振り返り強化のための模擬インシデント訓練による リスクアセスメント情報共有システム

宮崎 凌大，後藤田 中，米谷 雄介，小野 滋己，青木 有香，
八重樫 理人，藤本 憲市，林 敏浩，今井 慈郎，喜田 弘司，最所 圭三
香川大学
s15t269@stu.kagawa-u.ac.jp

An Information Sharing System of Risk Assessment by Training of Imitation Incident as Enhancement Review

Ryota Miyazaki， Naka Gotoda，Yusuke Kometani，Shigemi Ono，Yuka Aoki，
Rihito Yaegashi，Ken’ichi Fujimoto，Toshihiro Hayashi，Yoshiro Imai，Koji Kida，Keizo Saisho
Kagawa Univ.

概要

標的型攻撃が増加し、それに伴い CSIRT 対応が増えている。コマンダが考える最適なインシデント対応において、慎重な判断を要する際、アセスメント基準をメンバと共有することが有益な場合がある。そのようなインシデントを対象に、模擬インシデント活用を提案する。模擬インシデントとは、実際に発生したインシデントを基に作成した仮想的なインシデントの利用であり、類似した条件でも対応が大きく異なること等の知見を共有する。CSIRT 内でのアセスメントにおける認識の違いを共有し、チーム対応の円滑化を行う。

1　はじめに

年々巧妙化する標的型攻撃[1]の対策として、情報セキュリティインシデント対応の専門チームとして、 CSIRT(Computer Security Incident Response Team)を組織する大学などの機関が増えている[2]。それに伴って、チーム共同でインシデント対応を行う場面が増えると考えられ、対応後の振り返りの場を設けることが望ましい。さまざまなインシデントの対応を行う中で、メンバが類似した条件だと判断したインシデントでも、CSIRT 全体統括(以下､コマンダ)はそれらのインシデントに対する対応が同じだと考えているとは限らない。このメンバとコマンダの認識の違いをチーム内で共有することで、メンバ相互に必要とする情報を暗黙的に調査･共有可能､指示内容が的確に伝達可能な、円滑なチーム対応の支援を目的とする。

先行研究として山崎ら[3]は、標的型攻撃などの個人端末の感染が原因となるインシデントの対応を対象とし、対応内容の蓄積と、リスクアセスメント情報の付加によって、CSIRT のチーム共同対応の円滑化を行った。インシデント対応情報(以下、対応情報)とは、縦が時系列で横が対応における役割を示す、表形式に報告や実作業を整理して記録した情報である。また、対応情報が記録された表の任意の項には、リスクアセスメント情報が付加されている。このリスクアセスメント情報を用いて、メンバ間のリスクアセスメントの違いを共有することで、メンバ同士のリスクアセスメントの違いを認識することを支援した。

本研究では、先行研究と同様に端末感染に関わるインシデント対応を対象にする。先行研究の情報共有を行う環境を利用した振返りに加えて、CSIRT のチーム対応のさらなる円滑化を目的とした模擬インシデントを導入する。この研究での模擬インシデントとは、自組織で起きた実際のインシデントの一部を改変した仮想的なインシデントを指す。メンバがあるインシデントの対応を行う際、手続き的に過去の類似のインシデントと同じ対応を取ればいいと判断しても、適切な対応が異なる可能性がある。CSIRT メンバ全員にこの意識を共有することに価値があると考える。模擬インシデントを用いた訓練を通して、コマンダが考える、リスクアセスメントにおける注意点を共有することで、インシデント対応の迅速さやイレギュラーが発生した際の柔軟さにつながり、CSIRT のさらなる円滑化に繋がる可能性がある。

2　リスクアセスメント支援の手法

山崎ら[3]は、コマンダによるリスクアセスメント情報を用いた訓練を通して、メンバ自身にアセスメント能力の差を認識させることを主眼に、支援環境を構築した。リスクアセスメントとは､図 1 のようにリスクの網羅とそれらの優先順位付けを行うことである。リスクアセスメント情報は、リスクアセスメントの結果から定めたリスクに、10

段階で数値化した発生可能性と影響度を紐づけて蓄積している情報である。その中で、実際に起こったインシデントを対象に対応訓練を行い、見過ごしがちなリスクアセスメント情報の共有によるメンバ間の要素の捉え方を、数値の違いとして明確に認識させる機会を設けた。

