Vol.2012-DPS-150 No.12
Vol.2012-CSEC-56 No.12
2012/2/29

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

松戸隆幸† 児玉英一郎† 王家宏† 高田豊雄†

Android 搭載端末では，アプリケーション導入時に，アプリケーションが利用する機能や情報をユーザに通知し承認を仰ぐことを安全性の根拠としている．しかし，承認内容を理解していない，または確認を怠る不注意なユーザの存在が問題となっている．また，複数の機能が組み合わされた場合の危険性を判断することは，技術に精通していないユーザには困難である．そこで本研究では，アプリケーション導入時に，ユーザの判断支援を行うシステムを提案し，プロトタイプの実装を行った．

A Proposal of Security Advisory System at the Time of the Installation of Applications on Android OS

TAKAYUKI MATSUDO† EIICHIRO KODAMA†
JIAHONG WANG† TOYOO TAKATA†

For an Android-powered device, its security is established such that an application, when it is installed, declares the functions and other information that it will use, and user approves or rejects the declaration according to reviewing results. The problem is that, however, it is difficult for users to completely understand the details of a declaration, and careless users may neglect the approval process. In particular, in the case that a combination of multiple functions is involved, it would be impossible for users who are unfamiliar with technical details to evaluate its risk. In this paper we propose a system model for supporting users' approval decisions when an application is installed, and describe an implementation of a prototype of the proposed system model.

† 岩手県立大学
Iwate Prefectural University

1. はじめに

近年，スマートフォンと呼ばれる高機能携帯電話が急速に普及している．スマートフォンの特徴として，汎用の OS を搭載し，必要に応じて利用者がアプリケーションを追加することで機能の拡張が可能であるという点があげられる．

スマートフォン向けオープンプラットフォームの一つである Android[1]では，アプリケーションの開発環境が無料で提供されており，多くの人が自由に開発を行うことができる．また，アプリケーションは Android Market[2]を通じて公開可能であり，闊達なアプリケーションの流通が実現している．その為，Android 向けのアプリケーションは爆発的に増加しており，現在 40 万本以上[3]のアプリケーションが Android Market で公開されている．

しかし，アプリケーションの増加に伴い，Android 端末を標的としたマルウェアの存在が問題となっている．Android Market では，アプリケーション公開の際に事前審査が不要な為，マルウェアが混入する可能性を孕んでいる．実際，Android 端末の位置情報や端末情報を狙ったマルウェア，SMS を悪用して不当にユーザから金銭を得ようとするマルウェアなどが度々発見され増加傾向にある[4].

Android では，このようなセキュリティ脅威を軽減する仕組みとして，パーミッション機構[5]が存在する．パーミッション機構とは，アプリケーション開発者が，マニフェストファイルと呼ばれるアプリケーションに関する情報を記述するファイルに，そのアプリケーションが使用する機能や情報をあらかじめ定義し，アプリケーションがインストールされる際に，定義した機能をパーミッションという形でユーザに通知し，承認を仰ぐ仕組みである．アプリケーションは，ユーザからパーミッションを承認されることで，パーミッションの範囲内でのみ機能を使用可能となる．しかし，パーミッション機構は,ユーザのセキュリティ管理上の負担を生むという問題点がある．実際，著者の所属する大学において Android ユーザを対象とした予備調査を行った結果，約 6 割のユーザがパーミッション機構を理解していない，または確認を充分に行っていないという結果が得られた．これでは，充分なセキュリティ確保は期待できない．また，パーミッション機構では，利用する機能や情報を大まかな単位でしか把握することが出来ず，複数のパーミッションが組み合わされた場合の危険性を判断することは技術に精通していないユーザには困難である．

そこで本稿では，Android 上でのアプリケーションインストール時における，ユーザのセキュリティ管理上の負担軽減と，アプリケーションの危険性理解補助の 2 点に着目し，ユーザの判断支援を行うシステムを提案する．

Vol.2012-DPS-150 No.12
Vol.2012-CSEC-56 No.12
2012/2/29

2. 背景

2.1 Android アプリケーション

Android にインストールされた各アプリケーションは，Dalvik 仮想マシンと呼ばれる仮想マシンのサンドボックス上で実行される．その為，デフォルトではアプリケーションはサンドボックス外の機能や情報にアクセスすることは出来ない．しかし，パーミッション機構により，ユーザから明示的に承認を得ることで，アプリケーションはサンドボックス外にアクセスすることができ，より利便性の高いアプリケーションが実現可能となる．

