

---

# 個人情報保護に関する法律についての スーパーマーケット業界ガイドライン

平成17年1月

社団法人日本セルフ・サービス協会  
社団法人全国スーパーマーケット協会  
日本スーパーマーケット協会

# 目次

---

はじめに	2
目的及び適用範囲	3
1 定義	
1 - 1 個人情報とは	4
2 個人情報データベース等	5
3 個人情報取扱事業者とは	6
4 個人データ・保有個人データ	7
5 その他の定義	8
2 個人情報取扱事業者の義務	10
2 - 1 利用目的の特定	11
2 利用目的の変更	12
3 利用目的による制限	12
4 適正な取得	13
5 利用目的の通知・公表	14
適用除外	15
6 安全管理措置	16
7 従業者の監督	22
8 委託先の監督	23
9 第三者への提供	24
10 第三者への提供の例外	26
11 保有個人データの公表・開示	28
3 その他	32
4 スーパーマーケット業で一般的な個人情報	33

# はじめに

---

個人情報保護法の施行(平成17年4月1日)に向けて、個人情報保護法第7条に基づき内閣府が事務局となって作成した「個人情報の保護に関する基本方針」が閣議決定(4月2日)。

ただし、基本方針の性格は、官庁各省が共通に行うべき取り組みについて定めたものであり、個々の業界、事業者が具体的にどのような対応を行えばよいかについては、基本的な枠組みを提示したものととどまっている。

このため、会員企業が対応を行う際の参考となるような規程・細則・マニュアルの作成が必要。

経済産業省では、当省の所管業種における個人情報保護法の適用をまとめた、「個人情報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」を策定した。社団法人全国スーパーマーケット協会、社団法人日本セルフ・サービス協会、日本スーパーマーケット協会においては、経済産業省作成のガイドラインを下敷きにして、会員企業が具体的にどのような対応を行えばよいのかの参考に供するべく業界特有の個人情報や運用方法をいくつか例示した。

なお、本ガイドラインの策定にあたっては、上記の3団体が実務者レベルのプロジェクトチームをおこし、相互に分担して検討を加えた。

# 目的及び適用範囲

## 本ガイドラインの目的

個人情報保護に関する基本方針に基づき、事業の実態に応じた個人情報の適正な取扱いの確保に関して行う活動を支援するための具体的な指針を示すものである。

本ガイドラインを見れば、個人情報保護法に関する対応についておおよそ理解できる内容を盛り込んでいる。

## 本ガイドラインの内容

団体傘下会員企業を対象とした自主的ルールである、事業者団体(業界)ガイドラインとして策定した。

中に、理解を助けるための参考例として、個人情報保護法のルールに適合している例と適合しない例の双方について具体的に記述した。

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況など諸環境の変化を踏まえて毎年見直しを行うよう努める。

## 情報保護のための運用の規定書類

このガイドラインを基礎に、基本規定、内部規定(規程)、細則、手引書など詳細な運用基準書が各事業者ごとに作成されていくものと予想されるが、この時点においては、本ガイドラインと基本規定を会員企業へ提示し、会員企業に向けての勉強会の教材とし、さらに会員企業の詳細な対策作業の一助としたい。

# 1. 定義

法律で用いられている基本的な用語の定義とその具体的事例を示す。

## 1 - 1 個人情報とは

法律第2条第1項 この法律において「個人情報」とは、生存する個人に関する情報であつて、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。

### ガイドライン

氏名、性別、生年月日等に限らず、個人の身体、財産、職種、地位身分、肩書き等を含め、事実・判断・評価を表すすべての情報をいう。評価情報、公刊物等によって公にされているものや、映像、音声も含まれ、暗号化されているかどうかを問わない。  
「生存する個人」は日本国民に限られず、外国人も含まれる。  
法人等の団体に関する情報は含まれない。

#### 【個人情報に該当する事例】

- ・本人の氏名、生年月日、連絡先(住所・居所・電話番号)、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報
- ・防犯カメラに記録された情報など本人が判別できる映像情報
- ・特定の個人を識別できるメールアドレス情報(keizai\_ichiro@meti.go.jpなど)
- ・雇用管理情報(会社が社員を評価した情報を含む。)
- ・官報、電話帳、職員録等に公にされている情報

#### 【個人情報に該当しない事例】

- ・企業の財務情報等、法人等団体に関する情報(団体情報) ・死者の情報(但し、死者情報が遺族情報となる場合があれば、個人情報となる)
- ・記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報(例えば、abc012345@ispisp.com)。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。
- ・特定の個人を識別することができない統計情報

# 1. 定義

## 1 - 2 個人情報データベース等

法第2条第2項 この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるものをいう。

- 一 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
- 二 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

### ガイドライン

特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した個人情報を含む情報の集合物  
コンピュータを用いなくても、カルテや指導要録など、紙面で処理した個人情報を一定の規則(例えば、五十音順、年月日順等)に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているもの

#### 【個人情報データベース等に該当する事例】

- ・電子メールソフトに保管されている電子メールアドレス帳
- ・従業員が、名刺の情報を業務用パソコン(所有者を問わない。)に入力・整理(データベース化)し、他の従業員等も検索できる状態にしている場合
- ・氏名、住所、企業別に分類整理されている市販の人名録

#### 【個人情報データベース等に該当しない事例】

- ・従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いてあっても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合
- ・アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

