2M-5

セキュリティ機能方針の具体化による セキュリティ機能要求分析手法

野呂　惇†　　小形　真平‡　　松浦　佐江子†

芝浦工業大学大学院理工学研究科電気電子情報工学専攻†　　信州大学工学部情報工学科‡

1. はじめに

脆弱性の少ないシステムを開発するために，我々は分析の複雑さを緩和し、漏れなくセキュリティ要件を抽出することを目的として，機能要求分析モデルにセキュリティ機能要求分析モデルを統合する手法[1]を研究している．機能要求分析モデルとは，分析対象システムのアクタ，アクタが利用するユースケース，ユースケースにおけるアクタとシステムの相互作用(インタラクション)の振る舞いとそれに関わる入出力およびエンティティのデータ，データ構造およびその関係と制約を UML のユースケース図，クラス図，アクティビティ図を用いて定義したものである．また，セキュリティ機能要求分析モデルとは，機能要求分析モデルをもとにシステムに対する脅威を分析し，脅威に対する対抗策をセキュリティ評価基準であるコモンクライテリア(以下 CC)[2]のセキュリティ機能コンポーネント(以下コンポーネント)から選択し，UML モデルで表したコンポーネントを機能要求分析モデルの要素により具体化することで定義される，セキュリティ機能の UML モデルである．

この手法ではコンポーネントをセキュリティ機能の振る舞いであると解釈し，その振る舞いを機能要求分析モデルの要素を用いて具体化することでセキュリティ機能を定義し，機能要求の振る舞いと共通するアクションやオブジェクトノードをキーにマージすることができたが，定義したコンポーネントをマージするためのポイントを特定することが困難であるという問題点があった．

本稿では，CC におけるセキュリティ機能方針(以下 SFP)を機能要求分析モデルの要素と対応付けることでセキュリティ機能要求を分析し，SFP を利用してセキュリティ機能を機能要求分析モデルに統合する方法について議論する．

2. セキュリティ機能方針

CC において，SFP は「評価対象のセキュリティ機能によって実施され，セキュリティ機能要件のセットとして表現できる特定のセキュリティのふるまいを記述する規則のセット」と定義されている．

SFP は CC の利用者データ保護(FDP)クラスのアクセス制御方針(FDP_ACC)ファミリと情報フロー制御方針(FDP_IFC)ファミリにより定義することができる．

2.1. アクセス制御方針

アクセス制御方針とは，情報を格納したコンテナへのアクセスを制御する SFP である．したがって，システムの情報に対して操作を行う主体(サブジェクト)，情報が格納されているエンティティ(オブジェクト)，サブジェクトがオブジェクトに対し行なうアクション(操作)のセットへの制御を定義する．

2.2. 情報フロー制御方針

情報フロー制御方針とは，コンテナと独立した情報に対するアクセスを制御する SFP である．したがってサブジェクト，情報，サブジェクトに対する双方向の情報の流れを生じさせる操作のセットへの制御を定義する．

3. 提案手法

3.1. セキュリティ機能方針の表現方法

本手法では SFP をテーブルで表現する．作成する SFP テーブルは各行がサブジェクト，オブジェクト，操作，ルールのセットとなるように作成する．

サブジェクトとオブジェクトの項目には，それらを識別するための名前とセキュリティ機能に必要な属性であるセキュリティ属性を，操作の項目にはサブジェクトがオブジェクトに対して行うアクションとそのアクションを行なっているユースケースのアクティビティ図名を，ルールの項目には SFP を決定または実現するために必要なコンポーネントごとに，サブジェクト・オブジェクト・操作のセットに対するルールを記述する．

3.2. セキュリティ機能方針テーブルの生成

サブジェクトをアクタ，オブジェクトをエンティティクラス，CC における操作を要求分析モデルにおけるアクティビティ図上のアクションだと解釈することで，SFP テーブルのサブジェクトの名前，オブジェクトの名前，操作の項目を要求分析モデルの要素を用いて具体化することができる．操作に関しては，アクセス制御方針は情報を格納するコンテナに対する操作を制限することから，システムパーティション上でエンティティクラスに対して操作を行なっているアクションを，情報フロー制御はコンテナと独立した情報，つまりユーザがシステムを利用することで得られる情報であるという解釈から，インタラクションパーティション上でエンティティクラスの情報を入出力しているアクションをそれぞれ操作として抽出する．

