IoTとデータプライバシー

国立情報学研究所（NII）

佐藤一郎

自己紹介：佐藤一郎

- 国立情報学研究所・副所長／教授
  国立大学法人総合研究大学院大学・複合科学研究科情報学専攻教授（兼任）
- 学歴
  - 慶應義塾大学理工学部電気工学科卒、
    同大学理工学研究科大学院計算機科学専攻
    後期博士課程修了、博士(工学)
- 講演に関係する委員会など
  - 内閣官房パーソナルデータに関する検討会委員
    ＆技術検討WG主査
  - 経済産業省産業構造審議会IT人材WG委員
- 専門は分散システム／クラウドコンピューティングの
  OS及びミドルウェア
  - 個人情報及びプライバシーは本来は専門では
    なかったはずですが・・・

国立科学博物館（上野）に
センサーネットワークを設置

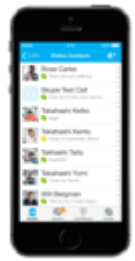
軍艦島（長崎）にセンサー設置・観測

講演概要

- IoT特有の10個のプライバシー問題
  - 気づかないうちにプラバシー侵害
  - 同意取得が難しい
  - 相違なデータの組み合わせ
  - カメラやセンサーの写り込み
  - 第三者提供を前提としたパーソナルデータの取得
  - 現実世界の情報によるパーソナルデータの名寄せ
  - マルチステークホルダー化
  - 現実世界へのフィードバック（サイバーフィジカルシステム）
  - センサーの高性能化
  - 脆弱なセキュリティ
- 今後に向けて

