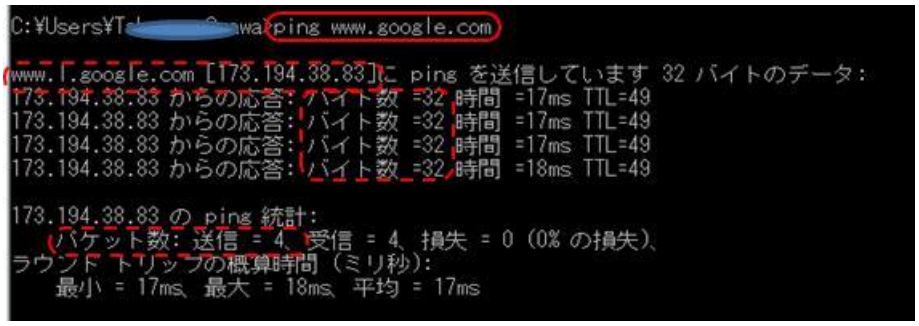
（補足）ping コマンドは、ネットワーク層（第 2 層）の ICMP（RFC792）が提供する“echo request”パケットを指定ホストに送信し、“echo reply”が返ってくるまでの時間や応答率から回線の状況を調べている。

【使用方法】

ping [-t] [-a] [-n 要求数] [-l サイズ] [-f] [-i TTL] [-v TOS] [-r ホップ数] [-s ホップ数]
[[-j ホスト一覧] | [-k ホスト一覧]] [-w タイムアウト] [-R] [-S ソースアドレス] [-4] [-6]
ターゲット名

【使用例１】　「ping www.google.com 」と入力

既定値　-n（エコー要求回数）＝4 回、-l（パケットサイズ）＝32B



（コメント）・入力した URL（www.google.com）が DNS の CNAME レコード（URL の名前から正規の名前を取り出す変換レコード）で www.1.google.com に変換されている。

・www.1.google.com の IP アドレスは 173.194.38.113 である。

・エコー要求回数に既定値の 4 回が、パケット長に既定値の 32B が用いられている。

・ 4 回すべてエコー応答を受信し、所要時間が 17~18ms（平均 17ms）であり、15（＝64－49）のルータを経由している。

【使用例２】　「ping www.google.com　-n 6　-l 1400 」と入力

-n（エコー要求回数）＝6 回、-l（パケットサイズ）＝1400B

（コメント）・入力した URL（www.google.com）が DNS の CNAME レコード（URL の名前から正規の名前を取り出す変換レコード）で www.1.google.com に変換されている。
・www.1.google.com の IP アドレスは 173.194.38.113 である。
・エコー要求回数が「-n 6」の入力で 6 回に、パケット長が「-l 1400」の入力で 1400B になっている。
・6 回すべてエコー応答を受信し、転送するパケット長が大きくなったので所要時間が 20~20ms（平均 20ms）と長くなり、15（＝64－49）のルータを経由している。

2）tracert（トレースルート）コマンド

Tracert コマンドは、ICMP を利用したネットワーク系コマンドであり、自ホストから指定ホストまでに中継したルータ（ゲートウェイ等）中継時間を表示するコマンドである。

- ネットワーク障害時に、障害区間の調査などに利用できる
- ハッカーからの攻撃時に、ハッカーからの攻撃経路の把握に利用できる

【使用方法】

tracert [-d] [-h maximum_hops] [-j host-list]　[-w timeout] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

【使用例】　「**tracert www.google.com** 」と入力

（注）ターゲット名「www.google.com 」を IP アドレス「173.194.38.115」に替えて入力しても同じである。

```
C:¥Users¥Takuzou Ogawa>tracert www.google.com

www.l.google.com [173.194.38.115] へのルートをトレースしています
経由するホップ数は最大 30 です:

  1    <1 ms    <1 ms    <1 ms  192.168.24.1
  2     *        *        *     要求がタイムアウトしました。
  3     6 ms     7 ms     6 ms  125.206.140.193
  4     6 ms     8 ms     6 ms  118.23.129.245
  5     8 ms     9 ms     7 ms  118.23.85.5
  6     6 ms     7 ms     6 ms  211.129.29.17
  7     6 ms     7 ms     6 ms  61.207.14.221
  8    11 ms     8 ms     9 ms  125.170.96.57
  9    13 ms    15 ms    13 ms  122.1.245.17
 10    17 ms    15 ms    15 ms  122.1.245.10
 11    16 ms    15 ms    15 ms  118.23.168.22
 12    16 ms    15 ms    16 ms  118.23.146.234
 13    31 ms    18 ms    18 ms  211.129.61.30
 14    17 ms    18 ms    17 ms  209.85.241.90
 15    18 ms    20 ms    17 ms  209.85.251.239
 16    17 ms    19 ms    17 ms  nrt19s18-in-f19.1e100.net [173.194.38.115]

トレースを完了しました。
```

