個人情報等の種類と規制の違い

～要配慮、プライバシー、個人関連情報、仮名加工情報、匿名加工情報等々～

ミス・間違い等もありえますので、必ず法律・GL等原典に当たっていただけますようお願いします。

22.8　弁護士　水町雅子

講師略歴

弁護士　　水町雅子　（みずまちまさこ）

http://www.miyauchi-law.com　　メール→osg@miyauchi-law.com

- 東京大学教養学部相関社会科学卒業
- 現、みずほ情報総研入社

ITシステム設計・開発・運用、事業企画等業務に従事

- 東京大学大学院法学政治学研究科法曹養成専攻（法科大学院）修了
- 司法試験合格、法曹資格取得、第二東京弁護士会に弁護士登録
- 内閣官房社会保障改革担当室参事官補佐

マイナンバー制度立案（特にマイナンバー法立法作業、情報保護評価立案）に従事

- 現、個人情報保護委員会上席政策調査員

マイナンバー制度における個人情報保護業務（特にガイドライン、特定情報保護評価）に従事

- 首相官邸IT総合戦略本部「パーソナルデータに関する検討会」参考人

個人情報保護改正検討

- 宮内・水町IT法律事務所（旧、五番町法律事務所）共同設立、現在にいたる

その他、東京都都政改革アドバイザリー会議委員や、地方公共団体の情報公開・個人情報保護審査会委員等を務める。
マイナンバー・個人情報に関する著書・論文・講演・TV出演・新聞取材等多数。『１冊でわかる！個人情報保護法』（労務行政、２０１７年）
金融法務事情Ｎｏ.２０４６「改正個人情報保護法と金融機関の実務対応」、労政時報３９１５号「実務に役立つ法律講座（２３）個人情報」
ＮＢＬＮｏ.９４７「ライフログにおける法的問題」等多数

AGENDA

個人情報等の種類

（１）個人情報／プライバシー権／営業秘密
（２）個人情報の定義
（３）個人データ／保有個人データ
（４）要配慮個人情報
（５）個人関連情報
（６）それぞれの違い

個人情報の利活用

（１）個人情報の利用（目的内利用／目的外利用）
（２）個人情報の外部提供

加工情報の利活用

（１）仮名加工情報／匿名加工情報
（２）行政機関等匿名加工情報
- 国・自治体の持つビッグデータ等をビジネス活用できる仕組み

（３）匿名加工医療情報（次世代医療基盤法）
- 医療データを本人保護及び安全を確保しつつより容易に入手できる仕組み

（４）その他のデータ関連政策

PIA

データ利活用政策の加速化

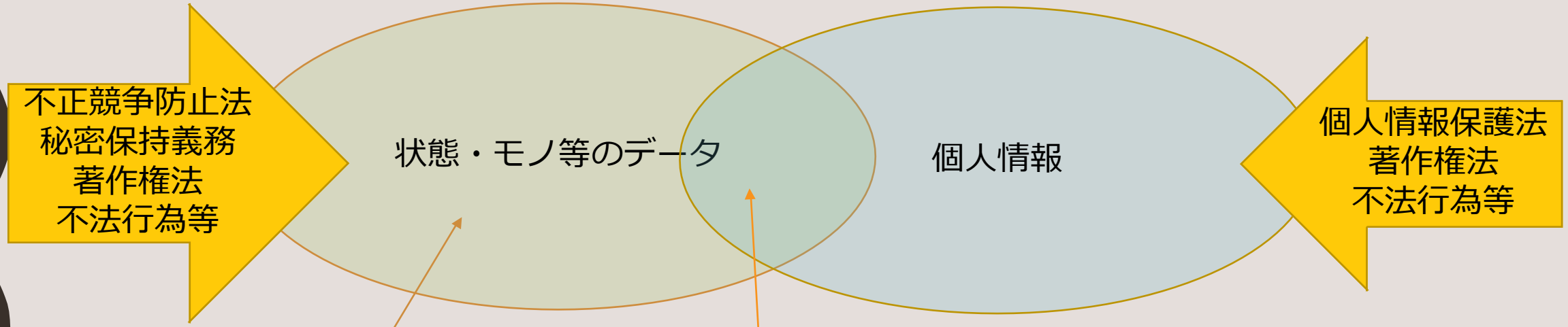
平成２５年	マイナンバー法（官・民）
平成２７年	個人情報保護法が改正（民） • 匿名加工情報の導入
平成２８年	官民データ活用推進基本法（官・民） • 官民データ活用推進計画の策定義務・努力義務
	行政機関個人情報保護法及び独立行政法人等個人情報保護法が改正（官） • 非識別加工情報の導入
平成２９年	次世代医療基盤法（医療ビッグデータ法）（官・民） • 匿名加工医療情報の導入
平成３０年	総務省「地方公共団体におけるデータ利活用ガイドブック」（官） • 個人情報の庁内利活用
令和元年	デジタルファースト法（デジタル手続法）（官・民） • 行政手続のデジタル化
令和２年	個人情報保護法が改正（民） • 仮名加工情報の導入
令和３年	個人情報保護法が改正（官） • 行政機関・独法・地方公共団体・地方独法の規制も個人情報保護法に一元化 • 行政機関等匿名加工情報の導入
	デジタル改革関連法が成立（官・民） • デジタル庁設置等

様々なデータが蓄積される時代

◆データが大量に発生するが、個人情報の場合と、非個人情報の場合とがある

◆状態・モノ等のデータであっても、個人情報に該当するものもあれば、そうでないものもある

◆AIで機械学習させるデータも、個人情報であったりそれ以外の情報であったりする



- 機械ログ、運行・走行情報
- 温度、湿度、センサー情報
- 地形、地図、測量情報
- 施設情報
- 生産過程、工事状況情報

等さまざま

- 人に関する情報であれば「個人情報」
- 例）電力消費量であれば、それが誰の情報かわかれば「個人情報」
- 例）車両運行情報であれば、乗客や運転手、通行人等、人に関する情報があって、それが誰の情報かわかれば「個人情報」

個人情報等の種類

（１）個人情報／プライバシー権／営業秘密

個人情報とプライバシー権の比較

「個人情報」「個人データ」「保有個人データ」「要配慮個人情報」といろいろ種類がある。
さらには、「匿名加工情報」「非識別加工情報」「匿名加工医療情報」という種類も。
でも、そもそも「個人情報」と「プライバシー」って違うの？同じなの？

種類	特徴	規制
個人情報 例）名刺、企業の役員情報、公開情報	■ 意外と範囲が広い ■ 内容の重要性・秘匿性は問わない	■ 規制は比較的弱め 正確にいうとH27法改正前までは弱く、H27以降の法改正で非常に細かくややこしい規制がかかってきている ■ 「個人情報」より「個人データ」「保有個人データ」に規制を強化
要配慮個人情報 例）カルテ情報、検査結果	■ 意外と範囲が狭い ■ 金融の場合は、さらに「機微情報」概念が加わる	■ オプトアウトしていなければ、通常の個人情報と基本的には差異なし
プライバシー権 例）購買歴、政治思想、不倫	■ 「個人情報」とは違う ■ 一般的な「個人情報」のイメージは、実は「プライバシー」	■ 個人情報保護法（行政による指導等）ではなく、 民法（裁判による解決）

制裁の比較

種類	制裁
個人情報保護法違反 例）不適正取得、第三者提供規制違反、 目的外利用規制違反	■ 行政（個人情報保護委員会）による助言・指導・勧告・命令 ■ 基本的には行政指導、命令違反に対して罰則 ■ 一定の悪質行為には、命令を経ずに罰則（直罰） ■ 個人情報保護法に基づく直接的な賠償責任はない ■ 要配慮個人情報も個人情報も個人データも保有個人データも、個人情報保護法に違反していれば、同様
プライバシー権侵害 例）ネットに他人の私生活上の問題を書き込む、特定商品の購買者情報を売却	■ 基本的に罰則はない（脅迫罪等を構成する場合は別） ■ 謝罪広告や賠償責任を負う（裁判、和解）

✓ 個人情報保護法対応：「個人情報」「個人データ」「保有個人データ」の範囲を正しく理解することが重要。個人情報保護法違反は行政による指導がメイン（罰則もある）。

✓ プライバシー権保護：個人情報保護法だけを遵守すればよいというものではなく、一般に不法行為を行えば、裁判で敗訴する可能性（賠償責任を負う）

プライバシー権（判例）

プライバシー権

① 私生活上の事実又は私生活上の事実らしく受け取られる恐れ（私生活性）

② 一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること、換言すれば一般人の感覚を基準として公開されることによって心理的な負担、不安を覚えるであろうと認められること（非公開の期待）

③ 一般の人々に未だ知られていないこと（非公知性）

④ （本人との同定可能性）

宴のあと事件(東京地判昭和39年9月28日判時385号12頁)、防衛庁リスト事件(新潟地判平成18年5月11日判時1955号88頁)、石に泳ぐ魚事件一審判決(東京地判平成11年6月22日判タ1014号280頁) 二審判決(東京高判平成13年2月15日判タ1061号289頁)等

POINT

- 個人情報よりも狭い。非公開の期待＋非公知性が求められる。
- 特殊な個人の感受性ではなく一般人の感受性が基準。
  もっとも、特殊な情報であっても、一般人がその人の立場に立ったならば非公開を欲する場合は、保護対象となる点に十分留意が必要。

営業秘密（不正競争防止法）

営業秘密

① 秘密として管理されている（秘密管理性）

② 生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって（有用性）

③ 公然と知られていないもの（非公知性）

不正競争防止法２条６項

POINT

- 個人情報以外も含む概念だが、個人情報に当たって、かつ営業秘密に当たるものも多数ある
- 顧客名簿の売却などは、不正競争防止法の罰則で処罰されることもある

個人情報等の種類

～様々な概念が複雑に入り組んでいる

個人関連情報

検索性等 （官）	個人情報　個人データ　保有個人データ　個人識別符号 保有個人情報　個人情報ファイル
内容・文脈	要配慮個人情報　機微情報（センシティブ情報） プライバシー　営業秘密
加工度合い （特殊）	個人情報　仮名加工情報　匿名加工情報　統計情報 行政機関等匿名加工情報　匿名加工医療情報

個人情報とは何か

（２）個人情報の定義

個人情報の定義

定義

「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう（２条１項・２項）。

① 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

② 個人識別符号が含まれるもの
※個人識別符号とは、指紋、掌紋、パスポート番号、健康保険証番号等、特定の個人を識別することができるもの

生きている人の情報

誰の情報かわかるもの

POINT

- 個人情報保護法の細かい論点に入り込むと、本質が見えにくくなる傾向も。
- 定義について細かい点を抑えるのは後回しにして、
まずは①生きている人の情報、②誰の情報かわかるものという２つの要件を満たせば個人情報であると理解しよう。

個人情報の定義：生存者

個人情報であるためには、**生存者の情報**であることが必要

- 民間企業等の法人の情報は、個人情報に当たらない
  - もっとも、法人の役員や従業者の情報は、生存している者の情報であり、個人情報に当たる。

「株式会社はろうの平成２８年売上高は、〇円」

個人情報に該当しない
∵生きている人の情報ではない

「株式会社はろうの代表取締役社長は、情報太郎である」

個人情報に該当する
∵生きている人の情報である

  - Cf.　プライバシー情報と個人情報は異なる。重要情報・秘密情報でなくても、個人情報に該当する。

- 死者の情報は、原則として個人情報に当たらない
  - もっとも、それが生存者の情報にも該当するような情報、例えば「故情報太郎氏の財産は100億円であり、相続人である情報花子氏が単独で相続する」ことは、個人情報に該当する。

個人情報の定義：特定の個人を識別できる

- 誰の情報かわからなければ個人情報には該当しない。
  - したがって、「東京都民の平均年収は〇百万円である」といった情報は、個人情報に該当しない。
- 一方で、誰の情報かわかれば個人情報に該当するため、「氏名が記載されていなければ個人情報に当たらない」という理解は、誤りである。
  - 「うちの会社の社長は四国出身だ」「今の東の関脇は…」「今の阪神の監督は…」「昭和最後の内閣総理大臣は…」
  - 氏名が含まれていなくても、顔写真や指紋があれば、一般に誰の情報かがわかるといえ、個人情報に該当する。
  - また、ユーザIDとだけ結びついている購買履歴であったり、特定のブラウザ情報とだけ結びついているWeb閲覧履歴であったり、匿名のブログに記載された内容であっても、ものによっては、誰の情報かがわかる場合があるので、その場合は個人情報に該当する。いわゆる「特定」。
  - 氏名が記載されていなくても、誰の情報かわかる場合は意外と多い。

個人情報の定義：特定の個人を識別できる

- さらに、誰の情報かは、その情報単体でわからなくてもよい。
  - 例えば、表1には仮名とだけ結びついているデータがあり、表2には仮名と実名の結びつきのデータがあったとして、表1と表2を困難なく組み合わせることができれば（→容易照合性）、個人情報に該当する。

仮名	乗降履歴			
A1	2016年6月20日7時32分	千葉駅		
	2016年6月20日8時38分	市ケ谷駅		
	2016年6月20日19時55分	市ケ谷駅		
	2016年6月20日21時3分	千葉駅		
B2	2016年6月20日8時35分	新宿御苑前駅		
	2016年6月20日8時58分	四ツ谷駅		
	2016年6月20日18時3分	四ツ谷駅		
	2016年6月20日18時25分	銀座駅		
	2016年6月20日23時35分	銀座駅		
	2016年6月20日23時53分	新宿御苑前駅		

仮名	実名
A1	情報太郎
B2	難波舞

キーワード
容易照合性

個人情報の定義の改正

改正前

「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう（旧２条１項）

改正後

※実質的改正箇所は下線部参照

「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。（２条１項・２項）

①当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

②個人識別符号が含まれるもの

POINT

- 最初の（）の追加については、記述等は、文書だけに限定されず、幅広い一切の事項をいうという改正で、これまでの明確化
- ２条１項２号の「個人識別符号」は、次のスライドにて詳解

個人識別符号

個人識別符号

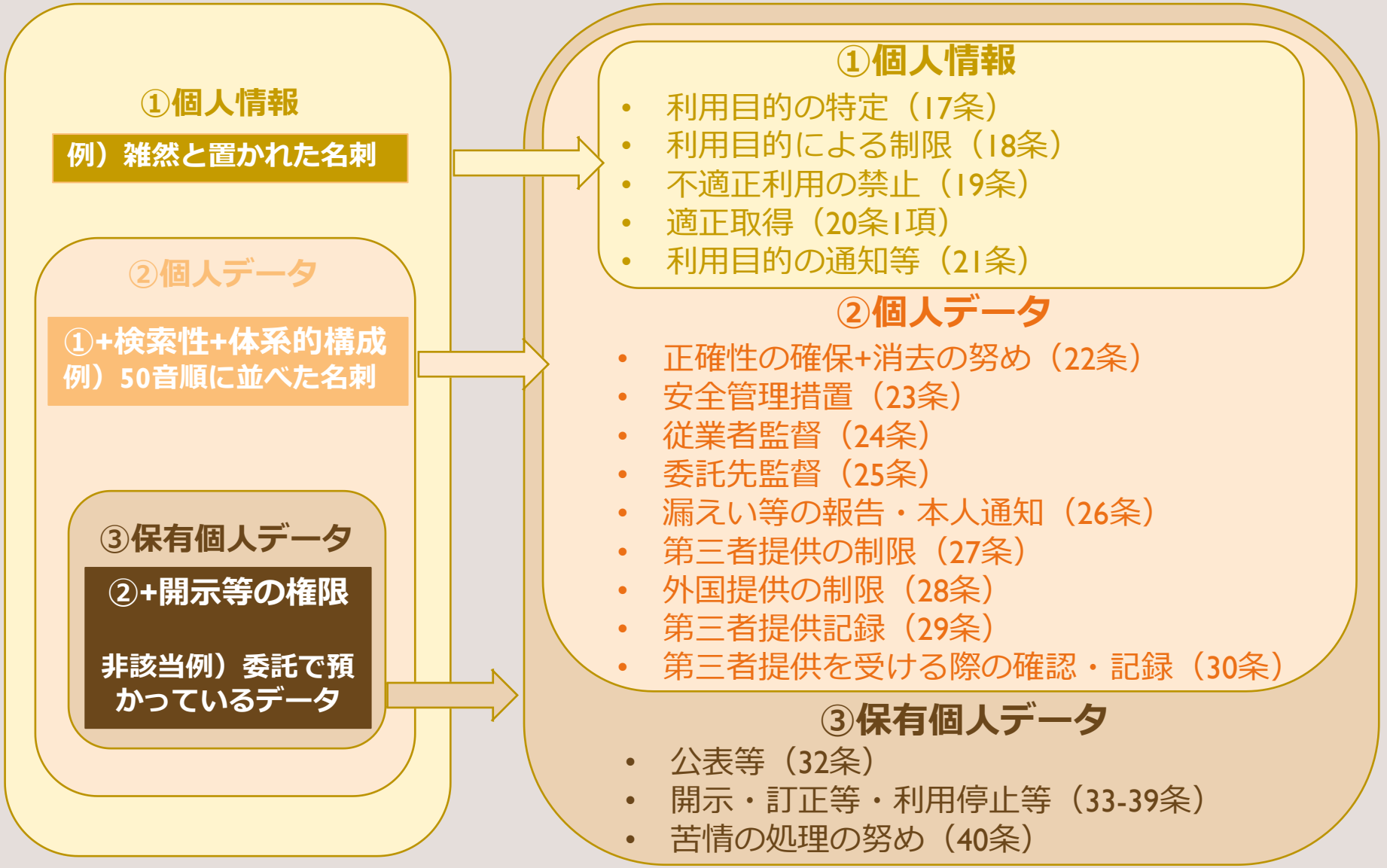
身体特徴系符号（法２条２項１号符号）	番号系符号（法２条２項２号符号）
イ）ゲノムデータ ロ）容貌 ハ）虹彩 ニ）声 ホ）歩行の態様 ヘ）静脈 ト）指紋又は掌紋 ※これらの組み合わせも含む ※ガイドライン通則編９~１１ページ 本人を認証することができるようにしたもの	イ）パスポート番号等 ロ）基礎年金番号 ハ）免許証番号 ニ）住民票コード ホ）個人番号（マイナンバー） ヘ）保険証等の記号、番号及び保険者番号等 ト）雇用保険証番号

※旧法でも個人情報として扱ってきたもの
　実務上も、「容易照合性」等その他から、個人情報として取り扱ってきたものと思われる

個人情報とは何か

（３）個人データ／保有個人データ

個人情報の定義が広いからこそ、規制対象が異なる



このほかに、
以下の規制もある

- 要配慮個人情報の取得規制（20条2項）
- 個人関連情報の提供制限等（31条）
- 仮名加工情報（41-42条）
- 匿名加工情報（43-46条）

個人情報の定義が広いからこそ、規制対象が異なる

- 個人データ
  - この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。
- 個人情報データベース等
  - この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。
    - 一　特定の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
    - 二　前号に掲げるもののほか、特定の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として政令で定めるもの

