スマートフォンの不正アプリに対するリスク意識調査

リスク工学グループ演習　第 7 班
加地慧留　渋木孝行　桑原惇　平野翼
アドバイザー教員　岡本　栄司

1　はじめに

1.1　研究の背景

総務省 [1] によれば，平成 25 年末，日本国内におけるスマートフォン (以下，スマホとする) 端末の世帯所有率は 62.6% に達し, パソコンによるインターネット利用が減少する一方, スマホ端末を活用したインターネット利用率は急増傾向にあり, 今後も更なる増加をしていくと予想される．スマホ端末は個人情報の集合体であり，より重要度の高い個人情報を扱うことができるようになり, 高い利便性を獲得したことから急激な普及率の伸びを見せているが, その一方で, 犯罪に悪用されていることも事実である．

実際，平成 25 年 9 月に発覚した事件 [2] において，公開された不正なアプリケーション (以下，不正アプリとする) が，約 8,000 台もの端末にインストールされ，約 70 万件もの個人情報が流出している．不正アプリに関して見れば，平成 26 年 3 月までに累計約 200 万種類のスマホ向け不正アプリが確認されている [3].

しかしながら，情報処理推進機構が 2013 年度に実施したウェブアンケート [4] によれば，スマホに有償のセキュリティソフトを導入していたのは 17.6% と非常に低い数値を示している．また，2011 年度に実施された同様のアンケート [5] によれば，スマホの個人ユーザーのうち，58.8% が『スマホをターゲットとしたウィルスについて，聞いたことはある程度，もしくは，全く知らない』と回答しており，多くのユーザーが，スマホをターゲットとした犯罪に対する認識が希薄であることがわかる．このことからも，個人ユーザーはスマホに対するリスク意識を十分に持っていない可能性がある．

本演習では不正アプリの定義を, 過去の情報漏洩事件例等を参考に,「個人ユーザーに対し悪意を持って公開され，個人ユーザーがダウンロードすることによって，その端末の情報を得ようと動作するアプリ」とする．また，個人ユーザー間で監視, 盗聴などの行為に繋がる，いわゆる盗難防止アプリや，情報漏洩を目的とせず端末の情報を破壊するようなアプリについては本演習では扱わないこととする．

1.2　目的

本演習では，個人ユーザーの不正アプリに関するリスク意識について， 個人ユーザーがアプリを危険かどうか判断する際に重要視している事象や, アクセス許可項目についての理解に関して, 調査分析を行い, 現状におけるアクセス許可項目に関する課題を明らかにする．その後, 今後のセキュリティ対策として, 個人ユーザー視点での不正アプリ対策案を検討していくこととする．

2　不正アプリに関する情報漏洩例

実際に不正アプリによって情報が漏洩した例について述べる．

2012 年 10 月 13 日, ザ・ムービー事件と呼ばれる事件の関係者が逮捕された．この事件では, 人気ゲームなどの名称の後ろに「the movie」を付け加えたアプリ名として配信された．約 9 万人から情報を取り込み, 約 1183 万件の電話番号やメールアドレスが流出, 出会い系サイト勧誘に悪用された．情報漏洩の手口として, アプリをインストールする際の同意画面において「アプリに許可する権限」として「連絡先データの読み取り」という項目を許可させることで情報を抜き取った．

2013 年 3 月頃, LIMEPOP と呼ばれる LINEPOP に似せたゲームがアプリページに新しく登録された．このアプリは起動するとゲームサーバーへの接続を試行中であるというメッセージ表示後, すぐに「通信状況を確認して下さい」という表示に変わる．この時点で連絡先のデータが詐欺グループサーバーにアップロードされてしまう．これは Android.Enesoluty と呼ばれるウィルスの亜種とされており, 違いとしてはマルウェアの外見的な変化だけである [6].

