インシデントリテラシ向上のための情報セキュリティゲームに導入教育を採用することの検証

廣瀬　司
放送大学
ergate24@gmail.com

藤井　辰雄
放送大学
robitalemon@gmail.com

中谷　多哉子
放送大学
tinakatani@ouj.ac.jp

要旨

近年，個人情報漏えい事件の増加により，情報セキュリティ教育が重要視されている．これまで我々が開発したゲームは，学習者が体験したインシデントを説明するゲームと，インシデントの解決策を手持ちの札から選ぶゲームから構成されていた．しかし，インシデントを説明する際，会話の内容がインシデントに焦点を当てることができずに解決策を選ぶゲームのためのインシデント事例を十分に収集できないという課題があった．この課題を解決するために，一つ目のゲームを行う前に，インシデントの導入教育を行うことにした．本研究は，ゲームの前に情報セキュリティ教育を導入教育として採用することにより，ゲームの有効性が向上したかを検証した．結果，導入教育を行ったことで，知識が増え，ゲームでの話題が情報セキュリティに関するインシデントに焦点が当たったといえる．したがって，インシデントリテラシ向上のための情報セキュリティ教育ゲームに導入教育を採用することは有効であった．

1. はじめに

人に起因する情報セキュリティの事件・事故 [1] は，情報セキュリティの重大課題とされており，情報セキュリティ教育は重要である [2]．企業が行う社員向けの情報セキュリティ教育 [3] には，集合型研修，テキストやメールの配布，ビデオや e-Learning コンテンツの受講などが存在する．これら知識伝達型講義は，組織での情報セキュリティに関する情報共有が可能である一方で，学習者が能動的に参加できない，理解不足などの課題がある．情報セキュリティ教育では各人が内容と対策について深い理解を示すことは重要 [4] である．
情報セキュリティ事象 [5] は情報セキュリティインシデント (以下，インシデント) を内包する,「違反」「不具合」であると定義されている．さらにインシデントは「望ましくない」「予期しない」情報セキュリティを脅かす確率が高いものとされている．

我々は，学習者を主体とする情報セキュリティ教育ゲーム（以下，本ゲーム）を開発し [7]，学習効果があったことを検証した．本ゲームは，学習者によるインシデントを収集する第一ステージと，続けて収集したインシデントを利用して，学習者が解決策を思考し，正解を決める解決策を思考する第二ステージの二つで構成される．

第一ステージでは，インシデントを説明する方法として，情報セキュリティ事象で不安なこと，危険な目にあったことを学習者が発話する「いやな話」ゲームを行う．参加者する学習者は順に前の人より「いやな話」を行い，最も「いやな話」をした人を勝者とする．学習者が自分で，インシデントを発見し，具体的に危険性を説明できることができれば，情報セキュリティ事故を想定できると期待する．
本ゲームは Salen and Zimmerman のいう「マジックサークル」というゲームの場と時間，ゲームに参加するという日常空間からは切り離された安全な空間の中 [8] で行い，その中での制約に従う.「いやな話」ゲームはインシデントの会話ゲームであるが，役割と順番を決めて制度的会話とする.「いやな話」の会話でのルールは，以下のとおりである．

- 話す順番はあらかじめ決めておく

- 全員が 1 話話すことを 1 巡として何回廻ったらゲームを終えるかあらかじめ決めておく，ただし最初の人は前の人が不在という不利な条件を避けるために 2 巡以上廻る
- 学習者の一人が話し手となるとき，周囲は聞き手となる
- 話す内容はインシデントに関する内容とする
- 前の人より「いやな話」をする
- 自分の順の「いやな話」をしないで終える，パスは禁止する
- 周囲が不快になる反社会的話題は禁止する

参加者は「キング　オブ　いやな話」を目指し，前の人よりいっそう「いやな話」をする．勝者を決めるのは，それまでの話と比較することで内容が凡庸になるのを防ぐ，ゲームの進行が滞るのを防ぐ，参加者の気分を盛り上げるためである．同様に,「いやな話」を提供しないのは場が白け るので，会話に参加しない「パス」を認めない．第一ステージで目指す成果はインシデントの話を収集することである．

