様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年５月２１日現在

機関番号：１２６０４
研究種目：基盤研究（Ｃ）
研究期間：2010～2012
課題番号：２２５００９１０
研究課題名（和文）　ソフトウェアセキュリティ学習環境の研究

研究課題名（英文）　Study on constructing a learning environment for software security

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

研究成果の概要（和文）：本研究は、ソフトウェアセキュリティに関して体系化された知識ベースを参照しながら、セキュアなソフトウェア開発を学習する学習環境を構築した。学習環境は知識ベースの構築、維持管理を支援する知識ベース管理サブシステムと、学習成果物の管理を支援する学習支援サブシステムから構成される。学習支援サブシステムにおいて、学習者が学習成果を登録する際、その作成根拠として参照した知識ベース中に知識と関連付けを行うことを可能にする。また、学習成果物に対して他者によるレビューを行うための機能を提供しているが、その際にも、コメントの根拠となる知識ベース中に知識と関連付けを行うことを可能にする機能を提供した。本研究では、学習環境を構築するとともに、ソフトウェアセキュリティに関する文献サーベイを行った。そしてその結果に基づき、Web アプリケーション開発のための知識ベースを構築した。

研究成果の概要（英文）：This study has constructed a learning environment for secure software development. The environment consists of two major sub-systems, that is, knowledge base management sub-system and learning support sub-system. The knowledge base management sub-system supports creation or maintenance of the knowledge base. The learning support sub-system manages learning artifacts. When a learner registers an artifact, the learning support sub-system enables him/her to associate it with pieces of knowledge in the knowledge base as design rationale. The learning support sub-system provides a review function. When a reviewer registers review comments, the sub-system enables him/her to associate them with pieces of knowledge in the knowledge base as design rationale. The information is reused for other learners. This study conducted literature survey to construct a knowledge base for software security. Based on the result of the survey, this study constructed a knowledge base for a web application development.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,200,000	360,000	1,560,000
２０１１年度	1,000,000	300,000	1,300,000
２０１２年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：ソフトウェア工学、ソフトウェア工学教育
科研費の分科・細目：科学教育・教育工学・教育工学
キーワード：ソフトウェアセキュリティ、知識ベース、学習環境、設計根拠

１．研究開始当初の背景

社会の情報化、とりわけインターネットに代表される情報通信技術の進展はめざましく、さまざまなネットワークを介したサービスが提供されてきた。それに伴い、セキュリティの問題も顕在化してきた。近年ではサービスの多くがソフトウェアで実現されており、ソフトウェアセキュリティの重要性が認識されてきた[McGraw 2004]。ソフトウェアセキュリティとは、悪意をもった存在がいるという前提で，正しく機能し続けるようソフトウェアを開発することと述べられており、ソフトウェア開発ライフサイクル全体でセキュリティに取り組む必要があると認識されている。

ソフトウェアセキュリティに関する技術は近年活発に研究されてきた[Yoshioka 2011]。それらはプロセス、セキュリティパターン、ガイドラインなどである。しかし、ソフトウェア開発者がセキュリティに関する知識を十分に保持していない現状が指摘されている[Stoneburner et al. 2004]。また、これらの知識をどのように活用すればよいのかが十分に明らかにされていないという問題も指摘されている[Axelle&Makan 2005], [Yoshioka 2011]。

参考文献

[Axelle&Makan 2005] Apvrille Axelle and Pourzandi Makan, Secure Software Development by Example, IEEE Security & Privacy, Vol.3, No.4, pp.10-17, 2005.

[McGraw 2004] Gary McGraw, Software Security, IEEE Security & Privacy, Vol.2, No.2, pp.32-35, March/April 2004.

[Stoneburner et al. 2004] Gary Stoneburner, Clark Hayden, and Alexis Feringa, NIST Special Publication 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, 2004.

[Yoshioka 2011] 吉岡信和, セキュリティの知識を共有するセキュリティパターン, 情報処理, Vol.52,No.9, pp.1134-1139, 2011.

