情報処理学会論文誌　教育とコンピュータ　Vol.8　No.2　76–81 (June 2022)

ショートペーパー

攻撃者視点を取り入れたクロスサイトスクリプティング対策の実践的演習システムの開発と評価

岸本 和理[1,a)]　谷口 義明[2,3,b)]　井口 信和[2,3,c)]

受付日 2021年6月10日，再受付日 2021年10月28日 / 2022年1月28日，
採録日 2022年3月8日

概要：Web アプリケーションの脆弱性を悪用した主要な攻撃の 1 つにクロスサイトスクリプティング（XSS）攻撃がある．Web アプリケーション内の XSS 脆弱性を減らすためには，Web アプリケーション開発者が，XSS 攻撃および対策手法を学ぶだけでなく，攻撃者視点で XSS 脆弱性を発見するための知識やスキルを習得することが重要であると考えられる．そこで本稿では，攻撃者視点を取り入れた XSS 演習システムを開発する．学習者は Web ブラウザ，仮想ネットワーク上に構築した Web サーバ，攻撃者ホストを使って学習や演習を実施する．情報系学科の学生を対象とした実験の結果，本システムを用いることにより座学と比較して XSS 対策の学習を支援できることを確認した．

キーワード：ネットワークセキュリティ，仮想化技術，Web アプリケーション，セキュアプログラミング，演習システム

Development and Evaluation of a Hands-on System Incorporating the Attacker's Perspective for Learning Cross-site Scripting Countermeasures

Kazuri Kishimoto[1,a)]　Yoshiaki Taniguchi[2,3,b)]　Nobukazu Iguchi[2,3,c)]

Received: June 10, 2021, Revised: October 28, 2021/January 28, 2022,
Accepted: March 8, 2022

Abstract: Cross-site scripting is a typical attack that exploits web application vulnerabilities. In this paper, we develop a hands-on system incorporating the attacker's perspective for learning how to create secure web applications against cross-site scripting. Our system considers not only learning of attack and countermeasure methods but also learning of vulnerability detection methods. As a result of experiments targeting students, we confirmed that our system can support learning of cross-site scripting measures compared to classroom lectures.

Keywords: network security, virtualization technology, web application, secure programming, hands-on system

1. はじめに

総務省によると，令和元年の不正アクセスの認知件数は 2,960 件であり，前年度と比較して 99%増加している [1]．不正アクセスの要因として脆弱性を含んだ Web アプリケーションの存在があり，Web アプリケーションの脆弱性を悪用した主要な攻撃の 1 つにクロスサイトスクリプティング（以下，XSS）攻撃がある．XSS 攻撃は，ユーザのアクセス時に表示内容が生成される動的 Web ページの脆弱性を

1 近畿大学大学院総合理工学研究科
Graduate School of Science and Engineering, Kindai University, Higashiosaka, Osaka 577–8502, Japan
2 近畿大学情報学部情報学科
Faculty of Informatics, Kindai University, Higashiosaka, Osaka 577–8502, Japan
3 近畿大学情報学研究所
Cyber Informatics Research Institute, Kindai University, Higashiosaka, Osaka 577–8502, Japan
a) kishimoto0030@gmail.com
b) y-tanigu@info.kindai.ac.jp
c) iguchi@info.kindai.ac.jp

利用し，Web サイトを閲覧したユーザ端末側で任意のスクリプトを実行させる攻撃である．XSS 攻撃は 1990 年代に存在が確認されたよく知られた攻撃であるが，XSS 攻撃の手法は年々高度化，複雑化している．

XSS の抜本的な対策手法としてサニタイジングがある．しかし，開発者の知識やスキル不足，外部ライブラリや古くからあるコードを引き継いで利用しているなどの理由により，XSS 対策が行われていない Web アプリケーションがある．また，XSS 対策として，クライアントからの入力文字数を制限する，特定のキーワードの使用を不許可とする，Web Application Firewall を導入する，などの対策のみを行っている Web アプリケーションも多くある．そのような Web アプリケーションは XSS 対策が十分でなく XSS 脆弱性を持つ場合がある．実際，Web アプリケーションに含まれる脆弱性の中で XSS 脆弱性は 2013 年より 6 年連続で検出数第 1 位であり，XSS は現在でも Web アプリケーションの主要な脅威である [2]．

