

情報セキュリティインシデントボード訓練と 振り返りシステムを組み合わせた学習支援の提案

Propose an Educational Support with an Information Security Incident Board Training and Reflection System

金山 岳生^{*1}, 後藤田 中^{*2}, 大野 真伯^{*3}, 小野 滋己^{*4}, 米谷 雄介^{*5}, 難波 夏貴^{*6}

喜田 弘司^{*7}, 八重樫 理人^{*8}, 林 敏浩^{*9}, 亀井 仁志^{*10}, 最所 圭三^{*11}

Takao KANAYAMA^{*1}, Naka GOTODA^{*2}, Masanori ONO^{*3}, Shigemi ONO^{*4}, Yusuke KOMETANI^{*5}, Natsuki NANBA^{*6}

Koji KIDA^{*7}, Rihito YAEGASHI^{*8}, Toshihiro HAYASHI^{*9}, Hitoshi KAMEI^{*10}, Keizo SAISHO^{*11}

^{*1}香川大学電子情報工学科

^{*1}Kagawa University, Faculty of Engineering

Email: s17t228@stu.kagawa-u.ac.jp

あらまし：大学 CSIRT は部局横断的な組織で、あらゆる部局でインシデントが発生した際にも、即時的な情報収集が欠かせないため、あらゆる部局の教職員との協力体制が不可欠である。したがって教職員が CSIRT への協力の必要性を理解しなければならない。本研究ではインシデント対応ボードゲームを基にした情報セキュリティインシデントボード訓練と、振り返りシステムを提案した。ボード訓練と振り返りシステムを組み合わせて用いた、教職員を対象とした、CSIRT への協力の必要性を理解する支援を目的とした。実験結果から、ボード訓練と振り返りシステムを組み合わせた学習によって、被験者が CSIRT への協力の必要性の理解をすることが推察された。

キーワード：大学 CSIRT, リスクアセスメント, 協力体制, 振り返り学習, ボード訓練

1. はじめに

近年のサイバー攻撃の増加・巧妙化に伴って、CSIRT(Computer Security Incident Response Team)を組織し対応に当たる企業が増えてきている。本研究では大学に設置されている大学 CSIRT に着目した。大学 CSIRT はインシデントの発生時に、あらゆる部局の教職員(以下、教職員)と協力して、即時的な情報収集を行う。しかし、CSIRT と教職員の協力体制が構築されていなければ、適切なリスクアセスメント(以下、アセスメント)ができず、組織へ悪影響を及ぼす可能性がある。したがって、本研究では教職員を対象として、インシデント発生時の CSIRT への協力の理解を深めることを目的とした。そのために、インシデント対応ボードゲーム(以下、ボードゲーム)⁽¹⁾を基にした新たなコンテンツの作成と学習システムの開発をする。

2. インシデント対応の現状課題と解決手法

2.1 インシデント対応における現状課題

大学 CSIRT はインシデント発生時に、インシデント情報収集のため、教職員との協力体制が不可欠である。しかし、教職員は、インシデント発生時における CSIRT への協力の必要性を理解していない。それは、インシデントの知識を深める機会や学習環境がなく、インシデントへの関心を持つことができず、アセスメント時のインシデント情報の重大性を認識していないためである。

そこで、我々は教職員を対象に、インシデント発生時における CSIRT への協力の必要性を理解する学習支援が必要であると考えた。

2.2 CSIRT への協力の必要性を理解する手法

教職員が CSIRT への協力の必要性を理解するには、インシデントへの関心を持つことと、適切なアセスメントを行うためのインシデント情報の重大性を認識することが必要であると考えた。

まず、インシデントに関心を持つには、インシデント対応を体験する必要があると考えた。しかし、知識がない人が単独で、適切なアセスメントを行うことは困難であると考え、集団で議論を行い、理解しやすいボードゲーム形式でアセスメントを行う、情報セキュリティインシデントボード訓練(以下、ボード訓練)を作成した。

次に、実例を用いた具体的なアセスメントを行い、CSIRT の実際に行ったアセスメントと比較し、学習することで、CSIRT がインシデント被害の最小化を行うために、必要なインシデント情報の重大性を教職員が認識できると考えた。そこで、篠原ら⁽²⁾が開発した振り返りモジュールを用いた、Web ブラウザでアセスメント学習を行う振り返りシステムを提案する。

以後、ボード訓練と振り返りシステムを組み合わせた学習環境(以下、組み合わせ学習環境)について述べる。

3. 組み合わせ学習環境の概要

ボード訓練は、集団で議論を行うことでインシデント対応を体験できる。さらに、専門的な知識が必要なアセスメントは、動画で説明した。したがって、インシデントに対して知識のない教職員が、内容を理解することができ、インシデントの重大性とインシデント対応の大変さを実感し、関心を持てる。

振り返りシステムでは、過去のインシデント事例に対して、リスクや発生する可能性、発生した場合

の影響度、リスクの優先度を想定する詳細なアセスメントを入力する。そして入力した内容と CSIRT が入力した内容を対象者が比較することで、アセスメントを学習できる。これによって、適切なアセスメントを行うためにはインシデント情報が重大であることを認識できる。

