

<ダイレクトセリング業界の個人情報保護ガイドライン>

公益社団法人日本訪問販売協会

目 次

	頁
「ダイレクトセリング業界の個人情報保護ガイドライン」の改正にあたり	3
第1章：ガイドラインの目的	4
第1条（目的）	4
第2章：定義	5
第2条（ガイドラインにおける用語の定義）	5
第3章：ガイドラインの適用範囲	15
第3条（適用範囲とガイドラインへの準拠）	15
第4章：事業者の義務等	17
第1節：内部規程の策定及び保護方針の公表に関する措置	17
第4条（個人情報保護方針の公表等）	17
第5条（内部規程の策定等）	18
第2節：個人情報の取得等に関する措置	20
第6条（利用目的の特定）	20
第7条（利用目的による制限）	21
第8条（適正な取得）	24
第9条（利用目的の通知又は公表）	25
第10条（書面等により本人から直接に個人情報を取得する場合の措置）	27
第11条（利用目的の変更時の措置）	28
第12条（取得時及び利用目的等の変更時の措置の適用除外）	29
第3節：個人情報の管理に関する措置	30
第13条（個人データの正確性の確保）	30
第14条（安全管理措置）	30
第15条（従業員の監督）	44
第16条（委託先の監督）	45
第17条（連鎖販売業におけるビジネス参加者に対する措置）	48
第4節：個人情報の提供に関する措置	49
第18条（第三者提供の制限）	49
第19条（第三者に提供できる場合）	50
第20条（第三者提供に該当しない場合）	51
第5節：開示・変更・利用停止等の求めに関する措置	54
第21条（保有個人データに関する事項の公表等）	54
第22条（開示）	56

第 23 条（訂正等）	57
第 24 条（利用停止等）	58
第 25 条（理由の説明）	59
第 26 条（開示等の求めに応じる手続き）	60
第 6 節：苦情対応に関する措置	62
第 27 条（苦情への対応）	62
第 7 節：個人情報保護の適正管理義務に関する措置	63
第 28 条（個人情報保護管理者の設置）	63
第 29 条（個人情報保護管理者の責務）	64
第 8 節：緊急時における連絡体制の確立に関する措置	65
第 30 条（関係機関への連絡）	65
第 31 条（報告等）	66
第 9 節：経過措置	67
第 32 条（本人の同意に関する経過措置）	67
第 33 条（通知に関する経過措置）	67
第 10 節：個人情報保護体制の見直しに関する措置	68
第 34 条（事業者における個人情報保護体制の見直し）	68
 第 5 章：ガイドラインの見直し	 70
第 35 条（ガイドラインの見直し）	70
附則	

「ダイレクトセリング業界の個人情報保護ガイドライン」の改正にあたり

平成17年4月に個人情報保護法が全面施行されてから、すでに4年半が経過し、個人情報保護に係る事業者側の取組みも、当初の混乱状態・過剰反応などからすれば相当程度の整理がなされ、落ち着いた対応が行われるようになっております。

このように、個人情報保護に係る事業者側の取組みは進んでおりますが、依然として事業者からの情報漏えい事案が発生していることもまた事実で、委託先、再委託先に対して委託元が十分に監督を行っていなかったことが原因と考えられる事案（地方自治体の2次委託先から住民基本台帳の個人情報約5万5千件が漏えいした事案、大手印刷会社の3次委託先からクレジットカード情報を含む個人情報が約860万件漏えいした事案など。）が発生した際には、マスメディアを通して広く報道され、こうした状況を背景として我が国における個人情報を巡る国民の認識や社会情勢も変化がみられるようになりました。

このような状況を踏まえ、経済産業省では平成21年10月に「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」を改正し、“ガイドラインの共通化”“性質に応じた個人情報の取扱い”“事業承継に係るルールの明確化”“共同利用制度の利用普及に係る具体策”“不正取得の事例の追加”などを盛り込んだ改正ガイドラインを告示したところです。こうした見直しの作業は、業界ガイドラインにおいても同様に実施しなければなりません。社会を取り巻く情勢に合わせてのアップデート作業の必要性については、業界ガイドラインにも規定しているところです。幸いなことに訪問販売業界では大きな漏えい事故などは発生しておりませんが、個人データの記録された媒体を社外に持って出た際に、紛失してしまうといった、従業員の“うっかりミス”が原因の事案が、少なからず発生しております。

今回、以上のような状況を踏まえて、業界ガイドラインの見直しを行い、行政等の動きに合わせた改正作業を実施致しました。会員各位には、本改正の趣旨等を十分にご理解いただき、改正内容を踏まえて、その遵守徹底をお願いするとともに、非加盟の事業者につきましてもガイドラインに準じた取組みの実施について、ご理解並びにご協力を賜りますようお願い申し上げます。

平成22年1月
公益社団法人日本訪問販売協会

第1章：ガイドラインの目的

第1条（目的）

本ガイドラインは、個人情報の保護に関する法律（以下、「個人情報保護法」又は「法」という。）及びその他の関係法令に基づき、訪問販売業及び連鎖販売業（以下、この二業態を一括して「ダイレクトセリング」という。）における個人情報の適正な取扱いに関して基本的な事項を示し、各事業者がマネジメントシステムを策定する等、個人情報保護に関する法令を遵守するうえでの体制づくりを支援し、またそれを促進することで、個人情報を適切な保護のもとで有効に活用することにより、ダイレクトセリングの健全な発展に寄与することを目的とする。

＜解説＞

1) 訪問販売や連鎖販売取引のように店舗外での取引が基本となる業態では、販売員が消費者と対面で商談を進めるケースが大半を占めることから、販売員が直接に相手方消費者から入手した情報を記録して整理し、そうしたデータを基に消費者のニーズに合わせた付加価値の高いサービスを提供できるところが大きな特徴となっています。

こうした個人情報は事業者にとって貴重な資源であり、消費者にとっても利便性の向上など大きなメリットをもたらすものである半面、情報の漏洩事件等が相次いで発生するなど、近年はその安全管理に関しての不安感が社会全体に高まっており、個人情報保護法をはじめ、関係法令を遵守した適正な取扱いが事業者の義務として規定されるようになりました。

2) このガイドラインは、公益社団法人日本訪問販売協会（以下、「当協会」という。）の会員のうち、訪問販売及び連鎖販売取引を業とする事業者が、当該事業において個人情報の保護に関する法令を遵守するうえでの指針として示すものであり、各事業者がこのガイドラインを基に個人情報保護のためのマネジメントシステムを整備することを支援し、及び促進することで、顧客等の個人情報保護に係る権利利益を保護しつつそれを有効に活用することによりダイレクトセリング産業の振興に役立たせることを目的とするものです。

3) このガイドラインは、経済産業省が定める「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。）に沿って策定されています。経済産業省ガイドラインは、個人情報保護法第7条第1項に基づき平成16年4月2日に閣議決定された「個人情報の保護に関する基本指針」（平成20年4月一部変更）及び同法第8条に基づき、経済産業省が所管する分野及び同法第36条第1項により経済産業大臣が主務大臣に指定された特定の分野（以下「経済産業分野」という。）における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定められたもので、その後平成19年、20年に改正が行われ、また今回平成21年10月にも改正が行われています（本ガイドラインはこれらの経済産業省ガイドラインの改正内容に適応したものとして作成されています。）。

第2章：定義

第2条（ガイドラインにおける用語の定義）

本ガイドラインにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一 訪問販売、連鎖販売取引：

「訪問販売」とは、特定商取引に関する法律第2条に、「連鎖販売取引」とは、同法第33条にそれぞれ規定する取引形態をいう。

二 ダイレクトセリング：

「ダイレクトセリング」とは、訪問販売業と連鎖販売業の二業態を一括りにまとめて表現したものをいう。

三 個人情報：

「個人情報」とは、生存する「個人に関する情報」であって、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ものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない（ただし、安全管理措置（法第20条関連）の対策の一つとして、高度な暗号化等による秘匿化を講じることは望ましい。）。

なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。

また、「生存する個人」には日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため、法人等の団体そのものに関する情報は含まれない（ただし、役員、従業員等に関する情報は個人情報）。

四 個人情報データベース等：

「個人情報データベース等」とは、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、又はコンピュータを用いていない場合であっても、カルテや指導要録等、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をいう。

五 個人情報取扱事業者：

「個人情報取扱事業者」とは、国の機関、地方公共団体、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）で定める独立行政法人等、地方独立行政法人法（平成15年法律第118号）で定める地方独立行政法人並びにその取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ない

者を除いた、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。

ここでいう「取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ない者」とは、個人情報の保護に関する法律施行令（以下、「政令」という。）第2条の規定のとおり、その事業の用に供する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（当該個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等であって、次の各号のいずれかに該当するものを編集し、又は加工することなくその事業の用に供するときは、当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人数を除く。）の合計が過去6か月以内のいずれの日においても5千を超えない者とする。

1. 個人情報として次に掲げるもののみが含まれるもの

イ) 氏名

ロ) 住所又は居所（地図上又は電子計算機の映像面上において住所又は居所の所在の場所を示す表示を含む。）

ハ) 電話番号

2. 不特定かつ多数の者に販売することを目的として発行され、かつ、不特定かつ多数の者により随時に購入することができるもの又はできたもの

特定の個人数が5千を超えるか否かは、当該事業者の管理するすべての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数の総和により判断する。ただし、同一個人の重複分は除く。

ここでいう「事業の用に供している」の「事業」とは、一定の目的を持って反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものをいい、営利事業のみを対象とするものではない。

法人格のない、権利能力のない社団（任意団体）又は個人であっても事業者該当し得る。

六 事業者：

「事業者」とは、当協会の会員のうち、訪問販売及び連鎖販売取引を業として営む者であって、個人情報データベース等を当該事業の用に供している者をいう。

ここでいう「事業の用に供している」の「事業」とは、一定の目的を持って反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものをいい、営利事業のみを対象とするものではない。

七 個人データ：

「個人データ」とは、事業者が管理する「個人情報データベース等」を構成する個人情報という。

八 保有個人データ：

「保有個人データ」とは、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のすべてを行うことができる権限を有する「個人データ」をいう（受託して処理しているものは除く）。ただし、次の①又は②の場合を除く。

- ①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
- (1) 本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの
 - (2) 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もの
 - (3) 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又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
 - (4) 犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの
- ②6ヶ月以内に消去する（更新することは除く。）こととなるもの

九 本人：

このガイドラインにおいて個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

十 本人に通知：

「本人に通知」とは、本人に直接知らしめることをいい、事業の性質及び個人情報の取扱い状況に応じ、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。