次に行う第二ステージの「解決の沼」は，インシデントの解決策を思考演習するゲームである．解決策のヒントとなるカードを作成しておいて，ゲームの前に手札として学習者に配っておく．場に置いたインシデントカードをデックから順に引き，そのインシデントにふさわしい解決策を学習者が順番に自分の手札を使って説明していく．その解決策がインシデント解決にふさわしいか否かは他の参加者の話合いで決める， 解決策がふさわしくないと，順の学習者の手札が増えていく．解決策にふさわしいと手札を捨てることができ，手札が減っていく．最初に手札が空になった人，あるいは時間内に手札が一番少ない人が勝者となる．インシデントをカードデックにして学習者自身にどのインシデントが割り振られるかは，カードを引くまでわからない．解決の手札もどの解決策がを手札として得られるかわからない．どのインシデントが学習者自身にふりかかってくるか判明しない状況がインシデントの疑似体験に近しい．ふさわしい解決策を参加者全員の話合いで決めるのは，自分の順番にあたらなかったインシデントについても，全員で情報共有して理解を深めるためである．勝者を決めるのは，ゲームの進行が滞るのを防ぐ，参加者の気分を盛り上げるためである.「解決の沼」でも「パス」を認めない．インシデントについて不明な点は「いやな話」でインシデントの文を提供した人が「解決の沼」に参加しているので，その場で質問をし，疑問を解消できる．第二ステージで目指す成果はインシデントを自分の事として解決策を思考し，他の参加者に説明することで解決策の思考演習を行うことである．

また，本ゲームではゲームを円滑に進行するためにファシリテータを関与させる．ファシリテータの役割はゲームのルールを理解できない学習者に対して，説明をする，さらにインシデントの会話に積極的でない学習者の発話促進を行うためである．また，学習者の話題がルールから逸脱しないよう，ファシリテータが制御する．さらにファシリテータは，学習者だけで決めた解決策の中身が，誤った解決策になるのを防ぐ必要がある．ただし，ゲームの進行や制御のためにファシリテータが学習者の発言を否定したり，会話を遮ったりすると，学習者の主体性を失わせ，ゲームの不活性化を導く可能性がある [9]．本ゲームは学習者主体であることを重視して, ファシリテータは，教師的にふるまわないこととする．

2018 年，我々は本ゲームを実施した実験群と別の情報セキュリティ教育ゲームを実施した統制群との間で，インシデントの解決策について知識の定着の比較を行った．結果，本ゲームの有効性がみとめられた．課題として，第一ステージの「いやな話」で学習者がインシデントの説明に会話の焦点を当てることができなかった．情報セキュリティではなく，学習者の感じている日常の不満や不安に注意を向けてしまった．これにより，次の解決策を選ぶゲームのためのインシデント事例を十分に収集できなかった．この課題を解決するために，本研究において第一ステージのゲームを行う前に，インシデントの知識を増やすために導入教育を採用することにした．

本稿では，ゲームの前に導入教育を採用することによって，情報セキュリティに関するインシデントが収集できたかを検証する．また，インシデントリテラシとは，インシデントを具体的に説明できるようになること，そして，そのインシデントと解決策を関連付けることができることと定義する．

本研究の目的は，学習者がインシデントリテラシを身につけることである．本稿は以下の構成になっている．次の 2 章では，関連研究を述べ，3 章では研究のアプローチを述べ，4 章では，実験内容を述べ，5 章では結果を述べ，6 章では考察を述べる．

2. 先行研究

近年，ゲームを利用した教育についてさまざまな効果がみとめられている．井上 [10] は，ゲームを利用した教育において，学習効果は内発的な動機づけから発生し，能動的な学習態度が期待され，協調学習，学習者中心の学習，学習者同士の意見交換，繰り返し行うことで知識の蓄積がのぞまれると述べた．標葉らは，ゲームを利用した教育で，学習者が問題の解決のために， 多様な視点を獲得するカードゲームを開発し，その効果を測定した [11]．学習者はゲーム内で提示された一見，不可思議な問題に対して解決策の思考演習を行う．その後，ファシリテータが提示した正解を聞いて，学習者 はその内容について続けて議論を行う．標葉らは，学習者が想定し得なかった正解と解決策に，問題に対する多様な考え方を獲得することができると述べた．多角的視点を涵養するために学習者の日常から乖離した問題と正解を用意するため深く議論を重ねることとなった．一方で問題と正解の解決策の説明が困難で学習者の理解が得られず，ファシリテータによるゲームの遂行が困難であるという課題があった．このゲームには，勝敗が存在しないことから，ゲームの終了が判明しにくく，学習者の興味が薄れてしまう場合があった．

