Vol.2018-DPS-175 No.38
Vol.2018-MBL-87 No.38
Vol.2018-ITS-73 No.38
2018/5/25

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

菅沼 拓夫[1,a)]　安本 慶一[2]　加藤 由花[3]

概要：本研究では，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を実現することを目的とする．具体的には，ロボット，IoT機器，新世代ネットワークを高度に融合することで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の構築を目指す．本フレームワークを実現するため，A) プライバシ情報の取得・可視化，B) プライバシ適正化のためのインタラクション，C) コミュニケーションロボットへの応用，の3つの研究項目を掲げ，それぞれの解決手法を探求することにより，これらの要素技術が人間と機械の関係性に与える影響について明らかにする．本発表では当該フレームワークの基本構想について述べる．

1. はじめに

あらゆるモノをネットワークに接続するInternet of Things (IoT) 技術が登場し，世界中でサイバー・フィジカルシステム (CPS) の研究開発が進められている．米シスコシステムズは，2020年までに，500億個のモノがネットワークに接続され，14兆円もの市場になると予測している．IoT技術は，現在の人間社会を根本から変革する可能性を秘めているが，多くの未解決課題を残している．

その中でも，IoT機器が生成するデータストリーム（「情報流」と呼ぶ）の実時間での流通・利活用と，情報流利活用時における安全・安心の保証は，クラウドに対しThingsに近い末端サイドで処理を行うエッジコンピューティングが注目される中，最も重要な課題の一つとなりつつある．しかしながら世界的に見てもこの点に着目して組織立った研究開発を進める研究コミュニティは数少なく，特に安全・安心な情報流に関する研究開発はいまだ萌芽期である．

IoT機器からは，プライバシ情報として，位置情報に加え，画像・音声情報，生体情報，テキスト情報等がネット上に流通する可能性がある．一般のユーザにとって，提供した情報の利用のされ方，流通範囲が不明なため，情報の提供には抵抗があり，IoTデータ流通の阻害要因となっている．さらに，人がIoT機器とインタラクションする際に，何がセンシングされているのか分からないことも問題である．一方で，人と人のインタラクションにおいては，人は意外にも，プライバシ情報や機微情報をあっさり公開してしまうことも多い．これは，人と人のインタラクションでは，信頼関係がすでに構築されていて情報の秘匿が守られる安心感があり，また，人は聞いたことをすぐに忘れるという点が考慮されるからである．以上のことから，IoTデータ（情報流）の広い流通・利活用のためには，人と機械（IoT機器）の間の信頼関係構築が不可欠であると言える．

前述の情報流に関しては，その活用の課題解決に焦点を当て，安本を中心に，世界に先駆けて「情報流プロジェクト」を結成し，2014年から活動を続けている [1], [2], [3]．また菅沼は， CPSの研究潮流に先行して2003年より現実空間とサイバー空間の共生に関する研究開発を推進しており [4]，近年では総務省SCOPE国際連携プロジェクト [5] 等で，IoTにおけるプライバシ情報の流通に関する研究を進めている．また，加藤は，ネットワークロボットと人とのインタラクションの研究を推進している [6]．以上の研究経験と実績から，IoTの真の普及のためには，情報提供者である人と情報の管理・流通を行う機械の間で信頼関係を構築できる仕組みが最も重要との共通認識に至っている．

本研究では，ロボット，IoT機器，新世代ネットワークを高度に融合することで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の構築を目指す．特に情報流の発生源周辺においては，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

[1] 東北大学 サイバーサイエンスセンター
Cyberscience Center, Tohoku University, Sendai, Miyagi 980–8578, Japan
[2] 奈良先端科学技術大学院大学 先端科学技術研究科
Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma, Nara 630–0192, Japan
[3] 東京女子大学 現代教養学部 数理科学科
School of Arts and Sciences, Tokyo Woman's Christian University, Suginami, Tokyo 167–8585, Japan
[a)] suganuma@tohoku.ac.jp

