

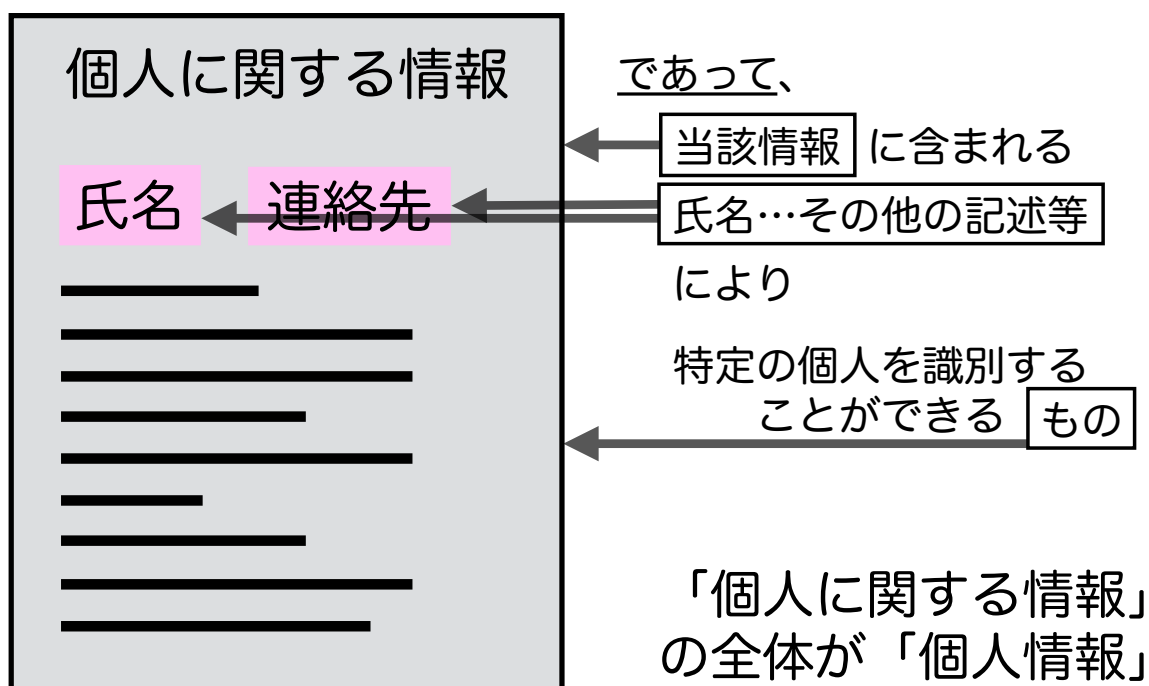
FIT2014 イベント企画 パネルセッション
 「新しい個人情報保護の枠組みとパーソナル
 データの匿名化措置はどうか？」
 2014年9月3日

準個人情報とは何だったのか どうあるべきなのか

産業技術総合研究所
 セキュアシステム研究部門
 高木 浩光

現行法の理解(1)

- 個人を特定する情報が「個人情報」なのではない

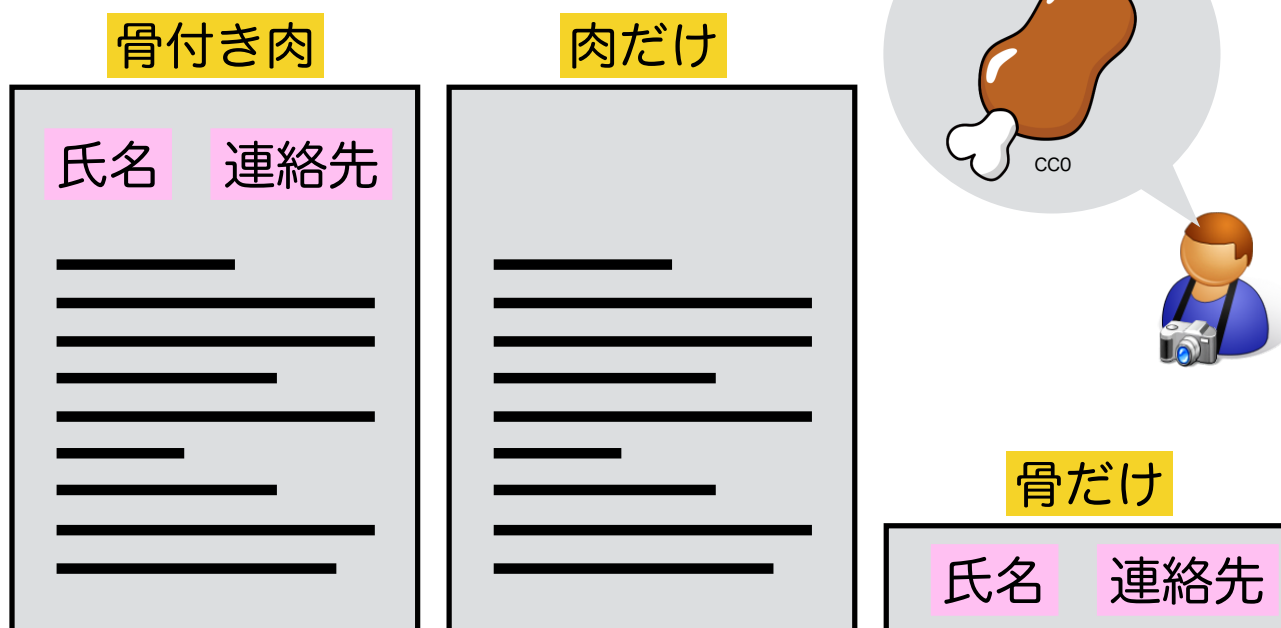


現行法の理解(2)

