情報処理学会論文誌 Vol.56 No.12 2302–2312 (Dec. 2015)

Androidマルウェアの対策行動へ利用者を誘導する警告ダイアログの提案と評価

高橋 雅香[1,a)] 高田 哲司[1,b)]

受付日 2015年3月9日, 採録日 2015年9月2日

概要：Android 端末をターゲットにしたマルウェアは急増し，セキュリティ上の問題となっている．これに対する現実の対応策は Anti-Virus（AV）ソフトウェアを利用することである．しかし，Android 用 AV ソフトウェアはマルウェアを削除することができず，利用者に対策行動を実施させる必要がある．その役割は AV ソフトウェアのダイアログによって行われているが，実際には利用者を対策行動まで誘導できていないと考えられる．そこで本研究では，警告通知と対策行動への誘導というダイアログの 2 機能について改善案を提案し，それらの効果について被験者による評価実験を行った．これにより利用者を対策行動に誘導しうる新たなダイアログを提案し，その改善効果の可能性を示すことができた．本論文では，この改善版ダイアログの提案と評価実験について報告する．

キーワード：携帯端末，マルウェア，アンチウィルスソフトウェア，警告画面，インタフェースデザイン，脅威認知，モバイルセキュリティ

Designing Effective Alert Dialog to encourage Android Users to take Countermearsure Action to Android Malware

Motoka Takahashi[1,a)] Tetsuji Takada[1,b)]

Received: March 9, 2015, Accepted: September 2, 2015

Abstract: Malware applications for the Android OS has been released in the Internet and an application market. A threat caused from malware applications becomes non-negligible issue. A prior measure against the malware applications is an Anti-Virus software and the software notifies users of a malware infection to their terminals by a dialog interface. However, the dialogs in commercial Anti-Virus software products did not play a role of a risk notification and are simply ignored by mobile phone users. This is a serious issue for mobile phone security. Therefore, we propose an alternative customized malware notification dialog for both “leading users a better counter action to malware” and “inducing users to understand a security threat from a dialog information”. We also conducted a user evaluation study for measuring an effectiveness of the proposed dialogs.

Keywords: mobile phone, Android, malware, Anti-Virus software, alert dialog, interface design, threat recognition, mobile security

1. はじめに

アプリケーション（以降，本論文ではアプリと記す）のインストールが可能な携帯端末は，その普及にともないマルウェアの感染先として注目されるようになった．Alcatel-Lucent の “MALWARE REPORT-Q4 2013” [1] によると，2013 年には世界で 1,160 万台以上の携帯端末がマルウェアに感染しているとされている．中でも Android OS を搭載した携帯端末を狙うマルウェアの数は，2013 年の 1 年間で 5 万未満から約 45 万の約 20 倍と急速に増加していると報告している．Android OS では，次のような理由からマルウェア配布が容易であるとされている．

[1] 電気通信大学
The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[a)] m.takahashi@mail.uec.jp
[b)] zetaka@computer.org

- 公式アプリマーケットが自動審査である
- 公式アプリマーケット以外のサードパーティマーケットや任意の Web サイトでもアプリの配布が可能

Android の公式アプリマーケットでは「Bouncer」と呼ばれる不正アプリ検出機能でアプリの審査を行っている [2]．Bouncer は，アプリのアップロード段階でそのアプリが既知のマルウェアかどうか判断する．またクラウド上で，端末でのアプリ稼働をシミュレートすることによって危険な挙動の有無を調査する．しかしこの仕組みでも，新種のマルウェアが検証をすり抜ける可能性がある．またサードパーティマーケットや Web サイトにおいて，マルウェアが配布される可能性もある．携帯端末向け OS の 1 つである Apple 社の iOS と比較すると，iOS では公式アプリマーケットは手動審査であり，公式アプリマーケット以外でアプリを配布することはできない．このことから，Android OS は他の携帯端末向け OS よりもマルウェア配布が容易であると考えられる．

この問題に対し，セキュリティベンダは Android OS 向けの AV ソフトウェアを研究・開発している．Android OS のアプリが個人情報に関するコンポーネントを利用する場合，ユーザによる許可（パーミッション）を得る必要がある．そこでパーミッションを用いた静的解析や，実際の挙動を調べる動的解析などがマルウェア検知に用いられている．

しかし Android OS において，AV ソフトウェアはマルウェアを削除することができない．PC 向けの AV ソフトウェアはマルウェアを検知した場合そのまま削除に至るが，Android OS ではアプリの削除をユーザの承諾なしに行うことができないため，検知を通知することしかできない．したがって，AV ソフトウェアにおいて重要なのは，ユーザにマルウェアに関する情報を「通知」する仕組みと，その通知によってユーザによる対策行動を「実行させる」ことである．

マルウェアを検知した AV ソフトウェアは，ユーザに対して警告を発する．本研究の調査では，17 製品中 17 製品がダイアログを用いて警告を発していた．AV ソフトウェアの警告ダイアログは，ユーザに対してセキュリティ脅威を通知する．しかし既存手法では，セキュリティに関心の低いユーザは，セキュリティ脅威を認識せず，警告を無視するという問題がある．また Trend Micro Mobile Security [3] では，Android OS の標準ダイアログを用いて**図 1** のような警告を表示するが，この警告が表示された際，警告ダイアログ以外の画面部分（図中の赤線枠内）を触れることにより警告を閉じることができる．そのため，警告が表示された際に誤って警告以外の部分に触れてしまい，警告を見ずに閉じてしまうという問題がある．本研究における調査では，既存の Android OS 向け AV ソフトウェアの 17 製品のうち，Trend Micro Mobile Security をはじめとする 5 製品がこのような仕様であった．

図 1 Android OS の標準ダイアログ例 [3]
Fig. 1 Alert dialog on Android OS [3].

