

推薦論文

エンターテイメントを活用したセキュリティ強化： パスワード強化要素を組み込んだゲームの実装とその有効性

藤田 真浩¹ 山田 眞子² 西垣 正勝^{1,a)}

受付日 2016年3月10日, 採録日 2016年9月6日

概要：ヒューマンファクタを考慮してセキュリティの強化を達成する方法の1つとして、セキュリティとエンターテイメントの融合が提案されている。既存研究では、セキュリティシステムの安全性や利便性を改善させる目的で、セキュリティ技術の中にエンターテイメント因子を導入する試みが報告されている。本論文では、ユーザのセキュリティ意識やスキルを向上させる目的で、エンターテイメントの中にセキュリティ因子を埋め込む新たな試みを提案する。さらに、その一方式として、パスワードをゲーム内のコマンドとして組み込む方式を提案・実装する。実装したシステムを利用してユーザ実験を行った結果、提案方式がユーザに、強力なパスワードを容易に覚えさせることに寄与することを確認した。

キーワード：エンターテインメント, ユーザ認証,ゲーミフィケーション, パスワード

Security Enhancement through Entertainment: Implementation of game in which password enhancement factor is embedded and its effectiveness

MASAHIRO FUJITA¹ MAKU YAMADA² MASAKATSU NISHIGAKI^{1,a)}

Received: March 10, 2016, Accepted: September 6, 2016

Abstract: There could be two approaches for combining security with entertainment; (i) an entertainment factor is embedded in security technology and (ii) a security factor is embedded in entertainment technology. Since most previous studies focused on approach (i), we examined approach (ii). As the first attempt, this paper tried to embed a password enhancement factor into games. We designed a password enhancement scheme which enables users to easily memorize strong passwords while playing games. We also discuss the effectiveness of our scheme through a user experiment.

Keywords: entertainment, user authentication, gamification, password

1. はじめに

情報システムは人間（ユーザ）が利用するためのものであり、情報システムに攻撃を仕掛けるのも人間であることから、安心・安全な情報システムの実現には、ヒューマンファクタ（人的要因）を考慮したシステム設計が必須であ

る。その1つの試みとして、エンターテイメントとセキュリティの融合により情報システムのセキュリティを強化する方法が検討されている [1], [2], [3], [4]。

「エンターテイメントとセキュリティの融合」は、セキュリティ技術にエンターテイメント因子を導入するアプローチと、エンターテイメントにセキュリティ因子を導入するアプローチに大別される。前者が、ユーザのセキュリティシステム利用時における安全性や利便性を改善することが

¹ 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University, Hamamatsu, Shizuoka 432-8011, Japan

² 静岡大学情報学部
Faculty of Informatics, Shizuoka University, Hamamatsu, Shizuoka 432-8011, Japan

^{a)} nisigaki@inf.shizuoka.ac.jp

本論文の内容は2014年10月のコンピュータセキュリティシンポジウム2014にて報告され、同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である。

目的であるのに対し、後者は、ユーザの日常生活の中でセキュリティ意識やスキルを向上させることを目的としている。しかし、著者らの調べた限りでは、現在までに行われてきた研究は前者のアプローチをとる研究が一般的であり、後者のアプローチに関する研究はほとんどなかった。そこで本論文では、後者の「エンターテインメントにセキュリティ因子を導入するアプローチ」に対する検討を行う。

今回はその第1報として、ユーザにとって最も身近なエンターテインメントの1つである「ゲーム」と、情報システム利用時にユーザが最初に直面する「ユーザ認証」に注目する。具体的には、「ゲーム」というエンターテインメントに「パスワードの強化」というセキュリティ因子を導入し、ユーザ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を記憶することを促進する仕組みを提案する。

本論文の構成は次のとおりである。2章でエンターテインメントとセキュリティの関係についてまとめる。3章で提案手法を詳細に述べた後、4章で提案手法の実装例を示す。5章で実験を行った後、6章で実験結果に対する考察を行う。7章で提案方式に関するさらなる検討を行った後、最後に8章でまとめと今後の課題を述べる。

2. 関連研究

2.1 セキュリティとエンターテインメントの融合の既存研究

文献[1]の4コマ漫画 CAPTCHA では、「CAPTCHA」というセキュリティ技術に「4コマ漫画の並べ替え」というエンターテインメント因子を導入している。ユーザは、シャッフルされた4つのコマを起承転結が正しい順序となるように並び替える。人間のより高度な認知能力である「ユーモアを解する能力」を利用しているため、高い機械解読耐性を有する CAPTCHA が実現されている。通常の文字判別型 CAPTCHA よりも複雑な作業を正規ユーザに求めているものの、4コマ漫画を読む楽しさ、パズルを解く(4コマ漫画を正しく並び替える)楽しさが、利便性の低下を抑えている。

文献[2]の DCG-CAPTCHA は、「CAPTCHA」というセキュリティ技術に「ゲーム」というエンターテインメント因子を導入した事例である。ユーザは、指示に適するオブジェクトを選択するというゲームを行う。たとえば、図1では、複数のオブジェクトの中から船のオブジェクトを選択(ドラッグ)し、海の上に配置(ドロップ)することができればゲームクリアとなる。システムユーザビリティスケール評価[14]の平均スコアは73.25(標準偏差15.07)であり、DCG-CAPTCHA の高い利便性を示している。また、ユーザがゲームをプレイする際のリアルタイム性に着目し、ユーザと CAPTCHA との間のインタラクションのタイミングを検査することによってリレーアタックの検出を実現している。

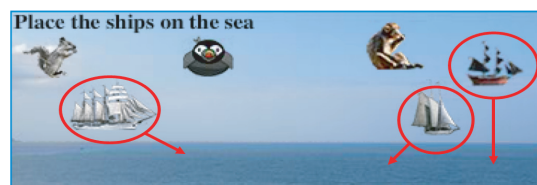


図1 DCG-CAPTCHA

Fig. 1 DCG-CAPTCHA.

文献[3]の間違い探し認証では、「ユーザ認証」というセキュリティ技術に「間違い探し」というエンターテインメント因子を導入している。登録フェーズでは、多数のキャラクタが配置された1枚の「問題用画像」がユーザに提示され、ユーザはその中の複数のキャラクタを「パスキャラクタ」として選択する。認証フェーズでは、問題用画像とその鏡像画像がユーザに提示される。ここで、問題用画像と鏡像画像においては、一部のキャラクタに間違い(キャラクタのポーズや色の変化、キャラクタ自体の変化)が混入しており、ユーザはパスキャラクタ中の何体が間違っているか解答する。パスキャラクタ以外のキャラクタにも間違いは含まれるため、間違いが混入しているパスキャラクタの数を正答することができるのは、パスキャラクタを知っている正規ユーザだけであることが期待される。間違いが混入するキャラクタが認証試行の度に変化するため、パズルを解く(間違い探しをする)という楽しさの持続と認証のワントタイム化が同時に実現されている。

文献[4]は、「パスワード認証」というセキュリティ技術に「ユーザが嗜好する画像」というエンターテインメント因子を導入した事例である。パスワード登録時にユーザが強度の高いパスワードを設定するほど、ユーザにとって誘引度の高い画像が表示される仕組みを運用することによって、ユーザに強いパスワードを登録させるように仕向けている。

