情報の伝達と通信 (その 2)

山本昌志*

2007 年 11 月 7 日

概 要

情報通信の基本的な仕組み，インターネットの通信方法，誤りがある通信路について学習する．

1 本日の学習内容

現代の情報の通信方法についてが学習する．

- プロトコルの役割が分かる．
- 公開鍵方式の暗号とデジタル署名の方法が分かる．
- 情報ネットワークの方式とインターネットでの情報の伝達が分かる．

教科書 [1] の pp.46–70 が本日の範囲である．

2 情報通信

2.1 プロトコル

2.1.1 プロトコルの必要性

ネットワークを使って，コンピューター同士が通信を行うときの約束事をプロトコルと言う．コンピューター同士，融通の利かない機械同士が通信を行うため，双方がプロトコルを守らないと，通信ができなくなってしまう．別の言い方をすれば，プロトコルさえ守っていれば，良いと言うことになる．

一般に，プロトコルはプログラムあるいはネットワークのインターフェースで決められる．例えば，2 つのプログラムが通信する場合，それぞれの送信/受信データに約束事が決められる．二つのプログラムのインターフェースは，それぞれのデータが担う．

プロトコルをしっかり決めると，入り口と出口を規約通りに作ればよい．中身は設計者の自由にできる．また，他のプログラムのことに関心を払う必要もない．

*独立行政法人　秋田工業高等専門学校　電気情報工学科

2.1.2 アプリケーションとプロトコル

コンピューターを用いて通信を行う場合，普通 2 つのプログラムを動作せせる．情報を要求する方をクライアント (プログラム)，情報を提供する側をサーバー (プログラム) と言う．これらの 2 種類のプログラムが相互に通信を行い，情報の受け渡しを行う．

2 つのプログラムが協働して情報の伝達を行うことは，人間同士の会話による情報伝達と似ている．人間同士での会話では，双方が理解できる同じ言語を使って情報伝達を行うのと同様に，コンピューターのプログラム—サーバーとクライアント—も同じ言語で話さなくてはならない．

その言語の仕様みたいなものが，アプリケーションプロトコルである．インターネットでサービスを行うサーバープログラムでは，このプロトコルがきちんと決められている．例えば，WEB の文書は W3C と言う組織が決めている．クライアント，およびサーバーのプログラムを開発する場合，このプロトコルを守らなくてはならない．守らないプログラムは，どんなに良くてもだれも使わないだろう．

2.1.3 プロトコルと階層

さまざまな方法でインターネットに接続して，通信することができる．分かりやすい例だと，いろいろなケーブルを使うことができる．多くの場合ツイストペアが使われているが，光ファイバーや同軸ケーブルなども使える．ケーブルばかりではなく，通信の機器にはハブやルーターなども使っている．ハードウェアーのみならず，ソフトウェアーもいろいろある．

これら，さまざまな方法で通信可能な場合，それぞれに合わせて，コンピューター間の接続方法を決めていては，手間; コストがかかる．たとえば，5 種類のケーブル，3 種類の通信機器，8 種類のソフトウェアーがあると，合計 $5 \times 3 \times 8 = 120$ 種類の接続の組み合わせがある．これでは大変である．また，新しい技術が開発される都度，新たに仕組みを考えなくてはならない．

ネットワークの機能をモジュール化することにより，これらの問題が解決できる．それぞれの階層—ここの例ではケーブル，通信機器，ソフトウェアー—で入り口と出口の規格を決める．要するに，入り口と出口のみを決め，それを守ればどのような機器，ソフトウェアーも使えるようにするのである．コンピューターの通信では，通信の入出力は通信のプロトコルとして決められている．

ネットワークの機能のモジュール化では，OSI 参照モデルがよく引き合いに出される．それを表 1 に示す．ネットワーク必要なものがモジュール化されていることが分かる．上位と下位の層 (モジュール) では，データの受けた渡し方法をきちんと決める．

この OSI 参照モデルは，各種の試験によく出題される．「**物**で**ねーと**，**せっ**かくの**プレゼント**も**あ**りがたくない」と覚えるとか [2].

