空間を限定した
プライバシー情報保護・活用基盤

馬場口　登

大阪大学大学院工学研究科

2014年2月3日
Intl WS Information Systems for Social Innovation@NII

1　プライバシー・アウェア社会

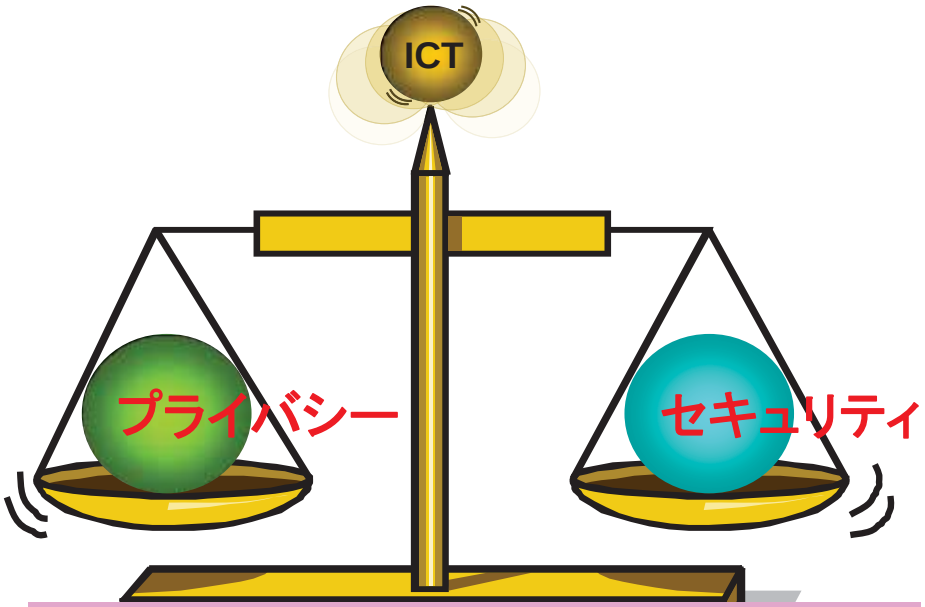
- サーベイランス（監視カメラ）映像
- Web映像/画像
- SNS画像/映像

プライバシー・アウェア社会の到来

- プライバシー権
  - 基本的人権（憲法第13条、幸福追求権）
  - 現代的プライバシー権：自己情報コントロール権
- 個人情報保護法（2005年4月施行）
  - 「プライバシー」は規定・記述なし
  - 個人情報の取得：オプトイン（承諾）
- ICTの利用で、個人情報の足跡（履歴：電話・メール・検索・位置（移動）、購買、道路通行など）を残す

  ⇒ビッグデータ
- セキュリティ（安心安全）とプライバシーのバランス

セキュリティ　vs　プライバシー



President Barack Obama “I think it’s important to recognize that you can’t have 100 per cent security and also then have 100 per cent privacy and zero inconvenience” (NSA surveillance: June 07, 2013)

