スマートフォン向けWeb媒介型サイバー攻撃観測機構を用いた潜在的リスクのあるアプリ追跡に関する報告

三村 隆夫[1,a)]　梅本 俊[1]　中嶋 淳[1]　巻島 和雄[1]　岩本 一樹[1]

概要：近年，スマートフォンのセキュリティに関する啓蒙活動が継続的に行われる一方，スマートフォンに対する攻撃手法の巧妙化も指摘されている．攻撃に対して適切に対処するためには，その実態を把握することが重要である．我々は，Web 媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive）において提案，設計・実装された攻撃観測システムを用いて，Android スマートフォンに対する Web 媒介型攻撃の調査を実施した．この攻撃観測システムは，WarpDrive でのユーザ参加型の実証実験において稼働しているものであり，実験に参加する Android スマートフォン端末から情報を収集する仕組みとなっている．調査により，リスクが報告されるファイルが埋め込まれ正規版とは異なる証明書で署名されたリパッケージアプリ，および，宅配系の偽アプリを配布すると考えられる Web サイトの痕跡情報を確認した．本稿では，潜在的にリスクがある Android アプリの発見・追跡を主目的とする調査の結果について報告する．

キーワード：Web 媒介型攻撃，スマートフォン，Android，リパッケージ

A Report of Tracing Potentially Risky Apps by Using the Framework for Monitoring Web-based Attacks Targeting Smartphone

Takao Mimura[1,a)]　Shun Umemoto[1]　Jun Nakajima[1]　Kazuo Makishima[1]　Kazuki Iwamoto[1]

Abstract: While recent effort to make smartphone users conscious of security is taking place, the sophistication of attacks against smartphones has been reported. The observation of such attacks is important to appropriate defense. We have performed an analysis using the framework for monitoring web-based attacks targeting smartphone, which has been proposed and designed/implemented in WarpDrive (Web-based Attack Response with Practical and Deployable Research InitiatiVE). The framework has been used for an experiment with voluntary participants and gathers various information from the Android device of each participant. Our analysis has found a repackaged app with an embedded file which was deemed risky and some signs of web pages distributing fake Android apps. In this paper, we report the result of the analysis that primarily focuses on discovering and tracing risky Android apps.

Keywords: Web-based Attacks, Smartphone, Android, Repackage

1. はじめに

近年，スマートフォンに対する攻撃手法の巧妙化が指摘されている [1], [2], [3]．新種のマルウェアについても，定期的に一定数は発見される傾向が統計データで報告されている [4]．

Android に対するサイバー攻撃事例として，SMS（ショートメッセージ）を経由した不正アプリへの誘導の増加が報告されている [5]．この事例では，不正アプリが正規に提供されているとユーザに誤認させることで攻撃を達成できる容易さがあり，報告件数の増加要因になっていると考えられる．インストールされたアプリは，所与の権限内において任意の処理を実行可能であり，アンインストールされるまで動作を継続する．したがい，不正な意図を目的として

[1] 株式会社セキュアブレイン
SecureBrain Corporation
[a)] *takao_mimura@securebrain.co.jp*

作成されたアプリは，インストールされることで永続性を持つ実際的な脅威となりえる．

我々は，ソーシャルネットワーク（SNS）で情報共有され，インターネット上で配布される Android アプリ（APK，Android PacKage）に対する研究を行っている．先行研究 [6], [7] では，Twitter を対象とする調査により，リスクが認められる多数の APK に関する情報共有が行われている実態を示した．この調査では，既存のアプリに改変を加えるリパッケージと呼ばれる手法が適用された APK を発見し，アプリが表示する広告の追加や削除，特定サイトへの誘導といった改変事例を確認した．

本研究では，Web 媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive: Web-based Attack Response with Practical and Deployable Research InitiatiVE）[8] において提案，設計・実装された攻撃観測システムを用いて，Android スマートフォンに対する Web 媒介型攻撃の観測を実施した．この攻撃観測システムは，WarpDrive でユーザ参加型の実証実験において稼働しているものであり，実験に参加する Android スマートフォン端末から情報を収集する仕組みとなっている．先行研究では，Twitter での情報共有されインターネットで配布される APK に関する分析を実施したのに対して，本研究では，ユーザ参加型実験データを調査・分析することでリスクのある APK 利用の実態を明らかにすることを目的とする．実態の把握については，対策技術の研究開発における必須要素という側面もある．調査・分析の結果，危険性が報告されるファイルが埋め込まれたリパッケージアプリ，および，偽サイト配布を行うと考えられるサイトへの誘導の痕跡を確認した．

