

データベースサービス産業 個人情報保護ガイドライン

平成 18 年 3 月
財団法人データベース振興センター
日本データベース協会

目 次

はじめに

第 1 章 総則

- 第 1 条 目的
- 第 2 条 適用範囲
- 第 3 条 定義

第 2 章 規定・方針等

- 第 4 条 個人情報保護方針
- 第 5 条 法令及びその他の規範
- 第 6 条 内部規程

第 3 章 運用

第 1 節 取得及び利用

- 第 7 条 利用目的の特定
- 第 8 条 利用目的による制限
- 第 9 条 適正な取得
- 第 10 条 取得に際しての利用目的の通知または公表
- 第 11 条 直接書面等による取得
- 第 12 条 利用目的の変更時の措置
- 第 13 条 取得時及び利用目的の変更時の措置の適用除外
- 第 14 条 特定の機微な個人情報の取得等の禁止

第 2 節 個人データの管理

- 第 15 条 データ内容の正確性の確保
- 第 16 条 安全管理措置
- 第 17 条 従業者の監督
- 第 18 条 委託先の監督

第 3 節 個人データの第三者への提供

- 第 19 条 第三者への提供の原則
- 第 20 条 オプトアウト
- 第 21 条 第三者への提供に該当しない場合

第 4 節 開示・訂正等・利用停止等の求めへの対応

- 第 22 条 保有個人データに関する事項の公表等
- 第 23 条 保有個人データの開示
- 第 24 条 保有個人データの訂正等
- 第 25 条 保有個人データの利用停止等
- 第 26 条 理由の説明
- 第 27 条 開示等の求めに応じる手続

第 5 節 苦情への対応

- 第 28 条 苦情への対応

第 4 章 漏えい等が発生した場合の措置

- 第 29 条 漏えい等が発生した場合の措置

第 5 章 推進体制

- 第 30 条 個人情報保護管理者の指名
- 第 31 条 個人情報保護管理者の責務
- 第 32 条 個人情報保護監査責任者の指名
- 第 33 条 個人情報保護監査責任者の責務

第 6 章 その他

- 第 34 条 プロデューサーの代表者による見直し
- 第 35 条 改廃

補足解説 ディストリビューターの個人情報保護法上の位置づけについて

はじめに

(財)データベース振興センター並びに日本データベース協会は、「個人情報の保護に関する法律(平成15年法律第57号)」の成立を受けて、個人情報を含む商用データベースを扱うデータベースサービス事業者が、その実態に応じたコンプライアンス・プログラムを策定する際の参考にされるよう「データベースサービス事業者個人情報保護ガイドライン」を作成し、これを公表、普及・啓発活動を行うこととした。これをもって高度情報ネットワーク社会の健全な発展に寄与することを願うものである。

第1章 総則

(目的)

第1条 このガイドラインは、データベースサービス事業者が第三者に提供することを目的とするデータベースに含まれる個人情報の適切な保護のため、データベースサービス事業者がその実態に応じた個人情報保護の規定を策定するための指針であり、これによってデータベースサービス事業者がコンプライアンス・プログラムを策定することを支援し、促進することを目的とする。

参考 個人情報保護法第1条

(適用範囲)

第2条 このガイドラインは、データベースサービス事業者が個人情報を含む商用データベースを取り扱う場合に適用する。

2 ただし、次のものは対象外とする。

- (1) 商用データベースのうち、新聞等の記事情報などの報道を目的とするもの
- (2) 顧客情報や雇用管理情報等として保有する個人情報

3 データベースサービス事業者は、次の場合に、このガイドラインを用いることができる。

- (1) コンプライアンス・プログラムを策定し、実施し、維持し、改善する場合
- (2) 策定したコンプライアンス・プログラムがこのガイドラインに適合していることについて自ら確認し、表明する場合

[解説]

1. このガイドラインは、データベースサービス事業者が自発的に採用するものであり、法的な拘束性を持つものではないので、その取り扱う個人情報の量や利用方法により事業者等を限定しない。
2. 顧客情報については、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン(以下、「経済産業省ガイドライン」という。)」(厚生労働省経済産業省告示第4号)に従い、また雇用管理情報については、「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」(厚生労働省告示第259号)に従って、社内規定を定めることが望ましい。
3. 本ガイドラインの解説は、経済産業省ガイドラインから抽出して、一部文言に加筆している。同ガイドラインの全てを記載していないので、コンプライアンス・プログラムの策定に当たっては必要に応じて同ガイドラインを参照する必要がある。また、本ガイドラインにおいて使用する用語は、別に定める場合を除き、同ガイドラインにおいて使用する用語の例による。
4. データベースサービス事業者には、自らデータベースを作成し第三者に提供するサービスを行うプロデューサーと、他業者の作成したデータベースの提供を受け、第三者に提供するサービ

スを行うディストリビューターの2つの業態が存在する。本ガイドラインは、両者に共通して適用する規定・解説と、いずれか一方に適用する規定・解説から構成される。

(定義)

第3条 このガイドラインで用いる用語の定義は、次による。

(1) データベース

相互に関連のあるデータを整理・統合し、コンピュータ処理によって、検索可能な状態に体系化したものをいう。

(2) 商用データベース

データベースサービス事業者が保有し商行為を目的に第三者に提供するデータベースをいう。

(3) 個人情報

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。

(4) 個人情報データベース等

個人情報を含む情報の集合体であって、次のものをいう。

特定の個人情報をコンピュータを用いて検索できるように体系的に構成したもの

コンピュータを用いていない場合であっても、含まれる個人情報を一定の規則に従って整理することにより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情報の集合体であって、目次、索引、符号その他検索を容易にするためのものを有するもの

(5) 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をいう。

(6) 保有個人データ

データベースサービス事業者が、本人またはその代理人から求められる開示、内容の訂正、追加または削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する「個人データ」をいう。ただし、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以下のものに該当する場合及び6ヶ月以内に消去するものは除く。

本人または第三者の生命、身体または財産に危害が及ぶおそれがあるもの

違法または不当な行為を助長し、または誘発するおそれがあるもの

国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれまたは他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

犯罪の予防、鎮圧または捜査その他の公共安全と秩序の維持に支障が及ぶおそれがあるもの

[解説]

1. 一般にデータベースに含まれる個人データは、プロデューサーにとり保有個人データに該当する。一方、ディストリビューターは、通常プロデューサーからデータベースの提供を受けるに当たり、著作権がプロデューサーにあること、データベースの改変等を禁ずること等を内容とした利用契約を締結しており、本人からの開示等の求めのすべてに応じる権限を有さないこと

から、ディストリビューターの保有個人データには該当しないと考えられる（巻末補足 「ディストリビューターの個人情報保護法上の位置づけについて」参照）。

2. 一般的にデータベースサービス事業者は顧客企業と利用契約を結ぶが、その条件は第三者提供を禁じる（＝再販しない）ことを目的としており、顧客企業が社内でデータのマージや項目の修正等の各種処理を行うことに対して制約を加えるものではない。

顧客企業がデータベースサービス事業者から提供を受けたデータベースに含まれる個人データについては、自社データベースに編入した場合、訂正等が可能となり、顧客企業の保有個人データとなり得ることに留意する必要がある。なお、顧客企業がデータを編集せず閲覧や印刷のみ行う場合は、顧客企業の保有個人データとはならない。

(7) 本人

個人情報によって識別される特定の個人をいう。

(8) データベースプロデューサー（プロデューサー）

自らデータベースを作成し、その全部または一部を第三者に提供するサービスを行う法人その他の団体または個人をいう。

(9) データベースディストリビューター（ディストリビューター）

他業者の作成したデータベースの提供を受け、その全部または一部を第三者に提供するサービスを行う法人その他の団体または個人をいう。

[解説]

1. ディストリビューターによる顧客への個人情報を含むデータベースの提供事業を個人情報保護法上の観点からみると、以下の2類型に整理される。

プロデューサーの「委託先」に相当するケース（プロデューサーから委託を受け、顧客に対しデータベースへのアクセスを許諾することで個人データの提供を行う）

自らの「第三者提供」に相当するケース（自らが主体となって顧客へ個人データを提供する）
（詳細は、巻末補足 「ディストリビューターの個人情報保護法上の位置づけについて」参照）

