北海道情報大学　通信教育部
コンピュータネットワーク

2024年3月29日

講義補助資料（スライド一覧）

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

教科書と注意事項

- 情報通信ネットワーク入門
  尾崎 博一　著　コロナ社　2023年
- 注意：
  - 授業は全て受講すること。
  - 授業に関してノートを作ること。

Blank Page

コンピュータネットワーク

第1回
序論

今回の到達目標

1. 10進数，2進数，16進数の間で基数変換ができるようになる。
2. ビットとバイトの意味を説明できるようになる。
3. 単位の接頭語を覚える。
4. 情報通信ネットワークとは何かを説明できるようになる。
5. 通信の形態を説明できるようになる。
6. インターネットの歴史を説明できるようになる。
7. インターネットおよび通信一般に関係する組織を挙げて説明できるようになる。

10進数，2進数，16進数

- 10進数（0～9で表現）
  - 私たちの普段の生活で用いられる。
- 2進数（0と1で表現）
  - コンピュータやネットワークの装置内で用いられる。
- 16進数（0～9，A～Fで表現）
  - 2進数を短く表記するために用いられる。
  - 16進数であることを明示する時は先頭に「0x」をつける。
- 基数変換
  - 10進数，2進数，16進数の間で変換を行うこと。

ビットとバイト

- ビット（bit）
  - 2進数のひとけた（0または1）
- ビット列
  - ビットの並び（例：01011100・・・・・・）
- バイト（byte）
  - 長さ8のビット列（例：01011010）
- バイト列
  - バイトの並び（例：01011010 11011010 ・・・・・・）

1バイト（8ビット）で表される数値

10進数	2進数	16進数	10進数	2進数	16進数
0	0000 0000	0x00	16	0001 0000	0x10
1	0000 0001	0x01	····	····	····
2	0000 0010	0x02	31	0001 1111	0x1F
3	0000 0011	0x03	32	0010 0000	0x20
4	0000 0100	0x04	····	····	····
5	0000 0101	0x05	63	0011 1111	0x3F
6	0000 0110	0x06	64	0100 0000	0x40
7	0000 0111	0x07	····	····	····
8	0000 1000	0x08	127	0111 1111	0x7F
9	0000 1001	0x09	128	1000 0000	0x80
10	0000 1010	0x0A	····	····	····
11	0000 1011	0x0B	254	1111 1110	0xFE
12	0000 1100	0x0C	255	1111 1111	0xFF
13	0000 1101	0x0D			
14	0000 1110	0x0E			
15	0000 1111	0x0F			

10

1バイトの基数変換

- 2進数から10進数への変換
  - 「1」の立っている桁を足し算する。
- 10進数から2進数への変換
  - 「128, 64, 32, 16, 8, 4, 2, 1」を順次引き算する。
    引き算でマイナスにならない桁に「1」を立てる。
- 16進数から2進数への変換
  - 16進数のひとけたを2進数で表して連結
- 2進数から16進数への変換
  - 2進数の4桁を16進数で表して連結

11

2進数→10進数の変換例

Most Significant Bit: **MSB**　　Least Significant Bit: **LSB**

1101 0101

128 + 64 + 16 + 4 + 1 = 213

12

10進数→2進数の変換例

249

あるいは

2) 249
2) 124 … 1
2) 62 … 0
2) 31 … 0
2) 15 … 1
2) 7 … 1
2) 3 … 1
1 … 1

249 − 128 = 121　1
121 − 64 = 57　1
57 − 32 = 25　1
25 − 16 = 9　1
9 − 8 = 1　1
1 − 4 < 0　0
1 − 2 < 0　0
1 − 1 = 0　1

1111 1001

13

単位の接頭語（SI接頭語）

接頭語（記号）	読み方	意味
P	ペタ（peta）	10^{15}（1000兆）
T	テラ（tera）	10^{12}（1兆）
G	ギガ（giga）	10^{9}（10億）
M	メガ（mega）	10^{6}（100万）
k	キロ（kilo）	10^{3}（千）
m	ミリ（milli）	10^{-3}（千分の一）
μ	マイクロ（micro）	10^{-6}（100万分の一）
n	ナノ（nano）	10^{-9}（10億分の一）
p	ピコ（pico）	10^{-12}（1兆分の一）
f	フェムト（femto）	10^{-15}（1000兆分の一）

SI: Le Système International d'Unités（仏: 国際単位系）

14

伝送速度

- ネットワークにおいて情報を伝える速度
  - 「毎秒何ビット送ることができるか」で表す。
  - 表し方はいろいろある。
    - ビット／秒，bit/s，b/s，bps（ bit per second）
    - 教科書ではbps（ビーピーエスまたはビットパーセコンド）を採用
  - 例
    - 毎秒1,000ビット　：1kbps（1キロビーピーエス）
    - 毎秒10億ビット　：1Gbps（1ギガビーピーエス）

15

通信ネットワークの発展

- 高速化，大容量化，高信頼化

16

コンピュータの発展

- 小型化、省電力化、高性能化

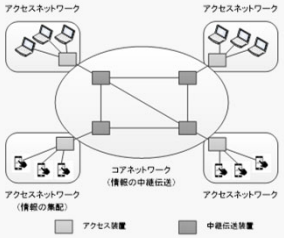
17

情報通信ネットワークとは

- コンピュータと通信ネットワークが融合したもの
- 高度に発達した通信技術を利用するコンピュータネットワーク
- ICT（Information and Communications Technology）
  - 情報通信ネットワークを実現する技術

18

情報通信ネットワークの構成



19

伝送媒体と伝送路

- 伝送媒体
  - 信号が流れる媒体（電気や光のケーブル，空間）
- 伝送路
  - 信号が流れる物理的な経路

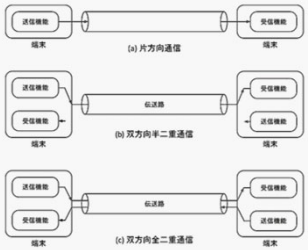
20

通信の形態

- 伝送媒体による分類
  - 有線通信と無線通信
- 通信の方向による分類
- 通信相手の数による分類
- ネットワークのトポロジーによる分類

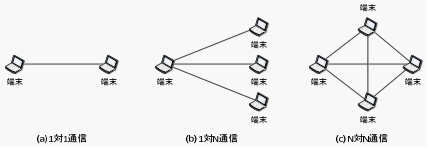
21

片方向，双方向（半二重，全二重）



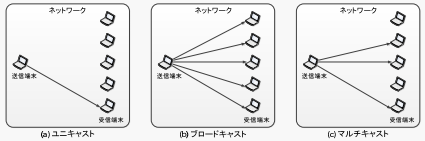
22

1対1，1対N，N対N通信



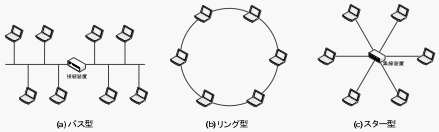
23

ユニキャスト，ブロードキャスト，マルチキャスト



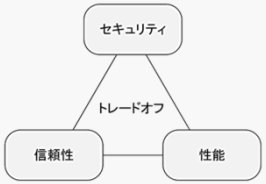
24

ネットワークトポロジー



25

情報通信ネットワークに対する要求



26

インターネットの歴史

- ARPANET
  - ARPA（高等研究計画局）による実験的なコンピュータネットワーク
  - 初めは4つの大学・研究機関を接続
  - その後，急速に参加するネットワークが増加
- NSFNET
  - NSF（全米科学財団）によるコンピュータネットワーク
  - ARPANETを引き継ぐ。
- Internet
  - 世界規模のコンピュータネットワーク

27

インターネット及び通信に関係する組織

- ICANN
  - コンピュータやネットワークの名前や番号を世界規模で調整
- IETF
  - インターネットの技術仕様（RFC）を策定
- IEEE
  - LAN（Local Area Network）の技術仕様を策定
  - ネットワーク機器の物理アドレスを管理
- ITU-T
  - インターネットを除く通信一般の標準（勧告）を策定

RFC

- IETFが作成するインターネットの技術仕様

RFC	タイトル	内容
RFC 791	INTERNET PROTOCOL	IPv4の基本仕様
RFC 792	INTERNET CONTROL MESSAGE PROTOCOL	ICMPv4の基本仕様
RFC 9293*	Transmission Control Protocol (TCP)	TCPの基本仕様
RFC 768	User Datagram Protocol	UDPの基本仕様
RFC 8200	Internet Protocol, Version 6 (IPv6) Specification	IPv6の基本仕様
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	ICMPv6の基本仕様

*TCPの基本仕様は長くRFC 793であったが，2022年8月にRFC 9293に置き替えられた。

今回学んだこと

1. 10進数，2進数，16進数の間の基数変換
2. ビットとバイトの意味
3. 単位の接頭語
4. 情報通信ネットワークとは何か。
5. 通信の形態
6. インターネットの歴史
7. インターネットおよび通信一般に関係する組織

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第2回
ディジタル通信技術（1）

今回の到達目標

1. アナログとディジタルの意味を理解する。
2. ディジタル信号の特徴を理解する。
3. 信号の劣化と修復方法を理解する。
4. アナログ信号をディジタル信号に変換する方法を理解する。
5. ベースバンド伝送とブロードバンド伝送の意味を理解する。
6. 正弦波と信号の周波数成分を理解する。

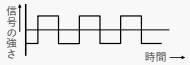
アナログとディジタル

- アナログ（analog）
  - 連続的に変化する現象一般を指す。
  - たとえば音や光などの自然現象はアナログ的。
- ディジタル（digital）
  - 離散的かつ数値的なものを指す。
  - たとえば0と1で表現される情報はディジタル的。

アナログ信号とディジタル信号

- アナログ信号
  - アナログ的な情報をそれに類似する電気や光の連続的な変化で表した信号。

- ディジタル信号
  - ディジタルで表された情報を電気や光の離散的な変化で表した信号



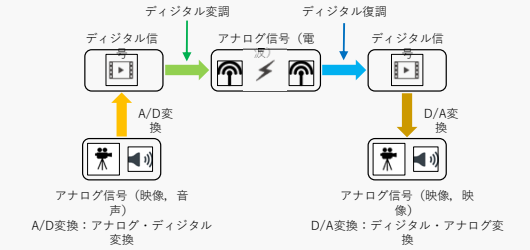
ディジタルかデジタルか

- ディジタル
  - 原音[dídʒətl]に近い。
  - JIS（日本工業規格）の用語では「ディジタル」
  - 情報系の各種資格試験も「ディジタル」
- デジタル
  - 日本人には発音しやすい。
  - デジタル庁，デジタルビジネスのように最近は普及している。
- 教科書および授業では「ディジタル」とする。

アナログとディジタルの関係（1）

- インターネットやLANなどのコンピュータネットワークではディジタル信号が用いられる。
- しかし，アナログ信号も重要である。
  - アナログ情報（音声，映像）を運ぶ必要がある。
  - アナログ信号を用いてディジタル情報を運ぶ場合がある。（無線通信）

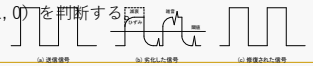
アナログとディジタルの関係（2）



10

ディジタル信号の特長

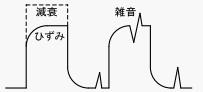
- 途中で信号の劣化が発生しても修復しやすい。
- 信号の劣化
  - 減衰　：信号の強度が弱くなること。
  - ひずみ：信号の形が変わること。
  - 雑音　：無関係な信号が混入すること。
- 修復の方法
  - ある閾値（しきいち）を定めてそれよりも大きいか小さいかで
    情報（1, 0）を判断する。



11

ディジタル信号の特長（1）

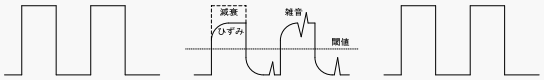
- 途中で信号の劣化が発生しても修復しやすい。
- 信号の劣化
  - 減衰　：信号の強度が弱くなること。
  - ひずみ：信号の形が変わること。
  - 雑音　：無関係な信号が混入すること。



12

ディジタル信号の特長（2）

- 修復の方法
  - ある閾値（しきいち）を定めてそれよりも大きいか小さいかで
    情報（1, 0）を判断する。



(a) 送信信号　(b) 劣化した信号　(c) 修復された信号

13

信号の遅延

- 信号が宛先に遅れて届くこと。
- 信号自体の劣化とは異なる。
- 以下の４つが原因となる。
  - 処理時間（processing time）　→処理遅延
  - 伝送時間（transmission time）　→伝送遅延
  - 待ち時間（queuing time）　→待ち行列遅延
  - 伝搬時間（propagation time）　→伝搬遅延
- インターネットで問題となる遅延はおもに伝送遅延と待ち行列遅延

14

遅延の原因となる時間


伝送時間

- 処理時間
  - 端末や中継装置における信号の処理時間
- 伝送時間
  - 信号を伝送路に送り出すために必要な時間（bit÷bps）
- 待ち時間
  - 信号を伝送する前に待つ時間
- 伝搬時間
  - 信号が伝送媒体を物理的に伝わる時間
    - 無線通信（電波）：30万km/秒，有線通信（ケーブル）：20万km/秒

15

情報のディジタル化

- A/D変換
  - アナログ信号をディジタル信号に変換すること
  - 標本化（sampling），量子化（quantization），符号化（coding）の3つの処理を順に行う。
- D/A変換
  - ディジタル信号をアナログ信号に変換すること

16

標本化，量子化，符号化

- 標本化
  - アナログ信号の瞬間の値（標本値）をある時間間隔（通常は
    一定間隔）で採取すること
- 量子化
  - 標本化された値から端数を取り除き整数にすること（切り上げ，
    切り捨て，四捨五入など）
- 符号化
  - 量子化で得られた値を数値（n進数）で表すこと
    - n=2の場合が多いが，それに限られるわけではない。

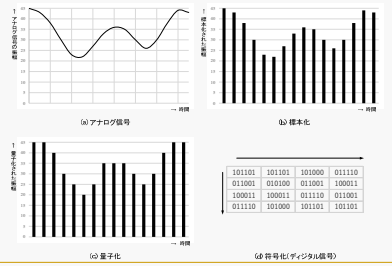
17

標本化定理

- 標本化周波数の下限を与える。
- 標本化周波数はもとのアナログ信号に含まれる最高周波数の2倍以上とすればよい。

18

A/D変換の例



(a) アナログ信号　(b) 標本化　(c) 量子化

101101	101101	101000	011110
011001	010100	011001	100011
100011	100011	011110	011001
011110	101000	101101	101101

(d) 符号化(ディジタル信号)

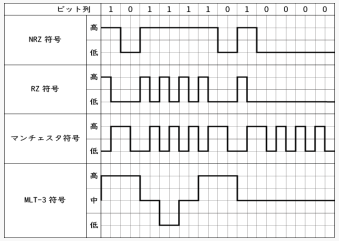
符号化

- 情報源符号化
  - 情報の冗長性（無駄や繰り返し）を取り除き伝送効率を高める。
- 通信路符号化
  - 冗長性を付け加えて信頼性を高める。
    - 誤り検出や誤り訂正のための情報を追加する。
- 伝送符号化
  - 伝送路に適した符号にする。

ベースバンド伝送とブロードバンド伝送

- ベースバンド伝送
  - ディジタル化された情報（ビット列）をそのまま電気や光のレベルの高／低に対応させて情報を伝える。
  - 有線LANや光通信で用いられる。
- ブロードバンド伝送
  - あらかじめ規則正しい信号（正弦波）を流しておき，それに変化を与えることによって情報を伝える。
  - 無線LANや携帯端末の通信で用いられる。

ベースバンド伝送の符号例



同符号連続の問題

- 同符号連続
  - 「0」が連続すること，または「1」が連続すること
  - ベースバンド伝送において望ましくない現象
  - 受信側において同期（タイミング）が取れなくなり，信号の平均的なレベルが変動し，信号を正しく判定できなくなる。
- 同符号連続への対処
  - スクランブル：一定の規則でランダム化する。
  - 符号の変換：同符号連続のない符号に変換する。

4B/5B符号

- 4ビットの情報を5ビットで表し「0」の連続を抑制
  - 100MbpsのEthernet（イーサネット）で採用されている。

4B	5B	4B	5B
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

ブロードバンド伝送

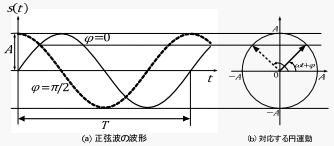
- あらかじめ規則正しい信号を流しておき，それに変化を
  与えることで情報を伝える。
- 搬送波（キャリア）
  - あらかじめ流しておく規則正しい信号（通常は正弦波）
- 変調
  - 搬送波に信号による変化を与えること。
- ブロードバンド伝送の長所
  - 信号をより遠くに伝えることが可能
  - 同じ伝送路に異なる信号を乗せることが可能（多重化）

正弦波（1）

- 通信において最も基本的で重要な波形

$$s(t) = A\sin(\omega t + \varphi) \qquad (2.1)$$

時刻　振幅　位相
角周波数（1秒間に回転する角度）



(a) 正弦波の波形　(b) 対応する円運動

正弦波（2）

- 角周波数 ω，周期 T，周波数 f の関係

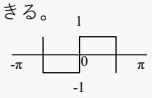
$$\omega T = 2\pi \qquad (2.2)$$
$$\omega = 2\pi/T \qquad (2.3)$$
$$\omega = 2\pi f \qquad (2.4)$$

- 周波数を用いた正弦波の表現

$$s(t) = A\sin(2\pi f t + \varphi) \qquad (2.5)$$

正弦波による波形の合成と分解

- どんなに複雑な波形も正弦波に分解できる。
- どんなに複雑な波形も正弦波で合成できる。
- 例
  - 周期2πの矩形波（四角い波形）

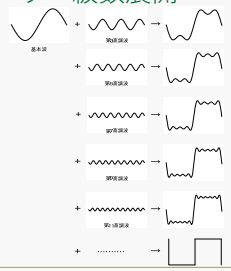


$$s(t) = \begin{cases} -1 & (-\pi \le t < 0) \\ 1 & (0 \le t < \pi) \end{cases} \quad (2.6)$$

$$s(t) = \frac{4\sin t}{\pi} + \frac{4\sin 3t}{3\pi} + \frac{4\sin 5t}{5\pi} + \cdots + \frac{4\sin(2n+1)t}{(2n+1)\pi} + \cdots \quad (2.7)$$

28

矩形波のフーリエ級数展開



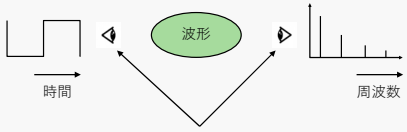
29

一般の波形の周波数成分

- 周期的でない波形についても周波数成分を求めることができる。
- フーリエ変換
  - 時間の関数として表された波形を周波数の関数に変換する。
  - 波形に含まれる周波数成分とその寄与を明らかにできる。
- 逆フーリエ変換
  - 周波数の関数を時間の関数に変換する。

30

時間軸上で見る／周波数軸上で見る



どちらも同じ現象を見ている。
見方が異なるだけ。

31

今回学んだこと

1. アナログとディジタルの意味
2. ディジタル信号の特徴
3. 信号の劣化と修復方法
4. アナログ信号をディジタル信号に変換する方法
5. ベースバンド伝送とブロードバンド伝送の意味
6. 正弦波と信号の周波数成分

32

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第3回
ディジタル通信技術（2）

今回の到達目標

1. ブロードバンド伝送とはどのようなものかを理解する。
2. アナログ変調とディジタル変調の意味を理解する。
3. ディジタル変調の具体的な方法を理解する。
4. 多重化とはどういうことかを理解する。
5. 回線交換とパケット交換とはそれぞれどのようなものかを理解する。
6. コネクション型通信とコネクションレス型通信の違いを理解する。