2.2 セキュリティとエンターテインメントの融合に向けての2つのアプローチ

元来、セキュリティ技術の導入は利便性の低下を招く。すなわち、安全性と利便性はトレードオフの関係にある。この問題に対し、前節の既存研究は、「楽しさ」や「嗜好」というエンターテインメント要因を活用することによって、セキュリティ技術の利便性や安全性を改善することに成功している。すなわち、これらの既存研究は、

(1) セキュリティ技術にエンターテインメント因子を導入するアプローチ

による「セキュリティとエンターテインメントの融合」に類別されるものである。

しかし、一般的なユーザにとって、エンターテインメントとは余暇を過ごすためのものであり、エンターテインメントと仕事(業務)との親和性は決して高くはない。たとえば、

ユーザが勤務先での正規業務の中で情報システムを利用する場合には、エンターテインメント性（楽しさ）は業務の緊張感を途切れさせてしまうことになり、逆に、ユーザに煩わしさを感じさせてしまう元凶になりかねない。たとえば、間違い探し認証 [3] に対しては、ユーザは「ただでさえ業務が忙しいのに、認証のたびに間違い探しをする暇はない」と腹を立てるだろう。

(1) のアプローチの有効性が限定的となるこのようなケースに対しては、

(2) エンターテインメントにセキュリティ因子を導入するアプローチ

を検討することも重要となる。(1) が、セキュリティシステムの利便性や安全を直接向上するために、セキュリティシステムの中にエンターテインメント要因を導入するものであるのに対し、(2) は、逆に、日頃のエンターテインメントの中にセキュリティ要素を組み込むことによって、日常生活の中でユーザのセキュリティ意識やスキルを向上させ、セキュリティ強化を間接的に達成するものである。(1) と (2) の両者のアプローチが補完しあうことによって、セキュリティとエンターテインメントの融合が実効的なものとなると期待される。

2.3 セキュリティの教育と実践

娯楽コンテンツの中に教育要素を埋め込むことで、聴講者を教育する「edutainment」と呼ばれる取り組みが知られている。セキュリティ分野においても、すごろくで遊びながらセキュリティについて学ぶセキュろく [17] や、ドラマ [18] や漫画 [19], [20] などを通じてセキュリティ対策の重要性を学ぶコンテンツが公開されている。これらは、エンターテインメントにセキュリティ因子を導入するという観点では、本論文が取り扱うアプローチ (2) と共通している。

一方で、情報システムのセキュリティを担保するうえで、セキュリティに関する知識を獲得させること（教育）にとどまらず、獲得した知識をいかにユーザに実践させるかがより重要な観点となる。本論文の目的は、娯楽要素を用いてユーザのセキュリティ意識や実践的スキルを強化する点にある。たとえばパスワード認証を例にとって説明すると、本論文における「エンターテインメントへのセキュリティ因子の導入」は、ユーザに強力なパスワードを利用すべきことを教えるための教材開発がゴールではなく、ユーザに強力なパスワードを実際に記憶させるためのメソッドを提供することを意味している。

3. 提案方式

3.1 コンセプト

本論文では、エンターテインメントにセキュリティ因子を導入するアプローチの第 1 報として、「ゲーム」というエンターテインメントに「パスワード強化」というセキュリティ

因子を組み込むことで、ユーザが日常生活においてゲームで遊んでいる間にセキュリティ強度の高いパスワードを容易に記憶することを促進する仕組みを提案する。

3.1.1 ゲームの利用

近年、スマートフォンの普及にともない、多くのゲームアプリが続々と開発・公開されており、日常的にゲームで遊ぶユーザはますます増えている。したがって、ゲームは、ユーザに最も身近なエンターテインメントの 1 つであると考えられる。そこで本論文では、エンターテインメントとして「ゲーム」に焦点を当てる。

ゲームの利用 (gamification) は、ヒューマンコンピュータシミュレーション [6] あるいはクラウドソーシング [12] の分野でも注目されており、その好例が Foldit [13] や ESP ゲーム [7] である。Foldit では、ゲームがタンパク質の 3 次元的な分子構造を解明することにつながっている。ESP ゲームでは、2 人 1 組のプレイヤーによる連想ゲームが画像にラベル（名称）を付与するタスクを成している。これらは、「人間ベースの計算ゲーム (Human-based computation game)」または「目的をとめたゲーム (Games with a purpose)」と呼ばれ、人間の能力を利用することで、コンピュータにとって困難な「直観に基づく計算」や「画像の意味の認識」などのタスクを実行する仕組みとなっている。

これらのタスクをコンピュータゲームという形でユーザに提供することによって、「ゲームをクリアしたい」あるいは「高得点を狙いたい」というユーザのゲームに対する欲求を、コンピュータがタスク達成のために活用するという状況が実現されている。これは、ゲームを通じて「ユーザのセキュリティ意識やスキルを高める」というタスクを達成する仕組みを提案するという本論文のコンセプトに主旨を同じくするものである。

3.1.2 パスワードの強化

Web サービスの台頭によって、ユーザが利用する情報システムの数は一増し、ユーザが管理すべきパスワードの数も増加している。セキュリティ確保のためには、Web サイトごとに異なるパスワードを利用することが理想的であるが、人間の記憶できるパスワード数には限界があるため、複数のサイトでパスワードを使いまわすユーザが後を絶たない [8]。

複数のパスワードの管理については、パスワード管理ツールの助けを借りるなどの対策が有効なケースもあるだろう [9], [10], [11]。しかしながら、パスワード管理ツールはマスターパスワードが特定された場合に、ツールが管理しているすべてのパスワードが漏えいするリスクがある。パスワード管理ツールの利用を選択した場合であっても、マスターパスワードの管理は必要となる。

ユーザ認証は、情報システム利用時にユーザが最初に直面する関門であり、あらゆる情報システムのセキュリティの起点である。すなわち、パスワードに対するセキュリ

ティ意識およびスキルの向上は、ユーザにとって非常に重要な要件である。そこで本論文では、セキュリティ因子として「パスワード強化」に焦点を当てる。

3.2 ゲームを通じたパスワード強化

ゲームの中にパスワード強化の要素を組み込む方法としては様々なアイデアが考えられるが、今回は、その具体的なアイデアの1つとして、パスワードをゲーム内における「コマンド」として扱う方法を説明する（ここで示す方法はあくまでも1例である）。

ゲーム内でコマンドを繰り返し入力しているうちに、そのコマンドを記憶し、そのコマンドを見ずとも入力できるようになることは、ゲームのプレイヤなら誰もが経験することである。ここで、コマンドを「パスワード」としてとらえれば、ユーザはゲームの中でパスワード（コマンド）を覚えることが達成されている。そこで、パスワードを「コマンド」として事前に登録しておき、ゲーム中の適切なタイミングで「登録したコマンド」の入力をユーザに求めることによって、ゲームを通じてパスワード強化を促す。

たとえば、ロールプレイングゲームの中でモンスターと格闘する場面において、キャラクターの必殺技を発動するための「コマンド（パスワード）」を事前に登録しておく。ゲーム中にユーザが必殺技を発動するには、あらかじめ登録しておいた「コマンド」の入力が必要となるため、ユーザはゲームで遊ぶうちにこのコマンドを覚えることが期待される。ユーザは、このコマンドを、自身のパスワード管理ツールや Web サイトへのログインパスワードとして使用すればよい。

