

監修のことば—「個人情報法 3.0」のその先へ

個人情報保護法は、データの専門家にとっても、一般の法律家にとっても、わかりにくい特殊な法律である。

個人情報保護法は、公的部門（行政機関、地方公共団体等）はもちろん、すべての事業者がおよそ「個人情報」を取り扱う限りは規律の対象とする。そして、個人に関する情報を、事業者がどのような形態で保有・利用するか（民間部門であれば、個人情報—個人データ—保有個人データ）によって、規制の内容が変わる。その代表的なものは、個人データの第三者提供には原則として本人の同意が必要であるという規制である。同法の定める規制に違反した場合には、個人情報保護委員会による監視・監督の対象となる。

その反面で、個人のプライバシーの保護ないし自己情報コントロール権の実現を目指して、同法の規制が首尾一貫しているわけでもない。そもそも同法の目的には、プライバシーが正面から掲げられておらず、また、本人による事業者への開示請求等が認められるのは、保有個人データを対象として、法定の事由がある場合に限られる。むしろ、事業者は利用目的を特定すれば、原則としてその目的の範囲内で個人情報を取り扱うことができる。

このような個人情報保護法の規制は、見方によっては、民間部門のビジネスや公的部門の正当な行政活動に対する過剰な制約のようにも映るし、逆に個人の利益保護に必ずしも十分ではないように感じられる場面も出てくる。これは、原則として情報の内容・性質やその利用のもたらす実体的なリスクではなく、個人に関する情報の取扱い一般に関する権限を、個人と民間部門・公的部門の間で段階的に分配するというグラウンドデザインに立脚していることの、宿命であろう。

デジタル社会は、データ駆動型社会である。IT・ICTの進展、ビッグデータ、そしてAIの普及といったテクノロジーやビジネスの急激な変化に対応して、データの保護と利活用のバランスを適切に実現すべく、個人情報を取り扱うあらゆる主体が、適切な個人情報保護法の運用を探らなければならない。デジタル社会における個人や企業の活動がグローバルな側面をもつことからすれば、国際的な制度の動向に調和し、かつ、現実に執行可能なものとなるよう、法の内容そのものを不断に見直すことも求められている。

2003年の個人情報保護法の制定を「個人情報法 1.0」とすれば、民間部門の監督

権限を個人情報保護委員会に集約し、個人識別符号・要配慮個人情報・匿名加工情報等の新たな規律を設けた2015年の改正は「個人情報法2.0」と、そしてその施行の経験を踏まえて仮名加工情報等の規律を加えた2020年の改正は、「個人情報法2.1」と、それぞれ呼ぶことができる。そして、新型コロナウイルス感染症の経験を踏まえて公的部門と民間部門の縦割りの法制を一元化し、国と地方のルールを共通化した2021年の改正は、「個人情報法3.0」と呼ぶことができよう。

2024年5月現在、2020年改正法施行後のいわゆる「3年ごと見直し」の作業が本格化しているが、個人情報保護委員会が挙げた論点案や検討の進め方に対しては、経済界や識者から様々な議論が提起されているところでもある。しかし、現行法の内容とその運用を正しく理解した上で、法制度や行政・司法のあり方一般と関連づけつつ、データの取扱いに関するビジネス等の実務に関する規制の影響やその限界を的確に把握しなければ、もはや個人情報保護法のあり方を論じることは不可能になっている。

本書は、個人情報保護法の制度と実務に通暁した弁護士グループによる本格的な解説書である。政令・規則・ガイドラインの詳細はもちろん、個人情報保護委員会による行政指導等の事例も素材として、最新の知見に基づき、制度の趣旨・内容やその運用を正確かつ詳細に紹介するだけでなく、具体的な解釈上の論点を発見・分析し、さらには望ましい規制のあり方にまで踏み込んで検討を行っている点で、本書は類を見ないものと評することができよう。

本書の元になったNBL誌上での連載に当たって、筆者は毎回、素稿を用意した本書の執筆者と2時間前後、ディスカッションの機会を持った。憲法の研究を本業とする筆者にとって、企業によるデータ活用の最前線、そして規制当局の目指す方向や悩み的一端に触れながら、同時に自分よりも若く優秀な法曹と、個人情報保護法の様々な論点について、対等な立場で徹底的に議論するのは、ただただ有益な貴重な機会であったことを、この場で告白しておきたい。連載の内容が改めて体系的に整理されるとともに、最新の状況が加筆された本書のドラフトに目を通して、個人情報保護法がいよいよ本格的な解釈論の対象となった時代が到来したことを、研究者として痛感させられた。解釈論を意識しない立法論は空虚であり、立法の可能性を検討しない解釈論は自らそれと知らず限界を引くことになるが、本書は今後の法令やガイドラインの見直しにとって、第一級の基礎文献でもある。

本書が、法律家、それぞれの組織で個人情報に関するコンプライアンスに責任を有する人々はもちろん、広くデータガバナンスに関わる人々や研究者に広

く読まれることを期待して止まない。

2024年5月

東京大学教授 穴戸 常寿

はしがき

本書は、「個人情報の保護に関する法律」（個情法）をめぐる実務と立案に弁護士として深く関与してきた筆者らが、実務対応の最前線において議論されている様々な論点を幅広く紹介し、理論面での整理にも可能な限り言及しつつ、個情法の解釈を網羅することを試みた本格的な体系書である。

個情法は、2003年に成立してから既に早くも20年以上が経過したが、これまでの社会的、技術的な変化に対応して2015年、2020年、2021年に主な改正を経てきたほか、様々な解釈上の工夫も積み重ねられてきた。個人情報保護・プライバシーをめぐる法律と実務は、国内外において激動の最中にあり、海外では幅広い地域で様々なデータ保護法が制定され、グローバルなデータコンプライアンス実務においてめまぐるしい地殻変動が起きているほか、国内でも、形式的な法律の遵守にとどまらず、透明性、公正性、アカウントビリティなどを核とするプライバシーガバナンスの考え方も徐々に根付きつつある。

このような背景の下、近年、個情法の解釈や運用をめぐる議論は、急速に複雑化・高度化してきた印象がある。しかし、このように複雑で多岐に亘る論点を、理論と実務の両面から精緻に深掘りし、バランスよく体系的に解説した文献は乏しいのが実情である。当局から公表されているガイドライン（GL）やQ&Aは一見すると情報量が充実しているようにみえる一方で、実務上悩ましいセーフとアウトの境界線上の事例についての手掛かりは少なく、当局が結論を示すに至った議論・思考過程の紆余曲折が表に出ることもほとんどない。また、巷には個情法の解説書も溢れているが、単にGLやQ&Aの記載を再構成・補足した程度の情報や、当局の見解とは離れた独自の見解を述べるもの、木を見て森を見ずの断片的分析など、その内容は玉石混交である。そのため、企業の実務担当者や法曹実務家が実際の案件で直面する課題を、当局の思考様式もふまえつつフレキシブルに解決するというニーズに正面から応えられている文献は、驚くほど少ない。

筆者らは、そのような問題意識に基づき、2021年10月から2023年7月にかけて、「個人情報保護をめぐる実務対応の最前線」（NBL）と題した全16回の長期連載を行い、有難いことに多くの読者から高い評価を得ることができた。本書はこれと同様のコンセプトを踏襲しつつ、NBL連載ではカバーしきれなかった多数の論点を加筆し、直近の法改正等に基づくアップデートも拡充

した上で大幅にバージョンアップしたものである。

すなわち、本書では、単なる個情法の条文やGL、Q&A等の解説に留まらず、仮想事例をふんだんに盛り込み、実務家目線での踏み込んだプラクティスの解説を心掛けています。本書の執筆に参加している北山昇、小川智史、松本亮孝弁護士はいずれも個人情報保護委員会事務局での勤務を通じて実務と立案の双方に深く関与しており、彼らの深い経験が本書の重要なバックボーンとなっている。本書のような意欲的なプロジェクトを少人数のメンバーで完遂することは非常に難儀な作業であったが、結果として、少数精鋭を貫いたことが、全編を通じた高いクオリティと一貫性の維持を可能にしたと考えている。

