Vol.2018-SE-199 No.21
2018/7/19

情報セキュリティ教育のためのカードゲームの検証

廣瀬司[†1]　中谷多哉子[†1]

概要：情報セキュリティ教育において，セキュリティ教材の開発者と学習者の間には，時間的あるいは立場的に差があり，教材の内容が実践の場で活用されていないことが現状の課題である．我々は情報セキュリティ教育では，学習者が問題を自身に置きかえ，能動的に活動に関与することが，教育の効果を上げると考える．このことにより，学習者の身近な情報セキュリティの事象を自身の発話によって収集し，自身がその解決策の思考演習を行うことで教育の効果がのぞめる手法として，ゲームを用いた教材を開発した．本研究では，発話ゲームと解決策の思考演習ができるカードゲームの組み合わせによって，その効果を確認することとした．ゲーム終了後，学習の内容を想起できる度合いにより，その有効性を検証したところ，ゲームにより獲得した情報セキュリティの知識であるのか，学習者個人の既知の知識であるかの判別がつかなかった．また，ゲームを適切に誘導すべくファシリテータを設定してゲームを進めたが，ファシリテータによる学習者の制御が上手くいかなかった．今後の課題として，有効性検証実験の見直しと，ファシリテータの役目について検討していくこととする．

キーワード：情報セキュリティ教育，カードゲーム，ゲーム教育，解決策の思考演習，発話による情報収集

The Card Game for Information Security Education

TSUKASA HIROSE[†1]　and　TAKAKO NAKATANI[†1]

Abstract: In the Information Security Education, there is a temporal and standpoint difference between developers of Learning Contents .It is a problem that the Learned Contents are not utilized in the real world. We believe that it is effective for Learners to think about problems themselves and Learners to do activities. By doing this, we created a Card Game where Learners gather by talking about familiar events of Learners, and Learners doing training to think about the solution. In this research, we aim to confirm the effect of education by using a combination of conversation game and card game which can train solution. After the game, the effectiveness was verified by the number of times of remembering the content of learning.
However, it was not possible to distinguish whether it is knowledge of information security obtained by the game or known knowledge of the learner. Also, I set a mediator to properly guide the game and recommended the game, but the Facilitator 's game control did not go well. As a future task, I would like to review the way of experiments to prove that the game is effective and think about the role of mediator.

Keywords:
InformationSecurityEducation,CardGame,GameEducation,Trainingonsolution,InformationGatheringbyConversation

1. はじめに

独立行政法人情報処理推進機構（以下，IPA）の「情報セキュリティ 10 大脅威 2017」 [1]では，人に起因する情報セキュリティ事象 [2]がランクの上位に挙がっている．人為的なミスや過失など，人に起因する情報セキュリティの問題は 2010 年 [3]から，情報セキュリティの重大課題として繰り返し警告されている．

この対策として JIS 規格(JIS Q 27002:2014)では，利用者への実践的な情報セキュリティ教育を推奨 [4]している．情報セキュリティ教育は単純な知識だけではなく，議論などを行うこと [4]で学習者にセキュリティに対して理解を高めることが求められる．

企業が行う社員向けの情報セキュリティ教育の形式 [5]には，集合型研修，テキストの配布，ミーティング，e-Learning，ビデオの視聴，メール配布，社外講師による研修などが存在する．集合型研修，テキストの配布，メール配布では情報セキュリティ事象・解決策について，一度に大人数での情報共有，意識付けが行われる利点がある．一方で情報セキュリティ事象・解決策について聞く・読むだけでは内容を簡単には理解できない，聞いていない，読んでいないなどの問題がある．また，ミーティングでは情報セキュリティ事象・解決策について，問題の洗い出しを行えるが，上司や一部の人しか発言しない，聞いていないなどの問題がある．e-Learning は社員個人の都合のよいタイミングで学習できる利点があるが，各自が勝手に行う，情報共有できないなどの問題がある．