十一 公表：

「公表」とは、広く一般に自己の意思を知らせること（国民一般その他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。ただし、公表に当たっては、事業の性質及び個人情報の取扱い状況に応じ、合理的かつ適切な方法によらなければならない。

十二 本人に対し、その利用目的を明示：

「本人に対し、その利用目的を明示」とは、本人に対し、その利用目的を明確に示すことをいい、事業の性質及び個人情報の取扱い状況に応じ、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。

十三 本人の同意：

「本人の同意」とは、本人の個人情報が、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。）。

また「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該事業者が認識することをいい、事業の性質及び個人情報の取扱い状況に応じ、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方法によらなければならない。

なお、個人情報の取扱いに関して同意したことによって生ずる結果について、十分な判断能力を有していない子ども及び成年被後見人などから同意を得る場合は、本人のほか法定代理人等からの同意を得るなどの配慮が必要である。

十四 本人が容易に知り得る状態：

「本人が容易に知り得る状態」とは、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。

十五 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。）：

「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。）」とは、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、又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、前号の「本人が容易に知り得る状態」及び本号の「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。

十六 提供：

「提供」とは、個人データを利用可能な状態に置くことをいう。個人データが、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。

十七 個人情報保護管理者：

「個人情報保護管理者」とは、本ガイドラインが適用される事業者の内部において、代表者により指名された者であって、個人情報保護に係るマネジメントシステムの実施及び運用に関する責任と権限をもつ者をいう。いわゆる CPO（チーフ・プライバシー・オフィサー）はこれに該当する。

<解説>

1) 「個人情報」の定義関係：

(1) 「他の情報と容易に照合することができ、・・・」とは、例えば通常の作業範囲において、個人情報データベース等にアクセスし、照合することができる状態をいい、他の事業者への照会を要する場合や、当該事業者内部でも取扱部門が異なる場合等であって照合が困難な状態を除きます。

(2) 個人情報に該当する場合及び該当しない場合に関して、経済産業省ガイドラインでは次のような具体的な事例を挙げています。

【個人情報に該当する事例】

事例1：本人の氏名

事例2：生年月日、連絡先（住所・居所・電話番号・メールアドレス）、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

事例3：防犯カメラに記録された情報等本人が判別できる映像情報

事例4：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 等のようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイイチローのメールアドレスであることがわかるような場合等）

事例5：特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報

事例6：雇用管理情報（会社が従業員を評価した情報を含む。）

事例7：個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できた場合は、その時点で個人情報となります。）

事例8：官報、電話帳、職員録等で公にされている情報（本人の氏名等）

【個人情報に該当しない事例】

事例1：企業の財務情報等、法人等の団体そのものに関する情報（団体情報）

事例2：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.jp。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。）

事例3：特定の個人を識別することができない統計情報

(3) 訪問販売や連鎖販売取引のような対面販売においては、個々の販売員において自己の顧客等の嗜好をデータとして整理しているケースがしばしば見受けられます。こうした個人の嗜好については、それが識別性を有する場合には「個人情報」に該当します。ただし市場調査等の統計目的で個人を特定しない形で行われる情報収集や、個人名を伏せるなど個人が特定できない態様で匿名化して取り扱う情報はこのガイドラインの対象となりません。

2) 「個人情報データベース等」の定義関係：

(1) 個人情報データベース等に該当する場合及び該当しない場合に関して、具体的には次のような事例を挙げることができます（経済産業省ガイドラインより。）。

【個人情報データベース等に該当する事例】

事例1：電子メールソフトに保管されているメールアドレス帳（メールアドレスと氏名を組み合わせた情報を入力している場合）

事例2：ユーザーID とユーザーが利用した取引についてのログ情報が保管されている電子ファイル（ユーザーID を個人情報と関連付けて管理している場合）

事例3：従業者が、名刺の情報を業務用パソコン（所有者を問わない。）の表計算ソフト等を用いて入力・整理し、他の従業員等によっても検索できる状態にしている場合

事例4：人材派遣会社が登録カードを、氏名の五十音順に整理し、五十音順のインデッ

クスを付してファイルしている場合

事例5：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】

事例1：従業者が、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いても、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

事例2：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

(2) ダイレクトセリング業界においては、いわゆる「顧客台帳」、「客先手控え」、「見込み客リスト」など紙ベースのファイリングされた情報がありますが、それらのデータベースは、一定の規則に従って整理・分類され、特定の個人情報を容易に検索できるように体系的に構成されて、目次、索引、符号等が付され、他人によっても容易に検索が可能な状態に置かれているものは「個人情報データベース等」に該当することとなります。

3) 「事業者」の定義関係：

(1) 個人情報保護法では、取り扱う個人情報の量及び利用方法によっては適用除外となる事業者の範囲を規定しており、政令により『事業の用に供する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月以内のいずれの日においても5千を超えない者』と定めています(5000人を超えるか否かは、当該事業者の管理するすべての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との総和により判断します。)。しかし、このガイドラインではダイレクトセリング業界の業況等を考慮し、第3条の解説2)に示すとおり、その取り扱う個人情報の量により適用除外となる事業者等を規定していません。

なお、政令では、市販のカーナビゲーションシステムや電話帳CD-ROM等にある個人情報を編集・加工することなく事業に使用するときは、それによって識別される特定の個人数は算入から除かれており、このガイドラインもそれに準じることとし、個人の権利利益を侵害するおそれが少ないと考えられるこれらの利用方法(次項4)「個人データ」の定義関係の(2)に解説する①～③の要件のすべてに該当する場合)以外の利用を行っていない場合は、ここでの事業者には該当しません。

(2) 上記(1)の「特定の個人の数に算入しない」具体的な事例としては次のようなものを挙げることができます(経済産業省ガイドラインより。)

【特定の個人の数に算入しない事例】

事例1：電話会社から提供された電話帳及び市販の電話帳CD-ROM等に掲載されている氏名及び電話番号

事例2：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(ナビゲーションシステム等が当初から備えている機能を用いて、運行経路等新たな情報等を記録する場合があ

ったとしても、「特定の個人の数」には算入しないものとする。）

事例3：氏名又は住所から検索できるよう体系的に構成された、市販の住所地図上の氏名及び住所又は居所の所在場所を示す情報

【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】

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

4)「個人データ」の定義関係：

(1) 個人データに該当する場合及び該当しない場合に関して、具体的には次のような事例を挙げることができます（経済産業省ガイドラインより。）。

【個人データに該当する事例】

事例1：個人情報データベース等から他の媒体に格納したバックアップ用の個人情報

事例2：コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

【個人データに該当しない事例】

事例：個人情報データベース等を構成する前の入力帳票に記載されている個人情報

(2) 政令では、市販のカーナビゲーションシステムや電話帳 CD-ROM 等にある個人情報を編集・加工することなく事業に使用する場合は、その利用方法からみて個人の権利利益を侵害するおそれが少ないと考えられることから、これによって識別される特定の個人数は、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数から除外されています。具体的には以下の三要件のすべてに該当する場合です（前項3）「事業者」の定義関係の（1）の解説もご覧ください。）。

①個人情報データベース等の全部又は一部が他人の作成によるものであること。

②氏名、住所・居所、電話番号のみが掲載された個人情報データベース等（例えば、電話帳やカーナビゲーション）であること、又は、不特定かつ多数の者に販売することを目的として発行され、かつ、不特定かつ多数の者により随時に購入することができる又はできた個人情報データベース等（例えば、自治体職員録、弁護士会名簿等）であること。

③事業者自らが、その個人情報データベース等を事業の用に供するに当たり、新たに個人情報を加えることで特定の個人を増やしたり、他の個人情報を付加したりして、個人情報データベース等そのものを編集・加工していないこと。

5)「保有個人データ」の定義関係：

(1) 個人情報保護法では、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のできる権限を有する個人データのうち、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（このガイドラインの第2条第1項第8号①の(1)から(4)を参照。）又は政令で定める短期間（6ヶ月以内）に消去されるものについては適用除外とされています。このガイドラインも個人情報保護法に準じて、この範囲の個人データについては適用対象としていません。

（2）「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の具体的事例は次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの】

事例：家庭内暴力、児童虐待の被害者の支援団体が、加害者（配偶者又は親権者）及び被害者（配偶者又は子）を本人とする個人データを持っている場合

【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もの】

事例1：いわゆる総会屋等による不当要求被害を防止するため、事業者が総会屋等を本人とする個人データを持っている場合

事例2：いわゆる不審者、悪質なクレマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人データを保有している場合

【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又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】

事例1：製造業者、情報サービス事業者等が、防衛に関連する兵器・設備・機器・ソフトウェア等の設計、開発担当者名が記録された個人データを保有している場合

事例2：要人の訪問先やその警備会社が、当該要人を本人とする行動予定や記録等を保有している場合

【犯罪の予防、鎮圧又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】

事例1：警察からの捜査関係事項照会や搜索差押令状の対象となった事業者がその対応の過程で捜査対象者又は被疑者を本人とする個人データを保有している場合

事例2：犯罪収益との関係が疑わしい取引（以下「疑わしい取引」という。）の届出の対象情報

6) 「本人に通知」の定義関係：

「本人に通知」の具体的な事例は次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【本人への通知に該当する事例】

事例1：面談においては、口頭又はチラシ等の文書を渡すこと。

事例2：電話においては、口頭又は自動応答装置等で知らせること。

事例3：隔地者間においては、電子メール、ファックス等により送信すること、又は文書を郵便等で送付すること。

事例4：電話勧誘販売において、勧誘の電話において口頭の方法によること。

事例5：電子商取引において、取引の確認を行うための自動応答の電子メールに記載して送信すること。

7)「公表」の定義関係：

「公表」の具体的な事例は次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【公表に該当する事例】

事例1：自社の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、自社の店舗・事務所内におけるポスター等の掲示、パンフレット等の備置き・配布等

事例2：店舗販売においては、店舗の見やすい場所への掲示によること。

事例3：通信販売においては、通信販売用のパンフレット等への記載によること。

8)「本人に対し、その利用目的を明示」の定義関係：

「本人に対し、その利用目的を明示」の具体的な事例は次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【利用目的の明示に該当する事例】

事例1：利用目的を明記した契約書その他の書面を相手方である本人に手渡し、又は送付すること（契約約款又は利用条件等の書面（電子的方式、磁気的方式その他の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。）中に利用目的条項を記載する場合は、例えば、裏面約款に利用目的が記載されていることを伝える、又は裏面約款等に記載されている利用目的条項を表面にも記載する等本人が実際に利用目的を目にできるよう留意する必要がある。）

