Vol.2014-DPS-158 No.46
Vol.2014-CSEC-64 No.46
2014/3/7

# Android OS端末の情報漏えい通知における Just-In-Time Notificationの改良

山方 雄太[1]　金岡 晃[1]

**概要**：Android OS からの情報漏えいに対し、Balebako らは SOUPS2013 において漏えい時に通知をあげる Just-In-Time Notification を提案し、それを実装した。しかし Balerako らの通知手法は利用者に漏えいを認知させるため手法としては改良の余地がある。本論文では Just-In-Time Notification の通知手法を改良し、提案手法を Android OS の端末上に実装し、その効果をユーザ実験を行うことで確認した。

## 1. はじめに

スマートフォンの多機能性は、パーソナルコンピュータとは異なるセキュリティとプライバシの脅威をユーザにもたらしているが、急激に広まるスマートフォンに対してその脅威への対策が急がれている。スマートフォンにおけるアプリケーションの中には、ユーザの意図しないタイミングでユーザ情報を外部に送信してしまうものがある。こういった意図しない送信による情報漏えいやプライバシの侵害に対応するため、Android ではインストール時にそのアプリケーションが持つパーミッションを提示している。しかしそのパーミッションについては、ユーザの知識レベルの差異による理解の不足や、そもそもパーミッションに関心を示さないなどの問題が確認されており、それらの対策の研究も様々なアプローチで行われている [1], [2]。

Android におけるセキュリティやプライバシの対策の 1 つに、インストール時の脅威判断材料の提示ではなく、脅威が発生した瞬間に通知を行う研究がある。Balebako らは Privacy Leaks と名付けたアプリケーションにおいて、Just-In-Time Notification（以後 JIT 通知）を提案し実装した [3]。そこでは、ユーザの情報が漏えいした瞬間に Android の通知領域等に情報を提示するものである。ユーザのインストール時の関心の薄さが指摘されていることから、脅威が発生した瞬間に着目した提案であり、その効果が実験で示されている。しかしその実装はシンプルなものであり、より高い効果が得られる通知インタフェースを検討することが可能である。

本論文では、Balebako らが提案した JIT 通知を改良するために、その改良アプローチを検討し、Android の開発要件と合わせた実現方法を提案する。さらに、通知インタフェースのより高い効果を狙うものとして、全ユーザを対象とした画一的な通知インタフェースではなくユーザの属性に応じたインタフェースを提供するような通知の仕組みを提案する。提案した手法を実装しユーザ実験によりその効果を確認した結果、Balebako らの通知インタフェースを模したものよりも高いリスク認知効果を示すことに成功した。

## 2. 関連研究

スマートフォンでのアプリケーションインストール時にプライバシとセキュリティのリスクを理解することの難しさについて、Kelley らは Android ユーザがそのパーミッションの用語等の理解に困難を感じていることを示した [1]。また Felt らはインターネットを利用し Android ユーザ 308 人、また研究室において 25 人について調査を行い、その結果 17% だけがインストール時のパーミッション情報に注意を払っていることを示した。さらに、3%の回答者がパーミッションを表示する画面内容のすべてを理解していることを示した [2]。Android ユーザはインストール時にはそのパーミッションへ関心を示すことが少なく、また理解もしていないことが示されており、それらに対する研究もさまざまなアプローチでされている。

本研究では、インストール時でのプライバシとセキュリティのリスクを認知させるのではなく、実際にリスクが発生するタイミングの周辺においてその認知をさせることに着目した。関連する研究では、Cranor らが 2006 年に Privacy Bird を提案し実装している。これは Web ブラウザに適用するエージェントであり、Web サイトのプライ

