グロッサリ

ここでは各論文で触れられている用語について概説する．情報標準に関する国際的な標準機関や，デジュール標準とデファクト標準の関係など一般的な用語は 2010 年に発行したデジタルプラクティス Vol.1, No.2 も参考にされたい．

学会試行標準

情報処理学会試行標準(学会試行標準と略称)とは，情報処理学会情報規格調査会で規格化が行われている情報技術分野における標準である．情報規格調査会が情報処理学会における研究活動との連携を深め，従来型の標準開発ばかりでなく，試行段階の技術仕様や情報技術分野における標準開発，研究開発，システム開発に有用な技術情報等を学会試行標準として制定し，情報規格調査会のウェブページ上に公開して広く意見を求めるとともに，それらの利用と普及を促進することを目的としている．

ハードリアルタイムとソフトリアルタイム

ハードリアルタイム (Hard real time) 性とは, 処理や通信に対して与えられた時間制約(デッドラインや周期等)を必ず守らなければならない性質であり，時間制約を少しでも破ると価値がゼロになる性質である．狭義には，時間制約を破った場合，システムに損害を与える可能性のあるリアルタイム性のことである．主に制御系の処理や通信が要求するリアルタイム性である．

一方ソフトリアルタイム(Soft real time)性とは，処理や通信に対して与えられた時間制約（デッドラインや周期等）を多少破ることを許容する性質であり，時間制約を破っても価値はただちにゼロにはならない. 多くの場合，時間制約を破ると, 時間経過と共に価値が減少していく．また，時間制約を破っても，システム自身に損害を与えることはない．多くのマルチメディア系（動画・音声処理等）の処理や通信はソフトリアルタイム性を必要とする．

アクセシビリティ

アクセシビリティ（Accessibility）とは，高齢者・障害者を含む多くの人が，様々な製品やサービス等をどのくらい利用できるかの度合を表す概念である．

例えば，健常者だけではなく，高齢者や障害者にも困難なく使えるように設計された製品やサービスは，アクセシビリティが高いということになる．逆に，高い能力を持つ一部の利用者にしか使えない製品やサービスは，アクセシビリティが低いということになる．鉄道の駅の券売機で，ボタンを通常の高さだけでなく車椅子の利用者が楽に操作できる位置にも付けたり，硬貨の投入口を皿のような受口にしたりしてアクセシビリティを高めることができる．

また，製品やサービスの設計の段階で，高齢者・障害者を含む多くの人が使えるように配慮することを, “アクセシビリティに配慮する”と表現することがある. さらに, 利用対象となる製品やサービスが“情報”である場合は、これを利用できる度合いを“情報アクセシビリティ”と呼ぶこともある．

製品やサービスの中で，一定のアクセシビリティを実現するために設けられた事項は，“アクセシビリティ○○”と表現することがある．例えば，高齢者・障害者がコンピュータを利用可能にするための音声読上や画面拡大などの機能は，“アクセシビリティ機能”と呼び，それを設定することを“アクセシビリティ設定”と呼ぶ．

なお, JIS X8341-1:2010 では次のとおり定義している．

アクセシビリティ（accessibility）

様々な能力をもつ最も幅広い層の人々に対する製品，サービス，環境又は施設（のインタラクティブシステム）のユーザビリティ．

注記 1　アクセシビリティの概念では, 能力の多少を問わずすべての利用者を対象とし，障害者と正式に認められた利用者に限定していない．

注記 2　ユーザビリティ指向のアクセシビリティの概念は，すべての利用者の能力の全範囲に十分に注意を払うと同時に利用の特定の状況を考慮し、できるだけ高い水準の有効さ，効率及び満足度を達成することを目指している．

暗号

暗号（Cryptography, Cipher, Code）は，メッセージを送出する送信者とメッセージを受け取る受信者の間で，通信路上の第三者に知られることなくメッセージを伝達する手法であり，その歴史はギリシャ・ローマ時代にまで遡ることが出来る．一般的には通信路における“盗聴”からメッセージを保護する手段として理解されているが，

1970 年代半ばに出現した「現代暗号」では，機密性だけでなく完全性，相手認証，アクセス制御，否認拒否といった近代暗号以前の暗号にはなかった新しい機能を実現できる様になった．

