個人情報の保護に関する法律準拠の為の行動規範

cloud security alliance®

CLOUD PRIVACY WORKING GROUP, NOVEMBER 2021

日本版提供に際しての告知及び注意事項

本書「個人情報の保護に関する法律準拠の為の行動規範（CoC　JP）」は一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）が公開するものです。

以下の変更履歴（日付、バージョン、変更内容）をご確認ください

変更履歴

日付	バージョン	変更内容
2021 年 11 月 17 日	1.0	初版発行

用語については特に定めのない限り個人情報保護法及び関連法令やガイドラインにおける各用語の定義と同一と致します。

CSAジャパンは、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．責任の限定

CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性

(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと

(3) 本書の内容に基づいて行われた判断や行為がもたらす結果

(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。

(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。

(3) CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。

(4) 転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３．本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければな

りません。

(3) 本書をダウンロードした者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4) 本書を印刷した者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

５．その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、本書または本書の提供場所に記載の問合せ先までお願いします。

日本版作成に際しての謝辞

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」の作成は、CSAジャパンの「クラウドプライバシー・ワーキンググループ」に参加するメンバーを中心とした、CSAジャパン会員の有志により行われました。

作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。

以下に、作業に参加された方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。（氏名あいうえお順・敬称略）

笠松 隆幸

勝見 勉

サルギシャン アレクサンドル：ファイルフォース株式会社

新貝 知晃： 株式会社日立システムズ

高瀬 一彰

竹内 智子：株式会社クリエイティブジャパン

谷本 茂明

津嶋 紀宏：株式会社日立システムズ

成川 達也

前川 浩司：BSIグループジャパン株式会社

諸角 昌宏

山本 博崇

山崎 万丈

目次

I. 序論

個人情報保護は、全世界的にはリスクベースの評価になってきている。個人情報の管理者は、彼らが処理する個人データの適切な保護レベルを組織内で決定し実施する責任を負う。その決定においては、最先端技術、実装費用、データ処理の性質、範囲、内容および目的を勘案し、また個人の権利及び自由に対する主張の可能性および深刻さが変動するリスクを考慮する必要がある。その結果、クラウド事業者（CSP）は、彼らが処理する個人データに求められる保護レベルを自ら決定する責任を負う。

日本においては、「個人情報の保護に関する法律」(以降、個人情報保護法) が２０１８年より改正版での運用が開始されている。個人情報保護法に関しては２０２２年４月に改正法が施行されるが本書では参考程度に留める。

更に各種ガイドライン(保護法とガイドラインを総称して個人情報保護法等と表記する)が個人情報保護委員会より出されており、CSAジャパンは、これらの法令の準拠のための「個人情報の保護に関する法律準拠の為の行動規範」を作成した。

２０１８年に発行された「CSA GDPR準拠の為の行動規範(CSA CoC(PLA[V3]))と同様に、CSPとクラウド利用者に個人情報保護法準拠のためのソリューションを提供し、CSPが提供するデータ保護レベルに関する透明性ガイドラインを提供することを目指している。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」は、実質的に以下を提供するものである:

あらゆる規模および所在場所のCSPにとっての、個人情報保護法に遵守し、利用者に提供している個人データ保護レベルを、体系化された方法で明示するための例示と解説。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」は、主に法的要件に重点を置いているため、Cloud Control Matrix（CCM）やSTAR認証（またはSTAR評価証明またはSTARセルフアセスメント）などの他のCSA作成の実践規範および認証と組み合わせてこの規範を採用することを提案し、情報セキュリティの必要な要件をCCM/ISMSなどとの対比を本文中に記載している。

このような状況において、Cloud Control Matrixまたはそれと同等のもの（例えば、ISO 27017またはISO 27018による補完を伴うISO 27001）といった情報セキュリティの技術標準の採用や、それらに関連する認証スキーム（例えば、STAR認証、STAR評価証明、STARセルフアセスメント、ISO 27001、またはSOC2）は、CSPがセキュリティプログラムまたは情報セキュリティ管理システム（ISMS）を実装し、これらのリスクアセスメントで概説された脅威から利用者のデータを適切に保護している証拠を提供する。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」は、個人情報保護法等のクラウド分野に関連する要件を反映し、CSA Security, Transparency and Assurance Registry（STAR）の一部を構成する。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」の対象読者には、CSP、クラウド利用者と潜在利用者、クラウド監査者、およびクラウドブローカーのように、クラウドコンピューティングおよび個人データ保護法制に関心のあるすべての利害関係者が含まれる。

最後に、「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」に対するいかなる認証も、管理者（Controller）または処理者（Processor）が個人情報保護法等を遵守する責任を軽減するものではなく、国の個人情報保護委員会の任務および権限を損なうものではないことに注意することが重要である。

II. 背景

欧州では2016年5月にREGULATION (EU) 2016/679 ("GDPR") が発効し、2018年5月25日以降すべてのEU参加国において直接適用されることになった。米国でもカリフォルニア州消費者プライバシー法（CCPA：the California Consumer Privacy Act）やカリフォルニアプライバシー権法（CPRA: the California Privacy Rights Act of 2020）に加え、連邦データプライバシー法案としてCOPRA（Consumer Online Privacy Rights Act）（消費者オンラインプライバシー法）という法案が審議されている。

このように消費者のプライバシーにかかわる法制化は世界的なトレンドであり、プライバシーという権利を法的に認める流れにある。

日本では個人情報全般に関する扱いを個人情報保護法等によって定めてきていたが、欧米に比べあいまいな部分も多く、企業活動の国際化やクラウドコンピューティングの進展に伴う国境をまたいだデータの移動・処理・保管が常態化した中で各国法制度との差を埋める(GDPRに求められる十分性認定)活動などが必要になってきている。

日本では個人情報と個人データ・保有個人データによって事業者の義務が異なっている点が留意すべき点である。

表 1　定義の整理

個人情報
生存する特定の個人を識別できる情報 個人識別符号が含まれるもの
個人データ
個人情報を検索できるように体系的に構成したもの
保有個人データ
個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データ

表 2　義務の観点での整理

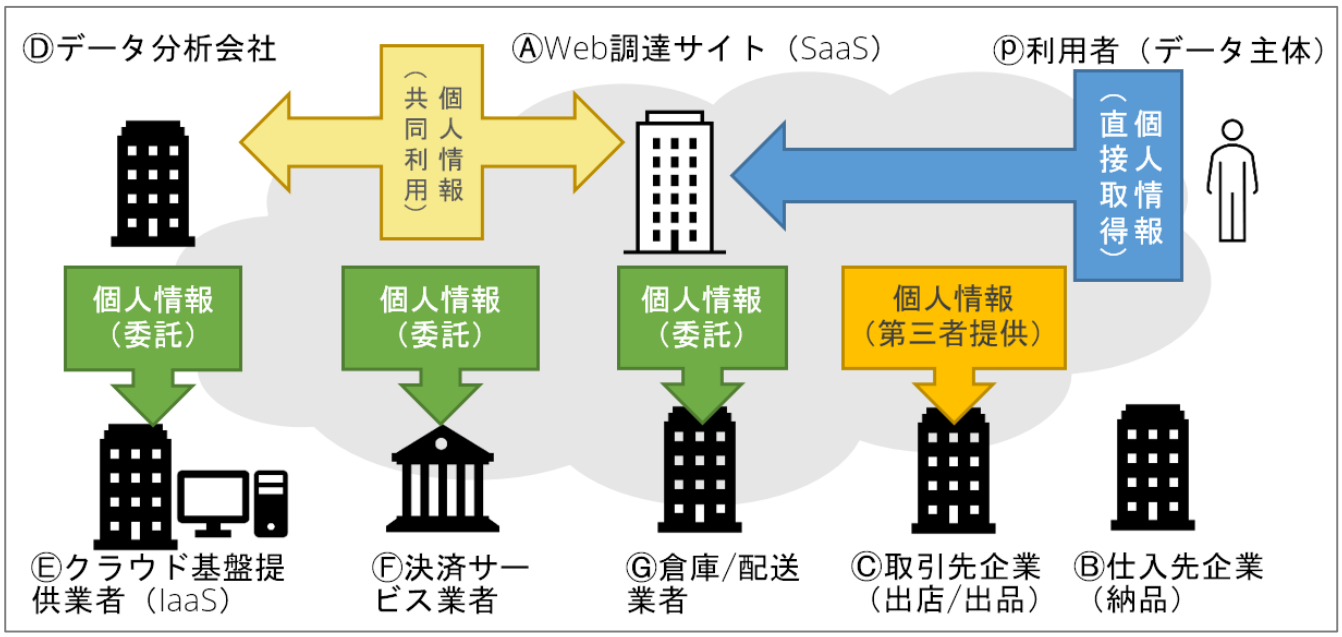
保有個人データ		
個人データ		
個人情報 第 15 条 利用目的の特定 第 16 条 利用目的による制限 第 17 条 適正な取得 第 18 条 取得に際しての利用目的の通知等 第 35 条 個人情報取扱事業者による苦情の処理	第 19 条 データ内容の正確性の確保等 第 20 条 安全管理措置 第 21 条 従業者の監督 第 22 条 委託先の監督 第 23 条 第三者提供の制限 第 24 条 外国にある第三者への提供の制限 第 25 条 第三者提供に係る記録の作成等 第 26 条 第三者提供を受ける際の確認等	第 27 条 保有個人データに関する事項の公表等 第 28 条 開示 第 29 条 訂正等 第 30 条 利用停止等 第 31 条 理由の説明 第 32 条 開示等の請求等に応じる手続 第 33 条 手数料

日本では個人情報保護法の制定により、個人情報は利用目的の特定・管理下にある情報の安全管理・削除訂正などの要請対応に関する事項が定められているが、経済活動活性化のためにより踏み込んだ議論が必要であるとCSAジャパンクラウドプライバシーワーキンググループは認識し本書を取りまとめた。

III. 理解促進のための参照モデル

本文書では理解を促進するために以下のようなモデルを定義した。必要に応じこのモデルを利用しての解説を行う。尚、その解説はあくまで理解の助けのためであり、必要事項の全てを記述するものではない点について了承されたい。以降、本文書では単に「参照モデル」と記載する。

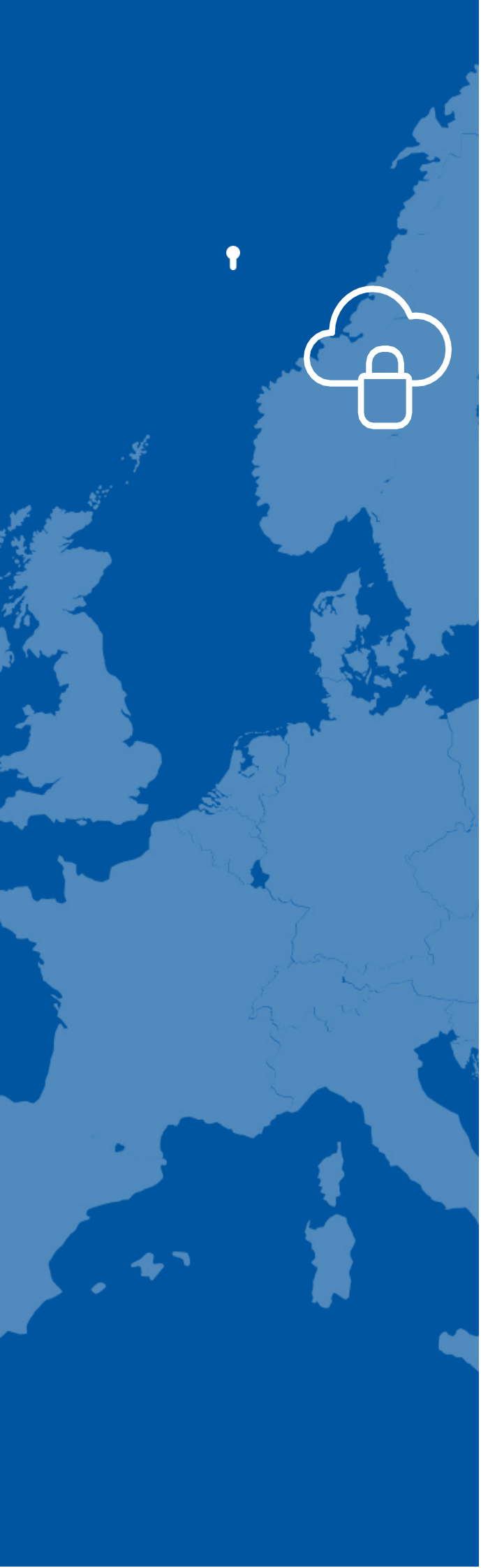
図１　Web調達サイト（法人向けECサイト）のモデル



- Ⓐ Web調達サイト運営会社は、ⓟ利用者（データ主体）の個人情報を直接取得する。口コミ情報等も収集する場合がある。利用者はWeb調達サイトの会員登録時に、利用目的の記載された会員規約に予め同意しているものとする。この中には、委託・共同利用および第三者提供の記述も含まれている。
- Ⓑ仕入先企業は、Ⓐ Web調達サイトに商品を納品する。ⓟの個人情報はⒷには提供されない。
- Ⓒ取引先企業（出店／出品者）は、Ⓐ Web調達サイトに出店/出品して、ⓟ利用者に商品を販売する。ⓟの個人情報はⒶより第三者提供される。
- Ⓓデータ分析会社は、Ⓐが収集する個人情報や購買情報などのデータを解析し、Ⓐと共同でマーケティングに活用する。
- Ⓔクラウド基盤提供業者（IaaS）は、ⒶのSaaSインフラとしてクラウド基盤を提供する。（個人情報取扱事業者としては扱われない場合がある）
- Ⓕ決済サービス業者は、Ⓐからの委託で決済処理を行う。
- Ⓖ倉庫/配送業者は、Ⓐからの委託で、品物をⒸまたはⒼ倉庫からⓟに届ける。

表３　Web調達サイト（法人向けECサイト）のモデル

	個人情報取扱事業者	Ⓐからみた位置づけ	保有個人データを扱う	CoC-JPでの表記
Ⓟ利用者（データ主体）	非該当	利用者	ー	利用者
ⒶWeb調達サイト運営会社（SaaS）	該当/直接取得	ー	○	CSP
Ⓑ仕入先企業	非該当	仕入先	ー	サプライヤー
Ⓒ取引先企業	該当/第三者提供	出店/出品者	○	クライアント
Ⓓデータ分析会社	該当/共同利用	共同利用先	○	CSP（共同利用者）
Ⓔクラウド基盤提供業者（IaaS）	該当/委託 または非該当	委託先	×	CSP（委託先）
Ⓕ決済サービス業者	該当/委託	委託先	×	CSP（委託先）
Ⓖ倉庫/配送業者	該当/委託	委託先	×	委託先



実践規範

第１章　個人情報の取得や個人データの留保に関する事業者の対応（第15条、第16条、第17条、第18条、第19条）

第１節 個人情報の取得

個人情報取扱事業者が、個人情報を取得する場合には、あらかじめその利用目的を特定したうえで、その目的達成に必要最小限の情報を取得する。取得に当たっては、その利用目的を本人に通知又は公表が必要となる。

表４　個人情報の取得に関する法の記述（抜粋）

項目　［該当条文］	事業者の対応	ガイドライン[1]（補足）
利用目的の特定［第 15 条］	•個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。 •個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。	個人情報が個人情報取扱事業者において、最終的にどのような事業の用に供され、どのような目的で個人情報を利用されるのかが、本人にとって一般的かつ合理的に想定できる程度に具体的に特定することが望ましい
利用目的による制限［第 16 条］	•個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。 •個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。	変更後の利用目的が変更前の利用目的からみて、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲内で変更することは可能である。変更された利用目的は、本人に通知するか、又は公表しなければならない。
適正な取得　［第 17 条］	•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ない。 •個人情報取扱事業者は、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。	個人情報取扱事業者が要配慮個人情報を書面又は口頭等により本人から適正に直接取得する場合は、本人が当該情報を提供したことをもって、当該個人情報取扱事業者が当該情報を取得することについて本人の同意があったものと解される。
取得に際しての利用目的の通知等［第 18 条］	•個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。 •本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。	ー

2022年4月施行予定の改正法では「16条-2（不適正な利用の禁止）個人情報取扱事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。」との記載がある。このため、たとえ利用目的の範囲であっても、利用者に不利益になると疑われる使いかたは避けなければならない。また、利用者に丁寧に説明することが大切である。

日本では新型コロナウイルスの感染者と濃厚接触した可能性がある場合、スマートフォンに通知が届く「接触確認アプリ」の運用を2020/6/19に始めた。このアプリをインストールしたスマートフォン

[1] 個人情報保護委員会（平成 28 年 11 月）（平成 31 年 1 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」

同士が近接した場合、互いに接触符号をBluetooth通信で提供し記録する仕組みになっている。各国により仕様は異なり、シンガポールなどは当局が個人情報を取得しており、接触者を特定し連絡が可能となっているが、日本は接触者データは個人のスマホで管理するため、政府や保健所等が個人情報を取得することはない。万一感染が確認された場合には、本人が同意した利用規約に基づきアプリで陽性者であることを登録し、匿名化された接触識別子（日次鍵）が中央サーバに送られ、その情報がブロードキャストされる。受信した端末側で濃厚接触したかどうかが判定されるのみで、中央では把握ができない。以上の仕組みのため、このアプリ利用にあたって、プライバシーポリシーにも、陽性者の処理番号と日次鍵および本アプリの改善のために必要な本アプリの動作情報等以外の個人情報は取得しない旨が記されている。[2]

第２節 個人データの留保

個人情報を取得した場合、その個人データを留保するにあたって、法では、データ内容の正確性の確保と、利用する必要がなくなったときは遅滞なく消去の2つの努力義務について規定している。[第19条]

表５　データ内容の正確性の確保等に関する法の記述（抜粋）

項目　［該当条文］	事業者の対応	ガイドライン（補足）
データ内容の正確性の確保等［第19条］	個人情報取扱事業者は、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よう努めなければならない。	保有する個人データを一律に又は常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すれば足りる。
	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。	法令の定めにより保存期間等が定められている場合は、この限りではない。 「個人データの消去」とは、当該個人データを個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含む。

法令順守のため、個人情報取扱事業者は何をしなければならないか。

CCMでは、データの正確性確保のため、そのデータが個人データであることを分類・管理化し、ラベル付けを行ってセキュリティーポリシーを確立、管理責任者を設定するなどのデータセキュリティと情報ライフサイクル管理、そのデータの保持ポリシーを設定し廃棄の際には確実に廃棄することを盛り込むよう記述されている[表6]。

表６　データ内容の正確性の確保のためCCM管理策

CCM V3.0 Control ID	項目	管理策
DSI-01	分類	データタイプ、価値、機微性、組織にとっての重要性に基づいて、データの所有者によって分類されなければならない。

[2] 厚生労働省「接触確認アプリケーションプライバシーポリシー」
https://www.mhlw.go.jp/stf/seisakunitsuite/japanese_pp_00027.html（2021/8/17 時点アクセス）

