SURE 静岡大学学術リポジトリ
Shizuoka University REpository

機械解読耐性の向上とユーザのメンタル負荷軽減を両立するCAPTCHA出題形式に関する検討

メタデータ	言語: Japanese 出版者: 公開日: 2017-11-02 キーワード (Ja): キーワード (En): 作成者: 佐野, 絢音, 藤田, 真浩, 西垣, 正勝 メールアドレス: 所属:
URL	http://hdl.handle.net/10297/10421

機械解読耐性の向上とユーザのメンタル負荷軽減を両立する CAPTCHA 出題形式に関する検討

佐野 絢音[†1]　藤田 真浩[†1]　西垣 正勝[†1]

概要：著者らは、CAPTCHA の総当たり攻撃耐性とユーザのメンタル負荷軽減の両方を向上させる出題形式「Directcha-maze」を提案している[佐野 17]．Directcha-maze は、分岐点に 3 次元オブジェクトが配置された迷路形式の出題方式となっており、スタートから各オブジェクトの正面方向を辿ることによってゴールに到達できる．「迷路を解く」というタスクの中に「オブジェクトの正面を答える」という CAPTCHA タスクを複数埋め込むことによって，CAPTCHA タスクを繰り返すことに対するユーザのメンタル負荷軽減をしている．さらに，迷路形式にはゲーム要素が含まれるため，ユーザは楽しみながら CAPTCHA を回答できる．本稿は，Directcha-maze に関してコンセプトの再検討とさらなるユーザビリティ向上の実現を提案するものである．具体的には，以下の二点から構成される．(i) Directcha-maze で CAPTCHA タスクを繰り返すことは，総当たり攻撃耐性の向上にとどまらず，機械学習攻撃耐性の向上にも効果を発揮することが示す．(ii) 回答時間の短縮を実現するために，ゴールを複数設置する．改良した Directcha-maze の実験システムを実装し，その有効性を確認した．

キーワード： CAPTCHA，メンタル負荷，機械解読耐性，メンタルローテーション

A Study of CAPTCHA Configuration with Machine Attack Defensibility and User Convenience Consideration

Ayane Sano[†1]　Masahiro Fujita[†1]　Masakatsu Nishigaki[†1]

Abstract: In order to satisfy brute-force attack tolerance and user convenience, we proposed "Directcha-maze" [Sano 17]. In it, multiple CAPTCHA tasks are implicitly embedded in a maze. What users are conscious of is a maze solving task, and thus it is expected that users do not feel psychological burden for repeating CAPTCHA tasks; rather, solving a maze should be an enjoyable task for users. In this paper, we show another advantage of Directcha-maze which we did not find in the prior work and, in addition, propose a method to reduce the response time. Specifically, this paper is organized as follows. (i) We rethink the concept of Directcha-maze. As the result, the authors found that our method contributes to improve not only brute-force attack tolerance but also machine learning attack tolerance. (ii) In order to reduce the response time of the method, we propose using some goals on a maze. Developing a system of the maze which has a start and four goals, we checked the effectiveness of the method.

Keywords: CAPTCHA, Psychological Burden, Machine Attack Tolerance, Mental Rotation

1. はじめに

Web サービスの普及により，自動プログラム（マルウェア）による Web サービス提供サイト等に対するスパムコメントやアカウントの不正利用が定常的に行われている．この対策のために，人間による正規利用とマルウェアによる不正利用を区別する技術が必要とされている．その技術の一つに CAPTCHA（Completely Automated Public Turing test to tell Computers and Human Apart）がある．CAPTCHA は人間には正解が容易であり，機械には正解が困難な問題をユーザに出題し，正解したユーザを人間と判定する技術である[1]．現在では，多くの Web サービス提供サイトで文字判読型 CAPTCHA（図 1）が採用されている．しかし，この CAPTCHA は OCR（自動文字読取）や機械学習を備えたマルウェアにより突破され得ると指摘されている[3]．これらのマルウェアに対抗するために，人間のより高度な認知能力を利用した，画像の意味を問う CAPTCHA（画像 CAPTCHA）がかねてから提案されてきた[2][4][7]．これらの CAPTCHA は，人間が高度な認知能力を利用して解くタスク（CAPTCHA タスク）を用意し，そのタスクを行えたユーザを人間と判定するものである．しかし，これらの CAPTCHA は，1 タスクあたりの総当たり数が少ない傾向にあることが知られている．これら画像 CAPTCHA において，文字判読型 CAPTCHA と同程度の総当たり数を確保するためには，ユーザにそのタスクを複数回行わせる必要が

図 1　文字判読型 CAPTCHA の認証画面例
Figure 1　Example of text-based CAPTCHA.

