

ディペンダビリティ保証入門

ー安全分析・MBSE・アシュアランスケースによる統合アプローチー

松野 裕・高井利憲・岡本圭史

【共著】

コロナ社

ま え が き

本書は、複雑化・高度化する現代のシステムの安全性と信頼性を保証するための手法を体系的に解説しています。

自動運転システムをはじめとする現代のシステムは、ソフトウェアとハードウェアが密接に連携し、外部環境とつねに相互作用するオープンシステムです。このようなシステムの安全性を確保することは、従来のシステム以上に困難な課題となっています。本書では、この課題に対応するための手法として、安全・セキュリティ分析、モデルベースシステムズエンジニアリング (MBSE)、そしてアシュアランスケースを統合的に解説します。本書では、開発と運用のライフサイクル全体を通じてディペンダビリティを継続的に保証するための枠組みとして「継続的ディペンダビリティ保証モデル」を提示し、このモデルを中心に各手法を体系的に位置づけています。

本書の構成は以下のとおりです。まず1章でディペンダビリティ（総合信頼性）の基礎概念と ISO 26262 や ISO/SAE 21434 などの関連する国際規格を紹介します。2章では従来の安全分析手法である FTA と FMEA、およびセキュリティ分析への応用を解説し、3章では MIT で開発された新しい安全分析手法 STAMP/STPA を紹介します。4章では MBSE によるシステム設計手法を、5章では GSN 記法を用いたアシュアランスケースと D-Case 手法による合意形成を解説します。そして6章では、L4 自動駐車システム (L4 CPP) を題材に、これらの手法を統合的に適用する総合演習を行います。7章では、本書全体のまとめとして各手法の位置づけと使い分け、安全性とセキュリティの統合、今後の展望について述べます。

本書が扱う内容は、まだ大学の教育課程に十分に組み込まれていませんが、自動車産業をはじめとする安全性が重要な分野では必須の内容です。本書を通じ

て、これらの手法を習得し、安全で信頼性の高いシステムの開発に役立てていただければ幸いです。

本書の内容の多くは、2006年に開始されたJST CREST研究領域「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」(DEOSプロジェクト, 研究総括: 所真理雄先生)に端を発しています。DEOSプロジェクトでは、変化し続けるオープンシステムのディペンダビリティをいかに確保するかという課題に取り組み、オープンシステムディペンダビリティ (OSD) の概念、DEOSプロセスとアーキテクチャ、そしてアシュアランスケースによるステークホルダー間の合意形成手法であるD-Caseが生み出されました。これらの成果は、2018年に国際規格IEC 62853: Open systems dependabilityとして結実しています。

著者らは2009年頃よりこのプロジェクトに参加し、D-Caseの研究を通じてディペンダビリティ保証の考え方を深めてきました。本書で提示した継続的ディペンダビリティ保証モデルも、DEOSプロジェクトで培われた知見を基盤としています。DEOSプロジェクトの関係者の皆様に深く感謝いたします。

2026年7月

松野 裕, 高井利憲, 岡本圭史

執筆分担

松野 裕	1, 2, 5, 6, 7 章
高井利憲	4, 6 章
岡本圭史	3 章

目 次

1. ディペンダビリティの基礎

1.1 システムのディペンダビリティ：基礎概念と現代的課題	1
1.1.1 システムとはなにか	1
1.1.2 ディペンダビリティの概念	2
1.2 ディペンダビリティの体系と用語	3
1.2.1 ディペンダビリティ属性	4
1.2.2 ディペンダビリティへの脅威	5
1.2.3 ディペンダビリティへの脅威に対処する手段	5
1.2.4 関連する国際規格	7
1.3 現代のシステムとディペンダビリティの課題	8
1.3.1 システムの複雑化と近年のインシデント	8
1.3.2 本書のアプローチ：継続的ディペンダビリティ保証モデル	11
1.4 本書の構成と各章の関係	12
1.4.1 各章の概要	13
1.4.2 手法間の関係	13
引用・参考文献	14

