■S4 群（宇宙・環境・社会）－ 6 編（安全・安心・安定）

3 章 共通手法

【本章の構成】

本章では以下について解説する.

3-1 安全性解析
3-2 PSA
3-3 フォルトトレランス
3-4 フェイルセーフ
3-5 ヒューマンエラー分析
3-6 セキュリティ
3-7 ソフトウェアと安全性

■S4 群－6 編－3 章

3-1 安全性解析

3-1-1 FMEA

（執筆者：清水洋孝）［2011 年 6 月 受領］

(1) FMEA とは

FMEA は Failure Mode and Effects Analysis の略であり，一般的に「故障モード・影響解析」と呼ばれ，予測に基づく未然防止のための手法として有用である．故障要因の抽出方法としてよく用いられる信頼性解析手法の一つである．FMEA は，FTA とともに IEC の国際規格になっている．医療分野では，ヒューマンエラー未然防止に FMEA が活用されている．

(2) 解析実施の流れ

FMEA では，システムの構成機器の一つに故障が発生した場合に，システムに及ぶ影響に対してワークシート（図 1･1･1 参照）を用いて解析する．特に，ワークシートは限定されていないので解析目的に見合ったワークシートを自分達で決める必要がある．FMEA の使用用途のワークシートはそれぞれ異なる．解析対象当該機器の本来の機能，発生しうる故障モードと原因，影響，故障検出方法，是正処置などの項目について検討する必要がある．見落としを避けるため，システムを系統的に調べる手順が定められている．

(3) FMEA の目的

FMEA の目的は，次のようにまとめられる．

① 潜在化した設計，システム，業務プロセス（医療やユーザなどの誤使用なども含む）上の問題点の早期検出
② 重点指向による開発期間の短縮
③ 信頼性試験・評価の効率化
④ 後工程への情報提供
⑤ 予防保全計画策定
⑥ 固有技術の統合化
⑦ 評価技術や情報の技術標準としての蓄積
⑧ 製品安全（Product Safety）のための手法

(4) FMEA 手順

一般的な設計 FMEA 手順を示す．

1. 必要な解析対象システムの理解をし，情報収集は，設計情報，全体システム，サブシステム，モジュールの関係を調査する．更に，要求仕様書，環境条件，使用条件，信頼性要求，保全性要求 [1] を階層的に行う．
2. FMEA 対象部位の選定を行い，システム，サブシステムなどの分解レベルを決める．
3. 装置の仕様と製造図面をもとに要求される機能を記述する機能ブロック図の作成．機能ブロック図は，装置を構成している部品間の電気的，機械的などの機能のつながりを示す．
4. 装置を構成している部品間の故障のつながりの信頼性ブロック図を作成する．
5. FMEA ワークシート，故障データを用いて構成要素に生じうる不具合の種類，故障モー

ドの列挙，抽出と選定をする．

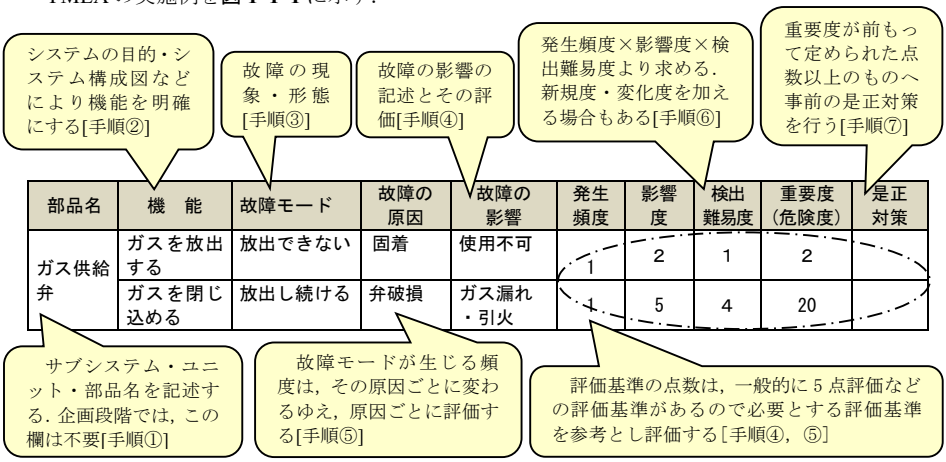
6. 評価点表に基づく故障の発生頻度，影響度，検出難易度の評価を実施．
7. 重要度評価（＝発生頻度×影響度×検出難易度）と事前対策すべき最終的影響故障モードの選出を行い，評価した故障順位の高いものについて設計変更の要否などの検討を行う．
8. 想定した故障からシステムを防御するための方法として，各種対策への展開は，故障検出の方法，是正処置の検討と記述を実施する．
9. 対策・是正処置の実施．

(5) FMEA の評価基準

一般的な評価基準は，発生頻度・影響度・検知難易度による評価基準（5 点評価法）が示されているので，必要とする目的の評価基準を分析者が選択すること．参考となる規格の基準では，MIL-STD-1629A[2]，IEC 60812[3] の厳しさ等級基準，及び，発生確率レベル等級基準，ISO/TS 16949[4] の評価基準，IEC 60300-3-9:1995[5] のリスクマトリクス，SAE ARP 926[6] の致命度指数計算がある．

(6) FMEA 実施

FMEA の実施例を**図 1･1･1** に示す．



部品名	機　能	故障モード	故障の原因	故障の影響	発生頻度	影響度	検出難易度	重要度（危険度）	是正対策
ガス供給弁	ガスを放出する	放出できない	固着	使用不可	1	2	1	2	
	ガスを閉じ込める	放出し続ける	弁破損	ガス漏れ・引火	1	5	4	20	

図 1･1･1　FMEA の例（ガスライター）[7]

(7) フォローアップ

(1) 対象の実施は，FMEA 結果に基づいて対策を行う．また，対策実施後の再評価は，対策の結果が低減されたかどうかの確認をし，対策実施によって新たな問題が発生していないかを検証する．

(2) 重要故障モードは，どうしても対策ができなかった構成要素・故障モードについては情報の共有を図り，今後に活かす．

(8) まとめ

将来起こりうる問題を事前に予測し，絶対に起こしてはいけないものを抽出し，その未然防止を図るのが FMEA である．基本にある考え方は，多く存在する故障モードの中で重要なものは実際に僅かである．これらの重点管理を行うことで問題の大半は防止できる．

