Voice Assistant アプリの大規模実態調査

刀塚 敦子[1,a)]　飯島 涼[1,2]　渡邉 卓弥[1,3]　秋山 満昭[3]　酒井 哲也[1]　森 達哉[1,2,4]

概要：Voice Assistant の代表的な実装例である Google Assistant では，Action と呼ばれる，公式もしくはサードパーティ製の Voice Assistant アプリ (以下 VA アプリ) が提供されている．VA アプリはスマートフォンにおけるアプリとは異なり，端末へのインストールを必要としない．VA アプリはクラウド上で動作するため，その挙動の大部分はユーザーに対する透明性に欠けている．Voice Assistant の代表的な実装例である AI スピーカの普及が進む中，VA アプリの挙動が持つ不透明性は，意図せぬプライバシー情報の漏洩につながるリスクがある．本研究では Google Assistant を対象に，サードパーティによって開発された日本語版 VA アプリの大規模実態調査を行う．事前調査として VA アプリのメタデータを収集し，アプリの基礎統計を調査する．また，音声コマンドによって VA アプリとの対話を行い，その内容に応じてどのような手法でユーザーをトラッキングしているかを網羅的に調査する．調査の結果，42%の VA アプリが何らかの方法でユーザーをトラッキングしていること，及びプライバシーリスクの懸念がある方法でトラッキングを実施している VA アプリの存在を明らかにした．本論文ではトラッキングを行う VA アプリの特徴を示すとともに，VA アプリの理想的なトラッキング方法について議論する．

キーワード：Voice Assistant，クラウドアプリ，トラッキング

A Large-scale Investigation of Voice Assistant Apps

Atsuko Natatsuka[1,a)]　Ryo Iijima[1,2]　Takuya Watanabe[1,3]　Mitsuaki Akiyama[3]　Tetsuya Sakai[1]
Tatsuya Mori[1,2,4]

Abstract: In Google Assistant, which is a typical example of Voice Assistant systems, functions are provided by official or third-party Voice Assistant applications (VA apps). Unlike mobile app, a VA app is not installed on a device and works as a cloud service. Therefore, behaviors of VA app are not transparent to users. As the AI speakers are increasingly becoming popular, the lack of transparency could lead to the unintentional privacy risks. In this research, we conduct a large-scale investigation of Japanese version third-party VA apps, targeting Google Assistant. As a pre-survey, we conduct metadata survey of VA apps and take statistics. We call VA apps by voice commands acquired from the statistics and investigate how they get information. As a result, we found that 42% of VA apps perform user tracking and there are several VA apps that track users in a way with the concerns of privacy risks. Finally, we demonstrate the characteristics of VA apps with user tracking and discuss the ideal user tracking for VA apps.

1. はじめに

Voice Assistant とは，音声コマンドにより様々なタスクやサービスを実行するシステムである．Voice Assistant とユーザーの対話は Voice Assistant アプリ (以下，VA アプリ) によって成り立っている．ユーザーの音声リクエストに対し，適切な VA アプリが Voice Assistant を通じて呼び出され，リクエストに答える．例えば「今日の天気」という音声リクエストに対して VA アプリが呼び出され，リクエストを受けた日の天気，気温及び降水確率などをレスポンスとして，ユーザーに返す．このような天気を答える

[1] 早稲田大学 (Waseda University)
[2] 情報通信研究機構 (National Institute of Information and Communications Technology)
[3] NTT セキュアプラットフォーム研究所 (NTT Secure Platform Laboratories)
[4] 理研 AIP (RIKEN AIP)
[a)] natatsuka@nsl.cs.waseda.ac.jp

© 2019 Information Processing Society of Japan

シンプルなものから，あたかも人間と対話しているかのような複雑な会話が可能なものまで幅広い VA アプリが存在している．Google Assistant や Amazon Alexa などの代表的な Voice Assistant プラットフォームでは，ユーザーの要求に答える多種多様な VA アプリが，公式もしくはサードパーティによって開発されている．今日，家庭あるいは企業で利用される Voice Assistant として最も普及した端末である AI スピーカでも VA アプリが利用可能である．

VA アプリの特徴は，Android や iOS のようなモバイルプラットフォームを対象としたアプリとは異なり，クラウド上で動作するため，端末へのインストールを行わない点にある．VA アプリの開発者は，公式もしくは自分が用意したサーバー上で VA アプリのプログラムをデプロイする．VA アプリのプログラムがどのような動作をするのかは，開発者に委ねられている．ここで問題となるのは，VA アプリの挙動はユーザーに対して不透明な点である．すなわち，VA アプリがユーザーとの対話を通じて得た情報の利用方法は，ユーザーが直接アクセスすることができないクラウド上で動作するプログラムによって決定され，どこに情報が保存され，またどのように情報が利用されるかに関して，ユーザーが陽に知る手立てが用意されていない．実際，Abdi らが実施したユーザースタディ [1] では，Voice Assistant に対するユーザーのセキュリティとプライバシーの認識は不完全であり，サードパーティの存在を意識していないユーザーが多いことを明らかにしている．

