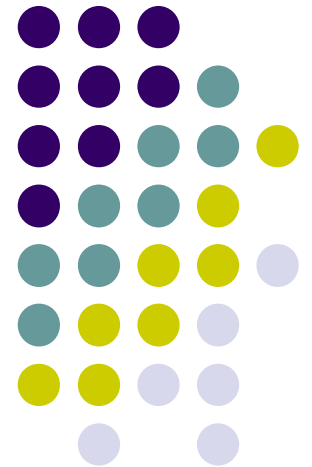
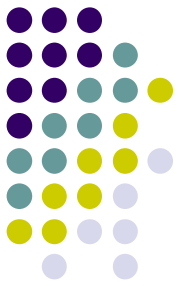


ネットワークについて

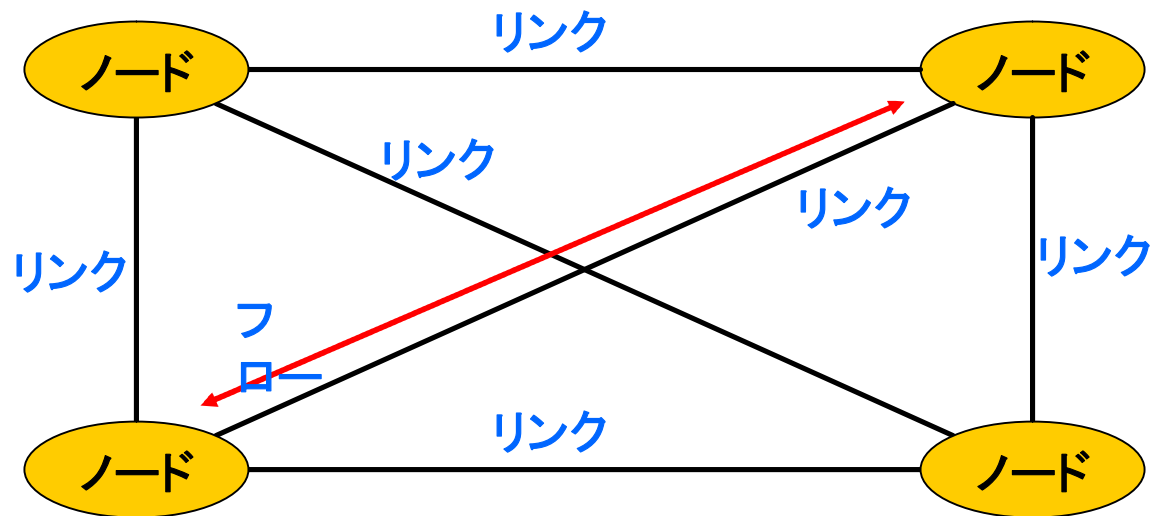




> ネットワークとは？

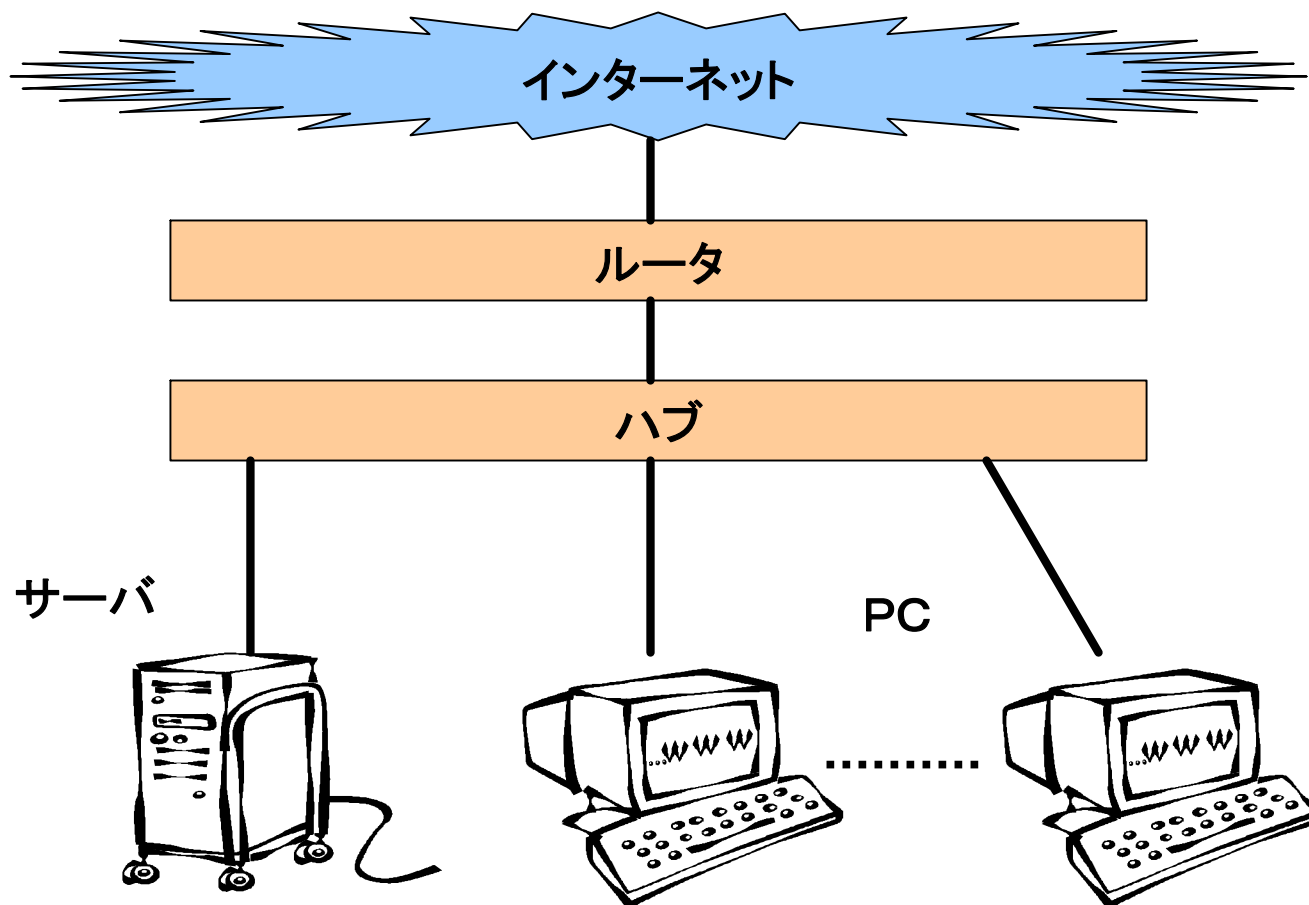
- 「ネットワーク」の意味

ノード(節点)とリンク(経路)から構成され、
フロー(流れ)が発生するもの。





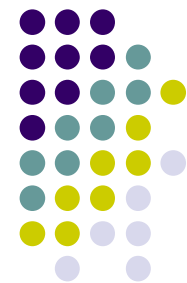
> 簡単なネットワークの構成





> ネットワーク階層

- OSI (Open System Interconnection) とは、1977年にISO (International Organization for Standardization: 国際標準化機構) が発表した、異なる機種のコピュータのデータ通信を実現するためのネットワーク構造の設計方針を定めた規格のことです。
- アプリケーション層、トランスポート層、ネットワーク層、ネットワークアクセス層の4つの階層から成り立っています。TCP/IPにおける各層は、次ページのようにして、OSI参照モデルと対応しています。



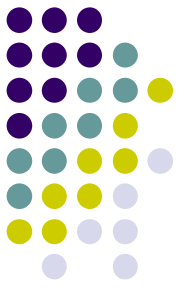
> ネットワーク階層

OSI参照モデル	TCP/IP	(例)
アプリケーション層	アプリケーション層	各種プロトコル ・HTTP (web・ブラウザ) ・FTP (ファイル転送)
プレゼンテーション層		
セッション層		
トランスポート層	トランスポート層	TCP UDP
ネットワーク層	ネットワーク層	ルータ IP
データリンク層	ネットワークアクセス層	スイッチングハブ
物理層		LANケーブル リピータハブ ネットワークカード 無線LAN



