情報セキュリティマネジメント
本科生
見本テキスト

《内容》

- 試験対策テキスト　抜粋

TAC

情報セキュリティマネジメント

試験対策テキスト

Information
Security
Management
Examination

TAC

はじめに

ITの専門家だけが情報セキュリティを考える時代は終わってしまいました。私たちの何気ない行動やミスが，セキュリティ事故に発展して莫大な被害が発生するようなことも，十分に起こり得るのです。今や情報セキュリティは，ITを使用する私たち全員が意識しなければならない課題なのです。

そんな中，待ちに待った情報セキュリティマネジメント試験が，ついに始まりました。ITの専門家に限らず「仕事でITに触れる人」に向けた資格試験で，社会人の必須スキルとして，あるいはこれから社会人を目指す人の武器として，大いに活用できるはずです。

本書はその情報セキュリティマネジメント試験に合格するためのテキストです。覚えるべき知識は整理すると共に，表面的な理解に終わらないように説明すべき点はキッチリ説明することを心掛けています。重要なポイントは，演習問題や事例で振り返ることができるようにも配慮しました。本書を活用して，ぜひ合格を勝ち取っていただきたいと思います。

TAC情報処理講座

目　次

第2部
関連分野

情報セキュリティマネジメント試験の午前試験では，情報セキュリティ分野の知識に加え，関連分野の知識に関する問題も出題されます。

関連分野は，データベースやネットワークなどの応用技術や，プロジェクトマネジメント，企業活動などのマネジメント系・ストラテジ系の分野など，多岐にわたります。

第2部では，これらの関連分野の基礎知識を紹介します。午前試験対策として活用してください。また，情報セキュリティ分野の学習で登場した用語が分からないときなどのリファレンスとしても利用してください。

なお本書では，以降の内容は第1部の第5章から続く第6章として，“6.1”などのように記したうえで各知識を解説します。

6. 1 システム構成要素

【Guide】
情報システムにはどんな処理形態があるのか，性能や信頼性を高めるにはどんな技術を用いるのかについて学びましょう。

(1)　システムの処理形態・利用形態

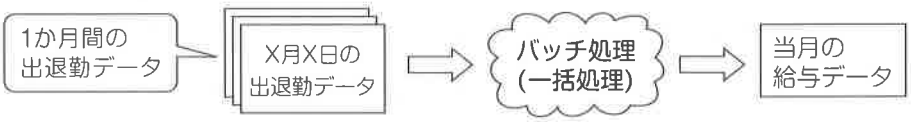
①　処理形態の分類

業務システムの処理形態は，処理のタイミングによって次のように大別できます。

バッチ処理（一括処理）	処理すべきデータを蓄積しておき，特定のタイミングで一括して処理する
リアルタイム処理	処理要求が発生するたびに，そのつど処理を行う

■バッチ処理

バッチ処理システムは，たとえば，給与計算や売上高の集計，バックアップの取得など「即時性は求められず，かつ大量のデータをまとめて扱うような処理」に適しています。



■リアルタイム処理

リアルタイム処理の代表的な処理形態としては，次の二つがあります。

・オンライントランザクション処理(OLTP：On-Line Transaction Processing)

トランザクション（関連するいくつかの処理をまとめた一連の処理単位）が通信回線を通じてサーバなどに届き，そのたびに処理するような形態です。単にオンラインリアルタイム処理ということもあります。

たとえば，銀行のATM端末における処理や座席予約など，できるだけ速い応答が求められるような処理に適しています。

・リアルタイム制御処理

微小な時間単位で状況を監視しながら，事象の発生（状況の変化）に応じて迅速に対応を行う形態です。たとえば，工場用ロボットの自動運転の制御や家電製品に組み込まれたマイコンなどに用いられています。

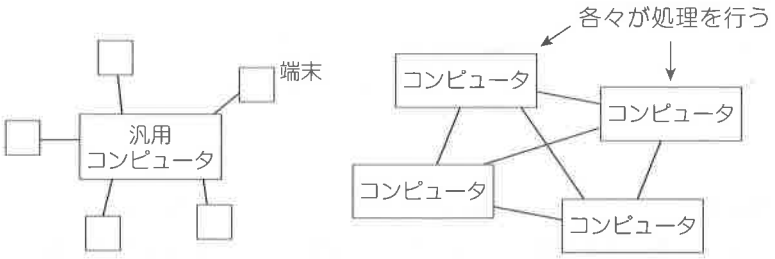
リアルタイム処理のうち，「データを入力 → 結果を表示 → 次のデータを入力 → …」のように，要求とそれに対する応答を繰り返しながら処理を進めるものを，対話型処理ということがあります。

