セーフティ&セキュリティ入門

AI、IoT時代のシステム安全

日科技連 SQiP 研究会
セーフティ&セキュリティ分科会 編
金子 朋子 著

日科技連

まえがき

安全安心はいつの時代も社会の最優先事項である。現在、異なる製品やサービスがインターネットを通じてつながり、新たなサービスや価値が提供されるIoT（Internet of Things）が実現しつつある。また、社会のさまざまな仕組みのコントールに深層学習に代表される高度化した人工知能（AI：Artificial Intelligence）の実用化が急速に進んできている。

このようなAI、IoT時代に、安全安心が確保されたシステム構築へのニーズはいやが上にも増している。セーフティとは「偶発的なミス、故障などの悪意のない危険に対する安全」を示す。一方、セキュリティとは「悪意をもって行われる脅威に対しての安全」まで確保することをさす。したがってセキュリティによる安全は、気がかりのない「安心」をもたらすとも捉えられる。筆者は「システム思考」と「レジリエンス・エンジニアリング」などのシステム安全理論と技術の普及展開に取り組んできた。また、セーフティやセキュリティ技術をばらばらに取り扱うのではなく、統合的に組み合わせて、安全安心なシステムを構築するための開発方法論を長年、研究してきた。

「システム思考」とは現代の環境問題などのように複雑なメカニズムが互いに絡み合っているときに全体から関係性を捉える重要な思考方法である。最近、「レオナルド・ダ・ビンチが万能の天才になれたのは、システム思考によって、異なる知識を結びつける能力があったからではないか」と最新AIが天才の謎を明かしたことで「システム思考」が注目された。つまり、システム思考は、広汎な事象に対して普遍的な意味を関係性から捉える方法である。

また「レジリエンス・エンジニアリング」はレジリエンス（＝回復力、復元力、弾力性）を工学的に扱う研究である。2020年、野口聡一宇宙飛行士を乗せた米国民間宇宙船が打上げに成功した。宇宙船の名前は日本語で「困難な状況から立ち直る力」などを意味するレジリエンスと名づけられた。サイバーセキュリティにおいても、攻撃に対して、レジリエントに対応することが求められている。

本書は、最近、大変注目されてきているこの「システム思考」と「レジリエンス・エンジニアリング」をセーフティとセキュリティ双方に適用してきた筆者の研究成果を紹介するものである。ただし、難解な解説ではなく、多角的な専門家の解説や詳細な事例分析を含んだセーフティ・セキュリティ技術、方法論の入門解説書として、技術者が利用できるように、できる限りわかりやすく、体系的に示そうとするものである。

また、日本科学技術連盟ソフトウェア品質管理研究会（SQiP研究会）で筆者が主査を務める「セーフティ＆セキュリティ」分科会において取り組んできた演習実践的な学習内容をなるべく、具体的な紙上に再現することを意図している。

本分科会は2017年4月に筆者がセーフティとセキュリティとの統合実践的研究を志し、企画立案し、「セーフティ＆セキュリティ」をテーマにした日本で最初の技術者向けの演習コースとして発足した。当初は髙橋雄志副主査、勅使河原可海アドバイザーの体制であった。2018年からは佐々木良一アドバイザーに代わり、2020年から研究コースになったが今日まで一貫してセーフティとセキュリティの技術の実践と研究に取り組んでいる。本コースでは、セキュリティの研究者であり企業でのITシステム構築の実践者でもある筆者が、IoT時代に重要であるフィジカルなシステムと人間との安全を中心に発展してきたセーフティとの統合をいかに実現すべきかを講義と演習を通して指導した。また、トラスト、プライバシー、セキュア通信など関連分野の研究者や航空宇宙などの最先端安全性を実現してきた技術者などの専門家による講義を提供してきた。さらに、本コースは企業から集まったメンバーとともに探求してきた研究の実践の場でもあった。

