Androidを対象とした利用者の意図しないWebサイトの分類

利穂 虹希[1]　折戸 凜太郎[1]　佐藤 将也[1]　山内 利宏[1]

概要：モバイル端末が普及している現代において，モバイル版 Web ブラウザの利用率は PC 版 Web ブラウザの利用率を上回っている．また，モバイル端末が普及するにつれて，モバイル端末を対象とした悪性サイトが増加している．その中でも，利用者の意図しない Web サイトにリダイレクトによって誘導する手口が増加している．また，このような Web サイトの中には，Android にマルウェアをインストールさせることが目的の悪性 Web サイトや，詐欺が目的の悪性 Web サイトがある．利用者の意図しない Web サイトについて調査を行うことで，悪性 Web サイトの検知が容易になる．悪性 Web サイトには，Web サイトの構造が似ているにも関わらず違う Web サイトとして異なるドメインをもつものや，同一の Web サイトに異なるドメインで接続されるものなど様々な種類がある．我々はこれらについて分類を行った．本稿では，発見した悪性 Web サイトとその分類について報告する．

キーワード：Android，悪性 Web サイト，Web ブラウザ，Web 媒介型攻撃

Unwanted Web Site Classification for Android

Koki Riho[1]　Rintaro Orito[1]　Masaya Sato[1]　Toshihiro Yamauchi[1]

Abstract: As the spread of mobile devices, mobile web browsers have been used rather than desktop and the number of mobile malware cases has increased. In addition, with the spread of mobile devices, malicious websites for mobile devices are increasing. Especially, redirection to unwanted websites increases. The purpose of the above websites vary as follows: induction to install malicious apps or phishing. Surveying the unwanted websites will help us to detect malicious websites. There are various types of malicious websites, such as websites with similar structure but different domains as different websites, and websites with different domains connected to the same website. In this paper, we report the detected malicious websites and their classifications.

1. はじめに

モバイル版 Web ブラウザの利用率が PC 版 Web ブラウザの利用率を上回るほどモバイル端末が普及している [1]．また，モバイル端末が普及するにつれて，モバイル端末を対象とした悪性 Web サイト（以降，悪性 Web サイト）が増加している [2]．悪性 Web サイトに利用者を誘導する方法には，Web サイトを閲覧した際に意図しないリダイレクトによりページを遷移させるものがある．利用者の意図しない Web サイトの中には，広告を目的としたものや有料サービスの登録を促すような間接的な被害を与えるものだけでなく，金銭的被害を与えることやマルウェアのインストールなど直接的な被害を与えるものがある．モバイル向け Web サイトを利用した攻撃手法について研究がなされているものの，Web サイトのデザインや構造に注目して分類を行った研究は，我々の調査した限り不十分である．利用者の意図しない Web サイトについて，Web サイトの目的やデザインに注目して分類を行うことで，異なるドメインを持っていても，デザインが同じ Web サイトや，偽の警告画面を表示する Web サイトの特徴を認識でき，悪性

[1] 岡山大学 大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University

表 1　調査環境

Android 端末	Pixel2
Android バージョン	Android 6.0
ブラウザ	Google Chrome 67.0.3396.87

Web サイトを検知するために有用な情報が得られる可能性がある．本稿では利用者の意図しない Web サイトを目的別に分類し調査した結果を報告する．

2. 関連研究

悪性 Web サイトを判定するための研究として，文献 [3], [4] がある．文献 [3] では，ドメインの登録日に注目することで，悪性 Web サイトであるか判定する手法を提案している．文献 [4] では，Web サイトの被リンク数と URL の属性情報から，悪性 Web サイトを判定する手法を提案している．これらの文献は，スマートフォンを対象とはしていない．

スマートフォンを対象とした利用者の意図しない Web サイトに着目した研究として，文献 [5], [6], [7] がある．文献 [5], [6] では，意図しないタップを誘発することで，利用者の意図しない操作が行われるように仕組まれた Web サイトの対策を行っている．文献 [7] では，QR コードを悪用する攻撃に対策をしている．