2. 安全分析の基本手法：FTA と FMEA

2.1 FTA と FMEA の概要	17
2.2 FTA	19
2.2.1 FTA の概要と目的	19
2.2.2 FT 図の作成と定量的解析	21

2.2.3	FT 図で定性的に解析する	27
2.2.4	FTA 実施上の留意点	29
2.2.5	身の回りの事象の FT 図	29
2.3	FMEA	30
2.3.1	実施のタイミングと目的	31
2.3.2	FMEA での主要なプロセス	32
2.3.3	設計 FMEA の効果的な実施	33
2.3.4	故障モードの抽出法	36
2.3.5	評価結果の判断について	37
2.3.6	新しい FMEA 手法：AIAG-VDA FMEA	38
2.3.7	FMEA の実践例：設計 FMEA	39
2.4	ソフトウェアへの FTA・FMEA の適用	40
2.4.1	ソフトウェアへの適用における課題	41
2.4.2	ソフトウェア FTA の実践	41
2.4.3	ソフトウェア FMEA の実践	41
2.5	セキュリティ分析への応用	42
2.5.1	Attack tree	42
2.5.2	TARA	42
2.6	本章のまとめ	43
引用・参考文献		44

3. 安全分析手法：STAMP/STPA

3.1	STAMPの概要	45
3.2	STPA	46
3.2.1	STPAの手順	46
3.2.2	Step 1「分析目的の定義」	47
3.2.3	Step 2「安全制御構造図のモデル化」	50
3.2.4	Step 3「非安全なコントロールアクションの識別」	53
3.2.5	Step 4「ロスシナリオの識別」	55
3.3	脅威分析手法：STPA-Sec	58

3.3.1	STPA-Sec Step 1	59
3.3.2	STPA-Sec Step 2	60
3.3.3	STPA-Sec Step 3	61
3.3.4	STPA-Sec Step 4	61
3.3.5	ウォーゲーム	63
3.4	事例：自動車への STPA の適用	66
3.4.1	Step 1「分析目的の定義（自動車規格対応）」	67
3.4.2	Step 2「安全制御構造図のモデル化（自動車規格対応）」	68
3.4.3	Step 3「非安全なコントロールアクションの識別（自動車規格対応）」	69
3.4.4	Step 4「ロスシナリオの識別（自動車規格対応）」	70
3.5	本章のまとめ	71
	引用・参考文献	72

4. モデルベースシステムズエンジニアリング (MBSE)

4.1	システムズエンジニアリングの概要	74
4.1.1	システムズエンジニアリングとは	74
4.1.2	事例で見るシステムズエンジニアリングの役割	75
4.2	MBSE	78
4.2.1	MBSE の 概 念	78
4.2.2	システムズエンジニアリングのためのモデリング言語：SysML	79
4.2.3	モデルの種類例	82
4.2.4	SysML による概念の共有	83
4.3	事例：巨大ショッピングセンターの駐車場	86
4.3.1	システムズエンジニアリング活動の計画	87
4.3.2	課 題 定 義	88
4.3.3	モデルの記述準備	89
4.3.4	モデルの記述	96
4.3.5	モデルの評価	100
4.3.6	本節のまとめ	103
	引用・参考文献	105

