Vol.2018-DPS-174 No.15
Vol.2018-CSEC-80 No.15
2018/3/5

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

服部 夢二[1]　高田 哲司[1]

概要：知識照合型個人認証は，「理論的な安全性」よりも実質的な安全性は低くなると言われている．その原因は，ユーザが「安全な秘密情報」を設定せず，また利用しないことにある．この状況に対し，パスワードメータ，セキュリティポリシ，教育，システム生成パスワードの利用などが対策としてあるが，ユーザにその受容が困難なコストを強いるものばかりであり，安全な秘密情報の利用を前向きに考えさせることにはつながっていない．そこで本研究では，そのコストを前向きにとらえられる仕組みを個人認証に付与すればこの問題は改善できると考えた．この仕組みとして，本論文では幅広いユーザ層に対して楽しみを与えることができるゲームを用いることとした．この提案に基づき，携帯端末のパターンロック認証を対象としたプロトタイプシステムを実装し，被験者による評価実験を行った．その結果，安全な秘密情報を設定する動機付けは可能であり，その継続利用についても可能性が示唆される結果となった．

キーワード：個人認証，ゲーム，ゲーミフィケーション，動機付け，セキュリティ

Attaching Game function to User Authentication encourages Users to use Secure Credential

Yumeji Hattori[1]　Tetsuji Takada[1]

Keywords: User Authentication, Game, Motivation, Incentive, Secure behavior, Security

1. はじめに

個人認証は，情報システムやネットワークサービスを利用する上で欠かすことのできないセキュリティ機能である．個人認証には大きく３つの手法があることが知られているが，その中でも広く利用されているのがパスワードや暗証番号に代表される知識照合型個人認証 (以降，本論文では個人認証と記す) である．しかし，この手法には問題がある．それは，ユーザが「望ましい形で個人認証を利用しない傾向にある」という点である．「望ましい形での利用」とは「安全性の高い秘密情報を設定し，それをもって個人認証を行う」ことである．しかし，ユーザの能力には限界があるため，この実行に必要なコストを負担できず，結果として安全性向上は実現できないという状況にある．残念ながら，現時点においてこのコストを下げることは困難な状況にあり，上記の目標を達成するには別の方法を検討する必要があった．この状況下において，可能な範囲で「望ましい形での利用」に近づける方法として，そのコストを前向きに負担するようユーザを動機づける方法はないかと著者らは考えた．そこで我々は，個人認証を「ゲーム化」することにより，上記の動機付けができるのではと考えた．

以降，本論文では「個人認証のゲーム化」に関するアイデアについて述べるとともに，実装したプロトタイプ・システムと実施した評価実験とその結果を解説し，提案するアプローチの可能性について議論する．

[1] 電気通信大学
The University of Electro-Communications, Chofu, Tokyo 1828585, Japan

2. 個人認証における現状認識と改善アイデア

知識照合型個人認証は，安全性とコストのトレードオフの問題を抱えている．個人認証において安全を確保するためには，複雑な秘密情報を利用するべきであるが，それによって生じるコストを負担するのは多くのユーザにとって容易なことではない．

長くて複雑なパスワードをユーザに利用させるための方法として以下の 4 つの方法がある．

(1) **システムが生成する秘密情報の利用**：「長くて複雑なパスワード」をユーザが作成するかわりに，必要な要件を満たすパスワードをシステムが生成し，それをユーザに利用させる手法である．これにより脆弱な秘密情報を利用しないようにする．

(2) **セキュリティポリシ**：各組織ではセキュリティ対策の一環としてセキュリティポリシを策定し，所属メンバにそれに従うことを求める状況にある．個人認証におけるパスワードは，その要件をポリシの 1 つとして定義し，その定義に反するパスワードは個人認証で利用できないようにする対策が行われている．

(3) **パスワードメータ**：パスワードメータとは，パスワードの安全性を可視化するシステムである．自分が決定したパスワードが，どの程度の安全性を持つのかを利用者にフィードバックすることで，より安全なパスワードの設定を促すものである．

