氏　　名	宝　達
博士の専攻分野の名称	博士（工学）
学位記号番号	博理工甲第 1135 号
学位授与年月日	平成 31 年 3 月 20 日
学位授与の条件	学位規則第 4 条第 1 項該当
学位論文題目	Supporting Environment for IT System Security Evaluation based on ISO/IEC 15408 and ISO/IEC 18045 （ISO/IEC 15408 および ISO/IEC 18045 に基づく IT システムのセキュリティ評価のための支援環境）
論文審査委員	委員長　准教授　後藤　祐一 委　員　教　授　吉田　紀彦 委　員　教　授　吉浦　紀晃 委　員　准教授　大久保　潤

論文の内容の要旨

The standardization of IT system security is always a common issue all over the world. The security of a system is only as strong as the weakest link. For software engineering, the “link” means each task in different process, such as design, implementation, test, operation, maintenance and so on. The whole security of IT systems can be guaranteed only when each task has been performed properly according to consistent standard.

ISO/IEC 15408 and ISO/IEC 18045 are a pair of international standards for information security evaluation. Rigorous evaluation based on the two ISO standards provides a unified way of comparisons among IT systems, such that the developers can rationally show the security strength of their products and the customers can easily choose suitable systems according to the evaluation results. ISO/IEC 15408 and ISO/IEC 18045 establish a trustworthy relationship with common basis among all stakeholders of the target system, wherefore ISO/IEC 15408 and ISO/IEC 18045 are widely used as national standard all over the world.

Security evaluation based on ISO/IEC 15408 and ISO/IEC 18045 is very complex. The whole security evaluation process can be summarized as evaluators receive the evaluation evidence from the developer performs the evaluation activities and provides the results of the evaluation assessment. Evaluators perform evaluation activities to verify whether the target system complies with ISO/IEC 15408 and ISO/IEC 18045. Although, two ISO standards have given a set of instructions to guide the evaluation activities and specified detailed procedures how to carry out those activities. It is not clear enough and difficult even for experienced evaluators to accomplish the security evaluation. The security evaluation process involves tens of documents and a wide variety of tasks. Such heavy work shall cost lots of time and complex evaluation activities may cause evaluators making mistakes. Moreover, to manage a lot of intermediate data in evaluation process is difficult even for experienced evaluators. It is also difficult to ensure that evaluation is fair and transparent. Although each evaluator tries to evaluate a target system earnestly, evaluation results may be different

among evaluators because of evaluators' biases. These issues not only may result in consuming a lot of time, but also may affect the correctness, accuracy, and fairness of evaluation results. Thus, it is necessary to provide a supporting environment that supports all relevant tasks in the evaluation process to reduce the complexity of all evaluators' work and guarantee the quality of evaluation results at the same time. However, there is no such environment existing until now.

This thesis presents a supporting environment for IT system security evaluation based on ISO/IEC 15408 and ISO/IEC 18045 that integrates various supporting tools to perform a complete process of security evaluation on the target IT system. This supporting environment can provide facilities for evaluators to perform all tasks in the evaluation process in a guided order. This supporting environment can promote each task with locating the relevant contents in tens of documents and providing helpful information or functions for evaluators to determine whether these relevant contents are up to the standard. The supporting environment can provide facilities for evaluator to manage all evaluation-relevant documents, intermediate information and their reviews on the target systems during the evaluation.

To provide full facilities for performing the security evaluation process, we firstly analyzed the whole security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045 and clarified 674 necessary evaluation tasks. We also clarified the procedure and detailed actions for each task. Under the consideration that tasks with similar procedural pattern can be supported by the same method, we then classified the detailed evaluation tasks into 7 groups according to the pattern in the procedures and proposed appropriate supporting methods for each group of evaluation tasks. According to these supporting methods, we designed and implemented each necessary supporting tool. Considering the complicated relationship among various evaluation tasks, we clarified the sequence of evaluation tasks and implement a supporting tool to guide evaluators perform all tasks in right order. We analyzed all evaluation-relevant documents, intermediate information and evaluators' reviews, and then designed matched formats to transfer this information into structured data that can be easily managed and used in the evaluation process.

We then evaluated the completeness, usability and efficiency of the evaluation supporting environment. We proposed an evaluation method to show the completeness of this supporting environment and evaluated it at design level and implementation level based on the method. We then discussed how this supporting environment is capable and useful to provide comprehensive facilities to perform all tasks in evaluation base ISO/IEC 15408 and ISO/IEC 18045. We also show the efficiency of this supporting environment by comparing the consumed time between evaluation with this supporting environment and a normal evaluation.