さらに、ユーザにより強度の高いパスワードをコマンドとして利用してもらうための仕掛けとして、「リワード」の考え方を取り入れる。リワードとは、ゲームの進行を有利にする要素を意味し、ゲームを進める上でのユーザのインセンティブとなる要素を指す。また、リワードはゲームの面白さ（ゲーム性）を高めるための要素としても重要な役割を担っている。

今回のゲームにおいては、長くて複雑なコマンド（パスワード）であるほど、より高いリワードがユーザに与えられる。上記のロールプレイングゲームにおける必殺技の例では、たとえば、「威力」をリワードにすることが考えられる。短くて簡単なコマンドであれば必殺技発動時の威力は通常攻撃力の2倍となり、長くて複雑なコマンドであれば通常攻撃力の10倍の威力とするなどの設定が可能であろう。この結果、ユーザは、ゲーム内でより高いリワードを得るために長くて複雑なコマンド（パスワード）を進んで設定するようになり、かつ、ゲームプレイ中に何度もそのコマンドを入力するうちにそれを記憶できるようになることが期待される。

本来、強力なパスワードを記憶することはユーザにとっ

て非常に面倒で負担の大きな作業である。提案方式のような仕組みを用意することによって、ユーザに強力なパスワードを容易に記憶させることが可能となる。

4. 実装

4.1 概要

提案方式の有効性を確認するために、3章に示した「パスワードをコマンドとして組み込んだ（シンプルな）ゲーム」を実装した。HTML と javascript を用いて開発した、シンプルなダンジョン探索ゲームである。ダンジョンは、複数のフロア（1階、2階…）から構成されており、各フロアにはランダムに生成された迷路が表示される。

本ゲームは、図2、図3、図4に示す3つの画面から構成される。フロア画面（図2）、戦闘画面（図3）、コマンド確認画面（図4）の3つの画面である。プレイヤは、「現在のフロア番号」、「拾ったアイテムの数」という2つのステータスを有する。各ステータスの詳細は、以下の項で説明する。

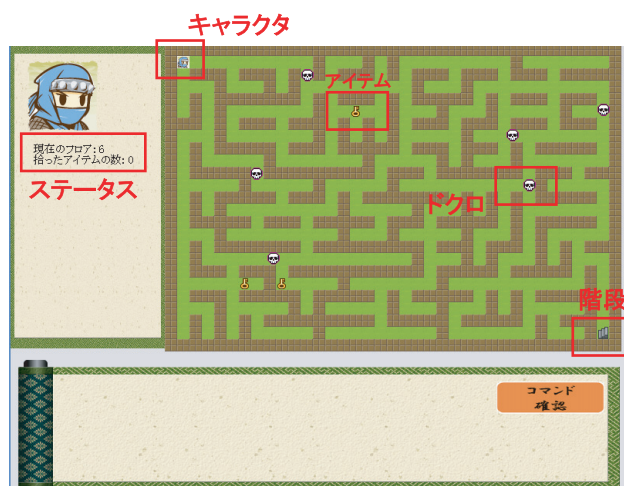


図2 フロア画面

Fig. 2 Floor view.



図3 戦闘画面

Fig. 3 Battle view.

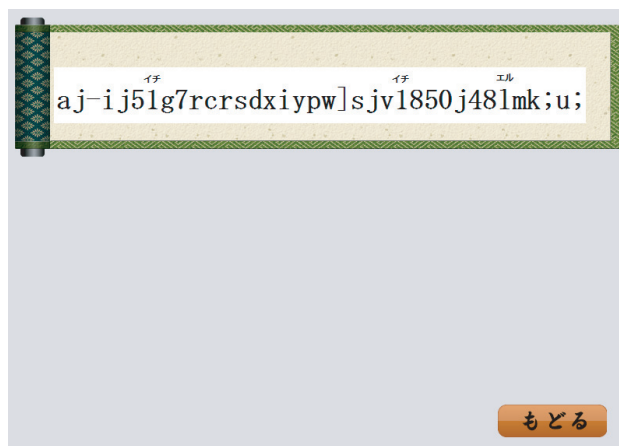


図 4 コマンド確認画面

Fig. 4 Commandcheck view.

4.2 フロア画面

プレイヤーは、キャラクタ（忍者）をキーボードの上下左右キーを押して移動させ、迷路を探索する。初期フロアは1階であり、キャラクタの初期位置は、左上のマス（図2は初期位置にキャラクタがいる時点の図）である。迷路中には、3つのアイテム（鍵）がランダムなマスにそれぞれ配置されており、キーと同じマスにキャラクタが移動した場合に、キャラクタの拾ったアイテムの数が1増加する。ただし、フロア内には複数のドクロ（障害物）が移動している。キャラクタがドクロに触れると、拾ったアイテムの数が1減らされたうえで、フロア内のランダムなマスに1つアイテムが配置される（アイテムを落としたことに相当する）。フロアの右下のマスには、階段が配置されている。階段と同じマスへキャラクタが移動した際、フロア中のすべての鍵を集め終わっていたら（拾ったアイテムの数が3だったら）次のフロアへ移動する。最終フロアから次の階へ移動すると、ゲーム終了となる。今回の最終フロアは12階とした（キャラクタが13階に到達した時点でゲーム終了となる）。

迷路を探索している途中には、1回（1マス）の移動につき一定の確率（今回は0.05）で、敵（モンスター）と遭遇し、戦闘画面へ遷移する。

4.3 戦闘画面

戦闘画面において、プレイヤーと敵には、「体力」というパラメータが設定されている。敵の体力は現在のフロアに依存して決定される。今回は、「現在のフロア $\times$ 3 = 敵の体力」とした。たとえば、図3の場合、現在のフロアが1階であるため、敵の体力は3である。プレイヤーの体力は一定であり、今回は30とした（前の戦闘の状態が次の戦闘へは引き継がれない。すなわち、戦闘開始時に必ず30となる）。

プレイヤーはテキストボックス内にコマンドを入力した後、キーボードのEnterボタンを押すことで敵に対して攻撃を行う。ここで、3章のリワードの考え方をとりいれ、

入力したコマンドが長ければ長いほどプレイヤーの攻撃の威力（敵に与えるダメージ）が上昇する。具体的には、 n 文字のコマンドを「登録コマンド」として登録しているプレイヤーが、 k 文字のコマンドを「入力コマンド」として入力した上で攻撃した際、入力コマンド k 文字が登録コマンドの先頭 k 文字と一致していた場合（以下、「 k 文字のコマンド入力に成功する」と表記する）に、文字数 k をプレイヤーの攻撃の威力とした。なお、コマンド入力に失敗した場合の攻撃の威力は0となる。

プレイヤーの攻撃によって、敵にダメージが与えられる。敵に与えるダメージは、上述のとおり、入力に成功したコマンドの長さ k である。攻撃による敵との接触の際に、プレイヤーも敵からの攻撃を受け、ダメージを負う。1回の敵との接触の際にプレイヤーの受けるダメージは、今回は10とした。お互いの現在の体力からダメージを減算した結果、敵の体力が0以下になった場合、プレイヤーの勝利である。フロア画面へと戻り、プレイヤーはゲームをそのまま継続する。プレイヤーの体力が0以下になった場合、プレイヤーの敗北である。フロア画面へ戻るにあたって、プレイヤーの「拾ったアイテムの数」を0にし、プレイヤーが有していたアイテムと同数のアイテムを、迷路中のランダムな座標に再配置する。プレイヤーはそのフロアの初期位置（左上のマス）からゲームを再開することになる。

