NAIST-IS-MR1551004

課題研究

画像型 CAPTCHA の分析とバイオメトリクス適用の検討

新垣 杏里

2018 年 3 月 15 日

奈良先端科学技術大学院大学
情報科学研究科

本報告書は奈良先端科学技術大学院大学情報科学研究科に
修士 (工学) 授与の要件として提出した課題研究の報告書である。

新垣 杏里

審査委員：

藤川 和利 教授	（主指導教員）
安本 慶一 教授	（副指導教員）
笠原 正治 教授	（副指導教員）
新井 イスマイル 准教授	（副指導教員）
猪俣 敦夫 教授	（東京電機大学）

画像型 CAPTCHA の分析とバイオメトリクス適用の検討*

新垣 杏里

内容梗概

Web サービスに対する自動化プログラムを用いた機械攻撃が頻繁に発生している．そのため，これらの機械攻撃を防ぐ技術として CAPTCHA(Computer Automated Public Turing test to tell Computers and Humans Apart) が利用されている．文字型 CAPTCHA が広く利用されていたが，OCR(Optical Character Recognition) 技術の発展などにより，機械攻撃によって破られるようになった．この理由から，近年では新たな CAPTCHA の研究が盛んに行われている．そこで，本論文では課題研究として，近年の CAPTCHA 研究と画像処理技術を応用した攻撃を考慮した将来の CAPTCHA の研究の方向性の検討を行う．

CAPTCHA の研究事例と画像解析技術の調査の結果から，現状の CAPTCHA は大体が視覚的なもので,「人間らしい」判断や解析を可能とする研究が進んでいることがわかった．そこで，確実に人間と機械を区別する可能性を高める手法として，バイオメトリクスの適用を検討した．その事例案として「インカメラによる顔認識」を挙げた．この例は自動化プログラムによる攻撃を無効化する等の特徴があるが，人面らしき物体を人間と認識する可能性やプライバシ問題といった課題点が残った．この他，CAPTCHA 研究に関する今後の課題として，リレーアタック耐性をもつ CAPTCHA の開発と安全性を保つ基準の再設定を指摘した．

キーワード

CAPTCHA, 機械攻撃, 認知能力, 画像処理, バイオメトリクス

*奈良先端科学技術大学院大学 情報科学研究科 課題研究, NAIST-IS-MR1551004, 2018 年 3 月 15 日.

A Survey of Image-Based CAPTCHA and A Consideration of Applying Biometrics*

Anri Arakaki

Abstract

Machine attacks using automated programs for web services are frequently occurring. Therefore, CAPTCHAs are used to prevent these machine attacks. Text-based CAPTCHAs were widely used, but with the development of OCR technologies, machine attacks become be able to break them. For this reason, researches on new CAPTCHAs have been actively conducted in recent years. In this paper, we study the the future direction of research on CAPTCHA considering recent it and image processing technologies.

Analysis of research on CAPTCHAs and image analysis techniques revealed that most of the current CAPTCHAs are visual and researches which enable "human-like" decision and analysis are on going. Therefore, we considered the application of biometrics to CAPTCHA as a method to increase the possibility of reliably distinguishing between humans and machines. we cited "Face Recognition by In Camera" as a case of it. This example has features such as invalidating machine attacks, but it remains problems such as on privacy. In addition, we pointed out the development of them with relay attack tolerance and reestablishment of standards for maintaining safety as a future works.

Keywords:

CAPTCHA, machine attack, cognitive ability, image processing, biometrics

*Master's Report, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-MR1551004, March 15, 2018.

目 次

図 目 次

表 目 次

1. 序論

1.1 節では、研究背景について述べ、1.2 節では、本課題研究の目的について述べる。

1.1 研究背景

Web サービスに対する自動化プログラムを用いた機械攻撃が頻繁に発生している．例えば，迷惑メール送信のために無料のメールアカウントを不正に取得する攻撃や，ブログへのスパムコメントの書き込みといったものが挙げられる．そのため，これらの機械攻撃を防ぐ技術として CAPTCHA(Computer Automated Public Turing test to tell Computers and Humans Apart) が利用されている．

CAPTCHA とは人と機械を区別するチューリングテストである．一般的に文字型 CAPTCHA が利用されているが，OCR(Optical Character Recognition) 技術の発展などにより，文字型 CAPTCHA では機械攻撃によって破られるようになった．この理由から近年では新型の CAPTCHA の研究が盛んに行われている．

1.2 研究目的

そこで本研究では，近年の画像型 CAPTCHA と画像処理技術を考慮した将来の CAPTCHA 研究の方向性を検討することを目的とする．CAPTCHA の誕生から最新のものへの変遷をまとめ，CAPTCHA の要件とそれを満たすために対策すべき攻撃を述べる．そして，近年の CAPTCHA の研究と画像処理技術から，今後の CAPTCHA はどのように改善するべきか等の方向性を検討する．

2. CAPTCHA の概要

1.1 で述べたように，CAPTCHA とは人と機械とを区別するチューリングテストのことを指す．今ではインターネットの利用が広く普及し，様々な Web サービスが展開されている．それと同時に自動化プログラムによる攻撃が盛んになってきたため，人と機械とを識別するシステムが必要となり CAPTCHA の導入が一般的になっている．

2.1.1 では CAPTCHA が開発されるに至った背景と変遷を述べ，その過程で分類できるようになった CAPTCHA の形態とそれぞれの特徴を 2.2 で紹介する．また、2.3 で CAPTCHA の要件とそれを満たすために対策すべき攻撃等を説明する．

2.1 CAPTCHA の誕生と変遷

2.1.1 CAPTCHA の誕生

CAPTCHA は 2003 年にカーネギーメロン大学の Ahn，Blum，Hopper，Langford[19] によって発明された自動化チューリングテストである．2000 年代前半には，インターネットの利用が一般家庭に広く普及すると同時に，Yahoo! や Microsoft などの企業によるインターネットを活用したサービスが多く展開し始めていた．文献 [19] によると，CAPTCHA の開発に至る当時の背景には次のような事象や問題があったと記述されている．

- オンライン投票事件

  1999 年 10 月，*http://www.slashdot.com* が最も優れる大学院コンピュータサイエンス科を尋ねるオンライン投票をリリースした．一人につき一回の投票となるよう，投票者の IP アドレスは記録されるようになっていたが，カーネギーメロン大学の学生がプログラムを用いて自身が所属する大学へ何千もの投票をする方法を考案した．それと同様に，マサチューセッツ工科大学の学生も自身がコーディングしたプログラムを使用してカーネギーメ

ロン大学に対抗するような投票を行った．その結果，両校の投票数が 21,000 を超える数であったことに対して，他校の投票数は 1,000 を満たさなかった．

- フリーメールサービス

  いくつかの企業によるフリーメールサービスの提供が開始されたが，毎分何千ものメールアカウントを登録する攻撃が発生した．そのため，無料の電子メールアカウントを取得する前にユーザーが人間であることを証明する必要が生じた．

- クローラー

  Web ページのなかには検索エンジンにインデックスされないよう推奨されるものも存在する．そのため，クローラーが該当 Web ページを読み込まないようにする専用の html タグが用意されている．しかし，そのタグはクローラーが Web ページを読み取らないことを保証するものではない問題があった．

この他にも，CAPTCHA は電子メールの添付ファイルや USB メモリ等を介してコンピュータに侵入し自己増殖するプログラムであるワームと，スパムメール，及び，辞書攻撃を防ぐ手段として活用できると考えられいた．

このような背景から開発された CAPTCHA は，様々な組織や個人の Web ページで扱われるようになり，広く普及していった．

2.1.2 CAPTCHA の変遷

初期の CAPTCHA は文字列の字体が波のように歪んだ形状であったが，CAPTCHA の誕生以降は歪ませた文字を二重にするなどの様々なノイズフィルターを掛ける文字型 CAPTCHA が開発された．新たな CAPTCHA が研究される一方で，それを突破する研究も活発に進められた．文字型から始まり，2011 年までには音声型，画像型，パズル型といった様々な形態の CAPTCHA が開発された．

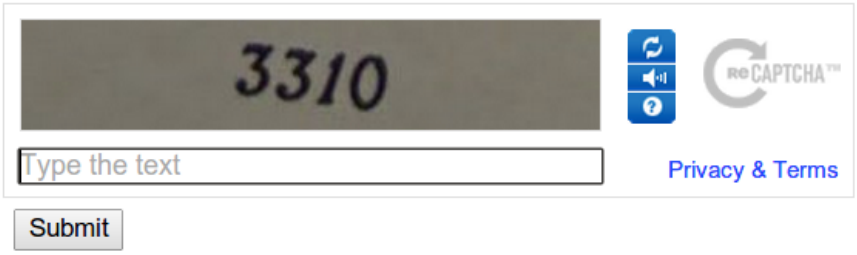

図 1　文字型 CAPTCHA の一例 (参考文献 [1] より引用)

2.2 CAPTCHA の形態

CAPTCHA は大きく分けて 5 つの形態が存在する．文字型，画像型，音声型，動画型そしてパズル型である．それぞれの形態の特徴とその一例を簡潔に紹介する．

2.2.1 文字型 CAPTCHA

文字型 CAPTCHA は最も広く普及している形態である．その一例である図 1 は一見シンプルに見えるが，背景は斑があり文字には各々異なる歪みが生じている．一目で理解しやすいため CAPTCHA チャレンジの正答率が高い．その一方で，OCR 技術の発展などにより機械的に突破可能となった．文字型 CAPTCHA は歪みやノイズなどのフィルターを掛けたランダムな文字列の形式をしている [20]．また，文字を 3D にする [21] など，様々な出題形式のものが存在する．