POINT ⇒ 検索性　体系的構成

↑図はR2改正法対応未済

個人情報の定義が広いからこそ、規制対象が異なる

- 保有個人データ
  - この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のものをいう。

POINT ⇒ 開示等の権限

個人情報 ＞ 個人データ ＞ 保有個人データ

↑図はR2改正法対応未済

個人情報とは何か

（４）要配慮個人情報

個人情報の保護の観点

- 情報は、その内容や性質によって、一概に悪い、良いと決められるものではない

内容

- どういう内容かに着目する。例えば、名刺１枚とカルテ情報が同様の取扱いでよいのか。
- **要配慮個人情報**、センシティブ情報、機微情報の議論につながる。
- しかし、病歴（要配慮個人情報）であっても、医療に必要であれば私たちは開示するし、医療従事者の間の共有や、医学研究者による活用も許容。ブログやＳＮＳなどで病状を公開する人も。

文脈

- どういう文脈で個人情報が取り扱われるかに着目する。例えば、治療なのか、興味本位なのか。
- **利用目的**の議論につながる。
- 名刺情報であっても、挨拶なのか、必要な情報の送付のためなのか、不要な勧誘電話のためなのか。
- 江沢民事件

検索性

- 利活用の程度、被害のおそれの程度に着目する。
- **個人データ**、個人情報データベース等、**マイナンバー**の議論につながる。

要配慮個人情報

要配慮個人情報

人種	本人の**人種**（法2条3項）	
信条	**信条**（法2条3項）	例）政治的思想
社会的身分	**社会的身分**（法2条3項）	
障害・健康等	**障害**（法2条3項、政令2条1号） 身体障害、知的障害、精神障害（発達障害を含む。）その他の規則で定める心身の機能の障害*があること	例）療育手帳を交付され所持している
	病歴（法2条3項）	例）ガンにり患
	診療等（法2条3項、政令2条3号） 健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための**指導**又は**診療**若しくは**調剤が行われたこと**	例）インフルエンザのため、2月11日にA病院内科を受診した
	健康診断等の結果（法2条3項、政令2条2号） 本人に対して医師その他医療に関連する職務に従事する者（「医師等」）により行われた疾病の予防及び早期発見のための健康診断その他の検査（「健康診断等」）の結果	例）健康診断の結果、ストレスチェックの結果、特定健康診査の結果

要配慮個人情報

要配慮個人情報

犯罪等	**犯罪の経歴（法2条3項）**	例）強盗の前科2犯
	刑事事件（法2条3項、政令2条4号） 本人を被疑者又は被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと	例）窃盗を被疑事実として逮捕された
	少年事件（法2条3項、政令2条5号） 本人を少年法3条1項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと	例）少年時代に傷害で審判を受けた
犯罪被害	**犯罪により害を被った事実（法2条3項）**	例）空き巣に入られた

法律による規制

- 原則として本人の同意を得て取得・提供
  - 実務的には、**オプトアウトによる第三者提供・取得の禁止**（２７条２項・２０条２項）

但し、金融ガイドラインに注意！

要配慮個人情報を取得・提供できる場合

類型	場合	取得	提供
法２７条１項類型	同意	○（法２０条２項柱書）	○（法２７条１項柱書）
	法令に基づく場合	○（法２０条２項１号）	○（法２７条１項１号）
	人の生命・身体・財産の保護のために必要で、 同意を得ることが困難	○（法２０条２項２号）	○（法２７条１項２号）
	公衆衛生の向上・児童の健全な育成推進のために 特に必要で、同意を得ることが困難	○（法２０条２項３号）	○（法２７条１項３号）
	国・自治体・受託者に協力する必要があり、 同意を得ると支障のおそれ	○（法２０条２項４号）	○（法２７条１項４号）
	取得者が学術研究機関等で学術研究目的で取り扱う必要	○（法２０条２項５号）	○（法２７条１項７号）
	提供者が共同研究者の学術研究機関等で学術研究目的で取得・提供する必要	○（法２０条２項６号）	○（法２７条１項６号）
	学術研究機関等が学術研究の成果の公表又は教授のためやむを得ないとき		○（法２７条１項５号）
	オプトアウト	×（法２０条２項になし）	×（法２７条２項）
非第三者 （法２７条５項類型）	委託	○（法２０条２項８号・政令９条２号）	○（法２７条５項１号）
	事業承継	○（法２０条２項８号・政令９条２号）	○（法２７条５項２号）
	共同利用	○（法２０条２項８号・政令９条２号）	○（法２７条５項３号）
法２０条２項類型	公開（by本人・国・自治体・規則）	○（法２０条２項７号）	―
	本人を目視又は撮影して、外形上明らかな 要配慮個人情報を取得する場合（政令７条１号）	○（法２０条２項８号・政令９条１号）	―

具体例で考える個人情報／個人データ／保有個人データ

例	個人情報か	個人データか	保有個人データか
注文書・注文請書・契約書	○	△	△
→担当者名、社長名等でも個人情報 →一枚でただ紙としてあるだけなら、個人情報ではあるが個人データではないが、顧客別にバインダで綴ったりすれば個人データかつ保有個人データ。			
監視カメラの映像	○	×	×
→映りこんでいる人の氏名がわからなくても基本的には個人情報 →通常は特定の個人が検索できるようになっていないので、基本的には個人データではない。			
社員情報・社員家族情報	○	△	△
→外部情報に限らず社員情報であっても個人情報			
社員の健康診断の結果	○	△	△
→要配慮個人情報に該当。 →一枚でただ紙としてあるだけなら、個人情報ではあるが個人データではないが、対象者別にバインダで綴ったり、データ管理すれば個人データかつ保有個人データ。			

※プライバシー権で保護されるかは、内容・文脈等による
※営業秘密の場合は、不正競争防止法による保護も及ぶ

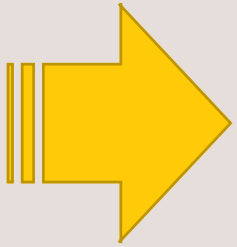
具体例で考える要配慮個人情報

例	個人情報か	個人識別符号か	要配慮個人情報か
履歴書の賞罰欄に記載された前科	○	×	○
→本人の意思で記載しているのであれば、会社は、本人同意に基づき取得できる。			
保険証の情報	○	○	△
→法律上は要配慮個人情報ではないが、マル障受給者証などは要配慮個人情報。			
ガン治療中の情報	○	×	○
→要配慮個人情報			
風邪やものもらいで受診した	○	×	○
→特に知られたくない傷病名でなくとも、要配慮個人情報			

- 要配慮個人情報に該当しない機微情報の例としては、薬局で自分で購入した薬の情報など（保健医療）

具体例で考える要配慮個人情報

例	個人情報か	個人識別符号か	要配慮個人情報か
健康診断を受けた	○	×	×
→受けた事実だけでは、要配慮個人情報ではない			
健康診断の結果	○	×	○
→健康診断の結果になると、要配慮個人情報			
身長、体重、体温データ	○	×	△
→健康診断、 診療等の事業及びそれに関する業務とは関係ない方法により知り得た場合は、要配慮個人情報ではない			



- 要配慮個人情報に該当したとしても、オプトアウトしていなければ、改正法による影響は基本的には受けない
- 本人から問診票や口頭で聞き取った場合、同意があると考えられる。緊急時に親族から病歴を聞き取ることも可（法２０条２項２号）

個人情報とは何か

（５）個人関連情報

個人データの提供規制

個人データを提供する際は規制がかかる。
それは当然だと思うが、では「個人データかどうか」はどう判断する？

提供元基準説？
（提供「元」にとって「個人データ」に当たるか）

提供元

ID	氏名
123	水町雅子
234	難波舞

ID	成績
123	80点
234	90点

個人データ

…個人データの提供規制に服する？

この提供元では、IDから名前を簡単にたどれるので、「容易照合性」があり、「個人データ」を保有

提供先

ID	成績
123	80点
234	90点

…個人データや個人情報を取得するわけではないので、個人情報の取得規制には服さない

個人データ**ではない**

提供する情報自体は、誰かわからない情報のみ。提供先においては、依然として誰かわからない状態のまま。

個人データの提供規制

個人データを提供する際は規制がかかる。
それは当然だと思うが、では「個人データかどうか」はどう判断する？

提供元基準説を取れば、個人情報保護法の規制が及ばない？

提供元

ID	成績
123	80点
234	90点

個人データではない

この提供元では、IDから名前等をたどれない

…個人データや個人情報を提供するわけではないので、個人データの提供規制には服さない？

提供先

ID	成績
123	80点
234	90点

ID	氏名
123	水町雅子
234	難波舞

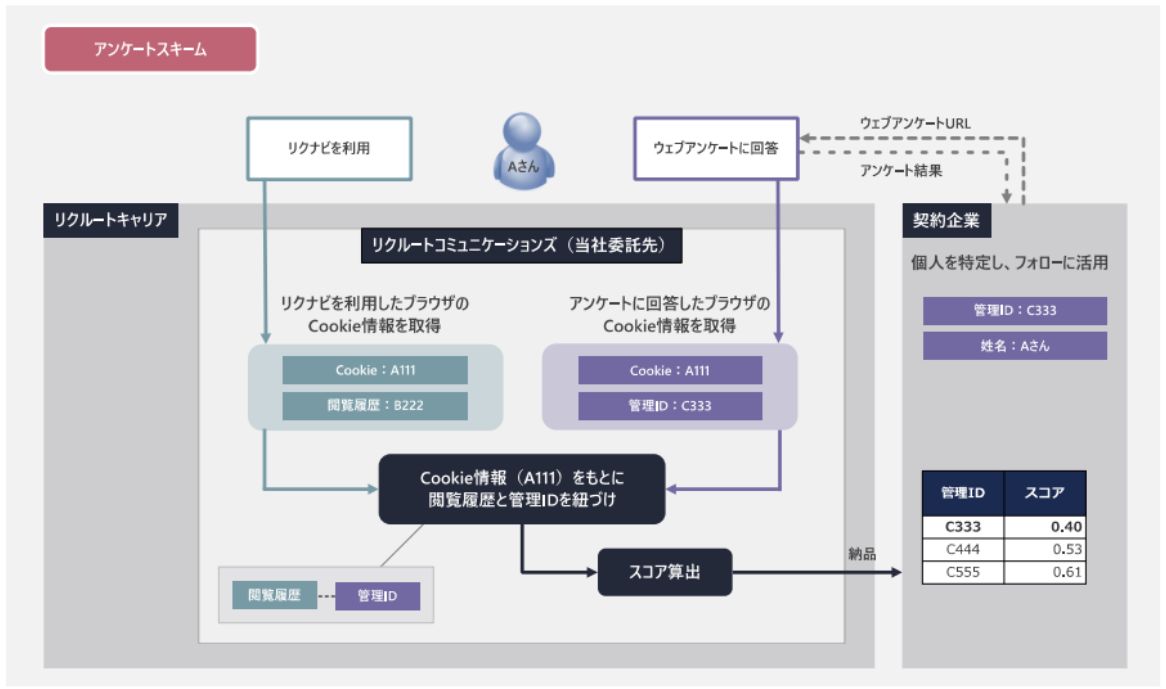
個人データ

…個人情報を取得するわけではない？？

取得する情報自体は、非個人情報。提供先で持っている他の個人データと照合して、誰かわかる。

個人関連情報の提供規制新設の背景（リクナビ）

<図 1> アンケートスキームにおけるデータの流れ



図Iスキームでのデータの状態

- リクルートコミュニケーションズでは、図Iの場合、氏名・住所等は保持していない
- 契約企業に提供する際は、管理IDとスコアのみ
- 契約企業では、管理IDから氏名等がわかる
- ※もっとも、別サービスのためリクルートコミュニケーションズ同一部署内で氏名等を保有しており、容易照合性から個人情報に該当（同社文書1pより）

法解釈はどうなるか、どうあるべきか

- 「提供元基準」を取ると、提供元である、リクルートコミュニケーションズにとっては個人データではない
- しかし、提供先においては個人情報として活用可能。
「提供元基準」「非個人情報構成」を用いた、不適切スキーム
- 「提供元基準」「非個人情報構成」を基に、
個人情報保護法適用を逃れようとしても、結局炎上する
- 大きくとらえれば、誰が内定辞退しそうかどうかの予測を、顧客企業に売却しているわけであり、不法行為に該当しそう。細かい点や技巧的解釈をこねくり回すよりも、ビジネスを大きく捉えたときに、一般人が本人の立場に立ってみたときに、素朴な感情として違和感・不快感を感じないか、消費者目線・相手方目線を忘れないようにする！

個人関連情報の提供規制新設の背景（リクナビ）

<図 7> 誤認識に基づく個人情報の第三者提供の流れ

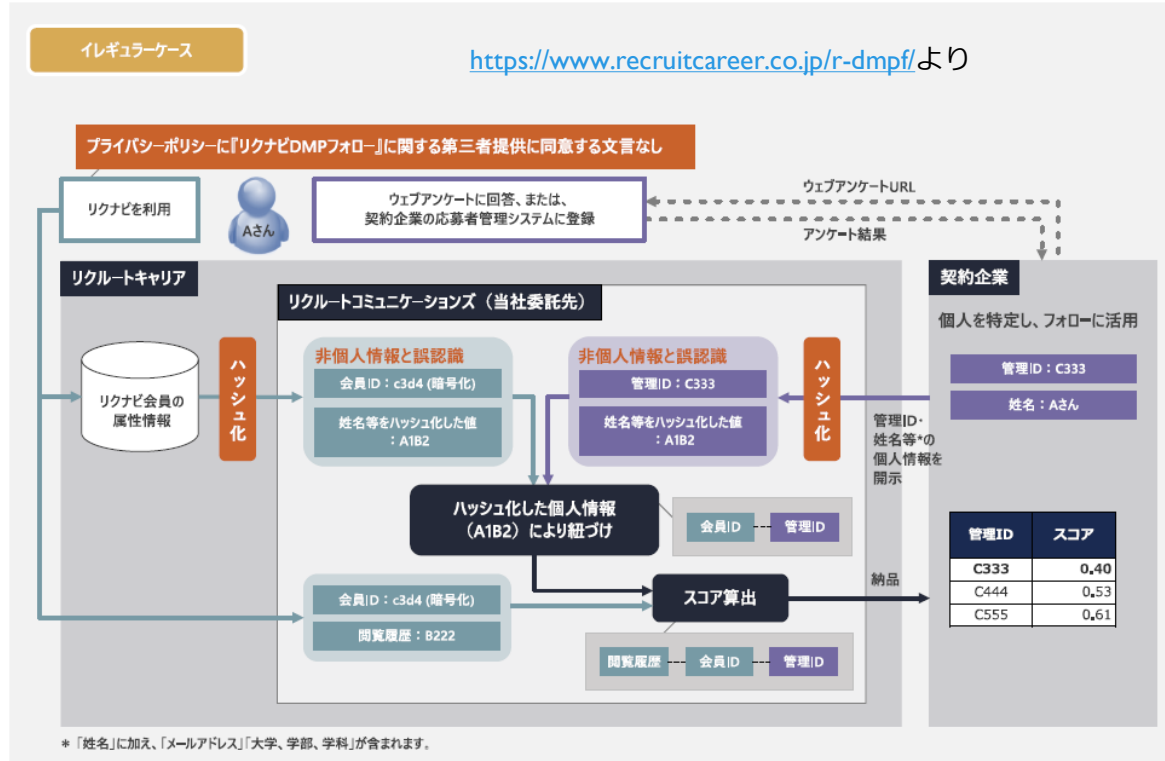


図7スキームでのデータの状態

- リクルートコミュニケーションズでは、氏名等は読めない（ハッシュ化）
- 氏名等が読めるのは、別会社のリクルートキャリアと、別会社の訳企業
- ただリクルートコミュニケーションズでも、氏名等は読めないものの同一人物かどうかがわかり、異なるID同士を氏名等ハッシュで紐づけられる（異なるIDでも同一人物のものか特定できる）

法解釈はどうなるか、どうあるべきか

- リクルートコミュニケーションズでは、個人情報ではないと誤認識したと公表
- またリクナビ側で同意を取得できていなかったケースがあったと公表
- いくら同意のチェックボックスを設けても、プライバシーポリシーや利用規約に記載していても、通常の合理的な人間なら同意しない内容を同意させるのは、「適切な同意」を取得できたとは言えないのではないか（ユーザは読まずに同意ボタンをクリックしている場合も）

個人関連情報の提供規制　新設

個人関連情報の提供規制の新設

前提	• 個人データを外部提供することは、一定の場合にしか認められない（法27条）。 • **個人データでなければ、外部提供に当たって特に法規制はなかった。**
法改正	• 自分にとって個人データでなくても、個人情報でなくても、**提供先が個人データとして取得することが想定***されるときは、提供が規制される（改正法31条）　→「**個人関連情報**」 ✓ *提供元が現に認識している場合及び同種の事業を営む事業者の一般的な判断力・理解力を基準にして通常想定できる場合をいう（GL85P) ✓ 契約で定めると良いが、契約していても個人データとしての利用・取得がうかがわれる場合は確認要（GL85P) • 提供できる場合は、**次の場合に限定** ✓ **法27条1項各号（法令に基づく場合等）** ✓ **本人同意が得られていることを確認した場合** • **記録・保存義務あり**（改正法31条3項で準用される30条3・4項。なお改正法31条3項では30条2項も準用。） • **外国への提供であっても同様**
改正背景	• リクナビのCookie情報の外部提供を踏まえての規制新設。したがって、Cookie等規制のための改正ともいえる。 • しかし、改正法ではCookie情報のみが規制されているわけではなく、**Cookieでなくても「個人関連情報」であれば規制対象。**
必要な対応	• 自社で、**個人関連情報を提供しているか**確認 ⇒　提供している場合、**本人同意**の取得、**記録の作成・保存対応**のスキーム・実務フロー等の検討

https://www.ppc.go.jp/files/pdf/201120_shiryou-1.pdf

個人情報とは何か

（６）それぞれの違い

個人情報等の種類
～様々な概念が複雑に入り組んでいる

個人関連情報

検索性等 （官）	個人情報　個人データ　保有個人データ　個人識別符号 保有個人情報　個人情報ファイル
内容・文脈	要配慮個人情報　機微情報（センシティブ情報） プライバシー　営業秘密
加工度合い （特殊）	個人情報　仮名加工情報　匿名加工情報　統計情報 行政機関等匿名加工情報　匿名加工医療情報

