Vol.2018-SPT-31 No.12
Vol.2018-EIP-82 No.12
2018/11/2

情報セキュリティ意識向上を目的とした企業内教育用ゲームの検討 —パスワード強化を例に—

萩谷 文[†1]　稲葉 緑[†1]

概要：企業や組織は、情報セキュリティ対策の一つとして、継続的に従業員への教育を実施している。しかし情報セキュリティ対策に関する知識の教育を受けたにもかかわらず、その対策の実施に消極的な従業員は少なくない。我々は、上述した従業員に対し、「自分が情報セキュリティ対策を実施しなくてはならない」との意識を（あるいは、認識を）喚起させる教育コンテンツについて検討する。本研究では、「安易なパスワード運用」への対策を例として、従業員がパソコン上で取り組むゲーム形式のコンテンツを作成する。このゲームでは、攻撃者目線で安易なパスワードを推測するクイズを学習者に回答させることで、自身が使用するパスワードの危険性について考える機会を提供する。今回は、このゲームを試作し、そのわかりやすさやユーザビリティを評価した結果を報告する。

キーワード：情報セキュリティ意識、企業内教育、ゲーム

Study of an educational game aimed at improving information security awareness of employees - A case for enhancing creating strong passwords –

AYA HAGIYA[†1]　MIDORI INABA[†1]

Abstract: Companies and organizations have been continuously educated employees as one of information security measures. Despite receiving education on knowledge on information security, many employees seem to be reluctant to perform information security behaviors. We will consider educational programs that evoke the consciousness such as "I must personally perform information security behaviors" for the employees mentioned above. We create each educational program in the form of a game that works on personal computers. This research reports the game focusing on educating strong passwords. This game tries to provide the employees opportunities to think about the risk of the password used by themselves. In this game, employees play an attacker and guess passwords with clues that are provided. We would like to show results of evaluating the usability and the expected effectiveness of a prototype of the game.

Keywords: Information security awareness, corporate educational, Game

1. はじめに

多層防御による技術的な情報セキュリティ施策は広く普及し、企業、組織のサーバは情報システム管理者による管理監視のもと、攻撃に対する耐性が高まっている。それに対し、クライアント PC への情報セキュリティ対策は未だ行き届かない部分が多い。攻撃者は、強固に防御されたサーバではなく、十分に管理されていないクライアント PC 及びそれを利用する従業員の行動を直接狙い、人的脆弱性を足掛かりにサイバー攻撃を仕掛ける場面が増えた。また、働き方改革の一環によりテレワークが再び普及する等、従業員は一人複数台のデバイスを用いて業務システムを活用した業務を遂行している。そうした従業員の行動や選択ひとつひとつに情報セキュリティリスクが潜んでいるため、企業や組織の情報セキュリティ対策において、人的問題の占める割合は拡大したと言える。しかし従業員らは、情報セキュリティ対策は情報システム担当者が実施すればよいと考え、積極的に情報セキュリティ行動をとらない場合があることが指摘されている[1][2][3]。企業や組織の安全な日々を維持するためには、情報システム担当者による技術的な情報セキュリティ対策実施に加え、従業員ひとりひとりの情報セキュリティ行動は欠かせない。従業員は、自身の行動が情報セキュリティインシデントを誘発する要因とならないよう、業務へ取り組む際には情報セキュリティ行動を意識することが必要である。

2. 先行研究と研究テーマ

2.1 先行研究調査

自身の行動や選択に情報セキュリティインシデントを誘発する要因があるために、「自分が情報セキュリティ対策に取り組まなくてはならない」と認識（以下「自分事認識」

†1 情報セキュリティ大学院大学
Graduate School of Information Security INSTITUTE of Information Security

と言う）することを、本研究では情報セキュリティ意識のひとつであると考える。情報セキュリティ意識とは、身近な情報セキュリティに関する話題に関心を持つ、情報セキュリティ脅威に対して注意を払う、といった、情報セキュリティ行動を心がけようとする態度、と定義する。情報セキュリティ意識向上のために、情報セキュリティの知識や背景、なぜその行動を選択せねばならないのかといった理由を学習者へ教授する教育は多い[4][5][6][7]が、それだけでは自分事認識を相手に持たせることができるとは限らない。情報セキュリティの知識を得た結果、それは情報システム担当者等がやればよい、もしくは、自分には情報セキュリティインシデントは起こらないので、該当しないと誤って理解する可能性がある。自分事認識を醸成するためには、情報セキュリティインシデントの原因が、発生時の被害の大きさ、コンプライアンスといった外的要因だけではなく､自身の脆弱性にもあると把握することが必要である。情報セキュリティに関する知識があったとしても、自分事認識が欠落していた場合、企業や組織における人的セキュリティ対策の多くは用をなさないため、本研究では各従業員の自分事認識の醸成について、先行研究を調査した。