さらに、個情法の条文や解釈は、今後も時代のニーズや国際的動向に応じて不断に検証し、必要があれば従来の実務や伝統的な解釈・規定を変更することも視野に入れた柔軟さが求められている。折しも個情法の2025年改正に向けたいわゆる「3年ごと見直し」の検討が現在進行形で進む中で、法のあるべき原点に立ち返って、従来積み上げられてきた解釈を再検証する必要性に思いを致すことは少なくない。そのため、NBL連載当初の段階より、東京大学の宍戸常寿教授から貴重なお時間を頂戴し、ディスカッションを通じ、実務家では見落としがちな俯瞰的な視点も含め、第一線の研究者としてのお立場からさまざまなご示唆を頂くことができた。そのような研究者と実務家の対話の成果としてのディスカッションの要旨を、本書の末尾に掲載している。もとより本書の文責は筆者ら（岡田、北山、小川、松本）にあることは言うまでもないが、宍戸教授には、本書の監修者としての役割をお引き受け下さり、いつも私達との議論に辛抱強くお付き合いいただくとともに、数えきれないほど貴重なコメントをお寄せ下さったことに、改めて御礼申し上げたい。

本書が、理論と実務の両面を深く追求するという観点から、入門者や初学者の読者にとってはやや難解な記述が少なからず含まれているかもしれない。しかし、個情法についての最低限の知識を身につけたものの、もう少し本格的に学びを深めてみたい読者の皆様のほか、明確な答えのない日々の難題に取り組む中で、他の文献等を読んでも手掛かりを得られなかった法務担当者や弁護士、研究者の皆様におかれては、是非とも本書を手にとって、その答えを探してみたい。本書が、皆様にとっての頼れる道標として、他の類書にはない解答やヒントを提供できているであろうことを、私達としては自負しているからである。

最後に、本書の執筆にあたっては、株式会社商事法務の榎元ちづる氏に、校

はしがき

正その他について多大なご尽力をいただいた。いつも直前まで私達からの無理難題に辛抱強くおつきあいいただいたことに、この場をお借りして厚くお礼を申し上げる次第である。

2024年5月

執筆者を代表して
森・濱田松本法律事務所
弁護士 岡田 淳

目 次

監修のことば—「個情法 3.0」のその先へ *i*

はしがき *iv*

凡 例 *vii*

執筆者・監修者紹介 *xiii*

第 1 編 総 論

第 1 章 個人情報保護法の変遷	2
Ⅰ 個情法制定（平成 15 年）	2
Ⅱ 個情法の平成 27 年改正	8
Ⅲ 個情法の令和 2 年改正	12
Ⅳ 個情法の令和 3 年改正	14
Ⅴ 個情法制定から令和 3 年改正までの変遷のポイント	16
第 2 章 個人情報保護法の法目的と基本理念	19
Ⅰ 個情法の法目的（法 1 条）	19
Ⅱ 個情法の基本理念（法 3 条）	26
第 3 章 基本方針・基本原則・ガイドライン等	27
Ⅰ 基本方針	29
Ⅱ 基本原則	30
Ⅲ 補完的ルール	31
Ⅳ 個人情報取扱事業者等に係るガイドライン等	33
Ⅴ 特定分野ガイドライン等	35
Ⅵ 行政機関等に係るガイドライン等	38
Ⅶ その他	39
第 4 章 個人情報保護委員会	40
Ⅰ 個人情報保護委員会の設置	40
Ⅱ 個人情報保護委員会の任務・所掌事務	42
Ⅲ 個人情報保護委員会、専門委員、個人情報保護委員会事務局	44

第 2 編 個人情報取扱事業者等の義務等

第 1 章 総 説	48
-----------	----

目 次

第2章 定 義	51
I はじめに	51
II 個人情報	53
III 個人識別符号	69
IV 要配慮個人情報	74
V 非個人情報	84
VI 個人情報データベース等（法16条1項関係）	86
VII 個人情報取扱事業者（法16条2項・2条9項、10項、11項・ 別表第2関係）	92
VIII 個人データ（法16条3項関係）	94
IX 保有個人データ（法16条4項関係）	96
X 個人関連情報（法2条7項関係）	98
XI 個人関連情報取扱事業者（法16条7項関係）	99
XII 仮名加工情報（法2条5項関係）	100
XIII 仮名加工情報取扱事業者（法16条5項関係）	101
XIV 匿名加工情報（法2条6項関係）	102
XV 匿名加工情報取扱事業者（法16条6項関係）	103
XVI 「通知」	104
XVII 「公表」	105
XVIII 「取得」	106
XIX 「提供」	108
XX 「利用」	109
XXI 「本人」	109
XXII 本人の同意	110
第3章 個人情報に関する規律	130
I 個人情報の利用目的	130
II 不適正利用の禁止	148
III 個人情報の取得	159
第4章 個人データに関する規律	178
I 個人データの管理（法22条～25条関係）	178
II 個人データの漏えい等報告・本人通知	263
III 個人データの第三者への提供	308
IV 個人データの第三者提供の例外としての「委託」	340

V	個人データの第三者提供の例外としての「事業承継」	356
VI	個人データの第三者提供の例外としての「共同利用」	358
VII	外国にある第三者への提供の制限（法 28 条関係）	368
VIII	外国から日本に越境移転された個人データの取扱い	408
IX	第三者提供に係る確認・記録義務	420
第 5 章	個人関連情報に関する規律	440
I	個人関連情報の第三者提供規制が創設された背景	440
II	法 31 条の適用の有無	453
III	本人の同意の取得方法	471
IV	提供元の確認義務・記録義務	481
V	提供先の第三者における確認義務・記録義務	485
第 6 章	保有個人データに関する規律	487
I	はじめに	487
II	保有個人データに関する事項の公表等（法 32 条 1 項関係）	488
III	保有個人データの利用目的の通知	494
IV	保有個人データの開示	496
V	第三者提供記録の開示	509
VI	訂正等の請求	512
VII	利用停止等の請求	515
第 7 章	仮名加工情報に関する規律	524
I	はじめに	524
II	仮名加工情報を作成する個人情報取扱事業者の義務等	531
III	仮名加工情報の取扱いに関する義務等	540
第 8 章	匿名加工情報に関する規律	555
I	はじめに	555
II	匿名加工情報を作成する個人情報取扱事業者の義務等	570
III	匿名加工情報の取扱いに関する義務等	584
第 9 章	認定個人情報保護団体	592
I	はじめに	592
II	認定個人情報保護団体の業務	594
III	認定の申請と対象範囲	597
IV	認定個人情報保護団体の個人情報保護指針と対象事業者の監督	599
V	認定個人情報保護団体の今後	600

目 次

第10章 本人同意原則の例外・適用除外	601
I はじめに	601
II 本人同意原則の例外（法18条3項、20条2項、27条1項、28条1項、31条1項関係）	602
III 適用除外（法57条関係）	631
第11章 域外適用	637
I はじめに	637
II 個情法における域外適用の立法経緯	638
III 域外適用が問題となる場面	645
IV 「国内にある者に対する物品又は役務の提供に関連して」	649
V 域外適用の理論と執行	652
第12章 インシデント対応（漏えい以外）、監督、罰則	655
I はじめに	655
II インシデント（漏えい等事案以外）発生時の対応	656
III 個人情報保護委員会による監督	662
IV インシデントの予防及び準備	678
V 罰 則	680
第13章 プライバシーガバナンス	686
I はじめに	686
II プライバシーガバナンスへの取組の重要性	687
III プライバシーガバナンスへの取組として実施すべき内容	692
IV プライバシーリスクへの対応の方法	704
第14章 新たなテクノロジーを取り巻く課題	711
I カメラ	711
II AI	730
III メタバース	747
IV ブロックチェーン	758

第3編 行政機関等の義務等

第1章 総 説	776
I 令和3年改正による個人情報保護法制の一元化	776
II 法第5章の規律対象となる主体	778
III 第5章の規律対象となる情報	786

