機械システムの安全と管理

担当：環境エネルギー工学専攻　谷本 潤 教授

システム安全の良否を判定する要因としては，性能，コスト，時間的因子，人間との関係，社会への影響など様々な要素が考えられるが，その中でも信頼性は最も重要なファクターである．重要なシステムほど高度の信頼性が要求され，二重三重の安全対策を講じておかねばならない．ここでは，**信頼性工学**の初歩を演習を交えて解説する．信頼性工学は確率論の応用であり，あらゆる工学分野で要求される基礎的素養である．

参考書：塩見弘「信頼性工学」丸善

参考一般書：畑村洋太郎「失敗学のすすめ」講談社，
柳田邦夫「マッハの恐怖」新潮文庫（正・続）

※本講義のスライドを研究室のwebページからDLしておくこと．

システムの信頼性を巡る基本的な3課題

＃1．要求されるレベルの問題

●超過危険率と云う発想／家電システムの故障<<空調システム（TAC*% etc）<<構造物の耐震性（*年に一回生起する地震に耐えるetc），自動車の安全性（M自動車のプロペラクシャフト耐応力過小設計），飛行機の信頼性

●一般にタンデム系である工学システムの“どこで”防止するか･･･完封は不可能．許容出来るレベルは？　cf.パラレル冗長系：フェイルセーフ

＃2．トレードオフ問題

●コストを厭わなければ，限りなくゼロに近い故障率，事故率は達成出来るが･･･やるかやらないかは？

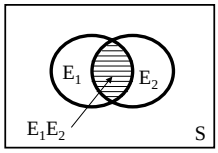
＃3．期待損失の効用推定

●生起確率→期待損失には，損失期待効用を決めている関数を決める必要がある．人命の金銭効用換算を無理矢理行う；損害賠償．

確率論の基礎の基礎　#1　条件付き確率，乗法定理

条件付き確率：E_2 なる事象が生起すると云う条件下で事象E_1が生起する確率$P(E_1 \mid E_2)$を与える．

$$P(E_1 \mid E_2) = \frac{P(E_1 E_2)}{P(E_2)}$$



乗法定理：結合事象E_1E_2が生起する確率を条件付き確率により表すと，

$$P(E_1E_2) = P(E_1 \mid E_2)P(E_2)$$
$$P(E_1E_2) = P(E_2 \mid E_1)P(E_1)$$

事象E_1とE_2が**独立**である特別な場合は（小学校以来の常識として承知しているであろう）以下となる．

$$P(E_1E_2) = P(E_1)P(E_2)$$

確率論の基礎の基礎　#2　条件付き確率を例題でイメージしてみる①

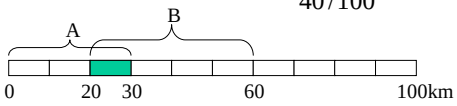
延長100kmの国道を考える．この区間では道路の状態や交通量は一様で，事故率も一様であるとする．次なる確率事象を定義する．

A=0〜30km区間で事故が起きる，B=20〜60km区間で事故が起きる

題意より，$P(A) = 30/100$　および，$P(B) = 40/100$

ここで，“区間(20,60)で事故が起きた場合，それが事象Aである確率”を考える．すなわち，事象Bが生起したという条件下で事象Aが生起する条件付き確率を求めると，

$$P(A \mid B) = P(AB)/P(B) = \frac{10/100}{40/100} = 10/40$$



10/40は図からも明である．

確率論の基礎の基礎　#3　条件付き確率を例題でイメージしてみる②

ある小都市の電力需要は2カ所の発電所a，bでまかなわれている．電力需要は時間的に変動するが，1つの発電所が故障しても，もう一方の発電所だけで全時間帯の75%の需要を満たすことが出来る．発電所の故障確率は，a，bともに0.1，同時にダウンする確率は0.02であると云う．事故発生時にこの都市の需要がなお満たされる確率は？

