情報処理学会論文誌 Vol.56 No.3 808–818 (Mar. 2015)

文字認識攻撃に耐性を持つ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] 久保田 真一郎[1] 油田 健太郎[2] 片山 徹郎[1] 朴 美娘[3] 岡崎 直宣[1,a)]

受付日 2014年6月25日, 採録日 2014年12月3日

概要：ボットによるWebサービスの不正利用対策として，CAPTCHAと呼ばれる反転チューリングテストが利用されている．Webサイトへの導入のしやすさや回答方式の理解のしやすさから，文字列の画像を用いたCAPTCHA方式が広く普及している．しかし，ボットによる文字認識技術の発展が著しく，高い確率でテストが突破されるなど，その脆弱性が指摘されている．高度化するボットの文字認識技術に対抗し，解読難度を高くしたCAPTCHAや画像識別などの人間の高度な能力を利用するCAPTCHAが提案されているが，利便性が低いことや特定の攻撃に弱い点が問題となっている．本稿では，人間特有の画像認識能力を利用することで，利便性を保ち十分な堅牢性を持つ新たなCAPTCHA方式を提案する．提案手法は，判定に利用する提示画像に正答の文字列を含まないようにすることで文字認識攻撃に耐性を持たせた．また，提示画像には，人間が画像を補完して認識できる程度の妨害図形を付加し，堅牢性を向上させた．提案手法の有効性を確認するため，画像CAPTCHA方式において考えられる攻撃への耐性を考察し，利便性の評価としてアンケートによるユーザビリティ評価を行った．その結果，システム実装に必要な妨害図形の量に関する閾値を明らかにし，提案手法が攻撃に対して十分な耐性を持ち，ユーザビリティが優れていることを示した．

キーワード：画像CAPTCHA方式，ボット，妨害図形

A Proposal of an Image-based CAPTCHA Using Random Obstruction Figures to Absorb OCR-based Bot-attacks

Takumi Tamura[1] Shin-ichiro Kubota[1] Kentaro Aburada[2] Tetsuro Katayama[1]
Mirang Park[3] Naonobu Okazaki[1,a)]

Received: June 25, 2014, Accepted: December 3, 2014

Abstract: A reversal turing test called CAPTCHA is used in many webservice sites to prevent the automatic program called bots from making unauthorized accounts. The CAPTCHA with images of correct answer string, called as the text-based CAPTCHA, is widely prevalent because of an ease implementing in the website. The optical character recognition technologies enable bots solve the text-based CAPTCHA automatically. Any researchers have pointed out the vulnerability of the text-based CAPTCHA. Absorbing the vulnerability of the text-based CAPTCHA, the image-based CAPTCHA is proposed, which use the human abilities to discern objects in images. However, the existing image-based CAPTCHAs also have problems about usability and robustness. In this paper, we propose a new image-based CAPTCHA using images without a correct answer string and with obstruction figures, to achieve high usability and robustness. In order to confirm a effectiveness of the proposed method, we argue to absorb some considerable attacks in the image-based CAPTCHA, and conduct assessment of usability through our questionnaire. The results show that the proposed system absorb the attacks adequately and has usability.

Keywords: image-based CAPTCHA, bot, obstruction figures

[1] 宮崎大学
University of Miyazaki, Miyazaki 889–2192, Japan
[2] 大分工業高等専門学校
Oita National College of Technology, Oita 870–0152, Japan
[3] 神奈川工科大学
Kanagawa Institute of Technology, Atsugi, Kanagawa 243–0292, Japan
[a)] oka@cs.miyazaki-u.ac.jp

1. はじめに

Webサービスの普及により，誰でも様々なWebサービスを利用することが可能となっている．それらのWebサービスに対してボットが不正なアカウントを取得する不正行為があり，その対策として，CMU（Carnegie Mel-

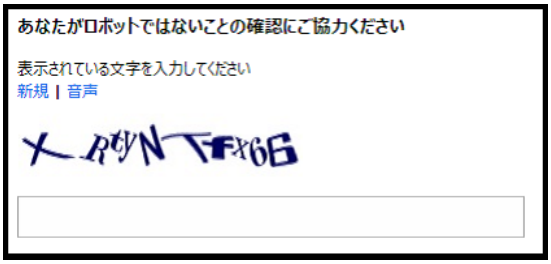


図 1 Microsoft 社のサイトで利用されている CAPTCHA（文字列 CAPTCHA）[6]
Fig. 1 CAPTCHA [6] used on Microsoft Web site.

lon University）の研究者によって開発された CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart）と呼ばれる人間とボットを識別する反転チューリングテストによる判別手法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，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**）．

この CAPTCHA を自動的に突破する技術が発達し，人間の文字列判読能力を試す CAPTCHA に対して，OCR（Optical Character Recognition）機能を備えるボットによる攻撃（OCR 攻撃）が存在する [2], [3]．OCR 攻撃への対策として，文字列に加える変形やノイズを強くする対策がとられるが，変形やノイズの大きい文字は人間も認識が困難であり，人間による正答率も低下する．また別の対策として，動物や物などの画像を識別する人間の高度な能力を利用する CAPTCHA [4] が提案されているが，この CAPTCHA 手法も脆弱であることが文献 [5] に述べられている．したがって，高度な機能を有するボットに対して耐性を持つ，新たな CAPTCHA の導入が強く望まれる．

2. 関連研究

CAPTCHA には，人間と機械を識別するために，文字列画像や具体物の画像，あるいはそれらを併用した方式がある．この章では既存の CAPTCHA のメリットとデメリットについてまとめ，我々の研究において解決すべき問題点を明らかにする．

2.1 文字列 CAPTCHA 方式

現在，最も広く利用されている CAPTCHA は文字列 CAPTCHA 方式で，文字列画像の読解能力を用いて人間と機械の識別を行うものである．文字列 CAPTCHA 方式には Gimpy [7], EZ-Gimpy [7], r-Gimpy [8], reCAPTCHA [9] などがある．

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，画像の中にそれを 5 セット表示する表示された 10 個の単語の中から 3 つを答えさせる CAPTCHA である．文字列 CAPTCHA 方式として最も頻繁に使用される EZ-Gimpy および 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る CAPTCHA である．reCAPTCHA は，新聞紙の記事や本などの電子書籍化を行う際に OCR ソフトウェアが読み取れなかった文字画像を認証手順の一部に導入し，人間に解読させ電子書籍化と CAPTCHA の両方に利用する取り組みである．

表 1 入力文字数が 4 と 10 の場合の文字列画像のパターン数
Table 1 Numbers of images in cases of which numbers of input strings is 4 and 10.

