高信頼システム 01

～信頼性の基礎～

張山昌論

2019年

連絡先

- 張山昌論 (はりやままさのり)
- メールアドレス: hariyama@tohoku.ac.jp
- 居室: 3号館 308号室 (地下鉄青葉山駅の後ろ)
  (事前にアポイントいただけますよう)
- 電話: 022-795-7153

授業の資料

- 張山のWEBの授業のページでPDFを公開
  - http://www.ecei.tohoku.ac.jp/hariyama
  - PC / タブレットで持ち込んでも結構です

評価方法

- 基本的にはテストで成績を判定する
  - 授業中に渡した印刷資料と自筆ノートを持ち込んで良い.
  - 電卓持ち込みOK．通信機能のあるデバイス使用はダメ
- レポートなどの平常点を考慮する場合もある
- 出席はとらない

本講義で主に対象とするシステム：情報システム

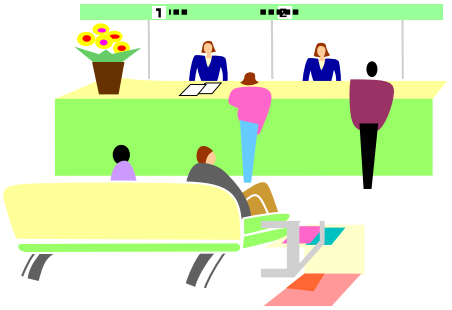
IoT: Internet of things, 全てのモノが情報システム

自動車

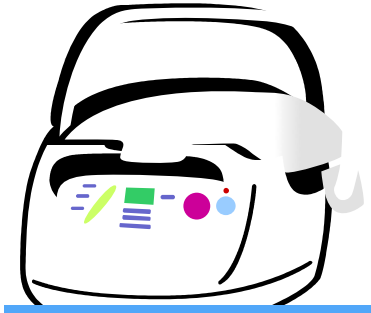
100個以上のLSI！

携帯

銀行システム



家電



インターネット・クラウド

スーパーコンピュータ，
サーバー

システムの信頼性が損なわれるとパニックに

信頼性とは？

システムが与えられた条件で規定の期間中，
要求された機能を果たすことができる性質

システムは時間が経てば故障する

どの程度時間が経つとシステムが壊れるのか？
単位時間内にシステムが壊れる確率は？

システムを安定的に運用できる

情報システムの高信頼化の課題

● 故障・誤動作の観点

- コンピュータの部品（HDD,メモリ）の故障
- ネットワークルータの故障
- 厳しい環境での組み込みシステム
  - 自動車の制御用LSI→電磁波・高熱による誤動作
  - 人工衛星用コンピュータ→強烈な宇宙線による誤動作

情報システムの高信頼化の課題（続き）

- プログラムにおけるバグ
- 集積回路（LSI）の設計におけるバグ
- プリント基板の製造時の欠陥：半田の不良

情報システムの高信頼化の課題

●情報セキュリテイへの対策

- データの改ざん，システムのハッキング

近年，自動車などの組み込みシステムでも重大な問題に！

「プリウス」がハッキングされる現実

清水 直茂＝日経Automotive Technology　2014/01/14 10:46　1/1ページ

この記事どう？

1
ためになった

仕事に役立つ

知っておくべき

検索する

コメント投稿

印刷

その他 ▼

自動車の情報セキュリティに関して昨年の最大のトピックと言えるのが、著名なハッカーらがトヨタ自動車「プリウス」と米Ford Motor社「Escape」をハッキングしたことです。この事実は自動車業界の関係者を震撼させました。

ハッカーは、現在米Twitter社に籍を置くCharlie Miller氏と、米IOActive社のChris Valasek氏。両氏は米国における情報セキュリティ関連のイベント「DEFCON（デフコン）」で成果を発表しました。発表ではステアリングやドアなどを自在に操ることを証明し、ハッキングに必要な情報を詳細に書いた論文も公開しています。

もちろん、両氏が実行したことを現時点で誰もができるわけではありません。高度な技術と時間、ある程度の資金がいるからです。その上、今回の成果は広域無線通信網を使った遠隔攻撃ではなく、実際に車両に乗り込んで実施するもの。難度は高いと言えます。

それでも両氏の論文は、自動車の情報セキュリティは無防備に近いと言えることを明らかにしました。特に、自動車で標準的に使われる車載ネットワーク「CAN」における情報セキュリティは「ないに等しい」のです。