（コメント）・入力した URL（www.google.com）が DNS の CNAME レコード（URL の名前から正規の名前を取り出す変換レコード）で www.1.google.com に変換されている。
・www.1.google.com の IP アドレスは 173.194.38.115 である。
・各ルータの中継時間は、3 回ずつ測定されて、その結果を表示する。
・1 番目（出発点）は、デフォルトゲートウェイの「192.168.24.1」である。
・2 番目（フレッツ光のマンション内分割用ルータ？）で、タイムアウトが発生？
・16 番目（到着点）は、173.194.38.115(＝www.1.google.com)である。

・16 番目にある「nrt19s18-in-f19.le100.net」は、DNS らしい（？）

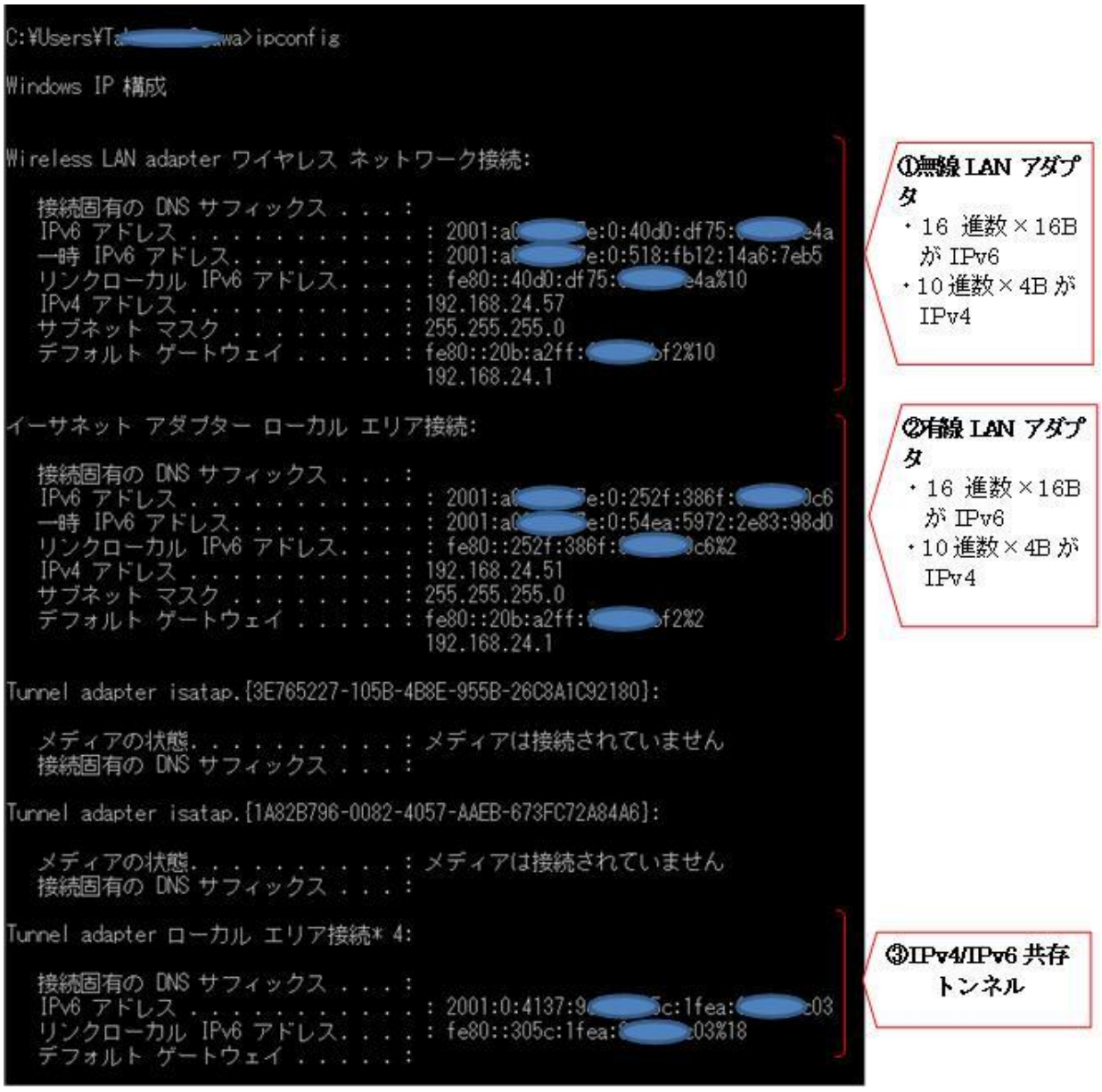
3）ipconfig（アイピーコンフィグ）コマンド

ipconfig コマンドは、パソコン（装着された通信アダプタ毎）に設定されているネットワーク接続情報（IP アドレス、サブネットマスク値、デフォルト･ゲートウェイ、DNS サーバ、MAC アドレス等）を確認し、あるいは必等に応じて設定値を変更できる。