5. アシユアランスケースと D-Case による合意形成

5.1 はじめに	106
5.2 アシユアランスケースの概要	108
5.2.1 背景と登場の経緯	108
5.2.2 アシユアランスケースの定義と基本構造	109
5.2.3 日本国内におけるアシユアランスケース導入の動き	109
5.3 GSN によるアシユアランスケースの可視化	110
5.3.1 GSN Community Standard とは	111
5.3.2 GSN コア要素	111
5.3.3 リンク（矢印）による論証構造	113
5.3.4 GSN Community Standard における拡張と実践的ガイドライン	114
5.3.5 GSN を用いたアシユアランスケース作成の効果と留意点	115
5.3.6 本節のまとめ	116
5.4 D-Case による合意形成	116
5.4.1 D-Case の概要	116
5.4.2 D-Case ステップ	117
5.4.3 D-Case ステップの事例：テスト戦略の合意	119
5.4.4 D-Case ステップの事例：ET ロボコンへの適用	120
5.4.5 D-Case の活用ポイントと留意点	120
5.4.6 本節のまとめ	121
5.5 事例：自動運転への GSN の適用	122
5.5.1 背景：オープンシステムとしての自動運転	122
5.5.2 事例概要：塩尻市での実証実験	122
5.5.3 トップレベルのアシユアランスケース構造	123
5.5.4 ハザード分析（GSN モジュール M2）	125
5.5.5 安全距離の定義	126
5.5.6 妥当性確認の GSN（GSN モジュール M4）	126
5.5.7 モニタリングシステムとの連携	128
5.5.8 本事例から得られた知見	129

5.6 D-Case を用いた合意形成の評価手法	131
5.6.1 背景：ステークホルダーとの合意形成の課題	131
5.6.2 事例概要：TIER IV によるレベル 4 実証実験	131
5.6.3 合意形成プロセスの概要	132
5.6.4 GSN モデルの構造	132
5.6.5 Safety status report（安全性現状報告書）	133
5.6.6 アンケートによる合意度評価	134
5.6.7 Consensus score（合意度スコア）	135
5.6.8 従来の CAM との比較	137
5.6.9 本事例から得られた知見	137
5.7 本章のまとめ	138
引用・参考文献	141

6. 総合演習：自動運転システムの安全性分析と保証

6.1 演習の概要	143
6.1.1 対象システム	143
6.1.2 想定シナリオ	143
6.1.3 システム構成要素	144
6.1.4 演習の全体像	144
6.1.5 関連する国際規格	145
6.1.6 手法間の受け渡し対応表	145
6.2 総合演習 1：従来手法（FTA・FMEA）による安全分析	146
6.2.1 FTA によるハザード分析	146
6.2.2 FMEA による故障モード分析	147
6.2.3 従来手法の限界についての考察	147
6.3 総合演習 2：STAMP/STPA による安全分析	148
6.3.1 ロス・ハザード・安全制約の識別	148
6.3.2 安全制御構造図の作成	148
6.3.3 UCA の識別	148
6.3.4 ロスシナリオの識別	148

6.3.5	FTA・FMEA との比較	149
6.4	総合演習 3：セキュリティ分析	149
6.4.1	Attack tree による脅威分析	149
6.4.2	TARA (ISO/SAE 21434 準拠)	149
6.4.3	安全性・セキュリティ統合分析	150
6.5	総合演習 4：MBSE によるアーキテクチャ記述	150
6.5.1	ステークホルダーと関心事の識別	150
6.5.2	ビューポイントとビューの定義	150
6.5.3	オントロジーの定義	151
6.5.4	ビューの記述	151
6.6	総合演習 5：アシュアランスケースによる保証	151
6.6.1	トップゴールと前提の設定	151
6.6.2	サブゴールへの分割	151
6.6.3	GSN 図の作成	152
6.6.4	D-Case 手法による合意形成	152
6.7	総合課題：レポート作成	152
6.7.1	分析結果の統合	152
6.7.2	ディペンダビリティ特性の評価	153
6.7.3	国際規格への適合性	153
6.8	本章のまとめ	153

7. まとめと今後の展望

7.1	本書の振り返り	155
7.1.1	ディペンダビリティの基礎 (1 章)	155
7.1.2	安全分析の基本手法：FTA と FMEA (2 章)	156
7.1.3	安全分析手法：STAMP/STPA (3 章)	156
7.1.4	モデルベースシステムズエンジニアリング (MBSE) (4 章)	156
7.1.5	アシュアランスケースと D-Case による合意形成 (5 章)	156
7.1.6	総合演習：自動運転システムの安全性分析と保証 (6 章)	157

