空間軸を限定したプライバシー情報保護活用基盤

Space Bounded Protection and Utilization of Privacy Information

馬場口 登（大阪大学）
Noboru Babaguchi (Osaka Univ.)

1. はじめに

プライバシー情報は，適正に保護すべきものであるが，情報推薦やサービス提供におけるその有用性は論を俟たない．このためにプライバシー情報を保護しつつ適切に開示する枠組が必要となる．しかしながら，いかなる時，いかなる場所において，プライバシー情報を開示するのは不可能である．そこで我々は，空間的に限定されたフィールド（駅，テーマパーク，商業施設など）において，プライバシー情報の開示と開示によってこそ得られる利得のバランスを着目する．以下では，フィールドに対して形成される実空間とサイバー空間がリンクされた情報基盤の一種である調和的情報フィールド (Harmonized Information Field: HIFI)[1]の概略，およびその中心となるプライバシー情報の収集，管理について述べる．

2. HIFI の概要

HIFI では，ID と結びつけられた人間に関する種々の情報，すなわち顔，容姿，服装，動作，移動履歴，位置軌跡，嗜好，興味などを広義のプライバシー情報と捉える．これらのプライバシー情報を能動的あるいは受動的なセンシングによって収集し，時空間軸で集積・構造化し，構造化された情報のプライバシー保護を行い，種々の立場からプライバシー情報を有効活用する．

図１のように，HIFI とユーザ（HIFI への来場者）との界面は，「プライバシー情報の開示」と「上質な情報の提示」である．そのために，センシングを通して開示されたプライバシー情報が安心して集積され，有効活用されることにより，ユーザに上質な情報をフィードバックするメカニズムの構成が不可欠となる．HIFI では，プライバシー情報の収集提示，保護，集積・構造化，活用というプロセスに分け，プライバシー情報の処理を進める．

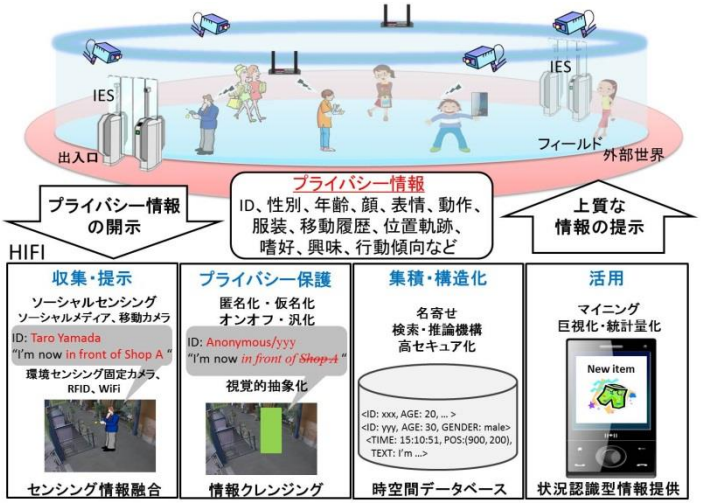

図１　HIFI の概要

3. 情報エントリーシステム

HIFI と外部世界の境界に，入退場のためのゲートとなる情報エントリーシステム(Information Entry System: IES)[2]を設ける．IES を通じて，ユーザは，自身のプライバシー情報を差し出し，その開示レベルを設定することにより，HIFI にプライバシー情報管理の同意を与えるという重要なプロセスを実行する．

図２のように IES は，中央のタッチモニタ，その上部に取り付けられたカメラ，そしてタッチモニタの左右に設置された Kinect によって構成される．IES は対話的に顔や衣服などの外見情報，年齢や性別などの属性情報を収集する．収集されたプライバシー情報は，過去の来場時に収集されたプライバシー情報との対応付けを行うために利用される．ユーザは HIFI に対する入退場時に必ず IES を通過するため，ユーザへの負荷が大きくならないように設計する．

