様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　　５　日現在

機関番号：　１２６０４
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０３９４

研究課題名（和文）モデリングツールとソフトウェアセキュリティ知識ベースを連携したモデリング学習環境

研究課題名（英文）A Security Modeling Learning Environment Integrating a Modeling Tool with Software Security Knowledge Base

研究代表者

櫨山　淳雄（Hazeyama, Atsuo）

東京学芸大学・教育学部・教授

研究者番号：７０３１３２７８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：　本研究ではソフトウェアセキュリティ知識ベースを参照しながら成果物(具体的には、セキュリティ要求分析におけるミスユースケース図)を作成可能な学習環境を構築した。この環境では設計根拠を記録することができるために、成果物の構成要素に対して、知識ベース中の知識を関連付けることができる。
　評価実験の結果、知識ベースの参照と成果物作成が同一環境で行えること、並びに、成果物の構成要素単位に知識を関連付けることの有効性が明らかになった。

研究成果の概要（英文）：This study has developed a learning environment that creates an artifact (misuse case diagram in a security requirement analysis) while referring to a software security knowledge base. The environment enables to associate knowledge with the elements of an artifact in order to record design rationale.
From the result of an evaluation experiment, we found effectiveness that both reference of knowledge base and artifact creation are conducted in the same environment. We also found effectiveness of association of the knowledge with the elements that compose of a diagram.

研究分野：　ソフトウェア工学，ソフトウェア工学教育

キーワード：　ソフトウェアセキュリティ　ソフトウェアセキュリティ知識ベース　ミスユースケースエディタ　設計根拠

１．研究開始当初の背景

インターネット上でのサービスは増大し続けている．それに伴い，セキュリティの重要性が高まっている．特に，多くのサービスがソフトウェアで実現されていることから，ソフトウェアセキュリティ技術の重要性が認識されるようになってきた[1]．ソフトウェアセキュリティではソフトウェア開発過程全体でセキュリティを扱うことを目指しており，これまでに開発プロセス・方法論，パターン，ガイドラインなどの技術が開発されてきた．特に，分析や設計といった開発の初期段階に対する技術開発への関心が高まっている．ソフトウェアセキュリティに関する知識を有するソフトウェア開発者が少ない[2]ことから，人材育成の必要性が認識されている．そのための 1 つの方法としてセキュリティの専門家でないソフトウェア開発者や学習者にセキュアなソフトウェア開発に関する知識を体系的に提供し，実践する場を提供することが考えられる．しかしながら現状ではソフトウェアセキュリティに関する知識の体系化が不十分な状況にある．このような背景から，ソフトウェアセキュリティ知識を体系的に扱うことが可能な枠組（メタモデル）を開発し，セキュリティ知識ベースのプロトタイプを開発した[3]．また，成果物とそれを作成するために参照した知識ベース中の知識を関連付けて設計根拠を記録する学習環境モデルを提案し，プロトタイプを開発した[3]．このような研究成果に対して，以下の課題も明らかになった．

課題(1) 知識ベースに格納されている知識は複雑な関連を有しているが，知識ベースの全体像を把握し，効果的に活用するための支援が必要である．

課題(2) 知識を関連付ける対象はファイル単位の成果物であり，成果物の構成要素単位で知識を関連付けることができず，設計根拠の記録として不十分である．

２．研究の目的

本研究は前章で述べた課題を解決することを目指す．

課題(1)の解決に向けた提案：知識ベース中の知識間の関連のネットワーク構造による可視化，工程等による知識の分類(タグ付け)，どの知識がどのような場面でどの程度利用されているのかという知識の活用頻度や活用事例を参照可能にする支援機能を開発する．

課題(2)の解決に向けた提案：ダイアグラムの構成要素レベルを管理できるモデリングツールを開発し，知識を関連付けて設計根拠を記録できるようにする．知識ベースはサーバ上に構築されており，Web ブラウザを通して利用可能であるので，モデリング学習環境も同様の環境で動作させる．