Point
・バッチ処理：ジョブを蓄積して一括処理
・オンライントランザクション処理：ジョブが発生するたびに処理
・リアルタイム制御処理：微小な時間ごとの状況変化を監視して即座に対応

②　集中システムと分散システムの比較

集中システム（集中処理システム）は，センタに配置されたコンピュータがすべてを処理し，端末は処理の投入と結果の回収を行います。これに対し，**分散システム**（分散処理システム）は拠点ごとに設置されたコンピュータを通信回線で結び，各コンピュータが連携して処理を行います。

・集中システム　　・分散システム



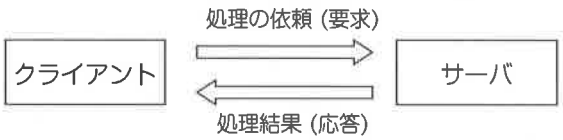
それぞれの特徴を整理してみましょう。

	集中システム	分散システム
障害発生時	センタに障害が起こると全体に影響する	影響範囲を局所化できるので，全体に影響が及びにくい。ただし障害発生箇所の特定は(集中システムと比べて)難しい
通信コスト	すべてセンタと通信(コスト高)	ある程度は各拠点ごとに処理できる(コスト低)
運用管理	(分散システムと比べて)容易	複雑
データ管理	センタのみ管理すればよい	拠点間で整合性を保つ必要がある
セキュリティの確保	(分散システムと比べて)容易	困難

分散処理システムは，分散の対象によって，役割を分担する「機能分散」と，仕事の量を分担する「負荷分散」に分けることができます。負荷分散において，処理要求を受け付け，各コンピュータに適切に振り分ける仕組みをもつ装置のことを，負荷分散装置（ロードバランサ）といいます。

③　クライアントサーバシステム

機能分散の分散処理システムの代表が**クライアントサーバシステム**です。**クライアントがサーバに処理を依頼し，サーバがそれに応える**という形で処理を進めます。



サーバは用途に応じて，

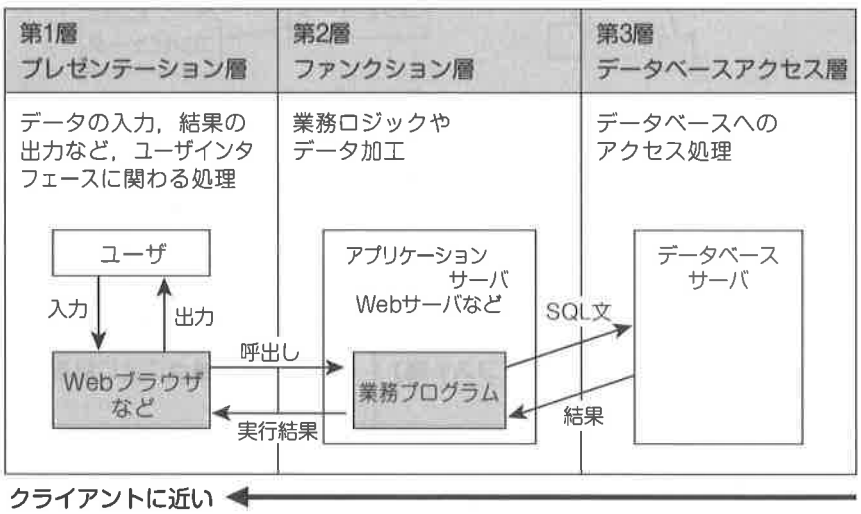
ファイルサーバ：ファイルの管理，アクセスを行う

データベースサーバ：データベースの管理，アクセスを行う

Webサーバ：ホームページなどのデータを要求に応じて返す

のような種類があります。たとえばインターネットのホームページ閲覧は，「パソコン上のブラウザがクライアントとなり，インターネット上のWebサーバにページ情報の要求を出して，Webサーバが応答を返す」という，クライアントサーバシステムの流れで実現しています。

クライアントサーバ構成のうち，データ処理機能を，図のような三つに分ける構成を**3層クライアントサーバシステム**とよびます。単に3層アーキテクチャということもあります。以下に，各層の役割とシステムの構成例を示します。3層クライアントサーバシステムに対し，従来のサーバとクライアントのみの役割分担で構成されるものは，2層クライアントサーバシステムといいます。



3層クライアントサーバシステムの代表例が，Webブラウザをクライアントとしてプレゼンテーション層に位置づけ，処理を行う**Webシステム**（**Webアプリケーション**）です。このようにすると，業務ロジックに変更が発生しても，サーバ側のプログラムのみ入れ替えればよく，クライアント側のプログラム入れ替えは不要になります。