矢守ら [12] が開発した，実際に発生した災害事象を題材としたカードゲーム,「防災クロスロード」は正解がない．ジレンマが起きるような災害の場面で，参加者に災害担当者としての役割を与え，あなたなら， Yes/No の二択のどちらを選ぶかを問うゲームである．ゲームで提示される問題は文字数を制限して，学習者の想像力が働くよう，あえて説明を粗にしている．実際の災害現場で様々な体験をした学習者は多様な状況を考慮して，解答の選択を行う．一方，災害事象に詳しくない学習者は，問題を理解しないまま，Yes/No の解答選択を行う．吉川ら [13] は，学習者が勝敗にこだわりすぎて，ゲームに勝つために思考演習に至らないという難点があると述べている．

また，情報セキュリティ教育を題材とした教育ゲームも開発されている．情報セキュリティ教育では，最新のインシデントとその対策を早く周知させる目的を果たすために，開発に多大な時間を費やすことはできない．カードゲームは装置や多大な開発時間がかからないため，手軽な開発手法であるといえる．国内では，情報セキュリティカードゲームとして,「情報モラルかるた (2017 年発表)」 [14] が有る．このゲームは読み札に合わせて，場のとり札を取るかるたの方式である．ゲーム教育を行う前に，導入教育として情報システムを利用した成功例の話をし，ICT 機器活用の負の面への過度な訴求 (危険，怖いなど) を取り除き，楽しく学ぶことを目指している．田中によるとグループで楽しく学習活動の展開ができた，学習者が札の文言を覚えて他人に薦めたいと思うなど教育効果があったとしている．一方で，出題する全ての札はゲームの開発者が考えて提案したものであり，必ずしも学習者の興味をひくものではなかった．学習者が興味を持たない札は，内容を理解しないままであったという課題があった．

3. 研究のアプローチ

3.1. 導入教育

学習者にインシデントの説明をさせるには，学習者自身が体験したインシデントについて考えさせる必要がある．ゲームの前に学習者にインシデントの話題に注意を集められるように情報セキュリティの知識を増やす教育を行う．教育は学習者の周辺にどのようなインシデントが存在するか，発見する手がかりとする．ゲームではインシデントの教育を受けた後に，学習者のインシデント体験が説明される．学習者は自分が話す前までの人のインシデント体験を聞き，それらの内容よりもさらに,「いやな話」をする．参加者が一番共感した話が「キング　オブ　いやな話」に決まり，この話をした学習者がゲームの勝者となる．

図 1 にインシデント会話ゲーム「いやな話」の構成イメージを示す．ゲームでは，教育，いやな話，前の人のいやな話を聞いた上で語られるキングオブいやな話とで，情報提供者とそれぞれの内容の構成要素が異なる．詳細を表 1 に示した．教育はゲームを開始する前に一回だけ行われる．いやな話は　参加者の人数　X　任意の回数行われる.「キング　オブ　いやな話」は全ての「いやな話」が終わったのちに，参加者の共感を最も得たインシデント体験として存在する．

3.2. 導入教育の選択

導入教育は，学習者自身が直面するインシデントについて考えさせるために，身近な話題である必要がある．2017 年の時点で，日本国内の情報通信機器の世帯保有

図 1. インシデント会話ゲームの構造イメージ

表 1. インシデント会話ゲーム「いやな話」の構成要素

内容	情報提供者	構成要素
教育	ファシリテータ	導入教育
いやな話	学習者	教育で知識を得た上で会話するインシデント体験
キングオブいやな話	学習者全員	周囲の人のインシデントの知識を得た上で参加者の共感を最も得たインシデント体験

率はスマートフォンがパソコンを上回り [15]，スマートフォンは身近な通信機器として普及している．スマートフォンには，経済産業省のキャッシュレス化の推進 [16] により，携帯電話決済機能や送金機能が追加された．2019 年の 11 月期に行われた電子決済には 349 万台のスマートフォンが使用され，2018 年 12 月には 273 万台であったことから 76 万台の増加があり [17]，スマートフォン決済が増加したことがわかる．またショートメッセージサービス (以下，SMS とする) 機能は，スマートフォンの基本機能であり，携帯電話会社からスマートフォン契約者への料金案内などに利用されている．この SMS を利用したフィッシング詐欺 (以下，スミッシング) は図 2 に示したように，増加 [18] 傾向にある．導入教育は，近年，スマートフォンの利用者が増加し，スマートフォンの決済機能などをねらった詐欺事件が増加していることから，学習者に起こりうるインシデント導入教育として，スミッシング防止対策を選択する．本研究では，スミッシングの内容をまとめたものを教材として開発した．