- 同じデータが氏名の有無で個人情報となったり、非個人情報となったりする
- 例：ICカード乗車券で**記録された乗降履歴**
 - 記名式（定期券等）なら個人情報
 - 無記名式なら非個人情報
- 現行法の立法時の狙いはどこにあったのか？
 - 氏名を保護しなかったわけではなく、「個人に関する情報」を保護したいが、全てをともしかないので、含むものに限定
 - 逐条解説
 - 「『個人に関する情報』のうち、特定の個人を識別できる情報は、コンピュータ処理によって『名寄せ』が容易であることに加えて、当該情報と本人との結びつきが明確であることから、（略）」

現行法の理解(3)

- 大事なものはどれなのか？



現行法の理解(4)

- 情報公開法との対比
 - 特定の個人を識別できないものも1号不開示情報となり得る

個人に関する情報であって、		情報公開法における開示	行政機関個人情報保護法における提供	個人情報保護法における提供データの第三者提供
提供元で特定個人識別できるものを、	提供先で特定個人識別できる形で	5条1号前段不開示情報となる	提供元基準で制限される	提供元基準（容易照合）で制限される
	提供先で特定個人識別できない形で	5条1号前段不開示情報だが、6条2項部分開示となる（場合がある）	提供元基準で制限される	提供元基準で制限されるが、k-匿名性があれば制限されない
提供元で特定個人識別できないものを、	提供先で特定個人識別できる形で	5条1号後段不開示情報となる	制限されない（ただし行政文書の利用目的に拘束される）	制限されない
	提供先で特定個人識別できない形で	5条1号後段不開示情報となる（場合がある）	制限されない（ただし行政文書の利用目的に拘束される）	制限されない

現行法の理解(5)

- 番号類は「特定の個人を識別できる」情報でないの？
 - 逐条解説
 - 「「その他の記述等」としては、例えば、住所、年齢、性別、電話番号、**個人別に付された番号、記号（会員番号、金融機関の口座番号、試験の受験番号等）**等が挙げられる。」
 - （でも、それ単体で「特定の個人を識別できる」とは言っていない……）
 - 昭和63年法での定義
 - 「当該情報に含まれる氏名、生年月日その他の記述**又は個人別に付された番号、記号その他の符号**により当該個人を識別できるもの」
 - なぜ後段が削られたのか謎
 - 情報公開・個人情報保護審査会の判断例
 - 「基礎年金番号及び年金コードは、その性質等からみて、法5条1号の**特定の個人を識別することはできないが**、なお個人の権利利益を害するおそれがある情報に該当する」（審査会答申15-231）

大綱の趣旨

- 個人情報の利活用（規制緩和）
 - 例：記名式ICカード乗車券の乗車履歴を、同意なく第三者提供できるようにする
 - 「個人特定性低減データ」に加工たうえで
 - 提供先（受領者）に対して、データから特定の個人を識別する行為等を法的に禁止（再特定禁止）としたうえで
 - この制度が本当に成立するのは未知数
- 非個人情報の一部を保護対象に（規制強化）
 - 例：無記名式ICカード乗車券の乗車履歴も、記名式と同じように保護対象とする
 - 現行法の（未完成だった）本来の趣旨を実現するものとして
 - 「準個人情報」として案が検討されたが、ボツになった

準個人情報は何だったか(1)

- 4月の事務局案（定義部分）
 - 個人情報に該当するものを除き、生存する個人に関する情報であって、次に例示するもの及びこれに類するものを含む情報
 - ① パスポート番号、免許証番号、IPアドレス、携帯端末ID等の個人または個人の情報通信端末（携帯電話端末、PC端末等）等に付番され、継続して共用されるもの
 - ② 顔認識データ、遺伝子情報、声紋並びに指紋等、個人の生体的・身体的特性に関する情報で、普遍性を有するもの
 - ③ 移動履歴、購買履歴等の特徴的な行動の履歴
- 最終的に
 - 技術WG報告書で③が消滅
 - 大綱で「準個人情報」の語は消滅、①が外され、②のみが例示されて「等」が付いた

準個人情報は何だったか(2)