解答

事象A，Bを夫々,発電所aが故障，bが故障，と定義すると，

$$P(A) = P(B) = 0.10$$
$$P(AB) = 0.02$$

従って，

$$P(A \mid B) = P(B \mid A) = \frac{0.02}{0.10} = 0.20$$

故障が生じた場合に，それが2つのうち1つでの発電所のみの故障である条件付き確率は，

加法定理

$$P(A\bar{B} \cup \bar{A}B \mid A \cup B) = P(A\bar{B} \mid A \cup B) + P(\bar{A}B \mid A \cup B)$$
$$= \frac{P[A\bar{B}(A \cup B)]}{P(A \cup B)} + \frac{P[\bar{A}B(A \cup B)]}{P(A \cup B)}$$

積事象①･②を考えるとき②は①に対して自明

$$= \frac{P(A\bar{B})}{P(A \cup B)} + \frac{P(\bar{A}B)}{P(A \cup B)}$$

乗法定理

$$= \frac{P(\bar{B} \mid A)P(A) + P(\bar{A} \mid B)P(B)}{P(A) + P(B) - P(B \mid A)P(A)}$$

ベン図を思い浮かべて･･･

$$= \frac{0.8 \times 0.1 + 0.8 \times 0.1}{0.1 + 0.1 - 0.2 \times 0.1} = 0.89$$

以上より，0.89×0.75=**0.67**

確率論の基礎の基礎 #4 ベイズの定理

事象Aが生じる場合に特定のE_iが生起している確率は，条件付き確率と乗法定理を適用して以下で表すことが出来る．これをベイズの定理（Bayes' Theorem）と云う．

$$P(E_i \mid A) = \frac{P(A \mid E_i)P(E_i)}{P(A)}$$

$$= \frac{P(A \mid E_i)P(E_i)}{\sum_{j=1}^{n} P(A \mid E_j)P(E_j)}$$

全確率の定理

全確率を加法定理で開いている･･･当たり前の書き換え

信頼度と不信頼度

システム要素の寿命試験を行うと，経過時間とともに残存率は低下する．ある時刻において，当該システム要素が無故障で稼働する確率を信頼度と云う．故障である状態（モード）は無故障の余事象であることから不信頼度が定義される．

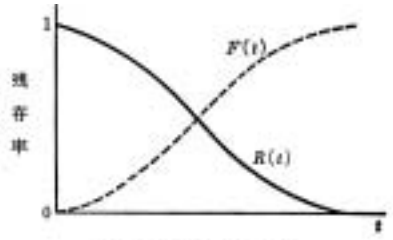


図 13.1 信頼度と不信頼度

$$R(t) + F(t) = 1$$

故障密度関数

確率論における確率と確率密度の関係は，微分積分関係であったが，それに準えて故障密度関数が定義出来る．

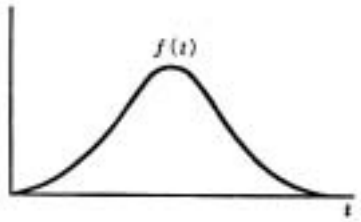


図 13.2 故障密度関数

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \quad \text{または，} \quad R(t) = \int_{t}^{\infty} f(t)$$

