博士論文

個人情報・個人データ保護法制における健康・医療情報の
センシティブ情報への該当性とその取扱要件

Tomoki TANIGUCHI
谷口 友樹

情報セキュリティ大学院大学
情報セキュリティ研究科
情報セキュリティ専攻

2023年9月

目次：

Ⅰ 序（P5）
1. はじめに（P5）
1.1 個人情報を取り巻く環境（P5）
1.2 問題提起（P6）
1.3 本テーマの主題（P6）
1.4 本稿の構成（P7）
2. データローカライゼーション規制（P8）
2.1 規制の概要（P8）
2.2 日欧米中におけるデータローカライゼーション規制(広義)の比較（P8）
Ⅱ 法制概観（P11）
1. 日本（P11）
1.1 個人情報保護法制（P11）
1.1.1 該当法令（P11）
1.1.2 目的・法益（P11）
1.1.3 適用範囲（P12）
1.2 定義（P12）
1.2.1 個人情報（P12）
1.2.2 センシティブ情報（P14）
2. EU（P16）
2.1 個人情報保護法制（P16）
2.1.1 該当法令（P16）
2.1.2 目的・法益（P16）
2.1.3 適用範囲（P17）
2.2 定義（P17）
2.2.1 個人情報（P17）
2.2.2 センシティブ情報（P19）
3. 米国（P20）
3.1 個人情報保護法制（P20）
3.1.1 該当法令（P23）
3.1.2 目的・法益（P25）
3.1.3 適用範囲（P26）
3.2 定義（P29）
3.2.1 個人情報（P29）
3.2.2 センシティブ情報（P31）
4. 中国（P34）
4.1 個人情報保護法制（P34）
4.1.1 該当法令（P35）
4.1.2 目的・法益（P37）
4.1.3 適用範囲（P38）
4.2 定義（P39）
4.2.1 個人情報（P39）

4.2.2 センシティブ情報（P41）

5. 小括（P43）
5.1 日米欧中における法制に関する共通点と相違点（P43）
5.2 日米欧中における個人情報の範囲に関する共通点と相違点（P46）
5.3 日米欧中におけるセンシティブ情報の範囲に関する共通点と相違点（P50）
Ⅲ センシティブ情報取扱いに対する規制の厳格化（P51）
1. 日本（P51）
1.1 一般的な個人情報の取扱いに対する規制（P51）
1.1.1 日本国内における個人情報の取扱いに関する主な法令要件（P51）
1.1.1.1 取得・利用（P51）
1.1.1.2 第三者提供・委託（P52）
1.1.1.3 保管・管理（P52）
1.1.1.4 データローカライゼーション規制（P52）
1.1.1.5 体制・責任者（P56）
1.1.1.6 本人の権利（P56）
1.1.1.7 データ侵害・インシデント（P56）
1.2 センシティブ情報の取扱いに対し法令要件が厳格化される局面及びその加重要件(P57)
1.3 仮名化及び匿名化（P59）
1.3.1 仮名化（P59）
1.3.2 匿名化（P60）
1.3.3. 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和（P60）
2. EU（P63）
2.1 一般的な個人情報の取扱いに対する規制（P63）
2.1.1 EU域内における個人データの取扱いに関する主な法令要件（P63）
2.1.1.1 取扱いの基本原則（P63）
2.1.1.2 取扱いの適法性（P64）
2.1.1.3 データ管理者の義務（P64）
2.1.1.4 データ処理者の義務（P65）
2.1.1.5 データ管理者及びデータ処理者の両方にかかる義務（P65）
2.1.1.6 データ主体の権利（P65）
2.1.1.7 データ侵害・インシデント（P67）
2.1.1.8 データローカライゼーション規制（P69）
2.2 センシティブ情報の取扱いに対し法令要件が厳格化される局面及びその加重要件(P72)
2.3 仮名化及び匿名化（P78）
2.3.1 仮名化（P78）
2.3.2 匿名化（P78）
2.3.3. 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和（P78）
3. 米国（P79）
3.1 一般的な個人情報の取扱いに対する規制（P79）
3.1.1 米国内における個人データの取扱いに関する主な法令要件（P79）
3.1.1.1 取得・利用・提供（P79）

3.1.1.2 委託（P81）
3.1.1.3 保管・管理（P81）
3.1.1.4 データローカライゼーション規制（P82）
3.1.1.5 体制・責任者（P82）
3.1.1.6 本人の権利（P82）
3.1.1.7 データ侵害・インシデント（P83）
3.2 センシティブ情報の取扱いに対し法令要件が厳格化される局面及びその加重要（P83）
3.3 仮名化及び匿名化（P86）
3.3.1 仮名化（P86）
3.3.2 匿名化（P86）
3.3.3. 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和（P88）
4. 中国（P89）
4.1 一般的な個人情報の取扱いに対する規制（P89）
4.1.1 中国内における個人データの取扱いに関する主な法令要件（P89）
4.1.1.1 取得・利用（P89）
4.1.1.2 第三者提供・委託（P89）
4.1.1.3 保管・管理（P90）
4.1.1.4 データローカライゼーション規制（P90）
4.1.1.5 体制・責任者（P91）
4.1.1.6 本人の権利（P91）
4.1.1.7 データ侵害・インシデント（P91）
4.2 センシティブ情報の取扱いに対し法令要件が厳格化される局面及びその加重要件(P92)
4.3 仮名化及び匿名化（P92）
4.3.1 仮名化（P92）
4.3.2 匿名化（P92）
4.3.3 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和（P93）
5. 小括（P95）
5.1 日米欧中における個人情報取扱い規制に関する比較（P95）
5.2 日米欧中におけるセンシティブ情報取扱いの厳格化に関する比較（P96）
Ⅳ 結語（P99）
1. 総括（P99）
1.1 各章のまとめ（P99）
1.2 ヘルスケア分野における仮名化処理又は匿名化処理の有用性（P100）
2. 実務的観点での提言（P101）
2.1 実務上の問題点（P101）
2.2 施策の提言（P102）
3. 立法的観点での提言（P103）
3.1 要配慮個人情報の定義に関する問題点（P103）
3.2 個人情報保護法令における改正の提言（P106）
3.2.1 個人情報保護法令に関する本論文における改正提案（P107）
3.2.2 情報セキュリティ管理法令に関する本論文における改正提案（P117）
3.3. 最後に（P120）

Ⅰ 序

第Ⅰ部では、本論文の序章として、本稿の主題を明確にする。

1. はじめに

本章では、ヘルスケア事業をグローバルで運営する企業が、センシティブ情報をクロスボーダーで取り扱うことによって生じる問題を提起した上、その問題を解決するにあたっての論点を整理する。

1.1 個人情報を取り巻く事業環境

Data Free Flow with Trustが提言される中、グローバルでヘルスケア事業を展開する法人その他組織・団体（以下、総称し「グローバルヘルスケア法人」という。）は、国毎に制定されている個人情報保護法制上の法令要件を具備しなければならない。

その主な背景として、まずグローバルヘルスケア法人における事業スキームの変容が挙げられる。

デジタルトランスフォーメーション（以下、「DX」という。）の進展に伴い、生活様式や商品・サービス形態の"リモート化・遠隔化"が浸透し始めたことに伴い、個人情報がクロスボーダーで取り扱われグローバルに流通する傾向にある。特にコロナ禍を契機として、グローバルヘルスケア法人は、遠隔診療支援サービスその他医療機関向けアプリケーション/Webサービス（以下、「医療支援サービス」という。）や、一般消費者及びユーザー等、セルフメディケーションを支援するデータ主体向けリモートサービスその他アプリケーション/Webサービス（以下、「健康管理サービス」という。）のローンチを進めている。それらサービスは、AWS (Amazon Web services)、GCP (Google Cloud Platform)や、Azure (Microsoft Azure)といったプラットフォーマーのクラウドサービスを基盤とし、医療支援サービス又は健康管理サービス（以下、両方を称して、「健康・医療サービス」という。）をグローバル展開することで、健康・医療情報のクロスボーダーでの取扱いが常態化している。

併せて、DXの進展に伴い、欧米のみならず日本でも、個人の健康状態や服薬履歴等を本人や家族が随時確認でき、日常生活の改善や健康増進につなげるための仕組みである PHR(Personal Health Record. 以下、「PHR」という。)[1]の整備を推進している[2]。

一方で、このような健康・医療サービスで取り扱う情報は一般の個人情報とは異なり、慎重な取扱いが求められる。世界各国では、個人情報・個人データ保護法令その他個人情報の取扱いを規制する法制度（以下総称し、「個人情報保護法制」という。）の整備が進展しているが、これら法整備は、国毎に行われるため、個人情報及びセンシティブ情報の定義並びにそれらの取扱要件は、各国で異なることが少なくない。とりわけ、国によっては、クロスボーダーでの個人情報の取扱いを制限するため、データの国内保存等を義務付けるデータローカライゼーション規制を設ける国もある。

---

[1] 内閣官房「未来投資戦略2018 -「Society 5.0」「データ駆動型社会」への変革- 平成30年６月15日」（3.(1)②(P9)）https://www.cas.go.jp/jp/seisaku/seicho/kettei.html、株式会社野村総合研究所「令和元年度 内外一体の経済成長戦略構築にかかる国際経済調査事業 （我が国の PHR の利活用・事業創出の推進に向けた調査）報告書」2020年3月（P14-P15）https://iss.ndl.go.jp/books/R100000002-I030616818-00

[2] 経産省HP PHRサービス事業協会（仮称）」を設立します ～健康・医療データ（PHR)を活用したサービス産業発展へ環境整備を加速～ https://www.meti.go.jp/press/2022/06/20220620005/20220620005.html

1.2 問題提起

センシティブ情報とは、個人のプライバシーを保護する上で、とりわけその取扱いに配慮を要する類の情報である。そのため、センシティブ情報は、住所・氏名・電話番号といった一般的な個人情報（本稿では、このような非センシティブ情報となる個人情報全般を以下、「一般的な個人情報」という。）に比して、より厳格な取扱要件及び情報セキュリティ管理が要求される。

一方で、センシティブ情報は、グローバルで統一された定義はなく、各国が個人情報保護法制の中でそれを定義し、且つその取扱要件又は情報セキュリティ管理措置について定めているのが現状である。

そのような状況下において、グローバルヘルスケア法人が、健康・医療サービスを通じて取得する個人情報をクロスボーダーで取り扱うと、当該情報は、X国で非センシティブ情報であっても、Y国ではセンシティブな情報に該当することもあり得る。その場合Y国では、一般的な個人情報の取扱いに比し、より厳格な取扱要件が適用され得る。そのため、グローバルヘルスケア法人は、健康・医療サービスを提供する国の法制と、取扱う情報の性質を踏まえ、国毎にセンシティブ情報の該当性を慎重に検討した上で、判断しなければならず、判断が不適切であった場合には、法令違反を招く可能性もある。それに伴い更には、重大なプライバシー侵害やレピュテーションリスクの発生といった重大な事態に陥るおそれもあり、これは、法的観点だけでなく、倫理的及び社会的な観点からも、決して許されるものではない。そのためこのような自体に陥ってしまうと、法令上の罰則が科されるのみならず、レピュテーションリスクも負うこととなり、事業の持続可能性が極めて不透明となってしまいかねない。それでは、グローバルヘルスケア法人が、全ての個人情報を最も厳格なセンシティブ情報の規制に適合するようにグローバルで取り扱えばよいかといえば、そうすると、厖大なコストが生じることは避けられず、事業を展開する上で大きな負担が生じることになってしまう。

1.3 本テーマの主題

上述の問題への解決にあたっては、国毎に個人情報保護法制で定めるセンシティブ情報の定義及びその取扱要件を明らかにした上、それらを比較することで、各国で共通する点と相違する点を把握する必要がある。そこで、本稿では、日米欧中における法制度を比較し、ヘルスケア分野で取り扱う医療情報・健康情報のセンシティブ情報への該当性とその規制についての検討を行い、健康・医療サービスを提供する際に適用される各国法規制の共通点と相違点を明らかにしたい。

そこで、下記の通り論点を整理した上、設定した問いについて論じていく。

なお本稿では、①医療に関する患者情報（個人識別情報）を含む情報で、医療従事者が作成・記録した情報、及び医療従事者の指示に基づき介護事業者が作成・記録した情報（以下、「医療情報」という。）[3]、及び②健康管理サービスの提供に伴い、データ主体が、家庭用健康・医療機器、スマートフォンやウェアブル端末等で測定し自己管理しセルフメディケーションを行うための体重・BMI、体温、血圧・脈拍、心電・心拍、SpO2(血中酸素飽和濃度)、血糖値、喘鳴、尿中のNa/K比(ナトリウムとカリウムの比率)又は睡眠等の情報（以下、「健康情報」という。）の2つを取り上げ、日米欧中における法制の比較を通じ、各国でのヘルスケアでのセンシティブ情報の位置付けを明らかにする。

[3]「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」経済産業省 令和2年8月（令和4年８月改訂）P6（https://www.meti.go.jp/policy/mono_info_service/healthcare/01gl_20220831.pdf）、及び「医療情報システムの安全管理に関するガイドライン 第5.2版 本編」厚生労働省 令和4年3月 P3（https://www.mhlw.go.jp/content/10808000/000936160.pdf）

(1) 各国の個人情報保護法制において、センシティブ情報はどのように定義されているのか。また、医療情報及び健康情報は、それに該当するのか。

(2) センシティブ情報は、一般的な個人情報に比し、どのような取扱局面において、取扱要件が厳格化されるのか。とりわけクロスボーダーで取り扱う局面において、厳格化されるのか。

(3) 取扱要件が厳格化される場合、加重される要件は何か。またセンシティブ情報に仮名化または匿名化処理を施すことにより、取扱要件は緩和されるのか。

(4)上記(1)乃至(3)において、日米欧中各国で、共通する点と相違する点は何か。

最後に上記(1)乃至(4)の問いについての論述を取り纏めた上、ヘルスケア分野におけるグローバルでの法動向とPHRの観点より、センシティブ情報に係る法規制に関する施策や法制上の問題点を整理する。その整理にあたっては、グローバルヘルスケア法人における自律的な自助努力により解決を図るという実務的観点と、それでは解決することができないため、法令改正によって解決を図るといった立法的観点の両面から検討をした上で、提言を行いたい。また、後者においては、個人情報保護法令上のヘルスケア分野に係るセンシティブ情報の定義のみならず、センシティブ情報の情報セキュリティ管理を定める法令についても、併せて改正に関する提言を行う。

なお、提言にあたっては、日本発となるグローバルヘルスケア法人が、先行し日本で、健康・医療サービスのProof of Concept（以下、「PoC」という。）を実施した後、海外とりわけ米欧中へサービス展開していくというサービスデザインプロセス（以下、「DRプロセス」という。）を前提とする。

1.4 本稿の構成

上述の主題を踏まえ次のように本稿を構成する。

第Ⅰ部は導入部として、上述の通り、個人情報を取り巻く環境を踏まえた問題提起を行った上で、本テーマの主題を設定し、それに沿った本稿の構成を予め述べておく。

第Ⅱ部では、上述1.3(1)及び(4)を踏まえ、日米欧中において、健康情報及び医療情報（以下、併せて「健康・医療情報」という。）が、センシティブ情報に該当するのか、について明らかにしていく。

それを明らかにするにあたり、各国において、センシティブ情報を定義する個人情報保護法制を特定し、その法制概観を通じて、個人情報及びセンシティブ情報の定義を整理した上で、それらに関する共通点と相違点について考察する。

第Ⅲ部では、上述1.3(2)乃至(4)を踏まえ、日米欧中において、①一般的な個人情報に比し、健康・医療情報の取扱いが厳格化される局面及びその局面における加重要件は何か、とりわけセンシティブ情報のクロスボーダーでの取扱いにおける厳格化について明らかにしていく。

併せて、②個人情報の仮名化処理及び匿名化処理の定義・考え方、についてもここで予め整理した上で、上記①及び②に関する共通点と相違点について考察する。

最後に第Ⅳ部では、第Ⅰ部乃至第Ⅲ部を総括し、実務的観点と立法的観点から、日本のセンシティブ情報に関して、ヘルスケア法人向けの施策と併せて、法令改正についての提言を行う。

2. データローカライゼーション規制

本章では、法制概観へ入る前にデータのクロスボーダーでの取扱いに対して制限を加えるデータローカライゼーション規制の概要について、予め触れておくこととする。

2.1 規制の概要

プライバシーの保護、自国内産業の保護、安全保障の確保、法執行/犯罪捜査等の理由から、国家にとって重要なデータを自国内に留める（ローカライズする）ことを目的として、自国に所在する個人からデータが直接又は間接的に取得される局面において、当該国がそのデータの取扱いに対して、一定の制限や義務を課すことをデータローカライゼーション規制という。

この規制は狭義と広義の定義があり、狭義では国内保存義務又は国内設備設置義務を指し、広義ではその義務と併せて、海外移転制限を含めた規制を意味する。ここで国内保存義務とは、自国所在の個人から取得したデータを自国に保存させる義務、また国内設備設置義務とは、データを処理・保存するシステム・サーバー等の設備を自国内に設置させる義務をいう。海外移転制限とは、自国所在の個人から取得したデータの海外への移転を制限する規制のことをいう。

なお、データローカライゼーション規制は、自国に所在する法人（以下、「国内法人」という）だけでなく、自国外に所在する海外法人（以下、「海外法人」という。）にも適用される、いわゆる域外適用がなされる場合がある。

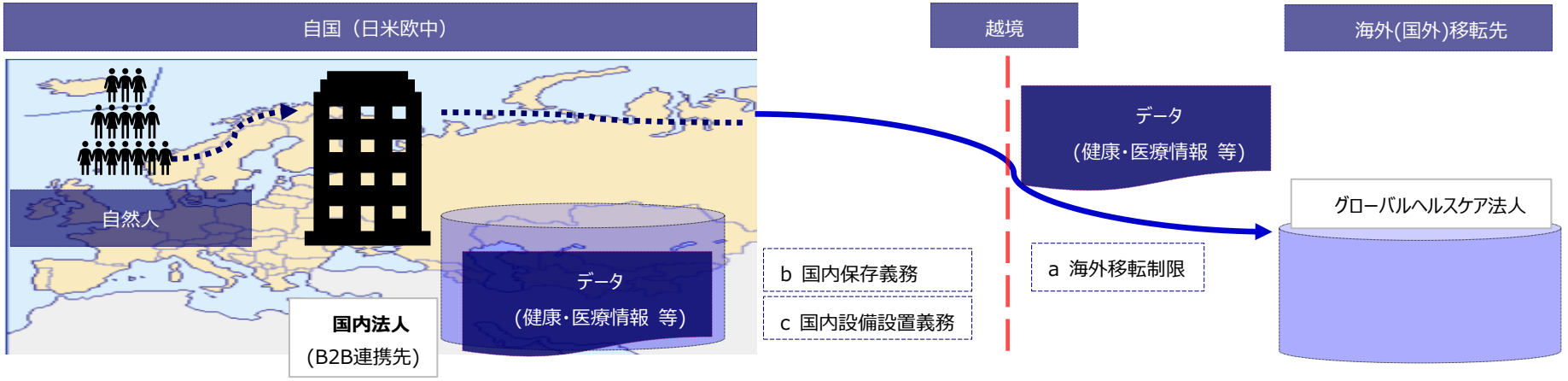
以上の規制概要を図示したものが、下記図Ⅰ2.1である。

2.2 日欧米中におけるデータローカライゼーション規制(広義)の比較

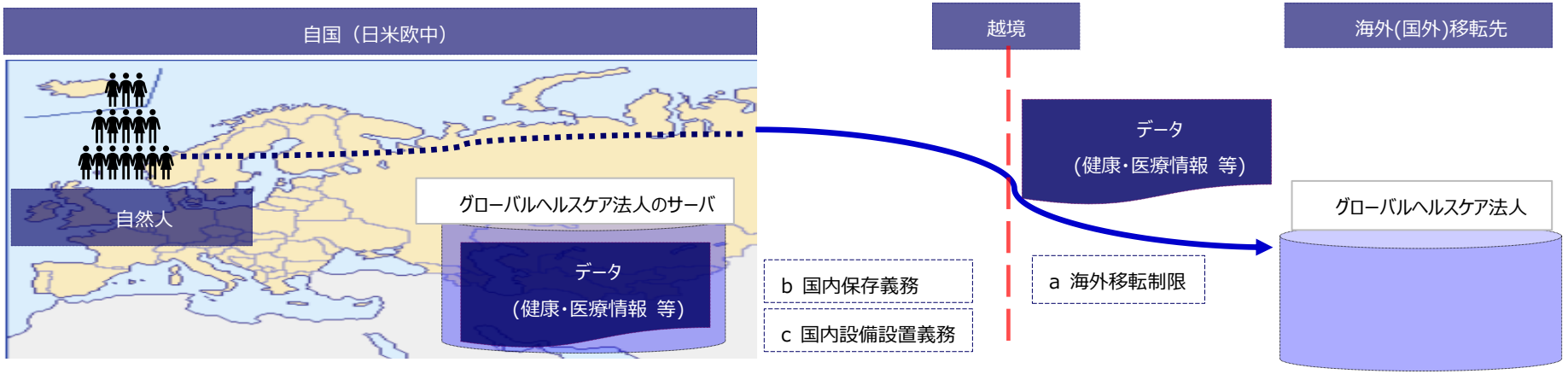
日米欧中4カ国において、国内保存義務又は国内設備設置義務を課す国は中国1カ国、また海外移転制限を課す国は中国の他、日本及び欧州を含めた3カ国である。このことから、海外移転制限及び国内保存義務又は国内設備設置義務の両方の規制を定めている国は中国1か国、一方でデータローカライゼーション規制そのものを定めていない国は、米国1カ国のみであることが分かる。また域外適用については、明確な法規定の有無や適用範囲等異なる点もあるが、4カ国とも採用している。以上の比較の概要をまとめたものが、下記表Ⅰ2.2である。なお、日欧米中におけるデータローカライゼーション規制にまつわる説明は、第Ⅲ部で行う。

図 I 2.1 データローカライゼーション規制：

(1) 国内法人が、自国内に所在するデータ主体からデータを取得し、海外法人へ、データを海外移転する場合：
国内法人が、原則としてデータローカライゼーション規制の対象となる。



(2) 海外法人が、自国内に所在するデータ主体からデータを直接取得し、データを海外移転する場合：
域外適用の制度がある場合、原則として海外法人が、データローカライゼーション規制の対象となる。



表Ⅰ2.2 比較一覧：

制度		日本	欧州	米国	中国
データローカライゼーション規制	国内保存義務 （又は国内設備設置義務）	N/A	N/A	N/A	○
	海外移転制限	○	○	N/A	○
域外適用	―	○	○	○	○

○: 該当, N/A: 非該当

Ⅱ 法制概観

ここではまず日米欧中において、センシティブ情報を定義しその取扱いに対する規制を定めた法令を取り上げ、個人情報保護法制を概観した上で、各国において、健康・医療情報がセンシティブ情報に該当するのか考察する。

1. 日本

1.1 個人情報保護法制

個人情報保護の一般法である個人情報の保護に関する法律（以下、「個人情報保護法」という。）が、整備されており、個人情報保護法にセンシティブ情報である要配慮個人情報の定義及びその取扱いに対する規制が定められている。日本に関しては以下、個人情報保護法を取り上げる。

1.1.1 該当法令

個人情報保護法は、令和3年の法改正により、基本法に当たる第1章乃至第3章、並びに民間部門に適用される第４章「個人情報取扱事業者等の義務等」、及び公部門に適用される第5章「行政機関の義務等」で構成される。[4]個人情報保護法は、2003年に成立し、令和3年の法改正が、直近の改正である。また、2016年には、個人情報の保護に関する法律についてのガイドライン(通則)（以下、「通則」という。）、個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編)（以下、「外国にある第三者への提供編」という。）、個人情報の保護に関する法律についてのガイドライン(第三者提供時の確認・記録義務編)（以下、「第三者提供時の確認・記録義務編」という。）及び、個人情報の保護に関する法律についてのガイドライン(仮名加工情報・匿名加工情報編)（以下、「匿名加工情報・匿名加工情報編」という。）が制定され、適宜改正されている。

1.1.2 目的・法益

個人情報保護法は、個人の権利利益の保護を主目的としている。

個人情報保護法第1条では、「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。」と規定する。

[4] 個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の３法を１本の法律に統合し、公的部門・民間部門における規律が一覧できるようにするとともに、地方公共団体の個人情報保護制度についても統合後の法律において、全国的な共通ルールを規定した。（宇賀克也 「新・個人情報保護法の逐条解説」 有斐閣 2021年12月 P37）。

「個人情報の有用性」とは、公益、他人にとっての有用性だけでなく、個人にとっての有用性も含まれる。「個人の権利利益」とは、個人の人格的な権利利益と財産的な権利利益の双方を含む。「個人の有用性に配慮しつつ、個人の権利利益を保護する」とは、個人の権利利益の保護のみを唯一絶対の目的とするのではなく、個人情報の有用性も斟酌することを意味しているが、両者を対等に比較衡量するのではなく、個人の権利利益の保護が最重要の目的であることを表現している。[5]

1.1.3 適用範囲

個人情報保護法第４章で定める義務等の適用対象は、個人情報保護取扱事業者である。

個人情報保護取扱事業者とは、個人情報データベース等を事業の用に供している者をいう。個人情報データベース等を事業の用に供している者は、個人情報データベース等を構成する個人情報によって識別される特定の個人情報の多寡に関わらず、権利能力のない社団（任意団体）又は個人であっても、個人情報保護取扱事業者に該当する。また「事業の用に供している」の「事業」とは、一定の目的をもって反復継続して遂行される同種の行為であって、且つ社会通念上事業と認められるものをいい、営利・非営利の別は問わず、NPOのような非営利事業を行う者も含まれ得る。なお、個人情報取扱事業者が取り扱う個人情報は、居住地や国籍を問わず個人情報保護法による保護対象となり得るため、外国に居住する外国人の個人情報もその対象となる。但し、別途法令で定める独立行政法人等や地方独立行政法人を除く。

加えて、個人情報保護法は域外適用の規定を設けており、海外に在る事業者であっても、国内にある者に対する物品又は役務の提供に関連して、国内に在る者を本人とする個人情報、当該個人情報として取得されることとなる個人関連情報又は当該個人情報を用いて作成された仮名加工情報若しくは匿名加工情報を、外国において取り扱う場合、同法第4章の一部条項が適用される（同法第75条）。

1.2 定義

1.2.1 個人情報

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、特定の個人を識別することができるもの、又は個人情報の保護に関する法律施行令（以下、「政令」という。）で定めた生体情報を含む個人識別符号を個人情報と定義している（法第2条）。

個人情報保護法第2条第1項では、「この法令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。」と規定の上、同項第1号で、「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

[5] 宇賀克也 「新・個人情報保護法の逐条解説」 有斐閣 2021年12月 P48

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。）」と定めている。

また同条第1項第2号では、「個人識別符号が含まれるもの」と定めている。これを受け本条第2項では、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。」と規定の上、同項第1号は、「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」、同項第2号は、「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」と定めている。

なお、政令第1条は、個人情報保護法第2条第2項の「文字、番号、記号その他の符号」として、下記の通り定めている。

(1) 次に掲げる身体の特徴のいずれか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、特定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するもの
  イ 細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列
  ロ 顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌
  ハ 虹彩の表面の起伏により形成される線状の模様
  ニ 発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化
  ホ 歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様
  ヘ 手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状
  ト 指紋又は掌紋
(2) 旅券法第6条第1項第1号の旅券の番号
(3) 国民年金法第14条に規定する基礎年金番号
(4) 道路交通法第93条第1項第1号の免許証の番号
(5) 住民基本台帳法第7条第13号に規定する住民票コード
(6) 行政手続における特定の個人を識別するための番号の利用等に関する法律第2条第5項に規定する個人番号（マイナンバー）
(7) 次に掲げる証明書にその発行を受ける者ごとに異なるものとなるように記載された個人情報保護委員会規則で定める文字、番号、記号その他の符号
  イ 国民健康保険法第9条第2項の被保険者証
  ロ 高齢者の医療の確保に関する法律第54条第3項の被保険者証
  ハ 介護保険法第12条第3項の被保険者証
(8) その他前各号に準ずるものとして個人情報保護委員会規則で定める文字、番号、記号その他の符号

このように静脈形状等生体情報の個人識別符号や、マイナンバー等公的機関発行の個人識別符号も個人情報に該当するが、一方オンライン識別子等の識別非特定情報は含まないという特色がある。

なお、日本法令外国語訳DBシステムでは、個人情報保護法第2条第1項を、“The term "personal information" as used in this Act shall mean information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).”と訳している。このことより日本の個人情報保護法では、「その情報が、特定の個人を識別可能な性質」か、即ち「その情報が、誰かが分かる情報である」かどうかという観点より、個人情報の該当性を判断するものと考えられる。

1.2.2 センシティブ情報[6]

個人情報保護法第2条第3項では、要配慮個人情報を「本人の人種、信条、社会的身分、病歴、 犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。」と定義している。

ここでいう「病歴」とは、病気に罹患した経歴を意味するもので、特定の病歴を示した部分（例：特定の個人が癌に罹患している、統合失調症を患っている等）が該当する（通則2-8）。

「政令で定める記述等」については、政令第2条で下記の通り列挙している。

(1) 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員 会規則で定める心身の機能の障害があること。
(2) 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の結果
(3) 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。
(4) 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。
(5) 本人を少年法第3条第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。

上記(2)について、通則は、「疾病の予防や早期発見を目的として行われた健康診査、健康診断、特定健康診査、 健康測定、ストレスチェック、遺伝子検査等、 受診者本人の健康状態が判明する検査の結果が該当する。」としている。

その上で、要配慮個人情報に該当する具体的な事例として、以下を挙げている。

① 労働安全衛生法（以下、「安衛法」という。）に基づいて行われた健康診断の結果、同法に基づいて行われたストレスチェックの結果、高齢者の医療の確保に関する法律に基づいて行われた特定健康診査の結果等

[6] 宇賀克也「新・個人情報保護法の逐条解説」 有斐閣 2021年12月 P50～P52

② 法律に定められた健康診査の結果等に限定されるものではなく、人間ドックなど保険者や事業主が任意で実施又は助成する検査の結果
③ 医療機関を介さないで行われた遺伝子検査により得られた本人の遺伝型とその遺伝型の疾患へのかかりやすさに該当する結果等

併せて要配慮個人情報に該当しない具体的な事例として、以下も挙げている。
① 健康診断等を受診したという事実
② 身長、体重、血圧、脈拍、体温等の個人の健康に関する情報を、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

上記(3)について、通則2-3は、次の通り補足説明を加えている。
「健康診断等の結果に基づき、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が行われたこと」については、「健康診断等の結果、特に健康の保持に努める必要がある者に対し、医師又は保健師が行う保健指導等の内容が該当する。」とし、指導が行われたこととして、下記を挙げている。
① 安衛法に基づき、医師又は保健師により行われた保健指導の内容、及び医師により行われた面接指導内容
② 高齢者の医療の確保に関する法律に基づき医師、保健師、管理栄養士により行われた特定保健指導の内容等
③ 法律に定められた保健指導の内容に限定されるものではなく、保険者や事業主が任意で実施又は助成により受診した保健指導の内容も該当する。なお、保健指導等を受けたという事実

また、「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診療が行われたこと」については、「病院、診療所、その他の医療を提供する施設において診療の過程で、患者の身体の状況、病状、治療状況等について、医師、歯科医師、薬剤師、看護師その他の医療従事者が知り得た情報全てを指す。」とし、次のような例を挙げている。
① 診療記録等
② 病院等を受診したという事実

更に「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調剤が行われたこと」については、病院、診療所、薬局、その他の医療を提供する施設において調剤の過程で患者の身体の状況、病状、治療状況等について、薬剤師（医師又は歯科医師が自己の処方箋により自ら調剤する場合を含む。）が知り得た情報全てを指す。」とし、例として下記を挙げている。
① 調剤録、薬剤服用歴、お薬手帳に記載された情報等
② 薬局等で調剤を受けたという事実

なお、非該当となる事例として、ここでも「身長、体重、血圧、脈拍、体温等の個人の健康に関する情報を、健康診断、診療等の事業及びそれに関する業務とは関係のない方法により知り得た場合」を挙げている。

上述の通り、要配慮個人情報は、医療従事者によるといった医行為の過程で行われる診断・検査その他結果、及びその結果に基づき指導、診療又は調剤等が行われた事実が該当するため、医療情報は要配慮個人情報に該当し、一方で健康情報はそれに該当しない、といえる。

2. EU[7]

2.1 個人情報保護法制

EEA（European Economic Area．欧州経済領域）域内に適用される統一的な個人情報保護の一般法として、「個人データの取扱いと関連する自然人の保護に関する、及びそのデータの自由な移転に関する、並びに指令95/46/EC を廃止する欧州議会及び理事会の2016年4月27日の規則(EU) 2016/679 (一般データ保護規則)（REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [8]を以下、「GDPR」という。）が整備されており、GDPRにセンシティブ情報に関する定義がなされている。

なお、英国では、EUからの離脱の移行期間終了時、GDPRを英国版「UK GDPR」[9]に変換の上、GDPRに基づいて制定された国内法であるData Protection Act of 2018[10]と共に同国の個人情報保護法制を構成している[11]。

本稿では、EUの個人情報保護法制としてGDPRを取り上げる。

2.1.1 該当法令

GDPRは、173項の前文と99条の条文で成り立ち、主に条文の第2章乃至第5章（第5条乃至第50条）で順守すべき具体的なルールを規定し、各種ガイドラインでそれらルールを補足し詳細を定めている。また、GDPRはEEA域内各国に直接適用される一方、加盟国の裁量にも配慮した構成になっている。

2.1.2 目的・法益

GDPRは、自然人の個人データ保護の権利、及び個人データのEU域内での自由な移動を保護することを目的としている（GDPR第１章第１条）。

なおGDPR前文では、欧州連合基本権憲章及び欧州連合の機能に関する条約[12]を引用し、個人データ保護が基本的人権であることを謳っている（GDPR前文(1)）。一方で、個人データ保護の権利は絶対的な権利ではなく、社会におけるその機能との関係において判断されなければならず、且つ他

---

[7] EU加盟国並びにEEAの一部であるアイスランド、ノルウェー及びリヒテンシュタイン（以下同様）。

[8] EUR-LEX（https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1683624465297）

[9] https://www.legislation.gov.uk/eur/2016/679/contents

[10] https://www.legislation.gov.uk/ukpga/2018/12/contents

[11] 岩村浩幸「欧州・英国データ保護法制の現状整理と今後の展望」ビジネス法務 2021年7月号 P118

[12] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Art. 16, 2010/C83/01 of 30 March 2010, O.J.（C83）1, ***55.*** and Charter of Fundamental Rights of the European Union, Art. 8, 2010/C83/02 of 30 March 2010, O.J. (C83) 389, 393.
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ%3AC%3A2010%3A083%3ATOC

の基本的な権利とバランスのとれたものでなければならないことについても併せて言及している（GDPR前文(4)）。

2.1.3 適用範囲

個人データの取扱いが、EU域内で行われるか否かを問わず、EU域内のデータ管理者[13]又はデータ処理者[14]の拠点の活動の過程における個人データの取扱いに適用される。

併せて、GDPRは域外適用の規定を設けており、(a)EU域内のデータ主体へ商品若しくはサービスを提供する場合、又は(b)EU域内のデータ主体の活動を監視する場合には、EU域内に拠点の無い管理者又は処理者によるEU域内のデータ主体の個人データの取扱いにも適用される（GDPR第3条「地理的範囲」）。

「EU域内で行われるか否かを問わず」について補足すると、個人データの取扱場所は、GDPRの適否に影響を与えない。地理的位置は、個人データの管理者又は取扱者自身（EU域内の設立か否か）、EU域外の管理者又は取扱者の事業が実在すること（EU域内に事業所を有するか否か）との関係では重要であるが、取扱場所やデータ主体の位置との関係では重要でない。

2.2 定義

2.2.1 個人情報[15]

「個人データ」とは、識別された自然人又は識別可能な自然人（「データ主体」）に関する情報を意味する。識別可能な自然人とは、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、識別されうる者をいい（GDPR第4条1項）、例えば、IP アドレス、電子メールアドレス、または電話番号も含まれ得る。[16]

ある自然人が識別可能であるかどうかを判断するためには、「選別のような、自然人を直接又は間接に識別するために管理者又はそれ以外の者によって用いられる合理的な可能性のある全ての手段を考慮に入れなければならない」（GDPR前文26項）とした上で、「自然人は、インターネットプロトコルアドレス、クッキー識別子、又は、無線識別タグのようなその他の識別子といったような、当該自然人のデバイス、アプリケーション、ツール及びプロトコルによって提供されるオンライン識別子と関連付けられうる。これは、特にサーバによって受信されるユニーク識別子及びその他の情報と組み合わされるときは、自然人

[13] 自然人又は法人、公的機関、部局又はそのほかの組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者を意味する（GDPR第4条(7)項）。

[14] 管理者の代わりに個人データを取扱う自然人若しくは法人、公的機関、部局又はその他の組織を意味する（GDPR第4条(7)項）。

[15] 個人情報保護委員会Webサイト上に掲載されているGDPR前文及び条文の翻訳で、Personal Dataを個人データと訳されていることより、本稿もまた同様に表記。（https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/）。

[16] ㈱ITリサーチ・アート「EU 各国における個人情報保護制度に関する調査研究報告書」平成30年3月29日 P7（https://www.soumu.go.jp/main_content/000545719.pdf）

のプロファイルをつくり出し、そして自然人を識別するために用いられうる痕跡を残しうるものである。」と規定している。（GDPR前文第30条）

なお、GDPR第4条第1項では、"'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" と規定している。このように同法では、個人データ[17]を、識別された自然人又は識別可能な自然人に関する情報とし、識別可能な自然人とは、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、識別されうる者と定めている。

併せて、前文第26項では、 "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." と規定している。このようにデータ保護の基本原則は、識別された自然人又は識別可能な自然人に関する全ての情報に対して適用するとした上で、ある自然人が識別可能であるかどうかを判断するためには、選別のような、自然人を直接又は間接に識別するために管理者又はそれ以外の者によって用いられる合理的な可能性のある全ての手段を考慮に入れるべきとしている。

その上で、GDPR前文第30項では、"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."と規定している。このように前文では、自然人は、オンライン識別子と関連付けられうること、特に、サーバによって受信されるユニーク識別子及びその他の情報と組み合わされるときは、自然人のプロファイルをつくり出し、そして、自然人を識別するために用いられうる痕跡を残しうるものであるとしている

このように同法では、「識別可能な個人」に関する情報か、という「個人の識別可能性」の観点より、個人データの該当性を判断するものと考えられる。[18]その識別可能性の判断にあたり、不特定多数の個人の中からある1人を選別するような手段が用いられることを考慮に入れるべきことを示した上で、個人へユニークに割り当てられるような識別子は、個人に関連付けられ、個人を識別するものと同法の前文で記述していることから、同法では、氏名や顔写真といった、誰であるかが分かる性質の情報のみならず、クッキー識別子等オンライン識別子のような1人を選別する手段に用いられる、個人に関連付けられる情報もまた個人データと位置付けられるものと考えられる。