> OSI参照モデル

- 第7層(アプリケーション層)は、データ通信を利用した様々なサービスを人間や他のプログラムに提供する。
- 第6層(プレゼンテーション層)は、第5層から受け取ったデータをユーザが分かりやすい形式に変換したり、第7層から送られてくるデータを通信に適した形式に変換したりする。
- 第5層(セッション層)は、通信プログラム同士がデータの送受信を行なうための仮想的な経路(コネクション)の確立や解放を行なう。
- 第4層(トランスポート層)は、相手まで確実に効率よくデータを届けるためのデータ圧縮や誤り訂正、再送制御などを行なう。
- 第3層(ネットワーク層)は、相手までデータを届けるための通信経路の選択や、通信経路内のアドレス(住所)の管理を行なう。
- 第2層(データリンク層)は、通信相手との物理的な通信路を確保し、通信路を流れるデータのエラー検出などを行なう。
- 第1層(物理層)は、データを通信回線に送出するための電気的な変換や機械的な作業を受け持つ。ピンの形状やケーブルの特性なども第1層で定められる。



> ネットワーク機器

- ハブ

ネットワークケーブル集線し、
通信を中継する装置

- ルータ

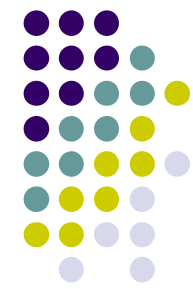
通信の宛先のアドレスを元に経路を判断し、
中継を行う装置





> ネットワーク機器(ルータ)

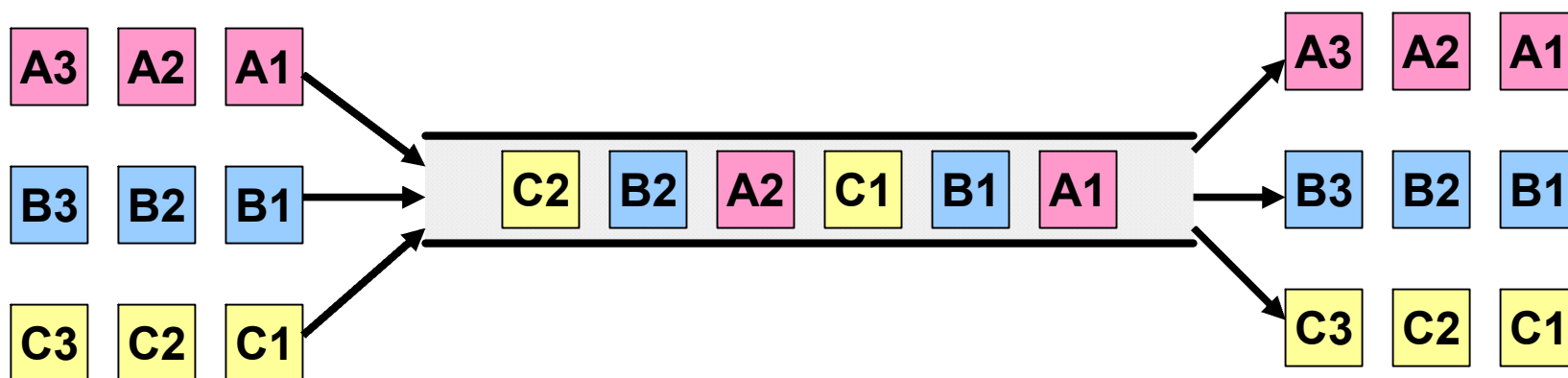
- ファイアウォール
通信の制限を行うルータ
特定の送信先・送信元の通信を遮断できる
- ゲートウェイ(ブリッジルータ)
異なるネットワークを接続するルータ
- ブロードバンドルータ
複数のPCをインターネットに接続する為の
家庭用ネットワーク機器