我々は，開発中の Web アプリケーションに XSS 脆弱性が含まれないようにするためには，Web アプリケーション開発者が，攻撃者視点で Web アプリケーションを解析し，対象の Web アプリケーションで施されている XSS 対策手法や内在する XSS 脆弱性を把握，発見するスキルやそのための知識を習得することが重要であると考えている．ここで，本稿では，攻撃者視点で Web アプリケーションを解析し，Web アプリケーションの構造を把握，サーバで動作しているコードや施されているセキュリティ対策手法を推測し，内在する XSS 脆弱性を発見する手法を XSS 脆弱性発見手法と呼ぶ．また，発見した XSS 脆弱性を利用してセッションハイジャックや Web サイトの改ざんなどを実施する手法を XSS 攻撃手法と呼ぶ．XSS を対象とした実践型のセキュリティ演習システムはいくつか開発されているが [3], [4], [5], [6]，これら既存システムでは，XSS 脆弱性発見後の攻撃手法や対策手法を学ぶことを重視しており，XSS 脆弱性の発見手法まで含めて学ぶことを想定していない．また，既存システムでは，実際にシステムを使って XSS 対策の学習をした場合の学習効果が十分に評価されていない．

そこで我々は，Web アプリケーションに対する XSS 対策の実践的な学習を支援することを目的に，脆弱性を発見するという攻撃者視点を取り入れた XSS の演習システム（以下，本システム）を開発してきた．なお，我々は本システムの途中経過を国際会議で報告してきた [7]．本稿は，この報告 [7] を発展させたものである．本稿では，攻撃者視点を取り入れるという観点から本システムの位置づけをまとめ直すとともに，システムの詳細や関連研究との比較を拡充し，分散分析を使った評価結果を追加した．

本システムは，1 台のコンピュータ内の独立した仮想ネットワーク上に演習用 Web サーバと攻撃者視点での演習用のホスト（以下，攻撃者ホスト）を構築するため，実運用されているネットワークやサーバに影響を及ぼさずに，演習を実施可能である．学習者は Web ブラウザと演習用 Web サーバ，攻撃者ホストを使って，XSS に関する学習や攻撃者視点を取り入れた演習および対策演習を実施する．また，本稿では，実験協力者に実際に本システムを利用した学習を実施してもらい，システムを利用した場合の学習効果を評価する．

2. 関連研究

高度化，複雑化するサイバー攻撃に対しては机上学習だけでなく，実践形式のサイバー演習が有効であることから，様々な実践型のセキュリティ演習システムが提案，開発されている [8], [9], [10]．XSS を対象とした実践型のセキュリティ演習システムもいくつか開発されている [3], [4], [5], [6]．

AppGoat [3] は，情報処理推進機構が提供している，Web アプリケーションやサーバ・デスクトップアプリケーションの脆弱性とその対策手法を学習できる脆弱性体験学習ツールである．AppGoat では，ホスト OS 上で脆弱性を含んだ Web サーバを起動して脆弱性の体験学習を行う．そのため，安全上の理由から AppGoat を利用する場合には，PC をインターネットと切り離すよう要請される．これに対して本システムでは，仮想ネットワーク上に脆弱な仮想 Web サーバを用意することで安全性を確保している．また，本システムでは，Web において実際に使用されているソフトウェアを利用しており，より実践的な演習が可能である．さらに，AppGoat では，攻撃手法と対策手法の学習に重点を置いているのに対して，本システムでは，脆弱性の発見手法の学習も支援できる．

Zeng 氏は XSS 教育のための攻撃および防衛ラボ環境の開発を行っている [4]．このシステムでは演習環境として Windows 系 OS，ASP.NET，Access を使用している．しかし，サーバサイド言語として最もシェアが高いのは PHP である（2021 年 3 月時点での PHP のシェアは約 80%，ASP.NET のシェアは 9%程度）[11]．本システムでは，演習環境として Linux，PHP，MySQL を使用しており，本システムの方がより一般的な対策演習を実施可能である．また，本システムでは，Zeng 氏らのシステムでは考慮していない，脆弱性の発見手法の学習も可能である．

