安全要求分析

平成 27 年度シラバス

２０１５年１月９日

国立情報学研究所

トップエスイープロジェクト

代表者　本位田　真一

1. 科目名

安全要求分析

2. 担当者

吉岡 信和、宇佐美 雅紀、田原 康之、大久保 隆夫、金子 浩之

3. 本科目の目的

近年、情報流出や不正アクセスの危険性など、情報システムのセキュリティは現代社会に多大の影響を及ぼすようになってきています。また、自動操縦機能が付いた車が現実に利用できるようになり、ソフトウェアに起因する大事故が懸念されています。しかしながら、他のハードウェア製品やインフラと比べて、情報システムの安全を高める技術はまだ十分とは言いがたいのが現状です。現代社会は、情報システムのインフラに支えられているため、情報システムに想定外の事故が起こった場合、社会に膨大な影響を及ぼす可能性があります。すなわち、情報システムが社会のリスクになってきています。そのため、安全なシステムを開発するための、体系的な方法論が必要です。

本科目では，要求分析段階におけるセキュリティやセーフティなどの安全性に関する問題の発見、および整理をする手法を学びます。安全な計算機システムを構築するためには、セキュリティ上の障害やシステム障害など様々な原因を事前に評価し、その危険性を要求の段階で除去しておく必要があります。しかし、一口に計算機システムといっても、多様な情報を扱う企業情報システムから厳密な処理を必要とする組み込みシステムまで様々な形態のシステムがあり、それゆえ、安全上の問題もおのずから多様とならざるを得ず、それぞれのシステムの特徴に合わせた分析技術が必要となります。本科目では、システムの脅威、脆弱性、利用者の悪意や誤操作、システムへの攻撃や重大事故などの脅威が発生する原因といったセキュリティやセーフティの問題を予測・発見し、その対策方針を導出するための手法を紹介し、演習を通して、安全を実現するための要求を分析、策定する方法について学びます。具体的には、まず体系的な手法として、ハザード分析手法、ユースケース・ミスユースケースとゴール・エージェント指向要求分析方法論によるセキュリティ要求・セキュリティ機能の分析・獲得方法を習得します。また、現実的なシステムに適用可能とするため、リスク管理手法や、システムの安全性評価に関する国際標準規格（ISO 26262、ISO/IEC 15408 (通称Common Criteria；CC)）を取り入れています。

4. 本科目のオリジナリティ

近年において情報システムのセキュリティや利用者に被害を及ぼさないセーフティが重要であるとの認識により、数多くのセキュリティやセーフティに関する講座・講義が開かれています。しかし、セキュリティとセーフティの両方を含む安全要求の分析・獲得手法の習得という点では、それら既存の講座・講義にはいくつかの問題点があり、安全性を高

める技術として円滑に開発現場に適用する際の妨げとなっています。本科目では、それらの問題点を解決し、開発現場において、セキュリティ、およびセーフティ（安全性）の要求・安全方針・対策機能の分析・獲得を効果的に可能としています。表１に、既存の講座・講義の問題点と、本科目における解を示します。

表 1 既存の講座・講義の問題点と、本科目における解

既存の講座・講義の問題点	本科目における解
セキュリティやセーフティ要件[1]の特徴として、分類が多岐にわたるという点がある。たとえば、潜在的脅威の種類(不正アクセス、ウィルス、意図しない使い方など)、守るべき資産(個人データやハードウェア資源など)、およびセキュリティやセーフティを高める技術(暗号化、アクセス制御、冗長化など)といった、多くの分類観点がある。しかし、既存の講座・講義では、細かく分類された項目を個別に教えるものがほとんどで、開発現場において、どの技術をどの場面で適用すればよいかの判断が難しい	個別の項目の習得に先んじて、体系的な安全要件の獲得・分析手法として、ミスユースケース手法、およびゴール・エージェント指向要求分析手法をベースとした方法論を習得し、その上で個別の技法(リスク管理手法など)を習得する。また、それら個別の技法を、ベースとなる方法論のどの場面でどのように適用するのかを、両者の対応関係を明確にしながら習得するので、開発現場において、各技術を適切な場面で容易に適用が可能である。