個人情報等の種類
～様々な概念が複雑に入り組んでいる

検索性等

（官用語は割愛）

個人情報
（個人識別符号含む）

個人データ

保有個人データ

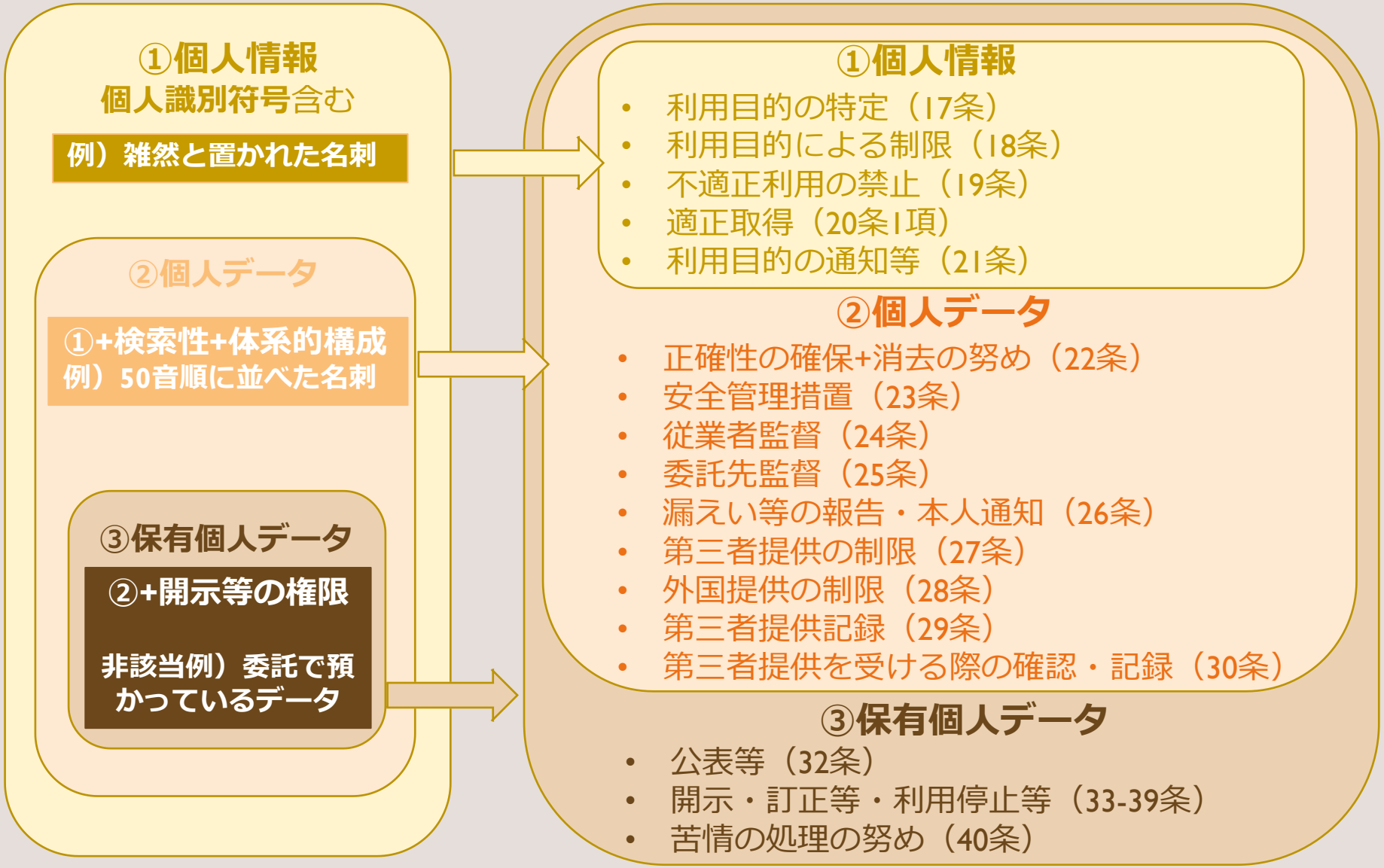
- 個人識別符号であれば個人情報となる。
- 個人情報（個人識別符号含む）が個人データかは、検索性・体系的構成があるかによる
- 個人情報（個人識別符号含む）が保有個人データかは、開示等の権限があるかによる

個人関連情報

- 個人関連情報は、自分にとっては個人情報ではない
- 提供先にとって個人データである

規制は次ページに
個人関連情報規制は前々ページに

個人情報の定義が広いからこそ、規制対象が異なる

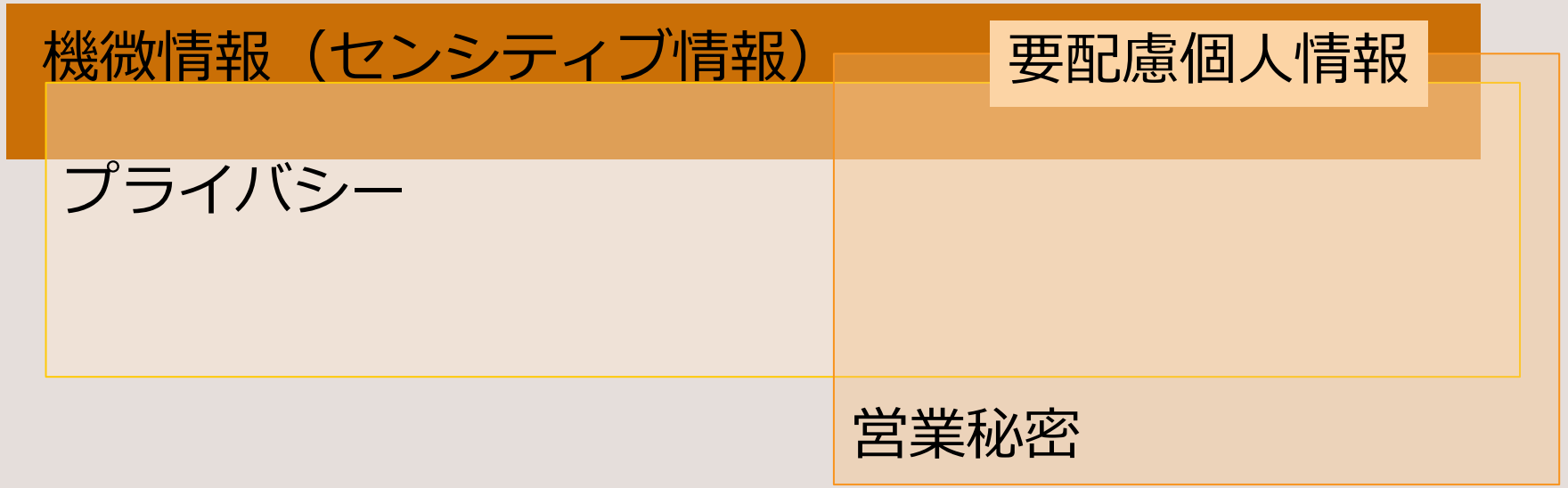


このほかに、
以下の規制もある

- 要配慮個人情報の取得規制（20条2項）
- 個人関連情報の提供制限等（31条）
- 仮名加工情報（41-42条）
- 匿名加工情報（43-46条）

個人情報等の種類
～様々な概念が複雑に入り組んでいる

内容・文脈



- 機微情報は金融GLの定義と自治体定義と一般用語があり、定義が定まらないため、広い
  →規制は金融GLが強い。自治体だと収集の原則禁止など。
- 要配慮個人情報は個人情報保護法上の定義があり、範囲が確定
  →特有の規制は、オプトアウト禁止（官はファイル簿への記載）。
- プライバシーは、機微情報・要配慮・営業秘密と重なる部分と重ならない部分がある
  →プライバシーの場合、不法行為による救済（損害賠償）等。
- 営業秘密は、機微情報・要配慮・プライバシーと重なる部分と重ならない部分がある
  （重ならない場合も多い。顧客名簿が営業秘密の場合、個人情報でもある場合が。
  宗教・医療情報を含む顧客名簿などは、機微情報・要配慮・プライバシーでもありうる。
  →営業秘密の規制は、不正競争防止法等。

個人情報の利活用

個人情報等の種類（加工強度別）

規制強い
加工強度弱い

生の個人情報	• そのままの状態（生データ）

仮名加工情報
NEW
	• パッと見、誰かわからなくなっている情報だが、法的には原則個人情報のまま
	  • ①特定の個人を識別できる記述等（氏名・住所・生年月日・郵便番号等）の削除・置換
	  • ②個人識別符号の削除・置換
	  • ③不正利用により財産的被害のおそれがある記述等の削除・置換
	• 個人情報への**義務が一部軽減**
	• **内部利用目的に限定**

匿名加工情報	• 誰かわからなくなっている情報
	  • ①特定の個人を識別できる記述等（氏名・住所・生年月日・郵便番号等）の削除・置換
	  • ②個人識別符号の削除・置換
	  • **④連結符号等の削除・置換**
	  • **⑤特異な記述等の削除**
	  • **⑥個人情報データベース等の性質を踏まえたその他の措置**
	• **容易な手続で**利活用・外部提供可能
	• 内部利用目的に**限定されない**
	• 再識別は禁止

統計情報	• 特定の個人との対応関係がなく、完全に個人情報でも個人に関する情報でもない • 匿名加工情報との境界は曖昧な部分が残る

規制弱い
加工強度強い

個人情報を利活用できるのか

個人情報というと「同意」がないと何ら使えないという誤解もあるが、以下を正しく検討し、利活用できるか考えよう

⓪使いたい情報は「個人情報」なのか、それ以外なのか

それ以外：個人関連情報／仮名加工情報／匿名加工情報等

①自分のやりたい行為が「利用」なのか「提供」なのか

- 同一法人内での「**利用**」なのか
- 同一法人ではない者に渡したりもらったりする「**提供／取得**」なのか

②「利用」なら「目的内利用」なのか「目的外利用なのか」

- 使いたい個人情報の「**利用目的**」をプライバシーポリシー等で確認する
- 自分のやりたい行為が、その範囲内なら「**目的内利用**」、範囲外なら「目的外利用」

③「提供」ならどの法的根拠に基づくのか

- 委託、オプトアウト、共同利用、公衆衛生、事業承継　等々

個人情報の利活用

（１）個人情報の利用（目的内利用／目的外利用）

個人情報を取得するに当たって

個人情報を
何のために聞かれているのか
何に使われるのかわからない
怖いかも・・・

個人情報を
このために使いますよ

- 何に使うか（利用目的）をまず特定する
  - 例えば、商品や案内の送付、マーケティング、人事管理など
  - 個人情報保護法第１７条第１項

個人情報を取得するに当たって

個人情報を
何のために聞かれているのか
何に使われるのかわからない
怖いかも・・・

個人情報を
このために使いますよ

- 何に使うか（利用目的）が相手にわかるようにする
  - 例えば、書面に記載して渡す、Webサイトで公表するなど
  - 本人から直接取得する場合は、あらかじめ、本人に示す
  - それ以外は、あらかじめ公表するか、取得後速やかに通知するか、取得後速やかに公表する
  - 利用目的が明らか、本人・第三者の権利利益を害する恐れがある場合などは、通知・公表等不要（個人情報保護法第２１条第４項各号）
  - 個人情報保護法第２１条

利用目的の考え方

- 個人情報保護法というと、本人同意を取得しなければならない規制との誤解もあるが、個人情報保護法の規律の要は「**利用目的**」
- 情報は、その内容や性質によって、一概に悪い、良いと決められるものではない

内容

- どういう内容かに着目する。例えば、名刺１枚とカルテ情報が同様の取扱いでよいのか。
- 要配慮個人情報、センシティブ情報、機微情報の議論につながる。
- しかし、病歴（要配慮個人情報）であっても、医療に必要であれば私たちは開示するし、医療従事者の間の共有や、医学研究者による活用も許容。ブログやＳＮＳなどで病状を公開する人も。

文脈

- どういう文脈で個人情報が取り扱われるかに着目する。例えば、治療なのか、興味本位なのか。
- 利用目的の議論につながる。
- 名刺情報であっても、挨拶なのか、必要な情報の送付のためなのか、不要な勧誘電話のためなのか。
- 江沢民事件

検索性

- 利活用の程度、被害のおそれの程度に着目する。
- 個人データ、個人情報データベース等、マイナンバーの議論につながる。

利用目的の意義

個人情報を
何のために聞かれているのか
何に使われるのかわからない
怖いかも・・・

個人情報を
このために使いますよ

- 「私の個人情報を何に使うのだろうか」
- 「こんなつもりで使われるとは思わなかった」
- 「こんなつもりで提供したわけではなかった」

といった、誤解をなくす。本人がわかるようにする。

個人情報を利用するに当たって

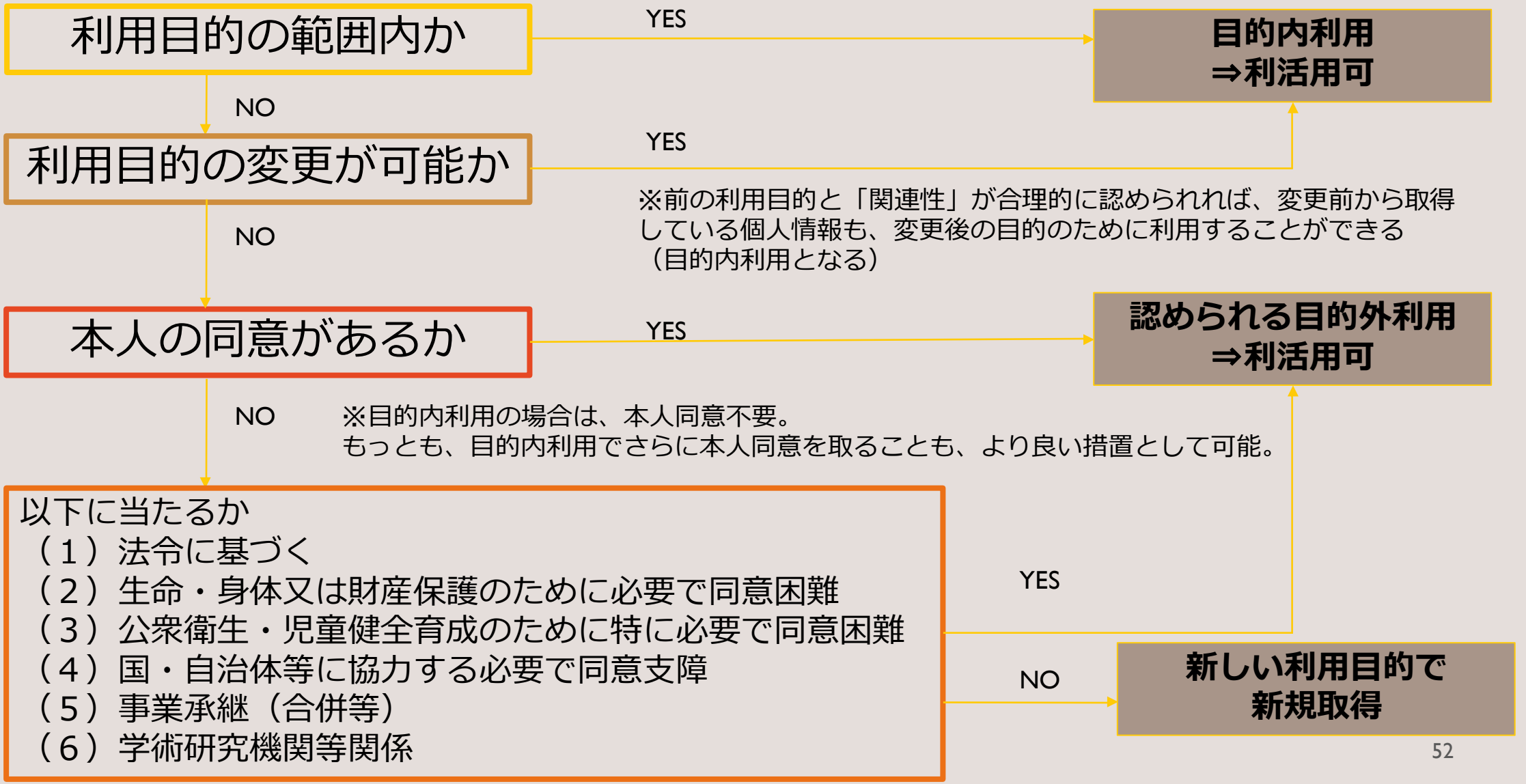
約束した範囲外には、
ご本人の同意があるか、
法令で認められた場合以外、
個人情報を使いませんよ

- 本人の同意なく、利用目的の範囲を超えて、個人情報を取り扱わない
  - ○　誰が利用者で、連絡先はどこか、既往歴は何かを、○○サービスの実施のために把握・管理する
  - ×　新しい事業を始めたので、取得していた個人情報を使って、宣伝の電話をかける、手紙を送る
    - →もっとも、利用目的として、これを特定すれば、利用可
    - →本人の同意をとれば、利用目的として特定していなくても、利用可
  - ○　急病のため、把握していた病歴・連絡先を利用する
    - **→利用目的として特定していなくても、生命・身体・財産の保護のために必要があって、同意を得ることが困難な場合は、利用目的の範囲外でも取り扱える**
  - 個人情報保護法第１８条第１項・第３項

利用目的に基づく規律

利用目的を 特定する （１７条１項）	やるべきこと	• 本人が自分の個人情報を何に使われるかわかるようにする • 何のために使うのか、本人がわかるレベルで特定する
利用目的を 公表等する （２１条１・２項）	やるべきこと	• 本人が自分の個人情報を何に使われるかわかるようにする • Ｗｅｂ公表、ポスター掲示、本人に書面交付等
利用目的の 範囲内で取り扱う （１８条）	やるべきこと	• あらかじめ決めた利用目的の範囲内で取り扱う 例外）同意、法令、生命・身体・財産の保護、公衆衛生の向上又は児童の健全な育成の推進、国・自治体・受託者への協力の必要 例外）第三者提供規制は、利用目的の範囲内か問わない

個人情報利用の検討フロー



目的内利用の解説

利用目的の範囲内か

YES

目的内利用
⇒利活用可

NO

利用目的の変更が可能か

YES

- 法律上、「利用目的の特定」「通知又は公表」義務がある。
- 通常は、プライバシー・ポリシーなどで公表しているので、プライバシー・ポリシー等に記載している利用目的を確認する。
  ※公的機関はファイル簿を要確認
- 今、行いたい利用が、既存の利用目的に含まれるかを検討する。

- 既存の利用目的を確認する。
- 既存の利用目的と今、行いたい利用の目的との間に「関連性」が合理的に認められるかを検討する。
- H27法改正で、利用目的変更の範囲が拡大されたものの、厳しい判断に変わりはないので、変更できる場合は限定される
- 利用目的の変更ができれば、変更前から取得している個人情報も、変更後の目的のために利用することができる（目的内利用となる）
- 仮名加工情報でもよければ、「関連性」がなくとも自由に利用目的の変更が可能なので、仮名加工情報を検討しても良い。

目的内利用の解説：利用目的の変更

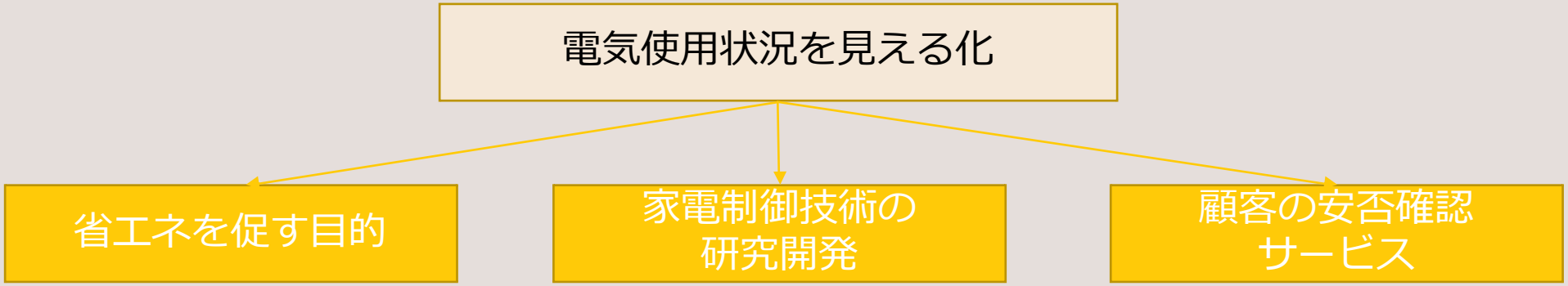
- 一度利用目的を特定しても、その後、別の目的のために利用する必要性が生じる場合も
- 再度利用目的を特定しなおして、個人情報を取得しなおすのは、事業者にとっても本人にとっても負担になる場合も