[1] 東邦大学
2-2-1, Miyama, Funabashi, Chiba 274–8510, Japan

バシポリシを読み込み、ユーザの選んだ設定 (Preference) と異なる動作を行う場合は音とアイコンにより通知を行うものであった [4]。 Balebako らは Privacy Bird の考えを Android に拡張し、JIT 通知と漏えいした情報についての表示の 2 つを備えたアプリケーション Privacy Leaks を提案している [3]。Android ではないが JIT 通知と類似するセキュリティ・プライバシ対策機構として Wi-Fi Privacy Ticker がある [5]。暗号化がされていない Wi-Fi アクセスポイントを利用している際にあらかじめユーザが登録してある情報の漏えいを防ぐ仕組みである。対象となる情報が送信される前に遮断（Drop）し、また画面上に通知を出す。

## 3. JIT 通知の改良

### 3.1 JIT 通知

Balebako らは Privacy Leaks において 2 つの機能を提案し実現している。1 つは漏えいするアプリケーションと漏えいする情報の可視化であり、もう 1 つは漏えいするタイミングでユーザに通知を行う JIT 通知であった。JIT 通知は情報が漏えいした瞬間に音（水が滴る音）とバイブレーションで端末に通知を行う。また通知領域に漏えいの事実を伝え、また通知ドロワにおいてより詳細な情報を提示する。

JIT 通知で表示される情報は以下となっている [*1]。

- 通知領域：文章のみの表示
  - アプリケーション Toss It での例： Toss It leaked Phone ID
- 通知ドロワ：文章のみの表示
  - アプリケーション Toss It での例： Toss It leaked your Phone ID Location at 2:26 PM

いずれも単純な表示となっている。

Balebako らは、Privacy Leaks の評価として 19 名の研究室実験を行い、最初に Privacy Leaks をインストールしていない端末において情報漏えいを行うアプリケーション（2 種類のゲーム）をプレイしてもらい、その後情報の漏えいについてのインタビューを行った。続いて同じ 19 名に対し Privacy Leaks をインストールした端末を渡し、同様に 2 種類のゲームをしてもらい、その後同様のインタビューを行った。インタビューの結果では、Privacy Leaks の有用性について同意あるいは強く同意をするユーザは 16 名 (84.2%)、Privacy Leaks が意味する情報を理解したかという質問には 6 名（31.6%) が同意あるいは強く同意をした一方で、どちらでもないまたは同意しないを選択したユーザが 13 名 (68.4%) いた。また提示された情報の妥当性については 16 名（84.2%）が妥当である旨を表明し、通知が邪魔だとしたユーザは 3 名（15.8%) に対し、迷惑と感じないとしたユーザが 15 名 (78.9%) とあり、PrivacyLeaks がユーザビリティを損ねることなく情報を提示できていることを示していた。

Privacy Leaks の問題点は、ユーザビリティを損ねることなく通知している一方でその内容の理解を提供していないことにある。本研究では、その問題点を通知領域と通知ドロワ等の JIT 通知の単純さにあると仮定をし、その改良をすることでより高い効果を求めるものである。

### 3.2 提案手法 1：Android 機能の活用

#### 3.2.1 Toast、Notification

ここでは Android 機能の Toast と Notification の 2 種類に注目する。

Toast は、ポップ形式のメッセージが一定時間表示され、自動的に消えるシステムである。ユーザーの現在の操作を中止することなく通知が行えるという特徴を持っている。メッセージは、画面の下部に、水平方向でセンタリング表示され、数秒間 (2 秒〜4 秒) 経つと自動的にフェードアウトしながら消える仕組みになっている。また Toast は、他のアプリケーションが全面に出ている時でも、バックグラウンドにあるアプリケーションが Toast を出すことができる。

Notification は、2 種類の通知箇所を使い、端末の状態をアイコンやメッセージなどで通知を行える特徴を持っている。また、サウンドやバイブレーション、LED などの通知方法を併用することで、ユーザーに対してより効果的な通知を行うことが可能である。以下に 2 種類の通知箇所を挙げる。

