L-026

# Android 向けセキュリティアプリにおける悪性 Web サイト検知率の調査
# Research on Malicious Website Detection Rate of Android Security Application

折戸 凜太郎 Rintaro Orito
佐藤 将也 Masaya Sato
山内 利宏 Toshihiro Yamauchi

## 1. はじめに

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 [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マルウェアの感染に繋がる Web サイト（以降，悪性 Web サイト）が増加している [2]．このため，モバイル端末における Web アクセスは高い安全性が求められる．

Android において，Web サイトを閲覧するために，Web ブラウザアプリおよびアプリ内ブラウザが利用されている．また，これらのブラウザを用いて Web サイトを閲覧する際に，悪性 Web サイトへの Web アクセスを検知する方法として，Web ブラウザに標準搭載されているセキュリティ機能やセキュリティアプリを用いる方法がある．しかし，これらの機能やアプリは，適用できるブラウザが異なる．また，それぞれの機能やアプリの悪性 Web サイト検知率は明らかではない．

本稿では，Google Safe Browsing（以降，GSB），および 2 つのセキュリティアプリの悪性 Web サイト検知率を調査した結果を述べる．また，悪性 Web サイト検知率の調査結果をもとに，適用するセキュリティ機能やセキュリティアプリによる Web アクセスの安全性の違いを述べる．

## 2. Android における Web を経由した攻撃

モバイル端末を対象としたマルウェアが急激に増加している．これらのマルウェアは，Web を経由して Android 端末へ導入されることが多い．Android 端末へは，Web を経由して秘密裏にソフトウェアをインストールさせることはできない．このため，Web 上で虚偽の情報を表示し，ユーザを欺くことで，ユーザが同意したうえで不正ソフトウェアをインストールさせる手法が増加している [2]．この手法の代表例として，フィッシングサイトおよび偽警告画面を表示する Web サイトがある．

## 3. 悪性 Web サイト検知率の調査

### 3.1 目的

2 章で述べたように，Android 端末への Web サイトを経由した攻撃が存在する．このため，Web サイトを閲覧する際，悪性 Web サイトを検知することでユーザを保護することが重要となる．また，悪性 Web サイトへの Web アクセスを検知し，ユーザを保護することを目的として，多くのセキュリティ機能やセキュリティアプリが開発されている．このため，これらの機能やアプリを用いることで，2 章で述べた攻撃へ対処できる可能性がある．しかし，Android には様々なブラウザが存在する．また，ブラウザごとに適用できるセキュリティ機能やセキュリティアプリが異なる．さらに，それぞれの機能やアプリの悪性 Web サイト検知率は明らかではない．このため，ユーザがより安全に Web サイトを閲覧する方法を選択することは難しい．

そこで，2 章で述べたフィッシングサイトおよび偽警告画面を表示する Web サイトを検知対象として，GSB および 2 つのセキュリティアプリにおける悪性 Web サイト検知率を調査した．

### 3.2 調査方法

ブラウザが利用可能なセキュリティ機能である GSB，および Google Play においてユーザ満足度が高い 2 つのセキュリティアプリ（以降，アプリ A とアプリ B）の悪性 Web サイト検知率を調査した．各セキュリティ機能の悪性 Web サイトを識別する手法，および適用できるブラウザを以下に示す．

**Google Safe Browsing**
ブラウザが HTTP リクエストを送信する前に，その URL をブラックリストと比較する．悪性と判断された場合，その Web アクセスを防止する．また，同様の手法を用いて，Web サイトに埋め込まれている悪性 Web サイトの URL に対する Web アクセスも防止する．GSB は，Google Chrome，Firefox およびアプリ内ブラウザである Chrome Custom Tabs と WebView に適用できる．

**アプリ A**
ブラウザが HTTP リクエストを送信する前に，要求された URL のセキュリティリスクを評価するために，Web セキュリティデータベースサーバへ問い合わせを行う．そこで，要求された URL を評価する値として評価スコアを算出する．この値が定義された閾値を超えない場合，その URL を悪性 Web サイトと判断し，Web アクセスを防止する．この手法に，URL ブラックリスト方式を組み合わせる．また，同様の手法を用いて，Web サイトに埋め込まれている悪性 Web サイトの URL に対する Web アクセスも防止する．アプリ A は，Google Chrome や Firefox などの多くのブラウザアプリに適用できる．また，特定のアプリにおいて，アプリ内ブラウザである Chrome Custom Tabs に適用できる．

**アプリ B**
Web サイトへ Web アクセスするごとに，アクセス先の URL と URL ブラックリストを比較する．その URL を悪性と判断した場合，その Web アクセスを検知する．アプリ B は，アクセス先の URL を

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 評価環境

| | |
|---|---|
| Android 端末 (Nexus 6P) | Android 6.0 |
| Google Chrome | 71.0.3578.98 |