第2章 個人情報等の取扱いに関する規律	789
I 総説	789
II 保有に関する制限（法61条1項・2項）	790
III 取得及び利用の際の遵守事項	791
IV 安全管理措置等	793
V 漏えい等の報告等	795
VI 利用及び提供の制限	797
VII 個人関連情報、仮名加工情報の取扱い	800
第3章 個人情報ファイルに関する規律	802
I 総説	802
II 個人情報ファイルの保有等に関する事前通知	803
III 個人情報ファイル簿の作成及び公表	805
第4章 開示、訂正及び利用停止に関する規律	807
I 総説	807
II 開示	808
III 訂正	814
IV 利用停止	816
V 開示決定等に対する審査請求	818
第5章 匿名加工情報に関する規律	819
I 総説	819
II 行政機関等匿名加工情報の取扱い	820
III 行政機関等匿名加工情報以外の匿名加工情報の取扱い	826
第6章 行政機関等の監視	827
第7章 公的部門規律と民間部門規律の交錯	829

研究者と実務家の対話—穴戸常寿教授との議論をふまえて

第1編 総論	832
第2編 個人情報取扱事業者等の義務等	835
第3編 行政機関等の義務等	887

事項索引	889
------	-----

細目次

監修のことは—「個情法 3.0」のその先へ *i*

はしがき *iv*

凡 例 *vii*

執筆者・監修者紹介 *xiii*

第 1 編 総 論

■ 第 1 章 個人情報保護法の変遷	2
I 個情法制定（平成 15 年）	2
1 OECD 8 原則	2
2 個情法制定に至る経緯	5
3 平成 15 年制定当時の個情法の概要	6
II 個情法の平成 27 年改正	8
1 平成 27 年改正に至る経緯	8
2 平成 27 年改正の概要	8
3 行個法・独個法の改正（平成 28 年改正）	10
III 個情法の令和 2 年改正	12
1 令和 2 年改正に至る経緯	12
2 令和 2 年改正の概要	12
IV 個情法の令和 3 年改正	14
1 令和 3 年改正に至る経緯	14
2 令和 3 年改正の概要	14
V 個情法制定から令和 3 年改正までの変遷のポイント	16
1 個人情報保護法制の一元化	16
2 監視監督権限の一元化	17
■ 第 2 章 個人情報保護法の法目的と基本理念	19
I 個情法の法目的（法 1 条）	19
1 個情法の法目的	19

2 「個人の権利利益」と「プライバシー」	20
(1) 「プライバシー」に関する最高裁判例	21
(2) 自己決定を中心に据える見解—自己情報コントロール権	22
(3) 自己決定を中心に据えない見解—個人情報保護を求める権利	24
(4) 個人データ処理における妥当性の利益（関連性原則）の確保を説く見解	25
II 個人情報法の基本理念（法3条）	26
■第3章 基本方針・基本原則・ガイドライン等	27
I 基本方針	29
II 基本原則	30
III 補完的ルール	31
IV 個人情報取扱事業者等に係るガイドライン等	33
V 特定分野ガイドライン等	35
VI 行政機関等に係るガイドライン等	38
VII その他	39
■第4章 個人情報保護委員会	40
I 個人情報保護委員会の設置	40
II 個人情報保護委員会の任務・所掌事務	42
III 個人情報保護委員会、専門委員、個人情報保護委員会事務局	44
1 個人情報保護委員会	44
2 専門委員	45
3 個人情報保護委員会事務局	45
第2編 個人情報取扱事業者等の義務等	
■第1章 総説	48
■第2章 定義	51
I はじめに	51

II 個人情報	53
1 「生存する」個人に関する情報	53
2 生存する「個人に関する情報」	55
コラム1 フェイク情報（個人情報該当性、訂正等、利用停止等）	56
3 特定の個人を識別することができる（個人識別性）	59
(1) 個人識別性の意義	59
コラム2 端末識別子の個人情報該当性と国際的ハーモナイゼーション	60
(2) 個人識別性の判断基準	61
(3) 当該情報に含まれる記述等による個人識別性	61
4 他の情報と容易に照合することができる（容易照合性）	61
コラム3 暗号化・ハッシュ化と個人情報該当性	64
5 個人情報（又は個人データ）該当性に関する裁判例	65
III 個人識別符号	69
1 1号個人識別符号	69
2 2号個人識別符号	71
IV 要配慮個人情報	74
1 要配慮個人情報の種類	74
2 政令で定める記述等	76
(1) 身体障害、知的障害、精神障害（発達障害を含む。）その他の規則で定める心身の機能の障害があること（政令2条1号関係）	77
(2) 本人に対して医師等により行われた健康診断等の結果（政令2条2号関係）	78
(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（政令2条3号関係）	79
(4) 本人を被疑者又は被告人として、逮捕、搜索、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（犯罪の経歴を除く。）（政令2条4号関係）	80
(5) 本人を少年法3条1項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保	

護事件に関する手続が行われたこと（政令2条5号関係）	80
3 機微（センシティブ）情報	80
コラム4 海外のデータ保護法と個情法のセンシティブデータの対象の違い	83
V 非個人情報	84
VI 個人情報データベース等（法16条1項関係）	86
1 「個人情報を含む情報の集合物」	86
2 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの（法16条1項1号）	87
コラム5 検索エンジン	87
3 特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの（法16条1項2号）	89
4 適用除外	89
VII 個人情報取扱事業者（法16条2項・2条9項、10項、11項・別表第2関係）	92
VIII 個人データ（法16条3項関係）	94
IX 保有個人データ（法16条4項関係）	96
X 個人関連情報（法2条7項関係）	98
XI 個人関連情報取扱事業者（法16条7項関係）	99
XII 仮名加工情報（法2条5項関係）	100
XIII 仮名加工情報取扱事業者（法16条5項関係）	101
XIV 匿名加工情報（法2条6項関係）	102
XV 匿名加工情報取扱事業者（法16条6項関係）	103
XVI 「通知」	104
XVII 「公表」	105
XVIII 「取得」	106
XIX 「提供」	108
XX 「利用」	109
XXI 「本人」	109
XXII 本人の同意	110
1 同意をめぐる議論の法的な枠組みと一般的な解釈	111
(1) 同意の法的性質（個情法上の同意と私法上の同意）	111
(2) 個情法上の同意の取得方法	112

ア	明示の同意と黙示の同意	112
イ	個別の同意と包括的同意	113
ウ	具体的に問題となりやすい同意の取得方法	114
(3)	同意の法的位置付けについての国際比較	116
2	プライバシーポリシーを通じた同意取得に伴う実務上の論点	118
3	同意の撤回、意思表示の瑕疵	123
(1)	同意の撤回の可否	123
(2)	意思表示の瑕疵	124
4	本人が未成年である場合の同意	125
5	通信の秘密との交錯をめぐる実務上の論点	126

■第3章 個人情報に関する規律……………130

I 個人情報の利用目的……………130

1	はじめに	130
2	利用目的の特定	131
(1)	具体的な特定の程度	131
	コラム6 業界団体やプラットフォームの自主ルール、各国法への対応	132
(2)	処理方法を特定することの要否	133
	コラム7 プロファイリング	135
	コラム8 アルゴリズムの開示をめぐる議論	136
(3)	第三者提供と利用目的の関係	137
(4)	第三者から受領した個人情報と利用目的の関係	137
(5)	委託先における利用目的の特定	138
(6)	非個人情報として活用する場合の、利用目的の特定	138
(7)	特定分野ガイドラインにおける規律	139
ア	金融 GL	139
イ	信用 GL	140
3	利用目的の変更	140
(1)	変更が認められる範囲	140
(2)	平成27年改正との関係	143
(3)	変更後の手続（通知・公表）	144