IoTとパーソナルデータ

- **IoTの対象は現実世界**
  - 現実世界には人間が含まれることは多い
  - IoTが取得する情報には人間に関わるパーソナルデータが含まれる

非接触IC カード改札	ポイントカード／ 電子マネー	ウェアラブル デバイス	ソーシャル ネットワークサービス	通話 アプリ
				
乗降駅と 乗降時間	購買品、年齢、 性別、生活圏	心拍数、血圧 ランニング距離・位置	関心事、交友関係、 移住地、学歴、職歴	通話記録、 位置情報、電話帳

大きなビジネスチャンス

- **パーソナルデータ、特に行動履歴から見えてくること**
  - **特定の個人の識別**
  - **個人のプライバシー**

IoT特有の10個のプライバシー問題

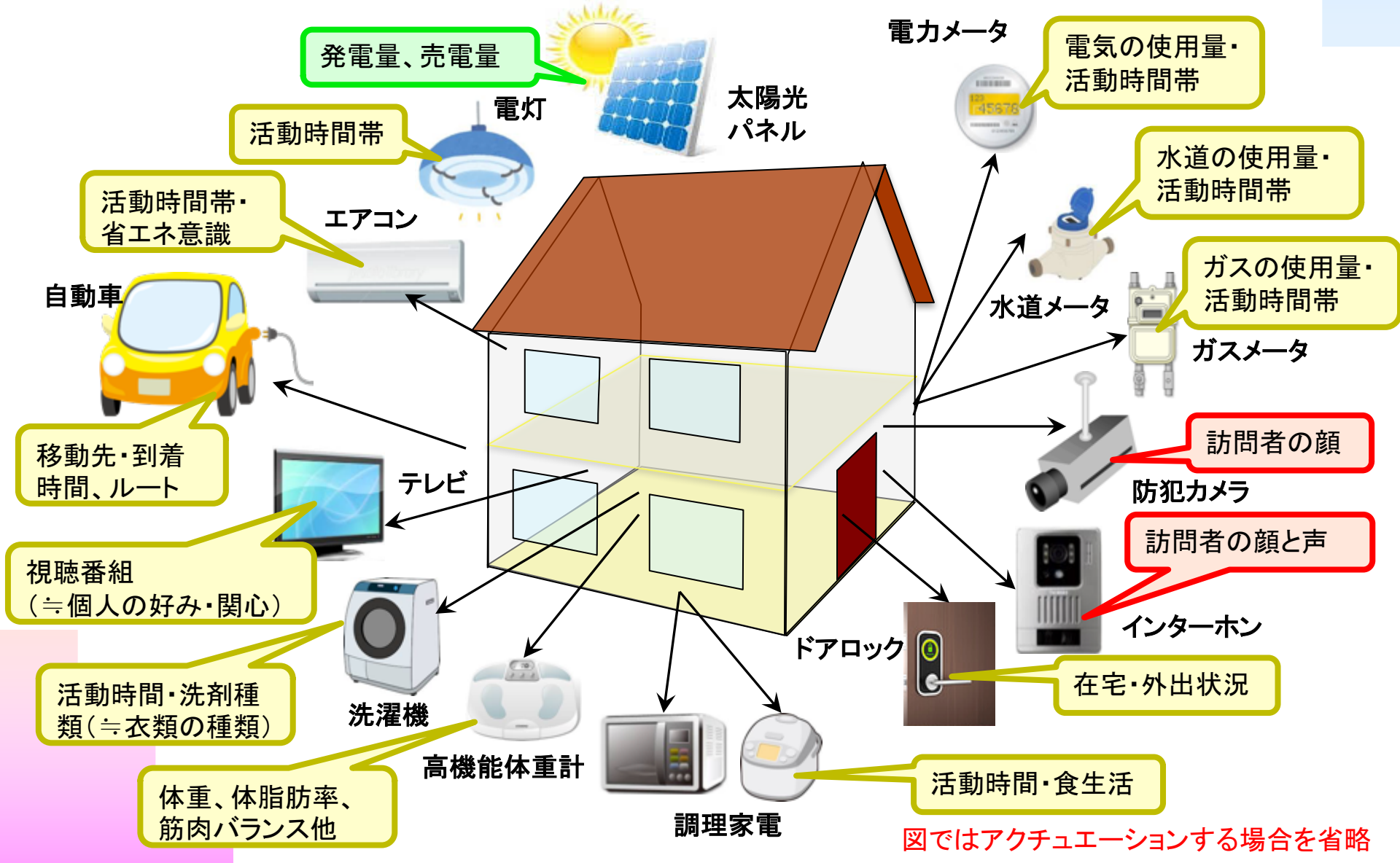
- IoTにおけるプライバシー問題は従来技術と重なるが、特有なものも多い
  - 気づかないうちにプラバシー侵害
  - 同意取得が難しい
  - 相違なデータの組み合わせ
  - カメラやセンサーの写り込み
  - 第三者提供を前提としたパーソナルデータの取得
  - 現実世界の情報によるパーソナルデータの名寄せ
  - マルチステークホルダー化
