# ＧＤＰＲと個人情報保護制度の動向

2020.02.26.
小向　太郎 Taro KOMUKAI, Ph.D.
日本大学　危機管理学部　教授

1.　GDPRの概要
　1-1.　GDPRの影響
　1-2.　GDPRの条文構成
　1-3.　対象となる情報

2.　個人データ処理の適法化根拠
　2-1.　適法な処理の要件
　2-2.　「本人の同意」と「適法な利益」
　2-3.　「本人の権利」に関する規定

3.　日本の制度見直しへの影響
　3-1.　制度改正大綱
　3-2.　制度枠組みの違い
　3-3.　今後の課題



# 自己紹介：小向太郎

日本大学　危機管理学部　教授
デジタル・フォレンジック研究会　理事
【専門分野】
情報法、情報通信法
【主な著書】
『情報法入門（第5版）デジタル・ネットワークの法律』NTT出版、2020
『概説GDPR　世界を揺るがす個人情報保護制度』共著、NTT出版、2019
『情報通信法制の論点分析』共著、商事法務、2015
『入門　安全と情報』共著、成文堂、2015
『表現の自由Ⅱ-状況から』共著、尚学社、2011
『プライバシー・個人情報保護の新課題』共著、商事法務、2010　等

# 1. GDPRの概要



## 1-1. GDPRの影響

- 「EU一般データ保護規則（GDPR）」
  - 欧州連合（EU）における個人情報保護の新しいルール
  - 法的強制力を持ち高額な制裁金が科せられることもある強力な法律（EU法）

- 世界的に甚大な影響を及ぼすと考えられている理由
  - EUは、個人情報保護政策をリードしてきた世界のトップランナーであり、個人情報保護を求める声の高まりを受けて、他国の制度にも大きな影響を持つ
  - EUは以前から、個人情報保護が十分になされていない国への個人情報の移転を原則として禁止している。GDPR成立後は、より厳格にEU域外への移転が制限されることになる
  - GDPRは、EU域外の者が、EU域内にいる人（EU市民等）の個人情報を取扱う場合にも、広く適用されるという立場を採っている

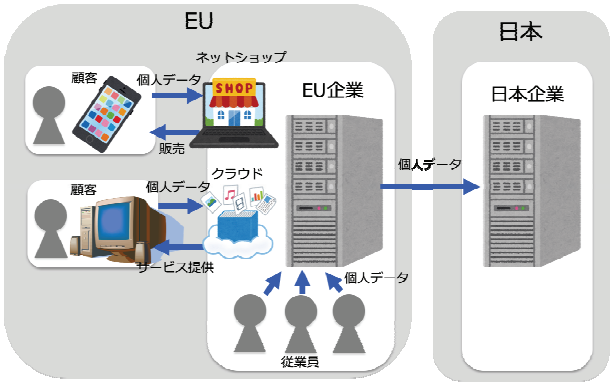
# （参考） 域外適用と域外移転

| ビジネス種別 | 域内拠点 | EU市民等の個人顧客 | 主な対象情報 | 対応義務 |
|---|---|---|---|---|
| ① EU 域 内 でのB2C | ○ | ○ (B2C) | 顧客情報 従業員情等 | 全規定の遵守* |
| ② EU 域 内 でのB2B | ○ | X (B2B) | 従業員情報等 | 全規定の遵守* |
| ③EUを対象としたB2C | X | ○ | 顧客情報 | 全規定の遵守 代理人の設置 |
| ④EUからの域外移転 | X | X | EUから提供された個人データ | 十分性認定 PPC-GL遵守 |