4	利用目的による制限（法 18 条）	144
(1)	目的外利用の制限（法 18 条 1 項）	144
	コラム 9 データ最小化原則との関係	146
(2)	事業の承継（法 18 条 2 項）	146
(3)	利用目的による制限の例外（法 18 条 3 項）	147
II	不適正利用の禁止	148
1	はじめに	148
2	各要件の意義	149
(1)	「違法又は不当な行為」	149
(2)	「助長し、又は誘発する」	149
(3)	「おそれ」がある方法	149
3	不適正利用に該当する具体例	150
	コラム 10 不適正利用と独占禁止法における優越的地位の濫用	153
	コラム 11 内定辞退率の提供と不適正利用	154
4	個情法のあるべき姿との関係（手続的規律から実体的規律へ）	155
III	個人情報取得	159
1	はじめに	159
2	適正取得（法 20 条 1 項）	159
(1)	規律の内容	159
(2)	カメラ画像の取得と適正取得の関係	161
(3)	「取得の委託」と適正取得をめぐる論点	163
(4)	サイバーセキュリティと適正取得をめぐる論点	165
3	要配慮個人情報の取得（法 20 条 2 項）	165
(1)	本人からの同意取得の原則	165
(2)	プロファイリングを通じた要配慮個人情報の生成	166
(3)	例外	167
4	取得に際しての利用目的の通知・公表等（法 21 条）	170
(1)	はじめに	170
(2)	直接書面取得の場合のルール（法 21 条 2 項）	170
	ア 直接書面取得の範囲	171
	イ 「明示」の意義	173
	ウ 適用除外事由	173
(3)	間接取得、直接非書面取得の場合のルール（法 21 条 1 項）	174

コラム 12 求人・求職の場面における個人情報の取得	174
(4) 適用除外事由（法 21 条 4 項）	175
ア 法 21 条 4 項 1 号	175
イ 法 21 条 4 項 2 号	175
ウ 法 21 条 4 項 3 号	176
エ 法 21 条 4 項 4 号	176

■ 第 4 章 個人データに関する規律178

I 個人データの管理（法 22 条～25 条関係）178

1 はじめに	178
2 データ内容の正確性の確保等（法 22 条関係）	179
(1) 個人データの正確性・最新性の確保	179
ア 個人データの正確性・最新性を確保する義務の趣旨（努力義務）	179
イ 「利用目的の達成に必要な範囲内」	180
ウ 「正確かつ最新の内容」	180
(2) 個人データの消去義務	182
ア 個人データの消去義務の趣旨（努力義務）	182
イ 「利用する必要がなくなったとき」	183
ウ 「遅滞なく消去」	184
3 安全管理措置（法 23 条関係）	184
(1) 概 説	184

コラム 13 サイバーセキュリティ 187

(2) 講ずべき安全管理措置の内容	188
ア 基本方針の策定	188
イ 個人データの取扱いに係る規律の整備	189
ウ 組織的安全管理措置	189
(ア) 組織体制の整備	190
(イ) 個人データの取扱いに係る規律に従った運用	190
(ウ) 個人データの取扱状況を確認する手段の整備	191
(エ) 漏えい等事案に対応する体制の整備	192
(オ) 取扱状況の把握及び安全管理措置の見直し	192

エ	人的安全管理措置	193
オ	物理的安全管理措置	194
	(ア) 個人データを取り扱う区域の管理	194
	(イ) 機器及び電子媒体等の盗難等の防止	195
	(ウ) 電子媒体等を持ち運ぶ場合の漏えい等の防止	196
	(エ) 個人データの削除及び機器、電子媒体等の廃棄	196
カ	技術的安全管理措置	197
	(ア) アクセス制御	198
	(イ) アクセス者の識別と認証	199
	(ウ) 外部からの不正アクセス等の防止	200
	(エ) 情報システムの使用に伴う漏えい等の防止	200
キ	外的環境の把握	201
(3)	安全管理措置義務違反と個人情報による執行事例	205
4	従業者の監督（法 24 条関係）	251
	(1) 「従業者」とは	251
	(2) 「必要かつ適切な監督」の内容	252
	コラム 14 社内モニタリングと従業者のプライバシー	253
5	委託先の監督（法 25 条関係）	254
	(1) 個人データの取扱いの全部又は一部を委託する場合	254
	(2) 必要かつ適切な監督	256
	ア 適切な委託先の選定	256
	イ 委託契約の締結	257
	ウ 委託先における個人データ取扱状況の把握	259
	(3) 監督義務の対象である「委託を受けた者」	260
	(4) クラウドサービスの利用が個人データの取扱いの「委託」に該当する場合の監督義務	261
II	個人データの漏えい等報告・本人通知	263
1	はじめに	263
2	「漏えい等」の考え方	265
	(1) 漏えい	265
	ア 漏えいの判断における個人情報取扱事業者の帰責性	266
	イ 第三者に閲覧されないうちに全てを回収した場合	267
	ウ 漏えいと提供の区別	268

コラム 15 第三者提供規制違反と漏えい等報告	269
(2) 減失	270
(3) 毀損	271
3 漏えい等事案への対応	272
(1) ガイドラインにおいて求められる対応	272
ア GL 通則編において求められる対応	272
イ 分野別 GL において求められる対応	272
(ア) 金融分野	273
(イ) 電気通信事業分野	275
(2) 対応の具体的な内容	275
ア 事業者内部における報告	275
イ 初動対応	275
ウ 対外的な対応とその後の調査	276
エ 再発防止策	276
オ 故意による漏えい等事案における、行為者等への対応	277
カ 本人に対する補償	278
コラム 16 自主的な補償と訴訟提起した場合の認容金額	278
キ 取引先に対する対応	279
(3) 漏えい等事案に備えた事前対応	280
ア 業務フローの確立、社内規程・マニュアルの整備	280
イ ログの取得・保存	280
ウ 個人データの取扱いを委託する場合の契約条項	280
4 漏えい等報告（法 26 条 1 項）	281
(1) 報告対象事態	281
ア いわゆる「漏えい元基準説」をめぐる論点	283
イ 要配慮個人情報への漏えい等（規則 7 条 1 号）	285
ウ 財産的被害の生じるおそれがある漏えい等（規則 7 条 2 号）	285
エ 不正の目的によるおそれがある漏えい等（規則 7 条 3 号）	287
オ 1,000 人を超える漏えい等（規則 7 条 4 号）	290
カ 漏えい等が発生したおそれがある事態	291
キ 漏えい等報告の対象外となるデータ	294
(ア) 高度な暗号化等の秘匿化	294
(イ) 仮名加工情報	296

(ウ) その他の情報	296
(2) 報告義務の主体	296
ア 委託の場合	297
イ 共同利用の場合	297
(3) 速報	297
ア 速報の時間的制限・報告事項	297
イ 報告先	299
ウ 報告の方法	300
(4) 確報	300
(5) 任意の報告	301
(6) 委託元への通知による例外 (法 26 条 1 項ただし書)	301
5 本人への通知 (法 26 条 2 項)	303
(1) 通知対象となる事態及び通知義務の主体	303
(2) 通知の時間的制限	304
(3) 通知の内容	304
(4) 通知の方法	305
(5) 通知の例外 (法 26 条 2 項ただし書)	306
(6) 公表	306
Ⅲ 個人データの第三者への提供	308
1 はじめに	308
2 どのような場面で第三者提供規制が適用されるのか	309
(1) 「個人データ」の意義 (いわゆる提供元基準説)	309
コラム 17 手術動画提供事案と「個人データ」該当性	311
(2) 「第三者」の意義	312
(3) 「提供」の意義	312
(4) 事業者を通じた第三者提供か、本人による直接提供か	314
(5) 事業者を通じた第三者提供か、第三者による本人からの直接取得か	314
(6) クラウドサービスの利用は「提供」に該当するか (いわゆる「クラウド例外」)	319
ア 従来からの議論をふまえた解釈	319
コラム 18 保守サービス事業者を活用する場面での「提供」の該当性	322