【使用方法】

Ipconfig [/allcompartments] [/? | /all |
/renew [アダプタ] | /release [アダプタ] | /renew6 [アダプタ] | /release6 [アダプタ] |
/flushdns | /displaydns | /registerdns | /showclassid adapter |
/setclassid アダプタ[クラス ID] | /showclassid6 adapter |
/setclassid6 adapter [classid]]

【使用例１】 「ipconfig 」と入力



（コメント）　**① 無線 LAN アダプタ**

以下、接続されている無線 LAN アダプタのネットワーク構成について説明する。

- **［IPv6 アドレス］**は、ネットワークアダプタ（例では無線 LAN アダプタ）に割り当てた IPv6 のグローバル･ユニキャスト･アドレスである

  （私見）下位 64bit（4B）のインタフェース ID 設は、MAC アドレスを基に自動設定（Modified EUI-64、IEEE 規格）したものではないので、DCHPv6 を利用して設定したものらしい

- **［一時 IPv6 アドレス］**は「匿名アドレス」とも呼ばれていて、ネットワークアダプタ（同上）に一時的に割り当てた IPv6 のグローバル･ユニキャスト･アドレスであり、自動的に生成され自動的に更新される

  ［一時 IPv6 アドレス］は、セキュリティを考慮して使用される IPv6 アドレスであり DNS への登録はなく、自分から始める通信の送信元アドレスとして優先的に使用する。

  （補足）下位 64bit のインタフェース ID は、有効期限（推奨値で 24 時間、最大で 7 日間）を過ぎると自動的に再生成することでセキュリティ対策としている

  また、Windows を起動した時にも自動的に再生成される

- **［リンクローカル IPv6 アドレス］**は、ネットワークアダプタ（同上）に自サブネット内だけの通信用に割り当てた IPv6 のグローバル･ユニキャスト･アドレスであり、IPv4 のプライベート･アドレスに相当する

  なお［リンクローカル IPv6 アドレス］の後ろにと表示されている「%nn」は、実装されているネットワークアダプタがある場合に、アダプタを識別するため記号である

- **［IPv4 アドレス］**は、ネットワークアダプタ（同上）に割り当てた IPv4 のプライベート･アドレスである

- **［サブネット･マスク］**は、ネットワークアダプタ（同上）に割り当てた IPv4 のサブネット･マスクである

  サブネット･マスクと IPv4 アドレスの AND（論理積）演算でネットワークアドレスとホストアドレスを識別できる

- **［デフォルト･ゲートウェイ**（上段）］は、自サブネットからの出入り口の内側のリンクローカル IPv6 アドレスであり、この出入口の外側にはグローバル･ユニキャスト･アドレスの IPv6 が付与されている

- **［デフォルト･ゲートウェイ**（下段）］は、自サブネットからの出入り口の内側のプライベート IPv4 アドレスであり、この出入口の外側にはグローバル IPv4 アドレスが付与されている

（コメント）　**② 有線 LAN アダプタ**

以下、接続されているイーサネットアダプタのネットワーク構成について説明する。

なお詳細な説明は、**① 無線 LAN アダプタ**　を参照すること

- **［IPv6 アドレス］**は、ネットワークアダプタ（例ではイーサネットアダプタ）に割り当てた IPv6 のグローバル･ユニキャスト･アドレスである
- **［一時 IPv6 アドレス］**は「匿名アドレス」とも呼ばれていて、ネットワークアダプタ（同上）に一時的に割り当てた IPv6 のグローバル･ユニキャスト･アドレスであり、自動的に生成され自動的に更新される
- **［リンクローカル IPv6 アドレス］**は、ネットワークアダプタ（同上）に自サブネット内だけの通信用に割り当てた IPv6 のグローバル･ユニキャスト･アドレスであり、IPv4 のプライベート･アドレスに相当する
- **［IPv4 アドレス］**は、ネットワークアダプタ（同上）に割り当てた IPv4 のプライベート･アドレスである
- **［サブネット･マスク］**は、ネットワークアダプタ（同上）に割り当てた IPv4 のサブネット･マスクである
- **［デフォルト･ゲートウェイ**（上段）］は、自サブネットからの出入り口の内側のリンクローカル IPv6 アドレスであり、この出入口の外側にはグローバル･ユニキャスト･アドレスの IPv6 が付与されている
- **［デフォルト･ゲートウェイ**（下段）］は、自サブネットからの出入り口の内側のプライベート IPv4 アドレスであり、この出入口の外側にはグローバル IPv4 アドレスが付与されている

