

データを処理するために用いる2進数、論理演算や情報量などの基礎理論、キューなどのデータ構造の特徴や流れ図の読み方、コンピュータシステムやネットワークの仕組み、セキュリティ対策など多岐に渡る出題範囲となっています。情報技術に直結するキーワードが数多く登場しますので、重要用語はしっかり理解しておきましょう。

基礎理論

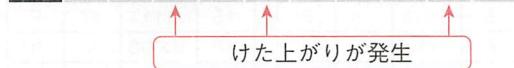
□ 2進数



数字を0と1の2種類の情報だけで表現するものです。0と1を電気信号のOFF, ONに対応させられることから、コンピュータとの親和性が高い表現方法です。コンピュータ上では、2進数の1桁をビットという単位で表します。

2進数では、2で割った上がりします。このけた上がりする基準となる数値を「基数」といい、2進数では「2」、10進数では「10」が基数となります。なお、2進数と10進数の対応関係は、次のようにになります。

10進数	0	1	2	3	4	5	6	7	8	…
2進数	0	1	10	11	100	101	110	111	1000	…



●出題例 「2進数」

【問題】

2進数 1.101 を 10進数で表現するといつになるか。(H22春問52改)

【解説】

2進数の各けたの重みは右図のとおり。

2進数 1.101 を 10進数で表すと、 $1 \times 2^0 +$

$$\begin{aligned} & \times 2^{-1} + 0 \times 2^{-2} + 1 \times 2^{-3} = 2^0 + 2^{-1} + 2^{-3} \\ & = 1 + (1/2) + (1/8) = 1 + 0.5 + 0.125 = 1.625 \end{aligned}$$

となる。

$$\begin{array}{ccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2^4 & 2^3 & 2^2 & 2^1 & 2^0 & 2^{-1} & 2^{-2} & 2^{-3} & 2^{-4} \end{array}$$

ワンポイントMEMO

数値をコンピュータで表現すること

日常生活では、私たちは0～9のアラビア数字と、その組合せによる数(10, 123, 3.1415…など)の表現方法(10進数)を無意識に用いています。しかし、数を表現するのにアラビア数字を必ず用いなければならないということではなく、他の文字や表現形式を用いることもできます。○と×の記号だけでも数を表現できます。○と×だけでは2種類の数しか表現できないように見えますが、この二つの記号を複数個組み合わせることで、任意の数を表現できます。

例えば、○と×の記号を二つ組み合わせると「○○」、「○×」、「×○」、「××」の4通りの相異なるパターンを作れます。これらの各パターンにそれぞれ異なる値を割り当てることで、4種類の数(例: 0～3)を表せます。アラビア数字で10個の記号(数字)とその記号の組合せ(数字列)を用いているのと、まったく同じことです。

○を電光掲示板などのライトの点灯、×を消灯と考えれば、多数のライトを用意して、ライトの点灯または消灯の組合せのパターンを数値に割り当てる

ことで、多数の数値を表現できます。このライトの点灯と消灯と同様に、コンピュータ内には電流のオン／オフを行うスイッチの組合せが多数あり、それを用いて値を表現します。○を1, ×を0とみれば、1と0の組合せによる値がコンピュータ内で表現されていることになります。この組合せによる数が2進数です。

2進数を用いることで、オン／オフの組合せだけを用いて数値を容易に表現できます。コンピュータ内の回路では、オンとオフの二つの状態だけを区別することができ、オンとオフの中間の状態を表現することはできません。すなわち、2進数による表現は、オンとオフだけを使うことができるコンピュータに向いているのです。

我々が用いている千, 万, …などの単位は、大きな数を簡潔に表現するためのものです。コンピュータで扱う値も大きな数になるので、k(キロ), M(メガ)などの単位を用いて、数を簡潔に表現することができます。

□ 8進数と16進数

2進数のままでは人間にとっては読みにくく、桁数も非常に多くなってしまうため、8進数や16進数が使用されることがあります。8進数1桁は、2進数3桁($2^3 = 8$)、16進数1桁は、2進数4桁($2^4 = 16$)で表現されます。

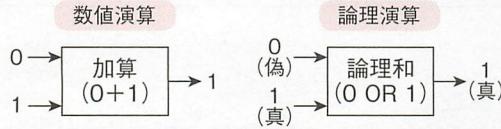
10進数	2進数	8進数	16進数
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9

10進数	2進数	8進数	16進数
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F
16	10000	20	10
17	10001	21	11
18	10010	22	12
19	10011	23	13

※ 何進数かを表示するために、 110_{10} , $(10010)_2$ のように表記する場合がある。

□ 論理演算

コンピュータが実行する演算処理には、加算、減算、乗算、除算といった数値演算のほかに、真・偽という論理値を扱う論理演算があります。



※論理演算の「0」、「1」は、論理値であって数値ではない。

□ 論理演算の種類



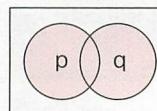
論理演算には、以下のようなものがあります。

名称	説明
論理和 (OR)	二つの論理値のいずれかが真である場合は結果が真となり、両方が偽である場合のみ結果が偽となる演算である。
論理積 (AND)	二つの論理値の両方が真である場合のみ結果が真となり、いずれかが偽である場合は結果が偽となる演算である。
否定 (NOT)	与えられた論理値に対して逆の結果となる演算である。すなわち、論理値が真の場合は偽と、偽の場合は真となる。
否定論理和 (NOR)	論理和 (OR) を否定 (NOT) した演算である。
否定論理積 (NAND)	論理積 (AND) を否定 (NOT) した演算である。
排他的論理和 (XOR)	二つの論理値の一方だけが真である場合は結果が真となり、両方が真または偽である場合は結果が偽となる演算である。

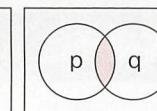
□ 論理演算とベン図

論理演算は、集合などで利用されるベン図を使って、次のように表現することができます。

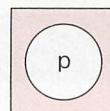
論理和 (OR)



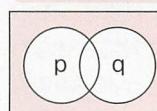
論理積 (AND)



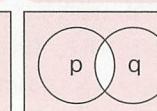
否定 (NOT)



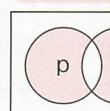
否定論理和 (NOR)



否定論理積 (NAND)



排他的論理和 (XOR)



□ 情報量の単位

コンピュータの記憶装置の情報量の単位は次のようにになります。

単位	読み	意味
1bit	1ビット	2進数の1けたに相当する情報量の単位。
1B	1バイト	$1B = 8\text{bit}$
1KB	1キロバイト	$1KB = 2^{10}B = 1,024\text{bit}$
1MB	1メガバイト	$1MB = 2^{20}B = 2^{10}\text{KB}$
1GB	1ギガバイト	$1GB = 2^{30}B = 2^{20}\text{KB} = 2^{10}\text{MB}$
1TB	1テラバイト	$1TB = 2^{40}B = 2^{30}\text{KB} = 2^{20}\text{MB} = 2^{10}\text{GB}$

□ 文字コード

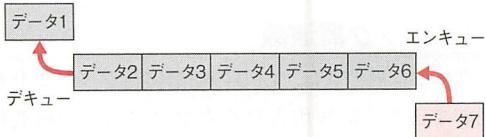
コンピュータで入出力される文字はすべて文字コードで処理されています。代表的な文字コードは、次のとおりです。

名称	説明
ASCIIコード	ANSI(米規格協会)が制定した、1文字を7ビットで表現する文字コード。
EBCDIC	IBM社が制定した拡張2進符号のこと。1文字を8ビットで表現する。
JISコード	JIS(日本工業規格)が制定したコード。数字・英字・各種記号・カタカナは1文字を8ビットで表現し、漢字は16ビットで表現する。
シフトJISコード	Microsoft社が制定した主にパソコンで使用されている文字コード。16ビットを使用して日本語で使用するほぼすべての文字を表現できる。
EUC	AT&Tが制定したUNIXなどで使用されている文字コード。日本語EUC(EUC-JP)は、2バイトで漢字も表現できる。

Unicode	ISOとIECが制定した、世界各国の言語体系に対応した文字コード。すべての国の文字を2バイト(16ビット)でほぼ網羅したUSC-2や、2バイトでは足りないために3バイト以上で表現するもの、4バイトで表現しているUSC-4などがある。
---------	--