西郡らは、情報セキュリティ意識向上のために、脅威を身近に捉えさせることを目的とし、ランサムウェアを題材とした複合的な手法によるアプローチを試みた[9]。エンターテイメント要素として漫画を用いたランサムウェアに関するケーススタディを実施後、実際にウイルス感染を視認させることで自分の問題として捉えさせた。さらに、受講者同士によるディスカッションの時間を設け、理解の深度化を図っている。アンケート結果にて、リスク認識向上が達成された結果が示されているが、この論文において高まった情報セキュリティ意識とは、脅威の恐ろしさを知り、同様の事象が発生した際、どのように対応すべきかを理解したという知識の側面であり、自分事認識が高まったかどうか関しては、アンケートにおいて具体的に評価されていない。

大久保らは、被害者目線での脅威体験型コンテンツを提案している[10]。各自がブラウザでサイトにアクセスすることで、様々なセキュリティ脅威について学ぶことができる。脅威に関する前提知識フェーズ、被害者目線で脅威を体験するフェーズ､脅威への対策知識フェーズで構成され､情報セキュリティ知識の習得と、被害体験の組み合わせにより、情報セキュリティ意識向上が検討されている。しかし､自分事認識の醸成という面では､｢脅威発生の仕組みは理解できたけれども、自分には発生しない」と考える従業員に対して､｢このままでは自分も引っかかってしまう」と認識させ、自分自身に発生のリスクがあることを実感させることができる構成ではない。

Raghu Raman らは、大学生に対し、実生活において情報セキュリティ行動をとらせることを目的として、実際の情報セキュリティインシデントに基づいたシナリオベースのゲームを使用し、学習効果に対する有効性検証を行った[11]。シナリオゲームにて情報セキュリティインシデント対応について習得した学生は、既存の授業形式にて同様の内容を習得した学生よりも、知識テストにおいて有意に高い値を示した。しかし、実生活へ反映したかどうかについての評価は示されておらず、またこの研究は大学生向けの教育プログラムであり、企業や組織における従業員をターゲットとしていない。

会田らは、情報セキュリティ意識の低い従業員に対し、情報セキュリティ教育に「楽しく」取り組ませることで情報セキュリティ意識を効果的に向上させることを目的として、セキュリティ双六「セキュろく」を開発した[6]。ボードゲームというエンターテイメント性により、情報セキュリティ教育の入口のハードルを下げることで、受講者を積極的に参加させることを可能とした。活発に行われた意見交換が、情報セキュリティ意識向上につながったと示されている。しかし、ここで述べられている情報セキュリティ意識とはインシデント発生時にどのような対策をとるべきかという知識の側面であり、自分事認識を喚起するものではないと思われる。

藤田らは、楽しみながら強度の高いパスワードを覚えさえる事を目的として、ゲーム形式でのコンテンツを提案している[5]。｢クリアしたい」｢高得点をとりたい」という意欲を、高い情報セキュリティタスクの達成に変換し、ユーザーが日常生活においてゲームで遊んでいるうちに、強度の高いパスワードの記憶を促進する結果が示された。情報セキュリティ意識向上という面では、知識・スキル側面の向上が確認されたと言えるが、自分事認識向上については目的対象になかったと思われる。

服部らは、情報セキュリティ意識の低いスマートフォン利用者であっても、安全に秘密情報を利用させる動機付けを行うことを目的として、その手段に利用者が求める「ゲーム」を用いた手法を提案した [12]。｢セキュリティ行動をとるため」ではなかなか得られないユーザーの能動的な関わりを、ゲームのエンターテイメント性にて引き出すことができることを示し、セキュリティ行動をとる動機付けとして、ゲームの手法が有効であることを示した。しかし、動機付けが目的であり、本研究の対象である自分事認識の喚起とは主旨が異なる。

稲葉らは、失敗経験減少による失敗回避能力の低下や、個人の慢心が増長することを防ぐために、エラ―体験型教育コンテンツを提案している[13]。従業員各自がパソコン上で取り組むゲーム形式にて、失敗（エラー）の機会提供を行う。エラー体験後、｢Know why」｢Know how」を従業員に身近な例を挙げ解説することで、従業員が自身の業務におけるエラーリスクを考え、その防止策を自ら実行することが示された。｢自分は失敗しない」と考えていた従業員

