

全面施行直前！企業が知っておくべき個人情報保護法の改正内容と対応・活用ポイント

2022年1月13日

東京中小企業家同友会千代田支部

工藤 敦子



本日のメニュー

<食材の説明>

<5種類の飲茶>

- 1 匿名加工情報・仮名加工情報の食べ比べ
- 2 個人情報の取扱い
- 3 個人データの取扱い
- 4 保有個人データに関する権利義務

＜食材の説明＞

個人情報保護法

情報の種類

事業者の種類

個人情報とは



個人情報保護法とは

- デジタル社会の進展に伴い個人情報の有用性が拡大
- 「個人情報の有用性」に配慮しつつ「個人の権利利益」を保護
- 個人情報を取り扱う際のルール

情報の種類

- 個人情報
- 要配慮個人情報
- 個人情報データベース等（個人データ）
- 仮名化工情報データベース等（仮名化工情報）
- 匿名加工情報データベース等（匿名加工情報）
- 個人関連情報データベース等（個人関連情報）

規制対象となる事業者の種類

- **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
- **仮名化工情報取扱事業者**
仮名化工情報データベース等を事業の用に供している者
- **匿名加工情報取扱事業者**
匿名加工情報データベース等を事業の用に供している者
- **個人関連情報取扱事業者**
個人関連情報データベース等を事業の用に供している者

個人情報とは

- **生存する個人**に関する情報
- それ自体、又は、他の情報と容易に照合することにより、**特定の個人を識別できるもの**（氏名が分からなくても、この人と分かればよい、例：「氏名と生年月日」「顔写真」）

又は

- **特定の個人を識別できる「個人識別符号」**が含まれるもの
- 名刺一枚、公表されているNTTの電話帳も個人情報
- 個人情報と結びついている情報も個人情報、「従業員名と営業成績」など

メールアドレスは個人情報？

- keizai_Ichiro@meti.go.jp
- kudo@kojimalaw.jp
- kudo@gmail.com
- 1234abc@kojimalaw.jp
- 小島国際法律事務所工藤 < 1234abc@kojimalaw.jp >

個人識別符号とは

(個人情報保護法施行令・個人情報保護委員会規則で限定的に規定)

- **電子計算機の用に供するために変換した身体的特徴**
DNAの塩基配列、顔の容貌、虹彩の模様、声帯、歩行の姿勢、手の静脈の形状、指紋・掌紋（横綱の手形の色紙は個人識別符号？）
- **個人に割り当てられた番号等**
旅券番号、基礎年金番号、運転免許証番号、住民票コード、マイナンバー、健康保険証の番号など
- 個人識別符号ではないもの（携帯番号、クレジットカード番号、国家資格の登録番号）

要配慮個人情報とは

(個人情報保護法・施行令で限定的に規定)

- 個人情報のなかでも、**センシティブな情報**
人種、信条、社会的身分、病歴、犯罪歴、犯罪被害の事実、
心身機能の障害、健康診断等の結果、診療・調剤情報、刑事
事件手続、少年の保護事件手続

個人情報が多く持っている方がいいの？

- 利用目的の通知、正確性確保、安全管理措置、従業者・委託先の監督、開示請求への対応など、**重たい義務**
- 個人情報保護委員会への報告・立入検査、指導・助言、勧告、命令
- **罰則**（1年以下の懲役または50～100万円以下の罰金）の対象となる場合も
- 漏洩による**レピュテーションリスク**や**損害賠償リスク**
- 「いつか役に立つかも」という情報は捨て、**最小限必要なものだけに**

匿名加工情報・仮名加工情報の食べ比べ



仮名加工情報導入の背景

- 2017年の個人情報保護法改正時に「匿名加工情報」を導入
- 個人情報を匿名加工することで、規制が大幅に緩和され、内部利活用や外部提供を容易にした
- しかし、厳しい「匿名加工基準」を満たすことが難しい、基準をクリアすると有用性が落ちるなどの理由で利用が進まず
- EUにおいて、「仮名化」により若干緩やかな取扱いが認められ、国際的にもその活用が進みつつある
- そこで、2020年改正で、個人情報と匿名加工情報の中間形態ともいえる「仮名加工情報」を新設した