□ キュー

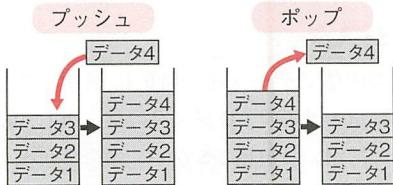
最初に格納したデータから順に取り出す、FIFO(First In First Out: 先入れ先出し)で動作するデータ構造です。キューでは、データを格納することをエンキュー、データを取り出すことをデキューといいます。



※データの番号は格納した順番を表します。

□ スタック

最後に格納したデータから順に取り出す、LIFO(Last In First Out: 後入れ先出し)で動作するデータ構造です。スタックでは、データを格納することをプッシュ、データを取り出すことをポップといいます。



□ 流れ図

フローチャートとも呼ばれ、論理的なアルゴリズムをわかりやすく記述する方法の一つです。JIS規格により定められている、流れ図の主な記号には次のようなものがあります。

名称	記号	説明
端子	○	処理の始まりおよび終了を表すときに使用する。サブルーチンの開始、呼び出し先に戻る場合にも使用する。
処理	□	処理を表現するときに使用する。「A+B→C」などの式を記述する場合だけでなく、「合計処理」などの言葉で記述する場合もある。
判断	◇	判断を行いたい場合に使用する。記述した条件によりその後の行き先が決定される。

ループ端		繰返しを記述する場合に使用する。繰返しを終了する条件を前もしくは後に記述する必要がある。
------	--	--

□ 決定表(デシジョンテーブル)

複数の条件の組合せに対応する処理について表現するために用いられる、二次元の表のことです。

決定表の例

		条件記述部			条件指定部	
		(1)	(2)	(3)		
(条件部)	条件 1	Y	—	N		
	条件 2	N	Y	N		
(処理部)	処理 1	X	X	—		
	処理 2	—	X	X		
		動作記述部			動作指定部	

□ マークアップ言語



マークアップ言語(markup language)は、テキストファイルの中で、文字装飾やレイアウトなどに関する設定情報をタグなどの記号で記述する言語です。文書整形言語ともいいます。マークアップ言語に対応したソフトウェア(例えばWWWブラウザ)を利用すれば、整形・装飾された美しい文書を画面表示・印刷できます。代表的なマークアップ言語は、次のとおりです。

名称	説明
SGML	現在Webページなどの作成で主に使用されているHTMLやXMLの基になったマークアップ言語。文章の論理構造(タイトル、日付、記述者など)を決めて記述できる。
HTML	W3Cによって標準化されたマークアップ言語。文字に加えて画像などを使用したWebページの作成や、他の場所への接続(ハイパーリンク)が可能である。
XML	HTMLと同様にWebページを作成する際に使用されている。ユーザが自ら決めた独自のタグを使用することもできるため、共通のデータフォーマットとしての利用も進んでいる。

□ ロードモジュール

コンピュータで実行が可能な機械語プログラムのことです。

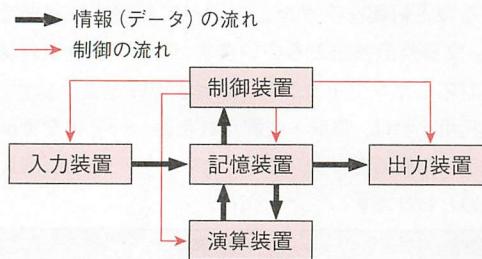
プログラムを作成するときに実行される手順と、各手順において用いられるソフトウェアを示します。
①C言語などのプログラム言語で、原始プログラムを作成する。

- ②原始プログラムを、コンパイラが解釈し翻訳することで、機械語で記述されたオブジェクトモジュールが作られる。
- ③オブジェクトモジュールには入出力機能などが組み込まれていないので、そのままでは実行できない。作成したオブジェクトモジュールに、入出力機能などを実行する汎用的なオブジェクトモジュール(ライブラリ)を結び付けることで、コンピュータで実行が可能なロードモジュールが作成される。この処理を行うソフトウェアがリンクである。

コンピュータシステム

□コンピュータの5大装置

コンピュータを構成するハードウェアの各要素は、一般に5大装置(演算装置、制御装置、記憶装置、入力装置、出力装置)として分類されます。5大装置の関係を図式化すると、次のようになります。



●出題例 「クロック周波数」

[問題]

クロック周波数が1GHzのCPUがある。このCPUの命令種別が、表に示す二つから成っているとき、処理能力は約何MIPSか。(FE H20春問19)

命令種別	実行時間(クロック)	出現頻度(%)
命令1	10	60
命令2	5	40

[解説]

$$\text{CPUで1クロックを刻むのに要する時間} = \frac{1}{1 \times 10^{-9}} = 1 \times 10^{-9} \text{秒。}$$

命令種別の表より、命令の平均実行時間(単位:クロック)の期待値を求めるとき、 $10 \text{クロック} \times 0.6 + 5 \text{クロック} \times 0.4 = 8 \text{クロック}$ となる。

□CPU

Central Processing Unit。単にプロセッサとも言われ、コンピュータの5大装置の演算装置と制御装置の二つの機能を併せ持っています。また、CPUは他の装置に制御用の信号を送ったり、主記憶装置から送られたプログラムやデータをCPU内の記憶装置であるレジスタを使用して計算したりするコンピュータの中枢部分を構成しています。

CPUには、データを転送する大きさによって32ビットや64ビットなどの種類があり、性能はクロック周波数(Hz)などで表されます。

□クロック周波数

クロック周波数は、CPUの命令実行タイミングを制御するために利用されるクロック信号の周波数で、Hz(クロック/秒)という単位で表記します。クロック周波数には、CPU内部にあってCPU自体の動作基準となる内部クロック周波数と、CPUと主記憶などの外部機器とを結ぶシステムバスの動作基準となる外部クロック周波数があり、両者は同一ではありません(通常、内部クロック周波数の方が高速です)。

□レジスタ

CPUの内部でデータを一時的に保存しておくための小容量のメモリ。レジスタには、CPUが演算を行うために用いる汎用レジスタ、命令実行後のCPUの状態を示すステータスレジスタ、アドレス計算を

(命令1) + 5 クロック × 0.4 (命令2) = 6 + 2 = 8 クロックになる。

$$\text{平均命令実行時間} = 8 \times 1 \times 10^{-9} \text{秒} = 8 \times 10^{-9} \text{秒。}$$

CPUのMIPS(1秒間に実行できる命令の数) = 1命令の平均実行時間(単位:秒/命令)の逆数 = $\frac{1}{8 \times 10^{-9}} = 0.125 \times 10^9 = 125,000,000 \text{命令/秒} = 125 \text{MIPS}。$

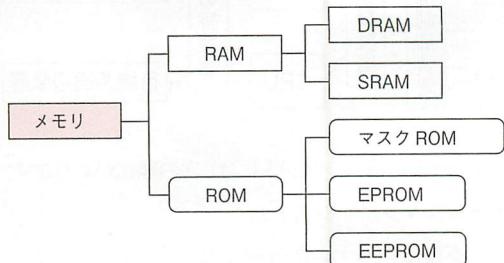
※ MIPS: 1秒間に実行できる命令の数を百万単位で表現したもの。

$$1,000,000 (\text{命令/秒}) = 1 \text{MIPS}$$

行うためのインデックスレジスタなどの種類があります。

□ メモリの種類

コンピュータで利用されるメモリには、大別してRAMとROMがあります。RAM(Random Access Memory)は、データの読み書きができるメモリです。電源を切ると、記憶内容は失われます(これを揮発性という)。ROM(Read Only Memory)は、電源を切ってもデータが失われないメモリです(これを不揮発性という)。



□ 仮想記憶方式

磁気ディスク装置などの補助記憶装置の一部を、仮想的な主記憶空間とみなして使用することにより、主記憶の容量よりも大きなメモリを必要とするプログラムを実行できるようになります。