に対し、エラー体験の機会を与えることで、意図的にエラーリスクを考えさせ、防止策を自ら実行させるという観点は、自身の脆弱性と情報セキュリティインシデントとの因果関係把握に共通するが、本論文は情報セキュリティに関する分野ではない。

2.2 研究テーマ

前節までの先行研究調査では、いずれにおいても従業員が「自分が取り組まなければならないという気持ちを高めたか」に言及しているものはない。自分事認識の向上に注目すると、集合的なディスカッション形式では、受講者のセキュリティ意識の高低により、参加度が大きく異なるという問題点が挙げられる[9]。情報セキュリティ意識が低く、参加度の低い受講生に、自分自身の脆弱性について考えさせ、自分事認識を喚起することは難しい。次に、被害者目線での脅威体験、実際の情報セキュリティインシデントをストーリーベースとしたインシデント対応体験では、自身の行動が脅威を誘発する要因となり、インシデントに繋がる可能性を実感することができる作りではないという問題点が挙げられる。個人の情報セキュリティ意識の高低によらず、自分自身の脆弱性について考える時間を作り出すためには、場所・時間にとらわれずに一人で取り組むことができることと、情報セキュリティ教育に対する能動的な態度が必要であると考えられる。先行研究で挙げられたゲームの手法[5][6][10][11][12][13]では、そのエンターテイメント性により、情報セキュリティ意識の低い受講生からも、能動的な関わりを引き出すことが示されていた。また、パソコン上で取り組む方式[10][11]であれば、時間・場所にとらわれずに一人で取り組むことが可能である。そのため本研究では、従業員個人の情報セキュリティ意識の高低に左右されず、自分自身を見つめ直し、自分事認識を高める可能性が高いことに注目し、ゲーム方式を採用する。このゲームでは、脅威を被害者目線ではなく、攻撃者目線で捉えさせる。受講者の身に覚えのある脆弱性を、自分自身で突破させるというストーリーフェーズと、どこに問題があったのかを示す解説フェーズに分けて構成する。自分自身の現状に脅威誘発のリスクがあると気づかせ、自分自身の持つ脆弱性について考える機会を提供する。自分事認識の向上に、ゲームの手法が有効かどうかを明らかにすることを研究テーマとする。ゲームの主題選定後、その中の一つについてゲーム試作・実験を行い、わかりやすさとユーザビリティの評価を行うことを目的とする。

3. 提案手法

3.1 ゲームの主題決定

はじめに、ゲームにて取り上げる教育トピックを、従業員の日常における非セキュリティ行動から選定した。非セキュリティ行動とは、企業や組織の情報セキュリティポリシーに違反する意図のある、なしに関わらず、企業や組織の情報セキュリティポリシーに違反する行動のことを指す。

非セキュリティ行動の列挙にあたり、次の 2 工程を実施した。①一般企業従業員の 1 日、1 週間、1 か月の PC を利用した業務を想定し、非セキュリティ行動を列挙した。これには、Kathryn Parsons らによる研究[2][8]、質問紙モデル HAIS-Q で用いられた情報セキュリティにおける 7 つの重要項目（パスワード管理、メール利用、インシデント報告、ネットワーク利用、情報管理、モバイルコンピューティング、SNS 利用）を活用した。7 項目別に非セキュリティ行動 33 項目を列挙した。②システム管理会社 A 社にて、日頃情報セキュリティ教育に携わる担当者 9 名へ、当該表の網羅性についてインタビューを行った。インタビュー結果より 3 項目を追加し、完成させた。この結果を表 1 に示す。

表 1：非セキュリティ行動一覧

Table 1　Unexpected information security behaviors.