文字数	4	10
総当たり数	1.48×10^7	8.39×10^{17}

文字列 CAPTCHA 方式のメリットは，システムが単純であり，Web システムへの導入が簡単である点と，総当たり攻撃に高い耐性を持つ点である．英字 52 字（大文字小文字を含む）と数字 10 字の合計 62 字の半角英数字が用いられる場合，判定のために求める文字数を a とすると，CAPTCHA に使用される文字列画像のパターン数は 62^a 通りである．判定のために求める文字数が 4 と 10 の場合の CAPTCHA に使用される文字列画像のパターン数を**表 1** に示す．

文字列 CAPTCHA 方式のデメリットは，OCR 攻撃への耐性が低い点である．Mori らの研究 [7] によると，OCR 機能を用いた突破テストで，191 個の EZ-Gimpy に対して攻撃テストを行い，83%の突破率であったことが報告されている．

文字列 CAPTCHA 方式の弱点である OCR 攻撃に対する耐性は，CAPTCHA の提示する文字列画像そのものが正答の文字列を含むことが原因であり，これを解決するためには正答の文字列が直接含まれない画像を用いる対策が有効である．

2.2 画像 CAPTCHA 方式

画像 CAPTCHA 方式は，具体物の画像を用いることで人間と機械を判別する．出題する問題の種類は様々なものがあり，用いる画像の枚数や回答方式の違いがある．主な画像 CAPTCHA 方式には，Asirra [4]，4 コマ漫画 CAPTCHA [10]，What's Up CAPTCHA [11]，Cortcha Challenge [12]，MULTI-MODAL CAPTCHA [13]，Image-Text Fusion CAPTCHA [14] などがある．画像を用いた問題を出題するものには画像を用いた個人認証として，複数の画像からユーザが特定の画像を選択するなぞなぞ認証 [15] や画像記憶のスキーマを利用したユーザ認証システム [16]，Use Your Illusion [17] などがあるが，ユーザが 1 度画像を見ている，あるいはユーザ自身が画像を答えとして選択す

るなど，画像記憶を用いているため，画像 CAPTCHA 方式に用いる問題よりも難しく設定することができる点で異なっている．

Asirra は，イヌとネコを見分ける人間の能力を利用してボットと人間を判別する．ユーザは提示された 12 枚のイヌまたはネコの画像のうち，ネコの画像をすべて選択することを要求され，正しくネコの画像を選択できた場合，人間と判別される．4 コマ漫画 CAPTCHA は，提示された 4 枚の画像から 4 コマ漫画となるよう順序を並べ替えることを要求され，正しく並べ替えることができた場合，人間と判別される．What's Up CAPTCHA は，提示された画像を適切な角度に回転させることを要求され，正しく回転させることができた場合，人間と判別される．Cortcha Challenge は，提示された複数のオブジェクトと画像から適切なオブジェクトを選択し，そのオブジェクトを画像の適切な位置に動かすことを要求され，正しくオブジェクトを選択し，移動することができた場合，人間と判別される．上記の画像 CAPTCHA 方式は，CAPTCHA の回答の数が限られており，誤って CAPTCHA の判定テストを通過する確率が高いといえる．

MULTI-MODAL CAPTCHA は，ある物体の画像上に答えとなる文字列のタグを複数上書きし，その中から物体の画像として正しいタグを選択し，テキストボックスへ文字列を入力することで人間と判断する．Image-Text Fusion CAPTCHA は，ヒントとなる文字列が上書きされた画像をユーザに提示し，正しい回答をすることで人間と判別される．上記の画像 CAPTCHA 方式は，文字列 CAPTCHA 方式と画像 CAPTCHA 方式の併用方式であるが，正答や正答と直結する文字列が画像内に存在するため，OCR 攻撃に耐性を持つとはいいきれない．

文字列を含まない画像による画像 CAPTCHA 方式のメリットは，ボットの OCR 機能に対して強い耐性を持つ点があげられる．また，人間は直感的な画像認識を行うことができ，文字列 CAPTCHA 方式に比べて所要時間を削減できると考えられる．画像を複数枚用いる CAPTCHA については所要時間を削減できず，ユーザビリティを損ねる場合がある．

デメリットは，誤って CAPTCHA の判定テストを通過する確率（偽陽率）が高い点である．たとえば，1 回の CAPTCHA 画像を 12 枚，そのうち選択すべき正答の画像が a 枚である場合，偽陽率は式 (1) となる．

$$\frac{1}{{}_{12}C_a} \tag{1}$$

正答画像の枚数 a が明らかでない場合，攻撃者は正答画像の枚数 a を知らないため，1/4,095 [*1] の確率で誤って判別テストを通過する可能性がある．この確率は表 1 にある文字数 4 つの場合と比較して非常に高く，画像 CAPTCHA 方式の偽陽率が，文字列 CAPTCHA 方式に比べて高いことが分かる．画像 CAPTCHA 方式において，偽陽率を下げるためには，表示画像枚数を増やす方法が考えられるが，大きな表示スペースが必要となり，各画像の一覧性が悪くなる．

画像 CAPTCHA 方式に対する攻撃としてデータベース攻撃，画像検索攻撃，機械学習を用いた攻撃（機械学習攻撃）が考えられる．

データベース攻撃とは，問題画像とその解を記録したデータベースをあらかじめ攻撃者が構築し，構築したデータベースを用いて CAPTCHA を自動的に通過する方法である．これは画像 CAPTCHA 方式で提示される画像が使いまわされたり，入手の容易な画像集などを用いることが原因となる．