DSI-02	データの管理表とフロー	クラウドサービスの地理的に分散した（実/仮想）アプリケーション、インフラストラクチャーネットワーク、及びシステムの構成要素内に（常時または一時的に）存在する、もしくは第三者と共有するデータのデータフローを作成し、文書化し、維持しなければならない。
DSI-04	処理 / ラベル付 / セキュリティポリシー	データ及びデータを含むオブジェクトのラベリング、処理取扱い、セキュリティのためのポリシー及び手順を確立しなければならない。
DSI-06	所有者/管理責任	すべての情報に対して管理責任者が指名され、その責任は定義され、文書化され、周知されなければならない。
DSI-07	安全な廃棄	記憶媒体の全てからデータを安全に廃棄し完全に除去すること
GRM-02	データフォーカスリスクアセスメント	定められた保存期間と、使用終了時の廃棄に関する要件の遵守
BCR-11	保持ポリシー	重要な資産の保持期間を、当該ポリシー及び手順に従って定義し、ならびに該当する法的または規制上の遵守義務に準拠するようになければならない。

（1）正確性の確保

「個人情報保護マネジメントシステム－要求事項」（JIS Q 15001：2017）では、正確性の確保とは、例えば、誤入力チェック、誤りなどを発見した場合の訂正、内容の更新、保存期間の設定、データのバックアップなどの手順を確立することであると記述されている。[3] 誤りなどを発見した場合の訂正、内容の更新は、利用者からの申請に基づき実施したり、利用者自身に実施してもらうためのマイページを用意したりするサイトも多い。これらは個人情報に関する本人の権利として知られ、第５章**で解説する。**

（2）保存期間

経理、税務関係の書類のうち、取引に関する帳簿類（取引に関して受領または交付する注文書、契約書、送り状、領収書、見積書など）は、法人税法や電子帳簿保存法により、保存期間が7年と定められている。これら文書に記載される個人情報の保存期間も同様と考えればよいだろう。金融商品取引法や犯罪収益移転防止法においても「取引記録」の作成・保存が義務づけられており、保存期間は取引の日からそれぞれ10年間、７年間となっており、長いほうに合わせる必要がある。

なお、**「個人情報保護マネジメントシステム－要求事項」**（JIS Q 15001：2017）では、個人情報の管理台帳に保管期限と利用期限を記載するよう規定されている。2022年4月施行予定の改正法第30条-5（「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には、当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる。」（第５章参照））において利用停止・消去等の個人の請求権の要件が緩和される見込みであり、利用期限と保管期限を区別して管理する必要が出てくる可能性もある。

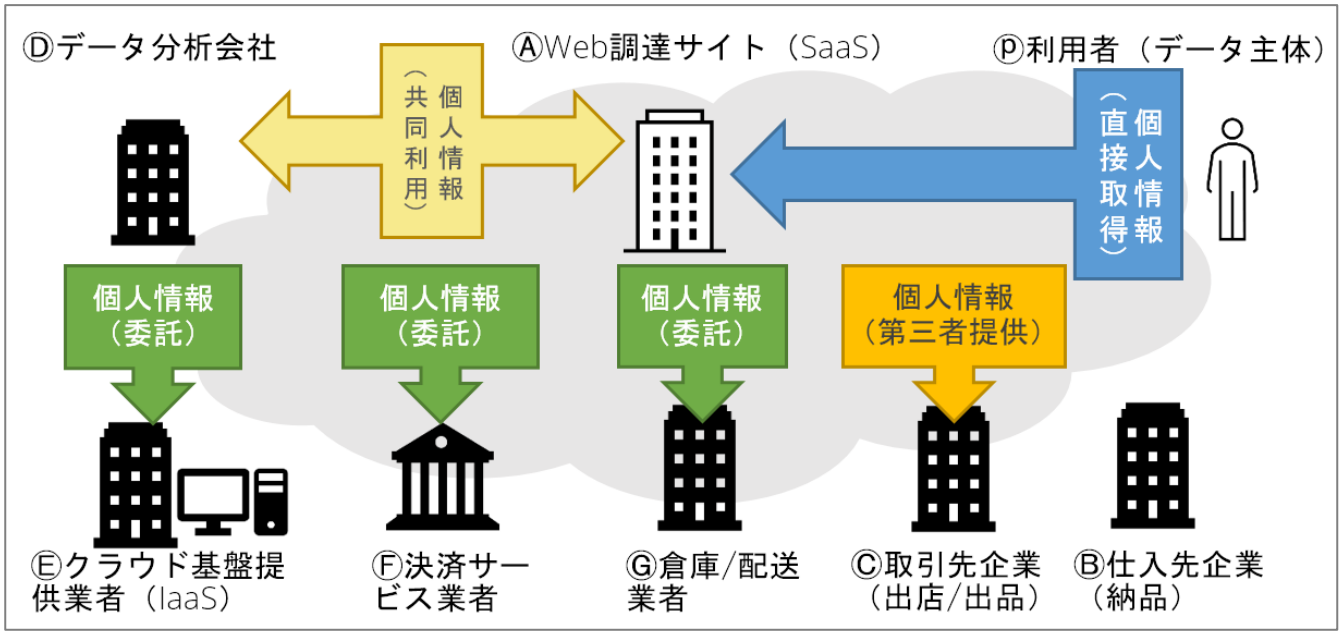
（3）データの消去

ガイドラインには、「「個人データの消去」とは、当該個人データを個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含む。」としており、DSI-07安全な廃棄にあるように、完全に除去することまでは求めていない。データの消去の請求があっても、利用停止するだけで用件は満たせるが、利用中データと利用停止データを、ラベル付けなどにより明確に分けて管理しておくべきである。

[3] **「個人情報保護マネジメントシステム－要求事項」**（JIS Q 15001：2017）［B.3.4.3.1 正確性の確保］

第３節 参照モデルでの対応例

（再掲）図１　Web調達サイト（法人向けECサイト）のモデル



Web調達サイト（Ⓐ）は、マーケットプレイスに陳列している商品の販売に当たり、利用者（Ⓟ）から個人情報を取得する。その場合、利用目的は、通常商品の配送や代金決済のためであるが、売れ筋商品の把握のため統計データを作成するだけであれば、利用目的として示しておく必要はない。[4] 配送や代金決済のために、利用者（Ⓟ）の氏名、住所、電話番号や、クレジットカード番号などを取得するとしても、年齢や性別などは必須でない場合は、漏洩等のリスクを避けるため取得しないほうが良い。ただし、売れ筋商品の把握のためにそれらの属性情報が必要なら、任意取得項目として利用者（Ⓟ）に利用目的の通知または公表を行い、同意を取る必要があろう。

配送や代金決済を代行業者（ⒼⒻ）に委託する場合は、委託契約を締結し、個人情報を委託先（ⒼⒻ）へ提供する。委託契約が無い場合は第三者提供となる（第４章参照）。クレジットカード番号は、委託先の代金決済会社（Ⓕ）のサイトで直接入力してもらうようにすれば、Web調達サイト（Ⓐ）では、それらの情報は保持する必要がなくなり、リスク低減となる。最近はそのような形態が増えている。[5]

第２章 安全管理措置（第20条）

本セクションの目的は、必要かつ適切な安全管理措置を手引きの形にリストアップすることではなく、一部の安全管理措置の重要性を改めて強調するものである。安全管理措置の全体に対しては、以下を考慮し個人情報の保護に関する法律のガイドラインに遵守することを強く推奨されている。

- 平成28 年11 月)（令和2年10月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」の「8（別添）講ずべき安全管理措置の内容」
- 日本規格協会の発行「個人情報保護マネジメントシステムー要求事項」(JIS Q 15001：2017)（平成29 年12月20日 改正）の「附属書C（参考）安全管理措置に関する管理目的及び管理策」
- (JISQ27001)「情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー要求事項」

[4] 「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ【Q2-5】

[5]割賦販売法の一部を改正する法律（「改正割賦販売法」）第 35 条の 16（クレジットカード番号等の適切な管理）加盟店におけるカード情報の「非保持化」、または カード情報を保持する事業者の PCIDSS 準拠の義務化

・　(JISQ27002)「情報技術−セキュリティ技術 − 情報セキュリティ管理策の実践のための規範」

さらに、2018年5月25日より（EUを含む欧州経済領域（EEA）域内で）適用された「EU一般データ保護規則」（英: General Data Protection Regulation; GDPR）[6]を踏まえて、国境の存在感を薄めつつあるクラウドサービスによる個人データ処理（移転など）に対する必要かつ適切な安全管理措置の選定には、クラウド環境および個人情報保護の国際トレンドを考慮する安全対策を図るのは有益である。ついては、個人情報取扱事業者が、Cloud Security Allianceが公開しているCCM(クラウド・コントロール・マトリクス)の管理策の要求事項および「GDPR 準拠の為の行動規範」の付属のPLA テンプレートの管理策の要求事項を満たし、遵守することを強く奨励する。

個人情報の保護に関する法律文

（安全管理措置）

第二十条　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、滅失又はき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。

個人情報取扱事業者は個人情報の保護に関する法律に基づきその取扱う個人データの漏えい、滅失又はき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ずる義務を負う。

表 7　安全管理措置に関連する各文書の該当箇所

個人情報の保護に関する法律	個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」	*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
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、滅失又はき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。	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が、当該措置は、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(取り扱う個人データの性質及び量を含む。)、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。具体的に講じなければならない措置や当該項目を実践するための手法の例等については、「8(別添)講ずべき安全管理措置の内容」を参照のこと。	*A. 3. 4. 3. 2；B. 3. 4. 3. 2*	*GRM-04*

その講ずべき必要かつ適切な措置の具体的な内容については、個人情報保護委員会が「通則編」を始めいくつかの個人情報保護法ガイドラインを公開している。「個人情報の保護に関する法律についてのガイドライン（通則編）」では講ずべき安全管理措置およびその措置が応じなければならないリスクについて次のように述べている。

> 「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が、当該措置は、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（取り扱う個人データ の性質及び量を含む。）、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

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN （英語）（2020 年 01 月 31 日時点アクセス）

> 要かつ適切な内容としなければならない。」。[7]

さらに、 同ガイドラインの「8（別添）講ずべき安全管理措置の内容」では個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等を示している。[8]

日本規格協会の発行「個人情報保護マネジメントシステムー要求事項」(JIS Q 15001：2017)（平成29年12月20日 改正）の「附属書A（規定）管理目的および管理策」のA.3.4.3.2では 「安全管理措置: 組織は，その取り扱う個人情報の個人情報保護リスクに応じて，漏えい，滅 失又はき損の防止その他の個人情報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。」[9]と記述されている。またその内容を補足する「附属書B（参考）管理策に関する補足」のB.3.4.3.2では 以下のように記述されている。

> 安全管理措置は、緊急事態が発生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，事業の性質及び個人情報の取扱状況などに起因する個人情報保護リスクに応じた必要かつ適切な措置を講じることが求められているのであって，全ての個人情報についての一律な措置を講じる必要がない。
>
> 安全管理措置とは，組織的安全管理措置，人的安全管理措置，物理的安全管理措置，及び技術的安全管理措置をいう。
>
> “組織的安全管理措置”とは，安全管理について従業者(法第21条参照)の責任及び権限を明確に定め， 安全管理に対する規程及び手順書を整備運用し，その実施状況を確認することをいう。
>
> “人的安全管理措置”とは，従業者(個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい，雇用関係にある従業員(正社員，契約社員，嘱託社員， パート社員，アルバイト社員など)だけでなく，取締役，執行役，理事，監査役，監事，派遣社員なども 含まれる。)に対する，業務上秘密と指定された個人データの非開示契約の締結，教育・訓練などを行うことをいう。
>
> “物理的安全管理措置”とは，入退館(室)の管理，個人データの盗難の防止などの措置をいう。
>
> “技術的安全管理措置”とは，個人データ及びそれを取り扱う情報システムへのアクセス制御，不正ソフトウェア対策，情報システムの監視など，個人データに対する技術的な安全管理措置をいう。
>
> “必要かつ適切”とは，経済的に実行可能な最良の技術の適用に配慮することをいう。
>
> “経済的に実行可能な最良の技術”は，組織の事業内容及び規模によって異なっても差し支えない。
>
> 個人情報の漏えい事例には，廃棄時の漏えいが多くみられることから，廃棄に当たっても，電子ファイルの消去，個人情報が打ち出された紙の破砕処理などによって，廃棄された個人情報が他者に流出することのないよう留意することが望ましい。
>
> なお，安全管理措置については，個人情報保護リスク軽減の観点から，個人情報を対象としている。[10]

これに続き「附属書C（参考）安全管理措置に関する管理目的及び管理策」では「表C.1に規定した

---

[7] 個人情報保護委員会 （平成28年11月）（令和2年10月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」(p. 41)

[8] 個人情報保護委員会 （平成28年11月）（令和2年10月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」(8（別途）講ずべき安全管理措置の内容)

[9] 日本本規格協会の発行「個人情報保護マネジメントシステムー要求事項」（JIS Q 15001：2017）（平成29 年12 月20 日 改正)”(p. 24)

[10] 日本本規格協会の発行「個人情報保護マネジメントシステムー要求事項」（JIS Q 15001：2017）（平成29 年12 月20 日 改正)”(p. 38-39)

管理目的及び管理策は，この規格の A.3.4.3.2 の安全管理措置に関する管理目的及び管理策の包括的なリストであり，JIS Q 27002:2014 の箇条 5～箇条 18 を基に作成したものである。この管理策は、リスク分析[6.1.2 d)]の結果を踏まえて安全管理措置としての個人情報に係る情報セキュリティを決定する際に適宜選択して利用することができる。」[11]と述べ、安全管理措置に関する管理目的及び管理策の一覧を示している。[12]

個人情報取扱事業者は通信中および保存中のすべての個人データに該当する情報の保護及びその情報のすべての取扱い過程、いわゆるデータライフサイクルの各段階においての個人データ漏えい、滅失又はき損、紛失、改変、改ざん、不正使用、不正改造、不正開示、不正アクセス、その他違法なまたは不適切な手段による個人データ取扱いの防止その他の個人データの安全管理及び取扱っている個人データ並びに取扱っている個人データを処理するシステムの機密性[13]、完全性[14]、可用性[15]のような特性[16]を維持する[17]ための技術的安全管理措置、物理的安全管理措置、組織的安全管理措置及び人的安全管理措置などの必要かつ適切な安全管理措置の実施および運用をしなければならない。[18]

パスワードおよび通信の強固な暗号化、二要素認証、システムバックアップ、システムを最新の状態に保つこと、アクセス制御、最小権限の原則、ネットワーク分離などの安全管理措置はどの状況でも基本的な安全対策またはセキュリティ・バイ・デフォルトとしてあらゆる分野において標準化されている中、必要かつ適切な安全管理措置の内容とその組み合わせを決定するにあたり、個人情報取扱事業者が直接または間接的に情報セキュリティ環境および活動に影響を与えるすべての要素を特定の上で最も相応しく効果的な安全管理措置を講ずるべきである。

前に引用した通り、個人情報保護委員会の発行の (平成28 年11 月) (平成31 年1 月一部改正) 「個人情報の保護に関する法律についてのガイドライン（通則編）」によると、当該措置は、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（取り扱う個人データの性質および量を含む）、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されている。[19]

特に、近年の技術発展およびクラウド環境普及に伴い、該当するデータの処理などに使われている（自動化）技術（RPA、AIなど）およびストレージの特性などが含まれる特定の状況に起因するリスク、例えば、物理的な破壊によるデータ削除が困難であるクラウド環境のストレージ、返却する必要があるリース端末などの自組織の管理外のストレージにおける安全なデータの削除の限られた選択を

---

[11] 日本本規格協会の発行「個人情報保護マネジメントシステムー要求事項」（JIS Q 15001：2017）（平成 29 年 12 月 20 日 改正)”(p. 48)

[12] 日本本規格協会の発行「個人情報保護マネジメントシステムー要求事項」（JIS Q 15001：2017）（平成 29 年 12 月 20 日 改正)”付属書 C（参考）安全管理措置に関する管理目的及び管理策(p. 48-59)

[13] 機密性（confidentiality)：認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。(JIS Q 27000：2019 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-用語 p 3.)

[14] 完全性（integrity)：正確さ及び完全さの特性。(JIS Q 27000：2019 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-用語 p 6.)

[15] 可用性（availability)：認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。(JIS Q 27000：2019 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-用語 p 3.)

[16] 個人情報取扱事業者は事業実態及び個人データの取扱い（送信、転送、保存、などの処理）に使用される機器取扱い方法によるさらに、真正性（authenticity)、責任追跡性（accountability)、否認防止（non-repudiation）および信頼性（reliability）のような特性を維持するための措置を検討しても良いと思われる。

[17]「JIS Q 27000：2019 情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-用語」(p 5.)により、情報セキュリティは情報の機密性、完全性、可用性を維持することと定義されている。

[18] 個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編)」(8（別途）講ずべき安全管理措置の内容)では、“個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例”は“基本方針策定”および“個人データの取り扱いに係る規律の整備”に続き“組織的安全管理措置”、“人的安全管理措置”、“物理的安全管理措置”、“技術的安全管理措置”に分けて示す。
または、日本本規格協会の発行「個人情報保護マネジメントシステムー要求事項」（JIS Q 15001：2017）（平成 29 年 12 月 20 日 改正)”(p. 38)による安全管理措置とは，組織的安全管理措置，人的安全管理措置，物理的安全管理措置，及び技術的安全管理措置をいう。

[19] 個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編)」(p. 41)

含むがこれらに限らず考慮しなければならない。このようなリスクベース・アプローチの取組みを採用することによって、よりセキュアな環境よびよりコスト効率化を実現可能だと思われる。

第１節 基本方針の策定

個人情報保護法ガイドライン（通則編）（8（別途）講ずべき安全管理措置の内容）： 8.1）

> 「個人情報取扱事業者は、個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。具体的に定める項目の例としては、「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問及び苦情処理の窓口」等が考えられる。」[20]

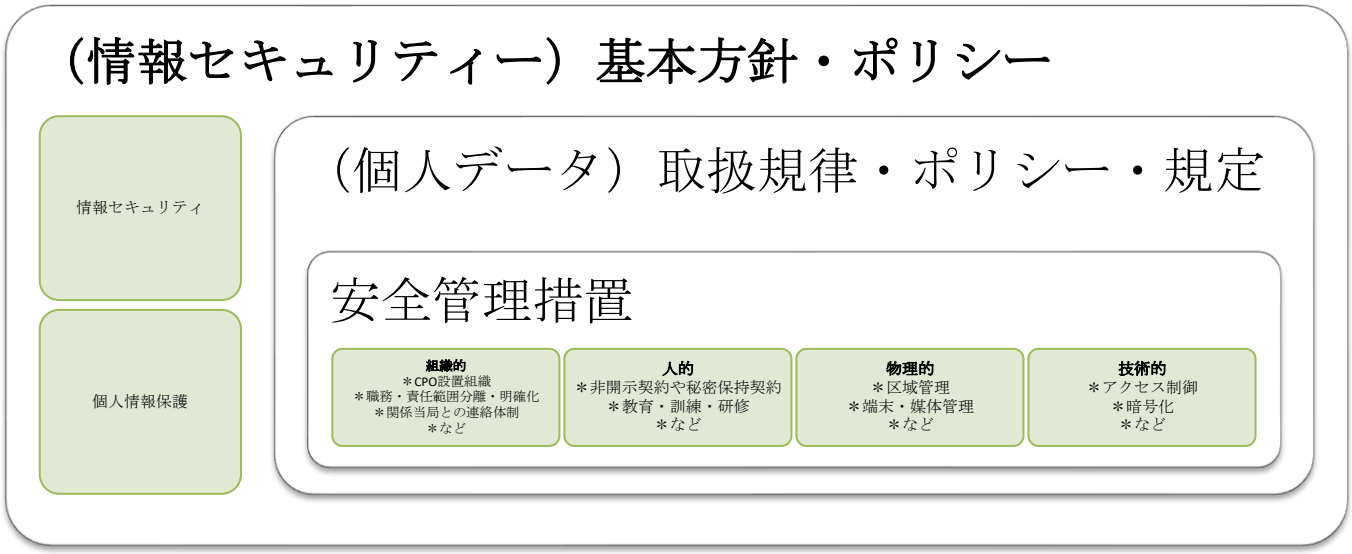
表８　方針に関する記述

個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」			*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
講じなければならない措置	手法の例示	中小規模事業者に置ける手法の例示		
基本方針策定	（上記の説明参照）		*A.3.3.1；A.3.3.2*	*GRM-09*