†1 静岡大学
Shizuoka University

ある．しかし，単純に CAPTCHA タスクを繰り返させるだけでは，ユーザの利便性を著しく減少させてしまう．

そこで著者らは，CAPTCHA タスクの繰り返しによる総当たり攻撃耐性の向上を達成しつつ，ユーザの利便性を維持する CAPTCHA 出題形式を模索している．その一実現例として，「Directcha-maze」と呼ぶ出題方式を提案・実装し，基礎実験を実施した[8][9]．提案方式は，1 枚の画像内に複数の 3 次元オブジェクトを配置した迷路形式の出題方式である．迷路の各分岐点にはそれぞれ 1 体のオブジェクトが置かれており，各オブジェクトの正面方向が正しい分岐路を示すようになっている。全オブジェクトの正面方向を正しく識別し，スタートからゴールまでの経路を正しく辿ることができたユーザを正規ユーザ(人間)として判定する．スタートからゴールまでの経路の候補数が Directcha-maze の総当たり数となる．

人間は，分岐点のオブジェクトの向き（正面方向）を識別しながら，スタートからゴールまで迷路を辿っていくが，ここにはメンタルローテーションと呼ばれる人間の高度な認知能力が関与している．すなわち，「オブジェクトの正面方向を識別する」という課題は CAPTCHA タスクの一種であり，著者らはこれを Directcha タスクと呼んでいる[7]．Directcha-maze では，ユーザは，各分岐点のオブジェクトに対して Directcha タスクを行っている．しかし，ユーザが認識するタスクは「迷路を解く」ことであり，個々の Directcha タスクは，アンコンシャスなサブタスクとなっている．これによって，Directcha タスクを繰り返し行うことに対するユーザのメンタル負荷が軽減されることとなる．さらに，迷路形式にはゲーム要素が含まれるため，ユーザは楽しみながら CAPTCHA（Directcha-maze）を回答できる．

本稿は，本方式 Directcha-maze に関して，コンセプトの再検討，改良，およびさらなる実験を施すものである．本稿が取り扱う具体的な問題設定については，2 章の最後で説明する．

2. Directcha-maze

2.1 メンタルローテーション CAPTCHA

Directcha-maze は，先行研究である Directcha [7]および Sketcha [4]から一部着想を得た研究である．これら二つの CAPTCHA はメンタルローテーションと呼ばれる人間の高度な認知能力を利用している．メンタルローテーションとは，人間はある視点から写された 2 次元オブジェクトや 3 次元オブジェクトを頭の中で回転させ，異なる視点から写された姿形を識別する能力である[5][6]．

2.1.1 Sketcha

Sketcha の認証画面例を図 2 に示す．認証画面には，8 問の問題画像が提示される．各問題画像は，3 次元モデルを 2 次元へ投影し，線画化した 2 次元画像であり，各 2 次元画像に対して 0，90，180，270 度のいずれかの回転が施されている．問題画像をユーザが 1 回クリックするごとに，2 次元画像が 90 度回転し，画像を正立状態（0 度の回転）に戻すことができたユーザを正規ユーザとして判定する．すなわち Sketcha は，「3 次元オブジェクトの鉛直方向を回答する」というタスクを利用している（以下，Sketcha タスクと呼ぶ）．人間の正答率は 1 問（1 タスク）あたり 98.6%であることが実験によって判明している．一方，回転方向を 4 つに限定しているため，CAPTCHA タスク 1 回あたりの総当たり数は高々4 通りである。また，機械学習に対しては 1 問あたり 61.0%の確率で突破されている．

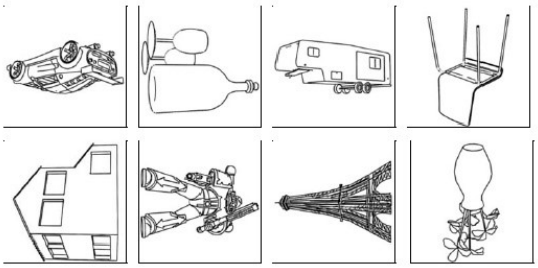

図 2　Sketcha の認証画面例

Figure 2　Example of Sketcha.

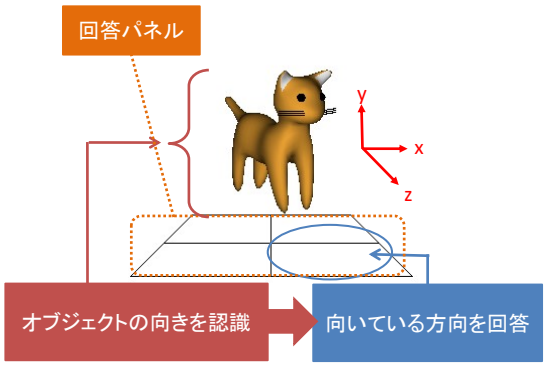

図 3　Directcha の認証画面例

Figure 3　Example of Directcha.

2.1.2 Directcha

Directcha の認証画面例を図 3 に示す．認証画面には，1 体の 3 次元オブジェクトと回答用パネルが表示される．パネルは「右前」「右後」「左前」「左後」に 4 分割されている。ユーザは，画像中のオブジェクトの向きに対応するパネルをクリックして回答する．すなわち Directcha は「3 次元オブジェクトの正面方向を回答する」というタスク（以下，Directcha タスクと呼ぶ）を利用している．人間であれば，メンタルローテーションを活用し，画像中のオブジェクトがどちらの方向を向いているか識別することが可能である[10]．基礎実験ではあるが，人間の正答率は 1 問(1 タスク)あたり 98.7%であることが示されている．一方，回転パネルが 4 分割されているため、Directcha における CAPTCHA タスク 1 問あたりの総当たり数は高々4 通りである．機械学習による評価は，現在までに実施されていないが，出題形式が類似している点から Sketcha と同程度であると考え

図 4　Directcha-maze の認証画面例

Figure 4　Example of Directcha-maze.

