「マルチメディア，分散，協調とモバイル
(DICOMO2019)シンポジウム」 令和元年7月

スマートフォンアプリにおける要求権限の可視化の提案

金杉洋[1] 松原剛[2] 柴崎亮介[1]

概要：個人が日常的に携行するスマートフォンを介して取得される様々なパーソナルデータは，有用な機能やサービスの提供に不可欠である一方で，プライバシーに関わる機微情報も含まれているため，アプリの利用に先立ってパーソナルデータの利用について利用者から明示的に同意を得ることが不可欠となっている．しかし，アプリ提供者が使用するパーソナルデータの種類と目的を示し同意取得を求める反面，アプリを利用する利用者は必ずしもそれを注意深く確認しておらず，自分自身がアプリに対しどの程度までパーソナルデータの利用を許可しているか把握しきれていない．本論文では，Android アプリのパーミッション管理に関わる機能に着目し，利用者の端末にインストールされたアプリのパーミッション情報を要約して示すアプリを試作し，利用者のアプリの機能要求への同意意識を測るツールとすることを目指す.

Proposal on Visualization of Permission Requests by Smartphone Apps

HIROSHI KANASUGI[1] GO MATSUBARA[2] RYOSUKE SHIBASAKI[1]

1. 背景

個人情報やパーソナルデータは，様々なサービスや有用な機能の提供に不可欠となっていおり，特に個人が日常的に携行するスマートフォンからは，アプリを介して多様なパーソナルデータが生成・取得されている．パーソナルデータは個人情報やプライバシーに関わる機微情報となるため，利用に際して個人への通知と同意の取得が必要とされている．日本では個人情報保護委員会が示す個人情報保護法のガイドライン[1]や，2018 年 5 月に正式に施行された EU 一般データ保護司令（GDPR: General Data Protection Regulation）[2]においても，パーソナルデータの取得には利用者からの同意取得が必要としている．そのため，通常，サービスの提供者は，利用規約・プライバシポリシーを提示し，その内容への同意を取得している．しかし，多数のサービスやアプリによって繰り返される同意取得の手続きは，多くの専門用語を含む利用規約・プライバシポリシーの読解の困難さ及びその分量から，利用者への負担が大きい．その結果，多くの利用者は内容を十分に把握しきれないまま提示される規約・プライバシーポリシーに同意し，実態として，利用者はサービス提供者がどんなパーソナルデータをどの程度まで収集・利用しているか把握できていない.

こうした状況に対し，岩本らは各サービスの利用規約からサービス内で利用されるパーソナルデータの項目と利用目的を抽出し，それらを対応付けて可視化すると共に，自身のパーソナルデータの利活用状況の定量化を試みている[3]．また，Android OS では従来包括同意となっていたアプリからのパーミッション要求を，個々の機能実行時に同意取得する機能(runtime permission)を導入している[4]．しかし，同意取得への柔軟性が増した反面，個別のアプリから要求されるパーミッションの一覧は，アプリの個別設定や Google Play ストアで個別に確認することになり，利用者の手間はあまり変わっていない．その一方で，Sebastian. Z らは Android アプリのパーミッション要求やライブラリの利用状況等の解析と，アプリ提供者の提示するプライバシポリシーの自然言語解析結果を組み合わせることで，プライバシー要件に対するアプリの適合状況を推測・提示する仕組みを提案している[5]. Play ストアで公開されているアプリを対象としているため，デバイスにプリインストールされたメーカ独自のアプリが含まれないことや，日本語を含む他言語の利用規約・プライバシポリシーの自然言語解析への対応が改善されれば，提供者と利用者の双方に有用な仕組みとなろう．また，十分な精度が得られるとは限らないプライバシポリシーの自然言語解析によらず，プライバシポリシーから，利用者の許容できる条件をデータ化することで，サービス提供者と利用者の間のポリシーのマッチングを図る仕組みとして PPM（Privacy Policy Manager）も検討されている[6].

以上の既往研究や活動のように，サービスやアプリの利用に際して，パーソナルデータの取得・利用に関わるサービス提供者と利用者との相互理解の溝や齟齬を埋める試みが行われてきている．サービス提供に必要なパーソナルデ

1 東京大学 空間情報科学研究センター
Center for Spatial Information Science, the University of Tokyo

2 東京大学 地球観測データ統融合連携研究機構
Earth Observation Data Integration & Fusion Research Initiative, the University of Tokyo

ータと技術的要件に，個人情報保護とプライバシ保護の要件を加えて明文化した上で，利用者の理解と同意を得る構造は，異なったそれぞれの側面からの要求を整理する複雑な課題となっている．サービス提供者が利用規約・プライバシポリシーを分かりやすく示すことも重要なのと同時に，利用者自身の理解を強化することも喫緊の課題と言えよう．