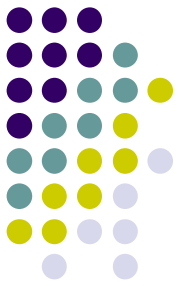


> ネットワーク通信

- パケット通信

LAN (Local Area Network) やWANに使われている技術は、通信データを細かく分割したパケット方式を利用している。これにより、複数のデータを1つの回線で送信できる。(小包方式)





> TCP/IPとは

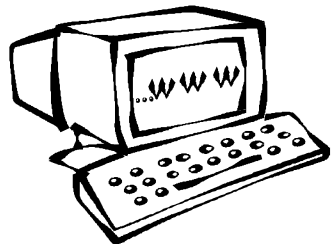
- TCP/IP(Transmission Control Protocol / Internet Protocol)は、データの送受信を行う為の
プロトコル(通信方式)で、TCPプロトコルとIPプロ
トコルから成り立っている。



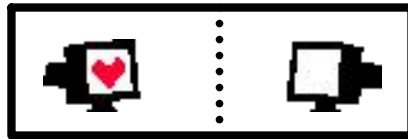
> IPプロトコルとは

コンピュータやルータに一意のIPアドレスを割り当て、通信先を特定し、データを送信する方式。

※バケツリレーのみ行う為、到達保障は無い。

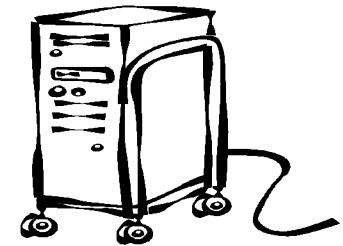


192.168.1.1

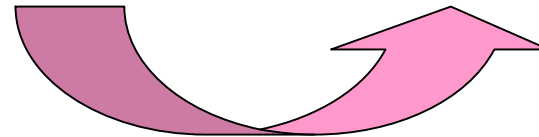


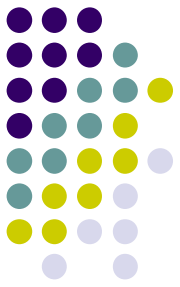
192.168.1.2

192.168.1.3



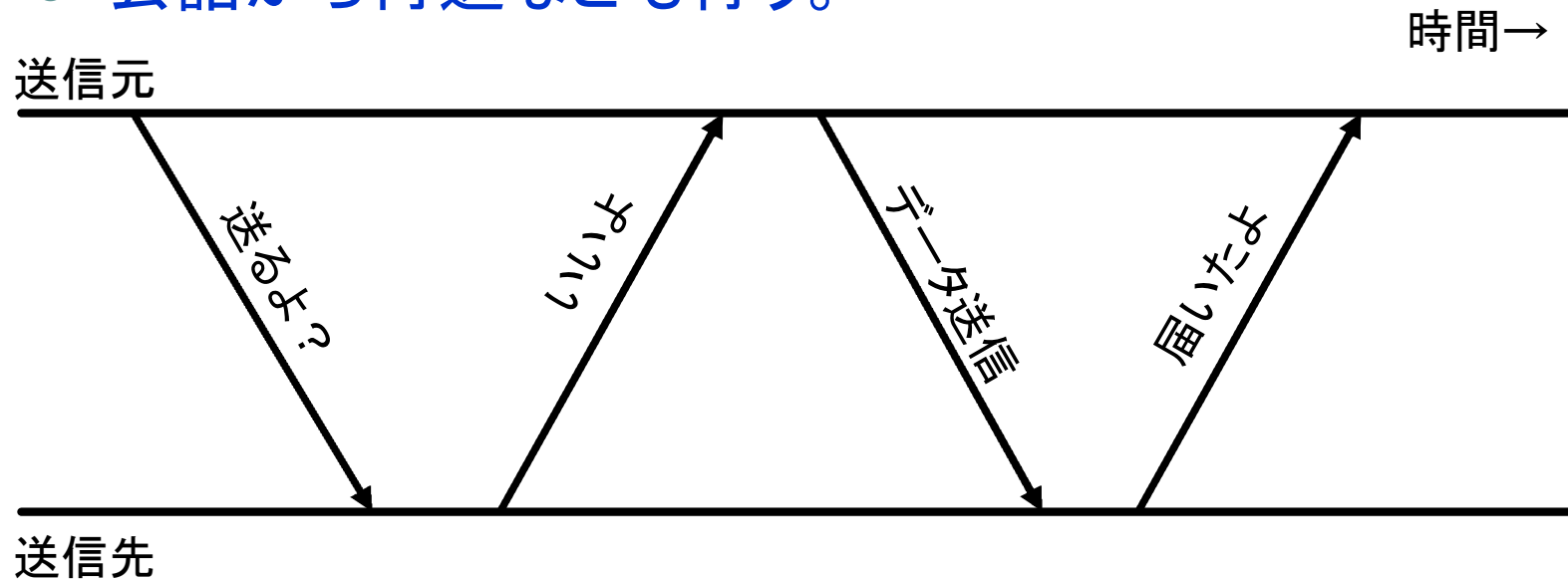
192.168.1.4





> TCPプロトコルとは？

- 通信の信頼性を高める為のプロトコル。
 - パケットに連番を振る
 - 届いたかどうか等会話を行う
 - 会話から再送なども行う。





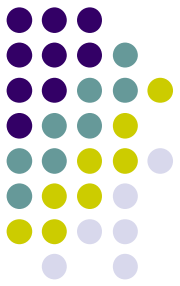
> IP アドレス

- IPアドレスは、ネットワークにおいて、各々のコンピュータを区別するために振られる番号です。IPプロトコルを利用するネットワークにおいて使用されます
- IPアドレスを表示するときは、10進法だけでなく、2進法や16進法も用いられます。例えば、次の数列はすべて同じIPアドレスを表しています。

①211.13.211.2(10進数での表示)

②11010011.00001101.11010011.00000010
(2進数での表示)

③D3.0D.D3.02(16進数での表示)



> 特別なIPアドレス

- プライベートネットワーク用