(10) データベースサービス事業者

プロデューサー及びディストリビューターをいう。

(11) 個人情報保護管理者

データベースサービス事業者の内部において代表者によって指名された者であって、コンプライアンス・プログラムの実施及び運用に関する責任と権限を有する者をいう。

(12) 個人情報保護監査責任者

データベースサービス事業者の代表者によって指名された者であって、個人情報保護管理者から独立した公平、かつ客観的な立場にあり、監査の実施及び報告を行う権限を有する者をいう。

(13) 従業者

データベースサービス事業者の組織内におい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、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等

も含まれる。

(14) コンプライアンス・プログラム

データベースサービス事業者が自ら保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメント・システムをいう。

(15) 本人の同意

本人の個人情報が、データベースサービス事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう（当該本人であることを確認できていることが前提。）。ただし、本人が子ども等の場合は、保護者の同意も得たことをいう。

(16) 本人が容易に知り得る状態

本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置いていることをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【本人が容易に知り得る状態に該当する事例】

事例1) ウェブ画面中のトップページから1回程度の操作で到達できる場所への掲載等が継続的に行われていること。

事例2) 事務所の窓口等への掲示、備付け等が継続的に行われていること。

事例3) 広く頒布されている定期刊行物への定期的掲載を行っていること。

事例4) 電子商取引において、商品を紹介するウェブ画面にリンク先を継続的に掲示すること。

(17) 本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）

ウェブ画面への掲載、パンフレットの配布、本人の求めに応じて遅滞なく回答を行うこと等、本人が知ろうとすれば、知ることができる状態に置くことをいい、常にその時点での正確な内容を本人の知り得る状態に置かなければならない。必ずしもウェブ画面への掲載、または事務所等の窓口等へ掲示すること等が継続的に行われることまでを必要とするものではないが、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

なお、ふだんから問い合わせ対応が多い事業者等において、ウェブ画面へ継続的に掲載する方法は、(16)「本人が容易に知り得る状態」及び(17)「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」の両者の趣旨に合致する方法である。

【本人の知り得る状態に該当する事例】

事例1) 問い合わせ窓口を設け、問い合わせがあれば、口頭または文章で回答できるよう体制を構築しておくこと。

事例2) 店舗販売において、店舗にパンフレットを備え置くこと。

事例3) 電子商取引において、問い合わせ先のメールアドレスを明記すること。

(18) 利用

データベースサービス事業者が当該事業者内で個人情報をコンピュータ処理することをいう。

(19) 提供

データベースサービス事業者が当該事業者外のものに自ら保有する個人情報を利用可能にす

ることをいう。

参考 個人情報保護法第2条・政令第1条・第2条・第3条・第4条

第2章 規定・方針等

(個人情報保護方針)

第4条 データベースサービス事業者の代表者は、次の事項を含む個人情報保護方針を定めるとともに、これを実行し維持しなければならない。また、当該代表者は、この方針を文書化し、従業者に周知させるとともに一般の人が入手可能な措置を講じなくてはならない。

- (1) データベースサービス事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること
- (2) 個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること
- (3) 個人情報保護に関する法令及びその他の規範を遵守すること
- (4) コンプライアンス・プログラムの継続的改善に関すること

(法令及びその他の規範)

第5条 データベースサービス事業者は、個人情報に関する法令及びその他の規範を特定し、参照できる手順を確立し、維持しなければならない。

(内部規程)

第6条 データベースサービス事業者は、個人情報を保護するための内部規程を策定し、維持しなければならない。

2 前項の内部規程には、次の事項を盛り込まなければならない。

- (1) データベースサービス事業者の各部門及び階層における個人情報を保護するための権限及び責任の規定
- (2) 個人情報の取得、利用、提供及び管理の規定
- (3) 本人からの個人情報に関する開示、訂正及び削除の求めに関する規定
- (4) 個人情報保護に関する教育の規定
- (5) 個人情報保護に関する監査の規定
- (6) 内部規程の違反に関する罰則の規定

3 データベースサービス事業者は、事業の内容及び規模に応じて、コンプライアンス・プログラムが確実に適用されるように内部規程を改定しなければならない。

第3章 運用

第1節 取得及び利用

(利用目的の特定)

第7条 データベースサービス事業者は、個人情報を取り扱うにあたっては、最終的にどのような目的で個人情報を利用するか、その利用の目的(以下「利用目的」という。)を可能な限り具体的に特定しなければならない。

- 2 利用目的を変更する場合には、変更前の利用目的と相当の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。

[解説]

1. データベースサービス事業者は、利用目的をできる限り特定しなければならない。
利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、事業者において最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定する必要がある。利用する個人情報の種類及び入手先の事業者名等を特定することまで求めているわけではない。
具体的には、「 事業における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられるが、定款や寄附行為等に想定されている事業の内容に照らして、個人情報によって識別される本人からみて、自分の個人情報が利用される範囲が合理的に予想できる程度に特定している場合や業種を明示することで利用目的の範囲が想定される場合には、これで足りるとされることもあり得る。しかしながら、単に「事業活動」、「お客様のサービスの向上」等を利用目的とすることは、できる限り特定したことにはならない。
2. データベースサービス事業者は、個人情報を第三者に提供することを想定している場合は、その旨を利用目的において特定しなければならない。
3. ディストリビューターがプロデューサーの委託を受けて、個人情報を第三者に提供することを想定している場合は、その旨を利用目的において特定しなければならない。

【具体的に利用目的を特定している事例】

- 事例 1) 「ご記入いただいた氏名、住所、電話番号は、商用データベースまたは人名録として販売致します。」
事例 2) 「他事業者から提供を受けて、個人情報を含むデータベースを販売致します。」
事例 3) 「他事業者から委託を受けて、個人情報を含むデータベースを販売致します。」

【具体的に利用目的を特定していない事例】

- 事例 1) 「事業活動に用いるため」
事例 2) 「提供するサービスの向上のため」
事例 3) 「マーケティング活動に用いるため」

4. 第 1 項により特定した利用目的は、社会通念上、本人が想定することが困難でないと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、または公表しなければならない。

参考 個人情報保護法第 15 条

(利用目的による制限)

第 8 条 データベースサービス事業者は、あらかじめ本人の同意を得ないで、前条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。

- 2 データベースサービス事業者は、合併その他の事由により他の事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。
- 3 前項の規定は、次に掲げる場合については、適用しない。
 - (1) 法令に基づく場合
 - (2) 人の生命、身体または財産の保護のために必要がある場合であって、本人の同意を得ること

が困難であるとき。

- (3) 公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
- (4) 国の機関もしくは地方公共団体またはその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

[解説]

1. データベースサービス事業者は、利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければならない。
2. 同意を得るために個人情報を利用すること（メールの送付や電話をかけること等）は、当初の利用目的として記載されていない場合でも、目的外利用には該当しない。

参考 個人情報保護法第 16 条 附則第 2 条

（適正な取得）

第 9 条 データベースサービス事業者は、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。

参考 個人情報保護法第 17 条

（取得に際しての利用目的の通知または公表）

第 10 条 データベースサービス事業者は、個人情報を取得する場合は、あらかじめその利用目的を公表していることが望ましい。公表していない場合は、取得後速やかに、その利用目的を、本人に通知するか、または公表しなければならない。

[解説]

法施行前から保有している個人情報については、法施行時に個人情報の取得行為がなく、法第 18 条の規定（取得に際しての利用目的の通知等）は適用されない。ただし、保有個人データに関する事項の本人への周知については、法施行時に法第 24 条第 1 項の措置（保有個人データに関する事項の公表等）を講ずる必要がある。

【本人に通知または公表が必要な事例】

事例 1) インターネット上で本人が自発的に公にしている個人情報を取得する場合

事例 2) インターネット、官報、職員録等から個人情報を取得する場合

事例 3) 電話による問い合わせやクレームのように本人により自発的に提供される個人情報を取得する場合（本人確認や問い合わせに対する回答の目的でのみ個人情報を取得した場合を除く。）

事例 4) 個人情報の第三者提供を受ける場合

[解説]

1. プロデューサーだけでなく、ディストリビューターにおいても、プロデューサーから個人情報を含むデータベースの提供を受けた場合は、その個人情報保護法上の類型に応じて、適切な利用目的を本人へ通知または公表することが必要となる。

参考 個人情報保護法第 18 条第 1 項

(直接書面等による取得)

第11条 データベースサービス事業者は、本人から直接書面(電子的方式・磁気的方式等による記録を含む。)に記載された当該本人の個人情報を取得する場合には、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。なお、口頭による個人情報の取得にまで、当該義務を課すものではない。

[解説]

