コンピュータネットワーク

2013-4 ～ 7

金田 泰

自己紹介

■なまえ: 金田 泰 (かなだ やすし)

■所属: 日立製作所中央研究所

■連絡先等: Yasusi.Kanada.yq@hitachi.com, http://www.kanadas.com/

■仕事

- 1981 年，修士課程修了後，日立製作所に就職．中央研究所に配属．
- 1981-85 年，Fortran 言語のコンパイラ開発．
  とくに，スーパーコンピュータ S-810 のためのコンパイラを開発．
  …
- 1996-99 年，百科事典や WWW などのための「軸づけ検索」を開発．
- 1999-2001 年，ネットワーク QoS とポリシーサーバ開発
- 2002-2006 年，立体音使用のスマートフォン型会話メディアや IP 電話関連の開発．
- 2007-2008 年，ネットワーク QoS など
- 2009 年–，ネットワーク仮想化技術の開発など．

教科書・参考書

■教科書は指定しない

■参考書

◆井戸 伸彦 著，法雲 俊邑 監修
新しい情報ネットワーク教科書，オーム社 (2300 円)

●昨年はこの本を教科書として指定した．
●講義内容や図・絵がこの本にそっている部分がある．

◆織田 薫，坪山 博貴 著，図解! よくわかるネットワークの仕組み，SoftBank Creative (980 円)

●この本からも図を借用する．

◆増田 直紀，今野 紀雄 著，「複雑ネットワーク」とは何か，講談社 (900 円)

●コンピュータ・ネットワークにかぎらない，ひとのネットワークをはじめとする多様な複雑ネットワークの性質についての本．

講義の概要

■参考: 昨年度のスライド

◆昨年度資料の完全版は kuport に電子教材として登録．

◆昨年度資料の公開版はブログに掲載 (ただし，借用した図はマスクされている)
http://www.kanadas.com/kogakuin-cn/

■1. さまざまなネットワークとその現状

◆さまざまな通信ネットワーク

◆ネットワークの数学的な理論とくに複雑ネットワークの理論

◆情報のながれとものののながれ (ネットワーク理論とネットワーク・フロー)

講義の概要 (つづき)

■2. 通信ネットワークの原理

◆プロトコル

◆アドレスと名前

◆回線交換とパケット交換

◆ユニキャストとブロードキャスト，有線通信と無線通信

◆回線交換とパケット交換

目 次

講義の概要 (つづき)

■3. イーサネット (LAN)

◆イーサネットの規格

◆イーサネットのアドレス

◆イーサネットにおける転送方法 (ブロードキャストとスイッチング)

講義の概要 (つづき)

■4. インターネットとインターネット・プロトコル (IP)

◆インターネット・プロトコルとグローバルな通信

◆IP アドレス

◆IP ネットワークの構造と障害に対するつよさ

◆ルータによるパケットの転送とルーティング

講義の概要 (つづき)

■5. インターネットとイーサネット (IP/Ethernet)

◆IP とイーサネットにおけるアドレスのあつかい

◆IP とイーサネットのスケーラビリティ

◆IP， イーサネットとループ

- IP/Ethernet と ARP

講義の概要 (つづき)

■6. プロトコルやネットワークの階層構造

◆プロトコルの階層化と OSI 基本参照モデル
(エンジニアリングにおける階層構造)

◆スケールフリーなネットワーク構造 (現象としての階層構造)

講義の概要 (つづき)

■ 7. プライベート・ネットワークとネットワーク仮想化
- ◆プライベート・ネットワーク
- ◆VLAN (LAN におけるネットワーク仮想化)
- ◆ネットワーク仮想化と新世代ネットワーク研究
- ◆ソフトウェア定義ネットワークと OpenFlow
- ◆日本におけるネットワーク仮想化研究と IPEC (IP-Ether-Chimera)

講義の概要 (つづき)

■ 8. ネットワーク・サービスの基礎プロトコル TCP と UDP
- ◆TCP, UDP とポート
- ◆TCP にもとづくさまざまなプロトコル: HTTP, FTP, SMTP, SIP など
- ◆TCP による高信頼・高性能・「フレンドリー」な通信

講義の概要 (つづき)

■ 9. インターネット上のネットワーク・サービス
- ◆ファイル転送
- ◆電子メール
- ◆Web (WWW)
- ◆IP 電話

講義の概要 (つづき)

■ 10. ネットワーク・セキュリティ
- ◆ネットワーク上の脅威とセキュリティの確保
- ◆ファイアウォール
- ◆共通鍵暗号・公開鍵暗号と TLS/SSL
- ◆認証・電子署名
- ◆アクセス制御
- ◆無線 LAN のセキュリティ

1. さまざまなネットワークとその現状

要点

■ 通信ネットワークにはコンピュータ・ネットワーク，電話網など，さまざまある.

■ さまざまなネットワークを抽象化して数学的に理論化されている.
- ◆コンピュータや通信のネットワーク以外にも，人間関係や交通・物流など，さまざまなネットワークがある.
- ◆最近，複雑ネットワークの理論が発展している.
- ◆古典的な理論として，ネットワーク最適化の理論，ネットワーク・フローの理論などがある.

コンピュータ・ネットワーク

■ コンピュータ・ネットワークの構成要素は 3 種類
- ◆リンク: 端末とノード，ノードどうしをむすぶ電線 (通信回線).
- ◆端末: 基本的に 1 本のリンクでノードに結合される (PC, サーバ, プリンタ, …).
- ◆ノード: 結節点 (ルータ, スイッチ, …

スイッチやルータのネットワークは固定的 (構造があまり変化しない)

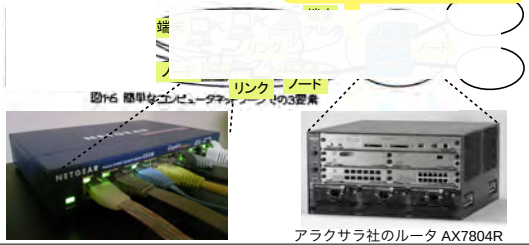


図1-5 簡単なコンピュータネットワークの3要素

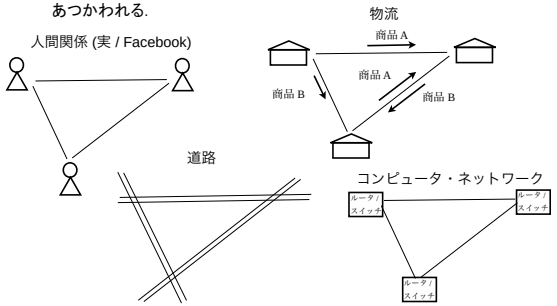
アラクサラ社のルータ AX7804R

携帯電話のネットワーク

図1-7 携帯電話ネットワークでの通信の3要素

さまざまなネットワーク

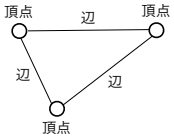
■ ひとのつながりもネットワーク
- ◆コンピュータ・ネットワークもひとのネットワークも「ネットワークの理論」であつかわれる.



さまざまなネットワーク (つづき)

ネットワークの抽象化

- さまざまな種類のネットワークを頂点と辺からなるグラフに抽象化する.
- グラフの辺や頂点に属性値 (距離など) をあたえたもの が (抽象的な) ネットワーク.
- 抽象的なグラフやネットワークの数学的理論を実際のネットワークに適用する.

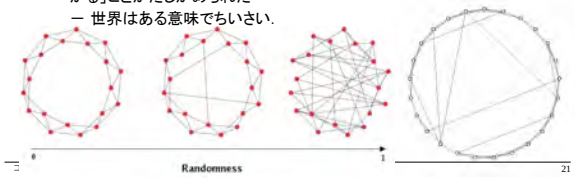


ネットワークの理論

- ネットワークの数学的な理論は (すくなくとも) 2 つある
  - 複雑ネットワークの理論
    - 最近発展した.
  - ネットワークの最適化, とくにネットワーク・フローの最適化
    - 歴史がある.
- 経済学・経営学なども複雑ネットワークの理論などに影響をうけている.

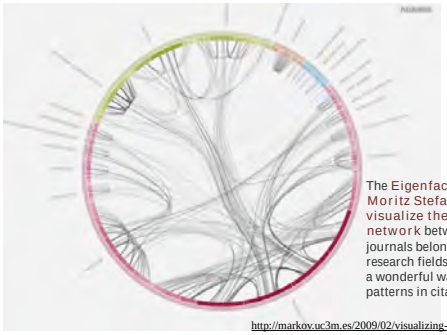
複雑ネットワークの理論: スモールワールド

- スモールワールド・ネットワークの理論が比較的最近, 発展
  - 社会心理学者スタンレー・ミルグラムによる実験 (1967): 送信相手を知り合いに限定した手紙が何回めに目的の相手にとどくかをしらべる.
    - ー 6 回めにとどいた.
  - その後のメールなどによる実験でも「世界の誰とでも 6 人 (程度) でつながる」ことがたしかめられた
    - ー 世界はある意味でちいさい.



スモールワールド・ネットワークの例

- 論文誌の論文間の参照関係

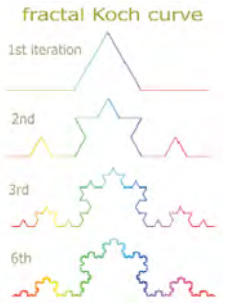


The Eigenfactor Project and Moritz Stefaner join efforts to visualize the citation network between different journals belonging to different research fields. It is amazing and a wonderful way to explore patterns in citation networks

http://markoy.uc3m.es/2009/02/visualizing-citation-networks/

複雑ネットワークの理論: スケールフリー

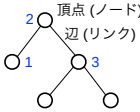
- スケールフリーとは?
  - 拡大してもおなじようにみえること.

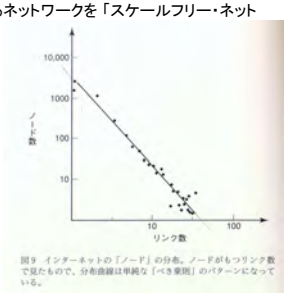


http://www.dichotomistic.com/hierarchies_fractals.html

複雑ネットワークの理論: スケールフリー (つづき)

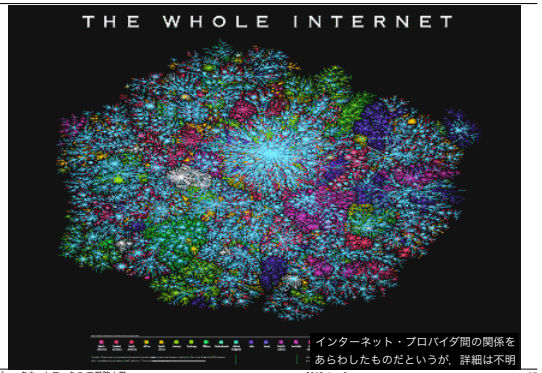
- スケールフリー・ネットワーク
  - 拡大してみてもおなじようにみえるネットワークを「スケールフリー・ネットワーク」という.
  - スケールフリー・ネットワークはべき乗則に支配されている. ⇒
  - 多くの現実のネットワークはスケール・フリーである.
  - インターネットもスケールフリーである.





- 参考書
  - バラバシ「新ネットワーク思考」, NHK 出版
  - ブキャナン「複雑な世界, 単純な法則」, 草思社

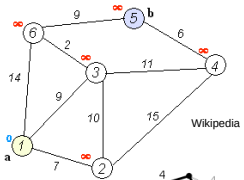
インターネット全体 (?!)

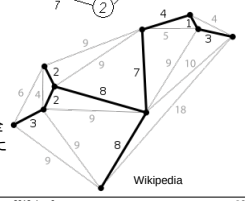


インターネット・プロバイダ間の関係をあらわしたものだというが, 詳細は不明

ネットワークの最適化

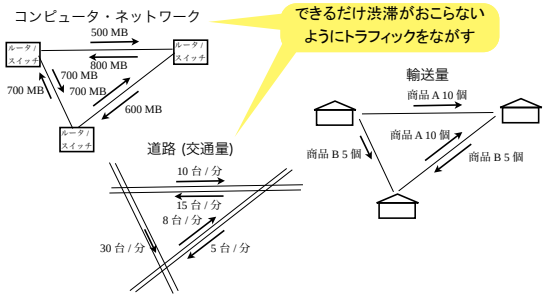
- さまざまな最適化問題がある.
  下記の問題はコンピュータ・ネットワークにおいて重要な問題の例.
  - 最短路問題 (Shortest path problem)
    - 与えられた重み付きグラフの 2 つの頂点間を結ぶ辺の中で最小の重みを持つ経路を求める問題
      -- インターネットに関係がふかい
  - 最小木問題 (Minimum spanning tree problem)
    - 各辺に重みが与えられたグラフにおいて, そのグラフ上に存在する全張木 (全域木) の中で辺の重みの総和が最小になるものを見出す問題
      -- イーサネットに関係がふかい





ネットワーク・フローの理論

- ネットワークをながれるトラフィック量 (流量) を最適化.
  - 代表的な最適化問題は最大流問題 (流量を最大化する).



ネットワークの分散制御と集中制御

■ ネットワーク・トラフィックの制御法としては，分散制御と集中制御とがある．

■ 道路交通網の場合

◆くるまは運転者が自律的に制御している -- 分散制御

◆信号機は集中制御されていることがある．

■ コンピュータ・ネットワークの場合

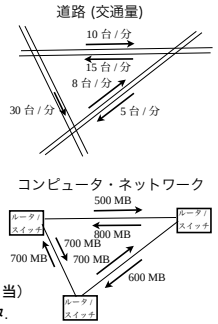
◆インターネットでは分散制御が基本．（スイッチやルータは自律的に動作する．）

◆電話のネットワークはより集中的に制御されている．

■ 道路とコンピュータのちがい

◆道路交通：自律要素はくるま (= パケット相当)

◆コンピュータ：自律要素はスイッチ / ルータ．



さまざまなネットワークとその現状のまとめ

■ 通信ネットワークにはコンピュータ・ネットワーク，電話網など，さまざまある．

■ さまざまなネットワークを抽象化して数学的に理論化されている．

◆コンピュータや通信のネットワーク以外にも，人間関係や交通・物流など，さまざまなネットワークがある．

◆最近，複雑ネットワークの理論が発展している．

◆古典的な理論として，ネットワーク最適化の理論，ネットワーク・フローの理論などがある．

2. 通信ネットワークの原理

要点

■ 通信の規約 (きまり) をプロトコルという．

◆プロトコルの主要素はデータ・フォーマットとシーケンス (手順)．

■ 通信相手を特定するのにアドレスがつかわれる．

◆相手を名前で特定することもできるが，固定長アドレスなら高速処理可能．

◆最近は名前とアドレスの分離をめざした研究開発がすすめられている．

■ 通信形態としてユニキャストとブロードキャストがあり，有線通信と無線通信にほぼ対応している．

◆ユニキャストは 1 対 1，ブロードキャストは 1 対多の通信形態．

◆有線通信の基本はユニキャストであり，無線通信の基本はブロードキャストである．

◆有線通信の方式として回線交換とパケット交換とがある．

プロトコルとは?

■ 通信するための約束ごとをプロトコルという．

■ プロトコルと標準化

◆みんながおなじプロトコルをつかわないと通信できない ⇒ 標準化が重要

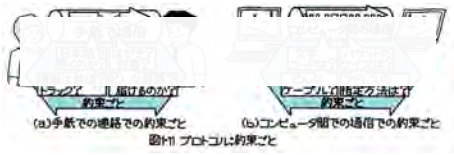


図1-1 プロトコルと約束ごと

プロトコルの表現

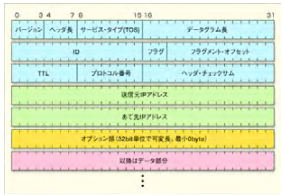
■ プロトコルはメッセージ形式とシーケンスとで表現する．

■ メッセージ形式

・XML によるプロトコルの例: SOAP

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="…"
    SOAP-ENV:encodingStyle="…">
 <SOAP-ENV:Header>
  <t:Transaction xmlns:t="…"
      SOAP-ENV:mustUnderstand="1">
   5
  </t:Transaction>
 </SOAP-ENV:Header>
 <SOAP-ENV:Body>
  <m:getPitchingResult xmlns:m="…">
   <m:name>Akinobu Yoshida</m:name>
   <m:No>00</m:No>
  </m:getPitchingResult>
 </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

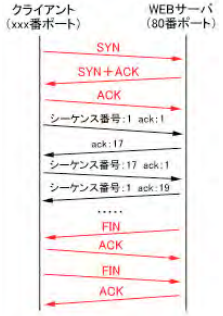
・バイナリ・プロトコル



プロトコルの表現 (つづき)

■ シーケンス図 (通信手順の図)

・例: TCP



ネットワークの分類

■ LAN (局所的なネットワーク) が WAN (広域ネットワーク) によってつながれている．

■ MAN (地域ネットワーク) ということばもある．

◆LAN, WAN ほど頻繁にはつかわれない．

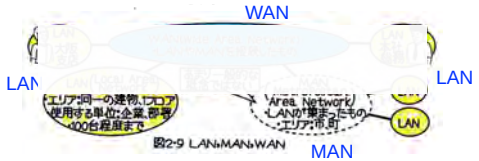
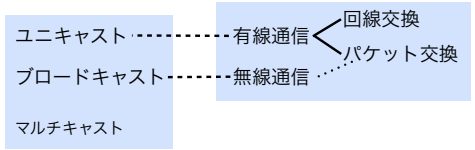


図2-9 LAN,MAN,WAN

通信形態の分類

■ 通信形態としてユニキャストとブロードキャストがあり，有線通信と無線通信にほぼ対応している．

■ 有線通信の方式として回線交換とパケット交換とがある．

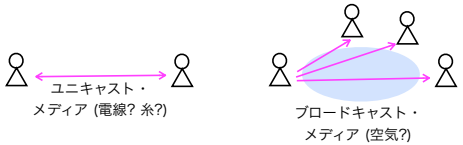


ユニキャストとブロードキャスト

■ 通信形態としてユニキャストとブロードキャスト (放送) がある．

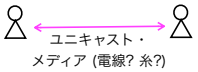
◆ユニキャストは 1 対 1，ブロードキャストは 1 対多の通信形態．

◆ユニキャスト / ブロードキャストはまずメディア (信号をつたえる媒体) できまる．



有線通信はユニキャスト

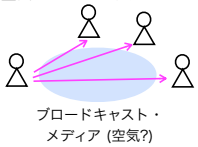
■ 有線通信の基本はユニキャストである.
- ◆ 電線はユニキャスト・メディア



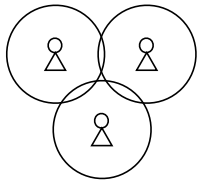
■ ただし，イーサネットでは 1 本の線に多数のコンピュータをぶらさげて (バス型)，ブロードキャストすることができる.

無線通信はブロードキャスト

■ 無線通信の基本はブロードキャストである.
- ◆ 真空 / 空気 はブロードキャスト・メディア

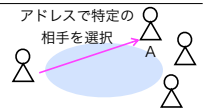


■ ただし，信号がとどく範囲は有限

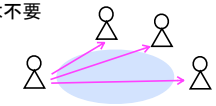


ユニキャスト，ブロードキャストとアドレス

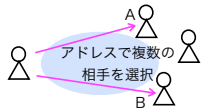
■ ユニキャストでは相手を選択するのにアドレスをつかう.



■ ブロードキャストではアドレスは不要



■ 複数の相手 (アドレス) を指定する通信をマルチキャストという.



アドレスと名前

■ 通信 (会話) 相手を識別するには，名前をつかうのが自然.
- ◆ 相手がどこにいても，名前で識別できる.

■ 名前の問題点
- ◆ 同姓同名がありうる (一意にきまらない)
- ◆ 名前は可変長なので，あつかいづらい (寿限無寿限無…)

■ 名前のかわりにアドレスをつかえば，問題が解決される.
- ◆ アドレスは一意にする.
- ◆ 固定長にする (Ethernet では 48 ビット，IPv4 なら 32 ビット).

■ アドレスにも問題が生じうる.
- ◆ アドレスを場所 (location) にむすびつけると，移動したときに通信できなくなる.

ID とロケータ (最先端のはなし)

■ ID: 通信相手を識別するための名前 (識別子，identifier)

■ ロケータ: 通信メッセージを相手に配送するためのアドレス

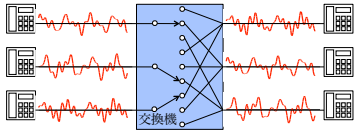
■ 郵便では ID は名前に相当し，ロケータは住所に相当する (わかれている)
- ◆ ID: ホリエモン (堀江 貴文)
- ◆ ロケータ: 六本木ヒルズ …

■ インターネットでは ID とロケータはおなじもの (IP アドレス)
- ◆ そのため，移動すると ID の変更が必要になる -- モバイル環境では不便
- ◆ 場所に依存しない ID をつかって通信するための研究開発がすすめられている.
  - ID Locator Separation (ID ロケータ分離)
  - LISP (Locator ID Separation Protocol)

回線交換とパケット交換

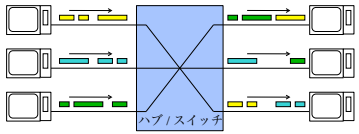
■ 有線通信の方式として回線交換とパケット交換とがある.

■ 電話網は回線交換網
- ◆ 通信前に回線を接続し，終了後に切断する.
- ◆ その間，回線を占有する.



■ IP 網 (インターネット, NGN) はパケット交換網
- ◆ パケット = 小包
- ◆ パケット 1 個ごとに宛先をみて配送する.

NGN = Next Generation Network
NwGN = New Generation Network



回線交換とパケット交換の比較

回線交換網	パケット交換網
高通信品質 (QoS*) が実現しやすい	通信品質の確保が困難
回線数以下の接続しかできない	接続数は柔軟に変化する
無信号時も回線を占有するため高コスト	回線を共有するため低コスト
ネットワークがインテリジェント	端末がインテリジェント (コンピュータを使用)
常時接続不可	常時接続が基本
呼設定が必要 (通信前に回線を確保する)	呼設定が不要 (いきなりパケットを送出すればよい)

* QoS = Quality of Service

電話と回線交換のはじまり

■ 電話 (電話器) は Alexander Graham Bell によって 1876 年に発明された.

■ 初期の電話器
- ◆ 基本のユーザインタフェースは変化していない.
  - ●相手に接続し，
  - ●1 個のマイクと 1 個のスピーカを使用して
  - ●1 対 1 で会話し，
  - ●おわったら接続をきる.

Bell の電話器
(http://www.phonedoc.com/Telephone_Story/telephone_story.html)

1878 年ころの電話器
(http://www.atcaonline.com/-phone/coffin.html)

スウェーデンの Ericsson が開発

日本 (電電公社) の黒電話

電話と回線交換のはじまり (つづき)

■ 最初の交換所は **1878** 年コネティカット州に設立された.

◆ なぜ回線交換が必要なのか?
= なぜネットワークが必要なのか?

[エピソード] “音室”コミュニケーションメディア voiscape

(2008 年度以前の「マルチメディアエ学」でした話)

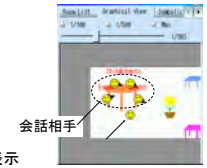
■ 音声コミュニケーション・メディア “voiscape” を開発した.
- ◆ 人間のコミュニケーション能力がいかせるように音 (3D 音響) を加工 .
- ◆ voiscape = voice + [land]scape (声の風景)
- ◆ このときはステレオ・ヘッドセットを使用 ― 将来はもっとよいものを…

■ 仮想の “音室” 内にコミュニケーションの場をつくる.
- ◆ 音の方向感・遠近感で空間を表現.
- ◆ 音室内を各人が自由に移動して, 会話相手や音源を選択 できる.

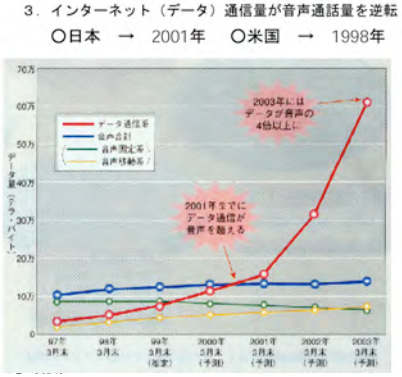
[エピソード] voiscape プロトタイプのインタフェース

■ 音室を選択する.
- ◆ 音室リストの例
  - オフィス (Office)
  - 会議室 (MeetingRoom A, B)
  - 家庭 (MyHome)

■ 入室すると音室の様子が表示される.
- ◆ 3D 音響によって音室を “聴覚表示” (auditory display)
  - 最近接の音源がもっともよくきこえるが, 同時に他の音源もきこえる.
  - このプロトタイプでは前後感はあまりえられない.
- ◆ グラフィクスによる視覚表示で補助
  - コミュニケーションの場をわかりやすく表示



電話網から IP ネットワークへ



電話網から IP ネットワークへ (つづき)

■ 音声通信量のほうがおおいとき **(2000** 年まで**)**
- ◆ データ通信にも電話網をつかうほうが経済的.
- ◆ つまり, インターネットにダイアルアップ接続すればよい.

■ データ通信量のほうがおおいとき **(**現在**)**
- ◆ 音声通信にも IP ネットワークをつかうほうが経済的.
- ◆ つまり, IP 電話をつかうほうがよい.
- ◆ とくに, 音声通信とデータ通信をくみあわせた複合的なサービスの提供には IP 網が適している.

通信ネットワークの原理のまとめ

■ 通信の規約 (きまり) をプロトコルという.
- ◆ プロトコルの主要素はデータ・フォーマットとシーケンス (手順).

■ 通信相手を特定するのにアドレスがつかわれる.
- ◆ 相手を名前で特定することもできるが, 固定長アドレスなら高速処理可能.
- ◆ 最近は名前とアドレスの分離をめざした研究開発がすすめられている.