本研究では，以上で示した VA アプリのプライバシーリスクを背景として，VA アプリの大規模調査を行う．Voice Assistant の実装例の一つである Google Assistant を対象とし，提供されているサードパーティ製の日本語版 VA アプリの収集, 解析を実施する．本研究の Research Question (**RQ**) は以下の通りである．

RQ1: ユーザーをトラッキングする VA アプリはどの程度存在し，どのようにトラッキングしているのか．
RQ2: ユーザーとの対話を通じて個人情報を取得する VA アプリはどの程度存在し，どのような情報を取得しているのか．
RQ3: ユーザーをトラッキングしている VA アプリに共通する性質はどのようなものか．

本研究の技術的チャレンジは，クラウド上で動作する VA アプリの挙動を解析する点にある．これまでに多数の実績があるモバイルアプリの解析と，本研究が対象とする VA アプリの解析が大きく異なるのは，VA アプリは端末上で動作しないため，静的解析や動的解析といった従来のアプリ解析手法を用いることができない点である．VA アプリの動作を解析するためには，クラウド上で動作するアプリと自然言語で構成される音声コマンドを用いた「対話」をし，入力した音声コマンドとアプリが出力したレスポンスを解析する「ブラックボックス」的アプローチを採用する必要がある．

上述の目的を実現するために，本研究でははじめに Assistant directory [3] に接続し，収集可能な全ての VA アプリのメタデータを収集する (2019/7/7 時点で 940 個)．取得したメタ情報から VA アプリの統計情報を解析するとともに，今回調査対象としたサードパーティ製の VA アプリ 782 個に対し，それぞれを起動するための音声コマンドを抽出する．

次に抽出した VA アプリの音声コマンドを使用し, Google Assistant で VA アプリの呼び出しを行う．VA アプリの呼び出し後に VA アプリのレスポンスを取得し，次のリクエストは行わずに VA アプリから退出する．対話の終了後，Assistant directory のアプリページに接続し， 2 章で説明する UserStorage [2] に保存されているデータを取得する．VA アプリの呼び出しから UserStorage データを取得するまでの処理は，各アプリに対して 2 回ずつ行う．2 回行って得られた VA アプリのレスポンス及び UserStorage データを用い，VA アプリがユーザーをトラッキングする方法，並びに収集している個人情報を判定・分類する (3 章)．最後に上記の分類結果をもとに，ユーザーをトラッキングする VA アプリのカテゴリーやトラッキングが必要となる正当な理由を調査する．

本研究の貢献は以下の通りである．

- VA アプリの大規模調査を実施した初の研究である．VA アプリの基礎的な統計を明らかにした．
- VA アプリが使用しているトラッキング技術を分類するフレームワークを開発した．調査対象となった VA アプリの半数以上が何らかの方法でユーザーをトラッキングしていること，及びそれらの大多数がユーザーに対する承認要求が不要な UserStorage を用いている事を明らかにした．
- VA アプリがユーザーとの対話を通じて取得する個人情報を分類・集計し，取得された個人情報はユーザーが認識していない範囲で外部サーバーに保存，二次利用されている可能性を示した．
- ユーザートラッキングを行う VA アプリが持つ共通的な性質を示し，VA アプリとして望ましいユーザートラッキングの方法を提言した．

2. 背景

本章では Google Assistant を対象とし，VA アプリの基本的な動作，及び VA アプリが利用可能なユーザートラッキング手法を示す．

2.1 VA アプリの基本的な動作

ユーザーが Voice Assistant クライアント端末に対して音声コマンド入力してから，音声によるレスポンスを得るま

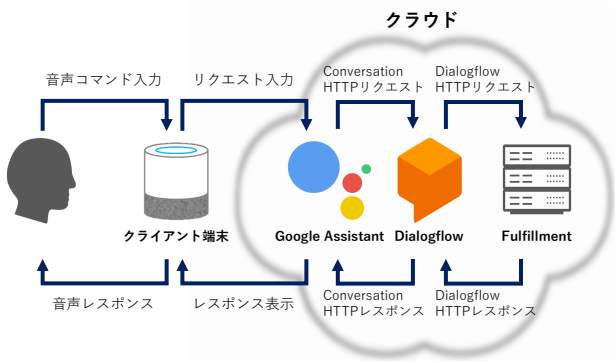


図 1　VA アプリの基本動作

でに関わるサービスは，Google Assistant，Dialogflow [2]，Fulfillment である．図 1 に上記のサービスを使用した VA アプリの概要を示す [2]．Google Assistant は VA アプリのインターフェースであり，音声による入力リクエストを音声認識システムにより自然言語に変換し，ユーザーの情報，使用端末情報など付加した Conversation HTTP リクエストを Dialogflow に送信する．Dialogflow は自然言語処理ツールであり，受信したリクエストテキストから VA アプリの起動，処理に必要な単語を抽出し，それらを Dialogflow HTTP リクエストに含んで Fulfillment に送信する．Fulfillment はクラウド上にある VA アプリの本体であり，受信した抽出単語からユーザーに表示するレスポンスを作成し Dialogflow に送信する．作成されたレスポンスは Dialogflow と Google Assistant，クライアント端末を通じてユーザーに返される．

