

# セキュリティ要求分析

平成 23 年度シラバス

2011年4月1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. 講座名

セキュリティ要求分析

## 2. 担当者

吉岡信和、田原康之、大久保隆夫、金子浩之)

## 3. 本講座の目的

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。しかし、他の種類の製品やインフラと比べて、情報システムのセキュリティを高める技術は、現状は十分とはいえないのが現状です。少なくとも、セキュアなシステムを開発するための、体系的な方法論を確立する必要があります。

この授業では、要求分析段階におけるセキュリティ問題の発見手法を扱います。セキュア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となる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、セキュリティ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。授業では、システムの脆弱性、利用者の悪意、システムへの攻撃といったセキュリティ上の問題を予測・発見し、それを克服するための手法を紹介し、演習を通して、実際の要求モデルをセキュリティという視点から分析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、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、セキュリティ要件・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/IEC 15408 (通称Common Criteria ; CC)を取り入れています。CCの専門家による概論の後、学んだ技術を使ってCCのためのセキュリティ要求ドキュメント (Security Target: ST) を作成する演習を行います。

## 4. 本講座のオリジナリティ

近年において情報システムのセキュリティが重要であるとの認識により、数多くのセキュリティに関する講座が開かれています。しかし、セキュリティ要件の分析・獲得手法の習得という点では、それら既存の講座にはいくつかの問題点があり、セキュリティ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。本講座では、それらの問題点を解決し、開発現場において、セキュリティ要件・セキュリティ機能の分析・獲得を効果的に可能としています。表1に、既存の講座の問題点と、本講座における解を示します。

表 1 既存の講座の問題点と、本講座における解

既存の講座の問題点	本講座における解
<p>セキュリティ要件の特徴として、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、ウイルスなど)、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を高める技術(暗号化やアクセス制御など)といった、多くの分類観点がある。しかし、既存の講座では、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</p>	<p>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(リスク管理手法やCC)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可能</p>

## 5. 本講座で扱う難しさ

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の機器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)のセキュリティ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
- ・ 機器メーカー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。

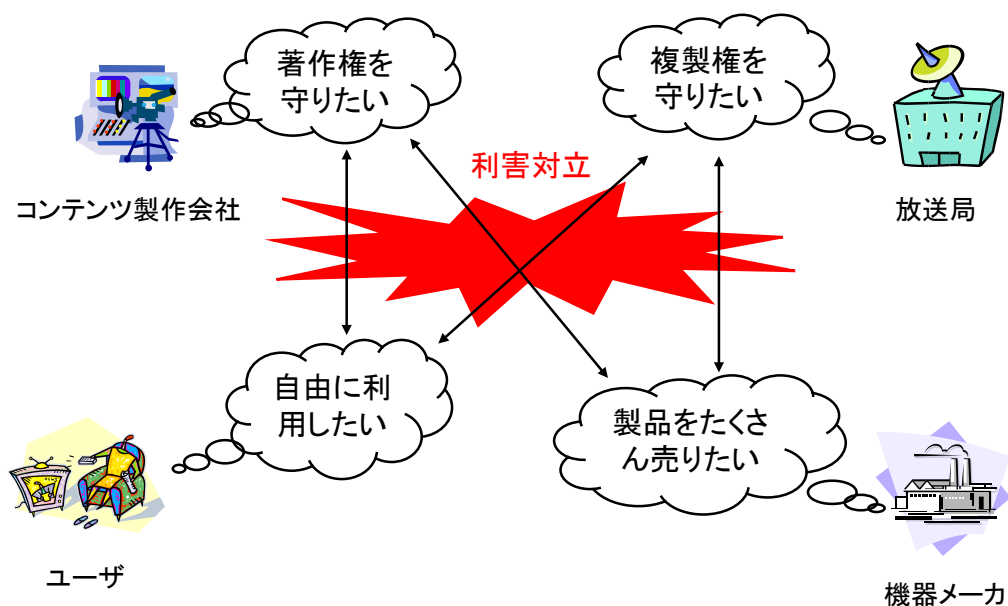


図 1 ネットワーク家電の安全性の難しさの例

## 6. 本講座で習得する技術

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るため、現在採用されているような、セキュリティ要件の分析手法では、セキュリティ要件を抜け・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。そこで本講座では、セキュリティ要件の分析・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、セキュリティ要件・セキュリティ機能の分析・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、セキュリティ要件・セキュリティ機能の分析・獲得に必要な、ノウハウや標準規格を扱います。また本講座では、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の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。さらに本講座では、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、本講座で習得したセキュリティ要件・セキュリティ機能の分析・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キュリティ要件を分析・獲得する方法論