事例2：ネットワーク上においては、本人がアクセスした自社のウェブ画面上、又は本人の端末装置上にその利用目的を明記すること（ネットワーク上において個人情報を取得する場合は、本人が送信ボタン等をクリックする前等にその利用目的（利用目的の内容が示された画面に1回程度の操作でページ遷移するよう設定したリンクやボタンを含む。）が本人の目にとまるようその配置に留意する必要がある。）

9)「本人の同意」の定義関係：

「本人の同意を得（る）」の具体的な事例は次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【本人の同意を得ている事例】

事例1：同意する旨を本人から口頭又は書面（電子的方式、磁気的方式その他の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。）で確認すること。

事例2：本人が署名又は記名押印した同意する旨の申込書等文書を受領し確認すること。

事例3：本人からの同意する旨のメールを受信すること。

事例4：本人による同意する旨の確認欄へのチェック

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

事例6：本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

なお、本ガイドラインでは、十分な判断能力を有していない者から同意を得る場合においては、配慮の必要性がある旨の加筆を行いました。これは、平成19年3月に改正された経済産業省ガイドラインに準拠して、子ども及び成年被後見人などの判断能力が十分でない者から同意を得る場合は、本人のほか法定代理人等からの同意を得ることとしたものです。

10) 「本人が容易に知り得る状態」の定義関係：

「本人が容易に知り得る状態」の具体的な事例は次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【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。

11) 「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。）」の定義関係：

「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。）」の具体的な事例は次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【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、口頭又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。

12) 「個人情報保護管理者」の定義関係：

このガイドラインでは「個人情報保護管理者」という用語で、個人情報の収集、利用又は提供の目的及び手段など個人情報の取扱いについて決定する権限を有し、個人情報保護に係るマネジメントシステムの実施・運用に関して責任を負う者（いわゆる CPO（Chief Privacy Officer））を定義しています。ある程度の規模を持つ事業者においては

代表者によって指名されますが、小規模事業者においては代表者自らがその任を負うこともできます。

第3章：ガイドラインの適用範囲

第3条（適用範囲とガイドラインへの準拠）

本ガイドラインは、当協会の会員のうち、訪問販売及び連鎖販売取引を業として営む事業者であって、取得した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することにより、及び、一定の規則に従って整理することで、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、目次、索引その他検索を容易にするための機能を持たせることにより、それらの個人情報を当該事業の用に供する事業者（以下、「事業者」という。）に適用するものとする。

2 事業者が個人情報を取り扱う際の基準又は個人情報保護に関する規程を策定する際は、このガイドラインに準拠するものとする。

3 本条第1項に該当しない訪問販売事業者及び連鎖販売事業者においても、個人情報を取り扱う際の基準又は個人情報保護に関する規程を策定する際の参考として本ガイドラインを用いることができる。

<解説>

1) このガイドラインは、当協会の会員のうち、訪問販売及び連鎖販売取引を業として営む事業者であって、取得した特定の個人情報を、検索することができるように体系的に構成することにより、それらの個人情報を当該事業の用に供する事業者を対象とします。ここでいう検索の機能については、コンピュータを用いるか否かを問わないものとし、書面等によるファイリング処理されたマニュアル情報なども、それが一定の規則に従って整理され、特定の個人情報を容易に検索できるように体系的に構成されて、目次、索引その他検索を容易にするためのものを有している場合は、このガイドラインの適用対象に含まれるものとします。訪問販売及び連鎖販売取引の業界（以下、「ダイレクトセリング業界」という。）における現状としては、こうしたマニュアル管理がコンピュータによる管理と併用されているケースが多いと考えられます。

適用対象となる事業者は、このガイドラインを遵守し、個人情報の取扱いが適切に行われていることを確認し、個人情報保護に対する体制を構築、整備しなければなりません。

2) このガイドラインは、ダイレクトセリング業界における事業規模や事業形態の多様性を考慮し、個人情報保護法における「個人情報取扱事業者」から除外される者（事業の用に供する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月以内のいずれの日においても5千を超えない者）の規定を定

めていません。これは、個人情報保護法の除外規定をそのまま採り入れた場合には適用対象から外れる事業者が出る可能性に配慮したもので、法的な拘束性を持たないガイドラインの適用範囲としては、その取り扱う個人情報の量によらず広く個人情報を取り扱う者を対象とすべきであるとの考え方に基づいています。

なお、事業者の系列にある代理店・営業所等、あるいは傘下の独立事業主（当該事業者が主宰するビジネスに参加する無店舗の個人を含む。以下同じ。）等の系列事業者が行う訪問販売業及び連鎖販売業については、このガイドラインが直接的に適用されるものではありませんが、事業者は、それら系列事業者においてもこのガイドラインに準じた保護措置が講じられるよう、契約上の義務として規定するとともに、そのために必要な指導・教育の徹底を図らなければなりません（それら系列にある代理店等、あるいは傘下の独立事業主等が個人情報保護法における個人情報取扱事業者に該当する場合は、このガイドラインの適用範囲外であっても個人情報保護法の規定を遵守しなければならないことに注意してください。）。

- 3) 当協会の団体会員に所属する訪問販売事業者及び連鎖販売事業者については、このガイドラインの適用を受けません（同時に当協会にも加盟している場合は適用対象となります。）。しかし、ダイレクトセリング業界における個人情報保護施策の推進のためには、業界全体での取り組みが必要であり、団体会員としても構成員に対し、このガイドラインに準じた保護措置の実施についてメンバー事業者への積極的な啓発活動を行うことが望まれます。
- 4) 事業者は、次の事項を行う際にはこのガイドラインを用いなければなりません。
 - (1) 個人情報保護に係るマネジメントシステムを策定し、実施し、維持し、及び改善するとき。
 - (2) このガイドラインとマネジメントシステムとの適合性について自ら確認し、適合していることを自ら表明するとき。
 - (3) 外部組織又は情報主体に、このガイドラインとコンプライアンス・プログラム等との適合性について確認を求めるとき。
- 5) このガイドラインでは、事業者がダイレクトセリングにおいて取り扱うすべての個人情報を適用の対象としますが、当該事業者の従業員等の個人情報（雇用管理に関するもの、いわゆる「インハウス情報」）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」（平成16年厚生労働省告示第259号）又は指導に従って別途細目を定めるなど必要な対応をお願いします。
- 6) 事業者は、顧客のクレジット契約に伴って、当該顧客の個人信用情報を取り扱う場合は、本ガイドラインに加えて、「経済産業分野のうち信用分野における個人信用情報ガイドライン」を遵守する必要があります。

第4章：事業者の義務等

第1節：内部規程の策定及び保護方針の公表に関する措置

第4条（個人情報保護方針の公表等）

事業者は、個人情報保護方針を定め、これを文書化して公表するものとする。

2 事業者は、個人情報保護法の施行後の状況等諸環境の変化を踏まえ、個人情報保護方針の見直しを行うよう努めるものとする。

<解説>

1) 事業者の代表者は、一般の人が誰でも入手・閲覧できるように、外部向けに文書化した個人情報保護方針を策定し、公表することとします。なお、このガイドラインでは公表の仕方について特段の定めを置いていませんが、具体的には、パンフレットなどの書面に記載して配布する方法やホームページに掲載する方法などが考えられるものの、店舗を持たない事業者が多いという業界の実情を考慮すれば、自社のホームページに継続的に掲載し、いつでも誰でも閲覧できる方法を用いるなどの対応が必要であり、内容についても、一般の人の理解が十分に得られるように分かりやすい表現にするなどの配慮も大切です。

2) 事業者が策定する個人情報保護方針に基本的に含まれる事項としては、以下の事項を参考にしてください（経済産業省ガイドラインより。）。

①事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。

i. 取得する個人情報の利用目的

ii. <本人の同意なく第三者提供する場合>

- ・利用目的に第三者提供が含まれていること。
- ・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。

iii. <共同利用する場合>

- ・特定の者との間で共同利用すること。
- ・共同して利用される個人データの項目
- ・共同利用者の範囲
- ・共同して利用する者の利用目的
- ・共同して利用する者のうち、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

iv. 以下の保有個人データに関すること。

- ・自己の氏名又は名称
- ・すべての保有個人データの利用目的
- ・「開示等の求め」に応じる手続き（定めた場合に限る。）
- ・保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合に限る）

- ・苦情の申出先（認定個人情報保護団体の対象事業者である場合には当該認定個人情報保護団体の名称及び苦情解決の申出先を含む。）
 - v. 開示等の求めに応じる手続に関すること。
 - ・申請書の様式（定めた場合に限り。）
 - ・受け付ける方法（定めた場合に限り。）
 - ・保有個人データの特定に役立つ情報の提供
 - vi. 問い合わせ及び苦情の受付窓口に関すること。
 - ②個人情報の保護に関する法律を遵守すること
 - ③個人情報の安全管理措置に関すること
 - ④個人情報保護に係るマネジメントシステムの継続的改善に関すること
- 3) 文書化した個人情報保護方針は、役員を含め、従業員全員に対する周知を徹底するとともに、個人情報保護法施行後の状況等諸環境の変化に対応すべく、見直しの実施に努めてください。

第5条（内部規程の策定等）

事業者は、策定した個人情報保護方針を基に、自らが導入している販売形態の特性や営業の実態、事業規模等を考慮し、個人情報を保護するための内部規程を策定し、周知するとともに、これを実行するものとする。

2 事業者は、個人情報保護の実施状況及びその他の営業環境等に照らし、適切な個人情報の保護を維持するため、定期的に内部規程を見直すものとする。

＜解説＞

- 1) 企業等組織化された事業者が個人情報保護を適切に行うためには、社内全体に通用する内部規程が必要です。こうした全社的な社内規程を基にして、細則や手順書（コンプライアンス・マニュアル）などを策定し、従業員全員が全社的規定に基づいた行動をとることができるような構成にしておく必要があります。
- 2) 内部規程に含まれるべき基本的な事項としては、次に掲げる(1)～(13)までの内容が考えられます。
 - (1) 目的、適用範囲、定義に関する規定：

その内部規程の目的、適用する業務範囲、使用する用語の定義を規定します。
 - (2) 個人情報保護管理者及び管理体制に関する規定：

個人情報保護に係る種々の措置等を実施するために、その組織内の管理体制を整備するに当たり、各部門及び階層を定め、当該各部門及び階層ごとに担当者の役割、責任及び権限を規定します。なお、このガイドラインの第28条と第29条に従い、管理体制の統括的な責任者として個人情報保護管理者の設置について規定し、その役割、責任及び権限を規定します。
 - (3) 個人情報保護方針に関する規定：

