JSiSE Research Report
vol.33,no.5(2019-1)

リスクアセスメント情報を活用した判断基準共有のための模擬インシデント訓練システム

宮崎 凌大[*1], 後藤田 中[*1], 米谷 雄介[*1], 小野 滋己[*1], 青木 有香[*1],
八重樫 理人[*1], 藤本 憲市[*1], 喜田 弘司[*1], 林 敏浩[*1], 今井 慈郎[*1], 最所 圭三[*1]
*1 香川大学

A Training System of Dearing with Imitation Incident by Information of Risk Assessment

Ryota Miyazaki[*1], Naka Gotoda[*1], Yusuke Kometani[*1], Shigemi Ono[*1],
Yuka Aoki[*1], Rihito Yaegashi[*1], Ken’ichi Fujimoto[*1], Koji Kida[*1],
Toshihiro Hayashi[*1], Yoshiro Imai[*1], Keizo Saisho[*1]
*1 Kagawa University

増加する標的型攻撃の対策として，インシデント対応時の判断基準を CSIRT 内に共有し，対応の重要点をメンバが理解しておくことは重要である．そこで，類似条件の模擬インシデントの訓練を比較することで，類似した条件でも対応が大きく異なる可能性があるなどの知見を共有する．本稿では，香川大学 CSIRT を対象に研究システムを用いた訓練実験と評価に関して報告する．

キーワード: セキュリティ，情報スキル，インシデント，リスクアセスメント，学習支援システム，

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・共有可能で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．

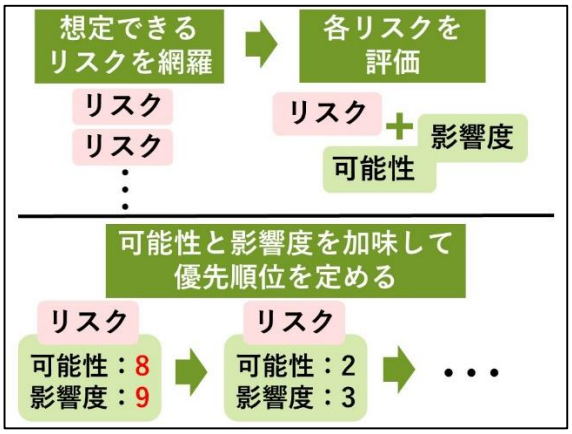

図 1 リスクアセスメントの過程

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．

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．

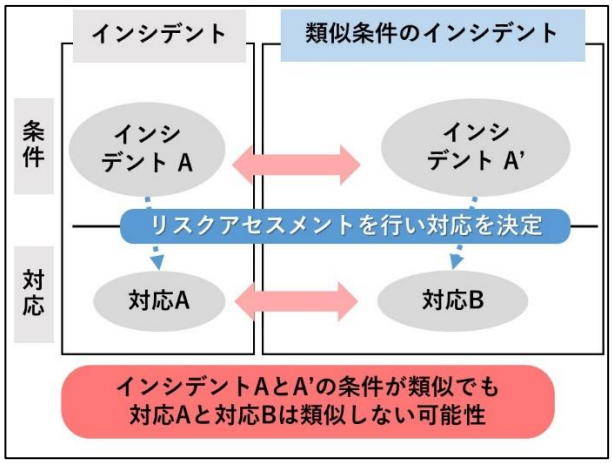

図 2 重要な点の変化に伴う対応の変化

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訓練できる．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．

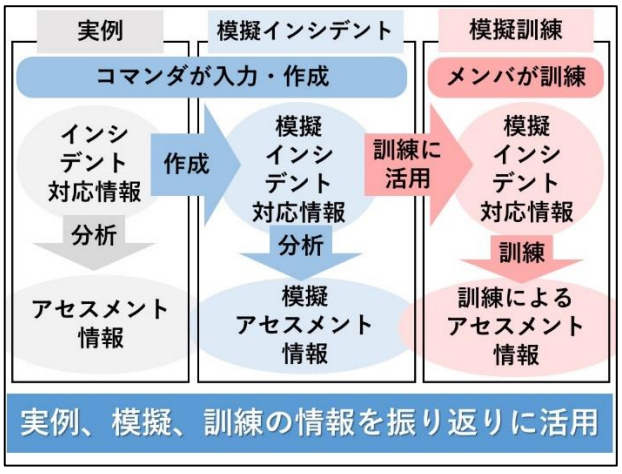

図 3 模擬インシデント作成とその対応訓練

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. 模擬インシデント訓練システム

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．

4.1 対応情報，アセスメント情報の蓄積共有

システムは縦軸に時間，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．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．