*日本の本社等への個人データの移転については、十分性認定に基づき行うことができる。



# （参考）域外移転



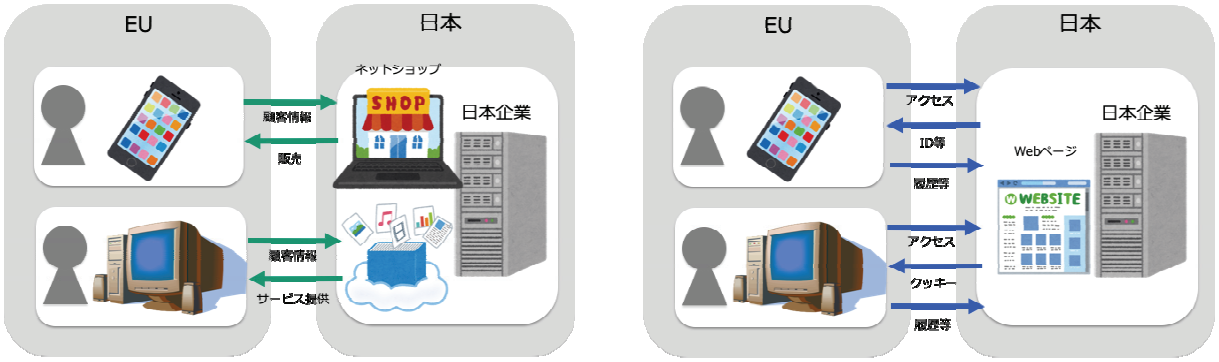

【域外移転が許される場合】
①十分性認定（第45条）
②拘束的企業準則(BCRs)
（第46条2項(b)号）
③標準データ保護条項(SPDCs)
（第46条2項(c)号、(d)号）
④行動規範（第46条2項(e)号）
⑤認証（第46条2項(a)号）
⑥特別の状況（第49条）

- 欧州委員会は、2019年1月23日に日本に対する十分性を認める決定を行っている
- 日本は、十分性認定を受けると同時に、EUを「我が国と同等の水準･･･外国」と認定した
- 個人情報保護の分野におけるはじめての相互認定

# （参考）EUに拠点のない事業者への域外適用

【物品またはサービスの提供】
（考慮要素例）
- EU加盟国名への言及
- EU の消費者の利用促進施策
- 観光事業など活動の国際性
- 専用アドレス・電話番号
- 「.de」「.eu」などのドメイン名
- EUからの移動案内
- EUに居住する顧客への言及
- 言語・通貨
- 商品の配送

【モニタリング】
（代表例）
- 行動ターゲティング広告
- 位置情報サービス
- クッキー・指紋認証等の追跡技術
- オンラインの個別顧客向け分析サービス（食事・健康）
- 監視カメラ
- 市場調査等の行動調査
- 健康管理サポート




出典：EDPB「地理的適用範囲（第3条）に関するガイドライン（案）（3/2018）」（2018年11月16日）をもとに作成



# （参考）欧州におけるデータ保護

- 欧州連合基本権憲章　第８条（個人データの保護）
  ①何人も、自分に関する個人データの保護を受ける権利を有する
  ②そのようなデータは、その情報の関係者の承諾か、その他の法定の適法な根拠に基づいて、限定された目的のために、公正に取り扱われなければならない。何人も、自分に関して収集されたデータに対してアクセスする権利および情報を訂正する権利を有する
  ③これらのルールの遵守は、独立の機関による監督を受けなければならない

- 「個人データ保護は、国際的な通商交渉等においてこれに関する譲歩はできないもの（non-negotiable）である」Jean-Claude Juncker, A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change

# 1-2.　GDPRの条文構成（１）

| 章立て | 規定内容 | ポイント |
|---|---|---|
| 第１章　一般規定 | 対象、適用範囲、定義等 | EUに関わる個人データに広く適用される |
| 第２章　基本原則 | 基本原則（適法性・公正性・透明性、目的の限定、データの最小化、正確性、記録保存の制限、完全性および機密性）、同意原則、子供の情報・センシティブデータ等 | 個人データの取扱いには、本人の同意か正当化事由が必要となり、同意は本人の意思を反映したものでなくてはならず、本人はいつでも撤回できる |
| 第３章　データ主体の権利 | 透明性および手順、アクセス権、訂正および消去、データポータビリティ、異議申立権・プロファイリング | 本人は自分に関するデータにアクセスし、訂正・消去や、他のプラットフォームへの移転ができる。同意に基づかない処理に対しては異議申し立てができ、個人データを使った自動処理で重要な決定を行うことは禁止される |
| 第４章　管理者および処理者 | 一般的な義務、安全性、データ保護影響評価、データ保護オフィサー、行動起案と認証 | 管理者と処理者は、適正な処理を行わなければならない。管理者はGDPRの遵守と説明責任を負う |

