可視化された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学習支援環境

齊藤 大仁[†] 櫨山 淳雄[††]

多くのサービスがソフトウェアで実現され，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．筆者らはセキュアなソフトウェア開発のための学習支援環境を構築することを目指している．本研究では先行研究での評価実験の結果をもとに，使用するソフトウェアセキュリティ知識等を可視化することで，より効果的な学習支援環境を提案する．

A Learning Support Environment for Secure Software Development Using Software Security Knowledge by Visualization

MASAHITO SAITO[†] ATSUO HAZEYAMA[††]

The importance of software security technologies is increasingly recognized with the increase in services available on the Internet. The authors aim to construct a learning support environment for secure software development. Based on the results from an experiment that was conducted in the previous study, this paper proposes an enhanced learning support environment by visualizing software security knowledge and introducing a traceability support of artifacts.

1. はじめに

情報通信技術の進展はめざましくネットワークを介した様々なサービスが提供されてきた．それとともにセキュリティの問題も顕在化してきた．特に近年，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，ネットワークセキュリティ技術のみでなくソフトウェアセキュリティ（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にソフトウェアを開発する）技術の重要性が認識されるようになってきている[1]．その一方で，ソフトウェアセキュリティ知識を熟知した人材が不足している現状から，ソフトウェアセキュリティ技術を身につけた人材育成の重要性が指摘されている[1]．高等教育では PBL（Project-Based Learning）形式のソフトウェア開発演習が行われているが，セキュリティを意識している事例は少ない[2]．

我々はソフトウェアセキュリティをソフトウェア開発ライフサイクル全体で学ぶための学習支援環境を構築することを目指している[3]．先行研究では，学習支援環境のプロトタイプを用いた評価実験を行った[4]．本論文では評価実験の結果をもとに，使用するソフトウェアセキュリティ知識の可視化など学習支援環境の効果的な利用のための支援を検討する．

†東京学芸大学大学院
††東京学芸大学

2. 学習支援環境への要件

2.1. 評価実験の結果からの要件

先行研究では学習支援環境を使用し，オンラインショッピングにおける利用者登録，利用者情報参照を対象にセキュリティ要求分析を行い，ミスユースケース図を作成する評価実験を行った[4]．対象は PBL 形式でのソフトウェア開発演習を経験し，2ヶ月間ソフトウェアセキュリティに関する講義を受けた大学院生である．次項で実験から得られた知見をもとに学習支援環境への改善要件を述べる．

2.2. 要件の抽出

2.2.1. ソフトウェアセキュリティ知識の可視化

本学習支援環境で扱うソフトウェアセキュリティ知識は 10 個の実体クラスとその関連としてモデル化されている[5]．実際に開発で利用する知識は各クラスのインスタンスであり，大規模かつ複雑なネットワーク構造をしている．評価実験では，「知識がクラスごとに管理されているため，探しやすい」という意見があった．その一方で，「学習者のソフトウェアセキュリティ知識への理解が足りない場合，求めるソフトウェアセキュリティ知識とその関連の検索が難しい」という意見もあった．そのため，各知識がどのクラスに属するのかを把握できるようにするとともに，ソフトウェアセキュリティ知識の全体像のネットワーク構造を直接俯瞰できるようにする必要が

ある．この時，初学者は何を行えばよいか十分理解していないことを想定し，知識はプロセスを起点としてそれに関連する知識を配置することを考える．さらに，多く閲覧されている知識，多く利用されている知識を視覚的に表現することにより，知識の効果的な利用につなげられると考える．

2.2.2. ソフトウェアセキュリティ知識と成果物間の関連の可視化

本学習環境で作成される成果物はそれを作成するために利用した知識を根拠として関連づけることを想定している[3]．知識は異なる抽象度のものが関連付けられていることもある．そのため，成果物は工程によりモデル化される抽象度が異なる．評価実験では，要求分析段階でどの程度まで詳細に記述するべきかという議論があった．異なる抽象度の知識が確実に開発に反映されることを追跡できるために，全工程の成果物を保管するとともに，その間の関連を管理してトレーサビリティ(追跡可能性)を実現する必要がある．

