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

A Proposal of Spatiometric Mental Rotation CAPTCHA

メタデータ	言語: jpn
	出版者:
	公開日: 2022-04-08
	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/10297/00028851

Copyright© 2016 The Institute of Electronics, Information and Communication Engineers

SCIS 2016 2016 Symposium on Cryptography and Information Security
Kumamoto, Japan, Jan. 19- 22, 2016
The Institute of Electronics, Information and Communication Engineers

Spatiometric 型メンタルローテーション CAPTCHA の提案
A Proposal of Spatiometric Mental Rotation CAPTCHA

佐野 絢音* Ayane Sano　藤田 真浩† Masahiro Fujita　西垣 正勝† Masakatsu Nishigaki

あらまし 人間の高度な認知能力を利用した CAPTCHA の一つとして，3 次元のメンタルローテーションを利用した画像 CAPTCHA が提案されている．しかし，Cognometric 型メンタルローテーションタスクを利用している既存のメンタルローテーション CAPTCHA は，「候補画像群から問題画像と最も近い特徴を有する画像を選択する」攻撃によって突破され得る．そこで，この攻撃に耐性を有するメンタルローテーション CAPTCHA「Directcha」を提案する．提案方式は，Spatiometric 型メンタルローテーションタスクをユーザへ求める．具体的には，問題画像中に写る 3 次元オブジェクトの向きを正しく回答できたユーザを，正規ユーザ（人間）として判定する形式である．本方式であれば，問題画像は 1 枚の画像（オブジェクト）であるため，「候補画像群から問題画像と近い特徴を有する画像を選択する」攻撃が適用不可能である．さらに，提案方式のプロトタイプシステムを実装し，ユーザビリティに関する基礎実験を行った．その結果より，提案方式が既存のメンタルローテーション CAPTCHA と同程度の利便性を確保していることを確認した．

キーワード CAPTCHA，メンタルローテーション，空間認識，3 次元コンピュータグラフィックス

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 は人間には容易に正解でき，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）や動物画像の判別を用いた Asirra（図 2）[2]が採用されている．しかし，これらの 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ることが可能であると指摘されている[3][4]．この問題に対し研究者たちは「人間の高度な認知能力」を用いることで CAPTCHA の攻撃耐性を向上しようと試みてきた[5]．その取り組みの中で，人間が有する「メンタルローテーション」の能力を利用した YUNiTi CAPTCHA[6]（図 3）が提案された．メンタルローテーションは，一つの視点から写された 2 次元物体や 3 次元物体を頭の中で回転させ，異なる視点から写された形姿を認識する能力であり，人間が有する空間認識能力の一つである．3 次元の空間認識はコンピュータが苦手とする分野の一つであり，YUNiTi CAPTCHA はマルウェアが正解困難である理想的な CAPTCHA の一つとして注目を集めた[7]．

図 1　文字判読型 CAPTCHA

YUNiTi CAPTCHA は，問題画像に写されている 3 次元オブジェクトと同一の 3 次元オブジェクトを候補画像群の中から正しく選択できたユーザを正規ユーザ（人間）として判別する．問題画像と候補画像ではオブジェクトの

* 静岡大学情報学部，〒432-8011，静岡県浜松市中区城北 3-5-1，Faculty of Informatics, Shizuoka University, 3-5-1, Johoku, Naka, Hamamatsu, Shizuoka, 432-8011, Japan.
† 静岡大学創造科学技術大学院，〒432-8011，静岡県浜松市中区城北 3-5-1, Graduate School of Science and Technology, Shizuoka University, 3-5-1, Johoku, Naka, Hamamatsu, Shizuoka, 432-8011, Japan. nisigaki@inf.shizuoka.ac.jp

図 2　Asirra の認証画面例

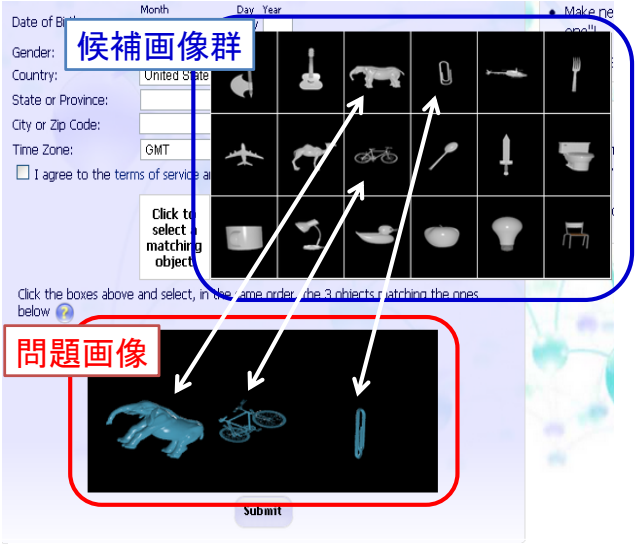

図 3　YUNiTi CAPTCHA の認証画面例

向きが 3 次元的に異なっており，Cognometric 型（囮オブジェクトの中に含まれる正解オブジェクトを選択する方式）の出題形式となっている．しかし，YUNiTi CAPTCHA のような Cognometric 型の CAPTCHA の場合，「候補画像群の中から問題画像と最も近い特徴を有する画像を選択する」という戦略を採るマルウェアに突破される懸念が存在する．近年では，SIFT や SURF といった画像中から特徴点を抽出する技術も発達してきており[8]，「候補画像群から問題画像と最も近い画像を選択する」攻撃に対する耐性をメンタルローテーション CAPTCHA へ付加することが急務である．