ⓒ 2018 Information Processing Society of Japan

Vol.2018-DPS-175 No.38
Vol.2018-MBL-87 No.38
Vol.2018-ITS-73 No.38
2018/5/25

が良好でないと，サービス利用の安心感・信頼感が損なわれ，十分なサービスを享受できない．そこで本研究では，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を研究開発する．具体的には，A) プライバシ情報の取得・可視化，および，B) プライバシ適正化のためのインタラクションにより，IoT機器がどのような情報を情報流として流しているかの状況を人間・機械協調系として処理することで，人の安心感の増幅を試みる．また，これらの技術の有効性を実環境で検証するため，C) コミュニケーションロボットへの応用を想定しつつ，実環境での実証実験と評価を通じてその有用性，実現可能性，効果等について明らかにする．

本稿では，当該フレームワークの基本構想として，研究の方向性，期待される貢献，それぞれの研究課題とその解決手法の概要等について述べ，さらに現在までの研究の進捗状況について紹介する．

2. 提案フレームワークの概要

2.1 研究課題の設定

本研究では，人と機械の信頼関係を構築することを目的に，以下の技術課題を設定する (図 1)．

課題１： 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ユーザに自然な形で提示するか

課題２： 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

上記の技術課題を解決できれば，ユーザがどれだけのプライバシ情報が既にセンシングされているのかを把握しながら，IoT機器との自然なインタラクションにより，適正な範囲に調整することができ，人と機械（IoT機器）の信頼関係を構築できるという仮定をおく．

課題1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．課題2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．

2.2 研究項目

上記を踏まえ，本研究では，以下の3つの研究項目：A) プライバシ情報の取得・可視化，B) プライバシ適正化のためのインタラクション，C) コミュニケーションロボットへの応用，を設定する．本研究では，家庭における日常生活を対象とし，家庭での生活を支援するコミュニケーションロボットに提案手法を適用することを想定した研究を実施する．

2.2.1 プライバシ情報の取得・可視化

本研究項目では，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，可視化する手法を開発する．点数化・可視化によりユーザのプライバシに関する意図が正確に表現されることを達成目標とする．

2.2.2 プライバシ適正化のためのインタラクション

本研究項目では，研究項目Aにより機械に把握されているプライバシ把握情報を，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法，および適正化のためのユーザインタフェースを開発する．適正化によりユーザのプライバシに関する意図の反映度が向上することを達成目標とする．

2.2.3 コミュニケーションロボットへの応用

本研究項目では，身体性をもつコミュニケーションロボットを利用し，研究項目A,Bの機能を対話的に実行可能なロボット機能を設計・実装して，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を構成する．研究項目A,Bの機能をロボットに装備することによって，信頼関係がどの程度変化するかを検証する．

2.2.4 実証実験

実験環境として，奈良先端大学に設置されているスマートホーム実験設備（1LDKの住環境）を用い，提案手法を実装したコミュニケーションロボットを配置して，実際の住環境において実証実験を行う．最終的に，ロボットとの信頼関係がどの程度構築されたかを調査する．

2.3 貢献

セキュリティやプライバシに関する研究分野においては，暗号化やk-匿名化等の技術的な手法に関する研究が盛んに行われているが，ユーザの観点からその安全性に対する感覚的な安心感・信頼感の向上にアプローチする研究例は少ない．本研究では工学的なアプローチによってプライバシ情報，機微情報の開示度を定量化・可視化し，不確実・不安定な人の感情をパラメータとして処理可能とする「Human-in-the-loop」の考え方の導入によってユーザの感覚に合った情報開示度を人・機械協調系で決定する点が学術的な特徴である．これにより人と機械の間の信頼性を構築できれば，IoTにおける情報流通の阻害要因の排除となるだけでなく，技術的特異点問題など，人とロボットの共生に関わる将来的な課題に対してもブレークスルーとなる可能性があり，将来の情報社会に対して大きなインパクトを与えることが期待できる．