■ 通信形態としてユニキャストとブロードキャストがあり, 有線通信と無線通信にほぼ対応している.
- ◆ ユニキャストは 1 対 1, ブロードキャストは 1 対多の通信形態.
- ◆ 有線通信の基本はユニキャストであり, 無線通信の基本はブロードキャストである.
- ◆ 有線通信の方式として回線交換とパケット交換とがある.

3. イーサネット (LAN)

要点

■ イーサネットは比較的せまい範囲でつかうのに適したネットワークの規格 (標準)
- ◆ もとは 500 m くらいの範囲でしかつかえなかったが, 現在では日本全体の数 10 拠点をカバーすることも可能

■ イーサネットのアドレスは 1 個ずつ, ばらばら
- ◆ ちかくに位置する PC でもアドレスは似ていない
- ◆ インターネットでは, ちかくに位置する PC はアドレス上位が一致

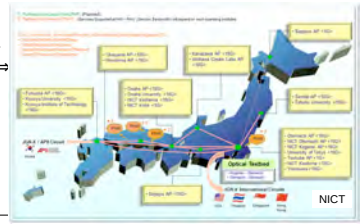
■ ネットワークにループがあると転送できない (ネットワークは木構造)
- ◆ 障害 (断線など) があると通信できなくなる.

■ パケットは 2 種類の方法で転送される.
- ◆ ブロードキャスト + 衝突検出 (CSMA/CD) -- ケーブルとリピータで転送
- ◆ スイッチング + 学習 --- スイッチで転送

イーサネットとは?

■ イーサネットは国際学会 IEEE で標準化された LAN の規格
- ◆ 標準の名称は IEEE802.2, IEEE802.3 など
- ◆ IEEE = the Institute of Electrical and Electronics Engineers (アイトリプルイー, 米国電気電子学会)
- ◆ LAN = Local Area Network

■ 初期には 500 m 程度の範囲でしかつかえなかったが, 現在は日本全国をむすぶ広域イーサネットもある.
- ◆ 例: JGN-X (研究用) ⇒
- ◆ ただし, インターネットほど多数のコンピュータをつなぐことはできない.



IEEE についての補足

■ IEEE が発行する論文誌や雑誌

イーサネットの標準化

■「標準」と「規格」― 英語では (どちらも) standard

■ イーサネット標準化の歴史

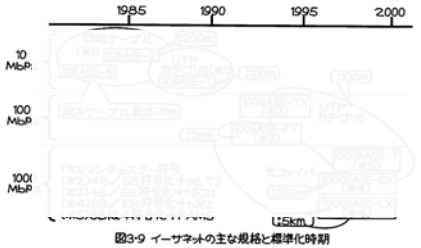
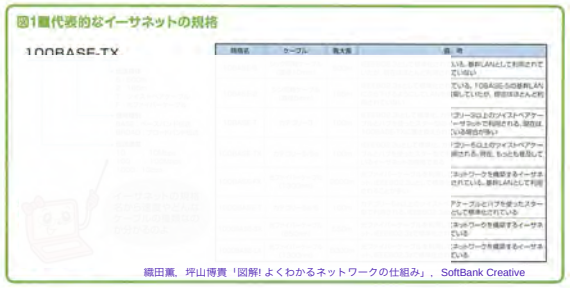


図3-9 イーサネットの主な規格と標準化時期

イーサネットの標準化 (つづき)

■さまざまな規格



織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

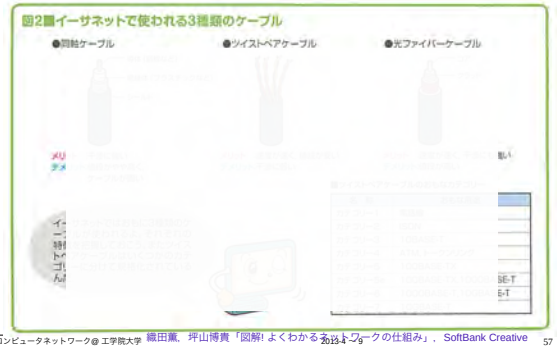
イーサネットの標準化 (つづき)

■イーサネット標準の構造

図3-10 LANの標準化　※LLC(Logical Link Control

LAN ケーブルの種類

■イーサネットでは 3 種類のケーブルがつかわれる.



織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

LAN ケーブルの種類（つづき）

■初期のイーサネットでは “yellow cable” という同軸ケーブルがつかわれた (直径 10 mm).

この写真は現在も売っている “THICKNET” (https://logistech.jp/iex/servlet/top)

LAN ケーブルの種類 (つづき)

■LAN のツイスト (より線) ケーブルには UTP と STP とがある.

◆シールド線はアースにつなぐ.

モジュラージャック － LAN ケーブルのためのジャック

■ツイスト線はモジュラープラグにつながれている.

◆プラグは透明なので，配線のようすがみえる.

■モジュラープラグを モジュラージャックにつなぐ.

図3-5 モジュラ　図3-6 RJ-45コネクタのピン配置

パソコンのイーサネットへの接続

■パソコンを LAN につなぐには，NIC (ネットワーク・インターフェース・カード) をつかう.

◆NIC のドライバー (ソフトウェア) をパソコンにインストールする必要がある.

パソコンには LAN 以外にもいろいろなインターフェースがある.

図3-2 LANカード　図3-3 パソコン背面の外部接続端子(例)

パソコンのイーサネットへの接続 (つづき)

■10 G イーサネットも普及してきた

◆10GBASE-T -- 銅線使用

◆10GBASE-LR など -- 光ケーブル

イーサネットの基本パケット転送法: ブロードキャスト

■イーサネットでの通信はブロードキャストが基本

◆通信可能な相手がすべて 1 本の線でむすばれる.

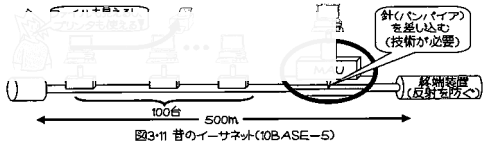


図3-11 昔のイーサネット(10BASE-5)

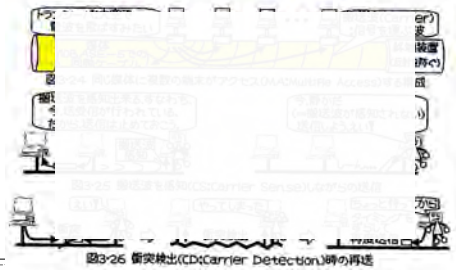
◆当初は 500 m 以内しか通信できなかった.

CSMA/CD (衝突検出)

■ イーサネットでは複数の端末が同時に出力することがあるため，衝突をさけるしくみが必要．

■ CSMA/CD はこの衝突をさけるしくみ．

- CSMA/CD - Carrier Sense Multiple Access with Collision Detection



CSMA/CD (衝突検出) (つづき)

織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

リピータによって通信距離をのばすことができる

■ デジタル信号レベルでコピー (リピート) される．

■ リピータで接続された全セグメントにブロードキャスト (一斉送信) される．

- 通常は 1 箇所でしか受信されないにもかかわらず…

パケットの選択的な送受信と MAC アドレス

■ ブロードキャストが基本なので，受信者が必要なパケットを選択する必要がある．

- 1 本の線でつなぐときでも送信先の指定が必要
  — MAC アドレスで指定する．

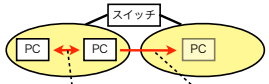
織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

MAC アドレス

■ MAC アドレスは位置とは無関係

IP アドレスとはちがう

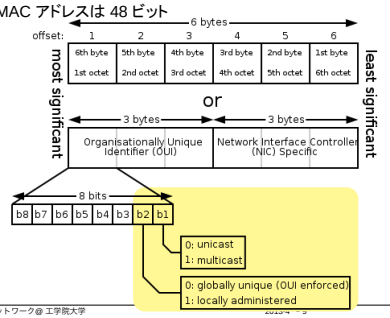
- ネットワーク上の位置とも，物理的な位置とも無関係 (他の位置に移動してもアドレスをかえなくてよい)
- 基本的にハードウェア (LAN カードなど) できまる (図 3.29).
- ただし，最近の LAN カードは MAC アドレスを変更できる．



MAC アドレス (つづき)

■ イーサネットのアドレスを MAC (マック) アドレスとよぶ．

- MAC = Media Access Control
- MAC アドレスは 48 ビット



MAC アドレス（つづき）

織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

プチ演習: MAC アドレス

■ 2 進数のアドレスを 16 進数で書きなおしてみよう．

- 000000000010000000100111101010100111001011100000
- 000001001010001100100011010111110100001100100011

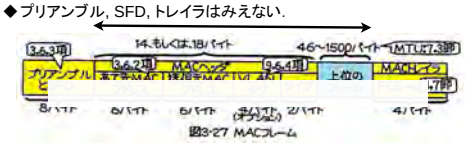
■ 16 進数のアドレスを 2 進数で書きなおしてみよう．

- 58-55-CA-FB-2D-B7
- 32-61-3C-4E-B6-05

イーサネットのパケット・フォーマット

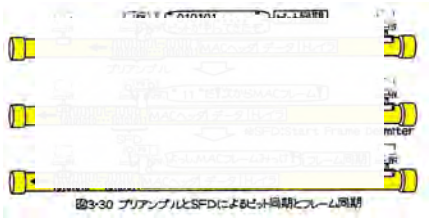
■ パケットとしてみえるのは MAC ヘッダ (14 ～ 18 バイト) と上位のフレームだけ．

- プリアンブル，SFD，トレイラはみえない．



イーサネット・パケットのプリアンブル, SFD, トレイラ

■ イーサネットのパケットは先頭と末尾にパケット内容でないものをふくむ.
- ◆プリアンブル, SFD: パケット (MAC フレーム) の先頭をみつけるための部分.
- ◆トレイラ: パケット内容の誤り訂正情報などをふくむ部分.



LAN の構造 (トポロジー)

■ 有線 LAN の基本構造には 3 種類ある.
- ◆バス型: 1 本の線 (バス) に全端末が接続される
- ◆スター型: 1 個のハブに全端末が接続される (ハブ & スポーク)
- ◆リング型: 各端末からでた 2 本の線でリングがつくられる

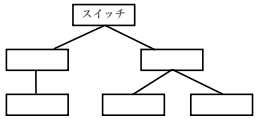
■ このような, ネットワークにおける接続関係 (グラフ構造) をトポロジーという.

イーサネットのためのネットワーク構造

Theo Gray, "Mad Science", Black Dog & Leventhal Publishers

イーサネットのためのネットワーク構造 (つづき)

■ ネットワークにループがあると転送できない (ネットワークは木構造)
- ◆ループをつくるとどうなる? -- ビデオ (EtherLoop.MTS)



■ 障害 (断線など) があると通信できなくなる.

ストレート・ケーブルとクロス・ケーブル

■ 10 M, 100 M のイーサネットではストレート・ケーブルとクロス・ケーブルをつかいわける必要がある.

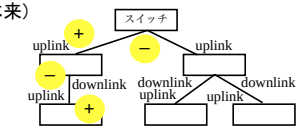
■ ギガビット・イーサネットでは自動認識されるので, 気にする必要がない.

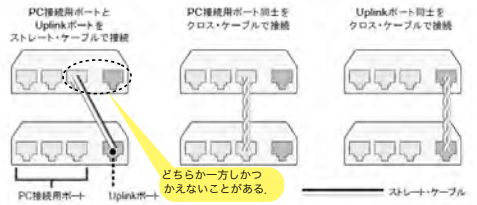
ストレート・ケーブルとクロスケーブル (つづき)

■「クロスケーブル (正確にはクロスオーバー・ケーブル)」は, インターネットにも他のプロトコルにも共通の概念.
- ◆マスターとスレーブがある物理プロトコルでマスターどうしをつなぐには, クロスケーブルが必要 (たとえばシリアル接続 – RS232C).

LAN ハブ (スイッチ) の接続法

■ 10 M / 100 M ハブには (本来) uplink ポートがある.
- ◆親には uplink でつなぐのが基本.
- ◆ほかのつなぎかたも可能.





http://itpro.nikkeibp.co.jp/article/COLUMN/20060318/232823/?SS=imgview&FD=5408972

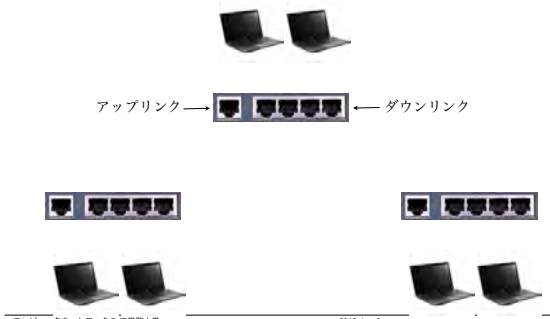
LAN ハブ (スイッチ) の接続法 (つづき)

■ 1 G (ギガビット・イーサネット) は自動で uplink / downlink がきりかわるので, くべつは必要ない.

■ 10 M / 100 M でも自動切替機能のあるハブもある.

プチ演習: LAN ハブの接続

■ つぎの LAN ハブと PC を接続せよ.



ブロードキャストと衝突によって発生する問題

■ ブロードキャストだと一度に複数の端末が送信することができない.

■ 衝突が発生しているときはどの端末も送信できない.

イーサネットの高性能な転送法: スイッチング

■ スイッチ (スイッチング・ハブ)
- ◆ ブロードキャストされるネットワーク (= コリジョン・ドメイン) をスイッチがつなぐ.
- ◆ コリジョン・ドメインをまたがると, 同時に送信しても衝突 (コリジョン) はおこらない.

■ ブリッジ
- ◆ 2 個のコリジョン・ドメインをつなぐ装置をブリッジという.
- ◆ スイッチはブリッジの機能を 3 個以上のネットワークに拡張したもの.

図4-13 ブリッジ

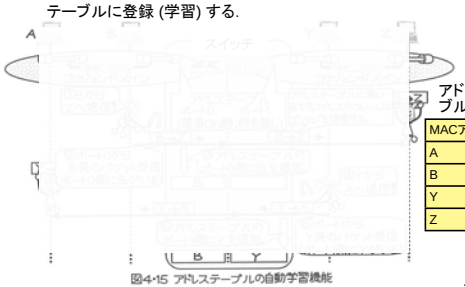
イーサネットの高性能な転送法: スイッチング (つづき)

■ 衝突のないイーサネット
- ◆ コリジョン・ドメイン内に 1 個の送信者しかいないようにすれば, 衝突はなくせる.

図4-18 スイッチングハブのみを用いた構成のLAN(構成例5)

イーサネットの高性能な転送法: スイッチング (つづき)

■ アドレス学習
- ◆ スイッチにパケットがとどくと, その送信者アドレスを学習する.
- ◆ スイッチは送信者アドレスとそれが入力されたポート番号とをアドレス・テーブルに登録 (学習) する.



アドレス・テーブルの形式

MACアドレス	ポート
A	0
B	0
Y	1
Z	1

図4-15 アドレステーブルの自動学習機能

無線 LAN

■ 無線をつかうイーサネットの規格 IEEE802.11, 802.11b, 802.11g, 802.11n などを総称して「無線 LAN」という.
- ◆ IEEE802.11 2.4 GHz 帯, 最大 2 Mbps
- ◆ IEEE802.11b 2.4 GHz 帯, 最大 11 Mbps, 1999 年に標準化
- ◆ IEEE802.11a 5 GHz 帯, 最大 2 Mbps, 1999 年に標準化
- ◆ IEEE802.11g 2.4 GHz 帯, 最大 54 Mbps, 2003 年に標準化
- ◆ IEEE802.11n 2.4 GHz / 5 GHz 帯, 最大 600 Mbps (通常は 300 Mbps まで), 2009 年に標準化

- ◆ 2.4 GHz 帯は電子レンジ, コードレス電話などでもつかわれているので干渉がおこりやすい.

無線 LAN (つづき)

■ 無線 LAN のためのデバイス (機器)

アクセスポイント (親機)

子機 (ノート PC 専用)

(最近のノート PC は子機を内蔵しているものが多い)

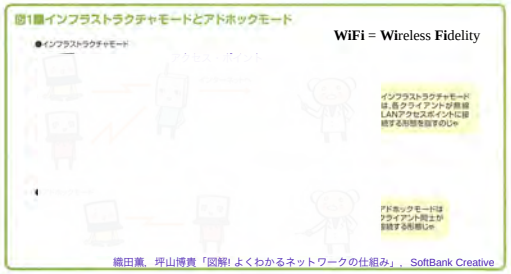
子機 (デスクトップ PC 専用)

子機 (汎用 ― USB 型)

http://ja.wikipedia.org/wiki/無線LAN

無線 LAN (つづき)

■ 無線 LAN (WiFi) には 2 つのモードがある.
- ◆ インフラストラクチャ・モードではアクセス・ポイント経由で通信する ― インターネット通信ではこのほうが便利.
- ◆ アドホック・モードでは PC どうしが直接, 通信する.



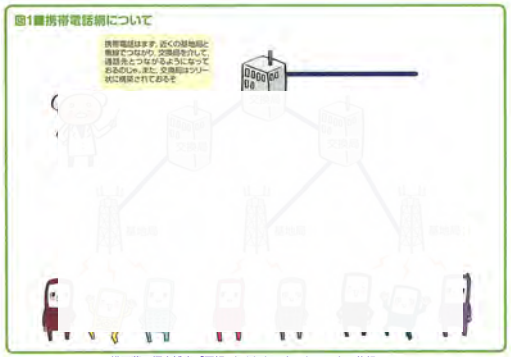
織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

無線 LAN (つづき)

■ 無線 LAN で広域をカバーする方法
- ◆ 携帯電話と同様の方法だが, 無線 LAN ではあまりつかわれていない.
- ◆ 無線 LAN ではこの方法が携帯電話ほど, うまくいかない ―― ハンドオーバがおそい.


織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

携帯電話と無線 LAN



織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

携帯電話と無線 LAN (つづき)

織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

携帯電話と無線 LAN (つづき)

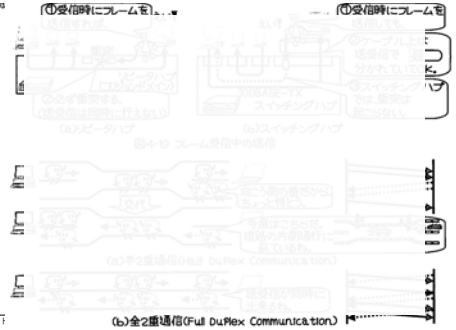
織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

携帯電話と無線 LAN (つづき)

織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

全二重通信と半二重通信

■ 双方向通信においては，双方向同時に通信する場合 (電話にちかい) と，片方向ずつ通信する場合 (アマチュア無線などにちかい) とがある．



演習問題: LAN の設計と動作

■ オフィスの形状と 8 個の机の配置をきめ，つぎの機器を設置する (設置場所もきめる)．

◆スイッチング・ハブ (uplink/downlink 自動認識):
ギガビット (1000BASE-T) 4 ポート: 1 台
100 M ビット (100BASE-TX) 8 ポート: 1 台
100 M ビット (100BASE-TX) 4 ポート: 1 台

◆サーバ 1 台 --- ギガビットでつなぐ (通信量が多いため)．

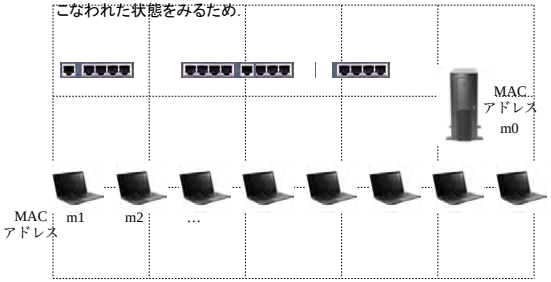
◆8 台の PC を机上に配置する．

◆配線: 基本的にはカテゴリー 5 (100 M ビット) のケーブル (ストレート・ケーブル) によるが，必要に応じてカテゴリー 6 (ギガビット) のケーブルを使用する．

演習問題: LAN の設計と動作 (つづき)

■ さらに，サーバおよび半数程度の PC がパケットを送信したあとの各スイッチのアドレス・テーブルの内容を記述する．

◆全部でなく半数程度としているのは，完全な学習でなく部分的な学習がおこなわれた状態をみるため．



演習問題 (レポート課題): LAN の設計と動作

■ 課題 1: 機器を手で (紙と鉛筆で) 配置・配線し，その結果を簡易レポートとして提出する (説明は不要．なぐり書きでよい)．
- ◆提出方法: 書いた紙を 5 月 25 日までに講義の際または教務課に提出．
- ◆採点: 課題を実施し提出したかどうかだけを採点する (内容は問わない)．

■ 課題 2: 最初のレポートで提出した配線をシミュレータで確認し，レポートとして提出する (レポートとしての体裁をととのえること)．
- ◆どこにどの機器を配置し，どのケーブルを使用したかを図示する．
- ◆サーバおよび半数程度の PC がパケットを送信したあとの各スイッチのアドレス・テーブルの内容を記述する．
- ◆どうかんがえて配置・配線したかを 10 行程度で書く (箇条書きがよい)．
- ◆講義の際の例題とはことなる配置にすること．(へやのかたちや机の配置などは自由にきめてよい --- 他人のコピーをしたら 0 点とする)
- ◆シミュレータは Python のプログラム (5/26 までに，Kuport にアップロード)
- ◆提出方法: 紙で (レポート用紙等に書いて / A4 上質紙に印刷して) 提出するのが基本．しかし，理由があれば電子的に提出することも可．
- ◆期限: 6 月 8 日 (土) (当日提出できなければ，事前に 教務課に (またはメイル等で) 提出すること．10 日以降に提出したものは減点の可能性あり)

演習問題 (レポート課題): LAN の設計と動作 (つづき)

■ 採点方法 (一部変更)
- ◆15 点満点
- ◆まちがいがなければ 15 点，まちがい 1 回ごとに基本的に −1 点．
- ◆工夫がある答案には最大 7 点加算 (テストで 7 点減点されても満点になりうる)．
- ◆シミュレータでの実験結果を記述すれば，加点の対象とする (必須ではない)．
  - ●実験の例
    - 複数のスイッチがあるネットワークにおいて，学習の順序によって MAC テーブルの内容がどう変化するか (端末の移動があると一致しないことがある) をしらべる．
    - タイムアウト (忘却) しないと通信できなくなるケースをしらべる．
    - スイッチの 2 個のポートをつないでループをつくって動作をみる．
    - プログラムをかきかえて，現在のプログラムでは実験できないことをしらべたり，プログラムのバグをなおして実験したりする．(バグをみつけたら報告してください．)
    - プログラムをかきかえて，複数のネットワーク・インターフェースをもつ PC を (シミュレータではない本物の) スイッチング・ハブにしたてる．

演習問題 (レポート課題): イーサネット・シミュレータ

■ シミュレータのプログラムは Kuport にアップロードした．
- ◆このプログラムに著作権はつけない (パブリック・ドメインとする)．

■ シミュレータは 1 台の PC 上で動作する．

■ Windows, MAC, Linux の Python 3 で動作する
- ◆プログラム内の指定の箇所をかきかえると Python 2 でも動作する．

■ シミュレータは 2 つのプログラムで構成されている: switch.py, term.py．

■ すべての機器 (スイッチ，端末) において，ことなるポート番号を使用する．
- ◆シミュレータはポート番号を UDP ポート番号として使用するので，ユーザが使用可能な番号を指定する．

■ 詳細は readme.txt 参照

演習問題 (レポート課題): イーサネット・シミュレータ (つづき)

■ switch.py はイーサネット・スイッチング・ハブのシミュレータ.

◆ 使用例

```
python switch.py \
    --nports 3 \        # スイッチのポート数 (最大で 8)
    --lp0 55000 \       # スイッチのポート番号 (使用できない値に注意!)
    --rp0 55100 \       # lp0 の接続先の端末のポート番号 (配線指定)
    --lp1 55001 --rp1 54001 --lp2 55002 --rp2 54002 \
                \       # スイッチの他のポートの配線を指定
    --dumpMAC \         # 指定すると MAC アドレス・テーブルをダンプ
    --monitor 0 \       # パケット送受信情報を出力するかどうかの指定
                \       #  (0 なら出力しない. 0, 1, 2 が指定できる)
    --timeout 30 \      # 学習結果のタイムアウト時間を変更
    --help              # コマンドライン・パラメタの説明を表示
```


演習問題 (レポート課題): イーサネット・シミュレータ (つづき)

■ term.py はパケットを送受信する端末 (PC) のシミュレータ

◆ 使用例

```
python term.py \
    --lm 000300000001 \     # この端末の MAC アドレス
                            # (16 進 12 桁 (48 bit) の値を自由に指定できる)
    --rm 000300000002 \     # 通信相手の MAC アドレス
    --lp 54001 \        # 端末のポート番号 (使用できない値に注意!)
    --rp 55001 \        # 接続先の端末のポート番号
                \       # (スイッチ側と配線指定を一致させること)
    --promiscuous \     # プロミスキャス・モードを指定
                \       # (この端末あて以外のパケットも受信する)
    --receiveOnly \     # パケットを送信しない
    --help              # コマンドライン・パラメタの説明を表示
```


イーサネットのまとめ

■ イーサネットは比較的せまい範囲でつかうのに適したネットワークの規格 (標準)

◆ もとは 500 m くらいの範囲でしかつかえなかったが, 現在では日本全体の数 10 拠点をカバーすることも可能

■ イーサネットのアドレスは 1 個ずつ, ばらばら

◆ ちかくに位置する PC でもアドレスは似ていない

◆ インターネットでは, ちかくに位置する PC はアドレス上位が一致

■ ネットワークにループがあると転送できない (ネットワークは木構造)

◆ 障害 (断線など) があると通信できなくなる.