本稿は，以下のように構成する．2 章では，WarpDrive の概略，利用するデータ種別，ならびに分析対象とする実証実験データセットについて説明する．3 章では，観測結果について述べる．4 章では，観測結果に関する考察を行う．5 章では，実証実験データのさらなる活用に向けた検討を試みる．6 章では，関連研究について述べる．最後に，7 章では本稿のまとめを行う．

2. WarpDrive

2.1 実証実験の概要

WarpDrive とは，Web 媒介型攻撃の実態把握と対策技術の向上を行うための産学連携の研究開発プロジェクトである．本プロジェクトでは，PC 版およびモバイル版としてユーザ参加型の実証実験を行っており，それぞれ Windows/macOS，Android スマートフォンが対象である．各プラットフォーム向けにデータ収集用プログラムを配布し，実験参加者の協力のもとに各種データの収集を行い，インターネット上に設置された分析基盤において調査・分析を実施している．

モバイル版実証実験向けのデータ収集用プログラム [9] は，タチコマ・セキュリティ・エージェント・モバイル（タチコマ SA）という名称の Android アプリとして実装され，Google Play で配布されている．タチコマ SA を Android スマートフォンにインストールし，実証実験に関する規約およびプライバシーポリシーに同意したユーザがモバイル版実証実験の参加者となり，そのスマートフォン端末からデータ収集が行われる．

表 1 利用データ一覧

項目名	概要
Web アクセス履歴	
種類	取得元アプリを示す識別子（Chrome, ChromeCustomTabs，PWA）
日時	データ取得時の日付・時間
URL	アクセス先の URL
タイトル	アクセス先 Web ページのタイトル
AMP	AMP（Accelerated Mobile Pages）かどうか
タブ識別子	タブを区別するための文字列
タブの数	現在開かれているタブの数
リンクテキスト	ハイパーリンクの表示文字列
バージョン	Google Chrome のバージョン
インストールアプリ一覧	
日時	データ取得時の日付・時間
パッケージ名	アプリのパッケージ名
表示名	アプリの表示名
バージョン	アプリのバージョン
インストール日時	アプリのインストール日時
最終更新日時	アプリの最終更新日時
インストール元パッケージ	対象アプリのインストール処理を行ったアプリのパッケージ名
パーミッションの一覧	要求しているパーミッション一覧
ハッシュ値	APK のハッシュ値
同梱ファイルの一覧	APK に同梱されているファイル一覧（ファイルパス，種別，ハッシュ値）
証明書情報	証明書に関する情報
構成要素の一覧	構成要素（コンポーネント）の一覧
SMS のメッセージに含まれる URL とメッセージのハッシュ値	
送信者のハッシュ値	送信者情報から算出されたハッシュ値
メッセージの種類	送信，受信，不明のいずれか
メッセージのハッシュ値	メッセージ本文のファジーハッシュ値
URL リスト	メッセージに含まれる URL の一覧
受信日時	メッセージの受信日時
表示日時	メッセージの表示日時
パッケージ名	収集対象 SMS アプリのパッケージ名
バージョン	SMS アプリのバージョン
端末情報	
日時	データ取得時の日付・時間
SDK バージョン	SDK バージョン
ABI 一覧	サポートしている ABI の一覧
製品名	端末のメーカーや製品の名前
モデル名	端末のモデルの名前
パッチレベル	セキュリティパッチレベル

2.2 利用データ種別

タチコマ SA が収集するデータ種別は，実証実験のデータ取扱規約として明記されており，Web サイト [8] での確認も可能である．

本稿で分析に用いたデータ種別は，Web アクセス履歴，インストールアプリ一覧，SMS のメッセージに含まれる URL とメッセージのハッシュ値，端末情報である．それぞれに含まれる内容を**表 1** に示す．ただし，SMS については，実証実験参加者のプライバシー保護を目的として，メッセージに URL が含まれる場合に収集の対象となる．

2.3 実証実験データセット

本稿では，2020 年 3 月 16 日から 2020 年 6 月 21 日にかけて収集された実証実験データ（実証実験データセット）を分析対象としている．実証実験データセットにおいて，分析対象となる実証実験の参加者数は 1,425 である．なお，この参加者数については，タチコマ SA の利用規約に同意し端末情報の送信が確認された件数であることに注意されたい．

Android OS バージョン

実証実験参加端末における Android OS バージョンの分布を**図 1** に示す．2020 年 8 月時点での最新バージョン（Android 10.0），およびその一世代前のバージョン（同 9.0）により，実験参加者の約 83%と大多数を占めている．一方，2015 年 10 月にリリースされ Android Open Source Project（AOSP）での最新リリースが 2017 年 10 月である Android 6.0[10] の利用者も約 2%存在する．