3.3. セキュリティ機能方針の定義

3.2で生成したテーブルをセキュリティ要求分析者が埋めていくことでセキュリティ機能方針を定義する．ルールの項目のコンポーネントは，システムの脅威に対する対策として選択したコンポーネント及びそれに依存性のあるコンポーネントを記述する．分析者は，各コンポーネントにおいてサブジェクト・オブジェクト・操作のセットに対して制約が必要な部分にセキュリティ上のルールを記述する．その際，ルールを記述する上で必要な属性がある場合は，それをセキュリティ属性として新規作成もしくは既存のエンティティクラスの属性から選択し，該当するセキュリティ属性の項目に記述する．また，ルールを記述するために必要な操作がテーブルに存在しない場合は，新たにテーブルに追加する．

Security Functional Requirements Analysis Technique based on Security Function Policies

†Atsushi NORO ‡Shinpei OGATA †Saeko MATSUURA

†Division of Electrical Engineering and Computer Science, Graduate School of Engineering and Science, Shibaura Institute of Technology

‡Department of Computer Science and Engineering, Faculty of Engineering, Shinshu University

表 1 LUMINOUS 掲示板システムのアクセス制御方針テーブル

サブジェクト		オブジェクト		操作		ルール			
名前	セキュリティ属性	名前	セキュリティ属性	アクティビティ図	アクション	FDP_ACF.1 セキュリティ属性によるアクセス制御	FMT_MSA.3 静的属性初期化	FMT_MSA.1 セキュリティ属性の管理	…
学生	役割(学籍番号)	BBS		話題を選択する(学生)	現在のBBSを取得する				
				質問を投稿する	BBSに新規話題履歴を追加する				
		コンテンツ		質問を投稿する	質問のコンテンツを生成する				
		話題履歴		話題を選択する(学生)	<現在のBBS>から話題を取り出す				
				話題を閲覧する(学生)	<話題履歴一覧>から<話題番号>の話題履歴を取り出す				
				質問を投稿する	話題履歴を生成する				
		話題		質問を投稿する	話題を生成する				
		日時		質問を投稿する	現在日時を取得する				
		投稿者	役割	話題を選択する(学生)	現在の利用者を取得する				
				質問を投稿する	投稿者を取得する				
		投稿内容		話題を閲覧する(学生)	投稿内容を取得する				
		添付ファイル	公開非公開	話題を閲覧する(学生)	添付ファイルをダウンロードする	公開非公開=公開 ‖ 投稿者.役割=サブジェクト.役割			
				質問を投稿する	添付ファイルを登録する		公開非公開=非公開		
教員	役割(教員)	BBS		話題を選択する(教員)	現在のBBSを取得する				
				質問に回答する	BBSを更新する				
		コンテンツ		質問に回答する	回答を作成する				
		話題履歴		話題を選択する(教員)	<現在のBBS>から話題を取り出す				
				話題を閲覧する(教員)	<話題履歴一覧>から<話題番号>の話題履歴を取り出す				
				質問に回答する	話題履歴を更新する				
		話題		質問に回答する	<話題履歴>から<質問番号>で話題を取得する				
				質問に回答する	<質問番号>により選択された話題を取得する				
				質問に回答する	回答を追加して話題を更新する				
		日時		質問に回答する	現在日時を取得する				
		投稿者	役割	話題を選択する(教員)	現在の利用者を取得する				
				質問に回答する	投稿者を取得する				
		投稿内容		話題を閲覧する(教員)	投稿内容を取得する				
		添付ファイル	公開非公開	話題を閲覧する(教員)	添付ファイルをダウンロードする				
				質問に回答する	添付ファイルを登録する		公開非公開=非公開		
					添付ファイルの公開非公開を公開に変更する			公開非公開=公開	
					添付ファイルの公開非公開を非公開に変更する			公開非公開=非公開	

4. LUMINOUS 掲示板システムへの適用例

4.1. 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，学生は自分の履修している授業の教材のダウンロードなど，教員は教材のアップロードなどができる．