2.2.2 画像型 CAPTCHA

画像型は近年採用されている新型の CAPTCHA である．文字型と同様に一目で理解しやすいが，機械的に回答することが難しい形態で，インターネット上に画像が大量に存在するため出題数が豊富な特徴をもつ．出題されたものを画像群から選択する形式 [22] や画像に含まれる要素をキー入力して回答する形式 [23] などがある．画像型 CAPTCHA の一例として図示した図 2 は前者のタイプである．

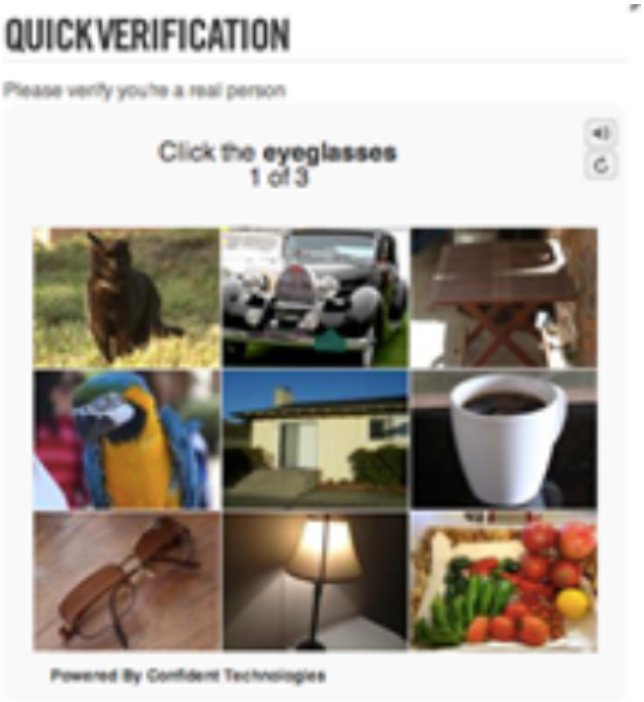

図 2 画像型 CAPTCHA の一例 (参考文献 [2] より引用)

このような出題形式の画像にはノイズや回転などのフィルターが掛けられているものが多い．最近の CAPTCHA の研究では特に盛んな形態である．

2.2.3 音声型 CAPTCHA

音声型は数字や単語などを音声出力で出題する形態である．図 3 にその一例を示す．従来の音声型 CAPTCHA は文字型 CAPTCHA と併用されている．図 3 の赤枠で囲った音声出力マークをクリックすると，図示された出題の文字や数字が一音ずつゆっくりと音読される．このように，音声型 CAPTCHA は視覚ではなく聴覚に作用する形態で，ノイズなどの工夫により解析を困難にしている．その一方で，”B”と”D”などの似た音の正答率が低い問題がある．音声型 CAPTCHA は視力に問題をもつユーザーに向けたものとして扱われている．例のように，出題した音声をキー入力する形式 [24] や，ユーザーに提示した文章を録音して回答する形式 [25] などが存在する．

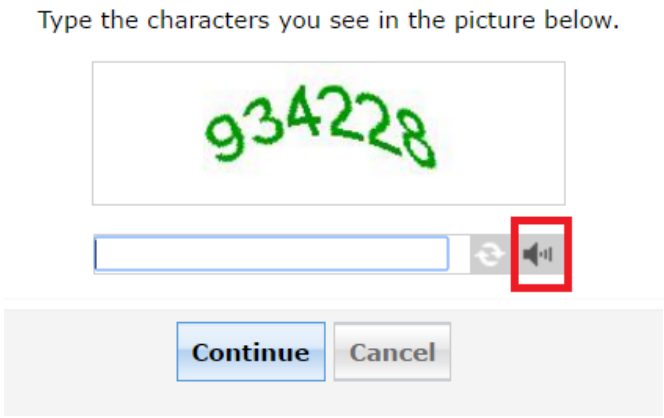

図 3　音声型 CAPTCHA の一例 (参考文献 [3] より引用)

2.2.4　動画型 CAPTCHA

動画型 CAPTCHA は出題が動画再生の形態をしている．その一例を図 4 に示す．この例の場合，動画中に映る赤文字のみを回答欄に入力することで CAPTCHA チャレンジに成功する．背景と特定の文字を数秒間連続して変化させることで OCR による解析を困難にする工夫を凝らしている．動画型 CAPTCHA は他の形態と比較して回答時間が長いが，エンタテイメント性のあるためユーザーに CAPTCHA を解く楽しさを与える．特定の動きをする人物やキャラクターの動画を再生し，その動作を説明する選択肢を選ぶ形式のもの [26] や不自然に途切れている動画の位置を選択する形式 [8] などが存在する．

2.2.5　パズル型 CAPTCHA

パズル型は一塊の出題画像を解く形態をしている．その一例を図 5 に示す．この例の場合，空白のピースに当てはまる適切なパズルピースを選択することで CAPTCHA チャレンジ成功となる．制限時間を設ける他，選択パズルピースの輪郭を容易に抽出できないようにパズルピースを重ねて表示するといった工夫が凝らされている．パズル型 CAPTCHA は文字通りパズル形式であるため，動画型と同様に CAPTCHA を解く楽しさがある．出題の難易度に差が出ることが問

図 4 動画型 CAPTCHA の一例 (参考文献 [4] より引用)

題点として挙げられる．パズル型 CAPTCHA はジグソーパズル形式 [27] や回転させた画像群をすべて正立させる形式 [28] の CAPTCHA などがある．

2.3 CAPTCHA の要件と代表的な攻撃

2.3.1 CAPTCHA の要件

様々な研究事例から，CAPTCHA の要件を満たす共通の要素として，安全性，利便性，出題の自動生成性がある [29]．この 3 つの要件以外の指標にも，文献 [12] のように言語に依存しないことや，文献 [7][8] でのエンタテイメント性等があるが，殆どの研究事例で共通する要件はこの 3 つである．安全性とは機械攻撃耐性が確保されていることを意味する．利便性は人間にとって解読と操作がしやすく，機械には難しい出題であることを指す．出題の自動生成性は自動で無数の出題を生成可能であることを示す．特に，出題の自動生成性について，出題のパターンが少ない場合はデータベース攻撃やインテリジェンスなしで機械に突破される可能性があるという重大な問題がある．

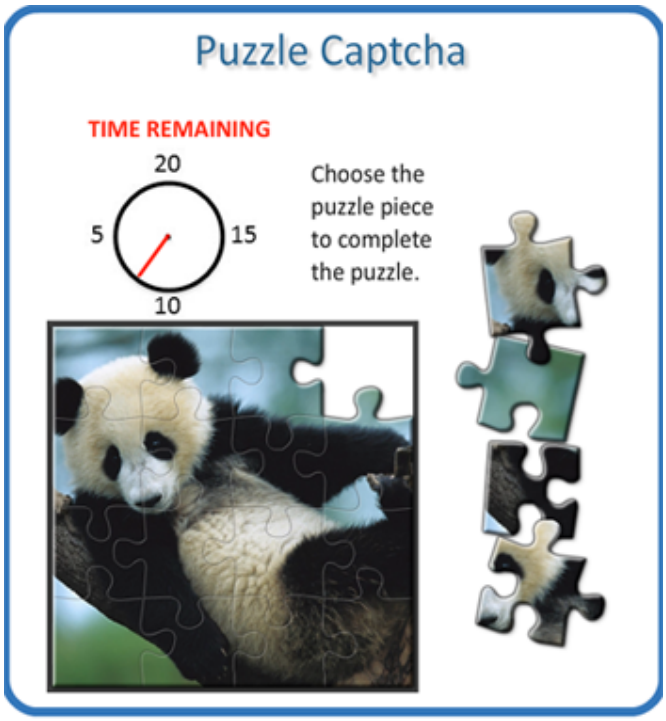

図 5　パズル型 CAPTCHA の一例 (参考文献 [5] より引用)

本論文で紹介する研究事例についてもこの 3 つの要件を明確に評価する．続く 2.3.2 では安全性の評価を左右する CAPTCHA に対する代表的な攻撃を紹介する．

2.3.2　CAPTCHA に対するの代表的な攻撃

CAPTCHA への代表的な攻撃は以下の 3 つが挙げられる．

- ブルートフォース攻撃

  自動化プログラムによる攻撃の一つとしてブルートフォース攻撃が挙げられる．この攻撃は考えられる様々な入力パターンを実行するため，CAPTCHA はそれに耐えうる組み合わせ数を確保しなければならない．

  文献 [6] によると Token Bucket Scheme，3 回チャレンジのうち 2 回成功しなかった IP アドレスを排除する機能を利用する場合，4,096 通りの CAPTCHA

チャレンジを確保できればブルートフォース攻撃の耐性は充分であると示した．

- データベース攻撃

  データベース攻撃とは問題と正解のデータベースを事前に構築し，その中から正解を検索して CAPTCHA チャレンジの成功を試みる手段である．インターネット上から画像や 3DCG 等のオブジェクトを抽出して利用する CAPTCHA は避けて通れない攻撃である．抽出した画像や 3DCG オブジェクトに歪みやノイズ，回転などの加工を施すことが対策の常套手段といえる [30]．