３．研究の方法

2 章で述べた目的を達成するために，次の方法で研究を進める．

- ソフトウェアセキュリティ分野の研究動向調査：知識ベースの内容を充実させるために，ソフトウェアセキュリティ知識に関する研究動向を把握する
- 知識ベースの全体像把握支援を実現するための環境調査：知識ベースは個々の知識とその間の関連として表現する．すなわち，グラフ構造をなしている．グラフ構造を直接表現可能な可視化方法を調査する
- モデリングツール実現のための環境調査：実際的な利用場面を考えると，特別なインストール作業を行うことなく学習環境を利用可能であることが望ましい．また，研究プロトタイプとして，学習環境を随時更新していける環境が望ましい．これらの要件を実現する環境を調査し，その上に学習環境を開発する
- 学習環境の実装と評価実験：調査の結果に基づいた環境上で学習環境を開発する．そして開発した学習環境の有効性を評価するために評価実験を行う

４．研究成果

4.1 学習環境の実装

開発した学習環境の画面を図１に示す．

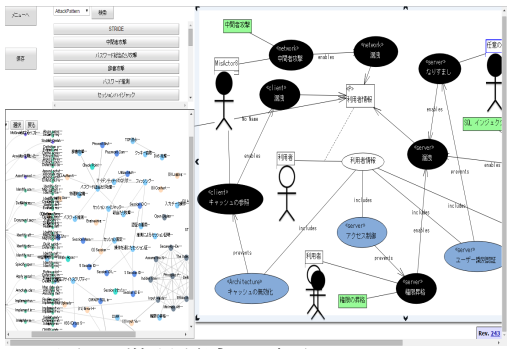

図１　学習環境の画面イメージ

画面の右が成果物を作成するエディタである．今回の実装ではセキュリティ要求分析で知られているミスユースケース図を対象とした．エディタ中の緑色のアイコンが知識であり，知識を成果物の構成要素単位に関連付けることができる．画面の左下が知識ベースの内容を可視化したものである．

知識ベースの可視化には D3.js を利用した．また，ミスユースケース図エディタはオープンソースソフトウェア GWTUMLDrawer をベースに開発した．

4.2　学習環境の評価実験

4.2.1 評価実験の目的

以下の観点から学習環境の有効性評価実験を行った：

- 成果物作成環境であるモデリングツールと知識ベースを統合した学習環境に対する有効性評価
- 成果物を構成する要素ごとにソフトウェアセキュリティに関する知識を関連付けることに対する有効性評価

4.2.2 実験協力者

実験協力者として，開発者とは所属の異なる 2 つの大学に在籍する大学院生に協力いただいた(それぞれを T 大学と I 大学と呼ぶ)．T 大学の協力者は大学院の講義で情報セキュリティの科目を学んでいる 17 名である．I 大学の協力者はセキュリティを専門にしている大学院生 3 名である．

4.2.3 実験の流れ

以下の項目をこの順序で実施した：実験の目的と背景知識の概説，学習環境の紹介と操作練習，課題の提示とモデリング実施，アンケート調査．

アンケートの項目を以下に示す：

問 1：演習前，ミスユースケース図の描き方を理解していましたか？(4 択)

問 2：演習前，ソフトウェアセキュリティの知識はどの程度お持ちでしたか？(4 択)

問 3：ミスユースケースエディタと知識の閲覧が同一学習環境上でできることはどう思いましたか？(4 択)

問 4：前問で，そのように判断した理由をお聞かせください(自由記述)

問 5：作成者として，セキュリティ知識（緑色のアイコン）をモデル図の構成要素に関連付けることを，どのように思いましたか？(4 択)

問 6：前問で，そのように判断した理由をお聞かせください(自由記述)

問 7：モデル図を閲覧する立場になったとした場合，モデル図の構成要素にセキュリティ知識（緑色のアイコン）が関連付けられていることを，どのように思いますか？(4 択)

問 8：前問で，そのように判断した理由をお聞かせください(自由記述)

4.2.4 結果

(1)T 大学での結果

T 大学での結果を述べる．アンケートの集計結果を表 1，表 2，図 2 に示す．

表 1 アンケート集計結果

項目	結果
実験協力者	17 名
アンケート回答者	7 名
アンケート回答率	41%

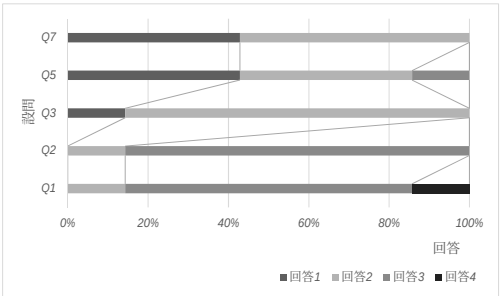

図 2 アンケート結果

実験を行う前の実験協力者たちのプロフィールはアンケートの問 1, 2 から伺える．大部分のアンケート回答者(86%)は実験実施前にはミスユースケースの描き方を理解しておらず，セキュリティに関する知識を十分に持ちあわせていないことがわかる．

