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

令和　２ 年　 ６ 月 １８ 日現在

機関番号：１２６０４
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００４７５

研究課題名（和文）セキュリティとプライバシーの知識を成果物に関連付ける根拠モデルに基づく学習環境

研究課題名（英文）A learning environment based on a rationale model associating of artifacts with knowledge on security and privacy

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）　　3,400,000円

研究成果の概要（和文）：セキュリティとプライバシーを考慮したソフトウェア開発を支援するための知識を体系的に整理した知識ベースの開発を行った。この知識ベースの１つの特徴として、脅威の型から解決策の型、具体的な解決策に関する知識が関連付けられていることがある。この知識ベースの知識をセキュリティ要求分析の成果物に組み込むことを可能にするツールを開発した。そして、設計段階では、その知識に関連付けられた知識が推薦され、設計学習を行うことが可能なツールも開発した。

研究成果の学術的意義や社会的意義
インターネット、スマートフォンの普及により、様々なアプリケーションを利用するようになった。アプリケーション開発者はセキュリティやプライバシーを考慮して開発を行わなければならない。しかし、セキュリティやプライバシーに関する知識は十分体系化されていない。従って、体系的な知識を開発する意義は大きい。本研究ではセキュリティに関する知識に加えてプライバシーを考慮したソフトウェア開発のための知識ベースを作成した。プライバシーにおける解決策の型に関する知識と原理原則に関する知識の関連付けに成功したことに特徴をもつ。また、知識ベースを介して要求分析の結果から、設計で参照すべき知識を推薦するツールを開発した。

研究成果の概要（英文）：This study aims to create a knowledge base for supporting secure and privacy friendly software development. The knowledge base has a feature that knowledge on threat type, knowledge on solution type to the threat type and concrete knowledge to the solution type are associated. In the security requirements analysis phase, threat types and their solution types are analyzed, and their relationships are embedded into an artifact. By following the relationships, in the design phase, appropriate knowledge is recommended. This study has developed a prototype tool that implements the concept.

研究分野：ソフトウェア工学

キーワード：ソフトウェアセキュリティ　プライバシーバイデザイン　知識ベース　設計根拠

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

インターネット上のサービスは増大し続けている。それに伴い、コンピュータセキュリティとプライバシー保護の重要性が高まってきている。近年、多くのサービスがソフトウェアで実現され、その複雑さが増大しているため、安全でプライバシーを考慮したソフトウェア開発の重要性が認識されている。セキュリティとプライバシーは関連する技術分野であるが、これまでは別々の研究分野として進展してきた。セキュリティについてはソフトウェアセキュリティ [1]という分野で研究が進められてきた。プライバシーの分野は Privacy by Design [2]や Privacy Enhancing Technologies (PET)という分野で研究が進められてきた。扱う技術は異なるものの両分野では、ソフトウェア開発過程全体でセキュリティやプライバシーを扱う必要があるということ並びにソフトウェア開発者はセキュリティやプライバシーの専門家ではないため支援を行いながら、それらの技術を身につけた人材育成が必要であるという認識は一致している。両分野では、方法論、原則、ガイドライン、パターンなどの技術開発がなされている。支援としては知識ベースと事例ベースの 2 つを開発し提供することが考えられる。このうち、知識ベースの枠組である知識の体系化についてはいくつかの研究事例が存在し、例えば、鷲崎らは、セキュリティとプライバシー知識を体系的に整理するためのメタモデルを構築している [3]。セキュリティ技術とプライバシー技術は関連をもつものの、その関連を陽に扱った研究は要求分析手法の PriS method [4]等まだごく一部である。

我々は、セキュアなソフトウェア開発を支援するためのアプローチとして、ソフトウェアセキュリティ分野で研究開発されてきた知識を体系化した知識ベースを構築してきた [5]。さらにセキュリティ要求分析でよく知られたミスユースケース図という成果物を作成するモデリングツールを開発し、知識ベース中の知識を参照しながら、成果物の構成要素単位に参照した知識を設計根拠として関連付けることを可能にし、それを事例として活用する学習支援環境を構築してきた [6]。一方で知識ベース中の知識を成果物に直接関連付けることに対する新規性を明らかにすることが求められた。