【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場合】

事例1) データベースや人名録に収録するための調査票に記載された個人情報を本人から直接取得する場合

事例2) ウェブ画面より本人から個人情報を直接取得する場合

参考 個人情報保護法第18条第2項

(利用目的の変更時の措置)

第12条 データベースサービス事業者は、社会通念上、本人が想定することが困難でないと認められる範囲内で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、本人に通知するか、または公表しなければならない。

参考 個人情報保護法第18条第3項

(取得時及び利用目的の変更時の措置の適用除外)

第13条 第10～12条の規定は、次に掲げる場合については適用しない。

- (1) 利用目的を本人に通知し、または公表することにより本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- (2) 利用目的を本人に通知し、または公表することにより当該事業者の権利または正当な利益を害するおそれがある場合
- (3) 国の機関または地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、または公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- (4) 取得の状況からみて利用目的が明らかであると認められる場合

参考 個人情報保護法第18条第4項

(特定の機微な個人情報の取得等の禁止)

第14条 データベースサービス事業者は、次に示す内容を含む個人情報の取得、利用または提供を行ってはならない。ただし、これらの取得、利用または提供について、明示的な本人の同意がある場合、法令に特別の規定がある場合、及び司法手続上必要不可欠である場合は、この限りでない。

- (1) 思想、信条及び宗教に関する事項
- (2) 人種、民族、門地、本籍地(所在都道府県に関する情報を除く。)、犯罪歴、その他社会的差別の原因となる事項
- (3) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項
- (4) 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項
- (5) 保健医療及び性生活に関する事項

第2節 個人データの管理

(データ内容の正確性の確保)

第15条 データベースサービス事業者は、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。

参考 個人情報保護法第19条

(安全管理措置)

第16条 データベースサービス事業者は、その取り扱う個人データの漏えい、滅失またはき損の防止その他の個人データの安全管理のために、その規模に応じた必要かつ適切な措置を講じなければならない。

[解説]

データベースサービス事業者は、その取り扱う個人データの漏えい、滅失またはき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない(電話帳、カーナビゲーションシステム等の取扱いについての場合を除く。)。その際、本人の個人データが漏えい、滅失またはき損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、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。

【必要かつ適切な安全管理措置を講じているとはいえない場合】

- 事例1) 公開されることを前提としていない個人データが事業者のウェブ画面上で不特定多数に公開されている状態を個人情報取扱事業者が放置している場合
- 事例2) 組織変更が行われ、個人データにアクセスする必要がなくなった従業員が個人データにアクセスできる状態を個人情報取扱事業者が放置していた場合で、その従業員が個人データを漏えいした場合
- 事例3) 本人が継続的にサービスを受けるために登録していた個人データが、システム障害により破損したが、採取したつもりのバックアップも破損しており、個人データを復旧できずに滅失またはき損し、本人がサービスの提供を受けられなくなった場合
- 事例4) 個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業員がそこから個人データを入手して漏えいした場合
- 事例5) 個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

組織的安全管理措置

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）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】

個人データの安全管理措置を講じるための組織体制の整備

個人データの安全管理措置を定める規程等の整備と規程等に従った運用

個人データの取扱い状況を一覧できる手段の整備

個人データの安全管理措置の評価、見直し及び改善

事故または違反への対処

【各項目について講じることが望まれる事項】

個人データの安全管理措置を講じるための組織体制の整備をする上で望まれる事項

• 従業者の役割・責任の明確化

個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。

• 個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（CPO））の設置

• 個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定

• 個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定

• 個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化

• 監査責任者の設置

• 監査実施体制の整備

- 個人データの取扱いに関する規程等に違反している事実または兆候があることに気づいた場合の、代表者等への報告連絡体制の整備

- 個人データの漏えい等の事故が発生した場合、または発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備

個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第31条を参照）。

- 漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
- 漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備

個人データの安全管理措置を定める規程等の整備と規程等に従った運用をする上で望まれる事項

- 個人データの取扱いに関する規程等の整備とそれらに従った運用
- 個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用

なお、これらについてのより詳細な記載事項については、下記の【個人データの取扱いに関する規程等に記載することが望まれる事項】を参照。

- 個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
- 個人データの取扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
- 定められた規程等に従って業務手続が適切に行われたことを示す監査証跡 の保持

保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかの記録）、教育受講者一覧表等が考えられる。

個人データの取扱い状況を一覧できる手段の整備をする上で望まれる事項

- 個人データについて、取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備
- 個人データ取扱台帳の内容の定期的な確認による最新状態の維持

個人データの安全管理措置の評価、見直し及び改善をする上で望まれる事項

- 監査計画の立案と、計画に基づく監査（内部監査または外部監査）の実施
- 監査実施結果の取りまとめと、代表者への報告
- 監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善

事故または違反への対処をする上で望まれる事項

- 事実関係、再発防止策等の公表
- その他、以下の項目等の実施
- ア) 事実調査、イ) 影響範囲の特定、ウ) 影響を受ける可能性のある本人及び主務大臣等への報告、エ) 原因の究明、オ) 再発防止策の検討・実施

【個人データの取扱いに関する規程等に記載することが望まれる事項】

以下、() 取得・入力、() 移送・送信、() 利用・加工、() 保管・バックアップ、() 消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項を列記する。

() 取得・入力

) 作業責任者の明確化

- 個人データを取得する際の作業責任者の明確化
- 取得した個人データを情報システムに入力する際の作業責任者の明確化
- (以下、併せて「取得・入力」という。)

) 手続の明確化と手続に従った実施

- 取得・入力する際の手続の明確化
- 定められた手続による取得・入力の実施
- 権限を与えられていない者が立ち入れない建物、部屋(以下「建物等」という。)での入力作業の実施
- 個人データを入力できる端末の、業務上の必要性に基づく限定
- 個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定(例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。)

) 作業担当者の識別、認証、権限付与

- 個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
- IDとパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定

- 個人データの取得・入力業務を行う作業担当者に付与した権限の記録

) 作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と、権限外作業の有無の確認

() 移送・送信

) 作業責任者の明確化

- 個人データを移送・送信する際の作業責任者の明確化

) 手続の明確化と手続に従った実施

- 個人データを移送・送信する際の手続の明確化
- 定められた手続による移送・送信の実施
- 個人データを移送・送信する場合の個人データの暗号化（例えば、公衆回線を利用して個人データを送信する場合）移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用）
- F A X等におけるあて先番号確認と受領確認
- 個人データを記した文書をF A X等に放置することの禁止
- 暗号鍵やパスワードの適切な管理

) 作業担当者の識別、認証、権限付与

- 個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
- ID とパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを

介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。)

- 個人データの移送・送信業務を行う作業担当者に付与した権限の記録

) 作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と、権限外作業の有無の確認

() 利用・加工

) 作業責任者の明確化

- 個人データを利用・加工する際の作業責任者の明確化

) 手続の明確化と手続に従った実施

- 個人データを利用・加工する際の手続の明確化
- 定められた手続による利用・加工の実施
- 権限を与えられていない者が立ち入れない建物等での利用・加工の実施
- 個人データを利用・加工できる端末の、業務上の必要性に基づく限定
- 個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定(例えば、個人データを閲覧だけできる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。)

) 作業担当者の識別、認証、権限付与

- 個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
- IDとパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定(例えば、個人データを閲覧することのみが業務上必要

とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。)

- 個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

) 作業担当者及びその権限の確認

- 手順の明確化と手順に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と権限外作業の有無の確認

() 保管・バックアップ

) 作業責任者の明確化

- 個人データを保管・バックアップする際の作業責任者の明確化

) 手順の明確化と手順に従った実施

- 個人データを保管・バックアップする際の手続の明確化

情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム（OS）やアプリケーションのバックアップも必要となる場合がある。

- 定められた手順による保管・バックアップの実施
- 個人データを保管・バックアップする場合の個人データの暗号化
- 暗号鍵やパスワードの適切な管理
- 個人データを記録している媒体を保管する場合の施錠管理
- 個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理
- 個人データを記録している媒体の遠隔地保管
- 個人データのバックアップから迅速にデータが復元できることのテストの実施
- 個人データのバックアップに関する各種事象や障害の記録

) 作業担当者の識別、認証、権限付与

- 個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定
- ID とパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。）
- 個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録

) 作業担当者及びその権限の確認

- 手順の明確化と手順に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と権限外作業の有無の確認

() 消去・廃棄

) 作業責任者の明確化

- 個人データを消去する際の作業責任者の明確化
- 個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

) 手順の明確化と手順に従った実施

- 消去・廃棄する際の手順の明確化
- 定められた手順による消去・廃棄の実施
- 権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施
- 個人データを消去できる端末の、業務上の必要性に基づく限定
- 個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に1回または複数回上書きする。）

