リスクアセスメント情報共有システムを用いたリスク絞り込み可視化に関する一考察

新田 和也，後藤田 中，米谷 雄介，小野 滋己，八重樫 理人，
林 敏浩，今井 慈郎，喜田 弘司，最所 圭三

香川大学

s16t256@stu.kagawa-u.ac.jp

A Consideration on Visualization of Risk Narrowing Using Information Sharing System of Risk Assessment

Kazuya Nitta，Naka Gotoda，Yusuke Kometani，Shigemi Ono，Rihito Yaegashi，
Toshihiro Hayashi，Yoshiro Imai，Koji Kida，Keizo Saisho

Kagawa Univ.

概要

サイバー攻撃の巧妙化・多様化は、セキュリティインシデント発生時の対応を複雑化させ、報告文書の表面上は前例のある手口であっても、コマンダのリスクアセスメントが異なるインシデントが発生している。そのため CSIRT スタッフにはコマンダのリスクアセスメント情報の共有が必要となる。しかし、部局、立場の差から情報共有の手段が報告書に限定され、コマンダが持ち合わせるインシデント対応時のリスクアセスメント情報の共有は難しい。そこで、本研究では情報共有の支援方法として、組織内の限定的な情報伝達ラインの課題を解決するために、従来のアセスメントシステムを用いたコマンダのリスクアセスメント情報の共有を、対応過程の把握・共有による組織の一貫性強化に活用するアプローチを提案する。従来研究より明らかになった、コマンダ、スタッフ間のリスクアセスメントの相違に対し、リスクの絞り込み過程に着目することにより、コマンダ、スタッフ間で対応過程の把握・共有可能な包括的な情報共有が可能な環境の構築を目指す。本稿では、明らかになったスタッフ間のリスクアセスメントの相違について、リスク絞り込みの観点から考察を述べ、コマンダ、スタッフ間のリスク絞り込み過程の把握・共有の支援実験のための計画について述べる。

1 はじめに

近年、サイバー攻撃の巧妙化・多様化が進み、多種多様の手口が用いられるようになった[1]。セキュリティインシデントの中には対応の際過去の事例を参考にした対応があてにならないケースもあり、調査・対応漏れによる組織への被害が懸念される[2-3]。したがって即時即断のインシデント対応の中でもマニュアルに従った機械的な対応ではなく、重要な局所部において慎重な判断を下せる能力が対応に当たるスタッフに必要である。そこで我々はインシデント対応に当たる際にインシデント対応要員が行うリスクアセスメントに着目し、リスクアセスメントの向上が巧妙なインシデントの対応過誤を防ぐと考えた。

既に先行研究では著者らがリスクアセスメント可視化による蓄積・共有、リスクアセスメントを入力しながら行う実践的な訓練を可能とするシステム環境（以下、リスクアセスメント情報共有システム）を構築している[4-5]。そしてシステムを用い、現状調査として香川大学 CSIRT（以下、本学 CSIRT）において CSIRT 全体統括（以下、コマンダ）[6]と他メンバのリスクアセスメントの差を観測できるか否かの検証実験を行った。結果として、コマンダと他メンバ間ではリスクアセスメントに相違があることが明らかになっている。

これらを踏まえ本研究では、コマンダと他メンバ間で明らかになったリスクアセスメントの差をメンバにフィードバックすることにより、メンバのリスクアセスメントの資質向上を試みる。本研

究と先行研究の差分の明確化のため先行研究、本研究のユースケース図を図 1､2 にそれぞれ示しておいた。

本稿では事前実験に対して新たに結果を再抽出し考察した内容について報告する。またその結果からインシデント対応の際に初動で挙げたリスクに対し、対応、それによるリスクの削除を順に行っていく過程（以下、リスク絞り込み過程）に着目し、これに関する考察を議論し、考察立証のための評価実験計画について述べる。

インシデント対応に対する組織・体制強化、対応者個人の支援のための手法、システムは先行研究[9-12]で議論されてきたが、コマンダ、スタッフ間に焦点を当てたリスク絞り込み過程に関しての議論は不足している。本稿はその不足部分の補完として位置づけることができる。