3　研究手法

本研究ではアンケートを用いてリスク意識に関する予備調査と本調査を行った．本調査は予備調査を基に，調査方法や質問項目の修正，目的に向けた質問項目の設定等を行い，作成した．アンケートについての概要を表 1, 2 に示す．

表 1　アンケート予備調査概要

実施日程	7 月
調査対象	主に学生
方法	アンケート用紙配布
サンプル数	79

表 2　アンケート本調査概要

実施日程	7 月～9 月
調査対象	主に学生
方法	アンケートボックスと 調査票の設置
サンプル数	98

4　結果および考察

4.1　予備調査

予備調査の結果より，ユーザーたちのリスク意識が高い人と低い人に分けることが可能ではないかという推測が生まれた．そこで本調査のアンケートにおいては，いくつかの質問項目を用いて，個人ユーザーの主観的な意識を基にリスク意識の高低を分類できるように作成した．

4.2　本調査の集計結果の考察

まず，集計結果の単純な考察を行う．

「スマートフォンアプリをダウンロードする事に，危険がともなうと思いますか」，「あなたがスマートフォンアプリを不正アプリ（悪意を持った動作をするアプリ）と知らずにダウンロードしてしまうことがあると思いますか」，「スマートフォンアプリ内でウェブサイトへのリンクが表示されるとき，そのサイトへのリンクが危険だと思いますか」という 3 つの質問について，「とてもそう思う (6)」「そう思う (5)」「少し思う (4)」のいずれかを回答したのはそれぞれ 69%，63%，76% となっており，少なからずスマートフォンアプリの利用が危険性をはらんでいるということを感じていることがわかる（図 1, 2, 3）．

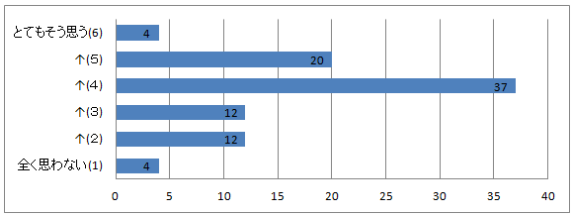

図 1　アプリをダウンロードすることに危険がともなうと思いますか

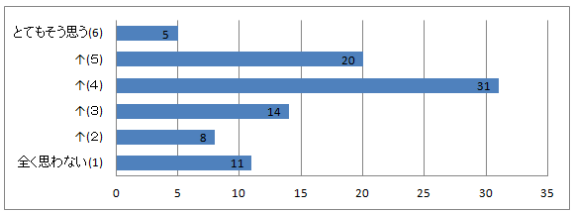

図 2　不正アプリと知らずにダウンロードしてしまうことがあると思いますか

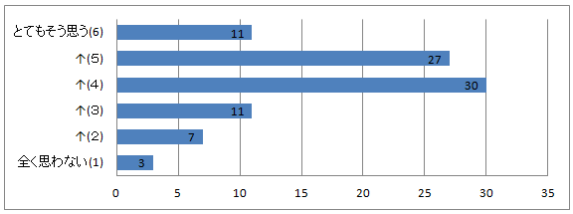

図 3　ウェブサイトへのリンクは危険だと思いますか

しかしながら「スマートフォンアプリの更新時に，そのアプリのアクセス権限を再確認しますか」という質問には対しては 43% が「必ず確認する (6)」「確認する (5)」「少し確認する (4)」のいずれかの回答をしており，確認している人は少ないことがわかる（図 4）．危険性を感じているユーザーは多いにもかかわらず，過半数のユーザーがスマートフォンアプリの更新時にアクセス権限を再確認していないことは，アプリの更新時にアクセス権限を追加されるような不正アプリに対しては脆弱であることがうかがえる．

アクセス許可項目はアプリの危険性に大きく関わる要素だと考えられる．そこで，アクセス権限に関する質問も行った．質問項目におけるアクセス許可項目の中で危険なアプリかどうかを判断するための重要度についての質問（図 5）に対して，「重要である (5)」または「とても重要である (6)」といった重要度の高い回答をした数が最も多かったのは「連絡

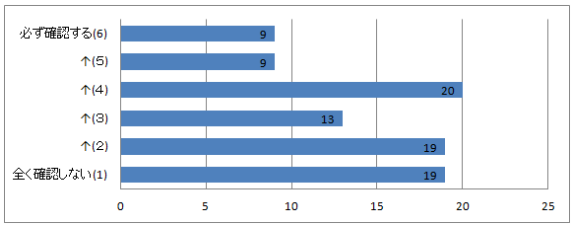

図 4　アプリの更新時, アクセス権限を再確認するか

先」であり，半数を占めている．一方で，全体的に「わからない」や「全く重要でない (1)」「重要でない (2)」といった重要ではないという回答が多くあり，アクセス許可項目の理解度の低さがうかがえる．また，最も少なかったのは「カレンダー」,「その他の項目」である．この理由として，カレンダーについては利用していないことが，その他の項目についてはリスクを考える上での重要性が実際に低いことや分からないことが挙げられる．

