

# 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

樋口和輝<sup>†1</sup> 佐野絢音<sup>†2</sup> 土屋貴史<sup>†2</sup> 藤田真浩<sup>†3</sup> 西垣正勝<sup>†3</sup>

**概要：**セキュリティとエンターテイメントの融合の一形態として、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方法が提案されている。その一方式として著者らが行った先行研究の中では、パスワードをゲームのコマンドとして組み込むことによって、対戦ゲームの中でユーザに30文字前後の乱数パスワードを容易に覚えさせることに成功した。しかし、ユーザはゲーム終了後にはそのパスワードを忘却してしまっていた。そこで本研究では、対戦ゲームを通じて記憶したパスワードをユーザに長期に渡って定着させるために、対戦ゲームの終了後にパスワードの記憶の維持を促す別のゲームへと移行させるというアプローチを検討している。本稿では、その第一歩として、記憶の維持を促すゲームの実施間隔に関する実験を行った。具体的には、対戦ゲームで覚えたパスワードに対して、一定期間ごとにパスワードを再入力してもらう復習タスクを被験者に行ってもらい、被験者がパスワードの記憶を保持できるかを調査した。その結果、1日1回の復習間隔から1日ずつ復習間隔を広げていくことによって、16名全ての被験者が4日に1回の間隔で復習タスクを実施すれば、30文字前後の乱数パスワードの記憶を維持できることを確認した。

**キーワード：**パスワード、記憶維持、復習、エンターテイメント

## Security Enhancement through Entertainment: A Study on review intervals for keeping a longer password in memory

Kazuki Higuchi<sup>†1</sup>, Ayane Sano<sup>†2</sup>, Takashi Tsuchiya<sup>†2</sup>, Masahiro Fujita<sup>†3</sup>,  
and Masakatsu Nishigaki<sup>†3</sup>

### 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きた[1][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技術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、従来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。

そこで筆者らは、文献[1]において、「ゲーム」というエ

ンターテイメント技術に「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手法を提案した。さらに文献[1]では、その具体的な一方式として、パスワードを対戦ゲーム内のコマンドとして取り扱う方式（以下、対戦ゲーム方式と呼ぶ）を示し、実証実験によりその有効性を評価した。その結果、対戦ゲームを1時間程度プレイする間に、ユーザは18~36文字の乱数パスワードを正確に記憶できることを確認した。

しかし、ユーザがパスワードを記憶することができていたのはゲームをプレイしている間だけ（ゲームをクリアするまで）であり、ゲーム終了後にはそのパスワードは忘却されてしまっていた。そこで、対戦ゲーム方式で記憶した乱数パスワードを長期に渡ってユーザに維持させるために、対戦ゲームの終了後にパスワードの記憶の維持を促す別のゲームへと移行させる方法について検討を行う。具体的には、対戦ゲームを通じて記憶した乱数パスワードの再入力を求めるゲームを開発し、ユーザに定期的にパスワードを復習させる方式（以下、復習ゲーム方式と呼ぶ）を提案する。本稿では、復習ゲームの設計に資する知見を得るために、パスワードの「再入力の頻度と記憶の定着度」の関係を測るためのユーザ実験を実施する。

本稿の構成は次のとおりである。2章では、対戦ゲーム方式の詳細を述べる。その後、対戦ゲーム方式で一時的に

<sup>†1</sup> 静岡大学情報学部

Faculty of Informatics, Shizuoka University

<sup>†2</sup> 静岡大学大学院総合科学技術研究科

Graduate School of Integrated Science and Technology, Shizuoka University

<sup>†3</sup> 静岡大学創造科学技術大学院

Graduate School of Science and Technology, Shizuoka University

記憶したコマンドを長期維持するための復習ゲーム方式を提案する。適切な復習頻度を探るためのユーザ実験を3章で行う。4章で実験結果を述べたのち、5章でその結果に対する考察を行う。最後に、6章でまとめと今後の課題を述べる。