2.2 パーミッション機構

アプリケーションが使用する機能や情報は，開発者によってマニフェストファイルに記述され，パッケージ内に付加される．そして，アプリケーションをインストールする際に，パッケージインストーラがマニフェストファイルを読み取り，図 1 のような「許可」としてパーミッション情報をユーザに提示する．ユーザが提示されたパーミッションを慎重に判定し，全てのパーミッションに同意できる場合のみ「同意してダウンロード」ボタンを押してインストールを完了する．また，一度与えられたパーミッションは，自動的に追加/削除されることはない．しかし，パーミッション機構には以下のような問題点がある．

- ユーザのセキュリティ管理上の負担が大きく，パーミッション機構を理解していない，または確認を怠る不注意なユーザの場合には，意図した通りの効力を発揮できない．
- 利用する機能や情報を大まかな単位でしか把握することが出来ない為，複数のパーミッションが組み合わされた場合の危険性を判断することは，技術的に精通していないユーザには困難．

2.3 関連研究

Android のセキュリティ問題についていくつか研究が行われている．

Enck らの研究では，インストール時にアプリケーションの持つパーミッションの組み合わせから危険性を簡易的に判断し，ユーザに提示する手法を提案している[6]．しかし，対象としている危険性の範囲が狭いことや，ユーザ提示を行うインターフェースについて考慮されておらず，ユーザが危険性を把握しづらいという問題点がある．

竹森らは，マルウェアの感染源であるマーケットプレイスが安全にあることで，多くのユーザの携帯電話を保護できるという考えのもと，アプリケーションのログ情報に基づく未知アプリケーションの事前審査支援ツールを提案している[7]．しかし，現状では一部のサードパーティマーケットでしか事前審査は行われておらず，ユーザ側での対策の必要性は依然として残っている．

Shin らは，パーミッション機構の欠陥を指摘し，不正に重要なパーミッションを取得する攻撃例を提示し，解決策について議論した[8].

図 1　パーミッション確認画面の例
Figure 1　Example of confirmation permission.

3. 提案

3.1 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

本提案手法によるセキュリティ助言システムは，アプリケーションのパーミッションに基づいた危険性検知, および危険性提示によるユーザの判断支援の 2 段階に分け，ユーザのセキュリティ管理上の負担軽減と，アプリケーションの危険性理解に関する支援を行う．

パーミッションに基づいた危険性検知では，あらかじめ危険性のあるパーミッションの定義ルールを作成する．そして，アプリケーション導入時に定義ルールとの比較を行い，定義ルールに当てはまる場合のみユーザへ危険性を提示する．提示の際は，検知されたアプリケーションの危険性レベル，危険性の種類，マーケット上から取得した情報をユーザに把握しやすい形で示し，ユーザの判断支援を行う．

セキュリティ助言システムの動作手順は以下の通りである．

(1) 危険性の検知

アプリケーションのインストール完了時に，アプリケーションのパーミッション情報とマーケット上の情報を取得し，あらかじめ定義されたルールを用いて危険性があるか判定する．

Vol.2012-DPS-150 No.12
Vol.2012-CSEC-56 No.12
2012/2/29

(2) **危険性の提示**

インストールされたアプリケーションに危険性があると判定した場合，ユーザに危険性を理解しやすい形で提示し，削除/許可の判断を仰ぐ．

3.2 パーミッションに基づいた危険性検知

危険性の検知は，アプリケーション導入時にそのアプリケーションに付加されたマニフェストファイルからパーミッション情報を取得し，定義ルールと比較を行う．あらかじめ危険性のあるパーミッション，またはパーミッションの組み合わせを定義し，それに当てはまるアプリケーションが検知された場合のみユーザに提示を行う．定義ルールは，関連研究で示されたパーミッションの組み合わせと，事前調査で収集したマルウェアに付加されていたパーミッション情報を参考に 21 パターンを作成した．

図 2 に定義ルールの例を示す．

- INTERNET & READ_PHONE_STATE
  - 端末情報の漏洩（電話番号やシリアル番号）
- INTERNET & READ_CONTACTS
  - 端末情報の漏洩（連絡先）
- INTERNET & ACCESS_FINE_LOCATION
  - 位置情報の漏洩（精細な位置）
- SEND_SMS
  - SMS スパム、プレミアムレート SMS の送信

図 2　定義ルールの例
Figure 2　Example of rules definitions.