2 巧妙化に伴う対応の過誤

2.1 巧妙なインシデント

インシデントの中には表面上は過去に事例があるインシデントに似ているが過去の事例とは対応が異なるというインシデントがあり、過去の事例と見せかけ騙すのが攻撃手の手口である[3]。

よって日々進化するインシデントに臨機応変に対応する能力がインシデント対応要員には必要となっている。

2.2 インシデント対応の方法と弱点

インシデント対応要員はインシデント対応にあたる際、即時即断[7]が求められるため、過去のインシデントの報告書を参考に対応する場合がある。しかし、報告書に頼り切った機械的な対応では巧妙なインシデントの対応を誤ってしまい、調査、対応漏れからインシデントを回避できない可能性がある。

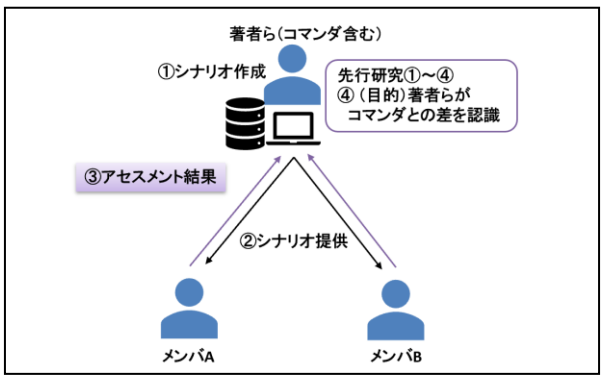

図 1　先行研究のユースケース図

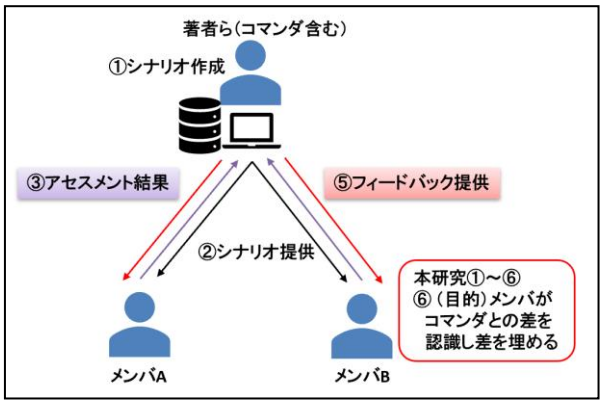

図 2　本研究のユースケース図

3 アセスメント共有による課題解決

前章で述べた課題解決のため、我々はリスクアセスメントに着目した。リスクアセスメントとはインシデント対応時の対応の根拠となる要素で、インシデント対応要員のインシデントへの知識・経験が反映されるため、部局や立場、経験の違いによって差が生じる。そこで我々はリスクアセスメントの共有がインシデント対応要員の資質向上に繋がると考えた。したがって、部局や立場などの障壁を払ったリスクアセスメント情報の共有が課題解決に必要である。まず我々は、コマンダとスタッフ間のリスクアセスメントの共有によるメンバのリスクアセスメントの資質向上が可能か調査することを試みた。

3.1 リスクアセスメント

リスクアセスメントとはトリアージ（インシデント発生時のアラートを分析し対応プラン、対応優先順位付けを行うインシデント対応フローの一部）の際に対応者が行う行為であり、一般的なリスクアセスメント実施過程[8]に基づき次のように定義した。

- **リスクアセスメント**

リスク列挙　インシデント発生時に収集されたアラートから、感染拡大後のリスク、発生原因だと考えられるリスク、事後のリスク、これらそれぞれの考えうる全リスクを列挙すること[7]

リスク評価　列挙したリスク一つ一つにそのリスクが起こる（起こっている）可能性、そのリスクの影響度の二つの指標で評価付けを行うこと

優先順位付け　評価したリスクの評価の度合いからどの順番で対応していくかの優先順位付けを行うこと

対応決定　各リスクへの適切な対応の決定を行うことで、リスクによって、応急処置の対応、原因特定・根絶の対応、事後処理の対応に分けられる[7]

