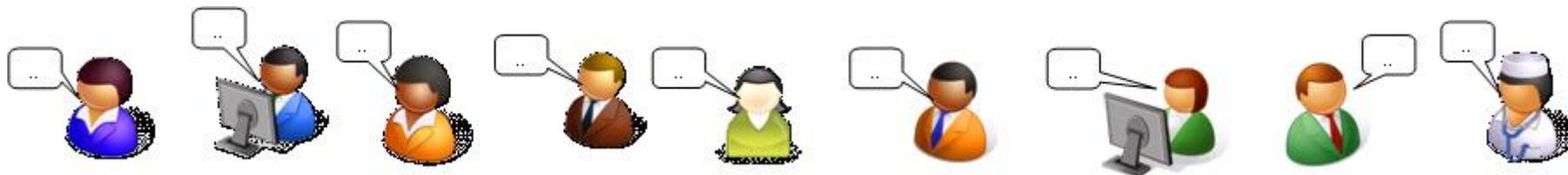


Internet Week 2013

プライバシー保護に係わる 技術・ビジネス・制度の動向

2013年11月28日

セコム（株） I S研究所 松本 泰



S10ビッグデータ時代のプライバシー保護技術

- オープンデータやビッグデータを活用した新事業、新サービス等への関心の高まり、番号制度の成立等から、パーソナルデータの保護と利活用のためのビジネス、技術、制度への取り組みが活発化しています。
- 本セッションでは、パーソナルデータ、ビッグデータに関するビジネスの要求、制動の動向等を概観した上で、パーソナルデータの保護と利活用の両立を目指したプライバシー保護技術の最新動向を解説します。

S10ビッグデータ時代のプライバシー保護技術

- プライバシー保護に係わる技術・ビジネス・制度の動向
 - 松本 泰（セコム（株） I S研究所）
- ビッグデータビジネスと程よいWebプライバシー
 - 吉井 英樹（ソフトバンクテレコム（株））
- ビッグデータと匿名化
 - 山口 利恵（東京大学）
- ビッグデータのプライバシー保護技術
 - 佐久間 淳（筑波大学コンピュータサイエンス専攻 准教授）

プライバシー保護に係わる技術・ビジネス・制度の動向

- 番号法の成立
- 「世界最先端IT国家創造宣言」
- 規制改革会議の要望
- パーソナルデータに関する検討会
- 技術検討WGにおける議論
- 規制とパーソナルデータの利活用の関係
- 残る疑問や今後の議論??

ビジネス

制度

行き過ぎた個人情報保護はイノベーションを阻害する

EUのデータ保護法は非関税障壁

個人情報保護法を国際基準に合わせて改正すべき

ビッグデータ・オープンデータが社会を変える

第三者機関設立は、規制緩和に反する

内閣府
パーソナルデータに関する検討会

医療に関するパーソナルデータは利活用されるべき

このままでは、ネットビジネスは、全て米国に持って行かれる

消費者庁
個人情報保護専門調査会

経済産業省
IT融合フォーラム
パーソナルデータWG

総務省 パーソナルデータの
利用・流通に関する研究会

FTC3要件って何だ

匿名化により自由にデータを使わせるべき

SUI**の第三者提供は違法だ

総務省3要件って何が違うの？

経済産業省
パーソナル情報研究会

情報大航海（後悔）プロジェクトってなんだっけ？

通信の秘密は原則

情報大航海プロジェクト
パーソナル情報保護・解析基盤

プライバシー権は、新しい人権

レセプト情報の活用は慎重に

k - 匿名性、l - 多様性、
l - 多様性

差分プライバシー

私の個人情報はどこにあるの？

「共通番号制」絶対反対！！

準同型暗号による処理

技術

利用者

権利

番号法の成立

紙台帳ベースの制度からデジタルデータベースの制度へ

- 個人番号（マイナンバー）
- 特定個人情報
- 特定個人情報保護委員会（第3者委員会）
- 特定個人情報保護評価（PIA）
- 番号法の付則（附則第6条）
 - 「政府は、この法律の施行後一年を目途として、この法律の施行の状況、個人情報の保護に関する国際的動向等を勘案し、特定個人情報以外の個人情報の取扱いに関する監視又は監督に関する事務を委員会の所掌事務とすることについて検討を加え、その結果に基づいて所要の措置を講ずるものとする」