3.3 危険性の提示によるユーザの判断支援

ユーザにアプリケーションの危険性を把握しやすくさせる目的で，以下の 4 つの項目を含んだユーザインタフェースを提示し，アプリケーション導入時の判断支援を行う．

3.3.1 危険性レベル

検知されたアプリケーションがどれくらいの危険性を持っているかを危険性レベルとして表示する．危険性レベルは全部で 5 段階とし，直感的にユーザが危険性を判断しやすいよう，レベルに応じて背景の色を変える．色は JIS の安全色[9]を参考に，危険レベルの高い順に赤/黄赤/黄/黄緑/緑と定義した．レベルは，検知された定義ルールとアプリケーションのマーケット上での評価･ダウンロード数を基に決定する．また，危険性レベルの項目をタップすることでレベルの設定理由，ユーザの行動の勧告を表示する．

危険性レベルの決定手順は以下のとおりである．

(手順 1) 危険性レベルの初期値として，あらかじめ 3.2 節で説明した定義ルールに 3~5 の値を設定する．

(手順 2) マーケット上の評価･ダウンロード数をそれぞれ 3 段階で判定し，段階に応じて−2/−1/0 と重みを付ける．マーケット上の評価･ダウンロード数と対応する重みを表 1 と表 2 に示す．

(手順 3) 手順 1 で設定されたレベルからマーケット上の評価･ダウンロード数の重みに応じてレベルを減算し，最終的な危険性レベルを決定する．レベルが 1 を下回った場合は全て 1 とする．

表 1　マーケット上の評価と重みの対応
Table 1　Market evaluations and the corresponding weights.

マーケット上の評価	4〜5	3〜4	3〜0
重み	−2	−1	0

表 2　マーケット上のダウンロード数と重みの対応
Table 2　Download numbers and the corresponding weights.

マーケット上のダウンロード数	50000 以上	1000〜50000	1000 未満
重み	−2	−1	0

3.3.2 危険性の種類

検知されたアプリケーションがどのような危険性を持っているかを危険性の種類として表示し，危険性を直接ユーザに知ってもらうことでより柔軟に判断を行えるようにする．種類は，位置情報の流出/携帯情報の流出/料金の自動発生/その他の危険性の 4 つに分類し，それぞれ検知された定義ルールに応じてアイコンを表示する．更に，アイコンをタップすることで危険性に関する詳細な説明を表示する．

3.3.3 マーケット上の評判

検知されたアプリケーションのマーケット上での評価とダウンロード数をそれぞれ 3 段階で判定し，段階に応じて星マークのアイコンを表示する．システム側で基準を明確にすることにより，アプリケーション導入に不慣れなユーザの判断を支援する．マーケット上の値に対するシステム上の判定を表 3 と表 4 に示す．

表 3　マーケット上の評価に対するシステムの判定
Table 3　Market evaluations and the corresponding evaluations of the system.

マーケット上の評価	4〜5	3〜4	3〜0
システム上の判定	☆☆☆	☆☆	☆

Vol.2012-DPS-150 No.12
Vol.2012-CSEC-56 No.12
2012/2/29

表 4　マーケット上のダウンロード数に対するシステムの判定
Table 4　Market download numbers and the corresponding evaluations of the system.