また，3層クライアントの考えを推し進めていくと，クライアント側のマシンにはWebブラウザなどの最小限の機能しかもたせず，残りの機能やデータはすべてサーバ側にもたせるという設計方針も考えられます。このような「最低限の機能しかもたないクライアント端末」のことを，**シンクライアント**(Thin Client)といいます。企業で用いられるシンクライアントマシンには，磁気ディスク装置を搭載せず（ディスクレス端末などという），余分なプログラム実行やデータ保存がいっさいできなくなっているようなものもあります。

> **参考：ピアツーピア**
>
> サーバとクライアントの区別を明確に設定するのではなく，各コンピュータが対等の立場となって，それぞれの資源をお互いに利用しあう形態もあります。このような形態をピアツーピア(peer ot peer，P2P)といいます。

④　クラウドコンピューティング

クライアントサーバの仕組みやインターネットを活用すると，手元のコンピュータの内部にデータやアプリケーションプログラムを置いておくのではなく，

「データやプログラムはインターネット上に置いておき，
必要なときに必要なだけ利用する」

という処理形態が実現できるようになります。このような処理のあり方のことを，**クラウドコンピューティング**といいます。

クラウドコンピューティングの考えを活用したサービス事業（プロバイダ事業）には，以下のようなものがあります。

SaaS：ユーザに対してアプリケーションソフトウェアの機能を提供する
PaaS：アプリケーションはユーザが管理し，プロバイダはその実行環境を提供する
IaaS：アプリケーションや実行環境はユーザが管理し，プロバイダはハードウェアなどの基盤（インフラ）部分を提供する

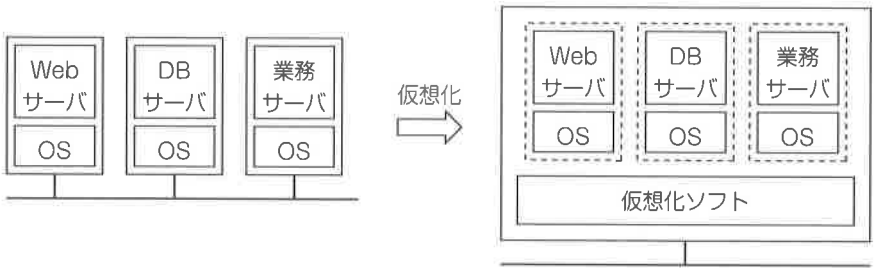
> **参考：DaaS**
>
> クラウドやシンクライアントの考えを推し進めると，アプリケーション機能だけでなく，デスクトップ環境そのものまでもがネットワーク経由で提供されるという形態も実現できます。このような「仮想のデスクトップ(Desktop)環境を提供する」サービス形態を，DaaS(Desktop as a Service)といいます。

⑤　仮想化技術

仮想化とは，

あるコンピュータ上で，複数の仮想マシン(OSとアプリケーション)を稼働させる技術であるといえます。仮想マシンは，外部からは本物と同じように見え，本物と同じように振る舞います。仮想マシンを作成し，稼働させるための基盤となるソフトウェアのことを，仮想化ソフトなどといいます。

仮想化技術を用いると，従来はサーバごとに別々に用意していたマシンが1台で済むなど，資源の有効活用が容易になります。また，コンピュータの性能が不足した場合は一部の仮想マシンを別のシステム上で稼働させて性能に余裕をもたせるなど，物理的な構成に依存しない柔軟な運用がやりやすくなります。



Point

・クライアントサーバシステム…クライアントが要求を出し，サーバが応答することで処理を実現

・3層クライアントサーバ：機能を以下の三つに分ける

　データベース層：データベースへのアクセス

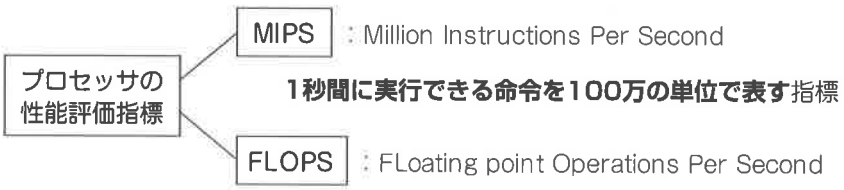
　ファンクション層：業務ロジック(データの加工)

　プレゼンテーション層：ユーザインタフェース

(2)　システムの性能

①　プロセッサの性能評価指標

プロセッサの性能を測る指標には，**MIPS**(ミップス，ミプス)と**FLOPS**(フロップス)があります。



たとえば，100MIPSのプロセッサは，1秒間に$100\times10^6=100{,}000{,}000$命令を処理できます。1命令当たりの処理時間は，1/100,000,000[秒] = 10[ナノ秒]です。

②　MIPS値の計算例

MIPS値を求める計算では，まず「1命令当たりの平均実行時間」を求め，その逆数をとるのが基本です。このとき，「ナノ秒」や「MIPSは100万単位」といった単位に注意しましょう。