- 明確な識別子（個人番号）に紐付けられた個人情報（特定個人情報）を用いた効率化、利便性
- 識別性の高い個人情報（特定個人情報）の保護等の明確化

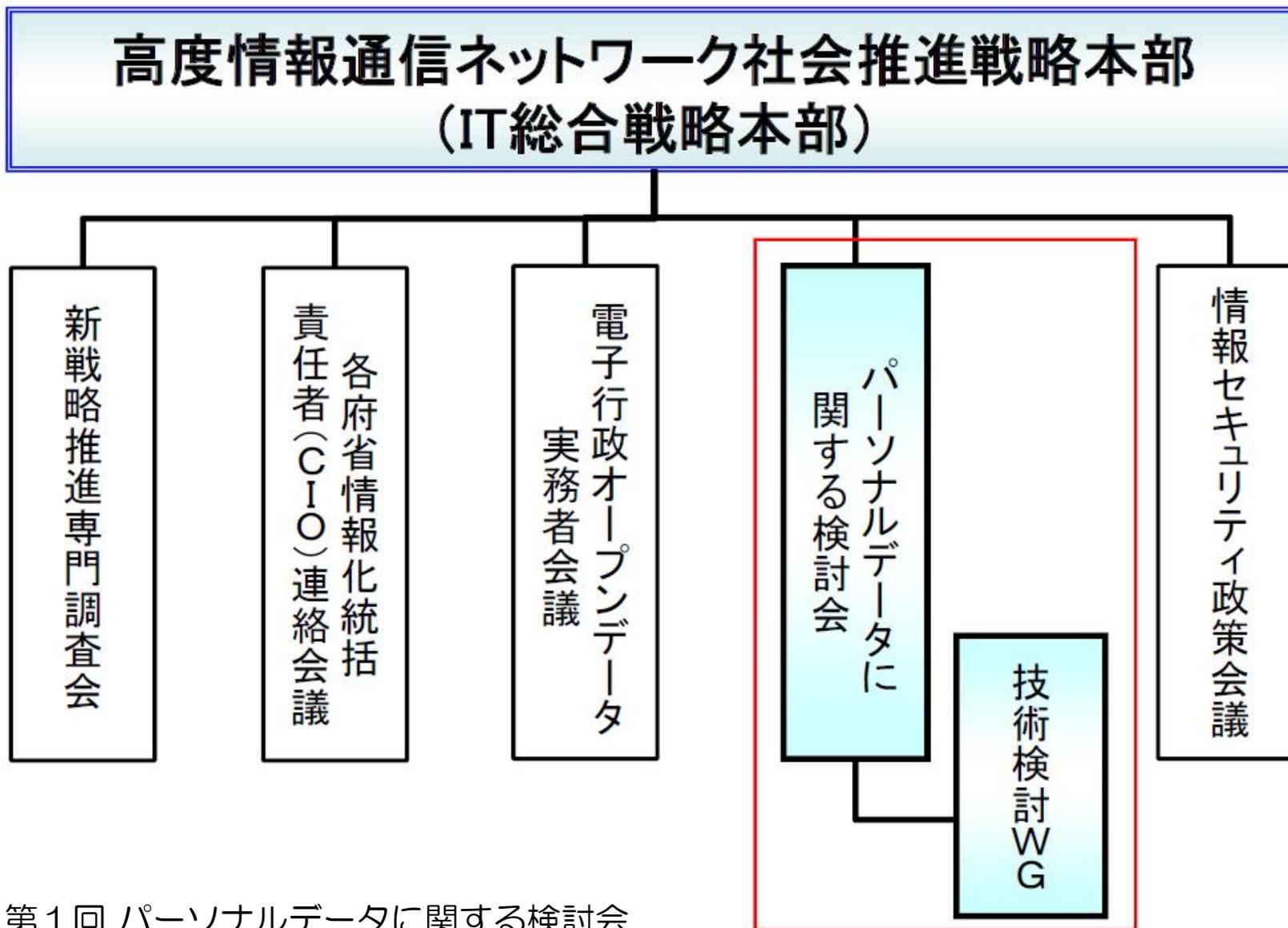
「世界最先端IT国家創造宣言」 (平成25年6月14日閣議決定)

- Ⅲ.目指すべき社会・姿を実現するための取組
- 1. 革新的な新産業・新サービスの創出と全産業の成長を促進する社会の実現
- (1) オープンデータ・ビッグデータの活用の推進
- ② ビッグデータ利活用による新事業・新サービス創出の促進
- (中略)
- 個人や機器・インフラの行動・状態等が日々刻々とITにより流通・蓄積されており、この「ビッグデータ」の利活用による、付加価値を生み出す新事業・新サービス創出を強力に推進する。
- (中略)
- また、速やかにIT 総合戦略本部の下に新たな検討組織を設置し、個人情報やプライバシー保護に配慮したパーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し、同意取得手続の標準化等の取組を年内できるだけ早期に着手するほか、新たな検討組織が、第三者機関の設置を含む、新たな法的措置も視野に入れた制度見直し方針（ロードマップを含む）を年内に策定する。
- (中略)

規制改革会議・創業等ワーキング・グループ・報告書

- 3.国民の利便性の確保や事業の効率化・低コスト化による最適なビジネス環境の整備
- (1)情報資源の有効活用
 - 現在、いわゆるビッグデータの利活用は（中略）ビッグデータの利活用による経済活性化が見込まれている。
 - ビッグデータの利活用を阻害する理由の一つとして個人情報保護法に起因する問題が指摘されており、例えば、事業者にとって、個人情報の利活用のルールが明確でないため、どのような利活用であれば適正といえるかの判断が困難である、事業者が消費者の反発によるリスクを感じ個人情報の利活用を躊躇(中略)
 - どの程度データの加工等を実施すれば個人情報保護法の制限を受けることがなくなるのかを明確化するためのガイドラインを策定する等。。。
- 【問題意識】
 - 米国FTCは、事業者が、1データに合理的な非識別化措置を講じること、2非識別化されたデータを再識別化しないことを公に約束すること、3非識別化されたデータを第三者に提供する場合、提供先が再識別化することを契約で禁止すること、の3要件を満たせば、合理的に連結可能なデータには当たらないとしている。
 - 我が国でも、ある事業者(X)が、もともと保有するデータ(元データ)と、加工等により特定の個人を識別できなくなったデータ(新データ)の両方のデータを保有し、新データのみを第三者(Y)に提供する場合において、X・Y間の契約でYによる再識別化が禁止されているときは、個人の権利利益の侵害のおそれはないのであるから、新データは「個人情報」には該当しない旨を明確化すべきではないか。