Android を対象とした悪性 Web サイトに関する研究は少ない．この理由は，Android を対象とした悪性 Web サイトについての調査が不十分なためである．Android を対象とした利用者の意図しない Web サイトの分類に関する研究については，我々が調査した限りでは見つからなかった．我々は，このような Web サイトについて調査を行い，36 件の Web サイトを発見し，分類を行った．

3. 悪性 Web サイトの調査方法

Android Studio 3.4.1 により，Pixel2 のエミュレータを用いて調査を行った．調査環境を**表 1** に示す．利用者の意図しない Web サイトの調査を行うために，利用者の意図しない Web サイトへページ遷移する Web サイトを調査した．この結果，利用者の意図しないページ遷移を引き起こす入り口サイトとして，複数の無料動画共有サイトを用いた．これらの利用者の意図しないページ遷移が発生する画面の例を**図 1** に示す．Web サイト (A) は利用者が動画共有サイトに訪れ，初訪問時に Web サイトの任意の場所をタップすることで，利用者の意図しないページ遷移が発生する．Web サイト (B) は動画の再生ボタンをクリックすることで，利用者の意図しないページ遷移が発生する．このような無料動画共有サイトに，表 1 に示した環境を利用してアクセスし，利用者の意図しないページ遷移を発生させ，最終的な遷移先の Web ページについて，Web サイトの URL，発見した日時，Web サイトのスクリーンショット，および遷移元の Web サイトの情報を記録した．1 週間あたり 4 時間の調査を 3 ヶ月行った．

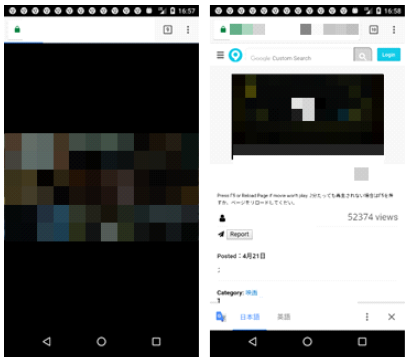


図 1　利用者の意図しないページ遷移が発生する画面

表 2　発見した Web サイトのまとめ

Web サイトの目的	発見した数（件）
他の Web サイトへの誘導	8
金銭の獲得	17
通知権限の獲得	6
アプリのインストール	3
広告の表示	2
合計	36

また，利用者の意図しないページ遷移が発生する Web サイトについて，日本語の他に韓国語で調査を行なった．我々が発見した Web サイトでは，韓国語の映像作品がアップロードされており，動画の再生ボタンをタップすることで，利用者の意図しないページ遷移が発生した．

これらの Web サイトを利用して発見した利用者の意図しない Web サイト 36 件について分類を行った．

4. 目的別 Web サイトの分類

4.1 発見した Web サイト

表 2 に 3 章で述べた調査により発見した Web サイトを目的別に分類した結果を示す．Web サイトは 5 種類に分類でき，金銭を得ることが目的の Web サイトが 17 件と最も多い結果となった．

(1) 他の Web サイトへの誘導
(2) 金銭の獲得
(3) 通知権限の獲得
(4) アプリのインストール
(5) 広告の表示

4.2 他の Web サイトへの誘導が目的の Web サイト

他の Web サイトに誘導することが目的の Web サイトとして，Web サイト自体に何も表示されず，画面遷移のみの Web サイトや，「loading...」と書いてある画像を表示する Web サイト，アンケート形式の Web サイトを発見した．これらの Web サイトはそれ自体が目的ではなく，中継サ

イトのようなものだと考える．アンケート形式の Web サイトは，利用者にアンケートを繰り返し，最後まで回答すると，出会い系サイトの入会画面へページ遷移する．それ以外の Web サイトは，どのような規則で利用者の意図しない Web サイトに誘導するか不明である．偽の警告画面を表示する Web サイトや，広告目的の Web サイトなど，様々な Web サイトにページ遷移する．

4.3 金銭の獲得が目的の Web サイト

金銭を得ることが目的の Web サイトとして，入金することで有利になるゲームの Web サイト，入金することで女性からのメッセージを閲覧することができる出会い系サイト，偽の懸賞当選画面を表示する Web サイト，イラストや写真を使うことで利用者を刺激して，会員制の Web サイトへの入会を促す Web サイトを発見した．