例えば，「1命令当たりの平均実行時間が8ナノ秒」というコンピュータの場合，MIPS値は次のように求められます。

1秒当たりに実行できる命令数
$= 1 / (8\times10^{-9})$
$= 125\times10^6$ [命令]
= 125 [MIPS]

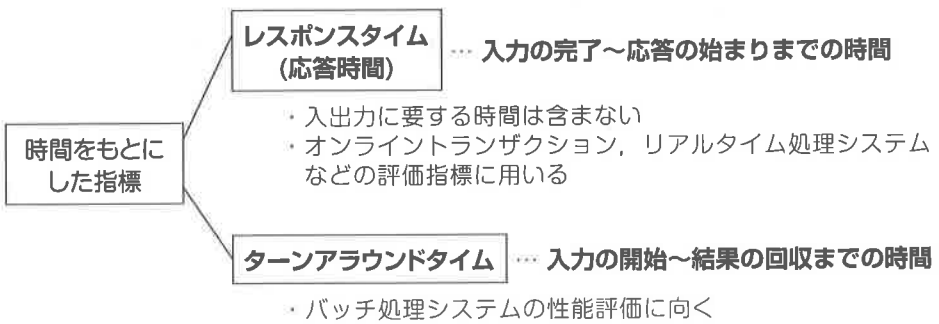
③　スループット

コンピュータやシステムの性能を評価するさいに用いる用語として，**スループット**があります。これは，**単位時間にコンピュータが処理できる「仕事量」**を指す言葉です。

たとえば，オンライントランザクション処理システムであれば“20件／分”のような「単位時間当たりの処理件数」がスループットの尺度になりますし，ネットワークであれば“1Mビット／秒”のような「単位時間当たりの伝送データ量」が尺度になります。

④　時間をもとにした指標

処理に要する時間をもとにした指標もあります。



⑤　ベンチマークテスト

ベンチマークは標準的なプログラムを実行することで，システムの性能を計測・比較する方法です。以下に代表的なベンチマークを挙げます。

SPECint　…　プロセッサの整数演算能力を測る
SPECfp　…　プロセッサの浮動小数点演算能力を測る

TPC-C　…　システム全体のトランザクション処理性能を測る

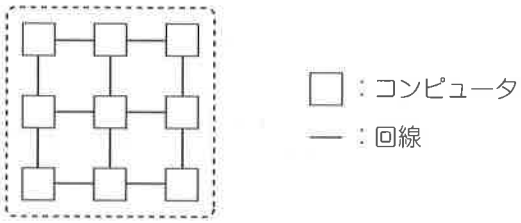
ベンチマークテストは，MIPS値やクロック数の単純な比較だけでは難しい，異機種間の性能比較に適しています。

Point
【プロセッサの性能評価】
・MIPS値：1秒当たりの命令実行数(100万単位)
・FLOPS値：1秒当たりの浮動小数点数演算の数
【システム性能指標】
・スループット：単位時間当たりの仕事量
・レスポンスタイム(応答時間)：入力完了から応答開始までの時間
・ターンアラウンドタイム：ジョブ提出から結果回収までの総時間
・ベンチマークテスト：標準的なプログラムを実行し，結果で相対比較

⑥　クラスタリング

クラスタリングは，ネットワークを介して複数のコンピュータを相互接続し，「1台の仮想的な高性能・高信頼コンピュータ」としてふるまわせる技術です。多数のコンピュータで負荷分散することで，非常に処理能力の高いシステムを実現します。また，一部のコンピュータに障害が発生しても，その部分は切り離して他の部分で処理を引き継ぐ(フェイルオーバ)ことで，高い信頼性も実現できます。。

「1台の高性能・高信頼コンピュータ」として振るまう



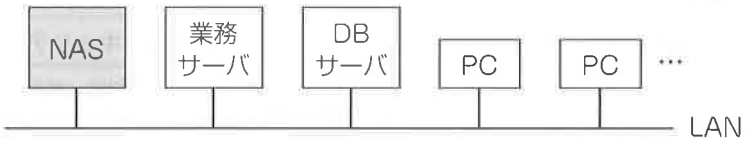
多数のマルチプロセッサ化やクラスタリングなどによって非常に性能の高いシステムを構築する，という考え方や技術を総称して，ハイパフォーマンスコンピューティング(HPC：High Performance Computing)といいます。

⑦　磁気ディスク関連のアクセス性能向上　(NAS，SAN)

コンピュータシステムでは，業務データなどを端末ごとの補助記憶装置にもたせるのではなく，ネットワーク上に大容量の専用補助記憶装置を接続して共有することがあります。このような補助記憶装置をネットワークストレージなどとよび，よく用いられるのが**NAS**，**SAN**といった仕組みです。

