脅威を引き起こすアプリケーションを アクセス権限などを用いて検出する手法についての考察

2015SE001 安藤花風里　2015SE028 伊藤美惟
指導教員：横森励士

1　はじめに

近年 Android を筆頭にスマートフォンが急速に普及し，スマートフォン上で動作させるアプリケーション (以下，アプリ) の需要が増加している．大量のアプリの中には悪意を持つものが存在しており，それらによって様々な脅威が日々引き起こされている．このような環境下では，アクセス権限など利用者に事前に公開される情報を利用して，悪意を持ったアプリによって引き起こされる脅威を未然に回避することが求められる．私たちはアプリの紹介ページで確認できる情報から，機械学習を行うことで，怪しいアプリであるかどうか推測できると考えた．具体的には，アクセス権限や，アプリのダウンロード数，カテゴリー，評価したユーザの人数などの情報を特徴量として加味することで，検出の精度が上がるのではないかと考えた．

本研究では，アクセス権限やアプリの紹介ページから得られる情報を特徴量として入手し，それらを機械学習の材料とすることで，悪質なアプリの検出を行う方法について調査する．アプリのジャンル分けを行った後で機械学習を行いどれだけの精度が良くなるか，特徴量を考察することでどのように結果が変化するかを調査する．提案手法を用いることで，悪意を持つアプリを検出することができれば，アクセス権限を認めることでもたらされる被害を未然に防ぐことができるのではないかと考える．

2　背景技術

2.1　Android アプリと悪意を持つアプリが引き起こす脅威について

代表的な Android アプリの配布サービスとして，Google Play[1] が提供されている．アプリを提供する側がアプリに関する情報を登録すると，マルウェアやウイルスなどの感染を機械的にチェックした上で，Google Play 上に公開される．チェックを通り抜ければ，悪意を持つアプリもそのまま公開されてしまうので，利用者はアプリをインストールする際に Google Play から与えられた情報をもとに自己判断を行う必要がある．

悪意を持つアプリが引き起こす問題の例としては，個人情報抜き取り，端末の遠隔操作，悪意を持った Web サイトへの誘導などがある．Android 不正アプリ検出数の割合 [2] を表 1 に示す．表で示す通り，“アドウェア”が約 8 割を占めており，“情報窃盗／バックドア”が残りの部分の半数を占めている．ユーザ側はこれらの脅威への対策としてセキュリティアプリを入れることが推奨されているが，そのどれもが一度アプリをインストールしてからチェックにかける方式をとっているので，インストールされた時点で何らかの被害を及ぼすアプリには効果が薄いと言える．

アプリをインストールする際には，Google Play はアプリが端末内のどの機能や情報にアクセスするかの情報を利用者に確認させる．Android6.0 以降では，悪用された場合に危険度が大きい権限のみを，大きく 9 のカテゴリー [3] に分け，表 2 のようにそれぞれの用途ごとにアクセス権限を利用者に要求する．ユーザが保存したデータや他のアプリ操作に影響を及ぼす可能性がある場合に，アプリがユーザの個人情報を含むデータやリソースを必要とする．

アドウェアの検出は，一般的に広告の内容を調査する必要があり，アクセス権限の有無から分類することが困難である．一方で情報窃盗やバックドアでは，悪意を持つアプリが脅威を引き起こすためには，利用者がアクセス権限の許可を与えることが必要であるので，要求する権限によって検出可能であると考えた．アクセス権限をもとに脅威を引き起こすアプリを検出する手法について考察する．

表 1　国内での不正アプリ検出種別割合 (2015) [2]

脅威の種類	割合
アドウェア	79.80 %
情報窃盗/バックドア	8.56 %
ネット詐欺	2.84 %
脆弱性悪用	1.46 %
プレミアム SMS 悪用	0.81 %
ランサムウェア	0.04 %
その他の不正アプリ	6.48 %

2.2　関連研究

Zhongmin らは，アプリのアクセス権限に対して，機械学習による分類分けを行い，悪意を持ったアプリの判別を行った [4]．[4] では，Google Play から提供されている無料 Android アプリを対象として，アプリの APK ファイルで記述されている要求権限を抽出し，機械学習に使用して，アプリのカテゴリーごとにしきい値を計算した．アプリのカテゴリーとアクセス権限は，密接な関係があるとし，本来のカテゴリーに属さないと判断されるアプリは悪意を持ったものである可能性が高いとした．

