科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　４　日現在

機関番号：　１３６０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００４２

研究課題名（和文）情報システムの要求分析段階における脆弱性除去と対策選択を支援するシステムの開発

研究課題名（英文）A supporting system for predicting vulnerabilities and their countermeasures of an information system during requirements analysis

研究代表者
海谷　治彦（KAIYA, Haruhiko）

信州大学・工学部・准教授

研究者番号：３０２６２５９６

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：情報システムの要求定義段階において，システムアーキテクチャに基づき，発生しうる脆弱性と，その対策群を予測するモデリング手法とツールを開発した．システム内の重要資産(アセット)の依存関係に基づきモデルは構築され，脆弱性と対策は，その依存関係グラフの構造的な特徴に基づき系統的に予測できる．ツールは独自のモデル検査エンジンによる予測の自動化と，予測結果の可視化を行う．これによって，セキュリティ分析者を含むシステム開発関係者が，予測結果の妥当性を吟味することが可能となった．

研究成果の概要（英文）：We have developed a method for security requirements analysis. In the method, vulnerabilities and their countermeasures are systematically predicted on the basis of the dependencies among assets and a system architecture in a system to be developed. We can re-examine vulnerabilities and their countermeasures when the architecture is changed but system functionalities are not changed. We have also developed a supporting tool for enacting the method. The tool consists of three components: a modeling editor, a model checker and a visualizer. With the help of the tool, stakeholders including security experts can validate the predicted results of the method because the tool can automatically derive the candidates of vulnerabilities on the basis of our original model checking engine and visualize the derived results.

研究分野：　ソフトウェア工学

科研費の分科・細目：　情報学，ソフトウェア

キーワード：　要求工学　モデリング　セキュリティ分析　アッセトフロー　モデル検査　システムアーキテクチャ　オントロジ

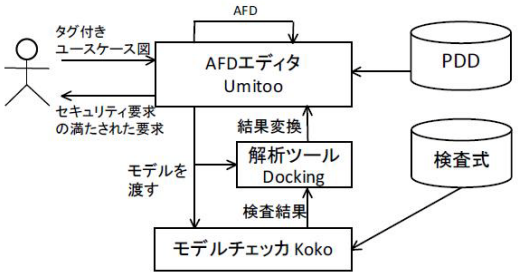
１．研究開始当初の背景
情報システム開発の要求定義段階において，システムが持つべき機能要求はシステムの利害関係者(ステークホルダ)から獲得することが可能である．しかし，システム保護に関する要求はセキュリティ専門家がシステムの導入される業務を理解した上で検討する必要がある．セキュリティ専門家は一般には業務の専門家ではないため，業務を容易に理解することは困難である．
そこで，情報システム開発において，セキュリティ上の脆弱性候補を要求仕様書に基づき系統的に発見し，どのような対策がステークホルダにとって望ましいかをシステム開発者が選択する活動の支援を行うことが有用となる．システム開発者が予め選択した脆弱性候補をセキュリティ専門家が吟味することは，セキュリティ専門家が業務を理解し起こりうる脆弱性を指摘するよりもはるかに負担は小さい．このような支援によって，システムを導入する業務の専門家およびセキュリティ専門家双方の労力を削減することが期待できる．
既存のセキュリティ要求分析手法は，既知の脆弱性をモデル化する目的には有効である．しかし，モデルに基づき脆弱性を発見し除去する作業はモデル分析者の個人的な資質に依存している．すなわち，モデルを参照し脆弱性を発見し除去できるか否かはモデル分析者の知識や経験に依存している．
一方，形式的に記述されたモデルの構造的な特徴を分析することで，モデルの持つ性質を機械的に発見するアルゴリズムは古くから研究されている．加えて，近年では，そのアルゴリズムを現実的な時間内に機械的に実行するシステムも提案されつつある．