上記情報セキュリティ教育ではミーティングを除いて知識伝達型講義を聞くという受動的学習であり，知識の取りこぼし，学習者が理解していないなどの問題が懸念され

†1 放送大学
The Open University of Japan

る．情報セキュリティ教育では，学習者に深い理解を促すために，学習者が能動的に活動に関与する [6]ことが必要である．

このような知識を得ることができる手法 [7]として，ゲームを活用した学習が近年，注目を集めている．

井上(2012)によるとゲームを利用した学習に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などさまざまな効果がみとめられる [8]. 一方で松本(2014)によるとゲーム学習の問題点として全ての学習者に有効であるとはいえない[9]という報告もされている．標葉ら(2017)の開発した科学技術と社会への多角的視点を涵養するカードゲーム [10]では，学習者が協力して問題を解き明かす活動を通じて新しい知識や視点の獲得に成功する利点があった．

しかしながら，開発者の用意した問いに対する正解に学習者が納得いかない，学習者が問いの要点を理解するのが困難である，用意した正解の解説が難解で進行役が負担であったという問題があり，ゲームをすすめるのが難しいとされている．

このことから，本研究の目的は，情報セキュリティ教育を手軽に実践できるゲームを開発し，学習者自身のこととして問題と解決策を理解し，実際に情報セキュリティの事象に直面したときに教育で学んだ成果を活用することを期待する．

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 章では本研究のアプローチを述べ, 4 章でゲーム方法を述べ, 5 章では実験結果を述べ, 6 章では考察を述べる．

2. 関連研究

(1) 情報セキュリティ教育におけるカードゲーム教材の概要

情報セキュリティ教育を手軽に実践できるという視点から，日本国内における情報セキュリティ教育のうちカードゲームを取り入れたものとして，JNSA の人狼ゲーム（2017 年 1 月発表） [11]，トレンドマイクロ社のインシデント対応ボードゲーム（2018 年 2 月発表） [12]，イーパーツのセキュろく（2013 年 1 月発表） [13]がある．

人狼ゲームは学習者の会話による心理戦であるが，情報セキュリティの事象は発表された当時のものである．

インシデント対応ボードゲームはイベントに対してチームで相談して対策を立てるものである．提示される情報セキュリティの事象はシステム管理者向けであるため，そうでない学習者には仕組みの説明，学習者の理解を得るためには身近な事象への置き換え，初学者でも興味を持つ解説が必要である．

セキュろくはすごろくであり，１問１答方式であるため，問題が理解できなければ解答を得ることが困難である．

いずれもゲーム内の問いとして提示される情報セキュリティ事象はゲーム開発時のものであり，学習者との間に時間差，意識差を生じる可能性があり，理解できないという結果になりうる．

(2) 本研究が取組む未解決の問題

従来のゲームを用いた教材では，開発者と学習者の置かれた立場に時間的，状況的に差があることで開発者が意図した正解を学習者が納得できないという問題が生じている．

実社会で発生している情報セキュリティ事象のゲーム教材への取り込みはゲーム制作時に行われ，発表，学習および実際に学習者が直面するセキュリティ事象の変化に対応できていない．

また，ゲーム開発者は学習者の立場や視点を開発時に充分取り込むことが困難なため，実際に起こりうるセキュリティ事象を想定できない可能性が高い．

多少のカスタマイズ用の追加カード等が用意されているゲームも存在するが, 一様にゲーム開発者側で正解を用意し，それを学習者が覚える形でゲームが進行していく．

このようなゲームでは，学習者の学習態度が能動的に変容し，意欲的にゲームに取り組んだとしても，固定的な情報セキュリティ事象と開発時に想定された，それに対応する解決策の知識しか得られないこととなる．学習者は実際に起こるさまざまな事象に対応できないといえる．

3. 研究のアプローチ

認知心理学において自身の経験した事象に関する記憶は, 一度しか学習の機会がなかったとしても,「エピソード記憶」となり，時空間的文脈とともに想起したという意識が持てることが特徴 [14]である．このことから，情報セキュリティの事象と解決策についても，自身の体験を伴うことがより長期の記憶を持ち，想起しやすくなることが考えられる．