□ 様々な補助記憶装置

主記憶装置が利用するプログラムやデータを蓄積し、必要に応じてこれを提供するための記憶装置です。主な補助記憶装置には、以下のようなものがあります。

種類	名称	記憶方式	記憶容量	アクセス速度
半導体ディスク	フラッシュメモリ	書き換え可能	～数TB	非常に高速
磁気ディスク	ハードディスク	書き換え可能	～3TB	高速
光ディスク	CD-ROM	読み取り専用	650MB他	やや低速
	CD-R	追記型	650MB他	
	CD-RW	書き換え可能	650MB他	
	DVD	読み込み/書き込み/追記	4.7GB / 9.4GB他	
	ブルーレイディスク	書き換え可能	25GB / 50GB	やや低速
磁気テープ	DAT	書き換え可能	数十GB他	低速

□ フラッシュメモリ

電気的に書き換えが可能なEEPROMの一種。電源を供給しなくても記憶内容が保持できるため、ディジタルカメラ用のメモリカードなど、小型の補助記憶媒体として広く普及しています。

□ キャッシュメモリ

キャッシュメモリ(cache memory)は、CPUと主記憶装置の間に置かれる高速なメモリです。CPUに一度読み込まれたデータはキャッシュメモリに保存され、次回読み込み時には主記憶装置ではなくキャッシュメモリから読み込まれます。このためCPUのデータの読み込み速度が向上し、データ転送を高速に行います。キャッシュメモリにはSRAMが使用されます(一般に、主記憶装置にはDRAMが使用される)。



□ インタフェースの種類

インターフェースは、ハードウェア間を物理的に結びつける接続部分もしくはその規格や方式をいいます。コンピュータと周辺装置の接続インターフェースには、直列のシリアルインターフェースと並列のパラレルインターフェースがあります。近年ではシリアルインターフェースが主流になっています。

□ USB

Universal Serial Bus。現在、ほとんどのパソコンで採用されているシリアルインターフェース規格です。キーボードやマウスの他、CD-ROMやハードディスクなどの補助記憶装置、プリンタ、スキャナなど、様々な周辺機器を接続できます。転送速度は、USB 1.1で1.5Mbps(ロースピードモード)と12Mbps(フルスピードモード)、USB 2.0では480Mbps(ハイスピードモード)があります。機器はハブを使ってツリー状に最大で127台まで接続できます。最新の規格は、転送速度が5Gbpsの3.0です。また、以下の機能があります。

機能	説明
プラグアンドプレイ	周辺機器をPCに接続するだけで、自動的に認識処理などが行われ、利用者が特別な設定をしなくても周辺機器が利用可能になる機能。
ホットプラグ	PCの電源を入れたままで周辺機器を着脱できる機能。

□ タッチパネル

指などで画面に直接触れることで、ファイルを開くなどのコンピュータの操作を行えるようにした装置です。銀行ATMの画面やスマートフォンの画面などに用いられています。

タッチパネルの主な方式を表に示します。

方式名	説明
抵抗膜方式	金属薄膜を2枚重ね、電圧をかけた上側の金属薄膜に触ると、下側の金属薄膜に電圧が発生する。その電圧を検知することで接触位置を特定する。 例：ニンテンドーDS
電磁誘導方式 (電子式)	電子ペンという専用の接触用装置が必要になる。磁界を発生させたパネルの上を電子ペンが動くと、ペン内のコイルに電流が発生し、その電流を検知することで接触位置を特定する。 例：ペンタブレット
静電容量方式 (静電式)	導電膜と指との間に発生する静電容量の変化を検知することで、接触位置を特定する。 例：スマートフォン、タブレット端末

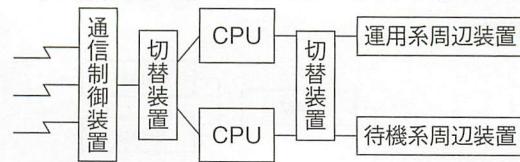
□ Bluetooth

Bluetoothは、2.45GHz帯を使用して10cmから

10m程度の範囲内で双方向1Mビット／秒の通信速度を実現している無線通信技術のことです。

□ デュプレックスシステム

デュプレックスシステムは、2系統のシステムで構成され、1系統はオンラインリアルタイム処理を行い、もう1系統は通常、バッチ処理を行うシステムです。オンライン処理系システムが故障した場合、バッチ処理系システムに切り替えて処理を継続します。



デュプレックスシステムには、次の種類があります。

ホットスタンバイシステム

本番系システムが故障したときは、本番系システムと同一の業務プログラムをあらかじめ起動して待機している予備系システムに即座に切り替えて、処理を続行する方式。

ワンポイントMEMO

命令実行の流れ

メモリ(主記憶装置)に記憶された命令をCPUが読み込んで実行するときの流れは、次のようにになります。

① プログラムカウンタが示すアドレスのデータを読み込む

プログラムカウンタは、次に読み込む命令が格納されている語のアドレスを記録するための回路です。例えば、一つの命令が2語にわたって格納されるコンピュータにおいて、プログラムカウンタに1000という値が記録されているとき、メモリの1000番地の語を先頭とする2語に格納されているデータを、後述する命令レジスタに読み込みます。

② 命令レジスタ内の命令を解釈し、実行する

命令レジスタは、メモリから読み込んだ命令を格納する回路です。命令レジスタに読み込んだ命令を解釈して、データの加減算を行ったり、メモリ上の特定のデータを参照したりするなどの、各種の処理を実行します。

③ プログラムカウンタの値の更新

②で実行した命令がジャンプ命令(プログラム中の任意の部分に制御を移す命令)の場合、当該命令の指定するアドレスの値がプログラムカウンタに格納されます。例えば、「2000番地の命令に制御を移す」というジャンプ命令の場合、プログラムカウンタの値は2000に更新されます。

実行した命令がジャンプ命令以外の場合、②で実行した命令の直後に格納されている命令が次に実行されるので、現在のプログラムカウンタの値に命令語長を加算した値が、プログラムカウンタに格納されます。例えば、1000番地の語を先頭とする命令を実行した場合、命令語長は2語なので、次に実行する命令の先頭の語は1002番地になります。よって、プログラムカウンタの値は $1000 + 2 = 1002$ になります。

④ ①に戻り、処理を繰り返す

次に実行する命令が格納されるアドレスを参照するため、①に戻ります。

ウォームスタンバイシステム

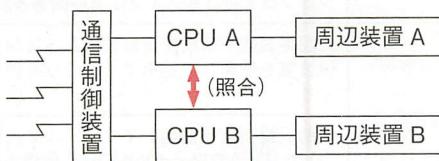
予備系システムは、電源を入れてOSが起動している（本番系システムと同じ業務プログラムは起動させていない）状態で待機させ、本番系システムが故障したときは、本番系システムと同じ業務プログラムを予備系システムで起動し、予備系システムに切り替えて処理を続行する方式。

コールドスタンバイシステム

予備系システムは電源を切って（もしくは他業務を実行させて）待機させておき、本番系システムが故障したときは、予備系システムの電源を入れて立ち上げ、本番系システムと同じ業務プログラムをロードして処理を続行する方式。

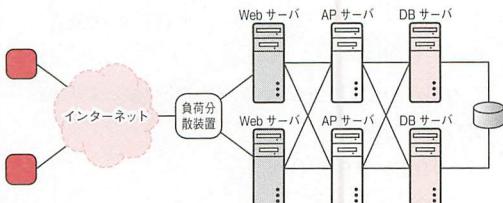
□ デュアルシステム

デュアルシステムは、2系統のシステムが同時に並行して同一の処理を実行し、相互に実行結果を照合するシステムです。二つのシステムの処理結果が異なる場合は、どちらかのシステムに何らかの故障が発生したと判断し、正常なシステムのみで処理を継続します。



□ クラスタシステム

信頼性向上などを目的として作られた、複数のコンピュータによって冗長構成されたシステムです。このシステムでは、複数のコンピュータを連携させ、全体を1台のコンピュータであるかのように扱います。また、このシステムでは連携させているコンピュータのいずれかに障害が発生すると、他のコンピュータに処理を代行させ、システム全体を停止させないようにしています。



