ランダム妨害図形を用いた 画像ベースCAPTCHA方式の提案

田村 拓己[1]　菅井 文郎[1]　朴 美娘[2]　岡崎 直宣[1]

概要：近年，WEBサービスが急激に普及する中で，それらのWEBサービスに対してボットと呼ばれる自動プログラムを使用し，不正にサービスを利用するという悪質な行為が問題となっている．このような問題を防止するために，CAPTCHAと呼ばれる反転チューリングテストが広く利用されている．CAPTCHAはチャレンジ/レスポンス型テストの一種であり，人間には容易に解けるがコンピュータには正しい答えを導き出すことが困難な問題を出題し，回答の正否により，対象が人間であるか機械であるかを判別する．しかし，近年，CAPTCHAを自動的に突破する技術が発達し，その脆弱性が多くの研究者に指摘されている．例えば，文字列CAPTCHAにおいては，すでに高機能なOCR（自動文字認識）機能を備えるボットが出現している．そこで本論文では，画像ベースの新たなCAPTCHA方式を提案し評価する．本提案手法では，機械では実現することが難しい人特有の画像認識能力を利用し，高いユーザビリティと同時に，提示画像の中に答えとなる文字を全く表示しないことでOCR機能を利用するボットと人間の高い判別率を実現する．

A Proposal of the Image-based CAPTCHA Using Random Obstruction Figures

Takumi Tamura[1]　Fumio Sugai[1]　Mirang Park[2]　Naonobu Okazaki[1]

1. はじめに

近年，WEBサービスの普及により，誰でも様々なサービスを利用することが可能となっている．しかし，それらのWEBサービスに対してボットと呼ばれる自動プログラムを使用し，不正にサービスを利用するという悪質な行為が最近問題視されている．このような問題を防止するためには，人間とボットを識別する反転チューリングテストが必要となり，現在，CMUの研究者によって開発されたCAPTCHAと呼ばれる方式が広く利用されている[1]．CAPTCHAとはチャレンジ/レスポンス型テストの一種であり，対象者が人間であるか機械であるかを判別する．一般的に利用されている手法としては，歪曲やノイズが付加された文字列画像をWEBページに提示し，閲覧者がその文字を判読できるか否かを試すものがある（**図** 1）．

しかし，近年，CAPTCHAを自動的に突破する技術が発達し，その脆弱性が多くの研究者に指摘されている．例えば，文字列の判読能力を試すCAPTCHAにおいては，すでに高機能なOCR（自動文字読取）機能を備えるボットが出現している[2][3]．その対策として，文字列に加える変形やノイズを大きくすることによってボットを排除する確率を向上させることはできるが，そのような文字は人間にとっても認識が困難になるため，人間の正答率まで低下させてしまう．この問題に対し，画像や音声をベースにした，人間のより高度な知識処理を利用するCAPTCHA[4]も提案されているものの，一部の手法ではボットによる突破が可能であるという指摘もされている[5]．さらに，ボットの能力（CAPCTHA解読アルゴリズム，およびPCのCPUパワー）は，日々強化されている．したがって，高度な機能を有するボットに対して耐性をもつ，新たなCAPTCHAの導入が強く望まれる．ただし，CAPTCHAは，安全性とユーザビリティがトレードオフの関係になっていること

[1] 宮崎大学
University of Miyazaki
[2] 神奈川工科大学
Kanagawa Institute of Technology

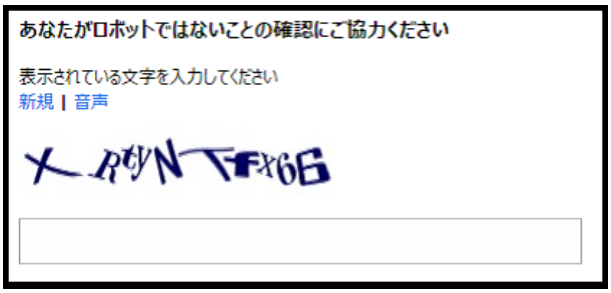

図 1 Microsoft 社のサイトで利用されている CAPTCHA（文字列 CAPTCHA）[6]

Fig. 1 CAPTCHA [6] used on Microsoft web site.

