Vol.2021-ASD-20 No.1
2021/3/5

人工生命技術を用いたパスワード更新個人管理の一方式

加藤達也 [1]　山田隆亮 [1]

概要：人工生命の成長度合いがパスワード変更に対応付き、育成者だけが、生命体の姿からパスワードを読み取れるパスワード更新個人管理システムを提案する。10 人までの被験者の協力を得てプロトタイプでの比較検証実験においてパスワードの再現性、多様性を確認した。

キーワード：人工生命，パスワード変更，情報セキュリティ

A Self Management Method for Password Update Using Artificial Life Technique

TATSUYA KATO[†1]　TAKAAKI YAMADA[†1]

Abstract: A self management method for password update using artificial life technique that image of growing life is proposed for rememberance of updated password. Cooperated by upto ten participants, experimental results showed its effectiveness in the variety and recall of password.

Keywords: Artificial life, Password change, Information security

1. はじめに

情報セキュリティにおける個人認証手段には生体情報、持ち物情報、記憶情報を用いる。生体情報を用いた認証には、指紋や顔といった個人を特定する身体的特徴を用いる[4]。持ち物情報として、認証サーバと同期する特殊なデバイスやソフトウェアを用いてワンタイムパスワードを生成する方法があり、デバイスさえ持っていればかなり高いセキュリティで使用することができる。

記憶情報を用いたパスワードの需要は根強く、例えば、Web サイトの会員ページ、銀行、スマートフォンのロック機能など身近な日常生活の中に定着している。そして個人情報にアクセスするにもよく使われている。記憶情報に基づくパスワード認証は簡易に運用できる一方、他人に類推されやすい点で他の方式よりも脆弱である。

一方でそのような情報を悪用するためパスワードを破ろうとする犯罪も少なくない[2]。パスワードが脆弱でも必ずしも被害に直結するわけではないが、そのようなリスクはなるべく下げておきたい。パスワードとして、自身の生年月日や学籍番号、好きな数字など自らに強く関連するものは記憶しやすい。しかし、そのようなパスワードのバリエーションには限りがあり、同じパスワードを使いまわしていると、1 つのパスワードが破られた時に同じパスワードを使う全サービスの認証が破られがちである。その対策の 1 つとして企業などの団体では定期的にパスワードの変更を求めている[10]。

1 大阪工業大学　情報科学部　情報システム学科
Osaka Institute of Technology

パスワードの変更において、例えば 1 文字を変更や、大文字小文字を入れ替えることで済ませる場合も多く、強く強要されない限り、パスワードをわざわざ変更しない人も存在する[5]。実際に 2018 年度は、パスワードリスト攻撃が原因とされる不正ログイン事案が多数発生､報道された。アカマイ・テクノロジーズ合同会社の調査結果によれば、2018 年 5 月から 6 月までの不正なログイン試行が 83 億件以上検出されていた等、パスワードリスト攻撃による脅威の増加が世界規模で確認されており、複数の Web サービスで同一 パスワードを設定していることを前提として、不正ログインを試みる手口である。そのため、サービス利用者が取るべき対策としては、パスワードの使い回しをしないことであると述べられている [9]。

本研究では、人工生命技術を用いたパスワード更新個人管理方式を提案し、試作評価を行ったので報告する。

2. 関連する研究

(1) セキュリティトークン

セキュリティトークンはコンピュータシステムのユーザ認証のために用いる小型の装置であって、暗号鍵など秘密の情報の保管、認証に用いる情報の生成や表示などのために使われる。よく使われるものの一つはワンタイムパスワードを生成するセキュリティトークンで、ログイン回数や現在時刻を元に、その場限りで有効なパスワードや暗証番号を利用者に通知する。また、公開鍵暗号の秘密鍵（私有鍵）を保管して暗号化やデジタル署名に用いるものもある。
形態としてはキーホルダー型やカード型が多く、パソコンなどに接続して利用するタイプの製品には USB コネクタ