個人情報保護法では、「個人情報」、「個人データ」、「保有個人データ」と用語を使い分けている。  
「個人データ」、「保有個人データ」については、後段の1 - 4 において定義をしている。

# 1. 定義

## 1 - 3 個人情報取扱事業者とは

法第2条第3項 この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。

### ガイドライン

個人情報を売り買ひする名簿業者を指すのではなく、社内に蓄積された個人についての情報あるいは社外から増補された個人情報を事業促進のため、あるいは、人事管理などの事業業務の処理のために、個人情報を活用している事業者(経営体)を言い、個人情報の件数の大小があるかもしれないが、ほとんどの事業者は、「個人情報取り扱い事業者」といってよい。

#### 例外

- 1:個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6ヶ月以内のいずれの日においても5000人を超えない企業。
- 2:カーナビ、電話帳のような他人の作成による氏名、住所又は電話番号のみを含んでいる個人情報データベースで、新たに個人情報を加えたり、他の個人情報を付加したりして、データベースそのものを変更するようなことをせずに、事業の用に供する場合は、その個人情報データベース等に含まれる個人の数は、上記 1の「特定の個人の数」には算入しない。

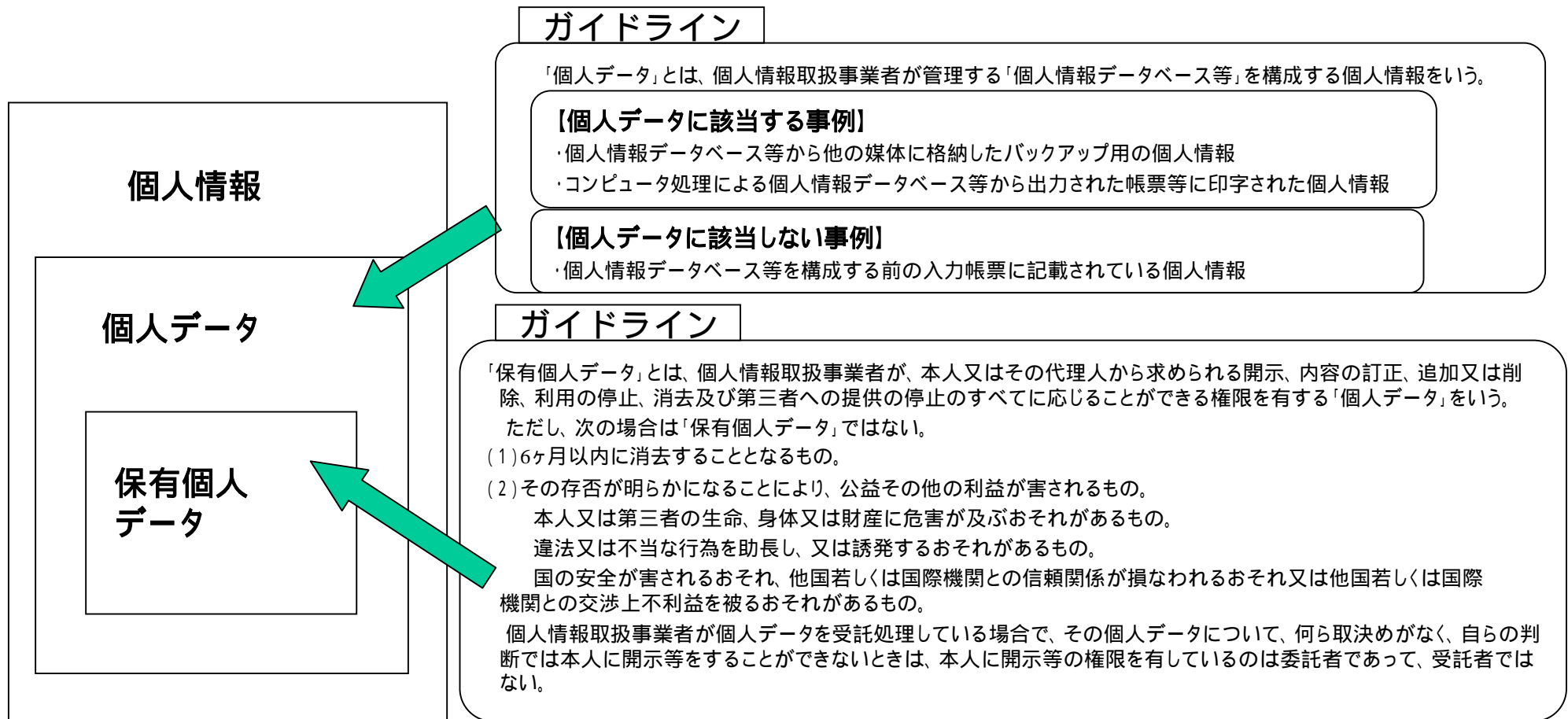
#### 【特定の個人の数に算入しない事例】

- ・電話会社より提供された電話帳および市販の電話帳CD-ROM等に掲載されている氏名及び電話番号
- ・市販のカーナビゲーションシステム等のナビゲーションシステムに格納されている氏名、住所又は居所の所在場所を示すデータ
- ・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、その情報の中に含まれる個人情報

## 1 - 4 個人データ・保有個人データ

法第2条第4項 この法律において「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。

法第2条第5項 この法律において「保有個人データ」とは、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であって、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で定めるもの又は1年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。