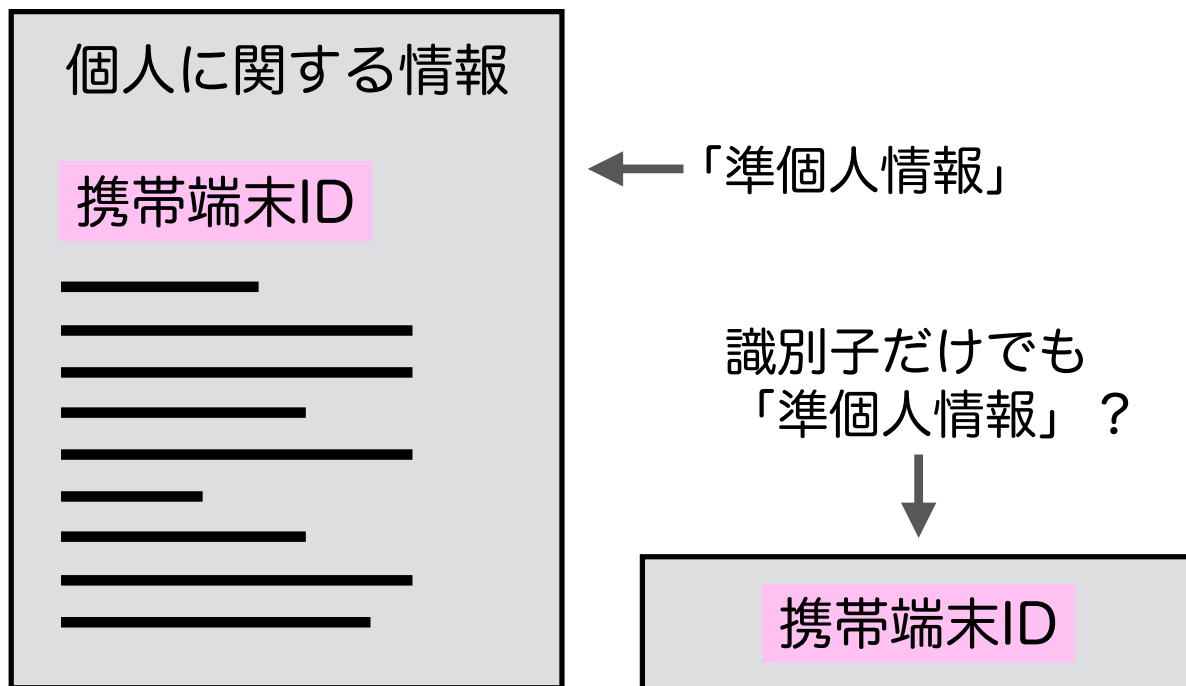
- 前提としたこと
 - 「特定個人を識別しないが、その取扱いによって本人に権利利益侵害をもたらされる可能性があるもの」として2つに分類
 - ①「準個人情報」から何らかの状況で個人が特定されてしまうことで、権利利益侵害が生じる場合
 - ②「準個人情報」から個人が特定されないままで、権利利益侵害が生じる場合
 - ①の「特定されてしまう」リスクについてのみを評価
 - ②について「技術的な見地からだけでは検討できないと判断」「個々のユースケースや制度面を含めて、別途検討すべきである」とした
- 検討内容
 - 「特に特定の個人を識別する蓋然性が高い識別子」の要件を示した
 - 本人/所有物付与、一意性、単射性、共用性、変更可能性、不変性、利用停止可能性、継続性、利用範囲の観点から
 - 「③ 移動履歴、購買履歴等の特徴的な行動の履歴」は「どのような状態…識別子として機能する特徴的な状態…一律に定めることは困難」とした

準個人情報は何だったか(3)

- 技術WG報告書より (p.7)
 - 我が国の法制度は、特定の個人が識別されなくても権利利益の侵害が生じ得ることを正面から認めている。例えば、「行政機関の保有する情報の公開に関する法律」第5条第1号は、「特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるもの」を不開示情報（略）としている。どのようなものがこれに当たるかについては、個人の人格に密接に関わる情報である等の説明がなされている³。
 - このように特定の個人を識別することなく権利利益の侵害が生じるおそれのあるものについては、その存在は明らかであり、また、識別子を利用した多量又は多様な情報の収集が、この種の権利利益の侵害につながる可能性があることも十分に予想し得るところである。しかしながら、結局のところ、どのような情報が「個人の人格に密接に関わる」か等は、WGの専門的知見の及ぶところではないため、この問題については、親会における検討に委ねることとする。
 - 親会での検討は行われなかった（時間切れで）

準個人情報は何だったか(4)

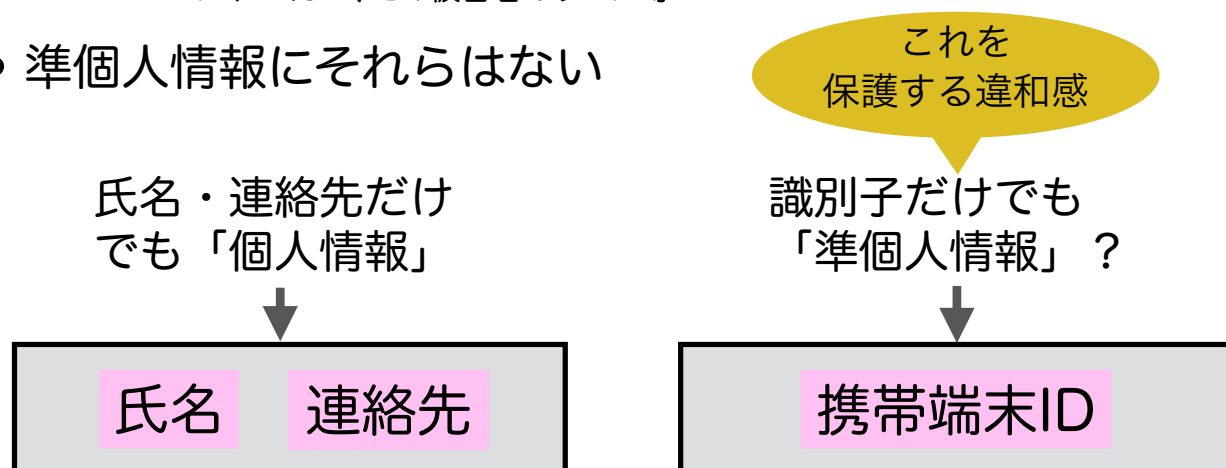
- 保護したいのは識別子なの？（そうではない）



準個人情報は何だったか(5)

- 個人情報の場合は
 - 氏名・連絡先だけでも保護する意義は一応あった
 - ダイレクトメールを無差別に送りつけられることを嫌とする
 - これはプライバシーの問題ではないのだが
 - 一部の人にとっては単に住所を知られることも嫌とされる
 - ストーカー、DV被害者のケース等

- 準個人情報にそれらはない



準個人情報は何だったか(6)