出典：GDPRの条文をもとに作成



# 1-2.　GDPRの条文構成（２）

| 章立て | 規定内容 | ポイント |
|---|---|---|
| 第５章　第三国または国際機関への個人データの移転 | 一般原則、十分性認定、適切な保護に従った移転、拘束的企業準則（BCP）、国際協力等 | EUが十分なレベルの保護と認めた国以外の第三国への個人データの移転は原則として許されない |
| 第６章　独立監督機関 | 独立的地位、権限 | データ保護のため監督機関は独立した権限あるものでなければならない |
| 第７章　協力と一貫性 | 監督機関間の協力、一貫性メカニズム、欧州データ保護会議 | 監督機関の間の連携や欧州としての規制の統一性を図る仕組みが整備される |
| 第８章　救済、法的責任および制裁 | 規制に対する異議申し立て、司法救済、制裁金等 | 巨額の制裁金を始めとして、具体的な救済措置が整備される |
| 第９章　特定の取扱いの状況と関係する条項 | 表現の自由、公文書、国民識別番号、被雇用者、公共の利益、守秘義務、宗教関連等 | 特別な配慮が必要な情報について、加盟国法で利用できる範囲が示される |
| 第１０章　委任される行為および実装行為 | 委任される行為の執行、委員会の手続き | GDPRの執行に関する欧州委員会の権限が示される |
| 第１１章　最終規定 | EUの他の制度との関係 | 95年指令はGDPRに改正され、関連規則も必要部分が変更される |

出典：GDPRの条文をもとに作成

# 1-3.　対象となる情報

| | |
|---|---|
| 個人データ | 識別された又は識別可能な自然人に関する情報。特に、氏名、識別番号、位置データ（location data)、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す一つ又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、識別されうる者（第4条（1））|
| （参考）<br>匿名化 | データ主体（本人）を識別できないようにすることを指し、匿名化されたデータは個人データに該当せず、GDPRの対象にならない（前文（26）項）。その情報から、ある個人一人が選び出されることがありえない場合*にのみ、匿名化された情報と認められる。 |
| （参考）<br>仮名化 | 当該追加情報が別に管理され、個人データを識別され又は識別され得る自然人に帰属させないことを保障するための技術的及び組織的措置に服することを条件に、追加情報を利用しないと、個人データをもはや特定の本人に帰属させることのできない態様による個人データの処理（第4条（5）項） |

- それぞれの情報が一人の個人と実質的に対応している限り、このような状態にすることは、現実にはかなり困難である



# （参考）匿名加工情報

- 定義
  - ①特定の個人を識別できないように個人情報を加工して得られる個人に関する情報であって、②当該個人情報を復元できないようにしたもの
  - いかなる方法を持ってしても、絶対に特定の個人を識別できないこと、特定の個人を復元できないことまでを要求するものではない

- 個人情報保護委員会の「補完的ルール」
  - EU域内から十分性認定に基づき提供を受けた個人情報については、個人情報取扱事業者が、加工方法等情報（匿名加工情報の作成に用いた個人情報から削除した記述等及び個人 識別符号並びに法第 36 条第 1 項の規定により行った加工の方法に関する情報（その情報を用いて当該個人情報を復元することができるものに限る）をいう）を削除することにより、匿名化された個人を**再識別することを何人にとっても不可能とした場合に限り**、法第2条第9項に定める匿名加工情報とみなすこととする

## （参考）何のために匿名化や仮名化を行うのか

- 日本における匿名化の議論は、個人情報該当性に集中する傾向がある
- 米国では、匿名化・仮名化によって軽減すべき義務がなく、安全管理措置としての側面が強い
- EUにおける匿名化・仮名化は、個人情報該当性だけでなく、多面的に評価される

| | 日本 | 米国 | EU |
|---|---|---|---|
| 個人情報該当性 | ◎ | △ | ○ |
| 安全管理措置 | △ | ○ | ○ |
| 正当化事由 | X | X | ○ |
| 消去・利用停止 | X | X | ○ |