## 1 - 5 その他の定義

---

1) 「本人」(法第2条第6項)

個人情報によって識別される特定の個人をいう

2) 「本人に通知」(法第18条第1項)

本人にその利用目的を直接知らしめることをいう

(事例) 面談では、口頭でまたは文書で知らせる

電話では、口頭または自動応答装置などで知らせる

ファックス、電子メールで文書を送信して知らせる

郵送して知らせる

3) 「公表」(法第18条第1項)

広く一般に自己の意思を本人にとって合理的かつ適切な方法で知らしめることをいう

(事例) ポスターなどでの店内掲示、通信販売用パンフレット、自社ホームページ

4) 「本人に対し、その利用目的を明示」(法第18条第2項)

本人に対し、その利用目的を本人にとって合理的かつ適切な方法でもって明確に示すことをいう

(事例) 利用目的を明記した契約書やその他の書面を本人に手渡すまたは送付する

自社のホームページ画面に明記する

個人情報をネットワーク上で取得する場合は、本人が個人データを送信する前に、その利用目的を

明瞭に読み取れるように文字のサイズ・色・配置に留意する

## 1 - 5 その他の定義

- 5)「本人の同意」(法第16条第1項)  
本人の個人情報、個人情報取扱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(但し、本人であることを確認できていることが必要)  
(事例)同意する旨を本人から口頭または書面(データ媒体を含む)で確認する  
署名または記名捺印した同意を明記した申し込み書等の文書を受領・確認する  
メールで同意の旨を受信する  
同意する旨のウェブ画面上のボタンをクリック  
同意確認欄へのチェック、音声入力、タッチパネルへのタッチでの同意表明
- 6)「本人が容易に知り得る状態」(法第23条第2項)  
本人が知ろうとすれば、時間的にも、その手段においても本人に認識される合理的かつ適切な方法によって簡単に知ることができる状態にしていることをいう  
(事例)広報紙などの定期刊行物への定期掲載  
事務所の見易い場所での継続的な掲示や備え付け  
ウェブ画面のトップページから、1回程度の容易な操作で到達できる場所への継続的な掲示
- 7)「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)」(法第24条第1項)  
本人が知ろうとすれば知ることができる状態にしていることをいう  
(事例)問合せ窓口を設けて、問合せがあれば、口頭または書面で回答できる体制を整えておく  
パンフレットを店舗内の分かりやすい場所に備え付けておく  
電子商取引で、問合せ先のアドレスやホームページを明記する
- 8)「提供」(法第23条第1項)  
個人データを利用可能な状態におくことをいう  
(事例)個人データが一見物理的に提供されていない場合であっても、ネットワークを利用することにより、個人データを利用できるのであれば、「提供」にあたる

## 2. 個人情報取扱事業者の義務

法第15条から法第36条に個人情報取扱事業者の義務が定められている。

事業者の義務のうち、特に、「利用目的の特定、通知・公表」、「安全管理措置」、「従業員の監督」、「委託先の監督」、「第三者提供の制限」については、義務の中核となることから、できるだけ具体的に取るべき措置を示す。

### 1. 利用目的による制限等

利用目的をできる限り特定しなければならない。(第15条)

利用目的の達成に必要な範囲を超えて取り扱ってはならない。(第16条)

### 2. 適正な取得、正確性の確保、安全管理措置等

偽りその他不正の手段により取得してはならない。(第17条)

取得したときは利用目的を通知又は公表しなければならない。(第18条)

正確かつ最新の内容に保つよう努めなければならない。(第19条)

安全管理のために必要な措置を講じなければならない。(第20条)

漏えい時の被害・事業の性質・リスクに応じた、必要かつ適切な措置であること

従業者・委託先に対し必要な監督を行わなければならない。(第21、22条)

### 3. 第三者提供の制限

本人の同意を得ずに第三者に提供してはならない。(第23条)

例外: オプトアウト(本人の求めに応じて提供を停止できることとしている場合)

### 4. 本人の関与

利用目的等を本人の知り得る状態に置かなければならない。(第24条)

本人の求めに応じて保有個人データを開示・訂正・利用停止等を行わなければならない。(第25条～第27条)

### 5. 苦情の処理

苦情の適切かつ迅速な処理に努めなければならない。(第31条)

## 2. 個人情報取扱事業者の義務

### 2 - 1 利用目的の特定

法第15条第1項 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。  
第2項 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。

#### ガイドライン

利用目的の特定に当たっては、可能な限り具体的に特定すること。個々の処理の目的を特定するにとどめるのではなく、個人情報取扱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特定する必要がある。

単に「当社の事業活動」、「お客様のサービスの向上」等を利用目的とすることは、特定したことにはならない。

例示すれば、「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、具体的な利用目的とする。

事業の特定に当たっては、社会通念からも、本人から見ても妥当であることが望ましい。例えば、日本標準産業分類の中分類から小分類程度の分類が参考になる。

#### 【具体的に利用目的を特定している事例】

- ・「事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用致します。」
- ・「ご記入頂いた氏名、住所、電話番号は、名簿として販売することがあります。」
- ・情報処理サービスを行っている事業者の場合は、「給与計算処理サービス、宛名印刷サービス、伝票の印刷・発送サービス等の情報処理サービスを業として行うために、委託された個人情報を取り扱います。」のようにすれば利用目的を特定したことになる。

