Androidマルウェアへの対策行動を誘導する警告手法の提案

高橋 雅香[1,a)]　高田 哲司[1,b)]

概要：Android をターゲットにしたマルウェアアプリケーションは急増し，セキュリティ脅威が問題になっている．これに対し，既存のアンチウイルスソフトのダイアログ警告は，セキュリティ知識のないユーザに対してもセキュリティ脅威を通知することができる．一方，セキュリティ脅威を懸念しないユーザは，警告を無視したり，誤って閉じてしまうという問題がある．そこで本研究では，警告無視の改善策として「マルウェア対策行動への誘導」「ダイアログ警告注視効果の向上」の 2 つを取り上げ，これらを実現する警告手法を提案する．提案手法と既存手法に関して評価実験を行った結果，提案手法において対策行動への誘導率の向上，警告注視効果の向上の可能性が見られた．今後は，ユーザが同じ警告を繰り返し目にすることによってそれに慣れてしまい，無視するようになる問題への対策のための改良を検討することで，更にマルウェア対策行動への誘導効果を高めていく．

キーワード：マルウェア，Android，セキュリティ警告，インターフェースデザイン，モバイルセキュリティ

Warning system to encourage mearsure action to Android malware

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

Abstract: A malware application for an Android terminal 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: Malware, Android, Security Warning, Interface Design, Security Dialog, Threat recognition, Mobile phone, Mobile Security

1. はじめに

アプリケーション（以下，本論文中ではアプリと記す）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．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，Alcatel-Lucent の“MALWARE REPORT - Q4 2013”によると，2013 年の 1 年間で約 20 倍と急速に増加している [1]．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．

- 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 Web サイトでのアプリ配布が可能

Android の公式アプリマーケットでは，不正アプリ検出機能でアプリの審査を行っている．しかし，このシステムでは既知のマルウェアしか検出できないため，新型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

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

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がある．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．ユーザがマルウェアアプリをインストールしてしまう問題は早急に対策が必要である．

この問題に対し，アンチウイルスソフトのダイアログ警告は，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[2] では，Android OS の標準ダイアログを用いて図 1 のような警告が表示されるが，この警告は表示された際，警告ダイアログ以外の画面部分（図中の赤線枠内）に触れることによって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 向けアンチウイルスソフトウェアの 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．

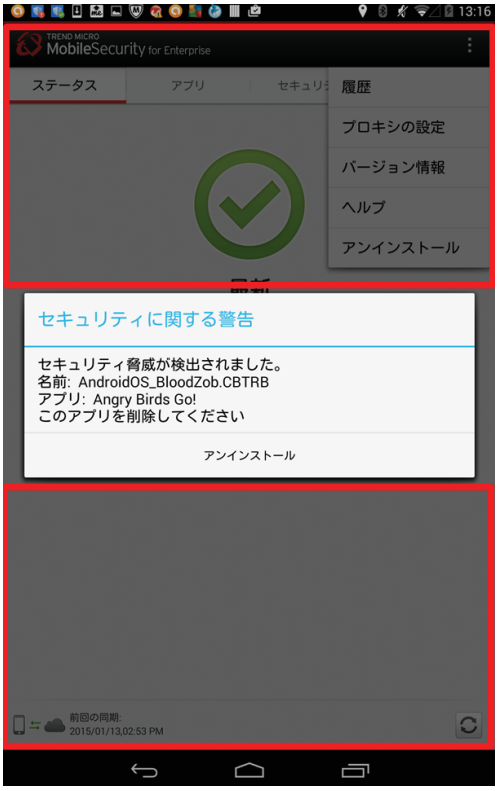

図 1　Android OS の標準ダイアログ例 [2]

そこで本研究では，警告無視の改善策として「セキュリティ脅威を懸念しないユーザをマルウェア対策行動へ誘導する」ことと，「ダイアログ警告注視効果を高める」ことの 2 つを取り上げ，これらを実現する警告手法を提案する．