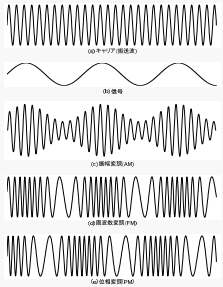
ブロードバンド伝送

- あらかじめ規則正しい信号を流しておき，それに変化を
  与えることで情報を伝える。
- 搬送波（carrier, キャリア）
  - あらかじめ流しておく規則正しい信号（通常は正弦波）
- 変調（modulation）
  - 搬送波に信号による変化を与えること。
- ブロードバンド伝送の長所
  - 信号をより遠くに伝えることが可能
  - 同じ伝送路に異なる信号を乗せることが可能（多重化）

アナログ変調

- アナログ信号で搬送波を変調すること。
- 搬送波の周波数は信号の周波数よりも高くする。
- 変調された波形は滑らかに変化する。
- 振幅変調，周波数変調，位相変調の3種類の方法がある。
  - 振幅変調　　：搬送波の振幅を変化させる。
  - 周波数変調　：搬送波の周波数を変化させる。
  - 位相変調　　：搬送波の位相を変化させる。
    - 周波数変調と位相変調をまとめて「角度変調」ともいう。

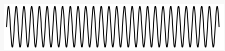
アナログ変調の例



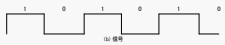
ディジタル変調

- ディジタル信号で搬送波を変調すること。
- 搬送波の周波数は信号の周波数よりも高くする。
- 変調された波形は急激に変化する。
- 振幅偏移変調（ASK），周波数偏移変調（FSK），
  位相偏移変調（PSK）の3種類の方法がある。
  - ASK　：搬送波の振幅を変化させる。
  - FSK　：搬送波の周波数を変化させる。
  - PSK　：搬送波の位相を変化させる。
- ASKとPSKが（組み合わせて）よく使われる。

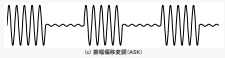
ディジタル変調の例



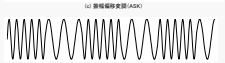
信号は「1」と「0」の繰り返し。



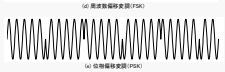
「1」で振幅そのまま
「0」で振幅小



「1」で周波数そのまま
「0」で周波数小



「1」で位相そのまま
「0」で位相を反転

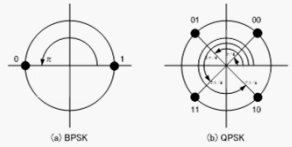


2値変調と多値変調

- 2値変調（binary modulation）
  - 「0」と「1」にそれぞれ異なる波形を対応させる。
- 多値変調（M-ary modulation）
  - 複数ビット列にそれぞれ異なる波形を対応させる。

PSKの2値変調と多値変調

- BPSK（binary PSK）
  - 「0」と「1」にそれぞれ異なる位相を対応させる。
- QPSK（Quadrature PSK）
  - 「00」「01」「11」「10」にそれぞれ異なる位相を対応させる。

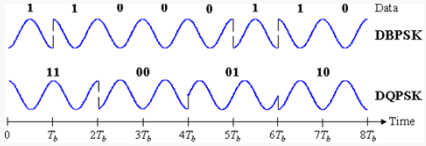


(a) BPSK　(b) QPSK

差分PSK（Differential PSK）

- 位相そのもので情報を送る場合は送信側と受信側で基準となる波形を共有する必要がある。
- 差分PSKでは位相そのものではなく，位相の変化で情報を伝える。（基準波形を共有する必要がない）
  - DBPSK（Differential PSK）
    - たとえば，「1」を送るときは位相を反転（πラジアン変化）させ，「0」を送るときは位相をそのままにする。
  - DQPSK（Differential QPSK）
    - 4種類の位相の変化で2ビットの情報を送る。

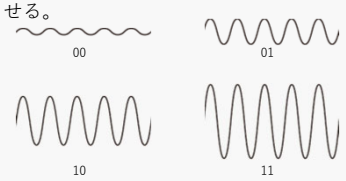
DBPSKとDQPSKの波形



出典：
https://ja.wikipedia.org/wiki/位相偏移変調#/media/ファイル:DBQPSK_timing_diag_fixed.png

ASKの多値変調

- たとえば「00」「01」「10」「11」にそれぞれ異なる振幅を
対応させる。



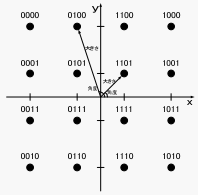
APSK

- ASKとPSKの組み合わせをAPSKという。
- 1回で送信できるビット数を増やすことができる。
  - たとえば4つの位相と4段階の振幅を組み合わせると4ビットを一挙に送ることができる。
- QAM（Quadrature Amplitude Modulation）はその一種。

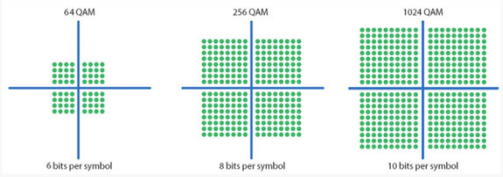
16-QAM

- 4ビットを平面上の16個の点に対応させる。
- 原点からの距離でASK，x軸正方向との角度でPSKを行う。

1回の送信で4ビットを送ることができる。



64-QAM，256-QAM，1024-QAM



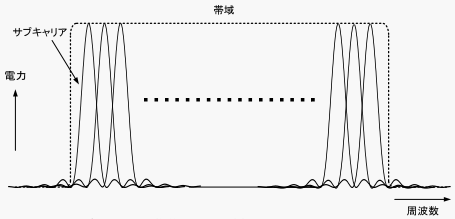
注：シンボル（symbol）とは1回に送信する情報のこと。

出典：https://www.researchgate.net/figure/64-QAM-256-QAM-and-1024-QAM-states-Source-QAM-modulator-and-demodulator-Faststream_fig1_365972263

OFDM（直交周波数分割多重）

- Orthogonal Frequency Division Multiplexingの略
- 周波数軸上に基準の整数倍の周波数をもつ搬送波（正弦波）を多数用意する。（サブキャリア）
- 上記の正弦波は互いに直交しているといい，足し合わせても元の波形に分離できる。
- 個々のサブキャリアを別々のビット列で変調し一度に多くの
  情報を転送する。
  - サブキャリアの変調にはBPSK，QPSK，QAMを用いる。

周波数軸上のサブキャリア



それぞれのサブキャリアが複数ビットの情報を運ぶ。
16-QAM: 4ビット，　64-QAM: 6ビット，　256-QAM: 8ビット，　1024-QAM: 10ビット

1次変調と2次変調

- 1次変調
  - 個々のサブキャリアを変調すること（振幅と位相を決める）。
  - BPSK, QPSK, QAM等が用いられる。
- 2次変調
  - 変調されたサブキャリアの情報をまとめてひとつの信号にすること。
  - OFDMがよく用いられる。

OFDMの変調

- 送信するビット列を分解しサブキャリアに対応させる。
- 個々のサブキャリアの情報を周波数軸上の標本点と捉える。
- 周波数軸上の標本点を時間軸上の標本点に変換する。
  - 逆離散フーリエ変換を用いる。
- 時間軸上の標本点をつないでひとつの信号とする。

OFDMの復調

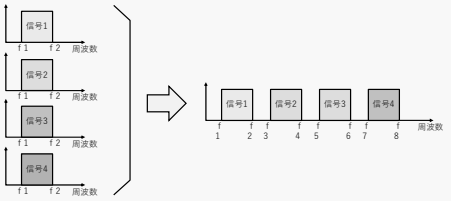
- 受信側では受信波形を標本化し，周波数軸上の標本点の情報（振幅と位相）を取り出す。
  - 離散フーリエ変換を用いる。
- 個々のサブキャリアの信号点に対応するビット列を求める。
- 信号点ごとのビット列をつないでもとのビット列を復元する。

多重化技術

- ひとつの伝送路上に複数の信号を同居させること。
- 周波数分割多重，時分割多重，符号分割多重，
  波長分割多重などの方式がある。
  - 周波数分割多重（Frequency Division Multiplexing）
  - 時分割多重（Time Division Multiplexing）
  - 符号分割多重（Code Division Multiplexing）
  - 波長分割多重（Wavelength Division Multiplexing）

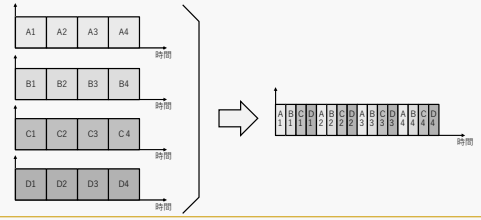
周波数分割多重（FDM）

- 周波数の異なる複数の搬送波を用意し，それぞれを独立に変調して足し合わせる。



時分割多重（TDM）

- 信号の速度を上げて時間軸上に並べる。



符号分割多重（CDM）

- それぞれの信号に特有の系列（ビット列）を与えて掛け合わせ，それらを足し合わせて送信する。
  - 掛け合わせる系列の周波数はもとの信号よりも非常に高くする。
- 受信側では個々の信号の系列を掛け合わせてもとの信号を復元する。

波長分割多重（WDM）

- 光通信で用いられる。
- 個々の信号に固有の波長を与え，足し合わせて送信する。
- 受信側では分波器を用いてそれぞれの信号を取り出す。

28

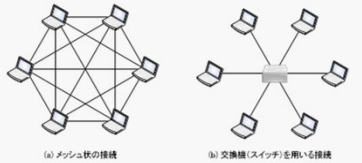
多元接続方式

- 同一のネットワークにアクセスするユーザを識別するための方式
- 周波数分割多元接続（FDMA）
  - ユーザごとに周波数を分ける。
- 時分割多元接続（TDMA）
  - ユーザごとにタイムスロットを分ける。
- 符号分割多元接続（CDMA）
  - ユーザごとに掛け合わせる系列を分ける。

29

交換の概念

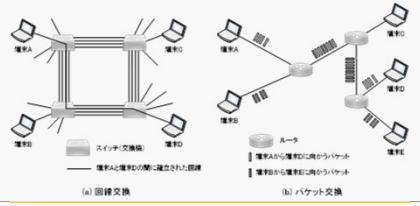
- すべての端末間に専用の伝送路を設けることは困難。
- 中央に交換機（スイッチ）をおいて端末は交換機を通じて互いに通信を行う。



30

回線交換とパケット交換

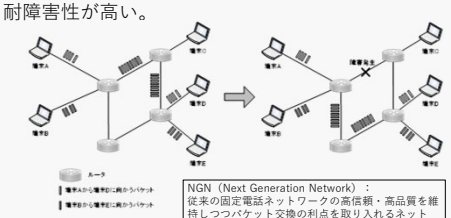
- 回線交換は伝送路を占有し，パケット交換は伝送路を共有する。



31

パケット交換の耐障害性

- パケット交換は通信中に経路を変更することが可能。耐障害性が高い。



NGN（Next Generation Network）：
従来の固定電話ネットワークの高信頼・高品質を維持しつつパケット交換の利点を取り入れるネットワーク

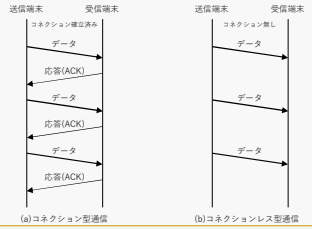
32

コネクション型通信とコネクションレス型通信

- コネクションとは端末間の論理的な接続関係。
- コネクション型通信
  - 通信に先立ち，端末間でコネクションを確立し通信中はそれを
    維持する。通信終了後に解放する。
  - 受信側はデータを受け取ると受け取り通知（ACK）を返送する。
  - 確実な通信が可能。
- コネクションレス型通信
  - コネクションを確立しない。

33

コネクション型通信とコネクションレス型通信の様子



34

今回学んだこと

1. ブロードバンド伝送とは
2. アナログ変調とディジタル変調の意味
3. ディジタル変調の具体的な方法
4. 多重化とは
5. 回線交換とパケット交換とは
6. コネクション型通信とコネクションレス型通信の違い

35

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第4回
通信プロトコル

今回の到達目標

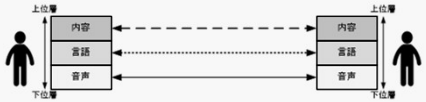
1. 通信プロトコルとはどういうものかを理解する。
2. プロトコル階層化の意味を理解する。
3. PDUとは何かを理解する。
4. プロトコル階層化の方法を理解する。
5. OSI基本参照モデルの7階層を理解する。
6. インターネットの4階層のプロトコルを理解する。
7. クライアント・サーバ型とピア・ツー・ピア型の通信形態を理解する。

プロトコル（protocol）とは

- もともとは「外交上の文書や儀礼」を表す言葉
- コンピュータ通信の世界に取り入れられて「通信を行う
  ための約束事（規則）」という意味になった。
- フォーマット（format）とプロシージャ
  （procedure）という二つの要素を持つ。
  - フォーマット
    - 情報転送単位の形式を定める規則
  - プロシージャ
    - 処理の手順を定める規則

プロトコルの例と階層化

- 対面での会話の例



「会話成立の条件」
1. 音声が伝わること
2. 同じ言語を用いていること
3. 内容に関して共通の理解を持っていること

通信プロトコルの階層化

- コンピュータ通信のプロトコルもいくつかの階層に分けられる。
  - 最下位層　：電気的・機械的につながること
  - 最上位層　：アプリケーションプログラムが互いに意思疎通できること
  - 中位層　：情報を転送できることや信頼性を確保できることなど

プロセスとプロセス間通信

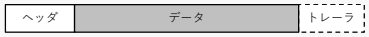
- プロセスとは
  - コンピュータ内で実際に動いているプログラムのこと
  - コンピュータ内には通常多くのプロセスが存在している。
- コンピュータ通信とは
  - 互いに離れたコンピュータ内のプロセスがネットワークを介して
    情報をやり取りすること
  - つまりプロセス間通信のことである。

PDU（Protocol Data Unit）

- PDUとは
  - コンピュータ通信における情報転送単位の総称
- 個々のプロトコルごとに固有の呼び方がある。
  以下はその例である。
  - Ethernet　：Ethernetフレーム
  - IP　：IPパケット
  - TCP　：TCPセグメント
  - UDP　：UDPデータグラム

PDUの構成

- ヘッダ（header）とデータ（data）からなる。
  末尾にトレーラ（trailer）がつくこともある。
  - データはペイロード（payload）と呼ばれることもある。
- ヘッダとトレーラ
  - 制御情報が格納される。ヘッダには宛先アドレス，
    送信元アドレスなど入る。
  - トレーラには誤り検出のための情報などが格納される。

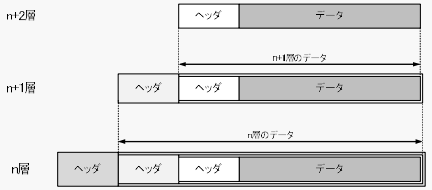


プロトコル階層化の利点

- 技術の発達に伴いプロトコルの変更を行いやすい。
  - あるプロトコルに閉じた内容は隣接する階層とのインタフェースさえ変えなければ自由に変更することができる。
  - プロトコルの実装方法を変えても他のプロトコルに影響を与えることがない。
    - あるプロトコルの処理を高速化する新しい技術が開発された場合，すぐにそれを採用することができる。

階層化の実現方法

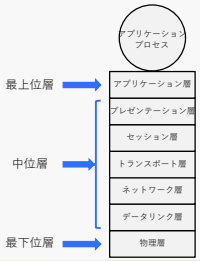
- PDUを入れ子（nest）にすることによって実現する。
  - PDUのサイズは上位層ほど小さく下位層ほど大きい。



プロトコル階層化のモデル

- OSI基本参照モデル
  - インターネット普及前に国際標準化機構が作成した。
  - 通信の機能を7階層に分けてモデル化した。
  - プロトコルそのものではなく階層化の考えを整理したモデルのひとつ。

OSI基本参照モデルの7階層



物理層（第1層）

- 電気的，光学的，機械的な接続を規定する。
  - 電気や光信号の速度
  - 信号の波形や強度
  - ケーブルやコネクタの種類や物理的形状
  - コネクタのピン配置
  - 信号の変調・復調の方法
  - 伝送符号化則

データリンク層（第2層）

- LAN（Local Area Network）のようなひとつのネットワーク内でコンピュータどうしが直接，確実な通信を行うための規則を定める。
  - 誤り検出
  - 再送（無線LANの場合）
  - 伝送媒体上の信号の衝突検出と回避

ネットワーク層（第3層）

- 異なるネットワーク間で情報（パケット）を転送する経路を定め，実際に転送を行う規則を定める。
  - ベストエフォート（best effort）による転送
    - 宛先に届ける最大限の努力はするが到達の保証はしない。
    - 何らかの原因でパケットを廃棄した時には送信元にエラーメッセージを返送する。

トランスポート層（第4層）

- 端末のプロセスどうしが確実に情報を伝え合うための処理の規則を決める。
  - PDUの破損・破棄の検出と再送
  - 受信端末でPDUを正しい順序に並べ替え
  - 受信端末の状況に応じて送信量を調整
  - ネットワークの混雑状況に応じて送信量を調整
- トランスポート層により通信の信頼性が確保される。

セッション層（第5層）

- セッションとは
  - アプリケーションのプロセスが通信を開始し終了するまでの論理的な接続関係とその期間
- セッション層はセッションの開始，終了，一時停止や再開などの規則を決める。
  - 同期点（通信を再開するポイントや半二重通信における通信方向の切り替えのポイント）を定める。

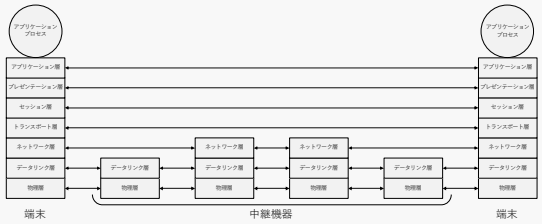
プレゼンテーション層（第6層）

- 情報の表現形式を規定する。
  - 情報を表現する符号化則
  - 文字コード（UTF-8やShift_JISなど）
  - 情報の圧縮の方法
  - 情報の暗号化の方法

アプリケーション層（第7層）

- 個々のアプリケーションプロセスに対してプロセス間通信のサービスを提供する規則を決める。
  - いろいろなアプリケーションに対してそれぞれ固有のプロトコルがある。
    - 電子メール，ファイル転送，Webサイト閲覧，遠隔コンピュータ制御など
  - アプリケーション層はアプリケーションそのものではない。
    - プロセスどうしが通信を行うための規則

OSI基本参照モデルとネットワーク装置



インターネットのプロトコル階層

ネットワークインタフェース層

- OSI基本参照モデルの物理層とデータリンク層に相当
  - 具体的なプロトコルとしてはEthernet（イーサネット）や無線LANのプロトコルなど
  - ハードウェアおよびデバイスドライバ（device driver）というソフトウェアで実現

ネットワーク層

- OSI基本参照モデルのネットワーク層に相当
  - 具体的なプロトコルとしては IP（Internet Protocol）とICMP（Internet Control Management Protocol）
    - IPにはバージョン4（IPv4）とバージョン6（IPv6）があり，ふたつの間に互換性はない。
  - コンピュータの基本ソフトウェアであるオペレーティングシステム（Windows，Linux，Android，iOSなど）の機能として実現

トランスポート層

- OSI基本参照モデルのトランスポート層に相当
  - 具体的なプロトコルはTCP（Transmission Control Protocol）またはUDP（User Datagram Protocol）
  - オペレーティングシステムの機能として実現

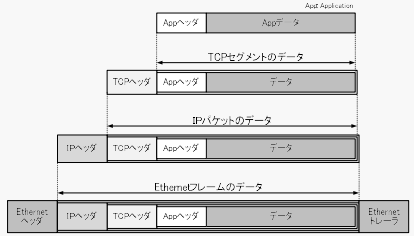
アプリケーション層

- OSI基本参照モデルのセッション層以上に相当
  - 使用されるプロトコルはアプリケーションごとに異なる。
  - アプリケーションプログラムの機能の一部として実現