- 機械学習を用いた攻撃

  機械学習を用いたサイバー攻撃に対する防衛機構の開発が盛んな一方で，それを攻撃する手段として活用する場面も増加の傾向にある．文字型 CAPTCHA は OCR 技術による解読が新たな CAPTCHA の必要性を訴えるきっかけとなったが，今ではその技術を超える性能で，機械学習による CAPTCHA チャレンジの成功が容易となっている．偏に機械学習を用いた攻撃といっても，その工程は前処理とデータの断片化という機械学習を必要としない二段階のプロセスも含まれている [31]．最初の前処理で，出題されたデータをノイズ低減技術などのデータ解析を容易にする技術を扱い，次に，クラスタリングアルゴリズムを用いて断片化することで Support Vector Machine (SVN) などの機械学習を使用して各断片にどのデータが含まれているかを認識する．

3. 近年の画像型 CAPTCHA の分析

文字型 CAPTCHA が機械的に解析可能となってからは画像型 CAPTCHA の研究事例が増加の傾向にあるが，画像型でも出題に示された画像を選択せよ，といった CAPTCHA は機械的に解析可能となっている．そこで，人間の高度な知識処理，または機械が苦手な空間認識などの分野に焦点を当て研究する事例が近年増加している．本章ではその研究に携わる 2011 年以降の画像型 CAPTCHA を紹介する．それぞれの研究事例について，CAPTCHA の 3 つの要件を満たしているか，また，その他の利点や欠点を述べる．

3.1 人間のユーモアを理解する能力に注目した CAPTCHA

人間の高度な認知処理の一つである，人間のユーモアを理解する能力に着目した研究事例を紹介する．

高性能な OCR 機能を備えるマルウェアが出回るようになってきた [32] ため，既存の文字型 CAPTCHA では有効なチューリングテストとは言えなくなってきた．文字画像の変形の強度を高めることでマルウェアの対策を取ることは可能だが，正規ユーザーには読み取ることが困難と成るため利便性が低下する問題がある．そこで，人間の「より高度な知識処理」を利用して強化する方法が検討されてきた [33]．その代表的な例として Asirra [6] が挙げられる．Assira では複数の動物の絵を表示し，その中から特定の動物の絵を選ばせる手法である．Asirra の認証画面例を図 6 に示す.「絵の意味を理解する」ことは人間の高度な認知メカニズムの 1 つであり、マルウェアによる不正回答は不可能であると考えられていたが，Asirra を破る自動プログラムに関する研究報告がされた [34]．このことから，マルウェアが高度になっても不正回答が根本的に不可能である「究極的なチューリングテスト」が必要とされる時代に成ってきたといえる，と可児らは主張した．また，彼らは，チューリングテストは人間にとっては煩わしい手間であるため，その手間を低減する要求を満たすことも重要であると示している．

そこで，可児らは人間の「ユーモアを解する能力」に着目した．可児らの 4 コマ漫画 CAPTCHA [7] はランダムに出題した 4 コマ漫画の画像を正しい順序に並

図 6　Asirra の認証画面例 (文献 [6]，p.366 より引用)

べる手法を提案している．本来煩わしい手間である CAPTCHA にエンタテイメント性を持たせ，ユーザに楽しさを与える CAPTCHA の実現を目指した．4 コマ漫画 CAPTCHA の認証画面例を図 7 に示す．この例の場合，4 コマ漫画が左から 1, 4, 3, 2 と並んでいるため，2 コマ目と 4 コマ目を入れ替えることで CAPTCHA チャレンジ成功となる．

この研究での評価実験は 3 つ行われた．先ず，コンテンツの内容による正答率の変化を評価した．次に，コンテンツの量の変化に伴う利便性と安全性の変化を調べ，最後に 4 コマ漫画 CAPTCHA のエンタテイメント性のアンケート評価を実施した．

それぞれの評価実験について具体的な説明を加える．コンテンツの質における

図 7　4 コマ漫画 CAPTCHA の認証画面例 (文献 [7]，p.2235 より引用)

表 1　4 コマ漫画のコンテンツ内容による正答率が最も高いもの

コンテンツ	平均正答率	回答時間
起承転結が明確なもの	98.0 %	28.5 s

実験は CAPTCHA の要件の一つである利便性を満たすものか，という目的を持つ．つまり，4 コマ漫画の種類はユーザへの出題難易度を左右するものであるかを検証した．コンテンツは，ネット上に公開されていたものから無作為に抽出したもの，起承転結が明確なもの，ある 1 コマを取り除くと残ったコマの順序が明確になるものの 3 種類を用意した．これら 3 つのタイプの中でも，起承転結が明確なコンテンツが最も正答率が高い結果を得られた (表 1)．2 つ目の評価実験では，ブルートフォース攻撃に耐えうる最適なコンテンツの量となる出題形式を構成して安全性の向上を図り，その利便性を再評価した．改良した出題形式は，基本方式を複数回繰り返す方法，ダミーのコマを加える方法，複数のコンテンツを混ぜ合わせる方法の合計 3 つを用意した．3 種類の改良方式の中でも，ダミーのコマをを 2 つ混ぜた方式が最も総合評価が高かったが，文字型と比較すると回答時間と総当り数に劣る結果となった．エンタテイメント性の評価では，従来の文字型 CAPTCHA ，4 コマ漫画 CAPTCHA の基本方式，改良方式 3 のそれぞれについて，回答する楽しさ，問題の簡易さ，回答の面倒さ，正解する嬉しさ，再挑戦したいか，統一するならどの CAPTCHA が良いかの 6 つのアンケートを用いて調査した．

これらの評価実験から，4 コマ漫画 CAPTCHA の回答時間は従来の文字型に劣るが，アンケートの調査結果から回答する楽しさがあるため利便性を少し満た

表 2　4 コマ漫画のコンテンツ量に伴う正答率と回答時間の変化

方式	平均正答率	回答時間	総当り数
文字型	92.86 %	12.63 s	26^7 通り
ダミー 2 コマ追加	96.43 %	28.24 s	360 通り

していると考えられる．しかし，起承転結が明確なコンテンツを自動収集する仕組みが確立していないこと，4 コマ漫画の利用に伴う著作権の配慮，加えて，ブルートフォース攻撃に弱いため，安全性と自動生成性の面で問題が残った．

3.2 違和感に着目した CAPTCHA

人間には可能，且つコンピュータには難しいとされているものの一つとして違和感が挙げられる．違和感とは，生理的または心理的に作用する感覚である．人間には食い違っていると感じてもコンピュータにはそれを認知することが不可能であるように工夫を凝らした CAPTCHA の研究事例を紹介する．

3.2.1 動画型ワンモア CAPTCHA

図 8　ワンモア CAPTCHA の認証画面例 (文献 [8]，p.5 から引用)

文字型 CAPTCHA の脆弱性が報告されてからは新しい CAPTCHA の研究が活発になっている．CAPTCHA の要件とされている安全性と利便性はトレード

表 3 ワンモア CAPTCHA の正答率の変化

CAPTCHA タイプ	初回正答率	2 回目の正答率
入れ替え型	90 %	100 %
切り抜き型	100 %	100 %

オフの関係であり，この関係のバランスを崩さず，且つ，正規ユーザーに煩わしさを感じさせない新しい手法を確立する必要があると可児らは主張している．そこで彼らは人間の「違和感を判別する能力」と「ユーモアを解する能力」に着目した．安全性の向上を「人間の高度な知識処理」で、利便性の向上を「クイズがもつエンタテイメント性」で作用させ、安全性と利便性のバランスを保つことを意図している．

違和感を判別する能力とユーモアを解する能力によってチャレンジする CAPTCHA として，可児らはワンモア CAPTCHA [8] を提案した．その提案内容は面白いストーリー性を持った動画から，そのシーンの中から入れ替えた位置，または，切り取られた適切なシーンの選択を回答することによるクイズ形式の CAPTCHA である．入れ替え型動画 CAPTCHA の認証画面例を図 8 に示す．この場合，トムがテニスコートにいる場面の途中に別のキャラクターに切り替わる．この瞬間に一時停止ボタンをクリックすることで CAPTCHA チャレンジの成功とみなす．切り抜き型の場合はその箇所の前後，誤差 1 秒程度で一時停止できれば CAPTCHA チャレンジ成功となる．

ワンモア CAPTCHA で利用する動画は，見て楽しい，無音声，且つ，ストーリーが明確である条件を満たした「トムとジェリー」を採用した．元動画の再生時間は 30 秒程度である．入れ替え型ではその 30 秒間のうちの 5 秒間を別のシーンに入れ替え，切り抜き型では 1〜2 秒間シーンを削った 28〜29 秒間の動画を用意した．この CAPTCHA は動画を見る回数には制限を設けないが，回答する回数には制限を課した．

可児らはワンモア CAPTCHA の正答率から利便性を評価し，安全性と自動生成性について考察を行った．動画入れ替え型と切り抜き型それぞれ 2 問を被験者に問いてもらった結果を表 3 に示す．ワンモア CAPTCHA の安全性について，そ