パーソナルデータに関する検討会

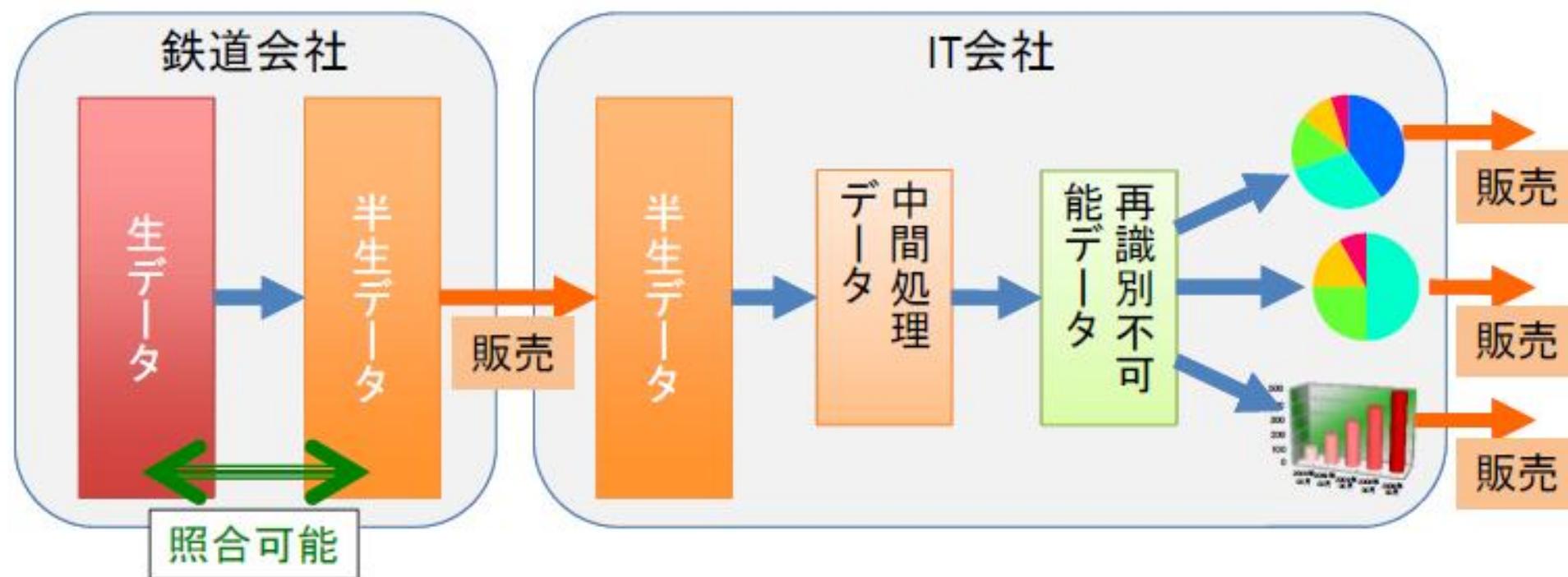


第1回 パーソナルデータに関する検討会

【資料1-3】 パーソナルデータに関する検討会の体制

パーソナルデータに関する検討会 第2回検討会での鈴木正朝構成員の提出資料

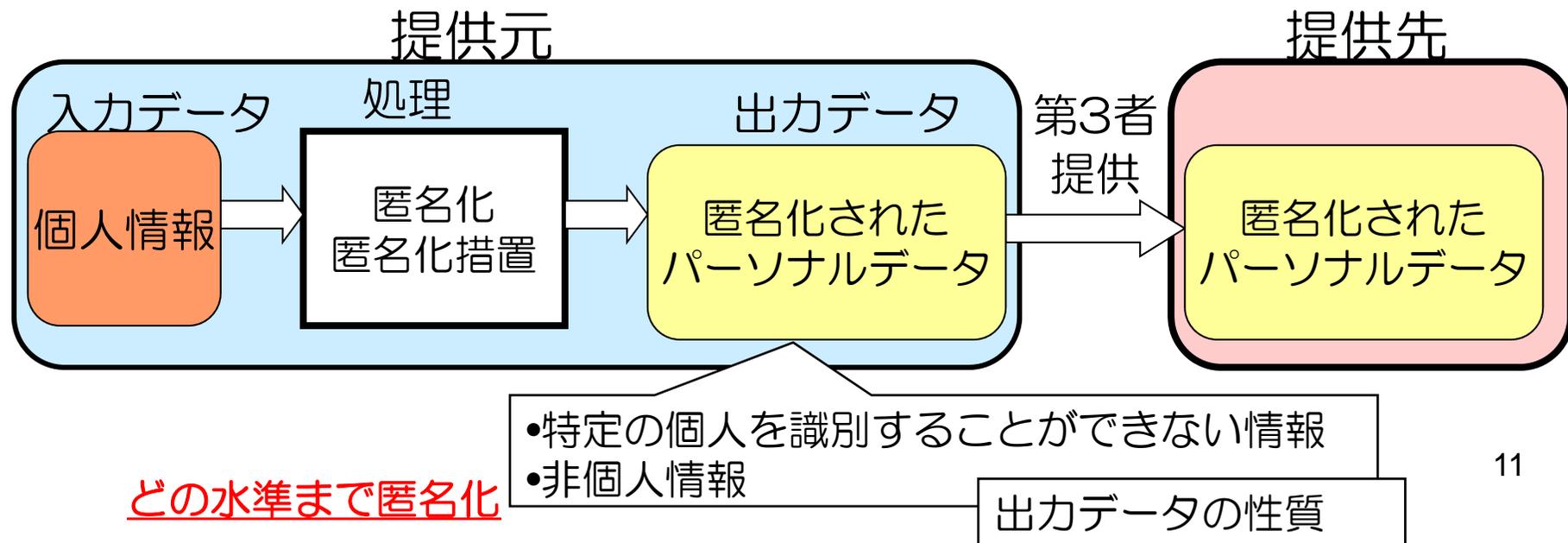
モデル1: ガイドライン対応
モデル2: 立法措置で実現



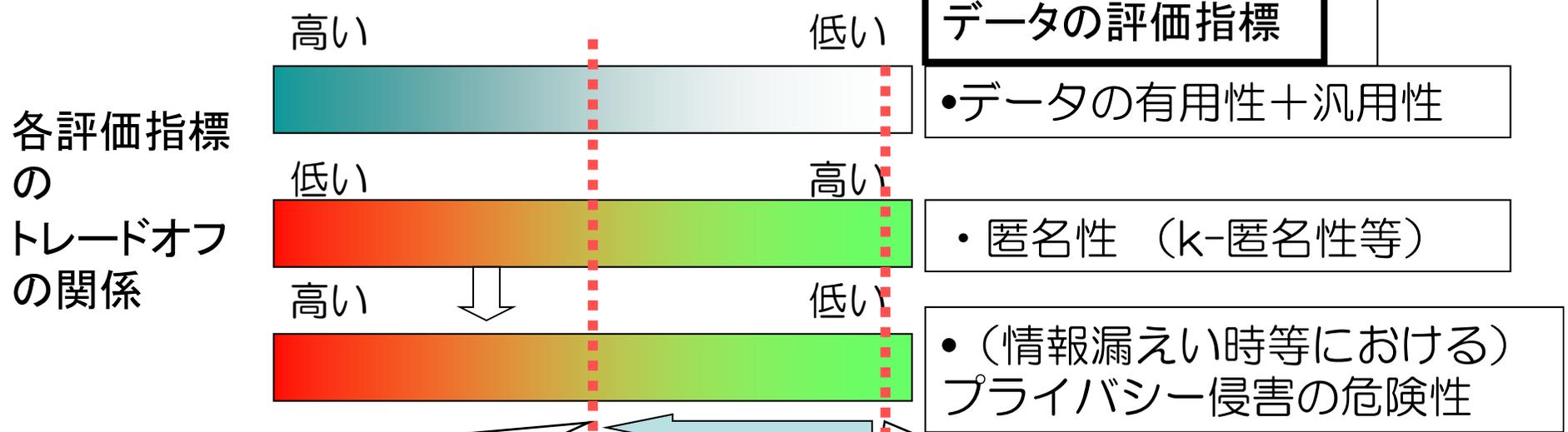