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製品・研究について取り上げる．

2.1 Android マルウェア検知を通知する既存製品

前章で述べた Android マルウェアの脅威に対して，セキュリティベンダは Android 端末をターゲットとしたアンチウイルスソフトウェア [2][4] を配布・販売している．これらのソフトウェアはマルウェアを検知するとアンインストールを促すダイアログ警告を表示する．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アンインストール，またはアプリの使用継続のみであり，アプリの使用を目的としているユーザは，目的を果たすため使用継続を選んでしまうという問題点がある．また，図 2 のように，マルウェアのセキュリティ脅威の詳細は，ユーザが自ら詳細ボタンを押して確認しなければならないため，セキュリティに関心の低いユーザは詳細を確認せず，セキュリティ脅威を認識しないという問題点もある．

図 2　ダイアログ警告例 [3]

2.2 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が表示される．しかし，アクセス許可は図 3 のように，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無視するという問題点が Kelley らの研究 [5] によって示唆されている．Kelley らの研究 [6] では，図 4 のように，アプリが収集する個人情報をチェックボッ

クス形式で表示して，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わ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，最大 28%のユーザのアクセス許可の認識を向上させることが判明している．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 [7] では，Google Play のインストール画面を改良して，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，ユーザに危険性が伝わりやすくする手法が提案されている．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判明している．しかし，この手法は端末を使用する場所が電車内など公共の場であった場合，個人情報が端末上に表示されることでプライバシー問題を引き起こす可能性があり，公共の場で使用することが望ましくない．

図 3　Google Play のアプリインストール画面

図 4　Kelley らの研究概要

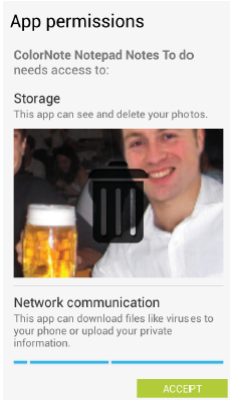

図 5　Harbach らの研究概要

2.3　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達する Privacy Leaks just-in-time(JIT)[8] 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ショートメッセージとして表示する．しかし，ステータスバーにショートメッセージが表示されるのは数秒であり，ユーザが見逃してしまうと通知領域を開かないと詳細がわからなくなってしまう．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わ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，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，ショートメッセージが表示されても無視してしまうことが懸念される．

3.　研究の目的

1 章で述べたように，Android マルウェアの脅威は大きくなりつつある．この問題に対し，様々な警告手法が研究・開発されている．

中でも，アプリ実行中におけるダイアログ警告は，藤原らの研究 [9] によると不快なインタフェースにおけるメッセージ因子に該当し，作業を邪魔されたと感じさせることによって危険な状態にあることを伝える効果があるとされている．これによって 2.2 節で述べた，インストール時にセキュリティに関心が低いユーザがアクセス許可によるセキュリティ脅威を認識しない問題を解決できると考えられる．また，ダイアログ警告においては，ユーザは必ず継続や削除などの行動を起こさなければならないため，2.3 節で述べた表示された警告を無視する問題を解決する．

本研究では以上の理由からユーザへのセキュリティ脅威の通知の手法としてダイアログ警告に着目する．しかし，2.1 節で述べたとおり，既存のダイアログ警告手法ではユーザが使用継続を選んでしまうという問題があった．この問題は，セキュリティへの関心が低いユーザがセキュリティ脅威を懸念しないことが原因であった．そこで，セキュリティへの関心が低いユーザにもマルウェアの危険性を認識させ，簡単に無視できない方法でユーザをマルウェア対策行動へ誘導する手法を考案する．

また，ユーザのセキュリティ警告注視効果を高めることがセキュリティへの関心が低いユーザにもマルウェアの危険性を認識させることに繋がると考え，警告を注視させることによってセキュリティ脅威の認識を促すような警告手法を考案する．

