JSiSE Research Report
vol.33,no.4(2018-10)

情報セキュリティアウェアネス向上のための意思決定トレーニング環境の提案

長谷川 忍[*1,*2], Deni Kurnia[*2], Zheyu Tan[*2], Beuran Razvan[*3]
*1 北陸先端科学技術大学院大学 情報社会基盤研究センター,
*2 北陸先端科学技術大学院大学 先端科学技術研究科

A Proposal of Decision-Making Training Environment for Information Security Awareness

Shinobu Hasegawa[*1, *2], Deni Kurnia[*2], Zheyu Tan[*2], Beuran Razvan[*2]
*1 Research Center for Advanced Computing Infrastructure, JAIST
*2 Graduate School of Advanced Science and Technology, JAIST

The purpose of this manuscript is to propose a training environment in information security awareness to improve skills regarding not only to knowledge and technical skills which are easy to be outdated but also to soft skills like decision-making which are more general. To design such environment, we first make modeling in training process for the decision-making as a cognitive skill and then propose a methodology to generate adaptive practice to focus on what a learner is weak based on required awareness level or his/her training status.

キーワード: 情報セキュリティアウェアネス，意思決定トレーニング，適応的支援

1. はじめに

あらゆるものがインターネットに接続される現代社会においては，社会インフラに不正に侵入してデータの詐取や破壊を行うサイバー攻撃もより一層グローバル化・巧妙化・複雑化している．このような状況の下，情報セキュリティ政策会議において「情報セキュリティ人材育成プログラム」が策定され(1)，サイバーセキュリティ戦略本部において「サイバーセキュリティ人材育成総合強化方針」が示される(2)など，情報セキュリティを確保するための高度人材育成は非常に重要な課題の一つとなっている．高等教育機関における情報セキュリティ教育の事例としては，分野や地域を越えた全国的なネットワークを形成し，実際の課題に基づく課題解決型学習等により高度な専門性と実践的な情報セキュリティ能力を有する人材の育成を目指す「情報技術人材育成のための実践教育ネットワーク形成事業(enPiT)(3)」などが挙げられる．

しかしながら，情報通信技術が社会インフラだけでなく Internet of Things (IoT)等を通じてパーソナルな空間までも行き渡る現代社会においては，製品やサービスの開発や運用を専門的に行う技術者だけでなく，それらを利用する一般ユーザの立場であっても情報セキュリティに対する適切な意識（情報セキュリティアウェアネス）を身につけることが必要不可欠である(4)．

しかしながら，情報セキュリティを取り巻く環境の変化は非常に急速であり，関連する知識や技術的スキルは陳腐化が起こりやすい．一方で，セキュリティに関わる事態において状況や情報を整理・判断するような意思決定スキルは，より普遍的なスキル（トランスファラブルスキル）として長期間にわたって活用が可能である．こうした認知的スキルは，知識として学ぶだけでなく，事例や演習，問題解決などといった実践的教育を通じて初めて身につけることが期待される．ただし，こうしたセキュリティ教育を行うことのできる教員及び時間には限りがあり，オンラインでそれぞれの学習者が経験・失敗を繰り返しながらボトムアップ的にトレーニングすることが求められる．

本研究の目的は，変化の激しい情報化社会において効果的な情報セキュリティアウェアネスを獲得するために，陳腐化しやすい知識や技術的スキルだけでなく，長期間にわたって活用可能な状況判断に関わるスキルを向上させるためのトレーニング環境を提案することである．具体的には，認知的スキルとしての意思決定とそのトレーニング過程をモデル化するとともに，学習者に要求されるアウェアネスレベルや当該スキルに関するトレーニング状態などの特徴に応じて，特に苦手なスキルを集中的に学習するための，適応的な課題生成手法の実現を目指す．

2. 意思決定トレーニングモデル

図 1 に本研究で想定する情報セキュリティ教育の構成要素を示す．情報セキュリティにおける知識とは，セキュリティ対策を実行する際にユーザが理解しておくべき基本方針（セキュリティポリシー）や対策基準（セキュリティガイドライン），その実施手順を指す．これらの知識はそれぞれの組織で定義されており，本稿では主に大学におけるセキュリティポリシーやガイドラインを対象とする．