マーケット上のダウンロード数	50000 以上	1000～50000	1000 未満
システム上の判定	☆☆☆	☆☆	☆

3.3.4 ネガティブ意見のコメント

検知されたアプリケーションのマーケット上のコメント中から評価が 0~2 の低いものだけを表示させる．これは評価が低いネガティブなコメントの中にアプリケーションの危険性を示唆したものが含まれているという仮定に基づいている．

4. 評価

本提案手法について，危険性検知と判断支援を行うユーザインタフェースそれぞれについてプロトタイプを作成した．危険性検知については，アプリケーションに付加されているマニフェストファイルからパーミッション情報を取得し，3.2 節で定義したルールと一致するかを判定するシステムをコンピュータ上で再現した．判断支援を行うユーザインタフェースについては，実際の Android アプリケーションとして実装し，ユーザ意見を参考に，文章の改善やアイコン表示を見やすくするなどの形成的評価を繰り返しつつ[10]，ユーザビリティの向上を図った．作成したユーザインタフェースのイメージを図 3 に示す．また，形成的評価の結果，危険性レベルが 1 の場合，殆どのユーザが安全だと判断するという結果が出た．その為，危険性レベルが 1 の場合はユーザインタフェースの提示を行わないものとした．

図 3　ユーザインタフェースのイメージ
Figure 3　User interface.

4.1 危険性検知の評価結果

定義ルールの有効性を示す為に，実際のマルウェア[a]180 個と Android Market 上から入手したアプリケーション[b]261 個を，それぞれ関連研究[6]の定義，本提案手法の定義で検知率の比較を行った．危険性検知の評価結果を図 4 と図 5 に示す．関連研究ではマルウェアの検知率が 47%であるのに対し，提案手法では 95%という高い値となり，より多くのマルウェアに対応できることが示された．しかし，Android Market 上から入手したアプリケーションについても，提案手法では 62%が危険性のあるアプリケーションと判定されており，誤検知も多いことが分かったが，必ずしも技術に精通していないユーザに対して，過去にマルウェアで用いられたパーミッションの組合せであることを積極的に提示することは有益であると考えられる．

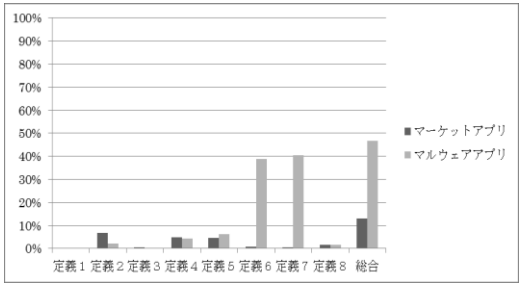

図 4　関連研究の検知率
Figure 4　Detection rate of the related study.

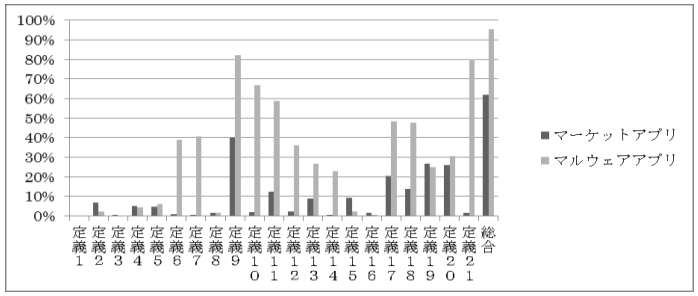

図 5　提案手法の検知率
Figure 5　Detection rate of the proposed approach.

a) 29 種のマルウェア名称に分類されるハッシュ値の異なる検体 180 個をインターネット上から入手した．
b) 2011 年 12 月時点で Android Market 上で公開されており安全と判断されている．

Vol.2012-DPS-150 No.12
Vol.2012-CSEC-56 No.12
2012/2/29

4.2 ユーザインタフェースの評価結果

ユーザインタフェースの有効性を示す為に，従来のアプリケーション導入手順と提案手法を使用したアプリケーション導入手順をユーザに比較してもらい，ユーザ負担，判断精度，使用感の面で総括的評価に関する実験を行った．評価実験には仮想的に作成した安全なアプリケーションの導入画面と危険なアプリケーションの導入画面を18 個ずつ用意し，被験者に危険なアプリケーションの判断を行ってもらった．対象となる被験者は，技術に精通していない，またはアプリケーション導入時にパーミッション確認を行ったことのない人に限定し，36 名に行ってもらった．

4.2.1 ユーザ負担

ユーザ負担について提案手法の有効性を示す為，事前に用意した 36 個のアプリケーション導入画面について危険性を判断する際に要した時間をそれぞれ計測し，評価を行った．評価結果を図 6 に示す．評価結果から，既存のダウンロード手順に比べて提案手法を使用したダウンロード手順の方がアプリケーションの危険性を判断する時間が短い結果となった．この関係を調査する為に検定を行った結果，両者の間に有意差があり(t 検定 t 境界値 片側 = 1.69, t = 7.27), ユーザ負担が少ないことが分かった．