#### 【具体的に利用目的を特定していない事例】

- ・「当社の事業活動に用いるため」、「当社の提供するサービスの向上のため」、「当社のマーケティング活動に用いるため」

## 2. 個人情報取扱事業者の義務

### 2 - 2 利用目的の変更

法第15条第2項 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。

法第18条第3項 個人情報取扱事業者は、利用目的を変更した場合には、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。

#### ガイドライン

特定された利用目的は、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が可能である。変更された利用目的は、本人に通知するか、公表しなければならない。

#### 【本人が想定することが困難でないと認められる範囲内に該当する事例】

・「当社のおこなう 事業において、新商品や新サービスに関する情報を電子メールで送信することがあります。」という利用目的に、「郵便によりお知らせすることがあります。」と追加することは許される。

### 2 - 3 利用目的による制限

法第16条第1項 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。

#### ガイドライン

個人情報取扱事業者は、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。同意を得るため、本人に電話をかけたリメールを送信したりすることは目的外利用には当たらない。

#### 【本人の同意が必要な事例】

・就職試験に提出された履歴書の情報をもとに、当社の商品や新サービスを掲載しているカタログと注文書を送る場合

## 2. 個人情報取扱事業者の義務

### 2 - 4 適正な取得

法第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。

#### ガイドライン

取得目的を伏せて取得したり、十分な判断能力を持っていない子供から親の同意を得ることなく家族の個人情報を取得したりしてはならない。

#### 【不正な手段による取得の事例】

- ・第三者提供制限(法第23条)違反をするよう強要して個人情報を取得した場合
- ・他の事業者に不正な手段で個人情報を取得することを指示して、その事業者から個人情報を取得する場合

不正の競争の目的で、秘密として管理している事業上有用な個人情報を詐欺等で取得したり、使用・開示したりした場合は、その者には不正競争防止法(平成5年)第14条により刑事罰(3年以下の懲役または300万円以下の罰金)が科される

法第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。

#### ガイドライン

個人情報取扱事業者は、個人情報データベース等の入力時の照合・確認の手続きの整備、誤りを発見したときの訂正の手続きの整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを性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。

#### 【注意】

- ・保有するデータを一律にまた常に最新にしておく必要はない。それぞれの目的に応じて、必要な範囲で正確性と最新性が保たれていればよい。

## 2. 個人情報取扱事業者の義務

### 2 - 5 利用目的の通知・公表

法第18条第1項 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。

第2項 個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面(中略)に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された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。(以下略)

#### ガイドライン

個人情報取扱事業者は、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、又は公表しなければならない。

##### 【本人に通知又は公表が必要な事例】

・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      ・個人情報の第三者提供を受ける場合

個人情報取扱事業者は、書面等による記載、ユーザー入力画面への打ち込み等により、直接本人から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。

##### 【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】

・申込書・契約書に記載された個人情報を本人から直接取得する場合  
・アンケートに記載された個人情報を直接本人から取得する場合      ・懸賞の応募はがきに記載された個人情報を直接本人から取得する場合

注意: ポイントカードなどカード会員の入会時申込書に記入されている情報は、その利用目的を申込書に記載して、明示すること。

## 2. 個人情報取扱事業者の義務

### 適用除外

以下のような場合には、本人の同意を得ることが求められていても、その適用を受けない

#### ・法第16条第3項において

以下のような場合には、利用目的による制限において本人の同意を得ることが求められる場合でも適用をうけない。

##### (1) 法令に基づく場合

刑事訴訟法第18条（令状による捜査）、地方税法第72条の63（事業税に係わる質問検査権）

##### (2) 人の生命、身体または財産の保護の場合

急病を訴えるお客さまを救急車等で病院へ搬送するにあたって、本人の家族、その連絡先、血液型などを医師、看護師、救急隊員へ提供する場合や業務妨害をおこなう者の情報について私企業間で交換する場合

##### (3) 公衆衛生の向上を目的とする場合

健康保険組合などの被保険者の健康診断や精密検査の結果を健康増進策の「立案」「施策の効果検証」に資するため、個人の名称等を伏せて研究者や研究機関へ提供する場合

##### (4) 国の機関等への協力

事業者が税務署の職員等の任意調査や警察署員等の任意調査において、個人情報の提供を求められた場合

#### ・法第18条第4項において

以下のような場合には、「利用目的の通知又は公表」「直接書面等による取得」「利用目的の変更」において本人の同意を得ることが求められる場合でも適用を受けない。

##### (1) 本人または第三者の利益権利を侵害するおそれのある場合

利用目的を本人に通知し、または公表することによって、到って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ことが予想され場合。総会屋の個人情報や不当要求の防止のために収集し、企業間で交換しているときに、情報提供者が総会屋関係者から脅迫を含む被害を被る場合などがこれにあたる

##### (2) 会員企業の権利等が侵害される場合

利用目的を通知・公表することを通して、企業機密が外部に明らかになる場合。営業のノウハウが漏れ伝わる場合など

##### (3) 利用目的が自明な場合

ギフト伝票に記入していただいたお名前、住所、電話番号等の情報を配送指図をおこなうためにのみ使用する、あるいはお問合せのために販売関係従業員がメモ・備忘録としてあつかう場合