そこで本稿では，この攻撃に耐性を有するメンタルローテーション CAPTCHA として「Directcha」を提案する．Directcha は，「Spatiometric 型」のメンタルローテーションタスクをユーザに求める．Spatiometric 型のメンタルローテーションタスクは，問題画像中に写る 3 次元オブジェクトの向いている方向を回答するタスクである．オブジェクトの向いている方向を正しく回答できたユーザを正規ユーザ（人間）として判定する．人間のメンタルローテーションタスクには，「オブジェクトの回転角度が大きいほどタスクに要する時間も長くなる一方で，オブジェクトが左向きか右向きかについては即座に識別している」という興味深い特徴が存在する．Spatiometric 型のメンタルローテーションタスクを用いる Directcha では，人間が有するこの特徴を活用することにより，YUNiTi CAPTCHA より攻撃耐性を高めているにも関わらず，YUNiTi CAPTCHA と同等の利便性を有することに成功している．

本稿の構成は次のとおりである．2 章では，既存のメンタルローテーション CAPTCHA（YUNiTi CAPTCHA）とその課題について述べる．3 章にて提案方式について説明した後，4 章で提案方式に対するユーザビリティに関する基礎実験の結果を報告する．その後，5 章で提案方式の攻撃耐性に関する考察を行い，6 章で自動生成に関する考察を行う．最後に，7 章でまとめと今後の課題を述べる．

2　YUNiTi CAPTCHA

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認識することが可能である．この能力は「メンタルローテーション」と呼ばれ，人間の高度な認知能力の一種として知られている[9][10]．

3 次元オブジェクトのメンタルローテーションを利用した CAPTCHA として YUNiTi CAPTCHA が提案されている[6]．YUNiTi CAPTCHA の認証画面例を図 3 に示す．YUNiTi CAPTCHA では，「候補画像群の中から問題画像と同じ 3 次元オブジェクトが写された画像を選ぶ」という Cognometric 型のメンタルローテーションタスクが採用されている．人間であれば，メンタルローテーションの能力を活用することで，問題画像に写っている 3 次元オブジェクトを頭の中で回転させ，候補画像それぞれと比較することで，候補画像の中から一致するオブジェクトが写る画像を選択することが容易に可能である．3 問の問題画像が一度に提示され，それぞれのオブジェクトが何であるかを 18 個の候補画像の中から正しく選択できたユーザを人間と判定する．問題画像は毎回異なる視点から 3 次元オブジェクトを写した画像となっている．候補画像群の撮影方向は不変であり，常に同一の候補画像群が表示される．

しかし，YUNiTi CAPTCHA のような Cognometric 型のメンタルローテーション CAPTCHA の場合は，姿形の異なる複数のオブジェクトの中に問題画像と同一のオブジェクトが 1 体だけ混入する形態となっているため，「候補画像群の中から問題画像と最も近い特徴を有する画像を選択する」という戦略によって，マルウェアにも正解画像を求められてしまう懸念がある．

3　Directcha

3.1　コンセプト

本稿では，「3 次元オブジェクトの向いている方向を回答する」というメンタルローテーションタスク（以下，「Spatiometric 型メンタルローテーションタスク」と呼ぶ）を利用した新たなメンタルローテーション CAPTCHA「Directcha」を提案する．Directcha の認証画面例を図 4 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．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．人間であれば，メンタルローテーションの能力を活用し，画像中のオブジェクトが正面方向を基準にどちらにどのように回転しているかを認識することが可能である [11]．なお，画像生成に使用する 3 次元オブジェクトの種類とその向きは生成の都度変更される．

Spatiometric 型メンタルローテーションタスクを採用することによって，認証画面は 1 枚の画像（オブジェクト）のみとなるため，YUNiTi CAPTCHA の課題であった「候補画像群から問題画像と最も近い特徴を有する画像を選択する」攻撃の対象になり得ない．さらに，人間のメンタルローテーションタスクには，「オブジェクトの回転角度が大きいほどタスクに要する時間も長くなる一方で，オブジェクトが左向きか右向きかについては即座に識別している」という興味深い特徴が存在することが知られている [10]．すなわち人間は，「右向きか左向きか」，「前向きか後向きか」という程度の雑駁な方向識別については直感的な判定が可能である．Spatiometric 型メンタルローテーションタスクにおいては，この人間の特徴を利用することが可能であり，Derectcha では，回転方向の分割度を 4 レベルに限定することによって認証にかかる時間を小さく押さえることに成功している．

