5L-7

Common Criteria を利用したモデル駆動アーキテクチャによるセキュリティ要求分析手法

野呂 惇† 松浦 佐江子‡
芝浦工業大学 システム工学部 電子情報システム学科†
芝浦工業大学 大学院理工学研究科 機能制御システム専攻‡

1. はじめに

セキュリティ要件を開発の上流工程で定義，モデル化することは脆弱性の少ないシステムの開発のために有益であるが，従来はシステム開発後にセキュリティの専門家が分析を行い，脆弱性を発見していることが多い．しかし，この方法では脆弱性を発見するたびに開発の手戻りが発生するため時間やコストがかかりすぎるという問題がある．したがって，できるだけ早い段階でシステム開発者が開発と並行してセキュリティ要件をシステムに組み込むことができれば，手戻りを少なく脆弱性を減少させることが可能である．

システム開発者はセキュリティの専門家に比べてセキュリティに関する知識が乏しいため，システム開発者がセキュリティ要求分析を行うためには知識を補う必要がある．そこで，本研究では Common Criteria(以後 CC)を用いることでセキュリティの知識を補うことを考える．

CC(SO/IEC 15408)とは、情報技術セキュリティの観点から，情報技術に関連した製品及びシステムが適切に設計され，その設計が正しく実装されていることを評価するための国際標準規格である．概要と定義などを記した Part1，セキュリティ機能コンポーネント(以後コンポーネント)を記した Part2，セキュリティ保証コンポーネントを記した Part3 から構成されている．

本研究ではシステムの要求分析時にセキュリティ要求をモデル化する手法として， Web-UI プロトタイプ[1]による機能の要求分析モデルに，CC を用いて分析したセキュリティ機能の要求分析モデルを合成することで，セキュリティ機能要求を含む機能の要求分析モデルを生成する手法を提案する．

2. 提案手法

2.1. 前提条件

本手法では Web-UI プロトタイプを用いたシステムの機能の要求分析結果であるユースケース図，アクティビティ図，クラス図を使用し分析を行う．Web-UI プロトタイプとは，web アプリケーションを対象に業務のワークフロー分析からシステムが提供するユースケースを抽出し，Unified Modeling Language(以後 UML)モデルからツールを用いてプロトタイプ(HTML で定義された Web ページ)を自動生成しながら UML 要求仕様を定義する手法である．

2.2. 分析対象システムに対する脅威の分析

ミスユースケース図[2]を用いて分析対象システムに対する脅威を分析する．

機能の要求分析を行ったシステムを悪用するアクターをミスユーザとし，ミスユーザが与える脅威を考える．脅威はユースケースを悪用して発生するため，ユースケースのアクティビティ図に注目する.フロー中のオブジェクトから守るべき情報を分析し，その情報に対する脅威をミスユースケースとして定義する．

2.3. Common Criteria からの対策の選択

前項で分析された脅威に対する対策を，CC Part2 のコンポーネントから選択する．コンポーネントはその機能のカテゴリによって分類されている．分析によって脅威もある程度カテゴリ分けすることができるため，コンポーネントと照らし合わせて選択することができる．また，選択したコンポーネントと依存関係にあるコンポーネントも脅威に対する対策を実現するために必要である．

また，コンポーネントは，システムが行わなければならない動作や条件がエレメントとして箇条書きで記されており，エレメントは割付としてコンポーネントのパラメタを特定することができる．したがって，エレメント，割付をそれぞれアクティビティ図のアクション，オブジェクトノードとして記述し，割付の関係をクラス図を用いて明らかにすることにより，コンポーネントをアクティビティ図とクラス図で表現することができる．

2.4. セキュリティ機能の作成

コンポーネントはあらゆるシステムのセキュリティを表現できるように高い抽象度で書かれているため，エレメントと割付を対象システムに既存の要素と対応付け，セキュリティ機能に必要な属性(以下セキュリティ属性)を作成することで具体化していき，分析対象システムに適合させることでセキュリティ機能を作成する．

2.5. モデル合成

前項で作成したセキュリティ機能をアクティビティ図のフローにマージする．セキュリティ機能をマージすべきアクティビティ図は，対象システムに既存の要素との対応関係から特定できる．作成されたセキュリティ属性も対応するクラスに追加する．これにより，セキュリティ機能を含む機能の要求分析モデルが生成できる．