4.　提案手法

本章では，本研究の提案手法について述べる．前章ではユーザをマルウェア脅威から遠ざけるための要件として，

セキュリティへの関心が低いユーザのマルウェア危険性認識と，マルウェア対策行動への誘導が必要であると述べた．

そこで，ユーザをマルウェア対策行動に誘導する手法として，類似アプリをお勧めすることによってアプリの乗り換えを行わせる Recommend Dialog，ユーザが警告を読まずにボタンを押すとアプリの削除が行われる Delete Dialog を提案した．また，ダイアログを注視させることによって警告の理解を促すような警告手法として，赤色への色反転を用いることでユーザをダイアログ警告に注目させる Invert Dialog，ダイアログの内容を読まなければダイアログを閉じることが出来ない Clear Dialog，正しいパーミッションが選択できなければダイアログを閉じることができない Question Dialog を提案した．図 6 に Recommend Dialog，Delete Dialog，図 7 に Invert Dialog，Clear Dialog，Question Dialog の画面例を示す．ただし，図 6(a) および図 7(a) は既存手法に用いられる Android OS の標準ダイアログである．

4.1 マルウェア対策行動へ誘導する警告手法

- Recommend Dialog
  図 6(b) は Recommend Dialog の画面例である．既存手法ではマルウェア対策行動はアンインストールのみであるのに対し，この手法はアプリの乗り換えを促すという特徴を持つ．類似アプリをお勧めという形で 2 つ表示し，タッチすることでインストールページへ遷移する．これによって，アプリを使用したいため削除を選択せず使用を継続していたユーザを，対策行動へ誘導することが期待される．
- Delete Dialog
  図 6(c) は Delete Dialog の画面例である．この手法は，ユーザがダイアログ内容を読まずにダイアログ下部にあるボタンを押した場合，ただちにアプリを削除し，マルウェアの脅威を取り除くことを目的としている．ダイアログ下部のボタンは削除ボタンであり，押した場合は Android OS の標準ダイアログと違い，アプリ削除の確認をせず即座にアプリを削除する．また，続行を選んだ場合，マルウェア詳細を表示したうえで更に続行か削除かを選ばせる．この手法では，既存手法での続行ボタンを誤って押してしまい，警告内容を読まずに使用を継続してしまう問題を解決することができる．

4.2 ダイアログ注視効果を向上させる警告手法

- Invert Dialog
  図 7(d) は Invert Dialog の画面例である．既存手法ではダイアログ警告が発生した場合，警告以外の部分は黒くなる．しかし，JIS が定める安全色 [11] によると，黒は安全マーキングとして用いるため，危険性を伝えるには適していないと考えられる．一方で，赤は停止や禁止を表す色であるとされている．藤原らの研究 [9] では，警告に赤色を使用することは，不快なインタフェースにおける見づらさ因子を有しており，注意を引き付けられることが示唆されている．
  そこで，この手法はアプリ画面の元画像において青い部分を赤に色反転させることで，警告に注意を向ける効果が期待できると考える．これによって，警告に注視せず警告以外の部分を押してしまい，警告を閉じてしまうといった操作ミスを防ぐ．
- Clear Dialog
  図 7(e) は Clear Dialog の画面例である．この手法は，ユーザが警告を無視してダイアログを閉じてしまう問題に対し，ダイアログを閉じるボタンを透明化することでボタンの位置を分からなくした．ボタンの位置はダイアログ中に記載されているため，ダイアログの内容を読まなければ分からず，内容を読まずにダイアログを閉じることが困難になるようにした．既存手法は全て，ダイアログを読まなくとも使用継続ボタンを即座に押すことが可能であった．しかし，Clear Dialog は必ずダイアログの内容を読まなければならないため，ユーザはダイアログに目を向けざるを得なくなる．これによって警告文の無視を減らすことができると考えられる．
- Question Dialog
  図 7(f) は Question Dialog の画面例である．この手法は，アプリのパーミッションによって起こり得る，個人情報に関するセキュリティ脅威を正しく答えなければ，ダイアログが閉じられない手法である．既存手法ではインストール時以外にユーザにパーミッションの確認を求めることはなかった．しかし，この手法では選択式でアプリのセキュリティ脅威の確認を求める．セキュリティ脅威を間違えて選択した場合，正しい答えを選択するまで再確認を求める．これによって，ダイアログを閉じるために正しいパーミッションを認識する必要があるため，ユーザは起こり得るセキュリティ脅威を認識することができる． この手法では，ユーザがセキュリティ脅威を認識しない問題に対して，正しいセキュリティ脅威を認識させる効果を期待する．