２．研究の目的
(1) 開発もしくは改造対象のシステムに脆弱性があるか否かを判定するためには，そのシステムをセキュリティの観点からモデリングする必要がある．よって，分析対象のシステムを脆弱性の検査がしやすい形でモデリングする手法が必要である．また検査の自動化のためにはモデリングツールの開発が必要である．これらを最初の目的とした．
(2) モデリングした分析対象システムを機械的にチェックして，脆弱性が存在するか否かを判定するためのアルゴリズムが必要である．また，アルゴリズムを自動的に実施するためのツールも必要である．これらアルゴリズムとツールの開発を次の目的とした．
(3) モデルの分析結果は人間にとって理解しやすい形であるとは限らない．そこで，分析結果としての脆弱性を可視化するアルゴリズムと可視化ツールの開発も目的とした．
(4) 一般に脆弱性に対する対策は複数通り存在する．それを客観的に比較する方法と，主観的に観察する方法の提供も目的とした．客観的な比較にはメトリクスの定義が有効である．主観的な比較には前述の可視化が有効である．
(5) 検査すべきセキュリティ上の特性は，セキュリティ専門家が収集・公開している脆弱性に関するカタログに基づき記述するのが実用的である．そのようなカタログは実装寄りの語彙に基づき記述される．しかし，分析対象のシステムは業務寄りの語彙を用いて仕様化されている．本研究のモデルは業務寄りの仕様に基づき構築されるため，既存の脆弱性に関するカタログの記述内容とは意味的な祖語がある．このような意味的祖語を解消するための手法とツールの開発も目的とした．

３．研究の方法
(1) 脆弱性とその対策を発見する支援のためのシステム開発が研究目的であるため，まず，脆弱性と対策を表現するためのモデリング言語の設計を行った．当初の計画ではユースケースモデルを基盤としたモデリング言語を設計する予定であったが，既存の脆弱性の性質やその対策の調査結果から，データフローに基づくモデリング言語の構築となった．
(2) 複数存在しうる対策の比較については，当初，モデルの構造的な特徴のみに基づく予定であった．しかし，既存システムが存在し，その改造開発を行うことが実世界では多いため，既存のソースコードにおける依存関係分析も利用することとなった．
(4) 支援システムの開発については，いくつかのモデリングのための枠組みを調査し，検査ツールとの親和性の良さや開発効率の観点から枠組みを選択した．結果として，Eclipse における EMF，GEF，GMF のフレームワークを用いることとなった．
(5) モデル検査については，既存のモデル検査ツールの特徴を調査し，比較を通して実現法を検討した．結果として，既存のモデル検査ツールではなく，独自のツールを開発することとなった．
(6) 評価については，文献にある例題や，実際にソースコードが存在し動作するシステムを用い，既知の脆弱性を発見し，対策することが可能か否かの観点で行うこととした．

４．研究成果
(1) 情報システムにおける重要資産(アセット)に関する依存関係に基づくモデリング手法 アセットフロー図(AFD)を考案した．アセットフロー図はウエブアプリケーションやクラウド等のシステム構成図(PDD)をもとに記述する形式とした．これによって，同じ機能のシステムでも，システム構成によって，起こりうる脆弱性や，とりうる対策が異なることを表現できる．アセットフロー図の上で，脆弱性となるフローを検知するためのアルゴリズムを既存のモデルチェック技術を参考に考案した．チェックするための脆弱性に

関する性質(検査式)を既存の攻撃パターンカタログ(OWASP)をもとに整備した.
(2) 発見された脆弱性を除去するための手段である対策を,脆弱性の原因となるアセットフローを除去することで発見する手法を考案した.ある脆弱性に対して対策は複数存在し,それぞれにコスト(除去の手間)は異なる.既存システムが既に存在することを想定し,ソースコード上のインパクト分析を用いて,どの除去手段が最も低コストかを判断するための手法を考案した.
(3) 脆弱性に対して発見された対策案が既知の対策と一致することを確認した.また,インパクト分析に基づき異なる対策のコスト差が実開発者の主観と一致することを実験的に確認した.
(4)前述の(1)のモデリングを行うためのツール Umitoo を Eclipse モデリングフレームワーク上に構築した.また,同ツールで作成されるモデルインスタンスに対して,脆弱性の有無を自動判定するためのモデル検査ツール Koko を Ruby を用いて構築した.検査結果を可視化するためにモデルに反映するための補助ツールとして,Docking も開発した.それぞれのツールの関係を下記の図に示す.



(5) モデリングツール上で脆弱性の原因となるアセットフローを可視化するための機能を構築した.複数の異なるフローがある場合,それぞれに可視化することが可能であり,フロー間の主観的な比較を可能とした.また,客観的な比較を行うためのアセットフローに関するメトリクスも提案した.
(6) OWASP 等の既存のセキュリティカタログは実装依存の語彙を用いて記述されている.一方,アセットフローや脆弱性パターンをモデリングする場合には,業務に近い非実装寄りの用語を用いる必要がある.このような用語に関する概念的なギャップを埋めるため,技術用語-一般用語対応表を用いた概念ギャップ除去手法と支援ツールのプロトタイプを行った.
(7) 開発したツール群を実ウエブアプリケーションの脆弱性分析に適用し,既知の脆弱性を発見できることを確認した.

