エンターテイメントを活用したセキュリティ強化：ユーザ認証の強化を導くルーチンのゲームへの埋め込み

山田眞子† 藤田真浩†† 有村汐里†† 池谷勇樹†† 西垣正勝††

†静岡大学情報学部 432-8011 浜松市中区城北 3-5-1
††静岡大学大学院情報学研究科 432-8011 浜松市中区城北 3-5-1

あらまし 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一つとして，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．本稿では，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．その第一報として，ゲームで遊んでいるうちにユーザが自然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具体化する．

Security enhancement achieved in entertainment: Embedment of routines to enhance password authentication in games

Mako Yamada† Masahiro Fujita†† Shiori Arimura†† Yuki Ikeya††

Masakatsu Nishigaki††

†Faculty of Informatics, Shizuoka University,
3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan
††Graduate school of Informatics, Shizuoka University,
3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan

Abstract As one way to achieve the security enhancement that give consideration to human factors, combining security with entertainment has been proposed. For the purpose of improving safety and usability of security systems, attempts to embed entertainment factors in security technology have been reported. In this paper, we propose a new approach to improving the skills and security awareness of users by embedding security factors in entertainment. As the first step, we designed a system that enables users to memorize a strong password naturally while playing a game.

1. はじめに

情報システムは人（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遺憾ながら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．その一つの試みとして，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行われていない．そこで本稿では，後者の「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」に対する検討を行う．

今回はその第一報として，ユーザにとって最も身近なエンターテイメントの一つである「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自然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．

本稿の構成は次のとおりである．2 章でエンターテイ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 章で提案手法に対する考察を行い，6 章でまとめと今後の課題を述べる．

2. セキュリティとエンターテイメント

2.1 既存研究

セキュリティとエンターテイメントの融合に関する既存研究を概説する．

文献[1]の 4 コマ漫画 CAPTCHA では，

図 1 DCG CAPTCHA の例[2]

「CAPTCHA」というセキュリティ技術に「4 コマ漫画の並び替え」というエンターテイ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ドラッグし，海の上に配置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[16]評価の平均スコアは 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．

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）が混入されており，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得るため，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）楽しさの持続と認証のワン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（露出度の高い女性の画像）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，エンターテイメントと正規業務との親和性は決して高くはない．たとえば，ユーザが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，セキュリティ技術の利便性や安全を直接改善するために，セキュリティ技術の中にエンターテイ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自然に向上させ，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メントの融合が実効的なものとなると期待される．

3. 提案方式

3.1 コンセプト

本稿では，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の第一報として，「ゲーム」というエンターテイメントに「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自然にセキュリティ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．

3.1.1 ゲームの利用

近年，スマートフォンの普及に伴い，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メントの一つであると考えられる．そこで本稿では，エンターテイメントとして「ゲーム」に焦点を当てる．

ゲームの利用は，ヒューマンコンピュテーション[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）または目的を伴ったゲーム（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，ユーザはゲームで遊んでいるうちに，気付かないままコンピュータのタスクを支援しているという状況が実現されている．これは，「ユーザがゲームで遊んでいる内に，自然にセキュリティ意識やスキルを高める仕組みを提案する」という本稿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激増し，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全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用な要件である．そこで本稿では，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一つとして，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一例である．）

ゲーム内でコマンドを繰り返し入力しているうちに，コマンドを記憶し（手が覚え），意識せずともそのコマンドを入力できるようになることは，ゲームのプレイヤなら誰しもが経験することである．ここで，コマンドを「パスワード」として捉えれば，ユーザはゲームの中でパスワード（コマンド）を無意識のうちに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において，キャラクタ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自然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．本稿における「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．

長くて複雑なコマンド（パスワード）であるほど，ユーザにより高いリワードが与えられる．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．

コマンドはいつでも再登録が可能であり，ユーザは，現在のコマンドに慣れてきたら，より複雑なコマンドを登録し直すことができる．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自然にそれを記憶できるようになることが期待される．

