基本情報技術者試験

更新日：2024年5月16日

目次

[1. A試験 2](#_Toc166771428)

[1.1. テクノロジー系 2](#_Toc166771429)

[1.1.1. 基礎理論 2](#_Toc166771430)

[1.1.2. コンピュータシステム 4](#_Toc166771431)

[1.1.3. 技術要素 12](#_Toc166771432)

[1.1.4. 開発技術 20](#_Toc166771433)

[1.2. マネジメント系 22](#_Toc166771434)

[1.2.1. プロジェクトマネジメント（PM） 22](#_Toc166771435)

[1.2.2. サービスマネジメント（SM） 23](#_Toc166771436)

[1.3. ストラテジ系 24](#_Toc166771437)

[1.3.1. システム戦略 24](#_Toc166771438)

[1.3.2. 経営戦略 24](#_Toc166771439)

[1.3.3. 企業と法務 25](#_Toc166771440)

[2. B試験 27](#_Toc166771441)

[3. 参照文献 27](#_Toc166771442)

# A試験

## テクノロジー系

### 基礎理論

#### 基礎理論

* 絶対誤差・相対誤差
* パリティチェック

データ通信．メモリチェックなどにおいてデータのビット誤りを検出する方法．

「1」のビット数が奇数にする→奇数パリティ

「1」のビット数が偶数にする→偶数パリティ

* + やり方（[[1]](#footnote-1)奇数パリティビットを付加する場合）

1. 16進数の文字コードを*n*ビットの2進数に変換
2. 「1」のビット数チェック
3. 「1」のビット数が奇数ならば．先頭に「1」追加
4. 16進数に戻す．

* アクチュエータ

入力された電気信号を力学的な運動に変換し、制御対象を一定の状態に保つなどの制御を行う装置のこと．空気圧，油圧，磁力，光エネルギーなどを動作に変換するものが存在する．

#### アルゴリズムとプログラミング

* アルゴリズム
* 探索アルゴリズム
  + 線形探索法
  + 二分探索法
  + ハッシュ表探索法
* 併合アルゴリズム
* 整列アルゴリズム

対象集合から基準要素を選び，大きいものと小さいものの集合に分割する

* + バブルソート
  + 選択ソート
  + 挿入ソート
  + シェルソート
  + マージソート
  + クリックソート
  + ヒープソート
* 再帰アルゴリズム
* 文字列処理アルゴリズム
  + 順次探索法
  + ボイヤ・ムーア法
* ファイル処理アルゴリズム
  + コントロールブレーク処理
  + 併合処理
* アルゴリズム評価
  + アルゴリズムオーダー記法

表 1　アルゴリズムの比較回数とオーダー記法

|  |  |  |  |
| --- | --- | --- | --- |
|  | アルゴリズム | 探索：平均繰り返し回数  整列：比較回数 | [[2]](#footnote-2)オーダー記法 |
| 探索 | 線形探索法 |  |  |
| 二分探索法 |  |  |
| ハッシュ表探索法 |  |  |
| 整列 | バブルソート |  |  |
| 選択ソート |  |  |
| 挿入ソート |  |  |
| シェルソート | 間隔に依存 |  |
| マージソート |  |  |
| クリックソート |  |  |
| ヒープソート |  |  |

* プログラミング言語
* マークアップ言語
  + HTML (=Hyper Text Markup Language)

Web上のドキュメントを記述するためのマークアップ言語．

* + CSS (=Cascading Style Sheets)
  + XML (=Extension Markup Language)

### コンピュータシステム

#### コンピュータ構成要素

* プロセッサ

コンピュータの中枢をなす部分．CPU (=Central Processing Unit)のことを指す．

* コンピュータの構成
* CPUの構成
  + 演算装置
  + 制御装置
    - レジスタ

処理中の命令などを一時的に記憶する領域のこと．

* + - * 命令レジスタ
      * 命令アドレスレジスタ
      * インデックスレジスタ
      * ベースレジスタ
      * アキュームレーター
      * 汎用レジスタ
      * スタックポインタ
    - デコーダ

プログラムの命令を解読する装置のこと．「命令解読器」，「復号機」ともいう．

* + - * 命令デコーダ

命令レジスタから受け取った命令を解読する

* アドレス指定方式

1. 直接アドレス指定：値そのまんま
2. 間接アドレス指定：主記憶上のアドレスを指定し，格納されている値
3. 指標アドレス指定：インデックスレジスタの値を加えたもの
4. 基底アドレス指定：ベースレジスタの値を加えたもの
5. 相対アドレス指定：プログラムカウンターの値を加えたもの
6. 即値アドレス指定：演算対象データ

* CPUの性能
  + クロック周波数
    - CPUの命令実行数

命令実行数を，クロックサイクル周波数をとする．GHzで動作できるCPUの1命令を平均クロックで実行するため，以下の式になる．

* + - CPUの1クロック当たりの処理時間

クロックサイクル時間をとすると，以下の式になる．

* + CPI (=Cycles Per Instruction)
    - CPUの1命令当たりの実行時間

1命令当たりの実行時間を，1命令当たりのクロック数をとすると，以下の式になる．

* + MIPS (=Million Instruction Per Second)

を1命令実行時に必要な時間とすると以下の式になる．

* + 命令ミックス
    - 命令ミックスのCPUの処理能力

命令ミックスのCPUの処理能力を，命令実行速度を，出現比率をとする

* CPUのアーキテクチャ
  + RISC (=Reduced Instruction Set Computer)

使用頻度の高い命令を固定長方式で単純化することで，パイプライン方式の効率を高め，動作速度の向上や処理速度の短縮を図るもの．PCやワークステーションなどのCPUに採用されている．