に留意しなければならない．

そこで本論文では，画像ベースの新たな CAPTCHA 方式を提案する．本提案手法では，人間の視覚補完を利用することと，画像を使用することでユーザビリティを確保しつつ，提示画像の中に答えとなる文字を全く用いないことで，OCR 機能を備えるボットの突破率を低下させる．また，ランダムで多数の種類の妨害図形を用いることと，使用画像を毎回インターネット上で検索し収集することでデータベースを用いた攻撃に対して耐性を持たせる．

2. 関連研究

2.1 CAPTCHA について

CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart：コンピュータと人間を区別する完全に自動化された公開チューリングテスト）は 2000 年にカーネギーメロン大学の Luis von Ahn, Manuel Blum, Nicholas Hopper, John Langford によって作られた．人間には容易に解くことが可能であるが，コンピュータには解くことが難しいものを出題し，正しい解答をした者を人間と判断する，チャレンジ/レスポンス型テストの一種である．

CAPTCHA では，人間と機械を区別するために，画像や音声，文字列などを用いる方式がある．次節から既存の CAPTCHA について紹介する．

2.2 文字列 CAPTCHA

現在，最も広く利用されている CAPTCHA は文字列 CAPTCHA である．文字列 CAPTCHA には Gimpy [7], EZ-Gimpy [7], r-Gimpy [8], reCAPTCHA [9][10] などの種類がある．

Gimpy は，2 つの単語が重複して印刷されているものを 1 セットとしたとき，ある画像の中にそれを 5 セット表示し，その 10 個の単語の中から 3 つを答えさせそれが正しければ解答者を人間と判別するものである．EZ-Gimpy 及び r-Gimpy は Gimpy を単純化したもので，1 つの単語，あるいはアルファベットと数字をランダムに並べた文字列

図 2 reCAPTCHA [9] による出題例

Fig. 2 Exsample of reCAPTCHA [9].

の画像を歪ませて表示し，その答えをテキストボックスに入力させ，解答が正しければ解答者を人間と判別する．

reCAPTCHA は，Web サイトの制限エリアへのアクセスを試みるボットからサイトを防御するために CAPTCHA を利用するのと同時に，その CAPTCHA に対する返答を紙の本のデジタル化に活かすシステムである．ユーザ側からみると従来の文字列 CAPTCHA と同じものを 2 つ 1 組で解くものになっている（**図 2**）．reCAPTCHA はニューヨーク・タイムズが持つ記事アーカイブの電子化，Google ブックスの書籍電子化に利用されている [11]．

reCAPTCHA では，スキャンされたテキストを 2 つの OCR プログラムで各々解析にかける．両プログラムの結果に相違が生じた場合，疑わしい文字を CAPTCHA に変換する．ただしこの時，すでに OCR で認識できている文字を制御文字としてこの CAPTCHA に添加して表示する．CAPTCHA をタイピングした人間が仮に制御文字を正しく認識していた場合，OCR で正確に読み取れなかった文字に対する CAPTCHA の解答も正しいものであるとシステムは仮定する．各 OCR プログラムにより文字認識に対しては 0.5 点を与え，人間の文字解釈に対しては 1.0 点が与えられる．ある文字認識が 2.5 点に一旦達した場合，スキャンされたテキストはこの文字認識であるとみなす．

reCAPTCHA では OCR で読み取れなかった (文字と認識できなかった) ものと読み取れたものを 2 つ 1 組のセットで使用するが，OCR が読み取れなかったものにはいろいろなものがあり，これらには人間でも解読が困難なものも含まれる．2 つの文字列のうち，どちらが OCR で読み取れて，どちらが読み取れていないかは，わからないように出題されるが，ヘブライ文字やアラビア文字，民族文字のように明らかに読み取りにくい記号が出てくる場合もある．その場合は，どちらが OCR で読み取れなかった文字かどうかは自明であり，その単語については，テキストボックスに何も入力しなくても認証することができる．

文字列 CAPTCHA のメリットとしては，システムとして単純であり，Web サイトに簡単に取り入れることが可能である点と，総当たり攻撃に高い耐性を持つ点が挙げられる．reCAPTCHA については，書籍電子化を同時に行うことができるというメリットもある．

これに対し，文字列 CAPTCHA のデメリットとしては，近年の OCR（自動文字認識）の性能向上により，ボット

でも簡単に文字を認識できるようになっていることが挙げられる．Gimpy，EZ-Gimpy では，まず，画像の中の文字をアルファベット 26 字と比較し，最も似ていると考えられる候補を 5 つほど選び出し，それらの組み合わせが単語になるかどうかを調べる．単語になったものを取り出し，その画像を歪め，最もよく元の画像と一致するスコアの単語を取り出すことによってこの CAPTCHA を破る．Mori らは，191 個の EZ-Gimpy に対して攻撃テストを行い，結果は 83 %の突破率であった [7]．reCAPTCHA も OCR に対しての耐性はないため，同様のデメリットがある．