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 を自動的に通過する手法である．

機械学習攻撃とは，サポートベクタマシン（SVM）などに画像の特徴をあらかじめ学習させておき，CAPTCHA で提示される画像を学習した特徴情報をもとに判別し，CAPTCHA を自動的に解くものである．文献 [5] によると SVM を用いた機械学習により，10.3%の確率で Asirra による判別テストが破られたと報告されている．

画像 CAPTCHA 方式では偽陽率が高いため，画像 CAPTCHA 方式の OCR 攻撃耐性を保ちつつ文字列 CAPTCHA 方式の文字入力による堅牢性が必要と考える．機械学習を利用した攻撃への耐性強化として画像データベースから選ばれる提示画像にランダムな妨害図形を描くという対策をとる．データベース攻撃に対する脆弱性に対して，画像 CAPTCHA 方式で提示する画像を繰り返し使用せず，容易に入手可能な画像集を利用しないことが必要である．画像検索攻撃に対する脆弱性に対しては，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いか確認する必要がある．所要時間とユーザビリティを考慮すると，出題問題の中で用いる画像枚数を 1 枚とするのが望ましい．

2.3 動画 CAPTCHA 方式

動画ベースの CAPTCHA 方式は，文字列方式や画像方式の拡張方式となっており，NuCAPTCHA [18] やアモーダル補完を利用した動画 CAPTCHA [19]，ワンモア CAPTCHA [20] などがある．文字列 CAPTCHA 方式を拡張した方式である 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

[*1] $\dfrac{1}{\sum_{a=1}^{12} {}_{12}C_a} = \dfrac{1}{4{,}095}$

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．アモーダル補完を利用した動画 CAPTCHA は，円画像を上書きした文字列画像を用いた動画 CAPTCHA で，欠損した文字であっても視覚補完し，認識できる人間の高度な能力を利用している．

動画 CAPTCHA のメリットは，動画を用いることにより文字列の色の変化や文字列の動きなど他の要素を追加することが可能となり，従来の文字列 CAPTCHA より問題の文字数を少なくすることができる．

デメリットは，動画があまりにも長い場合，ユーザは文字列動画を再生する時間と判読した文字列を入力する間，CAPTCHA に拘束されるため，利便性が低下する．動画 CAPTCHA 方式は，動画再生のための時間が必要となり利便性が低下するため我々は採用しない．

動画 CAPTCHA 方式のデメリットにあるように，CAPTCHA による判定テストを行う時間がユーザビリティに影響すると考えられる．我々はユーザビリティを重視し，CAPTCHA による判定テストの脆弱性対策だけではなく，CAPTCHA による判定テストの回答に必要とする所要時間も十分に検討しなければならないと考える．

3. 提案手法

現在の CAPTCHA 方式のメリットとデメリットを整理した結果を**表 2** に示す．

文字列 CAPTCHA 方式は OCR 攻撃に弱いが，画像 CAPTCHA 方式は OCR 攻撃に耐性を持ち，文字列 CAPTCHA 方式は偽陽率は十分低いが，画像 CAPTCHA 方式は偽陽率が高いというそれぞれにトレードオフの関係にある（表 2）．文字列 CAPTCHA 方式と画像 CAPTCHA 方式とが相互に弱点を補うよう，提示する画像に正答の文字列を含まず，文字列 CAPTCHA 方式のように文字列を入力する CAPTCHA 方式が有効と考えられる．つまり，ある物体の画像 1 枚を提示し物体の名詞の文字列を入力する CAPTCHA 方式を考える．ある名詞に結び付けられた加工を施していない画像を以降，物体画像という．

提案手法では，表示する画像が 1 枚なので画像表示スペースを省力化できる．また，提示する画像に正答の文字列が含まれないため OCR 攻撃に耐性を持つ．名詞を文字入力して判定するので偽陽率は低い．

物体画像を用いた画像 CAPTCHA 方式では，画像の特徴量が明らかなため画像検索攻撃や機械学習攻撃に対して脆弱である．そこで画像の特徴量を変化させるために物体画像に妨害図形を毎回ランダムに上から描くという対策をとる．これは人間であれば少々欠損した画像を見て何の画像であるか判別できるが，ボットには判別できない点を利用している．画像を使用した個人認証方法の文献 [16], [17] や画像の回転を用いた CAPTCHA の文献 [11] から，画像自体にぼかしやモザイク，回転を用いることもボットに対して有効であると考えられる．さらに，妨害図形が描かれた物体画像（以降，生成画像という）を画像検索により正答の名詞と一致しないかチェックすることで，画像検索攻撃に対する耐性を持たせる．

データベース攻撃に耐性を持つ CAPTCHA 方式とするために提示する物体画像をできるだけ豊富に準備し，1 度提示した画像を 2 度と提示しない方法とする．

動画 CAPTCHA 方式にあった CAPTCHA の判定テストに回答する所要時間については，実装後のユーザビリティ評価の項目に回答する所要時間を加え，提案手法が十分な機能を持つことを検証する必要がある．

以上により，我々の提案手法は，物体画像にランダムに妨害図形が描かれた画像をユーザに提示し物体の名詞文字列をユーザがキー入力する CAPTCHA 方式である．本提案手法では，妨害図形を含む画像を用いることで高度な知識処理が必要な人間の視覚補完を利用している．画像を理解したユーザがその画像の名詞を文字入力することでユーザビリティを確保し，提示画像の中に答えとなる文字が含まれないため，OCR 攻撃に対する耐性を持つ．また，画像に対してランダムで多種類の妨害図形を用い，使用画像をインターネット上で検索し収集することで画像データベースを用いた攻撃に対して耐性を持たせる．

以降，この提案する CAPTCHA 方式を IC-CAPTCHA（Imaged-based Character input type CAPTCHA）方式と呼ぶ．

次節では，この IC-CAPTCHA 方式を実装するためのシステムについて記述する．

3.1 IC-CAPTCHA システム

本稿で提案する 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ブルームフィルタを持つもの

表 2 CAPTCHA 方式の問題点
Table 2 Problems of CAPTCHA.

