セキュアなソフトウェア開発のためのソフトウェアセキュリティ知識ベースを活用したモデリングツールの提案

田中俊一[†1]　田中昂文[†2]　齋藤大仁[†2]　櫨山淳雄[†1]　橋浦弘明[†3]

あらまし　近年、ソフトウェアの脆弱性を狙ったサイバー攻撃が増加しており、ソフトウェアセキュリティの重要性が高まっている。そして、ソフトウェア開発過程でセキュリティを考慮したセキュアな開発の重要性が指摘されている。本論文では、先行研究であるソフトウェアセキュリティ知識ベースと成果物開発環境を統合したモデリングツールを提案する。作成される成果物の構成要素単位にソフトウェアセキュリティ知識を関連付けることにより、効率的に適切なセキュリティを施したソフトウェアセキュリティ開発成果物を実現する。提案するモデリングツールの要件を抽出し、開発に向けた設計を述べる。

Proposal of a Modeling Tool for Secure Software Development using Software Security Knowledge Base

SHUNICHI TANAKA[†1]　TAKAFUMI TANAKA[†2]　MASAHITO SAITO[†2]
ATSUO HAZEYAMA[†1]　HIROAKI HASHIURA[†3]

In recent years, cyber attacks targeted for software vulnerability increase, therefore importance for software security also increases. Software security aims to develop secure software by taking security into consideration in the whole software process. This paper proposes a modeling tool that integrates an artifact creation environment with a software security knowledge base. Associating of each element composing of an artifact with software security knowledge enables to create artifacts for secure software in an effective manner. This paper discusses requirements for the modeling tool and describes functional design of the tool.

1. はじめに

インターネットサービスの増加によりインターネット利用者数も増加しており、それとともに不正アクセスやWebサイト改ざんなどのサイバー攻撃も増加している。このような標準的な攻撃手口の多用や攻撃の多様化を防ぐために、情報の管理の徹底/強化やセキュリティ対策の重要性が高まってきている[1]。多くのサービスがソフトウェアで実現されているが、今日ではセキュリティなどの非機能要件に関わる部分もユーザーは重要視しており、その中でもセキュリティは施すべきこととし、機能要件として扱われてきている[2]。セキュリティをソフトウェア開発過程全体で扱うことを目指し、これまでに開発プロセス、方法論、パターン、ガイドライン、ルールなどのソフトウェアセキュリティ技術が開発されてきた。しかしながら、これらの技術には複雑な関連があり、各知識や技術をどのように活用してセキュアなソフトウェア開発を実現していくかという、活用技術に関する研究が少ない。

これに対し斉藤ら[3]は、ソフトウェアセキュリティに関する技術や知識を体系化したソフトウェアセキュリティ知識ベース管理システム(以下、知識ベースと呼称)と、作成された成果物を管理する成果物管理システムを連携させ、ソフトウェアセキュリティ知識(以下、知識と呼称)と成果物の関連を蓄積した事例ベース管理システムを開発した。しかしながら、有効性に関する評価実験から以下の3つの問題点が挙げられている。

(i) 知識ベースと成果物開発環境が異なるため知識との関連付けが困難である。

(ii) 知識は成果物単位で関連付いているため、知識が成果物のどの部分と関連しているか不明確である。

(iii) 考慮または実現すべきセキュリティに関する前提条件が明らかになっておらず何をどこで考慮すべきか、またどの程度のセキュリティを施せばよいか示されていない。

ソフトウェア開発でセキュリティを考慮したとき、無数に潜在する脅威を防ぐためにはそれぞれ適切な対策が必要であり、付随する正しい知識が求められる。したがって、ソフトウェア開発を通じて作成された成果物の構成要素ごとに適切なセキュリティを対策することが重要である。そこで本研究では、効率的にそれらを実現することと斉藤らの研究の問題解決を目的に、知識ベースと成果物開発環境を統合したモデリングツールの提案を行う。

2. モデリングツール

2.1. モデリングツールの要件

前節で述べた問題点の解決を踏まえた要件および提案するモデリングツールで必要となる要件について述べる。

要件1：成果物の作成としてモデル図が描写できること
要件2：知識ベースを使用できること
要件3：成果物の構成要素単位に、知識ベースに蓄積されている知識と関連付けられること
要件4：成果物の構成要素単位にコメント、レビューコメントを付与できること。またコメント、レビューコメントにも知識ベースの知識と関連付けることができること
要件5：成果物の管理および閲覧することができること
要件6：ソフトウェアセキュリティ考慮の基準などの前提条件が記述および閲覧できること

要件1、要件2は問題点(i)に対する要件であり、モデリングツールではこれらを統合させることにより、同じ開発環境下で知識と成果物の構成要素ごとに関連を持たせ、設

†1 東京学芸大学
Tokyo Gakugei University
†2 東京学芸大学大学院
Graduate School of Education, Tokyo Gakugei University
†3 日本工業大学
Nippon Institute of Technology

計根拠を明確にする。

要件 3 は問題点(ii)に関する要件である。成果物の構成要素ごとに存在する脅威はそれぞれ異なり、場合によっては 1 つの要素に対して複数の脅威が考えられ、それぞれ異なる知識を関連付ける必要がある。したがって、構成要素ごとに抽出した脅威を、知識ベースの 1 つ 1 つの知識と関連付けることにより、対象となる脅威に適切な対策を施し、対策の漏れを減少させることができる。

要件 4、要件 5 は開発者の成果物作成過程に関する要件である。成果物を記録するとともに、作成過程における開発者の意図を記録し設計根拠を明確にする。またレビューコメントから、成果物の要素と知識との整合性を確認したり考察することによって成果物の品質向上を促す。

