ソフトウェア開発初学者を対象とした SDPBL における学習者のセキュリティ意識向上を促す Bot システムの提案

山田侑樹† 櫨山淳雄†

概要：Web 上で様々なサービスが提供されるようになり，セキュリティへの関心はますます高まっている．これらのサービスを安全に利用するためには，利用者だけでなく開発者がセキュリティを考慮して開発することが重要である．そこでソフトウェア開発の一連の流れをプロジェクト形式で実践的に学ぶソフトウェア開発 PBL において初学者のセキュリティ意識向上を支援する Bot システムを提案する．

キーワード：ソフトウェアセキュリティ，セキュリティ教育，ソフトウェア開発 PBL

1. はじめに

近年，Web 上で様々なサービスが提供されている．これらのサービスを利用者が安全に利用するためには，利用者のセキュリティ意識を高めるだけでなく，開発者がセキュリティを考慮したシステムを構築することが重要である．しかしセキュリティ知識に乏しい開発者がセキュリティを意識して開発を行うことは困難である．システムのセキュリティを担保するためには，セキュリティ要求を正しく獲得する必要がある.セキュリティ要求を獲得するためには，システムに対する脅威の存在を認識する必要があり，脅威を認識できていない場合，結果としてシステムには脆弱性という形でセキュリティ上の欠陥が生じることになる．

本研究ではセキュリティ知識に乏しい開発者として，情報系を専攻する学部生を想定し，ソフトウェア開発の一連の流れをプロジェクト形式で学ぶソフトウェア開発 PBL（Software Development Project Based Learning: SDPBL）に注目する．はじめに，SDPBL において，彼らがどの程度までセキュリティを意識した開発を行っているのかを明らかにし，そこから得られた課題をもとにセキュリティを考慮した開発を進めるための支援を検討する．

本稿では,セキュリティ意識の現状と課題を述べたのち，それらの課題を解決する研究計画について述べる．

2. 現状と課題

本節では，本学で実施されている SDPBL 科目である「システム・プログラミング」の授業の概要と，これまでの受講生の成果物から受講生が考慮していたセキュリティ項目について述べる．

2.1 SDPBL の概要

本学で行われている SDPBL は情報系の学部 3 年生を対象に開設されており，課題に沿った Web アプリケーションをチームで開発する．１チームのあたりの人数は３～５名程度である．開発手順はウォータフォールモデルに準拠しており，要求定義，設計，実装，テストの 4 つの工程で進められる．受講生は上流工程において成果物が出来上がり次第，インスペクションという形で教授やティーチングアシスタント（TA）から所定の回数フィードバックを受けることができる．受講生は過去に Web アプリケーションを作成した経験があることを条件としており，講義の実施要領においてセキュリティに考慮して開発に取り組むことが示されている．

2.2 SDPBL の成果物から見られる受講生のセキュリティ意識とセキュリティ知識の現状

今回は，2017 年度，2018 年度の受講生が作成した要求仕様書と作成した Web アプリケーションの最終版を脆弱性診断ツール OWASP ZAP[1]を用いて作成したレポートから受講生が意識していたセキュリティ項目を確認した．2017 年度，2018 年度ともグループ数は 2 グループであり，計 4 つのグループを対象とした．それぞれの仕様書において確認されたセキュリティ項目を表 1 に示す．ログイン機能，ログアウト機能，XSS 対策の 3 つの項目は全てのグループで確認できた．他の項目についてはグループによって差が見られた．一方で，OWASP ZAP を用いて作成したレポートの結果の要約を表２に示す．OWASP ZAP では，診断結果の脆弱性のレベルを High，Medium，Low，Informational の４段階で示す．４グループ中３グループで High を示す脆弱性が確認された．この項目は「クロスサイト・スクリプティング（反射型）」であり，要求仕様書では対策を施すと記述されていた項目であった．ただし OWASP ZAP で発見される脆弱性は，1 箇所でも脆弱性が存在すれば，レポートでは脆弱性があると検出するため，受講生の成果物の全ての箇所で対策が不足しているとは言えない．また，ここで確認している成果物は全てチームでの成果物であり，受講生の個々人のセキュリティ意識については把握できていないということに考慮されたい．しかしながら受講生の成果物から，受講生のセキュリティ知識が不足しているの