4.4 コマンド確認画面

登録コマンドとして登録されている n 文字の文字列（パスワード）は、コマンド確認画面で確認することが可能である。この画面には、フロア画面の右下にある「コマンド確認」ボタンを押すことで遷移することが可能である。

今回のゲームにおいては、戦闘画面からはコマンド確認画面に遷移することはできないようにした。このためプレイヤーは、フロア画面内で迷路を探索している間（敵と遭遇して戦闘画面に遷移する前）に、コマンド確認画面を訪れてコマンドを記憶しておく必要がある（何文字記憶するかはプレイヤーの自由である）。

5. 実験

5.1 目的

4章で実装したゲームを用いて実験を行い、提案方式の有効性（パスワード強化要素をゲームに組み込むことで、ユーザが強力なパスワードを容易に覚えることが可能かの実現可能性）を検証する。

5.2 実験条件

被験者は本学情報学部に所属する学生10名、および、クラウドソーシングサービスであるランサーズ[15]を通じて依頼した被験者10名の計20名である。4章で実装したゲームをプレイしてもらった後、アンケートに答えてもらった。その

後、ゲームを通じて覚えたコマンドを覚えているかを1時間後、12時間後、24時間後の計3回の追加実験によって確認した。各被験者には、ゲームをプレイしてもらうことで1,000円を、1回の追加実験ごとに50円を報酬として支払った。

5.2.1 ゲームの設定

被験者が何文字のコマンドを記憶したかを共通の指標で評価するために、登録コマンドは被験者全員で共通の乱数文字列とした。使用される文字は、キーボード入力の容易性の観点から、SHIFTキーを押さずに入力できるキー「abcdefghijklmnopqrstuvwxyz0123456789-`¥@[:;],./」(計47文字)に限定した。これらの文字からランダムに36文字(12Fが最終フロアであるため、敵の体力は最大でも36であり、36文字の入力による攻撃ですべての敵を一撃で倒すことができる)を選んでコマンドとした。具体的なコマンドは「aj-ij51g7rcrsdxipw|sjv1850j48lmk;u;」である。

ゲームの操作方法は、ゲーム開始前に「操作説明書」を読んでもらうことによって被験者に伝えた。また、操作説明書を提供する際に、今回のゲームプレイが学術目的での依頼であることを伝えたくて、ゲーム内で用いるコマンドはテキストファイルやワードファイルにメモ書きせず、必ず記憶(暗記)するよう依頼した。この点を順守したかについては、実験後のアンケートの質問の1つとして被験者本人に確認を行った。

5.2.2 アンケート

実験終了後に行ったアンケートは、以下の質問から構成され、Webページ上で実施される。ただし、紙面スペースの都合上、各質問は要約している。

- ① 年代(10代以下・20代・30代・40代・50代・60代以上)
- ② 性別(男性・女性)
- ③ ゲーム内でコマンドを進んで覚えたか?(非常に進んで覚えた・進んで覚えた・どちらでもない・進んで覚えなかった・まったく進んで覚えなかった)とその理由
- ④ ゲーム内でコマンドが自然に覚えられたか?(とても自然に覚えられた・自然に覚えられた・どちらでもない・自然に覚えられなかった・まったく自然に覚えられなかった)とその理由
- ⑤ N(各被験者がゲームを通じて覚えたコマンドの文字数)文字の乱数パスワードを、今回のようにゲーム内で覚えることは面倒だと思うか?(まったく面倒でない・面倒でない・どちらでもない・面倒だ・とても面倒だ)とその理由
- ⑥ N文字の乱数パスワードを、タイピング方式^{*1}で覚え

ることは面倒だと思うか?(まったく面倒でない・面倒でない・どちらでもない・面倒だ・とても面倒だ)とその理由

- ⑦ N文字の乱数パスワードを覚える作業に対し、今回のようにゲーム内で覚える方式(今回の方式)とタイピング方式を比較して、どちらを利用したいか?(今回の方式・タイピング方式)とその理由
- ⑧ 確認事項:コマンドをメモ書きせず、記憶(暗記)して入力したか?(はい・いいえ)

5.2.3 追加実験

ゲームを通じて記憶したコマンド(パスワード)がどの程度保持されているかを分析するために、ゲームを終了してから数時間経過した後に、再度コマンドを入力する作業(追加実験)をユーザに依頼した。具体的には、以下の手順である。

- ① ゲーム終了後のアンケートを終えた被験者に、追加実験システムのURLを提示する。その際、追加実験の内容(数時間後にコマンドを再度入力すること)を被験者に伝える(ゲームプレイの最中には、被験者には追加実験の内容は伝えられていない)。
- ② 追加実験システムのURLに被験者が「特定の時間帯」にアクセスした場合、コマンド入力画面(図5)が表示される。今回、「特定の時間帯」には、アンケート終了時から
 - (ア)1時間後から3時間以内
 - (イ)12時間後から6時間以内
 - (ウ)24時間後から12時間以内
 の3つの時間帯を設定した。なお、被験者はすべての時間帯でコマンドを入力する必要はない(都合が良い時間帯のみでよい)が、入力しなかった時間帯に関しては報酬は支払われない。

5.3 実験結果

5.3.1 コマンドの記憶

コマンド入力ログを被験者ごとにまとめた結果を表1に示す^{*2}。「最大入力成功桁数」とはユーザがゲーム内で入力に成功したコマンドの長さを指す。表1では、ユーザがゲームプレイ中に入力に成功したコマンドのうち、その最大長を「最大桁数」として掲載した。「入力成功回数」は、ゲームプレイ中に最大桁数のコマンドの入力に何回成功したかを示す。「所要入力回数」は、その最大桁数のコマンドの入力にはじめて成功するまでに何回コマンドを入力した

^{*1} パスワードをテキストファイルやワードファイルへ何度も入力して覚える方法をいう。タイピング方式に関しては、今回は実験を行っていないため、被験者には「タイピング方式を用いて覚える」ことを想定してもらった上で回答をしてもらった。これらの点については、被験者に対してアンケートの質問中で詳細に説明した。

^{*2} 被験者Pについては、ゲームを始めてすぐのコマンド入力(1回目の入力)で36文字の入力に成功していた。入力ログを分析した結果、2回目の入力以降は、1文字から順に増えていったため、1回目のコマンド入力の際には36文字の乱数をメモ書き、あるいは、画面に表示させたまま試しにコマンド全文字を入力してみたものと推察された。したがって、被験者Pの1回目の入力については除外してある。

追加タスク(1回目)

最初のタスクで敵を攻撃するために入力したコマンドを、先頭から(覚えていない限り)出来る限り長く入力してください。
間違っても構いません。

送信

静岡大学西垣研究室

図 5 追加実験画面

Fig. 5 Additional experiment view.

表 1 実験結果

Table 1 Result of game play.