られる．

2.2 Directcha-maze

2.2.1 概要

Directcha や Sketcha は，メンタルローテーションと呼ばれる高度な認知能力を利用している点で非常に興味深い CAPTCHA である．しかし，Directcha タスクや Sketcha タスクには 1 回あたりの総当たり数が少ないという問題がある[a]．これに対する単純かつ容易な対策は，タスクを複数回繰り返すことによって総当たり数を確保する方法である．しかし，CAPTCHA タスクの繰り返しは，ユーザのメンタル負荷（利便性）を大きく増加させる．

そこで著者らは，総当たり攻撃耐性を向上しつつ，ユーザのメンタル負荷増加を抑制する CAPTCHA 出題形式として，「Directcha-maze」と呼ぶ出題方式を提案した[8]．Directcha-maze のコンセプト図を図 4 に示す．認証画像には，格子が描画され，ゴール地点を除く各格子点上には，「向き」を有する 3 次元オブジェクトが配置されている．各 3 次元オブジェクトは，4 方向（左後，右後，左前，右前）のいずれかを向いている．ただし，格子のスタート地点（図 4 の例では格子点(1,1)）からゴール地点（図 4 の例では格子点(4,4)）へ，オブジェクトの正面方向を辿っていけば到着できるように，オブジェクトの向きが設定されている．認証時にユーザは，画像中の各 3 次元オブジェクトの向きを識別し，それらの正面方向を辿る．オブジェクトの向いている正面方向を正しく識別し，スタート地点からゴール地点まで辿る（迷路を解く）ことができたユーザを正規ユーザ（人間）として判定する．

2.2.2 総当たり数

正解経路上に存在するオブジェクトの総数（ユーザがスタートからゴールまで辿っていく間に，通るオブジェクトの総数）を n とする．

Directcha-maze 1 問あたりの総当たり数は，スタートからゴールへの経路の候補数となる．ただし、経路の中には，n が非常に大きい経路も存在する．利便性をふまえると，実際の運用では，スタートからゴールまでのすべての経路から n が小さい経路から順に，必要な総当たり数となるまで抽出して利用することが望ましい．たとえば，図 4 に記した 6×6 の Directcha-maze の例では，n が 12 以下の経路のみを使用するという制限を加えると、経路の候補数（すなわち、この Directcha-maze の総当たり数）は 2172 通りとなる．

2.2.3 メンタル負荷の削減

人間であれば，各オブジェクトの向きを認識して，スタート地点からゴール地点へと正しい道を辿り，Directcha-maze を解くことが可能である．ユーザはスタートからゴールまで n 体のオブジェクトを辿る中で、n 回の Directcha タスクを実施している．しかし，ユーザが認識するタスクは「迷路を解く」ことであるため，n 回の Directcha タスクはアンコンシャスなサブタスクとなっている．これによって，Directcha タスクを繰り返し行うことに対するユーザのメンタル負荷が低減される．さらに，迷路形式にはゲーム要素が含まれるため，ユーザは楽しみながら CAPTCHA を回答できる．このゲーム性によって，ユーザのメンタル負荷がさらに削減される．

2.2.4 迷路形式に適する CAPTCHA タスク

迷路形式の出題方式においては，分岐点ごとに CAPTCHA タスクが配置される．これら個々の CAPTCHA タスクは，ユーザに「複数の分岐路の内の 1 つを選択させる」タスクでありさえすれば，任意の CAPTCHA を使用できる．すなわち，迷路形式の CAPTCHA を実現する場合には，サブタスクに「Sketcha タスク（オブジェクトの鉛直方向を識別するタスク）」を利用することも可能である．しかし，Directcha タスクをサブタスクとして用いることは，Sketcha タスクをサブタスクとして用いる場合よりもアド

a 本稿では紙面の関係上，Directcha および Sketcha に限定して，総当たり数が少ないことを指摘しているが，この問題は（文字判別型 CAPTCHA 以外の）画像 CAPTCHA 全般にいえる課題である．

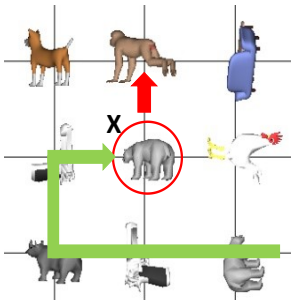

図 5　Sketcha をサブタスクとした場合

Figure 5　Example of Sketcha-maze.