表 4 ワンモア CAPTCHA の安全性についての評価項目

方式	動画の長さ	正解区間	総当り攻撃の成功確率
入れ替え型	30 s	5 s	1/6
切り抜き型	28〜29 s	2 s	1/14

れぞれのタイプの動画の長さ，正解区間から算出した総当たり攻撃の成功確率をまとめた表を表 4 に示す．このことから，可児らはワンモア CAPTCHA は安全性の要件を満たしていないと判断を下した．出題の自動生成性について，動画コンテンツはインターネット上に多数存在するため，コンテンツの量には問題はない．しかし，正答率に関わる，ストーリー性のあるコンテンツを自動的に収集することは現状難しいと可児らは判断した．加えて，彼らは文字型と 2 種類のワンモア CAPTCHA それぞれに対する利便性のアンケートを実施した．アンケートでは，それぞれの CAPTCHA を解く楽しさ，面倒さ，容易さ，正解できた嬉しさ，再挑戦したいか，総合点の 6 つを評価した．

評価実験から可児らの提案したワンモア CAPTCHA は回答時間が長いが，アンケート調査からエンタテイメント性がある結果を得られたため，利便性を少し満たしていると考えられる．しかし，動画全体と入れ替えたシーンの長さから，機械攻撃で 6 分の 1 の確率で CAPTCHA チャレンジが成功する問題，加えて，切り取り型だと 14 分の 1 の確率で成功するといった安全性の問題が残った．また，4 コマ漫画 CAPTCHA と同様に，ストーリーが明確なコンテンツを自動的に収集する方法と動画の著作権への問題があった．

3.2.2 非現実画像 CAPTCHA

文字型 CAPTCHA が機械的に突破可能となってからは新しい手法が必要となった．新しい手法として最も有効な手段の 1 つに人間の高度の認知能力が挙げられる．その中でも,「常識からの逸脱を認識する能力」を利用する方法が知られている．その関連研究として，Avatar CAPTCHA[9] と SS-CAPTCHA[35] が挙げられる．

Avatar CAPTCHA は本物の人間の顔と CG のものとを識別する CAPTCHA

である．その認証画面例を図 9 に示す．Avatar CAPTCHA ではアバターの顔をすべて選択できたユーザーを正規であると判断する．図 9 の場合，上段の左から 1 番目と 4 番目，加えて，下段の左から 1，3，6 番目をすべて選択することで CAPTCHA チャレンジ成功となる．人間は「人間に極めて似たもの」に対して違和感を覚えることが知られている．そのため，D'Souza らは Avatar CAPTCHA が新しい画像型 CAPTCHA として有効なものであると考えたが，物体認識の技術と機械学習を利用することで機械による突破が可能であると指摘されている [36]．また，自動的に本物の人間の顔画像を収集することが難しい問題があった．

SS-CAPTCHA は人間が作成した自然な文章と機械翻訳が生成したものとをそれぞれ複数出題し，自然な文章をすべて選択できたユーザーを正規のものと判断する．その認証画面例を図 10 に示す．機械翻訳技術は日々進歩しているが，多言語の文章を機械翻訳にかけて生成した日本語は不自然な文章になることも多く，自然な文章を自動的に作り出すことは非常に難しい技術である，と藤田らは述べている．SS-CAPTCHA の出題を自動生成するためには多くの自然な文章が必要であるが，自然な文章を機械が利用できない形で効率よく集めることは難しい課題が残っていた．

図 9　Avatar CAPTCHA の認証画面例 (文献 [9],p3 より引用)

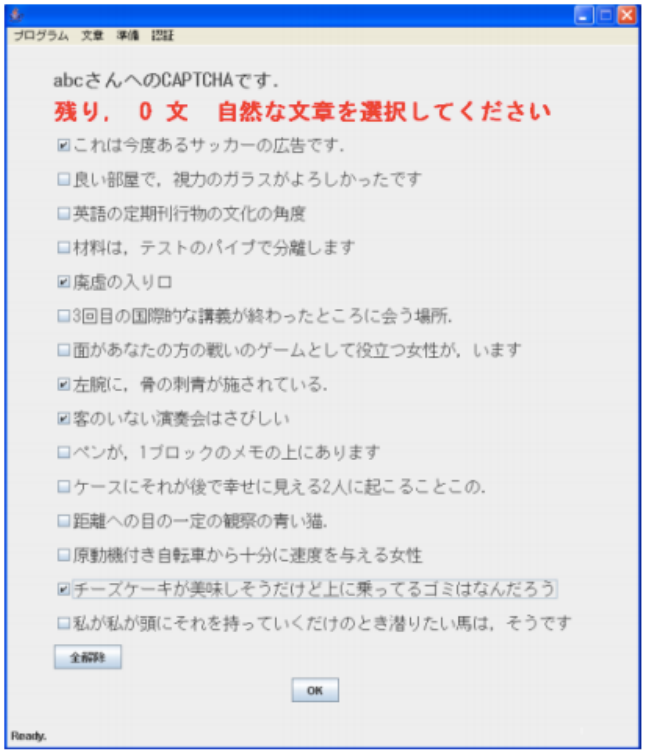

図 10 SS-CAPTCHA の認証画面例 (文献 [10], p7 より引用)

これらのことから，常識からの逸脱を認識する能力を利用した関連研究 [9][35] はいずれも安全性と問題の自動生成性を両立出来ていなかった．そこで，藤田らはこれらの問題を解決する CAPTCHA として，2 つの 3DCG オブジェクトをマージさせた一体の非現実オブジェクトと，複数の通常オブジェクトを一枚画像で出力し，非現実的なオブジェクトを選択させる方式を提案した [11].

藤田らの提案した CAPTCHA の認証画面例を図 11 に示す．図 11 のうち，車と犬を不自然にマージさせたオブジェクトを選択することで CAPTCHA チャレンジの成功とみなす.

評価実験はユーザーの利便性と 3DCG オブジェクトのめり込み検出に関する安全性の評価，加えて，自動生成性について考察を行った．利便性の評価では，オブジェクト数が 4，8，12，16 体，それぞれの正答率と回答時間を計測した．その結果，4 パターン全ての実験において正答率は 90%以上，平均回答時間は 5.5 秒

図 11　非現実 CAPTCHA の認証画面例 (文献 [11]，p.2328 より引用)

以下と，文字型より短い結果を得られた．オブジェクトめり込みの検出は遮蔽関係にある画像とめり込み画像を学習したニューラルネットワークを用いて実験を行った．その結果として,「めり込み」の判定は難しいため，機械学習を用いた攻撃に強いことを藤田らは示した．最後に，自動生成性について，藤田らは非現実画像 CAPTCHA に用いるオブジェクトには 4 つ制約が必要であるとしたが，そのどれもが自動的に識別する方法は実現可能であると示した．

これらの評価実験から，藤田らが提案した非現実画像 CAPTCHA の利便性と安全性は従来の文字型と同等であること，また，Web 上から収集した 3DCG オブジェクトを加工してから CAPTCHA で利用するため Web 探索攻撃の耐性があることを示した．加えて，自動生成性の要件を満たす可能性も高い利点がある．しかし，輪郭抽出技術を応用した機械攻撃により破られる可能性が挙げられる．

3.3　空間認識能力や形状認識能力に着目した CAPTCHA

3 次元の空間認識や人間が自然と共通意識を覚える形状認識能力はコンピュータが苦手としている分野の一つとされている．本節ではその分野を利用した CAPTCHA の研究事例を挙げる．

3.3.1 GISTCHA

従来の文字型 CAPTCHA の脆弱性の問題はもちろん，画像型でも限界がある．何故なら，データベース攻撃 [34][37] や画像認識 [31][38][39] による突破が可能であるためだ．また，文字型と音声型だと言語依存の問題も存在する．加えて，既存 CAPTCHA はパーソナルコンピュータ向けであるため，携帯型のデバイスで CAPTCHA にチャレンジするには操作が難しい．携帯型デバイスは急激に普及したため，それに適合する CAPTCHA も必要となってきた，と Yang らは主張している．

そこで彼らは，ゲーム型のイメージセマンティクスを用いた CAPTCHA である GISTCHA を提案した [12]．GISTCHA はキーボードを使用せず，ジェスチャや加速度計といった要素をもつスマートフォンでの使用を想定したものとなっている．Yang らは GISTCHA の手法を 2 種類提案した．1 つはローリングゲーム式 (図 12)，もう一方はダンス・ダンス・レボリューション (DDR) 式 (図 13) である．GISTCHA の操作イメージ図を図 14 に示す． ローリングゲーム式は直感的

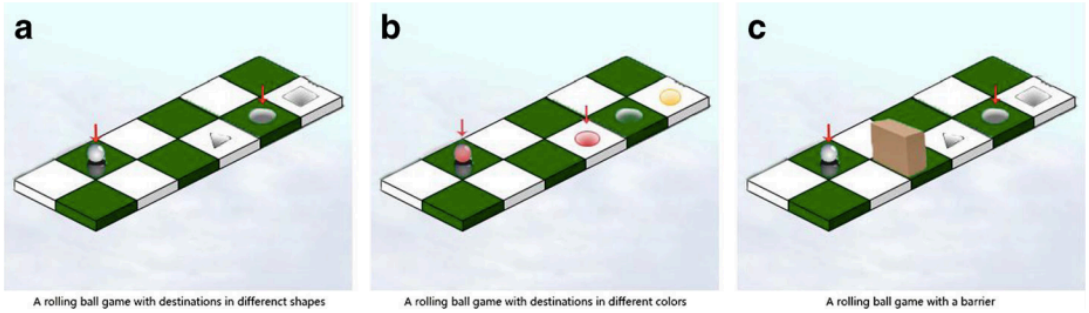

図 12 ローリングゲーム式 GISTCHA(文献 [12]，p.5145 から引用)

