



コンピュータ基礎(10)

11章 通信ネットワーク

ネットワーク（通信網）の発展




- 昔：コンピュータは単独で用いられてきた
 - コンピュータのある部屋へ行き、使う。
 - データは記録メディアに入れて持っていく など。
- ネットワークの普及
 - 1990年代「パソコン通信」と言われていた時代は、電話回線で（電話をかけて）通信をしていた。とても低速で、画像を送るのには時間がかかった。（1秒間に1200bit - 9600bitぐらい）
 - 建物内のネットワークは、企業では1990年代、家庭などでは2000年に入ってから普及してきた。
 - 自宅などに高速回線（いわゆる、ブロードバンド）を引くようになったのは2000年代になってから。

ネットワークの種類

-  (Local Area Network)
 - 構内通信網という。建物内（企業、家庭など）でコンピュータを相互に接続するのに使う。
 - 有線のもの、無線のもの（無線LAN）がある。
 - インターネットに対し**イントラネット**と呼ばれることもある。
-  (Wide Area Network)
 - 広域通信網という。LAN同士をつなぎ、広い地域で通信を行う。いわゆる「**インターネット**」。




通信サービスの種類

-  交換サービス
 - 電話のように相手との回線を接続する方式。
 - 携帯電話でいうと、通話中の状態。接続されている時間で通信料金が決まる。
-  交換サービス
 - 通信を「**パケット**」と呼ぶ小さなかたまりに区切って、1つ1つ宛先に届ける方式。
 - 携帯電話でいうと、メールなどの通信に使われている。料金はパケット数で決まる。
-  サービス
 - 企業内などで、特定の区間で回線を専用使用する通信の方法。

インターネット回線の種類

- ADSL
 - 電話回線に、インターネットの信号を重ねて送る方法。もともと音声用に敷設された回線を使うので、電話局から遠いと通信ができなかったり遅くなったりする。
- FTTH (Fiber to the home)
 - 光インターネット。家庭まで光ファイバーケーブルを新しく敷設して通信する方法で、速度が速い。
- モバイル通信
 - 携帯電話の回線（無線）などを用いて通信する方法。
 - 自由に移動することができる反面、遅くて、通信料金が安い。
- その他
 - ケーブルテレビの回線を流用する方式など。


転送速度について

- 転送速度の単位
 -  (bits per second) 1秒あたりに何ビットのデータを転送できるか。
 - kbps, Mbps, Gbps という単位もよく使われる。
- 例題
 - 1MBの画像ファイルを1Mbpsの回線で送ると何秒かかるか？
 - 1MB（1Mバイト）は8Mbitである。
 - 8Mbitを1Mbpsで転送すると、8秒かかる。

転送速度の例

- 音声通話は、概ね 8kbps 程度で良い (携帯電話)
- 音楽は、100kbps程度が多い(MP3など)
- 映像では、ワンセグ放送が128kbps
地上デジタル放送が15Mbps
- 無線LANは11Mbps~1.3Gbps
- 有線接続(LAN, USBなど) は10Mbps~1Gbps
- 実際の通信では
 - 送りたいデータそのものの他に、通信の宛先や誤り訂正のための情報なども入っているので、より長い時間がかかる。
 - プロトコルオーバーヘッドと呼ぶ。
 - 無線通信では電波状況が悪いと誤りが増えたり、再送信が行われたりして効率が非常に悪くなることもある

LANについて

- ・ 機器間のつなぎ方 (教科書p137参照)
 - 現在はスター型が広く用いられ、バス型・リング型はほとんど用いられていない。
- 伝送媒体
 - 有線 (ケーブル) 現在は 1Gbps (1ギガビット毎秒) の速度のものが普及している。
 - (Ethernet) という規格のものが使われている。
 - ケーブル同士は、ハブに接続して使う。その他、中継装置として、リピータ、ルータ、ゲートウェイなどがある。
 - 無線 (WiFi, IEEE802.11) 有線よりは遅く、11Mbps のものが多かったが、最近では100Mbpsを超えるものも増えてきた。

インターネット

- インターネットのサービス
 - **電子メール** hiura@hiroshima-cu.ac.jp のようなメールアドレスで通信相手を特定し、通信できる。
 - **Web(WWW)** 閲覧するページを表す文字列を という。www.hiroshima-cu.ac.jp など。
 - 前に http://などを付けることがあるが、これは通信方式 () を表す文字列である。
- 通信方式について
 - http のほかに、ftp (データ転送プロトコル。自分のホームページにファイルを掲載するときに使う) や smtp (メール送信のときに使われるプロトコル) など、多くの **通信規約 (プロトコル)** が定められている。


IPアドレスについて

- とは?
 - インターネットに直接接続されたコンピュータに与える 32bit の番号 (IPv4)。枯渇しかかっている。
 - 最近では 128bit にした への置き換えが進んでいる。
- - IPアドレスは記憶するのが難しいので、組織などに名称を付けることができるようになった。
 - www.hiroshima-cu.ac.jp のように、. で区切っていく。
 - ネームサーバ (**DNSサーバ**) に問い合わせると、ドメイン名とIPアドレスを相互に調べることができる。電話帳のようなもの。

コンピュータ基礎(11)

12章 情報セキュリティ

情報セキュリティとは?