## 2. ゲームを活用したパスワード強化

### 2.1 対戦ゲーム方式によるパスワード記憶

文献[1]にて筆者らは、エンターテインメント技術にセキュリティ因子を導入するアプローチの一つとして、「ゲーム」というエンターテインメント技術に「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を提案した。ゲームの中にパスワード強化を組み込む方法には様々なアイデアが考えられるが、文献[1]では、その一具体例として、パスワードをゲーム内のコマンドとして扱う方式を示した。ゲームの中でコマンドを入力しているうちに、そのコマンドが自然に記憶され、そのコマンドを見ずとも入力できるようになることは、ゲームのプレイヤー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、ゲーム内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。

文献[1]で開発した対戦ゲームは、ダンジョン探索ゲームである。ダンジョン探索中に敵が出現し(図1)、その敵を倒しながら、プレイヤーはゴールへと進んでいく。敵と遭遇した場合は戦闘シーンへと移行し、プレイヤーはコマンドを入力することによって敵を攻撃する。「コマンド(パスワード)」は事前に登録されている。プレイヤーはゲームプレイ中に敵に何度も遭遇し、そのたびにコマンド入力を繰り返す。その結果、プレイヤーはコマンドを見ずに正確に入力すること可能となる。

文献[1]では、ユーザ実験によって対戦ゲーム方式の有効性を実証している。アルファベット小文字・数字・記号、計47文字から構成される36文字の乱数パスワード(コマンド)がゲームに登録されている。このゲームをユーザ20名に各々1時間程度プレイしてもらった結果、すべてのユーザが18~36文字の乱数コマンドをそのコマンドを見ずに入力することに成功した。

ただし、文献[1]で、ゲームクリアから約24時間後に再度のコマンド入力を課したところ、多くのユーザが(ゲームプレイ中では入力成功していたはずの)コマンドを正確



図1. 文献[1]のゲーム中コマンド入力画面

に回答することができなかった。すなわち対戦ゲームは、短時間の内に一気に長いコマンドをユーザに記憶させることができる一方で、その記憶を定着させるまでの効果はなく、ユーザは短時間の内にそのコマンドを忘却してしまう。コマンドをパスワードとして利用するためには、対戦ゲーム方式で覚えた18~36文字のパスワードをユーザに長期記憶させる工夫が必須である。

### 2.2 記憶維持のための復習

文献[1]において、24時間後のコマンド入力の結果を分析した結果、多くのユーザは(コマンドの全文字を正確に入力することはできなかったが)コマンドの大部分の文字については正確に入力できていた(「正しいコマンド」と「ユーザが入力したコマンド」の間の編集距離が小さかった)。これより、多くのユーザの状況としては、対戦ゲーム方式によって一旦は完全にコマンドを記憶した状態であったものが、ゲーム終了後には記憶が一部曖昧となった状態へと劣化したのだということがわかる。

よって、対戦ゲーム方式で記憶したコマンドを長期に定着させるためには、「(i) 曖昧となった記憶を修正するフェーズ」と「(ii) 修正された記憶を強化するフェーズ」を繰り返す作業が必要となると考えられる。そこで本稿では、以下に示す2段階のコマンド復習法を採用する。

- ① 対戦ゲーム方式を用いてコマンドを記憶する。
- ② 対戦ゲーム終了後には、一部曖昧となったコマンドの記憶を修正するために復習を行う。  
(ア) ユーザは対戦ゲーム方式終了後、1日ごとに①で記憶したコマンドの復習を行う。

(イ) ユーザが「コマンドを正確に記憶した」と判定できた場合、③に移る。

③ コマンドの記憶を強化するために、復習の実施頻度を段階的に延ばしながら②の復習を続ける。

②が、(i)を実現するための復習であり、「コマンドを正しく記憶し直すため」の復習である。ユーザに1日ごとにコマンドの再入力を課すことによって、一部曖昧な記憶状態となってしまったコマンドを正確な記憶状態に修正することを支援している。③が、(ii)を実現するための復習であり、「コマンドの記憶をより長期化させるため」の復習である。1日ごとに実施していた②の復習を、2日ごと、3日ごと、・・・と徐々に延ばしていくことによって、記憶を強化してコマンドを長期定着させることを支援している。