■参考文献
1) 小野寺勝重：“グローバルスタンダード時代における実践 FMEA 手法,”日科技連出版社, pp.13-14, 1998.
2) MIL-STD-1629A：Procedure for performing a failure mode, effects and criticality analysis, p.9, 1980.
3) IEC 60812：Analysis techniques for system reliability－Procedure for failure mode and effects analysis (FMEA), p.35, 2006.
4) ISO/TS 16949：Quality management systems-Particular requirements for the application of ISO 9001: 2008 for automotive production relevant service part organization.
5) IEC 60300-3-9：Dependability management－part 3 Application guide－Section 9 Risk analysis of technical systems, p.47, 1995.
6) SAE ARP 926B：Fault/Failure Analysis Procedure, pp.37-38, 1997.
7) 鈴木和幸：“予測予防への FMEA の活用,”標準化と品質管理，日本規格協会, pp.6-7, 2007.

3-1-2 GOFLOW

3-1-3 ランクマトリクス法

（執筆者：鈴木喜久）［2010 年 1 月 受領］

信頼性では，部品の故障率から装置の故障率を算出し，更にその故障で安全に関するものを検討する手法がとられているが，安全の問題では，人間の関与の大きい場合があり，この部分が大きくなると，複雑になり，第 1 類の数値化が困難になる．最近はリスクという表現で，SIL というような第 3 類の数値が使用される場合もあるほどである．ここで，むしろ，第 3 類の数値として，ランクというもので表現する手法が出てきた．

安全ランクの基準は，

－2：絶対的に安全性のあるレベル
－1：十分，安全なレベル
0：経済的にも努力して達成できる安全レベル
＋1：現状で，通常達成している安全レベル
＋2：安全対策が必要なレベル
＋3：緊急に安全対策が必要なレベル

なお，安全を検討する項目は，過去の事例を参照する場合が多いが，これでは，それは考えていなかったというようなことになるので，また，複雑システムを人間が関与する場合としているので，人間の関与を一つの軸として，もう一つの軸には，対象により，適当な項目を選んで，検討する項目をマトリクスにした．2 次元マトリクスでなく，3 次元，4 次元を検討したいこともあるが，2 次元を標準としている．複雑システムの一例として，道路交通の場合を示しておく．ほとんどの場合，運転者の責任となる，すなわち，人間の関与する複雑なシステムなので，事例として適当と考えた．

表 1･3･1 マトリクスの一例（道路交通の安全性）

	設備（S）	ドライバ（D）	弱者（P）
制　度　（L）	ＬＳ	ＬＤ	ＬＰ
高速道路（H）	ＨＳ	ＨＤ	ＨＰ
幹線道路（B）	ＢＳ	ＢＤ	ＢＰ
生活道路（N）	ＮＳ	ＮＤ	ＮＰ
交差点　（C）	ＣＳ	ＣＤ	ＣＰ

ランクの算出（道路交通の設備関係 S）（自動車，道路，信号など）
(1) LS のランク，(2) HS のランク，(3) BS のランク（文献参照）
(4) NS のランク　0：路側帯確保，速度制限 20 km/hr
＋3：路側帯に標識あり
(5) CS のランク（交差点）
－2：交差点前に凹凸の設置，自動車にタグ検知装置
－1：センサシグナルの設置，鳥瞰センサの設置
0：歩車分離信号の設置，右折信号あり
＋1：一時停止方向の指定，適正ミラーの設置
＋2：角切りの完全実施
＋3：角切りなし
ランクの算出（ドライバ関係 D）
(6) LD のランク　－2：免許証に速度制限のタグ，自動車の改造
＋1：自転車の歩道走行可（年齢区分による）
（速度区分により，ランク 0 に）
(7) HD のランク　－2：道路改造と自動車改造による お猿運転
－1：免許証によるキー操作
(8) BD のランク　＋1：夜間，ライトの点灯（道路に検出警報装置の設置）
(9) ND のランク　－2：最高時速 20 km の実施
(10) CD のランク（文献参照）
ランクの算出（被害者関係 P）
(11) LP のランク　－1：歩行免許の導入（保険会社によるもの）
＋1：白線の引き方を歩行者優先に
(12) HP のランク　＋1：歩道橋の上から物を投げないこと（高い網を張る）
(13) BP のランク　－2：歩行タグの携帯（携帯電話に付与）
(14) NP のランク　－2：タグ付お守りの携帯
(15) CP のランク　＋2：左右の確認

■参考文献

1) 鈴木喜久：“道路交通の安全性,” ISSN 0913-5685, 電子情報通信学会安全性研究会資料, 信学技報, 109(348), SSS2009-29, pp.23～26, 2009.12.

3-1-4 マルコフモデル

3-1-5 製品安全解析技法 SU-H 法

（執筆者：和田　浩）［2010 年 1 月 受領］

(1)　過酷使用と製品安全の確保

消費者製品は，ユーザが製品知識や構造をよく知らないため多様な使い方をされる．例えば，長期使用（10～30 年間），厳しい環境での使用，取扱説明書と違う使い方，故障やその前兆に気付かないで使い続けるなどである．特に長期使用はすべての製品に共通する問題であり，市

場でも不安全事故が多く発生している．メーカはこれら過酷使用の実態，事例をよく把握して，安全性設計，製品安全の確保に取組んでいく必要がある．**図 1･5･1** にその概念図を示す．