■ パケットは 2 種類の方法で転送される.

◆ ブロードキャスト + 衝突検出 (CSMA/CD) -- ケーブルとリピータで転送

◆ スイッチング + 学習 -- スイッチで転送

4. インターネットとインターネット・プロトコル (IP)

要点

■ IP (インターネット・プロトコル) は世界中の多数のコンピュータをつなぐのに適したネットワーク標準

◆ 億単位のコンピュータをつないで, うごかせるネットワーク規格はほかにない.

■ IP のアドレスは位置でまとめられている

◆ ネットワーク上でちかくに位置する PC はアドレス上位が一致している.

■ ネットワークにループがあってもよい (ネットワークは任意のグラフ構造)

◆ 障害 (断線など) がおこっても通信がきれにくい.

■ パケットはルータによって転送される

◆ 転送先はルーティングによってきまる.

インターネットとは?

■ IP (インターネット・プロトコル) は IETF という標準化組織で標準化された, 世界中をつなぐためのネットワーク標準である.

◆ IETF = Internet Engineering Task Force

■ IP は世界中の多数のコンピュータをつなぐのに適したプロトコルである.

◆ 億単位のコンピュータがつなげるネットワーク標準はほかにない.

■ インターネットは「ネットワークのネットワーク」といわれる
— 地域ごとのネットワークをつなぎあわせて, つくられている.

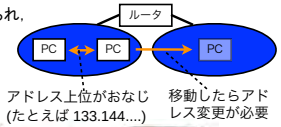
IP アドレス

■ インターネットのアドレスを IP (Internet Protocol) アドレスという.

■ ちかい位置にあるコンピュータの IP アドレスは上位が共通

◆ ネットワークはセグメントにわけられ, セグメント内では IP アドレス上位 (サブネット) が共通.

◆ 他の位置に移動すると IP アドレスを変更する必要がある.



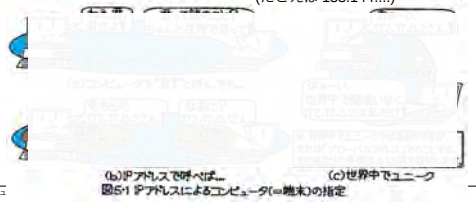


図5-1 IPアドレスによるコンピュータ(=端末)の指定

IP アドレス (つづき)

世界中のひとに 1 個ずつわりあてることもできない.

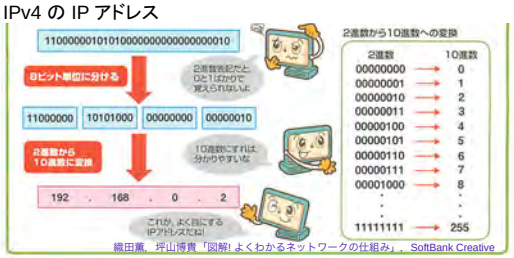
■ IP アドレスには 2 つのバージョンがある.

◆ IP バージョン 4 (IPv4) -- 現在でも主流だが, アドレス空間は 32 bit しかないので, 昨年, 枯渇した (新アドレスを IANA から配布できない).

◆ IP バージョン 6 (IPv6) -- アドレス空間が 128 bit ある (天文学的な数のアドレスがある) ので, 枯渇する心配がない.

Internet Assigned Numbers Authority

■ IPv4 の IP アドレス



プチ演習: IP アドレス

■ IP アドレスの記法

◆ つぎの IP アドレスを 2 進数および 16 進数で記述せよ.

10 進: 192.168.1.9　　10.232.50.81

2 進:

16 進:

◆ つぎの IP アドレスを 10 進表現になおせ.

16 進: 0x 85 90 0C 62　　0x CA 98 93 3A

10 進: ＿＿＿＿　　＿＿＿＿

IP パケットのフォーマット

■ IP パケットは IP ヘッダとペイロード (内容) とで構成される.

■ IPv4 ヘッダの構造

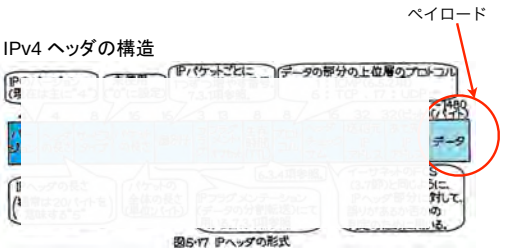
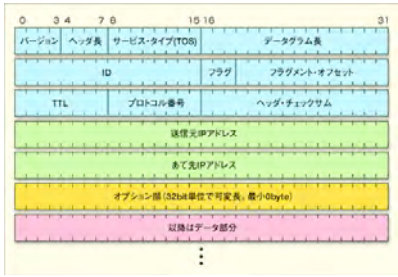


図5-17 IPヘッダの形式

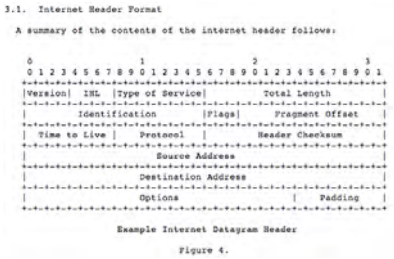
パケット・フォーマットの記述法と実際

■4 バイトごとに改行するのが流儀



パケット・フォーマットの記述法と実際 (つづき)

■IP のパケット・フォーマットは IETF の RFC 791 という標準ドキュメントで規定されている.


3.1. Internet Header Format

A summary of the contents of the internet header follows:

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version	IHL	Type of Service	Total Length
Identification	Flags	Fragment Offset
Time to Live	Protocol	Header Checksum
Source Address
Destination Address
Options	Padding

Example Internet Datagram Header

Figure 4.

IP パケットの転送とルータ

■IP パケットはルータによって転送される.

◆パケットに受信者と送信者のアドレスがふくまれているのはイーサネットとおなじ.

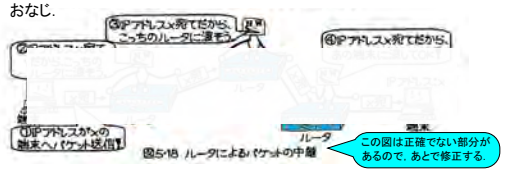


図5-15 ルータによるパケットの中継

◆しかし, イーサネットとはちがって「サブネット」を単位として転送される.

◆ただし, 同一 LAN セグメント内はルータを経由せず直接または LAN スイッチ経由でとどけられる.
(このようなイーサネットと IP とのくみあわせは 5 章であつかう.)

IP アドレスの構造とサブネット

■IP アドレスはネットワーク・アドレスとホスト ID とで構成される.

◆ネットワーク・アドレスはちかくに位置する PC 間で共通 (サブネット内で共通).

◆ネットワーク・アドレスのビット数 (アドレス空間のひろさ, アドレス数) はサブネット (LAN) ごとにことなる.

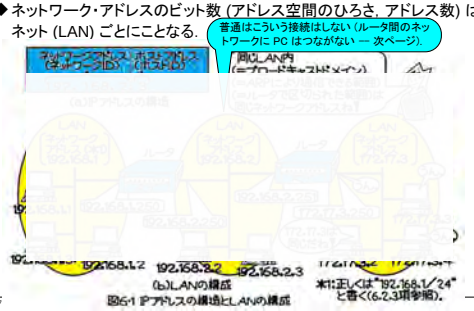


図5-1 IPアドレスの構造とLANの構成

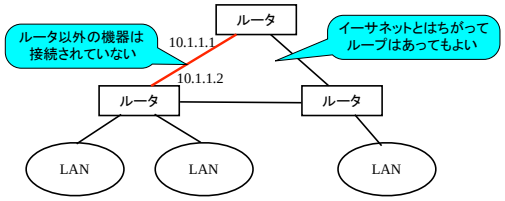
ルータとルータ, LAN の接続

■LAN は 1 個だけのルータに接続するのが基本.

■ルータ間をつなぐのは Ethernet とはかぎらない.

◆さまざまなメディア (L2 ネットワーク) がつかわれる: ATM, 光パス, 他.

■ルータ間を Ethernet でつなぐときも 1 本のリンクだけがあるのが普通.



3 とおりのサブネットの表現法

■ビット長による表現

◆サブネットが 24 ビット, ホストアドレスが 8 ビットのとき: /24 をつける.

◆例: 192.168.1/24 または 192.168.1.0/24

■サブネット・マスクによる表現

◆サブネット・マスクをつける.

◆例: 192.168.1.0/255.255.255.0

図6-2 サブネットマスク

■ワイルドカードによる表現 (正規表現)

◆ホストアドレスの部分をワイルドカード (*) で表現する

◆例: 192.168.1.*

◆ホストアドレスが 8, 16, 24 ビットのときだけしかつかえない.

むかしはこれでだいたいいつでも表現できた

サブネット内外との通信

■サブネット内は直接, 通信する (ルータを経由しない).

■サブネット外とはデフォルト・ゲートウェイ (LAN につながったルータ) 経由で通信する.

図6-3 サブネットマスクを使っての通信経路の判定

プチ演習: サブネットとホストアドレス

- IP アドレスが 192.168.4.3, ネットワークアドレスが 24 ビットのとき, つぎの値をもとめよ.
  - サブネットマスク _____
  - ネットワークアドレス _____ / 24
  - ホストアドレス (8 ビット) ___
- ネットワークアドレスが 10.50/16, ホストアドレスが 20.100 のとき, つぎの値をもとめよ.
  - サブネットマスク _____, IP アドレス _____
- IP アドレスが 192.168.4.3, ネットワークアドレスが 20 ビットのとき, つぎの値をもとめよ.
  - サブネットマスク _____
  - ネットワークアドレス _____ / 24
  - ホストアドレス (8 ビット) ___
- ネットワークアドレスが 10.50.128/18, ホストアドレスが 20.100 のとき, つぎの値をもとめよ.
  - サブネットマスク _____, IP アドレス _____

ルーティングとは?

■ルータはルーティング・テーブルにしたがってパケットの転送先 (ネクストホップ) をきめる.

■パケットの経路をきめる (ルーティング・テーブルを生成する) ことを「ルーティング (経路制御)」という.

◆パケットの「転送」はデータ・パケットを直接あつかう (データ・プレーンの処理).

◆「ルーティング」はデータ・パケット転送のための制御をするだけ (制御プレーンの処理) である.

●ただし, 制御情報のやりとりにもパケット (制御パケット) がつかわれる.

ルーティング・テーブルと転送

■ あらかじめつくったルーティング・テーブルの内容にしたがって，IP パケットを転送する．

図6-7 ルーティングテーブルによるパケットの中継

■ 経路はホップごと (1 回の転送ごと) に局所的にきめられる．

◆ ルータは通常はパケットの経路全体を知らない．

ルーティング・テーブルと転送 (つづき)

■ 隣接ルータにイーサネットで接続されているときの転送動作

◆ ネクストホップ IP アドレスからそれに対応する MAC アドレスをもとめて，イーサネットのしくみにしたがって転送する．

●MAC アドレスをもとめるには ARP テーブルをつかう -- 5 章であつかう．

ダイナミック・ルーティングとスタティック・ルーティング

■ ルーティングにはつぎの 2 種類がある．

◆ スタティック (静的) ルーティング：人手などであらかじめルーティング・テーブルを設定する ― 再設定するまでその内容は変化しない．

◆ ダイナミック (動的) ルーティング：ルーティング・アルゴリズムによってルーティング・テーブルを設定する ― その内容はルータの動作中に変化する．

図6-11 スタティックルーティングとダイナミックルーティング

ダイナミック・ルーティングの本質

■ ルーティングによってあらかじめ最短路をみつけておく．

◆ パケット転送時に最短路をもとめるのは困難なので事前にもとめる．

◆ みつけた転送先はルーティング・テーブルに保管する．

◆ ループのあるネットワークでもパケットを最短路でとどけることができる．

■ ルーティング・アルゴリズムは (近似的に) 最短路をみつける．

◆ 最短路探索の基本はダイクストラのアルゴリズム．

■ ネットワークの構造は変化するので，最短路をもとめなおす．

◆ ダイナミック・ルーティングは ネットワークの変化に応じて再計算するルーティング方式．

最短経路をもとめるダイクストラ法

■ ダイクストラ法はグラフの各点から特定の点への最短距離 (経路) を逐次的に (= 1 台のコンピュータで) もとめる方法である．

◆ ダイクストラ法 = ダイクストラののアルゴリズム

◆ 数学的なネットワーク (グラフ) のアルゴリズムとしてもっとも重要なもののひとつである．

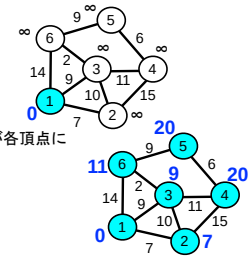
■ 入力

◆ グラフ (ネットワーク)

◆ グラフ上の終点 (「特定の点」)

■ 出力

◆ 最短距離 (に対応する隣接ノード) が各頂点に付加されたグラフ．



最短経路をもとめるダイクストラ法 (つづき)

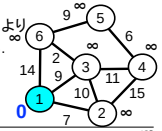
■ アルゴリズム

◆ 0. [初期化] 全てのノードの終点までの距離を無限大 (or 非常に大きな値) に初期化する (ただし終点の終点までの距離は 0 としておく)．

◆ 1. [ノードの確定] 未確定ノードのなかから終点までの距離が最小のノードを選択して確定ノードにする (確定ノードに隣接していないノードは無限大の距離を持つため，自然と確定ノードに隣接するノードの中から確定する)．

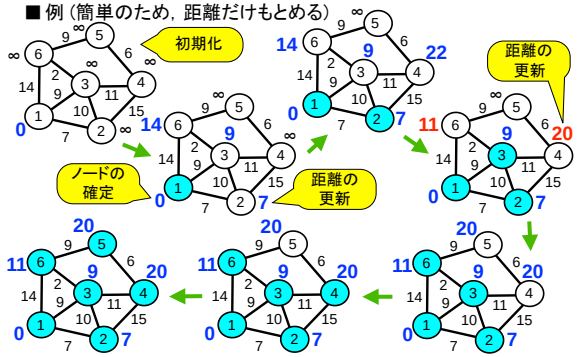
◆ 2. [距離の更新] 確定ノード a に隣接する全ノード bi に対して，つぎのようにして終点までの距離を更新する．
i) bi が確定済のノードなら何もしない．
ii) 確定ノード a の終点までの距離とノード a とノード bi 間の距離とをたした値をもとめ，これを d とする．
iii) d がノード bi に設定されている終点までの距離よりもちいさい場合は d を bi のゴールまでの距離にする．

◆ 3. [終了判定] すべてのノードが確定したら終了．それ以外は 1. へもどる．



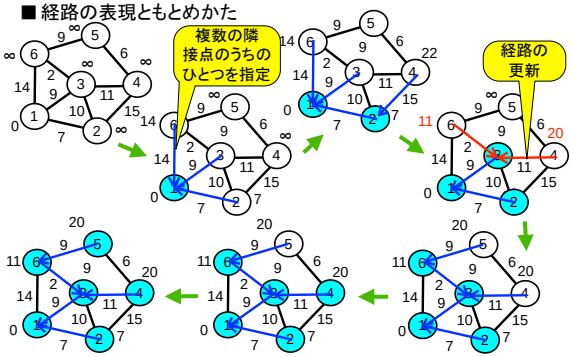
最短経路をもとめるダイクストラ法 (つづき)

■ 例 (簡単のため，距離だけもとめる)



最短経路をもとめるダイクストラ法 (つづき)

■ 経路の表現ともとめかた



ルーティング・アルゴリズムとダイクストラ法とのちがい

■ ひとつの経路か，複数か?

◆ ダイクストラ法においてはグラフの特定の頂点への最短経路をもとめる．

◆ ルーティング・アルゴリズムにおいてはグラフ (= ネットワーク) の各頂点 (= ルータ) と他の各頂点とのあいだの最短経路をもとめる．

■ 計算するのは 1 台か，複数か?

◆ ダイクストラ法においては 1 台のコンピュータによってもとめる．

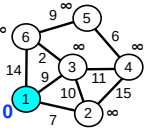
◆ ルーティング・アルゴリズムにおいては，通常は全ルータが参加してもとめる．

◆ ダイクストラ・ルーティングの計算や通信をルータから分離する方法も提案されている．

●1 個のサーバで計算する方法 (集中型)

●複数のサーバが連携して計算する方法 (ルータと同様に分散型)

ルーティング・サーバの亡霊 ?! (最近では OpenFlow がらみで復活)

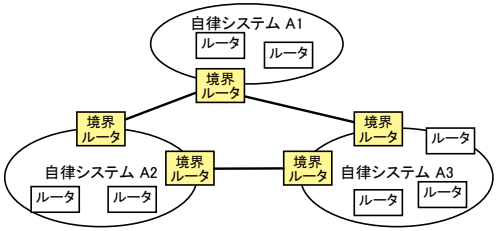


アルゴリズムによるルーティング法の分類

- 距離ベクトル・ルーティング (distance vector routing)
  - Bellman-Ford アルゴリズムにもとづいている.
  - 各ルータは自分と他のルータとの距離だけを管理する.
  - 距離ベクトルにもとづくルーティング・プロトコルとして **RIP** (Routing Information Protocol) が代表的である.
- リンク状態ルーティング (link state routing)
  - 各ルータが他の 2 個のルータ間の距離も管理する.
  - リンク状態にもとづくルーティング・プロトコルとして **OSPF** (Open Shortest Path First) が代表的である.

ネットワーク制御との関係によるルーティング法の分類

- [分類のための準備] IP ネットワークは自律システム (autonomous system, AS) とよばれる管理単位で構成される.
  - たとえば, ひとつのインターネット・プロバイダのネットワークがひとつの自律システム.



ネットワーク制御との関係によるルーティング法の分類 (つづき)

- **IGP (Interior Gateway Protocol)**
  - 自律システム内で使用されるルーティング・プロトコル.
  - 代表的な IGP として RIP, OSPF がある.
- **EGP (Exterior Gateway Protocol)**
  - 自律システム間で使用されるルーティング・プロトコル.
  - 代表的な EGP として BGP (Border Gateway Protocol) がある.

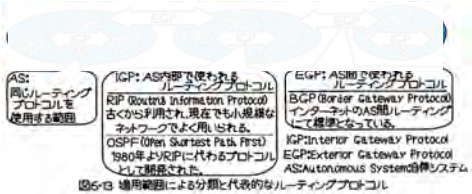


図6-13 適用範囲による分類と代表的なルーティングプロトコル

ダイナミック・ルーティングとネットワーク障害

- ダイナミック・ルーティングをつかっていれば, ネットワークに障害が発生しても自動的に迂回する (対処できる).

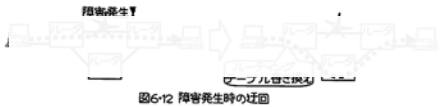


図6-12 障害発生時の迂回

ルーティングにおけるアドレスの集約

- 「集約」によってルーティング・テーブルのサイズをちぢめられる.

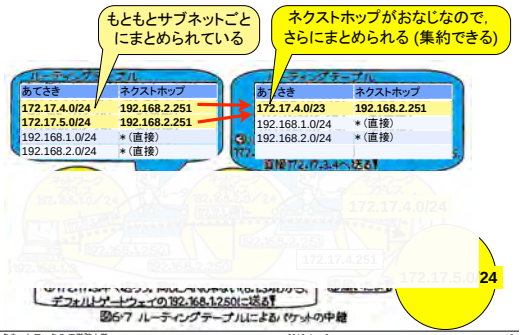
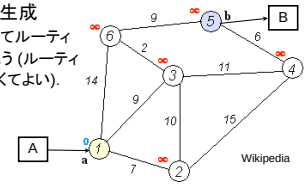


図6-7 ルーティングテーブルによるパケットの中継

プチ演習: ルーティング

- ルーティング・テーブルの手生成
  - A から B への最短路をもとめてルーティング・テーブルを生成してみよう (ルーティング・アルゴリズムどおりでなくてよい).



- 転送のシミュレート
  - 生成したルーティング・テーブルにしたがって A から B へのパケットの転送をシミュレートしてみよう.

インターネットの制御プロトコルと体験

- インターネットの設定, 通信のようす, 経路などをみてみよう.
- つぎのようなプロトコルやツールがつかえる.
  - IP の設定
    - コントロール・パネルなど.
  - パケットをみる.
    - wireshark によるキャプチャ.
  - 通信のようすをみるプロトコル ICMP と関連コマンド.
    - ping による応答時間などの把握.
    - traceroute による経路などの把握.
- 以下これらのプロトコルやツールについて説明する.

パソコンにおける IP の設定

- コントロールパネルにおける設定 (Windows のとき)

図6-24 Windows XPでのネットワーク設定

パソコンにおける IP の設定 (つづき)

- ipconfig (ifconfig) コマンドによる確認
  - Windows なら ipconfig, Linux/Mac などなら ifconfig コマンドをつかえば IP アドレスなどに関する設定内容をみることができる.

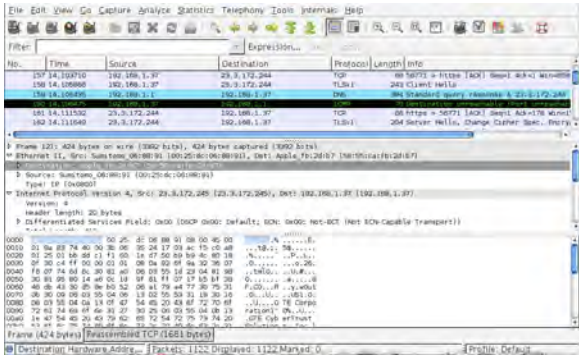
パソコンにおける IP の設定 (つづき)

■ ifconfig の実行例

```
MacBook-Kana:~ yk$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        ether 58:55:ca:fb:2d:b7
        inet6 fe80::5a55:caff:fefb:2db7%en0 prefixlen 64 scopeid 0x4
        inet 192.168.1.37 netmask 0xffffff00 broadcast 192.168.1.255
        inet6 2408:41:44cd::5a55:caff:fefb:2db7 prefixlen 64 autoconf
        inet6 2408:41:44cd::78d4:bfb2:daad:d3b7 prefixlen 64 autoconf temporary
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 0a:55:ca:fb:2d:b7
        media: autoselect
        status: inactive
MacBook-Kana:~ yk$
```


IP パケットのキャプチャ

■ Wireshark でパケットをみる.



インターネットの制御プロトコル ICMP と ping

■ 制御用のプロトコル ICMP (Internet Control Message Protocol)

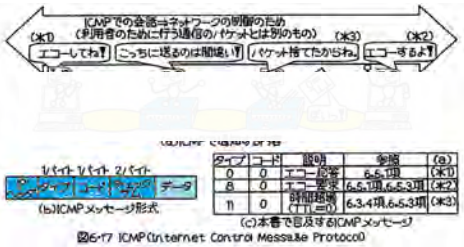


図6-17 ICMP(Internet Control Message Protocol)

インターネットの制御プロトコル ICMP と ping (つづき)

■ ネットワークの導通性をテストするコマンド ping

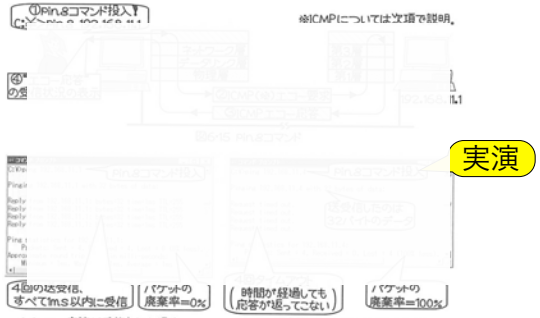


図6-16 Pingコマンドの投入例

インターネットの制御プロトコル ICMP と ping (つづき)

■ ping の実行例 (Macintosh)

```
MacBook-Kana:~ yk$ ping www.kanadas.com
PING kanadas.com (219.94.162.224): 56 data bytes
64 bytes from 219.94.162.224: icmp_seq=0 ttl=54 time=21.472 ms
64 bytes from 219.94.162.224: icmp_seq=1 ttl=54 time=14.725 ms
64 bytes from 219.94.162.224: icmp_seq=2 ttl=54 time=16.270 ms
64 bytes from 219.94.162.224: icmp_seq=3 ttl=54 time=17.375 ms
64 bytes from 219.94.162.224: icmp_seq=4 ttl=54 time=17.875 ms
64 bytes from 219.94.162.224: icmp_seq=5 ttl=54 time=22.389 ms
64 bytes from 219.94.162.224: icmp_seq=6 ttl=54 time=15.449 ms
64 bytes from 219.94.162.224: icmp_seq=7 ttl=54 time=17.093 ms
64 bytes from 219.94.162.224: icmp_seq=8 ttl=54 time=19.291 ms
64 bytes from 219.94.162.224: icmp_seq=9 ttl=54 time=21.739 ms
64 bytes from 219.94.162.224: icmp_seq=10 ttl=54 time=16.690 ms
64 bytes from 219.94.162.224: icmp_seq=11 ttl=54 time=15.533 ms
64 bytes from 219.94.162.224: icmp_seq=12 ttl=54 time=17.986 ms
64 bytes from 219.94.162.224: icmp_seq=13 ttl=54 time=15.859 ms
```


パケットの生存期間と traceroute

■ IP パケットの TTL フィールドによって生存期間がきまる.

- ◆ TTL = Time To Live
- ◆ パケットがルータ間で転送されるごとに, TTL は 1 ずつ, へらされる.
- ◆ TTL が 0 になるとパケットは廃棄される (「死ぬ」).

