セキュリティエンジニアを育成するための インストラクショナルデザインの考察

金子 晃介 [1)], 伴 芳龍 [,2)], 岡村 耕二 [1)]

1) 九州大学 サイバーセキュリティーセンター
2) 株式会社ヒューマンテクノシステム

kaneko.kosuke.437@m.kyushu-u.ac.jp

A Study on Instructional Design for Security Engineer

Kosuke Kaneko [1)], Yoshitatsu Ban [2)], Koji Okamura [1)]

1) Cybersecurity Center, Kyushu University
2) Human Techno System Co., Ltd.

概要

本発表では，九州大学で開講している「セキュリティエンジニアリング演習」の講義を事例に取り上げて，セキュリティエンジニアを育成するための効果的なインストラクショナルデザインについて考察する．また，上記講義の学習効果を測定するために実践している方法についても口述し，演習を取り入れたインストラクショナルデザインの学習効果を調査する研究の現状について発表する．

1 研究背景

近年，サイバー攻撃の増加に伴い，セキュリティエンジニア育成が急務になっている．情報処理推進機構の「情報セキュリティ人材の育成に関する基礎調査」（2014 年）によると，国内の従業員 100 人以上の企業において，情報セキュリティに従事する技術者は約 23 万人おり, 不足している人材は 2.2 万人と推定されている．また，上記 23 万人のセキュリティ人材のうち約 14 万人は, 何らかの教育やトレーニングを行う必要があると報告されている[1]．このような状況を受けてセキュリティ人材の育成と効果的なインストラクショナルデザインの構築が必要になってきている．

本研究では，九州大学で開講している「セキュリティエンジニアリング演習」[2] の講義（以下，本講義）を事例に取り上げて，セキュリティエンジニアを育成するための効果的なインストラクショナルデザインについて考察する．また，本研究では，セキュリティエンジニアの教育において，演習を取り入れたインストラクショナルデザインがセキュリティエンジニアの育成に効果があるのかを明らかにしていく．

本資料は，以下の内容で構成されている．第 2 章で関連する研究について簡単に紹介する．第 3 章では，実際に行なっている講義のインストラクショナルデザインを ADDIE (Analysis, Design, Development, Implementation, Evaluation)モデルに基づいて説明する．第 4 章では，本講義の評価方法について説明を行う．最後に，今後の展開について記述する．

2 関連研究

本研究の目的は，セキュリティエンジニアを育成するにあたって，演習における体験的な教育を取り入れたインストラクショナルデザインが，効果があるかどうかについて検証していくことにある．このような体感的な学習に対する効果検証を行う研究は，教育工学の分野で様々な研究が進んでいる[3]．また，本研究では，学習効果を測る 1 つの指標として，学習者の学習時のモチベーションを測ろうとしている．これらの学習時のモチベーションを測る指標としては様々なものが考えられるが, 本研究では ARCS[4] モデルに基づいたインストラクショナルデザインとそのモチベーションのアンケート指標である IMMS を用いる．

3 インストラクショナルデザイン

教育を行うにおいて，効果的なインストラクショナルデザイン提供できるかどうかは，学習者の

学習効果に大きく影響してくる．本章では，本講義を行うに当たって考案したインストラクショナルデザインについて，ADDIE モデルに基づいて説明する．

3.1 分析

分析（Analysis）の項目として，本講義の基本的な項目である，講義の目的，講義の対象，講義の概要などについて分析を行い内容を決定した．本講義の目的として,「セキュリティを考慮したものづくりができる人材を育成する」ことを講義の目的として定めた．講義の対象は，工学・芸術工学などのものづくりに関わる学部生・大学院生とし，対象学年は設定しなかった．講義の概要としては，各回で座学と演習の両方を行なうようにした．

3.2 設計

設計（Design）の項目として，各回でどのような内容を伝えていくかなどの講義の全体的な構成を具体的に考案した．本講義では，各回で特定のサイバー攻撃にフォーカスを当てた内容を設定した．表 1 は，本講義の全体的なスケジュールを示したものである．本講義では，セキュリティについてなるべく広く多くの事例を学習してもらうために，講義で利用する教材の対象として「IoT（Internest of Things）セキュリティ」を取り上げた．IoT セキュリティでは，ハードウェアに関するセキュリティからアプリなどのソフトウェア，そしてクラウドなどのサーバーサイドのセキュリティまで幅広くセキュリティのことを学ぶことが可能である．本講義の全体的な構成として，前半はサーバーサイドやソフトウェアに関するセキュリティについて学習し，後半はハードウェアに関するセキュリティについて学習する構成にした．また，最後の約 1 ヶ月間で，演習で学んだサイバー攻撃に対する対策方法を実践して，セキュリティを考慮した IoT プロダクトを開発してもらう時間を設けた．最終講義では，開発した IoT プロダクトのどの部分にセキュリティを考慮した設計を取り入れているかを発表してもらい．受講者同士でサイバー攻撃を仕掛けてもらい，プロダクトの頑健性を確かめる予定である．なお，本講義では，講義の対象学部や対象学年を明確に指定しなかったことから，受講生のセキュリティに関する事前知識のレベルに差があると考えられたため，各回の講義の内容を構成するに当たって以下のことに注意した．