  - 現実世界へのフィードバック（サイバーフィジカルシステム）
  - センサーの高性能化
  - 脆弱なセキュリティ

IoTの課題：気がつくとプライバシー侵害

- IoTは現実世界に関する情報を集める手段・設備
  - 現実世界の情報にはパーソナルデータ（個人に関する情報）が含まれる
  - 課題：IoTにより多様な個人行動監視や個人の特定を可能にしてしまう
    - 知らないうちに法的問題・プライバシー侵害を引き起こすリスク
  - 課題：IoTデータでビジネスになりやすいのはパーソナルデータ関連
    - 法的・社会的な制約
- 想定される問題
  - （結果としての）個人の特定と、それによる法的な問題
  - 情報による直接・間接のプライバシー侵害
  - 情報に関わるステークホルダー問題

IoTで覗けるプライバシー（住宅）

非個人情報
プライバシー
個人情報



図ではアクチュエーションする場合を省略

IoTの課題：同意取得が難しい

- パーソナルデータ取得・利用は適切な説明と個人本人の同意取得が原則
  - 個人情報に関しては法的にも同意が必要

- しかし、IoTでは明示的な同意取得は難しい
  - 空間・コンテキストによる取得と利用目的を提示と個人本人の意思が反映できる仕組み
    - 例：防犯カメラでは設置提示

