Android OSにおける不正アプリケーション取得防止のための セキュリティ評価システムの提案

喜多 義弘† 久保田 真一郎‡ 朴 美娘† 岡崎 直宣‡

†神奈川工科大学
243-0292 神奈川県厚木市下荻野 1030
y.kita@ccy.kanagawa-it.ac.jp
mirang@nw.kanagawa-it.ac.jp

‡宮崎大学
889-2192 宮崎県宮崎市学園木花台西 1-1
kubota@cs.miyazaki-u.ac.jp
oka@cs.miyazaki-u.ac.jp

あらまし 近年，Android OS 搭載端末の普及が進む一方で，不正アプリケーションが増加し，それによる個人情報漏洩が問題となっている．ユーザがインストール時に不正アプリケーションを取得しないように，アプリケーションが利用するパーミッション (権限) をユーザに通知し，取得の承認を仰いでいる．しかし，セキュリティに無関心なユーザや技術に精通していないユーザの，不正アプリケーション取得の危険性に対する認識不足が問題となっている．そこで本研究では，不正アプリケーションの取得防止を目的として，ユーザ主体によるレビュー評価，および，パーミッションの組合せによる危険性提示を統合したセキュリティ評価システムを提案する．

Proposal of Security Evaluation Systems to Prevent the Installation of Mal-Applications on Android OS

Yoshihiro Kita† Shin-ichiro Kubota‡ MiRang Park† Naonobu Okazaki‡

†Kanagawa Institute of Technology
1030 Shimo-Ogino, Atsugi-city, Kanagawa 243-0292, JAPAN

‡University of Miyazaki
1-1 Gakuenkibanadai-Nishi, Miyazaki-city, Miyazaki 889-2192, JAPAN

Abstract Recently, leakage of the personal information in Android OS powered device by mal-applications is becoming big issue. The user approves the installation of an application, and gets permissions to use by an application. However, the lack of recognition to risk of mal-application by the users which are indifferent to the permissions. In this paper, we propose the security evaluation systems to prevent the installation of mal-application on Android OS. The system is integrated two systems, review evaluation by users, and risk indication by the combination of the permissions.

1 はじめに

近年，スマートフォンをはじめとする携帯端末が広く普及しており，それに伴って携帯端末用の多種多様なアプリケーション (以降，アプリ) が増加している．しかし，アプリが増加するほど，様々なトラブルも増加している．トラブルの内訳は，個人情報の漏洩から端末のボット化まで多岐にわたるが，それらの主な原因の1つとして，不正アプリケーション (以降，不正

アプリ) をインストールしていることが挙げられる．

その対策として，Android OS 搭載の携帯端末 (以降，Android 端末) のアプリ配信サービスである Google Play[1] を運営する Google は，2012 年 2 月に Google Play のマーケット内の不正アプリを検知する Bouncer を実装した．しかし，不正アプリは無くならず，さらには Bouncer を合法的に破る方法も発見されている．また，情報処理推進機構がアプリ開発者に対し，アプリの脆弱性に関する指針 [2] を発行したが，アプリの脆弱性を完全に取り除くことは困難であり，不正アプリによる被害の拡大を抑制できていないのが現状である．

アプリ開発者側で不正アプリを作成しないように，セキュリティマネージャを用いた開発者管理システム [3, 4]，パーミッションの不正取得に対するセキュリティ技術 [5]，マーケット投稿時における動的解析によるマルウェア検知システム [6, 7] の研究が行われている．

一方，ユーザ側では，アプリのダウンロード時における使用パーミッションの提示や不正アプリの危険性を示すセキュリティ助言システム [8] があるが，専門知識を有することやパーミッションの組み合わせを考慮する必要があり，パーミッションを読むことを多くのユーザが敬遠している現状がある．

アプリに対するユーザからのレビューによって不正アプリを判断することも有用であると考えられる．しかし既存のレビューシステムでは，レビューの管理が十分ではないため，アプリの内容に無関係なレビューや悪意のあるレビューがあったり，開発者の利益を意識したレビュー操作が行われたりと，ユーザにとって有益な情報ではない場合がある．これらのことから，開発者側の対策だけでなく，ユーザ自身も不正アプリをインストールしないための策を講じる必要があるが，ユーザが不正アプリを判断することは難しいという問題がある．