(4) **セキュリティ教育**：セキュリティ教育とは，IT 機器やネットワークサービスを利用するユーザに対してセキュリティ脅威とその対策に関する知識を提供することを目的として行われる教育活動である．

しかし，これらの手法はどれも安全性向上のためにコストを発生させるため，結果的に安全性向上につながらない可能性がある．上記の (1),(2) や (3) は安全性確保の観点では望ましいが，秘密情報を記憶保持するためのコストを利用者に課すことになる．しかし利用者の多くはそのコストを受容できず，利用者が独自にコストを下げようと試みているのが現状であろう．安全性は低下するが記憶保持可能な秘密情報に変更したり，ポリシ要件を満たす範囲で簡単な秘密情報を作成したり，記憶とは別の方法で秘密情報を保持するなどが考えられる．

また (2) や (4) が原則論として正しいことに異論はないが，ポリシーを遵守する，また教育を通じて知り得た内容を実行する上でかかるコストが利用者の許容範囲を超える場合，同様の問題が発生する．つまり「理解はできる，しかし実行は困難」という結果を導くことになり，実質的にセキュリティ向上に結びつかないことになる．

この状況を改善するには，安全性確保のために必要なコストを削減・縮小するという方法が考えられる．しかし，現時点において，それは困難であると言わざるをえない．また少しでも多くのコストを受容できるよう，ユーザの能力を改善することも容易ではない．そこで我々は，このコスト負担を前向きにとらえるようユーザに動機を与えることで，限界はあるものの「望ましい形での利用」に近づけることができるのではと考えた．

利用者視点から考えた場合，個人認証を望ましい形で利用しようという動機はない．ユーザの多くは IT 機器やネットワークサービスを利用するのが目的であり，個人認証やセキュリティ対策を行うのが目的ではない．また個人認証を望ましい形で使用するべきという「必要性」を利用者が認識または実感する機会もないのが現状である．ログイン履歴情報の提供や不審な個人認証行為をメールで通知するといった対策は行われているが，“なりすまし”といった不正行為に関する情報を目にする機会は少なく，その必要性を実感させることにはなっていないと推測する．またこういう状況であるがゆえに正常化バイアスが働き，コスト負担の動機を与えるどころか「個人認証を利用しなくても大丈夫では？」と潜在的リスクを誤認識させ，動機を失わせる事態になっていると考える．

そこで本研究では「セキュリティ向上を目的とした動機付け」ではなく，外的要因による動機を個人認証に【付与】する，というアプローチを提案する．前述の通り，セキュリティ対策は必要不可欠であるが，その対策を行わせる動機付けのための根拠にするのは困難であると考えた．そこで我々は，個人認証におけるコスト負担を前向きにしうる仕組みを個人認証に【付与】することで，その動機付けを行う．その仕組みは，個人認証の利用者が欲するものである必要があるが，今回は老若男女で幅広く楽しむことができる「ゲーム」を適用した．ユーザにとって「面倒なこと・嫌なこと」に対してゲーム要素を取り入れ，「楽しいこと」に変換しうる手法として「ゲーミフィケーション」という手法があるが [1]，それと類似したアプローチであると考えている．

この動機付けについて，我々はもう 1 つの方針を決定した．それは，動機付けを継続して行うことである．個人認証は「秘密情報の設定・更新」と「個人認証の実施」の 2 つの作業で構成されるが，この双方において動機付けを行わないと目的が達成できないと考えたからである．パスワードメータ，セキュリティポリシそしてシステム生成パスワードの利用といった手法は，どれも「秘密情報の設定・更新」のみに着目し，安全な秘密情報の設定を強制または促しているが，それだけでは不十分である．なぜなら，そのコスト負担を受容できないユーザが，脆弱だがコストの小さい秘密情報に変更してしまうからである．我々の目標は，単に安全な秘密情報の設定を促すだけでなく，その秘密情報を個人認証で継続して利用させることにある．よって安全な秘密情報の継続利用についても動機づけを行い，

