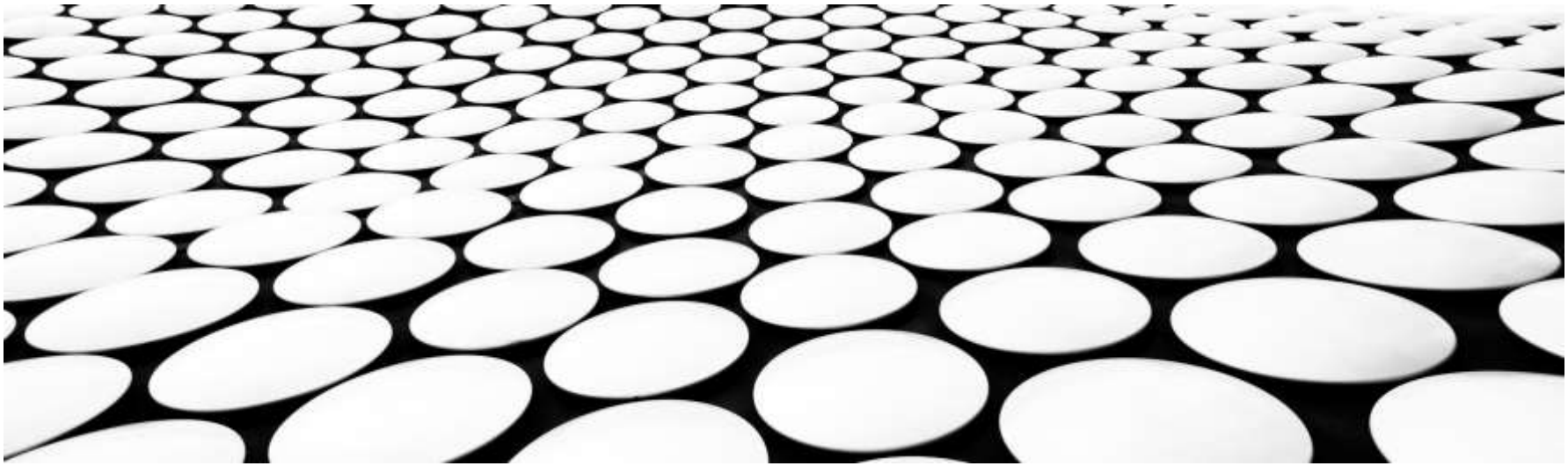
個人情報とパーソナルデータ

一般財団法人日本情報経済社会推進協会（JIPDEC）　主任研究員　郡司哲也



自己紹介

郡司　哲也（ぐんじ　てつや）

一般財団法人日本情報経済社会推進協会　勤務
（JIPDEC）

- 専門分野その1：GIS
  - 某大手航測会社でGISの構築・導入・運用支援
  - JISやISOの規格づくり
  - 自治体/中央省庁の調査事業や実証実験
- 専門分野その2：情報セキュリティ、プライバシー
  - 情報セキュリティマネジメントシステム（ISMS）の認定審査員
  - 個人情報保護やプライバシーの普及啓発
- オープンデータ活動との関わり
  - アーバンデータチャレンジ
    - 元）実行委員（審査委員もやっておりました）
    - 元）地域拠点 メンター
  - 経済産業省の事業
    - オープンデータ推進事業で各所の実証実験に参加
    - 主に、地理空間情報をキーワードにした活動（マッピングパーティや準天頂衛星システムの活用）
    - アイディアソンなどワークショップのコーディネート

本日お話するテーマ

- 個人情報保護法と個人情報、パーソナルデータ
- コンプライアンス（法遵守）と　信頼/信用
- パーソナルデータを取り扱う上で気をつけるべきこと

ITの発展（技術的 / 社会的背景）

- 情報（アナログ）から
  データ（ディジタル）へ
  - コピーすることができる
  - 簡単に渡すことができる
- ネットワークへの接続
  - インターネットの発展
  - パーソナルから共有へ
- デバイスの高度化
  - PCからスマートフォンへ
  - IoT：Internet of Things
- サービスの高度化・多様化
  - EC：Electronic Commerce、電子決済、インターネット銀行
  - SNS：Social Networking Service
  - シェアリング・エコノミー、オンライン完結社会の実現

情報が電子化され、コンピュータがネットワークにつながることでデータのコピーや流通が容易になり、デバイスの高度化によりそれが加速し、流通するデータの種類が増えることで、様々なサービスが生まれた。

アナログ時代には暗黙の了解によって当事者同士でしか扱われることがなかった個人情報が容易にコピー・流通することができるようになったことで、それらを保護する必要性が生じてきた。

個人情報の定義いろいろ

【個人情報保護法】

- 個人情報
  - 第２条　この法律において**「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。

    一.　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。次項第２号において同じ。）で作られる記録をいう。第18条第２項において同じ。）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。以下同じ。）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。**）