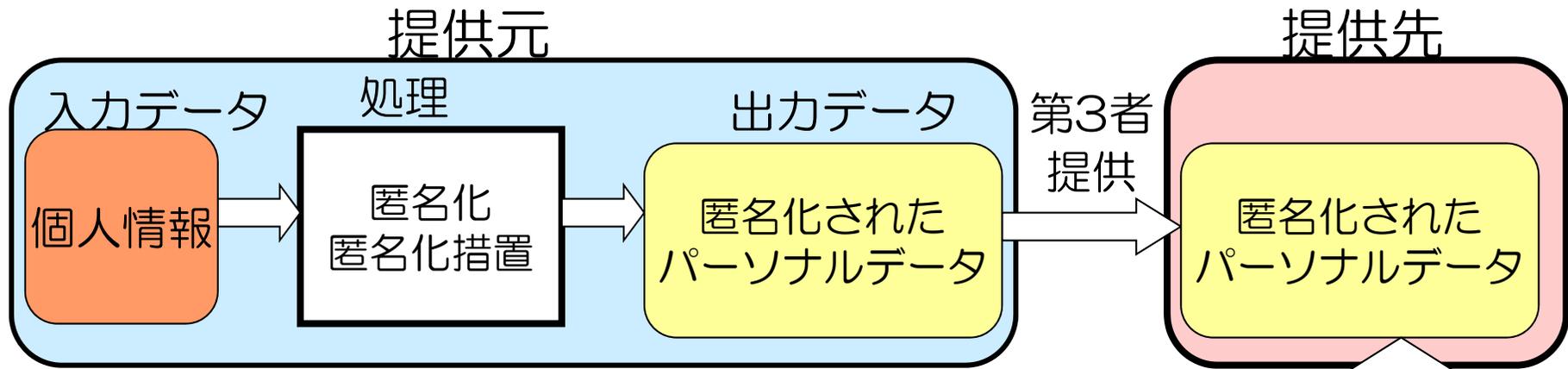
* 某交通カードの乗車履歴データ提供事案（現行法制下で違法）

技術検討WGへの要求と議論（と答え??）

- 親会（パーソナルデータに関する検討会）からのお題目
 - 匿名化されたパーソナルデータの扱い
 - ①現行法の解釈論として導入可能な「どの水準まで匿名化すれば、特定の個人を識別することができない情報（非個人情報）」となるか」の技術的内容について
 - ②新たな立法措置を前提とした匿名化措置を施した個人データの取扱いについて