Vol.2018-DPS-174 No.15
Vol.2018-CSEC-80 No.15
2018/3/5

可能な範囲で「望ましい形」での個人認証利用へ近づけることを試みる．

3. プロトタイプ:PatternLockAdventure

3.1 概要

前述の提案内容を携帯端末のパターンロック認証に適応したプロトタイプシステムとして “PatternLockAdventure”(以降，PLA と略す) を実装した[*1]．携帯端末における個人認証を対象とした理由は，個人認証の利用頻度が高いことと個人情報を持つ端末であることから，個人認証を望ましい形で利用するべきであると考えたからである．動機付けをゲームで行うと述べたが，PLA では Role-Playing Game(RPG) を利用することとした．動機付けを継続して行う必要があるためゲームとしても一定の継続性が必要だと考えたことと，また時間制限のもとで集中してプレイするようなものではなく，散発的に行われる個人認証行為をゲームにゆるやか反映可能であると考えたためである．PLA では個人認証の利用者が主人公となり，敵を倒していくことでストーリを進める RPG となっている．

個人認証において安全な秘密情報の利用を動機付けるため，PLA と個人認証間で以下の 2 つの連動を実現した．

「秘密情報の安全性」を「武器の強さ」と連動

つまり，安全な秘密情報を設定することで，強い武器を持つプレイヤとなり，ゲームを有利に進めることができる．これにより「安全な秘密情報の設定」を動機づけをする．

「個人認証の実施」を「敵との戦闘」と連動

PLA では，認証画面が敵との戦闘画面になり，個人認証を行うことで敵への攻撃が行われる．この際，利用している秘密情報の安全性が攻撃力として反映される．したがって，安全な秘密情報で個人認証を行うことにより，有利にゲームを進めることができる．これにより「個人認証で安全な秘密情報を利用する」動機付けをする．

3.2 ゲーム進行と動機付け

PLA における秘密情報の設定画面を図 1,2 に，個人認証時の画面を図 3,4 に示す．図 1,2 の設定画面は，パターンの初期設定，および再設定を行うことができる．ここでパターンを入力すると，リアルタイムで現在入力されたパターンの強度を Song らのアルゴリズム [2] を用いて判定し，キャラクタのテキストと武器のアイコンに反映される．安全性の低いパターンを入力すると，キャラクタからは弱い武器であるというセリフがフィードバックとして発生するため，より強い武器を装備したいプレイヤへの動機づけが可能である．

[*1] https://css.kinmemodoki.net

図 1 パターン設定画面 1

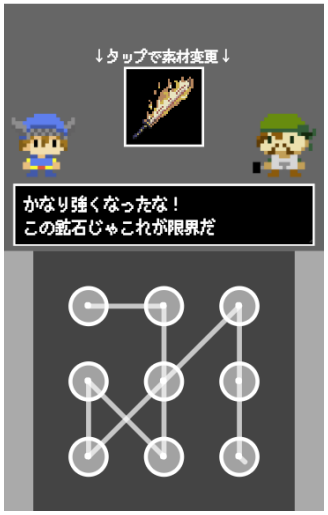

図 2 パターン設定画面 2

図 3 認証待受画面

図 4 認証入力画面

認証画面は待ち受け画面と認証画面の 2 画面構成となっている．図 3 が待ち受け画面であり，画面下部の”Attack”ボタンを押すと，図 4 の認証画面兼戦闘画面に遷移する．ここでユーザの秘密情報を入力すると，敵を攻撃することになる．この画面では，プレイヤが敵を攻撃するだけであり，敵から逃げたり，敵から攻撃されるということはない．よってユーザが認証行為以外の対応を考える必要はなく，既存の認証と同じように利用できる．

動機づけの継続性維持のため，ゲームには以下の考慮がなされている．

敵を多く倒すことで武器の強化が可能

プレイヤは個人認証を通じて敵を倒すと金貨を獲得する．この金貨を使用して武器素材を購入することができ，この武器素材を使用してさらに強い武器を作成することができる．つまり多くの敵を倒し，金貨を稼ぐことでゲームを有利に進めるられるようになっている．この仕組みは多くの敵を倒そうという欲求を生み，結果として強い武器で攻撃する，すなわち安全な秘密情

