ネットワーク･プロトコルの概要

パソ救・勉強会資料　2012(H24).9.23　まなび北新

2012(H24).8.30　*T.Ogawa*

Windows パソコンは、Windows、ネットワーク、ハードウェア、アプリケーションの技術に支えられている。このうち Windows については 2011/10 の「Windows の仕組み」で勉強したので、今回はネットワークについて勉強する。

勉強会では筆者がネットワークを理解するために作成した「ネットワーク･プロトコルについて（入門）」を基に、要点を取りまとめ編集した「ネット―ワーク･プロトコルの概要」を使用する。

資料作成にあたっては、**Wikipedia**（フリー百科事典）、**ITPro**（日経 BP 社）、**@IT**（アイティメディア社）、**ASCII.jp×TECH**（アスキー･メディアワークス社）、**All About From**（オールアバウト社）、マイクロソフト社の **Web サイト**、IT 用語辞典の **e-Words**、IT 用語辞典の **BINARY** 等々の最新 Web 記事（Word に変換して約 1000 頁）のを比較し参照しました。記事を公開してくださった各社に感謝いたします。
また、旧版ですが蔵書の通信関係の専門書数冊も参照しました。

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」と言いう。

1.1. ネットワーク･アーキテクチャの乱立と OSI

異なるメーカのコンピュータ間を相互に接続するのは困難であったので、それを解決するために、ISO（国際標準化機構）と ITU-T（国連内の電気通信連合・電気通信標準化部門）とが 1982 年に「（ＯＳＩ（オーエスアイ）（開放型システム間相互接続）」プロジェクトを作った。

1.2. OSI 参照モデルについて

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使われている「OSI 参照モデル」は、OSI プロジェクトの中で策定され 1984 年に承認された。

OSI 参照モデルにおけるプロトコルの 7 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	ユーザが利用するアプリケーションに関する取り決めである。 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	コンピュータ固有のデータ形式（文字コード、数値表現等）と通信共通のデータ形式（同）を相互に変換するための取り決めである。 相手コンピュータとやりとりするデータの文字コード変換、圧縮方式、暗号化／復号化等を規定する。
第５層	セッション層	アプリケーション間の通信で接続状態を制御し管理するための取り決めである。 アプリケーション間での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／再開等）を規定する。
第４層	トランスポート層	送信元から宛先に伝送されるデータが確実に相手コンピュータに届くことを保証するための取り決めである。 コンピュータ間のコネクション確立、エラー制御、フロー制御、セグメント分割、順序制御等について規定する。
第３層	ネットワーク層	送信元から宛先までデータを中継し伝送するための取り決めである。 送信元と宛先との間にある複数の経路を選択して、データリンク層の違いを吸収しつつ送信元ノードと宛先ノード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	通信媒体（ケーブル、無線塔）で直接つながっている隣接ノード（通信機器）間でデータを伝送するための取り決めである。 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	通信媒体に応じた信号の種類･内容やデータの伝送方式等に関する取り決めである。 物理的な接続のための電気信号、符号の変調方法等（例：コネクタ、ケーブル、電圧、変調、周波数、波形、暗号化等）を規定する。

1.3.　インターネット･プロトコル･スイート（TCP/IP プロトコル）

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、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。

TCP/IP プロトコルは、インターネットの普及に伴いデファクトスタンダード（事実上の標準）の地位を確立し、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。

【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	―	IEEE802 で規定

（参考）TCP/IP プロトコルを構成する個々のプロトコルは厳格な階層分類がなされていないので、説明者や筆者により異なる分類がなされることがある。

2.　プロトコル階層化とカプセル化

ここでは、TCP/IP プロトコルを例にしてカプセル化とカプセル解除の流れを説明する。

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

上位層から渡されたデータの前後にプロトコルで規定された情報（ヘッダ、トレーラ）を付加し、上位層のデータを包み込むことをカプセル化と言う。

① アプリケーション（第 4 層）は、プロトコル規定のアプリケーションデータを下位の TCP に渡す。

② TCP（第 3 層）は、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）単位に分割しながら、それぞれの分割データの前に TCP ヘッダを付加して TCP セグメントとしてカプセル化し、次々に下位の IP に渡す。

③ IP（第 2 層）は、受け取った TCP セグメントの前に IP ヘッダを付加して IP パケットとしてカプセル化し、下位のイーサネットに渡す。

④ イーサネット（第 1 層）は、受け取った IP パケットの前と後にイーサネットヘッダと FCS（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カプセル化し、下位の物理層を介して送信する。

2）宛先コンピュータでのカプセル化解除の流れ

送信元で付加された情報（ヘッダ、トレーラ）を参照し、包み込まれた上位層のデータを取り出すことをカプセル化解除（非カプセル化、逆カプセル化）と言う。

① イーサネット（第 1 層）は、下位の物理層を介して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、非カプセル化して IP パケットを取り出し、上位の IP に渡す。