２．研究の目的

前章で述べた問題指摘に対して、本研究は、ソフトウェアセキュリティを学ぶための学習環境構築を目的とする。本研究が目指す学習プロセスを図１に示す。この図はセキュリティを考慮していない成果物を入力として、ソフトウェアセキュリティに関する知識を参照しながらセキュアなソフトウェア開発を支援することを示している。

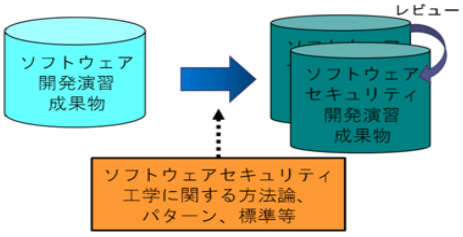

図１ ソフトウェアセキュリティ
学習プロセス

我々はこれまでにグループによるソフトウェア開発演習を Project-Based Learning (PBL)の形式で進めてきた[Hazeyama 2009]。その成果は演習支援環境[Hazeyama&Kobayashi 2008]に蓄積されている。この成果を入力として、ソフトウェアセキュリティで研究開発されてきた知識であるプロセス、ガイドライン、パターン等を活用して、セキュアなソフトウェア開発を行うことを支援する学習環境の構築を目指すものである。学習環境は、ソフトウェアセキュリティで研究開発されてきた知識を扱う部分（知識ベースサブシステム）と学習成果物を管理する部分（学習支援サブシステム）から構成される。

参考文献

[Hazeyama 2009] Atsuo Hazeyama, A Case Study of Undergraduate Group-based Software Engineering Project Course for Real World Application, Proceedings of the First International Symposium on Tangible Software Engineering Education, (STANS2009), pp. 39-44, 2009.

[Hazeyama&Kobayashi 2008] 櫨山淳雄, 小林祐介, 成果物管理とコミュニケーション支援を連携した非同期分散ソフトウェア開発支援環境, 情報処理学会ソフトウェアエンジニアリングシンポジウム 2008 ワークショップ (SES2008), pp. 5-6, 2008.

３．研究の方法

学習環境は著者らが開発した PBL 学習環境と同様に Web アプリケーションとして実現する。

ソフトウェアセキュリティ知識に関する知識ベースサブシステム構築のために、文献調査を行い、知識を体系化するためのデータモデルを構築する。そして、文献調査の成果として Web アプリケーション開発のための知識ベースを開発する。

４．研究成果

（１）学習環境の構築

図２に学習環境の全体像を示す。

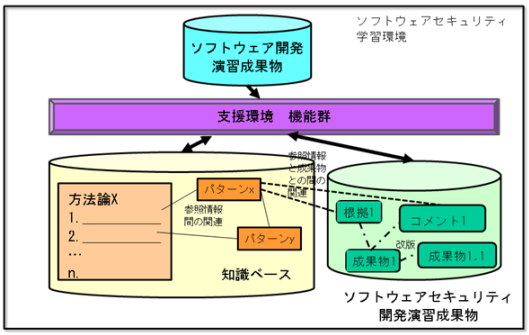

図２ ソフトウェアセキュリティのための学習環境の全体像

学習環境は次に示す４つの主要機能群から構成される。

① 知識ベースの構築

ソフトウェアセキュリティに関する知識と知識間の関連の登録・修正・閲覧・削除が行えるようにする。

② 成果物管理

演習の入力となるソフトウェア開発演習成果物並びに演習の成果物であるソフトウェアセキュリティ開発演習成果物の登録が行えるようにする。また、成果物の修正過程を追跡できるよう、成果物の版管理を行う。さらにソフトウェアセキュリティ開発演習成果物にはいくつかの種類があるので、それらの間の関連を設定できるようにする。