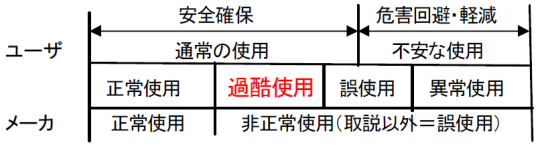


図 1･5･1　過酷使用と製品安全の確保

(2)　SU-H 法のねらいと特長

(1) ユーザの過酷使用（マン）と製品の故障メカニズム（マシン）とをマトリクス図法で組み合わせて（マン-マシンインタフェース，MMI 変換）して解析を進める．

(2) 安全性（危害防止）には結果（影響）解析が重視される．本技法は ETA を利用し，設計レビューができる．

(3) リスク解析-評価-対策のフローで未然防止マネジメントを完結する．SU-H 法の実施手順の中に解析後の評価，改善の進め方も織り込んでいる．

(3)　SU-H 法の実施手順と留意事項

(1) 過酷使用（SU）をリストアップする（表 1･5･1 参照）．

・長期使用（最年長チェック）を第 1 列に上げる．

・市場経験事例を調査把握し，その製品の代表的な厳しい使われ方を選定する．

(2) MMI 変換をする．

・過酷使用を技術（設計，頼性）に置き換える．過負荷ストレスによるダメージ（部位，故障モード）を想定する．

(3) 想定したすべての部品（ユニット）を H 欄に上げる．

(4) SU と H とのマトリクス欄の設計・技術的検討を行う．

・部品ごとに具体的な故障モードを上げる．複数個あるときは①，②，…記号で区別する．

(5) 各故障モードを初期事象とした ET 図を別紙に作成する（**図 1･5･2** に A-2②の ET 図実施事例を示す）．

・本来の ET 図は，成功失敗の両枝について展開するが，SU-H 法では失敗枝のみ展開する．

(6) すべての成功枝（推定仮説）について検証，評価をする．

・文書化した基準（書），マニュアルなどから基準規格値を明確にして，三現（現場・現物・現人）で対比する．

① 基準（値）が適正で，かつ現場で三現を順守している　　○（対策不要）

② 適正だが，順守していない　　×（対策必要）

③ 管理基準がない，または不備　　×（対策必要）

(7) 改善対策実施計画書を作成し，実践，フォローアップする．

・技術的（再発防止，指導訓練も含む）と管理的（未然防止，基準書の新作改正を含む）両面の対策が必要

表 1･5･1 に SU-H 法の実施事例を示す．

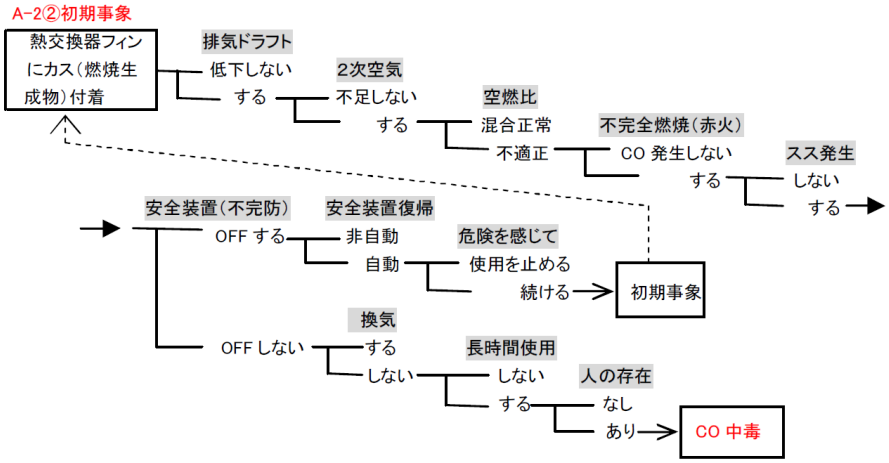


図 1･5･2　マトリクスの ET 図

表 1･5･1　SU-H 法の実施事例

SU-H 法	製品名（品番） ガス小型湯沸器	手順　MMI 変換→マトリックス検討→初期事象決定→ET 図 評価→対策　——：該当せず，（ ）：重複のため省略			実施日 担当・承認	
SU / H		記号	A	B	C	D
		過酷使用	長年（15 年以上）使用	長時間換気せず	不調のまま使用	室
		MMI 変換	・経時劣化（付着，ワレ，酸化，固着，摩耗，変形，つまり，腐食， ・安全装置の不動作	・酸素濃度低下で不完全燃焼 ・不完全燃焼による炎の立ち消え	・安全装置自動復帰による危険 ・不完全燃焼でススの付着	換 よ 阻 大
No	部品	機　能	故障モード			
	バーナ U	・混合ガス生成 ・完全燃焼	不完全燃焼	①炎口拡張，狭窄 ②吸気口ホコリつまり	酸欠燃焼	——	C
2	熱交換器	・温水熱交換 ・排気ドラフト	腐食穴明 ドラフト小	①水管腐食穴明きき ②フィンにカス付着	（ススト付着，つまり）	（ススト付着，つまり）	
3	ガスバルブ	一次ガス開閉	ガスもれ	摩耗によるガスもれ	——	——	
4	不完全燃	不完全燃焼を	不動作	①劣化による不動作	（ススト付着による	（ススト付着による	

3-1-6 ベイジアンネットワーク

3-1-7 RCA

（執筆者：清水洋孝）［2011 年 6 月 受領］

(1)　RCA とは

RCA は Root Cause Analysis の略であり，一般的に「根本原因分析」と呼ばれる．RCA は，不具合や事故から辿って直接原因分析を踏まえて，その背後に潜むシステムの問題，及び，ヒューマンファクタを探る手法である．更に，直接原因を未然に防止することができなかった組織活動に関わる要因を分析し，マネジメントシステムを改善する処置に貢献する．当該業務に関係するメンバーが集中討論し，原因の同定，追跡調査することで潜在的な問題を明らかにする

ことができる．分析のポイントと分析の基本的な流れは，**表 1･7･1** に示す．

表 1･7･1　分析のポイントと分析の基本的な流れ

項　目		具体的内容
分析のポイント		分析者は，①何が（What）起こったのか，②どのように（How）起こったのか，③なぜ（Why）起こったのか，を正しく理解する．また，現場，現物，現実をよく観察し，論理的な背後要因（なぜ，そうなってしまったのか）を深く探る．
分析の基本的流れ	［RCA の分析範囲］	
	(1) 分析からの事実把握と原因究明	①状況の把握は，「いつ」「誰が」「何をした」のか，事実を確認する．「出来事（事実）」を時系列に並べて，事実を正しく理解するために時系列事象関連図（事象と原因の時系列図）を作成（図 1･7･1 参照）する．事象発生における時間の経過と事実を確認する． ②時系列による事実の整理と把握については，“なぜなぜ”分析を実施（図 1･7･2 参照），根本原因の追究・事象を記述する手法は，VTA（Variation Tree Analysis）や医療分野では，出来事流れ図（フローチャート）を使用． ③問題点の抽出は，具体的に可能な限り簡潔・定量的に記述する． ④背後要因となる問題点を具体的に列挙し，因果関係図の作成結果に基づき，根本原因を確定（図 1･7･3 参照：原因究明）する．
	［RCA 結果に基づき，改善・改革ステップとして対策実施］	
	(2) 対　策	⑤考えられる対応策の列挙 ⑥実行可能な具体的対応策の決定
	(3) 実　施	⑦対応策の実施
	(4) 評　価	⑧実施した対応策（防護対策）の有効性評価，すなわち，是正処置及び予防処置が及ぼすと考えられる副作用の評価が行われていること．