そこで本研究では，AV ソフトウェアにおけるマルウェア検知の通知方法の改善を目的とする．この取り組みにより，Android マルウェアの情報がユーザに伝達され，その反応として利用者がマルウェア対策行動を行うことを期待する．これにより，Android 向け AV ソフトウェアがより良いマルウェア対策になることを目指す．

以降，本論文では 2 章で関連研究を紹介し，3 章で本研究の目標とアプローチを明確にする．4 章では警告ダイアログの改善案について説明し，5 章ではそれらの案の改善効果を検証する実験について述べる．6 章では得られた知見を基にした改良版ダイアログの概要を説明し，7 章で改良版ダイアログの評価実験について，8 章では改良版ダイアログに関する考察と今後の課題を述べる．

2. 関連研究

本章では，1 章で取り上げた問題を解決するのための既存研究・製品について取り上げる．

2.1 インストール時の警告手法

Android version 4.4.2 では，Android 公式マーケットである Google Play からアプリをインストールしようとすると，アクセス許可の確認画面が表示される．しかし確認画面は，**図 2** のように画面右端の矢印を押して詳細を確認しなくとも同意ボタンを押すことができるため，ユーザがアクセス許可を理解せずに許可を出すという問題点が Kelley らの研究 [6] によって示唆されている．Kelley らの研究 [7] では，**図 3** のように，アプリが収集する個人情報をチェッ

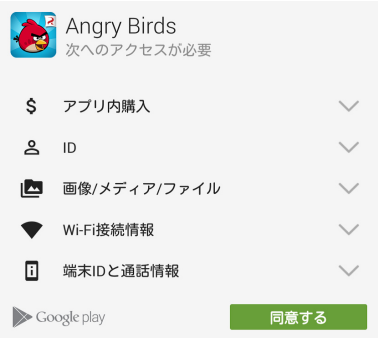

図 2 Google Play のアプリインストール画面
Fig. 2 Permission confirmation interface at Google Play.

図 3 Kelley らの研究概要
Fig. 3 Proposed dialog by Kelley et al.

クボックス形式で表示し，アプリによって漏えいする可能性のある個人情報を一目で分かるようにする手法が提案されており，被験者実験の結果，ユーザのアクセス許可の認識を最大で 28%向上させることが報告されている．しかしこの手法では個人情報が重要なものであるかを認識していない，セキュリティに関心が低いユーザへは効果的ではないことも判明している．

Harbach らの研究 [8] では，Google Play のインストール画面を改良し，アプリをインストールすることで取得可能になる情報を画像や具体的な数値でインストール前に提示することによって，ユーザに危険性を伝える手法を提案している（図 4）．被験者実験の結果，既存の手法と比べて個人情報漏えいの懸念によるインストール回避に，最大 23.7%の貢献をすることが報告されている．しかし，この手法はインストール前に個人情報を端末上に表示してしまうため，第三者に個人情報を閲覧され，漏えいされる可能性がある．また悪意のある第三者に端末が操作されないとしても，公共の場でアプリのインストールをしようとした際に意図せず個人情報が第三者に閲覧される懸念もある．

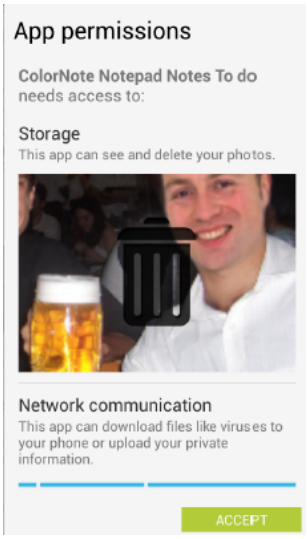

図 4 Harbach らの研究概要
Fig. 4 Proposed dialog by Harbach et al.

2.2 アプリ実行時の警告手法

Balebako らは，ステータスバーを用いてユーザに個人情報の送信を通知する Privacy Leaks just-in-time（JIT）[9] というシステムを提案している．JIT はアプリが個人情報を送信したことをステータスバー上にメッセージとして表示する．しかし，メッセージが表示されるのは数秒間であり，ユーザがそれを見逃すと通知領域を開かないかぎりそれに気づく機会がない．また，この研究では JIT を使用したあと個人情報が漏洩していることが分かったアプリを家族や友人にお勧めするかどうかを被験者に質問しているが，被験者 19 名のうち 12 名はゲームの機能性はデータ送信よりも重要であるため，お勧めすると回答している．したがって，個人情報について意識していないユーザは，メッセージが表示されても適切に対応しないことが懸念される．

また前章で述べた Android マルウェアの脅威に対し，セキュリティベンダは，Android 端末をターゲットとした AV ソフトウェア [3], [5] を配布・販売している．本研究で調査した結果，既存の 17 製品中 17 製品すべてがアプリ実行時にマルウェアを検知するとアプリの削除を促す警告ダイアログを表示していた．しかし，ユーザに与えられる選択肢は「マルウェアと判定されたアプリの削除」または「当該アプリの継続利用」の 2 つのみであり，アプリの使用を目的とするユーザは，目的を果たすため継続利用を選択してしまうという問題がある．またマルウェアによるセキュリティ脅威の詳細は，ユーザが能動的な行動をおこして確認する必要があることが多い．図 5 はその一例である．したがってセキュリティに関心の低いユーザは詳細を確認せ

図 5 AV ソフトウェアによるダイアログ警告例 [4]
Fig. 5 Example of alert dialog by Anti-Virus software [4].

ず，セキュリティ脅威を認識しないという問題もある．

3. 本研究の目標とアプローチ

本研究における目標は，携帯端末利用者にマルウェアのリスクを認識させ，その結果として適切な対策行動を行わせることのできるマルウェア警告ダイアログの設計である．そして提案ダイアログの有効性を被験者実験を通じて評価する．

Android OS が稼働する携帯端末において，マルウェア対策として AV ソフトウェアを導入した場合，その後の対応は**図 6** のようになる．デスクトップ PC で稼働する AV ソフトウェアの場合，マルウェアのスキャンから駆除まで自動で行われる．したがって利用者がその処理に介入する必要はなく，単に結果を通知するにとどまっている．これに対して Android OS の場合，AV ソフトウェアの動作権限の都合上，マルウェアを削除することはできない．したがって利用者に対策行動を実行させる必要がある．