- 個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）
-) 作業担当者の識別、認証、権限付与
- 個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定
 - ID とパスワードによる認証、生体認証等による作業担当者の識別
 - 作業担当者に付与する権限の限定
 - 個人データの消去・廃棄を行う作業担当者に付与した権限の記録
-) 作業担当者及びその権限の確認
- 手順の明確化と手順に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
 - アクセスの記録、保管、権限外作業の有無の確認

人的安全管理措置

人的安全管理措置とは、従業者に対する、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や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】

雇用契約時及び委託契約時における非開示契約の締結

従業者に対する教育・訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、法第 2 1 条を参照。

【各項目について講じることが望まれる事項】

雇用契約時及び委託契約時における非開示契約の締結をする上で望まれる事項

- 従業者の採用時または委託契約時における非開示契約の締結

雇用契約または委託契約等における非開示条項は、契約終了後も一定期間有効であるよ

うにすることが望ましい。

- 非開示契約に違反した場合の措置に関する規程の整備

個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。

従業者に対する周知・教育・訓練を実施する上で望まれる事項

- 個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知
- 個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施
- 従業者に対する必要かつ適切な教育・訓練が実施されていることの確認

物理的安全管理措置

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等の措置をいう。

【物理的安全管理措置として講じなければならない事項】

入退館（室）管理の実施

盗難等の防止

機器・装置等の物理的な保護

【各項目について講じることが望まれる事項】

入退館（室）管理を実施する上で望まれる事項

- 個人データを取り扱う業務上の、入退館（室）管理を実施している物理的に保護された室内での実施

- 個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置

盗難等を防止する上で望まれる事項

- 離席時の個人データを記した書類、媒体、携帯可能なコンピュータ等の机上等への放置の禁止
- 離席時のパスワード付きスクリーンセイバ等の起動
- 個人データを含む媒体の施錠保管
- 氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
- 個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

機器・装置等を物理的に保護する上で望まれる事項

- 個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

技術的安全管理措置

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等、個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】

個人データへのアクセスにおける識別と認証

個人データへのアクセス制御

個人データへのアクセス権限の管理

個人データのアクセスの記録

個人データを取り扱う情報システムについての不正ソフトウェア対策

個人データの移送・送信時の対策

個人データを取り扱う情報システムの動作確認時の対策

個人データを取り扱う情報システムの監視

【各項目について講じることが望まれる事項】

個人データへのアクセスにおける識別と認証を行う上で望まれる事項

- 個人データに対する正当なアクセスであることを確認するためにアクセス権限を有する従業員本人であることの識別と認証（例えば、ID とパスワードによる認証、生体認証等）

の実施

ID とパスワードを利用する場合には、パスワードの有効期限の設定、同一または類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID を停止する等の措置を講じることが望ましい。

- 個人データへのアクセス権限を有する各従業員が使用できる端末またはアドレス等の識別と認証（例えば、MAC アドレス認証、IP アドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施

個人データへのアクセス制御を行う上で望まれる事項

- 個人データへのアクセス権限を付与すべき従業員数の最小化
- 識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）
- 従業員に付与するアクセス権限の最小化
- 個人データを格納した情報システムへの同時利用者数の制限
- 個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）
- 個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウ

ール、ルータ等の設定)

- 個人データにアクセス可能なアプリケーションの無権限利用の防止(例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる従業員が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等)

情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。

特権ユーザーに対するアクセス制御については、例えば、トラステッドOSやセキュアOS、アクセス制御機能を実現する製品等の利用が考えられる。

- 個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証(例えば、ウェブアプリケーションのぜい弱性有無の検証)

個人データへのアクセス権限の管理を行う上で望まれる事項

- 個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施(例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。)
- 個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

個人データへのアクセスの記録を行う上で望まれる事項

- 個人データへのアクセスや操作の成功と失敗の記録(例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録)
- 採取した記録の漏えい、滅失及びき損からの適切な保護

個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留

意する。

個人データを取り扱う情報システムについて不正ソフトウェア対策を実施する上で望まれる事項

- ウイルス対策ソフトウェアの導入
- オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用
- 不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）

個人データの移送（運搬、郵送、宅配便等）・送信時の対策の上で望まれる事項

- 移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化）
- 盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業員による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化

個人データを取り扱う情報システムの動作確認時の対策の上で望まれる事項

- 情報システムの動作確認時のテストデータとして個人データを利用することの禁止
- 情報システムの変更時に、それらの変更によって情報システムまたは運用環境のセキュリティが損なわれないことの検証

個人データを取り扱う情報システムの監視を行う上で望まれる事項

- 個人データを取り扱う情報システムの使用状況の定期的な監視
- 個人データへのアクセス状況（操作内容も含む。）の監視

個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。

(従業員の監督)

第 17 条 データベースサービス事業者は、従業員に個人データを取り扱わせるにあたっては、当該個人データの安全管理が図られるよう、当該従業員に対する必要かつ適切な監督を行わなければならない。

2 前項の監督にあたっては少なくとも次の事項を行わなければならない。

- (1) 規程類を策定し従業員に周知すること。
- (2) 従業員に対して個人情報の保護に関する教育を実施すること。
- (3) 個人データが適切に取り扱われているかを必要に応じて確認すること。

参考 個人情報保護法第 21 条

(委託先の監督)

第 18 条 データベースサービス事業者は、個人データの取り扱いの全部または一部を委託する場合は、その取り扱いを委託した個人データの安全管理が図られるよう、受託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。

2 前項の監督にあたっては、このガイドラインに従い、少なくとも次の事項を行わなければならない。

- (1) 委託先の選定基準を策定すること。
- (2) 前号の基準に照らして委託先の評価を行うこと。
- (3) 個人情報の保護に関する事項を契約書等に明記すること。
- (4) 前号の契約の内容が遵守されていることをあらかじめ定めた間隔で定期的に確認すること。

[解説]

- ディストリビューターによる顧客への個人情報を含むデータベースの提供事業を個人情報保護法上の観点からみると、以下の 2 類型に整理される。

プロデューサーの「委託先」に相当するケース

自らの「第三者提供」に相当するケース

(第 3 条 (9) データベースディストリビューター、巻末補足 「ディストリビューターの個人情報保護法上の位置づけについて」参照)

の「委託先」を構成するには、個人情報保護法 22 条に基づき、プロデューサーがディストリビューターに対し「必要かつ適切な監督」を行う必要があり、注意を要する。「経済産業省ガイドライン」では、「『必要かつ適切な監督』には、委託契約において、当該個人データの取扱に関して、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。」としている (P34 ~ 36 2. (3) 4)委託先の監督 (法第 22 条関連) 参照) 。

参考 個人情報保護法第 22 条

第 3 節 個人データの第三者への提供

(第三者への提供の原則)

第 19 条 データベースサービス事業者は、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。ただし、次に掲げる場合を除く。

- (1) 法令に基づく場合
 - (2) 人の生命、身体または財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (3) 公衆衛生の向上または児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
 - (4) 国の機関もしくは地方公共団体またはその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- 2 同意の取得に当たっては、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示さなければならない。

[解説]

1. 個人情報を含む主要なデータベースとして、人物情報データベースや企業情報データベースなどがあり、個人情報の取得は、本人等による調査票への記入が大きなルートとなっている。同意を得る方法は、原則としてこうした書面によることとし、次のような方法がある。
事例 1) 同意文言を記載した調査票上に、本人の署名(・押印)を徴求し、受領し、確認する。
事例 2) 本人による同意する旨の確認欄へのチェック
事例 3) 本人が署名または記名押印した同意する旨の文書を受領し確認すること。
事例 4) 本人からの同意する旨のメールを受信すること。
事例 5) 本人による同意する旨のウェブ画面上のボタンのクリック
2. 個人情報法の施行前に第三者提供を認める旨の同意に相当するものがある場合は本条の同意があったものと認められる。

参考 個人情報保護法第 23 条第 1 項、付則第 3 条

(オプトアウト)

