

# 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

喜多 義弘<sup>1</sup> 菅井 文郎<sup>2</sup> 朴 美娘<sup>1</sup> 岡崎 直宣<sup>2</sup>

**概要**：近年，スマートフォンなどの携帯端末の普及に伴い，不正アプリケーションによるトラブルが増加している．マーケット内に出回った不正アプリケーションは完全には規制できないため，ユーザ自身がその対策を講じる必要がある．しかし，アプリケーション導入時にユーザに与えられるアプリケーションの情報は少なく，不正アプリケーションを判断することが難しい．そこで本研究では，ユーザ自身が不正アプリケーションを判断しやすく，かつ，アプリケーションの公正な評価ができるように，ユーザ主体によるレビュー評価システムを提案する．具体的には，パーミッション情報を基にしたアプリケーションの危険度を6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．そして，その賛否に基づいた評価値を，レビューを書いたユーザに通知するシステムである．

## Proposal of Review Evaluation System of Application for Android by Users

YOSHIHIRO KITA<sup>1</sup> FUMIO SUGAI<sup>2</sup> MiRANG PARK<sup>1</sup> NAONOBU OKAZAKI<sup>2</sup>

### 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いる．それに伴い，携帯端末用のアプリケーションも需要が増え，多種多様なアプリケーションによるビジネスモデルが確立しつつある．

しかし，需要が増加するほど，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をインストールしていることが挙げられる．

AndroidOS 搭載の携帯端末 (以降，Android 端末) のアプリケーション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ケーションを検知する Bouncer を実装した．しかし，不正アプリケーションは無くならず，さらに

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，アプリケーションの脆弱性に関する指針 [2] を発行したが，アプリケーションの脆弱性を完全に排除することは困難であり，不正アプリケーションによる被害の拡大を抑制できていないのが現状である．

このように，不正アプリケーションの規制は完全ではないため，現在の対策としては，アプリケーション開発側で不正アプリケーションを作らないように，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] や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] の研究が行われている．一方，ユーザ側では，不正アプリケーションの危険性を示すセキュリティ助言システム [6] やユーザによるレビューシステムがあるが，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，企業の利害を意識したレビュー操作が行われたり，新規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ケーションをインストールしない対策を講じる必要があるが，ユーザが不正アプリ

<sup>1</sup> 神奈川工科大学  
Kanagawa Institute of Technology, Atsugi, Kanagawa 243-0292, Japan

<sup>2</sup> 宮崎大学  
University of Miyazaki, Miyazaki, Miyazaki 889-2192, Japan

ケーション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、ユーザ自身が不正アプリケーションを判断しやすく、かつ、アプリケーションの公正な評価ができるように、ユーザ主体によるレビュー評価システムを提案する。具体的には、パーミッション情報を基にしたアプリケーションの危険度を5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する賛否をつける。そして、その賛否に基づいた評価値を、レビューを書いたユーザに通知するシステムである。ユーザ主体の評価を行うことにより、各ユーザがアプリケーションに対する評価への意識を向上させると共に、不正アプリケーションのインストール防止を狙う。

## 2. 関連研究

### 2.1 既存のアプリケーション評価システム

Google Play[1]などに用いられているアプリケーション評価システムは、ユーザが5段階評価を行い、使用した感想や改善点をレビューとして書き込むシステムである。これらは、新規ユーザがアプリケーションを取得する際の指標として有用である。しかし、誰でもレビューを書くことができるものの、このシステムを利用する人は一部であり、アプリケーション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、アプリケーションによる利益を獲得するために、開発者や企業がユーザに成りすまして積極的なレビューを書く場合もある。この場合、過大評価なレビューになり、客観的ではない。また、不正アプリケーションの場合、それを導入させるために誇張されたレビューや偽のレビューを書くため、一般のユーザがこれらのレビューを見て不正アプリケーション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。

これらのことから、アプリケーション評価システムには、公正で客観的なレビューが求められる。

### 2.2 セキュリティマネージャ [3], [4]

安全なアプリケーションの提供を実現するために、独自のセキュリティマネージャを提案している。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、該当のアプリケーションを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。