Android アプリ

実証実験データセットには，ユニークな APK（Android Package）として 111,360 件, パッケージ種類としては 20,665 件のアプリ情報が含まれている．

本稿では，APK に対する評価として，VirusTotal File Report（FR）[11] を利用している．APK ファイルのハッシュ値を基準として，評価結果が利用可能な 68,636 件の VirusTotal FR を取得した．VirusTotal FR が利用可能な APK 群では，パッケージ種類数は 16,038 である．

VirusTotal FR による評価結果としては，検知なしが 67,028 件（97.7%），検知あり（検知数 1 以上）が 1,608 件（2.3%）であった．後者の検知ありグループについて，APK ごとの検知数の傾向を**図 2** に示す．検知数 1 が 1,294 件（80.5%）と大部分を占めているが，検知数が 10 以上についても 26 件（1.6%）と一定数確認されている．なお，検知あり APK 群に含まれるパッケージ種類数は，1,034 件である．VirusTotal FR での検知とは，各セキュリティベンダがユーザに対して警告すべき対象とみなしているものであり，以下，本稿では検知数が 1 以上の APK を要注意 APK と呼ぶ.

3. 実証実験データセットの分析

3.1 インストール元パッケージ

インストール元パッケージとは，APK のインストール処理を実行したアプリのパッケージ名であり，APK の出所を示す情報として利用可能である．一例として，Google Play からインストールされたアプリの場合，*com.android.vending* となる．本稿では，パッケージ名が *com.android.packageinstaller*，または，*com.google.android.packageinstaller* であるインストール元パッケージを標準パッケージインストーラと呼ぶ.

インストール元パッケージ別に集計したアプリの要注意割合を**表 2** に示す．要注意割合とは，APK インストール件数に対する要注意 APK 数の割合であるが，インストール件数が少ないと数件の要注意 APK により高い数値が算出されることになる．ここではそれらを除外するため，要注意 APK が 10 件以上確認されているインストール元パッケージを集計対象とした．集計の結果，要注意 APK 割合の高いインストール元パッケージとして，標準パッケージインストーラおよび Package Installer A が確認された．

対象が少数であることから表 2 には含まれていないが，要注意 APK のインストールのみが記録されたインストール元パッケージとして，11 種類が確認されている．これらのインストール元パッケージでは，それぞれ 1 件の要注意 APK のインストールが記録されていた．

本実証実験データセットで確認された 1,608 件の要注意 APK のうち，Google Play からのインストールは 898 件，それ以外のインストール元パッケージからのインストールは 727 件であった．Google Play およびそれ以外でのインストール元パッケージによりインストールされた APK 群について，2 つの集合 A，B の類似度を $\frac{|A \cap B|}{|A \cup B|}$ により示す Jaccard 係数を用いて評価すると，0.01（積集合に出現する APK 数は 17）であった．

要注意 APK のパッケージ種類数 1,034 件のうち，Google Play からのインストールに出現するパッケージ種類数は 552 件，それ以外のインストール元パッケージからのインストールでは 513 件であった．インストール元パッケージ（Google Play およびそれ以外）によるパッケージ種類群に関する Jaccard 係数は，0.03（積集合に出現するパッケージ種類数は 31）であった．

3.2 リパッケージアプリ

リパッケージアプリとは，既存の APK の一部を改変することで作成されるアプリである．人気のゲームやアプリをリパッケージした事例が報告されている．我々の先行研究 [6] では，リパッケージにより広告の追加や削除，特定