２．研究の目的

上述の背景に基づき、本研究では、次の 3 点を明らかにすることを研究の目的とした。

(1) 知識ベースの知識を成果物に関連付けることに関する設計根拠研究における新規性の明確化

セキュリティやプライバシーの要求分析や設計で作成する成果物には、通常利用するシステムの機能や資産に対して、それを脅かす脅威（攻撃）並びにその対策を表現することが提案されている。成果物の構成要素に知識ベースの知識を直接関連付けるというコンセプトは、要求分析や設計で表出された脅威や対策が当該分野のどのような知識に依るものかを根拠として記録することになり、セキュリティの専門家ではないソフトウェア開発者を支援できると考えたものである。根拠の記録と蓄積は Design Rationale [7]という分野で研究がなされており、根拠を記録するための構造に関する研究が進められている。Design Rationale 分野の知見とセキュリティやプライバシーの知識とを融合させた理論的新規性を明らかにする。

(2) セキュリティとプライバシーの関連を扱った知識ベースの構築

セキュリティとプライバシーを考慮したソフトウェア開発のための方法論、ガイドライン、パターン等の知識の開発はそれぞれの分野で活発に行われているが、それら知識間の関連は十分に整理されていないのが現状である。さらに、セキュリティとプライバシーは密接に関わりあう分野であるにも関わらず、その知識間の関連は十分に整理されていない。本研究では、これら知識間の関連を整理した上で、知識ベースの構築を行う。

(3) セキュリティとプライバシー知識を活用して、要求分析・設計活動を支援するモデリングツールの開発

(2)で開発した知識ベースを参照しながら、セキュリティとプライバシーを扱った要求分析・設計活動を支援するツールを開発する。

３．研究の方法

研究目的で挙げた 3 項目に対する研究の方法を述べる。

(1) 知識ベースの知識を成果物に関連付けることに関する設計根拠研究における新規性の明確化

ソフトウェア開発を対象とした Design Rationale 分野に対して系統的文献調査 (Systematic Literature Review: SLR)を実施する。SLR において、設計根拠の情報源として知識ベースを活用している研究動向を把握する。

(2) セキュリティとプライバシーの関連を扱った知識ベースの構築

セキュリティを考慮したソフトウェア開発のために構築した知識ベースの手順に基づき、プライバシーを考慮したソフトウェア開発のための知識ベースを開発する。そのために、これまで行った文献調査、関連研究並びにセキュリティのための知識ベースの知識構造から、知識ベースの基礎となるメタモデルを開発する。続いて、文献調査で得られた既知の知識をメタモデルの実体とする知識ベースを開発する。

(3) セキュリティとプライバシー知識を活用して、要求分析・設計活動を支援するモデリングツールの開発

これまでセキュリティ要求分析の学習を対象に、知識ベースを参照しながらミスユースケース図という成果物を作成するツールを開発した [6]。知識ベースには、セキュリティ要求分析段階で使用する知識と設計段階で使用する知識が関連付けられている場合がある。そのため、セキュリティ設計の成果物を作成する際、その前段階のセキュリティ要求分析で作成された成果物に使用された知識に関連付けられている知識を抽出し、学習者に推薦することが可能になる。学習者はその中から必要な知識を選択して、設計に関する成果物の作成を行うことができる。

４．研究成果

(1) 知識ベースの知識を成果物に関連付けることに関する設計根拠研究における新規性の明確化

Scopus という文献データベースに対してソフトウェア工学における Design Rationale の文献を検索した。概要を読んで、題意に適合する文献を取捨選択した結果 43 件を得た。この中から設計根拠の情報源として知識ベースを活用したものは 1 件であった。しかし、この論文の知識ベース活用方法は我々が意図したものとは異なるものであり、我々の提案は設計根拠の分野において新規性がある可能性を明らかにできた。本成果をコラボレーション技術に関する研究会 [8]並びに国際会議のポスターセッション [9]で発表した。

(2) セキュリティとプライバシーの関連を扱った知識ベースの構築

研究方法で示した手順に従いプライバシーを考慮したソフトウェア開発を支援する知識の概念を整理したメタモデルを開発した (図 1)。また、既存の文献から得られた知識により構築した知識ベースの一例を図 2 に示す。

