Computer Security Symposium 2018
22 - 25 October 2018

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

三村 隆夫[1,a)]　巻島 和雄[1]　岩本 一樹[1]

概要：スマートフォン向け OS である Android では，公式ストア以外からアプリをインストールすることが可能であり，不正アプリを不注意に導入してしまうリスクが指摘されている [1]．スマートフォンの普及とともにインターネット上のコミュニケーションではソーシャルネットワーク（SNS）が幅広く利用されており，知り合いだけでなく不特定多数と任意の話題に関する情報交換が行われている．SNS はコミュニケーションツールとして有用ではあるが，匿名利用者による不適切な情報発信に代表されるように，やりとりされる情報の取り扱いには注意が必要である．そこで本稿では，匿名利用が可能な SNS のひとつである Twitter で共有される Android アプリ情報を収集し，その特徴や危険性に関する実態を報告する．

キーワード：SNS，Android，リパッケージ，サードパーティマーケット

A study of Android applications shared in Social Network Services

Takao Mimura[1,a)]　Kazuo Makishima[1]　Kazuki Iwamoto[1]

Abstract: Android, a smart phone OS, allows users to install apps distributed outside the official app store, which poses the risk of illegitimate apps to be installed accidentally by careless users. The wide spread of smart phones has accelerated the use of social network services (SNS). It enables communication in various topics among not only acquaintances but also the general public. Although SNS is a useful communication tool, one must pay attention to communications there, as anonymous users can disseminate inappropriate information. In this study, we report features and danger of information and Android apps that are shared on Twitter, an SNS which accepts anonymous users.

Keywords: SNS, Android, repackage, third party market

1. はじめに

近年，スマートフォンの爆発的な普及およびそれに伴う SNS の利用増加が報告されている [2]．

スマートフォン OS の一つである Android 向けには，Google が運営する公式ストア Google Play において多数のアプリが配布されている．悪性なアプリが報告されることもあるが [3]，Google によって Bouncer[4] と呼ばれるマルウェア検知機構が運用されており，安全性を向上させる取り組みが行われている．

インターネット上では Google Play 以外でも Android 向けアプリが多数配布されている．既定の設定では Google Play 以外からのアプリインストールはできないが，ユーザが許可することは可能である．Google Play 以外の配布経路としては，Amazon が運営するアプリストア [5] や開発者による直接配布 [6] などがある．

Android アプリの配布とは，技術的にはアプリケーションパッケージ（APK）を端末にダウンロードさせることであり，Web サーバでの配信により容易に実現可能である．組織的に運営されるマーケット以外では，Bouncer に代表されるセキュリティ検査を行うことは現実的に困難であり，サードパーティマーケットで配布される APK の危険

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

性が報告されている [7].

また，SNS の利用増加により，インターネット上のコミュニケーションが活発化している．SNS の一つである Twitter では，#記号と文字列を組み合わせたハッシュタグ [8] と呼ばれる機能があり，会話のトピックを明示することができる．特定トピックに興味を持つユーザと積極的に情報共有できるため，発信側，受信側ともに利用されている．Android アプリに関するツイートについてもアプリ名称を利用したハッシュタグを用いた更新情報の通知やプロモーション目的の情報共有が行われている．

加えて，Twitter では複数のアカウントを作成することが可能であり，コミュニケーションの相手や内容を使い分けることによりインターネット上で完結する任意の人格として振る舞うことが可能となる．よって，インターネット特有の匿名性による不適切な行動 [9] やフィッシング等のサイバー攻撃に利用される事例 [10] が報告されている．

SNS では円滑なコミュニケーションや効率的な情報収集が可能な反面，近年社会問題となっているフェイクニュース [11] に例示されるようにやりとりされる情報の取り扱いには注意が必要である．

そこで本稿では，匿名で情報発信が可能な SNS である Twitter において，ツイートを介して情報共有される Android アプリに関する分析を行い，その特徴や危険性に関する実態を報告する．

本稿の 2 章では Twitter から収集したデータセットについて説明する．3 章では収集した Android アプリに対する表層分析の結果をまとめる．4 章ではリパッケージアプリに対する分析結果をまとめる．5 章では 2 章から 4 章の分析結果を考察する．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. データセット