*1 組織名を含む一部名称は Package Installer A-C としている

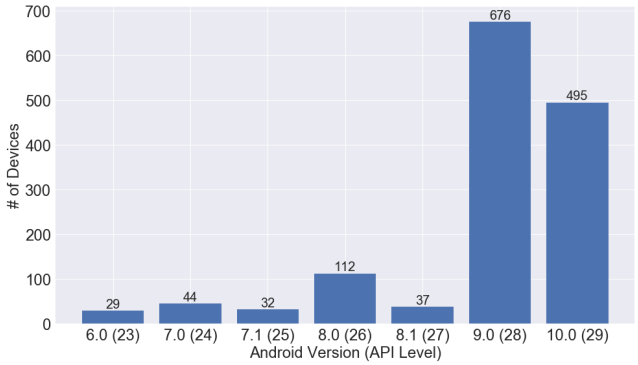

図 1　Android OS バージョンの分布

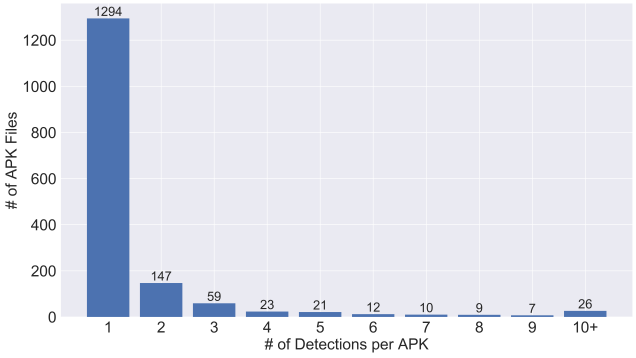

図 2　VirusTotal FR における検知数の傾向（検知数 1 以上）

表 2　インストール元パッケージ別の要注意 APK 割合

インストール元パッケージ*1	APK		要注意	備考
	件数	要注意数	割合	
com.android.packageinstaller	107	24	22.4%	標準パッケージインストーラ
com.google.android.packageinstaller	868	113	13.0%	標準パッケージインストーラ
Package Installer A	156	17	10.9%	機種変更時のデータ移行用アプリ
Package Installer B	422	14	3.3%	特定通信キャリア向けインストーラアプリ
Package Installer C	557	17	3.1%	特定端末メーカー向けインストーラアプリ
com.android.vending	38,125	898	2.4%	Google Play
Empty	27,280	487	1.8%	パッケージ名取得結果が空文字列となったケース，adb（Android Debug Bridge）の利用時，プリインアプリでの該当例を確認

サイトへ誘導する実装が追加された事例を確認している．

リパッケージアプリ分析を実施するため，*(a)* パッケージ名が一致する *(b)* 証明書が一致しない *(c)* バージョンが一致する *(d)* Google Play からインストールされた APK が存在する，という条件全てに一致するアプリ情報を抽出した．

実証実験データセットでは，上記条件に合致する APK の組み合わせが複数抽出された．この組み合わせより，意図的に APK のコンポーネントおよび構成ファイルの改変が行われたと考えられるリパッケージアプリの事例を一件確認した．これ以外の組み合わせでは，リパッケージに起因する実質的な差分は確認されなかった．

事例：ゲームアプリのリパッケージ

本項では，日本のゲームメーカが有料で提供するアクションゲームに対して行われたリパッケージ事例を示す．以下では，リパッケージに対する差分として，アプリのコンポーネント，APK に含まれるファイル，パーミッション，証明書に関する比較結果を示す．なお，コンポーネントとは，Android アプリのマニフェスト（AndroidManifest.xml）で定義される部品であり，代表例として Activity や Service がある．

アプリコンポーネントの差分として，正規版に含まれる一部コンポーネントの削除が確認されている．以下に，削除されたコンポーネント名を示す．なお，これらのコンポーネント名に含まれるパッケージ名については，対象アプリのパッケージ名を示すものではないことに注意されたい．

- *activity/com.google.android.gms.auth.api .signin.internal.SignInHubActivity*
- *activity/com.google.android.gms.common.api .GoogleApiActivity*
- *meta-data/com.google.android.gms.games.APP_ID*
- *service/com.google.android.gms.auth.api .signin.RevocationBoundService*

正規版 APK には 138 ファイル（ファイルハッシュ値ベースでは，137 ファイル），リパッケージ版 APK には 142 ファイル（同 142 ファイル）が含まれている．正規版，リパッケージ版に含まれるファイルを Jaccard 係数による比較では，ファイルパスを基準とすると 0.34（一致数は 71），ハッシュ値ベースでは 0.24（同 54）であった．ファイルパス，ハッシュ値がともに一致するファイルとして，22 件が確認された．

本事例では，Java/Kotolin 言語で記述されるアプリ本体である classes.dex のハッシュ値は，正規版，リパッケージ版で異なっていた．C++言語等で記述され，ネイティブライブラリとして lib 以下に格納される共有ライブラリのハッシュ値は一致していた．

assets ディレクトリには，以下のファイルが追加されていた．

- *assets/lib*****.so*[*2]
- *assets/lib*****_a64.so*
- *assets/lib*****_x86.so*
- *assets/.appkey*

拡張子.so を持つファイルは，ELF フォーマットの共有ライブラリであることが確認されている．.appkey については，その内容は判明していない．追加された ELF ファイルのうち，*lib*****.so* については，VirusTotal FR による評価において，以下の名称で検知されていた．

- *AdLibrary:Generisk*
- *a variant of Android/Packed.*****.D potentially unsafe*
- *Trojan.*****.Android.332*[*3]