表 2 アンケートにおける定性記述

設問	回答
Q4	P1：おおまかにどういった攻撃手段があるかを確認しながらミスユースケースの設置ができる事は視覚的にはとても快適だと感じたため． P2：関連する知識をすぐに知ることができるため．
Q6	P1：今回では取り立てて特に「良い」とは感じてはいなかったが， いずれ使う可能性もあり，また，なくて良いというものでは絶対ないと思ったため． P2：どこにセキュリティ知識が対応するのかが分かりやすくなるため．
Q8	P1：ノート PC のモニタの都合もあるとは思うが， 関連項目が少々固まっていて見づらい，クリックしにくいなどは少々感じた．便利には感じている． P2：ひと目で分かりやすいため．

知識を参照しながら成果物を作成することができる学習環境の有効性について問 3 に結果を示している．アンケート回答者全員が肯定的な回答を示している．そのように判断した理由は問 4 への回答として表 2 に記述されている．P1，P2 ともに学習環境上で知識を閲覧できることの有効性を述べている．P1 はまた可視化の利点にも言及している．

問 5 は設計根拠を記録する立場の時に，成果物の構成要素単位に知識を関連付けることの意義を問うている．結果はアンケート回答者の 86%が肯定的な回答を示している．そのように判断した理由は問 6 への回答として記述されている．P2 は成果物の当該箇所に当該の知識を関連付けることにより，ダイアグラムがわかりやすくなるという意見を述べている．

問 7 はダイアグラムを参照する時に，成果物の構成要素単位に知識が設計根拠として関連付けられていることの意義を問うている．結果はアンケート回答者全員が肯定的な回答を示している．そのように判断した理由は問 8 への回答として記述されている．P1 は学習環境のユーザビリティの問題を指摘しながらも便利さという肯定的な意見を述べている．P2 は作成時同様に閲覧時においても分かり易さという有効性を述べている．

(2)I 大学での結果

I 大学での結果を述べる．アンケートの集計結果を表 3，表 4，図 3 に示す．

実験を行う前の実験協力者たちのプロフィールはアンケートの問 1, 2 から伺える．問実験協力者全員がミスユースケースの描き方を理解しており，セキュリティに関する知識を十分に持っていることがわかる．

表 3 アンケート集計結果

項目	結果
実験協力者	3 名
アンケート回答者	3 名
アンケート回答率	100%

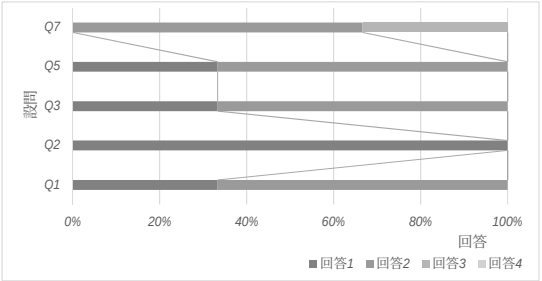

図 3 アンケート結果

表 4 アンケートにおける定性記述

設問	回答
Q4	P3： 知識のない者にとって参考になる．知識がある者にとっても理解の一助になる．知識を蓄積していける． P4：用語の統一など属人性の排除にも使えると感じた． P5：知識は脅威と攻撃方法が一緒になっていて，どれを選ぶか作成者によって異なる．
Q6	P3：脅威・攻撃手段とその対策について，より具体的に検討するのに役立つ．ただし，図が増えると見やすさがなくなり，複雑な図になってしまう． P4：アイデアはとても良いと思うが，事前設定されるものに限界を感じる． P5：技術的対策に限定しないならば，技術的，物理的などユースケースを分けないとわかりにくい．セキュリティ要件でミスユースケースが爆発してしまい，分析に時間がかかる．
Q8	P3：攻撃手段と脅威の関連性がわかり易くなる． P4：対応した典型的な対策にも関連させれば便利そう． P5：Q4 に書いたように，分類の細分化，新たな知識をカスタマイズできる仕様がほしい．