犯罪予防目的の撮影録画の場合、犯罪発生の蓋然性、緊急性、防犯カメラ設置の必要性、撮影態様の相当性を総合的に考慮し、必要最低限な範囲に限定されるべき

取得の拒否ができるかも重要

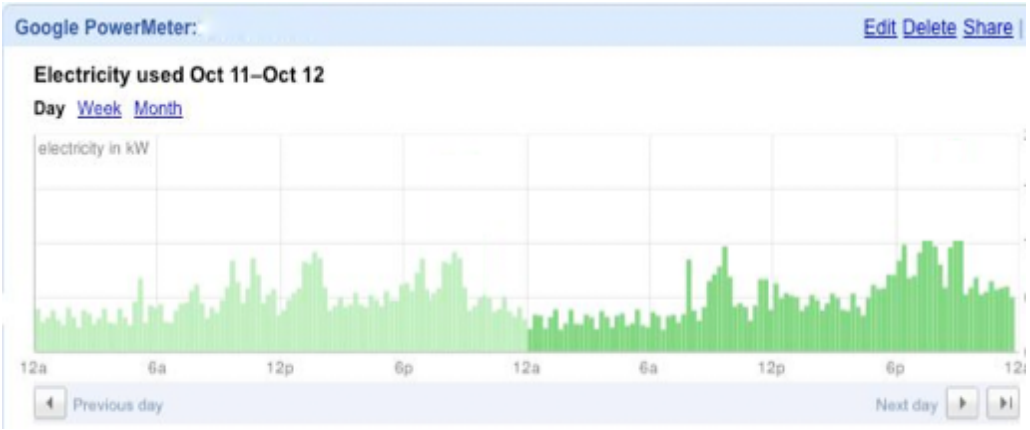
  - 将来的には個人のAI・エージェントが同意の代行もできるはず

- 同意を取るのは難しいといわれますが、同意は事業者への信頼の証
  - 信頼されていない事業者は同意を取るのは困難
  - 同意内容に反した利用や提供をすれば信頼を失う

IoTの課題:相違なデータの組み合わせ

- 自宅(講演者)の電力監視

TED 5000 (Energy Inc.)



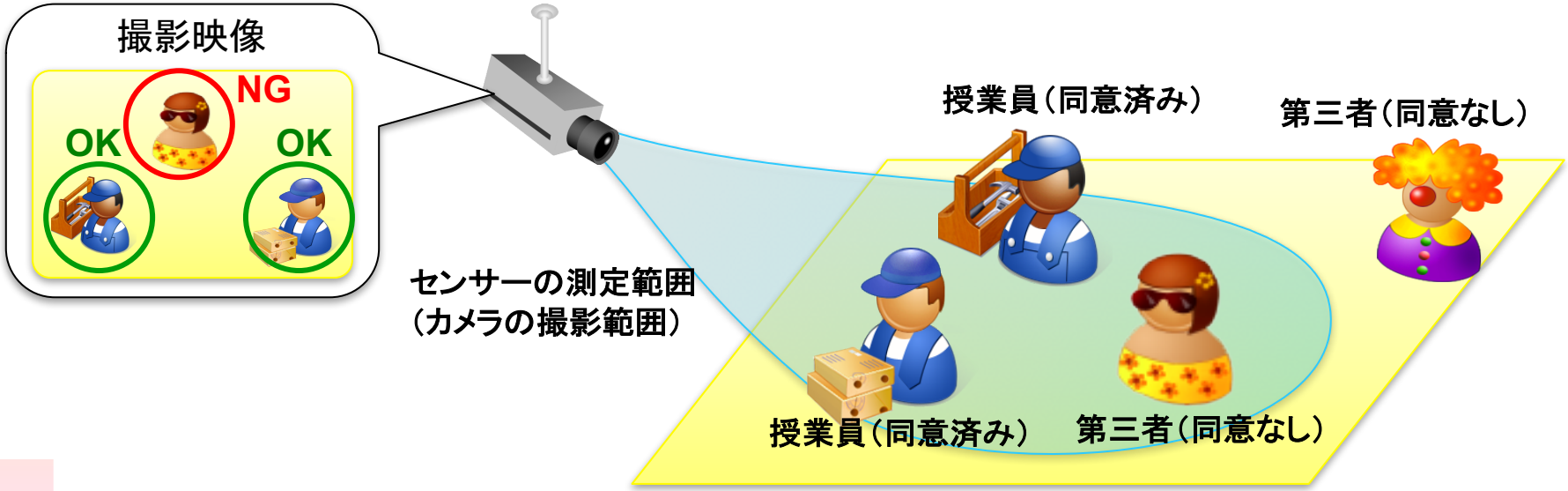
- 電力監視データからは本人ですら電力消費と利用家電の相関がわからない
  - 単体のIoTデータの多くは個人特定やプライバシー侵害は少ないが・・・

