

軽率な言動について考えさせ 鍵暗号方式の理解も深めるコンテンツ GOKEICHO（ご傾聴，ご軽佻）

小川悠輝^{†1} 伊藤一成^{†1}

昨今 Twitter や Facebook などの SNS の普及が急速に進み、個人でも気軽に不特定多数の人に対して情報発信可能な時代になっている。そのような状況の中、軽はずみな気持ちから投稿してしまった文章が大きな事故や事件に発展してしまうような事例が多く見られる。しかし、軽率な投稿かどうかということは主観では気づきにくい。そこで「ご軽佻」と「ご傾聴」のメタファに基づき、投稿内容が適切か事前に他者にチェックしてもらうことで、軽率な言動を抑制するコンテンツ GOKEICHO を設計、製作した。投稿文書を鍵暗号方式で暗号化してインターネット上を通信しており、同時に鍵暗号方式の理解を促す側面も有しているのが特徴である。

The Content that Make The User Think About Rash Speech and Enhances to Understand Key Cryptosystem - GOKEICHO (“Listening Closely” or “Levity”)-

YUKI OGAWA^{†1} KAZUNARI ITO^{†1}

Recently, social networking service (SNS) like Twitter and Facebook have become rapidly popular, and one can post messages to an unspecified number of people more easily. In this situation, there are many cases in which postings to SNS with rash feelings can cause accidents and incidents have been reported. However, it is difficult to recognize whether our postings are rash or not. It is therefore important for us to get an objective perspective when posting.

We have implemented the Web application GOKEICHO that make users refrain from rash speech with metaphor of “listening closely” and “levity”. The characteristic of this Web application is that it also enhances a user’s understanding of key cryptosystem.

「ご軽佻 防ぐためには ご傾聴」¹

1. はじめに

昨今 Twitter や Facebook などの SNS の普及が急速に進み、個人が気軽に不特定多数のユーザに情報発信することが可能になった。そのような状況の中、軽はずみな気持ちから投稿してしまった文章が、大きな事故や事件に発展してしまうような事例が多く見られる。また、SNS での情報

発信は、コンテキストやモダリティの欠落が想定外の誤解を招きうる。しかし、自身の投稿に問題があるかどうかは主観だけでは気づかない。

例えば、「免許ないけど、昨日友達のバイクを借りて乗りまわした。」という文章があった場合、無免許運転をしたと解釈されても仕方ないであろう。しかし、「昨日友達のバイク乗った。はやく免許欲しい」という文章を考えると、投稿者は「昨日友達のバイク(の後部座席に)乗った。はやく免許欲しい。」という意味で投稿したとしても、不特定多数に閲覧される上で、無免許運転をしたのではないかと曲解されてしまい、炎上してしまう可能性がある。

また、SNS 投稿の気軽さや、自己効力感を満足させられ

^{†1} 青山学院大学 社会情報学部
School of Social Informatics, Aoyama Gakuin University

るというメディアの特性が軽はずみな投稿を加速してしまっている現状は何らかの対策を講じる必要がある。そこで、自身が投稿しようとしている文章が軽はずみなものかどうかを他者に判定してもらい、情報発信について考えさせる機会を作ることが重要である。さらには SNS に限らず日常生活全般でも、他人の意見を真摯に傾聴するという姿勢を養うことは、軽はずみな発言や行動を防ぐ上で重要であろう。

そこで自律的に投稿内容を考えさせるコンテンツ GOKEICHO を設計、製作した。

以下 2 章では GOKEICHO と命名した理由、3 章では GOKEICHO の設計指針における特徴を 3 点明示し、4 章にてモラル、倫理の視点から考察する。5 章で実際に製作したコンテンツについて説明する。6 章では、鍵暗号方式の体験型学習コンテンツの側面としての GOKEICHO について説明し、7 章でまとめる。

2. GOKEICHO (ご傾聴, ご軽佻) について

今回提案するコンテンツの名称「GOKEICHO」は、「傾聴」と「軽佻」の両単語に、それぞれ尊敬語の「ご」を付与した「ご傾聴」「ご軽佻」のローマ字表記である。本提案では、両語彙が持つ語意や解釈が重要となるので、本章で説明する。

2.1 傾聴

傾聴は、小学館のデジタル大辞泉の解説によると、

1. [名] (スル) 耳を傾けて、熱心に聞くこと。「傾聴に値する意見」「傾聴すべきお話」とある。

軽はずみな情報発信を防ぐためには、自身で投稿内容について考えることも非常に重要ではあるが、他者からの意見を客観的に傾聴し、それを元に情報発信の重要性を考えることこそが最も大切である。

2.2 軽佻

軽佻は、小学館のデジタル大辞泉の解説によると、

1. 落ち着きがなく、言動が軽はずみなこと。また、そのさま。軽薄。「成程江戸っ子の一な風を、よく、あらわしてる」とある。

軽佻浮薄¹という言葉もあるように、考えや言動が軽はずみで、気持ちが浮ついた状態で情報を発信してしまうと、テーマでもある軽佻な投稿を行い、事件・事故に発展してしまう恐れがある。