そこで本論文では特に Android アプリに着目し，個別の端末にインストールされたアプリが．どの程度プライシーリスクのある機能を要求し利用しているかの可視化を試みる．具体的には，個々の Android アプリに含まれる manifest 情報から，アプリの要求するパーミッションを抽出し，特に留意が必要なパーミッション（Dangerous Permission）がどの程度含まれているかを簡易的に可視化する．アプリに対する利用者の同意の認識と実態との乖離度合いを測るツールとなることを目指す．

2. Android アプリのパーミッション

Android アプリでは，インターネットアクセスや位置情報の取得等，端末の機能の利用には各機能に該当するパーミッションを利用者に要求し，同意を得る仕組みになっている．特に，利用者の個人情報を含むリソースにアクセスする場合や，利用者の保存したデータや他のアプリに影響を及ぼす可能性がある場合には，Dangerous Permission が割り当てられており，その機能の利用に際して利用者から明示的に許諾を得る仕組みになっている（Runtime Permission）[4]．Android SDK version 28 時点では，26 種類の Dangerous Permission とそれをまとめる 10 種類の Permission Group が定義されている（Table 1）．ただし，端末にプリインストールされたシステムアプリ等，デバイスメーカ等が独自に拡張定義した Permission Group も存在するため，メーカや機種によっては Table 1 よりも種類が多い可能性があることを留意されたい．また，パーミッションも同様にアプリ毎に独自に拡張して定義が可能であるため Table 1 の限りではない．また，インターネットアクセス等の Permission Group に属さないパーミッションは，その他の権限に分類される．

各アプリから要求されるパーミッションは，Dangerous Permission に該当するか否かによらず，アプリのメタデータを含む manifest.xml に記述され，Google Play ストア (Figure 1)や端末のアプリ情報から確認できる他，他のアプリからも SDK を介して参照可能である．本論文では，端末にインストール済みのアプリから，SDK を介してパーミッション情報を抽出する．

3. パーミッション可視化アプリの試作

端末にプリインストールされたシステムアプリを含め，インストールされた全アプリてについて，前述の Permission Group に該当するパーミッションが要求されて

Table 1. Permission Group と Dangerous Permission (Android SDK version 28)

Permission Group	Dangerous Permission
CALENDAR	READ_CALENDAR
	WRITE_CALENDAR
CALL_LOG	READ_CALL_LOG
	WRITE_CALL_LOG
	PROCESS_OUTGOING_CALLS
CAMERA	CAMERA
CONTACTS	READ_CONTACTS
	WRITE_CONTACTS
	GET_ACCOUNTS
LOCATION	ACCESS_FINE_LOCATION
	ACCESS_CORSE_LOCATION
MICROPHONE	RECORD_AUDIO
PHONE	READ_PHONE_STATE
	READ_PHONE_NUMBERS
	CALL_PHONE
	ANSWER_PHONE_CALLS
	ADD_VOICEMAIL
	USE_SIP
SENSORS	BODY_SENSORS
SMS	SEND_SMS
	RECEIVE_SMS
	READ_SMS
	RECEIVE_WAP_PUSH
	RECEIVE_MMS
STORAGE	READ_EXTERNAL_STORAGE
	WRITE_EXTERNAL_STORAGE

Figure 1. Google Play ストアの Facebook アプリの権限表示

いる状況を可視化するアプリ PermissionViewer[7]を試作した（Figure 2, Figure 3）．ただし，Permission Group には該当しないが，プライバシーを考慮する上で重要な項目として，インターネットへのアクセス要求の有無を明示的に追加して示している．

PermissionViewer はサマリビューとリストビューの 2 種類のビューで構成される．サマリビューでは，Permission Group（独自拡張がある場合は全て）とインターネットアクセスのそれぞれについて，パーミッションを要求しているアプリ数をインストールされたアプリ総数の割合として単純に正規化し，レーダーチャートで示す構成としている．Figure 3 には Samsung Galaxy S8(Android version 9) でシステムアプリを含めた全アプリを含めた場合の画面を示した．Figure 3 左の通り，SDK で定義された Permission Group に加えて，「モバイル端末の管理」が独自拡張として追加されていることがわかる．

他方のリストビューでは，個別アプリがどの Permission Group を要求しているかをアイコンの濃淡で示し，要求するパーミッションの数と合わせて一覧表示する形式とした．各アイコンと Permission Group の対応関係は，Figure 4 に示した通りであり，インターネットアクセスと独自拡張分を除き，全て Android OS の標準アイコンを使用している．また，上部のフィルタ設定で，要求している Permission Group 単位での絞り込みを行う．加えて，個々のアプリのリスト項目をタップすることで，対象アプリの詳細設定画面が開くため，アプリのより詳細な情報の確認や設定変更へ繋がる仕組みとしている．