プロトコル名	意味	用途
DHCP	Dynamic Host Configuration Protocol	IPアドレスその他の設定
DNS	Domain Name System	ドメイン名とIPアドレスの変換
SMTP	Simple Mail Transfer Protocol	電子メール送信
POP3	Post Office Protocol 3	電子メール受信
IMAP4	Internet Mail Access Protocol 4	電子メール受信
FTP	File Transfer Protocol	ファイル転送
HTTP	Hyper-text Transfer Protocol	Webサイト閲覧
SSH	Secure Shell	遠隔コンピュータ制御
SNMP	Simple Network Management Protocol	ネットワーク管理

28

インターネットのPDUのカプセル化



TCPはUDPになることもある。Ethernetは他のネットワークインタフェースプロトコルになることもある。

29

クライアントとサーバ

- プロトコルの上位層は下位層のサービスを利用し，下位層は上位層にサービスを提供
- 上位層をクライアント（顧客側），下位層をサーバ（奉仕側）と呼ぶ。
  - アプリケーション（クライアント）⇔TCP（サーバ）
  - TCP（クライアント）⇔IP（サーバ）
  - IP（クライアント）⇔Ethernet（サーバ）

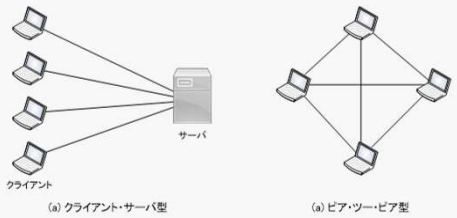
30

二つの通信形態（1）

- アプリケーションプロセスそのものもクライアントまたはサーバのいずれかの立場に分かれて通信を行うことが
  非常に多い。
- ふたつのプロセスが同格の立場で通信を行う形態もある。これをピア・ツー・ピア型という。

31

二つの通信形態（2）



32

二つの通信形態（3）

- クライアント・サーバ型の例
  - WebブラウザとWebサーバ
  - メーラとメールサーバ
- ピア・ツー・ピア型の例
  - IP電話
  - ファイル交換ソフト

33

今回学んだこと

1. 通信プロトコルとは
2. プロトコル階層化の意味
3. PDUとは
4. プロトコル階層化の方法
5. OSI基本参照モデルの7階層
6. インターネットの4階層のプロトコル
7. クライアント・サーバ型とピア・ツー・ピア型

34

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第5回
LAN(1)

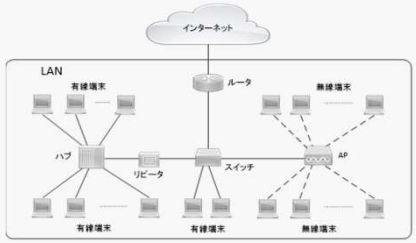
今回の到達目標

1. LANとはどのようなネットワークかを理解する。
2. 有線LANの代表的な規格であるEthernetの内容を理解する。
   1. フレーム構成
   2. アドレス解決（ARP）
   3. 媒体アクセス制御（CSMA/CD）
3. Ethernetに用いられる機器の機能を理解する。
   1. リピータ，リピータハブ
   2. ブリッジ，スイッチングハブ，スイッチ

LAN（Local Area Network）

- コンピュータネットワークの最小単位
- インターネットは世界中の無数のLANの結合体
- LANの規模はさまざま
  - ホームLAN　　：小規模
  - 大学や企業の構内LAN　：大規模
- LANの対義語はWAN（Wide Area Network）
  - 広い範囲に及ぶネットワーク
  - 狭義にはLANとLANをつなぐネットワーク

LANの構成例



LAN内の通信

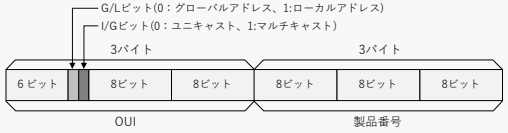
- 基本的にネットワークインタフェース層（物理層とデータリンク層）による通信が行われる。
- LAN外部（インターネットなど）との通信にはネットワーク層やトランスポート層の機能が必要になる。

MACアドレス

- MACとは
  Media Access Control（媒体アクセス制御）の略
- LANの内部で端末どうしが通信するために使われる物理アドレス
  - 機器の工場出荷時に通信インタフェース部に設定される。基本的に変更されることは無い。
  - 世界で唯一のアドレスであり，他の機器と重複することはない。

MACアドレスの構成

- 6バイトで構成される。
  - 前半3バイト（OUI）はアドレスの種類と製造メーカを表す。
  - 後半3バイトは製品番号（機種や製造番号など）を表す。



OUIは製造メーカがIEEEに申請して取得する。

10

MACアドレスの表記方法

- 1バイトを前半と後半の4ビットに分けてそれぞれを16進数で表し，6バイト分並べて表現
- バイトの区切りはコロン（:）またはハイフン（-）
- 例

00000000 00000000 01011110 00000000 01010011 00000001

↓

00:00:5E:00:53:01

- FF:FF:FF:FF:FF:FFはブロードキャストアドレス

11

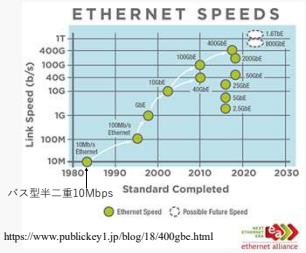
Ethernet（イーサネット）

- 世界でもっとも普及している有線LANの規格
- Ethernetのプロトコルは，ネットワークインタフェース層（OSI基本参照モデルでは物理層とデータリンク層に対応）に属する。

https://shimatake-web.com/ethernet-lan-difference/

12

Ethernetの発展



バス型からスタートし現在はスター型。時代とともに高速化が進んでいる。

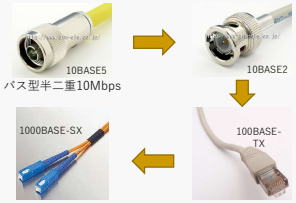
バス型半二重10Mbps

https://www.publickey1.jp/blog/18/400gbe.html

13

Ethernetの物理層

- 電気（または光）のベースバンド伝送



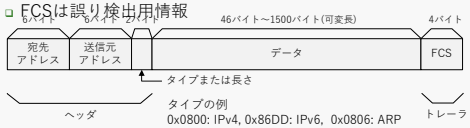
バス型半二重10Mbps

スター型全二重100Mbps

14

Ethernetの基本フレーム構成

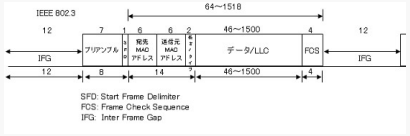
- ヘッダ（14バイト），データ（46～1500），トレーラ（4バイト）
  - 宛先／送信元アドレスはMACアドレス
  - タイプまたは長さ：1500以下は長さ，1500超はタイプ
  - FCSは誤り検出用情報



15

プリアンブル，SFD，IFG

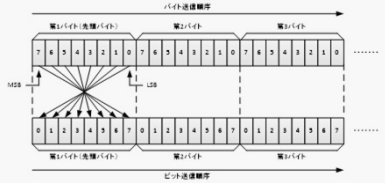
- プリアンブルとSFD
  - 受信側にフレーム到着を予告する。
    - プリアンブル：「10101010」が7バイト連続
    - SFD：「10101011」



16

Ethernetのバイト／ビット送信順序

- 先頭バイトからバイト順に送信
- バイト内はLSBからMSBに向かって送信



17

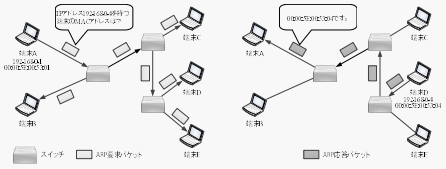
ARP（Address Resolution Protocol）

- Address Resolution（アドレス解決）とは
  宛先IPアドレスに対応するMACアドレスを取得すること。
  - IPアドレス：コンピュータのネットワークインタフェース部に
    付与される論理的なアドレス
- ARP
  - 宛先MACアドレスを取得するためのプロトコル

18

ARP要求とARP応答

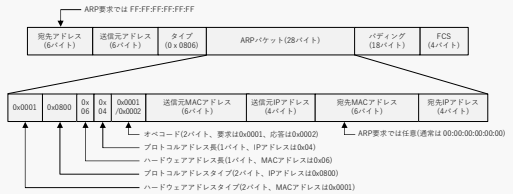
- 要求はブロードキャスト，応答はユニキャスト



19

ARPパケット

- Ethernetフレームにカプセル化される。



20

ARPテーブルの例

IPアドレス	MACアドレス
192.168.0.1	00:00:5E:00:53:04
192.168.0.4	00:00:5E:00:53:02
192.168.0.3	00:00:5E:00:53:01
192.168.0.8	00:00:5E:00:53:10
・・・・	・・・・・・
・・・・	・・・・・・
・・・・	・・・・・・
・・・・	・・・・・・
192.168.0.13	00:00:5E:00:53:26

ARPテーブルの各行は一定時間経過すると削除される（エージアウト）。

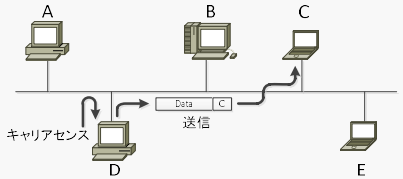
21

媒体アクセス制御（MAC）

- Media Access Control: MAC
- 伝送媒体上でフレームの衝突を検出・回避すること
- Ethernetの媒体アクセス制御はCSMA/CD（Carrier Sense Multiple Access with Collision Detection）
- Ethernetの初期（バス型ネットワーク）に開発された方式

22

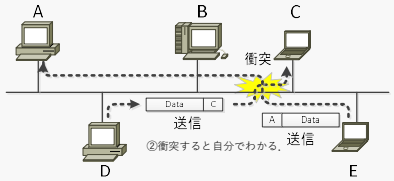
CSMA/CD（送信開始）



だれも使っていなかったら出す．

23

CSMA/CD （衝突の検出）



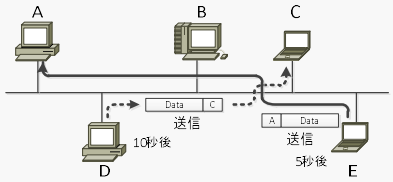
①送り出すとともに自分の信号をモニターする．

②衝突すると自分でわかる．

③衝突が分かったら皆に知らせる．（Jam信号）

24

CSMA/CD （再送信）

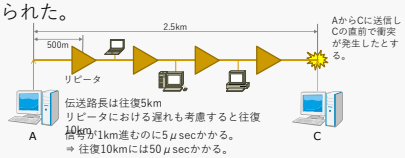


衝突したらランダムな時間待って再送信する．

25

Ethernetの最短フレーム

- Ethernetの最短フレーム64バイトはCSMA/CDから決められた。



伝送路長は往復5km
リピータにおける遅れも考慮すると往復10kmか？
信号が1km進むのに5μsecかかる。
⇒ 往復10kmには50μsecかかる。

伝送速度は10Mbps ⇒ 1ビット送るのに0.1μsecかかる。
50μsec以内に送信が終わってしまってはいけない。

ビット数に換算すると50/0.1＝500ビット ⇒ 512ビットとする．
⇒ 512ビット＝64バイト

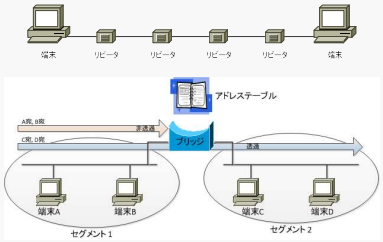
26

Ethernetに用いられる機器

- リピータ　　：中継装置（物理層）
- ブリッジ　　：セグメント間の中継装置
  - 物理層とデータリンク層の機能を持つ。
  - アドレス学習機能を持ち余計なフレームを流さない。
- ハブ　　：集線装置
  - リピータハブ（物理層）
    - 受信フレームを他のすべてのポートから送信（フラッディング）
  - スイッチングハブ（物理層とデータリンク層）
    - アドレス学習機能を持ち宛先につながるポートから送信
- スイッチ　　：高機能なスイッチングハブ

27

リピータとブリッジの動作



28

MACアドレスの学習

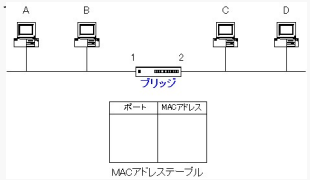
- ブリッジやスイッチングHUBはEthernetヘッダを解釈して，自分のどのポートの先にどのコンピュータが接続
  されているか，を学習していく。
- 学習した結果はアドレステーブルに記録する。
  - ただし，一定時間経過すると削除する（エージアウト）

ポート	MACアドレス
1	04-A3-43-5F-43-23
2	04-A3-43-5F-12-34
3	04-A3-43-5F-56-78
・・・	・・・

29

アドレス学習のプロセス(1)

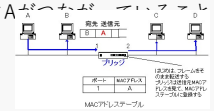
- ブリッジの電源を入れた時はMACアドレステーブルには
  何も入っ



30

アドレス学習のプロセス(2)

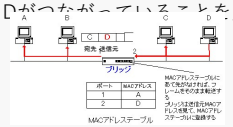
- AからB宛のフレームが送信されるとブリッジは
  それを他のセグメントにも流す
  - なぜならアドレステーブルには何も書かれていないから。
    これをフラッディング（Flooding）という。
- ブリッジはそのフレームの送信元アドレスからポート1に
  コンピュータAがつなが っていることを覚える。



31

アドレス学習のプロセス(3)

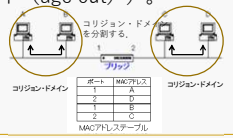
- DからC宛のフレームが送信されるとブリッジは
  それを他のセグメントにも流す。
  - なぜならアドレステーブルにCのアドレスがないから。
- ブリッジはそのフレームの送信元アドレスからポート2に
  コンピュータDがつながっていることを覚える.



32

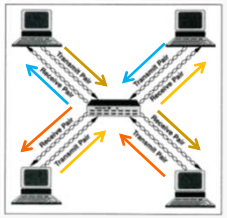
アドレス学習のプロセス(4)

- 同様の学習を行うことで以下のテーブルが完成。
- セグメント内の通信は他のセグメントに流さない。
- ブリッジの電源を切るとテーブルの中味は消える。
- 一定時間通信が無いと学習した情報を削除する
  （エージアウト（age out））。



33

スイッチングHUBの全二重通信（Full Duplex）



それぞれの信号線はスイッチングHUBでドメインが分離される。
→衝突が発生しない。

送信用信号線と受信用信号線が別。

送信しつつ受信ができる。
→全二重通信

スイッチングHUBはすべてのポートをPoint-to-Pointで同時並行的に動作させられる点がポイント

34

今回学んだこと

1. LANとはどのようなネットワークか
2. 有線LANの代表的な規格であるEthernet
   1. フレーム構成
   2. アドレス解決（ARP）
   3. 媒体アクセス制御（CSMA/CD）
3. Ethernetに用いられる機器の機能
   1. リピータ，リピータハブ
   2. ブリッジ，スイッチングハブ，スイッチ

35

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

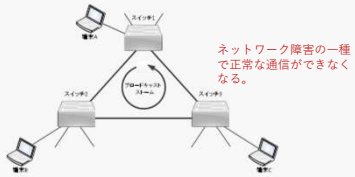
第6回
LAN(2)

今回の到達目標

1. ブロードキャストストームとはどのような現象か理解する。
2. スパニングツリープロトコルの目的と機能を理解する。
3. リンクアグリゲーションの目的と機能を理解する。
4. VLANとはどのようなものかを理解する。
5. 無線LANの規格と通信方法を理解する。
6. PANとはどのようなネットワークかを理解する。

ブロードキャストストーム

- LAN内にループ（閉路）ができるとブロードキャストフレームが増殖しつつ循環する現象



スパニングツリープロトコル（STP）

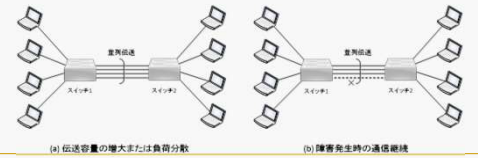
- Spanning Tree Protocol: STP
- LAN内のループ形成を防ぐためのプロトコル
  - ループを形成せずにすべての端末をつなぐ経路（ツリー）を構成する。
    - STPはスイッチやスイッチングハブにインストールされる。
    - 機器どうしで制御フレーム（Bridge Protocol Data Unit: BPDU）を交換
    - 中心となる機器（ルートブリッジ）を選挙で選出し，そこから枝を伸ばしていく。（span: 段々に進む）
    - ネットワークに変化があればツリーを再構成する。

STPの動作

STPの動作を高速化したRSTP（Rapid STP）が広く使われている。

リンクアグリゲーション

- Link Aggregation
- スイッチ間を複数の伝送路で接続する手法
  - 伝送容量の拡大，負荷分散，信頼性向上を図る。
  - 手動または自動（LACP）で設定される。

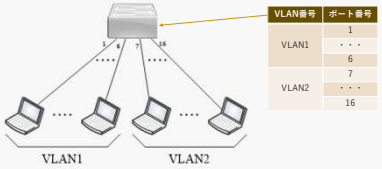


VLAN

- Virtual LAN（仮想LAN）
  - LANの内部を複数の仮想的なLANに分割する技術
- VLANの利点
  - 柔軟なネットワーク構成（ソフトウェアによる設定）
    - 機器の物理的な配置や配線の変更が不要
  - 通信の効率向上
    - ブロードキャストの範囲が個々のVLAN内に制限される。
  - セキュリティの向上
    - 通信が個々のVLAN内に閉じる。

ポートベースVLAN

- スイッチの各ポートにVLAN番号を設定する。
  - ポートに到着するフレームをそのVLANに所属すると認識する。

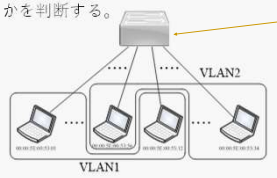


VLAN番号	ポート番号
VLAN1	1
	・・・
	6
VLAN2	7
	・・・
	16

(a) ポートベースVLAN

MACベースVLAN

- MACアドレスとVLANの対応関係を記憶させる。
  - 受信するフレームの送信元MACアドレスからどのVLANに属するかを判断する。

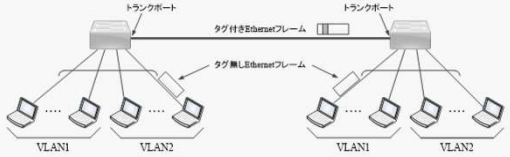


VLAN番号	MACアドレス
VLAN1	00:00:5E:00:53:01
	00:00:5E:00:53:12
VLAN2	00:00:5E:00:53:56
	00:00:5E:00:53:34

(b) MACベースVLAN

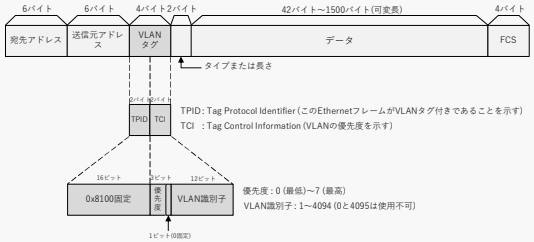
タグVLAN

- フレーム内にVLANタグのフィールドを追加し，所属するVLANの番号を明示的に表す。
  - タグはスイッチ間のフレーム転送時に挿入・削除される。



(c) タグVLAN

VLANタグ付きEthernetフレーム



無線LAN

- IEEE802.11として標準化され複数の規格を含む。

規格	IEEE802.11a	IEEE802.11b	IEEE802.11g	IEEE802.11n	IEEE802.11ac	IEEE802.11ax
周波数帯	5GHz帯	2.4GHz帯	2.4GHz帯	2.4G/5GHz帯	5GHz帯	2.4G/5G/6GHz帯
最大速度	54Mbps	11Mbps	54Mbps	600Mbps	6.933Gbps	9.6Gbps
チャネル幅*	20MHz	22MHz	20MHz	20, 40MHz	20, 40, 80, 160MHz	20, 40, 80, 160MHz
1次変調方式	BPSK, QPSK, 16-QAM, 64-QAM	DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
2次変調方式	OFDM	DSSS**	OFDM	OFDM	OFDM	OFDMA***
互換性	11n/ac/ax と互換	11g/n/ax と互換	11b/n/ax と互換	11a/b/g/ac/ax と互換	11a/n/ax と互換	11a/b/g/n/ac と互換