しかしながら，情報セキュリティの事象と解決策を実体験させることは困難である．ここでは，疑似体験として，学習者自身が身近な情報セキュリティの事象を発話すること，他者の発話を注意深く聞くこと，後にその解決策を自身のこととして話し合いにより解決していく演習を行う．後にこの体験は「エピソード記憶」として実際に情報セキュリティの事象に直面した際に, 自身のこととして想起し，適切な解決策の選択を可能にする．

このことが情報セキュリティ教育に有効である．

(1) カードゲームの構成方法

学習者が情報セキュリティに対する関心を高めるためには，ゲームのテーマは身近である必要がある．最新の情報セキュリティの事象動向から開発者がテーマを取上げても，学習するまでに情報や知識の陳腐化，学習者の立場との相違が考えられる．情報セキュリティの事象は学習者が所属す

る組織，個人の利用するサービス [15]，コミュニティ，文化の中で発生するものである．

本研究で開発するゲームは学習者自身の身近な情報セキュリティの事象を取上げる．学習者自身が発話し，問題提起することは，今，その学習者が正に考える情報セキュリティの事象そのものをテーマに取上げてゲームが進行していくもので，都度，学習者にとって最も重要な問題である．この学習者自身が提起した，情報セキュリティイベントをプレイ参加者全員でカードゲームを通じて，話し合い解決することにより，学習者自身のこととして適切な解決策を選択していく．また，学習者同士が話し合って，新たな対策を考案した場合は追加可能にしておくことが必要である．このことから，本研究で開発するゲームは情報セキュリティの事象を学習者自身の発話で収集し，後にカードゲームにおいてその解決策を検討する 2 段階の形とした．

(2) ゲームの有効性の評価方法

開発したカードゲームで学習した後に，学習者自身が発話した情報セキュリティの事象に対する解決策を選択できることは，エピソード記憶として情報セキュリティの事象と解決策を一連の出来事を想起できることを示す．このことは実践の場において学習者が置かれた状況，立場に応じて適切な解決策を選択できることとなり，情報セキュリティ教育が有効であったことを示す．

この有効性を評価するために，開発したカードゲームで学習したとき，ゲーム内で出現した情報セキュリティの事象に対する解決策の内容を後日，アンケートに記述させ，想起できるかを確認する．

また，比較するために，開発したカードゲームとは異なる従来のカードゲームを行った後の解決策の内容を後日，アンケートに記述させ，想起できるかを確認する．

図 1 情報セキュリティ教育のカードゲームと従来のゲームを比較する実験の流れに概要を示す．

開発したカードゲームで学習する群を実験群とし，従来のゲームを行う群を統制群とする．既存のゲームはトレンドマイクロ社のセキュリティインシデント対応ボードゲームとする．双方を比較する実験の流れは，実験群では情報セキュリティの事象収集ゲームと解決策の思考演習を実施する．

統制群では，これらのゲームを行わない代わりに既存のカードゲームを行う．実験群の解決策の思考演習ゲームでは，既存のゲームの解決策カードを用いて，解決策の思考の糸口とする．後日ゲーム内で提示した問いの解決策として想起されるものをアンケートで問う．

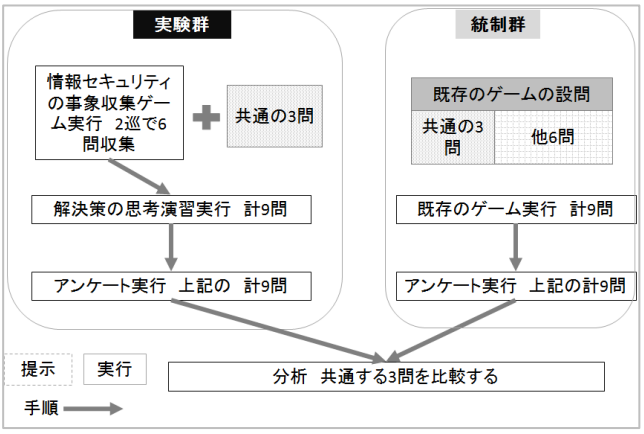

図 1 情報セキュリティ教育のカードゲームと従来のゲームを比較する実験の流れ

開発したカードゲームでの学習は，学習者の発話による情報セキュリティの事象の提示，学習者の話し合いによる解決策の選択・提示が行われ，結果，エピソード記憶として記憶されることが期待される．