本論文では，以下の 2 つの理由から AV ソフトウェアの警告ダイアログにおける「通知」と「対策処理」に注目した改善提案を行う．1 つめの理由は，改善の余地が大きいと考えるからである．図 6 から分かるとおり，この 2 つの機能は警告ダイアログが担っている．しかし現状のダイアログは，既存のダイアログを流用するにとどまり，目的にあわせた設計がなされていないと考えるからである．もう 1 つの理由は，警告ダイアログは Android OS のマルウェア対策において重要な要素だからである．Android OS の設計ポリシーが現状のままで変更されないかぎり，AV ソフトウェアが管理者権限で動作することはない．それゆえ，AV ソフトウェアはマルウェアの検知は可能だが，削除処理は行えない．したがって，なんらかの方法で検知結果を端末利用者に通知し，その対応として利用者に対策行動を実行させる必要がある．警告ダイアログはその手段として重要である．

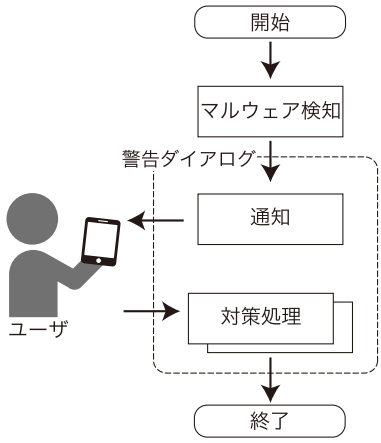

図 6 Android 端末におけるマルウェアへの対応
Fig. 6 Supposed process against malware in Android OS.

次章では図 6 に基づき，警告ダイアログの役割を「通知」「対策処理への誘導」の 2 つに分類し，それぞれの問題点を整理したうえで，改善手法を提案していく．

4. 警告ダイアログの改善案

4.1 警告注視の改善について

4.1.1 問題点

警告ダイアログにおける通知の役割とは，ダイアログに記載の内容を利用者に読ませ，その内容を理解してもらうことである．これに対する利用者の反応は「読んで理解した」「読んだが理解できず」「読まない」の 3 つである．このうち，後者の 2 つは内容を理解するに至っていない点で同一とみなし，以降では「警告を理解した」「警告を理解しなかった」の 2 点に集約して議論を進める．

ここで望ましい結果は「警告を理解した」であり，整理すべきは「警告を理解しなかった」状況になった理由である．議論の結果，この状況になる理由は以下の 2 つであると著者らは考えた．

`Prob A)` マルウェアの警告だと思わなかった．

`Prob B)` 警告に興味がない．

4.1.2 改善案

前節をふまえ，我々は 3 つの改善手法を提案する．

Invert Dialog

Invert Dialog の画面例を**図 7** に示す．本ダイアログの特徴は警告メッセージの周囲領域を赤系統色に反転することで警告ダイアログであることを視覚的に示す方法である．既存のダイアログはその内容が警告であるとないとにかかわらず同系色で提示される．したがって，警告とそれ以外のダイアログを視覚的には判断できず，結果として警告を警告ではないと勘違いするのである．なお赤色を選択した理由は，禁止・停止を意味する色として JIS [12] の規定を応用したものである．本ダイアログは `Prob A` に対する改善案となる．

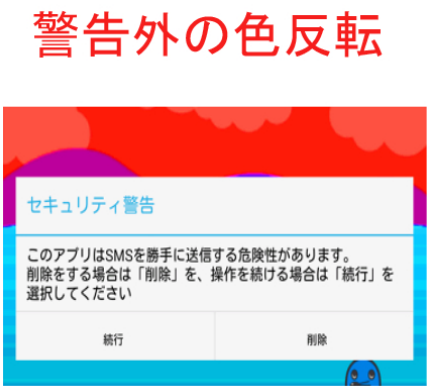

図 7 Invert Dialog の画面例
Fig. 7 Screen snapshot of the Invert Dialog.

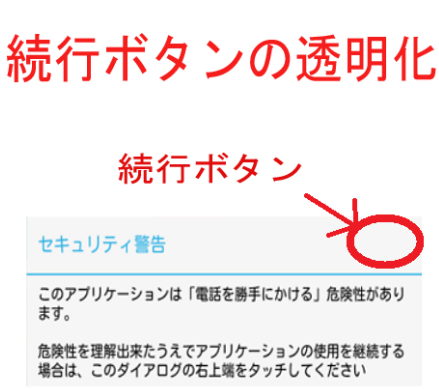

図 8 Clear Dialog の画面例
Fig. 8 Screen snapshot of the Clear Dialog.

Clear Dialog

Clear Dialog の画面例を**図 8** に示す．本ダイアログの特徴はダイアログを閉じるボタンを半透明として不可視にし，かつランダムな位置に配置する点にある．既存のダイアログでは，警告内容を読まずにボタンを押してダイアログを閉じる利用者がいる．そういった安易な対応を困難にするため，ボタンを不可視にしてその位置を警告メッセージ内に記載し，警告メッセージを読まざるをえない状況にする．これにより警告内容の注視を確実にする．本ダイアログは Prob B に対する改善案となる．

Question Dialog

Question Dialog の画面例を**図 9** に示す．本ダイアログの特徴は，警告内容をクイズ形式で利用者に問い，その問いに正解しない限りダイアログが閉じられない仕組みにある．質問内容は当該アプリの Permission であり選択形式で回答可能となっている．これにより単に警告メッセージを読むだけではなく，利用者がその内容を理解しているかを検証可能にしている．なお不正解時はあらためて質問画面に戻るが，正解を安易に探索できないよう回答選択肢の表示順は毎回ランダムに変更される．本ダイアログは Prob B に対する改善案となる．

図 9 Question Dialog の画面例
Fig. 9 Screen snapshot of the Question Dialog.

