Vol.2014-DPS-158 No.17
Vol.2014-CSEC-64 No.17
2014/3/6

パーミッション制御ツールを利用した Google Play でユーザに提供するべき情報の検討

中佳博 †1　　中沢実 †1

Android OS 搭載携帯電話の高機能性と，その利用者の増加からユーザがアプリに対して個人情報の流出の点で注意を払うことが求められている．しかし一般のユーザにはアプリが要求しているパーミッションについての情報や，そのパーミッションをどのようにアプリが用いるのかという情報が提供されていない．そこで，本研究では，パーミッションの観点からアプリをインストールするためのマーケットである Google Play において，インストールする前にユーザに提供するべき情報について検討し，アプリへの信頼性を向上させる新たな手法を考案する．

Study on Information of should be provided to users in Google Play using on Permission control tool

YOSHIHIRO ATARI†1　MINORU NAKAZAWA†1

Recently, as high performance of the cellular phone equipped with Android OS and an increase of the number of the users, the user is requested to pay the application program attention in the point of the personal information leak. However, the point of the permission that the application demands against the ordinary user. The point how the application uses the permission is not being offered. Then, in this research,from the viewpoint of the permission in Google Play that is the market to install the application program, at first, we considered information that had to be offered to the user before it installed it. Next, we propose a new technique for improving the reliability to the application program.

1. は　じ　め　に

Android OS 搭載携帯電話の高機能性と，その利用者の増加からユーザはアプリケーションに対して個人情報の流出の点で注意を払うことが求められている．しかし一般のユーザにはアプリケーションが要求しているパーミッションについての情報や，そのパーミッションをどのようにアプリケーションが用いるのかという情報が提供されていない．そのような状態で，インストール後は自己責任という環境は，専門知識のないユーザにはとても危険な状態である．また，そのような専門知識のないユーザは，なす術なく不用意にアプリケーションをインストールしている．これは対処しなければならない問題と考えられる．

過去の研究例としては，アプリケーションケーションの挙動を可視化することによるセキュリティ対策(戸田　尚希・鈴木　秀和・旭　健作・渡邊　晃,2012)[1]や，Android OS における機能や情報へのアクセス制御機構の提案(川端　秀明・磯原　隆将・竹森　敬祐・窪田　歩・可児　潤也・上松　晴信・西垣　正勝,2011)[2]などがある．前者は多数のアプリケーションに対しての不審な情報をサーバーで解析することにより安全性の判断の補助を行うものであり，後者は Android OS の処理に割り込み処理機能を加えたカスタム OS によりパーミッション使用毎にユーザへの許可を求めるものである．どちらもパーミッションの観点から，不審なパーミッションに対してユーザに注意を呼びかけるものである．

これら 2 つのような研究では，実際に動作しているアプリケーションから不審な点を見つけ出すものであるが，本研究では，アプリケーションをインストールするためのマーケットである Google Play において，インストールする前にユーザに提供するべき情報について研究し，アプリケーションへの信頼性を向上させる新たな手法を考案する．

方法としては，まずユーザは現状の Google Play のどの部分の情報を得てアプリケーションに対しての信頼性を得ようとしているのか．また，そこからユーザが知っておくべき情報と Google Play が提供するべき情報を導きだす．

具体的には，ユーザはインストール時のパーミッション警告画面をどの程度確認しているかを調査し，不要にパーミッションを許可するとどのような危険性があるのかをユーザに示す．また，既にインストールしてしまっているアプリケーションで危険性のあるものをユーザに示し，パーミッションの除去を行なった後，アプリケーションに対して安心感がどれほど向上したかを調査する．これらの結果から，ユーザはインストールする際にどのような情報を提供されるべきなのかを考察する．

ⓒ2014 Information Processing Society of Japan

Vol.2014-DPS-158 No.17
Vol.2014-CSEC-64 No.17
2014/3/6

2. 概　要

2.1 アンドロイドアプリケーションの概要

アンドロイドアプリケーションは Google Play を公式のマーケットとして配布されておりユーザの多くは，公式である Google Play からのダウンロードは安全であると思っている．しかし過去に何度か Google Play からアンドロイド型のマルウェアが発見されたことがあり，ユーザにはアプリケーションへの注意が求められている．