場面		非セキュリティ行動	原案	補完
オフィス編				
1	パスワード管理	初期パスワード運用	○	
		安易なパスワード運用	○	
		パスワード使いまわし	○	
		他人に教える・紙に記載して添付	○	
		不適切な共有	○	
2	メール利用	メール送信時の宛先誤り	○	
		個人情報や社外秘情報をメール本文に記載	○	
		個人情報や社外秘情報ファイルをPWなしに添付	○	
		怪しいメールを開き、添付ファイル/リンクを実行する	○	
		業務外のメール利用	○	
		CC、BCC取違い		○
3	インシデント報告	マルウェア検知後、離線しない	○	
		マルウェア検知後、報告しない	○	
		マルウェア検知後、現場を荒らす	○	
		同僚の不正行動を見逃す	○	
4	ネットワーク利用	業務に必要ではないデータ閲覧	○	
		業務に必要ではないインターネット閲覧	○	
		業務に必要ではないソフトウェアダウンロード	○	
		業務に必要なインターネット閲覧によるウイルス感染	○	
		URLを確認せずに検索結果のリンクをクリックする	○	
		外部のパブリッククラウドサービスを利用	○	
5	情報管理（デバイス管理）	OS、S/Wアップデートを怠る	○	
		セキュリティパッチ適用を怠る	○	
		ウイルス対策ソフト警告無視	○	
		私物のUSBメモリを社内OA端末、業務用端末に接続	○	
		私物スマートフォンを社内OA端末、業務用端末に接続	○	
		実在性確認/貸し出し管理の形骸化		○
外出・出張・自宅編				
6	モバイルコンピューティング	人通りの激しい場所でノートPCから社内システムにログイン	○	
		公衆無線LANに接続し、社内システムログイン	○	
		カフェでノートPCにて業務作業中、離席	○	
		自宅NWでの業務作業（自宅NWのセキュリティ）		○
		社用PC、USBの紛失	○	
		社用PC、USB、タブレットを家族に使用させる	○	
7	SNS利用	「これから○○へ出張」とSNSに記載	○	
		会社の悪口をSNSに記載	○	

「場面」として挙げた 7 つの大項目が、HAIS-Q で用い

られた 7 つの重要項目である。それぞれに列挙した非セキュリティ行動の内、先に筆者にて列挙した内容を「原案」、インタビューにて補完した内容を「補完」として丸印を付け、示している。次に、上に示した 35 項目の非セキュリティ行動をもとに、前述の情報セキュリティ教育担当者へ半構造式インタビュー調査を実施した。発生時の影響度が高いにも関わらず、既存の手法では、原因となる非セキュリティ行動にアプローチしきれていない項目について尋ねた。まず、パスワードの運用に関して、規程の文字数や大文字・小文字・数字の混合といったポリシーは守られているものの、誕生日や辞書用語、数字の羅列といった安易な設定が多く、その問題性を従業員に認識させることが難しいという点が挙げられた。次に、SNS 利用について、主に新人を対象とした情報セキュリティ研修で「業務情報を SNS に掲載してはならない」ことを伝えているが、受講生に「自分のこと」と捉えさせることが難しい点が挙げられた。最後に、継続的に情報セキュリティ教育の場で発信しているにもかかわらず、情報セキュリティインシデントの発生件数が一定数存在し続けるテーマとして、許可されていない USB メモリの社内 OA 端末への接続を起因とするウイルス感染と、業務に必要なサイト閲覧中のフィッシング詐欺被害が挙げられた。したがって、本研究では「安易なパスワード運用」、業務に関連のある事柄を調べる過程で発生する「フィッシング詐欺」、特に新入社員との価値観の差が危険視される「SNS への業務情報投稿」の 3 項目をゲームの主題として選定する。中でもまず、情報システムを利用するすべての従業員が最初に直面するパスワードに注目し、「安易なパスワード運用」への対策としてゲームの実装に着手した。

3.2 ゲームのコンセプト

多くの企業や組織では、情報セキュリティポリシーの中にパスワードポリシーを制定し、従業員へ遵守を求めている。また、技術的に入力ステータスを制御し、ポリシーに満たないパスワード入力を排除しているケースもある。しかし、技術的な排除がない場合、安易な数字の羅列、安易なキーボード配列の利用、氏名と誕生日の組み合わせといった脆弱なパスワードを、本人はそうとは知らずに運用している場合があることが示されている[14]。また、強度の高いパスワードを生成したとしても、他人と共有する、紙に書いて PC 本体に添付するといった、管理に問題がある場合についても同様に指摘されている。そのような従業員に対し、攻撃者目線で安易なパスワードを推測するクイズを解答させることで、自身の使用するパスワードの脆弱性について考える機会を提供する。