□仮想化技術

1台のコンピュータ上で複数のサーバプログラムを同時に立ち上げて稼働させ、複数のサービスを利用者に同時に提供する技術のことです。近年のコンピュータは性能が非常に向上しており、1台のコンピュータ上で複数のサービスを実行しても、問題なく処理できます。よって、可能ならば1台のコンピュータだけで複数のサービスを提供する方が、費用や負荷を減らすことができます。

□ システムの評価指標



コンピュータシステムの性能を表す場合、スループット、ターンアラウンドタイム、レスポンスタイムなどの指標が利用されます。

名称	説明
スループット	システムが単位時間当たりに処理できる仕事量。仕事量は、トランザクションやジョブなどで表される。
ターンアラウンドタイム	バッチ処理において、ホストコンピュータに処理（ジョブ）を依頼してからその処理結果を受け取るまでに要する時間。コンピュータの処理時間の他、データの転送時間、人間の操作時間なども含まれる。
レスポンスタイム	システムに処理要求を送ってから、その応答が戻って来るまでに要する時間。応答時間ともいう。

□ 稼働率



全時間のうちで該当の機器がどのくらいの時間動作しているのかという、可用性評価の指標です。次の式で求められます。

$$\text{稼働率} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{\text{全運転時間} - \text{修理時間}}{\text{全運転時間}}$$

● MTBF (Mean Time Between Failure)

平均故障間隔。稼働しているシステムで、故障が回復してから次の故障が生じるまでの平均時間です。MTBFが長いほど、システムの信頼性は高くなります。

● MTTR (Mean Time To Repair)

平均修理時間。稼働しているシステムで、故障が発生してから修復するまでに要する平均時間です。MTTRが短いほど、システムの保守性は高くなります。

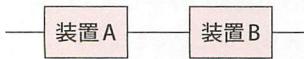
□複合システムの稼働率



複数の装置が接続されているシステム全体の稼働率は、どのように(直列／並列)接続されているかによって計算方法が異なります。

●直列構成システムの稼働率

システムを構成しているすべての装置が稼働している場合にだけ、全体が稼働するシステム。



$$\text{稼働率} = \text{A の稼働率} \times \text{B の稼働率}$$

●並列構成システムの稼働率

システムを構成している装置が一つでも稼働していれば、全体が稼働するシステム。



$$\text{稼働率} = 1 - (1 - \text{A の稼働率}) \times (1 - \text{B の稼働率})$$

□高信頼性設計

システムの信頼性を高める仕組みの代表的なものには、次のような種類があります。

名称	説明
フォールトトレーラント	障害が発生しても、支障をきたすことなく継続運転させようとする仕組み。

フェールソフト	障害が発生した場合に全面停止とせずに、必要最小限の機能を維持して処理を続ける仕組み。
フェールセーフ	障害が発生した場合にその影響が及ぶ範囲を最小限にして、システムの安全を保った上でシステムを停止し、安全性を高める仕組み。
フルブループ	設計において、操作ミスなどによる障害を防止しようとする考え方。利用者が安全にシステムを利用できるようにする仕組み。

□OSの機能

OSは基本ソフトウェアに分類されます。ソフトウェアが必要とする基本的な作業(タスク管理(CPU管理のこと)、メモリ管理、データ管理など)をまとめて処理できるため、OSを基に様々なアプリケーションソフトを実行することが可能となります。

機能	説明
ジョブ管理	ジョブは、ユーザがコンピュータに与えられた仕事の単位。例えば、チケットを発券する処理の場合、ユーザは複数枚発券する場合でも、発券処理の指示は1回だけである。
タスク管理	タスクはコンピュータが処理する仕事の単位。ここでは、CPUの管理を行なう。例えばチケット発券が100枚あれば、ジョブは1回でもタスクは100回ある。
メモリ管理	主記憶装置や補助記憶装置にある仮想記憶装置を使用して効率よくメモリを管理する。
ファイル管理	補助記憶装置を使用してファイルを入出力したり、そのファイルが同時に使用されていないか確認するなどの管理を行う。

●出題例 「複合システムの稼働率」

[問題]

東京～大阪及び東京～名古屋がそれぞれ独立した通信回線で接続されている。東京～大阪の稼働率は0.9、東京～名古屋の稼働率は0.8である。東京～大阪の稼働率を0.95以上に改善するために、大阪～名古屋にバックアップ回線を新設することを計画している。新設される回線の稼働率は最低限幾ら必要か。(FE H21春問16)

[解説]

大阪～名古屋間にバックアップ回線を新設すると、東京～大阪間は以下の二つの経路で結ばれる。

- 東京～大阪の経路
- 東京～名古屋経由～大阪の経路

新設されるバックアップ回線の稼働率をAとおき、次の経路の稼働率を求める。

東京～大阪の経路の稼働率 : 0.9

$$\begin{aligned} \text{東京～名古屋経由～大阪の経路の稼働率 : } \\ 0.8 \times A = 0.8A \end{aligned}$$

東京～大阪間は、この二つの経路による並列構成の通信回線によって結ばれているので、全体の稼働率は次のようになる。

$$\begin{aligned} \text{全体の稼働率 : } & 1 - (1 - 0.9) \times (1 - 0.8A) \\ & = 1 - 0.1 \times (1 - 0.8A) = 1 - 0.1 + 0.08A \\ & = 0.9 + 0.08A \end{aligned}$$

この値が0.95以上になるために必要なAの値は次の通りである。

$$0.95 = 0.9 + 0.08A$$

$$0.05 = 0.08A$$

$$\therefore A = 0.05 / 0.08 = 0.625$$

入出力管理	デバイスドライバを使用して外部の入出力装置(プリンタなど)を利用できるようにする。
ユーザ管理	ユーザ別の利用権限の設定やその利用時に必要なIDの登録などを行う。

□ ルートディレクトリ

ディレクトリ構造で、その最上層にあるディレクトリです。ルートディレクトリの下にはサブディレクトリを設定できますが、同一ドライブにルートディレクトリを複数作成することはできません。

□ カレントディレクトリ

ディレクトリ構造で、システムが現在処理対象としているディレクトリのことを指します。

□ 絶対パス指定

ディレクトリ下にあるファイルを指定する際に、ルートディレクトリから出発して、目的のファイルにいたるまでの途中のすべてのサブディレクトリ名を指定する方法です。

□ 相対パス指定

ディレクトリ下にあるファイルを指定する際に、カレントディレクトリから出発して、目的のファイルにいたるまでの途中のすべてのサブディレクトリ名を指定する方法です。

□ 表計算ソフト



行と列からなる表のセルに数値や計算式などを記述することで、各種の演算や在庫管理などの業務処理に利用できるソフトウェアです。

	A	B	C	N
行 1	月	1月	2月	計
2	売上高	500	600	10,400

セル 列

□ オープンソース ソフトウェア



OSS : Open Source Software。著作権を維持しながらコンパイルを行う前のプログラムコード(ソースコード)を公開して、その改良を認め、改良後のプログラムの再配布などを自由に行うことのできるようにしたソフトウェアのことです。OSSのソースコードなどは、無償で提供することも、有償で頒布することも認められていますが、配布先を制限した

り、特定の用途での使用を禁止したりすることは認められていません。

□ シンクライアントシステム

利用者が使用するノート型PCなどのクライアントPC(以下、PCという)にはデータを記録せず、サーバのみにデータを記録させる形態のシステムです。このシステムでは、PCはハードディスクをもたず、メモリ(主記憶)だけをもっています。OSを立ち上げる際には、PCはネットワーク上のサーバからOSのイメージをメモリにダウンロードして、立ち上げを行います。

シンクライアントシステムを用いると、社外へ持ち出すノート型PCに、個人情報など重要な情報が含まれたデータを一切保存させないようにできます。そのため、ノート型PCが盗難されるなどの被害に遭っても、重要なデータは漏えいしないため、セキュリティが強化され安全性が向上します。

□ フラグメンテーション

ハードディスクに対してデータの追加や削除を繰り返すことで、ハードディスクの未使用領域が断片化されて、利用可能な未使用領域の大きさが小さくなり、一つのファイルを一つの未使用領域内に収めることができなくなることがあります。その結果、一つのファイルが複数の未使用領域に分割されて格納され、ファイルのアクセス効率が低下する現象です。