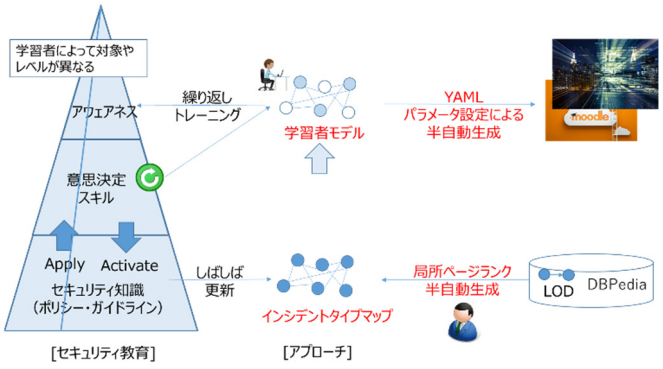

図 1. 情報セキュリティ教育の構成要素

意思決定スキルは図 2 に示すようにセキュリティ事象（インシデント）に対してセキュリティ知識を適用することで適切な行動を選択一連のプロセスである．セキュリティにおけるインシデントを規定する要素は，フィッシングメールやメール誤送信などといったインシデントの種類，被害を受けた場合の影響の大きさや範囲，行動に対する時間的・金額的コスト，などから構成される．筆者らが先行研究で提案した災害対応における意思決定スキル学習支援モデル[5]を拡張して，これらの要素を変動パラメータとすることで同様のシナリオであっても異なる意思決定トレーニングを繰り返して行うことが可能となる

また，社会的実践の場におけるインタラクションを通じた認知スキルの学習過程モデルの一つである認知的徒弟制[6]のアプローチを意思決定スキルのトレーニングに適用すると，概念を理解させるためにデモンストレーションを行う「モデリング」や，意思決定に対するヒントやフィードバックを与える「コーチング」，手掛かりや支援を上達に伴い減らしていく「足場づくり」などの支援戦略を組み合わせることも可能となる．

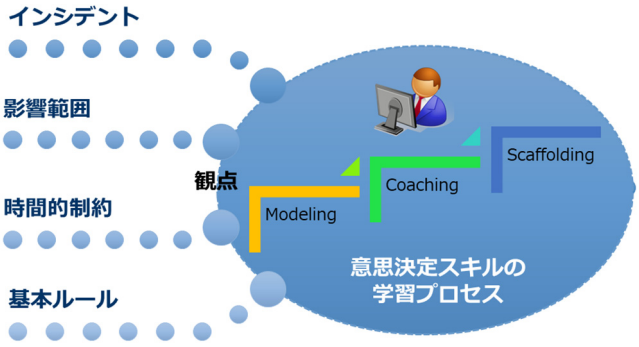

図 2. 意思決定トレーニングモデル

3. 適応的トレーニングの生成手法

3.1 インシデントタイプマップの生成

セキュリティの脅威が急速に進化していることから，どのようなセキュリティインシデントの種類をトレーニング対象として取り入れるかを検討する上で実用的な指針が必要であると考えられる．そこで本研究では，Linked Open Data (LOD)に基づくデータセット，特に Wikipedia から抽出された構造化データセットである DBpedia[7]に局所的なページランクアルゴリズムを適用することで，インシデントの種類に関するコンセプトマップを生成する手法を提案している[8]．これにより，新しいセキュリティインシデントや特定の学習者のトレーニングギャップに応じて，関心のあるインシデントを対象としたトレーニングを行うことが可能となる．

3.2 意思決定要素に対するオーバレイモデル

情報セキュリティアウェアネスの文脈における意思決定スキルとは，既に述べた通り，インシデントの種類だけでなく，影響の大きさや範囲，時間的・金額的コストなどから総合的に判断することが求められる．金子らは形式知学習において学習者の不得意分野をオーバレイモデルによってシステムが同定し，次に提示する問題を決定する手法[9]を提案しているが，セキュリティアウェアネスの個人差に対応する上では，それぞれの意思決定の要素について得意不得意な境界を推定し，不得意な要素をより多くトレーニング課題とする方法が考えられる．そこで，本研究では意思決定の要素に基づくオーバレイモデルを実装する．具体的には，意思決定スキルをその構成要素とトレーニング履歴からなる表として展開し，時系列を加味したクラスタリングを行うことで，各学習者の得意・不得意な要素を表現する．

3.3 トレーニング課題の生成

学習者の不得意な要素に関するトレーニングシナリオのパラメータを変動させることで，演習課題を適応的に生成する．具体的には，図 3 に示すように，初学者に対してはパラメータを大きく変動させ，熟練者に対しては意思決定におけるしきい値の周辺で小さく変動させる乱数を生成することで，学習者が同じタイプの異なるトレーニングを繰り返し行うことができるようにする．

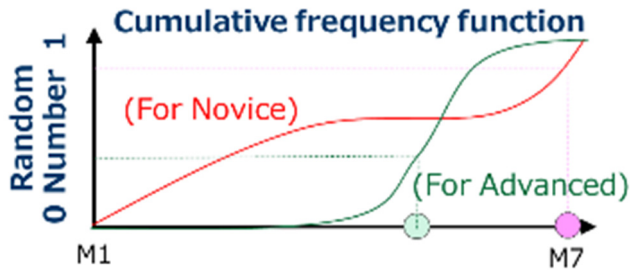

図 3. パラメータ設定手法の概要

3.4 トレーニング環境の実装

本研究では学習環境のプラットフォームとして，オープンソースの学習管理システム(LMS)である Moodle を採用し，事前にデータベースに格納した事例や演習のシナリオに基づいて，演習のためのトレーニング環境を自動的に生成するプラグインとして開発する．具体的にはトレーニングのためのシナリオを構造化データ表現記法である YAML フォーマットで記述することにより，Moodle 内で利用可能な SCORM パッケージとしてトレーニングを展開できるプラグインを開発している[10]．YAML フォーマットは直感的にシナリオ設定を記述することが可能であり，記述内容に従ってパラメータを変更可能なトレーニングコンテンツを自動で生成できるため，オーサリングのコストを低減することができる．さらに，トレーニング時の意思決定に関連する活動を学習履歴として収集する機能を開発中であり，これらにより，Moodle を利用可能な他機関においても活用できる形式とする．