ⓒ 2018 Information Processing Society of Japan

Vol.2018-DPS-175 No.38
Vol.2018-MBL-87 No.38
Vol.2018-ITS-73 No.38
2018/5/25

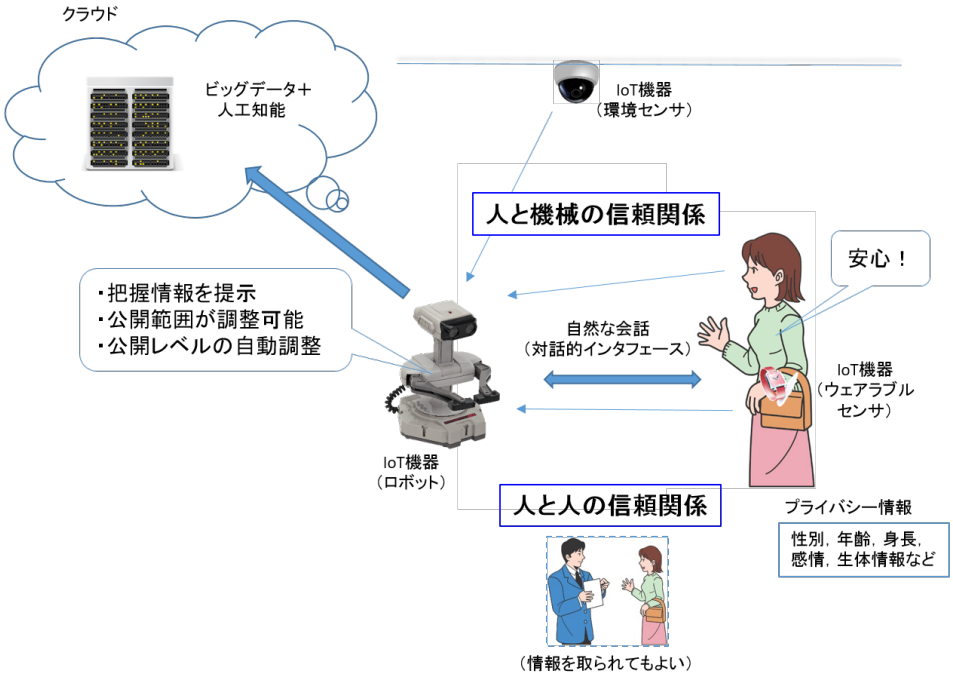


図 1　人と機械の信頼関係構築フレームワークの概要

3. プライバシ情報の取得・可視化

3.1 概要

プライバシ情報の取得や可視化，および研究項目 B) プライバシ適正化のためのインタラクションに関する研究の一部として，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) 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も考慮した適切な設定を推薦する手法について検討した [7].

サービス事業者が提供する各種サービスの利用時には，ユーザは自らの個人情報 (PD) について，属性ごとにそれぞれ公開の可否を指定するが，サービスが多岐にわたりかつ多数となり，属性数も増えるにしたがって，適切な PD の開示度設定が困難になる．本機能は，ユーザが指定した PD の公開の可否の適正度について評価し，適正でない場合はユーザに修正案を可視化し，推薦提示する．この機能によるユーザの心理的な信頼感と，研究項目 B で開発中のユーザインタフェースによる表層的な安心感の相乗効果により，人と機械の信頼関係をより高めることが可能になると考えられる．

3.2 設定の一貫性に基づく情報リテラシ推定と開示度設定の調整

多様なユーザに対して効果的な PD の流通支援を可能とするため，PD の公開度に関する設定履歴から求めた設定の一貫性に基づき情報リテラシを推定し，推定した情報リテラシに応じて平均化と個人化の程度を調整した設定（調整設定）を推薦する手法を提案する（図 2）.