に正解と判断したマス，図 12(a) の場合は白い円状のマスへ，図 12(b) の場合は赤い円状のマスへボールを進めることで CAPTCHA チャレンジ成功となり，DDR 式は左上から右下の矢印と同じ方向に携帯端末を傾けることで CAPTCHA チャレンジ成功となる．

GISTCHA のコンセプトは次の通りである．

- 複数のシンプルな Web ゲーム型

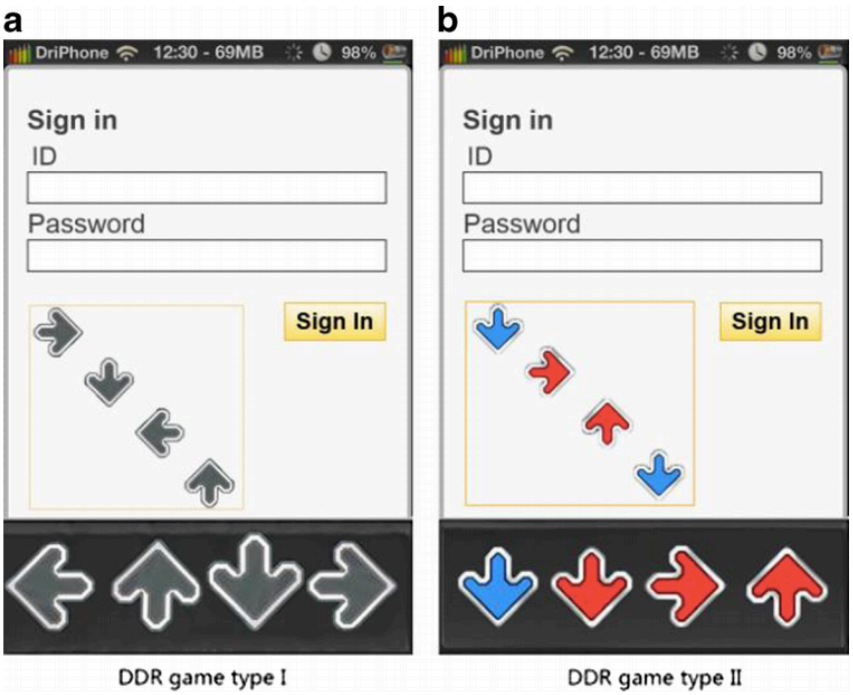

図 13　ダンスレボリューション式 GISTCHA(文献 [12]，p.5149 から引用)

この形式を採用する理由として，複数の種類のゲームを解くことは人間にとって容易であるが，機械には難しいことを挙げている．

- キーボードを使用しない操作

  ジェスチャと加速度計による操作にすることで，年齢や言語に依存しない CAPTCHA チャレンジが可能であることを目的とする．

ローリングゲーム式 GISTCHA の場合，人間は自然とボールをそれと似た形状の目的地マスへ移動するが，この認知処理が機械にとっては難しいとされている．また，図 12(b) のように目的地マスの形状がすべて同じものに変化しても，人間は操作するボールと共通点を感じるものがゴールであるという認識を抱く．このような高度な人間の認知処理を GISTCHA で活用している．

この研究では従来のものも含めた 6 つの CAPTCHA チャレンジの初回正答率と各コントロールシステムの平均操作時間の調査による利便性の評価，及び従来

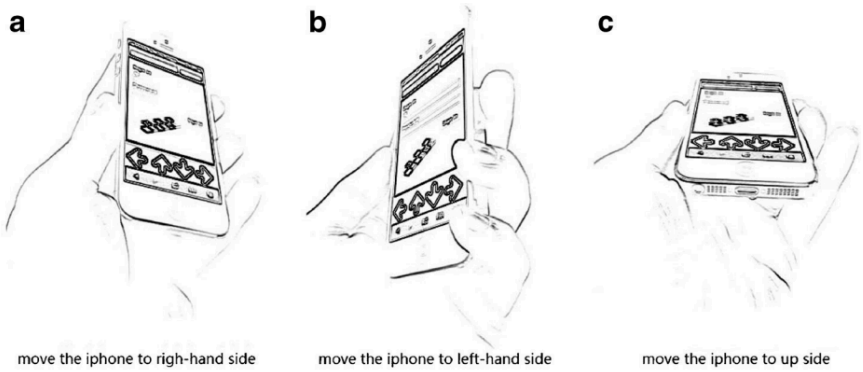

図 14 GISTCHA の操作イメージ図 (文献 [12]，p.5147 から引用)

表 5 GISTCHA の初回正答率

GISTCHA タイプ	初回正答率
ローリングゲーム式	95 %以上
DDR 式	90 %以上

手法と比較したアンケート調査を実施した．GISTCHA は本来キーボードを利用しないことを想定しているが，従来法との比較のため今回はキーボードとマウスでも操作可能とした．

Yang らはローリングゲーム式 3 種，DDR 式 2 種それぞれの初回正答率とコントロールシステム別の平均操作時間から GISTCHA の利便性を測った．ローリングゲーム式と DDR 式の初回正答率はどちらも 90%以上 (表 5) の結果が得られ，コントロールシステム別の平均操作時間はキーボード操作では GISTCHA が勝り，加速度計を用いた操作においては DDR 式が優れている結果が出た．安全性面ではブルートフォース攻撃と機械学習に対して Yang らは考察を行った．まず，現状のマップ及び矢印の数だと総当り数は 50 を満たさないため，現状のままだとブルートフォース攻撃に弱いと指摘した．また彼らは機械学習による画面イメージ学習による分類に対して，ローリングゲーム式だと 3 次元空間のゲームであるため分類は難しいとされたが，DDR 式は指向性のある平面的なゲームであるため機械学習による突破される可能性があると考えた．

評価実験の結果から，Yang らが提案した GISTCHA は初見での正答率が高く，

文字型を上回る操作性があることがわかった．また，ゲーム型であるためエンタテイメント性を持ち，言語と年齢に依存しない CAPTCHA を確立できたといえる．その一方で，ブルートフォース攻撃の耐性がなく，DDR 式は機械学習による突破の可能性がある安全性の問題や，携帯端末型以外のデバイスでの利用を想定していない利便性の問題があった．加えて，自動的に問題は生成できるが，現状のままでは出題数が少ない問題も残った．

3.3.2 Directcha

文字型 CAPTCHA が機械的に突破可能となってからは新しい手法が必要となった．新しい手法として最も有効な手段の 1 つといわれる人間の高度の認知能力の中には「メンタルローテーション」が存在する [35][9]．メンタルローテーションとは，1 つの視点から写された 2 次元オブジェクトや 3 次元オブジェクトを思考で回転させ，異なる視点から写された形式を認知する能力のことを指す．この認知能力を利用した関連研究の 1 つに YUNiTi CAPTCHA [40] が挙げられる．YUNiTi CAPTCHA は Cognometric 型メンタルローテーション，つまり，候補画像群の中から出題画像と同じ 3 次元オブジェクトを選択する方式を採用している．その認証画面例を図 15 に示す．3 つの回転されたオブジェクトと同じオブジェクトを候補画像群からすべて選択できた場合に CAPTCHA チャレンジ成功とみなす．出題オブジェクトの回転角度はランダムであるが，候補画像群は常に一定の方向を保っている．YUNiTi CAPTCHA 場合,「候補画像群の中から出題画像と最も近い特徴を有する画像を選択する」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と佐野らは述べた．

そこで彼らの研究では同じオブジェクトを選択するのではなく，オブジェクトの向きを回答する CAPTCHA を提案した．

佐野らが提案した Spatiometric 型メンタルローテーション CAPTCHA [13] はパズル型に近く，出題画像の 3 次元オブジェクトの向きを回答する形式をしている．その認証画面例を図 16 に示す．図 16 の場合，上方左手前側のパネルをクリックすることで CAPTCHA チャレンジ成功となる．評価実験は利便性の評価と安全性及び自動生成性の考察を行った．利便性評価では総当りの数 4 と 8 の Directcha，

図 15 Cognometric 型メンタルローテーション CAPTCHA ”YUNiTi CAPTCHA” の認証画面例 (文献 [13]，p.2 から引用)

YUNiTi CAPTCHA の合計 4 つの出題の正答率と回答所要時間の調査を実施した．総当りの数が 4 つの場合，Directcha は選択パネルが 4 つ，YUNiTi CAPTCHA は回答する候補画像群が 4 つとなる．利便性の評価実験の結果を表 6 に示す．佐野らが提案した Directcha は YUNiTi CAPTCHA と比較して平均正答率は低い結果となっているが，どれも 90%以上を超えており，間違えた原因を聞き取り調査したところ，クリックのミスによる不正解もあったため正答率および回答時間は YUNiTi CAPTCHA とほぼ同等であると示した．続いて佐野らは評価実験 1 を基に基準値を満たす総当り数を確保した場合の正答率と回答時間の期待値の算出，データベース攻撃と機械学習に対する考察を行った．その結果，Directcha は総当り数を確保した条件のもとでも正答率が 90%以上，回答時間が 7.2 秒であることを示し，また，オブジェクトを加工して出題すること，加えて，将来的に 3