- 個別データで見えないプライバシーも相違データの組合わせで見えてくる
  - 実例:水道メータとガスメータの遠隔共同検針の実証実験(2002年)
    - プライバシー情報が見えてしまい、実験中止

- データの組み合わせ方は事前に予測できない、組み合わせによる個人特定やプライバシー侵害の責任関係は議論・整理が必要

IoTの課題：写り込み

- カメラを含むセンサーは対象者以外の情報を取得してしまう
  - センサーの情報量は増えている（例：カメラの高解像度化）
  - 写り込んだ個人の特定や行動捕捉は可能



- センサーの範囲と精度をいかに制御するのか
  - 現状はセンサーの設置場所や建物構造で工夫の段階
    - 例：ビルなどで通行人が見える窓の方向にカメラを向けない

IoTの課題：第三者提供とビジネス

ネットワークビジネスモデルの変化

- 広告枠を販売（ユーザは顧客ではない）
  - 広告を表示することで、広告主から広告料を稼ぐ
    - 例：既存の多くの無料ネットサービス（Googleを含む）
- サービスを販売（ユーザが顧客）
  - 所定期間・回数・取得情報に応じてユーザから利用料をもらって稼ぐ
    - 例：ネットゲーム、新聞オンライン版、LINE（スタンプ）
- ユーザ情報を販売（ユーザが商品）
  - サービスを通じてユーザに関する情報を収集し、その情報を売って稼ぐ
    - 例：Twitter、無料ヘルスケアサービス

IoTの課題：現実情報による名寄せ

- 現実世界は一人の人間は唯一無二、同じ現実世界を他者と共有
  - 同じ世界（例：同じ空間&同じ時刻）に関する情報が複数存在しうる
    - 例：その場にいる人も同じ空間&同じ時刻を共有

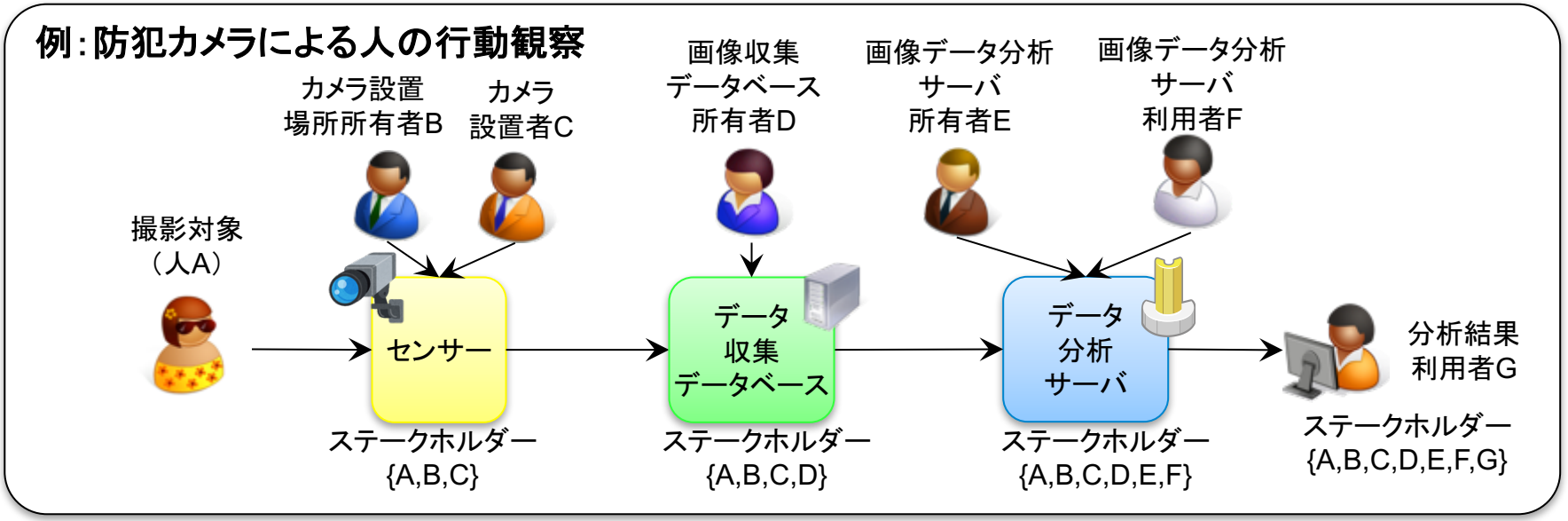
- 場所や時刻の組み合わせにより、同じ対象に関する情報と容易にわかる
  - 例：時刻情報が秒単位の鉄道乗降履歴と改札付近の（防犯）カメラ映像

