実践的セキュリティ要求工学に向けて

山本 修一郎
(株)NTT データ 技術開発本部 システム科学研究所

ソフトウェア開発現場で必要となるセキュリティ要求工学の知識として，投資対効果の評価手法，セキュリティ要求工学プロセス，企業情報システムのセキュリティ・アーキテクチャ，セキュリティ専門家とのチームワークを考慮したプロジェクト管理などの取り組み事例について解説することにより，現場で使える実践的セキュリティ要求工学の現状と課題を紹介する．

特にブレインストーミングに基づく簡便な資産分析手法とモデル検査を用いた IC カードのセキュリティ特性の自動的な確認手法など容易な現場導入が期待される手法について具体的に説明する．

最後に，今後の情報システム開発におけるセキュリティ要求工学の実践的研究への期待について述べる．

セキュリティ要求工学を実践する上での課題

セキュリティ要求工学を産業界が導入する上での課題を整理すると，次のようになるだろう．

まずシステム開発プロセスの中でセキュリティ要求工学を実施するためには，その投資対効果を明らかにする必要がある．

次にセキュリティ要求工学の導入が決まると，要求獲得，仕様化，要求確認，要求管理という要求工学の基本プロセスの中でどのようにセキュリティ要求を扱うのかを具体化する必要がある．この過程で開発対象システムのアーキテクチャに基づいてシステム構成要素とセキュリティ要求との関係を明らかにしておく必要がある．またセキュリティ専門家と開発者によって円滑に情報共有できるように協調的なチームが形成してプロジェクト管理面を工夫する必要がある．

上述したことをまとめると**表 -1** のようになる．以下ではこれらについて解説する．

分類	実践的な課題
投資対効果	セキュリティ要求工学の客観的な導入判断基準
要求工学プロセス	セキュリティ要求獲得 セキュリティ要求の仕様化 セキュリティ要求の確認 セキュリティ要求の管理
アーキテクチャ	システム・アーキテクチャと資産分析の一貫性 複数システム間のセキュリティ・アーキテクチャ 企業間システムにおけるセキュリティ・アーキテクチャの統合
プロジェクト管理	セキュリティ専門家とシステム開発者の情報共有 セキュリティ要求工学の教育と適用法

表 -1　セキュリティ要求工学の実践的な課題

◆セキュリティ要求工学の投資対効果評価

セキュリティ要求工学の投資対効果を評価するために活用できる手法として Carnegie Mellon 大学の SIDD（Security Investment Decision Dashboard）がある [1]．SIDD はセキュリティ対策の投資対効果について意思決定するための手法であって，セキュリティ要求工学だけに限定した手法ではない．しかしシステム開発全体の中でどのようなセキュリティ対策をとるべきかという総合的な観点からセキュリティ要求工学の必要性を評価することが重要である．

SIDD では 7 分類 33 指標を用いてセキュリティ対策技術を定量的に採点しダッシュボードで視覚的に提示することにより，総合的に経営層が投資対効果を判断できるという特徴がある．なお SIDD の 7 分類の内容は，コスト，重要度とリスク，フィージビリティ，変更容易性，参画性，可測性，所要時間と工数である．

◆セキュリティ要求工学プロセス

基本的なプロセスである要求獲得，仕様化，要求確認，要求管理の点から課題を整理してみよう（**図 -1**）．

【セキュリティ要求獲得】

セキュリティ要求獲得では，システムに含まれる資産に対してセキュリティ上の脆弱性を分析することによりセキュリティ要求を獲得する．たとえば 2008 年から開始された EU による産学連携の Shields プロジェクトでも資産分析手法を開発している [2), 3)]．Shields プロジェクトについては後述する．

