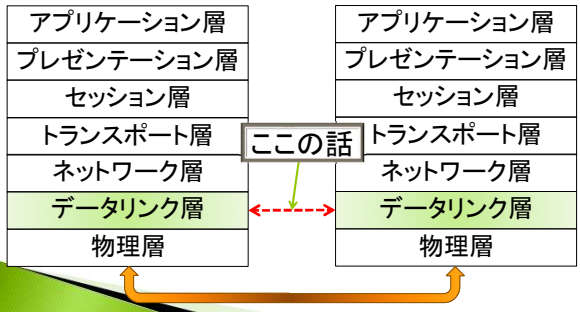
データリンク層

花田　英輔

1

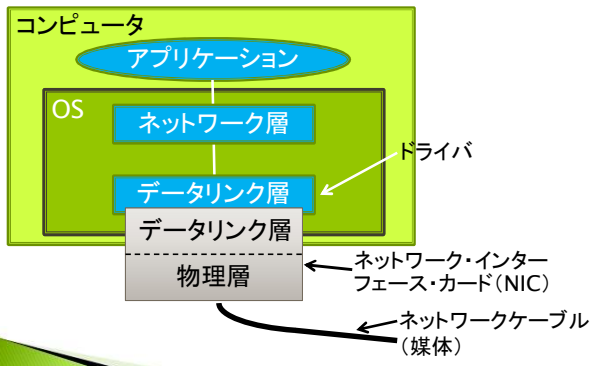
データリンク層（OSIモデル第2層）

- 物理層はビット列の送受信
- データリンク層はフレーム単位での送受信



2

第1層と第2層の実装形態



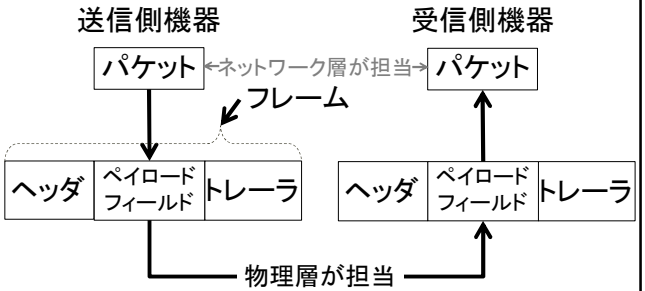
3

データリンク層がすること

1. 物理層（第1層）とネットワーク層（第3層）に対してインターフェースを提供する
   - データ形式において次の変換を行う
     - 「フレーム」と「パケット」の変換（第2層vs第3層）
     - 「ビット列」と「フレーム」の変換（第1層vs第2層）
2. 伝送誤りに対応する
3. データの流れを制御する
   - 遅い受信者が早い送信者のデータで溢れることが無いように

4

フレームとパケット



5

フレームのフォーマット(例)

1）イーサネット(DIX)

	プリアンブル	宛先アドレス	送信元アドレス	タイプ	データ	パッド	チェックサム
バイト	8	6	6	2	0～1500	0～46	4

2）IEEE802.3（SFD(Start Frame Delimiter)：1バイト）

	プリアンブル	SFD	宛先アドレス	送信元アドレス	長さ	データ	パッド	チェックサム
バイト	8		6	6	2	0～1500	0～46	4

- プリアンブル：データの開始を示す記号
  - 1~7バイトは10101010、8バイトのみ10101011
  - クロックの同期に使用される

6

ビットとフレーム（物理層とのインターフェース）

- 物理層からはビット列を受け取る
- いかにビット列からフレームを取り出すか？
  - （重要条件）
    - フレーム毎に長さと構造（データ順）は決まっている
  1. ヘッダから情報を取り出す
  2. フレームの終わりを知る
  3. 終わりまで受信して組み立てる
  4. 誤りが無いか確認する
- ビット列は必ずしも正しく届くとは限らない
  - ビットが反転して届く可能性はある

7

フレーム取出し手法の例

A) チェックサムの利用
- バイト単位のデータを用いて計算で得る「チェックサム」について、受信データから計算した値と受信した値で比較する
  - 一致すればデータは正しい、不一致ならエラー有

B) ベッダ内のバイト数を利用
- ヘッダ内（先頭）にフレームのバイト数を入れることにしておく
  - 数値が正しければOK
  - 正しくないと次のフレーム長がおかしくなる

8

チェックサム(Check sum)

- 入力されたデータ列の誤りを検出する手法
- データの最後にデータの合計値(Sum)を付け加え、データから算出された値と比較することにより誤りの有無を検出する
  - 総計のどのビット群を符号値とするか、符号値をどのように扱うかなどで、派生した種類がある
- 調べる対象が数字のみの場合はチェックデジット(Check Digit)を用いる方が信頼性は高い

9

チェックサムの使用例（もっとも単純な場合）

- ワード列の個々のワードの総計(sum)の下位1ワードをそのまま符号値とする
  - 1ワードを何ビットとするかは実装によって異なる

例）
- 8ビットのワード列「00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F」の総和は「78」であるので、そのチェックサムは「78」