開発者側でセキュリティを開発することにより、不正アプリケーションが出回ることが抑えられるが、出回ってしまった不正アプリケーションに対しては、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対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、アプリケーションに脆弱な部分が発生することがある。アプリケーション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、アプリケーション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。特に、ユーザによってはインストールしているアプリケーションの種類や数が大きく異なるため、各ユーザが各アプリケーション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 [6]

ユーザに対し不正アプリケーションの危険性を示すために、パーミッションの組合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、そのアプリケーションの危険性を提示するシステムを提案している。

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. ユーザ主体によるレビュー評価システム

### 3.1 レビュー評価システムの概要

本研究では、ユーザ自身が不正アプリケーションを判断しやすく、かつ、アプリケーションの公正な評価ができるように、ユーザ主体によるレビュー評価システムを提案する。ユーザによるレビュー評価を容易に行うために、Android端末内のアプリケーションを管理するアプリケーションマネージャ (Application Manager: 以降, AM) を導入する。レビュー評価システムは以下の構成から成る。

- アプリケーションストア  
Google Playなどの従来からあるアプリケーション用マーケットである。
- レビューデータベース  
各アプリケーションのレビューを保管しているデータベースである。管理するデータは、アプリケーション名、ユーザ名、レビューである。
- マルウェアデータベース  
公的機関が報告したマルウェア名とパーミッションとその組合せについて保管しているデータベースである。
- アプリケーションマネージャ (AM)  
ユーザのAndroid端末内のアプリケーションを管理するためのアプリケーションである。全てのアプリケー

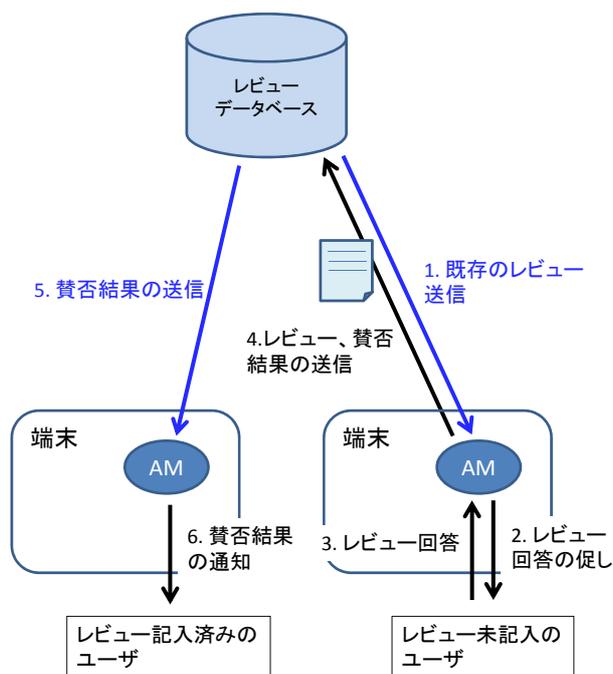


図 1 レビュー回答の流れ  
Fig. 1 Flow of review entry

アプリケーションのダウンロード、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。

ユーザーが実施するレビューは、以下の構成とする。

- Pos/Neg 値  
レビューの内容が積極的 (Positive) か消極的 (Negative) かを示す。これはレビューの指向性を示すものであり、レビューを記入するユーザー自身が値を決定する。
- レビュー本文  
レビューの本文は、ユーザーが自由に記述する。
- レビュー評価値  
レビューに対する他のユーザーからの評価を数値化したものである。

各ユーザーのレビューをレビューデータベースが、不正アプリケーションの情報をマルウェアデータベースがそれぞれ管理し、アプリケーションストアからアプリケーションをダウンロードする新規ユーザーの AM は、これらのデータベースからそれぞれのデータを収集してユーザーに提示する。

### 3.2 アプリケーションマネージャを用いたレビュー評価手法

AM を用いたレビュー評価手法について述べる。この手法は、レビュー回答とレビュー提示の 2 つの構成に分かれている。それぞれについて、以下に述べる。

#### 3.2.1 レビュー回答

アプリケーションをインストールしているユーザーに対し、そのアプリケーションのレビューの回答を促す。レビュー回答の流れを、図 1 に示す。以下の手順における AM は、レビュー回答を行うユーザーの AM とする。