本書ではこれらの取組みをできる限りSTAMP（System Theoretic Accident Model and Processes）、FRAM（Functional Resonance Analysis Method）、GSN（Goal Structuring Notation）などのセーフティ技術やコモンクライテリアなどセキュリティ標準の概論や筆者の研究であるセーフティ・セキュリティの統合手法STAMP S&Sや開発方法論CC-Caseを記述し、前述の専門家の講義の要旨をコラムで伝え、年度ごとのメンバーの先進的な研究内容を事例として、解説する。

本書のテーマは「セーフティとセキュリティの統合的エンジニアリング」である。

第1章では、セーフティとセキュリティの理論、分析技術、標準・ガイドラインの概要と、セーフティ・セキュリティの統合分析手法、STAMP S&Sの要旨を解説する。

第2章では、新しいセーフティの2大理論の1つであるシステム理論にもとづく事故モデルSTAMPと、ハザード分析手法STPA、事故分析手法CASTとそのセキュリティ応用について、具体的な事例で解説する。

第3章ではセーフティのもう1つの理論であるレジリエンス・エンジニアリングについて解説し、機能共鳴分析手法FRAMの具体的な事例を紹介する。

第4章では、「セキュリティ・バイ・デザイン」の概念を解説したうえで、セキュリティ技術について解説する。現実にセキュリティにかかわる課題にどのように対処してきたのかについても紹介する。

第5章では、ITセキュリティ標準であるコモンクライテリア(CC)とセーフティ検証・妥当性確認に用いられるアシュアランスケースを中心に、標準とアシュアランスについて解説する。また、本書で取り上げるセーフティとセキュリティの技術要素を統合的に用いる開発方法論であるCC-Caseについて説明する。

第6章では、さまざまなものがつながるIoTの安全安心を実現するために、アシュアランスケースと重要なIoT高信頼化機能について、説明する。さらにIoTセキュリティに対してアシュアランスケースを用いて妥当性確認をする事例を紹介する。

第7章では、機械学習を含んだシステムの安全性の課題を提示する。また、AIとセキュリティの現状について、概説する。

「安全安心が重要だ」とことあるごとに人は言うが、本書が「コンピュータシステムの開発から見た安全安心はどのようなものか」について考えていただくきっかけになれば幸いである。

2021年9月

金子 朋子

セーフティ&セキュリティ入門
AI、IoT時代のシステム安全

目　次

まえがき……iii

第1章　セーフティ&セキュリティ概説……1

1.1　セーフティ……1
1.2　セキュリティ……12
1.3　セーフティとセキュリティ……15
1.4　セーフティとセキュリティの統合……22
Column 1　ネットワークセキュリティの CIA……32

第2章　システム理論とSTAMP……35

2.1　システム理論……35
2.2　システム理論にもとづく事故モデル STAMP……45
2.3　ハザード分析手法 STPA……52
2.4　CAST の概要と手順……64
2.5　CAST のセキュリティインシデント分析への応用……81
Column 2　デジタルフォレンジック……89