必要かつ適切な安全管理措置の確実な実施および効率的な運用においては、何よりも重要なのはそれを可能にする組織の全体的な取り組み及び管理体制である。安全管理措置などを含む情報セキュリティ全般、法令の遵守、連絡の窓口など、さらにデータ保護・バイ・デフォルトまたはデータ保護・バイ・デザインの原則へ組織のコミットメントを盛り込んだ方針の策定が重要である。

尚、ISO/IEC 27001 には「情報セキュリティのための方針群」を規定せよとの記載がある。ここに個人情報に関する方針を位置づけることが多く、その場合には以下の図のようになる。

図２　ISMSと個人情報保護方針・安全管理措置等の位置づけ例



第２節 個人データの取扱いに係る規律の整備

（個人情報保護法ガイドライン（通則編）（8（別途）講ずべき安全管理措置の内容）： 8.2）

> 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等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない。[21]

[20] 個人情報保護委員会（平成 28 年 11 月）（平成 31 年 1 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」（p. 87）

[21] 個人情報保護委員会（平成 28 年 11 月）（平成 31 年 1 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」（p. 87）

表９　規律に関する記述

個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」			*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
講じなければならない措置	手法の例示	中小規模事業者に置ける手法の例示		
個人データの取扱いに係る規律の整備	取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定することが考えられる。なお、具体的に定める事項については、以降に記述する組織的安全管理措置、人的安全管理措置及び物理的安全管理措置の内容並びに情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）は技術的安全管理措置の内容を織り込むことが重要である	・個人データの取得、利用、保存等を行う場合 の基本的な取扱方法を整備する。	*A.3.3.5; C.5.1.1; C.5.1.2; C.7.2.1*	*AIS-04; AAC-03; GRM-06; GRM-09*

データのライフサイクルの全過程（データが保存、転送などの処理されている装置の管理を含む）におけるデータセキュリティを確保するためにデータの取り扱い方法、責任者などを明確に文書化し、維持しなければならない。ロケーションやどのようなアクセスを受けているなどの要素を考慮し、（情報）セキュリティの視点から「情報ライフサイクル」を診るデータセキュリティライフサイクル[22]を参照するのは有用である。

第３節　組織的安全管理措置

（個人情報保護法ガイドライン（通則編）（8（別途）講ずべき安全管理措置の内容）：　8.3.(1)～(5)）

> 「個人情報取扱事業者は、組織的安全管理措置として、次に掲げる措置を講じなければならない。
>
> (1) 組織体制の整備

[22] データセキュリティライフサイクルは、データに関するセキュリティ境界とコントロールを理解するのに役立つツールであるが、すべてのタイプのデータに対する厳密なツールとしての利用を想定したものではない。データセキュリティを大ぐくりのレベルで評価し、焦点を当てるべきポイントを発見することを支援するモデリングツールである。（CSA ジャパン「クラウドコンピューティングのためのセキュリティガイダンス v4.0」 p.60-63）

安全管理措置を講ずるための組織体制を整備しなければならない。

(2) 個人データの取扱いに係る規律に従った運用

あらかじめ整備された個人データの取扱いに係る規律に従って個人でータを取り扱わなければならない。 なお、整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、利用状況等を記録することも重要である。

(3) 個人データの取扱状況を確認する手段の整備

個人データの取扱状況を確認するための手段を整備しなければならない。

(4) 漏えい等の事案に対応する体制の整備

漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。 なお、漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である(※)。 (※)個人情報取扱事業者において、漏えい等の事案が発生した場合等の対応の詳細については、別に定める(4(漏えい等の事案が発生した場合等の対応)参照)。

(5) 取扱状況の把握及び安全管理措置の見直し

個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。」[23]

表 10　組織的安全管理措置に関連する記述

個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」			*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
講じなければならない措置	手法の例示	中小規模事業者に置ける手法の例示		
(1) 組織体制の整備	（組織体制として整備する項目の例） ・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 ・個人データを取り扱う従業者及びその役割の明確化 ・上記の従業者が取り扱う個人データの範囲の明確化 ・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の事案の発生又は兆候を把握	・個人データを取り扱う従業者が複数いる場合、責任ある立場の者とその他の者を区分する。	*A.3.3.4; C.6.1.1; C.6.1.2*	*AAC-03; DSI-06; GRM-03; HRS-07; HRS-10*

[23] 個人情報保護委員会（平成 28 年 11 月）（平成 31 年 1 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」(p. 88)

	した場合の責任者への報告連絡体制 ・個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化			
(2) 個人データの取扱いに係る規律に従った運用	個人データの取扱いに係る規律に従った運用を確保するため、例えば次のような項目に関して、システムログその他の個人データの取扱いに係る記録の整備や業務日誌の作成等を通じて、個人データの取扱いの検証を可能とすることが考えられる。データの取扱いの検証を可能とすることが考えられる。 ・個人情報データベース等の利用・出力状況・個人データが記載又は記録された書類・媒体等の持ち運び等の状況 ・個人情報データベース等の削除・廃棄の状況(委託した場合の消去・廃棄を証明する記録を含む。) ・個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況(ログイン実績、アクセスログ等)	・あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。	*A.3.7.1; C.8.1; C.8.2; C.8.3; C.12.4.3*	*AAC-03; DSI-06; DSI-07; GRM-03; HRS-07; HRS-10*
(3) 個人データの取扱状況を確認する手段の整備	例えば次のような項目をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可能とすることが考えられる。 ・個人情報データベース等の種類、名称・個人データの項目 ・責任者・取扱部署	・あらかじめ整備された基本的な取扱方法に従って個人でータが取り扱われていることを、責任ある立場の者が確認する。	*C.8.1; C.8.2; C.9.1.1*	*DSI-01; DSI-04; DSI-06*

	・利用目的 ・アクセス権を有する者 等			
(4) 漏えい等の事案に対応する体制の整備	漏えい等の事案の発生時に例えば次のような対応を行うための、体制を整備することが考えられる。 ・事実関係の調査及び原因の究明 ・影響を受ける可能性のある本人への連絡 ・個人情報保護委員会等への報告 ・再発防止策の検討及び決定 ・事実関係及び再発防止策等の公表等	・漏えい等の事案の発生時に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認する。	*A.3.3.7; C.6.1.3; C.6.1.4*	*SEF-01; SEF-04; STA-02*
(5) 取扱状況の把握及び安全管理措置の見直し	・個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。 ・外部の主体による監査活動と合わせて、監査を実施する。	・責任ある立場の者が、個人データの取扱状況について、定期的に点検を行う。	*A.3.7.1; A.3.7.2; A.3.7.3*	*AAC-02; GRM-09;*

必要かつ適切な安全管理措置を確実に講じ、効率的に機能させるための組織体制を整備しなければならない。組織体制整備の第一の目標は組織の個人情報保護体制の中心となる「個人情報保護管理者（責任者）」[24]（CPOなど）および個人情報保護監査責任者を任命し、その責任と役割を明確化すること、並びに組織内でデータのライフサイクルの全過程における個人情報を取り扱っている職務を最小権限の原則に基づいて分離し責任範囲を明確化することは重要です。インシデント対応一環として法執行機関及び関係当局との侵害や漏洩などのインシデントが発生した時に72時間以内に確実に報告[25]できる直接的な連絡体制を確立し維持することが大切です。さらに業界団体及び専門機関（有志会などを含む）との情報セキュリティ向上や教育目的で連絡体制（参加）を確立し維持することも望ましい。

第４節　人的安全管理措置

> 個人情報取扱事業者は、人的安全管理措置として、次に掲げる措置を講じなければならない。また、個人情報取扱事業者は、従業者に個人データを取り扱わせるに当たっては、法第21条に基づき従業者に対する監督をしなければならない(3-3-3(従業者の監督)参照)。

[24] 個人情報保護管理者：　日本規格協会の発行「個人情報保護マネジメントシステム－要求事項」（JIS Q 15001：2017）（平成29年12月20日　改正）(p.8) による個人情報保護管理者は「トップマネジメントによって組織内部に属する者の中から指名された者であって，個人情報保護マネジメントシステムの計画及び運用に関する責任及び権限をもつ者。注記：“個人情報保護管理者”は、個人情報の取扱いに関する安全管理面だけではなく、組織全体のマネジメントを含む全体の管理である。」注記　“個人情報保護管理者”は，個人情報の取扱いに関する安全管理面だけではなく，組織全体のマネジメントを含む全体の管理者である。

[25] GDPRに基づく要求事項である。「EU一般データ保護規則」（英: General Data Protection Regulation; GDPR）第33条　個データの侵害に関する監督機関への通知（Article 33 Notification of a personal data breach to the supervisory authority）

〇従業者の教育

従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。[26]

表 11　人的安全管理措置に関連する記述

個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」			*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
講じなければならない措置	手法の例示	中小規模事業者に置ける手法の例示		
従業者の教育	・個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。 ・個人データについての秘密保持に関する事項を就業規則等に盛り込む。	（同左）	*C.7.1.2;* *C.7.2.1;* *C.7.2.2;* *C.7.3.1;* *C.13.2.4;*	*HRS-03; HRS-06; HRS-09; MOS-01; MOS-04; MOS-05*

確立されたポリシー及び手順に沿った定期的な個人情報取扱いについて全従業員（雇用形態を問わず）を対象にした教育及び研修のみならず情報セキュリティ全般に関わる最新情報やトレンドに対応した教育および研修の実施は望ましいです。秘密保持につきましては組織内の全従業員（雇用形態を問わず）だけではなく、組織が取り扱う（個人）データにアクセスが許可された外部の者も対象にした非開示契約や秘密保持契約を締結あるいは同様な法的な拘束力のある文書に秘密保持に関する事項を盛り込むことが重要です。

第５節　物理的安全管理措置

（個人情報保護法ガイドライン（通則編）（8（別途）講ずべき安全管理措置の内容）：　8.5.(1)～(4)）

「個人情報取扱事業者は、物理的安全管理措置として、次に掲げる措置を講じなければならない。

(1) 個人データを取り扱う区域の管理

個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域(以下「管理区域」という。)及びその他の個人データを取り扱う事務を実施する区域(以下「取扱区域」という。)について、それぞれ適切な管理を行わなければならない。

(2) 機器及び電子媒体等の盗難等の防止

個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない。

(3) 電子媒体等を持ち運ぶ場合の漏えい等の防止

個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。 なお、「持ち運ぶ」とは、個人データを管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、事業所内の移動等であっても、個人データの紛失・盗難等に留意する必要がある。

[26] 個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」（p. 92）

(4) 個人データの削除及び機器、電子媒体等の廃棄

個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければならない。

また、個人データを削除した場合、又は、個人データが記録された機器、電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要である。」[27]

表 12　物理的安全措置に関連する記述

個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」			*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
講じなければならない措置	手法の例示	中小規模事業者に置ける手法の例示		
(1) 個人データを取り扱う区域の管理	（管理区域の管理手法の例） ・入退室管理及び持ち込む機器等の制限等 なお、入退室管理の方法としては、IC カード、ナンバーキー等による入退室管理システムの設置等が考えられる。 （取扱区域の管理手法の例） ・間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止	・個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置を講ずる。	*C.11.1（全項目）*	*DSI-02; DCS-06; DCS-07; DCS-08; DCS-09*
(2) 機器及び電子媒体等の盗難等の防止	・個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤ	（同左）	*C.11.2.1*	*DCS-02*

[27] 個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」（p. 93）

	一等により固定する。			
(3)電子媒体等を持ち運ぶ場合の漏えい等の防止	・持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 ・封緘、目隠しシールの貼付けを行う。 ・施錠できる搬送容器を利用する。	・個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。	*C.8.3.1;* *C.8.3.3;* *C.11.2.5*	*DSI-04*
(4)個人データの削除及び機器、電子媒 体等の廃棄	(個人データが記載された書類等を廃棄する方法の例) ・焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。(個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄する方法の例) ・情報システム(パソコン等の機器を含む。)において、個人データを削除する場合、容易に復元できない手段を採用する。 ・個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する。	・個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄したことを、責任ある立場の者が確認する。	*C.8.3.2;* *C.11.2.7*	*DSI-07; DCS-05*

クラウド(技術・サービス)活用により、個人情報取扱事業者は(物理的)安全管理措置の視点からクラウド事業者に一部のリスクを移転することは可能な場合がある。(「委託先の監督」を参照)

第６節 技術的安全管理措置

(個人情報保護法ガイドライン(通則編)(8(別途)講ずべき安全管理措置の内容): 8.6.(1)～(4))

> 「個人情報取扱事業者は、情報システム(パソコン等の機器を含む。)使用して個人データを取り扱う場合(インターネット等を通じて外部と送受信等する場合を含む。)、技術的安全管理措置として、次に掲げる措置を講じなければならない。
>
> (1) アクセス制御
>
> 担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制

御を行わなければならない。

(2) アクセス者の識別と認証

個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。

(3) 外部からの不正アクセス等の防止

個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。

(4) 情報システムの使用に伴う漏えい等の防止

情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。」[28]

表 13　技術的安全管理措置に関連する記述

個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」			*個人情報保護マネジメントシステム－要求事項（JIS Q 15001：2017）*	*CCM*
講じなければならない措置	手法の例示	中小規模事業者に置ける手法の例示		
(1) アクセス制御	・個人情報データベース等を取り扱うことのできる情報システムを限定する。 ・情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ・ユーザーID に付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。	・個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止す る。	*C.9.1(全項目)*	*AIS-02; HRS-08; IAM-02; IAM-10; IVS-11*
(2) アクセス者の識別と認証	(情報システムを使用する従業者の識別・認証手法の例)・ユーザーID、パスワード、磁気・IC カード等	・機器に標準装備されているユーザー制御機能(ユーザーアカウント制御)により、個人情報データベース等を取り扱う情報システ ムを使用する従業者を識別・認証する。	*C.9.2(全項目); C.9.4.2*	*HRS-08; IAM-03; IAM-04; IAM-05; IAM-06; IAM-09; IAM-12; IVS-11*
(3) 外部からの不正アクセス等の防止	・情報システムと外部ネットワークとの接続箇所にファイアウォール等	・個人データを取り扱う機器等のオペレーティングシ	*C.12.2; C.12.4(全項目); C.14.2.4*	*IVS-01; IVS-06; IVS-07; TVM-01*

[28] 個人情報保護委員会（平成 28 年 11 月）（令和 2 年 10 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」(p. 96)

	を設置し、不正アクセスを遮断する。 ・情報システム及び機器にセキュリティ対策ソフトウェア等(ウィルス対策ソフトウェア等)を導入し、不正ソフトウェアの有無を確認する。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ・ログ等の定期的な分析により、不正アクセス等を検知する。	ステムを最新の状態に保持する。 ・個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。		
(4)情報システムの使用に伴う漏えい等の防止	・情報システムの設計時に安全性を確保し、継続的に見直す(情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。)。 ・個人データを含む通信の経路又は内容を暗号化する。 ・移送する個人データについて、パスワード等による保護を行う。	・メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。	*C.10(全項目)；* *C.12.6.1*	*AIS-04；EKM-03；* *IVS-05；IVS-10；* *TVM-02*

近年、様々な内部の要因（働き方改革、ワーカーの多様性、DXなど)・外部要因（インフルエンザなどの感染症の大流行、災害など）による急速に変化している労働環境はセキュリティ上の新たな課題が露呈しています。特に、リモートワークや在宅勤務の場合はBYOD、VPNアクセスなどによる情報へのリモートアクセスや情報の持ち出しなどにおけるセキュリティリスクが高まっているとは言え、より一層の安全管理対策が求められている。

第３章　事業者による従業員および委託先の監督（第20条、第21条）

個人情報取扱事業者は法の規定により従業員、および委託先の監督義務を負う。

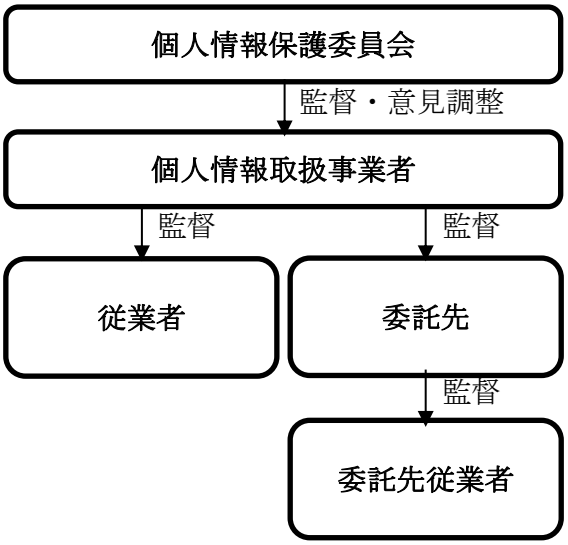
表 14　監督義務に関する規定（抜粋）

項目　［該当条文］	事業者の対応	GDPR との比較
従業者の監督 ［第 21 条］	個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。	GDPR では、監督義務を負うのは各国の監督機関であり、Data Controller と Data Processor は監督機関への協力義務がある。（第 31 条）
委託先の監督 ［第 22 条］	個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、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、委託を受けた者に対する必要 かつ適切な監督を行わなければならない。	

司

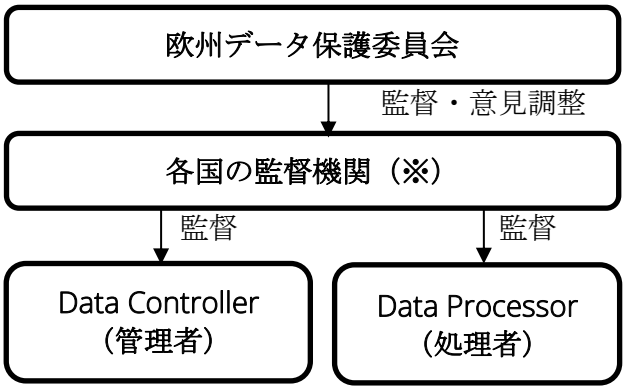
図３　個人情報保護法とGDPRの執行体体制の比較

個人情報保護法の監督・執行体制



義務を負う主体：　個人情報取扱事業者
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。ただし、次に掲げる者を除く。（法第2条第5項）
(1) 国の機関
(2) 地方公共団体
(3) 独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平 成 15 年法律第 59 号）第 2 条第 1 項に規定する独立行政法人等をいう。以下同じ。）
(4) 地方独立行政法人（地方独立行政法人法（平成 15 年法律第 118 号）第 2 条第 1 項