3.2　手順

Directcha の認証手順を以下に示す．なお，システムのデータベースには向き（正立と倒立，正面と背面）を有する 3 次元モデルが，どちらが正立であるか，どちらが正面であるかという情報とともに，大量に登録されていることを前提とする．

(1)　システムは，問題に利用する 3 次元モデルをデータベースからランダムに選ぶ．
(2)　システムは，(1)で選んだ 3 次元オブジェクトを x,y,z 軸に対してそれぞれ任意の角度に回転させる．
(3)　システムは，回答用パネルの上に(2)のオブジェクトを配置する．
(4)　システムは，(3)を 2 次元画像へ投影することによって，問題画像を生成する．
(5)　システムは，ユーザへ問題画像を表示する．
(6)　ユーザは，問題画像の 3 次元オブジェクトが向いている方向を認識し，向きに対応する回答パネルをクリックする．
(7)　システムは，正解できたユーザを人間，正解できなかったユーザをマルウェアとして判別する．

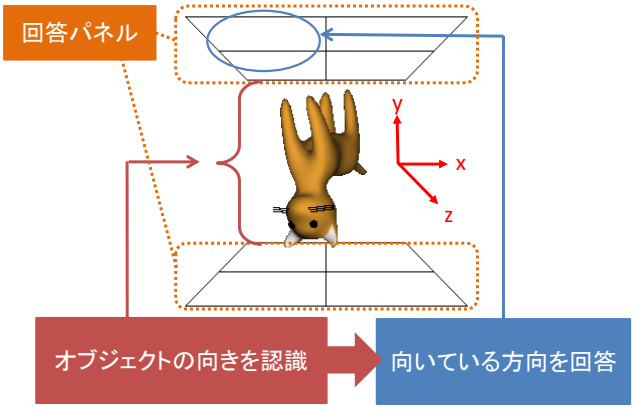

図 4　提案 CAPTCHA の認証画面例

マルウェアは，問題画像の情報（2 次元情報）だけを用いて，問題画像に写っているオブジェクトの向き（回転角度）を認識しなければならない．これに対し，システムは自動生成の過程（手順(2)）でオブジェクトの回転角度を知っている．これが「落とし戸」となり，システム（機械）が「マルウェア（機械）には認識できない問題」を自動生成し，かつ，「システム（機械）自身がユーザの回答に対する正解判定を行う」ことが可能となっている．

3.3　実装

提案方式の基礎実験を行うため，実験システムの実装を行った．実験システムの認証画面例を図 5 と図 6 に示す．図 5,6 に示すとおり，総当たり数 4（正立したオブジェクトが向いている方向を 4 方向（y 軸に対する第 1 象限～第 4 象限）から選択する），総当たり数 8（オブジェクトが正立か倒立であるかを含めて，オブジェクトが向いている方向を 8 方向から選択する）の Directcha を実装した．ユーザはオブジェクトの向いている方向を，画像に表示されているパネルをクリックして回答する．クリックしたパネルがオブジェクトの向きと一致している場合に認証成功となる．図 5 の例では，問題画像に写る猫のオブジェクトは，正立した状態で右前を向いている．したがって，下側の右前のパネルをクリックすれば正解となる．図 6 の例では，問題画像に写る猫のオブジェクトは，倒立した状態で右奥を向いている．したがって，上側の右奥のパネルをクリックすれば正解となる．

提案方式においては，画像の生成にあたって，問題のサイズ，モデルの回転角度について制約が存在する．これらの制約に関するパラメータは，システム実装にあたって予備実験を行い，経験的に適切な値を定めた．以下に，それぞれの詳細について述べる．