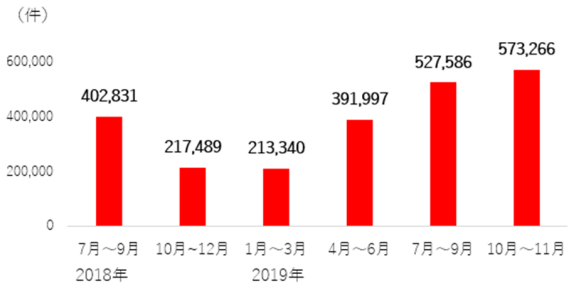

図 2. 不正サイトへ誘導された国内モバイル利用者数推移

3.3. 導入教育の内容

導入教育の目的はスミッシングの仕組みと概要を知り，インシデントの知識を増やすこととする．

教育対象は，スマートフォンを所有し，SMS を見る機会がある人とする．学習目標は，教育を受けた受講者がスミッシングの概要と内容を説明できるようになることとする．教育の方法は，パワーポイントを使ってファシリテータが説明する．時間は 15 分程度とする．内容 1 として，スミッシングの概要を知る スミッシングの仕組と被害増加の要因を説明する．内容 2 として，スミッシングメッセージの確認方法を説明する．また，スミッシングの対策法として，教育後，受講生が最新情報を得ることができる関連情報サイトを紹介し，継続的な情報収集を行えるよう配慮した．

3.4. 共起ネットワーク図による分析

情報セキュリティの導入教育を行い，その後ゲームを利用して収集したインシデントの文と，過去にゲーム前に導入教育を行わなかった実験で収集したときのインシデントの文を比較する．インシデントの文の特徴を分析するために，どのような単語が同時に出現しているか，単語同士にまとまりがあるかを感覚的にとらえるために，テキストマイニングツール KH Coder3 を使って共

起ネットワーク図を描いて分析する．
次に共起ネットワーク図の中から，まとまりの数と，単語の出現回数，まとまりの中で中心性が高いものを重要な役割を果たしている単語とし，単語が実際にどのように使われているか確認する．単語が，情報セキュリティに関係する単語であれば，ゲームで集めたインシデントは適切であったとする．本研究では，インシデントの文を収集する際の会話分析は行わない．学習者が発話したゲームのインシデントをファシリテータが，その場で要約し,「こういった内容ですね」と学習者に確認したものを，テキストデータ化し，導入教育の有無の別に分け分析する．

4. 実験

4.1. 実験の流れと概要

情報セキュリティ導入教育による教育を行い，その後にゲームを実施した．導入教育のテーマは，スマートフォンのスミッシングについて取り上げた．
また，実験を円滑にすすめるために，実験者がファシリテータとなり，導入教育の説明を行い，ゲームをすすめる役割を担った．実験は，参加者に特定の条件（年齢，職業，性別など）を付けなかった．導入教育がスミッシングであることから，携帯電話を持っている人を対象とした．
参加者を実験者の職場の会議室に集合させ，実験内容を説明し，参加を呼びかけた．参加人数に制限を設けず，実験に協力してくれる有志を集めた．参加者には，事前に実験の主旨を説明し，自由意志でいつでも参加を中止できることを伝えた．この条件で参加者を募集したところ，職員他 4 人が参加者となった．4 人の年齢は 30 代，40 代，50 代，60 代であった．最初に導入教育でスミッシング防止対策の教育を行い，次に学習者主体によるインシデントの収集ゲーム「いやな話」を 2 巡行った．参加者が勝者である「キング・オブ・いやな話」を決め，ファシリテータが「いやな話」の内容を「こういうことですね」と発話者に確認してテキストデータにして終えた．
実験日時 : 2020 年 1 月 20 日休憩時間を利用して，15 時から実施
場所：実験者の職場会議室
実験に要した時間 : パワーポイントとスクリーンを利用して導入教育に 15 分，インシデント文収集に 20 分間要し，8 文集まった．