10

IPパケットに応用した場合の例 (Wikipediaより)

1. IPヘッダのチェックサムフィールドにゼロをセット
2. IPヘッダを16ビット単位で加算
3. 総計の下位16ビットの補数をIPヘッダのチェックサムフィールドへセットして送信
4. 受信側でIPヘッダを16ビット単位で加算
5. 総計がゼロなら正常
   - チェックサムフィールドにはチェックサムフィールドがゼロの場合のチェックサムの補数がセットされているので、ゼロになれば正しい
   - 総計＝チェックサムフィールド以外のチェックサム＋チェックサムフィールド以外のチェックサムの補数

11

チェックデジット付与手法の例

- JAN体系（13ケタ）
  - 構成

    企業コード＋商品アイテムコード＋チェックデジット

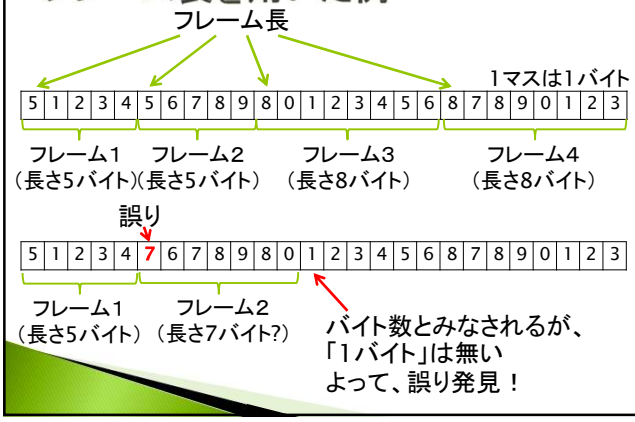
    右の例）
    - GS1事業者コード (JAN企業コード): “456995112”
    - 商品アイテムコード:"619“
    - 算出方法「モジュラス10/3ウェイト」

1. 事業者コードと商品アイテムコードを連続した数列作成
   - 今回の例:“4569951126l9”
2. 偶数桁の数値の和を求める
   注:数列の偶奇は右から数える
   - 4+6+9+1+2+1=23
3. 奇数桁の数値の和を求め、結果を3倍
   - (5+9+5+1+6+9)*3=105
4. 2の結果と3の結果の和を求める
   - 23+105=128
5. 4の結果の下1ケタを10から引いた結果がチェックデジット
   - 10-8=2

- この場合のチェックデジット:”2”
  - 結果が0ならチェックデジットは0
- コード全体:”4569951126192”
  - バーコードではこの結果をコード化

12

フレーム長を用いた例



13

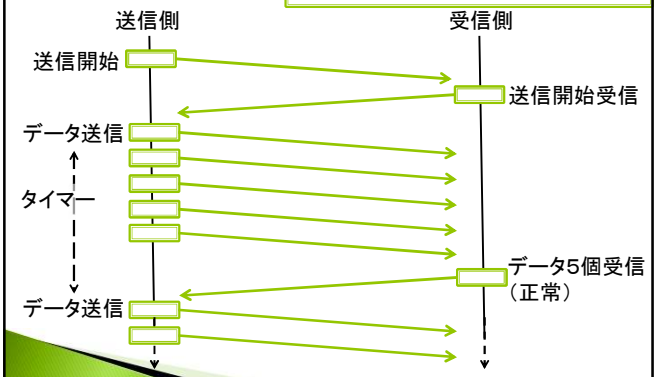
誤りの制御

- 受信したビット列に誤りを発見したらどうするか？
  → フレームを再送させる！（受信側では修復しない）
- といって、再送が多いとネットが混む
- 同じデータを2回以上受信する可能性も
- 受け取ったかどうかわからなくなるかも
  → 受信側から「受信確認」のデータを送信
  → 送信側にタイマーを仕掛ける

14

受信確認の例

- 次の場合は再送開始
  - 「正常」が来ないとき
  - 返事が無いままタイマー時間切れ



15

誤り検出

- 送信の際に、余分なデータ（バイト）を加えることで、受信者が受信データに誤りがあるか否かを判断させること
  1. 誤り検出符号（Error Detecting Code）
     - 受信データに誤りがあることを検出可能にするための情報（→結果、再送を要求する）
  2. 誤り訂正符号（Error Correcting Code）
     - 受信データに誤りがあることを検出し正しいデータに修正可能にするための情報

16

誤り検出符号

- 誤り率が低い伝送路（光ファイバ等）向け
  - 次のような技術がある
    - パリティ
      - 偶数パリティ、奇数パリティ
    - チェックサム
    - 巡回冗長検査（CRC）
    - 多項式符号