3.3 ゲームを通じたパスワード運用の強化

ゲームでは親しみやすいストーリーを用意し、情報セキュリティ対策への苦手意識を擁する従業員であっても、気軽に取り組むことができるよう配慮した。また、集合的な研修ではなく、個々人がフレキシブルに本ゲームを活用することを想定し、ゲーム全体を 10 分程度で終えられるように配慮した。ゲームは、大きく分けてクイズフェーズと、解説フェーズによって構成される。前節で示した通り、学習者がパスワードを推測し、パスワードを見破る側として、クイズ形式のゲームを進めていく。クイズフェーズ終了後、なぜパスワードが推測されてしまったのか、どうすれば推測されにくくなるのかを解説するフェーズが始まる。全編を通して、学習者自身が業務上、あるいは日常生活において、実際に使用しているパスワードについて考えさせる。自分自身がゲームにて使用した手法によって、自分自身のパスワードが推測されてしまうのではないかと思い、情報漏洩につながる可能性があるというリスクに気付いた場合、改めて自分自身のパスワードを見直し、強度の高いパスワードの生成、および、適切な管理に繋がることを期待する。

3.4 ゲーム試作

非セキュリティ行動の列挙と、それに基づくインタビュー調査より導き出したゲームの主題の内、「安易なパスワード運用」について、HTML と javascript を用いて、実際にゲームとして試作した。先行研究[13]でも用いられたシリアスゲーム方式である。シリアスゲーム方式とは、学習内容を提供するゲームのことである。従業員が実際に攻撃者となって他者のパスワードを推測する行為は望ましくない。シリアスゲームは、そのような実際には体験することが難しい事柄を、教育を目的として模擬的に体験させる。ゲームを通じて知識を身に着けたり、提供された問題について考え、実感を伴って理解させたりすることができるとされている[15]。ゲームのストーリーは、グリム童話「おおかみと七匹の子ヤギ」をベースとした。学習者はおおかみとなって、子ヤギがパスワードを設定し、隠れている「シェルター」のパスワードを推測していく（図 2、図 3、図 4、図 5）。子ヤギたちはあらかじめ、お母さんヤギから、パスワードポリシーに相当する情報セキュリティ知識を与えられているが、必ずしもそのパスワードポリシーを守ってはいない。一方、おおかみは事前に、パスワードの推測に役立つヒント集を「おおかみハンドブック」（図 6）として得ており、その情報を活用して「シェルター」を 1 つずつ開け、中の子ヤギを食べる。クイズそれぞれの難易度については、自身のパスワードも簡単に推測されてしまう可能性を、学習者が実感できるよう配慮した。パスワードを推測するためのヒントやガイドを多く用意することで、最大 3 回程度の入力で正しいパスワードを見破らせ、ゲームを進めていくことができるよう調整した。推測されやすいパスワードの特徴については、Blasé Ur らによる、平均的なユーザーのパスワード強度に関する誤解を明らかにするための質問

紙調査[14]の結果考察より、次の 3 点の特徴を抽出した。①自身の名前、誕生日が使用されていること、②家族やペットの名前、誕生日が使用されていること、③キーボード/テンキー配列が使用されていることである。さらに、ゲームの主題決定の際に実施したインタビュー結果のうち、情報セキュリティ教育担当者が現状の従業員らのパスワード運用における課題として挙げた、以下 2 点も抽出した。④パスワードを付箋に書いて PC 等にわかりやすく添付する運用、⑤初期パスワードのまま変更を行わない運用である。

図 1　試作ゲーム画面 1（スタート画面）
Figure 1　Screen1 of the test game. (Start Screen)

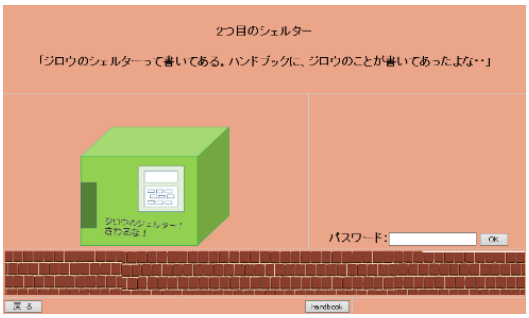

図 2　試作ゲーム画面 2
（パスワードを推測するクイズ画面）
Figure 2　Screen2 of the test game
(Screen guessing the passwords)

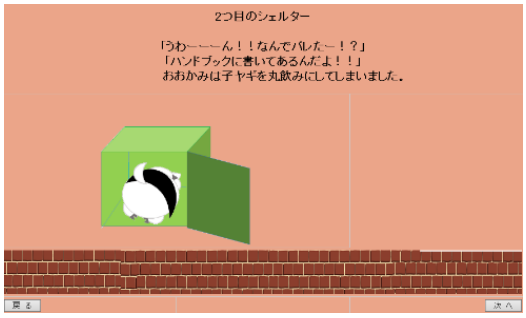

図 3　試作ゲーム画面 3（クイズ正解画面）
Figure 3　Screen3 of the test game
(Screen Guessing right on a Quiz)