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 上田 健之, 小形 真平, 海谷 治彦, 海尻 賢二. 情報検索手法に基づくトレーサビリティリンク回復のための手法オプションについてのマイニングの提案と評価. 電子情報通信学会論文誌, Vol. J97-D, No. 3, pp. 414-426, Mar. 2014. 査読有.
②田中 賢, 海谷 治彦, 大西 淳. 機能要求に必要な品質要求の機械学習による予測法. 電子情報通信学会論文誌, Vol. J96-D, No. 11, pp. 2646-2656, Nov 2013. 査読有.
③Haruhiko 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, Jul.-Sep. 2013. DOI: 10.4018/jsse.2013070103 査読有.
④ Haruhiko Kaiya, Masahiro Umemura, Shinpei Ogata, and Kenji Kaijiri. Spectrum analysis on quality requirements consideration in software design documents. SpringerPlus, Vol. 2, Issue 1, No. 310, pp. 1-14, 11 Jul. 2013, DOI:10.1186/2193-1801-2-310, 査読有.
⑤ Motoshi Saeki, Shinpei Hayashi, 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, pp. 695-720, Jun. 2013. DOI: 10.1142/S0218194013500174 査読有.
⑥ Haruhiko Kaiya and Atsushi Ohnishi. Finding incorrect and missing quality requirements definitions using requirements frame. IEICE Transactions on Information and Systems, Vol. E95-D, No. 4, pp. 1031-1043, Apr. 2012. DOI 10.1587/transinf.E95.D.1012 査読有.
⑦ Takako Nakatani, Narihito Kondo, Junko Shirogane, Haruhiko Kaiya, Shozo Hori, and Keiichi Katamine. Toward the decision tree for inferring requirements maturation types. IEICE Transactions on Information and Systems, Vol. E95-D, No. 4, pp. 1021-1030, Apr. 2012. DOI 10.1587/transinf.E95.D.1021 査読有.
⑧ Shinpei Hayashi, Daisuke Tanabe, Haruhiko Kaiya, and Motoshi Saeki. Impact analysis on an attributed goal graph. IEICE Transactions on Information and Systems, Vol. E95-D, No. 4, pp. 1012-1020, Apr. 2012. DOI 10.1587/transinf.E95.D.1031 査読有.
⑨ Takao Okubo, Haruhiko Kaiya, and Nobukazu Yoshioka. Analyzing Impacts on

Software Enhancement Caused by Security Design Alternatives with Patterns. International Journal of Secure Software Engineering (IJSSE), IGI Global, Vol. 3, No. 1, pp. 37-61, Jan.-Mar. 2012. DOI: 10.4018/jsse.2012010103 査読有.
⑩ 海谷 治彦, 原 賢一郎, 小林 亮太郎, 長田 晃, 海尻 賢二. ソフトウェアが中心でない製品における既存技術を利用したソフトウェア改訂支援. 情報処理学会論文誌, Vol. 53, No. 2, pp. 653-661, Feb. 2012. 査読有.
⑪ 海谷 治彦, 鈴木 駿一, 小川 享, 谷川 正明, 梅村 真弘, 海尻 賢二. 分析履歴を用いたソフトウェア品質要求のスペクトル分析法. 情報処理学会論文誌, Vol. 53, No. 2, pp. 510-522, Feb. 2012. 査読有.
⑫ 海谷 治彦, 清水 悠太郎, 安井 浩貴, 海尻 賢二, 林 晋平, 佐伯 元司. 要求獲得のためのオントロジを Web マイニングにより拡充する手法の提案と評価. 情報処理学会論文誌, Vol. 53, No. 2, pp. 495-509, Feb. 2012. 査読有.