表 1: OSI 参照モデル．役割は，主に文献 [3] から引用．

層 (レイヤ)		役割
第 7 層	アプリケーション層	プログラムの API．アプリケーション間のデータのやりとりを行う．
第 6 層	プレゼンテーション層	データ翻訳/変換．プロセスで扱うデータの型や符号を，共通のものに変換あるいは逆変換する．
第 5 層	セッション層	通信プログラム同士がデータの送受信を行なうための仮想的な経路 (コネクション) の確立や解放を行なう．
第 4 層	トランスポート層	相手まで確実に効率よくデータを届けるためのデータ圧縮や誤り訂正，再送制御などを行なう．
第 3 層	ネットワーク層	相手までデータを届けるための通信経路の選択や，通信経路内のアドレスの管理を行なう．
第 2 層	データ層	通信相手との物理的な通信路を確保し，通信路を流れるデータのエラー検出などを行なう．
第 1 層	物理層	データを通信回線に送出するための電気的な変換や機械的な作業を受け持つ．ピンの形状やケーブルの特性，LAN カードなども第 1 層で定められる．

2.2 通信の秘密と相手の認証

途中でデータが盗まれないようにするためには，暗号が必要である．また，本人を証明するために，デジタル署名が必要である．

2.2.1 共通鍵暗号と公開鍵暗号

共通鍵暗号 (common key cryptosystem) 方式は，送信者と受信者が同じ鍵を使う方式である．送信者が平文を共通鍵で暗号化し，受信者は同じ鍵で復号する．かなり複雑な共通鍵が使われたりしたが，見破られる可能性が高い．

1975 年までの暗号は全て，この共通鍵暗号方式であった．ドイツの有名なエニグマもこの共通鍵方式であった．ただ，複雑かつ頻繁に鍵を変えていたので，なかなか暗号解読ができなかったが，第二次大戦末期には解読していたようである．

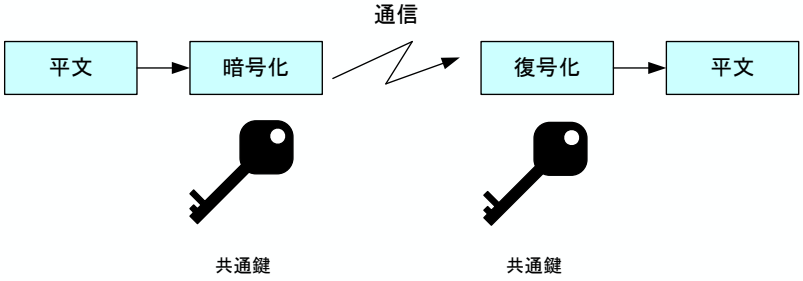

図 1: 秘密鍵暗号方式．暗号化と復号化には同じ秘密鍵を用いる．

暗号化と復号で異なる鍵を使う方法が公開鍵暗号 (public key encryption system) である．メッセージを受け取りたい方は，公開鍵を公開する．この鍵は誰でも使うことができる．メッセージ (平文) を送る側は，この公開鍵で暗号化して，暗号化されたメッセージを送る．この暗号化されたメッセージは公開鍵では復号することができない．唯一，復号ができるのは受信者が持っている秘密鍵だけである．

このようなことが技術的に可能なのか?—という疑問が湧くだろう．大きな数の因数分解が困難であることを利用した RSA 暗号がこの公開鍵方式となっている．詳細は，省略．興味のある者は調べよ．

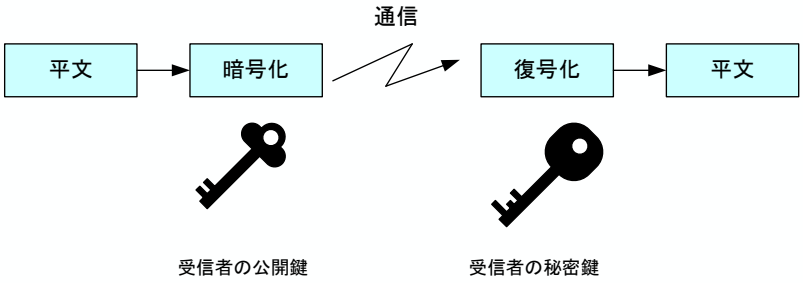

図 2: 公開鍵暗号方式．受信者の公開鍵をもしいて暗号化し，受信者の秘密鍵を用いて複合化する．

2.2.2 デジタル署名

現在，デジタル化されたデータは世界中のコンピューターを伝って，伝達が行われる．そんため，途中で容易にデータの改ざんができる．そもそも，デジタルデータは容易に改ざんできるものである．

デジタル署名では，通信の途中でデータの改ざんが分かる．デジタル署名は，次のようにする．

送信者　本人が確かに書いたと証拠を示して送信する必要がある．

- メッセージを一方向ハッシュ関数にとおして，ハッシュ値を得る．このハッシュ値を電子指紋に使う．メッセージが変わればハッシュ値が変わる．メッセージを操作して，任意のハッシュ値を得ることは