(2)　RCA（根本原因分析）

(a) 事象と原因の時系列図

時系列分析は，事象の全体を流れ図で示し，始点と終点を選び，状況に関連したすべての重

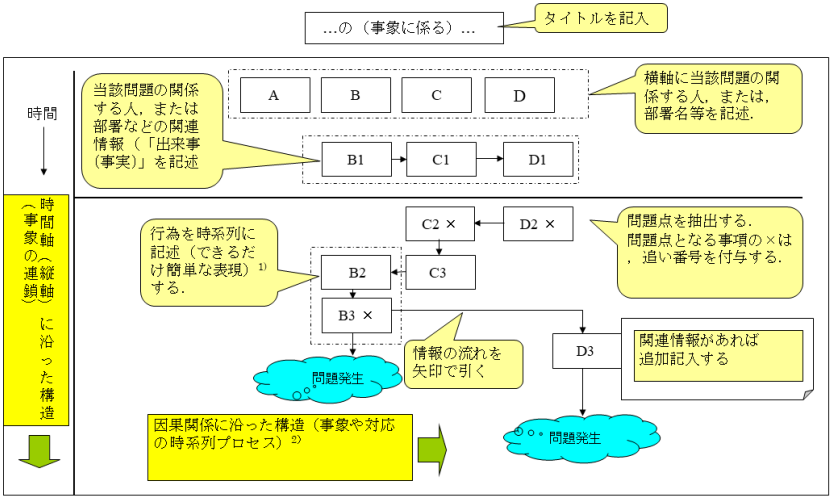


図 1･7･1　事象と原因の時系列図

要な情報を時系列に記入して事象関連図を作成する方法である（**図 1･7･1**）．関連した状態，二次的な事象，想定などの状況の特徴を時系列に記入して関連を見る．根本原因分析では，明確に系統立てた手法があるわけでなく，手法の使い勝手や特徴に応じて分析を行う必要がある．時系列からの事象をもとに要因の抽出を行う場合は，なぜなぜ分析が用いられる．この分析は，ある事象がなぜ発生したのか理由を「なぜなぜ」を繰り返す．一般的に「なぜなぜ」を 5 回繰り返すと根本原因が浮かびあがるとされている（図 1･7･2 参照）．

(b) 根本原因の追究

① RCA の基本“なぜなぜ分析”（**図 1･7･2**）

“なぜなぜ”分析を繰り返し，根本原因を追究する．

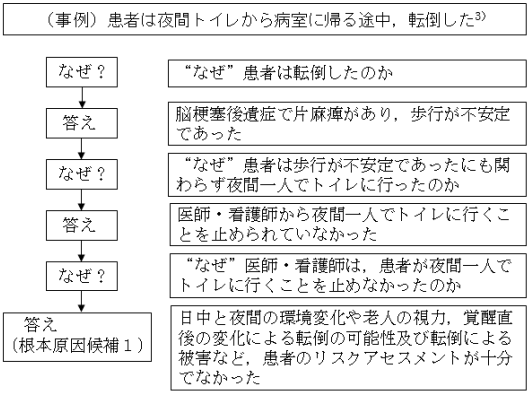


図 1･7･2　なぜなぜ分析事例

② 因果関係図作成・根本原因の確定（**図 1･7･3**）

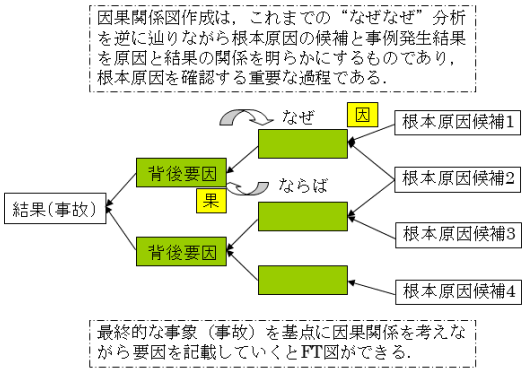


図 1･7･3　因果関係図の作成

(3)　まとめ

RCA は，有害事象やヒヤリハットの原因となった潜在的障害やシステム障害を追求するた

めの定性的分析手法であり，システム的あるいは組織的な問題を追究し，人間が複雑なシステムと関わることから生じるエラーを認識することを目的としている．適切な方法で RCA を実施すれば，改善すべき点が明らかになる．

■参考文献
1) 飯田修平，柳川達生：“RCA の基礎知識と活用事例,” pp.38-39, 2006.
2) 原子力安全基盤機構：平成 19 年度人間・組織等安全解析調査等に関する報告書「根本原因分析ガイドラインと教育資料作成」,” pp.20-21, 2008.
3) 石川雅彦：“RCA 実践マニュアルー再発防止と医療安全教育への活用－.” pp.34-35，医学書院, 2007.