GDPRの監督・執行体制



※ Data Controller とData Processor は、複数の加盟国にまたがって事業を行う場合、原理的には、複数の加盟国の監督当局を相手にする必要がある。

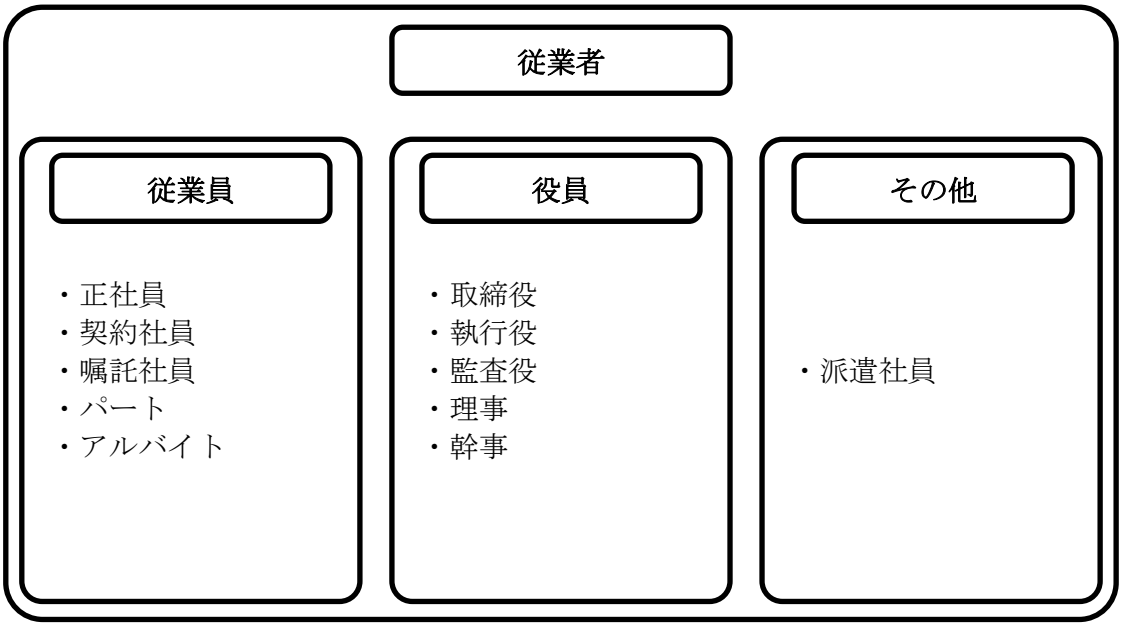
義務を負う主体：
(1) Data Controller（管理者）
(2) Data Processor（処理者）
上記2区分に該当する場合、法人格の有無、営利性の有無は問わず、自然人、法人、公的機関、行政機関又はその他の団体の全てが適用対象となる。（第4条第7号・第8号）

第１節 個人情報取扱事業者の従業者監督義務（第21条）

第１項 従業者の定義

従業者とは、個人情報取扱事業者の組織内にあって、直接または間接的に事業者の指揮監督を受けて事業者の業務に従事している者を言う。

図４　従業者の定義



第２項 従業者の監督方法

個人情報保護法上は、「当該従業者に対する必要かつ適切な監督」について具体的な規定を設けてはいない。そのため、実務上の必要な措置を講じる場合は、「個人情報保護法ガイドライン（通則編）」や「（別添）特定個人情報の適正な取り扱いに関する安全管理措置の内容」、東京都が発行している「個人情報保護制度パンフレット（平成30年3月度版）」が参考となる。

表 15　【個人情報保護法ガイドライン（通則編）】抜粋

【従業者に対して必要かつ適切な監督を行っていない事例】
事例 1） 従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを確認しなかった結果、個人データが漏えいした場合
事例 2） 内部規程等に違反して個人データが入ったノート型パソコン又は外部記録媒体が繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、当該パソコン又は当該記録媒体が紛失し、個人データが漏えいした場合

表 16　【（別添）特定個人情報の適正な取り扱いに関する安全管理措置の内容】抜粋

Ｃ 人的安全管理措置
事業者は、特定個人情報等の適正な取扱いのために、次に掲げる 人的安全管理措置を講じなければならない 。

ａ 事務取扱担当者の監督
事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。

ｂ 事務取扱担当者の教育

事業者は、事務取扱担当者に特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う。

【手法の例示】

＊ 特定個人情報等の取扱いに関する留意事項等について、従業者に定期的な研修等を行う。
＊ 特定個人情報等についての秘密保持に関する事項を就業規則等に 盛り込むことが考えられる。

表 17　東京都 個人情報保護制度パンフレット（平成30年3月度版）抜粋

組織体制の整備	● 個人情報保護に関する責任者を決め、それぞれの部署の役割を明確にする ● 個人データの取り扱いに関するチェック体制や、事故発生時における体制を整備する
規定類の整備	● 個人データの取得、利用、送信、保管、廃棄といった取り扱いフローごとに手続きを定める
個人データ取扱状況の一覧	● 取り扱っている個人データの項目、利用目的管理方法を記載した個人情報取り扱い DB を整備し、取り扱っている個人データの把握に努める
雇用時の契約	● 従業員の採用時に個人情報の取扱に関する契約を交わす
従業員の教育	● 従業員の役割を明記した規定の周知を行う ● 定期的に研修を行う
セキュリティ対策	● 個人情報を取扱うファイルや端末にパスワードをかける。 ● ウイルス対策を行う ● 情報にアクセスできる従業員は限定する ● データ送受信の際、個人データは暗号化する

読み取れるポイント（講ずべき措置）としては

① パソコンや電子記録媒体等の管理を徹底する

② 文書管理を徹底する

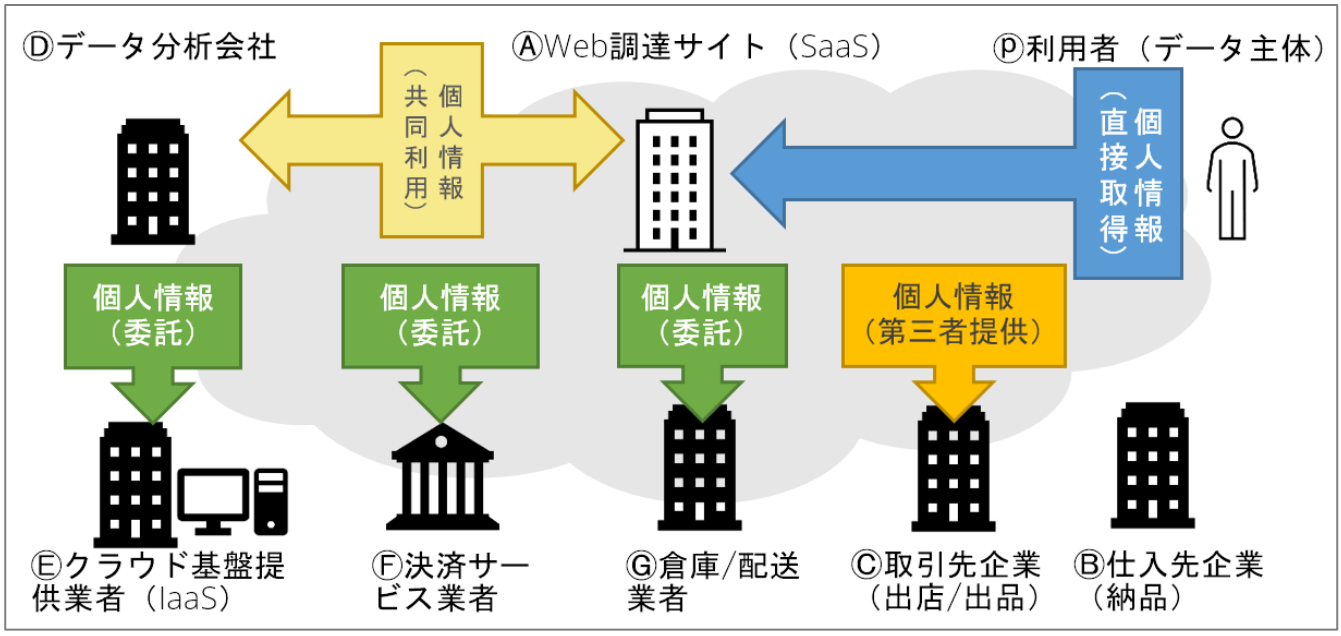
③ 個人情報の取り扱いに関するマニュアルの配布し、定期的な研修を行う

④ 秘密保持に関する事項を就業規則等に 盛り込み、情報漏洩しない旨の誓約書を取り付ける

といったことが挙げられる。

第３項 参照モデルでの対応例

（再掲）図１　Web調達サイト（法人向けECサイト）のモデル



- Web調達サイト（Ⓐ）の管理に携わる従業者に対しては非開示契約を締結し、誓約書の提出を義務づける。
- 個人情報保護の規程・手順に関しては周知徹底し、教育・訓練を実施したうえで、定期的に個人情報の取扱い状況に対するモニタリングを実施する。
- 従業員以外では、Web 調達サイト（Ⓐ）のシステム開発や機器のメンテナンスを外部委託している場合、当該業務に携わる者も対象とみなす。そのほか、Web調達サイト（Ⓐ）が稼働している建物等に立ち入る可能性ある者、例えば建物の清掃担当者や警備員に関しても同様に対象とみなす。
- 近年ではクラウド基盤提供業者（Ⓔ）からリソースを調達することが多いと思われるので、選定の際に前述の仕組が導入された「信頼できる企業」であることを確認する必要がある。

第２節 個人情報取扱事業者の委託先監督義務（第22条）

万が一、監督を怠った結果として委託先から個人情報が漏洩した場合、委託元は個人情報漏洩の責任追及を免れることができない。よって、委託元は業務委託時に、委託先が法人・個人であるかを問わず、非開示契約を締結し、委託先への監督権限や損害賠償の可能性を担保しておかねばならない。

第１項 委託先の定義

「個人情報保護法ガイドライン（通則編）」の「3-3-4 委託先の監督（法第 22 条関係）」によると、「個人データの取り扱いの委託」とは契約の形態・種類を問わず、個人情報取り扱い事業者が他の者に個人データの取り扱いを行わせることをいい、「委託先」とは、個人情報取扱事業者から、個人データの取扱いの全部又は一部の委託を受けた者を指す。

第２項 委託先の監督方法

従業員の監督方法同様に、個人情報保護法上は、「委託を受けたものに対する必要かつ適切な監督」について具体的な規定を設けてはいない。実務上の必要な措置を講じる場合は、「個人情報保護法ガイドライン（通則編）」が参考となる。

表 18　個人情報保護法ガイドライン（通則編）3-3-4 委託先の監督（法第 22 条関係）要約

（1）適切な委託先の選定	● 委託先の安全管理措置が、少なくとも法第 20 条及び本ガイドラインで委託元に求められるものと同等であることを確認する ● 具体的には「8（（別添）講ずべき安全管理措置の内容）」に定める各項目が、委託する業務内容に沿って、確実に実施されることについて、あらかじめ確認する
（2）委託契約の締結	● 当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込む
（3）委託先における個人データ取扱状況の把握	● 定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価する ● 委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データの取扱方法等について、委託先から事前報告を受け又は承認を行う

読み取れるポイントとしては委託先に対して最低でも

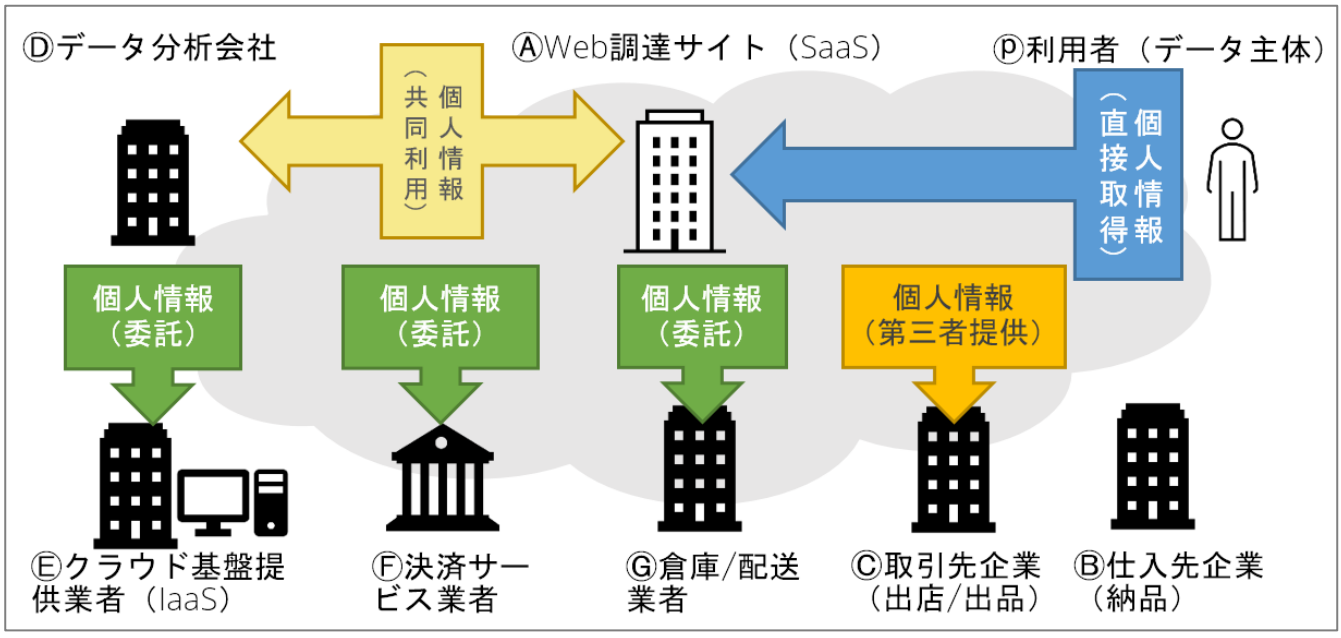
①　法第20条で委託元に求められた水準の安全管理措置

②　法第21条で委託元が求められた水準の従業員監督

が求められていると考えられる。なお、委託先が再委託を行う場合や、再委託先が再々委託を行う場合も同等の水準の措置が求められると考えるべきである。

第３項 参照モデルでの対応例

（再掲）図１　Web調達サイト（法人向けECサイト）のモデル



Web調達サイト（Ⓐ）の委託先（Ⓔ, Ⓕ, Ⓖ）へ個人情報を委託する際、考えうるリスクとしては以下のものが考えられる。

表 19　考えうるリスク

リスク項目	例
収集に関するリスク	・委託先（Ⓔ）との通信の盗聴による情報漏洩 ・委託先（Ⓔ）サーバの脆弱性をついた攻撃による情報漏洩
利用に関するリスク	・委託先（Ⓔ）サーバのウイルス感染による情報漏洩 ・委託先（Ⓔ）サーバの脆弱性をついた攻撃による情報漏洩 ・委託先（Ⓔ）従業者の目的外の情報利用発覚
廃棄に関するリスク	・委託先（Ⓔ）の不適切な HDD 廃棄 ・委託先（Ⓔ）の不適切な紙媒体廃棄 ・委託先（Ⓔ）の記憶媒体の廃棄忘れ
監査・事後対応に伴うリスク	・加入者（Ⓟ）からの損害賠償請求 ・事故の発生による信用失墜

これらのリスクに対して、委託先（Ⓔ）とは非開示契約を締結し、監督権限や損害賠償の可能性を担保する。契約締結に際し、盛り込むことが推奨される事項は下表を参照。

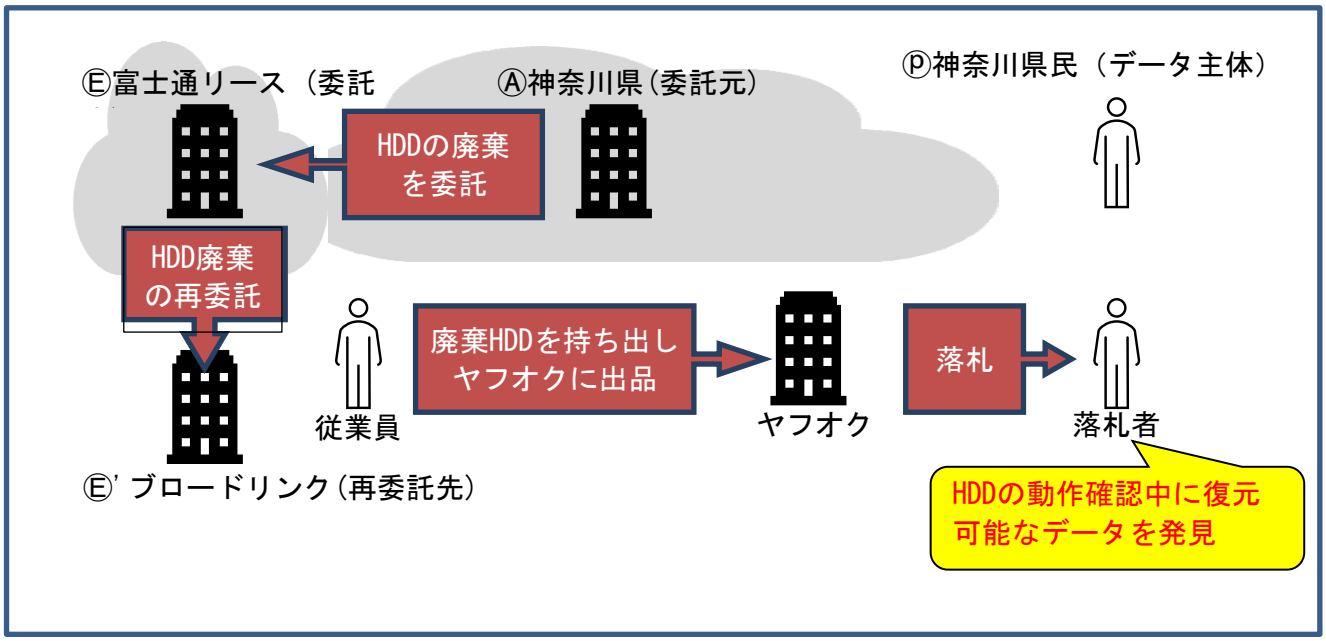
表 20　個人情報の取扱いを委託する場合に契約に盛り込むことが推奨される事項

1.　委託者及び受託者の責任の明確化
2.　個人情報の安全管理に関する事項
3.　再委託に関する事項
4.　個人情報の取扱状況に関する委託者への報告の内容及び頻度
5.　契約内容が遵守されていることの確認
6.　契約内容が遵守されなかった場合の措置
7.　セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

第３節 実際に発生したセキュリティ事故から見る法第21条、第22条

実際に発生した事故としては、2019年12月6日、インターネットオークションで落札したハードディスクから神奈川県の行政文書とみられるデータが復元された事例がある。
HDDは神奈川県各部局の共有ファイルサーバーで利用されていたものであり、流出経路は以下の通りである。

