Internet Week 2012

意外と知らないソーシャルメディアの落とし穴

国際的な取り組み
―「プライバシーの権利」（米）と「個人データ」（EU）・「個人情報」（日）

平成24年11月21日

新潟大学 大学院実務法学研究科・法学部 教授　鈴木 正朝

わが国の「個人情報保護法」をとりまく内外の状況

国際動向

背景： インターネット / クラウド/ビッグデータ/ライフログ

① OECD: 「プライバシーガイドライン」改正要綱

② APEC: 「CBPR(APEC越境プライバシールール)制度」

③ EU: 「個人データ保護指令」「e-プライバシー指令」,「個人データ保護規則案」

④ 米国:「消費者プライバシー権利章典」, 個別法, (集団訴訟＋懲罰的損害賠償)

国内動向

背景： 少子高齢人口減少社会/社会保障と税の一体改革

① 一般法: 「個人情報保護法」改正の動向 (消極的)

② 特別法: 「マイナンバー法案」、「医療個人情報保護法案」、「政府CIO法案」

→ 新しい行政組織: 「番号情報保護委員会」、「政府CIO 」

③ 告示: 「個人情報保護ガイドライン」(弥縫策)

④ 国内規格: JIS Q 15001 (法との不整合)

⑤ 民間認証制度: プライバシーマーク制度 (問題山積)

米国プライバシー保護法制（個別法）

全業界を包括する一般法はなく次の個別法により保護している。なお、米国には、強力なプライバシーの権利の民間保護団体と司法救済（集団訴訟・懲罰的損害賠償等）がある。

(1) 公正信用報告法

Fair Credit Reporting Act, 1970

(2) プライバシー法

Privacy Act, 1974

(3) 家族の教育上の権利及びプライバシー法

Family Educational Rights and Privacy Act, 1974

(4) 情報公開法

Freedom of Information Act, 1974

米国プライバシー保護法制（個別法）

(5)外国諜報活動偵察法

Foreign Intelligence Surveillance Act, 1978

(6) 金融プライバシー権法

Right to Financial Privacy Act, 1978

(7) プライバシー保護法

Privacy Protection Act, 1980

(8) ケーブル通信政策法

Cable Communications Policy Act, 1984

(9) 電気通信プライバシー法

Communications Privacy Act, 1984

(10)ビデオ・プライバシー保護法

Video Privacy Protection Act, 1988

米国プライバシー保護法制（個別法）

(11)ポリグラフ（嘘発見器）からの従業員保護法
Employee Polygraph Protection Act, 1988

(12) 電話加入者保護法
Telephone Concumer Protection Act, 1991

(13) 運転免許プライバシー保護法
Driver's Privacy Protection Act, 1994

(14) 電気通信法
Telecommunications Act, 1996

(15) 子どものオンライン上のプライバシー保護法
Children's Online Privacy Act, 1998

(16)金融サービス近代化法
Financial Modernization Services Act, 1999
GLBA: Gramm-Leach-Bliley Act

米国プライバシー保護法制（個別法）

(17)連邦取引委員会法

FTCA : Federal Trade Commission Act, 1914

(18)健康保険に関する携行性及び説明責任に関する法律

HIPAA: Health Insurance Portability and Accountability Act, 1996, 2002

(19)経済的及び臨床的健全性のための医療情報技術に関する法律

HITECH: Health Information Technology for Economic and Clinical Health Act , 2009

(20) 米国愛国者法

USA Patriot : Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

米国消費者プライバシー権利章典（2012年2月）

Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy

個人データ

集積されたデータを含むあらゆるデータであって、特定個人と結びつき得る（Linkable）もの。

→特定のコンピュータまたはほかの装置と結びつくデータを含む。

個人データ概念が特定個人の識別情報（PII）から拡大。

例：スマートフォン等の識別子

EU個人データ保護法制（包括法）

(1)「個人データの自動処理に係る個人の保護に関する条約」
　　Convention for the Protection of Individuals with regard to Auto- matic Processing of Personal Data, 1985
(2)「個人データ保護指令」
　　Data Protection Directive, 1995
(3)「eプライバシー指令」
　　e-Privacy Directive, 2002
(4)「eプライバシー指令」の一部改正
　　Telecom Reform Package, 2009

EU個人データ保護法制（包括法）

(5)「一般データ保護規則提案」（2012年1月）

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

EU個人データ保護法制（包括法）

(2)「個人データ保護指令」（1995年）

第2条(a)　個人データ（personal data）

＜特定個人の識別（可能）情報＞

　識別された自然人、又は識別されうる自然人に関する全ての情報を意味するものとする。

　識別されうる人とは、直接的又は間接的に、とりわけ識別番号又は当該人物の肉体的、生理学的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な1つ以上の要素を参照することによって、識別が可能な人のことである。