3.3.1.　画像サイズ

問題画像のサイズは，縦 300 画素×横 300 画素とした．

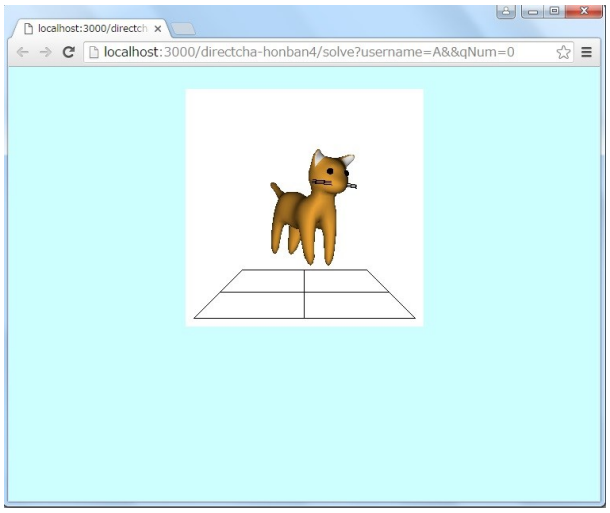

図 5　総当たり数 4 の Directcha 認証画面例

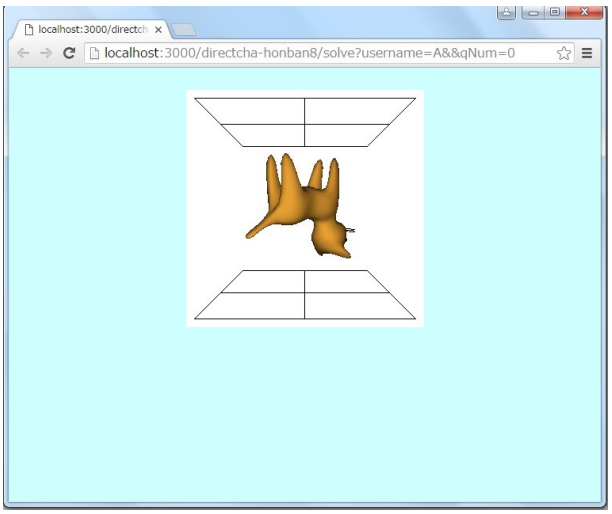

図 6　総当たり数 8 の Directcha 認証画面例

画像の左上が第(0,0)画素，右下が(299,299)画素である．

3.3.2.　回転角度

提案方式は，3.2 節手順⑵でオブジェクトを x,y,z 軸に対して任意の角度で回転している．ただし，今回の実装では次に示す制約を設けた．

y 軸において隣り合う象限同士の境界に近い角度がオブジェクトの回転角度として選択された場合，ユーザは画像に写るオブジェクトがどの方向（象限）を向いているか判定することが困難である．たとえば，正面（y 軸方向の回転角度が 0 度）を向いているオブジェクトは，右前を向いているか左前を向いているかを判断することは不可能である．したがって，y 軸の回転角度は，反時計回りに 25 度～65 度，115 度～155 度，205 度～245 度，295～335 度の範囲から選ばれるようにした．

さらに，予備実験を通じて，x 軸および z 軸の回転角度が大きい場合には，ユーザの回答時間が大幅に遅延することが確認された [1]．したがって，x 軸の回転角度は，反時計回りに-10 度～10 度の範囲から選ばれるようにした．z 軸の回転角度は，総当たり数 4 のときは，反時計回りに-5 度～5 度の範囲から，総当たり数 8 のときは，反時計回りに-5 度～5 度，175 度～185 度の範囲から選ばれるようにした．

4　ユーザビリティに関する基礎実験

4.1　目的

提案方式と YUNiTi CAPTCHA（正確には，YUNiTi CAPTCHA を模したシステム．以下，単に YUNiTi CAPTCHA と呼ぶ）を用いてユーザビリティに関する基礎実験を行う．提案方式と YUNiTi CAPTCHA を正答率，回答時間の観点から比較することで，提案方式のユーザビリティを評価する．

[1]　この理由の詳細な検討は今後の課題であるが，現実世界において x 軸および z 軸方向に対して回転をしたオブジェクトを目にすることが少ないことが理由の一つとして考えらえる．

4.2　諸元

被験者は情報系の大学生 12 名であり，全被験者を無作為に 4 つの被験者群に分けた．具体的には，総当たり数 4 の Directcha を 8 問解く 3 名（被験者群 A），総当たり数 8 の Directcha を 16 問解く 3 名（被験者群 B），総当たり数 4 の YUNiTi CAPTCHA を 8 問解く 3 名（被験者群 C），総当たり数 8 の YUNiTi CAPTCHA を 16 問解く 3 名（被験者群 D），である．実験システムの操作に慣れるために，いずれの被験者群においても，本番の回答に取り掛かる前に被験者が満足するまで練習を行うことを許した．

4.2.1.　提案方式の実験システム

提案方式の実験システムは 3.3 節で実装したシステムである．実験で使用する 3 次元モデルは，Web 上から収集したフリー素材であり，上下前後関係が明瞭なモデル 16 種類（モデル A～P）である．A～H が練習用のモデル群であり，I～P が本番用のモデル群である．今回の実験では，提案方式と YUNiTi CAPTCHA で同じモデル群（A～P）を使用する．次節に示すとおり，YUNiTi CAPTCHA の制約から，A～H のモデル群には同じカテゴリに属するモデルは含まれていない．I～P も同様である．

被験者群 A の練習では，モデル A～D をランダムに使って問題を生成する（被験者は，練習を繰り返すうちに，同じモデルに関する問題を複数回目にすることがありえる）．被験者群 A の本番では，モデル I～L をランダムな順序で 2 回ずつ使って問題 8 問を生成する（被験者は，4 種類のモデルに関する問題をそれぞれ 2 回ずつ目にする）．被験者群 B の練習では，モデル A～H をランダムに使って問題を生成する．被験者群 B の本番では，モデル I～P をランダムな順序で 2 回ずつ使って問題 16 問を生成する．