4. ゲームの開発

4.1 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，世界中に公開することができる．そこで，本稿では，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．既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．

パスワード強化ライブラリに含まれるモジュールの例を以下に示す．

【クラス：Password】
・メンバ変数：string password
　パスワードを格納する変数．
・メソッド：void set (string)
　引数を password に格納する．
・メソッド：double getStrength()
　登録済みのパスワード（password）の強度を取得する．
　強度の算出には，既存のパスワード強度メータ[14][15]を利用することができる．
・メソッド：bool equal(string)
　引数が登録済みのパスワード（password）と一致しているかどうかを調べる．

【パスワード登録関数：RegisterPassword()】

```
Password RegisterPassword(){
        Password pwd = new Password();
        string command;
        /*  ユーザにコマンドの入力を促す  */
        command = inputCommand();
        /*  パスワードを登録  */
        pwd.set(command);
        /*  登録済みパスワードを返す  */
        return pwd;
}
```

【パスワード検査関数：VerifyPassword()】

```
double VerifyPassword(Password pwd){
        string command;
        /*  ユーザにコマンドの入力を促す  */
        command = inputCommand();
        /*  入力されたコマンドが登録済みパスワードと一致する場合は  */
        if (pwd.equal(command) == true) {
        //  パスワードの強度を返す
        return(pwd.getStrength());
        } else {
        //  エラーを返す
        return(ERROR);
        }
}
```