* チャネル幅：ひとつの通信に使用する帯域幅　** DSSS：Direct Sequence Spread Spectrum（直接拡散方式）
*** OFDMA：OFDMを利用する多元接続。複数のユーザがサブキャリアを共有する。

互換性とは，同じ周波数帯では互いに通信が可能であることを意味し，通信速度は低い方に合わせられる。

ISM帯

- Industrial, Scientific, Medical band
- 一定出力以下であれば許可なしに用いてもよい周波数帯
  - 無線LANの周波数帯として使われる。
  - ISM帯の電波は他の機器（たとえば電子レンジなど）からも発せられるので，使用にあたっては干渉への注意が必要。

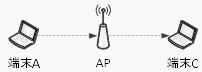
Wi-Fi（ワイファイ）

- Wi-Fiとは無線LANに関する登録商標。
- 業界団体Wi-Fi Alliance（ワイファイ アライアンス）の相互接続試験で認定された機器はWi-Fiのロゴマークを使用することができる。
- IEEE802.11n，IEEE802.11ac，IEEE802.11axはそれぞれWi-Fi4，Wi-Fi5，Wi-Fi6とも呼ばれる。

Wi-Fiのロゴマーク

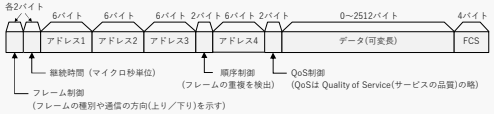
無線LANの通信の特徴

- 端末はアクセスポイント（AP）を介して他の端末と通信を行う。端末はAPへの登録が必要。
  - APもMACアドレスを有する。
- 半二重通信（空間という媒体を共有）
  - 媒体アクセス制御はCSMA/CAによって行う。
- 正常受信時には確認応答（ACK）を返送する。
- 通常は有線LAN（Ethernet）に接続される。

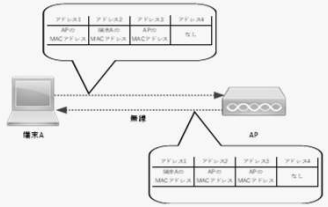


無線LANのフレーム

- 無線環境への対応や有線ネットワークへの接続などのためにEthernetよりも複雑。
  - 管理フレーム，制御フレーム，データフレームの3種類のフレームがある。

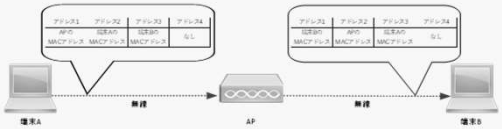


アドレスフィールドの使い方（1）



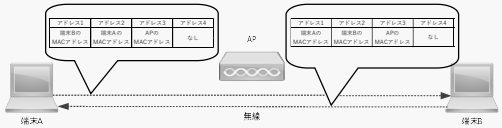
(a) 無線端末とAPが管理／制御フレームを送受信する場合

アドレスフィールドの使い方（2）



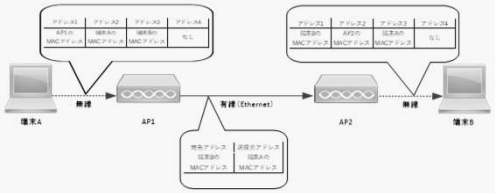
(b) 無線端末どうしがAPを介して通信する場合

アドレスフィールドの使い方（3）



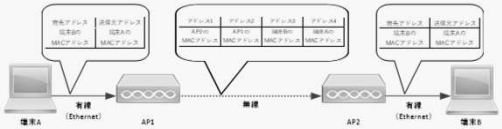
(c) 無線端末どうしがAPを介さずに直接通信する場合

アドレスフィールドの使い方（4）



(a) AP間が有線（Ethernet）で接続される場合

アドレスフィールドの使い方（5）



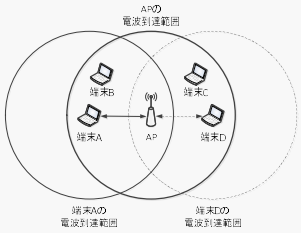
(b) AP間が無線で接続される場合

CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance
- 無線LANにおける媒体アクセス制御
  - 他の通信が行われている時は送信しない。
  - 他の通信が終わった後，ランダムな時間待って送信を始める。
  - 送り始めたフレームは最後まで送り切ってしまう。
  - 衝突の検出は行わない。
  - 正常に受信した端末またはAPはACKを返送する。

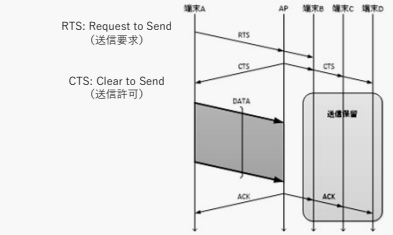
隠れ端末問題

端末どうしが相手の存在に気づかず，同時に通信を
始めてAPでフレームの
衝突が発生する問題



(a) 隠れ端末問題

制御フレームによる回避策



(b) RTS, CTSによる衝突回避

PAN

- Personal Area Network
- おもに個人が利用する機器どうしを接続しデータを送受信するための小規模なネットワーク
- LANとは目的や性格が異なる。
- 通常，無線通信を利用する。
  - WPAN（Wireless PAN）
- 無線通信技術としてBluetoothとZigBeeがある。

Bluetooth（1）

- 短距離，低消費電力，低コスト，低速の無線通信規格
- APのようなインフラを必要としない。
- おもにディジタル機器どうしの接続に利用される。
  - PCとマウス，キーボード，スピーカ，マイク，ヘッドセットなどの
    周辺機器との接続
- IEEE802.15.1で標準化され，周波数は2.4GHz帯を使用。

Bluetooth（2）

- 通信速度は3Mbps未満，到達距離は10m未満が基本
  - Bluetooth3.0　：24Mbpsの速度が可能
  - Bluetooth4.0　：速度を1Mbpsに抑えて低消費電力化
  - Bluetooth5.0　：速度2Mbps
  - Bluetooth5.3　：最新版（2022年時点）

ZigBee（1）

- Bluetoothよりもさらに低消費電力，低速度，低頻度の無線通信規格
- ミツバチ（Bee）がジグザグに飛び回る様子に由来
- ZigBeeの物理層とMAC層はIEEE802.15.4で標準化
- 上位層のプロトコルは業界団体のZigBeeアライアンスが仕様を策定

ZigBee（2）

- スリープ時の消費電力がBluetoothよりも小さい。
- スリープからの復帰時間が短い。
- センサネットワークのようにノード数が多くスリープ時間が長くかつ送信データが少ない利用シーンに適している。

今回学んだこと

1. ブロードキャストストームとは
2. スパニングツリープロトコルの目的と機能
3. リンクアグリゲーションの目的と機能
4. VLANとは
5. 無線LANの規格と通信方法
6. PANとは

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第7回
IPとルーティング(1)

今回の到達目標

1. IPの役割を理解する。
2. IPアドレスの必要性を理解する。
3. IPアドレスの構成と表記方法を理解する。
4. IPv4アドレスの枯渇問題とその対策を理解する。
5. IPv4パケットの構成を理解する。
6. IPv6パケットの構成を理解する。

IP（Internet Protocol）

- ネットワーク層に属するプロトコル
- 役割は送信元の端末から宛先の端末までパケットを送り届けること
  - 途中には異なるネットワークが存在する。
- バージョン4とバージョン6の2種類があり，それぞれIPv4，IPv6と呼ばれる。
  - 両者に互換性はない。

IP アドレス

- ネットワークインタフェースに与えられる論理的識別子
  - MACアドレスは物理的識別子
- 複数のIPアドレスを有するコンピュータもある。
  - 複数インタフェースを持つコンピュータ，中継装置（ルータ），
    仮想コンピュータ
- IPv4アドレス　　：4バイト（32ビット）の数値
- IPv6アドレス　　：16バイト（128ビット）の数値

IPアドレスの必要性

- インターネット上のすべてのコンピュータのインタフェースを一意に識別するため。
- MACアドレスは識別子として使えない。
  - 物理アドレスと論理アドレスは異なる。
  - MACアドレスでは情報の転送が不可能。
    - 機器は世界のどこに持ち出されるかわからない。
    - 機器の交換や廃棄も頻繁に行われる。
    - それをひとつひとつ追跡することは不可能。
- IPアドレスは体系的に配布される。
  - 世界（ICANN）→地域（RIR）→国（NIR）→ISP→組織または個人

IPアドレスの配布

- IPアドレスは体系的に配布される。
  - 世界（ICANN）→地域（RIR）→国（NIR）→ISP→組織または個人
- 連続するアドレスの束を小分けにして配っていく。
- ルータ（中継装置）はIPアドレスを見ることによって宛先がおよそどこにあるかがわかり，その方向にパケットを転送
  する。
  - 道路標識と同じ（〇〇方面は直進。△△方面は右）

IPv4アドレスの表記方法

- ドット付き10進表記
  - 4バイトを1バイトごとに区切ってそれぞれを10進数で表し，ドット（ピリオド）記号でつないで表現
  - 例

11001011 00000000 01110001 00000001

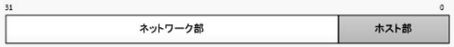
↓

203.0.113.1

10

IPv4アドレスの構成

- ネットワーク部（前半）とホスト部（後半）に分かれる。
  - ネットワーク部　：端末が所属するネットワークを示す。
  - ホスト部　　：どの端末（インタフェース）かを示す。



11

クラスフルアドレス

クラス	ネットワーク数*	ホスト数
A	126 $(=2^7-2)$	16,777,214 $(=2^{24}-2)$
B	16,382 $(=2^{14}-2)$	65,534 $(=2^{16}-2)$
C	2,097,150 $(=2^{21}-2)$	254 $(=2^8-2)$

*ネットワークアドレスの最大値と最小値は予約されており使用できない。

12

特殊なIPアドレス

- ネットワークアドレス
  - ホスト部をすべて「0」にしたアドレス
  - ネットワーク自身を表し，個別の端末には割り当てられない。
- （ダイレクト）ブロードキャストアドレス
  - ホスト部をすべて「1」にしたアドレス
  - ネットワークを指定してそこへブロードキャストする時に用いる。
  - 個別の端末には割り当てられない。
  - ルータは通常転送しない。
- （ローカル）ブロードキャストアドレス
  - 「255.255.255.255」
  - 端末が所属するネットワークにブロードキャストする時に用いる。

13

IPv4アドレスの枯渇問題

- IPv4のアドレスが不足し，新規に割り当てられなくなる問題
  - 32ビットで表現できる数値は約43億（$= 2^{32}$）
  - 地球の人口は80億人超（2022年時点）
    - 個人は複数のPCやスマートフォンを持ち，すべてのモノがインターネットにつながるIoT（Internet of Things）の時代
- クラスフルアドレスの構造的な問題が原因
  - クラスAのネットワークは大きすぎクラスCは小さすぎる。

14

CIDR

- Classless Inter-Domain Routing（サイダー）
- IPv4アドレスを配布・指定する際にネットワーク部とホスト部の境界を指定
  - 境界を自由に設定することにより，IPアドレスを柔軟に割り当てる。
    - プレフィックス（prefix）：CIDRのアドレスのネットワーク部
      - ドット付き10進表記では最後に「/」（スラッシュ）を付けて表示
    - 例

203.0.113.0/26

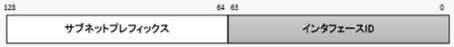
先頭から26ビットがネットワーク部，残り6ビットがホスト部。62台の端末を収容できる。

    - プレフィックスのビットを「1」，ホスト部のビットを「0」としてドット付き10進表記で表したものをサブネットマスクという。

15

IPv6アドレスの構成

- 2^{128}個のアドレスを表すことができる。
  - サブネットプレフィックス：ネットワーク部に相当
    - プレフィックス長は通常64ビット
  - インタフェースID：ホスト部に相当



16

IPv6アドレスの表記方法

- コロン付き16進表記
  - 16バイトを2バイトごとに区切って，それぞれを4桁の16進数で
    表し，「:」（コロン）でつないで表現
  - すべて「0」となるフィールドの連続は「::」と表記
    - ただし，1回しか使えない。
  - 例 00100000 00000001 00001101 10111000 00000000 ⋯⋯ 00000000 00000001

11バイト「0」が連続

↓

2001:0db8::0001 または 2001:db8::1

17

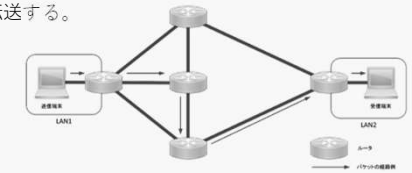
IPアドレスの設定方法

- IPv4アドレスの設定
  - 手動設定（固定）
  - DHCPサーバからの自動設定
    - DHCP: Dynamic Host Configuration Protocol
- IPv6アドレスの設定
  - NDP（Neighbor Discovery Protocol）による自動設定
    - 同じネットワーク内のルータからサブネットプレフィックスを取得し，
      インタフェースIDにMACアドレスを含める。
  - DHCPサーバからの自動設定

18

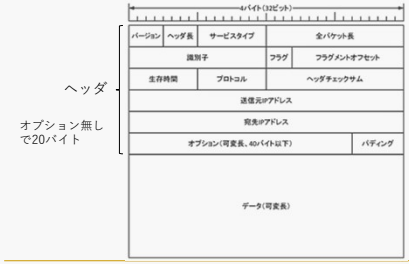
IP ネットワークの構成

- ルータが到着したパケットの宛先アドレスを見て次々の
転送する。



19

IPv4パケットの構成



20

サービスタイプ

- 優先度など関する情報を格納
- DSCP（DiffServ Code Point）：先頭6ビットで定義
  - 前半3ビット：優先度
  - 後半3ビット：破棄レベル

ビット	内容	使用方法
1～3	優先度	デフォルトは0で値が大きいほど高優先
4～6	破棄レベル	デフォルトは0で値が大きいほど破棄されやすい。
7, 8	輻輳通知	ネットワークの混雑を受信端末に通知

21

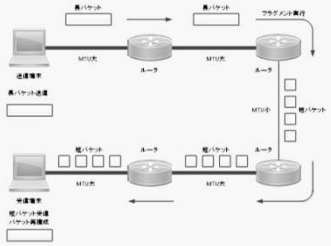
MTUとフラグメント

- MTU（Maximum Transmission Unit）
  - データリンク層が運べるデータの最大長
    - Ethernetでは1500バイト
- フラグメント
  - MTUの小さな部分を通過する時にパケットを小さなサイズに
分割すること。
    - 分割されたパケットの識別子は共通。フラグ（下記）でフラグメントの
状況を示し，フラグメントオフセットで位置を示す。

値	意味
000	フラグメントオフセットで位置を示すパケット
001	フラグメントされた最初のパケット，または途中のパケット
010	フラグメント禁止

22

フラグメントの様子



23

TTL，プロトコル，ヘッダチェックサム

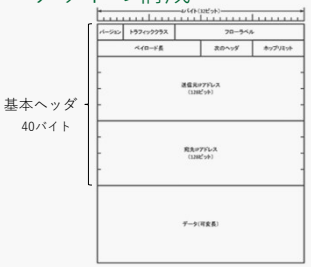
- 生存時間（TTL）
  - 送信端末で非零の初期値を格納され，ルータを経由するたびに
1ずつ減算
- プロトコル
  - データの中身をしめす。

番号	略称	プロトコル名
1	ICMP	Internet Control Message Protocol
6	TCP	Transmission Control Protocol
17	UDP	User Datagram Protocol
89	OSPF	Open Shortest Path First
番号は10進表記		

- ヘッダチェックサム
  - ヘッダの誤り検出用情報

24

IPv6パケットの構成



25

各フィールドの内容

- トラフィッククラス
  - IPv4のサービスタイプに相当（DSCPが入る）。
- フローラベル
  - フローとは端末間をある関係を持って流れる一連のパケット。
フローに対してルータで特別な処理を行う場合に個々の情報を使う。
- ペイロード長
  - 基本ヘッダを除くパケットの長さ（拡張ヘッダを含む）
- 次のヘッダ
  - 拡張ヘッダがある場合にその種別を示す。
- ホップリミット：IPv4の生存時間（TTL）に相当

26

グローバルアドレスとプライベートアドレス

- グローバルアドレス
  - ICANNを頂点として，体系的に配布されるIPアドレス
  - インターネット通信には必要不可欠
- プライベートアドレス
  - ある組織のネットワーク（たとえばLAN）の内部で自由に
使用できるIPアドレス

クラス	アドレスの範囲	基本プレフィックス長
A	10.0.0.0～10.255.255.255	8ビット
B	172.16.0.0～172.31.255.255	12ビット
C	192.168.0.0～192.168.255.255	16ビット

27

NATとNAPT

- NAT（Network Address Translation）
  - プライベートアドレスとグローバルアドレスの相互変換
    - ひとつのグローバルアドレスを複数のプライベートアドレスが共有する。
    - 1:1変換であるためひとつのグローバルアドレスを同時には共有できない。
- NAPT（Network Address Port Translation）
  - プライベートアドレスとグローバルアドレスの相互変換
    - ひとつのグローバルアドレスを複数のプライベートアドレスが同時に
      共有できる。「IPマスカレード」ともいう。
    - トランスポート層の識別番号でセッションを区別する。

28

NAT/NAPTとIPアドレス枯渇問題

- NATやNAPTによりグローバルアドレスを節約して使用できる。
- IPアドレス枯渇問題を緩和できる。

29

IPv4とIPv6

- 現在はIPv4からIPv6への移行期だが，その進展はゆるやか
- 互換性がないことおよびユーザにとってメリットのないことが原因
- IPv4ネットワークとIPv6の接続
  - カプセル化を行う。
    - IPv6 over IPv4：IPv6をIPv4パケットの中にカプセル化
    - IPv4 over IPv6：IPv4をIPv6パケットの中にカプセル化

30

今回学んだこと

1. IPの役割
2. IPアドレスの必要性
3. IPアドレスの構成と表記方法
4. IPv4アドレスの枯渇問題とその対策
5. IPv4パケットの構成
6. IPv6パケットの構成

31

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

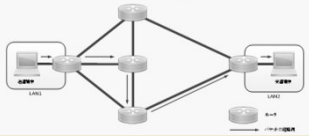
第8回
IPとルーティング(2)

今回の到達目標

1. ルーティングとはどのようなことかを理解する。
2. ルーティングテーブルにはどのような情報が含まれるかを理解する。
3. ASとはどのようなネットワークか理解する。
4. 代表的なルーティングプロトコルの動作を理解する。
5. SDN，MPLSとはどのような技術か理解する。
6. ICMPの働きを理解する。

ルーティング

- ルーティング（routing）とはIPパケットの経路を決定すること
- 経路に沿って実際にパケットを転送することはフォワーディング（forwarding）と呼ぶ。



ルーティングテーブル

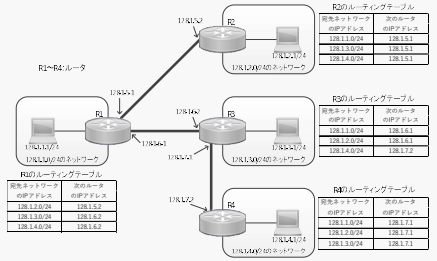
- 宛先ネットワークと次に転送するルータのIPアドレスの
  一覧表
- 各ルータが保持している。
- 例

