Vol.2019-DPS-180 No.11
Vol.2019-EIP-85 No.11
2019/9/19

ロボットサービスシナリオを用いた 人と機械の信頼関係構築フレームワークの有効性検証

赤羽根 里奈[2]　菊田 佳恵[1]　伊東 風弥[2]　加藤 由花[1,a)]

概要：ロボット，IoT 機器，新世代ネットワークを高度に融合し，IoT データの安全・安心かつ幅広い流通・利活用を実現する情報流基盤に対する期待が高まっている．我々はこれまで，セキュアな IoT サービスの実現に向けて，人と機械の信頼関係を構築し強化するフレームワークの研究開発を進めてきた．本稿では，スマートホームでの利用を前提とした具体的なロボットサービスシナリオを想定することで，このフレームワークの有効性を検証する．

1. はじめに

ロボット，IoT 機器，新世代ネットワークを高度に融合し，IoT データ（情報流）の安全・安心かつ幅広い流通・利活用を実現する情報流基盤構築に対する期待が高まっている [1]．これを実現するには，情報流の発生源周辺で，人とその人の生活空間に入り込んで近接する IoT 機器との関係性が良好であり，サービス利用の安心感・信頼感が醸成されることが必須である．そのため，我々は現在，セキュアな IoT サービスの実現に向けて，人と機械の信頼関係を構築し，強化するフレームワークの研究開発を進めている [2]．フレームワークのイメージを図 1 に示す．

ここでは，日常生活の場でセンサー等から得られるプライバシ情報をフレームワーク側で取得・可視化し，ユーザにその把握レベルを提示する．さらに，機械に把握されているプライバシ情報を，ユーザのプロファイルに基づくタイプごとに分類し，ユーザとのインタラクションにより開示度を適正化する．現在までの成果としては，ユーザの情報リテラシや好みに応じた適切な設定を推薦することで，プライバシ適正化を効率的に支援する手法の提案がある [3]．ここでは，シミュレーションによる評価実験が行われているが，実環境におけるユーザのパーソナルデータ流通制御は非常に複雑な要素によりなされるものであるため，実環境における実証実験を目指した検討も進めてきた [4]．具体的

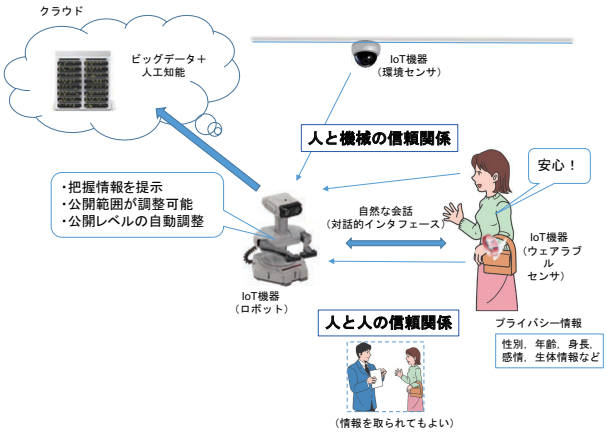

図 1　人と機械の信頼関係構築フレームワークの概要．

には，身体性を持ったコミュニケーションロボットを利用し，多種多様な IoT 機器とロボットを組み合わせたアプリケーションサービス（ロボットアプリケーション）を設計することで，フレームワークの検証を行うことを目指したものである．ここでは，一般家庭における日常生活の場で取得可能な情報で，それがプライバシ情報になり得る情報を抽出し，探索範囲の指定によりプライバシ情報の開示度を調整できる機能を有するアプリケーションを設計した．

本稿では，文献 [4] で設計したロボットアプリケーションを拡張し，さらに具体的なロボットサービスシナリオを想定することで，フレームワークの有効性を検証する．本稿の貢献は以下の 2 点である．

- フレームワーク検証のためのロボットサービスシナリオを設計する．
- 設計したサービスシナリオによりフレームワーク機能の実現可能性を検証する．

[1] 東京女子大学 現代教養学部
School of Arts and Sciences, Tokyo Woman's Christian University, Suginami, Tokyo 167–8585, Japan
[2] 東京女子大学 大学院理学研究科
Graduate School of Science, Tokyo Woman's Christian University
[a)] yuka@twcu.ac.jp

2. 人と機械の信頼関係構築フレームワーク

まず，本稿で考察対象とする「人と機械の信頼関係構築フレームワーク」について説明する．本フレームワークでは，人と機械（IoT 機器）の信頼関係を構築するために，以下の 2 項目の課題を設定し，その解決を目指したフレームワーク機能の設計を行っている [2].