- そこで個人情報保護法では利用目的の変更を認めている
- もっとも無制約に変更できてしまっては、利用目的の意味がなくなる

改正前	個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない（17条2項）。
H27改正後	個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない（17条2項）。
仮名加工情報 R2改正後	仮名加工情報、仮名加工情報である個人データ及び仮名加工情報である保有個人データについては、第十七条第二項、第二十六条及び第三十二条から第三十九条までの規定は、適用しない（41条9項）。

目的内利用の解説：利用目的の変更例

- 電力会社が、顧客に省エネを促す目的で、家庭内の機器ごとの電気使用状況を収集して、その使用量等を分析して顧客に提示をしていた場合、あるいは、同じ情報を用いて家電制御技術の研究開発とか、その顧客の安否確認のサービスを行うということができる
  - 山口国務大臣発言　第189回国会　内閣委員会　第4号（平成27年5月8日（金曜日））



目的外利用の解説

本人の同意があるか

YES → **認められる目的外利用 ⇒利活用可**

NO

※目的内利用の場合は、本人同意不要。
もっとも、目的内利用でさらに本人同意を取ることも、より良い措置として可能。

以下に当たるか
（１）法令に基づく
（２）生命・身体又は財産保護のために必要で同意困難
（３）公衆衛生・児童健全育成のために特に必要で同意困難
（４）国・自治体等に協力する必要で同意支障
（５）事業承継（合併等）
（６）学術研究機関等関係

YES → **認められる目的外利用 ⇒利活用可**

YES

NO → **新しい利用目的で新規取得**

- ◆ 目的内利用の場合は、本人同意不要
- ◆ 本人が真に同意しているかがポイント
- ◆ 書面（契約書、同意書等）でサインしてもらう必要はない、Webで同意ボタンクリックでもよい
- ◆ 口頭同意でもよいが、記録に残せる形が望ましい
- ◆ 明示の同意／ 黙示の同意という概念もある

- ◆ 目的外利用でも、個人情報保護法１８条２・３項に定める場合は、本人同意なく利用可能。
- ◆ 提供規制とほぼパラレルなので、詳細は提供規制をご参照。

個人情報の利用例

例１）自社のPC製品の顧客に新PC・付属品案内のDMを送付できるか

→通常は可能なようにプライバシーポリシーが作成されている

- 利用目的をプライバシーポリシーなどで確認
  - OKな利用目的例「商品・サービス・キャンペーン情報の提供・DM発送」
- DM発送とまで具体的に記載されていなくても、その利用目的を読んで、一般人が「これならDMも来るな」とわかればOK　※特電法(オプトイン規制等）に要注意
- 目的内利用として個人情報保護法上適法（＆本人提供は第三者提供に当たらない）

例２）企業の自社Webサイトでの行動履歴・購買履歴を分析できるか

→プライバシーポリシーに記載されている利用目的に依る

- 統計的把握でなく個人情報のまま〇〇さんがこういう行動をしていてこういうときにこういう商品を買っているなどの分析をすることも可能な場合がある。利用目的による。新商品開発？サービス改良？
- プライバシーポリシーなどで確認
  - 利用目的例「商品やサービスの開発・改善」←個人情報のままでOK・当然安全管理措置等が必要
  - 利用目的例「商品開発のための統計データの作成・集計」←統計のみOK
- 統計的把握なら、上記構成によらずとも、利用目的に明記していなくてもOK
- もっとも、Cookie規制等が強化される可能性もあり、最新動向に常に留意しないと違法となる恐れも

個人情報の利用例

例３）複数会社のWebサイト間で行動履歴・購買履歴を分析し潜在顧客にアプローチできるか

→情報の内容、分析の詳細、アプローチの方法等にもよって、大きく異なる

- このような個人情報利用について、社会的許容性や本人の予測可能性はあるか
- 複数会社間での情報授受について、法的根拠はあるか
  - 共同利用（複数会社が親子会社等の場合、共同キャンペーンの場合等）
  - 同意（本人へわかりやすく説明して、適切な同意を取れるか）
  - オプトアウト（本人へ拒否方法をわかりやすく説明して、通知また公表、届出を行う）
- 利用目的をプライバシーポリシーなどで確認
  - 例「Aサイト、Bサイト、Cサイトと共同で商品・サービス・キャンペーン情報の提供・DM発送」はどうか？
  - GDPR対応の企業サイトだと、かなり詳細に記載している例もある
- Cookie規制等の最新動向に常に留意
- 本人へのアプローチは拒否反応も強い
  - 特に、直接のメール、郵便、SMSなどは、拒否反応も強い

個人情報の利用例

例４）自社の通販サイトでどのような顧客が購入しているか、AIに学習させられるか

- 例２と同じ

例５）自社従業者の勤務状況をIoT製品でチェックできるか

→態様による

- 利用目的は何か
  - 「雇用管理」「勤怠管理」の場合、タイムカード的な利用は可能であろう
  - A処理に〇秒かけている、B処理は平均的従業員より処理が遅い、集中しておらずPCを打っていないなどと管理することは、違法性を帯びる可能性もある
- 仮に、利用目的として十分に特定されていたとしても、労働者の人権侵害に当たる可能性がある

個人情報の利活用

（２）個人情報の外部提供

個人情報を提供するに当たって

個人情報を
勝手に提供されないか
怖いかも・・・

個人情報は
法律上認められた範囲でしか提
供しません

- 個人情報を提供できる場合
  - 後述
- H27/R2改正法で、提供記録、外国への規制等

個人データを提供できる場合

ルール	第三者に個人データを提供できる場合は、法律上限定されている（27条）。

ポイント①　対象は「個人情報」ではなく「個人データ」

ポイント②　本人同意を得なくても、提供できることが法律上認められている

提供できる場合	
①　本人の同意がある場合（法27条1項柱書）	• 書面でなくてもよい • Webサイトでチェックボックスにチェックしてもらうなどの方法も可 • 口頭でもよいが、重要度によって、原則として記録が残せる形が良い
②　法令に基づく場合（法27条1項1号）	例）令状に基づき裁判所に提出
③　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（法27条1項2号）	例）災害時、意識不明時、重度の認知症の高齢者の状況を家族等に説明する等

個人データを提供できる場合

提供できる場合

④　公衆衛生の向上又は児童の健全な育成の推進のために特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（法27条1項3号）	例）健康増進法に基づく地域がん登録事業による国又は地方公共団体への情報提供 、児童虐待の情報提供
⑤　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行 することに対して協力する必要がある場合であって、本人の同意を得ることにより 当該事務の遂行に支障を及ぼすおそれがあるとき（法27条1項4号）	例）統計法に定める一般統計調査に協力する
⑥　学術研究機関等（法27条1項5～7号）	例）企業と大学で共同研究しており、企業から大学に研究用データを提供
⑦　**オプトアウト**（法27条2項）	例）一定事項を通知等要。本人に求められれば提供を止める
⑧　委託（法27条5項1号）	例）データ入力業者への委託、印刷業務の委託
⑨　事業の承継（法27条5項2号）	例）合併先の会社
⑩　**共同利用**（法27条5項3号）	例）一定事項を通知等必要。病院と訪問看護ステーション

個人情報保護法が適用されない場合

「個人情報保護法」によって憲法上の権利が脅かされないよう、適用されない場合（適用除外）が定められた（個人情報保護法57条）

放送機関、新聞社、通信社その他の**報道機関**（報道を業として行う個人を含む。）
→個人情報等及び個人関連情報の取扱目的の全部又は一部が、**報道**の用に供する目的の場合

著述を**業**として行う者
→個人情報等及び個人関連情報の取扱目的の全部又は一部が、**著述**の用に供する目的

宗教団体
→個人情報等及び個人関連情報の取扱目的の全部又は一部が、
宗教活動（これに付随する活動を含む。）の用に供する目的

政治団体
→個人情報等及び個人関連情報の取扱目的の全部又は一部が、
政治活動（これに付随する活動を含む。）の用に供する目的

※上記の者でも、上記目的外なら個人情報保護法が適用
例）報道機関や宗教団体が人事目的で従業員情報を取り扱う場合は適用

学術研究は？

これまでは適用除外

- **令和3年個人情報保護法改正までは**、学術研究機関等による学術研究目的の場合も個人情報保護法が**適用除外**されていた
- 個人情報保護委員会の勧告・命令等の権限行使についても、学問の自由を妨げてはならず、民間事業者が学術研究機関等に個人情報を提供する際も、個人情報保護委員会の権限は行使しないとされていた

EUとの個人データ授受

- 個人情報保護法の適用除外としている結果、ＧＤＰＲ十分性認定の効力が及ばず、日本とEUとで学術研究のためのデータの授受の支障にも

令和3年改正

- 学術研究機関等による学術研究目的の場合も**個人情報保護法が適用に（令和4年春目途）**
- 但し、通常の民間事業者よりも、内部利活用や個人データ授受が**比較的容易に**できるようにされた

受領者

個人データ

提供者

①学術研究の成果の公表・教授（27条1項5号）	
・受領者は誰でも可	・提供者は学術研究機関 ・当該個人データの提供が学術研究の成果の公表又は教授のためやむを得ない必要あり ・個人の権利利益を不当に侵害するおそれがある場合は提供不可
②学術研究目的での提供（27条1項6号、20条2項6号*）	
・受領者は共同して学術研究を行う者	・提供者は学術研究機関 ・当該個人データを学術研究目的で提供する必要があるとき（学術研究目的は提供目的の一部であっても可） ・個人の権利利益を不当に侵害するおそれがある場合は提供不可 ・**学術研究機関等による学術研究目的での取扱い（目的外利用）も可**（18条3項5号）
③受領者が学術研究目的（27条1項7号、20条2項5号*、18条3項6号）	
・受領者は、学術研究機関等で、当該個人データを学術研究目的で取り扱う必要があるとき（学術研究目的は取扱目的の一部であっても可）	・提供者は誰でも可（個人情報取扱事業者） ・個人の権利利益を不当に侵害するおそれがある場合は提供不可

学術研究機関等とは

・大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者をいう（個人情報保護法16条8項）。
・個人情報保護法がこれまで適用除外されてきたが、令和3年改正で適用除外されなくなった。GDPR適用上はこれで有利になるとも考えられる。
・報道機関、著述を業として行う者、宗教団体、政治団体についてはこれまで通り個人情報保護法が適用除外される（個人情報保護法57条1項）。

*は要配慮個人情報の取得規制の場合

個人情報の提供例

例１）委託先に個人情報を提供できるか（本人同意はない場合）

→本人の同意なくできる

- 委託に必要な個人情報であれば、本人同意なく提供可能
  - 委託に名を借りただけの不適切な提供は不可

例２）委託先から個人情報を収集できるか（本人同意はない場合）

→本人の同意なくできる

- 個人情報の収集を委託することは可能
- 例えば、マイナンバーの収集委託、顧客の住所変更事務委託などが可能
- もっとも、委託先が不適切な収集をしている場合は、委託元の責任を問われうる

個人情報の提供例

例３）自社の賃借人情報を他社に渡せるか（本人同意はない場合）

→本人の同意なくできる

- 不動産売買契約に付随して、不動産の売主から買主に対して、当該不動産の管理に必要な範囲で当該不動産の賃借人の個人データを提供することは、本人同意がなくてもできる（事業承継に当たる）
- 個人情報保護委員会Q&A　Q2-10-2

例４）自社の顧客情報を他社に売却できるか（本人同意がある場合）

→ケースバイケースだが、難しい場合が多い

- 本人同意があっても、常識的に見て本人が同意するとは思えないような場合は、本当に真の同意があるのかどうか疑われうる
- 本人への説明、本人が同意する意思、同意取得方法が十二分に適切である必要

個人情報の提供例

例５）自社が委託を受けて保持している個人情報を他社に渡せるか（委託先指示による場合）

→できる場合が多い

- 委託先が個人情報提供を指示した場合は、できる場合が多い
- もっとも、委託先からその相手への提供行為が違法かどうかはわからないので、委託先に保証してもらうべき

例６）自社が委託を受けて保持している個人情報を他社に売却できるか

→できない

- 委託を受けて保持している情報は、あくまで委託元のもの。自社（委託先）が好き勝手にできるわけではない。時々、自分のところで持っているデータは自分のものであり自由にできると勘違いしている企業がいるので、注意すべき。自社が委託元で外部に委託する場合、外部委託先がそのような勘違いをしていないかも十二分にチェック・監督し、委託契約で縛るなど必要な措置を取らなければならない
- もっとも、委託先指示による場合などで、そのことが立証できる場合など、あらゆる場合に不可能なわけではないかもしれない

加工情報の利活用

（１）仮名加工情報／匿名加工情報

個人情報等の種類（加工強度別）

規制強い
加工強度弱い

生の個人情報	• そのままの状態（生データ）

仮名加工情報
NEW
	• パッと見、誰かわからなくなっている情報だが、法的には原則個人情報のまま
	  • ①特定の個人を識別できる記述等（氏名・住所・生年月日・郵便番号等）の削除・置換
	  • ②個人識別符号の削除・置換
	  • ③不正利用により財産的被害のおそれがある記述等の削除・置換
	• 個人情報への**義務が一部軽減**
	• **内部利用目的に限定**

匿名加工情報	• 誰かわからなくなっている情報
	  • ①特定の個人を識別できる記述等（氏名・住所・生年月日・郵便番号等）の削除・置換
	  • ②個人識別符号の削除・置換
	  • **④連結符号等の削除・置換**
	  • **⑤特異な記述等の削除**
	  • **⑥個人情報データベース等の性質を踏まえたその他の措置**
	• **容易な手続で**利活用・外部提供可能
	• 内部利用目的に**限定されない**
	• 再識別は禁止

統計情報	• 特定の個人との対応関係がなく、完全に個人情報でも個人に関する情報でもない • 匿名加工情報との境界は曖昧な部分が残る

規制弱い
加工強度強い

個人情報の状態（例）

生の個人情報

氏名	住所	生年月日	性別	世帯年収	既婚／独身	子の有無
水町雅子	千代田区五番町2	1983/10/23	女性	300-400万	既婚	なし
水町雅男	千代田区五番町2	1984/05/03	男性	300-400万	既婚	なし
難波舞	千代田区霞が関3-1	1970/06/18	女性	800-900万	独身	なし
番号太郎	千代田区麹町1-2	1963/09/25	男性	500-600万	既婚	あり
千代田一郎	千代田区神保町2-3-5	1997/10/10	男性	5000万-5500万	独身	あり

抽象化情報

氏名	住所	生年月日	性別	世帯年収	既婚／独身	子の有無
ー	千代田区五番町2	1983/10	女性	300-400万	既婚	なし
	千代田区五番町2	1984/05	男性	300-400万	既婚	なし
	千代田区霞が関3	1970/06	女性	800-900万	独身	なし
	千代田区麹町1	1963/09	男性	500-600万	既婚	あり
	千代田区神保町2	1997/10	男性	5000万-5500万	独身	あり

削除

番地以下削除

年齢・月齢情報を保持したうえで日の削除

千代田区神保町2のデータは、
氏名等を加工しても、誰の情報かわかるおそれあり

72

個人情報の状態（例）

仮名加工情報

氏名	住所	生年月日	性別	世帯年収	既婚／独身	子の有無
－	千代田区五番町2	1983/10	女性	300-400万	既婚	なし
	千代田区五番町2	1984/05	男性	300-400万	既婚	なし
	千代田区霞が関3	1970/06	女性	800-900万	独身	なし
	千代田区麹町1	1963/09	男性	500-600万	既婚	あり
	千代田区神保町2	1997/10	男性	5000万-5500万	独身	あり

削除

番地以下削除

年齢・月齢情報を保持したうえで日の削除

財産的被害のおそれ？どう加工すればよいか？

匿名加工情報

氏名	住所	生年月日	性別	世帯年収	既婚／独身	子の有無
－	千代田区五番町2	1983/10	女性	300-400万	既婚	なし
	千代田区五番町2	1984/05	男性	300-400万	既婚	なし
	千代田区霞が関3	1970/06	女性	800-900万	独身	なし
	千代田区麹町1	1963/09	男性	500-600万	既婚	あり
	千代田区神保町2	1997/10	男性	2000万超	独身	なし

削除

番地以下削除

年齢・月齢情報を保持したうえで日の削除

上位・下位5%丸め処理

その他特異データの削除、ノイズ付加等

73

個人情報の状態（例）

統計情報

必ずしもここまで丸める
必要はない

住所	年齢構成	性別	世帯年収	既婚／独身	子の有無
千代田区五番町	高め（平均X)	男性55%	平均700万	既婚75%	あり55%
千代田区霞が関					
千代田区麹町					
千代田区神保町					

統計情報の場合、レコードが1になってはダメ。統計によって、3以上、5以上、10以上などのルールあり。

74

概要

	仮名加工情報	匿名加工情報
概要	◆ 個人情報パッと見*誰かわからなく加工する ◆ パッと見**誰の情報かわからなくさせる**ことで、個人（消費者等）を保護 ◆ 個人情報である場合とない場合がある ◆ 簡単な手続で、利用目的の変更（事実上の目的外利用）ができるが、外部提供は難しい	◆ 個人情報を完全に匿名加工する ◆ **誰の情報かわからなくさせる**ことで、個人（消費者等）を保護 ◆ 個人情報ではなくなる ◆ 簡単な手続で、内部での利活用や外部提供が可能
注意点	◆ 個人情報保護法の対象外となるわけではない。 すなわち、一切のルールが課されないわけではなく、一定のルールに従う必要がある。 もっとも、そんなに大変なルールではない。	
	◆ **法定の加工基準**を満たす必要があるが、法定基準が**簡素かつ比較的明確**	◆ **法定の加工基準**を満たす必要があるが、法定基準が**厳格かつ抽象的**。 自分が利活用したいデータが厳格な加工を施せるものか、適したものかを十分検討する必要がある。

加工基準

	仮名加工情報	匿名加工情報
加工基準	①　特定の個人を**識別**することが**できる記述等の削除**又は復元できない**置換** →例）氏名削除、住所丸め、生年月日の日削除	
	②　**個人識別符号の削除**又は復元できない**置換** →例）マイナンバー削除、保険証記号番号削除、生体認証情報削除	
		③　**情報を相互に連結する符号の削除**又は復元できない**置換** →例）内部IDの置換・削除
		④　**特異な記述の削除**又は復元できない**置換** →例）身長195センチ情報の丸め・削除　難
	③　不正に利用されることにより**財産的被害が生じるおそれのある記述等の削除**又は復元できない**置換** →例）クレジットカード番号削除	⑤　個人情報データベース等の性質を踏まえたその他の**適切な措置**　難