Aクラス 10.*.*.*

Bクラス 172.16.*.* ~ 172.31.*.*

Cクラス 192.168.*.*

※使用する台数によって選択する。

- ローカルマシン用

127.0.0.1 (ループバック)



>サブネットマスク

- サブネットマスク値からIPアドレスとビットの論理積を計算することによって、IPアドレスのネットワークアドレス部を取得できる。

例えば、サブネットマスクが2進数で 11111111.
11111111.11111111.00000000 ならば、IPアドレスのうち上位24ビットがネットワークアドレス、下位8ビットがホストアドレスである。

192.168.1.2というIPアドレスを255.255.0.0というサブネットマスク値を使って分割すると、このIPアドレスは、192.168というネットワーク上の、ホストアドレス1.2のホストという意味になる。



> サブネットマスクの計算

・ 192.168.0.1/24

192.168.0.1	→	11000000.10101000.00000000.00000001
255.255.255.0	→	11111111.11111111.11111111.00000000
<hr/>		
ネットワーク部		11000000.10101000.00000000.00000000 → 192.168.0.0
IPアドレス		11000000.10101000.00000000.00000001
(サブネットのnot)		00000000.00000000.00000000.11111111
<hr/>		
ホスト部		00000000.00000000.00000000.00000001 → 0.0.0.1

・ 192.168.1.100/28

192.168.1.100	→	11000000.10101000.00000001.01100100
255.255.255.240	→	11111111.11111111.11111111.11110000
<hr/>		
ネットワーク部		11000000.10101000.00000001.01100000 → 192.168.1.96
IPアドレス		11000000.10101000.00000001.01100100
(サブネットのnot)		00000000.00000000.00000000.00001111
<hr/>		
ホスト部		00000000.00000000.00000000.00000100 → 0.0.0.4