EU個人データ保護法制（包括法）

(5)「一般データ保護規則提案」（2012年1月）

第4条(2)　個人データ

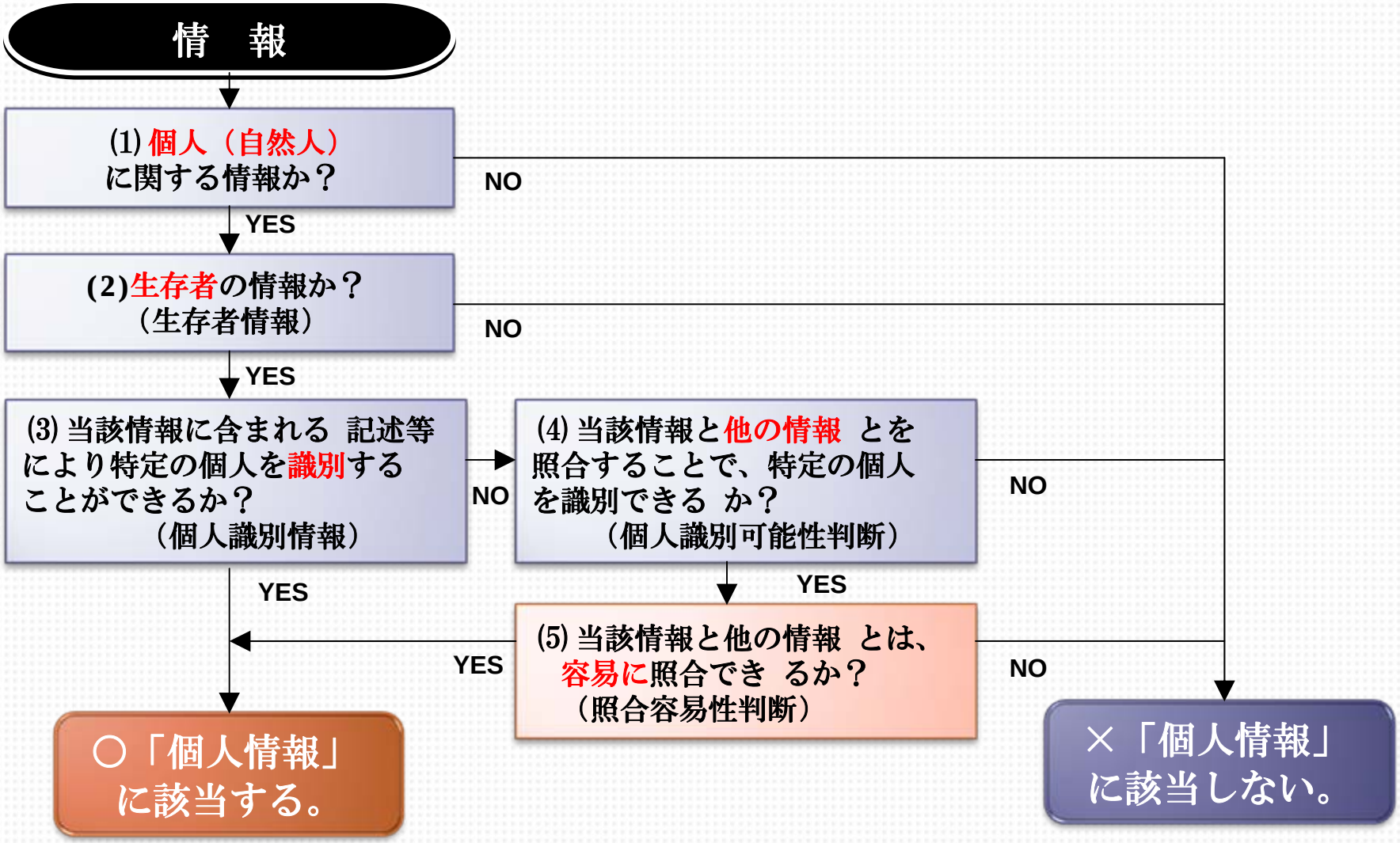
＜データ主体に関する全ての情報＞

第4条(1)　データ主体

　識別された自然人、又は管理者、若しくは他の自然人若しくは法人によって合理的に利用される可能性の高い手段によって、直接的若しくは間接的に、とりわけ識別番号、位置データ、オンライン識別子、若しくは当該人物の肉体的、生理学的、遺伝的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な1 つ以上の要素を参照することによって、識別されうる自然人

日本:「個人情報」の定義

「個人情報取扱事業者」の場合 （個人情報保護法2条1項）



個人情報保護法制の全体構造

「個人情報の保護に関する法律」

「基本法」部分

第１章　総則（目的・基本理念）
第２章　国及び地方公共団体の責務等
第３章　個人情報の保護に関する施策等

＊第５章　雑則（権限又は事務の委任、政令への委任など）

民間部門の「一般法」部分

第４章　個人情報取扱事業者の義務等
第５章　雑則　（適用除外）
第６章　罰則

「行政機関の保有する個人情報の保護に関する法律」

「独立行政法人等の保有する個人情報の保護に関する法律」

地方公共団体による「条例」
＊市区町村の「個人情報保護条例」
＊都道府県の「個人情報保護条例」

個人情報取扱事業者
（民間企業等）
民間部門

行政機関　独立行政法人等　地方公共団体等
公的部門

日本の現状と欧米の動向との違い

本人識別性	情報の重要度	日本	EU	米国
あり PII Personal Identifiable Information	①重要な特定個人の識別情報 ・センシティブ情報（EU) ・プライバシーの権利に係る情報（米）	○	◎	○
	②一般的な特定個人の識別情報	○	○	△
	③ゴミのような特定個人の識別情報	○	×	×
なし Non-PII	①危ない“識別子”等の情報 （Linkable）	×	○	○
	②その他の情報	×	×	×

SNS時代のプライバシー・個人情報保護

(1)SNS等の主要事業主体:
　　米国企業（Facebook, Twitter, Googleなど）
(2)適用法（プライバシーの保護）：
　　米国法
　　日本法が適用されない事例も登場
　　（例：Googleサジェスト機能仮処分事件）
(3)実質的な利用者（消費者）保護：
　　主要事業主体のサービス仕様に依存する。

