WEBアプリケーションにおけるセキュリティ診断の検討

久山　真宏[*1]　大西　荘一[*2]　高杉　祐太[*3]　鈴木　陵平[*4]　久保　翔太[*5]

<概要>　高度情報社会となり，インターネットを介したさまざまな問題が表面化している．eラーニングにおいても，インターネットを介してWEB上でサービスを提供するため，さまざまな脅威に晒されている．

eラーニングに用いられるWEBアプリケーションを脅威から守るため，テスト工程でセキュリティ診断を行いシステムの脅威を見つけ出す対策を行っている．しかし，セキュリティ診断を行うには専門家に依頼するか専用のツールを用いる必要があり，専門知識や高いコストがかかる．セキュリティは高いことにこしたことはないが，コストパフォーマンスも考えねばならない．そこで，本稿ではコストをかけずに脆弱性を検査するための簡易的な診断手法について研究したので報告する．

<キーワード>eラーニング，セキュリティ，プライバシー，個人情報，情報モラル

1. はじめに

岡山理科大学大西研究室で開発されたWEBアプリケーションであるLMS（Learning Management System）「MOMOTARO」（以下MOMOTARO)を用いて「加計サイバーキャンパス」を構築し，インターネットを介して大大連携及び高大連携遠隔授業を行っている．また，このMOMOTAROはサイバーキャンパス（図１）だけではなく，岡山理科大学の教員が利用できる学習管理システム（図２）など，複数のサーバで運用されている．

昨今，ICT関係のセキュリティ事件が後を絶たない．MOMOTAROにおいてもインターネットを通してサービスを提供しているWEBアプリケーションであり，利用者は岡山理科大学の学生だけでなく，他の大学の学生や高校生も利用しているため，高いセキュリティレベルが求められる．そこで，脆弱性を検査するためにセキュリティ診断が必要であると考えた．

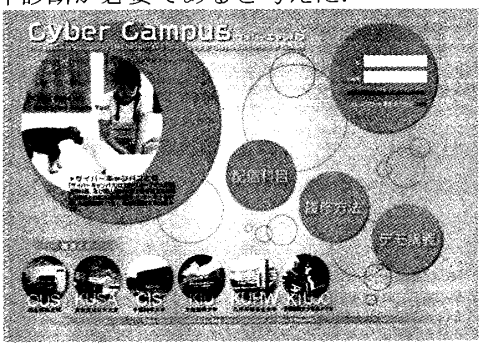

図１　サイバーキャンパス

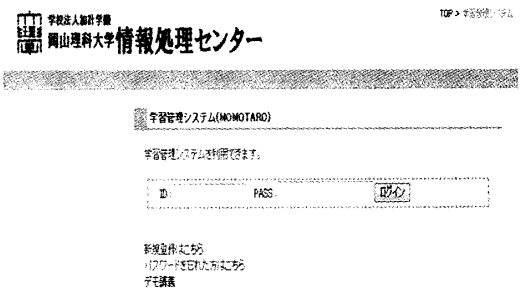

図２　学習管理システム

2. セキュリティ診断[1]

インターネットにより，様々なサービスを受けられるようになった半面，インターネットの持つ匿名性，地理的・時間的制約のなさ等を悪用した犯罪（サイバー犯罪）が多発している．この脅威からセキュリティリスクを把握する手段の１つとしてセキュリティ診断がある[2]．

セキュリティ診断を行う方法には，専門家に依頼する方法，専用のセキュリティ診断ツールを用いる方法，自力で診断する方法の主に３つがある．専門家に依頼して行うセキュリティ診断の精度は高いが，コストも高くなる．また，セキュリティ診断ツールは有償のものから無償のものまで様々なものがあり，どのツールにも一長一短があるため，どれを用いるべきかの判断が難しい．最後の自力で診断する方法は，セキュリティの知識・技術が求められること，

*1 Kuyama,Masahiro :岡山理科大学　e-mail=baku_bakun@yahoo.co.jp

*2 Onishi,Soichi :岡山理科大学　e-mail=onishi@mis.ous.ac.jp

*3 Takasugi,Yuta :岡山理科大学

*4 Suzuki,Ryohei :岡山理科大学

*5 Kubo,Syota :岡山理科大学

診断手段の情報に乏しかったこと等により容易に行うことは困難であったが,地方自治情報センター(LASDEC)から「ウェブ健康診断仕様」[3]等のWEBアプリケーションにおける簡易的なセキュリティ診断方法が公開され,無償のセキュリティ診断ツールを組み合わせることで,比較的容易に自力で診断することが可能になった.しかし,診断の精度は他の2つと比べると低く,手動で行うため,手間がかかる.