個人情報と匿名加工情報と仮名加工情報の違い

自社が保有する顧客情報について、顧客の属性ごとに購買履歴を分析したい場合

種類	個人情報	匿名加工情報	仮名加工情報
データの**状態**	**易** • 誰の情報かがわかる状態でOK • 生データの状態でよい	**難** • 誰の情報かがわからないように加工することが必要 • ただ、**活用できる度合いが低くなる可能性**も	**普通** • 利活用する情報だけでは、誰の情報かわからないように加工する必要 • ただ加工基準が明確
ルール **目的外利用**	**難** • **利用目的を確認**する • 利用目的に「顧客動向分析」などとあれば、利用目的の**範囲内**で、分析可 • 利用目的の**範囲外**なら、**本人の同意等**、個人情報保護法１８条に定める要件が必要 • 利用目的の**事後変更**もできるが、規制あり（関連性要）	**易** • **利用目的の範囲内でも範囲外でもOK**	**まあ易** • **利用目的の事後変更が制限なく可能** • 変更後の利用目的の範囲内なら、OK（OKなように利用目的を変更するということ） • 変更後の利用目的の公表等は必要 • 電話、郵便、FAX、電報、電子メール、SMS、住居訪問等は禁止

個人情報と匿名加工情報と仮名加工情報の違い

他社が保有する顧客属性情報と自社が保有するデータを組み合わせて分析したいので、
他社から情報を入手したい場合

種類	個人情報	匿名加工情報	仮名加工情報
前のスライドのルールに加えて……			
ルール 提供	**難** • グループ会社等で**共同利用**の要件を満たす場合は、個人情報保護法２７条５項３号で可 • **オプトアウト**（拒否されたらやめる）でも、個人情報保護法２７条２・３項で可能だが、社会的非難を浴びる可能性もある。また要配慮個人情報（健康診断結果、病院受診、病歴、犯罪歴等）はオプトアウト不可 • **本人同意**が必要な場合も多い	**易** • 以下の**簡易な手続で可** • 提供時に情報項目＆提供方法の**公表** • 提供先に対し匿名加工情報であることの**明示**	**大変難** • 法令に基づく場合以外、第三者提供不可（オプトアウトやその他の２７条１項各号不可）（４１条６項・４２条１項） • **委託・事業承継・共同利用**の第三者に当たらない場合は、提供**可**（４１条６項・４２条２項） • **本人同意**が必要な場合が多い

個人情報と匿名加工情報と仮名加工情報の違い

自社が保有する顧客情報について、顧客の属性ごとに購買履歴を分析したい場合

種類	個人情報	匿名加工情報	仮名加工情報
ルール 安全管理	**難** • **義務**（個人情報保護法２３条）	**普通** • **加工方法等については義務**（個人情報保護法４３条２項） • **匿名加工情報自体については努力義務**（個人情報保護法４３条６項・４６条）	**難** ・義務（個人情報保護法２３条・４１条２項・４２条３項）
ルール 開示等	**難** • 本人から求めがあれば、保有個人データは**原則開示が義務**（個人情報保護法３３条） • 訂正・利用停止請求も	**易** • 開示不要（反対に、誰の情報かわからないので、本人特定ができず、開示できない）	**易** • 開示不要（個人情報保護法４１条９項にて３３等条が適用除外）

匿名加工情報にかかるルール

規制総論	加工（４３条１項）
	■ 規則で定める基準（住所の市町村以下を削除、特殊な情報の削除、ノイズ付加等）・認定個人情報保護団体による自主ルールに従って加工 ■ 要配慮個人情報も匿名加工情報にできる
	安全管理措置（４３条２項・４６条）
	■ 削除した情報や加工方法に関する情報の漏えいを防止するために安全管理
	公表（４３条３・６項）
	■ 情報項目を公表。 匿名加工情報には開示等請求が認められていないため、公表によって、本人が関与
	識別禁止（４３条５項・４５条）
	■ **本人を識別するための行為をしない** ■ 自ら匿名加工情報を利活用することは可
提供規制	公表（４３条４項・４４条）
	■ 情報の項目と提供方法を公表 ■ 本人への通知や同意取得は不要
	提供先に明示（４３条４項・４４条）
	■ 提供先である第三者に、提供情報が匿名加工情報であることを明示

加工情報の利活用

（２）行政機関等匿名加工情報
国・自治体の持つビッグデータ等をビジネス活用できる仕組み

匿名加工情報

- 匿名加工情報と行政機関等匿名加工情報（旧、非識別加工情報）で、個人（消費者等）を保護しつつ、ビジネスのためにデータを利活用できるように
- 個人情報よりも制約が少ないので、簡単な手続で利活用や外部提供が可能に

種類	メリット	利活用例
匿名加工情報	• 個人情報ではないので、目的外利用や外部提供が容易	• 自社で持っている顧客購買履歴を分析 • 他社で持っている顧客属性情報と自社データを組み合わせて分析
行政機関等匿名加工情報	• 国や自治体からデータを入手できる • 国や自治体の持つ新鮮で正確なデータを入手できる	• 日本に出入国する外国人の情報を分析 • 古物商、風営法許可等の状況を分析 • 国家資格合格者の情報を分析 • 住民データを分析

非識別加工情報

店舗を新設したい。高収入の大人女性向けの店舗にしたい。
ターゲット層が近くに居住しつつも、類似店舗が少ない地域はどこだろうか。

国・自治体が持っているデータを利活用してはどうだろう。住所、生年月日、性別、世帯年収、子の有無などが国・自治体に情報としてあるはず。

個人情報だから取得できないのでは。

ビッグデータ等の利活用のために、「行政機関等匿名加工情報」ができたはず。
個人情報ではなく（注）データを丸めて加工した情報を国・自治体から民間が取得できる。

行政機関等匿名加工情報

概要

- 官の持つデータを民間が利活用するためのしくみ
- 官が豊富かつ新鮮な大量のデータを保有するのは、公の利益のため。
  官の持つデータ価値を民間に還元する。いわゆる「ビッグデータ等」の利活用のため。
- 提供を受ける民間においては、**誰の情報かわからなくさせる**ことで、個人（消費者等）を保護

利点

- 一般に広く公開情報とはなっていない情報を入手できる
- 行政機関等が業務遂行の目的で保有する個人情報をもとに加工を行うため
  - 情報が悉皆的であり個人の漏れがないこと
  - 個人に対する情報の種類や蓄積量が多いこと
  - 行政情報であるため情報が新鮮かつ正確であること

注意点

- 自分の欲しいデータが行政機関等匿名加工情報の対象かどうか確認要。
- 個人情報保護法に従った手続（提案書の作成、審査、契約）が必要となる。
  手数料も必要で無料ではない。
- 自治体が豊富なデータを保有するが、当分は都道府県・政令市のみ対応予定か？
  自治体にとっては、匿名加工を十分に行わないと、漏えいに当たるので慎重な対応が必要

参考）加工基準

	匿名加工情報（規則３４条）	行政機関等匿名加工情報（規則６２条）
加工基準 ⇒同じ	一　個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。 二　個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。 三　個人情報と当該個人情報に措置を講じて得られる情報とを連結する符号（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該個人情報と当該個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。）。 四　特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。 五　前各号に掲げる措置のほか、個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し、その結果を踏まえて適切な措置を講ずること。	一　保有個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。） 二　保有個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。） 三　保有個人情報と当該保有個人情報に措置を講じて得られる情報とを連結する符号（現に行政機関等において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該保有個人情報と当該保有個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。） 四　特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。） 五　前各号に掲げる措置のほか、保有個人情報に含まれる記述等と当該保有個人情報を含む個人情報ファイルを構成する他の保有個人情報に含まれる記述等との差異その他の当該個人情報ファイルの性質を勘案し、その結果を踏まえて適切な措置を講ずること。

匿名加工情報と行政機関等匿名加工情報

次ページで図表化

- ✓ 「匿名加工情報」も「行政機関等匿名加工情報」も、**生の個人情報を加工した**両方とも、**個人**（消費者・国民等）**を保護しつつ、データ流通を容易化する法制上の仕掛け**である。
- ✓ 「行政機関等匿名加工情報」は中でも、官の持つデータ民間が利活用するためのしくみ
  - 行政機関等匿名加工情報は行政機関／独立行政法人等／自治体／地方独法がもっているデータの状態をいい、
    行政機関等匿名加工情報が民間の手に渡った瞬間、「匿名加工情報」になる
  - 前までは「非識別加工情報」と言われており、官内では識別可能だったが、複雑との批判もあり、「行政機関等匿名加工情報」と名称変更した

行政機関等匿名加工情報
◆　官の持つデータを民間が利活用するためのしくみ
匿名加工情報
①自分の持つ個人情報を匿名加工情報に加工することで、簡単な手続での利活用ができる ②他社の持つ匿名加工情報を入手することで、簡単な手続での入手ができる ③行政機関等匿名加工情報は行政機関／独立行政法人等／自治体／地方独法がもっているデータの状態をいい、行政機関等匿名加工情報が民間の手に渡った瞬間、「匿名加工情報」になる

非識別加工情報と匿名加工情報

官（行政機関・独立行政法人等・地方公共団体等）

民（企業等）

加工

パターン①自社で匿名加工情報を作成

わが社

加工

パターン②他社から匿名加工情報を入手

他社

パターン③官から入手
※行政機関等匿名加工情報は民の手に渡った瞬間、「匿名加工情報」になる

※その他、他社から生の個人情報を入手し、自社で匿名加工情報化すること等もできるが、割愛

非識別加工情報入手の流れ

手続	概要
1）データの調査	入手したいデータがあるかe-Gov等で調べる
2）国への提案	提案書を作成し国に提出する
3）国での審査	提案書が審査される
4）国との契約	適当と認められると契約できる
5）データの入手	契約に基づきデータを入手する
6）データの利活用	法規制等に従ってデータを利活用する

加工情報の利活用

（３）匿名加工医療情報（次世代医療基盤法）

医療データを本人保護及び安全を確保しつつより容易に入手できる仕組み

医療ビッグデータ法の制定

H27改正個人情報保護法下の「要配慮個人情報」による規制強化

医療分野の研究開発力強化・医療分野のIT化促進の必要性

医療分野の研究開発等に困難を生じるのでは

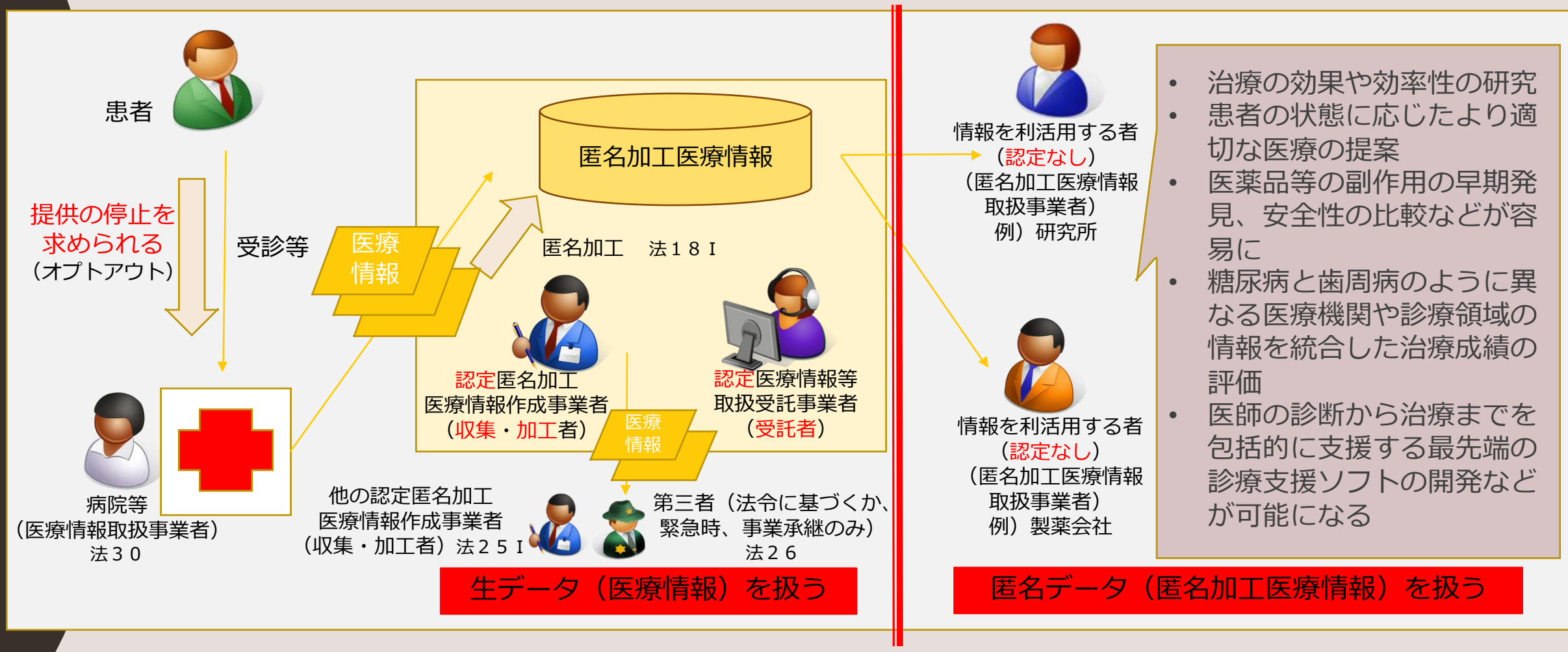
？

医療ビッグデータ法（次世代医療基盤法）の制定

- 改正個人情報保護法により、医療情報の多くが「**要配慮個人情報**」となり、規制が強化
  - ✓ 医療分野の研究開発等に困難を生じるという危惧
  - ✓ もっとも、改正個人情報保護法による変化は、オプトアウトの禁止のみ。学術研究の適用除外もある。
- 一方で、医療分野の研究開発力強化、医療分野のIT化促進の必要性

- そこで、改正個人情報保護法の**匿名加工情報とは異なる規律**として、医療ビッグデータ法（次世代医療基盤法）により、**匿名加工医療情報**をより容易に取得できるように改正。
  - ✓ もっとも、個人の不安払しょくのため、**大臣認定制度**を設け、**認定事業者については規制の大幅強化**し、かつ個人がこれに参加しないことを選択できる仕組み（**オプトアウト**）を設けた

匿名加工医療情報の全体イメージ



- 治療の効果や効率性の研究
- 患者の状態に応じたより適切な医療の提案
- 医薬品等の副作用の早期発見、安全性の比較などが容易に
- 糖尿病と歯周病のように異なる医療機関や診療領域の情報を統合した治療成績の評価
- 医師の診断から治療までを包括的に支援する最先端の診療支援ソフトの開発などが可能になる

現状の課題と新法のポイント

現状の課題	■ 現在、全国規模で利活用が可能な標準化されたデジタルデータはレセプトデータが基本。診療行為の実施結果（アウトカム＝検査結果、服薬情報等）に関する標準化されたデジタルデータの利活用は、世界的にも重要な課題 ■ 医療サービス提供者や保険者等（一次ホルダー）に関しては、レセプトや特定健診等のデータを収集する仕組みが整備されつつあるが、個別目的に基づいてシステムが構築され情報が分散。そのため、人の一生涯を通じた統合的な健康管理や、地域差や医療保険制度の違いを踏まえた医療費等の分析が困難 ■ 研究機関や民間事業者等（二次ホルダー）を含めると、実際の情報流通経路は複雑・多岐。個人は、どこでどのように情報が扱われるのか不安が払拭できず、サービス提供者・事業者（一次・二次ホルダー）は、同意取得や匿名化を含めたデータ処理やシステム構築・運用のコストが負担
新法の背景	■ H27改正個人情報保護法により、ビッグデータ利活用のための「匿名加工情報」という規律が新設 ■ しかし医療情報は通常のデータとは異なる配慮が必要 （個益・公益のための研究等の必要性、データの機微性）
新法のポイント	■ 医療ビッグデータ法（次世代医療基盤法）により「**匿名加工医療情報**」を新設 ■ 研究等に必要なデータを**より容易に**統合的に取得できるように ■ 一方で、データの機微性等から、**厳しい規律**に（大臣認定制度、認定事業者への規制の大幅強化、個人がこの制度に参加しないことを選択できる仕組み（オプトアウト）の導入）

匿名加工医療情報作成事業者の認定条件

認定条件	■ 申請者が、医療分野の研究開発に資するよう、医療情報を取得・整理・加工して、匿名加工医療情報を適確に作成・提供するに足りる能力を有するものとして主務省令で定める基準に適合していること（８条３項２号）
	■ 医療情報等及び匿名加工医療情報の漏えい、滅失又は毀損の防止その他の当該医療情報等及び匿名加工医療情報の安全管理のために必要かつ適切なものとして主務省令で定める措置が講じられていること（８条３項３号）
	■ 申請者が、医療情報等及び匿名加工医療情報の安全管理のための措置を適確に実施するに足りる能力を有すること（８条３項４号）
	■ 医療ビッグデータ法その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者は不可（８条３項１号イ）
	■ 認定を取り消され、その取消しの日から二年を経過しない者は不可（８条３項１号ロ）
	■ 匿名加工医療情報作成事業を行う役員又は主務省令で定める使用人に、成年被後見人若しくは被保佐人又は外国の法令上これらに相当する者、破産手続開始の決定を受けて復権を得ない者又は外国の法令上これに相当する者、この法律その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者、認定を取り消された場合において、その処分のあった日前三十日以内に当該認定に係る事業を行う役員又は主務省令で定める使用人であった者で、その処分のあった日から二年を経過しないものがいる場合は不可（８条３項１号ハ）
	■ 法人に限る（８条１項）

医療情報等取扱受託事業者の認定条件

認定要	■ 大臣認定を取得した受託者以外には、委託不可（２３条１項）
	■ 再委託以降も、大臣認定を取得した受託者以外不可、かつ委託者の許諾要（２３条２項）
認定条件	■ 医療情報等及び匿名加工医療情報の漏えい、滅失又は毀損の防止その他の当該医療情報等及び匿名加工医療情報の安全管理のために必要かつ適切なものとして主務省令で定める措置が講じられていること（２９条、８条３項３号）
	■ 申請者が、医療情報等及び匿名加工医療情報の安全管理のための措置を適確に実施するに足りる能力を有すること（２９条、８条３項４号）
	■ 医療ビッグデータ法その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者は不可（２９条、８条３項１号イ）
	■ 認定を取り消され、その取消しの日から二年を経過しない者は不可（２９条、８条３項１号ロ）
	■ その事業を行う役員又は主務省令で定める使用人に、成年被後見人若しくは被保佐人又は外国の法令上これらに相当する者、破産手続開始の決定を受けて復権を得ない者又は外国の法令上これに相当する者、この法律その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者、認定を取り消された場合において、その処分のあった日前三十日以内に当該認定に係る事業を行う役員又は主務省令で定める使用人であった者で、その処分のあった日から二年を経過しないものがいる場合は不可（２９条、８条３項１号ハ）
	■ 法人に限る（２９条、８条１項）

病院等（医療情報取扱事業者）のやるべきこと

提供義務	**医療情報を提供する義務はない**、また自ら匿名加工して個情法に従った外部提供も可能
提供時の義務	提供するなら以下の義務がある
	①　オプトアウト準備（３０条１項） ■ 本人に通知（提供すること、提供データの項目、提供方法、提供を停止する旨、提供停止の求めの受付方法） ■ 主務大臣への届出 ■ 初回のみではなく、一定事項に変更があれば、本人に通知＆主務大臣に届け出る（３０条２項） ■ 主務大臣は届け出られた内容を公表する（３０条３項）
	②　オプトアウトへの対応（３１条） ■ 求めがあれば、遅滞なく書面を交付（３１条１項） ■ 公布した書面の写しを保存（３１条３項） ■ あらかじめ承諾があれば、書面ではなくデータでも可（３１条２項・３項） ■ 提供を停止する（もっとも、**既に提供した情報の削除は法的には義務ではない**）
	③　記録（３２条） ■ 認定匿名医療情報作成事業者へ提供したときは、年月日等を記録し保存
監督	主務大臣による報告徴収・立入検査の可能性（３５条１項）　※内閣総理大臣、文部科学大臣、厚生労働大臣及び経済産業大臣（３９）
	主務大臣による命令の可能性（３７条５項）