- IoT 機器がどれだけのプライバシ情報を把握しているかをいかに自然な形で提示するか.
- 既把握のプライバシ情報のうち公開しても良い範囲をいかに自然なインタラクションで調整するか.

前者を解決するためには，プライバシ情報を取得する方法，プライバシの種類や度合いを計算する方法，計算結果をユーザに自然な形で提示する方法を開発する必要がある．後者を解決するためには，人と人の会話のように，IoT 機器と会話しながら，指定したプライバシ情報を公開しない（または，公開する）ように設定できる対話的なインタフェースを実現する必要がある．さらには，過去のインタラクション履歴等を踏まえて，空気を読み，ユーザが何も言わなくても，プライバシ情報の公開レベルを自動的に設定する機能も求められる．

これらの各課題に対応し，フレームワークは，大きく分けて 2 つの機能を有するものとして構成される．一つは，プライバシ情報の取得・可視化機能であり，もう一つは，プライバシ適正化のためのインタラクション機能である．これらの機能により，対象となるプライバシ情報の開示度が決定される．以下，これら 2 つの機能について，および対象となるプライバシ情報の分類結果について述べる．

2.1 プライバシ情報の可視化，点数化

本機能は，プライバシ情報として，マイク・カメラ等から得られる日常生活の映像・音声や，ウェラブルセンサーから取得される生体情報，SNS に投稿されるテキスト情報を対象とし，そこからプライバシにかかわる情報を抽出して点数化，可視化するものである．これまで，インターネットの各種サービスを利用する際の個人情報（PD: Personal Data）の開示度設定に際し，ユーザが持つ開示度の好みだけでなく，当該ユーザの情報リテラシを考慮して適切な設定を推薦する手法の検討が行われている [3]．ここでは，設定履歴を分析し，類似のサービス事業者に対して類似の設定を安定的に実施しているユーザに関して，設定の一貫性が高いと判定する．その後，設定の一貫性を他のユーザと相対的に比較し，それに基づき情報リテラシの程度に応じて適切な設定を推薦する．既存手法 [5][6] との比較により，手法の有効性も検証されている．

これにより，設定の半自動化が実現するが，PD の公開/非公開といった微妙な判断をそのときの事情に合わせて確実に行うためには，ユーザとの密なインタラクションによる適応的調整が不可欠である．そのため，可視化機能と合わせて，次節で述べるプライバシ適正化のためのインタラクション技術を組み合わせることにより，調整を実現する．

なお，本稿では，ユーザが持つ開示度の好みは別途与えられているものと仮定し，当該ユーザの情報リテラシは文献 [3] に示された手法により推定できるものとする．

2.2 プライバシ適正化のためのインタラクション

本機能は，機械に把握されているプライバシ情報を，ユーザのプロファイルに基づくタイプごとに分類し，適正化するインタラクション，および適正化のためのユーザインタフェースを実現する機能である．この機能により，ユーザのプライバシに関する意図がシステムに反映されるようになる．具体的には，以下の 3 つの事項をユーザが把握した上で，各プライバシ情報により生じるリスクと，情報を提供することで受けることができるサービスの利益の間のトレードオフを考慮しながら，利益の最大化もしくはリスクの最小化を行うように，情報の削除やアクセス権の制御などを施すことを目指すものである．

- どのようなプライバシ情報が IoT 機器によって取得されたのか，またそのリスクは？
- 取得されたプライバシ情報に誰がアクセスできるのか，またそのリスクは？
- 取得されたプライバシ情報はどのように悪用されうるのか，またそのリスクは？