ここで注意するべきことは，Google Assistant と Dialogflow は Google が提供するプラットフォームで動作するのに対し，Fulfillment は必ずしも Google が提供するプラットフォーム (Firebase) で動作するとは限らないことである．すなわち VA アプリはサードパーティが用意したサーバー上で動作する場合があり，そのようなケースにおいては，VA アプリの挙動を完全に理解することは開発者にしかできない．また，ユーザーの視点からは自身とクライアント端末間の対話がすべてであり，クラウド上でどのようなデータがどのように送受信されているかを把握することは困難である．

2.2　トラッキング手法

Actions on Google では，VA アプリを利用したユーザーのトラッキングを可能とするいくつかのメカニズムが用意されている．それらの概要を表 1 にまとめた．以下ではそれぞれのメカニズムの詳細を示す．

OAuth

Google が提供する Account linking には OAuth [2] によるユーザー認証機構が含まれる．Account linking では標準の OAuth 2.0 の認証フローをサポートしており，implicit コードフロー及び authentication コードフローと呼ばれる二つの認証フローが存在する．どちらもアクセストークンを記録しておくことにより，ユーザーをトラッキングすることが可能である．

表 1　トラッキング手法

手法	ユーザーへの事前承認要求
OAuth (account linking)	あり
Google Sign-In (account linking)	あり
Helpers インテント	あり
UserStorage	なし
userId (2019/7/29 廃止)	なし
lastSeen	なし

Google Sign-In

Google Sign-In [2] は Account linking の一つの手法である．この手法では，Google アカウント以外に他のサービスのアカウントは不要である．Google Sign-In の承認要求をユーザーが許可した場合，Google Assistant は VA アプリへ送信する Conversation HTTP リクエストに Google アカウントのユニーク ID，名前，メールアドレス，プロフィール写真を付加する．すなわちこのユニーク ID を記録しておくことでユーザーをトラッキングすることができる．

Helpers インテント

Helpers インテント [2] とは，Google によって予め定められているメッセージオブジェクトのことである．Helpers インテントによって取得できる情報には，ユーザーの名前，使用端末の現在地，住所などが含まれる．Helpers インテントの承認要求をユーザーが許可した場合，Google Assistant は VA アプリへ送信する Conversation HTTP リクエストに上記の情報を付加する．すなわちこの情報を記録しておくことでユーザーをトラッキングすることができる．

UserStorage

UserStorage とは，Google Assistant が VA アプリへ送信する Conversation HTTP リクエストに含まれている要素であり，ユーザーと VA アプリとの間で保持される固有のストレージである．VA アプリはクライアントライブラリ [2] を使用することで，いかなるデータも保存することが可能である．この手法を使用した場合，VA アプリはユーザーの明示的な承認を得る必要がないため，VA アプリが使用の同意を取らない限りユーザーは UserStorage に情報が保存されていることに気づくことが難しい[*1]．

userId

Conversation HTTP リクエストには，userId [2] というユーザー毎の ID が記述される．userId の利用にあたり，ユーザーに対する承認が不要であるため，ユーザーは userId によってトラッキングされる場合，そのことに気がつくことはできない．userId は 2019/7/29 をもって廃止

[*1] ユーザーは PC のブラウザ経由で Assistant directory にアクセスすることによって，UserStorage データの中身を確認できるが，その事実は一般的にはあまり知られていないと考えられる．

されたが，それ以前は userId を記録しておくことでユーザーをトラッキングすることが可能であった．Google は userId 廃止後の移行方法として，Account linking を使用する，もしくは UserStorage に VA アプリの Fulfillment で生成した値を保存することを推奨している．本調査を行った期間は userId の廃止直前であったため，調査対象の VA アプリには userId を 使用している可能性があるものが含まれていると考えられる．

lastSeen

Conversation HTTP リクエストに含まれる lastSeen 要素 [2] は，VA アプリに送信する初回のリクエストでは省略され，2 回目以降のリクエスト時に前回のリクエスト時間がタイムスタンプ形式で付加される．したがって，この要素の有無によりユーザーの呼び出し回数が 1 回目であるか，あるいは 2 回目以降であるかを見分けることができる．