→近年、日本政府及び日本の法制度の役割が急速に後退している。
　また、日本は、国際的なルール・メイキングの舞台から存在感が消えている。

対象情報の内容の質（機微性やプライバシー性）を踏まえずにルールを決定できるか？

情報の“機微性（sensitivity）”

形式的判断基準

特定個人の識別情報（PII)

実質的判断基準

情報の機微性（sensitivity）

個人の尊重の理念＋情報の機微性評価

＝プライバシー性の評価に近接しないか？

（公開・非公開を問うのか？）

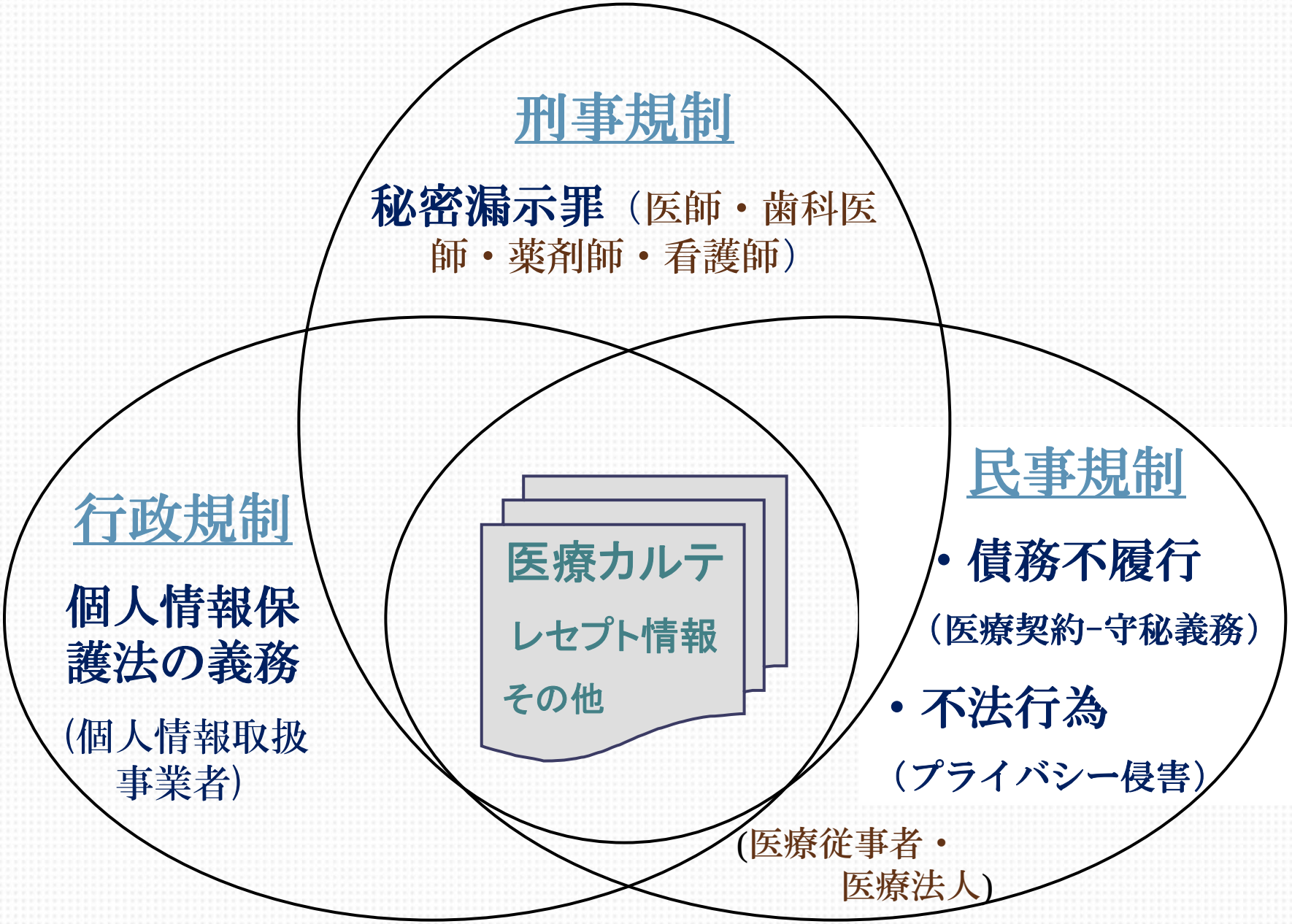
対象情報の性質だけでルールを決定できるか？

“Privacy by Design”の時代

「対象情報」の性質のみに着目して法律の適用及び適法・違法の判断をなし得るようなルールのあり方でいいのか？

①どのような対象情報を取り扱うのか？
　－匿名化処理の法的評価、機微性の法的評価
②どのような者が情報を取り扱うのか？
　－「事業」性は問うか？
③どのようなビジネスモデルか？
④どのような情報システム（データ連係）でそれを実現するのか？
⑤誰（全プレーヤー）がどのように運用するのか？