知識を参照しながら，成果物を作成することができる学習環境の有効性について問 3 に結果を示している．実験協力者全員が肯定的な回答を示している．そのように判断した理由は問 4 への回答として記述されている．P3 は知識を有しているか否かに関わらず知識を参照できることの有効性を評価している．P5 は学習環境の有効性を評価しているものの，知識の内容についてセキュリティ専門家の立場から問題点を指摘している．

問 5 は設計根拠を記録する立場の時に，成果物の構成要素単位に知識を関連付けることの意義を問うている．結果は実験協力者全員が肯定的な回答を示している．そのように判断した理由は問 6 への回答として記述されている．P4 は学習環境のコンセプトについては評価しているものの，専門家であるがゆえに事前設定されることに対する問題点を指摘している．また，P3 は図が複雑になることへの懸念，P5 は観点を分けた表現の必要性を指摘している．

問 7 はダイアグラムを参照する時に，成果物の構成要素単位に知識が設計根拠として関連付けられていることの意義を問うている．結果は 2 名の実験協力者が肯定的な回答を示しているが，1 名はやや否定的な回答をしている．そのように判断した理由は問 8 への回答として記述されている．P4 は成果物と知識が関連付けられた事例として活用することの有効性を指摘している．P3 は成果物と知識の関連づけによるわかり易さを指摘している．P5 は現状提供している知識の分類の曖昧さを指摘しており，知識を洗練する仕掛けが必要であると述べている．

4.2.5 考察

学習環境の有効性について実験結果を踏まえて考察する．

(1) 成果物作成環境と知識ベースを統合した学習環境に関する評価

アンケートの結果から，成果物作成環境と知識ベースを統合したことの有効性が示唆される回答を得られた．問 3 から 2 つの実験のアンケート回答者全員が有効であるという評価であった．知識を参照しながら成果物作成を効果的に行うことが可能な学習環境を提供できたと考える．

(2) 成果物の要素ごとに知識を関連付けることに関する評価

アンケートの結果から，知識を関連付けることの有効性が示唆される回答を得られた．成果物を構成する要素ごとにセキュリティ知識を関連付けることに関する問 5, 7 では，90%のアンケート回答者が有効と回答した．成果物を作成する段階，成果物と知識が関連付けられたダイアグラムを参照する段階いずれにおいても有効であるという意見が大半を占めた．知識をどのように利用しているかがひと目で分かるという事例としての価値を評価しているコメントがあった．一方で，現状の知識の分類の不十分さにより，作成者によってモデリングの意図がばらついてしまう可能性の指摘があり，知識ベースの内容，表示方法の改善が必要であることが明らかになった．

4.3 知識ベースを活用した分析から設計への支援

本研究ではソフトウェアセキュリティ知識ベースの構築を進めてきた．セキュリティ要求分析の知識が設計以降の知識と関連付けられているならば，セキュリティ要求分析で使用された知識に関連付けられた設計工程で考慮すべき知識を提示し，設計活動を支援することが可能になる．

設計において，開発者が要求分析の成果物を閲覧し，成果物に関連付けられている知識を選択すると，それに関連付けられている設計で考慮すべき知識が提示される．この時，設計で適用されるべき知識を抽出できる必要がある．知識ベースでは，各知識の適用工程を識別するため，各知識に適用工程をメタデ

ータとして付加する．

セキュリティ要求分析から設計へのシームレスな支援について，認証を例に説明する．「なりすまし」という脅威に対する対応策として「認証」が示されている．この抽象度の知識はセキュリティ要求分析で利用することを想定する．Hafiz はセキュリティパターンを体系化している[4]．その中に認証に関わるパターンとして Authenticator Enforcer (以下 Authenticator と記す)がある．我々の知識ベースでは，「認証」は Solution type のインスタンスとして管理し，それをセキュリティパターン Authenticator と関連づける(このパターンの適用工程として「設計」をメタデータに付与する)(図 4)．Hafiz の論文では Authenticator は[5]を参照しており，そこには，その構造がクラス図として提供されている．これらの情報を提案環境で参照できるようにすることで，認証をどのように実現すればよいのかという知識を開発者に提供することができる．