RISCのCPUでは，ハードウェアの回路で制御信号を発生させる「ワイヤドロジック（結線論理）方式」を用いられる．

* + CISC (=Complex Instruction Set Computer)

可変長方式の複雑な命令をCPUが理解できるようにすることで，全体的に高性能化を図るもの．スーパーコンピューター，汎用コンピュータなどのCPUに採用されている．

CISCのCPUは，1命令中での処理が複雑なため，「マイクロプログラム制御方式」を用いられる．

* + - マイクロプログラム

基本動作を記述したマイクロコード（単純な命令）でできたプログラムのこと．

* CPU高速化技術
  + パイプライン方式

命令の処理は，

1. 命令の取り出し（命令フェッチ）
2. 命令部の解読（命令デコード）
3. アドレス計算
4. データの読み出し
5. 命令の実行　など

いくつかの過程（ステージ）に分割できる．このステージをずらしながら同時に命令を処理することで高速化を図る技術のこと．

* + スーパーパイプライン方式

パイプライン方式のステージをさらに細分化して高速化を図る技術のこと．

* + スーパースカラ方式

複数のパイプラインを同時実行することで高速化を図る技術のこと．

* + VLMW (=Very Long Instruction Word)

依存関係にない複数の短い命令を，1つの命令にまとめて同時実行することで高速化を図る技術のこと．命令の長さは一定ではないため，長さが足りないときは「何もしない」という命令が挿入される．

* マルチプロセッサシステム
  + 蜜結合マルチプロセッサシステム
  + 疎結合マルチプロセッサシステム
* メモリ

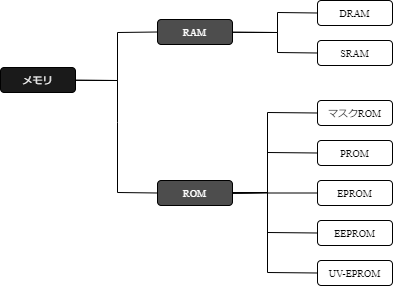


図 1　メモリの種類

* RAM (=Random Access Memory)

電源を切ると記憶している内容が消去される発揮性メモリのこと．

|  |  |
| --- | --- |
| 種類 | 説明 |
| DRAM  (=Dynamic Random Access Memory) | コンデンサとトランジスタで構成されたメモリ．自然放電のため，電気を再補充し，書き込みを行う「リフレッシュ」が必要である． |
| SDRAM  (=Synchronous Dynamic Random Access Memory) | システムバスに同期して動作をするDRAMのこと．非同期型DRAMより、データの読み書きが速く現在，主流のDRAMである． |
| SRAM  (=Static Random Access Memory) | トランジスタで構成されたメモリのこと．直前の状態を保持する「フリップフロープ回路」を使用するため，リフレッシュは不要である． |

* + フリップフロック回路：2つの安定状を持つことで1ビットの状態を表現することが可能な順序回路→SRAMの記憶セルに使用される
* ROM (=Read Only Memory)

読み出し専用，電源の供給が切れても内容を保持可能な不揮発性メモリで電源投入時に実行されるプログラムの格納に適する．

|  |  |
| --- | --- |
| 種類 | 説明 |
| マスクROM | キャッシュメモリと主記憶装置の両方に同時に書き込みを行う方式． |
| PROM |  |
| EPROM |  |
| EEPROM |  |
| UV-EPROM | 先に，キャッシュメモリだけに書き込みを行い，キャッシュメモリの退避後に，主記憶装置に書き込みを行う方式． |

* + BIOS (=Read Only Memory)
  + フラッシュメモリ

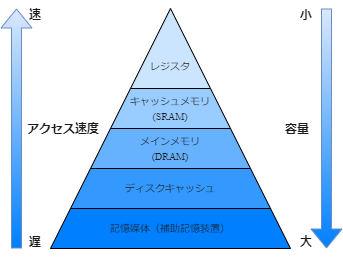


図 2　記憶階層

* キャッシュメモリ

CPUの処理速度と主記憶の読み出し速度の差を埋めるための装置のこと．

* + キャッシュメモリの書き込み方式

|  |  |
| --- | --- |
| 書き込み方式 | 説明 |
| ライトスルー方式 | キャッシュメモリと主記憶装置の両方に同時に書き込みを行う方式． |
| ライトバック方式 | 先に，キャッシュメモリだけに書き込みを行い，キャッシュメモリの退避後に，主記憶装置に書き込みを行う方式． |

* + ディスクキャッシュ

主記憶と記憶媒体（補助記憶装置）の処理速度の差を埋めるメモリのこと．

* + キャッシュメモリの平均実効アクセス時間

ヒット率を，主記憶装置のアクセス時間を，キャッシュメモリにある場合のアクセス時間を，ない場合のアクセス時間をとする．平均アクセス時間は，以下の式になる．

* 磁気ディスクのアクセス時間

アクセス時間は，待ち時間（平均シーク時間と平均回転待ち時間）とデータ転送時間の合計は，

1分間当たりの回転数を，1分をミリ秒()は，に変える．1回転時間は，

次に，平均回転待ち時間は，

さらに，1トラック当たりの記憶容量をとする．データ転送速度は，

そして，データ転送時間は，

よって，平均位置決め時間をとする．アクセス時間は

となる．

まとめると，

となる．

* デイジーチェーン接続

複数に機器を数珠つなぎに配線する接続形態（SCSI（スカジー））のこと．「PC－周辺機器－周辺機器」のような接続方法である．

* ビデオメモリ容量

RGB画像メモリ各ビット（表示色数は）の画素の記憶容量は，

カラービット数を含めると，

となる．

#### システム構成要素

* システム構成
  + デュアルシステム：同じ処理を2組のコンピュータで行い，照合機でチェックしながら処理を進行していくシステム．完全2系統であるため，稼働率，信頼性が高い．
  + シンプレックスシステム

