様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 １８ 日現在

機関番号：５３３０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ０１１６７

研究課題名（和文）仮想擬似情報セキュリティシミュレータの開発と実践的セキュリティ教育拡大と質の向上

研究課題名（英文）Development of the virtual information security simulator and improvement of practical security education

研究代表者

長岡　健一（Nagaoka, Kenichi）

石川工業高等専門学校・電子情報工学科・准教授

研究者番号：６０２４９７７９

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：情報セキュリティについて学習する仮想疑似情報セキュリティシミュレータをまず開発した。インターネット上の一般的な一連のサイバー攻撃をクラウド上のシステムを利用して学習者が擬似的に体験できる内容としている。これにより、クラッカーによる攻撃手法を学ぶことができ、その防御方法について考察できるようにしている。
研究代表者が担当している、情報セキュリティ教育科目で本システムを活用し、システムのユーザビリティ評価やアンケート評価を行うことで、学習者から高い評価を得ることができた。また、システム導入前後の達成度評価の比較を行うことで、システムの教育効果も明らかになり、セキュリティ教育の質の向上を達成できた。

研究成果の学術的意義や社会的意義
情報セキュリティ教育では実際の演習をとおして学習することが有用とされており、これまでにもサイバーレンジ（セキュリティ演習システム）が用いられてきた。しかし、サイバーレンジの多くは大規模なシステムで、利用にも費用が必要であるなど、高等教育機関における情報セキュリティ初学者の利用にはハードルが高かった。本システムはクラウド上で利用でき、初学者に必要なコンパクトな内容としており、上記のような問題点を改善できる。
本システムを利用した教育の質の向上が確認でき、今後の情報セキュリティ教育に活用することで、我が国で不足している情報セキュリティ分野の人材育成に役立つと考えられる。

研究成果の概要（英文）：We first developed a virtual information security simulator for learning about information security. The simulator allows students to simulate a series of common cyber attacks on the Internet using a cloud-based system. In this way, students can learn about the methods of cyber attack used by crackers and consider how to defend against them.
This system is used in our information security education course, and through usability evaluation and questionnaire evaluation of the system, we were able to obtain a high evaluation from students. In addition, by comparing the level of achievement before and after the introduction of the system, the educational effect of the system was clarified, and the improvement of the quality of security education was achieved.

研究分野：情報ネットワーク，教育工学

キーワード：セキュリティ　ネットワーク　情報教育

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

情報セキュリティ分野の人材育成が強く求められており，経済産業省「情報セキュリティ分野の人材ニーズについて」では，今後必要となるセキュリティ人材像に「ホワイトハッカーのような高度セキュリティ技術者」などを挙げている．我々もこのような人材育成を行うため，所属する高等専門学校（高専）において情報セキュリティに関する演習を実施してきた．この演習の理解に対して障害と感じたことについて学生アンケートを実施したところ，自宅等から演習環境を利用できず，自学・自習できないという回答が多かった．学生はより学習しやすい環境で自学・自習を行いたいと考えているといえる．なお，情報セキュリティ教材として，サイバーレンジの開発および利用が他の研究でも多く行われているが，いずれも実際のシステムに脆弱性を持たせたものをベースとしている．また，このようなサイバーレンジでは，システムが大規模であったり，演習内容も初学者に対しては対象が広すぎるなどの課題がある．今後我が国において，サイバーセキュリティ演習を通した教育の裾野を広げていく必要が特に求められるが，このような従来の教育手法では限界があると考えられる．

２．研究の目的

以上のような背景から，情報セキュリティ初学者に学びやすい情報セキュリティシミュレータをまず開発する．具体的にはクラウド上で利用でき，初学者に必要なコンパクトな演習を実施できるシステムとする．そして，開発システムを我々が担当する情報セキュリティ教育に活用し，その教育効果を評価することで情報セキュリティ教育の質の向上を確保し，我が国で不足している情報セキュリティ分野の人材育成の裾野を拡大することを目的としている．

２．研究の方法

まず，情報セキュリティ教育教材として，インターネット上で一般的なサイバー攻撃を体験できるセキュリティシミュレータを開発する．シミュレータはクラウド上に開発し，セキュリティ初学者でもブラウザ環境があれば利用できるものとする．また，システムを使用して学習を行うための e-Learning コンテンツも同時に開発する．
シミュレータでは，以下の一連の複数の攻撃の実行と暗号化手法を学習しながら，あるサイバー攻撃を達成するというストーリー性を持たせた内容とする．クラウドを用いたシステムのイメージを図１に示す．