Vol.2018-DPS-174 No.15
Vol.2018-CSEC-80 No.15
2018/3/5

報の継続利用の動機づけへとつながっている．

複数ステージの用意

PLA には複数のステージが用意されており，プレイヤは任意のタイミングでステージを選択できるようになる．ステージを変更すると認証画面における背景や出現する敵も変更される．後半のステージほど手ごわい敵が出現し難易度は上がるが，獲得できる金貨の量も増加するため，プレイヤへ後半のステージにも挑戦させる仕組みになっている．このように複数のステージを用意することで利用者の動機付けを途切れさせないように工夫している．

これらの工夫により，秘密情報の設定と個人認証の双方において，安全な秘密情報の設定・利用を動機付け可能にしている．

4. 評価実験

提案手法の有効性を検証するため，以下の 2 つの仮説を検証するべく被験者による評価実験を行なった．

仮説 1 安全な秘密情報の設定するよう動機付けができる
仮説 2 安全な秘密情報を継続して利用するよう動機付けができる

4.1 実験方法

以下の手順で実験を行なった．

(手順 1) 強度メータ付きシステムを用いた秘密情報の設定
(手順 2) 手順 1 で設定した秘密情報を利用して認証を実施（1 日）
(手順 3) プロトタイプシステムを用いた秘密情報の設定
(手順 4) 手順 3 で設定した秘密情報を利用した認証を実施（15 日間）

手順 1，2, 3 は仮説 1 を検証するため，手順 4 は仮説 2 を検証するための作業である．手順 1, 2 で強度メータによる秘密情報を設定させ，その後に手順 3 でプロトタイプシステムによる秘密情報を設定させた．これらの双方の手法で設定された秘密情報の強度を比較することで仮説 1 を検証する．手順 1 で利用した「強度メータ付きシステム」を図 5 に示す．パターンの強度算出に使用しているアルゴリズムは，プロトタイプシステムと同一のものを利用している．なお手順 2 で 1 日間認証を実施した理由は，安全だが記憶保持できない秘密情報を被験者が設定していないか検証するためである．なお手順 2 において，認証に失敗した被験者は 0 人だった．

手順 2,4 では SNS による通知を利用し，1 日に 3 回，9,12,18 時に認証を行うよう被験者に依頼した．この通知には認証画面へのリンクが含まれており，そのリンクを押すだけで図 3 または図 6 の認証画面にアクセスできるようになっている．

手順 4 は仮説 2 を検証するために行なった．なお，この

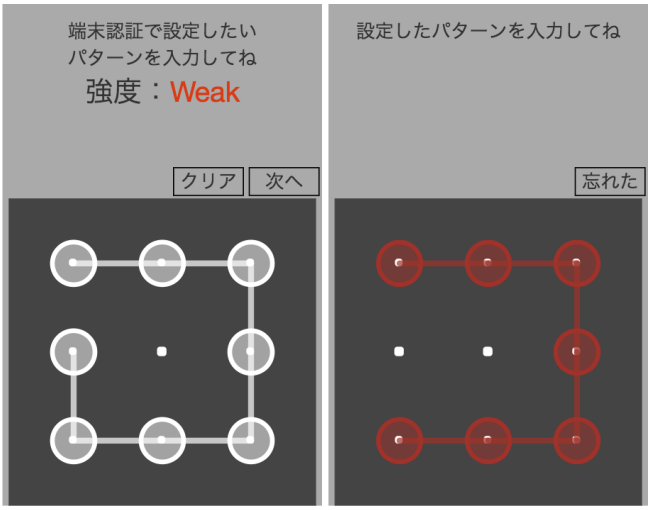

図 5 パターン設定画面

図 6 認証画面

手順実施期間内では，秘密情報を変更・再設定することを認めた．つまり，被験者はより簡単な秘密情報に変更したり，秘密情報を忘れたので再設定するといった行為を行うことができた．また，15 日という期間は，Egelman らがパスワードメータによってパスワードを変更させる実験 [3] で，2 週間以内にもとの脆弱なパスワードへ戻してしまったことを参考にした．被験者は 11 名（男性 9 名，女性 2 名），年齢層は 10 代〜50 代で実施した．なお報酬はなしでボランティアとして対応頂いた．

