

テクニカルノート

Android スマートフォンユーザ向け ワンクリック詐欺疑似体験教材の開発

新谷 洋介^{1,a)} 長谷川 元洋²

受付日 2013年2月5日, 採録日 2013年5月18日

概要: 筆者らは, Android スマートフォンでワンクリック詐欺を疑似体験できる Android アプリと解説教材で構成される中高生向け教材パッケージを開発した. A 教育委員会主催の教員研修会で 14 名の教員から教材パッケージに対する評価をしてもらったところ, 12 名の教師が, 「授業で使ってみたい」と評価した.

キーワード: ワンクリック詐欺, Android スマートフォン, 疑似体験教材

Development of a One-click Fraud Simulation Learning Material for Android Phone Users

YOSUKE ARAYA^{1,a)} MOTOHIRO HASEGAWA²

Received: February 5, 2013, Accepted: May 18, 2013

Abstract: The authors have developed a learning material package which includes a one-click fraud simulation learning Android Application and related learning manual. In the workshop for 14 in-service teachers held by an education board, 12 teachers answered that they wanted to use this teaching-material package in a lesson.

Keywords: one-click fraud, Android phone, simulation learning material

1. はじめに

1.1 先行研究と類似研究

筆者らは, 従来型の携帯電話やコンピュータなどのインターネット端末で「ワンクリック詐欺」や「フィッシング詐欺」などの携帯電話利用時の危険性を疑似体験できる Web 教材とそれを用いた授業を, 2007 年に開発し [1], それ以来, 全国の学校の授業や教員研修講座などで活用できるよう, その教材をインターネット上に無償公開してきた [2].

類似教材としては次のようなものがある. 岩手県立総合教育センターは 2008 年に, 教育センターや学校の内部サーバに教材をインストールして, コンピュータや携帯電

話で, 疑似体験できる教材を開発している [3]. 市販教材は 2009 年に 2 種類が発売されており, コンピュータ上の画面に, 仮想の携帯電話画面を表示させ, 携帯電話で起こりうる危険性の疑似体験ができる Sky 株式会社「SKYMENU」や [4], 校内サーバ上などに教材を用意し, 無線 LAN 対応の携帯電話で, 教材にアクセスし学習できる日本電気株式会社の「UNIVERGE ケータイ de モラル ソリューション」がある [5]. このように, コンピュータや従来型携帯電話で疑似体験できる教材はすでに存在しているが, スマートフォン用の疑似体験教材はまだない.

1.2 Android アプリの危険性

従来型携帯電話ユーザを狙ったワンクリック詐欺は, IP アドレスや携帯電話の機種名などを表示させ, 個人情報を取得したかのように見せかけ, 金銭を脅し取るものである. その際に取得される IP アドレスなどの情報から, 個人情報が得られることは通常はないため, 無視することが最善

¹ 北海道高等聾学校
Hokkaido, Hard of Hearing, High School, Otaru, Hokkaido
047-0261, Japan

² 金城学院大学
Kinjo Gakuin University, Nagoya, Aichi, 463-8521, Japan

^{a)} y-araya@newcanyon.com

の対処方法であった。

しかし、Android スマートフォンユーザを狙ったワンクリック詐欺アプリは、携帯電話番号などの個人情報にアクセスし、それを外部に送信する [6]。実際に、2012 年 5 月には、動画再生アプリと偽って、Android スマートフォンに不正なアプリをインストールさせ、名前、メールアドレス、電話番号などを送信させた事例が発生し、警視庁は 100 万人を超える個人情報が流出した恐れがあるとして、東京都内の企業などを家宅捜索した事件が発生している [7]。

携帯電話番号が送信されると、電話や SMS により直接自分の携帯電話宛に金銭を要求する電話がかかってきたりメッセージが届いたりすることが懸念される。つまり、実際に請求される状況が発生する可能性が生じることから、被害を予防することの必要性がより増している。

1.3 Android アプリの配布方法の特性から生じる危険性と危険回避のための教材の必要性

iPhone では、一般的な使用においては、Apple 社が運用している「App Store」に登録されている審査済みのアプリをインストールして利用する仕様になっている。しかし、Android スマートフォンでは、一部の携帯電話事業者が運営するサイトや、Google 社が運用している「Google Play」などを除き、第三者が作成したアプリが Web 上に事前審査なしの状態に登録される。さらに、電子メールに添付されたアプリも、「提供元不明のアプリ」のインストールを許可する設定をするだけで、だれもが簡単にインストールして利用できるようになっている。このことから、Android OS を搭載したスマートフォンやタブレット PC（以下、Android 端末と表す）は、iPhone よりも様々なアプリを自由に選択して利用できる反面、危険なアプリがインストールされる可能性が高いといえる。