また，利用者にクレジットカード情報の入力を求める Web サイトが多かった．このため，クレジットカード情報の悪用が目的である可能性もある．

4.4 通知権限の獲得が目的の Web サイト

スマートフォンに通知の許可を要求する Web サイトを発見した．利用者が通知を許可した場合，Google Chrome を通じて，出会い系サイトに登録している女性からメッセージが来たように見せるもの，育毛剤の広告，政治に関するある新聞の記事，およびブログの記事の広告などが通知に表示された．たとえば，女性からのメッセージをタップすると，出会い系サイトの登録画面や出会い系サイトを紹介しているブログに遷移した．

4.5 アプリをインストールさせることが目的の Web サイト

スマートフォンにウイルスが侵入していると偽の警告画面を表示して，ウイルスを削除するためのアプリをインストールさせようとする Web サイトを発見した．これらの Web サイトの中には，利用者の使っている端末の情報を画面に表示することで，利用者の不安を煽る Web サイトも発見した．

4.6 広告の表示が目的の Web サイト

ダイエット食品やゲームアプリの広告が目的の Web サイトを発見した．これらの Web サイトは，実在する商品の広告を行っていた．

5. 分類した Web サイトの詳細

以降では，4 章で分類した Web サイトごとの詳細を述べる．

表 3 他の Web サイトにページ遷移することが目的の Web サイトのまとめ

Web サイトの内容	発見した数（件）
アンケート形式	6
Loading の文字を表示	1
画面遷移のみ	1

表 4 金銭の獲得が目的の Web サイトのまとめ

Web サイトの内容	発見した数（件）
出会い系サイト	6
ゲームサイト	6
偽の当選画面を表示する Web サイト	5

5.1 他の Web サイトに誘導することが目的の Web サイト

他の Web サイトに誘導することが目的の Web サイトの分類を**表 3** に示す．他の Web サイトにページ遷移することが目的である Web サイトは，以下の 3 種類計 8 件を発見した．

(1) アンケート形式
(2) Loading の文字を表示
(3) 画面遷移のみ

アンケート形式の Web サイトは，1 回以上アンケートを行い，最後まで回答すると出会い系サイトの登録画面にリダイレクトする Web ページのデザインやドメインが異なるにも関わらず，タイトルが同一の Web サイトも確認した．なお，この Web サイト間では，アンケートの内容も同じであった．アンケートを行うことで，利用者を煽り，出会い系サイトに登録させることが目的であると考える．遷移先の出会い系サイトは 5.2.1 項に記述している．

Loading の文字を表示する Web サイトは「Loading...」と表示されるページが表示された後に他の Web サイトに遷移する．

画面遷移のみの Web サイトは何も表示されずに URL だけが切り替わる．これらの Web サイトの遷移先の Web サイトは様々であり，傾向の把握はできていない．

5.2 金銭の獲得が目的の Web サイト

金銭の獲得が目的の Web サイトの内容ごとに発見した数を**表 4** に示す．金銭の獲得が目的である Web サイトは，以下 3 種類の計 17 件を発見した．

(1) 出会い系サイト
(2) ゲームサイト
(3) 偽の当選画面を表示する Web サイト

5.2.1 出会い系サイト

出会い系サイトは計 6 件を発見した．**図 2** に出会い系サイトの画面を示す．Web サイト (A-2) および (B-2) の画面を比較すると，タブの配置，デザイン，タブを開いた画面が同じである．この他にも，相手を探すための画面や登録

図 2　出会い系サイトの画面

されている他のユーザの情報も同じであった．また，この出会い系サイトは，Web ページを開いてから数分待つと，女性からメッセージが大量に届く点も同じであった．

これらの Web サイトは，初訪問時にユーザ登録を行う．この際に，メールアドレス，パスワード，ユーザの住所（市まで），ユーザの性別，出会いたい対象の性別を登録する．登録した情報を元に，他のユーザからメッセージが届く．他のユーザがアップロードした写真を閲覧する操作や女性から届いたメッセージを閲覧する操作を行おうとすると，入金を要求する画面に遷移する．しかし，新規登録を行う度に同じユーザからメッセージが届くことや，登録したばかりのアカウントに 10 通以上のメッセージが届くことから，他のユーザからのメッセージが自動的に送信されている可能性が高い．