仮想環境を用いて XSS の学習を行えるものとして OWASP WebGoat [5] がある．WebGoat では，脆弱性を含む演習用の Web アプリケーションが複数用意されている．しかし，WebGoat では XSS 対策手法に関する演習は用意されていない．また，WebGoat は XSS についてある程度の知識を持つ学習者を対象としており，使用にあたってはセキュリティに関する前提知識やプログラミング言語に関する知識が要求される．そのため，初学者の学習用途としてハードルが高いという問題点がある．これに対して，本

システムでは，学習コンテンツとして XSS に関するテキストベースの解説や演習手順の動画を取り入れている．

竹下らは，XSS 脆弱性対策教育のための，WebGoat をベースとした学習コンテンツを開発している [6]．しかしながら，WebGoat と同様に，XSS 対策手法に関する演習は実施できない．また，竹下らは，システムを使った場合の学習効果に関する評価を実施しているが，システムを使わない場合との比較評価を行っておらず，評価が十分ではないと考えられる．一方，本研究では，座学による学習を行う場合とシステムを使う場合の比較評価を行う．

3. 開発システム

本章では，本研究で開発したシステムの説明を行う．

3.1 システム構成

本システムは，Web アプリケーション開発者を目指す初学者や，XSS に関する実践的な知識の不足している Web アプリケーション開発者をシステム利用者（以降，学習者）として想定する．なお，本稿では，学習者はアルゴリズム，ネットワーク，プログラミング，Web アプリケーションなどに関する科目のある情報系学科での学習，あるいは独学などにより，Web アプリケーション技術に関連する基本的な知識を備えていることを想定する．大学の授業などで Web アプリケーション技術について学習していても，実践的な XSS 対策まで含めて学習をしていない場合があり，そのような場合に，本システムが活用できると考えられる．

本システムの構成を**図 1** に示す．本システムでは，学習に用いる PC 内の仮想環境上に演習用 Web サーバと攻撃者ホストを準備している．演習用 Web サーバは，学習用コンテンツの提供と，XSS 脆弱性を持つ演習用 Web アプリケーションの提供のために用いる．攻撃者ホストは，演習用 Web サーバ上の Web アプリケーションの XSS 脆弱性の発見や XSS 攻撃といった攻撃者視点での学習を実施するためのものである．

本システムでは，仮想環境を構築するための仮想化ソフトウェアとして VirtualBox 6.1.4 を使用した．演習用 Web サーバの OS には Ubuntu 18.04 LTS，Web サーバソフトウェアには Apache 2.4.41，サーバサイド言語には PHP 7.2.24，データベースには MySQL 8.0.18 を導入した．また，攻撃者ホストの OS にはペネトレーションテストに用いられる OS である Kali Linux 2020.4 を導入した．

XSS に関する学習，演習を実施するため，本システムでは，演習用 Web サーバに，XSS 概要学習，XSS 脆弱性発見演習，XSS 攻撃演習，XSS 対策演習のための学習用コンテンツと，これらの演習を行うための脆弱性を持つ演習用 Web アプリケーションを開発，導入した．これらを使った学習手順については，次節で述べる．また，演習用 Web サーバの XSS 脆弱性を発見する演習を実施するために，攻撃者ホストに，演習用 Web サーバとブラウザ間の通信を解析するローカルプロキシツール OWASP ZAP 2.9.0 を導入した．加えて，演習用 Web サーバに対して XSS 攻撃を実施するために，攻撃者ホストに，Web ブラウザに焦点を当てたオープンソースのペネトレーションテストツールである BeEF（The Browser Exploitation Framework）0.5.0.0 を導入した．学習者は，攻撃者ホストに導入されたこれらのツールを操作して，攻撃者視点を取り入れた演習を実施できる．

なお，本システムは 1 台の PC 上で動作し，学習者は，個人の持つ PC あるいは教育機関から貸与された PC などを利用して学習することを想定する．また，学習環境を構築する手順書と本システムの導入された仮想環境のイメージファイルを使って，学習者自身が PC 上に学習環境の構築を行うことを想定する．本システムを使った演習の手順については次節で説明する．