4.2. 導入教育無の場合との比較

過去に実施した本ゲームの実験時に収集したインシデントの文と，今回のインシデントの文の比較を行った．

5. 結果

5.1. 導入教育無ゲームで収集したインシデントの文

過去に実施した本ゲームの実験は，2018 年 2 月 1 日，2 月 5 日，5 月 11 日の 3 回であった．実験参加者はそれぞれ 3 名ずつであった．この際に参加者に特定の条件（年齢，職業，性別など）を付けなかったが，参加者は実験者の職場の職員と放送大学のクラブ活動参加者であった．参加者の内容は，本稿の実験メンバーとは重複していなかった．毎回,「いやな話」をそれぞれ 2 巡ずつ行い，インシデントの文は 18 文集まった．過去 3 回実施した本ゲームで収集したインシデントの文を導入教育無データとしてまとめた．18 文のうち単語の総出現回数は 587 回，異なり単語数は 209 個であった．
この導入教育無データを共起ネットワーク図にしてを描画した．図 3 に示す．共起ネットワークを描く条件と

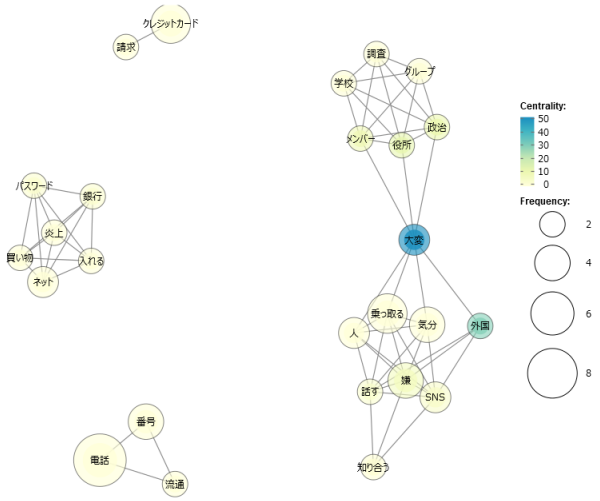

図 3. 導入教育無ゲームで収集した情報セキュリティインシデント文の共起ネットワーク

して，全ての単語を網羅すると，出現単語が多すぎて，描画が複雑になり特徴を捉えることが難しくなる．そこで単語の出現回数は 3 回以上に設定した．単語の出現回数の多さは円の大きさに比例する．また，円と円との関係が強いところは線の太さで表現した．共起ネットワークの中で単語が中心的な役割を果たす中心性（centrality）の度合いが強い単語は濃い色で示した．
出現回数の多いものは（以降，単語としてあらわすときは，わかりやすくするために『』で囲む）『電話』,『クレジットカード』,『乗っ取る』であった．

まとまりは 4 つあり，それぞれが結びつきのないものであった．大きなまとまりは,『大変』を軸にして，2 個のまとまりを 1 つにした形であった．この大きなまとまりは，それぞれ，役所，政治，学校などを結ぶまとまりと，外国，乗っ取る，気分，嫌，SNS，などを結ぶまとまりからできている．他には，クレジットカード，電話，炎上などを囲む小さなまとまりが存在する．

中心性の強いものは,『大変』が強度 50，次いで『外国』30，次が『役所』『政治』20 であった．文脈の中では中心性の強い『大変』は調査，隠す，ハラスメント，外交，政治,『外国』は飛行機，降ろす，日本人，目的,『役所』はマスコミ，不愉快，学校，忖度，乗っ取り,『政治』は人，言う，忖度，学校，大変という単語とともによく出現していた．
統制群で出現したインシデントは，政治やマスコミに対する不満，SNS を介した人付き合いが嫌になる話など情報セキュリティとは関係ない内容があった．

5.2. 導入教育有ゲームで収集した情報セキュリティインシデントの文

次に本研究で行った実験で収集した導入教育有データで共起ネットワークの描画を行った．本研究では 4 人が参加し,「いやな話」ゲームを 2 巡行い，集まった情報セキュリティインシデントの文は 8 つであった．単語の総出現回数は 351 回，異なり単語数は 129 個であった．