バンテージが存在する．

Sketcha タスクを用いて迷路形式の出題方式を実現した例を図 5 に示す．この方式においては，ユーザは，格子点 X に到達した場合，X にあるオブジェクトの鉛直方向を識別することによって次の格子点へと移動する．しかし，人間は日常的に，オブジェクトの顔や体が向いている方向を「オブジェクトの向き」として認識している．また，横に倒れたオブジェクトや倒立したオブジェクトを見慣れていない．このため，Sketcha タスク（オブジェクトの鉛直方向を識別するタスク）のメンタル負荷は，Directcha タスク（オブジェクトの正面方向を識別するタスク）と比較して高くなると考えられる．

2.2.5 基礎実験による有効性の検証

文献[8]で，著者らは，被験者 5 名に対して基礎実験を行って Directcha タスクを単純に繰り返す場合，Directcha-maze を解く場合，Sketcha-maze を解く場合のユーザビリティを比較した．これら 3 つの方式の総当たり数を 4096 で統一し（Directcha を単純に 6 問解く，総当たり数 4096 の Directcha-maze を 1 問解く、総当たり数 4096 の Sketcha-maze を 1 問解く），実験を行った．メンタル負荷，認証時間，正答率の観点から分析を行った結果を以下に示す。

- Directcha-maze の 1 問あたりの正答率、Sketcha-maze の 1 問あたりの正答率、Directcha を単純に 6 問解く場合の正答率は、それぞれ 96.0%，96.0%，96.0% であった。
- Directcha-maze の 1 問あたりの平均回答時間、Sketcha-maze の 1 問あたりの平均回答時間、Directcha を単純に 6 問解く場合の平均回答時間は、それぞれ 6.71 秒、6.76 秒、5.49 秒であった。
- 実験後のアンケート結果より，2.2.2 節，2.2.3 節に記した内容が妥当であることが示された．

メンタル負荷と正答率については、Directcha-maze の効果が確認された一方で，Directcha-maze 1 問を解くより，Directcha タスクを 6 問繰り返し解くほうが（メンタル負荷は小さいものの）回答時間は長いという課題が残るケ課となった．

2.3　本稿が取り扱う課題

本稿は，上述した Directcha-maze に関してコンセプトの再検討，改良，さらなる実験を行うものである．具体的には，以下の二つの課題を取り扱う．

① Directcha-maze を検討する中で，迷路形式で CAPTCHA タスクを繰り返す行為が，機械学習攻撃耐性の向上にも大きな効果を発揮することを示す（3 章）．

② 文献[8]で実装した Directcha-maze のシステムでは，ユーザの回答時間が（単純に Directcha タスクを繰り返す場合と比較して）長くなってしまうという課題があった．そこで，Directcha-maze に対してゴールを複数に設置するという改良を加えることで、回答時間の短縮を試みる（4 章，5 章）。

3.　迷路形式による機械学習攻撃耐性の向上

2.2.2 節に記したとおり，Directcha-maze では，迷路形式の採用によって，CAPTCHA 1 問あたりの総当たり数を「スタートからゴールまでの経路の候補数」に高めている．迷路のサイズ，スタートやゴールの位置，通るオブジェクトの総数 n の範囲を変えることによって，総当たり数を増加させることが可能な方式である[8][9]。

これに加え，CAPTCHA タスクの繰り返しは、CAPTCHA の機械学習攻撃耐性の向上にも有効である．以下では、CAPTCHA タスク 1 回あたりの人間の正答率を *HAR*，マルウェアの正答率を *MAR* として、Directcha-maze の機械学習耐性について説明する。

迷路形式の CAPTCHA には、1 問あたりに n 回の CAPTCHA タスクが組み込まれている．すなわち，人間も機械も、n 回の CAPTCHA タスクをすべて正解できなければ，迷路を正しく解くことができない．このとき，CAPTCHA タスク 1 回の場合には $HAR - MAR$ であった「人間とマルウェアの正答率の差」が，迷路形式（CAPTCHA タスクの n 回の繰り返し）を採ることによって $HAR^n - MAR^n$ となる．

CAPTCHA とは「人間には正解が容易であり，機械には正解が困難な問題」である。すなわち、*HAR* は十分に高く、*MAR* は十分に低いことが求められる。Directcha タスクや Sketcha タスクは，人間にとって容易なタスクであるため，1 問あたりの *HAR* は十分高いと考えてよい．一方で，近年の機械学習の急激な進歩によって、Directcha タスクや Sketcha タスクの 1 問あたりの *MAR* も（人間の正答率には及ばないものの）相応に高い値となってきている．したがって，CAPTCHA タスク 1 問あたりの人間とマルウェアの正答率の差 $HAR - MAR$ は僅少となってしまっているのが現状である。

一方で，CAPTCHA タスクを n 回繰り返した場合は、次のようになる．*HAR* は，100%に近い値であるため，n が増えていった時の HAR^n が減少していく速度はそれほど早く

ない. これに対して *MAR* は,（*HAR* に肉薄してきているが）*HAR* には及ばない値である．したがって，*n* が増えていった時に MAR^n が減少していく速度は，HAR^n と比べて速い．すなわち，*n* を増やすことによって，HAR^n–MAR^n は増大することになり，人間と機械の正答率の差が拡大（機械学習攻撃耐性の向上）される[b].