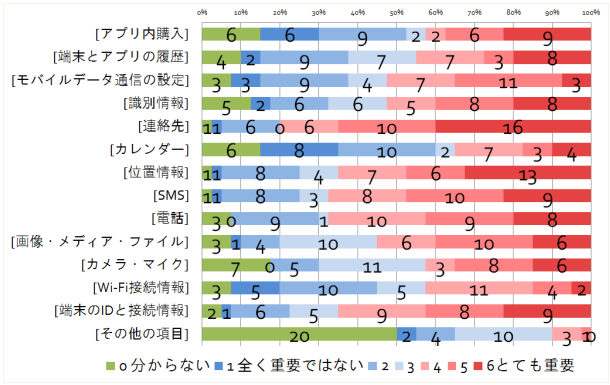

図 5　アクセス許可項目の重要度の回答

質問項目におけるアクセス許可項目の理解しづらさや, 表示画面の見づらさについて,「とてもそう思う (6)」「そう思う (5)」「少し思う (4)」のいずれかを回答しているのはそれぞれ 82%，71% となっており，とても多くなっている（図 6, 7）．これは，ユーザーがアクセス許可項目を理解できないことにつながり，例え理解できたとしても，アクセス許可項目の表示方法を間違えば，正しい理解とそれに基づいた許可を得られないことに繋がる可能性が高いため，早急に対処する必要があると考えられる．

次に，許可の確認方法についての質問を行った．スマートフォンアプリを起動するたびにアクセス権限を確認したいと思うかどうかについては, 回答に特別な偏りは見受けられないが，アクセスして

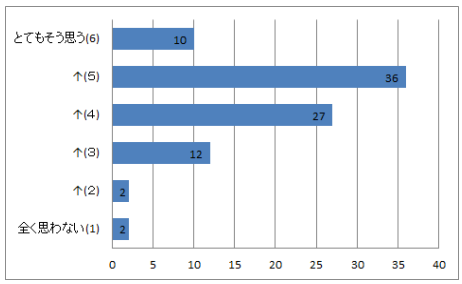

図 6　アクセス許可項目内容は，理解しづらいと思いますか

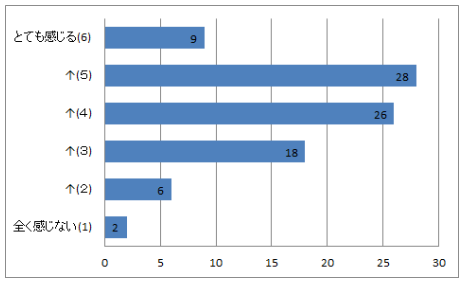

図 7　アクセス許可項目表示画面は，見づらいですか

いる項目を通知バーへ表示する方法についてでは 70% が表示されたら良いと答えており，手軽かつ操作の邪魔にならない確認方法が受け入れやすいと考えられる（図 8, 9）．

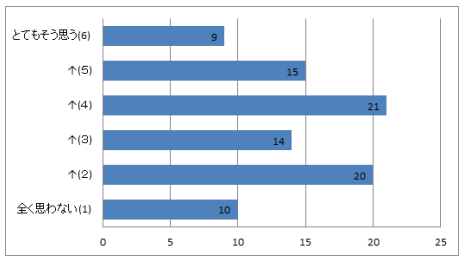

図 8　起動する度に，アプリに許可されている権限の内容を確認したいですか

また，スマートフォンアプリのアクセス権限を許可する方法について質問をした．現在，Android ではインストール時にすべてのアクセス権限を許可する．一方で，iPhone ではアプリ使用時に個別に権限を確認している．回答では「アクセス権限を個別に許可する」方法が最も多く，69% となっている（図 10）．