被験者	最大入力成功桁数				総入力回数	総プレイ時間 [分]	追加1		追加2		追加3	
	最大桁数	入力成功回数	所要入力回数	所要時間 [分]			入力桁数	編集距離	入力桁数	編集距離	入力桁数	編集距離
A	36	9	93	33:46	101	45:13					33	8
B	36	4	93	33:40	96	38:39						
C	36	8	20	11:09	66	62:27	36	1			36	1
D	30	81	28	15:50	129	65:03	30	0	30	0	30	0
E	36	5	111	27:42	118	37:27	34	4			34	8
F	36	11	102	30:19	116	41:44	36	3			36	5
G	36	4	138	35:07	142	46:42	36	3			35	2
H	36	59	47	25:38	115	75:15						
I	36	7	116	35:52	122	43:24	36	0	36	0	36	0
J	19	52	139	39:00	190	74:00	19	0	19	1	19	0
K	19	28	93	35:15	176	91:50						
L	36	5	121	34:37	126	56:21	36	0			36	2
M	18	66	50	11:44	143	43:03	18	0	18	0	18	2
N	19	29	144	55:08	173	79:32	12	0	12	0	12	0
O	36	76	34	13:27	112	60:52					36	0
P	23	1	66	18:27	149	44:29	20	0	17	0	13	0
Q	36	2	107	52:59	108	59:49	35	3	35	3	35	3
R	27	23	73	18:34	117	67:42	27	0	27	0	27	0
S	36	6	152	65:36	157	72:43						
T	36	10	78	39:04	87	63:59	36	1				

かを表す。「所要時間」は、ゲームを開始してから、その最大桁数のコマンドの入力にはじめて成功するまでに要した時間である。「総入力回数」と「総プレイ時間」は、ゲームをクリアするまでにコマンドを入力した回数とゲームクリアに要した時間である。「追加1」～「追加3」は追加実験の結果である。空欄は、被験者がその回の追加実験を実施しなかったことを意味している。各追加実験においては、「ゲーム中で覚えたコマンドをできる限り長く先頭から入力する」よう依頼している。「入力桁数」とは、その依頼に応じて被験者が何文字の長さのコマンドを入力したか（最大36）を表している。「編集距離」はその入力がどの程度正確であったかを表す値である。具体的には、被験者が入力したコマンドの長さLに対して、ゲーム中に入力したコマンド（36文字）の1文字目からL文字までの部分文字列を抽出した後、被験者が入力したコマンドとその部分文字列間のレーベンシュタイン距離を求めた値である。

表1の結果から、多くの被験者が1時間程度のゲームプレイを通じて18～36文字のランダム文字列を記憶できたことが分かる。

5.3.2 アンケート結果

被験者から得られたアンケート結果を表2に示す。紙面の都合上、質問③～⑥は、選択肢を5段階の数値に変換してある（質問③は、5：非常に進んで覚えた、4：進んで

表 2 アンケート結果

Table 2 Result of questionnaire.

被験者	①	②	③	④	⑤	⑥	⑦
A	20	女	5	4	4	1	今回の方式
B	20	男	4	5	1	1	今回の方式
C	20	男	4	4	4	3	今回の方式
D	20	女	5	5	4	2	今回の方式
E	20	男	3	5	3	1	今回の方式
F	20	男	4	4	4	2	今回の方式
G	20	男	4	4	4	2	今回の方式
H	40	男	5	2	1	2	タイピング方式
I	20	男	4	4	4	2	今回の方式
J	40	男	4	4	1	2	今回の方式
K	20	女	3	4	3	2	今回の方式
L	20	男	5	4	4	2	今回の方式
M	20	男	4	4	4	2	今回の方式
N	40	男	3	4	2	3	タイピング方式
O	20	男	4	4	5	2	今回の方式
P	20	男	2	5	2	2	タイピング方式
Q	30	男	4	5	4	2	今回の方式
R	30	男	4	4	2	1	今回の方式
S	30	女	4	4	1	2	今回の方式
T	20	男	5	4	5	4	今回の方式

覚えた、…、1：まったく進んで覚えなかった。質問④は、5：とても自然に覚えられた、…、1：まったく自然に覚えられなかった。質問⑤⑥は、5：まったく面倒でない、4：面倒でない、…、1：とても面倒だ。質問⑧は、全被験者が「はい」であった。

以下に、質問③～⑦の「理由」を記載する欄に被験者が記した回答をまとめる。各回答の末尾のアルファベットは回答者（被験者A～T）を表している。誌面のスペースの関係上、各回答は必要に応じて要約してある。また、同じ主旨の回答についてはグループ化し、代表的な回答を1つ選んで全回答者のアルファベットとともに掲載するようにした。

質問③「コマンドを進んで覚えたか」は、ゲーム性がコマンドを覚えようとする動機付けに寄与するかを評価するための質問である。

質問③において、「非常に進んで覚えた」または「進んで覚えた」を選択した被験者の理由は、

- 覚えたほうが一撃で敵を倒せるから (A, B, C, F, G, I)
- コマンドを18文字まで覚えれば、すべての敵を2ターン以内に倒すことができ、効率が良かったから (M)
- 自分のキャラクタをより強くしたいと思ったため (O)
- 早いうちから何度もコマンドを繰り返して覚えるのが得策だと考えたから (J, R)
- 覚えないとモンスターに勝てないから (D, L, Q, S, T)
- 覚えるようにという指示だったから (H)

だった。被験者 H については、「覚えることを強要された」という意味の理由であるため、本人は「進んで覚えた」を選択しているが、実際には「進んで覚えなかった」という意図であると考えられる。

「どちらでもない」または「進んで覚えなかった」を選択した被験者の理由は、

- 覚えられるのも限界があったため、初めからここまでは覚えよう、と決めていた (K)
- 敵を倒せる数だけ覚えればよいと思ったので、必要と思われるところまで覚えた (E, N)
- 何回も入力するうちに覚えてしまった (P)

だった。被験者 P については、「自らが進んで覚えようとするまでもなく、いつの間にか覚えてしまっていた」という意味の理由であるため、質問④との勘違いであると考えられる。

質問④「コマンドを自然に覚えたか」は、ゲームの中で繰り返されるコマンド入力コマンドの記憶を容易にしたかを評価するための質問である。

質問④において、「とても自然に覚えられた」または「自然に覚えられた」を選択した被験者の理由は、

- 敵にエンカウントするたびにコマンドを繰り返し入力していたら覚えられた (B, E, N, K, P, Q, R, S)
- 敵が強くなるにつれてパスワードを少しずつ覚えて行けたから (A, D, J, L, O, T)
- 敵を倒したいという欲求とコマンドを覚えることが直結していたから (I)
- ゲームの楽しさで、あまり意識していないうちに覚えることができていたから (G)
- コマンドを 3 文字くらいずつに分けていくと、まとまったリズムのように感じられて、覚えやすい (M)
- 敵を倒すために必要だったため (F)
- 覚えようと考えて覚えたので (C)

だった。被験者 F については、コマンドを記憶するにあたっての動機を答えているため、質問③との勘違いであると考えられる。被験者 C については、「意識して覚えた」という意味の理由であるため、「自然に覚えられたか」という質問文を「覚えようと意識しなくても覚えられたか」という意図だと勘違いしたのである。

「自然に覚えられなかった」を選択した被験者の理由は、

- 関連はなかったから (H)