パーミッション宣言については，正規版，リパッケージ版における差分は確認されなかった．

APK の署名に利用された証明書については，ハッシュ値だけでなく，設定内容においても差異が確認されている．正規版の証明書では，Subject DN（Distinguished Name），Issuer DN に会社名，住所情報が設定されていた．一方，リパッケージ版の証明書では，Subject DN，Issuer DN にアプリのクラックグループを意味する単語を組み合わせた文字列が用いられていた．

Twitter での共有されるリパッケージアプリ情報

追加調査により，Twitter において前述のリパッケージ事例と同じ名前のアプリに関する情報が共有されていることを確認した（**図 3**[*4]）．このツイートでは，配布サイトと考えられる URL とともに，このアプリがリパッケージを意味する改造版（MOD）であり，かつ無料（free）だとする主張が含まれている．

当該ツイートには，Bitly を利用した短縮 URL が含まれており，ツイートを行ったユーザ名を含むドメイン名の URL に関連付けられていた．調査目的で当該 URL へのアクセスを行ったところ，HTML 形式のファイルがダウンロードされたが，APK への直接的な URL は確認されなかった．したがい，実証実験データセットで確認されたリパッケージアプリと同一であるかは確認されていない．

3.3 偽アプリ配布サイトの痕跡

昨今，宅配系の偽アプリを配布するサイトへの誘導を目的とする SMS の存在が指摘されている [5]．ソーシャルネットワーク（SNS）やニュースサイトで事例が報告されている他，宅配事業者からの注意喚起も行われている．

実証実験データセットでは，偽アプリ配布サイトと推定

*2 英語ではない言語と思われる単語が用いられており，作成者に関する推測を避けるため一部を非表示とする
*3 セキュリティベンダの報告により特定の国との関連が示唆されているため一部を非表示とする
*4 情報の共有目的ではないため一部非表示とする

図 3 Twitter でのリパッケージ事例アプリに関するツイート

されるドメイン名を含む URL が Web アクセス履歴および SMS メッセージ履歴に含まれることを確認した．以下に，確認された URL を示す[*5]．

- *http://jp****-bbo[.]top*
- *http://jp****[.]top*
- *http://jp****-mu[.]top*
- *http://jp****-to[.]cc*

上記 URL について，WarpDrive 実証実験により可能な範囲で配布コンテンツ取得を試行した．ここでは，2 件の URL に対して調査目的でのアクセスを行なったが，一方は接続先ドメインの名前解決に失敗，他方はドメインが売り出し中であることを示す HTML コンテンツが取得される結果となった．偽アプリについては，拡張子.apk を持つファイルでの配布事例が報告 [5] されている．取得した HTML コンテンツでは，APK へのリンクを示す情報は確認されなかった．

3.4 インターネット配布 APK

Web アクセス履歴より，APK 配布を目的とすると考えられる Web サイトに対するアクセス記録を確認した．これらには，リパッケージと考えられる改造版（Mod）APK の配布を行うとするサイトも含まれていた．以下に，これらの Web サイトのドメイン名を例示する[*6]．

- ****mix[.]com*
- ****snake[.]com*
- ****award[.]com*

*5 セキュリティ上の理由により一部非表示とする
*6 情報共有目的ではないため，一部非表示とする

```
"access type": "Chrome",
"date": "2020/03/26 12:04:15",
"date url transition": "",
"exclude type": "",
"url": "[redacted].com/file/cfiles/gcm1/GCam_5beta6.200105.0445build-7.2.018.apk",
"is amp": false,
```


図 4　Web アクセス履歴の例


```
"package name": "com.google.android.GoogleCamera",
"label name": "カメラ",
"version": "5beta6.200105.0445build-7.2.018",
"install date": "2020/03/26 12:05:42",
"last update date": "2020/03/26 12:05:42",
"install market": "com.google.android.packageinstaller",
```


図 5　アプリ情報の例

事例：インターネット配布 APK のインストール

インターネットで配布される APK について，端末へインストールされたと考えられる事例を示す．なお，ここでは，実証実験データセットを用いることにより，一定の条件付きながら APK インストールが追跡可能であることを示すことが目的であり，当該 APK の悪性を示すものではない．

まず，Web アクセス履歴により，APK 配布 URL へのアクセスが行われたことが示されている（図 4）．次に，インストールアプリ一覧により，取得された APK と考えられるアプリのインストールが示されている（図 5）．ここでは，*(a)* APK 配布 URL におけるパスの拡張子が.apk である *(b)* 同 URL のパスからアプリバージョンと推定される文字列が含まれかつそれがインストール情報と一致する *(c)* APK インストール日時が当該 URL へのアクセス直後であることから，ダウンロードされた APK がインストールされたと判断しているが，あくまで推測であることに注意されたい．