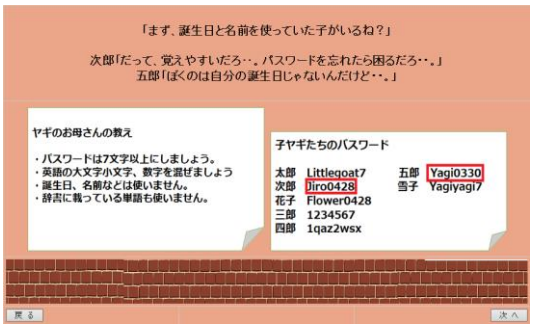

図 4　試作ゲーム画面 4（解説画面）
Figure 4　Screen4 of the test game
(Screen detailed commentary on Quiz)

図 5　おおかみハンドブック画面
Figure 5　Tips to guess the passwords for wolves

4. まとめと今後の予定

4.1 試作実験

3 章で試作したゲームを用いて実験を行い、提案方式の「パスワード運用強化」ゲームについて、わかりやすさとユーザビリティを検証する。被験者は本学の学生を予定している。ゲームプレイ後、アンケート調査を行う。ゲーム実施中は時間を測定し、想定の時間内にプレイし終わることが可能かについても検証する。ゲームの難易度、問題数、画面構成等に関しては、アンケート結果を反映し、調整を行う。

4.2 発表

SPT 学会発表当日は、前節にて実施した実験結果について発表を行う。

4.3 本実験

試作実験の結果をゲームに反映し、改良後、本実験を実施する。提案手法と、一般企業の情報セキュリティ教育にてよく用いられる、テキストによる座学形式での手法との比較実験を行う。実験後には知識テストとアンケート調査を行い、ゲーム手法の有効性を検証する。また、情報セキュリティ知識と、自分事認識の高まりを確認する。さらに、パスワードの変更または管理方法の変更を検討したかどう

かの追跡評価を予定する。

参考文献

[1] 大友ら、意志があるのに実施しない心理～リスクを高める潜在的動機～,2009,IPA 情報セキュリティと行動科学研究会
[2] Kathryn Parsons et all. Determining employee awareness using the Human Aspects of Information Security Quetionnaire(HAIS-Q), 2014,Computer & Ecurity
[3] 畑島 隆　坂本 泰久、情報セキュリティ不安全行動に対するテレワーク実施者の性向の分析,2017,情報処理学会論文誌
[4] 大和田ら、従業員のリスク行動に対する企業の取り組みモデルの提案,2010,研究報告マルチメディア通信と分散処理(DPS)
[5] 藤田ら、エンターテイメントを活用したセキュリティ強化：パスワード強化を組み込んだゲームの実装とその有効性, 2016,情報処理学会論文誌 Vol.57 No.12
[6] 会田和弘、セキュろくキッズ～双六を用いた情報セキュリティ教育の試み,2014,関西学院大学リポジトリ 総合政策研究 p89-p94
[7] Kathryn Parsons et all. The Information Security Awareness of Bank Employees, 2016, Computer & Ecurity
[8] 大賀ら、情報セキュリティ意識向上のための方策の一考察-セキュリティに関する教育（研修）に着目して-, 2014,研究報告電子化知的財産・社会基盤（EIP）
[9] 西郡ら、利用者のセキュリティ意識を高めるケーススタディの一考察,2017, 日本セキュリティ・マネジメント学会 No.31 pp.101-108
[10] 大久保隆夫　戦略的イノベーション創造プログラム（SIP）重要インフラにおけるサイバーセキュリティの確保　セキュリティ人材育成の研究開発, 2018 年
[11] Raghu Raman et all. Serious Games based approach to cyber security concept learning: Indian context, 2014, International conference on Green Computing Communication and Electrical Engineering(ICGCCEE)
[12] 服部ら、安全な秘密情報利用の動機付けを目的とした個人認証のゲーム化, 2018, 情報処理学会研究報告
[13] 稲葉ら、鉄道分野におけるヒューマンエラー教育-社員向けヒューマンエラー体験型学習ツールの開発を例に-, 2017, システム/制御/情報　Vol.61, No.6 pp.226-232
[14] Blasé Ur et al.”I Added ‘!’ at the End to Make It Secure”: Observing Password Creation in the Lab, 2015, Symposium on Usable Privacy and Security
[15] 藤本徹、シリアスゲーム 教育・社会に役立つデジタルゲーム、2007 東京電機大学出版局