すべての機器が１系列で構成され，必要最小限の機器で構成されたコンピュータシステムのこと．構成機器が１つでも障害が発生すれば動作不能に陥るため，稼働率，信頼性ともに低い．

* + デュプレックスシステム

主系と待機系からなる2系列の処理システム構成

* + - コールドスタンバイシステム

主系と待機系の2系統で構成されたシステム。障害発生時は手動で切り替える．

* + - ホットスタンバイシステム

主系と待機系の2系統で構成されたシステム。主系と待機系で別々の処理を行わず，待機系を常に主系と同じ状態で待機させておくことで、障害発生時は迅速に切り替えることが出来る．

* + ロードシェアリングシステム（負荷分散システム）
* クライアントサーバーシステム
  + シンクライアントシステム：シン(Thin)は「薄い，少ない」の意味で，使用する端末のサーバ接続するための最小限のネットワーク機能，入出力をするためのGUIなどだけを装備させ，ほとんどの処理をサーバ側で行うシステム，設計，端末そのものことを指す．
* RAID (=Redundant Arrays of Inexpensive Disks)

信頼性やアクセス速度の向上を目的とした障害対策のひとつ．複数のハードディスクをまとめて一つの装置として扱う技術のこと．レベルの区別は，データと冗長ビットの記録方法と位置の組み合わせにより分けられる．

|  |  |
| --- | --- |
| RAIDの種類 | 説明 |
| RAID0 | ディスクストライピングのことで，複数のディスクに分散してデータを書き込むことで，アクセス性能を向上させる技術． |
| RAID1 | ディスクミラーリングのことで，同じデータを2台のディスクに書き込むことで，信頼性を向上させる技術． |
| RAID2 | ストライピングとエラー訂正用のハミング符号を1台のディスクにビット単位で書き込む．最低でも5台構成である． |
| RAID3 | ストライピングとエラー修正用にパリティビットを1台のディスクにビット/バイト単位で書き込む． |
| RAID4 | RAID3とほぼ同様．パリティビットの書き込みをブロック単位で行う． |
| RAID5 | パリティビットもデータと同様に複数台のディスクに分散してブロック単位で書き込む． |
| RAID6 | パリティ情報を2つ生成し、すべてのハードディスクに分散して記録する． |

* NAS (=Network Attached Storage)

TCP/IPのコンピュータネットワークに直接接続して使用するファイルサーバでコントローラーとハードディスクから構成されている．データ共有単位は「ファイル」である．

* 信頼性設計

|  |  |
| --- | --- |
| 名称 | 説明 |
| フォールトトレラントシステム | システムの一部に障害発生しても，全停止することなく稼働を続け，その間に復旧を図るような設計となっているシステム |
| フェールソフト | 障害発生時に，システムが全面的に停止しない様に，必要最小限の機能を維持する． |
| フォールトアボイダンス | 機器自体の信頼性を高めることで故障しないようにする． |
| フェールセーフ | 障害発生時に，システムを安全な状態に固定し，その影響を限定する． |
| フールプループ | 利用者が本来の仕様からずれたことをしても，故障しないようにする． |

* システムの性能評価
  + スループット

システムで単位時間あたり処理される仕事の量を表す言葉．

* + システム性能指標
    - レスポンスタイム

コンピュータに処理を依頼してから，最初の反応が返ってくるまでの時間のこと．

* + - ターンアラウンドタイム

コンピュータに一連の処理を依頼してから，すべての処理結果を受け取るまでの時間のこと．

* + - * ターンアラウンドタイムの計算式

CPU時間を，入出力時間を，処理待ち時間をとすると，

となる．

* + - ベンチマークテスト

システムの使用目的に合わせたプログラム，あるいは評価対象の業務の典型的な処理プログラムを実行し，入出力や制御プログラムを含めたシステムの総合的な処理性能を測定する手法のこと．

* + - モニタリング

実際のシステムに性能を測定するための機器（ハードウェアモニタリング）やプログラム（ソフトウェアモニタリング）を組み込み、どのように動作するかを計測すること．

* + - キャパシティプランニング

予算や費用対効果を考慮しつつ，必要な性能要件を満たすようなシステム開発できるように管理するプロセスのこと．

* + - * キャパシティプランニングの手順

1. 現行システムをモニタリングし現状の処理能力の把握（案の評価・見直し）
2. 将来的に予想される端末数，利用者数の増加などを分析（増設検討）
3. 2．の分析結果からシステム能力の限界時期を予測（現状処理能力の把握と将来予測）
4. 新システム構成で実現すべき性能要件から必要なハードウェア増設を検討（増設検討）
   * 新しいコンピュータシステムを選択するときに行うシステムの性能評価について

実際の利用条件や環境（よく利用されるプログラム，処理時間が重要なプログラムなど）と同じような状況下で行うことで精度の高いデータが得られる．

* システムの信頼性と評価

表 2　RASIS

|  |  |  |
| --- | --- | --- |
| 英語名 | 日本語名 | 意味 |
| Reliability | 信頼性 | 故障しにくい |
| Availability | 可用性 | 稼働率が高い |
| Serviceability | 保守性 | 障害時に復旧しやすい |
| Integrity | 完全性 | データに矛盾が発生しない |
| Security | 安全性 | 機密性が高い |