（コメント）　**③ IPv4/IPv6 共存トンネル**

- 「ipconfig /all」で調べたら Teredo（RFC4380）プロトコル用の IPv6 アドレスであった

（補足）　Teredo を使用すると、通信経路の途中に複数の IPv4 の NAT ルータ（プライベート IP 変換）（NAT）あっても、Teredo サーバと Teredo リレールータを利用して、IPv6 対応サーバとの通信を可能になる

なお、Teredo で使用する Teredo サーバや Teredo リレールータはマイクロソフト社などが設置している（このプロトコルの提案はマイクロソフト社）

・ 「**IPv6 アドレス**（上段）」は、Teredo 用の IPv6 のグローバル･ユニキャスト･アドレスである
・ 「**IPv6 アドレス**（下段）」は、Teredo 用の自サブネット内通信用の IPv6 のグローバル･ユニキャスト･アドレスである

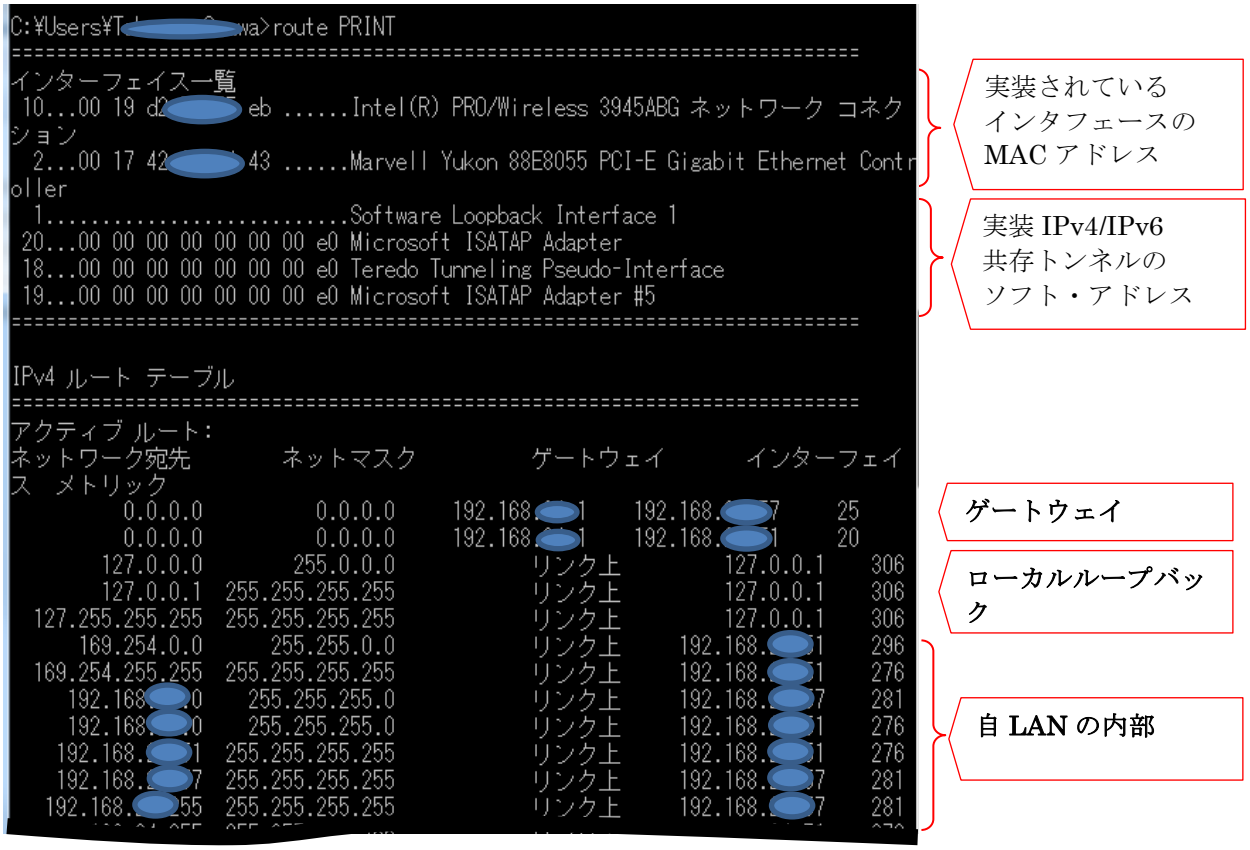
４）routeコマンド

route コマンドは、パソコンに設定されているルーティングテーブルの情報を確認できる。

【使用方法】

ROUTE [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]

【使用例】　「route PRINT 」と入力



（説明）［ネットワーク宛先］は宛先 IPv4 アドレス、［ネットマスク］はサブネットマスク、［ゲートウェイ］はデフォルトゲートウェイ、［インタフェース］は送信元 IPv4 アドレスを表している。なお［メトリック］は当該ルートの距離、ポップ数、負荷の尺度であり、値が少ないルートが優先して選択される。