4.　考察

4.1　インストール元パッケージ

実証実験データセットでは，標準パッケージインストーラおよび Package Installer A によりインストールされた APK の要注意割合が高いことが確認された．

標準パッケージインストーラでは，任意の APK をインストールすることが可能である．今回，Web アクセス履歴では，APK 配布を目的とすると考えられるサイトへのアクセスが確認されている．さらに，先行研究により，Twitter で情報共有され，インターネットで配布される APK の要注意割合が高いことが確認されている（先行研究におけるデータセットでの要注意 APK 割合は，文献 [6] では APK33,350 件に対して 42.3%，文献 [7] では同 66,996 件に対して 47.8%）．したがい，標準パッケージインストーラによりインターネットで配布される APK がインストールが行われており，これが標準パッケージインストーラにおける要注意 APK 割合の上昇要因となったことが考えられる．

Package Installer A については，端末のデータ移行用アプリであり，移行元端末にインストール済みアプリが処理対象になると考えられる．したがい，ここでの要注意 APK 割合については，標準パッケージインストーラと同様に，実証実験の参加者がインストールしたアプリに依存することに注意されたい．

一方，Package Installer B，C，Google Play については，上記と比較すると相対的に低い要注意割合であった．Google Play では，Google Play Protect[12] と呼ばれる取り組みにおいてセキュリティ検査が行われている．Package Installer B，C のインストール対象となるアプリについても，端末メーカー，通信キャリアにおいて相応の管理が行われていると推測される．これらの要因により，前述のインストール元より低い要注意 APK 割合になったと考えられる．

要注意 APK のインストールのみが確認されたインストール元パッケージでは，インストールされたアプリはそれぞれ一種類であった．これらの詳細については不明だが，アプリパッケージ名に成人向けコンテンツと思われる文字列が含まれ，かつ，インストール元パッケージとして標準パッケージインストーラと当該アプリパッケージが記録されているケースを確認した．状況としては，インターネットで配布される APK が標準パッケージインストーラでインストールされ，アップデート版がアプリに実装されたインストール機能でインストールされたものと推定される．

4.2　リパッケージアプリ

本稿で示したリパッケージ事例では，コンポーネントが削除され，共有ライブラリが追加されていた．削除されたコンポーネント名は，パッケージ名より Google モバイルサービスに関連し，Google Play での配布を前提とする処理で利用されていたと考えられる．追加された共有ライブラリは，VirusTotal FR の検知名より，アドライブラリに関連すると推測される．状況を整理すると，有料アプリとして配布されるゲームソフトに改造を行うことで料金を支払わずに利用可能とし，アドライブラリを追加することで本来の権利者の利益を窃取した可能性が示唆される．

なお，本リパッケージ事例では，classes.dex のハッシュ値が異なることが確認されている．実証実験データでは，コンポーネントやファイルの追加や削除，相違の有無の確認はできるが，classes.dex ファイルの差分を特定することはできないことに注意されたい．

本稿でのリパッケージ抽出では，Google Play で配布されるアプリの証明書を正規版判定の条件として利用する．日本国内での Google Play の利用状況を考慮すると，Android アプリの開発者は，Google Play でアプリを公開することが一般的だと考えられるためである．同一パッケージ名で異なる証明書が利用されている場合，そのアプリの作成者

は Google Play 公開版とは異なり，そのどちらか一方はリパッケージ版の可能性がある．ただし，人気のある一部アプリの開発者は，独自に運営するストアにおいて異なる証明書で署名したアプリを配布することがある．また，一部のストアでは，ストアの運営者によりアプリが再署名される仕様であることが知られている．本稿での抽出方法では，上記に該当する場合，False Positive が発生することに注意しなければならない．今回の調査では，抽出されたデータを個別に精査することで，複数の正規版証明書に該当する組み合わせを除外した．しかし，人手での確認には限界があるため，機械的な判定を行うことが求められる．

なお，リパッケージにおける正規版判定とは，本質的にアプリ作成者の同一性に関するものである．良性，悪性判定とは異なる指標であり，Google Play で配布されるアプリの非悪性を示すものではない．アプリユーザ視点では，リパッケージにおける本質的なリスクは，改造により追加，改変された実装に潜在する．ここで，正規版の実装による悪影響の有無については，スコープ外であることに注意されたい．