3.2 演習内容と手順

学習者は，PC のホスト OS 上の Web ブラウザから演習用 Web サーバに配置されている学習用コンテンツにアクセスし，XSS に関する学習，演習を行う．学習者が学習に用いる Web ブラウザ上の画面の 1 例を**図 2** に示す．これは，XSS 対策演習用のコンテンツの例である．画面の左側

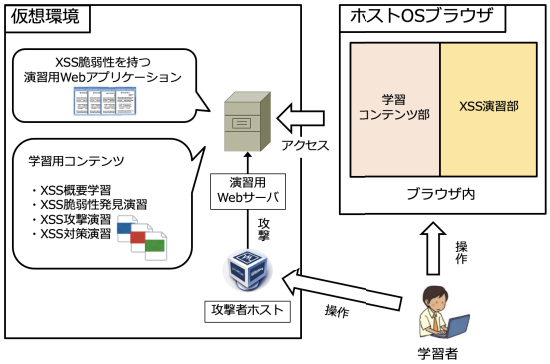

図 1　システム構成
Fig. 1　Overview of our system.

図 2　学習画面の 1 例
Fig. 2　An example of a learning web page.

図 3　XSS 概要学習用のコンテンツ例
Fig. 3　A content example for learning XSS overview.

図 4　XSS 脆弱性発見演習の学習用コンテンツ例
Fig. 4　A content example for learning XSS vulnerability detection.

は学習コンテンツ表示部であり，演習用 Web サーバ内にある学習用コンテンツが表示される．画面の右側は演習部であり，演習に用いる．この画面例の場合，演習部はさらに 2 つに分かれており，上部には脆弱な Web アプリケーションの含まれた Web フォーム，下部には XSS 対策を行うための演習用 Web サーバのコンソール画面が表示されている．学習者は，学習コンテンツに表示される解説や動画を参考にしながら，演習部に表示される Web フォームや Web サーバのコンソール，あるいは攻撃者ホストを操作し，演習を進める．なお，簡単な演習内容の場合，学習用コンテンツの中に演習のための Web フォームが含まれる場合もある．

本システムを用いて学習を行う場合，学習者は，まず，XSS 概要学習用のコンテンツを利用して XSS の概要を学ぶ．XSS 概要学習用コンテンツの一部を**図 3** に示す．学習者は，実際に Web ブラウザ上に表示される Web フォームに，学習コンテンツに従って入力を行い，Web ページ上に埋め込まれた脆弱な Web アプリケーションの挙動を確認する．演習問題としては，反射型 XSS，格納型 XSS などいくつかの種類の XSS に関する問題が用意されている．

続いて，学習者は，XSS 脆弱性発見演習用のコンテンツを利用して，XSS 脆弱性発見手法の学習と演習を行う．この演習では，十分な XSS 対策の施されていない，XSS 脆弱性を持つ Web アプリケーションを用いる．学習者は学習コンテンツに従って，攻撃者ホスト上のローカルプロキシツール OWASP ZAP を使用して，攻撃者ホストと演習用 Web サーバ間の HTTP リクエストと HTTP レスポンスを解析する．ローカルプロキシツールを用いて HTTP 通信を解析する手法を学ぶ学習用コンテンツの例を**図 4** に示す．解析することで，Web サーバで施されている XSS 対策手法の把握を行い，XSS 脆弱性を発見する．この演習を通して学習者は，Web アプリケーションに含まれる XSS 脆弱性の発見手法を習得する．

その後，学習者は XSS 攻撃演習用のコンテンツを利用して XSS 攻撃手法の学習と演習を行う．具体的には，発見した XSS の脆弱性に対してペネトレーションテストツール BeEF を用い，ブラウザの遠隔操作を行うなどの XSS 攻撃を実践する．これらを通して学習者は XSS 攻撃手法の習得とその被害を確認する．