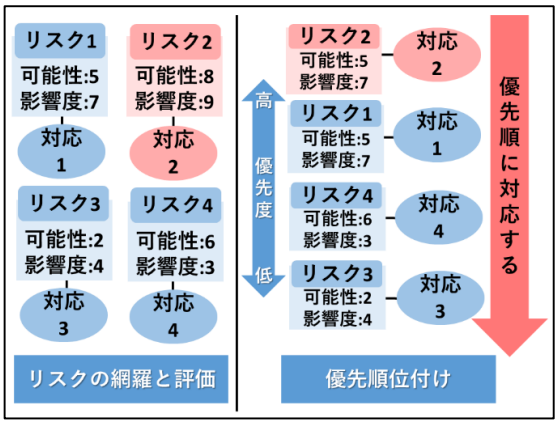

図 1 リスクアセスメントの過程

インシデント対応において、条件の変化によって適切だと考えられる対応が大きく変化する場合がある(図 2)。本研究では、アセスメント能力の差の認識に加えて、模擬インシデント訓練を通して、リスクアセスメントの重み付けの為の判断基準を認識させる環境を構築する。

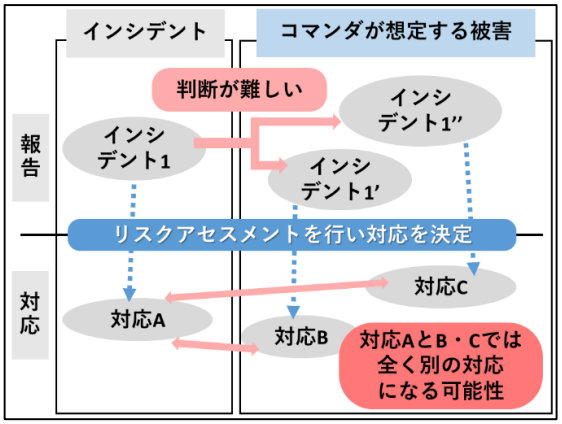

図 2 重要な点の変化に伴う対応の変化

本研究における重み付けのために重要な点とは、コマンダがインシデント対応する際に、メンバとの優先順位が異なる場合があり、対応チームとして慎重な対応が必要になる可能性が高い部分とする。例えば、あるサービスにおける運用担当メンバとコマンダの間で、サービスの継続とメンテナンスの優先順位が異なる場合があるように、重要な点の重み付けは、状況の変化よってさまざまに変化する。このため、ここでの判断基準とは、コマンダがリスクを分析する際、重きを置く要素を判別するための基準となっている。コマンダが考える重要な点を改変した模擬インシデントを作成し、メンバの訓練に活用する手法を用いて、リスクアセスメントにおける、メンバ間の判断基準共有を支援する。

3 模擬インシデント訓練と振り返り

コマンダとメンバが、リスクアセスメントの判断基準を共有するため、模擬インシデント訓練を提案する。模擬インシデントは、コマンダがアセスメントの際に重みをおいた要素に着目し改変した対応情報である。内容が変化し、適切だと考えられる対応が変わったと仮定したインシデントを用いた対応訓練を模擬インシデント対応訓練という。この過程でメンバは、変化した対応情報とそれに対するリスクアセスメント、そして最適だと考えられる実作業を実践的に享受できる。模擬インシデントの基となるインシデントは、コマンダが重要な点を含むと考えるものだけを対象にする。さまざまなインシデントを基にして、報告を改変した無数の模擬インシデントを作成可能だが、対象を絞ることでコマンダへの負荷の軽減を試みる。

あるインシデントを基に作成した、複数の模擬インシデント訓練の実施により、コマンダの考える重要な点をメンバに共有する。さまざまなインシデントを基に訓練を行うことで、コマンダが考える最適な重み付けのため判断基準を、メンバ間で共有する環境を構築する。