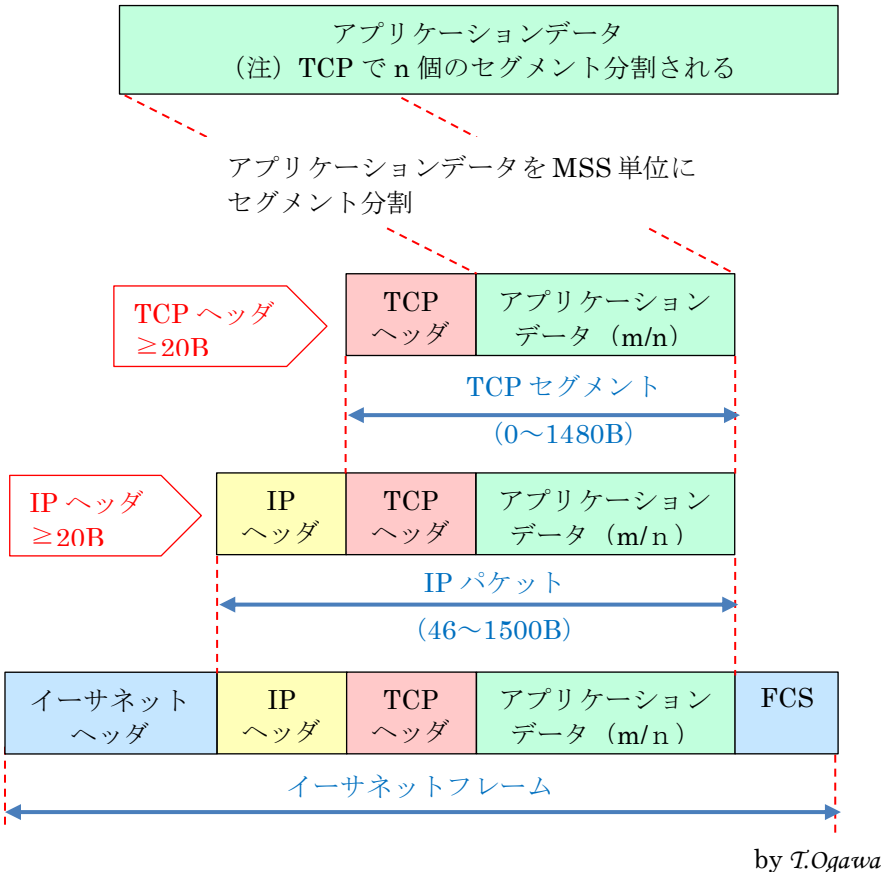
② IP（第 2 層）は、受け取った IP パケットの IP ヘッダを参照し、非カプセル化して TCP セグメントを取り出し、上位の TCP に渡す。

③ TCP（第 3 層）は、受け取った TCP セグメントの TCP ヘッダを参照し、非カプセル化しながら送信された順に組み立て直してアプリケーションデータを再現し、上位のアプリケーションに渡す。

④ アプリケーション（第 4 層）は、受け取ったアプリケーションデータを基にして、プロトコル規定の処理を行う。

2.2. カプセル化のイメージ図

前節の 1）項〔送信元コンピュータでのカプセル化の流れ〕で説明したカプセル化のイメージを次図に示す。



by *T.Ogawa*

3.　TCP/IP プロトコルの主なプロトコル

ここでは、次表に示す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
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	ARP、NDP、OSPF、L2TP（トンネリング）、PPP、PPPoE、MAC（イ―サネット、IEEE802.11、DSL、ISDN、FDDI）

3.1.　TCP/IP プロトコルの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

【表の説明】［備考］欄の上段はプロトコルの RFC 番号、中段の数字は対応アプリケーションのポート番号、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は、クライアント（パソコン等）と Web サーバ間でデータ転送を行って、Web ページを閲覧するためのプロトコルである。 ・ クライアントから Web サーバにリクエスト（指定データの転送要求、指定宛先へのデータ送信）を送信し、Web サーバはレスポンス（ハイパーテキスト、画像等）をクライアントに転送する	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は、クライアントからのメールを宛先の受信メールボックスに転送するためのプロトコルである。 ・ SMTP には 3 機能（クライアントからメールサーバへの転送、メールサーバ間の転送、受信メールボックスへの振分け）からなる	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 は、受信メールボックスに転送されたメールをクライアントが取り出すためのロトコルである ・ クライアントが取り出したメールはメールボックスから削除される	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は、受信メールボックスに転送されたメールにクライアントがアクセスするためのプロトコルである。 ・ 受信メールへのアクセスには、コピー、フラグ付加、削除等がある	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は、クライアントとサーバ間でファイルを転送するためのプロトコルである。 ・ クライアントが制御用ポートで「コマンド」を送り制御（フォルダ移動、ファイル送信、ファイル受信、ファイル削除等）を行いながら、データ用ポートでテータを転送する	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は、ドメイン名→IP アドレス変換、IP アドレス→ドメイン名変換を行うための階層的な分散型データベースに関するプロトコルである。 ・ DNS は、短いデータを UDP で送受信し高速処理を図っている	RFC1034、 RFC1035 53 UDP
ディーエッチシーピー D H C P	ドメイン ネーム システム Domain Name System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（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 サーバ等）を自動的に割り当てるためのプロトコルである。 ・ ブロードバンドルータや無線ルータ等は DHCP 機能を内蔵している	RFC2131 67（サーバ） 68（クライアント） UDP