	文字列	画像	動画
メリット	偶然に判定テストを通過する確率が低い	OCR 攻撃に対する耐性がある	問題文字数を少なくできる
デメリット	OCR 攻撃に対する耐性がない	偶然に判定テストを通過する確率が高い 複数枚画像を用いると画像の一覧性が悪い	動画再生のための時間が必要
考えるべき方策	OCR 攻撃耐性の向上	偶然に判定テストを通過する確率を下げる	CAPTCHA に必要な所要時間の短縮

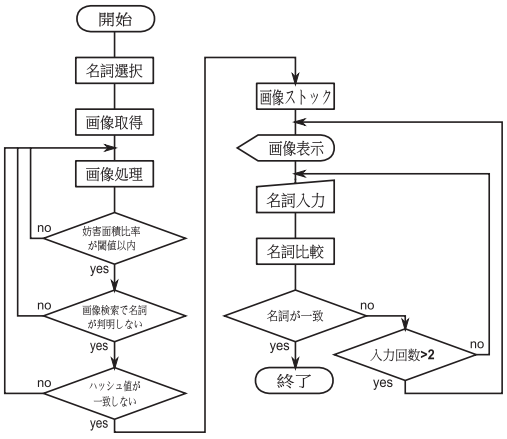


図 2 IC-CAPTCHA のフローチャート
Fig. 2 A flowchart of the IC-CAPTCHA.

とする．以下に IC-CAPTCHA システムの画像生成手順を示す．また，そのフローチャート図を**図 2** に示す．

【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）：Step1 で選ばれた名詞，あるいは名詞に結び付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（物体画像）を 1 枚取得する．

Step3（画像処理）：Step2 の物体画像に，妨害図形（ランダムな色やグラデーション，模様を用いた円，楕円・扇型，ポリゴン（多角形）など）を上書きし，画像処理（回転，モザイク，ぼかし，色反転など）を施す（生成画像）．

Step4（妨害面積比率チェック）：Step3 で生成される生成画像全体に対する妨害領域の面積比率（妨害面積比率）を計算し，計算した妨害面積比率が設定する閾値の範囲以内であるかを確認する．もし妨害面積比率が設定する閾値の範囲に収まらない場合は，Step3 に戻り，再度画像処理を行う．

Step5（画像検索チェック）：画像検索サイトを用い，Step3 の生成画像を入力値として画像検索を行った結果，その検索結果と正解名詞が一致しないかをチェックする．

Step6（ブルームフィルタチェック）：生成画像のハッシュ値をとり，そのハッシュ値でブルームフィルタを検索し，まだ登録されていなければブルームフィルタに登録する．もし登録されている場合は，Step3 に戻り，再度画像処理を行う．

Step7（画像ストック）：Step4，5，6 のチェックを通過した画像（提示画像）を Step1 で選んだ名詞と結び付けて，画像ストックへ保存する．

Step8（画像提示）：アクセス・認証が必要なとき，画像ストックから提示画像をランダムに選択し，ユーザに提示する．

Step9（名詞入力）：ユーザは，提示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．

Step10（名詞比較）：IC-CAPTCHA システムは，提示画像に結び付けられている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，認証したのち，提示画像を破棄する．マッチしなかった場合，k（繰返し入力許容回数）回目までは Step9 へ戻る．$k+1$ 回目は，Step8 へ戻り画像を変更し，1 度使用した提示画像は破棄する．

□

ここで，生成画像とは，物体画像の上に妨害図形を描き，モザイクなどの画像処理を施した後の画像である．提示画像とは，生成画像のうち，3.1 節で説明する提案システム内の 3 つのチェックを通過し，実際にユーザに提示される画像である．

3.2 名詞辞書

提案手法における名詞辞書の登録単語数は，偶然に認証を突破する確率とユーザの正解率に直結する．登録単語は，名詞であればよいわけではなく，具体物の画像が存在し，またユーザがその名称を一意に認識できるものでなくてはならない．以下に名詞辞書を構成しうる単語の要件を述べる．

(1) 名詞であること
(2) 名詞から具体物の画像が得られること

名詞辞書の作成については，WordNet [21] における名詞に属する単語の中で，単語説明の画像欄に画像が存在するものを自動的に登録することで登録単語を確保することを想定しているが，検証が必要である．

上記の要件で辞書作成を行うと，たとえば「ネーブル」，「はっさく」，「いよかん」など，一般人には差異の認識が難しい単語も辞書に含まれるため，人間による認証の正答率は格段に下がってしまうことが予想される．そこで，上記の要件で辞書作成を行った後，実装システムを運用するうえで，認証の正答率が低い単語を名詞辞書から排除する対策が必要となる．

3.3 実装

開発言語は C++を，画像処理ライブラリは Open CV を用い，仮想 PC 上の Ubuntu11.10 で画像生成プログラムを実装した．IC-CAPTCHA システムでは，どのような CAPTCHA 画像が生成されるかによりシステムの安全性と利便性が決まる．そこで，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），Step8（画像提示），Step9（名詞入力），Step10（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

図 3 生成画像の例（りんご）
Fig. 3 An example of an IC-CAPTCHA image (apple).

Google 画像検索に自動プログラムを用いた使用に対して制限があったため，素材となる複数の物体画像をそれぞれの名詞ごとにあらかじめ収集した．

Step3 の実装プログラムの画像処理では，モザイク，ぼかし，色反転，画像回転を用い，物体画像の上に描く妨害図形に，円，楕円・扇型，ポリゴン（多角形），文字を用いた．妨害図形の種類は，srandom 関数によりランダムに選択され，物体画像内のランダムな位置に描かれる．また，妨害図形どうしが重ならないよう一定比の距離をとる制約を設けたうえで位置を調整する．実装したプログラムによる IC-CAPTCHA システムの生成画像を図 3 に示す．

4. 評価と考察

まず静的な評価を行ったうえで，調査項目を整理し，必要な動的評価を行う．静的評価では，考えられる攻撃に対する耐性についての評価を行う．動的評価では，提案手法における画像検索チェックの廃棄率を調査するため，実際の生成画像を用いて Web 上の画像検索を行い，評価を行った．提案手法が既存手法のユーザビリティを改善していることを確認するため，実装した CAPTCHA 実装プログラムで作成した生成画像を用いてユーザビリティ評価を行った．また，2 つの動的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に関する妨害面積比率評価を同時に行った．

