【産業競争力懇談会　2016年度　プロジェクト　最終報告】

【IoT 時代のプライバシーとイノベーションの両立】

～appendix～

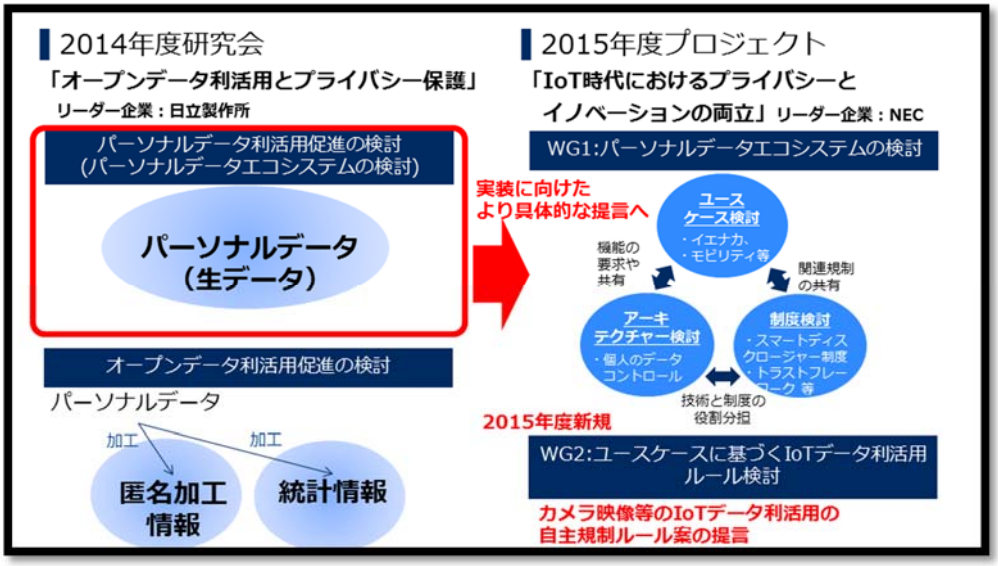
２０１７年２月１５日

産業競争力懇談会 COCN

目次

1. 昨年度までの報告概要

2014 年度「オープンデータ利活用とプライバシー保護」研究会および 2015 年度「IoT 時代のイノベーションとプライバシーの両立」プロジェクトの報告概要について以下に説明する。



1.1. 2014 年度

2014 年度の「オープンデータ利活用とプライバシー保護」では、公共機関のデータだけでなく、企業や個人が所有するパーソナルデータを組み合わせて得られる知見を個人や社会に還元し、ひいては経済の活性化や産業競争力強化につなげるため、パーソナルデータの利活用とプライバシー保護を両立するモデルの立案と政策提言を行った。

1.1.1. 検討の視点と範囲

パーソナルデータの利活用に対して国民のコンセンサスを得るためには、データ保護に必要な法制度の整備だけでなく、ライフサイクルの様々な場面に応じてパーソナルデータを開示することが個人へのメリットにつながることを、具体ケースを例にして示すことが有効と考えられる。そこで 2014 年度は国による調査結果を踏まえて、個人のメリットが分かりやすいと考えられる「防災」「医療・ヘルスケア」「オリンピック・パラリンピック」を具体ケースとして取り上げ、これらの具体ケースを通じて国民のコンセンサスの壁を打破することで市場の拡大につながることが期待できないか検討を行った。国民のコンセンサスを形成する上で重要となるパーソナルデータの利活用パターンは、法令の適用による義務的な利活用(パターン①)、個人の意思・同意による利活用(パターン②)、本人同意を必要としない利活用(パターン③)に分けられる。昨年度は個人の同意に着目し、パターン②およびパターン③について提言としてまとめた。パターン②に対応して、個人による主体的なデータの集約・管理・利活用を行う仕組みとして、パーソナルデータ・エコシステムの構築を提言した。パーソナルデータ・エコシステムとはパーソナルデータを個人が集め、管理し、様々な組織や企業に利用させることで個人が直接的に利益を得るシステムである。さらにパターン③に対応して、個人情報保護法等の制度改正で導入された匿名加工や統計加工によるデータ利活用を促進するための環境整備について提言を行った。個人の特定できないよう加工した匿名加工情報の活用を促進することで、民間企業での新たな価値創造や社会的課題(防災、医療・ヘルスケアを始め、交通・物流、都市計画、エネルギーコントロール等)の解決などが期待できる。これらを円滑にす

すめるためにも国民のコンセンサスは必要不可欠のものである。

1.1.2. 産業競争力強化のための提言と施策

[提言1]日本版パーソナルデータ・エコシステムの構築

諸外国と比して、日本では国民のプライバシーに対する不安感が高い傾向にある。パーソナルデータ利活用促進のために個人情報保護法が改正されたが、法制度の整備だけで個人の不安感や不利益感が解消されるものではない。そこで、法令の遵守に留まらず、個人のプライバシーを守りながら個人に対して新たな価値やメリットを提示する仕組みとして日本版パーソナルデータ・エコシステムを官民連携して構築する。

（施策1）個人によるデータコントロール環境整備の推進

個人が自分のデータを自分で管理できる PDS 等の仕組みを推進するため、企業等によるマシンリーダブルな形式でのパーソナルデータ開示と、データ形式の標準化を進める。企業等が足並みを揃えた取組みを行うように、国が PDS 推進のための積極的な旗振りを行う。

（施策2）トラストフレームワークの整備

パーソナルデータを授受する個人や企業などが互いに相手を信頼できるものとみなすことができる仕組みとしてのトラストフレームワークをグローバル視点で整備する。

（施策3）パーソナルデータ・エコシステムを前提とした新産業創出支援

個人によるパーソナルデータの提供・開示に対して金銭的対価・利便性向上・社会的意義等のインセンティブを与えるようなサービス事業者の育成を支援する。

[提言2]産業競争力強化に向けた環境整備

ビッグデータの利活用加速のため、オープン化した行政情報だけでなく企業や個人の持つパーソナルデータの利活用を促進する。プライバシー保護に配慮した形でパーソナルデータの利活用を進めるためには国民のコンセンサスが必要不可欠である。そこでコンセンサスの壁を構成する国民の不安や不満を解消するため、パーソナルデータを利活用するプロセスに関する環境整備を官民共同で加速する。

（施策1）匿名加工に対する安心感醸成に向けた国民への発信

匿名加工に対する運用規定の整備や具体例を通したメリットの体験など、国民に対する不断の情報発信を行う。

（施策2）オプトアウト規定の見直しを踏まえた利活用ガイドライン整備

個人の求めに応じた利活用の円滑な停止のため、IT の導入を念頭においた事業分野ごとのパーソナルデータ利活用のガイドラインを整備する。

（施策3）個人が利活用できるパーソナルデータの政策的な充実と管理強化

諸外国での取り組みを踏まえて政府主導で個人が利活用できるパーソナルデータを政策的に充実するとともにセキュリティ対策についても強化する。

（施策4）国民が自ら実践できるプライバシー保護対策の認知度を向上し、安全な情報化社会を構築する。

[提言3]具体ケースでの実証によるコンセンサスの形成

個人にとってパーソナルデータの提供メリットがわかりやすいもの(例えば「防災」「医療・ヘルスケア」「オリンピック・パラリンピック」)を具体ケースとして取り上げ、実証実験を通じて国民がメリットを体感できるようにする。同時に匿名加工などの技術実証を行う。

1.2. 2015 年度

2015 年度の「IoT 時代のプライバシーとイノベーションの両立」では、2014 年度の活動からパーソナルデータの利活用に関する議論をさらに深める活動を実施した。2014 年度に具体ケースを提示したパーソナルデータ・エコシステムについては、社会実装を実現するために必要な環境整備、仕組みの在り方について立案および政策提言を行った。産業界におけるビジネス環境からの現場の声として、プライバシーに配慮し社会受容性を得た上でのカメラ画像を利活用したサービスの実現が喫緊の課題であったことから、マルチステークスホルダー・プロセスを前提としたコンセンサス獲得に向けた商用利用のための自主ルールを作成した。

1.2.1. 検討の視点と範囲

2015 年度は主に2つの視点をベースとした活動を実施した。1 つ目は、個人主導のパーソナルデータ流通・活用(WG1)、2 つ目は、IoT 由来のパーソナルデータ利活用(WG2)である。

個人主導のパーソナルデータ流通・活用(WG1)については、事業者や公的機関等が保有するパーソナルデータや本人由来のパーソナルデータを本人に集約し、自らの意思でそのデータを事業者や他の個人に提供できるようにすることにより、個人主導によるディープなパーソナルデータの流通とそれによる新たな事業機会の創出をスコープとした。事業者や公的機関等が保有するパーソナルデータを、扱いやすい形式の電子データとして本人に提供すること(スマートディスクロージャ)を起点に、データ主体の意思により事業者の間でパーソナルデータを容易に移転可能とするデータポータビリティ制度や、個人が自身のパーソナルデータの利活用をコントロールする手段として期待されている「パーソナルデータストア」を社会実装するための関連事例調査やユースケース検討に基づいた要件の検討、及び個人によるデータコントロールがもたらす新たな社会価値の検討を行った。

IoT 由来のパーソナルデータ利活用(WG2)では、カメラ画像に代表される本人同意取得が困難なパーソナルデータ活用の在り方とスコープとした。

日本の顔認証技術、画像解析技術、およびカメラ技術は世界トップレベルにあり、経済効果や社会課題の解決への期待も大きいが、特性上個人のコントロールや事前の本人同意に基づいた活用が難しく、また監視社会に対する生活者の懸念によりコンセンサスのハードルも日増しに高まり、事業者が利活用を躊躇する事態が生じていた。

この課題への対応について、各社から課題となるサービス事例を募り、マルチステークスホルダー・プロセスを前提としたカメラ画像の商用利活用自主ルール案を策定することとした。ルール化の基本方針はプライバシーとイノベーションのバランスの取れた個人識別情報取得を推奨することであり、特に「個人の行動に関する情報が、どれだけ長期に保存され、その本人に紐つく形で取り出しうるか」の観点から、システムの類型化を図り、各類型に対する具体的なルール案として『カメラで取得された人物関連デ

ータの商用目的における利用ルール』を策定した。通知・公表方法、開示・消去請求対応など、生活者目線な行為規範とすること、透明性やアカウンタビリティを重視することなどをポイントに、合意形成の足掛かりを築いた。

1.2.2. 産業競争力強化のための提言と施策

＜個人主導のパーソナルデータ流通・活用＞

[提言1]基盤技術の強化

新たなパーソナルデータ活用サービスの創出やパーソナルデータによる社会課題の解決を促進する共通的なプラットフォームとして、個人主導のパーソナルデータ流通やプライバシー保護に関する基盤技術を強化する。(施策 1)政府主導のプロジェクトにより、データの形式や取引条件の表現方法などパーソナルデータを活用したサービスを創出し普及させるために共通であることが望ましい技術を開発する。

[提言2]制度検討

パーソナルデータ関連の法制度の改正を視野に入れ、個人の意思に基づく事業者間の容易なデータ移転を担保するデータポータビリティ制度、データポータビリティのためのスマートディスクロージャの方法、及び個人がパーソナルデータ流通のメリットとリスクを容易に理解できる第三者認証等の在り方を検討する。

(施策 1)内閣官房 IT 総合戦略室主導で「データポータビリティ制度」を検討する産官学連携タスクフォースを設立する。

(施策 2)情報通信技術(IT)の利活用に関する制度整備検討会にて示された代理機関(特に個人情報収集分析型代理機関)に対して、代理機関が収集したパーソナルデータについて本人の意思によるデータポータビリティを担保する手段の提供を義務付ける。

(施策 3)民間主導で、信頼性評価を行う第三者機関の創設を見据えた産官学連携コンソーシアムを構築し、「利用目的の分かりやすさ」、「プライバシー影響評価」、「データポータビリティへの対応」等の評価軸や評価指標など、事業者の信頼性評価の枠組みを策定する。

(施策 4)施策 3 に示した産官学連携コンソーシアムが信頼性評価を実施し、その評価結果の公表などを通じ、多くの個人がデータリテラシーの程度によらずデータ利活用のメリットやリスクを容易に理解できる環境を整備する。

[提言3]社会受容性検証

個人に集約された時系列のデータや分野横断のデータの活用によるサービスの創出や社会課題の解決への期待が高い領域について、その仮説検証を実施する。

(施策 1)国のプロジェクトとして、個人が自身のデータを自ら集約しデータ活用事業者に提供するという一連のデータ流通によって生ずる価値に関して本報告のユースケースで示した仮説を検証するための実証事業を実施する。

(施策 2)委託管理型代理機関等のパーソナルデータ活用が求められる国や自治体のプロジェクトに、本報告に示す個人主導のパーソナルデータ流通の要件を追加する。

＜IoT 由来のパーソナルデータ利活用＞

[提言1]マルチステークホルダー・プロセスによる利活用ルールの整備

個人情報保護関連法において検討・想定されているマルチステークホルダー・プロセスに基づいた利活用ルールの整備

（施策 1）サービサー、適用ケースに沿った業界団体、消費アドバイザー、個人情報保護やプライバシー保護に関する有識者などを交えたルールの詳細検討

（施策 2）個人情報保護等に関する機関など行政等へのルール説明と議論

[提言2]カメラ画像に関する改正個人情報保護法に基づいた運用体制の整備

カメラ画像を対象とする業種業態に関わらないサービスや事業者を対象とした認定個人情報保護団体の枠組みや機能分担など運用体制の整備

（施策 1）オリンピック・パラリンピックなど重要イベントや、科学技術基本計画などに基づく社会課題対応などにおけるカメラ画像利活用に関する要件整合とロードマップ作成

（施策 2）既存の防犯カメラに関する法規や関係団体との整合、およびドローンや移動カメラなど新たな利用形態の検討

（施策 3）カメラ画像を活用するサービスに対し、評価、認定制度の検討

（施策 4）上記を踏まえ、個人情報保護委員会、受け皿として想定される認定個人情報保護団体を交えた検討の早期着手

（施策 5）上記につきカメラ画像に関する課題を横断的に対応する、産官学による「カメラ画像利活用推進コンソーシアム（仮称）」を創設。

[提言3]官民一体となった普及と啓発

政府機関や関係団体の参画による実証プロジェクトの立ち上げを模索し、利活用ルールの定着活動を推進

（施策 1）行政や民間企業のユースケースをもとに、複数の実証プロジェクトにて利活用ルールを適用し、生活者の受容性を確認しつつルールの普及・定着化を推進する。

（施策 2）「IoT 推進コンソーシアム」において、本ルールを活用することにより、カメラ画像を活用した新たなビジネスモデル創出を促す。

（施策 3）内閣官房 IT 戦略本部が検討している代理機関構想におけるカメラ画像に関する代理機関の機能や認定基準の検討プロセスを共有、整合し、新たな制度においても国民のコンセンサス獲得を促進する。

要件		技術的対応	制度的対応
データ流通の推進	スマートディスクロージャに基づくデータポータビリティ	語彙、データ形式の標準化、API 公開、PDS	データポータビリティ制度
	個人、事業者間の取引条件の合意	マッチング	個人情報保護法、契約
トラストの担保	個人、事業者の確からしさ	ID 連携トラストフレームワーク	
	データの確からしさ	電子署名、タイムスタンプ	
	取引条件の表現	権利記述言語	個人情報保護法、契約
	データ利用目的の分かりやすさ	プライバシーポリシー表記（アイコン等）の標準化	第三者認証、監査
	データ利用目的の遵守、取引条件の強制	DRM	
	データ不正利用の検知	監査証跡	
	自己情報のトレーサビリティ	コンセントレシート、監査証跡	個人情報保護法

2. Mydata2016 レポート

背景

- 米国のIT企業GAFA: Google Amazon Facebook Apple がパーソナルデータをどんどん収集して囲い込み、利益を上げている現状

- 収奪されるEU、収奪されるデータ主体の個人
- GDPRで反撃しているが、それだけではEUの産業は育たない
- EUの個人データのプライバシー（＝人権）の危機。だが、産業は興さないと低落するのみ

- 個人データはデータ発生源であるデータ主体の個人が管理
- その枠組みの標榜と、ビジネス育成がテーマ

- 2017年8月31日から9月1日　Helsinkiにて　MyData2017の会議開催

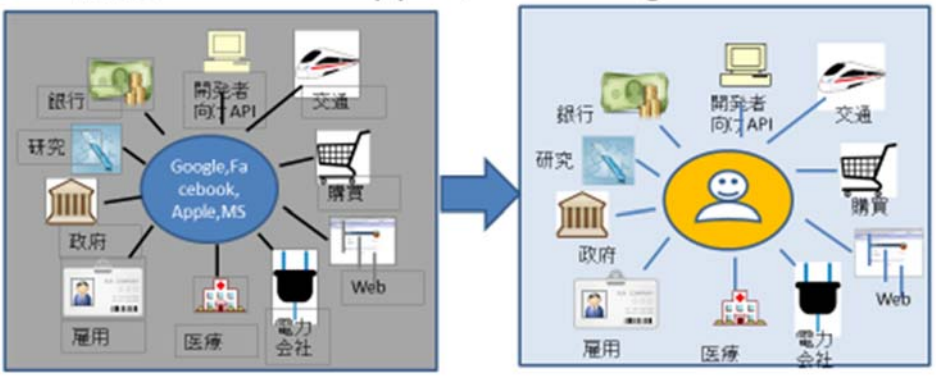
会場の様子

ORGANIZERS

Aalto University

個人データ管理はGAFAから データ主体の個人へ

- 個人データをディジタル人権に基づき産業に応用する。
- 標語：Make it happen, make it right!



データ管理をデータ主体の個人に取り返すための技術的ポイント

- パーソナルクラウド
- インターネットにおけるIdentity認証
- 個人データのポータビリティ
- Block Chainによる個人のIdentity認証
- プライバシー保護(暗号化,MPC, etc.)
- 公平性、透明性

規模

- 参加者　650人
- 発表者　140人
- 7会場の並列セッション構成
  - プログラムはここからアクセスできる

- フィンランド交通通信省が推進するMyDataプロジェクトが運営母体
  - 最終日に交通通信省の大臣が来て講演

- SNSの活用
- セッション中に会議サイトにコメントを書き込むと、その会議サイトで即時閲覧可能
  - どんな意見なのかがリアルタイムで分かる。
  - 講演への質問も書き込める

本レポートの以下の部分

- トラックのプログラムのリスト
- 各トラックにおける重要なセッションの内容紹介
- セッションの個別発表のいくつかを紹介

メイン会場のセッション

- Opening - why are we here?
- Challenges for the data-driven society
- Show me the power of individuals
- Empowering people with their data
- Collaborating for a better data future
- Closing - ACTION!

COLLABORATING FOR A BETTER DATA FUTURE

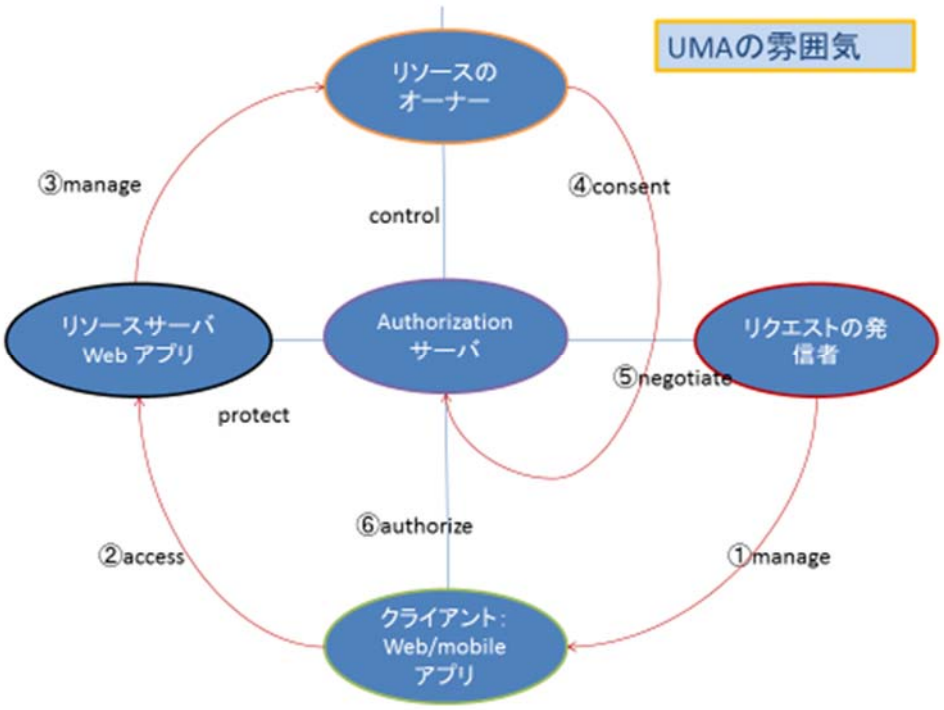
- data, identity, privacy, security and consent（同意）が合わさって、EUのディジタル経済を根本的に変えていく（というメッセージ）
  - 所有可能、取引可能、だが独占は許さない → オープンデータ化に進展をめざす
  - API-of-Me による多数の人、企業からの操作は可能か
    - Freedom vs Monopoly
  - 公共の個人データをこのようにオープン化するには政治的なポリシーが必要と主張

第2会場のセッション：ポリシー＋技術

- Future of digital self
- Trust me!
- Data-empowered everyday life
- Technical horizons
- Policy-making for personal data

TECHNICAL HORIZONS

- インターネットIdentityの認証技術がテーマである。
  - OAuth, Open ID Connectの紹介
    - これらはインターネットIdentityの認証技術
    - OIDCはOAuthの上に構築されたIdentityの認証プロトコル
  - UMA (user managed access):
    - OAuthを用いて、情報資源管理者が利用者からの保護されている情報資源アクセス要求を制御するプロトコル
  - XDI:
    - 参加者間の契約(link contract)に基づくデータ交換プロトコル
  - VRM:
    - Doc Searlsのプロジェクトのツールとして実装



第3会場のセッション:テクノロジー等

- Anatomy of personal data storage
- Blockchain and Personal Data
- Strategy and tactics for MyData design
- MyData Design - Challenges, Opportunities, Insights
- Challenges in Big / Small Personal Data Analytics

ANATOMY OF PERSONAL DATA STORAGE: Cozy Cloud

- Interoperability, consent management は大変
- そこで personal data storage（PDS)からpersonal cloud に移行＝Cozy Cloud。ようするにPDSのクラウド化をサポートするシステム
- 特徴:
  - Single sign-on,
  - global srarch
  - APPとの円滑な統合
  - IoTのハブになる
  - プライバシー確保
- 20名の社員で5,200,000ユーロ
- Together, let's Uberize GAFAs!!

ANATOMY OF PERSONAL DATA STORAGE: FreedomBox

- 位置づけ: Frerdom Box as a Personal Cloud/PSD/PIMS
- ポリシー: MyData= Self-Sovereign Identity
- データ表現形式: RDF, JSON, XDI,
- Identity 認証技術: OAuth2, ODIC, UMA

ANATOMY OF PERSONAL DATA STORAGE:Digital me

- Knowledege Worker が中心
- Digital Interaction は全てlogされる
  - プライバシー保護
  - 個人情報流通のトレース
  - → 個人による個人データのcontrol

- 技術
  - Java, Spring Boot,
  - RESTful API, JSON
  - DB: SQL Hibernate or MongoDB
  - テキスト検索はLucene
  - MacOS X, Linux, Windows でローカルに稼働

ANATOMY OF PERSONAL DATA STORAGE: My Data Store

- TIM(Telecom Italia)
- An Eco-System of Trusted Services with User Control & Transparency

  - 多ソースからのデータ収集
  - プライバシー バイ デザイン
  - 個人の完全なcontrol と透明性、信用できるAPPによるエコシステム、他との比較可能、詳細データのauditができる

BLOCKCHAIN AND PERSONAL DATA

- 個人のDigital IdentityをBlock Chainで管理する方法が焦点
  - Digital CATAPULT

  – コピー制限、流通経路の把握、identityの確認
  – プライバシーと個人IDの流出が危ない
  – 悪意ある行為の抑止方法
    ➢ゼロ知識証明で解決する方法の示唆あり

CHALLENGES IN BIG / SMALL PERSONAL DATA ANALYTICS

- プライバシー保護しつつ、有益なデータマイニングを行う方法の模索

  – 公平性、理解可能性、説明責任、機械学習アルゴリズムの透明化
  – センシティブな個人データに関しては、データマイニングなどの結果のみ表示。
    - → 秘密計算：MPC（Multi Party Computation)
  – 個人データが使われた場所と利用法を知ることができること

第4会場のセッション：応用

- Health and wellbeing
- Mobility, energy and smart cities
- Insurance and finance
- IoT
- Research and education

MOBILITY, ENERGY AND SMART CITIES

- ENEDIS(フランスの電力会社）はスマートメータを導入（全家庭の20%）
  - 個人が自分のエネルギー消費量を知ることになより環境保護意識が促進できる
  - 家庭、ないし個人のエネルギー消費データを集めることはできるが、プライバシーが脅かされる。

IOT

- センサーデータの管理と共有
- プライバシーを保護しつつ、データの共有と個人へのアクセス手段の提供を異なるプラットフォーム上で実現したい
  - IoTから集まる個人データの現状とプライバシーリスクの明確化
    - 暗号化はデフォールトであろう
  - 個人データの真正性はBlock Chainの提案多し：Block Chainのセクションでも同様。
  - Identityの確認（既存の　internet identity の仕掛けに言及したものは見当たらず）
  - データの転送
    - トランザクション化、およびその内容の整備
  - IoT固有というよりは、個人データ管理の問題一般に通ずる話が多かった。

INSURANCE AND FINANCING

- AXA フランス
- AXA Groupのデータプライバシーへの取り組み
  - ドライビング・パターンの抽出と保険
  - ビッグデータ分析の可能性と課題，法制度，倫理
  - 第三者機関French Data Protection Authority (CNIL) および
  - EUの15のデータ保護機関から承認を得ている.

- 加藤綾子先生の紹介記事より

第5会場のセッション：社会制度

- Public services
- Platform Economy
- Legal frameworks
- Quantified employee
- Economics of data management

PLATFORM ECONOMY

- André Golliez, Adrian Wyss, Aline Zaugg "– MIDATA.coop – my data our health (SWISS)" (Platform economys/Engage 8／31）

- 医療応用の話、様々なユースケースに対して実践的に実践している印象あり
- ビジネスモデルとしての共同組合方式(coop)など、興味深い

- ユースケース1 手術後のフォーアップ
  - 対象 脂肪過多、胃のバイパス手術を受けた患者、
  - 利用アプリ： MIMOTI－„Mini Motivation"
- 他にも多くのユースケースあり

- 各ユースケースでの共通項目 →信頼
  - Data protection, Data sharing, Mobile access through Apps, Citizen empowerment, Added value, Open platform with clear governance

- 石垣一司さんの紹介記事より

LEGAL FRAMEWORKS

- A trust-based framework for the data-driven economy:
  - Nicolo Zingales, Tilburg Institute for Law
  - GDPRは同意ではなくデータ管理者(data controller)の責任を重視する方向
  - 32%のプラットフォームは匿名化、仮名化を拒否
  - EUのユーザの52%（88%）は同意なしのデータ削除（アカウント削除）OK
  - 80%はユーザは第3者がのぞきにくることOK
  - 62%のユーザは商業利用でデータの共有OK
  - 52%のユーザはサービスをまたがるデータ集約OK
  - 38%のユーザ複数IoTデバイスをまたがるデータ集約OK

- TYPES　Project
  - Miguel Perez Subias: AUI Internet Users Association

- 90%は収集された個人データをcontrolできることは重要と思う
- 71%は代替サービスがないので、しかたなく個人データを晒してサービスを利用する。
- 1/7の人は収集されたデータの目的外利用に関心を持つ
- データポータビリティや透明性があれば、サービス提供者側に競争が生まれるので、良い方向になるが。

- TYPES (Towards transparency and privacy in the online advertising business) というプロジェクト
  - プライバシー保護を確保しつつ、サービス業者側が広告目的でユーザデータを利用できる仕組みを作る
  - つまり、ユーザに相当な自己情報コントロール能力を与える
  - この目的のための　ブラウザ・プラグインを開発

QUANTIFIED EMPLOYEE

- 個人の健康状態などまで定量評価された被雇用者のイメージ
- 当然、以下のような問題がある
  - 労働者の権利
  - プライバシー
  - 技術的プラットフォーム

QUANTIFIED EMPLOYEE
:Digi Clinic, Mehiläinen（発表者）

- ヘルシンキの代表的な私立病院の一つ
  - 外務省ホームページで紹介されている3つの病院うちの1つ
- データの種類
  - ① 同社が有する Occupational Data
  - ② KanTa のデータ
  - ③ Self Measurement Data
    - 自己測定データが容易に測定・蓄積可能になってきたし，医師がそれを参照できるようになってきた．(例：血圧，睡眠時間，労働時間など)
- 産業保健において，これらのデータを用いると
  - 医師がデータから労働環境を評価できたり，比較できたりする．
  - 労働能力(Working Ability)を評価できる。これらのデータを集約(gather)しようとしている．

- 加藤綾子の紹介記事より

QUANTIFIED EMPLOYEE
:Digi Clinic, Mehiläinen　つづき

- 労働環境と個人の健康・幸福
  - HeiaHeia (プラットフォーム)
    - ウェルネスや，ライフスタイルのデータ
  - HR プロフェッショナル (?) ＝法人顧客の話しを引用:
    - (法人は)被雇用者が自身の健康や労働能力に責任が持てるようにする必要がある.
  - 当初は，被雇用者がそうするためのツールが課題であった.
  - だが，Aikaniなど，ワークフローや時間を測定するためのアプリケーションが登場し，データを連携(combine)して，何にどれだけの時間を費やしているかが把握できるようになってきている.
  - メイン・イシュー
    - 産業保健の観点からは，従業員と医師の対話(Sessions)を支援するようなデータをどのように取得するかが問題である.
- 産業保健プロバイダーとして法人顧客に何をすべきか?
  - 我々は，被雇用者に対してコンサルやサポートができるし，彼らが働くことに関して責任が持てるよう補助することができる.

• 加藤綾子の紹介記事より

ECONOMICS OF DATA MANAGEMENT

- Privacy as a Business Enablerという考え：以下が一例
- スキポール空港を世界最高のデジタル空港のする　→ ポイントは
  - プライバシー保護
  - データセキュリティ
  - Trust＝（親密さ＋信用）／リスク
    - 親密さ＝対話性、透明性、公開性
- GDPRの精神を活かしたい
  - Privacy By Design

Privacy as a Business Enabler

- スキポール空港を世界最高のデジタル空港のする　→ ポイントは
  - プライバシー保護
  - データセキュリティ
  - Trust＝（親密さ＋信用）／リスク
    - 親密さ＝対話性、透明性、公開性
- GDPRの精神を活かしたい
  - Privacy By Design

第6，7会場のセッション：ワークショップ

- Academic workshop
- MyData business models
- Examples, experiences and case studies!
- Global winds from Japan to Silicon Valley　日本

- Critical technology education
- MyDatan mahdollisuudet kaupungeille (FI)
- Managing researcher's identity
- PIMS roundtable

Global winds from Japan to Silicon Valley

- 日本からの発表：日米共同セッション
- "Global winds from Japan to Silicon Valley:
- Personal Data Ecosystems over the Pacific"

- 日本における取り組みの全体像
  - *Kazue Sako (NEC)：司会
- 日本とEUの法制度比較，制度的課題と仮名化*Naoto Ikegai (東京大学)
  - *Hiroshi Nakagawa (東京大学)
- 分散PDSとPLRの紹介
  - *Koiti Hasida (東京大学)：セッションホスト
- 社会実装の取り組みとPersoniumの紹介
  - *Kazushi Ishigaki (富士通研究所)，*Akio Shimono (富士通)
- 銀行のメタファーを用いた社会デザインの試み
  - *Ryosuke Shibasaki (東京大学)，Hideki Sunahara (慶應義塾大学)
- 米国の法制度と市場動向
  - *Andreas Berger (Humada Inc.)，*Hans-Martin Hellebrand (Humada Inc.)

Personal Information Management Service (PIMS)

- 各システム，アプリケーションに概ね共通する基本機能
  - 事業者と個人の間で保有されている個人情報や取引履歴などを，個人の側で一元的に把握できる(Gather own data)
  - データ使用の如何を自分自身が決定できる(Access control)
  - 本人確認(Identity)
  - データ貯蔵庫：
  - パーソナルサーバ，パーソナルクラウドが主流か
- スタートアップ企業ベンチャーキャピタルや大手企業からの投資を獲得

3. 個人主導のデータ流通のストーリー、ユースケース

3.1. 個人サイドのストーリー

3.1.1. 食生活

最近の我が家は、みんな体調がいい。それは、数年前に家具や家電のほとんどを IoT 化したからであろう。きっかけは、私の病気と健康管理アドバイスサービスというサービスを知ったことだった。健康管理アドバイスサービスは、例えば、スマート調理家電を使って何を調理した

か、それをダイニングテーブルで家族の誰が何をどのくらい食べたかを記録し、1週間や1か月単位で確認できる。ベッドでは睡眠の時間や質を確認できる。そのおかげで、仕事がハードだった時や疲れていると感じたときは、起床時間から逆算した就寝時間が提案され、最適な睡眠時間をとることで、以前より疲れが残らなくなった。また、数年前から私の会社では昼食のカロリーや栄養素の可視化を行うサービスを導入したおかげで、私はその電子データを見て、1週間の栄養バランスを意識し始めた。妻の会社もそのようなサービスがあるらしい。子供の通う保育園での昼食の情報も電子的に見ることができるので、妻は私たちのデータを活用して夕飯の献立を立てる楽しみが増えたと言っている。

それは、栄養素やカロリーのデータをレシピアドバイスサービサーに提供することで、家族にとって最適なレシピの提案を受けることが出来るというものだそうだ。このレシピサービスでは、利用しているスマート調理家電の情報や食事のデータを登録することで、レシピに最適な設定をスマート調理家電で行うことができる。これによって、献立のレパートリーは増え、調理時間はグッと短縮した。これらのサービスは共働きの我々にとってとても助かっている。最近仕事のストレスで上がり気味の血圧も、科学的エビデンスに基づいたレシピサービスで血圧のコントロールが可能となった。

しかも、今日の献立を妻が選ぶとスーパーに、今晩のレシピに不足している食材のリストが送信され、取り置きをしてくれる。その値段と受取り番号が私のスマートフォンに送られてくるので、買い物もお会計だけであっという間に完了する。これもレシピアドバイスサービスの一部だ。

私の行きつけのスーパーマーケットは電子レシートを発行しているので、このスーパーマーケットで買った食材の情報はレシピアドバイスサービサーに提供している。このことで、レシピアドバイスサービスは、我が家の購入した食材と消費した食材を記録してくれることで、食材が余ることも捨てることも無くなりゴミがかなり減った。我が家の生活にとって、これらのデータを連携させたサービスは、なくてはならないものだ。

3.1.2. 子供の健康

「17 時 30 分時点の体温は 37.4℃。風邪の兆候あり。手洗いとうがいを念入りに。夕飯にはかぼちゃと人参の煮物がおすすめ。部屋の湿度に注意を。」健康管理アドバイスサービスから連絡が入った。ここ数日の子供の健康情報を見返すと、半年前に長引いた風邪のときと同じ兆候を示している。今週は大事な会議が控えており、仕事を休めそうにない。子供が風邪をひかないよう、今日はビタミン A の摂取と湿度に注意しなければと気を引き締めながら保育園の迎えに向かった。

我が家では、子供の食事、運動、睡眠、体温、予防接種などの健康に関する情報を電子的に記録している。特に子供が喜んでいるのが、手洗いとうがい、歯磨きをした記録が残るアプリで、毎日の頑張りが可視化されるのは大人も子供も同じようだ。電子化が進んだ保育園での健康情報も合わせて、健康管理アドバイスサービサーに提供することで、最適なアドバイスをもらえるようになった。そのおかげか、いままでよりも風邪で通院した回数はここ数年でグッと減った。

万が一、子供が病気になってしまった場合には、保育園をお休みにしなければならないが、夫婦ともにどうしても抜けられないことも多々ある。そんなときには、病児保育サービスやベビーシッターの確保を健康管理アドバイスサービサー経由で行っている。私がお願いしているベビーシッターは、病児への対応経験が豊富で、栄養士の資格を持っており、評判がとてもいいので、いつも安心して任せられる。

健康情報を提供することに最初は抵抗があったが、子供の成長に合わせた個別のアドバイスは、風邪の予防だけではなく、子育ての精神的なサポートにもなっている。いつでもどこでも確認できるので、旅先での急な体調不良への対処や、引っ越し先で小児科を初めて受診する際にも活用できる。当然ながら、保育園の申込や定期健康診査など公的サービス利用時にも反映が可能だ。

子供の健康情報には夫やベビーシッターもアクセスできる設定にしているので、私が体調不良でも適切に情報共有できる。健康情報を含めた PDS へのアクセス権限を子供自身に渡す日が正真正銘の自立と言えるのかもしれない。社会的意義の観点で考えれば、多くの人が出生時からの健康情報を提供することで、子供の病気やアレルギーの要因解明の一助となるかもしれない。PDS によって、社会全体で子供の健康を守ろうとする意識が広がるのではないかと考えている。

3.1.3. 祖父母の健康

私と妻の祖父母は共に遠く離れて夫婦二人で住んでいる。祖父母は 65 歳を超えており最近では医療機関にお世話になることも多くなってきた。国主導の医療データの標準化、一元管理が進み、医療のビッグデータの活用により、より質の高い医療の提供が受けられるようになってきた。数年前から祖父母の家でも家具や家電など IoT 化を進めており、離れていても普段の食事や行動の情報など把握することができるようになった。また、見守りサービスを行う企業が増えており、情報をタームリーに提供することで、緊急時の対応も受けられる。さらに、運動・食事などの情報も健康管理アドバイザーに提供し、最適な健康メニューのアドバイスも受けられるようになっており、祖父母の健康管理の関する意識も高まってきている。