4. おわりに

本研究ではセキュリティアウェアネスの基礎となる意思決定スキルのトレーニング要素をセキュリティインシデントのタイプ，影響範囲，コスト等の要素を組み合わせたオーバレイモデルで表現し，学習者の達成状況と重ねることで不得意部分の特定と不得意部分の要素を持つトレーニング課題を提示する適応的なトレーニング環境を提案した．現在，Moodle 上のモジュールとしてトレーニング環境の実装を進めており，開発できた機能は随時 GitLab で公開している．

これまでにもセキュリティ教育を対象とした学習環境やトレーニング環境は提案されてきているが[11]，それらの多くは作りこまれた環境となっている．本提案は，セキュリティインシデントの流行に合わせたコンテンツの追加などが容易な仕組みとなっており，対象領域の発展が著しい情報セキュリティ分野では効果的な手法であると考えられる．

今後の課題としては，パラメータを変動可能なコンテンツの生成手法の実現と，認知的徒弟制に基づく適切なフィードバック手法の実装が挙げられる．さらに，適応的課題生成アルゴリズムを評価するために，大学院学生に対するセキュリティ教育の一環として，トレーニング課題に関する条件群と統制群による比較実験を予定している．評価の方法としては，主観的なアウェアネスの状態を測定するためのルーブリック評価と客観的なセキュリティポリシー・ガイドラインに対す

る理解度を測定するためのテストの得点からプレテストとポストテストの差を比較する．また，プロセス評価として，学習履歴に基づいて意思決定の観点や基準が時系列でどのように変化したかを分析することも予定している．さらに，フィードバックの手法やシステムのユーザビリティ等，運用に必要不可欠な要素についても評価・改善を行いたい．また，トレーニングを一定期間にわたって行うことで，今回提案した手法の有用性を確認することも重要な課題の一つである．

謝辞

本研究の一部は，JSPS 科研費基盤研究(B) (No.17H01992)，基盤研究(C) (No.17K00478) (No. 17K00479)の助成による．

参 考 文 献

(1) 情報セキュリティ政策会議 : 新・情報セキュリティ人材育成プログラム，(2014)

(2) サイバーセキュリティ戦略本部 : サイバーセキュリティ人材育成総合強化方針，(2016)

(3) enPiT : 分野・地域を越えた実践的情報教育協働ネットワーク, http://www.enpit.jp/ (2018 年 9 月 27 日確認)

(4) 花田 経子：情報セキュリティ人材に求められるスキルと人材育成，情報処理学会研究報告，Vol.2012-CSEC-58 No.39, pp.261-266, (2012)

(5) Wahyudin, D., and Hasegawa, S.: Mobile Serious Game Design for Training Ethical Decision Making Skills of Inexperienced Disaster Volunteers. The Journal of Information and Systems in Education, Vol.14, No.1, pp.28-41, (2016)

(6) Collins, A., Brown, J. S. and Newman, S. E.: Cognitive apprenticeship: Teaching the craft of reading, writing, and mathematics, Technical Report, No. 403, BBN Laboratories, Cambridge, MA. Centre for the Study of Reading, University of Illinois, (1987)

(7) DBpedia Association: DBpedia Website, https://wiki.dbpedia.org/ (2018 年 9 月 27 日確認)

(8) Tan, Z., Hasegawa, S., and Beuran, R.: Concept Map Building from Linked Open Data for Cybersecurity Awareness Training, in Proceedings of the Japanese Society for Artificial Intelligence (JSAI) Special Interest Group on Advanced Learning Science and Technology Workshop (SIG-ALST83), pp. 1–6, (2018)

(9) 金子 真也, 上之薗 和宏, 橘 知宏, 佐藤 彰紀, 橋立 真理恵, 古宮 誠一 : “学習者の不得意分野を同定する CAI システム ： 学習者モデルと教授ロジックの提案，”電子情報通信学会技術研究報告，知能ソフトウェア工学 108(384), pp.25-30, (2009)

(10) Cyber Range Organization and Design (CROND): GitHub Repository for CyLMS https://github.com/crond-jaist/cylms, (2018 年 9 月 27 日確認)

(11) Md. H. Noor Azam and R. Beuran: Usability Evaluation of Open Source and Online Capture the Flag Platforms,” Japan Advanced Institute of Science and Technology (JAIST), Tech. Rep. IS-RR-2018-001, (2018)