個人情報保護方針は個人情報保護の取組みを社内外に示す手段であり、その決定のプロセスや内容、公表の仕方等について規定します。

(4) 法令及びその他の規範の特定及び参照、個人情報の特定に関する規定：

事業者は、その組織内における個人情報の取扱いに関する業務について、法令その他の規範がある場合は、それを遵守する必要があります。そのために法令その他の規範を特定し、かつそれを参照できる手順を定めた規定を設けます。また、計画段階では、事業者が現段階で自ら保有するすべての個人情報を特定することが必要ですが、マネジメントシステムの整備後においても新たに発生する業務、プロジェクト等に対応する必要から個人情報を特定するための手順を確立しておくことが重要です。

(5) 個人情報の利用目的の特定、利用目的の制限、適正な取得、取得に際しての利用目的の通知等、利用目的の変更時の措置に関する規定：

このガイドラインの第6条から第12条までに従って規定します。

(6) 個人データの内容の正確性の確保及び安全管理措置に関する規定：

このガイドラインの第13条と第14条に従って規定します。

(7) 従業員の監督、委託先の監督、ビジネス参加者に対する措置及び第三者提供の制限等個人データの管理及び従業員への教育訓練に関する規定：

このガイドラインの第15条から第20条までに従って規定します。

(8) 情報管理技術及び個人情報保護管理技術の採用等に関する規定：

事業者が取り扱う個人情報に関する具体的なリスクを明確にした上で、どのような情報管理技術及び個人情報保護管理技術を採用するかを決定するプロセスを規定します。

(9) 保有個人データに関する事項の公表等及び保有個人データの開示、訂正等、利用停止等並びにその求めに応じる手続等に関する規定：

このガイドラインの第21条から第26条までに従って規定します。

(10) 苦情対応に関する規定：

このガイドラインの第27条に従って規定します。

(11) 個人データの紛失、破壊、改ざん及び漏えい等が発生したときの対応並びにその是正措置に関する規定：

事業者が取り扱う個人情報に関する具体的なリスクを明確にした上で、そのような事態が起こったときの対応及びその是正措置を規定します。なお、個人データの漏えい事件等が発生した場合における連絡体制の確立及び個人情報の取扱いについて報告が求められたときの対応については、このガイドラインの第30条及び第31条に従って規定します。

(12) 個人情報保護に関する監査及びマネジメントシステムの見直しに関する規定：

このガイドラインの第34条を参照してください。

(13) 内部規程に違反した場合の罰則に関する規定：

一般的には、社員の就業規則における罰則の条項を適用する等が考えられます。

3) 内部規程及びその運用状況については、定期的に監査し、個人情報保護法及びその他の関係法令に合致していることの確認をとることとしています。なお、事業者の代表者は、監査において指摘された事項について、改善状況を必ず確認し、内部規程の見直しを指示することが望めます。それらの指摘事項や指示の内容については、その実施結果も含めて管理しておくことが重要です。

第2節：個人情報の取得等に関する措置

第6条（利用目的の特定）

事業者は、個人情報を取り扱うに当たっては、その利用目的をできる限り具体的に特定しなければならない。

2 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。

＜解説＞

1) 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できる限り具体的に特定する必要があります。

具体的には、「〇〇商品の訪問販売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ますが、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、自分の個人情報を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ますが、多くの場合、業種の明示だけでは利用目的をできる限り具体的に特定したことにはなりません。また、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、できる限り具体的に特定したことにはなりません。

また、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、規模及び実態に応じ、事業内容を勘案して顧客の種類ごとに利用目的を限定して示したり、本人の選択によって利用目的の限定ができるようにしたりする等、本人にとって利用目的がより明確になるような取組が望めます。

なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨が特定されている必要があります。

具体的には次のような事例を挙げることができます（経済産業省ガイドラインより。）。

【具体的に利用目的を特定している事例】

事例1：「〇〇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。」

事例2：「ご記入いただいた氏名、住所、電話番号は、名簿として販売することがありま

す。」

事例3：例えば、情報処理サービスを行っている事業者の場合であれば、「給与計算処理サービス、あて名印刷サービス、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】

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」

事例4：「ご提供いただいたクレジットカード情報は、今回ご購入いただいた商品・サービスの決済のために利用します。」

- 2) 雇用管理情報の利用目的の特定に当たっても、単に抽象的、一般的に特定するのではなく、労働者等（事業者で使用されている労働者、事業者を使用される労働者になろうとする者及びなろうとした者並びに過去において事業者で使用されていた者。以下同じ。）本人が、取得された当該本人の個人情報が利用された結果が合理的に想定できる程度に、具体的、個別的に特定しなければなりません。

第7条（利用目的による制限）

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。

2 事業者は、合併その他の事由により他の個人情報取扱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 前二項の規定は、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、身体又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）公衆衛生の向上又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）国の機関若しくは地方公共団体又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) 事業者は、特定した利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければなりません。なお、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ません。

具体的には次のような事例を挙げることができます（経済産業省ガイドラインより。）。

【同意が必要な事例】

事例：就職のための履歴書情報をもとに、自社の商品の販売促進のために自社取扱商品のカタログと商品購入申込書を送る場合

2) 事業者が、合併、分社化、営業譲渡等により他の個人情報取扱事業者から事業の承継をすることに伴って個人情報を取得した場合であって、当該個人情報に係る承継前の利用目的の達成に必要な範囲内で取り扱う場合は、目的外利用には該当しないため、本人の同意を得る必要はありません。

3) なお、子ども向けの商品やサービスを取り扱う事業者などにおいては、例えば、アンケートへの回答等により個人情報を取得する場合に、相手方が児童や生徒などの子どもになる場合があります。この場合、当該本人は、自己や保護者の個人情報が事業のために取得され、利用されることについて理解し、認識し得る十分な能力を有していないと考えられます。このような場合は、後々当該本人やその保護者が不利益を被ることのないように、あらかじめ親権者への十分な説明を行うなど、アンケート等の実施に関して認識し得る機会を提供する必要があります。

個人情報に対する認識が十分でないと考えられる「子ども」の年齢層は、一般に、12歳から15歳までの年齢以下を指すものと考えられます。

4) このガイドラインの第7条第3項は、個人情報保護法第16条第3項第1号から第4号に対応する除外規定となっています。各事項の解説及び具体的な事例は次のとおりです。

(1)「法令に基づく場合」とは：

法令に基づいて個人情報を取り扱う場合の根拠となる法令の規定としては、刑事訴訟法第218条（令状による捜査）、少年法第6条の5（令状による触法少年の調査）、所得税法第234条（所得税に係る税務職員の質問検査権）、地方税法第72条の7（事業税に係る徴税吏員の質問検査権、各種税法に類似の規定あり）等が考えられます。これらについては、強制力を伴っており、回答が義務づけられているために、一律これに該当します。具体的な事例は次のとおりです。

事例1：金融商品取引法第211条により裁判所許可状に基づいて証券取引等監視委員会の職員が行う犯則事件の調査への対応

事例2：犯罪による収益の移転防止に関する法律第9条第1項に基づく特定事業者による疑わしい取引の届出

事例3：児童虐待の防止等に関する法律第6条第1項に基づく児童虐待に係る通告

事例4：所得税法第225条第1項等による税務署長に対する支払調書等の提出

事例5：統計法第13条による国勢調査などの基幹統計調査に対する報告

一方、刑事訴訟法第197条第2項（捜査と必要な取調べ）や少年法第6条の4（触

法少年の調査に必要な質問や調査関係事項照会等）は、強制力を伴わないが、法令に根拠があるのでこれに該当します。また、弁護士法第23条の2（弁護士会からの照会）の場合も同様に対象となると考えられますが、提供に当たってはこれらの法令の目的に則した必要性和合理性が認められるかを考慮する必要があります。具体的な事例は次のとおりです。

事例1：金融商品取引法第210条により証券取引等監視委員会の職員が行う犯則事件の調査への対応

事例2：刑事訴訟法第507条による裁判執行関係事項照会への対応

事例3：刑事訴訟法第279条、心神喪失等の状態で重大な他害行為を行った者の医療及び観察等に関する法律第24条第3項による裁判所からの照会への対応

事例4：民事訴訟法第186条、第226条、家事審判規則第8条による裁判所からの文書送付や調査の嘱託への対応

事例5：家事審判規則第7条の2に基づく家庭裁判所調査官による事実の調査への対応

事例6：犯罪被害財産等による被害回復給付金の支給に関する法律第28条による検察官や被害回復給付金の支給に関する法律第28条による検察官や被害回復事務管理人からの照会への対応

事例7：会社法第381条第3項による親会社の監査役の子会社に対する調査への対応

事例8：会社法第396条及び証券取引法第193条の2の規定に基づく財務諸表監査への対応

事例9：製造・輸入事業者が、消費生活用製品安産法第39条第1項の規定による命令（危害防止命令）を受けて製品の回収等の措置をとる際に、販売事業者が、同法第38条第3項の規定に基づき製品の購入者等の情報を製造・輸入事業者に提供する場合

事例10：統計法第30条及び第31条による国勢調査などの基幹統計調査に関する協力要請への対応

（2）「人の生命、身体又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」とは：

人（法人を含む。）の生命、身体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情報の利用が必要であり、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。）は、これに該当します。具体的な事例は次のとおりです。

事例1：急病その他の事態時に、本人について、その血液型や家族の連絡先等を医師や看護婦に提供する場合

事例2：私企業間において、意図的に業務妨害を行う者の情報について情報交換される場合

事例3：消費者に危害を及ぼす事故が起こる危険性のある製品をリコールする場合で、当該製品の購入者に緊急に連絡を取る必要があるときに、販売事業者等からリコ

ールを実施するメーカー等に対して、製品の購入等の情報を提供する場合
(3)「公衆衛生の向上又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」とは：

公衆衛生の向上又は心身の発達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。）は、これに該当します。具体的な事例は次のとおりです。

事例1：健康保険組合等の保険者等が実施する健康診断やがん検診等の保健事業について、精密検査の結果や受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的として疫学研究又は統計調査のために、個人名を伏せて研究者等に提供する場合

事例2：不登校や不良行為等児童生徒の問題行動について、児童相談所、学校、医療行為等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合

(4)「国の機関若しくは地方公共団体又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」とは：

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り、協力する民間企業等が目的外利用を行うことについて、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と認められる場合は、これに該当します。具体的な事例は次のとおりです。

