Voice Assistantアプリ解析ツールによる挙動解析

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

概要：Voice Assistant では，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 アプリはクラウドで動作するため，その挙動は透明性に欠ける．また，既存のアプリ解析手法は VA アプリに適用することができない．VA アプリの挙動が不透明な状況では，ユーザに予期せぬプライバシーリスクをもたらす可能性がある．本研究では，VA アプリの対話型解析システムを開発し，Google Assistant を対象に，サードバーティ製 VA アプリの挙動解析を実施する．始めに，VA アプリのメタデータを収集する．次に対話型解析システムでは，自然言語処理による解析により，VA アプリとの対話を行う．続いて VA アプリのプライバシーポリシー解析ツールを開発し，記載内容の解析を行う．これら三つの工程を経て取得したデータの相関関係を分析し，VA アプリの実態を明らかにする．調査の結果，プライバシーに懸念のある VA アプリの挙動を明らかにした．そのような実態を踏まえ，本論文では透明性の高い VA アプリを開発していくための解決策を議論する．

キーワード：Voice Assistant，クラウドアプリ，自然言語処理，トラッキング，プライバシーポリシー

Behavior Analysis with Voice Assistant App Analysis Tools

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

Abstract: In Voice Assistant, official or third-party Voice Assistant apps (VA apps) are provided. Since a VA app works as a cloud service, most of the app's behavior lacks transparency. In addition, conventional app analysis methods cannot be used for VA apps. That is, there is a lack of tools for analyzing VA apps. The current situation where the actual condition of VA apps is not fully understood could lead to unexpected privacy risks. In this research, we have developed an interactive analysis system for VA apps and conduct a behavior analysis of third-party VA apps for Google Assistant. First, we collected the metadata of the app. Next, the interactive analysis system interacted with apps. Also, we developed a tool that automatically analyzes privacy policy of VA apps. We found several VA apps that behave in a way raising concerns about privacy. Finally, we discuss solutions for developing a highly transparent VA apps.

Keywords: Voice Assistant, Cloud App, Natural Language Processing, Tracking, Privacy Policy

1. はじめに

Voice Assistant とは，ユーザからの音声リクエストによってサービスを提供するシステムである．スマートホームの制御やオンラインショッピング，ゲーム体験などの用途で使用される．これらのサービスを提供するアプリケーションのことを Voice Assistant アプリ（以下 VA アプリ）と呼ぶ．VA アプリはサードパーティも開発でき，VA アプリの多様性につながっている．

VA アプリの特徴は，従来のモバイルアプリとは異なり，クラウドで動作する点にある．ユーザが直接やり取りするのは，Amazon や Google を代表とする Voice Assistant プラットフォーマが提供するインタフェースであり，VA アプリの複雑な処理の大部分は開発者が準備するサーバ上で動

[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 社会情報研究所 (NTT Social Informatics Laboratories)
[a)] natatsuka@nsl.cs.waseda.ac.jp

作する．ここで問題となるのは，クラウド上で動作している VA アプリの処理を，ユーザだけでなくプラットフォーマ自体も把握することが難しい点である．実際，Cheng らが実施したプラットフォーマによる VA アプリの公開認証審査の信頼性検証 [1] では，ポリシー違反 VA アプリの 6 割が審査を通過したこと，および公開 VA アプリにポリシー違反のアプリが含まれていることを明らかにしているため，そのような問題が存在することは明白である．プラットフォーマを含め，VA アプリの実態を把握しきれていない現状は，ユーザに悪影響を与えつつある．

本研究では，VA アプリの対話型解析システムおよびプライバシーポリシー解析ツールを開発し，プライバシーリスクにつながる恐れのある VA アプリの実態を調査する．特に Voice Assistant の代表的な実装例の一つである，Google Assistant の日本語版アプリを調査対象とした．本研究の Research Question (**RQ**) は以下の通りである．

RQ1: VA アプリはどのようなトラッキング手法を利用し，明確にトラッキングの理由を説明しているのか．
RQ2: Google Assistant が提供している user storage [4] を利用してユーザの情報を保存する VA アプリはどの程度存在し，保存したデータをどのように利用しているのか．
RQ3: ユーザとの対話を通じて VA アプリはどのような情報をどのような状況下で取得・保存しようとしているのか．
RQ4: VA アプリのプライバシーポリシーにはどのような問題点が存在しているのか．

本研究の技術的なチャレンジは，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．VA アプリのソースコードは公開されていないため，VA アプリを解析するためのデータは，メタデータの収集および VA アプリとの対話によって取得しなければならない．