宛先ネットワークのIPアドレス	次のルータのIPアドレス
128.1.2.0/24	128.1.5.2
128.1.3.0/24	128.1.6.2
128.1.4.0/24	128.1.6.2

ルーティングの方法

- 静的ルーティング（静的経路制御）
  - 手動で経路情報を設定する。
- 動的ルーティング（動的経路制御）
  - 自動で経路情報が設定される。
  - ルータどうしが経路情報を交換しルーティングテーブルを作成する。
  - 経路情報の交換はルーティングプロトコルによって行われる。

ルーティングテーブルの例



AS（Autonomous System）

- 自律システム
- ひとつの管理規則にしたがって管理されるネットワーク
- ISP，通信事業者，大企業などがASを所有
  - ASの内部には複数のルータが存在
- AS番号が割り当てられている。
  - 16ビットまたは32ビットの識別番号
  - ICANNを頂点として体系的に付与

10

IGPとEGP

- IGP（Interior Gateway Protocol）
  - AS内部の経路制御に使用されるルーティングプロトコルの総称
  - 効率を優先したルーティングを行う。
    - 最短経路，最小コストなど
  - 具体的なプロトコルとしてはRIP，OSPFなど
- EGP（Exterior Gateway Protocol）
  - AS間の経路制御に使用されるルーティングプロトコルの総称
  - 政策的な判断を加えてルーティングを行う。
  - 具体的なプロトコルとしてはBGP

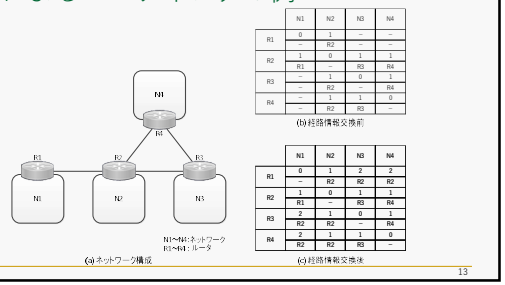
11

RIP（Routing Information Protocol）

- 小規模なネットワークで使用されるIGP
- アルゴリズムが単純で実装しやすいが，収束が遅い。
- アルゴリズムは距離ベクトル型（distance vector）
  - 各ルータは他のすべてのルータとの距離（ホップ数）を隣接ルータに通知する。
    - RIPのホップ数の最大値は15
    - 初期のRIPは可変長のサブネットマスク（Variable Length Subnet Mask: VLSM）を扱うことができなかったが，改訂後のRIP2は扱うことができる。

12

RIPによるルーティングの例



(b) 経路情報交換前

	N1	N2	N3	N4
R1	0	1	–	–
	–	R2	–	–
R2	1	0	1	1
	R1	–	R3	R4
R3	–	1	0	1
	–	R2	–	R4
R4	–	1	1	0
	–	R2	R3	–

(c) 経路情報交換後

	N1	N2	N3	N4
R1	0	1	2	2
	–	R2	R2	R2
R2	1	0	1	1
	R1	–	R3	R4
R3	2	1	0	1
	R2	R2	–	R4
R4	2	1	1	0
	R2	R2	R3	–

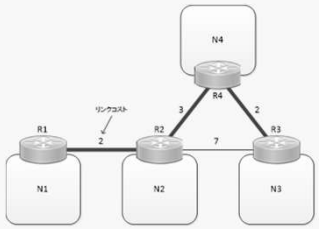
13

OSPF（Open Shortest Path First）

- 広く使われているIGP
- RIPよりもアルゴリズムが複雑であるが，収束が速い。
- 情報交換のアルゴリズムはリンクステート型
  - リンク（隣接ルータ間の伝送路）にコストを付与
  - 各ルータは隣接ルータとの接続情報をネットワーク内のすべてのルータに通知（全ルータが接続情報を共有）
- 経路決定のアルゴリズムはダイクストラのアルゴリズム

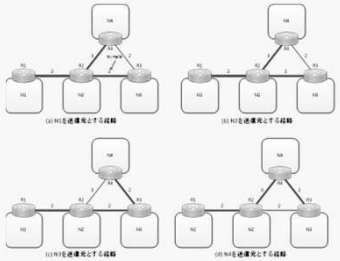
14

OSPFによるルーティングの例（1）



15

OSPFによるルーティングの例（2）



16

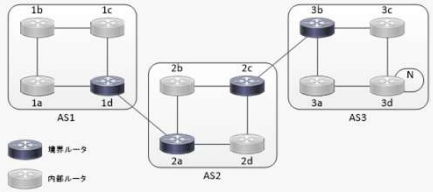
BGP（Border Gateway Protocol）

- 実質的に唯一のEGP
- アルゴリズムはパスベクトル型
  - 途中につながるAS情報を串刺しにして伝えていく。
- 現在のバージョンは4（BGP4）
- TCPコネクション上でメッセージを交換（信頼性重視）
- パス属性により政策的経路制御を実現する。

17

BGPによるルーティングの例（1）

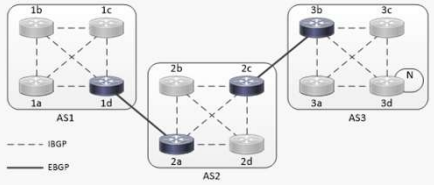
- 3つのASが接続されているとする。



18

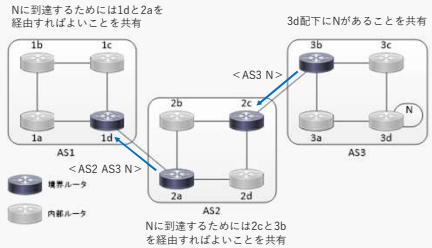
BGPによるルーティングの例（2）

- IBGP（BGP内コネクション）はメッシュ型



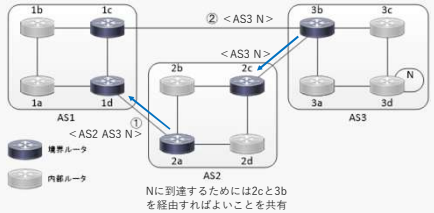
19

BGPによるルーティングの例（3）



20

BGPによるルーティングの例（4）



21

パス属性

- 経路決定に政策を反映させるための情報
- 経路ごとのBGPメッセージに含まれる。
- 特に重要なパス属性
  - NEXT_HOP
    - つぎのASの境界ルータのIPアドレス
  - AS_PATH
    - 宛先ネットワークに至るAS番号の列
  - LOCAL_PREF（Local Preference）
    - ASの管理者が境界ルータに設定する非負の整数値
    - 値が大きいほどその経路が選ばれ易い。

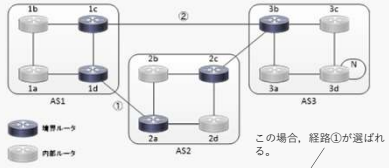
22

パス属性の優先度

- LOCAL_PREFが最も大きな経路
- LOCAL_PREFが同じであればASパス長の短い経路
- ASパス長も同じであればそのASから最短で抜け出せる経路（ホットポテトルーティング）

23

BGPによるルーティングの例（5）



経路	宛先	NEXT_HOP	AS_PATH	LOCAL_PREF
①	N	2a	AS2 AS3	300
②	N	3b	AS3	100

(注) Nはネットワークアドレス，2a, 3bは左隣インタフェースのIPアドレス

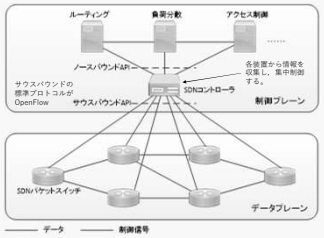
24

SDN（Software Defined Network）

- 従来のルーティングは分散制御
  - 各装置への初期設定や設定変更などに手間がかかる。
- SDNは集中制御
  - 1か所に制御装置（SDNコントローラ）を置き，各装置やパケットの情報を集め，制御装置のソフトウェアが全装置を集中的に制御する方式
  - ネットワーク上のデータ信号の流れ（データプレーン）と制御信号の流れ（制御プレーン）が論理的に分離される。
  - 管理上のコストを削減し，ネットワークの状況やネットワークの変更・拡張に応じてより柔軟に経路制御を行うことができる。

25

SDNによるネットワークの例



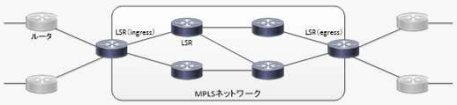
26

MPLS（Multi-Protocol Label Switching）

- パケット転送の高速化とともに柔軟な経路制御を行うために用いられるプロトコル
- MPLSのネットワークでは入り口（ingress）でIPパケットの先頭にラベル（label）という情報（一種のヘッダ）を付加
- ネットワーク内ではMPLSルータ（Label Switching Router: LSR）がラベルのみを見てハードウェアによる高速転送を行う。

27

MPLSネットワークの例



- MPLSネットワーク内はハードウェアによる高速転送
- ラベル付与の方法によって経路を柔軟に制御することが可能（トラフィックエンジニアリング）

28

ICMP（Internet Control Message Protocol）

- IP通信の制御や通信状態の調査などを行なうためのプロトコル
- IP層に属する（IPパケットにカプセル化）
- 送信元へのエラー通知やコマンドによるネットワークの
  調査に利用される。
  - 宛先到達不能
  - 生存時間超過
  - コマンドによる宛先への到達確認：「pingコマンド」

29

ICMPv4のメッセージ

タイプ（10進）	メッセージ	内容
0	Echo Reply	Echo Requestメッセージが到着したことを送信元に知らせる。
3	Destination Unreachable	パケットが宛先に到達できないことを送信元に知らせる。
4	Source Quench	送信元に送信の中断または送信速度の低減を要求する。
5	Redirect	送信元にパケットのルート変更を要求する。
8	Echo Request	宛先にエコーメッセージへの応答を要求する。
11	Time Exceeded	パケットのTTLが0になり破棄されたことを送信元に伝える。
12	Parameter Problem	IPパケットのパラメータに異常が検出されたことを送信元に知らせる。
13	Timestamp Request	宛先端末の現在時刻を要求する。
14	Timestamp Reply	Timestamp Requestメッセージの受信時刻と返信時刻を知らせる。
17	Address Mask Request	サブネットマスクを要求する。（端末から同一ネットワークのルータに送信する）
18	Address Mask Reply	サブネットマスクを応答する。

30

今回学んだこと

1. ルーティングとは
2. ルーティングテーブルに含まれる情報
3. ASとは
4. 代表的なルーティングプロトコルの動作
5. SDN，MPLSとは
6. ICMPの働き

31

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第9回
TCPとUDP（1）

今回の到達目標

1. ポート番号とは何かを理解する。
2. ソケットとは何かを理解する。
3. TCPの役割を理解する。
4. TCPセグメントの構成を理解する。
5. コネクション確立と解放の手順を理解する。
6. 再送制御とはどのようなことか理解する。
7. 順序制御とはどのようなことか理解する。
8. 再送タイマーの設定方法を理解する。
9. アプリケーションとTCPの関係を理解する。

プロセスとポート番号

- プロセスとはコンピュータ内で実行されているプログラム
  - 通常，多数のプロセスが活動している。
- ポート番号とは送信元と宛先のプロセスを識別する番号
  - MACアドレス　　：コンピュータを物理的に識別
  - IPアドレス　：コンピュータを論理的に識別
  - ポート番号　：コンピュータ内のプロセスを識別

ポート番号

- 16ビットの数値
  - 通常，10進数で表記される。
- ウェルノウンポート番号
  - インターネットでよく使われるアプリケーションプロセスのポート番号
  - サーバ側のポート番号になる。
- エフェメラルポート番号
  - セッションやコネクションごとに使われるポート番号
  - クライアント側のポート番号（ランダムな値）

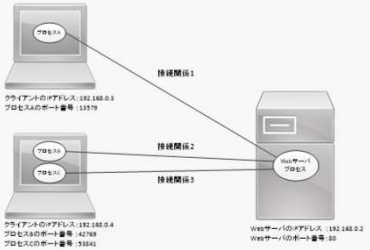
ウェルノウンポート番号の例

ポート番号	プロトコル名	目的
20	FTP（データ）	ファイル転送
21	FTP（制御）	
22	SSH	リモートログイン（暗号文）
23	TELNET	リモートログイン（平文）
25	SMTP	電子メール送信
80	HTTP	Web閲覧
110	POP3	電子メール受信
143	IMAP4	電子メール受信
179	BGP4	AS間ルーティング

IPアドレスとポート番号の組合せ

- 送信元IPアドレス，送信元ポート番号，宛先IPアドレス，宛先ポート番号の組合せでプロセス間の論理的接続関係は一意に定まる。
- 4つのうちひとつでも異なれば別の接続関係とみなされる。

ポート番号による接続関係の識別



10

ソケット（socket）

- コンピュータ通信における情報の論理的な受け渡し口
  - IPアドレスとポート番号を含むいくつかの属性を持つ。
  - ひとつのソケットで双方向の通信を行う。
  - システムコール（アプリケーションがOSに仕事を依頼する命令）で作られ利用される。
    - ソケットの生成
    - ソケットの属性設定
    - ソケットを利用する送受信
    - ソケットの削除

11

TCPの役割

- 通信に信頼性を与える。
  - IPはベストエフォートのプロトコルであり，宛先への正しい到達を保証しない。
    - つまりIPネットワークは信頼できないネットワークである。
  - TCPは失われたパケットの再送，正しい順序への並べ替え，送信量の調整等を行い確実な通信を実現する。
  - コネクション型の通信を行う。
- 送信元アプリケーションと宛先アプリケーションの識別を行う。
  - ポート番号による識別

12

TCPセグメントの構成

13

ヘッダの各フィールド

- 送信順序番号（シーケンス番号）
  - 送信データの先頭バイトの番号（初期値はランダム）
- 確認応答番号
  - 受信データの末尾バイト＋1
- ヘッダ長
  - 4バイト単位でカウント。オプション無しで「5」（20バイト）
- ウィンドウサイズ
  - 受信バッファの空き容量（バイト単位）
- チェックサム
  - 誤り検出用の情報

14

制御ビット

「1」でアクティブ，「0」で非アクティブ

CWR	ECE	URG	ACK	PSH	RST	SYN	FIN

CWR :Congestion Window Reduced
ECE :Explicit Congestion Echo
URG :Urgent
ACK :Acknowledgement
PSH :Push
RST :Reset
SYN :Synchronization
FIN :Finish

ビット名	意味
CWR	輻輳ウィンドウを縮小したことを受信側に通知する。
ECE	輻輳が発生していることを送信側に通知する。
URG	緊急データを含んでいることを示す。
ACK	受信または了解を通知する。
PSH	受信バッファからすぐにアプリケーションに渡すことを要求する。
RST	強制的にコネクションを切断することを通知する。
SYN	コネクションの確立を要求する。
FIN	コネクションの開放を要求する。

15

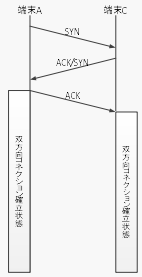
オプションフィールドの使い方

- MSSオプション
  - MSS :Maximum Segment Size
  - コネクション確立時にMSSを通知する。
- タイムスタンプオプション
  - 送信側で送信時刻を挿入，受信側はそのまま送り返す。
  - 往復時間（Round Trip Time）の計測に利用する。
- SACKオプション
  - SACK :Selective ACK（選択的ACK）
  - 受信済みのデータの先頭バイト番号と末尾番号を通知

16

コネクションの確立

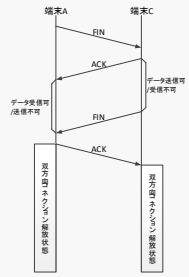
- 双方向で一挙に確立
  - 3回の送受信が発生
  - 3ウェイハンドシェイクと呼ぶ。



17

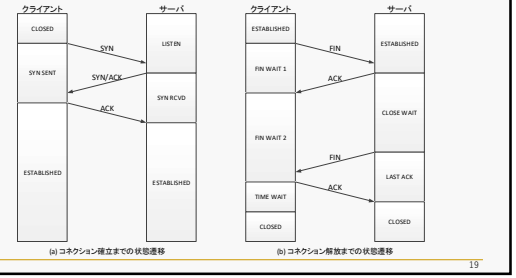
コネクションの解放

- 片方向ずつ解放
  - 送信データが無くなった方から解放要求を送出



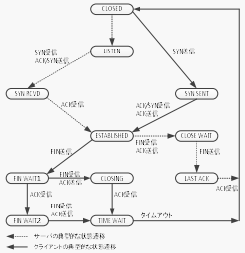
18

TCPの状態遷移（1）



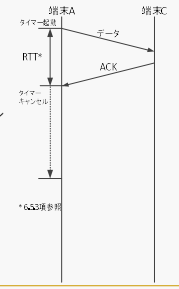
(a) コネクション確立までの状態遷移　(b) コネクション解放までの状態遷移

TCPの状態遷移（2）



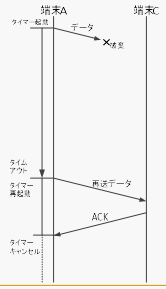
再送制御（1）

- データ送受信正常の場合
  - 送信時にタイマー起動
  - ACK受信でタイマーキャンセル



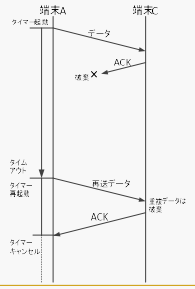
再送制御（2）

- 送信データが破棄された場合
  - 送信時にタイマー起動
  - タイムアウトで再送
  - 再送時にタイマー再起動

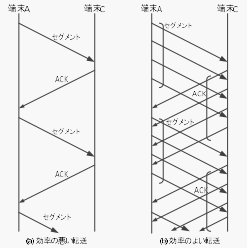


再送制御（3）

- ACKが破棄された場合
  - 送信時にタイマー起動
  - タイムアウトで再送
  - 再送時にタイマー再起動
  - 受信側で重複データは破棄



セグメントの送信方法

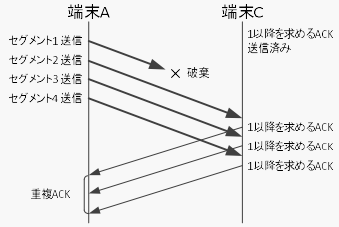


(a) 効率の悪い転送　(b) 効率のよい転送

順序制御（1）

- 受信データに不連続（飛び）が発生するとACKを再送信する（重複ACK）。
- 欠落データが届くとデータを正しい順序に並べ替え次のデータを要求する（正しいACK）。

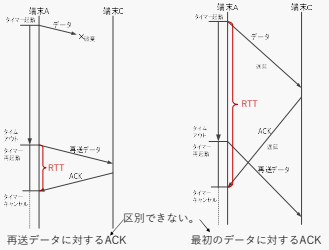
順序制御（2）



再送タイマーの設定

- RTT（Round Trip Time）
  - 送信してからACKが戻るまでの時間（往復時間）
  - RTTは常に変動する。
    - ルーティングにより経路は常に変動する。
    - ネットワークの混雑状況によって遅延が変動する。
- 適切なタイマー値の設定
  - RTTを常に計測する。
  - RTTの計測値に基づきタイマー値を決定する。
    - RTTの過去の値を重視するように加重平均を取り，それにいくらかの
      余裕を加えて決定する。

再送時のRTT計測値



28

カーンのアルゴリズム

- Karn's algorithm
- データを再送した場合のRTT計測値はタイマー値決定のためには採用しない。
- 再送時はタイマー値を一時的に2倍とする。
  - 再送無しでACKが返ってきた時に元に戻す。

29

アプリケーションとTCPの関係

- アプリケーションからの指示で行う制御
  - コネクションの確立
  - コネクションの解放
  - データの送信
  - 受信データの引き取り
- TCP自身の判断で行いアプリケーションには見えない制御
  - 再送制御
  - 順序制御
  - フロー制御
  - 輻輳制御

30

今回学んだこと

1. ポート番号とは
2. ソケットとは
3. TCPの役割
4. TCPセグメントの構成
5. コネクション確立と解放の手順
6. 再送制御とは
7. 順序制御とは
8. 再送タイマーの設定方法
9. アプリケーションとTCPの関係