図6-10 TTLによるパケットの廃棄

パケットの生存期間と traceroute (つづき)

■ TTL を利用して経路をしらべるコマンド traceroute

図6-18 tracertコマンド

パケットの生存期間と traceroute (つづき)

■ traceroute の実行例 (Macintosh)

```
MacBook-Kana:~ yk$ traceroute www.kanadas.com
traceroute to kanadas.com (219.94.162.224), 64 hops max, 52 byte packets
 1  ntt.setup (192.168.1.1)  10.494 ms  0.966 ms  0.914 ms
 2  tkynikz.asahi-net.or.jp (202.224.37.87)  4.738 ms  9.640 ms  3.990 ms
 3  tkybi4-v15.asahi-net.or.jp (202.224.37.81)  9.538 ms  3.854 ms  5.689 ms
 4  kddni93.asahi-net.or.jp (202.224.32.93)  4.990 ms  5.456 ms  8.137 ms
 5  as9370.ix.jpix.ad.jp (210.171.224.113)  5.964 ms  4.465 ms  4.838 ms
 6  tkgrt1s-ort3-10g.bb.sakura.ad.jp (59.106.251.34)  6.113 ms  5.418 ms
    tkwrt1s-ort3.bb.sakura.ad.jp (59.106.251.138)  5.301 ms
 7  tkwrt3-wrt1s.bb.sakura.ad.jp (59.106.247.118)  6.393 ms  5.480 ms  5.255 ms
 8  oskrt1-tkwrt3.bb.sakura.ad.jp (59.106.255.238)  16.961 ms  14.623 ms  16.774 ms
 9  osnrt1s-krt1.bb.sakura.ad.jp (59.106.255.18)  14.450 ms  14.893 ms  13.659 ms
10  osnrt102b-nrt1s.bb.sakura.ad.jp (59.106.244.142)  14.891 ms
    osnrt101b-nrt1s.bb.sakura.ad.jp (59.106.244.138)  13.447 ms
    osnrt102b-nrt1s.bb.sakura.ad.jp (59.106.244.142)  13.561 ms
11  osnrt108e-nrt102b.bb.sakura.ad.jp (59.106.253.190)  13.817 ms
    osnrt108e-nrt101b.bb.sakura.ad.jp (59.106.253.86)  14.795 ms
    osnrt108e-nrt102b.bb.sakura.ad.jp (59.106.253.190)  14.241 ms
12  www1384.sakura.ne.jp (219.94.162.224)  15.459 ms  15.008 ms  19.607 ms
MacBook-Kana:~ yk$
```


インターネットと IP のまとめ

■ IP (インターネット・プロトコル) は世界中の多数のコンピュータをつなぐのに適したネットワークの規格

- ◆ 億単位のコンピュータをつないで, うごかせるネットワーク規格はほかにない.

■ IP のアドレスは位置でまとめられている

- ◆ ネットワーク上でちかくに位置する PC はアドレス上位が一致している.

■ ネットワークにループがあってもよい (ネットワークは任意のグラフ構造)

- ◆ 障害 (断線など) がおこっても通信がきれにくい.

■ パケットはルータによって転送される

- ◆ 転送先はルーティングによってきまる.

5. インターネットとイーサネット

要点

■ [比較] IP とイーサネット
- ◆IP は転送時にアドレスを集約してあつかえるが，イーサネットは個別にあつかう必要がある．
- ◆そのため，IP はスケールする (大規模ネットワークに適用できる) が，イーサネットはスケールしない．
- ◆IP ネットワークにはループが許容されるが，イーサネットにはループが許容されない．

■ [くみあわせ] LAN ではイーサネットと IP をかさねてつかう (IP/Ethernet)
- ◆プロトコルが層をなしているときは，内側のプロトコル (IP) をみたすように外側のプロトコル (イーサネット) で通信する．
- ◆イーサネットにも IP にもアドレスがあるので，それらを対応づけるのが重要 -- ARP というプロトコルをつかって対応づける．

イーサネットと IP の共通点

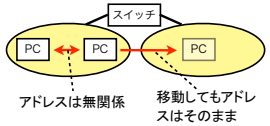
■ ネットワークに複数のコンピュータがつなげる．

■ 複数のなかから相手をアドレスで選択して通信できる．
- ◆複数の相手に送信することもできる (ブロードキャスト または マルチキャスト)

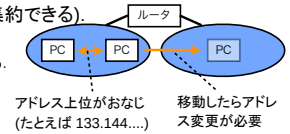
■ [まとめ] 基本的な機能は似ている．
- ◆通信するために，本来はどちらか一方だけをつかえばよいはず．

[比較] イーサネットと IP のアドレス

■ イーサネットのアドレス (MAC アドレス) は 1 個ずつばらばらである．
- ◆MAC アドレスは基本的にハードウェア (ネットワーク・インターフェース) によってきまっている．
- ◆ちかい位置にあるコンピュータの MAC アドレス間に関係はない．
- ◆コンピュータをほかの位置に移動させても MAC アドレスは変更する必要がない．



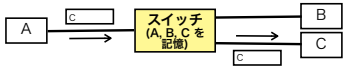
■ IP アドレスはまとめられる (集約できる)．
- ◆セグメント内のコンピュータの IP アドレスは上位が共通である．
- ◆コンピュータをほかのセグメントに移動させると IP アドレスを変更する必要が生じる．



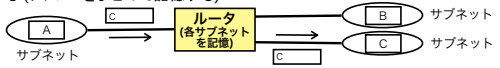
[比較] パケット転送法

■ イーサネット
- ◆リピータ: リピータをつかうと，ひとつのパケットがネットワーク内のすべての端末にとどく (その端末があてさきでなくても)．

- ◆スイッチ: パケットが到達するすべての端末のアドレスを記憶する．

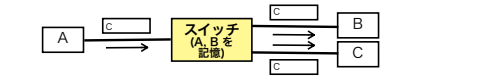


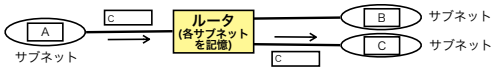
■ IP
- ◆ルータ: パケットが到達するネットワークのサブネット・アドレスを記憶する (アドレスをまとめて記憶する)．



[比較] パケット転送法 (つづき)

■ イーサネットのアドレス・テーブルと IP ネットワークのルーティング・テーブルとの比較
- ◆アドレス・テーブルにない (学習していない) アドレスへもイーサネット・パケットをとどけることができる -- ブロードキャスト (正確にはフラディング) による．
- ◆ルーティング・テーブルにないアドレスには IP パケットをとどけることができない．





[比較] スケーラビリティ

■ イーサネット (リピータ)
- ◆端末にすべてのパケットがとどくので，大規模なネットワークではパケットがあふれて，スケールしない (ブロードキャスト・ストームがおこる)．

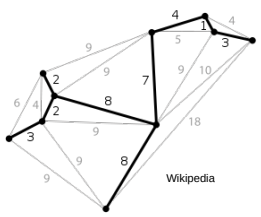
■ イーサネット (スイッチ)
- ◆スイッチが全アドレスを記憶するので，大規模なネットワークではアドレス・テーブルがあふれて，スケールしない．
- ◆リピータによるネットワークよりはスケールする．

■ IP
- ◆ルータはサブネット・アドレスだけを記憶すればよいので，スケールする．

[比較] ループの許容

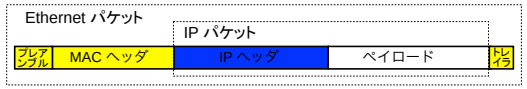
■ IP ではループが許容される ― 任意のグラフ構造．

■ イーサネットではループが許容されない ― 木構造．



[くみあわせ] プロトコルが階層化されているときの通信

■ LAN ではイーサネットと IP をかさねてつかう．
- ◆IP/Ethernet (アイピー・オーバー・イーサネット) ではイーサネットのパケットが IP のデータ (フレーム) をふくむ．



- ◆プロトコルが階層化されているときは，両方のプロトコルが要求する条件をみたす必要がある．

[くみあわせ] かなめとなるプロトコル ARP

■ IP とイーサネットをつなぐ必要性
- ◆イーサネットで通信するには MAC アドレスを知る必要がある．
- ◆IP で通信するときは，通信相手については IP アドレスしかわからない．
- ◆IP アドレスから対応する MAC アドレスをもとめるのに ARP (Address Resolution Protocol, アドレス解決プロトコル) をつかう．

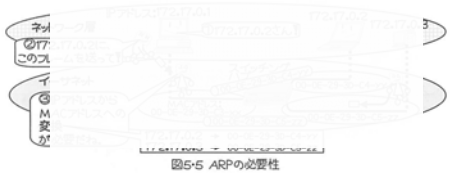


図5-5 ARPの必要性

[くみあわせ] かなめとなるプロトコル ARP (つづき)

■ ARP によって IP アドレスと MAC アドレスとの関係をといあわせる.
- ◆ ARP はイーサネット以外のプロトコル (IP/ATM など) でもつかえる.
- ◆ その IP アドレスをもつコンピュータ (やルータ) が応答する.
- ◆ 相手がどこにいるかわからないので, といあわせはブロードキャストする.

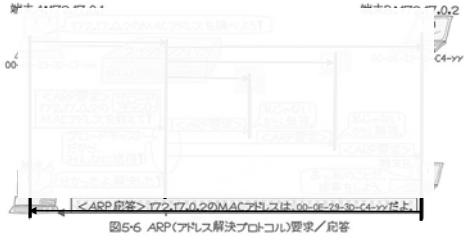


図5-6 ARP(アドレス解決プロトコル)要求／応答

[くみあわせ] ARP とブロードキャスト・ストーム

■ ブロードキャストされる ARP がとどく範囲がひろいと, ネットワークは ARP パケットであふれる.
- ◆ これが, イーサネットが大規模につかえない理由のひとつ (多数のコンピュータからなるネットワークにつかえない).


図5-11 世界中の端末をスイッチングハブで接続したら...

[くみあわせ] ブロードキャスト・ドメインの分割

■ ブロードキャスト・ストームをふせぐため, ブロードキャスト・ドメインを分割する.

■ IP ネットワークによって (IP ルータによって) ブロードキャスト・ドメインをつなぐ.


図5-12 ブロードキャストドメインとルータ(構成例6)

パソコンの MAC アドレスと IP アドレス

■ Ethernet のネットワーク設定をみるには IP と同様に ipconfig / ifconfig コマンドをつかう.

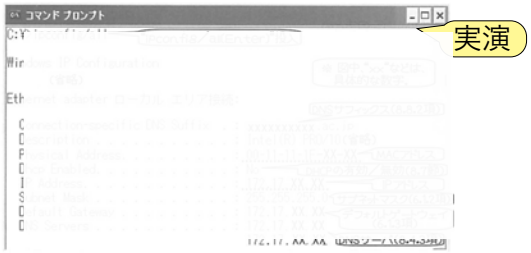


図5-21 IPconfig&コマンド投入結果

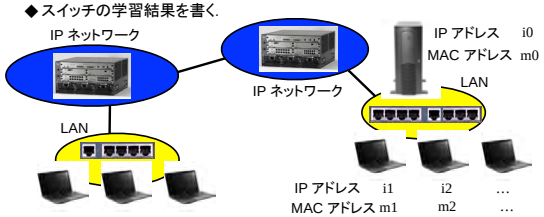
パソコンの MAC アドレスと IP アドレス (つづき)

■ Macintosh の場合

```
MacBook-Kana:~ yk$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        ether 58:55:ca:fb:2d:b7
        inet6 fe80::5a55:caff:fefb:2db7%en0 prefixlen 64 scopeid 0x4
        inet 192.168.1.37 netmask 0xffffff00 broadcast 192.168.1.255
        inet6 2408:41:44cd::5a55:caff:fefb:2db7 prefixlen 64 autoconf
        inet6 2408:41:44cd::78d4:bfb2:daad:d3b7 prefixlen 64 autoconf temporary
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 0a:55:ca:fb:2d:b7
        media: autoselect
        status: inactive
MacBook-Kana:~ yk$
```


演習問題: IP/Ethernet ネットワークの設計と動作

■ 例題: 各地に 2 個のルータと 2 個のスイッチを設置して, それらの動作をみる.
- ◆ 接続をきめる.
- ◆ IP アドレスをつける.
- ◆ ルーティング・テーブルの内容をきめる (ダイナミック・ルーティングの動作まではかんがえない -- スタティック・ルーティングとかんがえてよい).
- ◆ スイッチの学習結果を書く.



インターネットとイーサネットのまとめ

■ [比較] IP とイーサネット
- ◆ IP は転送時にアドレスを集約してあつかえるが, イーサネットは個別にあつかう必要がある.
- ◆ そのため, IP はスケールする (大規模ネットワークに適用できる) が, イーサネットはスケールしない.
- ◆ IP ネットワークにはループが許容されるが, イーサネットにはループが許容されない.

■ [くみあわせ] LAN ではイーサネットと IP をかさねてつかう (IP/Ethernet)
- ◆ プロトコルが層をなしているときは, 内側のプロトコル (IP) をみたすように外側のプロトコル (イーサネット) で通信する.
- ◆ イーサネットにも IP にもアドレスがあるので, それらを対応づけるのが重要 -- ARP というプロトコルをつかって対応づける.

6. プロトコルやネットワークの階層構造

要点

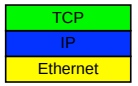
■ 現実のネットワークは複雑であり, 工学的にも現象的にも階層構造をつくっている.

■ [工学的に] プロトコルを階層化することによって, 低機能のプロトコルを利用して高機能のプロトコルがつくれる.
- ◆ たとえば, IP を利用して TCP, UDP などのプロトコルがつくれる.
- ◆ OSI 基本参照モデルでは 7 層のプロトコルが規定されている.

■ [現象的に] ネットワークの構造も階層的だが, どの階層もおなじようにみえる.
- ◆ おおくのネットワークはスケールフリー

プロトコル・スタック

■ プロトコルを階層化することによって, 低機能のプロトコルを利用して高機能のプロトコルがつくれる.
- ◆ たとえば, IP を利用して TCP, UDP などのプロトコルがつくれる.
- ◆ イーサネットと IP も階層化されている.



■ このように階層的につみかさねたプロトコル群を「プロトコル・スタック」という.

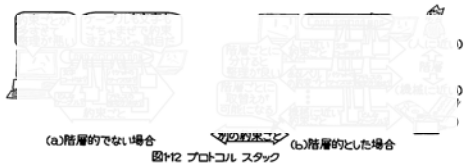


図1-2 プロトコル スタック

OSI

■ OSI とは 1978 ～ 1985 年に ISO で標準化されたネットワーク・アーキテクチャ
- ◆OSI = 開放型システム間相互接続 (Open System Interconnection)
- ◆ISO = 国際標準化機構

■ OSI では OSI 参照モデルというプロトコルのモデルをさだめ，それにもとづく具体的なプロトコルをさだめた．
- ◆OSI 参照モデル = OSI (Basic) Reference Model

OSI 参照モデル

■ OSI において標準化された 7 層からなるプロトコルのモデルを OSI (基本) 参照モデルという．
- ◆TCP/IP のほうが普及したため，OSI 標準プロトコルはほとんどつかわれていない．
- ◆プロトコル階層化のモデルとしては現在でも参照される (ネットワークの教科書などには，かならず登場する)．

図1-3 OSI基本参照モデル

OSI 参照モデル (つづき)

■ 各層の機能の概要はつぎのとおり．

OSI 参照モデル (つづき)

■ インターネットと携帯電話における各層の機能

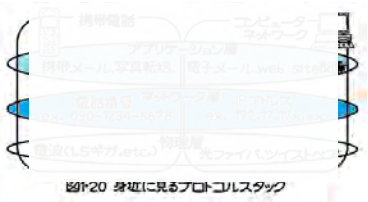
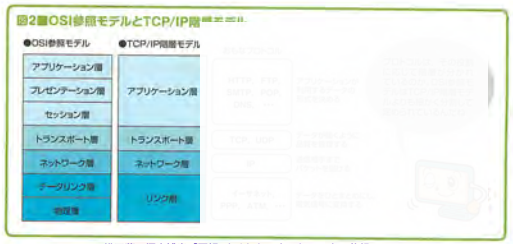


図1-20 身近に見るプロトコルスタック

TCP/IP と OSI 参照モデル

■ TCP/IP の各層は OSI 参照モデルと正確に対応してはいない．
- ◆物理層からトランスポート層まではほぼ対応している．
- ◆OSI のセッション層からアプリケーション層までは「アプリケーション層」にまとめられている．

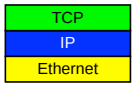


織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

プロトコル・スタックとパケット・ヘッダとの関係

■ パケットにおいては，プロトコル・スタックにおける順番にヘッダがならぶ．

プロトコル・スタック

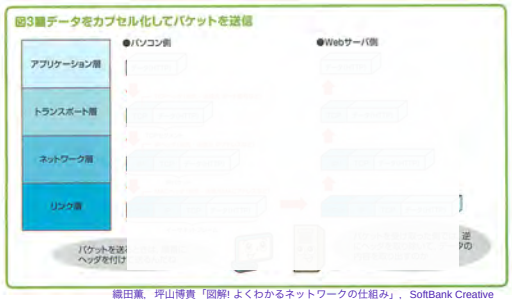


パケット・フォーマット

プロトコルの階層とパケットの構造，受信・送信

■ 送信時には上位層から階層にいくにつれてヘッダをつけていく．

■ 受信時には下位層から上位層にいくにつれてヘッダをとっていく．

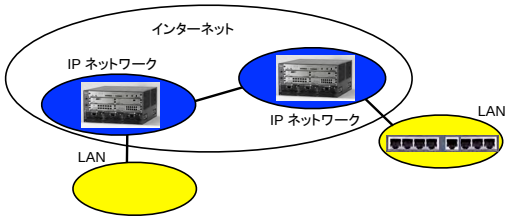


織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

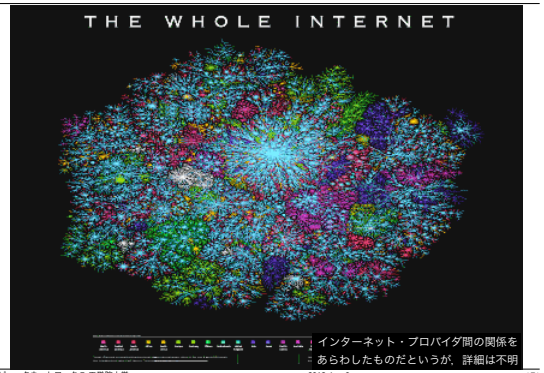
ネットワークの構造

■ 通常は LAN が末端にあり，IP ネットワークがそれをつないでいる．

■ パブリックな IP ネットワークをつないだものがインターネット．



インターネット全体の構造



インターネット・プロバイダ間の関係をあらわしたものだというが，詳細は不明

インターネット全体の構造 (つづき)

2 つの階層構造のちがい

- プロトコルの階層構造は人間が意図的につくったものだが，ネットワークの構造はより自然発生にちかいものである．
- ネットワークの階層構造には自然の階層構造 (複雑ネットワークの構造) にちかいところがある．

インターネットの構造もスケールフリー

- つまり，全体をみても一部だけみても，似た構造をしている
  - インターネットはべき乗則に支配されている．⇒

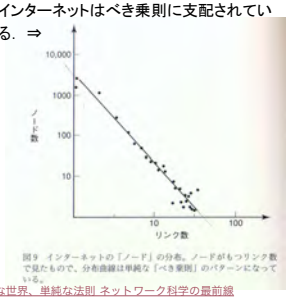
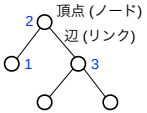


図9 インターネットの「ノード」の分布．ノードがもつリンク数で見たもので，分布曲線は単純な「べき乗則」のパターンになっている．



複雑な世界，単純な法則 ネットワーク科学の最前線
マーク・ブキャナン 阪本 芳久 (単行本 – 2005/2/25)
p.129,Fig.9,インターネットのノード分布,Node distribution of the Internet

プロトコルやネットワークの階層構造のまとめ

- 現実のネットワークは複雑であり，工学的にも現象的にも階層構造をつくっている．
- [工学的に] プロトコルを階層化することによって，低機能のプロトコルを利用して高機能のプロトコルがつくれる．
  - たとえば，IP を利用して TCP, UDP などのプロトコルがつくれる．
  - OSI 基本参照モデルでは 7 層のプロトコルが規定されている．
- [現象的に] ネットワークの構造も階層的だが，どの階層もおなじようにみえる．
  - おおくのネットワークはスケールフリー

7. プライベート・ネットワークとネットワーク仮想化

要点

- インターネットからきりはなされたプライベート・ネットワークではセキュリティが確保しやすく，従来のプロトコルにしばられない．
  - プライベート・ネットワークには物理的なものと仮想化されたもの (VPN) とがある．
- 仮想化されたネットワークとして VLAN があり，企業などでつかわれている．
- 仮想化にはつぎのような種類がある．
  - 質の仮想化と量の仮想化，分割型仮想化と融合型仮想化．
  - コンピュータの仮想化とネットワークの仮想化．
- ネットワーク仮想化の研究によって，プログラマブルで自由なプロトコルがつかえる仮想ネットワークが開発されつつある．
  - 仮想ネットワークにおいては，プライベート・ネットワークの利点をいかして IP やイーサネットとはことなる新プロトコルの実験が自由にできる．
  - 世界各地で新世代ネットワークの研究開発，とくにネットワーク仮想化の研究や実験がおこなわれている．(アメリカで GENI というプロジェクト，日本で AKARI や仮想化ノード (VNode) 開発・利用プロジェクトなど)．

プライベート・ネットワークとパブリック・ネットワーク

- インターネットはだれもが接続できるパブリックなネットワーク．
- 秘密情報などをあつかうため，特定の企業などだけが接続できるようにしたプライベート・ネットワークもある．
- パブリック・ネットワークからプライベート・ネットワークにアクセスできるようにするため，ゲートウェイが設置される．
  - プライベート・ネットワークは接続可能な場所が限定されるため，それをひろげるためにゲートウェイがつかわれる．
  - 不正使用をなくすため，ゲートウェイでは厳重な認証・制限が適用される．

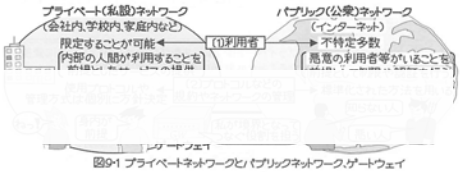


図9-1 プライベートネットワークとパブリックネットワーク,ゲートウェイ

プライベート・ネットワークの利点

- 第 1 の利点はセキュリティ (秘密情報保護)．
  - パブリック・ネットワークでは秘密が漏洩しやすい．
- パブリック・ネットワークの制約にしばられないことも利点．
  - パブリック・ネットワークは多数のユーザに共用されるので，性能 (通信速度，QoS (サービス品質) など) も保証しにくい．
  - パブリック・ネットワークでつかわれるプロトコルにしばられない (たとえば，IP や TCP と共存できないプロトコルもつかえる)．

IP によるプライベート・ネットワーク

- プライベート・ネットワークでは IP 以外のプロトコルもつかえるが，現在はほとんどのネットワークで IP がつかわれている．
  - 現在つかえるアプリケーションはほとんどすべて IP を使用するため．
  - プライベート・ネットワークからパブリック・ネットワークにつなぐには IP が必要なため．

IP によるプライベート・ネットワークのアドレス

- プライベート・ネットワークからインターネット (パブリック・ネットワーク) につなぐなら，インターネットと重複するアドレスはつかえない．
- IETF できめたプライベート IP アドレス (下表の範囲) をつかう．

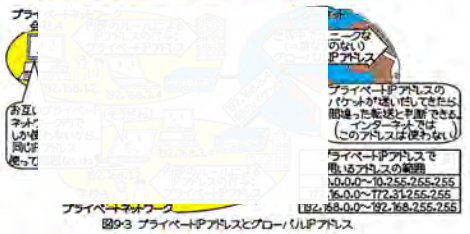


図9-3 プライベートIPアドレスとグローバルIPアドレス

ゲートウェイのやくわり

■ ゲートウェイはプライベート・ネットワーク内部のアドレスをかくす.
- ◆ 同一のプライベート IP アドレスがほかでもつかわれているので, 外部にみせてはいけない (アドレスの唯一性を保証するため).
- ◆ プライベート IP アドレスが外部からわかると不正にアクセスされる可能性があるので, わからないようにする (セキュリティのため).

■ ゲートウェイは内部への不正アクセスをふせぐ.
- ◆ ファイアウォール: 不正アクセス防止機能をもつゲートウェイのこと.
- ◆ 特定のパターンの通信だけをゆるす (たとえば, 通信開始は内側からにかぎるなど).

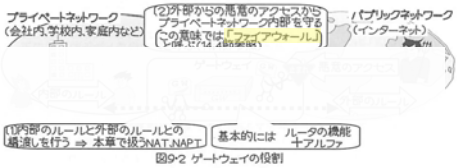


図9-2 ゲートウェイの役割

ゲートウェイとブロードバンドルータ

■ 一般家庭などでつかうためのゲートウェイは ブロードバンド・ルータとよばれている.

織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

アドレス変換と通信

■ パブリック・ネットワークに対して内部のアドレスをかくすための機能がアドレス変換.

■ 変換法には NAT と NAPT とがある.
- ◆ NAT はアドレスを 1 対 1 に変換する.
- ◆ NAPT (IP マスカレード) ならグローバル・アドレスが 1 個ですむため, 通常は NAPT がつかわれる.