Android OS 搭載型のスマートフォンはアプリケーションをインストールすることにより高機能化を図ることができる．アプリケーション自体はユーザから様々な権限を許可されることにより，その能力を増やすことができる．もちろんパーミッションを一切要求せずに使用することも可能であるが，機能が大きく制限されるため市場に出回っているほとんどのアプリケーションはインストールの際にパーミッションを要求する．

アンドロイド型のマルウェアはこのパーミッションを不正に利用することで，ユーザの意図しない挙動をとることができる．そのため，ユーザにはパーミッション警告画面に注意することと，信頼できるアプリケーションのみをインストールすることが求められている．

2.2 アンドロイドアプリケーションの課題

アンドロイドアプリケーション型のマルウェアの被害にあわないために，ユーザにはアプリケーションに対する注意が呼びかけられている．しかし，ユーザには身を守るために提供されている情報がとても少ないことが現状である．

まずアプリケーションについての情報としてインストール時のパーミッション警告画面がある．実際に Google Play からアプリケーションをインストールしようとした際に表示される画面を図 1，図 2 に示す．図 1 が，インストール時にまず初めに表示される画面であり，下部にあるボタンをタップすることで図 2 の画面を表示することができる．図 2 の状態が表示できる全てのパーミッションの情報であるが，実際にはこれはアプリケーションが要求しているパーミッションを全て表示しているわけではない．図 1 で表示されている画面には危険とみなされているパーミッションが表示されている．図 2 のように画面を開くと，低リスクとみなされているパーミッションを追加で表示することができる．具体的には，protectionLevel が dangerous のパーミッションが図 1 で表示されており，normal のパーミッションが図 2 のように画面を開くことで表示することができる．protectionLevel が signature と signatureOrSystem のパーミッションに関しては表示されることはない．また，図 1，図 2 から分かるように，それぞれのパーミッションについての説明はとても希薄であり，パーミッションを許可することでアプリケーションにどのような挙動をとらせることができるのかを把握することは難しい．



図 1　警告画面①



図 2　警告画面②

3. 実　験

3.1 実験方法の考案

これまでの研究例として，アプリケーションケーションの挙動を可視化することによるセキュリティ対策(戸田尚希・鈴木　秀和・旭　健作・渡邊　晃,2012)[1]や，Android OS における機能や情報へのアクセス制御機構の提案(川端秀明・磯原　隆将・竹森　敬祐・窪田　歩・可児　潤也・上松　晴信・西垣　正勝,2011)[2]があり，インストール済みのアプリケーションの挙動から，不審なパーミッションを持つアプリケーションをユーザに示す取り組みや，組み込み処理を取り入れたカスタム OS を用いる手法が提案されている．どちらもアプリケーションの挙動を監視し，検証結果からユーザの判断の補助を行っており，効果的な方法である．しかし，これらはアプリケーションをインストールした後の検証方法でありアプリケーションンストール前にユーザへの判断の補助を行うには別の手法が必要となる．

今回は，インストール前にユーザが自ら判断するためにはどのような情報の提供が必要であるのかということと，現在 Google Play で提供されている情報が希薄である点に焦点を当てて検討を進めた．

3.2 実験方法

実験の方法は，まずユーザがどの点でアプリケーションに対して不信感を抱いているのかを調査した．その目的として端末内のアプリケーションが取得しているパーミッションから脅威を予測し，ユーザに示した．脅威の予測手法としては，「タオソフトウェア出版 Android Security　安全なアプリケーションケーションを作成するために」の第 6 章に記載されている「疑われやすいパーミッションの組み合わせ」[3]を用いた．例えば、インターネット通信のよう

ⓒ2014 Information Processing Society of Japan

Vol.2014-DPS-158 No.17
Vol.2014-CSEC-64 No.17
2014/3/6

な外部との通信機能と、連絡先や通話履歴を読みとる機能のパーミッションの両方とも持つアプリケーションケーションは、ユーザに無断で連絡先などの個人情報を外部に送信できる、というように予測を行う。脅威の予測からユーザに注意を呼び掛け，脅威の対象になっているパーミッションと予測される脅威の内容を伝え，ユーザに不審なパーミッションを選択してもらう．その後，アプリケーションから不審を抱いているパーミッションの除去を行う．パーミッションが除去され予測される脅威がなくなった状態でアプリケーションを使用してもらい，ユーザの安心度を計る．ここで，ユーザからは不審なパーミッションを除去することでアプリケーションに対する不信感が取り除かれていることを確かめる．その結果から，ユーザはどのような情報が提供されればアプリケーションに対しての安心感が向上するのかを調査する．