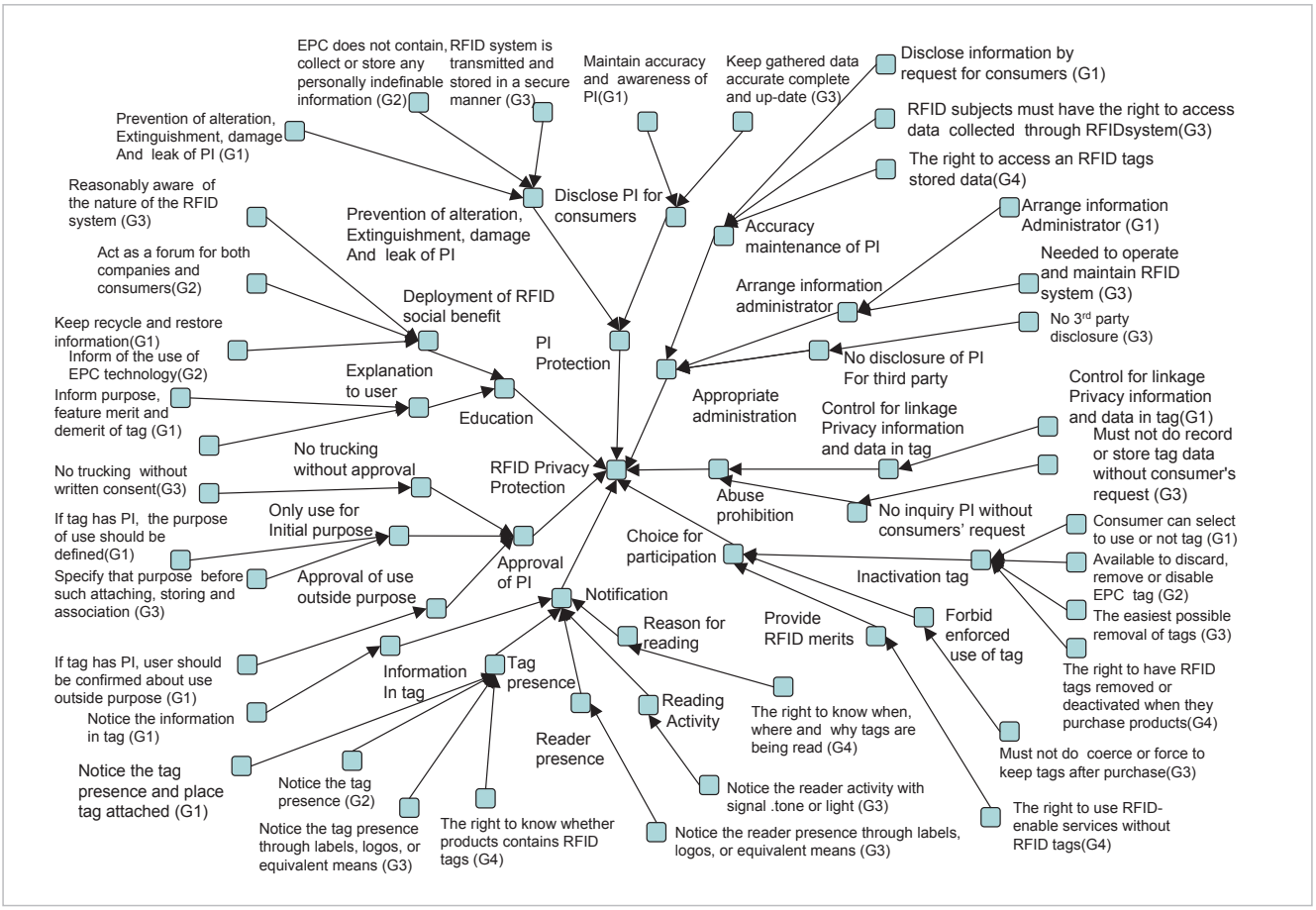

図 -1　RFID プライバシー保護オントロジー

またセキュリティ要求に対してどのようなセキュリティ機能があるかという知識をあらかじめオントロジーとして体系的に整理しておくことによりセキュリティ機能要求の獲得を支援できる．筆者らは RFID によるプライバシー要求知識について図 -1 に示すようなセキュリティオントロジーを構成している[4]．このオントロジーではプライバシー保護というセキュリティ要求に対してセキュリティ機能要求とセキュリティ機能を関連付けている．