そこで,自動的に簡易的なセキュリティ診断を行えるようにするための手法を検討する.

3. セキュリティ診断の自動化

セキュリティ診断を自動的に行えるツールの開発とその資料の作成を行うことにした.そこで,オープンソースソフトウェアのOWASP Zed Attack Proxy (以下ZAP) を基に開発を行うこととした. ZAPを選んだ理由としては,OWASPはセキュリティ診断の必要性を訴え,セキュリティ診断をいかにすばやく,正確に,効率的に行えるかといったことを追求し,ZAPにおいてセキュリティ診断を簡易的に行えるように自動化している.また,ZAPは改変可能なオープンソースソフトウェアであるためである[4].

4. ZAP

ZAPは日本語に対応しており,URLを入力し,実行するだけで自動的に診断を行ってくれる.また,診断結果はHTML形式で出力されるため,情報の共有にも容易に行うことが出来る (図3).しかし,レポートは英文で出力されるため英語の読解力が求められる.また,これらは不正アクセス等の攻撃から防ぐための診断であり,防げなかった場合のことまで視野に入っていない.

そのため,診断結果のレポートを日本語化し,電磁的記録の証拠保全および調査・分析を適正に行う技術であるデジタルフォレンジックを組み込むことで[5], セキュリティ診断結果の分析をより効率的に行えるようなり,また,インシデント発生時の事後対応まで視野に入れることで,より多くの脅威から身を守ることができるようにする.

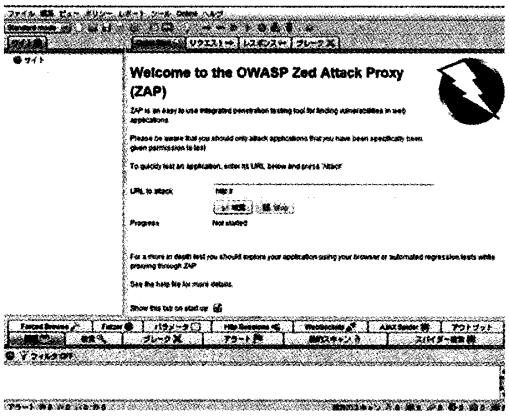

図3 OWASP Zed Attack Proxy

5. おわりに

セキュリティ診断は管理下にあるサーバないしWEBアプリケーションに対して行うことが前提となる.しかし,セキュリティ診断を自動的に行えるということは,他のサーバないしWEBアプリケーションに対して自動的に攻撃することが可能である危険性がある.そのため,セキュリティ診断ツールの公開および運用には注意を払う必要がある.

また,セキュリティインシデントを考えると,インシデントが発生しないようにすることも必要ではあるが,インシデント発生時の事後対応のことも視野に入れてシステムを構築する必要があると考える.

参考文献

[1] 徳丸浩. 安全なWebアプリケーションの作り方. 初版, ソフトバンククリエイティブ, 2011, pp.496.

[2] 警察庁, ISOG-J. サイバー攻撃からビジネスを守る. 初版, NTT出版, 2013, pp.154.

[3] WEB健康診断アーカイブ, https://www.lasdec.or.jp/cms/12,1284.html(参照 2013-08-28)

[4] OWASPテスティングガイド, https://www.owasp.org/images/1/1e/OTGv3Japanese.pdf(参照 2013-08-28)

[5] 高橋渉, 佐々木良一, 上原哲太郎. Android携帯を用いた証拠保全作業支援アプリケーション. 日本セキュリティ・マネジメント学会 第26回全国大会発表要旨, 2012, p.181-186.