3.1 実例に基づき作成する模擬インシデント

コマンダの判断基準をメンバに共有するため、先行研究で蓄積した。実際に発生したインシデントを基にして模擬インシデントを作成する。模擬インシデントは、模擬インシデント対応情報と、模擬アセスメント情報で構成される。作成は、コマンダの考えを共有する目的で、コマンダが担当する。コマンダの負荷が高くなってしまうので、実際に発生したインシデントの対応情報の一部を改変する手法を用い、負荷軽減を図る。

模擬インシデントの作成手順は、図 3 の「コマンダが入力作成」の部分に該当する。まずコマンダは、先行研究で蓄積した、実際に発生したインシデント対応情報から、基となるインシデントを選択し、複製することで模擬インシデントのベースを作成する。次にコマンダは、対応情報の状況報告の中から重要な点を定め改変し、模擬インシデント対応情報を作成する。リスクアセスメント

を行う際は、模擬インシデント作成のために対応情報を改変した部分だけでなく、対応情報全てに対して再度アセスメントを行う。これは、コマンダが対応情報の一部を改変したことによって、改変されていない部分に影響を及ぼす可能性を考慮するためだ。作成した模擬インシデントを用いて、メンバにコマンダが判断に迷う重要な部分の共有を行うための訓練を実施する。

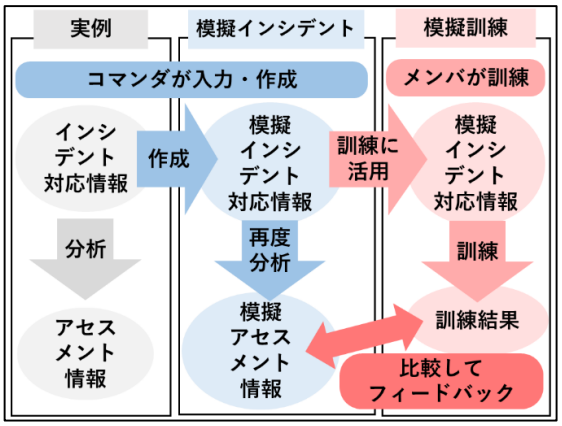

図 3 模擬インシデント作成とその対応訓練

3.2 模擬インシデント対応訓練

メンバに対して、コマンダが作成した模擬インシデントを活用して実践的な訓練を行う手法で、メンバにコマンダの判断基準の共有を試みる。この手順は図 3 の右側、「メンバが訓練」の部分に該当する。訓練では、対応情報に記録された報告や実作業を時系列順に追いながら、リスクアセスメントを行い、その時点で最適だと考える対応を選ぶことを繰り返す。

訓練においてメンバが行うリスクアセスメントの方法は、コマンダがリスクアセスメント情報を付加する際と同様である。想定できるリスクに、可能性と影響度の指標で数値化し紐づけた、リスクの情報を利用する。メンバは、ある時点でのリスクが網羅できたら、紐づけた指標を参考に対応の優先順位を付ける。次にメンバは、最も優先度の高いリスクを処理するための対応を、メンバの負荷を抑えるために選択式で決める。選択肢のうち、一つはコマンダが対応情報に入力した対応である。報告書から一度にすべての結果を見るのではなく、報告や状況の変化を追って、都度リスクアセスメントを行う形式の訓練により、実践的な対応訓練の提供を試みる。

訓練の最後には振り返りを行い、用いた模擬インシデントにおけるコマンダと訓練者のリスクアセスメントの違いの共有を支援する。さらに、同じインシデントを基にした複数の模擬インシデントを用いた訓練を繰り返すことで、コマンダのリスクアセスメントにおける判断基準自体を CSIRT 全体に共有を試みる。これにより、メンバ同士の判断基準を理解して対応に当たることができるようになれば、より円滑なチーム対応に繋がると考えられる。

4 振り返り強化のためのシステム

4.1 対応情報、アセスメント情報の蓄積共有

山崎らのシステム[3]は縦軸に時間、横軸に役割を取る表形式(図 4)で、実例の対応情報とリスクアセスメント情報が蓄積されている。一つの項にはある時点でのある役割による状況報告・実作業が入力されており、任意の項にはリスクアセスメント情報が付加されている。付加情報は、図 5 のようなシステム UI で入力する。なお、セキュリティの観点から本稿で扱うインシデント情報等は、実際に香川大学で発生したインシデントではない。