7.2 各手法の位置づけと使い分け	157
7.3 安全性とセキュリティの統合	158
7.4 今後の展望	158
7.4.1 AI システムとディペンダビリティ	158
7.4.2 運用中の継続的保証	159
7.4.3 規制の動向と人材育成	159
7.5 実務への適用に向けて	159
7.6 おわりに	160
引用・参考文献	161
 付録：略語・用語集	162
A.1 略語一覧	162
A.2 関連規格	163
A.3 主要用語	163
 総合演習解答例	167
総合演習 1：従来手法（FTA・FMEA）による安全分析	167
課題 1-1 解答例：FT 図の作成	167
課題 1-2 解答例：最小カット集合の導出	167
課題 1-3 解答例：FMEA ワークシート記入例	168
課題 1-4 解答例：従来手法の限界についての考察	168
総合演習 2：STAMP/STPA による安全分析	169
課題 2-1 解答例：ロス・ハザード・安全制約の識別	169
課題 2-2 解答例：安全制御構造図のモデル化	169
課題 2-3 解答例：UCA 表の作成	169
課題 2-4 解答例：ロスシナリオの作成	169
課題 2-5 解答例：FTA・FMEA と STPA の比較考察	171
総合演習 3：セキュリティ分析	172
課題 3-1 解答例：Attack tree の作成	172
課題 3-2 解答例：脅威分析とリスク評価（TARA）	172

課題 3-3 解答例：安全性・セキュリティ統合分析の考察	173
総合演習 4：MBSE によるアーキテクチャ記述	173
課題 4-1 解答例：ステークホルダー分析	173
課題 4-2 解答例：ビューポイントとビューの定義	174
課題 4-3 解答例：オントロジーの作成	175
課題 4-4 解答例：ビューの記述	175
総合演習 5：アシュアランスケースによる保証	177
課題 5-1 解答例：トップゴールの設定	177
課題 5-2 解答例：分割戦略の選択	177
課題 5-3 解答例：GSN 図の作成	177
課題 5-4 解答例：ステークホルダー間の合意形成	177
総合課題：レポート作成	178
総合課題 1 解答例（要約）：総合レポート	178
総合課題 2 解答例（要約）：ディペンダビリティ特性の評価	179
総合課題 3 解答例（要約）：国際規格への適合性	179
索引	180

1

ディペンダビリティの基礎

【この章で学ぶこと】

- ディペンダビリティの基本概念と五つの属性（可用性・信頼性・安全性・完全性・保全性）
- 欠陥・エラー・障害の因果連鎖
- ISO 26262, ISO/SAE 21434 などの関連規格の概要
- 本書で扱う五つの手法の全体像と各章の関係

1.1 システムのディペンダビリティ：基礎概念と現代的課題

1.1.1 システムとはなにか

私たちの日常生活において、「システム」という言葉をよく耳にします。しかし、この概念を正確に定義するのは簡単ではありません。ここでは、文献1)の定義を示します。

定義 1-1：システム (system)^{1)†}

システムとは、ほかのシステムと相互作用する実体である。ここでいうほかのシステムには、ハードウェア、ソフトウェア、人間、および自然現象を伴う物質的世界が含まれ、これらが当該システムの環境である。システム境界は、システムとその環境が接する境目である。

システムはサービスを介して相互作用を行います。文献1)のサービスの定義

[†] 肩付きの番号は、章末の引用・参考文献を示します。

を示します。

定義 1-2：サービス (service)¹⁾

システムが（提供者の役割によって）提供するサービスとは、その利用者から見える振舞いである。ここで利用者とは、提供者からサービスを受ける別のシステムである。提供者のシステム境界のうちサービス提供がなされる部分を提供者のサービスインタフェースという。

システムはつねに特定の環境に置かれており、その環境との相互作用を通じて機能します。例えば、自動車というシステムは道路という環境のなかで機能し、気象条件や交通状況などの環境要因の影響を受けます。