③ 成果物と知識ベース・設計根拠の関連づけ、リンクによる相互参照

学習において学習者がどのような情報に基づき、どのように考え、成果物作成を行ったのかという根拠を記録するとともに、根拠とソフトウェアセキュリティ開発演習成果物との間に関連を設定できるようにする。さらに、その根拠と関連する知識ベースとの関連を記録し、閲覧できるようにする。

④ ソフトウェアセキュリティ開発演習成果物に対するコメントづけ

ソフトウェアセキュリティ開発演習成果物に対してレビューコメントを記述でき、当該成果物との関連を設定できるようにする。このとき、レビューコメントの根拠となる知識ベースとの間にも関連を設定できるようにする。

このうち、知識ベースを管理するためのデータモデルとして、本研究では、Barnum と McGraw が提案した知識のモデルを拡張したデータモデルを提案した。図３に本研究で開発したデータモデルを示す。

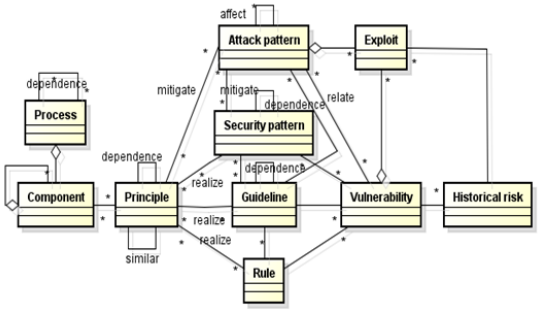

図３ ソフトウェアセキュリティ知識ベースのためのデータモデル

（２） 知識ベースの構築

知識ベース構築のために、ソフトウェアセキュリティに関する文献調査を行った(主な発表論文②，④)。調査対象としたものを表１に示す。

表１：ソフトウェアセキュリティ知識体系化のために行ったサーベイの調査対象

知識の実体	具体事例
Process	● CLASP プロセス(開発に関わる BP の 3 と 4 を対象) ● Sindre と Opdahl によるセキュリティ要求獲得手法
Principle	● Saltzer と Schroeder ● BuildSecurityIn ● CLASP ● NIST
Security pattern	● Yoder と Barcalow
Guideline	● マイクロソフトの Web アプリケーションのための設計ガイドライン ● Mozilla プロジェクトの Web アプリケーションのためのセキュアコーディングガイドライン
Rule	● OWASP Cheat sheet
Attack pattern	● CAPEC

そして、文献調査の結果から Web アプリケーション開発のための知識ベースの構築を行った。図 4 に構築した知識ベースを示す。図からわかるように知識ベースはグラフ構造をしている。図４のノードは表１の具体事例を構成する構成要素である。ノード間の関連は、表１の具体事例の記述にノード間の関連が明記されたものを抽出し、関連として表現している。

図４が示すように、ソフトウェアセキュリティに関する知識は数多くあり、かつ知識間には複雑な関連があることが分かる。

現状の学習環境では、知識間の関連は HTML のハイパーリンクとして表現しているにとどまっている。今後は図４のようなグラフ構造として知識を可視化するとともに、知識を活用するための効果的なナビゲーション支援に関する研究を進めていく必要があることが明らかになった。今後とも研究を継続し、

これらの課題に取り組んでいく予定である。

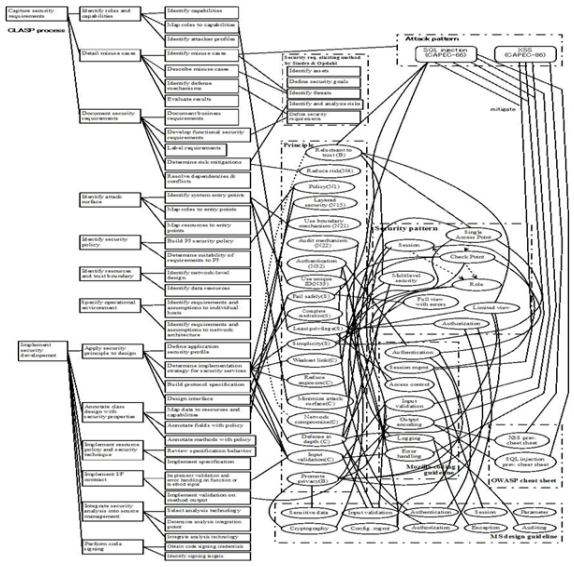

図 4 Web アプリケーション開発のための知識ベース

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 櫨山淳雄, Web アプリケーション開発のためのソフトウェアセキュリティ知識ベース KBSSD の提案, 電子情報通信学会技術報告知能ソフトウェア工学 KBSE2012-72, Vol. 112, No.496, pp.19-24, 2013年3月, 査読無.