型や PC カード型などもある。単体で使用する装置は内蔵の電池で駆動し、筐体前面に小型の液晶画面や数字を入力するキーパッドなどがついている。携帯電話などの機器の一部としてあらかじめセキュリティトークンの機能が内蔵されている場合もある。コンピュータに導入・実行できるソフトウェアによってセキュリティトークンの機能を実現するものはソフトウェアトークンと呼ばれ、スマートフォンアプリなどの形で提供されているものがある[6]。

特殊なデバイスやソフトをユーザに個別に配る導入作業が高コストであること、ユーザにとっても同期設定などに時間や手間がかかり運用に課題を残す。

(2) パスワード生成ツール

パスワード生成ツールはパスワードを条件に合わせて提案してくれるシステムをいう[7]。お好みのパスワードを自動生成することができるツールでパスワードに使用する文字の種類（数字、英文字、記号)、文字数の長さ、生成する個数を指定可能で希望のセキュリティ強度、文字、文字数、個数を入力、選択後に「生成」ボタンをクリックすることでパスワード生成することができる。例えば、m4cu9d などのようにランダム生成されるため不規則かつ多様なパターンを提案してくれる。

しかし、不規則がゆえに覚えにくく、記憶情報として提案された文字列を覚えておくことに課題を残す。

(3) パスワードヒント

EpisoPass は忘れることがないエピソード記憶にもとづく秘密の質問を使って強力なパスワードを生成/管理するシステムである[8]。ユーザが作成した秘密の質問への回答にもとづいてシード文字列を換字することによってパスワード生成する。シード文字列や解答のバリエーションによって異なるパスワードが生成されるので様々なサービスに対して異なるパスワードを生成できることに加え、シード文字列を逆計算することにより既存のパスワードの管理もできる。適切な運用により、パスワードに関連するあらゆる情報を秘密にすることなく強力なパスワードの生成/管理ができる。しかし、ローカル保存した秘密の質問が漏洩するとパスワードが類推されやすくなる脅威が生じる。また、エピソード記憶に結び付いた画像と質問をユーザが用意しなくてはならない。

(4) パスワード更新の課題

自動パスワード作成ツールが提案してくれるような複雑な文字列であっても長期間に渡って何度も使っていれば記憶可能だが、半年ごとにパスワード更新していてはパスワード忘れに伴うトラブルを避けにくい。

パスワードを忘れないようにパスワードヒントとなる質問文を登録しておく方法では、連想が成立する範囲のパスワードに使えるが、近年では数字や記号の組み合わせを求められていて、より複雑なパスワード変更がユーザの責任に預けられている。むやみにパスワードを複雑にするたびに記憶が困難になり、個人で管理することができずメモのようなものに書いておくと盗み見される危険を伴う。度々パスワードの変更を求められると、変更パターンが似たようなものになりがちで脆弱化し、変更パターンなどに偏りが現れることもある。

パスワード更新では、安全なパスワードは覚えにくく、覚えやすいパスワードは脆弱であるというジレンマがある。すなわち、更新文字列の多様性と、記憶上の再現性を両立することが難しい。

3. 人工生命技術を用いたパスワード更新個人管理方式

3.1 利用イメージ

ある画像を見て想起する言葉が個人的経験や知識などによって個人差があることに着目し、人工生命の成長過程を見て想起する用語を用いて、更新パスワードの多様性と再現性を確保するパスワード更新個人管理方式を提案する。

人工生命の成長過程のバリエーションを描いた絵柄をあらかじめ多種類用意しておき、想起画像と呼ぶ。時間経過によって想起画像を入れ替えることによって、人工生命の成長を示す。2 分岐構造を用いて成長の仕方を管理し、同じ時間経過でも乱数を用いてユーザによって異なる想起画像を出力する。人工生命の成長が進み、想起画像が変化するが、パスワード自体を管理しない。想起画像を見て思いつく文字列をユーザのパスワードとする。

