氏　　名	堀江　大輔
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 734 号
学位授与年月日	平成 21 年 3 月 24 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	Development of ISEE: An Information Security Engineering Environment （情報セキュリティ工学環境 ISEE の開発）
論文審査委員	委員長　教　授　程　京徳 委　員　教　授　大澤　裕 委　員　教　授　吉田　紀彦 委　員　准教授　吉浦　紀晃

論文の内容の要旨

An information security engineering environment is needed for supporting continuous and consistent the tasks. An intrinsic difficulty in ensuring security of information systems is that crackers are active persons who can get knowledge day after day and then continuously attack target systems always with new techniques. Therefore, it is important to continuously perform what not only in design and development but also in management, maintenance, and abolition. Moreover, the whole security of a system is only as strong as the weakest link: the most vulnerable component in systems. Each task should be performed according to consistent standards for ensuring the whole security of a system. It is required to support continuous and consistent design, development, management, maintenance, and abolition of security facilities of information systems.

There have been no environment that can support continuous and consistent design, development, management, maintenance, and abolition of security facilities. In software engineering, some software engineering environments are developed and used for supporting design and development of information systems with high reliability requirements. However, these software engineering environments are specialized in ensuring reliability of systems. The environments do not support to rapidly add and improve security facilities in management, maintenance, and abolition of developed systems. Moreover, the environments do not ensure the whole security of a system, because the environment supports each task and development of each component according to individual methods or standards. Therefore, the environments are not enough to support continuous and consistent design, development, management, maintenance, and abolition of security facilities. In information security engineering, databases that can support development of authentication systems and management of security specifications are developed and used. However, the databases are specialized in supporting a particular function in security facilities or a particular task in design, development, management, maintenance, and abolition of security facilities.

We propose an information security engineering environment, named ``ISEE'' to support continuous and consistent design, development, management, maintenance, and abolition of security facilities. This thesis presents our basic considerations on ISEE, its requirement analysis, design, prototype implementation, and evaluation.

We defined concrete policy for developing ISEE to support continuous and consistent design, development, management, maintenance, and abolition of security facilities. ISEE supports not only design and development of security facilities but also management, maintenance, and abolition of them. For supporting consistently performing the tasks, each the task should be performed according to consistent standards. Therefore, ISEE forces users to perform the tasks according to rules of ISO standards and formal methods. Moreover, ISEE forces users to rapidly and repeatedly the tasks in appropriate sequence.

To define requirements for ISEE, we clarified detailed tasks in design, development, management, maintenance, and abolition of security facilities. We also clarified ISO standards for the tasks and a sequence of the tasks. ISEE should continuously and consistently support the tasks according to the sequence and standards. We then defined requirements for ISEE according to the tasks, the standards, and the sequence.

We designed ISEE satisfying the requirements. ISEE consists of a central database system, named ``ISEDS (An Information Security Engineering Database System),'' and some tools. ISEDS manages the data of security facilities and ISO standards for security. The support tools also support to create, verify, validate, and review documents for security facilities. We then implemented some components of ISEE: ISEDS, a security target generation tool, and a security target verification tool according to international standard ISO/IEC 15408. Current ISEDS can manage and retrieve data of security requirements provided by the standard and published/personal cases described on security targets. The security target generation tool can generate templates of security targets from certified security targets according to the standards. The security target verification tool can support verifying design specifications described on security targets with security requirements defined on ISO/IEC 15408. We then evaluated cost, usability, power, a standard that assure minimum security, applicability of international standards, applicability of formal methods, and propriety of sequence of ISEE.

This thesis is organized as follows. Chapter 1 presents the background, motivation, and purpose of this research, and related works. Chapter 2 explains the concept of an information security engineering environment. Chapter 3 presents a requirement analysis of ISEE. Chapter 4 presents a design of ISEE. Chapter 5 presents an implementation of ISEE. Chapter 6 presents an evaluation of ISEE. Concluding remarks are given in Chapter 7.

論文の審査結果の要旨

インターネットの普及と情報化社会の高度化に伴って、情報システムに対する安全性要求がますます高まっており、今日、ほとんどの情報システムの設計と開発においては、情報セキュリティに対する要求を考慮しそれらを保証する機能を実現しなければならない状況になってきた。また、高安全性が要求される情報システムにおいては、次々と新たな攻撃方法を編み出す攻撃者の存在を常に考慮しなければならない。このため、高安全性情報システムが一定以上の安全性を保つために、その設計や開発だけなく運用や保守や廃棄をも一貫してかつ継続的に行わなければならない。しかし、現在、これらの作業を一貫してかつ継続的に行う系統的な方法論がまだ確立されておらず、支援する環境も全く存在していなかった。

本論文は、情報システムのセキュリティ機能の設計から開発、運用、保守、廃棄までを、一貫してかつ継続的に支援する情報セキュリティ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、５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。まず、情報システムにおけるセキュリティ機能を保つことにおける難しい課題を列挙し、ソフトウェア工学および情報セキュリティ工学における従来の関連研究を概観した。そして、高安全性情報システムにおけるセキュリティ機能の設計から開発、運用、保守、廃棄までを一貫してかつ継続的に行うことの必要性を述べ、本研究の目的として、情報セキュリティ機能の設計から開発、運用、保守、廃棄までを一貫してかつ継続的に支援する情報セキュリティ工学環境を開発することを定めた。

第２章では、従来のソフトウェア工学環境により提供されている技法とツールは、情報セキュリティ工学の観点から見ると、高安全性情報システムが一定以上の安全性を保つことにとって不十分であることを指摘し、本研究の基礎である、情報セキュリティ工学環境という新しい概念を提案した。情報セキュリティ工学環境は、情報システムにおけるセキュリティ機能の設計から開発、運用、保守、廃棄までの全ての作業を、一貫性および継続性の観点から支援する技法とツールを統合する環境であり、高安全性情報システムが一定以上の安全性を保つことに役に立つと期待される。

第３章では、ISO 国際規格に基づく情報セキュリティ工学環境 ISEE (Information Security Engineering Environment) の設計について述べた。まず、ISEE の開発に関する基本的な考え方を述べた。次に、ISEE の支援対象である情報セキュリティ機能の設計、開発、運用、保守、廃棄の作業および作業手順を明確にしたうえ、ISEE の要求定義および機能設計を述べた。

第４章では、情報セキュリティ工学環境 ISEE の実現と評価について述べた。まず、ISEE の中核的なコンポーネントである、様々な ISO 国際規格および関連文書を格納する情報セキュリティ工学データベースシステム ISEDS の実現と評価について述べた。次に、対象システムに関するキーワードに基づき、検証済みのセキュリティ機能設計仕様書から、対象システムのセキュリティ機能設計仕様書の雛形を自動的に生成するツール GEST の実現と評価について述べた。更に、ISO 国際規格 15408 を妥当性基準として対象システムのセキュリティ機能設計仕様書を形式的手法を用いて検証するための支援ツール FORVEST の実現と評価について述べた。

最後に、第５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８編の学術論文として、学会論文誌や査読付きの国際会議論文集において公表され、あるいは、公表が決定されている。

以上のように、本論文は、情報システムのセキュリティ機能の設計から開発、運用、保守、廃棄までを一貫してかつ継続的に支援するために、情報セキュリティ工学環境という新しい概念を提案し、世界最初の情報セキュリティ工学環境である ISEE の設計、実現、評価について述べた。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。