4.2 対策行動への誘導改善について

4.2.1 問題点

マルウェアの警告ダイアログで提供される対策は「アプリの継続利用」と「アプリの削除」の 2 つである．具体的な調査結果はないが，利用者は多くの場面で「アプリの継続利用」を選択していると推測される．つまり問題は「アプリの削除」が選択されないことにある．これでは AV ソフトウェアを導入していても実質的にはないのと同等である．この理由として以下の 2 つの原因が考えられる．

1 つは「警告を理解しなかった」ので「アプリの継続利用」を選択した場合である．これは「アプリの削除」を選択するのに必要な情報を得ていないので，自然な反応であるといえる（Prob C）．もう 1 つは「警告を理解した」にもかかわらず「アプリの継続利用」を選択した場合である．これはマルウェアによるリスクとアプリ利用を比較検討した結果，アプリの利用を優先する判断をしたといえる．しかし，この状況において利用者がとりうる選択肢は「アプリの継続利用」しかない（Prob D）．これを改善するには，別の選択肢を用意する必要があると著者らは考える．

4.2.2 改善案

前節の問題に対し，2 つの改善手法を提案する．

Delete Dialog

Delete Dialog の画面例を**図 10** に示す．本ダイアログの特徴は，既定のボタン位置に「アプリの削除」ボタンしかない点である．利用者の一部は警告内容を理解せず，安易にアプリの利用を継続しようと画面内のボタンを押下する．これによる警告の形骸化を防ぐため，既定のボタン位置には「アプリの削除」ボタンを設置するとともに，アプリの利用を継続したい場合は警告内容を読まなければダイアログが消えないようにした方法である．本ダイアログは Prob C に対する改善案となる．

Recommend Dialog

Recommend Dialog の画面例を**図 11** に示す．マルウェ

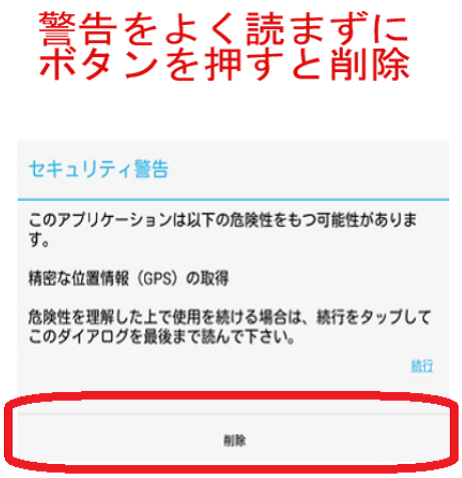

図 10 Delete Dialog の画面例
Fig. 10 Screen snapshot of the Delete Dialog.

図 11 Recommend Dialog の画面例
Fig. 11 Screen snapshot of the Recommend Dialog.

アによるリスクよりもアプリ利用の方が優先度が高い利用者に対し，第三の選択肢として「類似アプリの利用」を推奨するのがこのダイアログの特徴である．画面中央のアイコンは，現在利用中のアプリと類似機能を持つアプリのアイコンである．このアイコンを押下するとアプリマーケット内の当該アプリのページに遷移する．利用したい機能を持つ別のアプリへ利用者を誘導することにより，マルウェアを継続して利用する可能性を低減できると考える．本ダイアログは Prob D に対する改善案となる．

5. 評価実験

4 章で提案した 5 種類の警告ダイアログ案について，期待される効果の有無を被験者実験にて評価した．

5.1 実験設計について

本研究は AV ソフトウェアの警告ダイアログを想定した研究であり，AV ソフトウェアに提案ダイアログを組み込んで評価を行うのが理想である．しかしそれは困難であるため，自作のゲームアプリに各ダイアログを実装し，シミュレーション形式で評価を行った．組み込み先のアプリとしてゲームを選択した理由は，マルウェアである可能性が他分野のアプリよりも高いからである．また実験用端末は著者らが用意した端末を使用した．警告ダイアログに対する被験者の反応を評価するうえで，被験者自身の端末で評価する方が現実に近い条件といえる．しかし，端末に実験用アプリをインストールしなければならないほか，実験条件の統一も困難となるため，この条件とした．実験で使用した端末は ASUS 社製 Android 端末 Nexus 7（2013 LTE モデル）であり，Android OS のバージョンは 4.4.2 である．

表 1 利用したゲーム
Table 1 Games in the experiment.

以下の 3 手法の 1 つを実施	全被験者が実施
Game A+Invert Dialog	Game A+既存 Dialog（1 回）
Game A+Clear Dialog	Game B（2 回）
Game A+Question Dialog	Game C（2 回）
	Game D（2 回）
	Game E（2 回）

また実験中は被験者自身による判断と対応を促すため「自分が所有する端末だと想定して実験を行って下さい」と事前に指示し，実験中は被験者からの質問をいっさい受け付けなかった．したがってゲーム中にダイアログが提示された場合には，被験者自身の判断で対応せざるをえない状況であった．さらに「警告ダイアログへの対応を評価する実験」と被験者に事前説明すると被験者の判断や評価結果に影響を及ぼす恐れがあるため，本来の実験目的は隠蔽し「携帯ゲームの操作実験」と称して実験を行った．つまり間接的に警告ダイアログの効果測定を行ったことになる．また同様の理由により，実験端末の AV ソフトウェアのインストール状況についてもいっさい言及しなかった．以降，本論文で述べる実験はすべてこれらの条件のもとで実施した．

5.2 警告注視に関する評価実験

実験方法

3 つの提案ダイアログにおける警告内容注視について被験者実験を行った．前述のとおり，ゲームの操作実験と説明し 5 種類の Game A，B，C，D，E を 2 回ずつ計 10 回操作させる実験とした．**表 1** にあるとおり，Game A にはそれぞれ 3 種の提案ダイアログと既存ダイアログを組み込み，ゲーム開始から 5 秒後にダイアログが表示される仕組みとなっている．また Game B，C，D，E は 1 ゲームのプレイ時間が Game A と同程度の市販ゲームを利用した．被験者には Game A を 2 回操作させる中で既存ダイアログと 3 種の提案ダイアログのうち 1 つをランダムで選択して

