様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 １６ 日現在

機関番号：６２６１５
研究種目：基盤研究(B)
研究期間：2012～2014
課題番号：２４３０００１１

研究課題名（和文）セキュリティの変化に迅速に対応できるパターン指向ソフトウェア開発法の研究

研究課題名（英文）A Pattern Oriented Software Development Method for Agile Adaptation to Security Changes

研究代表者

吉岡　信和（YOSHIOKA, Nobukazu）

国立情報学研究所・アーキテクチャ科学研究系・准教授

研究者番号：２０３９０６０１

交付決定額（研究期間全体）：（直接経費）　　13,700,000円

研究成果の概要（和文）：セキュリティ要求の変化に対して迅速な対応を行うためには、対策の設計を行う前に、複数の対策から適切な対策を選択する指針となる高精度な対策コストの予測と、選択した対策が可能な限り自動的に追加できる仕組みが必要である。そこで、本提案では、セキュリティパターンを脅威・攻撃・対策パターンの３つに分類し、それぞれの関連を明らかにすることで、各開発工程でモデル化されるセキュリティの関心事間の関連を導出できるようした。さらにアプリケーションとパターンの関連を明らかにするために、セキュリティパターンにより得られる情報を、セキュリティモデル中のステレオタイプで付加する方法を提案した。

研究成果の概要（英文）：We need a security development method to quickly adapt to changes of security requirements. In other words, we firstly estimate the impact on a software system to change it for implementation of security countermeasures before the implementation to know the security costs with the method. Additionally, the method should allow us to apply security countermeasures semi-automatically to reduce the implementation costs. In this research, we have proposed three kinds of security patterns: threat patterns, attack patterns and countermeasure patterns with the relationships among them. In addition, we illustrate relations between these patterns and a design of applications with security stereo-types of UML.

研究分野：セキュリティソフトウェア工学

キーワード：セキュリティ　ソフトウェア学　パターン　脆弱性分析　セキュリティ要求

１．研究開始当初の背景

近年、企業や官公庁の公開サービスへの攻撃やその被害にみられるように、ソフトウェアセキュリティは企業の存続や国家の活動に対する大きな脅威になってきている。そのため、セキュリティを考慮したサービス構築法の確立は社会的に急務である。日々新しい攻撃が発見され、また、ビジネスの状況は変化するために、セキュリティのリスクも変化する。そのため、特にセキュリティを考慮したソフトウェア開発手法もその変化に対応する必要がある。

２．研究の目的

本研究では、サービス公開当初は、リスクとして顕在化していなかったセキュリティも、サービス公開途中に新たに発見され、リスクとして認識された脅威や攻撃に対して、迅速に対策を施すことができるソフトウェア開発手法、およびそれをサポートする開発環境を構築する。具体的には、複数考えられる対策案から、適切な対策を迅速に選択できるようにするために、目標①高精度に対策のコストを予測する手法、および、目標②選択した対策を可能な限り自動で追加できるメカニズムを開発する。

３．研究の方法

セキュリティに関する関心ごとは、ソフトウェアの開発プロセス全体に密接に関連する。要求段階では、保護資産を中心に資産をどのように守るのかのセキュリティ目標、想定できる脅威、対策方針を定める必要がある。設計段階では、この保護資産をソフトウェア上でどのように表現されるかを分析し、脅威を実現する攻撃があるかどうかの検討、それに対策するセキュリティ機能の仕様、および、その仕様を満たす対策の設計を行う必要がある。そのため、新しい脅威に対する対策案を検討する際には、これら開発工程間の関連をたどるための情報が必要となる。
さらに、セキュリティ要求の変化に対して迅速な対応を行うためには、対策の設計を行う前に、複数の対策から適切な対策を選択する指針となる高精度な対策コストの予測と、選択した対策が可能な限り自動的に追加できる仕組みが必要である。
そこで、本提案では、セキュリティパターンを脅威パターン、攻撃パターン、対策パターンの３つに分類し、それぞれの関連を明らかにすることで、各開発工程でモデル化されるセキュリティの関心事間の関連（縦方向のトレース）を導出できるようにする。さらにアプリケーションとパターンの関連（横方向のトレース）を明らかにするために、セキュリティパターンにより得られる情報を、セキュリティモデル中のステレオタイプで付加する方法を提案する。これらの分析結果を新しい攻撃や脅威の対応の際に再利用することで、対策コストの予測やその自動追加が実現できる。