2.3 画像 CAPTCHA

文字列 CAPTCHA と違い，画像 CAPTCHA は文字列を使用しないことでユーザビリティを向上させている．主な画像 CAPTCHA には，Asirra [4]，PIX [12]，4 コマ漫画 CAPTCHA [13] などがある．

ここでは例として Asirra を挙げる．Asirra は，人間とボットのイヌとネコを見分ける能力の違いに基づいている．まず利用者に 12 枚のイヌまたはネコの画像を提示する．そして，利用者はネコ画像を全て選択する．ネコの画像を正しく選択できれば，利用者を人間と判別する．

Asirra のメリットとして，イヌとネコの分類には専門的・文化的知識は必要とせず，人間は素早く正確に解くことができることが挙げられる．Elson らの 4717 枚の画像と 147 人の利用者を用いた実験では，人間は 98.5% の正確さでイヌとネコを見分けることができた．この場合，人間の利用者は 83.4% の正確さで，12 枚の画像を用いた Asirra を解くことができる．さらに，飼い主のいない動物の画像を用いることでそれらの動物の飼い主探しにつながるといった，他の利点もある．

デメリットとしては，テキストベースの CAPTCHA に比べて大きなスペースを使うことが挙げられる．また，近年，サポートベクターマシン（SVM）を用いた機械学習によって Asirra が破られたことが報告されている [5]．SVM はデータを 2 つのクラスに分離する超平面を作る教師つき学習方法である．分類手法には，色の特徴を用いた分類，テクスチャの特徴を用いた分類，2 つの特徴を組み合わせた分類の 3 種類がある．2 つの特徴を組み合わせた分類のとき突破率が一番高く，8000 枚の画像で学習し，2000 枚の画像で実験したとき 82.7% の正確さで分類することができた．Asirra のテストを解くためには 12 枚の画像を分類する必要があるため，一番精度の高い，2 つの特徴を組み合わせた分類手法で Asirra の突破を試みた場合，突破できる可能性は 10.3% である [5]．

2.4 動画 CAPTCHA

動画ベースの CAPTCHA は，基本的には文字列ベースの拡張方式と言える．NuCAPTCHA [14] やワンモア

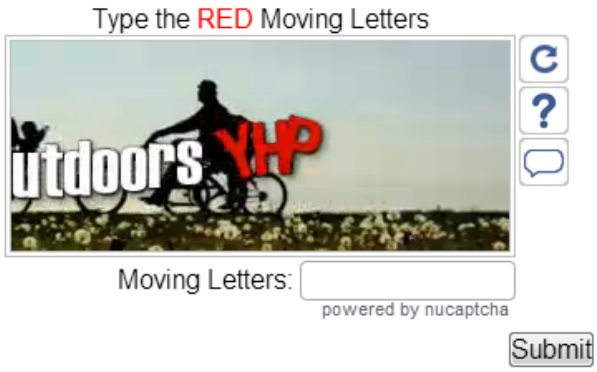

図 3 NuCAPTCHA の出題例 [14]
Fig. 3 Exsample of NuCAPTCHA [14].

CAPTCHA [15] などの種類がある．例えば, NuCAPTCHA は，近年難読化されている文字列 CAPTCHA によるユーザの苦痛をなくし、ユーザフレンドリな CAPTCHA を実現しようとしている（**図 3**）．NuCAPTCHA は，複数のフォントを用いたランダムな文字列が動画で表示され，ユーザは動画上部に表示される色指定などを読み取り，動画中に流れる文字列の中から該当文字列をテキストボックスに入力する．

動画 CAPTCHA のメリットとしては，動画を用いるため文字列 CAPTCHA より高いユーザビリティを実現できることが挙げられる．

デメリットとしては，文字列 CAPTCHA の拡張方式であるため，OCR を用いたボットに対する脆弱性が挙げられる．近年，NuCPTCHA を破るアルゴリズムも考案されている．NuCAPTCHA に対する攻撃手法 [16] は 5 段階の攻撃アルゴリズムを利用する．まず背景を取り除いて CAPTCHA を白黒化する．白黒化した CAPTCHA に対して，フレーム解析を行い，各フレーム内のオブジェクトを特定する．クロスフレーム解析とセグメンテーションを通じて CAPTCHA の文字を抜き出し，個々の文字を判別する．この行程は，市販のソフトウェアを使って実行できるといわれている．