視覚情報(Web画像)でのプライバシー問題

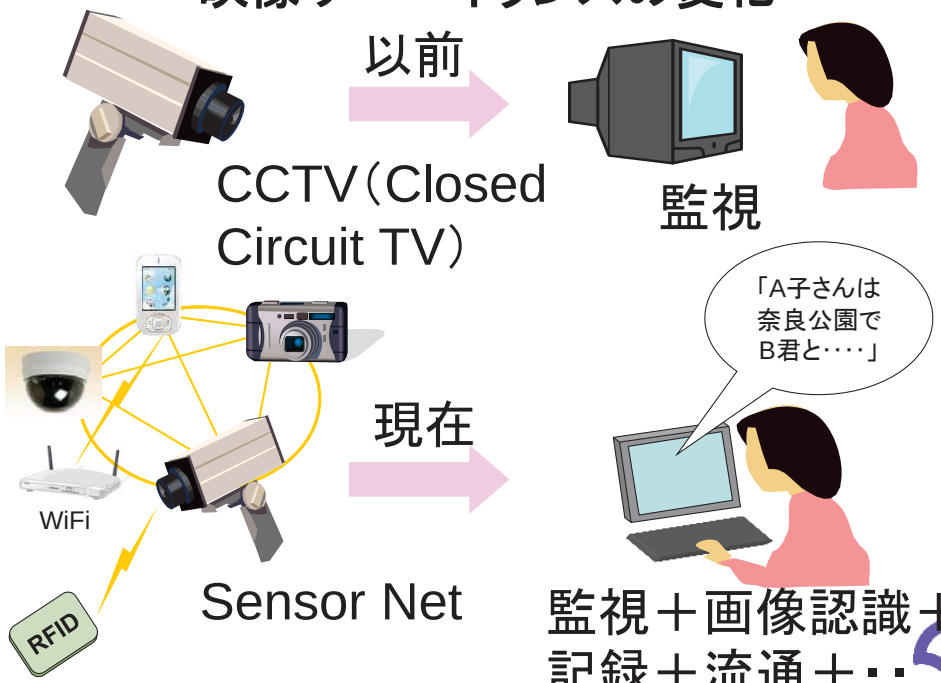
Google Street View

- 総務省：原則として個人情報保護法違反やプライバシー・肖像権の侵害にはあたらないとの見解（2009年6月）
- 福岡地方裁判所判決：原告が自宅アパートのベランダに洋服や下着を干していたところ、Googleが画像撮影し、インターネット上で公開したという訴訟。本件行為については権利侵害・違法性がないとして、請求棄却(2011年3月16日)

サーベイランス（監視）カメラのある社会

日本での推計は350万台!?
英国では420台(2010年頃)

映像サーベイランスの変化



顔認証-最近のテレビ番組から-

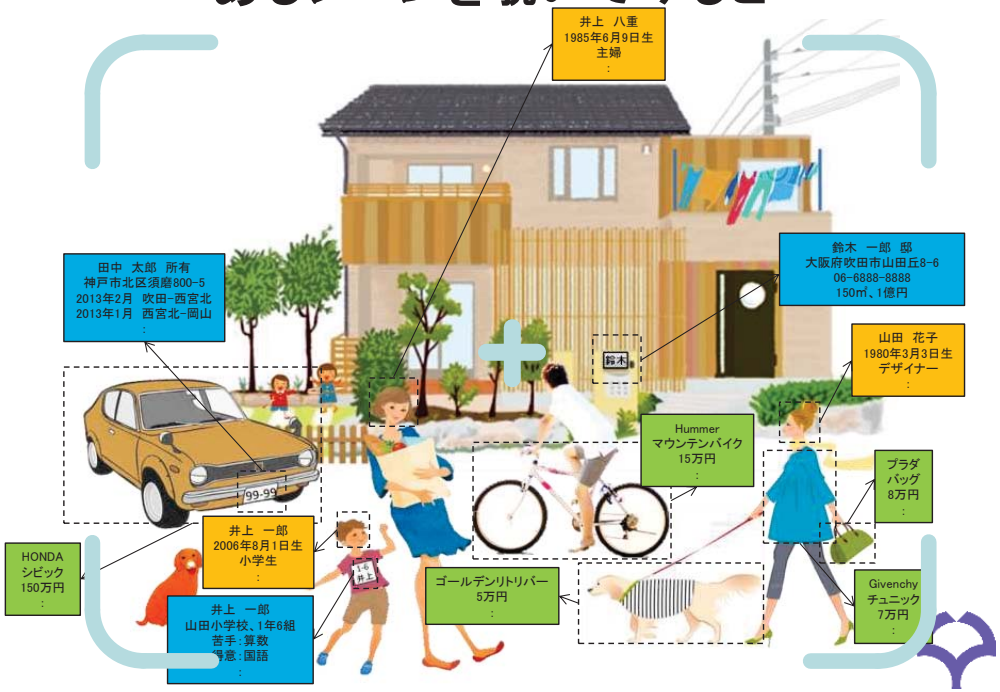
- 2013年5月29日7:30pmNHK「クローズアップ現代」
- 顔から個人情報が流出する
  ～広がる“顔認証”技術～
- 佐藤洋一先生＠東大が出演（視聴率10.1%!!）