提案手法は，まず，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でき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を推定する．次に，情報リテラシの程度に応じて適切な設定を推薦する．具体的には，情報リテラシの低いユーザに対しては，他のユーザが行う安心な設定となるよう平均化の程度を高め，情報リテラシの高いユーザに対しては，個人の好みを反映した快適な設定となるよう個人化の程度を高めた調整設定を推薦する．

3.3 シミュレーション結果

提案手法を評価するため，ユーザ，PD 属性，サービス事業者，支援手法を構成要素とする PD 流通制御シミュレータを実装した．シミュレータでは，まず，事業者がユーザに対して PD 提供を要求する．次に，支援手法がユーザに

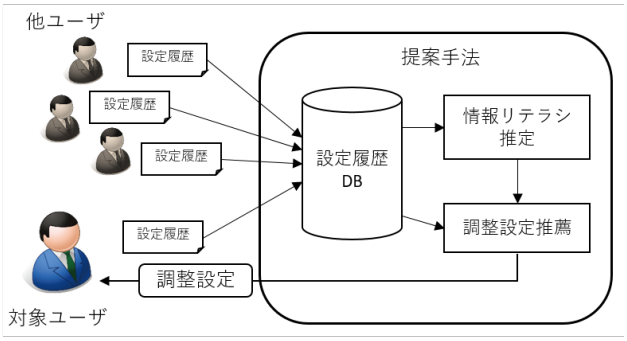


図 2　ユーザの多様性を考慮した PD の公開度設定支援手法の概要

ⓒ 2018 Information Processing Society of Japan

Vol.2018-DPS-175 No.38
Vol.2018-MBL-87 No.38
Vol.2018-ITS-73 No.38
2018/5/25

対して設定を推薦する．最後にユーザは，推薦設定を利用するのか，自身で設定するのかを選択し，設定を実施する．ユーザそれぞれに [0.0,1.0] の範囲で情報リテラシの程度 (θ) を割り当てており，情報リテラシが低いユーザほど一貫性のない設定を実施する．

PD 流通制御シミュレータによるシミュレーション実験により，提案手法の有効性を確認した．具体的には，既存研究 [8] を参考にして実装した平均化に基づく推薦手法 (平均設定推薦手法)，既存研究 [9] を参考にして実装した個人化に基づく推薦手法 (個人設定推薦手法)，および提案手法のそれぞれが推薦する設定を比較し，評価した．

評価指標として，ユーザに割り当てた情報リテラシと提案手法が推定した情報リテラシが一致している程度を示す AI，支援手法が推薦した設定が平均的な設定との一致率 CA，ユーザ自身が行った設定との一致率 CP を用いた．情報リテラシの低いユーザに対して CA が高く，情報リテラシの高いユーザに対して CP が高いほど，提案手法が平均化と個人化の程度を適切に調整できていることを意味する．

図 3 より，情報リテラシが低いユーザに対して，平均設定推薦手法には及ばないものの，提案手法が高い CA を示したことを確認した．また図 4 より，情報リテラシが高いユーザに対して，提案手法が個人設定推薦手法と同程度の高い CP を示したことを確認した．以上より，提案手法が高い精度で情報リテラシを推定でき，推薦する設定の平均化と個人化の程度を適切に調整できることを確認した．

3.4 考察

本提案手法は，主にユーザに対して PD の公開/非公開に関する設定の推薦を行うものであり，その推薦に応じてユーザが適正な設定変更を行うことを前提とした，設定の半自動化を目指したものである．しかしながら PD 設定は，サービス事業者の PD の扱いに関する評判や，セキュリティインシデントによる影響，PD の公開に関する一般認識の変化等，社会的な PD に関する情勢に敏感に反応しながら成されるものである．従って，PD の公開/非公開といった微妙な判断をその時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．この点に関しては，研究項目 A の可視化のみでは不十分であり，4 章で述べる研究項目 B のプライバシ適正化のためのインタラクションの技術により補っていく必要がある．