世界中からアクセスできる (みえる) アドレス

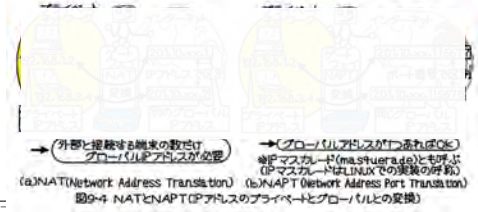
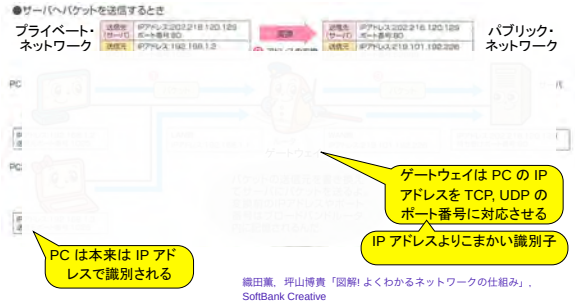


図9-4 NATとNAPT(IPアドレスのプライベートとグローバルとの変換)

NAPT のしくみ

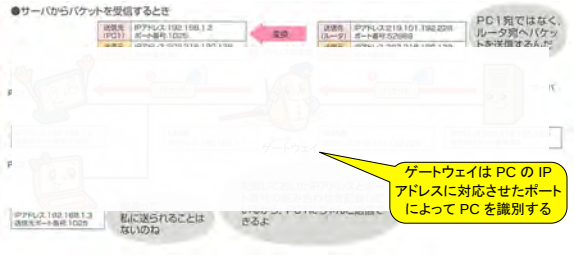
■ プライベート・ネットワークからの送信
- ◆ 外部のサーバをアクセスするとき.



織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

NAPT のしくみ (つづき)

■ プライベート・ネットワークでの受信
- ◆ 基本的に, 送信したパケットに対する応答だけをうけとる.
- ◆ パケットを送信していない PC は外部からのパケットをうけとらない.

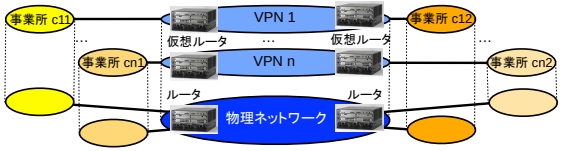


織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

プライベート・ネットワーク -- 物理的なものと仮想的なもの

■ 広域に物理的なプライベート・ネットワークをつくるのは高コスト
- ◆ ルータやスイッチを各地に設置して, その間をケーブルで接続する必要がある. 設置場所も用意する必要がある. (それぞれ設置コストがかかる)
- ◆ ルータ / スイッチ, ケーブル, 設置場所などの管理コストがかかる.

■ インターネットや共用 IP ネットワーク (電話会社などのもの) 城に仮想的なプライベート・ネットワークをつくれば低コスト
- ◆ このようなネットワークを VPN (virtual private network) という.
- ◆ 物理ネットワークの設置コストや管理コストはわけて負担すればよい.



仮想プライベート・ネットワーク (VPN)

■ 複数の拠点をもつ企業のニーズ
- ◆ 拠点間をむすぶプライベート・ネットワーク (専用線によるネットワーク) は高価なので, さけたい.
- ◆ 拠点間はプライベート・ネットワークと同様に自由な通信が可能にしたいが, 同時にセキュアに通信したい.

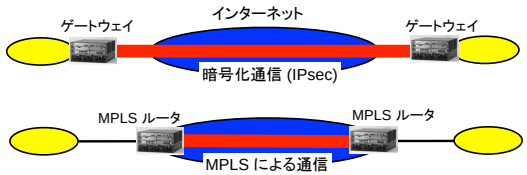
■ このようなニーズをみたす方法が VPN である.

■ VPN における物理と論理
- ◆ VPN は複数拠点間を物理的には共用ネットワークでむすぶ.
- ◆ VPN は他のネットワークとは論理的に独立な (たがいに干渉しない) ネットワークを実現する.

図9-28 VPN(Virtual Private Network)

IP 用 VPN の種類

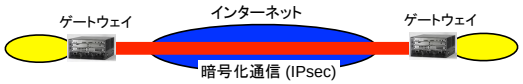
■ (IP をつかうための) 代表的な VPN には 2 種類ある.
- ◆ インターネット VPN (IPsec VPN)
- ◆ IP VPN (MPLS VPN)



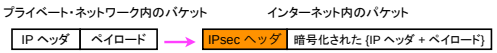
- ◆ 以下これらの VPN について説明する.

IP 用 VPN の種類 (つづき)

■ Internet VPN (IPsec VPN)
- ◆ インターネット上で暗号化通信をする
  ― 暗号化によってセキュリティを確保.



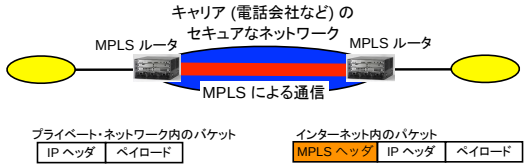
- ◆ IPsec というプロトコルでカプセル化する.



- ◆ 高性能な暗号化はコストがたかいことが欠点.

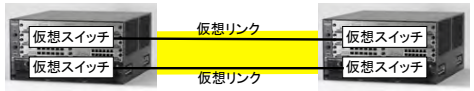
IP 用 VPN の種類（つづき）

- IP VPN (MPLS VPN)
  - MPLS (Multi-Protocol Label Switching) というプロトコルを使用する.
  - インターネットではなく，あらかじめセキュリティが確保されたネットワークを使用する.
  - 暗号化はしない -- 暗号化は高コストなので，さける．暗号化しなくてもインターネットのような危険はない.



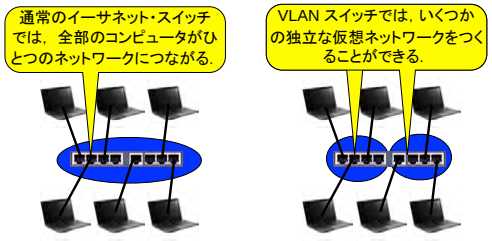
イーサネットの仮想化のためのしくみ: VLAN

- イーサネット上に仮想ネットワークをつくるためのしくみ VLAN が IEEE で標準化されている (IEEE802.1Q).
- VLAN のポイントはスイッチの仮想化とリンクの仮想化



VLAN におけるスイッチの仮想化

- VLAN をつかうと，1 個のスイッチを複数の独立なスイッチのようにつかうことができる.



VLAN におけるリンクの仮想化

- VLAN では 1 本の物理リンクを仮想的に複数のネットワーク (イーサネット) で使用できる.
  - このようなリンクをトランクリンクという.
  - トランクリンクでは VLAN タグによって仮想ネットワークをくべつする.

図9-23 トランクリンクの必要性

VLAN タグとパケット・フォーマット

- VLAN タグは MAC ヘッダのなかにうめこまれる.
  - VLAN パケットのフォーマットは IEEE802.1Q によって標準化されている.

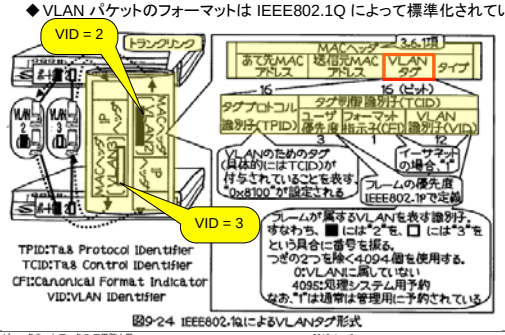


図9-24 IEEE802.1qによるVLANタグ形式

VLAN の利点 -- 企業などの組織の場合

- VLAN は物理的にちらばった組織を容易に論理的にまとめることができる.
  - VLAN をつかわないと組織がかわるたびに物理配線を変更しなければならない.
  - VLAN をつかえば物理配線はかえずに仮想リンクをかえることができる.

図9-21 VLANの構成例

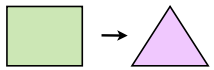
仮想化とは?

- 仮想化とは，物理的なコンピュータやネットワークがもつ機能とは質や量においてことなる機能を実現することである.
- 仮想化の分類
  - ◆質の仮想化
  - ◆量の仮想化
    - ●分割型の仮想化
    - ●融合型の仮想化

量の仮想化と質の仮想化

- 量の仮想化
  - ◆仮想化によって数量をふやす，またはへらす.

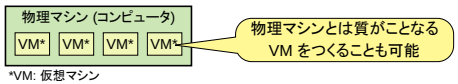
  - ◆仮想化前と質はかわらない (かもしれない).
- 質の仮想化
  - ◆仮想化によって質をかえる.



  - ◆仮想化前と数量はかわらない (かもしれない).

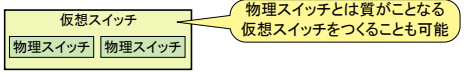
分割型仮想化と融合型仮想化

- 分割型仮想化
  - ◆1 個のコンピュータやネットワークのなかに複数の仮想的なコンピュータやネットワークをつくる.
  - ◆例:



*VM: 仮想マシン

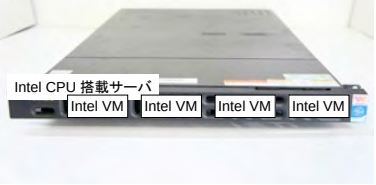
- 融合型仮想化
  - ◆複数のコンピュータやネットワークを仮想的に 1 個のコンピュータやネットワークにみせる.
  - ◆例:



- 現在，実用化・実験されている仮想化技術のおおくは分割型仮想化を実現している.

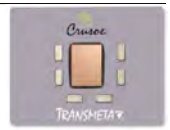
コンピュータ (サーバ) の仮想化

- 融合型の仮想化はほとんどない (?)
- 量の仮想化 (分割型)
  - 最近話題になるサーバ仮想化は量の仮想化: 物理コンピュータとおなじアーキテクチャの仮想コンピュータが複数個つくれる.
  - たとえば Intel CPU 搭載の物理コンピュータから, 複数の Intel 仮想マシンがつくれる.



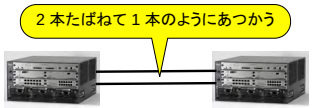
コンピュータ (サーバ) の仮想化 (つづき)

- 質の仮想化 (分割型)
  - 物理コンピュータとはことなるアーキテクチャのコンピュータをつくる.
- 質の仮想化の例
  - トランスメタ社の Crusoe, Efficeon: Intel x86 の命令を独自の命令 (VLIW) に翻訳して実行する CPU (2002-2004 年ごろ).
  - Intel Pentium Pro (とそれ以降の CPU): 複雑な x86 命令を単純な RISC 風命令にハードウェアで翻訳して実行する.
  - P コード・マシン: コンパイラの仕事が容易になるような仮想マシンを定義して, シミュレータで実行する. N. ヴィルトの Pascal P が有名.
  - バイトコード・マシン: Smalltalk, Java などの言語はバイトコードとよばれる仮想的な機械語を実行する仮想マシン (シミュレータ) で実行される.



ネットワークの仮想化

- 分割型仮想化の例
  - VLAN
  - VPN
- 融合型仮想化の例
  - リンク・アグリゲーション: 複数の物理リンクをたばねて, 1 個のリンクにみせる.

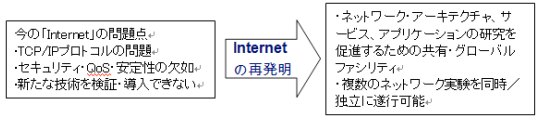


プライベート・ネットワークとネットワーク仮想化

- プライベート・ネットワークの利点のひとつは, パブリック・ネットワークではつかえないプロトコルが自由につかえること.
- ところが, 従来の VPN では基本的に IP しかつかえない.
- 「ネットワーク仮想化」の研究とは?
  - 従来の VPN と同様のプライベートなネットワークをつくり, そのうえでさらに自由に新プロトコルが開発・使用できるようにする.
  - 新プロトコルがつかえるためにはネットワーク・ノード (スイッチ, ルータ) がプログラマブルであることが重要
    - 仮想ネットワークの所有者がネットワーク・ノードを自由にプログラムできる (C などでプログラム開発できる) ようにする.

新世代ネットワーク研究とネットワーク仮想化

- インターネットの限界
  - インターネットが登場してから 30 年以上経過し, 現在のニーズにはかならずしもあっていないところがある.
  - 既存のインターネットに対してセキュリティ, QoS (Quality of Service), 安定性などの面で限界があることが指摘されている.
- クリーンスレート構想
  - 米国では 2000 年ごろから既存のインターネットを根本から見直して将来のネットワークを構築する「クリーン・スレート・インターネット構想」が議論されるようになった.



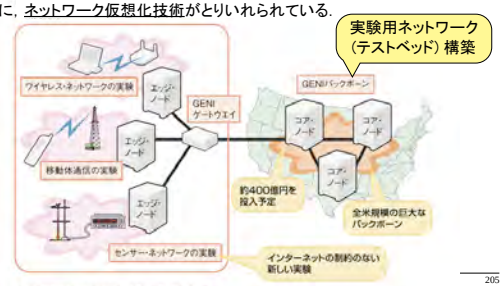
アメリカにおける新世代ネットワークとネットワーク仮想化

- インターネットはネットワークの進化をとめている ?!
  - アメリカなどでは, インターネットとはまったくちがう, あたらしいネットワークをつくる必要があることが合意された.
- FIND (Future Internet Design)
  - アメリカの科学財団 (NSF) ではあたらしいネットワークをつくるため, FIND という研究ファンド・プログラムを設置した.

EU (ヨーロッパ) では FP7 (7th Framework Programme) というプロジェクトをやっている

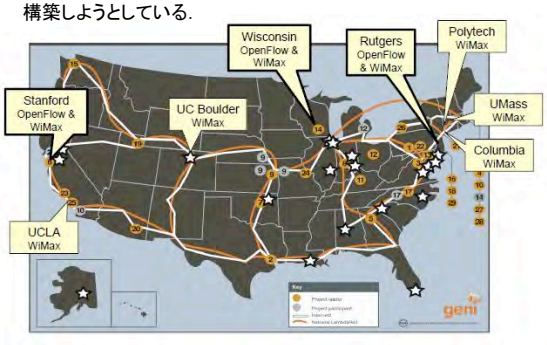
アメリカにおける新世代ネットワークとネットワーク仮想化 (つづき)

- GENI (Global Environment for Network Innovations)
  - 現在のインターネットにはとりいれるのがむずかしい IP に依存しない新技術を開発するために GENI というプロジェクトが開始された.
  - GENI では, かぎられた物理ネットワーク上でさまざまな実験ができるように, ネットワーク仮想化技術がとりいれられている.



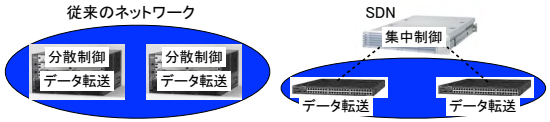
アメリカにおける新世代ネットワークとネットワーク仮想化 (つづき)

- GENI では全米規模のバックボーン (骨格となるネットワーク) を構築しようとしている.



ソフトウェア定義ネットワーク

- ソフトウェア定義ネットワーク (Software Defined Network: SDN)
  - これまでは機種依存だったスイッチやルータの制御を外部のコントローラ上のソフトウェアによって一元的におこなえるようにしたネットワーク.
  - OpenFlow が代表的な制御方式.
- SDN の基本思想: コントローラ – データ分離
  - コントローラがスイッチに規則を配布し, 各スイッチはそれにもとづいて動作する.



ソフトウェア定義ネットワーク (つづき)

■ ソフトウェア定義ネットワークの利点
- ◆スイッチング，ルーティングの方法・方針 (ポリシー) などをかんたんにためすことができる.
- ◆スイッチやルータの従来は外部から制御できなかった部分が，制御できるようになる.
- ◆従来は機種依存の方法でしか制御できなかったスイッチやルータの機能が統一的な方法で制御できるようになる.

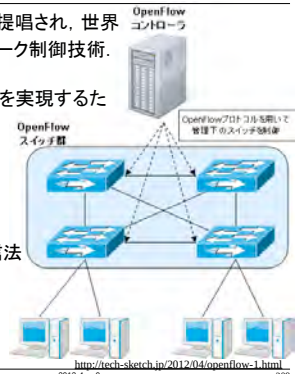
OpenFlow 概論

■ 2008 年に Stanford 大学で提唱され，世界中で注目されているネットワーク制御技術.
- ◆イーサネット上でつかわれる.

■ ソフトウェア定義ネットワークを実現するための最有力な方法.

■ OpenFlow ネットワークのハードウェア構成
- ◆OpenFlow スイッチ
- ◆OpenFlow コントローラ

■ スイッチとコントローラの通信法
- ◆OpenFlow プロトコルによる.



http://tech-sketch.jp/2012/04/openflow-1.html

OpenFlow 概論 (つづき)

■ 通常のスイッチやルータで構成された既存のネットワーク上にOpenFlow スイッチをおいて使用することができる.
- ◆つまり，従来技術と共存できる.

■ ベンダのなかでは NEC がもっとも積極的にとりくんでいる.
- ◆NEC の製品 →

OpenFlow のしくみ

■ OpenFlow による制御は条件と動作との組 (規則) により指定される.

■ 条件は処理の対象であるパケットを特定する.
- ◆MAC アドレス，IP アドレス，TCP/UDP ポート番号など，物理層 (L1) からトランスポート層 (L4) まで，どの階層のデータもあつかえる.
- ◆例: TCP ポート番号が 80 のパケット.

■ 動作は条件に合致したパケットに対し行う動作を規定する.
- ◆他のポートへの転送，ヘッダのかきかえ，パケットの破棄などが指定できる.

■ 規則の例: TCP ポート番号が 80 のパケットは破棄する.

OpenFlow による制御の例

■ OpenFlow で「ルータ」をつくることも可能.

■ IP/Ethernet のルータは「とどいたパケットの IP アドレスの判定結果にもとづいて，そのパケットの MAC アドレスをかきかえて，しかるべきインタフェースに転送する」.
- ◆ 受信者 MAC アドレスをネクストホップの MAC アドレスにかきかえる.
- ◆ 送信者 MAC アドレスをそのルータの MAC アドレスにかきかえる.
- ◆ ネクストホップにつながるネットワーク・インタフェースから出力する.

■ これをサブネットごとに規則として記述して設定すれば，OpenFlow スイッチはルータとして機能する.
- ◆つまり，ルーティング・テーブルのかわりに規則のならびを使用する.

ルーティング・テーブルの例

あてさき	ネクストホップ
172.17.4.0/24	**192.168.2.251**
192.168.1.0/24	＊(直接)
192.168.2.0/24	＊(直接)

等価な OpenFlow の規則
if 受信者 IP アドレスの先頭 24 ビットが 172.17.4 **then**
受信者 MAC アドレス =
192.168.2.251 に対応する MAC アドレス
送信者 MAC アドレス = 自 MAC アドレス
受信者 MAC アドレスにつながるインタフェースに出力

OpenFlow による制御の例 (つづき)

■ OpenFlow による制御の長所と短所
- ◆長所: IP やイーサネットの制御は一層 (IP, イーサネット) でとじていたが，OpenFlow では層にまたがる制御ができる.

IP アドレスだけをみている / IP アドレスと MAC アドレスをあわせて読み書きしている

ルーティング・テーブルの例

あてさき	ネクストホップ
172.17.4.0/24	**192.168.2.251**
192.168.1.0/24	＊(直接)
192.168.2.0/24	＊(直接)

等価な OpenFlow の規則
if 受信者 IP アドレスの先頭 24 ビットが 172.17.4 **then**
受信者 MAC アドレス =
192.168.2.251 に対応する MAC アドレス
送信者 MAC アドレス = 自 MAC アドレス
受信者 MAC アドレスにつながるインタフェースに出力

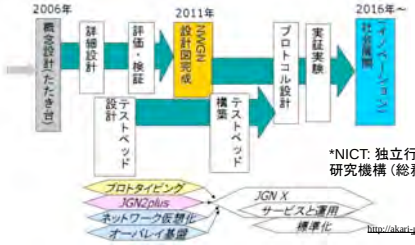
- ◆短所: IP/Ethernet だけでしかつかえない.
  - ●IP, Ethernet 以外のプロトコルではつかえない.
  - ●IP とイーサネット以外のリンク層，イーサネットと IP 以外のネットワーク層のくみあわせでもつかえない.
- ◆長所/短所: ネットワークが集中制御される (コントローラで).

AKARI ―― 日本における新世代ネットワーク研究

■ 2015 年に新世代ネットワークの基礎技術を実現することをめざして，NICT* 中心に 2006 年からつづけられてきたプロジェクト.

■ まったくあたらしいネットワークアーキテクチャを確立し，それにもとづいたネットワーク設計図を作成することを目的としている.

■ クリーンスレートをめざしている ―― インターネットにとらわれない.

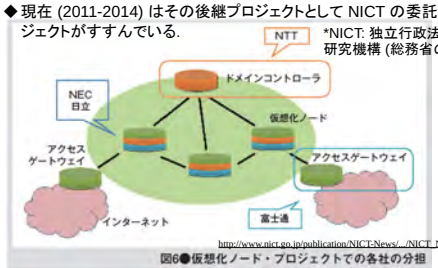


*NICT: 独立行政法人 情報通信研究機構 (総務省の外郭組織)

http://akari-project.nict.go.jp/index2.htm

VNode -- 日本におけるネットワーク仮想化研究

■ 日本の代表的なネットワーク仮想化研究プロジェクトとして「仮想化ノード (VNode) プロジェクト」(とその後継プロジェクト) がある.
- ◆VNode プロジェクト (2009-2010) では，NICT という場で東大，NTT，富士通研究所，NEC，日立が共同研究してきた.
- ◆現在 (2011-2014) はその後継プロジェクトとして NICT の委託研究プロジェクトがすすんでいる.



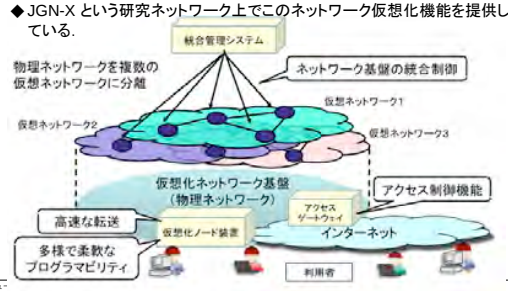
*NICT: 独立行政法人 情報通信研究機構 (総務省の外郭組織)

http://www.nict.go.jp/publication/NICT-News/.../NICT_NEWS_1006_1.pdf

図6●仮想化ノード・プロジェクトでの各社の分担

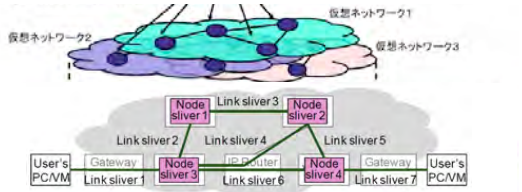
VNode -- 日本におけるネットワーク仮想化研究 (つづき)

■ VNode プロジェクトの成果
- ◆仮想化ノード (VNode) という装置によって構成される物理ネットワーク (ネットワーク仮想化基盤という) 上に仮想ネットワーク (スライスという) が生成できるようにした.
- ◆JGN-X という研究ネットワーク上でこのネットワーク仮想化機能を提供している.



VNode における仮想ネットワークのモデル

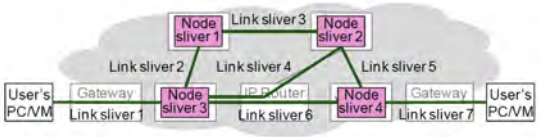
■ スライス (仮想ネットワーク)
- ◆自由な構造のスライスをつくることができる: 任意の個数の仮想ネットワーク・ノードをつくり, 物理的なリンクに制約されない仮想リンクでむすぶことができる.
- ◆「スライス」とよばれる理由: 物理的なネットワークを仮想的に分割して (スライスして) 仮想ネットワークをつくることができるから.



- ◆仮想ノードの機能は自由にプログラムできる (プログラムする必要がある).

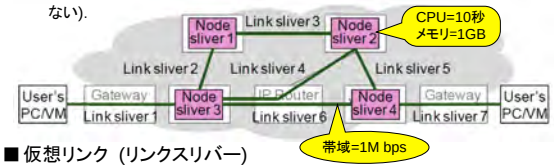
VNode における仮想ネットワークのモデル (つづき)

■ 仮想ノードと仮想リンク
- ◆仮想化されたネットワーク資源はスリバー (sliver) とよばれる.
- ◆VNode プロジェクトではとくに仮想ノードをノードスリバー, 仮想リンクをリンクスリバーと呼んでいる. (が, ここではより一般的な用語である仮想ノードと仮想リンクということばをつかう.)



VNode における仮想ネットワークのモデル (つづき)

■ 仮想ノード (ノードスリバー)
- ◆VNode (プログラマ) 内の計算資源 (CPU 時間, メモリなど) をあらわす.
- ◆おもにプロトコルの処理や制御などにつかう -- その機能は自由にプログラムできる.
- ◆どんなパケット・フォーマットでもあつかえる (IP やイーサネットにしばられない).

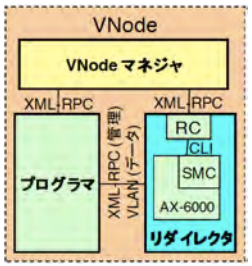


■ 仮想リンク (リンクスリバー)
- ◆ことなる VNode 内の 2 つの仮想ノードをつなぐ仮想リンクのネットワーク資源 (帯域など) をあらわす.
- ◆どんなパケット・フォーマットでもあつかえる.

VNode の構造: プログラマとリダイレクタ

■ プログラマ (Programmer)
- ◆パケットの加工や転送先の決定などの処理をおこなう (計算 / ストレージ・リソースをもつ).
- ◆プログラマブルなので「プログラマ」とよぶ.

■ リダイレクタ (Redirector)
- ◆パケットを他の VNode 等から受信してプログラマにリダイレクトし, プログラマからのパケットを他の VNode などに送信する (ネットワーク・リソースをもつ).



VNode への仮想ネットワーク定義

■ 管理サーバ (ドメイン・コントローラ) に XML で記述した「スライス定義」をあたえると, スライスが生成される.
- ◆ネットワーク配線や機器の設置などの手間をいっさいかけずに, のぞみのネットワークをつくることができる.