だった。「自分の実際の生活には何の関わりもない文字列であるため、覚えようと思って覚える必要があった」という意味だと思われるので、被験者 C と同様、質問文を「覚えようと意識しなくても覚えられたか」という意図だと勘違いしたのである。

質問⑤「乱数パスワードを覚える場合、今回の方式を面倒だと思うか？」において、「まったく面倒でない」または「面倒でない」を選んだ被験者の理由は、

- ゲームをしながら覚えられるので楽しいため (A, D, G, I, M)
- 暇つぶしにゲームをやっている間に覚えることができるため (L, O, Q, T)
- ゲームの要素が入っているので、多少は楽しく覚えられのかもしれないと思ったから (ただし、今回のゲーム自体はあまり面白いとは思わなかった) (C)
- 覚えるという目的以外にゲームをクリアするという目的があったため (F)

だった。

「どちらでもない」または「面倒だ」または「とても面倒だ」を選んだ被験者の理由は、

- ゲームをしているうちに覚えられるのであれば、面倒ではないだろうが、これはゲームの内容や面白さに依存すると思う (E)
- 何度もタイピングするときがあり、面倒だという考え方はあったが、同時に達成感もある (K)
- ゲームに時間がかかるから (B, H, J, P)
- 結構時間がかかったし、ゲームとしてはそれほど面白いものではなかった (N)
- 暗記のためだと思うとたとえゲームでも苦痛を感じる (R)
- 覚えなくてはならないと思うとなかなか頭に入ってこなそう (S)

だった。

質問⑥「乱数パスワードを覚える場合、タイピング方式を面倒だと思うか？」において、「面倒でない」または「どちらでもない」を選んだ被験者の理由は、

- タイピングもタイピングゲームとしてとらえれば、負荷に感じないと思うから (T)
- 覚える必要があるならどちらでもない (C)
- ゲームよりは時間がかからないと思うが、覚えるためにやるとなると面倒ではないとはいえないので (N)

だった。

「面倒だ」または「とても面倒だ」を選んだ被験者の理由は、

- ひたすら写経して覚えさせられるのは面倒であり苦痛である (A, D, E, G, K, L, M, P)
- モチベーションが上がらない (F, Q, S)
- 面白みがないから (I, O)
- タイプミスのチェックを自分でしなければならないから (J, R)
- 何度も入力して覚えたパスワードでも、そのパスワードを何度も使う機会がない場合などはいずれにせよすぐに忘れてしまう (B)
- タイプしなくても覚えられパスワードにするから (H)

だった。被験者 B と H は、質問⑥の意図を誤解したと思

われる。

質問⑦「乱数パスワードを覚える場合、今回の方式とタイピング方式どちらがよいか？」において「今回の方式」を選んだ被験者の理由は、

- 何もなく淡々と覚えるよりは、ゲーム要素があったほうが飽きずに楽しんで覚えられる (A, G, I, L, O)
- ゲーム感覚で達成感を求めてプレイしながら覚えていくことの方が続けられると思う (K, Q)
- 何か目的があったほうが覚えやすいから (B, F, M)
- 今回の方式の方がまだ退屈や苦痛な作業をとまわずに覚えられるように感じたから (D, E, S, T)
- もう少しゲームとして楽しいなら迷わず今回の方式を選ぶが、現状のものではどちらでもよい (C)
- コマンド入力以外のイベントやタスクがあるおかげで、コマンド想起時の脳の負荷が高くなっているように感じた。こちらの方が記憶に残りやすい気がする (R)

だった。

「タイピング方式」を選んだ被験者の理由は、

- ゲームをするのは面倒くさいから (H, P)
- ゲーム方式だと途中でゲームを中断するとまた初めからやり直さなければならないから (J)
- 時間がかからないと思うし、繰り返し連続でタイピングすると手(指)の感覚で覚えてくると思うので (N)

だった。

6. 実験結果に関する考察

6.1 強力なパスワードを記憶できたか

文献 [16] で, Bonneau らが文字列パスワードは 56 bit 長のエントロピを持たせることで, 攻撃者の総当たり攻撃にかかるコストを限りなく高くできることを示している^{*3}. 今回の実験では, 表 1 に示したとおり, ほとんどの被験者が少なくとも 18 文字の乱数列 (コマンド) を 2 回以上入力することに成功している. 被験者 P に関しては, 23 文字の入力成功は 1 回のみだったが, 21 文字の入力は 5 回成功していた. 成功した乱数列は 47 種の文字から構成されているため, 18 文字の乱数列のエントロピは約 100 [bit] である. 本結果は, ユーザはゲームを通じて強力な乱数列パスワードを (少なくともゲームをしている間は) 記憶可能であることを示している.

6.2 パスワード記憶に対するモチベーション

タイピング方式のパスワード記憶の場合も, ユーザが「強力なパスワードを覚えたい」という高いモチベーションをもって継続的に取り組めば, 30 文字程度の乱数パスワード (強力なパスワード) を記憶することは不可能ではないであろう. しかし, アンケートの質問⑥の結果のとおり, 多

くの被験者はタイピング方式によって乱数パスワードを覚えることは面倒だと認識している. これは, 単にパスワード強化という目的だけでは, ユーザは強力なパスワードを記憶する努力を許容することができない傾向にあることを示している.

これに対し, 提案方式は, ゲームにパスワード強化要素を組み込むことによって, ユーザのモチベーションをゲームへと向かわせている. アンケートの質問⑤の結果では, 過半数の被験者が, ゲームで乱数パスワードを覚えることを「まったく面倒でない」, 「面倒でない」と回答しており, その理由を「楽しいから」, 「ゲームの達成感がある」などと述べている.

その一方で, 提案方式を面倒だと回答した被験者も一定の割合で存在した. その理由は「今回プレイしたゲームが面白くなかった」, 「そもそもゲームをするのが面倒」という 2 つの理由に大別される. 前者については, 今回利用したゲームのゲーム性が低かった (シンプルなゲームだった) ことが原因であると考えられる. 後者については, ふだんからゲームを行わない被験者の回答である可能性が高い.

以上の議論より, 提案方式は, ユーザのモチベーションをゲームへ向けることに一定の割合で成功しており, 乱数コマンド (パスワード) を覚える心理的負荷を小さくすることに十分に貢献しているといえよう. この結果は, 質問⑦で実際に提案方式とタイピング方式を比較した際, より顕著に表れており, 多くのユーザが提案方式を好意的に受け止めている. ただし, 今回のゲームを楽しめなかった被験者やふだんからゲームをしない被験者にとっては, その効果は限定的であったといえる. 前者の被験者に対しては, 多数のゲームを用意する (ユーザが自身の楽しめそうなゲームを選択できる) ことによって提案方式の恩恵を与えることが可能であろう. 後者のユーザに対しては, 「ゲーム」以外のエンターテインメント要素の活用を模索する必要がある.

6.3 パスワードを容易に記憶できたか

今回の実験結果から, 多くのユーザがゲームをする中で容易に乱数パスワードを覚えることができているといえるだろう. 実際, 質問④では多くの被験者が, コマンドはゲームをプレイする中で覚えることができたと回答している.