コラム 19 SaaS へのクラウド例外の適用	323
イ 令和 2 年改正法による影響	324
3 第三者提供規制が適用される場合の本人同意原則	327
(1) 原則的な考え方	327
(2) 個人関連情報の第三者提供に係る同意との対比	328
4 本人同意原則の例外（法 27 条 1 項各号）	329
5 オプトアウトによる第三者提供（法 27 条 2 項～4 項）	329
コラム 20 「闇名簿」の社会問題化と個人情報への対応	331
(1) オプトアウトが認められる個人データの範囲	331
コラム 21 二重のオプトアウト禁止規定と、企業データベース事業への影響	332
(2) 本人に事前通知等する必要のある事項	333
ア 「必要な期間」の意義	335
イ 「本人が容易に知り得る状態に置く」の意義	336
(3) 個人情報への事前届出	337
コラム 22 事前届出制の実務における運用	337
(4) 個人情報及び事業者による公表	338
(5) オプトアウト事項の変更等	338
IV 個人データの第三者提供の例外としての「委託」……………	340
1 はじめに	340
2 委託に関する基本的な概念	341
(1) 個人データの取扱いの委託と業務委託の関係	341
(2) 戻し行為と取得の委託	342
ア 戻し行為	343
イ 取得の委託	343
3 個人データの取扱いの委託を分析する視点	344
(1) 問題となる行為の特定	344
(2) 解釈上のルール	345
ア 委託先による独自利用の禁止（上記(1)④に関連）	345
(ア) 原則的な考え方	345
(イ) 取得の委託の場合	346
(ウ) 「委託された業務における個人データの取扱い」につ	
いての判断	347

(エ) 委託先における匿名加工情報の作成・統計情報の作成	348
(オ) 委託先における独自利用が行われた場合の個人情報との関係	349
イ いわゆる「混ぜるな危険」(上記(1)②・③に関連)	350
(ア) 原則的な考え方	350
(イ) 戻し行為がない場合	352
(ウ) 「混ぜるな危険」に抵触しないための対応	353
(エ) 委託先による統計情報の作成	354
V 個人データの第三者提供の例外としての「事業承継」	356
VI 個人データの第三者提供の例外としての「共同利用」	358
1 はじめに	358
2 共同利用の具体例と要件	358
(1) 共同利用の要件	359
(2) 共同利用に係る事項の変更	360
(3) 共同利用に際して事業者間で取り決めるべき事項	361
3 共同利用者の範囲、追加	362
(1) 共同利用者の範囲	362
(2) 共同利用者の追加	364
4 すでに取得済みの個人データを他の事業者と共同して利用する場合の留意事項	364
5 共同利用にも「混ぜるな危険」のルールが適用されるか	366
VII 外国にある第三者への提供の制限(法28条関係)	368
1 はじめに	368
2 越境移転規制の概要	368
3 「外国にある第三者」の意義	370
(1) 「外国」の意義	370
(2) 「第三者」の意義	370
ア 別の法人格を有するかという基準	370
イ サーバの所在地は判断基準ではない	371
ウ 外国法人が日本国内で個人情報取扱事業者であるとき	371
4 基準適合体制の整備の基準	372
(1) 当該第三者との間で、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、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（規則 16 条 1 号）	373
ア 適切かつ合理的な方法	373
イ 法第 4 章第 2 節の規定の趣旨に沿った措置	374
(2) 当該第三者が、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（規則 16 条 2 号）	376
コラム 23 APEC/CBPR	376
5 外国にある第三者への個人データの提供を認める旨の本人の同意	377
6 越境移転に係る情報提供義務等	378
(1) 本人の同意に基づく場合の情報提供義務	378
ア (I) 外国の名称	381
イ (II) 当該外国における個人情報の保護に関する制度	381
ウ (III) 外国にある第三者が講ずる個人情報の保護のための措置に関する情報	386
エ 本人の同意に関する論点	386
(ア) 本人の同意を得る時点で提供先が特定できない場合等の取扱い	386
(イ) 本人の同意を得る時点で提供先等は特定できるが調査義務を果たせない場合	388
(ウ) 同意取得後に外国の個人情報保護制度に変更があった場合の取扱い	390
(エ) 委託先に対する個人情報上の監督義務と提供の根拠との関係	391
(2) 基準適合体制の整備を根拠とする場合に講ずべき措置と情報提供義務	392
ア 提供元の事業者が講ずべき「必要な措置」の内容	393
(ア) (I) 移転先における相当措置の実施状況及びそれに影響を及ぼし得る外国の制度の有無・内容の定期的な確認（定期的な確認義務）	393
(イ) (II) 適正な取扱いに問題が生じた場合の対応	395
イ 相当措置の継続的な実施の確保に関する情報提供	396
ウ 基準適合体制の整備に関する論点	399
(ア) 国内の委託先が外国にある第三者に再提供する場合の	

法 28 条 3 項の義務を負う主体	399
(イ) 提供先の外国にある第三者による個人データの再提供 への対応	399
7 越境移転のための法的根拠の選択肢の比較	400
(1) 法 28 条の本人の同意を根拠とする場合	402
ア 情報提供義務	402
イ 定期的な確認義務及び監督義務	403
(2) 基準適合体制の整備を根拠とする場合	403
ア (Ⅱ) 法 27 条の委託・共同利用等	403
(ア) 情報提供義務	403
(イ) 定期的な確認義務、監督義務	404
イ (Ⅲ) 法 27 条の本人の同意	404
(ア) 情報提供義務	404
(イ) 定期的な確認義務、監督義務	405
(3) 法 28 条の国・地域指定を根拠とする場合	405
8 越境移転に係る情報提供義務と外的環境の把握との異同	405
Ⅷ 外国から日本に越境移転された個人データの取扱い	408
1 はじめに	408
2 外国にある事業者から個人データの提供を受ける場合の規律	408
3 充分性認定とは	409
4 充分性認定に基づき欧州から移転された個人データの取扱い (補完的ルールの解説)	411
(1) 補完的ルールの適用範囲	411
(2) 補完的ルールの内容	411
ア 要配慮個人情報(法 2 条 3 項関係)	412
イ 利用目的の特定、利用目的による制限(法 17 条 1 項、18 条 1 項、30 条 1 項・3 項関係)	412
ウ 外国にある第三者への提供の制限(法 28 条、規則 16 条関 係)	415
エ 仮名加工情報(法 2 条 5 項、16 条 5 項、41 条関係)	417
オ 匿名加工情報(法 2 条 6 項、43 条 1 項・2 項関係)	418
Ⅸ 第三者提供に係る確認・記録義務	420
1 はじめに	420

2	確認・記録義務の適用範囲	421
(1)	総論	421
(2)	法令上の例外	422
(3)	解釈上の例外1—提供者・受領者に確認・記録義務が適用されない場合	422
ア	「提供者」の考え方	422
(ア)	本人による提供	422
(イ)	本人に代わって提供	423
イ	「受領者」—本人側に対する提供の考え方	425
ウ	「提供」行為の考え方	426
(4)	解釈上の例外2—受領者に確認・記録義務が適用されない場合	426
ア	「個人データ」該当性	427
イ	「提供を受けるに際して」の該当性	428
3	確認記録義務の履行方法	429
(1)	受領者の確認義務	429
ア	確認事項・確認方法	429
イ	同一の提供者から個人データの提供を受ける場合	431
(2)	提供者・受領者の記録義務	432
ア	記録事項	432
(ア)	提供者の記録事項	432
(イ)	受領者の記録事項	433
(ウ)	記録事項の省略	435
イ	記録の作成方法	435
(ア)	記録の作成主体	435
(a)	記録の作成義務の代行	435
(b)	委託先が「提供」した場合／「提供を受けた」場合	435
	コラム 24 委託先の記録作成義務	436
(イ)	記録を作成する媒体	436
(ウ)	記録の作成方法	436
(a)	原則	436
(b)	一括して記録を作成する方法	437
(c)	契約書等の代替手段による方法	437
ウ	記録の保存期間	438