最後に，学習者は XSS 対策演習用のコンテンツを使って対策手法の学習と演習を行う．学習者は，Web ブラウザの右下に表示される演習用 Web サーバのコンソール画面（図 2）を通じて，演習用 Web サーバ内の脆弱な Web アプリケーションのソースコードを閲覧，修正する．具体的には，XSS 対策としてソースコードにサニタイジング処理を追加する．学習者は，ソースコードの修正後，再度 XSS 攻撃を行い，XSS 脆弱性が解消されたことを確認する．また，学習者は，PHP の設定ファイル上での HttpOnly 属性，Secure 属性の設定による Cookie の漏洩対策や，Content-Type ヘッダの指定などによる XSS 対策手法に関する演習も実施する．これらを通して学習者は XSS 対策手法を習得する．

4.　評価

冒頭で述べたように，XSS に関する学習を行える実践型のシステムはいくつか開発されているが，いずれもシステムを利用した場合の学習効果については評価されておらず，効果が不明である．そこで，本稿では，近畿大学理工学部情報学科 4 年生および当学科を卒業した大学院生の合計 16 名を実験協力者とし，本システムを用いた学習効果の初期評価実験を行った．なお，当学科では 3 年生までにアルゴリズム，ネットワーク，プログラミング，Web アプリケーション構築などに関する授業や実習があり，実験協力者は Web 技術に関連する基本的な知識を備えている．

評価実験では，実験協力者を，本システムを使って XSS

問 6
クロスサイトスクリプティングを防ぐ上で Web アプリケーションでの対策は次のうちどれか，
当てはまるもの全て答えよ．
ア．タグの属性値などに含まれるメタキャラクタのエスケープ処理を行う．
イ．HTTP リクエストヘッダの Content-Type フィールドに文字コードを指定する．
ウ．タグの属性値を必ずダブルクォートで囲む．
エ．タグの属性値を必ずシングルクォートで囲む．
オ．全ての入力と出力に対して，メタキャラクタのエスケープ処理であるサニタイジングを行う．
カ．HTTP レスポンスヘッダの Content-Type フィールドに文字コードを指定する．

問 7
Web サーバが HTTPS 通信の応答で Cookie に Secure 属性を設定した時のブラウザの処理はどれか．
ア．ブラウザは Cookie の"Secure="に続いて指定された時間を参照し，
　指定された時間を過ぎている場合にその Cookie を削除する．
イ．ブラウザは，Cookie の"Secure="に続いて指定されたホスト名を参照し，
　指定されたホストにその Cookie を送信する．
ウ．ブラウザは，Cookie の"Secure"を参照し，HTTPS 通信時だけその Cookie を送信する．
エ．ブラウザは，Cookie の"Secure"を参照し，ブラウザの終了時にその Cookie を削除する．

図 5　事前テストの例
Fig. 5　An example of pre-test.

問 6
クロスサイトスクリプティングを防ぐ上で Web アプリケーションでの対策は次のうちどれか，
当てはまるもの全て答えよ．
ア．TRACE メソッドを無効にする．
イ．タグの属性値を必ずダブルクォートで囲む．
ウ．タグの属性値などに含まれるメタキャラクタのエスケープ処理を行う．
エ．タグの属性値を必ずシングルクォートで囲む．
オ．HTTP レスポンスヘッダの Content-Type フィールドに文字コードを指定する．
カ．全ての入出力に対して，メタキャラクタのエスケープ処理を行う．

問 7
Cookie に Secure 属性を付けなかったときと比較した，付けたときの動作の差はどれか．
ア．Cookie に指定された有効期間を過ぎると，Cookie が無効化される．
イ．JavaScript による Cookie の読み出しが禁止される．
ウ．URL のスキームが https の時だけ，Web ブラウザから Cookie が送出される．
エ．Web ブラウザがアクセスする URL 内のパスと Cookie によって指定されたパスのプレフィックスが
　一致するとき，Web ブラウザから Cookie が送出される．

図 6　事後テストの例
Fig. 6　An example of post-test.