なお，本稿では，文献 [2] に示された手法により，リスク度合いの算出方法をパーソナライズ化することができていると仮定する．

2.3 プライバシ情報の分類

上記の機能（プライバシ情報の取得・可視化，およびプライバシ適正化のためのインタラクション）で対象となるプライバシ情報は，対象ドメインにより異なる．本稿では，スマートホームでのコミュニケーションロボットの利用を前提に，一般家庭における日常生活の場で取得可能な情報（非侵襲型のセンサーで取得できるものを対象とする）で，それがプライバシ情報になり得る情報を対象とする（文献 [2] の結果を利用する）．機械と人間のインタラクションはマルチモーダルに行われ，これをユーザにとって自然な形で実現するためには，インタフェースとして多種多様なセンサーとアクチュエータを搭載するコミュニケーションロボットが適している考えられるためである．

ここでは，文献 [7] をベースに，感情や社会的情報を付加した上で，ある情報から直接，または間接的に類推可能な情報を有向枝で結ぶことで，情報間の関係を明示した分類を行っている．分類結果を **図 2** に示す．これらの情報は階層的に分類され，各情報感は，直接類推可能な場合は実線で，間接的に類推可能な場合は点線で結ばれている．

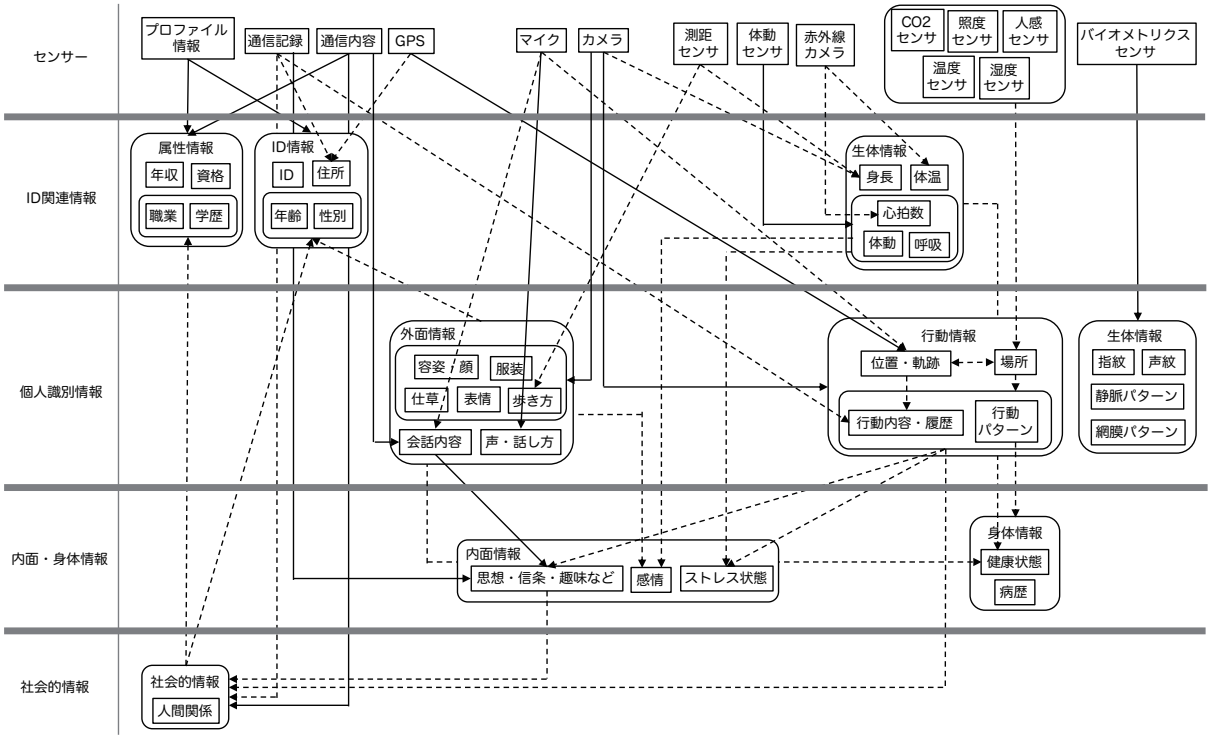

図 2 プライバシ情報となり得る情報の分類結果（文献 [2] より引用）．最上位はセンサーで直接計測されるデータである．ある情報から直接類推可能な情報は実線の矢印で，間接的に類推可能（データ統合，分析等により類推可能）な情報は破線の矢印で結ばれている．