【セキュリティ要求の仕様化】

セキュリティ要求は，非機能要求であると同時にアスペクト要求でもある．アスペクト指向要求定義では，開発対象システム全体で共通する関心事（アスペクト）を分離独立させて定義することによって要求定義の重複を削減することができる．また要求 B の構成要素が要求 A を必要とするとき要求 A が要求 B をクロスカットするという．

たとえばプライバシーや機密性は複数の機能に分散するだけでなく同時に必要となることもあるのでクロスカット要求である．

したがってセキュリティ要求は仕様書の中で分散するだけでなく複数個所で同時に必要となることも多いので，可能な限り独立させて定義しどこで参照するかを明確化しておく必要がある．

【セキュリティ要求の確認】

高信頼性が要求される IC カードシステムなどでは ISO 15408 の EAL レベル 7 のように開発対象システムが所望のセキュリティ要求を満足することを示すために形式手法を用いた厳密な証明が求められている．しかしながらどのような形式手法を採用するかだけでなく，どのように形式手法を適用すればよいかについて，まだ十分なコンセンサスが得られていないため，開発対象システムごとに形式手法の適用法を模索している状況である．

たとえば後述する IC カードシステムに関する形式手法を用いた CC（Common Criteria，コモンクライテリア）認証の事例では，次のような手順を構築している．まずセキュリティ要求に対して脅威分析を実施してセキュリティ特性を抽出し，次いで IC カードとその利用環境に対する状態モデルを作成することにより，この 2 つのプロセス間のメッセージ交換によって状態モデルがセキュリティ特性を満足することをモデル検査している[5]．

必ずしも形式手法に限定するわけではないが，現場の開発者にとって受容性の高い簡便で信頼性の高いセキュリティ要求の確認手法を開発する必要がある．

【セキュリティ要求の管理】

セキュリティ要求の仕様化でも述べたように，セキュリティ要求はクロスカット要求であるため，セキュリティ機能要求との関係だけでなくセキュリティ要求間の依存関係も管理する必要がある．またセキュリティ要求獲得でも指摘したように，開発対象システムに含まれる資産に対してセキュリティ要求を定義するため，開発対象システムのアーキテクチャとの対応関係を管理する必要がある．つまり，機密性やプライバシーなどの抽象的なセキュリティ要求ではなく，具体的な資産に対するセキュリティ要求を定義するためにはシステムのアーキテクチャが定義されている必要がある．この理由はアーキテクチャが明確でなければ保護すべき資産としての構成要素を識別できないからである．また資産に対する運用手順も明確にする必要がある．そうしないと資産に対する脅威を定義できないからである．

また企業情報システムのガバナンスを考えると，システムごとのセキュリティ要求ではなく，企業情報システム全体に対する統合的なセキュリティ要求の管理が重要になると思われる．たとえば，企業が顧客の口座に対して異なるサービスを提供している場合，サービスごとに顧客の認証機能が提供される．もし一方のサービスでパスワードなどの認証情報が攻撃されて漏洩した場合，他のサービスで漏洩したのと同じ認証情報を用いていたとするとこのサービスも悪用される可能性がある．このような問題に対処するためにはサービスごとにセキュリティ要求を獲得するだけでなく，企業が提供するシステム全体でどのようなセキュリティ要求が必要となるかを考慮した上で，個別のシステムにおけるセキュリティ要求の必要性を明らかにすることが重要となる．

さらに企業間の情報流通に関するセキュリティ要求の管理も重要である．たとえばBoeing社のDAM（Digital Access Management）では，企業間情報流通で必要となるアクセス権管理E2ERM（Enterprise to Enterprise Rights Management）の標準化を提唱している[6]．

DAMでは，企業間で情報交換する場合に流通対象となる情報だけでなく，情報に関するアクセス権というメタ情報も保護対象となるとして資産として扱う必要があると指摘している．またOSやミドルウェアなど異なる情報基盤間で相互接続性や拡張性などのDAMに対する要求条件を提示している．これらの非機能要求はDAMという企業間除法流通におけるセキュリティ機能要求が満たすべきソフトゴールを定義していると考えられる．

以下では，これらの課題に対してセキュリティ要求工学を導入する上で参考になると思われるShieldsプロジェクトと形式手法によるICカードのCC認証の取得事例を紹介する．