事例1：事業者等が、税務署の職員等の任意調査に対し、個人情報提出する場合

事例2：事業者等が警察の任意の求めに応じて個人情報提出する場合

事例3：一般統計調査や地方公共団体が行う統計調査に回答する場合

第8条（適正な取得）

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。

<解説>

1) 事業者は、偽り等の不正の手段により個人情報を取得してはなりません。例えば次のような行為は、「偽りその他不正の手段」に該当すると考えられます。

- ・個人情報を収集していることや、その目的を隠す
- ・収集目的を偽る
- ・違法な第三者提供を唆す
- ・他の法律に違反して個人情報を取得する
- ・他人の管理下にある個人情報を正当な権限なく取得する
- ・人を脅したり騙したりして個人情報を取得する

また、次のような行為は不正の手段による取得と判断される場合がありますので、注意してください。

- ・不正に取得されたことが容易に判断できる個人情報を取得する
- ・違法に第三者提供されていることが明らかな個人情報を取得する

なお、経済産業省ガイドラインでは、次のような具体的事例を挙げています。

【事業者が不正の手段により個人情報を取得している事例】

事例1：親の同意なく、十分な判断能力を有していない子供から、取得状況から考えて関係のない親の収入事情などの家族の個人情報を取得する場合

事例2：法第23条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合

事例3：他の事業者に指示して上記事例1又は事例2などの不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合

事例4：法第23条に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず個人情報を取得する場合

事例5：上記事例1又は2などの不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず当該個人情報を取得する場合

2) 不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、不正に取得したり、不正に使用・開示した場合には不正競争防止法（平成5年法律第47号）第21条、第22条により刑事罰（行為者に対する10年以下の懲役若しくは、1000万円以下の罰金、又はその併科。法人に対する3億円以下の罰金）が科され得ます。

3) ダイレクトセリング業界では、販売員が、既存の顧客等からその者が所属する学校や団体等が作成している名簿を借りて、勧誘先リストを作成することがありますが、名簿を借りる行為に不正がなくとも、その名簿に「譲渡禁止」「貸与禁止」といった禁止文言が記載されている場合は、それを借りて個人情報を収集し、勧誘のためのダイレクトメール等を送る行為は、不正な個人情報の取得となり得ると考えられますので注意が必要です。

4) なお、事業者がリストハウス等から個人情報を間接的に取得する場合は、当該提供者により第三者提供に係る法的手続き（オプトアウトの措置を含む。）がとられていることについて確認するなどの対応が望まれます。

5) 「住民票コード」のように法令により使用を禁止されているものから取得してはなりません。

第9条（利用目的の通知又は公表）

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。あらかじめ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。

＜解説＞

1) 訪問販売も連鎖販売取引も消費者との対面による販売形態がその中心であるものの、近年は留守家庭の増加などから、いわゆる飛び込みセールスはその効率面の悪さが目立っています。そこで、業界内では事前の準備として勧誘対象を絞り込む作業を行うため、個人情報の収集を行うケースが増えており、直接的に本人から取得される個人情報に加えて、本人以外から間接的に取得される個人情報についても貴重な資源としてその利用価値が高まっています。

2) 個人情報保護法第18条第1項では、事業者が個人情報を取得したときの措置として、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又は公表することが義務づけられています。また、経済産業省の個人情報保護ガイドラインは、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としています。このガイドラインでは、経済産業省ガイドラインに準じ、先ず、あらかじめ利用目的を公表することが望ましい旨を定め、それができない場合には、事後における通知又は公表でもよい旨を規定しています。

なお、個人情報保護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ありませんので、法第18条第1項の規定は適用されません。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項の措置を講ずる必要があります。

3) 「公表」については、このガイドラインの第2条（ガイドラインにおける用語の定義）の解説7）をご参照ください。

4) あらかじめ利用目的の公表が必要な具体的事例としては次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【本人への通知又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

事例5：個人情報の取扱いの委託を受けて、個人情報を取得する場合

5) 個人情報保護法では、経済産業省の旧ガイドラインが規定していた特定の機微な個人情報に係る条項を設けていません。このガイドラインも個人情報保護法に準じて特定の機微な個人情報に係る条項は設けないこととします。ただし、個人の権利利益の一層の保護を図り、個人情報の取得に関するトラブル等の発生を未然に防止するという点では、次に掲げる種類の内容を含む個人情報に関しては、それを取得する場合に、より厳格な安全管理体制の下で第三者提供は行わないといった措置を実施することが望まれます。

- (1) 思想、信条又は宗教に関する事項
- (2) 人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く）、身体・精神障害、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、請願権の行使その他の政治的権利の行使に関する事項
- (5) 保健医療又は性生活に関する事項

第10条（書面等により本人から直接に個人情報を取得する場合の措置）

事業者は、前条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（電子的方式、磁氣的方式その他の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。以下この項において同じ。）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。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

<解説>

- 1) 個人情報保護法第18条第2項では、契約書等の書面に記載してもらうことや、インターネット等の情報ネットワーク上において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することが義務づけられています。このガイドラインでは、第9条で個人情報取得に際しての原則的な措置を定めていますが、とくに本人との間で契約書等の書面で個人情報を直接に取得する場合の措置についてはこの第10条で規定することとし、個人情報保護法に準じて、あらかじめ、本人に対し、その利用目的の明示を義務付けています。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ありませんが、その場合は法第18条第1項に基づいて、あらかじめ利用目的を公表するか、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りません。
- 2) 「本人に対して、その利用目的を明示」については、第2条（ガイドラインにおける用語の定義）の解説8）をご参照ください。
- 3) 訪問販売や連鎖販売取引においては、特定商取引に関する法律で書面の交付義務が事業者課されているため、本人に対する利用目的の明示は、多くの場合その利用目的を明記した契約書その他の書面を相手方（本人）に対し手渡し、又は送付する方法により行われるものと思われますが、その際は、本人が実際に利用目的を目にすることができるよう、利用目的が記載されている箇所について伝える、又は、表面の見やすい部分に利用目的条項を記載するなど、後になって本人から気が付かなかったと言われないように措置しておくことが必要です。なお、ウェブ画面上から個人情報の入力を求めるときには、本人が送信ボタン等をクリックする前に、その利用目的が本人の目にとまるよう（利用目的の内容が示された画面に1回程度の操作でページ遷移するよう）措置して

おく必要があります。

4) 例えば、アンケート等により取得した個人情報を基に商品販売の勧誘目的で当該住居等を訪問したり、ダイレクトメール等を発信することについては、本人がアンケートに記入又は入力する際にそこまでの認識をしていない場合がありますので、そのような勧誘活動を行ったり、情報提供を行う予定がある場合は本人に対し、事前に明示しておく必要があります。

5) あらかじめ、本人に対して、その利用目的を明示しなければならない場合の具体的事例としては次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【あらかじめ、本人に対して、その利用目的を明示しなければならない場合】

事例1：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

事例2：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

事例3：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

第11条（利用目的の変更時の措置）

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。

＜解説＞

1) 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、又は公表しなければなりません。なお、本人が想定することが困難でないと認められる範囲を超える変更を行う場合は、第7条の規定に基づき、あらかじめ本人の同意を得る必要があります。

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としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【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】

事例：「当社の行う〇〇事業における新商品・サービスに関する情報のお知らせ」とした利用目的において、「既存の商品・サービスに関する情報のお知らせ」を追加することは、許容される。

2) 訪問販売及び連鎖販売取引については、店舗を介さずに販売員が消費者と対面で勧誘活動を行うという特徴から、販売員の退職や顧客の転居などにより利用目的の変更に関して本人との連絡が取り難いケースも予測されます。そのような場合に備え、あらかじめホームページ上での公表や本人への電子メールでの通知等が可能となる体制を整えるなどの措置を講じておく必要があります。

第12条（取得時及び利用目的等の変更時の措置の適用除外）

第9条、第10条及び第11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、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- （2）利用目的を本人に通知し、又は公表することにより当該事業者の権利又は正当な利益を害するおそれがある場合
- （3）国の機関又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、又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

<解説>

1) この第12条(1)～(4)に係る除外規定は、個人情報保護法第18条第4項に規定されている事項です。

2) この第12条(1)に掲げる事項の具体的事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

事例：いわゆる総会屋等による不当要求等の被害を防止するため、当該総会屋担当者個人に関する情報を取得し、相互に情報交換を行っている場合で、利用目的を通知又は公表することにより、当該総会屋等の逆恨みにより、第三者たる情報提供者が被害を被る恐れがある場合。

3) この第12条(2)に掲げる事項の具体的事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

事例1：通知又は公表される利用目的の内容により、当該事業者が行う新商品等の開発内容、営業ノウハウ等の企業秘密に関わるようなものが明らかになる場合。

事例2：暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、業務妨害行為を行う悪質者情報を取得したことが明らかになることにより、情報提供を受けた企業に害が及ぶ場合

4) この第12条(3)に掲げる事項の具体的事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

事例：公開手配を行わないで、被疑者に関する個人情報を、警察から被疑者の立ち回りが予想される事業者に限って提供する場合、警察から受け取った当該事業者が、利用目的を本人に通知し、又は公表することにより、捜査活動に重大な支障を及ぼすおそれがある場合。

5) この第12条(4)に掲げる事項の具体的事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

事例1：商品・サービス等を販売・提供する場合、住所・電話番号等の個人情報を取得する場合があるが、その利用目的が当該商品・サービス等の販売・提供のみを確実にを行うためという利用目的であるような場合。

事例2：一般の慣行として名刺を交換する場合、書面により、直接本人から、氏名・所属・肩書・連絡先等の個人情報を取得することとなるが、その利用目的が今後の連絡のためという利用目的であるような場合（ただし、ダイレクトメール等の目的に名刺を用いることは、自明の利用目的に該当しない場合があるので注意を要する。）。

第3節：個人情報の管理に関する措置

第13条（個人データの正確性の確保）

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。

<解説>

1) 事業者は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つよう努めなければなりません。この場合、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、その必要な範囲で正確性・最新性を確保すれば足ります。

第14条（安全管理措置）

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。

<解説>

1) 事業者は、その取り扱う個人データの漏れい、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、及び技術的な安全管理措置を講じなければなりません。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大きさを考慮し、事業の性質及び個人データの取扱い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します。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ずることが望まれます。とくに、ダイレクトセリング業界では、販売員が個人データを記録した媒体を携帯しつつ営業活動を行うことも少なくないため、可搬的な記録媒体については、CD-ROM やフロッピーディスクをはじめ、携帯電話やPDAなど私的に使用している通信機器などについても、あらかじめ安全管理措置について必要かつ適切な措置を講じ、個人データを携帯して営業活動を行う場合における一定のルールづくりも必要です。具体的には次のような基本的なルールが考えられます。