被験者に実施させた．5 種 10 回のゲームの実施順も偏りのないように配慮して実験を行った．

この実験では 2 つの値を測定した．1 つは警告内容注視率である．この値は実験終了後に警告ダイアログの記載内容をアンケートを通じて自由記述形式で回答させた．回答結果は以下の 3 つに分類し数値化した（式 (1)）．なお一部正答の定義は「完全正答ではないが，正答に含まれる単語がアンケート回答に含まれている場合」とした．

$$S_i = \begin{cases} 1 & (\text{完全正答}) \\ 0.5 & (\text{一部正答}) \\ 0 & (\text{無回答，誤回答}) \end{cases} \quad (1)$$

もう 1 つの測定値はダイアログ表示時間である．ダイアログが画面に表示されてから利用者によってダイアログが消されるまでの時間をアプリを通じて測定した．

被験者情報を**表 2** に示す．被験者は 3 種のダイアログについて 5 名ずつ，計 15 名である．全員が 20 代であり高等教育を修了している被験者であった．

実験結果

実験結果を**表 3** に示す．表 3 中の平均警告注視率（S）は，式 (2) によって算出した．式中の S_i は各被験者の実験結果スコアであり，n は被験者数である．

$$S = \frac{\sum_{i=1}^{n} S_i}{n} \times 100 \quad (2)$$

実験結果から警告注視率が最も高いのは Question Dialog であった．まだダイアログ表示時間も Question Dialog が最も長く，また最も短いのは既存ダイアログとなった．また Clear Dialog は既存のダイアログよりも警告注視率が低い結果となった．

5.3 対策行動への誘導に関する評価実験

実験方法

2 つの提案ダイアログにおける利用者の対策行動選択に関して被験者実験を行った．この実験も警告注視の評価実験と同様，5 つの Game を 2 回ずつ計 10 回のゲームを操作させ，そのうち Game A に既存ダイアログと提案した 2 種のダイアログを組み込んで実験に利用した（**表 4**）．被験者には既存ダイアログと提案 2 手法のうちのどちらかをランダムに選択して操作をさせ，評価を行った．

この実験では 2 つの値を測定した．1 つは利用者が選択した対策行動であり，アプリを通じて記録した．その記録は以下の 2 つに分類し，数値化した（式 (3)）．

$$R_i = \begin{cases} 1 & (\text{利用続行以外を選択}) \\ 0 & (\text{利用続行を選択}) \end{cases} \quad (3)$$

もう 1 つはダイアログ表示時間である．これは警告注視実験と同様，アプリを通じて計測した．

被験者情報を**表 5** に示す．2 つのダイアログについて各 5 名ずつ計 10 名である．被験者は全員が 20 代で高等教育を修了している方々であった．

実験結果

実験結果を**表 6** に示す．なお対策行動誘導率（R）は，以下の式 (4) によって算出した．式中の R_i は各被験者の対策行動スコアであり，n は被験者数である．

$$R = \frac{\sum_{i=1}^{n} R_i}{n} \times 100 \quad (4)$$

実験結果から，対策行動誘導率が最も高かったのは Recommend Dialog であった．一方，Delete Dialog と既存ダイアログは対策行動への誘導という点において差がないという結果となった．

表 2 警告注視に関する実験の被験者情報
Table 2 Demographic information of the subjects.

	被験者総数	女性被験者数	Android 経験者
既存手法	15	4	9
Invert	5	1	3
Clear	5	2	4
Question	5	1	2

表 3 平均警告注視率・平均ダイアログ表示時間
Table 3 Average alert capturing rate, average dialog display time.

	平均警告注視率 S（%）	ダイアログ表示時間（sec）
既存手法	40	8.57
Invert	40	13.26
Clear	20	9.95
Question	50	42.19

表 4 実験に利用したゲーム
Table 4 Games in the experiment.

以下の 1 つをランダムに選択	全被験者が実施
Game A+Delete Dialog	Game A+既存 Dialog（1 回）
Game A+Recommend Dialog	Game B（2 回）
	Game C（2 回）
	Game D（2 回）
	Game E（2 回）

表 5 対策行動に関する実験の被験者情報
Table 5 Demographic information of the subjects.

	被験者総数	女性被験者数	Android 経験者
既存手法	10	3	7
Delete	5	2	4
Recommend	5	1	3

表 6 平均対策行動誘導率・平均ダイアログ表示時間
Table 6 Average action induction rate, average dialog display time.

	対策行動誘導率 R（%）	表示時間（sec）
既存手法	40	10.62
Delete	40	16.80
Recommend	60	8.85

表 7 警告注視と対策行動誘導の改善結果
Table 7 Evaluation results of alert capture and better decision.

	警告注視	対策行動誘導
Invert	△	-
Clear	×	-
Question	○	-
Delete	△	×
Recommend	×	○

5.4 評価実験総括

表 7 はこれまでの実験結果を総括したものである．この結果から，Question Dialog と Recommend Dialog を基本とし，それらに Invert Dialog と Delete Dialog で状況改善の可能性が示唆された以下の特徴を取り入れることが望ましいと考える．

- ダイアログを既存の色とは異なる警告色に変更することは警告注視に一定の効果がある（Invert Dialog）
- ダイアログ画面内の既定のボタン表示位置には「アプリ削除ボタン」のみとする（Delete Dialog）
- 問題に対して適当に回答する利用者に対する対策（Question Dialog）

6. 統合版警告ダイアログ

本章では 5 章で得られた知見をもとに統合版警告ダイアログを 2 手法提案する．

手法 1: Market Dialog

Market Dialog は Recommend Dialog をベースとし，その問題点を Delete Dialog および Invert Dialog の特徴を取り込んで提案する改良版警告ダイアログである．**図 12** は，Market Dialog の画面例である．

Recommend Dialog は以下の問題があった．

- 「アプリ削除」の対策行動が選択肢にない．
- 「利用続行ボタン」が画面内の既定位置にある．よって警告内容を理解せずにダイアログを消そうとする利用者を利する画面になっていた．
- 利用者に対して警告を注視させる効果がない．既存のダイアログと同系色であり，警告ダイアログであることが視覚的に伝わらない．

