インシデント対応におけるログ分析とそのリフレクションを支援する学習環境の設計・開発

Design and development of a learning environment to support log analysis and reflection in incident response

岩井　亮太*1，西村　浩二*2，渡邉　英伸*2
Ryota IWAI*1，Kouji NISHIMURA*2，Hidenobu WATANABE*2
平嶋　宗*3，林　雄介*3
Tsukasa HIRASHIMA*3，Yusuke HAYASHI*3
*1 広島大学工学部
*1 Faculty School of Engineering Hiroshima University
*2 広島大学情報メディア教育研究センター
*2 Information Media Center Hiroshima University
*3 広島大学大学院工学研究科
*3Graduate School of Engineering Hiroshima University
Email: iwai-r@lel.hiroshima-u.ac.jp

あらまし：インシデント対応のための有力な方法の一つとして，ログ分析がある．このログ分析の方法を習得するためには，知識として学ぶだけではなく，実際にインシデント発見のためにログ分析を行う経験が重要であるとされている．この経験を得るための演習において，（1）学習者の行うログ分析プロセスを記録し、（2）そのプロセスを決定木の形で可視化し，（3）その決定木をリフレクション・再分析する，ことを可能にする学習環境を実装した．
キーワード：ログ分析，経験，決定木，リフレクション

1.　はじめに

近年サイバー攻撃が深刻化してきている．例えば大企業を標的にした標的型攻撃の脅威が顕在化してきている．そのため，システムへの侵入を行かに早く検知し，対応をとることが大事になってくる．しかし，セキュリティ技術者の人材不足とスキル不足もまた、深刻化してきている．情報処理推進機構(IPA)が発表した「情報セキュリティ人材の育成に関する基礎調査（2014 年）」によれば，情報セキュリティ従事者は 23 万人，情報セキュリティ技術者は 2.2 万人の不足，情報セキュリティ技術者として、スキルが不足している人材は 14 万人に上るとされている(1)．サイバー攻撃などによるインシデント対応の方法の一つに，ログ分析がある．しかし，人材不足により、一人当たりの負担が大きくなり，また，スキル不足によりインシデント特定に時間がかかってしまっているのが現状である．

そこで，本研究では，スキル不足に着目して，インシデント対応のためのログ分析に不慣れな人を育成するために，リフレクションによりログ分析演習の学習をサポートできるシステムの設計・開発を行った．

2.　インシデント対応とその経験の蓄積

ここでは，インシデント対応のログ分析について述べた後，経験学習モデルについて述べる．

2.1 インシデント対応

コンピュータセキュリティインシデントとは、「情報システムの運用におけるセキュリティ上の問題として捉えられる事象」である．JPCERT/CC では、コンピュータセキュリティインシデントを「インシデント」と呼び，そのインシデントの発生が起きた場合，特定→防御→検知→対応→復旧の順番で解決を行っている．インシデント発生の原因となる標的型攻撃によるマルウェアなどの脅威は，ネットワークを通して複数の通信記録にまたがって行われている．そのため，監視したいネットワークにおけるあらゆる通信記録のログデータを収集してインシデント発生後の特定や対応，検知に役立てることができる．

2.2 経験学習モデル論

コルブはデューイの学習理論(2)を，実務家に利用可能な循環論に単純化した．デューイの経験と学習に関する理論を「活動―内省」と「経験―抽象」という二軸からなる理論空間に構成しなおし，これら諸関係の間に循環型サイクルを仮定し，経験学習モデルという概念を構築した(3)．経験学習モデルとは図 1 のとおりである．

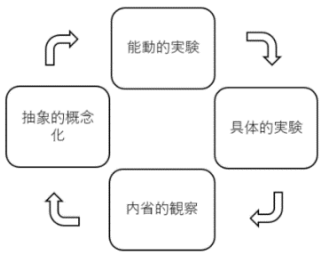

図 1 経験学習モデル(出典：Kolb(1984))

3.　ログ分析演習とそのリフレクション

本研究で開発したシステムは，実際にインシデント特定のためのログ分析を行い，その後，自身が行ったログ分析のプロセスを決定木の形で木構造として可視化し，リフレクションを行ってもらうものである．この二つの過程を繰り替えし行うことにより，経験を積むことができる．これにより，学習者はログ分析終了後に自身の分析手順を振り返ることができ、どの手順で分析をしたから結果が出たのか，なぜうまくいかなかったのか，などのリフレクションを行うことが可能である．

3.1 ログ分析演習

本研究で使用したログは広島大学におけるキャンパスネットワークで収集されたログを用いて行った．本システムではインシデント対応におけるログ分析は IP アドレスから個人を特定する分析の演習を用意した．複数あるログの選択はタグを用いて行う．