システムとサービス、および環境の関係を図 1.1 に示します。

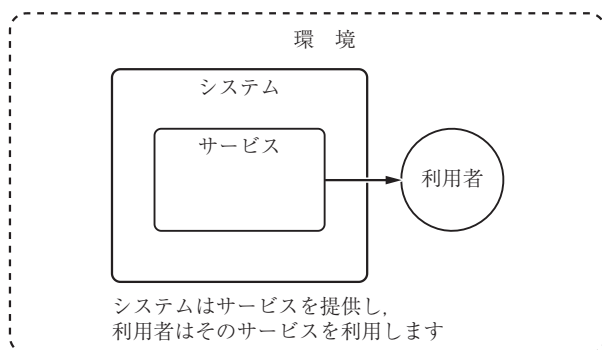


図 1.1 環境におけるシステムとサービス

上記の定義は抽象的ですが、サービスは、システムによって私たちに提供される機能や便益です。私たち利用者（ユーザー）は、このサービスを通じてシステムと関係を持ちます。例えば、スマートフォンというシステムは、通話、メッセージング、インターネット閲覧などのサービスを提供します。

1.1.2 ディペンダビリティの概念

ディペンダビリティ (dependability) は、日本語では「安心して任せられる、信頼できる」という意味です。日本産業規格として発行されている JIS Z 8115

ディペンダビリティ（総合信頼性）用語では、ディペンダビリティには「総合信頼性」の訳があてられています。本書では「ディペンダビリティ」を用います。

ディペンダビリティの定義を二つ示します。

定義 1-3：ディペンダビリティ

- 容認できる以上の頻度と深刻さのサービス障害を防ぐシステムの能力¹⁾
- アイテムが、要求されたときに、その要求どおりに遂行するための能力^{2), 3)}

ディペンダビリティは従来、可用性や信頼性などの非機能要求を総合した概念として扱われてきました。また、ディペンダビリティの起源はシステム間の信頼関係にあり、サービス障害を防ぐことを重視しています。

可用性や信頼性は、システムがディペンダブルであるために必要な非機能要求です。ただし、システムは環境に置かれ、利用者によってサービスが使用されるため、必要となる機能や非機能要求は環境や利用者によって異なります。また、システムに障害が発生した場合には、すみやかに復旧を行い、サービスを継続しなければなりません。

以上をまとめると、システムがディペンダブルであるためには、以下の条件を満たす必要があります：

- ある環境において利用者などが望む性質をもち続けること
- サービスを継続的に提供すること

これらを満たすためには、システムがその性質を失った場合（つまり、ディペンダブルでなくなった場合）には、すみやかに復旧を行い、サービスを継続する能力も求められます。

1.2 ディペンダビリティの体系と用語

ディペンダビリティの概念は、1980年代から国際的な研究グループ（IFIP WG 10.4 “Dependable Computing and Fault Tolerance” など）によって体

系化され、用語の整理が行われてきました。「耐故障性」研究から発展し、近年ではセキュリティの概念も含めて議論されています。

本節では、Avizienis らによる体系¹⁾に基づいて、ディペンダビリティの主要な概念を紹介します。

1.2.1 ディペンダビリティ属性

ディペンダビリティ属性は、システムがディペンダブルであるためにもつべき特性を表します。おもな属性には以下のものがあります：

- 可用性 (availability)：正しいサービスの即応性
- 信頼性 (reliability)：正しいサービスの継続性
- 安全性 (safety)：利用者と環境に壊滅的な結果をもたらないこと
- 完全性 (integrity)：不適切なシステム変更がないこと
- 保全性 (maintainability)：変更と修理を受け入れられること

近年では、これらに加えてレジリエンス (resilience) が重要な概念として注目されています。レジリエンスとは、予期しない障害や変化に対して、システムが適応し、回復する能力を指します。従来のディペンダビリティが「障害を防ぐ」ことに重点を置いていたのに対し、レジリエンスは「障害は起こりうる」という前提のもと、いかに迅速に回復し、サービスを継続するかを重視します。