4.2 実験結果と考察

各被験者ごとに前述の手順で設定したパターンの安全性強度を時間変化としてとらえた結果を表 1 に示す．1 日目のみ強度メータで設定したパターンの強度であり，2 日目以降はプロトタイプシステムによって設定されたパターンの強度である．各セル内の数値はパターンの強度を表しており，3 段階の数値でその値が大きいほど強度が高いことを示している (3:Strong, 2:Medium, 1:Weak)．欄内に複数の数値があるものは，1 日で複数強度のパターンで認証タスクを行ったことを示している．数値の順番は左から認証タスクが行われた時系列順になっている．例えば，被験者 B の 6 日目では，Strong，Medium で認証タスクが行われたあと，再び Strong のパターンが使用されている．また数値のない欄は，認証タスクで認証成功事例がなかったことを示している．

4.2.1 仮説 1

今回の実験で，強度メータ付き認証システムにおいて最高強度である「Strong」のパターンを設定しなかった被験者は 11 名中 6 名だった（被験者 B,E,F,G,J,I）．その後，実験 3 日目には 6 名全員が強度メータ付き認証システムよりもより安全なパターンを設定した．このことから，強度メータよりも提案手法は安全な秘密情報を設定させる動機づけが可能であることがわかる．

Vol.2018-DPS-174 No.15
Vol.2018-CSEC-80 No.15
2018/3/5

表 1　認証タスクで利用されたパターンの強度

	1日目	2日目	3日目	4日目	5日目	6日目	7日目	8日目	9日目	10日目	11日目	12日目	13日目	14日目	15日目	16日目
被験者A	3	3	3	3	3	3	3	-	-	-	3,2,3,2	-	-	-	3,1,2,3	-
被験者B	2	2	2,3	3	3	3,2,3	3	3	-	3	3	3	3	3	3	3
被験者C	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
被験者D	3	3	3	3	3	3	3	3	3	3	3	3	3	3	-	3
被験者E	2	3	3	3	3	3	3	3	3	-	3	-	3	3	3	-
被験者F	1	1,2,3	-	3	-	-	-	-	-	-	-	-	-	-	-	-
被験者G	1	1,2	2	2	2	-	-	-	2	3	3	3	-	3	3	-
被験者H	3	3	-	-	-	-	-	3	3	-	-	3	-	-	3	-
被験者I	3	3	3	-	-	-	-	-	-	-	3	3	3	-	-	-
被験者J	2	2,3	-	3	-	-	-	-	-	-	3	-	-	-	-	-
被験者I	2	3	3	-	-	-	-	-	-	-	-	-	-	-	-	-

1：Weak，2：Medium，3：Strong　　欄内に複数の値：同日に複数種類パターンで認証

さらに，被験者 G は実験 2 日目で「Weak」から「Medium」へ上昇した後，6 日目には「Strong」のパターンを設定するようになった．そのため，提案手法は安全な秘密情報を設定する動機づけが可能であるといえる．

被験者 G がより安全なパターンを設定する動機づけに時間が要した理由として，ゲームの操作方法が複雑で，ゲームへの没入度が低かった点が挙げられる．被験者 G に対してアンケートにて調査をしたところ，「敵を倒したくてパターンを安全にしたが，敵を倒す以外のゲーム操作がわからなかった」という回答を得た．このことから，効率的にモンスターを倒す動機が薄れ，安全な秘密情報を設定する動機づけの効果が現れづらかったと推測した．

4.2.2　仮説 2

本実験では，日々の認証の中での利用されるであろう秘密情報を調査するために，その状況再現をすべく認証タスクを依頼した．そのため，認証タスクを遂行した日が 15 日間の半数である 8 日未満だった被験者は今回の結果の考察からは除外した．そのため，本実験における仮説 2 の考察対象となる被験者は A,B,C,D,E,G の 6 名とした．