この危険性に対し、Android 端末用のセキュリティソフトが提供されているが、危険なアプリかどうかを判断する機能はなく、新たに公開された危険なアプリに対しては対応できないことがある。そのため、Android 端末用のアプリの利用は、インストール時に求められる各種データに対するアクセス許可によって、アプリが外部に送信するデータの種類やそれにより生じる状況を利用者が自分で考え、自己責任で判断する必要があることになる。

もちろん、被害に遭わないよう、広く注意を呼びかけることは必要であるが、振り込め詐欺被害防止の啓発活動によって被害をゼロにすることができていないことを考えれば、それだけでは不十分であるといえる。そこで、被害防止を目的とした講習会や授業で利用可能な、携帯電話番号などを取得される状況を体験できる Android スマートフォン向けワンクリック詐欺疑似体験教材を開発することにした。

2. 設計方針

2.1 Android スマートフォンを狙ったワンクリック詐欺の特徴

現在、Android スマートフォンを狙ったワンクリック詐欺は 2 種類存在する。1 つは、従来型携帯電話ユーザを狙ったワンクリック詐欺サイトをスマートフォン向けにデザインだけ変更したものである。もう 1 つは、不正なアプリをインストールさせるものである。1.2 節で述べたように、前者は代金請求のメッセージを無視しておけば被害にあうことはないが、後者は個人情報を抜き取られてしまい、実際の被害に遭う可能性が高い点で大きく異なる。

2.2 仕様

2.1 節で述べた特徴を持つアプリの被害を防ぐには、アプリのインストール時に表示される「アプリがアクセスする情報」について冷静に検討し、個人情報が含まれる情報にアクセスを求めるケースかどうかを判定する必要がある。そのためには、その情報を正しく判定するための知識を持っている必要がある。そこで、不正なアプリを動作させ、個人情報を抜き取られてしまうまでの手順とその方法について分析し、疑似体験アプリの仕様を決定した。

利用者が不正なアプリを動作させてしまうまでの主な手順は、次のとおりである。

- ① 利用者の興味を引く内容が掲載されている Web ページから希少な情報やお得な情報などが得られるアプリをインストールするように誘導される。
- ② アプリをダウンロードする。
- ③ 「提供元不明のアプリ」のインストールを許可する。
- ④ 許可権限を確認する。
- ⑤ インストールする。
- ⑥ 実行する。

「『③ 提供元不明のアプリ』のインストールを許可する」は、危険ではあるが、キャリアやスマートフォンメーカーの公式サイトを利用する際にも許可する必要がある、利便性を考えて許可する設定にしているユーザが多いと推測することから、「④ 許可権限を確認する」が重要なポイントであると考えられる。

この許可権限は、Android アプリの特徴であり、アプリの動作に関する許可権限はアプリのユーザの判断にゆだねられている仕様からくるものである。求められる「許可する権限」は、「個人情報」、「開発ツール」、「料金の発生するサービス」、「送受信したメッセージ」、「現在地」、「ネットワーク通信」、「アカウント」、「ストレージ」、「電話/通話」、「ハードウェアの制御」、「システムツール」、「端末限定」の 12 種類ある。

既存のワンクリック詐欺アプリは、「現在地」、「ストレージ」、「ネットワーク通信」、「電話/通話」の許可権限を要求

表 1 既存ワンクリック詐欺アプリの許可権限
Table 1 Permission of a one-click fraud application.

許可する権限	内容
現在地	GPS情報を読み取る
ストレージ	電話帳などの情報を読み取る
ネットワーク通信	インターネットを利用した情報の送信
電話／通話	電話番号などの情報を読み取る

している [6]. これらの「許可する権限」から、表 1 に示す情報を収集されるなど、個人情報を読み取られてしまう危険性があることが分かる.

疑似体験アプリでは、利用者が安全な状況で教材を利用できるように、「ネットワーク通信」の許可は求めず、「電話/通話」のみを許可させることにした. これにより、アプリが携帯電話の番号が外部に流出しない安全な状況下で、学習者は読み取り画面に表示されて個人情報を抜き取られてしまう状況を疑似体験できる仕様にした. また、これは、教育の場における倫理の観点から、個人情報を盗み取られる危険性を教える際に学習者の個人情報を取得してしまわないようにした仕様でもある.

3. 開発

3.1 開発環境、動作環境

開発環境および動作環境を表 2 に示す. なお、動作確認は、Optimus bright L-07C (Android 2.3) および Optimus LTE L-01D (Android 4.0) を用いた.