上述の目的を達成するために，本研究でははじめに対話型解析システムを開発する．対話型解析システムとは，自然言語処理によって VA アプリの挙動解析を自動化するシステムである．次に VA アプリのプライバシーポリシー解析ツールを開発する．解析手法には，予め収集したワードの利用によるパターンマッチングを採用する．

二つの解析ツールの開発を終えた後は，ツールを利用して VA アプリが持ち得る全てのデータの収集に移る．まずは，全ての公開されている VA アプリの情報が記載されている Assistant directory [5] からメタデータを収集する．収集対象となる VA アプリは日本のマーケットで公開されている VA アプリである．そしてメタデータを利用して，調査対象となる VA アプリを決定する．次に対話型解析システムを利用して，調査対象 VA アプリとの対話を実行し，アプリのレスポンスなどを収集する．収集後には，Assistant directory から user storage に保存されているデータの収集を行う．最後にプライバシーポリシー解析ツールを利用して，プライバシーポリシーを七つのタイプに分類する．

収集後は取得したデータを利用して，VA アプリの実態を解析する．使用するデータは，2021/6/26 から 2021/7/27 にかけて収集された日本語版 VA アプリ 467 個のデータである．まずは，取得したレスポンスを解析してトラッキング手法利用やユーザ情報取得の実態を調査する．次に user storage データを利用して，その利用状況を調査する．続いて分類されたプライバシーポリシーを利用して，メタデータや対話型解析システムで得られたデータとの関連性を調査する．最後に全ての解析データを基に，VA アプリに固有な問題を明らかにする．

本研究の貢献は以下の通りである[*1]．

- VA アプリのプライバシーポリシーの正当性を検証することを目的とした解析ツールを開発した．ツールの精度は約 9 割と，高い精度を発揮している．
- VA アプリのトラッキング手法利用状況を解析する手法を提案し，手法を利用するアプリがユーザに対してその利用目的を明示していない可能性を明らかにした．
- VA アプリのユーザ情報取得状況を解析する手法を提案し，その利用目的が不明なアプリが存在することや情報が保存されることによるリスクを明らかにした．
- VA アプリ開発者が提示するプライバシーポリシーの大部分においてプラットフォーマが提示する要求事項のいずれかが欠落していることや，一部のアプリのプライバシーポリシーは閲覧不可能であることを発見した．
- 取得された全てのデータから，VA アプリに存在する問題を明らかにし，それらに対する解決策を提案した．

2. 背景

2.1 VA アプリの構造

Google Assistant 上の VA アプリは，Google Assistant，Conversational Action，Fulfillment Service という要素から成り立っている [4]．VA アプリの全体図を図 1 に示す．Google Assistant とは，ユーザが VA アプリを使用するためのインタフェースであり，ユーザの音声リクエストをテキストに変換し，Conversational Action に渡す．Conversational Action とは，ユーザとのインタラクションモデルを意味し，VA アプリの呼び出し方やリクエストへの応答方法を定義する．Fulfillment Service とは，VA アプリのレスポンスを柔軟に生成するための仕組みである．必要に応じて Conversational Action がリクエストを Fulfillment

[*1] 著者らが CSS2019 で発表した研究 [9] と ICSS 研究会 (2021 年 3 月) で発表した研究 [10] との差分は以下の通り: (1) VA アプリクローラの大幅改良 (2) VA アプリのプライバシーポリシー解析ツールを開発 (3) VA アプリのトラッキングやユーザ情報取得の実態を調査 (4) VA アプリのプライバシーポリシーと平均評価・評価人数の関連性を分析 (5) VA アプリに固有な問題の解決策を提案.

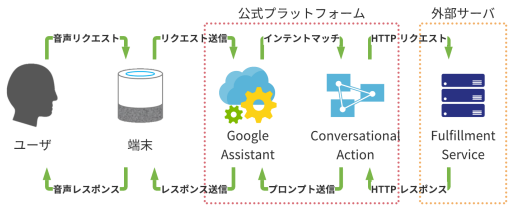


図 1: VA アプリの全体図

Service に送信し，VA アプリのレスポンスが生成される．

ここで着目するべき点は，Google Assistant と Conversational Action が Google の開発プラットフォーム上で動作する一方で，Fulfillment Service はサードパーティが用意した外部サーバにホストすることが可能であるという点である．このような場合，VA アプリの挙動を把握することは開発者にしかできず，VA アプリにおいてどのようなデータが処理されているのかを知ることは困難である．また，Fulfillment Service にホストしたソースコードは審査に提出する必要がないため，VA アプリの透明性を損なわせる一因となっている．