3.1.4. 出張

国内出張となった。仕事が終わった後にその土地の名店などで料理やお酒を味わうのがいつもの楽しみだが、初めて行く土地なのでどこによいお店があるのか皆目見当がつかない。私は現在地と食事の予算規模と、普段の飲食の情報や健康情報をいくつかのグルメ検索サービスに提供し、私の好みや体調にあったおすすめのレストランを推薦してもらった。その中の 1 社が勧めてくれた普段よりもワンランク上のワインが飲める店が気に入ったので、そちらで食事をして良い時間を過ごすことができた。このように PDS には私の様々な飲食の記録が残っているため、各サービス会社はその情報から私の嗜好を読み取り、それぞれ独自の提案があり、そのサービス品質に非常に満足している。

この店での食事の情報もレシピアドバイスサービサーに提供されている。少し飲み過ぎたら

しく、臨床で有効性が確認された肝機能を低下させるサプリメントの服用を強く推奨された。
終日出先だったので携帯電話の電源が切れてしまったようだ。家族との連絡は取れないが、私の購買データや電車の乗降データは家族で共有できるから、妻はその気になれば、私の状況を把握できるだろう。

家族との連絡手段が無い状態で、私が災害や事故に遭い、特に私の意識が無い場合を想定し、我が家では、医師や救命救急士などの生命に関わる職業の人が健康に関する情報を必要な時に閲覧できるようにしている。仮に私が意識を失っている状態で、家族と連絡が取れない場合であっても、医師や救命救急士は、私の指紋や毛髪 DNA をアクセスキーにして私の PDS に蓄積されている健康情報を閲覧できるだろう。このようなサービスのお陰で、万が一持病を抱えていながら、かかりつけ医のいない見知らぬ土地でアクシデントに遭ったとしても安心して出張や旅行ができる。

もちろん、私の PDS へのアクセス履歴はログとして残っており、不正なデータの参照などによるプライバシー侵害リスクには対応しているが、当然ながら生命に関わる専門家による不正利用は無い。

3.2. 産業サイドのストーリー

3.2.1. 労働者の確保

今後、当社が取り組む新事業に必要な人材像が明確になったので、その人材像を基に求人を行っている。当社は、求める人材像を明確にするとともに、当社と共に仕事をすることがいかに本人にとってのキャリア形成に貢献するかも訴求している。

当社の求人に対して、様々な経歴、資格を持つ人材が応募してきている。本業で培っているノウハウを発揮して副業として当社の新事業立ち上げに貢献したい方や、育児との両立を重視し短時間の勤務で自分の経歴を活かして新事業立ち上げに貢献したい方や、次のキャリアアップを見据えて新事業の遂行を行いたい方など、動機もスキルセットもさまざまである。数年前なら、求人から長くて数か月待たなければ多くの応募が集まらなかったが、最近では、応募者が自分の PDS に蓄積しているキャリア情報や当社で即時応募も可能になっており、応募時にキャリア情報から想定されるキャリアプランの簡単なシミュレーションも見えるようにしたことも好評なようだ。

今では、業務で生成されたパーソナルデータについて、企業のオーナーシップが認められる側面と、できる限り個人にデータを還元しようとする側面のいずれの状況も、かなり進展している。当社でも、従業員の出勤時間や出勤日数などのデータは、機械可読式の電子データで保管し、従業員が各自のデータを PDS 経由で入手できるようにしている。当社の臨時職員の一人で、複数のパートタイムの仕事を掛け持ちしているある者は、各パート先の出勤簿のデータを PDS 経由で合算し、フリーランス向けの保険に加入しているそうだ。PDS で合算された総勤務時間のデータを根拠として、最近は有給休暇を取得したらしい。非正規雇用が大半を占める今、このようにワーカー個人が自分自身で労務管理をしたり、健康管理をしたりすることは、さほど珍しいことではなくなった。

当社では、スキルセット、マインドセットと業務とのマッチングにより、多様性に富んだ人材マネジメントを実現しており、最近では働きやすい企業ランキングの上位になってきた。

例えば当社では、ハンディキャップを有する者が数多く働いている。仮に本人が自分自身の状況について上手く説明することができない場合でも、就業上の忌避事項や、過去の業務実績のデータはPDSにあるため、必要に応じて当社の責任者が確認すればよい。歩行が困難であるため在宅勤務を希望する者や、対話が不得意であるが特定の作業に秀でた者、たとえ健康であっても体力が乏しい者など、働き方における個人の事情はさまざまである。当社では、本人同意のもとパーソナルデータを積極的に利活用しており、IoT デバイス等を用いて、勤務時間中の従業員の状況や仕事の達成度合いなどを適切かつ、つぶさにデータで把握している。これにより経営上の管理コストや従業員間の調整コストがかなり抑えられ、当社は従業員に対して今までのような平均的な働き方を課す必要がなくなった。個人の事情に応じた柔軟な働き方ができる当社の評判は高まり、有能な人材が次々に集まるようになった。労働人口が減少する中であっても当社が人材不足に悩むことはほとんど無い。

以前は、人事採用に多大な労力を要していた。今では、社会保障関連の届け出書類はすべて電子化されているし、有資格者の資格保有状況はオンラインで照会手続きを済ませることができる。また以前は、応募者の適性やスキル、経験値などを、主に履歴書と面接で評価し、判断の大部分は人事担当者の経験と勘に委ねるしかなかった。今では応募者が、前職の実績の根拠となるようなデータを個人の PDS 経由で開示してくれるため、採用側はそのデータをもとに応募者の経験値などを客観的に見積もることができるようになってきた。

例えば当社は介護事業も手掛けているが、そこでの事例を紹介しよう。有資格者である介護士やヘルパーが従事した業務内容は、介護報酬の算定やその根拠となる介護記録などによって把握可能である。介護サービス利用者のプライバシーを侵害しないよう利用者のデータとは切り離した上で、当社は介護記録などをもとに、介護業務を行った介護士やヘルパーの業務実績を得点化してそのデータを本人に還元している。介護士やヘルパーは、ワーカーとして業務行為を重ねる毎に、この得点を伸ばすことができる。得点データはワーカー個人が PDS に蓄積しているため、転職・求職時には本人がそのデータを自身の実績証明として活用することができる。

当社のみならず他社も、業務実績を得点化して個人に還元するようになってきている。当社が最近採用した介護士は、ここ数年、出産・育児と親の介護が重なり、資格を活かして介護関連の職に就いたとしても、長時間や長期間の勤務が続けられない状況にあった。しかしながら、その介護士の PDS に蓄積されている業務実績の得点データを参照すると、当社が必要としている業務経験を豊富に有していることが分かった。そこで、当社はその経験を買って採用し、その介護士には本人の経験を活かすことのできる業務を割り当てるようにしている。

このように、個人の実績証明となるようなデータを PDS 経由で確認できるようになって以降、人材と業務のミスマッチングが格段に減っている。適材適所の人材を採用し配置できるようになったため、当社のサービスに対する利用者からの評判は大きく向上した。また、従業員が皆それぞれ個別の事情を抱えながらも、いきいきと働いているため、当社は人気企業の一つに

数えられている。さらに当社は、従業員に対して可能な限り就労関連データや業務実績データを還元しており、そのデータの精度も高いため、従業員が離職した後の転職先企業からの評判も良い。

また、当社と関わりのあった人材に対しては、当社を退職した後であっても、最新のキャリア情報を参照する本人許諾がある限り、キャリア情報に基づいて本人のキャリア形成に貢献しうる業務のオファーを出している。このような形で、当社は従業員や過去従業員だった者との信頼関係の形成に努めており、結果的には新たなリクルート手段の獲得に繋がっている。

ところで、HEMS のデータや、活動量計などのデータ、移動履歴のデータなどが個人の PDS に集約されてくると、それらのデータをもとに個人の体力とその消耗度合い、稼働量などが推計できるようになってくるだろう。他方で、これまで家庭内で、家事や育児、介護などに専念していた者が働きに出るようになると、家事代行サービスの需要が高まる可能性がある。当社はこの新規需要に着目し、個人が許諾した範囲の PDS データを用いて、個人の生活全般をサポートするサービスを立ち上げようと目論んでいる。ただし、家事代行サービスを常時利用する敷居はまだ高いようで、よほど仕事が立て込むタイミングや健康状態が芳しくない時のみ利用したいという声がしばしば聞こえてくる。そこで、当社の新規事業では、PDS のデータから、個人が次に置かれることになるであろう状態を先回りして分析・予測し、成約率の高まりそうなタイミングで、必要とされるサービスの選択肢を提案する仕組みを開発しようとしている。なお、家事代行を行うワーカーについても、ワーカー個人の適性や経験が PDS のデータをもとに精査されるので、彼らの多様な働き方もまた確保されることとなるだろう。当社はこのような雇用とサービスの創出を通じて、社会的な価値を生み出している。

3.2.2. 新サービス創出

医療分野では、病院、診療所のような医療機関、及び医学系研究機関や製薬企業において、診断・治療や手術等から得られた膨大な医療データから、エビデンスに基づいた最適な治療、投薬が可能になっている。しかし、以前のヘルスケア分野では、食事の情報、睡眠の情報、運動の情報、生活環境の情報など健康に影響を与えうるデータは収集されていたとしても各サービサーに分散して管理されていたため、ヘルスケア分野でのエビデンスに基づく健康維持アドバイスサービスなどは極めて困難であった。

しかし、数年前から PDS によって個人の一生涯を通じたヘルスケア情報が医療データと共に一元的に集約され、必要な情報を自らの意思で提供することが可能になったことで、健康度合いと健康に影響を与えうる因子の因果関係の分析による個人に最適な健康管理アドバイスサービスが立ち上がった。また、IoT 化の進展によって、これまで同時に取得が困難だった情報をリアルタイムに取得し、活用することが可能となった。

健康管理アドバイスサービスの立ち上げ後、PDS を利用する人も増え、健康管理アドバイスサービスの会員数も増えることで、データ分析による因果関係の予測精度が向上し、更なる会員増につながるなど、情報のエコシステムが循環するようになり、この新規サービスは軌道に乗りつつある。

3.2.3. 蓄積データのマネタイズ

健康管理アドバイスサービサーである当社には、個人に名寄せされた形で運動や食事など健康に関する情報が集約されているので、ヘルスケア領域の PDS 事業者と言えるかもしれない。

当社に対して、ベンチャー企業が当社の会員向けにデータを活用したサービスを提供したい旨の申し出があった。当社の会員に対する付加価値向上に繋がりうるので、本人同意のあった会員のデータをベンチャー企業に提供し、ベンチャー企業がサービス提供することとなった。

当社はデータ提供するにあたって、クラウド技術を活用している。こうすることで、実際のデータそのものを提供するのではなく、当社の用意したインタフェースで分析に必要な情報を必要に応じて利用可能としている。データのダウンロードや転送などの機能は無い。データの活用に関して本人同意もとより、データの安全管理措置などの観点からセキュリティ対策を行った上で、基準を満たした企業が会員データを分析する方法をとっている。

ベンチャー企業が当社の会員データを活用して開発したサービスは、収益の一部を、当社にレベニューシェアする方法を取り入れている。こうすることで、当社はデータの利活用に協力いただいている会員に一部還元をしている。他方でベンチャー企業は自社の運営資金や次回の開発費などに充てているようだ。さらに、こうした取り組みの場合、当社は該当サービスにご協力いただいているベンチャー企業名や紹介の記事などを掲出することで、両社の関係が良好になるよう努めている。

3.3. ユースケース別の個人の価値、産業的価値、社会的価値の整理

3.3.1. 訪日外国人向け観光における PDS を活用したデータ流通

外国人が訪日旅行履歴や今回の旅行に対するニーズを表明し、それに対し地方が魅力的な観光プランなどの提案を行うこと、及び両者のマッチングを行うことをユースケースとして取り上げる。

表に地方自治体や各サービス提供者(ホテル、土産物屋など)が各々に観光客データを集めて活用する場合と比較して、PDS の仕組みによるデータ流通を実現したときの価値(社会、産業、および個人)についてまとめた。

表 3　インバウンド領域で PDS を導入することにより得られる価値

価値の種類	得られる主な価値
社会的価値	地方の観光活性化による地方創生および訪日外国人客の増大、おもてなしサービスの高度化、それによる世界から見た日本への評価の向上
産業的価値 (地方自治体，ホテルなど)	旅行者のニーズに対する自社サービスのアピール、満足度の高いサービスの提供による企業評価の向上、マーケティングのためのデータ収集のコスト削減、地方の魅力のある観光資源の発掘および集客戦略の立案

個人価値 (訪日外国人)	自分の嗜好や期待に見合う旅体験の享受(旅行計画時の労力の削減、旅行中の自身の体調面やアレルギー、好み等に応じた適切なサービスの享受)、宿泊時のチェックインや旅行保険の加入手続き等の各種煩雑な手続きの簡略化・帰国後のお気に入り地域情報の享受

利用した旅行会社や無線 LAN サービスなどが各々で過去の訪日外国人の情報を蓄積する現状では、個人の属性や趣味趣向に関するデータが分散してしまっている。つまり、各事業者や地方自治体は一部のパーソナルデータのうちで分析することになり、「実際の多くの訪日外国人にとって、魅力のある観光資源やサービス(モノやコト)とは何か」を正確に掴むことはできない。その結果、発信力のある大都市や有名観光地にのみ旅行者が集中することになり、地方はニーズを知り、それに応える機会が少なかった。PDS の導入は、訪日外国人個人の情報を幅広く提供、流通させることにより、上記のような 3 者の価値を生み出すことができると考える。

3.3.2. キャリア形成 PDS

個人の就業関連データ(勤務データ、給与関連データ、人事データ、仕事実績等)を雇用主のみならず、個人も PDS で管理することによって、個人が自分の意思で就業機会を広げることができる。また、個人が保有する仕事の実績データを用いることで、人材の適切な再配置や業務割当てが可能となり、社会全体として生産性向上を図ることができる。

表 4　キャリア形成領域で PDS を導入することにより得られる価値

価値の種類	得られる主な価値
社会的価値	PDS の就業関連データ活用による高精度かつ効率的な業務割当てや人材の再配置は、労働人口減少に伴う労働力不足の解消および労働生産性の向上に寄与する。また、PDS データによる実績証明は、雇用や業務委託のミスマッチを防ぐ。ハンディキャップを有する者や非定型的な働き方を希望する個人が、就労に際する制約事項などのデータを PDS に入れておくことで、事業者等は多様なバックグラウンドの人材を採用し易くなる。これにより多様な就労形態の実現が促進される。就業関連データが事業者等による縦割り管理ではなく、個人による一元管理となるため、人材流動性の向上も期待される。
産業的価値 (雇用事業者)	事業者等はこれまで多くの場合、履歴書と面談で人材のスキルや適性を判断しなければならなかったが、これは必ずしも容易ではない。仕事の実績データが個人から提供されるようになれば、事業者等はより高い精度で人材を評価・選定し、効率的に業務割当てを行い、ひいては生産性向上を図ることができるだろう。人材仲介業やクラウドソーシング業界は、PDS の就業関連データを用いた質の高いマッチング・サービスを提供することで競争優位性

	の獲得を図ることができる。
個人価値 (勤労者)	就業関連データはこれまで雇用主単位で管理されることが多かった。パートタイム就労やダブルワーク、フリーランス等の多様な働き方が広がる中、個人が複数の事業者等との間に業務契約を有する場合であっても、それらのデータを個人の PDS で一元管理することができれば、蓄積された時系列データを個人の一連の実績証明として用いることができる。また、個人が自身の実績データを保有して事業者間を異動できるようになれば、転職や休職などがあっても、キャリアの中断や分断を防ぐことができる。

3.3.3. ヘルスケア

〇ヘルスケア領域における PDS 型データ流通によって目指す未来像

- いつでも、どこでも自分の過去データをベースとした最適な医療を迅速に受けることができる
- 個人に最適化された健康指導や(先制)医療により、発症予防・重症化予防が行われ、健康寿命が延伸される
- 取得・集積される健康・医療データは学術的に付加価値が高いため、これらデータの解析から疾病発症のメカニズム等が解明される
- 新たな疾病・介護予防産業の創出や治療技術革新へ貢献する

〇未来像実現の手段としての PDS 型データ流通の位置づけ

- 個人の健康・医療データの非連続性(胎児期、出生～幼児期、少年・青年期、中年期、壮年期、老年期)の解消と見える化の実現
- 各データホルダーが個々の目的でデータを集積して個々のシステムで管理していた各健康・医療データが統合されて個人による一元管理が可能

表 5　ヘルスケア領域で PDS を導入することにより得られる価値

価値の種類	得られる主な価値
社会的価値	・健康寿命の延伸によって労働生産人口が拡大して、日本経済の活性化が期待される ・いつでもどこでも最適な医療が迅速に受けられる安心・安全な社会の形成 ・医療先進国日本をアピールできグローバルにおける地位向上が期待される ・健康医療において「治療から予防へ」のパラダイムシフトにより、医療費の適正化が期待される。
産業的価値 (健康サービス産	・科学的根拠のある新しい健康サービス提供産業の振興 ・製薬産業における新薬・治療法や新技術の開発

業、製薬産業、医療機器産業など）	・医療機器産業における新しい医療機器や医療システムの開発 ・医療機関、保険者、自治体等は個々のシステムで管理していた健康・医療データを保有する必要はなく、個人データ流出リスクやコストの低減が期待される
個人価値	・個人で自分の健康・医療データを一元管理可能となり、「見える化」によって健康管理意識が高まる。さらに個人に最適化された健康指導や（先制）医療が受けられるため、健康寿命が延伸して、健康上の問題で日常生活が制限されない状態で長い期間生活できる ・旅先や転居先においても健康指導や（先制）医療が受けられ、安心できる。

3.3.4. 消費（小売り・広告）

昨年度報告書から引き続き、消費者が信頼する企業へデータ開示が可能な PDS の仕組みと共に、事業者間のデータ流通を消費者が管理(コントロール)することによって、消費者の質の高いディープデータを事業者がマーケティングに利活用し、生活者の消費活動の効率化や利益最大化を実現するための仕組みとなる CSP(Consumer Side Platform)をユースケースとして推し進める。

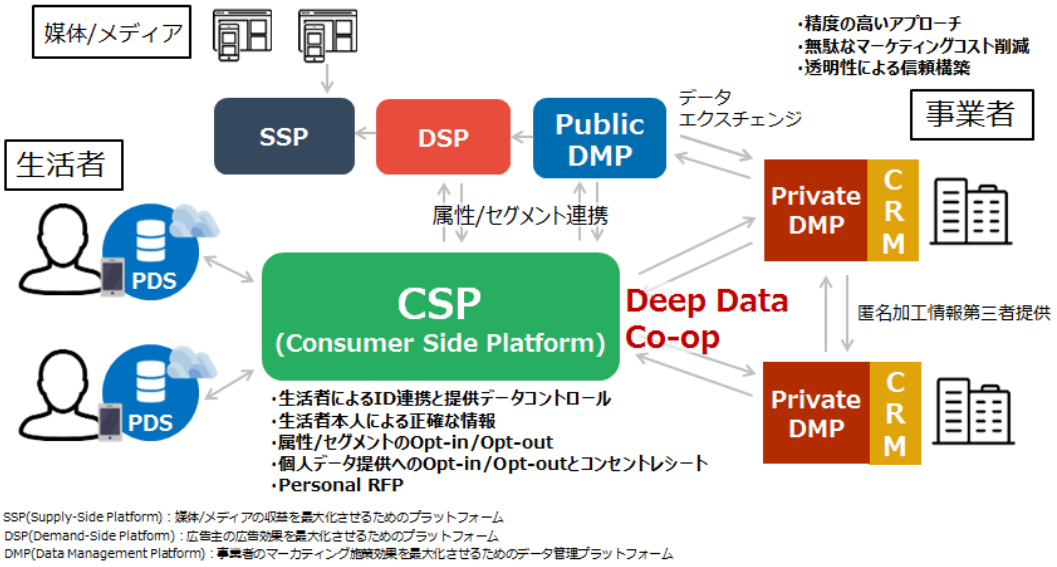


図 1.1：データ流通における CSP(Consumer Side Platform)の概略図

表 6　消費領域で PDS を導入することにより得られる価値

価値の種類	得られる主な価値
社会的価値	消費者による自己情報コントールが実現すれば、透明性や説明責任を果たして消費者から信頼される事業者へ多くの消費行動データが流れ、更にその事業者が消費者の求めるサービスを提供するグッドサイクルになれば、それらの事業者に更に多くのデータ流通が進むことになり、消費者からの信頼を得られない

	事業者が淘汰され、健全な市場競争が生まれる。
産業的価値 (広告産業など)	近年のアドテクノロジーに代表されるマーケティングテクノロジーの進化は著しく、特に効率最大化を目的として、適切な商品やサービスを適切なタイミングに適切なヒトへマーケティングする仕組みは進化しているものの、既に購入済みの商品情報や消費者自身による正確なデモ属性・意識情報が得られれば、広告やプロモーションの“無駄撃ち”を削減し、更に効率的なマーケティングができるだけでなく、消費者の需要創出を目的としたマーケティングによって消費市場の拡大も期待できる。
個人価値	これまで消費行動データの流通は事業者が中心となり、自身のどのような情報がどのような目的でどのような事業者に渡っているのかを把握することは困難で、知らずのうちに誰かに“自分のことを自分以上に知られてしまう”リスクがあった。消費者が中心となってデータ流通が実現できれば自身が信頼する事業者にのみデータの開示やデータエクスチェンジがされるようになる。 正確な情報を事業者に提供、もしくは事業者保有データの修正が出来ることによって、的はずれな広告/プロモーションとのタッチポイントが減少し、自身の求める情報提供や精度の高い広告やレコメンドを受けることができる。

4. 生活者受容性調査

4.1. 第三回 ビッグデータで取り扱う生活者情報に関する意識調査

4.1.1. 調査目的及び調査概要

株式会社日立製作所と株式会社博報堂は、両社におけるビッグデータ利活用の事業推進の一環として、パーソナルデータ利活用に対する生活者の意識を調査した「第三回 ビッグデータで取り扱う生活者情報に関する意識調査」を協働で実施した。当該調査の目的は、パーソナルデータの利活用が進む中、生活者の意識の変化や新たな技術に対する関心などを定量的に把握することを目的としている。また、2013 年に第一回、2014 年に第二回の調査を行っており、今回で三回目の調査となる。調査概要は以下の通りである。

【調査概要】

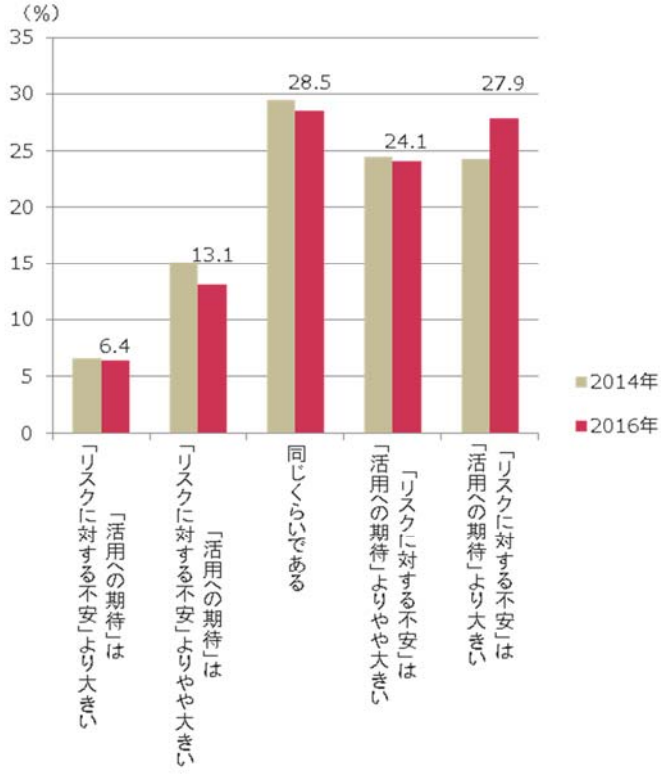
調査手法	インターネット調査
サンプル数	計 1,030 名
対象者	成人男女 (20 代～60 代の男女、性別ごとに 10 歳きざみを 1 セルとして各セル 103 名)
エリア	全国
調査時期	2016 年 9 月 15 日
実施者	株式会社日立製作所、株式会社博報堂

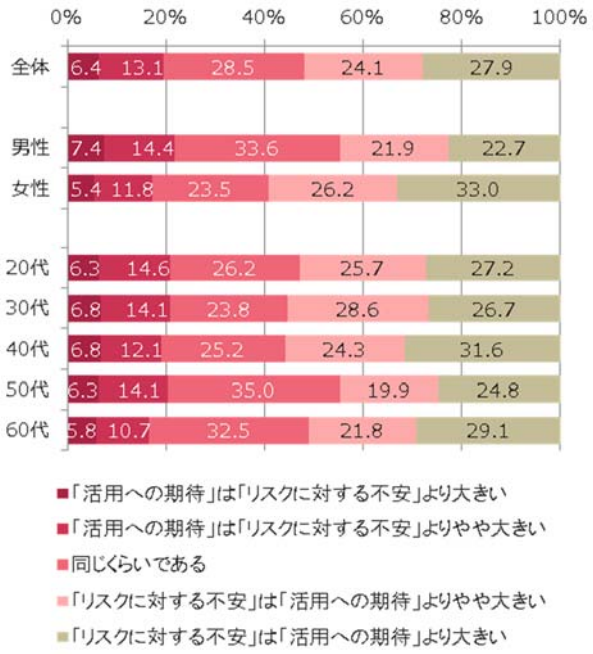
4.1.2. 調査結果

【パーソナルデータ利活用に対する期待と不安の比較】

「不安が期待より大きい」が、やや増加したものの、「不安が期待より大きい/やや大きい」と回答した生活者が約半数と同等である。

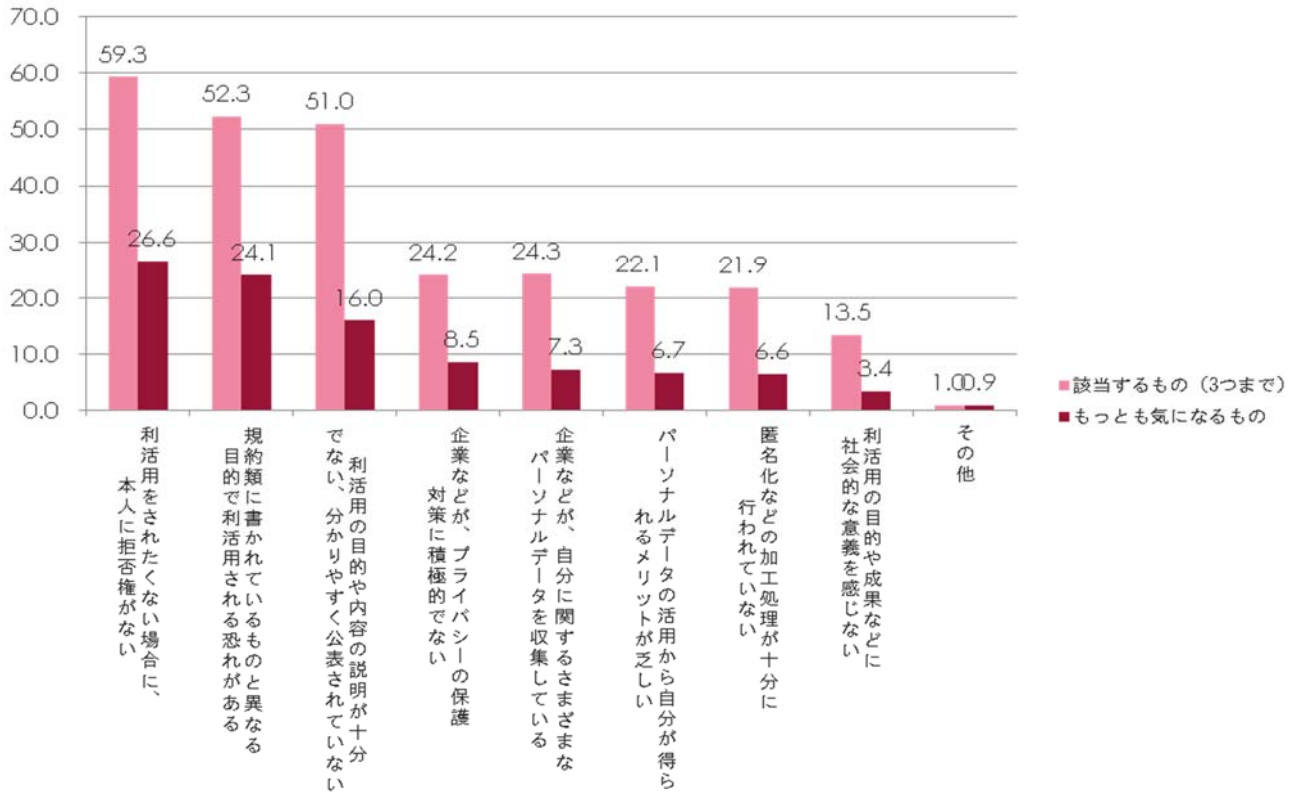
・ 女性の方が男性よりも不安が大きい傾向にある。





【パーソナルデータ利活用に対する不安の要因】

・ 不安要因として「利活用に対する拒否権がない」、「規約類に書かれた目的以外で利用されるおそれ」、「説明が十分でない、公表の分かりやすさの不足」の 3 項目が高い。



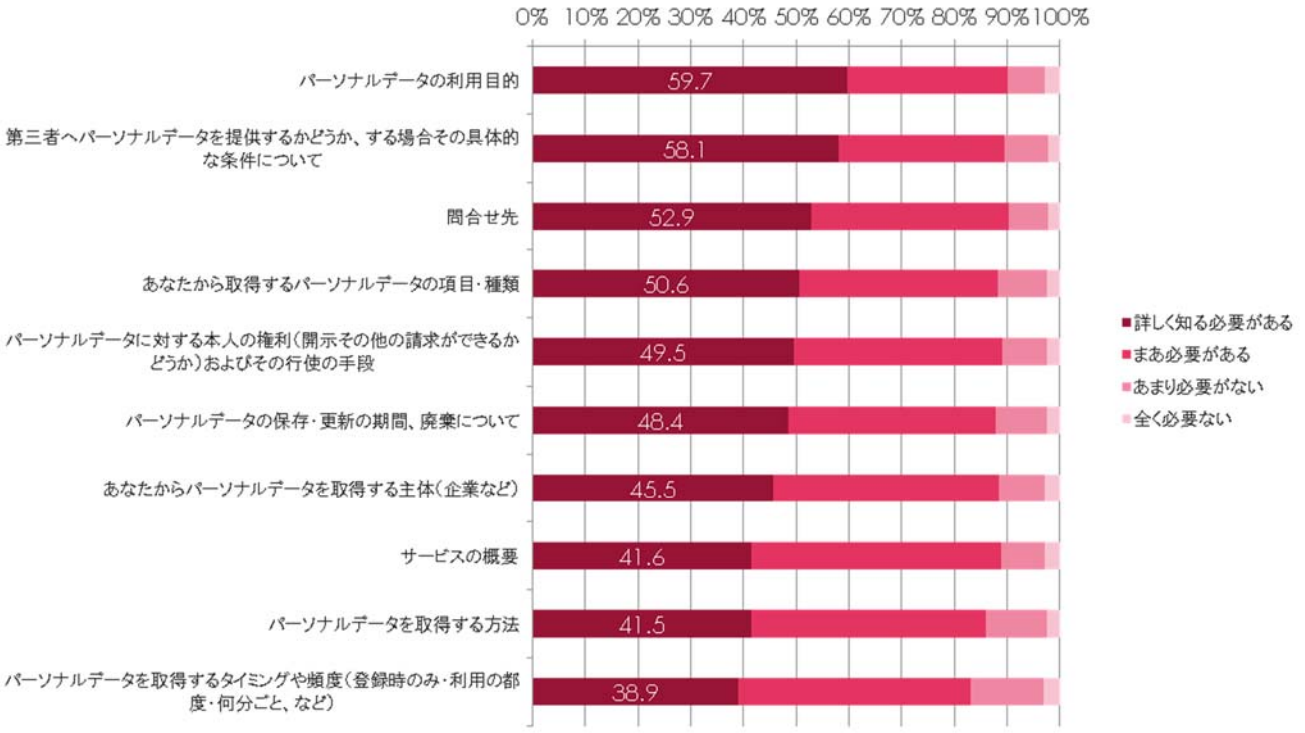
【生活者の不安を軽減させるための対策】

不安軽減につながる対策として、「いつでも利用を停止することができる」、「利用終了後、適切に破棄する」という施策においては 7 割以上の回答者が、不安が軽減すると回答している。

不安を覚える主な理由（該当者数）	利用に対する拒否権がない（n= 542）		当初と異なる目的での利用（n= 478）		説明・公表が不十分（n= 466）	
不安が軽減する対策 1位	本人からの求めがあれば、いつでもパーソナルデータの利用を停止する	77.5%	本人からの求めがあれば、いつでもパーソナルデータの利用を停止する	77.8%	本人からの求めがあれば、いつでもパーソナルデータの利用を停止する	74.5%
2位	利用終了後、パーソナルデータを適切に破棄する	73.6%	利用終了後、パーソナルデータを適切に破棄する	77.0%	利用終了後、パーソナルデータを適切に破棄する	71.0%
3位	パーソナルデータを第三者に提供しないこと、または提供する場合は同意取得する	73.4%	利用するパーソナルデータを限定する	76.6%	パーソナルデータの利用目的を限定、明確化する	70.8%

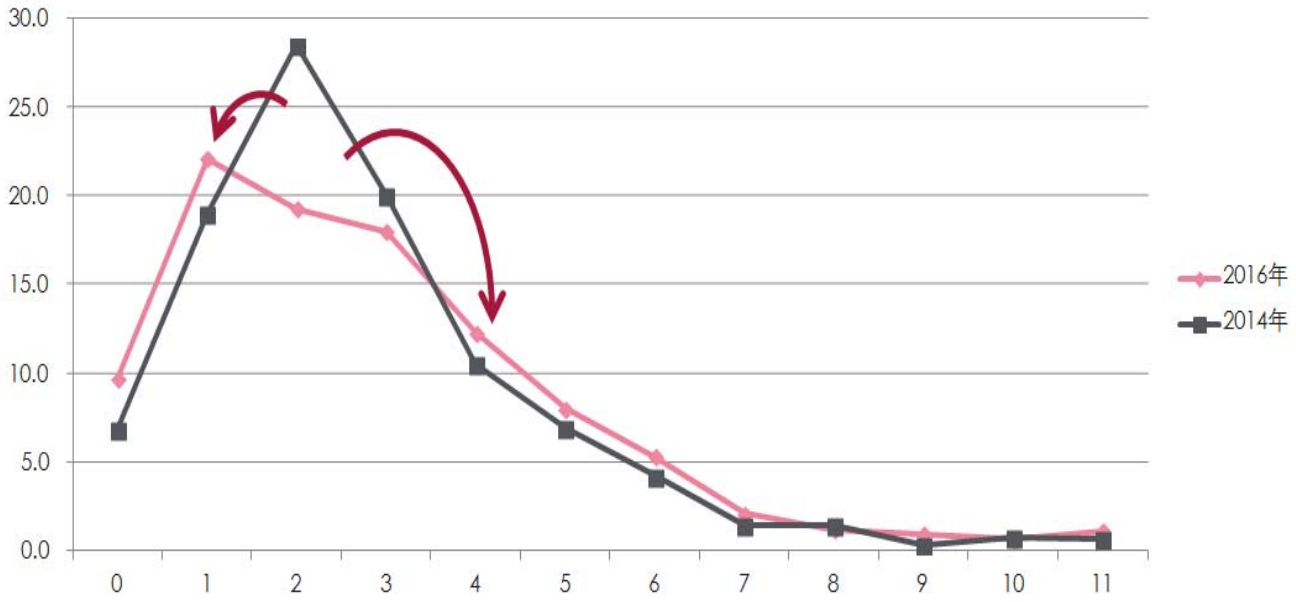
【生活者への説明内容】

パーソナルデータの利活用にあたって、生活者に詳細な説明が求められている内容として、「利用目的」、「第三者提供の有無」、「問い合わせ先」が高い傾向にある。



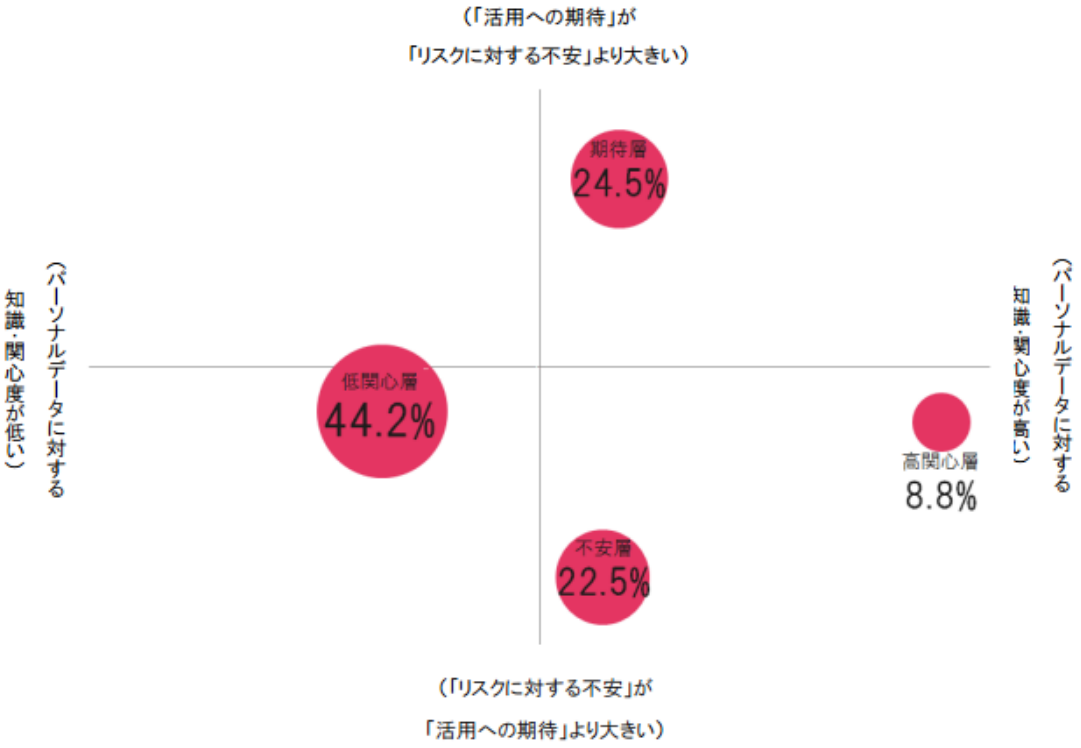
【パーソナルデータ利活用に対する知識・関心】

パーソナルデータの活用に対する「知識・関心」度の状況を調べると、2014 年調査時の分布状況と比べて、平均スコアはやや向上したが、全体として「高知識・高関心」、「低知識・低関心」の両方向への分散が目立ち、二極化の始まりとも見られる傾向にある。