a) IoT セキュリティの講義を行う前に, IoT やネットワーク及びハードウェアに関する基礎知識を教えること．
b) 演習を行うに当たって多くの知識を必要とする場合，2 回以上に分けて講義を構成すること．
c) 各回でわかりやすい具体的なサイバー攻撃のシナリオを用意すること．
d) 学生のレベルに合わせて，臨機応変に教材の内容を変更できるように教材を制作すること．

a) に関しては，表 1 の講義の全体構成の中で，第 1 回で IoT とは何かについて学習し，第 2 回でネットワークの基礎的な知識（インターネットの仕組みや IP アドレスやポート番号など）について学ぶ講義を入れた．また，講義後半のハードウェアのセキュリティに入る前に，ハードウェアに関する基礎知識を体得するために，第 7 回のハードウェア仕組みを学習する時間を設けた．b) に関しては，インストラクショナルデザインを考案する中で，SQL インジェクションの講義を行うには，事前にリレーショナルデータベースや SQL の知識が必要になるという意見が上がっていたため，データベース関連の項目として，第 4 回と第 5 回はセットでデータベースや SQL の基礎知識について学習するように設定した．具体的には，第 4 回で，暗号化・匿名化の内容と一緒に，リレーショナルデータベースについて学習する時間を設けた．また，第 5 回の SQL インジェクションの演習につなげるために，第 4 回のデータベースの暗号化・匿名化の項目で事前に，SQL を使ってデータベースの中の値を確認する簡単な SQL 演習などを行うようにした．その他にも，演習でハードウェアの回路の設計を行うには，ハードウェアに関する基礎知識が必要になるとの意見が上がっていたので，第 7 回~第 9 回もセットでハードウェアの回路を設計するための基礎知識を学習するための時間を設けた．具体的には，第 7 回でブレッドボードを使って回路設計を行う演習を行い．その後の第 8 回，第 9 回では，第 7 回で体得した知識と技術を元にセキュリティを考慮した回路の設計を行うことにした．c) に関しては，IoT セキュリティのセキュリティが扱っている項目が広いので，学習者がどういう部分のセキュリティを取り扱っているのかが理解できるように，各回でどういうシチュエーションで，ハッカーはどういう攻撃を仕掛けよう

としていて，学習者は演習でどの部分の対策を試みようとしているのかを具体的に描いたシナリオを設定した．表 2 は，第 3 回のアカウントハッキングの際に用意したシナリオである．各回のシナリオは表 1 に記載している．d) に関しては，教材をモジュール化して制作することで，学生のレベルに合わせて，モジュールをどこまで用意しておけば良いかを自由に構成できるように教材を設計した．具体的な内容に関しては，次節の 3.3 で説明を行う．上記の項目を考慮しても，学習者が講義についていけなくなることが考えられるため，講義では 2~3 人で構成されるグループを作り，わからない部分があったら互いに教えあいながら演習を進めることができるように，自由に話し合いながら講義を受けれる環境を心がけた．

表 1. 講義の全体構成

	タイトル	内容	シナリオ
第1回	ガイダンス	演習環境構築	
第2回	サーバーサイドエンジニアリング	Linux コマンドの使い方	見守り用カメラをハッキングされ盗撮される.
第3回	アカウントハッキング	ブルートフォースアタックと対策	同上.
第4回	データベースの暗号化・匿名化	暗号化・匿名化 リレーショナルデータベースと SQL	暗号化されていないデータベースが流出する.
第5回	SQL インジェクション	SQL インジェクション対策	SQL インジェクションによってデータベースの内容が流出する.
第6回	Wi-Fi の通信内容の盗聴	Wi-Fi の通信内容の盗聴	LAN 内に侵入されて, Wi-Fi の通信内容を盗聴される.
第7回	ハードウェアエンジニアリング	回路設計	
第8回	インプットデバイス	センサーデバイスを用いた回路設計	改ざんされた回路の情報をサーバーに送られる.
第9回	アウトプットデバイス	モーターを用いた回路設計	モーター制御のコンピューターに異常値が送られる.
第10回	Bluetooth の通信内容の盗聴	Bluetooth を利用した回路設計	暗号化されていない Bluetooth の通信内容が盗聴される
第11回	OTA アップデート	遠隔からの IoT 機器の脆弱性の修正	脆弱性があるまま放置されているハードウェアがハッキングされる.
第12回	中間テスト	これまでの知識を問うテストを行う.	
第13回	アイディア発表	最終課題の IoT プロダクトのアイディアを発表する	
第14回	開発サポート	最終課題の IoT プロダクトの開発サポートを行う.	
第15回	プロダクトの発表	開発した IoT プロダクトを発表してもらう	