31

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

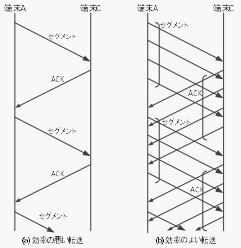
コンピュータネットワーク

第10回
TCPとUDP(2)

今回の到達目標

1. TCPのウィンドウ制御とはどのようなことか理解する。
2. TCPのフロー制御とはどのようなことか理解する。
3. TCPの輻輳制御とはどのようなことか理解する。
   1. スロースタート
   2. 輻輳回避
   3. 高速再送と高速回復
4. UDPの役割とデータグラムの構造を理解する。

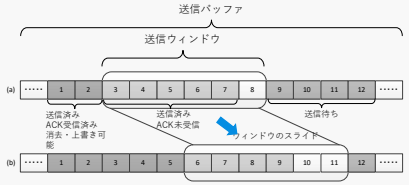
セグメントの送信方法



送信ウィンドウ制御（1）

- 送信バッファ
  - アプリケーションから受け取ったデータをセグメントに分解して格納するメモリ上の領域
- 送信ウィンドウ
  - 送信可能セグメントを指定する送信バッファ内のひと続きの領域
  - 送信ウィンドウ内のセグメントを一挙に送信しACKの返送を待つ。
  - 送信ウィンドウのサイズは相手端末から通知される「ウィンドウサイズ」で決まる。

送信ウィンドウ制御（2）

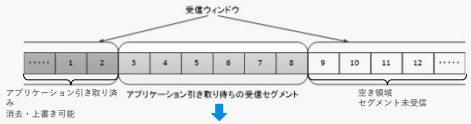


フライトサイズ　：送信済みでACKを受け取っていないデータのバイト数

受信側のウィンドウ制御（1）

- 受信バッファ
  - 受信セグメントの一時保管場所としてメモリ上に確保された領域
  - アプリケーションは受信バッファからデータを引き取っていく。
- 受信ウィンドウ
  - 受信バッファ内のひと続きの空き領域

受信ウィンドウ制御（2）

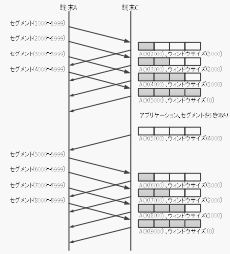


一種のウィンドウ。アプリケーションの引き取りで左端が右に進み，セグメントの受信で右端が右に進む。
しかし，これを受信ウィンドウとは言わない。

フロー制御

- Flow control
- 相手端末の受信バッファの空き状況に応じて送信量を調整すること。
  - 受信バッファを溢れさせないようにする。

フロー制御の例



輻輳制御

- 輻輳（ふくそう）
  - 英語ではcongestion
  - ネットワーク上で発生するパケットの混雑・渋滞
  - 端末がネットワークの容量を超えるデータを送信することによって発生する。
- 輻輳制御
  - congestion control
  - 輻輳を回避するために送信量（セグメントの送信数）を調整すること。

フロー制御と輻輳制御

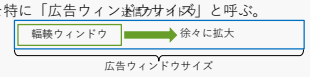
- フロー制御は相手端末に合わせて送信量を調整すること
  - 自身および相手端末のため
- 輻輳制御はネットワークに合わせて送信量を調整すること
  - 自身と相手を含むネットワーク全体のため

輻輳の検出

- TCP自身は直接的に輻輳の兆候・発生を知ることはできない。
  - 輻輳はネットワーク層で発生する現象
- 2つの現象に着目して輻輳を推定する。
  - 再送タイマーのタイムアウト
    - 輻輳により途中でパケットが破棄されたと判断
  - 重複ACK（3回）の受信
    - 輻輳によりパケットが破棄され，不連続（飛び）が発生したと判断

送信量の調整方法

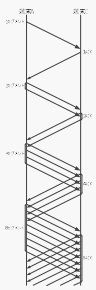
- 送信ウィンドウの中に「輻輳ウィンドウ」という小さな領域を作り，送信セグメント数を制限する。
- 輻輳ウィンドウはネットワークの状況に合わせて徐々に
  拡大する。
  - 最大値は受信側から通知されるウィンドウサイズ
    - これを特に「広告ウィンドウサイズ」と呼ぶ。



スロースタート（slow start）

- 輻輳ウィンドウの初期値は基本的に1セグメント
- ACKが1つ返送されるたびに輻輳ウィンドウを
  1セグメント拡大する。
  - 最初に1つのセグメント送信
  - 1つのACK受信→輻輳ウィンドウを2（=1+1）セグメントとする。
  - 2つのセグメント送信
  - 2つのACK受信→輻輳ウィンドウを4（=2+1+1）セグメントとする。
  - 輻輳ウィンドウは指数関数的に拡大
    - 1→2→4→8→16→・・・・

スロースタートの様子



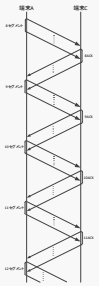
北海道情報大学　通信教育部
コンピュータネットワーク
2024/03/29

輻輳回避（congestion avoidance）

- スロースタートで拡大したした輻輳ウィンドウが予め決められたサイズ（スロースタート閾値：ssthresh）に
達すると輻輳回避の動作に移行する。
- 輻輳回避では一度に送信したセグメントの集合に対するACKの集合の受信で輻輳ウィンドウを約1セグメント分
拡大する。
  - そのような割合になるように一つひとつのACK受信に対して輻輳ウィンドウを拡大する。

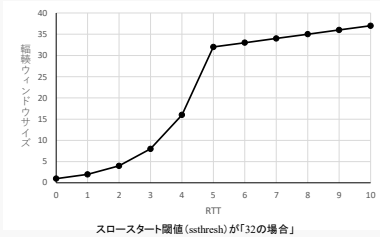
19

輻輳回避の様子



20

スロースタートと輻輳回避



スロースタート閾値（ssthresh）が「32の場合」

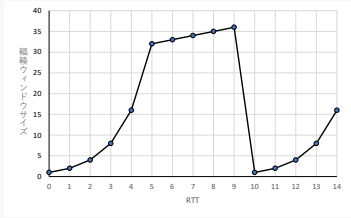
21

輻輳検出時の動作

- タイムアウト発生と重複ACK3回受信では動作が異なる。
- タイムアウト発生時
  - 輻輳ウィンドウを1セグメントに減らし，スロースタートから
やり直しを行う。
  - スロースタート閾値（ssthresh）はフライトサイズの1/2にする
（但し2セグメント以上）。
- 重複ACK3回受信時
  - 欠落したと思われる1セグメントをすぐに再送
  - 輻輳ウィンドウを約1/2にして輻輳回避を継続する。

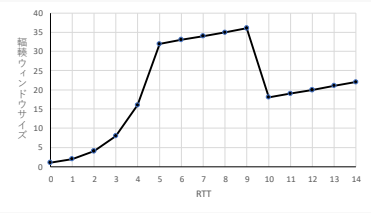
22

タイムアウト発生時の動作



23

重複ACK3回受信時の動作



24

重複ACK3回受信時の動作詳細

- 欠落したと思われる1セグメントをすぐに再送
  - ジェイコブソンの高速再送（Jacobson's fast retransmit）
- スロースタート閾値はフライトサイズの1/2とする。
- 輻輳ウィンドウのサイズを上記＋3セグメント分に設定
- 重複ACKがひとつ返るたびに輻輳ウィンドウサイズを
1セグメント分増加させる。（インフレーション）
- 正常ACKの受信でインフレーションを帳消しにし，
輻輳回避を継続
- 上記の過程を高速回復（fast recovery）という。

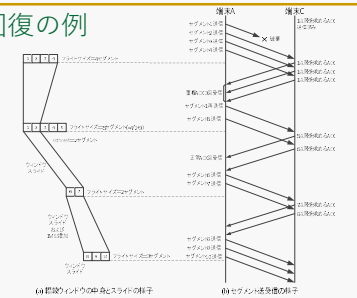
25

重複ACK受信中のインフレーション

- 重複ACK受信中はウィンドウはスライドしない。
  - 新しいセグメントは送信できない。
  - それでは効率が悪いのでなるべく一時的に輻輳ウィンドウを
膨張させてセグメントの送信を続ける。
  - 輻輳ウィンドウの一時的な膨張を「インフレーション」という。
    - ACKの受信は相手端末がセグメントを受信している証拠。
    - 輻輳は軽微であると判断して送信を継続

26

高速回復の例

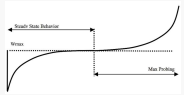


(a)輻輳ウィンドウの増加とスライドの様子　(b)セグメント送受信の様子

27

輻輳制御の標準とcubic

- 以上示した輻輳制御は最も標準的なものであり，通称「Reno」と呼ばれる。
  - Renoの改良版（ウィンドウ内の複数のセグメント欠落に対応）は「New Reno」と呼ばれる。
- 最近では3次関数を利用してウィンドウサイズを急速に増加させるアルゴリズム「cubic」（キュービック）が広く使われている。



28

UDP

- User Datagram Protocol
- TCPは再送制御，フロー制御，輻輳制御を行うため，データの転送に時間がかかる。
- リアルタイムデータの転送にはUDPを用いる。
- UDPの機能
  - ポート番号によるアプリケーションプロセスの識別
  - チェックサムによる誤り検出（ただし使用は任意）
  - アプリケーションのデータをほぼ素通しでIP層に渡す。
  - 1対N通信，N対N通信が可能。

29

UDPデータグラムの構造

30

今回学んだこと

1. TCPのウィンドウ制御
2. TCPのフロー制御
3. TCPの輻輳制御
   1. スロースタート
   2. 輻輳回避
   3. 高速再送と高速回復
4. UDPの役割とデータグラムの構造

31

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第11回

インターネットサービスと
プロトコル（1）

今回の到達目標

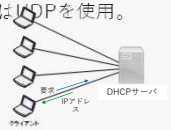
1. 代表的なインターネットサービスを実現する
   アプリケーションプロトコルを理解する。
   1. DHCP
   2. DNS
   3. 電子メール
   4. ファイル転送

IPv4アドレスの設定

- 手動設定（固定）と自動設定の2通りがある。
  - 手動設定
    - 右の図（例）
  - 自動設定
    - DHCPによる。

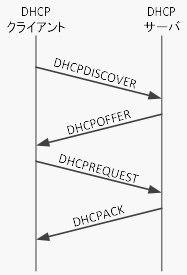
DHCP（1）

- Dynamic Host Configuration Protocol
- コンピュータがサーバからIPアドレスを取得するための
  プロトコル
- UDPまたはTCP上で動作。通常はUDPを使用。
  - クライアントのポート番号：68番
  - サーバのポート番号：67番



DHCPの通信

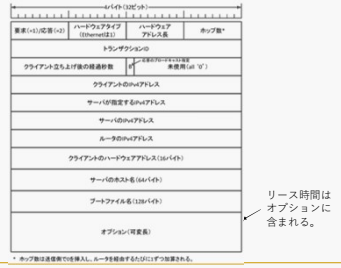
- DHCPDISCOVER
  - DHCPサーバの探索
  - ブロードキャストを使用
- DHCPOFFER
  - IPアドレス，リース時間の提案
- DHCPREQUEST
  - 提案されたIPアドレスを要求
- DHCPACK
  - IPアドレスの確定通知



DHCPの設置場所と個数

- サーバはクライアントが属するネットワークの外部に
  設置されることもある。
  - ルータを介してメッセージが転送される。
- 複数のDHCPサーバが設置される場合もある。
  - DHCPOFFER（提案）が複数返る。
  - クライアントはその中から選択してDHCPREQUEST（要求）を
    送信する。

DHCPメッセージの構成



10

IPアドレスとドメイン名

- IPアドレスは数値
  - ユーザにとっては覚えにくい。
- IPアドレスをユーザが覚えやすい文字列（ドメイン名）に
  対応づけておく。
- 例
  - 北海道情報大学の公式サイト（Webサーバ）
    - IPアドレス：150.31.181.70
    - ドメイン名：www.do-johodai.ac.jp
  - メールアドレスの「@」の右側
    - alice@example.com

11

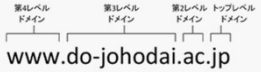
DNS（Domain Name System）

- IPアドレスとドメイン名の対応付けを行うためのシステム
- DNSサーバ
  - DNSを実現するサーバ
  - クライアントはDNSサーバにドメイン名を送り，対応するIPアドレスを取得する。これを「名前解決」という。
  - 電話に例えればDNSサーバは電話帳
  - DNSのプロトコルはUDPまたはTCP上で動作する。
    通常はUDPを使う。

12

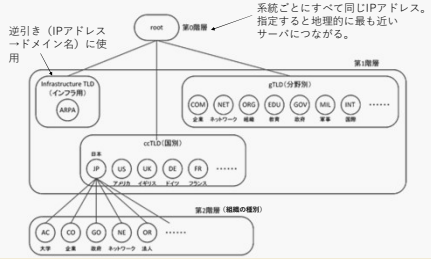
ドメイン名の構成

- レベル分けされている。
  - 右端がトップレベルドメイン
- ピリオド「.」で区切って下位のドメイン名を並べる。
- 大文字，小文字は区別しない。
- FQDN（Fully Qualified Domain Name）
  - すべてのドメインを省略せずに書いたドメイン名



13

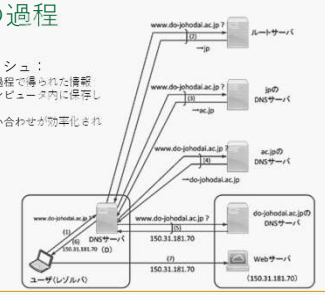
ドメイン名の階層化



14

名前解決の過程

DNSキャッシュ：
問い合わせの過程で得られた情報を一定期間コンピュータ内に保存しておくこと。問い合わせが効率化される。



15

電子メールシステム

- メールサーバがメールの受付，転送，配送を行う。

16

メールの提出，転送，受信

- 提出
  - 送信者から送信側メールサーバに送られて一旦保管される。
    - 保管場所は待ち行列（メッセージキュー）になっており，順次転送される。
- 転送
  - 送信側メールサーバから受信側メールサーバに送られて保管される。
    - 宛先ごとに保管場所（メールボックス）がある。
- 受信
  - 受信者が受信側メールサーバにアクセスし受信する。

17

電子メールのプロトコル

- SMTP（Simple Mail Transfer Protocol）
  - メールの受付と転送を行う。
- POP3（Post Office Protocol version 3）
  - ユーザの要求に基づいてメールの配信を行う。
- IMAP4（Internet Mail Access Protocol version 4）
  - ユーザの要求に基づいてメールの配信を行う。
- POP3とIMAP4はいずれか一方を選択して使用する。
- いずれもTCP上で動作する（信頼性重視）。

18

電子メールプロトコルの特徴

- テキストベース
  - 文字コード（文字と数値の変換規則）はASCIIコード
  - 電子メールヘッダの例

```
To: alice@example1.com
Subject: Information and Communication Networks
From: bob@example2.com
Date: Sat, 29 Oct 2022 01:30:34 +0900
Message-ID: <・・・・・・・・・・・・・・・>
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
```

- 添付ファイルも文字情報に変換されて送られる。
  - MIME（Multi-purpose Internet Mail Extension，マイム）

SMTP

- 宛先ポート番号は基本的に25番
  - ユーザのメール提出時は587番
  - メールサーバ間の転送時は25番
- ヘッダの内容

```
宛先→ To: alice@example1.com
件名→ Subject: Information and Communication Networks
送信元→ From: bob@example2.com
日付→ Date: Sat, 29 Oct 2022 01:30:34 +0900
メッセージ番号→ Message-ID: <・・・・・・・・・・・・・・・>
データ形式/文字コード→ Content-Type: text/plain; charset=UTF-8
符号化則→ Content-Transfer-Encoding: 8bit
```


POP3とIMAP4

- POP3
  - 宛先ポート番号は110番
  - ユーザのパスワード認証，メールの引き取り，メールボックスの更新（メール削除）を順に行う。
- IMAP4
  - 宛先ポート番号は143番
  - 閲覧されたメールはユーザが指示しない限り削除されない。
  - フォルダを作りメールを分類・整理することが可能
  - メールの検索も可能

添付ファイル

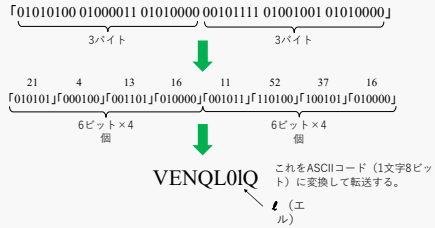
- あらゆる種類のファイルを添付可能。
  ただし，容量制限がある。
- ファイルは文字情報に変換される。
  - BASE64がよく用いられる。
    - 一続きの長いバイト列を3バイト（24ビット）ずつに区切る。
    - 24ビットを6ビットを単位とする4個のビット列に分ける。
    - 6ビットが表す数値（0～63）を64個の文字「A～Z，a～z，0～9，+，/」に
      この順で対応させる。
    - 文字をASCIIコード（8ビット）で転送する。

BASE64変換表

10進	2進	文字	10進	2進	文字	10進	2進	文字	10進	2進	文字
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/

出典：https://bootmacos.com/archives/6753

BASE64による変換の例



ファイル転送

- ネットワークを介してクライアントとサーバの間で
  ファイルを転送する。
- FTP（File Transfer Protocol）
  - インターネットの初期に作られたファイル転送用プロトコル
  - TCP上で動作する。
  - TCPコネクションは2つ（データ転送用と制御用）
  - 宛先ポート番号（アクティブモード）
    - データ転送用　　：20番
    - 制御用　　：21番

FTPの2つのモード

データ転送用コネクションはサーバから要求する。（サーバがアクティブ）

データ転送用コネクションはクライアントから要求する。サーバは宛先ポート番号を指定する。（サーバがパッシブ）

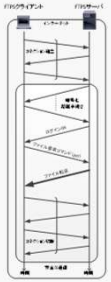
FTPの問題点と代替プロトコル

- セキュリティの問題
  - ユーザのIDやパスワードを含むすべての情報を暗号化せずに転送する。
  - インターネット上ではそのまま使えない。
- 代替プロトコル
  - FTPS（File Transfer Protocol over SSL/TLS）
    - SSL/TLSは暗号化と認証を行うプロトコル
  - SFTP（SSH File Transfer Protocol）
    - SSH（セキュアな遠隔コンピュータ制御）を利用
    - SSHについては次回解説

FTPSのプロトコル階層

FTPSの動作概要

SSL/TLSで認証を行い，
暗号化の準備を行ってから
ファイル転送を始める。



28

プロトコルとセキュリティ

- インターネットの初期に作られたプロトコルはセキュリティの問題を有する。
  - FTP，SMTP，POP，IMAP，HTTP（次回解説）
  - 上記は認証や暗号化を行わない。
  - 今日ではSSL/TLS上で動作させる。
    - FTPS，SMTPS，POPS，IMAPS，HTTPS
    - ウェルノウンポート番号は本来のものとは異なる。
      - 例
        - FTPS（データ転送用）　：989番
        - FTPS（制御用）　：990番

29

今回学んだこと

1. 代表的なインターネットサービスを実現するアプリケーションプロトコル
   1. DHCP
   2. DNS
   3. 電子メール
   4. ファイル転送

30

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第12回

インターネットサービスとプロトコル（2）

今回の到達目標

1. Webサービスを実現するプロトコルと関連する技術を
   理解する。
   1. HTTP
   2. キャッシュサーバ
   3. CGI
   4. Javascript
   5. cookie
2. 遠隔コンピュータ制御とネットワーク管理のプロトコルを理解する。