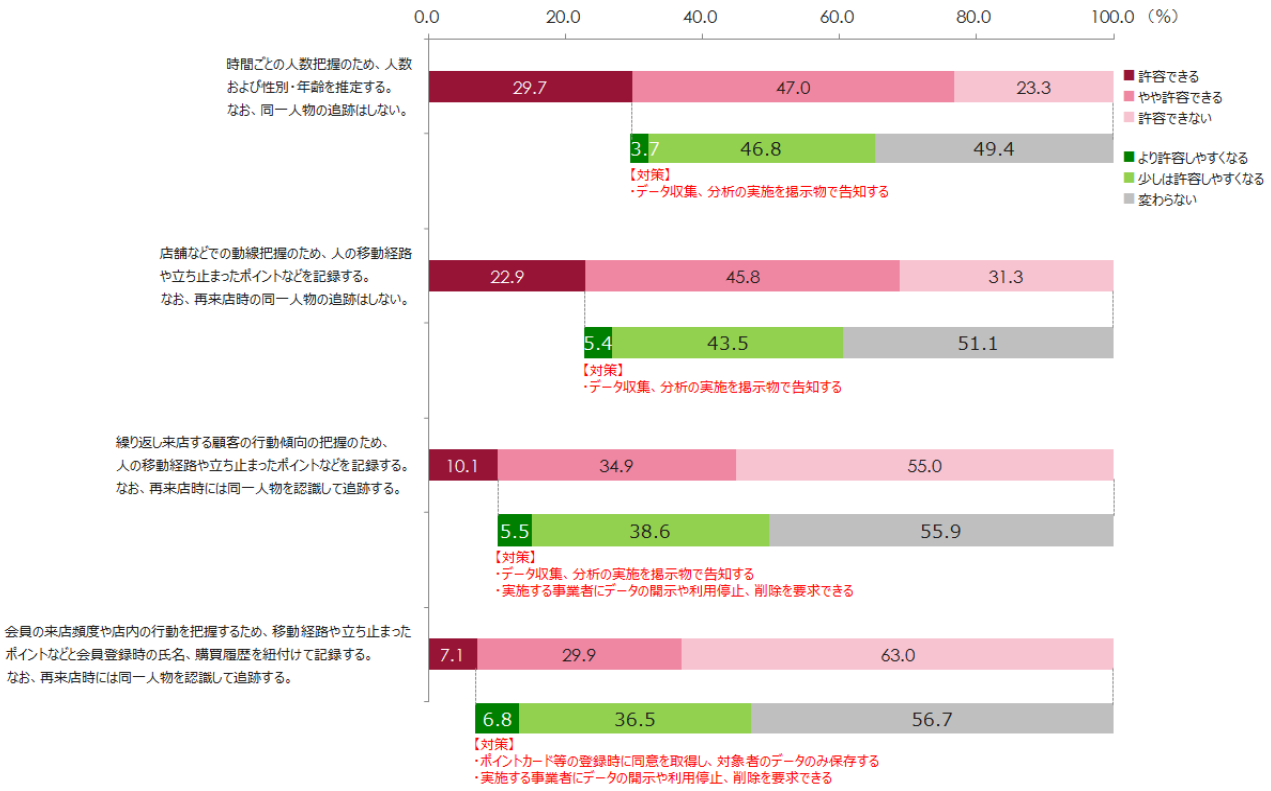
【生活者の分類】

・　パーソナルデータに対する知識・関心度と、期待/不安の度合いをかけ合わせてマップ化した。
・　知識や関心が低いまま漠然とした不安を示す「低関心層」が一番大きなグループを形成している。
・　ややパーソナルデータに対する知識・関心度が高い層においては、期待/不安を示す 2 つのグループが存在している。
・　さらに、知識・関心度が高く、やや不安が大きいグループである「高関心層」が存在している。



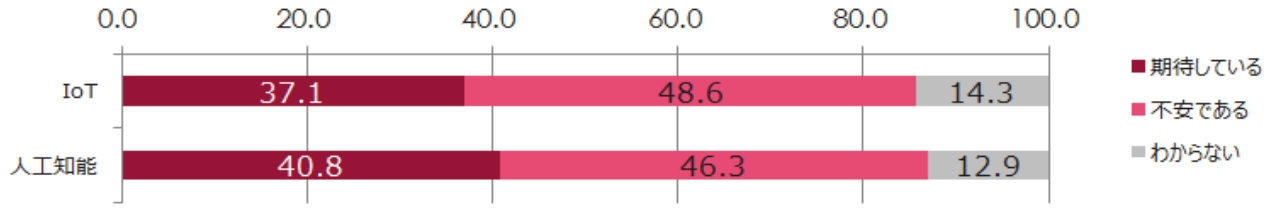
【カメラ映像利活用に対する許容度】

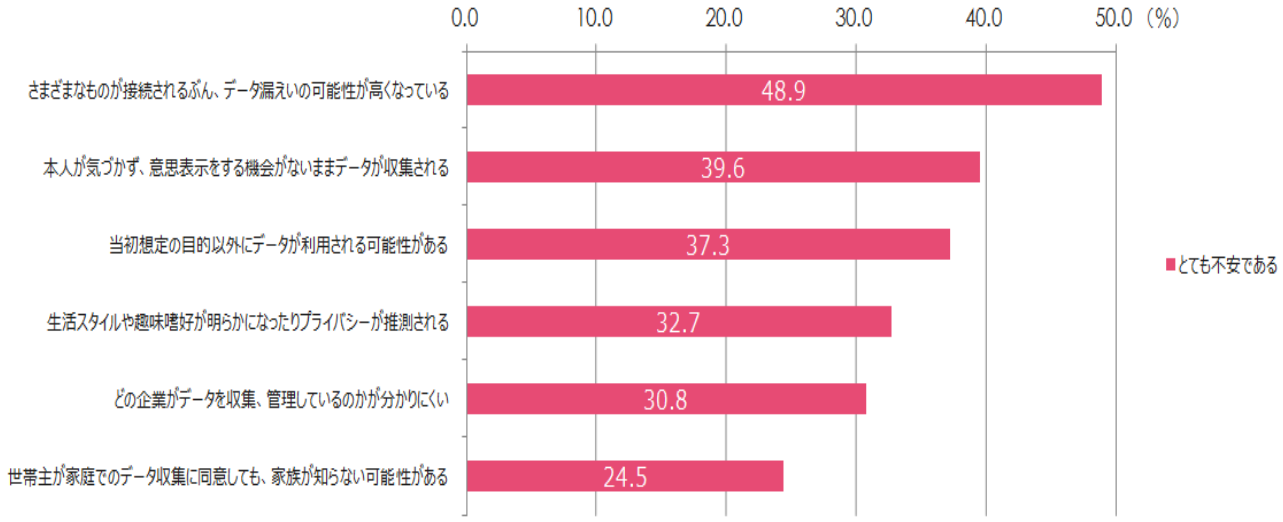
公共空間内のカメラ映像利用では、告知や本人請求への対応で約半数の回答者の許容度が向上している。



【IoT・人工知能への期待と不安】

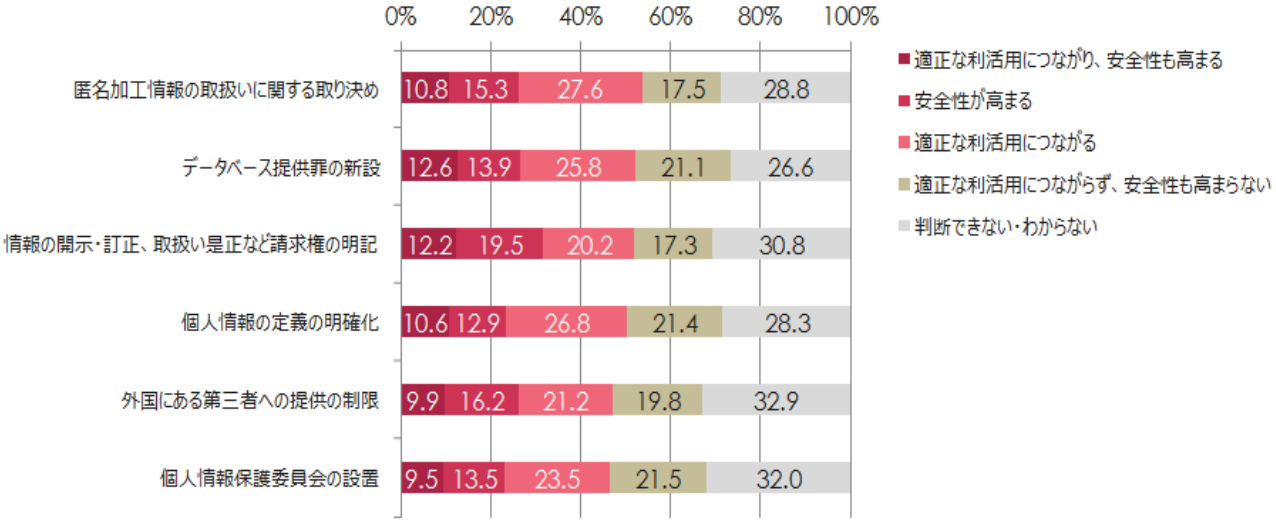
- 急速な成長を見せる IoT、人工知能の分野でのプライバシーに不安を覚える生活者は約半数となる。
- 情報量の急増や処理の高度化による、『意図せざる』リスクへの対策が課題である。





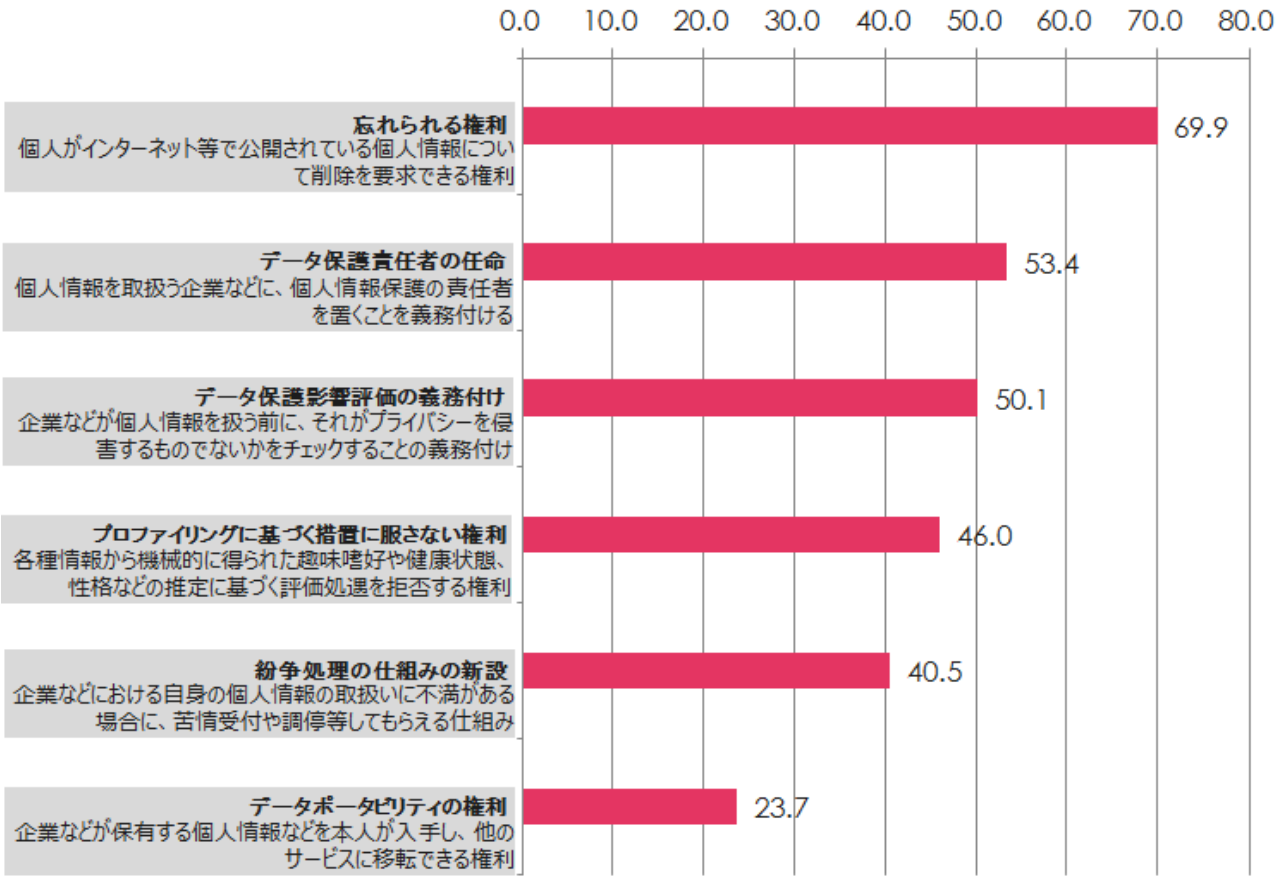
【改正個人情報保護法に対する評価】

法改正について、「企業による適正な利活用」または「個人の安全性が高まる」と一定の評価を得ていることが分かった。一方で 3 割が判断できないと回答している。



【今後の法制度検討において検討するべき項目】

今後の法規制検討で重要とされるのは、「忘れられる権利」「データ保護責任者の任命」「データ保護影響評価の義務化」が高い。



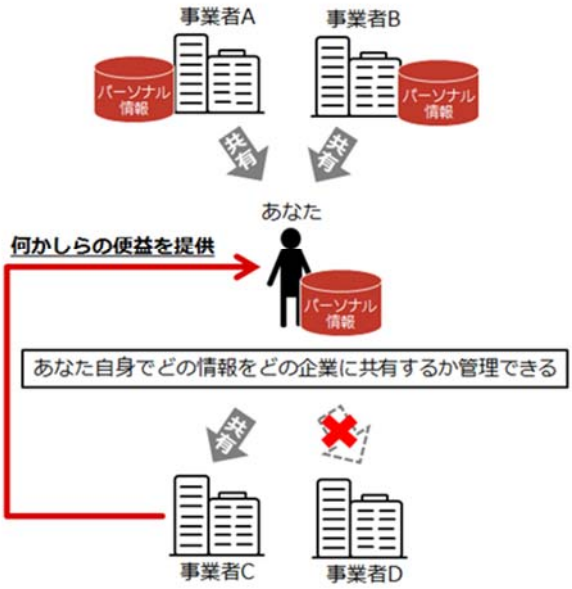
4.2.　インテージ実施「データ流通とプライバシーに関する意識調査」

【調査概要】

調査手法	インターネット調査 ※インターネット人口でウェイトバック集計
サンプル数	計 10,000 名
対象者	成人男女 （20 代～60 代の男女、性別ごとに 10 歳刻みを 1 セルとして各セル 1,000 名）
エリア	全国
調査時期	2016 年 9 月 30 日～10 月 2 日
実施者	株式会社インテージ

回答者は PDS や情報銀行について事前知識が無いことを前提に、それぞれ「個人が自分の情報を管理できる仕組み」「個人が自分の情報を信頼できる者に託し本人や社会のために活用する仕組み」として図とともにそれぞれが保有する機能を提示した上で利用意向を聞いている。それらは、本報告書に記載されている PDS と情報銀行の定義とは厳密には異なることには留意したい。

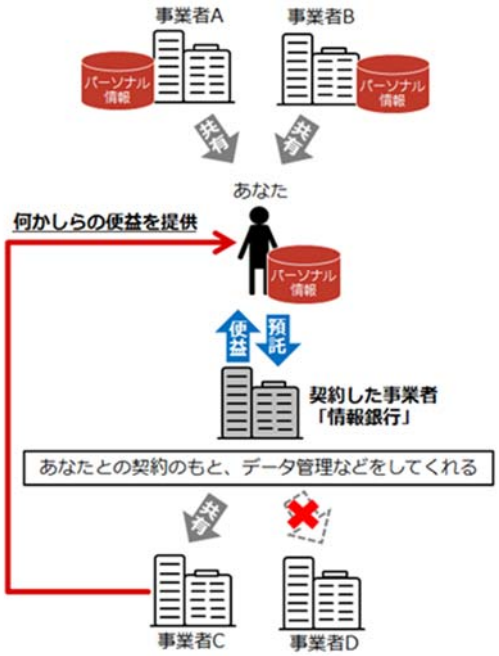
個人が自分の情報を管理できる仕組み「PDS」



- ✓ 企業が保有しているあなたの情報を閲覧できる
- ✓ 企業が保有しているあなたの情報の第三者提供先と何を提供されるのかを自分で選択できる
- ✓ 企業があなたの同意を得ずにあなたの情報を第三者へ提供していないか追跡できる
- ✓ 様々な企業が保有しているあなたの情報を自分に集約できる
- ✓ あなたが集約・保有している情報の共有先と何を共有するのかを選択できる
- ✓ あなたが共有した情報の企業による利用履歴を確認できる

etc.

個人が自分の情報を信頼できる者に託し本人や社会のために活用する仕組み「情報銀行」

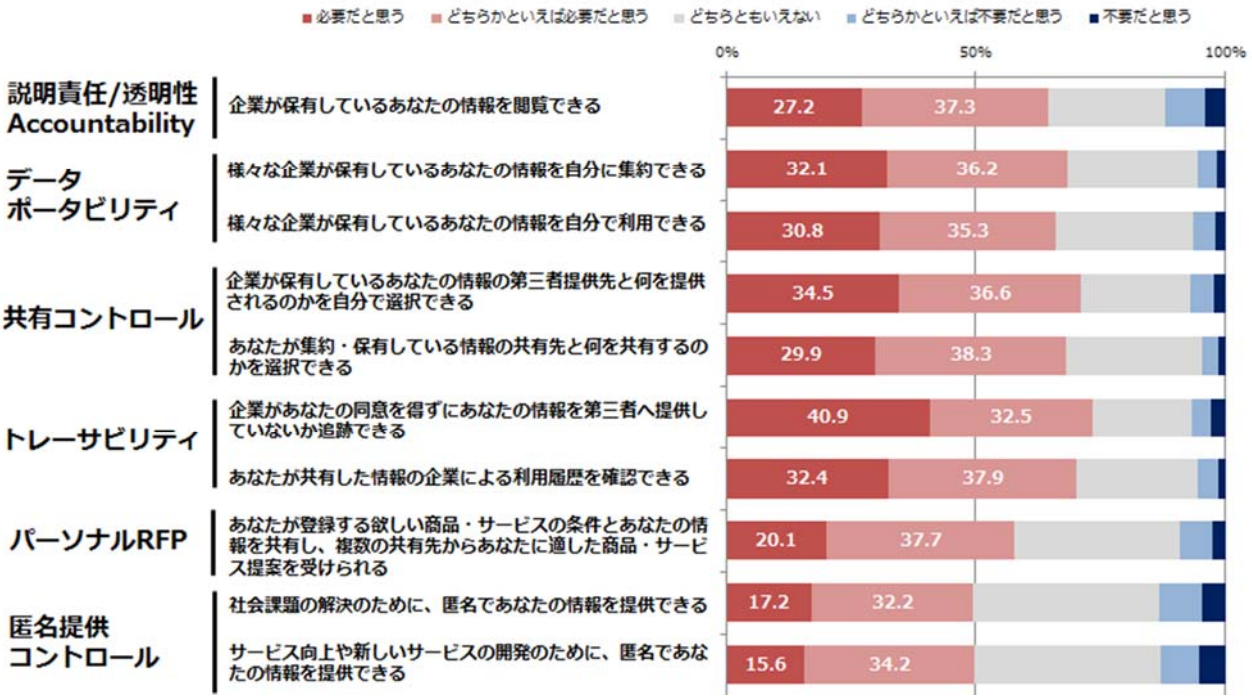


- ✓ あなたの情報を様々な企業から集約してくれる
- ✓ あなたの情報の提供を代理し、情報提供先からポイント還元などを受けられる
- ✓ あなたが登録する欲しい商品・サービスの条件とあなたの情報の共有を代理し、複数の共有先からあなたに適したサービス提案を受けられる
- ✓ あなたの情報を分析し、第三者に情報を提供・共有することなく、あなたが興味関心ありそうなサービスや商品をレコメンド（推薦）してくれる

etc.

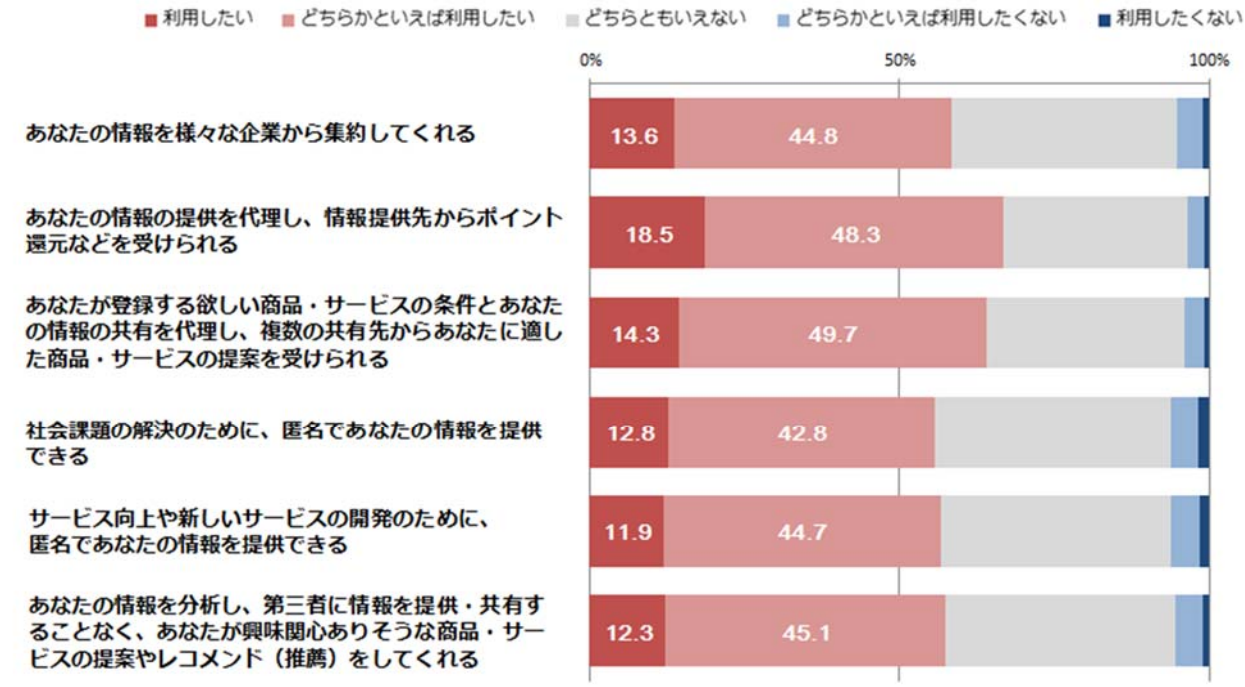
PDS 各機能の必要性

※PDSを利用したい人ベース

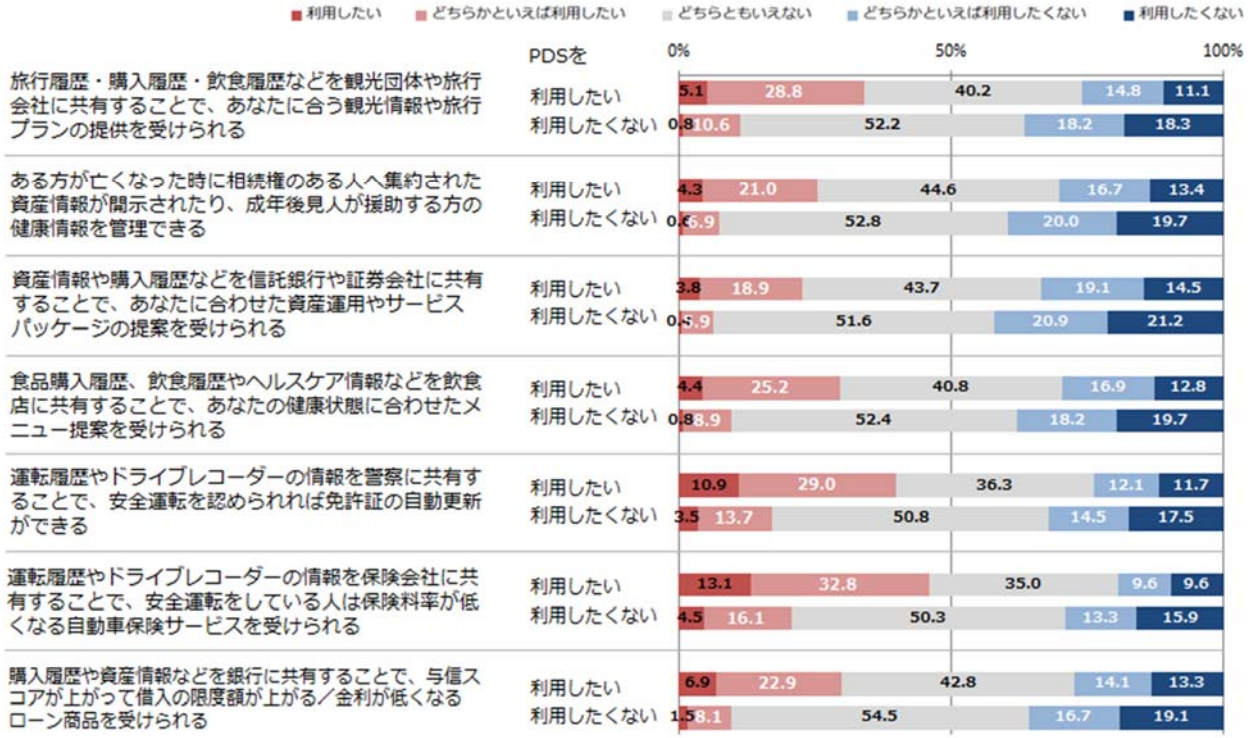


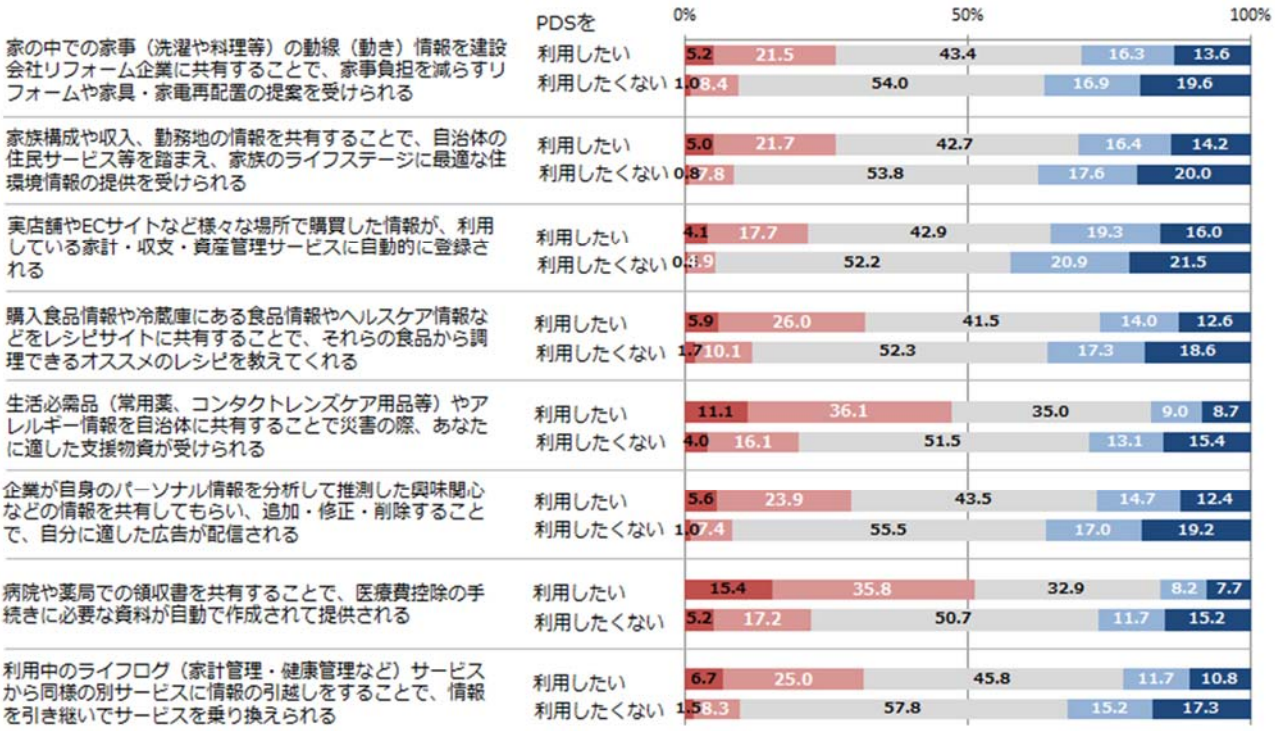
情報銀行 各機能の利用意向

※情報銀行を利用したい人ベース



PDS/情報銀行のユースケース





5. 未来価値創造ワークショップ

本プロジェクトで策定されたビジョン「個人ひとり一人が、自分自身のパーソナルデータを安心して最大限活用し、生活を自ら豊かにする社会」を検証するために、未来創造デザインワークショップ（以下では未来創造デザイン WS）を実施した。以下概要を示す。

日時：2016年12月11日（日曜日） 9:00～17:30

参加者：本 COCN プロジェクトメンバー、家のハックを実施している先進ユーザ、UX およびサービスデザインの専門家、学生、女性、シニア等25名程度

ワークショップの流れ：

	9:00-9:30	Check-in
午前	9:30-9:45	STEP 0. オープニング
	9:45-10:15	STEP 1. ペルソナ設定
	10:15-10:45	STEP 2. フォーカスポイント決定：ペルソナ & 利用シーン
	10:45-11:15	STEP 3. ペルソナの切実なニーズとゴールの具体化
	11:15-12:00	STEP 4. IoTで実現する/IoTで変えられる生活のアイデア創出
	12:00-13:00	未来図スキット・昼食
	13:00-13:15	午後の流れ紹介
	13:15-14:00	STEP 5. エコシステム：だれが何をしてどのように協力するのか？
午後	14:00-15:00	STEP 6. 実現するために解決すべき問題は？（バックキャスト）
	15:00-17:00	発表・議論
	17:00-17:30	今日の気づき・インサイトの共有
	Next step	ラップアップ

参加者の気づき：

社会の仕組み作りに本気で取り組もうとするメンバーがいた。課題感・論点等を共有できる方々が、様々な会社にいることが分かった。

社会システムの変化は、身近な小単位の変化から始められることが見えてきた。

なにより価値観の変化・適応が最もハードルが高いことに気がついた。

パーソナルデータを活用する「目的」は何か？について深く考えることができた。単なるデータだけではなく、「感情」や「＋αの要素がどれだけ意味のある価値を創り出す可能性があるのかという観点を検討する必要があると感じる。

2025年の未来図（最悪の状況から良い状況を創りだす）を検討することで、制度面や社会面での変化のありたい姿を描けた。その時、全体最適を目標とするより、「この領域のこの人向け」というものを検討する。即ち、「あるケース」で検討してスパイラルアップに、全体へ拡張していくことに気づいた。

以下、チーム活動の様子。

未来創造デザイン WS（A チーム）

未来創造デザイン WS（C チーム）

未来創造デザイン WS（E チーム）

6. 要素技術詳細編

本章では、プライバシーに留意したデータ流通の推進において鍵となるパーソナルデータストア（PDS）に関し、その実現と普及を支える仕組みについて、主に技術視点から検討を行う。

6-1. PDS を支える技術の全体像

パーソナルデータのデータ利活用権は基本的にデータ主体である個人にあるという立場に立てば、パーソナルデータ流通を個人主導で行えるような運用の仕組みである PDS の構築と利用が望まれる。子供や高齢者など IT リテラシーが高くない利用者にも考慮しつつ、個人のプライバシーを保護しながらパーソナルデータを流通させるためには、個人による自己情報コントロール機能を支援（エンパワメント）する各種技術を PDS に総合的に活用することが重要である。

PDS を利用した自己情報コントロールは、下記の二段階により実現される（図 6－1）。

1） データ取引契約交渉

データ主体である個人とパーソナルデータ利活用事業者との間で、本人意思に沿ったデータの取引の実行を担保するために行う契約交渉。個人のパーソナルデータポリシーと、事業者が提示する取引条件（どのパーソナルデータをいつ、どのような形態（原データ、匿名化データ、等）で、何の目的のために開示し、利活用を許可するか、データ利活用による結果報告、報酬等の規定など）とに基づき、両者間の合意を形成する。

2） データ取引実行

データ利活用事業者は、合意した取引条件に基づき、PDS よりパーソナルデータを入手し、データ分析を行う。PDS は、合意した条件に基づきパーソナルデータが利用されるように制御や検査を実行する。また、サービス事業者が提供するサービスを利用した場合の記録（購買データ、ヘルスケアデータ、等）に関し、PDS はデータ自身の提供を受けるか、サービス事業者

側のサービス利用記録を参照できるようにすることで、パーソナルデータを収集、蓄積しておく。

自己情報コントロールを実現するためには、上記の各段階で求められるそれぞれの機能を、確実、かつ効率的に実行する技術が求められる。データ取引契約交渉段階を支える主要技術には、ポリシーや取引条件の構造化表現、取引条件の画一化、合意形成（マッチング）のための合意プロトコルがあり、これらに関しては、6—2 で述べる。データ流通実行段階を支える主要技術には、パーソナルデータ利用の制御・検査を支えるトレーサビリティ（認証、認可、アクセス制御、監査、等）と、パーソナルデータの収集・連携のためのデータ標準化があり、これらについては、6－3 で述べる。

一方、パーソナルデータ流通での自己情報コントロールは、技術による実現が唯一のアプローチというわけではない。システム運用、ルール・義務、監査・認定、教育・啓蒙活動、ホワイト事業者育成へのインセンティブや評価システム、企業の社会的責任（CSR）が技術を補完する可能性があり、PDS 実現にあたっては、システムデザイン、法制度、等を含めた総合的アプローチが求められる。これらについては、6—4 で述べる。

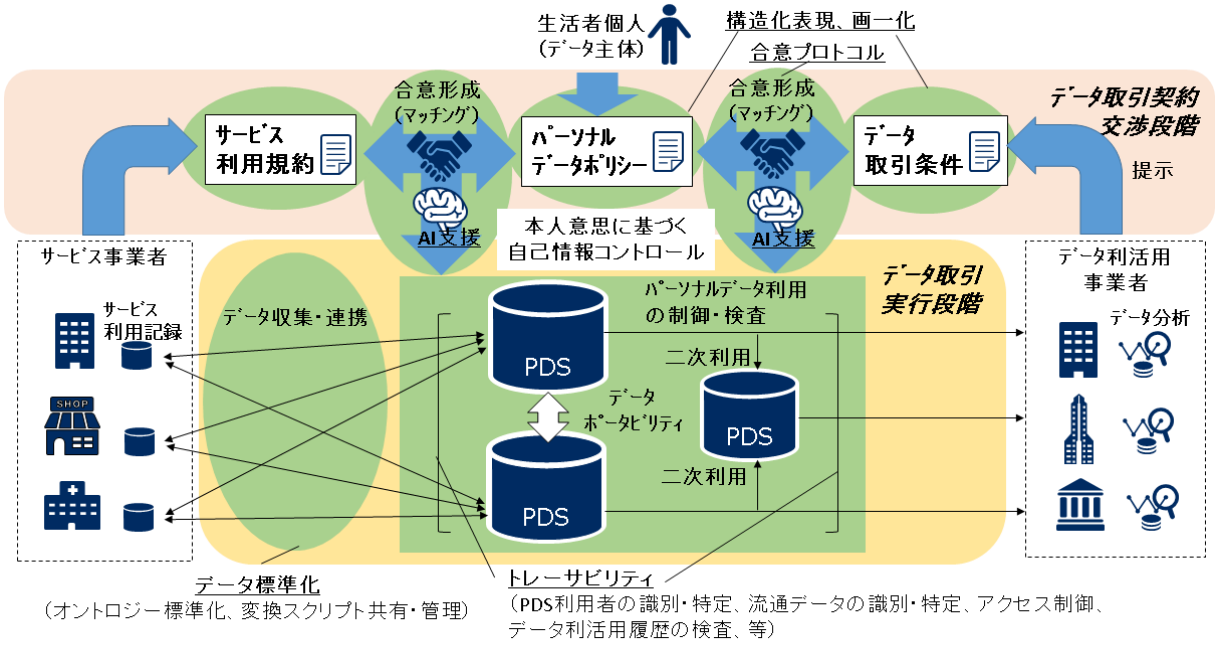


図 6.1　PDS によるパーソナルデータ流通を支える関連技術の全体像

6-2.　パーソナルデータ流通での取引契約交渉（合意形成）段階を支える技術

合意(consensus; consent)はあらゆる取引(社会的相互作用)の前提であり、経営・企画・研究以外の最も重要な問接業務が合意形成(の具現化としての契約)である。合意形成の効率と合意の精度を高めることにより取引のリスクとコストを低減し社会全体の生産性を高めることができる。

個人と事業者の取引においては手間を省くために付合契約(一方の当事者が前以て定めた契約内容に他方の当事者が従うことで成立する契約)が用いられることが多い。しかし、特にパーソナルデータの授受を含む取引の場合、そのデータの扱いに関する実効的な合意がなさ