[1] 本シラバスでは、ユーザが持つ「要求（requirements)」と、システムが満たすべき「要件（specification)」を区別しています。

5. 本科目で扱う難しさ

近年、ネットワーク家電市場が急速に立ち上がりつつあり、そのニーズの複雑性や変化の速度は、従来の家電をはるかに上回っています。特にセキュリティやセーフティに対するニーズや要求については、ハードウェア・ソフトウェアの両面からさまざまなものがあります。また、ユーザの手元にある機器のみならず、ネットワークで接続された遠隔地のサーバなどとの連携時の安全性も考慮しなければなりません。さらに、エンドユーザのセキュリティだけでなく、全てのステークホルダ(機器製造業者、AV 機器に対する放送局など)の安全性に対するニーズもあります。

ネットワーク家電の安全性の難しさの例を図 1 に示します。図 1 は、HD/DVD レコーダへのセキュリティ要求として、コンテンツの著作権に関するものを示しています。詳しくは、コンテンツの著作権に関し、次のように多数のステークホルダが利害関係を持っているものとします。

- コンテンツ制作会社は、自社のコンテンツの著作権を守りたい
- 放送局は放送したコンテンツの複製権を持っており、これを守りたい
- 機器メーカはユーザのニーズを満足する製品を販売したいが、そのための機能が著作権に抵触する可能性がある
  - 例：コピー機能、ネットワーク接続機能、CM スキップ機能
- ユーザは、コンテンツを自由に利用したいが、著作権に反する利用を行う可能性がある

まとめると、コンテンツの著作権に関して、ステークホルダによって相反する要求が存在し，したがって、製品開発においては、このようなトレードオフを考慮しなければなりません。

