資 料 5

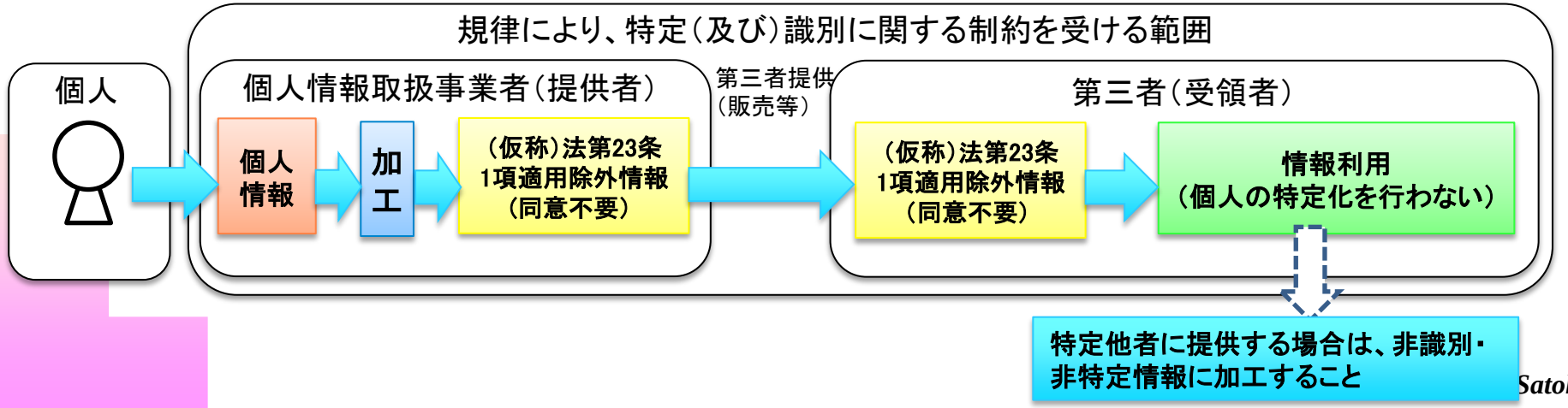
位置情報とパーソナルデータ

国立情報学研究所・アーキテクチャ科学研究系・教授
ISO/IEC SC31-WG4（Real-Time Locating Systems）規格委員
政府IT総合戦略本部「パーソナルデータに関する検討会」委員
／同検討会技術検討ワーキング主査