[17] 個人情報保護委員会Webサイト上に掲載されているGDPR前文・本文の仮翻訳で、Personal Dataを個人データと訳していることに合わせ個人データと記述。 https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

[18] 浅井 敏雄「GDPR 関連資格 CIPP/E 準拠 詳説GDPR (上) - GDPRとCookie規制」UniServ Publishing P145-150

2.2.2 センシティブ情報[19]

GDPR第9条は、特別な種類の個人データの取扱いについて、「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される」と規定し、同条に掲げるデータがセンシティブ情報であることを規定している。

ここでいう「健康に関するデータ」とは、GDPR第4条15項で、「医療サービスの提供を含め、健康状態に関する情報を明らかにする、自然人の身体的又は精神的な健康と関連する個人データを意味する。」としている。また、GDPR前文第35項で、「データ主体の健康状態と関係のあるデータであって、データ主体の過去、現在及び未来の身体状態又は精神状態に関する情報を明らかにする全てのデータを含む。」とされ、このデータは、欧州議会及び理事会の指令2011/24/EU9に定める医療サービスのための当該自然人の登録過程において、又はその医療サービスの当該自然に対する提供の過程において収集されるその自然人に関する情報（医療上の目的で自然人をユニークに識別するために自然人に対して特別に割り当てられた番号、シンボル又は項目）、遺伝子データ及び生化学的資料を含め、身体の一部又は身体組成物の試験若しくは検査から生じる情報、並びに医師その他の医療専門職、病院、医療機器又は体外臨床検査のような当該情報の情報源の別を問わず、例えば、データ主体の疾病、障害、疾病リスク、病歴、診療治療、生理学的状態又は生物医学的状態を示す全ての情報を含む。」と説明している。[20]

[19] GDPR第9条は、センシティブ情報を “Special categories of personal data” と規定している。個人情報保護委員会Webサイト上に掲載されているGDPRの翻訳では、これを「特別な種類の個人データ」と訳していることより、本稿もまた同様に表記。

[20] EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62020CJ0184&from=en
（22年8月、欧州裁判所は、類推等のデータ処理により、特別な種類の個人データを導き得るのであれば、その処理は、GDPR第9条で定める取扱いに該当し得るとの判断を下している。そのため例えば、健康管理サービスのアルゴリズムを用いて、何らかの症候群・疾病等の兆候がある等、健康情報・状態を類推し得るのであれば、その情報もまた特別な種類の個人データであると考えられる。）

3. 米国

3.1 個人情報保護法制[21]

米国において、連邦法は州際に亘る事項を規定し、州法は州内の事項を規定している。

連邦法においては、公的部門及び民間部門を包括的に規制する個人情報保護法制は制定されておらず[22]、分野毎に個別法を制定するセクトラル方式が採用されている。併せて個別分野における規律として、FTCレポートや民間での自主規制も重要な役割を果たしている。なお、連邦法として、包括的なプライバシー保護法の制定に向けた動きがある。

一方、州法においては、カリフォルニア州に続き、バージニア州及びコロラド州において、包括的な個人情報保護法が制定されている。それ以外の州においても、プライバシー保護の関連法に関して、立法手続中又は法案作成中である州も少なくない。なお、個人情報漏洩等のセキュリティ侵害に関する消費者等への通知義務を定めた法律については、2002年カリフォルニア州が制定したのを皮切りに50全ての州及びワシントンD.C.において制定されている。

このように個人情報保護を規定する法令が多岐に亘ることから、下記表の通り予め、民間に適用され得る主な法令をまとめた上、その中から本稿で、どの法令を取り上げるのかを整理する。

（1）個人情報保護に関する規定を含む主な連邦法

日本で特定分野としてガイドライン・ガイダンスを定めている医療分野、情報通信分野及び金融分野に関して、米国では個別法で個人情報保護を規定していることがうかがえる。そこで、連邦法として民間部門に適用される主だった法令、及びそれら法令が適用される分野・対象について、表Ⅱ3.1.1(1)の通り整理した。その中から本稿では、医療分野に適用される法令である1)、5)及び8)について取り上げることとする。

[21] 米国の個人情報・プライバシー保護のための制定法や連邦取引委員会のプライバシー保護政策は、「公正な情報取扱慣行に関する原則」“Fair Information Practice Principles: FIPPs”を基礎として構築されている。（松前恵環「米国の法制度の概要と近時の議論動向」NBL No.1185(2021.1.1)号 P81）

[22] 包括的な連邦法を制定する動きはある。2019年合衆国消費者データプライバシー法(USCDPA)や消費者オンラインプライバシー権法(COPRA)等の法案が、過去議会に提出されている。（松前恵環「米国の法制度の概要と近時の議論動向」NBL No.11852021.1.1)号 P84-P85）

表Ⅱ3.1.1 (1) 連邦法として民間部門に適用され得る主な法令（時系列順）

	制定年	名称	分野・対象
1)	1914年	Federal Trade Commission Act of 1914[23]，FTC法（連邦取引委員会法）	原則、全分野
2)	1934年	Communications Act of 1934[24]（連邦通信法）	通信（対象:電気通信事業者）
3)	1986年	Electronic Communications Privacy Act of 1986[25], ECPA（電子通信プライバシー法）	通信
4)	1988年	Video Privacy Protection Act of 1988[26]，VPPA（1988年ビデオ・プライバシー保護法）	ビデオレンタル・購入記録
5)	1996年	Health Insurance Portability and Accountability Act of 1996，HIPAA[27]（医療保険の携行性と責任に関する法律）	医療
6)	1998年	Children's Online Privacy Protection Act of 1998[28], COPPA（児童オンラインプライバシー保護法）	児童
7)	1999年	Gramm-Leach-Bliley Act[29]，GLBA（グラム・リーチ・ブライリー法）	金融
8)	2009年	Health Information Technology for Economic and Clinical Health Act of 2009[30]，HITECH Act（経済的及び臨床的健全性のための医療情報技術に関する法律）	医療

[23] https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act
[24] https://www.govinfo.gov/app/details/COMPS-936
[25] https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848
[26] https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap121-sec2710/summary
[27] https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
[28] https://www.govinfo.gov/app/details/USCODE-2011-title15/USCODE-2011-title15-chap91-sec6501/context
[29] https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
[30] https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html#:~:text=The%20Health%20Information%20Technology%20for,use%20of%20health%20information%20technology.

（2）州法として包括的な個人情報保護を定めた州法（時系列順）

カリフォルニア州での制定を皮切りに下記表3.1.1(2)の通り、近年制定が続いている。本稿では、同表の1)-1及び1)-2について取り上げることとする。

表Ⅱ3.1.1 (2) 州法として包括的な個人情報保護を規定した主な法令（時系列順）

	可決・成立年月	名称	州
1)-1	2018年6月 （2020年1月施行）	California Consumer Privacy Act of 2018[31], CCPA （カリフォルニア州消費者プライバシー法）	カリフォルニア州
1)-2	2020年11月 （2023年1月施行）	California Privacy Rights Act of 2020[32], CPRA （カリフォルニア州プライバシー権法）	同上
2)	2021年３月 （2023年1月施行）	Consumer Data Protection Act[33], CDPA	バージニア州
3)	2021年７月 （2023年7月施行）	Colorado Privacy Act[34], CPA	コロラド州
4)	2022年3月 （2023年12月施行）	Utah Consumer Privacy Act[35]	ユタ州
5)	2022年5月 （2023年7月施行）	An Act Concerning Personal Data Privacy and Online Monitoring[36]	コネチカット州
6)	2023年3月 （2025年1月施行）	ACT RELATING TO CONSUMER DATA PROTECTION, PROVIDING CIVIL PENALTIES, AND INCLUDING EFFECTIVE DATE PROVISIONS[37]	アイオワ州
7)	2023年5月 （2025年7月施行）	Tennessee Information Protection Act[38]	テネシー州
8)	2023年5月 （2024年10月施行）	Montana Consumer Data Privacy Act	モンタナ州

[31] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100.

[32] https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

[33] https://legiscan.com/VA/text/SB1392/id/2328317

[34] https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

[35] https://le.utah.gov/~2022/bills/static/SB0227.html

[36] https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF

[37] https://www.legis.iowa.gov/legislation/BillBook?ba=SF%20262&ga=90

[38] https://legiscan.com/TN/text/SB0073/2023

（3）連邦法としての包括的な個人情報保護法案（時系列順）

共和党と民主党の両党から以下の通り、法案が提出・公開されているが、現時点で民主党案である下記1)または6)が制定される可能性が高いとみられ、またいずれも執行部門をFTC法の所管機関であるFTCとしていることから、法案ではあるが、本稿では下記1)乃至6)の法案から、現行制定法と併せて1)及び6)を取り上げることとする。

表Ⅱ3.1.1 (3) 連邦法としての包括的な個人情報保護法案（時系列順）

	公表等時期	名称	党派
1)	2019年11月	Consumer Online Privacy Rights Act，COPRA（消費者オンラインプライバシー権法）	民主党議員
2)	2019年	United States Consumer Data Privacy Act，USCDPA（合衆国消費者データプライバシー法）	共和党議員
3)	2020年3月	Consumer Data Privacy and Security Act，CDPSA（USCDPAの改訂草案）	共和党議員
4)	2020年6月	Data Accountability and Transparency Act[39]	民主党
5)	2020年9月	Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act: SDA)	共和党議員
6)	2022年6月	the American Data Privacy and Protection Act	超党派議員

3.1.1 該当法令

米国の個人情報・プライバシー保護のための制定法やFederal Trade Commission（連邦取引委員会。以下「FTC」という。）のプライバシー保護政策は、「公正な情報取扱慣行に関する原則」を基礎として構築されている。

まず、連邦法としては、FTCが制定した、不公正若しくは欺瞞的な行為又は慣行[40]を規制するFederal Trade Commission Act of 1914（連邦取引委員会法。以下、「FTC法」という。）が、顧客へのプライバシー及びセキュリティの保護に広く適用される。

[39] 顔認証技術使用や人種差別的利用の禁止、所管省庁新設等独自規定を含む（Scott W. Pink，座波優子「民主党案・共和党案を比較 米国包括的個人情報保護法制定の動向」ビジネス法務 2020年10月号 P4-P5）

[40] ある行為又は慣行が不公正であるとする要件として、①消費者への実質的な損害があること、③対抗利益が当該損害を上回らないこと、及び③当該損害が、消費者により合理的に回避できないこと、の3つに基づき判断されているとされる。また、ある行為又は慣行が欺瞞的であるとする要件として、①消費者を誤解させる可能性のある虚偽、不作為その他の慣行であること、②ある行為又は慣行の解釈は、合理的な消費者の見地からなされること、及び③当該虚偽、不作為その他の慣行が、重要なものであることが必要であるとされる。（松前恵環「米国における個人情報・プライバシー保護監督機関－FTCを中心に」NBL No.1201(2021.9.1)号 P90-P91）

FTCは、FTC法第5条「不公正若しくは欺瞞的な行為又は慣行」[41]に基づき、欺瞞的取引を規制する権限を有しており、この権限をプライバシー保護のために活用し、FTCは、企業が公表しているプライバシー保護の内容と、企業による実際の個人情報の取扱いの間に齟齬がある場合、欺瞞的な取引に該当する、としている。

また、医療保健分野の個別法としては、Health Insurance Portability and Accountability Act of 1996（「1996年医療保険の相互運用と説明責任に関する法律。以下、「HIPAA」という。）が制定されている。[42]HIPAAは、Department of Health and Human Service（米国保健福祉省。以下、「HHS」という。）の長官に対し、健康情報のプライバシー及びセキュリティ保護する具体的な規則の制定を求めている。これに基づき、HHSが、Standards for Privacy of Individually Identifiable Health Information, Privacy Rule（個人識別可能な健康情報のプライバシーに関する規則。以下、「HIPAAプライバシー規則」という。）及び、Security Standards for the Protection of Electronic Protected Health Information, Security Rule（電子的な健康情報の保護のためのセキュリティに関する基準。以下、「HIPAAセキュリティ規則」という。）を定めている。[43]

同じく医療保健分野として、HIPAAプライバシー規則及びHIPAAセキュリティ規則を補足する“Health Information Technology for Economic and Clinical Health Act of 2009（2009年　経済的及び臨床的健全性のための医療情報技術に関する法律。以下、「HITECH」という。）も制定されている。HITECHは、医療情報技術の導入や相互運用性の促進を目指すものであるが、その13編のサブタイトルD「プライバシー」で、HIPAAによって定められたプライバシー及びセキュリティ保護のためのルールを強化する規定を置いている。これを受け、HHSは、2013年にHIPAAプライバシー規則とHIPAAセキュリティ規則等を改正する最終規則を公表している（以下、HIPAA、HIPAAプライバイシー規則、HIPAAセキュリティ規則及びHITECを総称し、「HIPAA等」という。）。

上述の他、民間部門に適用され得る個人情報保護を規定した連邦法としては、個人のビデオレンタル記録・購入記録の保護を目的としたVideo Privacy Protection Act of 1988（1988年ビデオ・プライバシー保護法。以下、「VPPA」という。）、児童（13才未満）のプライバシー保護を目的とするChildren’s Online Privacy Protection Act of 1998（児童オンラインプライバシー法。以下、「COPPA」という。）、電子通信のプライバシー保護を目的とするElectronic Communications Privacy Act of 1986（電子通信プライバシー法。以下「ECPA」という。）が挙げられる。

次に州法としては、カリフォルニア州で、2018年6月にCalifornia Consumer Privacy Act of 2018（2018年カリフォルニア消費者プライバシー法。以下、「CCPA」という。）が成立し、2020年1月から施行されている。更に2020年11月にCCPAを改正し、消費者の権利拡大や、カルフォルニア州プライバシー保護局の設立等を規定するCalifornia Privacy Rights Act of 2020（2020年カリフォルニア州プライバシー権法。以下、「CPRA」という。）に関する提案「プロポジション24」が住民投票に

[41] https://www.govinfo.gov/app/details/USCODE-2011-title15/USCODE-2011-title15-chap2-subchapI-sec45a/context

[42] HIPAAと州法の関係として、州法がHIPAAと矛盾する場合、HIPAAの規則が専占するが、州法の規定が特定の目的のために必要又は規則よりも厳格な規定であるといった事由に該当するとHHSが判断したときは、州法の優先が認められている。（松前恵環「米国の法制度の概要と近時の議論動向」NBL No.1185(2021.1)号 P82）

[43] https://www.govinfo.gov/app/details/CFR-2009-title45-vol1/CFR-2009-title45-vol1-sec164-500/summary
https://www.govinfo.gov/app/details/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-302/context

より可決され、2023年1月から施行されている。CPRAは、CCPAで定めていなかったセンシティブデータについて定義している。

また、バージニア州では2021年3月に「Consumer Data Protection Act」が成立し、2023年1月から施行予定、またコロラド州では2021年7月に「Colorado Privacy Act」が成立し、2023年7月施行予定である。[44]

なお、前述の通り、連邦法として、包括的なプライバシー保護法の制定の動きがある。2019年、民主党議員からConsumer Online Privacy Rights Act（以下、「COPRA」という。）、共和党議員からUnited States Consumer Data Privacy Act（以下、「USCDPA」という。）、また翌年には、共和党議員からCDPAの改訂草案としてConsumer Data Privacy and Security Act（以下、「CDPSA」という。）が法案化されている。更に2022年6月the American Data Privacy and Protection Act（以下、「ADPPA」という。）が、連邦議会超党派議員により公表されている。[45]米国連邦としてのデータプライバシー法案の立法化は、ADPPA又はCOPRAが現状有力候補であると考えられ、その枠組みが維持され立法化される可能性はあり得る。

本稿では、一般消費者及びユーザーのプライバシー保護の観点から規制がなされ得る連邦法としてFTC法、医療・保健分野でのプライバシー保護を定めたHIPAA/HITEC、及び州法ではあるが包括的な個人情報保護法の先駆けとなったカリフォルニア州の法制、並びに未だ法案ではあるがFTC法と同じくFTCが執行機関であり、立法化の可能性が高く且つセンシティブデータの定義も規定していることから、前述の通り併せて、COPRA及びADPPAについて取り上げることとする。[46]

3.1.2 目的・法益

米国における個人情報・プライバシー保護のための制定法は、基本的にプライバシーの権利保護を目的に捉えているものと解される。その制定法であるVPPA、COPPA、ECPA、HIPAA/HIPAAプライバシー規則、CCPA若しくはCPRA、又は法案ではあるがCOPRA、CDPA若しくはCDPSAの法令名称をみてみると、そこには“Privacy”が含まれていること、また、例えば連邦の行政機関の個人情報に関する1974年プライバシー法に関する「議会の認識及び目的の宣言」では、「プライバシーの権利は、合衆国憲法によって保障される個人的且つ基本的な権利である」とした上で、「個人のプライバシーの侵害に対して、個人に一定の保護措置を提供することを目的とする。」と述べられている他、ECPAに関する議会の認識においても、「有線通信及び口頭の会話に関する個人のプライバシーを保護する必要性が示唆されている」等、日本の個人情報保護法が保護法益を「個人の権利利益」と掲げるにとどめその明示を避けた「プライバシー」への言及が、米国のそれら制定法には随所にみられることからも、そのように解され

---

[44] 経産省「データの越境移転に関する研究会報告書 2022年2月28日」P21
（https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_2.pdf）

[45] ADPPAは、法案ではあるが制定の可能性が高いとみられ、また米国国家としてのプライバシー保護についての考え方や国家戦略が垣間見えるため、今回取り上げることとするが、あくまで現時点での法案を基に記述することとし、制定後改めて検証する。ADPPAは以降、塗本麻佑子、長谷川紘「連邦プライバシー法案の公表」長島・大野・常松法律事務所 2020年9月
（https://www.noandt.com/publications/publication20220901-1/）、及び石川智也、河合優子、大竹祥太、佐々木将也、小出章広、水谷有希、久保慶太郎、平岡咲耶「米国個人情報保護法最新動向」（西村あさひ法律事務所 個人情報保護・データ保護規制ニューズレター 2022年9月6日～11月25日を参照する。

[46] COPRAは、ADPPA同様、法案ではあるが制定の可能性が高いとみられ、また米国国家としてのプライバシー保護についての考え方や国家戦略が垣間見えるため、今回取り上げることとするが、あくまで現時点での法案を基に記述することとし、制定後改めて検証する。

る。[47] なお、FTC法は、第５条(a)で、不公正な競争方法、及び不公正若しくは欺瞞的な行為又は慣行を禁止している。FTCは本条を企業のプライバシー及びセキュリティデータ保護ポリシーを規制するために用いており、“不公正若しくは欺瞞的な行為又は慣行”として、消費者のプライバシー侵害も含まれるとされていることから、消費者のプライバシー保護も目的としているといえる。またHIPAAは、その前文で①団体及び個人の市場における医療保険の補償範囲の携行性及び継続性を改善すること、②医療保険及び医療供給の浪費、詐欺及び濫用に対抗すること、③医療貯蓄口座の利用を促進すること、④長期のケアサービスへのアクセス及びその保障範囲を改善すること、⑤医療保険の運営をシンプルなものにすること等を目的とすると述べているが、上述の通りHIPAAプライバシー規則より、プライバシー保護もまた目的としているといえる。

3.1.3 適用範囲

法令毎に適用範囲が異なる。

FTC法では、原則として、アメリカ合衆国内の全ての企業に対して適用される。[48]FTCは、2010年公表の報告書で、保護対象となる消費者の個人情報一般についての基準を提示し、プライバシー保護のためのフレームワークは、「特定の消費者、コンピューターその他のデバイスに合理的に結び付けられ得る消費者のデータを収集又は利用する全ての事業者に適用される。」としている。また明文規定はないが、アメリカ合衆国内の商業に影響を与える場合、域外適用が可能である。[49]

HIPAA/HIPAAプライバシー規則では、医療機関及び医療供給者に対して適用され、これら適用対象となる組織体（Covered entities）には、①保健計画（Health plans．医療サービスを提供する又はその支払いを行う、個人又は集団の計画であり、従業員福利厚生計画、健康保険業者等を含む。）、②保健医療クリアリングハウス（Health care clearinghouses．標準化されていない健康情報を受領してその標準化を行い、他の組織等に提供する又はその逆を行う、公的又は私的な組織）、③HHSが採用した基準の対象となる処理に関連して全ての医療情報を電子送信する保健医療提供者（Health care providers．保健医療サービスの提供者、及び通常の事業活動において保健医療の提供、宣伝、若しくは支払いを行うあらゆる人又は組織）が含まれる。またHITECによって、HIPAAの直接的な適用範囲に協力事業者（Business associates．対象組織との契約に基づいてProtected health information（以下、「PHI」という。）の利用又は開示等を含む活動を行う者・事業提携者。）を追加している。[50]

CCPAでは、次の２つの条件を満たす営利目的の事業者に限定される。

① 条件1：カリフォルニア州の住民の個人情報を収集(又は代理で収集)し、単独又は他者と合同で、消費者の個人情報の取扱いの目的及び手段を決定し、カリフォルニア州で事業を営む
② 条件2：以下のa)b)c)いずれかを充足すること

---

[47] 石井夏生利・曽我部真裕・森亮二「個人情報保護法コンメンタール」勁草書房 2021年2月 P11-P12、松前恵環「米国の法制度の基底をなす思想とプライバシーの権利」NBL No.1187(2021.2.1)号 P8

[48] 渥美坂井法律事務所・外国法共同事業「諸外国の個人情報保護制度に係る最新の動向に関する調査研究報告書」平成30年3月 P13（https://www.ppc.go.jp/files/pdf/201803_shogaikoku.pdf）

[49] FTCその他のアメリカの規制機関は、プライバシー及びデータセキュリティに関するアメリカの法令・規則は、アメリカ国外に移転されたデータにも適用されるという立場をとっているといわれている。（同上 P15）

[50] 同上 P20、石井夏生利・曽我部真裕・森亮二「個人情報保護法コンメンタール」2021年2月 P80

a）年間総売上高が2,500万ドルを超えていること
b）1年当たり、併せて５万件以上の消費者、世帯、物理的なデバイスの同州の住民の個人情報を、購入、商業目的で受領、又は販売していること
c）年間売上高の50%以上を同州の住民の個人情報の販売から得ていること

上記b)について補足すると、５万件は一見高いようにみえるが、個人情報の定義が比較的広いため、容易に達成する可能性が指摘されている。具体的には、カリフォルニア州から５万人以上の訪問者がいるWebsiteでは、通常IPアドレスを取得していることから、本項を充足しないかどうかの検討の必要性が指摘されている。また、b)及びc)の「販売」とは、「金銭又はその他の有価物としを対価として、売却、賃借、公表、開示、流布、提供、譲渡又は口頭・書面・電子的手段その他の手段により伝達すること」を指すため、データベースビジネスのみならず、有償或いは取引の一環として、情報を開示する場合を広く含む。同州の住民は、①一時的又はトランジット目的以外で、同州に所在する全ての人（国籍不問）、及び②一時的又はトランジット目的で州外に所在する、州の居住者を含む。

また、同州に拠点を有しない事業者が、カリフォルニア州の住民をターゲットにサービスを提供する場合でも、カリフォルニア州で事業を行っていないことが明白でない限り、CCPAが適用される可能性は否定できない。少なくとも、米国内に拠点を有する事業者については、同州の顧客から収益を上げている限り、同州内で事業を行っていることを否定するのは難しいと指摘されている。なお、対象事業者の関係会社・グループ会社であっても、下記(ｉ)と(ｉｉ)のいずれも満たす場合は、CCPAが適用されるため、例えば同州に子会社を有する米国国外に所在する親会社は、適用対象となる可能性があり、これによりCCPAは域外適用が可能であるといえる。[51]

（i）CCPAが適用される事業者を支配し、又はこれに支配される事業者であって、
（ii）共通ブランドを有する事業者

CPRAでは、上述したCCPAの条件2のb)及びc)が、下記の通り一部修正された。

b）1年当たり、併せて“10”万件以上の消費者、世帯、物理的なデバイスの同州の住民の個人情報を、購入、商業目的で受領、販売、又は“共有”していること
c）年間売上高の50%以上を同州の住民の個人情報の販売又は“共有”から得ていること

併せて、上記（i）及び（ii）に加えて、（iii）当該事業者と個人情報を共有している、という条件が追加された。

更にCPRAでは、上述以外にも、下記の通り適用対象となる要件が2つ新設された。1つは、対象事業者が40%以上の持分を有するジョイントベンチャー又はパートナーシップ、もう1つは、CPRAを順守し、その拘束を受ける旨の証明書をカリフォルニア州プライバシー保護局に提出したカリフォルニア州の企業、がその要件である。[52]

---

[51] 中崎 尚「実務解説 GDPR対応済み企業も要注意 米国カリフォルニア州消費者プライバシー法への対応」ビジネス法務 2019年12月号 P110、小野 順平「カリフォルニア州消費者プライバシー法と日本企業における実務対応」国際商事法務 Vol.47 No.12(2019年) P1516、浅井 敏雄「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第54回 カリフォルニア州消費者プライバシー法の成立とその概要」国際商事法務 Vol.46 No.8(2018年) P1119、及び「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第77回 カリフォルニア州消費者プライバシー法（CCPA）の論点」国際商事法務 Vol.48 No.8(2020年) P1118-P1121

[52] 井上 乾介「カリフォルニア州プライバシー権法（CPRA）の概要－「機微情報」,「共有」規制の新設ほか」ビジネス法務 2021年6月号 P115-P117

なお、CCPAは、医療情報又は金融情報の中、既存の規制でカバーされている範囲には適用されない。例えば、医療情報であれば、CMIA（カリフォルニア医療情報秘匿法）の対象となる医療情報、又はHIPAA/HITEC対象のPHIに関しては、CCPAは適用されず、CMIA又はHIPAAが適用されることとなる。

COPRAでは、①FTC法の適用対象であり、且つ②COPRAの適用対象となるデータを処理又は譲渡する事業者又は個人に適用される。また対象事業者が米国内で設立されたかどうかは問わず、例えば、外国で設立された事業者であっても、米国在住の個人に対して、商品又はサービスを提供する場合、若しくは米国在住の個人からCOPRAの適用対象となるデータを収集している場合には適用され得る。なお、①対象事業者を支配し、②対象事業者に支配され、③対象事業者と共通支配下にあり、又は④共通ブランド（共通名称、サービスマーク、又は商標）を共有する事業者又は個人も含まれる。但し、小規模事業者は除外されるが、その基準は、過去3年間、（i）年間平均総収入が2,500 万ドルを超えず、（ii）年間ベースで平均 10 万以上の個人、世帯もしくは個人又は世帯が使用する機器の対象データを処理しておらず、かつ（iii）個人の対象データの譲渡から年間収入の50%以上の収入を上げていない、という3要件をいずれも満たす必要がある。[53] このようにCOPRAの適用対象要件は、CCPAのそれと類似する点がある。

ADPPAでは、下記a.又はb.に該当する者を対象エンティティと定義している。

a. 次のｲ）及びﾛ）の要件を満たす者
   ｲ）対象データの収集、処理又は移転の目的及び手段を、単独で又は第三者と共同で決定する者
   ﾛ）（ⅰ）FTC法の適用を受ける者、（ⅱ）連邦通信法第2節の適用を受けるコモンキャリア、又は（ⅲ）非営利団体（自身又はその構成員の利益のために事業を行うことを目的として、組織されていない団体）
b. 他の対象エンティティを支配する者、他の対象エンティティにより支配される者、又は他の対象エンティティと共同の支配下にある者

特に上記a.ﾛ)（ⅰ）については、FTC法5条が米国内又は米国と外国との間の商取引に対して不公正又は欺瞞的な影響を及ぼす行為又は実務を広く規制の対象としており、米国外の事業者に対する域外適用の余地もあり得る。

[53] 日本貿易振興機構（ジェトロ）サンフランシスコ事務所 海外調査部「米国連邦データプライバシー法案の概要」2021年6月 P10-12（https://www.jetro.go.jp/world/reports/2021/01/7f744522a1ddc8eb.html）。なお、ここでいう「支配」とは、ある事業者に関して、a）あらゆる種類の議決権の発行済み株式の50%以上の所有権又は議決権、b）取締役の過半数の選任を何らかの方法で支配する、又はc）経営に対して支配的な影響力を行使する権限のことをいう。

3.2 定義

3.2.1 個人情報

法的保護の対象となる個人情報に関する用語や定義は、法令により異なり、それら法令で定める個人情報は、医療、通信、金融等、ある特定の分野に特化した情報に限定されている。

FTCでは、1998年「プライバシー・オンライン」[54]と題した報告書で、PI（Personal Information）には、下記の通り、PII、及び人口統計・嗜好に関する情報の２つが含まれるとしている。

（1）Personal Identifying Information，PII

氏名、住所、eメールアドレス等の個人識別情報

（2）人口統計・嗜好に関する情報

年齢、性別、所得水準、趣味等市場分析のように個人を識別しない態様での集積に利用する、又は消費者の詳細な個人プロファイルを作成するために個人識別情報と結び付けて利用し得る情報

併せて、FTCは、2012年「FTC報告書：急速に変化する時代における消費者プライバシー保護」（FTC Report: Protecting Consumer Privacy in an Era of Rapid Change）に記述の通り、下記についても個人情報として保護すべきものとしている。

（3）「特定の消費者、コンピューターその他の機器に合理的に結び付けることのできるデータ」（consumer data that can be reasonably linked to a specific consumer, computer, or other device）

HIPPA/HIPAAプライバシー規則は、PHI（Protected health information. [55]保護対象健康情報。）を適用対象情報とした上で、PHIとは、「個人を識別し得る健康情報」（Individually Identifiable Health Information[56]）であるとし、下記４つの要件を具備する情報と定義している。

- 統計的情報を含む、個人から収集される健康情報の一部であること
- 保健医療提供者、保健計画、雇用者又は保健医療クリアリングハウスが、作成又は受領した情報であること
- 個人の過去・現在・将来の身体的若しくは精神的な健康状態、個人に対する保健医療の提供、又は個人に対する保健医療の提供に係る過去・現在・将来の支払いに関する情報であること
- 上記各要件を充足することにより、個人が識別されるもの又は個人を識別するために利用され得ると信じるに足る合理的な根拠があること

具体的な例として、PHIには、氏名、住所、生年月日、社会保障番号と合わさった健康情報等が含まれると解される。[57]なお、上記4要件の具備を要することを鑑みると、PHIは、前述Ⅰ1.1で挙げた

---

54 U.S. Federal Trade Commission, Privacy Online: A Report to Congress, 20 (1998). https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

55 https://www.govinfo.gov/app/details/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-500/context

56 https://www.govinfo.gov/app/details/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-500/context

57 石井夏生利・曽我部真裕・森亮二「個人情報保護法コンメンタール」勁草書房 2021年2月 P76、松前恵環「米国における「個人情報」の概念と個人識別性」NBL No.1189(2021.3.1)号 P52-P54

B2Cとしてデータ主体を相手方とする健康管理サービスというよりむしろ、B2Bとして保険医療事業者等を相手方とする医療支援サービスの提供にあたって取扱い処理される情報といえる。

CCPAでは、PI[58]を「特定の消費者若しくは世帯を識別する、関連する、叙述する、関連付けることができる情報、又は直接的若しくは間接的にそれらと合理的に結び付けられる情報」と、「世帯」を識別し得る情報にまで個人情報の範囲を拡大し定義している。世帯が追加されることで、スマートメーターやスマートモビリティに設置されたGPS情報等、必ずしも個人に紐付くものでないが、世帯を構成する誰かに直結する、といった情報も個人情報となる。

個人情報として、下記11通りの具体例が挙げられる。[59]

（1）実名、仮名、郵便住所、固有（一意）の個人識別子、オンライン識別子、IPアドレス、電子メールアドレス、アカウント名、ソーシャルセキュリティナンバー・社会保障番号、運転免許証番号、旅券番号その他類似の識別子
（2）第1798.80条(e)項に規定される個人情報の種類
（3）カリフォルニア州法又は連邦法の下で保護される分類の属性
（4）商業的な情報（個人資産の記録、商品の購入やサービス利用に関する情報、その他購買履歴、購買傾向の情報等）
（5）生体情報（心理的特徴、生物的特徴、行動的特徴をいい、DNA、指紋・掌紋、虹彩・網膜、声紋、歩様、キーストロークパターン等含む）
（6）インターネットその他の電子ネットワーク活動に関する情報（ウェブサイトの閲覧履歴、検索履歴、ウェブサイト・アプリケーション・広告の利用情報等）
（7）地理的位置情報
（8）音声、電子、視覚、温度・熱、嗅覚、他類似の情報
（9）職業又は雇用に関する情報
（10）教育に関する情報（非公開情報に限定）
（11）消費者の嗜好・特徴・心理トレンド・行動・意見・知能・能力・適性に関するプロファイルを作成するため、これら情報から導出された推測・推論

COPRAでは、米国在住の個人又は個人の機器を識別するか、関連付けられているか、合理的に関連付け可能な情報を対象データとしている。例として、氏名、地理的位置情報、電子メールアドレス、電話番号、機器識別子、IPアドレス、クッキー、ビーコン、ピクセルタグ、モバイル広告識別子、顧客番号等が挙げられている。

ADPPAでは、単独で又は他の情報と組み合わせて、個人若しくは端末（個人を識別し、又は個人と関連付けられ、若しくは合理的に関連付けられる可能性のあるものに限る。以下同じ。）を識別し、又は個人若しくは端末と関連づけられ、若しくは合理的に関連づけられる可能性のある情報をいい、派

[58] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140.
[59] 石井夏生利・曽我部真裕・森亮二「個人情報保護法コンメンタール」勁草書房 2021年２月 P78-P79、中崎 尚「実務解説 GDPR対応済み企業も要注意 米国カリフォルニア州消費者プライバシー法への対応」ビジネス法務 2019年12月号 P109-P110、小野 順平「カリフォルニア州消費者プライバシー法と日本企業における実務対応」国際商事法務 Vol.47 No.12 (2019) P1515-P1516、浅井 敏雄「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第54回 カリフォルニア州消費者プライバシー法の成立とその概要」国際商事法務 Vol.46 No.8(2018) P1119、及び「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第75回」国際商事法務 Vol.48 No.6(2020) P822-P823

生データや一意の永続的識別子も含まれ得る。[60]なお端末は、対象データを収集、処理又は移転することができるあらゆる電子機器であって、1人又は複数の個人によって使用されるように設計されたものと定義されている。[61]

3.2.2 センシティブ情報

現行の連邦法においては、センシティブ情報として特別の保護を必要とする情報に関する定義を明文で定めていない。

一方で、FTCの2012年報告書では、ある情報がセンシティブであるかどうかは、複数の主観的な考慮要素によるものとし、センシティブ情報を明確にしていないものの、子供に関する情報、金融情報、健康情報、社会保障番号及び正確な位置情報は、センシティブ情報であるとの見解を示している。

その見解を踏まえると、HIPAA/HIPAAプライバシー規則・HITECで定義しているPHIは、センシティブ情報であると位置付けることができると考えられる。

また、日本の個人情報保護委員会も、特定分野として、医療分野、情報通信分野及び金融分野において、通則以外に別途分野毎に個別ガイドライン・ガイダンスを定めている。[62]

一方、CPRA及びCOPRAにおいては、センシティブ情報を定義している。

CCPAではセンシティブ情報の定義は規定されていないが、CPRAでは機微個人情報を個人情報の新しいカテゴリーとして新設した。[63]機微情報としてあげられているのは、下記９つの情報である。

（1）社会保障番号、運転免許証番号、州IDカード番号、旅券番号、
（2）消費者のアカウントへのアクセスを可能にするセキュリティ・コード若しくはアクセス・コード、パスワード、又は認証情報と組み合わせたアカウント・ログイン情報、金融機関口座情報、デビットカード情報、クレジットカード情報
（3）正確な位置情報（デバイスから取得される半径1,850フィート（約564メートル）以下の円内で消費者の位置を特定するために利用されるデータ）
（4）人種的又は民族的起源、宗教又は思想・信条、労働組合への加入状況、
（5）郵便、電子メール、テキストメッセージの内容（事業者がこれらの受取人として意図されている場合を除く）
（6）遺伝データ
（7）消費者を一意に識別することを目的とした生体認証情報（生理学的、生物学的又は行動上の特徴に関する情報であって、単独又は相互に若しくは他の識別データとの組み合わせにより、個人の識別のために利用される情報）
（8）消費者の健康に関連して収集及び分析された個人情報、
（9）消費者の性的生活又は性的指向に関連して収集及び分析された個人情報

COPRAでは、下記の通り健康情報を含め14つの情報がセンシティブデータとされている。

（1）社会保障番号、パスポート番号、運転免許証番号等の政府発行の識別子

---

60 https://docs.house.gov/meetings/IF/IF17/20220623/114958/BILLS-1178152ih.pdf
61 https://docs.house.gov/meetings/IF/IF17/20220623/114958/BILLS-1178152ih.pdf
62 石井夏生利・曽我部真裕・森亮二「個人情報保護法コンメンタール」勁草書房 2021年2月 P79
63 “SEC.10. 1798.121. Consumers’ Right to Limit Use and Disclosure of Sensitive Personal information”において、“sensitive personal information”と規定している。そのため本稿では、機微個人情報と記述する。
（ https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article= ）

（2）個人の過去、現在、又は将来の身体的健康、精神的健康、障害、又は診断を説明又は明らかにする情報
（3）銀行口座番号、デビットカード番号、クレジットカード番号、又は当該銀行口座へアクセスするのに必要なセキュリティ又はアクセス・コード、パスワード若しくは資格情報
（4）生体情報
（5）個人又は機器の過去又は現在の物理的位置を明らかにする正確な位置情報
（6）対象事業者が交信の受信者である場合を除き、個人の私的交信のコンテンツ又はメタデータ、又は当該交信の当事者の身元情報
（7）電子メールアドレス、電話番号、又はアカウント・ログイン資格情報
（8）個人の人種、民族、国籍、宗教、又は組合員としての地位を当該情報の開示に関する個人の合理的な期待と矛盾する方法により、明らかにする情報
（9）当該情報の開示に関する個人の合理的な期待と矛盾する方法で、個人の性的指向又は性的行動を明らかにする情報
（10）オンライン活動を時間の経過とともに及び第三者のウェブサイト又はテキストのログ、写真又はビデオ
（11）個人の機器で保持されるカレンダー情報、アドレス帳情報、電話又はテキストの ログ、写真又はビデオ
（12）個人の裸又は下着を着た私的領域を示す写真、フィルム、ビデオ録画、又は他の同様の媒体
（13）上記のデータ種類を識別するために処理または譲渡されるその他の対象データ
（14）連邦法第5章553項に従って、FTCが規則作成を通じて、センシティブ対象データであると判断したその他の対象データ