### 2.3 復習法とゲームの利用

前節の②③の復習法をゲームとして実装することによって、復習ゲーム方式によるパスワード記憶が可能となる。具体的な復習ゲーム方式の設計と実装は今後の対応となるが、たとえば、定期的にペットに食事を与える育成ゲーム（コマンドを入力するとペットに食事が与えられる）や定期的に敵が攻めてくる防衛ゲーム（敵を倒すためにはコマンドを入力しなければならない）などは、②③を組み込むのに適したゲームであると考えられる。ユーザがこれらゲームをプレイすることで、自然に②③の復習が達成されることが期待される。

対戦ゲームと復習ゲームが揃うことによって、対戦ゲーム方式を用いてユーザにコマンドを記憶させ（前節の①）、対戦ゲーム終了後は復習ゲーム方式に移行してその記憶を定着させる（前節の②③）ことが可能となる。

## 3. 基礎実験

### 3.1 目的

2.2 節に示した手順②③に従うことで、ユーザが対戦ゲーム方式で覚えたコマンドの記憶をどの程度定着させることが可能であるかを調査する。具体的には、ユーザがコマンドを正確に記憶するまでにかかる期間（手順②から③へ移行するまでにかかる日数）を探る（調査項目1）。さらに、正確に覚えたコマンドを記憶維持するための復習頻度を探る（調査項目2）。

### 3.2 対戦ゲームの実装

対戦ゲームは、文献[1]で実装したシステムをそのまま利用した。コマンドは全ユーザ共通で、「abcdefghijklmnopqrstuvwxy0123456789-^@[:;.,/」（計47文字）から生成したランダムな文字列「t2-0fyphjqfks]xul]k8rrg[g@ttiy5]c[@k]」（36文字）である。この対戦ゲームをクリアするためには、被験者は最低12文字のコマンドを記憶する（見ずに入力）する必要がある。実装の詳細に関しては、文献[1]を参照されたい。

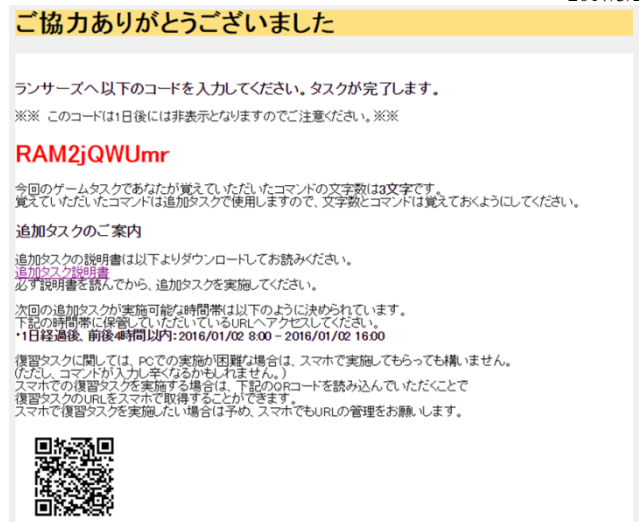


図 2: 待機ページ

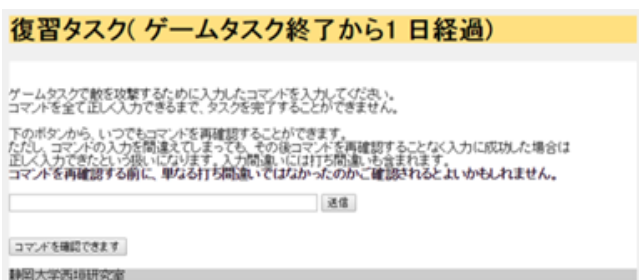


図 3: 復習ページ



図 4: コマンド確認ページ

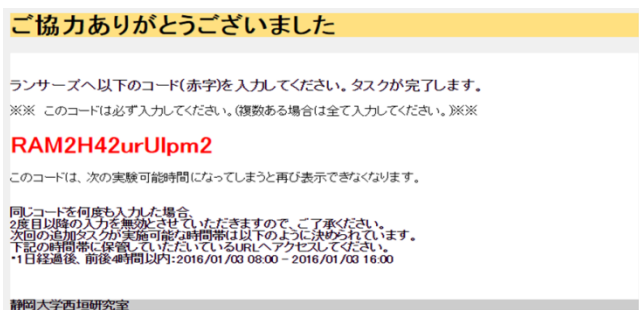


図 5: 次回復習時間帯通知ページ

### 3.3 復習システムの実装

2.2 節の手順②③を実施するため実験用 Web ページを復習システムとして実装した。被験者が復習システムにアクセスした際には、通常は待機ページ（図 2）が表示されるだけであるが、復習作業の実施時間にアクセスした場合には、待機ページから復習を行うページへ遷移することがで