CMUの研究事例

- 写真（画像データ）から名前、誕生日、出生地、SSNを推定する実験
- 推定率：29/93=31%
- 顔画像⇒顔照合⇒Facebook情報（画像）を検索

あるシーン

あるシーンを覗いてみると



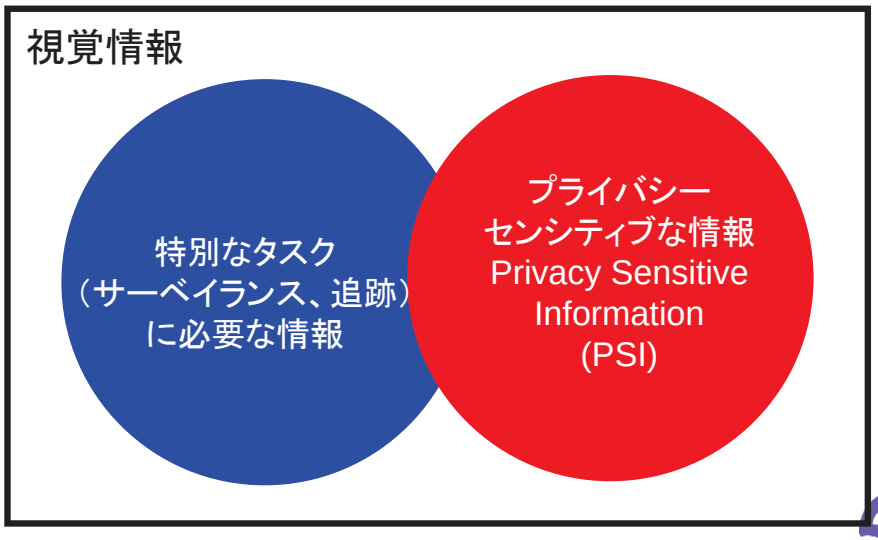
デジカメ・スマホ画像とSNS

- 画像（写真）JPEG
- EXIFデータ（メタデータ）
  - 撮影日時、撮影機器のメーカー名、モデル名、画像全体の解像度（水平・垂直方向）、撮影方向、シャッタースピード、絞り（F値）、ISO感度、測光モード、フラッシュの有無、露光補正ステップ値、焦点距離、色空間、GPS情報（緯度・経度）、サムネイル（160 × 120 画素）
- Flickrなどにアップしたら、EXIFデータはタグとして保存⇒写真だけを出してるつもりが、場所時間がわかる

2　視覚情報に対するプライバシー保護

- プライバシーセンシティブ情報PSI
- PSIの保護処理
- 関連研究

プライバシーセンシティブな情報



PSIの種類

- PSI:実世界のセンシング情報からそれを抽出するとプライバシー侵害になり得る情報[馬場口2010]

1）個人 ID 識別情報:個人 ID (名前)に到達可能な情報
  - 顔,容姿, 歩き方,移動軌跡, 声,名札, など.

2）ID関連情報:もともとPSIではないが、人（個人ID）と関連付けることによってPSIになりうる情報
  - 所持品, ペット(動物), など

3）私的（プライベート）領域:
  - 家の中,物干し場,携帯やPCの画面, など

PSI処理の特性

- プライバシー感覚: 個人性、主観性、コンテキスト・センシティブ(context-sensitive)
  - Webページの顔、ブログ
- 誰(who)が、いつ(when)、どんな状況(in what situation)で、何(what)を見れば、PSIになるか?
  - 家族、近所の人、警察、見知らぬ人
  - 昼間、夜間、街中、リゾート
- PSI は変わりうる!:PSI処理の困難性

視覚的PSIに対する保護処理

- プライバシーセンシティブな情報PSIである顔、姿、服装、表情….を隠す（保護する）
- 視覚的なPSIを見えなくする:Hide (Protect) visual PSI from being seen
  - 解像度を荒く:モザイク(pixelize)、ボカシ(blur, obscure)
  - 塗りつぶす(block)、マスク掛け(mask)
- 2000年以降、研究が活発化

プライバシー処理関連研究の変遷

- 1）盲目的・網羅的保護　＜顔／人物検出＞
  - 怪しいところは全て隠す
  - シルエット[Tansuriyavong2001]、モザイキング[北原2004]、平均顔[Newton2005]、マスキング[Cavallaro2005]、Google Street Viewでの実利用[Frome2009]ほか
- 2）選択的保護　＜顔／人物検出・認識・位置同定＞
  - プライバシーポリシーなどで柔軟な保護
  - ポリシー記述[Wickramasuriya2004]、PrivacyCam[Senior2005]、PriSurv[知野見2008]ほか
- 3）セキュリティ・符号化技術との関係
  - 情報ハイディング[Zhang2005][Li2009]、スクランブル[Dufaux2006]、暗号、アクセス制御[Winkler2012]、圧縮データでの処理
- 4）開示と利用
  - 時間と空間の軸：非常時、限られた空間（フィールド）

Google Street Viewでの保護処理

A.Frome, G.Cheung, A.Abdulkader, M.Zennaro, B.Wu, A.Bissacco, H.Adam, H.Neven, L.Vincent, “Large-scale Privacy Protection in Google Street View”, Proc. ICCV 2009, pp.2373-2380　顔：89%、車両番号：95%