この導入教育有データを共起ネットワーク図にしてを描画した．図 4 に示す．出現回数の多いものは『電話』,『クレジットカード』,『インターネット』であった．まとまりはおよそ 3 つあり，全て複数の結びつきがあった．単語『サイト』を中心にして『特定』を経て『攻撃』や『メール』に繋ぐ関係と,『詐欺』を経て『クレジットカード』に繋ぐ関係と『買い物』から『電話』を経て『プログラム』に至る関係が結ばれていた．全てのまとまりは何らかの関係でつながっていた．中心性の強さを表す指標の高いものは,『サイト』が一番強い 50，次いで『クレジットカード』40，次が『攻撃』『メール』『プログラム』30 であった．文脈の中では中心性の強い『サイト』は詐欺，SSH，海外，買い物，攻撃,『クレジットカード』は，ない，使う，決済，情報，買い物,『攻撃』は，SSH，受ける，ズレ，サイト，個人,『メール』はアドレス，経由，電子，ウィルス，パソコン,『プログラム』は，ブロック，仕込む，削除，ハッカという単語がよく出現していた．
実験群で説明されたインシデントは，サーバがゼロディ攻撃に合い，苦労して復旧した話，インターネットで買い物をした際のトラブルなど情報セキュリティに関する話があった．
また，スミッシング詐欺被害防止導入教育の利用にあたり，スミッシング被害体験の有無を学習者にたずねたが，全員，スミッシング被害体験が無かった．

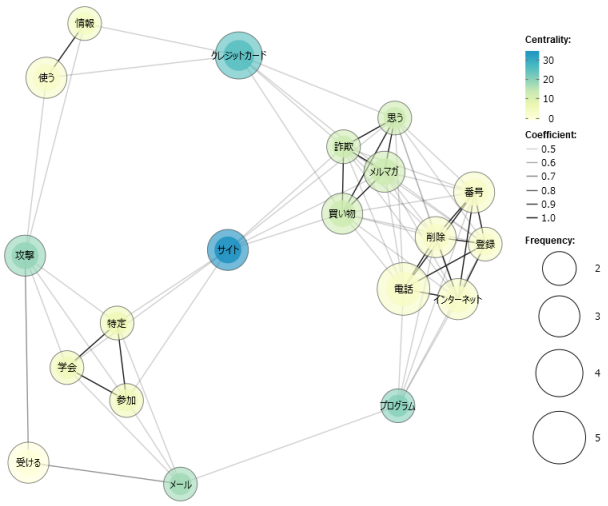

図 4. 導入教育有ゲームで収集した情報セキュリティインシデント文の共起ネットワーク

6. 考察

インシデントの文の中の単語の出現回数について比較すると，導入教育無ゲームでも，導入教育有ゲームでも，『電話』が 1 番出現回数が多かった．近年，電話はほとんど携帯電話を指し，携帯電話はほとんどコンピュータの機能を搭載している．学習者の最も身近なコンピュー

タであるという見方をすると,『電話』はコンピュータの代名詞であるともいえる．次いで,『クレジットカード』であった．クレジットカードが経済的被害を及ぼすという意味で上位に挙がったと考えられる．今後，携帯電話の決済機能の利用増加があると，さらに『電話』『クレジットカード』の出現割合が上昇する可能性がある．3 番目に出現回数の多い単語は，導入教育無ゲームでは『乗っ取る』であった．乗っ取るは気分，マスコミ，人格，社会，役所といった単語とともに文脈に出現し，情報セキュリティ関連としての『乗っ取る』とは異なる意味で使われている．導入教育無ゲームのインシデントの文が情報セキュリティの話題でないものが含まれていることがわかる．導入教育有ゲームで 3 番目に出現回数が多かった単語は『インターネット』であった．導入教育有ゲームのインシデントの文は情報セキュリティの話題が多かったことがわかる．

共起ネットワーク図のまとまりを比較したところ，導入教育無ゲームでは，4 つのまとまりに分かれていたが,．まとまりの間に関連はない，導入教育有ゲームでは，まとまりは 3 つであるが全てのまとまりに関連があった．導入教育無ゲームより，導入教育有ゲームのほうが，インシデントの文の単語に共通性があった．インシデントの文における単語の重要な役割をはたす中心性の強さでは，導入教育無ゲームで，最も中心性のある単語が『大変』である.『大変』の意味からインシデントが学習者にとって「はなはだしい程度」であり,「一大事件」であることを示している．周囲には,『外国』,『役所』,『政治』があり，これらの出現する文脈では，政治や外交，マスコミや不愉快，学校や忖度などの単語がよく出現し，政府やマスコミに対する不満，人付き合いへの嫌悪感などが話された．これは必ずしも情報セキュリティに関する話題でないことがわかる.「いやな話」のルールとして,「いやな話」をするという部分は作用していたといえるが,インシデントに関する内容というルールは守られていなかったといえる．実際には学習者はインシデントの話といっても何を言っていいかわからないことがある．誰かが話題を身の回りの不満や不安の話に変えると，それに引きずられる傾向にあった．ファシリテータがインシデント以外の話題への変化に気づき，学習者の気分を損ねないように制御することが求められるところである．しかし．ファシリテータの力量のみに頼るのは難しい．