れないことによりデータの不正使用等のリスクが生ずる。

それを防ぐため、両当事者が各々取引条件を提示してそれらがマッチングする場合に契約を成立させるという方法が考えられる。特に個人と事業者との契約は日常的にきわめて頻繁になされるので、そのためのマッチングを人工知能によって自動化することが望ましい。それには、各主体の取引条件(取引に関与するための条件)を機械に理解可能なデータとして表現し、それらを自動的にマッチングする技術や人間にわかりやすく提示する技術が必要である。これに関する既存の取り組みとして WS-Agreement や TACML がある。

6-2-1. 取引条件での本人意思の表現を支える技術

データ取引契約交渉においては、まず、データ主体の個人が、自らのパーソナルデータの提供に関する本人意思をパーソナルデータポリシーとして、明確に表現することが必要である。また、PDS よりデータ提供を受けたいデータ利活用事業者は、データ取引条件を個人に対してわかりやすく提示する必要がある。ポリシーや取引条件の明確で、わかりやすい提示は、作成・読解のコストを下げるとともに、合意の精度を高める。このためには、文書データの構造化表現(図 6－2)が有効である。また、合意形成と、その後のデータ取引を合意条件に基づいて効率的に実行するためには、AI 活用を念頭に、機械可読な取引条件の表現の利用が望ましい。

さらに、合意形成での確率を高め、効率向上のためには、パーソナルデータに関する取引条件の画一化やベストプラクティスの共有などを通して、パーソナルデータに関する取引において個人が一般的に同意する条件を盛り込んだ標準パターンを用意しておくことも重要である。例えば、「パーソナルデータの取り扱いに関し、元データを人間が見たり、平文でファイルに保存したり、外部に送信したりしない」という条件を取引条件に含めるようにすれば、個人からのパーソナルデータ開示に関する同意取得のハードルは下がり、合意の可能性が高くなる。この条件は、インメモリでのデータ分析・処理アプリケーションの実行と、真正 OS がアプリケーションソフトの署名を検証して不正なアプリを排除する方法を採用すれば、事業者側の利便性を損なわれずに、低コストでの実現が十分に可能と思われる。プライバシー保護に配慮しつつ、個人からの同意取得の確率が高い取引条件の基本として、多くの事業者による採用が望まれる。

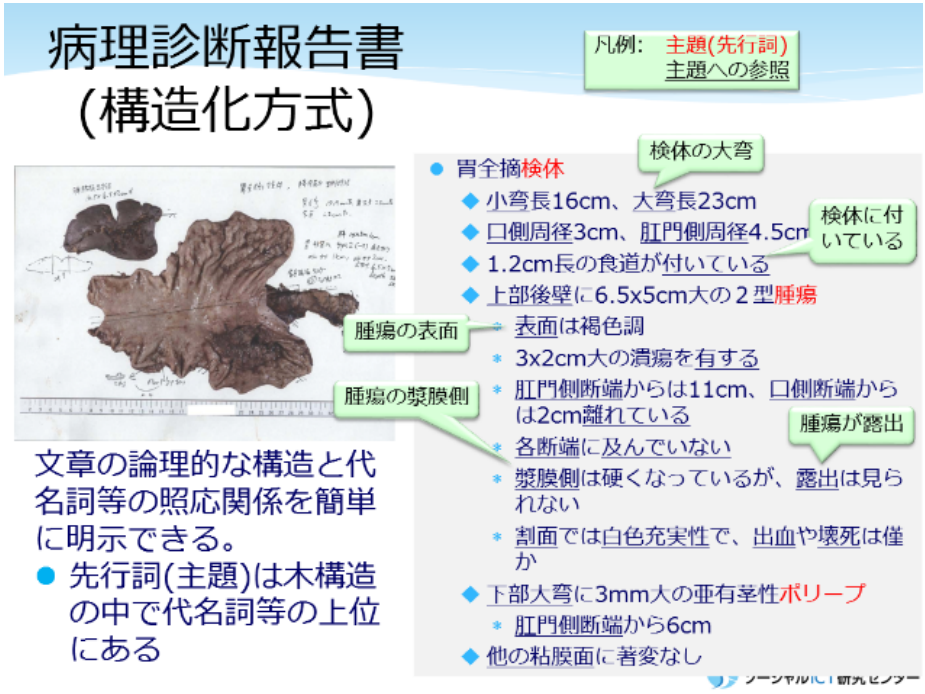


図 6.2　構造化方式による内容の分かりやすい提示（病理診断報告書での事例）

6-2-2.　合意形成（本人意思と取引条件とのマッチング）を支える技術

WS-Agreement [1,2]は、相互の義務を含むような動的な協力関係を設立したい当事者（例えばグリッドやクラウドの環境でのサービス提供者(Service Provider)とサービス消費者(Service Consumer)の間での電子的な合意を得るメカニズムを提供するために OGF（Open Grid Forum）で策定された標準規格である。

WS-Agreement は主に以下の 3 つの要素からなる。

- 合意文書のテンプレート（Agreement Template）と合意文書のフォーマットの記述
- 合意を形成するための基本的なプロトコル
- 実行時に合意事項をモニタするためのインタフェース仕様

合意形成は、合意形成開始者（Agreement Initiator）と合意形成対応者（Agreement Responder）という 2 種の当事者を含む。これらは、サービス消費者およびサービス提供者の概念とは独立している。すなわちサービス消費者もサービス提供者も、合意形成開始者にも合意形成対応者にもなり得る。

合意文書のテンプレートは、合意形成開始者が要請する機能を記入する合意文書のひな形である。WS-Agreement の合意形成プロセスにおける基本的なプロトコルは以下の3ステップからなる。

(1)　合意形成開始者が、合意形成提供者から合意文書のテンプレートを取得し、必要な要求事項（例えば CPU の台数やメモリ容量、通信速度など）を記入した上、合意形成提案（Agreement Offer）として CreateAgreement 操作を用いて、合意形成提供者に合意要求を投げる。

(2) 合意形成対応者は、要求に応じられるか否かを判断し、合意(Accept)か拒否(Reject)を返す。

(3) 合意が帰ってきた場合は、交渉が成立したと見なして、サービスを実行する。このとき、合意された SLA などが遵守されているか否かを合意形成開始者・対応者がモニタすることが可能である。拒否が帰ってきた場合はその時点で交渉を終了する。

図 6.3 に合意形成開始者がサービス消費者である場合のプロトコルの例の流れを示す[2]。なお、基本的な WS-Agreement では、上記のように、要求事項に対応できない場合、交渉は拒否されて終わるが、拡張されたプロトコルである WS-Agreement-Negotiation [3]では再交渉が行われることもある。

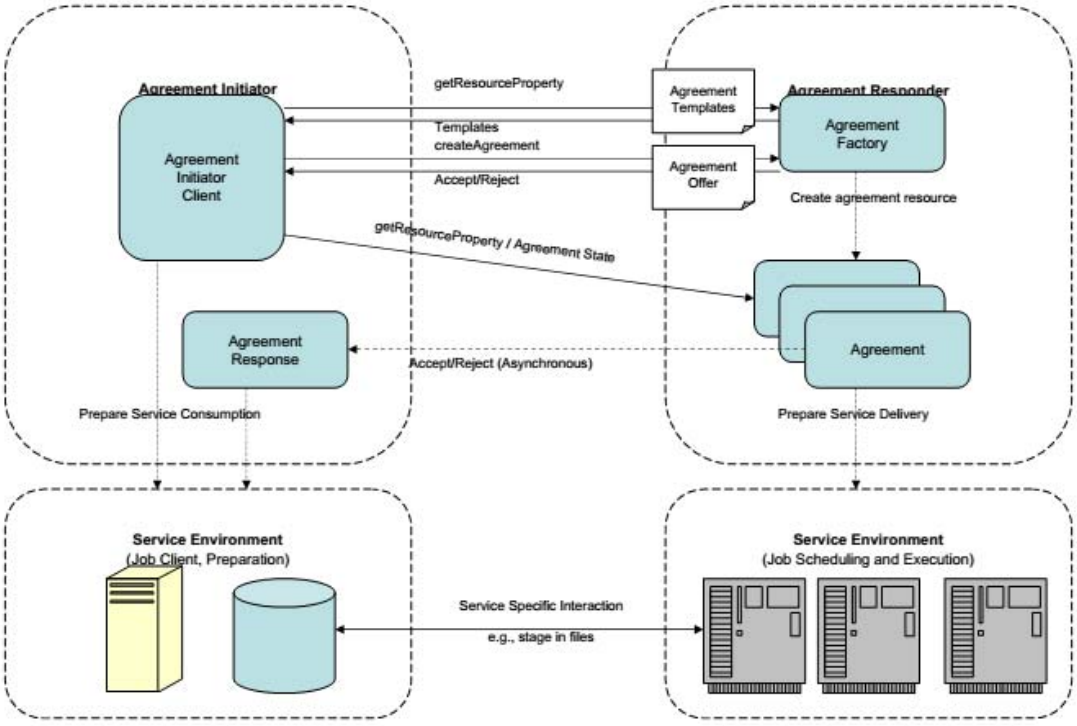


図 6.3 WS-Agreement の概念とインタフェース

WS-Agreement は交渉合意のための一つの標準化されたプロトコルであるが、PDS で本格的に利用するためには、以下の拡張が望ましい。

1. 現時点では実行時状態のモニタリングは、合意形成開始者が合意形成対応者に対して実行できるのみであるが、本来は合意形成対応者が合意形成開始者の状態をモニタリングできることも必要となる。そのためには合意形成開始者の Port Type にもモニタリングインタフェースを追加する必要がある。

2. 現在は Agreement の停止(Termination)は合意形成開始者からしか、依頼できないが、対

称性の観点からは合意形成対応者から Agreement の指示を依頼することも可能にすべきである。

3. そもそも、契約の各当事者が自らの取引条件を確定するには、あり得るすべての取引のメリットやリスクを予め完全に理解しておく必要がある。しかし、それは一般には不可能である。そこで、取引参加者同士がデータを共有し、具体的な状況に応じて同意を部分的に拡張したり取り消したり(動的同意; dynamic consent)できれば、合意形成の効率と同意の精度が大幅に向上し、またそのような動的なプロセスを通じて取引条件の完全性を徐々に高めて行くことができるものと期待される。

6-3. パーソナルデータ流通のデータ取引実行段階を支える技術

6-3-1. パーソナルデータ利用の制御、検査を支える技術（トレーサビリティ）

PDS には、自己情報コントロールのために、どのパーソナルデータを何のために誰と共有しているかを本人が把握し管理するトレーサビリティ機能が必要である。 本節では、トレーサビリティをパーソナルデータの利用を制御・検査できる性質と広く捉え、関連技術と課題を考察する。

パーソナルデータのライフサイクルを考えると、購買行動や医療・ヘルスケアサービス利用によりデータが発生してから当該データが PDS へ保管、連携(紐づけ)されるまでの過程と、PDS 上のデータが検索され、利活用される過程がある(さらに、PDS からデータが消去される過程もあるが、ここでは除く)。前者においては、サービス事業者側でのデータ発生、データ利用、データ移転・連携、本人への通知・開示があるが、サービス利用契約で規定された条件の下で取扱いがなされているかをチェックできるようにするべきであるが、本節でのトレーサビリティの検討は、後者に焦点を絞る。データが PDS で保管されて以降のデータ流通におけるトレーサビリティにも、「データ主体である本人が、何のデータが、いつ、誰に、どのような条件の下で取引され、どのように(利用条件の通りに)使われたかを把握できること」(順方向トレース)と、「PDS を介したデータ提供により、本人が何らかの不利益を被った場合、あるいは不正利用の疑義が生じた場合、どのデータのどのような形での提供により、それが生じたのか把握できること」(逆方向トレース)の2つの側面がある。

トレーサビリティを実現するために、PDS は、一般的な情報セキュリティにおける認証、認可、アクセス制御、監査の機能を持たねばならない。また、自己情報コントロールを実現するために、情報の所有者が自らその保護状態を変更できる任意アクセス制御方式を取る必要がある。従来型のデータベースシステムやファイルシステムでは、利用者の認証やアクセス権限の設定と制御はそのシステムに閉じている。一方、Web サービスでは、自律分散型のインターネット上で認証、認可、アクセス制御を実現するための標準プロトコルとして OpenID Connect、OAuth、UMA などが利用されている。PDS も自律分散型の運用をしつつ、PDS 相互または各種アプリケーションとの連携のために、これら Web サービスの標準技術を利用することが適切と考える。

必須の機能要件

PDS のトレーサビリティを実現するにあたり、必要な機能と利用可能な既存技術・仕組みを下表に整理する。

機能要件（必須）	既存技術・仕組み
PDS 利用者を識別・特定できる	認証（OpenID Connect）、ID 連携トラストフレームワーク
データを識別・特定できる	デジタルオブジェクト識別子
どのデータに、誰が、どうアクセスできるかを決めて、これを守らせる	アクセス制御（OAuth、UMA）、デジタル著作権管理（DRM）
データの利用履歴を検査できる	ログ/監査証跡（ブロックチェーン）、否認防止（タイムスタンプ、デジタル署名、ブロックチェーン）、監査基準

DRM のように、データ自体の暗号化とデータ処理を行う機器・アプリの制限との組合せは、PDS において合意した取引条件の実施を強制・保証する技術として有効であると考える。DRM によるパーソナルデータ管理を個人単位へ適用することは、多様な機器・アプリの利用や管理対象の数を考えると現実的に難しいが、事業者単位への DRM 適用は有効に機能する可能性がある。データ利活用事業者がデータを統計分析する場合、暗号化されたパーソナルデータの提供を受け、復号化したデータはインメモリ内のみで処理して、平文では外に出さないようにする。利用アプリが適切なデータ処理ツールであるかどうかは、OS がアプリの正当性をその署名で検証すればよい。事業者が利用するパーソナルデータ処理のツール群（SW パッケージ）を動作保証されたツール群に制限したり、オープンソフト化によりソフトの中身（データの取り扱い方法）を誰もがチェックできるようになれば、事業者でのパーソナルデータの適切な利用を低コストで実現できる可能性がある。

ブロックチェーンのように一旦記録した内容を改変できない仕組みは、利用者と事業者との取引条件の合意（コンセントレシート）の管理には有効である。パーソナルデータ自体のトレースを考えると、データ処理がブロックチェーンの中に閉じて完結している必要がある。トレーサビリティへのブロックチェーン適用に関しては、今後の検討課題である。

利便性向上のための機能要件

PDS に必須とまでは言えないが、利用者の利便性を高める主な機能を下表に示す。

機能要件	既存技術・仕組み
データのアクセス権限付与（他者との共有）を容易に設定できる	マッチング、テンプレート（PPM[4]など）
データ共有の状況を容易に把握できる	可視化（PPM など）

PDS にどのようなデータが存在するかを、すべてのデータにアクセスせずに知ることができる	メタデータ、秘匿検索

上記の機能要件を踏まえたPDSのアーキテクチャの具体例に関しては、文献[5](p.28の図4－1)を参照されたい。

パーソナルデータのトレーサビリティ実現のためには、さらに以下を検討する必要がある。

- トレーサビリティをどの程度のデータ粒度で制御するか

（データの識別単位、データ検索のための識別子付与、識別子からデータの探索方法）

識別子に関してはデジタルオブジェクト識別子（DOI）の仕組みが参考になると思われる。また、PDSデータの多様性（例えば、画像には複数のデータが混在）や時系列視点などを考慮すると、データの識別子には階層性を持たせる必要がある。データ検索に関しては、オープンデータのコミュニティではOpen Knowledge FoundationによるCKANが広く用いられているが、PDSでもパーソナルデータの検索性を高める何らかのデファクト標準が必要となるであろう。

- 利用者数とデータの量・種類数が大きいとき、トレーサビリティを十分に達成できるか

秘匿検索技術は、セキュリティを担保しながら検索を可能とするため、パーソナルデータ処理での有力な技術手段であるが、データ量が膨大な場合、その処理速度が課題となる。暗号化されたデータベースの必要な部分とQueryを復号化し、平文での高速処理を事業者にも見せずに実行する仕組みが必要となろう。

また、パーソナルデータを提供する個人の許可を取った上で、PDSにおいて匿名データとして検索し、答えを返すサービスを用意すれば、データ自体の暗号化が不要となり、高速処理実現が可能となる。誰がPDS事業者に検索を依頼したか自体も匿名化し、検索依頼者と検索対象者との間で情報交換しないProxy対Proxyの構図とする。　PIR（Private Information Retrieval)の仕組みの活用も選択肢となり得る。

- 利用者の身元確認をどのように行うか

公的個人認証サービスにより、実在性を認証することが必要となろう。

- PDS事業者がトレーサビリティ機能を正しく実現・実施していることをどのように担保するか

PDS事業者へのDRM適用が有効ではないか。また、併せてPDS事業者の監査・認定も必要となるであろう

- 利用者（データ利活用事業者）側での適切なデータ利活用をどのように担保するか

利用者へのDRMを適用するアプローチ、PDS事業者、あるいはメディエータ自身が利用者に対しては、データ提供ではなく、自らの（安全な）検索ツールの利用のみをサービス提供するアプローチ、利用者側にデータ入手経路の立証義務を負わせて不正利用を抑止するアプローチ（6-4参照）などが考えられる。

● 利用履歴（ログ）もパーソナルデータと見做せるが、これをどのように扱うか
PDS を利用するデータ利活用事業者側の権利に管理しては、今後の検討課題である。

6-3-2. データの標準化

多種のセンサーやサービスの出力データを他のサービスに入力したりビッグデータとして集約して分析したりするには、データの仕様の標準化が必要である。しかし、新たなセンサーやサービスは次々に出現し、それらの標準化を従来のデジュール標準化のプロセスで扱うのは不可能である。そこで、データの標準化に当っては、パーソナルデータに限らず、データ流通に共通する課題であるが、

● 標準的なデータ仕様を規定するオントロジー
● この標準オントロジーと個別データ仕様との間でのデータ変換を行なうスクリプト

を集めたリポジトリを構築・運用し、多数の参加者がこのオントロジーとスクリプトを共同で増補・更新し続ける必要がある。これは、集合知（クラウドソーシング）を活用したデータ標準化の現実解であり、ここでは“集合的標準化”と呼ぶことにする（図6－4）。集合的標準化には多数の協力者が必要であり、効率的に推進するためには、変換スクリプトの作成を支援するユーザインタフェース、ツールの用意が必要である。

集合的標準化には、Wedata.net のようにオープンな機関の取り組みばかりではなく、トリップアドバイザやマネーフォワードなど、個々の民間企業が自らの企業活動の中で推進、運用しているものもある。これらを含め、民間のサービス事業者が収集するパーソナルデータを PDS でのデータ獲得に利用することは効率的である。サービス事業者が集めたパーソナルデータをデータ主体である本人自身が利活用する場合は、サービス事業者との契約範囲の中で許される可能性が高いであろう。しかし、本人が、その収集データを PDS で管理し、さらに別の事業者（第三者）に提供して二次的な利活用に及ぶ場合は、データを収集した民間事業者との間での利益分配など、データ収集コスト負担に配慮しつつ、データ流通を促進する仕掛けの検討が必要となろう。

データ共有、連携は、個人、社会にとって大きな利便性があるという観点からは、データ標準化は積極的に進めるべきであり、そのためには、データ収集事業者側でのデータ仕様の積極的開示、データ標準化推進への政策的誘導も必要である。集合的標準化の普及には、標準化貢献者に対してインセンティブが賦与されることで多くの貢献者が集い、標準化の利便性が高まり、持続的に発展していくようなシステムの設計と運用が不可欠である。

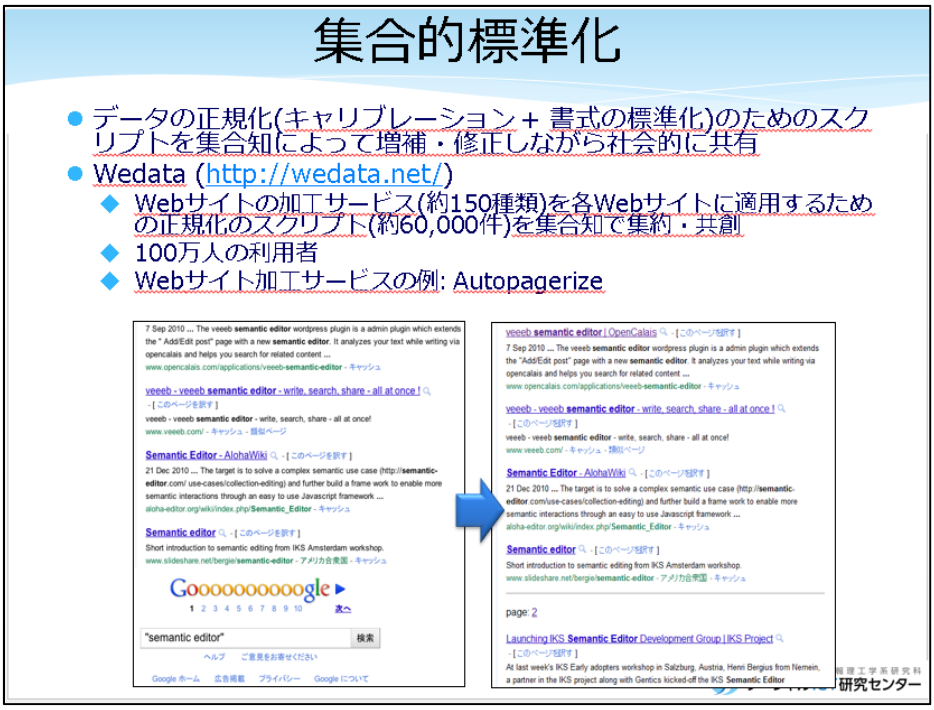


図 6.4　集合的標準化

6-4.　システムデザイン、法制度、等を含めた総合的アプローチ

PDS に基づくパーソナルデータ利活用の実現上の課題を解決する手段には技術的手段以外にも、運用、ルール・義務、監査・認定、教育・啓蒙、評価、インセンティブなど、様々な手段があり（図 6.5）、これらの総合的な組み合わせが課題解決での現実解となる。以下では、パーソナルデータ利活用の課題解決における非技術手段に関し、そのいくつかを具体的に例示する。

データ取引条件と合意形成（マッチング）に関して言えば、パーソナルデータ流通に伴うメリットとデメリット、サービス利用に伴うリスク、個人と事業者との責任分解、等に関する正しい理解が前提となっており、プライバシー保護とパーソナルデータの利活用に関する教育・啓蒙を通してのデータ主体である個人の自己情報コントロールに関するリテラシー向上と自覚が不可欠である。AI 進化に伴う PDS の技術的手段の向上は、パーソナルデータ流通のリスクとコストの低減、個人の物理的、精神的負担の軽減に大きく貢献するようになることが期待される。また、個人主導の自己情報コントロールに関する法制度の整備、ベストプラクティスの共有、等による適切な運用の確保、支援も必要である。

トレーサビリティに関しては、6－3－1 で述べた技術的実現だけでなく、ルール・義務による（補完的）解決が考えられる。例えば、データ利活用事業者に、「PDS より入手したデータの移転履歴に関して、本人（データ主体）への開示手段を保有していること」、「データ主体からの求めがあった場合、データ入手経路の正当性を証明できること」の2つを義務付けることができれば、正しいデータ流通の促進と不正なデータ入手・利用への抑止につながるであろう。さらに、個人による自己情報コントロールの実現のために積極的な情報開示手段を備え、社会的責任

を果たそうとする優良企業を積極的に評価し、それらを分かりやすく表示する仕組みができれば、プライバシー保護に配慮したパーソナルデータ利活用推進の後押しとなる。企業にとっても、正当な入手経路による取得データの利活用の方が安全であり、技術的にも簡単で使いやすい仕組みが実現できれば、プライバシーとイノベーション両立の好循環社会が実現するであろう。社会全体での Trust の総合的な仕組み作りが必要である。

データの標準化に関しては、オントロジーを整備し、集合的標準化を進める業界に対する制度的支援や推進施策の展開、企業努力で集合的標準化を進めるサービス事業者への利益分配（事業者が収集したパーソナルデータを個人が第三者へ提供して二次利用する場合）の仕組みの構築は、パーソナルデータ利活用推進に効果的である。

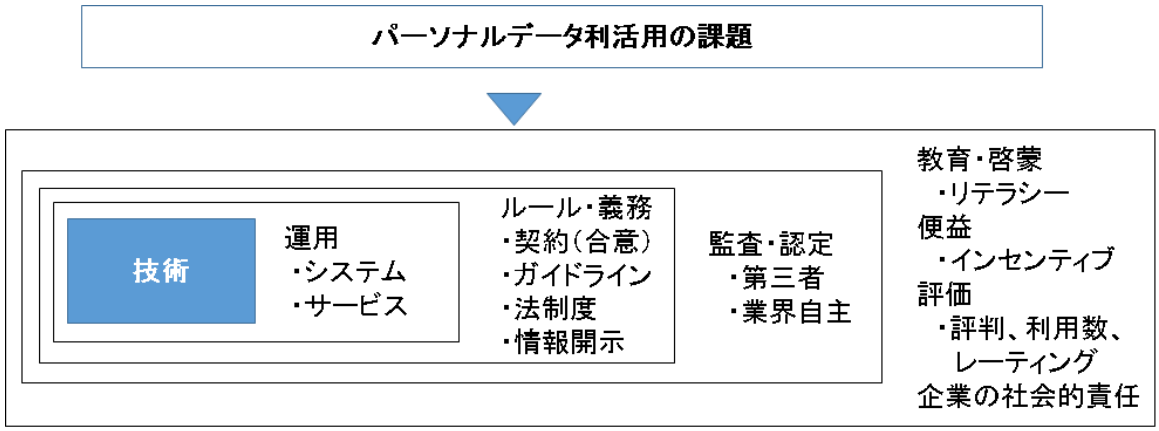


図 6.5　パーソナルデータ利活用の課題解決の総合的枠組み

参考文献

[1] A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, and M. Xu “Web Services Agreement Specification (WS-Agreement)”, Open Grid Forum, GFD-107, 2007/05.

[2] H. Ludwig, T. Nakata, O. Waldrich, P. Wieder, and W. Ziegler “Reliable Orchestration of Resources Using WS-Agreement”, Int. Conf. on High Performance Computing & Communications (HPCC), pp.753-762, 2006/09

[3] O. Waeldrich, D. Battré, F. Brazier, K. Clark, M. Oey, A. Papaspyrou, P. Wieder, and W. Ziegler: “WS-Agreement Negotiation Version 1.0”, Open Grid Forum, 2011/01

[4] 奥井 宣広 “プライバシー保護、PPM を用いたプライバシー保護アーキテクチャ”, ARIB・TTC 共催セミナー「IoT 標準化最新動向 ～oneM2M 技術仕様リリース 2 の全貌～」, 2016 年 9 月 9 日

[5] 集めないビッグデータコンソーシアム（東京大学）“パーソナルデータ・エコシステムの実現(平成 27 年度成果報告書)”. 2015 年 10 月 5 日.
http://www.ducr.u-tokyo.ac.jp/jp/materials/pdf/research/dbd-conso_seika.pdf

7. 社会実装タスクフォース

社会実装タスクフォースでは、個人主導のデータ流通を実現する仕組み（PDS）を社会実装するための様々な課題を、具体的なフィールドとユースケースに基づいて議論、検討することを目的に活動を実施した。

具体的なフィールドとして、東京都下 A 市で検討中の地域・健康系のユースケース（サステナブルヘルス PJ）を想定した。サステナブルヘルスは A 市の地方創成加速化交付金 PJ などで具体化を検討中のプロジェクトで、

① 健康寿命の延伸のための健康無関心層の行動変容の実現、と

② 獲得されたデータに基づく（生活課題解決）産業創生

を目的としたものである。

本タスクフォースでは、技術、経済、社会面で想定される課題を整理し、検討をおこなった。（図 7.1）

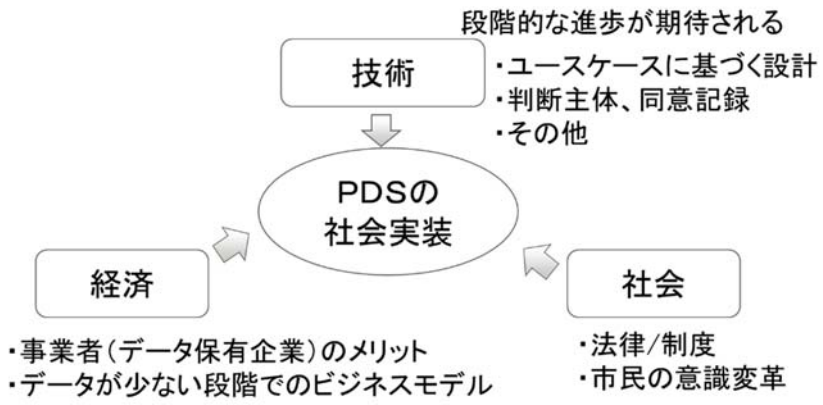


図 7.1. 検討の全体像

7.1. 想定したユースケース

A市のサステナブルヘルス PJ で具体的にどのような活動を実施するかは本タスクフォースのテーマではないので、ここでは仮のユースケースとして下記の二つの健康サービスを地域 PDS によって結びつけるものを想定した。（図 7.2）

① スマートフォンによる栄養指導システム（食事写真と管理栄養士の指導実績を記録）

② ウェアラブルデバイスによるバイタルデータ収集

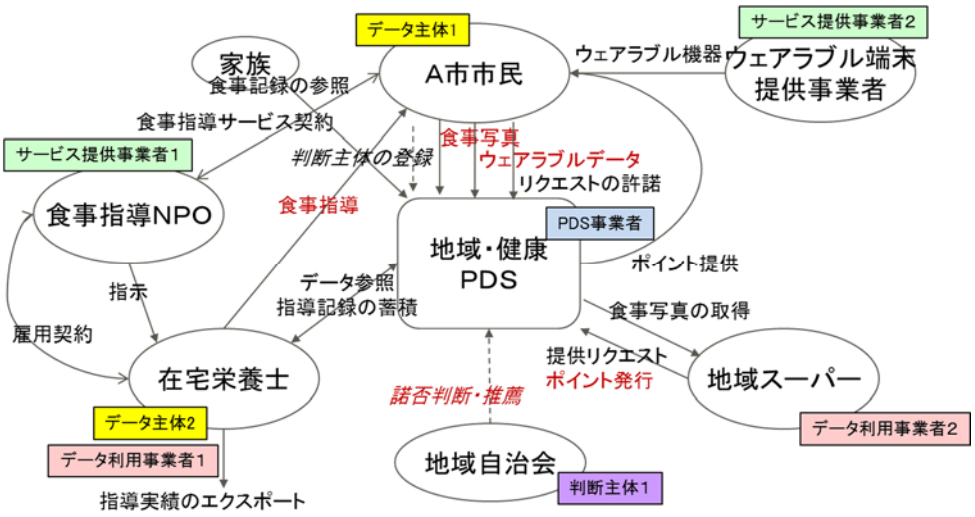


図 7.2 想定したユースケース

この二つのサービスを地域 PDS で結びつけることで、下記のような価値が実現できるのではないかと考える。

A) 二つのサービスを結び付けることで、ここのサービスの価値が向上

B) 蓄積された食事写真データの地域事業者（スーパー）へ提供によるマネタイズ

C) 在宅で働く管理栄養士の指導実績を PDS に蓄積・証明することで、栄養士が新しい仕事を獲得したり、自身のキャリアアップを図る

7.2. 技術面の検討

本社会実装タスクフォースでは、上記ユースケースを設定し、以下のような検討を行った。

① （本ユースケースを実現に必要な）PDS が実現すべき要件の明確化

② PDS 利用者のユーザ体験(UX)とスマートフォンの UI 画面のデザイン

③ 上記ユーザ体験を実現するための、PDS の上位 API 仕様の検討（途中）

なお、本検討では、既存のパーソナルデータ管理機構に自己情報コントロール機能と第三者アクセス制御機能を加えた図 7.3 のようなアーキを想定した。

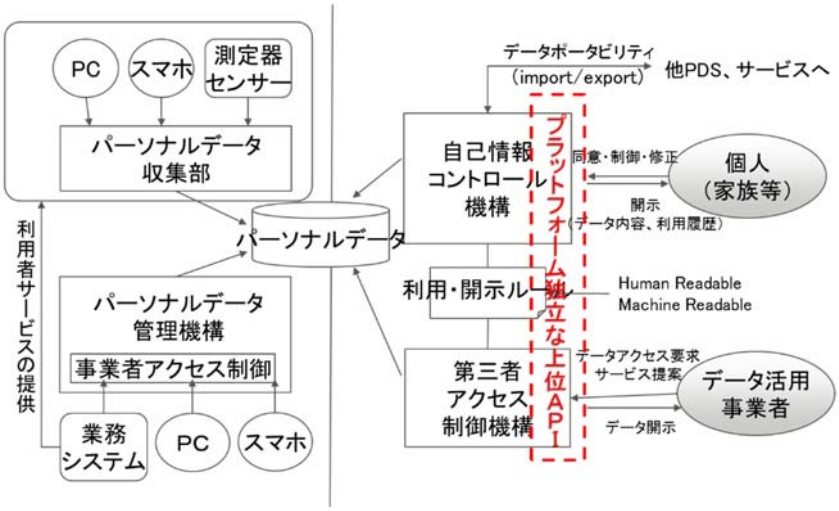


図 7.3. 当初設定した概要アーキ

・ 実現すべき要件

本タスクフォースでは、具体的なユースケースやユーザ体験を議論するなかで、通常の PDS の実現価値に加え、下記のような機能も重要ではないかとの議論になった。

① 栄養士、ヘルパーなど、専門資格をもった市民の PDS への実績蓄積、証明機構

② 同意記録証明による、ホワイトな事業者を支援（証明）する機能の実装

③ 個人メリットだけでなく、地域や社会へメリットを還元する仕組み

④ 信頼する個人や団体などの許諾判断を流用する「判断主体」の概念の導入

図 7.4 は、上記に基づいて、本ユースケースを実現するために整理した要件(案)である。

1. 安心・安全な管理
   - セキュリティリスクに対応し、安全にデータを保管する
   - 変更や誤りのあるデータに対する本人による更新・修正（＋事業者への通知）
2. 見える化・証明機能
   - どのようなデータがあるか（人間に分かり易い＆機械可読）
   - どのように利用されているか（利用履歴、提供履歴、同意記録）
   - 蓄積データや実績の証明（活動履歴など）
3. 本人同意に基づくパーソナルデータの活用（プラットフォーム機能）
   - 事業者の許諾リクエストに対する同意制御（判断主体などの支援機構）
   - 事業者からの問い合わせ・紹介機能（匿名性を保証）
   - ワンストップ更新・通知機能
   - 利用実績の証明とデータ取得事業者への対価の還元
   - 同意記録証明など、提供先における適切な利用を保証するための仕組み
4. 外部とのデータ連携
   - 外部からのパーソナルデータのインポート（ID連携、スクレイピングなど）
   - 外部へのエクスポート（データポータビリティ機能の提供）
5. その他（古いデータの圧縮・廃棄、事業者付加情報の管理など）

図 7.4. 実現すべき要件

・ 実現すべきユーザ体験（UI画面）

本タスクフォースでは、上記シナリオと要件をベースに、利用者にとって望ましいユーザ体験を検討し、スマートフォンの UI 画面（イメージ）を策定した。（図 5）（本検討の結果は、2016/10/14 に開催された「データ流通環境整備検討会：AI,IoT 時代におけるデータ活用ワーキンググループ（第二回）」の配布資料1（事例紹介）のなかで、アプリケーション、サービス概要のイメージ図 P4-P15 として紹介されている）

図 7.5. 検討した UI 画面の例

・ 必要とされるAPI構成

本タスクフォースでは、上記要件やユーザ体験をベースに、PDS として必要な API をプラットフォーム独立な形で策定することを目標とした。現在、まだ途中であるが、今後、継続して検討を行う予定である。

図 7.6 は、本検討で仮に策定した API 構成案（詳細は今後）である。本検討は、他の PDS の実装や API を規定するものではないが、オープンソース PDS：Personium に実装予定であり、これをオープンソースで公開することを計画している。データストアとしての狭義の PDS に加え、データ流通機構（メディエータ、情報銀行など）的な機能も含めた広義の PDS で、一つの参考実装になればと考えている。

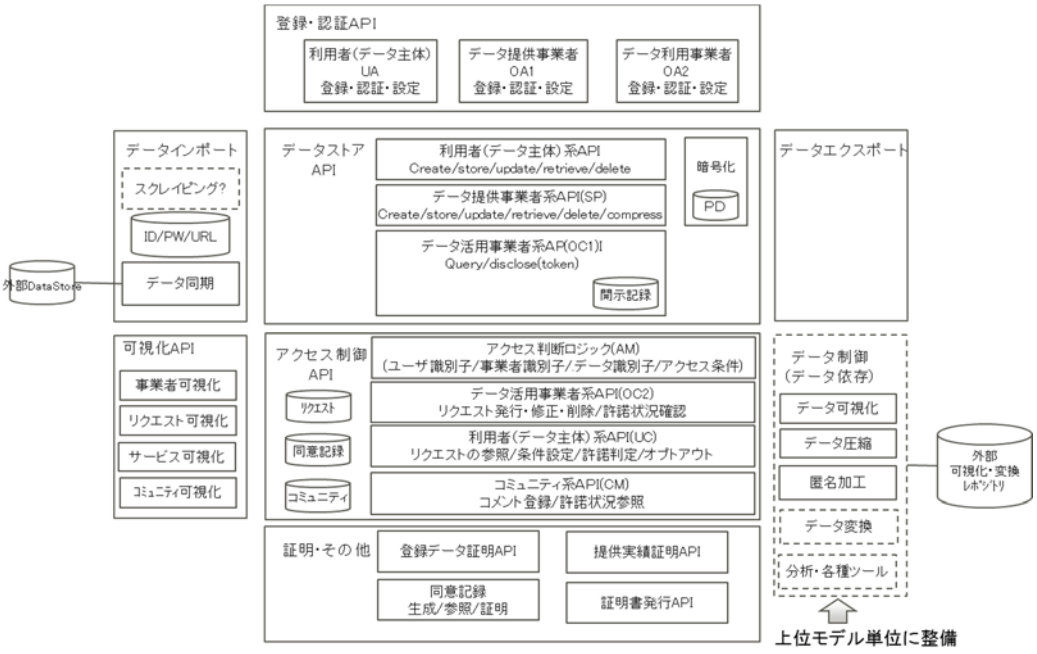


図 7.6. 検討中の API 構成

7.3. 経済面の検討

PDS の社会実装には、技術面に加え、経済面（事業性、ビジネスモデル）での検討が必須という認識から、下記の二点に対する検討を実施した。

① データ蓄積が少ない段階での PDS 事業者のビジネスモデル

② すでにデータ保有する事業者がデータを PDS に預ける経済的メリット

・ PDS 事業者のビジネスデモル

PDS の形態には、個人が事業主体となる形と、サービス提供事業者が事業主体となる形、独立した事業者が事業主体になる形があるが、地域系PDSであれば、サービス提供事業者とは独立した（ある程度公共性をもった）事業者が事業主体となることが想定される。