* 稼働率

稼働率，平均故障間隔を，平均修復時間を，全運用時間を，故障時間をとする．

* 故障率

稼働率，平均故障間隔を，故障率をとする．

* 直列システム稼働率
* 並列システム稼働率

#### ソフトウェア

* スプーリング

CPUが低速な入出力装置の処理を持たなくてもいいように出力データを補助ディスク装置に一度送り，データ転送する仕組み

* タスク管理

|  |  |
| --- | --- |
| タスク管理方式 | 説明 |
| 優先度方式 | 各タスクに設定された優先度の高い順に実行する方式 |
| タイムスライス方式 | 一定時間ごとにタスクを切り替えながら実行する方式 |
|  |  |
|  |  |
|  |  |

* 記憶管理
  + ページング方式

仮想空間データを固定長に分割し，主記憶と補助記憶装置のアドレス変換する方式

* + スラッシング

ページング処理の多発で処理効率が低下する現象

コンパイラ：ソースコードを機械語などに一括翻訳するソフトウェア

### 技術要素

#### ヒューマンインタフェース

* IrDA (=Infrared Data Association)

携帯電話のアドレス帳などのデータ交換を行う場合に．赤外線を用いて無線通信をする技術

#### マルチメディア

#### データベース

* スキーマ

データの内容，論理構造，記憶形式，構成などデータベースの構造を記述したもの

* 共有ロック（読み込みロック）：データ読み込み時に使うロック
* 専有ロック（排他ロック）：データ更新時に使うロック

表 3　ロックの獲得

|  |  |  |
| --- | --- | --- |
|  | 専有ロック | 共有ロック |
| あとから実行して獲得するロック | × | × |
| × | 〇 |

〇：ロックを獲得できる

　×：ロックを獲得できない

* ログデータ

データベースの更新履歴のようなもの

* ストアドプロシージャ

データベースに対する一連の処理をまとめた手続きにして，データベース管理システムに保存したもの

#### ネットワーク

* ネットワーク形態
* ネットワーク技術
* ネットワークポロシ
* 通信プロトコル

|  |  |  |  |
| --- | --- | --- | --- |
| OSI基本参照モデル | | 中継装置 | TCP/ID |
| 第7層 | アプリケーション層 | ゲートウェイ | アプリケーション層 |
| 第6層 | プレゼンテーション層 |
| 第5層 | セション層 |
| 第4層 | トランスポート層 | トランスポート層 |
| 第3層 | ネットワーク層 | ルータ | インターネット層 |
| 第2層 | データリンク層 | ブリッジ．スイッチングハブ | ネットワークインターフェース層 |
| 第1層 | 物理層 | リピータ．ハブ |

* LAN内の中継装置
  + リピータ

物理層で接続．データ伝送中に弱くなった電気信号を増幅することでデータの伝送化の距離を延長する装置

* + スイッチングハブ

データリンク層で接続．宛先MACアドレスが存在するLANポートだけパケット転送する機能を持っているハブのこと．

* LANとWANの中継装置
  + ブリッジ

データリンク層で接続．通過パケットのMACアドレスを見てパケットを中断するか判断する装置

* + ルータ

ネットワーク層で接続．通過パケットのIPアドレスを見てパケットを最適な経路および中継する装置

* + ゲートウェイ

7層すべてを認識．トランスポート層以上でプロトコルの異なるネットワーク同士を接続する役割を持つ装置

* アプリケーション層プロトコル

|  |  |
| --- | --- |
| 名称 | 説明 |
| SMTP  (=Simple Mail Transfer Protocol) | 電子メールを送信または，メールサーバ間での転送するプロトコル． |
| POP3  (=Post Office Protocol Version 3) | メールサーバからメールを取り出すときに使用するプロトコル． |
| IMAP4  (=Internet Message Access Protocol Version 4) | メールサーバから電子メールを受信するプロトコル． |
| HTTP  (=Hyper Text Transfer Protocol) | ハイパーテキストを転送するプロトコル． |
| FTP  (=File Transfer Protocol) | ファイル転送を行うための通信プロトコル． |
| TELNET | ネットワーク経由でコンピュータをリモートで遠隔操作するプロトコル． |
| SNMP  (=Simple Network Management Protocol) | TCP/IPプロトコルで，構成機器や障害時の情報収集を行うために使用されるネットワーク管理プロトコル． |
| DNS  (=Domain Name System) | ドメイン名とIPアドレスを結び付けて変換する仕組み． |
| DHCP  (= Dynamic Host Configuration Protocol) | TCP/IPネットワークで，IPアドレスを自動的に行うプロトコル． |
| NTP  (=Network Time Protocol) | ネットワーク経由で．各装置の時刻を同期するプロトコル． |

* トランスポート層プロトコル

|  |  |
| --- | --- |
| 名称 | 説明 |
| TCP  (=Transmission Control Protocol) | データ送信が正常かの確認をしながら通信を行い，信頼性の高いデータ転送サービスを提供する． |
| UDP  (=User Datagram Protocol) | データ送信が正常かの確認をしないため信頼性の保証がないが，高速データ転送サービスを提供する． |

* + ポート番号

表 4　代表的なポート番号

|  |  |
| --- | --- |
| ポート番号 | プロトコル |
| 20, 21 | FTP |
| 23 | TELNET |
| 25 | SMAP |
| 80 | HTTP |
| 8080 | 代替HTTP |

* インターネット層プロトコル

|  |  |
| --- | --- |
| 名称 | 説明 |
| IP  (=Internet Protocol) | ネットワーク上で一意のアドレスを使い，個別のコンピュータやサーバを認識するプロトコル． |
| ICMP  (=Internet Control Message Protocol) | IPパケットによる通信状況をメッセージで送信するプロトコル． |
| ARP  (=Address Resolution Protocol) | IPアドレスから対応する機器のMACアドレスを取得するプロトコル． |