3. メタデータ収集・分類方法

本章ではメタデータ収集方法及び VA アプリの分類方法を示す．

3.1 メタデータ収集

Assistant directory から，メタデータ収集を行う．Assistant directory は Google が提供する Web サイトであり全ての VA アプリの詳細が記されている．ディレクトリには全ての VA アプリに紐付けられたアプリページが配置されている．アプリページには VA アプリ名，開発者名，説明，音声コマンド，カテゴリー，対応端末，平均評価，レビュー，プライバシーポリシー，UserStorage データが記されている．アプリページからメタデータを収集するために，クローリングを行う．クローリングは 2019/4/28 から 2019/7/21 にかけて実施した．手順は，アプリページを開き，記されている VA アプリの全ての情報を取得するというものである．クローリング終了後は，収集した VA アプリのデータから，VA アプリの総数，並びに開発者毎，カテゴリー毎の VA アプリの統計をとる．以降に示す全てのデータは 2019/7/7 時点のものである．

3.2 VA アプリの呼び出し

3.2.1 呼び出し手順

3.1 節で得られたデータから VA アプリの音声コマンドを抽出しリストにする．このとき開発者が Google であるもの，カテゴリーがスマートホームであるもの，メッセージアプリを呼び出すものを除く．研究対象がサードパーティ製の VA アプリであるため Google のものは除外するとして，それ以外の VA アプリはスマートホームデバイスがないと使えない，メッセージアプリを呼び出す以外の機能を持たないため除外している．その結果，音声コマンドを抽出した VA アプリ数は 782 個であった．それらの VA アプリの呼び出しを Google Assistant SDK [5] と Android タブレットにおいて音声コマンドを自動入力することにより行う．VA アプリを呼び出しレスポンスを取得した後は，リクエストを送信せずに VA アプリから退出する．その理由は，呼び出された後の VA アプリに対するリクエストは VA アプリによって多種多様であり，リクエストの自動入力が困難であるからである．全ての VA アプリの呼び出し終了後は，アプリページから UserStorage データを取得する．呼び出し手順は 2 回実施する．

3.2.2 Google Assistant SDK

Google Assistant SDK とは，自分の端末に Google Assistant を埋め込み，その機能を拡張することができるツールセットのことであり，Google Assistant Service と Google Assistant Library という 2 種類の SDK が提供されている．Google Assistant Service は gRPC に対応している全てのプラットフォームで利用可能であり，本研究の使用プラットフォームは Windows 10 であることから，Google Assistant Service を利用する．Google Assistant Service で呼び出せなかった VA アプリは，次項で示す Android タブレットにインストールした Google Assistant から呼び出しを行う．

3.2.3 Android Debug Bridge

Android タブレットにインストールした Google Assistant に音声コマンドを自動入力するために，Android Debug Bridge [4] (以下 adb) を利用する．adb は PC と USB 接続された Android 端末と通信するためのコマンドラインツールであり，PC から Android 端末への文字入力を行うことができるが，マルチバイト文字を入力できないため，ADBKeyBoard [7] を併用して入力する．ADBKeyBoard は GitHub で公開されている Android 用キーボードである．これらを利用し PC から日本語版 VA アプリの音声コマンドを自動入力する．VA アプリが呼び出されたら adb によりスクリーンショットを撮影し，PC に取り込む．Tesseract OCR [8] によってスクリーンショットを解析し，VA アプリのレスポンスを文字で読み取る．

3.3 VA アプリの分類

VA アプリをユーザートラッキング種別に応じて分類するフレームワークを図 2 に示す．最初に VA アプリのレスポンスを解析し，OAuth，Google Sign-In，Helpers インテントのうち，いずれかの承認要求をしているかを検証する．承認要求をしていた場合は，該当する承認要求を行うグループ，すなわち「**OAuth**」，「**Google Sign-In**」，「**Helpers インテント利用**」のいずれかに分類する．次に UserStorage データの有無を検証する．データが存在する場合は「**UserStorage 利用**」に分類する．データがない場合は 1 回目のレスポンスと 2 回目のレスポンスを比較し，VA アプリを呼び出した回数が 1 回目か 2 回目かでレスポンスを変えている場合は「**トラッキング手法不明**」に分類