そこで本研究では，不正アプリの取得防止を目的としたセキュリティ評価システムを提案する．具体的には，ユーザが不正アプリを判断しやすいように，パーミッション情報を基に，アプリの危険度を 3 段階で提示する．さらに，レビュー評価システム [9] も導入し，ユーザに公正なレビューを促すことにより，不正アプリを判断するための一指標として有用性の高いレビューを提示し，不正アプリの取得防止を狙う．

2 関連研究

2.1 既存のアプリ評価システム

Google Play[1] などに用いられているアプリ評価システムは，使用しているパーミッションとユーザのレビューを提示する．パーミッションには，アプリでの挙動と予想される危険性を明記しているため，アプリの危険性を予想することができる．しかし，他のパーミッションとの組み合わせによる危険性については触れられていないため，アプリの危険性を十分に示していない．また，Android 端末の機能やセキュリティに関する専門知識を有していないと，パーミッションからアプリの挙動を把握することは難しい．

レビューは，新規ユーザがアプリを取得する際の指針として有用である．しかし，レビューを書き込むユーザは一部であり，アプリの内容に無関係なレビューや悪意のあるレビューが増えている．一方，アプリによる利益を獲得するために，開発者がユーザに成りすまして積極的なレビューを書く場合がある．このとき，レビューは過大評価なものになり，客観的ではない．また，不正アプリの場合，それをインストールさせるために開発者が誇張されたレビューや偽のレビューを書き込み，ユーザがそれらのレビューを信用して不正アプリをインストールしてしまい，被害に遭うことが考えられる．

2.2 開発者およびマーケット側における不正アプリへの既存対策

安全なアプリの提供を実現するために，開発者側での対策としてセキュリティマネージャ[3, 4] が提案されている．これは，セキュリティ上の重要となるイベントは必ずセキュリティマネー

ジャに通知することを開発者に義務づけたシステムである．開発者がこの義務を怠ると，該当のアプリを Android 端末上から削除し，Android マーケットの管理者にその旨を伝える．

一方，マーケット側での対策として，動的解析によるマルウェア検知システム [6, 7] が提案されている．このシステムは，アプリを実行して，その実行ログを基に個人情報や端末情報へのアクセスおよび漏洩を監視するシステムである．動的解析である以上，実行するアプリをインストールする必要がある．そのため主に，開発者がマーケットにアプリを投稿する際に，マーケット側で仮実行して動的解析を行うことを想定しており，Android 端末上で実行しない．

開発者やマーケット側で不正アプリ対策を行うことにより，不正アプリがユーザ間に出回ることを抑えられるが，出回ってしまった不正アプリについては，ユーザ自身が対策を講じる必要がある．

2.3 パーミッションの不正取得にたいするセキュリティ技術 [5]

パーミッションやその組合せによっては，アプリに脆弱な部分が発生することがある．アプリによるパーミッションの不正取得への対策を施すために，アプリの開発者と端末拡張機能の開発者の間でパーミッションの利用許可書を発行して，パーミッションのアクセス制御を実現する技術を提案している．

この技術は開発者側の負担が大きく，パーミッションの組合せによっては開発者が予期しないトラブルを招く問題点が残っている．そのため，各ユーザが各アプリのパーミッションを把握する必要があるが，全てのユーザにとってパーミッションの把握は現実的に困難である．

2.4 セキュリティ助言システム [8]

ユーザに対し不正アプリの危険性を示すために，パーミッションの組み合わせやマーケット上での評価およびダウンロード数によって，そのアプリの危険性を提示するシステムを提案している．