故障率

時刻tまで無故障でいて，t+dtに故障してしまうサンプルがどれくらいの割合か，を故障率と定義する．すなわち，故障率は単位時間当たりの故障度数で定義される．

$$\lambda(t) = -\frac{dR(t)}{dt} / R(t) = -\frac{d(\ln R(t))}{dt}$$

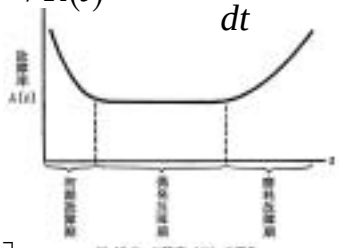
または，

$$R(t) = \exp\left[-\int_{0}^{t} \lambda(t)dt\right]$$

湯槽曲線 Bath-Tub Curve

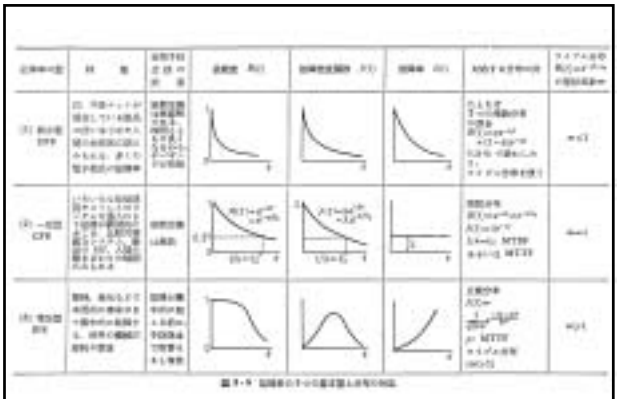
観察事実から故障率の時間変化は湯槽曲線で表されることが知られている．

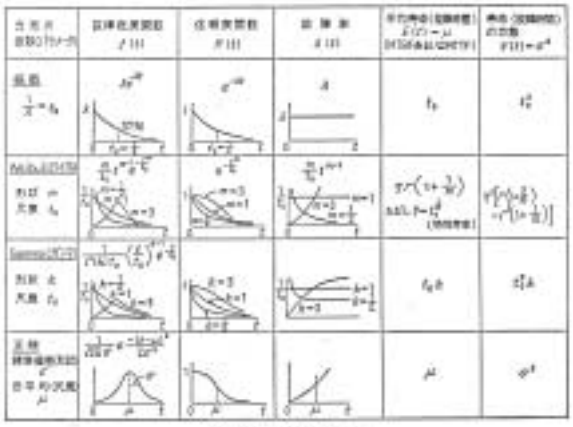
$$\lambda(t) = -\frac{dR(t)}{dt} / R(t) = -\frac{d(\ln R(t))}{dt}$$



偶発故障期では，故障率は時不変だから

$$R(t) = \exp\left[-\int_{0}^{t} \lambda(t)dt\right] = \exp(-\lambda t)$$





平均寿命 MTTF, mean time to failure

平均的耐用時間.

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty t \cdot f(t)dt$$

平均値(1次モーメント)の確率的定義から自明

考えてみよう！ヒント:部分積分.

確率変数$f(t)$のn次モーメントの定義 $\int_{-\infty}^{\infty} t^n \cdot f(t)dt$

もし故障率一定で時不変なら

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

考えてみよう！単に積分を実行すればいいだけ.

非修理系 vs 修理系, アベイラビィティ

非修理系(**壊れたらそれっきり;部品, 材料･･･人間**):平均(故障)寿命MTTF.

修理系(**繰り返し使うシステム**):平均故障間隔MTBF, mean time between failure. 信頼度R(t), 不信頼度F(t)に加えて保全度M(t)を定義し,(MTTFと同様に考えて),一旦故障した場合の平均的な修復時間;平均修復時間MTTR, mean time to repairを定義する.

$$MTTR = \int_0^\infty t \cdot \frac{dM(t)}{dt} dt$$

システムの非常事態に対する健常性を

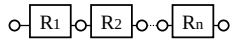
アベイラビリティ=MTBF/(MTBF+MTTR)

と定義し, これにより評価する.

タンデム(直列)系 vs パラレル(並列)系

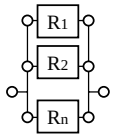
タンデム系:システムのどこかで故障が起きれば全体が動作不能.

$$R = \prod_{i=1}^{n} r_i$$



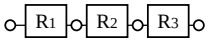
パラレル系:フェールセーフな系. コスト高.

$$R = 1 - F = 1 - \prod_{i=1}^{n} (1 - r_i)$$



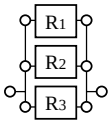
システムの信頼性 #1

･･･3node タンデム系, 3node パラレル系



$$R = r_1 r_2 r_3$$

$r_1 = r_2 = r_3 = r$ ならば $R = r^3$



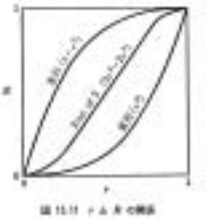
$$R = 1 - F = 1 - r_1 r_2 r_3$$

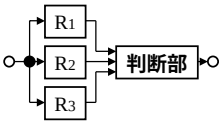
全で同時故障
その余事象

$r_1 = r_2 = r_3 = r$ ならば $R = 1 - r^3$

システムの信頼性 #2 ･･･2 out of 3

同種類のセンサを3つ並列に配置し, 3つのうち2個以上が異常を検出したときに異常と判定. 並列による信頼性向上と異常検出の誤作動を防止とに配慮. 原子力プラントの異常検知に用いられている.





$$R = 1 - F = 1 - \{r_1(1-r_2)(1-r_3) + r_2(1-r_1)(1-r_3) + r_3(1-r_1)(1-r_2) + (1-r_1)(1-r_2)(1-r_3)\}$$

センサ2と3が同時故障. 1は正常. センサ1と3が同時故障. 2は正常. センサ1と2が同時故障. 3は正常. 全センサが同時故障.