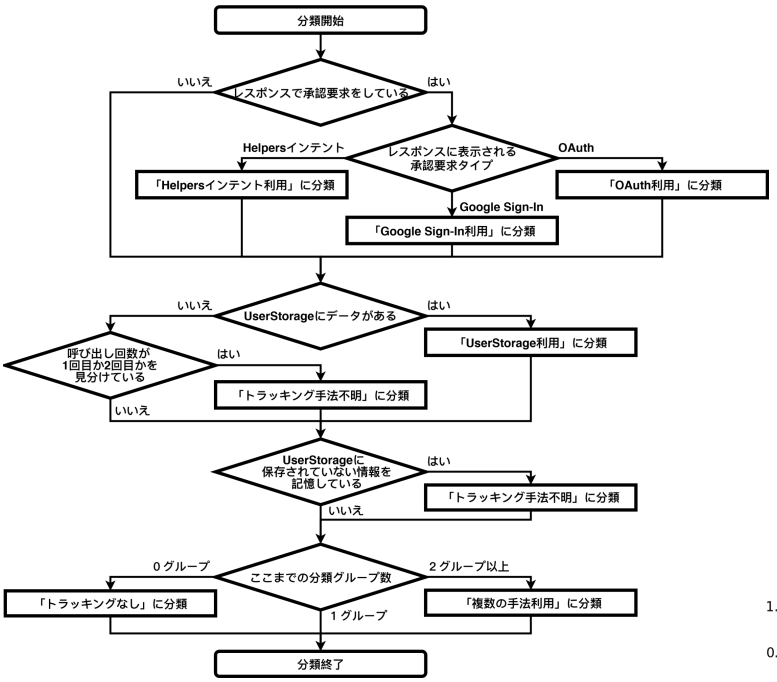


図 2 VA アプリ分類フローチャート

表 2 カテゴリー毎 VA アプリ数

順位	カテゴリー	個数
1	ゲーム＆娯楽	248
2	教養＆知識	118
3	スマートホーム	116
4	仕事効率化	77
5	音楽＆オーディオ	73
6	子供＆ファミリー	43
7	アート＆ライフスタイル	40
8	ニュース＆雑誌	33
9	ビジネス＆金融	31
9	フード＆ドリンク	31
9	健康＆フィットネス	31
12	ソーシャル＆コミュニケーション	22
13	地域	21
14	旅行＆交通機関	16
15	映画＆写真＆テレビ	11
16	ショッピング	10
16	天気	10
18	スポーツ	9

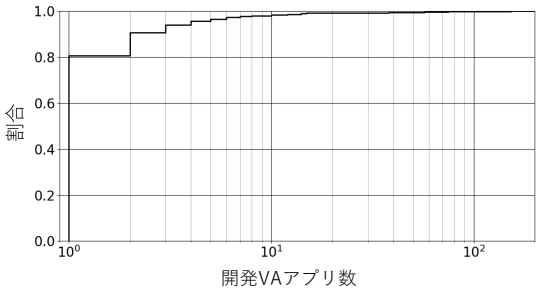


図 3 開発者毎 VA アプリ数の累積分布

する．その理由は userId や lastSeen，もしくは未知の手法を利用することで，VA アプリ呼び出し回数を数えている可能性があるためである．これら手法の内どれが使われたかは，クライアント側から区別することが原理的にできない．次に記録を保存する機能を提供する VA アプリについては，承認要求を許可しない上で記録の保存を試み，記録が UserStorage に保存されていないにもかかわらず参照することができた場合は「**トラッキング手法不明**」に分類する．その理由は，VA アプリが userId または未知の手法を利用して外部のデータベースを参照している可能性があるためである．最後にここまでの分類過程で，分類されたグループ数を検証する．どのグループにも属していない場合は「**トラッキングなし**」に分類し，2 グループ以上に属している場合は「**複数の手法利用**」に分類する．

上記の分類グループとは別に，VA アプリのレスポンスを参照して個人情報の取得を 2.2 節で示した手法を利用，またはユーザーとの対話で個人情報の入力を要求することにより試みている VA アプリを収集する．また収集した VA アプリが取得している個人情報及び取得方法も記録する．

4. VA アプリの分析結果

本章では VA アプリの分析結果を示す．

4.1 VA アプリの統計

はじめに 3.1 節で示したメタデータ収集で得られた VA アプリの統計を示す．VA アプリの総数は 940 個である．表 2 にカテゴリー毎の VA アプリ数を示す．VA アプリに娯楽的な機能が求められていること，もしくは開発者が作りたい VA アプリは娯楽的なものが多いことが推測される．

開発者の人数は 424 人である．図 3 に開発者が開発した VA アプリの累積分布を示す．約 9 割の開発者が 2 個以下の VA アプリを公開している一方，単独で 50 以上の VA アプリを公開した開発者もいる．表 3 に VA アプリの公開数が多い開発者 Top 10 を示す．アプリページに開発者名を記していない VA アプリが 153 個も存在していることが分かる．VA アプリ申請時の開発者名の入力はオプションであるため，入力しない場合アプリページに開発者名が記されないと推測する．また Google が開発している VA アプリの開発者名が統一されていなかった．公式名の表記が定まっていないことはユーザーの混乱を招き，説明やプライバシーポリシーに開発者名が記されていない場合，ユーザーが開発者の情報を見て，その信頼性を評価する手段が存在しないことにつながり，透明性の観点で問題があると考えられる．

4.2 VA アプリのトラッキング手法別分類

3.2 節で得られたデータから VA アプリのトラッキングの有無を判断した結果を表 4 に示す．16 個の VA アプリは呼び出されなかったため呼び出し不可に分類している．表 5 にトラッキングをしている VA アプリを 3.3 節で示したグループに分類した結果を示す．無記名及び Google Inc.

