IPA

# 2009 年度下期未踏 IT 人材発掘・育成事業　採択案件評価書

## 1. 担当PM

夏野　剛（慶應義塾大学　政策・メディア研究科　特別招聘教授）

## 2. 採択者氏名

チーフクリエータ：小瀬木　浩昭（特定非営利法人ITプロ技術者機構）
コクリエータ：なし

## 3. プロジェクト管理組織

コシキ・バリューハブ株式会社

## 4. 委託金支払額

6,500,000 円

## 5. テーマ名

ユーザフレンドリかつ不正攻撃に強い、コンピュータと人間の識別能力の違いを活用した判別基盤の開発

## 6. 関連Webサイト

なし

## 7. テーマ概要

利用者が使いやすく不正な攻撃に強い人と機械の判別基盤の構築を通して、世界中のスパムを削減し、IT 資源と人資源の効率的な利用をはかり、持続可能な IT 社

会の実現を目指すことが、本提案の目的である。具体的には、使いやすく攻撃に強い人と機械の判別基盤を構築することで、以下のような IT 社会の実現を目指す。

・世界中のスパムを削減し、不正行為を防止する安全・安心な IT 社会
・IT 資源と人資源の効率的な利用をはかる、持続可能な IT 社会

このような社会の実現を目指すために、システムの正当な利用者である人間と、スパムを送信する不正なプログラムである機械を、短時間で判別する技術「CAPTCHA」を開発する。

開発する CAPTCHA は以下の特長を持つ。
・CAPTCHA の利用が CAPTCHA の強化につながる、持続可能なスパム防止基盤を構築する特長
・CAPTCHA を解く人間の労働力を有用な目的に役立てることで、人資源の有効活用をはかる特長

本提案の開発目標は、持続可能なスパム防止基盤を構築し、IT 資源と人資源の有効活用をはかるための、利用者が使いやすく不正な攻撃に強い人と機械の判別基盤を開発することである。

## 8. 採択理由

コンピューターと人間の識別能力の違いを利用し、効率的にスパムを防止するプラットフォームへ転換させている点が非常にユニークであり、新規性という点で高く評価できる。また技術的に実現性が高く、未踏プロジェクト期間中に一定の成果を出すことが期待できる。スキャナー読み込みデータの補正などにも拡張的に使用可能であり、是非とも採択したい。

## 9. 開発目標

本プロジェクトの目的は、利用者が使いやすく不正な攻撃に強い人と機械の判男リ基盤の構築を通して、世界中のスパムを肖リ減し、IT 資源と人資源の効率的な利用をはかり、持続可能な安全・安心な IT 社会の実現するために、新しい発想や斬新な技術を駆使し、システムの正当な利用者である人間と、スパムを送信する不正なプログラムである機械を、短時間で判男リする新しい「CAPTCHA 」を開発することである。

## 10. 進捗概要

ほぼ予定通りに実施した。

## 11. 成果

新しいCAPTCHA技術を実現するために、今回のプロジェクトでは下記4点を開発した。

- CAPTCHAアルゴリズム
  Oblivious CAPTCHAとReading CAPTCHAに適したCAPTCHAアルゴリズム
- Oblivious CAPTCHA CAPTCHAの新しい耐性強化軸として、真の文字列に"ダミー文字"を挿入し、真の文字列やその個数を答えさせるCAPTCHA。 利用者が使えば使うほどダミーの精度が高まり、ダミーの基礎個数が増える仕組みを備える。
- Reading CAPTCHA 機械が読み取れなかったスキャンされた紙媒体の文字を人間が読むCAPTCHA。利用者が使えば使うほど紙媒体の文字の電子化が進み、また電子化の精度が高まる仕組みを備える。
- CAPTCHAサーバとWeb・携帯プラグイン CAPTCHAをWebサービスとして提供するための、CAPTCHAサーバとWebプラグイン（サーバが提供するWebサービスを、Webサイト・携帯向けWebサイトが容易に利用・組み込み可能な形にするためのWebサイト用の拡張機能）。

### 1 CAPTCHAアルゴリズム

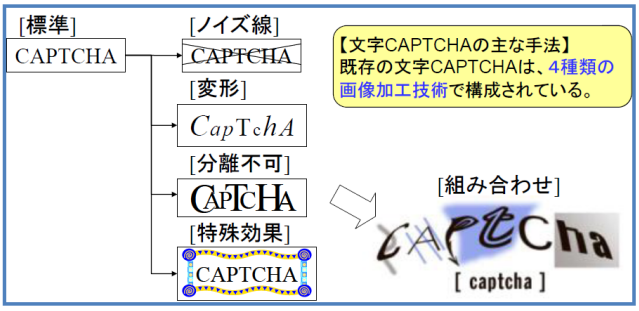


図1：文字CAPTCHAに使われている既存手法

図1は、文字CAPTCHAに使われている既存の手法を示している。 文字CAPTCHAに使われている既存の主な手法は、ノイズ線（arc）、変形（deform）、分離不可（undividable）、特殊効果（special effects）の、4種類の画像加工技

