



# 目次

日本の読者へのまえがき	v
序文	vii
著者紹介	xii
<b>第1部 リスクの性質</b> .....	<b>1</b>
<b>第1章 近代社会におけるリスク</b>	<b>3</b>
1.1 リスクに対する考え方の変化 .....	4
1.2 懸念の高まりは当然か? .....	6
1.3 産業化社会における独特なリスク要因 .....	7
1.3.1 新たなハザードの登場 .....	7
1.3.2 複雑さの増大 .....	8
1.3.3 曝露の増大 .....	9
1.3.4 エネルギー量の増大 .....	9
1.3.5 増加する手動操作の自動化 .....	10
1.3.6 集中化と規模の拡大 .....	11
1.3.7 技術的変化の加速 .....	12
1.4 どれほど安全なら十分なのか? .....	13
1.4.1 リスク便益分析とその他の分析方法 .....	14
1.4.2 トランスサイエンス (科学を超越した) 問題 .....	17
<b>第2章 コンピュータとリスク</b>	<b>21</b>
2.1 事故におけるコンピュータの役割 .....	22
2.2 ソフトウェアの神話 .....	26
2.3 ソフトウェアエンジニアリングはなぜ難しいのか? .....	32
2.4 直面している現実 .....	38

<b>第3章 事故の階層的考察</b>	<b>39</b>
3.1 因果関係の概念	39
3.2 因果関係を考える際の主観性	43
3.3 因果関係を定める際の過度の単純化	44
3.3.1 因果関係への法律的なアプローチ	45
3.3.2 ヒューマンエラー	45
3.3.3 技術的な故障	46
3.3.4 組織的要因	47
3.3.5 事故の多元的な解釈	48
3.4 因果関係への階層的アプローチ	48
<b>第4章 事故の根本原因</b>	<b>53</b>
4.1 安全文化の欠陥	53
4.1.1 自信過剰と自己満足	54
4.1.2 安全に低い優先順位を割り当てること	68
4.1.3 相反する目標への間違っ解決	69
4.2 効果的でない組織構造	73
4.2.1 責任と権限の分散	73
4.2.2 独立性の欠如と安全担当部門の低い地位	74
4.2.3 限定された情報伝達経路と貧困な情報の流れ	74
4.3 効果的でない技術活動	76
4.3.1 表面的な安全活動	76
4.3.2 有効でないリスク制御	76
4.3.3 変更に対する評価の失敗	79
4.3.4 情報の不足	81
4.4 まとめ	87
<b>第5章 ヒューマンエラーとリスク</b>	<b>89</b>
5.1 ほとんどの事故の原因は人間なのか？	90
5.2 自動化システムにおける人間の必要性	97
5.3 人間とタスクのミスマッチとしてのヒューマンエラー	99
5.3.1 スキルベースの行動	101
5.3.2 ルールベースの行動	101
5.3.3 知識ベースの行動	102
5.3.4 実験とエラーの関係	103
5.4 まとめ	104

<b>第 6 章</b>	<b>自動化システムにおける人間の役割</b>	<b>107</b>
6.1	メンタルモデル	109
6.2	監視者としての人間	111
6.3	バックアップとしての人間	118
6.4	パートナーとしての人間	121
6.5	結 論	123
<b>第 2 部</b>	<b>システム安全への序論</b>	<b>125</b>
<b>第 7 章</b>	<b>システム安全の創設</b>	<b>127</b>
7.1	第二次世界大戦以前の安全工学	127
7.2	システム理論	133
7.2.1	創発と階層	135
7.2.2	通信と制御	136
7.3	システム工学	137
7.4	システム分析	140
<b>第 8 章</b>	<b>システム安全の基本</b>	<b>141</b>
8.1	システム安全の発展の歴史	141
8.2	システム安全の基本概念	146
8.2.1	ハザード分析	148
8.2.2	安全のための設計	149
8.2.3	管 理	150
8.3	ソフトウェアのシステム安全	151
8.4	システム安全の費用と有効性	154
8.5	安全への他の手法	156
8.5.1	産業安全	156
8.5.2	信頼性工学	157
<b>第 3 部</b>	<b>定義とモデル</b>	<b>163</b>
<b>第 9 章</b>	<b>用 語</b>	<b>165</b>
9.1	故障とエラー	166
9.2	事故とインシデント	169
9.3	ハザード	170
9.4	リスク	173