このような場合、PDS 事業を地域行政の負担に頼ることは想定しづらく、自立運営できる収益モデルが必要である。しかしながら、通常想定される蓄積されたデータの流通手数料（銀行での融資に相当）はデータ規模が小さい間はあまり期待できない。また、利用者からの利用課

金も PDS の立ち上げ段階では困難で、基本は無料としないと参加者を集めることは困難であろう（サービスが拡大時のフリーミアム課金はあり得るが）。

このため、本タスクフォースでは、一つの可能性として、地域 PDS を運営する事業者（母体）として、企業と市民、行政が共同で新しいサービスや商品の企画・設計・検証を行う「リビングラボ」を検討した。（図 7.7）

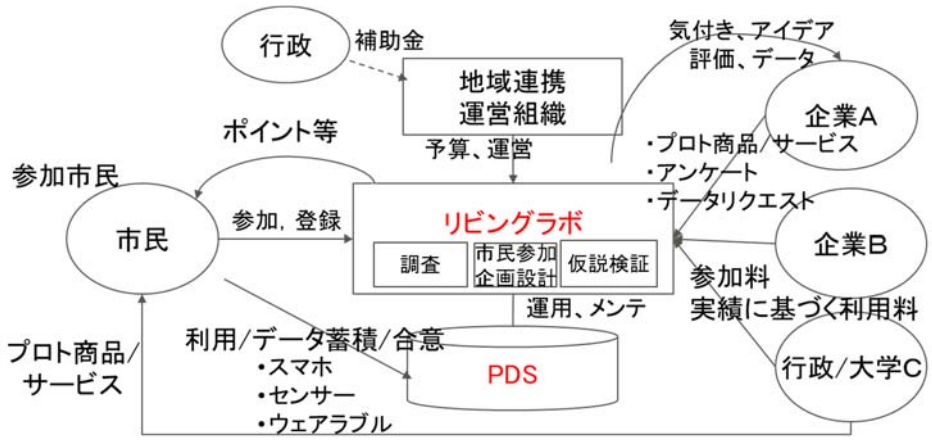


図 7.7. リビングラボ

リビングラボは、欧州などで展開している企業と市民による参加型商品/サービス企画・設計、検証の場であり、企業からの依頼（有償）を受けて、市民が商品開発の各工程（調査、企画、設計、検証など）に参加する活動である。国内では、松本市の松本ヘルス・ラボなどが知られており、地域におけるヘルスケアビジネスの創出に向けて、次世代ヘルスケア産業協議会のアクションプラン 2015 などでその整備が期待されている。

本タスクフォースでは、通常のリビングラボの機能に、PDS の機能を加え、仮説検証工程で利用者の生活環境での定量的な検証が可能になる。

本仮説での PDS 事業者の収益は

① リビングラボ（PDS）の利用に対する企業の参加料、実績に基づく利用料

② PDS により実現された有償サービスの実施に対する実績型手数料

③ アンケート機能など、各種リビングボ（PDS）のサービスに対する利用料

などを想定した。

この他、本モデルによらず、PDS 事業者が期待できる収益としては

④ パーソナルデータ委託管理料

⑤ 各種サービスに対する利用料（実績証明、ワンストップ情報更新など）

⑥ 使用者へのターゲット型広告収入（許諾を受けた範囲での）

⑦ データの匿名化による販売収入

⑧ フリーミアム型の利用者のプレミアムサービス利用料

などが考えられる。

なお、本モデルでは、活動の公益性を根拠に、立ち上げ段階での行政からの補助金も想定

している。データが蓄積されてくれば収益規模が拡大し、徐々に補助金を削減することが可能とも思われ、自立運営も可能になるかもしれない。

・　データ保有事業者の参加メリット

本ユースケースの実現には、多様なデータ保有事業者の参加が必要である。PDS に参加するためには既存のデータ管理に加えた追加投資が必要であり、法令等で強制されない限り、経済的な側面からもメリットを明確にする必要がある。

データ保有事業者の参加メリットは、既に大規模なパーソナルデータ管理機構を保持・運営している大規模事業者と、十分な管理機構や体制を持たない（負担になっている）中小規模事業者により異なるが

① 他社サービス（データ）との連携による自社サービスのユーザ体験レベルでの価値向上
② PDS にデータを預けることでの事業者の信頼の強化（任意時点でのオプトアウトなど自己情報コントロールや、同意記録証明など）
③ ワンストップ更新機能による、利用者情報のタイムリーな更新
④ 自社提供データに基づく他社の有料サービス実施時のデータ利用料の還元（要実績証明）
⑤ 自社グループ単独では得られない、多様な事業者の参加による自社取得データを中心としたエコシステムの実現

などがメリットとして考えられ、実証実験等でこうしたメリットを具体的に立証することが重要と思われる。

さらに、中小規模の事業者であれば、

⑥ 現在や将来のセキュリティ・プライバシー規制強化への対応を軽減する委託管理

なども大きなメリットと考えられる。

図 7.4 に整理した PDS として実現すべき要件は、こうした経済的な側面を検討した結果も反映させたものである。

7.4. 社会面の検討

PDS の社会実装には、制度検討 SWG にて検討されている法律や制度（データポータビリティ、推進組織）の整備に加え、データのオーナーである「市民の意識変革」が重要な課題である。

日立と博報堂が 2016 年 9 月に実施した第三回プライバシー意識調査によればパーソナルデータに活用について「活用への期待がリスクに対する不安より大きい/やや大きい」と答えた市民は二割弱にとどまり、「不安が期待より大きい/やや大きい」と答えた市民が約半数であった。このように、一般市民は「パーソナルデータは事業者の責任で守るべきリスク」という考えが主流であり、「パーソナルデータを自らの資産（アセット）として、（一定のリスクを理解したうえで）活用できるもの」という考えをもっている人は多くない。

PDS の社会実装には、このような市民の意識変革を図る必要があり、本タスクフォースではこのような意識変革にむけて、下記のような段階的アプローチを検討した。

① PDS という仕組みや手段を知ってもらう
② データ利活用で自分（や家族、社会）にとってメリットがあると知ってもらう
③ 自分にも使いこなせるという意識をもってもらう（自己効力感の獲得）
④ 不安なく使える、という意識をもってもらう
⑤ PDS という新しい仕組みに積極的にチャレンジし回りの市民に影響を与える「ロールモデル」を育成する

今回の社会実装タスクフォースでは、このような市民サイドでのアプローチを整理する段階にとどまり、残念ながら実際の市民への具体的働きかけ方法の検討や、実施に基づく見直し、改善する段階には至っていない。市民意識の変革には、長い時間が必要であり、国として継続的に取り組むべき課題であろう。なお、本検討の一環で、PDS の概念を理解してもらうための下記のような「ビデオ」を作製した。

YouTube の URL：https://www.youtube.com/watch?v=FKCV8XuXsmg

7.5. 今後の予定

社会実装タスクフォースの COCN としての活動は、今年度の最終報告書（本稿）をもって一段落するが、社会実装に向けたまだまだ初めの段階であり、今後、産官学が共同でさらなる検討と実証を継続していくべきと考えている。その一部として、（COCN の枠を離れても）参加メンバーの有志により検討や実践を継続したいと考えている。

技術面では、これまで策定した要件に基づく API の上位仕様（現在途中）を明確にし、これをオープンソース PDS である「Personium」に実装し、オープンソースで公開したいと考えている。また、上記ユースケースを実現するプロトタイプも作成予定である。

経済面、社会面に関しては、具体的なプロジェクトの立ち上げを目指し、国プロ等で予算が獲得できれば、実践ベースで検討、検証、改良していきたいと考えている。

PDS の社会実装は、実践によって利用者意識と事業者意識の変革を図ることが第一ステップであり、十分な社会的合意ができた段階で法制・制度の充実を図り、本格的な社会実装につなげる必要がある。PDS はデジタル革新時代の日本の競争力獲得や超少子高齢化での持続可能な社会(Society 5.0)の実現のために必ず実現すべきものであり、継続して、産官学民の共同、オープンイノベーションのアプローチで推進していくことが望まれる。

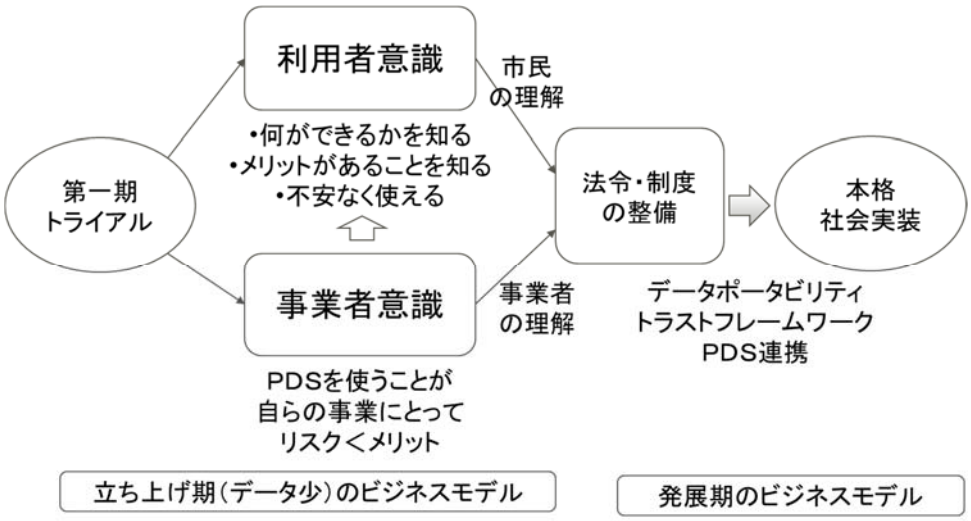


図 8. 社会実装に向けたステップ

8. COCN カメラ画像利活用ルール

カメラで取得された人物関連データの商用目的における利用ルール（WG2 検討案）

COCN「IoT 時代におけるプライバシーとイノベーションの両立」WG2

本文書は、個人情報保護法のマルチステークホルダー・プロセスに乗っ取り、将来的に事業者・消費者・行政等の関与により制定される「自主規制ルール」の現案となることを念頭に、事業者サイドの有志の集まりとしての COCN プロジェクト参画メンバーおよび大学・研究機関等の有識者との議論により作成されたものである。

本文書は、今後より参加者を拡大された意見交換の開始点となることを想定しており、現時点で直ちに事業者サイドとして、施設の利用者等に対して特定のルールを適用することを意図したものではない。

前文

０．１　背景

商業目的では情報化以前より、店頭の来訪者の年齢層や（見た目の）性別等の属性を店員などの人が集計し、客層分析やサービスの改善などに用いることは広く行われてきていた。こういった場面では、施設の利用者側にとっても、およそどのような情報が取得可能であるか、またどれくらいの精度の情報として後から利用されるかは、「同じくらいの能力の一人の人から見える範囲」として想像ができることから、少なくとも日本社会においては、さほどの嫌悪感は無く受け入れられてきていると考えられる。

一方で、近年の画像認識技術や情報処理技術の進展により、カメラなどによって取得された画像データから、人物に紐付く様々な属性データを推測し大規模に集計することや、さらに人物の詳細な画像データなどを元に、長期間にわたって特定の顧客を追跡することが技術的に可能になってきた。また、ビッグデータ処理の隆興により、極めて多数の画像情報や、カメラ以外の様々な Web 空間の情報との突き合わせにより、人間が行っていた情報収集とは次元の違う、極めて精度の高く機微な情報を推測することも可能になってきつつある。

このような状況の元では、商業施設等の利用者にとっては、カメラで画像を取得されたことの影響として、どのような目的で、どのような範囲で追跡され、また情報漏洩などにより自らにどれだけの被害リスクが想定されるのかが全く想像できない。また、多かれ少なかれ「気配」を感じることができる、嫌であれば避けることができると（少なくとも感情的には）受け入れられる人による情報収集と異なり、四方八方に張り巡らされたカメラ群から、気づきようも避けようもないうちに大量に情報を取得されることも、これまでの人間主体の集計などとは全く異なる不安感や不信感を生む源泉となっている。

利用者サイドの立場から見たときの問題は様々な角度から議論されているが、整理すると、

・　自分がどれだけのカメラから情報取得されているのかが想像・把握できないこと。

・　一旦画像データを取得されてしまうと、その情報がどれだけ情報社会で流通するか、全く想像が付かないこと。

・　どのような属性情報や画像情報を取得しているカメラであっても、見た目には同じにしか見えないこと。

・　機械処理により、取得された自分に関するデータからどれだけの情報が推測・導出されるのかが想像できないこと。

・　さらに、情報が流通した結果、自ら予想もしない不当な不利益を受けた際に、自らの権利とプライバシーをどのように回復できるかが明らかでないこと。

・　自らの権利保護のために何が主張でき、何を主張すべきなのか、どこまでは社会コンセンサスとして受容すべきなのかの指針が全くないこと。

の 6 点に集約できると考えられる。特に、機械化された個人情報取得では、利用者本人の、周囲の人間も認識できるであろう「現在の行動」が単体で取得されることそのものよりも、その取得データが本人のコントロールの及ばないところで保存され、複数回・複数箇所で取得されたデータが本人の意図に反して結びつけられ一体と流通することにより、過去に買った商品や訪問の頻度、時刻など、自らもコントロールしきれない本人の「過去の行動」が、それらを通常知り得ない店員や周囲の人に暴露されることが、個人のプライバシーに対する大きな脅威になると考えられる。

実際には、現在の日本において上市されている技術には利用者のプライバシー保護に関心を持って設計されているものも多くあるが、一方では個人情報保護法やその源泉となる個人のプライバシー権に対する配慮の甘い製品や、一方的に取得者側のメリットのみを追求した製品があるのも事実であり、そういった一部の製品の存在がまた、利用者の不安や不信を増大する状況になっている。

また、事業者サイドから見た場合には、このような不安に誠実に答えるベスト・プラクティスが確立されていないことにより、どのような対策を取れば利用者のプライバシーに配慮したことになるのか、どのようにその配慮を利用者に伝えたら良いのかがわからないことが、事業者がカメラデータの商用利用そのものを躊躇する萎縮要因となっている。特に、消費者保護をきちんと考えている事業者であればあるほど、技術の導入を躊躇しがちになるこの状況は、消費者保護をきちんと考えたより良い製品が市場を獲得し、社会全体で普及していくというあるべき姿に対して、明らかに負の要因となっている。

こういった状況に対し本ルールは、事業者にとって守るべき施設利用者のプライバシー保護のベスト・プラクティスを整理し、取得する情報の範囲とそれに応じた個人情報保護やプライバシー権の保護に対する方策を明らかにすることと、さらにそれを類型化し利用者にわかりやすく提示することにより、カメラ画像認識技術の商業利用が不用意に利用者のプライバシーを侵害しないことと、さらに消費者のプライバシーより商業価値を優先した不誠実なシステムに対して、きちんと権利保護を考慮した誠実なシステムが、市場において高い価値を獲得することを目指す。

０．２　本ルールの基本的な構成と考え方

カメラ画像等の取扱いルールを定めるにあたっては、システムごとに利用者に与えるプライバシーの影響や、情報漏洩のリスクなどを検討する必要がある。特に、個人情報の保持期間と利用の仕方に着目して、対象となるシステムを 4 つのタイプ（タイプ０～タイプ３）に分類し、それぞれにデータの取扱い方法な

どを定めることとした。このうち、はじめの 2 つ、タイプ 0 およびタイプ 1 は、本質的には取得対象を「匿名の集団の 1 人」として扱い、長期間にわたる個人を特定できる情報の保存・保持を行わないものであり、あとの 2 つ、タイプ 2 およびタイプ 3 は、長期間にわたり個人を「1 人の人間」として把握し、その情報を蓄積する、潜在的にプライバシーへの影響の多いタイプのものである。

長期間にわたり個人を把握しようとしないタイプについてはさらに、短期間であっても対象を 1 人の個人として追跡しようとするか否かに応じて、タイプ 0(第 3.1 節)とタイプ 1(第 3.2 節)に細分した。これらにおいては、個人情報の取得から処理までの早い段階において、その情報を取り扱う技術的方法に制限をかけることにより、プライバシーへの影響の大きい情報がそもそも保存されないことを担保することで、利用者のプライバシーが一定以上に最初から保たれるように配慮した。また、個人追跡を可能としないこの類のシステムにおいては、事後に情報の開示や個別の削除などに答えることが難しくなる。個人情報保護法において、個人がもはや特定できない情報は個人情報には直ちに当たらず、開示などの対象としなくてもよいのであるが、実際にシステムを運用する場面では、利用者にとって個人情報を保存するシステムか否かの判断が付かないことから、事業者が「技術的に開示できません」と正直に伝えた場合であっても、このことを納得してもらうのは難しいと考えられる。一方で、これらの開示請求にきちんと答え、また開示により他者のプライバシーを侵害しないことを保証するためには、精度の高い個人特定可能な情報をシステムに保存することが必要となり、却って情報漏洩などのリスクを高めることに繋がりかねない。本ルールではこのような観点から、タイプ 0 およびタイプ 1 を「そもそも開示対象となる情報を全く保存しないルール」と位置づけ類型化することで、事業者・利用者の双方にとってわかりやすい取扱いとなることを意図した。

一方、長期間にわたり個人を把握し追跡するタイプについては、利用者個人の過去の行動が他人に知られるリスクを制御する観点から、顕名などの個人情報と結びつけられるか、あるいは目の前にいる店員などに知られることがあるか否かの、いわば事後の情報の扱い方に着目し、タイプ 2(第 3.3 節)とタイプ 3(第 3.4 節)に細分化した。特にタイプ 2 として、追跡した行動記録を本人に結びつけずに統計的な集団としてのみ活用するタイプを分離し、その取扱いの限界を定めるとともに、オプトアウトの整備を原則とすることで、個人の自己プライバシー管理権に配慮することとした。また、積極的に「特定の人」に関する情報として利用するタイプをタイプ 3 とし、オプト・インによる事前の本人同意を原則とする方向で体系化した。合わせて、カメラからの画像認識という 100%の精度が保証できない手段により取得した情報についての、開示や削除に関する手続きについて、ガイドライン的な規定を設けることとした。これについては、海外における監視カメラの画像開示に関する取扱いルールの事例を一部参考にしている。

０．３　個人による自己情報コントロールへの対処について

カメラという装置は、店舗などに設置すればその性質上どうしても、「撮られたくない」人が映り込むことは避けられない。現時点において「カメラで撮られない権利」が直接的に確立しているとは言えないまでも、「本人の同意なしに個人情報を安易に流通されない権利」は「個人情報の自己コントロール」として本プロジェクトでも強く打ち出されている方向性であり、カメラを特に商業目的に使うに当たっては、自己情報コントロールと情報取得のバランスについて、慎重な判断が求められる。また、近年ではビッグデータ解析などにより、複数のデータを寄せ集める(名寄せ・突合処理)ことにより、個別のデータでは匿名性

が保たれていても、全体として予想も付かない人物像が明らかにされるリスクも不安視されており、対策が必要と考えられる。

本ルールではこのような問題に対して装置側から取り得るアプローチとして、利用の「目的」による制限、技術的な「手段」による制限、本人同意等の「手続き」による制限、の 3 つの取りうる手段から、次のような方向付けで整理を図り、護られる利用者のプライバシー、特に「自己情報コントロール」への配慮をできるだけ明らかにするように努めた。

1） まず、カメラ等を利用した装置のうち「人に関する情報を取得しないことを意図したセンサー」を特定し（第 5 条）、これらから取得された情報については、個人を追跡する目的で使わないことを明確化させる（同条後段）。

2） 次に、店員による従来の手法による属性情報（年齢層や性別・人数等）の取得とさほど変わらない情報しか取得されないと考えられるシステム（タイプ 0 システム）を同定し、これらについては、取得できる情報の種類（第 3 条・第 20 条）やそのデータ処理の手法（第 18 条）などを強く限定することで、撮影対象のプライバシーへの影響が限定されるように意図した。また、名寄せ・突合の処理を明示的に禁止（第 22 条）するとともに、匿名性についても一定の基準（第 4 条）を設けることで、名寄せリスクを最低限に抑えることにも留意した。このような制限は事業者側にとって、システムをタイプ 0 システムの範囲に収まるように設計することにより、利用者のプライバシーに配慮した扱いに自然になるようなものとして、またそのような配慮を簡明に利用者に説明できるようにするという、ある種のガイドラインとなることも意図している。

また、人の流れを追跡するシステムのうち、プライバシーリスクの比較的低いものとして、同一個人の複数回の来店等を追跡しないものをタイプ 1 システムとして整理し、タイプ 0 システムと同じ方向性で整理した。

4） 次に、本人同意の元で情報を取得するケースについて、タイプ 3 システムとして整理した。ここでは、情報の取得範囲や流通については、本人の同意を得ることを前提に強い限定をせず、その代わりにその同意にかかる必要条件を明確化し、利用者の意図に反して同意が取得された扱いとならないことを主に担保する方向で、扱いのルールを整備した。また、カメラというデバイスの性質上、まず情報を取得してから本人同意の有無を確認する流れとなることから、本人同意が確認できる以前の情報の仮の取扱いについても規定した（第 83 条第 1 項）。

5） 最後に、本人の同意なく個人の動線などの流れに関する情報を詳細に追跡するシステムについては、本ルールの対象の中でも（本人同意の有無まで考慮した場合にはタイプ 3 システム以上に）プライバシーへの懸念が大きいことから、慎重な判断が必要となる。この類型に入るシステムは「タイプ 2 システム」として整理しているが、取得対象の除外登録（第 47 条）や情報開示等（第 48 条・第 49 条）の対応を義務づけるとともに、さらに取得したデータを匿名化せずにサービス現場で直接利用することを禁止し（第 45 条第 1 項）、さらにそのような機能を実装すること自体も明文で制限した（同条第 2 項）。これは、この種のシステムにおいて、利用者にとって最も辛いプライバシーへの侵害の 1 つが、目の前にいる人に自分の過去の行動を意図せず開示されることであろうとの観点から、個別データの利用をマーケッティング部署などの間接部門や、計算機内に閉じた機

械統計に限定する趣旨である。この制限により、カメラにより実現できるサービスの設計が不自由になることや、除外請求への対応にかかるコストも無視できないものであることも当然ルール作成時点で想定しているが、同時にこれは、そのようなシステムはできるだけ本人同意の下（タイプ 3）で実現するか、使い方を工夫してプライバシー問題の小さい範囲（タイプ 0）で実現することを推奨する、というメッセージでもある。マーケティングなどの現場ではどうしても、「できるだけ多くの情報を取っておけば、何かしら役に立つはず」という発想からデータを余計に取得しがちになることに対して、最初から必要なデータだけを取る、最初から機械での集合化処理を前提にシステムを設計する、というプライバシー寄りの発想への転換を誘導することも、本ルールの意図の 1 つである。

第１節 総論

第1条　　本ルールは、商業上の情報を取得するために商業施設等に設置される、可視光カメラまたはモノクロの赤外線カメラにて取得した画像情報を単独で、またはその他のセンサー類と組み合わせて処理するシステムを対象とする。

２　本ルールでは、下記のシステムは対象から除外する。ただし、当該システムが本ルールの定める条件を満たす場合においては、設置者の判断によりルールの対象とすることを妨げない。

(ア) 被写体となる顧客の希望により行われる、画像そのものの撮影・処理をサービスとするシステム。

(イ) 取得した画像を即時に画面等に表示し、蓄積・解析等を行わないモニタカメラシステム。

(ウ) 取得した画像に対し、人物の特徴の抽出・追跡等の処理をせずに蓄積し、防犯目的でのみ利用する防犯カメラ単独目的のシステム。

(エ) 店舗のバックヤード等、通常の顧客が出入りしない領域のみを対象に情報を取得するシステム。

(オ) 行政施設等と一体化した施設など（空港等）において、法令の定めにより個人画像等の取得が強制されている（オプトアウトが禁止されている）システム。

(カ) その他、法 18 条第 4 項第三号に該当するシステム。

（補足）（ア）の装置は、証明写真機やいわゆる「プリクラ」の装置などがその例に当たる。
（イ）のモニタカメラシステムおよび（ウ）の防犯カメラシステムについては、防犯カメラシステムや駅で車掌などが用いる乗降モニタなどについて、主に既設の単機能のもの本ルールの対象から除外するものである。監視カメラとして情報を取得・保存するとともに、当該カメラの情報から商用目的の情報をも取得するタイプの複合的なシステムや、既存の防犯カメラの画像に商業目的の二次利用を追加する場合については、本ルールの対象とし、第 4.2 節のオプション機能として定義する。
（オ）のような強制的な性格の強いシステムについては、本ルールの対象となる他のシステムと大きくそのプライバシー保護の考え方が異なることから、「本ルールに準拠したシステム」として利用者に統一的に提示することが不適切と考えられることから、対象から除外する。

３　本ルールは、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」または「法」という。）の諸規定並びに関連政令・個人情報保護委員会規則等に基づき運用されるものとする。

第2条　　本ルール中で用いるデータの種類に関する特定の語の定義は、以下によるものとする。

(ア)「個人特定情報」：個人の顔・指紋・虹彩などの画像・映像の他、データを変換することにより、人間に知覚可能な形で、ある特定の個人を特定することのできる画像等を復元できるデータのこと。

（解説）この種の情報は、単独で個人情報保護法における「個人情報」に該当する。

(イ)「個人特徴情報」：特徴点・量の抽出などの技術的手段により変換され、データからは元の個人の画像等を復元できないが、同じ個人の画像等と照合することにより、データが同

ーの個人である可能性が高いか否かを判定できるデータのこと。また、車の登録番号等、個人との結びつきが強くその相関が推測できるデータについても、個人特徴データに準じて扱う。

（解説）この種の情報は、単独で個人情報保護法における「個人情報」に該当する。

（補足）カメラ装置が JPEG 等の汎用の画像圧縮技術を用いる場合において、たまたま圧縮に使われた特徴が結果的に個人の特徴を反映したものであった場合においても、後段の情報処理においてその特徴を意図的に利用しない限りにおいては、当該データは個人特徴情報とは見なさない。

(ウ)「個人属性情報」:特徴量の抽出などの技術的手段により変換され、複数の個人が同一の属性の集合に変換されるため、同じ個人の画像や個人特徴データ等を新たに提示された場合であっても、データが同一の個人である可能性が高いか否かを判定できないデータのこと。

（解説）この種の情報は、単独では個人情報保護法における「個人情報」には該当しないと考えられる。ただし、他の個人を特定する情報と容易に紐付けができる場合には、全体としては「個人情報」に含まれることになる。

（補足）本ルールでは、混雑度の追跡などで用いられる、ただ「人がそこにいる」などの属性情報を伴わない存在データについては、便宜上、単一の属性まで縮減された「個人属性情報」の一種として扱う。

(エ)「個人行動情報」:カメラ・その他のセンサーなどで取得されたデータから、動線抽出技術などを用いて抽出した、人の動線や振る舞いその他、取得対象者の行動に関するデータ。

（解説）この種の情報は、単独では個人情報保護法における「個人情報」には該当しないと考えられる。ただし、他の個人を特定する情報と容易に紐付けができる場合には、全体としては「個人情報」に含まれることになるほか、個人属性データと異なり人のプライバシーに関するより詳細な情報が含まれるため、取扱いに注意を要する。

(オ)「人物関係情報」:上記(ア)～(エ)に該当するデータ。

2　本ルール内で用いる以下各号の用語の意味は、以下に示すところによる。

(ア)「設置事業者」:本ルールに準拠するセンサー情報利用システムを、自己の管理する施設に設置する事業者をいう。

(イ)「設置施設」:本ルールに準拠するセンサー情報利用システムを設置する施設をいう。

(ウ)「委託データ処理事業者」:設置事業者からの委託等により、システムの情報処理の一部または全部を行い、またはシステムから取得した人物関連情報を保存・管理する事業者をいう。

(エ)「システム開発事業者」:本ルールに準拠するセンサー情報利用システムの各々について、当該システムの全体を設計・開発した事業者をいう。

(オ)「統括団体」:本ルールの業界自主規制ルールとしての運用を統括し、個人情報保護体制の社会実装を推進する団体をいう。

（解説）本項の団体は、個人情報保護関連法において検討・想定されているマルチステークホ

ルダー・プロセスにおいて、いわゆる「自主規制団体」と呼ばれる団体が今後組織され、本ルールを運用することを想定している。

(カ)「突合」:同一の事象から、同一の個人からなど、繋がりがある源から発生したと思われる、独立した情報として存在する 2 以上の情報について、時刻情報などその情報の特徴から関連性を推測し、同一の事象に基づく単一の情報として結合すること、および同一の事象に基づくものとして取り扱うこと。

（解説）プライバシーの概念として「脱匿名化 (de-anonymization)」と呼ばれる操作にあたる。

(キ)「利用者」:本ルール中では、システムを利用する者としての営業主体ではなく、施設を利用する者としての画像取得の対象となる人を指す。

第3条　　本ルール中、「人間が容易に知覚できる属性情報」とは、画像情報から取得した、以下に列挙する属性の推定情報を指す。

- **年齢層に関する推定情報**
- **性別に関する推定情報（容姿から推測したものに限る。）**
- **服装・色彩等に関する可視範囲の情報**
- **その他、明らかにその場にいる人間が感知できる属性情報**

（解説）本条は、将来のセンサー技術の進展により、人の内面・健康・病気・感情等に関する情報で、その人が周囲の人に隠している可能性のある情報が、本人の同意無くセンサーにより取得され、周知になることがないことを保証するためのものである。

第4条　　本ルール中、「匿名性が保たれると認められる属性区分」とは、情報を取得する対象について、その区分数が下記のいずれかの条件を満たすものを言う。

(ア) 識別する属性の区分数が 1 である（属性識別を行わない）もの。

(イ) 属性取得の対象人数の、1 週当たりの平均想定数が、識別する属性区分数の 10 倍を超えるもの。

(ウ) システムが統計的な処理を行った結果のみを出力するものであって、その統計単位時間当たりの属性取得の対象人数の想定が 5 人以上であり、統計情報の出力時に、区分に含まれる情報が 5 未満である区分を自動的に統合または除却し、出力結果において各属性区分に含まれる情報数が 5 以上であることを保証するもの。

（解説）本条の条件は、属性別のデータを出力した際に、入力のデータ数が少なすぎることにより、実質的に特定の属性のデータが特定の個人に紐付き、必要以上の個人情報が取得されることを防ぐものである。

例えば年齢層で 7 層（10 歳以下、10 代、20 代、…、60 代以上）、性別で 2 種の計 14 通りの属性を識別するシステムにおいて、1 週当たりの想定来客数が 140 人を超える箇所に設置する場合には、特に追加の処理をせずとも本条の条件（イ）を満たすと評価する。

一方、140 人の来客が見込めない場合でも、例えば 10 代男子が 3 人、10 代女子が 3 人であった場合、自動的にこの 2 つの情報を統合し、10 代 6 人の情報として出力するようなシステムであれば、本条（ウ）の条件に適合する。この場合、条件（ウ）を満たすことが確定するまでは、属性情報と紐ついた個々のデータを取り出すことができないよう、システムを構築する

必要があることに留意する必要がある。

第5条　　人物関連情報を検知して自動的に削除するなど、人に関する情報を取得しないことを目的として開発されたセンサーから取得された情報については、本ルールにおいては人物関連情報とみなさない。ただし、当該のセンサーに偶然人物関連情報が混入される可能性がある場合には、その可能性および発生の具体的頻度が十分低いことを実証すること、偶然取得された人物関連情報については削除し他の目的に利用しないこと、その条件とする。

2　個々のセンサー技術について、前項の条件への適合を判断する具体的要件については、別途定める。

（解説）本条のセンサーは赤外線センサーなどのそもそも画像を取得しないセンサーのほか、例えば、十分にぼかしの処理を入れる、時間方向の変化を検出して長時間変化が無いバックグラウンド情報だけを抽出する、高い位置から垂直に見下ろして顔が映らないようにする、などの対策を施したカメラなどが該当する。

具体的要件については今後検討するが、センサーの設置条件などによることも多いので、一定の技術要件を設けるほかに例えば、「実際に一定期間の試験運用で映り込む頻度が少ないことを検証する」「市場に提供する最も高性能な人物検知技術を用いても追跡できないことを確認する」などの手法も考えられる。

第２節　共通ルール

２．１　事業者ごとの責務

第6条　　本ルールに準拠するシステムの設置事業者は、当該システムを利用した個人関連情報取得とその後の利用、データ廃棄に至る全ての段階について、利用者に対する説明と結果の責任を負うとともに、システムが本ルールの趣旨に基づき適切に運用されること、本システムに関係して取得した個人情報が故意ないし事故により外部に流出しないよう適切な管理と監査を行わなければならない。

2　設置事業者は、自らを含む本システムに関わる個人関連情報を取り扱う情報システムを運用する者に対し、適切な ISM ガイドライン等を策定させ、情報漏えいを防ぐ適切な管理体制を構築させなければならない。

第7条　　本ルールにおける委託データ処理事業者は、設置事業者からの委託に基づき、適切に個人情報を処理するとともに、受託して保管・管理する個人情報が故意ないし事故により外部に流出しないよう適切な管理と監査を行わなければならない。

第8条　　本ルールにおけるシステム開発事業者は、設置事業者に提供するシステムが本ルールの条件を適切に満たすよう、特に本システムの外部に開示すべきでない個人関係情報が取り出し可能にならないよう、システムを設計・実装するとともに、事業者が個人情報の管理を適切に行えるよう、必要に応じてアクセス権限の設定など導入の支援を行わなければならない。

第9条　　本ルールの統轄団体は、本ルールが設置事業者において、消費者保護の立場から適

切に運用されるよう、必要なガイドライン等の制定と改正などを行うとともに、消費者保護委員会などの公的機関と連携し、不適切な設置事業者に対する指導など、その社会全体における運用を適切に保つよう努力しなければならない。

2　統括団体は、本ルールの事業者および消費者への普及啓発活動などに努めるものとする。

2．2　利用タイプの特定と利用者への通知

第10条　　本ルールに準拠するシステムの設置事業者は、その設置施設ごとに、システムが本ルールの第 3 節に定めるタイプのいずれに該当するかを特定し、それぞれに定める提供条件を満たさなければならない。

2　単一のシステムが第 3 節に定めるタイプの複数に該当する機能を同時に実装する場合、または第 4 節に定めるオプション機能を加えて実装する場合には、カメラ、計算機その他の機構を共有することができる。ただし、その場合、タイプの異なる機能ごとに独立して、それぞれに定める提供条件を満たさなければならない他、本ルール内で特記する場合を除き、タイプの異なる機能間でデータの突合・結合などを行ってはならない。

第11条　　設置施設には、その施設の入り口等、通常その施設を利用する利用者が施設に入る前に容易に認知すると考えられる位置に、下記の情報を掲示しなければならない。

- **本ルールに準拠したシステムにより、カメラ・センサー等で人物関係情報を取得している旨**
- **情報を取得するセンサーの種類**
- **情報を取得する目的の概要**
- **タイプごとに定める情報**
- **詳細の情報を公表する方法（Web サイトの URL 及び 2 次元コードなど。）**

2　前項の掲示における「詳細の情報の公表」には、下記の情報を含めなければならない。

- **前項に定めた情報**
- **情報を取得する目的**
- **取得するデータの種類の詳細**
- **データを取得する主体の名称と住所・問い合わせ先**
- **データ処理を外部に委託する場合には、委託先の名称等**
- **タイプごとに定める情報**
- **システムの利用登録および利用停止等の手続きに関する詳細**

3　1 つの施設内に複数のシステムを設置する場合、および前条第 2 項により複数のタイプのシステムの機能を実装する場合には、それぞれのタイプ毎に、第 1 項および第 2 項の情報を併記しなければならない。

4　同一法人・ブランドの運営者等の設置事業者が同一の取扱い条件によるシステムを 2 以上の箇所に導入する場合、第 2 項の詳細の情報の公表はこれを複数箇所に共用することができる。

5　第 1 項の掲示並びに第 2 項の詳細の情報の掲示方法の詳細については、付録 A および付録 B において基本的な要件を定める。

２．３　利用目的の特定と、目的外利用の制限

第12条　　設置事業者は、本ルールに準拠するシステムで取得した人物関連情報を利用する際には、各タイプに定める制限の範囲内において、事前にその目的を具体的に特定し、第 11 条に従いそれを利用者に周知しなければならない。

第13条　　設置事業者は、個人特定情報、個人特徴情報、個人属性情報および、これらから得られるデータと紐付けられるシステム以外から取得されるデータを利用する場合には、前条で特定しデータ取得時点において周知した範囲を超えて利用してはならない。ただし、以下に該当する場合は、この限りではない。

（ア）利用範囲の変更について、本人から個別の同意を取得した場合。

（イ）法令に基づく義務を履行する場合。

（ウ）法令に基づき、法執行機関および行政機関の請求または協力の要請があった場合、その請求または要請に応えるために必要な範囲のデータを提供する場合。

（エ）その他、個人情報保護法第 16 条第 3 項に定める事由に該当する場合。

（解説）本条について、「データ取得時点において」利用者に周知した範囲を超えたデータの利用を認めないことから、データ取得後に利用目的を追加し新たに周知しても、追加前に取得したデータをその新たな目的に流用することはできない。この場合、（1）利用目的の変更以前に取得したデータを一括して破棄する、（2）利用目的の変更通知前後でデータを分別管理する、のほか（3）各データに対し、周知した利用目的通知の版数（新たに個別に取得した同意によるものを含む）等を付加して管理し、その付加情報に基づき処理方法を変更する、などの方法が考えられる。