例えば，マイクによる音響センシングの結果からは，声・話し方等の外面情報が直接取得可能であるが，音の発生源までの距離を分析することで移動軌跡が推定されるならば，間接的に行動情報の取得も可能であることになる．また，行動内容や行動パターンなどの行動情報は，他の情報と統合することで，人間関係等の社会的情報を類推可能であり，その結果，職業等，個人の属性情報が類推される可能性が出てくる．

3. ロボットアプリケーション

前述したフレームワークの検証を行うために，ロボットアプリケーションの設計を行う．以下，フレームワーク機能を含んだシステムの構成，およびアプリケーションのサービス内容について説明する．

3.1 システムの構成

フレームワークの 2 つの機能を実現するために設計したシステムの構成を **図 3** に示す [8]．システムは，ユーザと機械のインタフェースとなる IoT 機器（コミュニケーションロボット，タブレット PC，環境に配備される IoT 機器から成る），IoT サービスをユーサに提供するためのクラウド・エッジサービス，提供可能なプライバシ情報の設定を自然なインタラクションにより実現するためのプライバシ適正化サービスの 3 つの部分から成る．各部分に配備される機能モジュールを組み合わせることにより，ユーザへのサービス提供に加え，プライバシ情報の取得・可視化，およびインタラクションの各機能を実現する．

各機能モジュール間での処理の流れは以下のとおりである．まず，ユーザが IoT サービスを利用する場合，IoT 機器やロボットによるセンシング結果がプライバシ適正化モデルに従って分析され，プライバシ情報として蓄積されるとともに，IoT サービスが提供される．このとき，プライバシ情報は，適正化モデルに従い，ユーザにとっての適切な開示度に基づき利用・蓄積される．蓄積されたプライバシ情報は，ユーザ特性に応じて点数化・可視化がなされ，その結果がユーザに提示される．このときユーザは，機械との自然なインタラクションにより適正化モデルを更新する．このインタラクションの過程でユーザ特性をプロファイリングし，この結果を適正化モデルに反映する．

なお，本稿では，人と機械のインタフェースとして，コミュニケーションロボットとタブレット端末を組み合わせて利用する．コミュニケーションロボットとしては，テーブルトップサイズの普及型ロボットプラットフォームを用いることにする．ロボットの機能は以下のとおりである．

- 人間との音声対話機能
- カメラ・マイクでの環境情報の取得
- LED ライトによる感情表現
- 胴体 1 軸，腕 2 軸 × 2，首 3 軸の合計 8 自由度（移動機能は有しない）
- クラウドサーバや外部機器との連携