について学習するグループ 8 名と，座学で XSS について学習するグループ 8 名の 2 つに分割した．学習時間はいずれのグループとも 30 分間とした．なお，座学学習のグループの実験協力者には，情報処理安全確保支援士試験の参考書 [12] の XSS に関して記述された箇所（2.8.2 項，pp.144–158）を使って自習をしてもらった．また，本システムを利用するグループの実験協力者には，学習環境の構築手順書と本システムの導入された仮想環境のイメージファイルを配布し，自身の PC に学習環境を構築してもらった．それぞれ学習の前後に XSS に関する事前・事後テストを実施した．テスト内容は情報処理安全確保支援士試験の参考書 [12] と過去問を基に作成した．事後テストは事前テストと同レベルの別の問題を用いた．事前テストと事後テストの一部を**図 5**，**図 6** に示す．問題数はそれぞれ 10 問とし 1 問 1 点とした．また，事前テストの解答を実験協力者に知らせずに，事後テストを行った．

実験協力者の事前テストおよび事後テストの点数の平均と標準偏差を**表 1** に示す．表に示されるように，事後テストの点数の標準偏差は事前テストと比較して小さく，本システム利用・座学ともに実験協力者は学習によって一定の

表 1　実験結果
Table 1　Evaluation results.

	事前テスト		事後テスト	
	平均	標準偏差	平均	標準偏差
本システム	4.75	1.28	8.75	0.88
座学	5.12	2.03	7.87	0.99

水準の学習レベルに到達したと考えられる．また，座学による学習者は平均点が 2.75 点上昇しているのに対して，本システムを利用した学習者は平均点が 4.00 点上昇している．本システムを利用する場合，XSS 脆弱性の発見，攻撃から対策までを演習を実施しながら学習するため，XSS に関する理解が深まるものと考えらえる．

加えて，実験協力者のテスト結果に関する 2 要因混合計画の分散分析（学習者間要因：学習者［本システムを利用した学習者群，座学による学習者群］× 学習者内要因：テスト［事前テスト，事後テスト］）を行った．実験協力者の単純主効果の検定を行ったところ，本システムを利用した学習者群における学習者内要因の単純主効果（$F(1,7) = 112$，$p < 0.001$）および座学による学習者群における学習者内要因の単純主効果（$F(1,7) = 13.4$，$p < 0.01$）が認められた．したがって，いずれの学習方法も効果があったといえる．また，事前テストにおける学習者間要因の単純主効果（$F(1,14) = 0.195$，ns）は認められなかったが，事後テストにおける学習者間要因の単純主効果（$F(1,14) = 3.46$，$p < 0.1$）が認められ，座学による学習者群よりも本システムを利用した学習者群の方がより有意に事後テストの点数が高いことが分かった．したがって，本システムを利用した学習が座学による学習と比較して有効であるといえる．これらの結果から本システムが XSS 対策の学習を支援できていることが分かる．

さらに，本システムを使った実験協力者に対してアンケートを実施した．その結果，「攻撃と防御の両視点から学習が可能なので，実際に起きているサイバー攻撃の実態を理解することができた」，「ブラウザだけで学習が完結するので，利用しやすかった」，「Web アプリケーションを作成する際のセキュアなコーディングなどに意識を向けていこうと思った」などの本システムに対して肯定的な回答を得た．一方，「セキュリティの知見がほとんどないため，少し難しかった」という回答もあり，学習用コンテンツの改良が必要であると考えられる．

本稿では，実践型の XSS 演習システムを用いることによる学習効果を検証するための基礎評価を行った．一方，本システムを用いて XSS 脆弱性を発見するといった攻撃者視点での学習を行うことにより，たとえば，学習者が開発する Web アプリケーション中に含まれる XSS 脆弱性の数が減る，などの効果も期待される．そのような，攻撃者視点を導入することの効果の評価については今後の課題と

する．

5. おわりに

本研究では，Web アプリケーションに対する XSS 対策の実践的な学習を支援することを目的に，脆弱性を発見するという攻撃者視点を取り入れた XSS の実践的演習システムを開発した．また，本システムを利用した場合の学習効果に関する初期評価を行った．