4.1 攻撃に対する耐性の評価

（1）OCR 攻撃

IC-CAPTCHA システムでは，提示画像内にノイズとして文字を上書きする場合はあるが，画像内に答えと結び付く文字列はまったく表示されない．そのため，OCR 機能を持つボットがその文字を識別できたとしても CAPTCHA を突破することはできないため，OCR 攻撃に対して十分耐性を持つ．

（2）辞書を利用した brute-force 攻撃

回答方式に物体画像の名詞をキー入力する IC-CAPTCHA システムでは，名詞辞書を利用した brute-force 攻撃が考えられる．ここでは，攻撃者が実装システムの名詞辞書を何らかの方法で入手あるいは作成し brute-force 攻撃を行う場合を考える．Step1 で使用する名詞辞書の登録単語数が多ければ多いほど，辞書を利用した brute-force 攻撃に対する耐性は強化される．たとえば，CAPTCHA の推奨強度 [4] を目指すならばシステムが保有する名詞辞書の登録単語数は 4,096 語程度が求められ，携帯端末向けの個人認証における偶然認証程度の強度 [22] を目指すならば 16,000 語程度の登録単語数が求められる．辞書を利用した brute-force 攻撃に対する耐性を強化するため，IC-CAPTCHA システムでは，Step10 において 1 つの提示画像に対する名詞文字列の入力を 3 回までと制限している．

現在の IC-CAPTCHA システムで，辞書を利用した brute-force 攻撃に対する耐性を CAPTCHA 推奨強度（1/4,096）まで高めるには，名詞辞書の登録単語数を 4,096 以上にしなければならない．WordNet の登録単語数は約 93,834 語以上で，WordNet に登録された名詞をもとに，3.2 節の名詞辞書の要件を満たし，4,096 語以上を収録する名詞辞書を構成できる可能性はあるが，人間が画像を見て一意に対象物の名詞を認識できる単語に絞られることもあり 4,096 語を確保できないことが懸念される．名詞辞書の登録単語数が 4,096 より小さくなる場合には，CAPTCHA の推奨強度を超える対策が必要である．たとえば，名詞辞書をもとに提示画像を 2 つ提示する対策が考えられる．提示画像を 2 つ提示し，2 つの名詞を答える CAPTCHA の場合，CAPTCHA の推奨強度を超えるために必要な名詞辞書の必要登録単語数は 64 語以上となる．幼児学習用の単語とその画像を収録したアプリの名詞辞書の登録単語数が 100 語以上 [23] であり，WordNet を利用して十分な名詞辞書を構築できなかった場合には，64 語以上の名詞辞書を用い提示画像を 2 つ提示する対策が可能と考えられる．

（3）データベース攻撃

もし，データベース攻撃側の持つ物体画像があったとしても，ランダムな妨害図形と画像処理を施すため，加工後にまったく同じ生成画像になることは実用上ない．また，1 度提示した画像は破棄され，Step6 でブルームフィルタチェックを行うため，データベース攻撃側が保持する画像と提示画像が一致することはない．以上のことから，データベース攻撃は成り立たない．

（4）画像検索攻撃

画像検索攻撃に関しては，Step5 で画像検索チェックをすることで，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たとしても正解名詞が判明しないようにしている．しかしながら，画像検索チェックを行うことで，IC-CAPTCHA システムでは妨害図形を上書きした生

成画像の廃棄を行うことになる．このため，画像検索チェックを行うことでどれほどの画像の廃棄率が発生するかは検証が必要である．このことについては 4.3 節で述べる．

（5）機械学習攻撃

機械学習攻撃とは，画像 CAPTCHA の Asirra に対して有効な攻撃で，SVM を用いて行われる．攻撃者は，色情報やテクスチャ情報に基いて正しくラベル付けされた一定の枚数の画像を取得し，2 つのクラスに分類するように機械を訓練した後，それを用いて実際の CAPTCHA を解かせる．この攻撃は，Asirra のように少ない種類の画像しか表示されない場合には有効な方法となりうる．一方，提案手法では，表示される画像の種類が非常に多く，機械学習が実質的に困難であるため，適用が難しいと考えられる．

（6）画像差分攻撃

差分攻撃とは，提案手法における提示画像のうち元画像が同じものを取得し，妨害図形を上書きしていない画像を生成し，画像データベースを作ることで IC-CAPTCHA を突破する攻撃である．しかしながら，妨害図形の上書きしていない物体画像を生成するためには，手作業で同じ物体画像の提示画像を複数取得することが必要となるため，システム内の名詞辞書の登録単語数が多い場合には，画像データベースの作成に多大な労力と時間がかかる．その労力を考えると，上記の既存の Web 上の画像データベースを用いる画像検索攻撃の方が効率的な攻撃を行えるため，攻撃者がこの攻撃方法を行うとは考えにくい．また，そのようなコストをかけてこの攻撃方法を用いたとしても，攻撃者はコストに見合うだけの利益をあげることができないため，この攻撃は現実的ではない．よって，提案手法では，差分攻撃は特に考慮しないものとする．

4.2 妨害面積比率の評価

人間が提示画像から名詞を判別する際，どの程度の妨害面積が許容されるかについて調査するため，妨害面積比率について評価する．妨害面積比率とは，生成画像全体に対する妨害領域の面積比率である．

妨害面積比率の評価では，宮崎大学工学部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，ある名詞の物体画像について妨害図形（円・楕円・扇型・多角形・文字）の個数を 4 から 20 までに変えた生成画像をそれぞれ 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．本調査の結果を**表 3** に示す．同表より，被験者ら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中央値は 10.5 となる．そこで，以下の動的評価では，妨害図形数を 10 として評価を行った．また，妨害図形数 10 と 11 のときの画像 20 枚の妨害面積比率の平均値は 0.304（SD = 0.075）であった．この値が妨害面積比率チェックの閾値の目安となる．