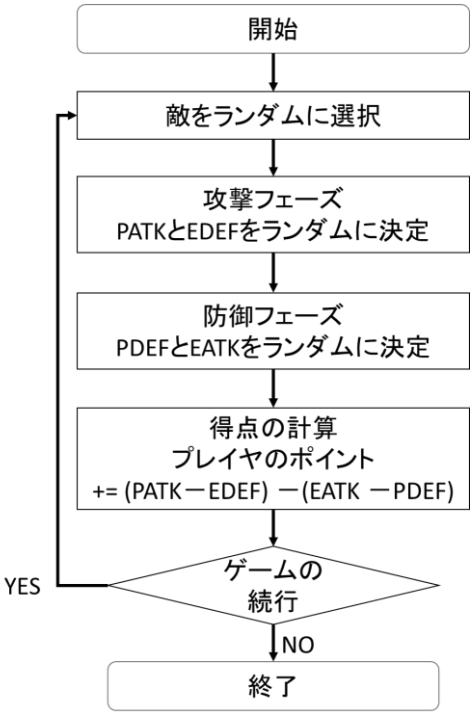

図 2 オリジナルのゲーム例

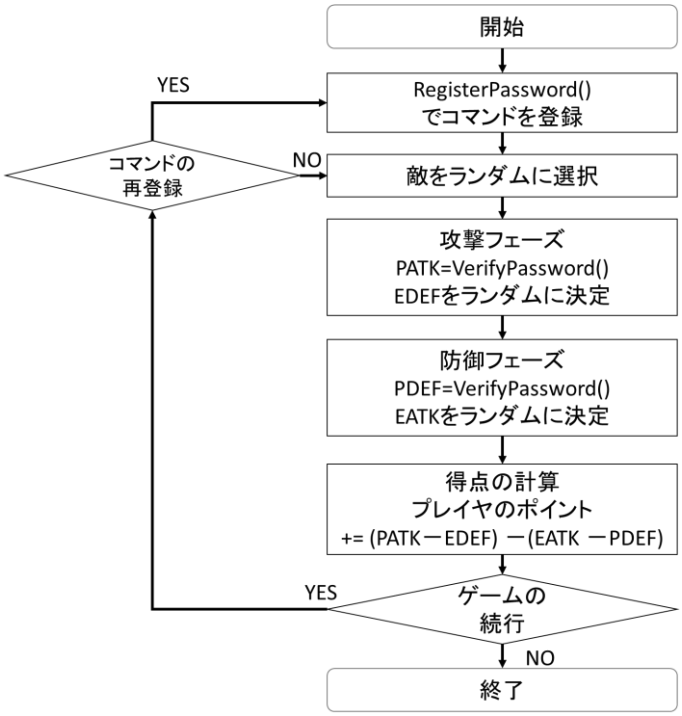

図 3 パスワード強化要素を組み込んだゲーム例

4.2 ゲームの実装例

ここでは，単純なゲームを例に，4.1 節で示したパスワード強化ライブラリを使って，プレイヤにパスワードの強化を促す要素を組み込んだゲームの開発について説明する.

図 2 は，ゲームにおける「敵との戦闘アルゴリズム」を示したフローチャートである. 毎回の敵がランダムに選ばれ，プレイヤと敵が交互に 1 回ずる攻撃と防御を実行する. プレイヤの攻撃フェーズでは，プレイヤの攻撃力 PATK と敵の防御力 EDEF がランダムに決められる. 敵の攻撃フェーズでは，プレイヤの防御力 PDEF と敵の攻撃力 EATK がランダムに決められる. その上で，プレイヤの攻撃成功ポイント(PATK－EDEF)と防御成功ポイント(PDEF－EATK)が，プレイヤの得点に加算されていく.

図 2 のゲームに対して，パスワード強化の要素を組み込んだ例が図 3 のフローチャートである. 図 3 では，図 2 に対して，プレイヤの攻撃力および防御力を高めるコマンド(パスワード)が導入されている. 図 3 に示されているように，ゲームアプリ開発者は，ゲームの最初または途中に「プレイヤがコマンド(パスワード)を登録するための関数 RegisterPassword()」を追加し，プレイヤの攻撃力と防御力を決定するフェーズで「プレイヤがコマンド(パスワード)を正しく入力できたか検査するための関数 VerifyPasspword()」を追加するだけで，オリジナルのゲーム(図 2)にパスワード強化のための要素を組み込むことができるようになっている.

5. 考察

5.1 パスワード強化に対する実効性

5.1.1 パスワードの記憶

ユーザは，ゲームの中でコマンド(パスワード)を幾度となく入力するうちに，いつの間にかそのコマンドを覚えていく. すなわち，ユーザは，日常生活においてゲームで遊んでいるうちに，自然に強度の高いパスワードの記憶が促される.

ユーザ(プレイヤ)にとっては，パスワードを入力しているという認識はなく，ゲーム攻略のために「コマンド」を入力しているに過ぎない. コマンド入力によって得られるリワードが，パスワ

ード強化の促進とゲーム性の向上を同時に引き出している．また，ユーザは，ゲームを有利に進めたいという気持ちがあるため，最初の登録時から複雑なコマンドを登録しようと努力するはずである．同様の理由で，ユーザは，コマンドを覚えるということに対してそれほど苦痛を感じないことが期待される．

5.1.2　パスワードの逐次強化

より長いパスワードを覚えるために，覚えるべきパスワードを徐々に長くしていく方法が有効である場合も多い．提案方式においては，パスワードの強度に応じたリワードをユーザに供与することによって，パスワードの逐次強化をサポートしている．

たとえば，コマンド「axdegh」を登録したユーザを考えよう．このユーザは，ゲームで遊んでいるうちに，いつかコマンド「axdegh」を記憶することができるようになるであろう．そして，その時点で，更に高いリワードが得られるようにコマンドを更新すると考えられる．その際，このユーザにとって容易な方法は，既に覚えているコマンド「axdegh」の末尾にもう 1 文字を付加し，たとえば「axdeghz」というコマンドへと拡張することである．

「axdegh」というコマンドを記憶しているユーザにとって，最後に 1 文字増えただけのコマンド「axdeghz」を覚える際の記憶負荷はそれほど高くないことが期待される．これを繰り返すことで，最終的には十分に長くて複雑なコマンド（パスワード）を，効率良く記憶することが可能であると期待される．