9.5	安全	175
9.6	安全性とセキュリティ	176
9.7	まとめ	177
<b>第10章</b>	<b>事故とヒューマンエラーモデル</b>	<b>179</b>
10.1	事故モデル	180
10.1.1	基本的なエネルギーモデル	180
10.1.2	ドミノモデルと単一事象モデル	182
10.1.3	事象連鎖モデル	187
10.1.4	システム理論に基づくモデル	195
10.2	ヒューマンタスクとエラーモデル	197
10.2.1	タスクと環境モデル	198
10.2.2	認知メカニズムに基づくモデル	200
10.2.3	社会心理学モデル	216
10.3	まとめ	216
<b>第4部</b>	<b>セーフウェアプログラムの要素</b>	<b>217</b>
<b>第11章</b>	<b>安全を管理すること</b>	<b>219</b>
11.1	一般経営者の役割	220
11.1.1	安全方針の設定と目標の定義	221
11.1.2	責任、説明責任、および権限	222
11.1.3	情報伝達経路の確立	223
11.1.4	システム安全組織の設立	223
11.2	組織構造における安全部門の位置付け	226
11.3	文書類	230
11.3.1	計画	230
11.3.2	安全情報システム	233
11.3.3	安全報告	237
<b>第12章</b>	<b>システムとソフトウェア安全プロセス</b>	<b>241</b>
12.1	一般的なタスク	242
12.1.1	概念開発タスク	242
12.1.2	システム設計タスク	246
12.1.3	本格的な開発タスク	248
12.1.4	システムの開発および展開タスク	250
12.1.5	システム運用タスク	251

12.2 事例	252
12.2.1 地下鉄道駅	252
12.2.2 軍用兵器システム	258
12.2.3 NASAのスペースシャトル計画	266

## 第13章 ハザード分析 277

13.1 ハザード分析プロセス	279
13.1.1 ハザード分析の目標	279
13.1.2 定性分析と定量分析	280
13.1.3 分析者の役割と資格	281
13.1.4 効果的なハザード分析プロセスの一般的な機能	282
13.1.5 ハザード分析プロセスのステップ	283
13.1.6 ハザードの識別	284
13.1.7 ハザードの原因分析	290
13.1.8 リスクアセスメントと許容分析	291
13.2 システムモデルの種類	294
13.3 分析の一般的な種類	295
13.3.1 順方向探索と逆方向探索	296
13.3.2 トップダウン探索とボトムアップ探索	297
13.3.3 組み合わせた探索	298
13.4 ハザード分析の限界と批判	298

## 第14章 ハザード分析モデルと技法 301

14.1 チェックリスト	302
14.2 ハザード指数	303
14.3 フォールトツリー解析 (FTA)	305
14.4 MORT解析	313
14.5 イベントツリー解析 (ETA)	314
14.6 原因結果解析 (CCA)	319
14.7 HAZOP	322
14.8 インタフェース分析	327
14.9 故障モード影響解析 (FMEA)	328
14.10 故障モード、影響、および致命度解析 (FMECA)	330
14.11 障害ハザード分析	332
14.12 状態機械ハザード分析	333
14.13 タスクとヒューマンエラーの分析技法	336
14.13.1 定性的技法	336

14.13.2 定量的技法 .....	337
14.14 ハザード分析技法の評価 .....	343
14.15 結 論 .....	344
<b>第 15 章 ソフトウェアハザードと要求分析</b> .....	<b>345</b>
15.1 プロセスの考慮事項 .....	346
15.2 要求仕様の構成要素 .....	348
15.3 要求仕様の完全性 .....	348
15.4 要求分析のための完全性基準 .....	350
15.4.1 人間とコンピュータのインタフェースの基準 .....	352
15.4.2 状態の完全性 .....	353
15.4.3 入出力変数の完全性 .....	356
15.4.4 トリガー事象の完全性 .....	357
15.4.5 出力仕様の完全性 .....	365
15.4.6 トリガー事象への出力の関係 .....	371
15.4.7 状態間遷移の仕様 .....	372
15.5 制約事項分析 .....	376
15.6 仕様と基準とのチェック .....	378
<b>第 16 章 安全性のための設計</b> .....	<b>379</b>
16.1 設計プロセス .....	381
16.1.1 規格、実施規定、およびチェックリスト .....	381
16.1.2 ハザード分析によって導かれる設計 .....	383
16.2 設計技法と優先順位の種類 .....	384
16.3 ハザードの除去 .....	387
16.3.1 置換 .....	387
16.3.2 単純化 .....	389
16.3.3 分離 .....	394
16.3.4 特定のヒューマンエラーの除去 .....	396
16.3.5 ハザードをもたらす物質または条件の低減 .....	397
16.4 ハザードの低減 .....	398
16.4.1 制御性のための設計 .....	399
16.4.2 防護壁 .....	405
16.4.3 故障の最小化 .....	414
16.5 ハザード制御 .....	422
16.5.1 曝露の制限 .....	423
16.5.2 隔離と封じ込め .....	423