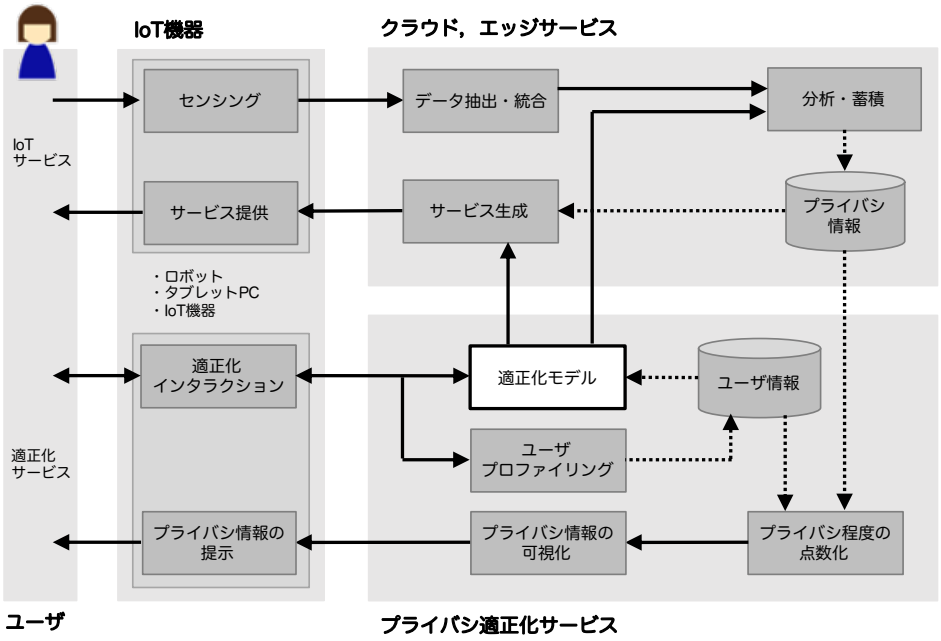

図 3 ロボットアプリケーションの構成（文献 [8] の図を一部変更）．システムは，ユーザと機械のインタフェースとなる IoT 機器，IoT サービスを提供するクラウド・エッジサービス，提供可能なプライバシ情報の設定を自然なインタラクションにより実現するためのプライバシ適正化サービスの 3 つの部分から成る．

3.2 設計結果

本アプリケーションは，プラットフォームの検証を目的とするため，設計にあたり以下の指針を策定した．

(1) プライバシ情報の提示，適正化インタラクション，IoT サービスの提供という 3 種類のインタラクションがすべて含まれていること．

(2) 適正化モデルにより，IoT サービスの提供内容が異なる複数種類のサービスが含まれていること．

これらの設計指針に基づき，3 種類の基本サービスと 1 種類のオプションサービスから成るロボットアプリケーションを設計した．いずれもスマートホームでの利用を前提に，ユーザ属性はユーザ情報として事前に取得されており，サービス提供時にはユーザを識別した上でユーザ属性が取得可能であるものとする．また，サービスごと，ユーザごとにプライバシ情報の開示度レベル設定が可能であり，各サービスは，ユーザグループ（情報リテラシの程度等）ごとに，ユーザ個人に依存しない平均開示度レベルを持つものとする．各サービスの概要を以下に示す．

基本サービス 1：
ロボットに「プライバシチェック」と話しかけると，タブレット端末経由でサービスごとのプライバシ情報開示度レベルを確認できる．ここでは，プライバシ情報とユーザ情報から，サービスごとに開示度を算出し，ユーザに提示する．

基本サービス 2：
ロボットに「プライバシチェック」と話しかけると，タブレット端末経由でサービスごとのプライバシ情報開示度レベルを変更できる．ここでは，サービスごとの開示度レベルの変更結果を適正化モデルに入力し，その結果に基づきユーザ情報を変更する．また，明示的な変更要求がなくても，他のサービスの変更結果に基づいて，該当サービスにおける開示度レベルの変更が推薦される場合もある．

基本サービス 3：
ロボットに「スケジュール」と話かけると，カレンダーアプリの情報を取得し，その日のスケジュールを知らせてくれる．これは，標準的な IoT サービスの例であり，ユーザの識別は顔認証で行い，クラウドサービスと連携することで，スケジュールを読み上げる．フレームワークにスケジュール情報を把握されるが，利便性が高いサービスである．

オプションサービス：
ロボットにあらかじめ設定しておいた言葉で話しかけると，顔画像から表情を認識することでその時点でのユーザの感情を推定し，タブレット端末からユーザの気分に合わせた音楽を流してくれる．これは，感情等，より多くのプライバシ情報が取得されるサービスの例である．顔認証，感情推定，音楽配信はクラウドサービスを利用する．

ここでは，基本サービス 1，2，3 により，3 種類のインタラクションを実現することにより，設計指針（1）を満たす．また，基本サービス 3 とオプションサービスにより，

適正化モデルが異なる複数サービスを含むことにより，設計指針（2）を満たす．

3.3 取得されるプライバシ情報

各サービスにおいて取得されるプライバシ情報は，図 2 に示す階層ごとにプライバシ情報の開示レベルを設定した場合，以下のようになる．なお，開示により以下の項目が必ず取得されるようになるわけではなく，「取得が可能になる」という状況である点に注意が必要である．