			CSIRT
10月13日	13:00	13:00	
		13:10	ファイアウォールのログから不正なSMTP通信確認
		13:20	パソコン使用者の特定 当該パソコンの認証拒否による切断 部局システム管理者および工学部情報セキュリティ管理責任者へ連絡
		13:30	使用教員に呼び出しを依頼 当該学生を呼び出してパソコン確保 聴取及びUSBブートでのウイルス調査を開始

図４ システムに蓄積された情報

4.2 システムから見た模擬インシデント作成

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，図 4 の「CSIRT の行」の項目を，図 5 のように自由記述で改変する．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５ 模擬インシデント作成画面

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 判断基準を共有する環境

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．訓練画面は縦に 3 分割されており，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 6 は，訓練者に対して訓練における現在の状況を表示する部分である．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．

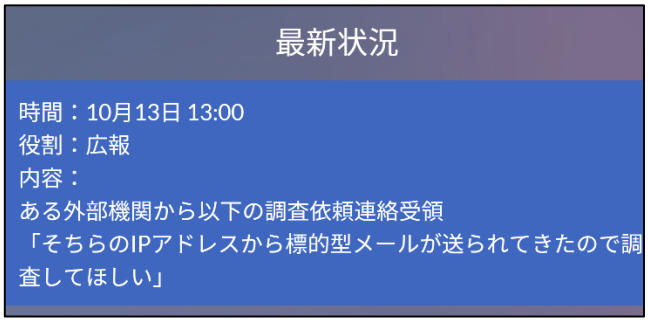

図 6 訓練画面:現在の状況部分

図 7 はリスクアセスメントを入力する部分である．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．

図 8 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 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 7 訓練画面:リスクアセスメント情報入力部分

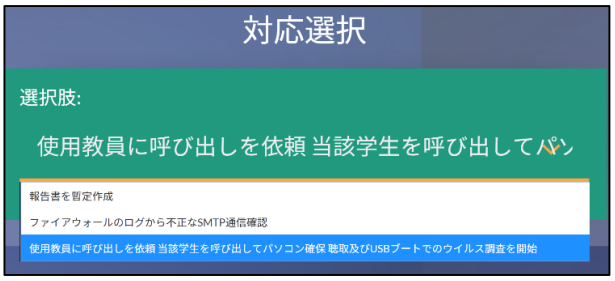

図 8 訓練画面:実作業選択部分

訓練者は，インシデント情報の最後の対応を終えた後，図 9 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．左側には訓練者の選択した対応とアセスメント情報，右側にはコマンダ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 9 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. 模擬インシデント訓練実験

香川大学 CSIRT を対象に，訓練システムを用いて研究目的が達成可能か調査した．4 名の被験者に対して上述の模擬訓練を実施し，アンケートを用いて判断基準共有の程度を調査した．実験環境や考察を以下に示す．

5.1 実験目的

模擬インシデント対応訓練による，CSIRT のインシデント対応における判断基準の共有ができているか評価する．また，将来的には香川大学 CSIRT(以下，本学 CSIRT)にて訓練システムとして導入することを目指す．そのため，本学 CSIRT の協力の下，過去に香川大学で発生したインシデント事例を用いて訓練する．

5.2 実験対象者

本実験の対象者は本学 CSIRT のメンバである．被験者は 2 種類あり，模擬インシデントの作成を行う被験者(コマンダ役)と作成された模擬インシデントを用いて訓練を行う被験者(訓練者)である．コマンダ役は，本学 CSIRT でコマンダを担当する職員が行う．この被験者は，コマンダを担当するとともに実際にコマンダとしてインシデント対応の管理を行っている．