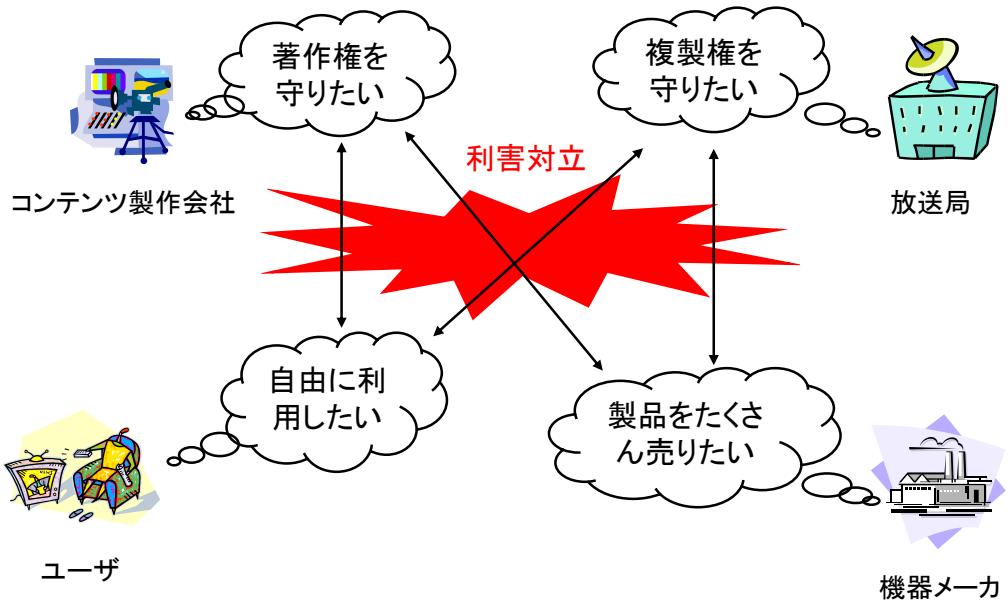

図 1　ネットワーク家電の安全性の難しさの例

6. 本科目で習得する技術

将来のネットワーク家電では、そのニーズが多様化･複雑化し、ニーズの変化も急速になっているであろう。そのため、現在採用されているような、安全性に関する要求の分析手法では、その要件を抜け・漏れなく的確に分析し、迅速に製品開発･出荷に反映させることが困難になってきています。そこで本科目では、安全性に関する要求の分析・獲得を体系的に行う手法として、ゴール・エージェント指向要求分析方法論とユースケース図，ミスユースケース図による、セキュリティをはじめとする要求やその対策の分析・獲得方法を習得します。その上で、現実的なシステム開発における、安全性の要求・セキュリティ機能などの対策の分析・獲得に必要な、ノウハウや標準規格を扱います。また本科目では、それら個別のノウハウや標準規格を、ベースとなる方法論のどの場面でどのように適用するのかを、両者の対応関係を明確にしながら習得します。さらに本科目では、現実的なシステム開発の例を題材に、実習中心で以上の項目を習得します。これにより、本科目で習得した安全性に関する要求や対策案の分析・獲得方法を、開発現場において、速やか、かつ円滑な適用を可能とします。具体的な習得項目、および取り扱う事例は、次の通りです。

- 習得項目
  - 代表的なゴール指向要求分析方法論である、i*、および KAOS と、従来の安全性に関する理論(HAZOP、FTA、他)を統合した方法論
  - ユースケース・ミスユースケースを用いてセーフティやセキュリティの要求を分析・獲得する方法論

本科目では、具体的な要求分析のためのツール群を使用します。これらは、安全性の要求・対策案の分析・獲得において、それぞれ KAOS、および i*の要求モデル作成に最適なツールです。また、「ゴール指向分析」でも使用しているので、履修済みの受講生は円滑に本科目で使用できます。そのほかに、ユースケースモデル作成のために、astah*ツールも使用します。

7. 前提知識

本科目の受講生は、以下の項目を習得済みであることが望ましい。

1. UML：特にユースケースによる要求モデル記述
2. ゴール指向要求分析手法 KAOS、i*の基礎

なお、これらの項目は、トップエスイー開講科目「ゴール指向分析」で習得可能です。

8. 講義計画

・ 概要

第 1 回：安全性入門、機能安全概論

第 2 回、第 3 回：セキュリティ要求獲得概論

第 4 回、第 5 回：ミスユースケースによる脅威分析

第 6 回、第 7 回：ゴール指向要求分析手法 i*、Secure Tropos、KAOS 等 を用いた安全要求分析法とその演習

第 8 回、第 9 回：コモンクラテリア

第 10 回、第 11 回：セキュア i *と CC

第 12 回、第 13 回、第 14 回：グループ演習（１）

第 15 回：グループ発表と議論

・ 詳細

第 1 回：安全性入門、機能安全概論

- 本科目を受講する際に必要な基礎知識を学習する
- 座学中心
  - 安全性に関する定義
  - セーフティに関する要求に関して、特に機能安全概要説明

第 4 回、第 5 回：ミスユースケースによる脅威分析

- ミスユースケースを使った安全要求分析法の概要を説明する
- 座学中心
  - セキュリティの性質(Confidentiality, Availability, Integrity)
  - セキュリティリスク
  - ソフトウェアセキュリティ(ユーザ認証, アクセスコントロール, 暗号)
  - セキュリティ認証の国際標準(CC)
- ユースケース図から安全性へどのようにアプローチされているかを概観する
  - Abuse/Misuse/Security ユースケース図の説明
  - 例題
- 演習問題
  - 上記のユースケース図を用いた安全要件の分析・獲得方法を学ぶ
  - 利用ツール(Jude)

第 6 回、第 7 回：ゴール指向要求分析手法 i*、Secure Tropos、KAOS 等を用いた安全要求分析方法とその演習

- i*と Liu 手法によるセキュリティ要求分析、HazOp と FMEA の適用
- セキュリティ要求分析手法：Secure Tropos 法によるセキュリティ要求の規定
- KAOS による障害分析

第 8 回、第 9 回：コモンクライテリア(CC)

