様式 C-19

科学研究費補助金研究成果報告書

平成２３年　６月　１日現在

機関番号：62615
研究種目：若手研究（Ｂ）
研究期間：　平成２０年度　～　平成２２年度
課題番号：２０７０００３６
研究課題名（和文）　マルチビューに基づく安全なシステム設計法の研究

研究課題名（英文）　Secure System Design based on Multi-view

研究代表者
吉岡 信和　(Nobukazu Yoshioka)
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

研究成果の概要（和文）：
本研究では、セキュリティの関心事を網羅的に整理したモデル化を行う為、通常の設計モデルに加え、システムに対する攻撃モデル、脆弱モデル、そして、安全モデルの三つの新たなモデル(マルチビュー)を導入する。これにより、セキュリティに対する関心事を段階的に整理、分析し、最終的には、安全なシステムを設計可能となる。

研究成果の概要（英文）：
In this research, we have proposed a three view modeling method with an attack model, a threat model and security model to design secure system in addition to usual design model. The multi-view modeling allows us to separate security concerns into an integrated design method and to design secure systems step-by-step.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
平成２０年度	800,000	240,000	1,040,000
平成２１年度	900,000	270,000	1,170,000
平成２２年度	1,500,000	450,000	1,950,000
総　計	3,200,000	960,000	4,160,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：セキュリティ、設計手法、関心毎の分離、パターン、分散システム

１．研究開始当初の背景

近年のオープンなサービスの利用拡大と、その社会への浸透にともない、セキュリティは益々重要になってきている。しかしながら、セキュリティを考慮した安全なシステムの構築には、様々な要素を考慮しなければならず、その構築が困難である。アドホックなパッチに頼った対応は、サービスの信頼性を低下させるだけでなく、より大きな脅威の引き金にもなりかねない。そのため、サービスの設計工程からセキュリティを考慮することが重要である。

セキュリティに関する情報を設計レベルで扱うために、UML をベースとしたセキュリティに関するモデルが提案されている。また、セキュリティの設計を容易にするために、セキュリティに関するデザインパターン（セキュリティパターン）も多数提案されてきている。今後は、このような設計手法やパターンが実際の開発に活用されていくものと思われる

２．研究の目的

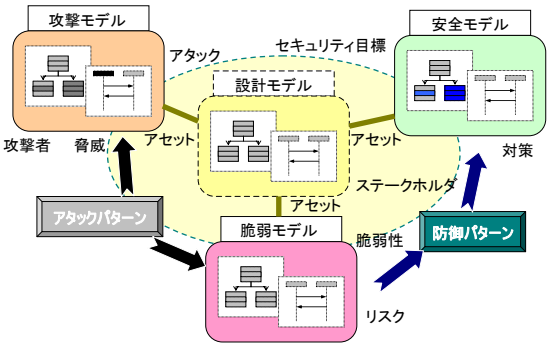
本研究では、セキュリティの関心事を網羅的に整理したモデル化を行う為、通常の設計モデルに加え、システムに対する攻撃モデル、脆弱モデル、そして、安全モデルの三つの新たなモデル(マルチビュー)を導入する。これにより、セキュリティに対する関心事を段階的に整理、分析し、最終的には、安全なシステムを設計可能となる。そして、上流工程か

ら下流工程までの一貫性をチェックするため、まず、セキュリティパターンに関する言語を上記の三つのモデルの観点で整理する。パターンによりセキュリティに関する条件を明らかにし、モデルを詳細化する際にその条件を調べることで、工程にまたがるモデル間の一貫性をチェック可能になる。

３．研究の方法

本研究では、セキュリティの関心事を網羅的に整理したモデル化を行う為、通常の設計モデルに加え、システムに対する攻撃モデル、脆弱モデル、そして、安全モデルの三つの新たなモデル(マルチビュー)を導入する。攻撃モデルは、システムの脆弱性を明らかにするために設計し、攻撃者や具体的な攻撃、脅威を表現する。そして、攻撃モデルを分析した結果から脆弱モデルを構築する。さらに、その脆弱性に対する対策・防御を行うため安全モデルを構築する。これにより、セキュリティに対する関心事を段階的に整理、分析し、最終的には、安全なシステムを設計可能となる。そして、上流工程から下流工程までの一貫性をチェックするため、まず、セキュリティパターンに関する言語を上記の三つのモデルの観点で整理する。具体的には、攻撃、および、システムの脆弱性を規定したアタックパターンの構築を行い、従来のセキュリテ