- 義務規定の案、誰も望まない案だった

25

【参考】 今後の個人情報取扱事業者等の義務イメージ

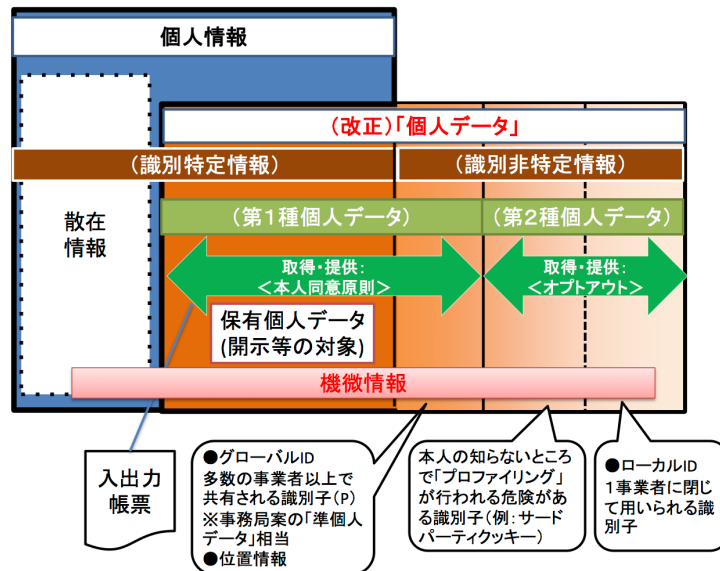
事業者 ※準個人情報、個人特定性低減の仮称を省略		個人情報取扱事業者		個人情報取扱事業者、 準個人情報取扱事業者	個人、準個人、個人特定 性低減データ取扱事業者
データ		個人情報、個人データ 保有個人データ	機微情報	準個人情報 準個人データ	個人特定性低減データ
データ取得	利用目的の特定(§15)	取得データの利用目的を特定			義務なし
	適正な取得(§17)	適正に取得する			
	取得時(§18)	利用目的の通知または公表	本人から 同意取得	あらかじめ、または取得後速 やかな利用目的の公表等	個人情報、準個人情報から 作成するため該当しない
	書面での取得	利用目的の明示			
取扱い	利用目的の公表(§24)	利用目的を公表			義務なし
	取得時の 利用目的を 変更(§16)	利用目的内	本人へ通知または公表	本人を特定しないため義務なし	
		利用目的外	本人から同意取得	あらかじめの公表等により 利用	
	取扱い (§19-22)	正確性の確保	データ内容を正確かつ最新の内容に保つ		
		安全管理	安全管理・従業員の監督・委託先の監督		
	個人特定性 低減データ	加工・提供者	適正に個人が特定される可能性を低減する措置を施し、元データとの突合を禁止		
		受領者	対象外		特定の個人を識別禁止
第三者への 提供 (§23)	オプトアウト	本人から同意取得	あらかじめ、第三者提供を 利用目的とする	本人を特定して個人情報として 同意を得る または個人が特定される可 能性を低減する措置を施す	第三者機関へ報告
		共同利用	あらかじめ、共同利用を利用目的とする	禁止	禁止
	利用目的内(§24)	求めに応じて通知		本人を特定しないため義務なし	
本人の求め	開示等請求(§25-27)	求めに応じて開示			

法案化に向けて

- 大綱での記述
 - 「個人の権利利益の保護と事業活動の実態に配慮しつつ、指紋認識データ、顔認識データなど個人の身体的特性に関するもののうち、保護の対象となるものを明確化し、必要に応じて規律を定めることとする。」
- この法が対象とすべき情報の範囲は？
 - 身体的特性情報に限るべきでない
 - 準個人情報の語を使うとそれで足りるとの意味になりかねない
 - そのためどの語も用いられていない
 - 「個人に関する情報」の語を用いてはどうか
 - それ全体が保護対象なわけではなく
 - 機動的に柔軟に保護の範囲を定めるその大枠を指す語として

鈴木正朝委員の対案(1)

- 個人データ拡張案（第8回検討会 資料4-1）
 - 識別非特定情報の全部を対象とするという考え方
 - 特定されやすさは義務の強弱の区分に

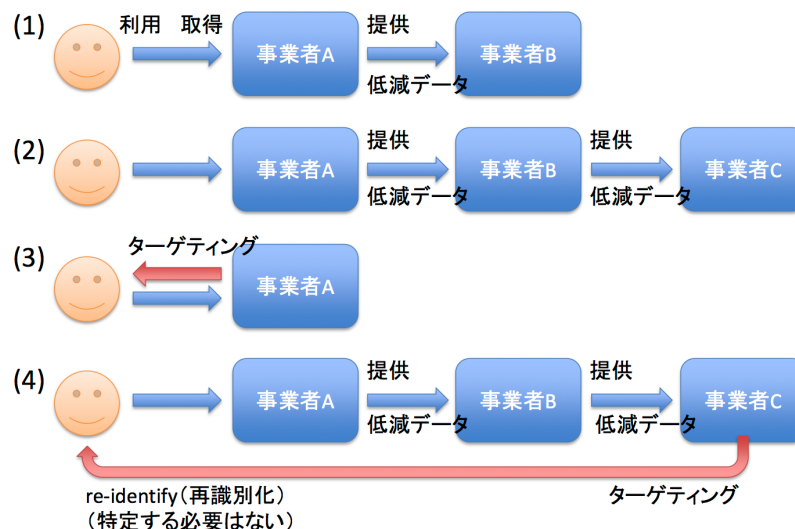


9

鈴木正朝委員の対案(2)

- 想定する利活用のモデルの整理がないと指摘
 - 行動ターゲティング広告が事務局案の想定にない
 - 最終的に統計データに加工されるモデルだけが検討された

想定する利活用のモデル



10

広告業界の動向(1)