表 3　開発者毎の VA アプリ公開数 Top 10

順位	開発者名	個数
1	無記名	153
2	恵比寿ボイスプロダクション	75
3	Beyond, Inc.	57
4	Google Inc.	38
5	MEDIA KOBO, INC.	15
6	Healing.fm	14
7	tocie	12
8	VoiceApp Lab	10
8	がおまるラボ	10
10	@takatama_jp	8

表 4　トラッキングの有無による VA アプリ分類

分類	個数
トラッキングなし	371
トラッキングあり	395
呼び出し不可	16

表 5　VA アプリのトラッキング手法 ※割合は重複を含むため 100%を超える．

グループ	個数	割合
OAuth 利用	35	8.9%
Google Sign-In 利用	10	2.5%
Helpers インテント利用	10	2.5%
UserStorage 利用	310	78%
トラッキング手法不明	42	11%
複数の手法利用	12	3.0%

を除く表 3 に含まれる開発者の 8 割がトラッキング手法を使用していた．また調査した VA アプリの 5 割がいずれかのトラッキング手法を利用していることが判明した．特に UserStorage を利用している VA アプリが多く，これらはいずれも陽に UserStorage 使用の同意をユーザーに取っていなかった．すなわちユーザーからは不透明な状態でトラッキングが行われる状況にある．Account linking を利用している VA アプリについても，手法を利用する理由を示さずに承認要求をしている VA アプリが大部分を占めた．トラッキング手法が不明である VA アプリに関しても，ユーザーに対してトラッキングをしている事実に関する透明性が低いため，プライバシーリスクを引き起こす懸念がある．

4.3　トラッキングアプリが取得する情報

3.3 節で示した個人情報取得を行う VA アプリを収集した結果，89 個存在することが分かった．表 6 に取得されている個人情報毎の VA アプリ数を示す．生年月日等には生まれ月など，住所等には地区名などが含まれている．表 6 に示した個人情報は一度 VA アプリに取得されると，開発者が消去機能を提供していない限りユーザーが任意に消去することができない．したがって，ユーザーは無暗に承認要求を許可する，及び対話中に個人情報を提示することは，思わぬプライバシーリスクにつながる可能性を認識しておく必要がある．

4.4　トラッキングアプリに見られる特徴

各トラッキング手法と，そのトラッキング手法を用いた VA アプリが属するカテゴリーの内，最も代表的であったものを表 7 に示す．VA アプリのカテゴリーによって，使

表 6　個人情報別取得方法及び VA アプリ数

個人情報	取得方法	個数
生年月日等	対話	16
名前	対話	2
	Google Sign-In	10
	Helpers インテント	1
メールアドレス	対話	1
	Google Sign-In	10
プロフィール写真	Google Sign-In	10
現在地	Helpers インテント	10
住所等	対話	7
年齢	対話	2
血液型	対話	2
電話番号	対話	1
性別	対話	1

表 7　トラッキング手法と最も代表的なカテゴリーの関係

トラッキング手法	VA アプリカテゴリー
OAuth 利用	仕事効率化
Google Sign-In 利用	アート＆ライフスタイル
Helpers インテント利用	旅行＆交通機関
UserStorage 利用	ゲーム＆娯楽
トラッキング手法不明	仕事効率化
複数の手法利用	旅行＆交通機関

用されるトラッキング手法が異なる傾向にあることが分かる．表 7 に示す各トラッキング手法から VA アプリをランダムに取り出し，VA アプリがトラッキング手法を利用する理由及びその妥当性を，プライバシーポリシーに記述されている個人情報使用目的を参考にして検証した．

ケース 1 (OAuth) 自宅で行方不明なスマートフォンを鳴らす VA アプリを検証した．この VA アプリは，プライバシーポリシーにおける個人情報利用目的として，プレゼントの発送を示している．しかし VA アプリの説明にはその点の言及がなく，アプリが本来持つ機能との関係は薄い．

ケース 2 (Helpers インテント) 最寄りのバス停の情報を教える VA アプリを検証した．この VA アプリは機能提供のために発話内容及び使用履歴を取得していると示しているが，最寄りのバス停を探すために現在地を取得しているにもかかわらず位置情報取得の記載がない．またプライバシーポリシーには個人情報の扱い方の記述がなく，個人情報利用方法に不透明さがある．

ケース 3 (UserStorage 利用) 探索ゲームができる VA アプリを検証した．この VA アプリは，UserStorage にユーザー識別子及びゲームの経過情報を保存する．しかしプライバシーポリシーには個人情報を扱わないとの記載があり，VA アプリの説明にもユーザー固有のデータを保存していることは記述していない．すなわちユーザーはアプリページから UserStorage データを閲覧しない限り，情報が保存されていることに気が付くことはできない．

ケース 4 (複数の手法) 使用端末の現在地を教える VA アプリを検証した．この VA アプリは使用端末の現在地を取得して表示する機能を提供しているため，Helpers インテントの利用は自然である．しかしプライバシーポリシーが削除されていたため，妥当性の検討が不可能であった．VA アプリ申請時にプライバシーポリシーは必須事項であるにもかかわらず，プライバシーポリシーが存在しない VA ア