認定事業者等の義務の比較

※利活用者は、個情法の義務に注意 ※８条３項２号「提供能力」で利活用者との契約基準等をチェックされる	認定匿名加工医療情報作成事業者（収集・加工者）	認定医療情報等取扱受託事業者（受託者）	匿名加工医療情報取扱事業者（利活用者）※
大臣認定	○（８条）	○（２９条、８条）	×
帳簿	○（１３条）	○（２９条、１３条）	×
目的外利用の厳格化	○（１７条）	○（２９条、１７条）	×
主務省令基準に従った医療情報の加工	○（１８条１項）	○（２９条、１８条１項）	×
識別禁止	○（１８条２項・３項）	○（２９条、１８条２項）	○（１８条３項）
消去義務（**努力義務ではない**）	○（１９条）	○（２９条、１９条）	×
安全管理措置	**○（２０条）**	**○（２９条、２０条）**	△※
従業者の監督	○（２１条）	**○（２９条、２１条）**	×
従業者等の秘密保持義務	○（２２条）	**○（２９条、２２条）**	×
委託先の監督	○（２４条）	**○（２９条、２４条）**	×
第三者提供制限の厳格化	○（２６条）	**○（２９条、２６条）**	×
苦情処理（**努力義務ではない**）	○（２９条）	**○（２９条、２７条）**	×

個人情報等の種類
～様々な概念が複雑に入り組んでいる

加工度合い

強い

個人情報	･･･生データ	個人情報
仮名加工情報	･･･簡単な加工データ。 何かと照合しなければ誰かわからない情報に加工 ①氏名等②個人識別符号③財産的被害おそれ情報の削除・置換	個人情報 個人に関する情報
個人関連情報	･･･加工データではないが、提供元にとっては個人情報ではなく、 提供先にとっては個人データ	個人情報 個人に関する情報
匿名加工情報	･･･複雑な加工が必要となり得る。 単体で誰かわからない情報に完全に加工する必要あり ①氏名等②個人識別符号③連結符号 ④特異な記述等の削除・置換⑤適切な措置	非個人情報 個人に関する情報
行政機関等匿名加工情報	･･･匿名加工情報とほぼ同じ。 官が持つデータを民がビジネスに活用できる。	非個人情報 個人に関する情報
匿名加工医療情報	･･･匿名加工情報とほぼ同じ。 医療情報を大臣認定事業者が匿名加工して活用できる。	非個人情報 個人に関する情報
統計情報	･･･個人との対応関係が排斥されている。	非個人情報 非個人に関する情報

仮名加工情報でも元情報削除の場合等は非個人情報。匿名加工情報系は加工度合いはほぼ一緒。

個人情報等の種類
～様々な概念が複雑に入り組んでいる

- 個人関連情報は、提供元にとっては「個人に関する情報」で、提供先にとっては「個人情報」
  →うまく図示できないため、図では割愛
- 匿名加工情報＝仮名加工情報となる場合もあるので、匿名と仮名は一部重複する。
- 行政機関等匿名加工情報は、匿名加工情報とほぼ同じだが、官情報
- 匿名加工医療情報も、匿名加工情報とほぼ同じだが、大臣認定事業者とそこから提供を受けた者が保有する情報

その他データ関連政策

官民データ活用推進基本法（H28）

民間も公的機関もデータを活用しよう！
官データと民データを掛け合わせてもいいね
国・自治体で計画を立てて推進します

対象データ	官データ（国データ・独法データ・自治体データ） 例）気象、自動車、免許、許認可、施設情報、税情報
	民間データ 例）企業情報、地図、ドラレコ、混雑率、顧客層
手法	• ネットで行政手続（お役所に行かずにスマホ等から簡単に）10条1項 • 電子契約（契約もIT化）10条2・3項 • オープンデータ／非識別加工情報／匿名加工情報　**→次スライド以降** • AI／IoT／クラウド　16条 • マイナンバーカード／電子証明書　13条 • IT整備・BPR　15条　人材確保・教育　17・18条
効果	• 便利な社会、国民が安全で安心して暮らせる社会及び快適な生活環境の実現 • EBPM、透明で開かれた効率的な行政 • 新事業創出、産業発展、国際競争力の強化、地域活性

オープンデータ

子どもができたよ。そこで近所の保育園・子ども関連施設を調べようと思っても、無料の地図アプリに全部表示されているわけではないし、自治体のWebサイトを見ると、住所が載っているだけで、自分で住所をコピペして地図アプリに入れないと、場所もよくわからない。なんてこの国は不親切なんだ。

私が、子育て支援アプリを作るよ。保育園・幼稚園・学校・公園・民営遊び場などの子ども関連施設情報を地図に落とし込んで、かつ保護者の口コミを載せたアプリにしよう。

僕もエンジニアだから、自分で作ろうとも思ったけどね。自治体のWebサイトに載っている住所を自分でコピペしてアプリに情報登録するのは、面倒だよ。子ども関連施設は増減するから、新規／廃止があるたびに自分で修正処理をしないといけないんだよ。

データ利活用のために、「オープンデータ」政策があるはず。
国・自治体が持つデータ（個人情報ではない）を中心として、機械処理できるような形状で公開して、商用利用も可能とする政策だよ。

オープンデータ

名称	概要
オープンデータ • http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/opendata/opendata01.html • http://www.data.go.jp/	■ 非識別加工情報と同様に、国・自治体等が保有する公共データ等をビジネスで活用できるようにする仕組み。 ■ オープンデータも非識別加工情報も、原則として対象範囲に限定はないものの、オープンデータは、概して法令に基づく制度ではないため、人に対するデータというよりは、気象情報、地盤情報、運行情報、駅・バス停の位置情報、農水産物の栽培情報・検査情報・農薬情報、観光情報、公的施設情報などの、物・状態に対するデータがメインとも考えられる。非識別加工情報は、法令に基づく制度のため、個人情報保護のための手当てが法令上整理されており、物・状態に対するデータも対象ではあるが、それよりもさらに人に関するデータを入手しやすい。 ■ オープンデータの場合は、「人が読む」という利用形態に適したデータではなく、機械判読に適したデータでなければならない。非識別加工情報も、書面ではなく電子データで入手はできるものの、必ずしも機械での自動処理が容易な形式で提供されるものではない。 ■ 各行政機関・自治体等がどのようなデータを持っているかという「データカタログ」から入手したいデータを検索し、Webサイトから直接ダウンロードするなどの方法によってデータを取得できる。

個人情報リスク評価PIA＋＋

個人情報の利活用に際しては個人情報保護が大前提。PIA（DPIA）は、個人情報保護・リスク対策を対外的にアピールする仕組みとして有望。

個人情報リスク評価PIA++とは

■ 個人情報を活用するビジネスや仕組みに有用な取組み
■ その仕組みがもたらすメリット、個人情報が必要な理由、個人情報保護対策を体系的に説明できる
■ 諸外国でも取り入れられている仕組みで国際的アピール力もある

- 個人情報を取り扱う制度・事務・ビジネス・ITシステム等を開始する前に、プライバシーに対して与える影響を検討するための仕組み
- 個人情報を取り扱うとプライバシーに対して悪影響が生じるおそれ。その悪影響を緩和・軽減するための方策を検討する。透明性のある企業経営・行政運営等に資する。
- イギリス、アメリカ、香港、オーストラリア、ニュージーランド、カナダ、韓国その他さまざまな国で実施されているPIA（Privacy Impact Assessment）を参考
- 日本で行われている特定個人情報保護評価を基に、消費者にも企業にも行政にも役立つPIAを目指して水町が再構築したもの（簡易的に個人情報リスク評価PIA++と表記する場合もある）。
- 行政機関、医療機関、民間企業などさまざまなアクターの経営診断等に適用可能

意義（ユーザ・消費者・市民にとって）

◆ **個人から見た意義**

- 今まではブラックボックスだった個人情報の取扱いを透明化
- プライバシー・ポリシーのあるべき姿をイメージ

私の個人情報は
誰にどのように
取り扱われているの？

私の個人情報は
何に使われるの？

私の個人情報は誰に提
供されていくの？

私の個人情報は
どのように管理されて
いるの？

私の個人情報は
ちゃんと守られているの？

意義（実施側にとって）

◆ **評価実施側から見た意義**

- プライバシー保護を体系的に理解・説明できるようになる
  - ✓ 個人情報といっても、漏えいさえしなければいいというものではない
- 個人情報を取り扱う必要性をユーザ・消費者に理解してもらえる
  - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、具体的に説明できる
- 個人情報を取り扱うに当たって注意すべき点がわかる
  - ✓ 従業員の意識の向上
  - ✓ 研修といった座学だと当事者意識が生まれないことも
  - ✓ 「自分が行っている業務」における注意点を具体的に検討する
- 個人情報を適切に取り扱うことをユーザ・消費者にアピールできる
  - ✓ 取扱いの適正性を具体的にアピール
  - ✓ 「炎上」する前に
  - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、詳細な評価書を基に、問題点を具体的にユーザと討論できる

意義（実施側にとって）

コミュニケーション手段としての側面も強い	
対・従業員	個人情報・プライバシーの重要性 業務上の注意点
対・顧客	信頼の獲得
対・ ITシステムベンダー	個人情報・プライバシーの重要性 要求仕様

プライバシー影響評価でわかること

実施側が宣言すること

- **個人情報**を取り扱う**必要**があるので取り扱います
- 個人情報を**このように**取り扱います
- 個人情報を**適切に取り扱うために各種リスク対策を事前に講じます**

評価書からわかること

- どんなふうに個人情報を取り扱うの？
- どんなリスク対策を講じるの？
- プライバシー保護についてどのように取り組んでいるの？

PIA++の実施例

顔認証を利用した顔パス イベント入場に関する

個人情報リスク評価 DPIA・PIA

(Data Protection/Privacy Impact Assessment)

初版　2021年3月

弁護士　水町雅子
作成協力者　日本電気株式会社デジタル・ガバメント推進本部部長　岩田　孝一

このPIAに用いた「顔認証を利用した顔パス イベント入場プロジェクト」は、

個人情報保護に関する民間の自主的取組に資するために、

実案件を模して定義した「ダミープロジェクト」であり、

実在の人物・団体・事件などには一切関係ありません。

Agenda

1 顔パス入場とは
- 1.1 顔パス入場の概要
- 1.2 顔パス入場の仕組み

2 本評価について
- 2.1 本評価の目的
- 2.2 本評価の対象
- 2.3 顔パス入場全体図と本評価の対象詳細

3 顔パス入場の個人情報保護のポイント（対策まとめ）

4 顔パス入場全体スキーム・関係者図

5 リスク対策
- 5.1 なりすまして別人が入場することはないのか
- 5.2 誤認証・誤認識で入場できないことはないのか
- 5.3 入場するために顔画像を登録しなければならないのか
- 5.4 顔画像や特徴量等の個人情報は誰がどこで保管するのか
- 5.5 顔認証・顔画像が不正利用されないのか
- 5.6 漏えい対策は
- 5.7 もし特徴量が漏えいしたらどうなるのか
- 5.8 知らない間に顔画像が撮影されないのか
- 5.9 顔画像や特徴量を他人に提供することはないのか
- 5.10 顔写真・特徴量を確実に削除するのか
- 5.11 監視につながらないのか
- 5.12 その他のリスク対策（個人情報の取得に関して）
- 5.13 その他のリスク対策（個人情報の利用・提供に関して）
- 5.14 その他のリスク対策（個人情報の安全管理措置に関して）
- 5.15 その他のリスク対策（個人情報の管理に関して）
- 5.16 その他のリスク対策（全般に関して）
- 5.17 個人情報保護法への適合性（抜粋）

6 総括
- 6.1 まとめ
- 6.2 水町雅子のコメント

7 参考
- 7.1 パーソナルリファレンスアーキテクチャ
- 7.2 本評価書と特定個人情報保護評価書との対照関係
- 7.3 参考URL

1　顔パス入場とは

1.1　顔パス入場の概要

①申込時

利用者

・Webから申込み
・氏名、生年月日、住所、電話番号、メールアドレス、パスワードを入力する
・**「顔パス入場」を利用したい場合に限り**、顔写真データの登録の同意を行い、顔写真データをアップロードする
・いったん登録した後に、顔写真登録の取消も可能

②入場時

顔パス利用者

※顔パス入場者以外は、通常ゲートから通常通り入場

・顔パス入場者は、顔パス入場ゲートのカメラで撮影した顔写真データをアップロードして識別･認証することの同意を行う。同意された場合のみウォークスルー用のゲートに進む
・ゲートのカメラで顔写真を撮影
・認証できた場合は、入場ゲートが自動的に開く
・認証できなかった場合は、通常ゲートから通常通り入場するか、係員に問い合わせる

1.2　顔パス入場の仕組み

①申込時

①-1　利用者が登録した画像中から顔を検出

①-2　顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した特徴量を抽出

①-3　利用者が登録した顔写真データを削除、特徴量をイベント管理システムに登録

②入場時

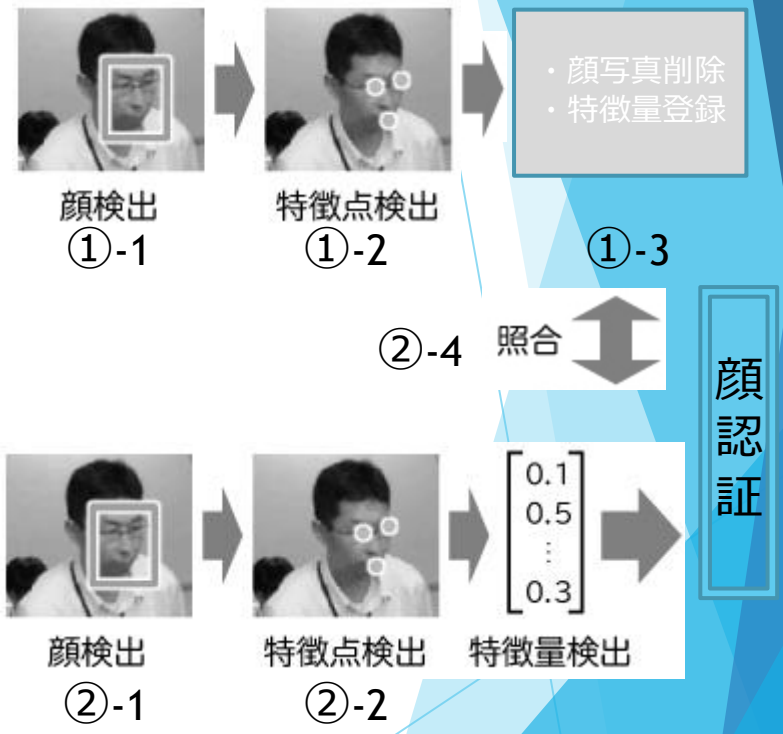
②-1　顔パス入場ゲートのカメラで撮影された画像中から顔を検出

②-2　顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した特徴量を抽出

②-3　撮影された顔写真データを削除

②-4　ゲートのカメラで撮影された画像の特徴量データ（②-2）と、利用者が登録した画像の特徴量データ（①-2）とで顔識別･顔認証を実施し、認証できた場合はゲートを開放

②-5　ゲートのカメラで撮影された画像の特徴量データ（②-2）を削除



2　本評価について

2.1　本評価の目的

顔認証のメリットと懸念

- 顔認証により、来場者は手ぶら（チケットレス）で、そして入場待ち時間が短縮する等、スムーズにイベントに参加することができます。また、不正入場の防止や接触レスなどの利点もあります。
  他方で、重要な個人情報である顔画像が万一悪用されたり流出してしまえば、プライバシーに与える影響は非常に大きく、また様々な場所での監視につながる懸念や、顔認証の精度の問題等もあります。

個人情報やプライバシー権の保護が大前提

- 顔認証の活用といった比較的新しい取組みはイノベーションに欠かせないものではありますが、個人情報やプライバシー権の保護がまずもって大前提であり、プライバシーに与える悪影響を防止・軽減する対策を事前に十分講じた上で、適法・適正に技術が活用されていくことが重要です。

顔認証に対するプライバシー影響評価

- 個人情報・プライバシー権保護のための手法として、海外で普及する「DPIA*」「PIA**」というスキームがあります。ビジネスを開始する前に、そのビジネスが個人情報・プライバシーに対してどのような悪影響を与える可能性があり、その悪影響を防止・軽減するためにどのような対策を講じるかを検討するスキームです。
- 本評価では、「DPIA」「PIA」スキーム（以下、単に「PIA」といいます。）を用いて、顔認証を利用したイベント入場におけるプライバシーへの影響及びそれを防止等する措置を検討します。

*DPIA：GDPR（一般データ保護規則）に規定されたデータ保護影響評価（Data Protection Impact Assessment）
**PIA：英・米・カナダその他の様々な国で実施されているプライバシー影響評価（Privacy Impact Assessment）

2.2　本評価の対象

- 個人情報保護委員会「個人情報保護に関する民間の自主的取組の在り方」に関する調査の一環として、顔認証サービスを展開する日本電気株式会社（以下、「NEC」といいます。）及びJIPDEC（一般財団法人日本情報経済社会推進協会）協力の下、顔認証を利用したイベント入場に関してDPIA・PIAスキームを用いた本評価を実施しました。
- 本評価は、弁護士水町雅子が、NECから資料提供やヒアリングを受けながら実施し、上記個人情報保護委員会「PIA検討会」に提出したものです。なお、NECは、本評価書に記載された内容に偽りがないことを事前に確認しています。
- 本評価は、「NEC顔認証機能を利用した顔パスイベント入場」（以下「顔パス入場」といいます。）をその範囲・対象としています。NECは様々な場面（出入国管理、企業の入退室管理、顔認証決済等）で利用できる顔認証サービスを提供していますが、今回は顔認証を利用したイベント入場を対象に、本評価を実施します。なお、顔認証入場に際する個人情報・プライバシー保護全般を目的としており、実際に稼働しているイベント入場に対する評価ではなく、NEC顔認証技術を元にイベント入場管理を行うことを想定した評価になります。そのため、本評価中に登場するX社・Y社はあくまで仮定の企業になります。

3　顔パス入場の個人情報保護のポイント（対策まとめ）

顔写真データは、大変重要な個人情報です。また、顔認証が悪用等されると、なりすましや監視等につながる懸念もあります。顔認証技術を利用・提供する企業にはこれらのリスクその他のプライバシー権侵害や不正行為を防止するため、様々な対策を応じる必要があります。NECでは本評価記載の通りの措置を講じており、その主なポイントは以下の通りです。

主なポイント

① **顔写真データ自体はすぐに削除**

・顔写真データを利用者が登録後、速やかに顔認証システムでは「特徴量抽出*」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。