4. プライバシ適正化のためのインタラクション

4.1 解決すべき課題

本章では，IoT 機器が取得したプライバシ適正化のためのユーザインタフェースについて述べる．

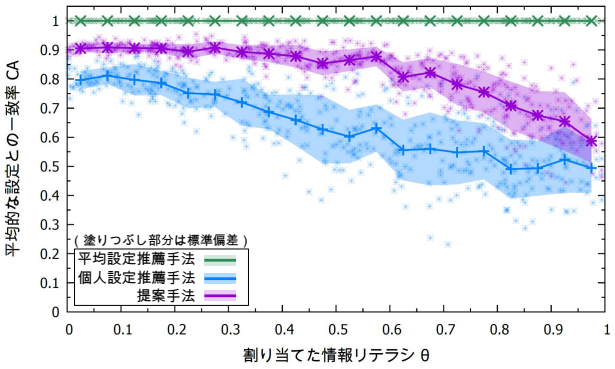


図 3　平均的な設定との一致率 CA の結果

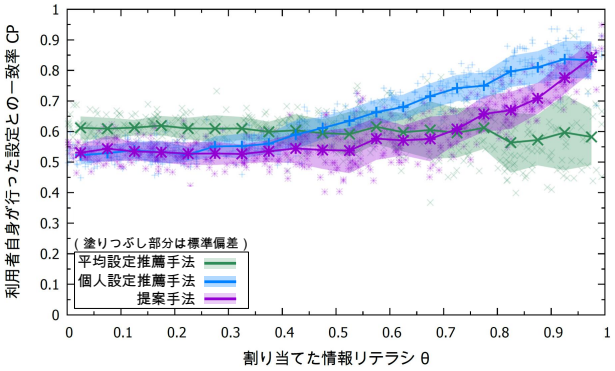


図 4　ユーザ自身が行った設定との一致率 CP の結果

プライバシ情報を適正化するには，IoT 機器のユーザは，以下の 3 つの事項について知っておく必要がある．

Q1: 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？

Q2: 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？

Q3: 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？

その上で，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，アクセス権の制限などを施すことが望ましい．

4.2 提案するユーザインタフェース

本稿では，前節の Q1:「どのようなプライバシー情報が IoT 機器によって取得されたのか．またそのリスクは？」，を対象に，リスクを最小化するためのインタラクションを可能にするユーザインタフェースを提案する．Q2，Q3 を対象としたインタラクションの設計は今後の課題である．

Q1 を扱うためのインタフェースへの要求事項として，以下を設定した．

R1: どの IoT 機器がどんな情報を取得しているかが把握できる．

ⓒ 2018 Information Processing Society of Japan

Vol.2018-DPS-175 No.38
Vol.2018-MBL-87 No.38
Vol.2018-ITS-73 No.38
2018/5/25

R2: 各情報についてプライバシリスクはどの程度なのかを把握し，対応策を施す．
R3: 多数の IoT 機器が広範囲に設置されていても，高リスクの IoT 機器，情報に容易にアクセスできる．
R4: 高リスクの IoT 機器，情報にどう対処したら良いかがわかる．

上記要求事項 R1–R4 を満たす，プライバシ情報適正化インタフェースを提案する．

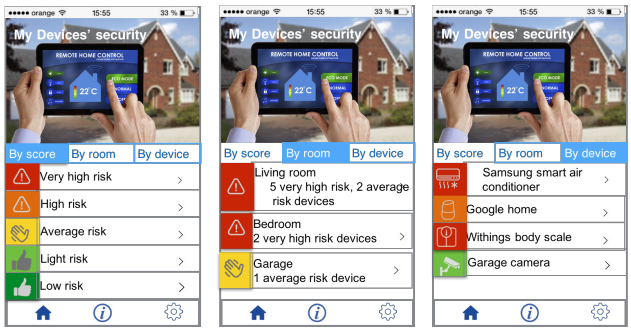


図 5　ユーザインタフェース：カテゴリ別ビュー

図 5，6 に，提案するユーザインタフェースの画面例を示す．なお，5 章で述べるように，将来的には，画面だけでなく音声なども併用するマルチモーダル・ユーザインタフェースに発展させることを想定している．

要求事項 R3，R4 を満たすため，提案するインタフェースでは，全ての IoT 機器に対し，リスク度合いを表すスコアを算出・付与し，リスク度合い別（図 5 左），部屋別（図 5 中央），機器別（図 5 右）のビューを提供する．