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のトラッキングを可能とする，OAuth，Google Sign-In，Helper インテントという，三つのメカニズムが用意されている．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 [4] によるユーザ認証機構が含まれる．標準の OAuth 2.0 の認証フローをサポートしており，implicit コードフローと 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，ユーザをトラッキングすることが可能である．

Google Sign-In

Google Sign-In [4] 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サービスのアカウントは不要である．利用をユーザが許可した場合，Google Assistant は VA アプリへ送信するリクエストに 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．このユニーク ID を記録することでユーザをトラッキングすることができる．

Helper インテント

Helper インテント [4] 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．Helper インテントによって取得できる情報には，ユーザの名前，使用端末の現在地，住所などが含まれる．利用をユーザが許可した場合，Google Assistant は VA アプリへ送信するリクエストに上記の情報を付加する．この情報を記録しておくことでユーザをトラッキングすることができる．

2.3 User storage

User storage [4] とは，VA アプリとユーザ間において保持される固有のストレージである．開発者は Fulfillment Service 上で user storage に任意のデータを保存する．ユーザは Web ブラウザからアクセスできる Assistant directory のアプリ専用ページを開くことで，保存済み user storage データを確認・削除できる．しかし，大部分の VA アプリは Assistant directory や user storage を意識せずに使えるよう開発されているため，ユーザは行動・発話データが保存されていることに気づくことが難しい．

3. VA アプリの解析手法

3.1 メタデータ収集・解析

Assistant directory からメタデータ収集を行う．まず収集の事前準備として，VA アプリを検索するための単語リストを作成する．検索用単語は，Wikipedia の記事データベース [7] から記事名を取得し，自然言語処理 (以下 NLP) の一種である形態素解析を実施して抽出された名詞である．次に Assistant directory を開き，検索ボックスから検索用単語リストを利用して VA アプリを検索し，表示された VA アプリの詳細ページへのリンクを全て取得する．リンクを取得したら，リンクを利用してアクセスし，詳細ページに表示されている，VA アプリ名，開発者名，アプリの説明，呼び出しコマンド，カテゴリー，対応端末，平均評価，評価人数，プライバシーポリシーへの URL を取得する．クローリング終了後は，収集できた VA アプリから調査対象となるアプリを選定する．選定条件は，「開発者が Google でないもの」，「カテゴリーがスマートホームでないもの」，「呼び出しコマンドが存在するもの」である．

3.2 対話型解析システムによる解析

本節では，対話型解析システムの設計を示す．

対話型解析システムの全体像

本研究で開発した対話型解析システムは，Google Assistant の VA アプリを対象としている．本システムはユーザが VA アプリを利用するのと同様に，VA アプリと対話を行う．対話は，NLP の一種である構文解析により，VA アプリが発するレスポンス内の係り受け関係を抽出することで成り立つ．係り受け関係は，レスポンスからリクエストを生成するために利用される．また，VA アプリを網羅的に調査する仕組みとして，過去のレスポンス構造を記録するツリー構造を導入する．ツリー構造は下記で詳しく説明する．さらに本システムは，開発プラットフォームのシミュレータ [3] 上で VA アプリを呼び出すことにより対話を行う．本システムによって VA アプリとの対話中に得られた収集データには，VA アプリのレスポンスやツリー構造などが含まれている．対話の終了後には user storage データ

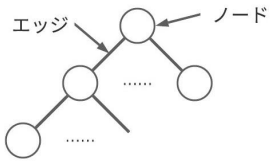


図 2: ツリー構造

を取得する．収集した全てのデータについて，調査対象とした全ての VA アプリとの対話終了後に，データ単体およびデータ間の関係について解析を行う．

ツリー構造

過去のレスポンスを記録する仕組みとして，対話型解析システムは VA アプリと対話を行いながらツリーを構築する．ツリーの具体例を図 2 に示す．ツリーが構築される流れを説明する．まず VA アプリが呼び出され最初のレスポンスを取得したら，ツリーの根ノードを生成する．次にリクエストを生成したら，1 リクエストにつき 1 エッジ，根ノードに生成する．その後システムがリクエストを入力しレスポンスを取得したら，対応するエッジの先にノードを生成する．レスポンスとリクエストの取得に応じてノードとエッジの構築を繰り返し行うことでツリーを構築する．またツリー構造は，VA アプリのインタラクティブモデルに対して対応関係を持つという性質がある．インタラクティブモデルとは，VA アプリがユーザとの自然な対話を行うために必要なモデルである．このモデルは，インテントと呼ばれる，リクエストに対するレスポンスを定義するデータが複数連結された構造であり，その連結構造は疑似的なツリーと見なせる．すなわち，本研究で開発した対話型解析システムが構築するツリー構造は，アプリのインタラクティブモデルとほぼ同じ構造になると考えられる．そのため本研究では，対話後に得られるツリー構造を利用して，VA アプリのインタラクティブモデルも分析している．