第3章 レジリエンス・エンジニアリングとFRAM……91

3.1　レジリエンスとレジリエンス・エンジニアリング……91

3.2　機能共鳴分析手法 FRAM……93

3.3　セキュリティ・レジリエンス……100

Column 3　トラスト……112

第4章 セキュリティ・バイ・デザイン……113

4.1　セキュリティ・バイ・デザインの定義……113

4.2　セキュリティ開発プロセス……116

4.3　セーフティを守れるセキュリティ……125

Column 4　ロジックツリーの応用としての GSN……128

第5章 ITセキュリティ標準コモンクライテリアとCC-Case……131

5.1　システムの保証とは？……131

5.2　IT セキュリティ標準コモンクライテリア（CC）……132

5.3　要求と保証の開発方法論 CC-Case……137

5.4　CC-Case の要求と保証の手順……143

Column 5　個人情報とプライバシー……160

第6章 アシュアランスケースとIoTのセーフティとセキュリティ……163

6.1　アシュアランスケース……163

6.2　現在の IoT 開発の課題……172

6.3　IoT の特徴と求められていること・ガイドライン……173

6.4　IoT のセーフティとセキュリティ……178

Column 6　日本のエネルギー政策とスマートハウス……181

第7章 機械学習システムのセーフティとセキュリティ……183

7.1　機械学習システムの安全性……183

7.2　機械学習システムの安全性の課題……185

7.3　全体システムとしての安全性確保……189

7.4　AI とセキュリティに関する 4 つの課題……191

7.5　セーフティ＆セキュリティの今後……195

Column 7　セキュリティパターン……197

あとがき……199

参考文献……201

索　引……215

装丁・本文デザイン＝さおとめの事務所

第1章

セーフティ&セキュリティ概説

セーフティ(Safety)もセキュリティ(Security)のもどちらも「安全」を意味する。ただし、セキュリティは「安心」と捉えることも可能であり、その場合、両方で「安全安心」となる。しかし、両者の違いがわからない方も多いだろう。1.3節に詳述するが、本書では、セーフティとは「偶発的なミス、故障などの悪意のない危険に対する安全」、セキュリティとは、「悪意をもって行われる脅威に対しての安全」と定義している。

本章ではセーフティとセキュリティのそれぞれの特徴、主な技術や手法(技法)、標準を解説する。これはソフトウェア品質標準(SQuBOK V3)[1]に則したものなので、セーフティとセキュリティのそれぞれの基礎を学びたい方にも利用してほしい。表1.1にソフトウェア品質標準(SQuBOK V3)のセーフティ領域、セキュリティ領域と本書での記述個所の対応を示す。ちなみに筆者はSQuBOK V3のセーフティ・セキュリティ部分の執筆に参画してきた。なお、本書は標準のように、全体を網羅して記述するのが目的ではなく、コンピュータシステムで安全安心を実装する際、筆者が研究してきた技法をより具体的に伝えるものである。さらに本章ではテーマであるセーフティとセキュリティの統合を考えるために必要なソフトウェア工学での設計技法を解説し、5階層モデルを通じて、セーフティ&セキュリティのあるべき姿を示す。

1.1 セーフティ

1.1.1 セーフティとは?

セーフティとは、システムが、障害や危険事象が発生しても、人間の生命を損なったり、身体に害を及ぼしたり、社会に広範な悪影響を与えたりしない性質や回避できる性質、および、そもそも障害や危険事象の発生を抑制できる性質である。1.3節に詳述するが、これらを何から守るのかの観点で要約すると、