表 3 妨害図形数アンケート結果

Table 3 Results of the survey about a number of the 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

4.3 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チェックを行う際に，どれほどの廃棄画像を出すのかを評価することを目的とする．

評価方法は，Google 画像検索 [24] 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．以下に調査手順を示す．

(a) 適当に選択した 10 個の名詞ごとにそれぞれ 3 枚の物体画像を Web 上の画像検索よりランダムに取得する．
(b) 3 枚の物体画像それぞれに対して，生成画像を 10 枚ずつ作成する．
(c) Google 画像検索を用いて，作成した生成画像を 1 枚ずつ手作業で検索にかけ，判明条件に従って判明した画像の枚数を数える．

今回の調査に用いた名詞および画像枚数を**表 4** に示す．Google 画像検索の検索結果には「この画像の最良の推測結果」として入力した検索キーの画像ファイルから推測される語句が返され，「類推する画像」として入力した検索キーの画像ファイルから類推される画像の一覧が出力される．Google 検索により判明したか否かを議論するために，正答の名詞が判明したと判断する条件を規定したうえで以降の議論を進める．以下に Google 画像検索により判明したと判定する条件を示す．これらの条件が満たされる場合に，判明したと判断する．

- 「この画像の最良の推測結果」に正解名詞が表示される．
- 「類似する画像」の中に，正解名詞の画像が過半数以上表示される．

Google 画像検索を用いて調査手順 (b) で生成した画像を検索し評価した結果を**表 5** に示す．ここで，判明数とは調査手順 (b) で生成した 300 枚のうち判明条件に適合した画像の枚数を表す．表 5 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．ここで判明と判断された画像は画像生成手順の Step5 の手続きにおいて廃

表 4 画像検索評価画像枚数

Table 4 Numbers of images for the survey about image search evaluation.

名詞数	10
名詞ごとの物体画像枚数	30
合計画像枚数	300

表 5 画像検索評価結果
Table 5 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
排除率	11.3%										

棄される．また，表 5 における排除率とは，生成画像のうち廃棄される画像の出現する確率を表す．

4.4 ユーザビリティ評価

ユーザビリティ評価では，文献 [25] を参考に，CAPTCHA の正答率や満足度，解きやすさ，覚えやすさ，回答に要する所要時間から，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．比較する既存 CAPTCHA としては，それぞれの種類の CAPTCHA の中で最も使用されている文字列 CAPTCHA の Gimpy-r [6] と画像 CAPTCHA の Asirra [4] を用いた．

ユーザビリティ評価は，情報関連の学科・専攻の大学生および大学院生 14 名を対象として行った．内訳は，女性 8 名，男性 6 名で，日本人 11 名，留学生 3 名とした．

Gimpy-r と Asirra の CAPTCHA についての説明を行い，被験者に Gimpy-r と Asirra，IC-CAPTCHA を慣れるまで数回問題を回答してもらった後，Gimpy-r と Asirra，IC-CAPTCHA の順で各手法を 10 回ずつ回答してもらい，その後，アンケート調査を実施した．Gimpy-r は，Windows 7 で問題画像をあらかじめ収集しておき，Windows フォトビューアを用いて被験者に問題画像を提示し，メモ帳に回答を入力する方式とした．Asirra は，Windows 7 上の Asirra の Web サイトを使用し，サイト内で問題画像を選択し，回答ボタンをクリックする方式とした．IC-CAPTCHA は，VMware 上の Ubuntu11.10 の実装した試作アプリケーションを用い，問題画像に対して回答をテキストボックスへ入力する方式とした．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．回答までに要する時間は，Gimpy-r と IC-CAPTCHA では，問題画像が提示された時点からメモ帳あるいはテキストボックスへの回答の入力が終了し，エンターキーを押した時点まで，Asirra では問題画像が提示された時点から回答ボタンをクリックするまでをストップウォッチで計測した．CAPTCHA の説明と，CAPTCHA とアンケートの回答はすべて同じ 1 台の PC を用い，誰とも会話や相談などが行えない状態で個別に行った．

アンケート項目とその評価点を**表 6** 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 7** 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，平均所要時間と正否の調査結果は**表 8** のようになった．

表 6 ユーザビリティ評価の評価項目
Table 6 The usability evaluation items.

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

表 7 ユーザビリティ評価の結果（評価値）
Table 7 The usability evaluation 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？	4.21	1.93	4.00
解くことは面倒だったか？	4.86	1.43	3.43
解くことは簡単だったか？	4.50	2.36	4.36
CAPTCHA が使いやすかったか？	4.57	2.00	3.79
Web サービス上で使いたいか？	4.29	2.29	3.43

表 8 所要時間と正答率
Table 8 Required times and correct answer rates.

	正答率（%）	平均所要時間（sec）
IC-CAPTCHA 提案手法：妨害図形数 10	97.85	6.34
文字列 CAPTCHA	72.14	15.45
Asirra	95.71	14.19

表 7 より，5 つの質問事項すべてでその評価値が IC-CAPTCHA，画像 CAPTCHA，文字列 CAPTCHA の順になった．また，表 8 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分かる．

4.5 考察

画像検索評価から，300 枚の生成画像を画像検索にかけた結果，34 枚の生成画像で名詞が判明した．4.3 節の評価では，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物体画像の特徴量 [28] が違い，特徴量が多い物体画像の場合，すべて妨害することができなかったため，判明数が多かったと考えられる．表 5 の結果から，IC-CAPTCHA システム内で画像検索チェックを実行した場合，生成画像が廃棄される確率である廃棄率は 11.3%となる．これは，画像ストックの大きさを決めるうえで重要な指標である．ユーザビリティ評価から，既存の文字列 CAPTCHA，画像 CAPTCHA（Asirra）と比べて，提案手法の IC-CAPTCHA のほうが回答に要する所要時間が短く，正答率が高いという結果が得られた．提案手法が高いユーザビリティを有しているという結果を確認することができた．特に，回答所要時間では比較実験で用いた CAPTCHA の回答所要時間の平均値の半分以下の値となっており，提案手法の IC-CAPTCHA 方式が十分優れていることが分かる．しかし，提案手法にも CAPTCHA による判定テストに失敗したケースがあった．失敗したケースを考察すると，留学生による回答で，「みかん」の画像

