プロジェクト名：　国際標準に基づく汎用的情報セキュリティ工学環境の構築

プロジェクト代表者：　程 京徳（大学院理工学研究科・教授）

１．研究の目的

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、悪意のある攻撃者らの知識や技能も時間と共に増えるので、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。情報システムの設計者、開発者、運用者、保守者は、責務として、システムに情報セキュリティ機能を実装するばかりではなく、システムが攻撃を受けたとき、情報セキュリティ機能が適切かつ迅速に動作することを常に保証しなければならなく、システムが攻撃を受けて正常に稼働できないとき、迅速に回復することをも保証しなければならない。従って、高安全性情報システムが一定以上の安全性を常に保つために、その設計や開発だけなく運用や保守をも一貫して継続的に行わなければならない。

一方、情報セキュリティ工学は多くの面でソフトウェア工学と本質的に違っているので、従来のソフトウェア工学環境が提供できる支援は高安全性が要求される情報システムの設計、開発、運用、保守にとって不十分である。しかし、現在、情報セキュリティ機能の設計・実現から運用・保守までを一貫して国際標準に基づいて継続的、系統的、統合的に支援できる情報セキュリティ工学環境は全くない。

本研究は、高安全性が要求される情報システムにおける情報セキュリティ機能の設計・実現から運用・保守までを一貫して継続的、系統的、統合的に支援するために、情報セキュリティに関する様々なISO/IEC国際標準に基づいて、情報セキュリティ工学データベース、情報セキュリティ機能保証技法と支援ツールを開発し、それらを統合する汎用的情報セキュリティ工学環境を構築し、その有効性と実用性を実証すると共に、世界の産業界に提供することを目的としている。

２．研究の進め方および研究の成果

（１）　情報セキュリティ工学環境ISEE(Information Security Engineering Environment)の要求分析と定義、機能設計、アーキテクチャー設計、コンポーネント詳細設計を行った（公表論文：1, 5, 6）。ISEEは、世界初の情報セキュリティ工学環境であり、今現在、唯一のものである。

（２）　情報セキュリティ設計仕様書検証支援ツールFORVEST(FORmal VErification Support Tool of security specifications)を開発した（公表論文：2）。我々は既に国際標準ISO/IEC 15408に基づく設計仕様の形式的検証法を提案した。しかし、この技法は数学、論理学、形式的手法に関して高度な知識が要求されるので、初心者にとって、必ずしも使いやすい技法と言えない。FORVESTというツールにより提供した支援で、利用者にとって、従来必要であった９種類の知識のうち、７種類の知識が不要になり、２種類の知識の必要性の程度も軽減されている。即ち、FORVESTを使えば、我々が既に開発した設計仕様の形式的検証法をもっと簡単に実施することができる。

（３）　情報セキュリティ機能設計仕様書自動生成ツールGESTを開発した（公表論文：3）。情報技術セキュリティ評価国際標準規格ISO/IEC 15408は、情報技術セキュリティの観点から、

情報技術に関連した製品およびシステムが適切に設計され、その設計が正しく実装されているかどうかを評価するための国際標準規格である。現在、世界において、多くの国々はISO/IEC 15408を政府調達基準、即ち、政府が利用するIT関連製品のセキュリティ機能・品質をチェックするための基準としている。情報システムがISO/IEC 15408に基づいて認証されるには、まずセキュリティ設計仕様書を作成しなければならない。しかし、このセキュリティ設計仕様書作成という仕事は容易なことではない。我々は、多くの利用者がセキュリティ設計仕様書をもっと容易に作成するために、セキュリティ設計仕様書雛形生成ツールGEST(GEnerator of Security Targets)を開発した。GESTは、利用者に指定された条件（言語、国際標準ISO/IEC 15408の版、評価保証レベルEAL、キーワードなど）および情報セキュリティ工学ISEDSに保存されている認証済みのセキュリティ設計仕様書に基づいて、セキュリティ設計仕様書の雛形を生成し出力する。利用者は、指定条件を繰り返し修正し、GESTを用いて、自分が作成したいセキュリティ設計仕様書に最も近い雛形を手に入れることができる。

（４）　高安全性情報システムの継続的設計、開発、保守に関するソフトウェアライフサイクルプロセスを提案した（公表論文：4）。国際標準ISO/IEC 12207に定義されたソフトウェアライフサイクルプロセスを参考にして、情報システムのセキュリティ機能の設計、開発、運用、保守、廃棄における様々な作業を分析したうえ、順序付けした。このような順序で、各作業を繰り返し行えれば、対象システムの安全性を一貫して維持することができる。

（５）　情報セキュリティマネジメントの実践のための規範である国際標準ISO/IEC 27002の有効利用のためのデータベースを構築した（公表論文：7）。

３．公表論文

1. Jingde CHENG, Yuichi GOTO, Shoichi MORIMOTO, and Daisuke HORIE, “A Security Engineering Environment Based on ISO/IEC Standards: Providing Standard, Formal, and Consistent Supports for Design, Development, Operation, and Maintenance of Secure Information Systems,” Proceedings of the 2nd International Conference on Information Security and Assurance, pp. 350-354, Busan, Korea, IEEE Computer Society Press, April 2008.
2. Kenichi YAJIMA, Shoichi MORIMOTO, Daisuke HORIE, Noor Shelia AZREEN, Yuichi GOTO, and Jingde CHENG, “FORVEST:A Support Tool for Formal Verification of Security Specifications with ISO/IEC 15408,” Proceedings of the 4th International Conference on Availability, Reliability and Security, pp. 624-629, Fukuoka, Japan, IEEE Computer Society Press, March 2009.
3. Daisuke HORIE, Kenichi YAJIMA, Noor AZIMAH, Yuichi GOTO, and Jingde CHENG, “GEST: A Generator of ISO/IEC 15408 Security Target Templates,” in R. Lee, G. Hu, and H. Miao (Eds.), “Computer and Information Science 2009,” Studies in Computational Intelligence, Vol. 208, pp. 149-158, Springer-Verlag, May 2009.
4. Daisuke HORIE, Toshio KASAHARA, Yuichi GOTO, and Jingde CHENG, “A New Model of Software Life Cycle Processes for Consistent Design, Development, Management, and Maintenance of Secure Information Systems,” Proceedings of the 8th IEEE/ACIS International Conference on Computer and Information Science, pp. 897-902, Shanghai, China, IEEE Computer Society Press, June 2009.
5. Jingde CHENG, Yuichi GOTO, and Daisuke HORIE, “ISEE: An Information Security Engineering Environment,” Proceedings of International Conference on Security and Cryptography, pp. 395-400, Milan, Italy, INSTICC Press, July 2009.
6. Jingde CHENG, Yuichi GOTO, Daisuke HORIE, Junichi MIURA, Toshio KASAHARA, and Ahmad IQBAL, “Development of ISEE: An Information Security Engineering Environment,” Proceedings of the 7th IEEE International Symposium on Parallel and Distributed Processing with Applications, pp. 505-510, Chengdu, China, IEEE Computer Society Press, August 2009.
7. Ahmad IQBAL, Daisuke HORIE, Yuichi GOTO, and Jingde CHENG, “A Database System for Effective Utilization of ISO/IEC 27002,” Proceedings of the 4th International Conference on Frontier of Computer Science and Technology (the 1st International Workshop on Security Engineering Environment), Shanghai, China, IEEE Computer Society Press, December 2009.