きる(図3)。なお、今回の実験では、被験者には(パスワードという単語は使わず)対戦ゲームのコマンドの再入力を依頼するという形で作業の説明をした。

図2が、待機ページのスクリーンショットである。待機ページにおいては、次回復習を行う時間帯が表示されている。

図3が、復習ページのスクリーンショットである。画面にはテキストフォームが表示されており、被験者は対戦ゲームを通じて記憶したコマンドをこのフォームへ入力する。入力後、「送信」ボタンを押すと、「被験者が入力したコマンド」と「当該被験者が対戦ゲーム内で記憶したコマンド」の一致判定が行われ、一致していれば(正しければ)、「次回復習時間帯通知ページ(図5)」へ移動する。不一致だった場合(間違っていれば)、間違っていると表示され、コマンドの再入力を促される。被験者は、正しいコマンドを入力できるまで、入力を何度も送信することが可能である。どうしてもコマンドを思い出せなかった場合、「コマンドを確認できます」ボタンから「コマンド確認ページ」(図4)へと遷移することが可能である。被験者が正確にコマンドを記憶できている場合は、コマンド確認ページを参照する必要がない。

図4が、コマンド確認ページのスクリーンショットである。コマンド確認ページには、対戦ゲーム内で被験者自身が入力したコマンドが表示される。図4は、対戦ゲーム内で36文字のコマンドを覚えた被験者の例である。被験者は、これを見てパスワードを再度改めて記憶することが可能である。「入力ページに戻る」ボタンによって復習ページ(図3)へ戻ることが可能である。

### 3.4 手順

3.2節、3.3節で実装した復習システムを利用した実験手順を示す。実験は、ゲームタスク(2.2節の①)と復習タスク(2.2節の②③)の二つのタスクに分けられる。本研究が学術目的の依頼であること、コマンドのメモ書きは禁止であること、ゲーム終了後に追加タスクの実施が求められることを、ゲームタスクの開始時に被験者へ知らせる。ただし、追加タスクの内容(復習タスクの実施が求められること)は、ゲームタスク終了の時点で、初めて被験者に知らされる。

#### 【ゲームタスク】

1. 対戦ゲームのURLを提供する。
2. 対戦ゲームをプレイさせてコマンドを記憶させる
3. アンケートに回答させる。アンケートは文献[1]で実施したアンケートに下記2問を追加して作成をした。

・12階(最後の階)で入力した一番長いコマンドを入力してください。

・もし、より長いコマンドを入力できる自信がある方は、そのコマンドを入力してください。(こちらは入

力しなくても構いません)

これらの質問で入力されたコマンドを、「被験者がゲームタスクで記憶した」コマンドとして利用する。この質問については、対戦ゲーム方式では、ログとして被験者毎入力した最大文字数を残しているが、例えば被験者が徐々に入力する文字数を伸ばしたが、敵の体力や自分の記憶の限界を考えて最大文字数から、文字数を下げて入力を続けた場合、被験者にとって一番打ち慣れた文字数はその時の文字数となる。そのため、復習タスクにおいてもその文字数を使用してもらうため、今回このような質問を追加した。

アンケート回答終了時刻 $h$ を基準に復習タスクにおける復習実施可能時間は決定される。

#### 【復習タスク】

1. 対戦ゲームをプレイ後、復習タスクのURLを知らせる。
2. 2日目(ゲームタスクを実施した翌日):時刻 $h$ に復習ページを表示させ、復習をさせる。ただし、時刻 $h$ ちょうどに実施させることは困難であるため、実際は $h$ の前後4時間でも実施可能であるように設定した。
3. 3日目:同上。
4.  $d$ ( $d>3$ )日目:同上。 $d$ 日目の復習を終えた際、ユーザが $d$ 日目、 $d-1$ 日目、 $d-2$ 日目に一度もパスワード確認ページを確認しなければ、⑤へ移る。