技術要素

□ ピクセル

一般にドットと同じ意味で用いられますが、正確にはディスプレイ表示などにおいてコンピュータがコントロールできる最小単位のことです。画素ともいいます。

□ 解像度

画像の細かさの度合いのことです。画像を表示する際のディスプレイ装置、印刷を実行するときのプリンタ、文字や画像などを読み込む場合のスキャナなどで使用されます。1インチの長さにどのくらいのドットが表示されるかを表した単位にdpi(ドット/インチ)があります。

□ マルチメディアで扱うデータ形式

マルチメディアシステムでは、大容量のデータを高速で処理するために、圧縮／伸張と呼ばれる技術を用いた、次のような形式のデータを利用します。

種類	データ形式	対象	説明
静止画データ	JPEG	24ビットのカラー静止画像	ISO/IECで定められた圧縮静止画の国際規格。非可逆圧縮方式を用いているため、圧縮率により色数は変化する。
	GIF	256色(8ビットカラーの静止画像)	可逆圧縮可能な静止画の規格である。色数は最大256色までをサポートできる。
	TIFF	高密度のカラー静止画像	様々な圧縮方式が可能であり、また解像度や色数などが異なる画像を一つのファイルにまとめることが可能な静止画の規格である。
	PNG	48ビットカラーの静止画像	GIFの機能を拡張した、可逆圧縮可能な静止画の規格であり、最大48ビットまでサポート可能である。

MPEG	—	ISOで定められた圧縮動画の国際規格。
動画・音声データ	MPEG1	カラー動画像と音声
	MPEG2	カラー動画像と音声
	MPEG4	カラー動画像と音声
	MIDI	電子楽器で作成された音楽データ
音楽データ	PCM	音声データ
	MP3	音声データ

ワンポイントMEMO

ワープロソフトウェアの処理

Wordや一太郎などのワープロソフトウェアでは、文書の構成を適切に保ったり、印刷作業を便利にしたりするための各種の処理を行っています。

● 禁則処理

「」や「。」などの句読点や閉じ括弧「」が段落中の行頭に配置されたり、開き括弧が段落中の行末に配置されたりすると見づらくなります。

<例>

私は20歳です。また
私はある私鉄のB駅(　
××市の近郊に存在する
)に住んでいます。

入力中の文章においてこのような配置になった場合、ワープロソフトウェアは段落中の文字間隔を詰めたり広げたりして、段落中の行頭や行末に特定の文字が配置されないようにしています。この処理を禁則処理といいます。

● 差込印刷

表計算ソフトウェアなどを用いて作成したデータを1行(1レコード)ずつ取り出し、ワープロソフトウェアの文書の特定の箇所に埋め込んで印刷することで、例えばあて名だけをそれぞれ異なる表記にし、それ以外の部分を共通の表記にして、一度に多数のはがきや封筒を印刷できます。この機能を差込印刷といいます。

表計算ソフトウェアで作成した住所録

no	氏名	住所
1	○○○夫	××市…
2	△△△子	* * 市…
3	□□□太	●●区…

ワープロソフトで
作成したはがき

××市…
○○○夫

様
暑中見舞い

* * 市…
△△△子

様
暑中見舞い

[] 内が差込印刷で埋め込んだデータ

□ データベース管理システム (DBMS) の役割

データベース管理システムとは、データベースを管理するためのソフトウェアです。主に次のような機能があります。

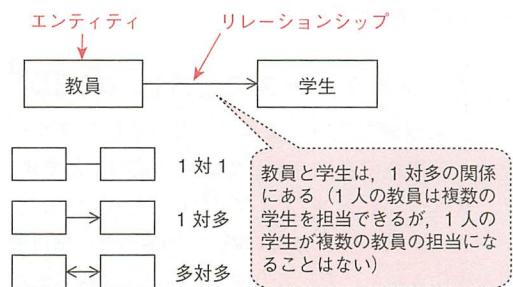
機能	説明
データの管理	データベースを磁気ディスクに記録して管理する。データの整合性チェックなども同時に実行する。
障害復旧	データベースの障害に備えて、データベースの更新履歴などを管理し、障害が発生した場合にデータを障害発生前の状態に戻す。
データベースへのアクセス	ユーザがデータベースにアクセスして、データの参照や更新を行うための環境を提供する。

□ E-R図

情報システムに関する各種のデータや現実世界の事物などをエンティティ(実体)といいます。エンティティ間の関係性(関連)のことを、リレーションシップ(関連)といいます。情報システムを構成するエンティティと、エンティティ間のリレーションシップを表現するための図がE-R図です。

E-R図は、関係データベースを利用するシステム

を設計する際に、関係データベースの表をエンティティ、表と表の間の関係をリレーションシップとして表現するためによく用いられます。



□ 主キー



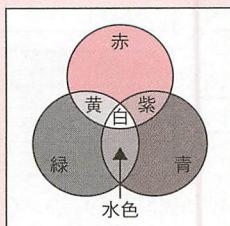
関係データベースの表の行を検索するときなどに、行を一意に区別するための値が必要となります。この値をもつ列のことを主キーといいます。関係データベースでは、表の一つの列または複数の列の組が主キーとして用いられます。関係データベースの表の作成者は、表の主キーとなる列を指定する必要があります。主キーの値を指定すると、表のただ一つの行だけが抽出されます。また、主キーの列の値が重複する行が、表の中に複数存在してはならないという規則があります。

ワンポイント MEMO

コンピュータでの色の表現

紙に写真などを印刷する際には、シアン、マゼンタ、イエローの三つの基礎的な色(原色)の組合せで色を表現します。それに対して、コンピュータを用いてディスプレイに色を表現するときは、赤(R)、緑(G)、青(B)の三つの原色の組合せを用います。この三つの色を、光の三原色といいます。

光の三原色の組合せによって、次の図のような色を表現できます。



一般的なディスプレイでは、赤、緑、青の各色の

強さをそれぞれ256通り(0~255の数値で表される)まで選べるようにして、 $256 \times 256 \times 256 = 16,777,216$ 種類の色を表現することができます。例えば、紫色を表現する場合、赤の強さ=255、緑の強さ=0、青の強さ=255とします。このような方法を用いて、16,777,216種類の色を画面上で同時に表現できることをフルカラーといいます。

WWW(World Wide Web)の黎明期には、フルカラーに対応しておらず同時に256種類の色しか表現できないパソコンがあり、フルカラーの色を当該パソコンで再現できないことがありました。そのようなパソコンでも、できる限りWebページ作成者の意図した色に近い色を表現できるようにするために、赤、緑、青の各色の強さを6段階として、 $6 \times 6 \times 6 = 216$ 種類の色を定めました。この216種類の各色をWebセーフカラーといいます。

□ インデックス

データベース中に格納されたデータの格納場所を特定して高速な検索を実行するために、データとは別に用意される索引です。

□ 関係データベースの正規化

表の関連性を失うことなく、表の項目をグループ化して複数の表に分割していく作業のことです。データベースを一つの大きな表としてもっていると、データの修正、追加、削除の際に、関連のない項目までが操作されることになります。正規化を行って表を分割すれば、冗長構成を排除することができます。

ワンポイント MEMO

正規化の例

非正規形の表

社員番号	氏名	所属部署ID	所属部署名	担当業務1	担当業務2	担当業務3
10001	○○	101	総務部	事務	涉外	—
10002	□□	102	営業部	A社担当	B社担当	C社担当
10003	△△	101	総務部	渉外	—	—

担当業務1, 2, 3,が繰返し項目になっています。一人の社員が、それぞれ異なる数の業務を担当しているので、例えば社員番号10003の社員は担当業務2以降の列にデータが格納されず、無駄になっています。繰返し項目を排除して担当業務の列を一つだけにすることで、第1正規形にします。

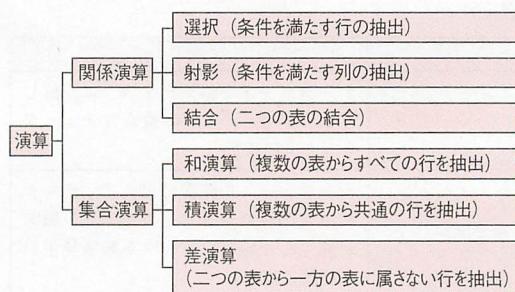
第1正規形の表（下線は主キーの列を表す。以下同じ）

社員番号	氏名	所属部署ID	所属部署名	担当業務
10001	○○	101	総務部	事務
10001	○○	101	総務部	渉外
10002	□□	102	営業部	A社担当
10002	□□	102	営業部	B社担当
10002	□□	102	営業部	C社担当
10003	△△	101	総務部	渉外