3.2 リスクアセスメント情報の共有

リスクアセスメントは対応当事者が行うもので、インシデント発生事後に作成される報告書には未記載の情報である。つまり報告書には対応の根拠となる情報が欠けている。振り返りの際、またインシデント対応の際、組織のインシデント対応要員全員が報告書と同時にリスクアセスメント（対応の根拠）情報を共有することで、インシデント対応要員の資質が向上し、巧妙なインシデントへの対応の過誤を取り除くことに繋がる。

4　共有手法とシステム概要

リスクアセスメント共有手法について述べる。山崎らは実例のインシデント情報に可視化したリスクアセスメント情報を付加して蓄積するシステムを開発した[1]。またそのシステムでは過去のインシデントをリスクアセスメントを入力しながら実践方式で訓練でき、コマンダのリスクアセスメント情報の共有が期待できる。宮崎らは模擬インシデント訓練システムを既存システムに拡張機能として加えた[2]。

本研究ではこのシステムを用いることを手法とし、山崎らが開発したシステムを用いてリスクアセスメントを共有する。本章ではシステム概要を順に述べていく

なお、システム画面等で記載されているインシデントは実際のインシデントではない。

4.1 リスクアセスメント可視化・訓練システム

まず山崎らが開発したリスクアセスメント可視化及び訓練システム（以下、実例インシデント訓練システム）について一つの訓練画面の構成要素、図 3、4、5 を用いて説明する[1]。

図 3 の画面では報告を受けている情報（現在の状況）を表示している。図 4 は現在の状況に対してリスクアセスメントを行い、判断結果を入力する画面である。図 4 の画面においてリスク評価の可能性、影響度にそれぞれ数字を入力しているがこれらリスク評価の尺度は表 1 のように定められており、10 段階で数値化されている。

図 5 では最優先のリスクへの処置となる対応を選択する。対応については処置すべきリスクが決まれば実施手順書に従った対応をとるため、比較的判断の比重が少ないことから入力方式ではなく選択方式にしている。これら 3 要素でひとつの画面が構成されており、このひとつの画面が 1 フェーズ（インシデント対応進行状況の局面）を表している。