- 参考人JIAAの意見（第9回検討会 資料1-4）
 - JIAA - 一般社団法人インターネット広告推進協議会
 - 3月にガイドラインを改訂
 - 「個人関連情報」を定義し、義務を規定
 - 行動履歴情報がこれに含まれるとした
 - 義務内容は個人情報保護法の個人データとほぼ同じ
- 私の意見
 - これを法制化しても事業者は困らないのではないかと
 - 既に米国の自主規制ルールに従っているのと同様（にできる）
 - むしろ「正直者が馬鹿を見る」事態を防止でき、真っ当な広告事業者には好都合なはず
 - （ただし、散在情報を除く件と、取得の委託モデルと取得の制限の件が盛り込まれていない点で不完全）

広告業界の動向(2)

- 検討会第9回でのJIAA意見陳述

 Japan Internet Advertising Association

ガイドラインによる自主規制の課題

前提：広告は消費者が直接的に接触する情報サービスのため、その安全性、信頼性を幅広く担保する必要

1. 協議会内外の事業者がガイドライン履行を徹底できるか。ガイドラインの趣旨を消費者へ周知できるか
2. 国内、海外の事業者が等しく同様な基準でガイドラインを理解、実行できる体制を構築できるか
3. スマートフォン広告とPC広告を同様な基準でガイドラインの趣旨を制度的、技術的に統一できるか

* インターネット広告はその仕組みが消費者から直接的には可視化されないため、あまねく広告は評価される

パーソナルデータ検討会第9回 資料1-4 より

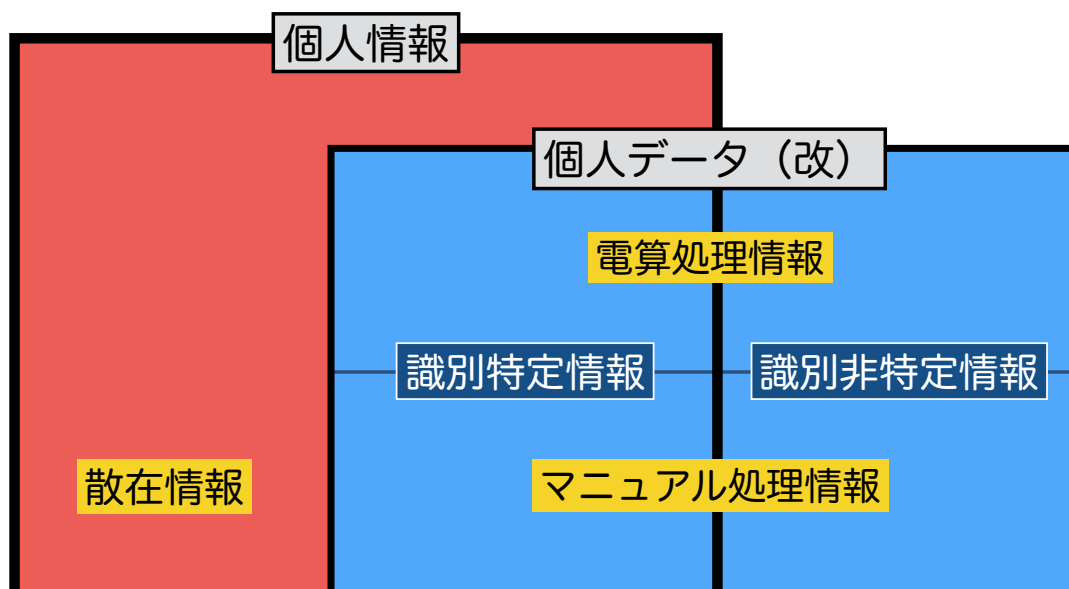
22

どうなったか

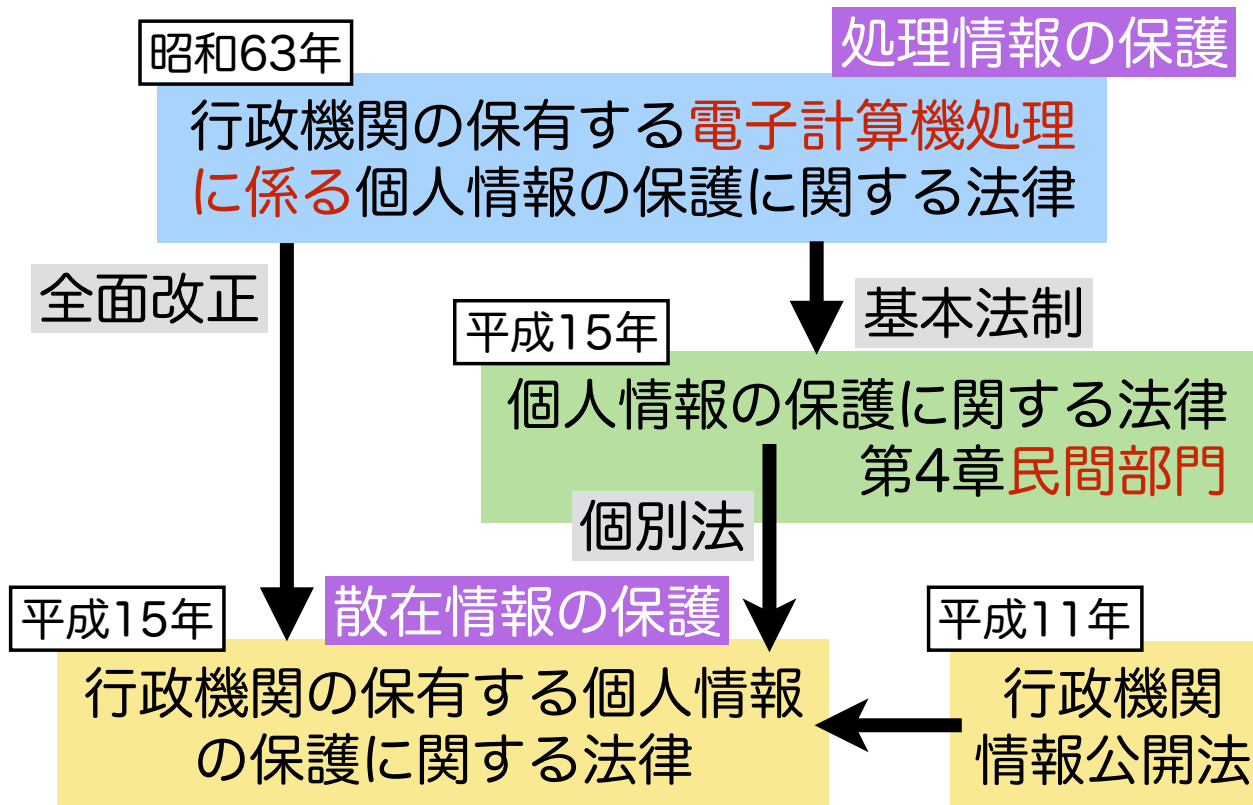
- 肝心の検討（行動ターゲティングの想定）
 - 技術WG報告書の言う「個人が特定されないままで、権利利益侵害が生じる場合」にこれが該当
 - 「親会における検討に委ねる」とされたが時間切れで検討されていない
- プロファイリングの問題として
 - 検討会で複数の委員から指摘
 - 米国ではFTCが2000年からonline profilingの問題として報告書を出しているし、EU規則提案でもprofilingに関する権利が明記
 - 大綱に書き込まれたが「継続的な検討課題」として先送りに
 - 「いわゆるプロファイリング - 多種多量な情報を、分野横断的に活用する（略）プロファイリングの対象範囲、個人の権利利益の侵害を抑止するために必要な対応策等については、現状の被害実態、民間主導による自主的な取組の有効性及び諸外国の動向を勘案しつつ、継続して検討すべき課題とする。」