3. 提案手法

本章では，3.1 で提案手法の目的を述べ，3.2 で満たすべき要件について説明し，3.3 で，提案手法に至る経緯と，実際に提案手法を用いて CAPTCHA 画像を生成する手順を紹介する．

以降，提案する CAPTCHA 方式を IC-CAPTCHA（Image-based Character input type CAPTCHA）と呼ぶ．

3.1 目的

既存手法では，文字列 CAPTCHA において，OCR 機能を持つボットに対する耐性の低さとユーザビリティの低さ，画像 CAPTCHA において，総当り攻撃に対する耐性の

低さとデータベース攻撃に対する耐性の低さが問題であった．従って提案手法では，画像 CAPTCHA におけるデータベース攻撃に対する耐性と総当たり攻撃に対する耐性に重点をおき，既存の文字列 CAPTCHA と比べて，OCR 機能を持つボットに対する耐性をもち，ユーザビリティに配慮した CAPTCHA を作成することを目的とする．

3.2 満たすべき要件

3.1 より，満たすべき要件を 2 つ挙げる．

(1) データベース攻撃に対する耐性

画像 CAPTCHA における脆弱性にデータベース攻撃がある．データベース攻撃には，攻撃者がデータベースを構築し，そのデータベースを利用して攻撃を行うものと，画像検索エンジンなどの Web 上のデータベースを用いて攻撃を行うものの 2 つの種類がある．そこで，本論文では，前者をデータベース攻撃，後者を画像検索攻撃と呼ぶ．

データベース攻撃というのは，問題画像とその解を記録したデータベースを構築し，このデータベースを用いて問題を解く方法である．これは，画像 CAPTCHA のシステムに使用される画像枚数が有限であることが原因となる．従って，データベース攻撃に対する耐性を持つ CAPTCHA を生成するためには，画像 CAPTCHA システム内で使用する画像枚数に，なるべく制限が無いようなシステムであることが望ましい．

画像検索攻撃とは，CAPTCHA の問題として提示された画像を Web 上の検索エンジンで検索することで，正答または正答に直結するキーワードを取得し，CAPTCHA を自動的に解くものである．画像検索攻撃に対する耐性については，問題として提示する画像を画像検索した際に，答えとなる名詞，または類似画像が判明しなければ良い．

(2) 総当たり攻撃に対する耐性

総当たり攻撃というのは，暗号や暗証番号などで理論的にありうる全てのパターンを入力し解読する暗号解読法である．画像ベース CAPTCHA においては，方式自体が並べ替え方式，クリック方式，種類の分別方式，など解答の組み合わせの最大数が少ないものが多い．これは，総当たり攻撃において脆弱であるといえる．画像ベースの CAPTCHA の場合，総当たり攻撃に対して，解答誤入力に回数制限をかける，解答時間に制限を設ける，などの対策を講じることを考慮しても，銀行 ATM に用いられている認証方式 PIN（1/10000）程度の強度を保つことが望ましいと考える．

3.3 IC-CAPTCHA システム

3.2 の要件を満たす新たな CAPTCHA の作成を考えた結果，できるだけ実用的であり，認証する際に時間がかからないものを目指した．CAPTCHA には文字ベースと画像ベースの大きく分けて 2 つのベースが存在するが，提案手法では画像ベースを選択した．CAPTCHA には動画ベースも存在するが，文字ベースの拡張方式であるとの考えから除外した．これは，OCR 機能を搭載したボットの能力は日々強力になっており，OCR ソフトの本来の使い道から考えても，これからもさらなる発展をすることが予想されるため，文字列を用いた CAPTCHA には，たとえ，時間制限などを用いたとしても限界があると考えたためである．

実用的な CAPTCHA を目指す中で，人間の視覚補完能力を生かすことはできないかと考えた．人間であれば，画像を見たときに少々欠損した画像であっても，その画像がなんの画像であるか判別が可能である．そこで，ある名詞の画像に妨害図形を上書きすることで，総当り攻撃や OCR ボットによる攻撃に耐性をもたせつつ，名詞の単語を入力するだけ，という実用的な CAPTCHA ができるのではないかと考えた．ただし，画像ベース CAPTCHA であるので，システム内の画像になるべく限界を持たせないようにするため，CAPTCHA で提示する元画像は Web 上より，画像検索を用いて取得することとした．

本論文で提案する IC-CAPTCHA システムは画像から容易に名詞を対応付けられる名詞群からなる名詞辞書と加工後画像のハッシュ値を登録したハッシュ辞典を持つものとする．以下に IC-CAPTCHA システムの画像生成手順を示す．