3.3 システム概要

作成するシステムとして，パーミッションの組み合わせから予測される脅威をユーザに提示し，除去したいパーミッションを選択後アプリケーションのパッケージをパーミッション除去処理先に送信するまでを作成したアプリケーションで行う．送信先でパーミッション除去をした後，ユーザにパッケージファイルを送信しアプリケーションを再インストールしてもらう．不審なパーミッションを除去したアプリケーションを使用することでユーザの安心度がどう変化したかを考察し，Google Play で提示すべき情報を導きだす．図 3 にシステム概要のイメージ図を示す．

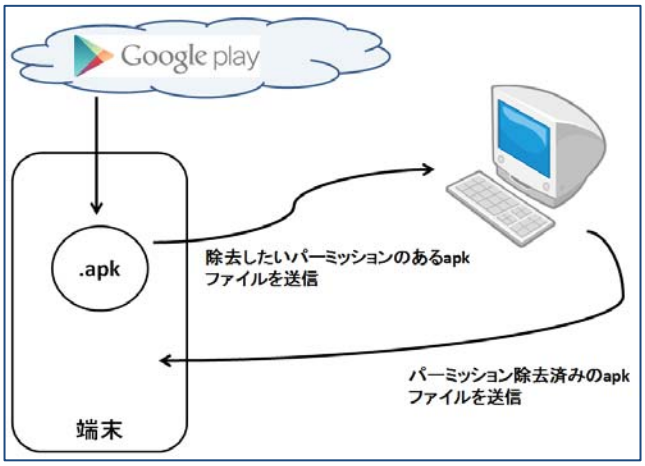


図 3　システム概要のイメージ図

3.4 試作したパーミッション除去アプリケーション

本研究で開発したアプリケーションは，端末内にあるアプリケーションが何のパーミッションを許可されているのかという情報を取得し，その中から危険な組み合わせのパーミッションを許可されているアプリケーションを探しだす．危険な組み合わせの対象となっているパーミッションと，どのような危険性があるのかをユーザに示す．その後ユーザが不審だと思ったパーミッションがあれば，パーミッションを選択してもらい，そのパーミッションの情報とアプリケーションのパッケージをパーミッション除去の処理先に送信する．実験対象となる端末は，アンドロイドバージョンが 2.3.3～4.1 までのものとした．これは，本研究を始めた時期に日本で最も多く使用されているアンドロイドバージョンが 2.3.3 であったことと，その当時リリースされている最新のバージョンが 4.1 だったことからこのバージョンを選択した．

開発環境については，windows7 のマシンで Eclipse[4] と Android SDK[5]を用いて開発を行った．Eclipse とはソフトウェアの統合開発環境であり，Android SDK とはアンドロイド向けソフトウェアを開発するための開発環境である．

3.5 パーミッション除去の方法

アプリケーションから送信された除去したいパーミッションの情報とアプリケーションのパッケージを用いてパーミッションの除去を行い，送信元の端末にパーミッションを除去したアプリケーションのパッケージを送信する．その後再インストールを行う．パーミッションを除去する方法として，そのアプリケーションが要求するパーミッションを記述している部分を書き変える．具体的には，まずアプリケーションのパッケージファイルである apk ファイルを解凍し，パッケージを分解する．その中の一つである AndroidManifest.xml にアプリケーションが要求するパーミッションについての情報が書かれているため，その部分を消去する．編集した AndroidManifest.xml を用いて分解したパッケージファイルを再度圧縮する．ここまででパーミッションを除去したアプリケーションのパッケージが生成され，これを端末に送信し再インストールを行う．再インストールの際の警告画面では除去したパーミッションは要求されず，インストール後も除去したパーミッションは使用されない．このようにすることで，ユーザから見るとパーミッションの除去が実現されている．なお，apk ファイルの解凍から AndroidManifest.xml の編集，再圧縮の工程は apktool[6]を用いて行う．apktool とは，アプリケーションのパッケージを解凍し，ソースコードを編集し，再度圧縮を行うツールである．また，アンドロイドアプリケーションのパッケージである apk ファイルは zip 形式で圧縮された書庫ファイルになっており，一般の zip 形式のファイルを解凍する手法で容易に解凍することができる．図 4 にパーミッション除去のイメージ図を示す．