## 2 - 6 安全管理措置

法第20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。

### ガイドライン

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、**組織的、人的、物理的、及び技術的の安全管理措置**を講じなければならない。

その際、本人の個人データが漏えい、滅失又はき損等をした場合に、本人が被る権利利益の侵害のリスクとその大きさを考慮して、必要かつ適切な措置を講じる。

被る不利益(リスク)には、次のようなものが想定される。

- ・あるべき、残っているべき情報が消滅した
- ・外部に漏洩された情報が金銭取引の対象になった
- ・情報の、データの原型が歪曲された、破壊された
- ・秘匿されている情報が外部に漏れる、盗用された
- ・情報、データは有用でなくなる、使用不可能になった

### **組織的の安全管理措置**

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を整備し、それらに基づき運用し、その実施状況の確認を行うことをいう。個人データ取扱台帳の整備、安全管理措置の評価、見直し及び改善を含む。事故や違反が生じた場合、事実関係を速やかに調査しその結果や再発防止策を公表することが望まれる。

### **人的の安全管理措置**

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・訓練などを行うことをいう。

### **物理的の安全管理措置**

従業者や外部関係者の入退館(室)の管理、個人データの盗難の防止、機器・装置等の物理的な保護などの措置をいう。

### **技術的の安全管理措置**

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。情報を取り扱う従業者の権限・情報システムへのアクセスについてのさまざまな対策やデータの移送・通信時の対策 などを含む。

## 2 - 6 安全管理措置

### **組織的安全管理措置**

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)を整備し、それらに基づき運用し、その実施状況の確認を行うことをいう。個人データ取扱台帳の整備、安全管理措置の評価、見直し及び改善を含む。事故や違反を想定した備えを取っておくことも含む。

#### 具体的な措置例

- ・個人情報の安全管理を進める「個人情報保護管理者」を任命する
- ・個人情報の保護を宣言した企業方針(コンプライアンス)に照らして、企業内部の管理運用を監査し改善を提案する「個人情報保護監査責任者」を任命する
- ・個人情報の取り扱いを委託している委託先との間で、個人情報についての責任の範囲や従業員教育の定期実施などの取り決めを定める
- ・個人情報を機密重要度の観点から、極秘、部外秘、社外秘に分類し、情報の漏洩が事業に与える影響を大・中・小に分類し、現在の管理方法の弱い点を分析して改善策をたてておく

### **人的安全管理措置**

従業者および委託先に対する、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・訓練などを行う。

#### 具体的な措置例

- ・個人情報保護管理者あるいはそれに代わる役職者は、つぎの内容を中心とした教育訓練を継続しておこなう
  - 立法遵守(コンプライアンス)の重要性と利点
  - コンプライアンスに適應するために果たさなくてはならない責任と役割分担
  - コンプライアンスに違背したときにおこりうる社会的ダメージ
- ・従業者の採用時または委託契約時における非開示契約には、「契約終了後もその契約は一定期間有効である」とすることが望ましい。従業者ではないが、清掃・警備関係者、情報システム開発者・保守者など、個人データを保有している建物や情報機器に接近できる可能性のある場合を想定して、アクセス可能な関係者の範囲の特定、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。

## 2 - 6 安全管理措置

### **物理的安全管理措置**

従業者や外部関係者の入退館(室)の管理、個人データの盗難の防止、機器・装置等の物理的な保護などの措置をいう。

具体的な事例

- ・来訪者がすぐに目に出来る場所に、情報が含まれるコンピューターを設置しない
- ・情報やデータが集中して保管されている、いわゆるコンピューター室への入退室について、特定した従業者に限ってしか入室を許さない、従業者カードを使った入退室管理装置やシステムを用意する
- ・個人情報・データを保管する書庫、書棚には施錠をする。
- ・企業事務所等で使用するパソコンを従業者が自宅等へ持ち出すことを禁止する。同様に、媒体を持ち帰ることを禁ずる。
- ・個人データを取り扱う機器・装置等の、盗難・破壊・破損などの脅威や火災・被水・停電による被害から、物理的に保護を講じる。

### **技術的安全管理措置**

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(情報やデータベースを保持するコンピューターの操作開始)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。ネットワーク上でのデータの移送・通信、データを収録するCD、MD、メモリースティックの携帯移動についての対策を含む。

【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者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、同一又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者が使用できる端末又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者数の最小化
- ・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、識別されていないことになる。このような場合は、パスワードを知っている者が特定され、かつ、アクセス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)
- ・アクセスには、操作者固有の数字やアルファベットで構成されるコードを定め、操作者にそのコードの使用の強制
- ・従業者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、ファイアウォール、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者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望ましい。

## 【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

- ・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)
- ・侵入破壊する行為に対し、不正侵入を防ぐファイアウォール(防護壁)の設定

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又は運用環境のセキュリティが損なわれないことの検証

## 【各項目について講じることが望まれる事項】

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
- ・データの複写について、万一のための退避や二重保持(バックアップ)を目的とする以外の、禁止
- ・データやデータベースをコピーして外部作業に役するために、帯行できる各種媒体の使用の制限や特定条件化
- ・期限の切れたデータを廃棄する際、紙類の断裁処理、磁気媒体の専用ツール消去、磁気ファイルの完全消去
- ・パソコンや小型コンピューターの廃棄には、内部のハードディスクの取り出しと破壊を行って廃棄する