プリが使用できる状況にあることは問題である．

4.5 トラッキングに関する詳細解析

本節では，トラッキングに関して，特に興味深い事例の詳細解析を行う．

サードパーティフレームワーク　UserStorage データの検証時，データの形式が相互に類似している VA アプリを 52 個発見した．形式は開発者が自由に決めることができるため，開発者が同一であればデータの形式が類似することは自然である．しかしながら，これらの VA アプリは開発者が異なっているにもかかわらず形式及び要素の名前まで全て同一であった．これらの VA アプリに共通する性質はクイズを行う点であるため，クイズを行う VA アプリを開発するためのフレームワークがサードパーティによって提供されている可能性がある．フレームワークが開発者以外のサードパーティによって管理されている場合，開発者が意図しなくともサードパーティがユーザーから得た情報を収集・利用するリスクが想定される．これはモバイルアプリにおける，サードパーティライブラリに起因する問題 [9], [10] と類似している．

Fulfillment 共有　VA アプリの呼び出しに失敗した場合に表示されることがある「システムメッセージ」に固有な特徴がある VA アプリを 3 個発見した．通常システムメッセージには呼び出した VA アプリの名前が含まれるが，これらの VA アプリのシステムメッセージに表示される名前は同一であった．なお，この名前を持つ VA アプリは 2019/7/7 時点で存在しない．システムメッセージが表示される仕組みを考察すると，Google Assistant は接続する Fulfillment から VA アプリの名前を取得し，システムメッセージに表示すると推測される．すなわち Fulfillment が同一であれば，システムメッセージには同じ VA アプリ名が表示されると考えられる．したがって，Fulfillment を通じて VA アプリ間で情報を共有することで，VA アプリ間でユーザーをトラッキングできる可能性がある．

5. 議論

本章では本研究の制限事項及び研究倫理，並びに正しいトラッキング及び今後の課題について論じる．

5.1 制限事項

本研究の調査対象は Google Assistant の日本語版 VA アプリであり，他の Voice Assistant の実装例及び他言語の VA アプリは調査していない．よってそれらの実態は不明である．また本研究では VA アプリを呼び出した後，リクエストを行わずに VA アプリから退出している．VA アプリとの対話を続けることにより，VA アプリのトラッキングや，個人情報取得状況をさらに深く分析することができる．

5.2 研究倫理

本研究の調査の結果判明した，プライバシーリスクの懸念がある VA アプリ及び開発者に関して，個別の実名は公表せず，統計値のみの記述に留めた．幸い，本研究の調査では悪性度がきわめて高い VA アプリの発見には至らなかったが，今後調査を継続する課程でそのような悪性 VA アプリを発見した場合は，JPCERT/CC への報告・相談を進めるとともに，該当するアプリ事業者，Voice Assistant 事業者との相談・調整を進めた上で，適切な方法で情報開示を行う予定である．

5.3 望ましいユーザートラッキング

トラッキングはユーザーコンテキストに適した機能を提供することを可能とする．トラッキングを適切に利用することで，ユーザーは高い利便性を享受することができる．一方，本研究の調査により，トラッキングをしている VA アプリの内，9 割がユーザーの承認を得ることなくトラッキング手法を利用していることが明らかになった．これらのすべてが問題のある挙動を示しているわけではないが，このような状況下ではユーザーにとって，個人情報を取得する目的の検討や個人情報利用方法の把握は困難であり，プライバシーリスクにつながる懸念がある．

望ましいユーザートラッキングとは，個人情報を利用する目的と情報の流れをユーザーに明示すること，及びユーザーの同意を得ることである．まずユーザーに対し個人情報を利用する目的を，実際には読まれることが少ないプライバシーポリシーに記載するだけでなく，アプリページの説明で明示することが望ましい．またアプリページの説明を読まずに VA アプリを利用するユーザーが存在することを踏まえると，VA アプリが呼び出された時にも提示することが望ましい．さらに情報の流れの把握のため外部のサーバーやデータベースを利用しているのかどうかを明示すると良い．次に利用目的を明示した上でユーザーの同意を取ることが望ましい．ウェブサービスやモバイルアプリにおけるトラッキングの是非に関する研究と法的な議論がなされてきたが，新興分野である VA アプリについてはほとんど検討されていない．しかしトラッキングを行い，個人情報を保存することは国によって GDPR などの法律により規制されていることを踏まえると，ユーザーの同意を得るメカニズムを備えることが本質的に重要である．このような要件を，ユーザビリティを損なうことなく VA アプリ・プラットフォームで実現する手法の提案は今後の課題である．

5.4 今後の課題

本研究で使用した分類・分析手法は手動で行うものであるため，時間的コストが大きく精度が保証されない．それらを改善するために，VA アプリとの対話システム及び VA

アプリの分類システムを設計することが早急に解決するべき課題であると考える．これらのシステムを利用して，本研究では対象としていない Voice Assistant の実装例の調査，及び他言語の VA アプリの調査を今後の課題とする．

また，説明及びプライバシーポリシーと実際の挙動に齟齬がある VA アプリが存在する可能性がある．渡邉ら [10] が実施した Android アプリの解析では，説明と実際の挙動が異なるアプリの存在を明らかにしている．同様の解析を VA アプリに対して行うことも今後の課題とする．