ⓒ2014 Information Processing Society of Japan

Vol.2014-DPS-158 No.17
Vol.2014-CSEC-64 No.17
2014/3/6

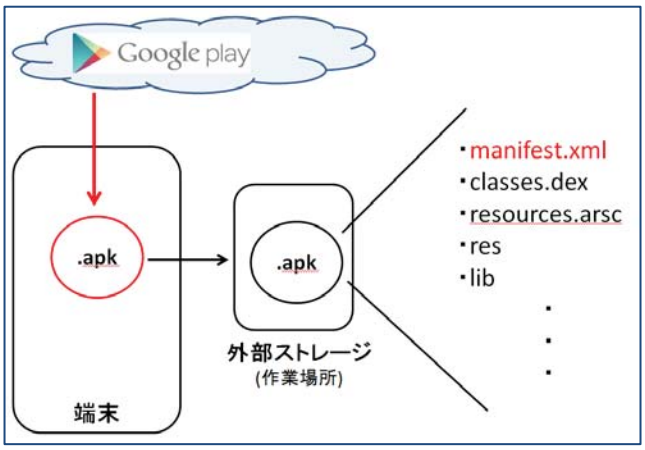


図 4　パーミッション除去のイメージ図

3.6 検証結果

今回作成したシステムを実際にアンドロイドアプリケーションのユーザに使用してもらい，アンケートを行った．アンケートを行う目的としては，以下の 3 つの仮説が正しいかどうかを検証するために行う．

- ユーザがアプリケーションに対して不信感を抱いている
- 適切な情報を与えることでユーザの安心度が向上する
- ユーザが求めている Googe play で提供するべき情報を導くことができる

また，今回作成したシステムは不特定多数の人に使われない想定をしているため，より多くの人に検証したときの状態を予想するためにもアンケート調査は必須であると考えた．

アンケートは，私の身の回りにいる知人の 20 代～50 代の男女 28 名に行った．アンケート項目の作成には，『アンケート調査の方法(NISHINO Hideki, 2004)』[7]を参考に作成した．作成したアンケートの内容を表 1 に示す．また，アンケート結果を表 2 に示す．

3.7 考察

表 2 のアンケート結果から，質問項目 3 の「パーミッション警告画面の内容を確認し，要求されているパーミッションについて把握，同意できたか」という質問に対し「把握せず，同意した」と答えた人が全体の 100%であった．また，質問項目 4 の「要求されているパーミッションを把握していないが同意した人はなぜ同意したのか」という質問に対し「アプリケーションが欲しかったから」と答えた人が 71%であり，最も高い数値となった．また質問項目 5 の「アンドロイドアプリケーションについて，アプリケーションが個人情報を流出するなどの危険があることを知っていたか」という質問に対し「はい」と答えた人は全体の 43%であり，半数以上の人がアプリケーションの個人情報流出について知らなかったことが分かった．ここから，現状のパーミッション警告画面の情報ではユーザに適切な情報は提供されておらず，ユーザもパーミッションについて危険視せずにインストールを行っていることが分かる．

また，質問項目 6「これまで知らなかったアプリケーションの危険性について知ることができたか」質問項目 7「パーミッションを除去することでアプリケーションに対しての安心度は上がったか」質問項目 8「今後アプリケーションをインストールする際に開発者からのパーミッションについての情報を知りたいか」という質問に対し，「はい」と答えた人はどれも 85%以上いる結果となった．このことからユーザは，現状のパーミッション警告画面のようにパーミッションの内容を述べているだけの内容ではなく，どのような危険性があるのかという情報と，不審に感じるパーミッションがあったとしてもそれに代わる開発からの説明を必要としていることが分かる．またこれらの結果から，アンケートを実施する際に立てた 3 つの仮説は確かめられていることが分かる．