3. LUMINOUS 掲示板システムへの適用例

3.1. LUMINOUS 掲示板システム

LUMINOUS とは本学で使用されている学習支援サイトのことである．学生は自分の履修している授業の教材のダウンロードやレポートの提出などを行うことができ，教員は教材のアップロードやレポートの作成，採点などを行うことができる．

この LUMINOUS に，学生が質問を投稿し，教員が回答を行う LUMINOUS 掲示板システム(以後掲示板システム)を追加した．掲示板システムの主な機能は学生が質問を投稿すること，教員が投稿された質問に回答すること，学生と教員が投稿された質問と回答のまとまりである話題を閲覧できることである．また，質問と回答にはファイルを添付する事ができ，閲覧時にダウンロードできる．

3.2. 脅威の分析

悪意のある学生をミスユーザとして分析を行う．分析結果を図 1 に示す．

Security Requirements Analysis Technique using Common Criteria based on Model Driven Architecture
†Atsushi Noro ‡Saeko Matsuura
†Department of Electronic Information System, collage of System Engineering, Shibaura Institute of Technology
‡Division of Functional Control Systems, Graduate School of Engineering and Science, Shibaura Institute of Technology

Copyright ©2012 Information Processing Society of Japan.
All Rights Reserved.

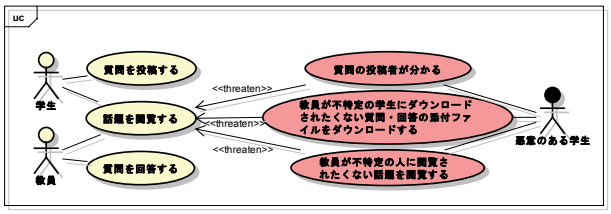

図 1.ミスユースケース図

3.3. 対策の選択

分析した脅威は，話題と添付ファイルという利用者データへのアクセスに関する脅威であると判断できる．したがって，利用者データ保護クラスのアクセス制御機能の中からセキュリティ属性によるアクセス制御を，対策となるコンポーネントとして選択する．図 2 はセキュリティ属性によるアクセス制御というコンポーネントをアクティビティ図で表したものである．

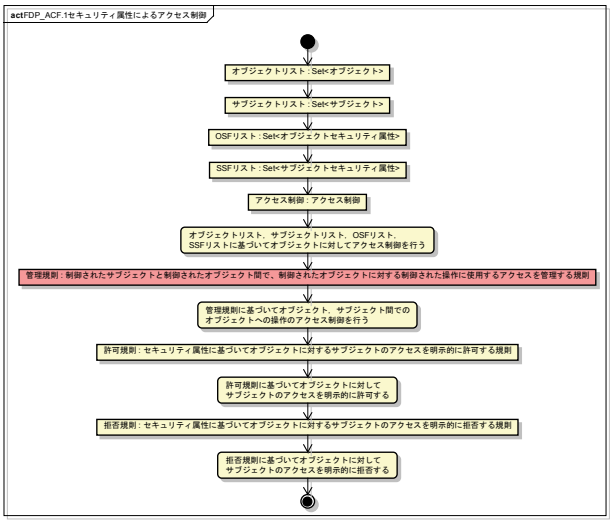

図 2. セキュリティ属性によるアクセス制御

3.4. セキュリティ機能の作成

選択したコンポーネントのアクティビティ図を掲示板システムに合わせて具体化する．表 1 は，図 2 中の「制御されたサブジェクトと制御されたオブジェクト間で，制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則」を具体化したものである．

表 1.管理規則

サブジェクト	サブジェクトセキュリティ属性(役割)	オブジェクト	オブジェクトセキュリティ属性	操作
学生	学生番号（アルファベット+五桁の数字）	BBS		質問を投稿する:更新する 話題を閲覧する:取得する
		話題履歴		質問を投稿する:生成する/更新する 話題を閲覧する:参照する
		話題	公開	話題を閲覧する:参照する
		話題	非公開	質問を投稿する:生成する
		コンテンツ		質問を投稿する:生成する 話題を閲覧する:参照する
		投稿内容	添付ファイル公開	話題を閲覧する:参照する 話題を閲覧する:添付ファイルをダウンロードする
		投稿内容	添付ファイル非公開	質問を投稿する:作成する 話題を閲覧する:参照する
		投稿者		質問を投稿する:取得する 話題を閲覧する:取得する 話題を閲覧する:参照する
		日時		質問を投稿する:取得する
教員	教員	BBS		質問を回答する:更新する 話題を閲覧する:取得する
		話題履歴		質問を回答する:取得する/更新する 話題を閲覧する:参照する
		話題	公開 非公開	質問を回答する:取得する 話題を閲覧する:参照する
		コンテンツ		質問を回答する:作成する 話題を閲覧する:参照する
		投稿内容	添付ファイル公開 添付ファイル非公開	質問を回答する:作成する 話題を閲覧する:参照する 話題を閲覧する:添付ファイルをダウンロードする
		投稿者		質問を回答する:取得する 話題を閲覧する:取得する 話題を閲覧する:参照する
		日時		質問を回答する:取得する