これらを組み合わせた学習環境によって、対象者が CSIRT への協力の必要性を理解できる。

4. 実験

4.1 実験目的

ボード訓練と振り返りシステムを組み合わせた学習環境によって、対象者が CSIRT に協力する必要性の理解を深めることを目的とし、実験を行った。

4.2 実験設定

本実験は香川大学生 4 名を被験者とした。本研究の対象は教職員であるが、ボード訓練と振り返り学習による CSIRT への必要性を理解する効果を確認するため、インシデントに対して知識や関心がない香川大学生を被験者とした。

本実験の流れは、①ボード訓練、②振り返りシステム、③アンケートの順で行う。②振り返りシステムで用いるインシデントは 7 つの状況に分かれており、それぞれの状況でアセスメントを行い、入力する。比較学習時には、被験者が入力したアセスメントの変更や追加を聞き取り、その変化を見ることでアセスメントの学習ができているかを確認する。③アンケートでは、ボード訓練と振り返りシステムによる効果があったかを調査する。

4.3 実験結果・考察

被験者が振り返りシステムによって入力したアセスメント内容を比較学習の前後で比較する。被験者 4 名すべてが比較学習の前後で、想定したリスク数が増加したことに加え、発生する可能性と発生した場合の影響度に対する評価が増加した。比較学習の前後のリスク数を図 1 に示す。この結果から被験者が各ステップで想定したリスク数の変化が全員増加しており、特に被験者 2 が最も増加していた。図 1 から 1 つの状況で平均 1 個のリスク数が増加していたことがわかる。さらにこのことから振り返りシステムによって、被験者のアセスメントの理解度が上昇したという結果になった。

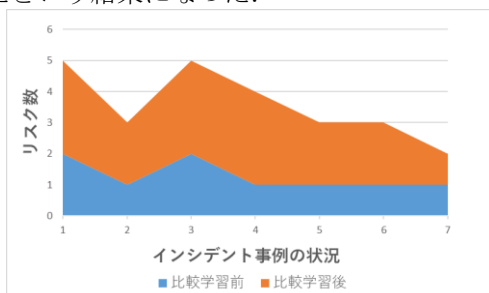


図 1 比較学習前後のリスク数比較

次にアンケート結果から考察する。このアンケートは 3 つのパートに分かれており、第 1 パートでは

実験前、第 2 パートはボード訓練後振り返り学習前、第 3 パートは振り返り学習後の被験者の状態を 5 段階評価で聞き取る。アンケート結果から被験者 4 名中 3 名がボード訓練の前後で、インシデントとその対応への関心が高まっていることが分かった。被験者の協力の必要性の理解度のパートによる推移を図 2 に示す。図 2 から、被験者 4 名全員がボード訓練と振り返り学習によって、CSIRT への協力の必要性の評価が増加していることがわかる。これらの実験結果から、ボード訓練と振り返りシステムを組み合わせることで、被験者が CSIRT への協力の必要性を理解したことが推察された。

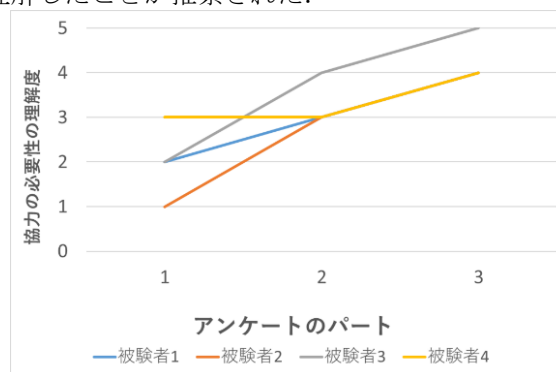


図 2 協力の必要性の評価推移

5. おわりに

大学 CSIRT はあらゆるインシデントが発生した際に、即時的な情報収集が欠かせないため、あらゆる部局の教職員との協力体制が必要である。

教職員はインシデントを学ぶ機会や学習環境が少なく、協力体制の構築が難しい。そこで我々は、教職員に対して、CSIRT に協力する必要性の理解を深めることを目的とした、ボード訓練と振り返りシステムを組み合わせた学習支援を提案した。

実験結果から、ボード訓練と振り返りシステムを組み合わせた学習支援によって、被験者が CSIRT への協力の必要性を理解したことが推察された。

謝辞

本研究のインシデント対応ボード訓練は、トレンドマイクロ株式会社から提供していただいたものである。

参考文献

- (1) トレンジマイクロ株式会社, “インシデント対応ボードゲーム大学版”, https://resources.trendmicro.com/jp-docdownload-form-m265-web-incidentboardgame_s_university.html, (閲覧日:2022/2/8)
- (2) 篠原 俊介, 後藤 田中, 大野 真伯, 小野 滋己, 米谷 雄介, 喜田 弘司, 八重樫 理人, 林 敏浩, 今井 慈郎, 最所 圭三, “香大 CSIRT を対象としたインシデント対応訓練システムのアセスメント分割モジュール開発”, 信学技報, Vol. 120, No. 424, pp. 103-108, 2021