提案方式を実装搭載したパスワード提案システムの利用イメージを図 1 に示す。利用者が別システムのサービスを利用する際にパスワードが求められる。そこでユーザはパスワード提案システムを起動する。パスワード提案システムは人工生命の成長過程を表示する。ユーザは想起画像を見てパスワードを想起する。そのパスワードを別システムに入力し、ユーザ認証をパスすればサービスを受ける。

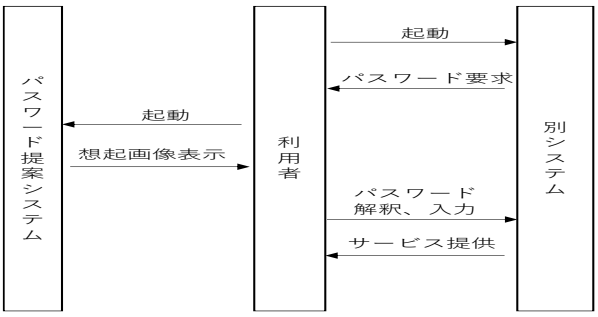

図 1　想定する利用イメージ
Figure 1　Assumed image of a usecase.

3.2 ソフトウェア構成

提案方式の処理は、（1）初期設定処理、（2）想起画像提案処理、から構成する。初期設定処理は初期時間と乱数としての育成変数を設定する。想起画像提案処理は、想起画像を初期時間と現在時刻をもとに計算した経過時間、育成変数に基づいた想起画像を表示する。

初期設定処理で利用する初期時間の取得で用いる数値は1970年1月1日から現在までの経過時間をミリ秒単位で取得できる関数を用いる。育成係数は1から100の乱数で取得した数値を用いる。これらの取得した数値を数値データとして保存し、セキュア領域に格納する。想起画像提案処理ではセキュア領域に格納された数値をもとに想起画像を判別する。想起画像は2分岐の木構造上でセキュア領域に格納されており対応する画像を表示させる。ソフトウェア構成を図2に示す。

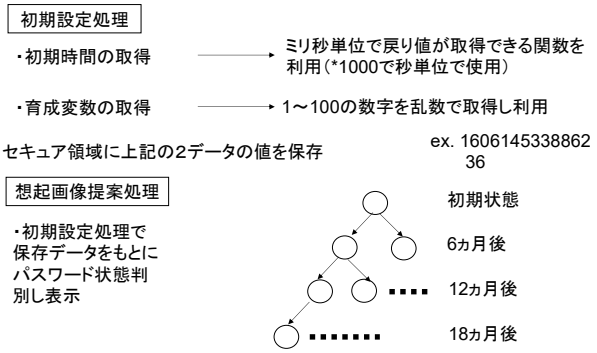

図 2　ソフトウェア構成図

Figure 2　Software architecture.

3.3 入出力データフロー

起動すると、初期設定処理でテキストファイルに格納した初期時間と育成係数を読み込む。現在の時刻を取得し、初期時間と現在時間をもとに経過時間を取得する。成長する時刻を設定し、経過時間、育成係数をもとに現在の状態を判別しディスプレイに出力する。

2つの処理のデータフローを図3に示す。

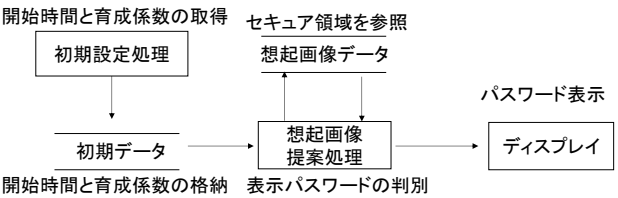

図 3　パスワード更新個人管理方式のデータフロー

Figure 3　Dataflow.