## 2.　個人データ処理の適法化根拠

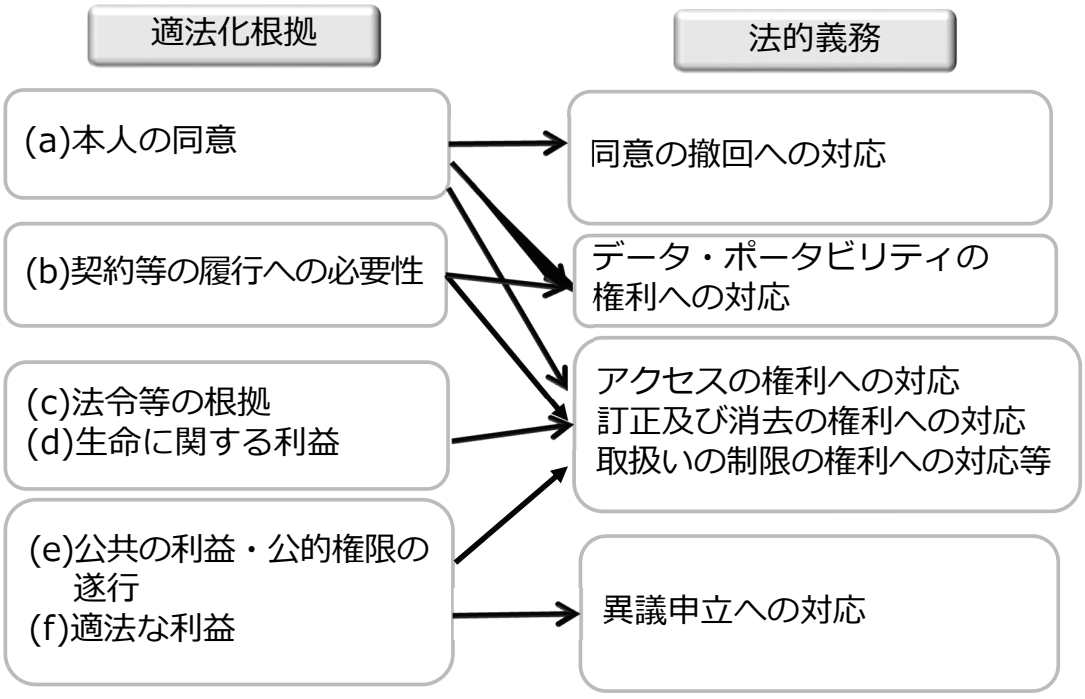
# 2-1.　適法な処理の要件（１）

| 適法化根拠 | 処理が適法化される場合 |
|---|---|
| (a)本人の同意 | 本人が、一つ又は複数の特定の目的のための自己の個人データの処理に関し、同意を与えた場合 |
| (b)契約等の履行への必要性 | 本人が契約当事者となっている契約の履行のために処理が必要となる場合、又は、契約締結の前に、本人の要求に際して手段を講ずるために処理が必要となる場合 |
| (c)法的義務 | 管理者が服する法的義務を遵守するために処理が必要となる場合 |
| (d)生命に関する利益 | 本人又は他の自然人の生命に関する利益を保護するために処理が必要となる場合 |
| (e)公共の利益・公的権限の遂行 | 公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために処理が必要となる場合 |
| (f)適法な利益 | 管理者によって、又は、第三者によって求められる適法な利益の目的のために処理が必要となる場合。ただし、その利益よりも、個人データの保護を求める本人の利益並びに基本的な権利及び自由のほうが優先する場合、特に、その本人が子どもである場合を除く。 |