3-1-8 HAZOP

3-1-9 ペトリネット

（執筆者：中村英夫）［2011 年 11 月 受領］

ペトリネット（Petri Net）は，離散的な分散システムを数学的に表現する手法として 1962 年にカール・アダム・ペトリが考案したモデリングツールである．分散システムの状態を「条件に相当するプレース（Place，円で表記）」，「事象を表すトランジション（Transition，棒または細長い矩形で表記）」という 2 つのノード（Node）と，ノード間の遷移を示すアークと呼ぶ有向枝を用いて表記する．システムの動的な状態変化は，プレースに置かれるトークン（Token）と呼ばれる点の移動で表現できる．システムのある時刻 t における各プレース上のトークンの配置をマーキング（Marking）といい，時刻 t におけるシステムの状態を表す．

多くのモデル記述言語がシステムを静的にしか表現できないのに対し，システムの動的な振る舞いが表現できるため，仕様の無矛盾性やシステムの挙動におけるデッドロックの有無などの解析に用いられる．

3-1-10 FTA

■S4 群－6 編－3 章

3-2 PSA

■S4 群－6 編－3 章

3-3 フォルトトレランス

（執筆者：中村英夫）［2011 年 11 月 受領］

フォルトトレランス（Fault Tolerance）とは，システム内に故障が発生したときにも，機能を維持し続ける能力，故障に対するシステムの障害の程度を最小限度に抑える能力のことをいう．また，フォルトトレランスに配慮されたシステムをフォルトトレラントシステム（Fault Tolerant System）という．

フォルトトレランスには，故障に対し機能劣化を完全に防止するフォルトマスキング（Fault Masking）というレベルと，一部機能低下は容認しつつも，一部機能を維持し続けるフェールソフト（Fail Soft）[†1]，そして，機能は停止するものの確実に安全側に停止させるフェイルセーフの 3 レベルに分けられる．

その実現手法も多様であり，システムに求められる水準に対して適切な手法の選択と確実な作り込みが求められる．その実現には対象とする故障レベルの定義によって満足するアーキテクチャが左右される．故障モードでは同時多重故障を想定した設計が最も厳しい要件である．この厳しい要件に対しては，特殊な回路の場合ではあるが非対称誤り特性を持つリレーによって単一系でフェイルセーフを実現できることが明らかとなっている．実際に，リレーによる鉄道信号用継電連動装置は，非対称誤り特性を持った信号用継電器によってフェイルセーフ名装置を実現している．この詳細は 3-4 節のフェイルセーフを参照して欲しい．

一方，コンピュータシステムなどにおいては，同時多重故障ではなく若干要件を緩和した非同時多重故障までを想定したフォルトトレラントシステムの構成が一般に用いられており，実現手法には，何らかの冗長構成（多重系）を用いることが多い．

また，フォルトトレラントシステムで重要な回路構成法に W. C. Carter らが 1970 年代後半に発表したセルフチェッキング回路がある．セルフチェッキング回路は，情報のとり得る空間を符号語空間で定義し，故障状態のモードとして出力が正規な符号語をとる場合（これは問題ない）と，とり得ない非符号語空間の値をとるか誤った符号語をとるケースがあるとして，回路の性質を次のように定義している．回路中に故障があっても，非符号語をとるまでの符号語は正しいことが保障される回路をフォルトセキュア（Fault Secure）とし，一方，故障があれば通常の入力が与えられることにより必ず非符号語を出力することが保障される回路をセルフテスティング（Self Testing）と定義する．更に，回路がフォルトセキュアでかつセルフテスティングなら，出力が符号語空間のものであれば正しいとして利用できる．このような回路をトータリィセルフチェッキング（Totally Self-Checking）回路と定義する．トータリィセルフチェッキング回路であるなら，出力値が非符号語の値をとったときに安全側に遷移させる仕組みを付加すればフェイルセーフシステムにも利用できる．

この場合，非符号語をとったか否かの検査回路が重要な意味を持つが，検査回路に要求される性質としてコードディスジョイント（Code Disjoint）を定義している．コードディスジョイントは，非符号語入力に対しては必ず非符号語出力をとることが保障される性質で，*n*-ビットの入力を 2-ビット対の出力に圧縮する検査回路などが提案されている．また，回路がトータリィセルフチェッキングであり，かつコードディスジョイントであるなら，その回路の前段に検

[†1] グレースフルデグレデーション（Gracefully Degradation，優美劣化）と称することもある．

査回路を置く必要がないため，回路規模の縮小に有効である．

トータリィセルフチェッキングの概念は単一故障モードを前提としていたが，更に非符号語が出力されるまでは，多重故障であっても出力符号語の正しさを保障するストロングリィフォルトセキュアの概念がセルフチェッキング回路の最高のクラスとして定義されている．南谷らは，セルフチェッキングシステムにおける誤り安全性と誤り伝搬性の概念を発表し，ストロングリィフォルトセキュアシステムの構成方法を明らかにしている．コンピュータを処理部として用いる今日のシステムのフェイルセーフ化においても重要な概念と言える．

■S4 群－6 編－3 章

3-4 フェイルセーフ

（執筆者：中村英夫）［2011 年 11 月 受領］

フェイルセーフ（Fail Safe）とは，回路・装置・システムにおいて，何らかの故障が発生した場合に，常に安全側の状態を維持もしくは安全側の動作状態に遷移する特性をいう．フェイルセーフ性を有したシステムを，フェイルセーフシステムと呼ぶ．装置やシステムは必ず故障するし，人間の誤操作も不可避である．鉄道や産業機械などのように安全性が要求されるシステムでは，これらの如何なる不具合に対しても，安全性を保障するフェイルセーフシステムが開発され用いられてきた．

論理回路のフェイルセーフはこのような配慮の積み重ねの中から経験的に構築されてきたが，その実態を論理的に解明したのは 1965 年頃であった [1]．例えば，回路出力の 0 側誤りを安全側と仮定する．~~図 2 において出力段から安全側を割り当てていく．~~出力端の AND 素子は 0 側非対称誤り素子を使えばよい．このようにして，入力まで安全側を割り当てていくと，A には 1 側非対称誤り特性を有した入力を，B,C には 0 側非対称誤り特性を持つ入力を使えば，回路としてのフェイルセーフ性が達成できる．これに対し，~~図 3 に示した回路は，~~排他的論理和を実現する回路であるが，同様に出力から安全側状態を割り当てていくと，NOT 素子からは 1 への誤りが，一方，AND 素子からは 0 への誤りが要求され，矛盾するので，対応できない．

この 2 つの回路を比較する．回路を表現した論理式において，それぞれの入力変数が負論理，もしくは正論理の一方のみで構成される回路と，そうでない回路に別れる．前者の回路なら，「非対称誤り論理素子を用いて高々一重系でフェイルセーフ回路が構成できる」．このような回路をユネイト（Unate）な回路と呼んでいる．その後，「ユネイトでない回路のフェイルセーフ化」や，「対称誤り素子によるフェイルセーフ回路の構成方法」[3]，「非対称誤り論理素子の開発」[4] などの研究成果が相次いで発表され，フェイルセーフ論理回路の研究は我が国の独壇場となった．