ADPPAでは、センシティブデータに該当する対象データの内容は、概ね以下の通りである。
1）社会保障番号、パスポート番号、運転免許番号等の法律上公開されない政府発行の識別情報
2）個人の過去、現在又は将来の身体的健康、精神的健康、障害、診断又は健康管理の状態若しくは治療を明らかにする情報
3）金融口座番号、デビットカード番号、クレジットカード番号又は個人の収入水準若しくは銀行口座残高を明らかにする情報
4）バイオメトリック情報
5）遺伝情報
6）正確な地理的位置情報
7）ボイスメール、電子メール、テキスト、ダイレクトメッセージ若しくは郵便等の個人の私的な通信、又は通信の当事者 を特定する情報、音声通信、映像通信及び当該通信の伝達に関するあらゆる情報
8）アカウント若しくは端末のログイン認証情報又はセキュリティ・コード若しくはアクセスコード
9）個人の合理的な期待に反する方法で個人の性的行動を特定する情報
10）個人の私的な使用のために維持されている予定表情報、アドレス帳情報、電話若しくはテキストログ、写真、録音又はビデオ
11）個人の裸又は下着姿の私的な領域を映す写真、フィルム、ビデオ録画又はその他の類似の媒体
12）102条(4)に記載されたサービスの提供者ではない対象事業体により収集された、個人が要求又は選択したビデオコンテンツを明らかにする情報

13）対象事業体又はサービスプロバイダーが、17歳未満の個人であることを「認識」している個人に関する情報

14）個人の人種、肌の色、民族、宗教又は組合への加入状況

15）個人のオンライン活動を長期間に亘り、かつ、第三者のウェブサイト又はオンラインサービスに跨がって特定する情報

16）上記1)乃至15)の対象データを識別する目的で収集、処理又は移転されるその他の対象データ

4. 中国

4.1 個人情報保護法制

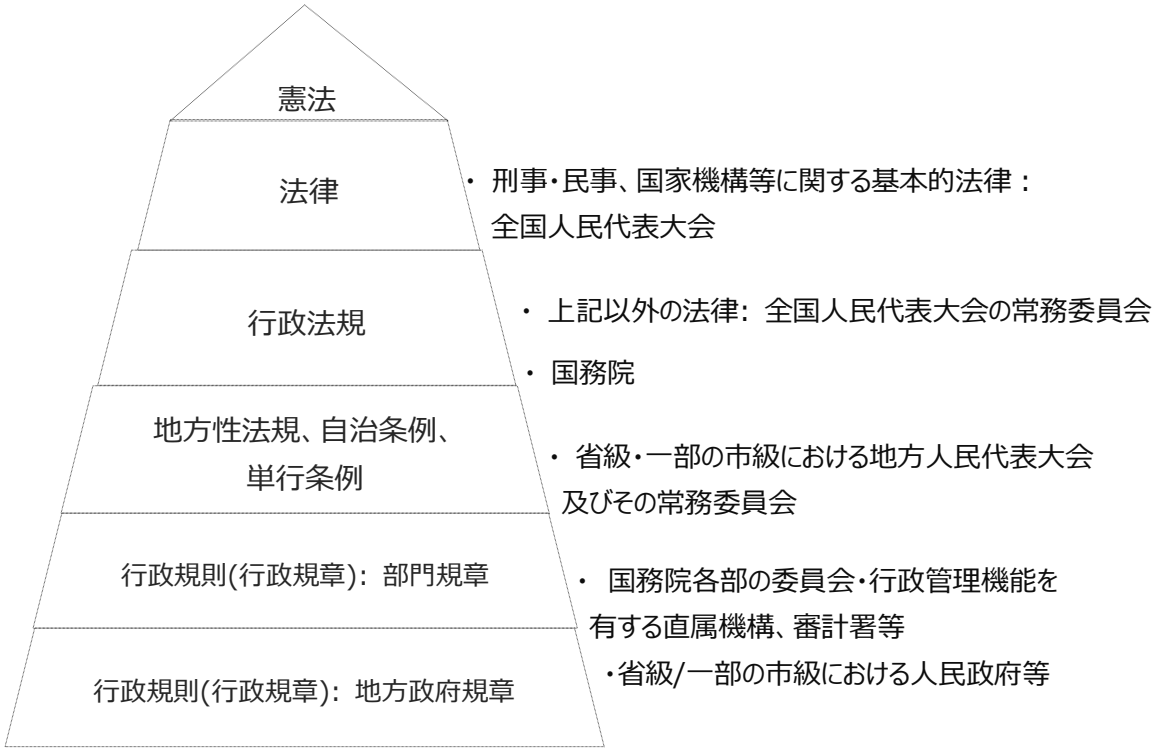
2021年8月に包括的な「個人情報保護法」（以下、「中国個人情報保護法」という。）が公布され、同年11月施行されている。[64]

その一方で、法律、行政法規、及び部門規則、並びに地方政府の法規・規則、司法解釈及び国家基準において、個人情報を含むデータの取扱い及び管理に関する規制が併存するため、各法規範で定める個人情報保護の規定が重畳的に適用され得る構造であるといえる。

加えて、法律の規定を補完する各種条例が、多岐に亘り、且つパブリックコメントの段階でとどまり、意見募集稿というドラフトの状態で何年も動きがないものが少なくない。

このような法環境のため、下記図の通り予め、法令体系のイメージと併せて、民間に適用され得る主な法令についてまず整理した上、その中から本稿で、どの法令を取り上げるのかを整理する。

図Ⅱ4.1 (1) 法令体系[65]



[64] 渡邉 雅之「逐条解説 中国個人情報保護法」三宅法律事務所の和訳を参照（同和訳では、「个人信息」を「個人情報」と和訳されていることより、本稿も同様に表記する）。
https://www.miyake.gr.jp/sites/default/files/attached/topics/zhu_tiao_jie_shuo_zhong_guo_ge_ren_qing_bao_bao_hu_fa__0.pdf

[65] 寺田 眞治「個人情報保護関連の海外の法制度の概要」JIPDEC 2019年９月 P14
（https://www.jipdec.or.jp/archives/publications/J0005156.pdf）

表Ⅱ4.1 (2) 個人情報の保護・管理を規定する主な法令等一覧[66]

公布時期	施行時期	直近改正時期	直近改正時期	法令等名称	採択・公布・発布機関
2016年11月	2017年6月	–	–	サイバーセキュリティ法	全国人民代表大会常務委員会
2017年12月	2018年5月	2020年3月	2020年10月	情報セキュリティ技術 情報セキュリティ規範	国家市場監督管理総局 国家標準化管理委員会
2021年6月	2021年9月	–	–	データセキュリティ法	全国人民代表大会常務委員会
2021年8月	2021年11月	–	–	中国個人情報保護法	全国人民代表大会常務委員会
2020年5月[67]	2021年1月	–	–	民法典	全国人民代表大会

4.1.1 該当法令

上記表Ⅱ4.1(2)の通り、個人情報を含むデータやそれらデータのセキュリティに関する法令が併存しているため、まず主な法令制定の背景・経緯を辿ることとする。

中華人民共和国国民経済及び社会発展第13次5か年計画綱要(2016年-2020年)（2016年3月17日公布。）の第28章において、データ資源の安全保護強化、インターネット空間の科学的管理、重要情報システム安全の全面保障等を実施する、と国家戦略を打ち立てている。[68] この戦略に沿って策定されたと考えられるのが、サイバーセキュリティ法[69]である。

また、中国国内に目を向けると、インターネット、ビックデータ、AIと実体経済の融合が飛躍的に進んでおり、データの安全性を確保することは、経済発展の重大な課題となっている。一方、中国国外に目を向けると、主要国等との間でのデータ覇権争いや経済安全保障の強化等が生じている。[70]国家レベルにおいても、国がネットワークと情報の安全保障システムを構築し、ネットワークと情報の確信技術、基礎

[66] サイバーセキュリティ法、データセキュリティ法及び中国個人情報保護法を併せてデータ三法といわれ、いずれも全国人民代表大会常務委員会で採択・公布されている。

[67] 統一の民法典は、これ以前にはなかった。（森・濱田松本法律事務所（令和2年度受託法律事務所）中国民法典について（日本民法との比較を中心に）令和3年1月）
（https://www.cn.emb-japan.go.jp/itpr_ja/00_000550.html）

[68] 渥美坂井法律事務所・外国法共同事業 「諸外国の個人情報保護制度に係る最新の動向に関する調査研究 報告書」平成30年3月 P113 （https://www.ppc.go.jp/files/pdf/201803_shogaikoku.pdf）

[69] 大地法律事務所「ネットワーク安全法（仮訳）」
（https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf）。「個人データ」でなく「個人情報」と和訳されているところ、本稿もサイバーセキュリティ法においては、個人情報と表記する。

[70] 中川裕茂 「中国の個人情報保護法の日本企業へのインパクト～GDPRとの対比を踏まえて～」国際商事法務 Vol.49, No.10(2021) P1241

的なインフラ、重要領域の情報システム、コントロール可能なデータの安全性を実現するとされている（国家安全法第25条）。これを受けて、全人代常務委員会立法計画（2018年9月公布）にデータセキュリティ法[71]が挙げられ、立法化されることとなった。

併せて、2018年5月GDPR施行をはじめとする各国での個人情報・プライバシー保護に関する法制整備の進展や規制強化から、中国個人情報保護法が制定されるに至った。

上記の背景・経緯を踏まえ、各法令の概要を以下の通り整理する。

サイバーセキュリティ法は、全7章全79条で構成され、同法第2条に規定の通り、中国（香港・マカオ除く。以下同様。）におけるネットワークの建設、運営、維持・保護、使用並びにネットワークの安全の監督管理について適用される。同法第4章（第40条乃至第50条）において、個人情報の取扱い及び管理について規定している。なお、同法では、第37条によりデータローカライゼーション規制としてデータの国内保存義務を定めている。

データセキュリティ法[72]は、7章全53条で構成され、同法第2条に規定の通り、中国国内において、データ処理活動及びその安全監督管理を展開する際に適用されるのと併せて、中国国外において、データ処理活動を展開し、中国国家の安全、公共の利益又は公民・組織の適法な権益を損なう場合にも、同法が適用され、法的責任を追求することができ、データの輸出規制の一面も有する。ここでいうデータについて、同法第3条で、「電子又はその他の方式による情報についての一切の記録をいう。」と定義していることから、同法は、個人情報を含むデータ全般に適用されることとなる。

上述のサイバーセキュリティ法、データセキュリティ法と併せてデータ三法と称されるのが、中国個人情報保護法である。同法は、全8章全74条で構成され、包括的な個人情報保護法として、同法3条に規定の通り、中国国内で個人情報を取り扱う活動に適用される。

併せて、法令ではないが国家標準として、GDPRやAPECプライバシー・フレームワーク等の先進主要国家の最新の立法成果を参考にした情報セキュリティ技術 情報セキュリティ規範(指導性技術基準 GB/T 35273-2017)（以下、「情報セキュリティ規範」という。）[73]が策定されている。[74]同規範は、全11条及び付属文書A乃至Dで構成され、企業等の組織又は個人による個人情報の収集、保存、使用、第三者提供・譲渡・共有及び公開・開示等の各情報処理プロセス並びに社内体制整備等について、詳細な実務指針を規定しているため、中国個人情報保護法が施行される前から、個人情報保護に関する実務的なガイドラインとして機能してきた。なお、同規範は、国家標準の中、国がその採用を奨励するとされる推奨標準であり、直接に拘束力のある規範ではなく、推奨的な基準に過ぎないが、サイバーセキュリティ法の適用において、本規範の趣旨を踏まえ、当局より是正命令を受けた例[75]が存在するため、参照するに値するといえる。

---

[71] 「データ安全法」ともいう。

[72] 渡邉 雅之「中華人民共和国データセキュリティ法（仮訳）」三宅法律事務所 2021年8月（zhong_guo_detasekiyuriteifa_zhong_guo_yu_ri_ben_yu__0.docx (live.com)）。

[73] 浅井敏雄「中国データ・情報関連法」Next Publishing Authors Press P128（「個人情報」と和訳されていることより、本稿も個人情報と記載）

[74] 渥美坂井法律事務所・外国法共同事業 「諸外国の個人情報保護制度に係る最新の動向に関する調査研究 報告書」平成30年3月 P117-P118（https://www.ppc.go.jp/files/pdf/201803_shogaikoku.pdf）

[75] 森規光、中国律師 吉佳宜「中国最新法律事情(218)情報安全技術 個人情報安全規範」国際商事法務Vol.46, No.4 (2018) P554-P556

また、民法典[76]においても、2020年改正により、同法第4編「人格権」に「第6章 プライバシー権と個人情報の保護」が新設され、個人情報の保護が、民事上の権利として認められることとなった。[77] 同章は、第1032条乃至第1039条の全8条で構成され、第1032条及び第1033条でプライバシー権、並びに第1034条乃至1039条で個人情報の定義、その処理及び権利について規定している。

本稿では上述の中、包括的且つ具体的な個人情報の取扱いや管理について定める中国個人情報保護法及び情報セキュリティ規範、並びにデータ三法である、データローカライゼーション規制を定めるサイバーセキュリティ法、及びデータの輸出規制を定めるデータセキュリティ法の計4つを取り上げることとする。

なお、センシティブ情報については、中国個人情報保護法及び情報セキュリティ規範で、その定義と取扱い及び管理について規定されている。なお、重要データとして健康関連情報を位置付けているものもある。2021年9月「重要データ識別ガイドライン」の公表、同年11月「ネットワークデータセキュリティ管理条例」の公表、2022年1月「重要データ識別ガイドラインの修正版」の公表、及び同年3月「重要データ識別規則」では、重要データを定義した上で、その1つとして健康情報を挙げているが、いずれも未だ試行・意見募集稿の状態である。[78]

4.1.2 目的・法益

中国個人情報保護法は、個人情報の権益を保護し、個人情報取扱活動を規範化し、個人情報の合理的な利用を促進することを目的とする（同法第1条）

情報セキュリティ規範は、個人情報に関するセキュリティ問題について、個人情報の取扱者が、収集、保存、利用、提供、譲渡、公開開示等の情報処理プロセスにおける関連行為を規律し、個人情報の違法収集、濫用、投漏洩等の混乱現象を抑止し、個人の適法権益と社会公共利益を最大限に保護することを目的とする。[79]

サイバーセキュリティ法は、ネットワークの安全を保障し、ネットワーク空間の主権並びに国の安全及び社会の公共の利益を保ち、公民、法人その他の組織の適法な権益を保護し、なお且つ経済・社会の情報化の健全な発展を促進することを目的としている（同法第1章総則第1条）。

データセキュリティ法は、データ処理活動を規範化し、データ安全を保障し、データ開発利用を促進し、個人・組織の適法な権益を保護し、国家の主権、安全及び発展利益を維持することを目的とする。

---

[76] 小田美佐子、朱曄「中華人民共和国 民法典」https://www.ritsumei.ac.jp/acd/cg/law/lex/20-2/010odaandzhu.pdf
法務省「中国民法典の制定について(3)第87号2021年6月
https://www.moj.go.jp/housouken/houso_houkoku_china.html
（いずれも「個人情報」と和訳されていることより、本稿も個人情報と記載）

[77] 神保宏充「中国ビジネス法務Q&A 第186回 中国民法典における個人情報保護規定」国際商事法務 Vol.48 No.11 (2020) P1605

[78] 「重要データの識別・認定」日本貿易振興機構 2022年11月
https://www.jetro.go.jp/world/reports/2022/01/5a02eed2b328b63b.html（何年にも亘って意見募集稿の状態が続く他の規則・条例や規範もまた複数存在するため、正式に施行が決まった段階で、改めて取り上げることとする。）

[79] 渥美坂井法律事務所・外国法共同事業 「諸外国の個人情報保護制度に係る最新の動向に関する調査研究 報告書」平成30年3月 P127（https://www.ppc.go.jp/files/pdf/201803_shogaikoku.pdf）

以上からデータ三法は、いずれも個人の権益保護と併せて、個人情報含むデータの適正な利活用を促進することを目的としているといえる。また、情報セキュリティ規範、サイバーセキュリティ法及びデータセキュリティ法では、加えて国家・サイバー空間の主権や、社会公共の利益を保護することも目的としている。

4.1.3 適用範囲

中国個人情報保護法は、中国国内で自然人の個人情報を取り扱う活動を適用対象としている。

併せて同法は、域外適用の規定を設けており、中国国外で中国国内の自然人の個人情報を取り扱う活動において、次のいずれかの事由に該当する場合も、適用されるとしている（同法第3条）。

・中国国内の自然人に商品若しくはサービスを提供することを目的とする場合
・中国国内の自然人の行為を分析、評価する場合
・法律、行政法規が定めるその他の場合

情報セキュリティ規範は、主管監督管理部門、第三者評価機構等の組織を含む各種組織による個人情報処理活動の規範化に適用されるとしている（同規範第1条）。

サイバーセキュリティ法は、中国国内におけるネットワークの建設、運営、維持・保護、使用並びにネットワークの安全の監督管理に適用するとしている（同法第2条）。同法の「第4章ネットワーク情報の安全」では、個人情報処理活動についての規定があり、それらの規定は、ネットワークの所有者及び管理者並びにネットワークサービスの提供者である「ネットワーク運営者」に適用される、としている（同法第76条）。なお、ホームページを開設する一般企業も、このネットワーク運営者に該当する。[80]そのため、大半の企業が、同法第4章で定める個人情報の処理の規定が適用されることになるといえる。

データセキュリティ法は、中国国内において、データ処理活動及びその安全監督管理を展開する際に適用されるとしている。

併せて同法は、域外適用の規定を設けており、中国国外においてデータ処理活動を展開し、中国国家の安全、公共の利益又は公民・組織の適法な権益を損なう場合には、法的責任を追及できるとしている。

以上から、下記の通り整理することができる。

・中国個人情報保護法、情報セキュリティ規範、サイバーセキュリティ法、及びデータセキュリティ法の４法規範いずれも個人情報処理活動に適用される。
・中国個人情報保護法及びデータセキュリティ法は、域外適用が認められる。

[80] 日本貿易振興機構（ジェトロ）北京事務所 ビジネス展開・人材支援部「中国におけるサイバーセキュリティー、データセキュリティおよび個人情報保護の法規制にかかわる対策マニュアル」2021年11月 P10
（https://www.jetro.go.jp/world/reports/2021/02/0c080037fe572f0d.html）

4.2 定義

4.2.1 個人情報

中国個人情報保護法は、第４条で、個人情報を「匿名化された情報を除き、電子的又はその他の方法で記録された、識別された又は識別可能な自然人に関連するあらゆる種類の情報である、と定義し、この規定は"識別性＋関連性"、即ち識別可能性を基準とした「関連説」が採用されているとみられる。関連説に立つと、理論上、世の中の自然人はみな既に識別され又は識別し得る対象であるため、たとえ当該情報だけでは、又はその他の情報と合わせても、特定の自然人を識別することができない情報であっても、ある特定の自然人に関わる情報であれば、同法でいう個人情報となり得る。例えば、スマートフォンのシリアルナンバーのような製品の個体識別番号は、販売以前の特定個人の利用に供されていない状態であれば、購入者名や連絡先等と紐付いていないため、個人情報に該当しない。しかし、個人向けに販売されれば、特定個人によって利用される端末となるため、関連説に従うと、この端末のシリアルナンバーは個人情報に該当するといえる。[81]

なお、同条では、匿名化処理された情報は個人情報に含まれない、としている。

情報セキュリティ規範は、第3.1条で、個人情報を「電子又はその他の方式により記録された、単独で、又はその他の情報と結びついて特定の自然人の身分を識別し、又は特定の自然人の活動状況を反映することができる各種の情報」と定義した上、個人情報の判定方法及び類型については、付属文書Aを参照することとしている。これを受け同付属文書Aでは、個人情報の判定基準を示しており、下記２つのルートを考慮しなければならないとし、いずれかに該当する場合、個人情報に該当する、としている。

① １つ目は、識別、即ち情報から個人のルートで、情報そのものの特殊性によって特定の自然人が識別されることであり、個人情報は特定の個人を識別する役割を果たすものでなければならない。
② ２つ目は、関連付け、即ち個人から情報へのルートで、例えば既に知られている特定の自然人について、当該特定の自然人の活動中に生じた情報

併せて、同付属文書Aで、13の分類に区分[82]し、次のような個人情報の例示等を挙げている。

a) 上記①に対応する例:
・個人基本的資料（氏名、個人の電話番号、Eメールアドレス等）
・オンライン身分識別表示情報（アカウント、IPアドレス等）
・個人常用デバイス情報（ハードウェアのシリアルナンバー、デバイスのMACアドレス、UDID等を

[81] 章 啓龍 (Zhang qilong)・刁 聖衍 (Diao shengyan)「連載 中国における近時の重要立法・改正動向 第7回 個人情報保護法」ビジネス法務 2022年4月号 P139-P140、原 洁 (Yuan Jie)「11月1日施行, 中国個人情報保護法の概要と日本企業への影響」ビジネス法務 2021年12月号 P78、今野由紀子「中国個人情報保護法・データ安全法の解説と企業対応実務 (上)」 NBL No.1204(2021.10.15)号 P60

[82] ①個人基本的資料、②個人身分情報（身分証等）、③個人生体識別情報（指紋等）、④オンライン身分識別情報、⑤個人健康生理情報（発病・治療関連記録(既往歴等)、個人の身体健康状況に関連する情報（体重、身長等)）、⑥個人教育就労情報（成績表等）、⑦個人財産情報（銀行口座等）、⑧個人通信情報、⑨連絡先情報（アドレス帳等）、⑩個人インターネット接続記録、⑪個人常用デバイス情報、⑫個人位置情報、⑬その他の情報（宗教信仰、性的指向等）

含む、個人の常用デバイスの基本的な状況が記述された情報）

b) 上記②に対応する例:

・個人通信情報（通信記録、ショートメッセージ、電子メール及び個人の通信が記述されたデータ、いわゆるメタデータ）

・個人インターネット接続記録（ウェブサイト閲覧記録等、ログを通じ保存された個人情報主体の操作記録）

・個人位置情報（移動軌跡、高精度位置情報、宿泊情報、経緯度等）

なお、同規範3.1の注書きで、ユーザプロファイル・特徴タグ等、個人情報管理者が、個人情報又はその他の情報の加工処理を通じて作成した情報は、単独で又はその他の情報と結びついて、特定の自然人の身分を識別し、または特定の自然人の活動状況を反映することができる場合、個人情報に該当する、としている。

サイバーセキュリティ法は、第76条第５項で、個人情報を「電子データその他の方式により記録され、単独又はその他の方式により記録され、単独又はその他の情報と組み合わせて自然人の個人身分を識別することができる各種情報」と個人情報を定義した上、「自然人の氏名、生年月日、身分証番号、個人の生物識別情報、住所、電話番号等を含むが、これらに限らない」としている。

データセキュリティ法は、4.1.1で記載の通り、データ全般を適用対象とするため、個人情報についての定義について、特段定めはない。

参考まで、民法典では、第1034条で、個人情報を「電子又はその他の方式により記録された、単独で、又はその他の情報と結合して、特定の自然人を識別することができる各種情報」と定義した上、例として「自然人の氏名、生年月日、身分証明書番号、生体識別情報、住所、電話番号、メールアドレス、健康情報、移動履歴情報等」を挙げている。

以上から、下記表の通り、個人情報の定義・範囲を整理することができ、中国個人情報保護法及び情報セキュリティ規範が、GDPRに類似し、日本より広く個人情報の範囲を規定しているといえる。

表Ⅱ4.2.1 (1) 個人情報の定義として個人の識別性/関連性の有無

法令・国家基準	識別性	関連性	補足
中国個人情報保護法	○	○	GDPRと類似（GDPRを参考に策定されている）
情報セキュリティ規範	○	○	中国個人情報保護法で定める個人情報を補完
サイバーセキュリティ法	○	N/A	中国個人情報保護法より範囲が狭い
データセキュリティ法	N/A	N/A	個人情報の定義無し（データ全般に適用）
民法典	○	N/A	–

○: 該当, N/A: 非該当

表Ⅱ.4.2.1 (2) 個人情報の定義

法令 国家標準	定義（各法令・国家基準より抜粋）
中国個人情報保護法	電子又はその他の形式により記録され、既に識別され、又は識別可能な自然人に関する各種の情報
情報セキュリティ規範	電子又はその他の方式により記録された、単独で、又はその他の情報と結びついて特定の自然人の身分を識別し、又は特定の自然人の活動状況を反映することができる各種の情報 ・ 識別、即ち情報から個人のルートで、情報そのものの特殊性によって特定の自然人が識別されることであり、個人情報は特定の個人を識別する役割を果たす情報 ・ 関連付け、即ち個人から情報へのルートで、例えば既に知られている特定の自然人について、当該特定の自然人の活動中に生じた情報
サイバーセキュリティ法	電子データその他の方式により記録され、単独又はその他の方式により記録され、単独又はその他の情報と組み合わせて自然人の個人身分を識別することができる各種情報
データセキュリティ法	N/A
民法典	電子又はその他の方式により記録された、単独で、又はその他の情報と結びついて、特定の自然人を識別することができる各種の情報

4.2.2 センシティブ情報

中国個人情報は、第28条で、機微な個人情報を「ひとたび漏洩したり不正に利用されたりすると、自然人の人間としての尊厳が侵害されたり、その人や財産の安全が脅かされたりするおそれのある個人情報」と定義した上で、例として「生体認証、宗教信仰、特定身分、医療・健康、金融講座、行方・移動経路等の情報、及び14歳未満の未成年の個人情報」を挙げている。[83]

情報セキュリティ規範は、第3.2条で、機微情報を「一旦漏えいしまたは不法提供もしくは悪用(濫用)された場合、個人または財産の安全に危害を及ぼしまたは個人の名誉または心身の健康が損なわれまたは差別的な扱いを受けることにつながり易い個人情報」と定義した上、個人情報の判定方法及び類型については、付属文書Bを参照することとしている。これを受け同付属文書Bでは、第3.2条で挙げた例示に「自然人のプライバシーに関係する情報」を加えた上、個人情報の判定基準を下記の通り３つ示している。

・ 漏洩：

[83] 同法第28条では、「敏感个人信息」と定義されている。渡邉 雅之（三宅法律事務所）の和訳では、これを「機微個人情報」と和訳されていることより、本稿も同様に表記する。
（ jia_yi_zhong_guo_ge_ren_qing_bao_bao_hu_fa_zhong_guo_yu_ri_ben_yu_.pdf (miyake.gr.jp) ）

個人情報がいったん漏洩すると、個人情報主体並びに個人情報を収集・使用する組織及び機構が、個人情報に対する管理能力を喪失することになり、個人情報の拡散範囲及び用途が制御不能となる。ある個人情報が漏洩した後、個人情報主体の意向に背く方式で直接使用され、又はその他の情報との関連分析が行われて、個人情報主体の権益に重大なリスクをもたらす虞がある場合（例：個人情報主体の身分証の写しが他人によって携帯電話番号カードの実名登録、銀行口座の口座開設・カード発行に用いられる等）

・ 不法な提供：

ある個人情報について、個人情報主体による授権同意の範囲外において拡散されるだけで、個人情報主体の権益に重大なリスクをもたらしうる場合（例：性的指向、預金情報、感染症病歴等）

・ 濫用：

ある個人情報が、授権の合理的な範囲を逸脱した場合において使用されると（例：処理目的の変更、処理範囲の拡大等）、個人情報主体の権益に重大なリスクをもたらす虞がある場合（例：個人情報主体による授権を取得していない場合において、健康情報を保険会社の営業販売及び個人保険料の高低の確定に用いる）

併せて、同付属文書Aで、5つの分類に区分し、次のような個人情報の例示等を挙げている。

表Ⅱ4.2.2 情報セキュリティ規範の付属文書で定めるセンシティブ情報

分類	例示
個人財産情報	銀行口座、識別情報（パスワード）、預金情報（貸金量、出入金記録等含む）、不動産情報、信用貸付記録、信用調査情報、取引及び消費記録、出納記録等並びに仮想通貨、仮想取引、ゲーム類引換コード等の仮想財産情報
個人健康整理情報	発病・治療等によって乗じた個人の関連記録（発症、入院記録、医師指示書、検査報告、手術及び麻酔記録、看護記録、投薬記録、薬物・食物アレルギー情報、出産情報、既往歴、診療状況、家族の病歴、現病歴、感染症病歴等）
個人生体識別情報	個人の遺伝子、指紋、声紋、掌紋、耳介、虹彩、顔認識の特徴点等
個人身分情報	身分証、軍官証、パスポート、運転免許証、勤務証、社会保険カード、居住証等
その他の情報	性的指向、婚姻歴、宗教信仰、未公開の違法犯罪記録、通信記録及び内容、アドレス帳、友人リスト、グループリスト、移動軌跡、ウェブページ閲覧記録、宿泊記録、高精度位置情報等

なお、サイバーセキュリティ法及びデータセキュリティ法では、機微な個人情報を定めていない。

そのため中国では、中国個人情報保護法及び情報セキュリティ規範の規定に則り、上述の通り機微な個人情報かどうかを判断することになる

5. 小括

ここまで日米欧中の法制を概観し、各国で個人情報保護を規定する法令、当該法令で定める目的・保護法益、適用範囲、並びに個人情報及びセンシティブ情報の定義についてまとめてきた。第Ⅱ部の小括として、日米欧中の法制比較を通じ、各国における共通点と相違点を整理し、国毎にどのような特徴があるのか明らかにする。

5.1 日米欧中における法制に関する共通点と相違点

下記表Ⅱ5.1の通り整理すると、以下のことがいえる。

4カ国中、日欧中3カ国は、国全体に適用される包括法としての個人情報保護法制が、制定されている、という点で共通する。[84]とりわけ、日本とEUは、下記表をみると、統一化・一元化された包括的法制となっており、各項目も共通している。このことから日欧は、４カ国中最も類似した法体系であるといえる。[85]

一方で、中国では包括法が存在する中で、サイバーセキュリティ法及び民法典にある個人情報保護の規定はそのまま残存しており、加えて多岐に亘る下位の法規範（行政法規、地方法規等）も重なり合って併存する構造のため、従来通り未だ重畳的な法体系であるといえる。

なお、各国法令における保護法益に着目すると、サイバーセキュリティ法及びデータセキュリティ法は、その対象が個人のみならず、国家や社会も含むことから、国益・公益保護の観点からデータ規制がなされる虞があること、併せて個人情報ではないデータに対してもその適用対象としていることを踏まえると、中国で個人情報の法対応を行うに当たっては、インフォームドコンセント等個人の権益を保護するための対応を行うこと以外にも、国益・公益を損なわないための対応についても、その実施を余儀なくされるといえる。

なお、日米欧中４カ国ともに共通する制度としては、個人情報の取扱いに対し、域外適用がなされ得る、ということが挙げられる。

[84] 米国で、COPRA等の法案が今後成立すれば、4カ国とも国全体に適用される包括法が存在するという点で共通することとなる。

[85] なお、GDPRは、Ⅱ2.1で紹介したその名称にも記載の通り、個人データ保護と併せて、EU域内での個人データの流通を促進することもまた目的としている。

表Ⅱ5.1 個人情報保護法制の比較

<table>
<tr><th rowspan="2">地域</th><th rowspan="2">法令</th><th rowspan="2">目的・保護法益</th><th rowspan="2">保護対象</th><th rowspan="2">包括法</th><th colspan="2">適用範囲</th><th colspan="2">定義の有無</th><th colspan="2">データローカライゼーション</th></tr>
<tr><th>対象地域</th><th>域外適用</th><th>個人情報</th><th>センシティブ情報</th><th>国内保存義務</th><th>海外移転制限</th></tr>
<tr><td>日本</td><td>個情法</td><td>個人の権益</td><td>個人</td><td>○</td><td>日本</td><td>○</td><td>○</td><td>○</td><td>N/A</td><td>○</td></tr>
<tr><td>EU</td><td>GDPR</td><td>・基本的権利・自由、特に個人データ保護の権利保護
・EU域内での個人データの自由な移動</td><td>個人</td><td>○</td><td>EU</td><td>○</td><td>○</td><td>○</td><td>N/A</td><td>○</td></tr>
<tr><td rowspan="6">米国</td><td>FTC法</td><td>消費者保護（不公正・欺瞞的行為等の防止）</td><td rowspan="6">個人</td><td>N/A</td><td rowspan="4">米国</td><td>○[86]</td><td>○</td><td>○</td><td rowspan="6">N/A</td><td rowspan="6">N/A</td></tr>
<tr><td>ADPPA</td><td>プライバシーの権利保護</td><td>〇</td><td>○[87]</td><td>○</td><td>○</td></tr>
<tr><td>COPRA</td><td>プライバシーの権利保護</td><td>○</td><td>○[88]</td><td>○</td><td>○</td></tr>
<tr><td>HIPAA等</td><td>医療保険制度の適正化・健全化</td><td>N/A</td><td>○[89]</td><td>○</td><td>○</td></tr>
<tr><td>CCPA</td><td rowspan="2">プライバシーの権利保護</td><td rowspan="2">○</td><td rowspan="2">加州</td><td rowspan="2">○</td><td rowspan="2">○</td><td>N/A</td></tr>
<tr><td>CPRA</td><td>○</td></tr>
</table>

[86] 渥美坂井法律事務所・外国法共同事業「諸外国の個人情報保護制度に係る最新の動向に関する調査研究報告書」平成30年3月 P15
（https://www.ppc.go.jp/files/pdf/201803_shogaikoku.pdf）

[87] SEC. 2. DEFINITIONS. (9) COVERED ENTITY. - The term ‘‘covered entity’’ - (A)（対象事業体にFTC法の適用を受ける者が挙げられている。）
https://docs.house.gov/meetings/IF/IF17/20220623/114958/BILLS-1178152ih.pdf

[88] 日本貿易振興機構 サンフランシスコ事務所 海外調査部 米国連邦データプライバシー法案の概要 2021年6月 Ⅱ8 Q2 P55
（https://www.jetro.go.jp/world/reports/2021/01/7f744522a1ddc8eb.html）

[89] HITECHはHIPAA適用範囲にBusiness associates: BAを追加している。HIPAA適用主体は、BAとBusiness Associate Agreement: BAAの締結を要し、BAはHIPAA等順守に必要となるBAAの契約内容を順守義務がある。BAに相当するグローバルで医療支援サービス提供する事業者もBAA締結によりその義務が課せられることより、実質域外適用がなされ得る。

中国	個人情報保護法	個人情報の権益保護と、合理的な利用促進	個人	○	中国	○	○	○	○	○
	情報セキュリティ規範	個人の適法権益と社会公共利益を最大限に保護	個人/社会	N/A		N/A	○	○	N/A	N/A[90]
	サイバーセキュリティ法	・ネットワークの安全保障、ネットワーク空間の主権 ・国の安全、社会の公共利益保持、経済社会情報化の健全な発展促進 ・公民・法人の適法な権益保護	・ネットワーク ・国・社会 ・個人	N/A		N/A	○	N/A	○	○
	データセキュリティ法	・データ処理活動の規範化、データの安全保障、データ開発利用の促進 ・国家の主権、安全、発展利益の維持 ・個人・組織の適法な権益保護	・データ ・国 ・個人	N/A		○	N/A	N/A	○	○
	民法典	・個人の権益保護 ・社会・経済秩序の保護維持、社会主義核心的価値観の発揚	・個人 ・社会	N/A		N/A	○	N/A	N/A	N/A

○: 該当, N/A: 非該当

[90] セキュリティ規範9.8で、他の関連規定及び関連標準の要求を遵守することと規定されており、同規範独自の規制がないことから、本稿ではNAとする。

5.2 日米欧中における個人情報の範囲に関する共通点と相違点

次に前掲表Ⅱ5.1の中で、「定義の有無」の「個人情報」にフラグが立っている（「○」となっている）法令を取り上げ、各法令で定める個人情報の定義や範囲において、共通する点と相違する点について明らかにする。それにあたって、平成27年法改正の方向性を検討するために内閣官房高度情報通信ネットワーク社会推進戦略本部で設けられたパーソナルデータに関する検討会（以下、「パーソナルデータに関する検討会」という。）で検討された個人情報の定義や考え方を軸に整理していくこととする。

日本では、個人情報を「特定の個人を識別することができる情報」と定義しているが、これは、社会通念上、一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認めるに至ることができることをいう（この性質を以下、「個人識別性」という。）。[91]

まず、個人識別性は、「識別」と「特定」の２つの要素で構成される。識別とは、ある誰か1人の情報であると分かる状態のことである。特定とは、識別から更に進んで、その1人の情報が、誰の情報か分かる状態のことをいう。

この2つの要素から、個人に関する情報を次の3つに分類することができる。

（1）識別特定情報:
それが誰か1人の情報であることが分かり、更にその1人が誰であるかも分かる情報

（2）識別非特定情報:
それが誰か1人の情報であることは分かるが、その1人が誰であるかまでは分からない情報

（3）非識別非特定情報:
それが誰の情報であるかが分からず、更にそれが誰か1人の情報であることも分からない情報

次に特定の個人を識別することができる情報には、次の2つが挙げられる。

（ｲ）それ単体で個人識別性を有する「個人識別符号」を含む情報

（ﾛ）個人識別符号以外の記述で個人識別性を有する情報

個人識別符号に該当するかを判断する基準として、①社会的な意味合い、②一意性等本人との結び付きの程度、③不変性、及び④本人到達性、といった性質を有するか、が挙げられている。

上記（ｲ）の通り、個人識別符号自体が、個人情報とみなされる社会的な背景・経緯として、ICTの急速な進展に伴い、特定の個人を識別することなく、1人の人間を識別する識別子を用いて膨大な個人に関する情報、即ちパーソナルデータを収集してそれらを利用するようになっていることが挙げられる。こうしたパーソナルデータは、ある時点では特定の個人を識別することができなくとも、他のパーソナルデータと容易に結合し、特定の個人が識別される蓋然性が高く、その取扱いによっては、特定の個人が識別される虞がある、という性質を備えている。

更に個人識別符号は、以下の通り分類することができる。

（1）前述Ⅱ1.2.1（1）の通り、DNAを構成する塩基配列、容貌、虹彩の線状模様、声紋、歩行の姿勢・態様、静脈の形状、指紋又は掌紋等、身体の特徴を変換した符号（以下、「生体個人識別符号」という。）

（2）次のいずれの要件も具備する符号（以下、「公的個人識別符号」という。）

[91] 個人情報保護委員会「「個人情報の保護に関する法律についてのガイドラインに関する」に関するQ&A」Q1-1
https://www.ppc.go.jp/files/pdf/2305_APPI_QA.pdf

ⅰ）行政機関（それに準ずる公的機関を含む）が付番するもの、又は付番に当たり本人確認が法定されているもののいずれかに当たり、本人であることが確実であるもの

ⅱ）法人その他の団体の番号と紛れる虞がないこと

ⅲ）社会において広く流通し、利用される実態があること

ⅳ）番号の存続期間が非常に短いものでないこと

例として、前述Ⅱ1.2.1（2）乃至（7）の通り、旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、国民健康保険者証・介護保険者証の番号等が挙げられる。また、個人識別符号以外にも、日本以外の国・地域では、それ単体で個人情報となり得る識別子がある。本稿ではその識別子を下記の2つに分類し取り上げることとする。