- 通知領域
- 通知ドロワ

通知領域は、端末の画面上部に位置しており、短いメッセージでユーザーに通知を表示後、4 秒後にアイコンに切り替わる仕組みになっている。通知ドロワは、通知領域を上から下になぞるような動作を行うことで表示することができる。通知ドロワで通知領域に表示されているアイコンの詳細を確認することができ通知内容によって、WEB サイトに移動したり、メールの返信が行えたりする。この通知ドロワを開き、内容を確認することで通知領域のアイコンが消える仕組みになっている。通知ドロワは、Android4.1 より新たに 3 つのスタイルが加わり、また拡張ビューが使えるようになった。拡張ビューには、最大 3 つのボタンを表示させることができ、これらのボタンを押すことにより、Web サイトに移動したり、メールの返信が行えたりする。

- Big picture：大きく写真を表示可能
- Big text：長いメッセージを表示可能
- Inbox：複数行に分けてメッセージを表示可能

#### 3.2.2 改良アプローチ

Balebako らの JIT 通知では、音として水が滴る音、振動としてはバイブレーション、表示としては Notification を

[*1] 通知画面については Balebako らの論文 [3] を参照されたい

利用し通知領域と通知ドロワに単純な文章を利用していた。これらの改良にあたって、以下の点の改良が考えられる

- 通知領域の表示方法
- 通知ドロワの表示方法
- Toast の利用
- 音
- バイブレーション

通知領域の表示方法については以下の改良案が考えられる。

- 表示アイコンの拡大（縦、あるいは横）
- 複数のアイコン表示による表示ゾーンの占拠
- カラー化
- 動くアイコン（アニメーション Gif 等）

しかし、Android アプリケーションの開発制限により、表示アイコンの拡大、複数のアイコン表示、動くアイコンは実施できないため、カラー化のみが改良対象となる。

通知ドロワの表示方法についても、以下の方法案が考えられる。

- 表示アイコンの拡大（縦、あるいは横）
- 複数アイコンの表示による表示ゾーンの占拠
- カラー化
- 動くアイコン（アニメーション Gif）
- 通知ドロワ表示時にさらにアピール (通知ドロワ画面上で振動させる、点滅させる等)

しかし、こちらも Android アプリケーションの開発制限により、複数のアイコン表示、動くアイコン、通知ドロワー画面の振動は実施できない。そのため、表示アイコンの拡大、カラー化が改良対象となる。

Toast の利用は Balebako らの研究では採用されていない手法だが、ユーザーへの通知方法としては効果が望める。しかし Toast も制限があり、表示位置や字の大きさ、色は変更できるが、表示時間は 2 秒または 5 秒のみ設定が可能である。最長で 5 秒間の表示であるため、文章の量の調整が必要となる。

音とバイブレーションに関しては、監視対象となっているアプリケーションの音やバイブレーションと混同されにくい仕組みが必要となる。

本論文では、以下の点について改良を行った。

(1) 通知領域の表示：カラー化
(2) 通知ドロワの表示：表示アイコンの拡大、カラー化
(3) Toast の利用
(4) 音：シンプルなブザー音

本論文ではバイブレーションについての改良は行わなかった。後述する実験に用いた端末がバイブレーションに非対応のタブレット端末であったためであるが、その効果を否定するものではない。

### 3.3 提案手法 2：ユーザ属性に応じた通知方法：SUN（Shimura Ushiro Notification）

Egelman らは、最適なリスク緩和に向けた方策として個別化（Individualization）という方向性を示した [7]。そこでは、現在の Usable Security の文脈では人間の振る舞いを集合体として扱って極大値を得たものを対象にしたソリューションとなっているが、どの個人もそういった「平均のユーザ」ではないことを指摘しており、今後の方向性として個別化があることを主張している。しかし個別化を実現するためには、個別化するための情報を詳細に得なければならず、また、例えば Android の通知に限った話であっても個別化に対しての表示情報の切り替えなどは簡単には実現できるものではないことが容易に考えられる。

本研究では、個別化に向けた段階の 1 つとしてユーザ属性に応じた表示方法についてを検討する。これまでの Android におけるリスク認知の手法はユーザ属性を絞ったアプローチはされておらず、人間という大きな範囲で画一的に語られていた。個別化にいたる前の段階として、ユーザが持つ属性に応じて表示を変えることで、より効果的かつユーザビリティの高いリスク認知ができる可能性がある。ユーザが持つ属性は様々なものがあるが、その属性の中で強く共通する事象等が存在すれば、それらを応用することで効果的なリスク認知をできると仮定し、本論文ではそれらの機構を SUN（Shimura Ushiro Notification）と名付けた。