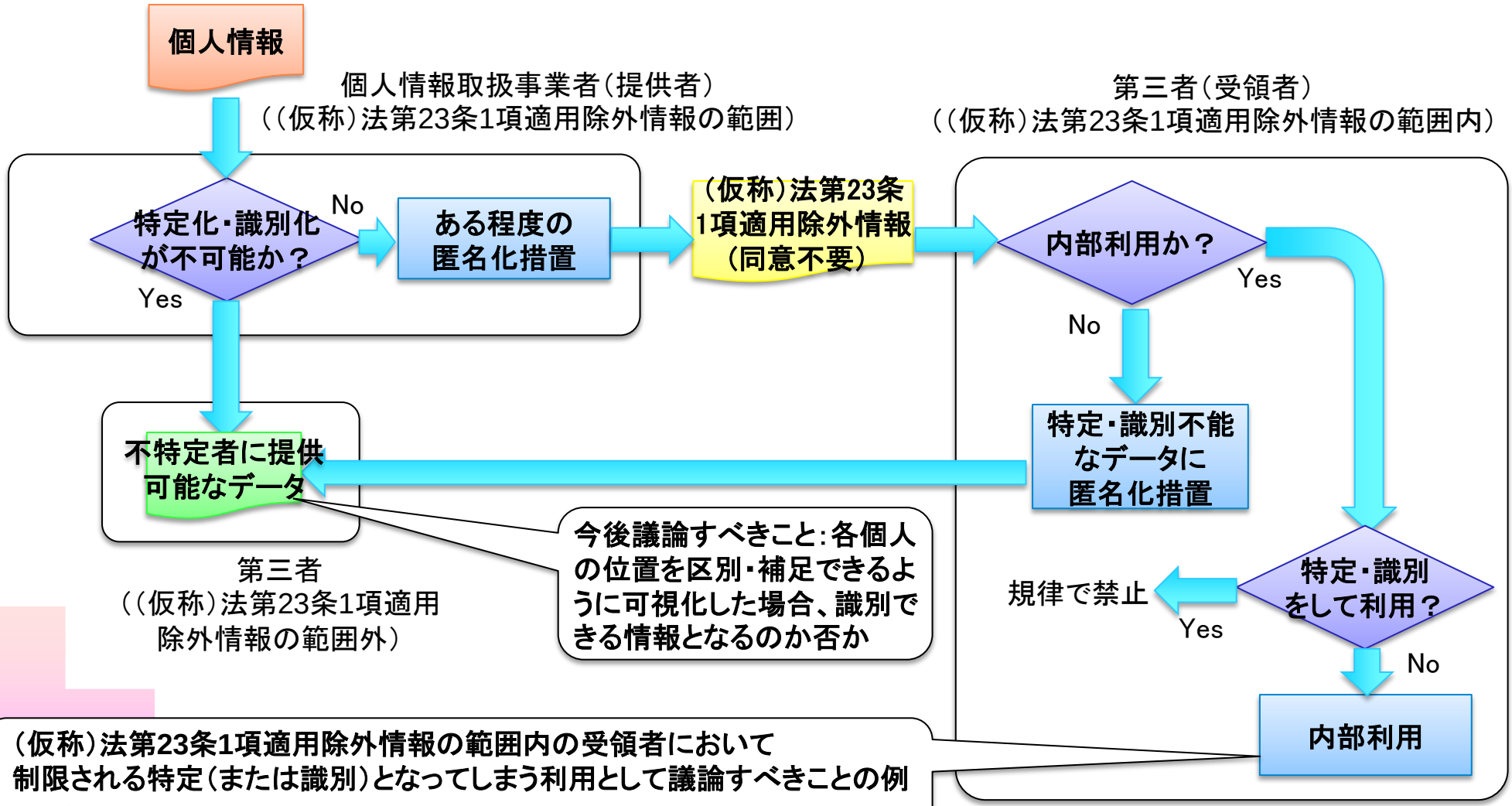
佐藤一郎

IT総合戦略本部「パーソナルデータに関する検討会」技術検討WGの議論

- 個人情報を特定と識別の観点から整理
- 匿名化による限界を（あらためて）示す
  - （利活用と両立しながら）任意のあるデータに対して、100%の特定・識別を排除するような汎用的な匿名化方法はない
- 第三者提供を前提にしたデータ類型（（仮称）法第23条1項適用除外情報）を例外的な取り扱いとして提案
  - **提供者はデータ提供の前に、ある程度の匿名化することを求める**
  - **提供者及び受領者は個人の特定・識別を行わないことを規律で制限**



（仮称）法第23条1項適用除外情報（続き）



（仮称）法第23条1項適用除外情報の範囲内の受領者において制限される特定（または識別）となってしまう利用として議論すべきことの例

- 各個人の情報とその個人に関わる外部情報を付き合わせ

Ichiro Satoh

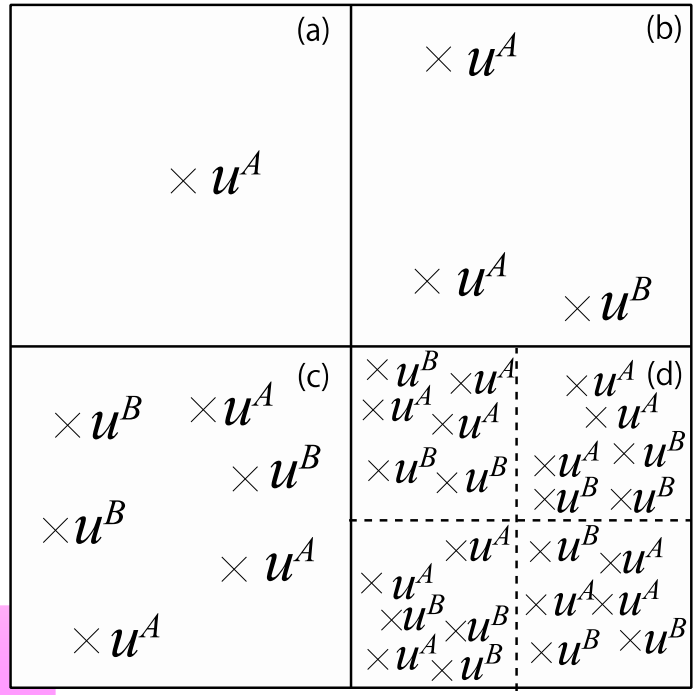
（仮称）法第23条1項適用除外情報

- （仮称）法第23条1項適用除外情報＝同意なし第三者提供可能情報
  - 同意が基本、同情報はあくまでも例外として位置づけ
  - 同情報はある程度の匿名化措置されていることが前提
    - その匿名化程度や規律は技術WGでは厳密に定義していない
    - 特定・識別に及ばない範囲に利用内容も制限される

- 技術WGではFTC3要件をベースに運用手法議論（FTC3要件とは独立）
  - 匿名化措置は約束・公表を想定
    - 届出や登録に代えることを議論したが、事務手続きが大きい
    - この他、受領者（及び提供者）を許認可制にするなども議論されたが、技術WGの範疇を超えるので、詳細は議論していない
  - FTC3要件では、問題が発生した場合、事業者責任が前提
    - 第三者機関の役割はあえて議論していない