第14条　　設置事業者は、個人特定情報および個人特徴情報については、第 12 条でデータ取得時点において周知した範囲を超えて第三者への提供を行ってはならない。ただし、前条但し書きのいずれかに該当する場合においては、その限りでない。

第15条　　設置事業者は、個人属性データおよび個人行動データについては、第 12 条で周知した範囲を超えて第三者への提供を行ってはならない。ただし、第 13 条但し書きのいずれかに該当する場合と、そのデータを匿名加工情報（平成 27 年法律第 65 号で改正される法第 2 条 9 項に定める「匿名加工情報」の条件に合致するデータをいう。）として取扱う場合においては、その限りでない。

２　前項において、データを匿名加工情報として第三者提供する場合には、法の定める要件に加え、以下の各号の条件を全て満たさなければならない。

（ア）第三者提供する情報の種類を、第 11 条第 2 項の詳細の情報において明らかにすること。

（イ）そのデータに含まれる属性情報が第 4 条の「匿名性が担保されると認められる属性区分」の範囲に含まれること。

（ウ）データ提供の受領者（受領者から間接的に提供される二次以降の受領者を含む。）による他のデータとの突合などにより、匿名性が満たされなくなることがないことを、提供契約に付す条件などにより明示的に担保すること。

第16条　　本節の他の規定に関わらず、設置事業者は、そのシステムの情報処理の一部を、法第 23 条第 4 項一号に基づき外部の委託データ処理事業者に委託して行わせることができる。この場合において設置事業者は、その委託データ処理事業者を第 11 条第 2 項の詳細の情報において特定し通知するほか、当該事業者と本ルールを前提とした秘密保持契約等を締結しなければならない。

（解説）本条は、SaaS や IaaS などのクラウドデータ処理技術が一般的になってきていることを踏まえ、そのようなサービスを用いて本ルールが対象とする情報の処理を行う事を追認するものである。ただし、この追認はあくまで、システムを実装した単独の装置を現場に設置し自ら運用した場合と同じ範囲でしか情報が共有されないことを前提とする。

2　前項の委託データ処理事業者は、前項に基づき委託されたデータ処理を第三者に再委託する場合は、当該の再受託者と本ルールを前提とした秘密保持契約等を締結しなければならない。その受託者が更に第三者に再委託する場合もこれに準ずる。

3　第 1 項の委託データ処理事業者および前項の再受託者が、本条に基づき異なる複数の情報源から処理の委託を受ける際には、それぞれの情報源から得られたデータを分別し、それぞれを独立に取扱わなければならない。委託先が複数のデータ源から得られたデータを総合的に処理して解析を行う場合等においては、当該処理は本条の委託とみなすことはできず、第 41 条または第 53 条に基づくデータの共有または第 15 条に基づく第三者提供として扱わなければならない。

4　前三項の規定は、設置事業者または委託データ処理事業者が、第三者の計算機資源を借用してシステムの情報処理を行う場合に準用する。但し、第 1 項の規定中、利用者への通知については、これを適用しない。

（解説）クラウドの利用形態として、計算リソースの単位で資源を借用し、借用者が自らデータ処理を行う場合においては、データ処理の実質的主体は借用者にあり、借用先の情報を開示することの意義が薄いことから、通知を必要としないこととする。
（補足）また、計算資源借用にかかる契約または約款に、個人情報保護法等に適合する秘密保持条項が一般的な条項としてあらかじめ含まれている場合、当該条項は本項で準用する第 1 項の「本ルールを前提とした秘密保持契約等」の要求を満たすものとする。

第 3 節　タイプ毎の個別ルール

3．1　タイプ 0 システム

（解説）本タイプのシステムは、個々のカメラから取得した画像情報から、人数のカウントや属性情報の推定などを行ってその場で利用するが、一切の個人特定・追跡可能な情報を保存しないシステムを想定としている。
　本タイプのシステムで取得する情報は、基本的には法で定める個人情報に該当しない情報のみになることを意図している。ただし、実際の個別のデータについては、データの突合や属性についての匿名性の不足なども考えられるため、本ルールをもって直ちに個人情報に該当しない、と断言はできないことには留意する必要がある。

第17条　　本ルールにおける「タイプ 0 システム」として提供するシステムは、本節の各条の条件を満たすものとする。

2　第 5 条に定める人物関連情報を取得しない機能からなるセンサーのみを用いて構築したシス

テムについても、「タイプ 0 システム」として扱うことができる。

第18条　　本タイプのシステムのセンサーで個人特定情報および個人特徴情報を取得した場合は、取得後直ちに属性推定等を行い個人属性情報に変換し、個人特定情報並びに個人特徴情報は直ちに破棄し、システムに記録・保存しないものとする。

第19条　　本タイプのシステムでは、単独のカメラで撮影される範囲を超えて、個人行動データを取得・追跡してはならない。

（解説）本タイプのシステムでは、例えば複数フレームの間で人数の重複計上を防止する、あるいは人の出入りの方向を認識するなどの目的に限り、個人特定情報を利用しない範囲で「物体としての人」の動きを追跡することを許容する。ただし、個人特定情報や個人特徴情報の利用の有無にかかわらず、複数のカメラにまたがって広い範囲で映った人間の一人一人の流れを繋げて追跡する場合などには、タイプ 1 システムとして扱うこととする。例えば、ID タグなどカメラ以外の手段により追跡を行う場合についても同様にタイプ 1 に該当する。

第20条　　本タイプのシステムで取得する人に関する情報は、第 3 条で定める「人間が容易に知覚できる属性情報」の範囲に限る。

第21条　　本タイプで取得した個人属性情報は、サービス提供（販売した物品等）の情報など、センサー以外から取得した個人を特定しない情報と紐付けて利用することができる。ただし、本タイプのシステム由来の個人属性情報については、第 4 条に定める「匿名性が保たれると認められる属性区分」を満たす必要がある。

第22条　　本タイプのサービスで推定した属性情報は、他の個人を特定する情報やタイプ 1 以上のシステムに相当する情報を取得するシステム等から取得した情報と突合してはならない。

（解説）例えば、本タイプのシステムで取得した情報を、氏名の記載・登録されたポイントカードの情報と紐付けて保存する場合、センサーで取得したデータが特定の個人と紐つくことから、全体をタイプ 3 のシステムとして扱わなければならない。
　一方、ポイントカードシステムに登録された情報などから年齢層や居住地域など第 4 条の条件を満たす情報を切り出し、システムで推定した個人属性情報を補正・補完する場合、補正・追加される属性情報は「個人を特定する情報」とは言えないので、引き続きタイプ 0 のシステムとして扱うことができる。
　また、例えば本タイプのシステムと個人別のポイントカード等が別のシステムとして運用され併用されている店舗において、時刻情報などでその 2 つのデータの突合を行い、本システムの匿名のあるデータが具体的な誰であるかをポイントカードの情報から推測しようとすることは、本条に抵触する。

第23条　　本タイプのシステムには、システムの利用登録および利用停止のための個人特定機能を実装しない。

（解説）個人情報保護の原則的な立場からいえば、カメラ画像等による個人識別については、システム利用の有無を個人が選択できることが望まれていると考えられる。一方で、システムの実装上、センサーから人・属性を認識するシステムに個別の利用停止の機能を実装するためには、利用停止対象の個人を特定する情報を長期にわたって保存し、利用時に個人識別をすることが求められる。タイプ 0 及び後述するタイプ 1 のシステムにおいては、個人情報保護のために積極的にそれぞれ「個人識別をしない」「個人特定可能な情報を長期保存せず破棄する」ことを機能として求めており、このようなシステムに利用拒否の機能を実装することは、シス

テム内に個人特定可能情報を保存することになり、本来の個人情報保護のためのシステム設計の趣旨と矛盾する結果になる。このような観点から、本ルールでは、タイプ 0 及びタイプ 1 のシステムには必ずしも利用停止の機能を実装しないこととし、また、利用停止機能を実装したシステムについては、システム内部に利用停止のための個人特定情報が保存されることから、後述するタイプ 2 のシステムとして取り扱うこととする。

第24条　　本タイプのシステムにおいては、個人を識別する機能を実装せず、特定個人に関連した情報を一切保持しないことから、個人を特定することを前提とした、自己情報開示・自己関連データ削除の機能を提供しないものとする。

（解説）本条も前条と同じく、タイプ 0 及び後述するタイプ 1 のシステムにおいては、個人情報保護のために積極的に「個人識別をしない」「特定可能な情報を長期保存せず短期破棄する」ことを機能として求めていることから、個人特定情報の保存を前提とした開示対象のデータが存在しないことを設計意図として追認するものである。なお、前条と同様、当該機能を実装する場合には、タイプ 2 のシステムとして取り扱う。

実際の現場においては、タイプ 0 およびタイプ 1 システムの保有する情報についての法 25 条による開示請求については、直ちにデータを削除する運用の結果として、同条の「データが存在しない旨を知らせる」ことになるものと想定される。

なお、本条の規定は、第 4 条の条件を満たさない情報の漏洩事故等により、実質的に個人情報が保存されていると認められる場合においてまで、自己情報開示・自己関連データ削除の請求を拒否してよい旨を定めるものではない。

第25条　　本タイプのシステムにおいては、第 14 条但し書きに該当する場合および、第 15 条の匿名加工情報の扱いに該当する場合のほか、人物関連情報を第三者に提供しないこととする。

第26条　　本タイプのシステムについて第 11 条に従い告知すべき情報は、同条に定めた情報とする。

3．2　タイプ 1 システム

（解説）本タイプは、「個人特徴情報」や複数のカメラ・センサーからの「個人行動情報」の連続的な追跡等により、施設利用者の「1 回の利用」の期間内において、各利用者を「匿名の個人」として認識し、行動の把握等を行うシステムを想定している。

第27条　　本ルールにおける「タイプ 1 システム」として提供するシステムは、本節の各条の条件を満たすものとする。

第28条　　本タイプのシステムのセンサーで取得した情報は、必要に応じて「個人特徴情報」の抽出と「属性情報区分」の推定を行い、それ以外の個人特定情報に属する情報を全て直ちに破棄するものとする。

（解説）本条は、必ずしも特徴情報の抽出と属性の推定を行わなければならない、というものではない。

第29条　　取得した個人特徴情報および人物行動情報は、利用者が施設の入場および退出をはっきりと認識できる単一の施設の中でのみ利用し、他の場所で取得した情報とは共有・突合しないものとする。

2　立地の都合等で見かけ上分割された同一の設置者による近接する店舗群等で、利用者にとってその施設群の利用が「連続した 1 回の施設利用」と認識される施設については、本節においてこれを複合施設群として、1 カ所の施設とみなすことができる。この場合には、その範囲をあらかじめ特定しなければならない。

（解説）例えば、上野動物園の東園と西園や、建物の都合で隣接分離している百貨店の本館と別館などは、本条における「単一と見なされる複合施設群」として扱うことができる。一方で、複数駅の駅ビルや、コンビニエンスストアの地域内の複数店舗などは、利用者にとって「複数回の独立した施設利用」と感じられることから、「複数の施設」として扱い、これらの間で人流の追跡をする場合には、タイプ 2 システムとして扱う。なお、例えば同じ駅構内のシステムであっても、鉄道会社による駅構内全体での人流追跡と、構内営業者による複数店舗間での追跡は、利用者にとって「1 回」「複数回」の施設利用の感じ方が異なることから、本条における取扱いが分かれることが有り得る。
　いずれにしても、「同一の施設群と扱う範囲」が利用者にとって自明で無い場合には、事前の告知掲示において明示しておく必要がある（付録 A の掲示例も参照）。

第30条　　取得した個人特徴情報は、システムが同一人物だと認識する対象毎に匿名 ID を付与して管理し、システム毎に事前に定める保存時間で破棄することとする。その保存時間は、24 時間を超えないものとする。

2　システムは、以下の時点を超えて取得した人物関連情報については、別の人物に関する情報として取り扱うものとする。

- **同一人物と認識する特徴量の最後の取得から 1 時間以内**
- **設置対象施設において、入場時・退場時それぞれに入館証の取得など入退館の手続きを取ることが求められている場合においては、退場の手続き時点・閉店時など、当該施設内に残留しないことが判明した時点**

3　前 2 項の他、対象者が設置対象の施設群を去ったことをシステムが認識した場合には、システムは当該対象者に係る個人特徴情報を破棄するものとする。

（補足）本項は、システムが必ず対象者の退出を認識できなければならない、という趣旨ではない。

第31条　　本タイプのシステムで取得する属性情報は、第 3 条で定める「人間が容易に知覚できる属性情報」に限る。

第32条　　本タイプのシステムで取得した個人属性情報、第 5 条に定める人物関連情報を取得しない機能からなるセンサーから取得した情報、センサー以外から取得した個人を特定しない情報、および、本タイプのシステムで取得した個人行動情報については、第 30 条で定める同一の匿名 ID に紐付けたものについて、単一の特定の匿名利用者に関する情報として利用することができる。ただし、本タイプのシステム由来の個人属性情報の利用については、第 4 条に定める「匿名性が保たれると認められる属性区分」を満たす必要がある。

第33条　　本タイプのサービスで匿名 ID と紐付けた情報は、他の個人を特定する情報やタイプ 2 以上のサービスから取得した情報と結合してはならない。

第34条　　本タイプのシステムで特定の対象者と紐付けた情報については、対象者を特定しない統計的な利用を除き、設置施設の現場において、対象者以外の人間（従業員を含む）に開示してはならない。ただし、取得する情報の種類と取得時点が明示されている場合において、本人の自由な申し出に基づきその情報を照会する場合は、この限りで無い。

（解説）本条の趣旨は、匿名を前提に ID に紐付けられた情報が、店頭で特定の個人と紐つくことにより、従業員等を通じた情報の漏洩が起こることを防止することである。例えば、1 カ所から見通せない規模の店内において、ある来客が「どれくらい在店しているか」「どの売り場を通ってきたか」などはプライバシー性の強い情報であり、このような情報を店頭で店員に知らせサービスに反映する場合には、タイプ 3 システムとして事前に顧客にその旨を通知し同意の元で提供することを求める。当然、本人の事前の同意が得られない場合には、そのような情報を取得できないことになる。
　なお、通常の 1 人で見通せる、カメラ 1 台で把握できる範囲において、その範囲内で即時にその情報を用いる場合は、システム全体をタイプ 0 システムとして構築することで、本条の制限を受けないことができる。
　一方、例えば「ある売り場を何人が通ったら、5 分後にはレジが混むので店員に事前アラートを上げる」などの統計的利用は、これに該当しないものとしてタイプ 1 システムにおいても現場で情報を扱うことができる。また、1 回の施設利用の中であっても、通ってきた売り場を元にリコメンドを行う場合等には、その取得した情報が対象者以外に知られることがないよう注意する必要がある。
　但し書きについては、例えば自動車の登録番号に基づき通常は機械処理される駐車場課金システムにおいて、駐車券を紛失した利用者が、自動処理システムに基づく料金の請求を従業員に希望した場合などが該当する。

第35条　　本タイプのシステムには、システムの利用登録および利用停止のための長期的な個人特定機能を実装しない。

第36条　　本タイプのシステムにおいては、個人を長期的に識別する機能を実装しないことから、特定個人を識別することを前提とした、自己情報開示・自己関連データ削除の機能を提供しないものとする。

（解説）第 23 条、第 24 条の解説を参照されたい。なお、第 24 条同様、本条の規定も、情報の漏洩事故等により、実質的に個人情報が保存されていると認められる場合においてまで、自己情報開示・自己関連データ削除の請求を拒否できる旨を定めるものではない。

第37条　　本タイプのシステムにおいては、第 14 条但し書きに該当する場合および、第 15 条の匿名加工情報の扱いに該当する場合のほか、人物関連情報を第三者に提供しないこととする。

第38条　　本タイプのシステムにおいて、第 11 条第 1 項の掲示および第 2 項の詳細の情報の公表には、同条の定めの他、第 29 条で特定した単一の施設群と見なす追跡の範囲に関する情報を含めるものとする。

3．3　タイプ 2 システム

（解説）本タイプは、長期（施設群の複数回の利用）にわたり各施設利用者を「匿名の個人」として認識し、その行動の追跡等を行うシステムを想定している。

第39条　　本ルールにおける「タイプ 2 システム」として提供するシステムは、本節の各条の条件を満たすものとする。

第40条　　本タイプのシステムのセンサーで取得した情報は、「同一個人追跡のための特徴量」と（必要であれば）第 4 条に定める「匿名性が保たれると認められる属性区分」の推定を行い、それ以外の個人情報を全て直ちに破棄するものとする。

第41条　　取得した特徴量は、同一の営業の主体による施設でのみ共有し、他の営業の主体等で取得した情報とは共有しないものとする。

（解説）本条における「営業の主体」は、必ずしも直接のサービス提供法人や、施設管理者には限定されない。例えば、コンビニエンスストアのフランチャイズチェーンのように、複数の法人で一体となって運営されるサービスにおいては、そのチェーン本部を営業の主体として、一体としてシステムを運用することができる。ただし、この主体はあくまで利用者から認識できる営業活動に直接に関係するものである必要があり、例えばデータ分析サービスのような、個人に対して直接に営業していない（利用者から営業主体と認識できない）法人等が、複数の異なる実質的営業主体を束ねてデータ分析をすることは認められない。

第42条　　取得した特徴量は、システムが同一人物だと認識する対象毎に匿名 ID を付与して管理し、システム毎に事前に定める期間で破棄することとする。その保存期間は、同一人物と認識する特徴量の最後の取得から 1 年を超えないものとする。

（解説）本条においては、第 30 条と異なり、実質的に期間内に複数回の同一特徴人物の施設利用があることを想定している。そのため、同条第 2 項にあるような、退店を認識した際のデータの切り離しなどは想定しない。

第43条　　本タイプのシステムで取得した属性情報、第 5 条に定める人物関連情報を取得しない機能からなるセンサーから取得した情報、センサー以外から取得した個人を特定しない情報、および、本タイプのシステムで取得した個人行動情報については、第 42 条で定める同一の匿名 ID に紐付けたものについて、単一の特定の匿名利用者に関する情報として利用することができる。ただし、本タイプのシステム由来の属性情報の利用については、第 4 条に定める「匿名性が保たれると認められる属性区分」を満たす必要がある。

第44条　　本タイプのシステムで匿名 ID と紐付けた情報は、他の個人を特定する情報やタイプ 3 以上のサービスから取得した情報と結合してはならない。

第45条　　本タイプのシステムで付与した匿名 ID およびその ID と紐付けた情報については、対象者を特定しない統計的な利用を除き、設置施設の現場において、対象者以外の人間（従業員を含む）に開示してはならない。

（解説）本条の趣旨は第 34 条と同じであるが、タイプ 2 システムでは複数回利用や複数店舗利用の情報が紐付けされることから、プライバシー性がより一層強い情報であり、その取得・保存した情報が対象者以外に知られることがないよう、細心の注意を払う必要がある。また、従業員に情報取得を認めるシステムを構築することのリスクがタイプ 1 システムより格段に大きいことから、本条では第 34 条に相当する但し書きを設けていない。

２　本タイプのシステムにおいては、匿名加工情報とされた情報を除き、タイプのシステムで付与した匿名 ID およびその ID と紐付けた情報について、個別に読み出し・取り出しのできる機能をシステムに実装してはならない。

第46条　　本タイプのシステムを設置する主体は、第 41 条における共有の範囲、第 42 条における紐付けて保存されるデータの保存期間、第 43 条における保存するデータの種類を特定しなければならない。

第47条　　本タイプのシステムには、原則としてシステムの利用登録または利用停止の機能のいずれかを設けることとする。

第48条　　本タイプのシステムを運用する設置事業者は、データの開示請求に原則として応じなければならない。開示するデータは、少なくとも第 46 条において特定した種類のデータを、その記録時刻・記録場所とともに含むものとする。

２　匿名 ID の識別精度が悪く、データの開示において他者のデータの混入の可能性が高く、かつそのデータの開示が他者のプライバシーを著しく侵害する可能性がある場合には、前項にかかわらず、当該のプライバシーを著しく侵害するデータの開示をしてはならない。この場合は、開示できないデータの種類とその理由をあらかじめ特定しなければならない。

第49条　　本タイプのシステムを運用する設置事業者は、個人データの削除請求を受け付けなければならない。削除請求があった場合、削除しないことに正当な理由がある場合を除き、その請求に原則として応じなければならない。

２　設置事業者は、データの削除請求について、データの削除に応じない可能性を留保する場合には、あらかじめその理由を特定しなければならない。ただし、前条第 2 項において開示を行わないデータが存在する場合、当該データについて削除の請求があった場合には、次項に該当する場合を除き、必ず請求に応じなければならない。

３　設置事業者は、第 13 条但し書きの各号に該当する場合において、法執行機関等から情報提供の請求を受けている場合または受ける可能性が高い場合においては、前 2 項に関わらず削除請求に応じないことができる。この場合においては、当該のデータについては情報提供以外の目的に利用しないものとする。

第50条　　システムの利用登録および利用停止、データ開示、データ削除に関しては、前 3 条のほか、第 6 節の一般原則に従う。

第51条　　本タイプのシステムにおいて、第 11 条第 1 項の掲示および第 2 項のサイトには、同条の定めの他、それぞれ以下の情報を含めるものとする。

（ア）第 1 項の掲示：第 41 条における共有の範囲、第 42 条における紐付けて保存されるデータの長期、システムの利用登録または利用停止を受け付ける旨の表記、第 48 条第 2 項に該当するデータの有無、第 49 条第 3 項に該当する場合にはその旨。

（イ）第 2 項のサイト：第 46 条で特定した情報の範囲、第 48 条第 2 項に該当するデータの種類とその開示のできない理由、第 49 条第 3 項に該当する場合にはその理由、第 85 条で定める情報の取扱いに関する共通の掲載事項。

３．４　タイプ 3 システム

（解説）本タイプは、長期（施設群の複数回の利用）にわたり各施設利用者を個人して認識し、その行動の追跡等を行うシステムのうち、非匿名のデータとの紐付けを行うか、従業員などを通じたサービス現場への直接的な反映を行う場合を想定している。

第52条　　本ルールにおける「タイプ 3 システム」として提供するシステムは、本節の各条の条件を満たすものとする。

第53条　　本タイプのシステムのセンサーで取得した個人情報及び特徴量は、同一の管理主体による施設でのみ共有し、他の管理主体等で取得した情報とは共有しないものとする。ただし、対象となる本人の明示的な合意がある場合にはその限りではない。

第54条　　取得した特徴量は、システムが同一人物だと認識する対象毎に ID と紐付けて管理し、システム毎に事前に定める期間で破棄することとする。その保存期間は、以下のいずれかを超えないものとする。

（ア）同一人物と認識する特徴量の最後の取得から 1 年以内

（イ）ID が会員登録など顕名の明示的な契約等と紐付けられた場合には、その契約等の有効期間内

第55条　　本タイプのシステムで取得した個人属性情報および個人行動情報については、システムが同一対象と認識した者に紐付けた情報について、単一の特定の利用者に関する情報として保存・利用することができる。

第56条　　本タイプのシステムで ID と紐付けた情報は、センサー以外から取得した情報や、他の個人を特定する情報と結合することができる。

第57条　　本タイプのシステムを設置する主体は、第 53 条における共有の範囲、第 54 条における紐付けて保存されるデータの保存期間、第 55 条における保存するデータの種類を特定しなければならない。

第58条　　本タイプのシステムは、システムの利用登録による利用者本人の明示的な利用意思の表明の機能を設けることを必須とする。

2　センサーから得られた情報を設置施設の現場において、対象者以外の人間（従業員を含む）に開示する場合には、利用登録の際に特に、利用者本人にその旨を説明しておかなければならない。

第59条　　本タイプのシステムを運用する設置事業者は、データの開示請求に原則として応じなければならない。開示するデータは、少なくとも第 57 条において開示した種類のデータ

を、その記録時刻・記録場所とともに含むものとする。

第60条　　本タイプのシステムを運用する設置事業者は、個人データの削除請求を受け付けなければならない。削除請求があった場合、削除しないことに正当な理由がある場合を除き、その請求に原則として応じなければならない。

2　設置事業者は、データの削除請求について、データの削除に応じない可能性を留保する場合には、あらかじめその理由を特定し、利用登録の際に利用者に通知しなければならない。

3　設置事業者は、第 13 条但し書きの各号に該当する場合において、法執行機関等から情報提供の要求を受けている場合または受ける可能性が高い場合においては、前 2 項に関わらず削除請求に応じないことができる。この場合においては、当該のデータについては情報提供以外の目的に利用しないものとする。

第61条　　利用登録の取り消し、データ開示、データ削除に関しては、前 3 条のほか、第 5 節の一般原則に準じる。

第62条　　本タイプのシステムにおいて、第 11 条第 1 項の掲示および第 2 項のサイトには、同条の定めの他、それぞれ以下の情報を含めるものとする。

(ア) 第 1 項の掲示:第 53 条における共有の範囲、第 54 条における紐付けて保存されるデータの保存期間(またはその最大期間)、第 58 条第 2 項に該当するデータがある場合にはその旨、利用登録を受け付ける旨の表記、第 60 条第 3 項に該当する場合にはその旨

(イ) 第 2 項のサイト:第 57 条で特定した情報の範囲、第 58 条第 2 項に該当するデータがある場合にはその該当する情報の範囲、第 60 条第 3 項に該当する場合にはその理由、第 85 条で定める情報の取扱いに関する共通の掲載事項

第 4 節　オプションルール

4．1　設置・調整オプション

第63条　　第 3 節で掲げる各タイプのシステム（以下、「基本システム」という。）には、当該システムを正しく動作させるための設置・調整作業のために、現場で取得する個人特徴情報の内容を確認する機能を設けることができる。当該機能を付加する場合には、本節の各条の規定によらなければならない。

2　当該付加機能は、設置・調整の作業の行われている期間のみ有効になり、通常の運用を行う時点においては有効にできないような仕組みとして実装されなければならない。

> （補足）具体的な仕組みとしては例えば、（1）システム開発事業者および当該事業者から委託された設置担当者のみがシステムの設置される現場で当該機能を有効とでき、設置事業者単独では有効にできないようなシステムや、（2）実運用と当該機能を排他的にしか有効にできないように実装され、当該機能により調整が行われている間は実運用に有効なデータを取得・保存・出力しないシステムなどが考えられる。

第64条　　当該付加機能で収集する人物関連情報は、基本システムにおいて特定し第 11 条で

利用者に周知したセンサーから取得される個人特定情報その他の情報に限る。

2　当該付加機能で収集する人物関連情報の利用者は、基本システムで特定された設置事業者、第 16 条第 1 項で特定した委託データ処理事業者、当該システムのシステム開発事業者および、両者からの委託により設置を担当する事業者等に限る。設置事業者以外のものが情報を利用する場合、設置事業者は当該利用者との間に本ルールを前提とした秘密保持契約の締結を行うか、または納入・設置作業等にかかる契約等に同等の約定を含めておかなければならない。第 16 条第 2 項の再委託の規定は、本条の設置事業者以外からの再委託に準用する。

第65条　　当該付加機能を付加したシステムを設置する設置事業者は、当該機能が有効となる期間中、第 11 条第 1 項における告知に、当該付加機能を使用している旨の追加の告知を行い、当該機能で取得した情報を利用する者、および当該付加機能で収集した情報の最長の保持期間を明示しなければならない。

第66条　　当該付加機能を付加したシステムを設置する設置事業者または当該システムの開発事業者は、当該付加機能が有効となる期間中、当該機能により人物関係情報を取得される個人に対し、システムの概要や取得対象となる情報、取得した情報の取扱いなどにつき十分な説明をできる対応体制を構築しなければならない。

第67条　　当該付加機能により取得された情報（第 11 条第 1 項および第 2 項における各告知に含まれる、基本システムで取得し利用する情報を除く。次条において同じ。）は、基本システムの設置およびその性能の最適化等の調整にのみ用いなければならない。

第68条　　当該付加機能で収集した情報は、その設置調整の作業が終わったとき、また情報の保持期間が第 65 条で告知した期間を経過する前に、全て破棄されなければならない。

4．2　研究開発オプション

第69条　　第 3 節で掲げる各タイプのシステムに付加する、システムおよびその要素技術自体の開発・改善のためのデータ収集に係る付加機能については、別途定める。

2　設置事業者は、この付加機能で収集した情報を利用する者をあらかじめ特定し利用者に告知しなければならない。

3　付加機能で収集した情報は、当該システムが設置された現場とから離れた、当該収集情報の漏洩を防ぐ確実な安全管理措置を施した場所で、当該現場と無関係の人によって行わなければならない。

4　当該付加機能で収集した情報は、データ処理システムおよびその要素技術の改善を除き、他の商業目的に一切用いてはならない。

（補足）本条項については、付録 D に背景説明を別途記載した。
　なお、基本システムの開発に関係しない学術研究機関等（大学など）への提供については、本ルールにおける第三者提供の枠組み（主に匿名加工情報の形による）か、本ルール外での個別の取り決めと利用者への告知による。

４．３　警備オプション１

第70条　　第３節で掲げる各タイプのシステム（以下、「基本システム」という。）には、そのカメラ等を防犯カメラの機能と共用することができる。当該機能を付加する場合には、本節の各条の規定によらなければならない。

２　本節の各条の規定の他、設置箇所に適用される防犯カメラの設置等に関する条例等が存在する場合には、当該条例等の規定にも従うものとする。この場合において、相反する規定がある場合には、当該条例等の規定を優先する。

第71条　　当該機能を付加したシステムを設置する設置事業者は、第 11 条第 1 項および第 2 項における各告知に、本オプションの機能の存在を明示しなければならない。

第72条　　本オプションと共用するセンサーから取得された情報は、その情報処理の可能な限り早期の段階で基本システムから複製され、基本システムとは独立に処理されるものとする。

（解説）本条の規定は、1 つの情報システムに一体のものとして基本システムと警備オプションの各機能を実装する場合と、カメラの画像をアナログ信号等の段階で 2 つに分離し、基本システムを実装した装置と監視カメラ装置のそれぞれに入力する場合の、両方を想定している。

第73条　　本オプションのために取得された画像情報は、個人認識・特定等の処理をすることなく、基本システムの用いない、本機能専用の記録装置に蓄積・保存されるものとする。なお、撮影対象の特定個人毎の特徴等に依存しない、時刻情報の付加、複数カメラ画像の合成、無人と思われる時間帯の記録の除去、映像の圧縮等の処理については、これらを行う事ができる。

２　本オプションを実装するシステムには、現在の画像を蓄積せずに表示するモニタ装置を設けることができる。

第74条　　本オプションのために収集され蓄積された、過去の時点に関する画像の情報は、カメラの撮影対象本人または法執行機関の要請による開示・提供を除き、当該設置施設を代表する権限のある責任者および設置施設の警備等を専ら担当する者の他、何人にも開示・提供してはならない。

２　システムの設置者は、蓄積された情報がみだりに読み出されないよう、適切なアクセス権限ならびにアクセス保護等の設定等をするものとする。

（解説）本条および次条括弧内の限定は、従来型の監視カメラの撮影画像の不適切な使用によるプライバシー被害が現に発生していることを踏まえ、店頭で業務を担当する従業員等、実際の客体と接する可能性のある者による不正アクセスに対する保護を要請するものである。

第75条　　本オプションのために収集され蓄積された情報は、設置施設内およびその付近での事件の検証および、法執行機関からの要請に基づく提供以外に用いてはならない。

２　法執行機関等などからの要請に基づく場合を除いて、本付加機能で記録された情報と、基本システムで記録した情報を同時に単一の目的に用い、あるいはそれらの突合の処理を行ってはな

らない。

（解説）基本システムと警備オプション１の機能の間では一切の情報を共有しない、突合しないことを原則とするが、法執行機関がその両方の情報の提供を要請した場合においては、結果的にこれらの間の突合が起こる可能性を想定し、除外条件を定めている。

４．４　警備オプション２

第76条　　前節に定めるほか、個人を認識する機能等を積極的に用いた警備への応用については、別途検討する。

２　当該機能から得られた情報は、警備以外の目的に一切用いてはならない。

３　当該検討対象の機能の運用は、警備業法に基づく警備会社による運用に限定する、当該付加機能から得られた警備情報の利用担当者と通常の接客等に携わる従業員等を明確に分離する、遠隔による監視対象の絞り込みに用途を限定し、サービス現場の従業員および周囲の他の客等に一切の情報が漏洩しないことを担保するなど、警備・監視対象者のプライバシーに十二分に配慮したものとなければならない。

（解説）本機能については、その技術適用の可能性を踏まえて最低限必要なプライバシー上の要件についての洗い出しを行ったが、その具体的ルールの制定においては、広範な範囲からの意見の聴取など、さらに深い検討が必要と考えられる。

第５節　利用登録、データ開示等に関する共通規定

第77条　　システムの利用登録（オプト・イン）およびその取り消し、利用停止（オプト・アウト）、データ開示、データ削除に関しては、第 3.2 節および第 3.3 節の規定の他、本節の定めによる。

（補足）本節で定めるデータ削除は、自己情報コントロールの観点から定めるものである。従って、法第 27 条に定める「事業者の利用に不正がある場合の利用停止請求」において、本ルールに従っていれば同条の条件を満たしたものと評価・追認する趣旨ではない。

第78条　　利用登録または利用停止の機能を実装するシステムを運用する設置事業者は、利用者からの当該請求や開示・削除請求に適切に応えるために必要な十分な体制を整備しなければならない。

第79条　　利用登録を受けないシステムにおいて、利用停止およびデータ削除の申し出を受け付ける場合においては、悪戯防止などのための必要最低限のものを超えて、氏名・住所等の個人情報を取得してはならない。

２　当該システムにおけるデータ開示の請求に対しては、前項によらず、請求者本人に関する住所など事後の連絡等が可能となる情報の提示を必ず求めなければならない。

（解説）利用登録を受けない形で運営されるタイプ 2 システムなどについては、利用者に対して詳細な情報取得を半ば強制する形で運営されることとなるので、個人プライバシーに結びつく情報の提供を望まない利用者に対して十分な配慮をする必要がある。特に、利用停止の申し出そのものがプライバシー侵害になることや、利用停止の申し出のハードルを上げることによ

り利用停止の希望そのものを忌避させるような状況は、設けてはならない。たとえそのことが取得できるデータの質を著しく下げる場合であっても同様である。
　具体的な申し出の受け方については、可能な限りサービスの現場において本人が簡単に申し出ることで、特徴情報以外の個人情報の取得なしに利用停止の登録が可能にすることが望ましい。例えば、レジでの登録や、特定の通路を通ることで自動的に登録されるなどの方法が考えられる。
　なお、データ開示については悪戯等により他者のプライバシー情報を不正に入手するリスクの方が、本人の申し出を忌避させるリスクより大きいことから、厳格な本人確認や、問題が起こった際の事後監査可能な情報の取得が必要と考えられるため、本条第 1 項の対象から意図的に除外している。

第80条　　システムの利用停止の申し出に関する有効期間および情報の保持期間は、原則として利用停止を行わない場合に情報が保持される期間と同一とする。ただし、その期間が 3 ヶ月を下回る場合においては、下限を 3 ヶ月とし、3 年を上回る場合は、上限を 3 年とする。

第81条　　特徴量以外の個人特定可能な情報を保存しない場合（タイプ 2 システムなど）においては、利用登録およびその取り消し、利用停止、データ開示、データ削除の取扱いを行う場合には、写真や本人などの特徴量抽出が可能な情報の提示をうけ、その特徴量を記録するとともに、その特徴量に紐付けられる匿名 ID に対しそれぞれ下記の取扱いを行うことで、当該取扱いの請求に応えたものとみなす。

（ア）利用停止または利用登録の取消しの請求があった場合には、その旨を記録し、該当する特徴量に該当する情報について、システムの追跡・処理対象から除外する。

（イ）利用登録の請求があった場合には、その旨を記録し、該当する特徴量に該当する情報についてのみ、システムの追跡・処理対象とする。

（ウ）データ開示、データ削除の請求があった場合には、当該特徴量に対応する ID に紐付けられた情報を開示・削除の対象とする。

（解説）センサーによる個人識別は常に特徴量にぶれがあり、低い確率で同一個人を別人と認識したり、別の人物を同一個人と認識したりする可能性があることから、たまたま申し出時の特徴量に対応するデータを利用停止対象として登録・開示・削除しても、正確に本人の全データを対象とできたと 100%確実に言うことはできない。また逆に、本人の申し出がなくても、たまたま他人のデータの削除請求に応えた場合に、自分のデータの一部または全部が同一個人として削除されてしまう可能性がある。このような場合に、特徴量の該当した ID のデータの処理をもって、請求に応えたものとみなす。

第82条　　前条において提供された利用停止（本条において、利用登録の取消しを含む。）のための個人特定情報、個人特徴情報およびその他の個人情報については、当該登録の処理以外には一切用いないものとする。

2　前項の情報および当該登録の申込みの有無に関わる情報については、確実にその申込みの本人であると特定できる者に対する場合を除き、一切第三者に開示・提供しないこととする。

3　設置事業者並びにシステム運用者等の関係者は、前 2 項の情報について、個人の最大限の秘密にかかる情報として、厳重な個人情報保護体制を構築し確実に運用するものとする。

第83条　　特徴量以外の本人特定可能な情報を保存するタイプ 3 システムにおいて、利用登録の申し出の記録が対象個人の特徴量に紐付けされていない場合など、画像取得段階において

対象人物の利用登録の有無を判定できない場合においては、システムはタイプ 1 システムで許容される範囲であらかじめ情報を仮に取得し、当該個人特定情報が提示された時点で、仮に取得したデータと当該個人との紐付けを行うものとする。この場合において、利用登録対象の個人を特定する情報が提示されないことが判明した場合には、直ちに当該の仮に取得したデータを削除するものとする。

2　画像取得段階において対象人物の利用登録の有無を判定できるシステムにおいては、システムは画像取得後ただちにその判定を行い、利用登録のない個人に該当するデータをその後の処理から除外する。この場合においては、画像から取得できる情報は、必ずしもタイプ 1 システムで許容される範囲に限定されない。

3　特徴量以外の本人特定可能な情報を保存するタイプ 3 システムにおいて、データ開示、データ削除の請求があった場合には、提示された本人特定可能な情報に対応する ID に紐付けられた情報を開示・削除の対象とする。