$r_1 = r_2 = r_3 = r$ ならば $R = 1 - \{3r(1-r)^2 + (1-r)^3\} = 3r^2 - 2r^3$

システムの信頼性 #3

並列と直列が混在する一般システムの計算法：信頼性構造モデルの出入口を結ぶ最小パスを全て調べる．i番目の最小パスだけが残り，残りのパスが全てダウンする確率をP_iとすると，

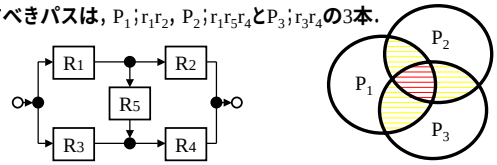
$$R = \Pr\left\{\bigcup_{i=1}^{M} P_i\right\}$$

を求めればよい．

ここで，∪はOR結合を意味し，Prは総合確率を表す．

システムの信頼性 #4 ･･･例3

考慮すべきパスは，P_1；r_1r_2，P_2；$r_1r_5r_4$とP_3；r_3r_4の3本．



$$R = \sum_{i=1}^{3}\Pr\{P_i\} - \sum_{i=1}^{3}\sum_{j>i}^{3}\Pr\{P_i \cap P_j\} + \sum_{i=1}^{3}\sum_{j>i}^{3}\sum_{k>j}^{3}\Pr\{P_i \cap P_j \cap P_k\}$$

不取敢，3つのパスの和集合

2重和（ベン図黄色部分）をダブルカウントし，3重和（赤色部分）をトリプルカウントしているから

左項でトリプルカウント補正した結果，赤色部分が欠落したから改めて3重和を加算

$$= \{r_1r_2 + r_1r_5r_4 + r_3r_4\} - \{r_1r_2r_5r_4 + r_1r_2r_3r_4 + r_1r_3r_4r_5\} + r_1r_2r_3r_4r_5$$

複数の故障様式 #1

システムの安全が損なわれる場合には，一般に複数の故障様式が想定出来る．

［例］“飛行機が墜落する”と云うfailureに至るには，エンジン故障，機体の破断（金属疲労により翼がもげるetc），人為的な操作ミス（酔っぱらい運転etc），天災（乱気流により予想外の力が機体にかかるetc）など多くの故障様式が想定し得る．

i番目の故障様式に対する信頼性を $p_{S_i} = P(\overline{E_i})$　E_i：i番目の故障様式が生起すると云う事象

システム全体の信頼性 $p_S = P(\overline{E})$

単モード極限値に関する命題

故障様式間に**正の相関**がある　$\prod_{i=1}^{k} p_{S_i} \le p_S \le \mathrm{Min}_i\left(p_{S_i}\right)$

故障様式間に**負の相関**がある　$p_S \le \prod_{i=1}^{k} p_{S_i}$

複数の故障様式 #2 ･･･例

洪水制御と水供給の二つの目的のために貯水池を設計する．洪水は先立つ冬に積もった雪が融けること（事象A）と春の多雨（事象B）とが組み合わさることにより，春だけに生じる現象である．一方，水供給については夏と秋のみに渇水となる場合があると云う．

つまり，水不足は冬と春の降水量の少ないことによる初夏の貯水量の低さ（事象C）と夏期の小雨（事象D）とが結びついて生起する．

斯くして，不適切な洪水制御（事象F）は　$F = A \cap B$

不十分な水供給（事象G）は　$G = C \cap D$

春の多雨は雪の多い冬に引き続いて訪れ，乾燥した夏は一般に小雨の春に続くものだと想定する．すなわち，事象AとB，事象CとDには正の相関が，而して事象FとG間には負の相関があることになる．各事象の年確率を以下と仮定する．