4.2.2.　YUNiTi CAPTCHA の実験システム

YUNiTi CAPTCHA の認証画面例を図 7，図 8 に示す．オリジナルの YUNiTi CAPTCHA は 18 枚の候補画像の中から正解画像を回答させるタスクを 3 問同時に提示する形態であるが，今回の実験では，提案方式の実験システ

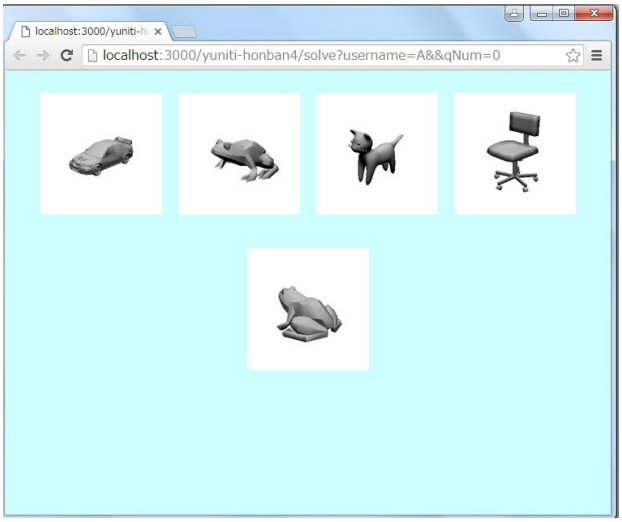

図 7 総当たり数 4 の YUNiTi CAPTCHA
認証画面例

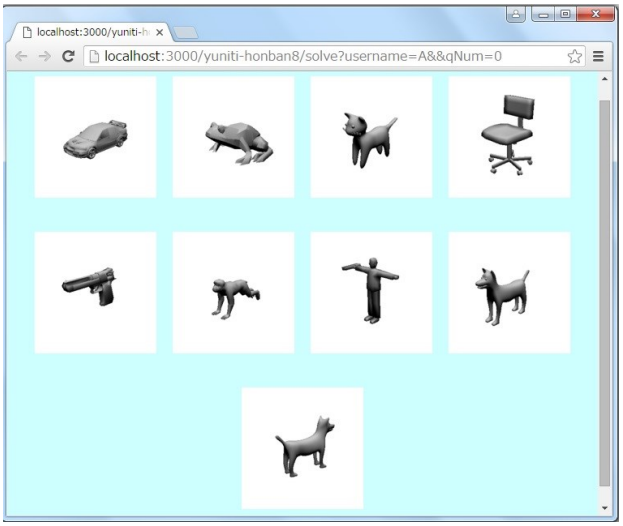

図 8 総当たり数 8 の YUNiTi CAPTCHA
認証画面例

ムと条件を同一にするために，被験者群 C に対しては「4 枚の候補画像群の中から 1 枚の正解画像を回答するタスク」（図 7），被験者群 D に対しては「8 枚の候補画像群の中から 1 枚の正解画像を回答するタスク」（図 8）をそれぞれ構成している．

問題画像および各候補画像の画像サイズは，縦 150 画素×横 150 画素である．オリジナルの YUNiTi CAPTCHA の仕様と可能な限り一致させるために[2]，各画像に写るオブジェクトは(R,G,B)＝(204,204,204)で単色化してある．また，候補画像に写るオブジェクトは，正面を基準として x, y, z 軸に対してそれぞれ 20 度，315 度，0 度回転したオブジェクトである．問題画像に写るオブジェクトは，x 軸に対して 20 度回転した後，y 軸に対して 0～359 度の範囲でランダムに回転したオブジェクトである．z 軸に対しては回転していない．

使用する 3 次元モデルは提案方式の実験システムと同じ 16 種類のモデル（A～P）である．Cognometric 型の YUNiTi CAPTCHA の場合，候補画像の中に類似したオブジェクトが含まれると，正規ユーザ（人間）の正答率が低下する．このため，今回の実験においては，A～H のモデル群には同じカテゴリに属するモデルを含めていない．I～P も同様である．

被験者群 C の練習ではモデル A～D を候補画像群として用い，その中から正解となるモデルをランダムに選んで問題を生成する．被験者群 C の本番では，モデル I～L を候補画像群として用い，モデル I～L をランダムな順序で 2 回ずつ問題画像として使って問題 8 問を生成する．被験者群 D の練習ではモデル A～H を候補画像群として用い，その中から正解となるモデルをランダムに選んで問題を生成する．被験者群 D の本番では，モデル I～P を候補画像群として用い，モデル I～P をランダムな順序で 2 回ずつ問題画像として使って問題 16 問を生成する．

[2] YUNiTi CAPTCHA の仕様の詳細は公開されていない．したがって，筆者らがオリジナルの YUNiTi CAPTCHA の問題画像と候補画像を複数確認した上で，できるだけオリジナルと近い条件となるよう条件を定めた．

4.3 実験結果

被験者ごとに正答率と平均所要時間をまとめた結果を表 1 に示す．表中の「平均所要時間」は本番における 1 問あたりの回答の所要時間の平均である．この結果をもとに提案方式のユーザビリティに関して分析を行う．