できない．したがって，メッセージの改ざんが行われれば，ハッシュ値が変わる．

- 得たハッシュ値 (電子指紋) は，送信者の秘密鍵で暗号化する．
- 送信者は，暗号化されたハッシュ値 (電子指紋) とメッセージを送信者に送る．

受信者　途中で改ざんが行われていないことを確認しなくてはならない．

- 暗号化されたハッシュ値 (電子指紋) を送信者の公開鍵で復号し，ハッシュ値を得る．
- 送られてきたメッセージを一方向ハッシュ関数に通して，ハッシュ値を得る．
- 二つのハッシュ値を比較する．この値が異なれば，途中で改ざんが行われたことになる．

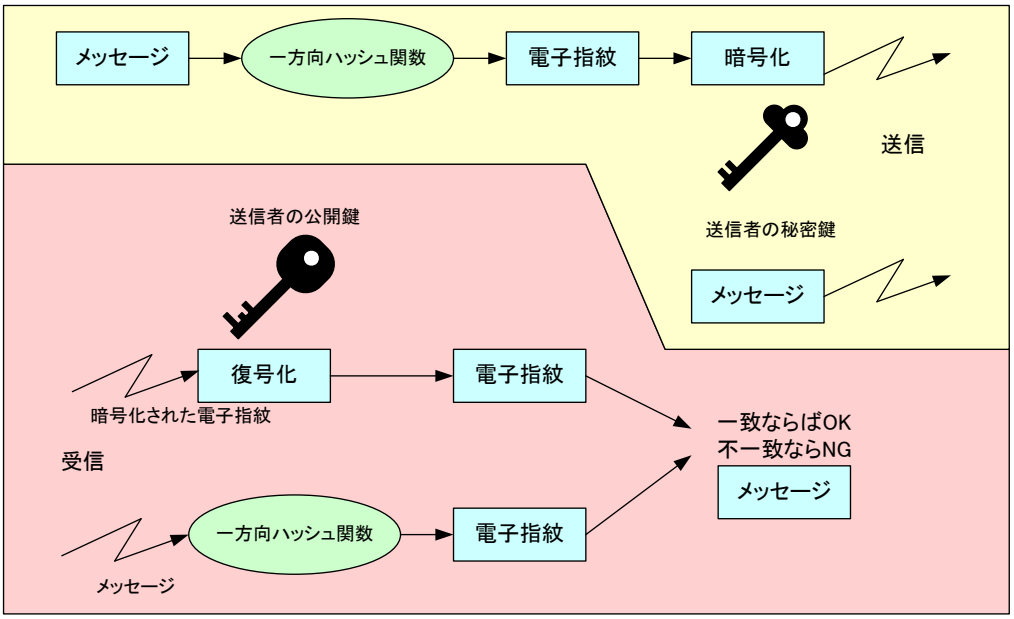

図 3: デジタル署名．途中でデータが改ざんされると，電子指紋が変化する．

3　インターネット

3.1　概要

インターネットは，世界中のコンピュータが接続されている巨大なネットワークである．現在，コンピューターの通信は，ほとんどインターネットを使っている．

1969 年，冷戦下に軍事攻撃から通信網を守るために開発された「ARPANET」から始まった．1 箇所にネットワークのコントローラーがあるシステムだと，そこが攻撃されると，システムは停止してしまう．そ

れを防ぐために，分散型の通信網を作った．今のインターネットも分散型で，一部のシステムが故障しても通信は可能である．

その後，1986 年には軍事用の ARPANET から分割さたので，大学を中心に学術研究用のネットワークが構築され始めた．1991 年，CERN のバーナーズ・リーにより World Wide Web(WWW) を開発し，その後のインターネットの普及に礎を作った．1995 年に Windows 95 が発売されると，大学のみならず，一般家庭でも爆発的にインターネットが使われるようになった．

インターネットでは，図 4 コンピューターやハブ，ルーターなどが通信線路で相互に接続されており，それらを通してコンピューター間でデータの交換が出来るようになっている．全体を見渡すと，接続はクモの巣 (web) のようになっている．