プライバシー保護画像？？

3　プライバシー情報処理関連プロジェクト

プライバシー処理関連プロジェクト

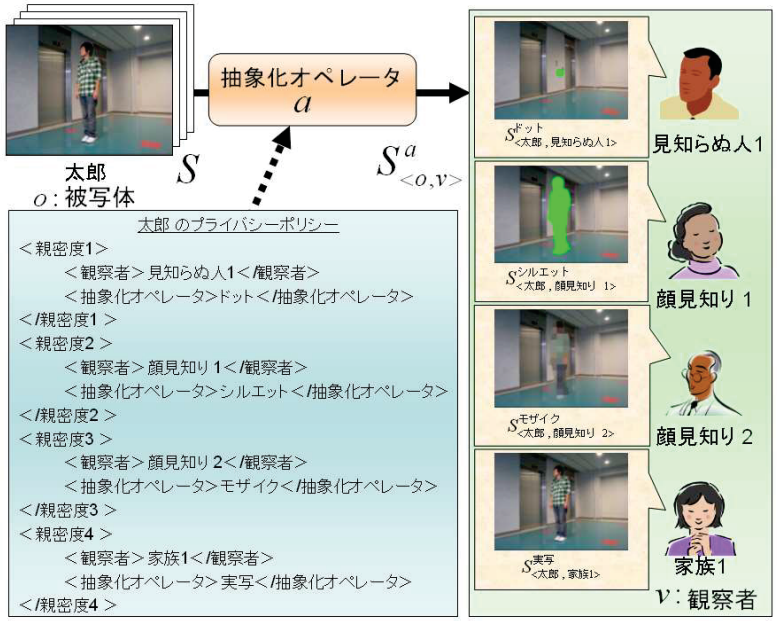
プロジェクト	イメージ図	対象	被写体	センサ	サポート
PriSurv		コミュニティ（地区、校区、オフィスなど）	メンバー／非メンバー	固定カメラ RFIDタグ・リーダ	総務省 SCOPE H18-20
ディジタルジオラマ		公共空間（大規模商業施設）	一般来場者	カメラ RFIDリーダ 無線LAN 赤外線センサなど	文科省 振興調整費 H19-21
MPP (Mobile Privacy Protection)		任意の屋外屋内環境	興味/非興味被写体	モバイルカメラ 慣性計測センサー	科研費 H21-23
HIFI (Harmonized Information Field)		フィールド（商業施設、テーマパーク、学校など）	ID種別をもつ来場者	固定カメラ モバイルカメラ ソーシャルメディア	科研費 H24-27

プライバシー保護機能をもつ映像サーベイランスシステム ーPriSurvプロジェクトー

-Privacy Protected Video Surveillance System-

Supported by 総務省・戦略的情報通信研究開発推進制度SCOPE（H18-H20）
次世代ヒューマンインターフェース・コンテンツ技術

被写体と観察者の関係による視覚情報制御



XMLで記述、心理学的な調査により設計[Babaguchi2009]

PriSurvの生成映像

サーベイランス映像

PriSurv映像

Mobile Privacy Protection(MPP) プロジェクト

固定カメラからモバイルカメラへ

Supported by 科学研究費補助金・基盤研究(A)
プライバシー・センシティブな視覚情報のセンシングと保護処理
(H21～23年度)

プライバシー保護映像生成の考え方

モバイルビデオカメラで撮影した映像
撮影者が撮影したい人物の他に
偶然に写り込んだ人物(通行人など)
が存在

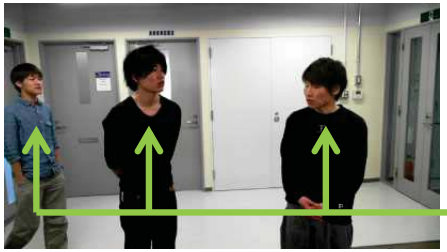
勝手にSNSにアップしたら
プライバシー侵害の危険

撮影したい人物:実写
その他の人物:視覚的抽象化(ぼかし、ボックス、透明化など)

アプローチ

映像中の人物から撮影意図に合う人物(意図人物)を推定

[Nakashima2010]



どの人物が意図人物？非意図人物？

考え方

意図人物の動きとカメラの動きには相関性がある

例:意図人物が右に動くと
撮影者はカメラを右に動かす

人物の動き・大きさとカメラの動き
により意図人物を推定
(学習型アルゴリズム)

試作システムの動作例

カメラ
Microsoft Webcam
LifeCam Studio

慣性計測デバイス
MicroStrain
3DM-GX3-45

ノートパソコン
Lenovo
ThinkPad
X201 Tablet
CPU:2.13GHz
Intel Core i7

処理能力:22.1fps
(640×360)

プロトタイプに表示
されている映像

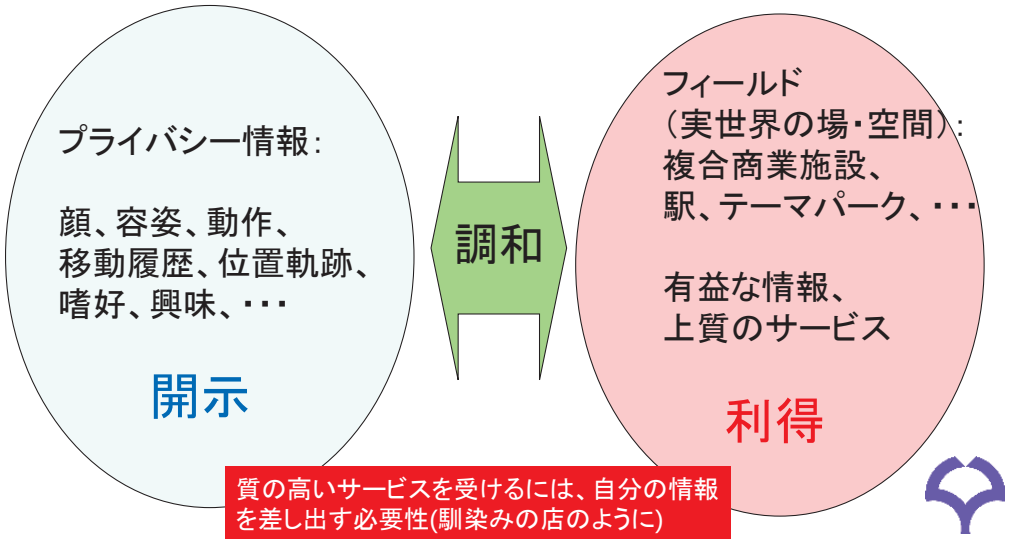
調和的情報フィールド (Harmonized Information Field: HIFI) プロジェクト