導入教育有ゲームでは，最も中心性のある単語は『サイト』であった.『サイト』は「Web サイト」であり，以下,『クレジットカード』,『攻撃』,『メール』,『プログラム』と続く．これらの出現する文脈では，SSH や攻撃，買い物や詐欺，ウィルスやブロックなどの単語がよく出現し，情報セキュリティに関することが話された．これは,「いやな話」をする前に導入教育を行ったことで，話題が情報セキュリティに関するインシデントにまとまったといえる．学習者は何を言っていいかわからないという混乱もなく，遅滞なくインシデントの説明を行えた．したがって，インシデントリテラシ向上のための情報セキュリティ教育ゲームに導入教育を採用することを検証した結果，有効であったといえる．

しかしながら，導入教育がインシデント収集に影響を与えるならば，収集したインシデントはスミッシング被害と一致するはずである．実験に参加した学習者全員にスミッシング被害体験が無かったことに関連があるかは不明である．次に本ゲームを行う際には，学習者に関連のある別の導入教育を用意して効果を確認する必要がある．また，本稿では，インシデント収集の際の課題解決に導入教育を採用することを検証したが，導入教育が，今後,「解決の沼」解決策思考演習においてどのような影響があるかを検証する必要がある．さらに本研究を一般化するにあたり，異なる状況設定，異なる参加者を設定し，実験を行う必要がある．今後は実験を整備し，他集団において実験することが必要である．

参考文献

[1] 独立行政法人情報処理推進機構. 情報セキュリティ１０大脅威　2018, 2018.

[2] JNSA(日本ネットワークセキュリティ協会). 2015 年情報セキュリティインシデントに関する調査報告書個人情報編, 2016.

[3] 株式会社日本シュレッダーサービス. 情報セキュリティに対しての教育, 2018.

[4] 日本工業規格. JIS Q 27002:2014 情報セキュリティマネジメントの実践のための規範, 2014.

[5] 日本工業規格. JIS Q 27000:2014 情報セキュリティマネジメントシステム-用語, 2014.

[6] 藤本徹. 効果的なデジタルゲーム利用教育のための考え方. コンピュータ & エデュケーション, Vol. 31, pp. 10–15, 2011.

[7] 廣瀬司, 中谷多哉子. 情報セキュリティ教育のためのカードゲームの検証. 研究報告ソフトウェア工学 (SE), Vol. 2018, No. 21, pp. 1–7, 2018.

[8] Katie Salen Tekinbas and Eric Zimmerman. *Rules of Play Game Design Fundamentals (The MIT Press)*. The MIT Press, new edition, 9 2003.

[9] 堀公俊. ファシリテーション入門. 日本経済新聞社, 7 2004.

[10] 井上明人. ゲーミフィケーション - ゲームがビジネスを変える. NHK 出版, 1 2012.

[11] 標葉靖子, 江間有沙, 福山佑樹. 科学技術と社会への多角的視点を涵養するためのカードゲーム教材の開発. 科学教育研究, Vol. 41, No. 2, pp. 161–169, 2017.

[12] 矢守克也. 巨大災害のリスク・コミュニケーション: 災害情報の新しいかたち. ミネルヴァ書房, 9 2013.

[13] 吉川肇子, 矢守克也, 杉浦淳吉, 主著に, リスク・コミュニケーション, 福村出版, 京都大学大, 生活, 防災. クロスロード・ネクスト. 続: ゲームで学ぶリスク・コミュニケーション-. ナカニシヤ出版, 223pp, 2009.

[14] 田中康平. 「情報モラルかるた」を活用した、楽しく学ぶ情報モラル・情報セキュリティ. 第 43 回全日本教育工学研究協議会全国大会, pp. 229–232, 2017.

[15] 総務省. 平成 30 年版情報通信白書, 2019.

[16] 経済産業省. キャッシュレスビジョン, 2018.

[17] 日本銀行. 決済動向 2019 年, 2020.

[18] 独立行政法人情報処理推進機構. 情報セキュリティ 10 大脅威 2019, 2019.