送信者側では，通信路上に想定される第三者から守るために暗号アルゴリズムと暗号化鍵を用いて，伝えたいメッセージを変形する操作を行う．この操作が暗号化である．暗号化されたメッセージは暗号文と呼ばれる．また，暗号化鍵は暗号アルゴリズムに与えられるパラメータであり，送信者に割り当てられる．受信側では，受信した暗号文を復号アルゴリズムと復号鍵を用いて，元のメッセージに復元する操作を行う．この復元の操作が復号であり，復号鍵は受信者に割り当てられたパラメータである．この暗号化鍵と復号鍵をまとめて「鍵」と総称する．

共通鍵暗号

共通鍵暗号（Secret Key Cryptography System）は、ギリシャ・ローマ時代から利用されてきた暗号技術．暗号化に用いる「暗号化鍵」と復号に用いる「復号鍵」が「共通」であることが最大の特徴．以前は，日本語でも「秘密鍵暗号」と記述することが一般的であったが，公開鍵暗号の"Private Key"を秘密鍵と訳したことから，混乱が生じてしまった．そのため，最近では「共通鍵暗号」と記述されることが一般的になりつつある．共通鍵暗号は，ビット毎に暗号化・復号するストリーム暗号とブロックと呼ばれる一定長のビット列の単位で暗号化・復号するブロック暗号に大別される．無線通信系ではストリーム暗号が利用されることが多く，計算機システム，有線通信網や IP 網ではブロック暗号が利用されることが多い．共通鍵暗号は，暗号化処理や復号処理が高速であるという特長を持つが，「鍵」を共通にするための「鍵共有」が必要となる．

公開鍵暗号

公開鍵暗号（Public Key Cryptography System）は，現代暗号を象徴する暗号．公開鍵暗号は暗号化に用いる「暗号化鍵」と復号に用いる「復号鍵」が異なっている暗号アルゴリズム．暗号化に用いる「公開鍵（Public Key）」と復号に用いる「プライベート鍵（Private Key）」は数学的に「対」となっている．公開鍵は，秘密にしておく必要はなくディレクトリサーバ等で公開される．公開鍵暗号を用いて暗号通信をしたい場合は，通信相手の公開鍵を用いて伝えたい情報を暗号化する．受信者だけが持つ公開鍵と対になったプライベート鍵を用いなければ，暗号文は復号できない．プライベート鍵は厳重に管理する必要があるが，共通鍵暗号に比べて鍵管理が簡便である．しかし，共通鍵暗号に比べて処理速度は大きく劣っている．

公開鍵暗号は，安全性の根拠となる数学的な問題によって分類されることが多い．例えば，RSA 暗号は素因数分解問題に安全性の根拠を置く方式であり，現在もっとも広く用いられている．離散対数問題を安全性の根拠とする公開鍵暗号の例としては，ElGamal 暗号や DH 公開鍵配送方式がよく知られている．また，近年急速に研究が進んでおり，応用が進んできた楕円曲線暗号は，楕円曲線上の離散対数問題を安全性の根拠においている．

デジタル署名

デジタル署名（Digital Signature）は，メッセージの正当性を保証するためにメッセージから生成される情報であり，デジタル署名を生成・検証する処理系を指すこともある．デジタル署名を用いることで，署名者を証明し，かつそのメッセージが改竄されていないことが保証できる．デジタル署名を生成・検証する処理系は，署名者だけが持つ秘密情報（署名鍵）とその秘密情報と対となる公開情報（検証鍵），署名生成アルゴリズム，および，署名検証アルゴリズムから構成さる．一般的に用いられているデジタル署名（添付型デジタル署名）では，署名の対象となるメッセージに対して，署名鍵と署名生成アルゴリズムを用いてデジタル署名を生成し，検証者は公開されている検証鍵，署名者からのメッセージ，および，メッセージに対応したデジタル署名を署名検証アルゴリズムに入力する．署名鍵と検証鍵が正当な対であり，かつ，メッセージとデジタル署名が正しい対となっていれば、署名検証アルゴリズムは，“真”を出力し，署名者がメッセージにたいして署名したことを裏付け，正当な対でなければ“偽”を出力して，不正行為があったことを示す．

また，ある種の公開鍵暗号では，プライベート鍵を署名鍵，公開鍵を検証鍵として用いることで，デジタル署名が実現できる．このような暗号では，プライベート鍵で暗号化された情報は，プライベート鍵の持ち主しか作成できない．一方，その暗号文の作成者は，万人が特定できることになる．これがデジタル署名のひとつの例である．なお，デジタル署名には，公開鍵暗号を使わない方式もある．

（山崎信行，関喜一，山本喜一，山岸篤弘，大蒔和仁，村上篤道）