・来場時にゲートで撮影した顔写真データも、速やかに特徴量抽出を行い、撮影データを削除します。

*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。

② **希望者だけが、顔パス入場**

・顔パス入場希望者以外は、通常ゲートから通常通り入場できます。

③ **NECが提供する顔認証機能では、氏名・住所等の情報は保持しません**

・ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。

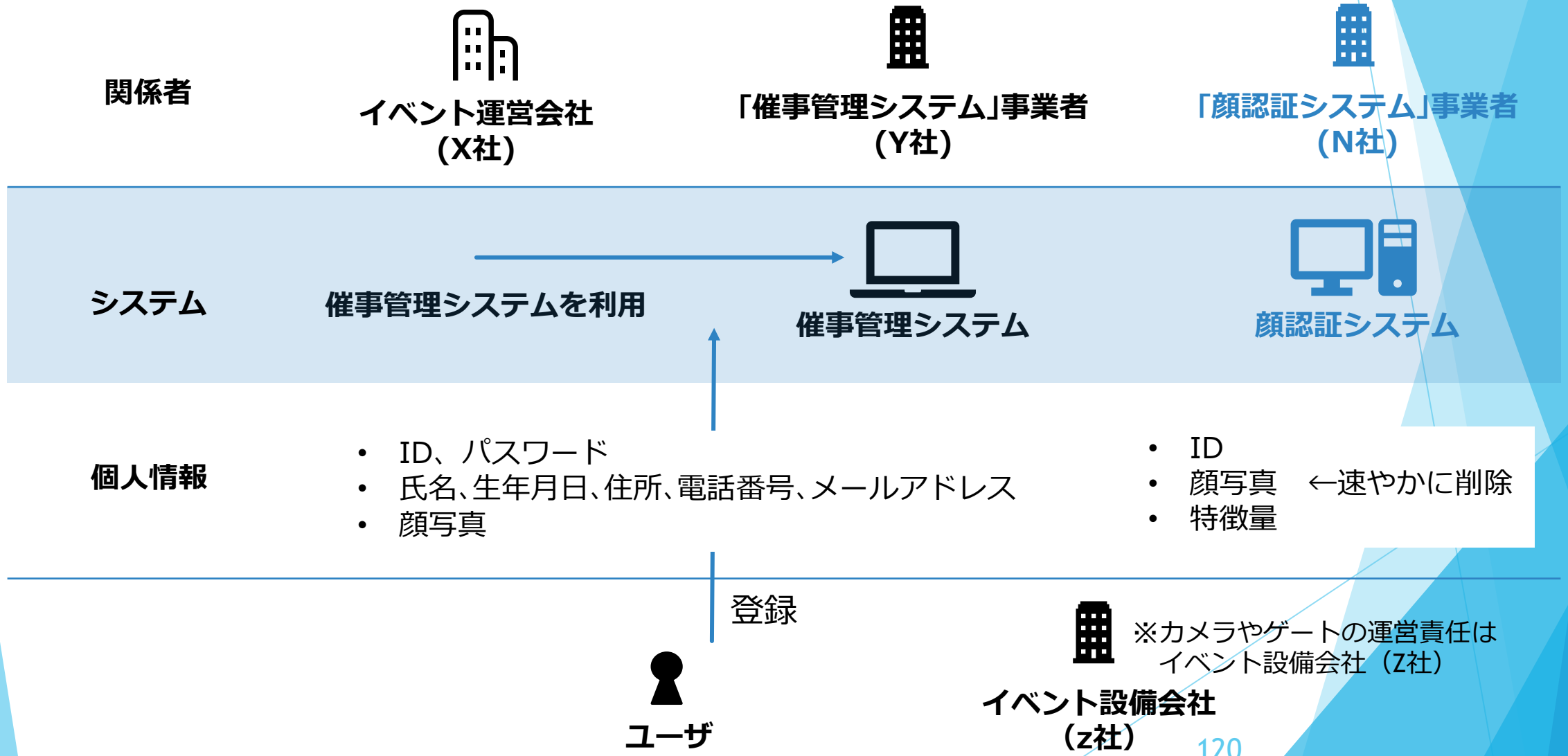
・但し、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ID等の情報を保存しています。

④ **セキュリティ**

・様々なセキュリティ対策を履践しています。NECではPマーク付与認定及びISMS認証を取得しています。

4　顔パス入場全体スキーム・関係者図

※本評価はＮ社のリスク対策を主としており、実際に稼働しているイベント入場に対する評価ではないため、Ｘ・Ｙ社で行うべきリスク対策等が残存リスクとして残ります。



5　リスク対策

個人情報・プライバシーへの影響とその対策

5.1　なりすまして別人が入場することはないのか

激戦を勝ち抜いてチケットを獲得しました。
別人が私になりすまして勝手に入場し、私が入場できなくなることはないのでしょうか。

高精度の認証技術

- 骨格の似た親兄弟でも違いを検知し、双子についても違いを判別します。
- NECの生体認証は、約70の国と地域1000システム以上の導入実績があります。なかでも顔認証は入出国管理や国民IDなど国家レベルでのセキュリティのほか、企業での入退管理や端末ログイン、決済など、様々な用途で使われています。
- NECの顔認証技術は、米国国立標準技術研究所（NIST）主催のベンチマークでNo.1の評価を5回獲得しています。米国国立標準技術研究所(NIST)が実施した最新の顔認証技術のベンチマークテスト(FRVT2018)において、1,200万人分の静止画の認証エラー率0.5%という、第1位の性能評価を獲得しました。なお、NISTのベンチマークテストは数千万人規模の大規模静止画データにおける認証精度と処理速度を評価するもので、使われる評価画像は、登録用画像として1200万人分の静止画像が登録され、照合画像としては未登録人物33万人分、登録人物15万人分が利用されるというものです。
  https://jpn.nec.com/biometrics/face/index.html
- 今後も、精度の維持・向上に努めていくことが求められます。

不正対策も

- 顔認証システムでは、「いつ・だれが入退したか」というデータをログとして正確に残せます。そのため、万一不正が起こっても、究明が可能です。
- 万一不正が起こった場合は、通常ゲートの会場係員が、催事管理システムからお客様のチケット情報を確認したり、どのような人物がお客様のチケットを用いて入場したかどうかを確認します。

5.2　誤認証・誤認識で入場できないことはないのか

激戦を勝ち抜いてチケットを獲得しました。
それなのに、顔認証システムが私を認識してくれなくて、入場できなくなることはないのでしょうか。

マスクやサングラス、横向きでも認証が可能

- NECの顔認証は、マスクやサングラスなどを装着した場合でも、事前に登録した画像データと照合し、本人かどうかを高精度で識別できます。人工知能（AI）の手法の一つである深層学習に、本人と似ている他人との違いを強調する独自の工夫を取り入れ、精度を高めることができました。マスクやサングラスを装着していたり、顔を横に向けていたりしても、正面で撮影した画像をもとに高精度で認証することができます。

入場前であれば顔写真データの差替も可能

- 昔の顔写真で申し込んでしまった場合や、申込後に顔を負傷した場合等であっても、入場前であれば、申込ページにログインいただいたうえで、顔写真データを差し替えることができます。

通常ゲートから入場可能

- 万一、認証エラーになった場合は、通常ゲートから通常の方法で入場できます。
- お客様が当日チケットをお持ちでなかったとしても、Web画面からお客様自身で催事管理システムにログインし、ご自身のチケット情報をご確認いただけますし、会場係員も催事管理システムにログインし、確認することができます。

5.3　入場するために顔画像を登録しなければならないのか

某イベントに参加したいです。
でも、そのために顔画像を登録したり顔認証をするのは嫌です。

希望者だけ、顔画像による顔パス。通常ゲートからチケット提示でも入場できます

- 顔認証による顔パス入場は、あくまで希望者だけが対象。
- 顔パス入場以外に、通常ゲートからチケットを提示し、通常の方法で入場することができます。顔パス入場か通常入場かは自由に選択可能です。通常入場を選択した場合にも来場者に不利益はありません（もっとも、通常入場の際は、入場待ちリスク、係員との接触リスク等はあり）

取消可能

- 一度顔パス入場を申し込んだ方でも、顔パス入場する前までであれば取消が可能。
- 取消を希望された場合は、顔写真､特徴量その他の個人情報を速やかに削除します（但し、問合せ対応のためIDだけは取消済のIDとして記録し保持しておく）。

残存リスク

- 取消時については、NECだけでなく、X社・Y社においても確実に削除されることを確認する必要があります。

5.4　顔画像や特徴量等の個人情報は誰がどこで保管するのか

私の顔画像や特徴量、氏名などの個人情報は誰がどこで保管するのですか？

NECでは顔写真、特徴量、IDのみ保持

- NECでは、顔写真データ、顔写真データから抽出した特徴量、IDのみを保持します。このうち、顔写真データは下記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。
- また、NEC顔認証機能で生成した特徴量は、X社・Y社に提供することはありません。NEC顔認証機能内で削除するまで保存されますが、X社・Y社には、認証OKか認証NGかの情報をNECから返すだけで、特徴量自体は提供しません。
- NECにおけるこれらの情報の管理方法・リスク対策については、5.6「漏えい対策は」を参照ください。

顔写真、氏名、住所等はX社・Y社

- ID・パスワード、氏名、生年月日、住所、電話番号、メールアドレス、顔写真といった、申込時に登録等していただいた情報は、イベント運営会社X社の責任で保管されます。
- 責任主体はイベント運営会社X社ですが、保管場所はイベント運営会社X社が利用する、Y社催事管理システムになります。Y社催事管理システムの提供・運営・保守等、X社から委託の範囲内でこれらの個人情報にアクセスすることができます。またX社もこれらの個人情報にアクセスすることができます。
- X社・Y社では上記の通り、特徴量はいっさい保持せず、NECから顔認証OKかNGかの情報が提供されるだけです。
- 4「顔パス入場全体スキーム・関係者図」もあわせてご覧ください。

残存リスク

- 催事管理システムでの管理方法・リスク対策については、催事管理システム事業者Yに確認する必要があります。
- ゲートカメラのデータ自体については、イベント設備会社Z社に確認する必要があります。

5.5　顔認証・顔画像が不正利用されないのか

顔画像を不正コピー等されて、違う目的に利用されることはないのですか？

顔パス入場にのみ利用します

- 顔認証・顔画像は、顔パス入場にのみ利用します。
- NECは委託を受けて顔認証機能を提供する立場であり、登録された顔画像とゲートで撮影された顔画像が一致するか否かを判断する目的以外に個人情報を利用することは、リーガル的にもできません。NECでは顔画像・特徴量の不正を防止するため、社内で権限を与えられた者以外はアクセスできないよう制御し（アクセス制御、入退館・入退室制限等）、アクセス者には守秘義務を課しています。また、顔画像・特徴量を保持する顔認証システムでは逐一ログを取得し、不正コピー・不正持出し・不正提供等を監視します。
- なお、特徴量はNECでのみ保持し、委託業務終了後に廃棄します。

残存リスク

- イベント運営会社X社がどのように個人情報を利用・管理するかどうかは、X社が通知・公表等する利用目的を確認する必要があります。
- 催事管理システム事業者Y社は、一般にX社から委託を受けて催事管理システムで入場申込・入場管理等の機能を提供する立場であり、委託の範囲を超えて個人情報を利用することはリーガル的にもできません。但し、Y社における個人情報の管理方法は、Y社に確認する必要があります。

5.6　漏えい対策は

顔画像や特徴量が漏えいしたら大変ではないですか？

対策

- NECでは、クラウドサービス等を行う上で重要とされるISO/IEC20000(JIS Q 20000:2007)、ISO9001(JISQ9001)、ISO/IEC27017、ISO/IEC27018、ISMS(ISO/IEC 27001/ JIS Q 27001)、プライバシーマーク(JIS Q 15001)、SOC1/SOC2、事業継続マネジメントシステム(ISO/IEC22301)等の認定・認証を取得しています。
- 開発プロセスの各フェーズで、セキュリティの観点から実施すべき事項をセキュリティタスクとして定義し、それらのタスクを ガイドラインに沿って実行することで配備されるソフトウェアは、適切なソースコード診断、脆弱性診断を経て実装されます。
- 不正プログラムの混入やその攻撃による各種の脅威（情報漏洩や可用性低下など）に対抗するために、ウイルス対策ソフトの導入、安全なプログラム設定、不要プロセスの削除等をセキュリティポリシーに纏め、同ポリシーに準拠した設計・構築及び運用体制を確立しています。
- 物理サーバのハードウェア障害時には別物理サーバ にて仮想サーバの自動再起動を行うなど、ハードウェアの故障等によるサービス停止リスクに対抗するための各種設計に基づいて、構成・運用をしています。
- システムの事故（ハードウェア 障害など）に対しては 、適切なモニタリングを行うことでそれを検出し 、可及的速やかに障害からの復旧を行います。
- 広域災害などサービスを継続できなくなる事態に備えて、遠隔地に退避したアプリケーションとデータを復旧することのできる環境で提供しています。
- インターネットに接している IPアドレスに関しては、脆弱性を定期的にスキャニングしています。

5.6　漏えい対策は

顔画像や特徴量が漏えいしたら大変ではないですか？

対策
■ 故障等によりストレージデバイスを交換する場合には、データ流出を防止するための廃棄プロセスが定義されており、それに従った廃棄（NSA（米国家安全保障局）推奨方式や DoD（米国防総省）準拠方式等の消去方式）を徹底しています。 ■ 盗聴による影響を軽減するために専用線接続サービスやVPN（公衆網内に構成するプライベートネットワーク）を採用し、さらにIDS（不正侵入検知システム）を利用することで不審なアクセスの試みを検知しています。 ■ システムメモリ上、またはハードウェア上に何らかの原因で残存するデータの処理に関して適切な管理を行うために、論理的なデータの取り扱い、物理的なデータが記録されている媒体の取り扱いに関して適切な運用規定を設け、運用管理を徹底し、運用内容は第三者機関によって定期的に監査され、必要に応じて改善を実施しています。 ■ ID アクセス管理機能で、リソースへのアクセスを安全にコントロールすることができ、運用担当者の特権 IDの利用に対して有効な統制を実施し、組織内で要求されるアクセス制御を確実に実施しています。
残存リスク
■ イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社がどのように個人情報を管理するかどうかは、それぞれの事業者に確認する必要があります。

5.7　もし特徴量が漏えいしたらどうなるのか

NECでは、顔写真データはすぐ削除し、特徴量とIDのみ保持するということはわかりました。
IDと特徴量が漏えいした場合、特徴量から私の顔がわかるのですか？
また漏えいした特徴量を悪用して、不正なりすましが起きませんか？

特徴量から顔画像の復元は困難です

- 現在の技術では、特徴量データから、顔画像データを復元することは困難です。特徴量データは、顔画像データ（元の生体情報）から不可逆的な方式で変換しています。また特徴量は顔の一部分の特徴のみ抽出するため、特徴量では把握できていない顔の部分が存在します。
- 特徴量データは、日本の個人情報保護法では「個人識別符号」に該当する情報です。氏名や顔画像データなどと紐づけて管理されていなくても、特徴量データ単体で個人識別符号に該当し、明確に個人情報であると定義されています。個人情報保護法に従って、NECでは厳格な管理を実施しています。
- 生体情報は、パスワードなどと異なり、他人に盗み見られたり、わすれてしまうリスクがありません。他方で、その人しか持たず簡単に変更できないという生体情報のメリットは、漏えいしてしまった場合に深刻な問題となります。「一生変わらない」という生体情報のメリットは、「一生変えられない」というデメリットにもなり得ます。そのため、生体認証技術を使う際の生体情報の管理には、厳重なセキュリティ対策が求められます。

5.8　知らない間に顔画像が撮影されないのか

知らない間に顔画像を撮影したり、顔認証したりしないですか？

知らない間に顔認証することはありません

- **顔パス入場ゲートでのみ**顔認証を行います。顔パス入場ゲートは通常ゲートと異なる**外観**になっており、顔認証を実施することを立看板で**周知**しています。
- なお、顔パス入場ゲートで顔画像を撮影した場合であっても、**事前に顔写真を登録していない場合は**顔認証エラーとなります。そして顔パス入場ゲートで撮影された顔画像・特徴量データは速やかに削除されます。
- 顔パス入場ゲート以外では、顔認証を実施しません。

残存リスク

- ゲートカメラの運営はイベント設備会社Z社に委ねられています。ゲートカメラで常時撮影しているか、人がカメラ前に立った時だけ撮影しているのかは、Z社に確認する必要があります。

5.9　顔画像や特徴量を他人に提供することはないのか

顔画像や特徴量を他人に提供することはないですか？

第三者提供は行いません

- NECでは、個人情報保護法に反して、顔画像や特徴量を第三者提供することはありません。NECでは顔認証システムの保守運用等に関して必要な範囲内で委託を行う可能性がありますが、その場合も、個人情報保護法及び同ガイドラインに則って委託先を監督します。
- イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社においても、法律に反した第三者提供を行えば、個人情報保護法違反になります。
- なお、個人情報保護法で認められている外部提供として、例えばイベント会場内で犯罪が発生した場合で、警察から令状に基づき来場者情報の提供を求められた場合等は、氏名・顔画像等を警察に提供することがあり得ます。

残存リスク

- イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社が、個人情報保護法を遵守した上で共同利用等を行う可能性も考えられなくありませんので、それぞれに確認する必要があります。

5.10　顔写真・特徴量を確実に削除するのか

顔画像や特徴量は確実に削除してもらえるのですか？
私が自分で削除依頼をしないといけないのですか？

顔写真データはすぐに削除します

- （申込時）顔パス入場を希望するユーザは顔写真データを登録します。その後、速やかに顔認証システムでは「特徴量抽出*」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。
- （来場時）ゲートで顔写真を撮影し、特徴量抽出*を行った上で、上記申込時に登録された特徴量と比較して顔認証を行います。顔認証システムでは、ゲートで撮影した顔写真データも速やかに特徴量抽出*を行い、速やかに撮影データを削除します。
  顔認証の実施後は、特徴量も速やかに削除します。
- スキーム詳細は前記スライド1.2をご参照ください。

*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。

- 削除に当たって申込者の方で特に必要な手続・操作等は一切なく、顔認証システム側で**自動的に削除**します。

残存リスク

- 催事管理システム側でも顔写真データを保持するので、同システムでの削除については催事管理システム事業者Yに確認する必要があります。
- ゲートカメラのデータ自体については、イベント設備会社Z社に確認する必要があります。

5.11　監視につながらないのか

カメラで様々な情報を撮影し、様々な場所の撮影データ等とつなげれば、
人の行動履歴等がつぶさにわかるのではないでしょうか。

監視社会につながらないのでしょうか。

最小限のデータしか取得しないように措置を講じています

■ **NECが提供する顔認証機能では、氏名・住所等の情報は保持しません**

・NECでは、ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。

・また、NEC顔認証機能で生成した特徴量は、X社・Y社に提供することはありません。NEC顔認証機能内で削除するまで保存されますが、**X社・Y社には**、認証OKか認証NGかの情報をNECから返すだけで、**特徴量自**体は**提供しません**。

・なお、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ID等の情報を保存しており、Y社は委託の範囲内でこれらの個人情報にアクセスすることができます。またX社もこれらの個人情報にアクセスすることができます。

本件顔パス入場にしか使いません

■ 本件で得た顔写真データ及び特徴量は、本件顔パス入場にしか使いません。

残存リスク

■ X社・Y社で、本件顔パス入場以外に利用したり、申込者が本件顔パス入場のために提供した個人情報以外と結合したりするリスクがありますので、X社・Y社にに確認する必要があります。