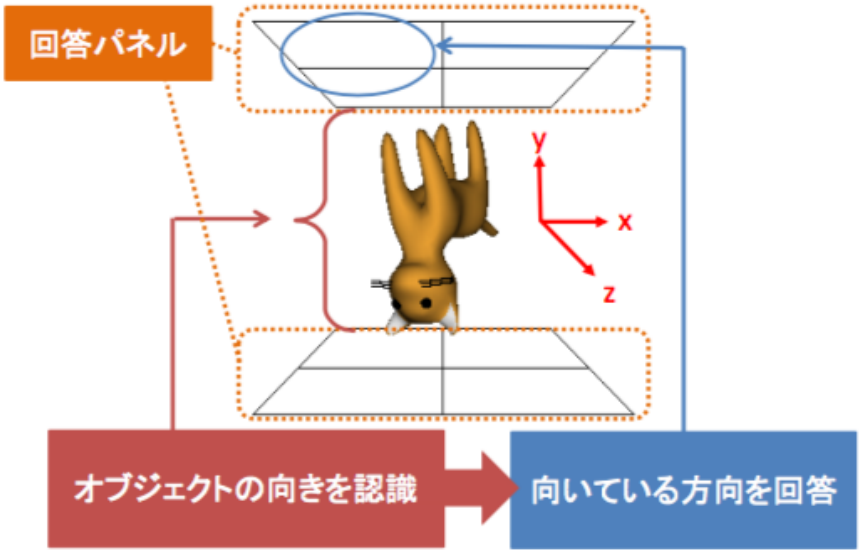

図 16　Sepatiometric 型メンタルローテーション CAPTCHA ”Directcha”の認証画面例 (文献 [13]，p.3 から引用)

次元モデルは無数に出回ると予測されることから Directcha はデータベース攻撃に耐え，機械学習によるオブジェクトの回転角度を識別する分類器を作ることは難しいと推測された．

自動生成性については向きを有する 3 次元オブジェクトの認識を可能にできれば，この要件を満たすと佐野らは考えた．

これらの評価実験から佐野らが提案した Directcha は基準値とされる総当り数を確保した場合でも正答率 90%以上と回答時間 10 秒未満であり，総当たり攻撃とデータベース攻撃への耐性があること，更に，将来的には 3 次元モデルは無数に出回ると予測することから機械学習による攻撃にも強いという利便性と安全性の要件を満たした．その一方で，現状では向きを持つ 3DCG オブジェクトの自動収集が難しい課題が残った．

3.4　感情表現に着目した CAPTCHA

本節では人の感情表現に焦点を当てた CAPTCHA の事例を紹介する．

表 6 評価実験 1: Directcha と YUNiTi CAPTCHA の平均正答率と平均解答時間

CAPTCHA	総当り数	平均正答率	平均解答時間
Directcha	4	91.7 %	1.52 s
	8	97.9 %	1.80 s
YUNiTi	4	100.0 %	1.44 s
	8	100.0 %	1.64 s

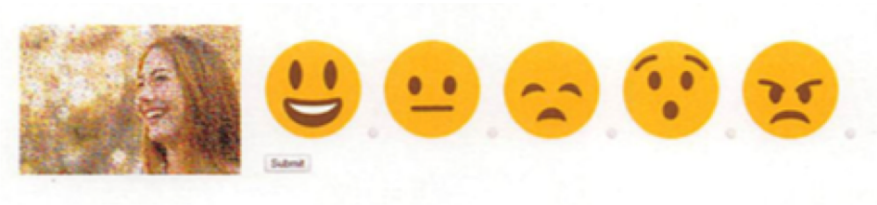

図 17 EmojiCHA の認証画面例 (文献 [14]，p.288 より引用)

既存の文字型 CAPTCHA が機械的に解析可能となってからは画像型 CAPTCHA が導入されるようになった．画像型 CAPTCHA ではオブジェクトまたは画像認識 [41][42] や，カテゴリ分類タスク [6][43][44] が主要な CAPTCHA チャレンジとなっている．しかし，この形態の CAPTCHA にはスケールの拡大が難しいという欠点が存在する．具体的には，使用する画像を手作業で収集，編集，タグ付け，索引付け，一意なものにする等といったプロセスを指す．また，攻撃者は画像処理とコンピュータビジョンツール [45] と新しい機械学習 [34] を用いてある程度，機械的に CAPTCHA チャレンジに成功している，と Lorenzi らは述べている．

そこで，彼らは「機械には難しく，スケーラブルで使いやすい画像型 CAPTCHA の開発」を研究目的とした．

EmojiTCHA は Lorenzi らに提案された，歪みやノイズ等のフィルターを掛けた出題画像の人物が表現する感情とそれに合致する絵文字を選択する CAPTCHA である [14]．その認証画面例を図 17 に示す．図 17 の場合，出題画像の女性は笑顔で嬉しそうな感情を表しているため，左端の絵文字を選択して送信ボタンを押すことで CAPTCHA チャレンジの成功となる．

彼らの提案手法では，画像内の顔識別，顔の表現の決定，適切な絵文字との

マッチングを自動的に決定する．人物の顔とその感情を特定するツールとして Microsoft の人工知能 Project Oxford が保有する API を活用した．Face API を用いて画像から人物の顔を検出し，Emotion API でその表情が表す感情のスコアを決定する．感情は anger, contempt, disgust, fear, happiness, neutral, sadness 及び surprise の合計 8 つを検知可能である．出題画像はインターネット上から抽出し，ノイズなどのフィルターを画像に掛けることでデータベース攻撃への耐性を付与した．Lorenzi らはまず，被験者の正答率と 8 つの感情毎の正答率を評価した．その結果，“悲哀，嫌悪，恐怖，軽蔑，怒り” の正答率が低い結果を得たため，感情を 5 つに絞って再度利便性を評価した結果、“通常”83%、それ以外の感情は 90%を超える正答率が得られた．

彼らはブルートフォース攻撃とデータベース攻撃に対しての安全性の評価も実施した．EmojiTCHA はブルートフォース攻撃に耐えうる基準値を満たす総当り数を確保する手段を確立できていないが，元画像を加工するためデータベース攻撃に耐えうると考えられた．

これらの評価実験からロレンジらが提案した EmojiTCHA は 5 つの感情による正答率が高く，データベース攻撃への耐性があることがわかった．また，出題に用いる画像はインターネット上に大量に存在し，顔認識および画像加工の手法を確立しているため自動生成性の要件を満たしている．その一方，回答群に使用する絵文字の数が少ないことから総当たり攻撃への耐性がなく，安全性の問題が残った．

3.5 既存手法と紹介事例のまとめ

既存手法である文字型，及び，音声型 CAPTCHA ，そして紹介した 6 つの研究事例の要件評価をまとめたものを表 7 に示す．この表から，安全性の要件を満たすのは難しい傾向にあることがわかる．

これらの中から要件をほぼ満たした事例は非現実画像 CAPTCHA と Directcha であるが，非現実画像 CAPTCHA も安全性には問題が残っている．Diretcha は唯一安全性に ○ 評価がついているが，自動生成性の条件を満たす「方向性のあるオブジェクトの自動収集」が可能となった場合，そのオブジェクトを識別する

技術が攻撃にも用いられる可能性があるため，自動生成性の条件を満たすには更なる安全性への配慮が必要となるだろう．

このように，ブルートフォース攻撃やデータベース攻撃だけでなく，安全性を満たすには画像解析技術が関わりつつある．

表 7 既存 CAPTCHA と 6 つの研究事例の要件評価

CAPTCHA	安全性	利便性	自動生成性	問題点
文字型	X	○	○	OCR 技術により突破可能
音声型	X	△	○	音声解析技術により突破可能
4 コマ漫画	X	△	X	コンテンツ自動収集が難しい
ワンモア	X	△	△	総当り攻撃の耐性がない
非現実画像	△	○	○	輪郭抽出を応用した攻撃の可能性
GISTCHA	X	△	△	携帯端末のみでの利用を想定，回答パターン数が少ない
Directcha	○	○	△	特定のオブジェクト収集が難しい
EmojiTCHA	X	○	○	総当たり攻撃の耐性が低い

4. 近年の画像及び動画解析技術

近年の画像処理や動画解析の精度は著しく進歩している．本章ではそれらに関する研究から，今後どのような解析が可能となるか考察する．

国内における事例の一つとして北海道大学情報科学研究科メディアダイナミクス研究室における研究を 4.1 で，世界での事例の一つとして Google の動画分析 API を 4.2 で紹介する．

4.1 北海道大学 情報科学研究科 メディアダイナミクス研究室における研究

北海道大学 情報科学研究科 メディアダイナミクス研究室では長谷山教授のもと，画像や映像を人間のように理解するシステムの実現を目標に，人間の感覚を基盤とした認識手法や，映像の復元手法などの技術開発を進めている [15]．この研究室における消失領域の復元技術 (図 18) は画像中の不要なオブジェクトの除去や経年劣化したフィルムの復元が可能である．また，インパルス性雑音除去技術 (図 19) の研究 [46] から，ノイズ等の加工を施した動画型 CAPTCHA も将来的には元の解像度に等しい動画へと再変換可能となるだろう．