1. 外部に持ち出す場合は、最低限必要な範囲内の個人データに限定し、PC等の記録媒体を用いて暗号化し、パスワードを付す。やむを得ず紙媒体で持ち出す場合は、個人データを保管する専用ケースを用い、他の書類とは別に保管する。なお、紛失した場合に備え、PCや専用ケースには連絡先を明記する。
2. 外部に持ち出す個人データの携帯の仕方として、持ち出す者が身体から離さない方法をとる（ショルダーバック等を用いるなど。）。
3. 外部に持ち出す個人データは必要最低限に絞り、その内容を社内で明確にしておく。
4. 個人データを持ち出す者の「うっかりミス」を防ぐために、日頃から会議や研修等でセキュリティ意識を身に付ける啓発を行う。

(1) 組織的安全管理措置について

組織的安全管理措置とは、安全管理について従業員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います。組織的安全管理措置として講じなければならない事項は、経済産業省のガイドラインに準じて次の①から⑤の事項とし、当該各事項を実践するために講じることが望まれる内容は当該事項ごとに下に掲げる手法が例となります。

①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実践するために講じることが望まれる手法の例示

- ②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
- ③個人データの取扱い状況を一覧できる手段の整備
- ④個人データの安全管理措置の評価、見直し及び改善
- ⑤事故又は違反への対処

①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実践するために講じることが望まれる手法の例示

●従業員の役割・責任の明確化・・・個人データの安全管理に関する従業員の役割・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又は兆候があることに気付いた場合の、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（漏えい、滅失又はき損）の事故が発生した場合、又は発生
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。

●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

**②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実践するた
めに講じることが望まれる手法の例**

●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

●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委託先の選定基準、委託契約書のひな
型、委託先における委託した個人データの取扱状況を確認するためのチェックリス
ト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正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ます。

**③個人データの取扱い状況を一覧できる手段の整備を実践するために講じることが望ま
れる手法の例示**

●個人データについて、取得する項目、明示・公表等を行った利用目的、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

**④個人データの安全管理措置の評価、見直し及び改善を実践するために講じることが望
まれる手法の例示**

●監査計画の立案と、計画に基づく監査（内部監査又は外部監査）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

⑤事故又は違反への対処を実践するために講じることが望まれる手法の例示

●以下の（ア）から（カ）までの手順の整備

ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられます。

（ア）事実調査、原因の究明

（イ）再発防止策の検討・実施

（ウ）影響範囲の特定

（エ）影響を受ける可能性のある本人への連絡

事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが重要です。ただし、例えば、以下のように本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられます。

- ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
- ・高度な暗号化等の秘匿化が施されている場合（ただし、（オ）に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。）
- ・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合。ただし、（オ）に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置の内容を具体的に報告すること。）

（オ）主務大臣等への報告

＜a. 個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合＞

認定個人情報保護団体の対象事業者は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができます。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告することになりますが、以下の場合、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが必要と考えられます。

- ・特定の機微な個人情報（（a）思想、信条又は宗教に関する事項、（b）人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、（c）勤労者の団結権、団体交渉その他団体行動の行為に関する事項、（d）集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、（e）保健医療又は性生活に関する事項）を漏えいした場合
- ・信用情報、クレジットカード番号が漏えいした場合等であって、二次被害が発生する可能性が高い場合
- ・同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合
- ・その他認定個人情報保護団体が必要と考える場合

＜b. 個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合＞

経済産業大臣（主務大臣）へ報告してください。

< c. 関係機関への報告 >

認定個人情報保護団体であるか否かにかかわらず、主務大臣への報告のほか、所属する業界団体等の関係機関への報告を行ってください（本ガイドラインでは第30条で漏えい等緊急時における経済産業省及び当協会への連絡を義務として規定しています。）。

なお、上記 a から c のいずれの場合も、事業者は次に挙げる事例について、認定個人情報保護団体又は主務大臣への報告を月に一回ごとにまとめて実施することができます。

- ・ F A X やメールの誤送信（宛名及び送信者名以外に個人情報が含まれていない場合に限る。）。なお、内容物に個人情報が含まれない荷物等の宅配又は郵送を委託したところ、誤配によって宛名に記載された個人データが第三者に開示された場合については、報告する必要はありません。

(カ) 事実関係、再発防止策等の公表

二次被害の防止、類似事案の発生回避等の観点から、個人情報の漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが必要と考えられます。ただし、例えば、以下のように二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられます。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で当該事案に関する情報が共有されることが望まれます。

- ・ 影響を受ける可能性のある本人すべてに連絡がついた場合
- ・ 紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
- ・ 高度な暗号化等の秘匿化が施されている場合（ただし、(オ)に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。）
- ・ 漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合。ただし、(オ)に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること。）

個人データの取扱いに関する規程には、個人データの取扱事務の流れに従い、次の1)～5)の事項について、各々以下に掲げる事項などを例として記載することが望まれます。

1) 取得・入力

i) 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。)

ii) 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 メモリ等の記録媒体を接続できないようにする。）

iii) 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

iv) 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

2) 移送・送信

i) 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

ii) 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等の秘匿化（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、簡易書留郵便その他個人情報が含まれる荷物を輸送する特定のサービスの利用）
- FAX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FAX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

iii) 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

iv) 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

3) 利用・加工

i) 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

ii) 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。）

iii) 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

iv) 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

4) 保管・バックアップ

i) 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

ii) 手続の明確化と手続に従った実施

- 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。
- 定められた手続による保管・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等の秘匿化
- 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

iii) 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

iv) 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

5) 消去・廃棄

i) 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

ii) 手続の明確化と手続に従った実施

- 消去・廃棄する際の手続の明確化
- 定められた手続による消去・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回又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。）

iii) 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

iv) 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、権限外作業の有無の確認

(2) 人的安全管理措置について

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います。人的安全管理措置として講じなければならない事項は、経済産業省のガイドラインに準じて次の①及び②の事項とし、当該各事項において講じることが望まれる内容は当該事項ごとに下に掲げる項目となります。

- ①雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結

- ②従業者に対する内部規程等の周知・教育・訓練の実施

①雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結を実践するために講じることが望まれる手法の例示

- 従業者の採用時又は委託契約時における非開示契約の締結

※雇用契約又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れます。

※個人情報に関する非開示契約は、必ずしも全ての従業者と個別に契約を締結する必要はなく、就業規則等の社内規程による包括的な契約をする方法でも差し支えありません。

※個人情報保護に関する非開示契約の締結の際に、営業秘密を対象とする秘密保持契約をあわせて締結する場合であっても、個人情報保護と営業秘密の保護はその目的・範囲等が異なるため、従業者の「納得感」の向上の観点からは、個人情報保護に関する契約と営業秘密に関する秘密保持契約は峻別する（別書面であるか否かは問わない）ことが望まれます。

- 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れます。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、警備員等が含まれます。

②従業者に対する内部規程等の周知・教育・訓練を実践するために講じることが望まれ

る手法の例示

- 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

(3) 物理的安全管理措置について

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います。物理的安全管理措置として講じなければならない事項は、経済産業省のガイドラインに準じて次の①から③の事項とし、当該各事項を実践するために講じることが望まれる内容は当該事項ごとに下に掲げる手法が例となります。

- ①入退館（室）管理の実施
- ②盗難等の防止
- ③機器・装置等の物理的な保護

①入退館（室）管理を実践するために講じることが望まれる手法の例示

- 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

②盗難等の防止を実践するために講じることが望まれる手法の例示

- 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及び車内等への放置の禁止
- 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

③機器・装置等の物理的な保護を実践するために講じることが望まれる手法の例示

- 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

(4) 技術的安全管理措置について

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います。技術的安全管理措置として講じなければならない事項は、経済産業省のガイドラインに準じて次の①から⑧の事項とし、当該各事項を実践するために

講じることが望まれる内容は当該事項ごとに下に掲げる手法が例となります。

- ①個人データへのアクセスにおける識別と認証
- ②個人データへのアクセス制御
- ③個人データへのアクセス権限の管理
- ④個人データのアクセスの記録
- ⑤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
- ⑥個人データの移送・送信時の対策
- ⑦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
- ⑧個人データを取り扱う情報システムの監視

①個人データへのアクセスにおける識別と認証を実践するために講じることが望まれる手法の例示

- 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適正なアクセス権限を有する者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れます。
- 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

②個人データへのアクセス制御を実践するために講じることが望まれる手法の例示

- 個人データへのアクセス権限を付与すべき者の最小化
- 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ります。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ります。）
- アクセス権限を有する者に付与する権限の最少化
- 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ことが望まれます。なお、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ます。

- 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）

③個人データへのアクセス権限の管理を実践するために講じることが望まれる手法の例示

- 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

④個人データへのアクセスの記録を実践するために講じることが望まれる手法の例示

- 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してください。

⑤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を実践するために講じることが望まれる手法の例示

- 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）

⑥個人データの移送（運搬、郵送、宅配便等）・送信時の対策を実践するために講じることが望まれる手法の例示

- 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等の秘匿化）
- 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等の秘匿化

⑦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を実践するために講じることが望まれる手法の例示

- 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

セキュリティが損なわれないことの検証

⑧個人データを取り扱う情報システムの監視を実践するために講じることが望まれる手法の例示

- 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可能性があることに留意してください。

2) 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及び安全管理措置の義務違反とはならない場合の具体的事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

＜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事者が個人データにアクセスできる状態を事業者が放置していた場合で、その従事者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又はき損し、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者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

事例6：委託する業務内容に対して必要のない個人データを提供し、委託先が個人データを漏えいした場合

＜安全管理措置の義務違反とはならない場合＞

事例1：内容物に個人情報が含まれない荷物等の宅配又は郵送を委託したところ、誤配によって宛名に記載された個人データが第三者に開示された場合

事例2：書店で誰もが容易に入手できる市販名簿（事業者において全く加工をしていないもの）を処分するため、シュレッダー等をせずに廃棄し、又は、廃品回収に出した場合

3) クレジットカード情報については、次に示す「クレジットカード情報を含む個人情報の取扱いについて」に掲げられた措置を講じることが望めます。

＜クレジットカード情報を含む個人情報の取扱いについて＞

クレジットカード情報（カード番号、有効期限等）を含む個人情報（以下「クレジットカード情報等」という。）は、情報が漏えいした場合、クレジットカード情報等の不正使用によるなりすまし購入などの二次被害が発生する可能性が高いため、クレジットカード会社のほか、クレジットカード決済を利用した販売等を行う事業者及びクレジットカード決済を利用した販売等に係る業務を行う事業者並びにこれら事業者からクレジットカード情報等の取扱いを伴う業務の委託を受けている事業者（以下「クレジットカード販売関係事業者等」という。）は、クレジットカード情報等の安全管理措置として、特に以下の措置を講じることが望ましい。