表 2. アカウントハッキングの演習のシナリオ

- あなたは，ブラックハッカーです.
- 攻撃対象は，高齢者の住む家の監視カメラです．攻撃対象の家には，「高齢者の見守りシステム（制御用のシステムと Web カメラ)」が置いてあります．このカメラの映像は接続サービスのシステム（正規の方法）を使って家族がいつでも閲覧できます.
- 攻撃目的は，監視カメラを不正に起動させて，家の中の様子を探り，侵入経路などを探ることです（**盗撮**）.
- 該当の家の無線 LAN ルーターは，デフォルトのパスフレーズで運用されています（ディクショナリーアタックで侵入可能）.
- 見守りシステム制御機器（**IoT 機器**）は，デフォルトのパスワードで運用されています（ディクショナリーアタックで侵入可能）.

3.3 開発

開発（Development）の項目として，3.2 の設計に基づいて開発した教材の構成について説明する．本講義では，演習に利用する教材としてシングルボードコンピュータである Raspberry Pi を中心として教材を構成している（図 1）．その他の教材の構成機器としては，LAN を構成するための Pocket Wi-Fi と Raspberry Pi を無線でコントロールするための無線 LAN アダプター，Raspberry Pi に電力を送るモバイルバッテリー，その他 Raspberry Pi に繋ぐ Web カメラや各種センサーを用意している．講義の前半に行われるサーバーサイド側のセキュリティの講義では，Raspberry Pi 上で動いている脆弱性のあるサーバーを用意している．また，講義の後半のハードウェア側のセキュリティの講義で

は，Raspberry Pi 上の GPIO ピンとブレッドボードを用いて回路設計を行いながら，実際に IoT 機器を開発していく．各回の演習の内容では，始めに脆弱性のある Raspberry Pi 側の設定に対して，学習者に各回で取り上げているサイバー攻撃を仕掛けてもらい，サイバー攻撃の恐ろしさを体感してもらう．その後，脆弱性のある Raspberry Pi に対して，サイバー攻撃への対策を施してもらい，サイバー攻撃を防げることを確認してもらう．本教材では，受講者のレベルに合わせて臨機応変に講義に対応できるように，各デバイスやソフトウェアをモジュール化し，モジュール部分をどこまで準備して講義の教材を提供するかを毎回考えながら，教材を提供できるようにしている．

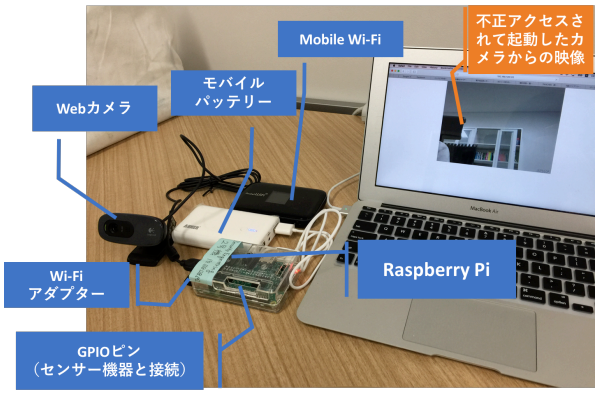

図 1. 本講義で使用している教材

3.4 実装

実装（Implementation）の項目として，3.2 の設計に基づいて，3.3 で開発した教材を利用して，現在，講義を行なっている．図 2 は，実際に行なっている講義の様子である．グループごとに分かれて，話し合いながら演習に取り組んでいる．図 3 は，講義の各回で行う内容についての説明を示したものである．各回は 90 分で実施しいる．まず，各回の開始時に 10 分間の事前テストを行う．このテストは学習効果測定に用いるためのもので，学習前に どのくらいセキュリティに関する知識があったかどうかを測るものである．この事前テストは，後半の事後テストの成績と比較される．学習効果の測定方法に関しての具体的な説明は次章で行う．事前テスト後，約 20 分間の座学を行い，後半に約 40 分間の演習を行う．演習後に，事後テストを行い事前テストの結果と比較して学習効果の測定を行う．