どうするべきか（鈴木対案）

- 「個人データ」を識別非特定情報まで拡張すればよい
 - 「個人データ」は現行法の定義語
 - 「個人情報データベース等」を構成する個人情報

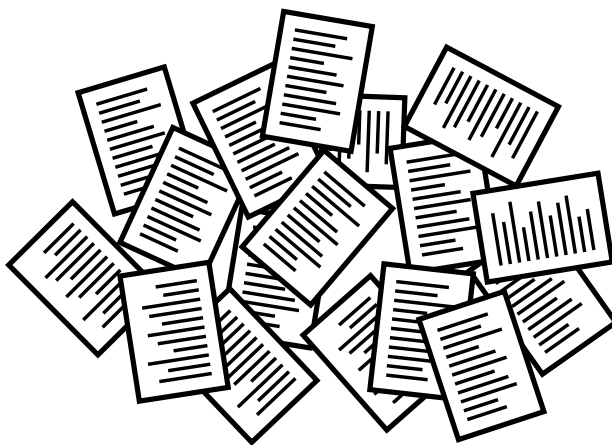


現行法までの流れ

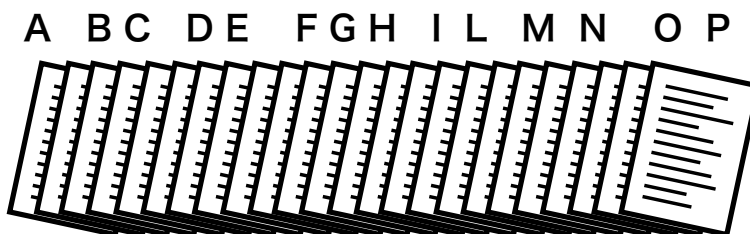


散在情報と処理情報

散在情報



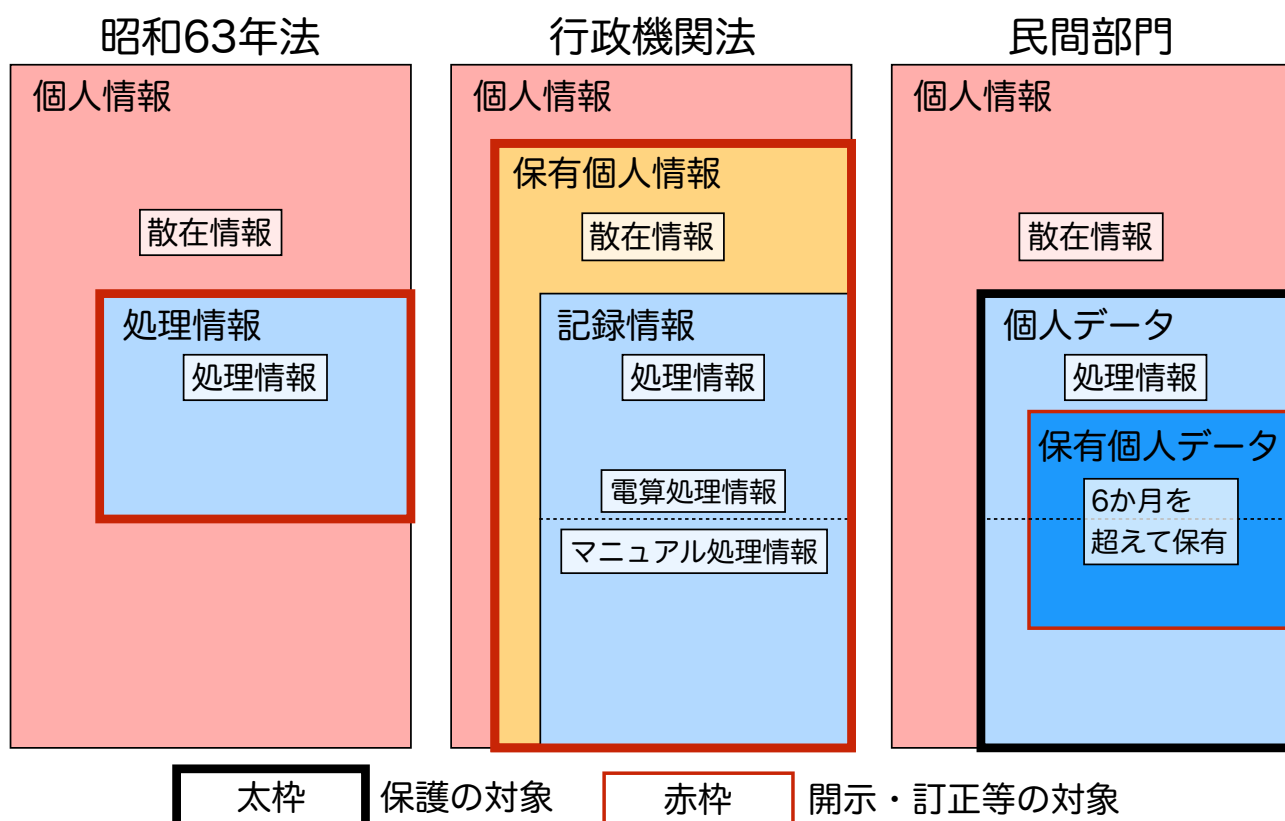
処理情報



「処理情報」とは(1)

- 昭和63年法 2条の定義
 - 五 処理情報 個人情報ファイルに記録されている個人情報という。
 - 四 個人情報ファイル 一定の事務の目的を達成するために体系的に構成された個人情報の集合物であつて、電子計算機処理を行うため磁気テープ（略）に記録されたものをいう。
- 行政機関個人情報保護法 2条の定義
 - この法律において「個人情報ファイル」とは、保有個人情報を含む情報の集合物であつて、次に掲げるものをいう。
 - 一 一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
電算処理情報
 - 二 前号に掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの
マニュアル処理情報

対象情報の変遷

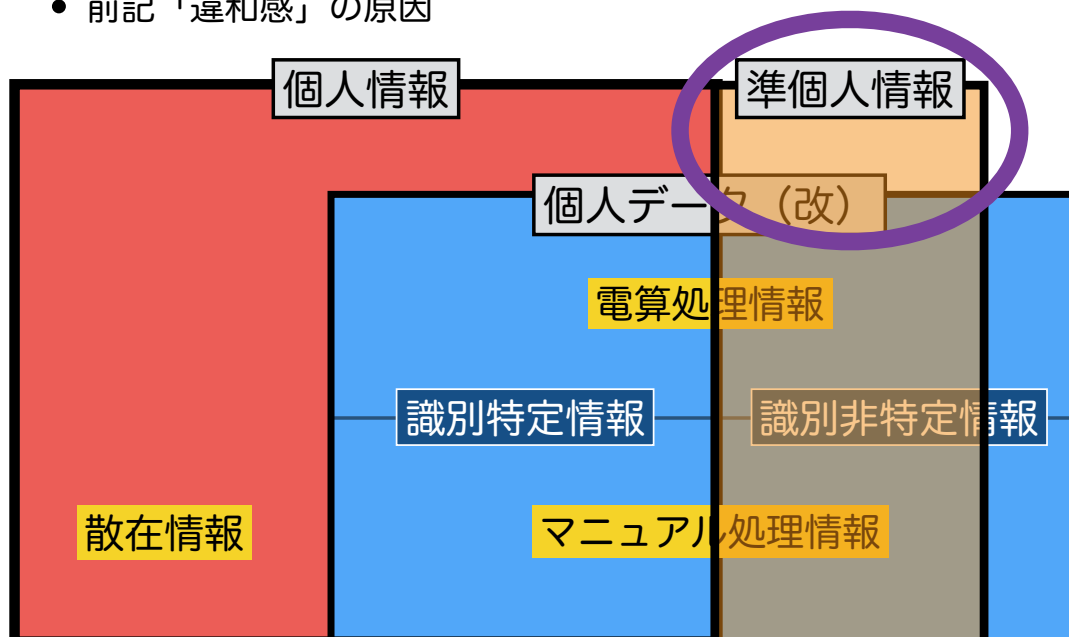