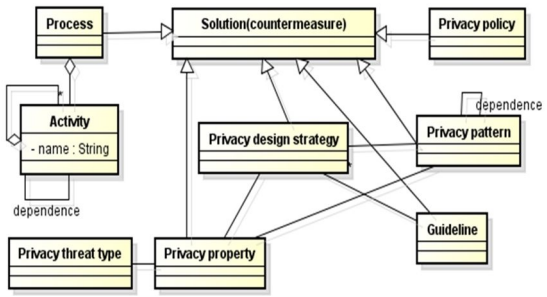

図 1：プライバシー知識ベースのメタモデル

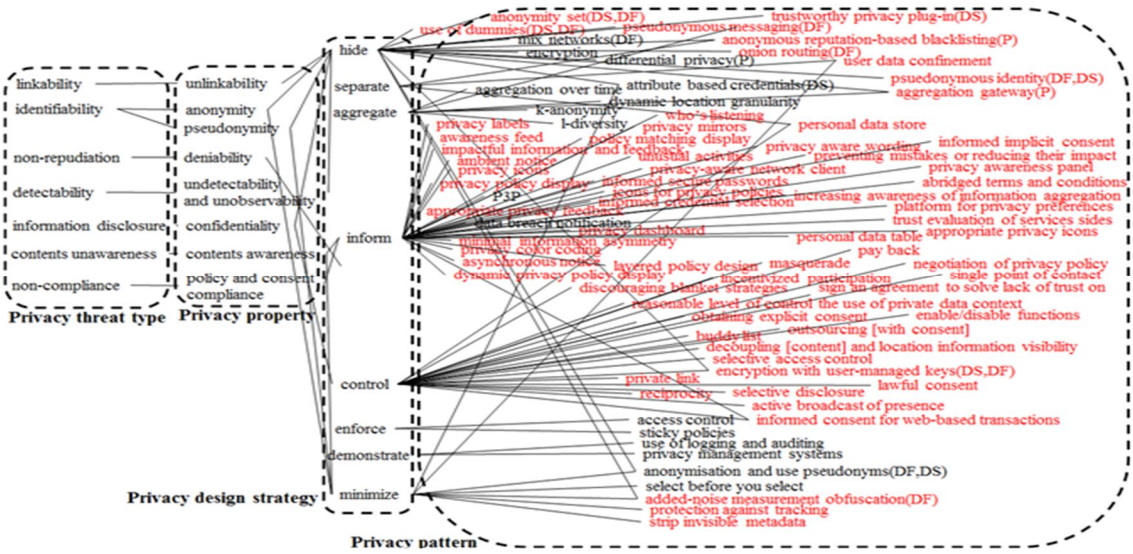

図 2：プライバシー知識ベースの一例

図 1 の構造はセキュリティ知識とプライバシー知識の構造の類似性から提案したモデルであるが、プライバシーの分野では Privacy property と Privacy design strategy を関連付けた研究は存在していなかった。本研究で、Privacy property と Privacy design strategy の既存知識を読み、それらの間に関連があるものを発見し、関連付けに成功した。この関連付けにより、セキュリティにおいて、脅威の型から解決策の型、具体的な解決策の知識を辿って分析から設計活動を支援するのと同様に、プライバシー脅威の型から、解決策の型 (Privacy property)、具体的な解決の知識 (Privacy design strategy, Privacy pattern, Guideline)へつなげる道を開くことができた。また、セキュリティとプライバシーの両分野に共通の脅威の型(情報漏洩)があり、そこを起点として、セキュリティ、プライバシー各々の対応策を、知識ベースを参照して把握することが可能になる。本成果を国内の研究会 [10]で発表するとともに査読付き国際会議に投稿し採録された [11]。