従来のゲームでの学習は，ゲーム開発者による，開発当時の情報セキュリティの事象の提示，ゲーム開発者による，開発当時の解決策の選択・提示がなされ，結果，後日想起されるものはゲーム時の固定的な知識として記憶されることが考えられる．

アンケートで提示する情報セキュリティの事象は，問いの内容による差異が出ないよう，同じ内容とする．このため，情報セキュリティの事象収集を行うグループでは，学習者の発話によらない情報セキュリティの事象を話し合いの解決の中で選択することになるが，そうでないグループもまた，意図した内容ではないため，特に問題があるとはいえない．

また，アンケートの回答は偶然の選択によりまぐれ当たりの出ないよう，選択式ではなく，記述式とする．

アンケートの回答は，ゲームの中で出現した解決策の内容の文言が記載されていた場合に出現回数を 1 回ずつ加算することで，情報セキュリティの事象に対する解決策を想起できたかを出現回数で比較することとした．

4. ゲーム方法

(1) 発話による情報セキュリティ事象の収集

セキュリティ教育の問いを学習者にとってより実践的で身近な事象にするために，情報セキュリティ事例収集としての準備段階のゲーム，”いやな話”ゲームを開発した．

“いやな話”は最低 2 人からできる会話ゲームである．発話を中心とするゲームなので，参加者数の制限は無く，時間，場所を選ばない．ルールは前の人より”いやな話”をすることである．話しの内容は，実話・創作を問わない．最初に話す順番を決め，1 番から順に”いやな話”をする．

ファシリテータは最初にこのゲームで使う情報セキュリテ

ィの話の「種」を決め，最低でも 1 巡目は，「種」に沿った内容でゲームが進行するようにコントロールする．「種」は後のカードゲームで利用する既存の情報セキュリティ事象の中から選択する（例：情報セキュリティの脅威としての『乗っ取り』）．

順番の 1 番は前の人が不在という条件を避けるため，全体で話しを 2 巡以上行う．一定の巡回を終えたところで，学習者全員で話しあい，一番”いやな話”を決める．話しあいの際には，学習者はいやな話の内容の不明な点について，当該のいやな話の発話者に自由に質問ができる．このことにより，後にカードゲームの問いとして利用する際に理解の度合いを深めておくことが可能になる．

一番”いやな話”を提供した人を”キングまたはクイーン オブ いやな話” として拍手をして讃える．”キングまたはクイーン”を決めるのは，話しの内容が凡庸になり，ゲームの進行が滞るのを防ぐためである．同様に，自分の順番になっても学習者が”いやな話”を提供しないのはゲームが滞るので「パス」を認めない．

ファシリテータは“いやな話”ゲームが終了したところで，収集した情報セキュリティ事象の概要をいやな話の札の裏側に記す．参加者全員はゲームの話しの内容が参加者に対する攻撃やハラースメントにならないよう注意をはらうこととする．

(2) 解決策の思考演習

学習者自身の発話による情報セキュリティ事象と「種」に関連する既存の情報セキュリティ事象を問いとして，解決策を参加者が議論するカードゲーム”解決の沼”を行う．

参加者は最低 2 人からカード枚数に応じてゲームを行える．場には“いやな話”ゲームで収集した事例と既存の情報セキュリティの事象を束ねていやな話デック（カードを積んだ山），既存の解決策が記載された解決カードのふた山をデックとして用意する．ゲームを始める前に学習者の順番を決め，解決カードを手札として適当な枚数配布しておく．