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可能性があることに留意する。

## 2 - 7 従業員の監督

法第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。

### ガイドライン

個人情報取扱事業者は、法第20条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない。  
のみならず、従業者に適切な教育訓練をほどこさなくてはならない。

「従業者」とは、個人情報取扱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主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)ばかりでなく、取締役、執行役、顧問、理事、監査役、監事、派遣社員も含まれる。

【従業者に対して必要かつ適切な監督を行っていない場合】

- ・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、定期的に確認せず、結果、個人データが漏えいした場合
- ・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を繰り返し持ち出し、それを放置した結果、紛失し、個人データが漏えいした場合

【従業者のモニタリングを実施する上での留意点】

個人データの取り扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング(以下「モニタリング」という)を実施する場合は、次の点に留意する。

- ・モニタリングの目的、即ち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
- ・モニタリングの実施に関する責任者とその権限を定めること。
- ・モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内  
に徹底すること。
- ・モニタリングの実施状況については、適正に行われているか監査、又は確認を行うこと。

## 2 - 8 委託先の監督

法第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。

### ガイドライン

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、法第20条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければならない。

「必要かつ適切な監督」には、委託契約において委託者である個人情報取扱事業者と受託者が同意した安全管理措置の内容を契約に盛り込むとともに、当該契約の内容が遵守されていることを、予め定めた間隔で定期的に確認することも含まれる。

委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は十二分な注意をする必要がある。

#### 【受託者に必要かつ適切な監督を行っていない場合】

- ・個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えい。
- ・個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えい。
- ・再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えい。

#### 【個人データの取扱いを委託する場合に契約書への記載が望まれる事項】

委託者及び受託者の責任の明確化

個人データの取扱状況に関する委託者への報告の内容及び頻度

個人データの安全管理に関する事項

- ・個人データの漏えい防止、盗用禁止に関する事項
- ・委託契約範囲外の加工、利用の禁止
- ・委託契約範囲外の複写、複製の禁止
- ・委託処理期間
- ・委託処理終了後の個人データの返還・消去・廃棄に関する事項

再委託に関する事項

- ・再委託を行うにあたっての委託者への文書による報告

契約内容が遵守されていることの確認 契約内容が遵守されなかった場合の措置

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

## 2 - 9 第三者への提供

第23条 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

第2項 個人情報取扱事業者は、第三者に提供される個人データについて、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としている場合であって、次に掲げる事項について、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は、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

### ガイドライン

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、個人データを第三者に提供してはならない。同意の取得に当たっては、事業の性質及び個人データの取扱い状況に応じ、本人が同意に係る判断を下す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すこと。

#### 【第三者提供とされる事例】

- ・親子兄弟会社、グループ会社の間で個人データを交換する場合
- ・同業者間で、特定の個人データを交換する場合
- ・フランチャイズ組織の本部と加盟店の間で個人データを交換する場合(\*)
- ・外国の会社に国内に居住している個人の個人データを提供する場合

#### 【第三者提供とされない事例】

- ・同一事業者内で他部門へ個人データを提供すること。

ただし、以下の場合には本人の同意なく第三者への提供を行うことができる。

- ・法令に基づいた個人データを提供する場合

事例) 法第42条第2項に基づき認定個人情報保護団体が対象事業者に資料提出等を求め、対象事業者がそれに応じて資料提出をする場合

・人(法人を含む。)の生命又は財産といった具体的な権利利益が侵害されるおそれがあり、これを保護するために個人データの提供が必要であり、かつ、本人の同意を得ることが困難である場合(他の方法により、当該権利利益の保護が十分可能である場合を除く。)

・公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合(他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。)

・国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であって、協力する民間企業等が当該国の機関等に個人データを提供することについて、本人の同意を得ることが当該事務の遂行に支障を及ぼすおそれがある場合

個人情報取扱事業者は、第三者提供におけるオプトアウトを行っている場合には、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。

「第三者提供におけるオプトアウト」とは、提供にあたりあらかじめ、以下の . ~ . の情報を、本人に通知し、又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。

- . 第三者への提供を利用目的とすること。
- . 第三者に提供される個人データの項目
- . 第三者への提供の手段又は方法
- . 本人の求めに応じて第三者への提供を停止すること。

\* ポイントカード(ハウスカード)入会時に利用目的として「この会員情報に基づきXXスーパー本部、各店、FC店(別法人)より会員各位に特売情報、季節買物情報を提供いたします。(詳細はホームページに掲載いたします)」と明記する。このようにカード情報の共同利用を会員に同意を得ることで第三者提供とならない。

#### 【オプトアウトの事例】

- . 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))
- . 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)

### 雇用管理に関する個人データ関連

個人データの第三者への提供のうち、雇用管理に関するものについては、次に掲げる事項に留意することが望ましい。

ここでいう雇用管理に関する個人データの第三者への提供とは、従業員の子会社への出向に際して、出向先に当該従業員の人事考課情報等の雇用管理に関する個人データを提供する場合や、労働者を派遣する際に技術者の能力に関する情報等の雇用管理に関する個人データを提供する場合を指すものである。

したがって、企業から、その従業員の氏名、役職等の個人データの提供を受け、当該情報をデータベース化し、公開、販売することを目的とする者への提供のような場合はこの限りではない。