図５　情報流出までの流れ



オンプレの環境のため参照モデルと完全に合致させることはできないが、この事件では、

神奈川県(委託元)　⇒ Ⓐ

富士通リース(委託先)　⇒ Ⓔ

ブロードリンク(再委託先)⇒ Ⓔ′

と見なした場合、法21条、法22条それぞれの観点で以下の問題点があると考えられる。

表 21　法21条の観点での問題点

組織	問題点
Ⓐ神奈川県（委託元）	● 取り外された HDD は外部記録媒体に相当するものと考えるべきであり、セキュリティを考慮した場合、格納されたデータは暗号化されていて然るべきものであるが、そのような処置は施されていなかった。（規定類の不備）
Ⓔ富士通リース社（委託先）	● 廃棄証明書の発行を再委託先に依頼できていない案件があるにも関わらず、組織内でチェックできていなかった。（整備された規定に従ったオペレーションが実行されていない/ 組織としてのチェック体制の不備）

組織	問題点
Ⓔ’ブロードリンク社 （再委託先）	● 以前より、インターネット掲示板等に内部の機器横流しの情報が出回っていたが、会社自身でそのような状況を把握できていなかった。 （組織としてのチェック体制の不備） ● 入庫、消去/破壊作業、出荷等の状況トレースが十分行われておらず、入庫数しか記録されていなかった。 （規定類の不備 / 組織としてのチェック体制の不備） ● 保管庫に監視カメラを設置するなどのセキュリティ対策を導入していたものの、モニタリングはほとんど行われていなかった。なお、監視カメラの記録には実際に従業員が HDD を持ち出すところが記録されていたことが判明している。 （整備された規定に従ったオペレーションが実行されていない / 組織としてのチェック体制の不備）

表 22　法22条の観点での問題点

組織	問題点
Ⓐ神奈川県 （委託元）	● HDD をリース会社（委託先）に返却した後、データ消去証明書を受け取ることになっていたが、流出が確認されたものを含め数百個の HDD で、リース会社から消去の証明書が提出されていなかったにも関わらず、組織内でチェックできていなかった。 （委託先の監督が適切に為されていない） ● 担当者は廃棄作業が委託先で行われておらず、実作業が再委託先で行われていることを把握していなかった。 （委託者及び受託者の責任、再委託に関する事項が明確にされていない）
Ⓔ富士通リース社 （委託先）	● 機器廃棄を完全に再委託先に丸投げしていた。 （委託者及び受託者の責任、再委託に関する事項が明確にされていない / 再委託先の監督が適切に為されていない）
Ⓔ’ブロードリンク社 （再委託先）	―

第４章　個人情報の提供（第23条、第24条、第25条、第26条）

第１節　日本における個人情報の提供

日本の個人情報保護法において、いくつかのケースを除いて第三者に対して個人情報を提供することは禁じられている（法第23条1項）が、相手先によっては第三者提供とみなされない場合もあり、条件によっては同意なしの第三者提供が許容されている場合もある。状況はやや複雑である。

整理のため、以降第三者とは何を示すか、提供とは何を示すか、第三者提供とみなされないケースや第三者提供が許されるケースとはどのような場合があるか等を、法やガイドライン等から読み取れる内容を基礎に整理していく。

本節ではいわゆる個人情報保護法は「法」、同法のガイドラインは「ガイドライン」、「「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ&A」は「QA」と記載する。尚、本節は2015年改正個人情報保護法を対象に記述し、2020年改正個人情報保護法については次節で解説されている。

第１項 「提供」の解釈

提供についてはガイドライン通則編に、以下のように記載されているため本文書内でもそのように解釈する。

> 「提供」とは、個人データ、保有個人データ又は匿名加工情報（以下この項において「個人データ等」という。）を、自己以外の者が利用可能な状態に置くことをいう。個人データ等が、物理的に提供されていない場合であっても、ネットワーク等を利用することにより、個人データ等を利用できる状態にあれば（利用する権限が与えられていれば）、「提供」に当たる。[29]

第２項 「第三者」の解釈

第三者とは、「①当該個人データによって特定される本人、②当該個人データを提供しようとする個人情報取扱事業者以外の者をいい、自然人、法人その他の団体を問」わない[30]。この第三者には親会社、子会社、グループ会社やフランチャイズ組織の本部および加盟店などが含まれている[31]。したがって、ある個人情報取り扱い事業者が、これら関連企業に対して個人情報を提供した場合、これは個人情報の第三者提供にあたる。

第三者の原則的な定義そのものは上述の通りだが、法律の規制のかかり方が、国内の第三者と「外国にある第三者」では差が出てくる。実質的に、国内の第三者への提供と外国にある第三者への提供と、それぞれに別の規制があるという事である。

以降、便宜上これらを分けて説明していく。

第３項 国内の第三者への提供に関する規制

国内の第三者の解釈

通常、単に「第三者」と呼ばれるが、本節では説明の便宜上「国内の第三者」と表記する。一般にはこのように明示されないので注意されたい。

さて、国内の第三者提供に関する規制にのみ適用される例外がある。個人情報取扱事業者が自身の組織の外部に個人情報を提供する場合において、条件によっては、その相手先は「第三者に該当しない」と定義づけられている[32]。

- 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合
- 合併その他の事由による事業の承継に伴って個人データが提供される場合
- 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

平たく言えば、以下の場合においては第三者提供についての規制を気にする必要はないと解すことができる。

- 個人情報の利用目的の達成に必要な範囲内において委託先に個人情報を提供するとき（ただし、委託先の監督などは必要である）

---

[29] ガイドライン（通則編）2-13 「提供」
[30] QA 1-5 Q-5-1 個人データの第三者への提供（法第 23 条～第 26 条関係）A5-1
[31] ガイドライン（通則編）3-4-1 第三者提供の制限の原則（法第 23 条第 1 項関係）
[32] 法第 23 条第 5 項

- 合併、分社化、事業譲渡等によって事業が承継されることに伴って、当該事業に関わる個人データが提供される場合。並びに、事業承継のための交渉等のために自社の個人データを相手会社へ提供する場合。ただし追加規制あり[33]。
- 提供先と共同利用を行うものとし、共同利用に必要な規制[34]をクリアしている場合

従って、ここでは第三者提供における国内の第三者を以下のように解する。

「本人および本人が個人情報を提供した先の個人情報取り扱い事業者（特定の法人・団体または個人）以外の全てを指す。ただし、利用目的の達成のために個人情報取扱事業者から委託される先・事業承継等が発生した場合の相手先ならびに共同利用先を除く」

尚、国内の第三者にあたらない場合であっても委託先の監督や共同利用に関する規制は適用されることに注意されたい。

国内の第三者提供に対する規制の原則

上述の「国内の第三者」にあたる他者に対して個人情報を「提供」しようとする場合にかかる規制が法第23条ということになる。

原則としては、法令などに基づく場合や本人に危険がある等の特別な場合を除いて、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない、とされている。

また、第三者提供時にはその提供者および受領者によって、提供および受領の記録がなされなければならないと規定されている[35]。これを第三者提供の確認・記録義務と称するが、第三者提供であってもこの義務が適用される場合と適用されない場合とがある。例としては、本人に代わって第三者提供を行う場合等がある。これら例外はガイドライン（第三者提供の確認・記録義務編）に詳述されているのでそちらを参照されたい。ここでは、第三者提供を行う場合には記録・確認義務が付随する場合があると覚えておいていただきたい。

例外として、オプトアウトによる第三者提供を行う場合には本人の同意なくして第三者に個人情報を提供することができる。次項で説明する。

同意なしの第三者への提供が許される場合

日本においてオプトアウトによる第三者提供と呼ばれるものだが、この呼称は極めて判りづらい。実態としては、個人情報取り扱い事業者が一定の条件を満たした場合、本人の同意なく第三者に個人情報を提供できるというだけのことである。またこの許可は、現行法では国内の第三者に提供する場合に限られる。

要件の詳細はガイドライン（通則編） “3-4-2-1 オプトアウトに関する原則（法第23条第2項関係）”に詳述されているため参照されたい。特徴のみ切り出せば以下のようになる。

- 本人の求めに応じて第三者提供を停止すること
- 法に定められている事項をあらかじめ本人に通知しまたは本人が容易に知り得る状態に置くこと
- オプトアウトによる第三者提供の届出を個人情報保護委員会に行うこと[36]

尚、二点目に定められている通知又は公表する事項には「第三者への提供を利用目的とすること」という記載がある。このため、すでに保有している個人情報の利用目的に第三者への提供が含まれて

[33] ガイドライン（通則編）3-4-3 (2) 事業の承継（法第 23 条第 5 項第 2 号関係）
[34] ガイドライン（通則編）3-4-3 (3) 共同利用（法第 23 条第 5 項第 3 号関係）
[35] ガイドライン（通則編）3-4-5 第三者提供に係る記録の作成等（法第 25 条関係）
[36] https://www.ppc.go.jp/personalinfo/legal/optout/

いない場合にはいわゆるオプトアウトによる第三者提供を行うことはできない。先に利用目的の変更に関する手続きを要する点に注意が必要である。

第４項 外国にある第三者への提供に関する規制

前述の通り、国内の第三者と外国にある第三者では定義が違い、また規制内容にも差異が認められる。

外国にある第三者の解釈

外国にある第三者においては、委託・事業承継等が発生した場合・共同利用等による提供であっても例外とはならず、第三者扱いのままである。このため原則本人の同意が必要となる。また、オプトアウトによる第三者提供も認められない。これは個人情報保護法24条（外国にある第三者への提供の制限）において、以下のように記述されているからである。

> (前略)前条第一項各号に掲げる場合を除くほか、あらかじ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。この場合においては、同条の規定は、適用しない。

一方、別の例外が存在しており、この例外が該当すると外国にある第三者扱いしなくてよい、というこになる。結果として23条（第三者提供の制限）が適用され、国内の第三者にあたるかどうかを評価する。

すなわち、個人情報の提供をするにあたり

- それが外国の第三者にあたる場合には、本人の同意が必要である（海外にある委託先の場合でも、外国にある第三者への提供である旨の通知と同意が必要である）
- 外国の第三者にあたらない場合には、23条が適用される

この外国の第三者の例外の条件であるが、「個人情報の保護に関するガイドライン（外国にある第三者編）」の総論[37]に以下のように記載されている。

> 個人情報取扱事業者は、個人データを外国にある第三者に提供するに当たっては、法第24条に従い、次の①から③までのいずれかに該当する場合を除き、あらかじめ「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」を得る必要がある。
>
> ①当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号。以下「規則」という。）で定める国にある場合（※1）
>
> ②当該第三者が、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として規則で定める基準に適合する体制を整備している場合
>
> ③法第23条第1項各号に該当する場合（※2）

上記①～③については、同文書の上記引用部分以降で詳述されているので参照されたい。

尚、上記引用およびその注釈の後に記載されている「外国にある第三者に対する個人データの提供が、法第23条に規定する方法のいずれにより行われるかによって、法第24条の適用が決まる」から「図：個人データを提供する方法と法第24条の適用関係」について記述が複雑であるが、要は上記の外国にある第三者の例外にあたる場合においては、23条が適用される、ということが書いてある。

第２節 第三者提供に関する法改正の補足及びＧＤＰＲとの比較考察

[37] https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/#a2

第４章の課題をCSA-JPプライバシーWGで検討するあたり、2015改正個人情報保護法について以下の条文とGDPRとの比較を行い、考察を述べる。

- 2015年改正個情法２３条：第三者提供の制限、
- 2015年改正個情法２４条：外国にある第三者提供への提供の制限
- 2015年改正個情法２５条：第三者提供に係る記録の作成等
- 2015年改正個情法２６条：第三者提供を受ける際の確認等（受領側に提供側の本人同意）

ただし、第一節については、現行法である2015改正個人情報保護法に対して、今年6月に公布された2020年改正個人情報保護法で講じられる措置が大きく異なり、留意すべき点を３つにまとめてみた。一つ目の留意点は、附則12条「いわゆる3年ごとの見直し」により、法の域外適用と越境移転の在り方が追加された。二つ目の留意点は、「第三者提供記録に本人が開示請求可、オプトアウト規定の範囲を縮小」などを定め、個人の権利の在り方が改正された。三つ目の留意点は、「個人情報取扱事業者、匿名加工情報取扱事業者、仮名加工情報取扱事業者、個人関連情報取扱事業者」と新しい定義も含め、取扱事業者別に守るべき責務の在り方が改正された。

これらの経緯を考慮し、当該第４章第２節を３項に分けて比較と考察を述べる。１項目は、現行法である2015改正個人情報保護法とGDPRとの比較を行う。２項目は、2020改正個人情報保護法とGDPRとの比較を行う。３項目は、CookieやIPアドレス等の識別子を例に比較を行う。

第１項　２０１５改正個人情報保護法とＧＤＰＲ

ここでは、現行法である2015改正個人情報保護法とGDPRとの間で第三者提供の比較を行う。

①個情法23条（第三者提供の制限）について

1. “第三者提供の許諾”は、要配慮情報だけが主体同意で、その他は公表同意（オプトアウト可）である。
2. “第三者提供の義務”は、提供元に（提供年月日、提供先氏名等の）記録作成の義務を課し、提供先には（受領年月日、提供元氏名等の）確認義務を課しているだけで、罰則のない配慮義務である。
3. “データ主体の権利”は、提供停止を求めることができるが、すでに提供済みのデータ削除を求める権利は条文に無い。

- 現行法で、提供時のオプトアウトを可能とした事例

  事例1　口頭同意＝本人からの同意する旨の意思表示を受ける場合

  事例2　書面同意＝本人からの同意する旨の書面（電磁的記録を含む。）を受ける場合

  事例3　チェック同意＝本人による同意する旨の確認欄(チェックボックス)にチェックする場合

  事例4　重ね同意＝本人による同意する旨の確認文＆ボタン（利用規約に同意して申し込む）をクリック

  事例5　任意同意＝「会員にメルマガ配布するため」と伝えた上で個人情報を利用する場合

  事例6　約款同意＝有効な約款に同意条項がある場合

  事例7　委託同意＝不動産所有者の個人情報を紹介する不動産業者が購入する業者に情報提供する場合

- 現行法で、第三者提供に該当していないとした事例

事例1　個人情報データベース等を構成する前の入力用の帳票等に記載されている個人情報を提供する場合

事例2　データの打ち込み等、情報処理を委託するために個人データを提供する場合

事例3　グループ企業で総合的なサービスを提供する為に取得時の利用目的の範囲内で情報を共同利用する場合

- 現行法で、提供時のオプトアウト制限した事例

事例1　会員名簿や卒業名簿等を売買する名簿業者

②GDPRにおける提供制限について

1. “第三者提供の許諾”は、16才未満の子供は親権者の同意が必要、その他は主体同意である。機微情報は、原則、取扱禁止である。
2. “第三者提供の義務”は、提供側も受領側も提供データの状況を本人に通知する義務がある。かつ第三者提供で有っても無くても、管理者と処理者である企業に罰則がある。
3. “データ主体の権利”は、訂正・削除・移転の権利がある、かつ、忘れ去られる権利・プロファイリングされない権利・異議を述べる権利を有する。

第２項　２０２０改正個人情報保護法とＧＤＰＲ

ここでは、2022年施行予定である2020改正個人情報保護法とGDPRとの間で外国への第三者提供の比較を行う。

① 個情法24条（外国にある第三者提供の制限）について。

1. 保護委員会告示1号で定めたEEA31カ国”に対して、外国であってもオプトアウトによる提供を認めた。
2. “外国提供の許諾”は、規則で定められた国への提供は、公表同意（オプトアウト可能）である。
3. “外国提供の義務”は、基本、国内の第三者提供と同じで、提供元に（提供年月日、提供先氏名等の）記録作成の義務を課し、提供先には（受領年月日、提供元氏名等の）確認義務を課しているだけで、罰則のない配慮義務である。
4. “データ主体の権利”は、提供停止を求めることができるが、すでに提供済みのデータ削除を求める権利はない。

② GDPRにおける外国への提供制限について

1. “外国移転の認定”は、EEA31カ国などGDPR十分性を認定した国・地域、および米国などデータ移転だけを認めた国・地域である。
2. “外国提供の許諾”は、16才未満の子供は親権者の同意が必要、その他は主体同意である。機微情報は、原則、取扱禁止である。
3. “外国提供の義務”は、提供側も受領側も提供データの状況を本人に通知する義務がある。かつ第三者提供で有っても無くても、管理者と処理者である企業に罰則がある。
4. “データ主体の権利”は、訂正・削除・移転の権利がある、かつ、忘れ去られる権利・プロファイリングされない権利・異議を述べる権利を有する。

上記の第１項と第２項を比較表の形式にまとた。

表 23　現行法との比較（個人情報保護法とGDPR）

比較対象 / 比較項目	（現行法）個人情報保護法 （2015改正、2017年施行）	（現行法）GDPR一般データ保護規則 （2016制定、2018年施行）
上位法令の違い	日本国憲法において、 「個人情報保護」の条文なし	EU 憲法において、 「I-51 条：個人情報保護」の条文あり
定義の違い	＜比較＞ ・法の対象者 　生存者、取扱事業者、第三者、委託先、共同利用者、事業継承者 ＜関連条文＞ 2 条（定義） ・生存者とは、生存する本人 ・取扱事業者とは、個人情報データベース等を事業の用にしている者 ・第三者とは、上記以外の者 その他 ・委託先とは、処理を委託される者 ・共同利用者とは、共同利用する者 ・事業継承者とは、合併等で事業を継承する者	＜比較＞ ・法の対象者 　自然人、管理者、共同管理者、処理者、取得者、第三者 ＜関連条文＞ 4 条（定義） ・自然人とは、データ主体 ・管理者とは、単独で取扱を決定する者 ・共同管理者とは、共同して決定する者 ・処理者とは、管理者に代わり取扱う者 ・取得者とは、開示請求を受ける者 ・第三者とは、上記以外の者
同意の違い	＜比較＞ ・個人情報の取扱は、公表同意 ・子供の同意は、明記なし ・要配慮情報は、提供が禁止 ・同意の撤回は、なし ＜関連条文＞ 15 条（利用目的の特定） 利用の目的を特定する。 16 条（利用目的による制限） 範囲を超えて取り扱わない。 18 条（利用目的の通知等） 利用目的は本人に通知または公表する。＞公表同意の意味	＜比較＞ ・個人情報の取扱は、主体同意 ・16 才未満の子供は、親権者の同意 ・機微情報は、原則、取得が禁止 ・同意の撤回は、何時でも可能 ＜関連条文＞ 6 条（取扱の適法性） 取扱はデータ主体から同意を得る。 7 条（同意の要件） 同意はオプトイン、いつでも同意撤回可 8 条（子供の同意要件） 16 才未満の子供は親権者の同意を得る。 9 条（機微情報の取扱） 人種/政治/宗教/生体データ等は原則禁止。