一人の社員が複数の業務を担当するので、社員番号が同じ行が複数存在します。社員番号だけでは行を一意に識別できないので、社員番号と担当業務の組が主キーになります。社員番号の値だけが決まれば、氏名、所属部署ID、所属部署名の値は一意に決まります。社員番号が同じ行が複数あり、氏名などが重複しているので、社員番号、氏名、所属部署ID、所属

□ 関係データベースの演算

関係データベースにおいて、表を操作、参照して新たな表を作成することを演算といいます。演算には、次のような種類があります。



部署名の組を別の表に移動し、第2正規形にします。

第2正規形の表

社員番号	担当業務
10001	事務
10001	渉外
10002	A社担当
10002	B社担当
10002	C社担当
10003	渉外

右の表では、所属部署IDの値が決まると所属部署名が一意に決まります。例えば、所属部署IDが101の部署の名称が変わると、右の表の複数の行の所属部署名を更新しなければならず、更新処理に時間が掛かります。このような部分をさらに別の表に移動し、第3正規形にします。

第3正規形の表

担当業務		
社員番号	氏名	所属部署ID
10001	○○	101
10002	□□	102
10003	△△	101

所属部署ID	所属部署名
101	総務部
102	営業部

右下の表では、所属部署IDによって行を一意に識別できるので、所属部署IDが主キーになります。

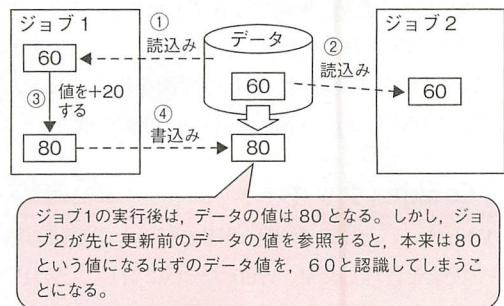
□ 排他制御

複数のジョブが同じ資源に対して同時に参照や更新を行うと、データの値に不整合が生じてしまうことがあります。

図は、初期値60のデータを更新するジョブ1と、当該データの値を参照するジョブ2が同時に実行された状況を示しています。図中の①～④は、処理の順序を示します。

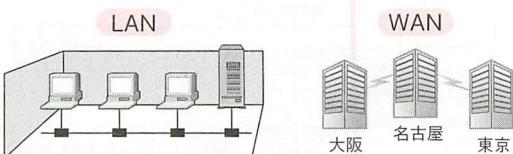
ジョブ1の更新結果がデータに反映されるのは、④の処理が行われた後です。しかし、④の前に実行された②の処理で、ジョブ2はデータの値を60（更新前の値）として認識し、更新後と異なる値を使用してしまうため、整合性が取れなくなります。

このような事態を防ぐため、一つのジョブが資源にアクセスしている間は、他のジョブをその資源にアクセスさせないで待機させておくという制御が必要です。この制御を「排他制御」といいます。



□ ネットワークの概要

個々に単独で動作していたコンピュータ（スタンドアロン）を無線もしくは有線データ通信を使用することで結んだものです。離れている場所の端末から別のコンピュータへのアクセスや、コンピュータを連携させた処理が可能となり、印刷やデータベースを共有管理できるようになります。LAN (Local Area Network) と WAN (Wide Area Network) に分類できます。

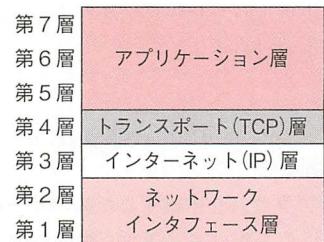


名称	説明
LAN	自前の有線もしくは無線の通信路で接続され、同じ建物内など限られた範囲内で使用できるネットワークのこと。主な接続形態にはバス型、リング型、スター型がある。

WAN	通信事業者（キャリア）の回線を借りて、国内はもとより世界中と接続することが可能なネットワークのこと。支社と本社を結んだネットワークなどが該当する。
-----	---

□ TCP/IP

Transmission Control Protocol/Internet Protocol。インターネットで使用されているプロトコルの総称のことです。ただ、狭い意味でのTCPは第4層に位置し、通信の際に相手にその送受確認を行う信頼性の高いプロトコルです。また、IPは第3層に位置し、相手にデータを送り届けるプロトコルです。



□ TCP/IPが提供するサービス

TCP/IPのアプリケーション層には、様々なプロトコルが用意されています。ネットワーク上のサーバは、これらのプロトコルを利用してサービスを提供して機能を実現します。主なサービスは次のとおりです。

名称	説明
Telnet	遠隔地のコンピュータをリモート操作する。
FTP	ファイルを転送する。
HTTP	WWWサーバとクライアント（ブラウザ）の間でデータを転送する。
SMTP	他のSMTPサーバへ電子メールを送信したり、受信した電子メールをサーバ上のメールボックスに保管したりする。
POP3	サーバ上のメールボックスから、電子メールを取り出す。

□ IPアドレス



ネットワーク間でデータ通信に使用されるアドレスで、現在多く使用されているものはIPv4 (IP version 4) と呼ばれています。長さ4バイト = 32ビットで構成されたアドレス体系で、内部の各ビットはネットワーク部とホスト部に区分されています。

近年、インターネット利用者数および接続機器数が非常に増加しています。これにより、IPアドレスの枯渇という現象が問題になっています。そこで、次世代のIPアドレスとして、IPv6が制定されました。IPv6は

128ビットの長さをもち、ネットワーク部とホスト部という区分がなくなったことなどが特徴です。

□ ポート番号

インターネット上で提供されるサービスの番号を指します。IPアドレスで通信相手のコンピュータを特定した後、ポート番号でどのサービス（アプリケーション）と通信するかを特定します。トранスポート層にあるTCPもしくはUDPでサービスを判断するため、IPパケットのTCP（UDP）フレームに書き込まれています。0～65535まで使用することができ、0～1023は決められたサービスを行うウェルノウンポート番号と呼ばれます。

□ プロキシ

組織の内部からインターネット上のサーバに対して送られるアクセスを中継するためのサーバのことです。プロキシを用いることで、組織内部のクライアントPCなどがインターネットに直接アクセスすることがなくなり、安全性が高まります。また、外部から攻撃される可能性のある機器がプロキシだけになるので、プロキシのセキュリティを強固にすることで不正アクセスなどの被害を低減させることができます。

□ MACアドレス

ネットワーク機器やコンピュータに内蔵されている、NIC（Network Interface Card）に物理的に書き込まれているアドレスで、OSI基本参照モデルのデータリンク層（TCP/IPのインターフェース層）において、コンピュータを識別するために使用されます。

□ LAN間接続装置

異なるLAN同士を接続する場合には、そのプロトコルの違いによって以下のような装置が必要になります。

名称	説明
リピータ	ハブとも呼ばれ、物理層でのデータの中継を行い、伝送されてくるデータの信号波形を増幅・修正するための装置。
ブリッジ	データリンク層のプロトコルに基づいてデータ送受信を行う機器。MACアドレスを基に送信先を決定することができます。

スイッチングハブ	LAN上の各機器のMACアドレスと、その機器がどのポートに接続されているかを記憶している。送信されてきたデータのヘッダ部分に記録されているので先MACアドレスから、データを必要最小限の送信すべきポートのみに送信し、他のポートには送信しないという処理（スイッチング）を行う。
ルータ	ネットワーク層のプロトコルに基づいてデータ送受信を行う機器。IPアドレスを基に送信先を決定することができる。
ゲートウェイ	アプリケーション層以下のすべての層について異なるLANの接続に用いる。