訓練者は本学 CSIRT のメンバから 4 名選出する．そのうち 2 名は，広報係と総務係である．残りの 2 名は本学 CSIRT でインシデント対応の技術的作業(実作業)を担当しているメンバである．ただし，1 名は勤続年数 5 年未満で実作業の経験がない者(メンバ A), 1 名は勤続年数 10 年以上でコマンダを担当した経験と実作業の経験のある者(メンバ B)である．訓練者によって違った役割や経験を持つ者を選出し，様々な背景に対する作用を調査する．

5.3 実験対象のインシデント

対象とするインシデントは，判断基準の共有が必要なインシデントのみに絞ることで，訓練コストを抑える．訓練に利用するかどうかの決定はコマンダ，あるいは部局のセキュリティ担当が行う．

5.4 評価アンケート

訓練結果の評価を特典などの数値化するのは困難なため，5 段階評価のアンケートを用いる．しかし，5 段階評価では順序しかわからないことや，訓練者ごとに 5 段階の理解度に対する認識がずれてしまい，訓練者同士のアンケートを比較することができない可能性がある．そこで，単純な 5 段階ではなく表 1～4 のように各指標に対応する内容を定めることで訓練者間の指標に対する認識の違いを最小限にすることを図る．

5.5 模擬インシデント訓練実験の手順

実験は以下の 3 段階で行う．

1.コマンダが模擬インシデントを作成

2.メンバが模擬インシデントの対応訓練

3.メンバがアンケートに回答

表 1 「リスクの網羅」に関する理解度の詳細

	Q. コマンダと同様に，リスクの「網羅」ができていたと思いますか.
理解度	内容
1	全く網羅できない
2	一部網羅できる
3	半分程度網羅できる
4	おおよそ網羅できる
5	コマンダ同様に網羅できる

表 2 「リスクの内容」に関する理解度の詳細

	Q. コマンダが考えるリスクの「内容」について，理解していたと思いますか.
理解度	内容
1	全く思いつかない
2	いくつかリスクの概要が思いつく
3	いくつかのリスクが思いつく
4	リスクが思いつく(可能性と影響度含まず)
5	リスクが思いつく(可能性と影響度含む)

表 3 「リスクの優先順位」に関する理解度の詳細

	Q. コマンダと同様に，リスクの優先「順位」付けができていたと思いますか.
理解度	内容
1	全くわからない
2	いくつかのリスクの優先順位がわかる
3	最優先のリスクはわかる
4	正しく順位づけできる
5	正しく順位付けでき，優先度合いもわかる

まず，模擬インシデント作成について説明する．コマンダが, 組織で実際に発生したインシデントのうち, メンバに判断基準を共有すべきだと考えたインシデントを改変して模擬インシデントを作成する．本研究における判断基準とは，リスクアセスメントを行うために必要な 4 つの能力(図 10)を合わせたものとする．

- 脅威を列挙できる
- リスク評価を正しくできる
- 優先対応を適切に決定できる
- 必要な対応がわかる

表 4 「対応の根拠」に関する理解度の詳細

	Q. コマンダが考える対応の「根拠」について，理解していたと思いますか.
理解度	内容
1	全く思いつかない
2	いくつか事象が思いつく
3	根拠になりそうな事象がいくつか思い当たる
4	全てではないが根拠がわかる
5	(コマンダと同程度に)根拠がわかる

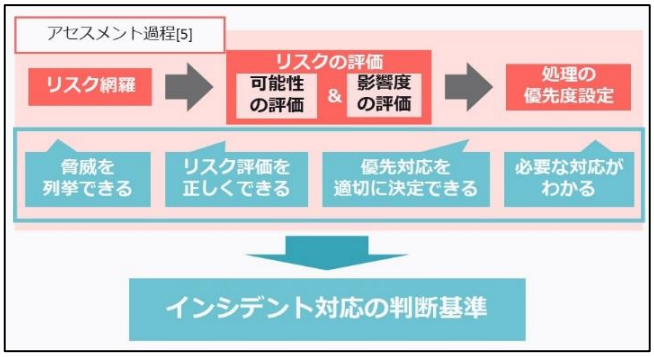

図 10 アセスメント過程と判断基準

実例から模擬インシデントを作成する際, コマンダは, 時系列で整理されたシステム上の対応上場から，上述の能力を用いてアセスメントを行った時点の報告を選択する．そして，選択した報告の時点で挙げたリスク一覧の優先順位が変化したと仮定して，選択した報告を自由記述で改変する．