「匿名性」と「有用性」のトレードオフ



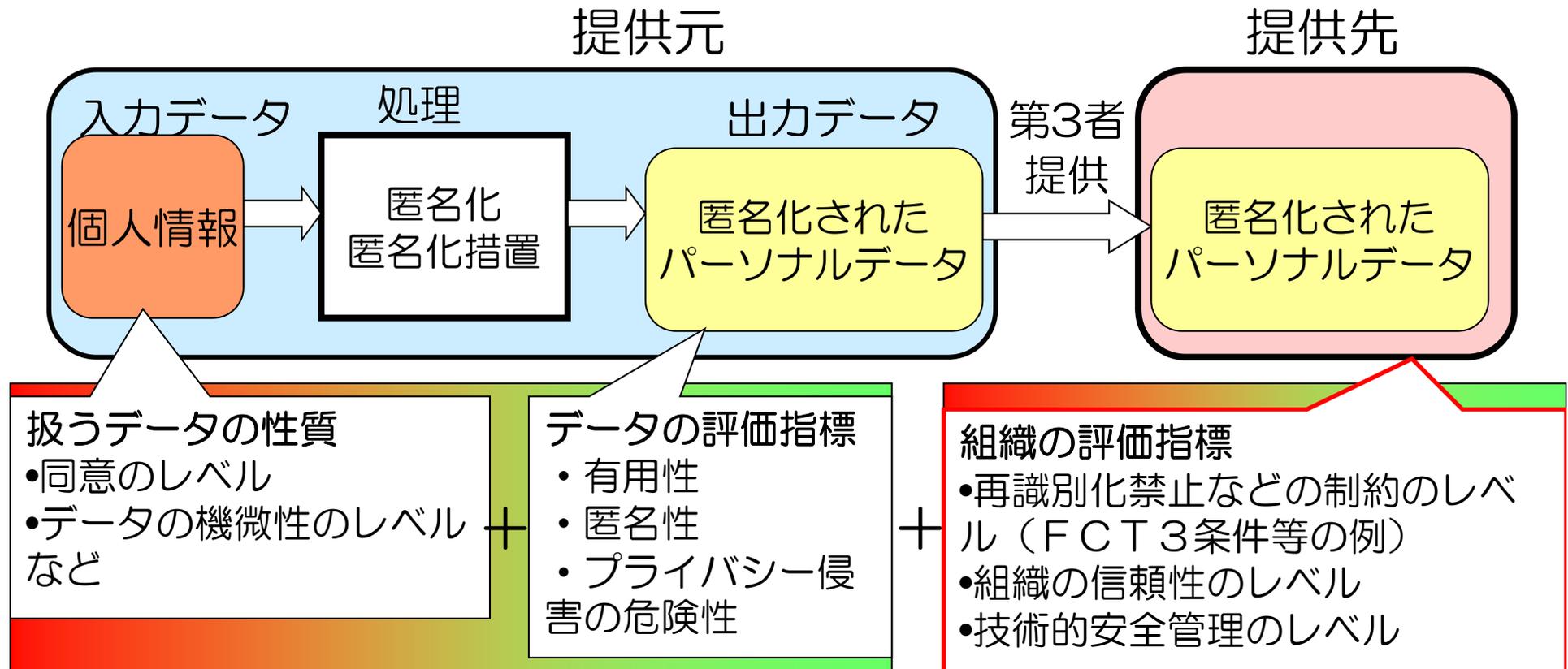
FTC 3条件等の制約により、より有用なデータを利用を可能にする

水準(レベル)

どの水準まで匿名化すれば、特定の個人を識別することができない情報 (非個人情報) となるか

データの有用性+汎用性もなくなる

松本の意見



• 松本の意見としては、

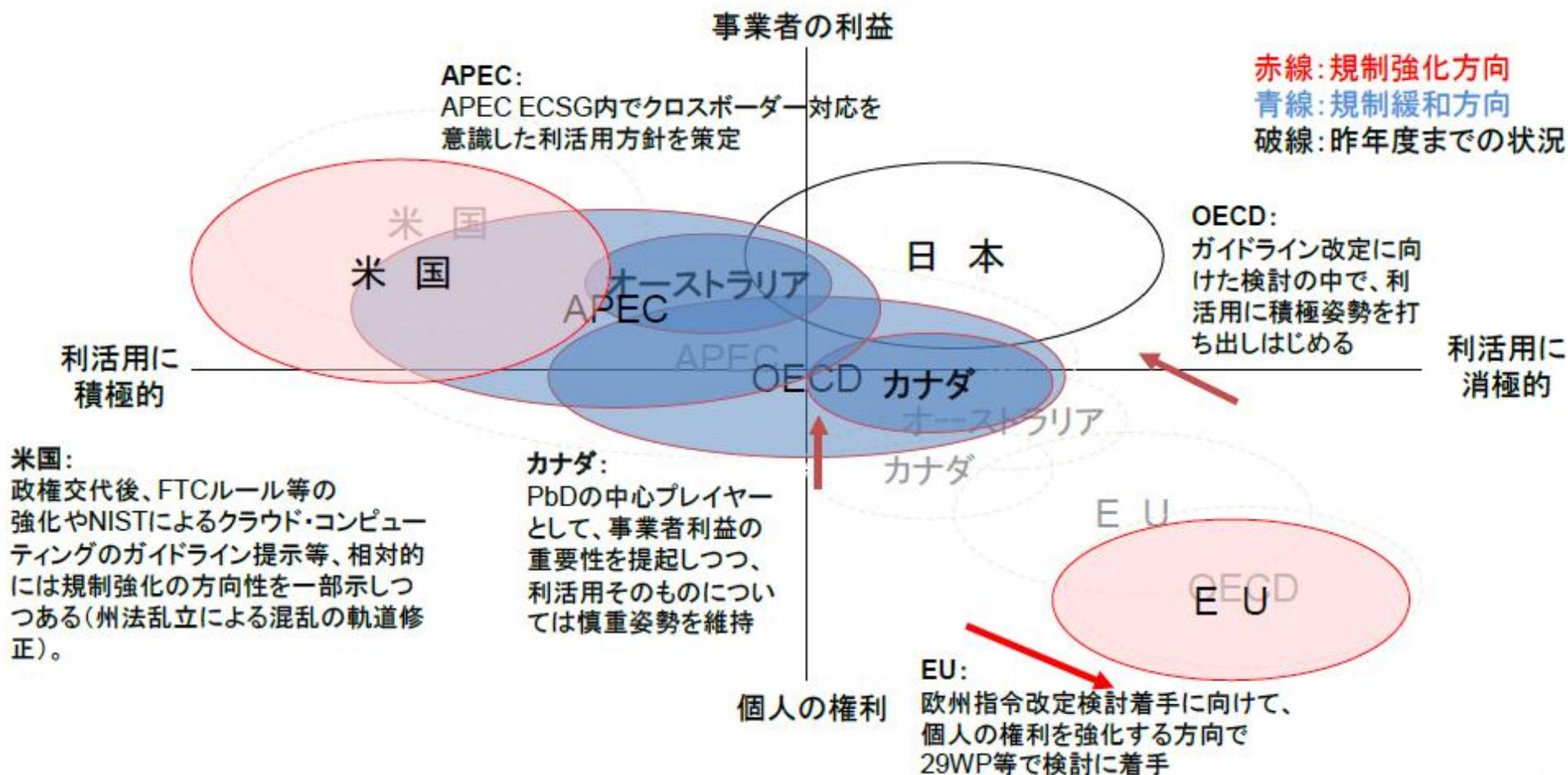
• 第3者提供データの「匿名化の水準（レベル）」だけが重要なのではなく、

-匿名性のレベル（匿名化の水準）を含め、その他の要素（機微性、組織の信頼性（ガバナンス等）、技術的信頼性（情報セキュリティ）、再識別化禁止等の契約での縛り）等の総合的なリスク評価（の指標）が重要なのではないか（PIAのガイドライン等??）。