- ［ネットワーク宛先］の 0.0.0.0 は全ての宛先を意味し、［ゲートウェイ］に 192.168.x. 1 が設定されていて、自 LAN から WAN への出入り口であるデフォルトゲートウェイを指している
- ［ネットワーク宛先］が 127.0.0.1～127.255.255.254 のルートは、ローカルループバックを指している。

  （補足）ローカルループバックは自分（インタフェース）から自分（同）へのループバック試験などで用いて TCP/IP プロトコルが有効であることが確認できる
- ［ネットワーク宛先］が 192.168.x.2～192.168.255.255 のルートは、自 LAN 内への直接接続を指している

6.　主なプロトコルのヘッダとフレームの構造

ここでは、TCP/IP プロトコルでデータのカプセル化に使用しているヘッダについて説明する。

1）TCP ヘッダの構造

位置	サイズ	名称	説明
0	2B	送信元ポート番号	送信元アプリケーションを通知
2	2B	宛先ポート番号	宛先アプリケーションを指定
4	4B	シーケンス番号	送信データの先頭（0）からのバイト位置
8	4B	確認応答番号	正常受信し次に受信したいデータのバイト位置
12	4bit	ヘッダ長	データのバイト位置（＝20+4n）
	6bit	予約	予備
	6bit	コードビット	制御ビット（緊急、ACK、同期、終了等）
14	2B	ウィンドウサイズ	受信バッファのサイズ（Max.65,535B）
16	2B	チェックサム	TCP セグメント全体のチェック
18	2B	緊急ポインタ	緊急データのバイト位置
	0～4nB	オプション	MSS のやり取りその他に使用
20+4n		データ	
		FCS	フレーム　チェック　シーケンス Frame Check Sequence（CRC 方式で使用）

2）IPｖ4 ヘッダの構造

位置	サイズ	名称	説明
0	4bit	バージョン	IPv4 は 4
	4bit	ヘッダ長	20+4nB
1	1B	サービスタイプ	7～5bit：優先度、4~0bit：TOS
2	2B	パケット長	IP ヘッダ＋データ
4	2B	識別子	パケット識別番号（パケット分割時の識別用）
6	3bit	フラグ	6bit：フラグメント禁止、5bit：継続フラグメント有り
	13bit	フラグメントオフセット	フラグメント先頭のバイト位置
8	8bit	生存時間	最大通過ルータ数
	8bit	プロトコル番号	TCP=6、UDP=11、ICMP=1
10	2B	ヘッダチェックサム	IPv4 ヘッダの誤りチェック
12	4B	送信元アドレス	送信元 IP アドレス
16	4B	宛先アドレス	宛先 IP アドレス
20	0～4nB	オプション	後半の不要部はパディング
20+4n		データ	

3）IP v 6 ヘッダの構造

位置	サイズ	名称	説明
0	4bit	バージョン	IPv6 は 6
	8bit	優先度	IPv4 の［サービスタイプ］に相当
	20bit	フローラベル	IPv6 ルータに特別処理を要求するパケット用の識別ラベル（現在はまだ実験段階であり、詳細は未定）
4	2B	ペイロード長	データのバイト長
6	1B	次ヘッダ	IPv4 のプロトコル番号に相当
7	1B	ホップリミット	IPv4 の生存時間に相当
8	16B	送信元アドレス	送信元 IP アドレス
24	16B	宛先アドレス	宛先 IP アドレス
40		データ	

4）イーサネットヘッダの構造

位置	サイズ	名称	説明
-8	8B	プリアンブル	信号の同期用（10101010 10101010 …10101011）
0	6B	宛先アドレス	宛先 MAC アドレス
6	6B	送信元アドレス	送信元 MAC アドレス
12	2B	タイプ	上位プロトコル（例：IPv4=0x0800、IPv6＝86DD、ARP=0x0806、RARP=0x8035、PPPoE（Discovery）＝0 x 8863、PPPoE（Session）＝0x8864 等
14	46～1500	データ	
		FCS	宛先アドレスの先頭～データの最後の CRC

5）PPP ヘッダの構造

位置	サイズ	名称		説明
-3	3B	プリアンブル		信号の同期用（01111110 11111111 00000011）
0	2B	プロトコル		上位プロトコル（例、IPv4＝0x0021、IPCP＝0x8021、LCP=0xC021、PAP=0xC023、CHAP=0xC223 等）
2	1B	データ	コード	例：設定要求＝1、ACK=2、NACK=3、拒否＝4、終了要求＝5、終了応答確認＝6 等
3	1B		ID 番号	セッション識別用の番号
4	2B		長さ	データ部の長さ
6	nB		データ	
6+n	2B	FCS		プロトコルの先頭～データの最後の CRC
8+n	1B	フラグ		0x7E（01111110）