2）第 3 層 トランスポート層の主なプロトコル

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 プロトコルの中核プロトコルである。 ・ 接続相手とのコネクションの確立、データ到着の確認、エラー制御、フロー制御、順序制御、データ重複／抜け検出等を行い信頼性が高い。 ・ 送信側 TCP は、アプリケーションから渡されたデータを MSS（最大セグメントサイズ）単位に分割し、分割データをカプセル化し TCP セグメントとして下位の IP に渡す	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は、信頼性を捨て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。 ・ 信頼性確保機能を持たず処理が速いため、DNS や DHCP で用いられる	RFC768

3）第 2 層 インターネット層の主なプロトコル

名称	プロトコルのフルネイムと概要	備考
アイピー I P	インターネット プロトコル Internet Protocol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 プロトコルの中核プロトコルである。 ・ IP ではルーティング（経路選択）機能、生存時間（TTL）機能、ヘッダ検査機能等を規定している ・ ルータを用いて異なる LAN、WAN、インターネットを相互接続して、IP パケットをバケツリレー式に中継して宛先まで伝送する	RFC791 （IPv4） RFC2460 （IPv6）
アイシーエムピー I C M P	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。 ・ 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り、エラーメッセージには、到達不能、パケット放棄、宛先不明等などがある	RFC792 （ICMPv4） RFC4443 （ICMPv6）

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

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）は、IEEE802.3 で標準化された LAN であり、リンク層のMAC（マック）フレームと物理層の CSMA/CD に関するプロトコルである ・ イーサネットは、TCP/IP が扱う MAC フレームを規定している	TCP/IP プロトコルの RFC と関係ない
ＰＰＰ（ピーピーピー）	Point（ポイント） to（トゥ） Point（ポイント） Protocol（プロトコル）は、通信回線を挟んだ 2 つの通信機器間でデータ通信を行うためのプロトコルである ・ ダイアルアップ接続（電話回線、ISDN 等）で使用されていて、2 点間のリンク確立（LCP）機能、ユーザ認証（PAP（パップ）、CHAP（チャップ））機能等を持っている	RFC1661 他
ＰＰＰｏＥ（ピーピーピーオーイー）	ＰＰＰ（ピーピーピー） ｏｖｅｒ（オーヴァー） Ethernet（イーサネット）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 ・ ブロードバンド（フレッツ光、フレッツ ADSL 等）接続のプロバイダ～ブロードバンドルータ（フレッツ光の CTU、フレッツ ADSL の ADSL モデム等）間のイーサネットで使用されていて、PPP が持つユーザ認証（PAP、CHAP ド）機能を利用してイーサネット環境上で実現する	RFC2516

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

1）IPv4 アドレスの枯渇と IPv6 への移行について

IPv4 は 32bit（ビット）（4 B（バイト））のアドレス空間を用いて最大 43 億個の IP アドレスを持つが、2011 年に枯渇した。このアドレス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、NAT（ナット）、CIDR（サイダー）等により IPv4 アドレスの節約と有効活用が図られてきた。

この資料を執筆中の 2012 年 6 月 6 日に、『World（ワールド） IPv6 Launch（ランチ）（世界の IPv6 開始）』イベントが催され、世界中の大手 Web サイトやプロバイダが一斉に IPv6 への対応を開始した。

2）IPv4 アドレスについて

(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、それぞれのブロックを 10 進数（0～255）で表記する
- 8bit の 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

(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
・ A（0 で始まる 8it）、B（10 で始まる 16bit）、C（110 で始まる 24bit）にクラス分け	・ クラス A は 24bit、クラス B は 16bit、クラス C は 8bit

(C) 「アドレスマスク」によるネットワークの分割

クラス A は 24bit で 16,777,225 個、クラス B は 16bit で 65,535 個ものホストアドレス持ち、アドレスに無駄が生じた。アドレス不足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へのアクセスに使用する IP アドレスであり、世界中に 1 つだけの IP アドレスである。

プライベート IP アドレスは自 LAN 内（家庭内、企業内等）だけで使用する IP アドレスであり、LAN が異なれば重複して使用できる

・ 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

「 /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（同 Ver.6）は、IPv4（32bit）の 4 倍の 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 アドレス持っているので、無限のアドレス空間と言われている。

(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 の 16 個の数字）で表記する。

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

10 進数	10	11	12	13	14	15
2 進数の 4 桁	1010	1011	1100	1101	1110	1111
16 進数の 1 桁	A	B	C	D	E	F