（3）商品・サービスの提供に伴い、企業その他民間組織が消費者へ付番するID・識別子（以下、「サービス等識別子」という。）。例として、携帯電話番号、メールアドレス、クレジットカード番号、サービスID等が挙げられる。

（4）Cookie-ID、IPアドレス等（以下、「オンライン識別子」という。）

以上を踏まえ、日米欧中の各法令で定める個人情報の定義・範囲の共通点と相違点について整理すると、下記表Ⅱ5.2の通りとなり、この表からは、以下のことがいえる。

日米欧中における個人情報保護を定めた包括法は、いずれも識別特定情報を個人情報とすることは共通するが、日本を除く米欧中の当該包括法については、識別非特定情報もまた個人情報に含んでいるといえる。

なお、EUでは、GDPRの特別法としての位置付けで、cookie等オンライン識別子を含む情報の取扱いルールを定めるeプライバシー規則案が作成・検討されている。その一方、日本では、2022年4月施行の改正個人情報保護法下、個人関連情報を新設し、一定の条件下での法令要件を設けているが、個人関連情報はそもそも個人情報、仮名加工情報及び匿名加工情報ではない情報、と位置付けられている。但し、今後、eプライバシー規則案が正式に制定されることになれば、EU間での十分性認定の維持継続の観点から、日本でも個人情報保護法の3年ごと見直しのタイミングで、個人情報の範囲の見直しや、オンライン識別子の保護強化について検討することが想定されるため、今後の法改正を注視する必要がある。

なお、令和4年6月、電気通信事業法の一部を改正する法律が可決・成立し、令和5年6月から施行されることとなっており、日本国内において、グローバルヘルスケア法人は、その規模や態様によっては電気通信事業法上の特定利用者情報の適正な取扱いも求められる。[92]

[92] PHR事業者は、その規模や態様によっては、「内容、利用者の範囲及び利用状況を勘案して利用者の利益に及ぼす影響が大きいものとして総務省令で定める電気通信役務を提供する電気通信事業者」として指定を受ける可能性があり、その場合は電気通信事業法上の対応も必要と考えられるが、本稿では日米欧中の個人情報・個人データ保護法の比較に焦点を当てる。

表Ⅱ5.2 個人情報保護法制の比較

			日本	EU	米国[93]				中国	
			個人情報保護法	GDPR	FTC法	CPRA	ADPPA	COPRA	個人情報保護法	情報セキュリティ規範
1. 個人情報・個人データ	(1) 識別/特定性	a 識別特定情報 （例: 下記(2)a･b, 氏名）	○	○	○	○	○	○	○	○
		b 識別非特定情報 （例: 下記 (2)c･d 等）	N/A	○	○	○	○	○	○	○
		c 非識別非特定情報 （例:上記abを含まない血圧値）	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
		d 統計情報[94]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	(2) 識別子	a 個人識別符号 ・ 身体の特徴を変換した符号	○	○	○	○	○	○	○	○
		b 公的個人識別符号 ・ 公的機関発行の符号 （例: マイナンバー）	○	○	○	○	○	○	○	○
		c オンライン識別子 （Cookie-ID, IPアドレス 等）	N/A	○	○	○	○	○	○	○
		d サービス等識別子 （消費者へ付番する識別子）	N/A	○	○	○	○	○	○	○

[93] HIPAAはそもそもPHIとしての4要件を具備した情報が保護対象のため、本表より除外（加重要件なく下記表2.4.3も同様）。

[94] 複数人の情報から、共通要素に係る項目を抽出して、同じ分類毎に集計し得られる情報。集団の傾向、性質等を数量的に把握するもので、特定の個人との対応関係が排斥されている情報（個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン」に関するQ&A 平成29年2月16日（令和4年5月26日更新) Q1-7 P2）

2. センシティブ情報	健康情報	a 診療・調剤等の業務と関係のない方法で取得した健康情報	N/A	○	○	○	○	○	○	○
		b 上記a.以外の健康情報全般	○	○	○	○	○	○	○	○
	医療情報	医療従事者が作成・記録した情報及び医療従事者の指示に基づき介護事業者が作成・記録した情報	○	○	○	○	○	○	○	○
	（参考）	金融情報（例：口座情報　等）	N/A	N/A	◯	○	○	○	○	○
		位置情報（高精度・正確な位置情報）	N/A	N/A	◯	○	○	○	○	○
		通信情報/メタデータ（例：電子メール等通信記録）	N/A	N/A	◯	○	○	○	○	○

○：該当, N/A：非該当

5.3 日米欧中におけるセンシティブ情報の範囲に関する共通点と相違点

上記表Ⅱ5.1の中で、「定義の有無」の「センシティブ情報」にフラグが立っている（「○」となっている）法令を取り上げ、各法令で定めるセンシティブ情報の定義や範囲において、共通する点と相違する点について明らかにする。

上記表Ⅱ5.2の通り整理すると、以下のことがいえる。

まず、前述Ⅰ1.3において、本稿の主材として取り上げることとした医療情報及び健康情報について着目する。

日米欧中いずれの該当法令においても共通することは、医療情報、即ち医療従事者の診療過程で収集されカルテ・診療録に記載される既往歴、疾病、服薬、遺伝子関連情報等が、センシティブ情報と位置づけられるという点である。相違する点としては、健康情報、即ちセルフメディケーションの目的で本人自身で自己管理する体重・BMI、体温、血圧・脈拍、心電・心拍、SpO2、血糖計喘鳴又は睡眠関連情報が、欧米中いずれの該当法令においてもセンシティブ情報である一方、日本では非センシティブ情報、即ち要配慮個人情報に該当しない、という点である。

次に医療情報及び健康情報以外の情報について着目すると、日欧と米中の間で、異なることが分かる。

まず識別子に着目すると、個人識別符号については、米中のCOPRA、ADPPA、及びCPRA並びに中国個人情報保護法及び情報セキュリティ規範において、センシティブ情報である点で共通する。また、それら包括法の中、州法であるCPRAを除き、連邦法案であるCOPRA及びADPPA並びに中国個人情報保護法及び情報セキュリティ規範では更に、オンライン識別子に紐付き集積される情報、例えばWeb又はアプリケーションの閲覧履歴又は検索履歴等について、同じくセンシティブ情報に該当する、という点についても共通する。

一方で、日本とEUは、個人識別符号[95]及びオンライン識別子に紐付き集積される情報いずれも、センシティブ情報とならない点で共通する。

更に金融情報、例えば口座情報、デビットカード情報、クレジットカード情報、それらへのアクセス・ログイン情報、高精度な位置情報、又は通信情報、例えばメタデータのような通信記録については、米中ではセンシティブ情報に該当するが、他方、日欧では、共通して非センシティブ情報となる。

このように日欧と米中間で、センシティブ情報の範囲が異なるのは、日欧では、その不適正な取扱いや漏洩等により、不当な差別、偏見その他の不利益といった社会的差別につながる虞のある個人情報をセンシティブ情報と位置付けているのに対し、米中では更に、その不適正な取扱いや漏洩等により、重大なプライバシー侵害を生じさせる可能性のある類の情報をセンシティブ情報に加え、社会的信用度や、行動・嗜好等から浮き彫りになる人物像が明らかになるような情報まで範囲を広げていると推察する。[96]

---

[95] 生体個人識別情報については、EUでは、自然人を一意に識別することを目的とする場合にはセンシティブ情報としている（GDPR第9条）。

[96] 表Ⅱ-5.1の「目的・保護法益」欄の通り、中国個人情報保護法は、原則個人の権益保護を目的とし、国益・公益の観点で重要データを定義し、その取扱いを厳格化するのは、サイバーセキュリティ法、データセキュリティ法及びその下位規定であると整理することができるため、ここでは保護法益の対象を国家でなく、個人として考える。

Ⅲ センシティブ情報取扱いに対する規制の厳格化

前述Ⅱでは、法制概観を踏まえ、日米欧中において、センシティブ情報とはどのようなものか、併せてセンシティブ情報の前提条件となる個人情報とはそもそもどのようなものか、を各国間での比較を通じ明らかにした上、健康・医療情報並びに健康・医療サービスで利活用し得る情報が、センシティブ情報に該当するのかについて明らかにしてきた。

これを踏まえ第Ⅲ部では、前述Ⅰ1.3(2)乃至(4)の論点を踏まえ、日米欧中において、一般的な個人情報に比し、健康・医療情報の取扱いが厳格化される局面、及びその加重要件は何か、並びにそれら情報に仮名化処理又は匿名化処理を施すことで、それら加重要件が緩和されるのか、という点について明らかにしていく。

それらを明らかにするにあたって、表Ⅱ5.2で取り上げた各法令において、まずは、一般的な個人情報に比し、センシティブ情報の取り扱いに対する法令要件が厳格化される局面及び加重要件をまとめ、次に仮名化処理及び匿名化処理の定義・考え方を整理した上で、各国間でのそれらに共通する点と相違する点を明らかにしていく。また、前述Ⅰ1.2の問題提起を踏まえ、センシティブ情報をクロスボーダーで取扱う局面を含めて考察していく。

1. 日本

1.1 一般的な個人情報の取扱いに対する規制

1.1.1 日本国内における個人情報の取扱いに関する主な法令要件

個人情報保護法は、概ね局面毎に法令要件を定めている。

1.1.1.1 取得・利用

まず、個人情報取扱事業者は、個人情報を取り扱うにあたって、その利用目的をできる限り[97]特定する必要がある（第17条第1項）。特定した利用目的は、関連性を有すると合理的に認められる範囲を超えて変更してはならず[98]（同条第2項）、当該範囲内で変更をした場合は、「変更された利用目的を本人に通知するか、又は公表しなければならない」としている（同法第21条第3項）。

上述通り利用目的を特定した上で、個人情報取扱事業者は、個人情報を取得した場合、速やかにその利用目的の本人への通知、又は公表を要する（同法第21条第1項）。また、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。）に記載された本人の個人情報を取得する場合、その他本人から直接書面に記載された本人の個人情報を取得する場合は、予め、本人に対しての利用目的の明示を要する。

個人情報の取得にあたって、個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならず（同法第20条第1項）、また予め本人からの明示的同意を得ず、要配慮個人情報を取得してはならない（同法第20条第2項）。

---

[97] この「できる限り」について、通則3-1-1では、「どのような取扱いが行われているかを本人が予測・想定できる程度」と補足している。https://www.ppc.go.jp/files/pdf/230401_guidelines01.pdf

[98] 当該範囲を超えて個人情報を取り扱う場合は、本人から事前同意の取得を要する（同法18条第1項）。

上述を踏まえ、GDPRと比較すると、本人へ一定の情報提供を要する点ではGDPRと共通するが、一方で、個人情報保護法は、明示的同意取得を要する局面を「本人が予測・想定しえない程度に利用目的が変更される場合に限る」とする点では、そのような限定なく、適法性の根拠として明示的な同意を求めるGDPRとは、異なるといえる。

1.1.1.2 第三者提供・委託

第三者への個人データの提供にあたっては、法定の例外事項を除き、オプトイン方式又はオプトアウト方式での本人同意の取得を要件としている（同法第27条5項）。但し、「第三者」に該当しない場合を3つ規定しており、その中の1つとして、「利用目的達成に必要な範囲内で個人データの取扱いを委託することに伴い当該個人データが提供される場合」を挙げている（同条同項）。

この委託に該当する場合、その取扱いを委託された個人データの安全管理が図られるよう、委託元が委託先に対し監督責任を負う（同法第25条）。この監督の一環として、委託元に対し、適切な委託先の選定、委託先との安全管理措置等について定めた委託契約の締結、及び委託先における定期的な監査等を通じて個人データ取扱状況を把握するよう定めている。

上述を踏まえ、GDPRで規定する第三者提供を含む取扱いの法令要件と比較すると、個人情報保護法は、オプトアウト方式での本人同意の取得をも要件として認めているが、GDPRは前述の通り明示的同意、即ちオプトイン方式での同意取得のみ適法性の根拠として認める点では異なるといえる。また、個人データ取扱いの委託にあたって、個人情報保護法が委託元の監督責任のみを定め、委託に対する同様の法定義務の規定がない点もまたGDPRとの異なる点であるといえる。

1.1.1.3 保管・管理

個人情報取扱事業者は、「個人データの漏洩、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と規定している（法第23条）。この安全管理措置について通則は別添で、組織的・人的・物理的・技術的な安全管理措置及び外的環境の把握の観点から執るべき具体的な措置を例示している。

併せて、「利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない」としている。

上述を踏まえ、GDPRで規定するデータの安全性と比較すると、個人情報保護法は、主に個人データの漏洩、滅失防止及び正確性の確保といったデータの機密性及び完全性を要求している点で、GDPRと共通するが、一方で、GDPRはデータの可用性についても要求している点では異なるといえる。

1.1.1.4 データローカライゼーション規制

個人情報保護法は、広義のデータローカライゼーション規制の中、海外移転制限について規定している。

個人情報保護法第28条は、外国にある第三者へ個人データを提供する場合、「予め外国にある第三者への提供を認める旨の本人の同意を得なければならない」としており、以下、若干の補足を行う。

同条でいう「外国」については、個人の権利利益を保護する上で、我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として、個人情報保護委員会規則で定める国を除く。現在、同規則で定める国・地域は、令和３年９月時点でEEA及び英国が該当する。[99]

同条でいう「第三者」については、個人データの取扱いについて、個人情報保護法第４章2節の規定により、個人情報取扱事業者が講ずべきこととされている措置に相当する措置（以下、「相当措置」という。）を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。これは同規定により、以下のいずれかに該当する場合と定めている。[100]

a）個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、本法第4章第2節の規定の趣旨に沿った措置の実施が確保されていること（法第28条第1項）。

この場合、当該第三者による相当措置の継続的な実施を確保するため、必要な措置を講ずるとともに、本人の求めに応じて、必要な措置に関する情報を本人に提供しなければならないとしている（法第28条第3項）。これは例えば、提供元が、提供先と、個人データの取扱いに関する契約を締結の上、その履行状況を定期的に確認し、履行困難な場合には、当該契約を解除するということや、提供先の個人情報保護に関する制度の動向について、定期的に確認すること等が想定される。

b）個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。この場合、CBPR（Cross Border Privacy Rules. APEC越境プライバシールールシステム）の認証取得が、例として挙げられている。

また、「外国にある第三者」とは、外国に所在する提供者とは別の法人格を指す。そのため、海外関係会社に個人データを提供する場合、当該第三者に該当するが、同一事業者における外国の事業所に個人データを提供する場合又は外国に設置したサーバに保存する場合には、本条は適用されない。

なお、外国にある事業者が日本国内に設置し運営するサーバへ個人データを保存する場合もまた、外国にある第三者への提供となるが、当該外国の事業者が、当該サーバに保存された個人データを日本国内で取り扱っており、日本国内で個人情報データベース等を事業の用に供していると認められる場合には、外国にある第三者への提供に該当しないことになる。この点、提供先及び提供先が設置するサーバの所在国に応じて、適用される該当条項は、下記表Ⅲ1.1.1.4(1)の通りとなる。[101]

---

[99] 平成31年個人情報保護委員会告示第１号「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国等」でEEA、同告示第5号で英国について、定めている。

[100] APEC/CBPRに基づく認証を受けている場合等が考えられる（第189回国会衆議院内閣委員会会議録第7号〔2015年5月20日〕27頁）

[101] 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ」平成29年２月16日（令和5年5月25日更新）Q12-3乃至Q12-5

表Ⅲ1.1.1.4 (1) 提供先及び提供先設置サーバの所在国により適用される該当条項

提供先	提供先のサーバ設置国	該当条項	補足
(1) 日本に在る第三者	(1)-1 外国	法第27条（第三者提供の制限）	－
	(1)-2 日本	同上	－
(2) 外国に在る第三者	(2)-1 外国	法第28条（外国にある第三者提供の制限）	関係会社でも外国にある場合は左記に該当
	(2)-2 日本	同上	日本国内で、個人データを取扱い、事業の用に供する場合には、当該外国にある第三者は、域外適用を受けるため、法第27条が提供され得る。

併せて、委託、事業承継又は共同利用に伴い個人データを提供する場合、提供先が国内事業の場合、個人情報保護法27条第5項及び第6項が適用され、当該提供先は同条でいう「提供先」に該当しないが、外国にある第三者への提供の場合、同条同項が適用されない。そのため、例えば、外国にある委託先に個人データを提供する場合も、第28条でいう「外国にある第三者への提供」に当たることとなる。

第28条でいう「同意」については、国内の第三者への提供時に認められている個人情報保護法第27条第2項乃至第4項のオプトアウト手続に係る規定は適用されず、予め本人へ以下の情報を提供した上で、本人同意の取得を要する。

1）提供先となる外国の名称
2）適切且つ合理的な方法により得られた当該外国における個人情報保護制度に関する情報
3）提供先である第三者が講ずる個人情報保護のための措置に関する情報

以上、海外移転を行う法令要件をまとめると、下記表Ⅲ1.1.1.4 (2)の通りとなる。

なお、提供元がEEA又は英国に所在し、日本へ個人データを移転する場合、その場合、個人情報保護法、通則その他同法のガイドラインに加えて、「個人情報の保護に関する法律に係るEU及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール(令和5年3月一部改正)」（以下、「補完ルール」という。）に則り、取り扱う必要がある。

表Ⅲ1.1.1.4 (2) 主な海外移転要件及びグローバルヘルスケア法人による移転の実現可能性

	海外移転の法令要件	補足	実現可能性
①	本人へ法定事項を通知の上、当該本人から明示的同意を取得	健康・医療サービスでは、左記の通知・同意措置の設定は比較的容易であり、且つ移転の是非を本人の自己決定に委ねるため、本人の権益保護も図りやすい。	高
②	個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国	左記対象国が現在、EU及び英国のみ（米国、中国その他国・地域は対象外）	中
③	個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制の基準		-
③-1	提供先が、CBPR等国際的枠組みに基づく認定取得済	実際に認められる左記認定の範囲及び認定取得企業の実体数を考えると、現実的には左記活用は限定的である。 （また、EU又は英国から日本へ移転した個人データを他国へ再移転する場合には、補完ルールの趣旨目的を踏まえると、左記要件のみを以て「再移転」することができるのか、疑問が生じる。）	低
③-2	・ 提供先とデータ取扱契約を締結（関係会社間であれば、共通適用されるプライバシーポリシーが存在）し、その履行状況の定期的確認（不履行の場合、契約解除も検討） ・ 提供先国の法動向の定期的確認 ・ 本人の求めに応じ、必要な措置に関する情報を本人に提供可能な仕組みの整備	移転先の現地企業・組織を実質管理監督していく必要があるといえ、そのためある程度の管理コストをみておく必要がある。	中

1.1.1.5 体制・責任者

後述するGDPRで定めるData Protection Officer: DPOのような制度はない。

一方で通則では、組織体制として講じるべき措置の例示として、個人データの取扱いに関する責任者の設置及び責任の明確化、法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合の責任者への報告連絡体制、個人データの漏えい等事案の発生又は兆候を把握した場合の責任者への報告連絡体制の整備等を挙げている。

1.1.1.6 本人の権利

個人情報取扱事業者は、名称、住所、代表者の氏名、保有個人データの利用目的、本人からの開示等の請求に応じる手続、適正な取扱いの確保に関する法定事項（安全管理措置、苦情の申出先等）について、ホームページへ掲載する等、本人の知り得る状態に置かなければならない（個人情報保護法第32条第1項）。

開示等の請求とは、保有個人データの開示、内容の訂正、利用停止、第三者への提供の停止、第三者提供記録の開示、又は消去の請求をいう。個人情報取扱事業者が、これらの請求又は利用目的の通知を求められた場合、法定の例外事項を除き、当該請求又は求めに応じなければならない。なお、利用停止の請求が、個人情報保護法第20条第2項の規定に違反し、本人同意なく要配慮個人情報が取得されたものであるという理由によって行われた場合もまた、原則として遅滞なく応じなければならない。

1.1.1.7 データ侵害・インシデント

個人情報取扱事業者は、その取り扱う個人データの漏洩、滅失、毀損（以下、「漏洩等」という。）その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、同規則に則り、個人情報保護委員会に報告しなければならない。

この「個人の権利利益を害するおそれが大きいもの」として同規則で定めるものは、次の各号のいずれかに該当するものである。

(1) 要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。）の漏洩等の発生又はその虞のある事態

(2) 不正に利用されることにより財産的被害が生じる虞がある個人データの漏漏洩等が発生又はその虞がある事態

(3) 不正の目的をもって行われた虞がある個人データの漏洩等が発生し、又はその虞がある事態

(4) 個人データに係る本人の数が千人を超える漏洩等が発生し、又は発生した虞があること

1.2 センシティブ情報の取扱いに対し法令要件を厳格化される局面及びその加重要件

要配慮個人情報が、一般的な個人情報の法令要件に比し、厳格化される局面として、次の通り4つ挙げられる。

1つ目として、取得の局面が挙げられる。要配慮個人情報を取得する場合には、法定の例外事項を除き、本人からの明示的同意を要する（法第20条第2項）。

2つ目として、第三者提供時の同意取得の方法が挙げられる。要配慮個人情報を第三者に提供する場合には、オプトアウト方式での同意は認められず、オプトイン方式での本人からの明示的同意を要する（法第2条第2項）。

3つ目として、事故発生時の対応の局面が挙げられる。要配慮個人情報において漏洩等の事故が発生した場合、高度な暗号化その他の本人の権益保護の措置を講じている場合を除き、当局（個人情報保護委員会）及び本人への報告を要する。なお、一般的な個人情報において漏洩等の事故が発生した場合、不正利用（財産的被害）の虞がある事故、不正目的での事故、又は千人超といった比較的規模の大きな事故に限り、当局及び本人への報告を要する（法第26条）。

4つ目として、本人の権利行使への対応の局面が挙げられる。上述の1つ目に挙げた本人同意を経ずに取得された場合に、本人から利用停止又は消去の請求があるときには、原則それに応じなければならない（法第35条）。

以上をまとめると下記表の通りとなる。

表Ⅲ1.2 取扱局面毎の主な法令要件とセンシティブ情報に対する要件の厳格化（日本）

局面	一般的な個人情報の主な法令要件	センシティブ情報の主な加重要件	
取得	ⅰ）利用目的の特定 ⅱ）本人への利用目的の公表又は通知(明示)* （* 直接書面による取得の場合）	○	本人から明示的同意の取得（オプトイン方式での同意取得）
利用	ⅰ）目的外利用の禁止 ⅱ）不適正利用の禁止	N/A	－
提供	ⅰ）本人同意の取得 a）オプトイン b）オプトアウト（法定通知事項有り） ⅱ）第三者提供に係る法定記録の保管	○	オプトアウトでの同意取得禁止
越境	ⅰ）本人への通知＋本人からの明示的同意の取得 ・ 又は、十分性認定 ・ 又は、CBPR等国際的枠組みに基づく認定取得済 ・ 又は、提供先とのデータ取扱契約の締結*、その履行状況の定期的確認及び提供先国の法動向の定期的確認、並びに本人の求めに応じ、必要な措置に関する情報を本人に提供可能な仕組みの整備（*関係会社間であれば、共通適用されるプライバシーポリシーも可） ⅱ）越境に係る法定事項の記録保管	N/A	－
保管	安全管理措置（機密性＋完全性(正確性)の確保*） *可用性は法定無し	N/A	－
体制	個人データの取扱いに関する責任者の設置	N/A	－
権利行使	ⅰ）法定事項の公表 ・ 組織名・住所・代表者名、利用目的、安全管理措置、権利行使の手続、苦情窓口 ⅱ）権利行使時の対応 ・ 利用目的の通知、個人情報の開示、訂正、消去、利用・第三者提供の停止	○	取得時の本人同意未取得に対する利用停止又は消去の請求
事故対応	下記該当の場合、当局（個人情報保護委員会） ・ 本人へ通知 ⅰ）不正利用されることにより財産的被害が生じる虞あり ⅱ）不正の目的をもって行われた虞あり ⅲ）千人超の漏洩等の虞あり ⅳ）要配慮個人情報を含む漏洩等の虞あり	○	左記ⅳ)に該当するため、当局・本人への報告必須（高度な暗号化等本人の権益保護の措置を講じている場合を除く）

○: 該当, N/A: 非該当

1.3 仮名化及び匿名化

個人情報保護法は、仮名加工情報と匿名加工情報について規定している。

1.3.1 仮名化

令和2年の個人情報保護法改正により、仮名加工情報が新設された。

2015年の同法改正により、既に匿名加工情報が導入されたが、個人情報取扱事業者において、一定の加工を施すことによる安全性を確保した上で、匿名加工情報よりもデータの有用性を保ち、詳細な分析ができるようにすることを目的として、仮名加工情報が導入された。

仮名加工情報とは、「他の情報と照合しない限り特定の個人を識別することができないよう、個人情報を加工して得られる個人に関する情報」をいう（個人情報保護法第2条第5項）。

当該仮名加工は、法定の基準に従い、個人情報に含まれる氏名、生年月日その他の記述等の一部を削除し、また当該個人情報に個人識別符号が含まれる場合は、当該個人識別符号の全部を削除することにより行う。併せて、当該個人情報に不正に利用されることにより財産的被害が生じる虞のある記述等、例えばクレジットカード番号等が含まれる場合には、その削除も要する。

また、「他の情報と照合しない限り特定の個人を識別することができない」という要件は、加工後の情報それ自体により特定の個人を識別することができないような状態にすることを求めるものであり、当該加工後の情報とそれ以外の他の情報を組み合わせることによって特定の個人を識別することができる状態にあることを否定するものではない。

そのため、仮名化個情報には、表Ⅲ1.3の通り、「個人情報である仮名加工情報」と、「個人情報でない仮名加工情報」の2つが存在する。

前者は、仮名加工情報取扱事業者[102]において、仮名加工情報の作成の元となった個人情報や、当該仮名加工情報に係る削除情報等[103]を保有している等により、当該仮名加工情報が、「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」状態にある仮名加工情報をいう。

一方、後者は、例えば、法第41条第6項又は第42条第1項若しくは第2項の規定により、仮名加工情報の提供を受けた仮名加工情報取扱事業者において、当該仮名加工情報の作成の元となった個人情報や、当該仮名加工情報に係る削除情報等を保有していない等により、当該仮名加工情報が「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」状態にない仮名加工情報をいう。

なお、要配慮個人情報を含む個人情報を加工し、仮名加工情報を作成することも可能である。[104]

但し、仮名加工情報は、法令で定める場合を除き、第三者提供は禁止されている。

---

[102] 仮名加工情報取扱事業者とは、仮名加工情報データベース等を事業の用に供している者のうち、国の機関、地方公共団体、法令で規定する独立行政法人等をいう（個人情報保護法第16条第5項）。

[103] 「削除情報等」とは、仮名加工情報の作成に用いられた個人情報から削除された記述等、及び個人識別符号、並びに個人情報保護委員会規則の則り行われた加工の方法に関する情報をいう（匿名加工情報・匿名加工情報編 2-2-1）
https://www.ppc.go.jp/files/pdf/220908_guidelines04.pdf

[104] 匿名加工情報・匿名加工情報編 4-1-2 A14-6（https://www.ppc.go.jp/files/pdf/2205_APPI_QA.pdf）。

1.3.2 匿名化

匿名加工情報とは、特定の個人を識別することが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、当該個人情報を復元することができないようにしたものをいう。このため、匿名加工情報は、個人情報に該当しない。また、匿名加工情報と異なり、法令で定めた例外事項に該当するしないにかかわらず、第三者へ提供することができる。

当該匿名加工は、法定の基準に従い、特定の個人を識別することができなくなるように当該個人情報に含まれる氏名、生年月日その他の記述等を削除し、また当該個人情報に個人識別符号が含まれる場合は、当該個人識別符号の全部を特定の個人を識別することができなくなるよう削除することにより行う。

この「削除すること」には、「当該一部の記述等」又は「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」とされる。

「復元することのできる規則性を有しない方法」とは、置き換えた記述から、置き換える前の特定の個人を識別することとなる記述等又は個人識別符号の内容を復元することができない方法である。

また、「特定の個人を識別することができない」という要件は、あらゆる手法によって特定することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人 及び一般的な事業者の能力、手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者[105]が通常の方法により特定できないような状態にすることを求めるものである。

また、「当該個人情報を復元することができないようにしたもの」とは、通常の方法では、匿名加工情報から匿名加工情報の作成の元となった個人情報に含まれていた特定の個人を識別することとなる記述等又は個人識別符号の内容を特定すること等により、匿名加工情報を個人情報に戻すことができない状態にすることをいう。

「当該個人情報を復元することができないようにしたもの」という要件は、あらゆる手法によって復元することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人及び一般的な事業者の能力、手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により復元できないような状態にすることを求めるものである。

なお、「統計情報」は、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに 集計して得られるデータであり、集団の傾向又は性質などを数量的に把握するものである。従って、統計情報は、特定の個人との対応関係が排斥されている限りにおいては、法における「個人に関する情報」に該当するものではないため、個人情報保護法による規制の対象外となる。

1.3.3 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和

個人情報取扱事業者が取り扱う個人情報に対し、局面毎に概ね19個の法令要件が適用される。

これに対し、個人情報取扱事業者である仮名加工取扱事業者が取り扱う個人情報である仮名加工情報に対して、局面毎に適用される法令要件は概ね14個であり、前者での約26%、即ち約4分の1に当たる法令要件が非適用となる。主に非適用となるのは、利用、本人からの権利請求への対応、及び漏洩等事故時の対応に関する局面においてである。具体的には、利用目的変更の制限、保有個

[105] 匿名加工情報取扱事業者とは、匿名加工情報データベース等を事業の用に供している者のうち、国の機関、地方公共団体、法令で規定する独立行政法人等をいう（個人情報保護法第16条第6項）。

人データに関する事項の公表、本人からの開示等の請求への対応、及び漏洩等事故時の監督機関（個人情報保護委員会）への報告及び本人への通知に関する法令要件が非適用となる。

更に仮名加工事業者が遵守する個人情報でない仮名加工情報の取扱いに対して、適用される法令要件は、概ね8個であり、上述の個人情報に対し適用される法令要件の約58%、即ち約6割が非適用となる。

上述の個人情報である仮名加工情報において非適用となる法令要件に加えて、取得及び一部保管時における局面でもまた非適用となる法令要件がある。具体的には、利用の局面において、適正取得及び要配慮個人情報の取得、保管・管理の局面において、個人データ内容の正確性の確保及び利用の必要がなくなった個人データの消去、並びに利用時の不適正利用及び目的外利用の禁止が、個人情報である仮名加工情報において非適用となる法令要件に加え、更に非適用となる法令要件である。

このように仮名加工情報は、仮名加工情報取扱事業者内での2次的な利活用を促進するにあたり、利用の局面及び本人からの権利請求への対応の局面における義務を緩和するとともに、仮名加工により一定の安全管理措置を講じていることから、漏洩等事故時の局面で事故対応の義務も緩和している。併せて、個人情報でない仮名加工情報には、更に取得の局面及び保管管理の局面においても一部義務を緩和しており、概ね全ての局面において義務を緩和しているといえる。但し、仮名加工情報の制度は、仮名加工を施していることを前提としていることからも、識別行為を禁止していることと併せて、仮名加工情報取扱事業者が、自組織内においての利活用促進を主な目的としていることから、本人からの明示的同意に基づく第三者提供についても禁止している。

他方、匿名加工取扱事業者が取り扱う匿名加工情報に対して、局面毎に適用される法令要件は概ね3個であり、個人情報取扱事業者が取り扱う個人情報における約84%の法令要件が非適用となる。このように大半の法令要件が非適用となる中、利用の局面において、識別行為の禁止、保管管理の局面において、匿名加工方法に関する安全管理措置、及び匿名加工情報に関する安全管理措置や苦情処理等の措置を自主的に講じて公表する義務等が規定されている。

上述から、仮名加工情報と匿名加工情報は、加工処理により本人の権益保護を図った上で、個人情報に比べ、その取扱事業者の義務を緩和していることから、特定の個人を識別する行為を禁止することと併せて、それを担保するための安全管理措置を執ること、また本人への説明責任、及び万が一法定義務の不履行がある場合、それを把握するためにも、苦情処理を行う義務を負う必要がある、という点で共通する。

以上をまとめると下記表の通りとなる。

表Ⅲ1.3 仮名加工情報と匿名加工情報において、適用される法令要件の比較

局面	取扱要件	仮名加工情報 (個人情報である)	仮名加工情報 (個人情報でない)	匿名加工情報
取得	・ 適正取得	○	NA	NA
	・ 利用目的の公表	○	NA	NA
	・ 要配慮個人情報取得時の同意	○ 注）	NA	NA
委託	委託先の監督	○	○	NA
提供	・第三者提供の禁止	○	○	NA (但,公表義務あり)
	・第三者提供時の記録	NA 注）	NA	NA
越境	海外第三者提供の禁止	○	○	NA
保管管理	・ 安全管理措置	○	○	○
	・ 従業者の監督	○	○	NA
	・ 正確性の確保・不要時消去の努力義務	○	NA	NA
利用	・ 不適正利用の禁止	○	NA	NA
	・ 利用目的変更の制限	NA	NA	NA
	・ 目的外利用の禁止	○	NA	NA
	・ 識別行為の禁止	○	○	○
	・ 本人への連絡等の禁止	○	○	NA
権利行使	・ 法定事項の公表	NA	NA	NA
	・ 権利行使への対応	NA	NA	NA
	・ 苦情処理	○	○	○ （努力義務）
事故	監督機関への報告／本人通知	NA	NA	NA

○: 該当, N/A: 非該当

注）仮名加工情報は、仮名加工情報取扱事業者が、本人から取得した個人情報に対し、法定基準に則った仮名加工処理を施し生成する。そのため、仮名加工情報を「取得」するという局面とは、仮名加工事業者が、仮名加工情報を第三者へ提供し、当該第三者が当該情報を「取得」することである。仮名加工情報の第三者提供は、原則禁止されているが、法定事項に該当する場合は認められている。なお、当該法定事項に該当する場合は、要配慮個人情報の取得にあたって、本人から明示的同意を取得するという法令要件や、第三者提供時の記録保管義務が無い。

2. EU

2.1 一般的な個人情報の取扱いに対する規制

2.1.1 EU域内における個人データ取扱いに関する主な法令要件

GDPRは、局面毎というよりむしろ、取扱い全般に対する基本原則を定めた上で、データ主体の権利、並びにデータを取り扱う者としてのデータ管理者及びデータ処理者に対する義務を規定している。

2.1.1.1 取扱いの基本原則

GDPR第4条第２項では、「取扱い」について、「自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しく は変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、個人データ実施される業務遂行を意味する。」と定義している。

GDPRは、日本の個人情報保護法のように取扱いの局面毎において、個人情報取扱事業者に対し、個人データの取扱い手順を定めているというよりむしろ、個人データの取扱い局面全般において、その取扱いに関する基本原則を定めた上、それら原則に基づき、データ管理者及びデータ処理者に対しては、取扱い及び管理上の義務を定め、データ主体に対しては、個人データに関する権利を与えている、といった建付けになっている。

まず、個人データの取扱いに関する基本原則として、以下7つ定めている。

1）適法性、公正性、及び透明性:

データ主体との関係において、適法、公正、及び透明性をもって取扱うこと

2）目的の限定:

特定された、明確且つ正当な目的のために収集されること、並びにその目的に適合しない態様での追加的取扱いをしないこと

3）データの最小化:

取扱う個人データが、取扱う目的との関係上、十分であり、関連性があり、かつ、必要のあるものに限定されること

４）正確性:

正確且つ最新の状態に維持し、取扱う目的を考慮した上で、遅滞なく、不正確な個人データが消去又は訂正されるための手立てを講じること。

5）記録保存の原則:

取扱う目的のために必要な期間だけ、データ主体の識別を許容する方式を維持すること

6）完全性及び機密性:

無権限による取扱い若しくは違法な取扱い、並びに偶発的な喪失、破壊又は損壊に対して、個人データの適切な安全性を確保する態様により、取扱われること

7）アカウンタビリティー:

データ管理者は、上記1）乃至6）について責任を負い、遵守を証明できるようにすること

2.1.1.2 取扱いの適法性

上述の基本原則に基づき、個人データの取扱いにおいては、適法性が要求される。GDPR第７条では、以下いずれかに該当する場合、適法性の根拠があると定めている。

1）データ主体が、特定の目的のための個人データの取扱いに関して、同意を与えた場合
なお、同意の要件も規定されている。

2）データ主体との契約履行のために取扱いを要する場合、又は契約締結前にデータ主体の要求に応じるため取扱いを要する場合

3）管理者が服する法的義務を遵守するために取扱いを要する場合

4）データ主体又は他の自然人の生命に関する利益を保護するために取扱いが必要となる場合

5）公共の利益、又は公的権限の行使のための職務遂行で取扱いを要する場合

6）管理者又は第三者の正当な利益のために取扱いを要する場合。但し、その利益より、データ主体の利益並びに基本的権利及び自由が優先する場合、特にデータ主体が子供である場合を除く。

2.1.1.3 データ管理者の義務

データ管理者は、GDPRに基づいた取扱いの遂行を確保し、かつそれを説明可能にするための適切な技術上及び組織上の措置、及びプライバシーポリシー等の適切なデータ保護方針を実装した上、それらの措置を必要に応じ、適宜最新に改める義務を負う（GDPR第24条）。

上述を踏まえ、GDPR第25条は、データ管理者に対し、データ保護バイデザイン及びデータ保護バイデフォルトの義務を次の通り定めている。

まずデータ保護バイデザインとして、データ管理者は、GDPRの規定する要件に適合し、かつデータ主体の権利を保護するため、データ最小化のようなデータ保護の基本原則を実装し、データ保護措置を統合するために設計された、仮名化のような、適切な技術的措置及び組織的措置を実装する義務を負う。

その上で、データ管理者は、取扱目的に必要な個人データのみが取扱われることをデフォルトで確保するための適切な技術的措置及び組織的措置を実装することが義務付けられている。この義務は、収集される個人データの分量、その取扱いの範囲、その記録保存期間及びアクセス可能性に適用され、とりわけそのような措置は、個人データが、その個人の関与なく、不特定の自然人からアクセスすることができないような措置のデフォルトでの確保を要する。

加えて、取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させる虞のある場合、データ管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響評価の実施を要する。その評価結果が、自然人の権利及び自由に対し高リスクをもたらす虞のあることを示す場合、データ管理者は、その取扱いを開始する前に、監督機関と協議する必要がある。

なお、管理者の代わりの者に取扱いを行わせる場合、その管理者は、当該取扱いがGDPRに適合すべく適切な技術上及び組織上の保護措置を実装することに十分な保証を提供する処理者のみを用い、かつデータ主体の権利保護を確保しなければならない。