1 考えや行動などが軽はずみで、浮ついているさま。

3. GOKEICHO の設計指針

筆者らはこれまでに情報機器の日常利用から内省と協調を促すコンテンツ GOSEICHO (ご清聴, 互成長) [1] や道聴塗説と同調圧力について考えさせるコンテンツ GODOUCHO (ご道聴, ご同調) [2], 表記誤りについて考えさせるコンテンツ GOTEICHO (ご丁重, ご低調) [3] をインターネット上で公開している^{2,3,4}。GOKEICHO も GOSEICHO, GODOUCHO, GOTEICHO と同様インターネット上で公開している⁵。

GOKEICHO の特徴は GOSEICHO や GODOUCHO, GOTEICHO と同様で、以下の 3 点である。

1. コンテンツに人型ピクトグラムを採用
2. 同音異義語 (ご傾聴, ご軽佻) を使用
3. 「ご傾聴」「ご軽佻」という言葉の意味から発生する認知的不協和を利用

この 3 点について、3.1 節から 3.3 節で詳しく説明する。

さらに GOKEICHO ではこれに加えて、

4. 鍵暗号方式の体験型学習コンテンツ

としての側面を有しているのが特徴である。これについては 3.4 節で概要を説明し、6 章で実装の視点からさらに言及する。

3.1 人型ピクトグラムの採用

ピクトグラムとは日本語で絵記号、図記号と呼ばれるグラフィックシンボルであり、意味するものの形状を使ってその意味概念を理解させる記号である。特に具象物を表現したピクトグラムはその抽象度の高さから、それを見た人物が自分自身や本人に関わる人物事物を想起させる効果があるとされている。人型ピクトグラムの例を図 1 に示す。

有名な「非常口」のピクトグラムは、デザイン策定の段階で、実際に避難中の人々が如何に出口へ向かって走る人型ピクトグラムと自身とを同一視するかにデザインの労力が払われた [4]。GOKEICHO では、画面デザインにおいて人型ピクトグラムを積極的に利用する。

つまり GOKEICHO で使用している人型の標準的なピクトグラムは知覚のレベルでは、人自体や人の特定の状態を想起させる。



図 1 人型ピクトグラムの例

2 <http://goseicho.com/>, <http://goseicho.info/>

3 <http://godoucho.com/>, <http://godoucho.info/>

4 <http://goteicho.com/>, <http://goteicho.info/>

5 <http://gokeicho.com/>, <http://gokeicho.info/>

一方認知のレベルでは、利用者の持つ知識や状況、それを駆動する能力により具体的な人物とマッピングされうる。

よって、表示された人型ピクトグラムやそれに付随するメタコンテンツの主体を、自分自身に投影する場合もあれば、他の特定の人物に射影して見なす者、特定のステレオタイプの象徴と見なす者もあり得る。写真では映っている特定の事物を想起し、イラストでも写実性の度合いに応じて想起の対象が限定されてしまい、ピクトグラムのような想起対象の多様性は生じにくい。

3.2 同音異義語とシャレの効用

日本語は、多くの同音異義語が存在するのが特徴である。同音異義語はシャレでよく利用される。織田はシャレの言語行動による理解と誤解において、同音異義語や音韻的類似を利用して文に2つの意味がある場合にもコミュニケーションが成立するのがシャレであると定義している[4]。また織田は、その二語の発音がより似ており、さらに語の意味がより異なるものほどシャレの効果が大きいと述べている。本コンテンツでは、2章で解説した「ご傾聴」「ご軽佻」の辞書的意味から、軽はずみな気持ち、もしくは自身の配慮不足から「ご軽佻」な文章を、客観的な意見を「ご傾聴」をすることができれば未然に防ぐことができるという解釈を採用し、二語の意味をより対比的に解釈することでシャレとしての効用を高める。シャレによる笑いやコミュニケーション創出の効用については社会学、認知言語学、感性工学や情報工学など様々な見地から研究が進められている[5][6]。

3.3 認知的不協和

人は、矛盾する2つの認知を同時に抱えている状態や、その状況下に置かれているときに不快感を感じてしまう。その結果、いずれか一方を否定して、矛盾を解消しようとする。これを社会心理学用語で認知的不協和という[7]。この認知的不協和を使った例に、トイレで「きれいに使って頂きありがとうございます」と掲示するというのがある。不協和を軽減させる方法には、1)認知を変える。2)新たな共和な情報を獲得する。3)重要度を変える。が挙げられる。油尾らは、ゴミの分別問題を題材に、感謝メッセージによる互惠性効果について分析している[8]。油尾は、感謝メッセージは、他者がメッセージに従っている時には、ポジティブな感情が生起し、互惠性が喚起されること示した。一方、環境自体が感謝メッセージに一致しない場合、抑止効果が軽減されてしまうことを実験から示している。