- コモンクライテリア(CC)概論
- CC に基づく保証・評価の実際

第 10 回、第 11 回：セキュア i* と CC セキュリティ分析方法論とその CC への適用

- セキュリティターゲット（ST）作成の演習

第 12 回、第 13 回、第 14 回：グループ演習（２）

- 車載 ECU の制御ソフトウェアを題材としたセキュリティターゲット（ST）作成の応用演習
  - ✧ グループによる討議

第 15 回：発表と議論

各グループの演習結果の発表、および議論

9.　教育効果

本科目を受講することにより、セキュリティとセーフティの定義とそれらの違い、および、それに対する分析・獲得について学び、総合的に安全なシステムに関する要求工学からのアプローチについて学べる。その結果、開発現場において、習得した安全要求・機能安全の分析・獲得方法を、速やかかつ円滑に適用することができるようになる。

10. 使用ツール

K-Tool：KAOS モデル作成ツール
astah*：UML ツール、ミスユースケースの記述に利用する
ST-Tool：i*モデル作成ツール
SecTro：Secure Tropos のモデル作成ツール

11. 実験及び演習

車載 ECU の制御ソフトウェアを例として機能安全や CC の安全要求仕様の作成を題材にして、小規模のシステムの安全要求分析・獲得を行わせる。3〜5 名程度の少人数で共同作業を行わせ、安全性に関する要求モデル作成の重要性と、安全要求分析・獲得の難しさを体験させる。グループ内で、各手法を利用した結果の比較を行い、手法の適用性を議論することにより、安全要求仕様の適切な定義、および安全要求分析・獲得の理解を促進し、適用ノウハウを習得させることに効果が期待できる。

12. 評価

演習課題レポート、プレゼン発表、出席日数を総合して評価する。
レポート課題の出題は下記を予定している。

- 第 3 回講義後（提出期限: 約 3 週間後）
- 第 5 回講義後（提出期限: 約 4 週間後）
- 第 7 回講義後（提出期限: 約 1 週間後）
- 第 9 回講義後（提出期限: 約 3 週間後）
- 第 11 回講義後（提出期限: 約 3 週間後）
- 第 15 回講義後（提出期限: 約 1 週間後）

※締切りは目安であり変更することもありえる
なお、最終レポートの評価に占める比重は高く、これを提出せずに単位を取得することは困難である。

13. 教科書/参考書

- E. Letier, “Reasoning about Agents in Goal-Oriented Requirements Engineering,” Université Catholique de Louvain, 2001.
  KAOS 手法について詳細に記述されている。
- P. Bresciani et al, “Tropos: An Agent-Oriented Software Development Methodology,” Autonomous Agents and Multi-Agent Systems, 2004
  i*を要求分析工程として含むソフトウェア開発方法論 Tropos について詳細に記述されている。
- E. Yu, “Towards Modeling and Reasoning Support for Early-Phase Requirements Engineering”, Proc. of RE’97, 1997
  i*の基本的な考え方をまとめており、上記教科書を補うのに最適である。
- M. Rausand, A. Høyland, “System Reliability Theory: Models, Statistical Methods, and Applications, 2nd Edition”, Wiley, 2003
  リスク管理の基本概念、ならびに FTA、HazOp、および FMECA といった個々のリスク管理手法についてまとめられている。
- L. Liu et al, “Security and Privacy Requirements Analysis within a Social Setting”, Proc. of RE 2003
  i*による安全要求分析手法について詳述している。
- D. S. Herrmann, "Using the Common Criteria for IT Security Evaluation", Auerback Publications, 2003
  CC に関する全体像を掴むのに適している。
- M. S. Merkow, J. Breithaupt, "Computer Security Assurance Using the Common Criteria", Thomson, 2005
  CC に関する概論，最新動向、PP の見本など CC について全般的に学ぶことが出来る。
- Sindre, G. and Opdahl, A.L.: Eliciting security requirements with misuse cases. Requirements Engineering vol.10, No.1, pp.34-44 (2004).
  Usecase を応用したセキュリティ要求分析手法に詳述している。
- 吉岡信和，田口研治編集，特集 セキュリティ要求工学の実効性，情報処理学会，情報処理，
  セキュリティ要求工学の全体像を掴むのに適している。