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

・ ブロックが“ 0 ”で始まる場合は、有効数字の前に続く“ 0 ”を省略できる（ゼロサプレス）

（例） 3ffe:2002:0021:0000:0009: 03ab:0000: ff01

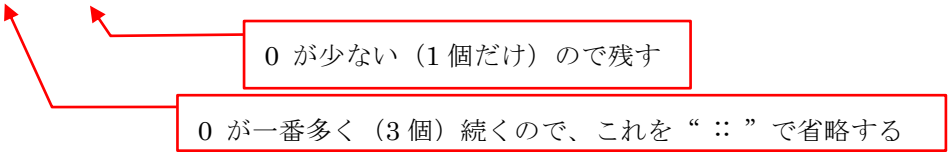
⇒ 3ffe:2002: 21: 0:9:3ab: 0: ff01

・ 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



・ 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 固定）
IPv6 グローバルユニキャストアドレス形式
（RFC3587、2003/8）</td><td rowspan="2">インタフェース ID（64bit 固定）
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 アドレスを加工して生成
・ 手動設定
・ DHCPv6（RFC3315）で自動設定
・ 匿名では履歴データを用いてランダムに生成</td></tr>
<tr><td>グローバルルーティングプレフィックス（n bit）
・ 2006/1 の配布ポリシーでは n＝48</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>

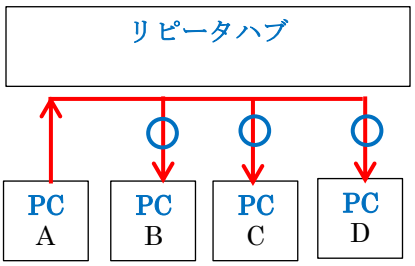
(C) IPv6 アドレスの種類とアドレス範囲

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
		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

4.　ネットワーク機器と通信媒体について

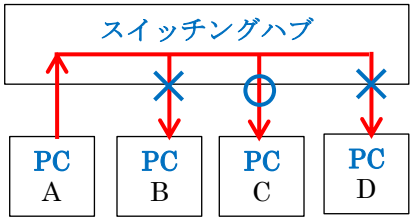
4.1. ネットワーク機器１）リピータハブ（ハブ）

リピータハブ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る。
スイッチングハブの低価格化(5～6 ポートで 4000 円前後)に伴い、市場で見かけることがなくなった。



２）スイッチングハブ（L2 スイッチ）

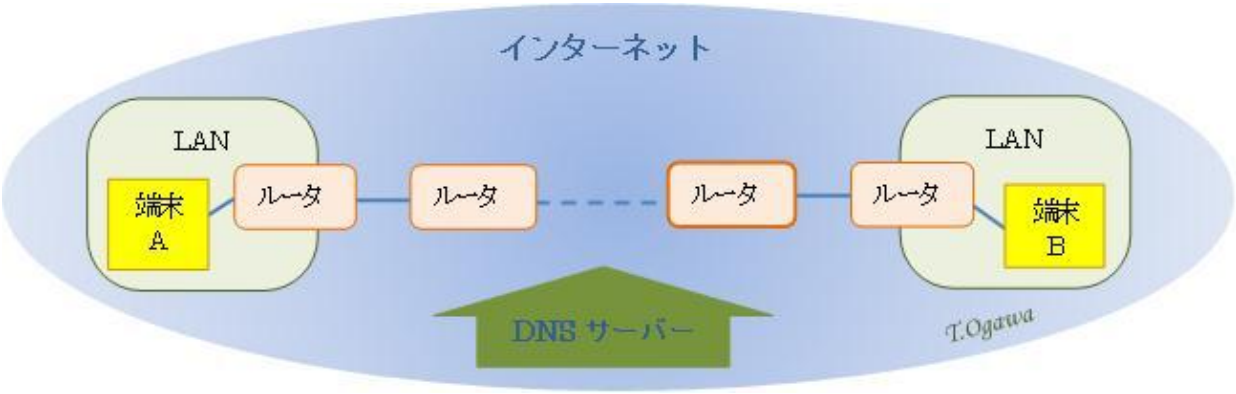
スイッチングハブは L2 スイッチとも呼ばれ、OSI 参照モデルの第 1 層～2 層（物理層、データリンク層）に対応するネットワーク機器である。
スイッチングハブは、再生したデータをイーサネットヘッダの宛先 MAC アドレスで指定した通信機器だけに中継する機器である。



- 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 アドレステーブルを作成する
- データを MAC アドレスで指定したポートだけに送信するため、衝突（Collision）が発生する確率が低く、ネットワークの利用効率が高い

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る。
ルータは、再生したデータを IP ヘッダの宛先 IP アドレスで指定した通信機器あるいは隣接するルータに中継する通信機器であり、ルータに設定されたルーティングテーブルを参照しながら経路を選択して、End To End（送信元端末～宛先端末）でデータを中継する。



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 回線を介して企業拠点間を接続
L3 スイッチ (※)	百万～数千万	同上（イーサネット専用）
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	次項を参照のこと