Shieldsプロジェクト[2)]

Shieldsプロジェクトの目的はセキュリティ技術者とソフトウェア開発者の壁を越えることによりセキュリティの脆弱性を解消することである．このため次のような技術を開発するようである．

- セキュリティ専門家がセキュリティの脆弱性を容易かつ迅速に識別して開発者のコミュニティと開発支援ツールを通じて情報共有できるように支援する
- 開発者が日常的に使用する開発支援ツールでセキュリティの脆弱性を検出し除去することを支援する
- ソフトウェア製品がセキュリティの脆弱性を解消していることを開発組織が検証することを支援する

Shieldsは EU-FP7 の ICT- プロジェクトでスウェーデン Linköping University の Nahid Shahmehri 教授がリーダである．この国際的な産官学連携プロジェクトには，スウェーデンの Linköping University のほか，ノルウェーの SINTEF，スペインの European Software Institute，ドイツの Fraunhofer IESE フランスの Institut National des Télécommunications と Montimage，ハンガリーの SEARCH-LAB とイタリアの TXT e-Solutions が参画している．

以下では，このプロジェクトの中で取り組まれている資産分析手法について説明する．

セキュリティ要求工学で資産の識別が重要であるにもかかわらず具体的な抽出手法が明確になっていないため，セキュリティの専門家でない一般のシステム開発者にとって資産分析は容易ではない．このためSINTEFでは以下の3ステップからなる資産識別手法を提案している．このプロセスには要求分析者を含むシステム開発者，顧客，セキュリティ専門家，エンドユーザが参加する．ただしセキュリティ専門家とエンドユーザは必ずしも参加しなくてもよい．

【ブレインストーミング】

まずポストイットと筆記用具を用意して，個人に与えられるアイディアを着想するための制限時間（例：5分）を決める．「資産は何か」などの質問を用意して参加者全員に見えるように貼り出す．参加者がアイディアをカードに1つずつ制限時間内で書き出していく．時間がきたらポストイットを壁に貼り全員でグループ化して

結果をまとめる．

【文書からの資産抽出】

開発対象システムに関する機能要求を記述した文書から重要な資産を見落としていないかどうかを調べる．この結果もし必要だと判断したらブレインストーミングを繰り返す．

【分類と優先付け】

資産が識別されたら分類して，顧客，システム提供者，資産の攻撃者という3つの立場ごとに機密性C：Confidentiality，整合性I：Integrity，可用性A：Availabilityに関する優先順位を3段階（1：高，2：中，3：低）で評価する．

資産の機密性，整合性，可用性の重要性に基づいて優先順位の高い資産を採用する．

このような資産識別手順であれば開発現場に容易に導入できることは明らかだろう．しかし，どのような資産が獲得できるかがブレインストーミング参加者のスキルに依存するという課題もあるだろう．これに対処するため，資産抽出のための事前質問やチェックリストを用意しておくなどの工夫が必要になるとしている．また機能要求を前提にして資産を識別する点についても，開発対象システムを利用する上での社会的な受容性，エンドユーザの安全性，相互接続性などの抽象資産を見落とす可能性がある．このような抽象資産は，システム内の情報やシステム構成要素から抽出される資産ではない．開発対象システムが顧客やエンドユーザに対して提供すべき価値の低下や消失によって失われる資産である．これらの抽象資産については，システムが提供すべき価値をソフトゴールとして抽出し，その価値の低下や消失を抽象資産に対する脅威，その対策を抽象資産に対するセキュリティ要求として抽出することになるだろう．ただし顧客価値向上などはソフトゴールであり，それを実現するのは機能要求とする方が一般的だと思われる．

ここで資産を整理しておくと次のようになるだろう．

抽象資産：システムを利用することで生まれる価値
メタ情報資産：システムに含まれる情報資産に関する情報
情報資産：システム構成要素とそれが持つ情報
物理資産：システム構成要素とその情報の保持・出力媒体