- . 提供先において、その従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし、又は盗用してはならないこととされていること。
- . 当該個人データの再提供を行うに当たっては、あらかじめ文書をもって事業者の了承を得ること。
- . 提供先における保管期間等を明確化すること。
- . 利用目的達成後の個人データを返却し、又は破棄し若しくは削除し、これと併せてその処理が適切かつ確実になされていることを事業者において確認すること。
- . 提供先における個人データの複写及び複製(安全管理上必要なバックアップを目的とするものを除く。)を禁止すること。

## 2 - 10 第三者への提供の例外

法第23条第4項 次に掲げる場合において、当該個人データの提供を受ける者は、前3項の規定の適用については、第三者に該当しないものとする。

第1号 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場合。

第3号 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、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。

### ガイドライン

#### **委託**

個人データの取扱いに関する業務の全部又は一部を委託する場合は、第三者に該当しない。個人情報取扱事業者には、委託先に対する監督責任が課される

#### **【業務の委託の事例】**

・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渡す場合      ・百貨店が注文を受けた商品の配送のために、宅配業者に個人データを渡す場合

#### **事業の承継**

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は、第三者に該当しない。  
但し、事業の承継後も、個人データが譲渡される前の利用目的の範囲内で利用しなければならない。

#### **【事業の承継の事例】**

事例1) 合併、分社化により、新会社に個人データを渡す場合  
事例2) 営業譲渡により、譲渡先企業に個人データを渡す場合

## 共同利用

個人データを特定の者との間で共同して利用する場合、以下のア)～エ)の情報を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おくとともに、共同して利用することを明らかにしている場合は、第三者に該当しない。

ア)共同して利用される個人データの項目

イ)共同利用者の範囲(本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。)

ウ)利用する者の利用目的(共同して利用する個人データのすべての利用目的)

エ)開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等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

### 【共同利用を行うことがある事例】

・グループ企業で総合的なサービスを提供するために利用目的の範囲内で情報を共同利用する場合

法第23条第5項 個人情報取扱事業者は、前項第3号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

上記ア)イ)については、変更することができないが、ウ)エ)については、社会通念上、本人が想定することが困難でないと認めれる範囲内で変更することができ、変更する前に、本人に通知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。

## 2 - 11 保有個人データの公表・開示

法第24条第1項 個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、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。個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。一～四(略)

法第25条第1項 個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示(当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。)を求められたときは、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。(以下略)

法第26条第1項 個人情報取扱事業者は、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当該保有個人データの内容の訂正、追加又は削除(以下この条において「訂正等」という。)を求められた場合には、(中略)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。

法第27条第1項 個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第16条の規定に違反して取り扱われているという理由又は第17条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去(以下この条において「利用停止等」という。)を求められた場合であって、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。

### ガイドライン

個人情報取扱事業者は、保有個人データについて、一定の情報を本人の知り得る状態に置かねばならない。

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。なお、保有個人データの全部または一部について開示しない旨の決定をしたときは、本人に対し、遅滞無く、その旨を通知しなければならず、併せてその理由を説明するように努めなければならない。

個人情報取扱事業者は、本人から、保有個人データに誤りがあり、事実でないという理由によって訂正等を求められた場合には、原則として、訂正等を行い、訂正等を行った場合には、その内容を本人に対し、遅滞なく通知しなければならない。なお、保有個人データの訂正をしない旨の決定をしたときは、本人に対し、遅滞無く、その旨を通知しなければならず、併せてその理由を説明するように努めなければならない。

個人情報取扱事業者は、本人から、手続違反の理由により保有個人データの利用停止等が求められた場合には、原則として、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。また、保有個人データまたは一部について利用停止しない旨の決定をしたときは、本人に対し、遅滞無く、その旨を通知しなければならず、併せてその理由を説明するように努めなければならない。

保有個人データに関する事項の公表

保有個人データの本人への開示

保有個人データの訂正・利用停止

## 2 - 11 保有個人データの公表・開示

### ガイドライン

個人情報取扱事業者は、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。なお、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ず、併せてその理由を説明するよう努めなければならない。

あらかじめ本人の同意を得ず、第三者に提供されているという理由によって、保有個人データの第三者提供の停止を求められた場合には、原則として、当該措置を行わなければならない。なお、第三者提供を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ず、併せてその理由を説明するよう努めなければならない。

開示等の求めに応じる手続(法第29条関連)

#### 法第29条第1項

個人情報取扱事業者は、第24条第2項、第25条第1項、第26条第1項又は第27条第1項若しくは第2項の規定による求め(以下この条において「開示等の求め」という。)に関し、政令で定めるところにより、その求めを受け付ける方法を定めることができる。この場合において、本人は、当該方法に従って、開示等の求めを行わなければならない。

#### 法第29条第2項

個人情報取扱事業者は、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、個人情報取扱事業者は、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。

#### 法第29条第3項

開示等の求めは、政令で定めるところにより、代理人によってすることができる。

#### 法第29条第4項

個人情報取扱事業者は、前3項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、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。