各法の趣旨

- 昭和63年法
 - 処理情報のみを対象とする
 - 照合による識別（照合性要件）は「容易に」に限定
- 行政機関法の趣旨
 - 処理情報について従来通りとしつつ、
 - 散在情報についても対象とする（情報公開法に合わせて）
 - より厳しい規律とするため照合性要件から「容易に」を削除
- 民間部門の趣旨
 - 昭和63年法を引き継ぎつつ、
 - 民間の営業の自由に配慮して過剰な規制とならないよう配慮
 - 目的別のデータ管理を求めず「個人情報データベース等」は事業者単位
 - 「容易に」は残したまま

準個人情報案のマズいところ

- 散在情報まで対象となるのを排除していない
 - 散在情報と処理情報の区別は検討会・WGで議論されなかった
 - 前記「違和感」の原因



識別非特定情報

- 技術検討ワーキンググループ報告書（2013年12月）
 - 個人識別性を「特定」と「識別」に分けて議論
 - 用語が以下のように整理された

識別特定情報	個人が（識別されかつ）特定される状態の情報 （それが誰か一人の情報であることがわかり、さらに、その一人が誰であるかわかる情報）
識別非特定情報	一人ひとりとは識別されるが、個人が特定されない状態の情報 （それが誰か一人の情報であることがわかるが、その一人が誰であるかまではわからない情報）
非識別非特定情報	一人ひとりが識別されない（かつ個人が特定されない）状態の情報 （それが誰の情報かわからず、さらに、それが誰か一人の情報であることが分からない情報）