- セキュリティを考えるための要素
 - 保護すべきもの (データ、システム)
 - 保護すべきものを脅かすもの ()
 - 保護すべきものを守る手段 (セキュリティ)
- 脅威の種類
 - 自然災害・天災 (地震、台風、洪水など)
 - 火災
 - 破壊 (建物・コンピュータ・データを故意に壊す)
 - 不正行為 (コンピュータ犯罪、改ざん、盗聴、なりすまし、漏えい、複製、抹消など)
 - 過失 (ミスによる様々な損失)
 - いたずら (侵入やコンピュータウイルスなど)

脅威と脆弱性

- **脅威**
 - [] ・ 他人の名前やID、パスワードを使う。
 - パスワードは、コンピュータの欠陥（脆弱性）について取得する他に、誕生日や子供の名前を調べるなどの**ソーシャルエンジニアリング**も用いられる。
 - [] ・ 正常なネットワーク通信が出来なくなるよう、大量のアクセスを行うなど。
 - [] ・ [] ・ 悪意を持って作られたプログラムで、他のコンピュータに入り込んだり、自己増殖したりする。
- **脆弱性**
 - **バグ** ・ プログラムのミス。
 - [] ・ バグや設計の不備により、侵入を許してしまうような欠陥のこと。

悪意で作られたプログラム

- []
 - 何らかの役に立つプログラムのように見せかけて、実は悪意を働くプログラム。パスワードを盗む、不正侵入経路（バックドア）を作る、など。
 - トロイア戦争（ギリシア神話）の木馬の故事から。
 - 中に兵士が入っている。敵が城に運び入れた後、夜に兵士が出てきて敵を滅ぼした。

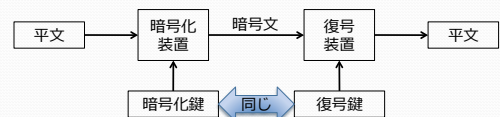


IDとパスワードについて

- **厳重に管理を！**
 - 絶対に他人に教えてはいけない
 - パスワードは、生年月日、英単語などではいけない
 - 辞書を使った攻撃によって簡単に破られる
- **より強固なセキュリティのために**
 - **ワンタイムパスワード**
 - 1度限りのパスワード。
 - 時間によってパスワードが変わるもの
 - 携帯電話にメールで送られてくるもの
 - **生体認証**
 - 指紋、虹彩、静脈パターンなど、体の特徴を用いて認証する

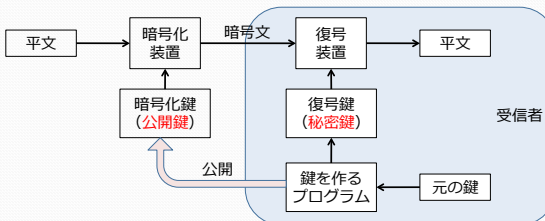


暗号化(1)



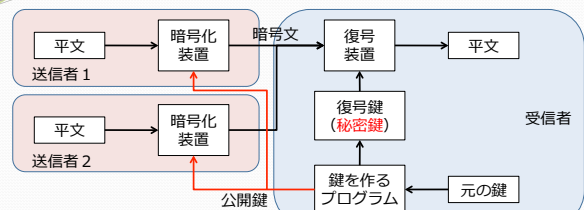
- [] **暗号方式**
 - **暗号化鍵と復号鍵が同じ**
 - お互いの持つ鍵を秘密にしておく必要がある
 - 鍵を相手へ「秘密に」届ける方法が問題となる。もし鍵が漏れると、他人が復号できてしまう（メッセージを読まれてしまう）。
 - 通信相手が増えると、鍵がその分増えてしまう。

暗号化(2)



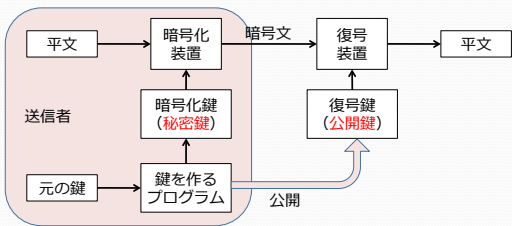
- [] **暗号方式**
 - 2個セットの鍵を作成し、暗号化鍵を公開する
 - 復号鍵は受信者から外に出ないので、復号鍵（秘密鍵）を盗まれる危険性が低く、安全性が高い

暗号化(3)



- **公開鍵暗号方式では**
 - 複数の送信者が同じ鍵でそれぞれ秘密のメッセージを送信できる。受信者以外は復号出来ない
- **問題点**
 - 公開鍵を手入れすればだれでも送信できるので、送信者を特定できない（偽情報を送ることができてしまう）
 - 他人が受信者になりすまして、偽の鍵を公開して情報を盗み出す危険がある→認証局の必要性

デジタル署名



- []
- 復号鍵をあらかじめ公開しておく。誰でも復号できる。
- 暗号化鍵は秘密なので、他人が同じ暗号データを作ることができない (本人が作ったデータであることが確か)

セキュリティを高めるために

- パスワードの管理の徹底
- [] の導入
 - 指紋, 光彩, 静脈パターン, などの身体情報を用いる。
- [] の設定
 - 許可されていない人には重要なデータを操作できなくするなど。情報処理センターの計算機でも。
- []
 - 通信経路の途中に設置するもので、通信内容に不正なものがないか进行检查し、不正なアクセスは遮断する。
- ウィルス対策
 - [] を導入し、**ウィルス定義**を定期的に更新する。
- 通信の暗号化