謝辞　本研究は JSPS 科研費 18K11592，21K12185 の助成を受けたものである．

参考文献

[1] 総務省：不正アクセス行為の発生状況 (2020)，入手先 ⟨https://www.soumu.go.jp/main_content/000671872.pdf⟩.
[2] LAC：セキュリティ診断レポート 2020 秋 (2020)，入手先 ⟨https://www.lac.co.jp/lacwatch/pdf/20201020_sec_report_vol7.pdf⟩.
[3] 情報処理推進機構：脆弱性体験学習ツール AppGoat，入手先 ⟨https://www.ipa.go.jp/security/vuln/appgoat/index.html⟩（参照 2021-03-01）.
[4] Zeng, H.: Research on Developing an Attack and Defense Lab Environment for Cross Site Scripting Education in Higher Vocational Colleges, *Proc. ICCIS 2013*, pp.1971–1974 (2013).
[5] OWASP: OWASP WebGoat Project, available from ⟨https://owasp.org/www-project-webgoat⟩ (accessed 2021-03-01).
[6] 竹下数明，小林偉昭，佐々木良一：脆弱性対策教育のための e ラーニングシステムの開発と評価，コンピュータセキュリティシンポジウム 2009 論文集，pp.1–6 (2009).
[7] Kishimoto, K., Taniguchi, Y. and Iguchi, N.: A practical exercise system using virtual machines for learning cross-site scripting countermeasures, *Proc. IEEE ICCE-TW 2020*, pp.623–624 (2020).
[8] 八代　哲，高橋和氏，渡辺亮平，角田裕太，田邉一寿，横山雅展，齋藤祐太，齋藤孝道：体験型サイバーセキュリティ学習システムの提案と構築，コンピュータセキュリティシンポジウム 2017 論文集，Vol.2017, No.4, pp.180–183 (2017).
[9] 千川尚人，小林康浩，石原　学，白木厚司，下馬場朋禄，伊藤智義：サービス拒否攻撃演習システムの実装とそのアクティブラーニングシナリオによるセキュリティ技術教育，電子情報通信学会論文誌，Vol.J103-B, No.4, pp.180–183 (2020).
[10] 湯川誠人，谷口義明，井口信和：攻防戦型ネットワークセキュリティ学習支援システム，電子情報通信学会論文誌，Vol.J103-D, No.8, pp.591–602 (2020).
[11] Q-Success: Historical yearly trends in the usage statistics of server-side programming languages for websites, available from ⟨https://w3techs.com/technologies/history_overview/programming_language/ms/y⟩ (accessed 2021-03-01).
[12] 上原孝之：情報処理教科書 情報処理安全確保支援士 2020 年版，翔泳社 (2019).

推薦文

本論文は，大学でのセキュリティ教育を行うために，攻撃者視点を取り入れたクロスサイトスクリプティングの実践的演習システムを開発している．筆者らは座学による受け身の教育だけでなく，自らウェブサイトの脆弱性を発見し，脆弱性を攻撃し，脆弱性を防ぐための対処を行うことまでを含めた，実践的なセキュリティ教育を提案している．実際に仮想マシンの上に学習サイトを構築し，授業で実践を行えている．読者にとって一定の参考になることが期待できることから，速報として推薦する．

（論文誌「教育とコンピュータ」編集副委員長
兼宗　進）

岸本 和理　（学生会員）

2020 年近畿大学理工学部卒業．同年同大学大学院総合理工学研究科博士前期課程入学，現在に至る．サイバーセキュリティの教育に関する研究に従事．

谷口 義明　（正会員）

2008 年大阪大学大学院情報科学研究科博士後期課程修了，博士（情報科学）．大阪大学サイバーメディアセンター助教，近畿大学理工学部講師，准教授を経て，2022 年より同大学情報学部准教授．情報ネットワーク，サイバーセキュリティ，ユビキタスコンピューティングに関する研究に従事．IEEE，情報処理学会，電子情報通信学会，電気学会各会員．本会シニア会員．

井口 信和　（正会員）

1988 年三重大学大学院修士課程修了．同年（株）豊田自動織機製作所入社．1992 年和歌山県工業技術センター研究員．2001 年大阪大学大学院基礎工学研究科博士後期課程修了，博士（工学）．2002 年近畿大学理工学部助教授．2008 年同大学教授．2015 年近畿大学総合情報基盤センター長を兼務．2020 年近畿大学情報学研究所所長代理を兼務．ネットワーク運用管理支援，情報ネットワーク応用，教育システム開発に関する研究に従事．情報処理学会，電子情報通信学会，IEEE，教育システム情報学会，農業情報学会各会員．本会シニア会員．