- ①クレジットカード情報等について特に講じることが望ましい安全管理措置の実施
- ②クレジットカード情報等の保護に関する規定を含む契約の締結
- ③クレジットカード情報等を直接取得する場合のクレジットカード情報等の提供先名等の通知又は公表

【上記各項目を実践するために講じることが望まれる手法の例示】

- ①クレジットカード情報等について特に講じることが望ましい安全管理措置の実施
 - クレジットカード情報等について、利用目的の達成に必要最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後を適切かつ速やかに破棄
 - クレジット売上伝票に記載されるクレジットカード番号を一部非表示化
 - クレジットカード読取端末からのクレジットカード情報等の漏えい防止措置を実施（例えば、クレジットカード読取端末にはクレジットカード情報等は保存されないようにする等）
 - クレジットカード情報等を移送・送信する際に最良の技術的方法を採用
 - 他のクレジットカード販売関係事業者等に対してクレジットカード情報等が含まれる個人情報データベース等へのアクセスを許容している場合においてアクセス監視等のモニタリングを実施
- ②クレジットカード情報等の保護に関する規定を含む契約の締結
 - クレジットカード情報等を取り扱う業務に係る契約の締結の際に、クレジットカード情報等の保護に関する規定を設定（例えば、クレジットカード情報等の保護の観点から情報提供を求める旨の規定やクレジットカード情報等の取扱いが不適切なことが明らかなる場合において当該情報を取り扱う業務の是正を求めることや当該業務に係る契約を解除する旨の規定を設定）
- ③クレジットカード情報等を直接取得する場合のクレジットカード情報等の提供先名等の通知又は公表
 - クレジットカード情報等を本人から直接取得する場合、法第18条各項の規定に基づき、本人に利用目的を明示又は通知若しくは公表するほか、クレジットカード情報等の取得者名、提供先名、保存期間等を通知又は公表

4) このガイドラインでは、各事業者がどの程度の安全管理措置を講ずるべきかについて、

必ずしも明確な指針を示していません。安全管理に関し、ダイレクトセリング業界として一律の保護レベルを事業者を求めることは、業種業態が多岐にわたり、また、個人独立事業主を含めて事業者の規模も大小広範囲に分布する業界の実情を考慮すれば極めて困難なことです。従って、事業者は自らの判断によって、その事業規模・環境や業種業態、保護しようとする個人情報の内容又は性質、利用方法等に照らして必要かつ適切な措置を定め、実施することとなります。なお、その際は本ガイドラインの内容を十分に踏まえたうえで決定される必要があります。

なお、事業者がセキュリティについて技術面・管理面の対策を講じる場合には、その規模等に応じて次の基準等を参考にすることができます。

- ・ I SMS 認証基準（日本情報処理開発協会）
- ・ コンピュータウイルス対策基準（経済産業省、平成 12 年 12 月 28 日告示第 952 号）
- ・ コンピュータ不正アクセス対策基準（経済産業省、平成 12 年 12 月 28 日告示第 950 号）

第 15 条（従業員の監督）

事業者は、その従業員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。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。

2 前項の監督に当たっては、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） 内部規程を策定し、従業員に周知すること。
- （2） 従業員に対して定期的に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。

<解説>

- 1) 個人情報保護法第 21 条では、事業者の義務として従業員に対する監督責任が規定されており、従業員に個人データを取り扱わせるときは、個人データの安全管理が図られるよう必要かつ適切な監督を行わなければならない。そのためには、あらかじめ雇用及び契約時における安全管理対策を講じておかなければならず、従業員の役割と責任などについて明確化し、規程として文書化しておくことが必要です。
- 2) 事業者の行う監督については、雇用関係にある従業員（正社員）のみならず、契約社員、嘱託社員、パート社員、派遣社員、アルバイトなどを含め、従業員全員を対象に個人情報保護に関する啓発活動や教育・訓練を反復継続して行うことが重要です。なお、「従業員」には、取締役、執行役、理事、監査役、監事も含まれることを忘れないようにしてください。
- 3) 従業員が、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、予め定めた間隔で定期的に確認することや、従業員に誓約書の提出を求めることな

どは、情報漏洩等のリスク回避には有効な手段となります。また、こうした監督体制により発見される事故や従業員による規約違反等に対して、迅速・的確に対処するためには、どのようなリスクが存在し、それに対しどのように対処すべきか等、あらかじめ必要な措置の内容を定め、全従業員への周知を徹底しておく必要があります。

4) 初めて個人情報に関する業務に就業する従業員に対しては、教育訓練をしてから配置することは当然ですが、対面販売が基本となるダイレクトセリング業界では、販売員が見込み客リストや顧客リストなどの個人情報を携帯しながら営業活動を行うことが考えられるため、セールス活動を初めて行わせる場合は、あらかじめ個人情報保護に係る教育訓練を実施したうえで、必要に応じて十分に教育された者が同伴するなどのサポート体制の下に営業を行わせることも必要です。

5) 従業員に対して必要かつ適切な監督を行っていない場合の具体的な事例は次のような例を挙げることができます（経済産業省ガイドラインより。）。

【従業員に対して必要かつ適切な監督を行っていない場合】

事例1：従業員が、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、あらかじめ定めた間隔で定期的に確認せず、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可搬型外部記憶媒体を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、紛失し、個人データが漏えいした場合

6) 個人データの取扱いに関する従業員及び委託先の監督、その他安全管理措置の一環として従業員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、次の点に留意してください。その際、雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて協議を行うことが望まれます。また、その重要事項を定めたときは、労働者等に周知することが望まれます。

- モニタリングの目的、すなわ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、従業員に明示すること。
- 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。

第16条（委託先の監督）

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。その際、委託する業務内容に対して必要のない個人データを提

供しないようにすることは当然のこととして、取扱いを委託する個人データの内容を踏まえ、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ずるものとする。

2 前項の監督に当たっては、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) 個人情報保護に関する事項（当該個人データの取扱いに関して、必要かつ適切な安全管理措置として、委託者・受託者双方が同意した内容を含む。）を契約書に明記すること。
- (4) 前号の契約の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。

＜解説＞

1) 近年、企業における情報処理業務の複雑化、多様化が進み、経営の効率化や顧客サービスの向上等のために情報処理業務を外部に委託するケースが増えています。ダイレクトセリング業界でも、連鎖販売取引を行う事業者の多くが販売員のマージン計算などの業務をアウトソーシングしています。こうした外部委託の増加に伴って、発生が予測される個人情報処理に関するトラブルを防止するために、個人情報保護法では第22条で委託先の監督義務を定めています。そこで、このガイドラインでは、個人情報保護法に準じて必要な措置を講じるべきことをこの第16条に定めました。

2) 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、このガイドラインの第14条に基づく安全管理措置を遵守させるよう、委託先に対し必要かつ適切な監督をしなければなりません。「必要かつ適切な監督」には次の事項が含まれます。

- ①委託先を適切に選定すること（委託先の選定に当たっては、委託先において実施される個人データの安全管理措置が、委託する当該業務内容に応じて、少なくとも個人情報保護法第20条で求められる安全管理措置と同等であることを、合理的に確認することが望まれます。）
- ②委託先に安全管理措置を遵守させるために必要な契約を締結すること（委託契約には、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、委託元と委託先の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合理的に把握することを盛り込むことが望まれます。）
- ③委託先における委託された個人データの取扱状況を把握すること（委託先における個人データの取扱状況を把握するためには、委託契約で盛り込んだ内容の実施の程度を相互に確認することが望まれます。）

なお、漏えいした場合に二次被害が発生する可能性が高い個人データ（例えば、クレジットカード情報（カード番号、有効期限等）を含む個人データ等）の取扱いを委託する

場合は、より高い水準において「必要かつ適切な監督」を行うことが望まれます。

また、消費者等、本人の権利利益保護の観点から、事業内容の特性、規模及び実態に応じ、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明性を進めることが望まれます。

3) 委託元が受託先について「必要かつ適切な監督」を行っていない場合で、委託先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ときは、元の委託元がその責めを負うことがあり得るので、再委託する場合は委託元へ文書による報告を義務付けることが望まれます。

4) 以上のことから、委託先の選定に当たっては、遵守すべき各種の安全対策に関する基準を設け、委託先との契約において、次に掲げる事項について取り決め、その内容を契約書面に記載して明確にすることが望まれます。

●委託元及び委託先の責任の明確化

●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
- ・委託契約期間
- ・委託契約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

- ・再委託を行うに当たっての委託元への文書による報告

●個人データの取扱状況に関する委託元への報告の内容及び頻度

●契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）

●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

5) 委託契約を締結する際など、委託元が優越的地位にある場合、委託先に不当な負担を課すことがあってはなりません。（例えば、本人からの損害賠償請求に係る責務を、安全管理措置にかかる責任分担を無視して一方的に委託先に課すなど。）。

6) 委託を受けた者に対して必要かつ適切な監督を行っていない場合の具体的な例としては、次のような事例を挙げることができます（経済産業省ガイドラインより。）。

事例1：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適宜把握せず外部の事業者に委託した場合で、委託先が個人データを漏えいした場合

事例2：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委託先に指示せず、結果、委託先が個人データを漏えいした場合

事例3：再委託の条件に関する指示を委託先に行わず、かつ委託先の個人データの取扱状況の確認を怠り、委託先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した場合

事例４：契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにもかかわらず、委託先に対して再委託に関する報告を求めるなどの必要な措置を行わなかった結果、委託元の認知しない再委託が行われ、その再委託先が個人データを漏えいした場合

第 17 条（連鎖販売業におけるビジネス参加者に対する措置）

当協会の会員のうち、連鎖販売取引を業として営む事業者は、傘下のビジネス参加者において個人情報の適正な取扱いが図られるよう、必要かつ適切な措置を講じるものとする。

<解説>

1) この第 17 条は、連鎖販売業を行う事業者が、傘下のビジネス参加者の行う個人情報の取扱いについて、一定の保護措置を施すことを義務づけたものです。連鎖販売業を行う事業者の傘下にある個々の独立事業主（無店舗の個人を含む。）については、必ずしもこのガイドラインの適用を受けるものではありませんが、そうした独立事業主がガイドラインに準じた保護措置を講じることができるように、事業者に対し、傘下の独立事業主への指導・教育の徹底を義務づけています。