	匿名加工情報	仮名加工情報
定義	特定の個人を識別できないように個人情報を加工して得られる個人に関する情報であり、個人情報を復元できないようにしたもの	他の情報と照合しない限り特定の個人を識別できないように個人情報を仮名加工した個人に関する情報
加工基準	個人を識別できる記述等の削除（置換） 個人識別符号の削除（置換） 情報を相互に連結する符合の削除（置換） 特異な記述等の削除（上位概念に丸める） その他、個人識別不可・復元不可とするために必要な適切な措置	個人を識別できる記述等の削除（置換） 個人識別符号の削除（置換） 不正利用により財産的被害のおそれのある記述の削除（置換）
個人情報か否か	「個人情報」ではない	他の情報と照合すれば、個人を識別できる場合は、「個人情報」であり、「個人情報データベース等」に該当 元の情報・削除情報を消去し、又は、仮名加工情報の提供を受け、個人を識別できない場合は、「個人情報」ではない

	匿名加工情報	仮名加工情報
利用目的の公表等	利用目的の特定・公表の必要はない	できる限り利用目的を特定して公表 利用目的の変更は自由だが、変更後公表
第三者提供	事前に提供される項目、提供方法を公表 提供先に匿名加工情報である旨を明示	法令に基づく場合、委託・事業承継・共同利用以外の第三者提供は禁止、本人の同意を得てもできない
識別行為	禁止 匿名加工情報取扱事業者（提供先）の削除情報・匿名加工方法の情報の取得禁止	禁止
利用制限	なし	本人への連絡等の禁止 目的外利用禁止（利用目的の変更は自由） 本人の同意を得ても目的外利用できない 利用目的達成時の消去（努力義務）
安全管理	匿名加工情報の安全管理措置（努力義務） 削除情報・加工方法の安全管理措置（法的義務）	仮名加工情報の安全管理措置（法的義務） 削除情報・加工方法の安全管理措置（法的義務）

個人情報・個人データに関する規制の適用

- 匿名加工情報は「個人情報」ではないので、適用なし
- 「個人情報」に該当しない仮名加工情報には、適用なし
- 「個人情報」に該当する仮名加工情報には、適用あり
ただし、保有個人データに該当する場合でも、開示等の請求等の対象にはならない

個人情報の取扱い



個人情報に関する規制

- データベース化の有無にかかわらず「個人情報」が対象
- 規制対象となるのは、「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）
- 個人情報データベース等を事業の用に供していない事業者や私人は、規制対象ではない
- 個人情報データベース等 = 複数の個人情報を検索可能にしたもの（電子的に限らない。名刺を50音順に並べたものなども含む。市販の電話帳、住宅地図、職員録、カーナビなどをそのまま使う場合は含まれない）

個人情報を取り扱うには

- 取得時まで、**利用目的の特定**（事業者の内部で決めておく）
- 特定の度合いは、取扱う個人情報の性質、事業の内容により異なる
- 「お客様サービスの向上のため」「事業活動のため」ではダメ
- 取扱主体、事業の種別、具体的な行為態様により特定
例「当社が発行する住宅地図の作成・販売のため」
- **取得前に公表**、又は、**取得後速やかに本人に通知**又は**公表**
- **本人から直接文書で取得する場合は、本人に明示**

利用目的の変更

- 変更前の利用目的と関連性を有する範囲でのみ可
- 変更後の利用目的を**本人に通知**又は**公表**

利用目的の通知・公表が不要な場合

- 通知・公表により本人又は第三者の権利利益を害するおそれ
- 通知・公表により事業者の権利又は正当な利益を害するおそれ
- 国等の法令の定める事務に協力する場合で、通知・公表により当該事務に支障を及ぼすおそれ
- 取得の状況からみて利用目的が明らか

目的外利用ができる場合

- 本人の同意
- 法令に基づく場合
- 人の生命、身体、財産の保護に必要かつ同意取得が困難
- 公衆衛生、児童の健全育成に特に必要かつ同意取得が困難
- 国等の法令の定める事務に協力する場合で、同意取得により当該事務に支障を及ぼす恐れ
- 学術研究機関等が学術研究目的に使う場合
- 学術研究機関等に個人データを提供する場合

不適正利用の禁止

- 違法又は不当な行為を助長又は誘発するおそれがある方法による利用の禁止

例

- ①差別を誘発（破産者マップの公表）
- ②違法な行為を営む疑いがある者への提供（特殊詐欺グループへの名簿の提供）
- ③不当要求対策のための反社会的勢力等の名簿の開示（反社会的勢力からの業務妨害・担当者への妨害行為のおそれ）