5. 評価実験

提案手法について，Android ゲームアプリにおいて，ゲーム開始から 5 秒後にダイアログ警告が出現するという形で疑似的に実装を行い，被験者による評価実験を行った．

5.1 マルウェア対策行動への誘導に関する実験

Recommend Dialog，Delete Dialog と，既存手法におい

図 6　マルウェア対策行動へ誘導する警告手法

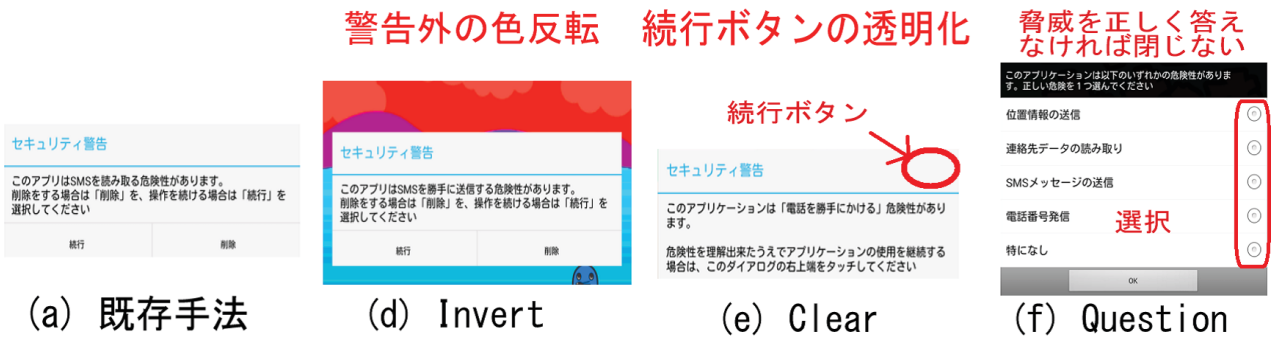

図 7　ダイアログ注視効果を向上させる警告手法

て対策行動への誘導に関する検証実験を行った．

5.1.1　実験方法

提案手法，および既存手法を実装したアプリを被験者に操作させ，ダイアログに対する利用者の対応行動を測定した．本実験では実験であることを意識しない状態でダイアログ警告への反応を見ることが必要であるため，ゲームアプリの操作実験として被験者への説明を行った．また，提案手法，および既存手法を実装したアプリを含め，５種類のアプリを２回づつ，合計１０回ほどゲームアプリの操作を行わせることによって，実験の目的がダイアログ警告に関する実験だと実験途中に悟られないよう配慮した．

本実験で用いられた端末は ASUS 社の Nexus 7(2013)[10] の LTE モデルであり，OS バージョンは Android OS version 4.4.2 であった．

被験者のダイアログに対する対応行動，およびダイアログが表示されてから閉じられるまでの時間をアプリ側で測定した．またすべてのアプリ操作の終了後，被験者にはアンケート調査を実施した．

全てのアプリ操作の終了後，被験者にはアンケート調査を行った．アンケート項目は，被験者の属性情報，および端末利用経験である．

被験者は提案手法１つにつきそれぞれ５名ずつであり (うち Recommend Dialog は女性 1 名，Delete Dialog は女性 2 名)，全員が 20 代，高等教育を修了している被験者であった．1 人の被験者は Recommend Dialog と Delete Dialog のどちらかと，既存手法のダイアログしか評価実験をしていない．