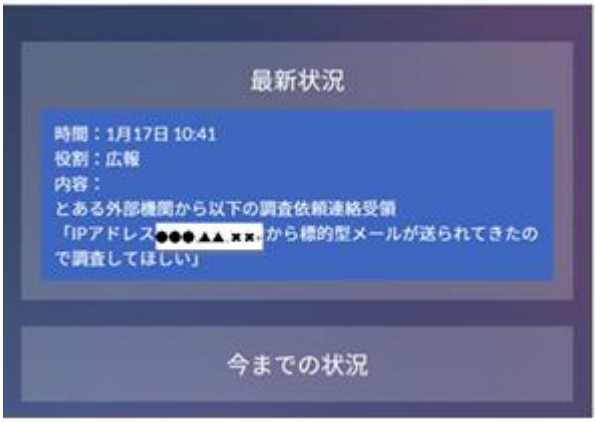

図 3　訓練画面：現在の状況

（文献[13]：図 6 より引用）

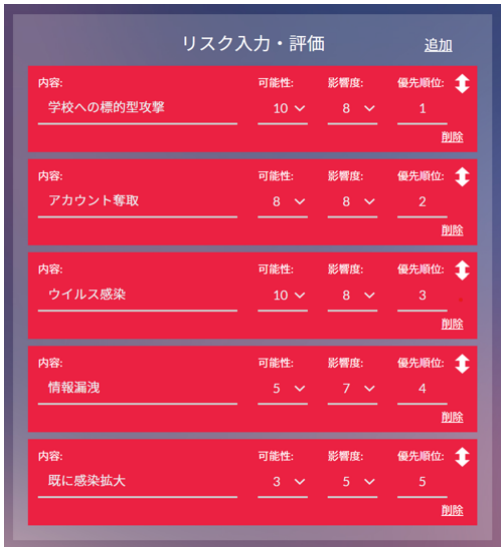

図 4　訓練画面：リスクアセスメント入力

表 1　リスク評価の尺度

評価	可能性	影響度
10	リスクが確実に顕在化	国民の生命，財産，プライバシー等へ重大な影響を及ぼす
9	リスク顕在化の可能性が約 90%	学内から学外へ重大な影響を及ぼす，重要度 3 の情報漏洩など
8	リスク顕在化の可能性が約 80%	学内から学外へ重大な影響を及ぼす，資産への深刻な損害・業務停止など
7	リスク顕在化の可能性が約 70%	行政事務の執行等に重大な影響を及ぼす，重要度 2 の情報漏洩など
6	リスク顕在化の可能性が約 60%	学内全体の業務に影響を及ぼすが学外への影響は無し，重要度 1 以下の情報漏洩など
5	リスク顕在化の可能性が約 50%	学内全体の業務に影響を及ぼすが学外への影響は無し，資産への被害など
4	リスク顕在化の可能性が約 40%	行政事務の執行等に軽微な影響を及ぼす
3	リスク顕在化の可能性が約 30%	所属部署の業務遂行に軽微な影響を及ぼす
2	リスク顕在化の可能性が約 20%	職員個人の業務遂行に軽微な影響を及ぼす
1	ほぼ顕在化の可能性無し	影響をほとんど及ぼさない

1 フェーズにて図 4 の画面のようにリスクアセスメントを行い、リスクの優先順位順に対応を選択し 1 フェーズ一対応でフェーズが進行していくのだが、対応を行い既に処理済みのリスクはその都度消していく。この消していく過程の様子がリスク絞り込み過程である。

次に訓練結果表示画面を図 6 に示す。結果画面では図 6 の画面のように 1 フェーズごとに表示され、左側に訓練者、右側にコマンダが入力したリスクアセスメントと選択した対応がそれぞれ表示され結果を比較することが可能である。この画面が訓練者の結果のフィードバック、コマンダのリスクアセスメント共有の役目に当たると期待される。

図 5　訓練画面：対応選択

図 6　訓練結果比較画面

4.2　模擬インシデント訓練システム

次に宮崎らが山崎らの開発したシステムに拡張したシステムである模擬インシデント訓練システムについて説明する[2]。模擬インシデント訓練システムは訓練方法、訓練結果表示方法は実例インシデント訓練と一緒であるが訓練の内容であるインシデントが異なる。

宮崎らは、巧妙なインシデントを模擬インシデントと名付け、山崎のシステムに蓄積されているインシデントから表面上似ているがとるべき対応が異なるよう構成されたインシデントを作成し、新たな訓練として拡張した。

4.3　アセスメント判断能力測定の手法

前節で説明したシステムにおける訓練者のリスク評価、優先順位付け等の入力値を訓練ログから抽出することでリスクアセスメントを測定する。

5　事前実験の結果と考察

宮崎らは、前章で説明したシステムを用いて本学 CSIRT を対象に、コマンダとメンバの間にリスクアセスメントの差があるか検証するための実験を行った[5]。本章ではその実験結果を新たに抽出し、我々の考察を述べる。

5.1　事前実験

5.1.1　実験内容

山崎らはリスクアセスメント情報情報共有システムを用いて以下の検証を行った[5]。

・コマンダと他メンバのリスクアセスメントの差が観測できるか否かの検証

本学 CSIRT 要員を対象に実例インシデント訓練と模擬インシデント訓練（シナリオは先の実例インシデント訓練のシナリオを改変して作成したもの）を実施し、二訓練のリスクアセスメントのログからリスクアセスメントを測定し評価した。

本学 CSIRT 要員のうち 2 名が総務係と、広報係に当たり、以下の図中ではメンバ C、メンバ D と表現している。

5.1.2　実験結果

実例、模擬インシデント訓練から測定したリスクアセスメントのうち、各フェーズにおいて訓練者が挙げているリスク数（以下、リスク列挙数）をグラフ化し図 7、8 に、実例インシデント訓練時のコマンダ、メンバ A のフェーズ 1 のリスクアセスメント入力画面を図 9，10 に示す。