ところで，Shieldsプロジェクトは2008年1月1日から2010年の6月30日までの予定で始まったばかりのところだが，セキュリティとソフトウェア開発を統合的に捉えるこのような取り組みは実践的なセキュリティ要求工学では重要である．企業内だけで見てもセキュリティ専門家とソフトウェア開発技術者との間でなかなか情報共有が進んでいないのは日本でも同様であろう．EUではセキュリティ技術とソフトウェア工学技術の融合を目指した研究開発が国際的かつ産学連携で進んでいるところにも技術開発に対するEUの高い戦略性を見ることができる．特定の国，特定の企業，特定の大学によって開発されるのではないことがグローバルに通用するセキュリティ要求工学技術を育てるために必要であろう．

形式手法を用いたICカードのセキュリティ開発技法

以下では，形式手法をICカードのセキュリティ開発にアジア圏で初めて採用して合格したNTTデータの事例を紹介する．この事例ではADV_SPM.3という形式手法のセキュリティポリシー適用を含んだCC認証に対してSPINによる検証を実施している．

◆評価対象の概要

評価対象TOE（Target Of Evaluation）はNTTデータが開発したXaica-Alpha上の電子パスポート（e-Passport）アプリケーションである．

評価対象が満たすべき要求定義書（調達仕様書）としてPP0017（Protection Profile，0017）を用いる．ここで電子パスポート用のPPであることを番号0017が示している．このPPに基づいてSecurity Target（セキュリティ設計書）を作成する．セキュリティ設計文書のセキュリティ要求を評価するためのCCには，構成管理ACM，展開と運用ADO，開発ADV，ガイダンス文書AGD，ライフサイクル支援ALC，テストATE，脆弱性アセスメントAVAがある．形式手法の適用が求められるのはEAL5以上のADV_SPM.3である．ここでADV_SPM（Security Policy Modeling）ファミリーの最高レベルがADV_SPM.3である．ADV_SPM.3では形式的手法（formal description）によるポリシーの定義と無矛盾性の証明（demonstration）が要求される．換言するとADV_SPM.3ではシステムが満たすべきセキュリティポリシーTSPとセキュリティ機能要求SFRの対応関係を開発者が証明する必要がある．

以下では，ICカードXaica-Alpha上の電子パスポート（e-Passport）アプリケーションを評価対象としてNTTデータ技術開発本部で実施した形式手法の適用事例について紹介する．

◆適用する形式手法の選択

開発現場への形式手法の適用では，まずどのような形式手法を選択するかを決める必要がある．

分類	性質	評価対象モデル	環境モデル
セキュリティターゲット ST	TOE セキュリティポリシー 脅威	セキュリティ機能要求（SFR） TSF TOE セキュリティ設計 TOE 実装（全部）	想定操作 セキュリティ対策方針 セキュリティ機能要求（SFR）
状態モデル	検証式	TOE モデル • 初期状態 • 資源 • インタフェース • 振舞い	環境モデル • ユーザ • シナリオ
形式モデル	LTL 式	SPIN ソースコード	

表 -2　モデル化の方法

IC カード開発に形式手法を適用した従来の事例では，B-method や Isabel などの形式的仕様記述言語などがある．一方 SPIN のような状態モデルに基づくモデル検査ツールを適用した事例は報告されていなかった．実際にフランスの認証機関でもこれまでモデル検査によって認証に合格した事例を経験していなかった．このため IC カード分野で実績のある形式的仕様記述言語に対して，そうではないモデル検査ツールを採用することには懸念があった．

しかし今回の適用では以下の理由から形式的仕様記述言語ではなくモデル検査を採用することにした．

IC カードと R/W という 2 つのプロセス間のメッセージ交換を SPIN により簡易に記述できるだけでなく網羅的にシミュレーションできる．

状態モデルによって，IC カード発行前，使用中，ロック中などの R/W による IC カードの操作状況ならびに，使用中やロック中などの鍵状態，パスワードによる IC カードの認証状態，ファイル状態など IC カード内の資源状態を容易に記述できる．

セキュリティターゲット ST として作成したセキュリティ評価対象 TOE に対する IC カードの状態モデルと R/W の状態モデルの下で，LTL 式で記述したセキュリティポリシーに関する検証式を満足することをモデル検査によって証明できる．