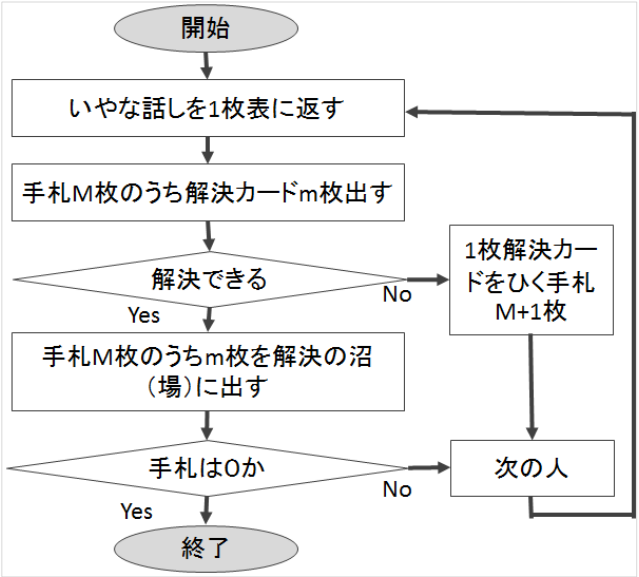

図 2 解決の沼カードゲームの流れ

図 1 解決の沼カードゲームの流れに示すように，学習者は最初に”いやな話”デックから 1 枚ひき，表に返す．

内容を見て，学習者は解決する策としてふさわしい解決策を手札から選び，解決の沼（場）に出す．参加者全員で解決の沼にある策がふさわしいか否かを判断し，ふさわしくない場合には手札を学習者に回収させ，”いやな話”カードに書いてある枚数の解決カードをデックから引かせる．

ふさわしい解決策であれば，学習者は無事に手札を減らすことができる．

この際にファシリテータは既存の情報セキュリティ事象であれば，用意された既存の解決策とその理由を解説し，学習者の理解を確認する．ファシリテータは”いやな話”で収集された内容であっても，適切な解決策となるようにゲームの流れをコントロールする必要がある．

参加者全員が協議した結果，既存の解決カードが不十分であればその場で解決カードを追加するなどの対応も必要である．次の学習者は次の”いやな話”カードのデックから 1 枚，表に返し，ゲームを続ける．

ゲーム終了は解決カード手札が無くなる学習者が出現するか，制限時間に到達した場合とする．制限時間に到達したときに解決カード手札が一番少ない学習者を勝者とする．

最後に解決の沼に置いた情報セキュリティ事象とその解決策のカードの組み合わせについて学習者から質問などがあればファシリテータが解説する．

(3) ファシリテータの役割

情報セキュリティの事象を収集する際に，学習者による全く自由な発話であると，情報セキュリティに関連する話題から逸脱する怖れ，会話が続かないなどの問題がある．また，今回の”いやな話”の核となる「種」となる話題の提供と説明，ゲームの主旨を学習者に理解してもらうことが必要である．そのために，“いやな話”では，ゲームの熟達者，あるいは情報セキュリティ関連の知識が豊富である，ファ

シリテータの存在が必要である．
解決策の思考演習である”解決の沼”におけるファシリテータの役割は学習者の話し合いの結果，安易な解決策に終結しないよう適切な解決策への誘導と，IPA などで推奨される最新動向の解決策 [6]を学習者が理解できるよう説明することである．
ファシリテータは学習者の能動的な意欲を引き出しつつ，同時にゲームのコントロールと情報セキュリティ教育として目指す適切な解決策への誘導をすることがのぞまれる．