適正な取得

- 犯罪行為・違法行為による取得禁止
- 利用目的の秘匿、偽り、誤解させての取得禁止
- 第三者提供の場合、提供先は、提供元の取得経緯の確認義務
- 要配慮個人情報は、本人同意なく取得禁止
ただし、例外として、法令に基づく場合等、目的外利用ができる場合と同じ場合に加え、要配慮個人情報が本人や国の機関等により公開されている場合、目視等により外形上明らかな要配慮個人情報を取得する場合、業務委託、事業承継、共同利用により提供を受ける場合

個人データの取扱い



個人データ

- 個人データ = 個人情報データベース等を構成する個人情報
- 個人情報データベース等 = 複数の個人情報を検索可能にしたもの（電子的に限らない。名刺を50音順に並べたものなども含む。市販の電話帳、住宅地図、職員録、カーナビなどをそのまま使う場合は含まれない）

個人データの取扱い

- データ内容の正確性の確保（努力義務）（消えた年金記録、別人の破産情報をクレカ会社に提供、カルテの記載ミスから医療過誤）
- 不要となった個人データの消去義務（努力義務）
vs 法定保存義務
復元不能な手段で廃棄・削除

個人データの安全管理措置（法的義務）

- セキュリティ管理（実効性のあるルール作り）
- 従業者・委託先監督
- 漏えい等の場合：個人情報保護委員会への報告（速報・確報）
確報（原因・再発防止策含む）は30営業日以内、故意の不正アクセスの場合は60営業日以内）
業務委託の場合：委託先→委託元に報告、委託元が委員会に報告
- 本人通知・本人通知が困難な場合は、代替措置（ウェブサイトで公表し、相談窓口を掲載など）
- 漏えい事件の慰謝料 1000円～500万円/件 × 漏えい件数

第三者提供の制限

原則 本人の事前同意（オプトイン）

例外1 適用除外（除外事由は目的外利用ができる場合とほぼ同じ）

例外2 オプトアウト制度

- 所定事項をあらかじめ本人に通知又は継続的に公表し、本人から要請があれば、第三者提供を停止する
- 所定事項（事業者名、住所、第三者提供を利用目的とすること、提供される個人データ項目、取得・提供・更新方法、提供開始予定日、本人の要請により第三者提供を停止すること、要請方法）
- 所定事項の委員会への届け出、所定事項の委員会による公表
- オプトアウトによる提供をやめたときは、その旨本人通知・公表・委員会への届け出

第三者提供の制限（続き）

- 例外 3 第三者に当たらない場合

- ① 業務委託先への提供

- ② 事業承継による提供

- ③ 共同利用者への提供

所定事項をあらかじめ本人に通知又は継続的な公表

所定事項（共同利用する旨、共同利用される個人データ項目、共同利用者の範囲、利用目的、管理者名）

クラウドストレージ・レンタルサーバーの利用は 第三者提供？

- クラウド事業者等が個人データを扱うか否かによる
 - 契約条項でクラウド事業者等が個人データを取り扱わない旨を定めること
 - 適切に、クラウド事業者等の個人データへのアクセス制御をしていること（安全管理措置）
- ➡ 第三者提供にならない

外国の第三者への提供

- 適用除外事由があれば、本人の同意なく提供できる
- オプトアウト制度は使えない（必ず事前同意が必要）
- 業務委託・共同利用の場合にも事前同意が必要

- ただし、認定国（現在はEU諸国と英国）は除く
- 基準適合体制整備者は除く
- 基準適合体制整備者（個人情報取扱事業者が講ずべき措置に相当する措置を講じる体制を整備している者）

第三者提供の記録義務

- 原則 3 年間、以下の記録事項を保存、但し、国などへの提供を除く

	提供年月日	提供先の氏名等	本人の氏名等	個人データの項目	本人の同意を得ていること
オプトアウトによる提供	○	○	○	○	
本人の同意による提供		○	○	○	○

第三者提供を受ける際の確認・記録事項

- 確認事項を確認し、原則3年間、以下の記録事項を保存

	提供年月日	提供元の氏名等	提供元の取得の経緯	本人の氏名等	個人データの項目	委員会により公表されていること	提供元が本人の同意を得ていること
確認事項		○	○				
オプトアウトによる提供	○	○	○	○	○	○	
本人の同意による提供		○	○	○	○		○
私人などからの提供		○	○	○	○		