- 第 20 条 データベースサービス事業者は、第三者提供におけるオプトアウトを行っている場合
- 1 には、前条の規定にかかわらず、本人の同意なく、個人データを第三者に提供することができる。
1 「第三者提供におけるオプトアウト」とは、提供に当たりあらかじめ、以下の(1)~(4)の情報を、本人に通知し、または本人が容易に知り得る状態に置いておくとともに、本人の求めに応じて第三者への提供を停止することをいう。
 - (1) 第三者への提供を利用目的とすること。
 - (2) 第三者に提供される個人データの項目
 - (3) 第三者への提供の手段または方法
 - (4) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
 - 2 本人の権利利益保護のためには、19条に定める本人からの事前同意取得がより望ましいことから、データベースサービス事業者は、極力その取得に努めることとするが、それが実務上困難な場合はオプトアウトを行う。
 - 3 第1項(2)または(3)に掲げる事項を変更する場合は、変更する内容について、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かなければならない。

[解説]

1. 個人情報保護法は、第 23 条第 1 項で原則として同意を得ないで個人データを第三者へ提供をしてはならないとしたうえで、第 23 条第 2 項で、オプトアウトを行う場合は、本人の同意なしに個人データの第三者への提供が許されるとする。

オプトアウトが認められた背景には、全国の世帯や事業所の表札や郵便受けから居住者名を取得して記載した住宅地図や、数百万件にも及ぶ個人情報や収録した人物情報・企業情報データベースなどが社会で有効に使われているという現実があり、これらについては同意原則を適用することは困難であり、有用性を損なう結果となるとの一般的な理解がある。

従って、データベースサービス事業を遂行するうえで実施が困難な場合についてまで、本人同意の取得を求めるものではない。しかしながら、本人の権利利益を保護しつつ、データベースサービス産業の透明性・信頼性を確保していくため、本条第2項において、本人の事前同意取得が原則であり、オプトアウトは例外的な措置であることを確認している。

プロデューサーは、機会があればできる限り本人の同意確認に努めるべきであり、調査の更新時などに少ない負担で可能な場合には進んで取り組むことが望ましい。

【オプトアウトの事例】

事例1) 住宅地図業者(表札や郵便受けを調べて住宅地図を作成し、販売(不特定多数への第三者提供))

事例2) データベース事業者(ダイレクトメール用の名簿等を作成し、販売)

【第三者に提供される個人データの項目】

事例1) 氏名、住所、メールアドレス

事例2) 氏名、商品購入履歴

【第三者への提供の手段または方法】

事例1) 電子媒体に変換して配布

事例2) インターネットに掲載

事例3) プリントアウトして交付等

2. オプトアウトを行う場合、本人から自己データの第三者提供停止要請があれば、速やかにこれに応じることが前提となる。顧客の窓口となるディストリビューターに対しても本人からの要請が見込まれるが、ディストリビューターにおいては、プロデューサーとの利用契約における著作権条項、改変禁止条項などのため、自社単独での対応が困難なケースが多いと考えられる。このため、本人からの第三者提供停止要請を含む、開示等の求めが行われた際、ディストリビューターにおいて望まれる対応については、第22条解説にまとめて記述した。
3. ディストリビューターによる個人情報の取得は、プロデューサーから個人情報を収録したデータベースの提供を受ける形で行われる間接取得であり、第三者提供について本人から同意を取得する機会はほとんどないため、自ら「第三者提供」を行うディストリビューターについては、オプトアウトの措置を行うのが現実的である。また、プロデューサーの「委託先」に相当するディストリビューターにおいては、法的には委託元のプロデューサーが本人同意取得もしくはオプトアウトの義務を負っている。
4. 本人が自発的に公にしている個人情報や、インターネット、官報等の公開された情報から取得した個人情報をデータベースに収録し販売する場合も、第三者提供についての本人の同意か、オプトアウトが必要であることに留意する。
5. 公開情報などから間接的に取得した個人情報をオプトアウトにより第三者提供する際、個人情報保護法上では転載できる内容に制限はない。ただし、14条に定めた機微情報の取得・利用・提供は原則として行わない他、プライバシーの観点から問題とならないよう十分配慮する必要がある。また、当該情報が著作物にあたる場合は、別途著作権法上の対応が必要になる。
6. 「本人が容易に知り得る状態」については、第3条(16)で定義されているが、「本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置いているこ

とをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法」によることが要求されている。データベース提供の方法としては、インターネットを中心とするオンライン経由のウエイトが高い状況や本人の利便性等を鑑みると、オプトアウトを行う場合、必要な事項を本人が容易に知りうる状態に置く方法としては、事例1で示されている「ウェブ画面中のトップページから1回程度の操作で到達できる場所への継続的な掲載等」がまず考慮されるべきである。

7. 個人情報法の施行前に本人に通知されているときは当該通知は法第23条第2項により行われたものとみなされる。

参考 個人情報保護法第23条第2項・第3項 附則第4条

(第三者への提供に該当しない場合)

第21条 次の各号のいずれかに該当する場合は、第19条の第三者への提供の制限にかかる第三者への提供に該当しないものとする。

- (1) 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に関する業務の全部または一部を委託する場合
- (2) 合併、分社化、営業譲渡等により事業が承継され個人データが移転される場合
- (3) 個人データを特定の者との間で共同して利用する場合であって、以下のことをあらかじめ、本人に通知し、または本人が容易に知り得る状態に置いているとき。

ア 共同利用する旨

イ 共同して利用される個人データの項目

ウ 共同して利用する者の範囲

エ 利用する者の利用目的

オ 当該個人データの管理について責任を有する者の氏名または名称

- 2 前項(3)に規定する項目のうち、エまたはオを変更する場合は、変更する内容について、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かなければならない。

[解説]

1. 上記1項(1)~(3)の場合は、第三者には該当しないため、本人の同意または第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができる。
2. 委託に当たっては、プロデューサーは、法22条にもとづき、委託先に対する監督責任が課されることに留意する。

参考 個人情報保護法第23条第4項・第5項 附則第5条

第4節 開示・訂正等・利用停止等の求めへの対応

(保有個人データに関する事項の公表等)

第22条 データベースサービス事業者は、保有個人データに関し、以下の情報を本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置かなければならない。

(1) 自社名

(2) すべての保有個人データの利用目的

(3) 保有個人データの利用目的の通知及び保有個人データの開示に係る手数料の額(定めた場合に限り)並びに開示等の求めの手續

1 「開示等の求め」とは、保有個人データの利用目的の通知、保有個人データの開示、保有

個人データの内容の訂正、追加または削除、保有個人データの利用の停止または消去、保有個人データの第三者への提供の停止の求めをいう。

(4) 保有個人データの取扱いに関する苦情及び問い合わせの申出先

2 データベースサービス事業者は、本人から、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を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、次のいずれかに該当する場合は、この限りでない。

(1) データベースサービス事業者が保有個人データに関して本人の知り得る状態に置いたことにより、当該本人が識別される保有個人データの利用目的が明らかな場合

(2) 13条（取得時及び利用目的の変更時の措置の適用除外）(1)～(3)までに該当し、通知、公表、明示を要しない場合

3 なお、データベースサービス事業者は、求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

[解説]

1. 第22条～第27条の、保有個人データに関する事項の公表、本人からの保有個人データの開示・訂正等・利用停止等の求めに対するのディストリビューターの対応義務

プロドューサーの「委託先」に相当するケース：

対応義務無し（提供するデータベースに含まれる個人データが、自らの保有個人データに当たらないため）ただし、委託元の企業との契約により、これらの対応業務を代行することは可能。

自ら「第三者提供」を行うケース：

対応義務あり。

(a) データベースの改変権限等があり、自らの保有個人データに当たる場合：

自ら対応する。

(b) データベースの改変権限等が無く、自らの保有個人データに当たらない場合：

本人からの開示等の求めに対し、自ら単独では対応できないので、当該データベースの保有個人データを持つプロドューサーと共同し、一体となって対応を行う。ただし、第22条の保有個人データに関する事項の公表義務は無い。

（巻末補足 「ディストリビューターの個人情報保護法上の位置づけについて」参照）

参考 個人情報保護法第24条・政令第5条

（保有個人データの開示）

第23条 データベースサービス事業者は、本人から、自己が識別される保有個人データの開示（存在しないときにはその旨を知らせることを含む。）を求められたときは、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法があるときはその方法により、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。

ただし、開示することにより下記の(1)～(3)のいずれかに該当する場合は、その全部または一部を開示しないことができるが、この場合は、遅滞なくその旨を本人に通知しなければならない。

(1) 本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

(2) 自社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

(3) 他の法令に違反することとなる場合

2 他の法令の規定により、別途開示の手続が定められている場合には、当該別途の開示の手続が優先されることとなる。

参考 個人情報保護法第25条・政令第6条

(保有個人データの訂正等)

