G-23

デジタルフォレンジック技術を短期間で学習する教材の開発

Development of the teaching materials learning digital forensics in a short term

○服部慶[1]，五味悠一郎[2]
*Kei hattori[1], Yuichiro Gomi[2]

Abstract: According to the Ministry of Economy, Trade and Industry, by 2020, the shortage of information security personnel is expected to rise to just under 200,000. Human resource development is an urgent issue because the demand for security is likely to continue to increase due to the emergence and development of new technologies and services such as big data and IoT. For human resource development, we thought that the development of teaching materials for beginners would be helpful, so that more people would like to be security engineers. In this report, we develop teaching materials for beginners, conduct lessons, conduct questionnaire surveys on tests and lessons, and verify the results to clarify the effectiveness of the developed teaching materials.

１．はじめに

経済産業省によると，2020 年には情報セキュリティ人材の不足数が 20 万人弱に上ると予想されている．ビッグデータ，IoT 等の新しい技術やサービスの登場，発展により，セキュリティに対する需要は引き続き増加する可能性が高いと見込まれているため，人材育成が急務である．[1]

人材育成のためには，セキュリティ技術者を志す者が増えるように，初心者に向けた教材の開発が必要になると考えた．

２．先行研究とその課題

本郷節之らの研究によって，AOS リーガルテック社製の PC 用フォレンジックツールである FinalForensics の使用法について，ファイル検索と復元を中心に学習する動画教材が開発されている[2][3][4]．この教材は，学習範囲を特定のツールの使用法に限定しているほか，動画教材であるため改変が難しく，教材として広く使用する事に不向きである．

FinalForensics はデータ保全，復元，分析，検索，分析レポート作成を一括して行うことができるパソコン用の有償フォレンジックツールだが，有償ツールでの学習は，金銭的な負担から初心者の学習における敷居が高くなるため，本研究ではフリーウェアを使用する方が適していると考える．

若月里香らの研究によって，Windows 標準搭載機能やフリーウェアを用いてデジタルフォレンジック技術を学習する大学講座が開発されている[5]．講座の形式を取っているため，学習に多くの時間を要するものであり，短期間での学習を可能とした教材は開発されていない．

以上のことから，短期間での学習が可能な，標準搭載機能やフリーウェアを使用する教材を開発することを本研究の目的とする．

３．教材の概要

教材開発に当たって，教材の使用者と範囲を想定する．教材の使用者は，人材の増加を目的とする場合，情報技術に対する関心を持ち，セキュリティに関する知識が不足している初心者を想定することが有効と考える．範囲は，IoT デバイスの普及によって需要が増加しているデジタルフォレンジックに絞り込むこととした．

初心者学習者の負担を減らすために学習期間が短いほど都合が良い．そのため，1～2 日間程度の短期間での学習を実現するために，エピソード記憶に着目した．エピソード記憶とは，個人が経験した出来事と，出来事を経験したときの付随情報に関する記憶である．内容のみが記憶される意味記憶と異なり，エピソードに準じた前後の繋がりがあるため，記憶されやすい．映画や小説などのストーリー内容を覚えるのもエピソード記憶に分類され，教材に活用する場合シナリオ型教材との相性が良いことから，実際のインシデントを想定したシナリオ型教材を開発する．

４．実験方法

被験者は大学生とし，被験者を対象に教材を使用した座学と演習を実施した．

座学ではデジタルフォレンジックの概要や必要性，演習で使用するツールの使用方法に関する解説を行い，演習では実際のインシデントを想定したシナリオ上での問題を各種ツールを使用して解決した．

１：日大理工・学部・情報　２：日大理工・教員・情報

座学，演習の終了後，アンケートを実施し，その結果に基づき教材の評価を行った．

５．実験結果

2018 年度の日本大学理工学部応用情報工学科 2 年後期に設置されている「情報セキュリティ基礎」の授業内で,「研究室の所属学生によって研究データが流出した」という状況を想定したシナリオをもとに演習を行った．設問は以下の通りである．

(1) Web サーバのアクセスログと学生名簿をもとに流出させた学生を特定する
(2) 該当者がファイルを公開するために Web サーバにアクセスした日時を特定する
(3) 流出したデータのハッシュ値を特定する
(4) 該当者の USB メモリイメージからハッシュ値が同一のファイルを特定する

各設問の正答率と使用したソフトウェアを Table1 に示す．

Table 1 正答率と使用したソフトウェア

設問	正答率	使用した機能またはソフト
(1)	47.37%	コマンドプロンプト（findstrコマンド）
(2)	37.93%	コマンドプロンプト（findstrコマンド）
(3)	46.67%	コマンドプロンプト（certutilコマンド）
(4)	85.71%	FTK imager Lite

アンケートの調査結果を Table 2 に示す．アンケート項目については 1〜5 点の間隔尺度を設定した一対比較法を用いた．また，アンケートの最後に自由記述欄を設けた．

Table 2 アンケートの調査結果

質問事項	平均値	標準偏差
デジタルフォレンジックに興味がある	3.43	0.82
デジタルフォレンジックツールは使いやすかった	3.18	0.89
講義は分かりやすかった	3.43	1.08
演習は楽しかった	3.54	1.15
演習は難しかった	3.14	0.87
演習は実際にありそうなストーリーだった	3.25	0.99
講義時間は適切だった	3.57	1.05
演習時間は適切だった	3.11	0.98
デジタルフォレンジックの授業に満足した	3.36	1.01

６．課題

今後は，アンケートに設けた自由記述欄における指摘を参考に 2019 年度の「情報セキュリティ基礎」授業での使用に向けて教材を改良する．その後，５．実験結果に示した 2018 年度の結果と比較し，教材の適切性と有効性を検証していく予定である．

７．参考文献

[1] 経済産業省 :「IT 人材の最新動向と将来推計に関する調査結果を取りまとめました（METI-経済産業省）」, http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html，(アクセス日：2019/2/12)

[2] 加藤大希，矢野祐樹，本郷節之 :「サイバー犯罪対処能力の向上に資するデジタルフォレンジックツール活用マニュアルの作成」, 工学教育研究講演会講演論文集，2015

[3] 加藤大希，矢野祐樹，本郷節之 :「デジタルフォレンジックツール使用法学習のための電子教材の開発」, 工学教育研究講演会講演論文集，2016

[4] 本郷節之，重山直人，加藤大希，高山純 :「デジタルフォレンジックツール使用法学習のための電子教材の導入」，工学教育研究講演会講演論文集，2017

[5] 若月里香，森直彦，後藤厚宏 :「「デジタルフォレンジック実践講座」開発の取り組み」，情報処理学会『デジタルプラクティス』，第 7 巻，第 3 号，pp.1-13，2016

[6] 日本ネットワークセキュリティ協会 :「NPO 日本ネットワークセキュリティ協会　報告書・公開資料 – JNSA」，https://www.jnsa.org/result/incident/，(アクセス日：2019/6/17)