4.2.2 判断精度

判断精度について提案手法の有効性を示す為，事前に用意した 36 個のアプリケーションのうち，安全なアプリケーションと危険なアプリケーションをどのくらい正確に被験者が判断できるかを評価した．評価結果を図 7 に示す．評価結果から，既存のダウンロード手順に比べて提案手法を使用したダウンロード手順の方が正答率が高い結果となった．この関係を調査する為に検定を行った結果，両者の間に有意差があり(t 検定 t 境界値 片側 = 1.69, t = −16.91)，ユーザが正確な判断を行いやすい事が分かった．

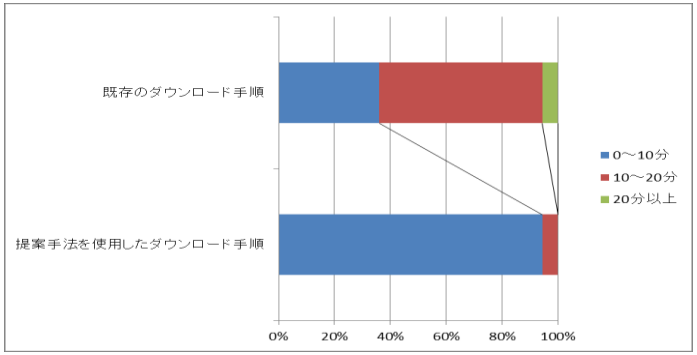

図 6　解答時間の比較
Figure 6　Response time.

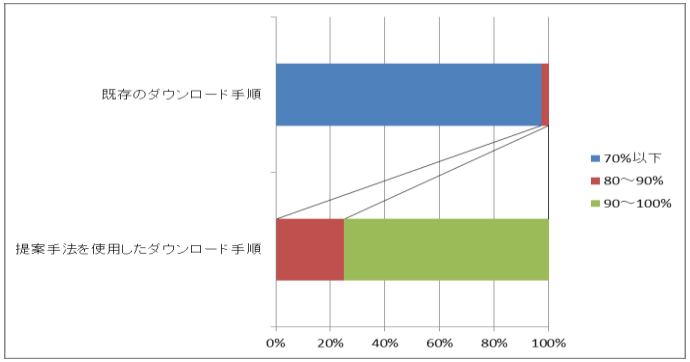

図 7　正答率の比較
Figure 7　Percentage of correct answers.

4.2.3 使用感

提案したユーザインタフェースについて，評価実験後にアンケートを実施し，分かりやすさと危険性を判断する上での参考度合いについて，それぞれ危険性レベル/危険性の種類/マーケット上の評判/ネガティブ意見のコメントの 4 項目に分け評価を行った．評価結果をそれぞれ図 8，図 9，図 10，図 11 に示す．危険性レベルと危険性の種類の項目については，分かりやすさ/参考度合い共に良い意見が 9 割を超え，被験者の評価が高かった．マーケット上の評判については，分かりやすさ/参考度合い共に良い意見が 7 割程度であったが，分かりづらい/あまり参考にならないという意見も少数あった．同じくネガティブ意見のコメントについても，あまり参考にならないという意見が少数あった．

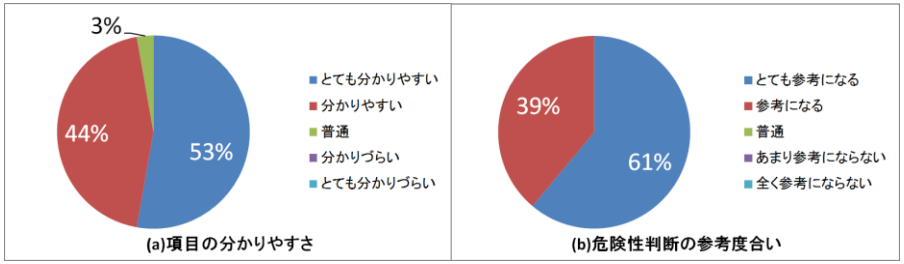

図 8　危険性レベルアンケート結果
Figure 8　Survey results of the risk levels.