出典：GDPRの条文をもとに作成

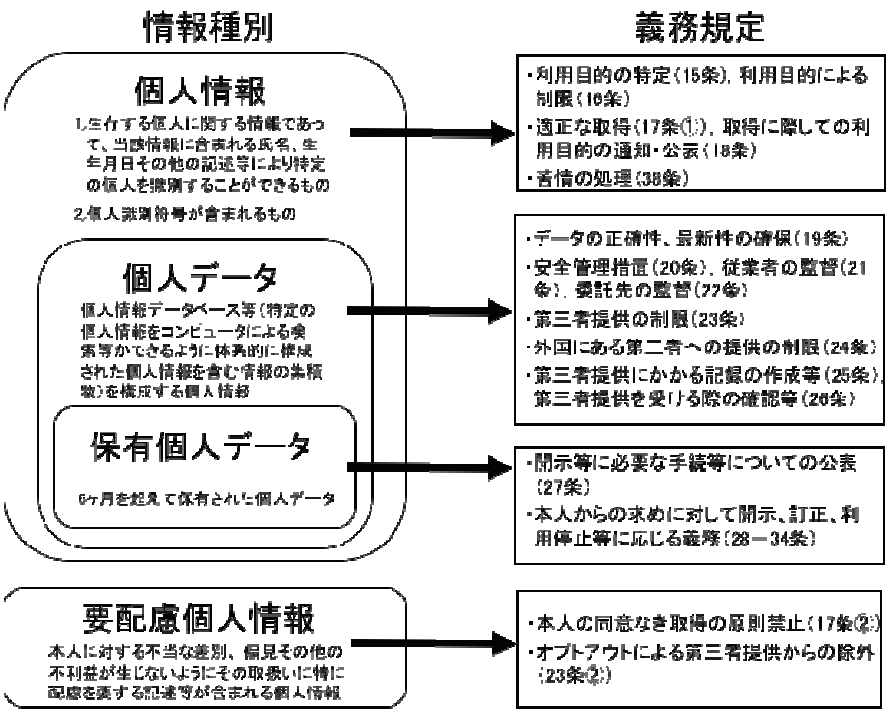


# 2-1.　適法な処理の要件（２）




出典：GDPRの条文をもとに作成

# （参考）個人情報保護法（日本）における事業者の義務




出典：　小向太郎「情報法入門（第4版）デジタル・ネットワークの法律」NTT出版（2018年）



# 2-2.　「本人の同意」と「適法な利益」（１）

【「本人の同意」の要件】

| | 概要 |
|---|---|
| ①自由な同意 | 本人が自由に選択したものでなければ、有効な同意とはみなされない。同意を拒否したり、あとで撤回したりすると不利益を受けたりするようなことがあれば、その同意は、自由な同意ではない |
| ②特定された同意 | 同意を取得する際には、どのような利用目的のためにどのように個人データが取り扱われるのかをはっきりさせ、その全てについて取得される必要がある。明らかに複数の利用目的がある場合に、包括的に同意取得することは許されない |
| ③事前説明を受けた同意 | 同意が有効であるためには、本人が、少なくとも、管理者の身元、及び、その個人データについて予定されている処理の目的を認識していなければならない |
| ④不明瞭ではない表示による同意 | 個人データの取扱いに対する同意であることがわかるように、他の契約条件等とは明確に区別して、本人の意思を確認する必要がある。一般の利用条件の中に同意を紛れ込ませてはならない。 |
| ⑤明らかに肯定的な行為による同意 | 同意は、本人がはっきりと表明したものでなければならない。 |

出典：第29条作業部会「同意に関するガイドライン（WP259 rev. 01）」（2017年11月28日、2018年4月10日最終修正・採択）等をもとに作成

# 2-2.　「本人の同意」と「適法な利益」（２）

【「適法な利益」の考慮要素】

| 本人の基本権とのバランス | 追加的な安全策の評価 |
|---|---|
| • 利益の性質（基本権、その他の利益、公共の利益）<br>• データが取り扱われない場合に、管理者、第三者又はより多くの人々が、被る可能性のある不利益<br>• データの性質（機微情報該当性）<br>• 本人（未成年者、従業員等）と管理者（市場支配的な地位にある企業かどうか等）の関係<br>• データの処理方法（規模、データマイニング・プロファイリングの有無、公表の有無）<br>• 本人の基本権や利益のうち、どのようなものが影響を受ける可能性があるのか本人合理的な期待を考慮する。<br>• 本人への影響と、管理者が得られる利益の具体的比較 | • データの最小化（例えば、データ収集の厳格な限定、又は使用後のデータの即時削除）<br>• 当該データを利用して、個人に関する意思決定その他の行為が行われないようにするための、技術的および組織的措置（「機能的分離」）<br>• 匿名化技術、データの集約、<br>• プライバシー向上技術（PET: Privacy Enhancing Technology）、<br>• プライバシー・バイ・デザイン、<br>• プライバシー・データ保護影響評価の幅広い使用<br>• 透明性、一般的かつ無条件に異議を申し立てる権利（オプト・アウト）、本人の自由度を拡大するためのデータ・ポータビリティとその関連措置の拡大 |