を総合的に評価できるルール作りが必要である。
特に、データ連係の情報システムの評価が重要！

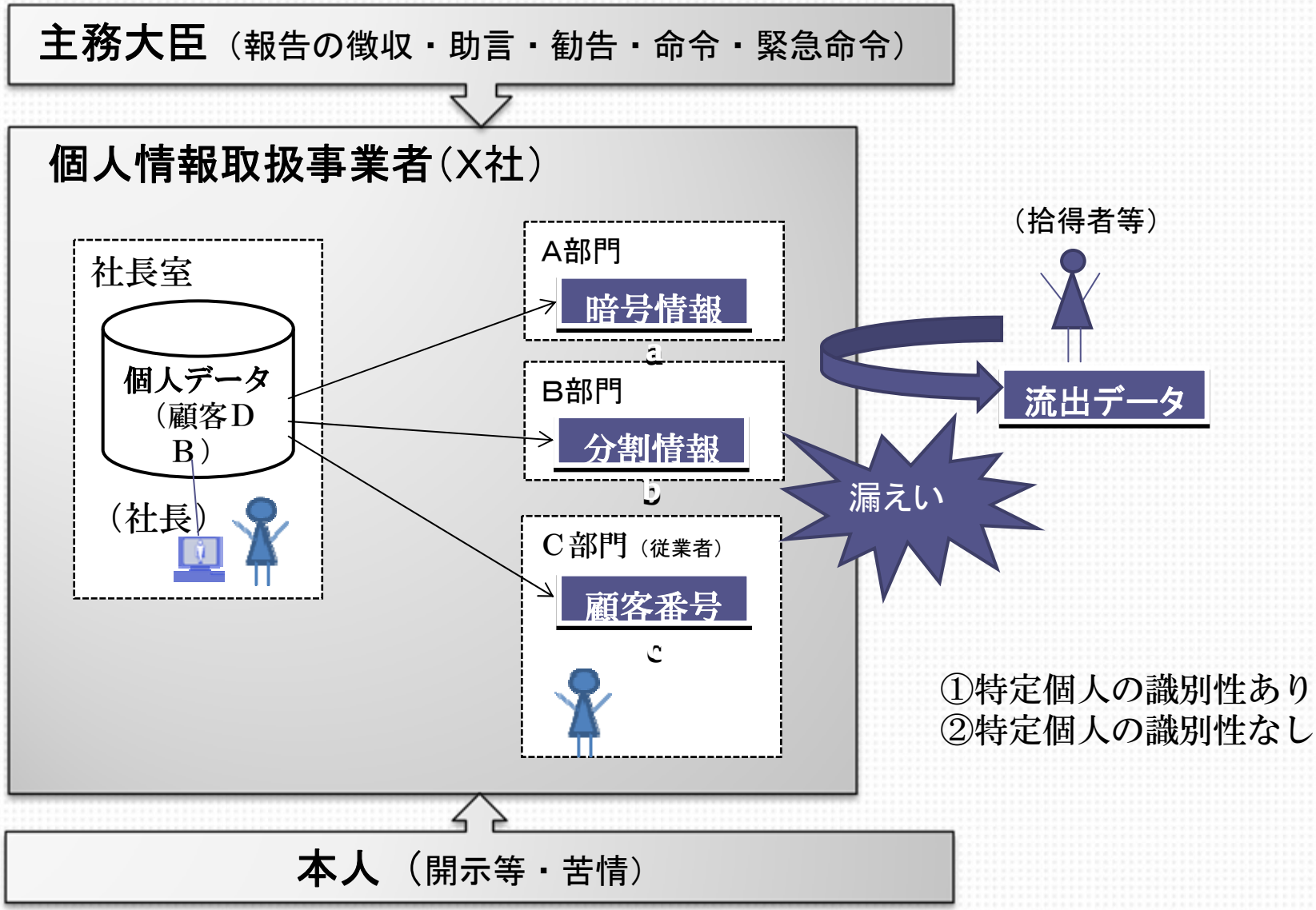

刑事規制
秘密漏示罪（医師・歯科医師・薬剤師・看護師）
行政規制
個人情報保護法の義務
(個人情報取扱事業者)
医療カルテ
レセプト情報
その他
民事規制
• 債務不履行
（医療契約−守秘義務）
• 不法行為
（プライバシー侵害）
(医療従事者・医療法人)