Vol.2012-DPS-150 No.12
Vol.2012-CSEC-56 No.12
2012/2/29

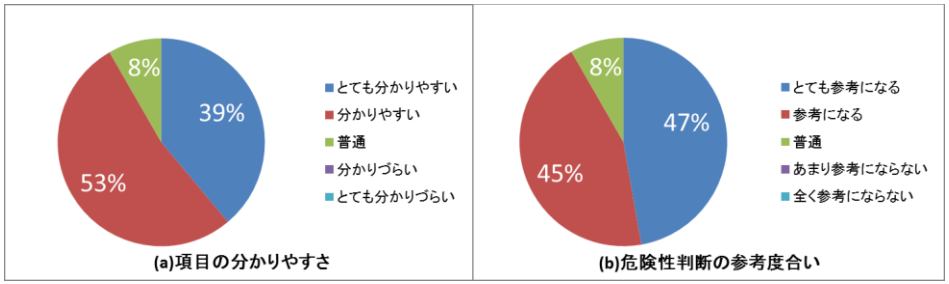

図 9　危険性の種類アンケート結果
Figure 9　Survey results of risk types.

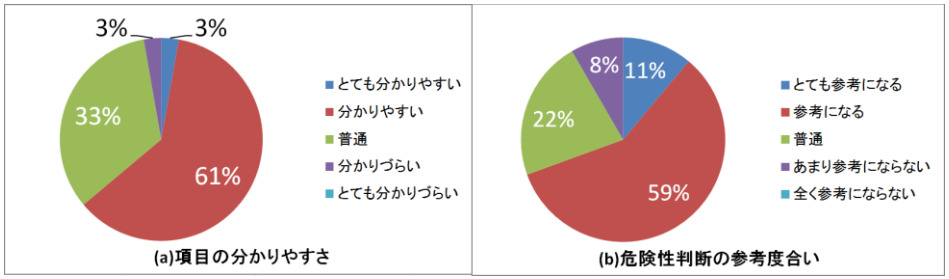

図 10　マーケット上の評判アンケート結果
Figure 10　Survey results of the market reputations.

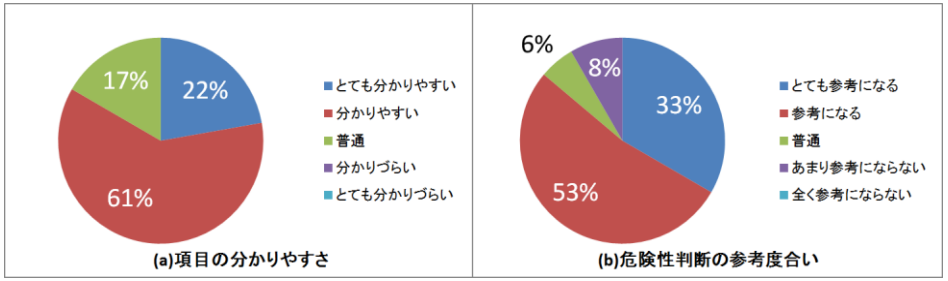

図 11　ネガティブ意見のコメントアンケート結果
Figure 11　Survey results of the negative comments.

4.3　マーケット上の評価数･ダウンロード数における判定基準の評価

3.3.1 節と 3.3.3 節で設定したマーケット上の評価･ダウンロード数の判定基準の妥当性について評価を行った．評価データは Android Market 上でのマルウェア情報が入手困難だった為，サードパーティマーケットに残されていたマルウェア公開時の情報を使用した[c]．評価数とダウンロード数それぞれのマルウェア分布割合を図 12，図 13 に示す．評価数に関しては，評価者が少数の場合信頼性に欠けると判断し，評価者数が 10 人以下の場合は評価数を考慮しないこととした．評価結果から，評価 4 以上の場合はマルウェアの存在は確認できなかった．また，評価 3~4 の範囲でもマルウェアの割合が 12%と比較的少なく，大半が評価 3 以下もしくは，評価者数 10 以下ということが分かった．ダウンロード数についても，50000 以上の場合はマルウェアの存在は確認できず，大半が 1000 未満ということが分かった．この結果から，マルウェアアプリケーションはマーケット上の評価が低い，あるいは評価者数が少なく，ダウンロード数も少ない傾向にあることがいえる．