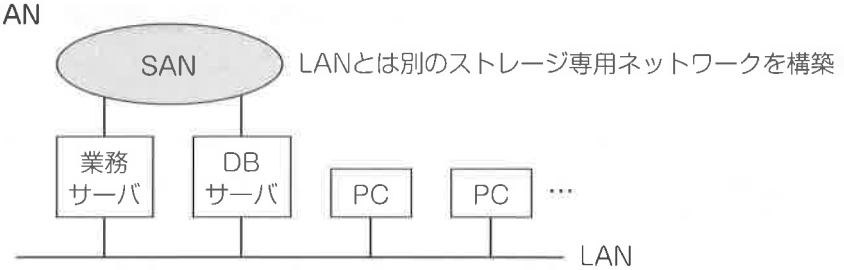
NAS (Network Attached Storage)	社内LANなどの通常のネットワークに(パソコンなどを経由することなく)直接接続することができる記憶装置。磁気ディスク装置，ネットワークインタフェース，OS，制御ソフトウェアなどから構成されている
SAN (Storage Area Network)	LANとは別のストレージ専用ネットワークに，磁気ディスク装置などの記憶装置を接続する方式。 通常のLANに大きな負担をかけることなくデータにアクセスできる

・NAS



LANに接続し，ファイルサーバとして機能

・SAN



NASは，ファイル単位でデータを共有でき，専用のファイルサーバとみなすこともできます。これに対してSANは，コンピュータからは直接接続されたハードディスクと同じように見えます。SANはSCSIと光ファイバを組み合わせた**ファイバチャネル**(**Fiber Channel**)とよばれる伝送技術などを用いて構築され，高性能ですがNASよりコストも高くなります。

Point
・NAS：LANに接続するファイルサーバ
・SAN：ファイル管理(ストレージ)専用の高速ネットワーク

(3)　システム信頼性

①　システムの信頼性とは

業務システムに求められる性質として，性能と並んで重視されるのが「システムの**信頼性**」です。信頼性とは，大まかにいうと

「システムが故障せず，かつ正しく(不都合なく)働きつづけられる」

という性質で，信頼性の高いシステムほど，故障しにくく安心して使いつづけられるシステムであるといえます。

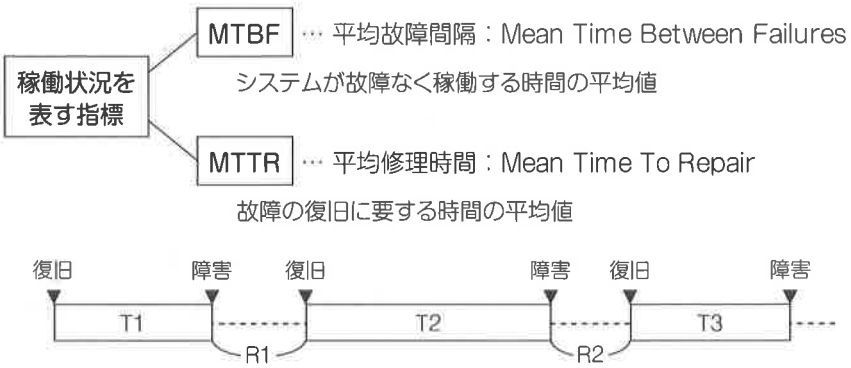
システムの信頼性を評価する概念として，(狭義の)信頼性(Reliability)，可用性(Availability)，保守性(Serviceability)の頭文字をとった“**RAS**(ラス)”と，RASに完全性(Integrity)，機密性(Security)を加えた“**RASIS**(レイシス，ラシス)”があります。

		指　標
信頼性(Reliability)	システムの故障のしにくさ	**MTBF** または 故障率
可用性(Availability)	システムを使用できる割合	**稼働率**
保守性(Serviceability)	保守の行いやすさ	**MTTR**
完全性(Integrity)	保全性ともいう。不整合の起こりにくさ	
機密性(Security)	犯罪や災害に対する強さ，いわゆるセキュリティ	

注：ここでいう故障率は，「故障回数／総稼働時間」で表される指標を指す。値は 1 ／ MTBF に等しくなる

②　MTBFとMTTR

システムの稼働状況を表す最も基本的な指標が，**MTBF**(**平均故障間隔**)と**MTTR**(**平均修理時間**)です。



T3終了までのデータから得られる

$$MTBF = \frac{T1+T2+T3}{3} \qquad MTTR = \frac{R1+R2}{2}$$

MTBFとMTTRは，名称が混乱しやすいので注意してください。MTBF(平均故障間隔)は，「故障(の復旧)から次の故障(の発生)までの間隔」の平均，つまり連続稼働している時間の平均値を表します。これに対して，MTTR(平均修理時間)は，「修理している時間」の平均を表します。