【IC-CAPTCHA システム画像生成手順】

Step1（名詞選択）: IC-CAPTCHA システムの持っている名詞辞書からランダムに 1 つの名詞を選ぶ．

Step2（画像取得）: その名詞，あるいは名詞に結びついている画像を検索エンジンを用いて検索し，その名詞に基づく画像を 1 枚取得する．

Step3（画像処理）: Step2 の画像に，妨害図形の上書きをし，背景処理（回転，モザイク，ぼかし，色反転等）の画像処理を施す．

Step4（面積比率比較）: Step3 の後の画像の妨害図形の妨害領域の面積比率を計算し，その値が閾値以内であるかを確認する．もし妨害領域の面積比率が閾値外の場合は，Step3 に戻り，妨害図形を上書きし直す．

Step5（ハッシュ検索）: Step4 の後の妨害図形の妨害領域が閾値以内であった画像のハッシュ値をとり，そのハッシュ値でハッシュ辞典を検索し，まだ登録されていなければハッシュ辞典に登録する．もし登録されている場合は，Step3 に戻り，妨害図形を上書きし直す．

Step6（画像提示）: ユーザに画像を提示する．

Step7（名詞入力）: ユーザは，画像から名詞を推測し，テキストボックスに名詞を入力する．

Step8（名詞比較）: IC-CAPTCHA システムは，Step1 で選んだ名詞とユーザの入力した名詞を比較し，マッチしたならば，ユーザを人間と認識し，認証する．マッ

チしなかった場合，2 回目までは Step5 へ戻る．3 回目は，Step1 へ戻り，名詞を変更する．

□

IC-CAPTCHA の画像生成手順のフローチャートを**図** 4 に示す.

3.4 IC-CAPTCHA システムの攻撃に対する耐性

総当り攻撃に対する耐性については，Step1 で使用する名詞辞書の単語登録数がそのまま総当たり攻撃に対する耐性になる．名詞辞書の単語登録数が少ないと総当たり攻撃に脆弱となってしまうが，他の方式と違い，画像の選び方や並べ方と関連しないため，名詞辞書の登録数を増やすことは比較的容易である．また，登録単語数を増加させることでユーザの負担が増えることはないため，ユーザビリティが低下する心配はない．さらに，Step8 において，1 つの提示画像に対する名詞入力を 3 回までとすることで，総当り攻撃に対する耐性を強化する．ただし，実用レベルでの使用を考えるならば，名詞辞書の登録数は，10000 語程度まで増やす必要がある．

また，Step2 では検索エンジンを用いて画像を毎回検索し，収集することでデータベース攻撃に耐性を持たせる．もし，同じ画像を加工することになったとしても，ランダムな妨害図形と背景処理を施すため，加工後に全く同じ画像になることは実用上ない．そのため，一度問題として提示された画像を用いて行うデータベース攻撃は成り立ちにくい.

Step5 では，ハッシュ検索を行い，全く同一な画像をユーザに提示しないようにする機能を強化している．ハッシュを用いると衝突が起こり，全く同一な画像でなくても生成画像を廃棄することがあると考えられるが，False Positeve であるので IC-CAPTCHA システム上は問題ない.

一方，画像検索攻撃に関しては，本提案手法では，元となる画像を画像検索を用いて取得するため，妨害図形が上書きされている提示画像を攻撃者が再度画像検索にかけることで，対象名詞が判明する可能性がある．そのため，本手法において，画像検索攻撃に対する耐性については評価が必要である．この件に関しては，5.2 節で述べる.

Step4 で，上書きする妨害図形について閾値を設け，生成される画像を篩に掛けることで，妨害図形が多すぎて人間であっても名詞が何であるか判らない，妨害図形が少なすぎて画像検索攻撃によって簡単に名詞が判明してしまう，という確率を下げる.

IC-CAPTCHA システムでは，画像内に答えと結びつく文字列は全く表示されないため，OCR 機能を持つボットに対しての耐性は考慮する必要はない.