Web アクセス履歴では，Twitter での追加調査で発見された改造版 APK 配布が目的だと思われるサイトと同じドメイン名（TLD は，.com）の URL が 3 件確認されている．確認された URL では，forum や ja，short というホストを含む FQDN となっており，パスは含まれていなかった．一方，ツイートで確認された URL では，ホスト名を含まない FQDN となっており，パスに game という単語やこのゲーム名と思われる文字列が含まれていた，したがい，Web アクセス履歴で確認されたアクセスについては，ユーザフォーラムや日本語ユーザ向けトップページを参照するものと考えられる．なお，Web アクセス履歴については，実証実験データセットに含まれていたことを示すものであり，特定ユーザとの関連を示すものではないことに注意されたい．

本稿でのリパッケージ事例については，Twitter で確認したツイートの日付は 2020 年 3 月上旬，リパッケージ事例アプリのインストール日時は 3 月下旬，タチコマ SA によるデータ収集は 5 月中旬であった．実証実験データセットに含まれる情報では，本リパッケージアプリの取得元を特定することはできなかった．しかし，前述のツイート情報は一般公開されており，検索エンジン等を経由したアクセスは容易であること，さらに実証実験の参加者という限られたグループにおいて改造版 APK 配布を主張するサイトへのアクセス履歴が存在することから，Twitter の情報共有を起点としてリパッケージ版のインストールに至った可能性はあると考える．

4.3 偽アプリ配布サイトの痕跡

実証実験データセットおよび追加調査では，3.3 節で示したように，実証実験の参加者向けに配信されたコンテンツは取得できなかった．実証実験データは 2020 年 3 月に生成されたのに対して，コンテンツ追加調査の実施は同年 7 月から 8 月であることから，追加調査前に当該 URL での配信が終了したと考えられる．

実証実験データセットには，Web アクセス履歴に含まれる URL で配信されるコンテンツを特定する情報は含まれていない．しかし，今回のケースでは，抽出された URL のドメイン名およびトップレベルドメインが宅配系事業者による偽アプリ配布サイトに関する注意喚起に一致することもあり，偽アプリ配布サイトであった可能性が高いと考えられる．

4.4 インターネット配布 APK

実証実験データより，APK 配布を目的とすると思われるサイトへのアクセス，インターネット配布 APK のインストール事例について示した．上記のようなサイトへのアクセスが確認されていることから，4.1 節で述べたように，インターネットで配布される APK については，一定の利用実態があるものと考えられる．

5. WarpDrive データ活用に向けた考察

本章では，WarpDrive 実証実験データのさらなる活用に向けた考察，試案を示す．

リパッケージアプリでは，APK の署名に用いられる証明書が作成者の真正性判定における重要な要素である．リパッケージアプリが攻撃に利用される文脈では，アプリの魅力を攻撃のターゲットに訴求する必要があり，多数のユーザが利用する人気のアプリは有力な候補になると考えられる．意図的なリパッケージアプリが配布され，一部の実証実験参加者が手違いでインストールしたとすると，分析基盤には，多数の正規版証明書情報，および，少数のリパッケージ版証明書情報が蓄積されることになる．ここで，個別の証明書情報だけでは，直接的にリパッケージ版証明書に問題があると判断することはできないことに注意されたい．同一パッケージ名で異なる証明書が存在し，一方は多数，他方は少数の場合，前者の方が信頼性があると考えられる．異なる証明書で署名された正規版アプリが別のストアで配布される場合でも，本来のストアで配布されるアプリのユーザ数に準ずる件数の証明書情報が蓄積されることが期待される．したがい，証明書情報の定量的評価，および，時系列情報（証明書情報の初出日時等）を併せることにより，正当な証明書を推定できる可能性があると考える．

インターネット配布 APK には相対的に高いリスクが認められることから，Web アクセス履歴から APK 配布 URL を追跡できることが望ましい．一般的なユースケースとして，Android スマートフォンユーザが APK をダウンロー

ドした場合，それほど間隔を開けずにインストールを行うものと思われる．この場合，APK が配信される URL へのアクセス時間とインストール日時が時系列的に近接することが期待される．したがい，標準パッケージインストーラによるアプリインストールを起点として，その直前にアクセスが行われた URL 群に対する調査を行うことにより，APK 配布 URL を発見できる可能性があると考える．

4.4 節で述べたように，収集された実証実験データに対して，タイムリーな対応が必要なケースが存在する．近年，フィッシングサイトの存続期間の短縮化が指摘 [13] されていることもあり，偽アプリ配布サイトにおいても Google Safe Browsing[14] に代表されるブロックリストでの検知を回避するため，生存期間が短縮化していると思われる．このようなコンテンツを取得するためには，クローキング対策と併せて調査目的でのアクセスを自動化することが有効だと考える．また，これによりコンテンツの取得が可能となれば，URL およびコンテンツを特徴量とする機械学習モデルによる偽アプリ配布ページの推定という方向への発展も可能だと考えられる．