第24条 データベースサービス事業者は、本人から当該本人が識別される保有個人データの内容が事実でないという理由によって訂正、追加または削除(以下「訂正等」という。)を求められたときは、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、訂正等を行わなければならない。

2 前項の規定に基づき訂正等を行ったときまたは訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨(訂正等を行ったときは、その内容を含む。)を通知しなければならない。

3 他の法令の規定により特別の手續が定められている場合には、当該特別の手續が優先されることとなる。

[解説]

1. 利用目的から見て訂正等が必要でない場合や誤りである旨の指摘が正しくない場合に、訂正等を行う必要はない。ただし、その場合には、遅滞なく訂正等を行わない旨を本人に通知しなければならない。
2. 調査や訂正は「利用目的の達成に必要な範囲内において」行うこととしているが、これは事業者においてその保有個人データを利用するうえで、厳密さがあまり求められないものまでその都度対応しなければならないとすると過度な負担となる可能性があるため、そのように定めている。

【訂正を行う必要がない事例】

事例) 訂正等の対象が事実でなく評価に関する情報である場合

参考 個人情報保護法第26条

(保有個人データの利用停止等)

第25条 データベースサービス事業者は、本人から、当該本人が識別される保有個人データが、第8条(利用目的による制限)または第9条(適正な取得)に違反しているという理由に基づき、当該保有個人データの利用の停止または消去(以下「利用停止等」という。)を求められた場合で、その求め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等、その実施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。

2 データベースサービス事業者は、本人から、当該本人が識別される保有個人データが、第19条(第三者への提供の制限)に違反しているという理由に基づき、当該保有個人データの第三者への提供の停止を求められた場合で、その求め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利用停止等に多額の費用を要する場合等、その実施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。

3 データベースサービス事業者は、求められた保有個人データの全部もしくは一部について利用停止等を行ったときもしくは行わない旨の決定をしたとき、または求められた保有個人データの全部もしくは一部について第三者への提供を停止したときもしくは停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

[解説]

1. データベースサービス事業者は、本人から、手続違反 1 の理由により保有個人データの利用停止等及び第三者への提供の停止が求められた場合には、原則 2 として、当該措置を行わなければならない。なお、利用の停止等を行った場合には、遅滞なく、その旨を本人に通知しなければならない。

1 「手続違反」とは、同意のない目的外利用、不正な取得、または同意のない第三者提供をいう。

2 「原則」...違反を是正するための必要な限度を超えている場合や手続違反である旨の指摘が正しくない場合には、利用の停止等を行う必要はない。ただし、その場合には、遅滞なく、利用の停止等を行わない旨を本人に通知しなければならない。

2. 個人情報保護法では、利用停止等に応ずる際、その実施に多額の費用を要する等によりその実施が困難な場合、あるいは、例えばデータベースサービス事業者が保有するデータベース内でその本人の個人情報のみ利用停止することで、データベースサービスが長期間提供できなくなり、顧客企業の業務上大きな支障が発生したりする場合は、そのことに代えて本人の権利利益を保護する措置が取れるのであればその限りでないとしており、本条においてもそれに従っている。

参考 個人情報保護法第 27 条

(理由の説明)

- 第 26 条 データベースサービス事業者は、保有個人データの公表・開示・訂正等・利用停止等・第三者提供の停止において、その措置をとらない旨またはその措置と異なる措置をとる旨を本人に通知する場合は、併せて、本人に対して、その理由を説明するように努めなければならない。

参考 個人情報保護法第 28 条

(開示等の求めに応じる手続)

- 第 27 条 データベースサービス事業者は、第 22 条～第 25 条による開示等の求めにおいて、その求めを受け付ける方法として下記(1)～(4)の事項を定めることができる。また、その求めを受け付ける方法を定めた場合には、本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置いておかななければならない。

(1) 開示等の求めの受付先

(2) 開示等の求めに際して提出すべき書面(電子的方式・磁気的方式による記録を含む。)の様式、その他の開示等の求めの受付方法(郵送、FAXで受け付ける等)

(3) 開示等の求めをする者が本人またはその代理人(ア)未成年者または成年被後見人の法定代理人、(イ)開示等の求めをするにつき本人が委任した代理人)であることの確認の方法

(4) 保有個人データの利用目的の通知、または保有個人データの開示をする際に徴収する手数料の金額と徴収方法(徴収する場合)

- 2 データベースサービス事業者は、本人に対し、開示等の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。

- 3 データベースサービス事業者は、開示等の求めに関する手続を定めるにあたっては、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。

- 4 次に掲げる代理人による開示の求めに応じなければならない。

- (1) 未成年者または成年被後見人の法定代理人
- (2) 開示等の求めをすることにつき本人が委任した代理人

5 データベースサービス事業者は、第22条の利用目的の通知、または第23条の開示を求められたときは、当該措置の実施に関し、手数料を徴収することができる。データベースサービス事業者は、当該手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

〔解説〕

1. 「開示等の求めの受付先」について

オンラインデータベースは、プロデューサーが作成し、複数のディストリビューターが顧客へ販売するケースが一般的であり、契約条件によるものの、基本的にプロデューサーの保有個人データとなる。一方、顧客の視点からは、当該データベースがどの事業者の保有個人データが分かりにくい場合もある。このため、ディストリビューターは顧客に対し、プロデューサーにおける開示等の受付先を明示することが望ましい。

また、プロデューサーとの契約により、ディストリビューターが顧客からの苦情の一次サポートを担当し、プロデューサーとの間を媒介するケースも考えられる。

- 2. 個人情報保護法第29条により、本人からの開示等の求めに対し、それらを受け付ける手続きを定めることができる。
- 3. ただし、手続きを定めるに当たっては、必要以上に煩雑な書類を求めることや、求めを受け付ける窓口を他の業務を行う拠点とは別にいたずらに不便な場所に限定すること等して、本人に過重な負担を課することのないよう配慮しなければならない。
- 4. 開示等の求めを受け付ける方法を合理的な範囲で定めたときで、求めを行った者がそれに従わなかった場合は、開示等を拒否することができる。
- 5. 開示等の求めを受ける方法を定めない場合には、自由な申請を認めることになる。
- 6. データベースサービス事業者は、円滑に開示等の手続が行えるよう、本人に対し、自己のデータの特定に必要な事項（住所、ID、パスワード、会員番号等）の提示を求めることができる。なお、本人が容易に自己のデータを特定できるよう、自己の保有個人データの特定に資する情報の提供その他本人の利便性を考慮しなければならない。
- 7. 本人に対し自己の個人データの開示を行う場合、その目的等を本人に尋ねる等により、本人への開示範囲を確認することができる。

8. 【開示の求めをする者が本人またはその代理人であることの確認の方法】

事例1) 本人の場合(来所): 運転免許証、健康保険の被保険者証、写真付き住民基本台帳カード、旅券(パスポート)、外国人登録証明書、年金手帳、印鑑証明書と実印

事例2) 本人の場合(オンライン): IDとパスワード

事例3) 本人の場合(電話): 一定の登録情報(生年月日等)、コールバック

事例4) 本人の場合(送付(郵送、FAX等)): 運転免許証のコピーと住民票の写し

事例5) 本人の場合(送付(郵送、FAX等)): 運転免許証や健康保険の被保険者証等の公的証明書のコピーの送付を顧客等から受け、当該公的証明書のコピーに記載された顧客等の住所にあてて文書を書留郵便により送付

事例6) 代理人の場合(来所): 本人及び代理人について、運転免許証、健康保険の被保険者証、旅券(パスポート)、外国人登録証明書、年金手帳、弁護士の場合は登録番号、代理を示す旨の委任状

- 9. 個人情報保護法第30条により、利用目的の通知及び開示の求めについては実費を勘案して合理的であると認められる範囲内において手数料を定め、徴収することができるが、訂正等及び利用停止等については、手数料を徴収することはしていないことに留意

する。

参考 個人情報保護法第 29 条・第 30 条・政令第 7 条・第 8 条

第 5 節 苦情への対応

(苦情への対応)

第 28 条 データベースサービス事業者は、個人情報の取り扱いに関する苦情の適切かつ迅速な対応に努めなければならない。

2 苦情処理を行うに当たり、苦情処理窓口の設置や苦情処理の手順を定める等必要な体制の整備に努めなければならない。

参考 個人情報保護法第 31 条

第 4 章 漏えい等が発生した場合の措置

(漏えい等が発生した場合の措置)