5. 実験結果

(1) 実験の概要

2018 年 5 月に放送大学学生を対象に情報セキュリティ教育の有効性を検証するという目的で実験を行った．対象となる学生には事前に実験の主旨，実験に係る時間，場所を告知し，任意で参加者を募り，実験を行った．参加者の事前の情報セキュリティにおける知識は特に確認していない．
実験は，統制群としてセキュリティインシデント対策ボードゲームを行う A グループ　3 人と実験群として“いやな話”と“解決の沼”ゲームを行う B グループ 3 人で行った．
A グループは解決策を決定するルールを記載したカードブックを参照してゲームを進めた．提示した情報セキュリティの事象は，セキュリティインシデント対応ボードゲームで用意された深刻度，影響度が高い赤のカード 9 種類（青のカードは深刻度，影響度が低いものとして用意されているが今回は使用しない）であった．解決策カードは同様にセキュリティインシデント対応ボードゲームのものを使用した．
B グループはファシリテータが“いやな話”の「種」として情報セキュリティの脅威としての『乗っ取り』を話題として提供した．これは，学習者が学生で，メールの乗っ取り，SNS の乗っ取りなど，身近な情報セキュリティの事象としてイメージし易い問題であるとファシリテータが想定したからである．
1 巡目はこれに沿った内容で，また，2 巡目は特に制御なく，学習者の発話したい内容でゲームをすすめ，6 話の”いやな話”を収集した．また，B グループの“解決の沼”では，収集した 6 話の”いやな話”とセキュリティインシデント対応ボードゲームで用意された深刻度，影響度が高い赤のカードのうち，セキュリティの脅威としての『乗っ取り』に関するものを取扱う 3 問の設問の合計 9 種類を提示し，適切な対策の選択と赤のカード 3 問について解決策の話合いとファシリテータの解説による学習を行った．
解決策カードは同様にセキュリティインシデント対応ボードゲームのものを使用したが，対策が空白になっている空札に学習者同士が話し合って決めた対策を記入できるようにした．
A グループの赤のカード 9 問は B グループの赤のカード 3 問を含み，両グループ共通のものとした．
実験に際しては A グループ，B グループともゲームの様子を録音にてデータを収集した．ゲーム内の各設問と，出された解決策カードと会話の内容を対応する形で保存した．
A グループのゲームにかかった時間は 13 分 45 秒，B グループのゲームにかかった時間は，“いやな話” をまとめてカードに記入する時間を含めて 1 時間 16 分 19 秒であった．
実験後，実験者が参加者対して 7 日後にメールでアンケート Web サイトを紹介し，7 日から 14 日の間に実験参加者全員の回答を回収した．

(2) 解決策アンケートの結果

情報セキュリティの事象に対するアンケートは A グループと B グループ共通のものである．
設定した設問は以下のとおりであった．

- 設問 1 : 自社（または自身の運営する Web サイト, SNS のグループ）のトップ画像が不正改ざんされた
- 設問 2 : 自社（または自分のメールアドレス）からスパムメールが実際に流出した
- 設問 3 : 自社（または自分）を装って不正アクセスを促すメールが拡散したと外部（他人）から指摘をうけた

回答にあたっては,「この問題を解決するにはどのようにしたらいいでしょうか？ゲームで出た解決策を思い出してください」と想起を促すようにした．
各設問に対するゲームで出現した解決策は以下のとおりであった．アンケートは Web で実施した．特に回答の様子を監視，回答を Web などで検索する，誰かに回答を質問することなどは禁じなかった．

- 設問 1 の解決策 : 対象機器を調査する，ぜい弱性を解決する修正プログラムを適用する，パスワードを変更する，バックアップから正常なファイルを復旧する，公的機関・外部機関に連絡する，自組織の公式見解を出す
- 設問 2 の解決策 : 対象機器を調査する，組織内から外部への特定の通信を停止・遮断する，パスワードを変更する，ぜい弱性を解決する修正プログラムを適用する，自組織の公式見解を出す
- 設問 3 の解決策 : 対象機器を調査する，組織内から外部への特定の通信を停止・遮断する，自組織の公式見解を出す

アンケートに記述された回答内に，各設問に対応した解決策の記述があれば，解決策の出現回数を 1 つずつ加算した結果，表 2 の結果となった．
ゲーム内で出現した解決策を回答記述の中に記述した回数は，A グループの参加者では 1.00 回となり，B グループの参加者では 1.33 回となった．解決策の出現回数の最大は 3

回,最少は 1 回であった.