論文の審査結果の要旨

IT システムの情報セキュリティ機能の標準化は世界中で常に共通の課題である。ISO/IEC 15408 と ISO/IEC 18045 は IT システムの情報セキュリティ評価のための国際規格である。両規格に基づく厳密な評価結果は異なる IT システムを比較する根拠となり、評価対象のシステムに関わる関係者たちの間で共通の信頼度を得られる。このため、ISO/IEC 15408 と ISO/IEC 18045 は世界中で様々な国の政府標準規格として広く使用されている。

ISO/IEC 15408 および ISO/IEC 18045 に基づく評価は非常に複雑なプロセスである。両規格において、一連の評価作業について抽象的な指示と実行方法の方針が説明されているが、その説明は十分ではないため経験豊富な技術者でも理解するのは困難である。また、セキュリティ評価プロセスには数十の文書と様々な作業が含まれるので評価を行うために多くの時間が必要となる。さらに、評価のための種々の作業において評価者はミスを犯す可能性が十分にある。その上、各評価者は評価対象を真剣に評価しようとしても、思い込みや偏見により評価結果が異なる可能性もあり得る。これらの問題は、多くの時間を費やすだけでなく、評価結果の適切性、正確性および公平性にも影響を与える可能性がある。 したがって、すべての評価者の作業の複雑さを軽減し、同時に評価結果の品質を保証するために、評価プロセスを支援する工学環境が提供されなければならない。 しかし、今までそのような支援のための工学環境は存在しない。

本論文は、IT システムの国際評価基準である ISO/IEC 15408 および ISO/IEC 18045 に基づく IT システムの評価プロセスにおいて評価の公平性、正確性、適切性を保証し、かつ、評価に費やされる時間的コストを削減するために、評価プロセスを支援する工学環境の開発について、著者の研究を通じて得た知見と成果を述べるものであり、6 章から構成されている。

第 1 章では、本研究の背景、目的、および位置付けについて述べた。ISO/IEC 15408 および ISO/IEC 18045 に基づく IT システムの評価フレームワークについて概観し、ISO/IEC 15408 および ISO/IEC 18045 を用いた先行研究調査について述べ、本研究の目的として、IT システムの評価プロセスにおいて評価の公平性、正確性、適切性を保証するために、評価プロセスを支援する工学環境を開発することを定めた。

第 2 章では、ISO/IEC 15408 および ISO/IEC 18045 に基づく評価における課題について述べた。まず、ISO/IEC 15408 および ISO/IEC 18045 の説明および評価プロセスに関連する諸概念について概観した。その後、評価プロセスにおける課題を列挙し、特に評価の公平性、正確性、適切性を保つことが難しいこと、また、評価に多くの時間を費やす必要があることを述べた。

第 3 章では、ISO/IEC 18045 で規定されている評価タスクに対する計算機を用いた支援方法について述べた。ISO/IEC 18045 では IT システムの開発や運用における 7 つの活動に対して 493 の評価タスクを規定している。しかし、これらの評価タスクは明示的あるいは暗黙的な複数の作業から成り立っており、計算機で直接的に支援するのは難しい。また、これらの評価タスクの実行順序は ISO/IEC 18045 では明示的に示されていない。さらに、評価タスクと評価に関わる関連文書、目的別に行うべき評価タスクを定めた評価保証レベル（EAL）の関係も複雑であり、評価者にとって理解が難しい。そこで、まず、493 の評価タスクを評価に関わる関連文書に対する単純な作業 674 個に分割した。そして、これらの作業を 7 つの活動および EAL に基づき分類した。また、これらの単純な作業には対象とする関連文書は異なるものの、その文書に対する作業手順が共通しているものがある。そこで、作業手順に着目し、単純な作業を作業パターンごとに 7 つに分類した。そして、作業パターンごとに計算機での支援方法を提案した。この計算機による支援により、評価者のミスや思い込み・偏見による不公正、間違い、不適切な判断を防ぐことがで

きる。また、計算機での支援により、評価にかかる時間を削減することが可能となる。

第４章では、ISO/IEC 15408 および ISO/IEC 18045 に基づく評価プロセスの支援環境の実現について述べた。支援環境は第３章で列挙した７つの支援方法を実現するツール、評価タスクを適切な順番で実行することを強制する順序制御部品、そして、関連文書や ISO/IEC 15408 および ISO/IEC 18045 を格納するセキュリティ評価データベースから成り立っている。また、関連文書および ISO/IEC 15408 および ISO/IEC 18045 を機械可読文書にするため XML に基づく文書形式を定義し、定義した形式に基づきセキュリティ評価データベースに格納している。本研究では支援環境実現の第一歩として、EAL１で定義されているすべての評価タスクについて支援を行えるように支援環境を実装した。

第５章では、実装した支援環境について支援可能な評価タスクのカバー率および、評価タスク実行時の効率性、支援環境の使いやすさの観点から評価を行い、その有用性を示した。

最後に、第６章では、本研究で得た成果と知見をまとめ、残された研究・開発課題を示した。

なお、本論文の主な内容は、既に７編の学術論文として、国際学術論文誌（Springer Lecture Notes）（４編）、および査読付きの IEEE 学会国際会議論文集（３編）において公表され、あるいは公表が決定されている。

以上のように、本論文は、IT システムの国際評価基準である ISO/IEC 15408 および ISO/IEC 18045 に基づく IT システムの評価プロセスにおいて、計算機の支援により評価者のミスや思い込みによる不公正、間違い、不適切な判断を防ぎ、かつ、評価に費やされる時間を削減するための評価プロセス支援環境の提案、設計、プロトタイプの実装を行い、また、支援環境の有用性について示した。これらの研究成果は、情報セキュリティ工学分野にとって新しい知見を示し大きく貢献するものである。従って、当学位論文審査委員会は、本論文が、博士（工学）の学位を授与するに十分値するものと判定した。