4.3.1. 正答率

表 1 より，総当たり数 4 の Directcha の正答率は，平均 92%（被験者 3 名×8 題＝24 題の回答を行ったうち，成功が 22 題，失敗が 2 題）である．総当たり数 8 の場合，平均 98%（被験者 3 名×16 題＝48 題の回答を行ったうち，成功が 47 題，失敗が 1 題）である．どちらの場合も 9 割以上の高い正答率を有している．しかし，YUNiTi CAPTCHA の正答率は総当たり数が 4 の場合も 8 の場合も 100%である．したがって，現時点では，提案方式は YUNiTi CAPTCHA と比較すると若干低い正答率となっている．

被験者が間違えた問題に関して，実験終了後に被験者への聞き取り調査の結果（間違えた理由を尋ねた）を参考にして分析を行った．分析の結果を以下に示す．

総当たり数 4 でユーザが間違えた問題の原因は，2 題ともユーザの誤クリックによるものであった．正解を認識した後，回答を行うクリック位置にマウスを移動する途中で，誤ってマウスをクリックしてしまったため，不正解と判定されていた（パネルの外部をクリックしていた）．これに関しては，パネルの外部のクリックは無効にすることによって対策が可能である．

総当たり数 8 でユーザが間違えた原因は，画像に写るオブジェクトが何であるかを認識できなかった（よって，オブジェクトの向きを認識できなかった）ことであった．すなわち，特定のオブジェクトが特定の角度で表示された際

表 1　実験結果

総当たり数4のDirectcha

被験者	正答率	平均所要時間[s]
1	6/8	1.05
2	8/8	1.80
3	8/8	1.69
平均	91.7% (22/24)	1.52

総当たり数4のYUNiTi CAPTCHA

被験者	正答率	平均所要時間[s]
4	8/8	1.57
5	8/8	1.53
6	8/8	1.22
平均	100.0% (24/24)	1.44

総当たり数8のDirectcha

被験者	正答率	平均所要時間[s]
7	16/16	2.09
8	15/16	1.83
9	16/16	1.50
平均	97.9% (47/48)	1.80

総当たり数8のYUNiTi CAPTCHA

被験者	正答率	平均所要時間[s]
10	16/16	1.44
11	16/16	1.85
12	16/16	1.65
平均	100.0% (48/48)	1.64

には，そのオブジェクトの向き（正解）を認識しにくい場合があることが判明した．ユーザが認識誤りを起こしやすいオブジェクトや回転角度の条件について，実験を繰り返すことで調査し，対策を講じていく必要がある．また，今回使用した 3 次元モデルはフリー素材であるため，シンプルに作られたモデルが多かった．3 次元モデルの中には細部まで緻密まで作りこまれたモデルも多く存在するため，そのようなモデルを利用することでユーザの認識を助けることが可能であると考えられる．

4.3.2.　回答時間

表 1 より，総当たり数 4 の Directcha の平均所要時間は 1.52 秒であり，総当たり数 4 の YUNiTi CAPTCHA の平均所要時間は 1.44 秒である．同様に，総当たり数 8 の Directcha の平均所要時間は 1.80 秒であり，総当たり数 8 の YUNiTi CAPTCHA の平均所要時間は 1.64 秒である．以上の結果より，提案方式は YUNiTi CAPTCHA と同程度の回答時間を有しており，十分に短い時間で回答可能な CAPTCHA であるといえるだろう．

5　攻撃耐性に関する考察

5.1　近い特徴を有する候補画像を選択する攻撃

YUNiTi CAPTCHA のような Cognometric 形式の CAPTCHA の場合，「候補画像群から問題画像と最も近い特徴を有する画像を選択する」という戦略を採るマルウェアに突破される懸念が存在した．これに対して，提案方式で用いる Spatiometric 型メンタルローテーションは，認証画面に 1 枚の画像（1 体オブジェクト）しか表示されない．したがって，「近い特徴を有する画像を選択する」という戦略をもって提案方式を解読することは原理的に不可能である．

5.2　総当たり攻撃

文献[17]では，画像 CAPTCHA の総当たり数として 4096 通りを確保できれば，Token Buckets Scheme を用いて誤答が多い Web クライアント（IP アドレス）からのアクセスを遮断することで，実質的な総当たり数を 560 万通り程度まで高めることが可能であることが示されている．そこで，4096 通りを画像 CAPTCHA が有するべき総当たり数であると想定して議論を進める．