規制とパーソナルデータの利活用の関係

「規制強化方向」≡「利用に消極的」なのか？

#規制改革会議の要望は、規制緩和？

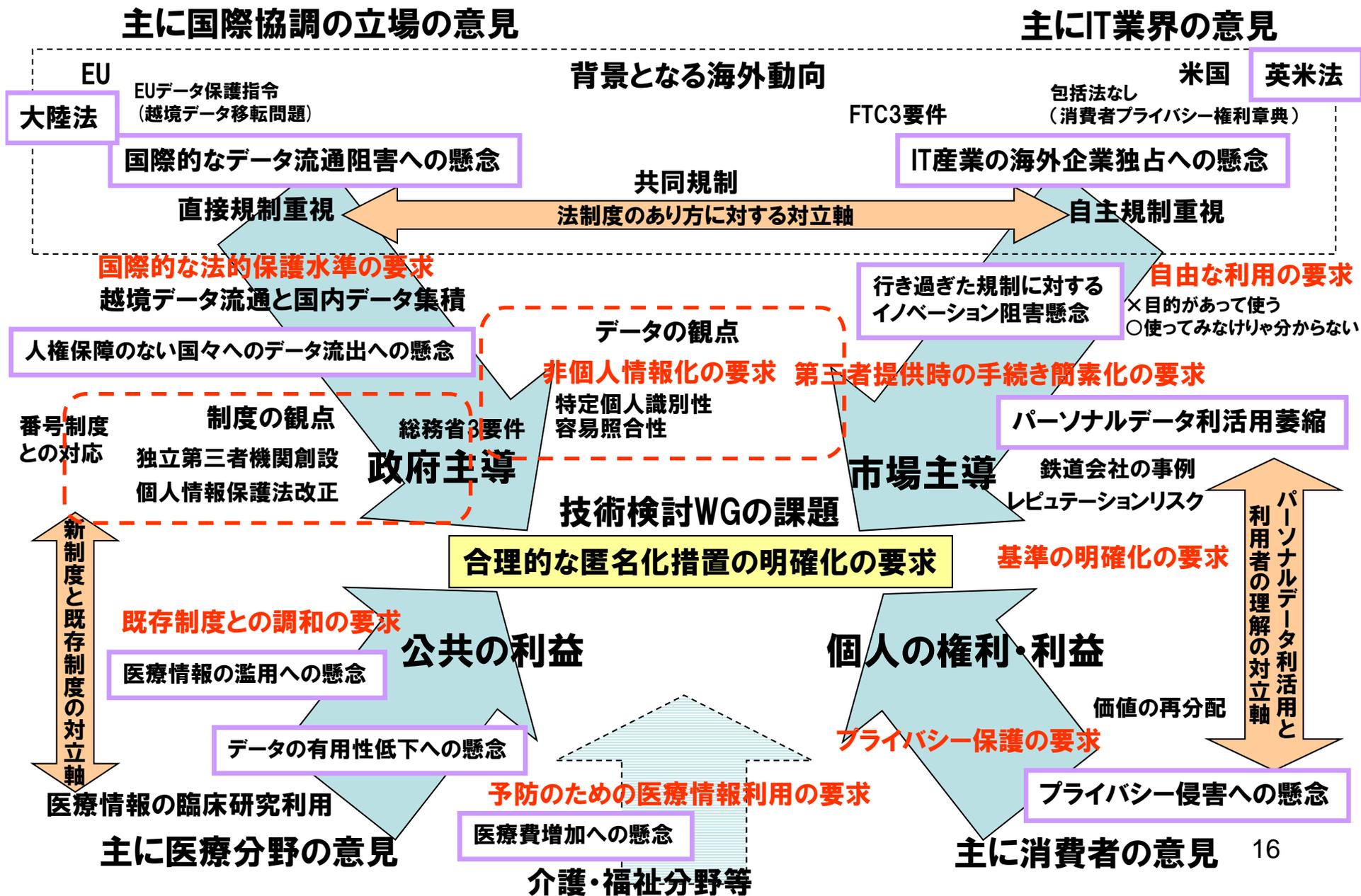


規制とパーソナルデータの利活用の関係

個人情報の利活用（と保護）に関するふたつの視点

- 新たな産業の視点（ネットビジネスなど？）
 - 規制があると産業が育たない、余計な制度はイノベーションを阻害する。
 - 業界自主ルールを尊重??
 - このままでは、セクトラルな個人情報保護法（グレーな分野がある）の米国に、個人情報を扱うビジネスを全部持っていかれてしまうという危惧????
 - 個人情報保護法の規制緩和への意見が多い
- 既存の規制の強い分野の視点
 - IT化を前提として「制度」を整備し、慣習も変えて行く努力をしないと何も動かない。
 - たとえば、医療サービス、行政サービス
 - この規制の強い分野にこそイノベーションが必要
 - 個人情報保護法の規制強化（ないしルールの明確化）への意見が多い