石田らによる研究 [5] では，多大なコストをかけることなく，効率的に悪意を持つアプリを検出するために，階層的クラスター分析によって同じような権限を要求するアプリに分類した上で，他のアプリと異なるアクセス権限を要求するアプリを仲間外れにすることで検出を行う分類手法

表 2 Android6.0 以降で Google Play がユーザに要求するアクセス権限の一覧 [3] より引用

アクセス権限	用途	アクセス権限	用途
ボディセンサー	心拍数モニターなどウェアラブルセンサーへのアクセスを許可する	ストレージ	端末のファイルや保存されているデータの使用を許可する
カメラ	端末のカメラの使用を許可する	マイク	端末のマイクの使用を許可する
SMS	端末のテキストメッセージやマルチメディアメッセージのサービスの使用を許可する	位置情報	端末の位置情報の使用を許可する
カレンダー	端末のカレンダーの情報の使用を許可する	電話	電話やその通話履歴の使用を許可する
連絡先	端末の連絡先情報の使用を許可する		

を提案した．評価実験の結果からは，提案手法により，似たアプリごとへの分類は行えていたが，悪意を持つアプリの検出の精度は十分ではないことが分かった．

3 提案手法

3.1 過去の手法と提案する手法

要求する権限をもとにしたクラスタリング [5] では，似たアプリの分類はできるが，悪意を持つアプリの検出までは難しかった．また，[4] の手法では，要求する権限から所属すべきアプリのジャンルを推測する手法をとっている．「異なるジャンルに配属されたアプリは悪質なアプリの可能性が高い」という仮説のもとに機械学習を行っているので，直接，アプリが悪質かどうかの判定は行っていない．

本研究では，あらかじめジャンル分けを行ったアプリの集合に対して，アクセス権限とそのアプリが悪質だったかどうかの情報を与えることで，悪質なアプリを機械学習によって検出する手法を評価する．あらかじめジャンル分けされたアプリに対して機械学習を行うことで，精度の向上を見込むことができると考えた．

さらに，悪意のあるアプリの場合，ただ単に必要とする権限が多くなるだけでなく，犯罪に対して足がつかないように所在地を明記していないなどのように，紹介ページで確認できる情報から怪しいアプリであることが推測できることがあると考えた．そこで，機械学習で入力する情報において要求する権限の情報だけでなく，アプリのダウンロード数，カテゴリー，評価したユーザの人数などの情報を特徴量として追加した手法とも比較し，それらの特徴量がどのように機械学習の精度に影響を与えるかを調べた．

3.2 追加する特徴量について

特徴量を追加する際にはアプリの紹介ページから情報を取得し，表 3 に示す 8 項目を機械学習において考慮する．それぞれの項目について，悪意のあるアプリとどう関連するか，悪意のあるアプリではその要素がどうなると考えられるかについて考察した．例えば，更新日という項目については，悪質なアプリはリリースしてその後は放置していたり，更新のためのコストをかけたりしないだろうという理由から，悪質なアプリでは更新されてから現在までの期間が長くなっていると考えられる．

3.3 本研究における分析する内容

1. 提案手法による機械学習において，どれだけの精度を見込むことができるか．

   1 つのジャンルのアプリ群に対して，データセットを 5 通り作成し，9 種類のアクセス権限を入力として，悪質かどうかを判定する機械学習を行った．それぞれの事例で，検出のしきい値を変えた時の再現率と偽陽性率をそれぞれまとめ，グラフとして表現する．各ケースで 1 番精度が高くなる場合を求め，提案手法によりどれだけの精度を見込むことができるかを調査した．

2. 特徴量をすべて追加した場合に，実験 1 の結果と比べてどのように変わったか．

   表 3 で示す特徴量をすべて入力に加えて，実験 1 と同様のアプローチで機械学習を行い，再現率と偽陽性率のグラフとしてまとめる．実験 1 の結果と比較することで，グラフがどのように変化したかを確認し，特徴量を加えることでどのように変化するかを調査した．

3. どの特徴量が結果に影響を及ぼしているか．

   表 3 で示す特徴量の中から一つだけ追加して，同様のアプローチで機械学習を行ったときに，それぞれの場合に再現率と偽陽性率のグラフがどのように変化したかを調査する．特徴量をすべて追加した場合の結果に近づくか，アクセス権限のみの結果と変わらないかを確認し，どの特徴量が結果に影響を及ぼしたかを調査する．