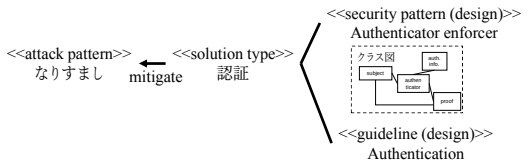

図 4 認証に関する知識間の関連

文献

[1] G. McGraw, Software Security, IEEE Security & Privacy, Vol. 2, No.2, pp. 80-83, 2004.
[2] A. Apvrille and M. Pourzandi, Secure Software Development by Example, IEEE Security & Privacy, July/August, pp. 10-17, 2005.
[3] A. Hazeyama and H. Shimizu, Development of Development of a Software Security Learning Environment, SNPD 2012, pp.518-523, IEEE, 2012.
[4] M. Hafiz, P. Adamczyk, and R. Johnson, Growing a Pattern Language (for Security), Proc. ACM International Symposium on New ideas, new paradigms, and reflections on programming and software, pp. 139-158, ACM Press, 2012.
[5] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns: Integrating Security and Systems Engineering, John Wiley & Sons, 2013.

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 4 件）

① 櫨山淳雄，田中俊一，田中昂文，宗藤誠治，大久保隆夫，ソフトウェアセキュリティ知識ベースを活用したセキュリティ要求分析支援システムの評価，電子情報通信学会技術研究報告ソフトウェアサイエンス，Vol. 116, No. 512, pp. 139-144, 2017 (査読無)．
② Masahito Saito, Atsuo Hazeyama, Nobukazu Yoshioka, Takanori Kobashi, Hironori Washizaki, Haruhiko Kaiya, and Takao Okubo, A Case-based Management System for Secure Software Development Using Software Security Knowledge, Procedia Computer Science, Volume 60, pp. 1092-1100, Elsevier, 2015, doi:10.1016/j.procs.2015.08.155 (査読有).
③ Atsuo Hazeyama, Masahito Saito, Nobukazu Yoshioka, Azusa Kumagai, Takanori Kobashi, Hironori Washizaki, Haruhiko Kaiya, Takao Okubo, Case Base for Secure Software Development Using Software Security Knowledge Base, Proceedings of the 39th Annual International Computers, Software & Applications Conference (COMPSAC2015), Volume 3, pp. 97-103, 2015, DOI:10.1109/COMPSAC.2015.86 (査読有).
④ 田中俊一，田中昂文，沓澤脩，橋浦弘明，櫨山淳雄，宗藤誠治，ソフトウェアセキュリティ知識ベースを活用したセキュアなソフトウェア開発のためのモデリングツールの開発，電子情報通信学会技術研究報告知能ソフトウェア工学，Vol．115，No．487，pp.31-36，2016（査読無）．

〔学会発表〕（計 2 件）

① 田中昂文，櫨山淳雄，鷲崎弘宜，吉岡信和，セキュリティ知識ベースと事例ベースを活用したセキュリティ要求分析・設計支援システムの提案，2017 年電子情報通信学会総合大会，2017 年 3 月 25 日，名城大学（愛知県・名古屋市）．
② 櫨山淳雄，宮原光，田中昂文，橋浦弘明，鷲崎弘宜，吉岡信和，海谷治彦，大久保隆夫，ソフトウェアセキュリティ知識ベースを活用したセキュリティ要求分析からセキュリティ 設計を支援するシステムの提案，情報処理学会第 79 回全国大会，2017 年 3 月 16 日，名古屋大学（愛知県・名古屋市）．

〔図書〕（計 1 件）

① Atsuo Hazeyama and Masahito Saito, Preliminary Evaluation of a Software Security Learning Environment, Studies in Computational Intelligence Vol. 578, 234 pages (pp. 113-125), Springer, 2014.

６．研究組織

(1)研究代表者

櫨山淳雄（HAZEYAMA Atsuo），東京学芸大学・教育学部・教授，研究者番号：70313278

(2)研究分担者

橋浦弘明（HASHIURA Hiroaki），日本工業大学・工学部・助教，研究者番号：20597083

(3)連携研究者

宮寺庸造（MIYADERA Youzou），東京学芸大学・教育学部・教授，研究者番号：10190802

(4)研究協力者

齋藤大仁 (SAITO Masahito)，田中俊一 (TANAKA Shun’ichi)，田中昂文 (TANAKA Takafumi)，海谷治彦(KAIYA Haruhiko)，大久保隆夫(OKUBO Takao)，吉岡信和(YOSHIOKA Nobukazu)，鷲崎弘宜(WASHIZAKI Hironori)