本講座では、具体的な要求分析のためのツール群を使用する。これらは、セキュリティ要件・セキュリティ機能の分析・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、「要求分析」講座でも使用しているので、履修済みの受講生は円滑に本講座で使用できます。そのほかに、ユースケースモデル作成のために、Jude ツールも使用します。

## 7. 前提知識

本講座の受講生は、以下の項目を習得済みであることが望ましい。

- UML：特にユースケースによる要求モデル記述
- 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、「ゴール指向要求分析」講座で習得可能です。

## 8. 講義計画

### ・ 概要

- 第1回：要求獲得概論，要求モデリング手法概論（KAOS, i\*）、リスク分析手法
- 第2回、第3回：ミスユースケースによる脆弱性分析
- 第4回、第5回：ゴール指向要求分析手法 i\*、Secure Tropos、KAOS 等 を用いたセキュリティ要求分析法とその演習
- 第6回、第7回：コモンクラテリア
- 第8回、第9回：セキュア i\* と CC
- 第10回、第11回：グループ演習（1）
- 第12回、第13回：グループ演習（2）
- 第14回、第15回：発表と議論

### ・ 詳細

- 第1回：要求獲得概論，要求モデリング手法概論（KAOS, i\*）
  - 本講座を受講する際に必要な基礎知識を学習する
  - 座学中心
    - ◇ 要求獲得についての基礎
    - ◇ 要求モデリング方法論についての概要説明
- 第2回、第3回：セキュリティ概論，ユースケース法
  - セキュリティに関する基本的な概要を説明する
  - 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4回、第5回：ゴール指向要求分析手法 i\*、Secure Tropos、KAOS 等を用いたセキュリティ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 によるセキュリティ分析

第 6 回、第 7 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 8 回、第 9 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 10 回、第 11 回：グループ演習 (1)

- Web サービス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

第 12 回、第 13 回：グループ演習 (2)

- Web サービス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 14 回、第 15 回：発表と議論

前の回の演習の各グループの発表、および議論

## 9. 教育効果

本講座を受講することにより、様々なセキュリティの概念とそれに対する分析・獲得について学び、総合的にセキュア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、習得したセキュリティ要件・セキュリティ機能の分析・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。

### ・ 使用ツール

K-Tool : KAOS モデル作成ツール

- ・ 使用する上での難しさ
  - モデル作成手順が難しい
  - 安全要件の表現が難しい
- ・ 使用上必要なノウハウ
  - モデル作成ノウハウ
    - ◇ モデル作成プロセス
  - 安全要件の表現ノウハウ
    - ◇ 安全要件の分類
    - ◇ **expectation** の利用
- ・ 選択理由、実用性 : KAOS モデル作成に最適

ST-Tool : i\*モデル作成ツール

- ・ 使用する上での難しさ
  - モデル作成手順が難しい
  - 安全要件の表現が難しい
- ・ 使用上必要なノウハウ
  - モデル作成ノウハウ
    - ◇ モデル作成プロセス
    - ◇ **HazOp** と **FMECA** の適用
  - 安全要件の表現ノウハウ
    - ◇ 脅威モデルの利用
- ・ 選択理由、実用性 : i\*モデル作成に最適

## 10. 実験及び演習

Web上の商取引(ネットショップ)を例としてCC適用によるST仕様の作成を題材にして、小規模のシステムの安全要件分析・獲得を行わせる。4～5名程度の少人数で共同作業を行わせ、要求モデル作成の重要性と、安全要件分析・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、安全要件分析・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。

### ・ 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。

• 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。