3.3 プライバシーポリシーの解析

Google Assistant を提供する Google は，プライバシーポリシーへのリンクをアプリ審査時に提出するように求めている．そのため，VA アプリ用プライバシーポリシーを作成するためのガイドライン [4] を提示している．ガイドラインでは，開発者に対して大きく三つの質問に答えるように要求している．三つの要求事項は以下の通りである．

(I) どのような情報を収集しているのか

VA アプリが収集し得る全ての情報を記載する必要がある．対象となる情報には，ユーザの個人情報に限らず，ユーザ識別子や VA アプリが自動的に収集する情報である，サーバログや HTTP ログ，Actions on Google からユーザに送信されるデータ，使用状況情報も含まれる．

表 1: プライバシーポリシー分類タイプの概要

タイプ	説明
NoProblem	全ての要求事項を満たすもの
NotPolicy	プライバシーポリシーではないもの
NotCollect	要求事項 (I) を満たさないもの
NotUse	要求事項 (II) を満たさないもの
NotShare	要求事項 (III) を満たさないもの
Either	いずれかの要求事項を満たさないもの
ALL	全ての要求事項を満たさないもの

表 2: プライバシーポリシー解析ツールの精度

タイプ	割合
NotCollect	89.2%
NotUse	95.8%
NotShare	84.4%

(II) 情報をどのように利用しているのか

VA アプリが収集した全ての情報の使用方法を具体的に記載する必要がある．

(III) どのような状況下で誰に情報を共有しているのか

VA アプリが収集した情報をどのような状況下で誰に共有するのかを記載する必要がある．サードパーティや他のユーザ，マーケティングパートナー，サービスプロバイダーなどの，情報が共有され得る相手について具体性が求められる．

本研究で開発する VA アプリのプライバシーポリシー解析ツールでは，これらの要求事項についてプライバシーポリシーが答えているかどうかに焦点を当てる．具体的には，プライバシーポリシーを七つのタイプ，すなわち **NoProblem**，**NotPolicy**，**NotCollect**，**NotUse**，**NotShare**，**Either**，**ALL** に分類するという手法を採用している．各分類タイプの説明を表 1 に示す．分類は，予め収集した単語を利用するパターンマッチングにより行っている．パターンマッチング用の単語は，収集されたプライバシーポリシーのリンクをランダムサンプリングし，要求事項 (I) 〜 (III) を満たすプライバシーポリシーに含まれる特徴的な単語や文を抽出することによって収集した．

4. VA アプリの解析結果

本章では，3 章で説明した解析ツールを利用して VA アプリを解析した結果を示す．利用したデータは 2021/6/23〜7/27 に存在した 467 個の VA アプリのデータである．

4.1 プライバシーポリシー解析ツールの評価

プライバシーポリシー解析ツールを評価した結果を示す．評価では，ランダムにサンプリングしたプライバシーポリシーが，**NotCollect**，**NotUse**，**NotShare** という三つのタイプにおいて適切に分類されているかを評価する．プライバシーポリシー解析ツールの精度を表 2 に示す．精度はどのタイプも 8 割を超える高い精度であり，全てのタイプの平均精度は約 9 割という結果になった．