■ 第5章 個人関連情報に関する規律	440
I 個人関連情報の第三者提供規制が創設された背景	440
1 はじめに	440
2 個人関連情報の第三者提供規制の位置づけ	440
(1) 個人情報の定義と提供規制の関係	440
(2) 個人関連情報の提供規制が創設された経緯	441
3 「個人関連情報」	444
(1) 「個人」の考え方	445
(2) 「関する」の範囲	446
コラム 25 個人関連情報の取得	447
(3) 個人情報か個人関連情報か	448
4 「個人関連情報データベース等」	451
5 「個人関連情報取扱事業者」	452
II 法31条の適用の有無	453
1 「提供」	453
(1) ウェブサイト間での情報の引継ぎ	453
(2) アクセス解析ツールの場合	456
ア 一次的な取得者をツール提供事業者とする考え方	457
イ 一次的な取得者をサイト運営者とする考え方	457
(3) いわゆるデータクリーンルーム	458
2 個人関連情報の第三者提供に委託の例外がないこと	460
(1) 委託先において個人関連情報となる場合の委託先から委託元への戻し行為	461
(2) 委託先において個人関連情報となる場合の個人データの取得の委託	462
3 「個人データとして取得することが想定されるとき」	464
(1) 「個人データとして取得する」	465
(2) 「想定される」	469
III 本人の同意の取得方法	471
1 明示の同意	471
2 同意の取得主体	472

(1) 個人関連情報の第三者提供の場合の考え方	473
(2) 個人データの第三者提供の場合の考え方	474
(3) 同意取得についての解釈上のルールの差異と今後の議論の方向性	474
(4) 同意の取得に関する実務的な対応	475
3 同意取得にあたって必要な要素と文言の例	477
4 第三者が外国に所在する場合の情報提供	478
5 同意取得に関する経過措置	478
(1) 第三者提供を受けて個人情報（個人データ）として取得すること	479
(2) 対象となる情報の特定	479
IV 提供元の確認義務・記録義務	481
1 提供元の確認義務	481
(1) 個人データとして取得することを認める旨の本人の同意が得られていること（法 31 条 1 項 1 号）	481
(2) 第三者が外国に所在する場合の情報提供の確認（法 31 条 1 項 2 号）	482
(3) 既に確認を行った第三者に対する確認の方法	483
2 提供元の記録義務	484
V 提供先の第三者における確認義務・記録義務	485
1 提供先の第三者における確認義務	485
2 提供先の第三者における記録義務	485
■第 6 章 保有個人データに関する規律	487
I はじめに	487
II 保有個人データに関する事項の公表等（法 32 条 1 項関係）	488
1 概要	488
2 公表等の対象となる事項	488
(1) 個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名	488
(2) 全ての保有個人データの利用目的（法 21 条 4 項 1 号から 3 号までに該当する場合を除く。）	489

(3) 通知、開示、訂正、利用停止等の求めに応じる手続（手数料を定めたときはそれを含む。）	489
(4) 保有個人データの安全管理のために講じた措置（ただし、本人の知り得る状態に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）	490
ア 概要	490
イ 外的環境の把握	491
(5) 保有個人データの取扱いに関する苦情の申出先	493
Ⅲ 保有個人データの利用目的の通知	494
1 概要	494
2 例外事由	494
Ⅳ 保有個人データの開示	496
1 概要	496
2 開示請求の手続	496
(1) 概要	496
(2) 開示等の請求等において事業者が定めることができる事項	497
(3) 本人又は代理人の確認方法	499
(4) 保有個人データを特定するに足りる事項	500
(5) 手数料	501
3 対象となる情報	502
4 開示の方法	505
(1) 原則的な考え方	505
(2) 本人が請求した方法による開示が困難な場合	506
5 不開示事由	507
(1) 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合	508
(2) 個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合	508
(3) 他の法令に違反することとなる場合	508
V 第三者提供記録の開示	509
1 概要	509
2 第三者提供記録の定義	509
3 第三者提供記録の開示の方法	510

4	第三者提供記録の不開示事由等	510
VI	訂正等の請求	512
1	概要	512
2	訂正等の要件	512
3	請求を受けた個人情報取扱事業者の対応	513
VII	利用停止等の請求	515
1	概要	515
2	利用停止等の要件	515
(1)	法違反の場合の利用停止等の要件	515
ア	法違反の場合の利用停止等	515
イ	法違反の場合の第三者提供の停止	516
(2)	個人の権利又は正当な利益が害されるおそれがある場合の 利用停止等の要件	516
ア	利用する必要がなくなった場合	516
イ	法26条1項本文に規定する事態が生じた場合	517
ウ	当該本人の権利又は正当な利益が害されるおそれがある場 合	518
(ア)	本人又は第三者の生命、身体、財産その他の権利利益 を保護するために当該保有個人データを取り扱う事情	519
(イ)	法令を遵守するために当該保有個人データを取り扱う 事情	519
(ウ)	契約に係る義務を履行するために当該保有個人データ を取り扱う事情	519
(エ)	違法又は不当な行為を防止するために当該保有個人デ ータを取り扱う事情	520
(オ)	法的主張、権利行使又は防御のために当該保有個人デ ータを取り扱う事情	520
3	請求を受けた個人情報取扱事業者の対応	522
(1)	利用停止等の要件の判断	522
(2)	要件を満たす場合の対応の限度	522
(3)	代替措置による対応	523

■ 第7章 仮名加工情報に関する規律	524
I はじめに	524
1 概要	524
(1) 仮名加工情報の制度概要・導入経緯	524
(2) 仮名加工情報制度の意義	525
2 仮名加工情報	527
(1) 仮名加工情報の定義	527
(2) 「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」	528
(3) 「個人に関する情報」	529
II 仮名加工情報を作成する個人情報取扱事業者の義務等	531
1 仮名加工情報の適正な加工	531
(1) はじめに	531
(2) 客観要件：規則 31 条各号の加工基準	531
ア 加工基準	531
イ 1号：特定の個人を識別することができる記述等の削除	532
ウ 2号：個人識別符号の削除	533
エ 3号：不正に利用されることにより財産的被害が生じるおそれがある記述等の削除	534
オ その他：共用性のある記述等の削除等	534
(3) 主観要件	536
コラム 26 主観要件	537
2 削除情報等の安全管理措置	538
III 仮名加工情報の取扱いに関する義務等	540
1 概要	540
2 個人情報である仮名加工情報の取扱いに関する義務等	540
(1) 概要	540
(2) 利用目的に関する規律	541
(3) 適正取得・不適正利用	542
(4) 安全管理措置に関する規律	543
(5) 第三者提供に関する規律	544
ア 第三者提供の禁止等	544

イ 委託に伴って仮名加工情報を提供する場合	544
ウ 共同利用により仮名加工情報を提供する場合	546
(ア) 過去データの共同利用による提供	546
(イ) 共同利用により仮名加工情報を相互に提供して突合する場合	547
コラム 27 共同利用者間の仮名加工情報の突合	550
(6) 保有個人データの開示等に関する規律	550
(7) 識別行為の禁止	550
(8) 本人への連絡等の禁止	552
3 個人情報でない仮名加工情報の取扱いに関する義務等	553

■ 第 8 章 匿名加工情報に関する規律555

I はじめに555

1 概要	555
(1) 匿名加工情報の制度概要・導入経緯	555
(2) 匿名加工情報制度の意義	556

コラム 28 匿名加工情報の活用実態 557

2 匿名加工情報	558
(1) 匿名加工情報の定義	558
(2) 「特定の個人を識別することができない」	558
ア 容易照合性非勘案説・容易照合性遮断擬制説・容易照合性遮断必要説	559
① 容易照合性非勘案説	559
② 容易照合性遮断擬制説	559
③ 容易照合性遮断必要説	560
イ 対応表・パラメータ	561
(3) 「復元することができない」	567
(4) 「個人に関する情報」	568