今後、情報セキュリティ面での対策がない自動車を造ることは、自動車メーカーにとって致命傷につながる可能性があります。自動車がハッキングされると即座に事故につながりうるからです。そうした危機感から、日本でも最近、自動車の情報セキュリティについての議論が進み始めました。ただし議論と対策では欧州と米国がはるかに先行するのが実状と言えます。

シラバス

１　情報システムの高安全化・高信頼化の背景
２　信頼性評価の基礎(信頼度、ＭＴＴＦ、アベイラビリティなど)
３　フォールト・トレラント設計: 静的冗長技術
４　フォールト・トレラント設計: 動的情報技術
５　フォールト・トレラント設計: 誤り訂正符号1
６　フォールト・トレラント設計: 誤り訂正符号2
７　システムの集中と分散
８　分散システムの構成
９　ソフトウェアシステム設計手法：オブジェクト指向モデリング1
１０ ソフトウェアシステム設計手法：オブジェクト指向モデリング2
１１ TDD（テスト駆動開発）によるソフトウェアの高信頼化設計
１２　情報工学的アプローチによる異常検知技術1
１３　情報工学的アプローチによる異常検知技術2
１４　高信頼システム設計の実例
１５　まとめ

信頼度評価の基礎

(信頼度、ＭＴＴＦ、アベイラビリティなど)

システムの信頼性の尺度

1.信頼性 (Reliability)
2.可用性 (Availability)
3.保守性 (Serviceability)

→ RAS技術

＋ 完全性 (Integrity), 安全性 (Security)
→ RASIS (レイシス)

1. 信頼性（Reliability）

部品/機器/システムが正しく機能していることを定量的に表現するための尺度

信頼度, 故障率

信頼度, 故障率

S(t): 総数N個のサンプルを動作させている時に，時刻 t まで正常に動作しているサンプル数

F(t): 時刻 t までに故障してしまったサンプル数

$$S(t) + F(t) = N$$

信頼度 R(t): $R(t) = \frac{S(t)}{N}$

故障率 λ(t): $\lambda(t) = \frac{1}{S(t)} \frac{dF(t)}{dt}$

残存している構成要素に対する単位時間の故障の数

故障率の意味

「動作中の装置が単位時間に故障する確率」

時間の単位として「hour」を用いた場合,

$\lambda = 10^{-5}$ [/hour]