GDPRは、データ管理者のみならず、当該データ処理者に対しても義務を課している。

2.1.1.4 データ処理者の義務

データ処理者は、管理者から指示がない限り、当該個人データを取扱ってはならない。またデータ処理者は、データ管理者から個別的又は一般的な書面による事前承認を得ることなく、別のデータ処理者を業務に従事させてはならず、一般的な書面による承認の場合、データ処理者は、データ管理者に対し、別のデータ処理者の追加又は交代に関する変更の予定を通知し、データ管理者に異議を述べる機会を与えなければならない。

データ管理者とデータ処理者は、GDPRで定める法定事項を約定した契約の締結を要し、データ処理者は、その契約に従い個人データの取扱いを行う。またデータ処理者は、別のデータ処理者を業務に従事させる場合、データ管理者と締結した契約と同等の契約を当該別のデータ処理者と締結し、その契約履行に対して、全面的な法的義務を負う。

2.1.1.5 データ管理者及びデータ処理者の両方にかかる義務

EU域外の企業その他組織が、データ管理者又はデータ処理者としてGDPRの域外適用を受ける場合、当該データ管理者又はEU域内における代理人の指定を要する。

データ管理者及びその代理人は、GDPRで定める事項を含む取扱いについての記録の保管を要する。またデータ処理者及びその代理人も、管理者の代わりに行う、GDPRで定める事項を含む全種類の取扱いについての記録を保管する。

データ管理者及びデータ処理者は、リスクに適切に対応する一定のレベルの安全性を確保するために以下を含め、適切な技術上及び組織上の措置を実装する。

a) 個人データの仮名化又は暗号化
b) 取扱うシステム及びサービスの機密性、完全性、可用性及び回復性を確保する能力
c) インシデントが発生時、個人データの可用性及びそれへのアクセスの復旧能力
d) 安全性を確保するための技術上及び組織上の措置の有効性を確認する定期評価の手順
e) GDPRで法定する条件下におけるデータ保護オフィサーの指名

2.1.1.6 データ主体の権利

データ管理者は、個人データを取得するにあたって、データ主体に対し、その取扱いに関する情報の提供を要する。データ主体へ提供する情報項目は、そのデータ主体から個人データを直接取得する場合と、そうでない場合とで異なり、表Ⅲ2.1.1.6の通り、GDPRで法定されている。

その上で、データ主体は、データ管理者に対し、以下の権利を有する。

1) 自身に関係する個人データを取り扱っているか確認の上、取り扱われているときは、その個人データ、及び表Ⅲ2.1.1.6の1) C)、F)、及びa)、b)、d)、f)、並びに2) D)、及びf)に関する情報にアクセスする権利
2) 不正確な個人データを訂正させ、また取扱いの目的を考慮に入れた上で、補足の陳述を提供する方法による場合を含め、 不完全な個人データを完全なものとさせる権利
3) 以下いずれかに該当場合、個人データを消去させる権利（忘れられる権利）

a) 収集・取扱目的の達成に不要となっている場合

b）第6条(取扱いの適法性)第1項(a)又は第9条(特別な種類の個人データの取扱い)第2項(a)に従い、その取扱いの根拠である同意を撤回し、かつその取扱いのための法的根拠が他に存在しない場合

c）そのデータ主体が、第21条(異議を述べる権利)第1項によって取扱いに対する異議を述べ、かつ、その取扱いのための優先する法的根拠が存在しない場合、又は同条条第2項によって異議を述べた場合

d）個人データが違法に取扱われた場合

e）個人データが、管理者がEU又はEU域内の各国法的義務を遵守するために消去を要する場合

f）個人データが、第8条(情報社会サービスとの関係において子どもの同意に適用される要件)第1項に定める情報社会サービスの提供との関係において収集された場合

4）以下いずれかに該当する場合、個人データの取扱いを制限する権利

a）個人データの正確性について疑義を提示している場合（その正確性を管理者が確認することができる期間内において取扱いを制限）

b）取扱いが違法であり、かつデータ主体が個人データの消去に反対し、その代わり、そのデータの利用の制限を求めている場合

c）管理者がその取扱目的のために個人データを必要としないが、訴訟の提起及び攻撃防御のためにそのデータを求める場合。

d）管理者の正当性の根拠がデータ主体の正当性の根拠よりも優先するか否かの確認を争い、第21条(異議を述べる権利)第1項により、取扱いに対する異議を申立てている場合訟の提起及び攻撃防御のためにそのデータを求める場合

5）第6条(取扱いの適法性)第1項(a)、若しくは第9条(特別な種類の個人データの取扱い)第2項(a)による同意、又は第6条第1項(b)による契約に基づくものであり、かつその取扱いが自動化された手段によって行われる場合は、個人データを構造化し、一般的に利用され機械可読性のある形式で受け取り、またその提供を受けた管理者から妨げられることなく別の管理者に対し、それらの個人データを移行する権利（データポータビリティの権利）。この権利には、技術的に実行可能な場合には、ある管理者から別の管理者へと直接に個人データを移行させる権利も含む。なお、この権利行使は、上述の「忘れられる権利」の行使を妨げない。

6）以下いずれかに該当する場合、異議を述べる権利

a）第6条(取扱の適法性)第1項(e)又は(f)に基づき、個人データを取扱う場合（同条項に基づきプロファイリングを行う場合も含む）

b）ダイレクトマーケティングの目的のために個人データが取扱われる場合（ダイレクトマーケティングと関係するプロファイリングを含む）

c）第89条(公共の利益における保管の目的、科学調査若しくは歴史調査の目的又は統計の目的のための取扱いと関連する保護措置及び特例)第1項により科学的研究若しくは歴史的研究の目的又は統計の目的で個人データが取扱われる場合（但し、公共の利益のための理由によって行われる職務の遂行のためにその取扱いが必要となる場合を除く）

7）専ら自動化された取扱いに基づいた決定の対象とされない権利（データ主体に関する法的効果を発生させる、又は当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含む）。但し、以下いずれかに該当する場合を除く。

a）データ主体とデータ管理者間の契約締結又はその履行のために必要な場合
b）データ管理者が服するEU方又は加盟国法によって認められる場合
c）データ主体の明示的な同意に基づく場合

なお、第9条(特別な種類の個人データの取扱い)第2項(a)又は(g)が適用され、且つデータ主体の権利及び自由並びに正当な利益の保護を確保するための適切な措置が設けられている場合を除き、上記a)乃至c)いずれかに該当するかどうかの決定は、同条第1項に規定する特別な種類の個人データを基礎としてはならない。

2.1.1.7 データ侵害・インシデント

個人データ侵害が発生した場合、データ管理者は、原則、その侵害に気づいた時から遅くとも72時間以内に所轄監督機関に対して、以下に関する通知しなければならない。

a）関係するデータ主体の類型及び概数、並びに関係する個人データの種類及び概数を含め、個人データ侵害の性質
b）データ保護オフィサーの名前及び連絡先、又はより多くの情報を入手することのできる他の連絡先
c）その個人データ侵害の結果として発生する虞のある事態
d）起こりうる悪影響を低減させるための措置を含め、その個人データ侵害に対処するため、データ管理者が講じた措置又は講ずるよう提案した措置

併せて、個人データ侵害が、データ主体の権利及び自由に対する高いリスクを発生させる虞のある場合、データ管理者は、そのデータ主体に対して、上記b)乃至d)の連絡をしなければならない。但し、以下いずれかに該当する場合を除く。

1）管理者が適切な技術上及び組織上の保護措置を実装しており、かつ、当該措置、特に暗号化のような、データに対するアクセスが承認されていない者にはその個人データを識別できないようにする措置が、 個人データ侵害によって害を受けた個人データに対して適用されていた場合。
2）管理者が、第1項で定めるデータ主体の権利及び自由に対する高いリスクが具体化しないようにすることを確保する事後的な措置を講じた場合。
3）それが過大な負担を要するような場合。そのような場合、データ主体が平等に効果的な態様で通知されるような広報又はそれに類する方法に変更される。

表 Ⅲ2.1.1.6 個人データを取得するにあたって、データ主体に情報提供すべき主な事項

1）データ主体から個人データが取得される場合において提供される情報	2）個人データがデータ主体から取得されたものではない場合
A）データ管理者の身元及び連絡先、及び管理者の代理人を設置する場合、その身元及び連絡先 B）データ保護オフィサーを設置する場合、連絡先 C）個人データの取扱い目的、及びその取扱いの法的根拠 D）その取扱いがGDPR第6条第1項(f)を根拠とする場合、データ管理者又は第三者が求める正当な利益 E）個人データの取得者又は取得者の類型 F）データ管理者が、個人データを第三国又は国際機関に移転する場合、その事実、及び欧州委員会による十分性認定の存否、又は第46条(適切な保護措置に従った移転)若しくは第47条(拘束的企業準則)に定める移転を行うとき、又は第49条(特定の状況における例外)第1項及び第2項後段に定める移転のときには、適切又は適合する保護措置、及びその複製物を取得するための方法、又はどこでそれらが利用可能とされたかについての情報 上記の付加的な情報としての以下の項目; a）その個人データが記録保存される期間又はそれが不可能なときは、その期間を決定するために用いられる基準 b）個人データへのアクセス、個人データの訂正又は消去、又はデータ主体と関係する取扱いの制限をデータ管理者から得ることを要求する権利、又は取扱いに対して異議を述べる権利、並びにデータポータビリティの権利が存在すること c）その取扱いが第6条(取扱いの適法性)第1項(a)又は第9条(特別な種類の個人データの取扱い)第2項(a)に基づく場合、その撤回前の同意に基づく取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利が存在すること d）監督機関に異議を申立てる権利 e）その個人データの提供が制定法上若しくは契約上の要件であるか否か、又は、契約を締結する際に必要な要件であるか否か、並びに、データ主体がその個人データの提供の義務を負うか否か、及びそのデータの提供をしない場合に生じうる結果について f）プロファイリングを含め、第22条第1項及び第4項に定める自動的な決定が存在すること、また、これが存在する場合、その決定に含まれている論理、並びに、当該取扱いのデータ主体への重要性及びデー タ主体に生ずると想定される結果に関する意味のある情報	A）同左 B）同左 C）同左 D）個人データの種類 E）同左 F）同左 上記の付加的な情報としての以下の項目; a）同左 b）同左 c）同左 d）同左 e）同左 f）どの情報源からその個人データが生じたか、及び、該当する場合、公衆がアクセス可能な情報源からその個人データを取得したものかどうか g）左記f)と同じ

2.1.1.8 データローカライゼーション規制

GDPRは、日本同様、広義のデータローカライゼーション規制の中、海外移転制限について規定している（GDPR第5章 第三国又は国際機関への個人データの移転）。同規定では、データ保護移転を行うための3段階の移転方法が設けられている。

第 1 の移転方法として、第 45 条第 1 項で「十分性に基づく移転」と題し、「第三国、第三国内の地域又は一若しくは複数の特定の部門、又は、国際機関が十分なデータ保護の水準を確保していると欧州委員会が決定した場合、当該第三国又は国際機関への個人データの移転を行うことができる。その移転は、いかなる個別の許可も要しない。」と規定している。欧州委員会が当該十分性決定を下した国は、日本を含め 14 カ国ある。[106]

第 2 の移転方法として、第 46 条第 1 項で「適切な保護措置に従った移転」と題し、「第 45 条第 3 項による決定がない場合、管理者又は処理者は、その管理者又は処理者が適切な保護措置を提供しており、かつ、データ主体の執行可能な権利及びデータ主体のための効果的な司法救済が利用可能なことを条件としてのみ、第三国又は国際機関への個人データを移転することができる。」と規定している。これは、十分性決定が得られていない場合における第 2 段階の移転手段と位置付けられる。この手段には、監督機関の許可を要するものと要さないものがあり、前者には拘束的企業準則"BCR" (Binding Corporate Rules)、後者には標準データ保護条項"SCC" (Standard Contractual Clauses)がある。BCR は主に多国籍企業を対象としており、監督機関により法的に執行可能であること、法令順守を運用する等実践的であること等に留意した「国際データ流通に対する拘束的企業準則」を策定し、EU 内の監督機関が当該ルールを許可した場合、多国籍企業間でのデータ流通が認められるという手段である。一方、SCC は、欧州委員会が認めた契約に基づく移転手段である。SCC の有効性が欧州司法裁判所で審議されてきたが、2020 年 7 月、有効と判断された。

EDPB(European Data Protection Board) が、2020 年 11 月、「第三国への個人データ移転のための SCC に関する決定」の案文を公表しており、本決定の別紙に SCC の改定版が示されている。具体的には、①管理者から管理者への移転、②管理者から処理者への移転、③処理者から処理者への移転、及び④処理者から管理者への移転の 4 つの契約条項が用意されている。

当該 SCC 改定版においては、2020 年 7 月の欧州司法裁判所 Scherms II 判決を受けて、データ移転の具体的な状況等、移転先の第三国の法令と実務、補完的措置の内容を評価した上で、当局の要求に備えて文書で記録しておくという Transfer Impact Assessment: TIA（以下、「TIA」という。）が明文化されている（Clause 14(b)(d)）。具体的には、以下の要素について適切に考慮する必要があると規定している。

① 移転の具体的な状況（処理の連鎖の長さ、関与する関係者の数、及び使用される伝送経路を含む）、意図されている転送、受領者の種類、処理の目的、移転される個人データの種類及び様式、移転が行われる事業部門、移転されるデータの保管場所
② 移転の具体的な状況、及び適用される制限・保護措置を踏まえた、移転先の第三国の法令及び実務（公的機関へのデータの開示を要求し、又は当該機関による閲覧を許可するものを含む）

[106] 個人情報保護委員会ホームページ参照（https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/）

③ 移送中及び移送先国での個人データの処理に適用される措置を含む、SCC に基づく保護措置を補完するために講じられる 契約上の保護措置又は技術的若しくは組織的な保護措置[107]

第 3 の移転方法として、第 49 条第 1 項で「特定の状況における例外」と題し、「第 45 条第 3 項による十分性認定がない場合、又は拘束的企業準則を含め、第 46 条による適切な保護措置がない場合、以下いずれかを満たしている場合においてのみ、第三国又は国際機関への個人データの移転又は個人データ移転の集合を行うことができる。」と規定している。

a）十分性認定及び適切な保護措置が存在しないために、そのような移転がそのデータ主体に対して発生させる可能性のあるリスクの情報提供を受けた後に、そのデータ主体が、提案された移転に明示的に同意した場合

b）データ主体と管理者との間の契約の履行のためにその移転が必要となる場合、又は、データ主体の要求により、契約締結前の措置を実施するためにその移転が必要となる場合

c）管理者及びそれ以外の自然人若しくは法人との間でデータ主体の利益のために帰する契約の締結、又は、その契約の履行のために移転が必要となる場合

d）公共の利益の重大な事由の移転が必要となる場合

e）法的主張時の立証、行使又は抗弁に移転が必要となる場合

f）データ主体が物理的又は法的に同意を与えることができない場合において、データ主体又はそれ以外の者の生命に関する利益を保護するために移転が必要となる場合

なお、上述a)乃至f)と、適法性の根拠となる要件を比較すると、全 8 要件の中、6要件(75%)が概ね同じ要件といえるが、「データ管理者又は第三者の正当な利益の目的」は、適法性の根拠の要件とはなり得るが、上述の特定の状況における例外の要件とはなりえないことがわかる。

[107] 注1) TIA: Data Transfer Impact Assessment (データ移転影響評価). TIAを通じ、移転先国における法制度の確認や、個人情報の保護のレベルを強化するために必要な追加的補充措置等をSCCに規定した上で、SSCを締結。

注2) 移転先に対するセンシティブデータの制限・保護措置義務(含追加的保護措置,開示に対する追加的制限）（21/6/4欧州委員会「第三国への個人データ移転のためのSCCに関する決定」による改訂版SCC「Clause8.6」に規定）

表Ⅲ2.1.1.8(1)特定の状況における例外による海外移転の要件と、適法性の根拠となる要件比較

	適法性根拠の要件	特定の状況における例外の要件
①	本人への情報提供(利用目的含む)及び本人の明示的同意	本人への情報提供（十分性認定及び適切な保護措置が存在しないことによる移転リスク）＋本人の明示的同意
②	本人が契約当事者となっている契約履行、又は契約締結前に本人の要求に際しての手段の実施	本人と管理者間の契約履行、又はデータ主体の要求により契約締結前の措置の実施
③	N/A	管理者と第三者間で、データ主体の利益となる契約締結、又はその契約履行
④	公共の利益、又は管理者による公的権限の行使	公共の利益の重大な事由
⑤	管理者における法的義務の遵守	法的主張時の立証、行使又は抗弁
⑥	本人その他自然人の生命保護	本人が物理的又は法的に同意を与えることができない場合、本人その他自然人の生命保護
⑦	N/A	EU法又は加盟国の国内法に従い、公衆に対して情報を提供することを予定しており、かつ公衆一般及び正当な利益をもつことを説明することのできる者の両者に対して開かれているが、個々の案件において、照会に関してEU法又は加盟国の国内法により定められた条件が充足する限度内のみに制限されている登録機関に限り、登録機関からの移転が必要となる場合
⑧	データ管理者又は第三者の正当な利益の目的。 但し、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的権利及び自由のほうが優先する場合、特にそのデータ主体が子どもである場合を除く。	N/A

上述及び表Ⅲ2.1.1.8(1)を踏まえ、グローバルヘルスケア法人が、個人データを海外移転するにあたって、自律的に具備し得る主な法令要件と、それらの実現可能性をまとめると下記の通りである。

表Ⅲ2.1.1.8(2) 主な海外移転要件及びグローバルヘルスケア法人による移転の実現可能性

	海外移転の法令要件	補足	実現可能性
①	十分性認定に基づく移転	左記対象国が現在、日米欧中の中、英国と日本のみ（米国、中国その他国・地域は対象外）	中
②	適切な保護措置に従った移転		ー
②-1	拘束的企業準則（Binding corporate rules: BCR）	監督機関の承認を要するため、相当程度の負荷・管理コスト要	低
②-2	・ データ移転影響評価（Data Transfer Impact Assessment: TIA） ・ 移転先とのTIAを踏まえた追加的補充措置を含む標準データ保護条項を規定した契約(Standard contractual clauses: SCC) の締結	一般的な移転方法（但し、左記の通りTIAの負荷・管理コスト要）	中
③	特定の状況における例外		ー
③-1	本人への移転リスク情報提供＋明示的同意の取得	健康・医療サービスでは、左記の通知・同意措置の設定は比較的容易であり、且つ移転の是非を本人が自己決定するため、本人の権益保護も図りやすい。	高

2.2 センシティブ情報の取扱いに対し法令要件が厳格化される局面及びその加重要件

人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は自然人の性生活若しくは性的指向に関するデータの取扱いは禁止される。

但し、以下いずれかに該当する場合を除く

1）データ主体が、一つ又は複数の特定された目的のためのその個人データの取扱いに関し、明確な同意を与えた場合。

2）EU 法若しくは加盟国の国内法により認められている範囲内、又はデータ主体の基本的な権利及び利益のための適切な保護措置を定める加盟国の国内法による団体協約によって認められる範囲内で、雇用及び社会保障並びに社会的保護の法律の分野における管理者又はデータ主体の義務を履行する目的のため、又はそれらの者の特別の権利を行使する目的のために取扱いが必要となる場合。

3）データ主体が物理的又は法的に同意を与えることができない場合で、データ主体又はその他の自然人の生命に関する利益を保護するために取扱いが必要となるとき

4）非営利組織による適切な保護措置を具備する正当な活動の過程において、当該取扱いが、その組織の構成員若しくは関係者のみに関するものであることを条件とし、かつ、データ主体の同意なくその個人データが当該組織の外部に開示されないことを条件として、取扱いが行われる場合
５）データ主体によって公開された個人データに関する取扱い
６）訴えの提起若しくは攻撃防御のため、又は、裁判所がその司法上の権能を行使する際に取扱いが必要となる場合
7）求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定めるEU法又は加盟国の国内法に基づき、重要な公共の利益を理由とする取扱いが必要となる場合
8）法令に基づき、又は、医療専門家との契約により、かつ、予防医学若しくは産業医学の目的のために、労働者の業務遂行能力の評価、医療上の診断、医療若しくは社会福祉又は治療の提供、又は、医療制度若しくは社会福祉制度及びそのサービス提供の管理のために取扱いが必要となる場合
9）データ主体の権利及び自由、特に、職務上の秘密を保護するための適切かつ個別の措置に関して定めるEU法又は加盟国の国内法に基づき、健康に対する国境を越える重大な脅威から保護すること、又は、医療及び医薬品若しくは医療機器の高い水準の品質及び安全性を確保することのような、公衆衛生の分野において、公共の利益を理由とする取扱いが必要となる場合。
10）求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定める法令に基づき、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために取扱いが必要となる場合

上述より、そもそも特殊な種類の個人データは、取扱い全般において、原則取扱いが禁止されているが、法定の例外事項に該当する場合に限り、その取扱いが認められており、以下局面毎に例を挙げる。

1つ目として、特殊な種類の個人データが越境する局面が挙げられる。この場合、移転先におけるセンシティブデータについて制限・保護措置（アクセス制限、仮名化等の追加的保護措置、又は更なる開示に対しての追加的制限を含む）を要する。これは、欧州委員会が2021年6月に公表した「第三国への個人データ移転のためのSCCに関する決定」[108]において、改訂版SCCに当該制限・保護措置の条項が追加されたことによるものである。

2つ目として、データ保護体制整備の一環として設置されるDPOの設置が挙げられる。GDPR第37条では、同条で定める3つの場合いずれかに該当する場合、DPOの設置を義務付けている。その3つの中の1つに「第9条による特別な種類のデータ、並びに第10条で定める有罪判決及び犯罪行為と関連する個人データの大規模な取扱いによって構成される場合」を挙げており、これに当てはまるときは、DPO設置が必須となる。

3つ目として、個人データ侵害が生じた場合が挙げられる。GDPR第34条は、「自然人の権利及び自由に対する高いリスクを発生させる可能性がある場合、管理者は、そのデータ主体に対し、不当な遅滞なく、その個人データ侵害を連絡しなければならない。」と規定している。前述の通りGDPR第9条により、「特殊な種類の個人データは原則として取扱いを禁止されている」ことの趣旨を踏まえると、当該データの侵害は、この「自然人の権利及び自由に対する高いリスク」に該当し得る。

[108] COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN

表2.2(1) 特別な種類の個人データの取扱いが認められる要件と、前掲の表Ⅲ2.1.1.8(1)の要件比較

項目 / No.	適法性根拠の要件 （第2章 基本原則 第6条）	特別な種類の個人データの取扱要件 （第2章 基本原則 第9条）	特定の状況における例外の要件 （第5章 第三国又は国際機関への個人データの移転 第49条）
1)	本人への情報提供（利用目的含む）及び本人の明示的同意	本人への情報提供（利用目的）及び本人の明示的同意	本人への情報提供（十分性認定及び適切な保護措置が存在しないことによる移転リスク）及び本人の明示的同意
2)	N/A	N/A	本人と管理者間の契約履行、又はデータ主体の要求による契約締結前の措置の実施
3)	本人が契約当事者となっている契約履行、又は契約締結前に本人の要求に際しての手段の実施	N/A	管理者と第三者間で、データ主体の利益となる契約締結、又はその契約履行
4)	公共の利益又は管理者による公的権限行使のための職務遂行	法令に基づき重要な公共の利益を理由とする場合	公共の利益の重大な事由
5)	管理者における法的義務の遵守（データ主体の義務履行又は特別な権限行使は要件でない）	雇用及び社会保障及び社会的保護の法令における管理者又はデータ主体の義務の履行又は特別な権利行使を行う目的	法的主張時の立証、行使又は抗弁
6)	本人その他自然人の生命保護	データ主体が物理的又は法的に同意ができない場合で、データ主体その他自然人の生命を保護するため	本人が物理的又は法的に同意を与えることができない場合、本人その他自然人の生命保護
7)	データ管理者又は第三者の正当な利益の目的。 但し、その利益よりも、データ主体の権益の方が優先する場合、	非営利組織による活動過程で、その構成員又は関係者に関するもので、かつデータ主体の同意なく個人データが開示されないことを条件とする場合	個々の案件において、照会に関して法定の条件を充足する限度内に制限されている登録機関からの移転が必要となる場合

	特にそのデータ主体が子供である場合を除く。		
8)	N/A	データ主体によって明白に公開された個人データ	N/A
9)	N/A	訴訟提起若しくは攻撃防御のため、又は裁判所の権能行使	N/A
10)	N/A	法令又は医療専門家との契約に基づき、かつ職務上守秘義務に服する職にある者の下で取り扱われ、医学のために、労働者の業務評価、又は医療・社会福祉制度及びそのサービス提供	N/A
11)	N/A	法令に基づき、公衆衛生おいて、公共の利益を理由とする	N/A
12)	N/A	法令に基づき、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的	N/A

N/A: 他の列に記載されている要件に類似するような要件が無いもの

表Ⅲ2.2(2) 取扱局面毎の主な法令要件とセンシティブ情報に対する要件の厳格化（EU）

局面	一般的な個人情報の主な法令要件	センシティブ情報の主な加重要件	
取得	ⅰ）適法性の根拠 （a.本人から明示的同意の取得, b.契約履行,c.法的義務履行, d.生命保護, e.公的権限行使, f.データ管理者・第三者の正当な 利益保護等, 法定事項を根拠） ⅱ）取扱活動に係る法定記録の保管 ⅲ）本人への法定事項の情報提供 ⅳ）DPIA実施（但,個人の権利・自由に 対する高いリスクを発生させる虞のある 場合）	○	1）原則取扱い禁止 但,以下10個のいずれかに 該当する場合を除く。 a）本人から明示的個別同意取得 b）EU/各国法令で認める範囲 c）本人の同意取得不可,且つ 自然人の生命保護 d）非営利組織での取扱い e）自然人が公開した個人データ 取扱い f）訴訟や司法権行使での取扱い g）EU/各国法法令に則り,重要な 公共利益を理由とする取扱い h）EU/各国法令・医療機関との 契約による医療・社会福祉サービス の提供 i）EU/各国法に則り,越境する 重大な健康への脅威からの保護、 医療、医薬品・医療機器の品質, 安全性確保等公衆衛生において, 公共利益を理由とする取扱い j）EU/各国法令に則り,公共利益 における保管の目的,科学的研究, 歴史的研究の目的,統計目的の ための取扱い 2）取得前のDPIA実施 （特別な種類のデータの大規模な取扱 いを行う場合(本稿では、健康・医療サ ービスがこれに該当するものと想定(表Ⅲ 5.2に含める)。） 3）移転先に対する特別な種類の個 人データの取扱制限・保護措置
利用提供	ⅰ）適法性の根拠 ⅱ）取扱活動に係る法定記録の保管 ⅲ）目的の限定 ⅳ）データの最小化	N/A	
越境	ⅰ）適法性の根拠 ⅱ）取扱活動に係る法定記録の保管 ⅲ）以下いずれか適用: a）十分性認定 b）適切な保護措置に従った移転 BCR、又はTIA及びSCC c）特定の状況における例外 本人への移転リスク情報の通知*、 及び明示的同意の取得 * 十分性認定及び適切な保護措置が 無いため、移転で生じうるリスクの情報 提供 等	○	
保管管理	ⅰ）適法性の根拠 ⅱ）取扱活動に係る法定記録の保管 ⅲ）安全管理措置（機密性・完全性・可用 性）	N/A	（上記1）と同じ）

体制	・ DPO設置（但,一定の場合に限る） ・ 代理人設置（但,域外適用の場合に限る）	○	DPO設置 （特別な種類のデータを大量に取扱う場合、設置要）
権利行使	本人からの権利行使の求めに応じる手続の公表と行使時の対応* （* 利用目的の通知，並びに個人情報の開示，訂正，消去，処理制限，データポータビリティ，及び異議申立(toデータ管理者)，不服申立(to当局)）	N/A	（健康・医療サービスの実務上、取得の局面において、①GDPRの第6条第1項(a)と②第9条第2項(a)との同意を纏めて取得することが想定される。その場合、表Ⅲ2.1.1.6 1)c)又は2)c)の同意を撤回する権利の行使として、仮に上記②の同意のみ撤回されるとすると、同サービスの性質上、実際にはサービス提供そのものを停止せざるを得なくなる。そのため本稿では要件の加重というよりむしろ、同サービス事業者において実質はサービス提供の停止と評価(表Ⅲ5.2でN/Aとする)。）
事故	監督機関へ個人データ侵害の通知: （個人の権利・自由へのリスクの虞の無い場合除く）	N/A	本人へ個人データ侵害の通知 （本人の権利・自由に対する高リスク発生の虞ある場合、通知要）

○: 該当, N/A: 非該当

2.3 仮名化及び匿名化

2.3.1 仮名化

「仮名化」とは、追加的な情報が分離して保管されており、かつ、その個人データが識別された自然人又は識別可能な自然人に属することを示さないことを確保するための技術上及び組織上の措置の下にあることを条件として、その追加的な情報の利用なしには、その個人データが特定のデータ主体に属することを示すことができないようにする態様で行われる個人データの取扱いを意味する（GDPR第4条第5項）。仮名化を経た個人データは、識別可能な自然人に関する情報、即ち個人データであると位置付けられている（GDPR前文第26項）。

併せて、個人データに仮名化を適用することは、データ主体に対するリスクを低減させ、また管理者及び処理者がそのデータ保護上の義務を遵守することを助ける（GDPR前文第28項）。そのため仮名化は、暗号化と並び、個人データ保護措置の1つとして位置付けられている（GDPR第6条第(e)、第25条第1項、第32条第1項(a)、第40条第2項(e)、及び第89条第1項、並びにGDPR前文第78項、及び第156項）。また、個人データを取扱う際に仮名化を適用するインセンティブをつくり出すため、仮名化を経た個人データの一般的な分析を認めている（GDPR前文第29条）。[109]なお、法定の場合には、GDPR第15条乃至第20条で定めるデータ主体の権利は適用されない（GDPR第11条）。

2.3.2 匿名化

GDPR前文では、ある自然人が識別可能であるかどうかを判断するためには、データ主体を直接又は間接に識別するためにデータ管理者又はそれ以外の者によって用いられる合理的な可能性のある全ての手段を考慮に入れた上で、合理的な可能性があるか否かを確認するために、取扱い時、利用可能な技術及び技術発展を考慮に入れて、識別のために要する費用及び時間量のような、全ての客観的な要素を考慮に入れなければならない、としている。

これを踏まえた上で、識別された自然人又は識別可能な自然人との関係をもたない情報、又は、データ主体を識別できないよう、個人データを匿名化した情報、即ちもはやデータ主体を識別することができないように処理することを、匿名化としている。

匿名化は、不可逆的に特定個人の識別を防止するものであり、加工の方法に関する情報が残存している場合、たとえ安全に分離管理されていたとしても、再識別の可能性があるとして、匿名化された情報とはみなされない、と考えられている。[110]

匿名化された情報は、GDPRの適用を受けない（GDPR前文第26条）。

2.3.3 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和

日本の仮名加工情報のように、個人情報に仮名加工処理を施した仮名化された個人情報について、一部法令要件の緩和が認められる（GDPR第11条）。他方、匿名化された情報は、上述の通りGDPRの適用対象外となる。

---

[109] 仮名化は、安全管理措置の一と考えられる（GDPR第6条第4項(e)、第25条第1項、第32条第1項(a)、第40条第2項(d)、第89条第1項）。

[110] 柳田宗彦「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第53回 EU一般データ保護規則(GDPR)および日本との相互認証について」 国際商事法務 Vol.46 No.7(2018) P993

3. 米国

3.1 一般的な個人情報の取扱いに対する規制

3.1.1 米国内における個人データの取扱いに関する主な法令要件

3.1.1.1 取得・利用・提供

COPRAでは、データの処理及び譲渡の詳細且つ正確な内容を記述したプライバシーポリシーを容易にアクセス可能な方法で公表することを対象事業者に義務付けている。

また、対象事業者に該当しないような、小規模事業者に該当する個人若しくは事業者又は非営利団体等の第三者[111]への譲渡については、選定する際に合理的なデューデリジェンス（Due Diligence．以下「DD」という。）を実施の上、当該委託先を合理的に監視し、委託先が担う義務への遵守を確保するものとしている。

なお、FTC法では、具体的な法令要件を定めた規定はないが、FTCが第５条「不公正若しくは欺瞞的な行為又は慣行」を適用し、法執行した以下のような事例がある。

1）個人情報の収集について、消費者へ通知していたが、長い規約の一部に極めてわかりにくい態様で表示していたことを欺瞞的であるとした事例

2）消費者の明示の同意なく第三者への個人情報の販売を行わないとしていたプライバシーポリシーを、第三者への販売をオプトアウトとするよう変更した点が、不公正であるとした事例 等

ADPPAでは、データの収集、処理及び移転活動に関する詳細且つ正確な表現を提供するプライバシーポリシーを、明確で見やすく、容易にアクセス可能な方法で、一般に公開することが義務付けられている。

また、利用・処理にあたっては、データの最小化が課せられる。これは法定[112]の目的のために合理的且つ相応な範囲を超えて、対象データを収集、処理又は移転してはならないとする義務である。併せて、忠実義務が課せられる。これは、社会保障番号の収集、処理又は移転等、法定の行為を原則禁止する義務を課すものである。

HIPAAプライバシー規則は、また、PHIの利用及び開示について、必要最小限の原則を掲げ、目的達成に必要最小限度にとどめるための合理的な努力を行うよう求めており、PHIの利用及び開示に関する一般的なルールを定めている。その中で「許容される利用及び開示」に関する規定より、利用及び開示を以下の場合に限定している。

1）情報主体に対する場合

2）治療、支払又は保健医療の実施のためであって、情報主体の同意ある場合

3）同規則の下で認められる利用又は開示に付随する場合

4）同規則の下で禁止される利用及び開示に当たる場合を除き、心理療法記録の利用又は

---

[111] 「第三者」とは、対象事業者によって譲渡される対象データを処理又は譲渡し、当該データに関しては、サービスプロバイダーではなく、且つ2つの事業者が共通の所有権又は企業の支配によって関連付けられ、共通のブランドを共有しない個人又は事業者を指す。本稿では、当該第三者についての記述は、以降割愛する。

[112] 個人によって求められた具体的な商品・サービスの提供・維持のため、本法案において明示的に許諾されている目的のため、等が定められている。

開示、マーケティング目的での利用又は開示、及び、販売について有効な許可がある場合[113]

5）ディレクトリ管理や家族等への通知のための利用又は開示であって、個人に選択の機会が付与されている場合

6）その他同規則の下で許容される場合

併せて、PHIの利用及び開示に関する一般的なルールの中、禁止される利用及び開示の規定により、以下を禁止している。

a）長期介護保険事業者を除くヘルスプランが、引受けに関する判断を行う目的で遺伝情報の利用及び開示を行うこと

b）情報主体の許可を得た場合を除き、対象組織又は事業提携車がPHIを販売[114]すること

併せて、同規則では、個人は、PHIの利用及び開示、並びに対象組織の義務に関して、適切な通知を受ける権利を有すると定められている。当該通知の内容については、注意喚起のための見出し、対象組織に認められるPHIの利用及び開示、PHIに関する個人の権利や対象組織の義務、苦情申立ての手続、担当者の氏名や連絡先等を含み、平易な文章で記述することが求められている。また、通知の方法について、ヘルスプラン及び保健医療提供者について、それぞれ具体的な規定を置くとともに、ウェブサイトを有する対象組織に対しては、ウェブサイトで明瞭に通知を掲載することを義務付けている。[115]

CCPAでは、消費者が、その個人情報を収集[116]する事業者に対して、事業者が収集する個人情報の種類及び特定の情報を開示することを要求する権利を有すると規定しており、消費者の個人情報を収集する事業者は、収集時又は収集前に消費者に対して、収集される個人情報の種類及び利用目的を通知しなければならない。[117]また、当該通知で知らせた種類以外の個人情報を収集すること、又は当該通知で知らせた利用目的以外で利用することは禁止されており、それらを行う場合には、改めて所定の通知手続を要する、としている。

また、個人情報を第三者に販売[118]する場合には、消費者にオプトアウト権を認めており、販売する可能性、及び消費者のオプトアウト手続に関して、プライバシーポリシー等で説明・公表しなければならない、としている。CPRAでは、販売とは別個に「共有」[119]という概念を新設し、共有に該当する場合にも、販売と同様のオプトアウト権を認め、対象事業者にその手続の公表を義務付けている。

---

113 有効な許可が必要とされるPHIの利用又は開示としては、心理療法記録の利用又は開示、マーケティング目的での利用又は開示、及び、販売が挙げられている（45 C.F.R. §164.508.）。これに対し、事業提携者は、事業提携契約その他の契約によって認められる若しくは要求される場合、又は法により要求される場合にのみ、PHIの利用又は開示を行うことができる（45 C.F.R. §164.502.）。

114 PHIの販売とは、PHIと引換えにPHIの受領者から直接又は間接に報酬を受けて行うPHIの開示と定義されている（45 C.F.R. §160.103.）

115 https://www.govinfo.gov/app/details/CFR-2011-title45-vol1/CFR-2011-title45-vol1-sec164-520/context

116 収集とは、消費者の個人情報を購入、賃借、収集、所有、受領又はアクセスすることを指し、行動の観察も含まれる。

117 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100.