表 3: VA アプリのトラッキング手法

グループ	個数	割合
OAuth	26	5.57%
Google Sign-In	37	7.92%
Helper インテント	8	1.71%

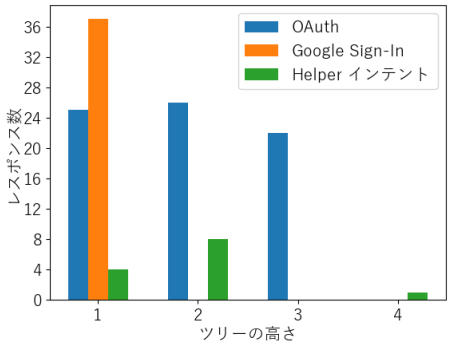


図 3: ツリーの高さ毎のトラッキング手法利用許可を求めるレスポンス数

4.2 トラッキング手法の利用状況

本節は，**RQ1** を検証することを狙いとし，対話型解析システムによって取得した VA アプリのレスポンスからトラッキング手法利用の有無を解析する．2.2 節で説明したトラッキング手法を利用している VA アプリ数を表 3 に示す．Google Sign-In が最も多くの VA アプリに利用されていた．また，ツリー構造を利用し，VA アプリがユーザと対話を何回行った後にトラッキング手法利用の許可を取得しているのかを調査する．トラッキング手法利用許可を求めるレスポンスが現れたツリーの高さを図 3 に示す．ツリーの高さが 1 から 4 のときに，トラッキング手法利用の許可を求めている．ツリーの高さは対話の回数を意味するため，これらの VA アプリは比較的対話を始めてからすぐに利用許可を取ろうとしていることがわかる．対話を始めてすぐに許可を取る場合，ユーザは VA アプリが提供しようとしている機能を明確に把握できないまま許可してしまう可能性が高く，悪意のあるアプリにトラッキングを可能とするユーザ情報を渡してしまう恐れがある．

4.3 User storage の利用状況

本節は，**RQ2** を検証することを狙いとし，対話型解析システムが取得した user storage のデータを分析する．結果，user storage を利用していたアプリは 79 個 (全体の 16.9%) 存在していることが判明した．また，特徴的なものを保存していたアプリの数を表 4 に示す．ユーザ識別子が最も user storage に保存されていた．これらの識別子は，VA アプリが外部サーバで生成したものが大部分を占めている．また，一部のアプリにおいて保存されている各データの利用目的を調査した．調査したアプリは，user storage を利用している VA アプリからランダムにサンプリングしたアプリである．その結果，大部分のデータについては利用目的が推測不可能であった．特にユーザ識別子については利用目的が不明であるものが多く占めていた．利用目的が推測できたデータについて一部紹介する．ユーザのアプリ利用回数を保存するアプリについては，利用回数によってユーザに提供するコンテンツを変化させていた．ユーザが該当アプリを初めて利用したかを判別するためのフラグを保存し，対応を変えているものも存在した．

表 4: User storage に保存されているデータ

グループ	個数
ユーザ識別子	42
ユーザの利用時間	7
ユーザの利用回数	4

表 5: 取得されているユーザ情報

ユーザ情報	取得方法	個数
名前	Google Sign-In	37
	対話	2
メールアドレス	Google Sign-In	37
プロフィール写真	Google Sign-In	37
住所	対話	12
現在地	Helper インテント	8
	対話	3
誕生日	対話	8
年齢	対話	3
使用電車路線	対話	2
勤め先	対話	1
性別	対話	1

4.4 ユーザ情報の取得状況

本節は，**RQ3** を検証することを狙いとし，対話型解析システムによって得られた VA アプリのレスポンスから，ユーザ情報を取得している挙動を分析する．分析した結果，ユーザ情報を取得している VA アプリは 67 個 (全体の 14.3%) 存在した．取得されているユーザ情報と取得方法，取得しているアプリ数を表 5 に示す．最も取得されている情報が「名前」となった．「名前」は個人情報に含まれ，取得された場合ユーザ個人をトラッキングされる恐れがある．また，「メールアドレス」を取得するアプリも多数存在し，取得された場合はフィッシングメールやランサムウェアの感染などのサイバー攻撃の被害に合う可能性がある．他にも複数の個人情報が取得されていた．これらのユーザ情報は，一度取得された場合，ユーザが容易に削除することができない．そのためユーザは，情報を入力したり，トラッキング手法の利用を許可したりした場合のプライバシーリスクを認識しておく必要がある．

また，ツリー構造を利用し，VA アプリがユーザと対話を何回行った後ユーザ情報を取得しているのかを調査する．ユーザ情報を求めるレスポンスが現れたツリーの高さを図 4 に示す．おおよそツリーの高さが 1 から 10 のときに，ユーザに対してユーザ情報の入力を求めている．しかし一方で，100 回以上対話を行ってからユーザ情報を求める VA アプリも存在する．多くの対話を行った後初めてユーザ情