表 1　実施したアンケートの内容

項目番号	質問内容	回答選択肢
1	インストールする際に、パーミッション警告画面の内容を確認したことがありますか	はい・いいえ
2	「はい」と答えた人、どのくらいの頻度で内容を確認しますか	・最初の 1回だけ ・3回に 1回ほど ・5回に 1回ほど ・10回に 1回ほど その他（　　）
3	内容を確認して要求されているパーミッションについて把握、同意できましたか	・把握して、同意した ・把握せず、同意した ・把握も同意もしない
4	要求されているパーミッションを把握してないが同意した人、なぜ同意したのですか	・アプリが欲しかったから ・良く分らなかったから ・なんとなく見ただけだったから ・公式で安全だと思ったから ・その他（　　）
5	アンドロイドアプリについて、アプリが個人情報を流出するなどの危険があることを知っていましたか	はい・いいえ
6	今回のツールを用いて、これまで知らなかったアプリの危険性について知ることができましたか	はい・いいえ
7	今回のツールを用いてパーミッションを除去し、アプリに対して安心度は上がりましたか	はい・いいえ
8	今後アプリをインストールする際に開発者からのパーミッションについての情報を知りたいですか	はい・いいえ
9	パーミッションを選択できるツールがあれば良いと思いますか	はい・いいえ
10	これまでパーミッションを除去したいと思ったことはありましたか	はい・いいえ

ⓒ2014 Information Processing Society of Japan

Vol.2014-DPS-158 No.17
Vol.2014-CSEC-64 No.17
2014/3/6

表 2　アンケート結果

項目番号	回答	回答の割合
1	「はい」と回答した人	50%
2	1で「はい」と答えて最初の1回だけ見る人	21%
2	1で「はい」と答えて最初の3回に1回ほど見る人	35%
2	1で「はい」と答えて最初の5回に1回ほど見る人	21%
2	1で「いいえ」と答えて最初の10回に1回ほど見る人	7%
3	1で「はい」と答えて把握せず、同意した人	100%
4	「アプリが欲しかったから」と回答した人	71%
4	「よく分らなかったから」と回答した人	35%
4	「なんとなく見ただけだったから」と回答した人	25%
4	「公式で安全だと思ったから」と回答した人	25%
5	「はい」と回答した人	43%
6	「はい」と回答した人	92%
7	「はい」と回答した人	85%
8	「はい」と回答した人	92%
9	「はい」と回答した人	85%
10	「はい」と回答した人	14%

4. 今後の展開

今回の研究では，パーミッションの観点からのみ Google Play でのユーザに提供するべき情報の問題点とその改善についての研究行ったが，改善した場合のユーザへの効果と，効率よく情報が提供されるためのしくみまでは研究を進めることができなかった．

今後の課題は，今回の研究から導きだした提供すべき情報を提供した場合の効果と，効率よく情報を提供するしくみを考察していくことである．

5. ま　と　め

今回，Google Play で提供するべきであるパーミッションについての情報について，ユーザはどのような点でアプリケーションに対して不信感を抱いているのか，どのような情報が求められアプリケーションに対して安心感を持つことができるのかという事柄について調査を行った．

これまで，ユーザはパーミッションへの注意が必要だと一般に言われてきたが，本研究からユーザに対して具体的にパーミッションのどのような情報の提供が必要であるかという指標を導きだすことができた．また現状のパーミッション警告画面の内容に加えてパーミッションがもつ危険性と，不審だと感じられるパーミッションについての開発者からの説明がユーザに安心感を与え，提供されるべき情報であるということを導きだすことができた．

参 考 文 献

1) 戸田，鈴木，旭，渡邊，” アプリケーションケーションの挙動を可視化することによるセキュリティ対策”(2012)
2) 川端，磯原，竹森，窪田，可児，上松，西垣，”Android OS における機能や情報へのアクセス制御機構の提案”(2011)
3) タオソフトウェア株式会社，”Android Security 安全なアプリケーションケーションを作成するために”(2012)
4) Eclipse 入門” http://www.javadrive.jp/eclipse3/”(2014/02/10アクセス)
5) Android SDK のダウンロードとインストール” http://www.javadrive.jp/android/install/index1.html”(2014/02/10 アクセス)
6)Android アプリの配布パッケージ apk の解析について” http://codezine.jp/article/detail/6992?p=2”(2014/0210 アクセス)
7) NISHINO Hideki，”アンケート調査の方法”< http://www.arch.kobe-u.ac.jp/~a7o/activity/sub/subzemi2004nishino-anketo2.pdf >(2013/12/20 アクセス) (2004)

ⓒ2014 Information Processing Society of Japan