認知的不協和により感じる不快感を警告やアウェアネス向上に応用した研究もある[9][10]。

3.4 鍵暗号方式の体験的学習コンテンツ

鍵暗号方式とは、データのやり取りをする際に鍵を用いて暗号化をし、通信経路で盗聴されても機密性を保持するための技術である。鍵暗号方式には大きく分けて2種類あり、ひとつは、暗号と復号を同一の鍵で行う共通鍵暗号方式で、もう1つは、復号に使う秘密鍵から生成した公開鍵を配布し、その鍵で暗号化された暗号文を自身の持つ秘密鍵で復号する公開鍵暗号方式がある。

平成25年に閣議決定された「世界最先端IT国家創造宣言」(以下「創造宣言」)[18]では、「初等・中等教育段階でのプログラミング、情報セキュリティを充実させる」ことが謳われている。

実際、平成22年に運用開始された、現在の高等学校共通教科「情報」の学習指導要領でも「鍵暗号化方式の理解」は、学習単元の1つに設定されている。しかし、座学形式での授業では理解が難しい。暗号技術の仕組みまで踏み込んで教授しようとする、数学的要素が含まれているため、高校生にとっては一層理解が容易でない。そのためCSアンプラグドの技法を用いて体験的に学習させるなど、様々な取り組みも行なわれている[15][16]。

さらに創造宣言では、「サイバーセキュリティの確保」や「IoTやAIの更なる進化により、実世界とサイバー空間が相互に連携する社会の実現」に向けて、セキュリティ技術の開発や、情報セキュリティ人材の育成が謳われており、鍵暗号化方式の概要は、全国民が理解すべき重要な項目となってきた。

4. モラル及び倫理との関係

GOKEICHOの目的の1つにGOSEICHO、GODOUCHO、GOTEICHOと同様、日常生活や状況に応じたSNSとの関わり方を支援することが挙げられる。そのためには設計段階から、モラル、倫理の視点を組み入れることが必須事項である。そこで今回も辰己平面を参考にする。記事[11]にて久野が「辰己平面」と呼称する平面を図2の左に示す。辰己平面では、モラル(道義、内なる自分が正しいと思う～思わない)の軸と倫理(社会規範に合致する～しない)の軸は直交しており、はっきり区別されるべきであることを端的に示している。

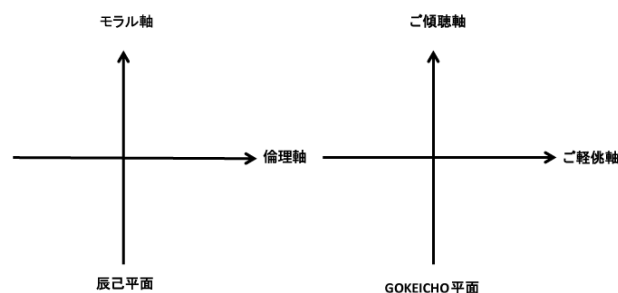


図2 辰己平面とGOKEICHO平面の比較

今回は、GOKEICHO（ご傾聴、ご軽佻）の解釈として、辰己平面にマッピングし、それをGOKEICHO平面と名付けることとした。GOKEICHO平面を図2の右に示す。「ご軽佻」は辰己平面の「倫理軸」と対応づける。自身の言動が軽はずみなものか否かは主観だけでは決定できず、自身の言動が社会規範に合致するか否かを客観的に判断する必要がある。

一方「ご傾聴」は辰己平面の「モラル軸」と対応づける。他人の言葉を真摯に傾聴した上で、さらに最終的に内なる自分が正しいと思うか思わないかを判断する能力を醸成する。

この両者を明確に分離することで、社会の中で軽はずみな言動を防ぐことが可能になるだろう。辰己平面と同様に二軸を明確に区別し、両方の能力をユーザが相補的に養っていただけることを実装に当たった設計指針の1つとする。

5. GOKEICHOの実装方式

5.1 概要

3章で紹介したGOSEICHO、GODOUCHO、GOTEICHOのプログラムを参考にGOKEICHOを実装した。GOKEICHOはWebアプリケーション形式で、単一のHTMLファイル（以下GOKEICHOファイルと呼ぶ）である。近年ではSPA(Simple Page Application)と呼ばれる全ての処理を単一のページで完結させるアプリケーションアーキテクチャが普及している。

またGOKEICHOはGOSEICHO、GODOUCHO、GOTEICHOと同様、HTML5、CSS(Cascading Style Sheet)、JavaScriptの学習コンテンツの用途を意識して実装されている[12]。Webアプリケーションなので、指定されたURIにブラウザでアクセスするだけで利用できる。