を提示した際，正答が「みかん」「orange」であるのに対して，「lemon」という回答がなされた例がある．この事例から，国や地域など個人の育ってきた環境により同じ提示画像に対応付ける名詞に違いがある．また，提示画像「パソコン」に対して，「パソコン」，「PC」，「ノートパソコン」，「コンピューター」，「コンピュータ」，「computer」，「端末」など，国籍や育ちが同じ人間であっても回答が多岐にわたる場合もある．この問題の対策として，名詞と名詞の単語間の距離をもとにした判定により，提示画像に対応する正答の名詞を収集し，システムに保有させるなどの検討が必要である．提案手法では，画像を Web 上から取得するため，取得された物体画像が適切な名詞の物体画像であるかどうかは検索システムの精度に依存する．そのため，今後はユーザの正答率から適切でない物体画像であるかどうかの判定を自動で行う手法を取り入れることが望ましい．

また，物体画像内に人物が写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．物体画像の著作権や知的財産権の問題では，文献 [26] のようなパブリックドメインである画像を検索・ダウンロードできる Web 画像検索サイトを利用することで回避できる．

5. まとめ

本稿では，現在多くの Web サービスに採用され，ボットに対するシステムとして高い重要度を持つ CAPTCHA について，既存の CAPTCHA 方式の問題点を整理し，その問題を改善する新たな画像 CAPTCHA 方式である IC-CAPTCHA を提案した．文字列 CAPTCHA 方式には OCR 攻撃に対する脆弱性，画像 CAPTCHA 方式には偽陽率の高さと複数枚の画像を使用した際の一覧性の悪さ，動画 CAPTCHA 方式には CAPCTHA を解く際の所要時間の長さといった問題があった．提案手法は，文字列 CAPTCHA 方式と画像 CAPTCHA 方式とが相互に弱点を補うよう，提示画像に正答の文字列を含まず，提示する画像は物体画像 1 枚で，物体の名詞の文字列を入力する CAPTCHA 方式である．また，提案手法は動画 CAPTCHA 方式のように動画を用いないため，所要時間についての利便性を損なわない．判定に利用する物体画像を Web 上から取得すること，色・形が毎回ランダムに異なる妨害図形を物体画像の上に描くこと，物体画像の名詞を文字入力する判定テストとすることで既存の CAPTCHA 方式の問題点を改善した．ユーザビリティアンケートの評価を行った結果，IC-CAPTCHA 方式は既存の各 CAPTCHA 方式をすべての質問事項で上回り，所要時間の短縮，正答率の向上など IC-CAPTCHA システムの有効性を確認した．また，提案システムの運用時に必要となる妨害面積比率および画像検索評価による廃棄率について考察を行った．その結果，運用に耐えうる妨害面積比率について知見を得ることができた．また，画像検索評価により廃棄される画像の割合についても知見を得た．これらの結果により，提案システムを運用するユーザが，妨害面積比率の閾値，提示画像ストックを生成する過程のロスについて判断できるようになった．

今後は，名詞辞書の登録単語数についての検証を行い，提示画像の妨害領域の面積比率の閾値の目安を設定したうえで，妨害図形チェックや画像検索チェック，ブルームフィルタチェックを実装し，画像を生成する際の総合的な廃棄率や CAPTCHA 設置 Web サイトのアクセス数なども考慮した画像ストックの大きさの指標を考えたい．また，写真を用いた画像認識サービス [27] や，提示画像の妨害されていない部分を入力値として画像検索を行う攻撃に対しても，システムに新たなチェックを取り入れることで対応できるシステムとしていきたい．

参考文献

[1] Von Ahn, L., Blum, M., Hopper, N.J. and Langford, J.: CAPTCHA: Telling humans and computers apart, *Advances in Cryptology, Eurocrypt '03*, Vol.2656 of Lecture Notes in Computer Science, pp.294–311 (2003).

[2] Yan, J. and El Ahmad, A.S.: Breaking visual CAPTCHAs with naive pattern recognition algorithms, *2007 Computer Security Applications Conference*, pp.279–291 (2007).

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

[4] Elson, J., Douceur, J.R., Howell, J. and Saul, J.: Asirra: A CAPTCHA that exploits interest-aligned manual image categorization, *Proc. 14th ACM Conference on Computer and Communications Security*, pp.366–374 (2007).

[5] Golle, P.: Machine learning attacks against the asirra CAPTCHA, *Proc. 15th ACM Conference on Computer and Communications Security*, pp.535–542 (2008).

[6] Microsft: Microsoft アカウント，Microsoft（オンライン），入手先 ⟨https://signup.live.com⟩（参照 2014-09-09）．

[7] Mori, G. and Malik, J.: Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA, *2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (*CVPR '03*), Vol.1, pp.134–144 (2003).

[8] Moy, G., Jones, N., Harkless, C. and Potter, R.: Distortion Estimation Techniques in Solving Visual CAPTCHAs, *Proc. 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition* (*CVPR '04*), Vol.2, pp.1123–1128 (2004).

[9] Von Ahn, L., Maurer, B., McMillen, C., Abraham, D. and Blum, M.: reCAPTCHA: Human-based character recognition via Web security measures, *Science*, Vol.321, No.5895, pp.1465–1468 (2008).

[10] 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-CSEC-52, No.13, pp.1–8 (2011).