これらの問題に対し，既定のボタン位置には「アプリ削除ボタン」だけ配置し，利用続行ボタンは警告内容を読まないと押せないようにした（Delete Dialog），またこのダイアログが警告を意味していることを視覚的に示すため，ダイアログ内部を警告色である黄色で着色した（Invert Dialog）．これらの改善により，1) 色により警告であることを視覚的に通知し，2) 安易にダイアログを消そうとするユーザは「アプリ削除」を実行することになる．また 3) 対策行動は「継続利用」「アプリ削除」および「別アプリへの乗り換え」の 3 つの選択肢が提供されることになる．

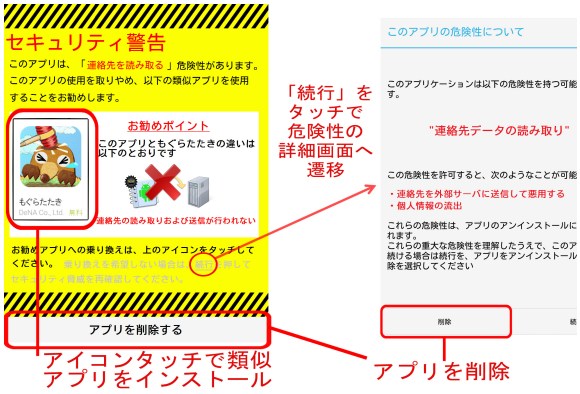

図 12 Market Dialog の画面例
Fig. 12 Screen snapshot of the Market Dialog.

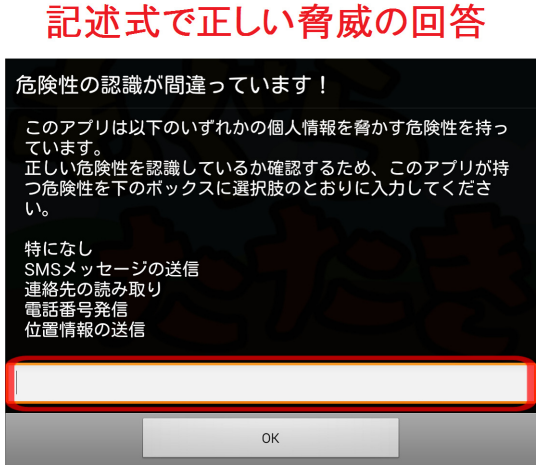

図 13 Writing Dialog の画面例
Fig. 13 Screen snapshot of the Writing Dialog.

手法 2: Writing Dialog

Writing Dialog は Question Dialog をベースとし，残されていた問題点を選択式回答から記述式回答にすることで改良を試みた警告ダイアログである．**図 13** は Writing Dialog の画面例である．Question Dialog には適当な回答を行ってダイアログを消し，アプリを継続利用してしまう懸念があった．また同一アプリにて繰り返し警告ダイアログに対応すると正解を記憶してしまい，迅速にアプリを利用継続できるようになる懸念もあった．そこで，これらの懸念に対して少しでもアプリの継続利用に手間がかかるよう以下の 2 つの改善を行った．

- 回答候補の提示順をダイアログ表示のたびにランダム化した．
- 1 回目の回答は選択式で回答可能とするが，1 回目の回答を誤ると 2 回目以降の回答は記述式（文章入力）にすることで手間がかかるようにした．

後者の実装について述べる．1 回目の回答は Question Dialog のように選択式で回答可能だが，1 回目の回答を誤

るとそれ以降は回答候補の 1 つを記述，すなわち文字入力させるようにした．これにより 1 回目の回答で正解することがアプリを継続利用するうえで最小の手間となる．このように 1 回で正解することに対してメリットを提供することで，警告内容を理解する行動に利用者を誘導することを目指したものである．

7. 統合版警告ダイアログの評価

改良版ダイアログ 2 種について，5 章同様，ゲームアプリに 2 つのダイアログを個別に実装して評価実験を行った．組み込んだゲームを Game A とすると以下のとおりとなる

- Game A + Market Dialog
- Game A + Writing Dialog

また前の実験同様，Game B，C，D，E を用意し，ゲーム操作の実験と称して 5 種類のゲームを 2 回ずつ，計 10 回操作させた．Game A の 2 回についてはゲーム開始 5 秒後に提案ダイアログが表示される実装とした．なお本実験では 5 章の実験とは異なり，既存ダイアログとの比較実験は行わず，各被験者は 2 種類の統合型警告ダイアログを評価させた．その他の実験条件は 5 章での実験条件と同一である．

測定値は，Market Dialog については警告注視に関する測定と対策行動誘導の測定の両方を実施した．Writing Dialog は警告注視に関する測定のみである．なおダイアログ表示時間は双方のダイアログに対して行った．

被験者は 13 名（うち女性 3 名）であり，全員が 20 代，高等教育を受けているか修了している被験者であった．Android 端末所持者は 7 名であった．なお本実験における被験者は統合前の提案手法に関わる評価実験（5 章）には参加していない．

7.1 実験結果

Market Dialog に関する実験結果を**表 8** に示す．また**図 14** に対策行動誘導率に関する既存ダイアログ，Recommend Dialog と Market Dialog との比較プロット図を示す．この結果から，Market Dialog は Recommend Dialog よりも対策行動への誘導効果が高い可能性が示されたといえる．

次に Writing Dialog に関する実験結果を**表 9** に示す．また**図 15** に警告注視率に関する既存ダイアログ，Question Dialog と Writing Dialog との比較プロット図を示す．図 15 のプロット図から Writing Dialog は警告内容を理解できていなかった利用者に対して警告内容を理解させることには一定の可能性があることを示している．一方，1 回目の回答で正解した場合のみ結果は，注視率が既存ダイアログと同程度にとどまっている．これは一部のユーザが警告を理解しないまま適当な回答で正解し，結果として警告注視率を下げていると考えられる．

表 8 Market Dialog の警告注視と対策行動誘導に関する実験結果
Table 8 Alert capture and action decision results in Market Dialog.