GOKEICHOコンテンツは大きく分けて2つのモードが存在する。両モードの遷移図を図3に示す。1つは、自身の文章が「ご軽佻」か否かを他者に判定してもらうGOKEICHO判定要請モード（図3の上）、もう1つは、自身の提起した問題に対して他者の回答を要請し、自身が他者からの回答に対して「ご傾聴」するGOKEICHO回答要請モード（図3の下）である。GOKEICHOのWebページは、アクセスの形態によりいずれかのモードで作用する。以下5.2節で、「GOKEICHO判定要請モード」、5.3節で「GOKEICHO回答要請モード」について解説する。

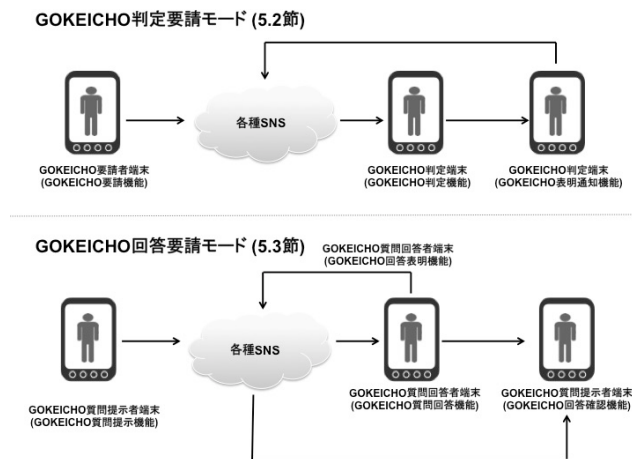


図3 GOKEICHO各モードの遷移図

5.2 GOKEICHO判定要請モード

5.2.1 GOKEICHO要請機能

GOKEICHO要請機能は、自身が情報発信しようとしている内容が軽はずみなものか否かを他者に判定してもらうために、各種SNSで判定を要請する機能である。スクリーンショットを図4に示す。

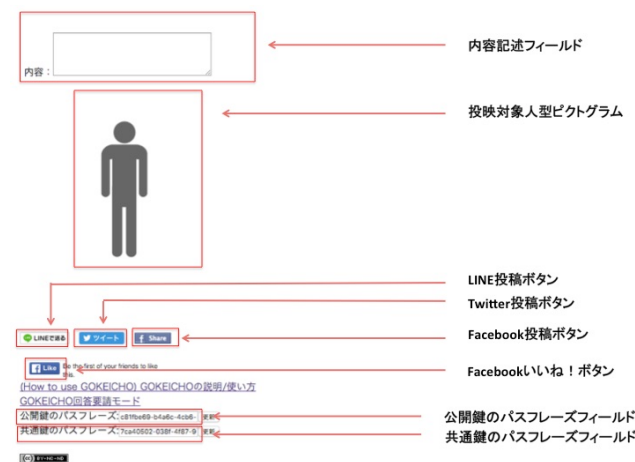


図4 GOKEICHO判定要請ページのスクリーンショット

図4のスクリーンショットの一番上部に表示されている「内容：」のラベルがついたテキストエリアに自身が投稿しようとしている内容を記述する。画面中央には人型ピクトグラムが表示される。内容を入力途中に、自分をピクトグラムに投影することで、情報発信者としての心構えを意識させるとともに、ピクトグラムが自身の投稿内容を「ご傾聴」していると錯覚させ、「ご軽佻」な投稿を抑制する。

内容入力後、図4の下部に表示される「LINE投稿ボタン」、「Twitter投稿ボタン」、「Facebook投稿ボタン」を押下するとそれぞれLINE、Twitter、FacebookのWeb

ページが、投稿文がそのまま投稿できる状態で立ち上がる。これにより GOKEICHO の要請が可能となる。

GOKEICHO の Web ページでは、初回アクセス時に一意のパスフレーズと共通鍵を生成し、以後永続的に端末内に保存している。パスフレーズはパスフレーズ表示フィールド、共通鍵は共通鍵表示フィールドに表示される。これらの文字列はユーザが自由に変更することができる。

図 4 はスマートデバイスでアクセスした場合のスクリーンショットであるが、PC の場合も同様の表示となる。

GOKEICHO 要請内容記述フィールドに自身が投稿しようとしている文章を入力した場合に自動的に生成される SNS 投稿文面は以下の表示になる。

以下のリンクの文章はご軽佻でしょうか？ご傾聴お願いします。 #gokeicho

<http://gokeicho.com?s=XXXXXXXXXXXXXXXXXXXX&qid=YYYYYYYYYY>

ここに記載されている URI 中の XXXXXXXXXX(s 属性値)は、図 3 中の GOKEICHO 内容記述フィールドに入力された文字列を crypto-js[17]という暗号化通信を行なうための JavaScript ライブラリを用いて暗号化した文字列である。共通鍵をキーに共通鍵暗号アルゴリズム AES アルゴリズムにより暗号化した文字列になっている。これは GOKEICHO 内容記述フィールドに記入された内容を不特定多数の人に見られないようにするためである。