この二つの時間やそれらから計算される値は，信頼性の指標に用いられます。

③　稼働率

稼働率は，「全運転時間のうち，正常に稼働している(故障していない)時間の割合」を表す数値であり，可用性の指標として用いられます。稼働率が1に近いほど，可用性が高くなります。

稼働率は，MTBFとMTTRを用いて次の式で計算されます。

$$稼働率 = \frac{MTBF}{MTBF+MTTR}$$

この式は，主に装置(機器)単体の稼働率を求めるさいに使われます。この式からわかるように，稼働率を高くするには「**MTBFを長く，MTTRを短く**」すればよいのです。

たとえば，MTBFが480時間，MTTRが20時間の機器があるとき，稼働率は次のように求められます。

$$稼働率 = \frac{MTBF}{MTBF+MTTR} = \frac{480}{480+20} = \frac{480}{500} = 0.96 = 96\,[\%]$$

なお，システムが「稼働していない確率」は，

1－稼働率

で求めることができます。先の例であれば，1－0.96＝0.04(4%)が「稼働していない確率」です。

複数の装置からなるシステムの場合，システム全体の稼働率は，個々の装置の稼働率を用いて計算できます。このとき，「装置を直列に接続したシステム」と「2重化などの並列システム」で計算方法が異なります。

■直列システム … すべての装置が稼働していなければならない

システム全体の稼働率は，「**各装置単体の稼働率を掛け算した値**」です。

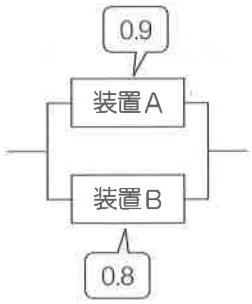
全体の稼働率 ＝ Aの稼働率×Bの稼働率
＝ 0.9×0.8
＝ 0.72

■並列システム … どれか1台でも稼働していればよい

どれか1台が稼働していればよいということは，「1台も稼働していない」ときだけ，全体として稼働していると見なせない，ということです。よって，システム全体の稼働率は，

1－(1台も稼働していない確率)

で計算されます。「1台も稼働していない確率」は，個々の装置ごとに「1－稼働率」を求めてそれを掛け算することで求められます。

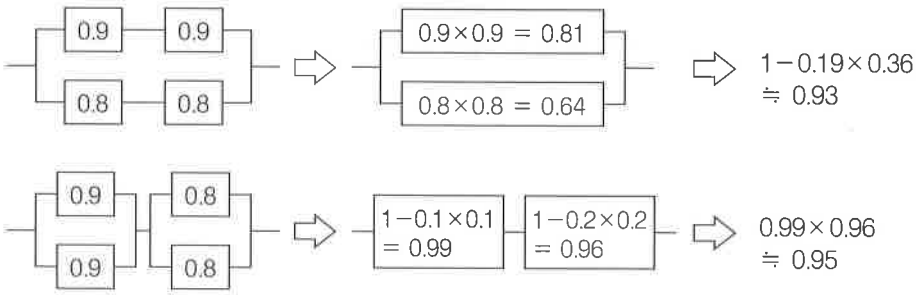


AもBも稼働していない確率

全体の稼働率 ＝ 1－(1－Aの稼働率)×(1－Bの稼働率)
＝ 1－(1－0.9)×(1－0.8)
＝ 1－0.02
＝ 0.98

■直列と並列の組合せ

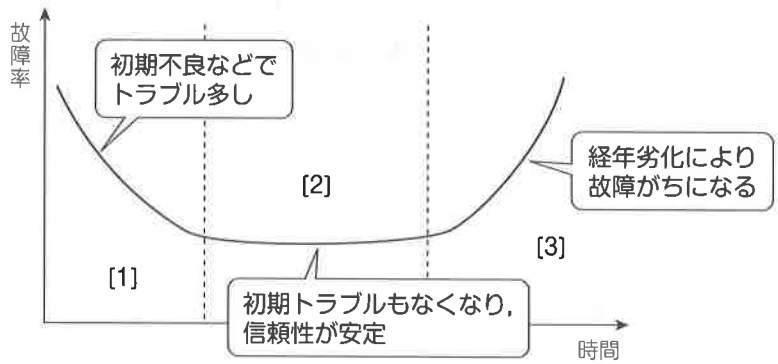
直列システムと並列システムが組み合わされている場合には，各部分の稼働率を求めながらシステムを単純化します。



