4N-06

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

山田 侑樹† 櫨山 淳雄† 吉岡 信和‡
東京学芸大学† 国立情報学研究所‡

1. はじめに

情報セキュリティにおける脅威は増大の一途を辿っており，毎年のように新たな脅威が出てきている[1]．一方，IT の高度化，多様化の中，情報セキュリティを担うセキュリティ人材が不足しているという問題点がある．セキュアなソフトウェアを開発する上で，セキュリティはソフトウェア開発の各工程で意識される必要がある．セキュリティ知識に乏しい開発者がこれを意識しソフトウェア開発を行うことは困難である．

文献[2]ではソフトウェアセキュリティのための知識を分類，関連付けを行うことでセキュリティ知識を体系的にまとめた知識ベースを開発している．この知識ベースを活用して，セキュアなソフトウェア開発事例とセキュリティ知識を結びつける事例ベースを開発する研究[3]，セキュリティ要求分析のためのモデリングツールの開発[4]，セキュリティ要求分析の結果からセキュリティ設計を支援する研究[5]がこれまで行われてきた．開発者がセキュアな開発を進めるために知識ベース内からセキュリティ知識を適切に選択する必要があるが，これまでの研究では，その支援はなされていない．

そこで本研究では，セキュリティ知識に乏しい開発者が適切にセキュリティ知識を選択するためにソフトウェアセキュリティ知識ベースを用いた知識の提示手法を提案する．対象とする開発者は Web アプリケーション開発者とする．本論文ではソフトウェア開発プロセスの要求分析時に開発者に対し，セキュリティ要求獲得のためのソフトウェアセキュリティ知識を提示し，そこで選択された知識からソフトウェアの設計のための知識を提示する手法を述べる．

2. ソフトウェアセキュリティ知識ベース

本節では，本研究の前提となるソフトウェアセキュリティ知識ベースの概要と課題，その課題に対する解決策の概要を述べる．

Proposal of Knowledge Presentation Method in Security Requirement Analysis and Design Using a Software Security Knowledge Base
† Yuki Yamada, Tokyo Gakugei University
† Atsuo Hazeyama, Tokyo Gakugei University
‡ Nobukazu Yoshioka, National Institute of Informatics

2.1 概要

文献[6]では Barnum と McGraw が 7 つの知識カタログ（principle, guideline, rule, attack pattern, vulnerability, exploit, historical risk）とその関連をモデル化したもの並びに文献[7]を参考に，14 個の知識とその関連により知識ベースのメタモデルを提案している．知識ベースの構築には Web 上で公開され入手可能な既存の成果を使用している．

2.2 課題と解決策の概要

ソフトウェアセキュリティ知識ベースはセキュリティ知識を関連に基づき整理したものだが，それらの知識をどのように使用するかの支援は十分でない．そこで知識を効果的に活用するためにいつどのように提示するかを考える必要がある．一般にソフトウェア開発は要求定義，設計，実装，テストという段階にわけて考えられる． OWASP Proactive Controls[8]によれば，セキュアなソフトウェアを実装する上で最も重要なことは「セキュリティ要求の定義」としていることから，開発の初期段階である要求定義において知識を的確に取り出すことは非常に重要である．以下では脅威の分析と対策時の知識の提示手法について述べる．

3. 脅威に関する知識提示の流れ

セキュリティ要求を定義するにはソフトウェアに対する脅威を特定する必要がある．今回は，脅威の分類手法である STRIDE[9]に注目し，これに基づいた脅威の知識の提示を行う．

3.1 STRIDE

STRIDE とは Microsoft がソフトウェアに対する脅威の分類として Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege の 6 つを定義し，その頭文字をとった脅威分類手法である．

3.2 具体的な脅威の特定

ソフトウェアセキュリティ知識ベースでは脅威に関する知識は Attack pattern のインスタンスとして管理されている．この Attack pattern の知識を STRIDE で分類することで具体的な脅威の知識の提示を行う．改ざんの分類により提示される脅威の知識の例を図 1 に示す．

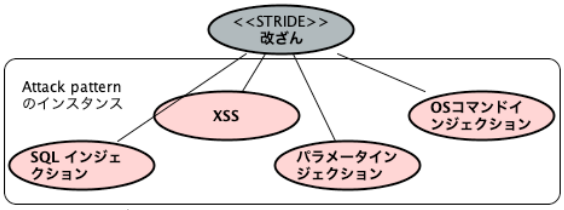

図 1：改ざんの分類により提示される知識の例

4. 対策に関する知識提示の流れ

セキュリティ要求分析では，特定された脅威への対策となるセキュリティ要求を規定する必要がある．ソフトウェアセキュリティ知識ベースでは Attack pattern への対策は Solution type に基づいて提示する．以下では Solution type について述べる．