ここで共通鍵によって暗号化することによって、共通鍵を知っている人でないと GOKEICHO 内容記述フィールドに記載された内容を参照することができない。

さらに YYYYYYYYYY (qid 属性値)は GOKEICHO 要請毎に自動生成された一意となる ID(UUID)である。

HTTP の GET メソッドを使い引数を受け渡す方式を採用しており、あらかじめ特定の URI へアクセスする QR コードを印刷し紙媒体にて配布する、この URI にアクセスする無線タグを設置してアクセスさせるなどの別の方法も適用できる。

5.2.2 GOKEICHO 判定機能

5.2.1 節で解説した GOKEICHO 要請機能を使用して自動生成された URI にアクセスした端末は、ブラウザ上に GOKEICHO ページが表示される。この場合、確認を要請された内容に対して GOKEICHO する画面が表示される。

GOKEICHO は、スマートデバイスでアクセスした場合、次に示す 4 状態を順番に遷移していく。

(1) GOKEICHO 判定状態…GOKEICHO の Web ページへアクセスし、ご軽佻か否かを判定

- (2) GOKEICHO 感謝状態…判定者に対して、ご傾聴してくれたことに感謝
- (3) GOKEICHO 判定表明状態…判定した結果を SNS で表明
- (4) 通常状態…GOKEICHO の Web ページを閉じて元の通常の使用状態に戻る

(1)「GOKEICHO 判定状態」では図 5 で示すように GOKEICHO 要請者が記入した文章とともに、その内容は「ご軽佻でしょうか？」という文章がページ上部に表示される。この際、要請者と判定者の共通鍵が一致している場合は平文として要請者が入力した内容が表示されるが、要請者の共通鍵と異なる場合は、図 5 に示すように暗号化された状態のランダムな文字列が表示される。すなわち、「ご傾聴」する際に要請者からあらかじめ共通鍵を覚えてもらう必要があり、これにより共通鍵暗号方式で鍵配送問題を体験的に学ぶことができる。そして、GOKEICHO ファイルにアクセスした者はその内容が「ご軽佻」なものかどうかを判定し、「ご軽佻である」と体に記載されているピクトグラムか、「ご軽佻でない」と体に記載されているピクトグラムかどちらかの右手をタップする。

右手の部分をクリックすると「ごけいちょうありがとうございます」の合成音声で再生され、(2)「GOKEICHO 感謝状態」に移行する。合成音声は Open JTalk で生成した [13]。

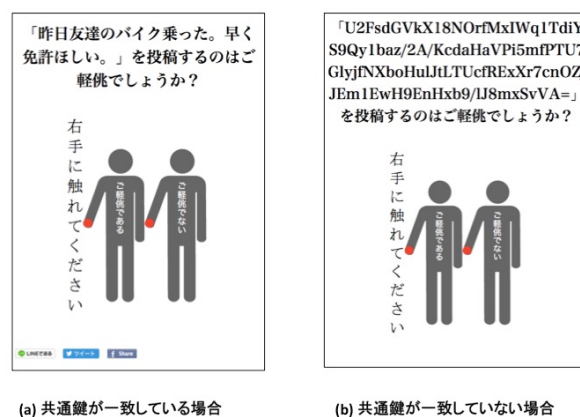


図 5 GOKEICHO 判定状態のスクリーンショット

(2)「GOKEICHO 感謝状態」では、GOKEICHO 要請者の文章について真摯に傾聴したことに対して図 6 に示すように「ご傾聴ありがとうございました」の文章と共に感謝の意を表現したお辞儀をしているピクトグラムが表示される。



図6 GOKEICHO 感謝状態のスクリーンショット

5.2.3 GOKEICHO 表明通知機能

5.2.2 項の GOKEICHO 感謝状態では、要請者の文章に対して判定者がご軽佻か否かを 各種 SNS で不特定多数に表明する機能を実装している。

(3)「GOKEICHO 感謝状態」において、画面上のソーシャルボタンを押下すると LINE, Twitter, Facebook の Web ページが、自動生成された投稿文がそのまま投稿できる状態で立ち上がる。Twitter の場合を例に以下に示す。LINE や Facebook のボタンを押下した場合も、同様の文面が自動生成される。

【「ご軽佻」だと表明する場合】

以下のリンクの文章はご軽佻です。 #gokeicho
<http://gokeicho.com?s=XXXXXXXXX &qid= YYYYYYYYYY>

【「ご軽佻」でないと表明する場合】

以下のリンクの文章はご軽佻ではありません。 #gokeicho
<http://gokeicho.com?s=XXXXXXXXX&qid= YYYYYYYYYY>

5.3 GOKEICHO 回答要請モード

質問内容について不特定多数から回答を得、さらに個々の回答内容を質問者以外が閲覧できないようなモードである。例えば、「自分はどういう性格ですか？」など個人のプライバシーにあたるような内容や、授業中に教授者が学習者に質問を提示し、回答を回収する場合がこれにあたる。