ルータの主な機能・役割は次のとおりである。

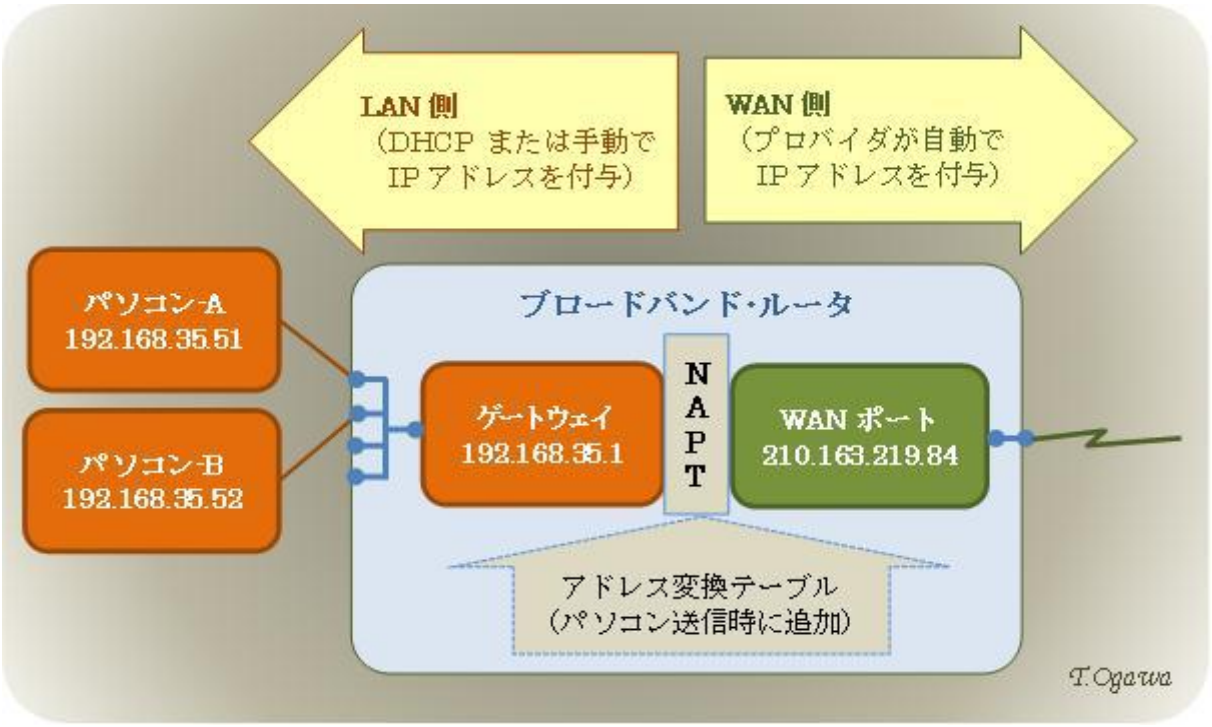
- 宛先 IP アドレスが自 LAN 内の場合は直接転送する
- 宛先 IP アドレスが自 LAN 外の場合は、次の処理を行い転送する
  - 送信伝送路に合わせて MAC フレームを生成し、それに IP パケットをいれて転送フレームを生成する
  - IP パケットを転送する際に、IP ヘッダの生存期間（TTL）を減算し書き換える
  - ルーティングテーブルを参照し、相互接続しているルータから適切なルータを選択しテータを転送する
- 相互接続した他のルータとの通信によってルーティングテーブルを常に最新状態に保つ

4）ブロードバンドルータ

broadband router（BB ルータ）とは、家庭や小規模事業所等で ADSL 、FTTH（光ファイバ）、CATV 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、中継専用の一般のルータには無い次のような機能がある。

- NAPT（NAT、IP マスカレードとも呼ぶ）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（192.168.0.0/16）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
- 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する
- 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
- スイッチングハブ機能を持ち複数の通信端末を接続できる



4.2. 無線 LAN

無線 LAN の規格は ITU-T の I E E E 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 と 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	2012.5 ドラフト 2.0	5GHz	433Mbps ～ 6.93Gbps	1 8	80/160MHz	80m（100Mbps）？ チャネルボンディング マルチユーザMIMO

（参考）2013 年に正式版になる予定の 802.11ac は、帯域幅が 2 倍の 160MHz、ストリーム数が最大 8 本で理論値最大 7Gbps であるが、製品目標は 1Gbps 程度と予想される。

2）Wi-Fi とは

Wi-Fi（Wireless Fidelity 、Fidelity＝忠実）は、機器が無線 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り、IEEE802.11n の無線 LAN とは全く定義が異なるものである。**⇦⇦⇦ 802.11b、802.11g 対応の製品でも Wi-Fi ブランドがある**

無線 LAN が出始めた 2000 年前後は、相互接続が保障されず普及を妨げる一因となった。この解決のため、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 が発足して認定業務を始めた。その後団体名を 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、Web ページで調べた「Wi-Fi CERTIFIDE」認証取得の状況は次表のとおりである。

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

Web ページで調べると、IEEE802.11n 対応の無線 LAN 親機やパソコンの無線 LAN 子機の最高通信速度が製品によりまちまちである。

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に、「MIMO（ミモ）」、「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 / MIMO	20MHz	40MHz チャネルボンディング	最高速度（2012.8 現在）	
			無線 LAN 親機	パソコン
1 ストリーム	72.2Mbps	**150Mbps**	◎	低価格機
2 ストリーム	144.4Mbps	**300Mbps**	○	中級機以上
3 ストリーム	216.8Mbps	**450Mbps**	△	×
4 ストリーム	288.9Mbps	**600Mbps**	×	×