    単体では個人情報にならなくても、同時刻の両情報を突き合わせれば、乗降履歴に関する個人の顔は容易にわかる

- IoTによる取得した情報は、一般のネットサービスで取得する情報より、複数情報を名寄せすることが容易

IoTの課題：マルチステークホルダー化

- IoTによる情報の取得、分析、利用にはステークホルダーが多数・複雑
  - データの対象者、所有者、設置者、分析者、分析結果の利用者他多様

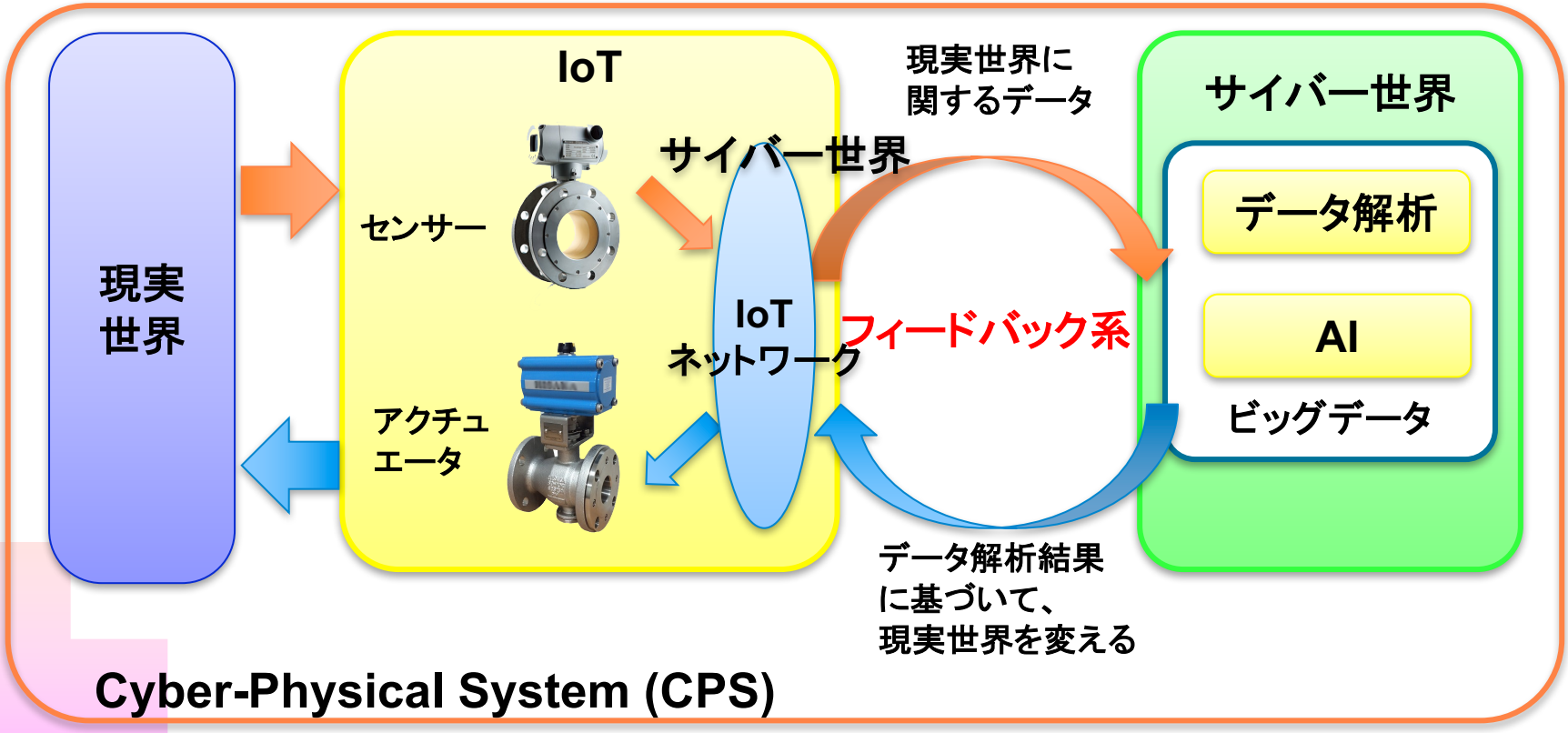


- ステークホルダー間利害関係を調整できないとIoTは利用できない
  - IoTにおける個人情報／プライバシー問題は、個人本人とデータ利用者という2者問題となり、マルチステークホルダー問題の一部にしかすぎない
    - 個人情報・プライバシー問題だけにとらわれるべきではない
  - 解決すべきはマルチステークホルダーを前提にした利害関係の調整
    - 受益者の応分負担と利用者により提供データを削除・加工

IoTの課題：現実世界へのフィードバック

- IoTとビッグデータは方向性は同じ
  - データを集めるところに着目すればIoT
  - データを分析するところに着目すればビッグデータ

} 両者は両輪 (=CPS)



現実世界へのアクチュエーションは諸法制度により規制される

IoTの課題：センサーの高性能化

- 4Kや8Kカメラなど高解像度カメラが普及すると

いままで見なかったものも見えてくる

- 天頂衛星システムなどの次世代GPSで測位精度が向上すると
  - 従来GPSでは測位精度は数メートルであり、その位置情報は個人の位置や移動経路の捕捉だったが
  - 次世代GPSでは測位精度は約10cmであり、位置情報を使って人混みの中でも、個人を特定できる

従来GPS
ある個人がいるエリア

次世代GPS
位置座標で個人を特定

IoTの課題：セキュリティ的脆弱性

- 現状ではIoTのセキュリティは高いとはいえず、情報漏洩を前提に制度設計すべき

- IoTは非力なコンピュータで構成
  - 高度なセキュリティ・暗号対策は困難
  - 対策：インターネットとの直接接続をさける
    - 閉じたネットワークで運用、または
    - ゲートウェイを介した接続による保護が望まれる
- センサーデータを含むデータ改ざん対策が重要
  - 周辺ノードとの比較による改ざん発見
- IoTを前提にしたアクセス制御が求められる
  - 誰に見せるかだけでなく、どのようなデータを見せるかが重要
    - 例：匿名化済みデータを提供など