■ 現在は人手で XML を記述する必要があるが, GUI などでさらに容易にスライスが記述できるようにすることをめざしている.

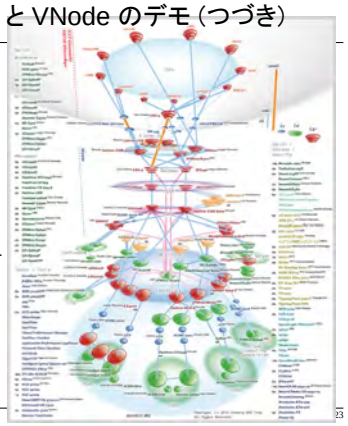
Interop Tokyo と VNode のデモ

■ 毎年 6 月にひらかれるインターネット関連の展示会 Interop Tokyo で展示・デモしている.

Interop 2010 の会場のようす

Interop Tokyo と VNode のデモ (つづき)

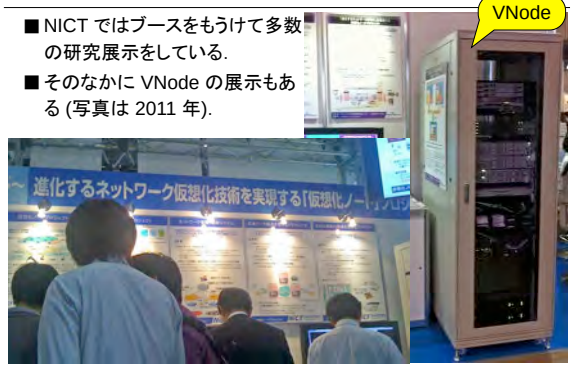
■ Interop Tokyo では毎年, ネットワーク構成にいろいろくふうをこらしている.
- ◆Cisco, Alaxala をはじめ, 多数の会社のネットワーク機器がつかわれ, 展示されている.
- ◆右図は 2010 年の構成.



Interop Tokyo と VNode のデモ (つづき)

■ NICT ではブースをもうけて多数の研究展示をしている.

■ そのなかに VNode の展示もある (写真は 2011 年).



研究用ネットワークへの展開

■ JGN-X という NICT 提供の研究用ネットワーク上に VNode を配置して, ネットワーク研究者などがつかえるようにしている.
- ◆VNode は東京に 2 台, 大阪, 名古屋, 北陸, けいはんな, 岡山などに各 1 台ある.

IP にしばられないプロトコルの研究例 -- IPEC

■ IPEC (IP Ether Chimera) は VNode プロジェクトのなかで金田が開発した実験的なプロトコル.

ギリシャ神話のキマイラ

2 種のネズミのキメラ

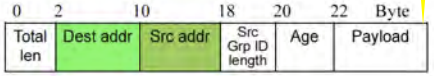
■ IPEC の開発目的は, IP と Ethernet の利点をかねそなえた単純なプロトコルをつくること.
- ◆ Ethernet の利点は単純さ
- ◆ IP の利点はネットワークにループを許容すること
- ◆ IP と Ethernet とをくみあわせる (IP/Ethernet) と, 両者のアドレスを対応づけるために複雑になる (ARP が必要になる).

IP にしばられないプロトコルの研究例 -- IPEC (つづき)

■ IPEC のアドレス・フォーマット

- ◆ ホスト ID: コンピュータごとにことなる識別子.
- ◆ グループ ID: コンピュータのグループごとにことなる識別子.

■ IPEC のパケット・フォーマット



- ◆ 受信者アドレス (dest addr)
- ◆ 送信者アドレス (src addr)
- ◆ Age: 転送されるごとに +1 される (IP の TTL に対応)
  -- これをつかってループをふせぐ.

IP にしばられないプロトコルの研究例 -- IPEC (つづき)

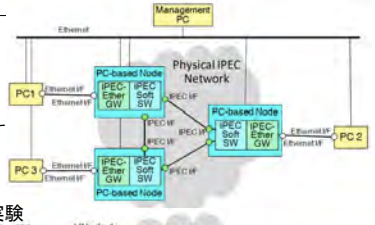
■ IPEC は IP と Ethernet の両方をおきかえる.
- ◆ 基本的にはネットワーク層 (IP のかわり) のプロトコルだが, Ethernet の転送機能もおきかえる.

■ IPEC の学習アルゴリズム
- ◆ 個々のアドレス (ホスト ID) を学習するのでなく, グループ ID を学習することで, 大規模なネットワークに適用できる.
- ◆ パケットの Age フィールドを利用して, おなじパケットが複数個とどいたときは最短経路を選択する.
  - ●それ以降は最短経路だけがつかわれる.
  - ●ネットワークにループがあってもよい.

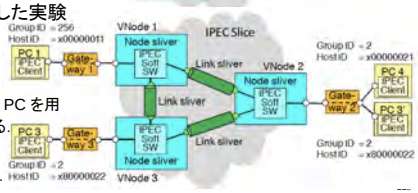
■ IPEC の転送アルゴリズム (基本的にイーサネットとおなじ)
- ◆ 学習していないあいだはブロードキャスト (フラディング) する
  -- パケットをコピーする.
- ◆ 学習したあとはその結果にしたがってスイッチする
  -- パケットをコピーしない).

IP にしばられないプロトコルの研究例 -- IPEC (つづき)

■ PC をつないでの IPEC の実験
- ◆ IPEC スイッチ用に 3 台, 端末用に 3 台の PC を用意して通信する.



■ VNode を使用した実験
- ◆ IPEC スイッチ用に 3 台の VNode, 端末用には 3 台の PC を用意して通信する.



IP にしばられないプロトコルの研究例 -- IPEC (つづき)

■ IPEC のデモ・ビデオ (GENI Engineering Conference むけ)

プライベート・ネットワークとネットワーク仮想化のまとめ

■ インターネットからきりはなされたプライベート・ネットワークではセキュリティが確保しやすく, 従来のプロトコルにしばられない.
- ◆ プライベート・ネットワークには物理的なものと仮想化されたもの (VPN) とがある.

■ 仮想化されたネットワークとして VLAN があり, 企業などでつかわれている.

■ 仮想化にはつぎのような種類がある.
- ◆ 質の仮想化と量の仮想化, 分割型仮想化と融合型仮想化.
- ◆ コンピュータの仮想化とネットワークの仮想化.

■ ネットワーク仮想化の研究によって, プログラマブルで自由なプロトコルがつかえる仮想ネットワークが開発されつつある.
- ◆ 仮想ネットワークにおいては, プライベート・ネットワークの利点をいかして IP やイーサネットとはことなる新プロトコルの実験が自由にできる.
- ◆ 世界各地で新世代ネットワークの研究開発, とくにネットワーク仮想化の研究や実験がおこなわれている. (アメリカで GENI というプロジェクト, 日本で AKARI や仮想化ノード (VNode) 開発・利用プロジェクトなど).

8. ネットワーク・サービスの基礎プロトコル TCP と UDP

要点

■ TCP, UDP では「ポート」によって, 複数の通信が並行してできるようにしている.
- ◆ 1 個の IP アドレス (1 台のコンピュータ) で複数のポートがつくれる.

■ TCP, UDP では「ポート」によって, さまざまなプロトコルをつかいわけることができる.
- ◆ Web のための HTTP, ファイル転送のための FTP, 電子メールのための SMTP などのプロトコルがある.

■ TCP では信頼性・性能のたかい通信を実現している.
- ◆ パケットが脱落しても再送する.
- ◆ 通信路を他の通信とうまくわけあって有効につかうしくみがある.

■ TCP は複数のパケットにまたがるメッセージを伝送できる.
- ◆ パケットの最大長 (MTU) にしばられない.

ポート番号と複数の通信

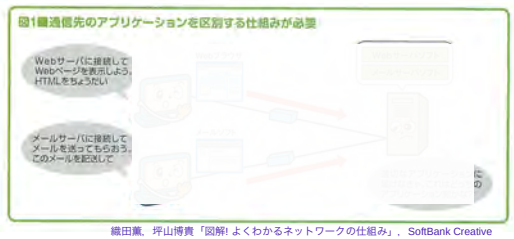
■ IP アドレスだけでは 1 台のコンピュータで複数の通信しようとしても, くべつできない.

■ TCP, UDP では自分と相手のそれぞれの IP アドレスにくわえて, それぞれのポート番号 (1 ～ 65535) が指定できる.

■ ポート番号がちがうと, ことなる通信とみなされる.
- ◆ 1 台のコンピュータで複数の通信ができる.

ポート番号と複数の通信 (つづき)

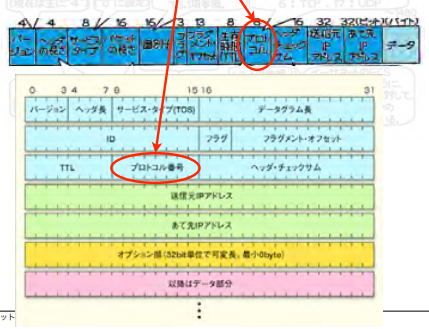
■ ポートごとに通信相手はことなっていてもよいし, 同一でもよい.



織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

IP ヘッダにおけるポート番号の指定

■「IP プロトコル」は IP ヘッダのプロトコル欄で指定される.
- ◆TCP なら 6, UDP なら 17 をここにいれる.



IP プロトコルごとにきめられたポート番号

■ HTTP, FTP などのプロトコルごとに固定のポート番号 (ウェルノウン・ポート) がわりあてられている.
- ◆たとえば HTTP では 80 --- Web をつかうときは基本的に 80 を指定.
- ◆ウェルノウン・ポート (well-known port) は 1023 まで.

表7・1 主なウェルノンポート番号

アプリケーション	ポート番号	サービス内容	アプリケーション	ポート番号	サービス内容
FTP	20,21	ファイル転送(第10章)	DNS	53	ドメインネームの解決(第8章)
SMTP	25	メール転送(第11章)	HTTP	80	Webページ(第12章)
			POP3	110	メール配信(第11章)

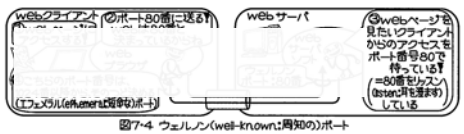


図7・4 ウェルノン(well-known:周知の)ポート

TCP はコネクション型，UDP はコネクションレス型

■ TCP は相手と接続してから通信する (= コネクション型).
- ◆電話をかけてから話をする，または橋をかけてからとおる ようなもの.

■ UDP は接続せずに通信する (= コネクションレス型)
- ◆郵便をおくるようなもの.

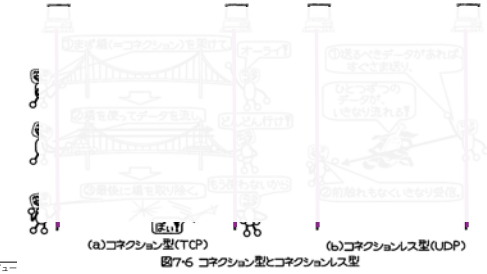


図7・6 コネクション型とコネクションレス型

TCP と UDP のヘッダ・フォーマット

■ TCP

■ UDP

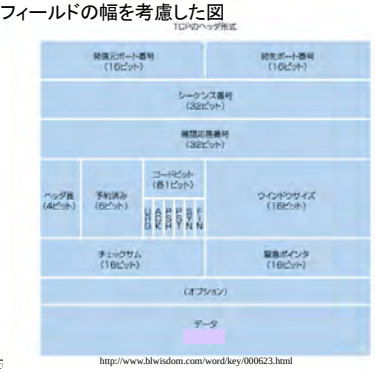
※1:MSS(7.3項)の交渉(7.6.2項,図7・21)で用いられる

図7・7 TCPヘッダ,UDPヘッダ

パケット・フォーマット

TCP と UDP のヘッダ・フォーマット (つづき)

■ TCP の各フィールドの幅を考慮した図



http://www.blwisdom.com/word/key/000623.html

TCP と UDP のヘッダ・フォーマット (つづき)

■ UDP の各フィールドの幅を考慮した図

TCP と UDP のヘッダ・フォーマット (つづき)

■ IETF の標準ドキュメントとパケット・フォーマットの表記
- ◆TCP は RFC 793, UDP は RFC 768 という IETF の標準ドキュメントで規定されている.
- ◆RFC では伝統的に図も文字でかく.

ネットワーク上での TCP と UDP の比率

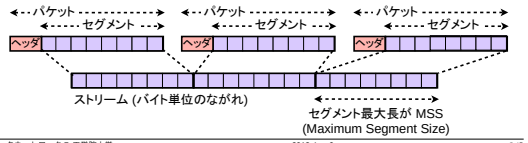
■ 日本では最近 UDP の使用が急速にふえている (らしい)
- ◆IIJ の総トラフィックにしめる UDP の割合は
  2009 年　2.2%
  2010 年　6.8%
  2011 年　10.0%
  (IIJ Internet Infrastructure Review vo. 8, vol. 12).
  のこりはほとんど TCP.
- ◆以前はほとんどが TCP だったことがわかる.

TCP の特徴

■ 全二重のコネクション型 (connection-oriented) の通信
- ◆電話のように接続してから通信する.
- ◆電話のように双方向同時に通信できる (全二重通信する).
  - ●双方向でも同時にできないトランシーバのような方式を半二重という.
    (たとえば，イーサネットでは全二重，半二重のどちらも選択できる.)

全二重と半二重

■ ストリーム型の通信 (stream-oriented)
- ◆バイト単位のストリング (文字列) を通信する.
- ◆セグメント (パケット) はデータ内容においては意味をもたない.



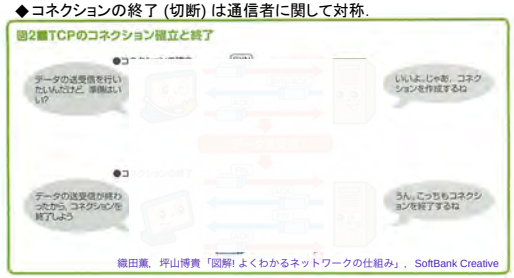
TCP のコネクション確立と終了

■ コネクションの確立には 3 つのメッセージを使用する (3 ウェイ・ハンドシェイク)

■ 通信の対称性

◆ コネクションの確立は通信者に関して非対称.

◆ コネクションの終了 (切断) は通信者に関して対称.



織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

TCP のコネクション確立と終了 (つづき)

■ 3 ウェイ・ハンドシェイクが必要な理由

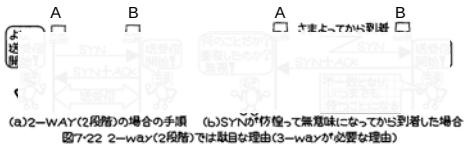
◆ 2 ウェイでは, メッセージがうまくとどかなかったときに, SYN の送信者 (A) が, 受信者 (B) がコネクションを OK したのかどうかを確認できない.

◆ メッセージがうまくとどかないケースにはいろいろあるが, どのケースでも 3 ウェイ・ハンドシェイクならうまくいく.

●SYN がとどかない / 到着がおくれる.

●ACK+SYN がとどかない / 到着がおくれる.

●ACK がとどかない / 到着がおくれる.



(a)2-WAY(2段階)の場合の手順　(b)SYNが彷徨って無意味になってから到着した場合

図7-22 2-way(2段階)では駄目な理由(3-wayが必要な理由)

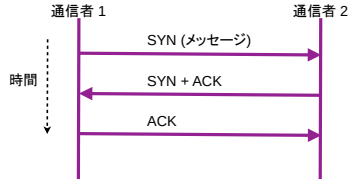
シーケンス図

■ 通信のながれを時系列的に図示する.

■ UML で定義されている.

◆ UML = unified modeling language (統一モデリング言語).
ソフトウェアの仕様を記述するための標準化された言語.
OMG によって標準化されている.

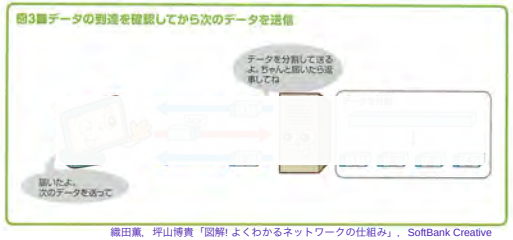
◆ このスライドのシーケンス図はかならずしも標準に準拠していない.



TCP によるデータ送受信の手順

■ データがとどいたかどうかを送達確認 (ACK) する.

■ 単純な方法は ACK がとどいてからつぎのデータをおくる方法だが, これでは性能がでない.



織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

TCP 高信頼化のためのしくみ: 送達確認

■ TCP ではデータが紛失しても再送される.

◆ パケットにシーケンス番号をつけておき, とどかなかったパケットを識別 (送達確認) して TCP が再送する.

◆ UDP では再送のしくみがないので, 必要ならアプリケーションが紛失を検出して再送する必要がある.

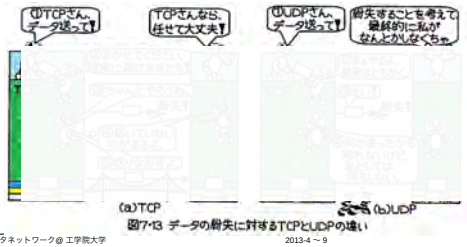


図7-13 データの紛失に対するTCPとUDPの違い

TCP 高信頼化のためのしくみ: 送達確認 (つづき)

■ 送達確認のため, TCP ヘッダ内のつぎのフィールドがつかわれる.

◆ シーケンス番号

◆ 確認応答番号

◆ ACK フラグ

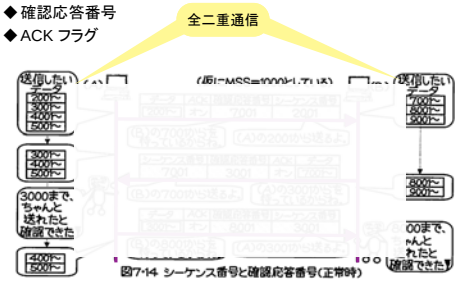


図7-14 シーケンス番号と確認応答番号(正常時)

TCP 高信頼化のためのしくみ: パケットの再送

■ 送信側でタイマーによる再送制御をおこなう.

◆ とどくはずのパケットがとどかないとき (ACK がとどかないとき) は, 再送する.

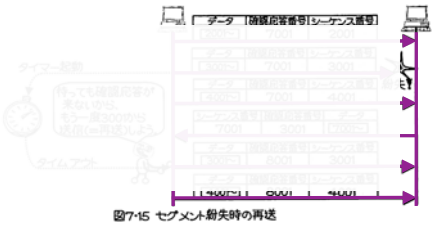


図7-15 セグメント紛失時の再送

TCP 高信頼化のためのしくみ: 転送制御

■ 受信側でシーケンス番号をみて, つぎの処理をする.

◆ パケットのならべかえ: シーケンス番号の順にならべる.

◆ 重複除去: 同一シーケンス番号のパケットが複数個とどいたら, ひとつだけにする.

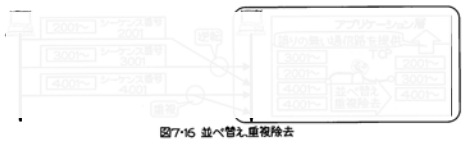
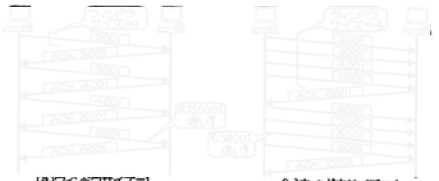


図7-16 並べ替え,重複除去

TCP 高性能化のためのしくみ: ウィンドウ制御

■ 送達確認 (ACK) をパケットごとでなく, まとめておこなうことで高性能化をはかっている.

◆ パケットごとに確認すると, 遠距離通信では通信速度が激減する.

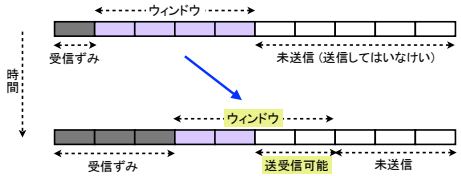


※ ウィンドウサイズ : ここでは「ACKを受け取る前に送信してよいセグメントの数」とする

図7-17 ウィンドウサイズによる転送速度の違い(動作例)

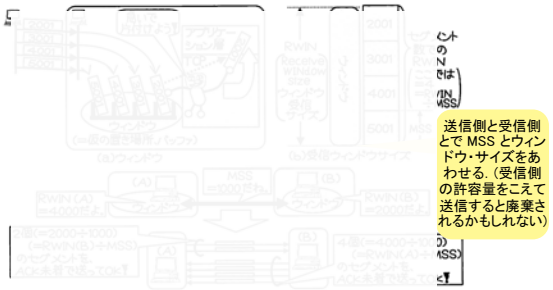
TCP 高性能化のためのしくみ: ウィンドウ制御 (つづき)

■ データ受信が確認されるごとに，送信側でウィンドウをずらす．



TCP 高性能化のためのしくみ: ウィンドウ制御 (つづき)

■ MSS (最大セグメント長) と RWIN (受信ウィンドウ・サイズ) をつかった制御



(c)RWINとMSSとを考慮した送信
図7-18 RWINとMSS

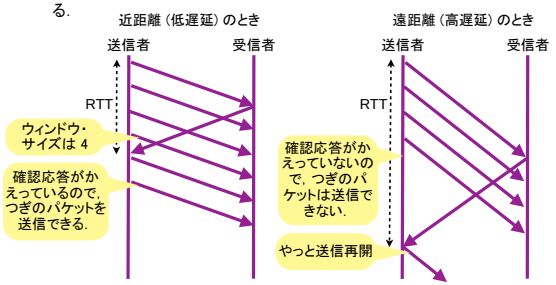
ウィンドウを利用した制御: フロー制御・輻輳制御

■ TCP では送信側で通信状態を把握して，ウィンドウ制御によって通信量を加減する．
- ◆いろいろな制御に利用できる．
- ◆受信側でウィンドウ・サイズを指定することもできる．

(a)ウィンドウサイズによる受信データ量の調整

ウィンドウを利用した制御: フロー制御・輻輳制御 (つづき)

■ TCP のウィンドウ・サイズと通信量との関係
- ◆パケットの往復時間を RTT 秒とする．--- 送受信者間を往復する時間
- ◆ウィンドウ・サイズを w とすると，1 個のパケットの送信に RTT / w 秒かかる．



ウィンドウを利用した制御: フロー制御・輻輳制御 (つづき)

■ フロー制御: TCP では受信側で処理がまにあわなくなりそうなときは，ウィンドウをちぢめる．

■ 輻輳制御: TCP ではネットワークが混んでいること (輻輳) を検知するとウィンドウをちぢめて通信量をへらす．
- ◆どうやって輻輳を知るのか?
  - ●パケットの廃棄を輻輳の兆候とみなす．
- ◆なぜ輻輳するとウィンドウをちぢめるのか?
  - ●ウィンドウをちぢめると輻輳が軽減されるとかんがえられるから．
  - ●他の通信との共存をめざしている．
- ◆輻輳制御がうまく動作するとはかぎらない (遠慮しすぎることがある)．

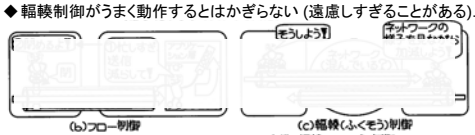


図7-19 ウィンドウサイズによるフロー制御・輻輳(ふくそう)制御

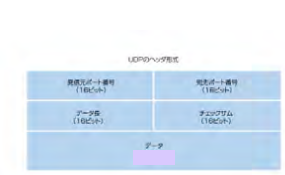
ウィンドウを利用した制御: フロー制御・輻輳制御 (つづき)

■ TCP の輻輳制御がうまくいくときと，うまくいかないとき
- ◆[うまくいく例] 輻輳点における通信がすべて TCP なら，うまくいく．
  - ●輻輳するとみんながウィンドウをちぢめて通信量をへらすから．
- ◆[うまくいかない例] UDP があるとうまくいかない．
  - ●UDP 通信では輻輳を検知しないので，UDP が勝つ (通信帯域を独占するかもしれない)．

■ TCP 親和性 (TCP friendliness)
- ◆TCP 以外のプロトコルでも輻輳時に通信量をへらして TCP と帯域をわけあうこと．

UDP の機能

■ UDP は IP の機能に送受信ポートの指定と誤り検出 (チェックサム) の機能だけをつけくわえる．
- ◆TCP のような高信頼化や高性能化のための機能はない．
- ◆UDP の標準ドキュメント RFC 768 は 3 ページしかない．



http://www.blwisdom.com/word/key/000625.html

UDP の特徴

■ リアルタイムの通信に適している．
- ◆高信頼性より低遅延であることが重要な通信に向いている．

■ TCP ではできない 1 対多 や 多対多 の通信ができる．

織田篤，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

TCP と UDP

■ ファイルを転送するときは，パケットが途中で廃棄されても自動的に回復してくれる TCP のほうが便利である．
- ◆UDP をつかうと，アプリケーションがパケットの再送を制御する必要が生じる．

図7-25 UDPで大きなファイルを転送する

TCP と UDP (つづき)

■ ちいさなメッセージをおくるには UDP のほうが効率がよい.
- ◆TCP では接続の負荷 (時間, 転送量) がおおきい.
- ◆TCP ではヘッダがおおきいため, データが少量だと効率がわるい (転送量).

図7-26 TCPで小さなメッセージを送る

TCP と UDP (つづき)

■ リアルタイムであることが重要なときは, TCP のパケット再送はじゃまになる.
- ◆データがそろうまでアプリケーションにわたされないから.