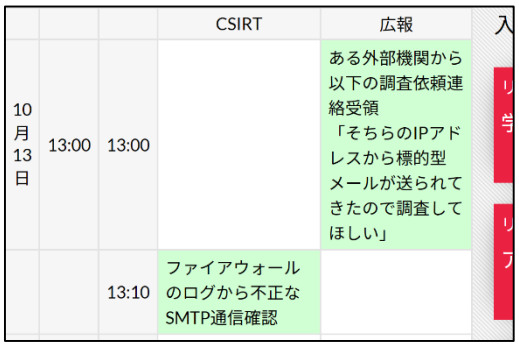

図 4 システムに蓄積された情報

先行研究のシステムは、対応情報を入力する入力共有部、アセスメント情報を付加する情報付加部、実例を活用した訓練を行う対応訓練部の 3 部に分かれている。山崎らは、これを活用した訓練を通して、メンバ間のリスクアセスメント能力差の理解を支援した。本研究では、この既存システムに、「模擬インシデント作成」と「模擬インシデント対応訓練」の二つの機能拡張を行い、先行研

図 5 アセスメント情報を付加するシステム UI

究システムの情報共有を用いた振り返りに加えて、模擬インシデント対応訓練を行う環境を提供し、判断基準を共有ができる環境を提供する。

4.2 システムから見た模擬インシデント作成

本研究のシステムでは、コマンダが作成する模擬インシデントを用いた訓練を利用して振り返りの強化を行い、CSIRT のチーム対応のさらなる円滑化を目指す。

コマンダが訓練を作成する際は、先行研究の入力共有部と同じ UI を用いる。既存インシデントの対応情報が入力された表から、任意の項を改変して模擬インシデントとする。図 4 の各項を作成する入力部の UI を図 6 に示す。入力する報告・実作業のデータには「時間」、「役割(所属部署)」、「タイプ」の情報を紐づけて入力する。時間は入力時間ではなく、報告・実作業を行った時間である。メンバの訓練時には入力した表の上段から、時間順にステップを作成し、段階的に訓練の進行を行う。項の種類は、報告の項と実作業の項がある。報告の項は、対応中に判明した報告や状況変化を記録したもので、訓練のステップごとにメンバに表示していく。実作業の項は、リスクに対処するための対応行動や作業で、メンバがリスクアセスメントの後に決める対応の選択肢に含まれる。項に入力されたデータが報告、実作業のどちらか判別するためにタイプを用いる。入力が「不審メールが検知された。」などの報告の場合は、受動タイプ、入力が「マシンのフルスキャンを行った。」などの実作業だった場合は、能動タイプに設定する。

図 6 模擬インシデント情報入力 UI

コマンダが改変する項は、コマンダがインシデント対応した際に、メンバとのアセスメントの優先順位が異なる可能性が高く、メンバ間で判断基準を共有する価値があると考えた部分である。既存データを改変する形でシステムに入力し、模擬インシデント対応訓練に活用する。

4.3 判断基準自体を共有するための環境

メンバが訓練者となり、コマンダとの判断基準共有を目的とする模擬インシデント対応訓練を行う。訓練画面 UI は、縦に 3 分割されており(図 7)、それぞれが状況の表示、リスクアセスメント入力、実作業の選択を担う。

図 7 訓練画面全体 UI

訓練画面の左部分は、訓練者に対して訓練における現在の状況を表示する(図 8)。下段には今までの状況を表示する。本訓練における「現在」とは、入力共有部で入力した「時間」を参照して作成したステップの、ある一つを指し、ステップは時系列順にすすめる。