たとえば, 2.1 節で示した文献[4][8]の実験結果（Directcha タスクの *HAR*:98.7%, Sketcha タスクの *HAR*:98.6%、Sketcha タスクの *MAR* : 61.0%）を参考に，*HAR* を 98.0%、*MAR* を 60.0%と考えると、CAPTCHA タスク 1 問あたりの人間と機械の正答率の差 *HAR–MAR* が 38.0%（98.0%-60.0%）であるのに対し、CAPTCHA タスク 6 問あたりの人間と機械の正答率の差 HAR^6–MAR^6 は，およそ 84.0%（98.0^6-60.0^6）まで広がる．

ユーザが *n* 回の CAPTCHA タスクをアンコンシャスのサブタスクとして実施することができる迷路形式の CAPTCHA は，ユーザにメンタル負荷を強いずに，人間と機械の正答率の差を広げる（機械学習攻撃耐性を向上させる）ことに成功している。

4. ゴールの複数設置による回答時間の短縮

2.2.5 節に示したとおり, 文献[8]では, Directcha-maze 1 問を解くより, Directcha タスクを 6 問（Directcha-maze 1 問と同じだけの総当たり数を確保するのに必要な問題数）解くほうが（メンタル負荷は小さいものの）回答時間は長いという課題が残っていた. 本稿では,「ゴールを複数設置する」というアイデアの導入によって、この課題の解決を試みる.

文献[8]の Directcha-maze では，スタートとゴールを一つずつ，固定した位置に配置していた（イメージ図として，図 4 のコンセプトを参照されたい）．文献[8]では，総当たり数（スタートからゴールまでの経路の候補数）が 4096 となるように，スタートとゴールの位置，迷路のサイズ、経路上で通過するオブジェクトの総数 *n*（CAPTCHA タスクの繰り返し数）を設定した．具体的には,

- 迷路のサイズを 6×6 とした
- 迷路中の格子点 (1,1)をスタート， (4,4)をゴールとした.
- 経路の候補数は 4096（*n*=6 の経路が 20 通り，*n*=8 が 120 通り，*n*=10 が 516 通り，*n*=12 が 1516 通り，*n*=14 が 1924 通り）とした.

という条件になっている.

上記の設定においては、経路上のオブジェクト数 *n* が 6～14 であるので，ユーザは「総当たり数 4096 の Directcha-maze」を 1 問解くにあたって，Directcha タスクを 6 回から 14 回繰り返していることとなる. 一方で,「総当たり数 4 の Directcha」の単純な繰り返しで総当たり数 4096 を達成する場合は，Directcha タスクを 6 回行うだけでよく、Directcha-maze を 1 問を解く場合と比較して, 大幅に少ない回数ですんでいる. 著者らは, Directcha-maze の回答時間が遅くなっている理由はこの回数の差が原因であると考えた.

Directcha-maze で Directcha タスクを繰り返す回数 *n* を小さくするために，本稿では「ゴールを複数設置する方法」を提案する．ゴールを複数設置することによって，CAPTCHA の総当たり数はスタートから各ゴールまでの経路数の総数となる．したがって，ゴールが一つだけ設置してある場合と比較して，より小さな *n* で 4096 通りを達成可能である.

適切な迷路のサイズ，ゴールの数，スタートとゴールの位置を計算するプログラムを実装した．このプログラムの動作を簡単に説明すると，次のとおりである.

> 考えられるすべてのパラメータの組み合わせに対して，スタートからゴール（複数）までのすべての経路から *n* が短い経路が順に 4096 個の経路を利用する．抽出した 4096 通りの経路の *n* の平均値を求める．この平均値がもっとも小さくなるパラメータを利用する.

この結果，今回は,

- 迷路のサイズは 7×7 となった.
- (4,1)をスタート，(0,0)，(0,4)，(2,6) , (5,5)にそれぞれゴール（4 つ）を設置した.
- 4096 通りの経路の候補の内訳は、*n*=5 の経路が 10 通り，*n*=7 が 139 通り，*n*=9 が 775 通り，*n*=11 が 3172 通りであった.

5. ゴール複数設置による回答時間の短縮の確認

5.1 目的

ゴールを複数にすることが Directcha-maze（および，Sketcha-maze）の回答時間が短縮され, Directcha タスク 1 問（および、Sketcha タスク 1 問）と同程度の認証時間に収まることを確かめる.

5.2 実装

今回利用する実験システムは，文献[8]で実装したシステムの改良したものである[c]. Directcha，Sketcha，Directcha-maze，Sketcha-maze の 4 つの実験システムが含まれる．各システムは以下のように条件を統一してある.

- 総当たり数：4096 通りで統一をした.
- 利用するモデルの統一 : 各実験システムでは同じ 3 次元モデルを利用した．これら 3 次元モデルは，Web 上から収集した素材である. メンタルローテーションタスクを利用する都合上（向きを回答する都合上），モ

b 正確には、$HAR^n - MAR^n$ はある正の *n* の値で極大値を取るため，n をむやみに増やせば良いというわけではない。この点も考慮して，*n* を設定すべきである.

c 本稿の範疇を超えるため，詳細は述べないが，本章における実験は大規模実験に向けた予備実験という意味合いもあった．したがって，回答時間の短縮を測れたか否かを検証するという目的を超えた修正がなされている（回答時間の短縮に関わる議論に影響を与えるものではない）.