6）PPPoE ヘッダの構造

位置	サイズ	名称	説明
-8	8B	プリアンブル	信号の同期用（10101010 10101010 …10101011）
0	6B	宛先アドレス	宛先 MAC アドレス
6	6B	送信元アドレス	送信元 MAC アドレス
12	2B	タイプ	上位プロトコル（例：PPPoE（Discovery）＝0 x 8863、PPPoE（Session）＝0x8864）
14	4+nB	データ	
		FCS	宛先アドレスの先頭～データの最後の CRC
		フラグ	

7.　通信回線について

7.1.　光ファイバー回線

ここでは NTT 西日本のフレッツ光の光通信サービスを例にして光ファイバー回線でのインターネット接続について説明する。

NTT 西日本のフレッツ光には従来技術の「フレッツ光プレミアム」と次世代技術の「フレッツ光ネクスト」があり、それぞれにファミリタイプ（戸建て住宅向け）とマンションタイプ（集合住宅向け）がある。

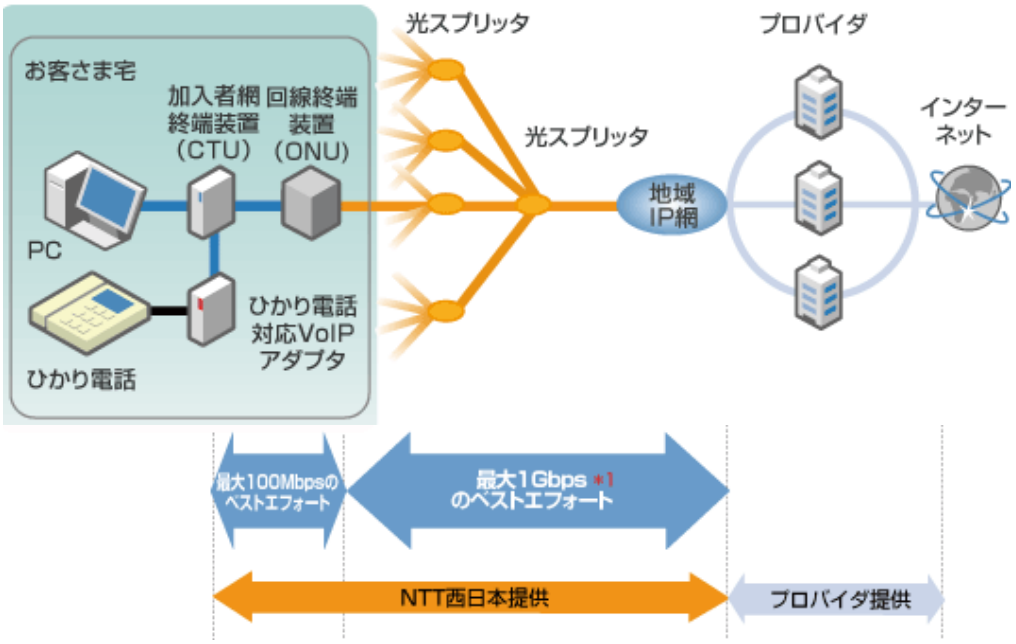
ここでは、フレッツ光ファミリータイプ（2012.3.31 販売終了）、マンションタイプ（VDSL 方式）、フレッツ光ネクスト・ファミリー・ハイスピードタイプの概要を説明する。

1）フレッツ・光プレミアム　ファミリータイプ

「フレッツ・光プレミアム」は、NTT 西日本ビルからユーザ宅までを最大 1Gbps（ギガ）の光回線で接続し、光スプリッタで複数のユーザで共有するサービスであり、上り／下りとも最大 100Mbps の通信サービスを提供する。接続イメージは下図のとおりであり、各通信機器の役割は次のとおりである。

- 光回線終端装置（ONU：Optical Network Unit（オプティカル ネットワーク ユニット））は、光通信の光信号とイーサネットの電気信号との変換をする通信機器
- 加入者網終端装置（CTU：Customer Terminal Unit（カスタマー ターミナル ユニット））は、ブロードバンドルータに相当する通信機器

  【重要】CTU はブロードバンドルータである。そのため CTU に無線 LAN（親機）を接続する場合は、ルータ機能が二重接続にならないよう、無線 LAN の「モード切り替えスイッチ（機種で名称が異なる）」を「アクセスポイント（AP or BRI 等名称が異なる）」に切り替えて使用すること。
- 光電話対応 VoIP（Voice over Internet Trotocol（ボイス オーバ インターネット プロトコル））は、インターネットの TCP/IP ネットワークを用いて音声データを送受信する通信機器であり、光電話（050-*****）にも対応可能