R1，R2 に対応するため，図 5 の画面でカテゴリを選択することで（この例では，Very high risk を選択），カテゴリに属する IoT 機器別のリスク度合いとデバイスのおすすめ設定例を表示する（図 6 左）．さらに，リストから個々の IoT 機器を選択することで（例では，Air conditioner を選択），収集されている情報の詳細（情報取得頻度，期間，共有先状況など）を表示する（図 6 右）．また，現在の情報取得方法（頻度，共有先など）を変更し，リスク度合いを再計算・表示する機能，自動算出されたリスク度合いを，自身が納得するリスク度合いに変更することで，算出方法をパーソナライズする機能を提供する．

4.3　リスク度合い（スコア）算出法のパーソナライズ

一般に，IoT 機器が取得するユーザのプライバシ情報のリスク度合いは，個々人によって異なってくると考えられる．例えば，体重計の情報を家族・友人に公開することに，抵抗のある人と無い人が存在し得る．そこで，提案手法では，以下のアプローチにより，リスク度合いの算出法をパーソナライズすることを検討している．

- IoT 機器 d が取得する情報種類の集合 I_d について，リスク度合い算出関数 $\forall i \in I_d, R(d, i, C_i)$ を定義する．

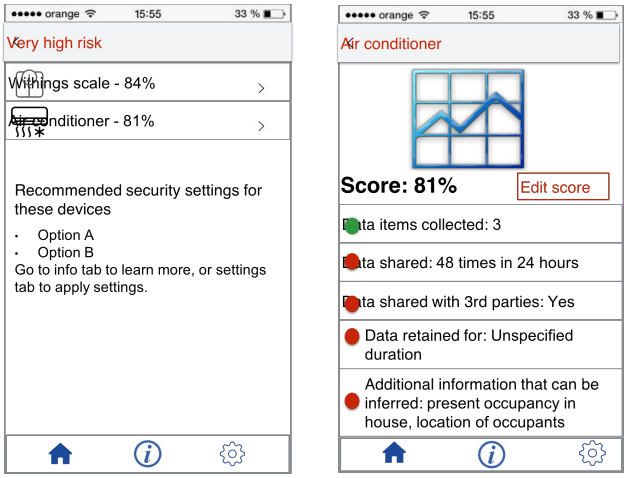


図 6　ユーザインタフェース：詳細ビュー

ここで，C_i は，情報 i に対するリスク度合いをパーソナライズする重み係数の集合である．

- 4.2 節において，ユーザがリスク度合いを変更した IoT 機器を d^*，情報 i に対する変更後のリスク度合いを $R^*(d, i)$ とする．
- $\forall i \in I_d, R(d, i, C_i^*) = R^*(d, i)$ となるよう，重み係数集合 C_i を C_i^* に更新する．

5.　コミュニケーションロボットへの応用

5.1　概要

提案するフレームワークを検証するために，本研究では，身体性を持ったコミュニケーションロボットを利用し，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）を対話的に実行可能なロボット機能を設計・実装する．これは，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と考えられるためである．

前述したプライバシ適正化を効率的に支援する手法 [7] においては，シミュレーション実験により利用者の多様性を考慮した効果的な支援が可能であることを検証しているが，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，本稿では，実環境（家庭における日常生活を対象とする）における実証実験によりフレームワークの検証を行う．ここでは，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（以降，ロボットアプリケーションと呼ぶ）を構成することで，提案フレームワークにより，人と機械の信頼関係がどの程度変化するかを調査する．本章では，このロボットアプリケーションの設計結果を示す．