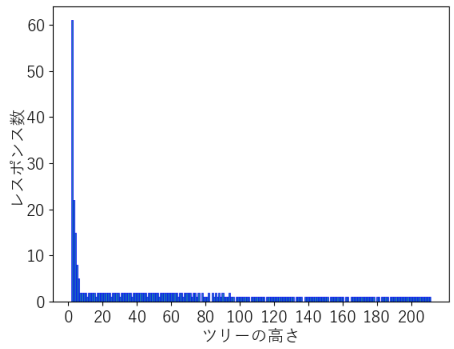
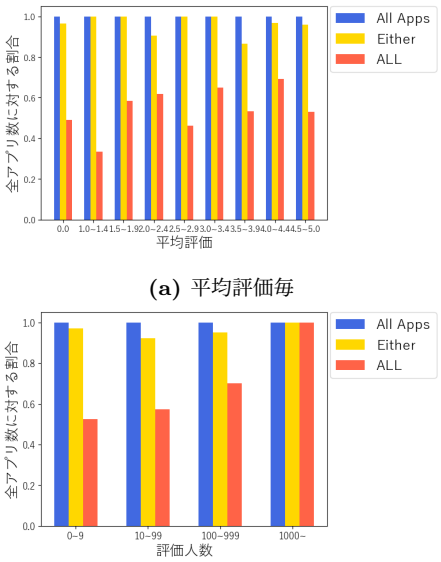


図 4: ツリーの高さ毎のユーザ情報を求めるレスポンス数

表 6: プライバシーポリシーの分類タイプ毎のアプリ数

タイプ	個数	割合
NoProblem	18	3.85%
NotPolicy	18	3.85%
NotCollect	377	80.7%
NotUse	248	53.1%
NotShare	327	70.0%
Either	449	96.1%
ALL	256	54.8%



(a) 平均評価毎

(b) 評価人数毎

図 5: 平均評価/評価人数毎の VA アプリ数に対する特定プライバシーポリシー分類タイプのアプリ数の割合

報の入力が求められている場合，アプリの公開認証審査において，ユーザ情報入力要求の実施が発見されない可能性がある．実際に Cheng らが実施したプラットフォーマが行う VA アプリ審査に対する信頼性検証では，審査における VA アプリのテスト回数が 3 回程度ということが判明しており，多数回対話が行われていない可能性が高い．このような審査の実態を利用して，悪意のある開発者がユーザに危害を与える恐れがある．

4.5 プライバシーポリシーの実態

本節は，**RQ4** を検証することを狙いとする．

プライバシーポリシー分類結果

Google の要求事項をプライバシーポリシーが満たしているかを調査する．プライバシーポリシー解析ツールによって，3.3 節で説明したタイプに分類された VA アプリ数を表 6 に示す．結果，プライバシーポリシーの情報がない VA アプリは 18 個存在した．プライバシーポリシーを記載していた Google ドキュメントが削除されたものや Web サイトのサーバが落ちているものが占めていた．このような VA アプリが公開されたままになっていることは非常に問題である．また，9 割以上のアプリのプライバシーポリシーにおいて，Google の要求事項のいずれかが欠落していることが判明し，問題がないものは極めて少なかった．

平均評価や評価人数との関係性

メタデータに含まれる平均評価と評価人数の情報を利用して，プライバシーポリシーと平均評価/評価人数の相関関係を分析する．平均評価毎もしくは評価人数毎のアプリ数を 1 とした時の **Either**/**ALL** に分類されたプライバシーポリシーを持つアプリ数の割合を図 5 に示す．

平均評価とプライバシーポリシーの関係性について，平均評価が増加/減少しても，プライバシーポリシー分類タイプ毎のアプリ数への影響は見られなかった．理由は，プライバシーポリシー自体を確認するユーザが少なく，プライバシーポリシーの内容が評価に影響を与えにくいからであると考える．一方で評価人数とプライバシーポリシーの関係性については，評価人数が多くなるほど，Google の要求事項が全て欠落しているプライバシーポリシーを持つアプリ数の割合が増加する結果となった．理由は，評価人数と開発者の規模の関係性に起因すると考える．これまでの調査で，開発者の規模が大きい程，知名度が高い VA アプリが開発され，評価人数も増加する関係が見受けられている．そのため，評価人数が多くなるにつれて開発者の規模も大きくなると見なせる．その点を踏まえると，開発者の規模が大きい程，プライバシーポリシーに十分な情報を記載していない傾向にあることが推測できる．実際にこれらの開発者が掲載しているプライバシーポリシーを確認すると，VA アプリに特化したプライバシーポリシーではなく，他サービスのポリシーを使い回しているものが多かった．そのため，Google の要求事項が満たされていない．一方で開発者の規模が小さい場合，VA アプリ用にプライバシーポリシーを作成している人が多い傾向にあった．すなわち，このような状況が評価人数とプライバシーポリシーの関係性に影響を与えたと考えられる．