④　ハードウェアの保守

ハードウェア（機器）には故障がつきものであり，故障を100%なくすことはできません。

ハードウェアが故障する確率（故障率）の大きさは，時間の経過にともなって，一般に次のような推移傾向を見せます。この曲線を**バスタブ曲線**といいます。



図中の[1]～[3]では，それぞれ主に次のような故障が発生します。

[1]　**初期故障**：部品の不良などが原因で，稼働後の早い時期に発生する故障

[2]　**偶発故障**：偶発的な原因によって，稀に発生する故障

[3]　**摩耗故障**：機械的に駆動する部品の摩耗などによって発生する故障。使用時間が長くなるほど，発生率が高くなる

予防保守を行うことで，ハードウェアのMTBF（平均故障間隔）を長くすることが期待できます。

Point
- **MTBF(平均故障間隔)：故障が直った直後から次の故障発生までの時間の平均**
- **MTTR(平均修理時間)：故障を直すのにかかる時間の平均**
- **稼働率＝MTBF／(MTBF＋MTTR)**

⑤　高信頼性システムの考え方

高信頼性システムを構築する指針として

「障害が発生しても，システムの運転(稼働)を継続できるようにしておく」

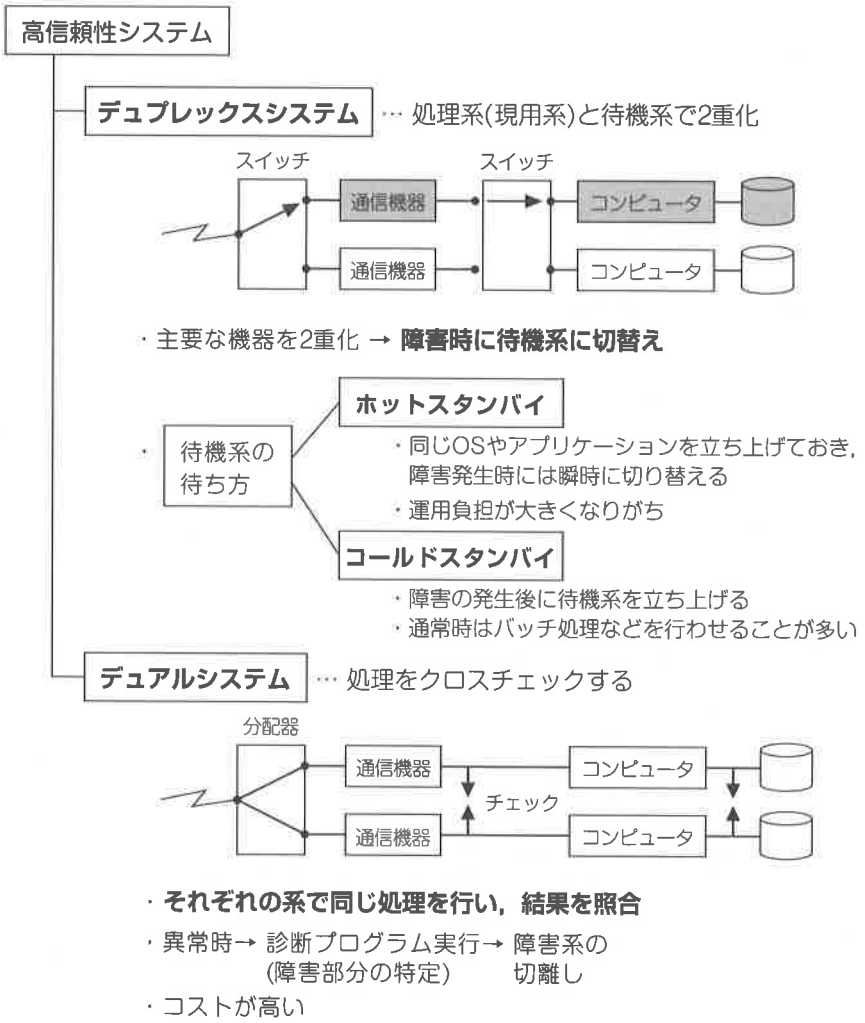
というものがあります。このような「信頼性が高い＝障害に強い」という性質を，**フォールトトレランス**とよびます。

信頼性を高めるための考え方には，フォールトトレランスを含めて，次のようなものがあります。

フォールトトレランス	障害が発生した場合でも，システムを稼働させ続けようとする考え方
フェールソフト	障害が発生した場合は故障部分を切り離すなど，機能を低下させてでも最低限の処理は継続させようとする考え方。故障部分を切り離して継続的に稼働させることを，縮退運転(フォールバック運転)とよぶ
フェールセーフ	障害による影響の拡大を防ぎ，システムをできるだけ安全な状態に導こうとする考え方。状況によっては処理の停止もやむを得ないとする
フールプルーフ	誤入力などの人為的ミスが起こりにくいように設計するという考え方
フォールトアボイダンス	システムの各構成要素の信頼性を上げるなどして，障害の発生そのものを防ぐ
フォールトマスキング	ある部分に障害が発生したとき，補正などを行って外部からは障害が分からないように隠ぺいしながら(稼働を継続しながら)，同時に自律的な障害修復も行う