比較対象 比較項目	（現行法）個人情報保護法 （2015改正、2017年施行）	（現行法）GDPR一般データ保護規則 （2016制定、2018年施行）
23条：第三者提供の制限	＜比較＞ ・第三者提供の許諾は、公表同意 ・要配慮情報は、オプトアウト禁止 ・他はオプトアウト可能 ・提供企業は、本人通知または公表 ＜関連条文＞ 23 条（第三者提供の制限） オプトアウト手続により第三者提供する者は、以下の事項を、本人通知または容易に知り得る状態に置き（公表等）、ならびに保護委員会に届け出る。 23 条 2（オプトアウト手続） 本人に通知または公表した上で、本人の主体同意を得ることなく第三者に提供すること。 ・個人データを第三者に提供する旨 ・提供する個人データの項目 ・提供方法 ・本人の要請で提供を停止する旨 ・提供の方法 ・提供停止の受付方法 25 条（提供元で提供記録の作成） 第三者提供しときは、保護委員会規則に従い、記録を作成する。 ・提供年月日 ・提供先の氏名等 26 条（提供先で確認） 受領側は、提供側で作成した記録の確認をする。	＜比較＞ ・第三者提供の許諾は、主体同意 ・すべて、原則、オプトアウト禁止 ・データ主体は、提供データの移転権 ・提供企業は、本人に情報提供 ・受領企業も、本人に情報提供 ＜関連条文＞ 13 条（直接取得時の情報提供） データ主体から収集する場合、データ主体に管理者の身元や連絡先および利用目的等の情報を提供する。 14 条（間接取得時の情報提供） データ主体から取得したものでない場合、データ主体に管理者の身元や連絡先および利用目的等の情報を提供する。 15 条（アクセス権） データ主体は管理者からアクセスする権利を有する。 16 条（訂正の権利） データ主体は管理者から訂正する権利を有する。 17 条（消去の権利：忘れられる権利） データ主体は管理者から消去する権利を有する。 18 条（取扱制限の権利） データ主体は管理者から取扱制限を得る権利を有する。 19 条（取扱制限の通知義務） 管理者はデータ開示者に対し通知する権利を有する。 20 条（データポータビリティの権利） データ主体は管理者からデータ移行する権利を有する。 21 条（異議を述べる権利） データ主体は管理者に異議を述べる権利を有する。 22 条（プロファイリングされない権利） データ主体は管理者からプロファイリング対象されない権利を有する。 23 条（制限） 国家安全保障/公衆衛生/犯罪捜査/司法手続き等の場合、12 条から 22 条および 34 条に定める権利・義務を制限できる。 24 条（管理者の責任） データ保護の技術上・組織上の措置を実装する。 25 条（データ保護梅デザイン） リスクを考慮したデータ主体の権利を保護する。 26 条（共同管理者） 27 条（EU 内に代理人を置く） 30 条（EU 内と域外利用の活動記録保管） 44 条～46 条　データの EU 域外移転は、移転国ごとに十分性認定が必要

比較対象 比較項目	（現行法）個人情報保護法 （2015改正、2017年施行）	（現行法）GDPR一般データ保護規則 （2016制定、2018年施行）
２４条：外国にある第三者への提供の制限	＜比較＞ ・外国提供の許諾は、公表同意 ・データ移転国は、EEA31 カ各国 ・要配慮情報は、オプトアウト禁止 ・他はオプトイン可能 ＜関連条文＞ 保護委員会：個情法の定める国 保護委員会：個情法の GDPR 補完的ルール 保護委員会告示１号：定める国 保護委員会告示５号；英国 GDPR 保護委員会ガイド：通則編 保護委員会ガイド：外国第提供編 保護委員会ガイド：提供記録義務編 保護委員会ガイド：匿名加工編 保護委員会ガイド：漏洩報告編 保護委員会ガイド：漏洩対応編 H27 年改正法 65 号個人情報保護法 ・本人同意の提供可 ・オプトアウト提供可 ・共同利用の提供可 ・委託・事業継承の提供可	＜比較＞ ・第三者提供の許諾は、主体同意 ・すべて、原則、オプトアウト禁止 ・データ主体は、提供データの移転権 ＜関連条文＞ 13 条（直接取得時の情報提供） データ主体から収集する場合、データ主体に管理者の身元や連絡先および利用目的等の情報を提供する。 14 条（間接取得時の情報提供） データ主体から取得したものでない場合、データ主体に管理者の身元や連絡先および利用目的等の情報を提供する。 15 条（アクセス権） データ主体は管理者からアクセスする権利を有する。 16 条（訂正の権利） データ主体は管理者から訂正する権利を有する。 17 条（消去の権利：忘れられる権利） データ主体は管理者から消去する権利を有する。 18 条（取扱制限の権利） データ主体は管理者から取扱制限を得る権利を有する。 19 条（取扱制限の通知義務） 管理者はデータ開示者に対し通知する権利を有する。 20 条（データポータビリティの権利） データ主体は管理者からデータ移行する権利を有する。 21 条（異議を述べる権利） データ主体は管理者に異議を述べる権利を有する。 22 条（プロファイリングされない権利） データ主体は管理者からプロファイリング対象にされない権利を有する。 23 条（制限） 国家安全保障/公衆衛生/犯罪捜査/司法手続き等の場合、12 条から 22 条および 34 条に定める権利・義務を制限できる。 24 条（管理者の責任） データ保護の技術上・組織上の措置を実装する。 25 条（データ保護梅デザイン） リスクを考慮したデータ主体の権利を保護する。 26 条（共同管理者） 27 条（EU 内に代理人を置く） 30 条（EU 内と域外利用の活動記録保管） 44条～46条　データのEU域外移転は、移転国ごとに十分性認定が必要

第３項 CookieやIPアドレス等

ここでは、CookieやIPアドレス等の識別子を例に比較を行う。

① 個情法2条（定義）について。

2条6において、「個人データ」とは、個人情報データベース等を構成する個人情報をいう。 _

② GDPRにおける定義について

1. 4条「において、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。
2. 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う。

上記の定義の違いから、識別子を個人データとしない2015年改正個人情報保護法と、識別子をも個人データとするGDPRの間で大きな違いがある。ただし、表中の＜参考＞に記載したように、2020年改正個人情報保護法（2022年春までに施行予定）においては、GDPRの定義を踏襲している。

表 24　現行法との比較（個人情報保護法とGDPR）

比較対象 / 比較項目	（現行法）個人情報保護法（2015改正、2017年施行）	（現行法）GDPR一般データ保護規則（2016制定、2018年施行）
識別子等の違い	＜2015 年改正の現行法＞ クッキーや IP アドレスは、それ自体では特定の個人を識別することができず 2 条 1 項 1 号の個人情報には該当しません。ただし、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場合には、2 条 1 項 2 号（個人識別符号が含まれるもの）として個人情報に該当します。 従って現行法では、原則、クッキーや IP アドレスのようなオンライン識別子は、個人情報には該当せず、クッキー利用の第三者提供について、本人の同意は法律上求められていません。 ＜参考＞ 2020 年改正の個人情報保護法（2023 年春までに施行予定で）は、「個人関連情報」が定義され、クッキーや IP アドレスのようなオンライン識別子も、個人情報に該当するようになります。 ＊個人関連情報の定義と例 個人関連情報とは、個人情報、匿名加工情報、仮名加工情報以外の個人に関する情報。 例 a. 個人関連情報データベース等を構成する個人に関する情報 例 b. データベース化されていない、書面・写真・音声等の記録 例 c. 他の情報と照合すれば識別できる、Cookie・IP アドレス等の識別子	＜GDPR4 条 1 項＞ 「個人データ」とは、識別された又は識別され得る個人（「データ主体」）に関するあらゆる情報を意味する。識別され得る個人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、又は当該個人に関する物理的、生理的、遺伝子的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な一つもしくは複数の要素を参照することによって、直接的または間接的に、識別され得るものをいう。 したがって、クッキー（Cookie）やＩＰアドレスなどのオンライン識別子、位置データなども個人データに該当する。 ＜参考＞ EU では、従前から、ePrivacy 指令（Directive on privacy and electronic communications（通称、e-Privacy Directive））５条３項においては、ユーザーの端末装置に蓄積された情報を保管し、また、それらの情報にアクセスするためには、クッキーの利用目的を分かりやすく説明した上で同意を取得すること（インフォームド・コンセント）が必要とされています。すなわち、ウェブサイトにおいて、ほとんど全ての Cookie や類似の技術（例えば、Web ビーコンや Flash Cookie など）を使用する前にユーザーの同意を取得することが必要です。 Cookie 利用の同意手順は、 ① インフォームド・コンセントを必要とする Cookie を使用してウェブサイトの全てのページに Cookie ヘッダーバナーを掲載し、

	例 d. 識別子に紐づいた、位置情報・閲覧履歴・趣味趣向等の情報	② Cookie 通知のページへのウェブリンクにアクセスできるようにし、 ③ Cookie を使用しているページについて、ユーザーが同意した場合のみコンテンツを表示できるようにする。

附則１（考察）

＜EU憲法　by 衆議院憲法調査会事務局訳＞

EU憲法　第I-51条（個人情報保護）

1. あらゆる人は、自らに関する個人情報を保護する権利をもつ。
2. 欧州法律において、連合機関、組織、独立部局および専門機関が行う個人情報の加工ならびに連合法の範囲内に入る活動を構成国が実施するにあたり行う個人情報の加工について個人の保護を行うことに関する準則、ならびに当該情報の自由移動に関する準則を定めるものとする。これらの準則の遵守は、独立の機関の統制に限るものとする。

＜越境操作の主権について考察＞

表 25　越境捜査の主権（立法管轄権、執行管轄権、司法管轄権）一覧

捜査対象 / 主権	データ主体への越境捜査	管理者への越境捜査	処理者への越境捜査
国家の主権（強制）	立法管轄権あり（国際法で強制捜査）	立法管轄権あり（国際法で強制捜査）	立法管轄権あり（国際法で強制捜査）
	執行管轄権あり（国間同意で差押え）	執行管轄権あり（国間同意で差押え）	執行管轄権あり（国間同意で差押え）
情報主体の主権（任意）		司法管轄権あり（裁判所が捜査依頼）	司法管轄権あり（裁判所が捜査依頼）
情報管理者の主権（任意）			司法管轄権あり（裁判所が捜査依頼）
情報処理者の主権（協力）			

※管轄権の留意点

1. 立法管轄権　国内立法に関する権限
2. 執行管轄権　行政が逮捕・差押をする権限
3. 司法管轄権　裁判所が事件を審理する権限

・多くの国は上記３つの管轄権を有し越境捜査を主張するが、「例えば、中国へ逃げた犯罪者を警視庁が中国内で直接逮捕できず、犯人引渡しを求めるのが現状」である。

・米国クラウド法は、「①米国内プロバイダーに対して米国外のデータ提出を要求できる。②米国外プロバイダーに対して米国外のデータ提出を要求できる」としている。

※国際法　サイバー犯罪条約：日米欧など63ケ国署名

EU著作権法＋EUデジタル指令（リンク税、アップロード条項）

＜個人データの域外適用について考察＞

表 26　個人データの域外適用（日本、EU、米国）一覧

比較国 / 適用項目	日本 個人情報保護法	EU GDPR規則	米国 FTC法
域外適用	（第75条） 国内にある者に対する物品又は役務の提供に関連してその者を本人	（第３条） 1. EU域内の管理者または処理者の拠点の活動	（15 U.S.C. §45(a)(4).） 「不公正または欺瞞的な 行為または慣行」に

	とする個人情報を取得した個人情報取扱事業者が、外国において当該個人情報又は当該個人情報を用いて作成した匿名加工情報を取り扱う場合についても、適用する （対象規定） ・ 個人情報取扱事業者の義務規定 ・ 委員会の権限等（第40条：報告及び立入検査、第42条2-3項の命令を覗く）	の過程における個人データの取扱い 2. EU 域内に拠点のない管理者または処理者による EU 域内のデー タ主体の個人データの取扱い: （a）EU 域内のデータ主体 に対する物品またはサー ビスの提供 （b）EU 域内で行われる行動の監視	は、 海外の商業活動で米国内 合理的に予測しうる範囲 の損害を米国内に生じる か、米国内に物理的影響 を及ぼすものも含む

※域外適用の留意点

1. 日本が執行管轄権を行使する際、他国の主権を侵害の恐れ
2. 日本が海外保有データを捜査する際、人権侵害となる恐れ
3. 日本が国外で公権力を行使する際、臆病なほど慎重な姿勢を取る恐れ

第５章　個人情報に関する本人の権利と事業者の対応（第27条、第28条、第29条、第30条、第31条、第32条、第33条、第34条、第35条）

第１節 開示等の請求への対応

第１項 本人の権利

個人情報に関する本人の権利に対する法の定めを整理しておく。例外規定は省く。

個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止（以下、開示等）を行うことのできる権限を有する個人データのことを、「保有個人データ」と呼ぶ[第2条7]。個人情報取扱事業者は，保有個人データに関して，本人から開示等の請求等を受け付けた場合は，法の規定によって，遅滞なくこれに応じなければならないとされている。

表 27　個人情報に関する本人の権利一覧（抜粋）

項目　[該当条文]	本人からの求めまたは請求	事業者の対応
利用目的の通知　[第 27 条]	当該本人が識別される保有個人データの利用目的の通知	遅滞なく、これを通知しなければならない。
開示　[第 28 条]	当該本人が識別される保有個人データの開示	本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない

項目 ［該当条文］	本人からの求めまたは請求	事業者の対応
内容の訂正、追加または削除 ［第 29 条］	保有個人データの内容が事実でないとき	利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。ただし、利用目的からみて訂正等が必要ではない場合、保有個人データが誤りである旨の指摘が正しくない場合には、訂正等を行う必要はない。［ガイドライン］[38]
利用の停止、消去 ［第 30 条］	当該本人が識別される保有個人データが第 16 条（利用目的による制限）の規定に違反して取り扱われているとき又は第 17 条（適正な取得）の規定に違反して取得されたものであるとき	その請求に理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない
第三者への提供の停止 ［第 30 条］	当該本人が識別される保有個人データが第 23 条（第三者提供の制限）第 1 項又は第 24 条（外国にある第三者への提供の制限）の規定に違反して第三者に提供されているときは、当該保有個人データの第三者への提供の停止を請求することができる。	その請求に理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。
理由の説明 ［第 31 条］	ー	本人から求められ、又は請求された措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。
開示等の請求等に応じる手続 ［第 32 条］ ／手数料 ［第 33 条］	事業者が指定する方法に従って、開示等の請求等を行わなければならない。	開示等の請求に関し、その求め又は請求を受け付ける方法を定めることができるとしている。本人に過重な負担を課するものとならないよう配慮しなければならない。利用目的の通知を求められたとき又は開示の請求を受けたときは、手数料を徴収することができる。

法令順守のため、個人情報取扱事業者は何をしなければならないか。

ガイドラインには、「消去」とは、保有個人データを保有個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含むとあり（**第１章第２節（3）データの消去参照**）、保有個人データの全部消去を求められた場合であっても、利用停止によって手続違反を是正できる場合であれば、そのような措置を講ずることにより、義務を果たしたことになり、必ずしも、求められた措置をそのまま実施する必要はない。な

[38] 個人情報保護委員会（平成 28 年 11 月）（平成 31 年 1 月一部改正）「個人情報の保護に関する法律についてのガイドライン（通則編）」3-5-3（p. 66）

お、手続違反である旨の指摘が正しくない場合は、利用停止等を行う必要はない。手続違反である旨の指摘が正しくない場合は、第三者提供を停止する必要はない。一方、**「個人情報保護マネジメントシステム－要求事項」**（JIS Q 15001：2017）には、消費者等、本人の権利利益保護の観点からは、事業活動の特性、規模及び実態を考慮して、保有個人データについて本人から求めがあった場合には、ダイレクトメールの発送停止等、自主的に利用停止に応じる等、本人からの求めにより一層対応していくことが望ましいと記述されている。[39]　どこまでの対応を行うべきか判断に迷うところではあるが、法令は最低限の順守事項を規定しているのであって、本人の権利を尊重する姿勢で臨むべきであろう。（法定保存期間については第1章参照）

なお、2022年4月施行予定の改正法では、利用停止・消去等の個人の請求権について、不正取得等の一部の法違反の場合に加えて、「改正法第30条-5　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には、当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる。」となっており、本人の権利が拡大される方向である。

2022年４月１日施行予定の新ガイドライン[40]では、

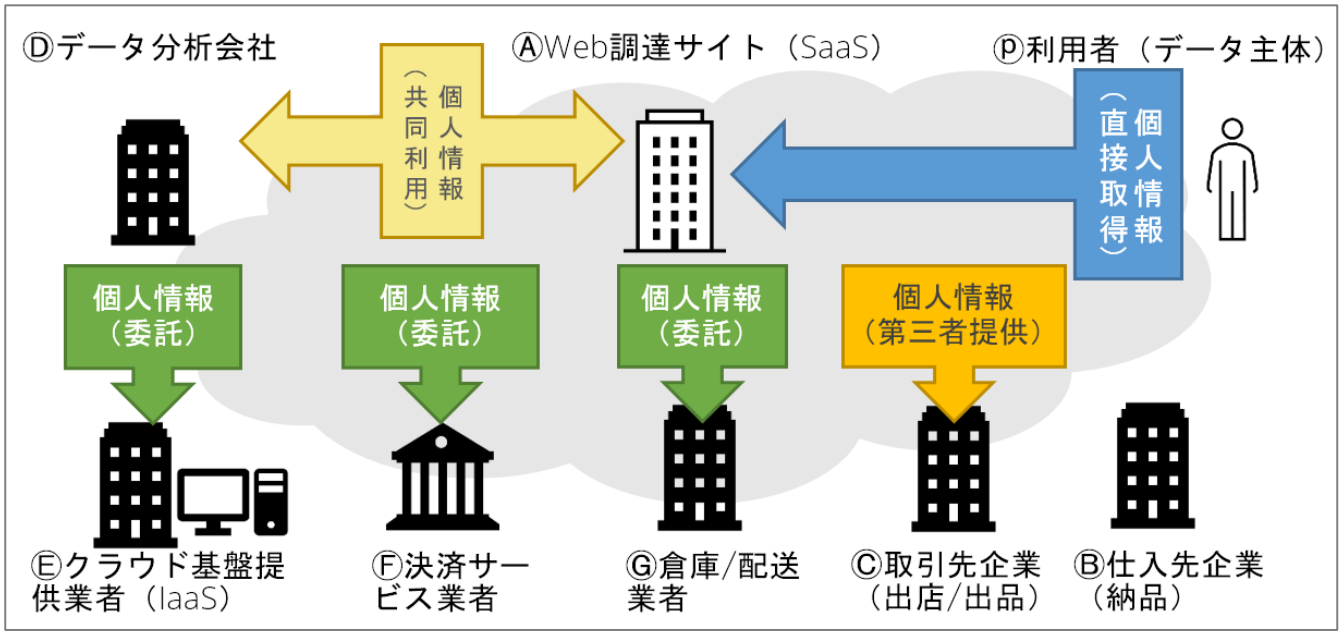
> **「本人の権利又は正当な利益が害されるおそれがある場合」とは、法目的に照らして保護に値する正当な利益が存在し、それが侵害されるおそれがある場合をいう。個人情報取扱事業者に本人の権利利益の保護の必要性を上回る特別な事情がない限りは、個人情報取扱事業者は請求に応じる必要がある。**

と記されており、本人の権利又は正当な利益が害されるおそれがあるとして利用停止等又は第三者提供の停止が認められると考えられる事例としては、以下の例示がある。

事例1）ダイレクトメールの送付を受けた本人が、送付の停止を求める意思を表示したにもかかわらず、個人情報取扱事業者がダイレクトメールを繰り返し送付していることから、本人が利用停止等を請求する場合