第 29 条 データベースサービス事業者は、個人情報の漏えい事案等の事故があった場合に備え、危機対応のための体制の整備及び手順の策定を行わなければならない。

2 データベースサービス事業者は、個人情報の漏えい事案等の事故があった場合は、以下の措置を講じる。

(1) 漏えい等の対象となった本人に速やかに漏えい等の事実関係等を通知し、または本人が容易に知り得る状態に置くものとする。

(2) 発生原因、対応策を所管する省庁に直ちに報告するものとする。

(3) 二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係、発生原因を遅滞なく公表するものとする。

第 5 章 推進体制

(個人情報保護管理者の指名)

第 30 条 データベースサービス事業者の代表者は、このガイドラインの内容を理解し実践する者を内部から 1 名以上指名し、個人情報保護管理者としての業務を行わせるものとする。

(個人情報保護管理者の責務)

第 31 条 個人情報保護管理者は、このガイドラインに定められた事項を理解及び遵守するとともに、従業者にこれを理解及び遵守させるために、規程類の整備、個人情報保護推進体制の整備ならびに周知徹底の措置、安全対策、従業者への教育訓練、委託先管理等の措置及び文書管理等を実施する責任を負うものとする。

(個人情報保護監査責任者の指名)

第 32 条 事業者の代表者は、個人情報保護管理者からは独立し、個人情報保護推進体制の妥当性、有効性及び実施状況について、本ガイドラインに定められた監査を実施する者を内部から指名し、個人情報保護監査責任者としての業務を行わせることが望ましい。

(個人情報保護監査責任者の責務)

第33条 個人情報保護監査責任者は、自社の個人情報保護体制の運営状況を定期的に監査し、監査報告書を作成し、事業者の代表者に報告する責任を負うものとする。

第6章 その他

(データベースサービス事業者の代表者による見直し)

第34条 データベースサービス事業者の代表者は、監査報告書及びその他の経営環境などに照らして、適切な個人情報の保護を維持するために、少なくとも年1回コンプライアンス・プログラムを見直さなければならない。

(改廃)

第35条 このガイドラインの改廃は、有識者から構成される委員会で審議し、その答申を受けた(財)データベース振興センター理事長の承認を得るものとする。

[参考資料]

- (1) 平成 16 年 10 月 22 日厚生労働省経済産業省告示第 4 号「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」
- (2) 日本工業規格 JIS Q 15001 : 1999「個人情報保護に関するコンプライアンス・プログラムの要求事項」
- (3) 電子商取引推進協議会「民間部門における電子商取引に係る個人情報保護に関するガイドライン (Ver.3.0)」
- (4) 情報サービス産業協会「情報サービス産業 個人情報保護ガイドライン (第 3 版)」

補足解説 ディストリビューターの個人情報保護法上の位置づけについて

1. 提供方式上の分類

ディストリビューターは、プロデューサーが作成したデータベースをユーザーの利用に供する事業者であるが、提供方式には大きく次の2つのパターンがある。1事業者が両方のパターンを採用しているケースもある。

ゲートウェイ方式

プロデューサーもしくは他のディストリビューターのデータベース・ファイルと自社のコンピュータシステムを通信回線をつないでユーザーに提供する。自社はデータベース・ファイルをもたない。

データベース・ファイルを預かり、提供する方式

プロデューサーからデータベース・ファイルの委託を受け、自社のコンピュータシステムに格納してユーザーに提供する。

2. 契約上の分類

データベースの提供に関するプロデューサーとディストリビューターの契約内容は多様であるが、大きく分類すると次の2つに分かれる。

利用許諾（ライセンス販売）

プロデューサーのデータベースをディストリビューターが契約期間中利用し、顧客に販売することを許諾する。プロデューサーは、ディストリビューターの売上高の一定割合等を代金として受け取る。データベースの著作権はプロデューサーが保有する。別途、ディストリビューターにおける改変を禁止する条項を追加する場合もある。契約終了後は、ディストリビューターは当該データベースの利用ができなくなる。

売り切り

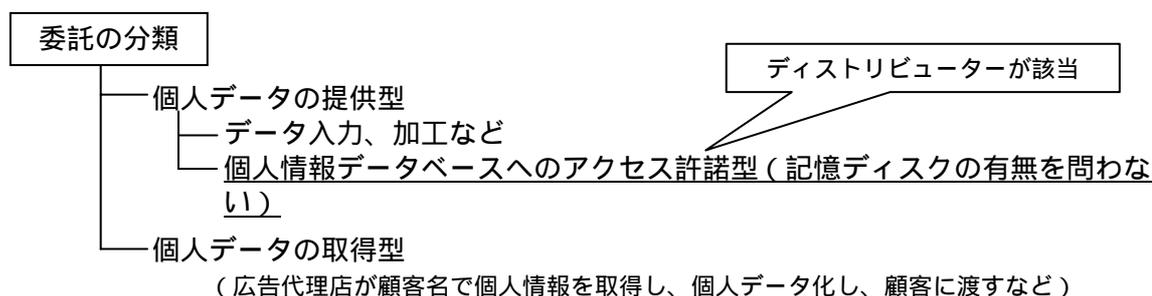
プロデューサーのデータベースをディストリビューターに販売譲渡する。ディストリビューターによるデータベースの改変等が可能となる。

3. 個人情報保護法上の分類

個人情報保護法では、個人情報の事業者間の移動については、「第三者提供」、または「委託」の2類型のみを想定している。ディストリビューターによる個人情報を含むデータベースの顧客への提供行為をこの2類型に当てはめると以下の様に整理される。

プロデューサーの「委託先」に相当するケース

個人情報の「委託」には、個人情報の取得型と提供型があり、ディストリビューターの事業は後者に該当する場合があると考えられる。



通常、データベースの提供に関するプロデューサー・ディストリビューター間の契約は、販売委託契約ではなく、2. の「利用許諾」契約である。ただし、個人情報保護法では契約の名称ではなく、個人情報の取扱いに関する委託の有無を問題としている。そのため、ディストリビューターは、プロデューサーから、データベースをユーザーへ提供する業務を委託されている、すなわち、プロデューサーの（個人情報）データベースへのユーザーのアクセス許諾を委託されていると考えることができる。この場合、アクセスする先のデータベース・ファイルがプロデューサー、または他のディストリビューターが保有するデータベース・ファイルであるか（ゲートウェイ方式）あるいは自社が預かるデータベース・ファイルであるかは問わない。

自らの「第三者提供」に相当するケース

- (a) プロデューサー・ディストリビューター間の契約が、2. の「売り切り」の場合は、ディストリビューターによる顧客へのデータベース提供行為にプロデューサーは関わりがなくなることから、ディストリビューターによる顧客への第三者提供に相当する。
- (b) また、2. の「利用許諾（ライセンス販売）」契約の場合であっても、ディストリビューターの事業実態によっては、プロデューサーからの委託ではなく、自らが事業主体として顧客への第三者提供を行っているとして位置づけることも可能と考えられる。

なお、上記の(a)(b)の各ケースにおいて、プロデューサーからディストリビューターへのデータベースの提供（販売）行為も第三者提供に該当する。通常、第三者提供された個人データは提供を受けた側で自由に処分できるが、(b)の場合は契約終了後の使用停止義務を負う。この場合はプロデューサーからディストリビューターへ期限付きで第三者提供が行われたものと解釈される。

4. 保有個人データへの該当性について

経済産業省ガイドラインでは、「保有個人データ」に関して以下の解説を行っている（7～8ページ）。

(1) 「保有個人データ」(法第2条第5項関連)

「保有個人データ」¹とは、個人情報取扱事業者が、本人又はその代理人から求められる開示、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のすべてに応じることができる権限を有する²「個人データ」をいう。

¹法は、「(1)個人情報」、「(4)個人データ」及び「保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。

²個人情報取扱事業者が個人データを受託処理している場合で、その個人データについて、何ら取決めがなく、自らの判断では本人に開示等を行うことができないときは、本人に開示等の権限を有しているのは委託者であって、受託者ではない。