5.1.3　ゲームアプリの豊富さ

4.1 節の「パスワード強化ライブラリ」並びに，4.2 節の図 2 および図 3 はあくまでも一例である．これ以外にも，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．

5.2　不正行為への対応

5.2.1　ユーザの不正

提案方式に対するユーザの不正として，「コマンドをメモにとる行為」「あらかじめコマンドをコピーしておき，ゲームプレイ時にペーストを繰り返す行為」の二つが予想される．これらの不正は，ユーザによるコマンド（パスワード）の記憶を阻害することになるため，対策が必要である．根本的な対策は今後の課題であるが，現時点では次のような対策を考えている．

コマンドをメモにとる行為に関しては，コマンドの「入力時間」をリワード算出の際の一要素として利用する対策が考えられる．ユーザがより高いリワードを得るためには，より高速にコマンドを入力しなければならない．メモを見ながらコマンドを入力する場合，「メモを見て書かれている内容を確認する」という動作が加わるため，記憶したコマンドを入力するよりも，多くの入力時間を要する見込みが高い．したがって，より高いリワードを得たいプレイヤは「メモをとる」という選択を捨てるのではないかと期待される．

コマンドのコピーアンドペーストに関しては，コマンドの入力フォーム上でのペーストを不可とする対策が考えられる．

5.2.2　ゲーム開発者の不正

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が，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．

6. まとめと今後の課題

本稿では，エンターテイ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メントの融合」について論じた．その第一報として，「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．本方式により，ユーザは日常生活においてゲームで遊んでいるうちに，自然に強度の高いパスワードを記憶することが可能となる．

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していきたい．ただし，本質的な問題としてゲーム開発者の不正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その解決が急務である．また，提案方式に従うことでユーザが本当にパスワードの記憶ができているかなど評価実験を行い，提案方式の有効性を測る必要もある．

参考文献

[1] 可児潤也，鈴木徳一郎，上原章敬，山本匠，西垣正勝：4コマ漫画 CAPTCHA，情報処理学会論文誌，Vol.54，No.9，pp.2232-2243 (2013/09)

[2] Mohamed, M., Gao, S., Saxena, N., et al.: Dynamic Cognitive Game CAPTCHA Usability and Detection of Streaming-Based Farming, Proc. *USEC'14* (2014/02)

[3] 小島悠子，山本匠，西垣正勝：間違い探しを利用したワンタイム・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 (2007/03)

[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 (2014/03)

[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 (2006/06)

[7] Ahn, L.V., Dabbish, L.: Labeling Images with a Computer Game, Proc. *CHI 2004*, pp.319-326 (2004/04)

[8] トレンドマイクロ株式会社：ーパスワードの利用実態調査 2014ー約 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 (2011/11)

[10] Stobert, E., Biddle, R.: The Password Life Cycle：User Behaviour in Managing Passwords, Proc. *Symposium on Usable Privacy and Security* (*SOUPS*) 2014, pp.243-255 (2014/07)

[11] Chiasson, S., Oorschot, P.C.V., Biddle, R.: A Usability Study and Critique of Two Password Managers, Proc. *15th USENIX Security Symposium*, (2006/08)

[12] Jeff Howe: The Rise of Crowdsourcing, *WIRED magazine* (online)，入手先〈http://archive.wired.com/wired/archive/14.06/crowds.html〉（参照 2014/08/24）

[13]Foldit，入手先〈http://fold.it/portal/〉(参照 2014/08/25)

[14] The Password Meter（オンライン），入手先〈http://www.passwordmeter.com/〉(参照 2014/08/25)

[15] マイクロソフト：パスワードのチェックーパスワードは強力か？（オンライン），入手先〈https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx〉(参照 2014/08/25)

[16] Brooke, J.: SUS: A Retrospective, JOURNAL OF USABILITY STUDIES, vol.8, No.2, pp.29-40(2013/02)