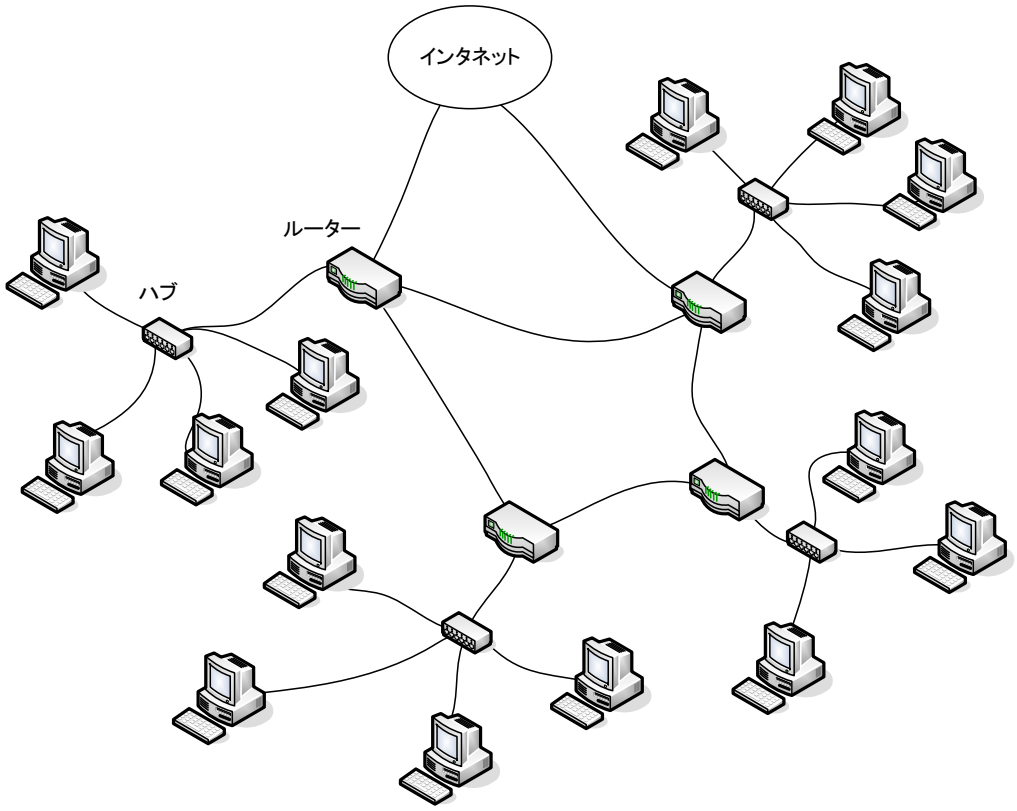

図 4: インターネットの全体像．インターネットはコンピューターとハブ，ルーターなどが通信線路で接続されている．

3.2 IP アドレスとの対応づけ—DNS

3.2.1 ホスト名

IP アドレスはコンピューターにとって，都合が良いが，人間には扱いにくい．IP アドレスの実態は，32 桁の 2 進数である．これはコンピューターにとって，非常に都合が良い．それを 8 桁毎に区切って，表示

しても，人間にはわかりにくい．そこで，IP アドレスと対応したホスト名が使われる．以下に，同じコンピューターを表す IP アドレスとホスト名を示す．

IP アドレスを 32 桁 2 進数で表現	11001010110111000000001100111100
IP アドレスを 2 進数の 8 桁毎に区切り 10 進数で表現	202.220.3.60
ホスト名で表現	www.akita-nct.jp

このホスト名と IP アドレスの対応を行う仕組みが DNS(Domain Name System) である．

付録 A　RSA 暗号の原理

このあたりの話は，文献 [4] や [5] を参考にしている．

付録 A.1　原理

公開鍵暗号方式は 1976 年、ディフィー (Whitfield Diffie) と ヘルマン (Martin E. Hellman) によって考案された．その方式には，様々な方法がある．その中でも，RSA 暗号[1]はその頂点に君臨している．

時間が無かったので載せることができなかった．ひまを見て，WEB に載せる．

付録 A.2　暗号化・復号化の例

参考文献

[1] 河合慧（編）. 情報. 東京大学出版会, 2006.

[2] 粂井康孝. 猫でもわかるネットワークプログラミング第 2 版. ソフトバンククリエイティブ (株), 2007.

[3] 小沢誠. Network 第 2 課–osi モデル. http://www.komazawa-u.ac.jp/ w3c/lecture/network/ccna2.html.

[4] 伊藤正史. サルにも分かる rsa 暗号. http://www.maitou.gr.jp/rsa/. かなり，分かりやすい.

[5] Rsa 暗号の原理. http://mathematics.web.infoseek.co.jp/pdf/rsa.pdf.

[1] 発明者であるロナルド・リベスト (Ronald Linn Rivest)，アディ・シャミア (Adi Shamir)，レオナルド・エーデルマン (Len Adleman) の頭文字をとって，RSA 暗号と名付けられた．