まず，ユーザは外部世界側から入場し，タッチモニタの前に移動する．次に，ユーザはユーザ種別をタッチモニタ上で選択し，これによってプライバシー情報の開示度をユーザ自身が決定する．その後，ユーザは HIFI 側を通って入場する．一方，退場時は，HIFI 側から外部世界側に移動しながら，記録されたプライバシー情報を保存するか，破棄するかを決める．

ユーザ種別は[実名]，[仮名]，[匿名]の三つを想定する．[実名]は外部世界と HIFI の両方で個人同定され，[仮名]は HIFI では同定されるが，外部世界では同定されない．[匿名]は何れでも一切同定されない．[実名]の場合，外見情報（顔，服装）が収集され，データベースに保持される．[仮名]の場合，外見情報は収集されるものの，入場から退場までの間でのみ使用され，その間の行動情報（移動履歴）などを保存するか，退場時に決める．[匿名]では，IES 及び HIFI 内で収集されるプライバシー情報は直ちに破棄される．

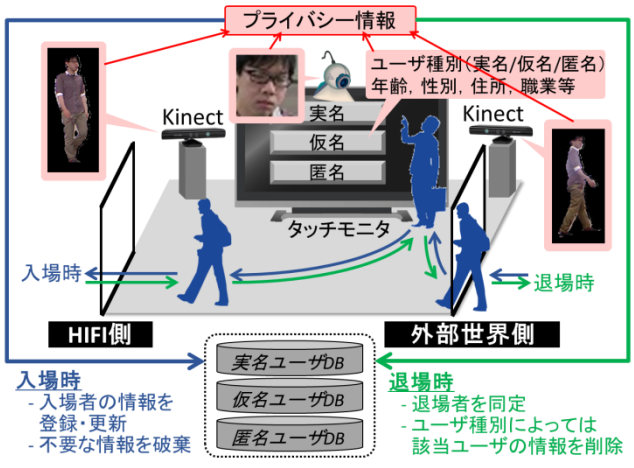

図２　IES

ここで IES に実装されている外見情報の収集法について述べる．IES 内をユーザが通過する間，Kinect は深度画像を用いて背景差分をとることにより，連続的に人物検出および人物領域の抽出を行う．抽出された人物領域とそのカラー情報を基に，ユーザの服装情報をカラーヒストグラムとして記録する．一方，タッチモニタ上のカメラから，ユーザがユーザ種別を選択するときに顔検出アルゴリズムを用いて正面顔を顔情報として収集する．

ユーザ種別の選択ボタンの表示位置について，以下の二つの工夫を行い，個人同定の精度向上およびユーザへの負荷軽減を図る．一つは，カメラに近いタッチモニタの上部に[実名]ボタンを配置することである．ユーザはユーザ種別を選択する際，無意識にタッチモニタに顔を向けるとともに，ボタンをタッチするとき，カメラに対して正面を向くと考えられるため，ユーザに明示的な指示を与えることなく，同定に有用な正面顔を収集することができる．もう一つは，ユーザの身長を推定し，その結果を選択ボタンの表示位置に反映することで，ユーザの身長に合わせた押しやすい位置に表示する．身長推定は，人物領域の高さと Kinect-ユーザ間の距離の相関を回帰分析により行う．

4. ユーザ種別ごとのプライバシー情報の保護

HIFI 内では様々なユーザ種別を許容するため，収集したプライバシー情報の利用に際してどのように保護するかが問題となる．そこで，１）ユーザ種別の設定によるプライバシー情報の選択的収集，２）ユーザ種別毎のプライバシー情報の匿名化処理を行う[3].