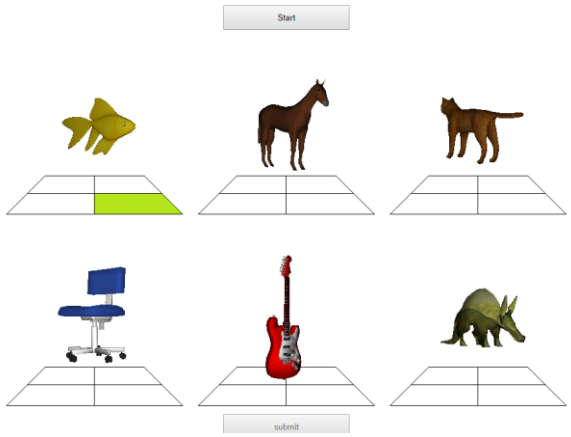

図 6　Directcha の実験システム認証画面例
Figure 6　Example of Directcha System.

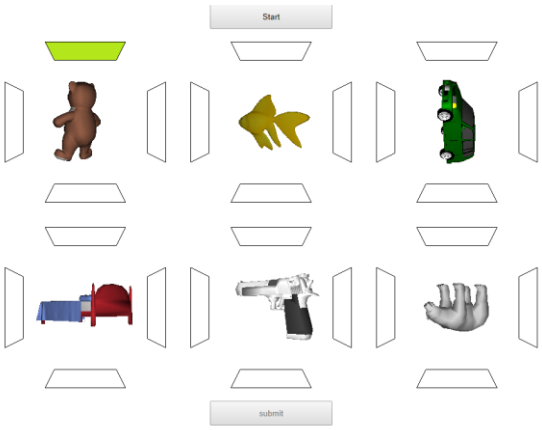

図 7　Sketcha の実験システム認証画面例
Figure 7　Example of Sketcha System.

デルを収集する過程で，上下前後関係が明瞭なモデルに限って収集をした．その結果，70 種類のモデルが収集された．練習と本番でモデルを変更することとし，練習で 20 種類のモデルを利用し，本番で 50 種類のモデルを利用して問題を生成した．なお，文献[8]では，30 種類のモデルを練習・本番で使いまわしていた．

- 画像の表示：問題画面上には，回答開始前から画像（群）が表示されている．
- 結果の表示：各問題画面には Submit ボタンが存在する．Submit ボタンが押されると，ユーザの回答が正解・不正解のどちらであったかと回答時間が記載されたダイアログが画面に表示される．ダイアログの OK ボタンを押すと，次のページへ遷移する．

5.3 実験システム

5.3.1 Directcha の実験システム

Directcha の実験システムの認証画面例を図 6 に示す．今回利用する Directcha の 1 問あたりの総当たり数は 4 通りである．問題 1 セットあたりの総当たり数を 4096 通りにするために，問題 6 問を 1 セットとして 1 ページ上に出題する．問題画像のサイズは，縦 300 画素×横 300 画素とした．各オブジェクトの y 軸の回転角度を 45 度，135 度，225 度，315 度の中からからランダムに 1 つ選んで回転している．

ユーザが，画面上部にある Start ボタンをクリックすると，そのページの回答が開始され，回答時間の計測が始まる．各問題画像において，ユーザはオブジェクトの向きに対応する回答パネルをクリックして回答する．選択後，クリックされたパネルは黄緑色に変更される（図 6 左上の問題は回答が完了した状態）．一度，回答を完了した後も，Submit ボタンをクリックするまでは回答を修正することが可能である．Submit ボタンは 6 問すべてを回答した後でないとアクティブにならない．6 問すべての問題に正解した場合に限って，「正解」と判定される．回答時間の計測は，ユーザが Start ボタンを押してから，Submit ボタンをクリックする前に解いた問題（6 問の Directcha の内，ユーザが最後に回答した問題）の回答パネルをクリックするまでとする．

5.3.2 Sketcha の実験システム

Sketcha の実験システムの認証画面例を図 7 に示す．各オブジェクトの上方向をクリックする形式である以外は，Directcha の実験システムと同じである．なお，オリジナルの Sketcha は，線画化したオブジェクト画像を利用しているが，今回の実験では，他の実験システムと条件を同一にするために，画像の線画化を行っていない．各オブジェクトは，各オブジェクトの y 軸の回転角度を 45 度，135 度，225 度，315 度の中からからランダムに 1 つ選んで回転させた後，z 軸に対して 0 度，90 度，180 度，270 度の中からランダムに 1 つ選んで回転している．

5.3.3 Directcha-maze の実験システム

Directcha-maze の実験システムの認証画面例を図 8 に示す．スタートとゴールの位置，経路の内訳は 4 章で述べたとおりである．ゴールが増えた以外は，問題画像のサイズは，縦 745×横 1200 画素とした．各オブジェクトの y 軸の回転角度は，45 度，135 度，225 度，315 度の中からからランダムに一つ選ばれる．x 軸，z 軸に関しては回転しない．