個人情報取扱事業者は、開示等の求め 1において、その求めを受け付ける方法として下記の . ~ .の事項を定めることができる。

. 開示等の求めの受付先

- . 開示等の求めに際して提出すべき書面(電子的方式、磁気的方式その他、人の知覚に よっては認識することができない方式で作られる記録を含む。)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)
- . 開示等の求めをする者が本人又はその代理人((ア)未成年者又は成年被後見人の法定代理人、(イ)開示等の求めをすることに つき本人が委任した代理人)であることの確認の方法(ただし、確認の方法は、事業の性質、保有個人データの取扱状況、開示等の求めの受付方法等に応じ、適切なものでなければならない。)

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

. 保有個人データの利用目的の通知、又は保有個人データの開示をする際に徴収する手数料の徴収方法

なお、開示等の求めを受け付ける方法を定めない場合には、自由な申請を認めることとなる。

個人情報取扱事業者は、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。

個人情報取扱事業者は、開示等の求めに応じる手続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。

## 手数料(法第30条関連)

### 法第30条第1項

個人情報取扱事業者は、第24条第2項の規定による利用目的の通知又は第25条第1項の規定による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。

### 法第30条第2項

個人情報取扱事業者は、前項の規定により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。

個人情報取扱事業者は、保有個人データの利用目的の通知、又は保有個人データの開示を求められたときは、当該措置の実施に関し、手数料の額を定めることができる。また、手数料の額を定めた場合には、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。

なお、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。

## 苦情の処理(法第31条関連)

### 法第31条第1項

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。

### 法第31条第2項

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。

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。また、苦情の適切かつ迅速な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。もっとも、無理な要求にまで応じなければならないものではない。

## 3. その他

### 3 - 1 経過措置

#### ガイドライン

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(取得に際しての利用目的の通知等)の規定は適用されない。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(28, 29ページ参照)を講ずる必要がある。

### 3 - 2 ガイドラインの見直し

#### ガイドライン

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて毎年見直しを行うよう努めるものとする。

### 3 - 3 参考となる事項・規格

#### ガイドライン

個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのコンプライアンス・プログラムを策定し、実施し、維持し及び改善を行うことが望ましい。

なお、その体制の整備に当たっては、日本工業規格 JISQ15001「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」を、個人データの安全管理措の実施に当たっては、日本工業規格 JISX5070「セキュリティ技術 - 情報技術セキュリティの評価基準」及び日本工業規格 JISX5080「情報セキュリティマネジメント」実践のための規範」等を参考にすることができる。

また、個人情報取扱事業者は、「個人情報保護に関する考え方や方針に関する宣言(いわゆる、プライバシーポリシー、プライバシーステートメント等)」を策定し、ウェブ画面への掲載等により公表することが望ましい。

## 4. スーパーマーケット業で一般的な個人情報

代表的なものをあげると、

1. お中元、お歳暮の受注伝票の記載情報  
送り元顧客 氏名、住所、電話番号  
送り先お相手 氏名、住所、電話番号
2. ポイントカードシステムなどの会員情報  
氏名、住所、電話番号、  
そのほかに、 職業、勤続年数、家族構成、住居所有、来店手段
3. 注文(オーダー)品の注文伝票の記載事項
4. 万引き防止のカメラ情報  
売り場の天井に設置しているカメラで撮影している顧客の画像(但し、画像が保存されない仕掛けであれば、個人データに当たらない)
5. 宅配会員情報  
お客さまのご自宅へご注文品を定期的に配達する仕組みを動かしている場合に、お客さまから記載してもらった以下の情報  
氏名、自宅(配達先)住所、住居所有の形態、電話番号、勤務先名、年収、  
宅配販売商品代金の回収のための金融機関の自動引き落とし口座
6. 掛売りのお客さまの情報  
飲食業を営む大口のお客さまを中心として、その販売代金を販売都度の精算でなしに、月に1,2度の支払を約束する掛売りをおこなっている場合の以下の情報  
氏名、業種(営業形態)、屋号、配達先住所、自宅住所、住居所有の形態、電話番号、年収、  
販売商品代金の回収のための金融機関の自動引き落とし口座
7. お取引先を組織化した会の名簿  
名称は、多種あるが、お取引先との情報交流など目的とした非事業組織として、多くの会員企業において存在する  
お取引先名称、代表者名、担当役職者名、部署名、住所、電話番号、ファックス番号  
そのほかに、取引先金融機関名、口座や取引金額等をメモとして、記入している例がある

---

特に、注意を要するものとして

2. ポイントカードシステムなどの会員情報

ほとんどの企業では、会員カードシステムの管理を外部事業者へ委託している。

カードの作成から始まって、会員募集と更新、ポイントの付与と還元方法など、複雑なシステムの企画を自社の社員では担えないといったことが委託する理由であろう。

会員マスター情報を中心に、情報のすべてが委託先のコンピューターの存在していることから、委託契約先との間の個人情報の管理を厳重に取り決め、定期的な点検を行うとともに、委託先の従業者に対する教育の定期的な実施をする。

委託先に個人情報の廃棄を委任する場合は、廃棄処分書の取り交わしなどを習慣化することにしたい。

ポイントカードの入会時申込書に利用目的を印字するなどして、本目的以外に流用しないことを明示することを努めたい。

5. 宅配会員情報、6. 掛売りのお客さま情報

販売代金の回収保全のために、会員の収入、住居所有形態、代金引き落とし金融機関口座の記載を求めている場合、それらの情報は、個々の会員・顧客にとって極秘中の極秘事項であるので、その取扱には慎重にも慎重を期さなければならない。