ユネイトでない回路のフェイルセーフ化に対しては，1 を(1, 0)，0 を(0, 1)という 2 ビットで表現する二線論理系が重要である．二線論理系の NOT は線を交差させればよい．したがって，ユネイトでなくても，論理回路（AND，OR，NOT で表現できる）を二線論理系で実現するなら，入力要素の正論理展開で構成されるためフェイルセーフにできることが分かる．更に，二線論理系では(1, 0)，(0, 1)という正規な情報のほかに(1, 1)や(0, 0)という誤り情報が定義できる．同時故障がないという前提は必要であるが，誤り情報が検出されたときに出力を安全側に制御すれば，非対称誤り論理素子でなく汎用の素子でもフェイルセーフ回路が構成できる．一方，回路レベルでも，正規な 1, 0 の状態値のほかに誤り状態値を定義すれば 3 値フェイルセーフ論理系になる [3]．また，二線論理系は情報を 2 ビットで表現したが，n ビットの符号語中に必ず k ビットの 1 を持つような符号を利用した k-out-of-n 符号語によるフェイルセーフ論理回路も考えられる．

非対称誤り素子によるフェイルセーフコンピュータの開発は，フェイルセーフ論理の黎明期の 1970 年頃にチャレンジされ成功している．しかし，汎用コンピュータの急成長もあり，経済性の隘路から普及するには至らなかった．

安全性が要求される制御分野に使えるフェイルセーフなコンピュータシステムの開発は

1980 年代に入り相次いで成果を挙げた．複数の MPU の処理を照合し，不一致を早期に検知して安全側に制御する機構の組み込みが一般的であるが，そのなかには，符号語と非符号語の概念に依拠し高信頼化を図ったフォルトトレランスの概念に符合するものもある．今日ではシングルチップの中に 2 つの MPU とフェイルセーフな照合部を組み込んだフェイルセーフ RISC プロセッサも実用化されている [6].

ハード的には解が得られたとはいえ課題もある．ソフトウェアの誤りはコンピュータ制御では致命的である．この件については，3-7 節ソフトウェアで触れる．

ところで，フォルトトレランスの項でも説明したが，我が国でフェイルセーフ論理の研究が盛んであったころ，米国ではフォルトトレラントシステムの研究が 1970 年代半ば頃から活発化し, やがてセルフチェッキング回路の構成概念が確立する [5]. セルフチェッキングの概念は，故障の有無を符号語，非符号語で弁別するもので，汎用素子を対象としたフェイルセーフ論理系の成果と符合する．回路中に故障があっても，非符号語をとるまでの符号語は正しく（フォルトセキュア性）故障があれば必ず非符号語を出力する（セルフテスティング性）トータリィセルフチェッキング回路は，故障が検出された段階で安全側に遷移させる仕組みを付加すればフェイルセーフシステムに利用できる．更に非符号語が出力されるまでは，多重故障であっても出力符号語の正しさを保障するストロングリィフォルトセキュア回路も，コンピュータを演算部として用いる今日のシステムのフェイルセーフ化において重要な概念と言える．

■参考文献

1) 渡辺，高橋：“フェイルセイフ形論理系の一般法,”信学全大, vol.72, 1965.11.
2) H. Mine and Y. Koga：“Basic properties and a construction method for a fail-safe logical systems,”IEEE Trans. Electronic Computer, vol.EC-16, no.3, pp.282-289, Jun. 1967.
3) 当麻，大山，坂井 :“対称誤りを考慮したフェイルセイフ順序回路の一構成法,”信学論(D), vol.55-D, no.3, pp.202-209, 1972.3.
4) 土屋：“3 値 C 型フェイルセイフ論理回路,”計自学論, vol.6, no.1, pp.81-88, 1967.2.
5) W.C.Carter, et al.：“C of self checking computer design,”Dig. Pap., FTCS-7, pp.117-123, Jun. 1977.
6) 高橋，中村，星野，三枝，平 :“フェールセーフプロセッサのシステム LSI 化,”信学技報, FTS2001-75, 2001.
7) 南谷，河村 :“セルフチェッキング・システムにおける誤り安全性と誤り伝搬性の概念,”信学論(D), vol.J68-D, no.12, pp.2007-2014, 1985.

■S4 群－6 編－3 章

3-5 ヒューマンエラー分析

■S4 群－6 編－3 章

3-6 セキュリティ

（執筆者：佐取　朗）［2009 年 10 月 受領］

セキュリティとは，様々な攻撃などの脅威から情報，人．財物などを守ることであり，情報を守る対策を情報セキュリティ，人，財物などを守る対策を防犯システム（セキュリティシステムともいわれている）という．どちらも安心・安全を求める時代になり，より重要性が高まってきている．本節では，それぞれについてページ数の関係もあり概略を説明する．

3-6-1 情報セキュリティ

現代は情報社会になり，インターネットでより広範なネットワーク化が可能になり，如何なる所ともつながってしまう．また，情報社会はあらゆるものがデータ化されネットワークを駆けめぐるようになっており，公共活動，企業活動，社会活動，日常の生活などすべての面でなくてはならないものになっている．これらのシステムが，何らかの行為によって停止することは社会機能を停止させてしまう．また，ネットワークから潜り込みにより，情報が窃取されることは個人情報，企業機密の漏洩など多大な被害を及ぼしてしまう．これらのことを発生させないためには，情報セキュリティが必修である．

情報に対する脅威は大別して，災害，故障，過失，窃盗，不正行為，破壊行為などが挙げられ，対策としては物理的，技術的，運用的対策の三本柱となるが，最近は人が絡む運用的部分でトラブルが多く発生している．また，モバイル PC，USB メモリの小型のものが出現したことによるトラブルが非常に多くなってきており，ネットワーク的にはしっかりしていても，それらのものに対する対策がポイントになりつつある．また，パソコンの個人所有も数多くあり，それらがネットワークを通じて悪さすることも増えており，全員の情報セキュリティに対する意識向上を図らない限り，成り立たない状況になってきている．