考察対象となった被験者 6 名のうち，認証タスクで利用したパターンの強度が低下した被験者は被験者 A および B の 2 名であった．

被験者 B が，既に利用しているパターンより安全性の低いパターンを利用して認証を行った理由としては，安全性の低いパターンを利用した場合にゲーム内でどういったフィードバックが起こるか「好奇心」によるものだと推測される．被験者 B が 6 日目で「Medium」を利用して認証を行った回数は 1 回であり，その後再び「Strong」のパターンを利用している．よって，被験者 B は安全な秘密情報を継続的に利用する動機づけがされていることがわかる．

一方，被験者 A の場合，「Medium」を利用した回数は 13 回であり，その後「Strong」のパターンを再設定することなく，11 日目の認証タスクを終了した．この結果に対して被験者 A にヒアリングしたところ，「最終ステージの敵を全て倒したため，安全な秘密情報を設定する動機が失くなった」という回答を得た．このことから，ゲーム内のコンテンツが全て消費されると動機づけの効果が失われることがわかる．

これらの結果から，提案手法における安全な秘密情報を継続的に利用する動機づけが可能となる仮説は可能性の示唆にとどまったと考えた．継続的に利用を動機づけるには，ゲーム内のコンテンツを繰り返し遊べるゲームデザインとするか，複数種類のゲームを用意する必要があることがわかった．

5.　今後の課題及び関連研究との比較

5.1　今後の課題

5.1.1　認証タスクの遂行率

今回，仮説 2 の安全な秘密情報を継続的に利用する動機づけを検証するにあたり，日常の中で行う認証を再現するために 15 日間の認証タスクを設けたが，8 日以上認証タスクを遂行した被験者は約 5 割にとどまった．

この認証タスクの遂行率から，原因となり実際に認証システムが利用される状況を再現が不十分であることが伺える．そこで，AndoroidOS は画面ロックをサードパーティ製アプリに置き換えることができることを利用し，プロトタイプを実際の Android の画面ロックアプリとして実装する方法がある．プロトタイプを被験者の画面ロックアプリとすることで，実際に認証システムが利用される状況での効果が測定可能となる．

5.1.2　覗き見攻撃へのリスク

今回のプロトタイプでは，認証を行う度に報酬が獲得できるゲームデザインとした．そのため，1 日に最大 293 回の認証を行った被験者も確認された．こうして繰り返し認証を行うことで複雑な秘密情報を記憶できるメリットがある一方，認証を覗き見されるリスクも増加する懸念がある．携帯端末を用いたゲームは満員電車などの覗き見攻撃のリスクが高い場所でもプレイが可能であることから，覗き見攻撃への対策は急務である．

この対策として，認証によって獲得できる報酬の時間制

限が挙げられる．例えば，一度認証したあと一定時間は認証を行わずとも継続的に報酬を獲得し続けるというゲームデザインである．

5.2 関連研究との比較

藤田らはセキュリティ問題に対するエンターテイメントの応用方法として「セキュリティ技術にエンターテイメント因子を導入」と「エンターテイメントにセキュリティ因子を導入」の２つの関係性があると述べている [4][5]．この分類によれば，本論文での提案手法は前者であろう．ただし著者らは，前者のアプローチとも異なるアプローチの提案であると考えている．それは以下の差異があると考えるからである．

- アプローチ A：エンターテイメント因子の導入による新しいセキュリティ技術により，利用者の行動変化を促す
- アプローチ B：エンターテイメント要素を既存のセキュリティ技術に「付与」し，期待される行動を利用者が行えば報酬が得られる仕組みとすることで行動変化を動機づける

Ebbers らによる「Ariadne PathLogin」[6] や小島らの間違い探し認証 [7] は上記のアプローチ A に該当すると考える．これらの手法の問題点は，その手法の利用を強制される懸念である．またその懸念を払拭するために複数の認証手法の１つとした場合，当該手法が利用されないという懸念もある．さらには新たな認証手法を肯定的に捉えられない利用者だったり，その認証手法が適切とは言えない利用場面がある場合，かえって逆効果になる懸念もある．