WWW（World Wide Web）

- ネットワーク上のコンピュータに格納されている情報（テキスト，画像，その他）を多くのユーザに提供するシステム
  - 世界規模の（World Wide）蜘蛛の巣（Web）の意
    - 単にWebとも言われる。
  - クライアント（ユーザ）はWebブラウザ（閲覧用ソフト）を使ってWebサーバにアクセスする。
  - 現在では電子メール（Gmail等），動画配信（YouTube等），SNS（Facebook，Instagram等）などの基盤システム

HTTP（Hypertext Transfer Protocol）

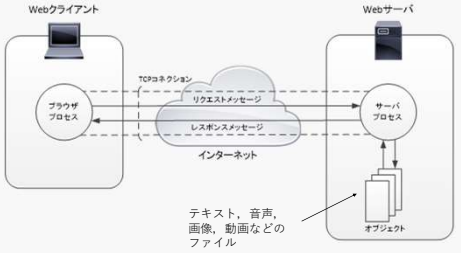
- クライアント（Webブラウザ）とWebサーバの間の通信に用いられるプロトコル
- 現在のバージョンは1.0，1.1，2，3の4種類
- TCP上で動作する。
  - 宛先ポート番号（Webサーバ側）は基本的に80番
  - 認証や暗号化を伴う通信（HTTPS）では443番
- 要求（request）と応答（response）によって情報の送受信を行う。

WebページとHTML

- Webページ
  - Webブラウザに表示される画面
- HTML（HyperText Markup Language）
  - Webページを記述する言語
    - HyperText とは，複数の文書（テキスト）を相互に関連付け，結び付ける仕組み
  - 情報の中身とその表示形式を記述する。
  - HTMLで記述されたファイルをHTMLファイルといい，拡張子は「.html」

HTMLの例

WWWの基本システム構成



HTTP/1.1のリクエストメッセージ（1）

HTTP/1.1のリクエストメッセージ（2）

- リクエスト行の例
  - GET /example/example1.html HTTP/1.1
- メソッド
  - GET（取得），POST（作成），HEAD（ヘッダ情報取得），PUT（作成/更新），DELETE（削除）など
- 主なヘッダ
  - Connection　：コネクションの取り扱い
  - User-Agent　：ブラウザの種類
  - Accept-Language　：受け入れ可能な言語

HTTP/1.1のレスポンスメッセージ（1）

HTTP/1.1のレスポンスメッセージ（2）

- ステータス行の例
  - HTTP/1.1 200 OK
- 主な状態コード

状態コード番号とフレーズ	内容
200 OK	正常に応答する。
301 Moved Permanently	指定URIの情報は移動された。
304 Not Modified	指定URIの情報は更新されていない。
400 Bad Request	リクエストをサーバが理解できない。
404 Not Found	指定URIの情報が存在しない。
505 HTTP Version Not Supported	指定したバージョンをサポートしない。

HTTP/1.1のレスポンスメッセージ（3）

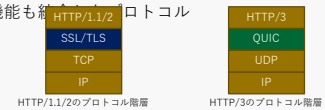
- 主なヘッダ
  - Connection　：TCPコネクションの状態
  - Date　：メッセージ送信の日時
  - Server　：サーバプロセスの種別
  - Last-Modified　：オブジェクトの最終更新日時
  - Content-Length　：オブジェクトのバイト数
  - Content-Type　：オブジェクトのタイプ

HTTP/2

- HTTP/2
  - リクエスト行とヘッダ行（ASCIIコード）の内容をバイナリデータ
    として表現
  - 必要に応じて分割し，フレームと呼ばれる情報転送単位に格納して転送
    - やり取りされる情報の意味内容（セマンティクス（semantics））はHTTP/1.1と変わらない。
  - ひとつのTCPコネクションの中にストリームという独立した情報（フレーム）の流れをつくり，ある情報が遅れても他の情報転送に影響が無いようにしている。

HTTP/3

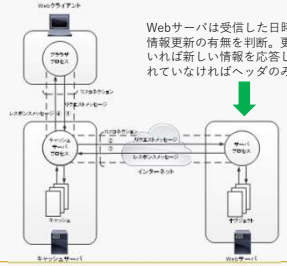
- TCPの代わりにUDPを使用し，QUIC（クイック）という
  新しいプロトコルを用いる。
- QUIC
  - UDP上で動作し，TCPと同様の信頼性に加えセキュリティ確保の機能も統合したプロトコル



キャッシュの利用

- キャッシュ（cache）
  - 一度取得した情報をその後も保存しておくこと，および保存された情報
- キャッシュサーバ
  - Web情報をキャッシュしておくためにクライアントの近くに設置される代理サーバ（proxy server）
  - クライアントは本来のWebサーバと通信する替わりにキャッシュサーバとHTTP通信を行って情報を取得

キャッシュサーバの働き

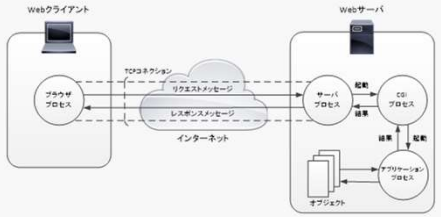


Webサーバは受信した日時から情報更新の有無を判断。更新されていれば新しい情報を応答し，更新されていなければヘッダのみを応答。

CGI（Common Gateway Interface）

- クライアントの要求に基づいてサーバ内の別のプログラムを起動しその処理結果と組み合わせて応答する仕組み
- サービスの高度化が可能となる。
  - 電子掲示板の読み書き
  - ウェブページ上でのアンケートへの回答
  - アクセスカウンターの累計
  - ブログシステムなど
- PHPなどの言語を用いても同様のことが可能

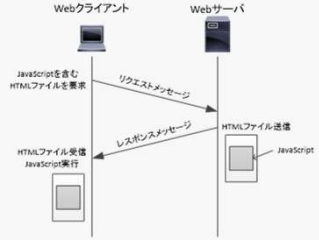
CGIを利用する構成



JavaScript

- Webサーバからブラウザに送信されブラウザ上で実行されるプログラム
- サービスの高度化が可能となる。
  - Webサイトに動きをつける。
    - ポップアップウィンドウ（警告表示など）
  - ページを移動せずに情報を取得または表示
    - 地図上の移動など

JavaScriptを用いるサービス

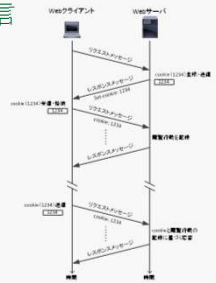


cookie（クッキー）

- Webサーバがクライアントを識別するために
  Webブラウザ内に格納しておく小さなファイル
  - クライアントがWebサーバに接続するとサーバからcookieが送信されブラウザ内に格納される。
  - クライアントがWebサーバに改めて接続するとcookieがWebサーバに送信され，クライアントが識別される。
  - HTTPヘッダ（Set-CookieおよびCookie）が利用される。

cookieを利用する通信

ビジネスに利用できるが，
セキュリティ上の問題もある。
ブラウザはcookieの拒否，
削除が可能。



遠隔コンピュータ制御

- 離れたコンピュータにログインしてそのコンピュータを
  操作すること
- インターネットの初期にTELNETが作られた。
  - セキュリティの問題があり，インターネット上では使われない。
  - 宛先ポート番号：23番（TCP上で動作）
- SSH（Secure Shell）
  - TELNETの代替プロトコル
  - 暗号・認証によって盗聴，改ざん，なりすまし等を防ぐ。

TELNETとSSHによる遠隔制御

ネットワーク管理

- SNMP（Simple Network Management Protocol）
  - ネットワーク機器や伝送路の状態監視
  - ネットワーク機器の制御（初期設定や設定変更）
  - ネットワーク管理者（管理用ソフトウェア）が使用するプロトコル（UDP上で動作）
    - 管理される機器のソフトウェア　：SNMPエージェント
    - 管理する機器のソフトウェア　　：SNMPマネージャ

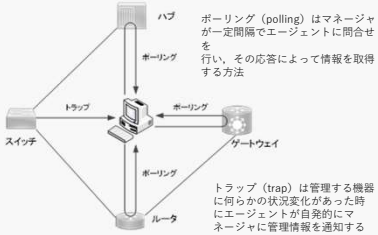
28

MIB（Management Information Base）

- SNMPエージェントが保持するデータベース
  - 以下の情報を階層的（ツリー状）に整理されたオブジェクトと
    して保持
    - 機器自身に関する情報（製造メーカ，型番，電源投入後の稼働時間など）
    - 機器が収集した情報（送信／受信したフレーム／パケット数，伝送路の状況など）

29

SNMPによるネットワークの監視



ポーリング（polling）はマネージャが一定間隔でエージェントに問合せを
行い，その応答によって情報を取得する方法

トラップ（trap）は管理する機器に何らかの状況変化があった時にエージェントが自発的にマネージャに管理情報を通知する方法

30

今回学んだこと

1. Webサービスを実現するプロトコルと関連する技術
   1. HTTP
   2. キャッシュサーバ
   3. CGI
   4. Javascript
   5. cookie
2. 遠隔コンピュータ制御とネットワーク管理のプロトコル（TELNET，SSH，SNMP）

31

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第13回
ブロードバンド通信と移動通信

今回の到達目標

1. ブロードバンド通信とは何かを理解する。
2. ブロードバンド通信を実現するシステムを理解する。
3. リアルタイム通信とは何かを理解する。
4. リアルタイム通信を実現するプロトコルを理解する。
5. 移動通信システムの現状（4G）と近未来（5G）を理解する。

ブロードバンド（broadband）通信

- 広い帯域を使って行う高速インターネット通信
  - ディジタル通信の帯域は通信の速度のことであり，単位にはbpsを用いる。
- コアネットワークの高速・大容量化
  - 1980年代の光通信の導入によって著しく進んだ。
- アクセスネットワークのブロードバンド化
  - 2000年頃から急速に進展した。

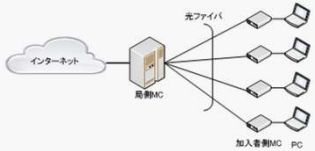
アクセスネットワークの変遷

- 2000年頃から国内ではADSL（Asymmetric Digital Subscriber Line）が一時期普及
  - 電話線を利用するブロードバンドアクセス方式
    - アナログ通信
    - 電話信号とインターネット信号を周波数多重する。
  - 速度や到達距離に限界があり，今では衰退（国内）
- 現在，国内の主流はFTTH（Fiber to The Home）*
  - 光ファイバを利用するブロードバンドアクセス方式
    - 光ベースバンド伝送
- ケーブルテレビや無線を利用する方式もある。

*FTTB（Fiber to The Building：光ファイバ＋電話線（VDSL：Very high bit rate DSL）の方式）

FTTH（1）

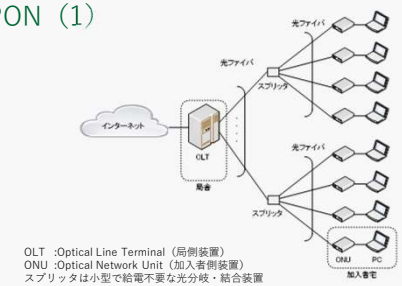
- メディアコンバータ（MC）を用いる1対1通信
  - シングルスター（SS）方式



FTTH（2）

- ダブルスター（DS）方式
  - 局舎の装置から加入者の近くまで1本の光ファイバを用いて接続し，そこから分岐して複数の加入者に接続する。
    - アクティブダブルスター　（ADS）　　：分岐装置に給電が必要
    - パッシブダブルスター　（PDS）：分岐装置に給電が不要
  - PDSが多く用いられPONと呼ばれる。
    - PON（Passive Optical Network）
    - 規格にはIEEEによるものとITU-Tによるものがある。
    - 日本ではIEEEが主流（GE-PON（Gigabit Ethernet PON））

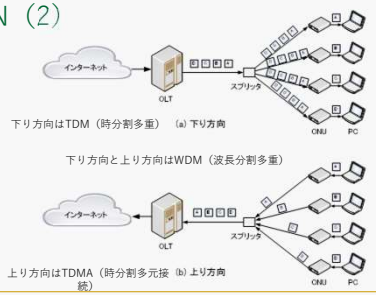
PON（1）



OLT　:Optical Line Terminal（局側装置）
ONU :Optical Network Unit（加入者側装置）
スプリッタは小型で給電不要な光分岐・結合装置

10

PON（2）



下り方向はTDM（時分割多重）　(a) 下り方向

下り方向と上り方向はWDM（波長分割多重）

上り方向はTDMA（時分割多元接続）　(b) 上り方向

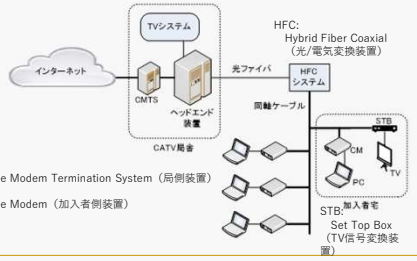
11

CATVによるインターネット接続

- CATV（Common Antenna Television）
  - 有線（ケーブル）でTV放送を配信するシステム
- CATVによるインターネット接続
  - TVの信号にインターネットの信号をFDM（周波数分割多重）

12

CATVインターネットシステム



13

公衆無線LAN

- 公衆無線LAN
  - 多数の利用者に無線でインターネットアクセスを提供するサービス
  - 有料で利用できるものと無料のものがある。
  - Wi-Fiスポット（Wi-Fi spot）
    - サービスを提供する場所
      - 人の集まる公共施設，商業施設，ホテル，駅，空港等
      - 鉄道車両，バスの車内，航空機の中

14

WiMAX

- Worldwide Interoperability for Microwave Access
- 無線でインターネットアクセスを可能とする通信規格（コネクション型通信）
  - 当初の目的はケーブルや光ファイバの敷設が困難な地域にインターネットサービスを提供すること
- その後，モバイルWiMAXの仕様（最新版はIEEE802.16m）が策定された。
- モバイルWiMAXは8.5節で述べる第4世代以降の移動通信方式に含まれる。

15

テザリング（tethering）

- スマートフォンを無線ルータ（中継装置）として利用し
  PC等をインターネット接続する方法
  - スマートフォンとPCの接続によって以下の種類がある。
    - Wi-Fiテザリング
    - USBテザリング
    - Bluetoothテザリング

16

リアルタイム通信

- ブロードバンド通信は大容量のリアルタイム通信を実現する基盤となる。
- リアルタイム通信に不向きなパケット交換でリアルタイム通信を実現する技術が必要となる。
  - 電話やTV会議などのサービスを実現

17

リアルタイム性

- 「処理に締め切り時刻があり，その時刻までに処理を完了しなければならない」という性質
- ハードリアルタイム性
  - 「締め切りに少しでも遅れたら意味がなくなる，または重大な結果をもたらす」性質
    - 工場の組み立てロボットや自動車のブレーキ，エアバッグ
- ソフトリアルタイム性
  - 「締め切りはあるが，情報の遅延・欠落が一定の範囲の中では
    許される」性質
    - 電話やTV会議

18

リアルタイム通信用プロトコル

- RTP（Realtime Transport Protocol）
  - 音声や映像などのデータそのものを運ぶプロトコル
- RTCP（Realtime Transport Control Protocol）
  - RTPの動作をサポートする制御プロトコル
- RTPとRTCPはUDP上で動作する。

RTPパケットの構成

RTPヘッダの内容

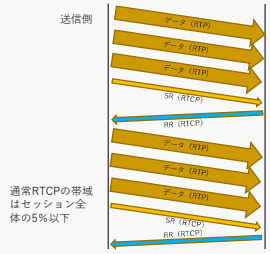
記号	名称	bit	説明
V	version(v)	1	現在のRTPのバージョンは2
P	padding(p)	1	RTPペイロードの最後にパディングがある場合に１になる。
X	extension(x)	1	RTP拡張ヘッダを利用する場合に１になる。
CC	csrc count(cc)	4	寄与するソースの数が入る．寄与するソースは，途中にミキサやトランスレータが入り，複数RTPストリームがマージされたときにマージされたソースを表すために利用される。
M	marker(m)	1	RTPストリームの重要なイベントに印をつけるために使う。このビットの利用方法は利用するRTPプロファイルやRTPペイロードフォーマットによって決まる。
-	ペイロードタイプ	7	ペイロードの種類を表す。実際には以下のように符号化方法を示している。 0：PCM μ-law, 3:GSM, 14:MPEG Audio, 26:Motion JPEG, 33:MPEG 2 video
-	順序番号	16	RTPパケットのシーケンス番号。パケットが送信される度にインクリメントされる。これを利用して受信者側でパケットロスを検知できる。
-	タイムスタンプ	32	タイムスタンプ．タイムスタンプの増加の刻みやどのタイミングでタイムスタンプが変化するかはペイロードフォーマットに依存する．
-	同期ソースのID	32	送信者識別子．ランダムに与えられる番号（送信元IPアドレスではない）
-	寄与するソースのID	32×n	RTPパケットに寄与する（参加する）送信者のID

RTCPパケットの構成

RTCPの各パケットタイプの内容

パケットタイプ	意味	内容
200	送信者レポート	送信時刻、累積送信パケット数、累積送信バイト数
201	受信者レポート	パケット損失率、累積損失パケット数、累積受信順序番号、ジッタ（受信間隔のゆらぎ）、前回の送信者レポートの時刻、前回の送信者レポートからの経過時間
202	ソースの説明	正式名称、eメール、電話番号等
203	離脱通知	離脱するソースID
204	アプリ定義パケット	試験用

RTPとRTCPの通信

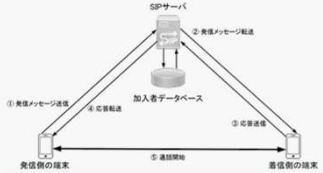


VoIP（Voice over IP）

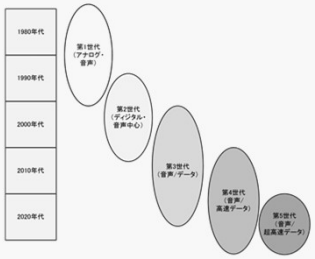
- パケット通信ネットワーク上でリアルタイムの音声通信を実現する技術の総称
- RTPとRTCPが用いられる。
- VoIPの課題
  - 失われたパケットの補償，遅延とジッタ（パケット到着時間の
    細かな揺らぎ）への対処
    - 失われたパケットの部分は無音または雑音に置き換えて，ユーザになるべく気づかれないようにする。
      - 遅延を150ミリ秒以内に抑えれば通話に支障はない。

SIP（Session Initiation Protocol）

- リアルタイム通信のセッション（接続関係）を確立し，通信終了時にセッションを解放する。
  - 通信中のデータ転送には関わらない。

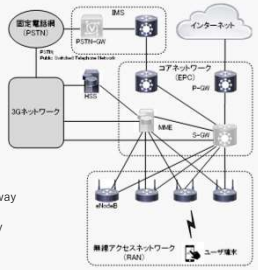


移動通信の変遷



4 Gの構成

- コアネットワークと無線アクセスネットワークから成る。
- すべての通信はパケット交換で行われる。



IMS　: IP Multimedia Subsystem
EPC　: Evolved Packet Core
P-GW: Packet Data Network Gateway
S-GW: Serving Gateway
MME : Mobility Management Entity
HSS　: Home Subscriber Server
RAN　: Radio Access Network

28

5 Gの特徴

- 超高速（10Gbps），超低遅延（1ミリ秒未満），多数同時接続（100万台/km^2）の通信
- コアネットワークの特徴
  - NFV（Network Function Virtualization）
    - ネットワーク機能の仮想化と汎用サーバの利用
  - SDN（Software Defined Network）
    - ソフトウェアによるネットワーク制御
  - 分散クラウド（distributed cloud）
    - サーバ機能の分散配置
  - ネットワークスライシング（network slicing）
    - 同一ネットワーク上に複数の仮想ネットワークを構築

29

今回学んだこと

1. ブロードバンド通信とは
2. ブロードバンド通信を実現するシステム
3. リアルタイム通信とは
4. リアルタイム通信を実現するプロトコル
5. 移動通信システムの現状（4G）と近未来（5G）