図7-27 TCPで実況中継のデータ(リアルタイムデータ)を送る

TCP と UDP (つづき)

■ ブロードキャストしたいときは, TCP ではできないので UDP をつかう.
- ◆TCP のコネクションは 1 対 1 にかぎられているので, ブロードキャストはできない.

図7-28 ブロードキャストはUDPのみ

TCP と UDP (つづき)

■ まとめ

表7-1 TCPとUDPの比較

		TCP (Transmission Control Protocol)	UDP (User Data&ram Protocol)
コネクション		コネクション型 (コネクションを確立してから送受信)	コネクションレス型 (いきなり送受信)
あだ名	ほめ言葉	多機能, 正確, 几帳面, まじめ	シンプル, 軽快, 軽いフットワーク
	悪口	大袈裟, 生まじめ, 馬鹿丁寧	機能ない, いい加減, お調子者
ヘッダの大きさ		大きい(20バイト)	小さい(8バイト)
上位とのデータの受け渡し		ストリーム(切れ目の無い流れ)	データの固まり(データグラム)
データの分割		あり(セグメンテーション分割)	なし(必要ならばIPフラグメンテーションに任せる)
信頼性		あり(シーケンス番号による送達確認あり)	なし
効率	大きなファイル	良い(セグメントの紛失を再送で防ぐ)	悪い(データグラムが失われれば失敗)
	小さなメッセージ	悪い(オーバーヘッドが大きい)	良い
リアルタイムデータブロードキャスト		不得意	得意

TCP, UDP 以外のトランスポート・プロトコル

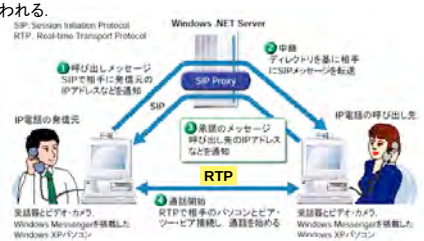
■ TCP, UDP 以外のプロトコルの必要性
- ◆TCP の特徴のうちの一部だけを利用したいことがある
  — たとえば高信頼性はほしいがストリーム型でないほうがよいとき.
- ◆UDP を高信頼化するのはプログラミングの負荷がたかい.

■ つぎのようなプロトコルがある.
- ◆音声, 動画などのリアルタイム伝送のための RTP.
- ◆バイト単位ではないストリーム伝送のための SCTP.
- ◆ストリームではない単独のメッセージの高信頼伝送のための DCCP (Datagram Congestion Control Protocol)

■ TCP, UDP とくらべると, それ以外のトランスポートの使用はずっとすくない.
- ◆UDP の半分以下 (2008 年で 2% 以下, 2010 年で 4% 以下 (IIJ))

TCP, UDP 以外のトランスポート・プロトコル (つづき)

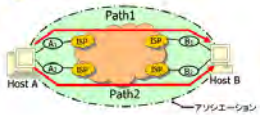
■ RTP (Real-time Transport Protocol)
- ◆音声, 動画などのデータ・ストリームのリアルタイム転送のためのプロトコルである.
- ◆IP 電話 (光電話など) でつかわれている.
- ◆制御のためのプロトコル RTCP (Real-Time Control Protocol) があわせてつかわれる.

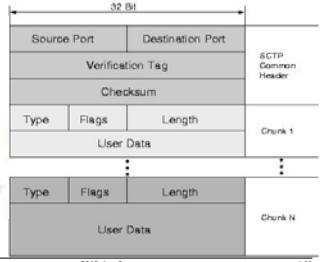


Copyright (c) 2002 Nikkei Business Publications, Inc.

TCP, UDP 以外のトランスポート・プロトコル (つづき)

■ SCTP (Stream Control Transmission Protocol)
- ◆2000 年に IETF で定義された, あたらしいプロトコル.
- ◆つぎの特徴を TCP と共有している: 輻輳制御, 到着順序保証 (再送制御)
- ◆TCP とちがって SCTP はフレームの列をあつかう (バイト列ではない).
- ◆TCP にはないいくつかの特徴をもっている.





ネットワーク・サービスの基礎プロトコル TCP と UDP のまとめ

■ TCP, UDP では「ポート」によって, 複数の通信が並行してできるようにしている.
- ◆1 個の IP アドレス (1 台のコンピュータ) で複数のポートがつくれる.

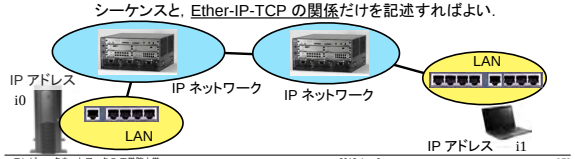
■ TCP, UDP では「ポート」によって, さまざまなプロトコルをつかいわけることができる.
- ◆ファイル転送のための FTP, 電子メールのための SMTP, Web のための HTTP などのプロトコルがある.

■ TCP では信頼性・性能のたかい通信を実現している.
- ◆パケットが脱落しても再送する.
- ◆通信路を他の通信とうまくわけあって有効につかうしくみがある.

■ TCP は複数のパケットにまたがるメッセージを伝送できる.
- ◆パケットの最大長 (MTU) にしばられない.

第 2 回 レポート課題

■ 課題: インターネット上にある Web サーバとクライアント (Web ブラウザ) とのあいだの通信のようすと, 途中にあるルータの状態を記述すること.
- ◆ネットワークはすくなくとも 2 台のルータをふくむ.
- ◆ネットワークの構造 (サブネットをふくむ) をきめ, IP アドレスをつける.
- ◆IP 通信: ルーティング・テーブルの内容をきめ, IP 通信のようすを記述する (スタティック・ルーティングとかんがえてよい).
- ◆TCP 通信: コネクション確立とデータ通信のようすを記述する.
  - ●ルータは TCP ヘッダをみないので, サーバ – クライアント だけのシーケンスと, Ether-IP-TCP の関係だけを記述すればよい.



第 2 回 レポート課題 (つづき)

■ 条件
- ◆サブネットのアドレスはつぎのなかからランダムにきめる.
  10.0.0.0/8, 172.16.0.0/16, 172.17.0.0/16,
  192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24
- ◆どのようにかんがえて答案を記述したかを 10 行程度にまとめる (箇条書きにするのがよい).

■ 提出方法など
- ◆紙で (レポート用紙等に書いて / A4 上質紙に印刷して) 提出するのが基本. しかし, 理由があれば Kuport 等で電子的に提出することも可.
- ◆期限: 7 月 13 日 (土) (当日提出できなければ, 事前に Kuport 等で提出すること. 22 日以降に提出しても得点はあたえない)

■ 採点方法
- ◆15 点満点
- ◆まちがいがなければ 15 点, まちがい 1 回ごとに基本的に -1 点.
- ◆くふうがある答案には最大 5 点加算 (5 個まちがいがあっても満点になりうる).

第 2 回 レポート課題のためのヒント

■ 以下のはヒントなので,
- ◆他の方法をつかってもよい.
- ◆以下の記述をまねしても, こたえにはならない.

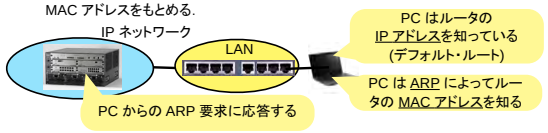
■ ネットワークの構造と IP アドレスをきめる.
- ◆さいころをふって (またはくじ引き, あみだくじなどで) サブネットをきめ, ルータのアドレスをきめる.

■ ルーティング・テーブルの内容をきめる.

図5-7 ルーティングテーブルによるパケットの中継

第 2 回 レポート課題のためのヒント (つづき)

■ 各 LAN のなかで ARP により MAC アドレスと IP アドレスが対応づけられるとして, ARP の通信を記述する (パケット・フォーマットまで書かなくてよい).
- ◆ 3 つの LAN とも同様なので, PC がある LAN だけ記述すればよい.
- ◆ LAN での通信には MAC アドレスが必要だが, PC は ARP によってルータの MAC アドレスをもとめる.



■ つぎに, IP 通信がどうやって実現されるかをかんがえる.
- ◆ルーティング・テーブルがどのようにつかわれて, IP パケットが PC - サーバ 間で転送されるかを記述する.
- ◆IP ネットワークでは通常, ルーティング・テーブルの内容はダイナミック・ルーティングできまるが, その過程まで記述しなくてよい.

第 2 回 レポート課題のためのヒント (つづき)

■ TCP による通信を PC -サーバ 間のシーケンス図によって記述する.
- ◆ シーケンスはコネクション確立からはじまりコネクション終了でおわる.
- ◆ コネクション確立につづいて, PC からサーバに TCP による Web (HTTP) の要求を送信する. (要求メッセージは 1 個の IP パケットにおさまるとする.)
- ◆ PC はサーバから TCP による Web の応答を受信する. (応答メッセージはウィンドウ・サイズをこえる個数のパケットにわかれるとする.)

9. インターネット上のネットワーク・サービス

要点

■ 人間とのインタフェースでは IP アドレスでなくドメイン名を使用する.
- ◆ドメイン名を IP アドレスと対応づけるのが DNS.

■ TCP 上のプロトコルをつかって, さまざまなサービスが提供されている.
- ◆HTTP をつかった Web
- ◆FTP をつかったファイル転送
- ◆SMTP, POP, IMAP などをつかった電子メール

■ UDP 上のプロトコルをつかったサービスもある.
- ◆SIP と RTP をつかった IP 電話

ドメイン名システム (DNS) の必要性

■ IP アドレスは人間が使用するのに適していない.
- ◆なまえをかえたくないが, サーバの移転などで IP アドレスの変更が必要なことがある.
- ◆IP アドレスは数値なので, おぼえにくい.

■ サーバなどにおぼえやすいなまえをつけるのが DNS (Domain Name System)

DNS の機能

■ DNS によってコンピュータやルータのなまえ (ホスト名) と IP アドレスが対応づけられる.

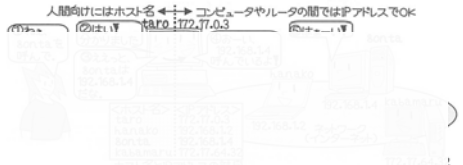


図8-2 ホスト名とIPアドレスの対応

DNS の機能 (つづき)

■ DNS によって階層的なななまえ (ドメイン名) がつけられる.
- ◆なまえの階層は IP アドレスの階層とは独立.
- ◆ことなる場所にあるおなじ組織のサーバをおなじドメインにおくことができる.
- ◆ドメイン名つきのホスト名を FQDN (fully-qualified domain name) という (www.google.co.jp = www (ホスト名) + google.co.jp (ドメイン名)).

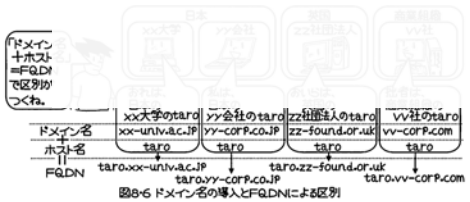


図8-6 ドメイン名の導入とFQDNによる区別

ドメイン名の階層構造

■ドメイン名は階層的な構造 (木構造) をしている.

図8-7 ドメイン名の階層(www.oh.msh.a.co.JPの例)

トップレベル・ドメイン名

- トップレベル・ドメイン (TLD) としては国コードをつかうのが一般的.
- インターネット発祥の地であるアメリカは以前からさまざまなトップレベル・ドメインをつかってきた.

表8-1 トップレベルドメイン(TLD)の分類

TLD名		
gTLD (g：generic) (この他に、新gTLDがある ex. biz.mobi)	com	商業組織用
	net	ネットワーク用
	org	非営利組織用
	edu	教育機関用
	gov	米国政府機関用
	mil	米国軍事機関用
	int	国際機関用
ccTLD (cc：country code)	JP(日本), uk(英国) など	各国／地域に割り当てられたTLD (米国の場合は…)

- 2001 年以降, .info, .biz, .coop, .museum, .name などのあたらしい TLD がつくられた.

日本のドメイン名

- 日本は TLD として jp をつかってきたが, 最近は自由化され, 多様化している.

表8-2 JPドメインのSLDの分類

SLD名		
組織種別型SLD	ac.JP	4年制…
	co.JP	株式会…
	go.JP	日本国…
	ad.JP	JPNIC…
	ne.JP	ネットワ…
	or.JP	財団法…
	gr.JP	任意団…
	ed.JP	高校～…
地域型SLD	shinjuku.tokyo.JP など	都道府…

- ◆ 以前はアメリカ中心につかわれていた .com, .org, .net などは日本でもつかえるようになった.
- ◆ 2001 年以降につくられた .biz, .info などのドメイン名は, はじめから日本でもつかえる.

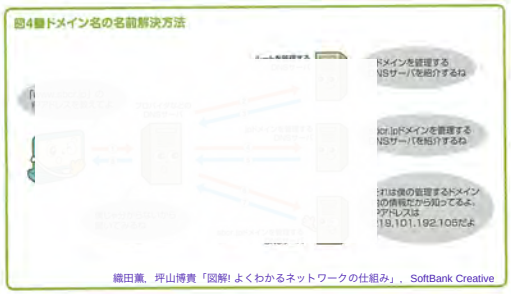
ドメイン名解決のしくみ

- ドメイン名に対応する IP アドレスが知りたいときは, ネーム・サーバにといあわせる.

PC にネームサーバを登録する
(DNS = 192.168.1.1 -- ブロードバンドルータはネームサーバもかねていることがおおい)

ドメイン名解決のしくみ (つづき)

- 1 台の DNS サーバがすべてのドメイン名を知っているわけではなく, DNS サーバどうしで通信して IP アドレスをもとめる.
  - ◆ そのため DNS へのといあわせには数 10 秒の時間がかかることもある.



絵田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

WWW (ウェブ) のための 3 つの基本技術

- Web ページ記述言語 HTML (HyperText Markup Language)
- Web のアドレス URL または URI (Unified Resource Locator/Identifier)
- Web のテキストを送信するためのプロトコル HTTP (HyperText Transfer Protocol)

図12-1 基本となる3つの技術(HTML,URI,HTTP)

WWW (ウェブ) のための記述言語 HTML

- Web ページを記述するための言語が HTML (HyperText Markup Language)
- HTML の特徴
  - ◆ HTML はマークアップ言語である.
  - ◆ HTML 文書はハイパーテキストである.

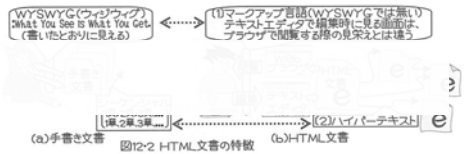


図12-2 HTML文書の特徴

HTML はマークアップ言語である

- HTML 文書は「タグ」によって構造や表示法がきめられる.
- タグをつかって他のファイル (画像, プログラムなど) がとりこめる.

図12-3 HTML:マークアップ言語

HTML 文書はハイパーテキストである

- リンクをクリックすると他の HTML 文書 (ページ) が参照できる.

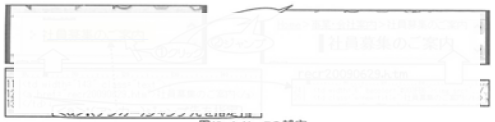


図12-4 リンクの設定

URL

- Web ページなどを識別するためのアドレスが URL または URI (Unified Resource Locator/Identifier) とよばれる.
  - ◆ 例: http://www.google.co.jp/

図12-5 URL(Uniform Resource Locator)とURN(Uniform Resource Name)

HTTP

■ Web のテキスト (ハイパーテキスト) をおくるためのプロトコルが HTTP (HyperText Transfer Protocol) である.

クライアント・サーバ・システムとしての WWW

■ HTTP は Web クライアント – Web サーバ 間のプロトコル
- ◆1 台の Web サーバを複数のクライアントが同時にアクセスできる.

■ HTTP は 要求応答型のプロトコル: 要求と応答をくりかえす
- ◆要求 (request) -- クライアントからサーバへ

```
GET / HTTP/1.1
Host: www.kanadas.com
…
```

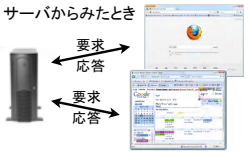
- ◆応答 (reply) -- サーバからクライアントへ

```
HTTP/1.1 200 OK
Date: Sat, 06 Jul 2013 07:01:26 GMT
Server: Apache/1.3.42 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.8e
Last-Modified: Sun, 17 Mar 2013 12:28:21 GMT
ETag: "54ac-5145b6e5"
Accept-Ranges: bytes
Content-Length: 21676
Content-Type: text/html

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
…
```


クライアント・サーバ・システムとしての WWW (つづき)

■ 要求–応答 のくりかえし

● サーバからみたとき

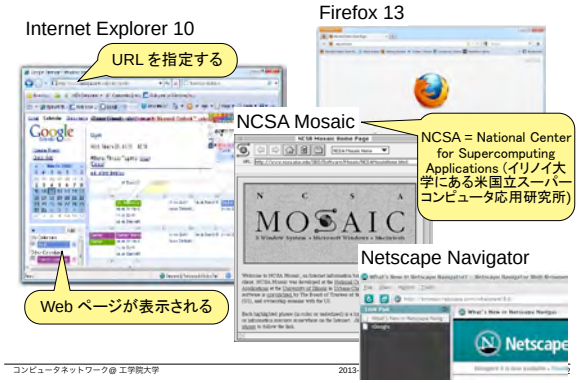


● クライアントからみたとき

● 現在では継続的な要求–応答のためのしくみもある.

セキュアな WWW 通信のためのプロトコル HTTPS において要求-応答 ごとに認証するのはおもすぎる.

Web クライアント (ブラウザ)



telnet コマンドで Web サーバにアクセスしてみよう

■ telnet コマンドをつかって Web サーバにアクセスできる.

```
$ telnet www.kanadas.com 80
Trying 219.94.162.224...
Connected to kanadas.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.kanadas.com

HTTP/1.1 200 OK
Date: Sat, 06 Jul 2013 07:01:26 GMT
Server: Apache/1.3.42 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.8e
Last-Modified: Sun, 17 Mar 2013 12:28:21 GMT
ETag: "54ac-5145b6e5"
Accept-Ranges: bytes
Content-Length: 21676
Content-Type: text/html

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head> … </head>

<body>

<h1><a href="/Kanada.html">Yasusi Kanada</a>'s Hub Page
  <small>(Home Page Ver. 4)</small>
</h1>
…
```

telnet も TCP を使用するアプリケーションのひとつ

TCP ポート 80

Macbook の Web サーバで実演

CLI と GUI

■ 人間がコンピュータにアクセスする基本的な方法は 2 つある.
- ◆CLI (Command-Line Interface): コマンドを文字によって入力する.
  - ●教科書には CUI と書いてあるが, これは Japanese English.
- ◆GUI (Graphical User Interface): 視覚的に表示されたメニューから, マウスなどのポインティング・デバイスで選択する.

図10-3 CLI と GUI

telnet によるリモートアクセス

■ 遠隔のコンピュータを CLI で使用するには telnet がつかわれてきた.
- ◆つぎのようなコマンドを使用する.
  - ●telnet XXXXXXXX.co.jp 23
  - ●telnet XXXXXXXX.co.jp

TCP ポート 23

TCP ポートは省略できる.

- ◆どんなコマンドでも入力できる (なんでもできる) ので強力.
- ◆パスワードをやぶられると非常に危険.

図10-2 アプリケーションプロトコルのtelnet

文字単位で動作する telnet

■ telnet では 1 文字 1 パケットでおくるのが基本
- ◆リモート・ホスト上のアプリケーションは 1 文字の入力で状態変化する可能性があるから.
- ◆しかし, 1 文字ずつおくるのは非常に効率がわるい (通常は行単位で十分).

図10-7 telnetは1文字ずつ送る(SINGLE CHARACTER MODE)

ファイル転送とファイル共有

■ 遠隔のコンピュータにあるファイルを利用する方法は 2 つある.

■ 1) ファイル転送: ファイルをコピーして, それぞれが使用する.
- ◆だれかがファイルを更新しても, ほかのひとはもとのファイルをみる.
- ◆FTP というプロトコルを使用してコピー (アップロード, ダウンロード) する.
- ◆最近は FTP のかわりに ssh というプロトコルを使用することが多い.

■ 2) ファイル共有: ひとつのファイルをみんなで使用する.
- ◆だれかがファイルを更新すると, ほかのひとも更新されたファイルをみる.
- ◆例: Windows でのファイル共有には Server Message Block (SMB) というプロトコルを使用する.

(b)ファイル転送 : 情報の共有

図10-1 基本的なネットワーク利用の2つの形態

ファイル転送のプロトコル FTP

- ファイル転送にはデータ送信用と制御用の 2 個の TCP ポート (20, 21) を使用する.
- 接続時にはユーザをパスワードで認証する.

織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

CLI による FTP: FTP サーバにアクセスしてみよう

- ftp コマンドを使用する.

公開された FTP サーバの例: 理化学研究所の FTP サーバ (riken = 理研, go = 政府機関)

公開された FTP サーバはユーザ名 anomymous でアクセスできる.

```
MacBook-Kana:~ yk$ ftp ftp.riken.go.jp
Connected to riksun.riken.go.jp.
220 ::ffff:134.160.38.1 FTP server ready.
Name (ftp.riken.go.jp:yk): anonymous
331 Anonymous login ok, send your complete email address as your password
Password: XXXXXXXX
230-------------------------------------------------------------------------
   This ftp/http/rsync service is an unsupported service of RIKEN
 Nishina Center for Research Support. Use entirely at your own risk
 - no warranty is expressed or implied. All transfers are logged.
 Request and questions should be sent to <admin@ftp.riken.jp>

 (news) 2009.03.27 ftp.riken.jp is connected to WAN at 10 Gbps.
-------------------------------------------------------------------------
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||6944|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   5 archive  archive        49 Jun 24  2011 11
drwxr-xr-x   3 root     root           20 Apr 13 08:44 12
drwxr-xr-x   3 root     root           23 Jun 24  2011 13
drwxr-xr-x   3 root     root           19 Jun 24  2011 14
lrwxrwxrwx   1 archive  archive        11 Aug 24  2010 CTAN -> tex-archive
drwxr-xr-x  17 archive  archive      4096 Jun 23 16:20 FreeBSD
...
ftp> get …
```

Macbook の FTP サーバで実演

CLI による FTP: FTP サーバにアクセスしてみよう (つづき)

- FTP のコマンド
  - ftp というプログラムにはさまざまなコマンドが用意されている.
  - もっとも基本的なのが get と put

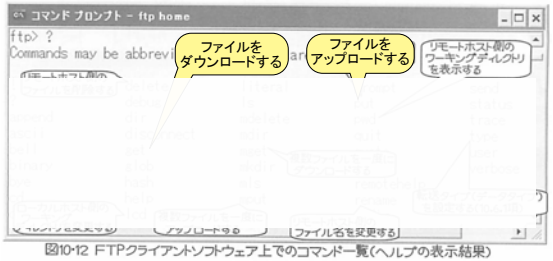


図10-12 FTPクライアントソフトウェア上でのコマンド一覧(ヘルプの表示結果)

GUI による FTP: Web/専用クライアント

Internet Explorer

URL として ftp://... を指定する.

FFFTP

2 つの telnet セッションによる FTP のシミュレーション

図10-23 シミュレーションの手順

SSH によるセキュアなファイル転送とログイン

- FTP と telnet の認証方法はパスワード認証にかぎられている.
- パスワード認証はやぶられやすいので, 最近は FTP, telnet を禁止して, 公開鍵認証をつかう SSH だけ使用できるサーバが多い.
  - SSH (セキュア・シェル) では TCP ポート 22 (だけ) を使用する.
  - ftp に対応するコマンドは sftp.
  - telnet に対応するコマンドは ssh.

```
MacBook-Kana:~ yk$ sftp XXXXXXXX@kanadas.com
ykanada@kanadas.com's password: XXXXXXXX
Connected to kanadas.com.
sftp> ls
AI-index.html                           AI-misc.html
...
sftp> get …
```

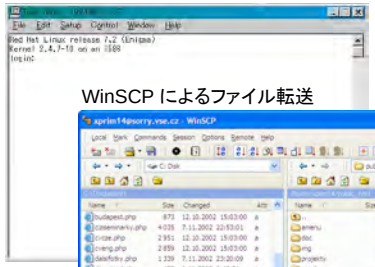
Macbook の ssh サーバで実演

```
MacBook-Kana:~ yk$ ssh XXXXXXXX@kanadas.com
ykanada@kanadas.com's password: XXXXXXXX
Last login: Sun May  6 17:24:06 2012 from 110.5.47.94
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.  All rights
reserved.

FreeBSD 7.1-RELEASE-p16 (SAKURA11S) #12: Mon Oct  3 17:12:59 JST 2011

Welcome to FreeBSD!

%ls
MT-5_04-ja.zip                  mt504.tgz
...
```

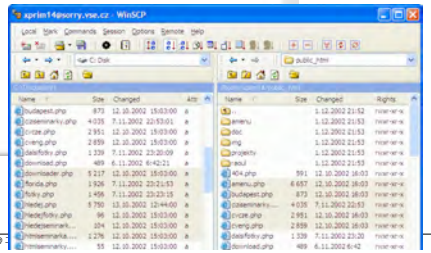
Macbook の ssh サーバで実演

SSH によるセキュアなファイル転送とログイン (つづき)

Tera term pro による Linux マシンへのログイン

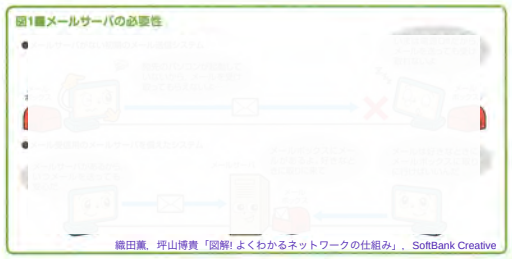


WinSCP によるファイル転送



電子メールとメールサーバ

- 電子メールはメールサーバ経由で配送する.
  - 正確には送信と受信にはことなるサーバを使用する.
- メールサーバがあれば, いつでもメールの送信・受信ができる.