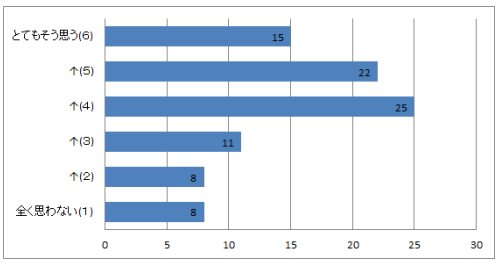

図 9　使用時に，アクセスしている項目が画面上部に表示されたら良いと思いますか

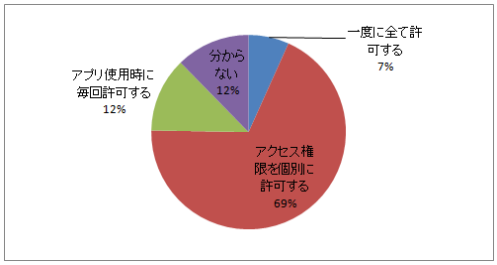

図 10　アクセス権限を許可する方法

4.3　リスク意識の差による比較

次に，本調査のアンケート結果を基にリスク意識の高い人と低い人に分割し，比較して分析を行った．分割に利用した項目は次の 7 項目である．

- あなたのスマートフォンに対するセキュリティ対策は万全だと思いますか
- 便利なスマートフォンアプリをダウンロードする時に，そのアプリが疑わしい動作をするかもしれないと感じた場合，あなたはダウンロードを止めると思いますか
- スマートフォンアプリの更新時に，そのアプリのアクセス権限を再確認しますか
- スマートフォンアプリをダウンロードする事に，危険がともなうと思いますか
- スマートフォンアプリを悪用した犯罪 （個人情報流出など） に関するニュースや記事に，関心はありますか
- あなたがスマートフォンアプリを不正アプリ（悪意を持った動作をするアプリ） と知らずにダウンロードしてしまうことがあると思いますか
- スマートフォンアプリ内でウェブサイトへのリンクが表示されるとき，そのサイトへのリンクが危険だと思いますか

また，分割には K-平均法 [7] によるクラスタリングを用いて，2 つのグループに分割した．そのクラスタの 1 つをリスク意識の高いグループ (グループ A)，もう 1 つをリスク意識の低いグループ (グループ B) とする．グループ A は 40 人，グループ B は 49 人という分類結果となった．

図 11, 12 のグラフを見ると，リスク意識が低いグループでは「わからない」という回答が多く，リスク意識が高いグループのほうが各項目で重要と答えている割合が大きいため，分類結果は妥当なものだと考える．

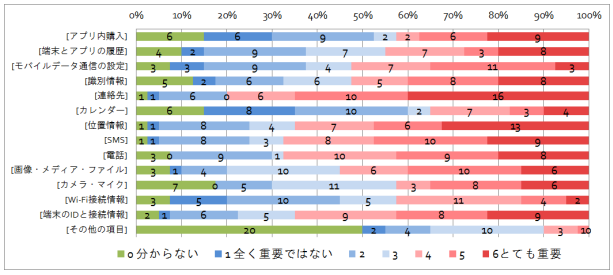

図 11　リスク意識が高いグループのアクセス許可項目の重要度

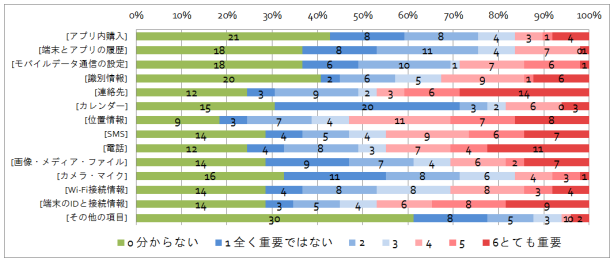

図 12　リスク意識が低いグループのアクセス許可項目の重要度

続いて，クラスタリングに用いた 7 項目の質問を除くアンケートの質問項目に対してグループ A とグループ B に差があるかどうかを確かめる．本調査では，主にリッカート尺度を用いた順序尺度を採用しているため，Mann-Whitney の U 検定 [8] を行い，それ以外の項目については χ^2 検定を行って確かめる．表 3, 4 に各質問項目に対する有意確率を示す．

これにより，有意水準 5% 下において有意差があったのは以下の項目であった．

- セキュリティソフトの導入について
- アクセス項目の重要度 (アプリ内購入，端末と

表 3　Mann-Whitney の U 検定による各質問項目に対する有意確率

	スマホを利用した年数の合計	1日のスマホの使用時間	アプリのダウンロード頻度
有意確率	0.193	0.976	1.000

アクセス許可項目の重要度				
［アプリ内購入］	［端末とアプリの履歴］	［モバイルデータ通信の設定］	［識別情報］	［連絡先］
0.001	0.000	0.000	0.004	0.008