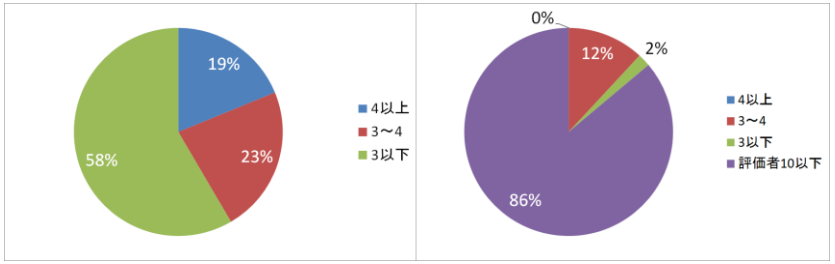

図 12　評価数に対するマルウェアの割合
Figure 12　Ratio of malwares with respect to evaluation number.

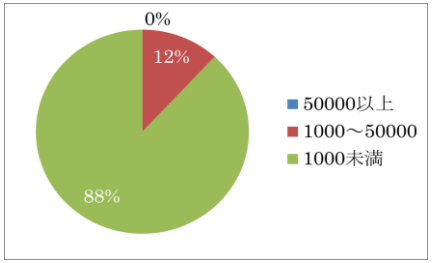

図 13　ダウンロード数に対するマルウェアの割合
Figure 13　Ratio of malware with to number.

c) サードパーティマーケットには Android Market 上のアプリケーション情報とリンクさせ公開しているものが存在する．

Vol.2012-DPS-150 No.12
Vol.2012-CSEC-56 No.12
2012/2/29

5. まとめ

本論文では，パーミッションに基づいた危険性検知，および判断支援を行うユーザインタフェース部分について提案し，プロトタイプを作成して評価を行った．評価結果より，パーミッションに基づいた危険性検知では，関連研究より多くのマルウェアに対応できることが示された．また，総括的な評価実験を行い，ユーザ負担軽減，危険性の判断補助，ユーザインタフェースの分かりやすさと危険性判断の参考度合いについてそれぞれ評価し，有効性を示した．しかし，分かりづらい/あまり参考にならないという意見も少数存在したため，改善の余地があると思われる．最後に，アプリケーションの評価･ダウンロード数についてシステム側での判定基準の妥当性を評価した．

謝辞 本研究は一部科学研究費(基盤研究(C)23500094)の助成を受けたものである．本研究を行うにあたって協力して頂いたセコム株式会社の葛野弘樹氏に感謝の意を表する．

参考文献

1) Android, http://www.android.com/
2) Android Market, https://market.android.com/
3) DISTIMO, Distimo Blog, Google Android Market Tops 400,000 Applications, http://www.distimo.com/blog/2012_01_google-android-market-tops-400000-applications/
4) McAfee Labs, McAfee 脅威レポート 2011 年第 3 四半期, http://www.mcafee.com/japan/media/mcafeeb2b/international/japan/pdf/threatreport/threatreport11q3.pdf
5) Access permissions, http://developer.android.com/intl/ja/reference/android/Manifest.permission.html
6) William Enck, Machigar Ontang, and Patrick McDaniel: On Lightweight Mobile Phone Application Certification, Proc. of 16th ACM Conference on Computer and Communications Security, pp.235-245 (2009).
7) 竹森 敬祐, 磯原 隆将, 窪田 歩, 高野 智秋: Android 携帯電話上での情報漏洩検知, Proc. of The 2011 Symposium on Cryptography and Information Security Kokura, Japan, Jan. pp.25-28 (2011).
8) Wook Shin, Sanghoon Kwak, Shinsaku Kiyomoto, Kazuhide Fukushima, and Toshiaki Tanaka: A Small but Non-negligible Flaw in the Android Permission Scheme, Proc. of IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY), pp.107-110 (2010).
9) JISZ9103:2005 安全色－一般事項
10) D.A.Norman, et al.: *User Centered Design*, Lawrence Erlbaum Assoc. Inc., Hillsdale, NJ (1986).