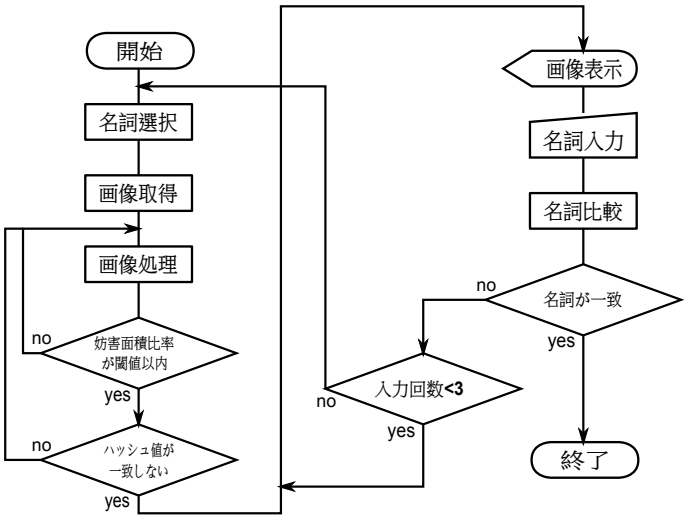

図 4 IC-CAPTCHA のフローチャート
Fig. 4 Flowchart of IC-CAPTCHA.

4. 実装

4.1 開発環境

開発言語は C++を，ライブラリは Open CV を用いて，仮想 PC 上の Ubuntu11.10 にて実装した.

4.2 実装プログラム

IC-CAPTCHA システムにおいては，どのような CAPTCHA 画像が生成されるかが，その安全性と利便性を決定付ける．そこで，本論文では IC-CAPTCHA 生成手順のうち，CAPTCHA 画像生成に必要な Step1（名詞選択），Step3（画像処理），Step6（画像提示），Step7（名詞入力），Step8（名詞比較）の部分を実装し，評価を行った.

Step2 の Web 検索を用いた画像収集では，検討していた Google 画像検索において自動プログラムを用いた使用に制限があったため，予め，素材となる複数の画像をそれぞれの名詞ごとに収集し，名詞ごとにフォルダを分別した．その名詞自体と，その名詞フォルダに何枚の画像が格納されているかを示したテキストファイルより辞書の読み込みを行った.

Step3 の実装プログラムの画像処理として，背景処理では，モザイク，ぼかし，色反転，画像回転を用い，上書きする妨害図形には，円，楕円・扇型，ポリゴン（多角形），文字を用いた．実際に実装したプログラムによる IC-CAPTCHA システムの生成画像は**図** 5 のようになる.

5. 評価

提案手法が既存手法のユーザビリティを改善し，画像 CAPTCHA の脆弱性であるデータベース攻撃に耐性を持つのか調査するため，実装した CAPTCHA 生成プログラムで生成した画像を用いてデータベース照合評価とユーザ

図 5 生成画像の例（りんご）
Fig. 5 Exsample of IC-CAPTCHA image.

表 1 妨害図形数アンケート結果
Table 1 Results of the questionnaire obstruct figures.

妨害図形数	4-7	8	9	10	11	12	13	14	15-20
人数	0	1	2	2	4	0	0	1	0

ビリティ評価を行った．また，2 つの評価を行うにあたって，生成画像のパラメータを調整する必要があったため，生成画像の妨害図形の個数に関する事前調査も同時に行った．

5.1 妨害図形数に関する事前調査

以前の結果 [17] から，画像検索攻撃に対する耐性に関しては，妨害図形の個数が関係していることがわかっている．しかし，人間の名詞の判別し易さと画像検索攻撃に対する耐性はトレードオフの関係となっており，妨害図形数を多くしすぎてしまってもいけないため，人間が判別しやすい最適妨害図形数についても調査を行う必要がある．そこで事前調査では，情報システム工学科の大学生 10 名に，IC-CAPTCHA システムの生成画像の妨害図形数に関してアンケートを行った．具体的には，ある名詞の画像について妨害図形の個数を 4 から 20 までに変えた画像をそれぞれ 10 枚ずつ作成し，名詞を判別可能である妨害図形の最大の個数について聞いた．その結果を表 1 に示す．

同表の結果より，人間が名詞判別をする際に許容できる妨害図形数の最大値の平均は 10.4 となる．そこで，以下では，妨害図形数を 10 として評価を行った．

5.2 画像検索評価

画像検索評価では，IC-CAPTCHA システムが画像検索攻撃に対する耐性をどの程度もつのかを評価することを目的とする．具体的な評価方法は，Google 画像検索を用いて，提案手法の生成画像を検索することで，元の名詞が推測されるか，類似画像として名詞の画像が検出されるかを調査した．

表 2 画像検索評価 画像枚数
Table 2 The number of images.

名詞数	10
名詞毎の画像枚数	30
合計画像枚数	300

表 3 画像検索評価結果
Table 3 Results of image search evaluation.

名詞	飛行機	りんご	バナナ	椅子	コップ	机	ライオン	みかん	鉛筆	靴	合計
判別数	6	1	4	0	0	0	23	0	0	0	34
判明率	11.3 %										

表 4 ユーザビリティアンケート項目
Table 4 The usability questionnaire item.