3.4 初期設定の処理フロー

初期設定処理を起動することでシステムの開始時間を取得し、初期データをセキュア領域に格納する。次に、育成係数を1から100の数値を乱数的取得する。また、その値をテキストファイルに格納する。これらの手続きを図4に示す。

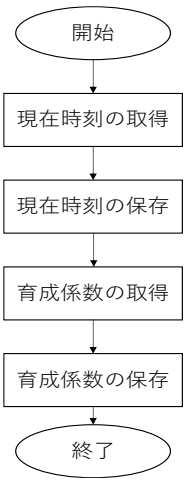

図 4　初期設定の処理フロー

Figure 4　Process flow for initialization.

3.5 想起画像提案の処理フロー

想起画像提案処理の処理フローを図5に示す。

Step 1. 画面操作によりプログラムを起動する。

Step 2. （Step.1）で保存したテキストファイルを読み込み、育成係数を取得する。

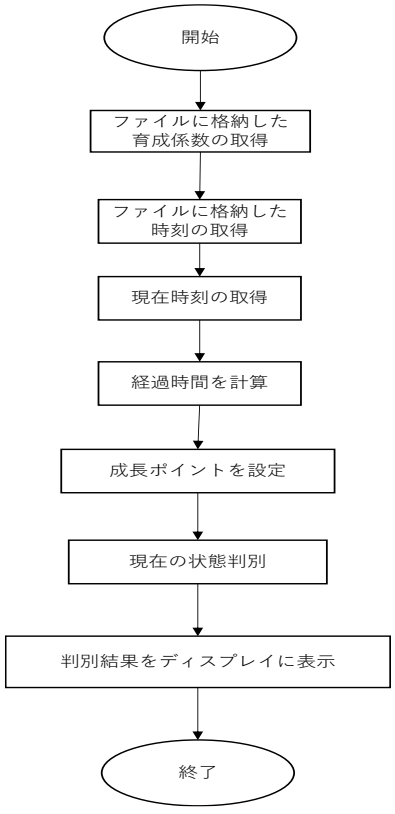

図 5　起画像提案の処理フロー

Figure 5　Process flow for displaying remeberance image.

Step 3. （Step.1）で保存したテキストファイルを読み込み、初期時間を取得する。
Step 4. 現在の時刻を取得する。
Step 5. 取得した現在の時刻と初期時間の差を求め、これを経過時間と呼ぶ。
Step 6. 成長する時刻を変数とし成長する時刻を定める。経過時間と育成係数をもとに育成状態の判別をする。
Step 7. 想起画像 15 枚をセキュア領域に保存しておき、2 分岐構造を用いて育成係数、経過時間をもとに判別する。
Step 8. 判別した育成状態をディスプレイに表示にさせる。（ユーザは表示した想起画像を元にパスワードを想起する。）

4. 評価実験

提案方式を実装したプロトタイプを開発し、評価実験を行った。

4.1 プロトタイプ

想起画像として、鶏キャラクターの成長過程を卵から焼き鳥まで描いた絵柄を準備した。想起画像の一覧を図 6 に示す。1 から 15 で割り振られた通し番号はプロトタイプで画像を管理する番号である。

図 6 想起画像の一覧
Figure 6 Remeberance images.

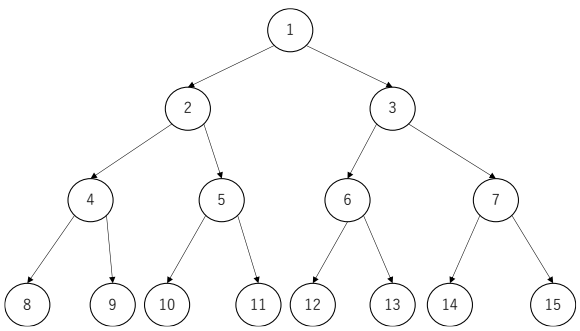

図 7 成長過程ツリー
Figure 7 Glowth tree.