(3) セキュリティとプライバシー知識を活用して、要求分析・設計活動を支援するモデリングツールの開発

研究の方法で述べたコンセプトをツールとして実現した。

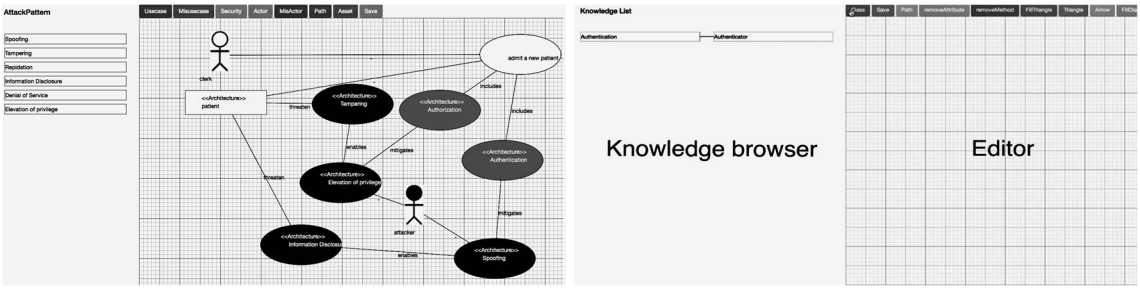

図 3：知識ベースを介したセキュリティ要求分析からセキュリティ設計を支援するツールの画面

図 3 は開発したツールの画面である。左側がセキュリティ要求分析の成果物であるミスユースケース図作成エディタで、右側がセキュリティ設計の成果物であるクラス図作成エディタである。Knowledge browser に推薦された知識が表示されている。例題を用いて、このツールの有効性を示した。エディタを開発すれば同様の考え方でプライバシーを考慮した要求分析から設計の成果物作成を支援することができると考えられる。

本成果を国内の研究会 [12]で発表するとともに査読付き国際会議に投稿し採録され、発表を行った [13]。

参考文献

[1] G. McGraw, Software Security, IEEE Security & Privacy, Vol. 2, No.2, pp. 80-83, 2004.

[2] OASIS Annex Guide to Privacy by Design Documentation for Software Engineers Version 1.0, 2014

[3] Hironori Washizaki, Sota Fukumoto, Misato Yamamoto, Masatoshi Yoshizawa, Yoshiaki Fukazawa, Shinpei Ogata, Eduardo B. Fernandez, Nobukazu Yoshioka, Takehisa Kato, Haruhiko Kaiya, Hideyuki Kanuka, Yuki Kondo, Takao Okubo, and Atsuo Hazeyama, A Metamodel for Security and Privacy Knowledge in Cloud Services, IEEE Services 2016, pp. 142-143, 27 June - 2 July 2016, San Francisco, USA. 2016.

[4] C. Kalloniatis, E. Kavakli, and S. Gritzalis, Addressing privacy requirements in system design: the PriS method, Requirements Engineering, Vol. 13, No.3, pp. 241-255, Springer, 2008.

[5] 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研究報告知能ソフトウェア工学 KBSE2012-72, pp. 19-24, 2013 年 3 月.

[6] 田中俊一, 田中昂文, 沓澤脩, 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 KBSE2015-53, pp. 31-36, 2016 年 3 月.

[7] T. P. Moran and J. M. Carroll Design Rationale: Concepts, Techniques, and Use, CRC Press, 1996.

[8]櫨山淳雄, ソフトウェア工学における設計根拠研究の Systematic Literature Review, 情報処理学会研究報告 Vol. 2019-GN-106, No. 15, pp. 1-6, 2019 年 1 月.

[9] Atsuo Hazeyama, Preliminary Systematic Literature Review on Design Rationale Studies in Software Engineering, The 25th International Conference on Collaboration Technologies and Social Computing (CollabTech2019) (poster), 4 pages, Kyoto, Japan, September 2019.

[10] 櫨山淳雄, 坂元穂波, プライバシーを考慮したソフトウェア開発支援のための知識ベースの提案, 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. 119, No. 467, pp. 61-66, 2020 年 3 月.

[11] Atsuo Hazeyama, Proposal of a Privacy Knowledge Base for Supporting Development of Privacy Friendly Software, Proceedings of the 24th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, September 2020.

[12] 宮原 光, 櫨山 淳雄, 田中 昂文, 鷲崎 弘宜, 海谷 治彦, 大久保 隆夫, 吉岡 信和, 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 KBSE2017-50, Vol. 117, No. 465, pp. 67-72, 2018 年 3 月.

[13] Atsuo Hazeyama, Hikaru Miyahara, Takafumi Tanaka, Hironori Washizaki, Haruhiko Kaiya, Takao Okubo and Nobukazu Yoshioka, A System for Seamless Support from Security Requirements Analysis to Security Design Using a Software Security Knowledge Base, The 6th International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE2019), Proceedings of the 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), pp. 134-140, September 2019.