3.2 教材パッケージの構成

今回、開発したスマートフォン用の教材パッケージは、① スマートフォン情報モラル解説 Web サイト「スマホモラル」、② スマートフォン情報モラル解説スマートフォン専用 Web サイト「スマホモラル for スマホ」、③ ワンクリック詐欺疑似体験スマートフォン専用 Web サイト「お〜る動画」、④ ワンクリック詐欺疑似体験アプリ「お〜るプレイヤー」の 4 つの要素で構成した.

スマートフォン情報モラル解説 Web サイト「スマホモラル」は、4 コマまんが風の解説サイトで、A4 用紙に印刷もできるようにレイアウトを工夫した解説教材である (図 1). ② スマートフォン情報モラル解説スマートフォン専用 Web サイト「スマホモラル for スマホ」は、①「スマホモラル」の内容をまとめ、スマートフォン用にレイアウトを整えた解説教材である. また、③ ④ の教材への目次の役割も担っている. 以下に、中心教材である ③ ④ について、それぞれ、3.3 と 3.4 節で解説する.

なお、「詐欺アプリに気をつけよう」のほかに、「パケット代は定額に」、「アプリの利用」、「個人情報がたくさん」、「カメラ機能の利用」、「Wi-Fi (無線 LAN) の利用」についての解説教材も開発した.

表 2 開発環境および動作環境
Table 2 Development environment and operating environment.

	Androidアプリ	解説Webサイト	
		コンピュータ画面向け	スマートフォン画面向け
開発環境	Android SDK 2.1 Eclipse 3.7 JDK 7.0.10	Adobe Dreamweaver CS5.5	
		HTML5	
		CSS3	
		jQuery Mobile 1.0	
動作環境	Android 2.1以降を搭載した、スマートフォン	HTML5およびCSS3対応インターネットブラウザ	



図 1 スマホモラル印刷イメージ
Fig. 1 SPM printing image.



図 2 疑似体験 Web サイト
Fig. 2 Simulation learning Web site.



図 3 ダウンロードページ
Fig. 3 Download web page.

3.3 疑似体験 Web サイト

疑似体験 Web サイトは、不正なアプリをインストールさせられてしまうまでの過程を体験できるように、教材にストーリー性を持たせた. リアリティを高めるために、既知のワンクリック詐欺サイトを参考にした [6].

疑似体験 Web サイトは、最新の映画やアニメなどの動画を見ることのできるサービスサイトを模している (図 2). 動画を再生するプレイヤーのダウンロードとインストールは無料であるが、多額の利用料が請求される体験ができるようにした. サイト上から、再生アプリを選択することにより、動画プレイヤーをインストールできるようにしている (図 3). トップページからは、ほかに、お知らせ、最新動



図 4 権限許可画面

Fig. 4 Screen shot of permission.

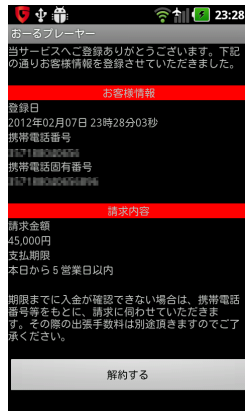


図 5 請求画面

Fig. 5 Screen shot of demand payment.

画、動画ランキングにアクセスできるようになっているが、すべて、再生アプリをダウンロードするように誘導する構成にした。

また、従来型携帯電話ユーザを狙ったワンクリック詐欺サイトについても学習できるように、その仕組みを利用したワンクリック詐欺疑似体験 Web サイトを、スマートフォンの画面で表示させる際に最適となるようにデザインして開発した。なお、この疑似体験 Web サイトは、iPhone用の教材としても利用できる。

3.4 疑似体験アプリ

疑似体験アプリは、Android スマートフォンで動作するネイティブアプリである。

疑似体験 Web サイトと連動した、動画を再生するためのプレーヤを模している。解説 Web サイトに示す方法により、Android スマートフォンにインストールされる。このアプリの実行には、「携帯のステータスと ID の読み取り」のみの許可が必要となり、インストール時に、許可を要求される (図 4)。なお、前述のとおり、安全な状況下で疑似体験をできる仕様、教育の場における倫理の観点から検討した仕様のため、「ネットワーク通信」の許可を要求していない。疑似体験アプリを実行すると、図 5 に示す請求画面が表示される。また、アプリの起動時には携帯電話番号を送信しているメッセージが表示されるようにした。

請求画面の表示項目は、① 登録日、② 携帯電話番号、③ 携帯電話固有番号、④ 請求金額、⑤ 支払期限であり、これらの情報をもとに請求にうかがうといった脅し文句で、支払いを促す文章を表示させた。また、⑥ 解約するボタンを用意し、これをクリックすると解説画面が表示されるようにした。① 登録日、② 携帯電話番号、③ 携帯電話固有番号は、アプリの機能により取得され、インストールしたスマートフォン固有の情報が表示される。