ⓒ 2018 Information Processing Society of Japan

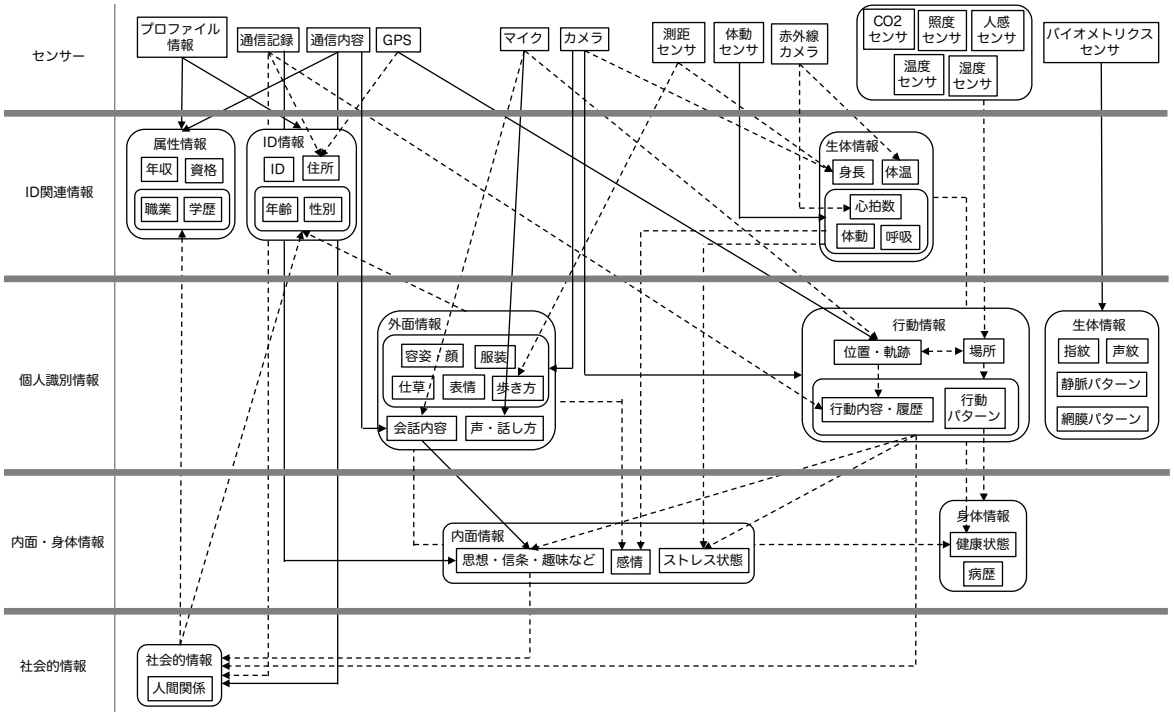


図 7 プライバシ情報となり得る情報の分類結果．最上位はセンサで直接計測されるデータである．ある情報から直接類推可能な情報は実線の矢印で，間接的に類推可能（データ統合，分析等により類推可能）な情報は破線の矢印で結ばれている．

5.2 プライバシ情報の分類

ロボットアプリケーションの設計にあたって，まず，一般家庭における日常生活の場で取得可能な情報（非侵襲型のセンサで取得できるものを対象にする）で，それがプライバシ情報になり得る情報を抽出する．これまでも，例えば文献 [10] において，個人情報ないしはプライバシ情報を ID 情報，ID 関連情報，個人識別情報，内面情報に分類し，各情報に対応する情報処理技術との関係を示した例などが存在する．本稿では，これらの情報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た．結果を **図 7** に示す．これらの情報は階層的に分類され，各情報間は，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．

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．

このように，この分類結果を用いると，階層間の矢印をたどることで取得可能なプライバシ情報を知ることができる．また，グラフ探索の範囲を指定することにより，機械に提供するプライバシ情報の範囲を指定することができるようになる．

5.3 システムの構成

次に，前節で抽出したプライバシ情報を収集し，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ロボットアプリケーションを設計する．システム構成を **図 8** に示す．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 サービスをユーザ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．

ここでは，IoT 機器やロボットによるセンシング結果は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・利用される（ 図 8 における，センシング→データ抽出・統合→分析・蓄積の部分）．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（ 図 8 における，点数化→可視化→提示の部分）．この時ユーザは，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し（同時にインタラクションによりユーザプロファイリングされ），その結果がプライバシ適正化を支援する（ 図 8 における，適正化インタラクション←→適正化モデル→分析・蓄積の部分）．前節の分類結果は，プライバシ情報の提示，および適正化モデルの部分に組み込み，これらのプライバシ情報