5.1.2　実験結果

マルウェア対策行動への誘導に関する実験の結果を，表 1 および図 8 に示す．ただし，被験者 i がマルウェア対策行動を取ったかどうかの値 R_i を式 (1) のように定め，被験者数 n における平均マルウェア対策行動誘導率 R を，式 (2) のとおりに定義する．

本実験では，２種類の提案ダイアログと標準ダイアログの３種類のダイアログで比較を行った結果，Recommend Dialog がマルウェア対策行動の誘導に最も効果的であることがわかった．一方で，Delete Dialog と既存手法においてはマルウェア対策行動誘導に関して差がないということが分かった．

$$R_i = \begin{cases} 1 & \text{（対策行動を選択）} \\ 0 & \text{（続行を選択）} \end{cases} \tag{1}$$

$$R = \frac{\sum_{i=1}^{n} R_i}{n} \times 100 \tag{2}$$

表 1　平均マルウェア対策行動誘導率・平均ダイアログ表示時間

	対策行動誘導率 (%)	表示時間 (秒)
既存手法	40	10.623
Recommend	60	8.850
Delete	40	16.799

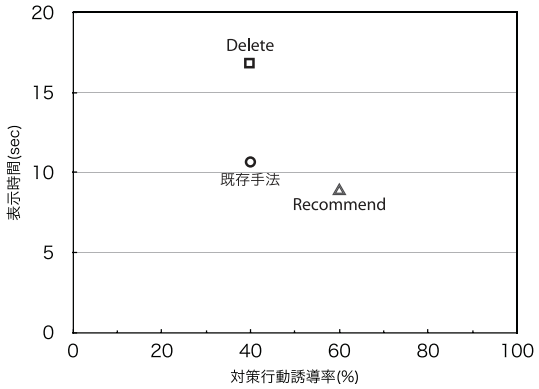

図 8　平均マルウェア対策行動誘導率・平均ダイアログ表示時間

5.2　ダイアログ注視に関する実験

Invert Dialog，Clear Dialog，Question Dialog と，既存手法においてダイアログ注視に関する評価実験を行った．

5.2.1　実験方法

提案手法，および既存手法を実装したアプリを被験者に操作させ，ダイアログに対する対応行動を測定した．本実験では実験であることを意識しない状態でダイアログ警告への反応を見ることが必要であるため，ゲームアプリの操作実験として被験者への説明を行った．また，提案手法，および既存手法を実装したアプリを含め，５種類のアプリを２回づつ，合計１０回ほどゲームアプリの操作を行わせることによって，実験の目的がダイアログ警告に関する実験だと実験途中に悟られないよう配慮した．

本実験で用いられた端末は ASUS 社の Nexus 7(2013)[10] の LTE モデルであり，OS バージョンは Android OS version 4.4.2 であった．

被験者のダイアログに対する操作の内容，およびダイアログが表示されてから閉じられるまでの時間はテキストデータとして SD カードに保存される．

全てのアプリ操作の終了後，被験者にはアンケート調査を行った．アンケート項目は，被験者の属性情報，および端末利用経験，ダイアログに書かれていたアプリの危険性の内容である．

被験者は各ダイアログに対し 5 名ずつであり，実験を 2 種類以上行った者はいない．また，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．被験者は提案手法 1 つにつきそれぞれ 5 名ずつであり (うち Invert Dialog は女性 1 名，Clear Dialog は女性 2 名，Question Dialog は女性 1 名)，全員が 20 代，高等教育を修了している被験者であった．１人の被験者が評価した提案ダイアログは 1 手法のみである．