2.1 Twitter からのデータ収集

本稿では，Public Streaming API[12]（track statuses/filter，キーワード “apk”）を用いて Twitter に投稿されるテキスト（ツイート）および包含される URL を収集し，当該 URL とそのリンク先に含まれる URL からコンテンツを取得した．取得コンテンツには HTML 等が含まれるため，以下の条件に全て合致するファイルを APK として抽出した．

- ZIP フォーマットである
- `classes.dex` および `AndroidManifest.xml` が存在
- `META-INF/` が存在

2.2 収集した APK およびツイート

2.1 節で述べた手順によるデータ収集を 2017 年 6 月 22 日から 2018 年 3 月 7 日にかけて実施した．APK ファイルとして 43,476 件を収集し，VirusTotal File Report（FR）[13] が利用可能な 33,350 件を本稿での調査対象（以下，データセット APK）とした．

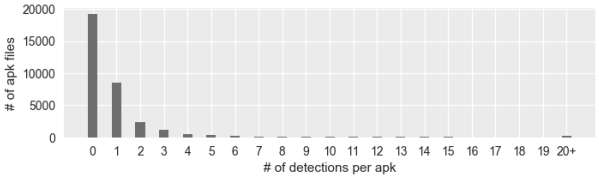

図 1 APK 検知数の傾向

表 1 APK 配布数 上位 10 ドメイン

順位	ドメイン名	APK 数
1	www.apkmirror.com	5,729
2	dl3.apko.org	3,474
3	dl3.uapkpro.com	3,390
4	dl2.apko.org	3,354
5	dl2.uapkpro.com	3,225
6	sirius.androidapks.com	2,195
7	dl5.apkhome.org	1,778
8	dl4.apkhome.org	1,535
9	dl.dropboxusercontent.com	1,512
10	dl.apkhome.net	1,133

データセット APK に関連するツイートとしては，ユーザアカウント数が 47,358，ツイート数が 196,508（重複を含まないテキスト種類数は 86,235）であった．ただし，これらのデータは本稿の実験環境で観測したものであり，Twitter API の仕様上，期間内に行われ条件に合致する全てのツイートが収集されたものではないことに注意されたい．

データセット APK に対する VirusTotal FR では，未検知が 19,233（57.7%），検知数 1 以上が 14,117（42.3%）であった（**図 1**）．検知数 2 以下の APK で全体の 90%（30,164）を占めている一方，検知数が 10 以上と多数のセキュリティベンダに危険性が認識されている APK も一定数（545 件，1.6%）確認されている．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，本稿では検知数が 1 以上の APK を要注意 APK と呼ぶ．

2.3 配布 URL の分析

データセット APK は，45,614 件の URL で配布されていた．複数の URL で配布されている APK も存在しており，最も多い例では一つの APK が 85 件の URL で配布されていた．配布 APK 数の多いドメインを**表 1** に示す．

50 件以上の APK を配布しているドメインを対象として集計すると，配布 APK の中で要注意 APK が占める割合において顕著な差が見られた（**表 2**）．上位，下位ドメインともに APK 配布目的と思われるサイトが大部分であるが，上位では改造版 APK やゲームの配布サイトが見られ

表 2　要注意 APK 割合 上位/下位 10 ドメイン

	上位		下位	
順位	要注意割合	APK 数	要注意割合	APK 数
1	0.99	79	0.06	610
2	0.97	235	0.08	5,726
3	0.97	86	0.1	67
4	0.82	74	0.14	2,188
5	0.82	90	0.15	309
6	0.75	1,517	0.16	116
7	0.69	1,752	0.18	62
8	0.69	67	0.2	55
9	0.68	132	0.21	111
10	0.68	66	0.21	75

表 3　ツイート数/APK 配布数 上位 10 ユーザ

順位	ユーザ名	ツイート数	APK 数
1	apkorg	6,944	6,800
2	UAPKPRO	4,935	4,914
3	Apkiosnet	4,690	4,653
4	DLSoftFree	3,898	3,817
5	ApkNeo	3,129	2,980
6	MixApkNet	2,650	2,508
7	apk2fun	1,781	1,770
8	APKMirror	1,696	1,680
9	A2Z_ApkHub	1,350	1,304
10	noobdownloadcom	1,137	1,071