第２項 参照モデルでの対応例

（再掲）図１　Web調達サイト（法人向けECサイト）のモデル



[39] 「個人情報保護マネジメントシステム－要求事項」（JIS Q 15001：2017）［B.3.4.4.7 保有個人データの利用又は提供の拒否権］

[40] 個人情報保護委員会の「法令・ガイドライン等」（https://www.ppc.go.jp/personalinfo/legal/）で公開されている（2021/11/05 時点）

Web調達サイト（Ⓐ）は、利用者（Ⓟ）の個人情報をIDと紐付けて管理することが一般的であり、利用者（Ⓟ）はIDとパスワードで認証してさまざまなサービスを受けることになる。このようなサイトでは利用者（Ⓟ）に対してマイページを提供することが一般的になっている。マイページ等の中で開示等の対応を機能として提供、ないし問い合わせ可能とすることが望ましい。

尚、本人の権利とは直接関連が無いが、ID管理の観点で、ユーザアクセス認可/取り消し等の管理策をCCMから抽出した。参考までに以下に記載する。

- Web調達サイト（Ⓐ）は、個人データを分類し、そのデータセキュリティライフサイクル[41]（取得・生成、保存、利用、共有、アーカイブ、廃棄）に沿ってデータのデータフロー（役割、権限）を作成し、文書化し、維持しなければならない。そのことにより、法令・法規制またはサプライチェーン契約(SLA)の順守に関する影響を確認し、データにひも付くその他の全てのビジネスリスクを把握しなければならない。クラウド基盤提供業者（Ⓔ）はWeb調達サイト（Ⓐ）に対し、要求に応じて、法令・規則の順守に関する影響とリスクについて、情報提供しなければならない。【DSI-02　データの管理表とフロー】
- 利用者（Ⓟ）がWeb調達サイト（Ⓐ）利用に当たり、利用者登録を行う。その登録に当たり、データ等へのユーザアクセスの設定（たとえば、利用者（Ⓟ）は、自身のデータのみアクセス可とする等）は、Web調達サイト（Ⓐ）の管理者によって認可され、定められたポリシーや手順に従って適切に制限されなければならない。【IAM-09　ユーザアクセス認可】
- 利用者（Ⓟ）のステータスの変更依頼に対応して、定められたポリシー及び手順に従い、データ等へのユーザアクセス権限の取り消し（解除または変更）を適時に行わなければならない。**マイページを用意するなどして**Web上で利用者（Ⓟ）が自ら行う場合でも、Web調達サイト（Ⓐ）の管理者が承認するプロセスを組み込むことが望ましい。また、取引先企業（出店/出品）（Ⓒ）や決済サービス業者（Ⓕ）がその管理の実施に対する責任の一部を共有したりしている場合は、Web調達サイト（Ⓐ）はこれらの変更をその企業（ⒸⒻ）に通知しなければならない。【IAM-11　ユーザアクセス取り消し】[42]
- 適切な本人確認、権限付与、アクセス管理を確実に実施するため、定められたポリシー及び手順に従って、ユーザアカウントの資格情報の作成から破棄に至るまでのライフサイクル管理を行うとともに、IDの再利用は行わない方が望ましい。【IAM-12　ユーザID資格情報】
- また、開示等の請求は、クラウド基盤提供業者（Ⓔ）がWeb調達サイト（Ⓐ）から受託するケースが多いと思われるため、Web調達サイト（Ⓐ）とクラウド基盤提供業者（Ⓔ）間で、そのサービス範囲やシステム、役割および責任などに関して双方で合意する必要がある。
- クラウド基盤提供業者（Ⓔ）とWeb調達サイト（Ⓐ）とのサプライチェーン契約書（例えばSLAなど）には、少なくとも、取引関係及び提供されるサービスの範囲について相互に合意した条項/条件を規定しなければならない。開示等の請求に対する対応手順についても、相互に取り決めておくべきである。委託先の管理は委託元にある【法22条】ことを念頭に、実現可能な方法で取り決めをしておくこと。【STA-05　サプライチェーンの合意】

第２節　苦情及び相談への対応

第１項　苦情及び相談

[41] CSA ガイダンス V4.0（DOMAIN 5 情報ガバナンス）データセキュリティライフサイクルは、データセキュリティを大ぐくりのレベルで評価し、焦点を当てるべきポイントを発見することを支援するモデリングツールである。
[42] 例示の Web 調達サイトでは、開示、内容の訂正、追加又は削除、利用の停止、消去は、Web 上で加入者（Ⓟ）が自ら行えるようになっているケースも多い。第三者への提供の停止は、サービスの利用条件になっているケースでは、個別の設定は難しいと思われる。

法[第27条～33条]で規定されている利用停止などを事業者へ請求しても解決できない場合は、苦情、訴訟という手段に訴えることが可能である。事業者は、苦情処理に必要な体制の整備に努めるとともに、苦情を受けた場合には適切かつ迅速な処理に努めなければならない。[第34条][第35条]

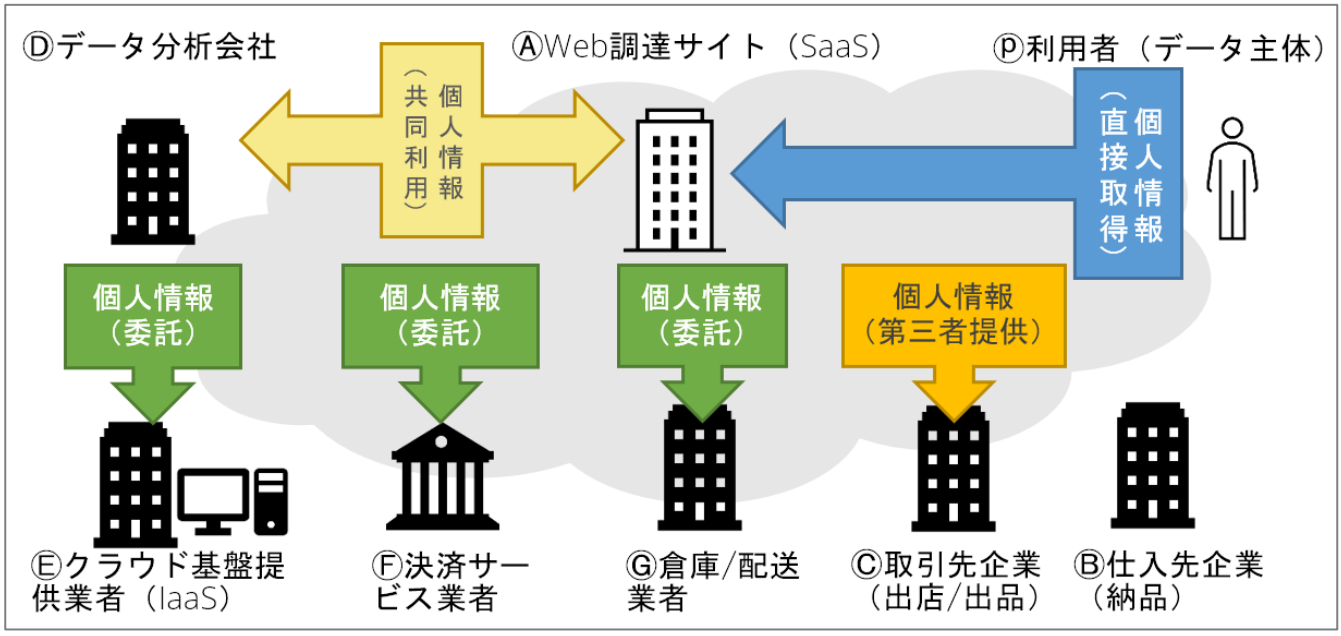
表 28　苦情および相談への対応に関する法の規制（抜粋）

項目　［該当条文］	本人からの請求に係る訴え	事業者の対応
事前の請求 ［第 34 条］	自己が識別される保有個人データの開示、訂正等又は利用停止等若しくは第三者提供の停止の個人情報取扱事業者に対する請求について裁判上の訴えを提起しようとするときは、あらかじめ裁判外において、その訴えの被告となるべき者に対し、あらかじめ、当該請求を行い、かつ、その到達した日から２週間を経過した後でなければ、その訴えを提起することができない。	―
個人情報取扱事業者による苦情の処理 ［第 35 条］		個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。 個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

法令順守のため、個人情報取扱事業者は何をしなければならないか。

第２項 参照モデルでの対応例

（再掲）図 1　Web調達サイト（法人向けECサイト）のモデル



苦情等は、利用者（Ⓟ）からWeb調達サイト（Ⓐ）への訴えとして受け付けられる。訴えの内容によっては、委託先等（ⒺⒻⒼ等）への対応が必要となることも想定される。必要な体制には、委託先等を含めた体制をあらかじめ検討し、委託契約等で規定し、運用手順化しておく必要がある。

「個人情報保護マネジメントシステム－要求事項」（JIS Q 15001：2017）の「B.3.6 苦情及び相談への対応」には、“必要な体制の整備”とは，例えば，常設の対応窓口の設置又は担当者を任命することなどをいう。ただし，個人情報保護管理者とは兼任をしても差し支えない。

本人から自分の個人情報の取得元の開示を請求された場合には、個人情報保護法上、本人に個人情報の取得元を明らかにすることを義務付ける規定はない。ただし、個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならないとされており（法第 35 条第１項）、開示請求というよりは苦情と受け止めて、まずは苦情相談窓口等において相談に対応することが望ましい。[43]

第６章　匿名加工情報個人情報に関する本人の権利と事業者の対応（第36条、第37条、第38条）

第１節 匿名加工情報に係る規程内容の概要

個人情報保護法では、「個人情報の有用性」と「個人の権利利益の保護」のバランスを図ることを目指しているが、ここでは「個人情報の有用性」を推進するための方策として導入された概念である「匿名加工情報」を対象として、係る法的要件とその対応方法を記載する。

「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、復元できないようにしたもの」である。また、匿名加工情報は、一定のルールのもとで、第三者提供や目的外利用の同意を得ることなく利用が可能な情報である。

個人情報保護法では、匿名加工情報に関連して、以下の5項目の内容を規定している。[44]

1. 匿名加工情報の作成のための適正な加工（36条1項 - 規則19条）
2. 匿名加工情報に係る安全管理措置（36条2項, 6項, 39条 - 規則20条, 21条）
3. 作成時の公表（36条3項）
4. 匿名加工情報の第三者提供（36条4項, 37条 - 規則22条, 23条）
5. 識別行為の禁止（36条5項, 38条）

上記条文で対象としている既定は、個人情報取扱事業者（作成者）と匿名加工情報取扱事業者（受領者）についての法的要件を記載したものである。（「図x.1　匿名加工情報の作成者・受領者が遵守すべき規定」参照）

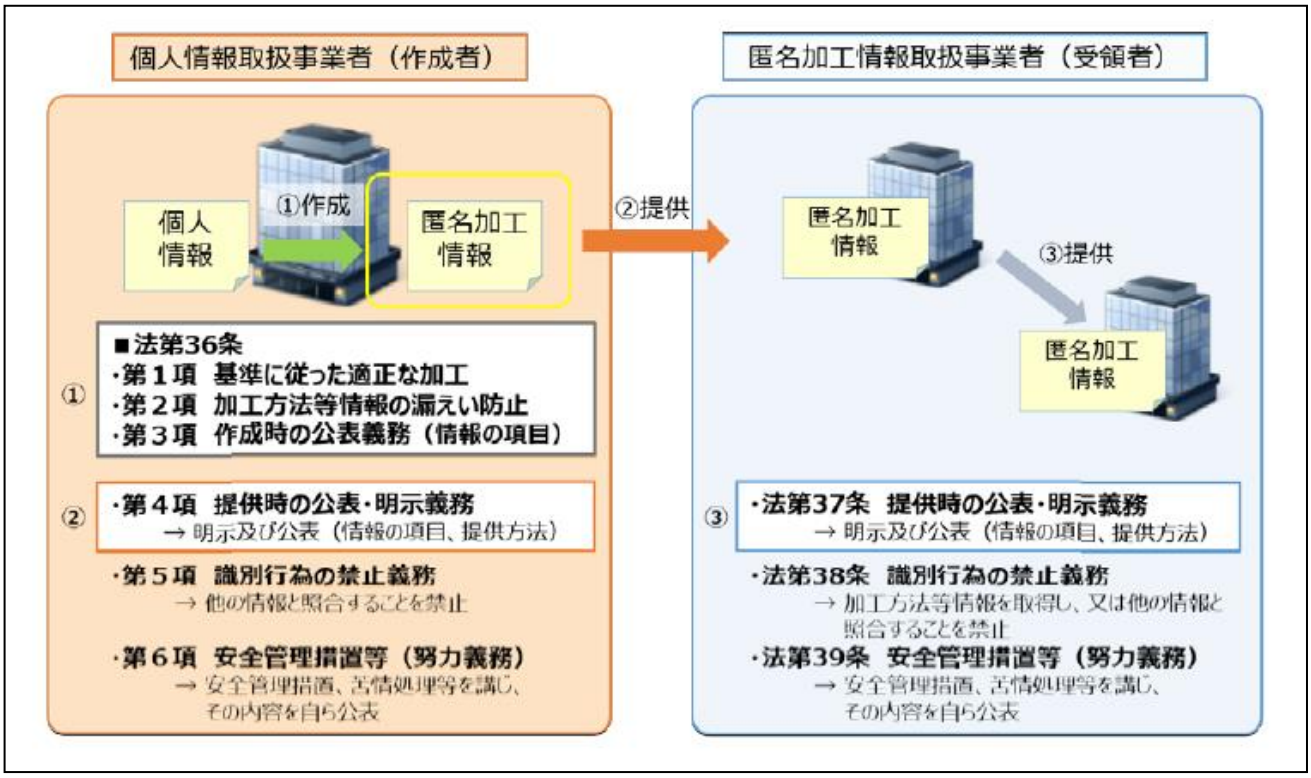
また、今回取り上げた条文では、「個人情報保護委員会規則で定める基準に従い、・・」といった表現でしばしば個人情報保護員会の定める規則[45]が参照されており、当ガイドでは、あわせてこちらからも引用している。（以下、規則という。）

[43] 個人情報保護委員会（平成 29 年２月 16 日）（令和元年 11 月 12 日更新）「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A　Q6-8（p. 44）

[44] 「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）（2016/11 月）（2017 年 3 月一部改正）」

[45] 「個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号）

図６　匿名加工情報の作成者・受領者が遵守すべき規定[46]



第２節　匿名加工情報に係る具体的な行動規範とそのポイント

ここからは、上記の各条文について、各組織で対応を検討する上での具体的な行動規範やそのポイントについて記載する。

第１項　匿名加工情報の作成のための適正な加工（36条1項 － 規則19条）

個人情報取扱事業者は、匿名加工情報を作成するときは、特定の個人を識別できないように、かつ、その作成に用いる個人情報を復元できないようにするために、規則第19条各号に定める基準に従って、当該個人情報を加工しなければならないとされている。

表 29　匿名加工情報の作成のための適正な加工（抜粋）

項目　［該当条文］	事業者の対応	ガイドライン（補足）
匿名加工情報の適正な加工［36 条 1 項］	個人情報取扱事業者は、匿名加工情報を作成するとき、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするため、以下に挙げる個人情報保護委員会規則で定める基準（規則第 19 条の各号）に従い加工しなければならない。 1. 特定の個人を識別することができる記述等の削除 2. 個人識別符号の削除 3. 情報を相互に連結する符号の削除	1. 特定の個人を識別することができる記述等の削除 事例）氏名、住所、生年月日が含まれる個人情報を、以下のように加工する 1）氏名を削除する 2）住所を削除、又は、〇〇県△△市に置き換える 3）生年月日を削除。又は、生年月に置き換える 2. 個人識別符号の削除 政令で定める以下のもの （1）生体情報（DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋）のデジタルデータで特定の個人を識別できるもの

[46] 「個人情報保護委員会事務局レポート　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて（2017 年 2 月）」

	4. 特異な記述等の削除 5. 個人情報データベース等の性質を踏まえたその他の措置	（2）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、各種保険証の番号等の公的機関が割り振る番号 3. 情報を相互に連結する符号の削除 事例）サービス会員の情報について、氏名等の基本的な情報と購買履歴を分散管理し、それらを管理用 ID を付すことにより連結している場合、その管理用 ID を削除する。 4. 特異な記述等の削除 事例 1）症例数の極めて少ない病歴を削除する。 事例 2）年齢が「116 歳」という情報を「90 歳以上」に置き換える。 5. 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 特定の個人の識別ができないようにするための匿名加工の手法 -項目削除、一般化、トップコーディング等 （別表参照）

下表には、先に挙げた事例に出てくる主な匿名加工の手法についてサマリーした。[47]

表 30 匿名加工の主な手法

手法名	解説
項目削除／レコード削除／セル削除	加工対象となる個人情報データベース等に含まれる個人情報の記述等を削除する。 例えば、年齢のデータを全ての個人情報から削除すること（項目削除）、特定の個人の情報を全て削除すること（レコード削除）、又は特定の個人の年齢のデータを削除すること（セル削除）。
一般化	加工対象となる情報に含まれる記述等について、上位概念若しくは数値に置き換えること又は数値を四捨五入などして丸めることとする。 例えば、購買履歴のデータで「きゅうり」を「野菜」に置き換えること。
トップ（ボトム）コーディング	加工対象となる個人情報データベース等に含まれる数値に対して、特に大きい又は小さい数値をまとめることとする。 例えば、年齢に関するデータで、80 歳以上の数値データを「80 歳以上」というデータにまとめること。
ミクロアグリゲーション	加工対象となる個人情報データベース等を構成する個人情報をグループ化した後、グループの代表的な記述等に置き換えることとするもの。
データ交換（スワップ）	加工対象となる個人情報データベース等を構成する個人情報相互に含まれる記述等を（確率的に）入れ替えることとするもの。
ノイズ（誤差）付加	一定の分布に従った乱数的な数値を付加することにより、他の任意の数値へと置き換えることとするもの。
疑似データ生成	人工的な合成データを作成し、これを加工対象となる個人情報データベース等に含ませることとする。

（※）匿名加工情報の作成に当たっての一般的な加工手法を例示したものであり、その他の手法を用いて適切に加工することを妨げるものではない。

[47] 個人情報保護委員会事務局、匿名加工情報の加工基準について https://www.soumu.go.jp/main_content/000462276.pdf

一般に、データを匿名化する際の処理の流れは、以下のようになる。[48]

① 利用用途の定義

② 対象データセットの選定

③ 対象データセットにおける識別子、準識別子、機密属性の定義

④ データセットの加工

⑤ （参考）ツールによる評価

上記処理の補足として、⑤の具体的なツールは、参考文献 [4]では、オープンソースのARX（https://arx.deidentifier.org/）といった匿名加工ツールを用いるとされているが、ARXは、主に研究者・技術者向けに用いられており、実務者が使うには一般的ではない。

また、匿名加工情報ツールは、**表** 31の加工手法への対応の他、各ツール独自の機能や活用支援サービスと共に、いくつかの会社から提供されている。

各社からは、匿名加工情報ツールの機能の一部として、各種支援サービス（AIによる支援サービスや適切な活用に向けた支援サービスなど）などが行われているが、各事業者にとっては、匿名加工情報のスキル育成も重要な課題である。一般財団法人日本情報経済社会推進協会（JIPDEC）では、認定個人情報保護団体対象事業者を対象とした匿名加工情報の取り扱いに関する支援も行われており、今後、このような支援やガイドラインによるスキル育成の進展も期待される。