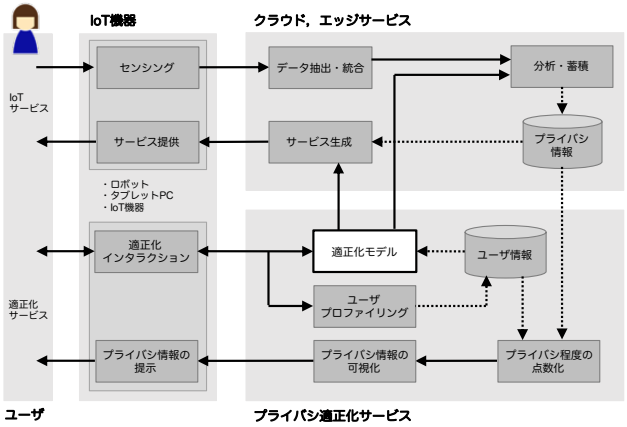


図 8　実験システムの構成．システムは，ユーザと機械のインタフェースとなる IoT 機器，IoT サービスを提供するクラウド・エッジサービス，提供可能なプライバシ情報の設定を自然なインタラクションにより実現するためのプライバシ適正化サービスの 3 つの部分から成る．

を，家庭内で共有可能，友人や近所の住人と共有可能，誰でも共有可能というように，公開可能範囲を容易かつ直感的に適正化できるようにする．

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．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

ここでは，このロボットをタブレット端末と組み合わせることで，人と機械のインタフェースとして用いる．また，環境側に配備する IoT 機器により，プライバシ情報として抽出した各種センサデータを取得する．具体的には，ユーザの感情や気分を読み取り，照明の明るさを調整する，窓を開ける等のサービス機能を設計することで，定義したプライバシ情報を収集するロボットアプリケーションを実現する．

5.4　スマートホームでの実験

今後，設計したロボットアプリケーションを用いて，被験者が家で生活する環境で，いかにプライバシを適正化しながらロボットと共同生活が可能かを実証する．具体的には，奈良先端科学技術大学院大学に設置されているスマートホーム実験設備（1LDK の住環境）に，各種センサ・コミュニケーションロボットを設置し実験環境を構築する．そして，数名の被験者に実際に生活してもらうシナリオを設計し，被験者がどの程度プライバシ情報をセンシングされていたかを把握でき，センシングされたプライバシ情報の公開範囲をいかに自然な形で（小さな負担で）調整できたか，ロボットの信頼関係がどの程度構築されたかを調査する．

6.　おわりに

ロボット，IoT 機器，新世代ネットワークを高度に融合することで，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，次世代情報流基盤のためのフレームワークを提案した．本発表では，特に当該フレームワークの基本構想と，現在までの研究の進捗状況について焦点を当て紹介した．今後は研究項目ごとに計画に沿って研究開発を推進し，実証実験を通じてその有効性を検証していく．

謝辞　本研究は，JSPS 科研費 17KT0080 の助成を受けたものである．また，日頃の議論により様々なアイデアや知見を与えてくれる情報流プロジェクトメンバー各位に感謝する．

参考文献

[1] Yasumoto, K. and et al.: 情報流プロジェクト，`www.infoflow.org`.
[2] Yasumoto, K. and et al.: Survey of Real-time Processing Technologies of IoT Data Streams, *JIP*, Vol. 24, No. 2, pp. 195–202 (2016).
[3] Yasumoto, K. and et al.: International Workshop on Information Flow of Things, `https://ubi-s13.naist.jp/ifot2016/`.
[4] 菅沼拓夫他：Symbiotic Computing －ポスト・ユビキタス情報環境へ向けて－，情報処理学会誌， Vol. 47, No. 8, pp. 811–816 (2006).
[5] iKaas Project: iKaaS, `http://ikaas.com/`.
[6] Kato, Y.: A Remote Navigation System for a Simple Tele-presence Robot with Virtual Reality, *Proc. IEEE/RSJ IROS2015*, pp. 4542–4529 (2015).
[7] 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).
[8] Agarwal, Y. and et al.: ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing, *Proc. MobiSys'13*, pp. 97–110 (2013).
[9] 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).
[10] 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).

ⓒ 2018 Information Processing Society of Japan