保有個人データに該当しないと考えられるケース

- (a) ディストリビューターのうち、提供方式が、上記1. の「ゲートウェイ方式」の場合は、そもそも、自らがデータベース・ファイルを保有しておらず、システムのデータベースの内容の訂正、追加又は削除等を行うことができないことから、提供するデータベースに含まれる個人データは、自らの保有個人データに該当しないと考えられる。
- (b) 一方、上記1. の「データベース・ファイルを預かり、提供する方式」の場合でも、プロデューサー・ディストリビューター間のデータベース提供契約が「利用許諾」契約である場合は、プロデューサーが著作権を所有しており、その同一性保持権を侵害できないこと、場合により改変禁止条項も加えられていることから、ディストリビューターによるデータベースの改変は契約上許されていないのが通常である。例外的に緊急時の措置としてディストリビューターが一部データの削除などを行う場合もあるが、あくまで事前のプロデューサーとの合意に基づく行為であり、ディストリビューターに「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のすべてに応じることができる権限」がある訳ではないことから、提供するデータベースに含まれる個人データは、自らの保有個人データに該当しないと考えられる（下記 (b) の場合を除く）。

これらのケースにおいては、プロデューサーの保有個人データに該当するものと考えられる。

保有個人データに該当すると考えられるケース

- (a) プロデューサー・ディストリビューター間のデータベース提供契約が「売り切り」であり、ディストリビューターがデータベースの訂正等を自由に行える場合は、当該データベースに収録された個人データはディストリビューターの保有個人データに該当すると考えられる。
- (b) また、両者の契約が「利用許諾」であっても、例外的にプロデューサーがディストリビューターにおけるデータベース・ファイルの自由な訂正等を許可する場合があります、この場合はディストリビューターの保有個人データに該当する可能性があるので注意を要する。

5. 提供方式・契約形態と個人情報保護法上の類型の関係

データベースの提供方式、プロデューサーとの契約形態と、適用の可能性がある個人情報保護法上の類型の関係を整理すると以下の様になる。

プロデューサーとの契約形態 提供方式	利用許諾	売り切り
ゲートウェイ	・委託 ・第三者提供	
データベース・ファイルを預かり、提供	・委託 ・第三者提供	・第三者提供

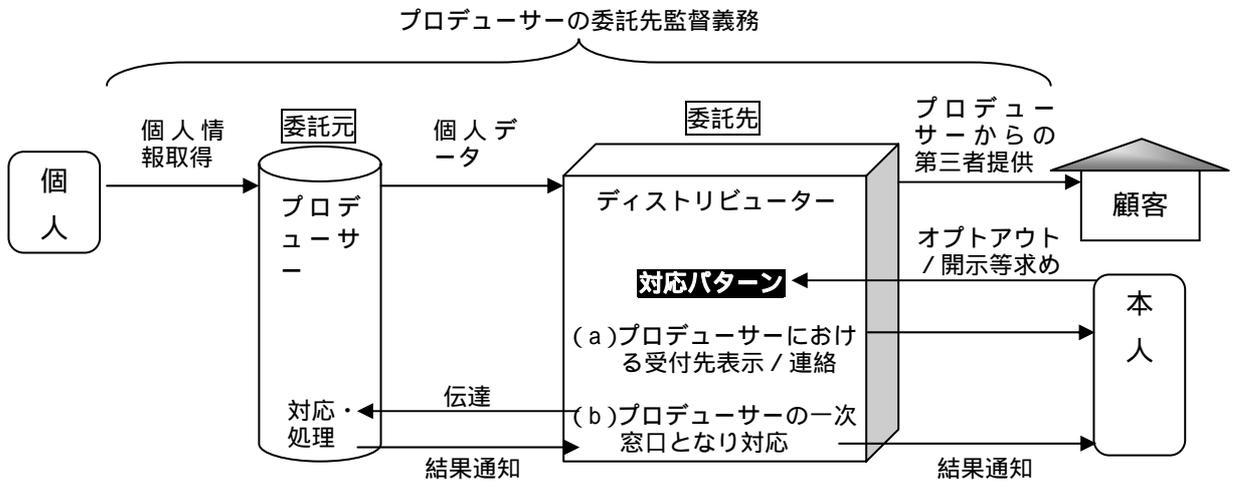
6. 各類型における個人情報取扱事業者としての義務の整理

個人情報取扱事業者の義務となる事項について、各類型別に、ディストリビューターにおける個人情報保護法上の対応の要否を整理すると、下表のようになる。本人の開示等の求めへの対応は、同法に対する上積みの部分も加えて(a)～(d)の4パターンとなる。

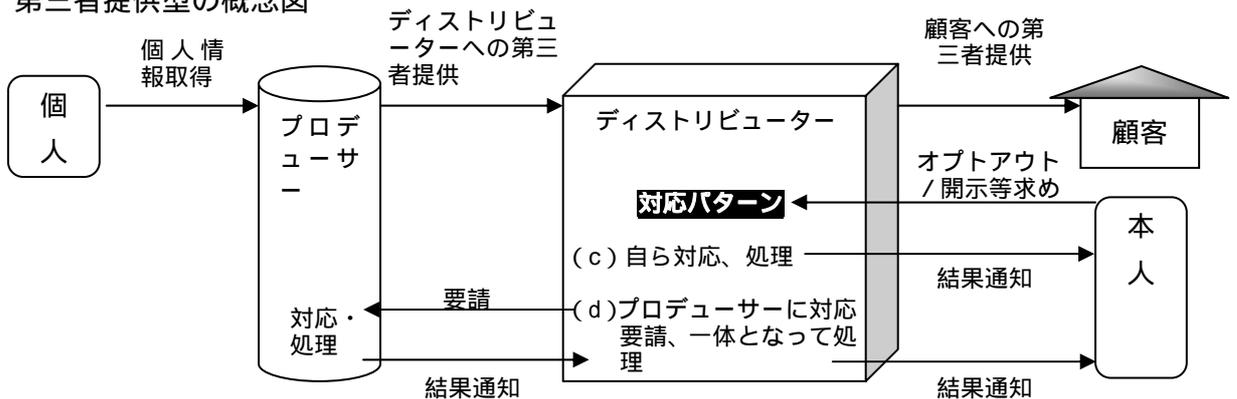
個人情報保護法上の類型	利用目的の特定	利用目的の通知/公表	安全管理措置	第三者提供への本人同意取得	オプトアウト手続き	保有個人データへの該当	保有個人データの必要事項公表	本人の開示等の求めへの対応
委託先型	(受託して取り扱う旨)		(プロデューサーとの契約等で担保)	×	×	しない	×	(a)パターン × (プロデューサーにおける受付先を表示するのみ) (b)パターン (本人に対し、プロデューサーの一次窓口として対応)
第三者提供型	(データベースとして販売する旨)		(自己で完結)	× (ほぼ不可能)		する		(c)パターン (自ら対応)
						しない	×	(d)パターン (プロデューサーに要請、一体となって処理)
個人情報保護法	15条	18条	20条	23条1項	23条2項	2条5項	24条	25～31条
DB 産業ガイドライン	7条	10,11条	16条	19条	20条	3条(6)	22条	23～28条

(注) = 対応が必要、× = 不要、 = 一部必要、

委託先型の概念図



第三者提供型の概念図



7. データベース中の個人情報を「事業の用に供していない」とみなされる可能性について

経済産業省ガイドラインでは、(個人情報データベース等に含まれる個人情報を)「事業の用に供しないため特定の個人の数に算入しない事例」として以下をあげている(6ページ)。

事例) 倉庫業、データセンター(ハウジング、ホスティング)等の事業において、当該情報が個人情報に該当するかどうかを認識することなく預かっている場合に、その情報中に含まれる個人情報

上記事例の個人情報については、個人情報取扱事業者としての義務が発生しないことになるが、多くのディストリビューターは、複数の提供データベースを「人物情報」等のジャンルに分類し、かつこれらを一括検索する「人物情報横断検索」機能等を付加していることから、経済産業省ガイドラインの事例のように「当該情報が個人情報に該当するかどうかを認識することなく預かって」おり、「事業の用に供していない」とみなされる可能性は高くないものと考えられる。

8. まとめ

個人情報を含むデータベースを提供するディストリビューターは、収録人数が5,000人以下等の小規模な数事業者を除き、大方が個人情報取扱事業者に該当し、自らが提供するデータベースに含まれる個人情報について適切な保護措置を講じることを求められていると考えられる。

個々のディストリビューターは、自らの事業実態に照らして、それが個人情報保護法上の類型では「委託先型」か、もしくは「第三者提供型」に相当するのかの判断をすると共に、本人の開示等の求めに対する対応方針などを決定することになるが、それぞれの類型や対応パターンにより、事業者の取るべき措置は大きく異なってくる。業界個人情報保護ガイドラインを参考とした適切な対応が広がることで、データベースとして提供される個人情報の利用増大が図られつつ、保護水準の向上が一層促進されることを期待したい。