II 匿名加工情報を作成する個人情報取扱事業者の義務等570

1 匿名加工情報の適正な加工	570
(1) はじめに	570
(2) 客観要件：規則 34 条各号の加工基準	570

ア	加工基準	570
イ	1号：特定の個人を識別することができる記述等の削除	572
ウ	2号：個人識別符号の削除等	572
エ	3号：情報を相互に連結する符号の削除	573
オ	4号：特異な記述等の削除	574
カ	5号：個人情報データベース等の性質を踏まえたその他の措置	574
(3)	主観要件	580
2	加工方法等情報の安全管理措置	581
3	匿名加工情報の作成時の公表	583
Ⅲ	匿名加工情報の取扱いに関する義務等	584
1	概要	584
2	匿名加工情報の第三者提供（法43条4項、44条）	584
3	識別行為の禁止（法43条5項、45条）	586
4	匿名加工情報の安全管理措置（法43条6項、46条）	588
コラム 29	次世代医療基盤法—医療情報の利活用	588
■	第9章 認定個人情報保護団体	592
I	はじめに	592
II	認定個人情報保護団体の業務	594
1	個人情報等の取扱いに関する苦情の処理（法47条1項1号）	594
2	対象事業者に対する情報の提供（法47条1項2号）	595
3	その他対象事業者の個人情報等の適正な取扱いの確保に関し必要な業務（法47条1項3号）	595
III	認定の申請と対象範囲	597
1	認定の申請	597
2	業務範囲の限定	597
IV	認定個人情報保護団体の個人情報保護指針と対象事業者の監督	599
V	認定個人情報保護団体の今後	600

■第10章 本人同意原則の例外・適用除外	601
Ⅰ はじめに	601
Ⅱ 本人同意原則の例外（法18条3項、20条2項、27条1項、28条1項、31条1項関係）	602
1 法令に基づく場合（法18条3項1号、20条2項1号、27条1項1号、28条1項、31条1項関係）	602
コラム30 捜査関係事項照会等への対応	605
コラム31 弁護士会照会と不法行為責任	606
2 生命、身体又は財産の保護のための例外（法18条3項2号、20条2項2号、27条1項2号、28条1項、31条1項関係）	607
3 公衆衛生例外（法18条3項3号、20条2項3号、27条1項3号、28条1項、31条1項関係）	609
4 国の委託事務の例外（法18条3項4号、20条2項4号、27条1項4号、28条1項、31条1項関係）	614
5 学術研究例外（法18条3項5号・6号、20条2項5号・6号、27条1項5号～7号、28条1項、31条1項関係）	615
(1) 「学術研究機関等」（法16条8項関係）	617
(2) 「学術研究目的」	619
(3) 本人同意原則の例外となる取扱い	619
ア 学術研究機関等における学術研究目的での取扱い（法18条3項5号、20条2項5号）	620
イ 学術研究目的の取扱いを必要とする学術研究機関等への提供（法18条3項6号、27条1項7号）	621
ウ 学術研究機関等による成果の公表等（法27条1項5号）	627
エ 共同研究における個人情報の取扱い（法20条2項6号、27条1項6号）	628
(4) 学術研究機関等の責務（法59条）	629
(5) 学術研究機関等による自主規範の作成・公表	629
6 その他要配慮個人情報の取得に関する例外	630
Ⅲ 適用除外（法57条関係）	631
1 放送機関、新聞社、通信社その他の報道機関（報道を業として行う個人を含む。）	632

2	著述を業として行う者	634
3	宗教団体	634
4	政治団体	635
■	第11章 域外適用	637
I	はじめに	637
II	個情法における域外適用の立法経緯	638
1	制定時における適用範囲の考え方	638
2	平成27年改正における域外適用	639
	(1) 本人からの直接取得	639
	(2) 適用条文の限定列举	640
3	令和2年改正における域外適用の再構成	640
	(1) 間接取得の場合も域外適用の対象となったこと	641
	(2) 域外適用の対象条文が個情法全体となったこと	642
	(3) 物品又は役務の提供の対象となる者と本人が同一である必要 がなくなったこと	643
III	域外適用が問題となる場面	645
1	外国事業者の支店等が日本にあるケース	645
2	外国事業者の支店等が日本にないケース	646
3	国内事業者の外国支店等が個人情報を外国で取り扱っている ケース	647
IV	「国内にある者に対する物品又は役務の提供に関連して」	649
V	域外適用の理論と執行	652
1	執行の重要性	652
2	外国事業者への執行手段	652
	(1) 段階的な制裁の仕組み	652
	(2) 刑事罰を科すことができるか	653
	(3) 課徴金制度の活用	653
■	第12章 インシデント対応（漏えい以外）、監督、罰則	655
I	はじめに	655
II	インシデント（漏えい等事案以外）発生時の対応	656

1	事業者内部における報告及び被害の拡大防止（違法状態の解消）	657
2	事実関係の調査及び原因の究明	657
3	影響範囲の特定	658
4	再発防止策の検討及び実施	658
5	個情委対応	658
6	本人への通知及び事案の公表	659
7	第三者を交えた調査委員会等の設置	660
Ⅲ	個人情報保護委員会による監督	662
1	報告徴収及び立入検査	663
2	指導・助言	665
3	勸告	666
4	命令	669
5	課徴金・罰金	671
6	個情委による公表	671
7	個情委による監督権限行使の流れのイメージ	676
Ⅳ	インシデントの予防及び準備	678
Ⅴ	罰則	680
1	個人情報データベース等の不正提供等に関する罪	680
(1)	導入の背景等	680
(2)	個人情報データベース等提供罪の構成要件等	681
ア	刑罰の対象となる主体	681
イ	個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）	682
ウ	その業務に関して取り扱った	683
エ	自己もしくは第三者の不正な利益を図る目的	683
オ	提供し、又は盗用したとき	683
カ	違反の効果（法定刑）	683
2	行政機関等の職員等に関係する罪	683
(1)	個人情報ファイル不正提供罪（法 176 条）	683
(2)	保有個人情報不正使用罪（法 180 条）	684
(3)	職権を濫用して文書等を収集する罪（法 181 条）	684
3	個情委の監督に関する間接罰	684
(1)	個情委による命令違反（法 178 条）	684

(2) 個人情報に対する虚偽報告等（法 182 条）	684
4 その他	685
■第 13 章 プライバシーガバナンス	686
I はじめに	686
II プライバシーガバナンスへの取組の重要性	687
1 企業価値の向上等	687
2 取組の難しさと対応策	688
3 個人情報法の解釈との関係	688
III プライバシーガバナンスへの取組として実施すべき内容	692
1 ガイドブックが掲げる三要件	692
2 プライバシーガバナンスに係る姿勢の明文化	692
(1) 従来のプライバシーポリシーとの明文化すべき内容の違い	692
(2) 明文化の具体例	694
(3) 各事業者の工夫	695
ア 株式会社リクルート	695
イ セーフイー株式会社	696
ウ NHK	696
エ 株式会社トヨタ	697
3 パーソナルデータの取扱いに係る説明の充実	697
4 消費者との継続的なコミュニケーション	700
5 体制の構築と運用	700
(1) プライバシー保護責任者・プライバシー保護組織の設置	700
(2) 外部有識者の活用	703
IV プライバシーリスクへの対応の方法	704
1 プライバシーリスクの評価手続	704
2 プライバシーリスク対策の例	706
■第 14 章 新たなテクノロジーを取り巻く課題	711
I カメラ	711
1 はじめに	711
2 カメラにより取得されるデータ・用途・特徴	711

細目次

(1) カメラにより取得されるデータ	711
(2) カメラにより取得されるデータの用途	712
ア 防犯目的	712
イ 商用目的	712
ウ その他の目的	712
(3) カメラにより取得されるデータの特徴・留意点	713
3 カメラにより取得されるデータの取扱いに関して参考となる各種文書	714
4 肖像権・プライバシーに関する留意点	716
5 個人情報上のカメラ画像や顔特徴データ等の取扱いに係る規律	716
(1) 個人情報該当性	716
(2) 要配慮個人情報の取得等	717
(3) 個人情報データベース等	717
(4) 保有個人データ	718
(5) 不適正利用の禁止	718
(6) 適正取得義務	719
(7) 利用目的の特定、通知・公表等	719
コラム 32 運用基準の在り方と透明性の確保	721
(8) 正確性の確保等	722
(9) 安全管理措置	722
(10) 第三者提供	724
ア 法令に基づく場合	724
イ 人の生命・身体又は財産の保護のために必要である場合や公衆衛生向上等のため	724
ウ 委託に伴う提供	724
エ 共同利用に基づく提供	725
6 その他事業者による自主的な取組	726
コラム 33 カメラによる撮影行為の在り方が議論された事例	727
II AI	730
1 はじめに	730
コラム 34 EUでの生成 AI サービス事業者に対する GDPR の執行事例	730
2 個人情報に基づく AI をめぐる主な論点	733