- (1) アプリケーションの使用累積時間または使用回数が一定の値に達したとき、AM はレビューデータベースから既存のレビューを受け取り、ユーザーへレビュー回答をアプリケーションの次回起動時に促す。(図 1 の手順 1,2)

- (2) レビュー回答のユーザーはレビュー回答方法として、レビューを記入する場合と記入しない場合の 2 通りのうちいずれかを選択する。

- レビューを記入する場合 (図 1 の手順 3,4)
  - (a) Pos/Neg 値を設定する。レビュー回答のユーザーはレビューの内容が積極的であれば Positive を、消極的であれば Negative を選択する。
  - (b) レビューの本文を記入する。
  - (c) AM はアプリケーション名、レビュー回答のユーザー名、レビューの本文、および Pos/Neg 値をレビューデータベースに送信する。
- レビューを記入しない場合 (図 1 の手順 3~6)
  - (a) レビューデータベースは、該当アプリケーションの他のユーザーを Pos/Neg 値別にランダムで複数選択し、彼らのレビューを AM に送信する。
  - (b) AM は受信したレビューを Pos/Neg 値別にレビュー回答のユーザーへ提示する。
  - (c) レビュー回答のユーザーは提示されたレビューから 1 つ以上選択し、そのレビューに対する賛否を回答する。
  - (d) AM はレビューの賛否結果をレビューデータベースに送信する。
  - (e) 賛否結果を受信したレビューデータベースは、そのレビューを記入したユーザーに賛否結果を送信する。

レビューを記入したユーザーの AM は、レビューの賛否結果を受信すると、結果が賛成の場合はレビューの評価値を 1 上げ、反対の場合はレビューの評価値を 1 下げる。

レビュー回答が自動的に促されるのは、各アプリケーションで 1 回のみであり、レビュー回答以降は促されない。ユーザーがレビューを再回答したい場合は、任意に記入画面を再表示することが可能である。また、アプリケーションがバージョンアップした場合は、以前のバージョンでのレビューは削除し、新規のレビューの記入を促す。レビューの変更や新規記入があった場合、評価値は初期化する。

#### 3.2.2 レビュー提示

アプリケーションをダウンロードする際の新規ユーザーに対し、そのアプリケーションのレビューを提示する。レビュー提示の流れを、図 2 に示す。

- (1) 新規ユーザーがアプリケーションをダウンロードする際、新規ユーザーの AM はレビューデータベースにアプリケーションの情報を送信する。(図 2 の手順 R1)
- (2) レビューデータベースは、受信したアプリケーション

R1, M1. 各データベースへアプリケーションの情報送信  
R2, M2. レビュー、不正アプリケーションのデータ送信

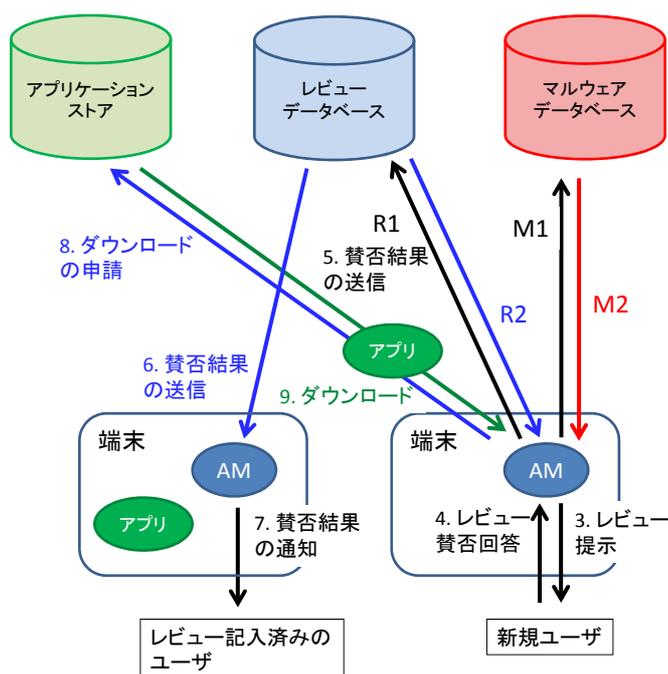


図 2 レビュー提示の流れ  
Fig. 2 Flow of review display

名に該当するユーザを Pos/Neg 値別にそれぞれ複数選択し、彼らのレビューを新規ユーザの AM に送信する。(図 2 の手順 R2)