る一方，下位には Google Play のミラーとされるサイトが含まれているなどの違いが見られた．

表 2 の上位と比較すると割合は低いが，著名なオンラインストレージでも一定数の要注意 APK の共有が確認された（要注意割合 0.39，APK 数 982）．

2.4　配布ユーザの分析

ツイート数，共有 APK 数の多いユーザを**表 3** に示す．APK 配布を目的とするサードパーティマーケットの運営者と見られるアカウントが大半を占めている．

ユーザのツイート数，要注意 APK にリンクされるツイート数を基準として分析すると *A*) 特定の APK 情報 *B*) 多数の APK 情報をそれぞれツイートするユーザが抽出された（**表 4**，**表 5** ）．これらのユーザは機械的な情報発信に利用されていると考えられ，表 4 のユーザでは特定 APK の定期的な通知が，表 5 のユーザではサードパーティマーケットの更新通知が確認されている．

2.5　ツイートの分析

本稿のツイートデータでは 86,235 件中 11,280 件（13.08%）のツイートにハッシュタグが含まれていた（破損のため利用不可のツイート 1 件を除き，ツイートを空白文字で分割し#記号から始まる文字列を抽出）．

*1　該当ユーザのツイートで要注意 APK へのリンクを含む割合

表 4　配布ユーザパターン A

	ツイート		APK	
	要注意 LNK 割合 *1	件数	要注意割合	件数
User A	1.0	6,060	1.0	1
User B	1.0	1,501	1.0	8
User C	1.0	1,112	1.0	2
User D	1.0	808	1.0	1
User E	1.0	737	1.0	1

表 5　配布ユーザパターン B

	ツイート		APK	
	要注意 LNK 割合	件数	要注意割合	件数
User F	0.98	230	0.98	227
User G	0.89	457	0.89	417
User H	0.78	641	0.78	593
User I	0.72	257	0.72	249
User J	0.72	180	0.73	172

表 6　ハッシュタグパターン A

	APK		
ハッシュタグ	要注意割合	件数	ツイート数
#岩手	1.0	4	2,604
#風俗	1.0	3	1,555
#デリヘル	1.0	3	1,555
#盛岡	1.0	2	1,552
#北上	1.0	3	1,145

表 7　ハッシュタグパターン B

	APK		
ハッシュタグ	要注意割合	件数	ツイート数
#jogos *2	0.66	133	132
#1	0.62	13	76
#androidgames	0.61	132	130
#modapk	0.58	52	268
#games	0.51	128	141

ハッシュタグとそのツイートからリンクされる APK に着目すると，2.4 節と同様に *A*) 特定の APK 情報 *B*) 多数の APK 情報 を共有するツイートが確認された．それぞれのツイートで確認されたハッシュタグを**表 6**，**表 7** に示す．

個別のツイート内容

個人ユーザ間での情報共有および特徴ある APK を共有するツイートを以下に例示する．

- 自身が Google Play で配布するアプリのサイズ超過による更新不可のため，別サイトからの取得案内を特定ユーザに対してリプライ（VirusTotal FR 検知数 30）
- あるユーザから格闘ゲーム中華版の利用方法を質問され手順をリプライ（VirusTotal FR 検知数 9）
- ルート化アプリを周知（VirusTotal FR 検知数 23）

*2　ポルトガル語で “ゲーム” を意味する

表 8　頻出パッケージ名 上位 10 件

順位	パッケージ名	APK 数
1	com.mojang.minecraftpe	243
2	com.whatsapp	187
3	com.google.android.gms	168
4	com.spotify.music	153
5	com.twitter.android	110
6	com.google.android.youtube	109
7	com.facebook.katana	100
8	com.facebook.orca	100
9	cm.aptoide.pt	99
10	com.google.android.googlequicksearchbox	94

表 9　パッケージ名別 要注意 APK の割合

	上位		下位	
順位	要注意割合	APK 数	要注意割合	APK 数
1	0.89	243	0.0	51
2	0.88	67	0.0	51
3	0.86	64	0.0	53
4	0.84	67	0.0	56
5	0.74	99	0.01	100
6	0.7	153	0.01	94
7	0.62	60	0.01	68
8	0.59	63	0.04	93
9	0.58	65	0.05	110
10	0.54	69	0.06	77