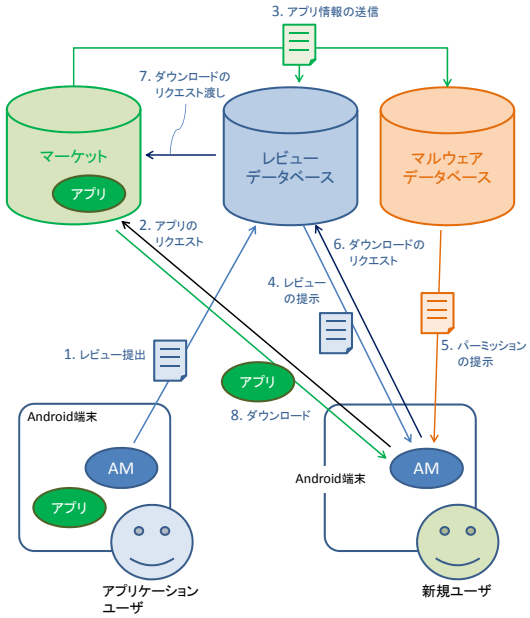

図 1: セキュリティ評価システムの全体図

このシステムは，危険性のレベルを決定する際にマーケット上での評価やダウンロード数を用いている．これらの値は，他のユーザによって意図的に操作することが可能であるため，客観的で公正な指標ではない．

3 セキュリティ評価システムの提案

3.1 セキュリティ評価システムの概要

本論文では，不正アプリの取得防止を目的としたセキュリティ評価システムを提案する．このシステムは，我々が以前提案したレビュー評価部 [9] に，パーミッションによるセキュリティ提示部を追加したシステムである．まず，アプリのユーザ全員からレビューを回収する．次に，新規ユーザがアプリをダウンロードする際に，既存のレビューと，パーミッションを基にしたアプリの危険性を新規ユーザに提示する．アプリの内容などのパーミッションのみでは推測できない事項を，レビューによって補う．セキュリ

ティ評価システムの全体図を，図 1 に示す．図中の各部位について，以下に述べる．

- マーケット

  Google Play などの既存の Android アプリ用マーケットである．

- レビューデータベース

  各アプリのレビューを保管するデータベースである．管理するデータとして，アプリ名，ユーザ名，およびレビューの 3 項目を各アプリごとに管理する．また，レビューとして，以下の項目を各ユーザごとにまとめる．

  - 記述内容
    ユーザが記述したレビューの内容である．
  - 指向性
    アプリに対するレビューの指向性であり，積極的なレビューであれば “Positive,” 消極的なレビューであれば “Negative” となる．ユーザが自身のレビューに合わせて任意に設定する．
  - 評価値
    他のユーザによる評価値であり，そのレビューに対する賛成数または反対数のそれぞれの合計値を格納する．

- マルウェアデータベース

  パーミッション情報と不正アプリ名を保管するデータベースであり，本提案で新たに追加した部分である．マルウェアデータベースでは，第三者の公的機関によって通報されたアプリ名を，不正アプリとして保管する．もしユーザによって通報された場合は，第三者の公的機関に調査を依頼し，不正アプリの判断を仰ぐ．そして，不正アプリであると判断した場合は，速やかにマーケットと該当アプリの全ユーザにその旨を送信する．

- アプリケーションマネージャ(AM)

  アプリケーションマネージャ(Application Manager: 以降，AM) とは，Android 端末内の全てのアプリを管理するアプリである．全てのアプリのダウンロード，レビューの記入，およびレビューの提示は AM を通じて行う．

3.2 パーミッションによるセキュリティ提示システム

この節では，本提案によって追加したセキュリティ提示システムについて述べる．このシステムの手順を，図 1 を用いて以下に述べる．

1. アプリユーザの AM は，自ユーザが使用中のアプリに対してレビューを促し，そのレビューをレビューデータベースに送信する．(図中の手順 1)
2. 新規ユーザの AM は，マーケットにアプリのリクエストを送信する．(図中の手順 2)
3. マーケットは，レビューデータベースおよびマルウェアデータベースに，該当アプリの名前をアプリ情報として送信する．(図中の手順 3)
4. マルウェアデータベースは，アプリ名と基にアプリに使用されているパーミッションや不正アプリとの照合を行う．
5. レビューデータベースは，アプリ名やアイコンなどのアプリ情報とそのレビューを新規ユーザの AM に送信する．(図中の手順 4)
6. マルウェアデータベースは，4 の照合結果を，使用しているパーミッションの情報と共に新規ユーザの AM に送信する．(図中の手順 5)
7. 新規ユーザの AM は，受信したレビューや照合結果をユーザに提示し，ダウンロードのリクエストがあった場合は，そのリクエストをレビューデータベースに送信する．(図中の手順 6)
8. レビューデータベースは，受信したリクエストにより新規ユーザがレビューやパーミッションの情報を閲覧したことを確認し，マー