* ネットワークインターフェース層プロトコル

|  |  |
| --- | --- |
| 名称 | 説明 |
| PPP  (=Point to Point Protocol) | 電話回線を通じてコンピュータをネットワークに接続するダイヤルアップ接続によく用いられ．2点間の接続でデータ通信を行うための通信プロトコル． |
| PPPoE  (=Point to Point Protocol over Ethernet) | LAN上でPPP機能を提供する．PPPを応用し，インターネットで利用できるようにしたもの． |
| IPoE  (=Internet Protocol over Ethernet) | LAN上でIPパケットを伝送して通信を行う．PPPoEと比較して，より高速通信が可能になる． |

* IPアドレス
  + MACアドレス(=Media Access Control Adress)

ネットワーク上の各機器を識別するために．原則的に世界中の機器に一意に割り当てられた番号のこと．前半24ビットは「OUI(ベンダID)(＝Organizationally Unique Identifier)」．後半24ビットは「固有製造番号」で構成されている．

* + アドレスクラス

|  |  |  |
| --- | --- | --- |
| アドレスクラス | 項目 | IPアドレス範囲 |
| A | アドレス範囲 | 0.0.0.0 ～ [[3]](#footnote-3)127.255.255.255 |
| グローバルIPアドレス | 1.0.0.0 ～ 9.255.255.255  11.0.0.0 ～ 126.255.255.255 |
| プライベートIPアドレス | 10.0.0.0 ～ 10.255.255.255 |
| B | アドレス範囲 | 128.0.0.0 ～ 191.255.255.255 |
| グローバルIPアドレス | 128.0.0.0 ～ 172.15.255.255  172.32.0.0 ～ 191.255.255.255 |
| プライベートIPアドレス | 172.16.0.0 ～ 172.31.255.255 |
| C | アドレス範囲 | 192.0.0.0 ～ 223.255.255.255 |
| グローバルIPアドレス | 192.0.0.0 ～ 192.167.255.255  192.169.0.0 ～ 223.255.255.255 |
| プライベートIPアドレス | 192.168.0.0 ～ 192.168.255.255 |
| D | アドレス範囲 | 224.0.0.0 ～ 239.255.255.255 |
| E | アドレス範囲 | 240.0.0.0 ～ 255.255.255.255 |

* + サブネットマスク

IPアドレスをネットワークアドレスとホストアドレスに分割した32ビット(IPv4アドレスの場合)のビット列のこと．

* + - 同一ネットワークかどうかチェックしたいとき

1. サブネットマスク，両PC のIPv4アドレスの後半を8ビットで2進数変換する．
2. 2進数変換した後半8ビットの論理和(AND)を求める．
3. 後半8ビットの論理和(AND)が一致すれば．同一ネットワークに属することがわかる．

* NAT (=Network Address Translation)

プライベートIPアドレスの１つの端末が，1つのグローバルIPアドレスを使ってアドレスを変換し，インターネット接続を利用する仕組みのこと．同時に複数のコンピュータが外部との通信する場合，接続する数だけのグローバルIPアドレスが必要になる．

* IPマスカレード（NAPT (=Network Address Port Translation)）

プライベートIPアドレスの複数の端末が，1つのグローバルIPアドレスを使ってアドレスを変換し，インターネット接続を利用する仕組みのこと．社内ネットワークに接続されたすべてのコンピュータで，インターネットへ同時接続できる．

クライアント側：プレゼンテーション層

* サーバ側：ファンクション層，データ層
* インターネット
* 電子メール
  + MIME (=Multipurpose Internet Mail Extension)

ASCII文字しか対応しないSMTPを利用したメールで．静止画．動画．音声などのデータ送信するための仕組み．

* Web関連
  + URL (=Uniform Resource Locator)

インターネット上のリソースを特定するための形式的な記号の並び．

URLの書式:「プロトコル名://[[4]](#footnote-4)FQDN/ディレクトリ名/ファイル名」

* + CGI (=Common Gateway Interface)

ユーザーの入力した情報により．表示するWebページを変化させるなど．動的なWebページを作成するための仕組み．

* 回線計算法

伝送時間を，データ量を，回線速度を，回線利用率をとする．

#### セキュリティ

* 情報セキュリティ三大要素

|  |  |
| --- | --- |
| 要素 | 説明 |
| 機密性 (Confidentiality) | アクセスを許可された者だけが、確実に情報アクセスできること． |
| 完全性 (Integrity) | 情報、処理方法が正確で、完全である状態に保たれていること． |
| 可用性 (Availability) | 認可された利用者が、必要な時に情報、関連する資産に確実にアクセスできること． |

* マルウェア・不正プログラム
* サイバー攻撃
  + パスワードクラッシュ

|  |  |
| --- | --- |
| 攻撃手法 | 説明 |
| 総当たり（ブルートフォース）攻撃 |  |
| 辞書攻撃 |  |
| パスワードリスト攻撃 |  |

* + 標的型

|  |  |
| --- | --- |
| 攻撃手法 | 説明 |
| APT (=Advanced Persistent Threats)攻撃 |  |
| 水飲み型攻撃 |  |
| やり取り型攻撃 |  |

* + サービス妨害

|  |  |
| --- | --- |
| 攻撃手法 | 説明 |
| DoS (=Denial of Service) 攻撃 |  |
| DDoS (=Distributed Denial of Service) 攻撃 |  |
| メールボム |  |

* + なりすまし

|  |  |
| --- | --- |
| 攻撃手法 | 説明 |
| セッションハイジャック |  |
| 踏み台 |  |
| IPスプーフィング |  |
| キャッシュポイズニング（DNSキャッシュポイズニング） | DNSサーバからのにウソのドメイン情報を注入して，偽装されたサーバに誘導する |
| MITB (=Main In the Bowser)攻撃 |  |
| SEO (=Search Engine Optimization)ポイズニング |  |