「データ連係」するためには

	刑事規制	民事規整	行政規制	データ連係
A	○	○	○	○
B	×	○	○	×
C	○	×	○	×
D	×	○	×	×

→刑事・民事の守秘義務（プライバシー権に係る情報等秘密情報）と（医療）個人情報保護法上の義務を遵守する必要がある。

「漏えい」の定義ー下記 a,b,cは漏えいになるか？

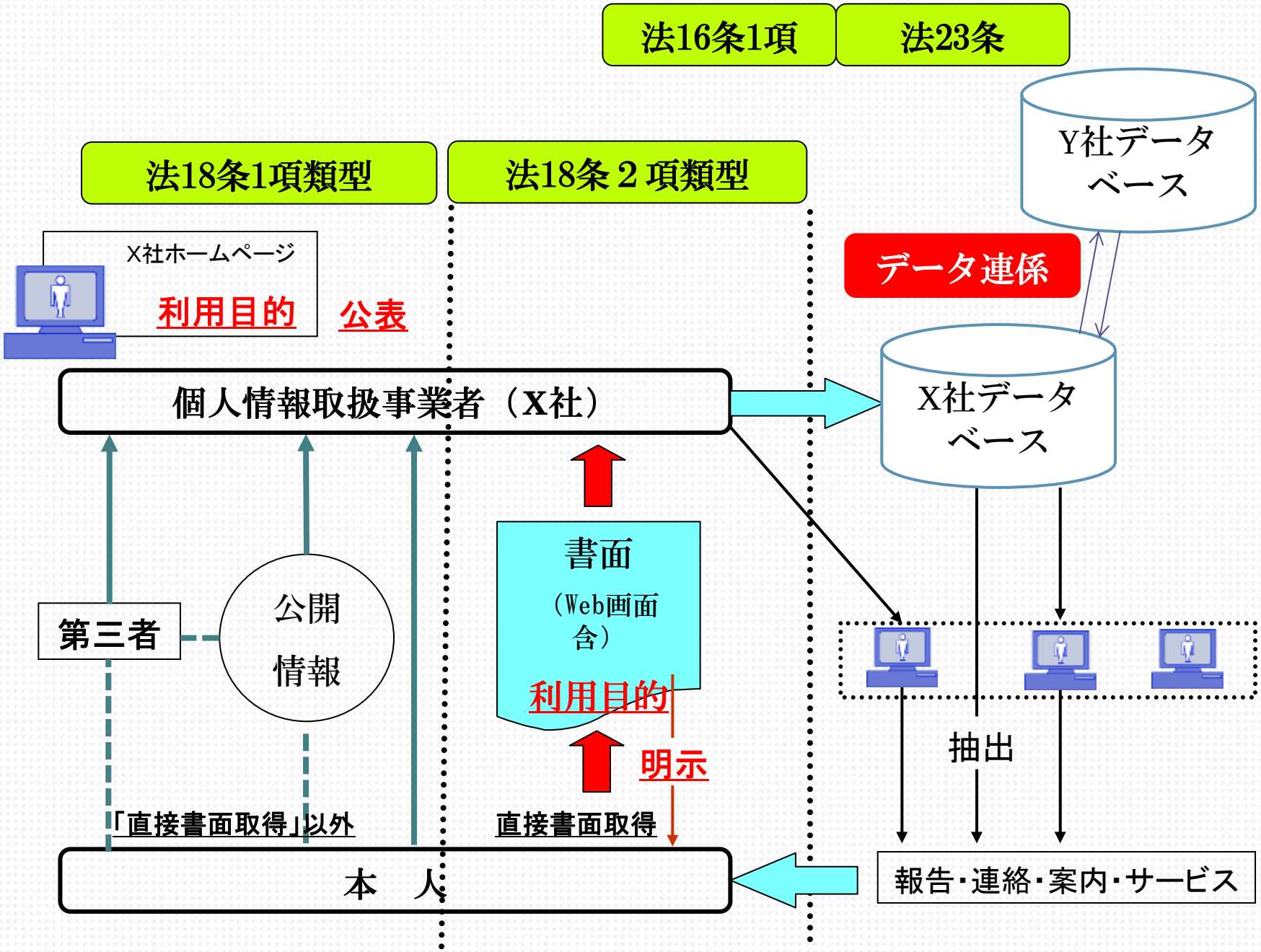


①特定個人の識別性あり
②特定個人の識別性なし

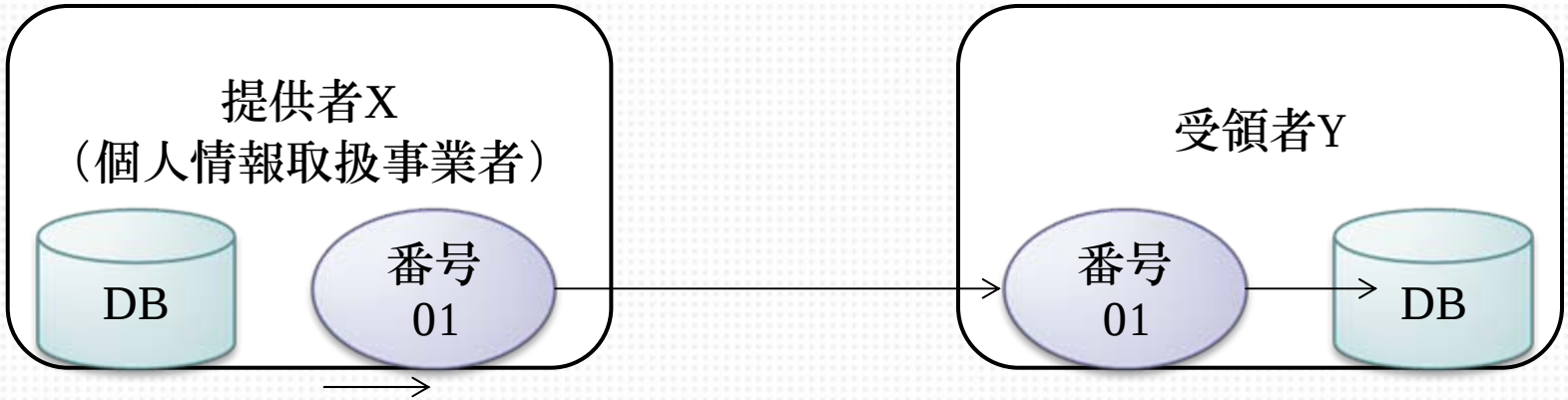
「識別」の解釈：誰が識別するのか？

その主語は条文上明らかではない。特定個人の「識別」可能性判断の主体は解釈上の論点となる。

(1)「事業者」基準：個人情報を取り扱う事業者を基準として判断する。
(2)「従業者」基準：個人情報を取り扱う事業者の従業者等自然人を基準として判断する。
(3)「本人」基準：情報主体である本人を基準として判断する。
(4)「一般人」基準：社会一般の人を基準として判断する。