加えて，メディアダイナミクス研究室は映像中のカメラの切り替わりや同一の話題を持つ区間を自動で検出する技術に関しての研究 [47] にも取り組んでいる．その他，画像に含まれる意味を解析し，その中から特定のオブジェクトを抽出する画像処理技術を確立した．

4.2 Google Cloud Video Intelligence API

上述の研究室と同じようにコンテンツ中の意味を把握するシステムの一つとして，2017 年 3 月，Google は動画の内容の意味を分析する API を発表した [16]．Google Cloud Video Intelligence API は入力した動画から，その内容を単語で表す Labels，動画のシーンが切り替わるタイミングで自動的に区切る Shots，そして API のリクエストとレスポンスの情報を表示する機能を持つ．Labels と Shots

図 18　消失領域の復元技術による画像中の不要なオブジェクトの除去 (文献 [15] より引用)

は，それぞれシーンに含まれる要素とその信頼度を示すスコアが付与されている．つまり，この API を利用することで，どのタイミングで，何が動画中に映っているかを容易に判断することが可能となった．図 20 は 左側に分析中の動画とその再生位置を，右側に Labels を表している．これらのことから，新規の CAPTCHA を提案する場合は一般的な CAPTCHA への攻撃耐性の評価のみならず，利用するコンテンツに関わるメディア処理技術にも注目することが重要になってくると考えられる．

紹介した事例のように，現状の CAPTCHA は視覚的に作用するものが大体を占めている．しかし，画像や動画の解析技術は向上する一方に加えて，解析技術は ”人間らしい” 判断・解析が可能となるような研究が進められていることがわかった．このことから，将来的には視覚的な CAPTCHA チャレンジを解析する技術は多く確立する可能性が高いと言えるのではないか．そのため，現状のままでは文字型 CAPTCHA のように，新しい手法が確立しては解析突破されて，といったイタチごっこになるのではないか．

では，確実に人と機械とを判別するにはどのような手段がよいのか．その可能性を高める手法としてバイオメトリクスを用いる方法を提案する．

図 19　インパルス性雑音除去技術の一例 (文献 [15] より引用)

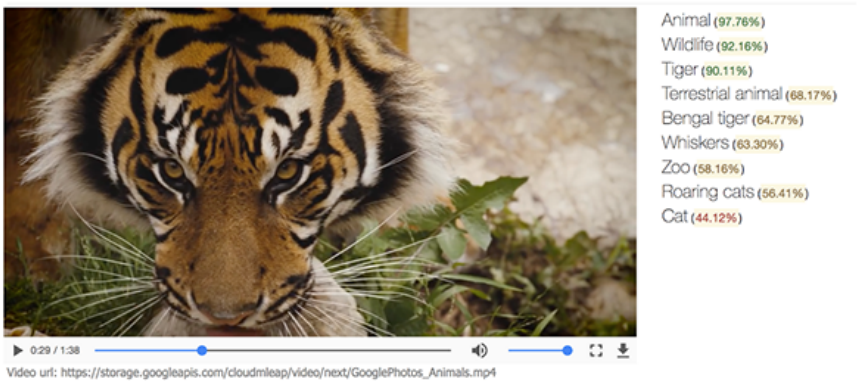

図 20　Google Cloud Video Intelligence API を用いた動画内検索の結果 (文献 [16] より引用)

5. CAPTCHA の改善案

本章ではバイオメトリクスを用いる改善を 5.2 で述べる前に，5.1 で紹介事例の 1 つである非現実画像 CAPTCHA の改善案を述べる．

5.1 非現実画像の改善案

3.2.2 で述べたように，藤田らが提案した非現実画像 CAPTCHA は利便性と安全性の要件を満たしているが，輪郭抽出技術を用いた機械攻撃により破られる可能性から安全性の評価が若干低い．この欠点を改善する案として，1 つの 3DCG の球体からオブジェクトを生成する過程を提示することを挙げる．

この改善方法の意図は，1 つの球体からオブジェクトを生成することですべてのオブジェクトを非現実的なものに見せることである．人間ならばオブジェクトの生成が途中であっても脳がオブジェクトを把握しようとするため自動的に補完機能が働くため，人間には非現実的なオブジェクトを選択することが容易である．その一方で，機械はオブジェクトの生成過程が終了した段階でないと各々のオブジェクトを把握できない．この改善案の問題点は，生成過程を観察しなければならないため，動画型 CAPTCHA のように CAPTCHA チャレンジ成功までに時間が掛かることである．この問題点を，人気のあるキャラクターをオブジェクトに加えてエンタテイメント性を持たせる等の方法で改良するのもまた一つの手である．

5.2 バイオメトリクスを用いた CAPTCHA

前章の末尾で，確実に人と機械とを判別する可能性を高める手法としてバイオメトリクスを用いることを提案する主張した．まず，バイオメトリクスを用いる理由を述べ，続いてそれを用いた CAPTCHA の例案を挙げる．

5.2.1 バイオメトリクスを採用する理由

バイオメトリクスを用いる理由は，人間の誰もが有し，機械には取り入れることができない要素であるためだ．人と機械との違いを考えると，生命体であるか否かという考えに至った．生命体には呼吸，血流，体温があり，目の瞬きや頬を手で触れる仕草といった自然な動きをすることが可能である．その一方，機械や人間に似たそうでないモノにはこれらの要素は持ち得ないため，バイオメトリクスを用いることで，確実に人間と機械を区別する可能性を高めるのではないかと考えた．

5.2.2 バイオメトリクスを取り入れた事例案

では，どのようにバイオメトリクスを CAPTCHA に取り入れるか．その一例として「インカメラによる顔認識 CAPTCHA」を挙げる．カメラを用いる理由は 2 つある．1 つは近年のコンピュータに付属されており，後付も可能なハードウェアであるため．2 つ目の理由は，監視カメラの需要は上昇の傾向にあることから，人を特定する機能の性能もそれに伴って向上すると推測したためである．

この事例案の特徴は次のようなものが考えられる．

- CAPTCHA チャレンジの存在を感じない
- CAPTCHA 解く必要がない
- 言語に依存しない
- 自動化プログラムによる攻撃を無効化する
- 視覚の問題をもつユーザにも対応可能

その一方で，人面らしき物体を人間と認識する可能性があること，及び，プライバシ問題といった課題が残る．

人間らしき物体を人間と認識する問題について少し掘り下げて考察する．画像や映像の解析技術だけでなく，ロボット工学の分野における人形ロボットの外見や動きの研究は活発的である．近年では外的な要素だけでなく，体温や発声といっ

た内部的な機能を搭載したものの開発も行われている．そのため，一概にバイオメトリクスを 1 要素のみ加えるだけでは生きた人間と人型ロボットを区別するのみ難しいものといえる．よって，バイオメトリクス性があると判断できる基準は生命らしい要素，もしくは生命らしさとロボットらしさの要素を最低 2 点以上判断可能な CAPTCHA であることだ．

現在普及しているコンピュータや携帯端末でバイオメトリクスを活用して認証することは当たり前でないといえる．しかし，Apple 社の携帯端末である iPhone シリーズでは指紋認証から始め，2018 年 1 月時点での最新型 iPhone X ではインカメラを用いた顔認証システム Face ID を導入した (図 21)[17]．また，携帯端末のアウトカメラと光学機器を利用した心拍数計測アプリケーション (図 22)[18] など，今後のバイオメトリクスを用いた認証システムや，カメラを用いたバイタルチェックシステムは発展途上にあると言えるのではないだろうか．

図 21　iPhone X による顔認証システム「Face ID」(参考文献 [17] より引用)

図 22　Sleep Cycle alarm clock による脈拍計測の説明画面 (参考文献 [18] より引用)

6. 結論

本論文では，CAPTCHA の誕生からその要件と形態について述べ，CAPTCHA に対する攻撃と恒常的に存在する問題について説明した．それに加えて，近年の画像処理研究や動画解析技術から，視覚的な CAPTCHA チャレンジを新たに提案する場合には，出題コンテンツに関するメディア処理技術に注目する必要があると考えた．

2011 年以降の CAPTCHA 研究は，人間のユーモアを理解する能力や違和感を覚える手法，空間認識能力や形状認識能力，人間の感情表現に注目するといった，人間の高度な認知能力に焦点をあてた研究や，オブジェクトの表面的な情報のみならず，それに含まれる意味に焦点を当てた研究が増加の傾向にあることがわかった．

しかし，画像や映像の解析技術は著しく向上しており，その研究の方向も人間と同様の処理を実行可能となるようにと進めているため，現状の CAPTCHA 研究では限界があるのではないかと推測した．そこで，今後の CAPTCHA の方向性として ”生命らしさ ” の要素を付与することを提案した．

近年の携帯端末は指紋認証や顔認証システム，それに付属した光学機器を利用した心拍数計測アプリケーションの事例から，今後のバイオメトリクスを用いた認証システムやカメラを用いたバイタルチェックシステムは発展途上にあると言えるのではないだろうか．

CAPTCHA の研究に関する今後の課題として，リレーアタック耐性をもつ CAPTCHA の開発が挙げられる．加えて，ブルートフォース攻撃に耐えうる CAPTCHA チャレンジ数の基準は 2007 年に定められたものであるため，安全性の基準の見直しが挙げられる．

謝辞

本研究を進めるにあたり，適切な研究のご指導を頂いた，主指導教員である本学情報基盤システム学研究室の藤川和利教授に深謝致します．副指導教員である，本学ユビキタスコンピューティングシステム研究室の安本慶一教授，並びに，本学大規模システム管理研究室の笠原教授には，本研究の方向性について貴重なご意見をくださいました．ここに心から感謝の意を表します．同じく，副指導教員であり，研究方針や論文執筆にあたり，熱心なご指導をしてくださいました本学情報基盤システム学研究室の新井イスマイル准教授に心から感謝の意を表します．研究の方針について，貴重なご助言をくださいました東京電機大学の猪俣敦夫教授に心から感謝致します．本研究を進めるにあたり，貴重なご意見をくださいました，本学情報基盤システム学研究室の垣内正年助教，油谷曉助教に心から感謝致します．また，日常の議論を通じて多くの知識や示唆を頂いた本学情報基盤システム学研究室の皆様，また，様々な面から研究活動を支援くださいました，本学総合情報基盤センターと辻本理恵女史，並びに，中野彩子女史に心から感謝を申し上げます．

最後に，経済面や生活面で援助をくださいました家族と，励ましを続けてくださいました友人たちへ心から感謝の気持ちを申し上げたく，謝辞にかえさせていただきます．

参考文献

[1] Google Developers. “reCAPTCHA Troubleshooting”. https://developers.google.com/recaptcha/old/docs/troubleshooting, 2018.3.7 アクセス.