> 実際の設定 ipconfig /allコマンド

Windows IP Configuration

Host Name : HIPS-3

Primary Dns Suffix :

Node Type : Hybrid

IP Routing Enabled. : No

WINS Proxy Enabled. : No

Ethernet adapter ローカル エリア接続:

Connection-specific DNS Suffix . :

Description : Intel(R) PRO/100 VE Network Connection

Physical Address. : 00-13-20-2F-8F-3A

Dhcp Enabled. : Yes

Autoconfiguration Enabled : Yes

IP Address. : 192.168.0.50

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.0.1

DHCP Server : 192.168.0.2

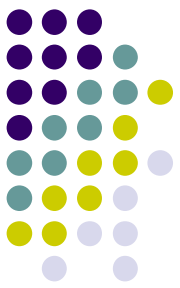
DNS Servers : 202.234.232.6

221.113.139.250

Primary WINS Server : 192.168.0.2

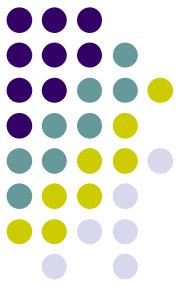
Lease Obtained. : 2006年6月9日 17:30:08

Lease Expires : 2006年6月10日 5:30:08



> DNS

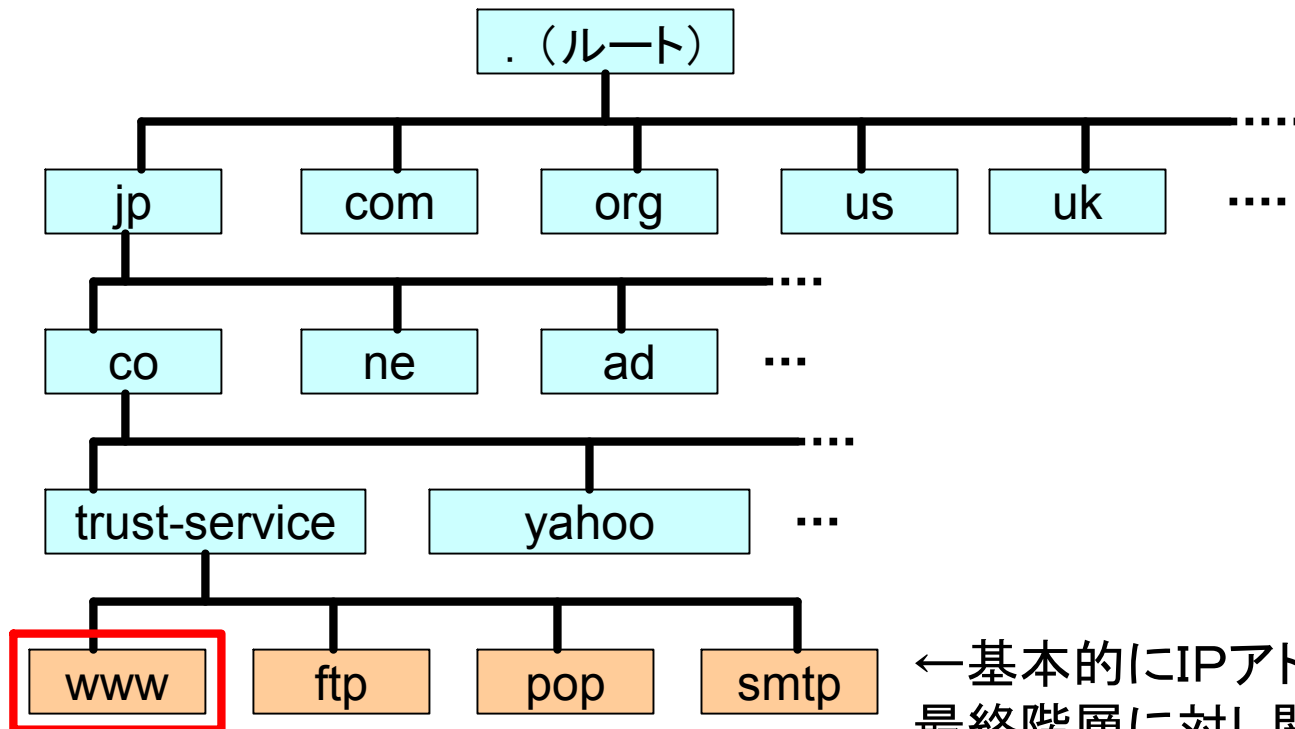
- インターネット上のコンピュータに付けられたIPアドレスは、人間にとって覚えにくいものです。IPアドレスに対して付けられた、人間にとってわかりやすい名前をドメイン名といいます。例えば、IPアドレス211.13.211.3に対するドメイン名はwww.vector.co.jpです。
- ドメイン名をIPアドレスに変換する仕組みをDNS(Domain Name System)といいます。また、ドメイン名をIPアドレスに変換する機能を持ったサーバをネームサーバと呼びます。



