持続可能な大学 CSIRT を目指した対応訓練システムの開発

山崎 勇二 [1)], 後藤田 中 [1)], 小野 滋己 [1)], 青木 有香 [1)], 八重樫 理人 [1)],
藤本 憲市 [1)], 林 敏浩 [1)], 今井 慈郎 [1)], 最所 圭三 [1)]

1) 香川大学

s14t278@stmail.eng.kagawa-u.ac.jp

Development of Response Training System aiming at Sustainable CSIRT for University

Yuji Yamasaki [1)], Naka Gotoda [1)], Shigemi Ono [1)], Yuka Aoki [1)], Rihito Yaegashi [1)],
Ken'ichi Fujimoto [1)], Toshihiro Hayashi [1)], Yoshiro Imai [1)], Keizo Saisho [1)]

1) Kagawa University

概要

情報セキュリティインシデントの対応を行う CSIRT が香川大学にも発足した。CSIRT は対応チームとして成長・持続していくことが非常に重要である。そこで、対応訓練システムを開発し、教育の場として提供することで、持続可能な CSIRT を目指す。

1 はじめに

近年、インターネットの普及に伴い、サイバー攻撃が急激に増加[1]し、様々な企業や組織で情報セキュリティインシデントの対応を行う Computer Security Incident Response Team (CSIRT)が組み込まれている。香川大学（以下「本学」）においても、情報セキュリティインシデントの増加から、2017 年 3 月に CSIRT が発足し、活動を行っている。活動の具体的な内容として、インシデントの初動対応や、学内外の関係組織との連携・情報共有、インシデント内容の調査と再発防止策の検討などを行っている。

一般的な CSIRT の現状として、メンバー全員が初めから対応に長けた能力を持っている、という状況は難しいが、その中でも、対応チームとして成長・持続していくことが非常に重要である。そこで本稿では、持続可能な大学 CSIRT を目指し、そのための教育の場として提供する、対応訓練システムの開発について述べる。

2 持続可能な CSIRT として

情報セキュリティインシデントの対応を行う CSIRT の一般的な課題として、生じたインシデントに対する評価基準が明確でなく、組織内部における重要性のメンバー間の認識の違い[2]が挙げられる。特に、発生したインシデントに対するリスクへの認識の違いが、メンバー間の考える優先順位や対応の差を生み出し、結果として CSIRT の機能停滞を引き起こす可能性が考えられる。したがって、持続可能な CSIRT を目指すには、メンバーのマニュアルによる知識的な教育などに加えて、インシデントに対するリスクアセスメント能力の向上のための実践的な教育が必要とされている。

その中で、大学によって情報セキュリティポリシーや、インシデント管理システムが異なる[3]ことも考慮すべき点として挙げられる。したがって、一般的な対応の教育に加え、本学のシステムや体制を考慮して教育に活用できることが望ましい。

3 対応訓練システム概要

本研究では、情報セキュリティインシデント対応へのリスクアセスメント能力向上のために、実践的な教育の場として提供する、対応訓練システムの開発を行う。開発はコンピュータへのインストールが不要な Web ベースで行う。

本学の体制を考慮するために、システムは過去に本学で発生したインシデントの情報を活用して訓練を提供する。そのため、本システムは対応情報の蓄積を行う入力共有システムと、実際に訓練を提供するシステムの 2 つから構成される。

3.1 情報の蓄積を行う入力共有システム

対応情報の入力・蓄積を行うためのシステムである。図 1 が入力共有システムの試作例である。

右側の入力画面で所属している部署、対応の内容などを入力し、左側で現在の対応状況をリアルタイムに表示、共有する。共有画面は、横軸に CSIRT の部署、縦軸に時間を取り、発生したインシデントに対してどういった流れで対応が行われているのかを可視化する。この入力共有システムを通して、実際のインシデントに対する対応情報をデータベースに蓄積していく。

蓄積された可視情報は、実際の初動対応において参照することで、判断の補助にも活用することを考えている。

図 1 入力共有システムの試作例

3.2 教育の場を提供する訓練システム

訓練システムは、入力共有システムで蓄積された対応情報を用いて行う。まず、システムが対応情報に基づいて、訓練のシナリオと理想の対応例、リスク一覧を生成する。実際の対応情報からシナリオなどを生成することで、本学のインシデント管理システムや体制に沿った訓練を提供する。また、CSIRT にはそれぞれ役割が分かれていることから、CSIRT メンバーである学習者は実際の役割を選択して訓練を開始する。役割に応じた訓練を行うことで、ほかの役割の代替要員の教育なども行えるようにする。

訓練では、システムがシナリオと役割に基づいて、学習者に報告や指示を表示する。図 2 が訓練システムの試作例である。学習者は、まず報告指示や状況から、行うべきだと考える対応を判断し、選択肢から選ぶ。そして、状況と行う対応に付随して起こり得る、リスクの選択と評価を行う。リスクの選択と評価をさせることで、リスクアセスメントの特定と分析、評価のプロセスを疑似的に行わせる。リスクの評価は、学習者が考える、そのリスクの可能性と影響度の大きさをいくつかの段階から選択させる。システムは、学習者が選択した対応に応じた報告・指示を返し、学習者は同様に行う対応とリスクの選択・評価、といった流れの繰り返しとなる。

図 2 訓練システムの試作例

学習者が訓練を終えると、その結果をシステムはあらかじめ設定していた理想の対応例とリスク一覧から、選択した対応の適切性、リスクアセスメントの性、そして訓練の所要時間から対応の迅速性を評価し、学習者の習熟度を測定する。そして、学習者の習熟度に応じた振り返りと、訓練の繰り返しを行い、対応に関する知識や、リスクアセスメント能力の向上、定着化を目指す。

4 おわりに

本稿では、過去のインシデント対応情報を活用することで提供する、持続可能な大学 CSIRT を目指した対応訓練システムの開発について述べた。今後は、実証実験などを通し、システムの運用を進めていきたい。

謝辞

本研究は、香川大学総合情報センター、学術・地域連携推進室情報グループの協力で行われている。ここに謝意を表す。

参考文献

[1] 独立行政法人情報処理推進機構、我が国の情報セキュリティ最新事情、http://www.hisco.jp/matching13/img/EguchiKoenSiryo.pdf [アクセス日：2017/9/30].

[2] 寺本直城、杉浦芳樹、林郁也、矢寺顕行、福本俊樹、近藤光、杉原大輔、我が国における CSIRT の現状と課題、経営情報学会、pp.57-60、2015.

[3] 永井 好和、多田村克己、小河原加久治、国立大学のインシデント管理システムを考える、研究報告情報システムと社会環境、pp.1-7、2014.