118 販売とは、金銭又はその他の価値のある対価のために、事業者が他の事業者又は第三者に対し、販売、賃貸、公表、開示、頒布又は取得利用可能にし、移転し、その他口頭、書面、電子的その他手段で伝えることをいう。

119 共有とは、金銭その他の価値ある対価と引換に行うか否かを問わず、事業者が、クロス・コンテクスト行動広告のために、第三者に、消費者の個人情報を共有、貸与、公開、開示、流布、利用可能な状態に置き、移転し、又は口頭、書面、電子的その他の手段により伝達すること、としている。ここでいうクロス・コンテクスト行動広告とは、いわゆる行動ターゲティング広告を指す（井上 乾介(アンダーソン・毛利・友常法律事務所 外国法共同事業 弁護士)「カリフォルニア州プライバシー権法（CPRA）の概要－「機微情報」,「共有」規制の新設ほか」ビジネス法務 2021.6 P116-P117）

なお、本章で取り上げている各法令では、プロファイリングやそれを用いた自動意思決定自体を特別に且つ直接規制するものはない。一方で、個別の問題毎に対応が検討されており、例えば行動ターゲティング広告については、FTCが透明性や消費者の選択の確保を中心とした自主規制原則を提示し、消費者がウェブサイトの閲覧行動の追跡を拒否しうるブラウザー機能（Do Not Track）の導入等を推奨している。またCCPA/CPRAにおいては、前述Ⅱ3.2.1の通り、「消費者の嗜好・特徴・心理トレンド・行動・意見・知能・能力・適性に関するプロファイルを作成するため、これら情報から導出された推測・推論」は、個人情報となるため、後述の通り、本人の権利行使の対象情報となり得る。

3.1.1.2 委託

COPRAでは、対象事業者は、サービスプロバイダー[120]を選定する際に合理的なデューデリジェンスを実施の上、当該委託先を合理的に監視し、委託先が担う義務への遵守を確保するものとしている。

HIPAAセキュリティ規則では、対象組織は、委託先（事業提携者）との間で締結された契約に基づき、事業提携者が適切に情報の安全を確保するという確証を得た場合、事業提携者に対し、電子化されたPHIの作成、受領、保管又は転送を自らに代わって行せることができるとしている。なお、再委託がなされる場合、対象組織は、再委託先に関してかかる確証を得ることは必要とされない。この場合、委託先は、再委託先との間で締結した契約に基づき、再委託先が適切に情報の安全を確保するという確証を得た場合に限り、再委託先に対し、電子化されたPHIの作成、受領、保管又は転送を委託先に代わって行うことを認めることができるものとしている。

CCPAでは、サービスプロバイダー[121]と法定事項を約定した契約書を締結する等の一定の法定要件を満たした場合、当該サービスプロバイダーのCCPA違反に対し免責される規定はある。なお、CPRAでは、サービス提供者に加えて、コントラクター[122]に対して開示している事業者についても、類似の免責規定を設けている。

3.1.1.3 保管・管理

ADPPAでは、不正なアクセス及び取得から保護するため、合理的な管理上、技術上、及び物理上のデータ・セキュリティ・プラクティス及び手続を確立し、実施し、維持する義務を負う。

FTCは、第５条「不公正若しくは欺瞞的な行為又は慣行」に基づく情報セキュリティに関する法執行[123]も行われており、FTCは求められる安全管理措置に関する幾つかの指針を公表している。

---

[120] 対象事業者(委託元)に代わって、又はその指示に従って、サービス又は機能を実行する過程で、(ⅰ)当該サービス又は機能の履行に関して、又は(ⅱ)法的義務を遵守するため、若しくは法的請求を確立、行使又は防御するために必要な限度で、対象データを処理又は譲渡する者(委託先)をいう。

[121] サービスプロバイダーとは、「事業者に代わり、個人情報を処理する者であって、業務目的のため、事業者と締結した所定の契約書に従い、事業者から又はこれに代わり消費者の個人情報を受領する者」をいう（井上 乾介「カリフォルニア州プライバシー権法（CPRA）の概要－「機微情報」,「共有」規制の新設ほか」ビジネス法務 2021年6月 P117-P118 ）。

[122] コントラクターとは、事業者と所定の契約書に従い、事業者が、業務目的で消費者の個人情報を利用可能にする者をいう（井上 乾介（同上 P117-P118）。

[123] 合理的且つ適切な安全管理措置を講じずに消費者の個人情報を漏洩させたことを不公正と判断した事例もある（（「第9回米国における個人情報・プライバシー保護監督機関－FTCを中心に」NBL No.1201(2021.9.1)号 P91））。

HIPAAプライバシー規則では、対象組織にPHIを保護するための適切な管理的、技術的及び物理的な安全管理措置を講ずることが義務付けられている。一方、HIPAAセキュリティ規則では電子的なPHIについて、同様に安全管理措置を講ずることを義務付けている。

CPRAでは、合理的セキュリティ措置を講じた上で、消費者のプライバシー又はセキュリティに重大なリスクをもたらす処理を行う事業者に対して、①毎年セキュリティ監査と、②当該処理に関するリスク評価を義務付けている。[124]

3.1.1.4 データローカライゼーション規制

FTC、COPRA、ADPPA、HIPAA等及びCPRAいずれも、データローカライゼーションを定めた規制はない。

3.1.1.5 体制・責任者

COPRAでは、1 人以上の適任の従業員をプライバシー責任者、及び同じく 1 名以上の適任の従業員をデータセキュリティ責任者として選任する義務がある。

ADPPAでは、プライバシー・オフィサー及びデータ・セキュリティー・オフィサーをいずれも1名以上選任する義務がある。

HIPAAプライバシー規則では、前述の通り、対象組織にPHIを保護するための適切な管理的、技術的及び物理的な安全管理措置を講ずることが義務付けられている。この管理的な安全管理措置として、セキュリティに関する責任者を指名することが挙げられている。

CCPA/CPRAともに特段規定はない。

3.1.1.6 本人の権利

COPRAでは、個人の権利として、個人情報に対するアクセス、訂正、消去、データポータビリティ、譲渡にあたってのオプトアウト、及びセンシティブ情報の処理及び譲渡にあたってのオプトインを求める権利が認められている。

ADPPAでは、個人の権利として、個人情報に対するアクセス、訂正、削除、データポータビリティ、並びにデータの移転及びターゲティング広告からのオプトアウトを求める権利が認められている。併せて、価格決定等に関する個人への条件付けを禁止している。これは例えば、データを提供することで価格を変更したり、サービスに違いを設けたりすることや、個人の権利を行使又は放棄しないことにより商品・サービスの提供を拒否・停止することを禁止するものである。

HIPAAプライバシー規則では、PHIの利用及び開示に関する一般的なルールの中で、要求される規定を定めている。そこでは、「対象組織は、個人が健康へのアクセス及び開示[125]を求めた場合や、組織の順守状況の調査又は決定のためにHHSから開示を求められた場合、PHIを開示しなくてはならない」と規定されている。

---

[124] 該当条項は§1798.100(e), §1798185(a)(15)。なお、重大なリスクをもたらす処理であるか否かを判断するにあたっては、事業者の規模や複雑性、処理活動の性質やスコープ等の要素が考慮されることとなる。

[125] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

CCPAでは前述通り、消費者が、その個人情報を収集する事業者に対して、事業者が収集した個人情報の種類及び特定の情報を開示することを要求する権利の他、個人情報の消去、前述のオプトアウト権による販売停止、及び消費者の権利行使を理由とした差別的な取り扱われないことを要求する権利を有すると規定している。

なお、CPRAでは、不正確な個人情報に対する訂正権、及びプロファイリング[126]を含む自動化された意思決定技術の使用について、オプトアウト権及び開示権、並びに機微個人情報の利用に一定の制限を加える権利も認めている。

3.1.1.7 データ侵害・インシデント

HITECでは、安全対策が施されていないPHIを取扱う対象事業者は、セキュリティ侵害を発見した場合、各個人[127]に対する当該侵害の通知義務が規定されている。併せて、一定の場合[128]には、州又は管轄地域の著名な報道機関への通知も要する。

CCPA/CPRAと別途、カリフォルニア州データ侵害通知法が制定されており、同法では、個人情報を漏洩させた可能性ある事業者は、本人への通知義務を負う。併せて、カリフォルニア州住民500名以上に侵害通知を行う場合には、同州の司法長官への通知も要する。

3.2 センシティブ情報の取扱いに対し法令要件が厳格化される局面及びその加重要件

FTC法では、2012年報告書で、健康情報を含むセンシティブ情報を取得する場合、事前に消費者から積極的な明示の同意を取得すべきとしている。

なお、COPRAでは、センシティブ情報の処理及び譲渡について、事前の積極的な明示の同意を取得することを要求している。

ADPPAでは、忠実義務において、個人の健康状態等センシティブ対象データに関し、収集及び処理、並びに第三者への提供その他法定の行為を原則禁止する義務を課す。但し、個人より明示的同意を取得する等、法定の例外要件を具備する場合を除く。

HIPAA/HITECでは、前述の2012FTC報告書により、健康情報はセンシティブ情報であると位置付けていることから、同法で定めるPHIそれ自体がセンシティブ情報であるといえるため、センシティブ情報であることにより要件が加重されるということがない。

CPRAでは、消費者の特徴を推測する目的で機微個人情報を取得・処理する事業者に対し、その処理・利用を平均的な消費者が合理的に期待するサービス・商品を提供するための利用・セキュリティ確保のための利用、短期的な一時利用等、利用目的を限定する権利を有する。

---

[126] プロファイリングを「自然人に関する一定の個人的側面を評価する個人情報の自動化された処理であり、特に当該自然人の仕事のパフォーマンス、経済状況、健康、個人的嗜好、興味、信頼性、行動、位置又は動作に関する側面を分析又は予測するもの」と定義している（§1798.140(z)）。

[127] 各個人とは、かかるセキュリティ侵害により、PHIへのアクセス、取得若しくは開示が行われた、又は、行われたと対象組織が合理的に信じる個人をいう。

[128] セキュリティ侵害により、500名を上回る、州又は管轄地域の安全対策が施されていないPHIへのアクセス、取得若しくは開示が行われた、又は、行われたと対象組織が合理的に信じる場合

表Ⅲ3.2 取扱局面毎の主な法令要件とセンシティブ情報に対する要件の厳格化（米国）

局面	法令[129]	一般的な個人情報の主な法令要件	センシティブ情報の主な加重要件	
取得	COPRA	プライバシーポリシーの公表	○	本人から明示的同意の取得
	ADPPA	・プライバシーポリシーの公表 ・データ最小化 ・忠実義務	○	・ 本人から明示的同意の取得 ・ 個人より要求された具体的な商品・サービスの提供・維持その他法定の目的に厳密に必要となる場合
	HIPAA	本人への法定事項の通知	－	－
	CPRA	本人への法定事項の通知	N/A	－
利用	COPRA	取得時公表・同意取得した範囲内での利用	N/A	（健康・医療サービスの実務上、取得の局面において、纏めて同意取得することが想定される。そのため本稿では、同サービス事業者における実質的な要件の加重に該当しないと評価(表Ⅲ5.2でN/Aとする)。）
	ADPPA	（取得時と同じ）	○	取得時と同じ
	HIPAA	HIPAAプライバシー規則での利用範囲の限定	－	－
	CPRA	取得時通知した範囲内での利用	N/A	－
提供	COPRA	非対象事業者に該当への譲渡： デューデリジェンス＋監視	N/A	（上記の利用の局面と同じ）
	ADPPA	（取得時と同じ）	○	本人から明示的同意の取得
	HIPAA	開示範囲の限定（45 C.F.R. §164.520 (a).）	－	－
	CPRA	販売・共有に関するオプトアウト手続の公表 （法定事項を約定する契約をサービスプロバイダーと締結することで、同プロバイダーのCCPA違反に対する免責措置あり)	N/A	－
越境	N/A	N/A	N/A	－
	COPRA	データセキュリティ慣行の確立	NA	－

[129] FTC法は、取得時を除き、局面毎にセンシティブ情報の具体的な取扱要件を定めるものではないため割愛。

保管管理	ADPPA	安全管理措置	NA	–
	HIPAA	安全管理措置 （45 C.F.R. §164.530.）	–	–
	CPRA	合理的セキュリティ管理措置、並びにセキュリティ監査及びデータ処理に関するリスク評価	NA	–
体制	COPRA	ⅰ)プライバシー・データセキュリティ 責任者の選任 ⅱ)FTC認証（毎年/COPRA順守体制整備）	NA	–
	ADPPA	プライバシーオフィサー/データセキュリティーオフィサーの選任	N/A	–
	HIPAA	N/A	–	–
	CPRA	N/A	N/A	
権利行使	COPRA	アクセス、訂正、消去、データポータビリティ、譲渡にあたってのオプトアウト、及びセンシティブ情報の処理及び譲渡にあたってのオプトインを求める権利への対応	○	同意の撤回 （含 明示的同意を撤回するための消費者に優しい手段の提供）
	ADPPA	・ アクセス、訂正、削除、データポータビリティ、オプトアウト(移転/ターゲティング広告)）権への対応 ・ 価格設定に関する個人への忠誠	N/A	–
	HIPAA	アクセス・開示権への対応	–	–
	CPRA	○ （販売の停止・所定事項開示,消去, 差別的取扱い禁止 ）	○	利用・開示制限の権利及び当該権利行使手続の公表

注）事故の局面は現時点、COPRAにおける詳細要件の把握が困難であるため割愛。

○: 該当, N/A: 非該当

3.3 仮名化及び匿名化

3.3.1 仮名化

CCPAでは、「仮名化する」又は「仮名化」[130]について、追加情報の利用なしには、個人情報を特定の消費者に帰属させ得ない態様で、個人情報を処理することであり、追加情報が特定の個人からは切り離して保管され、当該個人情報を識別された又は識別可能な消費者に帰属させないための技術的及び組織的な措置に服する場合をいうものとされる。仮名化は、個人情報を用いた研究[131]を行うための要件の１つとされている。なお、他の目的で事業者のサービス又はデバイスでの消費者とのやりとりの過程で消費者から収集された個人情報を用いた研究は、いくつかの要件を満たすことが必要とされ、その１つとして、個人情報が、特定の消費者を合理的に識別する、関連する、叙述する、若しくは関連付けることができないように、又は、特定の消費者と直接的若しくは間接的に結び付けることができないように、又は、特定の消費者と直接的若しくは間接的に結び付けることができないように、仮名化及び識別化され、又は、非識別化及び集積されること、が挙げられている。

他FTC法、COPRA、ADPPA及びHIPAAでは、仮名化による法令要件の軽減または免除等の規定はない。

3.3.2 匿名化

COPRAでは、「事業者が次の各事項を行う場合に、個人、世帯、又は個人若しくは世帯が使用する機器に関する情報を推測またはリンクするのに合理的に使用できない情報。」を非識別化データと定義し、適用除外になるとしている。

a）情報を個人、世帯、又は個人若しくは世帯が使用する機器に再識別又は関連付けできないようにするための合理的な措置を講じる。

b）目立った方法で、（i）匿名化された形式で情報を処理及び譲渡すること、並びに（ii）個人、世帯、又は個人若しくは世帯が使用する機器と情報を再特定又は関連付けようとしないことを公に表明する。

c）上記各事項を遵守するために、対象事業者から情報を受信する個人又は事業者に契約上の義務を負わせる。

ADPPAでは、非識別化データは、適用対象となるデータに含まれないとしている。非識別化データとは、情報が集積されている場合であるか否かを問わず、個人を識別しない又は個人とリンクしない若しくは合理的にリンク可能ではない情報又はデバイスと定義されている。[132]

HIPAAプライバシー規則には、「非識別化」（de-identification）された情報、即ち個人を識別しない、又はその情報が個人を識別するのに利用され得ると信ずるにつき合理的な根拠の無い情報は、「個人を識別し得る情報」に該当しないとし、当該情報には原則として同規則は適用されないとしている。

---

[130] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.140.&lawCode=CIV

[131] 研究とは、科学的で体系的な調査及び観察を意味するとし、公益のための且つ適用可能なあらゆる倫理及びプライバシー法を遵守する、基礎研究又は応用研究、又は、公衆衛生の分野における公益のための研究を含むものとする、としている。

[132] 非識別化データに該当するには、いかなる場合においても、当該データが、個人又はデバイスが再識別される形で用いられないことを確実にするための合理的措置を実施する等、法定の要件を具備する必要がある。

また、再識別化のリスクに対応するため、非識別化された情報に該当するための2つの基準を設けている。

第一は、「専門家決定基準」と呼ばれるもので、情報が個人識別可能でないと判断するための一般的な統計的・科学的原則及び方法に関して、適切な知識及び経験を有する者が、かかる原則及び方法を用いて、情報の予期せぬ受領者が、情報主体たる個人を識別するために当該情報を単独で、又は他の合理に入手可能な情報と結び付けて利用するリスクが極めて小さいと決定し、かつ、かかる決定を裏付ける分析方法及び結果を書面で立証した場合、非識別化がなされたとされる。同規則で公表されている指針では、リスクが極めて小さいかどうかについての明確な基準はないとされるが、リスク評価の際に専門家が参照し得る原則として、個人を特定し得る特徴を含むかどうか、当該情報へのアクセス可能性、情報主体が識別される程度といったものが挙げられている。

第二は、「セーフハーバー基準」と呼ばれるもので、個人に関する又は個人の親族、雇用者若しくは家族の構成員に関する、18項目の識別子[133]が削除され、かつ対象組織が、情報主体たる個人を識別するために当該情報が単独で又は他合理的に入手可能な情報と結び付けて利用されることについて実際に知らなかった場合、非識別化がなされたとされる。

この後者の要件については、対象組織が、上記について明確且つ直接的な認識を持っていた場合、即ち、当該情報が実際には非識別化された情報でないことに気づいていた場合は、「実際に知っていた」と解されている。

更に同規則は、非識別化された情報の再識別化に関する定めも設けられている。即ち、対象組織は、同規則が定めるルールの下で非識別化された情報を再識別化することができるように、コードその他の記録管理のためのIDを割り当てることができるが、当該コードその他の記録管理のためのIDは、個人に関する情報から抽出された又はそれに関連するものであってはならず、且つ、個人を識別するために変換可能なものであってはならないとする。また、対象組織は、コードその他の記録管理のためのIDを他の目的のために利用又は開示してはならず、再識別化の仕組みも開示してはならない。再識別化が行われた場合には、当該情報は、同規則の適用を受けることとなる。

また、FTCは、2010年公表の報告書において、保護対象となる消費者の個人情報一般について、新たな基準を提示し、プライバシー保護のためのフレームワークは、「特定の消費者、コンピューターその他のデバイスに合理的に結び付けられ得る消費者のデータを収集又は利用する全ての事業者に適用される。」とした上で、2012年公表の報告書で、「事業者のデータは、当該事業者がそのデータについて３つの重要な保護措置を実施している場合、特定の消費者又はデバイスに合理的に結び付けられ得ることとはならない。」として、データの非識別化のための以下３つの基準を示している。

・ 第1要件: 「事業者は、そのデータの非識別化を確保するために合理的な措置を講ずるべきである。」とされ、「合理的な措置」について、「事業者は、当該データが、特定の消費者、コンピューターその他のデバイスに関する情報を推測するために合理的に用いられない又は合理的にそれらに結び付けられないという、合理的なレベルの正当な信頼を確保しなければならない」とされている。

何が「合理的なレベルの正当な信頼」にあたるかは、利用可能な方法及び技術、問題となっているデータの性質又はその利用目的等の個々の状況により判断される。

---

[133] https://www.govinfo.gov/app/details/CFR-2021-title45-vol2/CFR-2021-title45-vol2-sec164-514/context
①氏名、②州以下の住所、③生年月日等を含む個人に直接関係する日の年月日、④電話番号、⑤FAX番号、⑥電子メールアドレス、⑦社会保険番号、⑧医療記録番号、⑨健康保険受給者番号、⑩口座番号、⑪資格等に関する番号、⑫自動車登録番号、⑬機器番号、⑭ウェブのURL、⑮IPアドレス、⑯指紋や声紋を含む生体情報、⑰顔写真その他の画像、⑱その他のあらゆる個人識別番号、特徴、又はコード、が挙げられている。

・ 第2要件:「事業者は、そのデータを非識別化された態様で保有及び利用し、そのデータの再識別化を試みないことを公に誓約すべきである」とされ、この誓約に反した再識別化は、FTC第５条での法執行の対象になるとする。
・ 第3要件:「事業者がかかる非識別化されたデータを他の事業者に提供する場合、それがサービス提供事業者であろうと、その他第三者であろうと、その事業者がデータの再識別化を試みることを契約で禁止すべきである」とされ、契約条項の遵守状況を監視し、契約違反に対して適切に対処するために合理的な監督を行うことが求められている。

CCPAでは、非識別化を「特定の消費者を合理的に識別することができない、それに関連しない、それを記述しない、それと関連付けることができない、又はそれと直接的若しくは間接的に結び付けることができない情報」と定義している。[134]

非識別化された情報を利用する事業者には、当該情報が帰属する消費者の再識別を禁ずる技術的な安全措置、当該情報の再識別化を明確に禁ずる手続き、及び、非識別化された情報の不注意による公開を防止するための手続を実施するとともに当該情報の再識別化を行わないことが求められる。

また、「個々の消費者の身元が除去された消費者のグループ又はカテゴリーに関する情報であり、何らかのデバイスを介しても、特定の消費者若しくは世帯に関連付けられていない、又は合理的に関連付けることができない情報」であり、集積者情報と定義し、更に集積者情報は、「非識別化された１つ又は複数の消費者記録を意味しない」としている。

CCPAでは、これら非識別化された情報及び集積消費者情報を収集、利用、保管、販売又は開示することは、同法によって制限されないと定める。

一方で、非識別化された情報を利用する事業者に、当該情報が帰属する消費者の再識別を禁ずる技術的な安全措置、当該情報の再識別化を明確に禁ずる手続及び非識別化された情報の不注意による公開を防止するための手続の実施と、当該情報の再識別化を行わないことを求めている。[135]

3.3.3 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和

COPRA、ADPPA、HIPAA等及びCCPAいずれも、日本の仮名加工情報のように、個人情報に仮名加工処理を施した仮名化された個人情報について、法令要件の具備を軽減・免責する制度は特段ない。一方で、匿名化された情報、即ち非識別化された情報は、各法令の適用対象外となる。なお上述通り、FTCやCCPA等では、再識別化を行わない義務を課している。

[134] CPRAでは、非識別化の定義を改正し、「特定の消費者に関する情報を推測するために合理的に利用されない、その他特定の消費者に合理的に結び付けられない情報」と定義している。

[135] CPRAでは、再識別化に関する規定が改正されており、非識別化された情報を保有する事業者に、特定の消費者や世帯に結び付けられないようにするための合理的な措置を講ずること、当該情報を非識別化された態様で保有及び利用し、再識別化を試みないことを公に誓約すること、及び当該情報の受領者に対して、これらのルールの遵守を契約で義務付けることが求められている。

4. 中国

前述の通り、センシティブ情報を定める法令・法規範は、中国個人情報保護法及び情報セキュリティ規範であるため、ここではその2つを中心に取り上げる。

4.1 一般的な個人情報の取扱いに対する規制

4.1.1 中国内における個人データの取扱いに関する主な法令要件

4.1.1.1 取得・利用

個人情報の取扱いにあたって、個人より同意を取得する等、法定の事由に依拠する必要がある（中国個人情報保護法第13条）。また、取り扱う前に下記事項の通知を要する（同法第17条）。

1）個人情報取扱者の名称又は氏名及び連絡方法
2）個人情報の取扱いの目的及び取扱方法、並びに取り扱う個人情報の種類及び保存期間
3）個人情報主体の権利行使の方法及び手続
4）法律・行政法規所定のその他の告知すべき事項

また、情報セキュリティ規範では、法定の例外事項に該当する場合を除き、個人情報の収集に際し、個人情報主体に一定の告知を行った上で同意取得を要するとしているため、上記の中国個人情報保護法の取扱要件と併せて要件整理すると、個人情報の取得・利用にあたっては、個人情報取得主体への法定事項の通知及び同意取得が必要である。

なお、情報セキュリティ規範では、個人情報支配者は、一定事項を含むプライバシーポリシーを制定し公表することもまた求めている。公表方法は、ホームページのトップページへの掲載その他目立つ位置にリンクを表示する等アクセスしやすくすべきとされている（同規範第5.5条）。

4.1.1.2 第三者提供・委託

まず、第三者提供に関する要件について整理する。

個人情報取扱者が、他の個人情報取扱者へ個人情報を提供する場合、個人情報の提供先、即ち受領者に関する下記の事項について、個人情報主体へ通知した上で、単独の同意を取得する必要がある（中国個人情報保護法第23条）。

1）受領者の名称又は氏名
2）連絡先
3）処理目的
4）処理方法
5）個人情報の種類

併せて、情報セキュリティ規範では、法定の例外事項に該当する場合を除き、個人情報の共有又は譲渡にあたって、下記の要件を具備する必要がある（同規範第9.2条）。

a）個人情報安全影響評価を行い、その評価結果に基づき、有効な保護措置を講じること
b）個人情報主体へ、①譲渡又は共有の目的、②受領先の類型及び③生じる可能性のある結果を通知した上、事前の同意を取得すること
c）機微情報を譲渡又は共有する場合、個人情報主体へ、上記b)と併せて、④機微情報の類型、

⑤提供先の身分（例えば、会社形態(外資、内資、合弁その他)等）、⑥データセキュリティ能力もまた通知の上、明示的同意を取得すること

d) 契約締結等を通じ、提供先の責任・義務を定める

e）記録・保存義務（①譲渡・共有の日付、②規模、③目的、及び④提供先の基本的な情報）

f）受領者(受信者)に法令違反のある場合、両当事者が個人情報処理に同意した場合、データ受領者に対し、①データ処理停止、②個人情報安全管理上のための措置、必要に応じ③取引関係の終了、④個人情報の削除、を求めること

g）データ主体の正当な権利利益を害するセキュリティ事故発生時には、個人情報管理責任者が責任を負うこと

h）個人情報主体が、自身の権利を把握することに関してサポートすること

i）個人生体識別情報は、原則として譲渡及び共有を禁止すること

次に委託に関する要件について整理する。委託元は、目的、期間、方法、対象となる個人情報の種類、保護措置、両当事者の権利義務等について、受託者と約定し、かつその約定に基づき受託者を監督しなければならない（中国個人情報保護法第21条）。なお約定する標準契約の雛型についても、同法で規定がなされている（同法第38条）。

併せて、情報セキュリティ規範では、委託先に対し安全影響評価を行い、受託者が十分なセキュリティの能力を備え、十分な安全評価レベルを提供することができることを確保し、個人情報の委託処理の状況を正確に記録・保存しなければならないと定めている（同規範第9.1条）。また、受託者が要求通りに個人情報を処理せず、保護義務を履行していないことを発見した場合、直ちに救済措置を講じ、必要に応じて受託者との業務関係を終了し、受託者に対して個人情報の即時削除を要求しなければならないとする（同規範同条）。

4.1.1.3 保管・管理

また、個人情報取扱者は、個人情報処理活動が、処理目的、処理方法、個人情報の種類、個人の権利と利益への影響、及び起こり得るセキュリティリスクに従って、法律及び行政規則に準拠することを保証するために法定の措置を講じ、不正アクセス、並びに個人情報の漏洩、改竄及び紛失を防止する安全管理措置を講じる義務を負う（中国個人情報保護法第51条）。

4.1.1.4 データローカライゼーション規制

中国個人情報保護法第38条では、海外移転制限について規定しており、「個人情報処理者が、業務上の必要性から、中華人民共和国外に個人情報を提供する必要がある場合は、以下のいずれかの条件を具備しなければならない」としている。

（1）本法第 40 条の規定に従って、国家インターネット情報公弁室によって策定されたセキュリティ評価に合格した場合

（2）国家インターネット情報公弁室の行政規則に従い、専門機関による個人情報保護認 証を実施する場合

（3）国家インターネット情報公弁室が策定した標準契約に従い、両当事者の権利及び義 務を規定した海外の受領者との契約を締結する場合

（4）法律、行政規則、又は国家インターネット情報公弁室によって策定されたその他の基準を満たす場合

また、同法第40条では、国内保存義務として、「重要情報インフラストラクチャー事業者及び国家インターネット情報公弁室によって定められた数を超える個人情報を処理する個人情報処理者は、中華人民共和国の国内で収集及び生成された個人情報を保存するものとする」と規定している。

併せて、「国外に提供する必要がある場合は、国家インターネット情報公弁室が主催する安全評価に合格しなければならない。」とし、「法律、行政規則、国家インターネット情報公弁室が安全評価を不要であると規定している場合は、当該手続に従うものとする」とも定めている。この安全評価については、2022年9月施行の「データ越境移転安全評価弁法」[136]に規定されている。

4.1.1.5 体制・責任者

当局の定めた数以上のデータを取り扱う個人情報取扱者は、個人情報取扱活動及び講じられた保護措置等の監督責任者である個人情報保護責任者の設置を要する（同法第52条）。

併せて、100万人超の個人情報、又は10万人以上の機微な個人情報を取り扱う管理者は、専任の同責任者の設置及び個人情報保護機構の設置も必要となる（情報セキュリティ規範第11条）。

4.1.1.6 本人の権利

個人情報主体は、自己の個人情報について、知る権利、処理について知ること及び決定する権利、アクセス権、複製・コピーの請求権、訂正請求権、削除請求権、個人情報処理規則に関する説明を要求する権利、同意の撤回権、が定められている（中国個人情報保護法 第15条、第44条乃至第46条、第48条）。なお、同法では、データポータビリティの権利についての定めはない。

また、情報セキュリティ規範では、中国個人情報保護法同様、訂正権、削除権、同意撤回権、複製・コピーの請求権と併せて、アカウント抹消請求権及び不服申立権を付与している（同規範第8条）。

4.1.1.7 データ侵害・インシデント

個人情報取扱者は、個人情報の漏洩等（漏洩、改竄若しくは紛失、又はそのおそれ）のある場合、直ちに是正措置を講じ、かつ、当局及び個人情報主体に通知する義務がある（中国個人情報保護法第57条）。

併せて、情報セキュリティ規範では、漏洩等の事案に対する緊急対応策を制定し、関連人員の緊急対応研修及び演習を少なくとも年１回行う必要がある。また有事の場合、制定した緊急対応策に従い、インシデント内容を記録し、その影響を評価した上で、必要な措置を講じる必要がある（同規範第10.1条及び第10.2条）

[136] 鹿 はせる「中国からの情報・データの越境移転に必要な安全評価申告の動向」長島・大野・常松法律事務所 2023年1月 https://www.noandt.com/publications/publication20230126-1/

4.2 センシティブ情報の取扱いに対し法令要件が厳格化される局面及びその加重要件

上述の中、主な加重要件を整理すると、下記の通りとなる。

1) 取扱い全般: センシティブ個人情報の取扱い全般に関して、下記1)且つ2)の場合のみ、その取扱いが認められる（中国個人情報保護法第4条第2項及び第28条第2項）。

① 特定の目的、及び目的に応じた十分な必要性があること

② 厳格な保護措置がとられていること

なお、センシティブ情報の取扱いが、個人情報主体の同意に基づく場合、個別の同意を取得する必要がある（同法第29条）。

併せて、個人情報取扱者は、センシティブ情報の取扱いに際し、事前に個人情報保護の影響評価を実施し、処理状況を記録することが求められる（同法第55条）。

更に当局の定めた数以上のデータを取り扱う個人情報取扱者は、個人情報取扱活動及び講じられた保護措置等の監督責任者である個人情報保護責任者の設置を要し（同法第52条）、10万人以上のセンシティブ情報を取り扱う場合、同責任者を専任とし、且つ個人情報保護機構の設置も必要となる（情報セキュリティ規範11.1）。

2) 取得・利用・提供: 個人情報主体への取扱いにあたり、上述Ⅲ4.1.1.1で記述の通知・告知事項と併せて、センシティブ個人情報を取り扱う必要性、及び個人情報主体の権益に対する影響についても、告知を要する（同法第30条）。なお、第三者提供時、機微情報に関しては、上記Ⅲ4.1.1.2に記述するc)の通り、一般的な個人情報に比し、通知事項が追加される。[137]

3) 保管: 情報セキュリティ規範6.3で、機微な個人情報の管理措置について記述があるが、上述Ⅲ4.1.1.3の通り、情報の種別に応じた措置をとる必要あり、実質的に特段の加重要件ではないと考える。

4.3 仮名化及び匿名化

4.3.1 仮名化

仮名化とは、個人情報を処理して、追加情報に頼らずに特定の自然人を特定できないようにするプロセスをいう（中国個人情報保護法第73条第3号）。つまり仮名化は、事業者において元の個人情報に復元可能となり得るものである。なお、仮名化は暗号化と並び、技術的安全管理措置の一方法であり、仮名化された情報は依然として個人情報に該当する。

4.3.2 匿名化

匿名化とは、個人情報を特定できず、処理後に復元できないプロセスをいう（中国個人情報保護法第73条第4号）。つまり「匿名化」は、事業者において「加工方法」や「個人情報から削除した情報」も完全に削除し、元の情報にいかなる方法をもってしても復元することのできないものである。なお、匿名化された情報は、個人情報に該当しない。

[137] 上述4.1.1.2に記述したc)の⑥を除くと、中国個人情報保護法第23条の通知事項及び同意取得方法に概ね包含し得る（そのため表Ⅲ5.2では、単独での加重要件とまではいえないと評価）。

4.3.3 仮名化又は匿名化されたセンシティブ情報に対する法令要件の緩和

日本の仮名加工情報のように、個人情報に仮名加工処理を施した仮名化された個人情報について、法令要件の具備を軽減・免責する制度は特段ない。一方で、匿名化された情報、即ち非識別化された情報は、上述の通り法令の適用対象外となる。

表Ⅲ4.2 取扱局面毎の主な法令要件とセンシティブ情報に対する要件の厳格化（中国）

局面	一般的な個人情報の主な法令要件	センシティブ情報の主な加重要件	
取得 利用	・ 適法性の根拠 ・ 本人へ法定事項を通知の上、明示的同意を取得 ・ プライバシーポリシーの公表	○	1）特定の目的と十分な必要性 2）告知事項の追加 3）本人から明示的・単独の同意取得（同意取得にあたっての通知事項の追加あり） 4）影響評価の実施 5）処理の記録 ※ 同意取得時にあたっての通知事項に追加あるものの、基本的には左記要件とほぼ同じ（参照：本稿注釈137）
提供	・ 個人情報主体への法定事項の通知＋単独の同意取得 ・ 個人情報主体が権利を把握することへのサポート ・ 個人情報安全影響評価 ・ 委託先との契約締結* ・ 記録・保存義務 （*委託の場合、併せて委託先の監督及び安全影響評価要）	N/A ※	
越境[138]	・ 移転先と標準契約の締結 （又は中国個人情報保護法§38で定めるその他いずれかの要件の具備） ・ 個人情報主体へ法定事項を通知の上、個別同意の取得	N/A	
保管管理	安全管理措置	N/A	（Ⅲ4.2 5)参照）
体制	・個人情報保護責任者の設置 ・個人情報保護機構の設置	○	（Ⅲ4.1.1.5参照）
権利	知る権利、処理について知ること及び決定する権利、アクセス権、複製・コピーの請求権、訂正請求権、削除請求権、個人情報処理規則に関する説明を要求する権利、同意の撤回権、並びにアカウント抹消請求権及び不服申立権に関する個人情報主体の権利行使への対応	N/A	—
事故	・ インシデント内容の記録 ・ 影響評価の上、是正措置を実施 ・ 当局及び個人情報主体に通知 ※平常時より緊急対応策を制定し、研修/演習年１回実施		

○: 該当, N/A: 非該当

[138] 但し、データ越境移転安全評価弁法では、直近年度の1月1日から起算して、国外に1万人のセンシティブ個人情報を提供したデータ処理者が国外に個人情報を提供するといった一定規模の越境に関しては、事前の安全評価申告を要する（本稿の注釈136参照）。なお、このような当局への申告については、膨大な書類作成や煩雑な手続きが求められることも想定され、そのため本稿では、健康・医療サービス実務上は、システム・サーバーを中国国内に設置し、当該情報へのアクセスも中国国内に限定する等、データ越境とならないサービススキームを検討すると考えられ、本稿では、グローバルヘルスケア法人における実質的な加重要件として扱わないこととする（表Ⅲ5.2ではN/Aとする）。

5. 小括

5.1 日米欧中における個人情報取扱い規制に関する比較

局面毎の取扱要件に関して共通する点について整理する。

日米欧中いずれも共通する点として、主に下記が挙げられる。

1）取得及び利用の局面に際して、原則、個人に一定事項の通知又は公表を行うこと。
それら通知又は公表事項の１つとして、利用目的があること。
2）利用・処理の局面に際して、原則、その利用目的の範囲内でのみ利用が可能であること。
3）委託の取扱局面に際して、原則、委託先に対する何らかの管理監督義務を負うこと。
その１つとして、委託先との間で権利・義務等を定めた契約を締結すること。
4）保管の局面に際して、一定の安全管理措置を実施すること
5）個人による権利行使の局面に際して、個人情報の開示の請求に対して、法的に対応義務があること。
6）インシデント発生の局面に際して、法定の場合には、当局・監督機関への通知と併せて、個人にも通知を要すること。

米国を除く日欧中に共通する点として、主に下記が挙げられる。

1）越境の局面に際して、海外移転制限が課せられており、移転可能となる要件の１つに、個人からの明示的同意の取得が含まれていること。
2）第三者提供又は越境の局面に際して、その記録を取得し保存すること

EUを除く日米中に共通する点として、主に下記が挙げられる。

第三者提供の局面に際して、オプトイン又はオプトアウトによる個人からの同意を要すること

上述した局面毎の共通点以外は、２カ国間でのみ類似する又はその国独自の取扱要件、即ち共通点というよりむしろ相違する点といえる。なお、そのような中でも、取扱要件自体に他国と比べ、特色のあるものとして前述Ⅰ2.で記述の通り、中国のみ、個人情報の国内保存義務が課せられる点が挙げられる。

また、仮名加工情報及び匿名加工情報といった、個人情報を仮名加工処理及び匿名加工処理を行うプロセス、当該処理後の情報の定義及び制度を明確に規定しているのは、日本のみといえる。

米中では、基本的に仮名化処理を施した個人情報は、個人情報として取り扱われるが、日本では、前述Ⅲ1.3の通り、一部要件が緩和される。また、GDPR上、データ管理者が、データ主体を識別する立場にないことを証明することができる、且つ、可能ならデータ主体へその旨通知する場合には、データ主体の権利に関する第15条乃至第20条は適用されないと定めていることから、EUでも仮名化による一部要件の緩和が認められている（GDPR第11条）。

匿名化処理を施した情報は、日米欧中においても非個人情報として扱われるが、米欧中では、個人情報保護法制の適用を受けないのに比べて、日本は前述Ⅲ1.3の通り、一部取扱要件の具備を要する点が、相違する点である。

5.2 日米欧中におけるセンシティブ情報取扱いの厳格化に関する比較

共通する点としては、取得の局面に際し、取扱要件が厳格化されていることが挙げられる。また、日本と同様の局面で取扱要件を加重しているのは、米国のADPPAがあげられる。それ以外は、下記表Ⅲ5.2[139]の通り、日米欧中４カ国で、同一局面で共通の加重要件はなく、各国それぞれ局面毎に加重要件を定めている。

[139] 詳細の加重要件まで含めると多岐に亘るため、本稿では、健康・医療サービスの実務上、加重要件に該当し得ると考えられる主だったものに絞り、要件整理する。

表Ⅲ5.2 センシティブ情報を取り扱うにあたって加重される主な要件

	日本	EU	米国[140]			中国
	個人情報保護法	GDPR[141]	CPRA	ADPPA	COPRA	個人情報保護法/セキュリティ規範
取得	○	○	NA	○	○	○
	明示的同意の取得	・明示的同意の取得 ・DPIA	—	法定の目的のため処理が厳格に必要とされる場合のみ取得可（忠実義務）	明示的同意の取得	明示的・単独同意の取得(含 同意取得にあたっての通知事項の追加)
利用	NA	NA	NA	○	NA	○
	—	—	—	法定の目的のため処理が厳格に必要とされる場合のみ処理可（忠実義務）	—	・ DPIAの実施, ・ 処理の記録・保存
提供	○	NA	NA	○	NA	NA
	オプトアウト禁止	—	—	明示的同意の取得（忠実義務）	—	—
越境	NA	○	NA	NA	NA	NA
	—	移転先に対する特別な種類の個人データの取扱制限・保護措置[142]	—	—	—	—

[140] FTCは取得時の明示的同意取得以外、局面毎の具体的な加重要件の規定ないため省略。またHIPAAは、PHI自体が健康・医療情報であり、別建てとしてのセンシティブ情報の定義なく、そもそも加重要件がないため省略。