	警告注視率 S（%）	対策行動誘導 R（%）	表示時間（sec）
Market	34.6	69.2	19.44

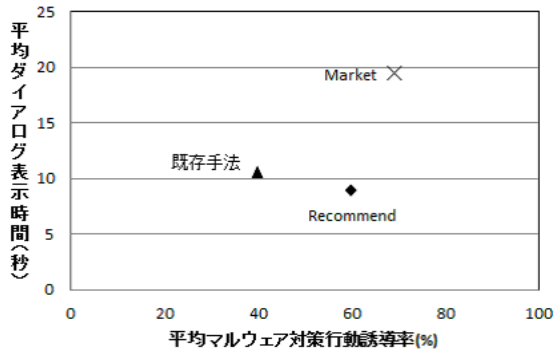

図 14 Market Dialog と Recommend，既存ダイアログとの対策行動誘導率の比較
Fig. 14 Comparison of the R values in Three Dialogs.

表 9 Writing Dialog の警告注視に関する実験結果
Table 9 Alert capture result in Writing Dialog.

	人数	警告注視率 S（%）	表示時間（sec）
Writing（全体）	13	38.5	44.56
Writing（1 回目で正答）	8	25	16.204
Writing（2 回以上回答）	5	60.0	89.93

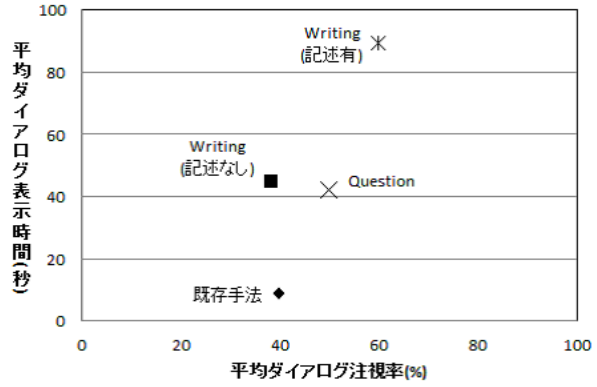

図 15 Writing Dialog と Question，既存ダイアログとの警告注視率の比較
Fig. 15 Comparison of the S values in Three Dialogs.

8. 考察と今後の課題

8.1 マルウェア対策行動への誘導に関する考察

評価実験より，Market Dialog は Recommend Dialog よりも高い対策行動誘導率となった．この結果から対策行動として「別アプリへの乗り換え」を提示することは有用である可能性があることがあらためて示された．またダイアログ表示時間も倍近く伸びている．これは Invert Dialog および Delete Dialog の特徴を Market Dialog に導入したことにより警告内容が注視されるようになったと考える．

一方，今回の評価実験でも 1 秒以内に削除ボタンを押下し，アプリを削除しようとした被験者が 2 名いた．ダイアログ内の警告内容を理解しようとせず拙速にダイアログを消そうとするユーザに対して Delete Dialog の特徴を取り込むことは，一定の効果があるということが再確認できたと考えている．

8.2 警告注視に関する考察

Writing Dialog の平均警告注視率は既存手法と同程度となった．しかし 1 回以上誤回答し，記述式回答へ移行した被験者の注視率は 60%と Question Dialog よりも高い結果となった．したがって，セキュリティ脅威を記述式で回答させることをダイアログを閉じる条件とすることは，警告注視の改善に効果があると考えられる．一方で，記述式へ移行した被験者の平均ダイアログ表示時間は約 90 秒となっており，既存手法に比べ大きく増加している．これにより利便性も低下しており，アンケートによって Writing Dialog への煩さしさを 5 段階評価（1：最も煩わしい〜5：最も煩わしくない）で評価した結果，選択式のみの被験者の回答平均は 2.75 なのに対し，記述式へ移行した被験者の回答平均は 1.60 となった．

8.3 今後の課題

今回対処できなかった問題として，馴化の問題がある．馴化とは，ユーザが同じ警告に繰り返し対応することにより慣れてしまい，警告内容に注意を払わなくなり，定型作業として警告を無視するようになることである．本研究における評価実験では，被験者は一度しか警告に対応しないため，馴化に関する評価はできていない．したがって提案する改善手法であっても，いずれは警告を見ずにダイアログを閉じてしまう可能性がある．Bravo-Lillo らの研究 [13] では，Windows の警告画面において，警告を閉じるために毎回異なる文章を入力させることが馴化に対して有効であるという結果を報告している．Writing Dialog がその特徴を備えていることから長期的な評価実験を通じて馴化に対する対策としての有用性について今後検証を行う必要がある．

また，今回の実験では警告文の文章について詳細な検討を行わなかったが，警告文の改善を図ることで注意を引き付ける効果も考えられる．Khovanskaya らの研究 [14] では，データマイニングへの警告文において，ユーザを脅すような書き方にすることや，わざと間違えたデータを表示すること，別のデータとの具体的な比較がユーザの個人情報への認識を向上させることを示している．したがって上記の知見を警告文に反映することが対策行動への誘導に効果があるかについても検討ならびに評価を行いたいと考えている．

Writing Dialog は文字入力に時間がかかるため，利便性低下の問題がある．改善策としては，セキュリティ脅威をそのリスクに応じて分類し，リスクの大きなもののみ記述式回答へ移行することとし，それ以外の場合については選択式回答で繰り返し回答可能にするという対応も考えられる．

なお本研究における評価実験は被験者数が少ないため，実験結果の信頼性が高いとはいえないことに注意しなければならない．今後，被験者を増やしたうえで評価実験を行うことは今後の課題である．また実験設計についても，議論の余地がある．例をあげる．今回の実験では本来の実験目的を隠蔽し「ゲームの操作実験」として間接的に警告ダイアログの評価を行った．この条件設定の理由は 5.1 節で述べたとおりである．しかしこれは望ましくない判断を被験者にさせる可能性がある．つまり「ゲームの操作実験なので警告ダイアログへの対応は実験とは無関係」という判断を被験者にさせた可能性がある．この判断は著者らが望む被験者の対応ではないことは明らかであり，今回の実験結果にはこのような判断による結果も含まれている可能性がある．このような可能性を低減するため，実験条件の妥当性についても今後議論を進めていく必要がある．