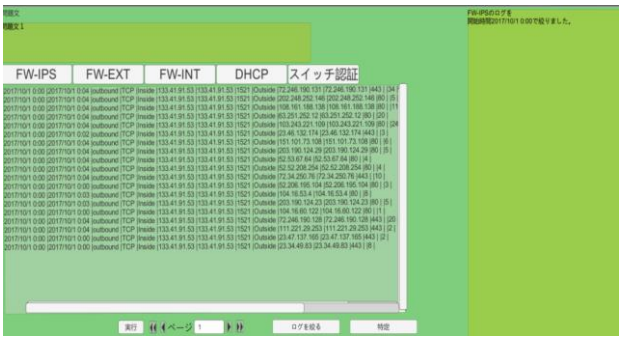

図２　ログ分析演習画面１

選んだログから絞り込みたい項目について学習者に絞り込みを行ってもらう．学習者が特定できたと判断した場合，特定ボタンよりフィードバック画面へ移行し、リフレクションを行ってもらう．

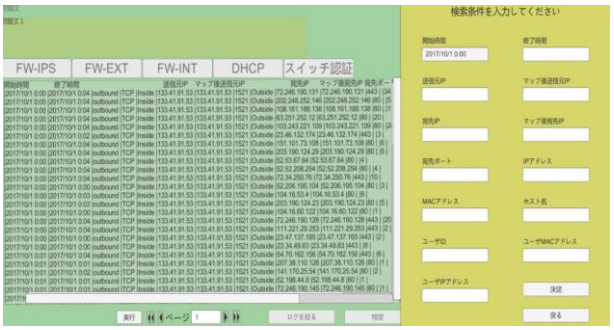

図３　ログ分析演習画面２

3.2 リフレクション

ここでは，学習者がログ分析を行った過程（具体的経験）を，木構造を用いてフィードバックを返す．ノードには学習者が選んだログの種類と，絞り込みを行ったログの項目とその値を記している．また，学習者がログ分析を行い，行き詰まりを感じた時に後戻りを行った際に分岐が生まれる．これにより，学習者に内省を行わせて（内省的観察），次の課題に向けての応用可能な知識を自ら気づくことが可能である（抽象的概念化）．また，フィードバック後に演習画面にもどり，もう一度問題を解くことにより，前回の経験を活かして新しくログ分析を行うことが可能である（能動的実験）。さらに，前回の分析と今回の分析を重ね合わせて比較し，その違いについて振り返ることも可能となる．

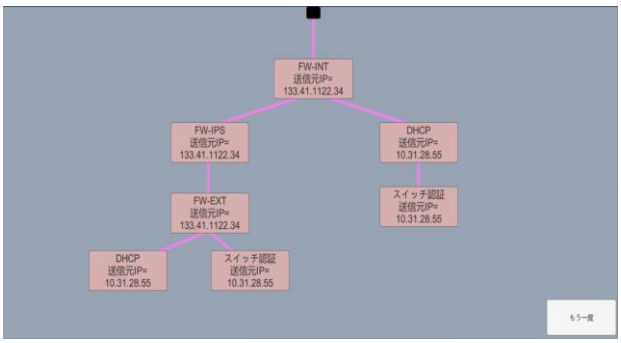

図４ リフレクション画面

3.3　自己説明

木構造に対するリフレクションにおいて，学習者自身が自分の決定理由を説明する自己説明をタスクとして与える予定である．自己説明を行うことで，自身の決定についての理解を進めることができるようになると期待できる．また，教授者が存在することを前提とすると，単に分析ができたかどうかだけではなく，分かったうえで分析できたかどうかを調べることも可能となる．さらに，学習者同士で決定木とその理由づけを供することができれば，協調的な学習のための題材として有効利用できる可能性がある．

4.　まとめと今後の課題

本研究ではログ分析演習での分析プロセスを記録し，インシデント特定後に学習者自身の分析手順をフィードバックとして返し，リフレクションを行わせることにより経験学習の支援を可能にした．

今後の課題として，フィードバック画面でのリフレクションを行う際に自身の分析手順について自己説明を行わせてその評価を行える機能の追加を考えている．

参考文献

(1) 情報セキュリティ人材の育成に関する基礎調査− 調査報告書 − <https://www.ipa.go.jp/files/000014184.pdf >(アクセス日：1/15)

(2) Dewey,J.(著)・市村尚久(訳)(2004)「経験と教育」講談社

(3) Kolb,D.A.(1984) Experiential Learning: Experience as the Sowrce of Learning and Development,Prentice Hall.