図 7，8 より実例、模擬共に、コマンダ、メンバ A はフェーズ 1 でリスクをいくつか挙げ、フェーズが進むにしたがってリスクの削除を行っている。

他メンバに関してはフェーズ 1 でのリスク列挙が少なく、訓練終了までリスク数が変わらない、または途中で増加している。

フェーズ 1 でリスクを列挙していたコマンダとメンバ A に図 9、10 から一部リスク名には等しい内容のものがあるが優先順位、リスク評価の値が異なっている。

5.2　事前実験の考察

メンバ A はリスクの絞り込みを行えていると考える。だが、コマンダと様子が異なるのはフェーズ 1 におけるリスクアセスメントに大きく差があり、その影響が絞り込み方に違いを生じさせていると考える。

リスクアセスメントに関してコマンダとメンバ A に差が生じたのは部局や立場（知識や経験）の差が影響しているからだと考える。

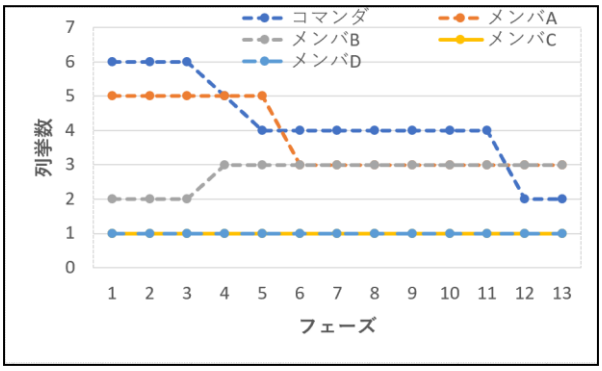

図 7 実例訓練時のリスク列挙数
（文献[13]：図 1 より引用）

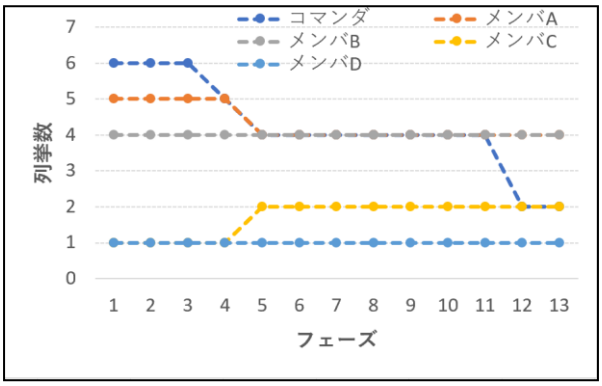

図 8　模擬訓練時のリスク列挙数

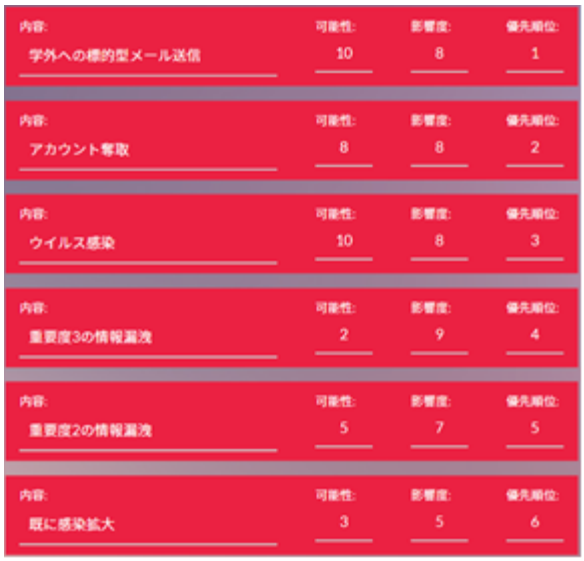

図 9　実例訓練時のコマンダのアセスメント

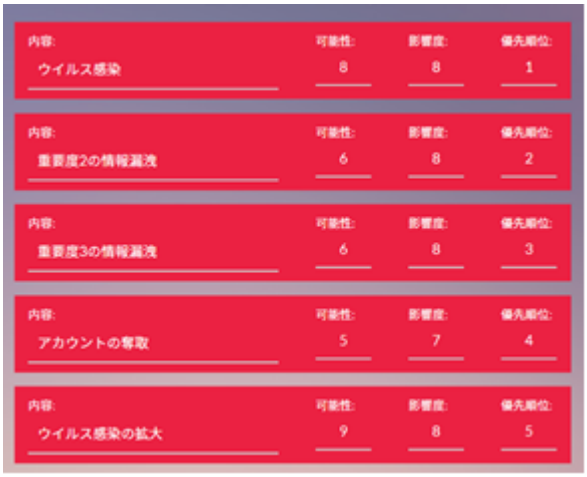

図 10　実例訓練時のメンバ A のアセスメント

他メンバに関してリスク絞り込みを行えていないのは、システムの説明不足や被験者に直接インシデント対応に従事しない総務係や広報係を選出しているのが原因だと考える。

以上のことからコマンダと他メンバでは違いの度合いはメンバによって異なるが、明らかにリスクアセスメントに差があることが分かった。

5.3　事前実験の考察を踏まえて

前節での考察を踏まえ、我々はリスク列挙数のフェーズごとの変化過程、つまりリスク絞り込み過程に着目し、リスク絞り込みはリスクアセスメントの共有によりある程度似通させることができるのではないかと仮説を立てた。

そこでその仮説を確かめる評価実験を行う必要がある。

6　アセスメント共有の評価実験

前章で述べた仮説を確かめるべく、リスクアセスメント情報共有システムを用い、本学 CSIRT を対象に評価実験を予定している。本章では、その実験計画を述べる。なお、実験計画に関してはコマンダとの差を共有（フィードバック）後に、その影響を訓練者からアンケートで得るか、再度訓練を実施し我々が判断するか検討中であり、本稿では後者の案で述べる。