モデル検査ツール SPIN の知識を習得した形式手法の専門家としての研究者がいた．

◆形式手法によるセキュリティ要求の検証手順

形式手法を用いた IC カードシステムのモデリングでは，**表 -2** に示すように，検証対象としてのセキュリティターゲットの抽出，評価対象モデルと環境モデルの定義，形式手法ツールによるモデル検査という手順で実施した．

検証対象として ADV の観点からセキュリティターゲットならびに TOE 設計と TOE 実装を抽出した．このとき保護すべき資産を特定して資産に対する脅威分析と対策を明らかにする．この対策に基づいてセキュリティ機能要求 SFR と対応するセキュリティ機能 TSF を定義する．TSF に基づいて TOE 設計ならびに TOE 実装を作成する．ただし TOE 設計と TOE 実装で検証対象とするのは TSF と関連する部分だけであり，関連しない部分については省略することが認められている．

［手順 1］TSP 仕様の作成

TSP 仕様ではセキュリティ特性とセキュリティ規則を定義する．

セキュリティ特性として IC カードの運用ライフサイクルならび，IC カード内のレジスタ，変数，認証フラグなどのデータやコマンドなどの機能とファイルや鍵などを定義する．

セキュリティ規則としてファイル操作とコマンド実行の事前条件，変数と内部的な振舞いの変化，事後条件を定義する．

［手順 2］TSP 状態モデルの作成

TSP の状態モデルでは TSP 仕様に基づいて AP 仕様と不変特性を定義する．

AP 仕様ではセキュリティ特性とセキュリティ規則を定義する．セキュリティ特性では外部ユーザ，配布鍵，IC カード運用フェーズなどの IC カードの外部環境の特性とコマンド機能，ファイル，暗号鍵などの IC カード内部の特性に基づいて環境状態モデル（環境モデル）と IC カード状態モデル（TOE モデル）を定義する．セキュリティ規則では，コマンド系列や鍵配布規則などを定義する．TOE モデルと環境モデルの関係を**図 -2** に示す．以下で述べるように，環境モデルと TOE モデルをそれぞれ R/W プロセスと IC カードプロセスに対応させることで SPIN によるモデル検査を実施できることになる．

不変特性として，セキュリティ特性の組合せ，リスク，資源のデッドロックを定義する．セキュリティ規則と不変特性に基づいて検証式を作成する．

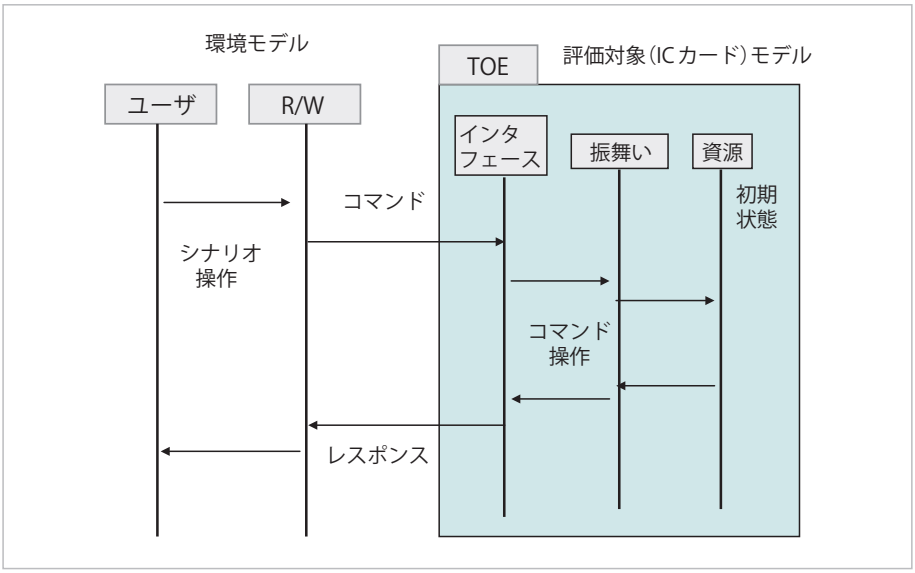

図 -2　環境モデルと評価対象モデルの関係

［手順 3］リスク定義

まず“X だけが…できる”という TSP 記述に対して，“X 以外のだれでも…できる”という否定的な記述を作成することで系統的に TSP に対するリスクを定義することができる．