→ 1時間以内に10^{-5}の確率で故障

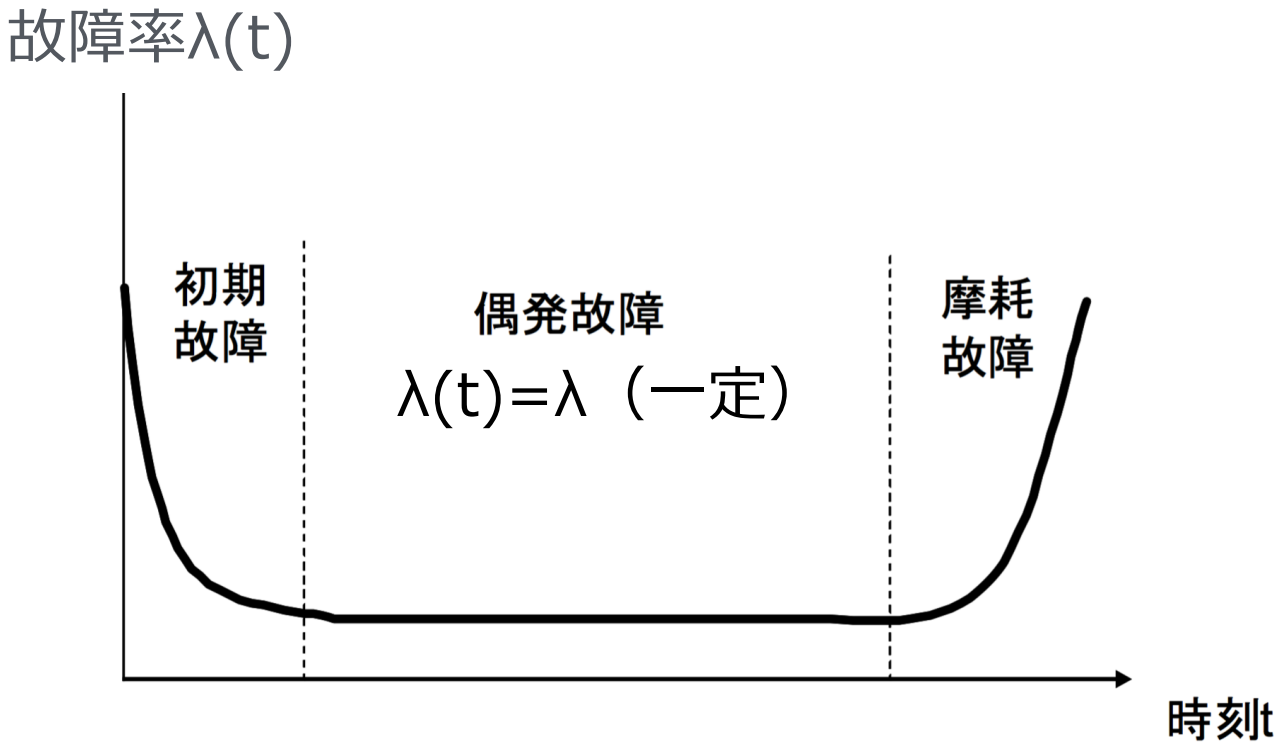
→ 10^{6}個の装置を使っていた場合,

1時間以内に1個が故障する

故障率の単位として，fit (failure in time) が用いられる

1[fit] = 10^{-9} [/hour]

故障率の変化のモデル：バスタブ(Bath-tub)



1. 初期故障期：初期不良が主たる故障の原因．故障率は時間と共に減少．
2. 偶発故障期：故障率は一定．λ(t) = λ → $R(t)=e^{-\lambda t}$ 次ページで補足
3. 摩耗故障期：故障率は時間と共に増加，寿命を迎える．

（補足）故障率が一定の場合の信頼度関数

$$R(t)=\frac{S(t)}{N}=\frac{\{N-F(t)\}}{N}=1-\frac{F(T)}{N}$$

$$\frac{dR(t)}{dt}=-\frac{\frac{dF(t)}{dt}}{N}\Rightarrow\frac{dF(t)}{dt}=-N\frac{dR(t)}{dt}$$