プライバシー情報の開示と利得

Supported by 科学研究費補助金・基盤研究(A)
センシングで得られるプライバシー情報の開示に調和した
ユーザ利得の創出(H24～27年度(予定))

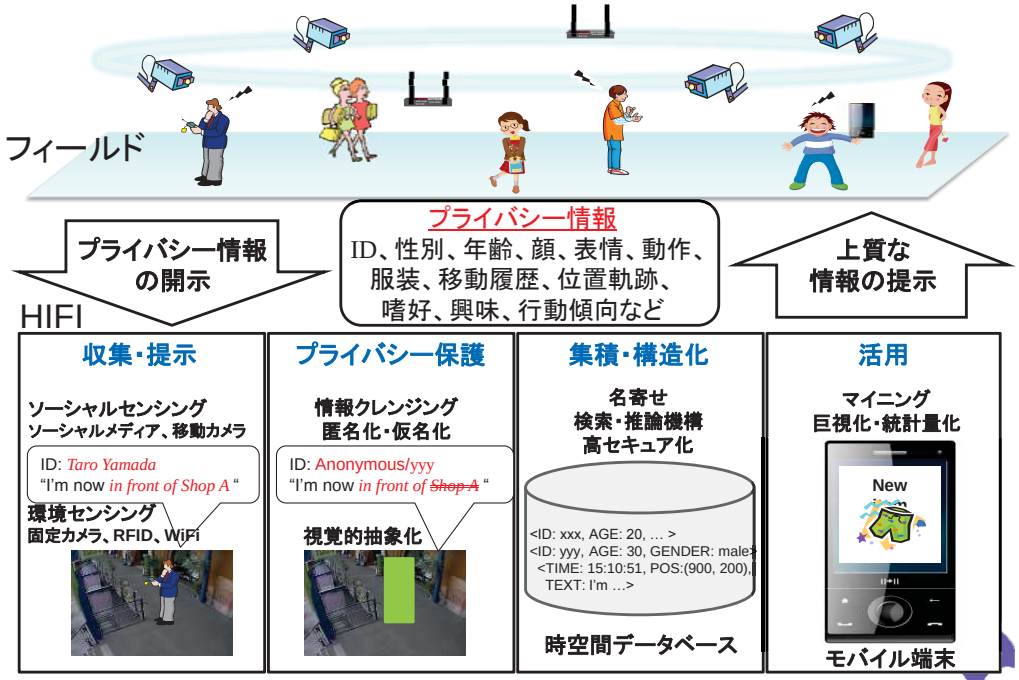
プライバシー情報の開示と利得の調和

調和的情報フィールドHIFI(Harmonized Information Field)