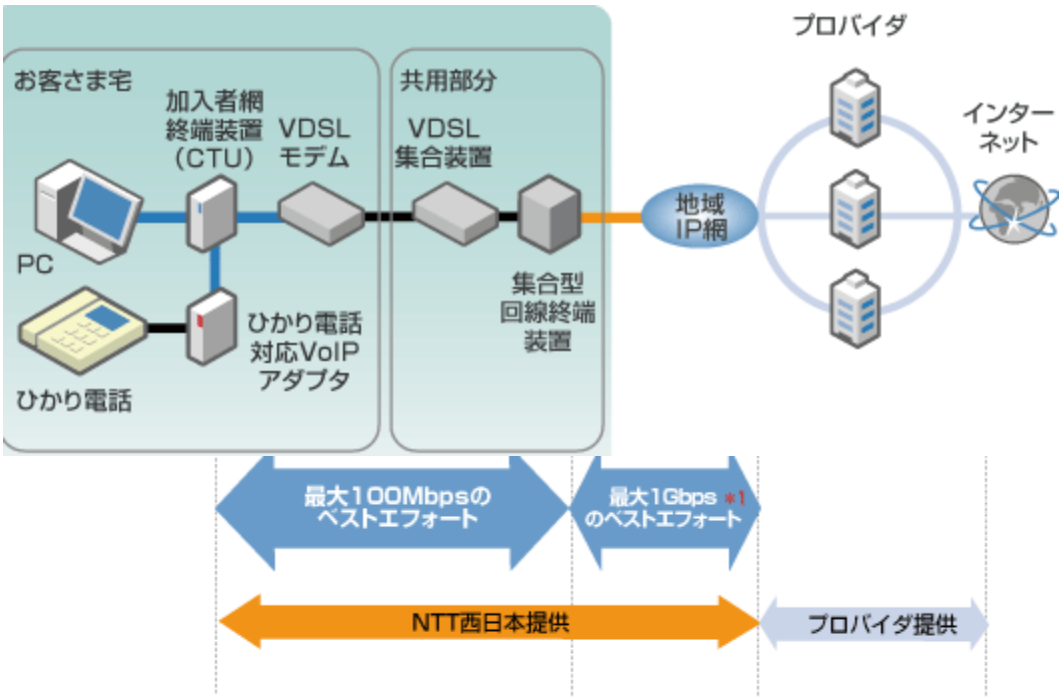


2）フレッツ・光プレミアム　マンションタイプ（VDSL 方式）

「フレッツ・光プレミアム」は、NTT 西日本ビルからユーザ宅までを最大 1Gbps（ギガ）の光回線で接続し、光スプリッタで複数のユーザで共有するサービスであり、上り／下りとも最大 100Mbps の通信サービスを提供する。接続イメージは下図のとおりであり、各通信機器の役割は次のとおりである。

- 共用部分の集合型光回線終端装置は、マンション管理室の MDF 近辺に設置され、光回線とイーサネットのメディア変換を行う通信機器
- 共用部分の集合 VDSL 装置は、マンション管理室の MDF 近辺に設置され、イーサネットのケーブルの電気信号を VDSL の電気信号に変換する通信機器であり、MDF に収容されている既設のユーザ電話回線に接続する
- ユーザ宅の VDSL（Very high speed Digital Subscriber Line（ベリー ハイ スピード ディジタル サブスクライバ ライン）、高速デジタル加入者回線）モデムは、既設の電話回線の VDSL の電気信号をイーサネットの電気信号に変換する通信機器である
- ユーザ宅の加入者網終端装置（CTU：Customer Terminal Unit（カスタマー ターミナル ユニット））は、ブロードバンドルータに相当する通信機器

  【重要】CTU はブロードバンドルータである。そのため CTU に無線 LAN（親機）を接続する場合は、ルータ機能が二重接続にならないよう、無線 LAN の「モード切り替えスイッチ（機種で名称が異なる）」を「アクセスポイント（AP or BRI 等名称が異なる）」に切り替えて使用すること。
- 光電話対応 VoIP（Voice over Internet Trotocol（ボイス オーバ インターネット プロトコル））は、インターネットの TCP/IP ネットワークを用いて音声データを送受信する通信機器であり、光電話（050-*****）にも対応可能