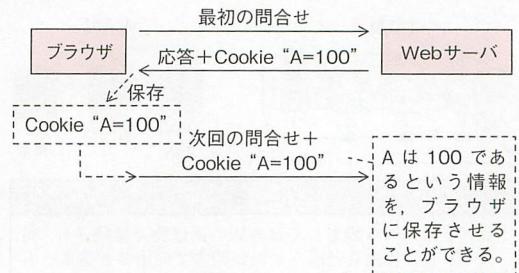
□ DNS

インターネットはTCP/IPを採用しているため、接続されたコンピュータや周辺機器はIPアドレスで識別されています。しかし、IPアドレスは数値だけで表記され、扱いにくいため、実際にはドメイン名というニックネームが利用されています。このドメイン名とIPアドレスを1対1に対応させ、相互の変換を行うシステムのことをDNS（Domain Name System）といいます。

□ Cookie（クッキー）



Webサーバとブラウザとの間でデータ送受信の順序や状態を管理したり、Webサーバに対してどのPCからアクセスが行われたかを識別したりするために用いられるものです。Cookieは、Webサーバで生成されてブラウザに送信され、ブラウザが稼働している利用者のコンピュータ内に保存されます。Cookieを送信してきたWebサーバにブラウザが再度アクセスする際には、ブラウザから送信される問合せの中にCookieが格納されます。この措置により、Webサーバからの情報をブラウザに一時的に保存させ、後で当該情報をWebサーバが参照することが可能になります。



□ RSS

RDF Site Summary または Rich Site Summary。Web

サイトの更新状況を外部に配信するための規約及びその文書形式のことです。RSSの表現にはXMLベースの言語が用いられます。RSSでは、Webページの見出し、リンク及び要約などを、決められたフォーマットに従って記述します。

□ アナログ／デジタル変換

アナログデータからデジタルデータへの変換は以下のような流れで行われます。

- (1) 標本化(サンプリング)：一定の間隔で、信号の波形の強弱をアナログ値として記録します。
- (2) 量子化：標本化において採取した信号の波形を示すアナログ値を、一定の範囲の整数値に変換します。
- (3) 符号化：量子化において変換した整数値を、一定の長さのビット列で表現します。

□ ADSL

インターネット接続回線の一つとして広く利用されるようになった通信回線および通信方式です。この方式では、アナログの電話回線を利用して、上り下りの速度が異なる高速伝送を行います。ADSLでは、スプリッタと呼ばれる機器を使用して、PCと電話機を同じ電話回線に接続しています。電話機が使用する周波数帯と、PCが使用する周波数帯は異なっているため、電話機とPCとを同時に使用していても、PCの回線速度には変化はありません。ADSLには、設置費用が少ないなどの利点がある反面、自宅に電話回線を引いている電話局(受容局)と自宅との間の距離が大きいと、伝送速度が低下するなどの欠点があります。

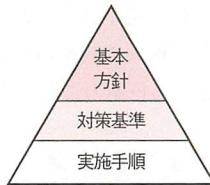
□ FTTH

インターネットに接続するための家庭向けの通信サービスの一つで、受容局から家庭まで引かれている通信回線には、光ファイバケーブルが用いられます。光ファイバケーブルは通信速度が高速なため、数十Mbps以上の高速通信を実現できます。

□ 情報セキュリティポリシー

企業などの組織が、自社の情報セキュリティを維持するための方針、システムや体制などについて規定し、その内容や内外に公表する文書のことです。情報セキュリティポリシーや、情報セキュリティポリシーに関連する文書を詳細化の順に並べると、図のよ

うになります。



名称	説明
基本方針	組織の情報セキュリティ対策についての根本的な考え方を、外部に公開するために重要な文書となる。この文書には、情報セキュリティを維持することについての組織の考え方や方針などが記載される。
対策基準	基本方針で示された情報セキュリティ対策を実現するために、組織が守るべき各種の行為や基準などを示したもの。
実施手順	対策基準で示された行為や基準などを、どのような方法や手順を用いて具体的に遵守・実行していくかを示したもの。

□ セキュリティ管理

セキュリティ管理とはシステムの運用管理の一つで、コンピュータシステムやデータなどに対する安全性を確保することです。セキュリティ管理が必要となる原因としては、障害・事故によるシステムやデータの破壊、ハードウェアの盗難、システムへの不正アクセス、コンピュータウイルスの侵入、データの漏えいや改ざんなどがあげられます。

□ シングルサインオン

一度利用者認証に成功すれば、その後はすべてのシステムを認証なしで利用できるようになるという形態のシステム及びこのようなシステムを実現するための技術です。シングルサインオンを導入することで、複数のシステムが存在し、それぞれのシステムについて異なるパスワードなどを用いて認証を受ける必要がなくなり、利用者にとって便利になります。また、管理者にとっても、複数の異なる仕様の認証システムを管理する体制をとる必要がなくなります。

□ ソーシャルエンジニアリング

人間が通常行うであろう社会的行動から、個人や企業にとって重要な情報を手に入れることをいいます。例えば、見積り書などの機密情報がゴミ箱に捨てられているのを拾うこと(スキャベンジング)や、パスワードなどを入力している際に横や後ろから覗き見すること(ショルダーハッキング)などがあります。

□ フィッシング

サイトの偽装や偽造電子メールの使用などの方法で、ユーザを騙して個人情報やパスワードなどを不正に入手しようとする行為のことです。

リスク保有

発生確率や被害額が小さいリスクに対して対策を行うと、想定される被害額よりも対策費用の方が大きくなり、かえって損をしてしまうことがある。そのため、発生確率や被害額が小さいリスクは、あえて対策を行わないままにすること。

□ SQLインジェクション

Webページの入力フォームに特殊な文字列を入力して不正なSQL文を作成させ、Webアプリケーションを誤動作させたり、データベースの内容を不正に閲覧・削除したりする攻撃方法のことです。

□ クロスサイトスクリピティング

悪意のあるサーバにアクセスすると、そこで埋め込まれたスクリプトが脆弱な別のWebサーバを経由して実行され、ユーザのCookie情報漏えいやハードディスクの破壊などの被害が起こります。

□ DoS攻撃

インターネット上で提供されているサービスに対する妨害行為です。具体的には、セキュリティホールへの攻撃や多量のデータを送りつけることによるサーバのダウンなどがあります。複数のマシンから同時に行われる場合は、DDoS(Distributed DoS)といいます。対策として、ネットワークの常時監視、パケットフィルタリングによる不審者からの要求の拒否などがあります。

□ リスクマネジメント

リスクとは、損害発生の可能性のことで、リスクマネジメントとは、損害発生を食い止めるために、起これうるリスクを想定して対応を検討することです。

リスクマネジメントは、データが破壊されたり、システムの可用性が損なわれたりした場合にシステムが使用不能の時間を最小限にするために実施します。リスクマネジメントは以下のようなものに分類されます。

名称	説明
リスク回避	リスクの発生原因を元から絶ったり、リスクに関連する事業から撤退したりすることなどによって、リスクそのものを発生しないようにすること。
リスク移転	保険に加入するなどの手段で、リスク発生時の損失や損害を他者に肩代わりさせること。
リスク低減	セキュリティ管理を厳重にしたり、障害発生時でも代替のシステムを稼働させて業務を継続できるようにしたりするなどの方法により、リスクの発生確率を減らすこと。

□ ID・パスワード管理

ユーザIDは、システムやファイルなどにアクセスする際に、どの利用者かを一意に識別するために設定する登録番号です。また、パスワードは、正当な利用者であることを確認するための合言葉です。パスワードを設定・管理する場合は、次の点に注意します。

注意点	説明
第三者に判断されやすい パスワードは避ける	名前やユーザID、生年月日など第三者に簡単に判別されるパスワードは避ける。一般に文字、数字、記号の組合せで設定することが望ましいとされる。
第三者への漏えいを防ぐ	パスワードは第三者へ漏えいしないよう注意する。パスワードの入力を他人に見られたりしない、また、パスワードをメモなどに書き残したりしない、など。
パスワードの定期的な変更	パスワードは同じものを長く使用せず、定期的に変更する。

□ ISMS

情報セキュリティマネジメントシステム。情報セキュリティを確保するための組織体制や取組みのことです。ISMSの導入、運用及び改善のために、PDCAサイクルが用いられます。