5. 議論

本章では本研究の制限事項および研究倫理，結果から判明した VA アプリに固有な問題に対する解決策を分析する．

5.1 本研究で開発した解析ツールの価値

VA アプリは，従来のモバイルアプリとは異なりクラウド上で動作するため，既存の解析手法を実施することが困難である．それに伴い，VA アプリを解析するためのツールが不足している．そのような現状に対して，本研究で開発した解析ツールは二つの価値を提供することが可能である．一つ目の価値は，VA アプリに対する審査の効率化と審査精度の向上である．二つのツールは手動で操作をする必要がないため，人的コストの削減や人的なミスが発生する可能性が減少する利点がある．二つ目の価値は，第三者による VA アプリの分析を可能にすることである．クラウドで動作する VA アプリの性質上，アプリの調査ができる者は，プラットフォーマ，開発者，VA アプリが動作するサーバの管理者に限られている．しかし，本研究で開発したような解析ツールが公開されることによって，それらに含まれない第三者が VA アプリの調査をすることができるようになる．それによって VA アプリの審査も，セキュリティを専門とする第三者機関に委託することが可能となり，プラットフォーマのコスト削減や審査の信頼性向上につながる可能性がある．結果として，より一層の VA アプリの発展が見込めるようになる．

5.2 VA アプリに見られた問題に対する解決策

本研究の調査の結果，VA アプリには複数の問題があることが判明した．それらは VA アプリの不透明性に起因するものであり，クラウド上で VA アプリが動作する限り，解決には困難を伴う．VA アプリの透明性を向上するために最も効果的な方法は，VA アプリの審査時に開発者が作成した外部サーバ上のソースコードを提出させ，従来の解析手法を実施する方法であるが，現状プラットフォーマはそのような手段を取っていない．そこで本研究では，ソースコードに依存しない，VA アプリの問題を解決するための四つの解決策を提案する．

(1) 解析ツールを活用したアプリ審査

VA アプリには従来の解析手法を実施することが難しいため，アプリを検証するには対話を行い，アプリの挙動を指し示すデータを収集する必要がある．そこで，対話を行うために利用可能なツールが，本研究で開発した対話型解析システムである．解析システムを利用すれば，自動でアプリと対話を行い，VA アプリを検証するための材料を収集できる．またプライバシーポリシー解析ツールも併用することで，審査の精度をより高めることも可能である．結果として，ユーザに危害を与える恐れがある VA アプリが公開されることを防ぐことができる．

(2) Assistant directory に対する定期的な検査

本研究による調査の結果，プライバシーポリシーへのリンクが切れている事例や，ポリシーが記載されている Google ドキュメントが削除されている事例などが明らかになった．このような VA アプリが公開されたままとなっている原因は，プラットフォーマである Google が定期的に公開アプリを検査していないからであると考えられる．これらの事例は，プライバシーポリシー解析ツールを活用することで容易に防ぐことができるため，ツールを利用した定期的な検査の実施が望ましい．

(3) プライバシーポリシーテンプレートの提供

プライバシーポリシー解析ツールによる調査の結果，大部分の VA アプリのプライバシーポリシーにおいて，何らかの情報が欠落していることが明らかになった．その原因として考えられるものは二つある．一つ目は，プライバシーポリシーの作成・公開に Google ドキュメントや Google サイトを利用する開発者が多いためである．ドキュメントやサイトが削除されてしまうと，ポリシーも削除されてしまう事態となる．二つ目は，VA アプリに適切なプライバシーポリシーの書き方に開発者が熟知していないためである．その結果，一般的なプライバシーポリシーのテンプレートやプライバシーポリシー作成サービスを利用する傾向にある．そこでこれらの原因を解決していくためには，VA アプリ用のテンプレートをプラットフォーマが提供することが望ましいと考える．また，ポリシーへのリンクが切れる事態を防ぐために，プライバシーポリシーを配置するための専用ホスティングサービスも提供すると良い．

(4) エコシステムを開示するためのインタフェース

本研究による調査の結果，トラッキング手法利用目的や収集しているユーザ情報，user storage 利用目的など，ユーザに対して明示的に示されていない情報があることがわかった．ある程度アプリを利用することで知ることはできるが，利用する前に知る手段が乏しい．したがって，ユーザが VA アプリを利用する前にセキュリティ・プライバシーに関わる情報を知るためのインタフェースが必要であると考える．そこで本研究では，Emami-Naeini らが提案しているセキュリティ・プライバシーラベル [2] を VA アプリ用に設計し，ユーザに表示することを提案する．スマートディスプレイのような画面付きの Voice Assistant 端末が普及しつつあり，ラベルは画面上に容易に表示することができるため，ユーザが VA アプリのエコシステムを把握しやすくなることに貢献すると考える．