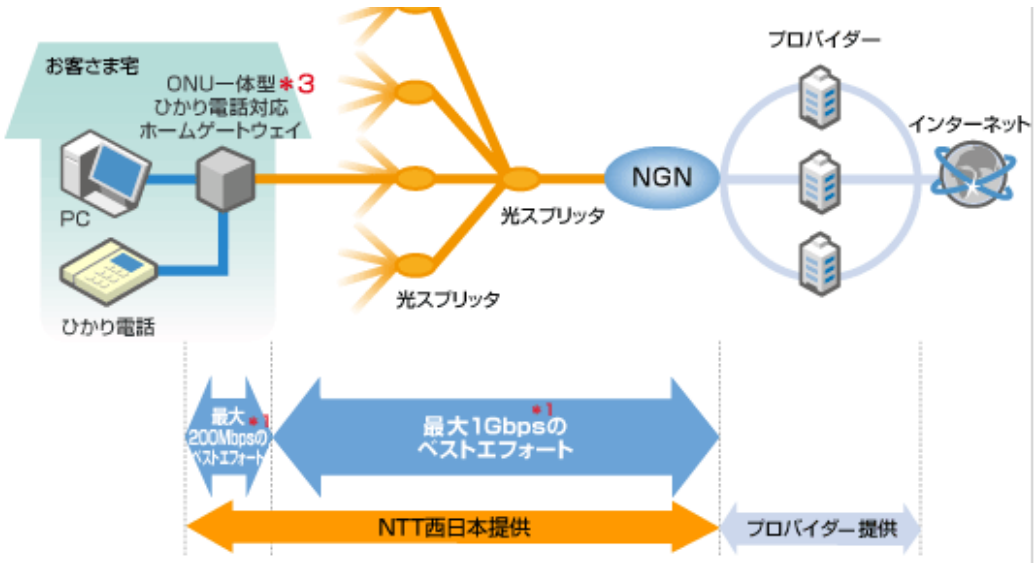
3）フレッツ光ネクスト・ファミリー

なおフレッツ光ネクスト・ファミリーには、最大スペード別に次の 3 タイプがある。

- ファミリー・エクスプレスタイプ：最大概ね 1Gbps（*1）の高速通信
- ファミリー・ハイスピードタイプ：最大 200Mbps（*1）の高速通信
- ファミリータイプ：最大 100Mbps（*1）の高速通信（2012.3.31 に販売終了した「フレッツ光プレミアム・ファミリータイプ」の後継のサービスともいえる）

ここでは、フレッツ光ファミリー・ハイスピードタイプについて説明する

・ ONU 一体型ひかり電話対応ホームゲートウェイは、光回線終端装置（ONU：光通信とイーサネット通信の変換をする通信機器）、ブロードバンドルータ、光電話アダプタ（イーサネット通信を電話通信に変換する通信機器）を合体した装置



7.2. ADSL

xDSL（ディーエスエル　デジタル　サブスクライバ　ライン Digital Subscriber Line、デジタル加入者線）は単に DSL とも言い、電話回線を用いて高速デジタル通信を行う技術の総称であり、音声通話（0.3～3.4KH z）で用いられていない高い周波数領域（ADSL の場合 25.875～138～1,104KHz）を用いることで高速なデジタル通信を行う技術である。

xDSL には、**ADSL**（Asymmetric（アシンメトリック） DSL：非対称デジタル加入者線）、SDSL、HDSL、**VDSL**（超高速デジタル加入者線）、RADSL 等の方式がある。

ここで説明する ADSL は、上り（最大 5Mbps）と下り（最大 47Mbps）の速度が等しくないことから非対称な DSL と言われている。

ADSL の通信業者には、ソフトバンク BB、Yahoo! BB、NTT 東、NTT 西、イー・アクセス等があるが、ここでは NTT 西日本のフレッツ ADSL を例にして説明する。

- NTT ビル内に ISP（プロバイダ）が設置した ADSL 収容ビル装置からのデータ信号と交換機からの音声信号をスプリッタで混合して電話回線に送信し、逆に受信した混合信号をスプリッタで分波してデータ信号を ADSL 収容ビル装置に送信し、音声信号を交換機に送信する
- NTT ビルからユーザ宅までの通信回線は、既存の電話回線をそのまま使用する
- ユーザ宅のスプリッタは、低い周波数の音声信号とデータ通信の高い周波数のディジタルデータ信号を分離させる分波機能、逆に音声信号とディジタルデータ信号を混合する機能を併せ持つ通信機器
  - ➢ スプリッタの TEL 端子（低い周波数の音声信号）を電話機に接続して、交換機を介した電話通信を行う
  - ➢ DATA 端子（高い周波数のデータ信号）を ADSL モデムに接続して、データ通信を行う
- ADSL モデムは、スプリッタからの ADSL 信号をイサ―ネットのデータ信号に変換するモデム機能の他に、ブロードバンドルータ機能を内蔵している

【重要】ADSL モデムはブロードバンドルータ機能を内蔵している。そのため ADSL モデムに無線 LAN（親機）を接続する場合は、ルータ機能が二重接続にならないよう、無線 LAN の「モード切り替えスイッチ（機種で名称が異なる）」を「アクセスポイント（AP or BRI 等名称が異なる）」に切り替えて使用すること。