「情報セキュリティ」とは「情報の機密性，完全性及び可用性を維持すること．更に，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めて良い」と定義されている[†2]．簡単に言えば，情報を守ることと言える．

以下に情報セキュリティについて概略であるが説明する．

まず，情報セキュリティに対する組織的取組みが重要で，セキュリティポリシー，管理に関する規定を定め，実践することが重要で，コンプライアンスも含めた推進体制をはっきりさせ，同時に情報資産のランク付け，その取扱いの方法や管理責任者などを定める．

また，重要な情報については，業務プロセスごとに，責任者や手順の明確化，取扱者の限定，処理の記録などが必要，外部に委託する場合なども，相手に対して明文化したものを示し，内部と同等レベルに管理させる．同時に情報に関する守秘義務にかかる手続きも行っておくことが必要で，一連のことを計画的に組織全員に教育することを繰り返し，関係者へ情報セキュリティに関するルールの周知と知識習得をさせる必要がある．

物理的セキュリティとしての機器，情報などの盗難対策，関係者のレベルに応じた出入管理，施錠管理，電源のバックアップ，通信回線の保護などと，重要書類，モバイル PC，記憶媒体の管理も重要である．

[†2] JIS Q 27001:2006.

情報システム，通信ネットワークに関して運用管理の明確化，ウィルス対策ソフト（ファイアウォール機能，スパムメール対策機能，有害サイト対策機能など）と，パターンファイルの更新を的確に行う．また，それらの持っている機能をフルに活用し，ウィルス検査を行うと同時に，システムに関する情報を定期的に入手し，パッチを的確に実施，脆弱性対策を行う．ネットワークに流れる情報は重要度に応じ暗号化するほか，ファイルによってはパスワードを設定する．情報システムのアクセス制御として，利用者にパスワードを付与し，アクセスログをとることで，不正使用などの確認を実施すること，許可されていないソフトなどを使用制限することも重要である．また，パスワードは定期的に変えるようにする必要である．モバイル PC，記憶媒体などの持ち出し規定を定め，重要度に応じ認証，暗号化を行う．開発，保守時にも利用者 ID の管理，利用者の識別と認証を実施．同時にプロセス管理も的確に実施する．

情報システムは故障，事故などが発生することもあり，それらを想定し発生時の対応を明確にしておき，被害を最小限にする方策も重要である．

以上のように，事前にあらゆる事態を想定し，対策を立て運用し，チェックを行い，そのときでのベストな状態に保っていくことが情報セキュリティである [1]．

3-6-2 防犯システム

防犯システムも，該当施設内に警備員がおり，現地で監視確認対応するものと，通信回線を介し遠隔地で監視確認し，該当施設へ警備員を車両などで急行対応させる機械警備システム（警備業法では機械警備業務という）がある．また，防犯カメラシステム（CCTV も含む），出入管理システムも，防犯システムの一部といえ，前者は現地監視と遠隔地監視の双方がある．

ここでは，伸びの著しい機械警備システムを主体に説明する．

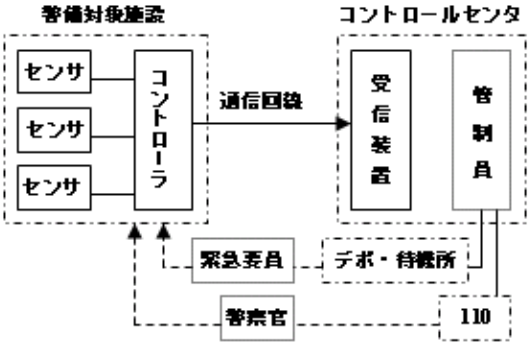


図 6・1　機械警備システム機能図

その仕組みは**図 6・1** に示す通りで，警備対象施設の必要な場所の窓，戸，扉，部屋内などへ目的に応じたセンサを設置し，それらの情報をその建物内に設置されたコントローラ（送信機）に集め，送受信装置に適合する各種通信回線を通じ，受信装置の設置されたコントロールセンタに接続される．その施設に泥棒が窓から侵入すると，その窓に設置されたセンサが感知し，その侵入情報をコントローラからコントロールセンタの受信装置に送信する．コントロールセンタではその施設に発生した変化情報とその施設に関する必要情報を表示し，管制員はその施

設を担当するデポ（発進基地），待機所（車両）に待機している緊急要員に対処を指示，緊急要員は現場に急行する．緊急要員は現場到着後点検を実施し，異常な状態が発見されたら，コントロールセンタへ報告し，コントロールセンタから 110 番通報を行う．緊急要員は現場到着した警察官と協力点検を行い，犯人を逮捕する．コントロールセンタは同時にその施設の責任者に通報する．その責任者の到着後，被害の確認を行う．その後正常復旧させ，警備状態に戻し警備を続行する．

このような侵入の他火災，設備異常，非常通報などの情報も監視している．コントロールセンタは都道府県ごとにあり，デポ，待機所は，警備業法に定められた対処規定時間内（25 分以内，一部地域が 30 分以内）に現場到着できる範囲内に設置されている．このシステムは全国で 215 万余件（20 年末）の施設の警備が実施されており，個人住宅から公共機関，金融機関，一般事務所，ビル，工場，学校，店舗など多くの施設まで広がっている．

(1) センサ

ここでいくつかのセンサについて解説する．

(a) マグネットセンサ

窓，戸，扉などの開を発見するもので，可動側にマグネットを設置し，固定枠側にリードスイッチ設置し，窓などが開くことによりマグネットが離れ．検出するもの．

(b) ガラスセンサ

ショーウインドーなどのガラス破壊侵入を発見するもので，ガラスに圧電素子を接着し，ガラス破壊時に発生する高周波の破壊振動を検出するもの．

(c) 壁センサ

コンクリート壁の破壊を早期に発見するもので，壁に圧電素子が設置され，壁破壊時の破壊振動を検出するもの．

(d) 対向，反射式赤外線センサ

赤外線遮断で侵入を発見するもので，近赤外線発光・受光ダイオードを使用し，発光・受光器間をビーム状に警戒，赤外光線の遮断を検出するもの．発光・受光器を一体に収容し，物体に当たった反射光を受光器で監視，その変化を捉えて検出する反射式のものもある．