ケットにダウンロードのリクエストを転送する．(図中の手順 7)

9. 新規ユーザの AM は，マーケットからアプリをダウンロードする．(図中の手順 8)

以上の手順により，新規ユーザはレビューとパーミッションの情報により，アプリの危険性や挙動をインストール前に把握することができる．

3.3 パーミッションを基にしたアプリの危険度の提示

マルウェアデータベースでは，READ_CONTACTS などのユーザの個人情報に触れるパーミッションや INTERNET などの通信を司るパーミッションの組合せや，不正アプリのデータを管理する．

パーミッションには，normal, dangerous, signature, signatureOrSystem の 4 つの保護レベルが存在する [10]．normal 以外の保護レベルであるパーミッションは，危険なパーミッションとして警戒する必要がある．

アプリの危険度の定義を，表 1 に示す．危険度は 3 段階とし，安全な 1 段階目を “Safety,” 2 段階目を “Caution,” 最も危険な 3 段階目を “Danger” とする．危険度が高いほど，不正アプリによって被害を受ける可能性が高い．危険なパーミッションの組み合わせ例を，表 2 に示す．それぞれのパーミッションの保護レベルが normal 以外であり，かつ，表中の左右のカテゴリによるパーミッションの組み合わせである場合を，危険なパーミッションの組み合わせとする．

これらの分類に当てはまるパーミッションをデータベース内より探索し，当てはまったものや複数組合されたものであれば，それに応じて危険度を上げる．

不正アプリの場合は，アプリストアやウィルス対策の公的機関によって不正の報告があったアプリを対象とする．これには，個人製作のアプリなど，アプリストアを通していない非正規のアプリも含む．不正アプリに該当した場合，危険度は Danger になり，不正の理由についても共に提示する．

表 2: 危険なパーミッションの組み合わせ例

端末内の個人情報に関するパーミッション	端末外への通信手段に関するパーミッション
READ_CONTACTS	INTERNET
WRITE_CONTACTS	SEND_SMS
READ_CALEMDAR	BLUETOOTH
WRITE_CALENDAR	NFC
READ_LOGS	USE_SIP
BIND_APPWIDGET	CHANGE_
READ_PROFILE	NETWORK_STATE
WRITE_PROFILE	BLUETOOTH_ADMIN

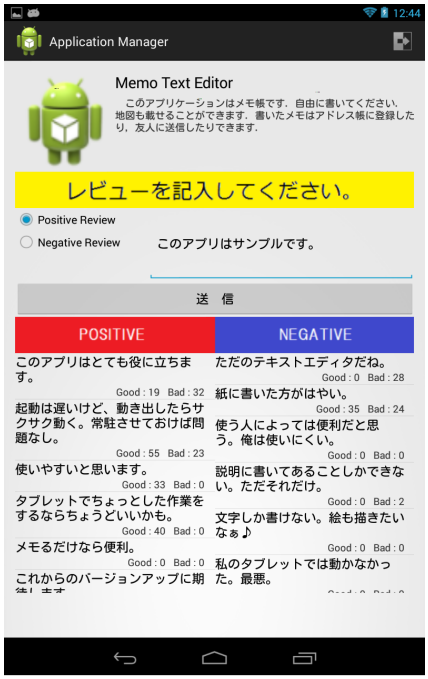

図 2: AM でのレビュー記入画面の例

3.4 アプリケーションマネージャの実装

提案したセキュリティ提示システムの有用性を確認するために，AM の実装を行った．AM の各画面の例として，レビュー記入画面を図 2 に，レビュー提示画面を図 3 に，パーミッション提示画面を図 4 にそれぞれ示す．

レビュー記入画面は，アプリのアイコン，名前，説明に併せて，新規レビューの記入と既存レビューへの賛否入力とに分けて提示する．レビューには Positive または Negative の 2 種類があり，それぞれのレビューを載せる．また，新規レビューにおいても Positive または Negative