出典：第29条作業部会「95年データ保護指令におけるデータ管理者の適法な利益の意義に関する意見書（844/14/EN, WP217）」2014年4月9日）



# 2-3.　「本人の権利」に関する規定

| 条文 | 規定 | 概要 |
|---|---|---|
| 第12条 | 情報提供の透明性 | 分かりやすい情報提供の措置を講じる |
| 第１３条～第１５条 | 情報提供及びアクセス権 | データ主体(本人)からの取得、本人以外からの取得のそれぞれについて、提供すべき情報の項目についての情報提供<br>本人が自分のデータに対してアクセスできる権利 |
| 第17条 | 削除権（「忘れられる権利」） | 管理者に対して自己に関する個人データの削除を求める権利 |
| 第20条 | データ・ポータビリティの権利 | 管理者に提供した個人データを他の管理者に移す権利（クラウド・コンピューティングやソーシャル・ネットワークサービスなどを想定） |
| 第 21 条 ～第22条 | 異議申立権、自動処理決定(プロファイリング関係) | ・処理に対して異議申立をする権利(プロファイリングへの異議申立も含む)<br>・コンピュータ処理のみによる不利益な判断に服さない権利 |

出典：GDPRの条文をもとに作成

# （参考）削除権（忘れられる権利）

- 第17条　削除権（忘れられる権利）

  第１項：(a)収集目的の終了、(b) 同意の撤回、(c) 異議申立、(d)違法な処理、(e)個人情報保護法の個別要請、(f)SNS等で集められた子供の情報

  第２項：公表情報の拡散先への通知等

  第３項：例外規定（表現の自由、法定の義務、公共の利益等）

- Google v. Mario Costeja González（欧州司法裁判所）

Press and Information

Court of Justice of the European Union
**PRESS RELEASE No 70/14**
Luxembourg, 13 May 2014

Judgment in Case C-131/12
Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González

**An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties**

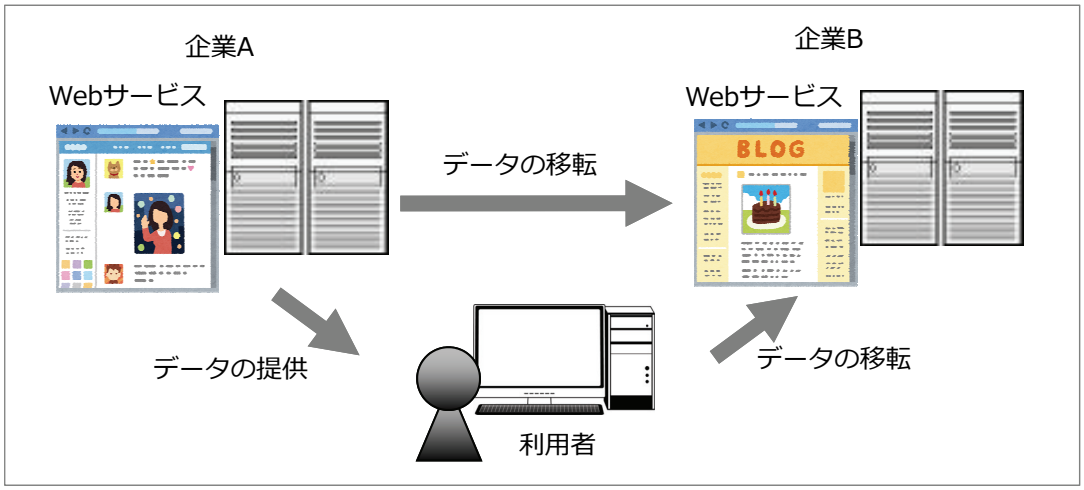
*Thus, if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results*