既存の SNS で回答要請モードと同様のことを行う場合、SNS の気軽に投稿できるという性質上回答者は真摯に傾聴せず、軽い気持ちで回答を作成することが考えられる。そのため、GOKEICHO コンテンツを通して回答を要請することで、きちんと傾聴した上での回答を得ることを目的

にしている。

質問者が提起した内容への回答について不特定多数の他者が閲覧できないように質問者の持つパスフレーズを元に生成した公開鍵を用いて暗号化を行い、質問者しか復号が行えないような公開鍵暗号方式を採用し実現する。

5.3.1 GOKEICHO 質問提示機能

GOKEICHO 質問提示機能は、自身が他者に対して提示した問いに対して、SNS を経由して GOKEICHO コンテンツ内で回答してもらう機能である。質問提示機能の画面を図 7 に示す。



図7 GOKEICHO 質問提示機能のスクリーンショット

図 7 のスクリーンショットの一番上部に表示されている「内容:」のラベルがついたテキストエリアに提示する問題の内容を記述する。画面中央には人型ピクトグラムが表示される。内容を入力途中に、自分をピクトグラムに投影することで、情報発信者としての心構えを意識させる。内容入力後、図 7 の下部に表示される「LINE 投稿ボタン」、「Twitter 投稿ボタン」、「Facebook 投稿ボタン」を押下するとそれぞれ LINE, Twitter, Facebook, 自動的に投稿文を生成する。これにより GOKEICHO の要請が可能となる。

5.2.1 節でもあるように、GOKEICHO の Web ページでは、初回アクセス時に一意のパスフレーズを生成し、以後永続的に端末内に保存している。例えば、GOKEICHO 問題提示記述フィールドに自身が投稿しようとしている文章を入力した場合に自動的に生成される文面は以下の表示になる。

以下のリンクの質問にご傾聴をお願いします。 #gokeicho

`http://gokeicho.com?s=XXXXXXXXXXXXXXXXXXXXX
&qid=YYYYYYYYYY&pkey=ZZZZZZZZZZ`

ここで URI の `s` 属性値は、GOKEICHO 問題提示記述フィールドに入力された文字列を含んでおり、`pkey` はパスフレーズを元に生成された文字列であり、問題提示者の公開鍵として 5.3.2 項の GOKEICHO 問題回答機能で回答者が入力した文章を暗号化する際に用いる。

`qid` 属性値は GOKEICHO 要請毎に自動生成された一意となる ID(UUID)である。

また HTTP の GET メソッドを使い引数を受け渡す方式を採用しており、あらかじめ特定の URI へアクセスする QR コードを印刷し紙媒体にて配布する、この URI にアクセスする無線タグを設置してアクセスさせるなどの活用方法もできる。

5.3.2 GOKEICHO 質問回答機能

GOKEICHO 質問回答機能では、5.2.2 項と同様に、自動生成された URI にアクセスした端末は、ブラウザ上に GOKEICHO ページが表示される。この場合、回答を要請された内容に対して GOKEICHO する画面が表示される。

GOKEICHO は、次に示す 3 状態を順番に遷移していく。

- (1) GOKEICHO 回答状態…GOKEICHO の Web ページへアクセスし、質問者が示した問いに対してご傾聴した結果、回答を作成
- (2) GOKEICHO 回答表明状態…回答した結果を SNS で表明
- (3) 通常状態…GOKEICHO の Web ページを閉じて元の通常の使用状態に戻る

(1)「GOKEICHO 回答状態」では図 8 で示すように GOKEICHO 質問提示者が記入した文章について、回答する記述フィールドが設けられる。

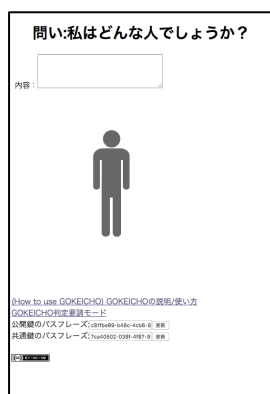


図 8 GOKEICHO 回答状態のスクリーンショット

回答を記述することにより、各種 SNS へのソーシャルボタンが表示され、回答を表明することができる。

5.3.3 GOKEICHO 表明通知機能

GOKEICHO 回答状態で問いに対して回答すると、質問提示者の質問に対して回答した内容を SNS で不特定多数に表明する機能を実装している。

この際、5.3.1 節でも紹介したように URI に含まれている質問提示者のパスフレーズから生成された `pkey` 属性値で回答内容を暗号化し、`answer` 属性値に設定する。これにより 5.3.4 節で紹介する GOKEICHO 回答確認機能で質問に対する回答内容を確認できるのは質問提示者本人だけという、公開鍵暗号方式での暗号化を実現している。

(1)「GOKEICHO 回答状態」において、画面上のソーシャルボタンを押下するとサービスに応じた文面が自動生成され、直ちに投稿、送信可能な状態となる。Twitter の場合を以下に示す。LINE や Facebook のボタンを押下した場合も、同様の文面が自動生成される。