[141] GDPR第9条第1項で原則取り扱い禁止と規定。但し同条第2項で、データ主体が特定の目的での取扱いに関する明確な同意を与えた場合、同条第1項は適用されないとの定めあり。同条を踏まえ実務上、データ主体より、プライバシーステートメント等により利用目的を明示の上、GDPRに則った方法で明示的同意を取得し、同意取得した利用目的の範囲内で、各局面においてデータを取扱うことになるため、取得時のみ○とする。

[142] 追加的保護措置及び開示への追加的制限を含む（21年6月欧州委員会「第三国への個人データ移転のためのSCCに関する決定」による改訂版SCC「Clause8.6」に規定）

保管	NA —	NA —	NA —	NA —	NA —	NA —
権利行使	○ 利用停止/消去の権利行使ある場合の対応義務[143]	NA —	○ 利用・開示制限権利行使求ある場合の対応義務[144]	NA —	○ 同意撤回の権利行使ある場合の対応義務(撤回手段の提供要)	NA —
体制等	NA —	○ データ保護オフィサー設置[145]	NA —	NA —	NA —	○ 個人情報保護責任者設置[146]

○: 該当, N/A: 非該当

[143] 明示的同意なく要配慮個人情報を取得した場合（通則3-8-5-1 https://www.ppc.go.jp/files/pdf/220908_guidelines01.pdf）

[144] 井上 乾介「カリフォルニア州プライバシー権法（CPRA）の概要 –「機微情報」,「共有」規制の新設ほか」ビジネス法務 2021年6月 P115

[145] 管理者又は処理者の中心的業務が、特別な種類の個人データの大規模な取扱いによって構成される場合（GDPR第37条第1項）

[146] 上述4.1.1.5に記述通り、10万人分の機微な個人情報を処理している場合、専任で設置することと併せて、個人情報保護機構の設置要

Ⅳ 結語

1. 総括

1.1. 各章のまとめ

前述Ⅰ乃至Ⅲにおいて、日米欧中の法制を概観し、各国法制の比較を基にⅠ1.3の(1)乃至(4)について論じることを通じ、米欧中と日本との間で、共通する点と異なる点を明らかにしてきた。

それを踏まえ本章で結語を述べるにあたり、各章での小括を総括した上で、日本の個人情報保護法制における特色について再度確認する。

総括の1つ目は、法制度についてである。

前述Ⅱ5.1及び表Ⅱ5.1より、日欧中3カ国においてはいずれも、国全体に適用される包括的な個人情報保護法制が整備されていること、また日米欧中4カ国においていずれも、個人情報保護法制の域外適用がなされ得る、という点で共通することがわかる。

そのことより、グローバルヘルスケア法人は、日米欧中に健康・医療サービスを展開する場合、各国における個人情報保護法制が適用されることになり、特に中国ではデータ三法、米国では連邦法や州法といったように同一国に複数の法令が存在することで、多岐に亘る法規制への対応を余儀なくされる。

総括の2つ目は、個人情報の定義についてである。

前述Ⅱ5.2及び表Ⅱ5.2より、日米欧中4カ国においていずれも、識別特定情報が個人情報に該当する点で共通すること、併せて米欧中3カ国においてはいずれも、識別非特定情報もまた個人情報に該当する点で共通することがわかる。

一方で日本では、静脈形状等生体情報や、マイナンバー等公的機関発行の個人識別符号は個人情報に該当するが、オンライン識別子等個人関連情報といった識別非特定情報はそれに該当しない、という特色のあることがわかる。

これにより米欧中と比べ日本では、個人情報が狭く定義されているといえる。

総括の3つ目は、センシティブ情報の定義についてである。

前述Ⅱ5.2及び表Ⅱ5.2より、日米欧中4カ国においていずれも、医療情報がセンシティブ情報に該当する点で共通すること、併せて、米欧中3カ国においてはいずれも、健康情報もまたセンシティブ情報に該当する点で共通することがわかる。

一方で、日本では、健康情報が非センシティブ情報、即ち要配慮個人情報に該当せず、この点に特色のあることがわかる。

これにより、米欧中と比べて日本では、個人情報の定義と同様に、センシティブ情報もまた狭く定義されているといえる。

また、総括2つ目及び3つ目より、日本では、氏名等識別特定情報に紐付く情報が健康情報である場合、その健康情報は一般的な個人情報であり、要配慮個人情報には該当しない。併せて、識別特定情報を含まず、且つオンライン識別子等個人関連情報に紐付く医療情報（以下、「個人関連医療情報」という。）及び健康情報（以下、「個人関連健康情報」という。）はいずれも、そもそも個人情報自体に該当しないため、要配慮個人情報にも該当しない、ということがいえる。

総括の4つ目は、一般的な個人情報の取扱い局面毎における規制についてである。

前述Ⅲ5.1より、日米欧中4カ国においていずれも、各局面において、共通する取扱要件があることがわかる。これを踏まえて、グローバルヘルスケア法人が、日米欧中に健康・医療サービスをローンチする場合を想定する。その場合、各国での個人情報保護法制の規制対応を行うにあたって、取扱い局面毎に共通する法令要件を整理し纏めることで、複数多岐に亘る法規制を1つ1つ個別に具備するといった過大な法令対応の工数、費用、時間等、負荷を平準化し、業務を標準化することが可能である。

総括の5つ目は、センシティブ情報についての厳格化の有無と加重要件についてである。

前述Ⅲ5.2及び表Ⅲ5.2より、日米欧中においていずれも、センシティブ情報は、法規制の厳格化がなされ、4カ国ともに取得や提供等いずれかの取扱い局面において、明示的な同意を加重要件としている。

しかし、どの取扱い局面においてどのような加重要件を課すのか、ということに関しては、国によって相違あることがわかる。なお、越境の局面で加重要件を課すのはEUのみであり、その要件は、移転先に対する特別な種類の個人データの取扱制限・保護措置であり、一方で、日米中3カ国においてはいずれも加重要件がないため、越境に際しては、一般的な個人情報と同様の法令要件の具備を要する。[147]

総括の6つ目は、センシティブ情報に仮名化または匿名化処理を施すことによる、加重要件が緩和・軽減されることの有無についてである。

前述Ⅲ5.1より、個人情報に仮名化処理と匿名化処理との処理の方法をガイドライン等で具体的に定め、その処理を施した情報を仮名加工情報及び匿名加工情報と明確に定義した上で、個人情報よりも法規制が軽減されること等を規定し制度として設けているのは、日本のみであるといえる。

まず、仮名化処理（日本では仮名加工処理）を施した個人情報については、米欧中においてはいずれも個人情報に該当する。日本では前述Ⅲ1.3の通り、個人情報である仮名加工情報と個人情報ではない仮名加工情報とが存在し、いずれも一部取扱要件が緩和され、法規制が軽減される制度となっている。[148]

また、各国法令に則り、匿名化処理（日本では匿名加工処理）を施した情報については、日米欧中4カ国においていずれも、基本的に非個人情報として扱われる点で共通する。なお、米欧中では、個人情報保護法制における法規制の適用を受けないが、日本は前述Ⅲ1.3の通り、匿名加工情報として一部取扱要件が定められており、その点が米欧中との相違点であるといえる。

このことより、個人情報とセンシティブ情報ともに、仮名化の処理を施したとしても、法規制の適用を受けることに変わりはないが、他方で、各国法令に則った匿名化処理を施した場合には、米欧中では個人情報保護法制の適用を受けず、法規制への対応が不要となる。

1.2 ヘルスケア分野における仮名化処理又は匿名化処理の有用性

総括6つ目より、センシティブ情報に仮名化処理を施しても法規制の適用を受けること、併せて各国の個人情報保護法制に則り、個人情報又はセンシティブ情報に匿名化処理、日本では匿名加工処理を施すと、法規制への対応が不要、日本では大半の法令要件が非適用[149]となることを確認した。

---

147 但し、脚注138の通り、中国は、データ越境移転安全評価弁法上、一定の場合には、事前の安全評価申告を要する。

148 なお、前述Ⅲ5.1で記述の通り、EUでも仮名化による一部要件の緩和が認められることがある（佐脇 紀代志「一問一答 令和2年改正 個人情報保護法」 商事法務 第2章 第2節 Q11）。

149 本稿Ⅲ1.3.2、Ⅲ1.3.3及び表Ⅲ1.3を参照。

ここで、匿名化処理を施したというためには、前述Ⅲの各国での仮名化及び匿名化の小節で触れた通り、再識別を不可能とする又はそれを禁ずるといった措置を講じなければならない。そのため、ヘルスケア分野においてはとりわけ、匿名化された医療情報または健康情報は、利活用が極めて困難であるといえる。

まず、1次利用即ち、健康・医療サービス運営それ自体に利活用するケースについて考えてみると、そもそも誰の医療情報又は健康情報なのか分からなくなってしまうことにより、サービスの提供そのものが不可能となってしまう。また、2次利用即ち、新たな健康・医療サービス開発のためのプログラムやアルゴリズム創出といった目的での利活用についても考えてみる。例えば、家庭血圧値が、普段は正常値内（135/85mmHg[150]）だが、ある日突然、187/147mmHgといった、正常値に比べ突出して高い数値が出た場合、ヘルスケア分野においては、その特異値・異常値にこそデータとしての価値や有用性が認められる。しかし、匿名化を施す過程で、再識別をすることができなくなる処理としてトップコーディング、いわゆる数値を丸める等の処理を経なければならず、そうすると匿名化されたデータは、健康・医療サービスにおいては、データの価値がそこなわれてしまうことになる。

そこで本稿においては、前述Ⅲでの整理を踏まえ本章で総括した結果として、健康・医療情報に対して、仮名化処理又は匿名化処理を施す措置については、Ⅰ1.2で提起したヘルスケア分野における問題に対する本質的な解決とはなり得ないと位置付けるものとする。

2. 実務的観点での提言

2.1 実務上の問題点

上述1.より、一般的な個人情報は、各国での複数多岐に亘る法規制の適用を受けることになるが、取扱い局面毎に共通する法令要件を整理し取り纏めることにより、概ね業務の標準化を行うことができるといえる。しかし健康・医療情報においては、クロスボーダーでの取扱いに際して都度、個別に国毎のセンシティブ情報への該当性が問題となる。センシティブ情報に該当すると、各国の個人情報保護法制がその取扱いに対し特別な配慮を要求する中、日米欧中の比較を踏まえると、その定義とりわけその加重要件は、国毎に異なる場合が数多く存在し得る。その一方で、実際のグローバルでのヘルスケア事業環境においては、健康・医療情報のクロスボーダーでの取扱いが常態化されていることを踏まえると、事業環境に適した法環境とはなっていない状況であるといえる。この状況こそが、グローバルヘルスケア法人がグローバルでヘルスケア事業を運営しクロスボーダーで健康・医療情報を取り扱うにあたって、相当な負担を課す土壌となっている。

そのような負担となるのは、法規制それ自体ではなく、最新の国毎の法規制を把握した上で、1つ1つ個別に加重要件に対して適合させていかなければならないことによるものである。そのため健康・医療サービスの提供国と、クロスボーダーで取り扱う健康・医療情報の性質を勘案し、国毎にセンシティブ情報の該当性について都度、個別にその法解釈を行った上で、該当すると判断した場合には、加重要件を漏れのないよう具備するといった法令対応が必要となる。そのような状況下、日本のみ健康情報が要配慮個人情報に非該当とする規定を置くことは、日本発のグローバルヘルスケア法人が、健康・医療サービスを海外展開するにあたり、国によっては健康情報がセンシティブ情報に該当することについて、そもそも認知すらすることなく、ローンチしてしまうおそれがある。

[150]「高血圧治療ガイドライン2019」第2章 P13（https://www.jpnsh.jp/data/jsh2019/JSH2019_hp.pdf）

それにより当該加重要件の不備に伴う法令違反が生じ、重大なプライバシー侵害やレピュテーションリスクを招き、延いてはヘルスケア事業の持続可能性が著しく損なわれてしまう、といった事態に陥ってしまいかねない。更には、そのような不備への是正対応として、DRプロセス上の大幅な手戻りや、プライバシーバイデザイン等を見直した上、設計変更やアプリケーション・システムの改修、といった本来避けることのできた不要且つ過度・過大な負担を強いられることとなってしまう。

この点、現行法令で、ヘルスケア分野における要配慮情報の定義を米欧中に比べ狭く規定されていることは、法人の負荷を考慮し法規制の軽減を狙ったものと考えられる。しかし上述を踏まえると、日本発となるグローバルヘルスケア法人が、グローバルで健康・医療サービスを運営し、クロスボーダーで健康・医療情報を取り扱うにあたってはむしろ、リスクと負担を増大させてしまうといえる。

2.2 施策の提言

このようなリスクと負担の増大に関する問題は、グローバルヘルスケア法人において、各国の法令調査の負荷・工数等を軽減させることと併せて、加重要件を具備する仕組みの整備を促進させることで、当該法人による自助努力を基本とした自律的な法令対応により、概ね解決し得る。そこで本稿では、その実現のために個人情報保護委員会等行政機関による下記3つの要素で構成されるガイダンス・ハンドブック等（以下、「ガイダンス等」という。）といったソフトローの策定・発行を提言する。

1つ目の要素は、日本発となるグローバルヘルスケア法人が、海外へのサービス展開を見込み先行し、日本で健康・医療サービスのPoCを実施するにあたり、健康・医療情報をクロスボーダーで取り扱うことを予め想定しそれら情報をセンシティブ情報とみなし取り扱うこと、について認知させることである。

なお、上述の表Ⅱ5.1及び表Ⅱ5.2のような参考資料を併せて提供し、国毎に都度、個別にセンシティブ情報にかかる該当性の具体的判断を行うことの負担とリスクを提示することで、その認知をより深めることができると考えられる。

2つ目の要素は、上述の通り認知させた上で、米欧中等主要各国におけるセンシティブ情報の定義や加重要件を明確にした情報提供を行うことである。[151]これによりDRプロセス上、どの国でどのようなサービス要件の定義を要し、その要件をどのように実装すべきか、といった要件の具現化がしやすくなり、そのためどの国順で行うと効率的且つ実効性・実現可能性が最適化されるのかといった、サービス事業戦略上の予測可能性を向上させることにつながると考えられる。

また、G20・グローバルサウス該当国も含めた、上述の表Ⅲ5.2のような参考資料も併せて提供し、加重要件に関するグローバルトレンドを提示することで、そのトレンドを捉えた要件について先行し、健康・医療サービスへ実装することができる。これにより、特に新興国や発展途上国において、これから新たに個人情報保護法制が制定され、また既存の法規制が強化されることでセンシティブ情報の加重要件が課せられた場合においても、プロセス上の手戻りやシステム改修といった加重の負荷を比較的軽減させることにつながると考えられる。[152]

---

[151] 現在、個人情報保護委員会は、諸外国・地域の法制度について公開している。
https://www.ppc.go.jp/enforcement/infoprovision/laws/
https://www.ppc.go.jp/files/pdf/201803_shogaikoku.pdf

[152] 健康・医療サービスのPoC・ローンチを法人の短期計画/中長期計画に計上し、当事国でのセンシティブ情報に関する加重要件を予め法令調査の上、把握しておくことで、計画的に加重要件への個別対応を実行することが可能となる。

3つ目の要素は、2つ目の要素を踏まえ最新の法動向を把握し、それら加重要件を実装する仕組みとなるプライバシーバイデザイン・プライバシーバイデフォルト（併せて以下、「プライバシーバイデザイン等という。）の整備を推奨すること、それを推奨するガイダンス等は法規範であると位置付けることである。

これは、各法人における社風・企業風土が多様であるため、その要否にかかる判断を法人のリテラシーだけに依存してしまうと、現実にはそれが後回しにされる等により実現困難となることも考えられるためである。例えば、PoCは本来、そこで発見された問題について、その重大性を判断し対策を講じるという手順を踏んだ上で、商用化につなげるというフェーズではあるが、社内外の様々な要因より、サービスの商用化・マネタイズが急かされそれを優先してしまうケース等も想定される。そのような場合には、目の前の納期をクリアすることが最優先され、日本で法定される必要最低限の取扱要件だけを具備することで、PoCを早期に収束させる方向に進むおそれがあり、プライバシーバイデザイン等の実現は極めて困難となり得る。特に実務の現場では、サービスのローンチを急かされる事業部や企画・開発部門と、法令順守・データ保護の機能を担う法務部門・情報セキュリティ管理部門において、コンフリクトの生じやすい組織構造であることも少なくない。そのため、後者の部門が拠って立つことのできる法規範を提示することが必要であると考えられる。

このようなガイダンス等により、法人自身の自助努力を促し、法人による自律的な法令対応が持続可能となるプライバシーバイデザイン等の仕組み整備を推進することで、法令違反、更には重大なプライバシー侵害及びレピュテーションリスクの低減につなげることができる。これは、実務上のベストプラクティスの1つとなり得る。なお、上述Ⅳ2.1の問題は、上述の通り法人自身の自助努力を促し、自律的な対応を推進することで概ね解決することができるため、必ずしもハードローとしての個人情報保護法の改正をしなければならないものではないと考えられる。

3. 立法的観点での提言

3.1 要配慮個人情報の定義に関する問題点

上述のような法人による自助努力のみでは解消されない問題もまた、存在すると考えられる。

PHRが進展する環境下、日本の要配慮個人情報の定義においては、健康・医療サービスの提供にあたり、一般的な個人情報である健康情報と、それを医療従事者が知り得た健康情報、即ち要配慮個人情報に該当する健康情報が、同一サーバ内に併存するといった事態を招いてしまう。

併せて、異なる健康・医療サービス間で相互運用を行うとすると、API(Application Programing Interface)等の技術を活用したデータ連携がなされることにより、他の健康・医療サービスのサーバ内でも類似した状況が発生し、更に他社とのデータ連携が続くと、その状況が拡大してしまうこととなる。これにより、実態は同一の健康情報であるにもかかわらず、法令上は取扱要件の異なる健康情報が混在・散在してしまう、といった事態も招いてしまう。

また、時系列で保管される健康情報については、医療従事者が、健康・医療サービスの活用を開始した以降の健康情報だけを参照した場合、参照された血圧値は要配慮個人情報となるが、一方でその開始前の血圧値については、参照されず氏名等の一般的な個人情報のままである、といった事態も招く。そうすると、実際には同一人物の健康情報であり、且つ同一サーバに保管されているにもかかわらず、法令上は、前者には加重要件が課されるが、後者は一般的な個人情報と同等の取扱要件のみ

適用されることとなる。このようにデータの性質は同じだが、サービス利用の開始前とその開始以降、即ち時系列のある時点から法令要件が異なる、といった事態も生じ得る。

この点、欧米では、PHRが普及している環境下においても、健康情報と医療情報はともにセンシティブ情報に該当するため、そのような事態は発生し得ず、これはPHR環境下における日本特有の問題であると考えられる。

そのような事態を招く背景として、まずそもそも医療の現場では、医療従事者が、診療・調剤等において、体重・BMI、血圧・脈拍、心電・心拍、体温、及び市販の医薬品その他患者の自己管理の下で服薬した記録等を既に活用している、ということが挙げられる。例えば前述Ⅱ1.2.2(2)で挙げる健康診断においては、健康状態を判明するにあたって、体重・BMI、血圧・脈拍、心電・心拍といった健康情報を測定する。また、前述Ⅱ1.2.2(3)で挙げる診療・調剤等の過程において、クリニック・医院や調剤薬局では、健康・医療機器、例えば体温計、電子血圧計や心電計といった機器で健康情報を計測することもあり得る。更に問診票等に、投薬記録のみならず、市販の医薬品等の服薬した記録その他自己の健康状態に関する情報を記入し提出することは一般的である。

併せて、診療・調剤等に際し、健康・医療サービス等を活用して、医療従事者が健康情報を参照する傾向にあり、そのため医療従事者による健康情報と医療情報との取扱いはシームレスな状態となっている（図Ⅳ3.1）。これには、B to Cと併せて、B to C to BやB to B to Mといった健康・医療サービスのスキームも登場する等、サービススキームの変容が影響していると考えらえる。例えば、患者であるユーザーが、健康情報や、服薬情報、既往歴、疾病等の記録を自己決定の下、医療従事者へ開示し、それら情報を診療や調剤等に活用できるようにした健康管理サービスも既に流通している。

このように昨今の診療・調剤等においてはもはや、健康情報と医療情報との境目は、実質上ほぼ無いといってもよい状態であり、両者を区別すること自体に無理があるといえ、PHRの環境下においてはむしろ両者を一体のものとして「健康・医療情報」と捉えるほうが実態に即しているといえる。

ここで、前述Ⅱ1.2.2で述べた要配慮個人情報の定義を再度確認する。政令第2条第2号では、「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（次号において「医師等」という。）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（同号において「健康診断等」という。）の結果。」とし、併せて政令第2条第３号では、「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。」と規定している。それらを補足する通則2-3のなお書きでは、「なお、身長、体重、血圧、脈拍、体温等の個人の健康に関する情報を、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該当しない。」と記述している。[153]

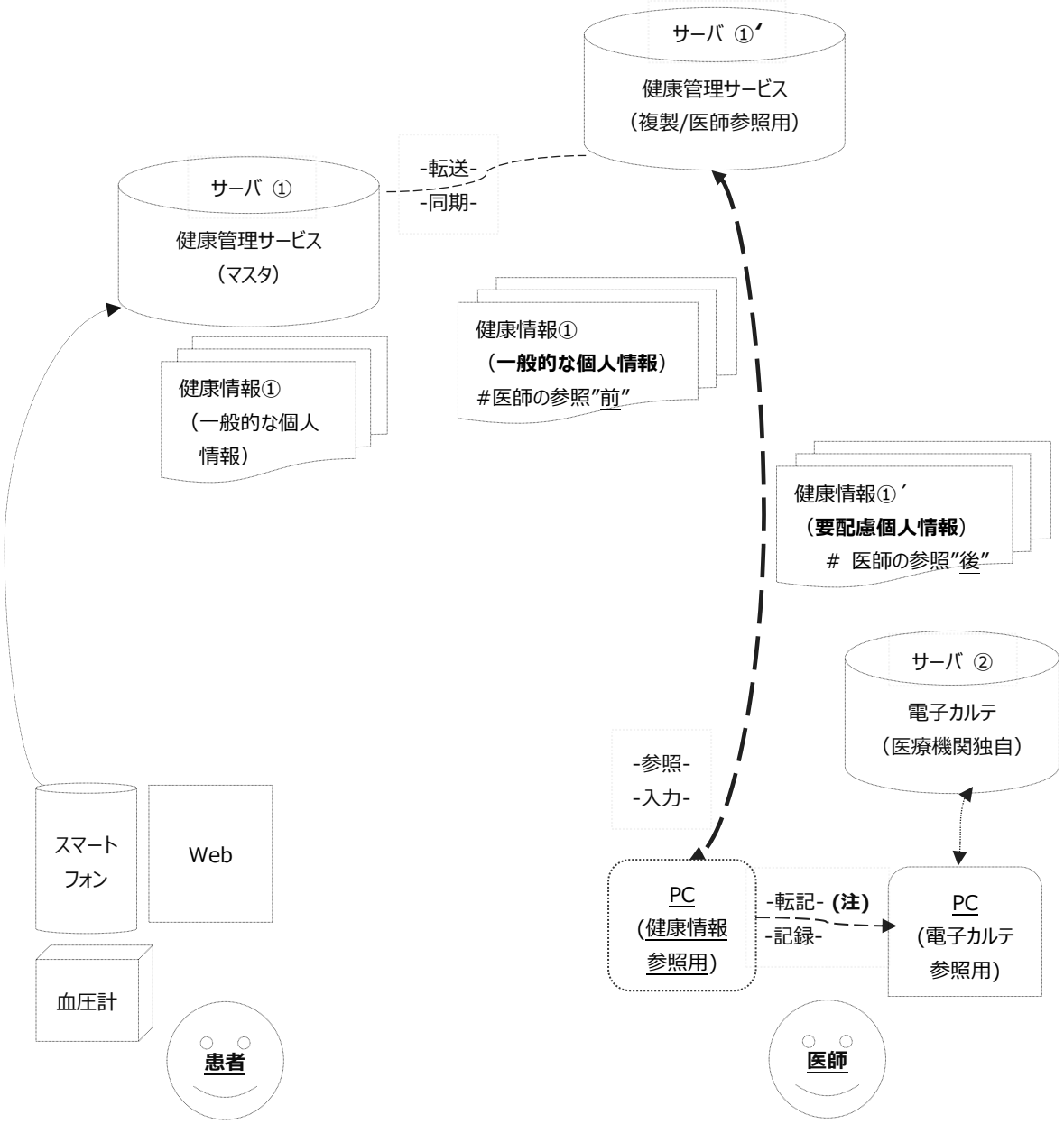
このような実態と現行法を踏まえると、健康情報と医療情報の取扱いがシームレス化し、両者が実質一体となっているにも拘わらず、医療従事者による診療等の行為の結果、及びその結果に基づく診療等の行為があったという事実、並びに診療等の過程において医療従事者が知り得た健康に関する情報をもって、要配慮個人情報と定義することが、PHR環境下、上述の問題を顕在化させる要因であると考えられる。そのため、この問題の主要因は、現行法令の法文そのものに内在すると考えられ、PHRという社会環境に見合うよう、法環境を整える又は見直す必要があるといえる。

[153] 当該政令・通則の規定では、要配慮個人情報が、法第2条でいう「本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要する」情報というより、医療従事者が守秘義務を負う情報であると捉えられかねないとも考えられる。

図Ⅳ3.1 健康サービスにおいて医療従事者が健康情報を参照する事例

・ ヘルスケア法人が、健康管理サービス上、明示的同意を得て、患者から健康情報を取得し、それをサーバ①で保管。サーバ①の健康情報を複製し、サーバ①'に転送後、サーバ①とサーバ①'の情報は持続的に同期（サーバ①とサーバ①'の健康情報は同一の状態）。
・ 以降、患者が明示的同意を行った提供先（医療機関・調剤薬局等）に対しては、健康情報を開示。それに伴い、医療従事者が、診療・調剤等において、日々の健康情報を参照する、即ち知り得た状態となる。
・ 医療従事者が診療・調剤等において知り得た健康情報は、要配慮個人情報となる。そのためサーバ①'では、医療従事者が、参照した後の健康情報即ち要配慮個人情報と、参照する前の健康情報即ち一般的な個人情報が、併存する状態となる。

(注) サーバ②内のデータ様式は、医療機関・調剤薬局毎に異なり、B to C to Mのスキーム上、サーバ①'とサーバ②間で、個別にその様式・仕様を合わせサーバ連携することは現時点、容易であるとはいえないが、今後データ様式が標準化されると、当該連携が普及され得る。



3.2 個人情報保護法令における改正の提言

上述より、現行の要配慮個人情報の定義は、PHR本来の在るべき姿に即していないといえ、法令が社会環境に適していない、追いついていないことを示しており、この点についてはもはや、法人の自助努力で解消し得る性質の問題ではないといえる。そのため、この問題の是正に関しては、ヘルスケア分野に係る要配慮個人情報についての定義の見直し、即ち法令改正が必要となる。

そこで、本論文における改正提案として、健康情報もまた医療情報と同様、要配慮個人情報に該当する、と要配慮個人情報を再定義し直す法令改正を提言したい。提言にあたっては、データの性質・機微度により要配慮個人情報を再定義するという方向で検討する。本論文における具体的な改正提案に入る前に一度、その妥当性について確認する。

まず、現行の通則2-3(9)においては、「なお、身長、体重、血圧、脈拍、体温等の個人の健康に関する情報を、健康診断、診療等の事業及びそれに関する業務とは関係のない方法により知り得た場合は該当しない。」と規定している。これは、当該業務と関係ある方法により知り得た場合には、身長、体重、血圧、脈拍、体温等であっても、要配慮個人情報に該当するものと言い換えることができると考えられ、このような健康に関する情報の機微度は、要配慮個人情報のそれに相当するものと解することができる。なお、個人情報保護委員会Webサイト掲示の「雇用管理分野における個人情報のうち健康情報を取り扱うに当たっての留意事項」（以下、「留意事項」という。）の「第2 健康情報の定義」では、健康情報を定義している。この第2では、政令第２条第２項で定める情報に関する例示のほか、第2の(18)において、「任意に労働者等から提供された本人の病歴、健康診断の結果、その他の健康に関する情報」も健康情報としている。その上で、留意事項「第3 健康情報の取扱いについて事業者が留意すべき事項」の「1 事業者が健康情報を取り扱うに当たっての基本的な考え方」(1)では、「第２の(１)から(18)に挙げた健康情報については労働者個人の心身の健康に関する情報であり、本人に対する不利益な取扱い又は差別等につながるおそれのある要配慮個人情報であるため、事業者においては健康情報の取扱いに特に配慮を要する。」と規定している。このことからも、健康情報の性質・機微度は、要配慮個人情報のそれに相当するものといえる。

次に、前述Ⅱ1.2.2を振り返ると、(1)乃至(5)の中、(2)及び(3)だけが、医療従事者が行った行為及び当該行為の結果を要件としているところ、それ以外は、「誰かが行った行為及びその結果」ではなく、「情報の性質・機微度」を要配慮個人情報の要件としていることがうかがえる。併せて同小節の「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実」という記述からも、それら情報が流出・漏洩する等し、本人に対する不当な差別、偏見その他の不利益が生じてしまうような機微度の高い情報に関して、特に配慮を要すると定めていると解される。そのため、必ずしも誰かが行った行為及びその結果を要配慮個人情報の要件とする必要はなく、むしろそれは異色の要件であるといえる。なお、血圧計、心電計、体温計や体重・体組成計といった機器での健康情報の計測は、取扱説明書等に従い正しく使用すれば、計測者が医療従事者であっても本人であっても、双方の計測値に基本、違いは生じないと考えられる。また、実際にも、前述通り、医療従事者が、患者本人が測定した健康情報を参照し、診療・調剤に活用していることからも、やはり「誰かが行った行為及びその結果」をその要件とする妥当性は特段見当たらないといえる。

以上より、医療従事者が取り扱わない血圧値・体重値といった健康情報全般においても、要配慮個人情報であると再定義することに妥当性があると考えられる。それを踏まえて、本論文における改正提案を行いたい。

3.2.1 個人情報保護法令に関する本論文における改正提案

健康情報に係る要配慮個人情報を見直し、表Ⅳ3.2.1(1)の通り、情報の性質・機微度をもって、要配慮個人情報と定義する。本論文における改正提案では、センシティブ情報の考え方を同じくし、今後もEUとの十分性認定の継続を図るにあたり、より法規制の在り方について整合をとっていくことが見込まれるGDPRにおいて定める「健康状態」を以て、健康情報に係る要配慮個人情報として、個人情報保護法第２条第３項に追加するものとする。これに伴い、政令第2条の第2項及び第3項は、「健康状態」に包含されるため、削除することとする。[154]なお、同条第3項は、「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。」と規定している。これは、心身の状態の改善が必要な状態、即ち、本人がおかれている「健康状態」を示す性質・機微度を有する情報であるといえる。このような本論文における改正提案は、他の要配慮個人情報の定義及び定義化された趣旨目的、並びにEUのみならず米中における健康情報に係るセンシティブ情報の定義と照らし、それらから大きく乖離し矛盾する点やバランスを欠くという点は特段見当たらず、むしろ現行の要配慮個人情報に内在されていた情報を例示し可視化するものであるといえる。

他方で、本改正提案は法令改正を伴うため、社会的影響度を検討する必要があり、そのため、それを採用することのメリットとデメリットとの比較考量を行う。

まず、本論文における改正提案を採用することのメリットとしては、前述Ⅳ3.1の問題解決へのアプローチとして、実務的観点での施策に比べて、より抜本的な解決策を提示することができるということが挙げられる。併せて、下記表Ⅳ3.2.1(2)の通り、米欧中では「健康情報」をセンシティブ情報に含むことより、欧米中での健康・医療情報におけるセンシティブ情報の定義と概ね同義となることで、定義のグローバル標準化にもつながることが挙げられる。

次にデメリットについても挙げていくが、本稿ではできる限り医療・介護の現場で生じ得る具体的な事例を提示することとする。

健康情報が要配慮個人情報に該当する場合、その取得、提供及び本人による権利行使の局面において、加重要件が課せられることとなる。当該加重要件として、前述の表Ⅲ5.2の通り、①取得時には本人からの明示的同意の取得、②提供時にはオプトアウトの禁止、並びに③利用停止及び消去の権利行使がある場合にその行使への対応義務が挙げられる。なお、当該③の権利行使については、表Ⅲ5.2の注釈143の通り、明示的同意なく要配慮個人情報を取得した場合に限定されている。そのため、要配慮個人情報に係る加重要件の要素は、本人からの明示的同意の取得であるといえる。

この点について、健康・医療サービス上は、アプリケーション/Webサービスであるため、ユーザー・患者等本人からの明示的同意の取得に係る設定を実施しやすい環境であるといえる。例えば、サービス利用開始におけるアカウント払出し時、再ログイン時、アプリケーション又はWebサイトのバージョンアップ

[154] 本論文における改正提案では、「健康状態」の例示として、通則2-3の新設(5)に記載することとする（参照：表Ⅳ3.2.1(1)）

時、といったタイミングで都度、アプリ内メッセージ等を用い個人情報の取扱いに関する通知を行い、アプリケーションやWebサイト上で、同意ボタン等を設定することで、明示的同意の取得又は取り直しを行うこと、即ちオプトインが都度可能である。また、そのようなサービスデザインにおいては、ユーザーにとって、サービスの開始・利用開時等に通知内容を確認の上、「同意する」あるいは「同意しない」を選択可能なフローも設定することができるため、本人のプライバシーや権益保護の観点からも、適切なサービス要件の実装が可能であるといえる。

このようなことから、健康情報に医療情報と同様の加重要件を課すことには、サービスの持続可能性に対してのボトルネックとなり得る程度のデメリットは、特段見当たらないといえる。

なお、明示的同意の取得に際して、特にアプリケーション・Webサービスのユーザーへの配慮の観点より、所謂「同意疲れ」[155]を軽減する措置と、併せてサービスの持続可能性の観点より、通知や同意取得の局面の増加に伴うユーザー離脱率を低下させる措置を講じることは別途必要であると考えられる。この措置においては、アプリケーションやWebサイト上での通知や同意措置に関するユーザビリティー、UX (User Experience)やUI (User Interface)を改善・向上させていくことが必要となる。しかし、そのような措置は、要配慮個人情報の加重要件への対応に限ったものではなく、一般的な個人情報の取扱要件として通知や同意取得を要する局面においてもまた、同様の検討を要するものであるといえる。

また、本論文における改正提案は、本稿で取り上げている健康・医療サービスといったデジタル上だけではなく、アナログ対応を併せもつ、健康・医療サービス等を導入していないようなクリニック・医院等の医療現場においても影響を与える可能性があり、そこでのデメリットについても確認しておきたい。

例えば、患者が紙・冊子の血圧手帳を診察時に医師へ提示する、といったケースが挙げられる。その場合、血圧手帳に記入の血圧値・脈拍値と別途、医師が血圧手帳に記入された血圧値を診療の過程で知り得た上で、診療録・カルテに転記されたそれら情報は、「医療に関する患者情報を含む情報で、医療従事者が記録した情報」即ち医療情報として保管・保存される。そのため、カルテ内で、一般的な個人情報に該当する健康情報と要配慮個人情報に該当する健康情報、そして医療情報と健康情報が混在する、という事態はそもそも、参照する健康情報が「紙」といったアナログであるゆえ想定され得ないと考えられる。なお、診療にあたり医師が血圧手帳を参照することで、当該手帳がたとえ要配慮個人情報に該当することになったとしても、基本的にそれは本人による自己管理の下、取り扱われ、保管される情報であることに変わりはない。

併せてその例外事例についても検討する。例えば、認知症を患う等、1人で医師に心身の状態を説明することや、身の回りのものを自己管理することが困難な介護施設の入居者に関して、介護士等が付き添い、血圧手帳等を本人に代わって、持ち運び医師に提示するケースも想定され得る。

この場合、介護士等が、同入居者から、要配慮個人情報の加重要件である明示的同意について、本人からの取得が困難であったとしても、個人情報保護法第20条第2項第2号[156]の適用等により、その行為は違法とはみなされず、また法令要件の異なる情報が混在するという事態も想定され得ない。

---

[155] 岩波 祐子「個人情報保護とデータの利活用 - デジタル化推進に向けた課題 -」立法と調査 2020.12 No.430 P29 https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2020pdf/20201218020.pdf

[156] 「個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。」の「次に掲げる」の中に「(2) 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」が掲げられている。

以上のことから、アナログ対応を併せ持つ中小規模の医療現場においても、本論文における改正提案を採用することにより、重大なプライバシー侵害を招くようなデメリットが生ずるということは、特段想定され得ないものと考えられる。

以上より、本論文における改正提案自体が、他の要配慮個人情報の定義及び定義化された趣旨目的に照らし、それらから大きく乖離し矛盾する点やバランスを欠くことなく、現行の要配慮個人情報に内在されていた情報を例示することにより可視化させることができるのと併せて、上述のメリットとデメリットを比較考量すると、法案としての妥当性は認められるといえる。

なお、補完ルール[157]は、個人情報保護法第2条第3項を引用し、それについて次の通り補完している。「EU又は英国域内から十分性認定に基づき提供を受けた個人データに、GDPR及び英国GDPRそれぞれにおいて特別な種類の個人データと定義されている性生活、性的指向又は労働組合に関する情報が含まれる場合には、個人情報取扱事業者は、当該情報について法第2条第3項における要配慮個人情報と同様に取り扱うこととする。」（補完ルール「(1)要配慮個人情報」）。本論文における改正提案が採用された際は、引用する当該法文が改訂されることは言うまでもないが、それを補完している当該規定自体には、変更は生じないといえる。むしろ今後、日本とEU及び英国間の十分性認定に係る見直しを行うにあたり、補完ルール(1)において、ヘルスケア分野での要配慮個人情報に関する追加の補完は、不要になると考えられる。

[157]「個人情報の保護に関する法律に係るEU及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール（令和5年3月一部改正)」（前述Ⅲ1.1.1.4）。

表Ⅳ3.2.1(1) 個人情報保護法令に関する本論文における改正提案（改正箇所： 下線部・太字箇所）

個人情報の保護に関する法律	本論文における改正提案
第2条第3項: この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。	第2条第3項: この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、**健康状態、**犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。
個人情報の保護に関する法律施行令	本論文における改正提案
第2条　法第二条第三項の政令で定める記述等は、次に掲げる事項のいずれかを内容とする記述等（本人の病歴又は犯罪の経歴に該当するものを除く。）とする。 (1) 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。 (2) 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（次号において「医師等」という。）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（同号において「健康診断等」という。）の結果 (3) 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。 (4) 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。 (5) 本人を少年法（昭和23年法律第168号）第3条第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。	第2条　法第二条第三項の政令で定める記述等は、次に掲げる事項のいずれかを内容とする記述等（本人の病歴又は犯罪の経歴に該当するものを除く。）とする。 (1) 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。 （**左記(2)を削除**） （**左記(3)を削除**） (**2**) 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。 (**3**) 本人を少年法（昭和23年法律第168号）第3条第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。
個人情報の保護に関する法律についてのガイドライン(通則)	本論文における改正提案
2-3 「要配慮個人情報」とは、不当な差別や偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして次の（1）から（11）までの記述等が含まれる個人情報をいう。	2-3 「要配慮個人情報」とは、不当な差別や偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして次の（1）から（11）までの記述等が含まれる個人情報をいう。