- (3) 新規ユーザの AM は受信したレビューを Pos/Neg 値別に提示する。
- (4) 新規ユーザはそれらのレビューから 1 つ以上選択し、それぞれのレビューに対する賛否をつける。
- (5) 新規ユーザの AM は、賛否結果をレビューデータベースに送信する。
- (6) 賛否結果を受信したレビューデータベースは、そのレビューを記入したユーザの AM に賛否結果を送信する。
- (7) レビューを記入したユーザの AM は、そのユーザに賛否結果を提示する。
- (8) 新規ユーザの AM は、アプリケーションのダウンロードの申請をアプリケーションストアに送信する。
- (9) アプリケーションストアからアプリケーションをダウンロードする。

### 3.3 アプリケーションの危険度の提示手法

#### 3.3.1 危険度の定義

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、不正アプリケーションのデータを管理する。

アプリケーションの危険度の定義を、表 1 に示す。危険

度のレベルが高いほど、アプリケーションによる危険性が高い。危険なパーミッションは、以下の 2 つに分類される。

- 端末内の個人情報に関するパーミッション READ\_CONTACTS, CONTROL\_LOCATION, UPDATES など
- 端末外への通信手段に関するパーミッション SEND\_SMS, INTERNET など

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のレベルを上げる。

不正アプリケーションの場合は、アプリケーション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ケーションを対象とする。これには、個人製作のアプリケーションなど、アプリケーションストアを通していない非正規のアプリケーションも含む。不正アプリケーションに該当した場合、危険度はレベル 4 以上になり、さらに危険なパーミッションの有無や組合せによってレベル 6 まで割り振る。また、レベルと共に不正の理由についても提示する。

#### 3.3.2 危険度の提示手法

危険度の提示手法について、以下に述べる。以下の手順における AM は、アプリケーションの新規ユーザの AM とする。

- (1) 新規ユーザがアプリケーションをダウンロードする際、AM はマルウェアデータベースにアプリケーション名と使用しているパーミッションを送信する。(図 2 の手順 M1)
- (2) マルウェアデータベースは、AM からの受信後、不正アプリケーションとしての登録の有無と、危険なパーミッションとその組合せについて、AM に送信する。(図 2 の手順 M2)
- (3) AM は受信した結果から、危険度を 6 段階で算出し、新規ユーザに提示する。
- (4) 不正アプリケーションである場合はその旨を警告する。

#### 3.4 不正アプリケーション通知手法

不正アプリケーションの報告があった場合のユーザへの通知手法について、以下に述べる。

- (1) マルウェアデータベースがアプリケーションストアやウィルス対策の公的機関から不正アプリケーションの報告を受ける。
- (2) マルウェアデータベースはレビューデータベースに不正アプリケーションの警告を送信する。
- (3) レビューデータベースは、不正アプリケーションを導入している全ユーザの AM に、受信した警告を転送する。
- (4) 警告を受信した AM は、ユーザへ即座にアプリケーション削除の警告を促す。

表 1 アプリケーションの危険度  
Table 1 Hazardous Levels of Applications

レベル	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合せ	不正アプリケーション(公的機関からの報告)
1	無し	無し	無し
2	有り	無し	無し
3	有り	有り	無し
4	無し	無し	有り
5	有り	無し	有り
6	有り	有り	有り

- (5) ユーザが削除に応じない場合、AM は被害拡大防止のためにアプリケーションのレビューの変更を促す。
- (6) AM は変更したレビューをレビューデータベースに送信する。
- (7) レビューが変更された場合、レビューデータベースはそのレビューの評価値を初期化する。