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf



# （参考）データ・ポータビリティ権

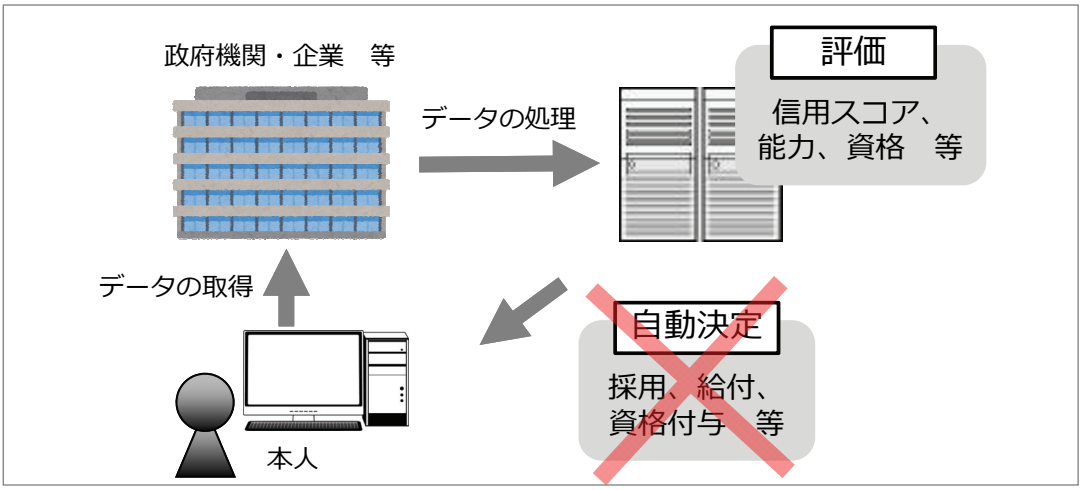
- クラウドやSNSで、利用者が新しいサービスに移行したいときに、データの移転を容易にするための権利
- 現在利用ている事業者から自分のデータを提供させ、他の事業者に移すことができる
- 技術的に実行可能であれば、事業者から事業者に直接に移行させることができる




出典：GDPRの条文をもとに作成

# （参考）プロファイリング関連

- 個人の評価を目的としたコンピュータによる個人データ処理
- 本人は、自己に関する法的効果をもたらすか、又は、それに類する重大な影響を自己にもたらす、コンピュータ処理のみに基づく決定に服さない権利を有する。この処理には「プロファイリング」が含まれる。オンライン採用や信用評価、教育を受ける場面などで問題となり得る。




出典：GDPRの条文をもとに作成



## 3.　新たな権利と日本への影響

# 3-1. 制度改正大綱（骨子案：2019.11.29.）

Ⅰ．個人データに関する個人の権利の在り方
　１．**利用の停止、消去、第三者提供の停止の請求に係る要件の緩和**
　２．開示のデジタル化の推進
　３．開示等の対象となる保有個人データの範囲の拡大
　４．オプトアウト規制の強化
Ⅱ．事業者の守るべき責務の在り方
　１．**漏えい等報告及び本人通知の義務化**
　２．適正な利用義務の明確化
Ⅲ．事業者における自主的な取組を促す仕組みの在り方
　１．認定個人情報保護団体制度の多様化
　２．保有個人データに関する公表事項の充実
Ⅳ．データ利活用に関する施策の在り方
　１．「仮名化情報」の創設
　２．提供先において個人データとなる場合の規律の明確化
　３．　公益目的による個人情報の取扱いに係る例外規定の運用の明確化
　４．　個人情報の保護と有用性に配慮した利活用相談の充実
Ⅴ．ペナルティの在り方
Ⅵ．法の域外適用の在り方及び越境移転の在り
　１．**域外適用の範囲の拡大**
　２．外国にある第三者への個人データの提供制限の強化
Ⅶ．官民を通じた個人情報の取扱い
　１．**行政機関、独立行政法人等に係る法制と民間部門に係る法制との一元化**
　２．地方公共団体の個人情報保護制度