いずれの Web サイトも，Web サイトのタイトルやドメインは異なる．しかし，デザインや，Web サイトの構造が同じであることから，同一の組織によって製作されている可能性がある．Web ページの IP アドレスを調べると，6 件の出会い系サイトはそれぞれ異なる IP アドレスであった．

5.2.2　ゲームサイト

Web サイトの内容ごとに発見した数を**表 5** に示す．ゲームサイトは以下 4 種類の計 6 件を発見した．

(1) デザインが似ているゲームサイト
(2) キャラクタのイラストを使うゲームサイト
(3) スロットゲームを用意するゲームサイト
(4) カジノ形式のゲームサイト

表 5　ゲームサイトのまとめ

Web サイトの内容	発見した数（件）
デザインが似ているゲームサイト	2
実在する作品のイラストを利用するゲームサイト	2
スロットゲームを用意するゲームサイト	1
カジノ形式のゲームサイト	1

図 3　デザインが似ているゲームサイトの画面

図 3 にデザインが似ているゲームサイトの画面を示す．これらの Web サイトは，Web サイトのタイトルは異なるものの，入金することでプレイ可能なカジノ形式のゲームを提供している点が同じである．出会い系サイトとは異なり，トップページのデザインが異なる．しかし，Web サイト (A) と (B) において，メニューバーのデザインやメニューのアイコンとして利用されている画像など，細かい点で似ている箇所がある．IP アドレスを調べると，2 件のゲームサイトはそれぞれ異なる IP アドレスであった．

デザインが似ているゲームサイトの他にも，日本のアニメーション作品やゲーム作品のキャラクタを利用したゲームサイトを発見した．キャラクタのイラストを見るためには入金が必要であった．また，スロットゲームを Web サイト内に用意しており，スロットで当たりを出すことで，カジノ形式のゲームサイトへ入会ボーナス付きで入会することができる Web サイトも発見した．このカジノ形式のゲームサイトは，図 3 で示した 2 つのゲームサイトとはデザインが異なる．

5.2.3　偽の当選画面を表示する Web サイト

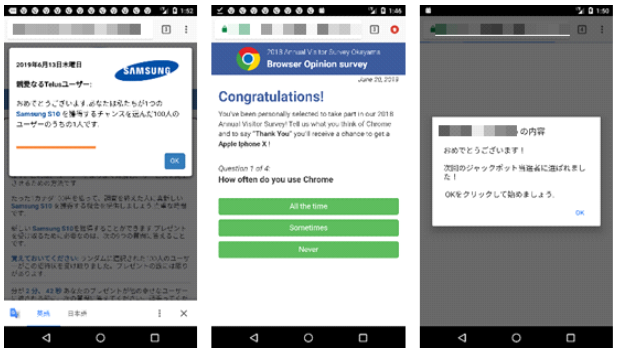
Web サイトの内容ごとに発見した数を**表 6** に示す．ゲームサイトは以下 3 種類の計 5 件を発見した．

(1) 実在する企業の名前やロゴを使用
(2) Google Chrome のアイコンを使用
(3) スロットゲームを用意するゲームサイト

図 4 に偽の当選画面を表示する Web サイトの画面を示す．Web サイト (A) は，実在する企業の名前やロゴを使用しており，Web サイト (B) は Google Chrome のアイコンを使用している．これらの Web サイトは，偽の当選画面を表示した後にアンケートを表示する．アンケートの内容

表 6　偽の当選画面を表示する Web サイトのまとめ

Web サイトの内容	発見した数（件）
実在する企業の名前やロゴを使用	3
Google Chrome のアイコンを使用	1
偽の当選を知らせるダイアログ表示	1



Webサイト(A)　Webサイト(B)　Webサイト(C)