法16条1項
法23条
法18条1項類型
法18条２項類型
Y社データベース
データ連係
X社ホームページ
利用目的
公表
個人情報取扱事業者（X社）
X社データベース
書面
（Web画面含）
利用目的
明示
第三者
公開情報
抽出
「直接書面取得」以外
直接書面取得
本　人
報告・連絡・案内・サービス

識別子と第三者提供（23条）の適用関係



提供者X	→	受領者Y	Xの法適用の有無
特定個人識別性あり ○	→個人 データ→	特定個人識別性あり ○	あり ○
特定個人識別性なし ×	→番号→	特定個人識別性なし ×	なし ×
特定個人識別性なし ×	→番号→	特定個人識別性あり ○	なし ×
特定個人識別性あり ○	→個人 データ→	特定個人識別性なし ×	経産省 ： あり○ 有力説 ： なし×

識別子と第三者提供（23条）の適用関係

1.第三者提供における「識別」性判断の主体は？
(1) 提供者基準
(2) 受領者基準
(3) 一般人基準

2.「識別」性の有無を判断をする際の“範囲”は？

3.「照合」性判断における主体は？
(1) 事業者基準（事業者全体から評価する。）
(2) 従業員基準（データを取り扱っている自然人を基準に(容易)照合性判断を行う。）