次に IC カードシステムの構成要素の状態の組合せに対して不変特性に基づいてリスク状態を定義する．たとえば，IC カードのセキュリティ状態が認証済み，鍵状態がロック中，IC カード内のファイル状態が書込み可能などの組合せに関するリスクを定義する．ただし複数の鍵やファイルがあるので網羅的に調べる必要がある．

このリスク定義に基づいて，次に述べるようにして，環境モデルと TOE モデル間のメッセージ交信の過程で IC カードシステム構成要素の状態の組合せがリスク状態に到達しないことを SPIN によって形式的に検証することができる．

［手順 4］検証

検証の実演では，認証機関に対して以下の 5 つの要件を示す必要があった．

【要求 1】TSP モデルに矛盾がないこと

【要求 2】TSP の規則および性質が TSP モデルに対応していること

【要求 3】TSP の振舞いモデルが矛盾しないこと

SFR に対して TSP モデルが完全であること

【要求 4】すべての TSP が SRF で表現されていること

【要求 5】セキュリティポリシーが SF によって実装されていること

要求 1，2，4，5 については作成した TSP モデルをレビューすることによって示す．

要求 3 に対して形式手法ツール SPIN を用いて以下の 2 条件を証明する．

（条件 1）TSP モデルがリスク状態に到達しないこと

（条件 2）TSP モデルが必要な状態に到達すること

具体的には，環境モデルに対して R/W プロセス，TOE モデルに対して IC カードプロセスを定義する．R/W プロセスでは，IC カードユーザを変更する手続きと IC カードにコマンドを送信しレスポンスを受信する手続きを用意する．IC カードプロセスでは R/W プロセスからコマンドとパラメータを受信する手続きと，R/W プロセスにコマンドのレスポンスを送信する手続きを用意する．ただし，これらの手続きでは，セキュリティ要求に関する処理だけを記述することを注意しておく．

これらの手続きはコマンドごとに異なるが IC カードの操作シナリオには共通する処理が多いことから，**表 -3** に示すような共通テンプレートを用意することにより，promela 記述作業の軽減を図った．

分類	R/W プロセス	IC カードプロセス
振舞い	主制御処理 コマンド送信処理 レスポンス受信処理 ユーザ変更処理	主制御処理 コマンド受信処理 コマンド対応処理 レスポンス送信処理 認証処理 アクセス制御処理 ファイルアクセス処理
インタフェース	コマンド処理 レスポンス処理	コマンド処理 レスポンス処理
資源	なし	鍵 ファイル 許容エラー回数
初期状態	なし	エラーカウンタ状態 ライフサイクル状態

表 -3　共通テンプレートの例

これにより R/W プロセスの記述ではシナリオ対応処理，ユーザによるコマンド操作処理，ユーザと外部環境の状態を記述するだけで，コマンドの送受信処理を記述する必要がなくなった．IC カードプロセスの記述では，基本となるコマンド処理はすべてテンプレートで用意したので，開発者が必要に応じて追加したコマンドとそのパラメータ，レスポンスならびに対応する資源，エラー処理と初期状態だけを記述することになった．このような共通化を図ったことにより，モデルの記述規模は SPIN のソースコードのステップ数で約 0.5K 行となった．

◆プロジェクト管理上の留意点

次に，形式手法を適用する場合のプロジェクト管理的側面として，チーム構成，形式手法の教育，内部レビュー，外部とのコミュニケーションの留意点について説明する．

形式手法の適用チームには，セキュリティターゲットを作成したセキュリティ専門家，形式モデルを作成した形式手法の専門家と IC カードシステムの開発者が参加した．

しかしセキュリティ専門家とシステム開発者には形式手法についての知識がなかったため，これらの技術者に対して形式手法の専門家が形式手法をまず教育した．

TOE モデルに基づいて形式モデルが作成された段階で各参加者の役割に応じて次のような観点から内部レビューを実施した．セキュリティ専門家は ST，TSP，CC 要求の観点から形式モデルの妥当性を確認した．形式手法専門家は，形式化と論理的合理性の観点から形式モデルの妥当性を確認した．システム開発者は TOE 設計と実装の観点から形式モデルの妥当性を確認した．