5.2.2　実験結果

ダイアログ注視に関する実験の結果を，表 2 および図 9 に示す．ただし，被験者 i がダイアログ注視したかどうかの値 S_i を式 (3) のように定め，被験者数 n における平均ダイアログ注視率 S を式 (4) のとおりに定義する．式 (3) において，完全回答はアンケート調査でアプリの危険性の内容を正しく答えた場合，一部単語のみ回答は，例えば危険性が SMS メッセージの送信であるとき，SMS のみやメッセージの送信のみを回答できた場合とする．

実験結果から，Question Dialog が最も平均ダイアログ注視率が高いということがわかった．したがって，Question Dialog が最もユーザをダイアログ警告へ注視させることができるという結果が得られた．また，ダイアログ表示時間は既存手法が最も短く，Question Dialog が最も長いということが分かった．

$$S_i = \begin{cases} 1 & (\text{完全回答}) \\ 0.5 & (\text{一部単語のみ回答}) \\ 0 & (\text{無回答，間違った回答}) \end{cases} \tag{3}$$

$$S = \frac{\sum_{i=1}^{n} S_i}{n} \times 100 \tag{4}$$

表 2　平均ダイアログ注視率・平均ダイアログ表示時間

	ダイアログ注視率 (%)	表示時間 (秒)
既存手法	40	8.568
Invert	40	13.255
Clear	20	9.954
Question	50	42.192

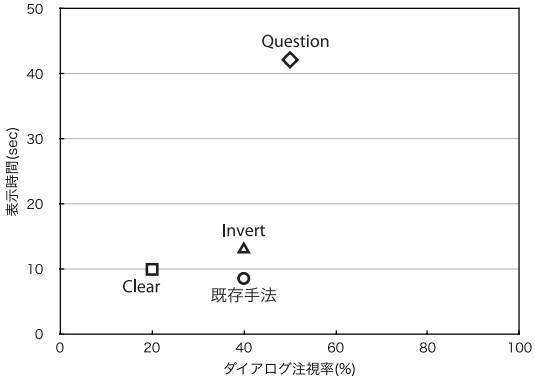

図 9　平均ダイアログ注視率・平均ダイアログ表示時間

6.　考察と今後の課題

6.1　マルウェア対策行動への誘導に関する考察

Recommend Dialog では，マルウェア対策行動誘導率に関して最もよい結果を得られたため，マルウェア対策行動としてアプリの乗り換えを提示することは有効である可能性が確認できた．一方で，アプリ操作中の類似アプリのア

イコン表示は，操作中にダイアログ内に表示される広告との混同の恐れがアンケート調査の結果から示唆されている．このことから，ダイアログの画面設計またはメッセージ内容，メッセージの提示方法を改善する必要がある．また，Recommend Dialog，および Android OS 標準ダイアログは，アプリの使用継続ボタンが即座に押せる位置に設置されているため，警告を読まずに即座に閉じてしまう問題に対しては解決できないと考えられる．

Delete Dialog では，ダイアログが表示されてから 1 秒以内に削除ボタンを押し，アプリを削除した被験者が 5 人中 1 人存在した．これは，誤って削除ボタンに触れたものであると推測される．したがって，Delete Dialog はダイアログの出現に対して注目せず，画面に対して連打するユーザに対して，危険性を認識していないものとしてアプリを削除する機能が効果的にはたらいたものと考えられる．また，1 秒以内にアプリを削除した被験者を除いた被験者のダイアログ表示時間はそれぞれ 19.282 秒，12.661 秒，34.531 秒，17.343 秒であり，平均ダイアログ表示時間は 20.954 秒である．これは既存手法の平均ダイアログ表示時間と比べて約 10 秒以上長くなっており，ダイアログを読ませる効果が向上していると考えられる．

6.2 ダイアログ注視に関する考察

Question Dialog ではダイアログ注視に関して最もよい結果が得られたため，アプリのパーミッションをダイアログを閉じる条件とすることは，ダイアログ注視に効果的であると考えられる．また，ダイアログ表示時間と Question Dialog を閉じるまでに選択肢を間違えた数の関係は，図 10 のようになった．間違い回数が多いほどダイアログ表示時間が長くなっており，セキュリティ脅威を認識しないユーザにダイアログを読ませる効果がはたらいたものと考えられる．一方で，選択式のセキュリティ脅威を憶測で答えて正解してしまうユーザが存在する可能性もある．それに対しては，記述式の回答方式にすることを今後検討する必要がある．