＜個人に関する情報＞

③番号（識別子） 共通番号，ケータイID，携帯電話番号,メアド,クレジット番号，顧客・社員番号，車のナンバー等

①識別情報（本人確認情報）

〇社会的情報
- 氏名
- 自宅住所（勤務先）
- 生年月日
- 年齢

〇生物学的情報
- 性別
- 肖像

- 位置情報などライフログ
- 身体的特徴（髪，目の色等）
- 生体情報（指紋，掌紋，虹彩，遺伝子等）

②属性情報（その他の情報）

〇内心の秘密
- 思想信条（思想良心の自由）
- 宗教（信教の自由）
- 趣味嗜好，性生活等

〇医療情報
- 病歴（カルテ，レセプト）・介護
- 健康状態，体力

〇個人信用情報
- 資産状況（不動産，金融財産，貴金属等保有状況，預貯金等）
- クレジットカード情報・納税・年金

〇購買履歴　〇通信通話情報

〇家族・身分関係　・戸籍情報（族称・僭称），内縁関係

〇経歴・社会活動等　・学歴，職歴，資格，所属団体，・政治活動，労働運動・犯罪歴，反社情報等ブラックリスト

本　人　（個人の尊厳）

イメージ・評価

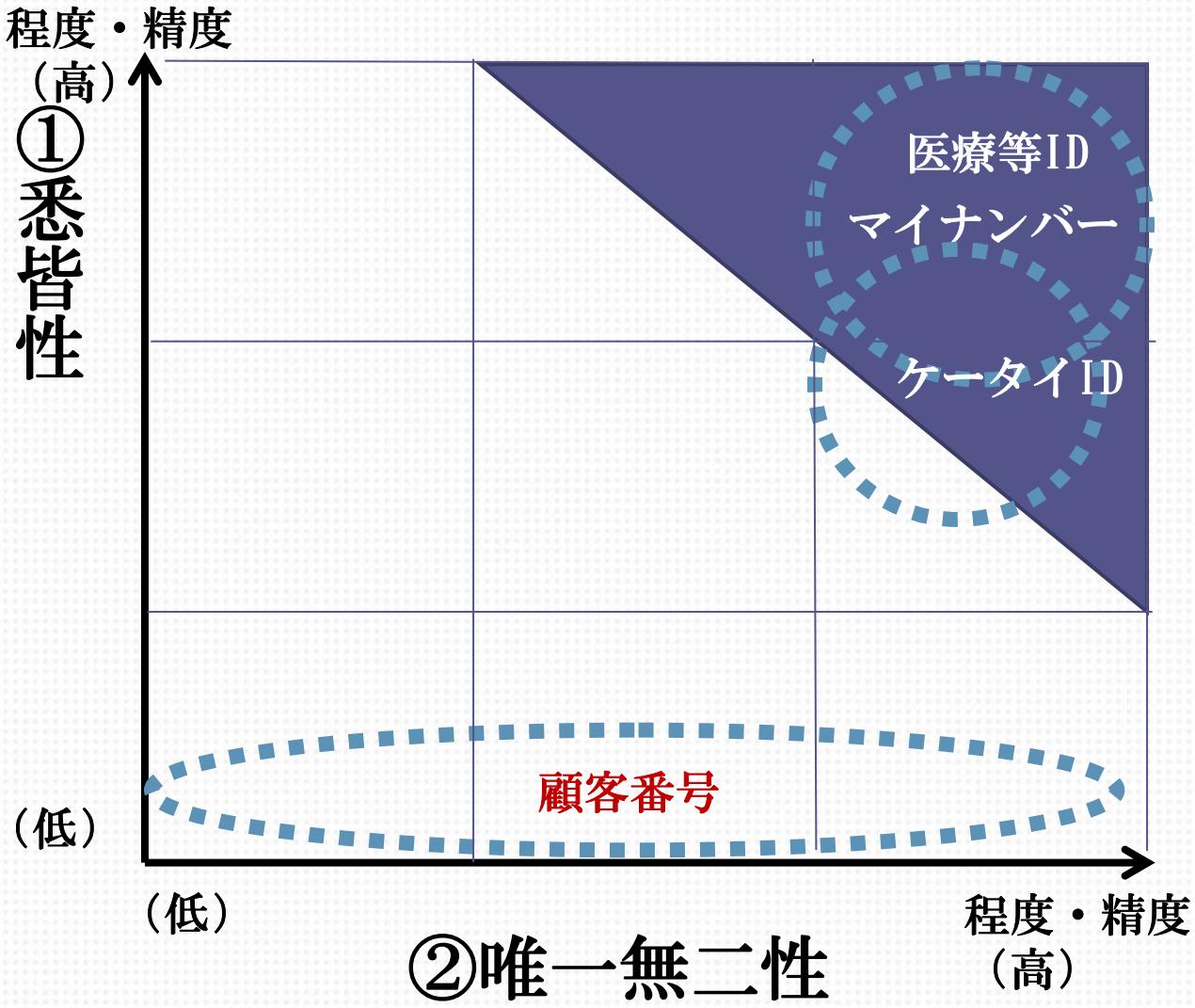
non-PII 系の「識別子」は保護すべきか？

－規制対象の対象情報＝“**特定個人の識別情報**”
「特定個人が識別されなければ本人被害は生じない」のか？
＝Personal Identifiable Information: **PII**　だけに個人の権利利益の侵害があるのか？

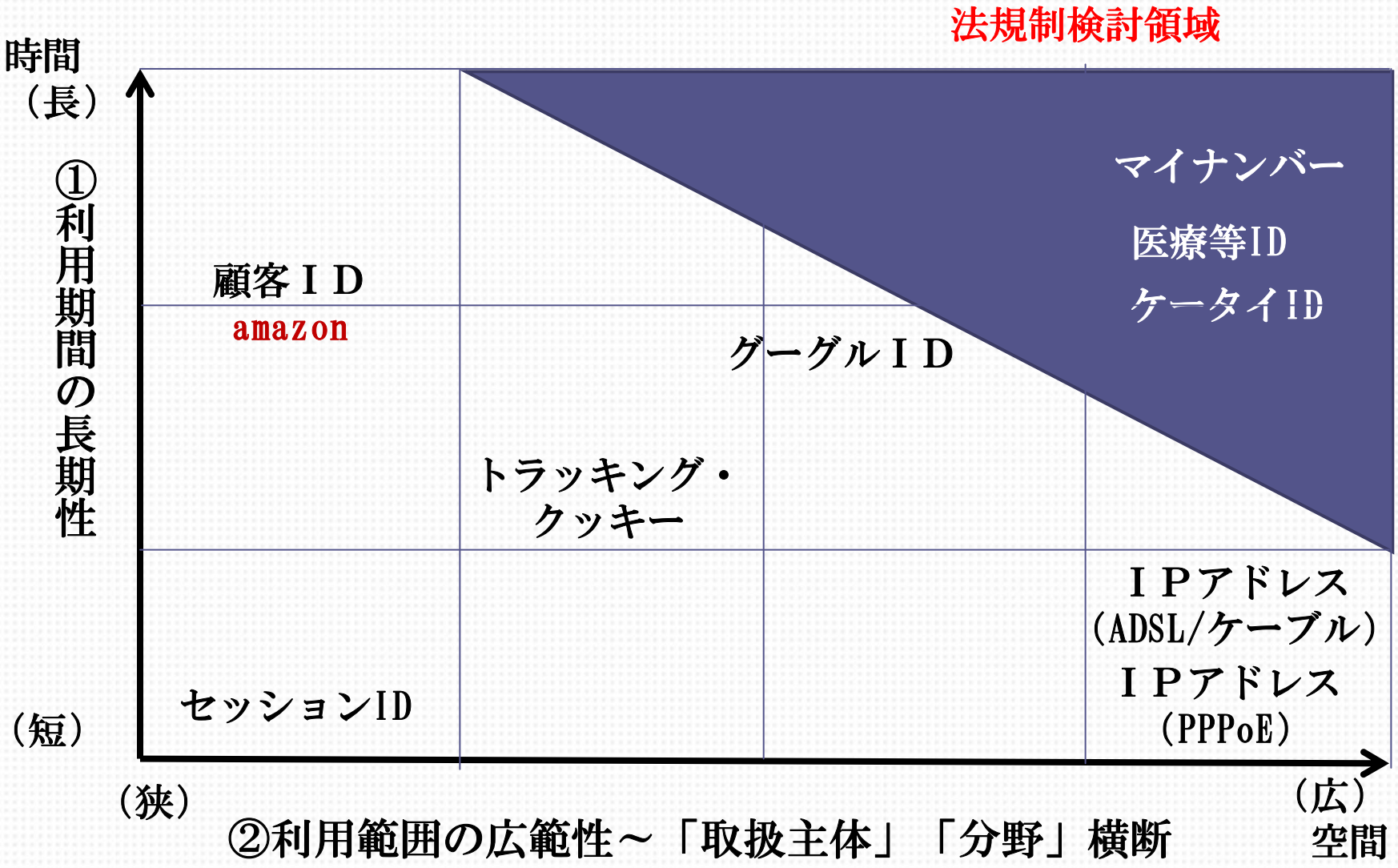
non-PII（DBと照合できない一定の性質を有する識別子等）におけるプライバシー侵害（Privacy Impact）の程度を評価をしなくていいのか？
（→Privacy Impact Assessment: **PIA**）