個人関連情報の第三者提供の制限

- 個人関連情報 = 提供元では個人情報でなく、提供先で個人を識別でき、個人データとなることが想定される情報
例：氏名と紐づけられていないウェブサイト閲覧履歴、位置情報、クッキー等
- 個人関連情報データベース等を構成する個人関連情報提供の場合：提供元は、提供先が、事前に本人同意をとっていることを確認（提供元が代理取得しても可）
- オプトアウト方式は不可
- CMP（コンセンスト・マネジメント・プラットフォーム）の活用

個人関連情報取扱事業者

- 個人関連情報 = 提供元では個人情報でない
- 提供元は、個人情報取扱事業者であるとは限らない
- 個人関連情報データベース等を業務の用に供している者を個人関連情報取扱い事業者とした
- 他方、提供先では、個人データになるので、提供先は、個人情報取扱事業者

保有個人データに関する権利義務



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・削除、利用停止、消去、第三者提供の停止を行う権限を持つ個人データ

ただし、その存否が明らかになることで、本人又は第三者に危害が及ぶおそれ、違法不当な行使を助長・誘発するおそれ、国の安全が害されるおそれ、他国・国際機関との信頼関係が損なわれる・交渉上不利益を被るおそれ、犯罪の予防・鎮圧・捜査・公共の安全秩序の維持に支障が及ぶおそれがあるものを除く

保有個人データに関する公表等

- 公表等の方法 = 事業所の窓口等での掲示・備付、ウェブサイトへの掲載、パンフレット・広報誌等への明記、問合せへの回答など
- 公表すべき事項
 - 個人情報取扱事業者の名称等
 - 利用目的（取得時に本人への通知等が不要な場合は不要。所得時に利用目的が自明の場合でも必要）
 - 開示等の請求等に応じる手続
 - 適正な取扱確保措置
 - 苦情の申出先
 - 認定個人情報保護団体の対象である場合は、その名称・苦情の申出先

開示等の請求等への対応

- 開示等の請求等の方法（申出先、申出様式・方法、請求者の確認方法、手数料の徴収方法）を決めた場合は、公表・問い合わせに応じて回答
- 決めなくてもよいが、決めた上でウェブサイト上に掲載しておくのが簡便
- 本人に過重負担を課さないよう配慮が必要
- 本人に保有個人データを特定する事項を請求できる
- 開示・利用目的通知請求に対しては手数料をとれるが、訂正等・利用停止等の請求に対しては手数料はとれない

開示請求

- 開示 = 保有個人データの存否、内容を通知すること
- 開示請求者は、開示媒体（文書、電子データなど）を指定できる
- 多額の費用を要するなど、指定された方法による開示が困難な時は、書面の交付でよい
- 本人・第三者の権利利益を害するおそれ、個人情報取扱い事業者の適正な業務実施に支障を及ぼすおそれ、法令違反になる場合は、その旨通知して、拒絶できる。保有個人情報の一部の開示が拒絶できる場合は、塗りつぶしなどして、他の部分だけ開示
- 個人データの存否が明らかになることにより、本人等に危害が及ぶのおそれがあり、保有個人情報に該当しない情報について開示請求があった場合には「保有していない」と回答すべき（総会屋情報・DV被害者情報等）
- 個人データの第三者提供記録についても、同様に開示請求できる

その他の請求

- 利用目的の通知
- 訂正等（客観的な事実と異なっている場合、利用目的の達成に必要な範囲）
- 利用停止・削除（利用目的による制限違反、不適正な利用の禁止違反、適正な取得違反の場合、違反の是正に必要な限度）
多額の費用を要するなど利用停止等が困難な場合、代替措置をとればよい（金銭賠償など、事業者の負担と侵害を受ける権利利益などのバランスにより判断）
- 第三者提供の停止（第三者提供の制限違反の場合）
困難な場合は、代替措置
- 保有個人データが不要になった場合、重大な漏えいの恐れがある場合、本人の権利利益が害される場合の利用停止等・第三者提供停止
困難な場合は、代替措置

請求後

- 請求された利用停止等・第三者提供の停止の措置を行うか否かを決定し、請求者に通知
- 開示請求、利用停止等・第三者提供の停止請求、第三者提供記録の開示請求をした後、2週間経過しないと、本人が個人情報取扱事業者に対し、訴訟（仮処分含む）は提起できない。ただし、事業者が対応を拒否している場合は直ちに提起できる。