* + 不正スプリプト・命令

|  |  |
| --- | --- |
| 攻撃手法 | 説明 |
| クロスサイトスクリプティング(XSS)  (=Cross Site Scripting) |  |
| クロスサイトリクエストフォージェリ (CSRF)  (=Cross Site Request Forgeries) |  |
| SQLインジェクション | Webアプリに対してデータベースへの命令文を構成する不正入力データを与え，想定外のSQL文を意図的に実行させることで，データベースの情報を改ざんおよび削除する攻撃 |
| ディレクトリトラバーサル |  |
| クリックジャッキング |  |
| ドライブバイダウンロード |  |

* + その他

|  |  |
| --- | --- |
| 攻撃手法 | 説明 |
| フィッシング |  |
| ワンクリック詐欺 |  |
| ゼロディ攻撃 | OSなどの脆弱性を突いて，提供前に攻撃を仕掛けること． |
| サイドチャネル攻撃 |  |
| バッファオーバーフロー |  |
| フットプリンティング |  |
| ポートスキャン | ポート番号にアクセスし．空いているポートを調べること．攻撃者は．侵入できそうなポートがあるかどうかを事前調査する． |
| セキュリティホール | 開発段階では想定していないセキュリティ上の脆弱性のこと． |

* セキュリティホール

開発段階では想定していないセキュリティ上の脆弱性のこと．

* ポートスキャナー

検査対象おコンピュータ，ルータの通信ポートに信号を送ることで，サービスの稼働状態を外部から調査するツール

* セキュリティ対策
  + ファイアウォール

インターネットからの不正侵入を防御する仕組みのこと．社内ネットワークとインターネットの出入口となって．通信を監視，不正通信の遮断を行う．

* + - WAF (=Web Application Firewall)

Webアプリに対する攻撃を検知したとき，アクセスを遮断できるファイアウォール．XSS，SQLインジェクションなどに有効である．

* + DMZ (=Demilitarize Zone)

社内ネットワークとインターネットなどの外部のネットワーク間に設置するネットワーク領域のこと．Webサーバ，メールサーバ，プロキシサーバなど情報ネットワークとの通信が必要なものにDMZに移す．

* + LANアナライザー

LAN上の通過するパケットの監視・記録するためのハードウェアまたは，ソフトウェアのこと．

* 暗号技術
  + 共通鍵暗号方式

暗号化と復号で同一の鍵（共通鍵）を使用する暗号方式のこと．共有鍵は，第三者に知られては，盗聴，改ざんを防げないため，秘密裏で共有しなければならない．「秘密鍵暗号方式」とも呼ばれる．

* + - 暗号アルゴリズム
      * DES (=Data Encryption Standard)

データを64ビット単位のブロックごとに暗号化する．

* + - * AES (=Advanced Encryption Standard)

DESの後継規格であり，暗号化・復号の処理が高速かつ強度が高いという特徴を持つ．

データを128ビット単位のブロックごとに暗号化をするし，鍵長は128，192，256ビットから選択する．

* + - 必要な共通鍵の総数

必要な共通鍵の総数をとする．

* + - ブロック暗号

データを一定の長さのブロックに区切り，ブロック単位で暗号化すること

* + - ストリーム暗号

データを1ビット単位または，1バイト単位で逐次暗号化する方式のこと．

* + 公開鍵暗号方式

暗号化と復号に異なる鍵を使用する暗号方式のこと．秘密鍵と公開鍵は必ずペアで生成され，公開鍵で暗号化された暗号文は，対象の秘密鍵しか復号できない．秘密鍵は，第三者に公開してはいけないが，公開鍵は，第三者に公開するため，「認証局(CA (=Certificate Authority))」に登録して公開する．

* + - 認証局(CA (=Certificate Authority))

公開鍵暗号方式，デジタル署名などに使用される公開鍵の正当性を保証するための証明書（デジタル証明書）を発行する機関のこと．

* + - RSA (=Rivest Shamir Adleman)

桁数の大きい数の素因数分解に，膨大な時間がかかることを利用した方式．鍵長は512, 1024, 2048, 4096ビットなどがあり，現在NISTは，2048ビット以上のRSAを米国水晶としている．

* + - 必要な鍵の総数

必要な鍵の総数をKeyとする．

* + - 楕円曲線暗号

公開鍵暗号方式の暗号アルゴリズムであり，楕円曲線上の演算規則を利用した方式

* + ハイブリット暗号方式
  + ハッシュ関数
  + 電子メール暗号技術
* コマンド，実行結果の漏洩を防止法

データベース接続プログラム間の通信を暗号化する

* 認識技術
  + デジタル署名
  + タイムスタンプ
  + チャレンジレスポンス認証
  + 公開鍵基盤(PKI (=Public Key Infrastructure))
    - 認証局(CA (=Certificate Authority))
    - デジタル証明書（公開鍵証明書）
* セキュリティ実装技術
* セキュリティプロトコル

|  |  |
| --- | --- |
| 名称 | 説明 |
| SSH  (=Secure Shell) |  |
| SSL/TLS  (=Secure Sockets Layer/Transport Layer Security) |  |
| IPsec  (=IP Security Protocol) |  |
| HTTPS  (=Hyper Text Transfer Protocol over Secure Sockets Layer/Transport Layer Security) | Web通信にSSL/TLSによるデータ暗号化機能を付加したプロトコルのこと．「なりすまし」，「盗聴」による攻撃から通信を保護できるようになっている．サーバはクライアントに対してデジタル証明書(公開鍵証明書，サーバ証明書)を提示することになっている |