$$\lambda=\frac{1}{S(t)}\frac{dF(t)}{dt}$$

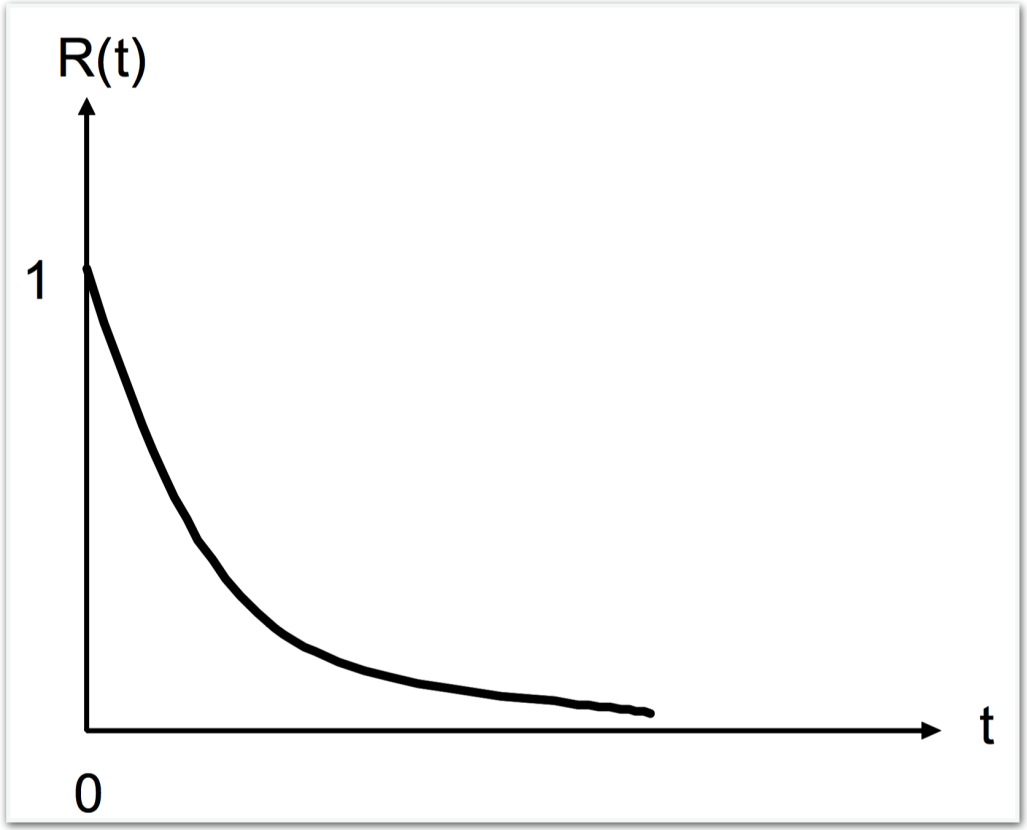
$$=-\frac{1}{R(t)}\frac{dR(t)}{dt}$$

λが一定であれば,

$$\lambda\int_0^t dt=-\int_1^{R(t)}\frac{1}{R(t)}dR(t)$$

$$\lambda t=-\left[\log_e R(t)\right]_1^{R(t)}$$

$$R(t)=\exp(-\lambda t)$$



故障率が一定の場合の信頼度関数

$\lambda t \fallingdotseq 0$ であれば $R(t) \fallingdotseq 1 - \lambda t$

MTBF，MTTF

MTTF: Mean Time To Failure（平均故障時間）

故障なしで使用できる時間の平均値.
非修理系（修理せず交換するシステム）に適用

例）部品類など → 故障の場合，修理せずに交換・廃棄

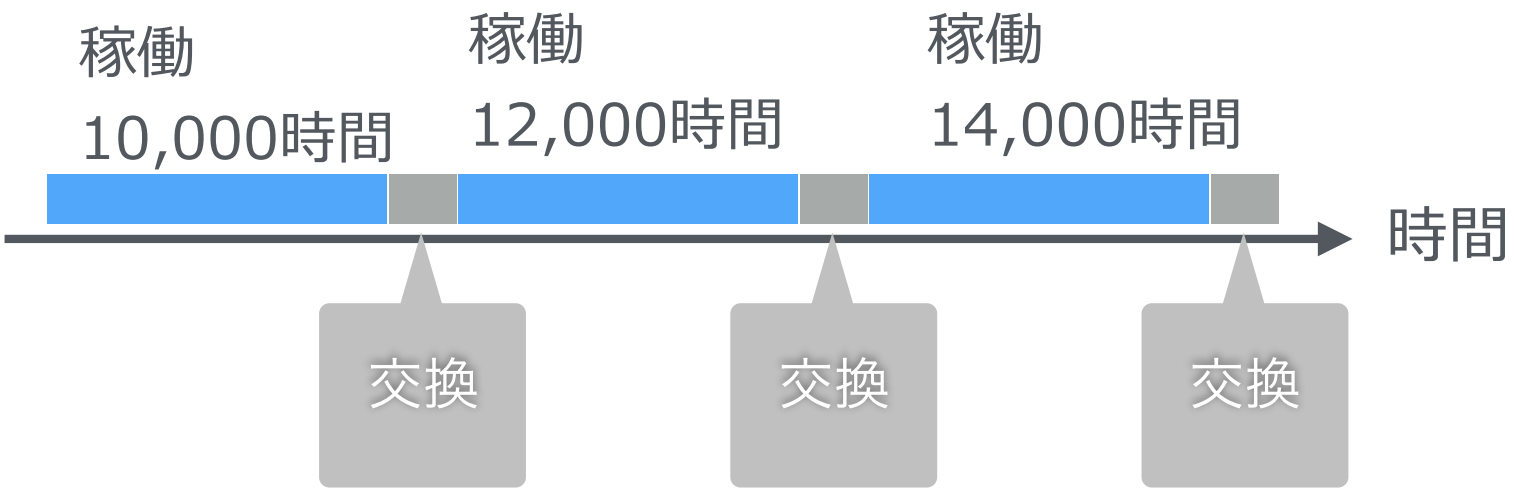
MTBF: Mean Time Between Failures（平均故障間隔）