また，Invert Dialog ではアンケート調査の自由記述において，以下のような回答をした被験者がいた．

「ダイアログが表示された時非常に驚いて，危険なようだったのでアンインストールした．」

このことから，ユーザに驚きを与え，危険性を伝える効果が見られたことが判明した．一方で，実験結果では既存手法と比較して，ダイアログ注視率，ダイアログ表示時間のともに差が見られなかったため，警告外を危険色で反転させたとしても，ユーザはセキュリティ脅威を認識することができないことが分かった．

Clear Dialog は，ダイアログ注視率では最も低い結果が出たものの，正しくセキュリティ脅威を答えられなかった被験者のうち，半数はアプリの危険性ではなく，ダイアログを閉じる条件を回答していた．このことから，ダイアログを目を向けさせることには成功しているものの，セキュリティ脅威の把握までに至らなかったことが判明した．

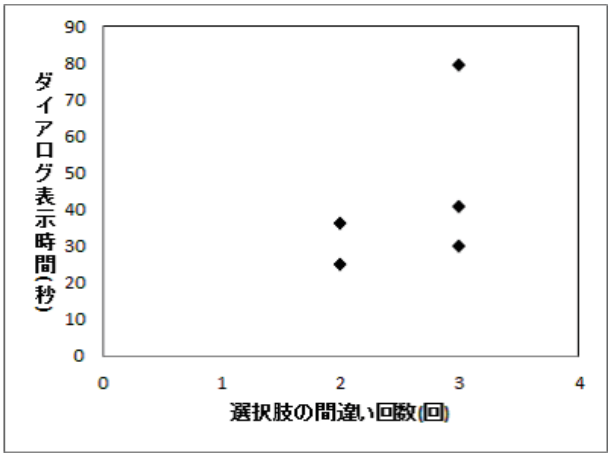

図 10　ダイアログ表示時間と選択肢の間違い数

6.3 ２つの実験から得られた総括

２つの実験の結果より，以下のようなことが判明した．

- 使用継続ボタンを即座に押せる位置に設置することは望ましくない
- ダイアログに注目しないユーザがアプリを削除するような位置に削除ボタンを配置することはマルウェア対策に有効である
- アプリのパーミッションをダイアログを閉じる条件とすることはセキュリティ脅威の認識に効果的であるが，選択式では憶測で答える可能性がある
- 警告色の使用は，驚きを与える効果は見られる
- 警告を閉じる条件を警告内容の文書と一緒に記述しても，ユーザは閉じるために必要な箇所にしか注目しない

以上を踏まえると，アプリの使用継続ボタンは即座に押下できない (例：ページ遷移した先など) 場所に設置すること，セキュリティ脅威をダイアログを閉じる条件としつつ，その条件を記述式で答えさせることが望ましいと考えられる．

6.4 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．馴化は，ユーザが同じ警告を繰り返し目にすることによってそれに慣れてしまい，警告内容に注目せず，無視するようになってしまうことである．本研究では警告表示は一度きりであり，馴化への対応が図れていない．よって，提案手法を使い続けた場合，警告を見ずに閉じてしまう問題が発生する可能性がある．馴化への対応はそれぞれの手法において次のような改善を図ることで対策できると考えられる．

- 続行ボタンをアイコン化し，お勧めアプリとの位置をランダムに変化させる．
- 続行，削除ボタンの位置をランダムに変化させる．
- 危険性のレベルに応じて警告外の色を変化させる．
- セキュリティ脅威の順番を，選択を間違える度に変化させる．
- ダイアログを閉じるボタンの位置をランダムに変化させる．