* 認証プロトコル

|  |  |
| --- | --- |
| 名称 | 説明 |
| OAuth  (=Open Authorization) |  |
| DNSSEC  (=DNS Security Extension) |  |
| EAP  (=Extensible Authentication Protocol) |  |
| EAP-TLS  (=Extensible Authentication Protocol -Transport Layer Security) |  |
| PEAP  (=Protected Extensible Authentication Protocol) |  |
| RADIUS  (=Remote Authentication Dial in User Service) |  |

* Webビーコン

Web標識という意味．Webページに埋め込んだみえないほど小さな画像の表示回数などにより，利用者のページ遷移などの情報を得る．

### 開発技術

#### 要件定義

* 要件定義手法

#### 設計

* システム設計
* モジュール
* モジュール強度
* モジュール結合度
* オブジェクト指向設計
  + 情報隠蔽

オブジェクトの属性を変更（参照）する場合は，オブジェクトのメゾットを利用する．ほかのオブジェクトによって直接属性を変更（参照）できないようにすること．

* + カプセル化

オブジェクト内で属性とメゾットを一体化し，情報隠蔽を実現すること．

* + クラス
  + 関連
  + 継承
  + デザインパターン
  + UML (=Unified Modeling Language)
    - ユースケース図
    - クラス図
    - シーケンス図

オブジェクト間のメッセージの流れを時系列に表す図

* + - アクティビティ図

システムなどのフローを記述する図

* + - コンポーネント図

インターフェースを介したコンポーネント同氏の関係や内容を表現する図

* + - 状態遷移図

時間経過．状態変化に応じて．状態が変わるようなシステムの振る舞いを記述するとき適した図式化手法

#### 実装・構築

#### テスト

#### 導入・受け入れ支援

#### 運用・保守

#### ソフトウェア開発管理技術

* 開発プロセス・手法
* アジャイル開発
  + XP (=Extreme Programming)（エクストリームプログラミング）

10人程度までの少人数チームで．小規模開発に適した手法．

設計より．コーディング．テストを重視し．フィードバックを得ながら修正．仕様変更を行うのが特徴．

|  |  |
| --- | --- |
| 名称 | 説明 |
| ペアプログラミング | 2人のプログラマーの協力で．１つのプログラムをコーディングする． |
| テスト駆動開発 | テストケースを先に設定し．プログラムをコーディングする． |
| リファクタリング | 外部仕様変更をせずに．プログラム内部構造を変更する． |
| プロトタイピング | 提供予定のソフトウェアの試作品を早期に作成する． |

* ソフトウェア構成管理(SCM (=Software Configuration Management))

ソフトウェア全体がどのような品目の組み合わせで構成されているかを管理する.

* ソフトウェア構成品目(SCI (=Software Configuration Item))

ソフトウェア構成管理で管理するソフトウェア資源や関連ドキュメント，ライセンスなどのこと．

## マネジメント系

### プロジェクトマネジメント（PM）

#### プロジェクトマネジメント（PM）

* PMBOK (=Project Management Body of Knowledge)
* プロジェクト体制
* プロジェクト統合マネジメント
* プロジェクトスコープマネジメント

プロジェクトの最終的な成果物（成果物スコープ）と．成果物を得るために必要な作業範囲（プロジェクトスコープ）を明確にし．プロジェクト全体を通じて管理していくこと．

* + WBS (=Work Breakdown Structure)

成果物を主体に改装的に要素分解したもの．「作業分解構成図」ともいうことがある．

* プロジェクトスケジュールマネジメント
* プロジェクトコストマネジメント
  + EVM (=Earned Value Management)

プロジェクトの作業を金銭の価値に置き換えて，コスト（*y*軸）とスケジュール（*x*軸）の2つを定量的に管理する進捗管理手法

* + コストの見積

|  |  |
| --- | --- |
| 名称 | 説明 |
| ファンクションポイント(FP =Function Point)法 | ソフトウェアの機能とその複雑さを基準に論理的に開発工程を見積もる方法．数値化したものは「ファンクションポイント」と呼ぶ． |
| 三点見積法 |  |
| 類推見積法 |  |
| ボトムアップ見積法 |  |
| LOC (=Lines of Code)法 |  |
| COCOMO (=Constructive Cost Model)法 | ソフトウェアの見積もりで，予想されるプログラム行数にエンジニアの能力や要求の信頼性などの補正係数をかけ合わせて開発工数や期間，要員や生産性を見積もる手法．それの見積手法を改良したものを「COCOMOⅡ法」という． |

* プロジェクト品質マネジメント
* プロジェクト資源マネジメント
* プロジェクトコミュニケーションマネジメント
* プロジェクトリスクマネジメント
  + リスク対応戦略

|  |  |
| --- | --- |
| 脅威への対応戦略 | 好機への対応戦略 |
| 回避：脅威の発生を避ける． | 活用：好機の発生を確実する． |
| 転嫁：他社に責任を移転する． | 共有：他社との好機を共有する． |
| 軽減：脅威の発生確率と影響度を下げる． | 強化：好機の発生確率と影響度を上げる． |
| 受容：驚異の発生時に対処する． | 受容：好機を受け入れる． |

* プロジェクト調達マネジメント
* プロジェクトステークホルダマネジメント

### サービスマネジメント（SM）

#### サービスマネジメント（SM）

* システムの移行計画：

環境を一部の共有→　移行確認がとりにくい

新旧システムの並行運用→　運用費が2倍になり，長引けばコストが掛かってしまう

移行データが多い→　トラブル時のリカバリ作業が大変

移行失敗時に旧システムに戻す→　適切

* 一斉移行方式

旧システムから新システムに一斉に切り替える方式

* + メリット：

両システムの並行稼働によるコスト増加の回避

データ交換するためのプログラムの用意が不要

* + デメリット：

運用後のトラブル発生率が高くなってしまうこと

* 順次移行方式

新旧システム比較しながら並行運用し，問題がなくなれば．新システムに移行する方式

* 新規システムのデータバックアップ方法

業務に支障が出てしまう場合，バックアップを業務時間外に実施する．

#### システム監査

## ストラテジ系

### システム戦略

#### システム戦略

ベンチーマーキング：自社製品・サービスなどを及びプロセスを定量的・定性的に測定し，ベスト企業と比較しそのギャップを把握する企業経営で用いられる分析手法

#### システム企画

### 経営戦略

#### 経営戦略マネジメント

* プロダクトポートフォリオマネジメント(PPM (=Product Portfolio Management)):