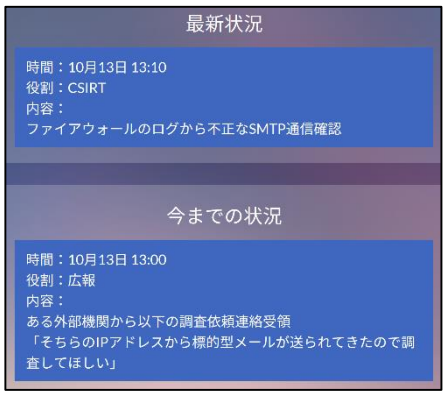

図 8 訓練画面:現在の状況部分

訓練画面の中央部分はリスクアセスメントの入力を行い(図 9)で、訓練者は、初期状態でリスクが入力されていない状態から、リスクの網羅と優先順位付けを行う。訓練者は、UI に表示された現在の状況を基に、リスクの網羅ができると考えるまで追加する。初期状態ではリスクの入力は無く、訓練者が自由にリスクを追加していく。訓練者によるアセスメント情報は、情報付加部におけるリスクアセスメントと同様に、可能性と影響度を数値化した指標を、リスクに紐づけて入力する。次に訓練者は、網羅したリスクの優先度が高いと考えたものほど上に並ぶようリスクに順位づけする。

訓練画面右部分は、訓練者がどの実作業を行うか選択肢から決定する部分である(図 10)。図 9 に自ら入力したリスクアセスメント情報を基に、適

切だと考える作業を選択する。

システムが対応の選択肢を作成する際、コマンダが入力した能動タイプの対応情報を利用する。対応の選択肢の一つは、訓練者と同じ時点でコマンダが入力した能動タイプの対応情報である、他の選択肢は、訓練における「現在」とは別の時点の能動タイプの対応情報からランダムに選出する。訓練者は対応を選んだら図 10 右下の送信ボタンを押して次の時点に進み、次の時点のリスクアセスメントと対応の選択を行う。

図 9 訓練画面:リスクアセスメント情報入力部分

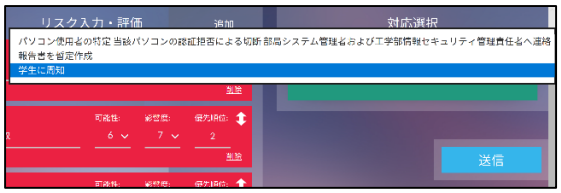

図 10 訓練画面:実作業選択部分

訓練者は、インシデント情報の最後の対応を終えた後、図 11 に示す画面でコマンダのインシデント対応との結果比較を行う。結果比較では、訓練者とコマンダの、リスクアセスメント情報と対応をステップごとに並べて表示する。図 11 の上部には受動タイプの対応情報が状況として表示され、下段左側には訓練者の選択した対応とアセスメント情報、下段右側にはコマンダの受動タイプの対応情報とアセスメント情報が表示され、ステップごとに対応の違いを確認できる。

図 11 模擬インシデント訓練の結果比較画面

本研究の模擬インシデントを用いた訓練は、訓練者が訓練を通してインシデント対応における、実践的なリスクアセスメントを行う環境の構築を試みた。さらに、訓練者がこの環境を用いて、同じインシデントを基に作成した複数の模擬インシデント対応訓練を行うことにより、コマンダが考えるリスクアセスメントの判断基準をメンバに共有できる可能性がある。

5 まとめ

標的型攻撃の巧妙化が進む中、専門チームである CSIRT でも、振り返りによって能力向上や対策を行うことが望ましい。本稿では、CSIRT の対応能力向上の支援を目的に、標的型攻撃が原因となるインシデントを対象とした、コマンダの判断基準をメンバに共有する手法について述べた。共有手法には実際に発生したインシデントに類似する模擬インシデントを用いた訓練を導入した。訓練の利用でメンバ間の判断基準共有を支援することによって、対応にあたるメンバ同士が必要とする援助を言外で自主的に行うことや、判断の相違により生まれる対応の遅れを軽減すること等を促進する。本研究のインシデント対応における情報共有手法によって、CSIRT のチーム対応を支援し、セキュリティ対策に役立てることを期待する。

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”、p.13、2016、http://www.hisco.jp/matching13/img/EguchiKoenSiryo.pdf .

[2] CSIRT 人材サブワーキンググループ、”CSIRT 人材の定義と確保(Ver.1.5)”、p.3,15、日本コンピュータセキュリティインシデント対応チーム協議会、2017 年.

[3] 山崎勇二、後藤田中、米谷雄介、林敏浩、八重樫理人、最所圭三、”インシデント対応におけるリスクアセスメント過程認識のための可視化・伝達を支援するシステムの開発と支援”、信学技報 vol.117 no. 469 ET2017-103、pp. 83-88、2018 年.