- センサー：マイク，カメラ
- ID 関連情報：ID 情報
- 個人識別情報：声・話し方，容姿・顔，表情，位置，場所，行動パターン
- 内面・身体情報：ストレス状態，感情
- 社会的情報：なし

4. 利用シナリオによる検証

4.1 シナリオの内容

本章では，3 章で設計したアプリケーションに対する利用シナリオを想定することにより，フレームワーク機能の有効性を検証する．ここでは，ユーザのタイプとして 3 種類を想定し，適正化インタラクションの前と後で，サービス内容およびプライバシ情報の開示度がどのように変わるかを検証する．ユーザのタイプは，情報リテラシが高くプライバシ情報の開示に対して厳格なユーザ，情報リテラシが高くプライバシ情報の開示に積極的なユーザ，情報リテラシが低くプライバシ情報の開示に対する意識が希薄なユーザの 3 種類である．

想定シナリオは以下を考える．

(1) 基本サービス 3 を実行する．
(2) 基本サービス 1 で，オプションサービスの開示度を確認する．
(3) 基本サービス 2 で，オプションサービスの開示度を変更する．
(4) 基本サービス 3 を実行する．
(5) オプションサービスを実行する．

4.2 検証結果

4.2.1 開示に厳格なユーザの場合

ユーザ属性として，情報リテラシが高く，情報開示に厳格なユーザの場合を考える．ここでは，厳格なユーザの平均的な開示度設定は，ID 関連情報までであると仮定する．シナリオ実行結果の一例として，平均的な開示度設定では利用できないオプションサービスの実行を希望し，開示度レベルを変えることとする．それに伴い，もともと利用できなかった基本サービス 3 の実行も可能になることを示す．具体的なシナリオは以下のとおりである．なお，以下の番号は，想定シナリオの番号と対応している．

(1) ロボットに「スケジュール」と話しかけると，平均的な開示度設定は ID 関連情報までであるので，顔画像による認証が行えず，基本サービス 3 は実行されない．
(2) ロボットに「プライバシチェック」と話しかけると，タブレット端末上でサービスの選択が可能になるので，オプションサービスを選択して設定内容を確認する．オプションサービスでは，内面・身体情報に分類される感情の推定が必要であるが，この情報は開示されていないので，サービスは実行されないことがわかる．
(3) そこで，タブレット端末上で，オプションサービスに対して感情情報の開示を選択する．それに伴い，顔画像の取得が行われるようになるため，フレームワークは，基本サービス 3 における顔画像データの開示度を変更することをユーザに提案する．
(4) ユーザがフレームワークの提案を受け入れた場合，基本サービス 3 は実行可能になる．
(5) オプションサービスに対しては，開示度を変更しているので，実行可能になる．

情報リテラシが高いユーザに対しては，設定の煩雑度を減らすために，開示に厳格なユーザに共通の設定をベースにしながら，IoT サービスの追加や削除に応じて，サービスごとのきめ細かな設定を実現する．

4.2.2 開示に積極的なユーザの場合

ユーザ属性として，情報リテラシが高く，開示に積極的なユーザの場合を考える．ここでは，開示に積極的なユーザの平均的な開示度設定は，内面・身体情報までであると仮定する．シナリオ実行結果の一例として，平均的な開示度設定では実行可能なオプションサービスに対し，感情情報の非開示を希望し，開示度レベルを変えることとする．このとき，基本サービス 3 はこの変更の影響を受けないことを示す．具体的なシナリオは以下のとおりである．

(1) ロボットに「スケジュール」と話しかけると，平均的な開示度設定は内面・身体情報までであるので，顔画像による認証が行われ，基本サービス 3 は実行される．
(2) ロボットに「プライバシチェック」と話しかけると，タブレット端末上でサービスの選択が可能になるので，オプションサービスを選択して設定内容を確認する．サービスは実行可能であるが，内面・身体情報に分類される感情の推定が必要であることがわかる．
(3) そこで，タブレット端末上で，オプションサービスに対して感情情報の非開示を選択する．この変更は基本サービス 3 には影響しないため，フレームワークはオプションサービスに対する開示度のみを変更する．
(4) 基本サービス 3 は実行可能である．
(5) オプションサービスに対しては，開示度を変更しているので，実行できなくなる．