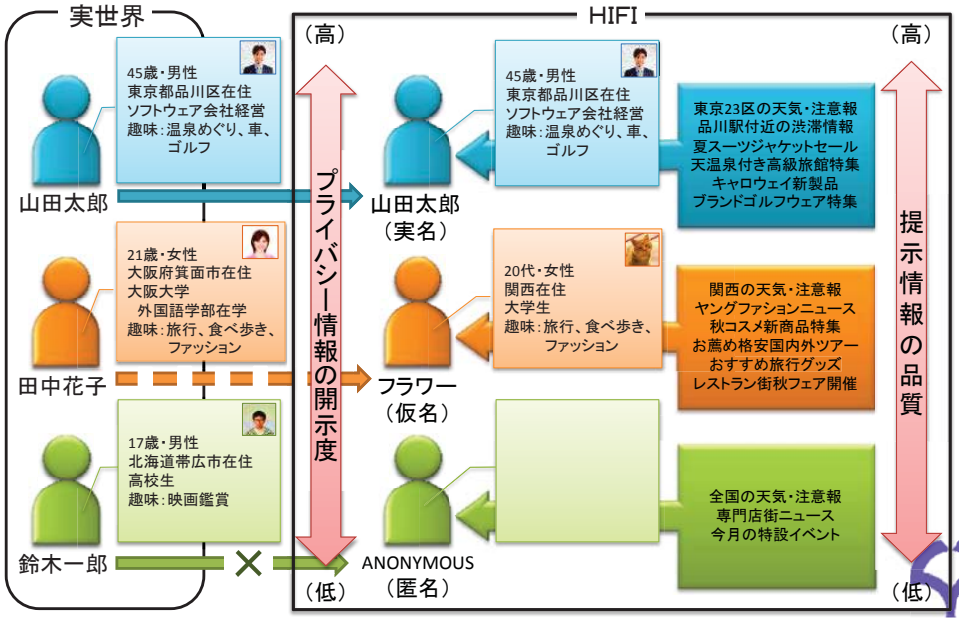


質の高いサービスを受けるには、自分の情報を差し出す必要性(馴染みの店のように)

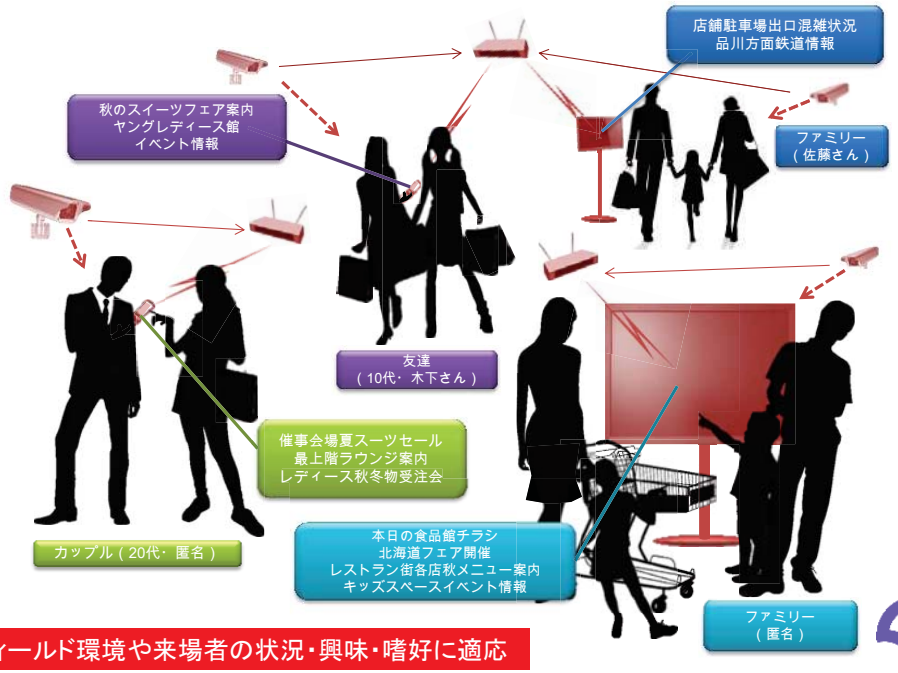
HIFIのプロセスフロー



ID種別,プライバシー情報の開示, 及び提示情報の品質

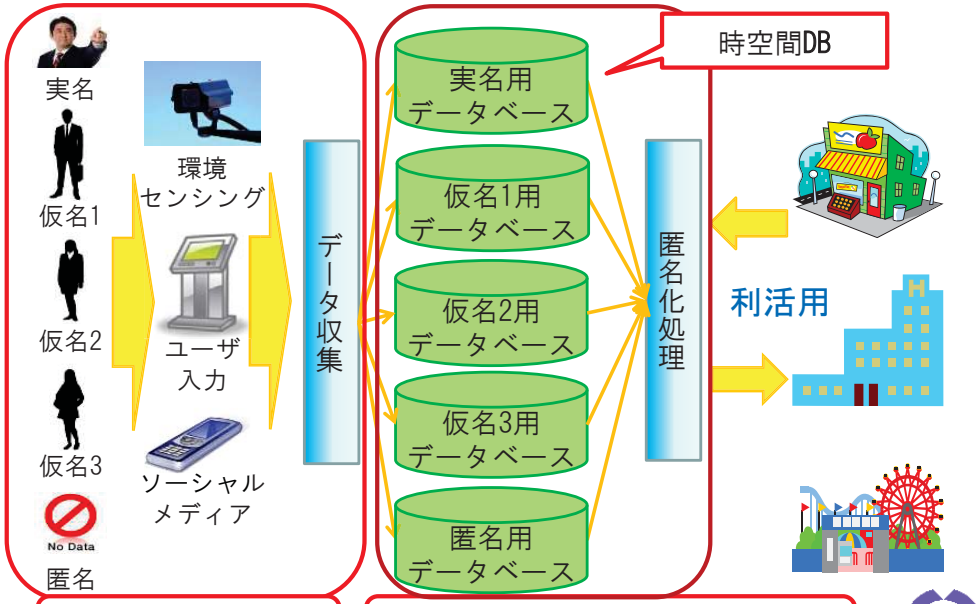


状況認識型情報提供のイメージ



フィールド環境や来場者の状況・興味・嗜好に適応

時空間DBに対するプライバシー保護



ID毎の情報に必要なデータを設定・取得

HIFI内で同定されないよう、ID別の属性データの処理(*K*-匿名化)