外部の認証機関とのコミュニケーションでは，どのような形式手法を選択するかについて合意することと，形式手法によって作成された TSP モデルが ADV_SPM.3 の条件を満足することの証明手順と証明結果を承認してもらう必要がある．

なお形式手法の適用期間をまとめると，学習，モデリング，実装を含めて 3 人体制で約 2 年だった．また実施工数については 3 人の技術者を平均して約 25％稼働だったので 3 人× 2 年× 0.25 = 1.5 人年である．この中には上述した欧州の認証機関との交渉も含んでいる．

今後の展望

本稿では，実践的なセキュリティ要求工学にはどのような知識が求められるのかについて具体的な事例に基づいて紹介した．上述したように，セキュリティ要求工学の投資対効果，セキュリティ要求獲得，仕様化，要求確認，要求管理だけでなく，通常の要求工学との統一も必要である．また抽象資産で示したようにゴール指向要求工学との関係の整理についても明確化する必要がある．さらに形式手法とのシームレスな統合の可能性も見えてきていることを示した．

しかし一般のシステム開発の現場にセキュリティ要求工学を導入していくためには，逆説的だが，ユビキタスコンピューティングでも社会の中にコンピュータが浸透することでコンピュータが見えなくなったように，セキュリティ要求工学をソフトウェア開発ツールの中に埋め込んで隠蔽することにより開発現場から見えなくすることも重要な課題である．意識しなければ使えないうちは技術としての成熟度がまだ低いのではないだろうか．ということはまた，研究の余地が大きいということでもあるので，この分野の研究開発が加速することを期待している．

筆者の力不足から，本稿ではこれらの課題を統一的な視点からロードマップ化することはできなかったが，セキュリティ要求工学が持つ現場導入への豊かな可能性については紹介できたのではないかと思う．いずれにしても上述したような課題をシームレスに解決できるような実践的セキュリティ要求工学とその環境が開発されることを期待する．

参考文献

1) Allen, J. H. : Making Business-Based Security Investment Decisions -A Dashboard Approach, https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/985-BSI.html
2) Shields, http://er-projects.gf.liu.se/~shields
3) Jaatun, M. G. and Tondel, I. A. : Covering Your Assets in Software Engineering, http://www.sintef.com/upload/IKT/9013/security/assets.pdf
4) 神戸雅一，桑田義隆，山本修一郎：RFID システムのビジネス適用におけるプライバシー保護に関する考察，人工知能学会研究会(2006)．
5) Ichihara, N., Kamoda, H. and Oguro, H. : Smartcard Security Development Using Formal Method Tool SPIN, 9th International Common Criteria Conference (2008), http://www.ssi.gouv.fr/en/confidence/certificats.html
6) Whitlock, S. T. and Dream, G. : Can the Twins Save Our Data?, https://www.opengroup.org/conference-live/uploads/40/17709/Mon_-_am_-_3_-_Whitlock.pdf

(平成 20 年 11 月 14 日受付)

山本 修一郎(正会員)　▶yamamotosui@nttdata.co.jp

1977 年名古屋工業大学情報工学科卒業．1979 年名古屋大学大学院工学研究科情報工学専攻修了．同年日本電信電話公社入社．2002 年（株）NTT データ 技術開発本部 副本部長．2007 年同社初代フェロー，システム科学研究所 所長．ソフトウェア工学，ユビキタスコンピューティング，知識創造デザインの研究に従事．本会業績賞，通信協会前島賞など受賞．博士(工学)．著書に，「IC カード情報流通プラットフォーム」(電気通信協会，2001)「要求定義・要求仕様書の作り方」(ソフト・リサーチ・センター，2006)「〜ゴール指向による〜システム要求管理技法」(ソフト・リサーチ・センター，2007) などがある．人工知能学会知識流通ネットワーク研究会主査(2007 〜)．電子情報通信学会，日本ソフトウェア科学会，人工知能学会，ACM，IEEE 各会員．