技術WGの「識別/非識別」の区分

- 散在情報^(※)に対してこの区分は無理がある
 - なぜなら散在情報^(※)の場合は
 - 「特定情報」なら「識別情報」でもあることは自明だが
 - 「非特定情報」だと「識別情報」か否か不明（定義不可）
 - 散在情報は、他の散在情報との関係が不明であるので
- 処理情報^(※)に対してこの区分は明確
 - 識別非特定情報 ∪ 識別非特定情報 = 処理情報^(※)
ということではないか

※ここでは、「散在情報」「処理情報」は、「個人情報」に該当しなくても「個人に関する情報」であれば該当するものとして拡張した用語

対象情報の比較

	昭和63年法	行政機関法	現行民間部門
利用目的の特定	個人情報ファイル 4条	個人情報 3条	個人情報 15条
保有の制限	個人情報ファイル 4条	個人情報 3条	—
利用目的による制限/目的 外利用の制限	処理情報 9条	保有個人情報 8条	個人情報 16条
適正な取得	—	—	個人情報 17条
利用目的の通知/公表	—	—	個人情報 18条
直接書面取得における利用 目的の明示	—	個人情報 4条	個人情報 18条
正確性の確保	処理情報 5条2項	保有個人情報 5条	個人データ 19条
安全管理/確保措置	個人情報 5条1項、11条	保有個人情報 6条	個人データ 20～22条
従事者の義務	個人情報 12条	個人情報 7条	—
提供の制限	処理情報 9条	保有個人情報 8条	個人データ 23条
受領者に対する措置要求	処理情報 10条	保有個人情報 9条	—
保有事項の公表	個人情報ファイル 6～8条	個人情報ファイル 10～11条	保有個人データ 24条
開示・訂正等	処理情報 13～17条	保有個人情報 12～44条	保有個人データ 25～30条
苦情の処理	処理情報 20条	個人情報 48条	個人情報 31条



処理情報に限られず
散在情報も含む
個人情報



処理情報に限られる
個人情報



太枠部分、なぜ
個人情報対象？

なぜ「個人情報」対象？(1)

- 昭和63年法の逐条解説（5条1項）
 - 「本項において、「処理情報」ではなく「個人情報」と規定したのは、入力のための準備段階の個人情報は、未だ「処理情報」とはいえないためである。」
 - 条文 5条1項（個人情報の安全確保等）
行政機関が個人情報の電子計算機処理又はせん孔業務その他の情報の入力のための準備作業若しくは磁気テープ等の保管（以下「個人情報の電子計算機処理等」という。）を行うに当たっては、当該行政機関の長（…）は、個人情報の漏えい、滅失、き損の防止その他の個人情報の適切な管理のために必要な措置（…）を講ずるよう努めなければならない。
- なるほどこれは納得
 - 開示対象としないが安全確保の対象としたい部分があるため

なぜ「個人情報」対象？(2)

- 民間部門の逐条解説（15条）
 - なお、取り扱う対象を「個人情報」とし「個人データ」としていないのは、いずれ個人情報データベースに記録され「個人データ」となるものであっても、取得段階では「個人情報」の状態であることによる。本条から第18条までの規定は、個人情報の取得段階を含む個人情報の取扱い全般を規律することから、「個人データ」（第2条第4項）ではなく「個人情報」（第2条第1項）を規律の対象としている。
- 本来の保護対象は「個人データ」だけだったのでは？
 - 入力段階も「個人データ」と定義すればよかったのでは？
 - できなかった事情
 - 事業者の意図を要件とせざるを得ないためか

個人情報を拡張してはだめ？(1)

- 大阪弁護士会の反対声明（2014年5月26日）
 - 「パーソナルデータの利活用に関する制度見直し方針」に対する意見書
 - 「平成14年意見書で述べたとおり、そもそも包括的な民間規制法による情報流通の規制は、民間の情報交換を直接に制約し、萎縮効果をもたらすことから、憲法21条の保障する表現の自由、知る権利、報道の自由等を不当に侵害するおそれが強い規制手段である。
見直し方針が示すように、包括的な民間規制法である個人情報保護法において、規制対象となる個人情報等の範囲を拡大することは、表現の自由等に対する深刻な脅威となると言わざるを得ない。」
- これは散在情報の話をしていると思われる
 - 処理情報（個人データ）の保護が表現の自由を脅かすことはほぼない

個人情報を拡張してはだめ?(2)

- 際限なく広がる？
 - 逐条解説
 - 「匿名の個人情報であっても、例えば知的所有権に係る情報等その取扱い次第で本人の権利利益侵害の可能性のあるものは皆無ではない。しかし、現実には匿名の個人情報がいかなる個人に関する情報であるのかは、一般に本人以外の他人にはわからないし、**このような情報まで含めるとすると「個人情報」の範囲が際限なく広がることともなりかねない。**匿名情報が問題となるのは特定の場合に限られ、**既に著作権法などで対応されているものもあるが、いずれにしてもこの法律とは別の法制度による仕組みが必要**であろう。そこで、本法では「個人に関する情報」のうち、**特定の個人が識別可能なもののみを「個人情報」と定義**している。

改正への立法技術的障害と解決

- 「個人情報」の定義を拡張したいが
 - 定義が広がりすぎて義務の履行が困難に？
 - たしかに、散在情報としての「個人情報」の定義が広がると、利用目的を特定しその目的でのみ利用しなくてはならないわけであり
 - 他の法令に含まれる用語「個人情報」をどうするのか
 - 行政機関個人情報保護法、独立行政法人個人情報保護法、個人情報保護条例の「個人情報」定義との整合性をどうするのか
- 「個人情報」を変更せず「個人データ」の拡張で解決
 - 併せて「個人データ」のみが対象であることを明確にする
 - 本来の法の趣旨に立ち戻って