[11] Gossweiler, R., Kamvar, M. and Baluja, S.: What's Up CAPTCHA?: A CAPTCHA Based on Image Orientation, *Proc. 18th International Conference on World*

Wide Web (*WWW*), pp.841–850, ACM (2009).
[12] Zhu, B.B., Yan, J., Li, Q., et al.: Attacks and Design of Image Recognition CAPTCHAs, *ACM Conference on Computer and Communications Security* (*ACM CCS*) *2010*, pp.187–200 (2010).
[13] Almazyad, A.S., Ahmad, Y. and Kouchay, S.A.: Multimodal captcha: A user verification scheme, *2011 International Conference on Information Science and Applications* (*ICISA*), pp.1–7 (2011).
[14] Ahn, Y.C., Kim, N. and Kim, Y.: A User-friendly Image-Text Fusion CAPTCHA for Secure Web Services, *Proc. International Conference on Information Integration and Web-based Applications and Services*, p.550 (2013).
[15] 増井俊之：インターフェイスの街角（49)—画像を使ったなぞなぞ認証，Unix Magazine（オンライン），入手先 ⟨http://www.pitecan.com/UnixMagazine/PDF/if0201.pdf⟩（参照 2014-09-09）.
[16] 原田篤史，漁田武雄，水野忠則，西垣正勝：画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997–2013 (2005).
[17] Hayashi, E., Dhamija, R., Christin, N. and Perrig, A.: Use Your Illusion: Secure Authentication Usable Anywhere, *Symposium on Usable Privacy and Security* (*SOUPS*), pp.35–45, ACM (2008).
[18] NuCAPTCHA: NuCAPTCHA (online), available from ⟨http://www.nucaptcha.com⟩ (accessed 2014-09-10).
[19] 森　拓真，宇田隆哉，菊池眞之：アモーダル補完を利用した動画 CAPTCHA の提案，マルチメディア，分散協調とモバイルシンポジウム 2011 論文集，pp.1518–1525 (2011).
[20] 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*, p.1 (2012).
[21] 情報通信研究機構：日本語 WordNet，日本語 WordNet（オンライン），入手先 ⟨http://nlpwww.nict.go.jp/wn-ja/⟩（参照 2014-09-09）.
[22] *NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline*, National Institute of Standards and Technology (2006). SP800-63 電子認証に関するガイドライン，独立行政法人情報処理推進機構 (2007).
[23] 骨導超音波補聴器と使える発話練習アプリ for iPad：独立行政法人産業技術総合研究所（オンライン），入手先 ⟨https://staff.aist.go.jp/s-nakagawa/speechtrainingdevice/speechtrainingdevice.html⟩（参照 2014-11-26）.
[24] Google：Google 画像検索（オンライン），入手先 ⟨https://www.google.co.jp/imghp?hl=ja&tab=wi⟩（参照 2014-09-10）.
[25] Yan, J. and Ahmad, A.S.E.: Usability of CAPTCHAs or usability issues in CAPTCHA design, *Proc. 4th Symposium on Usable Privacy and Security*, pp.44–52 (2008).
[26] Pixabay: Pixabay (online), available from ⟨http://pixabay.com/⟩ (accessed 2014-09-10).
[27] マイナビ：世界最高レベルの認識精度を誇るスマートフォンを利用した画像認識サービス，マイナビニュース（オンライン），入手先 ⟨http://news.mynavi.jp/news/2012/06/06/105/⟩（参照 2014-09-12）.
[28] Matthews, P. and Zou, C.C.: Scene tagging: Image-based CAPTCHA using image composition and object relationships, *Proc. 5th ACM Symposium on Information, Computer and Communications Security*, pp.345–350 (2010).

田村 拓己　（学生会員）

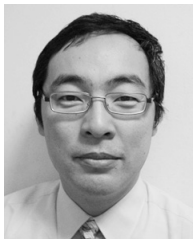
2013 年宮崎大学工学部情報システム工学科卒業．現在，同大学大学院工学研究科修士課程在学中．ネットワークセキュリティに関する研究に従事．

久保田 真一郎　（正会員）

1997 年熊本大学理学部物理学科卒業．1999 年同大学大学院理学研究科物理学専攻修士課程修了．2002 年鹿児島大学総合情報基盤センター文部科学事務官．2003 年鹿児島大学総合情報基盤センター技術職員．2006 年熊本大学大学院自然科学研究科物質生命科学専攻博士後期課程修了．2007 年熊本大学総合情報基盤センター助教．2013 年宮崎大学工学教育研究部准教授．コンピュータネットワーク，教育支援システムに関する研究に従事．博士（理学）．Association for Computing Machinery，教育システム情報学会，日本教育工学会各会員．

油田 健太郎　（正会員）

2003 年宮崎大学工学部情報システム工学科卒業．2005 年同大学大学院工学研究科情報工学専攻博士前期課程修了．2006 年熊本県立大学総合管理学部助手．2009 年宮崎大学大学院工学研究科システム工学専攻博士後期課程修了．同年大分工業高等専門学校助教．2012 年より同講師．コンピュータネットワークに関する研究に従事．博士（工学）．電子情報通信学会会員．



片山 徹郎　（正会員）

1991 年九州大学工学部情報工学科卒業．1993 年同大学大学院工学研究科情報工学専攻修士課程修了．1995 年同大学院工学研究科情報工学専攻博士後期課程修了．同年奈良先端科学技術大学院大学情報科学研究科助手．2000 年宮崎大学工学部情報システム工学科助教授．2007 年より同准教授．ソフトウェア工学，特にソフトウェアのテスト技法や信頼性に関する研究に従事．博士（工学）．電子情報通信学会，日本ソフトウェア科学会各会員．

朴 美娘 （正会員）

1983 年漢陽大学工学部電子工学科卒業．同年漢陽大学工学部助手．1993 年東北大学大学院工学研究科情報工学専攻博士後期課程修了．同年東北大学電気通信研究所助手．1994 年三菱電機株式会社入社．2010 年神奈川工科大学情報学部教授．ネットワークセキュリティ，暗号プロトコル設計，認証等の研究に従事．博士（工学）．電子情報通信学会，日本セキュリティ・マネジメント学会各会員．

岡崎 直宣 （正会員）

1986 年東北大学工学部通信工学科卒業．1991 年同大学大学院工学研究科電気及び通信工学専攻博士後期課程修了．同年三菱電機株式会社入社．2002 年宮崎大学工学部助教授．2007 年同准教授を経て，2011 年より宮崎大学工学教育研究部教授．通信プロトコル設計，ネットワーク管理，ネットワークセキュリティ，モバイルネットワーク等の研究に従事．博士（工学）．電子情報通信学会，電気学会，IEEE 各会員．