6.1　実験目的

リスクアセスメント情報共有システムを用いて訓練者にコマンダのリスクアセスメントの共有が可能か、またリスクアセスメント共有によりリスク絞り込み過程の様子がコマンダに似てくるか検証するためである。さらに本実験では模擬インシデント訓練の有用性を測るため、模擬インシデント訓練で訓練者が誤った対応を行うことがあるか検証する目的もある。

6.2　実験内容

本実験ではリスクアセスメント情報共有システムを用いて疑似的にインシデントハンドリングにおけるトリアージの訓練（以下、インシデント対応訓練）を実施し以下の検証を行う。

- 訓練者に自らのリスクアセスメントとコマンダのリスクアセスメントをフィードバック（比較・共有）することで、コマンダのリスクアセスメント共有が可能か
- リスクアセスメントが共有可能な場合、共有後にリスク絞り込み過程が似てくるか
- また、リスクアセスメントが共有可能な場合訓練者は巧妙なインシデントへの対応を誤らないか

訓練者によるインシデント対応訓練は以下の手順で実施する。

1. 実験の目的、手順、評価方法等の説明
2. システム利用方法の説明
3. 実例インシデント対応訓練
4. 訓練結果を基に訓練者たちを 2 グループ（グループ A、グループ B）に分割
5. グループ A にフィードバックを提供
6. 模擬インシデント対応訓練

訓練者のリスクアセスメント測定のため、訓練実施後にアセスメント入力内容のログを抽出し評価する。

6.3　実験条件

訓練者は皆本学 CSIRT 要員を用意する。人数については未定である。

実験者は実例インシデント訓練終了後に訓練結果から熟練度を均等に、グループ A､B にわける。2 グループの熟練度を均等にすることでフィードバック有無による比較を容易にするためである。

実例インシデント訓練、模擬インシデント訓練共にフェーズ 1 の訓練画面において実験者が全リスクを挙げておく。これはリスク入力を自由記述にしているため訓練者によってリスクの書き方に違いが出るとみられ、コマンダ、他訓練者との比較に支障をきたすたすためである。

対応選択に関しても実験者が適切な対応をフェーズごとに選択する。対応選択に関しては処置すべきリスクが決まれば実施手順書によって自ずと決まるものであり今回の評価実験に影響を及ぼさないと判断したためである。