[2] Confident Technologies. “Confident CAPTCHA”. http://confidenttechnologies.com/confident-captcha/, 2018.3.7 アクセス.

[3] ManageEngine. “MIT Technology Review Intelligent Machines Video Ads that Outwit Spammers”. https://www.technologyreview.com/s/421318/video-ads-that-outwit-spammers/, 2018.3.7 アクセス.

[4] Tom Simonite. “ManageEngine ADSelfService Plus Did you know: How to configure Audio CAPTCHA?”. https://www.manageengine.com/products/self-service-password/kb/adselfservice-plus-audio-captcha-configuration.html, 2018.3.7 アクセス.

[5] TYNAX PATENT LIBRARY. Captcha technology using a puzzle, 2018.3.14 アクセス.

[6] Elson J, Douceur JR, Howell J, and Saul J. “Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization”. In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007)*, pp. 366–374, 2007.

[7] 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. Vol.54, No. 9, pp. 2232–2243, 2013.

[8] 可児潤也, 上松晴信, 西垣正勝. “ワンモア CAPTCHA の提案”. 暗号と情報セキュリティシンポジウム 2012(SCIS 2012) 予稿集, pp. 1–8, 2012.

[9] D'Souza D, Polina PC, and Yampolskiy R. "Avatar CAPTCHA: Telling Computers and Humans Apart via Face Classification". In *Proc. 2012 IEEE International Conference on Electro/Infomartion Technology*, pp. 1–6, 2012.

[10] 山本匠, Tygar JD, 西垣正勝. "機械翻訳の違和感を用いた CAPTCHA の提案". Technical Report 37, 2009.

[11] 藤田真浩, 池谷勇樹, 可児潤也, 西垣正勝. "非現実画像 CAPTCHA : 常識からの逸脱を利用した 3DCG 画像 CAPTCHA". 情報処理学会論文誌, Vol. 56, No. 12, pp. 2334–2336, 2015.

[12] Yang TI, Koong CS, and Tseng CC. "Game-based image semantic CAPTCHA on handset devices". Multimedia Tools and Applications, 2013.

[13] 佐野絢音, 藤田真浩, 西垣正勝. "Spatiometric 型メンタルローテーション CAPTCHA の提案". 暗号と情報セキュリティシンポジウム 2016(SCIS 2016) 予稿集, 2016.

[14] *"EmojiTCHA: Using Emotion Regcognition to Tell Computers and Humans Apart"*, Vol. IFIP AICT 502, 2017.

[15] 北海道大学 情報科学研究科メディアダイナミクス研究室. 北海道大学 情報科学研究科 メディアダイナミクス研究室. https://www-lmd.ist.hokudai.ac.jp/, 2018.1.31 アクセス.

[16] Li FF. "Google Cloud Video Intelligence API とその他の Cloud Machine Learning の更新に関する発表". https://cloud.google.com/blog/big-data/2017/03/announcing-google-cloud-video-intelligence-api-and-more-cloud-machine-learning-updates, 2018.1.31 アクセス.

[17] Apple Inc. "iPhone X の概要". https://www.apple.com/jp/iphone-x/, 2018.1.31 アクセス.

[18] Northcube. "Sleep Cycle alarm clock". https://www.sleepcycle.com/, 2018.1.31 アクセス.

[19] Ahn L, Blum M, Hopper NJ, and Langford J. "CAPTCHA: Using Hard AI Problems for Security". Carnegie Mellon University Research Showcase@CMU, 2003.

[20] Mobile Multimedia Security. *"Protection Through Multimedia CAPTCHAS"*, 2010. MoMM2010 Proceedings.

[21] Montree Imsamai and Suphakant Phimoltares. "3D CAPTCHA: A Next Generation of the CAPTCHA". In *Information Science and Applications -ICISA 2010*, pp. 1–8, 2010.

[22] Shirali-Shahreza M and Shirali-Shahreza S. "Collage CAPTCHA". In *2007 9th International Symposium on Signal Processing and Its Applications(ISSPA 2007)*, 2007.

[23] Almazyad AS, Ahmad Y, and Kouchay SA. "Multi-Modal CAPTCHA: A User Verification Scheme". In *Information Science and Applications*, 2011.

[24] Shirali-Shahreza S, Abolhassani H, Sameti H, and Hassan M. "Spoken captcha: A captcha system for blind users". In *ISECS International Colloquium on Computing, Communication, Control, and Management (CCCM 2009)*, 2009.

[25] Gao H, Liu H, Yao D, Liu X, and Aickelin U. "An Audio CAPTCHA to Distinguish Humans from Computers". In *2010 Third International Symposium on Electronic Commerce and Security (ISECS 2010)*, 2010.

[26] Shirali-Shahreza M and Shirali-Shahreza S. "Motion CAPTCHA". In *2008 Conference on Human System Interactions*, 2008.

[27] Gao H, Yao D, Liu H, Liu X, and Wang L. "A Novel Image Based CAPTCHA Using Jigsaw Puzzle". In *2010 IEEE 13th International Conference on Computational Science and Engineering*, 2010.

[28] Ross SA, Halderman JA, and Finkelstein A. "Sketcha: a captcha based on line drawings of 3D models", 2010.

[29] *"Survey of Different Types of CAPTCHA"*, Vol. 5(2), 2014.

[30] *"A SURVEY OF CURRENT RESEARCH ON CAPTCHA"*, Vol. 7, 2016.

[31] Chellapilla K and Simard P. "Using Machine Learning to Break Visual Human Interaction Proofs (HIPs)". In *Advances in Neural Information Processing Systems (NIPS)*, 2004.

[32] Yan J and Ahmad ASE. "Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms". In *Twenty-Third Annual Computer Security Applications Conference(ACSAC 2007)*, pp. 279–291, 2007.

[33] Chellapilla K, Larson K, and Simard P. "Computers beat Humans at Single Character Recognition in Reading based Human Interaction Proofs (HIPs)". In *Conference on Email and Anti-Spam(CEAS 2005)*. Conference on Email and Anti-Spam(CEAS 2005), 2005.

[34] *"Machine Learning Attacks Against the Asirra CAPTCHA"*, 2008.

[35] Yamamoto T, Tygar JD, and Nishigaki M. "CAPTCHA Using Strangeness in Machine Translation". In *Proc. 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 430–437, 2010.

[36] *"Solving Avatar Captchas Automatically"*, 2012.

[37] Chew M and Tygar JD. "Image Recognition CAPTCHAs", 2004.

[38] Bursztein E, Martin M, and Mitchelll J. "Text-based CAPTCHA strengths and weaknessess", 2011.

[39] DONG NGO. "3D-based Captchas become reality", 2003.

[40] Google Developers. “reCAPTCHA Troubleshooting”. https://www.cnet.com/news/3d-based-captchas-become-reality/, 2018.3.15 アクセス.

[41] Gossweiler R, Kamvar M, and Baluja S. “What’s Up CAPTCHA? A CAPTCHA Based On Image Orientation”, 2009.

[42] Rui Y and Liu Z. “ARTiFACIAL: Automated Reverse Turing test using FACIAL features”, 2003.

[43] Datta R, Li J, and Wang JZ. “IMAGINATION: A Robust Image-based CAPTCHA Generaton System”, 2005.

[44] Shirali-Shahreza S and Shirali-Shahreza M. “Categorizing CAPTCHA”, 2011.

[45] Zhu BB, Yan J, Li Q, Yang C, Liu J, Xu N, Yi M, and Cai K. “Attacks and design of image recognition CAPTCHAs”, 2010.

[46] Kondo K, Haseyama M, and Kitajima H. “Efficient fixed-valued and random-valued impulse detection for accurate image restoration”. *Information Technology Letters*, Vol. 2, pp. 239–241, 2003.

[47] 宋妍, 小川貴弘, 長谷山美紀. “映像の構造に注目した MCMC 法に基づくシーン分割法”. 電子情報通信学会論文誌. D, 情報・システム, Vol. J97-D, No. 3, pp. 560–573, 2014.