### 3.5 アプリケーションマネージャにおけるユーザへの提示例

AM におけるユーザへの提示例として、レビュー記入画面を図 3 に、レビュー提示画面を図 4 に、アプリケーションの危険度の提示画面を図 5 に、それぞれ示す。

レビュー記入画面は、アプリケーションのアイコンと説明に併せて、レビューの記入と既存レビューへの賛否の入力とに分けて提示する。レビューの記入では、始めにレビューの内容が Positive か Negative かを選択し、本文を記入する。記入後は送信ボタンをタップし、レビュー回答を終了する。既存レビューへの賛否の入力は、Positive Review と Negative Review とに分けられたレビューから 1 つ以上選び、そのレビューに賛成であれば Good ボタンを、反対であれば Bad ボタンをタップする。いずれかのボタンをタップすると、レビュー回答は終了する。

レビュー提示画面は、アプリケーションのアイコンと説明に併せて、レビューの傾向と既存レビューへの賛否の入力を提示する。レビューの傾向は、Positive Review/Negative Review それぞれのレビュー数を分子、レビューの総数を分母とした円グラフを提示する。既存レビューへの賛否の入力は、レビュー記入画面と同様に、1 つ以上選択したレビューの Good ボタンまたは Bad ボタンをタップする。いずれかのボタンをタップすると、レビュー提示は終了する。

アプリケーションの危険度の提示画面は、アプリケーションのアイコンと説明に併せて、6 段階に示した危険度と理由、およびパーミッション情報を提示する。危険度の理由の文面は、パーミッションの組合せごとにマルウェアデータベースで管理し、AM はパーミッション組合せ情報と共にその文面も受信し、ユーザに提示する。パーミッション情報は、既存のアプリケーションマーケットと同様

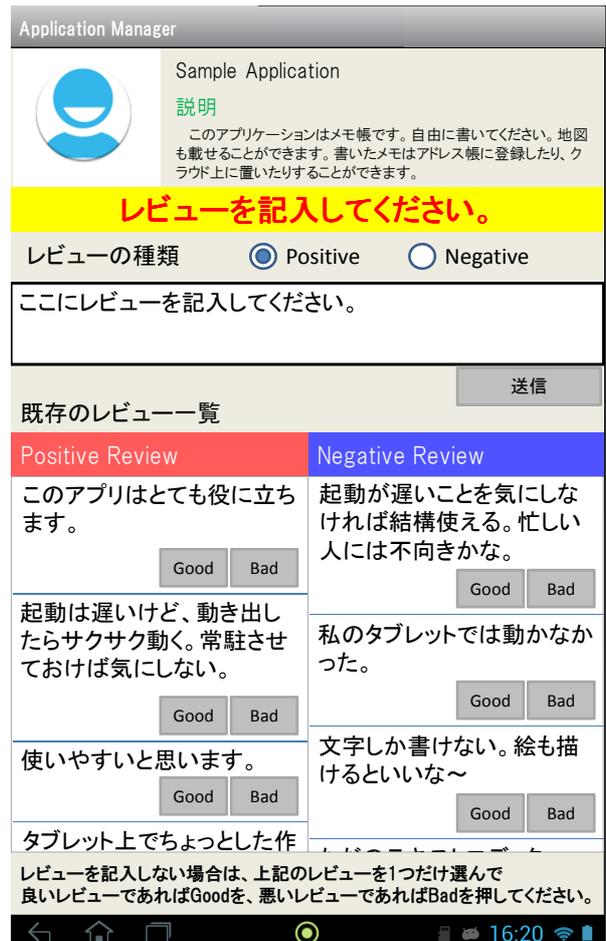


図 3 AM 上のレビュー記入画面

Fig. 3 Review entry on Application Manager

のものを提示する。

## 4. 考察

### 4.1 従来のレビューシステムとの比較

従来のレビューシステムは、パーミッションによる危険性が分かりにくく、レビューもアプリケーションの内容に無関係なレビュー、悪意のあるレビュー、または、利害によって操作されたレビューなど公正ではない場合がある。本提案手法では、アプリケーションの危険度をパーミッションを基に 6 段階にレベル分けすることにより、一目で