ユーザが，スタート地点にある旗をクリックすると，回答時間の計測が始まる．ユーザは，マウスを動かすことで，各オブジェクトの正面方向を辿る．辿った経過は，緑色の直線で表示される（図 8 は 3 体目までを辿った様子）．ある格子点 X から隣り合う格子点 X’へ移動した後，X’から X へ再度戻ることも可能である（その場合，X から X’は辿ったことにならず，画面上から X から X’の直線が消える）．ゴールまで辿った後，ゴールの旗をクリックしたら回答終了となる．Submit ボタンは，回答終了とともにアクティブとなる．回答時間の計測は，ゴールの旗をクリックした時点で終了している．

5.3.4 Sketcha-maze の実験システム

Sketcha-maze の実験システムの認証画面例を図 9 に示す．

図 8　Directcha-maze の実験システム認証画面例

Figure 8　Example of Directcha-maze System.

図 9　Sketcha-maze の実験システム認証画面例

Figure 9　Example of Sketcha-maze System.

表 1　実験結果

Table 1　Experiment results.

Directcha(1セットあたり)

被験者	正答率	回答時間[s]
1	5/5	5.76
2	5/5	7.40
3	5/5	6.61
4	4 /5	6.05
5	5 /5	5.43
平均	96.0%(24/25)	6.25

Directcha(1問あたり)

被験者	正答率	回答時間[s]
1	30/30	0.96
2	30/30	1.23
3	30/30	1.10
4	29/30	1.01
5	30/30	0.90
平均	99.3%(149/150)	1.04

Directcha-maze

被験者	正答率	回答時間[s]
1	5/5	5.17
2	5/5	6.05
3	5/5	6.38
4	5/5	6.48
5	4/5	7.62
平均	96.0%(24/25)	6.34

Sketcha(1セットあたり)

被験者	正答率	回答時間[s]
1	5/5	5.25
2	5/5	7.38
3	5/5	5.57
4	5/5	6.20
5	4/5	5.84
平均	96.0%(24/25)	6.05

Sketcha(1問あたり)

被験者	正答率	回答時間[s]
1	30/30	0.87
2	30/30	1.23
3	30/30	0.93
4	30/30	1.03
5	29/30	0.97
平均	99.3%(149/150)	1.01

Sketcha-maze

被験者	正答率	回答時間[s]
1	5/5	6.06
2	4/5	8.69
3	4/5	7.76
4	4/5	9.00
5	5/5	7.69
平均	88.0%(22/25)	7.84

各格子点上のオブジェクトの回転方向が異なる以外は，Directcha-maze の実験システムと同じである．回転方向は Sketcha の実験システムと同じである．

5.4　諸元

被験者は静岡大学に所属する学生 5 名である．各被験者に，Directcha，Sketch a，Directcha-maze，Sketcha-maze の 4 方式それぞれの問題を 5 問ずつ解いてもらった．順序効果に配慮し，4 方式をどの順番で行うかは，被験者ごとにランダムに決定した．実験システムに慣れるため，各被験者は，5 セットの実験本番の前に，自身が十分と思えるまで何度でも練習を行うことを許した．ただし，被験者全員に最低 5 セットは練習で解いてもらった．練習および本番で利用する問題は毎回自動生成を行っており，毎回異なる画像（あるいは，画像群）が出題される．

5.5　実験結果

5.5.1　正答率と回答時間

被験者ごとに Directcha-maze と Sketcha-maze の正答率と平均回答時間をまとめた結果を表 1 に示す．表中の「回答時間」は本番における 1 セットあたりの回答時間の平均である．以下にその詳細を示す．ユーザが間違えた問題の原因は，ユーザへのヒアリングを参考に分析した．

Directcha-maze の正答率は，平均 96.0%（被験者 5 名×5 セット＝25 セットの回答中，成功が 24 セット，失敗が 1 セット）である．被験者 5 が間違えた問題 1 セットの原因は，オブジェクトの対面方向の誤認識であった．平均回答時間は，6.34 秒である．

Sketcha-maze の正答率は，平均 88.0%（25 セットの回答中，成功が 22 セット，失敗が 3 セット）である．被験者 2,3,4 が間違えた問題それぞれの原因は，すべてオブジェクトの垂直方向を誤認識し，誤った方向へ進んだことだった．

平均回答時間は，7.84 秒である．

Directcha の正答率は，平均 96.0%（25 セットの回答中，成功が 24 セット，失敗が 1 セット）である．被験者 4 が間違えた問題 1 セットの原因は，単にパネルの押し間違いであった．平均回答時間は，6.25 秒である．

Sketcha の正答率は，平均 96.0%（25 セットの回答中，成功が 24 セット，失敗が 1 セット）である．被験者 5 が間違えた問題 1 セットの原因は，オブジェクトの垂直方向の誤認識であった．平均回答時間は，6.05 秒である．

5.6 議論

5.6.1 Directcha タスク繰り返しと Directcha-maze の比較

文献[8]では，総当たり数を 4096 で統一したとき，Directcha（6 問 1 セット）の正答率は 96.0%，平均回答時間は 5.49 秒であった．Directcha-maze（1 問，ゴール 1 つ）の正答率は 96.0%, 平均回答時間 6.76 秒であった. すなわち，Directcha-maze のほうが 1 秒以上遅い結果になっていた．