SUN では、前節で示した改良点について、ユーザの属性に合わせた改良を行うことでより強い効果を JIT 通知に与えるものである。属性は性別、年齢、所属、知識等さまざまなものが選択可能である。例えば、情報技術についての知識を深く持っている場合では、より正確な用語や情報技術の分野で共通したアイコンを利用することでリスク認知の効果を高めることが考えられる。

SUN の具体的実現では、最初に「年齢」に着目した。戦後の高度経済成長を経るなかで急激に発展したさまざまなメディアにおいて、現代とは異なる情報のインプットがされており、選択肢の少ない情報を多くの国民がそれを受容するという形が一般的であった。代表的なものとして、1970 年代から 80 年代にかけて小中学生に広く支持されていたザ・ドリフターズの「8 時だョ!全員集合」がある。これは 1969 年 10 月 4 日から 1985 年 9 月 28 日に TBS 系列で放送されていたテレビ番組である。番組全体での平均視聴率は 27.3%、また最高視聴率が 50.5%と、非常に広く支持されていたことがわかる。

番組内ではいくつものコントが行われていたが、代表的なコントの 1 つに探検をシチュエーションとしたものがあった。そこでは探検に出たメンバーの 1 人が道に迷うなどではぐれ、1 人になったところで周辺の彫刻やミイラなどが動き出す。メンバーの 1 人（当初はザ・ドリフターズ

のメンバーの加藤茶であったが、のちに志村けんが担当した）はその動き出した彫刻等に気づかず、観客が「志村！後ろ！」と大きな声で指摘をするが志村けんは気づかない、というところにコントの面白さを含ませていた。

この志村けんと「志村！後ろ！」という観客からの叫びの関係は、現在の Android ユーザと Android のアプリケーションに対するプライバシとセキュリティの警鐘を鳴らす現状況と類似していると考えた。またそのフレーズは該当番組が放送されていた期間に小学生あるいは中学生であった層には広く受け入れられるものであり、属性に応じた表示として適していると考えた。「8 時だョ!全員集合」の放送当時に小学生高学年（満 10 歳から 12 歳）であるユーザ（1957 年から 1975 年生まれ *2）を対象とした通知方法とし、その通知音にコント内で利用された音楽を利用し、通知領域に表示するアイコンには志村けんの画像を用い、また通知ドロワにはまず注目を促す機能が必要であると考え、画像と共に大きく「志村！後ろ！」と表示することとし、タップすることで詳細のリスク表示へ導くものとした。

## 4. 提案手法の実装

### 4.1 実装環境と通知トリガ

実装は Google 社の Android 端末 Nexus7（2013）で行った。また通知のトリガとなる情報取得のために Nexus7 に対し管理者権限を取るような修正を加えた。Balebako らの実証実験では TaintDroid を用いて通知トリガを仕込んでいたが、TaintDroid は実験の時点において Nexus7 において動作が確認されていなかったため、管理者権限でのログ監視をトリガとした。ログ監視は LogCat コマンドを利用し、一定間隔で LogCat コマンドを実施し前回コマンドとの差分から監視対象のログを発見し、漏えいが確認された段階で通知を行うこととした。Balebako らの実験でも利用されていたアプリケーション「Toss It」は、位置情報と Phone ID を送信しているが、LogCat コマンドの出力からは送信先 URL のみが現れ、情報の内容自体は観測できないため、本実装では「Toss It」に対しては該当 URL がログに出現した時点をトリガとした。