> ドメイン

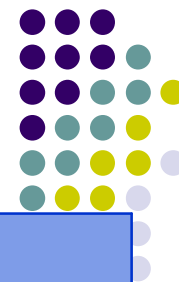
ドメインは階層構造をしており、URL等に表す場合は、最終階層から読む。

例) www.trust-service.co.jp



←基本的にIPアドレスは、最終階層に対し関連付けされる。

>サーバとクライアント



サーバ名	機能(サービス)
ウェブサーバ (WWWサーバ)	ウェブページを配信する。より詳しくは、HTML(Hyper Text Markup Language)と呼ばれる言語で記述されたデータを、HTTP(Hyper Text Transfer Protocol)と呼ばれるプロトコルを利用して配信する。
FTPサーバ	ファイルのダウンロード、アップロード、ファイル操作(ファイルやフォルダの作成・削除等)を行う。
POPサーバ	POP(Post Office Protocol)と呼ばれるプロトコルを利用して、送られてきたメールを受信し、クライアントごとに振り分けて保管する。クライアントはメールソフトを利用してPOPサーバからメールを取り出す。
SMTPサーバ	SMTP(Simple Mail Transfer Protocol)と呼ばれるプロトコルを利用して、電子メールを送信する。
ネームサーバ (DNSサーバ)	DNS(Domain Name System)というシステムを使って、ドメイン名(インターネット上でのコンピュータの名前)による問い合わせに対して、そのドメイン名に対応するIPアドレスを返答する。
DHCPサーバ	DHCP(Dynamic Host Configuration Protocol)機能によって、IPアドレスを各コンピュータに自動的に割り振る。
プロキシサーバ	LANからインターネットへの接続を管理する。キャッシュ処理を行う(頻繁にアクセスするウェブページのコピーをサーバで保存することで処理を高速化する)。
ファイルサーバ	共有ファイルを保管する。
プリントサーバ	複数のクライアントから送られてくる印刷データを管理する。

>通信プロトコル



プロトコル	簡単な説明
HTTP	Hyper Text Transfer Protocol。WWWブラウザがサーバプログラムと通信するときのプロトコル
FTP	File Transfer Protocol。ファイル転送プロトコル。ファイルを直接サーバから受信するときのプロトコル。
SMTP	Simple Mail Transfer Protocol。電子メールを送信するときのプロトコル。
POP	Post Office Protocol。メールボックスから電子メールを取り出すときのプロトコル。
NNTP	Network News Transfer Protocol。ネットワークニュースのメッセージを転送するときのプロトコル。
SNTP	Simple Network Management Protocol。ネットワークを管理するプロトコル。UNIX系のネットワークを中心に使われている。
TCP	Transmission Control Protocol。インターネット上の通信でパケット交換に関するプロトコル。
IP	Internet Protocol。インターネットプロトコル。インターネット上のデータの送受信に関するプロトコル。
PPP	Point to Point Protocol。電話線やISDN回線を使って二台のコンピュータを接続するときのプロトコル。
PPPoE	Point to Point Protocol over Ethernet。ADSL回線を使って二台のコンピュータを接続するときのプロトコル。