    二.　**個人識別符号**が含まれるもの

    ２　この法律において**「個人識別符号」とは、**次の各号のいずれかに該当する**文字、番号、記号その他の符号のうち、政令で定めるもの**をいう。

    一.　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、**当該特定の個人を識別することができるもの**

    二.　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、**特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの**

個人情報の定義いろいろ

【General Data Protection Regulation : GDPR】（一般データ保護規則）

※2018年5月にEUで施行された、今最も新しくて影響力が強いと言われている国際的な個人データ保護の規則

- personal data（個人データ）
  - ‘personal data' means any information relating to an identified or identifiable natural person ('data subject');
    an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
  - 「個人データ」とは、識別された又は識別され得る自然人（「データ主体」）に関するあらゆる情報を意味する。
    識別され得る自然人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、又は当該自然人に関する物理的、生理的、遺伝子的、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一つ若しくは複数の要素を参照することによって、直接的又は間接的に、識別され得る者をいう。

「プライバシー」とは何か？

- 「プライバシーを侵害された！」と感じるときは、どんなとき？
  - 例：
    - 全く知らない会社からDMが来た / わけのわからない会社から勧誘の電話が来た
    - 友人が、一緒に遊びに行ったときに撮った写真を、位置情報つきでSNSに投稿していた
    - etc…

- 個人情報の取扱いで不便に感じることは、どんなとき？
  - 例：
    - 子供のクラスの緊急連絡網が配られなくなった
    - セミナーやイベントで作成した連絡先リストを、終了後にどう扱うべきか悩ましい
    - etc…

皆さんの感覚や実体験は？

では、何をすれば良いのか？

- 「プライバシー侵害はしない」ことを約束する
- 個人情報を正しく取り扱うことを実践する

でも、どうやって？（HOW？）

- おそらく、これらをクリアにすることが、
  「個人情報を正しく取扱い、プライバシーを尊重すること」
  につながるのでは？

  - 個人情報保護法には、「あたりまえ」のことは書かれていても、現実社会と矛盾するようなことや理不尽なことが書かれているわけではない。
  - 法解釈が必要になったとき、素人には敷居が高すぎるので、専門家（弁護士など）に任せるのが吉。
  - それ以前に、「自分がプライバシー侵害だと感じたこと」を他人にしないように気をつけていれば、ほとんどの場合は問題など起きない。

個人情報保護に対するアプローチ

- 日本の個人情報保護法では：
  - （詳細は割愛）コレとコレは個人情報、と定義されている
  - 迷ったときは、「その情報を何かと組み合わせた結果、本人が特定できるか？」で判断

- 一般的に、海外の個人情報保護規則では：
  - 日本の個人情報保護法のように明確にコレとコレ、という定義ではなく、「個人に関するものすべて」という定義が一般的

- 一般市民の感覚はどちらに近いかを考える。
  - たぶん、後者（私の個人情報は、「私に関係するすべて」）。

訴訟や炎上のリスクを考えるなら、「個人情報なのかそうじゃないのか、よくわからない」ものについては、個人情報として取り扱うようにしておいたほうが無難。

個人情報とは結局何なのか

【定義】

- 個人情報保護法における「個人情報」の範囲は、（国際的なルールと比較すると）意外と狭い（限定的）。
- 一方で、世間一般的に「個人情報」として想起される内容は、OECDガイドラインやGDPRの定義に近い。

【なぜ定義が必要か？】

- 法律や規格で「定義」が必要なのは、法や規格を「適用」するため。

【実態】

- プライバシーは人それぞれの感覚によって温度差があるが、個人情報は定義をすることで一律の「対象」になりえる。
- ただし、個人情報の持ち主は個人であり、個人にとっての「個人情報」の定義（個人の情報として大事に扱ってもらいたい度合いや範囲）は異なる。
- プライバシーと個人情報保護は同列に語られることも多く、当然関連も深いが、本質的に概念が異なる。

自問自答：なぜ、個人情報を「保護」するのか

- 視点 1：法遵守（責務：最低ライン）
  - 個人情報保護法＝組織が国内で活動を行う場合に、個人情報を取扱う際のルール（何をして良く、何をしてはいけないかの定義）を定めたもの。
  - 個人情報保護法の遵守は、自動車が道路の右側を走行しないこと（道路交通法の遵守）と同様に、個人情報を取り扱う組織にとって明白な責務である。

- 視点 2：社会的信用（社会的認知）
  - 法を遵守してさえいれば、何をしても許されるか？　・・・否。
  - 組織が活動するためには、周りから認められる必要があり、それは法遵守の事実だけでは担保されない。