表 10　頻出証明書 上位 10 件

順位	証明書 SHA256	APK 数
1	a40da80a59d170caa950cf15c18c454d47a...	7,133
2	0cfb4663831a0fb8d6973aad44e221a8ba7...	1,776
3	f0fd6c5b410f25cb25c3b53346c8972fae3...	735
4	34df0e7a9f1cf1892e45c056b4973cd81cc...	671
5	0c3f90ab96c1a0a7cb02088f8f462e7494b...	541
6	e66033000dc6b8b93e1d487d01346c326ff...	457
7	3d7a1223019aa39d9ea0e3436ab7c0896bf...	363
8	e3f9e1e0cf99d0e56a055ba65e241b3399f...	356
9	465983f7791f2abeb43ea2cbdc7f21a8260...	239
10	ace1313608d3739d5c5afd61f796014657f...	204

表 11　証明書別 要注意 APK の割合

	上位		下位	
順位	要注意割合	APK 数	要注意割合	APK 数
1	1.0	172	0.0	51
2	1.0	58	0.0	53
3	1.0	52	0.0	56
4	0.99	81	0.0	59
5	0.98	239	0.0	60
6	0.98	135	0.0	65
7	0.96	114	0.0	87
8	0.93	7,133	0.01	161
9	0.92	1,776	0.01	77
10	0.91	457	0.02	363

3. 表層分析

3.1 パッケージ名

Android アプリはパッケージ名 [14] と呼ばれる識別子を持つ．パッケージ名は，アプリ開発者が自由に設定可能な属性であるが，他のアプリとの衝突を避けるためインターネットドメイン名を逆順にした文字列と組み合わせることが推奨されている．

本データセット APK では，12,473 種類のパッケージ名が確認された．頻出パッケージ名を**表 8** に示す．第 9 位はサードパーティのマーケットアプリであり Google Play では配布されていない．他は Google Play で配布される著名アプリである．

APK 数が 50 以上のパッケージ名を対象として，要注意 APK が占める割合の上位/下位を**表 9** に示す．パッケージ名によりその割合が大きく異なることが示されている．

上位第 1 位のパッケージ名については，Google Play で配信され 2018 年 7 月時点でダウンロード数が 1,000 万回超の有名な有料ゲームアプリである．本データセット APK では 9 種類の証明書が利用されており，多数の海賊版が流通し要注意割合の上昇に起因していると考えられる．

3.2 証明書

Android アプリは開発者が持つ秘密鍵で署名され，対応する証明書が設定される [15]．証明書を利用することで APK が同じ開発者により作成されたものと判別できる．

本データセット APK では，証明書として 7,149 種類が確認された．頻出証明書を**表 10** に示す．

APK 数が 50 以上の証明書を対象として，要注意 APK が占める割合の上位/下位を**表 11** に示す．証明書によりその割合が大きく異なることが示されている．

上位第 1 位の証明書については，172 件の APK（107 種類のパッケージ名）で使用されているが，証明書の識別名として組織名（o）に “google”，組織単位（ou）に “microsoft” が設定されており，アプリ開発者の身元識別は必要と考えない個人または組織により作成されたと考えられる．多数のパッケージ名向けに利用されているため，アプリのリパッケージに利用されている可能性も考えられる．

3.3 コンポーネント名

Android アプリを構成する代表的な要素として，Activity や Service，Content Provider，Broadcast Receiver（以下，コンポーネントと総称）がある．

本稿では，以下の手順でコンポーネント表層分析用データを取得した．まず，Android SDK[16] に同梱の aapt コマンドを実行し AndroidManifest.xml から APK 内に定義されたコンポーネント名を抽出する．次に，抽出したコンポーネントをパッケージ名毎にまとめ，それらを VirusTotal FR

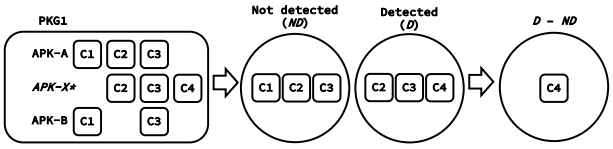

図 2 コンポーネント表層分析データ抽出

表 12 要注意 APK でよく見られるコンポーネント名

順位	コンポーネント名	出現 PKG 数
1	com.google.android.gms .ads.purchase.InAppPurchaseActivity	107
2	disabled_com.google.android .gms.ads.AdActivity	61
3	com.startapp.android.publish .list3d.List3DActivity	49
4	com.jirbo.adcolony.AdColonyOverlay	47
5	com.facebook.ads.InterstitialAdActivity	46
6	com.vungle.publisher.FullScreenAdActivity	37
7	com.my.target.ads.MyTargetActivity	37
8	disabled_com.unity3d.ads .adunit.AdUnitSoftwareActivity	35
9	com.unity3d.ads.android .view.UnityAdsFullscreenActivity	34
10	com.mopub.common.MoPubBrowser	31