以上が(i)の「曖昧となった記憶を修正するフェーズ」の手順である。この手順が示すとおり、3日間連続でコマンド確認ページを確認せずに入力できていることで、「被験者は正確にコマンドを記憶できた」と判定している。この3日間という期間は、予備実験によって経験的に定めた。ここまでにかかった日数を $D$ として、以下、手順の説明を進める。

- ・記憶維持のために2日ごとに復習を行う
5.  $D+2$ 日目( $D+2\times 1$ 日目):時刻 $h$ に復習ページを表示させ、復習をさせる。
  6.  $D+4$ 日目( $D+2\times 2$ 日目):同上
  7.  $D+6$ 日目( $D+2\times 3$ 日目):同上。  
ここで、復習の頻度を1日間広げる。
  - ・記憶維持のために3日ごとに復習を行う
  8.  $D+9$ 日目( $D+2\times 3+3\times 1$ 日目):同上。
  9.  $D+12$ 日目( $D+2\times 3+3\times 2$ 日目):同上
  10.  $D+15$ 日目( $D+2\times 3+3\times 3$ 日目):同上。  
ここで、復習の頻度を1日間広げる。
  - ・記憶維持のために、4日ごとに復習を行う。

:

以下、同様である。ただし、復習タスク期間が1か月(30

日)に到達した場合、その時点で復習タスクの実験を終了する。すなわち、最も順調に記憶・維持できたユーザは、復習を計12回(1日ごと3回, 2日ごと3回, 3日ごと3回, 4日ごと3回)実施することとなる。また、復習を1回でもやり忘れた場合、その被験者に対する復習タスクは終了することとした。

ここで、D+2日目以降の復習タスクは、(ii)の「修正された記憶を強化するフェーズ」の作業である。忘却を防ぐために復習を行う間隔はできる限り短いほうがユーザにとってより好ましい。本実験では、その間隔を次第に広げていくことで、その間隔の限界を探っている。

### 3.5 被験者属性と報酬

実験の被験者は、クラウドソーシングサービスであるランサーズ[3]を通じて依頼した被験者30名、筆者が所属する研究室の学生5名の計35名である。

ゲームタスクでは500円の報酬を被験者へ支払った。復習タスクにおいては、各被験者の実験経過によって、復習の実施頻度が異なる。各被験者で報酬が平等となるよう、i日ごとに復習を行っている被験者へ、復習を終えた際に50×i円の報酬を支払うようにした。

## 4. 実験結果

### 4.1 ゲームタスクの実験結果

表1にゲームタスクの実験結果を示す。表中「最大桁数」は、ゲームタスクでゲームをプレイする中、被験者が到達したコマンドの最大桁数を、「確認桁数」は、4.4.1節で記述したアンケートの質問で入力してもらったコマンドの桁数を指す。今回の復習タスクでは、こちらの「確認桁数」を用いて実験を行った。「成功回数」は、最大桁数のコマンドの入力に成功した回数を指す。「所要回数」は、最大桁数に到達するまでに入力に成功したコマンドの回数を、「時間」はゲーム開始時から所要回数までの時間を指す。「総入力回数」は、被験者が対戦型ゲーム中に入力に成功したコマンドの総回数を、「総プレイ時間」は、対戦型ゲームをプレイした総時間を指す。

### 4.2 復習タスクの実験結果

表2に復習タスクの2日目からD日目までの実験結果を、表3にD+2日目以降の結果を示す。ゲームタスクを行ったユーザのうち21名(A~U)のみが復習タスクを実施しており、残り13名(V~AI)は実施していなかった。このため、表2,3ではA~Uの実験結果のみ記載している。

表2は、3.4節の手順2~4に対応する結果であり、コマンドをすべて正確に記憶するまでの実験結果を示している。具体的には、「文字数」とは、各被験者が対戦型ゲームを通して最終的に記憶したパスワードの桁数を指す。「失敗回数」と「確認回数」については、それぞれn日目に何回パスワードの入力に失敗したか、と何回パスワードの再確