これらの機能を持つ疑似体験アプリを利用することで、学習者は、携帯電話番号が抜き取られる危険性を実感する

とともに、インストール時に動画再生ソフトに本当に電話番号の読み取りを許可する必要があるかどうかを判断する体験ができる。

なお、疑似体験アプリは、筆者が用意した Web サーバ上から配信しているため、本アプリを動作させるには、提供元不明のアプリのインストールを許可する必要がある。体験後に、「提供元不明アプリのインストールを禁止する設定にすること」、「原則として公式マーケットのアプリのみを利用すること」、「『ネットワーク通信』を許可してしまうと取得された電話番号などの情報が送信される危険性があること」、「個人情報を取られた場合、解約するボタンを押しても、高額な解約解除料を請求され、請求の脅しから逃れることができないこと」などをあわせて指導する必要がある。

4. 本教材を利用した研修会における教員の評価

平成 24 年 10 月に A 教育委員会主催の「ネットモラル」研修会において、本教材を用いて小中高の教員 18 名へ研修を行った。その結果、サイトへのアクセス、疑似体験アプリのダウンロード、インストール時の許可する権限の確認画面の表示、インストール、アプリを実行した際に自分のスマートフォンの電話番号が表示される画面の確認まで、スムーズに行うことができた。

研修会後に実施したアンケート調査では、参加者 18 名中 14 名からの回答が得られた。「従来型携帯電話とは異なる注意点があること」、「アプリのインストール時に求められる項目をよく確認する必要があること」、「不正なアプリで個人情報を抜き取られてしまう可能性があること」、および「4 コマまんが」について 14 名すべての教員からよく理解ができる教材であると評価を得られた。「解説プリントに書かれている内容」については、14 名中 12 名（無回答 1 名）の教員からよく理解ができる教材であると評価が得られた。

「体験教材を児童生徒の指導に使ってみたいか」については、14 名中 12 名（無回答 1 名）の教員から使ってみたいとの評価が得られた。使ってみたいと思わないと答えた理由として、「中学生以上では有効」などの回答が得られた。

以上のことから、教員研修会で利用できることを確かめることができたとともに、教育現場の教員から一定の評価を得ることができたといえる。

5. まとめ

本研究をとおり、電話番号が表示される新たな危険性に対応したスマートフォンアプリ型ワンクリック疑似体験教材を開発することができた。

今後、この安全にワンクリック詐欺を疑似体験できる教材を活用した授業や講座を実施し、効果を検証したい。

謝辞 教材開発に関わり，ご協力いただいた方に謹んで感謝の意を表する．また，本研究の一部は，JSPS 科研費（基盤研究 C：研究課題番号：22500943，研究代表長谷川元洋）の助成を受けて行われた．

参考文献

- [1] 新谷洋介，長谷川元洋：携帯電話のインターネット機能の特性を考慮した情報モラル教材の開発と授業実践，日本教育工学会第 23 回全国大会講演論文集，pp.657–658 (2007).
- [2] 新谷洋介：情報モラルをやってみよう，OCT くとと学ぼう（オンライン），入手先 <http://oct-kun.net/ktaimoral/>（参照 2013-05-23）.
- [3] 三田正巳：携帯電話を利用した「情報モラル」指導実践について，日本教育工学会第 24 回全国大会講演論文集，pp.121–124 (2008).
- [4] Sky 株式会社：SKYMENU Pro Ver.11 2009 年 6 月 22 日（オンライン），入手先 <http://www.skygroup.jp/news/090622/>（参照 2013-05-23）.
- [5] 日本電気株式会社：UNIVERGE ケータイ de モラル ソリューション（オンライン），入手先 <http://www.nec.co.jp/univerge/solution/pack/moral/>（参照 2013-05-23）.
- [6] Symantec：日本人を狙う，スマートフォンアプリを使ったワンクリック詐欺（オンライン），入手先 <http://www.symantec.com/connect/blogs-244>（参照 2013-05-23）.
- [7] 朝日新聞：ネット関連会社を捜索 スマホ情報流出でアプリ作成者特定へ，2012 年 05 月 18 日夕刊 1 社会 (2012).
- [8] 情報処理推進機構：コンピュータウイルス・不正アクセスの届出状況 [1 月分] について（オンライン），入手先 <http://www.ipa.go.jp/security/txt/2011/02outline.html>（参照 2013-05-23）.



新谷 洋介 （正会員）

北海道高等聾学校.



長谷川 元洋 （正会員）

金城学院大学.