4 評価実験

提案手法に基づいて機械学習を行う仕組みを構築した．以下では作成したデータセットを紹介するとともに，悪意のあるアプリをどのように定義するか，機械学習による実験において，どのように評価を行うかについて紹介する．

4.1 実験の準備

実験の準備として，実験におけるデータセット，悪質なアプリの定義，機械学習の方法について紹介する．

まず初めに，2018 年 7 月から 10 月の期間にデータセットとして，アプリのジャンルを 20 個選び，それぞれのジャンル毎にアプリを Google Play Store から抽出した．それ

表 3 提案手法 2 で機械学習を行う際に考慮する特徴量の一覧

項目	理由	悪意のあるアプリではどうなるか
ダウンロード数	良いアプリではなく広がりにくいから	ダウンロード数が少ない
リリース日	配信と削除を繰り返しているから	リリース日から日が経っていない
更新日	リリースしてその後は放置しているから	更新されてから日が経っている
その他のアプリ数	アプリごとに配信元を変えているから	1 つまたは数が少ない
配信元住所の明記	犯罪が起きた時に足がつかないようにするから	明記されていない
カテゴリー	法則性があると考えたから	-
評価したユーザ数	ダウンロード数に伴い少なくなるから	人数が少ない
レビューの最新日	使っているユーザが少ないから	最近のものではない

ぞれのアプリ毎に，表 2 の要求する権限の有無を 9 種類，表 3 の特徴量を 8 種類と，悪意を持つアプリであるかないかの情報の合計 18 種類を入手し，アプリデータとした．その後，悪質なアプリを 3 割以上含む，表 4 で示す 5 ジャンルについて機械学習を行った．事前に適用した際によい結果を示したロジスティック回帰のモデルを使用モデルとした．機械学習はこのデータを学習の材料として与え，訓練サブセット，テストサブセットの 2 つを作成し，学習と検証に用いる．

悪意を持つアプリとしては，セキュリティアプリに搭載されているアプリスキャン機能によってプライバシー保護の観点から危険性があると判断されたものと，Google Play 上において 2018 年 9 月から 11 月の間に該当アプリが削除されたものを悪質なアプリと定義した．

表 4 5 個の同種なアプリ群

アプリ群名	サンプル数	悪質なアプリ数
出会い系	101	30
バトルロワイヤル	75	35
ポケモン GO	60	37
マイクラ	51	16
マリオ	35	14

4.2 適用結果

1. 提案手法による機械学習において，どれだけの精度を見込むことができるか．

   表 4 で示す 5 ジャンルについて，アクセス権限のみを入力データとして訓練サブセットとテストサブセットを 5 通り作成し，それぞれの事例において，検出のしきい値を変えたときの再現率 (x 軸) と偽陽性率 (y 軸) の変化をまとめたグラフを図 1 に示す．実利用では，充分な再現率があって，精度が高いことが求められるので，再現率が 0.85 以上かつ偽陽性率が一番低いときを一番良い結果として，その場所に印をつけている．そのときの F 値について，5 回の事例の平均値をグラフ上に示した．[4] の実験では，F 値の平均が 0.652 であったのに対し，本実験の 5 ジャンルの F 値の平均は 0.7144 であった．あらかじめジャンル分けを行うことで，機械学習の精度を向上させることができると考えられる．

2. 特徴量をすべて追加した場合に，実験 1 の結果と比べてどのように変わったか．

   実験 1 のアプリ群に対して，アクセス権限と表 3 の特徴量すべてを入力データとして実験 1 と同様の実験を行った．その結果を図 2 に示し，図 1 と比べ，全体的に右下のグラフとなっており，偽陽性率が低く，適合率が高い，より正確に分類できている結果が得られやすくなっていることがわかる．F 値の平均も 0.7228 となり，実験 1 の結果より少し精度が上がった．

3. どの特徴量が結果に影響を及ぼしているか．

   アクセス権限に表 3 の特徴量の中からひとつだけ選んだ場合を比較したところ，ダウンロード数，レビュー数，更新日を含んだ場合は，全特徴量を含んだ場合の結果に近づいた．リリース日については，アクセス権限のみの結果とあまり変わらなかった．