$$P(A) = 0.15,\ P(B) = 0.20,\ P(C) = 0.10,\ P(D) = 0.20$$

貯水池が満足に機能しない確率は，

$$P(E) \equiv P(F \cup G) = P[(A \cap B) \cup (C \cap D)]$$

FとGには負の相関があるから，

$$1 - P(E) \le P(\overline{F}) \cdot P(\overline{G}) \quad \cdots (1)$$

AとBには正の相関があるから，

$$P(\overline{A}) \cdot P(\overline{B}) \le P(\overline{F}) \le \mathrm{Min}\left[P(\overline{A}), P(\overline{B})\right]$$

$$\Leftrightarrow (1-0.15)\cdot(1-0.20) \le P(\overline{F}) \le (1-0.20)$$

同様にCとDには正の相関があるから，

$$P(\overline{C}) \cdot P(\overline{D}) \le P(\overline{G}) \le \mathrm{Min}\left[P(\overline{C}), P(\overline{D})\right]$$

$$\Leftrightarrow (1-0.10)\cdot(1-0.20) \le P(\overline{G}) \le (1-0.20)$$

$P(E)$ の下方限界を知るには，(1)式より $P(\overline{F})$ と $P(\overline{G})$ の上方限界を与えればよいから，

$$P(E) \ge 1 - 0.80 \cdot 0.80 \ \Leftrightarrow\ P(E) \ge 0.36$$

マルコフ過程（Markov Process） #1

ある確率変数の状態が，時系列的に見た時間ステップを有限回数だけ遡及した過去の状態にだけ影響される･･･このような確率過程をマルコフ過程という．特に，前回の時間ステップの状態だけに影響される最も単純な場合を1重マルコフ過程という．

起こりえる事象E_1,･･･,E_nが定義され，時間ステップの進行に伴いE_iからE_jに推移する確率をP_{ij}で表すものとする（P_{ij}を状態推移確率と云う）．ここで，時間ステップkにおいて事象E_mが生起している状態を第m要素が1，他要素は0とするベクトル$\mathbf{x_k}$で表す．状態推移が以下のvector-matrix方程式で表記出来る系をマルコフ連鎖という．Pを状態推移行列と云う．ここで，Tは転置を表す．

$$\mathbf{x_{k+1}} = {}^{T}\mathbf{x_k} \cdot \mathbf{P}$$

ここで，$\mathbf{P} = \begin{bmatrix} P_{11} & \cdots & P_{1n} \\ \vdots & \ddots & \vdots \\ P_{n1} & \cdots & P_{nn} \end{bmatrix}$

ただし，$\sum_j P_{ij} = 1$

マルコフ過程 (Markov Process)　#2

ベクトル$\mathbf{x}_k$は，時間ステップkにおいて事象E_mが生起している状態であり，第m要素が1，他要素は0であるとしたが，各状態の時間推移が確率過程であり，確率分布で表すことが出来るとするなら，x_kは以下のような実数要素ベクトルであると概念拡張すればよい．

$$\mathbf{x}_k = \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}_k = {}^T\begin{bmatrix} s_1 & \cdots & s_n \end{bmatrix}_k$$

ここで，subscriptは時間ステップを表す．

ただし，$\sum_i s_i = 1$

マルコフ過程 (Markov Process)　#3

3つの状態E_1, E_2, E_3からなるシステムで夫々の状態推移確率がシャノン線図に示されるように与えられているとき，初期分布 (1,0,0) (すなわち初期状態がE_1である) から出発して2ステップ目に各状態にある確率は？

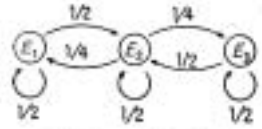


図 6・1 シャノン線図

枝分かれ図 (tree diagram) で考えると，

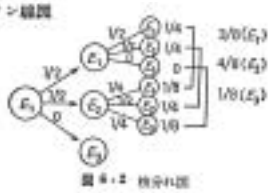


図 6・2 枝分れ図

マルコフ過程 (Markov Process)　#4

状態遷移行列は，

$$\mathbf{P} = \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/4 & 1/2 & 1/4 \\ 0 & 1/2 & 1/2 \end{bmatrix}$$

$\mathbf{P}^2$をとると，

$$\mathbf{P}^2 = \begin{bmatrix} 3/8 & 4/8 & 1/8 \\ 2/8 & 4/8 & 2/8 \\ 1/8 & 4/8 & 3/8 \end{bmatrix}$$