「XXX」という質問に対してご傾聴しました。 #gokeicho
`http://gokeicho.com?s=XXXXXXXXXX&qid=YYYYYYYYYY
&answer=ZZZZZZZZZZZZ`

5.3.4 GOKEICHO 回答確認機能

GOKEICHO 回答確認機能は、質問提示者が示した質問に対して行なわれた回答を、SNS に表明した際に生成される自動生成文に含まれる URI にアクセスすることによりアクセスする。画面には質問提示者が示した質問が「問い:」というラベルの後に記述され、その下の「回答:」というラベルに回答者が示した回答文が表示される。

ここで、5.3.3 節で暗号化され `answer` 属性として URI に埋め込まれた文章を抽出し、パスフレーズを秘密鍵として復号を試みる。暗号化に用いた公開鍵が復号を試みようとしているパスフレーズから生成されたものであれば、復号成功し図 9 の(c)に示すように回答は平文で表示される。

公開鍵の生成に使用したパスフレーズと復号を試みようとしているパスフレーズが異なる場合は、復号は失敗し図 9 の(d)に示すように URI に埋め込まれているランダムな文字列である `answer` 属性値の最初の 20 文字が画面に表示される。ここで復号に失敗した場合 20 文字しか表示しないのは画面レイアウトの都合上である。

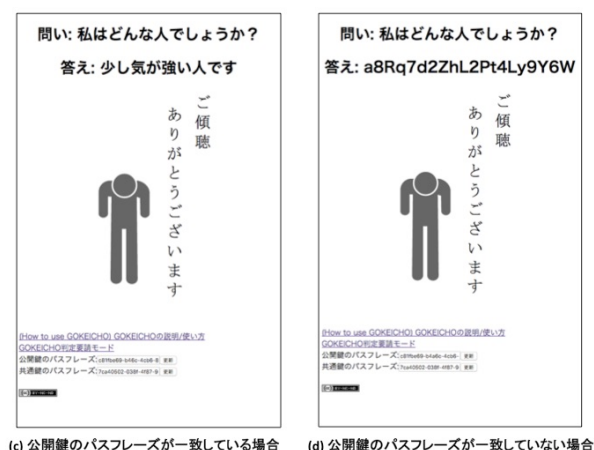


図9 GOKEICHO 回答確認のスクリーンショット

6. 鍵暗号方式の視点から見た GOKEICHO

GOKEICHO コンテンツには、5.2 節で解説した「GOKEICHO 判定要請モード」および 5.3 節で解説した「GOKEICHO 回答要請モード」の 2 つのモードを使って鍵暗号方式を体感的に学べる学習コンテンツとして設計されている。

「GOKEICHO 判定要請モード」では共通鍵暗号方式を体感的に学習できるコンテンツとして設計されている。共通鍵暗号方式は暗号化と復号化で同じ鍵を使う方式であり、「GOKEICHO 判定要請モード」では、共通鍵フィールドの値が鍵の役割を果たしており、要請者はそれを用いて GOKEICHO 判定要請フィールドに記述された内容を暗号化する。判定者は SNS より、要請者が投稿した自動生成文に含まれる URI より GOKEICHO コンテンツにアクセスする。この時、図 10 に示すように、要請者と判定者の共通鍵が不一致の場合、要請記述フィールドに記述した内容を復号しても平文にならないため内容確認できない。共通鍵いかにして配送するかという共通鍵暗号方式の鍵配送問題も体験できる。

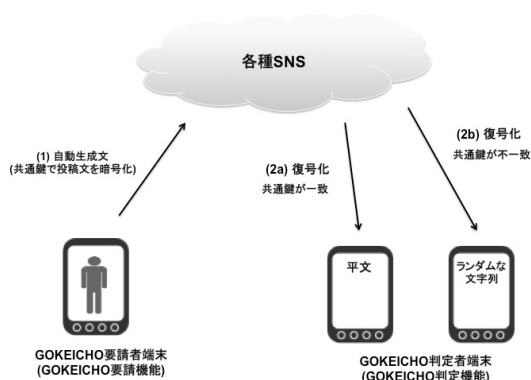


図10 GOKEICHO 共通鍵暗号方式の流れ図

「GOKEICHO 回答要請モード」では公開鍵暗号方式を体感的に学習できるコンテンツとして設計されている。流れ図を図 11 に示す。公開鍵暗号方式は、暗号化と復号化と別個の鍵を使用し、暗号化に使用する鍵を公開できるようにした暗号方式である。「GOKEICHO 回答要請モード」では、RSA アルゴリズムを用いて暗号化に使用する公開鍵を問題提示者のパズフレーズから生成し、問題提示者が投稿する際、公開鍵は、投稿文中に記載される URI 中の pkey 属性値に設定する。回答者は 5.3.2 項で紹介した GOKEICHO 質問回答機能においてテキストエリアに回答した内容を SNS へ回答表明する際、URI に含まれている pkey 属性値を用いて暗号化を行う。質問提示者は回答者が SNS に投稿した URI にアクセスし、質問提示者の端末内に格納されているパズフレーズを秘密鍵として回答者が暗号化した内容を復号する。