30

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第14回
ネットワークセキュリティ（1）

今回の到達目標

1. ネットワークセキュリティの要素を理解する。
2. ネットワークに対する脅威を理解する。
3. 脅威に対する対策を理解する。
4. 暗号とはどのようなものか理解する。
5. 共通鍵暗号AESを理解する。
6. 公開鍵暗号RSAを理解する。

知らせたい情報，知られたくない情報

- 知らせたい情報
  - Webサイトの情報，SNSの情報など
  - 倫理性，正確性，効率性が重要
- 知られたくない情報
  - 個人情報，企業秘密など
  - 機密性，非破壊性が重要

情報セキュリティの3要素

- 機密性（Confidentiality）
  - 正当な資格を持つ者だけが情報にアクセスできること
- 完全性（Integrity）
  - 情報が完全であり改ざんや破壊を受けないこと
- 可用性（Availability）
  - 資格のある者が必要時にいつでも情報にアクセスできること

情報セキュリティの7要素

- 3要素に以下の4要素が加わる。
- 真正性（Authenticity）
  - 情報やそれにアクセスする者が本物であると確認できること
- 責任追及性（Accountability）
  - アクセスの履歴を追跡できること
- 否認防止（Non-repudiation）
  - 情報を後から否定できないようにすること
- 信頼性（Reliability）
  - 情報システムが間違いなく動作すること

セキュリティに対する脅威（攻撃）

- インターネット上では脅威は常に存在している。
- 脆弱（ぜいじゃく）とは
  - 脅威に対して耐性が弱いこと
- 攻撃と対策の例

情報セキュリティの要素	攻撃の例	対策の例
機密性	盗聴， システムへの不正侵入・不正操作	暗号化，パスワード認証， ファイアウォールやIDSの設置
完全性	情報の改ざん・破壊	暗号技術を利用する改ざん・破壊の検出
可用性	システムへの攻撃・破壊	ファイアウォールやIDSの設置

（注）IDS（Intrusion Detection System）：侵入検知システム（9.2.5項参照）

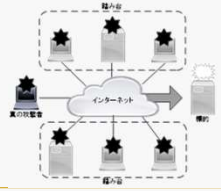
DoS攻撃

- Denial of Service
  - 標的とするコンピュータに大量のデータや不正パケットを送信し，過負荷の状態を作り出してサービス不能に陥らせる攻撃

10

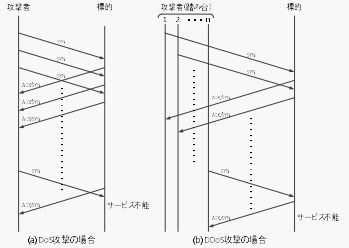
DDoS攻撃

- Distributed DoS
  - 多数のコンピュータ（踏み台）が一斉に大量のデータや不正パケットを標的に送りつけてサービス不能に陥らせる攻撃



11

TCPのSYNフラッド攻撃



12

さまざまな攻撃手法（1）

- DNSキャッシュポイズニング（DNS cache poisoning）
  - 利用者を偽のWebページに誘導し，パスワードなどの情報を入力させて不正に取得する（フィッシング）。
- 辞書攻撃（dictionary attack）
  - 辞書ファイルに基づいて単語の組み合わせを順次試すことでパスワードを取得する。
- 総当たり攻撃（brute force attack）
  - すべての文字の組合せを試すことでパスワードを取得する。

13

さまざまな攻撃手法（2）

- ドライブバイダウンロード（drive-by download）
  - ユーザがWebページを閲覧した時に密かに不正なプログラムをダウンロードする。
- SQLインジェクション（SQL injection）
  - 不正なSQLコマンドを送りつけてデータベースを改ざん，または情報を取得する。
- ゼロデイ攻撃（zero-day attack）
  - セキュリティホールが発見されてから修正プログラムが提供されるまでの期間を利用して攻撃を行う。

14

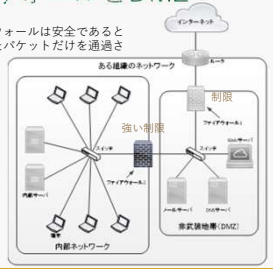
マルウェア（malware）

- 悪意を持ってネットワークやネットワーク機器に害を及ぼすソフトウェア
- 自己伝染機能，潜伏機能，発病機能のいずれかを持つ。従来は以下の3つの分類されてきた。
  - ウイルス（virus）
    - 他のプログラムやデータに寄生して動作する。
  - ワーム（worm）
    - 他に寄生せず単独で動作し，自己増殖する。
  - トロイの木馬（Trojan horse）
    - 有益なプログラムを装いながら裏で不正を行う。
- 最近は単純に分類できない混合型も多い。

15

ファイアウォールとDMZ

ファイアウォールは安全であると確認されたパケットだけを通過させる。



16

IDSとIPS

- IDS（Intrusion Detection System）
  - 侵入するパケットのデータ部分やパケットの挙動を監視し，疑わしいパケットを発見した場合はネットワーク管理者に通知するシステム
  - ネットワーク型とホスト型
  - パタン登録型と異常検知型
- IPS（Intrusion Prevention System）
  - 疑わしいパケットを除去するシステム

17

暗号技術

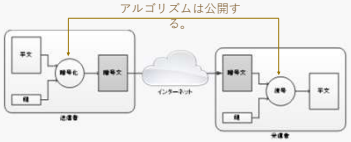
- ある情報を第3者には判読できないようにする技術
  - 暗号化（平文→暗号文）と復号（暗号文→平文）を行う。
  - アルゴリズムと鍵が必要
  - 換字式，転置式，挿入式およびこれらの組み合わせ

暗号の方式	アルゴリズムの例	鍵の例	平文の例	暗号文
換字式	アルファベットを右へ何文字かずらす	3文字	HELLO	KHOOR
転置式	5文字を単位として並べ替える	54321	HELLO	OLLEH
挿入式	鍵を分解して一文字おきに挿入する	BOOK	HELLO	HBEOLOLKO

18

ケルクホフスの原理

- 「暗号のアルゴリズムは公開し，鍵だけを秘密にする。しかし，それでも十分な強度を持たなければならない」



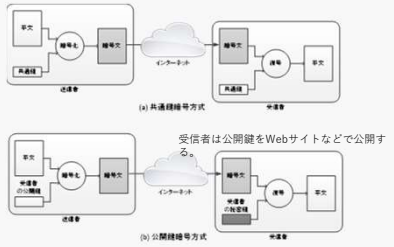
19

共通鍵暗号方式と鍵配送問題

- 共通鍵暗号方式
  - 暗号化と復号に使用する鍵が同じ（共通鍵）
- 鍵配送問題
  - 暗号通信に先立ち，共通鍵をどうやって相手に渡すのかという
    問題
  - 20世紀末にネットワークを通じた鍵交換方式と公開鍵暗号方式が発明され，解決された。

20

共通鍵暗号方式と公開鍵暗号方式



21

AES（Advanced Encryption Standard）

- 共通鍵暗号方式の標準
- 以前使われたDESや3DESの後継暗号
- 平文を128ビットのブロックに分割し，ブロックごとに暗号化を行う。
  - 鍵の長さは128ビット，192ビット，256ビットのいずれかを選択
    （通常は128ビットまたは256ビットを使用）
  - 高速に暗号化と復号ができる強力な暗号
    - 強度の理由はその鍵の長さにある。
    - DES（56ビット鍵）に比べて鍵の数が膨大
      - 総当たり攻撃は事実上不可能

22

RSA暗号

- 代表的な公開鍵暗号
- 素因数分解の困難性を利用した暗号
  - 極めて大きな素数どうしの積を素因数分解することは事実上不可能
- 公開鍵
  - 2つの整数の組(n, e)
- 秘密鍵
  - 2つの整数の組(n, d)

23

RSAの暗号化と復号の方法

- 平文の数値aの暗号化（公開鍵(n, e) を使用）
  - aをe乗してnで割り，余りbを求める。
  - bが暗号文の数値となる。
- 暗号文の数値bの復号（秘密鍵(n, d) を使用）
  - bをd乗してnで割った余りとして平文の数値aが得られる。

24

RSAの暗号化と復号の例

- 公開鍵を$(55, 7)$，秘密鍵を$(55, 23)$とする。
- 平文の数値「8」の暗号化
  - $8^7 = 2{,}097{,}152$を55で割ると商は38,130，余りは2であるから暗号文の数値は「2」
- 暗号文の数値「2」の復号
  - $2^{23} = 8{,}388{,}608$を55で割ると商は152,520，余りは8であるから平文の数値は「8」

25

公開鍵と秘密鍵の作り方

- 非常に大きな2つの素数pとqの積をnとする。
  - 例：$5 \times 11 = 55$
- $(p-1)(q-1)$と互いに素になる数としてeを選ぶ。(n, e) を公開鍵とする。
  - 例： $4 \times 10 = 40$と互いに素な数7→ $(55, 7)$
- eとの積を$(p-1)(q-1)$で割って1余る数としてdを求める。
  - 例： $7 \times 23 = 161$を40で割ると1余る。→ $(55, 23)$

26

RSA暗号の安全性

- 公開鍵から秘密鍵を求めることは事実上困難であるためRSA暗号は安全である。
- 困難な理由
  - 秘密鍵$(n,\ d)$のdを公開鍵$(n,\ e)$から求めるためには$(p-1)(q-1)$がわからなければならない。
  - そのためにはnを素因数分解してpとqを求めなければならない。
  - pとqが極めて大きな素数の場合，nを素因数分解するには高性能のコンピュータを用いても膨大な時間がかかり，事実上不可能

27

RSA暗号の課題と対策

- 暗号化と復号の計算に非常に時間がかかる。
- そこでRSA暗号で共通鍵を交換し，その後は共通鍵暗号で通信を行うことがよく行われる。
  - 鍵は短いので暗号化や復号は短時間でできる。

28

公開鍵暗号と共通鍵暗号の併用

29

今回学んだこと

1. ネットワークセキュリティの要素
2. ネットワークに対する脅威
3. 脅威に対する対策
4. 暗号とは
5. 共通鍵暗号AES
6. 公開鍵暗号RSA

30

コンピュータネットワーク

経営情報学部　システム情報学科
尾崎　博一

授業の計画(1/2)

1. 序論
2. ディジタル通信技術（1）
3. ディジタル通信技術（2）
4. 通信プロトコル
5. LAN（1）
6. LAN（2）
7. IPとルーティング（1）
8. IPとルーティング（2）

授業の計画(2/2)

9. TCPとUDP（1）
10. TCPとUDP（2）
11. インターネットサービスとプロトコル（1）
12. インターネットサービスとプロトコル（2）
13. ブロードバンド通信と移動通信
14. ネットワークセキュリティ（1）
15. ネットワークセキュリティ（2）
16. 期末試験

コンピュータネットワーク

第15回
ネットワークセキュリティ（2）

今回の到達目標

1. 電子署名とはどういうことか理解する。
2. 認証とはどのようなことか理解する。
3. 公開鍵暗号を用いる認証を理解する。
4. 公開鍵基盤とは何かを理解する。
5. セキュリティを実現するプロトコルを理解する。

電子署名（ディジタル署名）

- 紙の文書に署名や捺印を行うのと同様にネットワークを
  通して送る情報にも署名が必要な場合がある。
- 公開鍵暗号はそのために利用することができる。
  - 秘密鍵で暗号化（署名）を行う。
  - 公開鍵で復号し署名を確認する。
  - 秘密鍵で暗号化できるのは秘密鍵を持っている本人に限られる。
  - 公開鍵で復号し意味のある情報が得られた場合，それは秘密鍵の持ち主が作成したことの証明になる。

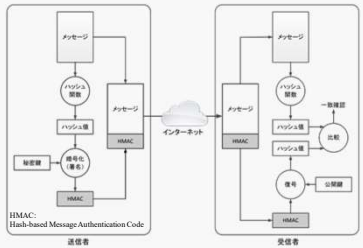
ハッシュ関数（hash function）

- 長いメッセージ全体に署名することは手間がかかり得策でない。
- メッセージを短い情報に要約し，それに署名を行う。
- ハッシュ関数はメッセージを固定長の短いデータ（ハッシュ値）に変換する。
  - 元のメッセージの中身が少しでも変わると出力されるハッシュ値が大きく変わるという性質を持っている。

ハッシュ関数の標準

- 従来はMD5（Message Digest 5）
  - 衝突（異なるメッセージから同じハッシュ値が得られる）の危険性が指摘され今では推奨されていない。
- 現在の標準はSHA（Secure Hash Algorithm）
  - ハッシュ値の長さ
    - SHA-1：160ビット
    - SHA-2：224，256，384，512ビットのいずれかを選択
    - SHA-1は危険性が指摘され現在では推奨されていない。

ハッシュ関数を用いる電子署名

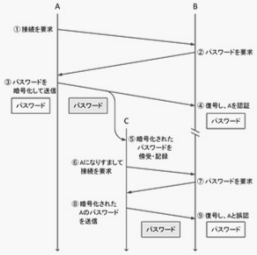


認証技術

- 通信相手が本当にその人本人であるかを確かめる技術
- パスワード（password）が用いられることが多い。
- パスワードは暗号化して送る必要がある。
- しかし，単に暗号化して送るだけでは不十分。
  - 暗号化されたパスワードが後で利用されてしまう。

10

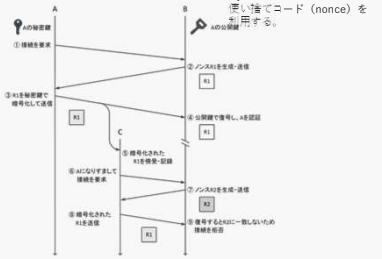
反射攻撃（リプレイアタック）



11

反射攻撃への対策

チャレンジレスポンス方式
使い捨てコード（nonce）を利用する。



12

公開鍵暗号方式の課題

- 公開されている公開鍵の持ち主が本当にその人本人であるかという問題
- 他人になりすまして自分の公開鍵を公開することが可能
  - それを信じた人はその公開鍵で暗号化した情報を送る。
  - 他人になりすましている当人は自分の秘密鍵でそれを復号
- なりすましを防ぐには公開鍵の認証が必要。

13

認証局（Certificate Authority: CA）

- 公開鍵自身を認証する信頼できる第三者機関
  - 公開鍵を証明する電子証明書（あるいはディジタル証明書）を
    発行する。
  - 認証局自身の公開鍵は広く公開されだれでも利用することができる。
  - 電子証明書
    - フォーマットはITU-Tの勧告X.509およびIETFのRFC 5280で標準化されている。
    - 認証局の秘密鍵で署名されている。
    - 公開鍵を印鑑とすれば電子証明書は印鑑証明書に相当する。

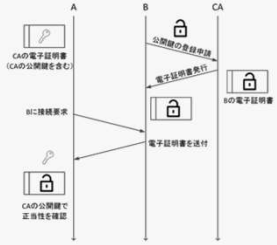
14

電子証明書の主な内容

項目	内容
版数	X.509の版数（最新は第3版）
シリアル番号	認証局が電子署名に付与する通し番号
署名アルゴリズム	認証局が電子証明書に署名する時に使用するアルゴリズム
発行者名	電子証明書を発行する認証局名
有効期間	電子証明書が有効である期間（開始日時と失効日時）
所有者	電子証明書が証明する公開鍵の所有者
公開鍵	上記所有者の公開鍵，暗号アルゴリズムおよびパラメータ
署名	認証局の秘密鍵による署名

15

電子証明書の登録と利用

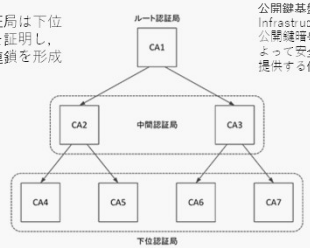


16

認証局の階層構造と公開鍵基盤

上位認証局は下位認証局を証明し，信用の連鎖を形成する。

公開鍵基盤（Public Key Infrastructure: PKI）：公開鍵暗号と電子署名によって安全な通信環境を提供する仕組み全体



17

プロトコルとセキュリティ

- データリンク層，ネットワーク層，トランスポート層の
  それぞれにおいてセキュリティを確保するための
  プロトコルがある。
  - データリンク層　　：無線LANのWPA
  - ネットワーク層　　：IPsec
  - トランスポート層　：TLS

18

WPA（Wi-Fi Protected Access）

- 無線LANにおいては盗聴の危険が大きいため，セキュリティの確保が極めて重要
  - 当初，WEP（Wired Equivalent Privacy）というプロトコルが使われていたが脆弱性が指摘され現在では使われていない。
- 現在はWPA2（Wi-Fi Protected Access 2）が広く使われている。
  - 暗号としてAESが用いられている。
  - さらにセキュリティを高めたWPA3も利用が始まっている。

IPsec（1）

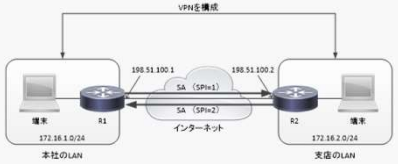
- ネットワーク層（IP層）における認証・暗号化のプロトコル
- VPNを構築するためによく利用される。
  - VPN（Virtual Private Network）とはインターネット上に構築されるセキュアな私設ネットワーク
- AH（Authentication Header）とESP（Encapsulation Security Payload）のふたつのプロトコルが含まれるが，一般にESPの方が広く用いられている。
  - IPsecのパケットにはトランスポートモード（transport mode）とトンネルモード（tunnel mode）というふたつの形態があるが，VPNではトンネルモードがよく使われる。

IPsec（2）

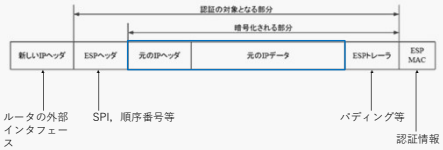
- 通信を始める前に送信元と宛先の間に論理的な接続関係SA（Security Association）を確立
  - SAは片方向の接続関係。双方向通信を行うには2つのSAを確立する必要がある。
    - SAの識別子をSPI（Security Parameters Index）という。
    - SAの属性
      - SPI，送信元，宛先，使用する暗号方式，暗号鍵，完全性確認の方法，認証鍵など

IPsec（3）

- IPsecを用いたVPNの例



IPsec ESPパケットの構成



TLS（1）

- Transport Layer Security
- トランスポート層における認証・暗号化のためのプロトコル
- もとになったプロトコルはSSL（Secure Sockets Layer）
  - TLSをSSLあるいはSSL/TLSと呼ぶこともあるが本来のSSLとは互換性がない。SSLは今では推奨されていない。
- 最新版はTLS1.3

TLS（2）

- 2つのソケット間で安全なコネクションを確立する。
- プロトコルの階層としてはトランスポート層（TCP）とアプリケーション層の中間に位置する。
- TLSハンドシェイク
  - TCPコネクションの確立後にクライアント・サーバ間のセキュリティパラメータの交渉，クライアントによるサーバの認証等が行われる。
    - 片方向ずつ共通鍵（暗号化）と署名鍵を使用。鍵は合計4本。
  - クライアント・サーバ間で基本的に2往復（2RTT）の通信が必要となる。

TLS（3）

- TLSを用いる場合の宛先ポート番号

ポート番号	元のプロトコル名	目的	ポート番号	TLSを用いるプロトコル名
20	FTP（データ）	ファイル転送	989	FTPS（データ）
21	FTP（制御）		990	FTPS（制御）
23	TELNET	リモートログイン	992	TELNETS
25	SMTP	電子メール送信	465	SMTPS
80	HTTP	Web閲覧	443	HTTPS
110	POP3	電子メール受信	995	POP3S
143	IMAP4	電子メール受信	993	IMAPS

今回学んだこと

1. 電子署名とは
2. 認証とは
3. 公開鍵暗号を用いる認証
4. 公開鍵基盤とは
5. セキュリティを実現するプロトコル
   1. WPA
   2. IPsec
   3. TLS