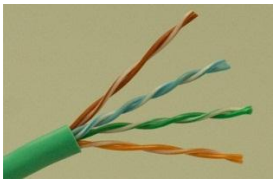
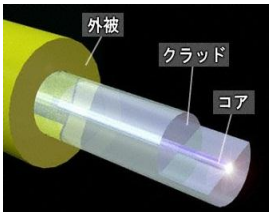
- MIMO（Multiple（マルチプル） Input（インプット） Multiple（マルチプル） Output（アウトプット）、多入力多出力）は、複数のアンテナ（802.11n は最大 4 本）を用いてデータを並列に転送し通信速度を高める技術を言い、送信側はデータを複数アンテナで並列送信し、受信側は複数アンテナで並列受信したデータを合成して元のデータに復元する。
- チャネルボンディング（channel（チャネル） bonding（ボンディング）、チャネル結束）は、無線 LAN の隣り合った 2 つのチャンネルを束ね帯域幅を広げて通信する技術を言い、802.11n では 2 チャンネル分の 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	ツイストペアケーブル	光ファイバケーブル
長所	（耐ノイズ）	価格、工事、（速度）	耐ノイズ、速度、（距離）
短所	速度、（価格、工事）	距離、（耐ノイズ）	価格、工事
ケーブル画像	 10Base2（φ5mm）	 UPT（非シールド）	

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。

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 1 対にして磁気ノイズに強くし、それを 4 対束ねて全体を被覆しているので断面が円形である。

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 対として磁気ノイズに強くし、それを 4 対横に並べて全体を被覆しているので断面が平型（例：幅 5mm×厚さ 1mm）である。

4）イサ―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。

現在よく使われているツイストペアケーブルの仕様を次表に示す。

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			
ツイストペア	IEEE802.3u	100BASE-TX	100Mbps	100m	UTP 4 対 CAT5 以上、RJ-45
	IEEE802.3ab	1000BASE-T	1Gbps	〃	UTP 4 対 CAT5e 以上、RJ-45
	IEEE8023an	10GBase-T	10Gbps	〃	UTP 4 対 CAT6 以上、RJ-45

5.　コマンドプロンプトについて

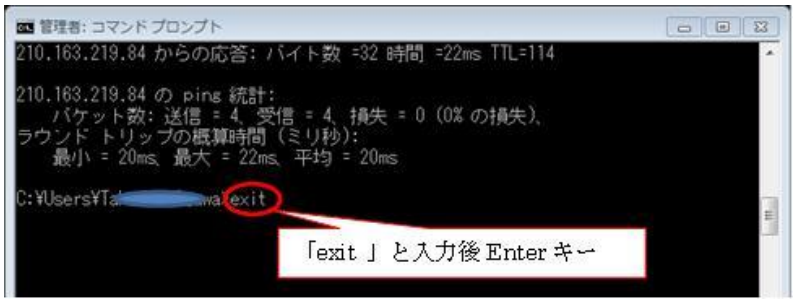
5.1.　コマンドプロンプトの操作方法

1）コマンドプロンプトの起動

［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

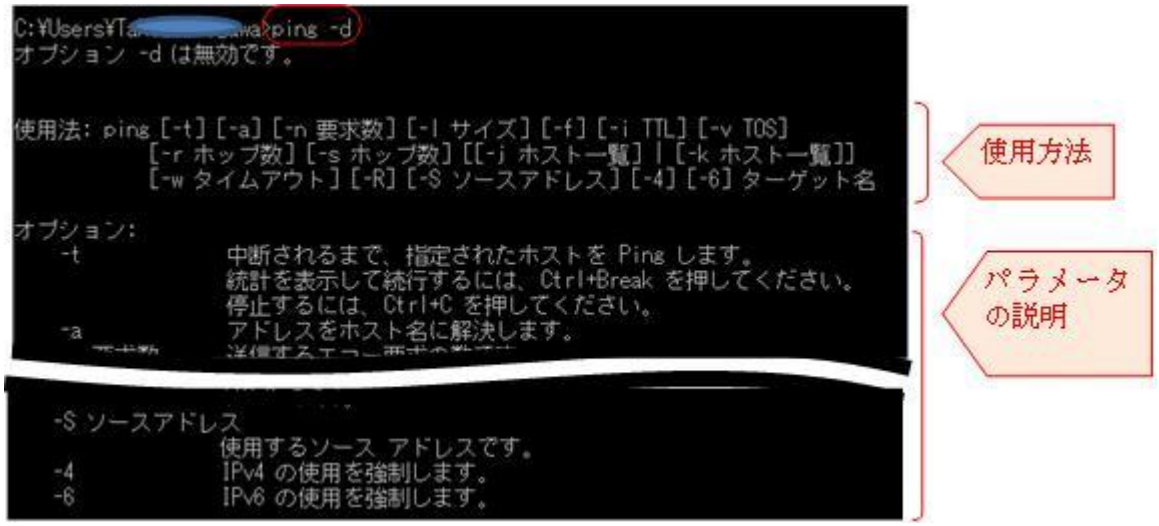
コマンドプロンプトのカーソル位置に「exit 」と入力し Enter キーを押す