情報リテラシが高いユーザに対しては，設定の煩雑度を減らすために，開示に積極的なユーザに共通の設定をベー

スにしながら，プライバシ情報の追加や削除に応じて，情報ごとのきめ細かな設定を実現する．

4.2.3 開示に対する意識が希薄なユーザの場合

ユーザ属性として，プライバシ情報の開示に対する意識が希薄なユーザの場合を考える．ここでは，意識が希薄なユーザの平均的な開示度設定は，個人識別情報までであると仮定する．シナリオ実行結果の一例として，平均的な開示度設定では利用できないオプションサービスの実行を希望し，開示度レベルを変えることとする．意識が希薄なユーザの場合は，原則，平均的な開示度を設定し，変更の自由度は低いが，サービスを限定して変更が許可される状況を示す．具体的なシナリオは以下のとおりである．

(1) ロボットに「スケジュール」と話しかけると，平均的な開示度設定は個人識別情報までであるので，顔画像による認証が行われ，基本サービス 3 は実行される．
(2) ロボットに「プライバシチェック」と話しかけると，タブレット端末上でサービスの選択が可能になるので，オプションサービスを選択して設定内容を確認する．オプションサービスでは，内面・身体情報に分類される感情の推定が必要であるが，この情報は開示されていないので，サービスは実行されないことがわかる．
(3) そこで，タブレット端末上で，オプションサービスに対して感情情報の開示を選択する．ただし，意識が希薄なユーザの場合は，変更は該当サービスに対してのみ適用される．
(4) 基本サービス 3 は実行可能である．
(5) オプションサービスに対しては，開示度を変更しているので，実行可能である．

4.2.4 考察

以上のように，ユーザ種別，および要求する開示レベルを設定することにより，ユーザの特性に応じた適正化モデルの更新が可能になることが確認できた．適正化モデルの更新方法（利便性とリスクを考慮した開示度の決定方法），具体的なインタラクションの方法（自然なインタラクション，インタフェース等）については今後の検討課題である．

5. おわりに

本稿では，ロボットアプリケーションを構築することで，フレームワークの有効性を検証した．具体的には，利用シナリオを提示することにより，フレームワーク機能の実現可能性を検証した．今後，アプリケーションの実装とそれを用いた評価実験を行う予定である．

謝辞 本研究は，JSPS 科研費 17KT0080 の助成を受けたものである．

参考文献

[1] Yasumoto, K., Yamaguchi, H. and Shigeno, H.: Survey of Real-time Processing Technologies of IoT Data Streams, *Journal of Information Processing*, Vol. 24, No. 2, pp. 195–202 (2016).
[2] 菅沼拓夫，安本慶一，加藤由花：セキュア IoT サービスに向けた人と機械の信頼関係構築フレームワークの基本構想，情報処理学会研究報告 DPS175，pp. 1–7 (2018).
[3] 萱場啓太，生出拓馬，阿部　亨，菅沼拓夫：利用者の多様性を考慮したパーソナルデータ流通制御支援手法，信学技報 IN，Vol. 117, No. 205, pp. 1–6 (2017).
[4] Ito, F., Ozawa, E. and Kato, Y.: Design of Robot Service Functions for a Framework Establishing Human-Machine Trust, *Proc. AINA 2019*, pp. 1193–1204 (2019).
[5] Agarwal, Y. and et al.: ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing, *Proc. MobiSys'13*, pp. 97–110 (2013).
[6] Liu, R., Cao, J., Yang, L. and Zhang, K.: Recommendation for Privacy Settings of Mobile Apps Based on Crowdsourced Users' Expectations, *Proc. IEEE MS 2015*, pp. 150–157 (2015).
[7] 馬場口登，西尾修一：ネットワークロボットのセンシングとプライバシー保護技術，信学会誌，Vol. 91, No. 5, pp. 380–386 (2008).
[8] 伊東風弥，加藤由花：人と機械の信頼関係構築フレームワークでの利用を前提としたロボットサービス機能の設計，情報処理学会 DICOMO2018，pp. 981–986 (2018).