図 4　偽の当選画面を表示する Web サイトの画面

は，Google Chrome の使用頻度など様々なものがある．全てのアンケートに回答すると，商品を発送するための送料を請求され，クレジットカード情報の入力を求められる．クレジットカード情報の悪用が目的である可能性もある．Web サイト (C) は当選ダイアログを表示した後に，振り込み手数料を請求される．

アンケートを行う目的は不明である．しかし，利用者が Google Chrome の使用頻度などについて答えることで，当選したという情報を利用者に信じさせることが目的であると考える．

5.3　通知権限の獲得が目的の Web サイト

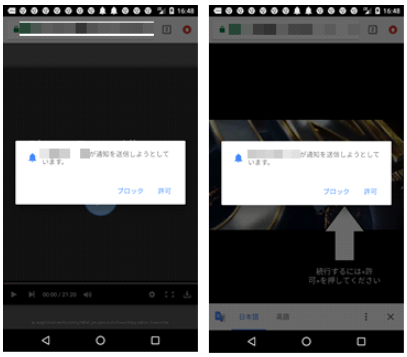
通知権限の獲得が目的の Web サイトの内容ごとに発見した数を**表 7** に示す．通知権限を要求する Web サイトは 2 種類計 6 件を発見した．

図 5 に通知権限を要求する Web サイトの画面を示す．これらの Web サイトは訪問すると利用者に通知権限を要求するダイアログを表示する．Web サイト (A) は，「Just one more step— “Allow” to continue」といった通知の許可を求める文章を表示する．Web サイト (B) は，通知を許可することで動画が再生可能であるように思わせるデザインの Web サイトである．なお，通知を許可した場合も拒否した場合も，別の通知権限を要求する Web サイト，もしくは他の利用者の意図しない Web サイトにページ遷移した．

通知を許可すると，Android 端末に個人ブログの広告や，女性からメッセージが届いたように見せて通知をタップすると出会い系サイトに遷移するもの，育毛剤の広告，チャットアプリのアカウントの URL，およびある新聞の政治に関する記事など様々な通知が届いた．通知内容と Web サイトの関連性については調査を行なっていない．

表 7　通知権限の獲得が目的の Web サイトのまとめ

Web サイトの内容	発見した数（件）
動画投稿サイトのようなもの	4
通知の許可を促す文章	2



Webサイト(A)　Webサイト(B)

図 5　通知権限を要求する Web サイトの画面

表 8　アプリをインストールさせることが目的の Web サ イトのまとめ

Web サイトの内容	発見した数（件）
Google のロゴを表示	1
Google のキャラクタを表示	1
アプリのアイコンを表示	1

Webサイト(A)　Webサイト(B)　Webサイト(C)

図 6　偽の警告画面を表示する Web サイトの画面

5.4　アプリをインストールさせることが目的の Web サイト

アプリをインストールさせることが目的の Web サイトの内容ごとに発見した数を**表 8** に示す．アプリをインストールさせることが目的の Web サ イトは 3 種類計 3 件を発見した．

これらの Web サイトは，端末がウイルスに感染していると利用者に警告し，ウイルスを削除するためのアプリケーションのインストールを促す．**図 6** に偽の警告画面を表示する Web サイトの画面を示す．Web サイト (A) および (B) は Google のロゴを表示する Web サイトや Google のキャラクタを表示して，利用者の端末がウイルスに感染していると警告する．これらの Web サイトは公式のロゴや

表 9　広告の表示が目的の Web サイトのまとめ

Web サイトの内容	発見した数（件）
ダイエット商品の広告	1
ゲームのタイトルを表示	1

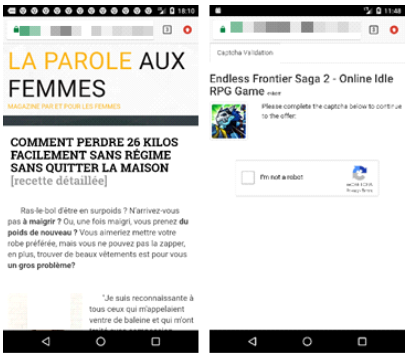


図 7　広告が目的の Web サイトの画面

キャラクタを利用することで，利用者の不安感を煽り，利用者がアプリケーションをインストールするように誘導することが目的である．Web サイト (A) は，利用者の使用する端末の情報を抜き出し，警告画面の生成に利用している．Web サイト (C) はインストールさせたいアプリケーションのアイコンを表示する Web サイトである．アイコンを表示することで，利用者にアプリケーションのアイコンを記憶させる目的があると考える．