システムが故障するまでの時間の平均値。
修理系（直しながら使うシステム）に適用

例）車，コンピュータ → 故障した部品を交換して再度利用可能.
修理・使用から再度故障するまでの時間

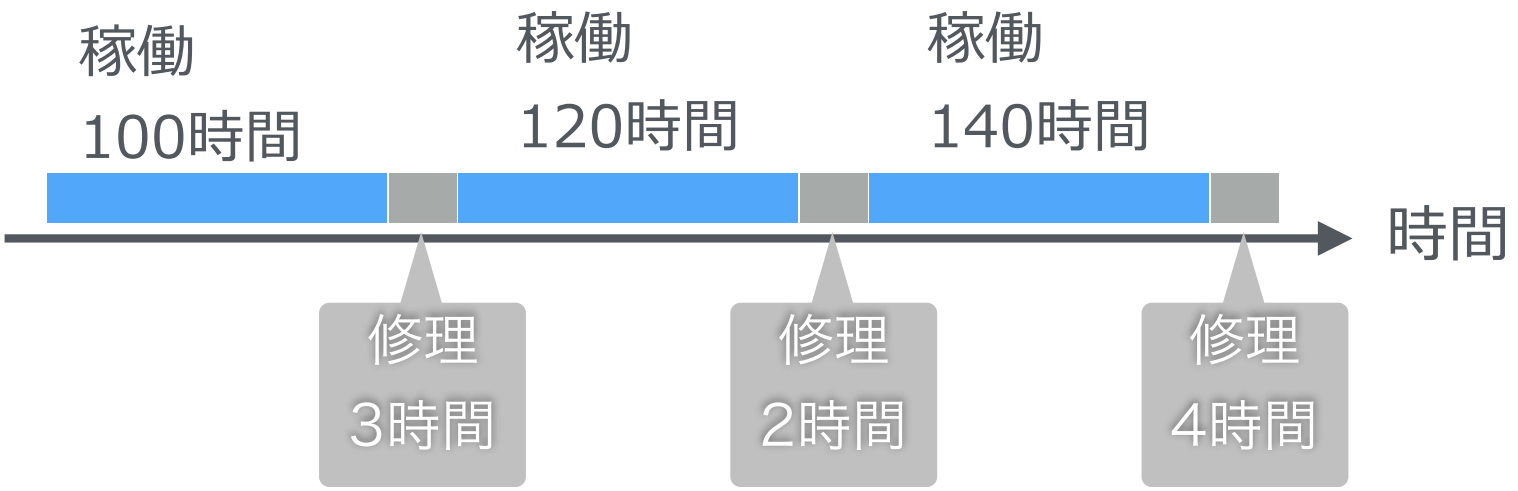
計算例 MTTF

コンピュータのハードディスクは下記のように稼働して故障し交換した.
ハードディスクのMTTFを求めよ.



計算例 MTBF

下記のシステムのMTBFを求めよ



MTTF，MTBFと故障率の関係

$$MTTF = \frac{1}{\lambda} \quad MTBF = \frac{1}{\lambda}$$

※故障率λが一定の場合

参考までに求め方：

$$\mathrm{MTTF} = \int_0^\infty \mathbf{R(t)dt} = \int_0^\infty \mathbf{exp(-\lambda t)dt} = \left[\exp(-\lambda t)/(-\lambda)\right]_0^\infty = 1/\lambda$$

演習

平均して20日で故障するシステムを考える.

(1) このシステムのMTBFを求めよ

(2) このシステムの故障率を求めよ

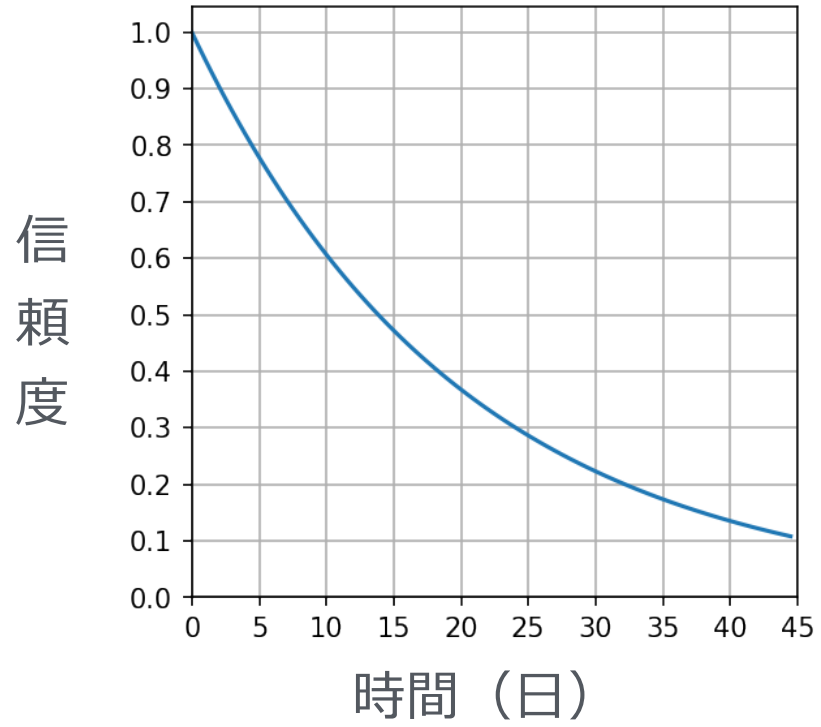
(3) このシステムの信頼度R(t)を求めよ

演習(続き)

(4) （修理が完了してから）20日でシステムが故障せずに動作している確率を求めよ．下記のグラフを使って良い．

(5) 信頼度が0.5となるのは何日目か．

λ＝1/20の時の信頼度のグラフ



2. 可用性 (Availability)

システムが利用可能であるかどうかを定量的表現

定量的指標：

稼働率（システムが利用可能である確率）

$$(\text{稼働率}) = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

※ 稼働率は定常アベイラビリティとも呼ばれる

MTBFが同じでも，MTTRが小さい方が稼働率が高い.