４．研究成果

平成２４年度はセキュリティ分析・設計に必要な情報を整理しながら行い、インパクトの予測と自動化が扱える統一的な言語を構築した。具体的には、セキュリティ情報を既存のモデルに追加する手法を吉岡が中心になって開発し、パターンからインパクトを分析する手法を海谷が開発した。そして、対策を自動追加する仕組みを鷲崎が中心に開発した。さらに、オープンソースの事例を使ってこれを評価した。平成２５年度は、さらに中規模な事例として大学の学生管理システムを提案手法に基づき設計し、その問題点をもとにメタモデルの改良を行った。図１にこのメタモデルをもとにセキュリティパターンを使った設計例を示す。

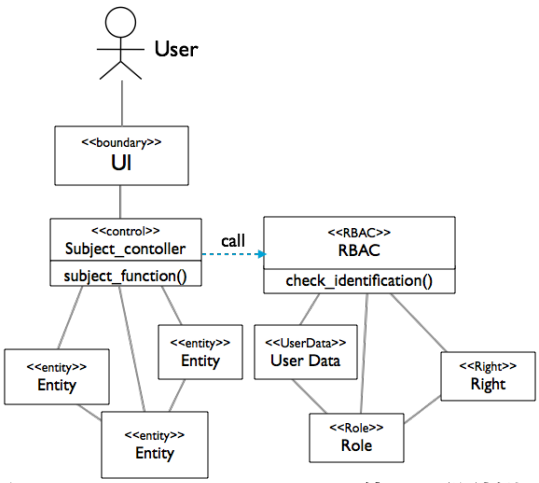

図１：セキュリティパターンを使った設計例

最終年度となる平成２６年度は、ツールを洗練し Web から公開を行った。さらに、プライバシーの考慮など、これまで提案手法で考慮していなかった観点についても分析を行い、ツールの有効性と今後の課題が整理できた。図２に開発したツールの画面イメージを示す。