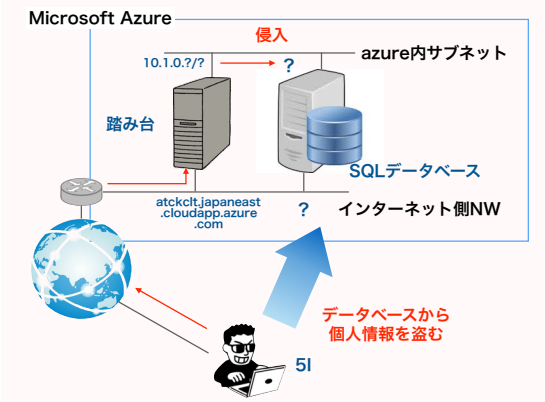

図１ クラウドを用いたシステムイメージ

- ポートスキャン
- パスワードの総当たり攻撃（辞書攻撃）
- 暗号解析（シーザー暗号および RSA 暗号）
- SQL インジェクション
- XSS（クロスサイトスクリプティング）

ただし，サイバー攻撃を行う対象は擬似的なシステムであり，実際に脆弱性を持つものではなく，安全に演習が行える．
続いて開発システムを，我々が所属する機関で行っている情報セキュリティ科目の演習に活用する．まず，ユーザビリティ評価をアンケート等によって行い，学習者からのシステムの評価を得る．２年間これを行うことで，評価結果からシステムの改善を行う．
改善されたシステムを用いて，システム利用前後の学生の達成度評価を比較する．達成度評価は演習課題のレポートをあらかじめ設定した評価項目で評価する．達成度評価を行い，本システムの教育効果の検証を行う．

４．研究成果

研究の方法で述べた情報セキュリティシミュレータおよび演習を行うための e-Learning コンテンツを開発した．シミュレータで実行する一連の手順を図２に，e-Learning コンテンツの一例

を図 3 に示す．また，開発したシステムを我々が担当する「電子情報工学実験」の「情報セキュリティ演習」で用いた．２年間のユーザビリティ評価に基づき当初開発したものを改善した．
開発システムを利用する前後で，学生が提出したレポートから達成度評価を行った．なお，システム利用前の演習内容については，学習する項目についてはほぼ同様ではあるが，それぞれ個別に準備した外部コンテンツや我々が提供したプログラムを用いており，一連の演習を通して行う本研究で開発したようなものとは異なっている．
また，評価対象は高等専門学校電子情報工学科 5 年生 40 名である．
図 4 に，システム利用前後の達成度評価の一例を示す．達成度評価をあらかじめ設定した評価項目を 5 点満点として評価しており，同図は 40 名の達成度評価の平均値を表している．

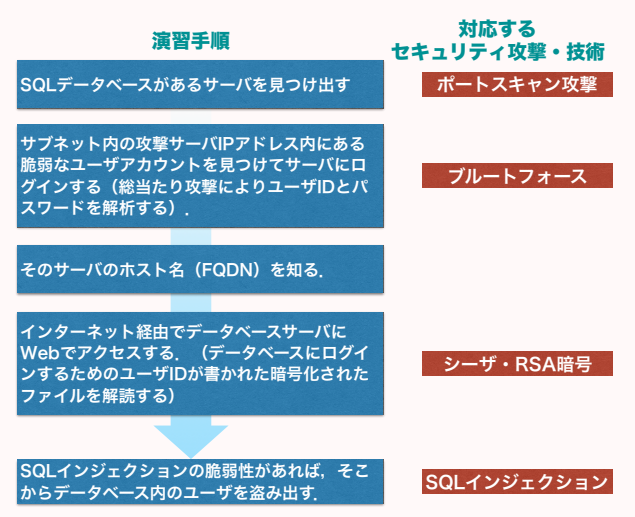

図 2 シリーズ化された演習手順

まず，図の達成度評価から，すべての項目と演習全体について達成度評価はシステムの導入前に比較して導入後の達成度評価が高くなっていることがわかる．特にブルートフォースアタックによるパスワード解析と SQL インジェクションについてはその度合いは高い．本システムではよりリアルに攻撃手法を体験することができており，学生の理解がより高まった結果といえる．
一方，暗号化解析についてはその度合いはそれほど高くなかった．プログラムを作成することで暗号解析についての理解を深めるものであるが，これは，システム導入前後でその演習手法に劇的に変わっていなかったことが原因であると考えている．
以上より，本研究で開発したシステムによって，我々が目指した情報セキュリティ初学者が，インターネット上で一般的に行われているサイバー攻撃手法を学ぶ演習として有効であることが明らかとなった．