3）コマンドの使用方法を調べる方法

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】　「ping　/?」と入力し Enter キーを押す



5.2.　コマンドプロンプト画面のテキストのコピー

コマンドプロンプト関係の資料の多くは、黒地に白字のコマンドプロンプト画面を Print Screen キーでコピーした後に貼り付けている。

ここでは、コマンドプロンプト画面のテキストを選択し［クリップボード］にコピーし、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。

（参考）手順の②で［範囲選択］をクリック後、ドラッグして反転表示させることで、テキストを範囲選択できる。

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】　「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

（参考）オプション省略時の既定値は、4 回、32B になる

（説明）・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 15（＝64－49）のルータを経由している。

２）tracertコマンド

tracert コマンドは、自ホストから URL（または IP アドレス）で指定したホストまでに中継した各ルータの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

（説明）・入力した URL（www.google.com）が DNS の CNAME 機能で 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、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か？

・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 サーバらしい（？）。

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 |

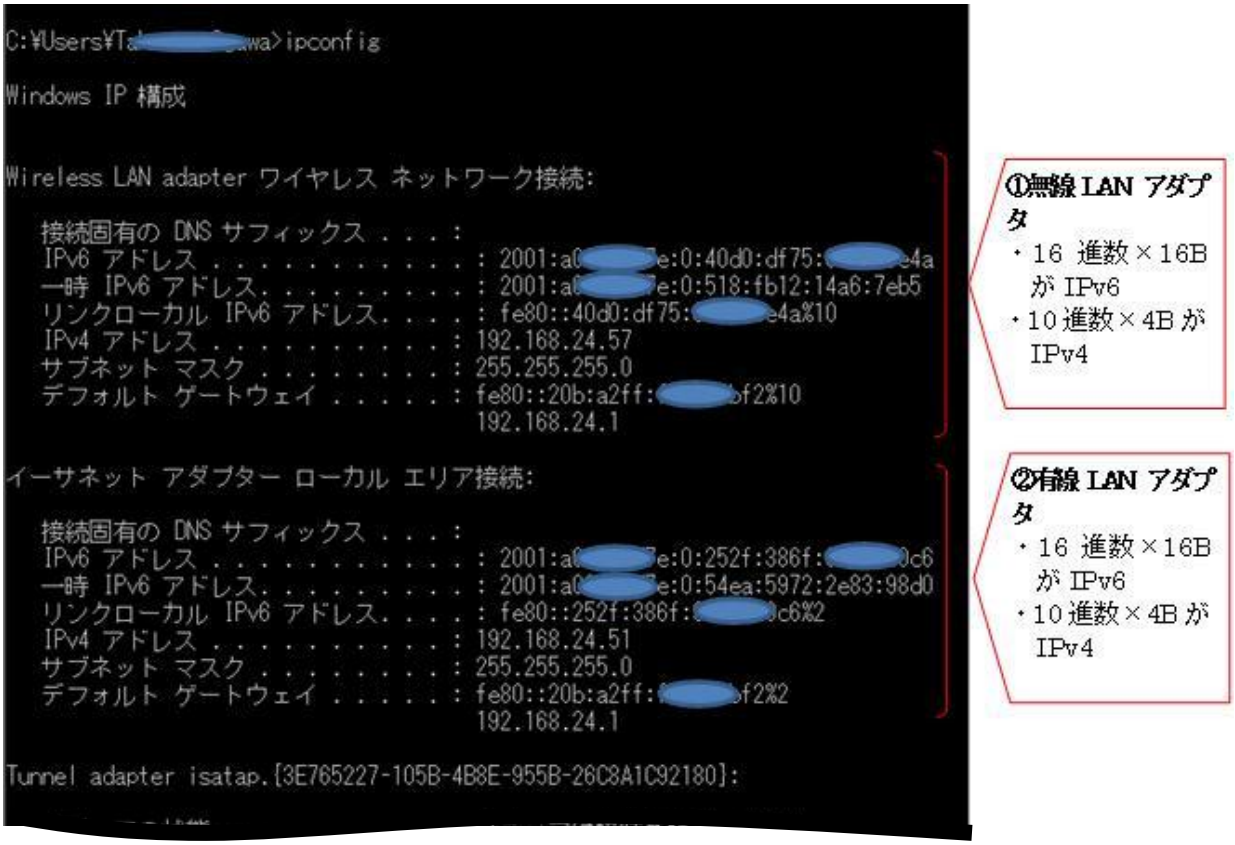
/renew [アダプタ] | /release [アダプタ] | /renew6 [アダプタ] | /release6 [アダプタ] |