4.1 Solution type の拡張

従来の Solution type[9]は STRIDE の抽象度に対応したものであり，具体的に特定した脅威から対策の知識を取り出すには抽象度が高すぎるという問題点があった．そこで Solution type を Microsoft が Microsoft Threat Modeling Tool の軽減策[10]で示す軽減策のカテゴリを用いて拡張する．拡張後の Solution type と STRIDE との関係を表 2 に示す．

表 2: 拡張後の Solution type と STRIDE の関係

Solution type(拡張後)	S	T	R	I	D	E
Authentication(認証)	○					
Session Management (セッション管理)	○					○
Input Validation(入力検証)		○		○	○	○
Auditing and Logging (監査とログ記録)		○	○			
Communication Security (通信のセキュリティ)		○		○		○
Cryptography(暗号化)		○		○		○
Sensitive Data (機密性の高いデータ)		○		○		○
Exception Management (例外管理)		○	○	○	○	
Authorization(承認)						○
Configuration Management(構成管理)		○		○	○	○

この分類に基づき Principle や Guideline，Security pattern の対策に関する知識を関連付ける．Principle はセキュアなソフトウェアを開発する上で経験から導かれたセキュリティ知識，Guideline は意味的なレベルで，行うべきことや避けるべきことをまとめたセキュリティ知識，Security pattern は繰り返し生じるセキュリティの問題に対して対策をパッケージしたセキュリティ知識である．入力検証の分類により提示される対策の知識の例を図 2 に示す．

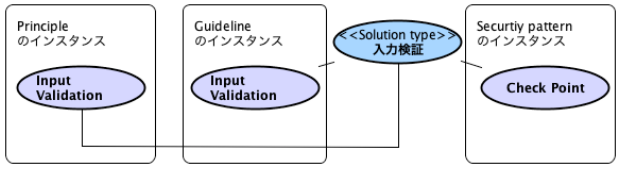

図 2: 入力検証の分類により提示される知識の例

5. おわりに

本研究では STRIDE による抽象的な脅威の分類からソフトウェアセキュリティ知識ベース内の脅威の知識を提示する手法と，その脅威の対策となる知識を提示する手法について述べた．STRIDE を用いることの利点は抽象的な脅威の分類であることにより，脅威の分析漏れをなくすことができ，かつ未知の脅威に対しても STRIDE で分類が可能な脅威であれば今後も提案手法が有効であることである．一方で STRIDE による分類は脅威の対策を規定するには抽象度が高いため Web アプリケーションに焦点を当てた対策の分類を付与することで脅威の対策の知識を関連付けることとした．本手法は Web アプリケーション開発に特化したものだが，提案手法を用いることで，ソフトウェアセキュリティ知識ベース内の知識を開発者がより効率的に活用できると考えられる．

謝辞

本研究の一部は科学研究費補助金基盤研究(B)15H02686 並びに基盤研究(C)17K00475 の助成の下で行われた．記して謝意を表す．

参考文献

[1] IPA 情報処理推進機構: 情報セキュリティ 10 大脅威 2018, https://www.ipa.go.jp/security/vuln/10threats2018.html (2018.12.8).
[2] 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, Vol.112, No.496, pp. 19-24, 2013.
[3] 櫨山淳雄他: 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 Web アプリケーション開発事例ベースの試作, 電子情報通信学会研究報告知能ソフトウェア工学, Vol.114, No.420, pp.49-54, 2015.
[4] 田中俊一他: 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.
[5] 宮原光他: 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, 電子情報通信学会研究報告知能ソフトウェア工学, Vol.117, No.465, pp.67-72, 2018.
[6] Atsuo Hazeyama, et al.: Security Requirement Modeling Support System using Software Security Knowledge Base, COMPSAC 2018, pp.234-239, 2018.
[7] Hironori Washizaki, et al.: A Metamodel for Security and Privacy Knowledge in Cloud Services, IEEE Services 2016, pp. 142-143, 2016.
[8] OWASP: OWASP Proactive Controls, https://www.owasp.org/index.php/OWASP_Proactive_Controls (2018.10.20).
[9] Microsoft: Microsoft STRIDE chart, https://cloudblogs.microsoft.com/microsoftsecure/2007/09/11/stride-chart/ (2018.11.12).
[10] Microsoft: Microsoft Threat Modeling Tool の軽減策, https://docs.microsoft.com/ja-jp/azure/security/azure-security-threat-modeling-tool-mitigations (2018.11.12).