表1.1　SQuBOKと本書の構成

SQuBOKV3	本書での記述個所
4.2　KA：セーフティ	1.1　セーフティ 1.1.2　本質安全と機能安全 第2章　システム理論とSTAMP 第3章　レジリエンス・エンジニアリングとFRAM
4.2.1　S-KA：セーフティ品質の概念	1.1.1　セーフティとは？ 1.3.1　セーフティとセキュリティの概念
4.2.2　S-KA：セーフティの技法	1.1.4　セーフティの技法 第2章　システム理論とSTAMP
4.2.2　1T：セーフティ実現のためのリスク低減技法	1.1.3　ハザードとリスク 1.1.4　セーフティの技法
4.2.2.2　T：セーフティ・クリティカルシステムのテスト	1.1.4　セーフティの技法
4.2.3　S-KA：セーフティ・クリティカル・ライフサイクルモデル	1.1.5　セーフティの規格 第2章　システム理論とSTAMP
4.2.3.1　T：電気・電子・プログラマブル電子安全関係の機能安全（IEC 61508）	1.1.5　セーフティの規格
4.2.3.2　T：自動車電子制御の機能安全（ISO 26262）	1.1.5　セーフティの規格
4.2.3.3　T：医療機器ソフトウェア―ソフトウェアライフサイクルプロセス（IEC 62304）	1.1.5　セーフティの規格
4.3　KA：セキュリティ	1.2　セキュリティ 1.3.2　セーフティとセキュリティの特徴と違い
4.3.1　S-KA：セキュリティの品質の概念	5.2　ITセキュリティ標準コモンクライテリア（CC）
4.3.1.1　T：情報セキュリティの定義	1.2.2　脅威、脆弱性とリスク
4.3.2　S-KA：セキュリティの技法	1.2.3　セキュリティの技法
4.3.2.1　T：セキュリティ要求分析	4.2　セキュリティ開発プロセス 4.2.1　セキュリティ要求分析
4.3.2.2　T：セキュリティ設計	4.2.2　セキュリティ設計
4.3.2.3　T：セキュリティパターン	Column 7　セキュリティパターン
4.3.2.4　T：セキュアコーディング	4.2.3　セキュアプログラミング
4.3.2.5　T：セキュリティテスト	4.2.4　セキュリティテスト
4.3.2.6　T：脆弱性管理	1.2.2　脅威、脆弱性とリスク 4.2.5　脆弱性管理
2.10.2　S-KAリスク識別および特定	6.1　アシュアランスケース

本書でのセーフティの定義である「偶発的なミス、故障など悪意のない危険に対する安全」となる。ISO/IEC Guide 51では、セーフティを『許容不可能なリスクがないこと』[2] と定義している。ナンシー・G. レブソン（Nancy G. Leveson）は著書のSafewareで「安全（safety）とは、事故や損失がないことである。」[3] と定義している。なお、ソフトウェア製品の品質モデルを規定しているISO/IEC 25010では、リスク回避性と称して「製品またはシステムが、経済状況、人間の生活または環境に対する潜在的なリスクを緩和する度合い」[4] と定義している。

ISO/IEC Guide 51では安全という概念について以下のように述べている。

【ISO/IEC Guide 51における「安全」の概念】

- 絶対的な安全というものはあり得ず、相対的に安全であるとしかいえない。
- 安全は、リスクを許容可能なレベルまで低減させることで達成される。
- 許容可能なリスクは、諸要因によって満たされるべき要件とのバランスで決定される。したがって、許容可能なレベルは常に見直す必要がある。
- 許容可能なリスクは、リスクアセスメントによるリスク低減のプロセスを反復することによって達成させると説明している。

セーフティの概念を理解するためには、危害（harm）とハザード（hazard）という2つの概念を理解しておく必要がある。

危害とは、「システムによって人間の生命が損なわれたり、身体に害が及ぼされたり、社会に広範な悪影響が与えられること」[1] をさす。

ハザードとは、「危害を発生させる原因」[1] である。

すなわちセーフティとは、「ハザードの発生を抑制する性質、システムにハザードが起こっても危害に至らない性質、システムにハザードが起こっても危害を回避できる性質」[1] を意味する。

なお、セーフティについてはシステム全体で検討する必要がある。機器やソフトウェアは単体で悪影響を及ぼすわけではなく、システムの他の要素と複合してセーフティを損なうことが多い。またシステムの動作環境や、そのシステムを操作する人間や利用者とも相互作用している。したがって限定した視点で

セーフティを保証するのではなく、動作環境や人間も含めたシステム全体でのセーフティを保証する必要がある。

レブソンはシステム全体で相互作用による事故をモデル化し、そのモデルにもとづく原因分析とリスク分析手法と人や組織を含めたセーフティを考えることが必要だとして、システム理論にもとづく事故モデルSTAMP[5]とその各種手法やプロセスを提示している。本書ではこれらの詳細を第2章で解説する。