表 1: アプリの危険度

危険度	危険なパーミッションの有無	危険なパーミッションの組み合わせ	不正アプリ (公的機関からの報告)
Safety	無し	無し	無し
Caution	有り	無し	無し
Danger	有り	有り	無し
	有り/無し	有り/無し	有り

図 3: AM でのレビュー提示画面の例

図 4: AM でのパーミッション提示画面の例

のいずれかを任意に選択できるようにしている．

レビュー提示画面とパーミッション提示画面は，アプリのダウンロード時に片方ずつ提示する．画面の切り替えは，ユーザによる画面上での横フリック操作によって切り替える．レビュー提示画面には，Positive と Negative の各レビューを提示し，その割合を円グラフによって表している．円グラフの Positive Score($PScore$) および Negative Score($NScore$) は、それぞれの総得点を S_{pos}, S_{neg}，それぞれのレビュー数を R_{pos}, R_{neg}，各レビューの賛成数を G_{pos}, G_{neg}，反対数を B_{pos}, B_{neg} として，以下の式により算出する．

$$S_{pos} = \sum_{k=0}^{R_{pos}} \{(1+\alpha)G_{pos} \times (1-\alpha)B_{pos}\},$$

$$S_{neg} = \sum_{k=0}^{R_{neg}} \{(1+\alpha)G_{neg} \times (1-\alpha)B_{neg}\},$$

$$PScore = \frac{S_{pos}}{S_{pos}+S_{neg}}, \quad NScore = \frac{S_{neg}}{S_{pos}+S_{neg}}$$

これらの式により，賛成を多く受けるレビューほどグラフの値に大きく反映され，逆に，反対を多く受けたレビューほど反映しにくくなる．α はレビュー評価のための定数であり，$0 \leq \alpha < 1$ の範囲で任意に決めることができる．α の値を増減することにより，レビューごとのグラフへの反映の度合いも増減する．そのため，レビューの賛成数と反対数に差がなく傾向を判別しづらい場合は，α の値を増加することでその差がより明確になる．円グラフによって，レビュー全体の傾向を把握しやすくなり，アプリをダウン

図 5: 各危険度の提示例

ロードするための指標になる．

パーミッション提示画面には，総合的な危険性を示す説明を青文字で示し，その下に各パーミッションの説明をリスト形式で提示する．また，レビュー提示画面とパーミッション提示画面の背景には，アプリの危険度を提示する．各危険度の提示例を図 5 に示す．1 段階目の Safety は緑，2 段階目の Caution は黄，3 段階目の Danger は赤で表す．これにより，ユーザは一目でその危険性を把握できる．

4　考察

4.1　既存研究との比較

表 3 に，ユーザ側での対策手法を対象とし，それぞれのパーミッション単体または組み合わせによる危険性確認の有無，および，レビューの有無についての比較を示す．表より，どの手法もパーミッション単体の危険性を提示するが，パーミッションの組み合わせによる危険性とレビューを提示するのは提案手法のみである．危険なパーミッションの組み合わせにより，パーミッション単体の機能だけでは捉えにくい危険性を発見することができる．また，レビューも併用することにより，アプリの内容と無関係なパーミッションや不審なパーミッション利用を推定し，そこから不正アプリへの発見へ繋がることも考えられる．

パーミッションの組み合わせの危険性提示やレビューにより，アプリの危険性や挙動をインストール前に把握できる．また，本提案手法では，ユーザの代わりに AM が各アプリのパーミッションの管理を行い，さらに危険度を 3 段階に分けて提示するため，ユーザは不正アプリの把握やパーミッションの管理が容易になると考えられる．

4.2　現在の問題点と今後の発展

提案手法の問題点として，以下の 2 点を挙げる．

- ユーザの負担の増加
- 各データベースへの負荷の増加

1 つ目のユーザの負担の増加については，レビュー評価をユーザ主体にしたことにより，全てのユーザがレビューの記入または評価を行う必要があり，それに伴ってユーザの負担が増加してしまうことである．そして，ユーザの中には，レビューを答えたくないユーザや，レビュー回答のたびにアプリを起動できないことに対して不満を抱くユーザも出てくることが予想される．そのため，レビュー拒否権などの各ユーザへの対策を講じる必要がある．