第84条　　設置事業者は、データ開示の請求があった場合には、原則として標準的な情報表現方式に基づく再利用可能な電子データとして開示を行うものとする。ただし、開示されるデータが極めて些少（A4 用紙 1 枚程度）の場合においては、電子データ以外による開示によることができる。

（解説）具体的な開示の情報表現方式については、今後のスマートディスクロージャなどの取り組みの流れにおいて様々な議論が期待されることから、本ルールでは具体的には定めず、「標準的な表現」と定めるに留める。一例として、単なる時刻情報の羅列であればコンマ区切り形式やエクセル形式（OOXML Workbook）などで、人の動きの情報であれば Open Geospatial Consortium の KML 形式の利用などが考えられる（本例示は他のファイル形式の利用を排除しない）。また、開示に用いる媒体については、一般に流通するメディアの他、標準的な暗号化方式（例えば、AES 暗号化された ZIP 圧縮ファイルなど）に基づく電子ファイルの送信と暗号鍵の郵送等による伝達なども考えられる。

2　前項に関わらず、データ開示の請求者が特に希望する場合には、設置事業者は紙媒体による開示を行う事ができる。この場合においては、設置事業者は法令等で許容される範囲において、紙媒体による開示により追加で必要となる費用に相当する手数料を、開示請求者に請求することができる。

第85条　　本節の対象となるシステムについて、第 11 条第 2 項の詳細な情報の公開には第 3 節に定めるもののほか、以下の情報を含めるものとする。

- **利用登録または利用停止の登録を受け付ける旨の表記**
- **記録・開示の対象となるデータの種別**
- **第 80 条に定める利用停止登録の有効期間**
- **利用停止または利用登録の取消しの請求を受け付ける方法の詳細**
- **データの削除請求を受け付ける方法の詳細**
- **データの開示請求を受け付ける方法の詳細**
- **それぞれの請求の際に提供が必要となる個人情報**

・　請求のために提供された個人情報の取扱い・管理・保存等に関する詳細

第 6 節 データ保護その他の規定

第86条　　本ルールを適用するシステムには、各タイプにおいて定めるルールにおいて「情報を開示しない」ことと定められた者について、それらの者によるデータの取得を可能とする機能を実装してはならない。

2　システムには、その他のデータについても、ルールと相反するデータアクセス機能を原則として実装しないものとする。やむを得ずデータアクセス機能を実装する場合においては、その機能を利用できる権限の範囲をシステム管理者など必要最低限に限定するとともに、アクセス者のユーザ認証、アクセスの監査ログの記録など、不正利用を防止する方策を合わせて実装することとする。

（解説）本ルールの条文の多くは、人物関連情報の取扱いを計算機の中に留めることにより、それらの情報の流れをシステム的にコントロールし、人に知られることがないことを保証することを意図したものであり、本条はこのような情報流のコントロールを、システムの実装に具体的に機能として反映することを求めるものである。例えば、個人特徴情報の元となる画像データや、第 34 条・第 45 条で定めるデータを、店頭の端末からアクセスする機能を設けないことにより、誤って従業員にデータがアクセス可能になることや、悪意を持った従業員がデータを閲覧することを防ぐ。

第 2 項の「やむを得ない場合」については、例えば設置作業において一般利用者を撮影対象とせずに行う動作の確認、捜査機関からの情報照会への対応などが相当する。

第87条　　設置事業者（以下本節において、第 16 条による外部委託先等を含む。）は、保有する人物関連情報（個人情報の該非を問わない）について、アクセス可能な者・部署や状況、アクセスの監査の記録方式などを定めた内部ルールをあらかじめ設け、適切に施行する。

第88条　　設置事業者は、保有する人物関連情報の漏洩・滅失・毀損その他を防止するため、安全管理のために必要な内部ルール並びに措置を策定し、適切に施行するものとする。

2　システムは、そのシステムの特定された目的に応じ、不要となった人物関連情報を速やかに破棄するように実装するものとする。

3　システムの実装者は、技術的・コスト的に可能な範囲において、できるだけ秘密分散、暗号化など、一部分の情報漏洩などにより発生する個人情報漏洩を抑える先進的なデータ保護の仕組みの検討・開発と導入に努める。

第89条　　その他、本ルールに準拠するシステムの安全な運用のために各事業者が定める対策基準が、最低限満たすべき安全性の要件については別に定める。

（解説）一定以上の規模の事業者等によるシステムの運用については、既に多くの事業者が十分なレベルの情報セキュリティ管理（ISM）のための基準をそれぞれに定めていると思われ、本ルールに定める情報の流れの制御を、それら既存の基準に従って実装すれば、十分な安全性が得られると考えられるため、本ルールにおいてそれらの基準と重なるところについて詳細なルールを定めることはしない。ただし、そういった基準を備えていない事業者が参入する可能性も踏まえ、最低限必要となる要件については、今後検討が必要と思われる。

付録 A（推奨規定） 店頭掲示に関するガイドライン（草案）

本ルールの第 11 条第 1 項に定める店頭表示については、統一化したアイコン等の表示を用いて、利用者が自らのプライバシーを守るために確認すべき内容をできるだけ少ないものとすることを推奨する。

本ガイドライン草案では、アイコン等の具体的表示を今後検討するために、元となる分類や項目を提示する。

・ 第 1 の表示

カメラ等により人物関係情報を取得するシステムを導入していることと、本ルールを規則として採用していることを表示するアイコンとする。

本アイコンは、例えば商標のように、類似表示等の不正利用に対する法的牽制機能を持つものとすることが望ましいと考えられ、その具体的な方法は今後検討する。

・ 第 2 の表示

センサーの種類と、センサーにより取得する情報の種類を、いくつかの類型に分類して示す。複数に該当する場合、＊の付いた情報については併記し、その他については最下位のものを残して省略する。

「人以外のものに関する情報（棚の在庫など）」

「カメラに写る人数」

「カメラに写った人の属性（年齢等）」＊

「カメラに写った人の動き（動線、振る舞い）」＊

「その他」（具体的な注記を表示する）＊

・ 第 3 の表示

情報を取得する目的を、いくつかの類型に分類して示す。

「今入店する顧客へのサービスの改善（待ち時間の減少等）」

「マーケティング等の統計情報の取得」

「顧客ごとに異なるサービスの提供（カスタマイズ、VIP 対応）」（黄色とする）

「警備・個人認証・監視」（黄色とする）

「その他」（具体的な注記を表示する）

・ 第 4 の表示

人物関連情報を取得し共有する範囲を、いくつかの類型に分類して示す。

「1 つの入り口からなる店舗」

「複数のゾーンからなる一連の施設群」（黄色とし、具体的な注記を表示する）

「相互に離れた場所を含む同一運営による施設群」（具体的な注記を表示する、橙色とする）

「その他」（注記を表示する、橙色とする）

・ 第 5 の表示

本ルール第 3 節に定めるシステムのタイプ別を、表示する。

「タイプ 0」（緑色または、周辺の表示と同色とする）

「タイプ 1」（同上）

「タイプ 2」（黄色とする）

「タイプ 3」（橙色とする）

ただし、タイプ 2 において開示しない情報があるケース、タイプ 2・タイプ 3 で情報の削除の請求に応じない可能性を留保するケースでは、表示は赤色とする。

・ 第 6 の表示

タイプ 2 またはタイプ 3 において、利用登録を受け付ける、または利用停止登録を受け付ける、のいずれかの区別を表示する。（第 5 の表示と同色とする）

・ 第 7 の表示

第 4 節のオプションルールを適用する場合には、当該ルールに対応するアイコンを表示する。

「研究開発オプション」（下記にかかわらず、緑色としない）

「監視オプション１」（下記にかかわらず、緑色としない）

「監視オプション２」（橙色とする）

なお、色の指定の無い表示の色は原則として、白、黒または周辺の表示と同色（緑色を除く）とする。ただし、赤色、橙色、黄色、緑色のいずれかが指定されているアイコンがある場合、表示の全体の色を当該の色（挙げた順に上位の優先順位とする。）とすることができる。

また、第 10 条第 2 項により同一のシステムが 2 つ以上のタイプのシステムを実装する場合には、上記第 1 から第 7 の表示をセットとして、複数列にそれぞれのタイプを表示するものとする。

（例）下線部は必須の表示内容

カメラルールアイコン	動線の追跡	マーケティング	店舗群	タイプ 1	2 次元コード

・ 当本館と向かいの別館を 1 店舗群として一連のお客様の動線を集計します。
・ 取得した情報は、店舗の商品売り場の配置の改善等に利用します。
・ 詳細ページ：https://www.example.com/info/camera-policy.html

カメラルールアイコン	属性の取得	マーケティング	1 店舗	タイプ 2	オプトアウト	2 次元コード

・ 当店舗に来店されたお客様について、顔映像から同一のお客様の再来店を把握し、
その頻度を集計し、商品開発に反映いたします。
・ 取得した情報は、最後のご来店から最長 1 ヶ月保存いたします。
・ 情報の把握を希望されないお客様は、店頭で追跡対象外の登録をいたします。
・ 詳しくは、下記 URL（または右上のバーコード）をご覧下さい。
・ 詳細ページ：https://shop.example.net/about-marketing-system.html

カメラルールアイコン	個人の識別	個別サービス	同一チェーン	タイプ 3	オプト・イン	2 次元コード

・ 当チェーンの「顔パスおなじみさん」サービスに登録された方について、
入店時にカメラでお客様を特定し、お客様ごとの接客をいたします。
・ 登録されていないお客様に関するデータは、一切保存いたしません。
・ 取得した情報は、最後のご来店から最長 1 年保存いたします。
・ 詳しくは、下記 URL（または右上のバーコード）をご覧下さい。
・ 詳細ページ：https://shop.example.net/about-marketing-system.html

付録 B（参考）　説明 Web サイトの表示例

本ルールの第 11 条第 2 項に定める詳細の情報については、利用目的・本ルールを適用する旨・本ルールにおけるタイプ別のほか、各条で定めた内容を簡潔に箇条書きで示すとともに、消費者にとってのメリットやデメリットを分かりやすく提示することとする。また、タイプ 2・タイプ 3 のシステムについては、利用登録または利用停止の手続きならびに削除・開示の手続きについて、その詳細の十分な説明を行うものとする。

各事業者の施設の状況や利用者の種類により適切な表示方法は変わる可能性もあるが、なるべく統一的な表示が望ましいことから、付録 C における適用例に示すような表示を、望ましい表示例として例示する。

付録 C（参考）　ユースケースごとのルール適用例

本節では、WG において議論された、いくつかのユースケースについて、その具体的なタイプ別の適用や、その他の留意事項を参考として示す。

C.1　店舗内の動線把握のために導入するシステム

店舗内に複数のカメラを設置し、人の流れを分析し、匿名の人の流れの束をもとに、動線が錯綜している売り場や、混雑が著しい地点などを把握し、店舗の棚配置の入れ替えなどの検討材料とするシステムを想定する。

・ タイプ別:

入店者それぞれの動線情報を取得し、一方で同一個人の入店を長期間に追跡する必要が無いシステムは、「タイプ 1 システム」として設計するのが最も適切と考えられる。

・ 実装方法の例:

個人情報をなるべく取得しない実装方法として、例えば次のようなものが考えられる。

- カメラから取得した情報からまず 1 カメラの視野の中での人の動きを把握し、それぞれの人について特徴量抽出を行いメモリ（DRAM の主記憶内）に保存する。
- あわせて、カメラ画像範囲内での人の動きのベクトルを検知し、部分的動線の情報を構築する。（この部分だけであれば、タイプ 0 システムに相当する。）
- メモリ内で、同じ特徴の人の情報を関連づけ、10 分間同じ人の検出がなくなった時点で、関連づけた動線情報を出現順に繋いで、当該情報の特徴量を廃棄し、動線情報と取得時刻帯だけをディスク装置に記録する。
- 1 月に 1 回程度、ディスク装置に記録された情報を取りだし、時間帯ごとに店内地図上にプロットし、紙上で検討する。

・ データの取扱いについて:

- 時刻情報付きの動線情報は、単独では匿名の情報と考えられるが、例えば個人情報付きのポイントカードに対応した POS システムを導入している場合には、時刻情報を突合することで、脱匿名化が可能になる可能性がある。そのため、生データでのそのままの取り出しを許す場合には、データの取扱いに関わる者に対し、本ルールに相反しない取扱い規則を事前に定め、遵守させる必要がある。
- 上記の実装例で示したように、さらに動線情報を時間帯で統合して線の密集度で判断させることや、いわゆるヒートマップの形にまで加工してシステムから取り出すようにするなどの実装の工夫により、データの取扱者に対する要求や、安全性へのプレッシャーを大幅に低減することができる。

・ 店頭への掲示について:

- 取得する情報としては、店舗の入り口に「店舗内での人の動き（動線データ）とその時刻」を明示する。取得範囲として、「本店舗内」を明示する。
- 取得目的として、例えば「売り場の配置の改善等」などの表示が考えられる。
- 店頭の掲示は、例えば下記のようなものになる。

カメラルールアイコン	動線の追跡	マーケティング	1 店舗	タイプ 1	2 次元コード

- 当店では、お客様の客層ごとに店舗内での動線を集計します。
- 取得した情報は、店舗の商品売り場の配置の改善等に利用します。
- 本システムの運用は、XYZ 株式会社に委託しています。
- 詳細ページ：https://www.example.com/info/camera-policy.html

・ Web ページでの告知は、例えば以下のようなものになる。

カメラによるマーケティング情報の取得について

当店では、店舗内でのお客様の動きをカメラを用いて分析し、店舗の棚配置等の改善のために利用しております。取得した情報については、お客様のプライバシーを保護するため、「カメラ利用に関する業界ルール（仮称）」に基づき、同ルールの「タイプ 1 システム」として、以下の通りの取扱いをしております。

1．情報取得の方法： 天井設置のカメラ 16 台
　当該カメラには、「マーケティング用」の表示をしております。
2．取得の目的： お客様の流れの滞留箇所などを把握し、商品の配置の改善や、通路幅

の検討の材料にいたします。
３．取得・保存するデータ：　お客様の１回の当店ご利用の、入店からの一連の移動経路と、年齢層（10 歳単位）・性別の推定情報、取得時刻。
４．動線データの取得範囲：　××店店内に限る。
５．データの取得主体：〇〇スーパー株式会社　××店
東京都芝区三浦０丁目４番７号　　TEL: 03-9999-0000
６．データ処理の委託先：XYZ 株式会社
東京都山手区港南台０丁目２番１号 2048
弊社と当該委託先の間には、秘密保持契約を締結しております。

なお、個人情報についてはその保護のため、顔等の画像については取得せず、お客様を特定できる特徴などについても、お客様のお帰り後 10 分で自動削除し、一切の保存をしないシステムとしております。詳しくは、下記までお問い合わせください。
〇〇スーパー株式会社　お客様相談係
東京都芝区三浦０丁目１番１号　　TEL: 03-8888-0000

C.2　店舗内のリピート客追跡により、新規客数とユニーク客数の把握のために導入するシステム

本節では、入店された顧客の来店頻度を分析し、初来店者と繰り返し来店者の人数を把握することにより、商品構成などの検討材料とするシステムを想定する。

・ タイプ別:
リピート客の把握のためには、個人を特定できる特徴を複数回の来店にまたがってシステムに保存し利用する必要があるため、最低限「タイプ 2 システム」に該当する。一方、情報の解析について、本件では店頭に置いて直ちに再来店と初来店を区別する必要は無く、現場である店頭にいる従業員等に、その判定結果を知らせる必要は無い。このような場合には、「タイプ 2 システム」に該当するものとして設計するのが最も適切と考えられる。
・ 特定すべき内容:
第 3.2 節の規定により、取得・保存する情報とその目的のほか、データの保持期間をあらかじめ特定する必要がある。
- 取得する情報として「来店者の客層と人数」を、取得範囲として、「1 店舗内」を明示する。
- 取得目的として、例えば「来店人数・リピート客の分布の把握」などを表示する。
- データの保持期間として、例えば第 42 条の 2 つの手法のうち(イ)を選び、「最後の来店から 1 ヶ月以内」と定める。この場合、最短ではデータが 1 ヶ月以下で削除されることになるが、月 2 回程度来店する場合には、保持期間が繰り返し更新されることになる。

・ 本ルール上、オプトアウトへの対応が求められることになる。対応方法はいくつか考えられる

がここでは、店頭でオプトアウトの申し出があったお客様について、店員の操作により登録をすることにする。その旨を、丁寧に説明する必要がある。

・ 店頭の掲示は、例えば下記のようなものになる。

カメラ ルール アイコン	属性の 取得	マーケ ティング	1 店舗	タイプ 2	オプトア ウト	2 次元 コード

・ 当店舗に来店されたお客様について、顔映像から同一のお客様の再来店を把握し、
その頻度を集計し、商品開発に反映いたします。
・ 取得した情報は、最後のご来店から最長 1 ヶ月保存いたします。
・ 情報の把握を希望されないお客様は、店頭で追跡対象外の登録をいたします。
・ 詳しくは、下記 URL（または右上のバーコード）をご覧下さい。
・ 詳細ページ：https://shop.example.net/about-marketing-system.html

・ Web ページでの告知は、例えば以下のようなものになる。

カメラによる情報の取得と個人情報の保存について

当店では、来店されたお客様の顔特徴を取得し、新規のお客様と繰り返し来店いただくお客様の人数の比率などを把握しております。取得した情報については、「カメラ利用に関する業界ルール（仮称）」に基づき、同ルールの「タイプ 2 システム」として、以下の通りの取扱いをしております。

1．情報取得の方法： 入り口天井設置のカメラ 1 台
当該カメラには、「マーケティング用」の表示をしております。
2．取得の目的： 来店客のリピート比率の把握・解析によるサービス改善
3．取得・保存するデータ： お客様の顔映像から取得させていただく識別用の匿名の特徴データ、ご来店の時刻。
4．個人データの保存期間： お客様ごとに、システムの把握する最後のご来店から 1 ヶ月間保存します。
5．データの取得主体：〇〇スーパー株式会社 △△店
東京都芝区三浦 3 丁目 3 番 3 号 TEL: 03-9999-0000
6．データ処理の委託先：XYZ 株式会社
東京都山手区港南台 0 丁目 2 番 1 号 2048
弊社と当該委託先の間には、秘密保持契約を締結しております。

なお、個人情報についてはその保護のため、顔等の画像については一切保存しておりません。お客様を特定できる特徴などについては、厳重に管理の上、保持期間後は直ちに削除いたします。詳しくは、下記までお問い合わせください。

〇〇スーパー株式会社 お客様相談係

東京都芝区三浦 0 丁目 1 番 1 号　　TEL: 03-8888-0000

個人の行動データの取得を希望されないお客様へ

行動データ（再来店の頻度）のシステムでの取得を希望されないお客様につきましては、店頭でのお申し出に基づき、追跡対象外（オプト・アウト）の登録をさせていただきます。その際、誠に恐縮ですが、顔画像の特徴を登録させていただき、システムでその後の把握から自動的に除外いたします。

追跡対象外の登録は、登録後 12 ヶ月有効とさせていただき、その間は厳重にデータを管理いたします。登録の有無につきましては、法令に基づく要請を除き、どなたにも開示いたしません。

また、データの削除を希望されるお客様についても、同様に店頭で対応いたします。

ご希望のお客様は、レジにてお申し付けください。

情報開示の請求について

情報の開示をご希望される方につきましては、上記３．で取得する、来店の時刻の記録について、電子データとして開示をいたします。

開示請求の際には、お客様の住所・氏名等のほか、開示対象データの検索のため、顔の写真データの提供をお願いしております。提供頂きました情報は、開示の手続きのほか、一切他の用途に利用せず、個人情報として厳重に管理いたします。

詳しくは、上記問い合わせ先までご連絡ください。

C.3　ポイントカード代わりに、「顔パスおなじみ様」サービスを導入するケース

・ タイプ別：リピート客の把握にともない、店頭でそのお客様ごとに異なるサービスを提供する本システムは、「タイプ 3 システム」に該当する。

・ このようなシステムでは、個別の合意によるオプト・インが義務づけられる。

・ 取得する情報として、「来店者の客層と人数のみ」を明示する。

・ 取得目的として、例えば「来店人数・リピート客の分布の把握」などを表示する。

・ 取得範囲として、「本店舗内」を明示する。

・ 店頭の掲示は、例えば下記のようなものになる。

カメラ ルール アイコン	個人の 識別	個別 サービス	同一 チェーン	タイプ 3	オプト・ イン	2 次元 コード

・　当チェーンの「顔パスおなじみさん」サービスに登録された方について、入店時にカメラでお客様を特定し、お客様ごとの接客をいたします。

・　登録されていないお客様に関するデータは、一切保存いたしません。

・　取得した情報は、最後のご来店から最長 1 年保存いたします。

・　詳しくは、下記 URL（または右上のバーコード）をご覧下さい。

・　詳細ページ：https://shop.example.net/about-marketing-system.html

・ Web ページでの告知は、例えば以下のようなものになる。

カメラによる情報の取得と個人情報の保存について

当店では、「顔パスおなじみさんサービス」を利用されるお客様のため、来店されたお客様の顔特徴を取得し、利用登録された方については、自動的に再来店頻度によるサービスなどの提供をしております。取得した情報については、「カメラ利用に関する業界ルール（仮称）」に基づき、同ルールの「タイプ 3 システム」として、以下の通りの取扱いをしております。

１．情報取得の方法：　入り口天井設置のカメラ 1 台
　　当該カメラには、「マーケティング用」の表示をしております。
２．取得の目的：　サービスに登録されたお客様の特定
３．取得・保存するデータ：　お客様の顔映像から取得させていただく特定用の特徴データ、過去のお客様のご注文等の履歴、ご来店の時刻。
４．個人データの保存期間：　登録されたお客様についてのみ、お客様ごとに、システムの把握する最後のご来店から 1 年間保存します。
５．データの取得主体：〇〇居酒屋　△△店
　　東京都江南区四ツ木 4 丁目 2 番 0 号　　TEL: 03-9999-0000
６．データ処理の委託先：XYZ 株式会社
　　東京都山手区港南台 0 丁目 2 番 1 号 2048
　　弊社と当該委託先の間には、秘密保持契約を締結しております。

個人情報についてはその保護のため、顔等の画像については一切保存しておりません。なお、ご登録をいただいていないお客様の映像につきましては、取得・判別後、直ちに削除しております。お客様を特定できる特徴などについては、厳重に管理の上、保

持期間後は直ちに削除いたします。詳しくは、下記までお問い合わせください。

〇〇居酒屋 △△店

東京都江南区四ツ木４丁目２番０号　　TEL: 03-9999-0000

個人の行動データの取得を希望されないお客様へ

当店では、事前に利用を希望された方以外については、一切の情報を保存しておりません。また、利用の中止を希望されるお客様、保存中のデータの削除を希望されるお客様については、店頭で対応いたします。

ご希望のお客様は、レジにてお申し付けください。

情報開示の請求について

情報の開示をご希望される方につきましては、上記３．で取得する、来店の時刻および過去の購入履歴について、電子データとして開示をいたします。

開示請求の際には、本人確認資料のほか、利用登録時にご提示いただいたポイントカードを確認させていただきます。提供頂きました情報は、開示の手続きのほか、一切他の用途に利用せず、個人情報として厳重に管理いたします。

詳しくは、上記問い合わせ先までご連絡ください。

なお、利用登録をされていないお客様につきましては、保存しているデータは一切ございません。

付録Ｄ（参考）　タイプ２システムとリピーター分析および再来店者把握に関する補足

画像情報を利用した顧客サービスの改善の目的において、リピーター分析の一環として、高い頻度で商業施設等に来客されるお客様に対し、積極的な声がけ等による接客の差別化を図りたいという需要がしばしばあるという分析がなされた。このようなシステムを実現する形態として、タイプ 2 のような事前登録を行わないシステムと、タイプ 3 のような事前登録をベースとしたシステムの 2 つの形態が考えられ、それぞれの文脈で具体的な安全確保のためのルールの検討を行った。

しかしながら、特にタイプ 2 のような事前登録無しでの利用に際しては、「過去の再来店記録に、店員に知られたくない情報が含まれていないことを保証できない」「現時点において、過去の再来店記録を知られたくない他人が近傍にいないこと」の 2 条件を確実に実現できるような、利用形態の詳細な制限の方法を明らかにできないことが、検討の段階でわかった。特に、診療所・薬局・美容など、いくつかの「高リスク」とわかる情報があることが明らかになった一方で、この情報が含まれていなければ問題ない、と

いう境界線をルールとして定義できないことが明らかになってきた。

個人情報保護法などの本ルールの上位規則が基本的には「守っていなければNG」「守っていてもOKとは限らない」という必要条件を定めているのと異なり、本ルールの性格は、「（ルールを悪用する意思がない前提下で）守っていれば、ある程度安全で、顧客に説明可能なシステムになっている」という、十分条件の参考になることも意図している。そのような文脈で、本人同意なしに過去の行動履歴を開示できる限界をルール中で具体的に定めることは、現時点で社会的合意が得られないと判断された。

このような観点から、現時点のルールとしては、再来店者であることを店員に本人同意無しに通知することは、タイプ2・タイプ3ともに実現できないような形で定めることになった。そのようなルールの下でも、再来店者へのサービス差別化を実現したい場合に取りうる手法として、ワーキンググループ中で下記の複数のサービス形態が議論された。

・ 記名の会員カードなどを発行し、登録手続きの中で再来店者へ提供するサービスを明示する。
・ 無記名の会員カード等を登録無しに一旦配布し、Web などで改めて利用登録をする際に、撮影画像によるサービスへの承諾を取得する。
・ スマートフォン等にアプリなどを登録し、本人しか見ない携帯電話の画面に情報を通知する。

このような手法はいずれも、基本的には本ルールのタイプ 3 として運用が出来るものであり、本人同意に基づくきめ細かいサービスを、店頭での登録対応等の負荷を現状から著しくあげることなく実現ができると考えられる。特に、匿名の運用であっても、タイプ 3 の情報としてカード等と紐付けることは、退会・情報削除などへの対応についてもタイプ 2 より格段に容易に行うことができるため、安全性や社会的信頼の面からも有用であると考えられる。

タイプ 2 での運用の要望については、今後社会的に利用の限界に関する合意が醸成された後に、改めて検討することが妥当と考えられる。

付録 E（参考）　研究開発オプション（第 69 条）に関する補足

カメラ画像と画像認識を用いたシステムにおいては、その撮影対象である利用者等に対するサービスの改善等の主目的の他にも、設備の設置・調整における動作状況の確認や、画像認識そのものの精度改善や運用状況の評価など、システムの運用において二次的に発生する画像の利用が存在する。このうち、現場で直ちに情報を利用し、限られた時間だけ情報を目視等で確認することの必要な設置・調整作業については、第 4.1 節で「設置・調整オプション」として整理した。

一方で、人工知能技術、特にフィードバックに基づく継続的な学習に基づき日々強化されるような認識システムが発展してきたことを踏まえると、システムを開発したシステム開発ベンダ等が設置事業者からセンサー情報の提供を受け、認識精度向上などの学習フィードバックに活用するケースも、今後技術トレンドとしては想定される。このような利用については、本ルール第 3 節の各タイプで定めるような利用形態の制限による安全性の確保よりは、データそのものを直ちに現場から引き離し、システムベンダの開発部・データセンターなど、ISMS などによる安全確保措置が万全に執られた閉鎖的な場所において、現場の顧客を知り得ない他人によって解析を行うことにより、時間的・空間的および「人物的」に情報を隔離することが、安全確保の有効な手段の 1 つとして考えられる。今回のルールの検討の段階においては、この考え方に基づき、一旦は「研究開発オプション」という形で具体的なルールの形に整理を行った。

しかし、その後の議論の中で実際の商業現場への展開方法を議論する中で、現時点では特に事業者間での秘密保持や責任分界のありかた、顧客への説明の方法や分担など、実展開へ向けた議論と合意形成が十分に進んでおらず、具体的に即適応が可能なレベルでのルールを定めることは、技術を採用する設置事業者等に対するメッセージとして時期尚早であるとの結論に達した。そのため、今回本ルール（第 69 条）では最低限の要求事項を列挙するに留め、今後継続的に検討すべき課題と整理することにした。一方で、検討の段階で整理した、最低限必要と現時点で考えられる取扱いのルールについては、参考として下記に条文案を掲載する。

E.1　当該付加機能で収集する人物関連情報は、基本システムにおいて特定し第 11 条で利用者に周知したセンサーから取得される個人特定情報その他の情報に限る。

E.2　当該付加機能を付加したシステムを設置する設置事業者は、第 11 条第 1 項および第 2 項における各告知に、当該付加機能の存在と、収集した情報の最長の保持期間を明示しなければならない。

E.3　当該付加機能で収集した人物関連情報は、あらかじめ特定した外部のシステム開発者等（基本システムの開発に関係する者に限る。以下、「システム開発事業者」という。）に提供することができる。この場合、設置事業者は当該システム開発事業者等との間に本ルールを前提とした秘密保持契約を締結するほか、本則第 65 条**エラー! 参照元が見つかりません。**の告知に、当該情報の提供先を明示しなければならない。

E.4　特定の人物に係る個人特徴情報を元に、複数箇所・複数回の同一人物の行動を認識する技術を開発する場合には、基本システムに利用登録または利用停止の機能を実装し、当該システムでデータの取得を行わないことを希望する利用者の情報を、本オプション機能の収集から除かなければならない。

E.5　当該付加機能で収集した情報を用いて行う研究開発は、当該基本システムが設置された現場と異なる場所で、当該現場と無関係の人によって行わなければならない。

E.6　当該付加機能で収集した情報を用いて行う研究開発の場所においては、入退室の管理、情報の隔離システム等、当該収集情報の漏洩を防ぐ確実な安全管理措置を取らなければならない。
2　前項の安全管理措置にかかる基準の詳細は別に定める。

E.7　当該付加機能で収集した情報は、設置事業者および第 66 条で特定したシステム開発事業者以外に提供してはならず、データ処理システムおよびその要素技術の改善を除き、他の商業目的に一切用いてはならない。
2　機械学習等の要素技術の改善に当該付加機能で収集した情報（この節で「学習元データ」という。）を用い、その情報を用いて改善された技術を外部に提供する場合、その提供技術には、学習元データそのものおよび当該情報を取得した場所・日時が特定可能となる情報、ならびにある人物が学習元データに含まれるか否かを通常の方法で識別できる情報が含まれていてはならない。

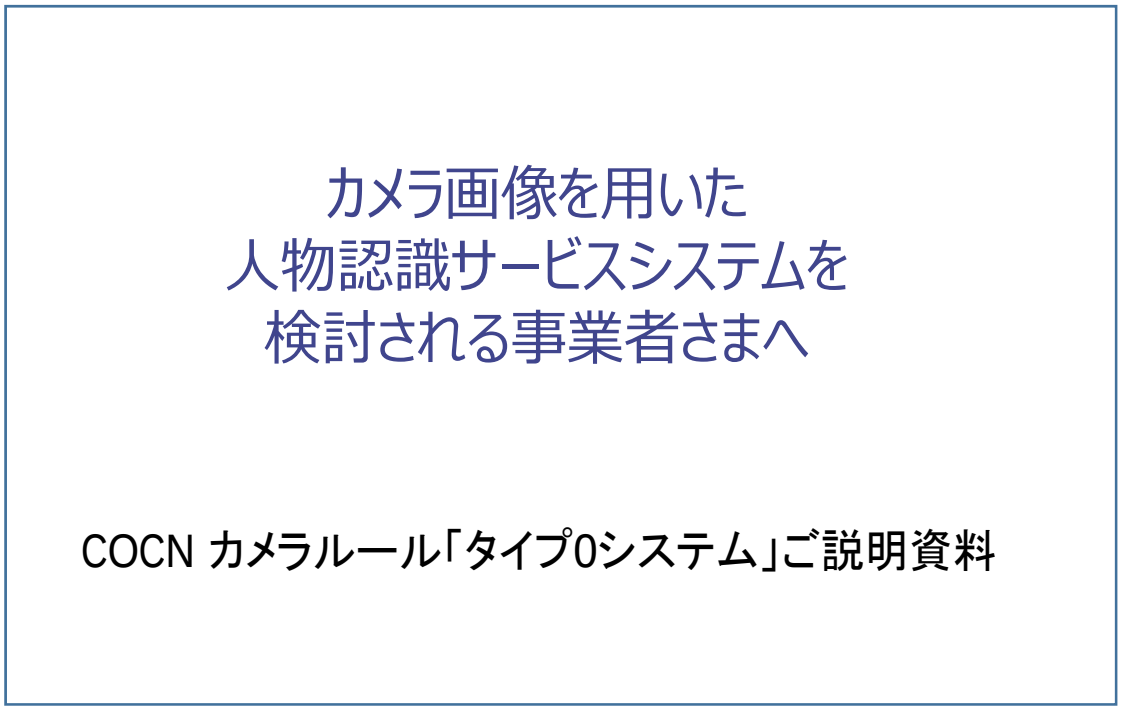
（解説）例えば、収集データを用いてニューラルネットワークを用いた強化学習に用いる場合、通常の手法で十分に多くのデータを用いて学習させた結果のみを用いるケースでは、学習元となる個別のデータの復元は一般には困難であると考えられるが、特異的なデータを含めて常に元データを復元不可能であることを厳密に保証することは困難である。
　そのため、本項では、新たな人物データが過去の学習対象と同一であったか否かを判別できないことを基本的な条件として求めるとともに、万が一過去の学習対象であったことが発見された場合においては、その学習の日時や場所が特定できないことを要求することにした。具体的には、複数業種の十分に多い場所から集めたデータを混合して学習させる方法などが考えられる。将来の方向性としては、本項で求める復元・識別が不可能なことを情報論的手段などにより保証する機械学習結果の評価技術などが開発されることが期待される。

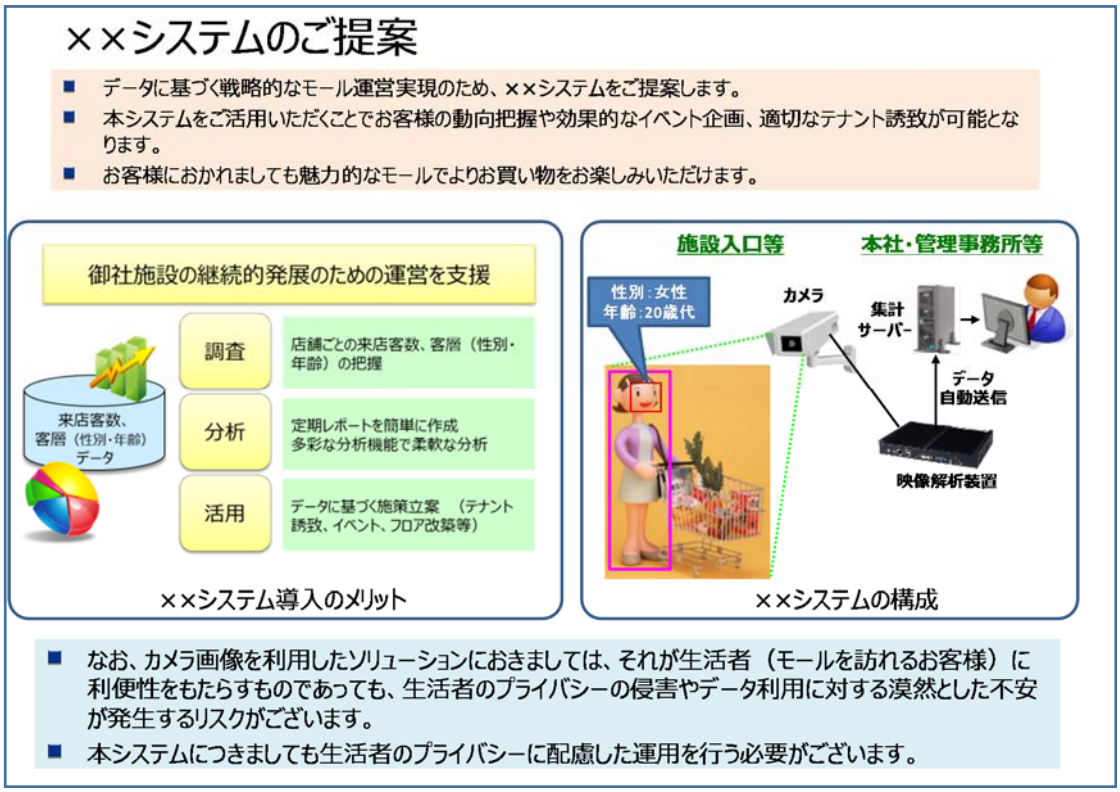
E.8　当該付加機能で収集した情報は、その研究開発が終わったとき、また情報の保持期間が E.2 並びに本則第 65 条で告知した期間を経過する前に、全て破棄されなければならない。

9.　ショッピングモールにおけるカメラ画像利活用のための説明ツール

本ツールはショッピングモールでのカメラ利用に於いてモール運営者がテナントや利用者（顧客）等への配慮事項を共有するために事業者が活用することを目的に検討を行った。

9.1.　タイプ 0





個人情報の保護およびプライバシーへの配慮について

カメラ画像の利用に関しては「カメラ画像利活用ガイドブック」(※1)に基づき、映像ソリューション提供各社および各機関(※2)が共同で「カメラ画像の商用利活用ルール」を策定しております。

「カメラ画像利用ルール」に基づいたシステム構築およびデータの取り扱いにより、お客様に対する個人情報保護法の遵守とプライバシー保護への配慮ができるものと考えております。

本提案のシステムにおいて、「カメラ画像利用ルール」が定める禁止事項

- カメラ映像を取得後すぐに属性情報に変換するとともに、個人が特定できる画像は破棄し、保存しない（第18条）
- 変換した属性情報は年齢・性別の推定情報や服装など「人間が容易に知覚できる情報」に限る（第20条）
- 複数のカメラを跨ぐ同一人物の追跡はしない（第19条）
- 取得した属性情報は他の個人を特定する情報と突合しない（第22条）
- システムの利用登録、利用停止のための個人特定機能は実装しない（第23条）
- 個人の特定を前提とした自己情報開示・自己関連データ削除機能は提供しない（第24条）
- 一定の要件を満たすことなく人物関連情報を第三者に提供しない（第25条）