図 7 に成長過程の管理構造を示す。人工生命は二分木に基づいてユーザごとに 4 段階の成長を行い、最下層では 8 通りの想起画像のいずれかが出力される。

4.2 実験方法

4.2.1 パスワード更新での想定する運用

パスワードは更新が半年ごとに求められる想定の下で、人工生命は 2 年間の育成で 4 段階成長して半年ごとに姿形を変えることとする。パスワード長は 8 桁以上とする。

4.2.2 パスワード評価方法

実際に想起画像で個性的なパスワード作ることができるか、同じ想起画像をもとに同じパスワードを再現できるか、という多様性と再現性についての検証実験を行う。

(1) **再現性評価**

被験者に従来方式と提案方式で生成されたパスワードを記憶させる。1 日後、7 日後の記憶されている割合で比較評価する。

(2) **多様性評価**

多様性の評価値として、2 つのパスワード文字列のレーベンシュタイン距離（編集距離）を計算する。2 つの文字列を同じにするために必要な編集操作（挿入，削除，置換）の最小回数を編集距離という[3, 11]。図 8 の計算手順において、比較文字列での i 番目の文字 x(i)と j 番目の文字 x(j)が異なる場合の編集操作コスト値の cost について、文献[11]では cost = 2 であり、文献[3]では cost = 1 である。文献[3]では Web 計算サービスが提供されていて小規模実験が簡便であり、本報告の実験は文献[3]の計算に基づく。

編集距離の値が大きいと、2 つの文字列が似ておらず、生成したパスワードの多様性が高い。すなわち、パスワード更新個人管理方式の備えるべき多様性の指標として好ましい。

Initialization:
$D(i, 0) = i$
$D(0, j) = j$

Recurrence Relation:
For each $i = 1 .. M$
For each $j = 1 .. N$

$$D(i,j) = min \begin{cases} D(i-1,j)+1 \\ D(i,j-1)+1 \\ D(i-1,j-1) \end{cases} + \begin{cases} cost & x(i) \neq x(j) \\ 0 & x(i) = x(j) \end{cases}$$

Termination:
$distance = D(N, M)$

図 8 レーベンシュタイン距離の計算方法[11]
Figure 8 Levenshtein distance.

4.2.3 実験手順

提案システムを用いての評価実験法は既存システム同様に被験者を集い、ある 1 つの想起画像を見てもらいパスワードを作ってもらう。その作られたパスワードをもとに多様性を評価する。続いて同じように 1 日目、7 日目にパスワードを想起画像で思い出せるかという再現性についても評価する。図 9, 図 10 は、それぞれ従来方式、提案システムを評価する方法を実験作業の流れとして示す。

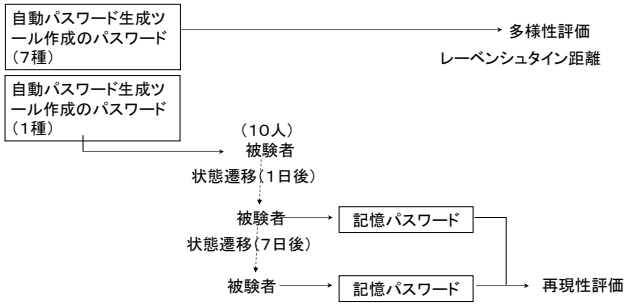

図 9　従来方式の実験手順

Figure 9　Procedure for evaluating conventional method.

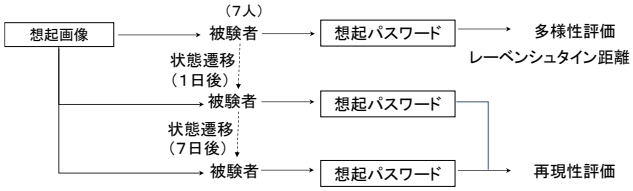

図 10　提案方式の実験手順

Figure 10　Procedure for evaluating proposed method.