縦軸「市場成長率」，横軸「市場占有率」とし．4つに分類する経営手法のこと．

* SWOT分析

企業がおかれている経営環境を分析し．今後の戦略立案に活かす方法の1つ．

SWOTのS (=Strength)は強み．W (=Weakness)は弱み．O (=Opportunity)は機会．T (=Threat)は脅威の4つの各単語の頭文字をとったもの．

|  |  |  |
| --- | --- | --- |
| 内部環境要因 | 強み(=Strength)  活かすべき強み | 弱み (=Weakness)  克服すべき弱み |
| 外部環境要因 | 機会 (=Opportunity)  利用すべき機会 | 脅威 (=Threat)  対抗する脅威 |

* 企業の競争上のポジション

|  |  |
| --- | --- |
| 名称 | 説明 |
| リーダー | 全市場をカバーし．最大シェアを確保する全方位戦略． |
| チャレンジャー | シェア追撃などのリーダー攻撃に必要な差別化戦略． |
| フォロワー | 市場チャンスに素早く対応する模倣戦略． |
| ニッチャ | 製品．市場の専門特化を図る特定化戦略． |

#### 技術戦略マネジメント

#### ビジネスインダストリ

* EDI (=Electronic Data Interchange)

企業間の商取引に関わる見積書．発注書などの書式や通信を統一し．電子的に取り交わす仕組みのこと．

* + RFID (=Radio Frequency Identification)

ID情報を埋め込んだRFタブ（ICタブ）と電磁界や電波を用いて．情報のやり取りを行うこと．タグの表面が汚れても読み取りができる．

* 行政・公共情報システム
  + EMS (=Energy Management System)

照明．空調などの設備にセンサーを内蔵し．エネルギーの使用状況をリアルタイムに計測して可視化し．適切に自動制御するシステムのこと．HEMS (=Home Energy Management System)は家電製品などをインターネット接続して．自動制御を行い．省エネ．ピークカット効果を目指す．

### 企業と法務

#### 企業活動

* 機能別組織

購買・生産・販売・財務などの仕事の性質によって，部門編成した組織

* ラインアンドスタッフ組織

ライン(直接)部門，スタッフ(間接)部門が補佐する組織

* 事業部制組織

製品，地域，顧客などを市場ごとに分化させ，自己完結的な営業活動が展開できる組織

* カンパニー制組織

迅速で柔軟な経営を実現するために社内の各部門をそれぞれ独立した会社のように分化し事業を運営する組織

* マトリックス組織

従来の職能別組織にそれら各機能を横断する組織

マトリックス＝「母体・基盤，行列」

* プロジェクト組織

戦略的目標達成をもとに専門家を編成し，機関と目標を定めて活動する一時的かつ柔軟な組織

* 経営者の役割

|  |  |
| --- | --- |
| 名称 | 役割 |
| CEO  (= Chief Executive Officer) | 「最高経営責任者」  会社代表としての経営責任者 |
| COO  (= Chief Operating Officer) | 「最高執行責任者」  CEOのもとでの業務運営責任者 |
| CIO  (=Chief Information Officer) | 「最高情報責任者」  情報管理・情報システム戦略などの情報関係責任者 |
| CMO  (=Chief Marketing Officer) | 「最高マーケティング責任者」  マーケティング・ブラント戦略責任者 |
| CISO  (=Chief Information Security Officer) | 「最高情報セキュリティ責任者」  情報セキュリティ関係責任者 |
| CFO  (=Chief Financial Officer) | 「最高財務責任者」  資金調達・財政などの財務関係責任者 |
| CPO  (=Chief Privacy Officer) | 「最高プライバシー責任者」  個人情報管理責任者 |

* 作業測定

|  |  |
| --- | --- |
| 名称 | 説明 |
| 作業時間分析法  (=ストップウォッチ法) | 作業時間の分析で．ストップウォッチを用いて測定をする． |
| PTS法  (=Predetermined Time Standard) | 作業の基本動作の標準時間から作業時間を割り出す． |
| ワークサンプリング  (=瞬間観測法) | 決められた時間に稼働状況を記録することを繰り返し，集まった観測結果を分析する． |

* 会計・財務
  + 売上総利益
  + 営業利益
  + 損益分岐点

#### 法務

# B試験

# 参照文献

1. 株式会社富士通ラーニングメディア. (2023). よくわかるマスター　令和5‐6年度版　基本情報技術者試験　対策テキスト. FOM出版.
2. 基本情報技術者試験ドットコム <https://www.fe-siken.com>

1. 偶数バリティビットを付加する場合も同様． [↑](#footnote-ref-1)
2. logの底は基本的に2で考えることが多いため，以降省略して記載する．ただし，底はネイピア数ではない． [↑](#footnote-ref-2)
3. 「127.0.0.0」で始まるIPアドレスは「ループバックアドレス」という．コンピュータに割り当てられない特殊なIPアドレスで，自分自身を表すIPアドレスとして使われる． [↑](#footnote-ref-3)
4. FQDN (=Fully Qualified Domain Name)はホスト名（コンピュータ名）を合わせた形の完全なドメイン名のこと． [↑](#footnote-ref-4)