Hall4のIoTタウン
国立情報学研究所・
北海道大学・大阪大学・九州大学ブースへ

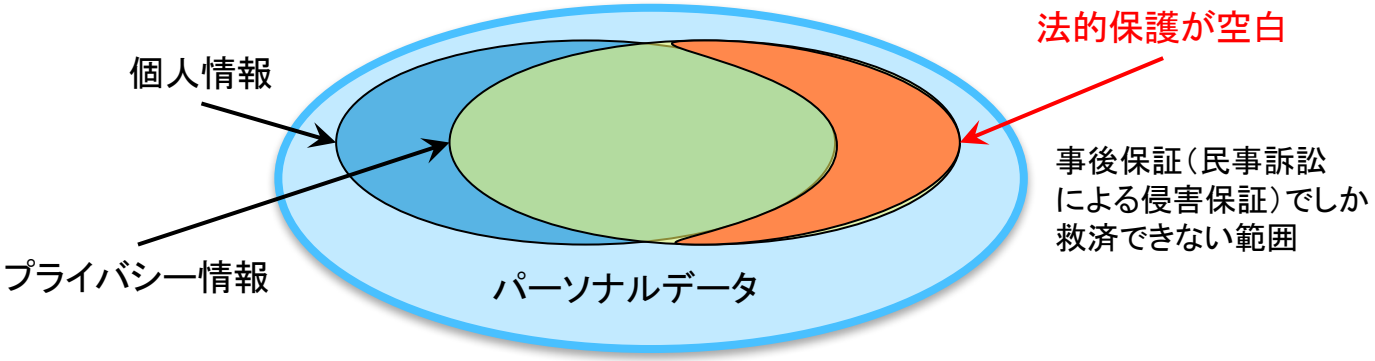
今後に向けて

国立情報学研究所　教授／所長補佐

佐藤一郎

プライバシー絡みで炎上が起きる背景

- 個人情報保護法などの法律上はOKなパーソナルデータの取得や利活用でも、社会的な批判（炎上）がおきうる
- OECD諸国のパーソンルデータに関する法体系の基本的な考え方
  - 守るべきはプライバシーだが、プライバシーは範囲が不明確
  - 代わりに個人情報（特定の個人を識別につながる情報）を保護することで、間接的にプライバシー情報を守る
- 法的に個人情報にならなくても、世の中の多くの人がプライバシーと思う範囲のパーソナルデータを保護しないと社会的批判が起きる



隠すべき情報だけを隠す

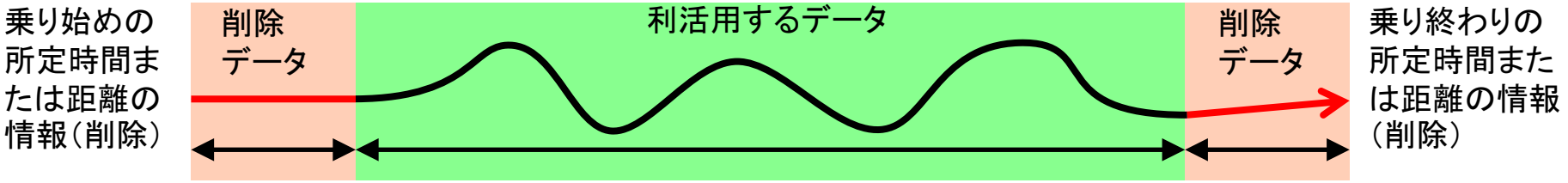
- 守りたい情報は何か、それに応じた対策をたてるべき
  - 情報そのものを隠す必要があるのか
  - その情報に関わる個人を隠したいのか
  - 個人の行動のうち何を隠したいのか

→ 一律に削除・加工するのではなく、守りたい対象を守るべき

例：欧州のカーナビ情報の匿名化（ユーザから利活用の同意取得）

TOMTOM

- 自動車や運転手を特定する情報（自動車ナンバーや所有者他）を削除
- 仮IDはナビゲーション一回ごとに割り当て（継続的トレースはしない）
- 乗り始めと乗り終わりのデータを削除（出発地と目的地の特定を防ぐ）



技術と制度の一体化

- ITの進歩は、大きな効用をもたらしたが、一方で問題を生み出している
  - 例：個人情報およびプライバシーに関わる権利・利益の侵害
    - ウェアラブルカメラとプライバシー
- 問題によっては技術だけでは解決できない
  - 制度による補完が必要
- 技術と制度を一体化で考えるべき
  - 研究開発段階から、技術が引き起こす問題を予測し、それを抑止・最小化する制度設計を行うべき
  - セキュリティファースト、プライバシーファースト

まとめ

- IoT特有のプライバシー・個人情報の課題
  - 課題に正面から取り組まないとIoTは普及しない
  - 課題を解決しないと、長期的には利活用は制限されるだけ
- 研究開発段階からプライバシー問題を考慮すべき
  - 起きうる問題を予測し、その問題を解決する技術や法制度を検討すべき
- IoTは現実世界を扱うため、現実世界のルールは避けられない
  - 技術と法制度は不可分とし、技術の開発段階から法制度を含めた検討が必要