による検知なし，ありの 2 つの集合に分割し，“検知あり” と “検知なし” の差集合を取得する（**図 2**）．コンポーネントの完全修飾名は例示すると “org.example.app.Activity” であり，当該差集合に含まれるドット区切りの先頭 2 要素でグループ化（“org.example”）し，最頻出のコンポーネント名をグループの代表値とする．これらの代表値を該当パッケージに属するコンポーネントリストとして抽出する．そして，一連の手順を各パッケージに対して適用することで，さまざまなパッケージの要注意 APK でよく見られるコンポーネントを抽出した．

上記手順を適用するためには，同一パッケージ名で VirusTotal FR の検知なし，検知ありの両方が必要である．本稿のデータセット APK では，条件に合致するものとして対象 APK パッケージ数が 1,657，検知なし APK が 7,386 件，検知あり APK が 6,834 件であった（aapt によるデータ取得不可の 1 件を除く）．

前述の手順を適用した結果を**表 12** に示す．表層的な名前の分析ではあるが，広告ライブラリとの関連が連想されるコンポーネント名が示されている．これらは，さまざまなパッケージ名の APK で出現していることから，第三者により追加されたと考えられる．また，“disabled_” で始まるコンポーネントについては，対象を無効化する意図による名称変更と推定される．

4. リパッケージアプリ分析

4.1 リパッケージペア

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たアプリである．APK では公開鍵証明書を利用したデジタル署名が行われており，証明書によりその作成者を識別可能である．APK は ZIP フォーマットであり改変が容易だが，秘密鍵の所有者以外は署名できないため，作成者が異なることを見分けられる．リパッケージアプリの作成は容易なため，人気ゲームやアプリをリパッケージしたマルウェアが報告されている [17].

リパッケージアプリの分析を行うため，データセット APK に含まれる任意の 2 つの APK について，以下の条件を全て満たす組み合わせをリパッケージペア候補として抽出した．

- パッケージ名が同一
- バージョン番号（versionCode）が同一
- 署名に利用される証明書が異なる

本稿では，Google Play で配布されるアプリを正規版として扱う．リパッケージペア候補と同じパッケージ名を持つアプリを Google Play からダウンロードし，抽出した証明書とリパッケージペア候補の証明書を照合しいずれかと一致した場合に有効なリパッケージペアとした．なお，日本では利用可能でないアプリ，Google Play からのアプリ収集に利用した端末（Fujitsu arrowsM03）が非対応，有料アプリは対象外とした．

4.2 リパッケージデータセット

4.1 節の基準を適用した結果，本稿のデータセット APK から 1,216 件のリパッケージペアを抽出した（4.3 節で述べる特徴情報を取得不可の 5 件を除く）．本ペアではパッケージ名は 459 種類，APK としては正規版が 947 件，リパッケージ版が 1,206 件であった．

正規版とリパッケージ版の検知状況を比較すると（**図 3**），正規版よりリパッケージ版の検知数が多いペアは 987（81.2%），検知数が同一のペアは 211（17.4%），検知数が少ないペアは 18（1.5%）であった．正規版・リパッケージ版ともに未検知のケースは 165（13.6%）であり，正規版が未検知かつリパッケージ版が検知されるケースが 865（71.1%）であることから，リパッケージ版の危険性 [18] を示す一例と言える．

本リパッケージペアでの頻出パッケージ名の上位 10 件を**表 13** に示す．これらのパッケージ名を持つアプリは 2018 年 7 月時点でいずれも 1,000 万回以上ダウンロードされており，人気の高いアプリがリパッケージ対象となっていることが示されている．