図 2. 本講義の講義中の様子

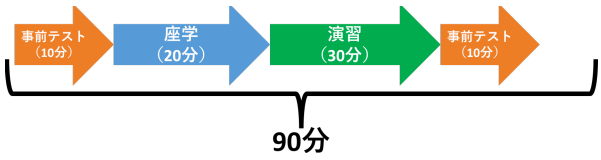

図 3. 各回の講義の構成

3.5 評価

評価（Evaluation）の項目として，3.4 で実践した事前テスト及び事後テストの結果を用いて評価を行う．また，演習による講義が学習者に与えるモチベーションを測定するために，ARCS モデルと IMMS によるアンケート指標を用いて学習者の学習モチベーションの分析を行う．具体的な評価方法の内容は次章で説明する．

4 評価の方法

本講義の効果測定は，事前テスト及び事後テストによるテストのスコアの分析と，学習者のモチベーション分析の 2 軸で行う．前述の通り，事前テストは，講義を受ける前に行い学習前にセキュリティについて，どの程度の知識があったかを測るためのものである．その後，講義後に，事前テストと同じ内容の事後テストを受けてもらい，学習前と比較してどの程度スコアが伸びたかを測定する．事前テスト・事後テストの内容は，各回で，5 つの問題から構成されており，各問題は 5 択の選択問題になっている．各問題は，座学で学んだ内容を問う問題が 2 問，演習で学んだ内容を問う問題が 2 問，座学と演習の知識が必要な問題が 1 問という構成になっている．このような問題の分類を行うことで，座学による学習効果や演習による学習効果を測る狙いがある．また，演習による講義が学習者に与えるモチベーションを分析するために，ARCS モデルに基づいた教材の設定を行い，IMMS によるアンケート指標を用いて分析を行う．本アンケートは，第 12 回の中間テストを行

う際に同時に実施する．上記の 2 軸からの分析による効果測定を用いて，本講義の学習評価を行うために，本講義を受けるグループとは別に，演習を行わない e-learning のみによる講義を受けた学習グループを用意する予定である．e-learning の内容は，本講義の座学で使用したものと同じもので，スライドと読み上げの音声による教材を提供する．e-learning を受けるグループにも，本講義を受けるグループと同様に，事前テスト及び事後テストを受けてもらう．e-leaning グループに使用する事前テスト及び事後テストの内容は，本講義を受けたグループのものと同じものを使用する．e-learning による学習後に，本講義を受けたグループと同様に IMMS によるアンケートをとり，2 つのグループの学習モチベーションを比較する．

5 今後の展開

本研究では，前述のインストラクショナルデザインに基づいて本講義を進め，セキュリティエンジニアを育成する教育において，演習を取り入れた教育方法の学習効果を測定するとともに，測定結果に基づいたインストラクショナルデザインの提案を行う予定である．本講義は，現在継続中であり，今後，前述の e-learning グループによるモニタリングを実施した後に，本講義を受けたグループとテストのスコア及び学習モチベーションのスコアを比較し，演習による講義の効果測定を行う予定である．

謝辞

本講義のインストラクショナルデザインを考察するにあたって，富士通株式会社サイバーディフェンスセンターの奥原様，須永様，鈴木様には，お忙しい中幾度かの会議を通じて，多くのご意見や助言を頂きました．心より感謝いたします．また，本講義の会議を行うにあたって準備や調整をして頂き円滑な会議の場を提供していただいた富士通株式会社九州支社の林様，久家様にも心より感謝いたします．

参考文献

[1] 情報処理推進機構，情報セキュリティ人材の育成に関する基礎調査，2014, https://www.ipa.go.jp/files/000014184.pdf

[2] セキュリティエンジニアリング演習講義シラバス URL：https://ku-portal.kyushu-u.ac.jp/campusweb/slbssbdr.do?value%28risyunen%29=2016&value%28semekikn%29=1&value%28kougicd%29=16533826&value%28crclumcd%29=ZZ

[3] J. M. Keller, Motivational Design for Learning and Performance: The ARCS Model Approach, Springer Science and Business Media, 2009.

[4] K. Kaneko, Y. Saito, Y. Nohara, E. Kudo, M. Yamada, A Game-Based Learning Environment Using the ARCS Model at a University Library, IIAI 4th International Congress on Advanced Applied Informatics, IEEE, pp.403-408, 2015.