第２項 匿名加工情報に係る安全管理措置（36条2項，6項，39条 － 規則20条，21条）

ここでは、匿名加工情報に係る安全管理措置として、2.1 加工情報等情報の安全管理措置と2.2 匿名加工情報の安全管理措置について記載されている。

1 加工情報等情報の安全管理措置

個人情報取扱事業者は、匿名加工情報を作成したときは、加工方法等情報の漏えいを防止するために、規則で定める基準に従い、必要な措置を講じなければならない。

当該措置の内容は、対象となる加工方法等情報が漏えいした場合における復元リスクの大きさを考慮し、当該加工方法等情報の量、性質等に応じた内容としなければならないが、具体的に講じなければならない項目及び具体例について、以下を参照いただきたい。

表 32　加工情報等情報の安全管理措置（抜粋）

項目　[該当条文]	事業者の対応	ガイドライン（補足）
加工方法等情報の安全管理措置 [法第 36 条（第 2 項）]	個人情報取扱事業者は、匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報の漏えいを防止するため、以下に挙げる個人情報保護委員会規則で定める基準（規則第 20 条の各号）に従い加工しなければならない。 1. 加工情報を取り扱う者の権限及び責任の明確化	1. 加工情報を取り扱う者の権限及び責任の明確化 具体例） ・加工方法等情報の安全管理措置を講ずるための組織体制の整備 2. 加工方法等情報の取扱いに関する規程類の整備等 具体例） ・加工方法等情報の取扱いに係る規程等の整備とこれに従った運用 ・従業員の教育 ・加工方法等情報の取扱状況を確認する手段の整備

[48] （引用）ラクスエンジニアリングブログ、実際の匿名化：データ匿名化 第 6 回、2019 年 9 月、https://tech-blog.rakus.co.jp/entry/20190930/kamisen

	2. 加工方法等情報の取扱いに関する規程類の整備等 3. 加工方法等情報を取り扱う正当な権限を有しない者による取扱いを防止するために必要かつ適切な措置	・加工方法等情報の取扱状況の把握、安全管理措置の評価、見直し及び改善 3. 加工方法等情報を取り扱う正当な権限を有しない者による取扱いを防止するために必要かつ適切な措置 具体例） ・加工方法等情報を取り扱う権限を有しない者による閲覧等の防止 ・機器、電子媒体等の盗難等の防止 ・電子媒体等を持ち運ぶ場合の漏えい等の防止 ・加工方法等情報の削除並びに機器、電子媒体等の廃棄 ・加工方法等情報へのアクセス制御 ・加工方法等情報へのアクセス者の識別と認証 ・外部からの不正アクセス等の防止 ・情報システムの使用に伴う加工方法等情報の漏えい等の防止

2 匿名加工情報の安全管理措置

個人情報取扱事業者又は匿名加工情報取扱事業者は、匿名加工情報の安全管理措置、苦情処理等の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。法第36条（第6項）では個人情報取扱事業者の法第39条では匿名加工情報取扱事業者の安全管理措置について記載している。

表 33　匿名加工情報の安全管理措置（抜粋）

項目　[該当条文]	事業者の対応	ガイドライン（補足）
匿名加工情報の安全管理措置等 [法第 36 条（第 6 項）]	個人情報取扱事業者は、匿名加工情報の安全管理や適正な取扱いを確保するために必要な措置（苦情の処理等）等を自ら講じ、かつ、その内容を公表するよう努めなければならない。	当該安全管理等の措置については、個人情報と同様の取扱いを求めるものではないが、事業の性質、匿名加工情報の取扱状況、取り扱う匿名加工情報の性質、量等に応じて、合理的かつ適切な措置を講ずることが望ましい。
匿名加工情報の安全管理措置等 [法第 39 条]	匿名加工情報取扱事業者は、匿名加工情報の安全管理や適正な取扱いを確保するために必要な措置（苦情の処理等）等を自ら講じ、かつ、その内容を公表するよう努めなければならない。	匿名加工情報には識別行為の禁止義務が課されていることから、匿名加工情報を取り扱う者が不適正な取扱いをすることがないよう、その情報が匿名加工情報である旨が一見して明らかな状態にしておくことが望ましい。

なお、安全管理措置の詳細については、個人情報保護全般について記載された以下の各条を参照頂きたい。

法第20条　：安全管理措置
法第21条　：従業者の監督
法第22条　：委託先の監督
法第35条　：個人情報の取扱いに関する苦情処理について

第３項 作成時の公表（36条３項）

表 34　匿名加工情報作成時の公表（抜粋）

項目　[該当条文]	事業者の対応	ガイドライン（補足）
匿名加工情報の作成時の公表 [法第 36 条（第 3 項）]	個人情報取扱事業者は、匿名加工情報を作成したときは、個人情報保護委員会規則（規則第 21 条）で定めるところにより、当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならない。 1　匿名加工情報を作成した後、遅滞なく、インターネットの利用その他の適切な方法により行う。 2 個人情報取扱事業者（A）が他の個人情報取扱事業者（B）の委託を受けて匿名加工情報を作成した場合は、（B）が公表する。また、当該公表により（A）が当該項目を公表したものとみなす。	【個人に関する情報の項目の事例】 事例）「氏名・性別・生年月日・購買履歴」のうち、氏名を削除した上で、生年月日の一般化、購買履歴から特異値等を削除する等加工して、「性別・生年・購買履歴」に関する匿名加工情報として作成した場合の公表項目は、「性別」、「生年」、「購買履歴」である。 「公表」とは、広く一般に自己の意思を知らせること（不特定多数の人々が知ることができるように発表すること）をいう。 また、ここでの「遅滞なく」とは、直後でなくても認められることを意味する。ただし、少なくともその利用又は第三者提供の前に、作成したことを一般に十分に知らせるに足る期間を確保しなければならない。許容される具体的な期間は、業種及びビジネスの態様によっても異なり得るため、個別具体的に判断する必要がある。

なお、公表に係る考慮点等の詳細については、個人情報保護全般について記載された以下を参照頂きたい。

法第18条　：取得に際しての利用目的の通知等

第４項　匿名加工情報の第三者提供（36条4項，37条 － 規則22条，23条）

個人情報取扱事業者又は匿名加工情報取扱事業者は、匿名加工情報を第三者に提供するときは（匿名加工情報をインターネット等で公開する場合も）、提供に当たりあらかじめ、インターネット等を利用し、匿名加工情報に含まれる個人に関する情報の項目や匿名加工情報の提供方法を公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を電子メール又は書面等により明示しなければならない。

また、上記の項目や加工方法が同じである匿名加工情報を復・継続的に第三者へ同じ方法により提供する場合には、最初に匿名加工情報を第三者提供するときに個人に関する項目を公表する際に、提供期間や又は継続的に提供されることとなる旨を明らかにしておくことにより、その後の公表は先の公表により行われたものと解される。

なお、法第36条（第4項）は個人情報取扱事業者（作成者）に、法第37条は匿名加工情報取扱事業者（受領者）についての法的要件を記載したものである。

表 35　匿名加工情報の第三者提供（抜粋）

項目　[該当条文]	事業者の対応	ガイドライン（補足）
匿名加工情報の第三者提供 [法第 36 条（第 4 項）]	個人情報取扱事業者が、当該匿名加工情報を第三者に提供するときは、以下の対応が必要。 1. あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。 ※公表は、インターネットの利用等により行う。 2. 当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。 ※明示は、電子メール送信、書面交付等により行う。	（1）第三者に提供する匿名加工情報に含まれる個人に関する情報の項目 事例）「氏名・性別・生年月日・購買履歴」のうち、氏名を削除した上で、生年月日の一般化、購買履歴から特異値等を削除する等加工して、「性別・生年・購買履歴」に関する匿名加工情報として作成して第三者提供する場合の公表項目は、「性別」、「生年」、「購買履歴」である。 （2）匿名加工情報の提供の方法 事例 1）ハードコピーを郵送 事例 2）第三者が匿名加工情報を利用できるようサーバにアップロード
匿名加工情報の第三者提供 [法第 37 条]	匿名加工情報取扱事業者が、他者が作成した匿名加工情報を第三者に提供するときにも、上記、法第 36 条（第 4 項）で定められた個人情報取扱事業者と同様の対応が求められる。	

第５項　識別行為の禁止（36条5項，38条）

匿名加工情報を取り扱う場合には、当該匿名加工情報の作成の元となった個人情報の本人を識別する目的で、他の情報と照合したり加工方法等情報を取得してはならない

表 36　識別行為の禁止（抜粋）

項目　[該当条文]	事業者の対応	ガイドライン（補足）
識別行為の禁止 [法第 36 条（第 6 項）]	個人情報取扱事業者は、個人情報に係る本人を識別するために、当該匿名加工情報を他の情報と照合してはならない。	【識別行為に当たらない取扱いの事例】 事例 1）複数の匿名加工情報を組み合わせて統計情報を作成すること。 事例 2）匿名加工情報を個人と関係のない情報（例：気象情報、交通情報、金融商品等の取引高）とともに傾向を統計的に分析すること。 【識別行為に当たる取扱いの事例】 事例 1）保有する個人情報と匿名加工情報について、共通する記述等を選別してこれらを照合すること。 事例 2）自ら作成した匿名加工情報を、当該匿名加工情報の作成の元となった個人情報と照合すること。
識別行為の禁止 [法第 38 条]	匿名加工情報取扱事業者は、個人情報に係る本人を識別するために、 当該個人情報から削除された記述や加工の方法に関する情報を取得したり、当該匿名加工情報を他の情報と照合したりしてはならない。	

第３節 まとめ

ここまで、現状の匿名加工情報に係る法的要件とその対応方法を記載してきたが、最後に2022年4月施行予定の改正法検討の中で挙げられた、データ利活用に関する施策の在り方について追記する。

匿名加工情報については、既に一定程度の活用が進みつつあるものの、「利用方法が分からない」、「自社データへのニーズがあるのか分からない」、「分析するための人材がいない」等の意見がみられ、したがって、委員会として、具体的な利活用モデルやベストプラクティス等の発信を進めていくことが重要との認識になっている。[49]

また、2022年4月施行予定の改正法では、イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和することとなった。

当項のまとめとして、以下に個人情報保護法に関連して定義されている、他の情報との比較表を記載する。これらの情報の違いを理解し、適材適所に活用することで、さらなる個人情報の活用を推進し、個人情報保護法が目指している、「個人情報の有用性」と「個人の権利利益の保護」のバランスを図り、個人情報保護と情報活用の両立を目指すことが肝要である。

また、一部の情報を削除あるいは分割する等の加工をする場合または個人情報から統計情報を作成する場合は、リスクを考慮して取り扱うことも忘れてはならない。

当項の記載が、新事業や新サービスの創出、国民生活の利便性の向上に向けた個人情報の有効活用の一助となれば幸いである。

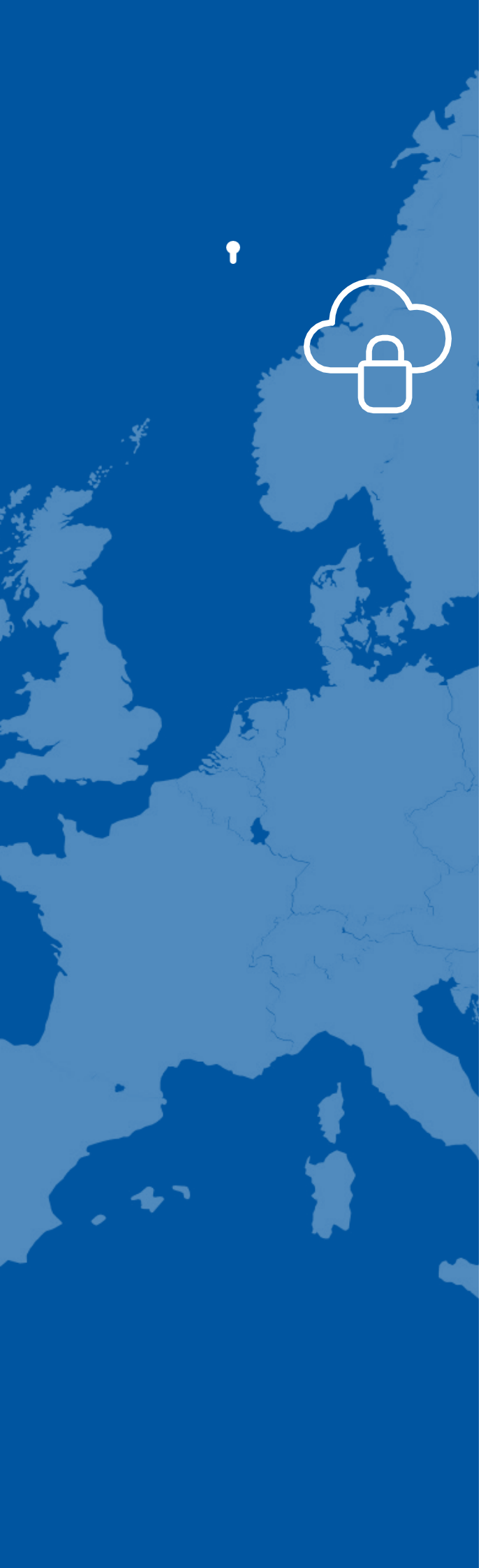
[49] 「個人情報保護法いわゆる 3 年ごと見直し制度改正大綱（2019 年 12 月 13 日）」 p21 他

表 37　個人情報関連情報の比較

	情報の定義	取り扱い	使い方
個人情報	生存する個人に関する情報であって、特定の個人を識別できるもの	個人情報の取得に際しては、利用目的を特定し、本人の同意を得る等の対応が必要[50]	以下の事例にように、利用目的を具体的に特定する必要がある 事例）〇〇事業における商品発送、関連するアフターサービス、新商品に関する情報のお知らせのため[51]
仮名加工情報	（2022 年 4 月施行予定の改正法により新設） 氏名等特定の個人を直接識別できる記述を置き換える又は削除する等、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に加工された個人に関する情報加	本人を識別する利用を伴わない、事業者内部における分析に限定するための一定の行為規制や、「仮名加工情報」に係る利用目的の特定・公表を前提に、個人の各種請求（開示・訂正等、利用停止等の請求）への対応義務を緩和し、また、様々な分析での活用が可能	匿名加工した情報では取り扱えなかった特異なデータや記述等をそのまま参照・活用できるため、匿名加工情報よりも加工が容易で、かつより実践的な分析等が可能となる。また、「関連性」を超えて、利用目的を変更することができる。 そのため、既に取得済みの個人情報（例えば、保険契約のデータ等）を AI を利用して分析する等の用途が想定できる
匿名加工情報	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、復元できないようにしたもの	本人の同意を得ることなく目的外利用及び第三者提供を可能とすることにより、事業者間におけるデータ取引・連携を含むパーソナルデータ利活用を促進	新事業や新サービスの創出、ひいては、国民生活の利便性の向上が期待される以下のような事例 ①ポイントカードの購買履歴や交通系 IC カードの乗降履歴等を複数事業者間で分野横断的に利活用することにより、新たなサービスやイノベーションを生み出す可能性 ②医療機関が保有する医療情報を活用した創薬・臨床分野の発展や、カーナビ等から収集される走行位置履歴等のプローブ情報を活用したより精緻な渋滞予測等
統計情報	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	統計情報の作成において、ある項目の値を所定範囲ごとに区切る場合、個人との対応関係が十分に排斥できるような形で統計化されていることが重要	集団の傾向又は性質などを数量的に把握

[50] 「個人情報保護委員会事務局レポート　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて（2017 年 2 月）」 p7 他

[51] 「個人情報の保護に関する法律についてのガイドライン（通則編）（平成 28 年 11 月）（平成 31 年 1 月一部改正）」　p26 他



付録

2020年12月13日　R2改正個人情報保護法に係る保護委員会施行規則、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補完的ルール（通称：GDPR補完的ルール）

保護委員会は、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して、国内の個人情報保護法令及びガイドラインに加えて、最低限遵守すべき規律として「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補完的ルール（通称：GDPR補完的ルールという）」を策定した。これにより両国間で移転される個人データの取扱事業者を拘束し、かつ法的拘束力を有し、個人情報保護委員会の執行対象とした。

補完的ルール①：特別な種類の個人データは要配慮個人情報とする

GDPR及び英国GDPR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、要配慮個人情報と同様に取り扱うこととする。法第2条第3項（要配慮個人情報）。

補完的ルール②：提供を受けた個人データは保有個人データとする

EU又は英国域内から十分性認定に基づき個人データの提供を受けた場合、6ヶ月以内に消去する個人データであっっても、保有個人データとして取り扱うこととする。また、「その存否が明らかになることにより公益その他の利益が害されるものとして政令第4条で定めるもの」に該当する個人データは、保有個人データとして取り扱うこととする。法第2条第1項（保有個人データ）。

補完的ルール③：提供を受ける前に利用目的と取得経緯を確認し、その制限範囲内で取扱う

EU又は英国域内の本人から個人データの提供を受ける場合及び他の個人情報取扱事業者からEU及び英国域内の個人データの提供を受ける場合は、特定された利用目的を含め、その取得の経緯を確認し、記録することとする。かつ利用目的の範囲内で制限することとする（法第15条第1項、法第16条第1項、法第26条第1項及び第3項）。

補完的ルール④：外国の第三者との個人データは拘束力のある契約を締結し、その制限範囲で取扱う

外国の第三者に個人データを提供する場合及び提供を受ける場合は、あらかじめ外国の第三者を認める旨の本人の同意を得ることとする。かつ国内の個人情報取扱事業者と外国の第三者との間で拘束力のある契約、又はグループ企業間で拘束力のある取扱い）により、同等水準の保護措置を連携して実施していること。法第23条第1 項各号（第三者提供の制限）、法第24条（外国にある第三者提供の制限）。

補完的ルール⑤：提供を受ける個人情報は匿名加工情報の義務を果たし、その制限範囲で取扱う

EU又は英国域内から個人情報の提供を受ける場合、匿名加工方法の情報を削除し、何人にとっても復元できないようにすること。法第2条第9項（匿名加工情報）。法第36条第1項（匿名加工情報の作成等）。

【凡例】

「法」　　R2改正：個人情報の保護に関する法律（平成15年法律第57号）

「政令」　　R2改正：個人情報の保護に関する施行令（平成15年政令第507号）

「規則」　　R2改正：個人情報の保護に関する施行規則（平成28年個人情報保護委員会規則第3号）

「通則ガイドライン」 個人情報の保護に関する法律についてのガイドライン（通則編）（平成28年個人情報保護委員会告示第6号）

「EU」　　欧州連合加盟国及び欧州経済領域(EEA: European Economic Area)協定に基づきアイスランド、リヒテンシュタイン及びノルウェーを含む、欧州連合(European Union)

「GDPR」　　個人データの取扱いに係る自然人の保護及び当該データの自由な移転並びに指令95/46/ECの廃止に関する欧州議会及び欧州理事会規則（一般データ保護規則）

（REGULTION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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)）

「英国GDPR」 個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する2016年4月27日欧州議会及び欧州理事会規則（英国一般データ保護規則）

（REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)）

「十分性認定」GDPR第45条に基づき、欧州委員会が、国又は地域等を個人データについて十分な保護水準を確保していると認める決定及び英国においてこれに相当する決定