② Atsuo Hazeyama, Survey on Body of Knowledge Regarding Software Security, Proceedings of the 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD 2012), pp.536-541, IEEE Computer Society Press, August 2012, 査読有.

③ Atsuo Hazeyama and Hiroto Shimizu, Development of Development of a Software Security Learning Environment, Proceedings of the 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD 2012), pp.518-523, IEEE Computer Society Press, August 2012, 査読有.

④ 櫨山淳雄, ソフトウェアセキュリティ知識体系化に関する研究動向, 電子情報通信学会技術報告知能ソフトウェア工学 KBSE2011-75, Vol.111, No.489, pp.37-42, 2012 年 3 月, 査読無.

⑤ 櫨山淳雄, 清水啓人, ソフトウェアセキュリティ学習環境の開発, 電子情報通信学会技術研究報告知能ソフトウェア工学 KBSE2011-24, Vol.111, No.211, pp.1-6, 2011 年 9 月, 査読無.

〔学会発表〕（計８件）

① 櫨山淳雄, Web アプリケーション開発のためのソフトウェアセキュリティ知識ベースの開発, 情報処理学会第 75 回全国大会, pp.1.291-1.292, 2013 年 3 月 7 日, 東北大学, 宮城.

② Atsuo Hazeyama, Toward Constructing a Software Security Knowledge Base for Web Applications Development, Poster session of The 7th International Workshop on Security, IWSEC2012, 8th November, 2012, Kyushu University, Fukuoka.

③ 櫨山淳雄, ソフトウェアセキュリティのための概念モデル, 情報処理学会第 74 回全国大会, pp.1.301-1.302, 2012 年 3 月 7 日, 名古屋工業大学, 愛知.

④ 大野稔裕, 清水啓人, 櫨山淳雄, ミスユースケース図を利用したセキュアプログラミング学習教材の提案とその評価, 情報処理学会第 74 回全国大会, pp.4.625-4.626, 2012 年 3 月 7 日, 名古屋工業大学, 愛知.

⑤ Atsuo Hazeyama and Hiroto Shimizu, A Learning Environment for Software Security Education, Proceedings of the 5th International Conference on Secure Software Integration and Reliability Improvement (SSIRI2011), pp.7-8, IEEE Computer Society Press, 27th June 2011, Jeju Island, Korea.

⑥ 櫨山淳雄, 清水啓人, ソフトウェアセキュリティ学習支援環境の提案, 情報処理学会第 73 回全国大会, pp.1.259-1.260, 2011 年 3 月 2 日, 東京工業大学, 東京.

⑦ 清水啓人, 櫨山淳雄, Web アプリケーション開発におけるミスユースケースを利用したセキュリティ要求獲得手法の提案, 情報処理学会第 73 回全国大会, pp.1.427-1.428, 2011 年 3 月 2 日, 東京工業大学, 東京.

⑧ 清水啓人, 櫨山淳雄, Web アプリケーション開発における脅威と攻撃の関連付けによるセキュリティ要求獲得手法の提案, 情報処理学会ソフトウェアエンジニアリングシンポジウム 2010 ポスターセッション, 2010 年 8 月 31 日-9 月 1 日, 東洋大学, 東京.

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

該当ありません。

(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

森本　康彦（MORIMOTO　YASUHIKO）
東京学芸大学・情報処理センター・准教授
研究者番号：１０３８７５３２