# 3-2. 制度枠組みの違い

| | 個人情報保護法（日本） | GDPR（EU） | FTC法（米国） |
|---|---|---|---|
| 取得・利用時 | 利用目的の特定、通知または公表等（原則自由） | (a) 本人の同意<br>(b) 契約等の履行への必要性<br>(c) 法的義務<br>(d) 生命に関する利益<br>(e) 公共の利益・公的権限の遂行<br>(f) 正当な利益の目的 | 不公正または欺瞞的な行為・実務は禁止<br><br>（参考）CCPA 消去・オプトアウトの義務等 |
| 利用目的の変更・第三者提供 | • 本人の同意<br>• 法令の根拠<br>• その他（生命の保護等） | | |
| 特徴 | ノーオプト型 | オプトイン型 | オプトアウト型 |

## 3-3.　今後の課題

- 個人情報保護法では、本人の意思を反映しうる場面が、ほぼ第三者提供と利用目的変更の場合だけに限定されており、例えば、本人が望まない情報が収集・利用されても、法律上は問題とされない場合がある。特に内部利用については、**そもそも本人の意思反映や弊害の除去を実現する制度になっていない**。
- 個人情報利用の多様化によって、内部利用についても、**本人の意思に反する利用を抑制**し、**弊害や危険の大きな行為類型を制限**することで、弊害を予防したり、解消したりする必要性は大きくなっている。**利用目的に本人の意思を反映させる制度を導入することは必要**である。
- 一方で、事後的に第三者提供や利用目的変更を行うための条件は厳格であり、社会的に許容されるべき利用が制限される可能性がある（例：情報セキュリティ対策のための情報共有等）。
- 第三者提供や利用目的変更について、「適正な利益の目的」のような一般規定を導入することも検討すべきである。このような規制を導入する場合には、個人情報保護委員会の裁量をある程度認め、実質的判断を行うようにする必要がある。



## （参考）情報セキュリティのための情報共有

- ネットワーク及び情報の安全性を確保する目的のために厳密に必要性であり、かつ、比例的な範囲内で行われる個人データの取扱い、例えば、保存される個人データ若しくは送信される個人データの可用性、真正性、完全性及び機密性を阻害し、また、公的機関、コンピュータ緊急対応チーム（CERT）、コンピュータセキュリティインシデント対応チーム（CSIRT）、電子通信ネットワークのプロバイダ及び電子通信サービスのプロバイダ、並びに、セキュリティ技術及びセキュリティサービスの提供者によって、そのネットワーク及びシステムを介して提供され又はアクセス可能なものとされている関連サービスの安全性を阻害する事故、又は、違法な行為若しくは悪意ある行為に対して、所与の機密性のレベルにおいて対抗するためのネットワークシステム又は情報システムの能力を確保することは、関係するデータ管理者の**正当な利益を構成する**。これには、例えば、電子通信ネットワークへの無権限アクセス及び悪意あるコード配布を防止すること、並びに、「サービス拒否」攻撃やコンピュータ及び電子通信システムの破壊行為を阻止することが含まれうる。
（GDPR前文（４９）個人情報保護委員会　仮日本語訳）

# （参考）「匿名化」「仮名化」

- **日本の「匿名化」に関する議論は、個人情報保護該当性に集中する傾向がある。**しかし、個人情報該当性を排除する「匿名化」は、グローバルには厳格に照合可能性を排除したものと考えられており、それぞれの情報が一人の個人と実質的に対応している限り、現実にはかなり実施が困難である。
- そもそも匿名化・仮名化には、**個人情報取扱いの安全性向上**や、**本人の権利利益侵害の可能性を低減**することで、「適正な利益の目的のための利用を可能にするなど、**多面的な目的**がある。
- 個人情報保護該当性が関心が集中する背景には、もともと個人情報の内部利用にあまり制約がなく、その一方で事後的な利用目的の変更や第三者提供について本人の同意が必要となるという、個人情報利用に関する自由度のギャップがある。
- **匿名加工情報の推進や「仮名化」の制度の検討には、ほとんど意味がない。**第三者提供や利用目的変更について「適正な利益の目的」のようなバランステストを伴う一般規定を導入することの方が、情報および匿名化技術のより有効な活用に資する。