フォールトトレランスの概念に基づいて信頼性を高めるシステム構成の代表として，システムの一部や全部を2系統用意する(2重化する)構成があります。このような構成を，**冗長構成**とよぶこともあります。

冗長構成には，次のようなものがあります。



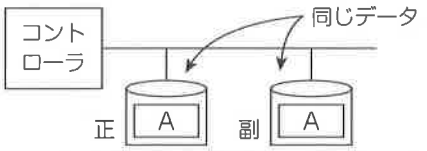
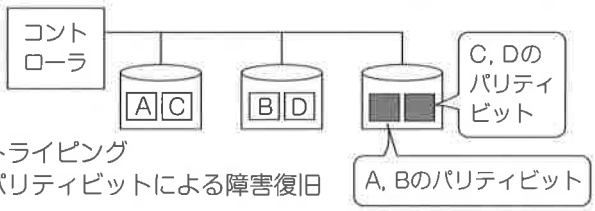
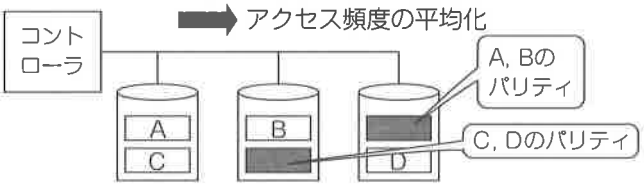
⑥ RAID

RAID(レイド)(Redundant Array of Inexpensive Disks)とは，複数台のハードディスク装置を併用する仕組みです。**ディスクアレイ**ともよばれます。RAIDの目的は，大きく二つあります。

[1]データを複数のハードディスク装置に分散して書き込み(**ストライピング**)，それらを並列にアクセスすることによって，**全体としてのアクセス速度の高速化**を図る。

[2]同じデータを複数ディスクに同時に書き込む(**ミラーリング**)，あるいは障害回復用の情報(パリティビット)を加えて書き込むことにより，**信頼性の向上**を図る。

RAIDはいくつかの種類に分類できますが，主なものは次のとおりです。

RAID 0	**ストライピングのみ。**障害復旧の機能はもたない
RAID 1	正副のディスクに 同じデータを記録 **(ミラーリング)** 
RAID 0+1	ストライピング＋ミラーリング
RAID 2	ストライピング＋ハミングコードによる誤り訂正
RAID 3	 ストライピング ＋パリティビットによる障害復旧
RAID 4	RAID 3の発展。ストライピング＋パリティを ブロック単位で管理 ➡ 並列アクセスの効果大
RAID 5	RAID 4の発展。**パリティブロックも分散記録する** 

参考：RAID6

RAID5を発展させ，さらに信頼性を高めたものにRAID6があります。RAID6では一組のデータについてパリティを2種類算出し，同時に2台が故障しても稼働を可能とします。

⑦　バックアップサイト

地震などの災害対策としては，本番システムと別の場所にバックアップ用のシステム環境を用意し，業務データなどを随時ネットワークで転送する，バックアップサイトという手法がよくとられます。バックアップサイトの種類は，準備体勢によっておおむね次のように分類できます。

ホットサイト：本番と同様の環境をあらかじめ用意しておき，障害時には即座に切り替える

コールドサイト：場所や基本設備だけ確保しておき，障害時にハードウェアやソフトウェアを搬入する

ウォームサイト：ホットサイトとコールドサイトの中間。施設を確保してハードウェアやソフトウェアを搬入しておき，障害時には業務プログラムやデータを搬入する

Point

【高信頼設計の考え方】

・フォールトトレランス：障害が起きても問題なく稼働できる性質

・フェールソフト：機能を落としてでも稼働を継続

・フェールセーフ：システムを常に安全な方向へ制御

・フールプルーフ：人為的ミスを予防・検知

【高信頼システム構成】

・デュプレックスシステム：現用(本番)系と待機系で冗長化

・デュアルシステム：2系列で同じ処理を行い照合

(4)　システムの経済性

システムの導入や保守を行うときには，性能や信頼性だけでなく，経済性からの評価も必要です。具体的には，購入費用などのイニシャルコスト(初期コスト)，消耗品費や電気代などのランニングコスト(運用コスト)の両面から，必要となる費用を見積り，費用対効果を考えながら導入・運用計画を立てることになります。

経済性評価によく用いられる指標としては，システムの導入から運用まで，保有に関して発生する費用の総額を表すTCO(Total Cost of Ownership)があります。

TAC