→ 故障を早く検出でき，修理しやすいシステムが大切

3.保守性 (Serviceability)

システムが故障→ 故障検出・部品交換・修理

故障検出から修理のしやすさまでを考慮した指標

定量的な指標：

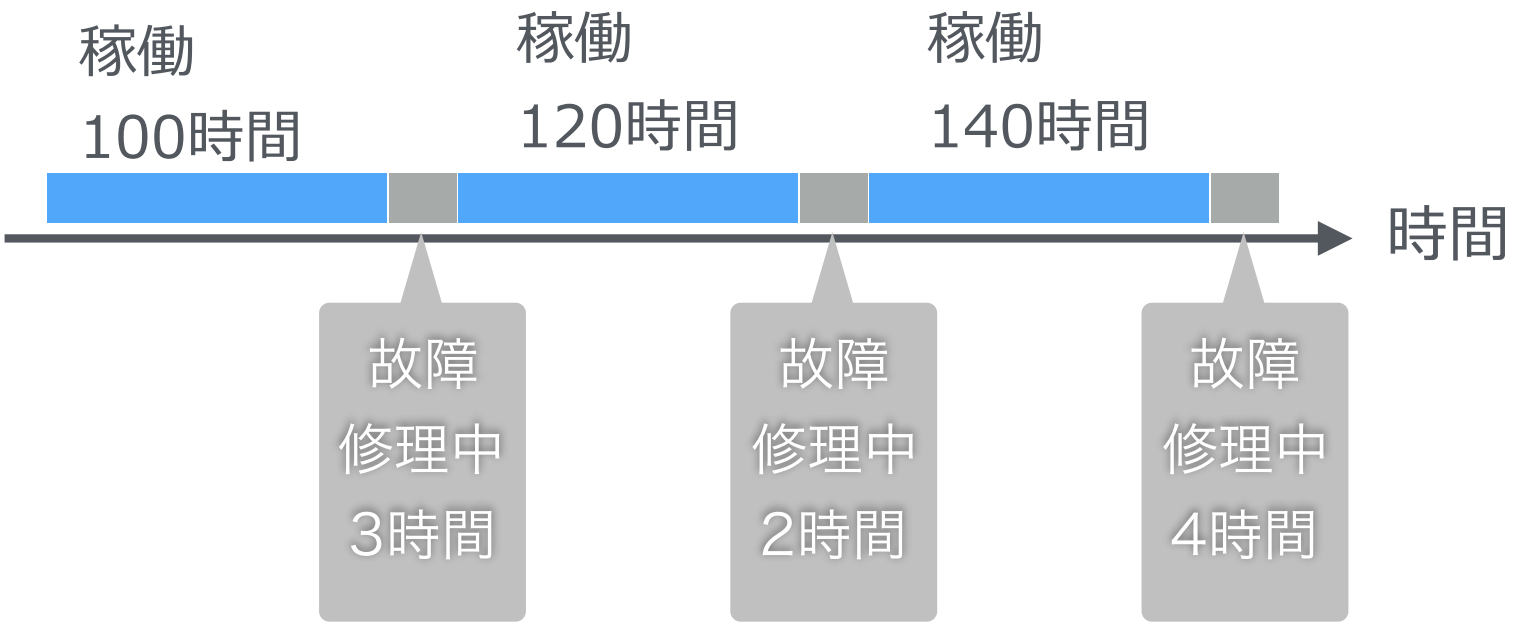
平均修理時間

（MTTR, Mean Time To Repair）

MTTRが小さい → 保守性が良い

計算例 MTTR

下記のシステムのMTTRを求めよ



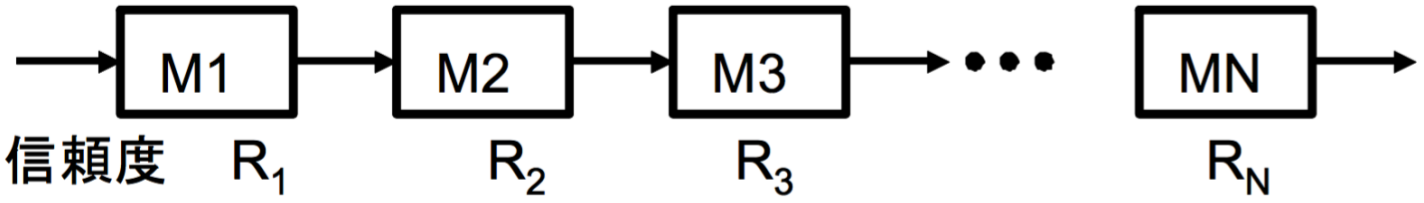
直列及び並列システム

世の中のシステムは，多くの部品・
サブシステムからなっている

直列システム（Series）の信頼度・稼働率

すべての構成要素が正常に動作 → システム全体が正常動作

直列系の信頼度グラフ　※故障は独立



信頼度グラフ: 左から右端まで繋がっている → システムは正常
故障により切断 → システムダウン

信頼度

$$R_{OV} = R_1 \cdot R_2 \cdot R_3 \cdots R_N$$

$$= \exp(-\lambda_1 t) \cdot \exp(-\lambda_2 t) \cdot \exp(-\lambda_3 t) \cdots \exp(-\lambda_N t)$$

$$= \exp(-(\lambda_1 + \lambda_2 + \cdots + \lambda_N)t)$$

なお, $R_{OV} = \exp(-\lambda_{OV} t)$ より $\lambda_{OV} = \lambda_1 + \lambda_2 + \cdots + \lambda_N$

