博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　CC-Case：セキュリティ要求分析・保証の統合手法
申請者　：　金子 朋子
審査委員会　：　主査　教授　田中 英彦
副査　教授　佐藤 直
副査　教授　後藤 厚宏
副査　教授　土井 洋

Ⅰ．論文内容の要旨

本論文は、「CC-Case：セキュリティ要求分析・保証の統合手法」と題し、８章と参考文献、更に付録からなる。一般にシステム開発において、要求分析をしっかりおこない後戻りの少ない設計を行う事は重要なポイントであるが、これはセキュアなシステム開発に於いては更に大切で、システム開発の成功を導く重要な要素である。しかし、従来、要求分析段階におけるそのための十分な手法が開発されているとは言い難い。この論文は、セキュアなシステム開発のための要求分析段階における、十分な脅威分析と対応手法の検討を可能にするとともに、顧客の合意プロセスとセキュリティに関する品質保証を与えることが可能な手法を提案し、その可能性を検討したものである。

第１章は「序論」で、セキュリティ要求分析を行う場合の問題点、更に、その分析結果に基づいて対策を講じる場合のセキュリティ保証のあり方、及び、システム開発における様々なリスクについて述べている。

第２章は、「研究の背景」で、セキュリティ要求分析手法として従来の研究を概観し、特に、i*-Liu 法、アクタ関係表、アシュアランスケース、セキュリティケース、及びセキュリティ評価の国際標準 Common Criteria(CC)について述べている。

第３章は、「CC-Case の全体像」で、この論文で検討するシステムセキュリティの課題をまとめた後に、提案手法 CC-Case を定義し、その目的を述べている。すなわち、CC-Case は、セキュリティ要求分析を実施するとともに、CC 準拠の保証を与える、セキュリティ要求と保証の統合開発方法論である。開発におけるセキュリティ対応をする上での課題が要求獲得段階の技術的な困難性にあり、それが、扱う情報の複雑性、状況の変化、更に他の要件とのトレードオフを考慮する必要性、などに起因すると分析している。それらに対して、本論文では、要求分析には、CC を用いたプロセスの明示化、機能要件の利用、セキュリティアクタ関係表の提案で対応し、更に、保証問題には、アシュアランスケースと CC を用いて対応することを提案している。
また、システムのライフサイクルを考慮すれば、開発の要求分析段階のみならず、設計、実装、運用段階に対するサポートが必要であるが、CC-Case の出力が証跡であることに鑑み、それらを集めたデータベースを使いまわすことでライフサイクルに跨る手法として発展させる可能性についても触れている。

第４章は「要求段階の CC-Case」で、要求分析と対策を立案する段階における CC-Case の詳細について述べたもので、まず、全体像を与え、入力データと分析を進めるプロセス、更にその出力としての証跡について示めすとともに、CC で用いられるセキュリティ目標（ST）や、適合性、セキュリティ課題定義、対策方針、セキュリティ要件などの文書と、本提案手法との対応関係について対応を論じている。次に、この段階の最上位のゴールを「CC-Case で作成されたセキュリティ仕様はセキュアである」と設定し、CC を前提として、セキュ

リティ仕様の妥当性を論証することにより、そのゴールを 3 つのサブゴールに分解している。すなわち、セキュリティコンセプト定義と、セキュリティ対策立案、並びにセキュリティ要約仕様という３つをセキュアに作成する小問題への分解となるが、更にその分解を進めて、それぞれの作成作業を分析することで詳細な作業プロセスを導出している。その分解の途中で、適当な箇所に顧客との合意プロセスを挿入している。この分解の最終段階は、作業結果を記述したものとなり、それは作業の証跡として機能する。すなわち、この分解の手続きは、アシュアランスケースをセキュリティ分析に適用したものであって、結果として、CC に適合した作業になっている。この章では更に、この手法を具体的な事例に適用し、得られた分析結果を詳細に与えている。

第５章は「アクタ関係表による脅威分析と CC 対応」で、要求分析における関係者としてのステークホルダを、サーバ管理者、オペレータ、ユーザ、攻撃者などとし、それらを表の縦と横に配置し、ステークホルダ間の関係をその対応欄に記述することで脅威分析をする手法 SARM について述べたものである。SARM の機能を限定するとグラフ図で分析する手法 i*Liu 法と等価になるが、これらの間の変換プログラムを用意することで両者の良いとこ取りをするスパイラルレビュー手法を提案している。また、11 名によるこの手法利用の評価を行い、手法の有効性を示している。CC-Case では、これをセキュリティ要求分析における脅威分析手法として用い、分析の容易化や網羅性を強化している。

第６章は「ケーススタディ」で、本手法を具体的な一つ事例に適用し、その分析結果をしめしている。

第７章は「考察」で、３章で分析したセキュリティ要求分析の問題点が、CC-Case によって如何に解決されているかを詳細に検討したもので、要求獲得の困難性対策、CC 準拠による保証、システム運用時のトラブル解決、CC それ自体の利用困難性の解決、アシュアランスケースの課題解決、などのポイントについて考察し、本提案の有効性を主張している。

第８章は、「結論」で、検討のまとめと今後の課題を述べている。

Ⅱ. 論文審査結果の要旨

これを要するに本論文は、セキュアなシステムを開発する場合の重要な段階であるセキュリティ要求分析における課題を解決するために、脅威分析には表形式手法を用い、要求分析と対策立案には CC とアシュアランスケースを融合させることで、要求分析段階における、十分な脅威分析と対応手法の検討を可能にするとともに、顧客の合意プロセスとセキュリティに関する品質保証を与えることが可能な手法を提案したもので、実際的な手法として評価でき、情報学に貢献するところが少なくない。

よって、本論文は、博士（情報学）の論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、平成 26 年 1 月 31 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。