アクセス許可項目の重要度				
［カレンダー］	［位置情報］	［SMS］	［電話］	［画像・メディア・ファイル］
0.004	0.034	0.005	0.065	0.001

アクセス許可項目の重要度			
［カメラ・マイク］	［Wi-Fi接続情報］	［端末のIDと接続情報］	［その他の項目］
0.000	0.138	0.048	0.098

アプリが危険かどうか判断するときの重要度				
［アプリについての説明］	［星などの点数による評価］	［レビューの文章］	［レビュー数］	［ダウンロード数］
0.164	0.963	0.441	0.940	0.170

アプリが危険かどうか判断するときの重要度		
［開発者］	［口コミや知人の紹介］	［アクセス許可の項目］
0.020	0.018	0.000

アクセス許可項目内容は、理解しづらい	アクセス許可項目表示画面は、見づらい	アプリに危険や不安要素が見られたとき、アンインストールする	起動する度に、アプリに許可されている権限の内容を確認したい	使用時に、アクセスしている項目が画面上部に表示されたら良い
0.004	0.437	0.375	0.009	0.889

表 4　χ^2 検定による各質問項目に対する有意確率

	スマホの種類 (OS)	セキュリティーソフト導入	アクセス権限を許可する方法
有意確率	0.114	0.000	0.063

アプリの履歴，モバイルデータ通信の設定，識別情報，連絡先，カレンダー，位置情報，SMS，画像メディアファイル，カメラマイク，端末の ID と接続情報)

- アプリの危険判断の重要度 (開発者，口コミ，アクセス許可)
- アクセス許可項目が理解しづらい
- 起動するたびアクセス権限を毎回確認したい

セキュリティソフトの導入については，グループ B では 10% と非常に低い導入率となっている（図 13）．また，グループ A でも 53% にとどまり，決して高くない導入率である．セキュリティソフトは不正アプリの検知やウイルス対策の要であるため，導入率が低いことは決して見過ごすことはできない．

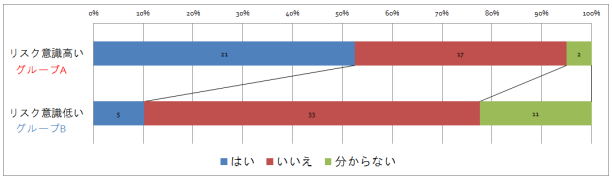

図 13　セキュリティソフトを導入しているかどうか

また，前述したとおり，アクセス項目の重要度の質問ではグループ B については，「わからない」を選択した人がとても多くなっている．このことからもやはり，グループ B は知識が不足していることがわかる．

アプリの危険判断の重要度については，グループ A はアクセス許可項目のほか，開発者，口コミのように知名度や話題からも情報を得ていることがわかる．

また，グループ B はアクセス許可項目がわかりづらく，権限の内容を確認したくないと思っていることが分かる．しかしながら，スマホの利用年数や使用時間については有意差がなかった．この原因として，スマホの扱いに慣れていないからアクセス許可に対する意識が薄いというよりは，元々の知識が不足していることや，楽観していること等が考えられる．

5　結論

以上の分析から，ユーザーは，アプリに対して危険性を感じているにも関わらず，セキュリティソフトを導入するに至っていないということが明らかとなった．また，アクセス許可項目の理解や認知が不足しており，危険回避のための判断基準が曖昧となり，選択肢中の「わからない」や低い重要度を選択する傾向にあったと考えられる．

また，ユーザーがアプリ利用時に重要視している項目や不正アプリに対して警戒しているアクセス許可項目などが明らかとなり，リスク意識の高い人と低い人で分類することができた．その分類では，アクセス許可項目に関する認識や重要度に差があり，その原因の一つとして，アクセス許可項目の煩雑さや，提示方法に大きな課題があることが明らかとなった．

本演習で明らかになった内容から，アクセス許可項目の煩雑さについては，許可項目を的確に表現する端的な項目設定ができていないことが要因として考えられる．これに関しては，ユーザーが一目で理解し，誤解を生じない項目を設定することが有効な