要配慮個人情報の取得や第三者提供には、原則として本人の同意が必要であり、法第27条第2項の規定による第三者提供（オプトアウトによる第三者提供）は認められていないので、注意が必要である（3-3-2（要配慮個人情報の取得）、3-6-1（第三者提供の制限の原則）、3-6-2（オプトアウトによる第三者提供）参照）。また、要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態が生じた場合には、個人情報保護委員会に報告しなければならない（3-5-3（個人情報保護委員会への報告）参照）。 なお、次に掲げる情報を推知させる情報にすぎないもの（例：宗教に関する書籍の購買や貸出しに係る情報等）は、要配慮個人情報には含まない。 （1）人種 人種、世系又は民族的若しくは種族的出身を広く意味する。なお、単純な国籍や「外国人」という情報は法的地位であり、それだけでは人種には含まない。また、肌の色は、人種を推知させる情報にすぎないため、人種には含まない。 （2）信条 個人の基本的なものの見方、考え方を意味し、思想と信仰の双方を含むものである。 （3）社会的身分 ある個人にその境遇として固着していて、一生の間、自らの力によって容易にそれから脱し得ないような地位を意味し、単なる職業的地位や学歴は含まない。 （4）病歴 病気に罹患した経歴を意味するもので、特定の病歴を示した部分（例：特定の個人ががんに罹患している、統合失調症を患っている等）が該当する。 （5）犯罪の経歴 前科、すなわち有罪の判決を受けこれが確定した事実が該当する。 （6）犯罪により害を被った事実 身体的被害、精神的被害及び金銭的被害の別を問わず、犯罪の被害を受けた事実を意味する。具体的には、刑罰法令に規定される構成要件に該当し得る行為のうち、刑事事件に関する手続に着手されたものが該当する。	要配慮個人情報の取得や第三者提供には、原則として本人の同意が必要であり、法第27条第2項の規定による第三者提供（オプトアウトによる第三者提供）は認められていないので、注意が必要である（3-3-2（要配慮個人情報の取得）、3-6-1（第三者提供の制限の原則）、3-6-2（オプトアウトによる第三者提供）参照）。また、要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態が生じた場合には、個人情報保護委員会に報告しなければならない（3-5-3（個人情報保護委員会への報告）参照）。 なお、次に掲げる情報を推知させる情報にすぎないもの（例：宗教に関する書籍の購買や貸出しに係る情報等）は、要配慮個人情報には含まない。 （1）人種 人種、世系又は民族的若しくは種族的出身を広く意味する。なお、単純な国籍や「外国人」という情報は法的地位であり、それだけでは人種には含まない。また、肌の色は、人種を推知させる情報にすぎないため、人種には含まない。 （2）信条 個人の基本的なものの見方、考え方を意味し、思想と信仰の双方を含むものである。 （3）社会的身分 ある個人にその境遇として固着していて、一生の間、自らの力によって容易にそれから脱し得ないような地位を意味し、単なる職業的地位や学歴は含まない。 （4）病歴 病気に罹患した経歴を意味するもので、特定の病歴を示した部分（例：特定の個人ががんに罹患している、統合失調症を患っている等）が該当する。 **（5）健康状態** **健康状態と関係のあるデータであって、データ主体の過去、現在及び未来の身体状態又は精神状態に関する情報を明らかにする全ての個人情報を含む。これには、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の結果や、当該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**

（7）身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること（政令第2条第1号関係） 次の①から④までに掲げる情報をいう。この他、当該障害があること又は過去にあったことを特定させる情報（例：障害者の日常生活及び社会生活を総合的に支援するための法律（平成17年法律第123号）に基づく障害福祉サービスを受けていること又は過去に受けていたこと）も該当する。 ①「身体障害者福祉法（昭和24年法律第283号）別表に掲げる身体上の障害」があることを特定させる情報 ・医師又は身体障害者更生相談所により、別表に掲げる身体上の障害があることを診断又は判定されたこと（別表上の障害の名称や程度に関する情報を含む。） ・都道府県知事、指定都市の長又は中核市の長から身体障害者手帳の交付を受け、これを所持していること又は過去に所持していたこと（別表上の障害の名称や程度に関する情報を含む。） ・本人の外見上明らかに別表に掲げる身体上の障害があること ②「知的障害者福祉法（昭和35年法律第37号）にいう知的障害」があることを特定させる情報 ・医師、児童相談所、知的障害者更生相談所、精神保健福祉センター、障害者職業センターにより、知的障害があると診断又は判定されたこと（障害の程度に関する情報を含む。） ・都道府県知事又は指定都市の長から療育手帳の交付を受け、これを所持していること又は過去に所持していたこと（障害の程度に関する情報を含む。） ③「精神保健及び精神障害者福祉に関する法律（昭和25年法律第123号）にいう精神障害（発達障害者支援法（平成16年法律第167号）第2条第1項に規定する発達障害を含み、知的障害者福祉法にいう知的障害を除く。）」があることを特定させる情報 ・医師又は精神保健福祉センターにより精神障害や発達障害があると診断又は判定されたこと（障害の程度に関する情報を含む。） ・都道府県知事又は指定都市の長から精神障害者保健福祉手帳の交付を受け、	**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、その他身長、体重、血圧、脈拍、体温等の個人の健康に関する情報が該当する。** （**6**）犯罪の経歴 前科、すなわち有罪の判決を受けこれが確定した事実が該当する。 （**7**）犯罪により害を被った事実 身体的被害、精神的被害及び金銭的被害の別を問わず、犯罪の被害を受けた事実を意味する。具体的には、刑罰法令に規定される構成要件に該当し得る行為のうち、刑事事件に関する手続に着手されたものが該当する。 （**8**）身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること（政令第2条第1号関係） 次の①から④までに掲げる情報をいう。この他、当該障害があること又は過去にあったことを特定させる情報（例：障害者の日常生活及び社会生活を総合的に支援するための法律（平成17年法律第123号）に基づく障害福祉サービスを受けていること又は過去に受けていたこと）も該当する。 ①「身体障害者福祉法（昭和24年法律第283号）別表に掲げる身体上の障害」があることを特定させる情報 ・医師又は身体障害者更生相談所により、別表に掲げる身体上の障害があることを診断又は判定されたこと（別表上の障害の名称や程度に関する情報を含む。） ・都道府県知事、指定都市の長又は中核市の長から身体障害者手帳の交付を受け、これを所持していること又は過去に所持していたこと（別表上の障害の名称や程度に関する情報を含む。） ・本人の外見上明らかに別表に掲げる身体上の障害があること ②「知的障害者福祉法（昭和35年法律第37号）にいう知的障害」があることを特定させる情報 ・医師、児童相談所、知的障害者更生相談所、精神保健福祉センター、障害者職業センターにより、知的障害があると診断又は判定されたこと（障害の程度に関する情報を含む。）

これを所持していること又は過去に所持していたこと（障害の程度に関する情報を含む。） ④「治療方法が確立していない疾病その他の特殊の疾病であって障害者の日常生活及び社会生活を総合的に支援するための法律第4条第1項の政令で定めるものによる障害の程度が同項の厚生労働大臣が定める程度であるもの」があることを特定させる情報 ・医師により、厚生労働大臣が定める特殊の疾病による障害により継続的に日常生活又は社会生活に相当な制限を受けていると診断されたこと（疾病の名称や程度に関する情報を含む。）	・都道府県知事又は指定都市の長から療育手帳の交付を受け、これを所持していること又は過去に所持していたこと（障害の程度に関する情報を含む。） ③「精神保健及び精神障害者福祉に関する法律（昭和25年法律第123号）にいう精神障害（発達障害者支援法（平成16年法律第167号）第2条第1項に規定する発達障害を含み、知的障害者福祉法にいう知的障害を除く。）」があることを特定させる情報 ・医師又は精神保健福祉センターにより精神障害や発達障害があると診断又は判定されたこと（障害の程度に関する情報を含む。） ・都道府県知事又は指定都市の長から精神障害者保健福祉手帳の交付を受け、これを所持していること又は過去に所持していたこと（障害の程度に関する情報を含む。） ④「治療方法が確立していない疾病その他の特殊の疾病であって障害者の日常生活及び社会生活を総合的に支援するための法律第4条第1項の政令で定めるものによる障害の程度が同項の厚生労働大臣が定める程度であるもの」があることを特定させる情報 ・医師により、厚生労働大臣が定める特殊の疾病による障害により継続的に日常生活又は社会生活に相当な制限を受けていると診断されたこと（疾病の名称や程度に関する情報を含む。）
（8）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（次号において「医師等」という。）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（同号において「健康診断等」という。）の結果（政令第2条第2号関係）（※） 疾病の予防や早期発見を目的として行われた健康診査、健康診断、特定健康診査、健康測定、ストレスチェック、遺伝子検査（診療の過程で行われたものを除く。）等、受診者本人の健康状態が判明する検査の結果が該当する。 具体的な事例としては、労働安全衛生法（昭和47年法律第57号）に基づいて行われた健康診断の結果、同法に基づいて行われたストレスチェックの結果、高齢者の医療の確保に関する法律（昭和57年法律第80号）に基づいて行われた特定健	（**左記(8)を削除**）

康診査の結果などが該当する。また、法律に定められた健康診査の結果等に限定されるものではなく、人間ドックなど保険者や事業主が任意で実施又は助成する検査の結果も該当する。さらに、医療機関を介さないで行われた遺伝子検査により得られた本人の遺伝型とその遺伝型の疾患へのかかりやすさに該当する結果等も含まれる。なお、健康診断等を受診したという事実は該当しない。 なお、身長、体重、血圧、脈拍、体温等の個人の健康に関する情報を、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該当しない。	
（9）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（政令第2条第3号関係）（※） 「健康診断等の結果に基づき、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が行われたこと」とは、健康診断等の結果、特に健康の保持に努める必要がある者に対し、医師又は保健師が行う保健指導等の内容が該当する。指導が行われたことの具体的な事例としては、労働安全衛生法に基づき医師又は保健師により行われた保健指導の内容、同法に基づき医師により行われた面接指導の内容、高齢者の医療の確保に関する法律に基づき医師、保健師、管理栄養士により行われた特定保健指導の内容等が該当する。また、法律に定められた保健指導の内容に限定されるものではなく、保険者や事業主が任意で実施又は助成により受診した保健指導の内容も該当する。なお、保健指導等を受けたという事実も該当する。 「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診療が行われたこと」とは、病院、診療所、その他の医療を提供する施設において診療の過程で、患者の身体の状況、病状、治療状況等について、医師、歯科医師、薬剤師、看護師その他の医療従事者が知り得た情報全てを指し、例えば診療記録等がこれに該当する。また、病院等を受診したという事実も該当する。 「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調剤が行われたこと」とは、病院、診療所、薬局、その他の	（**左記(9)を削除**）

医療を提供する施設において調剤の過程で患者の身体の状況、病状、治療状況等について、薬剤師（医師又は歯科医師が自己の処方箋により自ら調剤する場合を含む。）が知り得た情報全てを指し、調剤録、薬剤服用歴、お薬手帳に記載された情報等が該当する。また、薬局等で調剤を受けたという事実も該当する。 なお、身長、体重、血圧、脈拍、体温等の個人の健康に関する情報を、健康診断、診療等の事業及びそれに関する業務とは関係のない方法により知り得た場合は該当しない。	
「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ	本論文における改正提案
Q1-28 診療又は調剤に関する情報は、全て要配慮個人情報に該当しますか。 A1-28 本人に対して医師等により行われた健康診断等の結果及びその結果に基づき医師等により指導又は診療若しくは調剤が行われたことは、要配慮個人情報に該当します（施行令第２条第２号及び第３号）。具体的には、病院、診療所、その他の医療を提供する施設における診療や調剤の過程において、患者の身体の状況、病状、治療状況等について、医師、歯科医師、薬剤師、看護師その他の医療従事者が知り得た情報全てを指し、診療記録や調剤録、薬剤服用歴、お薬手帳に記載された情報等が該当します。また、病院等を受診したという事実及び薬局等で調剤を受けたという事実も該当します。	Q1-28 診療又は調剤に関する情報は、全て要配慮個人情報に該当しますか。 A1-28 **健康状態が含まれる情報は、要配慮個人情報に該当します （法第２条第３項）。これには、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も含まれます（ガイドライン(通則編)2-3(5)）。**
Q1-29 消費者直販型遺伝子検査の結果（いわゆるDTC 遺伝子検査の結果）は、要配慮個人情報に該当しますか。 A1-29 消費者直販型遺伝子検査の結果（いわゆる DTC（direct to consumer）遺伝子検査の結果）は、当該検査が施行令第２条第２号に規定する「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、かつ、疾病の予防及び早期発見のために行われたものである場合には、要配慮個人情報に該当します。	Q1-29 消費者直販型遺伝子検査の結果（いわゆる DTC 遺伝子検査の結果）は、要配慮個人情報に該当しますか。 A1-29 **健康状態が含まれる情報は、要配慮個人情報に該当します（法第２条第３項）。これには、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の結果も含まれます（ガイドライン(通則編)2-3(5)）。**

表Ⅳ3.2.1(2) 再掲：ヘルスケア分野におけるセンシティブ情報の定義 _米欧中（前述Ⅱ2.2.2、Ⅱ3.2.2及びⅡ4.2.2より抜粋）

EU	米国	中国
GDPR: 人種的若しくは民族的な出自、～（省略）～並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、**健康**に関するデータ～（省略） ・ 健康に関するデータ：医療サービスの提供を含め、**健康**状態に関する情報を明らかにする、自然人の身体的又は精神的な**健康**と関連する個人データ ・ データ主体の**健康**状態と関係のあるデータであって、データ主体の過去、現在及び未来の**身体状態**又は精神状態に関する情報を明らかにする**全てのデータ**含む ・ 医療サービスのための自然人の登録過程において、又はその医療サービスの当該自然に対する提供の過程において収集されるその自然人に関する情報(医療上の目的で自然人をユニークに識別するために自然人に対して特別に割り当てられた番号、シンボル又は項目)、遺伝子データ及び生化学的資料を含め、身体の一部又は身体組成物の試験若しくは検査から生じる情報、並びに医師その他の医療専門職、病院、医療機器又は体外臨床検査のような当該情報の**情報源の別を問わず**、例えば、データ主体の疾病、障害、疾病リスク、病歴、診療治療、生理学的状態又は生物医学的状態を示す全ての情報を含む。	FTC 2012年報告書: **健康**情報は、センシティブ情報であるとの見解 CPRA: ・ 遺伝データ ・ 消費者を一意に識別することを目的とした生体認証情報（生理学的、生物学的又は行動上の特徴に関する情報であって、単独又は相互に若しくは他の識別データとの組み合わせにより、個人の識別のために利用される情報） ・ 消費者の**健康**に関連して収集及び分析された個人情報 COPRA: ・ 個人の過去、現在、又は将来の身体的**健康**、精神的**健康**、障害、又は診断を説明又は明らかにする情報 ・ 生体情報 ADPPA: ・ 個人の過去、現在又は将来の身体的**健康**、精神的**健康**、障害、診断又は**健康**管理の状態若しくは治療を明らかにする情報 ・ バイオメトリック情報 ・ 遺伝情報	中国個人情報保護法: 生体認証、宗教信仰、特定身分、医療**・健康**、金融講座、行方・移動経路等の情報、及び14歳未満の未成年の個人情報 情報セキュリティ規範: 個人**健康**整理情報) 発病・治療等によって乗じた個人の関連記録 (発症、入院記録、医師指示書、検査報告、手術及び麻酔記録、看護記録、投薬記録、薬物・食物アレルギー情報、出産情報、既往歴、診療状況、家族の病歴、現病歴、感染症病歴　等)

注）健康情報に関する規定：　下線部・太字箇所

3.2.2 情報セキュリティ管理法令に関する本論文における改正提案

前述Ⅳ3.2.1では、本稿の主題である個人情報保護法制の観点からの提言を行った。但し、プライバシー保護という観点では、個人情報保護法制の遵守と併せて、情報セキュリティ管理によるデータの機密性・完全性・可用性の確保も必要であり、それらを両輪とした法令対応を講じることも重要である。そのため本小節では、情報セキュリティ管理関連法令の改正要否に関して、若干の提言を行いたい。

個人情報保護法は第23条で、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と規定している。それを受け通則3-4-2では、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならない。」としている。更に当該措置については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならないと補足している。その上で、講じるべき措置や当該措置を実践するための手法に関し、通則「10（別添）講ずべき安全管理措置の内容」[158]において、具体的な管理措置や手法の例示を挙げている。なお、個人情報保護法及び通則において、要配慮個人情報における安全管理措置上の加重要件は定めていないため、同法上、要配慮個人情報の安全管理措置は、一般的な個人情報のそれと同等となっている。

他方、医療情報に関する安全管理措置を定めた法令として、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下、「医療情報安全管理ガイドライン」という。）が制定されている。医療情報安全管理ガイドラインでは、医療情報を「医療に関する患者情報（個人識別情報）を含む情報で、医療従事者が作成・記録した情報、及び医療従事者の指示に基づき介護事業者が作成・記録した情報」と定義している。これは、個人情報の中、医療情報に該当する情報については、個人情報保護法で定める安全管理措置とは別途、医療情報安全管理ガイドラインに則った措置を講ずることについても要求するものであり、実質上、医療情報に対して、安全管理措置の側面から、加重要件を定めた法規範であるといえる。

ここで、医療情報安全管理ガイドラインの背景に存在する法律関係とその位置付けについて触れておく。

まず、医療機関・医療従事者（以下、「医療機関等」という、）と患者との間では、医療機関等は、患者との診療契約（準委任契約）による医療情報の善管注意義務を負い、且つ患者に対して刑法上の守秘義務を負う法律関係になると解される。当該善管注意義務及び守秘義務には、適切なセキュリティ体制を構築、維持、及び運用する義務が含まれる。このことから、医療情報安全管理ガイドラインの適用対象となる医療情報とは、医療機関等が、善管注意義務及び守秘義務を負い、且つ適切な安全管理措置を講ずべき義務を負う、診療において記録・作成した患者情報であるといえる。

次に、医療機関に健康・医療サービスを提供し、診療において医療情報を開示・参照させる等、医療情報における何らかの取扱いを受託するヘルスケアサービス法人と、医療機関等と間では、準委任契

[158] 通則「10 (別添)講ずべき安全管理措置の内容」P166～（https://www.ppc.go.jp/files/pdf/230401_guidelines01.pdf）

約の要素を含む契約が締結されると解される。それにより同法人は、医療機関等に対して、善管注意義務又はそれと類似の義務を負い、且つ契約上、一般的に機密保持義務を負うため、医療機関等が患者に負うのと同様に、医療機関等に対して善管注意義務及び機密保持義務を負う法律関係となる。そこで同法人は、医療機関等に対し、医療情報に関する安全管理義務を負い、患者に対する安全管理義務（の一部）の履行補助者という地位に立っているといえる。[159]そのため、医療情報安全管理ガイドラインは、当該安全管理義務を果たすために講ずべき管理措置を定めたものであるといえる。

上述を踏まえて、医療情報安全管理ガイドラインの健康情報への適用の要否について検討したい。

健康情報は、診療等の過程で、医療従事者が知り得た上、診療録・電子カルテに転記・記録された場合、その健康情報（以下、「記録健康情報」という。）は、要配慮個人情報と医療情報の両方に該当することとなる。その場合には、記録健康情報と、健康管理サービス・システムに保存され、且つ診療録・電子カルテに転記される前の健康情報は、同一の情報であるにもかかわらず、前者は医療情報安全管理ガイドラインが適用され、後者はそれが適用されないこととなる。

この場合を前述の図Ⅳ3.1に当てはめて検討すると、そもそもサーバ①に保存の健康情報と、それがサーバ①'へ転送された健康情報、及びそれをサーバ②に転記した健康情報、即ち記録健康情報いずれも実態としては同一の情報である。しかし、医療情報安全管理ガイドラインは、サーバ①には非適用、サーバ①'又はサーバ②においては、法解釈の余地あり、適用するとは断定し得ないものと考えられる。しかし、サーバ①、サーバ①'、又はサーバ②から健康情報が漏洩した場合を想定すると、いずれも実態としては同じ健康情報のため、漏洩によるプライバシーへの影響度という観点からは、いずれにおいても、その影響度は同等であるといえる。にもかかわらず、医療機関等に対するサイバー攻撃が多発する昨今、サーバ①には、個人情報保護法に定める一般的な安全管理措置だけを講じる一方で、仮にサーバ①'及び②には、それと別途、安全管理措置の加重要件を課すと解釈することは、法的なバランスを欠いているといえる。また、サーバ①'からサーバ②に転送・保存された健康情報を、もともとサーバ②に保存されている医療情報と区別し、医療情報安全管理ガイドラインの適用外と位置付ける解釈もまた、データの性質・機微度及びその取扱いの実態、並びに同ガイドラインの保護法益の考え方から乖離しているといえる。

この点を是正するためにまず以下３つの観点から、健康情報の同ガイドラインへの適用/非適用について、整理する必要があると考えられる。

１つ目は、データの性質・機微度及び医療現場におけるその取扱い実態に即しているか、という観点である。前述の通り、医療現場においては、健康情報と医療情報とは、別個の情報ではなく、実態としては同等の性質・機微度を有し、健康・医療情報という一体の情報としてシームレスに取り扱われている。

２つ目は法令の趣旨目的・保護法益に則った法解釈であるか、という観点である。

医療情報安全管理ガイドラインの対象である医療情報と、個人情報保護法上の医療情報に関する要配慮個人情報の定義は、類似しているといえる。これはいずれの情報も、無断で開示され又は漏洩してしまうことで、患者等本人に不当な差別等が生じないようにする、という本質的な保護法益が同じであることに起因するものと考えられる。

[159] 医療安全ガイドライン3.1.1(1)善管注意義務と守秘義務
https://www.meti.go.jp/policy/mono_info_service/healthcare/01gl_20220831.pdf

両者の定義における差異を敢えて挙げるとするとそれは、医療情報が、「医療従事者が（知り得た上で）作成・記録した」情報であるのに対して、要配慮個人情報は、「医療従事者が知り得た」情報であり、必ずしも「作成・記録」が要件とはなっていない、という点である。この点、図Ⅳ3.1に当てはめて考えてみたい。

まず、サーバ①‘の健康情報は、準委任契約の要素を含む契約に基づき、健康管理サービス事業者が医療機関等を代行し、サーバ①から転送することでサーバ①’に記録・作成した情報であると観念し得る。そうすると、サーバ①‘の健康情報は、「医療機関等が、善管注意義務及び守秘義務を負い、適切な安全管理措置を講ずべき、診療において記録・作成した患者情報」であると考えられ、実質、医療情報であるといえる。

また、図Ⅳ3.1の注書きの通り、健康サービスのサーバ①‘と電子カルテのサーバ②とのデータ連携は現時点において容易であるとはいえないが、仮にデータ様式・仕様を整合することができ、連携可能な場合についても考えてみる。この場合においても同様に、準委任契約の要素を含む契約に基づき、健康管理サービス事業者が医療機関等を代行し、サーバ①‘から転送することでサーバ②に記録・作成した情報であると観念し得る。そうすると、サーバ②の健康情報もまた、「医療機関等が、善管注意義務及び守秘義務を負い、適切な安全管理措置を講ずべき、診療において記録・作成した患者情報」であると考えられ、実質、医療情報であるといえる。

一方で上述した、医療情報安全管理ガイドライン上の医療情報と、個人情報保護法上の要配慮個人情報の定義の差異にのみ杓子定規に着目し判断すると、医療情報と健康情報は実質一体であるにも拘わらず、健康情報は、ある保存先サーバでは同ガイドラインが適用されるが、別の保存先サーバでは適用されないことになり得る。これは、法令の趣旨目的・保護法益に即さないものであるといえる。

３つ目は健康サービス事業者における事業運営上の特性をとらえているか、という観点である。

現行法上、健康情報は要配慮個人情報に非該当であること、その保存先によっては、医療情報安全管理ガイドラインが適用されない場合があること、併せてその適用に法解釈の余地があることから、ヘルスケア法人において、それが非適用になる方向へとバイアスがかかってしまうことが考えられる。これにより、たとえ健康情報が医療情報に該当する場合であったとしても、健康情報は非医療情報であるとの認知の歪みを生じさせ、安全管理措置の加重要件を課す医療情報安全管理ガイドラインが適用されないとの都合のよい解釈を行い、本来具備すべき加重要件を実装していないというような事態が生じることが想定される。

以上３つを踏まえると、上述Ⅲ3.2.1の本論文における改正提案と併せて、医療情報安全管理ガイドラインを改定し、健康情報が医療情報に該当するよう、医療情報を再定義する必要があると考えられる。その再定義により、健康情報に対して、その取扱いと安全管理との両方の側面から、法令要件を加重するという点で、整合がとれたものとすることが可能になる。

そこで、医療情報安全管理ガイドラインに関する本論文における改正提案としては、医療情報の定義は、個人情報保護法上の要配慮情報の定義を参照させる、又は要配慮情報の定義をそのまま引用し規定することを提案する。

併せて、安全管理措置を強化するには、負荷・工数を要するため、インセンティブを付けて推進する施策も必要であると考える。例えば、医療情報安全管理ガイドラインに準拠していることを訴求するためのマネジメントシステムの規格策定やその認証制度等の整備が挙げられる。その際、これらを独立の規格や認証制度とするのではなく、現行のISMS（情報セキュリティマネジメントシステム）やPIMS（プラ

イバシー情報マネジメントシステム）の規格を拡張し上乗せ・アドオン認証の制度とすることで、ヘルスケア法人において、類似のマネジメントシステム構築による重複する負荷をかけることのないような工夫を要する。

他方、医療情報安全管理ガイドラインに関する本論文における改正提案は、健康情報を取り扱うものの、医療情報安全管理ガイドラインの対象外とされてきた多数のサービス/システム・サーバーに対して、それが適用されることとなるため、健康サービス事業者のみならず、社会的影響度も少なくないと考えられる。そこで、本改正提案を採用するにあたってのメリットとデメリットを挙げ、比較考量を行う。

まず、この改定によるメリットとしては、上述の２つ目と３つ目の問題を解消することができ、また健康情報は、要配慮個人情報且つ医療情報であると、シンプルにわかりやすく整理することができる。これにより、データ保護の両輪である、データの取扱い手順・プロトコル（個人情報保護法）と、安全管理措置（情報セキュリティ管理法）との適用対象となる情報の定義を統一し、ヘルスケア法人における認知の歪みを防ぐことで、各法令要件を適切に実装することへつながることが期待される。また、昨今医療機関に対するサイバー攻撃が多発している中、健康・医療サービス事業者は、同サービスのアプリケーションやシステム・サーバーに関して、よりセキュリティレベルを上げていく必要がある。そのセキュリティ強化は、健康・医療サービスの差異化・優位性の確立につながり、併せて医療機関のみならず患者との間の信頼関係を構築することにもつながると考えられる。

一方、デメリットとしては、医療情報安全管理ガイドラインによる安全管理措置のシステム・サーバーへの実装に伴う工数・費用等の負担増が考えられる。ここで、同ガイドラインの主な規定を確認すると、安全管理措置に関して、①医療機関との間のリスクコミュニケーションを踏まえた合意形成、並びに②リスクマネジメントプロセスの整備及びリスクアセスメントを踏まえたリスク対応、を実施することと定めている。

この点、①については、顧客の要求事項の１つとして、何をサービス要件とし、要求仕様を定めてサービス実装するのか、また②については、リスク評価の上、回避・転嫁・軽減・受容等どのようなリスク対応を行うのか、といったように両方とも自社でそれらを判断・決定し管理し得る。このことから、予算や人的資源等のリソースを踏まえ、自社に見合った対応を行うことが可能であると考えられる。

このようにデメリットは適切に自社でセルフコントロールし得ることを踏まえると、サイバー攻撃が頻発する社会環境を鑑みた上で、メリットとの比較考量により、安全管理措置の不備による重大なプライバシー侵害とレピュテーションリスクの顕在化を防止し、サービス事業の持続可能性を確保するためにも、本論文における改正提案は必要且つ妥当なものであるといえる。

3.3. 最後に

ここで、センシティブ情報について少し振り返ってみたい。OECDの「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」において、勧告付属文書「プライバシー保護と個人データの国際流通についてのガイドライン」[160]（以下、「勧告付属文書」という。）が策定されている。勧告付属文書の「ガイドラインの適用範囲」第3条は、「本ガイドラインの原則は相互に補完的な関係にあり、すべての原則を総括的に解釈すべきである。本ガイドラインは、次のように解釈すべきではない。」とした上で、同条a)では、「個人データの性質及びその収集、保有、処理及び提供の情況から、個人デー

[160] JIPDEC (一般財団法人 日本情報経済社会推進協会) のWebサイトに掲載されているOECDプライバシーガイドラインを参照（https://www.jipdec.or.jp/library/archives/oecd_guideline.html）

タの種類の違いに応じて、異なる保護措置を適用することを妨げるもの」を挙げている。これは、ひとたび漏洩・流出した際、プライバシーを含む個人の権利利益に対して、重大な影響を及ぼす可能性ある性質や種類のデータについては、特に配慮を要する、即ち加重要件を課すことを、各国の個人情報保護法制で規定することを認めているといえる。そのことを踏まえて本稿では、国毎に個人情報保護法制上、一般的な個人情報に比べて加重要件が課される情報をセンシティブ情報であると整理する。

本稿では、当該センシティブ情報への健康・医療情報の該当性を整理した上で、主要国の中で日本のみ健康情報が非センシティブ情報に該当することを明らかにした上で、健康・医療情報の取扱い・管理に関する実務上・法令上の問題点を整理し、その解決にあたっての提言を中心に論述してきた。

最後に、前述Ⅳ1.1の総括の3つ目の後に挙げた、「日本では、個人関連医療情報及び個人関連健康情報（以下、両方併せて「個人関連健康・医療情報」という。）は、いずれも個人情報自体に該当しないため、要配慮個人情報に該当しない。」という点についての問題点とその見直しに関して、若干の示唆を提示し、結びとしたい。

個人関連健康・医療情報は、米欧中ではいずれもセンシティブ情報に該当するため、実質上は前述Ⅳ2.1で挙げた問題点が生じ得る。

これには、個人関連情報を個人情報とみなす、即ちオンライン識別子等も個人情報に該当すると定める法改正を行うことでも解決することはできるが、本稿のスコープから大幅に逸脱し、個人情報そのものの定義についての見直しにまで論点を拡大させてしまうこととなってしまう。そのため、当該問題に関しては、現時点ではやはり前述Ⅳ2.2で挙げた提言について、まずは実行することが妥当である。即ち、前述Ⅳ2.2で挙げたガイダンス等で、グローバルヘルスケア法人に対して、米欧中等海外へのサービス展開に際し、クロスボーダーで取り扱う個人関連健康・医療情報を個人情報、且つセンシティブ情報とみなすと明示し認知させ、主要各国におけるセンシティブ情報の定義等を明確にした情報提供を行った上で、プライバシーバイデザイン等の整備を促進させることが現実的であるといえる。

他方で、今後の法動向を鑑みると、個人関連健康・医療情報だけでなく、健康・医療情報に関しても、個人情報保護法とは別建ての法制を整備することが求められると考えられる。

直近では、例えば、電気通信事業法が2022年６月に改正され、利用者情報の外部送信規制（cookie規制）が整備されている。併せて、令和5年5月成立の「改正医療分野の研究開発に資するための匿名加工医療情報に関する法律」（改正次世代医療基盤法）が、研究開発等のために重要な情報を削除しない「仮名加工医療情報」を新たに創設し、個人情報保護法とは別建ての法制度を整備し、当該情報の利活用を促進している。そのため、このような法制度が体系的に整備されるまでは、上述の通りヘルスケア法人の自助努力を中心に対応するのが、当面の間は適当であると考えられ、当該法制度に関しては、今後の研究課題としたい。

参考文献：

浅井 敏雄「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第54回 カリフォルニア州消費者プライバシー法の成立とその概要」国際商事法務 Vol.46 No.8 (2018年)、「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第75回 カリフォルニア州消費者プライバシー法（CCPA）の論点」国際商事法務 Vol.48 No.6 (2020年)、及び「国際コンプライアンスの研究 第二部 国際コンプライアンスの諸相 第77回 カリフォルニア州消費者プライバシー法（CCPA）の論点」国際商事法務 Vol.48 No.8 (2020)

阿部克則「データローカライゼーション措置と国際経済法上の規律 -WTO と TPP における法的位置づけ」財務省財務総合政策研究所「フィナンシャル・レビュー 令和元年第５号（https://www.mof.go.jp/pri/publication/financial_review/fr_list7/index.htm）

渥美坂井法律事務所・外国法共同事業 「諸外国の個人情報保護制度に係る最新の動向に関する調査研究 報告書」平成30年3月（https://www.ppc.go.jp/files/pdf/201803_shogaikoku.pdf ）

石井 夏生利、曽我部 真裕、森 亮二「個人情報保護法コンメンタール」勁草書房 2021年2月

石田智也「データプライバシー・コンプライアンス体制構築のための基礎知識（前編）」ビジネス法務 2020年1月号、及び「データプライバシー・コンプライアンス体制構築のための基礎知識（後編）」ビジネス法務 2020年2月号

石川 智也、河合 優子、大竹 祥太、佐々木 将也、小出 章広、水谷 有希、久保 慶太郎、平岡咲耶「米国個人情報保護法最新動向」西村あさひ法律事務所 個人情報保護・データ保護規制ニューズレター 2022年9月6日～11月25（https://www.nishimura.com/ja/newsletters）

井上 乾介「カリフォルニア州プライバシー権法（CPRA）の概要－「機微情報」,「共有」規制の新設ほか」ビジネス法務 2021年6月号

岩村浩幸「欧州・英国データ保護法制の現状整理と今後の展望」ビジネス法務 2021年7月号

宇賀克也「新・個人情報保護法の逐条解説」有斐閣 (2021年12月)
小野 順平「カリフォルニア州消費者プライバシー法と日本企業における実務対応」国際商事法務 Vol.47 No.12(2019年)

木澤浩亮・丸山和子「Trend Eye 企業活動のグローバル化を支える 信頼ある個人データの自由な流通に向けた取組み」ビジネス法務 2020年4月号

クリス・フーフナグル著（宮下紘、板倉陽一郎、河井理穂子、國見真理子、成原彗、前田恵美訳）アメリカプライバシー法 勁草書房 2018年8月

経産省「データの越境移転に関する研究会報告書」2022年2月28日（https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/20220228_2.pdf）

今野由紀子「中国個人情報保護法・データ安全法の解説と企業対応実務（上)」 NBL No.1204(2021.10.15)号

章 啓龍（Zhang qilong）・刁 聖衍（Diao shengyan）「連載 中国における近時の重要立法・改正動向 第7回 個人情報保護法」ビジネス法務 2022年4月号

神保宏充「中国ビジネス法務Q&A 第186回 中国民法典における個人情報保護規定」国際商事法務 Vol.48，No.11 2020

Scott W. Pink，座波優子「民主党案・共和党案を比較 米国包括的個人情報保護法制定の動向」ビジネス法務 2020年10月号

鈴木翔平、松永耕明 「行動ターゲティング広告と日米欧のプライバシー保護規制（中）」ビジネス法務 2020年4月号

大地法律事務所「ネットワーク安全法（仮訳）」
（https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf）

逵本麻佑子、長谷川紘「連邦プライバシー法案の公表」長島・大野・常松法律事務所 2020年9月（https://www.noandt.com/publications/publication20220901-1/）

寺田 眞治「個人情報保護関連の海外の法制度の概要」JIPDEC 2019年９月
（https://www.jipdec.or.jp/archives/publications/J0005156.pdf）

中川裕茂「中国の個人情報保護法」の日本企業へのインパクト～GDPRとの対比を踏まえて～」国際商事法務 Vol.49，No.10 2021

中崎 尚「実務解説 GDPR対応済み企業も要注意 米国カリフォルニア州消費者プライバシー法への対応」ビジネス法務 2019年12月号

日本貿易振興機構 サンフランシスコ事務所 海外調査部「米国連邦データプライバシー法案の概要 2021年6月」（https://www.jetro.go.jp/world/reports/2021/01/7f744522a1ddc8eb.html）

日本貿易振興機構 北京事務所 ビジネス展開・人材支援部「中国におけるサイバーセキュリティー、データセキュリティおよび個人情報保護の法規制にかかわる対策マニュアル」2021年11月
（https://www.jetro.go.jp/world/reports/2021/02/0c080037fe572f0d.html）

松前 恵環「米国の法制度の概要と近時の議論動向」NBL No.1185(2021.1.1)号、「米国における「個人情報」の概念と個人識別性」NBL No.1189(2021.3.1)号、及び「米国における個人情報・プライバシー保護監督機関－FTCを中心に」NBL No.1201 (2021.9.1)号

森 規光、吉 佳宜「中国最新法律事情218 情報安全技術 個人情報安全規範」国際商事法務Vol.46，No.4 2018

森・濱田松本法律事務所（令和2年度受託法律事務所）中国民法典について（日本民法との比較を中心に）令和3年1月
（https://www.cn.emb-japan.go.jp/itpr_ja/00_000550.html）

渡邉 雅之「中華人民共和国データセキュリティ法（仮訳）」三宅法律事務所 2021年8月
（zhong_guo_detasekiyuriteifa_zhong_guo_yu_ri_ben_yu__0.docx）、
及び「逐条解説 中国個人情報保護法」三宅法律事務所
（zhu_tiao_jie_shuo_zhong_guo_ge_ren_qing_bao_bao_hu_fa__0.pdf）

原　洁（Yuan Jie）「11月1日施行，中国個人情報保護法の概要と日本企業への影響」ビジネス法務 2021年12月号

DLA Piper「*DATA PROTECTION LAWS OF THE WORLD*」
（*https://www.dlapiperdataprotection.com/index.html?c2=VN&c=CN&t=transfer*）

I. Glenn Cohen, Holly Fernandez Lynch, Effy Vayena and Urs Gasser "BIG DATA, HEALTH LAW, AND BIOETHICS" CAMBRIDGE UNIVERSITY PRESS (First published 2018 3rd published 2019)

Michael V. Tate "CALIFORNIA CONSUMER PRIVACY ACT: A Practical Guide to CCPA for Web Developers, Website Designers, and Internet Companies" RENVOI PRESS (April 2020 Edition)

Paul Lambert "The Manager's Data Protection Duties" CLARUS PRESS (2020)

Paul Lambert "Understanding the New European Data Protection Rules" CRC Press (2020)

Suzanne Dibble "GDPR" John Wiley *& Sons (2020)*

EUR-Lex（*https://eur-lex.europa.eu/eli/reg/2016/679/oj*）