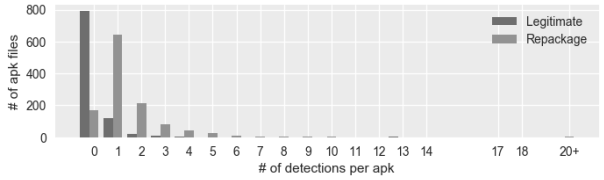

図 3 正規/リパッケージ版 APK 検知数の傾向

表 13 頻出パッケージ名上位 10 件

順位	パッケージ名	件数
1	zombie.survival.craft.z	37
2	com.com2us.smon.normal.freefull .google.kr.android.common	35
3	com.whatsapp	33
4	com.spotify.music	30
5	com.kiloo.subwaysurf	23
6	com.truecaller	17
7	com.wb.goog.mkx	16
8	com.oasisfeng.greenify	15
9	com.gameloft.android.ANMP.GloftA8HM	15
10	jp.konami.pesam	15

4.3 特徴情報の抽出

リパッケージアプリの調査では，追加された Java のコードを分析対象とした．本稿のリパッケージペアでは正規版とリパッケージ版のバージョン番号が一致しており，その差分はリパッケージに起因するとみなすことができる．以下の手順でリパッケージによる “増分” を特徴情報として抽出した．

(1) Apktool[19] で APK に含まれる DEX を Smali[20] に変換

(2) Smali から API コールを表すディレクティブ invoke-* を収集し，Java メソッド単位でリスト化

(3) 正規版/リパッケージ版で上記リストの比較を行い差分を unified diff として取得し，追加部分（+）を抽出

4.4 特徴情報の整理

上記の手法で増分を抽出した結果，337,744 件のデータが得られた．

正規版とリパッケージ版の差異について見ると，ひとつの APK で 8 万箇所以上の追加がなされているものもあれば，API コール追加という観点からは何も変化がないというものも 447 件の APK に存在する等ばらつきが見られる．

それぞれの増分の内容について見ると，ユニークなものは 176,511 種類存在し，うち 128,061 種が一度だけ登場している．すなわち，残りの 48,450 種については複数の APK で同じ API コールが追加されているということになる．

表 14 Apriori パラメタ

項目	設定値
MIN_SUPPORT	（登場回数 3 回以上）
CONFIDENCE	0.8
LIFT	5

特徴情報を整理するために，抽出したデータのグループ化を行なう．

リパッケージアプリの作成者が金銭的利益や情報の搾取等ある一定の目的を持っているとすると，その目的を実現するための特定の機能を追加する改変が様々な APK に共通して現れていると考えられる．

これはデータ中には幾つかの増分が同時に，複数の APK に現れているパターンとして現れ，そのようなパターンを調査することがリパッケージアプリの作成目的や危険性の解明に有益である．そういった共起確率の高い API コール群を探し出すため，以下のようにアソシエーション分析の手法を用いて得られたデータを処理する．

(1) Apriori アルゴリズム [21] で有意な相関ルールを抽出する

(2) 相関ルール A → B と B → A　双方が発現している場合，A と B をエッジで結ぶ

(3) 連結されている部分を共起確立の高い API コール群とする

尚，Apriori アルゴリズムのパラメタは**表 14** のように設定した．

以上の手法により 177 個の互いに関連する API コールのグループが得られた．

4.5 分析結果

得られた API コールのグループを調査した結果，以下のような内容を含むものが見られた．

広告の削除を行うもの

このパターンでは，AudienceNetwork　Adcolony TMMoreAppsActivity などの様々な広告モジュールに同じコードが書き加えられている．

private void NBMIEWKTYSB() のようにランダムな文字列で名付けられた追加メソッドがあり，ここでは Process.killProcess(Process.myPid()); によって自身を終了させる．それを onCreate タイミングで呼び出すことで広告の表示を防ぐ仕組みとなっているようだ．

広告の追加を行うもの

逆に flymob, myTarget, StartApp などのアドネットワークに関連する API コールが追加されており，新たな広告を導入しているらしきパターンが存在した．

内容の詳細な分析までは出来なかったが，アプリケーション起動時に表示される全画面広告である StartApp Splash

Ad について，表示時間等のパラメタを操作している例などが見られた．

特定サイトへの誘導

このパターンは 143 のリパッケージアプリに共通して現れており，パッケージ名を見るとゲーム系アプリが多い．ロシアのアプリ配布サイトへの誘導リンクを表示させる内容が含まれており，多くの場合で当該サイトのバナーらしき画像ファイルが追加されている．