† 東京学芸大学
Tokyo Gakugei University

ではないかということは示唆された．

表 1　仕様書から確認されたセキュリティ項目

セキュリティ項目	2017 年度		2018 年度	
	G1	G2	G1	G2
ログイン機能	○	○	○	○
ログアウト機能	○	○	○	○
XSS 対策	○	○	○	○
パスワードのハッシュ化	○			
アカウントロック		○		
ロールベースアクセス制御		○		○
セッションのタイムアウト				○

表 2　OWASP ZAP で作成したレポートの要約

脆弱性のレベル	2017 年度		2018 年度	
	G1	G2	G1	G2
High	0	1	1	1
Medium	4	4	1	2
Low	3	4	2	2
Informational	0	0	0	0
合計	7	9	4	5

3. 本研究の概要

前節より，受講生はセキュリティ知識が足りていないと仮定する．筆者らはこれまで，ソフトウェアセキュリティ知識ベースを用いてセキュリティ知識に乏しい開発者への支援について研究を行ってきた[2]．これらを活用して，SDPBL において受講生のセキュリティ知識を補う手法を提案する．以下では，提案手法について述べる．

3.1 提案手法

受講生に対しセキュリティに関するフィードバックを行うことで受講生のセキュリティ意識の向上を図る．フィードバックを行うタイミングとしては，SDPBL におけるインスペクション時とし，受講生の成果物に応じてフィードバックを行う．本研究が対象とすると SDPBL では要求定義，設計，実装，テストの 4 つに工程があり，要求定義，設計ではドキュメント形式の成果物が求められる．本研究では，このドキュメント形式の成果物に焦点を当てる．具体的には以下の手順で受講生にフィードバックを行う．

① 受講生は成果物を作成し，インスペクションを依頼する．
② 受講生の作成した成果物からセキュリティに関する項目を抽出する．
③ ②で抽出した項目をもとに関連する知識をソフトウェアセキュリティ知識ベースから取り出す．
④ 受講生にセキュリティ知識をフィードバックする．

これらの手順の②〜④は教員や TA が行うことも可能であるが，自動化されることが望ましい．よってこの手順を自動で行う Bot を作成する．Bot は GitHub 上で動作し，受講生のインスペクション依頼をトリガーに起動するものとする．Bot は開発工程の成果物に応じて受講生にセキュリティ知識をフィードバックする．例えば，受講生が要求仕様書を作成したタイミングでは，要求仕様書からセキュリティ項目を抽出し，関連しているセキュリティ知識をフィードバックする．図 1 に要求定義工程での Bot の動作イメージを示す．

図 1 提案する Bot の動作イメージ図

Bot がフィードバックとして返すセキュリティ知識には参照元のリンクを記載する．Bot の詳細な要件としては，要求定義，設計段階での受講生のドキュメント形式の成果物に対し，自然言語処理を用いてセキュリティ項目を抽出できること，抽出した結果に応じて適したセキュリティ知識のフィードバックが行えることが挙げられる．

4. おわりに

本稿では，ソフトウェア開発初学者として情報系を専攻する学部生を想定し，本学で実施されている SDPBL の成果物からソフトウェア開発初学者がどの程度セキュリティを意識しているかを明らかにし，そこから得られた課題をもとにソフトウェア開発初学者のセキュリティ知識不足を補う自動化された手法の研究計画について述べた．今後はこれらの手法を実現するツールの開発と初学者に提示すべき知識の整理，評価方法を検討する．また仕様書からは漏れているセキュリティ項目についても，機能要求から類推できるものをフィードバックする仕組みを考える必要がある．

参考文献

[1] “OWASP ZAP”. https://github.com/zaproxy/zaproxy, (参照 2019-06-25)
[2] 山田侑樹，櫨山淳雄，吉岡信和, “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その評価，電子情報通信学会知能ソフトウェア工学, ” vol. 118, no. 463, pp. 51-56, 2019 年 3 月．