模擬インシデント対応訓練では実験者が 1 フェ

ーズの訓練画面にてリスクを入力する際にフェイクのリスクを挙げておく。これは、訓練者が模擬インシデント（巧妙なインシデント）に騙され誤ったリスクを選択した場合を、騙されたと判断するためである。

7　おわりに

本稿では年々巧妙化するインシデントに対してリスクアセスメントに着目し、先行研究である従来のアセスメント共有システムから明らかになっていることから、リスク絞り込みの観点で考察を述べ、新たに解決策を提案した。

リスク絞り込み過程は、スタッフのリスクアセスメント共有によりある程度似通ったものになると考え、リスク絞り込み過程の統一は組織の一貫性の強化に伴うセキュリティ対策の強化に繋がると考える。

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たものである。

参考文献

[1] 独立行政法人情報処理推進機構（IPA）セキュリティセンター、情報セキュリティ 10 大脅威 2019、p.38、IPA、2019、https://www.ipa.go.jp/files/000072668.pdf(アクセス日：2019-09-17)

[2] トレンドマイクロ、トレンドマイクロセキュリティブログ、国内標的型サイバー攻撃の分析：巧妙化と高度化を続ける「気づけない攻撃」、トレンドマイクロ、2019-09-12、https://blog.trendmicro.co.jp/archives/14818.(アクセス日：2019-09-16)

[3] IT ジャーナリスト・三上洋、情報セキュリティコラム「The ANGLE」、第 16 回 手口がさらに巧妙化：進化する標的型攻撃メール、NEC、https://www.nec-solutioninnovators.co.jp/ss/insider/column16.html(アクセス日：2019-09-17)

[4] 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 vol.117 no. 469 ET2017-103、pp. 83- 88、2018.

[5] 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、喜田弘司、林敏浩、今井慈郎、最所圭三、“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”、教育システム情報学会 2018 年度第 5 回研究会 論文集、pp.67-74、2019-01-12.

[6] CSIRT 人材サブワーキンググループ、CSIRT 人材の定義と確保 (Ver1.5)、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 p.6ff、2017.3.13、https://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf(アクセス日：2019-09-16)

[7] 独立行政法人情報処理推進機構（IPA）セキュリティセンター、情報漏洩発生時の対応ポイント集、p.4、2012-09-03、https://www.ipa.go.jp/files/000002224.pdf(アクセス日：2019-09-15)

[8] 米国商務省 長官代理 Rebecca M. Blank、リスクアセスメントの実施の手引き、米国国立標準技術研究所、pp.33-40,2012-09、https://www.ipa.go.jp/files/000025325.pdf(アクセス日：2019-09-17)

[9] トレンドマイクロ株式会社、インシデント対応ボードゲーム （スタンダード版)、2018,https://resources.trendmicro.com/jp-docdownload-thankyou-m057-web-incidentboardgamestandard.html?aliId=283561021

[10] Kaspersky、Kaspersky Interactive Protection Simulation、2018、https://www.Kaspersky.co.jp/about/press-releases/2018_pro18102018(アクセス日：2019-09-17)

[11] 森健人、石井将大、松浦知史、金勇、北口善明、友石正彦、“セキュリティ事案における知見の蓄積・活用を可能とする対応フローの提案と実装”、研究報告インターネットと運用技術（IOT)、2019-IOT-46、2、pp1-8、2019-06-07

[12] 米谷雄介、後藤田中、小野滋己、青木有香、宮崎凌大、八重樫理人、藤本憲市、林敏浩、今井慈郎、最所圭三、“香川大学での標的型攻撃メール訓練の導入と改善点の検討”、学術情報処理研究、22 (2018)、1、pp.54-63、2018-09-18

[13] 新田和也、後藤田中、米谷雄介、小野滋己、青木 有香、八重樫理人、林敏浩、今井慈郎、

喜田弘司、最所圭三、“インシデント対応訓練を通じた CSIRT メンバ間のアセスメント結果の調査“、p.184、電気関係学会四国支部、2019-9-14