表 2 悪性 Web サイト検知率

| | GSB | アプリ A | アプリ B |
|---|---|---|---|
| フィッシングサイト（100 件） | 34% | 90% | 5% |
| 偽警告画面（20 件） | 0% | 65% | 0% |

悪性と判断した場合，警告を表示するのみであり，Web アクセスは防止しない．アプリ B は，アプリ A と同様の多くのブラウザアプリに適用できる．

悪性 Web サイト検知率を調査するために，フィッシングサイト (100 件) と偽警告画面を表示する Web サイト (20 件) を用いた．フィッシングサイトは，Web サイト [3][4] 上で開発者や研究者向けに無償で公開されている悪性 Web サイトのデータセットより収集し，調査を実施した 2018 年 12 月 19 日時点で最新の 100 件を利用した．偽警告画面を表示する Web サイトは，同様のデータセットから 2018 年 12 月 19 日時点で最新の Web サイト (5 件)，および独自に発見した Web サイト (15 件) を検知対象とした．データセットに加えて，独自に Web サイトを収集したのは，偽警告画面を表示する Web サイトに関する分析や対策を実施している先行研究が少なく，上記のようなデータセットであっても公開されている件数が少ないためである．

調査には表 1 の環境を用いた．調査では，Google Chrome を用い，3 つの機能のうち，1 つのみを有効にした状態で検知対象に Web アクセスし，検知の有無を確認した．

### 3.3 調査結果

調査結果を表 2 に示し，以下で説明する．

**フィッシングサイト**

フィッシングサイトの検知率は，アプリ A が 90%と高い．次に，GSB が高いものの，34%と低い．また，アプリ B は，5%と極めて低い．

**偽警告画面**

偽警告画面を表示する Web サイトの検知率は，アプリ A が 65%と十分ではない．また，GSB とアプリ B は，検知できるものはなかった．

この結果より，以下のことが分かる．

(A) アプリ A は，GSB やアプリ B と比較して検知精度が高い．これは，評価スコアを用いる方式と URL ブラックリストを組み合わせているためだと考えられる．

(B) GSB とアプリ B は，どちらも URL ブラックリスト方式を採用しているものの，GSB の方が検知率が高い．これは，ブラックリストの作成方法の違いによると推察できる．表 2 より，アプリ B が用いる URL ブラックリストには，今回用いたデータセットに含まれるフィッシングサイトがほとんど含まれないことが分かる．

(C) GSB およびアプリ B が偽警告画面表示する Web サイトを検知できない理由として，この攻撃方法が複雑であり，URL ブラックリスト方式のみでは対応できない可能性がある．または，偽警告画面を表示する Web サイトを検知の対象としてサポートしていない可能性がある．

### 3.4 ブラウザによる Web アクセスの安全性

アプリ A は，ユーザ利用率の高い Google Chrome や Firefox などのブラウザに適用できる．また，特定のアプリにおいて，アプリ内ブラウザである Chrome Custom Tabs にも適用できる．このため，アプリ A を用いることで，多くのブラウザにおいて，比較的安全に Web サイトを閲覧できる．

一方，アプリ B は，アプリ A と同様に多くのブラウザに適用できるものの，今回の調査で検知対象とした 2 種類の悪性 Web サイトの検知率は低く，これらの悪性 Web サイトへの対策としては期待できない．

GSB は，Google Chrome，Firefox およびアプリ内ブラウザである Chrome Custom Tabs と WebView に適用できる．また，今回評価に利用したセキュリティアプリと併用できる．GSB は，WebView に適用できる唯一のセキュリティ機能であるものの，3.3 節の評価結果では，GSB の悪性 Web サイト検知率は低い．このため，WebView において安全に Web サイトを閲覧するためには，GSB に加えて，有効な対策を検討する必要がある．

## 4. おわりに

Android における Google Safe Browsing，および 2 つのセキュリティアプリについて，悪性 Web サイト検知率の調査結果を述べた．また，この調査で得られた結果から，ブラウザによる安全性の違いを示し，WebView において有効な対策を検討する必要性を述べた．

**謝辞** 本研究成果は，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 2019-06-04).

[2] Wandera: 4 ways hackers are infiltrating phones with malware on Android phones, available from 〈https://www.wandera.com/malware-on-android/〉 (accessed 2019-06-04).

[3] OpenPhish: Timely. Accurate. Relevant Threat Intelligence., available from 〈https://openphish.com/〉 (accessed 2018-12-19).

[4] OpenDNS: PhishTank Out of the Net, into the Tank., available from 〈http://www.phishtank.com/phish_archive.php〉 (accessed 2018-12-19).