発生するインシデントの状況や対応手順が多種多様なものになるため，コマンダがドロップダウンリストやスライドバーなどシステムの機能で模擬インシデントを作成するのは困難である．そのため，コマンダが作成する際の負荷が増加してしまうが，作成の自由度を高めることに繋がる．そのため，自由記述で改変を行う．

次に，訓練実験について説明する．実例の対応訓練と模擬インシデントの対応訓練の２回の対応訓練を行い，対応の違いから判断基準の共有を図る．訓練は訓練者１人ずつと対面で行った．まず訓練者は，実例の対応訓練を行い，結果確認画面から訓練を振り返る．その後，模擬インシデントの対応訓練を行い，結果確認画面から対応を振り返る．最後に，訓練者は２つの訓練の内容と振り返りから判断基準の違いを考える．

最後にアンケート評価について説明する．訓練の振り返りの後，アンケートを用いて実験の評価を行う．質問項目は判断基準をもととなるアセスメントの理解度(図 13 参照)である．訓練者は表 1～4 を見ながら，訓練前と訓練後それぞれの理解度を回答する．

5.6 模擬インシデント訓練実験の結果と考察

本実験の対象者は１名のコマンダ役と４名の訓練者である．訓練者のアンケート回答結果を表 5 に示す．回答結果に 2 通りの傾向が見られたので，2 通りの訓練者に分けて考察する．

表 5 アンケート結果

被験者	時期	リスク	網羅	順位	根拠
広報係	実験前	2	2	2	1
	実験後	3	2	2	3
総務係	実験前	2	1	2	2
	実験後	4	4	4	4
メンバA	実験前	2	2	2	2
	実験後	4	4	4	3
メンバB	実験前	4	4	4	4
	実験後	4	5	4	4

1:理解度 最低 / 5:理解度 最高

メンバBは訓練前後を通じて理解度が高いと回答した. 表 5 の下１列に示した回答結果に関して考察する．訓練前は全項目で 5 段階中 4 と回答し，リスクアセスメントの各段階の能力に関する理解度が高いと認識していることがわかった．これは，過去コマンダを担当した経験があること, 10 年以上勤務などの背景が考えられる．訓練後は「リスクの網羅」の項目に 5 と回答し, 訓練前と比べて理解度が向上したと認識していた．他の項目は訓練前と変わらず 4 と回答した．

メンバ B は，コマンダを経験したことがあるため，理解度は訓練前から高いと予想していた．また，訓練の結果リスクを「網羅」する能力が向上したと回答したことは，コマンダ役の判断基準の共有ができたからではないかと考えられる．コマンダ役，メンバAのどちらもコマンダの役割を担当したことがあるが，全く同じ判断をすることは困難である．本実験の結果は，

そういった同じ役割だが違った判断基準を持つ場合のコマンダ役の判断基準を共有できたと考えられる．

次に，訓練前の理解度が，低いと回答した訓練者に関して考察する．その被験者は広報係，総務係，メンバ A で，アンケート結果は表 5 の上 3 列に示す．

総務，広報，メンバ A は訓練前の回答は，理解度 1 の「全く能力〇〇できない」または理解度 2 と認識していた．訓練後の回答は 3 名とも各理解度に対して変化なしまたは理解度が向上したと認識していた．ただし，この回答結果は，本実験で用いたインシデントに絞った判断基準の共有だと考えられるため，本学 CSIRT で導入し定期的に様々なインシデントを活用した模擬インシデント訓練を行うことで，より実用的な効果を発揮する事ができると考えられる．

本実験では，コマンダが模擬インシデントを作成する際，コマンダが自由記述で模擬インシデントを作成することで，多様なインシデントの対応における判断基準の共有に活用することができると考えられる．

また，インシデント対応を行う際のある判断基準を持つコマンダ役から別の判断基準を持つメンバ B に対して判断基準を共有する事ができたことや，対応経験のないメンバに対してコマンダの判断基準を共有できた，といったことからコマンダが作成した模擬インシデントを用いた対応訓練を活用することで，一定の判断基準を共有する事ができると考えられる．

6. おわりに

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，経営管理室総務グループ，経営理室広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)

(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)