誘導先は全て同じサイトなのに対しこの改変が為された APK の配布元は様々であり，リパッケージアプリがそのまま，或いは更なる改変を受けて他サイトで再配布される場合が多いことが推測される．

配布元の偽装

Android のアプリには非正規ルートでの配布を防止するため正規サイトからダウンロードされたものでない場合起動できないようにしているものが存在する．

このパターンはそういった対策を回避するためのコード [22] が含まれている APK 群と思われる．

配布サイト情報は getInstallerPackageName の戻り値で判別されるが，これを偽装することで対策をすり抜けるコードが追加されている．

他にもアプリの署名を予め収集しておいた正規版のものに偽装する，デバイス ID を偽装するなどのコードが含まれていた．

5. 考察

Twitter 上での APK 共有

Twitter において多数の APK が片方向，相方向のコミュニケーションにより共有されていることを確認した．片方向としてはサードパーティマーケット等による情報通知が，相方向としてはツイートに対するリプライが該当する．

サードパーティマーケット運営者による機械的なツイートにより多数の APK が共有され，ユーザや配布 URL により要注意 APK の割合が大きく異なることが確認された．

本稿では，オンラインストレージでの APK 共有についても確認した．サードパーティマーケットのような大規模なデータ配布では専用サーバや CDN を用いると考えられ，主として個人ユーザがオンラインストレージを利用していると推定される．2.3 節で述べたオンラインストレージでは，要注意 APK を含めて 2,189 ユーザによる APK 共有が観測された．

個人間，サードパーティマーケットを含めて Twitter での APK 共有には一定のリスクがあり，そのような APK を利用する際には対象 APK の出所や特徴，共有相手を確認する必要性が示されたと考える．

高リスクと考えられる APK

データセット APK では，ルート権限取得や Google Play 内で配布される有料アプリを無料で購入可能にするといった内容の APK が確認された．本稿ではこれらの動作は未確認だが，その通りに振る舞うと仮定するとさまざまな観点から問題を起こすと考えられる．一例として，ルート権限がマルウェアに悪用されることにより OS のセキュリティ機構の無効化やシステム改変 [23] の原因となる恐れがある．

リパッケージアプリ

本稿では，特徴情報（Java API 増分）に対してアソシエーション分析を適用することで共起確率の高い API コール群を抽出し，リパッケージにより埋め込まれたコードの挙動例を明らかにした．分析結果の範囲では，情報漏洩 [24] などリパッケージアプリの利用者に対して深刻な悪影響を直接及ぼす挙動は確認されていない．しかし，広告追加により利用者に余分な通信費が発生したり，広告削除により正規版開発者の逸失利益が生じるなど，悪影響が発生することは事実である．加えて，リパッケージアプリの作成者が悪性な動作を実装する可能性は否定できず，リパッケージアプリを利用すべきではないことが改めて示されたと考える．

6. 関連研究

Ando[25] は，サードパーティマーケットで配布される APK を収集するシステムを提案している．Ando の研究 [25] では，サードパーティマーケットで配布される APK を研究対象としているが，我々は SNS である Twitter 上で共有される APK を観測対象としている．

APK の表層解析として，西田ら [26] が APK で利用される証明書をヒューリスティック検知での要素技術一つとする手法を提案している．我々は，西田ら [26] の手法を Twitter で共有される APK 評価の指標の一つとして利用した．

リパッケージアプリの分析として，石井らの研究 [27], [28] がある．文献 [27] では，アプリのリソース情報を用いて正規版に類似する外観を持つアプリを抽出し，コード解析により得られる正規版との差分（増分）で類似アプリを分類している．文献 [28] では，大規模なデータセットに対してリパッケージアプリの分析を行い，マルウェアや広告挿入アプリなど 4 カテゴリに分類している．我々は，APK のバージョン番号を一致させたリパッケージペアを対象とすることで，より精緻な分析を行なっている．

7. まとめと今後の課題

本稿では，Twitter で共有される APK について，配布時の情報および表層的な特徴に基づく分析を行い，配布ユーザ，配布 URL，パッケージ名，証明書別に見ると要注意 APK の割合が顕著に異なることを示した．また，リパッ