要件 6 は問題点(iii)に関する要件である。ソフトウェアセキュリティを考慮した成果物を作成するときに、どのくらいセキュリティレベルを考慮するか、また作成したときにそれぞれのセキュリティをどこまで実現すればよいかの基準を明確にする。

全ての要件を満たすことにより、成果物の作成時にそれぞれの脅威にそれぞれの対策を効率的に関連付け、セキュアなソフトウェアの開発を実現していく。

2.2. モデリングツールの機能

前項で述べた要件を満たすモデリングツールが提供する機能について述べる。

(1) 成果物作成機能

要件 1,4 を満たすための機能で、ソフトウェア開発を通じて作成する成果物としてモデル図を対象とする。今回は、ミスユースケース図を拡張した大久保らの手法[4]を対象とする。また、成果物の構成要素ごとにコメントを記述することができ、作成された根拠も記録できる。成果物作成の一連の作業は逐次保存される。

(2) 成果物と知識の関連付け機能

要件 2,3 を満たすための機能で、作成された成果物の構成要素ごとに、知識ベースに蓄積された各知識の情報を付与することができる。

(3) 知識閲覧機能

要件 2 を満たすための機能で、これは知識ベース管理として実現されている。成果物の構成要素ごとに知識を関連付ける際、可視化された知識ベースを参照して適切な対策を選択する。また、選択された知識は概要や実装方法などの詳細情報を閲覧することができる。

(4) レビュー機能

要件 4 を満たすための機能で、成果物やその構成要素ごとにレビューコメントを記述することができる。また、レビューコメントにも根拠となる知識も関連付けることができる。

(5) 成果物閲覧機能

要件 5 を満たすための機能で、そのために成果物の版管理を行う。成果物は、同じ開発メンバー同士ならば閲覧およびレビューすることができる。

(6) 前提条件記述・閲覧機能

要件 6 を満たすための機能で、各プロジェクトの成果物を作成するときの考慮すべきセキュリティレベルや、成果物が作成されたときにどこまで実現すべきかを記述または閲覧することができる。

2.3. 画面設計

提案するモデリングツールの成果物作成時における画面イメージを図 1 に示す。図中の番号に分けてそれぞれの役割を記述する。

① 成果物作成領域

モデル図を描写して成果物を作成する領域である。

② 詳細確認領域

成果物の構成要素を選択したときに、その詳細情報を表示する領域である。この領域で値の編集を可能とし、結果を成果物にも反映することができる。

③ 知識ベース閲覧領域

斉藤らが開発した知識ベースを閲覧する領域である。選択した知識を④でその詳細情報を確認することができる。

④ 知識詳細確認領域

③で選択された知識の詳細情報を表示する領域である。また、表示された知識名を成果物の選択された構成要素と結びつけることができる。

⑤ 編集切り替え領域

タブを切り替えることによって成果物の作成やレビューコメントの記述/閲覧、また前提条件の記述/閲覧ができる領域である。

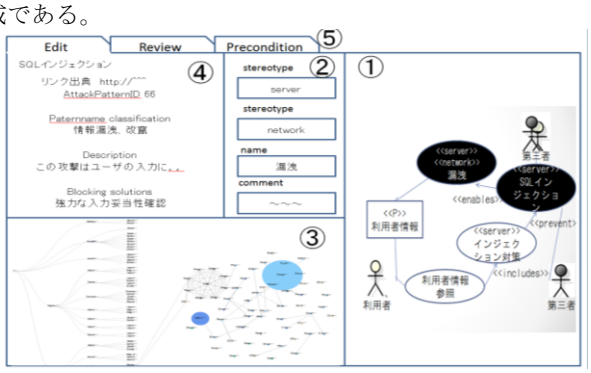

図 1. 成果物作成時の画面イメージ

3. 実装環境

前節で述べた機能を満たす実装環境について述べる。モデリングツールは OSS である GWTUMLDrawer[5]を改変し、拡張したミスユースケース図の描写および知識ベースの統合を行う。

4. まとめと今後の課題

本稿では、知識ベースと成果物開発環境を統合したモデリングツールの提案について述べた。斉藤ら[3]が述べた問題点の解決を目的に、成果物の構成要素ごとに知識を関連付けることによって、要素ごとに適切なセキュリティの識別とその対策を記述できる。また、知識ベースと成果物開発環境の統合により、効率的にセキュアな成果物を実現することを可能にする。

今後は成果物開発環境の実装および知識ベースと統合し、評価実験を行う予定である。

謝辞

本研究は科学研究費補助金基盤研究(C)26330394 の助成の下で行われている。

参考文献

[1] TRENDMICRO : サイバー攻撃の傾向と実態, http://www.trendmicro.co.jp/jp/sp/asr-2013/

[2] NPO 日本ネットワークセキュリティ協会(JNSA): JNSA セキュアシステム開発ガイドライン, http://www.jnsa.org/active/houkoku/web_system.pdf

[3] 斉藤 大仁, 櫨山 淳雄, 吉岡 信和, 小橋 孝紀, 鷲崎 弘宣, 海谷 治彦, 大久保 隆夫 : ソフトウェアセキュリティ知識を活用したセキュアなソフトウェア開発のための事例ベース管理システムの開発, 信学技報, KBSE2014-57, pp.31-36, 2015.

[4] 大久保 隆夫, 田中 英彦 : 効率的なセキュリティ要求分析手法の提案, 情報処理学会論文誌, Vol.50, No.10, pp.2484-2499, 2009.

[5] GWTUMLDrawer, http://gwtuml.googlecode.com/svn/trunk/GWTUMLDrawer/war/GWTUMLDrawer.html#Start