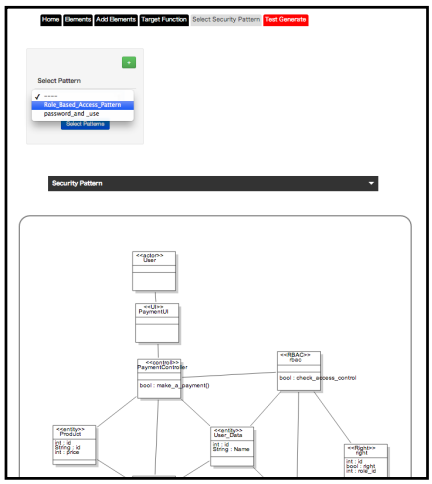

図２：ツールの画面イメージ

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 12 件）

1. Haruhiko Kaiya, Takao Okubo, Nobuyuki Kanaya, Yuji Suzuki, Shinpei Ogata, Kenji Kaijiri and Nobukazu Yoshioka. Goal-Oriented Security Requirements Analysis for a System used in Several Different Activities, The Third International Workshop on Information Systems Security Engineering (WISSE'13), LNBIP 148, Springer, pp.478-489,DOI:10.1007/978-3-642-38490 -5_43, 2013(査読有り)
2. Haruhiko Kaiya, Junya Sakai, Shinpei Ogata and Kenji Kaijiri. Eliciting Security Requirements for an Information System using Asset Flows and Processor Deployment. International Journal of Secure Software Engineering (IJSSE), IGI Global, Vol. 4, Issue 3, pp. 42-63, DOI:10.4018/jsse.2013070103,2013 (査読有り)
3. Motoshi Saeki, Shinpei Hayashi,and Haruhiko Kaiya. Enhancing Goal-Oriented Security Requirements Analysis Using Common Criteria-Based Knowledge. International Journal of Software Engineering and Knowledge Engineering (IJSEKE). World Scientific Publishing, Vol. 23, No. 05, DOI: 10.1142/S0218194013500174, pp. 695-720, 2013 (査読有り)
4. Takanori Kobashi, Nobukazu Yoshioka, Takao Okubo, Haruhiko Kaiya, Hironori Washizaki, and Yoshiaki Fukazawa. Validating Security Design Pattern Applications Using Model Testing, In Proc. of 2013 International Conference on Availability, Reliability and Security Conference (ARES 2013), IEEE CS, pp. 62-71, Germany, DOI: 10.1109/ARES.2013.13, 2013 (査読有り)
5. Seiji Munetoh and Nobukazu Yoshioka. Model-Assisted Access Control Implementation for Code-centric Ruby on Rails Web Application Development, The Eight International Workshop on Frontiers in Availability, Reliability and Security (FARES 2013), IEEE CS, pp. 350-359, DOI: 10.1109/ARES.2013.47, 2013 (査読有り)
6. Takao Okubo, Nobukazu Yoshioka and Haruhiko Kaiya. Security Driven Requirements Refinement and Exploration of Architecture with multiple NFR points of view, 15th IEEE International Symposium on High Assurance Systems Engineering (HASE 2014), IEEE Computer Society, pp. 201-20, DOI: 10.1109/HASE.2014.35, 2014 (査読有り)
7. Takao Okubo, Nobukazu Yoshioka and Haruhiko Kaiya. Requirements Refinement and Exploration of Architecture for Security and Other NFRs, The Fourth International Workshop on Information Systems Security Engineering (WISSE'14), LNBIP 178, pp. 286-298, DOI: 0.1007/978-3-319-07869-4_27, 2014(査読有り)
8. Haruhiko Kaiya, Sho Kouno, Shinpei Ogata, Takuo Okubo, Nobukazu Yoshioka, Hironori Washizaki and Kenji Kaijiri. Security Requirements Analysis using Knowledge in CAPEC, The Fourth International Workshop on Information Systems Security Engineering (WISSE'14), LNBIP 178, pp. 343-348, DOI:10.1007/978-3-319-07869-4_32, 2014 (査読有り)
9. Okubo Takao, Kenji Taguchi, Kaiya Haruhiko, and Yoshioka Nobukazu. MASG: Advanced Misuse case with Assets and Security Goals, Journal of Information Processing,Information Processing Society of Japan, Vo.22, No.3, pp.536-546, DOI:10.2197/ipsjjip.22.536, 2014 (査読有り)
10. Masatoshi Yoshizawa, Takanori Kobashi, Hiroyoshi Washizaki, Yoshiaki Fukazawa, Takao Okubo, Haruhiko Kaiya and Nobukazu Yoshioka. Verification of Implementing Security Design Patterns Using a Test Template, Proceedings of 9th International Conference on Availability, Reliability and Security (ARES2014), pp.178-183, DOI:10.1109/ARES.2014.31, 2014. (査読有り)
11. Takao Okubo, Yoshio Kakizaki, Yoshinori Kobashi, Hironori Washizaki, Shinpei Ogata, Haruhiko Kaiya and Nobukazu Yoshioka. Security and Privacy Behavior Definition for Behavior Driven Development, In proceedings of The 15th International Conference of Product Focused Software Development and Process Improvement (PROFES 2014), LNCS 8892, pp.306-309, DOI:10.1007/978-3-319-13835-0_28, 2014 (査読有り)
12. Takanori Kobashi, Nobukazu Yoshioka, Takao Okubo, Haruhiko Kaiya, Hironori Washizaki, and Yoshiaki Fukazawa. Validating Security Design Pattern

Applications by Testing Design Models, International Journal of Secure Software Engineering (IJSSE), Vol. 5, No.4,IGI Global,pp.1-30,DOI:10.4018/ijsse.2014100101, 2014（査読有り）

〔学会発表〕（計 2 件）

1. Eduardo B. Fernandez, Nobukazu Yoshioka and Hironori Washizaki, Patterns for cloud firewalls, 3rd Asian Conference on Pattern Languages of Programs (AsianPLoP 2014), 2014.3.6. 学術情報センター(東京都・千代田区)
2. Eduardo B. Fernandez, Nobukazu Yoshioka, Hironori Washizaki and Joseph Yoder, Abstract security patterns for requirements and analysis of secure systems, 17th Workshop on Requirements Engineering (WER 2014), 2014.4.23-25, Pucon (Chili)

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
http://patterns.fuka.info.waseda.ac.jp/

６．研究組織
(1)研究代表者
吉岡 信和（YOSHIOKA, Nobukazu）
国立情報学研究所・アーキテクチャ科学研究系・准教授
研究者番号：20390601

(2)研究分担者
鷲崎 弘宜（WASHIZAKI, Hironori）
早稲田大学・理工学術院・准教授
研究者番号： 70350494

(3)連携研究者
海谷 治彦（KAIYA, Haruhiko）
神奈川大学・理学部・教授
研究者番号： 30262596