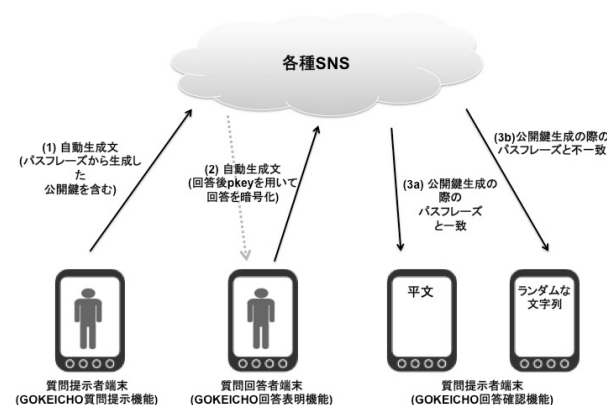


図11 GOKEICHO 公開鍵暗号方式の流れ図

7. おわりに

本稿では、「ご傾聴」と「ご軽佻」のメタファに基づき、軽はずみな言動を抑制しつつ鍵暗号方式の理解も深めるコンテンツ GOKEICHO (ご傾聴, ご軽佻) について解説した。今後は本コンテンツの機能拡張及び利用評価実験を行う予定である。

謝辞 本研究は JSPS 科研費 26330140, 25350322 の助成を受けたものです。

参考文献

- 1) 伊藤一成: PC やスマートデバイスの日常利用に気づきを与えるシステム GOSEICHO の拡張, 情報処理学会研究会「コンピュータと教育」, Vol.2013-CE-126, pp.1-6 (2014)
- 2) 伊藤一成: 道聴塗説と同調圧力について考えさせるコンテンツ GODOUCHO (ご道聴, ご同調), 情報処理学会・コンピュータと教育研究会情報教育シンポジウム SSS2015, pp.185-191 (2015)
- 3) 伊藤一成: 表記誤りについて考えさせるコンテンツ GOTEICHO (ご丁重, ご低調), 情報処理学会研究報告「コンピ

- ュータと教育」, Vol.2015-CE-131, pp.1-7 (2015)
- 4) 太田幸夫: 国際安全標識ピクトグラムデザインの研究
<http://www.tamabi.ac.jp/soumu/gai/hojo/seika/2003/kyoudou-ota1.pdf>
- 5) 織田 正吉, 野村 雅昭: シャレ・ダジャレ学事始(ことはじめ), 日本笑い学会 笑い学研究, Vol.6, pp. 55-67 (1999)
- 6) 木村洋二: 笑いの社会学, ISBN: 4790702553 (1983)
- 7) 濱田真樹, 鬼沢武久: 同音異義語の意味の多様性を構造にもつなぞなぞの生成, 日本知能情報ファジー学会誌 知能と情報, Vol.20, No. 5, pp.696-708 (2008)
- 8) レオン・フェスティンガー: 認知的不協和の理論, ISBN: 4414302102 (1965)
- 9) 油尾聡子, 吉田俊和: 迷惑抑止メッセージと記述的規範が社会的迷惑行為と感情に及ぼす効果, 日本応用心理学会論文誌, Vol.34, No.2, pp.155-165 (2009)
- 10) Yasuhiro Fujihara and Yuko Murayama: A User Survey on the Interface Causing Discomfort for Warning, User Interfaces, Rita Matrai (Ed.), ISBN: 9789533070841(2010)
- 11) 村上遥, 藤原康宏, 村山優子: 危険アウェアネスのための不快なインタフェースの実装, 情報処理学会 インタラクシオン 2009 (2009)
- 12) 久野靖: 情報科教員のための教員免許更新講習(前), 情報処理, Vol.56, No.5, pp.492-495 (2015)
- 13) 伊藤一成: HTML5 を体感的に学習できるコンテンツ GOSEICHO (5 成長), モバイル学会誌, Vol.5, No.1, pp.21-26, (2015)
- 14) 大浦圭一郎, 酒向慎司, 徳田恵一: 日本語テキスト音声合成システム Open JTalk, 日本音響学会春季講演集, Vol.I, 2-7-6, pp.343-344 (2010)
- 15) 間辺広樹, 兼宗進, 並木美太郎: アンブラグドを活用した公開鍵暗号学習プログラムの情報科教育への適用, SSS2010, pp.15-18 (2010)
- 16) 野部緑: CS アンブラグドを目指した公開鍵暗号の授業, SSS2010, pp.47-48 (2010)
- 17) crypto-js <https://code.google.com/p/crypto-js/>
- 18) 世界最先端 IT 国家創造宣言
<https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20150630/siryou1.pdf>