マルチビューモデリング



４．研究成果

平成 20 年度は、３つのモデルで定義するセキュリティ要素、および、表記法、モデルのセマンティクスを決定し、各モデルを構築するためのパターンを整理した。具体的には、攻撃モデルに関しては、アタックパターン・ミスユースパターンを整理し、それに基づく攻撃者の観点でのモデルを構築できるように、本モデルに含まれる情報を、攻撃者の意図、攻撃の状況（コンテキスト）、攻撃の手順などに整理した。さらに、脆弱性モデルは、攻撃が受けやすい状況（侵入の可能性のあるネットワーク、ホスト）や、攻撃を受けたことを確認・検証できるようにするための情報(Forensics)を含めるように設計した。そして、設計モデルでは、セキュリティの制約やセキュリティ機能を含めるようにした。パターンとしては、攻撃、その確認方法、対応を含めることに、これらの３つのトレーサビリティが保つことが可能となった。

上記で整理したミスユースパターンに対して、平成 21 年度は、そのミスユースを軽減するセキュリティ機能の使い方をあらわすセキュリティパターンとの関係、および、そのパターンとセキュリティ要件や保護資産との関係を明らかにした。具体的には、セキュリティ要件をセキュリティ目標と保護資産との関係としてユースケースモデルに表現することで安全モデルを構築する。さらに、保護資産やセキュリティ目標を破るという観点で攻撃モデルを構築する。そして、攻撃によって保護資産がどのような悪影響を及ぼすのか、また、関連する構成要素は何かという観点で、脆弱モデルを構築する。各モデルの情報を効率よく収集し、モデルを洗練させるためにミスユースパターンとセキュリティパターンが利用可能である。

平成 22 年度は、要求工程と設計工程、そして実装との一貫性を容易に保つために、それぞれのビューごとに、要求レベルのパターンと設計レベルのパターンを関連付けたセキュリティパターン言語を開発した。さらに、そのパターンに基づき、セキュリティの要求仕様の変更に対して、どの程度、既存の開発に影響を及ぼすかを分析するインパクト分析手法を提案した。これにより、セキュリティの設計、実装を行う前に、複数存在する対策候補の中で、必要十分、かつ開発コストの低い対策を選択できるようになった。

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５件）

① Takao Okubo, Kenji Taguchi, Nobukazu Yoshioka, “Misuse cases + Assets + Security Goals,” Proc. of Workshop on Software Security Process (SSP09), IEEE, pp. 424-429, 2009.(査読有)

② 城間祐輝, 久保淳人, 吉岡信和, 鷲崎弘宜, 深澤良彰, “パターン間の関係を考慮したセキュリティパターン適用支援,” ソフトウェアエンジニアリング最前線 2009, pp.75-82, 2009.(査読有)

③ Nancy R. Mead, 吉岡信和, “SQUARE ではじめるセキュリティ要求工学,” 情報処理, Vol. 50, No.3, pp. 193-197, 2009.(査読無)

④ 吉岡信和, Bashar Nuseibeh, “セキュリティ要求工学の概要と展望,” 情報処理,

Vol. 50, No.3, pp.187-192, 2009. (査読無)

⑤ Nobukazu Yoshioka, Hironori Washizaki,and Katsuhisa Maruyama, " A Survey on Security Patterns," Progress in Informatics, National Institute of Informatics, pp.35-47, 2008. (査読有)

〔学会発表〕(計４件)

① Kenji Taguchi, Nobukazu Yoshioka, Takayuki Tobita, Hiroyuki Kaneko, "Aligning Security Requirements and Security Assurance Using the Common Criteria," 2010 Fourth International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2010), 2010.

② Yuki Shiroma, Hironori Washizaki, Yoshiaki Fukazawa, Atsuto Kubo, Nobukazu Yoshioka, Eduardo B. Fernandez, "Model-Driven Security Patterns Application and Validation," 17th Conference on Pattern Languages of Programs (PLoP 2010), 2010.

③ 吉岡信和, 田口研治, 飛田孝幸, 金子浩之, "コモンクライテリアのためのモデリング手法の提案," 情報処理学会 168 回ソフトウェア工学研究会, 2009.

④ Eduardo Fernandez, Hironori Washizaki, Nobukazu Yoshioka, Atsuto Kubo, Yoshiaki Fukuzawa, "Classifying security patterns," the 10th Asia Pacific Web Conference, 2008.

〔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〕

ホームページ等

６．研究組織

(1)研究代表者

吉岡 信和 (Nobukazu Yoshioka)

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

(3)連携研究者

鷲崎 弘宜 (Hironori Washizaki)

早稲田大学 理工学術院・准教授

研究者番号：70350494