2 つ目の各データベースへの負荷の増加については，すべてのアプリ，ユーザ，レビュー，パーミッション，および不正アプリをそれぞれのデータベースが一括に管理するため，増え続けるアプリに伴い，各データベースの負荷も増加することが考えられる．そのため，負荷を削減または分散するようにシステム全体の改良を行う必要がある．

そして，ユーザがセキュリティに対して関心や知識を有するようになると，不正アプリの報

表 3: 既存研究とセキュリティ評価システムとの比較

手法	パーミッションの危険性提示の有無	パーミッションの組み合わせによる危険性提示の有無	レビューの有無
Google Play[1]	有り	無し	有り
セキュリティ助言システム [8]	有り	有り	無し
提案手法	有り	有り	有り

告がユーザ側から挙がりやすくなることも考えられる．そこで，ユーザ側からの報告に対処できるようにもシステムを改良する必要がある．例えば，ユーザ側の報告に対して調査を行うと同時に，関連するアプリの全ユーザに対して警告を促すシステムも考慮する必要がある．

5 おわりに

本研究では，不正アプリの取得防止を目的としたセキュリティ評価システムを提案した．具体的には，パーミッション情報を基にしたアプリの危険度を 3 段階に表す．さらに，レビューには評価値を設け，レビューを閲覧したユーザがそのレビューに対し賛否をつける．これにより，新規ユーザはアプリの危険性とレビューによって，不正アプリを判断することができると考えられる．

従来のレビューシステムや関連研究との比較によって，本提案手法の有用性と問題点を確認することができた．そして，提案手法により，ユーザ間でのセキュリティ対策が積極的に行われることにより，不正アプリによる被害を抑えることができると見込んでいる．

参考文献

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

[2] IPA テクニカルウォッチ - 「Android アプリの脆弱性」に関するレポート, 情報処理推進機構, 2012.

[3] 上松晴信, 可児潤也, 名坂康平, 川端秀明, 磯原隆将, 竹森敬祐, 西垣正勝: 安全な Android アプリの提供を実現するアプリ開発・管理方式 ADMS の提案, コンピュータセキュリティシンポジウム 2011(CSS2011), pp.774-778, 2011.

[4] 上松晴信, 可児潤也, 名坂康平, 川端秀明, 磯原隆将, 竹森敬祐, 西垣正勝: Android OS におけるマスカレーディングポインタを用いたプライバシー保護, 情報処理学会研究報告, Vol.2012-IOT-17, No.18, pp.1-6, 2012.

[5] 磯崎宏, 金井遵, 小池竜一: 不正な Web アプリケーションから端末プラットフォームを保護するセキュリティ技術, 東芝レビュー, Vol.66, No.11, pp.23-26, 2011.

[6] 磯原隆将, 竹森敬祐, 窪田歩, 高野智秋: Android 向けアプリケーションの挙動に注目したマルウェア検知, 暗号と情報セキュリティシンポジウム 2011(SCIS2011), 3B3-2, pp.1-7, 2011.

[7] 西本祐揮, 堀良彰, 櫻井幸一: 動的解析を用いた Android における端末情報の取得検知手法, 火の国情報シンポジウム 2012 論文集, C-3-1, pp.1-8, 2012.

[8] 松戸隆幸, 児玉英一郎, 王家宏, 高田豊雄: Android OS 上でのアプリケーション導入時におけるセキュリティ助言システムの提案, 情報処理学会研究報告, Vol.2012-CSEC-56, No.12, pp.1-7, 2012.

[9] 喜多義弘, 菅井文郎, 朴美娘, 岡崎直宣: ユーザ主体による Android アプリケーションのレビュー評価システムの提案, マルチメディア, 分散, 協調とモバイル (DICOMO2013) シンポジウム, pp.1-7, 2013.

[10] Andre Egners, Ulrike Meyer, and Bjorn Marschollek: Messing with Android's Permission Model, Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp.505-514, 2012.