質問事項	印象語と評価点
解いていて楽しかったか？	楽しくない 1 点← →5 点 楽しい
解くことは面倒だったか？	面倒だ 1 点← →5 点 面倒ではない
解くことは簡単だったか？	難しい 1 点← →5 点 簡単だ
CAPTCHA が使いやすかったか？	使いにくい 1 点← →5 点 使いやすい
Web サービス上で使いたいか？	使いたくない 1 点← →5 点 使いたい

今回の画像検索評価に用いた名詞，画像の枚数を表 2 に，実際に Google 画像検索を用いて，生成画像を評価した結果を表 3 に示す．ここで，判明数とは画像検索の結果，推測名詞又は，類似画像から名詞が判明した画像の枚数を表す．

表 3 の評価から，名詞によって判明数が 0 から 23 と大きなばらつきがあった．

5.3 ユーザビリティ評価

ユーザビリティ評価では，提案手法 IC-CAPTCHA が，既存 CAPTCHA と比べて使いやすいものとなっているかを調査することをその目的とする．具体的な評価方法としては，情報システム工学科の大学生 10 名に，文字列 CAPTCHA [6] と画像 CAPTCHA（Asirra [4]），提案手法の IC-CAPTCHA を各手法 10 回ずつ解いてもらい，その後，アンケート調査を実施した．アンケート項目とその評価点を表 4 に示す．ここで，各項目において，肯定的であるほどその評価点が高くなる．アンケートの結果を表 5 に示す．同表は，各項目の評価点の平均値を評価値として表している．また，CAPTCHA を解いてもらう際に，CAPTCHA の解答までに要する時間とその正否を調査した．その結果は表 6 のようになった．

表 5 より，5 つの質問事項全てでその評価値が IC-CAPTCHA，画像 CAPTCHA，文字列 CAPTCHA の順に良かった．また，表 6 より，IC-CAPTCHA は 2 つの既存手法より正答率が高く，平均所要時間が短いことがわかる．したがって，IC-CAPTCHA は実際に使用する際のユーザビリティにおいて他の 2 つの手法に比べて優れているといえる．

表 5　ユーザビリティアンケート結果（評価値）
Table 5　The usability questionnaire results.

質問事項	IC-CAPTCHA（提案手法）	文字列 CAPTCHA	Asirra（画像 CAPTCHA）
解いていて楽しかったか？	4	1.8	3.9
解くことは面倒だったか？	4.9	1.5	3.3
解くことは簡単だったか？	4.9	2.5	4.4
CAPTCHA が使いやすかったか？	4.8	2.1	3.7
Web サービス上で使いたいか？	4.4	2.4	3.4

表 6　所要時間と正答率
Table 6　The required time and correct answer rate.

	正答率（%）	平均所要時間（*sec*）
IC-CAPTCHA 提案手法:妨害図形数 10	97%	6.03
文字列 CAPTCHA	75%	15.19
Asirra	95%	14.04

図 6　飛行機の特徴点
Fig. 6　The feature point in an airplane image.

6. 考察

画像検索評価から，300 枚の画像を画像検索にかけた結果，34 枚の画像で名詞が判明したという結果が得られた．5.2 の評価では，名詞によって判明数に大きなばらつきがみられた．これは，名詞によって特徴点の数と大きさが違い，特徴点が多い飛行機（図 6）や特徴点が大きいライオンなどの画像では特徴点をすべて妨害することができなかったため，判明数が多かったのだと考えられる．

表 3 の結果から，攻撃者から画像検索攻撃を受けた際，突破される確率は 11.3 %となる．同じ画像ベース CAPTCHA の Asirra において，SVM を用いた攻撃による突破率は 10.3 %であるため，ほぼ同程度であるといえる．しかしながら，画像検索攻撃は，検索エンジンを用いるだけの簡単な攻撃であり，提案手法にとって最も脅威となる攻撃と考えられるため，より精度の高い妨害図形の実現が必要である．

ユーザビリティアンケートから，既存の文字列 CAPTCHA，画像 CAPTCHA（Asirra）と比べて，提案手法の IC-CAPTCHA のほうが所要時間が短く，正答率が高いという結果と，使いやすさのアンケート調査で高いユーザビリティを有することを確認することができた．特に，所要時間では既存の CAPTCHA の半分以下の値となっており，実用的な CAPTCHA という要件は達成できていると考えられる．しかし，提案手法にも CAPTCHA テストに不合格であった場合が存在する．この中には，留学生による回答で，「みかん」の画像を提示した際，「lemon」という回答がなされた例などがある．このように，国や地域など個人の育ってきた環境により同じ画像に対応付ける名詞に違いがあるため，考慮が必要である．