(1) 個人情報の利用目的規制	733
(2) 個人情報の取得規制	735
ア 公開されている要配慮個人情報の取得	735
イ プロファイリングなどを通じた要配慮個人情報の生成	737
(3) 個人情報の不適正利用の禁止	738
(4) 個人データの第三者提供規制	739
(5) 本人の請求権	739
3 具体的な事例における個情法の適用に関する検討	740
(1) AI 開発事業者が自ら学習用データを収集して大規模言語モデル (LLM) を構築するケース	740
(2) 事業者が外部の AI サービス事業者からサービス提供を受け、入出力の際に個人情報のやり取りが発生するケース	743
ア 事業者 C (利用事業者) の立場からの検討	743
イ 事業者 D (サービスプロバイダ) の立場からの検討	746
ウ API などを活用したサービスにおける検討	746
III メタバース	747
1 はじめに	747
2 メタバース (Metaverse) とは何か	748
3 メタバースにおける関連当事者	749
4 メタバースと個人情報保護法	750
(1) メタバースにおいて取得されるデータの特徴	750
(2) メタバースにおけるデータの個人情報該当性	752
(3) メタバースにおける個人情報の取得・利用に関する留意点	753
コラム 35 アバターのプライバシー	755
(4) メタバースと第三者提供規制及び越境移転規制	756
(5) 日本法の域外適用と海外のデータ保護法の域外適用 (適用されるデータ保護法)	756
IV ブロックチェーン	758
1 はじめに	758
2 ブロックチェーンとは	758
(1) ブロックチェーンの仕組み	758
ア ハッシュ	759
イ コンセンサスアルゴリズム	760

ウ	P2P ネットワーク	760
エ	公開鍵暗号とデジタル署名	761
(2)	ブロックチェーンの管理主体や参加者の範囲による分類	761
(3)	ブロックチェーンに記録される情報の性質	762
ア	ブロックチェーンに記録される情報	762
イ	ブロックチェーンで取り扱うデータの特徴	763
3	ブロックチェーンと個人情報保護法	764
(1)	個人情報取扱事業者に該当する者	766
(2)	域外適用	767
(3)	個人情報該当性	767
	コラム 36 ブロックチェーンとプライバシー保護	768
(4)	利用目的の特定	769
(5)	データ内容の正確性の確保等	770
(6)	第三者提供規制	770
ア	本人同意原則	770
イ	委託に伴う提供	771
ウ	共同利用	771
(7)	越境移転規制・外的環境の把握	772
(8)	保有個人データの訂正又は消去請求	773
(9)	オフチェーンの併用による解決	774

第3編 行政機関等の義務等

■	第1章 総説	776
I	令和3年改正による個人情報保護法制の一元化	776
II	法第5章の規律対象となる主体	778
1	行政機関等・行政機関の長等	778
(1)	行政機関等	778
(2)	行政機関の長等	780
2	法第4章の適用を受ける法人及び業務	780
(1)	医療分野・学術分野の独立行政法人等及び地方独立行政法人	782
(2)	地方公共団体が運営する病院・診療所及び大学、(独)労働	

者健康安全機構の病院部門	783
Ⅲ 第5章の規律対象となる情報	786
1 総説	786
2 個人情報	786
3 保有個人情報	787
4 個人情報ファイル	788
5 要配慮個人情報・条例要配慮個人情報	788
6 個人関連情報、仮名加工情報、匿名加工情報、行政機関等匿名加工情報	788
■第2章 個人情報等の取扱いに関する規律	789
I 総説	789
II 保有に関する制限（法61条1項・2項）	790
III 取得及び利用の際の遵守事項	791
1 利用目的の変更（法61条3項）	791
2 本人から書面により取得する際の利用目的の明示（法62条）	791
3 不適正利用・不適正取得の禁止（法63条、64条）	792
4 正確性の確保（法65条）	792
IV 安全管理措置等	793
1 安全管理措置	793
(1) 行政機関の長等の安全管理措置義務（法66条1項）	793
(2) 行政機関の長等の安全管理措置義務の準用（法66条2項）	793
2 従事者の義務	794
V 漏えい等の報告等	795
1 個人情報への報告	795
2 本人への通知	796
VI 利用及び提供の制限	797
1 利用目的以外の目的のための利用及び提供の禁止の原則	797
2 保有個人情報の提供を受ける者に対する措置要求	798
3 利用目的以外の目的のための外国にある第三者への提供	798
VII 個人関連情報、仮名加工情報の取扱い	800
1 個人関連情報の取扱い	800
2 仮名加工情報の取扱い	800

■ 第3章 個人情報ファイルに関する規律	802
I 総説	802
II 個人情報ファイルの保有等に関する事前通知	803
III 個人情報ファイル簿の作成及び公表	805
■ 第4章 開示、訂正及び利用停止に関する規律	807
I 総説	807
II 開示	808
1 開示請求権	808
2 開示請求の手続	808
3 保有個人情報の開示義務等	809
(1) 開示義務	809
(2) 部分開示	811
(3) 裁量的開示	811
(4) 存否応答拒否	811
4 開示請求に対する措置等	811
(1) 開示請求に対する措置等	811
(2) 事案の移送	812
(3) 第三者に対する意見提出の機会の付与	812
(4) 開示の実施等	813
III 訂正	814
1 訂正請求権	814
2 訂正請求の手続等	814
3 保有個人情報の訂正義務	814
4 訂正請求に対する措置等	815
(1) 訂正請求に対する措置等	815
(2) 事案の移送	815
(3) 保有個人情報の提供先への通知	815
IV 利用停止	816
1 利用停止請求権	816
2 利用停止請求の手続等	817
3 保有個人情報の利用停止義務	817

4	利用停止請求に対する措置等	817
V	開示決定等に対する審査請求	818
■	第5章 匿名加工情報に関する規律	819
I	総説	819
II	行政機関等匿名加工情報の取扱い	820
1	概要	820
2	行政機関等匿名加工情報・行政機関等匿名加工情報ファイル	821
3	行政機関等匿名加工情報の作成及び提供等	822
4	提案募集手続	823
5	作成済みの行政機関等匿名加工情報についての提案募集手続	824
6	識別行為の禁止・安全管理措置等	825
III	行政機関等匿名加工情報以外の匿名加工情報の取扱い	826
■	第6章 行政機関等の監視	827
■	第7章 公的部門規律と民間部門規律の交錯	829

研究者と実務家の対話—宍戸常寿教授との議論をふまえて

第1編	総論	832
第2編	個人情報取扱事業者等の義務	835
第2章	定義	835
II	個人情報	835
VI	個人情報データベース等	837
XIII	本人の同意	838
第3章	個人情報に関する規律	842
I	個人情報の利用目的	842
II	不適正利用の禁止	842
第4章	個人データに関する規律	844
I	個人データの管理	844
II	個人データの漏えい等報告・本人通知	844
III	個人データの第三者提供、IV 個人データの第三者提供の	

細目次

例外としての「委託」、VI 個人データの第三者提供の例外と としての「共同利用」	847
VII 外国にある第三者への提供の制限、VIII 外国から日本に越境 移転された個人データの取扱い	852
IX 第三者提供に係る確認・記録義務	857
第5章 個人関連情報に関する規律	858
第6章 保有個人データに関する規律	865
第7章 仮名加工情報に関する規律、第8章 匿名加工情報に 関する規律	867
第9章 認定個人情報保護団体	869
第10章 本人同意原則の例外・適用除外	870
第11章 域外適用	872
第12章 インシデント対応（漏えい以外）、監督、罰則	875
第13章 プライバシーガバナンス	878
第14章 新たなテクノロジーを取り巻く課題	882
I カメラ	882
II AI	882
III メタバース	885
IV ブロックチェーン	886
第3編 行政機関等の義務等	887
事項索引	889