今回は，表 1 に示したとおり，Directcha（6 問 1 セット）の正答率は 96.0%，平均回答時間は 6.25 秒であった[d]. Directcha-maze（1 問，ゴール 4 つ）の正答率は 96.0%，平均回答時間 6.34 秒であった. その範囲は 0.1 秒程度である．Directcha-maze の回答時間が，Directcha（6 問 1 セット）の回答時間と同程度の時間になったことから，ゴールを複数にすることは Directcha-maze の回答時間を短縮することに寄与していることがわかる．

5.6.2 Sketcha タスク繰り返しと Sketcha-maze の比較

文献[8]では，Sketcha 繰り返しに関する評価を行っていないため，今回の実験結果に限って議論を行う．

表 1 に示したとおり，Sketcha（6 問 1 セット）の正答率は 96.0%，平均回答時間は 6.05 秒であった．Sketcha-maze（1 問，ゴール 4 つ）の正答率は 96.0%，平均回答時間 7.84 秒であった．残念ながら，Sketcha と Sketcha-maze の間には，1 秒近くの差があった．

その理由について，実験終了後に Sketcha-maze に関する印象を被験者に尋ねることで分析を行った．その結果,「オブジェクトの上方向へ進んでいくということに違和感がある」という非常に興味深いが得られた. 一方で， Sketcha 単体に同様の意見（上方向をクリックするのは違和感がある）という意見は得られなかった.「上方向をなぞるのは違和感がある」が「上方向をクリックするのは違和感がない」というこの差が回答時間の差として現れているものと思われる. 本論文は, Directcha-maze の提案を行うものであるものの, この点についてはさらに深い検討を進める必要がある．

6. まとめ

文献[8]で提案した迷路形式の CAPTCHA 出題方式「Directcha-maze」を改良した．本稿では，人間と機械の正答率の差を用いた機械解読耐性の向上を報告した. さらに，ゴールを複数設置したことにより，回答時間の減少を達成した．これは，Directcha-maze が Directcha よりも回答時間が 1 秒以上遅かったという文献[8]の課題を解決したものである．今後は，大規模な実験を行って，提案方式の有効性を測るほか，攻撃耐性に関わるさらなる分析を行っていきたい．

謝辞 本論文を執筆するうえで，静岡大学 竹内勇剛教授に認知科学の観点からご助言を頂きました. 静岡大学 大木哲史講師に機械解読に関わるご助言を頂きました．本論文で使用した 3 次元オブジェクトは，メタセコ素材!（http://sakura.hippy.jp/meta/），TurboSquid（http://www.turbosquid.com/）3D MODELLE (http://ja.kostenlose3dmodelle.com/), 3D Warehouse(https://3dwarehouse.sketchup.com/?hl=ja)などで公開されている素材です．この場を借りて御礼申し上げます．

参考文献

[1] “The Official CAPTCHA Site”. http://www.captcha.net/ , (参照 2017-08-17).

[2] Elson, J., Douceur, J., Howela, J., et al.: Asirra: a CAPTCHA that exploit interest-aligned manual image categorization, Proc. ACM Conference on Computer and Communications Security (ACM CSS 2007), p.366-374.

[3] Yan, J. and El Ahmad, A.S.: Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms, Proc. Computer Security Applications Conference (ACSAC 2007), p.279-291.

[4] Ross, S.A., Halderman, J.A. and Finklelstein, A.: Sketcha: a captcha based on line drawings of 3D models, Proc. 19th Int. Conf. on World Wide Web, p. 821-830.

[5] Shepard, R.N. and Cooper, L.A.: Mental images and their transformations, The MIT Press, 1986

[6] Shepard, R.N. and Metzler, J.: Mental rotation of three dimensional objects, Science, New Series, 1971, Vol.171, No.3972, p.701-703.

[7] Sano, A., Fujita, M., Nishigaki, M.: Directcha: A Proposal of Spatiometric Mental Rotation CAPTCHA, Proc. 14th Int. Conf. on Privacy, Security and Trust, p.585-592

[8] 佐野絢音，藤田真浩，西垣正勝: 総当たり数の確保とユーザのメンタル負荷軽減を実現する CAPTCHA 出題形式の検討，2017 年暗号と情報セキュリティシンポジウム (SCIS2017) ，3B4-2，2017.

[9] Sano, A., Fujita, M., Nishigaki, M.: Directcha-maze: A Study of CAPTCHA Configuration with Machine Learning and Brute-Force Attack Defensibility along with User Convenience Consideration, 2017 The 12th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2017), (to be appeared)

[10] Takano, Y. and Okubo, M.: Encyclopedia of Cognitive Science, Mental Rotation, John Wiley & Sons, Tokyo,2006.

d 文献[8]は練習・本番で同じモデルを利用しており，今回は異なるモデルを利用している．Directcha の回答時間が遅くなっている理由はこれが原因であると考えられる．なお，実験ログを確認，ユーザへのインタビューを実施したところ，Directcha のみ操作ミス（パネルの押し間違い）が見られた．