よって，2ステップ目のE_1, E_2, E_3からの生起確率は，夫々，3/8，4/8，1/8と求まる．行列$\mathbf{P}^2$の行和をとった値が1になっていることを確認せよ．

マルコフ過程 (Markov Process)　#5

極限確率

$\mathbf{P}^n$は，n→∞で一定値に収束する場合があり，そのようなケースでは定常時の各状態の確率分布を知ることが出来る．

$\mathbf{P}^n$が収束するのは，有限ステップで任意の状態から任意の状態に推移出来る場合だけであり，このような性質をエルゴート性 (ergodic) と云う．

定常時には，$\mathbf{x} = \mathbf{x} \cdot \mathbf{P}$　ただし，$\sum_i s_i = 1$ が成り立つから，これを代数的に解けばよい．

前スライドの例では，(1/4,1/2,1/4)が定常分布である．

$$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} = \begin{bmatrix} s_1 & s_2 & s_3 \end{bmatrix} \cdot \begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/4 & 1/2 & 1/4 \\ 0 & 1/2 & 1/2 \end{bmatrix} \quad \text{かつ} \quad s_1 + s_2 + s_3 = 1$$

マルコフ過程 (Markov Process)　#6

ある装置の故障はそれ以前に故障していたか，いなかったかにより影響される．前使用時に正常で次に故障する確率をλ，前使用時に故障していて次には正常に復帰している確率をμとし，定常時の故障確率はどうなるか？

シャノン線図は，

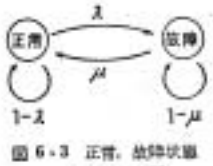


図 6・3 正常，故障状態のシャノン図

$$\mathbf{P} = \begin{matrix} \text{正常} \\ \text{故障} \end{matrix} \begin{bmatrix} 1-\lambda & \lambda \\ \mu & 1-\mu \end{bmatrix} \quad \begin{matrix} \text{正常} & \text{故障} \end{matrix}$$

$$\begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = \begin{bmatrix} s_1 & s_2 \end{bmatrix} \cdot \begin{bmatrix} 1-\lambda & \lambda \\ \mu & 1-\mu \end{bmatrix} \quad \text{かつ} \quad s_1 + s_2 = 1$$

これを解いて，$s_1 = \frac{\mu}{\lambda+\mu}, s_1 = \frac{\lambda}{\lambda+\mu}$

タンデム (直列) 系 の故障様式

タンデム系：システムのどこかで故障が起きれば全体が動作不能．

直列に結合された要素からなるシステムでは，構成要素のどこか一つが故障してもシステム全体は崩壊に至る．このようなシステムは冗長性がなく“最弱リンク”システム (weakest link system) とも云われる．このようなシステムの信頼性，安全性は，どの要素も故障しないことを要求する．

E_iを要素iの故障とすれば，直列システムの崩壊は事象

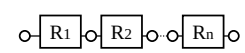
$$E_S = E_1 \cup E_2 \cup \cdots \cup E_m$$

であり，このシステムの信頼性は以下の事象で表される．

$$\overline{E_S} = \overline{E_1} \cap \overline{E_2} \cap \cdots \cap \overline{E_m}$$

各要素 (故障様式) が独立であれば，既述したように以下となる．

$$R = \prod_{i=1}^{n} r_i$$



タンデム（直列）系 の故障様式　#2　・・・例

20個の等しいリンクからなる鎖を考える（演習Ⅰの1．参照）．連結リンクの任意の1個（またはそれ以上）の破断が鎖全体の崩壊に至る，単純な直列システムの例である．

各リンクの破断確率を $p_{F_i}=1\times10^{-4}$ としてみよう．

システム全体の崩壊確率は各リンクの破断強度の相関性によりことなっていた．

＃1．個々のリンクの破断は統計的に独立

→どれが破断するかわからない・・・どれが壊れてもダメ→和事象をとる

$$p_F=\sum_{i=1}^{20}p_{F_i}=20\times1\times10^{-4}=0.002$$

＃2．個々のリンクの破断は統計的に完全相関

→壊れるときはみんな同時に生起（現実的には考えにくいが・・・）

$$p_F=p_{F_i}=1\times10^{-4}$$