なお，サマリビューとリストビューのどちらについても，メニューからシステムアプリを表示に含めるかどうかを切替を可能とした．

4. 考察

Figure 2 は筆者の端末にインストールされたアプリのうち，システムアプリを除いた状態でのパーミッション要求の状況を示している．Permission Group に含まれないインターネットアクセスが 95.7%（22/23）のアプリから要求されており最も割合が高く，内部ストレージへのアクセスが 87.0% (20/23)と次に高い．一見インターネットアクセスを必要としないと思われるアプリでも，広告や内部データの更新有無の確認でパーミッションを要求していることがある．同様に，他のパーミッションの要求についても，アプリの利用に必要不可欠か否かの判断は，一般の利用者には難しい．更に，位置情報とインターネットアクセスの組み合わせ等，複数のパーミッション要求の組み合わせになると，Permission Group の可視化のみでは，その利用目的を判断することが難しく，最終的にアプリのプライバシポリシーや，アプリを提供するサービスの利用規約を読み判断する必要がある．本論文の PermissionViewer ではプライバシ

Figure 2. アプリパーミッションの可視化（システムアプリなし）
左：サマリビュー（全アプリでのパーミッション要求概要），
右：リストビュー（個別アプリでのパーミッション要求状況）

Figure 3. アプリパーミッションの可視化(システムアプリ含む)
左：サマリビュー（全アプリでのパーミッション要求概要），
右：リストビュー（個別アプリでのパーミッション要求状況）

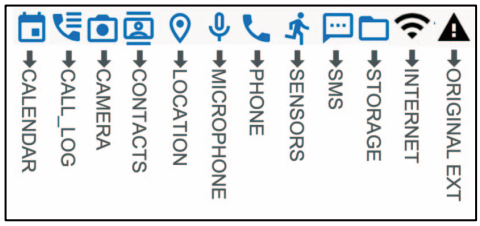

Figure 4. リストビューのアイコンと Permission Group の対応関係

ポリシーと対応付ける機能までは実現できていないが，S. Zimmeck ら[5]と同様に，プライバシポリシーの自然言語解析結果と連携し，アプリのパーミッション要求との対比が今後必要になろう．

また, Permission Group に該当しないパーミッションとして，今回はインターネットアクセスをオプションとして含めたが，ヘルスケア分野等でウェアラブルデバイスと連携しての利用が進む最近の状況を踏まえると，Bluetooth 等の外部機器との通信に関するパーミッション要求についても含めていく必要があろう．

5. まとめと展望

本論文では，Android アプリに着目し，個別の端末にインストールされたアプリがどの程度プライシーリスクのある機能を利用しているかの可視化を試みた. 具体的には, 個々の Android アプリに含まれる manifest 情報から，アプリの要求するパーミッションを抽出し，そこに Dangerous Permission がどの程度含まれているかを簡易的に可視化するアプリを試作した．

今後は，アプリに関わるプライバシポリシーや利用規約との紐づけにより，アプリから要求されるパーミッションとその利用目的との対応を明確化していく．また，ウェアラブルデバイス等，スマートフォンに付随した機器の利用も増加していることから，連携機器との通信に関わるパーミッションについても可視化の項目に追加していきたい．

参考文献

[1] 個人情報保護委員会, 個人情報の保護に関する法律についてのガイドライン（通則編）, https://www.ppc.go.jp/files/pdf/guidelines01.pdf, 最終アクセス 2019.05.06

[2] EU General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, 最終アクセス 2019.05.06

[3] 岩本佑太, 山内正人, 砂原秀樹, パーソナル情報可視化システムの提案, マルチメディア・分散・協調とモバイルシンポジウム(DICOMO2015), pp.1870-1871, 2015.07.

[4] Android Developers, Permissions overview, https://developer.android.com/guide/topics/permissions/overview, 最終アクセス 2019.05.05

[5] S. Zimmeck, Z. Wang, L. Zou, R. Iyengar, B. Liu, F. Schaub, S. Wilson, N. Sadeh, S.M. Bellovin, J.R. Reidenberg, "Automated Analysis of Privacy Requirements for Mobile Apps", NDSS'17: Network and Distributed System Security Symposium, 2017.02

[6] Shinsaku Kiyomoto, Toru Nakamura, Haruo Takasaki, Ryu Watanabe, and Yutaka Miyake, PPM: Privacy Policy Manager for Personalized Services, Security Engineering and Intelligence Informatics, CD-ARES 2013. Lecture Notes in Computer Science, vol.8128. pp.377-392, 2013

[7] PermissionViewer, https://play.google.com/store/apps/details?id=jp.ac.utokyo.shibalab.permissionviewer, 最終アクセス 2018.05.06