- 視点 3：プライバシーの尊重（目的：求められていること）
  - 個人の私生活に関する事柄やそれが他から隠されており干渉されない状態を要求する権利、を尊重すること。
  - 顧客や相手が「これをされたら嫌だ」と感じるようなことをしないこと。

個人情報保護は目的ではなく手段である

第１章　総則

（目的）

第１条　この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

わかりにくいので、分解。

- ■ 個人情報の適正な取扱いに関し、
  - ➢ 基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、
  - ➢ 国及び地方公共団体の責務等を明らかにするとともに、
  - ➢ 個人情報を取り扱う事業者の遵守すべき　義務等を定めることにより、
- ■ 個人情報の適正かつ効果的な活用が
  - ➢ 新たな産業の創出　並びに
  - ➢ 活力ある経済社会　及び
  - ➢ 豊かな国民生活の実現に資するものであることその他の　個人情報の有用性に配慮　しつつ、
- ■ 個人の権利利益を保護すること　を目的とする。

忘れがちな視点

- 個人の権利利益を保護するための「手段の一つ」が個人情報の保護であり、全てではないことに注意。（1:1 のイコールにはならない）
- 個人情報を保護し、適切に取り扱うことは、プライバシーを尊重すること（個人の権利利益を保護すること）につながる。
  （個人情報の保護は、個人の権利利益を保護する手段として有効である）

個人情報保護
＝　個人の権利利益の保護

個人情報保護
∈　個人の権利利益の保護

その個人データは、誰のものですか？

- 個人データは「モノ」か？
  - 個人データは「情報」であるので、個人データそのものは一般的にイメージする物理的な「モノ」ではないが、物理的な記憶媒体（DBやファイル、書類など）に格納（記録）することができる。
    - 間接的にではあるが「物理的なモノ」として取り扱うこともできる。
  - 似ているものとして・・・
    - 音楽（楽曲）　　：楽譜やCDという記憶媒体によって流通している。
    - お金：金属のコインや特殊な紙幣に価値を記録してやりとりされる。
    - 流通させる、人と人の間でやりとりされる、という点において、個人データや音楽やお金は意味的に同じ、かもしれない。
    - あげたり、貸したり、借りたりできる。
- 人から借りたものは、普通どうするか？（どうしているか？）
  - 借りたら返す（お金を返さなかったらどうなる？）
  - 知らずに他人に又貸し？
  - なくしてしまったら？

おまけ：OECDプライバシー8原則

1. 収集制限の原則（Collection Limitation Principle）
   - 個人データを収集する際には、法律にのっとり、また公正な手段によって、個人データの主体（本人）に通知または同意を得て収集するべきである。
2. データ内容の原則（Data Quality Principle）
   - 個人データの内容は、利用の目的に沿ったものであり、かつ正確、完全、最新であるべきである。
3. 目的明確化の原則（Purpose Specification Principle）
   - 個人データを収集する目的を明確にし、データを利用する際は収集したときの目的に合致しているべきである。
4. 利用制限の原則（Use Limitation Principle）
   - 個人データの主体（本人）の同意がある場合、もしくは法律の規定がある場合を除いては、収集したデータをその目的以外のために利用してはならない。
5. 安全保護措置の原則（Security Safeguards Principle）
   - 合理的な安全保護の措置によって、紛失や破壊、使用、改ざん、漏えいなどから保護すべきである。
6. 公開の原則（Openness Principle）
   - 個人データの収集を実施する方針などを公開し、データの存在やその利用目的、管理者などを明確に示すべきである。
7. 個人参加の原則（Individual Participation Principle）
   - 個人データの主体が、自分に関するデータの所在やその内容を確認できるとともに、異議を申し立てることを保証すべきである。
8. 責任の原則（Accountability Principle）
   - 個人データの管理者は、これらの諸原則を実施する上での責任を有するべきである。

1. 収集制限の原則（COLLECTION LIMITATION PRINCIPLE）

- 個人データを収集する際には、法律にのっとり、また公正な手段によって、個人データの主体（本人）に通知または同意を得て収集するべきである。

【解説】

- ✓ 個人データを不用意に集めすぎない、ということを徹底しなさい、本人の許しを得て取得しなさい、ということ。
- ✓ ８原則では、「通知または同意」というガイドラインにしているが、現在は「同意」をきちんと得るべき、という流れになっている。
- ✓ いずれにしろ、必要ではないかもしれない（ひょっとしたら使うかも知れないから集めておく）という行為はNG。

2. データ内容の原則（DATA QUALITY PRINCIPLE）

- 個人データの内容は、利用の目的に沿ったものであり、かつ正確、完全、最新であるべきである。

【解説】

- ✓ たとえば、何かの名簿を作成したとして、連絡先は常に最新で正確なものでなければならない、ということ。
- ✓ 携帯番号やメールアドレスが変わった、住所が変わった、結婚して姓が変わった、などは日常的に起こりうるので、見落とされがちだが個人データを取り扱ううえでは重要なポイント。
- ✓ この原則に従うのは意外とコストがかかるものでもあるので、不要になった個人データは消去してしまう、という解決法が最もシンプルかつ確実かもしれない。