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Atsuo Hazeyama, Hikaru Miyahara, Takafumi Tanaka, Hironori Washizaki, Haruhiko Kaiya, Takao Okubo and Nobukazu Yoshioka	４．巻 -
２．論文標題 A System for Seamless Support from Security Requirements Analysis to Security Design Using a Software Security Knowledge Base	５．発行年 2019年
３．雑誌名 Proceedings of the 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW)	６．最初と最後の頁 134-140
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/REW.2019.00029	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Atsuo Hazeyama, Shun'ichi Tanaka, Takafumi Tanaka, Hiroaki Hashiura, Seiji Munetoh, Takao Okubo, Haruhiko Kaiya, Hironori Washizaki, and Nobukazu Yoshioka	４．巻 2
２．論文標題 Security Requirement Modeling Support System Using Software Security Knowledge Base	５．発行年 2018年
３．雑誌名 Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)	６．最初と最後の頁 234-239
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC.2018.10235	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Haruhiko Kaiya, Nobukazu Yoshioka, Hironori Washizaki, Takao Okubo, Atsuo Hazeyama, Shinpei Ogata, Takafumi Tanaka	４．巻 CCIS 809
２．論文標題 Eliciting Requirements for Improving Users’ Behavior Using Transparency	５．発行年 2017年
３．雑誌名 Requirements Engineering for Internet of Things	６．最初と最後の頁 41-56
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-10-7796-8_4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 鹿子木 健太，野寄 祐樹，鷲崎 弘宜，深澤 良彰，小形 真平，大久保 隆夫，加藤 岳久，鹿糠 秀行，櫨山 淳雄，吉岡 信和	４．巻 2020-CSEC-88
２．論文標題 機械学習を用いたCVEからCAPECへの関連付け手法の提案	５．発行年 2020年
３．雑誌名 情報処理学会研究報告第182回マルチメディア通信と分散処理・第88回コンピュータセキュリティ合同研究発表会	６．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 櫨山淳雄，坂元穂波	4．巻 IEICE-119
2．論文標題 プライバシーを考慮したソフトウェア開発支援のための知識ベースの提案	5．発行年 2020年
3．雑誌名 電子情報通信学会技術研究報告知能ソフトウェア工学	6．最初と最後の頁 61-66
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 櫨山淳雄	4．巻 2019-GN-106
2．論文標題 ソフトウェア工学における設計根拠研究のSystematic Literature Review	5．発行年 2019年
3．雑誌名 情報処理学会研究報告第106回GN研究発表会	6．最初と最後の頁 1-6
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 山田侑樹，櫨山淳雄，吉岡信和	4．巻 118
2．論文標題 ソフトウェアセキュリティ知識ベースを用いた要求分析及び設計における知識提示手法の開発とケーススタディによる評価	5．発行年 2019年
3．雑誌名 電子情報通信学会技術研究報告知能ソフトウェア工学	6．最初と最後の頁 51-56
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 宮原 光，櫨山 淳雄，田中 昂文，鷲崎 弘宜，海谷 治彦，大久保 隆夫，吉岡 信和	4．巻 117
2．論文標題 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開発	5．発行年 2018年
3．雑誌名 電子情報通信学会技術研究報告知能ソフトウェア工学	6．最初と最後の頁 67-72
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　0件）

1．発表者名 橋浦 弘明，榎本 大貴，宇南山 直紀，櫨山 淳雄
2．発表標題 知識ベースを利用したIDPSルール自動生成手法の提案
3．学会等名 2020年電子情報通信学会総合大会
4．発表年 2020年

1．発表者名 山田 侑樹，櫨山 淳雄，吉岡 信和
2．発表標題 ソフトウェアセキュリティ知識ベースを用いた要求分析及び設計における知識提示手法の提案
3．学会等名 情報処理学会第81回全国大会
4．発表年 2019年

1．発表者名 櫨山淳雄，鷲崎弘宜，吉岡信和
2．発表標題 知識ベースを用いたプライバシーを考慮したソフトウェア開発支援に向けて
3．学会等名 2019年電子情報通信学会総合大会
4．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	大久保　隆夫 (0kubo Takao) (80417518)	情報セキュリティ大学院大学・その他の研究科・教授 (32721)	

6．研究組織（つづき）

	氏名 （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	海谷　治彦 (Kaiya Haruhiko) (30262596)	神奈川大学・理学部・教授 (32702)	
研究分担者	橋浦　弘明 (Hashiura Hiroaki) (20597083)	日本工業大学・先進工学部・准教授 (32407)	
研究分担者	吉岡　信和 (Yoshioka Nobukazu) (20390601)	国立情報学研究所・アーキテクチャ科学研究系・准教授 (62615)	
研究分担者	鷲崎　弘宜 (Washizaki Hironori) (70350494)	早稲田大学・理工学術院・教授 (32689)	