術である。Oblivious CAPTCHAとReading CAPTCHAのそれぞれに適したアルゴリズムを、上記の4種類の画像加工技術から選定または組み合わせて、開発した。

## 2 Oblivious CAPTCHA

Oblivious CAPTCHAは、CAPTCHAの新しい耐性強化軸として、真の文字列に"ダミー文字"を挿入し、真の文字列やその個数を答えさせるCAPTCHAである。Oblivious CAPTCHAは、利用者が使えば使うほどダミーの精度が高まり、ダミーの基礎個数が増える仕組みを備える。

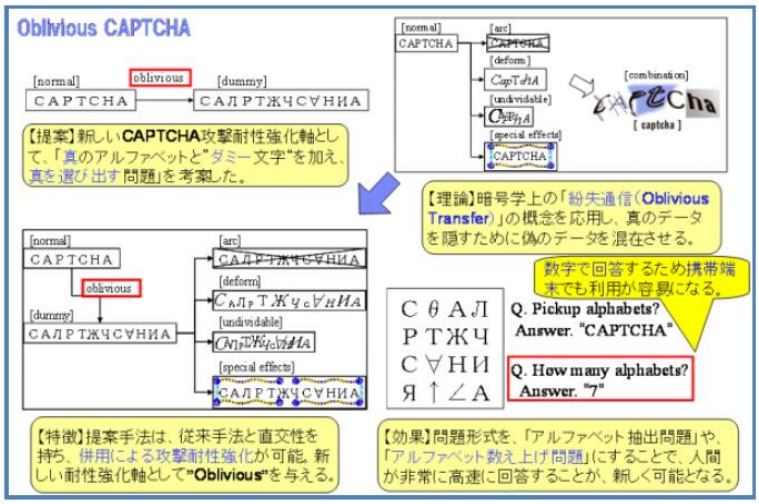


図2：Oblivious CAPTCHAの概要

図2は、Oblivious CAPTCHAの概要を示している。 Oblivious CAPTCHAは、利用者が使えば使うほどダミーの精度が高まり、ダミーの基礎個数が増える仕組みを備える。

利用者へダミーとして提示した記号の中で、多くの利用者がダミーと回答した記号は「良いダミー」として採用され、利用者により判断が分かれた記号はダミーから除外することでダミーの精度と品質を高める。また、ダミーか否か未知の記号を利用者に提示し、多くの利用者がその記号をダミーと回答すればダミーに採用され、利用者により判断が分かれた記号は却下することで、ダミーの基礎個数を増やすことができる。

## 3 Reading CAPTCHA

Reading CAPTCHAは、「人間は読めるが機械は読めない」というCAPTCHAの仕組みを利用して、機械が読み取れなかったスキャンされた紙媒体の文字を人

間が代わりに読むCAPTCHAである。Reading CAPTCHAは、利用者が使えば使うほど紙媒体の文字の電子化が進み、また電子化の精度が高まる仕組みを備える。

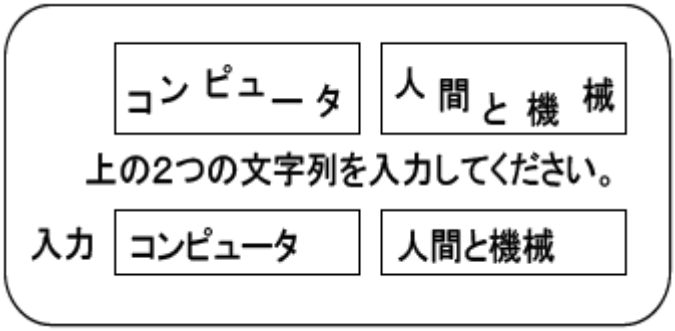


図3:Reading CAPTCHA

図3は、Reading CAPTCHAの概要を示している。
Reading CAPTCHAは、2つの文字列を表示する。両方とも紙媒体からスキャンされた文字であるが、正しい文字列が分かっている文字列は片方だけで、もう片方はOCRプログラムにより正しく読み取れなかったと警告された文字列である。利用者は両方の文字列を入力する必要があるが、スパム対策の確認に用いられるのは片方だけである。もう片方はOCRの結果の修正情報として利用する。正確さを保つため、正しい文字列が分かっていない文字列は複数の利用者に提示し、それらの入力を総合して正しい文字列を判断する。

既存の手法が利用者の労働力を人間確認だけに利用するのに対し、Reading CAPTCHAは人間確認と同時にOCRの修正という有用な目的に活用しており、既存手法と本質的に異なるアプローチである。