/flushdns | /displaydns | /registerdns | /showclassid adapter |

/setclassid アダプタ[クラス ID] | /showclassid6 adapter |

/setclassid6 adapter [classid]]

【使用例】　「ipconfig 」と入力



（説明）ここでは、「① 無線 LAN アダプタ」を例にして説明する。

- ［IPv6 アドレス］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･アドレスであり、これは IPv4 のグローバルアドレスに相当する。
- ［一時 IPv6 アドレス］は「匿名アドレス」とも呼ばれていて、無線 LAN アダプタ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（推奨値で 24 時間、最大で 7 日間、Windows 起動時）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。
- ［リンクローカル IPv6 アドレス］は、無線 LAN アダプタ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
  （補足）［リンクローカル IPv6 アドレス］の後ろに表示されている「%nn」は、接続されているネットワークアダプタを識別するため記号であり、ルーティングテーブルの「インタフェース一覧」にある識別番号と一致する。
- ［IPv4 アドレス］は、無線 LAN アダプタに割り当てた IPv4 のプライベート･アドレスである
- ［サブネット･マスク］は、無線 LAN アダプタに割り当てた IPv4 のサブネット･マスクである
  （補足）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］の上段は、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］の下段は、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

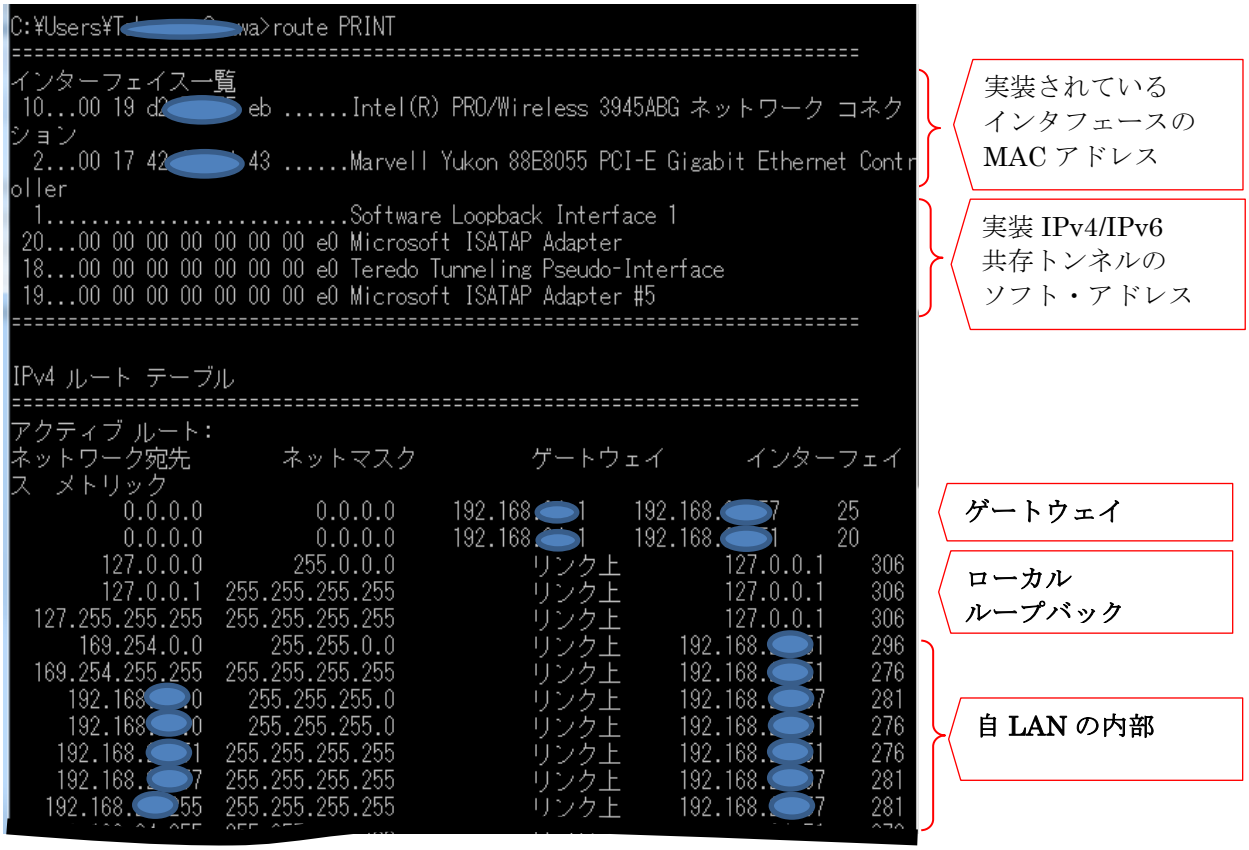
4）routeコマンド（ルート）

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の識別番号
2	2B	宛先ポート番号	宛先アプリケーションの識別番号
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 セグメント全体の誤りチェック
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	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 0x4
	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）IPｖ6 ヘッダの構造

位置	サイズ	名称	説明
0	4bit	バージョン	IPv6 は 0x6
	8bit	トラフィッククラス	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）＝0ｘ8863、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