表 1 情報セキュリティの事象の問いに対する解決策の出現回数

グループ	参加者	設問1 解決策出現回数	設問2 解決策出現回数	設問3 解決策出現回数	出現回数 平均値	グループ平均値
統制群 Aグループ	統制群1	3	1	2	2.00	1.00
	統制群2	2	0	1	1.00	
	統制群3	0	0	0	0.00	
実験群 Bグループ	実験群1	2	1	2	1.67	1.33
	実験群2	1	2	0	1.00	
	実験群3	1	1	2	1.33	

(3) 発話による情報セキュリティの事象収集ゲーム“いやな話”の結果

実験群の学習者は 1 巡目に，情報セキュリティの脅威としての『乗っ取り』の内容を「種」として，“いやな話”を提示した．内容は学習者が特定の組織・法人に属していないことなどから，個人としての情報，セキュリティ，乗っ取りというキーワードで関連する発話が為された．法人や組織の考える情報セキュリティとは異なるが，個人の抱える問題が提示された．

”キング　オブ　いやな話”は「ハイジャックに遭遇した．外国人だからパスポートを隠さなければいけないので，大変であった」というものであった．発話した学習者の実際に体験した話であったという．パスポートという国籍を特定する情報と，自身の命に関わる重大な危機であったという意味から，一番いやな話に選出された．

他には，SNS のグループの管理者権限を乗っ取られた実体験が提示されたが，他は学習者自身が日ごろ，インターネットを利用した体験で得た不快な内容，および社会報道を見聞きして不快に感じている内容が挙がった．

“いやな話”は情報セキュリティに関する事象収集ゲームであるが，学習者が日ごろ不快に感じている様々な事象を発話する場となってしまい，情報セキュリティとは関連のない内容で会話が盛り上がってしまったといえる．1 つの話題に様々な質問や意見がやりとりされ，情報交換という形になってしまった．

(4) 解決策の思考演習ゲーム“解決の沼”の結果

9 問の“いやな話”が提示され，うち，発話で収集されたもの 6 問の中，3 問が「解決できない」という結果になった．セキュリティインシデント対応ボードゲームで用意した 3 問の情報セキュリティの事象については，学習者同士の話し合いで解決した．そのうち 1 問については，用意してあった解決策カード以外に独自の解決策の追加を検討し，選択することにした．図 2 のいやな話のカードと解決策のカードに示すように，その場で情報セキュリティの事象と解決策を記入した．

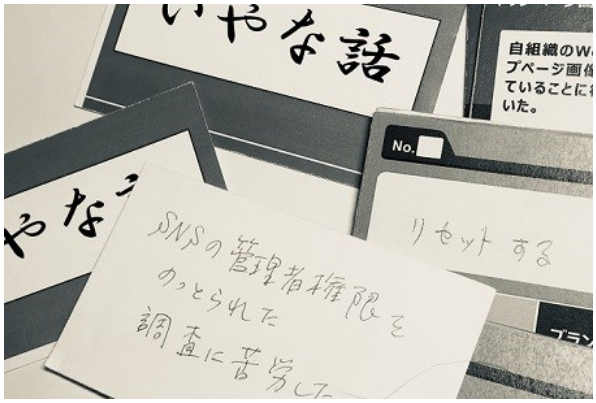

図 3 いやな話のカードと解決策のカード

(5) ファシリテータのゲームへの関与の結果

“いやな話”を収集する際に学習者の発話する内容を適切に制御できていたとはいえない．1 巡目は情報セキュリティの脅威としての『乗っ取り』の内容を「種」として，沿って発話を促す役割であったが，学習者の話を遮ることができず，結果として，情報セキュリティという内容とは離れたものとなった．

“解決の沼“では，収集した”いやな話”の解決策に大変時間がかかってしまい，結果，解決できないなど，学習者が真剣に検討しているところを遮り，方向性を変えることができなかったといえる．

ファシリテータは情報セキュリティとして適切な解決策を説明することは可能であったが，学習者の活動を制御し，誘導する技術が不足であった．

6. 考察

本研究において実験参加者の事前の情報セキュリティにおける知識は特に確認していない．従って，そもそも情報セキュリティに関する知識を持っている人が本研究の学習内容に関係なく，好成績を獲得する可能性がある．