ID種別毎の取得データの設定

5段階の種別を情報の有無と性質により設定

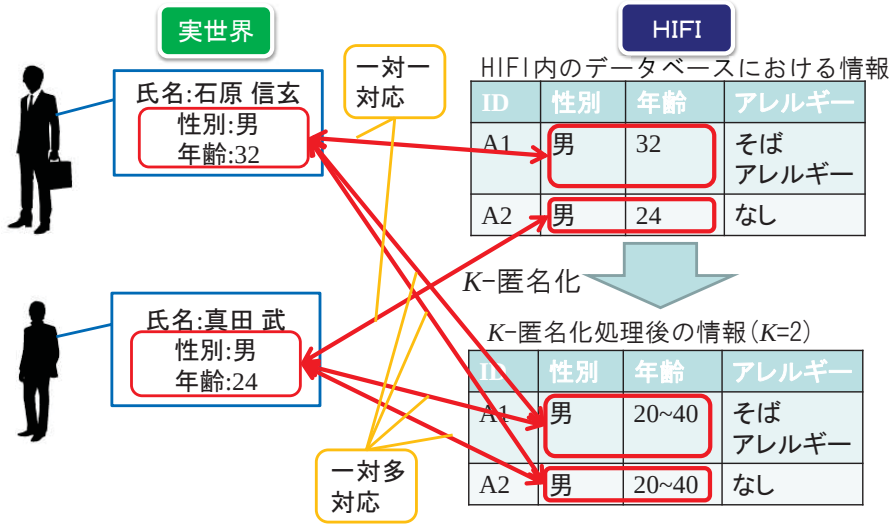
属性情報：個人の属性に関する情報（氏名, 性別, 住所, 生年月日等）
行動情報：センサから取得したHIFI内の行動に関する情報（移動履歴等）

- 匿名　：全ての情報を取得しない
- 仮名3：行動情報をその日のみ取得
- 仮名2：行動情報を日をまたいで取得
- 仮名1：行動情報と単独では実世界の本人と同定できない属性情報を取得
- 実名　：行動情報と実世界の本人を同定可能な属性情報を取得

ID種別	その日のみの行動情報	日をまたぐ行動情報	個人情報	実世界との結びつき
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