5.5　広告の表示が目的の Web サイト

広告の表示が目的の Web サイトの内容ごとに発見した数を**表 9** に，**図 7** に広告が目的の Web サイトの画面を示す．広告の表示が目的の Web サイトは 2 種類計 2 件を発見した．Web サイト (A) はダイエット食品の広告である．この Web サイトはフランス語のサイトであり，使用者の感想と商品の購入ボタンが表示される．Web サイト (B) は，ゲームアプリの名前とアイコンの表示のみで，実際のインストール画面に遷移することはなかった．ゲームの名前とアイコンを利用者に覚えさせることが目的であると考える．

6.　おわりに

Android を対象とした利用者の意図しない Web サイトについて調査を行い，36 件の Web サイトを 5 種類の目的別に分類し，その詳細を述べた．調査結果より，我々が発見した利用者の意図しない Web サイトは，他の Web サイトに誘導することが目的の Web サイトを除く以下の 4 種類の目的の Web サイトに遷移することがわかった．

(1) 金銭の獲得
(2) 通知権限の獲得
(3) アプリのインストール
(4) 広告の表示

本稿では，Web サイトの名前は異なるにも関わらず，デザインが同じ Web サイトを複数件発見したこと，同じ目的の異なる Web サイトを複数件発見したことを報告した．このことから，Web サイトのデザインや目的に注目して悪性 Web サイトの検知を行うことができると考える．

今回発見した Web サイト以外にも，利用者の意図しない Web サイトは存在する．たとえば，SNS を利用して利用者の意図しない Web サイトに誘導する例を発見している．このため，さらに調査を続ける必要がある．また，利用者の意図しない Web サイトは，戻るボタンをタップすることで利用者の意図しない他の Web サイトにページ遷移する．ページ遷移する Web サイト同士の関係についても調査し，傾向を分析することで悪性 Web サイトの対策を行うことができる．

謝辞　本研究成果の一部は，国立研究開発法人情報通信研究機構 (NICT) の委託研究「Web 媒介型攻撃対策技術の 実用化に向けた研究開発」により得られたものです．

参考文献

[1] McAfee LLC: McAfee Mobile Threat Report Q1,2018, available from 〈https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf〉(accessed 2019–08–05).
[2] Wandera: 4 ways hackers are infiltrating phones with malware on Android phone, available from 〈https://www.wandera.com/malware-on-android/〉(accessed 2019–08–05).
[3] 福島 祥郎，堀 良彰，櫻井 幸一：ドメイン情報に着目した悪性 Web サイトの活動傾向調査と関連性分析，情報処理学会シンポジウム論文集 (情報処理学会ワークショップ論文集)，Vol.2010，No.9，pp.759–764 (2010).
[4] 佐藤 祐磨，中村 嘉隆，高橋 修：通信遷移と URL の属性情報を用いた悪性リダイレクト防止手法，コンピュータセキュリティシンポジウム 2015 論文集，Vol.2015，No.3，pp.8–15 (2015).
[5] 向山 浩平，藤田 真浩，白井 丈晴，小林 真也，西垣 正勝：Slyware 対策：意図しないタップを誘発する Web サイトの対策に関する考察，マルチメディア，分散協調とモバイルシンポジウム 2016 論文集，Vol.2016，pp.387–395 (2016).
[6] 向山 浩平，藤田 真浩，白井 丈晴，西垣 正勝：Slyware 対策：意図しないタップを誘発する Web サイトの脅威とその対策に関する研究，情報処理学会論文誌，Vol.59，No.12，pp.2166–2179 (2018).
[7] Yao, H., Shin, D.: Towards preventing QR code based attacks on android phone using security warnings, Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, pp.341–346 (2013).