対策だと思われる． また, ユーザー自身で実施できる対策として, アクセス許可項目の内容をきちんと理解することが挙げられる．しかしながら, アクセス許可項目の詳細を知るすべは限られているため, ユーザー自身が自ら進んで理解を深め, 無知なことがリスクを高めているということを自覚することが必要である．さらに, 提示方法に関して，本調査で深く言及していないが，アクセス許可項目ごとの個別許可を充実させることや，アプリ起動中にそのアプリがアクセスしている項目を明示するなどの対策案があり，これらの対策の有効性を検討していくことが今後必要になってくると考えられる．

6 今後の課題

本演習を通して，不正アプリに関する多くの課題が明らかとなった．セキュリティ対策に関しては万全と答えている人は少ないのに対し，実際にセキュリティソフトを導入している人は少ない．近年，スマホのセキュリティが注目されており， 様々なセキュリティ対策ソフトが公開されている．ウイルス対策の機能を含む，セキュリティ対策ソフトの導入推進も非常に重要な課題の一つである．

また，セキュリティソフトで防ぎきれない部分についても，ユーザー自身で注意深くアクセス許可を行う必要がある．そのためには，アプリの入手元に関わらず，インストール時に表示されるアクセス許可の一覧を一読し，不自然であったり，疑問に思う点があれば，インストールを中止するような判断が求められていくであろう．

そして, ユーザー自身の判断を有効性を持たせるためにも，ユーザー視点に立ったアクセス許可項目の検討やインターフェースの構成も今後重要な課題となる．ユーザーが理解し，許可するはずの項目が，最も重要視されるはずのユーザーに理解されず，意図しない許可を実施していることは今後の重要な課題である．本調査では，ユーザーが求めるアクセス許可の方法を確認しているが，結果として，個別に許可する方法がユーザーにとって最も安心できる形式となった．個別にアクセス許可をする形式を実施したとしても，項目の内容をユーザーが把握していねければ意味がない．そのため，結論で述べたとおり，ユーザー視点に立った項目設定をする必要がある．また，ユーザーに対するアクセス許可項目の提示方法などについても，今後検証していく必要があるであろう．

参考文献

[1] 総務省, 平成 25 年通信利用動向調査，別添え 1，平成 26 年 6 月

[2] 産経ニュース, 「電池長持ちアプリで電話帳データ抜き取り」, http://sankei.jp.msn.com/west/west_affairs/news/130925/waf13092519060025-n1.htm（最終閲覧日：2014 年 10 月 7 日）

[3] TREND MICRO 社, セキュリティブログ, http://blog.trendmicro.co.jp/archives/8808（最終閲覧日 : 2014 年 10 月 7 日）

[4] 独立行政法人情報処理推進機構, 情報セキュリティの脅威に対する意識調査報告書 (2013 年 度), http://www.ipa.go.jp/security/fy25/reports/ishiki/index.html（最終閲覧日：2014 年 10 月 7 日）

[5] 独立行政法人情報処理推進機構, 情報セキュリティの脅威に対する意識調査報告書 (2011 年度), http://www.ipa.go.jp/security/fy23/reports/ishiki/index.html(最終閲覧日：2014 年 10 月 7 日)

[6] All of Connect — Symantec Connect,「Lime Pop : Android.Enesoluty の新しい不正アプリ」, http://www.symantec.com/connect/blogs/lime-pop-androidenesoluty（最終閲覧日：2014 年 10 月 12 日）

[7] 小田利勝, SPSS による統計解析入門, プレアデス出版, 2007

[8] 内田治，すぐわかる SPSS によるアンケートの統計的検定，東京図書，2011

[9] 警察庁，平成 25 年中のサイバー犯罪の検挙状況について，http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf（最終閲覧日：2014 年 5 月 30 日）

[10] 内閣府, 平成 26 年 3 月実施調査結果・消費動向調査，http://www.esri.cao.go.jp/jp/stat/shouhi/2014/201403shouhi.html(最終閲覧日：2014 年 5 月 30 日)

[11] 阿久津毅 (2011), 学生のスマホ使用に関する意識調査 (個人情報保護の観点から), 日本教育情報学会, 年会論文集 (27), 284-285, 2011/8/20