サブジェクトはアクター，サブジェクトセキュリティ属性はアクターを識別している属性，オブジェクトは entity クラスと対応付けることができる．オブジェクトセキュリティ属性については，アクセス制御をかけたいオブジェクトに対して新たに作成する．操作は要求分析モデルのアクティビティ図のアクションと対応付けることができる．また，アクセス制御方針や規則などセキュリティ要求に関わる要素は新たに作成する必要がある．

抽象度を掲示板システムに合わせた結果の例を図 3 に示す．これは表 1 でセキュリティ属性を追加したオブジェクト「投稿内容」に注目し，セキュリティ属性によって制御された操作「添付ファイルをダウンロードする」に対してアクセス制御を行うためのセキュリティ機能を作成したものである．

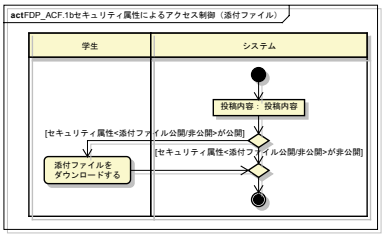

図 3. 添付ファイルに関するセキュリティ属性によるアクセス制御

3.5. モデル合成

作成されたセキュリティ機能を，ミスユースケース図を元に該当するユースケースのアクティビティ図の「添付ファイルをダウンロードする」操作に該当するアクションの前に追加する．合成した結果を図 4 に示す．

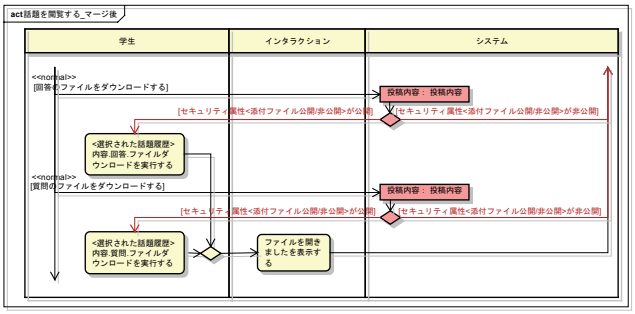

図 4. マージ後のアクティビティ図の一部

4. 考察と今後の方針

CC のコンポーネントを対象システムの要素を用いて具体化することで，セキュリティ要求を機能要求に組み込むことができた．したがって，本手法を用いることで開発者が要求分析モデルを用いてセキュリティ要求分析を行うことができると考える．しかし，本手法ではセキュリティ要求分析に漏れがあるかどうかを判断できない．

また，作成されたセキュリティ機能は，アクティビティ図にマージできるものだけではなく，アクティビティ図のフローは変えずにアクションに制約をつけるものなどもあり，合成の方法は複数のパターンが考えられる．

今後は CC Part3 の保証コンポーネントを用いて，セキュリティ要求分析が網羅的かどうか検証できないか検討する．また，より多くの事例に本手法を適用し，モデル合成のパターンを検証していく．そして本手法を用いた開発者向けセキュリティ要求分析支援ツールを作成し，要求分析時でのセキュリティ要求の導入を支援する．

5. 参考文献

[1] 小形，松浦：UML 要求分析モデルからの段階的な Web UI プロトタイプ自動生成手法，日本ソフトウェア科学会，コンピュータソフトウェア，Vol.27，No.2，pp.14-32，2010.

[2] Sindre, G and Opdahl, A. L.: Eliciting security requirements with misuse cases, Requirements Engineering Journal, 10 (1), pp.34-44 (2005).

Copyright ©2012 Information Processing Society of Japan.
All Rights Reserved.