また、2014年頃に「安全とは受容できないリスクがないこと」とするセーフティの考え方だけでは十分な結果が得られないとして、レジリエンス(Resilience)という考え方が登場している。レジリエンス・エンジニアリングでは、「安全は変化する条件下で成功する能力である」と定義する[6]。レジリエンス・エンジニアリングについて、本書では第3章で詳細を解説する。

セーフティが要求されるシステムの開発では、セーフティを確保する技術や標準の遵守より、セーフティを最優先する組織文化が最重要である。これは、機能安全規格の標準に沿い、認証を取得しレベルに応じたセーフティを確保していても、それは時間の経過に伴う変化、運用時の想定外の使用、技術者のモラルの低下などの要因により、事故を起こしてしまうことは多いからである。これらの人や組織を含めたセーフティについては、第2章、第3章で解説し、本書の主張である人や組織と社会を含めた社会技術システムのモデル化に関しては、本章の後半に解説する。

1.1.2　本質安全と機能安全

セーフティには、本質安全(Inherent Safety)と機能安全(Functional Safety)がある。

本質安全とは、「ハザードの発生を抑制する性質」[1]のことである。対策によってリスクをなくして安全を確保することといえる。

一方、機能安全とは、「システムにハザードが起こっても危害に至らない性質や、システムにハザードが起こっても危害を回避できる性質」[1]をさす。言い換えると、機能安全とはシステムのリスクを許容できる程度以下に対策して安全を確保することであり、機能による安全対策を行うことといえる。セーフティの確保には、本質安全と機能安全の両方が必要であり、どちらか片方だけでは達成が難しい。

本質安全を高めることは、例えば、「鉄道の場合、踏切を立体交差にするこ

著者紹介

金子 朋子（かねこ ともこ）
博士（情報学）
国立情報学研究所 特任准教授
㈱NTTデータ　エグゼクティブR&Dスペシャリスト
公認情報セキュリティ監査人
日本科学技術連盟SQiP研究会　セーフティ＆セキュリティ分科会主査
電子情報通信学会知能ソフトウェア工学研究会専門委員
日本セキュリティマネジメント学会IoTリスク研究会幹事
日本ソフトウェア科学会機械学習工学研究会　機械学習システムセーフティ・セキュリティWG幹事

経歴：㈱ NTT データに1期生として入社し、システム開発や品質保証業務を長年実施。2008年より社会人大学院で学び、2014年セキュリティ要求と保証の研究で学位を取得。

2016年-2019年　㈱情報処理推進機構（IPA）に在籍出向し、システム理論（STAMP）やレジリエンスエンジニアリング（FRAM）等の安全分析技術の普及展開に従事。

2019年-現在　国立情報学研究所に在籍出向し、「AIシステムの安全性」を研究。

主な著書（共著）：『A Closer Look at Safety and Security』（Jeff M. Holder編、Nova Science pub. Inc.、2020年）、『ソフトウェア品質知識体系ガイド第3版（SQuBOK V3）』（SQuBOK策定部会編、オーム社、2020年）、『つながる世界の開発指針』の実践に向けた手引き』『STAMPガイドブック ～システム思考による安全分析～』（IPA、2019年）などがある。

月刊『潮』（潮出版社）にて、「Safety & Security～ IT博士と学ぶ デジタル社会の歩き方」（漫画：もりたゆうこ）を連載（2021年1月号より連載開始）。

セーフティ＆セキュリティ入門
AI、IoT 時代のシステム安全

2021 年 10 月 26 日　第 1 刷発行

編　者　日科技連SQiP 研究会
セーフティ&セキュリティ分科会
著　者　金子　朋子
発行人　戸羽　節文

発行所　株式会社 日科技連出版社
〒 151-0051　東京都渋谷区千駄ケ谷 5-15-5
DS ビル
電　話　出版　03-5379-1244
営業　03-5379-1238

検　印
省　略

Printed in Japan

印刷・製本　壮光舎印刷

ISBN 978-4-8171-9737-5
URL https://www.juse-p.co.jp/