表 1. ゲームタスクの実験結果

被験者	最大入力成功桁数				確認最大入力成功桁数				総入力回数	総プレイ時間 [分]
	最大桁数	成功回数	所要回数	時間 [分]	確認桁数	成功回数	所要回数	時間 [分]		
A	19	18	198	36:09	19	18	198	36:09	217	39:32
B	36	11	56	19:51	36	11	56	19:51	66	25:26
C	31	3	208	70:45	30	3	208	70:45	214	73:04
D	18	45	30	11:49	18	45	30	11:49	79	28:47
E	30	8	133	56:07	30	8	133	56:07	171	70:23
F	36	4	89	55:24	36	4	89	55:24	92	57:31
G	36	6	89	52:08	36	6	89	52:08	94	55:39
H	12	144	108	37:24	12	144	108	37:24	251	52:42
I	36	11	91	73:58	36	11	91	73:58	102	89:52
J	36	36	51	22:22	36	36	51	22:22	115	46:12
K	15	4	170	46:54	15	4	170	46:54	173	47:41
L	36	4	108	34:16	36	4	108	34:16	111	36:06
M	36	36	92	44:57	36	36	92	44:57	129	73:53
N	13	65	98	20:44	13	65	98	20:44	180	34:30
O	12	61	100	22:48	12	61	100	22:48	162	33:47
P	26	1	124	28:34	26	1	124	28:34	166	42:12
Q	36	8	101	37:48	36	8	101	37:48	113	44:06
R	36	13	89	45:12	36	13	89	45:12	101	52:57
S	36	16	105	55:49	36	16	105	55:49	120	66:15
T	36	15	111	34:32	36	15	111	34:32	127	41:26
U	34	9	82	34:09	19	30	47	16:24	133	49:15
V	18	18	132	28:27	18	18	132	28:27	153	35:40
W	12	125	79	15:16	12	125	79	15:16	205	32:49
X	36	5	140	45:04	36	5	140	45:04	144	46:59
Y	23	3	112	34:10	23	3	112	34:10	160	46:15
Z	15	19	104	36:08	15	19	104	36:08	169	50:03
AA	24	35	48	25:29	24	35	48	25:29	116	50:30
AB	28	10	89	43:23	27	10	89	43:23	130	66:27
AC	32	17	111	38:59	32	17	111	38:59	135	50:43
AD	18	20	191	47:30	18	20	191	47:30	210	52:33
AE	17	10	150	37:03	17	10	150	37:03	172	40:45
AF	18	13	87	27:38	13	44	58	20:03	183	49:03
AG	23	7	229	87:59	23	7	229	87:59	238	90:02
AH	12	30	230	53:08	12	30	230	53:08	262	60:20
AI	36	6	74	44:35	36	6	74	44:35	79	48:16

表 2: D 日目までの実験結果

被験者	文字数	1日目		2日目		3日目		4日目		5日目		6日目	
		失敗回数	確認回数	失敗回数	確認回数	失敗回数	確認回数	失敗回数	確認回数	失敗回数	確認回数	失敗回数	確認回数
A	19	0	0	0	0	0	0						
B	36	0	0	0	0	0	0	0	0	0	0		
C	30	4	5	1	1	0	0	0	0	0	0		
D	18	0	0	0	0	0	0						
E	30	0	0	0	0	0	0						
F	36	1	3	2	2	1	1	0	0	0	0	0	0
G	36	0	0	0	0	0	0						
H	12	0	0	0	0	0	0						
I	36	0	0	0	0	0	0						
J	17	1	3	0	0	0	0	1	0				
K	15	0	0	0	0	0	0	1	0	0	0	0	0
L	36	0	0	0	0	0	0						
M	36	0	0	0	0	0	0						
N	13	1	1	0	0	0	0	0	0				
O	12	1	0	0	0	0	0						
P	30	1	0	3	0	0	0						
Q	36	1	0	0	0	0	0						
R	36	0	0	0	0	1	0						
S	36	1	1	1	0	0	0	0	0				
T	36	0	0	0	0	0	0						
U	19	0	0	1	1	0	0	0	0	0	0		

認を行ったかを指す。空欄については、その時点で被験者が3.4節の手順5に移ったことで、1日1回の復習を実施しなかったことを意味している。

表3は、3.4節の手順5以降に対応する結果であり、すべて正確に記憶したコマンドの忘却のために復習した結果である。具体的には、「文字数」については表2と同様である。「失敗回数」は、各「n日に1回」の復習頻度で、復習毎に何回パスワードの入力に失敗したかを指す。実験を1ヵ月間最後まで行ってくれた被験者は16名であった。空欄については、表2と同様に、その部分の復習に関しては、被験者が復習を実施しなかったことを意味している。