アンケートの質問③の結果より, 被験者はゲーム内でコマンドを積極的に記憶・入力しており, その理由を「覚えなくてクリアできないから」, 「ゲームを素早くクリアするため」, 「自分のキャラを強くしたいと思ったため」と回答している. すなわち, ユーザはコマンドを入力する理由を主に「ゲームを進めるため」と認識していたと考えられる.

また, 一部のユーザは「一度に覚えるのではなく, 敵を 1 回で倒せる程度にコマンドを覚えていった」のような回

^{*3} 乱数列であるため, 辞書攻撃や推測攻撃にも耐性を有している.

答をしている。長い文字列を覚える際には、覚える文字列を徐々に増やしていくことが効率的である。今回のゲームでは、徐々に敵を強くしていくことで、ユーザに効率良く乱数列を覚えさせるように導いていることが分かる。

さらに一部の被験者は、「一撃で敵を倒すため」に長い乱数列をコマンドとして打ち込んでいる。通常、ユーザに対して長い乱数列を記憶させるのは非常に困難な要求である。これは、「敵を倒す」というゲーム性を利用した本提案方式ならではの効果であるといえよう。

6.4 リワードの効果

今回実装したゲームでは、被験者は最低 12 文字のコマンドを覚えればゲームをクリアすることが可能である^{*4}。ただし、より長いコマンドを入力することによって、より大きなダメージを敵に与えることが可能であり、ゲームを有利に進めることが可能である。

表 1 のとおり、すべての被験者が必要文字数 (12 文字) より多くのコマンドを記憶している。大多数のユーザは 30 文字以上記憶をしており、その理由を「手早くクリアしたかったため」、「敵を一撃で倒せる」、「より強くしたかった」という理由を述べている。これは、リワードの効果が顕著に表れた結果であるといえよう。

一方で、「18 文字まで覚えれば、効率が良いと思った」、「初めからここまで覚えよう」、「必要と思われるとここまで覚えた」などの理由で、できるだけ長いコマンドを記憶しようとは思ったが、その長さに限度を設けていたユーザも存在した。ただし、これらのユーザも、最低文字数よりは長い文字数を覚えているため、一定のリワード効果は表れている。

以上の議論より、提案方式におけるリワードの要素は、ユーザに強いパスワードを記憶させることに寄与しているといえるだろう。引き続き、リワード要素が存在しないゲームとの比較やリワード要素のパラメータを変更した場合と比較実験を行うことで、リワードの効果についてより詳細な分析を行いたい。

6.5 記憶したパスワードを保持できているか

表 1 に示したとおり、1 回目の追加実験 (1 時間後) では 14 名中 8 名 (57%) の被験者が、2 回目の追加実験 (12 時間後) では 8 名中 6 名 (75%) の被験者が、3 回目の追加実験 (24 時間後) では 15 名中 7 名 (47%) の被験者が、正確にコマンド (パスワード) を入力できている。したがって、提案方式を 1 回プレイして覚えたコマンドは、1 日間程度であれば、約半数のユーザが記憶し続けているといえる。

誤って入力されたコマンドに対して、編集距離を求めた上で、誤った理由を分析したところ以下の 3 つの理由に大別された。

- (1) 入力ミス。たとえば、被験者 J は、2 回目の追加実験では 1 文字の編集距離で誤っているが、3 回目の追加実験では、その誤りが起きていない。
- (2) 入力コマンドの機微な記憶誤り。編集距離が 1~3 の場合は、この間違いがほとんどであった。
- (3) 記憶したチャンクの抜け落ち。一部の被験者は、連続した数文字が抜け落ち、その部分を除いた文字列は正確なコマンドを入力していた。これは、被験者がコマンドをチャンクに区切って覚えており、追加実験時には一部のチャンクを忘却していたことが原因であると推測される。

このうち、(1) については、通常のパスワード認証時と同様に、コマンドを入力した際に正解/不正解を表示することで改善が可能である。(2) または (3)、あるいはその両方を原因として間違えている場合に対しては、今後対策を講じていかなければならない。ただし、すべての文字を完全に記憶できてはいない被験者も、文字列の大部分は正確に記憶できている。記憶を長期間定着させるための手段として、数日間にわたって決まった時間に今回のゲームをプレイさせることがあげられる^{*5}。

6.6 注意点

今回は、報酬をとまなう「仕事」という形でユーザに評価実験への参加を依頼している。したがって、ゲームをプレイする本当の目的が「報酬を得るため」だった被験者も少なくないだろう。実際、一部の被験者は、アンケートにて「(コマンドを入力するのは) 覚えるようにという指示だったから」という回答を寄せている。

提案方式の評価においては、「乱数パスワードを覚えた状況下のユーザ」あるいは「当該ゲームで遊びたいユーザ」に対して、そのゲームを与えて評価実験を実施することが理想である。しかし、そのようなユーザを被験者として集めることは現実問題として不可能である。本論文の実験結果は、この制約の条件下で、仕事として実施した被験者の結果であることをふまえなければならない。

7. その他の考察

7.1 ゲーム開発者へのライブラリ提供

ゲーム市場に関する最近の特記事項として、スマートフォンゲームの爆発的な増加がある [5]。スマートフォンゲームは、個々のアプリ開発者が自由にゲームを作り、世

^{*4} プレイヤの体力は 30 であり、攻撃による敵との接触の度に 10 のダメージを負うため、プレイヤは敵への攻撃を 3 回行うことができる。敵の体力の最大値が 36 であるため、12 文字のコマンドによる攻撃を 3 回行うことによってすべての敵を倒すことができる。

^{*5} 今回の評価実験においては、ゲームを通じてパスワードを記憶することで「強力なパスワード」を「容易に」記憶できることの実現可能性を検証することが主目的である。したがって、これを検証するための必要最小限の設計になっており、ゲームは 1 回しかプレイさせていない。

界中に公開することができる。提案手法においては、ゲームの中にパスワード強化の要素を組み込むための共通モジュールを「パスワード強化ライブラリ」として、アプリ開発者に公開することで、開発者にとって開発コストを下げる事が可能である。この結果、ゲームアプリ開発者は、これらのパスワード強化ライブラリを自由に使って、パスワード強化のためのゲーム要素を自身が作成するゲームに容易に組み込むことが可能となる。すでに作成済みのゲームに後からセキュリティ強化要素を組み込むことも可能である。

ゲームアプリ開発者はパスワード強化ライブラリを使って、自身が作成したゲームを自由に拡張することが可能である。多くのゲームアプリ開発者がパスワード強化のための要素を組み込んだゲームを開発して公開するようになれば、ゲーム市場にパスワード強化を促すゲームが多数流通するようになり、ゲームを通じたパスワードの強化が効果的に達成される。

7.2 開発者の不正行為

提案方式は、パスワードそのものをコマンドとしてゲームに入力させているため、ゲーム開発者によるパスワードの不正取得に対する懸念がある。たとえば、外部と通信可能なゲームであれば、ゲーム中で取得したパスワードを、ユーザに無断で外部のサーバに送信することで、ユーザのパスワードを外部に曝露することが可能である。本件に対する防止策も今後の課題である。たとえば、パスワード強化要素が組み込まれたゲームを一般公開する前に、アプリマーケットがゲームのソースを審査する枠組みを設ける対策が考えられる。