規制とパーソナルデータの利活用の関係・背景となる利害関係



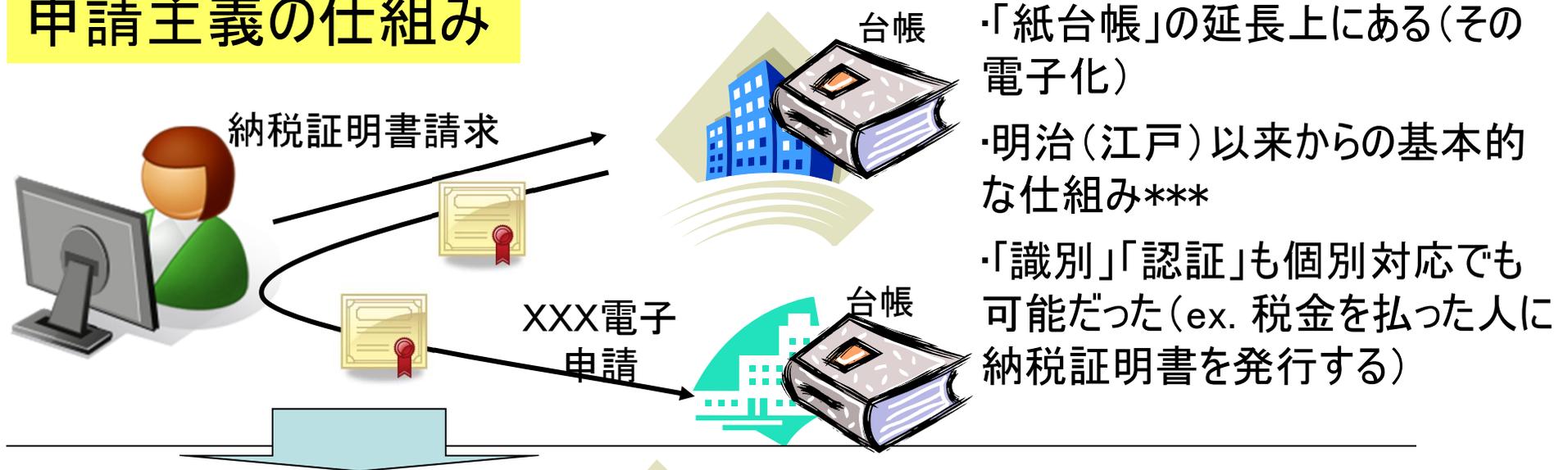
残る疑問や今後の議論??

- 狭義の匿名技術以外の技術の取り込み
 - 多様なプライバシー保護技術
 - さらなる技術と制度の噛み合わせの難しさ??
- 個人情報情報の範囲
 - 「特定個人識別」と「個人識別」の関係
- 利用目的・ビッグデータ・イノベーション
 - そもそも、規制強化、ルールの明確化、利用目的を明確化等で、ビッグデータによるイノベーションは、可能なのか?
 - 英米法的な、グレーな領域でのイノベーション
 - 大陸法的な、ビジョン先行のイノベーション
- 通信の秘密等のその他の制約を含めた日本のネットビジネスの競争力との関係

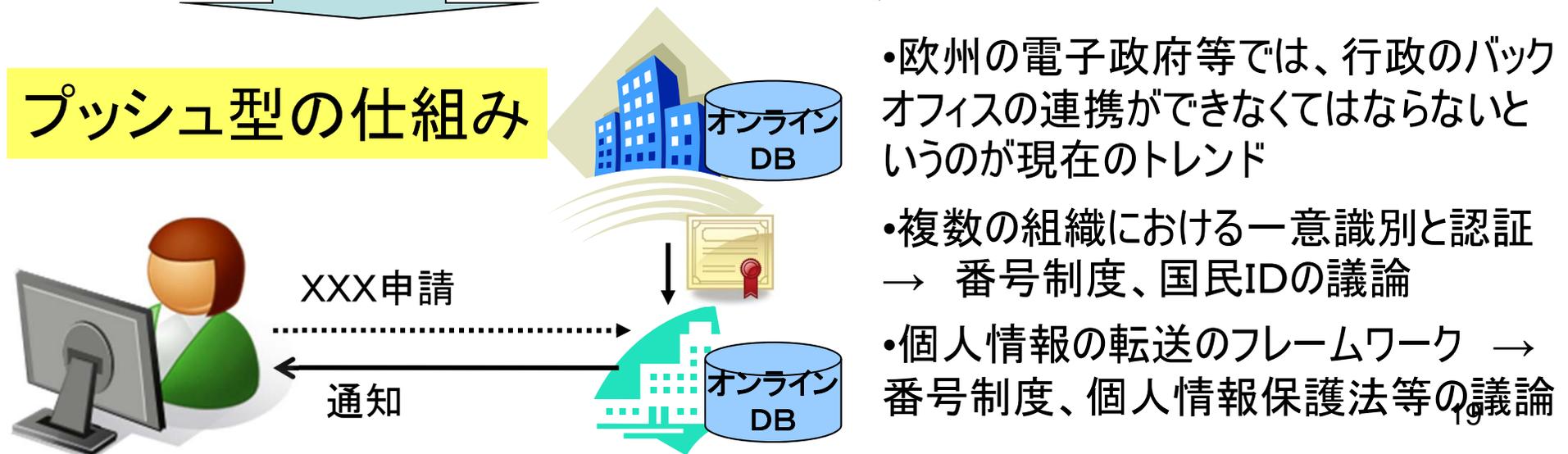
Backup

番号法の成立・申請主義からプッシュ型の行政サービスへ (紙台帳ベースの制度からデジタルデータ・ベースの制度へ)