稼働率

$$U_{OV} = U_1 \cdot U_2 \cdot U_3 \cdots U_N$$

並列システム（Parallel）の信頼度・稼働率

どれか1個の構成要素が正常に動作 → システム全体が正常動作

例）冗長システムで切り替えが完璧にうまくいく場合

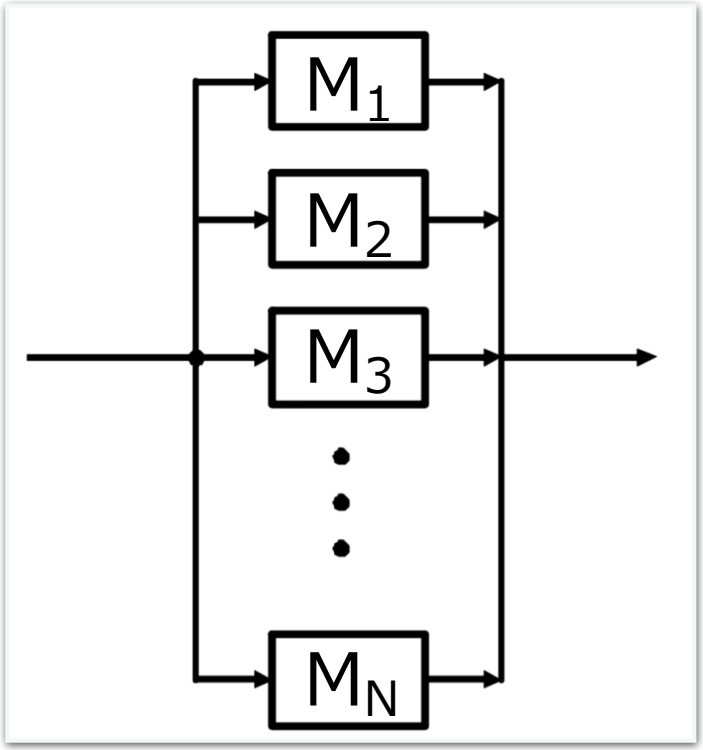
信頼度

$$R_{OV} = 1-(1-R_1)\cdot(1-R_2)\cdot(1-R_3)\cdots(1-R_N)$$

$$= 1-\{1-\exp(-\lambda_1 t)\}\cdot\{1-\exp(-\lambda_2 t)\}$$

$$\cdot\{1-\exp(-\lambda_3 t)\}\cdots\{1-\exp(-\lambda_N t)\}$$

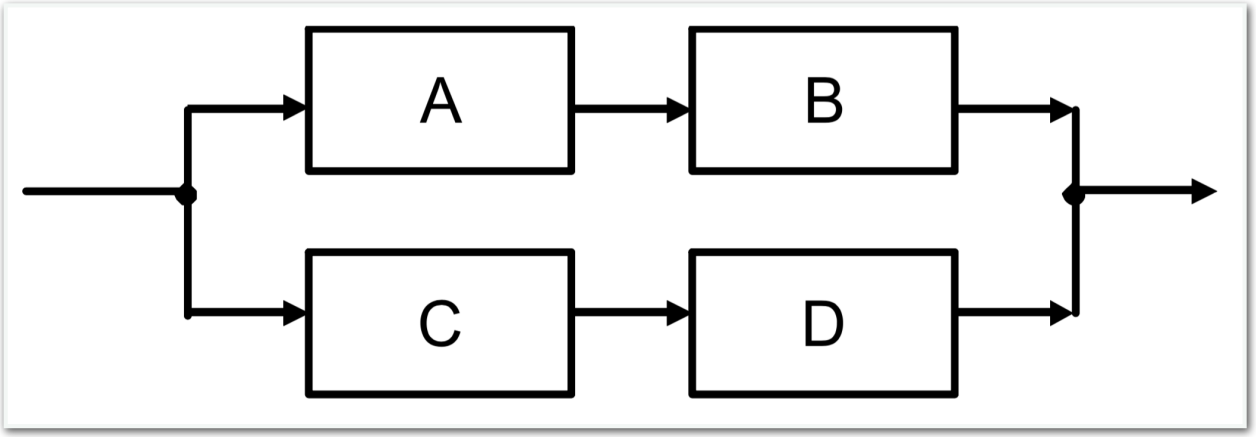
すべての構成要素が故障する場合以外の確率



稼働率

$$U_{OV} = 1-(1-U_1)\cdot(1-U_2)\cdot(1-U_3)\cdots(1-U_N)$$

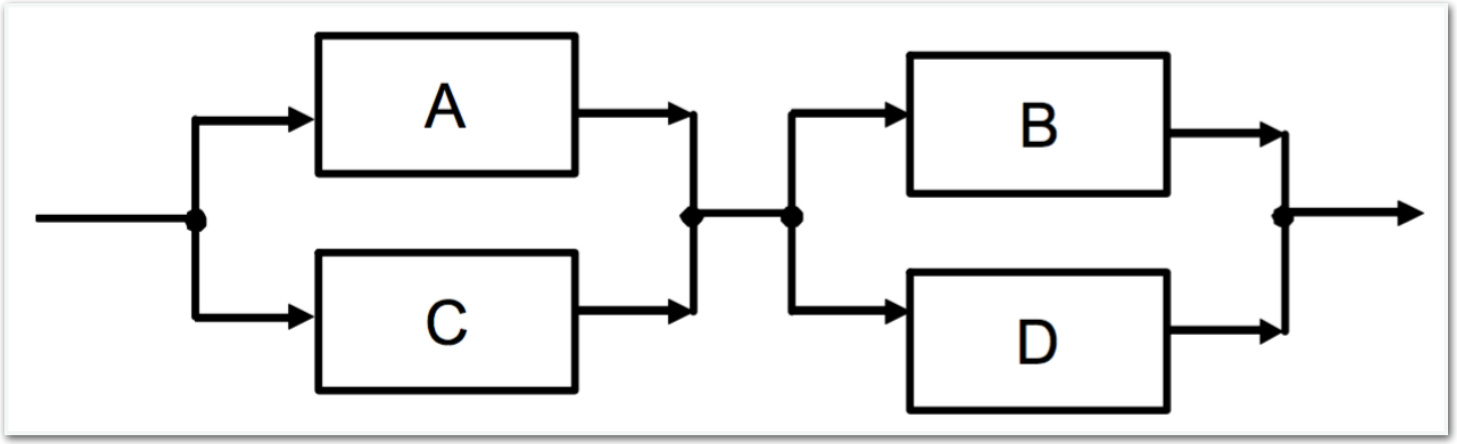
直並列(Series-to-Parallel) の信頼度



直並列の信頼度：

$$Rsp = 1 - (1 - R_A R_B)(1 - R_C R_D) = R_A R_B + R_C R_D - R_A R_B R_C R_D$$

並直列(Parallel-to-Series)の信頼度



並直列の信頼度：

$$Rps = \{1 - (1 - R_A)(1 - R_C)\} \{1 - (1 - R_B)(1 - R_D)\}$$

演習問題1

表よ示す構成のコンピュータシステムがある.
機能を満たすためには全ての構成部品が正常に
動作する必要があるとする.

（1）このシステムのMTBFを求めよ
（2）1000時間使用した時の信頼度を求めよ

部品	個数	故障率 [/hour]
メモリ	4	(λ_1) 10×10^{-7}
CPU	1	(λ_2) 20×10^{-7}
HDD	2	(λ_3) 200×10^{-7}
キーボード	1	(λ_4) 30×10^{-7}
ディスプレイ	1	(λ_5) 50×10^{-7}

演習問題2

N=2の並列システムにおいて，全てが同じ構成要素であり，1個の信頼度がR=0.75であるとする．この時の全体のシステムの信頼度を求めよ.