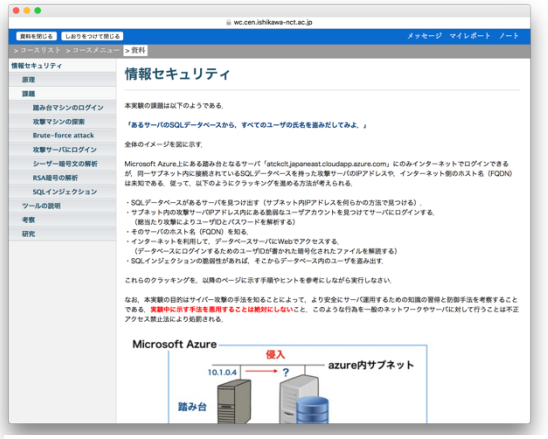

図 3 開発した e-Learning コンテンツの例

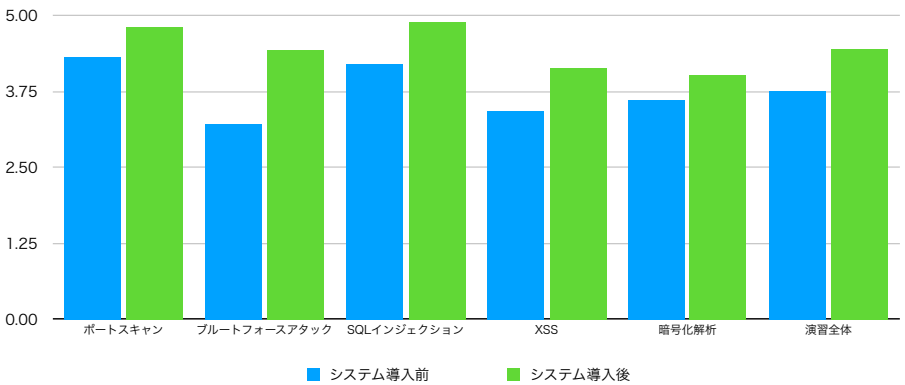

図 4 システム導入前後の達成度評価の比較

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Chun-Xiang CHEN, Kenichi NAGAOKA	４．巻 Vol.E102-D, No.5
２．論文標題 Analysis of the State of ECN on the Internet	５．発行年 2019年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 910-919
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018NTP0006	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 長岡健一, 陳春祥	４．巻 Vol.J103-A, No.1
２．論文標題 エラー発生に相関性がある2並列チャネルにおけるARQ方式のスループット効率	５．発行年 2020年
３．雑誌名 電子情報通信学会論文誌A	６．最初と最後の頁 25-34
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Chun-Xiang CHEN and Kenichi NAGAOKA	４．巻 VOL. E102-D, NO.5
２．論文標題 Analysis of the State of ECN on the Internet	５．発行年 2019年
３．雑誌名 IEICE TRANS. INF. & SYST.	６．最初と最後の頁 910-919
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018NTP0006	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 長岡健一, 飯田忠夫
２．発表標題 実践的ネットワーク工学教育
３．学会等名 平成31年度全国高専フォーラム
４．発表年 2019年

１．発表者名
阿知良綾，長岡健一

２．発表標題
インターネット上の混雑回避手法の性能評価に関する研究

３．学会等名
令和元年度北陸地区学生による研究発表会

４．発表年
2020年

１．発表者名
森幹太，長岡健一

２．発表標題
SNSにおける情報の信頼性評価に関する研究

３．学会等名
令和元年度北陸地区学生による研究発表会

４．発表年
2020年

１．発表者名
肥田木遼，長岡健一

２．発表標題
情報セキュリティ教材の開発と評価

３．学会等名
2019年度北陸地区学生による研究発表会

４．発表年
2019年

１．発表者名
天野博，長岡健一

２．発表標題
情報セキュリティ学習教材の開発と評価

３．学会等名
平成29年度学生による研究発表会

４．発表年
2018年

１．発表者名 荒井知大，長岡健一
２．発表標題 マイコンによるハッキング脅威に関する研究
３．学会等名 平成29年度学生による研究発表会
４．発表年 2018年

〔図書〕　計2件

１．著者名 岡田正，高橋参吉 編，長岡健一，新開純子，高橋章 著	４．発行年 2019年
２．出版社 実教出版	５．総ページ数 296
３．書名 情報基礎 ネットワーク社会における情報の活用と技術	

１．著者名 岡田正，高橋参吉 編，長岡健一，新開純子，高橋章 著	４．発行年 2019年
２．出版社 実教出版	５．総ページ数 64
３．書名 情報基礎 ネットワーク社会における情報の活用と技術 学習ノート	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関