3. 要件を実現するための機能開発

2 節の要件を実現するために，データに基づいて視覚的に表現することが求められる．可視化の手段としてD3.js[6]を使用した可視化を検討する．

3.1. ソフトウェアセキュリティ知識の可視化機能

知識とその関連をネットワーク構造として表現する．ノードはソフトウェアセキュリティ知識[5]を構成する各クラスのインスタンスであり，セキュアなソフトウェアを開発するためのプロセスを起点として配置する．また，同一のクラスの知識は同じ色にし，ノード上に知識名を表示する．リンクは関連が存在するノード間を結ぶ．ノードを選択した際に関連する隣接ノードを強調表示する．さらに，知識の利用頻度に対応してノードの大きさを変え，知識の閲覧頻度は全体像とは別に昇順のリストを表示することを提案する．これにより，プロセスを起点に各知識の関連を俯瞰，閲覧されている知識等の使用状況を視覚的に表現することができるため，要件 2.2.1 を満たす．ソフトウェアセキュリティ知識の全体像を図 1 に示す．

3.2. ソフトウェアセキュリティ知識と成果物間の関連の可視化機能

成果物と使用した知識の関連をネットワーク構造として表現する．ノードは成果物と各工程の成果物を作成するために使用したソフトウェアセキュリティ知識である．成果物のノードは同一の成果物の種類（仕様書，ユースケース図等）は同じ色にし，ノード上に成果物名を表示する．また，ソフトウェアセキュリティ知識のノードは，3.1 項と同様の色で表示し，知識名を表示する．リンクには成果物間の関連と，成果物と知識間の関連があり，それぞれ色分けすることを提案する．成果物とソフトウェアセキュリティ知識のノードの色が同じであっても区別可能なように成果物ノードを四角，知識ノードを円形で表示する．これにより，成果物を起点として，各工程の成果物と使用したソフトウェアセキュリティ知識を俯瞰することができ，同一画面上に表示することで関連の追跡が可能であるため，要件 2.2.2 を満たす．

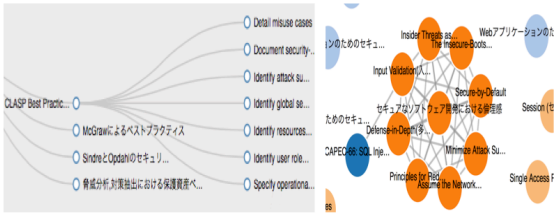

図1　ソフトウェアセキュリティ知識ベースの可視化

4. まとめ

本論文では，ソフトウェアセキュリティ学習支援環境のプロトタイプを用いた評価実験の結果をもとに，学習支援環境を効果的に利用するための支援を検討，実装した．評価実験の結果から，効果的な利用のためにソフトウェアセキュリティ知識と成果物，それらの間の関連の可視化支援が求められた．そこで，ソフトウェアセキュリティ知識や成果物の色分けを行い，全体像を把握可能な機能を実装した．今後は，これらの機能の評価を行うとともに，ライフサイクル全体での事例を作成することを予定している．

謝辞　本研究の一部は科学研究費補助金基盤研究(C)22500910 並びに 26330394 の助成のもとで行われた．記して謝意を表す．

参考文献

[1] McGraw, G.: Software Security, IEEE SECURITY&PRIVACY, Vol.2, No.2, pp.80-83, 2004.
[2] Du, W., Jayaraman, K., and Gaubatz B. N.: Enhancing Security Education with Hands-on Laboratory Exercises, Proc. ASIA'10, pp.56-61, 2010.
[3] 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開発，信学技報 KBSE2011-24，pp.1-6, 2011.
[4] Hazeyama, A., and Saito, M.: Preliminary Evaluation of a Software Security Learning Environment, Studies in Computational Intelligence, Springer, 2014 (To appear).
[5] 櫨山 淳雄: ソフトウェアセキュリティ知識体系化のための概念モデル，情報処理学会第 74 回全国大会, 2012.
[6] Murray, S.:インタラクティブ・データビジュアライゼーション - D3.js によるデータの可視化，オライリージャパン, 2014.