Web アンケートで提示された設問は全て既存の情報セキュリティの事象であることから，この解決策を既知のものとして回答する参加者の可能性は否定できない．

また，回答にあたって学習者が回答を調査しながら記述することを禁じていないことから，情報セキュリティの事象の問いに対する回答は果たして，実験結果によるものか否かの判断ができない．このことから，本研究では，開発した情報セキュリティ教育のゲームの有効性を論じることはできない．

また，情報セキュリティの事象収集ゲームにおいて，ファシリテータがその役割を充分に果たしておらず，学習者自身の身近な不快な話の交換に終始してしまった．ゲームのルールである，前の人より“いやな話”をするという部分から，前者の話はよく聞いていたといえる．いわゆる組織・法人の考える情報セキュリティの事象ではなかったといえるが，個人の抱える問題の情報交換ができたといえる．

一般的な情報セキュリティの事象からは逸脱していたといえる．
解決策の思考演習では，充分な意見交換ができ，新しい解決策を 1 つ追加できた．しかしながら，収集した事象が情報セキュリティの事象とは言い難いものが含まれていたので，情報セキュリティ教育を目的とした解決策の話し合いができたとはいえなかった．
本研究においてファシリテータの役割は大変重要であることが明確となった．ファシリテータが学習活動全般を制御することが本研究で開発した情報セキュリティ教育カードゲームにおいて必須である．
今後，ゲームの有効性の評価については，学習者個人の情報セキュリティについての知識によって有効性測定に差が生じないよう，同一人物において情報セキュリティ教育を受ける前後で対策についての質問を行い，その差を分析することで，教育効果を測る必要がある．

謝辞　実験の実施に際しては放送大学文京合唱部のかたがたの協力を頂きました．謹んで感謝の意を表します．

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 2017,” 2017. [オンライン]. Available: https://www.ipa.go.jp/files/000058504.pdf. [アクセス日: 1 5 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. [オンライン]. Available: http://www.jnsa.org/result/incident/data/2016incident_survey_ver1.2.pdf. [アクセス日: 1 5 2018].
[3]　独立行政法人情報処理推進機構, “情報セキュリティ白書 2009 第Ⅱ部,” 1 4 2010. [オンライン]. Available: https://www.ipa.go.jp/files/000016941.pdf. [アクセス日: 1 5 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, JIS 規格, 2014.
[5]　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,” 30 3 2016. [オンライン]. Available: https://www.masshou.com/shredder/enquete/216/. [アクセス日: 1 5 2018].
[6]　独立行政法人情報処理推進機構, “情報漏えい発生時の対応ポイント集,” 2018. [オンライン]. Available: https://www.ipa.go.jp/files/000002224.pdf. [アクセス日: 1 5 2018].
[7]　ケイティ・サレン , エリック・ジマーマン, ルールズ・オブ・プレイ（上） ゲームデザインの基礎, ソフトバンククリエイティブ, 2011.
[8]　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, 2012.
[9]　松本多恵, “ゲーミフィケーションとシリアスゲームの相違点について,” 情報の科学と技術, 第 巻 64, 第 11, pp. 481-484, 2014.
[10]　標葉 靖子, 江間 有紗 , 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, 第 巻 41, 第 2, pp. 161-169, 2017.
[11]　JNSA（日本ネットワークセキュリティ協会）, “セキュリティ専門家　人狼ゲーム,” 1 2017. [オンライン]. Available: http://www.jnsa.org/edu/secgame/secwerewolf/secwerewolf.html. [アクセス日: 1 5 2018].
[12]　株式会社トレンドマイクロ, “インシデント対応ボードゲーム,” 2 2018. [オンライン]. Available: https://appweb.trendmicro.com/doc_dl/select.asp?type=1&cid=205. [アクセス日: 7 2 2018].
[13]　認定 NPO 法人イーパーツ, “セキュろく,” 1 2013. [オンライン]. Available: http://www.eparts-jp.org/project/2013/01/securoku130118.html. [アクセス日: 7 2 2018].
[14]　太田信夫, 記憶の心理学, 放送大学教育振興会, 2008.
[15]　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,” 4 2018. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/10threats2018.html. [アクセス日: 1 5 2018].