織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

電子メールのメッセージ形式

- 電子メールの形式はエンベロープとメッセージとで構成される.
- エンベロープはメール・サーバのための情報であり, ユーザにはみえない.
- メッセージはユーザのためのものであり, サーバはみない.

図13 電子メールの形式

電子メールのアドレス

- 電子メールのアドレスはユーザ名とドメイン名とで構成される.
- 電子メールは指定されたドメインのメール・サーバに配送される.
  - DNS がメールサーバを知っているので, ドメインだけ指定すればよい.

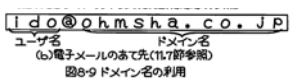


図8-9 ドメイン名の利用

日本語の電子メール

- 日本語の電子メールは ISO-2022-JP という文字コードで記述することにきまって (標準化されて) いる.
- 日本語の文字コードとしては現在では UTF (ユニコード) がつかわれることが多いが, 電子メールの標準はそのまえにきまった.
- 日本語の文字コードはいろいろあるので, 変換ミスなどによって文字化けをおこしやすい.

図11-7 日本語によるメールにおける問題の発生

電子メールと MIME (マイム)

- 電子メールで ASCII コード以外のデータをおくるときは MIME (Multipurpose Internet Mail Extensions) という方法をつかう.
  - 日本語 (ISO-2022-JP) をおくるのにも MIME を使用する.
  - UTF-8 など, 他の文字コードをおくることもできる.
  - 画像, 音声などもおくることができる.


図11-8 メールヘッダ中のエンコーディング法の指定

電子メール送信のためのプロトコル SMTP

- PC などからメールサーバにメールを送信するときは, SMTP (Simple Mail Transfer Protocol) を使用する.

織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

電子メール送信のためのプロトコル SMTP (つづき)

- SMTP は push 型のプロトコルである.
  - メール受信用のコンピュータで, 常時, サーバを動作させていることが基本である.
- パソコンは使用時だけ起動することが多いので, push 型ではメールをとりそこなう可能性がある.
  - メールの送信側は送信に成功するまでメールを保管するが, いつまでも送信されない可能性がある.
- POP, IMAP というプロトコルを使用すれば, この問題をさけることができる.

電子メール受信のためのプロトコル POP

- PC などでメールを受信するときは, POP (Post Office Protocol) というプロトコルを使用する.

織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

電子メール受信のためのプロトコル POP (つづき)

- POP は pull 型のプロトコルである.
  - ユーザはメールを受信したいときだけ POP でメール・サーバに要求すればよい.
  - 要求されないかぎり, メール・サーバがクライアントにメールを送信することはない.
  - そのため, メール・クライアントは一定時間ごとにメール・サーバにポーリング (くりかえし, といあわせること) するようになっている.
    - メール・クライアントの設定でポーリングの間隔を設定する.

電子メール受信のためのプロトコル IMAP

- メールの受信のためのプロトコルとして IMAP (Internet Message Access Protocol) もある.
  - 受信したメールをサーバ側で管理したいときには IMAP をつかう.
  - 複数の PC などでメールを読むときは IMAP のほうが便利である.

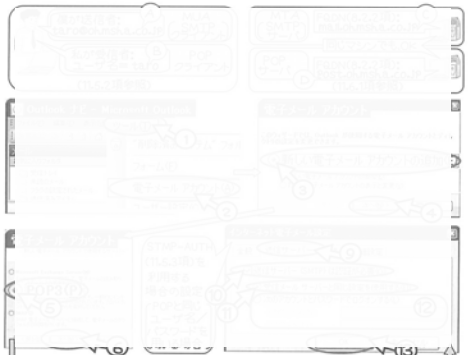
織田薫, 坪山博貴「図解! よくわかるネットワークの仕組み」, SoftBank Creative

電子メール受信のためのプロトコル IMAP (つづき)

- IMAP も pull 型のプロトコルである.
  - メール・クライアントの動作 (ポーリングなど) は POP のときと同様.

電子メール送受信のための設定

■ Windows の Outlook の例



SIP による IP 電話・テレビ電話

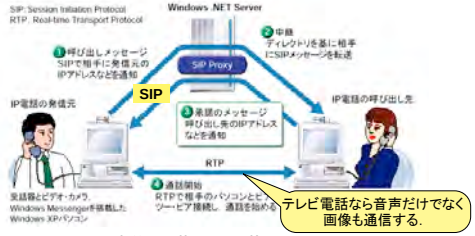
■ 公衆電話網 (PSTN，電話のネットワーク) はインターネットでおきかえられつつある.
- ◆PSTN = Public Switched Telephone Network.
- ◆NTT は 2025 年までに IP ネットワークに移行する予定.

■ インターネット上での電話 (IP 電話) などの制御のために，SIP (Session Initiation Protocol) がひろまりつつある.
- ◆SIP は IP, TCP などと同様に IETF で標準化された.
- ◆SIP は電話専用ではなく，汎用のセッション制御プロトコルである.

■ IP 電話では SIP とデータ通信用プロトコルとを併用する.
- ◆リアルタイム音声・動画通信には Real-time Transport Protocol (RTP) を使用する.

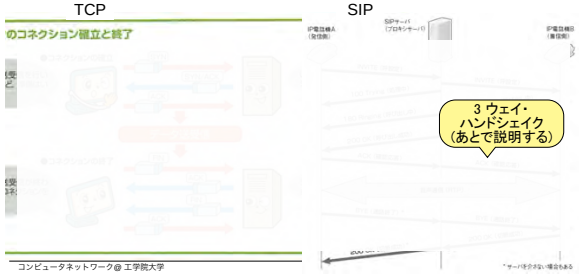
IP 電話の概要

■ SIP で (SIP プロキシ経由で) セッションを確立し，RTP で相手と直接音声通信する.
- ◆従来の電話では制御も音声通信も交換機をとおしていた.
- ◆ただし，送信者と受信者とで音声のプロトコルがことなるときなどは，音声にも制御装置が介在する.



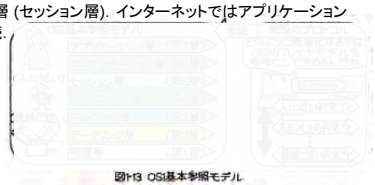
SIP の下位プロトコルと 3 ウェイ・ハンドシェイク

■ SIP は TCP をつかうこともできるが，UDP をつかうこともできる.
- ◆信頼性がひくい UDP 上でも信頼性を確保することができる.
- ◆そのために TCP と同様に接続時に 3 ウェイ・ハンドシェイクをつかう.



SIP の特徴

■ SIP は HTTP にちかいセッション制御用プロトコル.
- ◆「セッション」は「コネクション」にちかい概念だが，もっと高度な制御ができる接続のことをいう.
  - ●OSI では第 5 層 (セッション層). インターネットではアプリケーション層における接続.



■ SIP では送信者と受信者は対称，つまりどちらもサーバになり，どちらもクライアントになる.
- ◆HTTP ではユーザがクライアントとしてサーバにアクセスするという，非対称の通信をする.

SIP の特徴 (つづき)

■ HTTP と同様にテキスト・ベースのプロトコルである.
- ◆これに対して従来の電話のプロトコルはバイナリ・プロトコルである.
- ◆SIP メッセージの例 (相手のよびだし):

TCP を使用 (UDP でなく)　メッセージの配送先

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

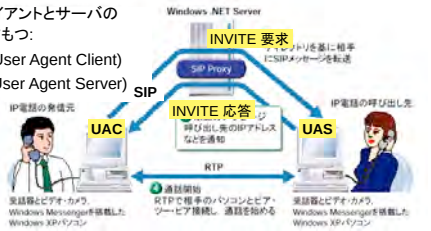
自分の URI (電話番号に相当)

相手の URI (電話番号に相当)

SIP 通信に登場する役者たち

■ SIP サーバ
- ◆制御通信を中継するサーバ.

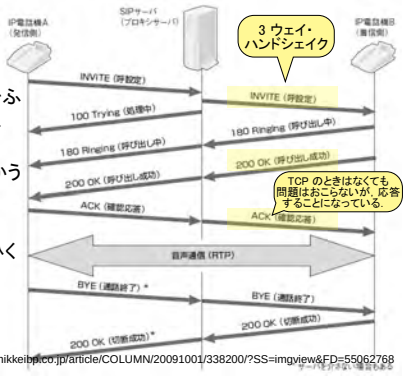
■ ユーザ・エージェント (UA)
- ◆ユーザのために通信するエージェント (代理者)
- ◆IP 電話でいえば電話機
- ◆UA はクライアントとサーバの機能を両方もつ:
  - ● UAC (User Agent Client)
  - ● UAS (User Agent Server)



SIP による IP 電話のシーケンス

■ 音声通信には RTP をつかう. (リアルタイム通信むけの機能をふくんでいるため).

■ 通信制御には SIP/UDP をつかうことがおおい (SIP/TCP よりサーバ負荷がひくいため).



http://itpro.nikkeibp.co.jp/article/COLUMN/20091001/338200/?SS=imgview&FD=55062768

インターネット上のネットワーク・サービスのまとめ

■ 人間とのインタフェースでは IP アドレスでなくドメイン名を使用する.
- ◆ドメイン名を IP アドレスと対応づけるのが DNS.

■ TCP 上のプロトコルをつかって，さまざまなサービスが提供されている.
- ◆HTTP をつかった Web
- ◆FTP をつかったファイル転送
- ◆SMTP, POP, IMAP などをつかった電子メール

■ UDP 上のプロトコルをつかったサービスもある.
- ◆SIP と RTP をつかった IP 電話

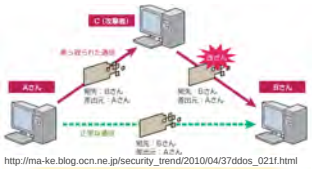
10. ネットワーク・セキュリティ

要点

- ネットワーク上の脅威とセキュリティの確保
  - ◆ネットワーク上には盗聴，中間者攻撃，DoS 攻撃，なりすましなどの脅威がある．
  - ◆セキュリティ確保の手段としては，ネットワークの隔離，認証，認可がある．
- ネットワークの部分隔離のためファイアウォールがつかわれる．
- 暗号には共通鍵暗号と公開鍵暗号があり，後者を使用して Web の暗号化・認証 (TLS/SSL) などが実現されている．
- 認証のため パスワードや公開鍵暗号を使用した電子署名が使用される．
- アクセス権限の認可にもとづいて，ファイアウォールなどではポリシー規則などにもとづくアクセス制御がおこなわれる．
- 無線 LAN のセキュリティのため，WEP, WPA, TKIP など，さまざまな方法が開発されている．

ネットワーク上の脅威

- 盗聴 (eavesdropping)
  - ◆通信路上の暗号化していないパスワードをぬすむなど．
- 中間者攻撃 (man-in-the-middle attack)
  - ◆通信経路を勝手に変更するなどして盗聴したり，メッセージをかきかえたりするなど．
- DoS 攻撃 (denial-of-service attack)
  - ◆サーバに多量のパケットを送信してサービスできなくするなど．
  - ◆多数の踏み台をつかうものを DDoS (分散 DoS) という．

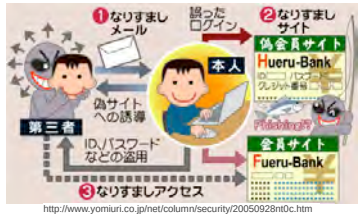


http://ma-ke.blog.ocn.ne.jp/security_trend/2010/04/37ddos_021f.html

http://ma-ke.blog.ocn.ne.jp/security_trend/2008/10/3_944e.html

ネットワーク上の脅威 (つづき)

- なりすまし (spoofing)
  - ◆にせのサーバやにせのユーザに偽装してパスワードなどの情報をぬすむ．



http://www.yomiuri.co.jp/net/column/security/20050928nt0c.htm

コンピュータへの侵入の方法と対策

- クラッカー (ハッカー) は認証の壁をやぶって侵入する．
  - ◆リモート・アクセスして，スーパーユーザのパスワードをぬすんで侵入する．
  - ◆暗号を使用した認証なら，平文による認証より安全である．

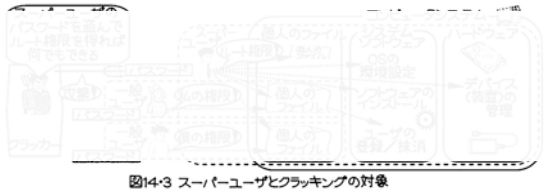


図14-3 スーパーユーザとクラッキングの対象

セキュリティ確保のための方法

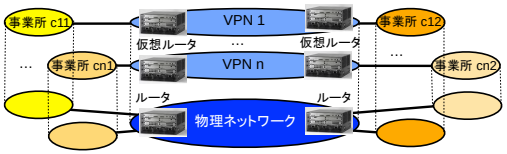
- 隔離
- 暗号化
- 認証
- 認可

- ネットワークの隔離
  - ◆プライベート・ネットワークを構築して，物理的または論理的にインターネットから隔離された環境をつくる．
  - ◆物理的に完全に隔離するのがもっともセキュアだが，それができないときはインターネットとのあいだにファイアウォールを設置する．
- 暗号化 (encryption)
  - ◆通信内容が暗号化されていれば，盗聴されても情報漏洩しない．
- 認証 (authentication)
  - ◆人などがネットワークや通信を利用する権限をもっていることを確認する．
  - ◆認証の手段としてパスワードや電子証明書などがある．
- 認可 (authorization)
  - ◆ネットワークや資源 (サーバなど) にアクセスする権限を設定する．
  - ◆認証された (アイデンティティが確立された) ユーザごと，またはそれ以外のユーザ (一律) に権限が設定される．

プライベート・ネットワークによる隔離

- 隔離
- 暗号化
- 認証
- 認可

- プライベート・ネットワークをつくることでインターネットから隔離され，セキュリティが確保できる．
  - ◆物理的なプライベート・ネットワークと仮想的なプライベート・ネットワーク (VPN) とがある．



- 完全に隔離すると不便なので，ファイアウォールを使用する．

ファイアウォールによるネットワークの隔離と接続

- 外部ネットワークから完全に隔離できないとき，ファイアウォールを設置して内部 (組織内ネットワーク) を脅威からまもる．
- 外部から隔離できない理由は，外部サービスの利用，外部へのサービスの提供など．

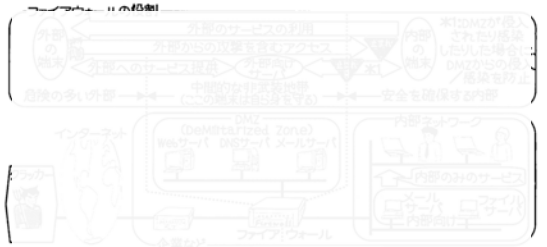


図14-14 ファイアウォール(Firewall)の役割と構成例

ファイアウォールにおけるパケット・フィルタ

- ファイアウォールにはパケット・フィルタ規則が設定される．

	許可/拒否	通信方向	プロトコル	送信元 IPアドレス	送信元 ポート番号	受信先 IPアドレス	受信先 ポート番号	内容
(1)	拒否	すべて	ICMP	すべて	—	すべて	—	Pingなどを無応答
(2)	拒否	すべて	TCP/UDP	すべて	すべて	すべて	137～139	ファイル共有を拒否(※5)
(3)	拒否	すべて	すべて	10.0.0.0～10.255.255.255	すべて	すべて	すべて	プライベートアドレスの遮断，図9-3中の他のアドレスも同様
(4)	拒否	すべて	すべて	すべて	すべて	10.0.0.0～10.255.255.255	すべて	
(5)	拒否	外→内	すべて	xxx.10.10.1～2	すべて	すべて	すべて	サーバを偽装したパケット遮断
(6)	許可	外→DMZ	TCP	すべて	すべて	xxx.10.10.1	80	wwwサーバ公開 (※1)
(7)	許可	外→DMZ	UDP	すべて	すべて	xxx.10.10.2	53	DNSサーバ公開 (※2)
(8)	許可	内→外	すべて	すべて	すべて	すべて	すべて	内部からの接続を許容(※3)
(9)	拒否	外→内	すべて	すべて	すべて	すべて	すべて	外部からの接続を拒否(※4)

※ 上記の設定は系統的なものではなく，設定例としての項目を列挙している．
※ 防御される攻撃の例： pingスイープ(図14-6(a))←(1)，IPスプーフィング(図14-8)←(3)，ICMPスプーフィング(図14-11(d))←(1)(3)(5)

図14-15 ファイアウォールでのパケットフィルタリングとその設定例

パソコンのファイアウォール

- パソコンにもファイアウォールを設定することができる．
  - ◆ファイアウォールはパソコンと外部との通信を監視する．
  - ◆家庭 / 職場内ネットワークの外部からのアクセスはきびしく制限する．


図14-17 Windows PCでのファイアウォールの設定

暗号とその種類

- 隔離
- **暗号化**
- 認証
- 認可

■ 暗号とは?
- ◆ 特別な知識なしでは通信内容がわからないように通信文を変換する方法.

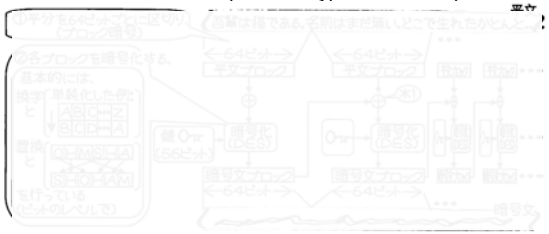
■ 暗号の種類
- ◆ 共通鍵暗号 (対称暗号)
  - ●暗号化と復号化とに同一の鍵 (秘密鍵) を使用する暗号方式.
- ◆ 公開鍵暗号
  - ●公開鍵によって暗号化した暗号文が秘密鍵を知らないと復号化できない暗号方式.

共通鍵暗号

■ 暗号化と復号化とに同一の鍵 **(秘密鍵)** を使用する暗号方式.

■ 基本的に 1 対 1 の通信だけに使用される.

■ 共通鍵暗号の例: DES (Data Encryption Standard)



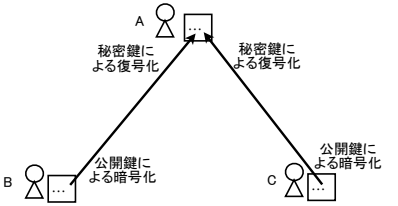
*1:同じ平文ブロックが同じ暗号文ブロックになるようなことを避けるために,前の暗号化ブロックを足しこんでいる(排他的論理和).このような繰り返し方法を「モード」と呼ぶ(図とは違う方法もある).

図14-20 DES(Data Encryption Standard)での暗号化の概要(対称暗号の例)

公開鍵暗号

■ 公開鍵によって暗号化した暗号文が, 秘密鍵を知らないと復号化できない (復号化に天文学的な時間がかかる) 暗号方式.

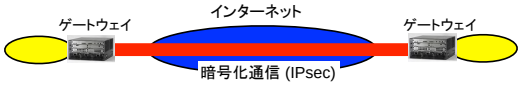
■ 多対多の通信に使用できる.



暗号化通信のためのプロトコル IPsec

■ IPSec はネットワーク層 (IP) において暗号化と認証をおこなうためのプロトコルである.

■ IPSec は VPN における暗号化のためにも使用される.
- ◆ Internet VPN (IPsec VPN) においてはインターネット上で暗号化通信をする.

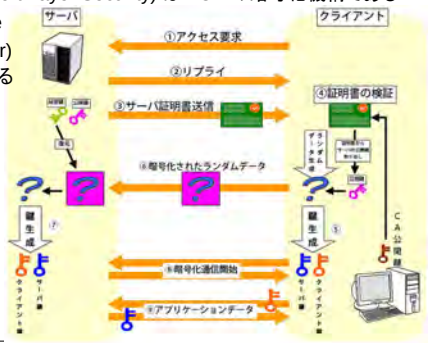


- ◆ IPsec によってカプセル化する.

TLS と SSL

■ TLS (Transport Layer Security) は TCP の暗号化機構である.

■ SSL (Secure Socket Layer) は TLS のふるい版である.



TLS と SSL (つづき)

■ TLS/SSL は Web の暗号化によく使用される.
- ◆ SSL は Netscape Navigator (Web ブラウザ) のために開発された.

認証の方法

- 隔離
- 暗号化
- **認証**
- 認可

■ 認証とは, 人などのアイデンティティを確認し, ネットワークや通信を利用する権限をもっていることを確認することである.

■ 認証の手段
- ◆ パスワード
- ◆ 電子署名

パスワード認証の弱点

■ パスワードは漏洩しやすい
- ◆ パスワードはくりかえし入力 (送信) される.
- ◆ 漏洩したパスワードをそのままつかえば認証される.

■ パスワードは発見されやすい
- ◆ みじかいパスワードはランダムに生成してもあてられる.
- ◆ パスワードにはおぼえやすいつづりがつかわれることが多い.
  - ●生年月日, こどものなまえ, など.

パスワード認証の改良: ワンタイム・パスワード

■ 毎回ことなるパスワードを入力することによって, ぬすまれるのをふせぐ.

■ 手でパスワードを計算するのは困難なので, PC がパスワードを生成してサーバにおくったり, 「トークン」を使用したりする.
- ◆ いずれの方法もサーバとユーザとが秘密情報 (関数など) を共有する必要がある.

■ 2 つの方法
- ◆ 時刻同期方式 (タイムスタンプ方式)
  - ●サーバとユーザ側とで時刻同期してパスワードを計算する.
  - ●ユーザは「トークン」に表示されたパスワードを入力する.
- ◆ チャレンジ・レスポンス方式
  - ●サーバからランダムな値をおくり, ユーザ, サーバ双方がそれにもとづく関数値を計算する. サーバがその値が一致するかどうかしらべる.

電子証明書による認証

■ 公開鍵暗号を使用した電子証明書を使用すれば，パスワードよりセキュアに認証できる．

■ 電子証明書は信頼できる機関 (認証局) が発行する必要がある．

認可とアクセス制御

■ 隔離
■ 暗号化
■ 認証
■ 認可

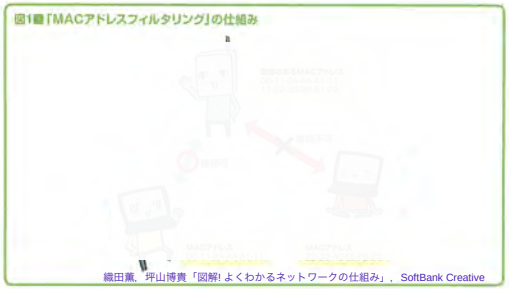
■ 認可とは，ネットワークや資源 (サーバなど) にアクセスする権限を設定すること．
  ◆ 認証された (アイデンティティが確立された) ユーザごと，またはそれ以外のユーザ (一律) に権限が設定される．

■ 認可にもとづいてネットワークや資源へのアクセス制御がおこなわれる．
  ◆ ファイアウォールにおいても，外部から内部，内部から外部へのアクセス制御がおこなわれる．

■ アクセス制御には，ポリシー規則やアクセス制御リストが使用される．
  ◆ ポリシー規則は “if 条件 then 動作” のかたちの規則．
  ◆ アクセス制御リスト (ACL) はオブジェクト (ファイルなど) に付加された，だれのどういうアクセスを許可するかをならべたリスト．

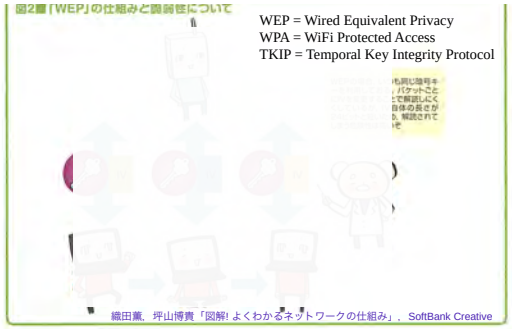
無線 LAN のセキュリティ

■ MAC アドレス・フィルタリングによって，特定の MAC アドレスをもつコンピュータだけがつなげるようにできる．



無線 LAN のセキュリティ（つづき）

■ WEP, WPA, TKIP などのしくみで暗号化通信ができる．
  ◆ 適切なしくみをえらんで，または自動的な方法で設定すればよい．



ネットワーク・セキュリティのまとめ

■ ネットワーク上の脅威とセキュリティの確保
  ◆ ネットワーク上には盗聴，中間者攻撃，DoS 攻撃，なりすましなどの脅威がある．
  ◆ セキュリティ確保の手段としては，ネットワークの隔離，認証，認可がある．

■ ネットワークの部分隔離のためファイアウォールがつかわれる．

■ 暗号には共通鍵暗号と公開鍵暗号があり，後者を使用して Web の暗号化・認証 (TLS/SSL) などが実現されている．

■ 認証のため パスワードや公開鍵暗号を使用した電子署名が使用される．

■ アクセス権限の認可にもとづいて，ファイアウォールなどではポリシー規則などにもとづくアクセス制御がおこなわれる．

■ 無線 LAN のセキュリティのため，WEP, WPA, TKIP など，さまざまな方法が開発されている．

「コンピュータネットワーク」試験実施の予告

■ 日時: 2012 年 7 月 27 日 (土) 18:00～19:20

■ 場所: A-0865

■ 条件
  ◆ 講義資料 (配布したものまたは Kuport 掲載のもの) もちこみ可．
  ◆ ノートもちこみ可 (コピーをふくむ)．
  ◆ 上記以外の本，書類や機器はもちこみ不可．

■ 付記
  ◆ 記憶をためす問題は基本的に出題しない．
  ◆ 問題は 3 題程度．
  ◆ イーサネット，IP，TCP/UDP にまたがる問題を出題する予定．
  ◆ 問題の難易度はレポートのできをみて調整する．