7.3 ゲームへのパスワード入力に対する嫌悪感

提案方式では、ゲーム画面にユーザが入力したコマンドが表示されている。したがって、入力している最中に、他人が自分のゲーム画面を覗き見た場合、(将来的にパスワードとして利用する) コマンドが第三者に知られてしまう危険性を有している。仮に画面上のコマンドを*マークで隠したり、表示しなくしたりしても、何度も入力シーン(たとえば、キーボード)を見る間に、コマンドを推測される可能性も十分にあるだろう。また、パスワードは本来、ユーザにとって他人の目に触れさせたくないものである。パスワードに相当するコマンドを何度もゲームへ入力すること自体に嫌悪感を覚えるユーザも少なくないかもしれない。これら2点の対策について、今後早急に検討を進め、対策を講じる必要がある。

8. まとめと今後の課題

本論文では、エンターテインメントにセキュリティ因子を導入するというアプローチによる「セキュリティとエン

ターテインメントの融合」について論じた。その第1報として、「ゲーム」により「パスワード認証」を強化する手法を提案した。実際にユーザ実験を通じて、提案方式がユーザに強度が高いパスワードを記憶させることに寄与することを確認した。

今回は「ゲーム」と「パスワード認証」に焦点を当てたが、これ以外の応用を検討することが今後の課題である。提案方式の有効性のさらなる検討を行うために、より大規模かつ長期的な実験の実施も必要である。ただし、本質的な問題としてゲーム開発者の不正、コマンド入力に対するのぞき見の脅威が課題として残っており、提案方式を安全に運用するためにはこれらの解決を行う必要もある。

謝辞 実験システムで利用した画像は、エトリエ(<http://etolier.webcrow.jp/>)等で公開されているフリー素材です。実験環境の準備にあたって、静岡大学土屋貴史氏、佐野純音氏にご協力をいただきました。また、査読者の皆様には、実験結果の分析に関して非常に的確なアドバイスをいただきました。この場を借りて御礼申し上げます。

参考文献

- [1] 可児潤也, 鈴木徳一郎, 上原章敬ほか: 4 コマ漫画 CAPTCHA, 情報処理学会論文誌, Vol.54, No.9, pp.2232–2243 (2013).
- [2] Mohamed, M., Gao, S., Saxena, N., et al.: Dynamic Cognitive Game CAPTCHA Usability and Detection of Streaming, Based Farming, *Proc. USEC '14* (2014).
- [3] 小島悠子, 山本 匠, 西垣正勝: 間違い探しを利用したワнтаイム・パスワード型画像認証の提案, 情報処理学会研究報告, 2007-CSEC-36-64, pp.375–380 (2007).
- [4] 黒沢秀太, 金岡 晃: より強いパスワード設定へと導くパスワードメータの提案, 情報処理学会研究報告, Vol.2014-SPT-8, No.34 (2014).
- [5] 株式会社 CyberZ: CyberZ、スマホゲーム市場調査を実施。2013 年スマホゲーム市場規模は国内ゲーム市場全体の約 5 割に到達 (オンライン), 入手先 (<http://cyber-z.co.jp/news/pressreleases/2014/0325.1497.html>) (参照 2014-08-21)。
- [6] Ahn, L.V.: Games With A Purpose, *IEEE Computer Magazine*, Vol.39, No.6, pp.96–98 (2006).
- [7] Ahn, L.V. and Dabbish, L.: Labeling Images with a Computer Game, *Proc. CHI 2004*, pp.319–326 (2004).
- [8] トレンドマイクロ株式会社: パスワードの利用実態調査 2014—約 7 割が自分のパスワード管理にセキュリティ上リスクがあると認識 4 割以上がパスワードを手帳やノートにメモして管理 (オンライン), 入手先 (<http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20140609010140.html>) (参照 2014-08-21)。
- [9] 平野 亮, 森井昌克: パスワード運用管理に関する考察および提案とその開発, 電子情報通信学会, 信学技報 ISEC2011-53, pp.129–134 (2011).
- [10] Stobert, E. and Biddle, R.: The Password Life Cycle: User Behaviour in Managing Passwords, *Proc. SOUPS2014*, pp.243–255 (2014).
- [11] Chiasson, S., Oorschot, P.C.V. and Biddle, R.: A Usability Study and Critique of Two Password Managers, *Proc. 15th USENIX Security Symposium* (2006).
- [12] Howe, J.: The Rise of Crowdsourcing, *WIRED magazine*

- (online), available from <http://archive.wired.com/wired/archive/14.06/crowds.html> available from (2014-08-24).
- [13] Foldit, available from <http://fold.it/portal/> (accessed 2014-08-25).
- [14] Brooke, J.: SUS: A Retrospective, *JOURNAL OF US-ABILITY STUDIES*, Vol.8, No.2, pp.29-40 (2013).
- [15] Lancers (online), available from <http://www.lancers.jp/> (accessed 2016-03-06).
- [16] Bonneau, J. and Schechter, S.: Towards reliable storage of 56-bit secrets in human memory, *Proc. 23rd USENIX Security Symposium*, pp.607-623 (2014).
- [17] 会田和弘：セキュロくキッズ—双六を用いた情報セキュリティ教育の試み，総合政策研究，Vol.46, pp.89-94 (2014).
- [18] 情報処理推進機構：映像で知る情報セキュリティ—映像コンテンツ一覧，入手先 <https://www.ipa.go.jp/security/keihatsu/videos/> (参照 2016-07-13).
- [19] 学研キッズネット：まんがひみつ文庫「サイバーセキュリティのひみつ」，入手先 <https://kids.gakken.co.jp/himitsu/111/index.html> (参照 2016-07-24).
- [20] 情報処理推進機構：パスワード—もっと強くキミを守りたい—，入手先 <https://www.ipa.go.jp/security/keihatsu/munekyun-pw/> (参照 2016-07-24).

推薦文

ゲームを用いて，品質のよいパスワードを無意識に記憶させるアイデアは，人間の記憶や振る舞いを決める因子とした新たな着目点であり，その価値が認められるため推薦したい。

(コンピュータセキュリティシンポジウム 2014

プログラム委員長 井上大介)



西垣 正勝 (正会員)

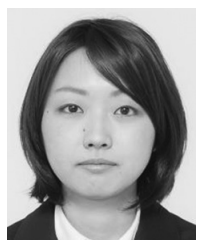
1990 年静岡大学工学部光電機械工学科卒業。1992 年同大学院修士課程修了。1995 年同博士課程修了。日本学術振興会特別研究員 (PD) を経て，1996 年静岡大学情報学部助手。同講師，助教授の後，2006 年より同創造科学技術大学院助教授。2007 年同准教授，2010 年同教授。博士 (工学)。情報セキュリティ全般，特にヒューマンクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事。2013-2014 年情報処理学会コンピュータセキュリティ研究会主査。2015 年より電子情報通信学会バイオメトリクス研究専門委員会委員長。



藤田 真浩 (学生会員)

2013 年 3 月静岡大学情報学部情報科学科卒業。2015 年 3 月同大学院修士課程修了。現在，同創造科学技術大学院博士後期課程。情報セキュリティ，ヒューマンインタフェースに関する研究に従事。2016 年度情報処理学会山

下記念研究賞受賞。



山田 眞子

2015 年 3 月静岡大学情報学部情報社会学科卒業。在学中，情報セキュリティに関する研究に従事。