〔学会発表〕(計 14 件)
① Takao Okubo, Nobukazu Yoshioka, and Haruhiko Kaiya. Security Driven Requirements Refinement and Exploration of Architecture with multiple NFR points of view. In 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering (HASE 2014), pp. 201-205, Miami, Florida, USA, 9-11 Jan. 2014. IEEE Computer Society, CPS. 査読有.
② Takeyuki Ueda, Shinpei Ogata, Haruhiko Kaiya, and Kenji Kaijiri. IR based Traceability Link Recovery Method Mining. In The Eightth International Conference on Software Engineering Advances (ICSEA13), pp. 278-284, Venice, Italy, 27 Oct. - 1 Nov. 2013. 査読有.
③ Takanori Kobashi, Nobukazu Yoshioka, Takao Okubo, Haruhiko Kaiya, Hironori Washizaki and Yoshiaki Fukazawa. Validating Security Design Pattern Applications Using Model Testing, In Proceedings of International Conference on Availability, Reliability and Security (ARES 2013), pp. 62-71, IEEE CPS, 2-6 Sep. 2013, Regensburg, Germany. 査読有.
④ 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. In Xavier Franch and Pnina Soffer, editors, Advanced Information Systems Engineering Workshops, Vol. 148 of Lecture Notes in Business Information Processing (LNBIP), pp. 478-489. Springer, 18 Jun. 2013, Valencia, Spain, The Third International Workshop on Information Systems Security Engineering - WISSE'13, 査読有.
⑤ Haruhiko Kaiya, Shunsuke Morita, Shinpei Ogata, Kenji Kaijiri, Shinpei Hayashi, and Motoshi Saeki. Model Transformation Patterns for Introducing Suitable Information Systems. In Proceedings of 19th Asia-Pacific Software Engineering Conference (APSEC 2012), pp. 434-439, Hong Kong, 4-7 Dec. 2012. 査読有.
⑥ Ken Tanaka, Haruhiko Kaiya, and Atsushi Ohnishi. Predicting Quality Requirements Necessary for a Functional Requirement based on Machine Learning. In The Seventh International Conference on Software Engineering Advances (ICSEA 2012), pp. 540-547, Lisbon, 18-23 Nov. 2012. 査読有.
⑦ Masahiro Umemura, Haruhiko Kaiya, Shinpei Ogata and Kenji Kaijiri. Validating Quality Requirements Considerations in a Design Document using Spectrum Analysis. Knowledge-Based Software Engineering, Proc. of the Tenth Joint Conference on Knowledge-Based Software Engineering (JCKBSE2012), pp. 88-97. IOS Press. Rhodes, Greece. 23-26 Aug. 2012. 査読有.
⑧ Takao Okubo, Haruhiko Kaiya, and Nobukazu Yoshioka. Mutual Refinement of Security Requirements and Architecture Using Twin Peaks Model. In 36th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW 2012), REFS 2012, pp. 367-372, Izmir, Turkey, 16-20 Jul. 2012. IEEE CS. 16-20 July 2012. 査読有.
⑨ Haruhiko Kaiya and Atsushi Ohnishi. Improving Software Quality Requirements Specifications Using Spectrum Analysis. In 36th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW 2012), REFS 2012, pp. 379-384, Izmir, Turkey, 16-20 Jul. 2012. IEEE CS. 16-20 July 2012. 査読有.
⑩ Haruhiko Kaiya, Shunsuke Morita, Kenji Kaijiri, Shinpei Hayashi, and Motoshi Saeki. Facilitating Business Improvement by Information Systems using Model Transformation and Metrics. In Proceedings of the Forum at the CAiSE 2012 Conference (CAiSE 2012 Forum), pp. 106-113, Gdansk, Poland, 28 Jun. 2012. ISSN 1613-0073, CEUR Workshop Proceedings, Vol-453. 査読有.
⑪ Takao Okubo, Haruhiko Kaiya, and Nobukazu Yoshioka. Effective Security Impact Analysis with Patterns for Software

Enhancement. In Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security (ARES), pp. 527-534, Vienna, Austria, 22-26 Aug. 2011. IEEE Computer Society, CPS. 査読有.
⑫ Haruhiko Kaiya, Shunichi Suzuki, Toru Ogawa, Masaaki Tanigawa, Masahiro Umemura, and Kenji Kaijiri. Spectrum Analysis for Software Quality Requirements using Analyses Records. In 35th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW 2011), pp. 500-503, Munich, Germany, 18-22 Jul. 2011. IEEE CS. 査読有.
⑬ Haruhiko Kaiya, Kenichiro Hara, Kyotaro Kobayashi, Akira Osada, and Kenji Kaijiri. Exploring how to support software revision in software non-intensive projects using existing techniques. In 35th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW 2011), pp. 327-334, Munich, Germany, Jul. 2011. IEEE CS. 18-22 July 2011, 査読有.
⑭ Haruhiko Kaiya and Atsushi Ohnishi. Quality Requirements Analysis using Requirements Frames. QSIC 2011, Proc. of The 11th International Conference on Quality Software, pp. 198-207, Madrid, Spain, 13-14 Jul. 2011. 査読有.

〔その他〕
ホームページ等
http://kaiya.cs.shinshu-u.ac.jp/~kaiya/COVA/

６．研究組織
(1)研究代表者
海谷 治彦 (KAIYA, Haruhiko)
信州大学・工学部・准教授
研究者番号： 30262596