本提案のシステムにおいて、「カメラ画像利用ルール」が定める許可事項

- 本システムで取得した個人属性情報とカメラ映像以外から取得した個人を特定しない情報（販売した物品等のサービス情報など）を紐付けて利用することができる（第21条）

（参考）「カメラ画像利活用ガイドブック」が推奨する配慮事項

- **基本原則**： データのライフサイクル(※3)を定めると共に、各工程におけるリスク分析を適切に実施することなど
- **事前告知等の配慮**： カメラ画像の撮影及び利活用を開始する場合、事前に十分な期間を持って事前告知を行うことなど
- **取得時の配慮**： カメラ画像の撮影及び利活用の運用中において、取得する内容及び利用目的の通知を行うことなど
- **取り扱い時の配慮**： 利活用に必要なデータを生成した後、カメラ画像は速やかに破棄することなど
- **管理時の配慮**： カメラ画像や抽出したデータに関する適切なセキュリティ対策および第三者への提供条件など

(※1)「経済産業省 IoT推進コンソーシアム」が、カメラ画像利活用に関して事業者が生活者に配慮すべき事項を整理して公開したガイドブック
(※2)「一般社団法人 産業競争力懇談会（COCN）IoT時代のプライバシーとイノベーションの両立」 参画各社
(※3) データの取得から加工、利用、廃棄までの流れを表す概念

本システムの運用管理ご検討のお願い

モール運営管理者様にて、お客様の個人情報保護およびプライバシーに配慮した本システムの運用管理をご検討頂きたく存じます。

データの管理（第6条）

- 本システムに関係した個人情報が故意ないし事故により外部に流出しないよう適切な管理と監査を行ってください
- 本システムにかかわる個人情報を取り扱う情報システム運営者に対し、情報漏えいを防ぐための適切な管理体制の構築をお願いしてください

お客様への通知（第11条）

- 本システムの運用を開始前に十分な期間をもって事前通知を行うと共に、システムの運用中につきましても通知を行ってください
- 通知は入り口やカメラ設置場所付近での物理的な方法（ポスター掲示やパンフレット配布）および電子的な方法（御社HP等）で行ってください
- 提示する情報は例えば下記としてください
  1. カメラで人物の属性情報等を取得している旨と取得の目的
  2. お客様に対するメリット
  3. 運用実施主体の名称および連絡先
  4. カメラの設置位置および撮影範囲

目的外利用の制限

- 一部の例外を除き、カメラ画像等の個人を特定できる情報や個人属性情報等をお客様に通知した範囲を超えた利用を行わないでください（第13条）
- 一部の例外を除き、カメラ画像等の個人を特定できる情報や個人属性情報等をお客様に通知した範囲を超えて第三者への提供を行わないでください（第14条）
- 一部の例外とは下記に該当するものです
  1. 利用範囲の変更についてお客様本人から個別の同意を取得した場合
  2. 法令に基づく義務を履行する、または法令に基づき法執行機関および行政機関の請求または協力の要請があった場合
  3. その他、個人情報保護法第16条第3項に定める理由に該当する場合

テナントとの契約

- カメラ画像等の個人を特定できる情報や個人属性情報等を各テナントに提供する場合は、共有する情報や範囲とその取り扱いに関する契約を結んでください

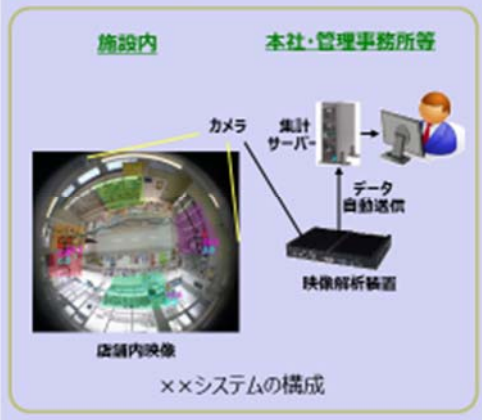
9.2.　タイプ 1

カメラ画像を用いた
人物認識サービスシステムを
検討される事業者さまへ

COCN カメラルール「タイプ1システム」ご説明資料

××システムのご提案

- データに基づく戦略的なモール運営実現のため、××システムをご提案します。
- 本システムをご活用いただくことでお客様の動向把握や効果的なイベント企画、適切なテナント誘致が可能となります。
- お客様におかれましても魅力的なモールでよりお買い物をお楽しみいただけます。



- なお、カメラ画像を利用したソリューションにおきましては、それが生活者（モールを訪れるお客様）に利便性をもたらすものであっても、生活者のプライバシーの侵害やデータ利用に対する漠然とした不安が発生するリスクがございます。
- 本システムにつきましても生活者のプライバシーに配慮した運用を行う必要がございます。

個人情報の保護およびプライバシーへの配慮について

- カメラ画像の利用に関しては「カメラ画像利活用ガイドブック」(※1)に基づき、映像ソリューション提供各社および各機関(※2)が共同で「カメラ画像利用ルール」を策定しております。
- 「カメラ画像利用ルール」に基づいたシステム構築およびデータの取り扱いにより、お客様に対する個人情報保護法の遵守とプライバシー保護への配慮ができるものと考えております。

本提案のシステムにおいて、「カメラ画像利用ルール」が定める禁止事項

- カメラ映像を取得後、追跡に必要な個人特徴情報以外の個人特徴情報は速やかに破棄し、保存しない（第28条）
- 取得した個人特徴情報および人物行動情報は、単一の施設内でのみ使用し、他の情報とは共有・突合しない(第29条)
  個人特徴情報は、システム毎に定める時間(24時間以内)で破棄する(第30条)
- 取得する属性情報は年齢・性別の推定情報や服装など「人間が容易に知覚できる情報」に限る（第31条）
- 取得した属性情報は他の個人を特定する情報と突合しない（第33条）
- 取得した特定の対象者の情報は、統計的な利用を除き、対象者本人以外に開示しない(34条)
- システムの利用登録、利用停止のための個人特定機能は実装しない（第35条）
- 個人の特定を前提とした自己情報開示・自己関連データ削除機能は提供しない（第36条）
- 人物関連情報を第三者に提供しない（第37条）

本提案のシステムにおいて、「カメラ画像利用ルール」が定める許可事項

- 本システムで取得した個人属性情報・個人行動情報とカメラ映像以外から取得した個人を特定しない情報（販売した物品等のサービス情報など）を紐付けて利用することができる（第32条）

（参考）「カメラ画像利活用ガイドブック」が推奨する配慮事項

- **基本原則：** データのライフサイクル(※3)を定めると共に、各工程におけるリスク分析を適切に実施することなど
- **事前告知等の配慮：** カメラ画像の撮影及び利活用を開始する場合、事前に十分な期間を持って事前告知を行うことなど
- **取得時の配慮：** カメラ画像の撮影及び利活用の運用中において、取得する内容及び利用目的の通知を行うことなど
- **取り扱い時の配慮：** 利活用に必要なデータを生成した後、カメラ画像は速やかに破棄することなど
- **管理時の配慮：** カメラ画像や抽出したデータに関する適切なセキュリティ対策および第三者への提供条件など

(※1)「経済産業省 IoT推進コンソーシアム」が、カメラ画像利活用に関して事業者が生活者に配慮すべき事項を整理して公開したガイドブック
(※2)「一般社団法人 産業競争力懇談会（COCN）IoT時代のプライバシーとイノベーションの両立」 参画各社
(※3) データの取得から加工、利用、廃棄までの流れを表す概念

本システムの運用管理ご検討のお願い

- モール運営管理者様にて、お客様の個人情報保護およびプライバシーに配慮した本システムの運用管理をご検討頂きたく存じます。

データの管理（第6条）

- 本システムに関係した個人情報が故意ないし事故により外部に流出しないよう適切な管理と監査を行ってください
- 本システムにかかわる個人情報を取り扱う情報システム運営者に対し、情報漏えいを防ぐための適切な管理体制の構築をお願いしてください

お客様への通知（第11条）

- 本システムの運用を開始前に十分な期間をもって事前通知を行うと共に、システムの運用中につきましても通知を行ってください
- 通知は入り口やカメラ設置場所付近での物理的な方法（ポスター掲示やパンフレット配布）および電子的な方法（御社HP等）で行ってください
- 提示する情報は例えば下記としてください
  1. カメラで人物の属性情報等を取得している旨と取得の目的
  2. お客様に対するメリット
  3. 運用実施主体の名称および連絡先
  4. カメラの設置位置および撮影範囲

目的外利用の制限

- 一部の例外を除き、カメラ画像等の個人を特定できる情報や個人属性情報等をお客様に通知した範囲を超えた利用を行わないでください（第13条）
- 一部の例外を除き、カメラ画像等の個人を特定できる情報や個人属性情報等をお客様に通知した範囲を超えて第三者への提供を行わないでください（第14条）
- 一部の例外とは下記に該当するものです
  1. 利用範囲の変更についてお客様本人から個別の同意を取得した場合
  2. 法令に基づく義務を履行する、または法令に基づき法執行機関および行政機関の請求または協力の要請があった場合
  3. その他、個人情報保護法第16条第3項に定める理由に該当する場合

テナントとの契約

- カメラ画像等の個人を特定できる情報や個人属性情報等を各テナントに提供する場合は、共有する情報や範囲とその取り扱いに関する契約を結んでください

9.3. タイプ 2

カメラ画像を用いた
人物認識サービスシステムを
検討される事業者さまへ

COCN カメラルール「タイプ2システム」ご説明資料

本資料の目的

- 顔認証装置などの人物特定技術を用いた顧客情報サービスの
  システム開発・導入を検討されている事業者さまに、
  実際のシステム開発の検討・打ち合わせのためのご参考に、
  COCN カメラルールの基本的な考え方をご説明します。

COCN カメラルール「タイプ２」とは

顔認証などの個人を識別する装置を用いてお客様を識別し、
ご来店の頻度や店内での動きなどを記録した上で、

- 来店者のリピート状況を匿名状態で把握し店舗運営に利用したり
- そのお客様本人のみが知りえる範囲でマーケティングに活用。

タイプ2システムの例：

- 販促がどれだけ再来店につながっているかの効果検証のためにリピーター情報取得
- 一定期間の来店者数の実人数をカウントする（同一人物の重複カウントの削除）

（ご参考）COCNカメラルールの「他のタイプ」

- タイプ0
  - お客様を個人単位で識別せず、年齢・性別等の基本的な属性や棚前等狭い範囲での動きのみを把握するタイプ
- タイプ1
  - お客様を個人単位で識別せず、複数カメラの広い範囲に渡って短時間お客様を追跡して、動線等を把握し、統計的に利用するタイプ
- タイプ3
  - 事前同意を前提にお客様の顔特徴データと個人情報を紐づけ、お客様のご来店頻度や店内での動きなどを記録したうえで、マーケティングを行うか、店員等に知らせお客様にその場で直接働きかけを行うタイプ

事業者様にお願いすること

- 個人情報取得と運営の主体の特定（7～8p）
- 取得する個人情報と取得パターンの決定（9～11p）
- お客様へのご説明方法の検討（12～13p）
- 取得した情報の取扱いについて（14～15p）
- お客様からの退会等の対応方法の検討（16p）
- お客様への情報開示のご検討（17p）
- 個人情報管理の内部統制にかかるご検討（18p）

個人情報取得と運営の主体の特定（1）

まず、お客様との関係において、「誰が」情報を取得するのかを明らかに特定する必要があります。

- 個人情報管理や苦情処理等の主体となります。
- 取得した情報を共有できる範囲にも影響します。

- 基本的に、「取得した情報を最も利用する方」が主体になります。
  - 多くの場合、実際にお客様にサービスを直接提供する方が該当します。
  - カメラを設置した（設置費用を負担した）者と同一である必要はありません。
  - モールとテナントのような関係性がある場合、どちらが主体になるかご検討下さい。
    - 共同で主体になることも可能ですが、他テナントとの関係などもご配慮下さい。
  - フランチャイズのケースでは、個店・ブランドのどちらが表に立つかもご検討下さい。

個人情報取得と運営の主体の特定（2）

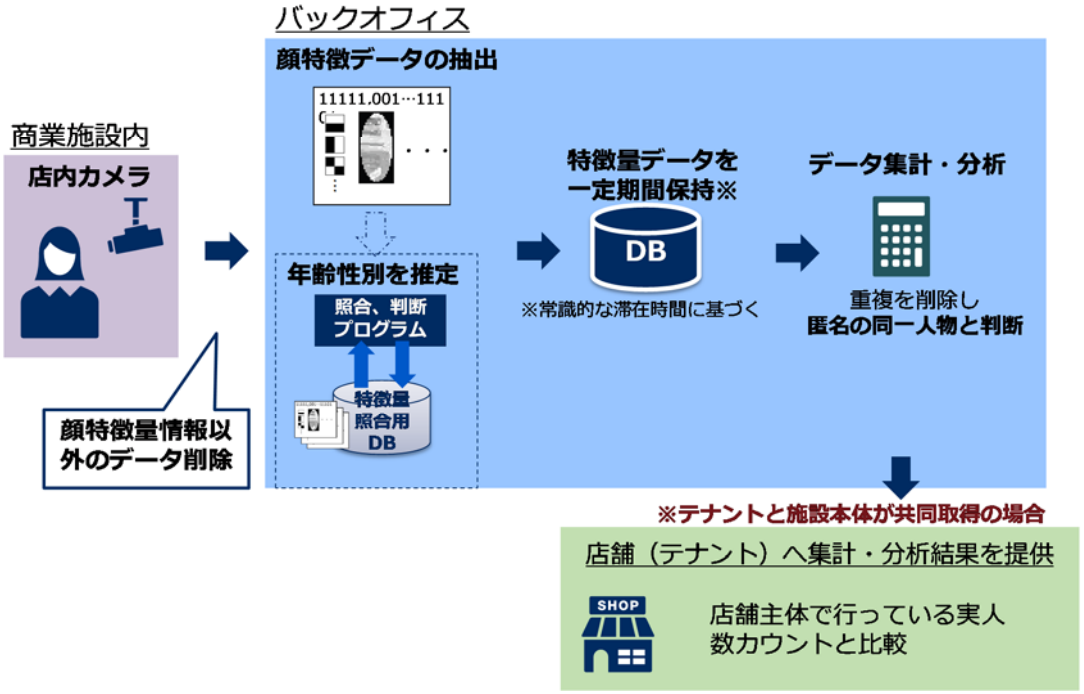
お客様との関係の運営主体とは別に、
実際のシステム運営は別の事業者に委託することができます。

- 委託先には、御社との間に守秘義務契約を締結して頂きます。
- （1次）委託先は、お客様へのご説明において明示することになります。
- 委託先は、貴社のサービス以外には取得情報を利用できません。
- 苦情受付の窓口業務等も委託できますが、
  最終的な責任はあくまで貴社にあることが前提となります。

「タイプ2システム」の主なパターン

- 実人数のカウント
  - ①複合商業施設に入場したユニークユーザー数を複合商業施設がカウントする。
  - ②複合商業施設に入場したユニークユーザー数を性・年齢別に複合商業施設がカウントする。
  - ③店舗に入店したユニークユーザー数を店舗がカウントする。
  - ④店舗に入店したユニークユーザー数を性・年齢別に店舗がカウントする。
  - ⑤【応用】複合商業施設に入場したユニークユーザー数と、店舗に入場したユニークユーザー数を店舗が比較する。
  - ⑥【応用】複合商業施設に入場したユニークユーザーの性・年齢別の人数と、店舗に入場したユニークユーザーの性・年齢別の人数を店舗が比較する。
- リピーターの分析
  - ①複合商業施設に入場した利用者が、過去一定期間中にいつ入場したかを複合商業施設が把握する。
  - ②複合商業施設に入場した利用者（性・年齢推定済み）が、過去一定期間中にいつ来場したかを複合商業施設が把握する。
  - ③店舗に入店した利用者が、過去一定期間中にいつ店舗に入店したかを店舗が把握する。
  - ④店舗に入店した利用者（性・年齢推定済み）が、過去一定期間中にいつ来店したかを店舗が把握する。
  - ⑤【応用】店舗に入店した利用者が、過去一定期間中にいつ複合商業施設に入場したかを店舗が把握する。
  - ⑥【応用】店舗に入店した利用者（性・年連推定済み）が、過去一定期間中にいつ複合商業施設に入場したかを店舗が把握する。

実人数のカウント実施イメージ



実人数のカウント実施時のルール

ルール一覧

導入前

・十分な期間をもった事前公知を行う（ガイドブック）
「カメラ画像の利活用目的」「カメラ画像利活用によって、来店者に生じるメリット」
「カメラ設置位置」「撮影範囲」「カメラ画像から生成するデータの概要」
「生成したデータからの個人特定の可否」「利活用実施期間」「実施主体の名称及び連絡先」等

取得時

・カメラ位置の明示（アイコン等の掲示）を行う（COCNルール）

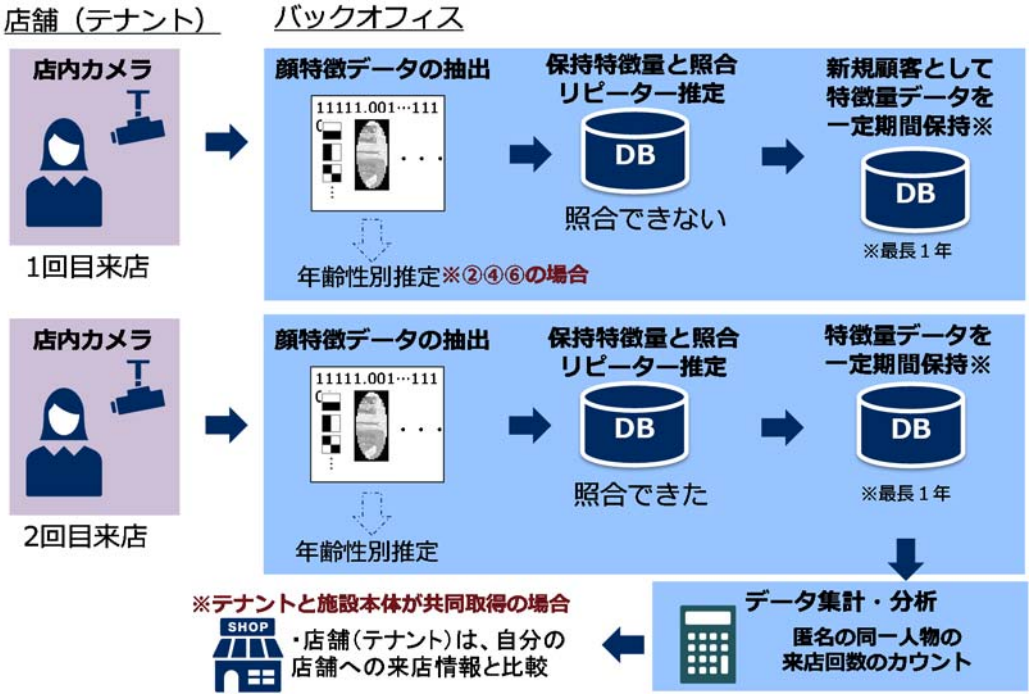
取扱い時

・必要な情報（顔特徴データ）以外は直ちに破棄する（ガイドブック）
・会員証など他の個人情報と紐づけを行わない（COCNルール）
・取得データが現場従業員等へ開示しない（COCNルール）
・特徴量データは事前に定めた一定時間の経過後削除（COCNルール）

管理

・消費者からの利用停止要求、開示請求、削除要望に対応する（COCNルール）
・他の営業主体へ共有を行わない（保護法）

リピーターの分析実施イメージ



リピーターの分析実施時のルール

ルール一覧

導入前

・十分な期間をもった事前告知を行う（ガイドブック）
「カメラ画像の利活用目的」「カメラ画像利活用によって、来店者に生じるメリット」
「カメラ設置位置」「撮影範囲」「カメラ画像から生成するデータの概要」
「生成したデータからの個人特定の可否」「利活用実施期間」「実施主体の名称及び連絡先」等

取得時

・安全管理措置（保護法）
・カメラ位置の明示（アイコン等の掲示）を行う（COCNルール）

取扱い時

・必要な情報（顔特徴データ）以外は直ちに破棄する（ガイドブック）
・会員証など他の個人情報と紐づけを行わない（COCNルール）
・取得データを現場従業員等へ開示しない（COCNルール）
・特徴量データは事前に定めた一定時間の経過後削除（COCNルール）

管理

・特徴量データの保有期間は最長1年とする（COCNルール）
・消費者からの利用停止要求、開示請求、削除要望に対応する（COCNルール）
※保有期間が６か月を超える場合は、保護法上の義務が発生
・他の営業主体へ共有を行わない（保護法）

お客様へのご説明と周知方法

店頭には、来店者向けの告知が必要です。
- カメラの運用・画像取得の主体
- カメラ画像を用いるサービスの目的

- 統一的な告知方法に関するガイドラインがあります。

取得した情報の取扱い（サービスでの利用）

取得した情報は、個人の同意を得ずに人物を判別しており、事前に回避が難しというカメラ固有の特徴があります。

- 現場におけるおもてなしのアクションはお客様ご本人だけでなく、例えばお連れの方や店員に情報を知られることで、お客様にご迷惑がかかる可能性があります。
- よって現場の従業員へ分析結果を共有し、何かしらの個人に対するアクションを行う場合には、基本的に本人の同意を得ることを推奨します（タイプ３）
  - 従業員が分析情報を得て、「いつもありがとうございます」とお声掛けしたいという場合など

取得した情報の取扱い（外部提供）

取得した情報は、個人のプライバシー情報でもあり、
企業秘密でもあります。

- 個人を特定する情報や行動履歴等は、十分に時間をとってサービス開始前にお客様にお知らせした範囲でしか流通できません。
- 来店人数等の統計的な情報等は、
個人が特定できない場合に限り一定の条件下で外部提供できます。
  - 具体的な統計処理方法の条件が、ルールに定められています。
    - 個人情報保護法の平成27年改訂における「匿名加工情報」にあたります。

お客様が取得されたくない場合への対応

- 本ルールで運用するサービスは、原則として
お客様からのデータ削除の要求を受け付ける必要があります。

- お客様からの申し出に基づき、あらかじめ提供された顔特徴データによって、データを取得しないという回避方法もあります。その場合、回避のために顔特徴データを保存することを十分に理解いただく必要があります。

お客様からの開示請求の対応

- 本ルールで運用するサービスは、原則として
  お客様からのデータ開示の要求を受け付ける必要があります。
- その場合、開示データの特定のために顔特徴データを取得することを十分に理解いただく必要があります。

- 会員向けWebシステムなどとセットでシステム構築することで、
  個別開示の対応を店頭で行うことを避け、
  運用コストを下げることをお勧めします。

個人情報管理の内部統制

- 個人情報の漏えいを防ぐため、個人情報管理の統制について
  システム設計段階で検討しておくことが求められます。
  - 個人情報にアクセスできる人はなるべく少なくしてください。
  - サービスの設計段階から、
    「誰が情報を必要とするか」の観点から検討を進めて下さい。
- また、このシステムから情報を開示される人に対しては、
  必ず守秘義務（雇用契約等を含む）を課し、
  適切な研修教育等をしてください。

最後に

- お客様に気持ちよく店舗をご利用頂くために、
  お客様との良い関係を築くため、
  今の段階からサービス・システム一体でのご検討をお願いします。

- システム開発事業者も、ご検討をお手伝いいたします。
- 詳しくは担当者までお問い合わせ下さい。

カメラ画像を用いた
人物認識サービスシステムを
検討される事業者さまへ

COCN カメラルール「タイプ3システム」ご説明資料

本資料の目的

- 顔認証装置などの人物特定技術を用いた顧客情報サービスの
  システム開発・導入を検討されている事業者さまに、
  実際のシステム開発の検討・打ち合わせのためのご参考に、
  COCN カメラルールの基本的な考え方をご説明します。

COCN カメラルール「タイプ3」とは

顔認証などの個人を識別する装置を用いてお客様を識別し、
ご来店の頻度や店内での動きなどを記録した上で、
- ポイントカードなどの個人情報と対応させてマーケティングを行うか、
- そのお客様の情報を店員等に知らせ、お客様に直接働きかけを行う

ようなシステムを指します。

タイプ3システムの例：
- 来客頻度・購買頻度が高いお客様のご来店時に、
  店員から直接お声がけをするため、店員に顧客情報を通知するサービス
- ポイントカードを提示しなくても、顔認証により自動的に
  購買ポイントをポイント口座に付与するシステム

（ご参考）COCNカメラルールの「他のタイプ」

- タイプ0
  - お客様を個人単位で識別せず、年齢・性別等の基本的な属性や
    棚前等狭い範囲での動きのみを把握するタイプ
- タイプ1
  - お客様を個人単位で識別せず、複数カメラの広い範囲に渡って
    短時間お客様を追跡して、動線等を把握し、統計的に利用するタイプ
- タイプ2
  - お客様の氏名等は特定しないまま、
    長期間にわたって個人識別のための情報（顔特徴など）を保存し、
    再来店頻度等の長期間の行動を追跡し、統計的に利用するタイプ

COCN カメラルール「タイプ3」の前提

COCNカメラルールでは、

- お客様の行動履歴を詳細に取得・蓄積し、
  店員等を通じて接客方法を変えるようなサービスについては、
  お客様に店内で不愉快・ご迷惑に感じていただかないよう、
  お客さまに十分納得して頂き、積極的にメリットを感じて使って頂く
  ことを前提としております。

そのため、

- 「タイプ3システム」は、お客様にあらかじめご説明頂き、
  何らかの形で事前にご同意を頂くことを前提としたルールとなっております。
- サービスを設計される当初より、あらかじめご理解のうえご協力ください。

事業者様にお願いすること

- 個人情報取得と運営の主体の特定（7～8p）
- 取得する個人情報と取得パターンの決定（9～11p）
- お客様へのご説明と同意の取得方法の検討（12～13p）
- 取得した情報の取扱いについて（14～15p）
- お客様からの退会等の対応方法の検討（16p）
- お客様への情報開示のご検討（17p）
- 個人情報管理の内部統制にかかるご検討（18p）

個人情報取得と運営の主体の特定（1）

まず、お客様との関係において、「誰が」情報を取得するのかを明らかに特定する必要があります。

- 個人情報管理や苦情処理等の主体となります。
- 取得した情報を共有できる範囲にも影響します。

- 基本的に、「取得した情報を最も利用する方」が主体になります。
  - 多くの場合、実際にお客様にサービスを直接提供する方が該当します。
  - カメラを設置した（設置費用を負担した）者と同一である必要はありません。
  - モールとテナントのような関係性がある場合、どちらが主体になるかご検討下さい。
    - 共同で主体になることも可能ですが、他テナントとの関係などもご配慮下さい。
  - フランチャイズのケースでは、個店・ブランドのどちらが表に立つかもご検討下さい。

個人情報取得と運営の主体の特定（2）

お客様との関係の運営主体とは別に、
実際のシステム運営は別の事業者に委託することができます。

- 委託先には、御社との間に守秘義務契約を締結して頂きます。
- （1次）委託先は、お客様へのご説明において明示することになります。
- 委託先は、貴社のサービス以外には取得情報を利用できません。
- 苦情受付の窓口業務等も委託できますが、
  最終的な責任はあくまで貴社にあることが前提となります。

取得する個人情報と取得パターンの決定

- タイプ3のシステムでは、カメラ等で取得する個人情報は、基本的にお客様との事前合意に基づいて決めることができます。
  - COCNカメラルールの他のタイプとは違い、ルール中での制限はありません。
- 但し、カメラに映ったお客様が、事前合意済みのお客様であることを確認できる時点以前に取得する情報には、制限があります。
- 撮影と、個人の識別（同意確認）のタイミング前後関係に御着目下さい。

「タイプ3システム」の主なパターン

パターンA
- ご来店時点から、カメラで画像を取得
- お客様を捕捉・追跡

↓

- レジで、IDカードを提示
- IDカードで、本人同意を確認
- 対応するお客様の追跡結果等を店員に提示
- 顧客別サービスを提供

画像取得と同時に本人同意が確認できないケース

パターンB
- ご来店時点でお客様の顔を認識
- 直ちにお客様を特定し同意を確認
- 店員にお客様の履歴等を提示

→ 店員が顧客別サービスを提供

パターンC
- レジにカメラを設置
- レジでお客様の顔を認識
- お客様を特定し本人同意を確認
- 顧客別サービスを提供

画像取得と同時に本人同意が確認できるケース

パターンごとの取得できる情報

- （パターンA）画像取得と同時に本人同意が確認できないケース
  - 取得して良い情報：
    ①来店者の顔特徴等の情報
    ②年齢・性別などの基本的属性
    ③1回の来店中の店内での動線等
  - 本人同意が確認できるまでは、②以外の情報は利用しない
  - 本人同意が確認できた時点で、①②③とも利用できるようになる
  - 不同意が確認された場合、①は直ちに消去する
    - ②③の統計的利用は、店頭で広く公衆に告知すれば可能

- （パターンB/C）画像取得時に本人同意が確認できるケース
  - 本人同意が確認できた場合、お客様同意済の情報は全て取得可
  - 本人同意が確認できない場合、基本的に情報を取得しない
    - 左記②③の統計的利用は、店頭で広く公衆に告知すれば可能

お客様へのご説明と同意の取得方法（1）

- 基本的には、ポイントカード等のIDを発行する際に、取得方法や利用方法を説明することが基本となります。
  - 基本的には、必ず「同意しない」選択肢を用意して下さい。
    （顔画像システムを必ず利用しなければ、店を利用する価値が無い場合などは除く）
  - 後々の紛争の防止等の観点からは、書類に同意の記録を頂くことが望ましいと考えられます。
  - 例えばIDカードを先に発行した上で、パンフレットをお渡しし、会員情報登録Webサイト等で同意の登録を頂くなどの手段も有効です。
    - 店頭での詳細な説明の時間を短縮し後回しにすることができます。
    - 登録時のボーナスポイントなどと組み合わせることも有効です。

お客様へのご説明と同意の取得方法（2）

店頭には、まだ利用同意していない来店者向けの告知が必要です。
- カメラの運用・画像取得の主体
- カメラ画像を用いるサービスの目的
- 利用同意をした人を対象とした「タイプ3」システムである旨
- 利用同意をまだしていない人から取得される情報の内容

- 統一的な告知方法に関するガイドラインがあります。

取得した情報の取扱い（サービスでの利用）

取得した情報は、個人のプライバシー情報でもあり、
企業秘密でもあります。

- お客様ご本人だけでなく、例えばお連れの方や店員に
  情報を知られることで、お客様にご迷惑がかからないか、
  事前によくシナリオベースでの検討を行って下さい。
  - お客様ご本人にのみ（例えばスマホの利用で）、
    あるいは限られた店員にのみ（例えばフロア責任者）情報を提示することで、
    お客様への万が一のご迷惑の可能性を大きく減らすことができます。

取得した情報の取扱い（外部提供）

取得した情報は、個人のプライバシー情報でもあり、
企業秘密でもあります。

- 個人を特定する情報や行動履歴等は、
  あらかじめ本人同意を取得した際にお客様にお知らせした
  範囲でしか流通できません。
- 来店人数等の統計的な情報等は、
  個人が特定できない場合に限り一定の条件下で外部提供できます。
  - 具体的な統計処理方法の条件が、ルールに定められています。
    - 個人情報保護法の平成27年改訂における「匿名加工情報」にあたります。

お客様からの開示請求の対応

- 本ルールで運用するサービスは、原則として
  お客様からのデータ開示の要求を受け付ける必要があります。

- 会員向けWebシステムなどとセットでシステム構築することで、
  個別開示の対応を店頭で行うことを避け、
  運用コストを下げることをお勧めします。

個人情報管理の内部統制

- 個人情報の漏えいを防ぐため、個人情報管理の統制について
  システム設計段階で検討しておくことが求められます。
  - 個人情報にアクセスできる人はなるべく少なくしてください。
  - 特に、今来店している目の前のお客様以外の情報については、
    まとめてアクセスできる人をできるだけ少なくすべきです。
  - サービスの設計段階から、
    「誰が情報を必要とするか」の観点から検討を進めて下さい。
- また、このシステムから情報を開示される人に対しては、
  必ず守秘義務（雇用契約等を含む）を課し、
  適切な研修教育等をしてください。

最後に

- お客様に気持ちよく店舗をご利用頂くために、
  お客様との良い関係を築くため、
  今の段階からサービス・システム一体でのご検討をお願いします。

- システム開発事業者も、ご検討をお手伝いいたします。
- 詳しくは担当者までお問い合わせ下さい。

10. モール運営者、サービサー間契約書要旨

モール運営者・サービサー間契約書要旨

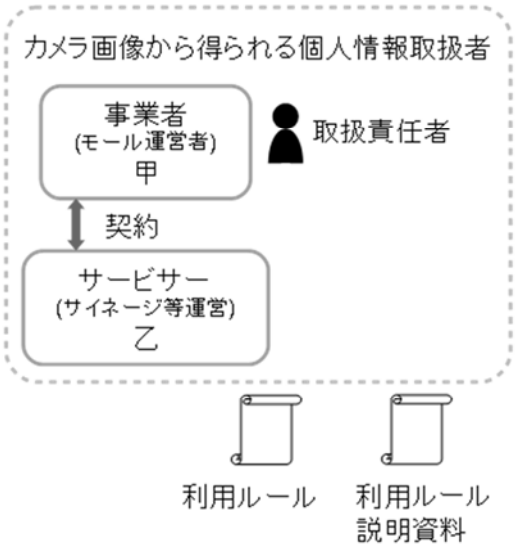
モール運営者が、サイネージ運用者などの「サービサー」と契約を結ぶ際に交わす契約書に盛り込むべき内容の概要を示す。

実際の契約書には扱う情報の範囲・情報処理の内容・秘密保持契約などの詳細が案件ごとに定められ、盛り込まれる。

サービサーはテナントとは直接は契約せず、モールを通じて契約すると想定する。

契約書要旨 たたき台 ケース1: 共同利用する場合

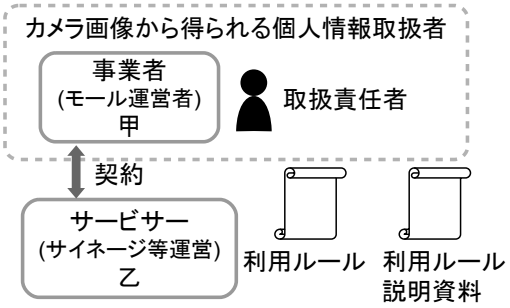
- モール運営者(甲)とサービサー(乙)は、カメラ映像から得られる情報の管理責任を一体となって負う。
- 甲および乙は、上記に係わる個人情報の取り扱い規定を次の通り整備する。→ COCNカメラ画像利用ルール。目的外利用の制限や第三者提供の制限や匿名加工情報の扱いなどはここに含まれる。
- 甲および乙は、上記に係わる取扱責任者を次の通り定める。
  → 明記する



サービサーが主体の一部となるので、基本的には利用ルールのままとなる。
特に、得られた情報の目的外利用や第三者提供はできない。
ただし、匿名加工化した情報は、一定の条件の元で利用できる。

契約書要旨 たたき台 ケース2: 匿名化情報のみを受け取る場合

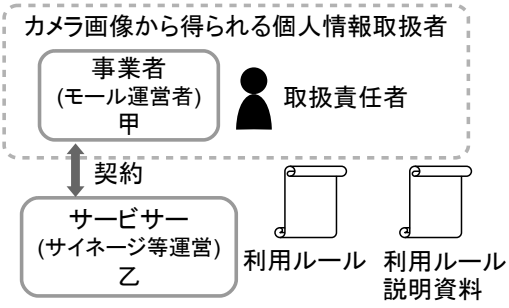
- モール運営者(甲)は、カメラ映像から得られる情報の管理責任を負う。
- 甲は、上記に係わる個人情報の取り扱い規定を次の通り整備する。→ COCNカメラ画像利用ルールのうち必要な部分。目的外利用の制限や第三者提供の制限などはここに含まれる。また、サービサーに提供する情報は利用者への告知事項に含める必要がある。
- 甲は、上記に係わる取扱責任者を次の通り定める。→ 明記する
- 甲はサービサー(乙)に対して、上記に係わる個人情報を提供しない。
- 甲は乙に対して、上記に係わる個人情報に関し、上記の規定に従い、匿名加工情報(〇〇と□□と……)を提供できる。
  → 提供する情報の種類は契約時に具体的に決める
- 乙は匿名加工情報の作成の元となった個人情報の本人を識別する目的で、他の情報と照合してはならない。
- 乙は、匿名加工情報を第三者に提供する際は、その第三者に本契約と同等の義務を課す。



サービサーが利用ルールの第15条における匿名加工情報の提供を受ける第三者となるため、その要件を満たす必要がある。

契約書要旨 たたき台 ケース3: システム運営のみを委託を受けて行う場合

- モール運営者(甲)は、カメラ映像から得られる情報の管理責任を負う。
- 甲は、上記に係わる個人情報の取り扱い規定を次の通り整備する。→ COCNカメラ画像利用ルールのうち必要な部分。目的外利用の制限や第三者提供の制限などはここに含まれる。また、サービサーの名前を委託データ事業者として利用者への告知事項に含める必要がある。
- 甲は、上記に係わる取扱責任者を次の通り定める。→ 明記する
- 甲はサービサー(乙)に対して、上記の規定に従い、個人情報を提供する。
- 乙は提供された個人情報に対して、本契約で定めた処理(〇〇と□□と……)のみを行う。→処理は契約時に具体的に決める
- 乙は提供された個人情報を他の情報源から得たデータと分別してそれぞれを独立に扱う。
- 乙は提供された個人情報を他の情報源から得たデータと統合して解析しない。
- 乙は提供された個人情報の秘密保持をする
  →契約時に秘密保持契約を具体的に定める。また、再委託する場合は、乙は再委託先と同等の秘密保持契約を結ぶ。



サービサーが利用ルールの第16条における外部の委託データ処理事業者となるため、その要件を満たす必要がある。

一般社団法人 産業競争力懇談会（ＣＯＣＮ）

〒100-0011　東京都千代田区内幸町２－２－１
日本プレスセンタービル　４階
Tel：03-5510-6931　Fax：03-5510-6932
E-mail：jimukyoku@cocn.jp
URL：http://www.cocn.jp/
事務局長　中塚隆雄