16.5.3 防護システムとフェイルセーフ設計 .....	424
16.6 損害の低減 .....	428
16.7 設計の修正と保守 .....	428
<b>第 17 章 ヒューマンマシンインタフェースの設計</b> .....	<b>431</b>
17.1 一般的なプロセスの検討 .....	433
17.2 人間の特性への仕事の適合 .....	436
17.2.1 用心深さの欠如との闘い .....	437
17.2.2 エラー耐性のための設計 .....	438
17.2.3 仕事の割り当て .....	442
17.3 セーフティクリティカルなヒューマンエラーの低減 .....	445
17.4 適切な情報とフィードバックの提供 .....	447
17.4.1 提示すべき情報 .....	448
17.4.2 情報提示の方法 .....	458
17.5 訓練スキルと保守スキル .....	465
17.5.1 オペレータへの安全特性の指導 .....	465
17.5.2 緊急事態に備えた訓練 .....	465
17.5.3 シミュレータ .....	467
17.6 安全な HMI 設計のための指針 .....	468
<b>第 18 章 安全性の検証</b> .....	<b>473</b>
18.1 動的分析 .....	476
18.1.1 プロセスの考慮事項 .....	476
18.1.2 試験の限界 .....	478
18.2 静的分析 .....	479
18.2.1 形式検証 .....	480
18.2.2 ソフトウェアフォールトツリー解析 (SFTA) .....	481
18.3 独立した検証と妥当性確認 .....	491
18.4 結 論 .....	492
<b>エピローグ：これからの展望</b> .....	<b>493</b>
<b>付 録</b> .....	<b>497</b>
<b>付録 A 医療機器：Therac-25 の歴史</b> .....	<b>499</b>
A.1 はじめに .....	499
A.2 背 景 .....	499
A.3 事 象 .....	504



A.3.1	1985年6月、ケネストーン地域腫瘍センター	504
A.3.2	1985年7月、オンタリオがん基金	505
A.3.3	1985年12月、ヤキマバレー記念病院	507
A.3.4	1986年3月、東テキサスがんセンター	508
A.3.5	1986年4月、東テキサスがんセンター	510
A.3.6	1987年1月、ヤキマバレー記念病院	519
A.4	原因因子	526
<b>付録B</b>	<b>航空宇宙：アポロ13号、DC-10型機、およびチャレンジャー号</b>	<b>531</b>
B.1	民間航空産業界における安全への取り組み	531
B.2	アポロ13号	533
B.2.1	背景	533
B.2.2	事象	534
B.2.3	原因因子	537
B.3	DC-10型機の貨物扉の物語	537
B.3.1	背景	537
B.3.2	事象	537
B.3.3	原因因子	541
B.4	スペースシャトル・チャレンジャー号事故	541
B.4.1	背景	541
B.4.2	事象	543
B.4.3	原因因子	548
<b>付録C</b>	<b>化学産業：セベソ、フリックスボロー、ボパール</b>	<b>551</b>
C.1	化学プロセス産業における安全性	551
C.2	セベソ	553
C.2.1	背景	553
C.2.2	安全機能	554
C.2.3	事象	555
C.2.4	原因因子	557
C.3	フリックスボロー	558
C.3.1	背景	558
C.3.2	事象	559
C.3.3	原因因子	561
C.4	ボパール	563
C.4.1	背景	563
C.4.2	安全機能	564

C.4.3 事象 .....	564
C.4.4 原因因子 .....	568
<b>付録D 原子炉事故：ウィンズケール、スリーマイル島、およびチェルノブイリ</b>	<b>571</b>
D.1 背景 .....	571
D.1.1 原子力発電所の原理 .....	571
D.1.2 安全性の特徴 .....	574
D.2 ウィンズケール原子炉事故 .....	576
D.2.1 背景 .....	576
D.2.2 事象 .....	577
D.2.3 事故の原因因子 .....	578
D.3 スリーマイル島原子炉事故 .....	578
D.3.1 背景 .....	578
D.3.2 事象 .....	582
D.3.3 事故の原因因子 .....	586
D.4 チェルノブイリ原子炉事故 .....	593
D.4.1 背景 .....	593
D.4.2 事象 .....	595
D.4.3 レベル2の原因（事故の条件） .....	597
D.4.4 レベル3の原因（事故の根本原因） .....	598
<b>参考文献</b>	<b>601</b>
<b>著作権表示</b>	<b>621</b>
<b>索引</b>	<b>625</b>
<b>訳者あとがき</b>	<b>629</b>