この LUMINOUS に追加する掲示板機能を本稿では LUMINOUS 掲示板システム(以下掲示板システム)と呼ぶ．主な機能要求は，学生が質問を投稿し，教員が回答すること，質問と回答にファイルを添付でき，学生と教員が話題(質問と回答のセット)の閲覧と添付ファイルのダウンロードをできることである．

また，この掲示板システムの要求分析モデルから分析された脅威として，「教員の意図していない学生が添付ファイルを閲覧できる」という脅威があり，対抗策として「FDP_ACF.1 セキュリティ属性によるアクセス制御」のコンポーネントを選択する．

4.2. セキュリティ機能方針テーブルの生成

掲示板システムの要求分析モデルの要素から SFP テーブルを生成する．表 1の太枠内の要素は掲示板システムの要求分析モデルのアクタ，エンティティクラス，アクティビティ図のアクションから取得したものである．

4.3. セキュリティ機能方針の定義

まず，対抗策として選択したコンポーネント「FDP_ACF.1 セキュリティ属性によるアクセス制御」と，それと依存性のあるコンポーネントをルールの項目に記述する．そして，各コンポーネントに必要なセキュリティ上のルールを定義する．

「FDP_ACF.1 セキュリティ属性によるアクセス制御」は，セキュリティ属性によってオブジェクトに対する操作を制御するコンポーネントである．分析された脅威は，教員が添付ファイルの公開非公開を決定し，公開である場合のみ投稿者以外の学生のダウンロードを許可することで防ぐことができる．したがって，ますこのルールに必要なセキュリティ属性である添付ファイルの「公開非公開」，投稿者の「役割」，サブジェクトの「役割」を記述する．そして，それらのセキュリティ属性を用いて学生の添付ファイルに対する「添付ファイルをダウンロードする」操作を制御するルール「公開非公開=公開||投稿者.役割=サブジェクト.役割」を記述する．

「FDP_MSA.3 静的属性初期化」は，オブジェクト生成時にセキュリティ属性を初期化するコンポーネントであるため，添付ファイルを生成している学生，教員それぞれの「添付ファイルを登録する」操作での初期値のルール「公開非公開=非公開」を記述する．

「FMT_MSA.1 セキュリティ属性の管理」は，セキュリティ属性に対する操作を制御するコンポーネントである．掲示板システムでは教員が添付ファイルの公開非公開を決定することで脅威に対抗するため，教員が添付ファイルの公開非公開を設定する操作が必要である．そのため，それに該当する「添付ファイルの公開非公開を公開に変更する」操作と「添付ファイルの公開非公開を非公開に変更する」操作を新たに追加し，その操作によるセキュリティ属性のルールを記述する．追加した操作に関しては機能要求のワークフローと合わせてどこに追加するかを検討する必要がある．

表 1は以上のプロセスで定義した掲示板システムのアクセス制御方針テーブルである．

5. まとめと考察

本手法では，要求分析モデルから生成されるテーブルをもとに SFP を定義した．このテーブルによってセキュリティ上のルールが必要なサブジェクト・オブジェクト・操作のセットが明確になるため，コンポーネントからセキュリティ機能を定義した際に要求分析モデルにマージするポイントを特定することができる．

また，本手法では SFP テーブルを機能要求と分離してセキュリティ要求を抽出することを目的に使用しているが，セキュリティ要件を検査する目的に SFP テーブルを使用できる可能がある．具体的には，セキュリティ要求を含む要求分析モデルからセキュリティ属性等も対応付けた SFP テーブルを生成し，CC のコンポーネントにもとづいてルールを定義し，このルールを検査式としてモデル検査技術を用いることで，要求分析モデルが CC の規則を満たしているかの検査を行うことができると考えている．

6. 参考文献

[1] 野呂惇，小形真平，松浦佐江子，“UML 要求分析モデルとコモンクライテリアに基づくセキュリティ要求分析の統合手法”，情報科学技術フォーラム講演論文集，vol.11，no.4，pp.77-80 (2012)．

[2] 独立行政法人 情報処理推進機構，“CC/CEM バージョン 3.1 リリース 3”，http://www.ipa.go.jp/security/jisec/cc/index.html