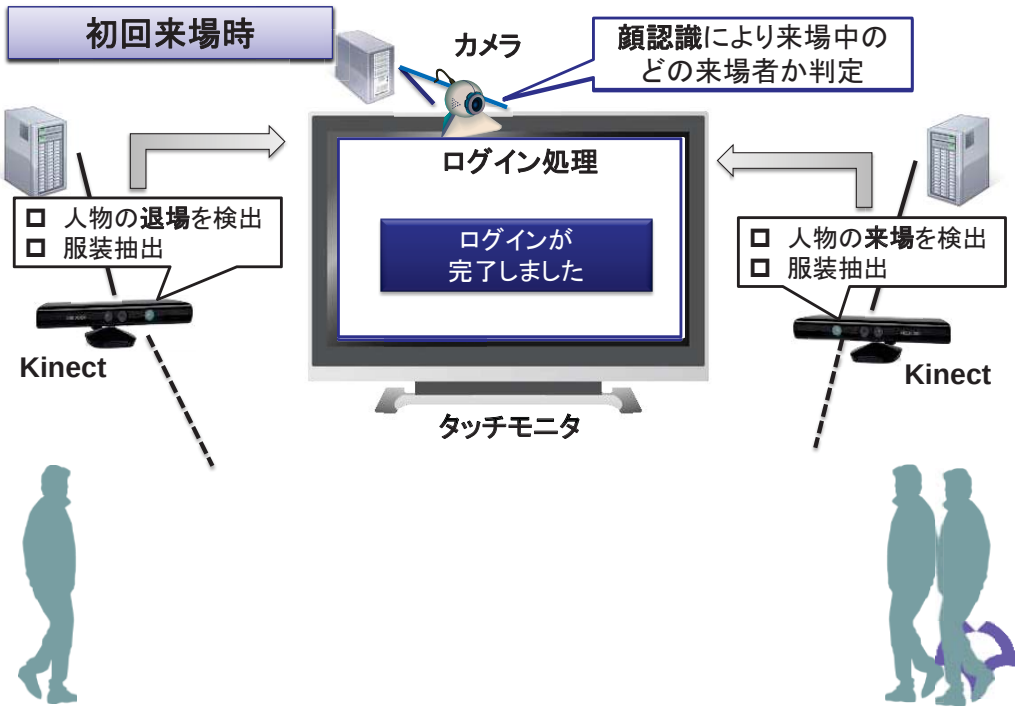
ID別の属性情報の処理：*K*-匿名化

候補が*K*人以上存在するようにデータを汎化

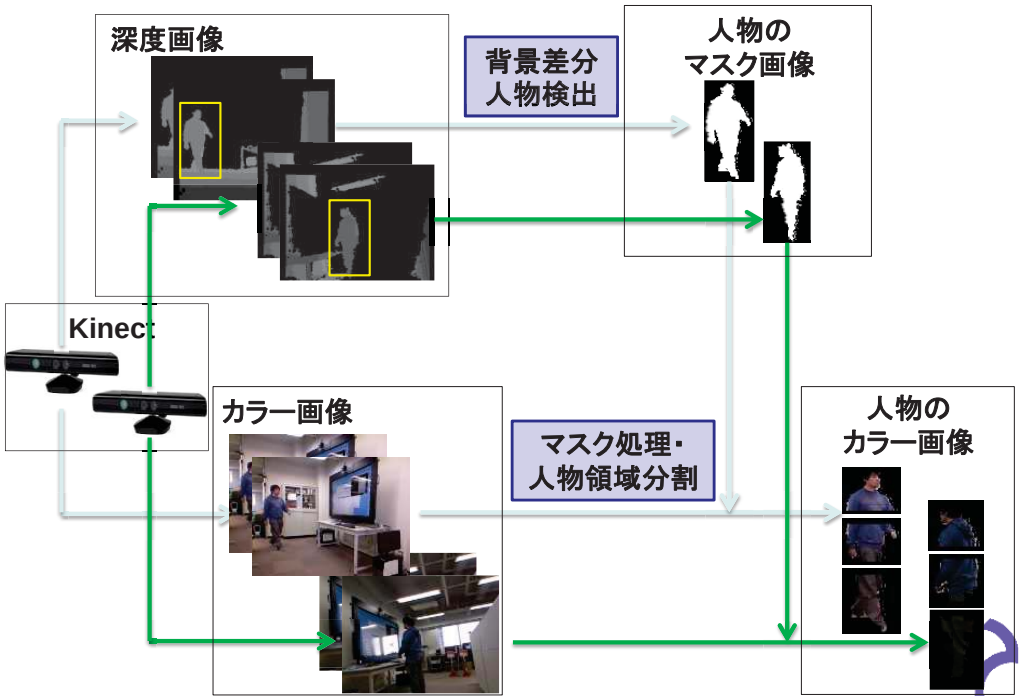


HIFI内での同定をブロックすることにより、実世界との対応付けをブロック

HIFIゲートでの情報エントリー



人物検出と服装抽出

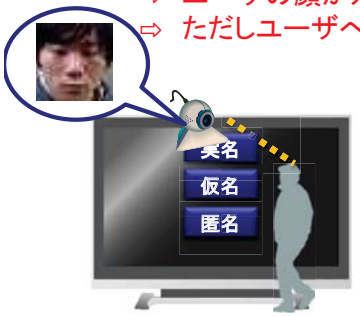


個人同定に有用な顔画像の取得とユーザの負荷の軽減

個人同定に有用な顔画像とは？ ・・・ **正面顔**

⇨ ユーザの顔がカメラに向くようにしたい

⇨ ただしユーザへの負荷が大きくならないようにしたい

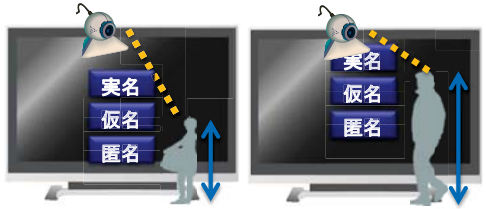


基本的な配置の工夫

個人同定が必要なユーザ種別は上側に配置

⇨ ユーザ種別を選択する際に自然に
顔がカメラに対して正面に向く

インタラクションによる負荷の少ない情報エントリ



身長推定による配置の工夫

**身長に応じてユーザ種別の
配置自体をコントロール**

⇨ ユーザの負荷を軽減

まとめ

- プライバシー処理研究
  - 網羅的保護⇒選択的保護⇒適切な開示と利活用
  - 専門書[Senior2009]、特集[例えばIEEE-TIFS2013]
  - 保護のための画像処理・解析：メディア処理技術の新しい付加価値や新しいシステム創成
- HIFI
  - 「開示」の対立概念としての「利得」
  - 質の高いサービスを受けようと思えば、自分の情報を差し出さねばならない、という自然な発想
  - 今後、要素技術・背景理論の開発とプロトタイピング