表 2　総当たり数 4096 を確保したときの正答率と回答時間の期待値

	正答率	平均所要時間[s]
総当たり数4	59.3%	9.1
総当たり数8	91.9%	7.2

4096 通りを確保するためには，総当たり数 4 の Directcha の場合，ユーザに 6 問の問題を正解することを求める必要がある．総当たり数 8 の場合では，4 問の問題を正解することをユーザに求める必要がある．4 章のユーザビリティ実験によって得た実験結果から，提案方式が総当たり数 4096 通りを満たすよう出題した場合の正答率と回答時間の期待値を求めた（表 2）．総当たり数 4 と 8 の Directcha の正答率の期待値はそれぞれ約 60%，約 92% である．総当たり数 4 の正答率が低い値となっているが，これは，4.3.1 節に示したとおり，被験者の誤クリックが原因であった．4.3.1 節に示した改良によって総当たり数 8 の正答率と同程度までは高めることが可能であろう．総当たり数 4 と 8 の Directcha の回答時間の期待値は，それぞれ約 9.1 秒，約 7.2 秒である．一般的に用いられている文字判読型 CAPTCHA（5～7 文字）の正答率は約 93%，平均回答時間は約 12.6 秒であるため[12]，正答率，回答時間ともに文字判読型 CAPTCHA と同程度以上の値を確保していることがわかる．

以上の議論より，複数の問題に対して正解することをユーザへ求めたとしても，提案方式の正答率，回答時間の低下は十分に許容できる範囲に収まる．したがって，提案方式は，総当たり攻撃に対して耐性を有する方式であるといえる．

5.3 データベース攻撃

画像 CAPTCHA に対しては，過去の問題画像とその解答のペアを大量に収集し，出題された問題画像と収集した問題画像を比較参照することによって CAPTCHA を突破する攻撃が知られている．この攻撃はデータベース攻撃と呼ばれる[14]．実際，オリジナルの YUNiTi CAPTCHA では，過去の問題画像と解答のペアを大量に集めることでマルウェアに突破可能であるという報告がなされている[13]．データベース攻撃に対抗するためには，CAPTCHA システムのデータベースに 3 次元モデルを大量に登録しておき，新しい問題を作り続けることが肝要である[14]．

3 次元モデルを利用したサービスは近年急激に増加しており，将来的には無数の 3 次元モデルが世の中に出回ることが予想される．提案方式は，これらの 3 次元モデルをシステムのデータベースに取り込み，新しい問題を作り続けることによって，データベース攻撃に対する耐性を高めることが可能な方式である．

5.4 機械学習

提案方式は，問題画像に写っているオブジェクトの向きを回答する CAPTCHA である．マルウェアは提案方式を突破するために，画像に写っているオブジェクトの角度を認識する分類機を構築しようと試みるだろう．具体的には，下記の手順が考えられる．

(1) 攻撃者は大量の問題画像（あるオブジェクトが任意の視点から写された画像）を用意する．
(2) 各問題画像から特徴量を抽出する．オブジェクトの「向き」を表す特徴量としては，画像中に含まれる直線群の向きなどが有力な候補となり得るであろう（たとえば，ガボールフィルタ[15]を利用する）．
(3) 各画像に対する「手順(2)で抽出した特徴量」と「オブジェクトの回転角度」を教師データとして機械学習を行い，「オブジェクトが写された画像を入力すると，画像に写っているオブジェクトの回転角度を出力する」分類機を構築する．
(4) マルウェアは手順(3)で構築した分類機を利用して提案方式の突破を試みる．すなわち，問題画像に写るオブジェクトの向きを認識する分類機を用いることで問題画像に写るオブジェクトの向きを求める．

上記の機械学習が提案方式に対してどの程度有効であるかは，今後定量的に評価しなければならない．しかし，3 次元モデルの種類が増加するほど，モデルの特徴量は多様化する．したがって，機械学習を行ったとしても，任意のオブジェクトの回転角度を精度よく評価することができる分類器を得ることは困難であると推測される[3]．

5.5 その他の攻撃

提案方式に対する攻撃手法のうち，典型的なものについては，前節までに考察した．しかし，マルウェアによる攻撃手法は多種多様であり，提案方式への攻撃耐性が理論的に証明されているわけではない．最先端の画像認識技術を調査したうえで，提案方式の攻撃耐性を引き続き分析する必要がある．

6 自動生成に関する考察

CAPTCHA に求められる要件の一つに問題の自動生成がある[16]．提案方式は 3.2 節に示したとおり，向きを有する 3 次元モデルが，どちらが正立か・正面かという情報とともに，データベースに大量に登録されているという前提のもとで，問題の自動生成を実現している．すなわち現時点では，データベースへ 3 次元モデルを登録する作業については，CAPTCHA システムの管理者が担うことを想定した運用となっている．登録作業が管理者にとってどの程度の負荷になり得るかは今後検討を進める必要があるが，多く 3 次元モデルが正立の状態で正面方向を基準として製作され流通している現状に鑑みれば，管理者の作業は，自動的に収集した 3 次元モデルが「向きを有しているか」を確認するだけであるため，それほど負荷にならないものと推測される．将来的には，条件を満たすモデルをデータベースへ自動的に登録する方法を模索していきたい．