これらの属性は相互に関連しており、時には相反する関係にあることもあります。システム設計者は、対象システムの要求に応じてこれらの属性のバランスをとる必要があります。ディペンダビリティ研究では文献1) などによって、セキュリティの概念との関係が議論されてきました。これらの属性に加え、秘匿性 (confidentiality) をセキュリティの属性とすることにより、図 1.2 のディ

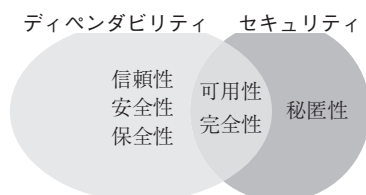


図 1.2 ディペンダビリティとセキュリティの関係

ペンダビリティとセキュリティの関係が定義されます。

1.2.2 ディペンダビリティへの脅威

システムのディペンダビリティを脅かす要因は、以下の三つの概念で整理されています：

- 欠陥 (fault)：エラーの原因となるとみなされる、あるいは推定される「もの」や「こと」
 - － 例：プログラミングミス、設計上の誤り、ハードウェアの製造欠陥など
- エラー (error)：障害が起こりうるシステムの状態。ただし、エラー状態になったからといって、必ずしも障害が起こるとは限らない
 - － 例：メモリのビット反転、不正な計算結果の生成、誤った状態遷移など
- 障害 (failure)：サービスが正しいサービスから逸脱する出来事。ユーザーが実際に不具合を観測する段階
 - － 例：システムクラッシュ、誤った結果の出力、応答停止など

欠陥、エラー、障害の関係は図 1.3 のように図示されます。

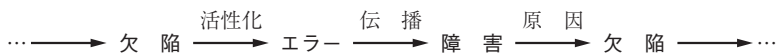


図 1.3 欠陥、エラー、障害の関係

1.2.3 ディペンダビリティへの脅威に対処する手段

ディペンダビリティへの脅威に対処するためには、欠陥、エラー、障害のそれぞれの段階で適切に対策を講じる必要があります。代表的な四つの手段として、以下が提案されています：

- 欠陥防止 (fault prevention)：開発や運用プロセスにおいて、そもそも欠陥を組み込まないようにする手段。適切な設計手法やレビュー、テスト手法の導入、および開発工程の標準化・自動化などによって、欠陥の導入を最小限に抑え、また発生しにくい仕組みを整備します。

索引

【あ】	継続的ディペンダビリティ	ステレオタイプ	83
アシュアランスケース	保証モデル 11, 155, 164	ストラテジ (GSN)	112
107, 109, 151, 157, 163	欠陥 5, 155, 164	【せ】	
安全機能 151	欠陥除去 6	正当化 (GSN)	112
安全性 4, 19, 153, 155, 164	欠陥防止 5	説明責任の達成	10
安全制御構造 46, 148, 164	欠陥予測 6	【そ】	
安全制約	【こ】	相互運用システム	77
45, 49, 151, 156, 164	合意度スコア 136	ソリューション (GSN)	112
【い】	構造重要度 28, 164	【た】	
イネープリングシステム 77	故障モード 30, 32, 158, 164	耐故障性	6
【う】	ゴール (GSN)	対象システム	76
ウォーゲーム 63	コンテキスト (GSN)	【て】	
【え】	コントローラ 51	ディペンダビリティ	
影響解析 30, 33	コントロールアクション	2, 3, 153, 155, 165	
エラー 5, 155, 164	51, 148	【と】	
【お】	コントロールアルゴリズム	統一アーキテクチャ	
オントロジー 83, 151, 156	51	フレームワーク 89, 165	
【か】	【さ】	トップ事象 18, 165	
ガイドワード 36, 164	最小カット集合	トップダウン 19, 156, 165	
仮定 (GSN) 112	27, 147, 164	【は】	
可用性 4, 153, 155, 164	サービス 2	ハザード 48, 148, 165	
完全性 4, 153, 155, 164	【し】	【ひ】	
【き】	システム 1	非安全なコントロール	
基本事象 20	システムズエンジニアリング	アクション 53, 165	
【け】	74, 77	被コントロール・	
継続的アシュアランス 122	システム保証 10, 107	プロセス 51	
	障害 5, 155, 164	非展開事象 20	
	信頼性 4, 19, 153, 155, 164	ビュー 89, 150, 156	
	【す】		
	ステークホルダー		
	10, 150, 155, 164		