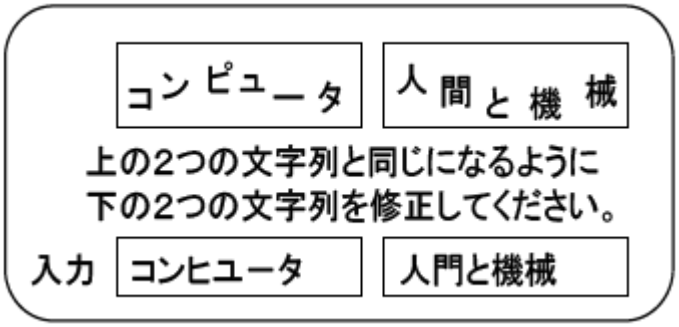


図4:誤り文字を修正する

図4は、誤り文字を修正する形態のReading CAPTCHAである。誤りの部分だけを入力することで、利用者の作業負担を軽減する。複数のOCRで事前実験した結果、特に日

本語文は漢字など1文字単位の認識誤りの割合が高く、修正を入力する形態で効率的なReading CAPTCHAが構成できる。 文字列は、適切な単位で区切り利用者に提示する。文字列が欧文など明確な区切りのある言語の場合、単語の区切りの空白を利用して単語単位で区切る。文字列が日本語など明確な区切りが無い言語の場合、適切な長さの文字数や句読点を単位として区切る。

利用者の負担を軽減するために、解く問題の選択権を利用者に与える。利用者は、提示されたReading CAPTCHAが解けない場合、別のReading CAPTCHAの問題や、通常の文字方式などのCAPTCHAの中から自分が解きたい（解くことが可能な）CAPTCHAを自由に選択することができる。

## 4 CAPTCHAサーバとWeb・携帯プラグイン

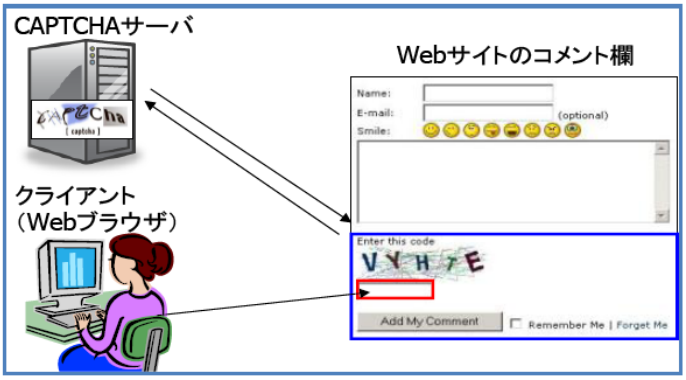


図5：利用シーン

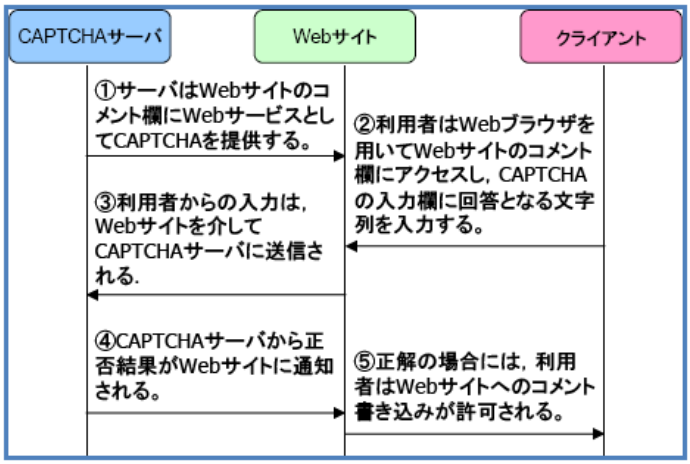


図6：利用シーン（シーケンス図）

新たに開発したCAPTCHAはWebサービスとして提供される。また、サーバが提供するWebサービスを、Webサイト・携帯電話向けWebサイトが容易に利用・組

み込み可能な形にするためのWebサイト用の拡張機能として、Webプラグイン・携帯プラグインを開発した。日本で広く普及している携帯電話向けWebサイトにも対応することで、CAPTCHAサービスの利用者数を増やし、利用者層を広げる。 図5は利用シーンのイメージ図である。また、図6はそのシーケンス図である。

## 12. プロジェクト評価

コンピューターと人間の識別能力の違いを利用し、効率的にスパムを防止するプラットフォームへ転換させている点が非常にユニークであり、新規性という点で高く評価できる。また技術的な実現性の面から、未踏プロジェクト期間中に、計画通り一定の成果を出したことも評価に値する。

CAPTCHA の提供者側と、スパム行為を行うスパマーとの戦いが、〝終りのないイタチごっこ〞であることを敢えて受容し、その上で「できるだけ延命できること」を考えているところが現実的であり、コンピュータ上の不正の防止に対して「人間の側ががんばらなくてはいけないというのは違うのではないか」という視点が新しい。

さらに、プライバシー保護や必要な情報量という面で、パスワードなどに比べて、キャプチャに優位性／有効性があることに対しても、綿密な調査を行っている専門性も評価している。

## 13. 今後の課題

市場の要請も高く、実用化への障害も低いことから、製品化やライセンスの仕方に対して、なるべく早期に事業化への道筋をつけるべきと考える。