4.3 実験結果

4.3.1 想起パスワード例

評価実験向けにプロトタイプが示した想起画像の例を図 11 に示す。プロトタイプを Java 実装し実行した際の表示画面である。図 11 において、左の図は経過時間 0 カ月から 6 カ月で表示される全ユーザ共通に表示される想起画像である。図 7 の①に当たる。次に、右の図に関しては経過時間 12 カ月から 18 カ月で表示される画像の一つである。図 7 の④に当たる。例で示されているものは実験で実際に想起されたパスワードの一部である。

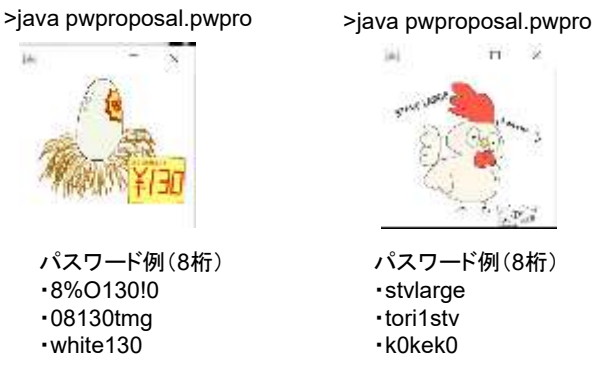

図 11　評価実験での想起画像とパスワードの例

Figure 11　Example rememberance images and passwords.

4.3.2 再現性と多様性の評価実験

被験者 10 名にパスワード自動生成ツール [7]を用いてランダムに生成された 8 桁のパスワードを記憶させた。1 日後には 8 名が記憶しており、7 日後には 5 名に減少した。それぞれの再現性は 80%, 50%である。一方、提案方式の想起画像をもとに 7 名の被験者に生成させ 1 日後に再現性のテストした結果、7 名全員が想起画像を元にパスワードを再現した。続いた 7 日後にも同じテストしたが 7 人ともが想起画像を元に再現した。いずれも再現性は 100%である。以上の実験結果をまとめて表 1 に示す。

多様性の実験では被験者 6 名(A～F)に対して、提案方式で想起されたパスワード同士の編集距離の平均値を計算した(表 2)。さらに、従来方式 [7]を用いて被験者と同じ文字数条件で生成したパスワード同士の編集距離の平均値を計算した(表 3)。従来方式の平均値は提案方式より多様性が高く、編集距離の差は 2.46 (=9.93 - 7.47)である。提案方式では 2～3 文字ほど生成されるパスワードが偏り、130 という想起画像中の数値に起因する。

提案方式は更新文字列の多様性と、記憶上の再現性をある程度両立する。なお、実験では被験者は総じて記憶力がよく、実験目的を理解した上で協力的だった。

表 1　再現性の評価実験結果

Table 1　Recall test result.

比較項目	被験者数	再現性 1 日目	再現性 7 日目
従来方式 [7]	10	8 人(80%)	5 人(50%)
提案方式	7	7 人(100%)	7 人(100%)

表 2　多様性の評価実験結果（提案方式）

Table 2　Variety test result for the proposed method.

	A	B	C	D	E	F
A	0	12	10	11	10	12
B		0	5	7	5	4
C			0	7	5	5
D				0	7	7
E					0	5
F						0

Average: 7.47

A: urikiregomen130, B: t0008130, C: egg¥0130

D: Tamago13, E: White130, F: 08％￥130

表 3　多様性の評価実験結果（従来方式[7]）
Table 3　Variety test result for the conventional method.

	A	B	C	D	E	F
A	0	14	14	14	13	14
B		0	8	8	8	8
C			0	8	8	8
D				0	8	8
E					0	8
F						0

Average: 9.93

A: pef5xpy7i8jq777, B: b9gk37x5, C: .r2woy$+
D: cF8UfudR, E: sB2pgqnr, F: g_7(z8h

4.4 従来方式との定性的比較

評価実験向けにパスワード生成ツール[7]、パスワードヒント[8]と提案方式の比較を表 4 に示す。記憶方法に関し、パスワード生成ツール[7]の記憶方法は提案された文字列を文字列として記憶しておく方法をとる。これは年齢、や記憶力の個人の能力などが大きく関わると考えられる。パスワードヒント[8]を用いる方式では自らの経験とそれに対する質問で記憶する。忘れがたい記憶臆しておくことは容易である考える。提案方式では、想起画像をみることによってパスワード生成する。記憶に関してはパスワードヒント[8]に似た形式をとる。