これに対して我々の提案方法は以下の利点を有しているため，上記の懸念はない．

- 既存のセキュリティ機能を変更せずに利用可能
- 利用者の振る舞いを矯正するのではなく，望む変化になるよう利用者を促す

提案手法では既存のパターンロックを流用しており，機能や操作性の変更は施していない．ゆえに利用者は新たな個人認証手法を学習する必要はなく，また新手法の利用を強制されることもない．また新手法を利用させることで，利用者の振る舞いを「矯正する」のではなく，エンターテイメント要素をセキュリティ機構に【付与】することで，望ましい振る舞いを行うよう利用者を「動機付ける」にとどめている．言い換えると，セキュリティ機能をエンターテイメント化するアプローチではなく，セキュリティ機能にエンターテイメント因子を疎結合で付与するアプローチであると言える．

このアプローチでは，利用者を「望ましい形」で利用させる効果が弱くなるという懸念がある．しかし，利用者のセキュリティに対する意識は様々であり，こういった仕組みが不要な人も存在する．個人認証は，多くの人利用する仕組みであり，本研究による動機付けが不要な人への配慮もできることが望ましい．提案手法は，セキュリティ機能に対する変更はないため，上記のような利用者でも追加の負担や操作を求めることはない．また完全に不要だということであれば，エンターテイメント要素と個人認証の結合を切れば良いのである．

6. おわりに

個人認証において安全な秘密情報が利用されない問題において，安全性強度メータなどを用いて安全な秘密情報の設定を促す対策が存在した．しかし，こうした対策はセキュリティ意識の低いユーザへの効果が低いことが懸念されると同時に，安全な秘密情報を設定した後も再び脆弱な秘密情報へ戻してしまう問題も存在した．

そこで，本研究では安全な秘密情報を利用させる動機づけをゲーム用いて行う手法を提案した．今回の提案手法では認証行為をゲーム操作の一環とすることで，安全な秘密情報の動機づけを試みている．評価実験では，強度メータよりも提案手法は安全な秘密情報を設定させることが可能であることがわかった．また，そこで設定された秘密情報が継続的に「利用される」かどうかは，被験者実験の認証タスク遂行率の問題により再検証が必要だが，その可能性は示唆された．

本研究では，安全な秘密情報を利用する動機づけの１手法として「ゲーム」を用いているが，今後より幅広いユーザへの動機づけを試みるため，様々な手法で動機づけを検討していく所存である．

参考文献

[1] Deterding, S., Dixon, D., Khaled, R. and Nacke, L.:From Game Design Elements to Gamefulness: Defining “Gamification”, Proceedings of *the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, pp.9-15 (2011).
[2] Song, Y., Cho, G., Oh, S., Kim, H. and Huh, J.H.:On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks,Proceedings of *the 33rd Annual ACM Conference on Human Factors in Computing Systems*,pp.2343-2352 (2015).
[3] Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K. and Herley, C.:Does my password go up to eleven?: the impact of password meters on password selection,Proceedings of *the SIGCHI Conference on Human Factors in Computing Systems*, pp.2379-2388 (2013).
[4] 藤田 真浩, 山田 眞子, 西垣 正勝: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, 情報処理学会論文誌, Vol.57, No.12, pp.2711-2722(2016).
[5] 樋口 和輝, 佐野 絢音, 土屋 貴史, 藤田 真浩, 西垣 正勝:エンターテイメントを活用したセキュリティ強化：長いパスワードの記憶維持に必要な復習頻度の検討, 研究報告マルチメディア通信と分散処理（DPS）, 2017-DPS-170, No.7(2017).
[6] Ebbers, F. and Brune, P.:The Authentication Game - Se-

cure User Authentication by Gamification?,Proceedings of *Advanced Information Systems Engineering: 28th International Conference*,pp.101-115 (2016).
[7] 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コンピュータセキュリティ（CSEC）,Vol.2007,No.16,pp.375-380(2007).
[8] Kroeze, C. and S.Olivier, M.: Gamifying authentication,Proceedings of *2012 Information Security for South Africa*, pp.1-8 2012.
[9] 黒澤 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, 電子情報通信学会技術研究報告,Vol.113,No.502,pp.197-202(2014).