＊「Identifiable（米国法の概念）=識別（日本法の概念」ではない。
・国際規格の概念との乖離
→越境データ連係に影響あり

識別子の強度～悉皆性・唯一無二性



識別子の法的評価～時間軸と空間軸



PIIだけを対象情報としていいのか？

例えばゲノム（遺伝子情報）は究極の「個人情報」または究極の「プライバシー権に係る情報」と言われてきたが、それは本人一人の判断で公開できる情報か？

①公共的利益	例：ビッグデータ（ライフログ）
②中間的利益？	例：ゲノム情報
③個人的利益	プライバシーの権利に係る情報

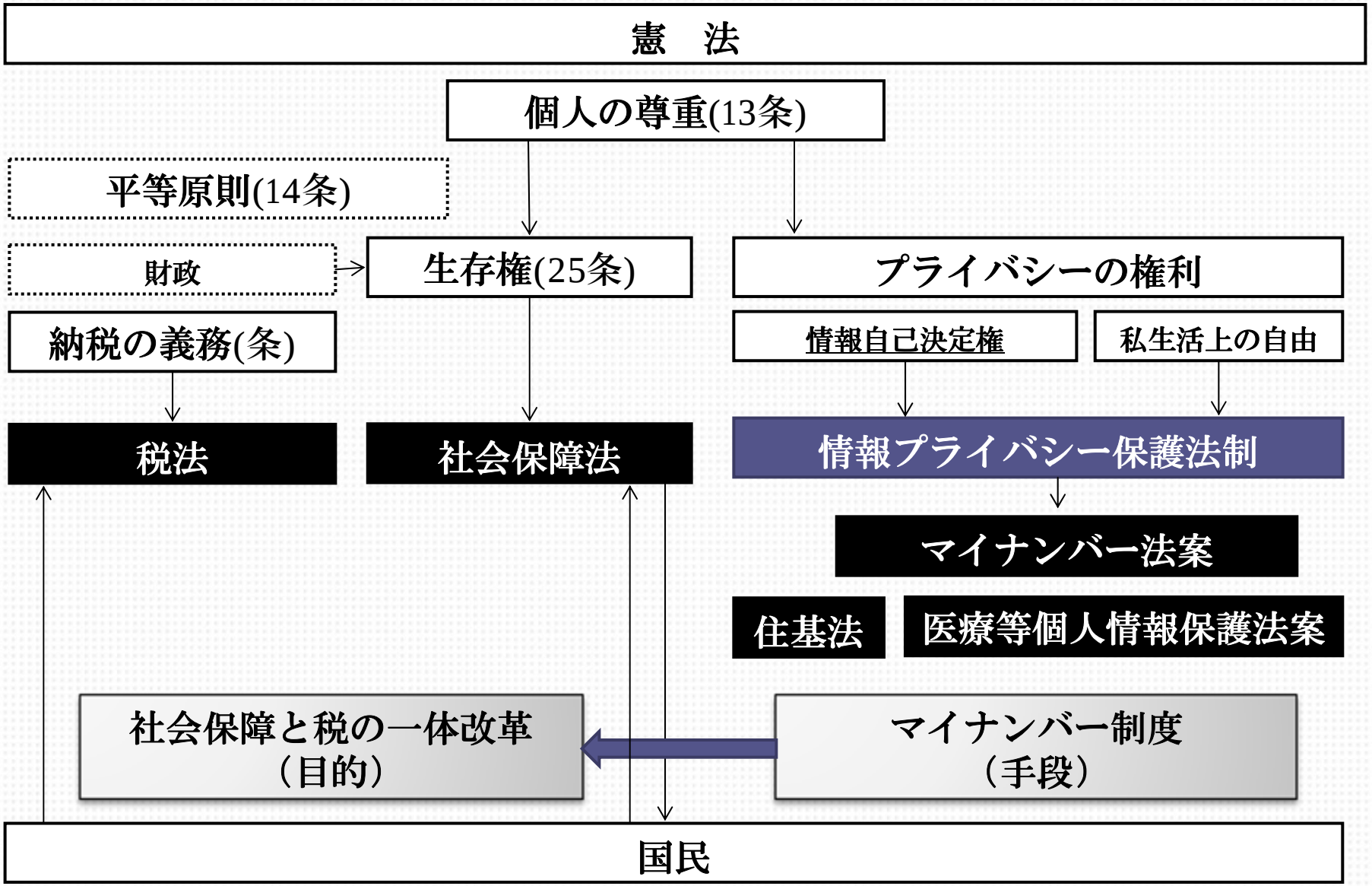
→ゲノム情報は、それに関係する者全員の利害関係を有しており、当該本人の自己決定のみで公開できる情報ではない。その意味で従来のプライバシー権による保護とは異なる保護を要する。

私見：法改正に向けた基本的な考え方

（１）理論的基礎の確立
- EU＝リスボン条約（憲法的保障）→EU指令
- 米国＝自然権→独立宣言→
  固有権（property）→プライバシー権
- 日本＝行政の取締規定（哲学なし）

（２）用語の概念定義－国際性：国際規格との整合
（３）論理性
（４）義務規定－実装を踏まえた落とし込み
  －Privacy by Design
（５）法律と規格（第三者評価認証制度）との整合
（６）行政法と不法行為法の特別法との両面から
（７）組織：政府CIO（執行）と第三者機関（監視）

私案：検討の射程の確認、部分最適から全体最適へ、個人情報保護法制から情報プライバシー保護法制へ



私案：人権の具体化法と行政組織（統治機構の具体化法）