### 4.2 提案手法 1

通知が行われた時、警告音による通知と画面中央部にアイコンを表示し、Toast で「アプリケーション「＜アプリケーション名＞」は個人情報を外部へ送信しました。詳細は通知領域を見てください。」と 5 秒間表示した。通知領域には、アイコンの表示と共に「警告：個人情報が漏洩しています」という表示を行う。通知ドロワには、拡張ビューの BigText スタイルを利用し「警告」という見出しを付け、「アプリケーション「＜アプリケーション名＞」は個人情報を外部へ送信しています」と表示した。また拡張ビューの特徴である、ボタンを 2 つ配置し、詳細表示と管理者への連絡 (メール送信画面の起動) を行えるようにした。Toast と通知領域、通知ドロワには、目立たせるために黄色い警告のアイコンを使用した (図 2)。

*2 2014 年に 39 歳から 56 歳となる年齢

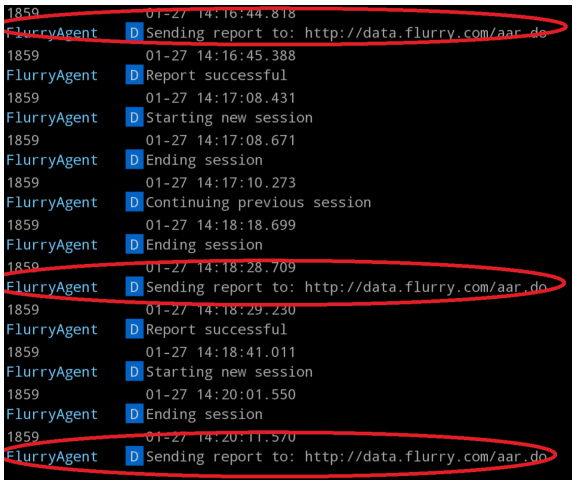


**図 1** アプリケーション「Toss It」のログ


**図 2** 提案手法搭載インターフェイス（アプリケーション Toss It 利用時）

### 4.3 提案手法 2

SUN の実装は、前節の「Android 機能の活用」をもとに、音を変更し、Toast、通知領域、通知ドロワに表示される画像と文字列を「提案手法 2：ユーザ属性に応じた通知方法：SUN（Shimura Ushiro Notification）」で示したものに変更し実現した。

## 5. ユーザ実験による提案手法の評価

### 5.1 実験の目的と実験概要

実際に提案手法 1 を実装したアプリケーションを用いてユーザ実験を行うことで提案手法の評価を行うためにユー

ザー実験を行った。

実験の被験者は、東邦大学理学部情報科学科の学生の Android ユーザー 14 人を対象とした。実験内容は提案手法 1 を導入したインターフェースと導入していない一般的なインターフェースの 2 種類の通知アプリケーションをインストールしたタブレット端末を渡し、ユーザーにどちらかのインターフェースをランダムで試してもらい、作業終了後に事後アンケートを実施してユーザに提案したインターフェイスが効果的なのかを確かめるというものである。

#### 5.1.1 本実験で利用した一般的なインターフェース

通知が行われた時、通知領域に「個人情報が外部へ送信されています」という警告文の表示のみを行うシンプルなインターフェースである。Balebako らの JIT 通知を参考にして作成した。通知領域のアイコンもシンプルな物を使い、通知ドロワには、標準ビューを利用し「個人情報が外部へ漏洩しています」と表示し、「詳細はこちらへ」を押すことで詳細表示のページへ移動する (図 3)。


**図 3** 本実験で利用した一般的な通知インターフェイス

### 5.2 実験内容

被験者には、JIT 通知アプリケーションをインストールしたタブレット端末「Nexus 7(2013)」で実験を行った。実験被験者には、本当の目的を知っているとプレイ中の振る舞いに偏りが生じる恐れがある為、「暗号機能の OS への動作影響について調べたい」と伝え、アプリケーション「Toss It」のプレイをしてもらう実験を行った。尚、実験の説明は、説明に偏りが出ないように実験協力書と題して用紙を配布して行った。

実験後に被験者に本来の目的である「Android アプリケーションの情報漏洩通知インターフェイスの研究」であると伝え、アンケートに協力を依頼した。尚、アンケート協力の際も説明に偏りが出ないように、アンケート依頼と題した用紙を配布した。通知インターフェイスは 2 種類あるため、アンケート依頼もそれぞれ、一般的な通知インターフェイスと提案手法 1 搭載インターフェイスの 2 種類を作成し、実験時に利用したインターフェイスの方のアンケート依頼のみ配布し回答を集めた。