—— 著 者 略 歴 ——

松野 裕（まつの ゆたか）

2001年 東京大学工学部電子工学科卒業
2003年 東京大学大学院新領域創成科学研究科
修士課程修了（基盤情報学専攻）
2006年 東京大学大学院新領域創成科学研究科
博士後期課程修了（基盤情報学専攻）
博士（科学）
2006年 東北大学産学官連携研究員
2008年 東北大学大学院教育研究支援者
産業技術総合研究所産総研特別研究員
2010年 東京大学特任講師
2012年 名古屋大学特任講師
2013年 電気通信大学大学院助教
2015年 日本大学准教授
2023年 日本大学教授
現在に至る

高井 利憲（たかい としのり）

1994年 豊田工業高等専門学校情報工学科卒業
1996年 九州工業大学情報工学部知能情報工学科卒業
1998年 奈良先端科学技術大学院大学情報科学研究科博士前期課程修了（情報処理学専攻）
2001年 奈良先端科学技術大学院大学情報科学研究科博士後期課程単位取得認定退学（情報処理学専攻）
2002年 博士（工学）（奈良先端科学技術大学院大学）
2001年 産業技術総合研究所テクニカルスタッフ
2012年 奈良先端科学技術大学院大学特任助教
2014年 奈良先端科学技術大学院大学特任准教授
2016年 株式会社チェンジビジョンチーフエンジニア
2026年 武庫川女子大学教授
現在に至る

岡本 圭史（おかもと けいし）

1991年 早稲田大学理工学部数学科卒業
1993年 早稲田大学大学院理工学研究科修士課程修了（数学専攻）
1998年 早稲田大学大学院理工学研究科博士課程退学（数学専攻）
2000年 東京女子大学非常勤講師
2002年 湘北短期大学非常勤講師
2003年 横浜国立大学非常勤講師
2004年 産業技術総合研究所招聘研究員
2008年 博士（理学）（早稲田大学）
2011年 仙台高等専門学校准教授
2018年 仙台高等専門学校教授
現在に至る

ディペンダビリティ保証入門

— 安全分析・MBSE・アシュアランスケースによる統合アプローチ —

Introduction to Dependability Assurance

—An Integrated Approach with Safety Analysis, MBSE, and Assurance Cases—

© Yutaka Matsuno, Toshinori Takai, Keishi Okamoto 2026

2026 年 9 月 25 日 初版第 1 刷発行



検印省略

著 者 松 野 裕
高 井 利 憲
岡 本 圭 史
発 行 者 株式会社 コ ロ ナ 社
代 表 者 牛 来 真 也
印 刷 所 三 美 印 刷 株 式 会 社
製 本 所 有限会社 愛 千 製 本 所

112-0011 東京都文京区千石 4-46-10

発 行 所 株式会社 コ ロ ナ 社
CORONA PUBLISHING CO., LTD.

Tokyo Japan

振替 00140-8-14844・電話(03)3941-3131(代)

ホームページ <https://www.coronasha.co.jp>

ISBN 978-4-339-02959-8 C3055 Printed in Japan

(田中)



JCOPY <出版者著作権管理機構 委託出版物>

本書の無断複製は著作権法上での例外を除き禁じられています。複製される場合は、そのつど事前に、出版者著作権管理機構（電話 03-5244-5088, FAX 03-5244-5089, e-mail: info@jcopy.or.jp）の許諾を得てください。

本書のコピー、スキャン、デジタル化等の無断複製・転載は著作権法上での例外を除き禁じられています。購入者以外の第三者による本書の電子データ化及び電子書籍化は、いかなる場合も認めていません。落丁・乱丁はお取替えいたします。