特集

セキュリティ要求工学の実効性

編集にあたって

吉岡 信和　　田口 研治
国立情報学研究所

本特集では，システム開発における要求獲得・分析工程において，セキュリティ要件をいかに獲得・分析するかについての方法論を中心に，企業におけるセキュリティへの取り組みを含めて現在の状況を概説する．セキュアなシステムの開発は現代社会にとり，非常に大きな課題であるが，必ずしも開発現場においては，そのための方法論が積極的に導入されているわけではない．そのため本特集では，まずセキュリティ要求工学の概論を紹介したのち，方法論の紹介を行い，後半では，企業における事例や研究例を紹介し，その実効性について論じる．

方法論としては，SQUAREと，セキュアトロポスとKAOSを取り上げた．これは，プロセス指向，エージェント指向，ゴール指向という3つのパラダイムを代表する方法論を取り上げることで，さまざまな異なるアプローチを概観できることを目指している．本特集では，それらを，各方法論の提案者自身と我が国の事情に詳しい日本人研究者との共同で執筆することにより，読者にとって分かりやすい解説となることを狙った．さらに，後半の事例紹介では，企業の第一線で活躍されている方々に解説いただいた．このような取り組みは世界でも例をみない試みであると思う．

本特集は，次の８つの観点からの解説となっている．

まず，「セキュリティ要求工学の概要と展望」（吉岡とBashar Nuseibeh氏）として，セキュリティ要求工学の必要性，定義，そして，その課題を整理している．セキュリティ要求工学は，セキュリティに関する要求工学であり，通常の要求工学と同様の部分も存在するが，複雑性や変化，トレードオフなど独自の難しさも存在する．本稿でこれらを整理し，以下の解説記事のガイダンスとなっている．

「SQUAREではじめるセキュリティ要求工学」（Nancy R. Mead氏と吉岡）では，セキュリティに関するシステムの品質を高めるためのプロセスモデルであるSQUAREを紹介している．これは，カーネギーメロン大学で開発された，セキュリティ要求を獲得し，分類，優先度付けするための９つの手順を規定している．

「セキュアトロポス（Secure Tropos）概論」（Haralambos Mouratidis氏と田口）においては，セキュリティ要件の獲得・分析方法論の１つであるセキュアトロポスについて，事例を基に紹介している．本方法論は，アクターとその間の依存関係とその関係上のセキュリティの制約を記述することで，対象システムに関するセキュリティ要件の獲得･分析を行うという特徴を持つ．基本であるアクター図とゴール図を用いていかにモデル化を行うかについて説明を行っている．

「KAOSによるセキュリティ要件の獲得・分析」（田原康之氏，Axel van Lamsweerde氏，Emmanuel Letier氏）では，ゴール指向要求分析方法論であるKAOSによるセキュリティへの取り組みについて，通常のゴールの概念の逆である攻撃者の持つ反ゴールを考慮した反モデルによる手法について説明している．

「実践的セキュリティ要求工学に向けて」（山本修一郎氏）では，投資対効果の評価手法，セキュリティ要求工学プロセスの事例，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，主に海外での取り組み事例について解説している．そして，現場で使える実践的セキュリティ要求工学とは何かを論じている．

「日本ユニシスにおけるエンタープライズ・セキュリティ・アーキテクチャ（ESA）」（平岡昭良氏）においては，企業が戦略的に情報セキュリティに取り組むためのフレームワークとしてのエンタープライズ・セキュリティ・アーキテクチャについて自社の取り組みを紹介している．セキュリティガバナンスから始まり，情報セキュリティ対策，セキュリティ組織レイヤなど，非常に詳細かつ体系的に，企業としてのセキュリティ活動について説明している．

「コモンクライテリアにおけるセキュリティ要求の規定の現状と課題」（金子浩之氏）では，IT製品に関するセキュリティ保証の国際標準であるコモンクライテリアに関する現場の状況と，実際のシステム開発における要求工学からのセキュリティ保証へのアプローチについて，ミスユースケースを用いたモデル化手法を基に論じている．

「企業におけるセキュリティ分析技術の実効性」（大久保隆夫氏）では，企業のソフトウェア開発におけるセキュリティ要求分析，設計の現状と課題について論じている．特に，実用的なセキュリティ分析手法として提案されている脅威モデリング手法に関して，その有効性と問題点について議論している．

この特集は，筆者らが中心に国立情報学研究所GRACEセンターで行っているセキュリティソフトウェア工学に関する研究プロジェクト[☆1]の成果の１つでもあり，お願いした執筆者のほとんどは，このプロジェクトで開催されたチュートリアル・シンポジウムの講演者である．特に2008年６月に行ったセキュリティ要求工学に関するシンポジウムでは，Bashar Nuseibeh氏，Nancy R. Mead氏，Emmanuel Leiter氏，山本修一郎氏らとでパネルディスカッションを行い，本特集の内容はその議論結果をふまえた内容となっている．これをきっかけに，セキュリティソフトウェア工学に関する研究，および，その実践が進み，IT技術を活用した安全・安心な世界を実現する助けになれば幸いである．

（平成21年２月９日）

☆1 http://www.grace-center.jp/prj_sse.html