## 5. 考察

### 5.1 対戦ゲーム方式で記憶したコマンドをすべて正確に維持するまでにかかる復習期間について

表2の結果から、1日1回の復習を3日（一度もコマンドの再確認を行うことなし）で、正確に維持する被験者が半分を超えたが、コマンドの再確認を行った被験者でも最長6日の日数で、正確に維持することができることがわかった。また、書面の関係上、記載はしていないが、コマンドに失敗した被験者のログを確認すると、失敗の仕方が、コマンドを部分的に間違えているといったコマンドが曖昧な状態であったことがわかった。そのため、その状態から徐々に失敗及び再確認の回数が減ることから、曖昧な状態から正確に維持できていることがわかる。

### 5.2 すべて正確に記憶したコマンドを記憶維持するための復習期間について

表3の結果から、その時の復習頻度で3回復習を行うことで、徐々に復習の頻度を拡大していくことが可能であり、最大で4日に1回の復習でコマンドの維持を行うことが可能だと分かった。コマンドに失敗した回数も、復習毎に1度だけとなっており、すぐにコマンドを自己修正することができていることがわかる。ただし被験者Iの「2日に1回」の頻度での「3回目」について、ログを確認すると、コマンド中の2文字の順番が入れ替わっているという入力失敗となっており、単なる打ちミスの可能性が高いと言える。

### 5.3 懸念事項

今回行った復習タスクについての、自由記述のアンケートから、「覚え続けるという意識があったからこそできたと思う」、「入力する必要のない日においても、今日は入力しなくていいのか、といったことを考えていた」というような回答が得られた。これについては、コマンドを入力する日（復習を行う日）以外も、頭の中でコマンドを思い浮かべている等の可能性が考えられる。本研究においては、復習を行う日以外については、コマンドのことは意識していない想定のため、今後新たなゲームを実装し、調査実験を行った際に、確認する必要がある。

表 3: D+2 日目以降の実験結果

被験者	文字数	失敗回数								
		2日に1回			3日に1回			4日に1回		
		1回目	2回目	3回目	1回目	2回目	3回目	1回目	2回目	3回目
A	19	0	0	0	0	1	0	0	0	0
B	36	0	0	0	0					
C	30	0	0	0	0	0	0	0	0	
D	18	0	0	0	0	0	0	0	0	0
E	30	0	0	0	0	0	0	0	0	0
F	36	0	0	0	0	0	0	0	0	
G	36	0	0	0	0	0	0	0	0	0
H	12	0	0	0	0					
I	36	0	1	3	0	0	0			
J	17	0	0	0	0	0	1	0	0	
K	15	0	0	0	0	0	0	0		
L	36	0	0	0	0	0	0	0	0	0
M	36	0	0	0	0	1	0	0	0	0
N	13	0	0	0	0	0	0	0	0	
O	12	0	0							
P	30	0	0	0	0	1	0	0	0	0
Q	36	0								
R	36	1	1	1	1	0	0	0	0	0
S	36	0	0	0	0	0	0	0	0	0
T	36	0	0	0	0	0	0	0	0	0
U	19	0	0	0	0	0	0	0	0	0

## 6. まとめと今後の課題

本論文では、先行研究（対戦型ゲームでパスワード強化）の問題点であった、記憶したパスワードを数時間で忘却してしまう点を解決するために、記憶したパスワードの維持に必要な復習頻度の調査を実施した。その結果、最大でパスワードを4日に1回復習することでパスワードを維持することができた。

今後は、今回得られた結果を元に、パスワードの維持に適切なゲームの検討を行う。また、考察で述べた懸念事項についても、詳細に検討を行っていく。

## 参考文献

- [1] 藤田真浩, 山田真子, 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(2016.12)
- [2] Joseph, B. and Stuart, S.: Towards reliable storage of 56-bit secrets in human memory, Proc. 23rd USENIX Security Symposium, pp.607-623 (2014).
- [3] Lancens (オンライン), 入手先 (<http://www.lancers.jp/>) (参照 2017/02/01)
- [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).