最後に研究成果の普及に向けた実現可能性について言及する．著者らが期待する提案ダイアログの実装組織は OS 提供者と AV ソフトウェアメーカである．理由は，両者ともに適切なマルウェア対策を実現することが製品の魅力向上につながること，ならびに提案内容の普及にともなう負担を担い，利用者に提供する責任を持つべき組織であると考えるからである．また別の実現方法として，AV ソフトウェアメーカと研究者による協働も考えられる．本研究を含む警告ダイアログに関わる関連研究の成果をもとに，携帯端末におけるマルウェア警告ダイアログの標準化と実装を複数の AV ソフトウェアメーカが共同で行い，それを各社の製品で警告ダイアログとして展開する．研究者は改善方法の考案とその効果を研究を通じて積み重ね，かつダイアログ実装に協力するという形態である．どちらの可能性についても，OS 提供者や AV ソフトウェアメーカが警告ダイアログの重要性を認識し，研究者と協力してその改良に取り組む枠組みが必要であると考える．

9. おわりに

Android OS を対象としたマルウェアは多数流布されており，携帯端末の利用者はセキュリティ脅威に晒されている．この問題に対する現実的な対応策としては Anti-Virus（AV）ソフトウェアを利用することである．ここで問題になるのは Android OS における AV ソフトウェアはマルウェアを駆除することができず，利用者に対してその行動を促し，実施させる必要があるということである．

そこで本研究では AV ソフトウェアのマルウェア警告ダイアログに着目し，既存の警告ダイアログが利用者をマル

ウェアの削除へ誘導できていないことに注目した．そこで本研究では，警告ダイアログを改善し，利用者をマルウェア対策行動へ誘導しうるダイアログを設計することを目的とした．

本研究では既存手法の問題点を整理し，ダイアログが警告通知と対策行動への誘導という 2 つの役割を担っていることに基づき，警告通知に対して 3 つの改善案，対策行動への誘導に対して 2 つの改善案を提案して，その効果について被験者による評価実験を行った．その結果，警告通知については警告内容を質問形式で確認する Question Dialog，対策行動への誘導については「継続利用」「アプリ削除」以外の第三の対策行動として類似機能を持つ別アプリへの乗り換えを勧める Recommend Dialog が最も良い効果を示すことを明らかにした．また，他の改善案についても一定の改善効果が見込まれることが分かった．

この実験結果をふまえ，5 種類のダイアログ案から改善効果が見込まれる特徴を組み合わせた統合版ダイアログとして Market Dialog と Writing Dialog を提案し，あらためて被験者による評価実験を実施した．その結果，Recommend Dialog と Question Dialog よりも望ましい効果が得られることを実験により明らかにした．

今後は，馴化の問題に対する改善案の検討とその評価のため長期間による評価実験を行うことと，被験者人数を増やしたうえでこれまでの評価実験を再検証する必要があると考えている．我々は，この研究を通じて Android OS を対象としたマルウェア対策として AV ソフトウェアの有効性を改善しうる警告ダイアログの実現に取り組んでいきたいと考えている．

参考文献

[1] KINDSIGHT SECURITY LABS: MALWARE REPORT - Q4 2013 (online), available from ⟨http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf⟩ (accessed 2015-02-06).

[2] Google: Official Google Mobile Blog (online), available from ⟨http://googlemobile.blogspot.jp/2012/02/android-and-security.html⟩ (accessed 2015-03-08).

[3] TREND MICRO: Trend Micro Mobile Security (online), available from ⟨http://www.trendmicro.co.jp/jp/business/products/tmms/⟩ (accessed 2015-02-06).

[4] Google Play：無料セキュリティ & ウイルス対策 — Lookout，入手先 ⟨https://play.google.com/store/apps/details?id=com.lookout⟩ （参照 2015-02-06）.

[5] Google Play: Mobile Security & Antivirus (online), available from ⟨https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity⟩ (accessed 2015-02-06).

[6] Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N. and Wetherall, D.: A conundrum of permissions: Installing applications on an android smartphone, *Proc. FC'12*, pp.68–79 (2012).

[7] Kelley, P.G., Cranor, L.F. and Sadeh, N.: Privacy as Part of the App Decision-Making Process, *Proc. CHI '13*, pp.3393–3402 (2013).

[8] Harbach, M., Hettig, M., Weber, S. and Smit, M.: Using Personal Examples to Improve Risk Communication for Security and Privacy Decisions, *Proc. CHI '14*, pp.2647–2656 (2014).

[9] Balebako, R., Jung, J., Lu, W., Cranor, L.F. and Nguyen, C.: Little brothers watching you: Raising awareness of data leaks on smartphones, *Proc. SOUPS '13*, Article No.12 (2013).

[10] 藤原康宏，村山優子：コンピュータ利用時の不快感を利用した警告インタフェースの提案，情報処理学会論文誌，Vol.52, No.1, pp.77–89 (2011).

[11] ASUS: Nexus7 (online), available from ⟨http://www.asus.com/jp/Tablets_Mobile/Nexus_7/⟩ (accessed 2015-02-06).

[12] 日本工業標準調査会：安全色—一般的事項（オンライン），入手先 ⟨http://www.jisc.go.jp/app/pager?id=1508207⟩（参照 2015-02-06）.

[13] Bravo-Lillo, C., Cranor, L. and Komanduri, S.: Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It, *Proc. SOUPS '14*, pp.105–111 (2014).

[14] Khovanskaya, V., Baumer, E.P.S., Cosley, D., Voida, S. and Gay, G.: Everybody knows what you're doing: A critical design approach to personal informatics, *Proc. CHI '13*, pp.3403–3412 (2013).

高橋 雅香

2013 年電気通信大学電気通信学部情報通信工学科卒業．2015 年同大学大学院情報理工学研究科総合情報学専攻博士前期課程修了．在学中は Android プラットフォームにおけるマルウェア対策の研究に従事．ネットワークセキュリティにも関心がある．

高田 哲司 （正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士後期課程修了．博士（工学）．2003 年ソニーコンピュータサイエンス研究所研究員．2005 年独立行政法人産業技術総合研究所情報技術研究部門研究員．2010 年電気通信大学大学院情報理工学研究科准教授現在に至る．個人認証，ユーザブルセキュリティ，情報視覚化に興味を持つ．IEEE/CS 会員．