ま　え　が　き

本書は安全分析、アシュアランスケース、モデルベースシステムズエンジニアリングを解説した本です。

2022 年 10 月

松野裕, 高井利憲, 岡本圭史

1 イントロダクション

この本はシステムの安全性分析および保証を解説する。近年、自動運転システムなどの人工知能を用いた複雑なシステムが実用化しつつある。しかしながらその安全性の分析や保証は従来よりも困難になりつつある。機械学習のモデルの出力

週 1 回 15 コマの授業を想定し、各コマで演習を行えるようにしている。

2 安全分析の基本手法: FTA と FMEA

3 安全分析手法STAMP/STPA

4 モデルベースシステムズエンジニアリング

5 アシュアランスケース

人工知能の研究開発は加速的に進み始めている。2022 年に登場した ChatGPT は、誰でも簡単にウエブ上で質問をすることができるチャットボットであるが、その回答の詳細さと自然さに、多くの人が驚いた。また歩行者や標識を自動認識する人工知能を持つ自動運転車は、アメリカの Waymo 社や日本の Tier4 社など、多くの企業が開発競争を繰り広げており、アメリカではすでにカリフォルニア州において自動運転タクシーが実用化されている。しかしながら、チャットボットや自動認識を行う人工知能は、100%正しい出力をするわけではない。であるにも関わらず、その圧倒的な利便性から、人工知能が組み込まれたシステムが加速的に普及していくことはより確実になってきている。そのような状況おいて、我々を取り巻くシステムが安心して利用できるものなのか、改めて社会的な合意形成が必要な時期になっている。

5.1 アシュアランスケースの記述方法

アシュアランスケースは基本的にドキュメントであり、多くの場合文書形式で記述される。近年では、アシュアランスケースの主張と議論構造、およびエビデンスのつながりをモデル化したグラフィカルな記述方法も用いられている。本著では、グラフィカルな記述方法の中で、Goal Structuring Notaion (GSN) を用いる。

GSN は主に以下のノードの種類からなる。

- ゴール (Goal)：システムに対して、議論すべき命題である。例えば「システムはディペンダブルである」とか「システムは適切な安全性をみたす」などである。
- 戦略 (Strategy): ゴールが満たされることを、サブゴールに分割して詳細化するときの議論の仕方である。例えば、「システムは安全である」というゴールに対して、現時点で識別されているハザードに対処できていることによって議論したいとき、戦略ノードとして「識別されたハザードごとに場合分け」を用いると、例えばひとつのサブゴールは「システムはハザード X に対処できる」となる。
- 前提 (Context): ゴールや戦略を議論するとき、その前提となる情報である。例えば、運用環境や、システムのスコープ、あるいは「識別されたハザードのリスト」などである。
- 未達成 (Undeveloped): ゴールを保証するための十分な議論もしくはエビデンスがないことを表す。

5.2　アシュアランスケースの例

5.3　アシュアランスケース記述ステップ

5.4　基　本　演　習

6 総合演習

7 まとめ