3. 目的明確化の原則（PURPOSE SPECIFICATION PRINCIPLE）

- 個人データを収集する目的を明確にし、データを利用する際は収集したときの目的に合致しているべきである。

【解説】

- ✓ 個人データを収集する際には、あらかじめ「何のために個人データを収集するのか？」ということを明確にすべし、ということ。
- ✓ また、一旦収集した個人データを利用する際には、4つ目の「利用制限の原則」でも掲げられているとおり、目的の範囲内で利用しなければならない。
- ✓ きちんと目的を明確化することができていれば、1つ目の「収集制限の原則」でも解説した「不必要に個人データを集めすぎない」ということにもつながる。

4. 利用制限の原則（USE LIMITATION PRINCIPLE）

- 個人データの主体（本人）の同意がある場合、もしくは法律の規定がある場合を除いては、収集したデータをその目的以外のために利用してはならない。

【解説】

- ✓「目的明確化の原則」に似ているが、これは一旦収集した個人データを利用する際に気をつけるべき内容。
- ✓ 目的外利用については、当然厳しく規制されるべき。
- ✓ これも、「個人データは本人から預かっているに過ぎない」という考え方に基づくもの。
- ✓ たとえば、友人にDVDを貸してあげたとして、それは友人が観るために貸したのであって、友人が勝手にほかの人に「又貸し」してしまうような行為は、利用制限の原則に照らせばNG。
- ✓「目的明確化の原則」と「利用制限の原則」で似たような内容になっているのは、それだけ重要なポイントだということ。

5. 安全保護措置の原則（SECURITY SAFEGUARDS PRINCIPLE）

- 合理的な安全保護の措置によって、紛失や破壊、使用、改ざん、漏えいなどから保護すべきである。

【解説】

- ✓ 個人情報保護法で言うところの「適切な安全管理措置」のこと。
- ✓ 個人データに限らず、ビジネス上知り得た情報のほとんどは、何らかの安全管理措置を講じているはず。
- ✓ 個人データで特に安全簡易措置が取り上げられるのは、大規模漏えいなどの事故が生じた時に、個人に対して不利益が生じる可能性が高いと考えられているため。
- ✓ とは言え、必要以上のコストを掛ける必要はなく、「合理的」な方法つまりリスクの特定と相応の対策を行うべし、ということ。

6. 公開の原則（OPENNESS PRINCIPLE）

- 個人データの収集を実施する方針などを公開し、データの存在やその利用目的、管理者などを明確に示すべきである。

【解説】

- ✓ いわゆる「プライバシーポリシー」を作成し、個人データの取扱い方針を公にすべし、ということ。
- ✓ Webサイトを公開している企業のほとんどは、プライバシーポリシーを掲載しているし、プライバシーポリシーを公開するということは、きちんとした個人データの保護方針を持っていることの外部的なアピールにもなり、社会的な信用も得られる。

7. 個人参加の原則（INDIVIDUAL PARTICIPATION PRINCIPLE）

- 個人データの主体が、自分に関するデータの所在やその内容を確認できるとともに、異議を申し立てることを保証すべきである。

【解説】

- ✓ この考え方は、個人データとは、個人データの主体（もともとの個人情報の持ち主である本人）のものである、ということに基づく。
- ✓ つまり、企業は個人から個人データを「借りて」いるだけであり、個人データは決して企業の所有物にはならない、ということ。
- ✓ 一時的に本人から個人データを預かっているだけなので、本人から「返してくれ」と言われれば返す必要があるし、「どんな使い方をしてるのか教えろ」と言われたらきちんと説明する義務がある。
  （要は、銀行が個人から貯金を預かっているのと一緒）

8. 責任の原則（ACCOUNTABILITY PRINCIPLE）

- 個人データの管理者は、これらの諸原則を実施する上での責任を有するべきである。

【解説】

- ✓ ここで言う責任とは、英語だと ”Accountability” であり、「この件は全部オレが責任をとる！」のほうの責任ではなく、「説明責任」というニュアンスで捉えたほうが良い。
- ✓ 個人データの扱いに限らず、データ漏えいなどの事故はどんなに対策をとっていても可能性をゼロにすることはできない。
  （自動車のゴールド免許の人が事故をおこさないという保証はどこにもない）
- ✓ 説明責任とは、
  - ✓ リスクをどのように設定し、
  - ✓ そのリスクに対してどの程度の脅威として評価し、
  - ✓ 対策として何を行ったか
  - ✓ （万一事故が起きたときに）どのように対処したか

  ということを、きちんと説明できるようにしておくべし！　ということ。