5.3 今後の課題

Cheng らによる検証で，VA アプリのレスポンスにプライバシーリスクにつながりかねない内容が含まれている事実が明らかにされている．そこで，プライバシーリスクの懸念があるレスポンスの目的を推測可能な，NLP による自動解析機を開発したい．また，トラッキング手法の利用目的や収集するユーザ情報を明示していないアプリや user

storage に使途不明のユーザ識別子を保存するアプリなど，ユーザへの情報の開示性が悪い VA アプリが見受けられたため，VA アプリのエコシステムを明示的にユーザに開示できる機能を提案していきたい．

5.4 制限事項

本研究で開発した対話型解析システムとプライバシーポリシー解析ツールが対象とする Voice Assistant は Google Assistant であり，他の Voice Assistant の実装例における VA アプリは調査していない．また，本システムは開発プラットフォームのシミュレータ上で動作させているため，実デバイス上の VA アプリの挙動は調査していない．その際，アプリとの対話はテキストベースで行われているため，VA アプリが発する音声データの解析は実施していない．

5.5 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．

6. 関連研究

Zhang ら [8] は公開 VA アプリの音声コマンドを乗っ取る Voice Squatting Attack と，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．Guo ら [6] は，VA アプリの挙動に関する体系的な研究を提案した．そのために，文法ベースでアプリを解析するシステム「SkillExplorer」を開発した．このシステムは Amazon Alexa Skill と Google Assistant Action との自動通信を可能にする．Cheng ら [1] は，Amazon と Google における VA アプリ審査の信頼性を評価するための調査を実施した．評価に当たり，実際にポリシー違反の VA アプリを複数作成し，審査プロセスに提出した．その結果，全ての Amazon Alexa Skill，全体の 39%の Google Assistant Action が審査を通過した．また，公開子供向けスキルに焦点を当てた実証研究を行った結果，ポリシー違反のスキルを特定した．

7. まとめ

Voice Assistant の代表的な実装例である，Google Assistant の VA アプリを解析するための二つのツールを開発し，VA アプリの挙動解析を実施した．対話型解析システムは，NLP により VA アプリのレスポンス解析とリクエスト生成を行うことで，VA アプリとの自動対話を実現する．プライバシーポリシー解析ツールは，パターンマッチングによりプライバシーポリシーを分類することで，Google の要求事項を満たすかどうかを調査する．これら二つの解析ツールにより VA アプリを解析した結果，プライバシーリスクにつながる恐れのある VA アプリの実態を明らかにした．このような VA アプリに存在する問題を解決していくためには，本研究で開発した解析ツールを利用するアプリの公開認証審査や公開 VA アプリに対する定期的な検査，開発者が適切なプライバシーポリシーを作成するためのテンプレート，エコシステムを開示するためのインタフェースが必要である．

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] Cheng, L., Wilson, C., Liao, S., Young, J., Dong, D. and Hu, H.: Dangerous Skills Got Certified: Measuring the Trustworthiness of Skill Certification in Voice Personal Assistant Platforms, *Proc. of the ACM CCS 2020*, pp. 1699–1716 (2020).

[2] Emami-Naeini, P., Agarwal, Y., Cranor, L. F. and Hibshi, H.: Ask the Experts: What Should Be on an IoT Privacy and Security Label?, *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 447–464 (2020).

[3] Google: Actions on Google, Google (online), available from ⟨`https://console.actions.google.com`⟩ (accessed 2021-07-27).

[4] Google: Google Assistant, Google (online), available from ⟨`https://developers.google.com/assistant`⟩ (accessed 2021-07-27).

[5] Google: Google アシスタント，Google（オンライン），入手先 ⟨`https://assistant.google.com/explore`⟩（参照 2021-07-27）．

[6] Guo, Z., Lin, Z., Li, P. and Chen, K.: SkillExplorer: Understanding the Behavior of Skills in Large Scale, *Proc. of 29th USENIX Security Symposium*, pp. 2649–2666 (2020).

[7] Wikimedia Foundation: Index of /jawiki/latest/, Wikimedia Foundation (online), available from ⟨`https://dumps.wikimedia.org/jawiki/latest/`⟩ (accessed 2021-07-30).

[8] 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).

[9] 刀塚敦子，飯島　涼，渡邉卓弥，秋山満昭，酒井哲也，森　達哉：Voice Assistant アプリの大規模実態調査，コンピュータセキュリティシンポジウム 2019 論文集，pp. 618–625 (2019).

[10] 刀塚敦子，飯島　涼，渡邉卓弥，秋山満昭，酒井哲也，森　達哉：Voice Assistant アプリの対話型解析システムの開発，*IEICE Technical Report Volume 120, Number 384*, pp. 132–137 (2021).