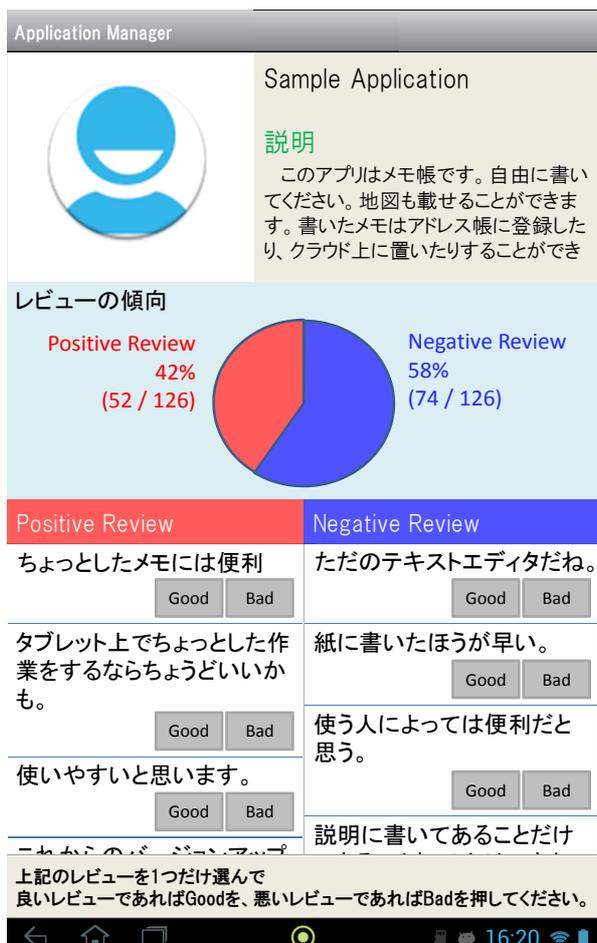


図 4 AM 上のレビュー提示画面

Fig. 4 Review display on Application Manager

不正アプリケーションを把握することができる。レビューシステムもユーザによる評価を重視し、ユーザが自身のレビューの評価値を把握することにより、ユーザ間で公正なレビューを心がけるようになり、悪意のあるレビューや操作されたレビューが減少することが考えられる。

#### 4.2 関連研究との比較

論文 [3], [4] では、不正アプリケーションが出回らないように、開発者によるセキュリティ対策を講じていた。これにより、不正アプリケーションが出回ることは減少するが、既にマーケット上に出回ってしまった不正アプリケーションについては有用ではない。本提案手法では、ユーザによって不正アプリケーションの判断を行うことにより、たとえ不正アプリケーションが出回ってしまった場合でも被害を最小限に食い止めることができると考えられる。

論文 [5] では、パーミッションのアクセス制御を行うことにより不正アプリケーションによる被害を抑えているが、開発者およびユーザともに負担が大きく、特にユーザが各アプリケーションのパーミッションの管理を行うことは困難である。しかし、本提案手法では、ユーザの代わりに AM が各アプリケーションのパーミッションの管理を



図 5 AM 上のアプリケーションの危険度の提示画面

Fig. 5 hazardous level display on Application Manager

行い、さらに 6 段階の危険度の提示により、ユーザは不正アプリケーションの把握やパーミッションの管理が容易になる。

論文 [6] では、アプリケーションの危険度をユーザに分かりやすく提示するが、その危険度の決定をパーミッションの組合せだけでなく、アプリケーションのマーケット上での評価やダウンロード数も基に行っている。これらの情報は第三者によって操作されやすいため、それに基づいた危険度は客観性に欠け、公正かつ正確に提示することが容易ではない。本提案手法では、危険なパーミッションの組合せや公的機関による不正アプリケーションの報告を基にアプリケーションの危険度を決定している。そのため、客観的で公正な評価によって危険度を把握できるため、ユーザに対して、より安全にアプリケーションの提供を行うことができると考えられる。

#### 4.3 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
  - レビュー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ケーション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のが予想される。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つ目のレビューデータベースへの負荷の増加については、すべてのアプリケーション、ユーザ、およびレビューを一括に管理するため、増え続けるアプリケーションに伴い、レビュー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、不正アプリケーションの報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、関連するアプリケーション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、ユーザ自身が不正アプリケーションを判断しやすく、かつ、アプリケーションの公正な評価ができるように、ユーザ主体によるレビュー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ケーションの危険度を6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。そして、その賛否に基づいた評価値を、レビューを書いたユーザに通知するシステムである。

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、不正アプリケーション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ト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] 松戸隆幸, 児玉英一郎, 王家宏, 高田豊雄: AndroidOS 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.