位置に関する匿名化

- 識別を避けるためには、ある位置にいる人数他で制限が必要
  - 例：都会と過疎地では位置情報から識別・特定可能性は違う
- 位置情報向けの匿名化手法は研究されている
  - 例：K匿名性を満足するように対象空間（の広さ）を変更
- 匿名化と利活用のトレードオフに要注意



u^A ：属性 A をもつユーザ
u^B ：属性 B をもつユーザ

(a) と (b) は 3- 匿名性なし
(c) と (d) は 3- 匿名性あり

(d) は点線で四分割しても
3- 匿名性があり

from to appear 佐藤一郎：
”ビッグデータとパーソナルデータ”,
法とコンピュータ学会誌, 2014

匿名化が引き起こす問題

- k-匿名性を実現すると、複数人が位置的には区別不能になるが
  - 範囲内の他の個人や施設にいると間違えられるケースも
    - リスクを説明しないと、あとから大きな反発となって跳ね返る

対象空間が狭い（K=1）

K匿名性のために対象空間を広げる

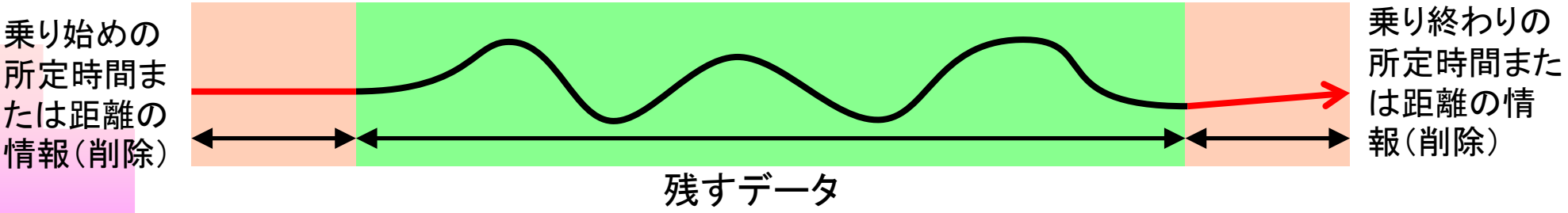
対象空間を広い（K=3）

- 自衛策：個人は人違いされたくな人たちがいる地域や、いると思われたくない場所のある地域を避けること、ただし結果として
  - 住居や行動範囲が地域的分断が生じる → 深刻な社会問題を引き起こす

守りたい情報は何か

- 守りたい情報は何か、それに応じた対策をたてるべき
  - 位置情報をそのものを隠す必要があるのか
  - ある位置にいるのが誰かを隠したいのか
  - ある個人の行動を隠したいのか

- 例：欧州のカーナビ情報の匿名化（ユーザから同意をとっている）
  - 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）



私見：位置情報の取り扱い

- 匿名化は簡単ではない、適切にできない事業者を前提に制度設計
  - 匿名化と分析は盾と矛、守る技術は攻める技術を知る必要がある
- 同意が基本だし、同意をとる方が自由度が高い
  - ただし、過去に不適切な同意取得事例があると、当該分野の利活用に大きく影響
- 個人情報の取り扱いはマルチステークホルダー問題の一部に過ぎない
  - ステークホルダーは主体（個人）と情報利用者だけではない
    - 例：WiFiによる位置推定では、アクセスポイントの設置者もステークホルダー
- 守るべき位置情報と守らなくても許される位置情報がある
  - 位置情報がプライバシー上の問題となるのは主体と紐付いたとき
- 人・状況によって、守りたい情報は変わる
  - 災害時はなんでもありでも、一方で位置情報を公開されたくない個人もいる
- 非本質的だが、個人情報の第三者提供はその対価次第
  - JR東日本はSuica導入時に問題視されたことが起きてしまった
- 技術進歩についていくこと
  - 次世代GPSやCSAC等のブレークスルー技術により測位精度の向上を考慮する

私見：位置情報の取り扱い

- 技術進歩でいま問題になっていない情報も将来はわからない
  - 測位精度の向上、外部情報増加により、状況は変わる
- 位置情報は有用性が高いが、個人行動の補足というプライバシーに関わる
  - 制度見直しではプライバシーの観点から個人情報を整理
    - 位置情報の取り扱いは厳しくなるのではないか
- 目的に応じたデータ取得・利用（不要なデータは取得しない）
  - 例：災害目的ならば現在位置情報で十分なケースも多いはず
  - 例：災害対策を名目にしたデータの目的外利用は、不信感を招き、災害に必要なデータが提供されず、国民の生命・財産に深刻な影響を与える

- 位置情報の災害時の第三者提供であれば、個人情報保護法第23条第1項第2号の「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」に該当するケースもある（内閣府Q&A)、ないしは第23条第1項に災害に関わる例外を追加すべき