申請主義の仕組み



プッシュ型の仕組み



番号法で必要とされた第三者機関 についての1999年頃の議論

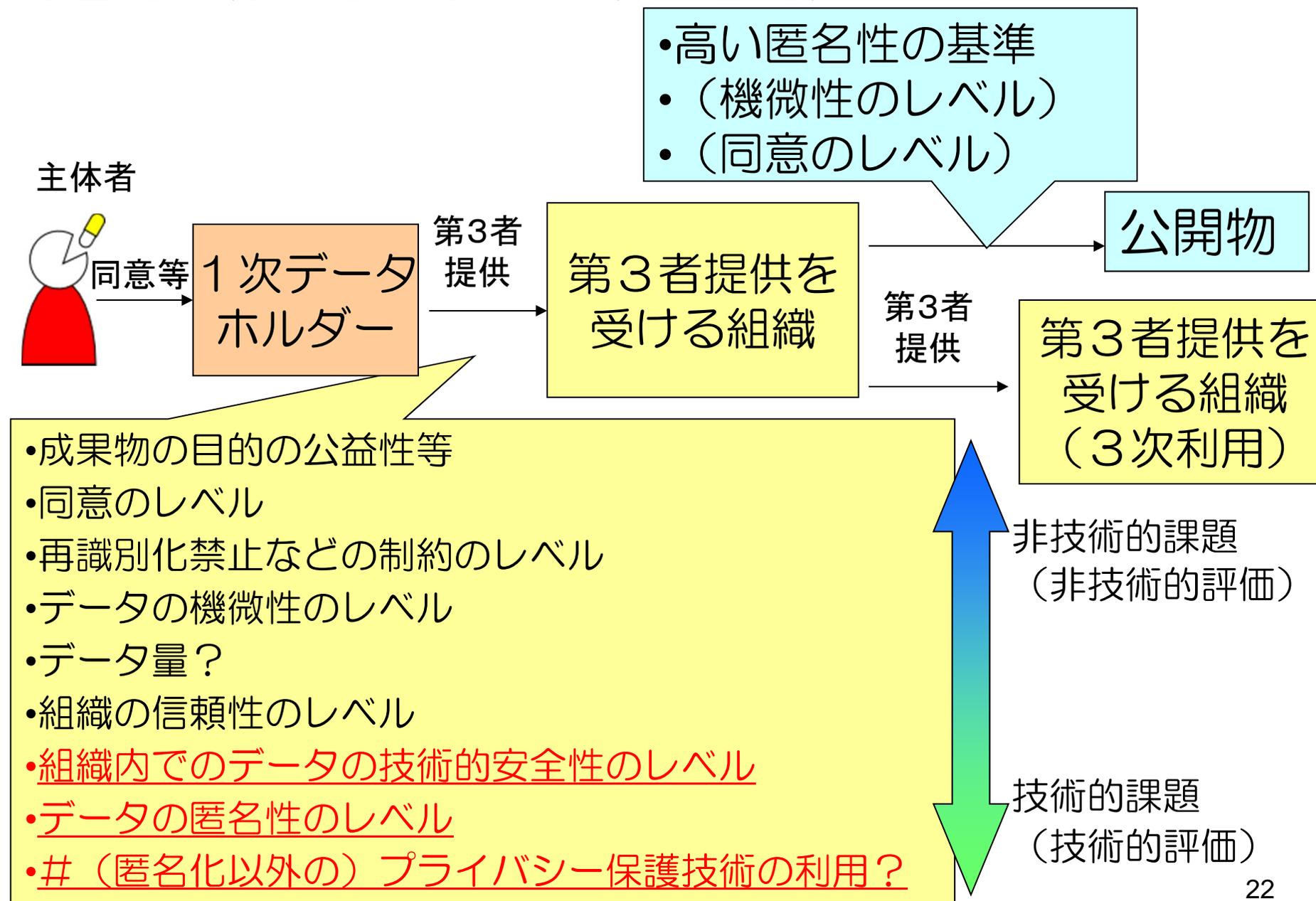
- ・ 我が国における個人情報保護システムの在り方について(中間報告)
- ・ 平成11年11月
- ・ 高度情報通信社会推進本部
- ・ 個人情報保護検討部会
- ・ <http://www.kantei.go.jp/jp/it/privacy/991119tyukan.html>
- ・ ※1 監督機関について
- ・ EUにおける「データ保護庁」のようなあらゆる分野を通じた規制権限を有する監督機関の創設は、一般多数の事業者に対する規制措置によって本来自由であるべき事業活動を大幅に制約することとなるなど、我が国の現状にかんがみると適切ではなく、また、**行政改革や規制緩和の流れにも反するところである。**
- ・ また、EU各国においても、データ保護庁は、まだ十分に機能、定着していないとの指摘もあり、このようなことから、我が国においては、基本的方向として、これを代替し得る全体として実効性ある事後救済システムの構築等を目指すことがむしろ適切であると考えられる。

・ 2013年成立の番号法では、情報連携を円滑に進めるために、（また行政改革のため？）「第三者機関」が必要という結論になった。

利活用の特性を踏まえた第3者提供の考察

- 「公表物」、「制約のないデータ販売」（コントロールの利かないパーソナルデータ）
 - 高い匿名性の基準があるべき
- データの利活用のための処理を行う組織等（コントロールの利く組織でのパーソナルデータ）への第3者提供（？）
 - 利活用ができないほどの匿名化されたパーソナルデータしか扱えなくなるのでは意味がない（成果物の有用性とのトレードオフがある）
 - ある程度の匿名性を高めたパーソナルデータ（例えば、連結可能匿名化）は、リスクインパクトを減らすために有効
 - そのための匿名性のレベルを測る「ものさし」は重要（匿名化ではなく）
 - 匿名性のレベルを含め、その他の要素（機微性、組織の信頼性（ガバナンス等）、技術的信頼性（情報セキュリティ）、再識別化禁止等の契約での縛り）等の総合的なリスク評価（の指標）が重要なのではないか（PIAのガイドライン等??）。
 - 第3者提供先の技術的な要件としては、医療情報（匿名化情報ではなく）の医療機関から委託先への要件になる「医療情報システムの安全管理に関するガイドライン」が参考になる。

利活用の特徴を踏まえた第3者提供の考察



匿名化の議論 – 匿名化は定義できるのか？

- 第三者提供時の同意を不要にしたい？という「匿名化」の要求???
- 現実には、
 - 匿名性は、グラデーション（「匿名化」のあまりにも多様な解釈）
 - 背景知識等による再識別化可能性の問題
 - ビッグデータ時代 = 多くの背景知識が容易に入手可能な時代へ？