6. 関連研究

リソースの類似性を利用するリパッケージ検知手法を提案する関連研究を先行研究 [6] で示している．他の関連研究として，[15], [16] が挙げられる．金井ら [15] は，検証用のコードをアプリに埋め込む実験によりアプリがリパッケージ適用可能であることを示し，自動リパッケージ対策の必要性を指摘している．秋本ら [16] は，Apache Cordova で作成される HTML5 ハイブリッドアプリについて，リパッケージによるプラグインの不正利用に対する防御手法を提案している．

7. おわりに

本稿では，WarpDrive モバイル版実証実験データセットを用いて，潜在的にリスクがある Android アプリの発見，追跡を目的とする調査を実施した．調査により，セキュリティベンダによって危険性が指摘されるファイルがリパッケージによって埋め込まれたアプリ，および，偽アプリ配布サイトに関する確度の高い痕跡を発見した．併せて，要注意割合が高いインターネット配布 APK が標準パッケージインストーラにより利用されている傍証を示した．以上より，本研究の目的とするリスクあるアプリ発見については，上記リパッケージ事例により達成した．一方，直接的な配布 URL の特定には課題が残っており，この解決には適切なタイミングでのコンテンツ取得が必要である．

WarpDrive 実証実験により収集されるデータ量は，増加する一方である．本稿では，手動による調査が中心であったが，分析を補完する外部データとの突合を含めて，定量的，機械的に実施可能とすることが課題として挙げられる．

謝辞 本研究は，国立研究開発法人情報通信研究機構の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」の成果の一部です．ご協力いただいた皆様に，深く感謝します．

参考文献

[1] IPA: 情報セキュリティ 10 大脅威 2020（2020）．入手先 ⟨https://www.ipa.go.jp/files/000080871.pdf⟩（参照 2020-08-19）．
[2] ESET: ANDROID BANKING MALWARE: SOPHISTICATED TROJANS VS. FAKE BANKING APPS（2019）．
[3] Lookout: SECURITY RESEARCH REPORT Monokle（2019）．
[4] McAfee: McAfee Labs Threat Report August 2019（2019）．
[5] IPA: 情報セキュリティ白書 2019（2019）．
[6] 三村 隆夫，巻島 和雄，岩本 一樹，“ソーシャルネットワークで共有される Android アプリケーションの実態調査，” コンピュータセキュリティシンポジウム 2018 論文集,2018(2),113-120
[7] 三村 隆夫，巻島 和雄，岩本 一樹，“Twitter で共有される Android アプリケーション配布ページの実態調査および検知手法の検討，” コンピュータセキュリティシンポジウム 2019 論文集,2019,1148-1155 (2019-10-14)
[8] WarpDrive 入手先 ⟨https://warpdrive-project.jp/⟩（参照 2020-08-19）．
[9] 山田 明，佐野 絢音，窪田 歩，嶌田 一郎，中嶋 淳，吉岡 克成，瀬尾 浩二郎，満保 雅浩，佐藤 将也，松村 礼央，田辺 瑠偉，小澤 誠一，田中 翔真，梅本 俊，松田 壮，山内 利宏，澤谷 雪子，“スマートフォンにおける Web 媒介型サイバー攻撃の観測機構：設計と実装，”2020 年暗号と情報セキュリティシンポジウム（SCIS2020）論文集 (01, 2020)
[10] Android Open Source Project: Codenames, Tags, and Build Numbers 入手先 ⟨https://source.android.com/setup/start/build-numbers⟩（参照 2020-08-19）．
[11] VirusTotal: Getting started 入手先 ⟨https://developers.virustotal.com/reference⟩（参照 2020-08-19）．
[12] Google: Google Play Protect 入手先 ⟨https://developers.google.com/android/play-protect⟩（参照 2020-08-19）．
[13] Akamai: 2019 年インターネットの現状／セキュリティ：フィッシング - 罠を仕掛ける詐欺師たち（2019）．
[14] Google: Google Safe Brwosing 入手先 ⟨https://safebrowsing.google.com/⟩（参照 2020-08-19）．
[15] 金井 文宏, 庄田 祐樹, 橋田 啓佑, 吉岡 克成, 松本 勉．Android アプリケーションの自動リパッケージに対する耐性評価．情報処理学会論文誌,Vol.56,No.12,2275–2288(Dec. 2015)
[16] 秋本 裕史，岸 知二．Cordova ハイブリッドアプリケーションにおけるプラグインに着目したリパッケージング攻撃の防御手法．第 82 回全国大会講演論文集,2020,77-478