ケージアプリの分析により，広告ライブラリの追加/削除や特徴的なリパッケージの挙動例を特定した．これらにより，Twitter で共有される APK に一定のリスクが存在することを明らかにした．

本稿では個別の要素（ユーザ，ツイート，配布 URL）と APK の表層的な特徴に対する分析を行なったが，APK とテキスト（ツイート，配布ページ）の関連や APK の振る舞いを特定するための静的解析は未実施である．また，リパッケージアプリ分析の対象データセットは，観測したものに限定されるため小規模である．これらの分析の実施やリパッケージペア拡充が今後の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] “Android マルウェアへの感染を避ける方法”, https://blog.kaspersky.co.jp/android-app-security/17887/
[2] “総務省 平成 29 年版 情報通信白書”
[3] “Google Play から拡散される新たなマルウェア”, https://eset-info.canon-its.jp/malware_info/trend/detail/180301.html
[4] “Android とセキュリティ”, https://japan.googleblog.com/2012/02/android.html
[5] “Amazon Appstore”, http://www.amazon.com/appstore
[6] “ウイルスバスター モバイル (Android) をインストールする方法”, https://esupport.trendmicro.com/support/vbm/solution/ja-jp/1097203.aspx
[7] MOBILE THREAT REPORT Q1 2014, F-Secure
[8] “ハッシュタグの使用方法”, https://help.twitter.com/ja/using-twitter/how-to-use-hashtags
[9] “大阪地震で SNS を活用した高校生たち–デマ拡散には注意”, https://japan.cnet.com/article/35121100/
[10] “SNS が新たなマルウェア感染ルートになりつつある —— どうする SNS セキュリティ”, https://eset-info.canon-its.jp/malware_info/trend/detail/150428.html
[11] “世論を操作する「フェイクニュース」、SNS の 1000「いいね！」も 2 円から購入可能”, https://is702.jp/news/2200/
[12] “Filter realtime Tweets”, https://developer.twitter.com/en/docs/tweets/filter-realtime/api-reference/post-statuses-filter
[13] “VirusTotal Public API v2.0”, https://www.virustotal.com/en/documentation/public-api/
[14] “Android manifest”, https://developer.android.com/guide/topics/manifest/manifest-element
[15] “アプリケーションへの署名”, https://developer.android.com/guide/publishing/app-signing
[16] “Command line tools”, https://developer.android.com/studio/command-line/
[17] INTERNET SECURITY THREAT REPORT, APRIL 2015 VOLUME 20, Symantec
[18] “不正 Android アプリの大量生産はどうすれば防げるのか (1/3)”, http://www.atmarkit.co.jp/ait/articles/1604/28/news010.html
[19] “Apktool”, https://ibotpeaches.github.io/Apktool/install/
[20] “Smali”, https://github.com/JesusFreke/smali
[21] R.Agrawal and R.Srikant: Fast algorithms for mining association rules, In Proceedings of 20th Int. Conf. Very Large Data Bases, VLDB, pp.487-499, 1994.
[22] “偽の Minecraft の Android アプリが Smalihook を使用”, http://blog.f-secure.jp/archives/50719626.html
[23] “How the CopyCat malware infected Android devices around the world”, https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/
[24] “「リパッケージ」と「贋作」による不正アプリの被害”, https://blog.trendmicro.co.jp/archives/7479
[25] Ruo Ando. An Empirical Study of Android APK Disributuion Sites Using Headless Browser with Navigation Scripting. コンピュータセキュリティシンポジウム 2015 論文集. 2015, vol. 2015, no. 3, p. 215-220.
[26] 西田 雅太, 神薗 雅紀, 星澤 裕二. 署名情報を利用した Android マルウェアの推定手法の提案. コンピュータセキュリティシンポジウム 2012 論文集. 2012, vol. 2012, no. 3, p. 28-35.
[27] 石井 悠太, 渡邉 卓弥, 秋山 満昭, 森 達哉. 正規アプリに類似した Android アプリの実態解明. 信学技報. 2015, vol. 114, no. 489, p. 187-192.
[28] 石井 悠太, 渡邉 卓弥, 秋山 満昭, 森 達哉. Android クローンアプリの大規模分析. コンピュータセキュリティシンポジウム 2015 論文集. 2015, vol. 2015, no. 3, p. 207-214.