□ ISMSのPDCAサイクル



ISMSの導入・運用・改善を継続して実行するために、PDCAサイクルが用いられます。ISMSにおいて用いられるPDCAサイクルの各フェーズの名称と概要を示します。

フェーズの名称	概要
計画(Plan)	情報セキュリティの手順を決めたり、ISMSを運用する組織の体制を構築したりして、ISMSの確立を行う。
実行(Do)	ISMSの導入や運用の他に、ISMSに関する従業者への教育や訓練が実施される。
点検(Check)	ISMSの運用状況を定期的に点検して問題点を見つけ出すために、ISMSの監視及びレビューが行われる。
処置(Act)	点検フェーズで発見された問題点を改めるために、ISMSの維持や改善が行われる。

□ 情報セキュリティの3要素

情報セキュリティとは、次に示す機密性、完全性、可用性という三つの要素を維持することです。これらの三つの要素を、情報セキュリティの3要素(CIA)といいます。

要素	性質
機密性 (Confidentiality)	アクセス権限を適切に管理し、権限をもたない利用者やプロセスから、データなどを不正に参照されないように非公開にすること。
完全性 (Integrity)	データの内容を常に正しい状態に保ち、改ざんや破壊などの被害を受けないようにすること。
可用性 (Availability)	情報システムをできる限り長い間利用できるように保ち、認められた利用者が必要なときに情報にアクセスできるようにすること。

□ 情報セキュリティ対策

ネットワークは、不特定多数が利用するため、それに対応したセキュリティ対策が必要になります。外部からの不正アクセス対策には、次のようなものがあります。

手法	説明
コールバック	電話の着信者が、発信者を確認していったん接続を切り、再度着信者側からかけ直すこと。社内ネットワークへの外部からの不正アクセスを防止するために利用される。
ワンタイムパスワード	利用者が一度しか使用できない使い捨てパスワード。パスワードが第三者に漏えいしても、再度利用することはできないので安全性が高い。

□ ファイアウォール

社内LANとインターネットとの間に設置される装置で、外部からの不正なアクセスなどを遮断するために用いられます。

□ DMZ

DeMilitarized Zone：非武装地帯。外部に公開するサーバを、ファイアウォールでインターネット及び社内LANの両方から隔離して配置する領域のことです。外部(インターネット)からDMZへのアクセスについては、一定の条件を満たす安全なパケットのみ通過させるようにします。

□ SSL

Secure Socket Layer。Webサーバとブラウザとの間で暗号化技術を用いて情報を安全に送受信するためのプロトコルです。このプロトコルでは、サーバ証明書を用いて、Webサーバの正当性をブラウザが確認できるようにしています。

□ バイオメトリクス認証

指紋、虹彩、網膜、顔の形状などの、人間の身体的特徴から個人の識別を行う認証システムです。このシステムでは、認証を受けるユーザの指紋の形状などと、登録した本人の指紋の形状などを比較し、両者の類似の度合いが一定以上であれば、本人と識別します。また、本人の行動的特徴を記憶し、認証を受けるユーザの行動がその特徴に従っているかどうかによって本人と識別する認証方法もあります。

□ コンピュータウイルス

コンピュータに侵入し、意図的にデータを破壊するなどのトラブルを発生させるプログラムです。ウイルスは、ネットワークなどを介して入手したプログラムから感染する場合が多く、ウイルスの検出や除去には、ウイルス対策ソフトを利用します。通常、他のプログラムに寄生するものを指しますが、広い意味では以下のようなものも含みます。

名称	説明
ワーム	自己伝染型のウイルスで、電子メールやWebなどを介して次々と感染してハードディスクを破壊したりする。
トロイの木馬	潜伏型のウイルスで、別のプログラムなどから感染することが多い。クライアントが何らかの処理を行わない限り発症はしないが、いったん発症するとそのクライアントを経由して別のコンピュータにアクセスしたりする。
マクロウイルス	ワープロや表計算で使用するデータに感染させるタイプのウイルス。

□ クラッキング

クラッカーが他人のコンピュータやネットワークに侵入し、データの改ざんや破壊、盗用などを行うことです。

□ ポット

bot。不正な動作を行うプログラム(ウイルスなど)の一種です。PCに感染したボットは、特定のタイミングで攻撃者から発せられた指示に従い、PCの

ネットワーク接続機能などを不正に操作して、特定のWebサーバなどに対して一斉にメッセージを送信し、当該サーバの処理を遅くするなどの攻撃を行うようになります。

□ アドウェア

PCの画面上に、広告を強制的に表示するソフトウェアのことです。広告(Advertisement)の略語である“Ad(アド)”が語源です。

アドウェアには、便利な機能を無料で利用できる代わりに広告を表示する形式の無害なものもあれば、スパイウェアによって不正にインストールされて強制的に広告を表示したり、利用者のPC内の情報を密かに外部に送信したりする有害なものもあります。

□ ランサムウェア

コンピュータに害を加えようとする、不正プログラムの一種です。「ランサム(ransom)」は「身代金」を意味します。

ランサムウェアは、攻撃対象のコンピュータに感染し、ファイルなどを勝手に暗号化して、利用者がデータを利用できないようにします。そして、データを元に戻すためのアプリケーションの購入を促すメッセージを表示するなどの方法で、利用者に代金を払わせようとします。

ランサムウェアには、ウイルスと同様の経路で感染するものや、トロイの木馬のように、有益なプログラムに見せかけて利用者のインストールを促すものがあります。

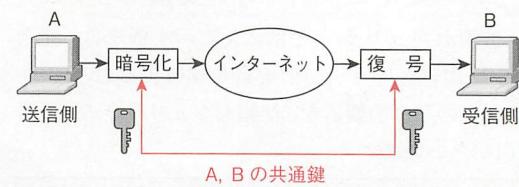
□ 暗号化方式



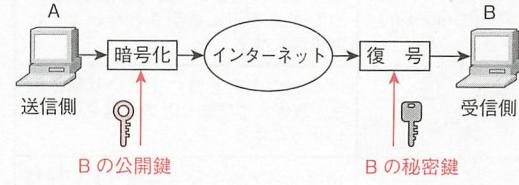
現在、一般に利用されている代表的な暗号化方式には、共通鍵暗号方式と公開鍵暗号方式があります。

名称	説明
共通鍵 暗号方式	暗号化と復号に同じ鍵を利用する方法。公開鍵暗号方式に比べて高速であるが、大量の鍵を管理する必要があることや、鍵の配達やその管理などに問題がある。代表的な方式に、DESやAESがある。
公開鍵 暗号方式	送信内容を秘匿したい場合、暗号化に公開鍵を、復号には公開鍵と対になる秘密鍵を利用する方法。暗号化は公開鍵を利用するため誰でも行うことができるが、復号は秘密鍵をもつ本人しかできない。代表的な方式に、RSAがある。

共通鍵暗号方式



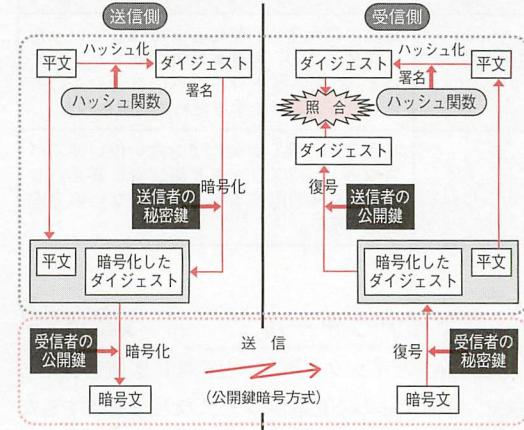
公開鍵暗号方式



□ デジタル署名



デジタル署名(電子署名)は、データを送信する際に署名情報を付加して、送信データが署名者本人からのものであるという正当性を保証する技術です。公開鍵暗号方式では誰もが暗号化の鍵(公開鍵)を入手できるので、暗号文の送信者が正当な相手であるかどうかを確認するためにデジタル署名が必要になります。



□ PKI

Public Key Infrastructure : 公開鍵基盤。公開鍵暗号方式及びデジタル署名の仕組みを応用した、公開鍵の正当性を証明するための各種の仕組みのことです。公開鍵の正当性を証明するために、認証局(CA)という機関が発行する公開鍵証明書が用いられます。