**表 1** 実験被験者男女合計人数

| | 一般的な通知 | 提案手法搭載通知 | 合計 |
|---|---|---|---|
| 男性 | 6 | 1 | 7 |
| 女性 | 1 | 6 | 7 |
| 合計 | 7 | 7 | 14 |

### 5.3 アンケート内容

アンケートは、まず属性を把握するために性別と年齢を記入してもらい、その後、知識レベルを問うために Android アプリケーションの中にはユーザ意図しないところで個人情報の漏えいがされているものがあることを尋ねた。

続いて、まず通知に気づいたことを尋ね、気づいたユーザには引き続き通知領域の確認を行ったかを尋ねた。さらに通知領域の確認を行ったユーザに対しては通知ドロワの確認有無を尋ねた。

またユーザのユーザビリティ低下に対する意識を問うために「音による通知はプレイ中の気をそらすか」「音が鳴っていても気にせずにゲームを続けられるか」を尋ねた。

### 5.4 実験の結果と考察

本実験は、14 人の被験者により行われた。14 人のうち男性は 7 人、女性は 7 人であった (表 1)。また被験者の年齢は、21〜23 歳であった。7 人 (男性 6 人、女性 1 人) が、一般的な通知インターフェイスで実験、7 人 (男性 1 人、女性 6 人) が提案手法搭載インターフェイスの実験を行った。

アンケートの「「Toss It」に限らず悪質な Android アプリが個人情報を流出している事をしっていましたか」に、「はい」と答えた被験者は、3 人 (一般的な通知 1 人、提案手法 1 搭載通知 2 人)。「いいえ」と答えた被験者は、11 人 (一般的な通知 6 人、提案手法 1 搭載通知 5 人) である。この結果から両インターフェイスの実験被験者に事前知識に偏りがないことが伺える。

問「情報漏洩リアルタイム通知に気づきましたか」に、「はい」と答えた被験者は、5 人 (一般的な通知 1 人、提案手法搭載通知 4 人)。「いいえ」と答えた被験者は、9 人 (一般的な通知 6 人、提案手法 1 搭載通知 3 人) である。この結果は提案手法 1 が有効であることを示唆する。一般的な通知と提案手法 1 の通知で通知に気づいた人数に差が生じたのは、今回の提案手法である、音と Toast の効果によると考えられる。ただし、音と Toast のどちらがより強い効果を生じさせたかについては、今回のアンケートでは判断がつかないものであった。

続く問「漏洩通知がされた時に画面上部通知領域を確認

しましたか (前問の回答がはいの人だけ確認)」に、「はい」と答えた被験者は、4 人 (一般的な通知 1 人、提案手法搭載通知 3 人)。「いいえ」と答えた被験者は、1 人 (一般的な通知 0 人、提案手法搭載通知 1 人) である。人数が少ないため、端的にデータを見ると、一般的な通知で通知領域を確認した被験者は 1 人中 1 人であり、対象者が 1 人であるため、傾向はつかめない。提案手法搭載通知は、4 人中 3 人が通知領域を確認している。この結果は、音と Toast の効果と考えることができ、音と Toast が通知領域に目を向かせる効果がある可能性があると言えよう。

問「通知ドロワーを確認しましたか (前問の回答がはいの人だけに確認)」に、「はい」と答えた被験者は、2 人 (一般的な通知 0 人、提案手法 1 搭載通知 2 人)。「いいえ」と答えた被験者は、2 人 (一般的な通知 1 人、提案手法 1 搭載通知 1 人) である。一般的な通知で通知ドロワーを確認した被験者は 1 人中 0 人であり、対象者が 1 人であるため、こちらも傾向はつかめない。提案手法 1 搭載通知は、3 人中 2 人が通知ドロワーを確認しているが、こちらも対象者が少ないため、傾向はつかめない。この結果から、通知領域の確認を行う原因として、「通知領域を確認をした場合は常に通知ドロワーを確認する」「提案手法により強く促された」「一般的な通知方式が強く促す効果がある」という 3 つの可能性が考えられるが、この結果からはそのいずれも支持・棄却ともにできない。

