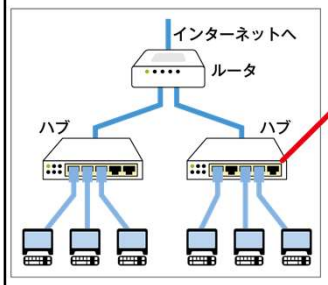
ネットワークの接続機器等

関連：pp.104-105



・**接続機器等の名称**

ルータ
ネットワーク同士を接続する装置

ハブ（集線装置）
ネットワーク内で機器を接続する装置

プロバイダ（ISP）
インターネット接続業者

IPアドレス・ドメインネームシステム

関連：pp.108-109

IPアドレス v4	インターネット上の住所（4つの8ビット数）
IPのバージョン	IPv4：32bit（8bit×4個を**ドット**で区切って表す） IPv6：128bit（16bit×8個を**コロン**で区切って表す） IPv6の記述例　20c1:0db8:bd05:01d2:288a:1fc0:0001:10ee
ドメイン名	文字列による名前　202.214.194.138 ←IPアドレス www.kantei.go.jp ←ドメイン名
DNS	IPアドレスとドメイン名を対応させる仕組み

w w w . k a n t e i . g o . j p

コンピュータ名　組織名称　組織種別　国名

第4レベルドメイン　第3レベルドメイン　第2レベルドメイン　トップレベルドメイン

www . example . co . jp

http://example.co.jp/を本体としたとき，http://sub.example.co.jp/ の下線の部分をサブドメインという。

電子メールアドレス

関連：pp.108-109

jouhou@kobe-hs.ed.jp

ユーザID（アカウント）　ドメイン名（IPアドレス）

本人確認のために［パスワード］が使われる。

SMTP	メールの送信・転送用プロトコル（ひたすらバケツリレー） Simple Mail Transfer Protocol
POP (POP3) IMAP	メールを受信のためのプロトコル（本人確認等） Post Office Protocol Version3 Internet Message Access Protocol

共通鍵暗号と公開鍵暗号　（仕組みのイメージ）

関連：pp.110-111

共通鍵暗号方式
- 同じ鍵を送り手と受け手の両方がもつ。
- 暗号化と復号では同じ鍵を使う。

問題点：鍵を受け手に安全に渡さなければならない。

錠・錠前

公開鍵暗号方式
- 二つの鍵（**秘密鍵**・**公開鍵**）を用意する。
  - **秘密鍵**で暗号化：**公開鍵**でなければ復号できない。
  - **公開鍵**で暗号化：**秘密鍵**でなければ復号できない。

公開鍵　誰に渡してもよい。

秘密鍵　自分専用。

問題点：本当にその人の公開鍵か？

ハイブリッド暗号方式（例：SSL/TLS）

関連：pp.110-111

① 共通鍵暗号方式：処理が速い
② 公開鍵暗号方式：鍵の管理は容易になるが処理が複雑

SSL/TLS
Secure Socket Layer
Transport Layer Security

最初だけ②の方式を利用して①用の鍵を渡す。
以降，①で暗号化して通信する。

- URLが https://・・・ならば，**SSL/TLS**が使われている。

現在使用されているのは**TLS**だが，SSLのみの表記も多い。

通信の暗号化

MEMO　通常のURLはhttp://で始まるが，入力内容が暗号化されるWebページはURLがhttps://になっている。

次は暗号の応用へ・・・

ディジタル証明書（電子証明書）

関連：pp.110-111

問題点：CがAだと名乗って**秘密鍵**を作り，その**公開鍵**をAの**公開鍵**だと偽る。

解決策：区役所の印鑑登録・印鑑証明と類似の方法。

認証機関（認証サーバ）　⇨　**公開鍵**が本人のものであることを，第三者が確認・証明するしくみ。

ディジタル証明書（電子証明書）　⇨　認証機関が発行した証明。

このしくみを**公開鍵（認証）基盤**（**PKI**：public key infrastructure）等という。