17

パリティ

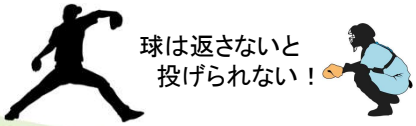
- データと共に「パリティ・ビット」（Parity Bit）を付加して送信
- パリティビットの決定法
  - 偶数パリティ：データ内の「1」のビット数が偶数→0
  - 奇数パリティ：データ内の「1」のビット数が奇数→0

例）
- データが1011010の時のパリティビットは？
- データ内の「1」のビットの数は4個（偶数）である
  → 偶数パリティの場合は0、奇数パリティの場合は1
  よって（偶数時）送信データは10110100
  （「偶数であること」を保っている）

18

データの流れ(フロー)の制御

- 送信側は受信側の状態を気にしない
→ 受信しきれないうちに送信しようとする
- 2つの方法がある
  1. フィードバックに基づく制御
  2. 速度に基づく制御(この層では行わない)
- 「フィードバック」は先に例示した「受信確認」ルールを適用することで実現可能



19

データの衝突と対策

- 送信側はタイミングを考えずに発信する
- データ搬送経路(通信路)は共有である
→ データの衝突(collision)が発生する！
- 考えられる対策
  - とにかく待つ
  - 通信路を常に占有制にする
  - 通信路を時間で区切り、区切られた時間だけ占有制にする

20

衝突回避手法

- 主な衝突回避手法
有線
  - 1-persistent CSMA
  - Non-persistent CSMA
  - P-persistent CSMA
  - CSMA/CD
    - CSMA:Carrier Sense Multiple Access
    - CD:(with) Collision Detection

無線
  - MACA(Multiple Access with Collision Avoidance)

21

CSMA/CD

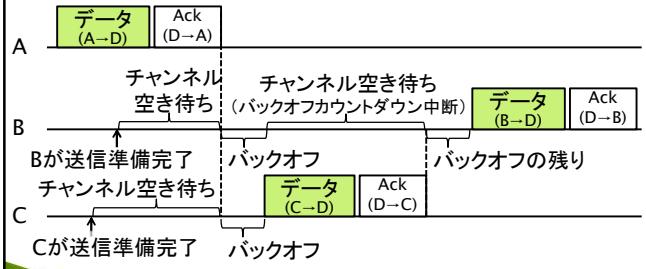
(Carrier Sense Multiple Access with Collision Detection)

- 通信路を3つの状態で管理する
  - 転送期間、競合期間、アイドル期間
- 転送期間:フレームが転送されている期間
- アイドル期間:何も転送されていない期間
- 競合期間:2つ以上の発信元が同時に送信を開始した場合
衝突が検知される
→すべての送信を停止
→ランダムな時間長だけ待つ
→再び送信開始

22

CSMA/CDを用いたデータ転送

- 仮定) B、Cがそれぞれ勝手にDにデータを送ろうとする場合



バックオフ:待ち時間、それぞれランダムに設定され、アイドル状態になるとカウントダウンを開始する

23

CSMA/CA

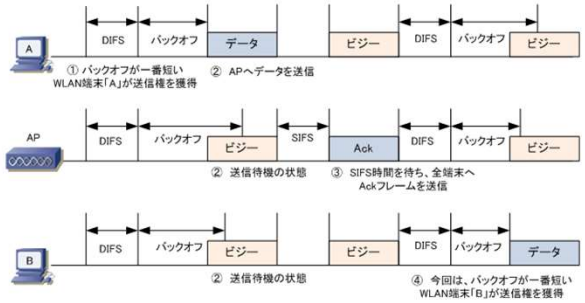
(Carrier Sense Multiple Access with Collision Avoidance)

- 無線LAN(IEEE802.11a/b/g)で使用
  - 無線LANでは「衝突」を検知できない
- 以下の手順で通信
  1. DIFSと呼ばれる時間において電波を検知しなければ、電波上で信号が流れていないと判断
  2. ランダムな時間(バックオフ)待ってデータ伝送開始
  3. APから端末へと送信されるAckはSIFSと呼ばれる時間を待った後に送信
  4. Ackのやりとりでデータの信頼性向上
    - Ackがなければ通信障害とみなしてデータ再送信

DIFS	ビジー状態のチャネルから信号が検出されなくなり、アイドル状態に移行したと判断されるまでの時間
SIFS	フレーム送信間隔における最短の待ち時間

24

CSMA/CA



- IEEE802.11a/b/gは半二重通信
  - ある瞬間にAPが通信している端末は1台だけ
  - 複数端末と同時に通信しているように見えるが、実際は複数の通信を順番に実施

25

今回の課題

1. 誤り「検出」符号と誤り「訂正」符号の違いを述べよ
2. CSMA/CDについて説明せよ
3. 本日の感想

- 締切：12月11日(月) 18:00
- 本講義に関する情報は(この講義資料も)次のWebpageに掲載するので、時々参照すること
  http://www.ai.is.saga-u.ac.jp/~hanada/DCT/

26