6. 関連研究

Abdi ら [1] は Voice Assistant に対するユーザーの認識に関する調査を行い， Voice Assistant 及び関連データアクティビティに対するユーザーの認識が不完全であることを発見した．また Voice Assistant の脅威モデルを検証し，攻撃から身を守るための非技術的対処戦略を提案した．さらに Voice Assistant に対する，ユーザーのセキュリティとプライバシーの期待に応えるための方法を提案した．Zhang ら [11] は既存 VA アプリの音声コマンドの乗っ取りをする Voice Squatting Attack 及び Voice Assistant または VA アプリに成りすます Voice Masquerading Attack という VA アプリに対する攻撃方法が存在することを，ユーザー調査及び実際に攻撃を行うことにより証明した．また類似した VA アプリ名を発見するスキャナーの使用により，既に攻撃が行われている可能性を提示した．さらに Voice Masquerading Attack を行う悪性アプリを識別する状況依存検出器を設計し，95%の精度を達成した．He ら [6] は IoT 機器のアクセス制御及び認証システムの再構想を行った．アクセス制御についてデバイス毎ではなく IoT 機器の機能毎に重点を置き，ユーザー調査によってデフォルトアクセス制御ポリシーの候補を選定した．またポリシーに影響を与える背景的要因を特定した．さらにアクセス制御ポリシーを指定するために必要な機能を持ちうる認証方法を提案した．

7. まとめ

Voice Assistant の実装例の一つである Google Assistant を対象として，VA アプリの大規模実態調査を行った．VA アプリのメタデータ収集の結果，2019/7/7 時点において 940 個の VA アプリが存在することを明らかにし，カテゴリー毎，開発者毎の統計を示した．VA アプリから選定した 782 個の VA アプリのトラッキング手法を調査した結果，395 個の VA アプリがユーザーのトラッキングをしていること，並びに個人情報を取得する VA アプリが 89 個存在することを明らかにした．トラッキングを行う VA アプリには，トラッキングする理由が VA アプリの機能と無関係であるもの，プライバシーポリシーの記載と齟齬があるもの等，問題があるアプリが存在することを明らかにした．それらの問題点を解決する，VA アプリの理想的なトラッキングとして，ユーザーへの詳細の周知方法，及びユーザーの同意の取得について議論した．ユーザーをトラッキングする VA アプリの調査方法の改善，VA アプリのレスポンスに対し適切なリクエストを行う対話システムの開発，ユーザビリティを損なうことなく理想的なトラッキングを実現するメカニズムの検討は今後の課題である．

謝辞 本研究の一部は JSPS 科研費 18K19789，および 19H04111 の助成を受けたものです．

参考文献

[1] Abdi, N., Ramokapane, K. M. and Such, J. M.: More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants, *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pp. 451–466 (2019).

[2] Google: Actions on Google, , available from ⟨https://developers.google.com/actions/⟩ (accessed 2019-08-08).

[3] Google: Assistant directory, , available from ⟨https://assistant.google.com/explore⟩ (accessed 2019-08-08).

[4] Google-Developers: Android Debug Bridge, , available from ⟨https://developer.android.com/studio/command-line/adb?hl=JA⟩ (accessed 2019-08-08).

[5] Google-Developers: Introduction to the Google Assistant Service, , available from ⟨https://developers.google.com/assistant/sdk/guides/service/python/⟩ (accessed 2019-08-08).

[6] He, W., Golla, M., Bochum, R.-u., Padhi, R., Ofek, J., Drmuth, M., He, W., Golla, M., Padhi, R., Ofek, J. and Markus, D.: Rethinking Access Control and Authentication for the Home Internet of Things (IoT) Weijia, *Proceedings of the 27th USENIX Security Symposium*, pp. 255–272 (2018).

[7] senzhk: ADBKeyBoard, , available from ⟨https://github.com/senzhk/ADBKeyBoard⟩ (accessed 2019-08-08).

[8] tesseract ocr: Tesseract OCR, , available from ⟨https://github.com/tesseract-ocr/tesseract⟩ (accessed 2019-08-08).

[9] Watanabe, T., Akiyama, M., Kanei, F., Shioji, E., Takata, Y., Sun, B., Ishi, Y., Shibahara, T., Yagi, T. and Mori, T.: Understanding the Origins of Mobile App Vulnerabilities: A Large-scale Measurement Study of Free and Paid Apps, *Proc. of the 14th International Conference on Mining Software Repositories (MSR)*, pp. 14–24 (2017).

[10] Watanabe, T., Akiyama, M., Sakai, T. and Mori, T.: Understanding the Inconsistencies between Text Descriptions and the Use of Privacy-sensitive Resources of Mobile Apps, *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 241–255 (2015).

[11] Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y. and Qian, F.: Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems, *Proc. of the 2019 IEEE Symposium on Security and Privacy*, IEEE, pp. 263–278 (2019).