(e) 熱線センサ

熱エネルギーで侵入を発見するもので，焦電素子，サーモパイルを使用し，監視空間をビーム，面，立体状に監視，その空間に侵入者が入ることによる熱エネルギー変化を検出するものである．パッシブタイプで光学系を換えることにより様々な監視パターンが得られること，対誤報性能が良いこと，低消費電力であることなどから数多く使用されている．

(f) 画像センサ

CCTV システムが防犯用にも数多く導入され，常時監視されていたが，ディジタルビデオレコーダで録画し，必要時に確認する形態も増えてきた．

機械警備システムで，最新のものは，CCD センサを用い，画像を常時取り込み，初期に設定した正常状態の画像と比較し，変化があれば異常として捉える．また，侵入者があった場合，動体抽出を行い，大きさ，人らしさなど，各種のアルゴリズムチェックにより，特徴量検出を行い，異常と判断し，コントロールセンタに異常信号を送出する．同時に画像圧縮技術により，現場の異常検出以前の画像，異常検出画像，その後の状態画像を送出し，コントロールセンタで，侵入した賊の確認ができる画像センサシステムまで実用化されている [2)]．

■参考文献

1) 岡本栄司 : “情報セキュリティ概説,” 電子情報通信学会（編） 情報セキュリティハンドブック, pp.3-6, オーム社, 2004.
2) 佐取　朗 : “防犯システム,” 室　英夫, 大和田邦樹, 佐取　朗, 石垣武夫, 石森義雄（共編） 次世代センサハンドブック, pp.1019-1023, 培風館, 2008.

■S4 群－6 編－3 章

3-7 ソフトウェアと安全性

（執筆者：中村英夫）［2011 年 11 月 受領］

シーケンス制御などの分野にコンピュータが導入されるようになった．なかでも，安全性に直結した原子炉や鉄道，航空機などの制御部に組み込まれたコンピュータシステムの安全性確保に，ソフトウェアの安全性は不可欠の課題とされた．

ソフトウェアのバグは，ハードウェアの故障と同様にシステムに致命的な影響をもたらす．しかも，ソフトウェアのバグはハードウェアの劣化故障とは異なり，生産プロセスで発生する Systematic Failure である．安全性の確保には，如何にしてバグの少ないプログラムを開発するか，という高信頼化プログラミングへのチャレンジとして定式化された．

この方法論は 2 つに大別できる．一つはバグそのもののないプログラムを開発しようというもので，形式的手法（Formal Method）がその代表である．

形式的手法は，仕様を形式的言語で記述し，その仕様の正当性を対象システムに普遍的に成立する公理系によって証明することで，仕様段階のバグを回避する．更に，形式的言語で記述された証明済みの仕様を，機械的にプログラミング言語に落とし込めれば，バグが入り込まないという考え方による．実際には，形式的に記述された仕様の証明や，形式的言語からプログラム言語に変換する際の正当性保障など，課題は多い．しかし，厳密な型チェックや仕様記述の形式的表現などによる高品質化への効果は無視できない．形式的手法には Z や VDM, LOTOS など様々なものが提案されている．

もう一つのアプローチは，プログラミングにはバグはつきものであるから，多様な設計や診断機構の組込みにより早期に検出し，信頼性を向上させようとする立場で，生産ラインにおける方法論としては，説得力もあり，普及している．代表的な手法はエアバスなどで採用されている Two-Version プログラミングや，モジュールの終了時に受け入れテストを行い，不合格時には代替モジュールを起動させるリカバリーブロックなどがある．

それぞれ，一定の有効性は認められるものの，決定的な方法論が定まらないなか，国際規格（IEC 61508）が一つの方向性を示した．要求された安全性水準に応じた作り方が，システムのライフサイクルの各フェーズでなされていることを第三者に認証してもらうことで安全性を立証しようという方法論であり，ソフトウェアの妥当性もこの範疇で扱えるようになった．産業界における今後の展開が注目される．

シングルスレッド方式に見る技術

鉄道の列車制御システムで用いられる電子連動装置は，いわゆる組込みシステムの一つである．一般に組込みシステムは，リアルタイム OS（RTOS）のもとで，様々な状況の変化に即応した処理が行われるよう，マルチタスク構成をとる．すなわち，外部イベントの変化を割込みとして取り込み，最も優先して行わねばならないタスクに切り替える（プリエンプション）ことでリアルタイム性を確保することが重視されている．

これに対し，電子連動装置のソフトウェアでは，割込みに応じたタスクの切替えを行わず，それぞれの処理を次々と実行する「シングルスレッド方式」を採用した（図 5 参照）．シングルスレッド方式では，タスクがシーケンシャルに起動される．

マルチタスク構成はリアルタイム OS（RTOS）の真髄とも言えるが，クリティカルなタイミングでのタスクのプリエンプションが思いがけないバグを誘発するというリスクを持つ．

シングルスレッド方式では各タスクの動き方が一義に定まっているので，クリティカルなタスクの切替えタイミングで発生するバグも回避できるし，タスクの誤った動きも検出が容易になる．このような思想のもと，我が国の列車制御の世界では，更に次のようにソフトウェア安全性に配慮した要件を義務づけ，実用システムを構築している．

① スレッド実行時は割込みを受け付けない
　タスクの動作中に割込みを受け付けず，一連の処理の最終タスク（スレッドの終りのタスク）が終わって，再度スレッドの先頭タスクに戻る際に，初めて割込みの有無と要因を分析し，次のスレッドで対応する処理を行う．

② 処理はサイクリックに行う
　イベント生成に応じて必要な処理を行うのではなく，シングルスレッドで繰り返し処理されるので，同じ処理がサイクリックに行われる．

③ タスク間通信には非対称な受け入れ検査を行う

④ 入力変化にも非対称診断を行なう
　入力の変化をそのまま受け入れるのでなく，安全性に配慮した妥当性診断処理を組み込む．

⑤ 入力変化の合理性診断
　入力変化に対しては，非対称診断に加え，処理上の合理性診断を行ったうえで使う．

この「ソフトウェアの安全性要件」は，マイクロエレクトロニクス指針のなかに組み込まれ，コンピュータ式信号システムの開発に利用された．我が国の鉄道信号では，国際規格 IEC 61508 などができた今日においても，ソフトウェアのアーキテクチャ要件として遵守されている．