■ ゲートカメラ自体のプライバシーリスク対策については、イベント設備会社Z社に確認する必要があります。

5.12　その他のリスク対策（個人情報の取得に関して）

上記のほか、個人情報の取得に際して次の措置を講じています。

個人情報を過剰取得しないか
■ 5.11「監視につながらないのか」参照
不正確な個人情報を取得しないか
■ 本人から直接顔写真データ等の提供を受けた上で、顔パス入場ゲートで実際に来場した人の顔写真を撮影して顔認証を行います。 ■ 本人が顔写真データ等を登録する際は、確認・修正画面から、登録内容を確認し、誤りを修正等することができます。
取得の際に個人情報が漏えい・紛失等しないか
■ 本人が顔写真データ等を登録する際は、Web画面から氏名、生年月日、住所、電話番号、メールアドレス、希望パスワード等の入力・確認を行うと申込者IDが付番され、電子メールで通知されたURLにアクセスすることで登録完了します。登録完了後は、申込者IDとパスワードでWeb画面にアクセスし、登録内容の修正・削除を行うことができます。 ■ Web画面、「催事管理システム」、「顔認証システム」といった各間の通信は、HTTPSで通信し、通信暗号化とサーバー認証を行っています。
取得の際に不正が起きないか
■ 本人の同意に基づき本人から直接顔写真データ等の登録を受ける方法を取っており、本人の知らない間にデータを取得することはありません。また、登録された顔写真データだけでは顔認証が行えず、顔パス入場ゲートで実際に来場した人の顔写真を撮影して顔認証を行います。 ■ また5.11「監視につながらないのか」の通り、顔パス入場の目的達成に必要な最小限の範囲内でのみ個人情報を取得します。

5.13　その他のリスク対策（個人情報の利用・提供に関して）

上記のほか、個人情報の利用・提供に際して次の措置を講じています。

個人情報を無関係の者に利用されないか
■ NECが提供する顔認証機能にアクセスできるのは、NECで正当な手続を経て権限を付与された社員・委託先のみです。NEC社員や委託先であっても誰でも閲覧できるわけではなく、業務上必要な範囲内で、正当な社内手続に沿ってアクセス権限を認められた範囲にのみアクセスできます。 ■ 5.11「監視につながらないのか」の通り、X社・Y社には、認証OKか認証NGかの情報をNECから返すだけで、特徴量自体は提供しません。
本件関係者が個人情報を私的利用・私的複製・悪用等しないか
■ →5.5「顔認証・顔画像が不正利用されないのか」、5.6「漏えい対策は」参照。
個人情報が不正提供されないか
■ →5.9「顔画像や特徴量を他人に提供することはないのか」参照。
目的外利用・過剰紐づけされないか
■ →5.5「顔認証・顔画像が不正利用されないのか」、5.11「監視につながらないのか」参照。

5.14　その他のリスク対策（個人情報の安全管理措置に関して）

上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程

- NECはJIS Q15001等に沿って個人情報保護マネジメントシステムを確立するために、「個人情報保護マネジメントシステムガイドライン」群を定めて、遵守しています。
- 事務取扱責任者を定め、各事務取扱責任者の責任範囲を規定します。事務取扱責任者は、事務取扱担当者を明確にし、各事務取扱担当者の役割と個人情報の取扱範囲を規定します。
- 事務取扱責任者は、個人情報の取扱状況を確認するために、個人情報ファイルの利用・出力状況の記録、書類・媒体等の持ち運びの記録、個人情報ファイルの削除・廃棄記録、削除・廃棄を委託した場合の確証、情報システムの利用状況の記録（ログイン実績、アクセスログ等）を記録します。
- 事務取扱責任者は、個人情報ファイルの取扱状況を確認する手段として、各個人情報ファイルの名称、種類、利用目的、取扱部署、責任者、アクセス権を有する者、削除・廃棄の方法を記録します。
- 事務取扱責任者は、管理区域において個人情報の情報漏えいを防止するために、情報システム機器等を設置するマシン室を「管理区域」として特定、入退場の履歴を記録（システムログ）、持ち込む機器を限定し、許可した機器以外の持ち込みを禁止、生体認証とその他個人認証（専用入室ICカード、社員証等）により、許可された者だけが入室できるように制限することを行います。
- 事務取扱責任者は、管理区域及び取扱区域において、個人情報が記録された情報機器及び電子媒体等は、紛失又は窃盗による情報漏えい等を防止するため、情報機器、電子媒体および書類等は、キャビネットや書庫等に施錠し保管、デスクトップ端末等においてキャビネットや書庫等に施錠保管が困難な機器は、セキュリティーワイヤー等で移動や持ち出しができないよう固定することを行います。

5.14　その他のリスク対策（個人情報の安全管理措置に関して）

上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程

- 事務取扱責任者は、管理区域又は取扱区域から、もしくは管理区域又は取扱区域へ、個人情報が記録された情報機器、電子媒体および書類等を持ち運ぶ際には、情報機器、電子媒体や書類等を持ち運ぶ際の記録、情報機器、電子媒体や書類等を持ち運ぶ際に、紛失や盗難等が生じないよう運搬担当者が安全な処置を講ずることを確認、機器、電子媒体や書類等を持ち運ぶ際に、紛失や盗難等に備え、追跡ができるよう持ち運びの履歴を記録（運搬担当者、運搬物等）、個人情報が記録された機器・電子媒体等は、データの暗号化又はパスワードにより保護等を行ったことを確認、書類等を持ち運ぶ際には処置（封筒への封緘、目隠しシールの貼付等) を行います。
- 事務取扱責任者は、個人情報の情報漏えいを防止するために、事務取扱担当者の役割や責任に応じて、データベース、フォルダ、ファイル等のアクセス可能領域を限定的に設定していることを確認、情報システムにアクセス可能な機器は、ＩＰアドレス等による端末接続制限により使用可能な機器を限定していることを確認、情報システムにアクセス可能な事務取扱担当者を、認証ＩＤ等により限定していることを確認、ＩＤ・パスワード及び専用ＩＣカード等の共同利用を禁止し、事務取扱担当者の個々に付与していることを確認、なりすましを防ぐため、多要素認証を適用していることを確認することなど、情報システム及び特定個人情報ファイルへのアクセス制御、アクセス者の識別・認証等に関するの対策を講じます。

5.15　その他のリスク対策（個人情報の管理に関して）

上記のほか、個人情報の管理に際して次の措置を講じています。

委託先の不正が起こらないか
■ 利用目的の達成に必要な限度において、個人情報を扱う事務を第三者に委託する場合、当該委託において取り扱う個人情報の安全管理措置が講じられるよう、委託先の適切な選定、委託先の安全管理措置を遵守させるために必要な契約の締結、委託先における特定個人情報の取扱状況の把握など適切な監督を行います。
個人情報が誤って消去等されないか
■ 保存期間内は定期的にデータバックアップを実施し、複数個所に保管します。利用目的の達成等により個人情報の保存の必要がなくなった場合で、法令により必要な一定期間の保存期間を経過した場合には、速やかに当該個人情報を削除または廃棄します。
不要な個人情報がいつまでも保管されないか、古い個人情報を誤って利用しないか
■ 5.10「顔画像・特徴量を確実に削除するのか」参照。

5.16　その他のリスク対策（全般に関して）

上記のほか、次の措置を講じています。

点検・監査等
■ NECではPマーク及びISMS認証を取得しています。 ■ システム監査を年１回実施します。 ■ NECでは、個人情報保護管理者のほか、個人情報保護監査責任者を指定し、監査計画及び監査の実施を行います。
従業者教育
■ NECでは、少なくとも年1回定期的に、かつ必要に応じて適宜、従業者への教育・啓発を行っています。
開示・訂正・利用停止請求
■ 個人情報保護法に則って、X社にご請求いただくことになります。
問合せ対応
■ NECでは、ユーザの方等からのお問合せに真摯に対応いたします。下記、お問い合わせ窓口までお問い合わせください。 https://jpn.nec.com/site/privacy/index.html
残存リスク
■ スライド5.12～5.16は全てNECにおけるリスク対策を記載しています。X社・Y社におけるリスク対策についてはX社・Y社に確認する必要があります。

139

5.17　個人情報保護法への適合性（抜粋）

取得フェーズ

- 適正取得（個人情報保護法17条）
  - 申込者・利用者が本件顔パス入場を理解した上で申し込んだり利用できるように、下記の通り利用目的の通知等を行っています。利用者に理解していただいた上でセキュリティを確保した方法で個人情報を取得しており、適正取得しています。
  - 仮に要配慮個人情報が映り込んだ場合でも、個人情報保護法17条2項に従った取得です。

利用フェーズ

- 利用目的の特定・公表等（個人情報保護法15条・18条）
  - 本件顔パス入場は、NEC・X社・Y社ともに、事前に特定・公表している利用目的の範囲内です。
  - NEC・X社・Y社ともに、プライバシーポリシー等で利用目的を公表していますが、さらに加えて、顔パス入場申込サイトや顔パス入場ゲートでも、利用目的の通知を行います。
- 目的内利用（個人情報保護法16条）
  - 本件は、事前に特定・公表している利用目的の範囲内の利用です。
  - 加えてNEC・Y社においては、委託の範囲内の利用です。

提供フェーズ

- 第三者提供（個人情報保護法23条）
  - 個人情報保護法23条に反した個人データの第三者提供は行いません。

140

6　総括

6.1　まとめ

- 本評価において、以下の項目について検討し、プライバシー等への影響を確認しました。

  - スキーム（1.1,1.2,2.1,2.2,4,5.4参照）
  - 個人情報の取扱い（7.1参照）
  - 個人情報利活用の効果（2.1参照）
  - 個人情報保護のポイント（3参照）
  - なりすまし対策（5.1参照）
  - 誤認証・誤認識対策（5.2参照）
  - 顔画像提供の任意性（5.3参照）
  - 個人情報不正利用リスク対策（5.5参照）
  - 個人情報の漏えいリスク対策（5.6,5.7参照）
  - 個人情報不適正取得リスク対策（5.8参照）
  - 個人情報不正提供リスク対策（5.9参照）
  - 個人情報未消去リスク対策（5.10参照）
  - プライバシー権侵害・監視リスク対策（5.11参照）
  - 個人情報の取得リスク対策全般（5.12参照）
  - 個人情報の利用リスク対策全般（5.13参照）
  - 個人情報の提供リスク対策全般（5.13参照）
  - 個人情報の管理リスク対策全般（5.14,5.15参照）
  - 個人情報のその他のリスク対策（5.16参照）
  - 個人情報保護法への適合性（5.17参照）

- 評価実施手続

  - 本評価は世界各国のPrivacy Impact Assessment (PIA)や日本の法制等を参考にして、弁護士水町雅子が評価項目を決定しています。
  - NECから資料提供やヒアリングを受けながら弁護士水町雅子が実施しました。

6.2　水町雅子のコメント

最後に、弁護士水町雅子の意見を次のとおり、述べます。

- 顔認証技術は、より豊かで便利な社会を実現する期待・可能性を有する一方で、プライバシー権侵害の危険性も同時にはらみます。具体的に誰がどのような管理方法で、またどのようなセキュリティ対策を講じて顔写真データや特徴量を保持するのか、顔写真データや特徴量データを具体的にどのように利用し、どのような利用目的で利用するのか、外部提供は発生するのか等々、個人情報・プライバシー等への影響とその対策についての明瞭・透明かつ具体的な説明がなされることが大変重要であると考えます。プライバシー等の人々の権利利益に対する影響を様々な角度から事前に検討し、十分な対策を予め講じておくことは、個人情報やプライバシー権の保護をまずもっての大前提とした上で、適法・適正に新しい技術を活用していくために大きな意義があると考えます。
- 本件顔パス入場は、本人の明示的な同意に基づき、希望者のみが利用し、また目的が限定されていて、顔写真データや特徴量も顔パス入場のためだけに利用するスキームであり、他の顔認証技術の活用手法と比べても、比較的社会的受容性も高いと考えられます。
- 顔認証技術を世界的にも展開しているNECが、「個人情報・プライバシー等保護」と「顔認証技術の活用」を両立させ、このようなPIAを実施することは大変意義深いことであり、顔認証以外の様々な分野における新技術の活用・導入にとっても、PIAの手法は有用であると考えます。今回、本評価に登場するX社・Y社は仮の企業でしたが、実際に顔認証技術を利用する企業においても広く、このPIAを参考にして、個人情報・プライバシー等保護を徹底するための施策・運用等を行っていっていただければ、非常に良いと思います。
- 顔認証技術は海外動向・海外規制、正答率、人権への影響等、様々な観点から、現在も変動している環境下にあります。今後も、様々な観点からのチェックを行い、社会に受け入れてもらえる適正な方法での活用を行っていっていただければと思います。

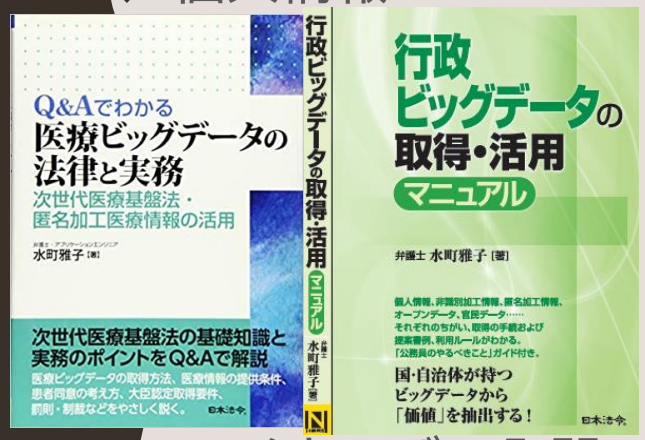
まとめ・参考

まとめ

- 個人情報等の種類
  - 個人情報、個人データ、保有個人データ、要配慮個人情報、プライバシー権、営業秘密、個人関連情報、個人識別符号などの様々な概念
    →技術的な定義よりも、**様々な観点から様々なデータが保護されている**ことをまず理解する
  - 加工度合いによって、仮名加工情報、匿名加工情報、行政機関等匿名加工情報、匿名加工医療情報、統計情報などの様々な概念も
    →**どの程度の粒度・加工度合いのデータで良いのか**を考える
    （＝粒度が粗くて加工度合いが高いデータで良いのであれば、規制も弱い）
- データ活用のルール
  - 取得、利用、提供、管理、本人からのアクセスというフェーズごとに考える
  - 利用目的と第三者提供がポイント
  - 同意がなければ、絶対に使えないというような法律ではない
  - 全体的なルールを把握してから、細かい点を書籍やガイドライン、Q&Aで確認しよう
  - 昔は比較的緩い規制法だったが、
    H27改正以降細かく技術的で対応に負荷がかかる規制が多くなっている

参考（書籍）

◆ 個人情報



「行政ビッグデータの取得・活用マニュアル」

（日本法令、２０１８年）←R3法改正未反映。「非識別加工情報」に関する書籍。

「Ｑ＆Ａでわかる医療ビッグデータの法律と実務」

(日本法令、２０１９年）←「匿名加工医療情報」「次世代医療基盤法」に関する書籍。

◆ マイナンバー入門

要点

「Q&A番号法」（有斐閣、２０１４年）

「マイナンバーから病歴・犯罪歴がわかってしまうの？」「国が情報を一元管理していいの？」という疑問から、番号法の解釈要点まで、番号制度のポイントを１問１答形式で解説。上中級者向けにも。

簡単

「担当者の不安解消! マイナンバーの実務入門」（労務行政、２０１６年）

非法律家の実務担当者向けにかなり平易にマイナンバーを解説。

詳細

「逐条解説マイナンバー法」（商事法務、２０１７年）

制度・法律を網羅的に解説。５００ページ超えの重厚解説書。

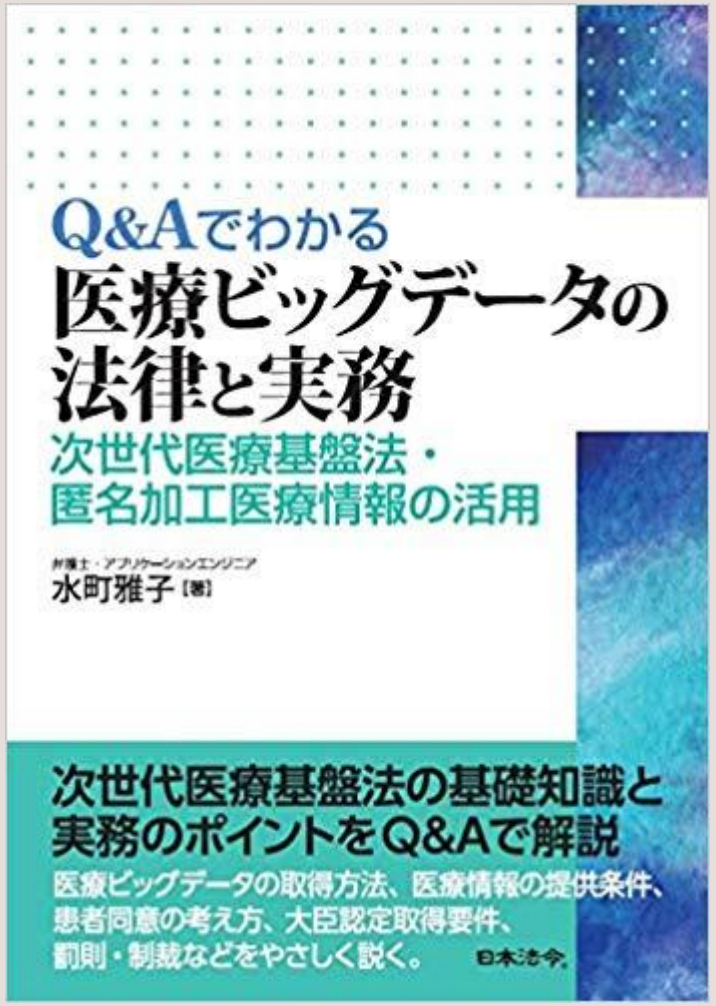
参考（WEB）

◆ ＩＴをめぐる法律問題について考えるブログ

https://cyberlawissues.hatenablog.com/

◆ 各種参考資料を事務所Webにて公表中

- 個人情報保護に関する社内整備と 関連規程の見直し
  http://www.miyauchi-law.com/f/170313piikaiseigaiyou.pdf
- 安全管理措置の比較
  http://www.miyauchi-law.com/f/170906anzenkanrisochi_comparison.pdf
- 個人データの取得/提供時の記録様式
  http://www.miyauchi-law.com/f/teikyoutoukiroku.pdf
- 医療ビッグデータ法の詳細概要
  http://d.hatena.ne.jp/cyberlawissues/20170816/1502870156
- 個人情報リスク評価PIA++
  http://d.hatena.ne.jp/cyberlawissues/20180628/1530155730



THANK YOU

個人情報、マイナンバー、PIA++、IT/ICT、規程策定、医療ビッグデータ法（次世代医療基盤法）のご相談、大臣認定申請支援、国との交渉、企業法務全般、条例策定支援その他に関するお問い合わせ、ご相談がありましたら、お気軽にどうぞ

http://www.miyauchi-law.com

宮内・水町IT法律事務所
弁護士　水町　雅子
電話　→　03-5761-4600
メール→　osg@miyauchi-law.com