Bravo-Lillo らの研究 [12] では，Windows 警告において，警告を閉じるために毎回異なる文章を記述させることが馴化に有効であることを示しており，セキュリティ脅威を記述させることは，馴化に有効であることが考えられる．

また，今回の実験では警告文について考慮を行わなかったが，警告文の改善を図ることで注意を引き付ける効果の向上も考えられる．Khovanskaya らの研究 [13] 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，個人情報漏えいによって引き起こされる具体的な脅威を，ユーザを怯えさせるような書き方で示すことを検討する必要もある．

今後，提案手法に対してこれらの改善を図り，評価実験を再度行うことを検討する．なお，今回の評価実験においては被験者数が少ないため，実験結果の信頼性が高いとは言えない．したがって被験者人数を増やした追加実験を行うことが必要である．

7. おわりに

Android マルウェアによって，セキュリティ脅威の問題が発生している．これに対し，マルウェアの検知をユーザに通知することで解決を図る手法が存在する．しかし，既存手法ではセキュリティに関心が低いユーザは警告を無視してしまう問題があった．

本研究ではこの問題に対して，マルウェアへの対策行動の誘導と，ダイアログの注視効果の向上が解決に繋がると考え，それらを可能にする手法を提案した．ユーザをマルウェア対策行動に誘導する手法として，類似アプリをお勧めすることによってアプリの乗り換えを行わせる Recommend Dialog，ユーザが警告を読まずにボタンを押すとアプリの削除が行われる Delete Dialog を提案した．また，ダイアログを注視させることによって警告の理解を促すような警告手法として，赤色への色反転を用いることでユーザをダイアログ警告に注目させる Invert Dialog，ダイアログの内容を読まなければダイアログを閉じることが出来ない Clear Dialog，正しいパーミッションが選択できなければダイアログを閉じることができない Question Dialog を提案した．

被験者における提案手法の評価実験を実施した結果，Recommend Dialog，Question Dialog において有用可能性を見出すことができた．これによって，ユーザが自らマルウェアへの対策行動を起こすことが期待される．

今後は，馴化への対応や警告文の改善を行い，再実験を行うことによって更にマルウェア対策行動への誘導効果を高めていきたい．

参考文献

[1] KINDSIGHT SECURITY LABS: MALWARE REPORT - Q4 2013 (online), 入手先 ⟨http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf⟩ (accessed 2015-02-06).
[2] TREND MICRO, Trend Micro Mobile Security（オンライン）, 入手先 ⟨http://www.trendmicro.co.jp/jp/business/products/tmms/⟩ (参照 2015-02-06).
[3] 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).
[4] Google Play, Mobile Security & Antivirus（オンライン）, 入手先 ⟨https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity⟩ (参照 2015-02-06).
[5] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, David Wetherall: A conundrum of permissions: installing applications on an android smartphone, In *Proc. FC'12*, pp.68-79 (2012).
[6] Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh: Privacy as Part of the App Decision-Making Process, In *Proc. CHI '13*, pp.3393-3402 (2013).
[7] Marian Harbach, Markus Hettig, SusanneWeber, Matthew Smit: Using Personal Examples to Improve Risk Communication for Security and Privacy Decisions, In *Proc. CHI '14*, pp.2647-2656 (2014).
[8] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, Carolyn Nguyen: "Little brothers watching you": raising awareness of data leaks on smartphones, In *Proc. SOUPS '13*, Article No. 12 (2013).
[9] 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）．
[10] ASUS, Nexus7 (online), 入手先 ⟨http://www.asus.com/jp/Tablets_Mobile/Nexus_7/⟩ (accessed 2015-02-06).
[11] 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).
[12] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri: Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It, In *Proc. SOUPS '14*, pp.105-111 (2014).
[13] Vera Khovanskaya, Eric P.S. Baumer, Dan Cosley, Stephen Voida, Geri Gay: "Everybody knows what you're doing": a critical design approach to personal informatics, In *Proc. CHI '13*, pp.3403-3412 (2013).