> ネットワークコマンド

- ping

パケットを送信して、通信確認と応答時間を確認

```
C:\>ping 192.168.0.1
```

```
Pinging 192.168.0.1 with 32 bytes of data:
```

```
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
```

```
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
```

```
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
```

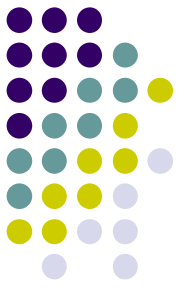
```
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
```

```
Ping statistics for 192.168.0.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



> ネットワークコマンド

- tracer

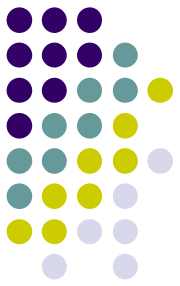
経由ルータ(通信経路)とその応答時間の確認

```
C:\>tracert 125.200.78.8
```

```
Tracing route to p41008-ipbffx02marunouchi.tokyo.ocn.ne.jp [125.200.78.8]  
over a maximum of 30 hops:
```

```
 1      <1 ms      <1 ms      <1 ms  192.168.0.1  
 2       3 ms       3 ms       3 ms  221.113.149.4  
 3       3 ms       3 ms       3 ms  221.113.149.1  
 4       4 ms       4 ms       4 ms  221.113.149.3  
 5       7 ms       6 ms       7 ms  p41008-ipbffx02marunouchi.tokyo.ocn.ne.jp  
      [125.200.78.8]
```

```
Trace complete.
```



> ネットワークコマンド

- netstat -a

空いているポートの確認

```
C:\>netstat -a
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	!TOH:smtp	!TOH:0	LISTENING
TCP	!TOH:http	!TOH:0	LISTENING
TCP	!TOH:epmap	!TOH:0	LISTENING
TCP	!TOH:https	!TOH:0	LISTENING
TCP	!TOH:microsoft-ds	!TOH:0	LISTENING
(中略)			
TCP	!TOH:netbios-ssn	!TOH:0	LISTENING
TCP	!TOH:1710	192.168.0.2:microsoft-ds	ESTABLISHED
(中略)			
UDP	!TOH:ntp	*:*	
UDP	!TOH:netbios-ns	*:*	
UDP	!TOH:netbios-dgm	*:*	



> ネットワークコマンド

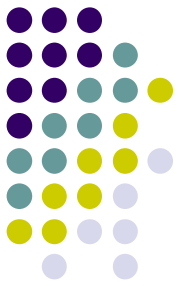
- telnet

コンソールにリモートログインする

```
c:¥>telnet www.trust-service.co.jp 80
GET /index.html HTTP/1.0(リターン) (←表示されない場合あり エコー設定)
(リターン)
HTTP/1.1 200 OK
Date: Tue, 13 Jun 2006 08:35:28 GMT
Server: Apache
Last-Modified: Tue, 16 May 2006 04:38:01 GMT
ETag: "c5d00e-3659-44695729"
Accept-Ranges: bytes
Content-Length: 13913
Connection: close
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html><!-- InstanceBegin template="/Templates/company-page.dwt" codeOutsideHTMIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<!-- InstanceBeginEditable name="doctitle" -->
<title>株式会社トラストサービス TRUSTSERVICE</title>
(中略)
</html>
```

ホストとの接続が切断されました。



> セキュリティについて

- ネットワークのセキュリティ対策
 - 使用しないポートは閉じる
 - 可能な限り送信元も制限する
 - Telnet等のリモートログインをはじめ、可能な限り暗号化通信（SSH等）を活用する



> セキュリティについて

- サーバのセキュリティ対策（webサーバ等）
 - セキュリティパッチは適用する
 - パスワードは長く、難しく
 - 辞書用語は使わない
 - 一定期間ごとに変更する
 - バージョンは明かさない（エラー画面等）
 - アカウントごとの使用できる範囲を限定する（FTP等）
 - 余計な機能は動かさない