7 まとめと今後の課題

本稿では，Spatiometric 型メンタルローテーションタスクを用いたメンタルローテーション CAPTCHA「Directcha」を提案した．3 次元オブジェクトの向きを認識するというメンタルローテーションタスク（Spatiometric 型メンタルローテーションタスク）を使用することで，Cognometric 型メンタルローテーションタスクを用いた CAPTCHA の課題であった「候補画像群から問題画像と最も近い特徴を有する画像を選択する」攻撃に耐性をもっていることが特長である．プロトタイプシステムを実装し，ユーザビリティに関する基礎実験を行った．その結果，提案方式の 1 問あたりの正答率と平均回答時間は，総当たり数 4 の場合はそれぞれ約 92%，約 1.5 秒であること，総当たり数 8 の場合はそれぞれ約 98%，約 1.8 秒であることを明らかにした．この結果を YUNiTi CAPTCHA の実験結果と比較することで，提案方式が

---

[3] オブジェクトの角度を認識する分類機が構築できた場合，YUNiTi CAPTCHA も次の手順によって突破されることに注意されたい．(1) 構築した分類機を用いて，問題画像の回転角度を認識する．(2) 候補画像の回転角度は固定であるため，ある候補画像から特徴点を抽出し，その特徴点が問題画像の回転角度ではどのように移動するかを求める．(3) (2)で抽出した特徴点が問題画像の特徴点と一致していた場合，その候補画像が正解画像となる．

YUNiTi CAPTCHA と同等の利便性を有することを示した．さらに，提案方式の攻撃耐性と問題の自動生成に関して考察を行い，提案方式が高い攻撃耐性と問題の自動生成を実現していることを示した．

今後は，被験者数を増やしつつ，使用する 3 次元モデル，オブジェクトの回転角度，実験のユーザインタフェースといった条件を変えながら評価実験を繰り返すことで，提案方式のユーザビリティに関して更なる評価を進める予定である．また，提案方式の攻撃耐性について理論的および実験的な評価も進める予定である．

謝辞

静岡大学大学院漁田武雄教授には，メンタルローテーションに関してご教授頂きました．本論文の評価実験で使用した 3 次元オブジェクトは，メタセコ素材！（http://sakura.hippy.jp/meta/）ならびに TurboSquid（http://www.turbosquid.com/）などで公開されている無料素材を利用させて頂きました．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/ >, 2015.12.10 閲覧

[2] ASIRRA – Microsoft Research, <http://research.microsoft.com/en-us/um/redmond/projects/asirra/> , 2015.12.10 閲覧.

[3] J. Yan, A.S. E. Ahmad, “Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms”, Proc. 2007 Computer Security Applications Conf., pp.279-291, 2007.

[4] P. Golle, “Machine Learning Attacks Against the ASIRRA CAPTCHA”, Proc. 2008 ACM Conf. on Computer and Communications Security, pp.535-542, 2008 .

[5] 山本匠，鈴木徳一郎，J.D.Tygar，西垣正勝，“人間の高度な認知処理に基づく CAPTCHA の提案”，映像情報メディア学会技術報告, vol.34, no.54, pp. 41-44，2010.

[6] YUNiTi.com, <http://www.yuniti.com/>, 2014.12.4 閲覧

[7] 3D-based Captchas become reality , CNET , < http://www.cnet.com/news/3d-based-captchas-become-reality/>, 2015.12.10 閲覧.

[8] 藤吉弘亘，安部満 “局所勾配特徴抽出技術―SIFT 以降のアプローチ”，精密工学会誌, vol.77, no.12, pp1109-1116, 2011.

[9] R. Shepard, L. Cooper “Mental Images and Their Transformations”, MIT Press, Cambridge, MA, 1986.

[10] R. Shepard, J.Metzler, “Mental Rotation of Three-Dimensional Objects”, Science, New Series, vol.171, no. 3972, pp. 701-703 , 1971.

[11] J. Hamrick, T. Griffiths, “What to simulate? Inferring the right direction for mental rotation”, Proc. 36th Annu. Meeting of the Cognitive Science Society, 2014.

[12] 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.

[13] How they’ll break the 3D CAPTCHA, <http://technobabblepro.blogspot.jp/2009/04/how-theyll-break-3d-captcha.html>, 2015.12.10 閲覧

[14] S. Ross, J. Halderman, A. Finkelstein “Sketcha: A Captcha Based on Line Drawings of 3D Models” , Proc. 19th Int. Conf. on World wide web, pp821-830, 2010.

[15] Tutorial on Gabor Filters, <http://mplab.ucsd.edu/tutorials/gabor.pdf>, 2015.12.10 閲覧.

[16] M. Fujita, Y. Ikeya, J. Kani, M. Nishigaki, “Chimera CAPTCHA：A Proposal of CAPTCHA using Strangeness in Merged Objects”, Proc. 17th Int. Conf. on Human-Computer Interaction, pp.48-58, 2015.

[17] J. Elson, J. Douceur, J. Howell, J. Saul, “Asirra: a CAPTCHA that exploits interest-aligned manual image categorization”，Proc. 2007 ACM Conf. on Computer and Communications Security, pp.366-374 , 2007