文字列の脆弱性に関して、パスワード生成ツール[7]はランダムで文字列を生成するため強固である。パスワードヒント[8]ではローカル保存された情報の管理に頼る部分が大きいと考える。提案方式ではセキュア領域のセキュリティに頼る部分が大きいと考えらえる。

最後に文字列の多様性に関して、パスワード生成ツール[7]は指定する条件次第で多様なパターンを生成できる。パスワードヒント[8]では、経験記憶と質問次第で多様であると考えられる。提案方式では適切な想起画像の種類や情景、状態である程度多様と考える。

表 4　従来方式との定性的比較
Table 2　Qualitative omparison.

比較項目	パスワード生成ツール[7]	パスワードヒント[8]	提案方式
記憶方法	文字記憶	経験記憶と質問	想起
文字列の脆弱性	強固	適切な運用の元で強固	適切な実装の元で強固
文字列の多様性	多様	ある程度多様	ある程度多様

5. おわりに

人工生命を用いたパスワード個人管理方式についての一考察として画像を用いたパスワード記憶と生成を軸に考えた。結果既存の技術より記憶面では優れていたが、多様性という面で少し物足りなさを感じた。時間の経過に伴いパスワードに対応する画像が変化していき、ユーザによって成長の仕方も変わっていき想起画像も変化することから今夏の実験よりも多様度は高くなると考えられる。

今後の課題には多様性の向上を含む。、本提案方式では想起画像により大きく結果が変わるものであると考える。よって想起画像をより複雑にすることでより良い結果が得られるとともにこの提案方式が有効であることも示せるだろう。現状、有効であるが今後の展望として想起画像をさらに増やし、多様なパスワードを生成できるようにする。規模を拡大し実用的なシステムにしていこうと考えている。

謝辞　田嶋心夏氏に人工生命の絵柄を提供いただいた。

参考文献

[1] Levenshtein V. I., Binary Codes Capable of Correcting Deletions, Insertions and Reversals, 1965, Doklady Akademii. Nauk SSSR, vol. 163, no. 4, p.845-848.
[2] “警察庁 サイバー犯罪対策：調査・研究”, https://www.npa.go.jp/ cyber/research/index.html (online 2020/12)
[3] “Javascript でレーベンシュタイン距離の実演”, http://www.mwsoft .jp/programming/munou/javascript_levenshtein.html (参照 2020-12-25)
[4] 妹尾尚一郎ほか. 生体認証によるネットワーク個人認証システム. 情報処理学会論文誌. 2003, vol. 44, no. 4, p. 1111-1120.
[5] 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. 2011, 電子情報通信学会技術研究報告, ライフインテリジェンスとオフィス情報システム, vol. 9, p. 111-286.
[6] “セキュリティトークン”, http://e-words.jp /w/ (参照 2020-12-25)
[7] “パスワード生成（パスワード作成）ツール”, https://www.luft.co. jp/cgi/randam.php (参照 2020-12-25)
[8] 増井俊之. EpisoPass: エピソード記憶にもとづくパスワード管理. 2013, コンピュータセキュリティシンポジウム論文集, p. 933-940.
[9] IPA. 情報セキュリティ白書. 2019 online (参照 2020-12-25)
[10] 長谷川孝博ら. 大学情報基盤におけるパスワード定期更新の運用と利用者動向. 2013, 学術情報処理研究, vol. 17 no. 1, p. 107-114.
[11] D. Jurafsky: Edit distance, Stanford CS124 website archive, https://web.stanford.edu/class/cs124/ (参照 2020-12-25)
[12] 符儒徳. 国際大学生の情報セキュリティ意識調査. 2020, 開智国際大学紀要, vol. 19, p. 177-192.
[13] 山田恒夫, 情報のセキュリティと倫理, 2014, 放送大学教育振興会.