4.3 考察と今後の課題

あらかじめジャンル毎にアプリを分類してから機械学習を行うことで，[4] のアプローチより精度の高い検出を得ることができると考えられる．また，機械学習において入力するデータを特徴量として追加することで，再現率や偽陽性率が全体として改善する傾向にあり，効果があることが分かる．中でも，ダウンロード数やレビュー数，更新日は判断材料として活用できると考えられる．実際には，ダウンロード数とレビュー数は共通因子の影響を受け，相互に関係性が強い指標であると考えられる．どう組み合わせるのが最善となるかを今後は調査したい．

実験を行う上で，データセットの作成を行うことが難しく，継続的な分析環境を実現するためにはデータセットの作成方法を考える必要がある．悪質なアプリは Google play 状から存在が抹消されてしまうので，悪質なアプリを認定するためにはある程度の期間をおいて確認することが必要である．抹消された後に新たな情報を入手することは難しいので，事前に入手できる情報をすべて入手し，それを管理するようなシステムのもとにデータセットを維持する必要がある．

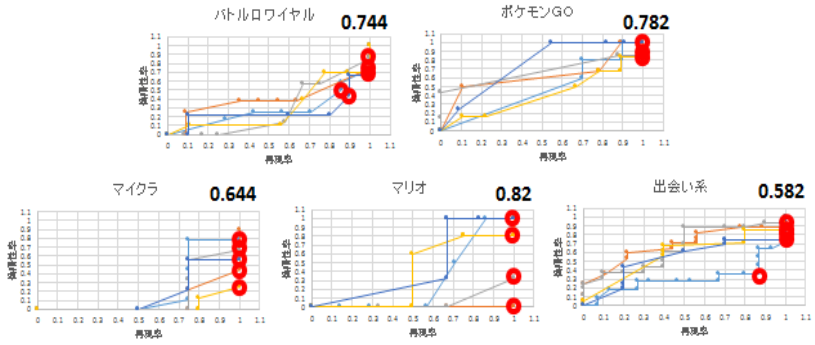

図 1　アクセス権限のみを使用した場合の再現率-偽陽性率グラフ

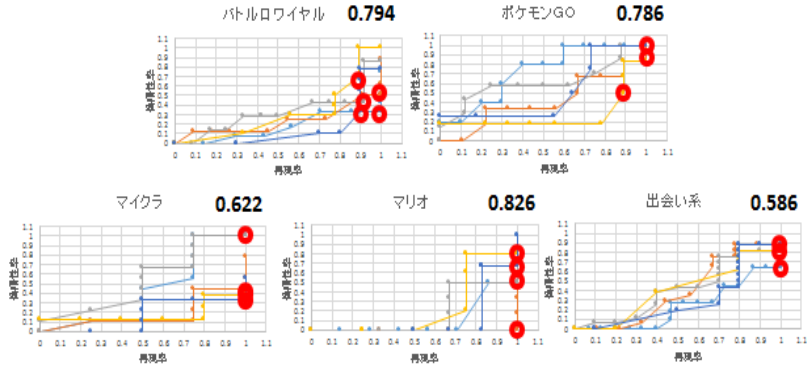

図 2　特徴量をすべて使用した場合の再現率-偽陽性率グラフ

5　まとめ

本研究では，アプリの紹介ページから情報を特徴量として入手し，アクセス権限に加えてそれらも機械学習の材料とすることで，悪質なアプリの検出の精度が向上するかを確認する手法を提案した．ジャンルごとに機械学習を行うことでより良い精度の分析ができることや，特徴量を考慮することでアクセス権限のみで機械学習を行うより精度が上がることを確認した．特徴量の中にも有効なものがいくつかあり，今後はそれらをどのように組み合わせることで最適の結果をもたらすかなどを調査することが課題である．

参考文献

[1] Google play：https://play.google.com/store/

[2] トレンドマイクロ：“1000 万個を突破した Android 不正アプリの「これから」”，http://blog.trendmicro.co.jp/archives/12960

[3] Google ヘルプ：“Android 6.0 以降のアプリの権限を管理する”，https://support.google.com/googleplay/answer/6270602

[4] Zhongmin Ma：“Android Application Install-time Permission Validation and Run-time Malicious Pattern Detection”，Master thesis of Virginia Polytechnic Institute and State University，2013.

[5] 石田尚也，小林薫，大野哲弥：“必要とするアクセス権限に基づく Android アプリケーション分類手法の提案”，南山大学理工学部 2017 年度卒業論文，2018.

[6] Andreas C. Müller，Sarah Guido：“Python ではじめる機械学習-scikit-learn で学ぶ特徴量エンジニアリングと機械学習の基礎”，オライリー・ジャパン，2017.