まず，１）について，収集するプライバシー情報を，個人の属性情報（年齢，性別など），および個人の行動情報（移動履歴など）に分類する．さらに行動情報は，時間軸により当日限りに取得を限定するか，限定せず複数日にわたり取得するかにより分類する．また，HIFI でのユーザ ID と外部世界の個人 ID が一意に結び付くかどうかを表す ID 可到達性に基づき分類する．ここでは，表１の通り，[仮名]を三つに分け，[実名]，[仮名１]，[仮名２]，[仮名３]，[匿名]という５種類の種別を設定し，種別に応じて収集する情報を変化させる．

表１　ユーザ種別毎の収集情報

ユーザ種別	当日限りの行動情報	複数日の行動情報	属性情報	ID 可到達性
実名	あり	あり	あり	あり
仮名１	あり	あり	あり	なし
仮名２	あり	あり	なし	なし
仮名３	あり	なし	なし	なし
匿名	なし	なし	なし	なし

次に，２）ユーザ種別毎のプライバシー情報の匿名化処理について述べる．[仮名１]，[仮名２]，[仮名３]のユーザに対しては，収集したプライバシー情報から外部世界の個人が結びつけられないよう，ID 可到達性を切り，プライバシーを保護する必要がある．そこで我々は，K-匿名化処理を施すことにより，ID 可到達性の遮断を試みる．K-匿名化処理[4]とは，情報をより一般的な情報に置き換える汎化処理と情報を消去する抑圧処理によって同一のプライバシー情報が保存されている ID が K 人以上となるように変更する処理を指す．

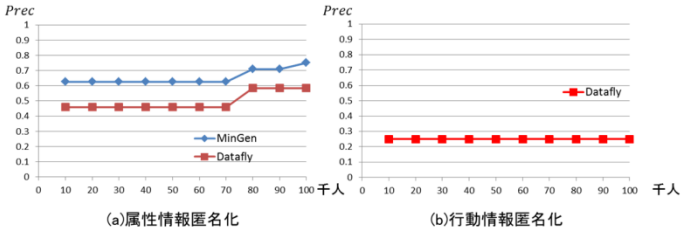

図３　匿名化による情報損失

HIFI のデータベースにプライバシー処理を施すため，階層構造を持つ汎化規則に基づく，属性情報に対する K-匿名化アルゴリズム MinGen[4]と Datafly[4]を適用する．さらに，行動情報にも対応できるよう階層構造を設定し，Datafly を行動情報に対して用いる．K=2 で匿名化した場合，データベースに格納する人数に応じて，情報がどのように変化したかを表す Prec 関数（元の情報からどれだけ情報が残っているかを示す関数）の変化をシミュレーションにより調べた．図３の結果より，属性情報に対する匿名化は， Prec 関数が 0.5 以上であり，MinGen では最大 0.75 となった．つまり，常に半分以上の情報を持ちつつ匿名化が可能であるため，属性情報に対しては有効である．一方，行動情報に対しては，どの人数でも Prec 関数が 0.3 を下回るため，匿名化により情報が大きく損失しており，行動情報に対しては不向きであることが分かる[3].

5. おわりに

HIFI は，プライバシー情報の「開示」に対立する概念として「利得」を取り上げ，両者の調和を図ることが主眼である．プライバシー情報を見せなければ，個人に適応した良質の情報・サービスを受けることは難しい，という自然な考え方を具体化するものである．また，自分の情報は自分でコントロールするという現代的なプライバシー権を組み入れた枠組ともいえる．HIFI の他の機能については別の稿に譲る．本研究の一部は，科学研究費補助金・基盤研究(A)による．

参考文献

[1] N. Babaguchi and Y. Nakashima, "Protection and Utilization of Privacy Information via Sensing (Invited Paper)," IEICE Trans. on Information and Systems (to be published)

[2] 小野士，中村和晃，馬場口登，“実空間における適応型サービスのための情報エントリーシステム，” 2014 年映像情報メディア学会年次大会（2014）．

[3] 新井健介，河野和宏，馬場口登，“ユーザの主観に適応した ID 種別毎のプライバシー保護，” 電子情報通信学会 2014 年総合大会，D-21-3，p. 194（2014）．

[4] L. Sweeney. “Achieving *K*-Anonymity Privacy Protection using Generalization and Suppression,” International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, Vol. 10, No. 5, pp. 571-588(2002).