問「音による通知はプレイ中の気をそらす」に、「非常にそう思う」と答えた被験者は、8 人 (一般的な通知 3 人、提案手法 1 搭載通知 5 人)。「ややそう思う」と答えた被験者は、3 人 (一般的な通知 2 人、提案手法 1 搭載通知 1 人)。「どちらでもない」と答えた被験者は、1 人 (一般的な通知 0 人、提案手法 1 搭載通知 1 人)。「ややそう思わない」と答えた被験者は、1 人 (一般的な通知 1 人、提案手法 1 搭載通知 0 人)。「そう思わない」と答えた被験者は、1 人 (一般的な通知 1 人、提案手法 1 搭載通知 0 人) である。この結果からは、音による通知は有効であると考えられるが、ゲームという利用者の本来の目的を阻害している可能性を示唆している。さらに、ユーザビリティとしては低下しており、リスク通知の有効性と一般アプリケーションのユーザビリティのトレードオフの可能性を示唆している。

問「音が鳴っていても気にせずゲームを続けられる」に、「非常にそう思う」と答えた被験者は、7 人 (一般的な通知 2 人、提案手法 1 搭載通知 5 人)。「ややそう思う」と答えた被験者は、4 人 (一般的な通知 3 人、提案手法 1 搭載通知 1 人)。「どちらでもない」と答えた被験者は、1 人 (一般的な通知 0 人、提案手法 1 搭載通知 1 人)。「ややそう思わない」と答えた被験者は、0 人 (一般的な通知 0 人、提案手法 1 搭載通知 0 人)。「そう思わない」と答えた被験者は、2 人 (一般的な通知 2 人、提案手法 1 搭載通知 0 人) である。この結果からも、ゲームという利用者の本来の目的を阻害している可能性を示唆している。

## 6. さいごに

本論文では、Balebako らの提案した「Privacy Leaks」の JIT 通知の改良を行い、より効果的な通知として、Android のユーザー通知システムの Notification と Toast の利用による通知インターフェイスの実装を行った。さらにユーザ属性に応じた通知として SUN（Shimura Ushiro Notification）を提案した。

実装したインターフェースの評価を得るために、ユーザー実験を行った。その結果、一般的なインターフェースで、漏洩通知を認知した被験者が 7 人中 1 人なのに対し、提案手法の通知は、7 人中 4 人の被験者が漏えい通知を認知した。提案手法の音と Toast による通知が有効的であったと言える。

今後の課題は、実験被験者数を増やし統計的検定を行うこと、音と Toast ではどちらが通知として強い結果が得られるのか研究すること、さらに強い通知手法を考えることが挙げられる。

### 参考文献

[1] P. Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, D. Wetherall, "A conundrum of permissions: Installing applications on an android smartphone", In Proc. of USEC 2012, 2012

[2] A. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, D. Wagner, "Android permissions: User attention, comprehension, and behavior", In Proc. of SOUPS 2013, 2012.

[3] R. Balebako, J. Jung, W. Lu, L. Cranor, C. Nguyen, ""Little Brothers Watching You:" Raising Awareness of Data Leaks on Smartphones", In Proc. SOUPS 2013, 2013

[4] L. Cranor, P. Guduru, and M. Arjula, "User interfaces for privacy agents", TOCHI, 13(2):135-178, 2006

[5] S. Consolvo, J. Jung, B. Greenstein, P. Powledge, G. Maganis, D. Avrahami, "The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on wi-fi", In Proc. of Ubicomp, 2010.

[6] J. Lin, S. Amini, J. Hong, N. Sadeh, J. Lindqvist, J. Zhang, "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing", In Proc. of UbiComp, 2012.

[7] S. Egelman, E. Peer, "Towards Optimal Risk Mitigation Through Individualization", Workshop on Risk Perception in IT Security and Privacy, 2013