提案手法では，画像を Web 上から取得するため，取得された画像が，適切な名詞の画像であるかどうかは検索システムの精度に依存する．また，画像内に人物が移りこんでいる場合も想定され肖像権などの問題も存在する．しかし，この問題については，顔やナンバープレートに自動的にモザイクをいれる技術を用いることで回避できると考えている．

7. まとめ

本論文では，既存の CAPTCHA 手法のデータベース攻撃に対する脆弱性，総当り攻撃に対する脆弱性，OCR ボットに対する脆弱性，ユーザビリティの低さという問題点を改善する新たな手法である IC-CAPTCHA の提案を行った．提案手法では，Web 上から画像を毎回取得することと，色・形が毎回ランダムな妨害図形を上書きすること，文字入力方式にすることによって，上記の問題の改善を目指した．また，画像検索評価とユーザビリティアンケートの 2 つの面から評価と考察を行い，IC-CAPTCHA システムの有効性を示した．

今後は，ハッシュ辞典検索を使用する上で検索時間の短縮を行うためにブルームフィルタを導入することや，名詞辞書の登録単語に階層的概念を用いてタグ付けを行うことで，正解名詞の判定をする方法について検討したい．

参考文献

[1] L. von Ahn, M. Blum, N. Hopper, and J. Langford, “CAPTCHA: Telling humans and computers apart,” Advances in Cryptology, Eurocrypt’03, vol.2656 of Lect. Notes Comput. Sci.,pp.294-311, 2003.

[2] J. Yan and A.S.E. Ahmad, “Breaking visual CAPTCHAs with native pattern recognition algotithms,” 2007 Computer Security Applications Conference, pp.279-291, 2007.

[3] K. Chellapilla and P.Y. Simard, “Using machine learning to break visual human interaction proofs（HIPs）,” Advances in Neural Infomation Processing Systems, vol.17, pp.265-272, 2005.

[4] Jeremy Elson, John Douceur, Jon Howell and Jared Saul,“Asirra: a CAPTCHA that exploits interest-aligned manual image categorization,” Proceedings of the 14th ACM conference on Computer and Communications Security, pp. 366-374, October 2007.

[5] P.Golle, “Machine learning attacks against the asirra CAPTCHA,” Proc. 15th ACM conference on Computer and Communications Security, pp.535-542, 2008.

[6] “Microsoft” アカウント
https://signup.live.com
[7] Greg Mori, Jitendra Malik, “Recognizing Objects in Adversarial Clutter:Breaking a Visual CAPTCHA,” cvpr,pp.134, 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR ’03) - Volume 1, 2003.
[8] Gabriel Moy, Nathan Jones, Curt Harkless, and Randall Potter, “Distorition Estimation Techniques in Solving Visual CAPTCHAs,” proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’04), 2004.
[9] “reCAPTCHA”
http://www.google.com/recaptcha
[10] L. von Ahn, B. Maurer, C.McMillen, D. Abraham, and M. Blum, “reCAPTCHA:Humen-based character recognition via Web security measures,” Sience, vol.321, no.5895, pp.1465-1468, 2008.
[11] “Google 会社情報”
http://www.google.co.jp/intl/ja/about/company/history/
[12] “PIX”
http://www.captcha.net/captchas/pix/
[13] 鈴木 徳一郎, 山本 匠, 西垣 正勝, “4 コマ漫画 CAPTCHA の検討”, 情報処理学会研究報告, IPSJ SIG Technical Report, Vol.2011-DPS-146 No.13, Vol.2011-CSEC-52 No.13, 2011-03-10.
[14] “NuCAPTCHA”
http://www.nucaptcha.com/
[15] 可児 潤也, 上松 晴信, 西垣 正勝, “ワンモア CAPTCHA の提案”, The Institute of Electronics, Information and Communication Engineers, The 29th Symposium on Cryptography and Information Security Kanazawa, Japan, Jan. 30-Feb. 2, 2012.
[16] “Yahoo Japan news”
http://headlines.yahoo.co.jp/hl?a=20120222-00000004-zdn_ep-secu
[17] 田村 拓己, 池田 匡視, 岡崎 直宣, “ランダム妨害図形を用いた画像ベース CAPTCHA の検討”, 火の国情報シンポジウム 2013, A-2-2, pp.1-6, 2013.