2) 連鎖販売業を行う事業者は、その定めるビジネスプランによっては傘下のビジネス参加者における個々の取引や契約について、必ずしも消費者と直接の関係を持たないケースがあり得ます。したがって、万一、個々のビジネス参加者から個人情報が漏洩した場合は、その責任は本来、当該ビジネス参加者が負うこととなるものですが、その一方でそのビジネスを主宰する事業者へ苦情等が寄せられることが予測されます。

そうした事態が発生した場合は、マスコミ報道等によりビジネスの主宰者が社会的な信頼性を失うなどのリスクも考慮しなければならず、傘下のビジネス参加者に対し、個人情報の取得や個人データの安全管理措置等について、必要かつ適切な措置を施すことが必要です。

3) 連鎖販売業を行う事業者は傘下のビジネス参加者に対して、ビジネス契約上の義務として、個人情報の取得やその安全管理について必要かつ適切な措置を施すことを規定するなど、その徹底を図ってください。なお、傘下のビジネス参加者が契約上の義務として行う個人情報の保護に係る具体的内容については、このガイドラインに示すとおりですが、ビジネス参加者の多くが無店舗の個人事業主であることを考えれば、例えば安全管理義務などは、このガイドラインで定める事項の内から、そのビジネス参加者の事業規模や環境などに応じて、必要かつ適切な範囲の措置を定め、実施するというのが現実的であろうと考えられます。

第4節：個人情報の提供に関する措置

第18条（第三者提供の制限）

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。

- （１）法令に基づく場合
- （２）人の生命、身体又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）公衆衛生の向上又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）国の機関若しくは地方公共団体又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得状況に応じ、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）個人情報保護法第23条第1項は、この第18条第1項（1）～（4）の場合を除いて原則としてあらかじめ本人の同意を得ることなく個人データを第三者に提供してはならないと規定しています。（1）～（4）に該当する具体的な事例は、第7条（利用目的による制限）の解説４）を参照してください。

なお、個人情報保護法第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を求め、対象事業者がそれに応じて資料提出をする場合は、この（1）に該当し、法令に基づいた個人情報の提供となります。

２）連鎖販売業では、多くの事業者が傘下のビジネス参加者へのサポート活動として、系列にある下位のビジネス参加者の商品購入履歴、販売実績、獲得ポイント等の個人情報を、同系列の上位にあるビジネス参加者に対し提供しています。こうした傘下ビジネス参加者の個人情報を一定範囲の他のビジネス参加者に提供する行為は、個人情報の第三者提供に該当することとなり、上記１）の解説に示すとおり、原則として、あらかじめ本人の同意を得なければなりません。

３）第三者提供とされる場合及び第三者提供とされない場合に関して、具体的には次のような事例を挙げることができます（経済産業省ガイドラインより。）。

【第三者提供とされる事例】

事例１：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

事例２：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

事例３：同業者間で、特定の個人データを交換する場合

事例４：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】

事例 1：同一事業者内で他部門へ個人データを提供すること。

第 19 条（第三者に提供できる場合）

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そ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、前条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。

- （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又は方法
- （４）本人の求めに応じて第三者への提供を停止すること。

２ 事業者は、前項(2)又は(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、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。

<解説>

１）前条で、原則として本人の同意なく個人データを第三者へ提供してはならないとしたうえで、この第 19 条に示す条件の下で第三者への提供を許すこととしています。すなわち、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提供を停止することとしている場合で、そのことを含めてこの第 19 条第 1 項(1)～(4)について本人に通知するか、本人が容易に知り得る状態に置くことにより、当該個人データを第三者に提供することが許されることを規定しています（これを第三者提供におけるオプトアウトといいます。）。ただし、法第 15 条第 1 項の規定により特定された利用目的に、個人情報の第三者提供に関する事項が含まれていない場合は、第三者提供を行うと目的外利用となるため、オプトアウトによる第三者提供を行うことはできません。

また、オプトアウトの方法によって個人データを第三者に提供する場合、例えば、名簿等の入手先を明らかにしないことを条件に販売するなどのように、提供元の個人情報取扱事業者は、提供先に対して、その個人データの入手先を開示することを妨げるようなことは避けることが望まれます。

２）本条第 1 項の（２）に規定する「第三者に提供される個人データの項目」の具体的な事例として、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

事例 1：氏名、住所、電話番号

事例 2：氏名、商品購入履歴

３）本条第 1 項の（３）に規定する「第三者への提供の手段又は方法」の具体的な事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

事例 1：書籍として出版

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

4)「本人が容易に知り得る状態」については、第2条（ガイドラインにおける用語の定義）第1項第14号及び同条の解説10)を参照してください。

第20条（第三者提供に該当しない場合）

次の各号のいずれかに該当する場合は、第18条の第三者提供の制限に係る第三者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又は一部を委託する場合
- （2）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
- （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
 - ①共同利用する旨
 - ②共同して利用される個人データの項目
 - ③共同して利用する者の範囲
 - ④利用する者の利用目的
 - ⑤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

2 事業者は、前項(3)に規定する項目のうち、④及び⑤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。

＜解説＞

1) 個人情報の取扱いに関して、データの入力業務等その処理を外部に委託する場合については、個人情報を取得した事業者の目的の範囲内で行われる一般的な行為として、個人情報保護法において当該委託先は第三者に該当しません。また、事業者の合併、分社化、営業譲渡等により事業の承継が行われ、併せて同じ目的の範囲内で個人データが移転（提供）される場合についても、個人情報保護法では提供された事業者を第三者とは見なしていません（ただし、事業の承継のための契約を締結するより前の交渉段階で、相手会社から自社の調査を受け、自社の個人データを相手会社へ提供する場合は、当該データの利用目的及び取扱方法、漏えい等が発生した場合の措置、事業承継の交渉が不調となった場合の措置等、相手会社に安全管理措置を遵守させるため必要な契約を締結しなければなりません。）。

2) 上記1)の具体的な事例は次のようなものを挙げることができます（経済産業省のガイドラインより。）。

【個人情報の取扱いに関する業務の全部又は一部を委託する場合の事例】

事例1：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

事例2：百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

【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

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、この第20条第1項(3)に規定する②から⑤まで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、当該個人データの提供を受ける者は、第三者に該当しません。また、共同利用する際は個人データが共同利用される前の利用目的の範囲で利用しなければなりません。

共同利用する場合、②から⑤までの情報のほか、あらかじめ一定の事項につき取り決めておくことが望まれます（一定の事項とは次のとおりです。）。

- ・ 共同利用者の要件（グループ会社であること、特定のキャンペーン事業の一員であること等、共同利用による事業遂行上の一定の枠組）
- ・ 各共同利用者の個人情報取扱責任者、問合せ担当者及び連絡先
- ・ 共同利用する個人データの取扱いに関する事項
 - 1) 個人データの漏えい等防止に関する事項
 - 2) 目的外の加工、利用、複写、複製等の禁止
 - 3) 共同利用終了後のデータの返還、消去、廃棄に関する事項
- ・ 共同利用する個人データの取扱いに関する取決めが遵守されなかった場合の措置
- ・ 共同利用する個人データに関する事件・事故が発生した場合の報告・連絡に関する事項
- ・ 共同利用を終了する際の手続き

共同利用の対象となる個人データの提供については、必ずしもすべての共同利用者が双方向で行う必要はなく、一部の共同利用者に対し、一方向で行うこともできます。

個人データの管理について責任を有する者は、利用目的の達成に必要な範囲内において、共同利用者間で利用している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りません。

なお、共同利用か委託かは、個人データの取扱いの形態によって判断されるものであって、共同利用者の範囲に委託先事業者が含まれる場合であっても、委託先との関係は、共同利用となるわけではなく、委託先の監督義務を免れるものではありません。例えば、グループ企業でイベントを開催する場合に、各子会社から親会社（幹事会社）に顧客情報を集めた上で展示会の案内を発送する場合は共同利用となりますが、自社でイベントを開催する場合に、案内状を発送するために発送代行事業者に顧客情報を提供する場合は、共同利用者の範囲に含まれるグループ企業内の事業者への提供であったとしても、委託であって、共同利用とはなりません。

この場合の具体的な事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【個人データを特定の者との間で共同して利用する場合の事例】

事例1：グループ企業で総合的なサービスを提供するために取得時の利用目的（法第1

5条第2項の規定に従い変更された利用目的を含む。以下同じ。)の範囲内で情報を共同利用する場合

事例2：親子兄弟会社の間で取得時の利用目的の範囲内で個人データを共同利用する場合

事例3：外国の会社と取得時の利用目的の範囲内で個人データを共同利用する場合

事例4：企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲で個人データを共同利用する場合

4) 個人データを共同利用する場合に、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事項に関しては、次の点に注意してください。

●「②共同して利用される個人データの項目」について・・・個人データ項目の具体例としては、次のようなものを挙げるができます。

事例1：氏名、住所、電話番号

事例2：氏名、商品購入履歴

●「③共同して利用する者の範囲」について・・・本人からみてその範囲が明確であることが必要ですが、範囲が明確である限りは、必ずしも個別列挙が必要でない場合もあります。例えば、最新の共同利用者のリストを本人が容易に知り得る状況に置いているとき等が該当します。

●「④利用する者の取得時の利用目的」について・・・共同して利用する個人データのすべての利用目的を明らかにすることが必要です。

●「⑤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・・・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を明らかにする必要があります（共同利用者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する事業者を、「責任を有する者」といい、共同利用者の内部の担当責任者をいうものではありません。）。

5) 第20条第2項は、同条第1項(3)に規定する④及び⑤を変更する場合について規定しています。すなわち、上記④及び⑤の変更については、社会通念上、本人が想定することが困難でないと認められる範囲内で行うことができ、変更する前に本人に通知又は本人が容易に知り得る状態に置くことが必要となります。また、同②及び③については原則として変更は認められませんが、次の場合は引き続き共同利用を行うことができます。

【引き続き共同利用を行うことができる事例】

事例1：共同利用を行う事業者や個人データの項目の変更につき、あらかじめ本人の同意を得た場合

事例2：共同利用を行う事業者の名称に変更があるが、当該事業者の事業内容に変更がない場合

事例3：共同利用を行う事業者について事業の承継が行われた場合

- 6) 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（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す。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ありません。）については、次に掲げる事項に留意することが望まれます。その際は、事業の性質及び雇用管理に関する個人データの取得状況等に応じ、必要かつ適切な措置を講じることが必要となります。
- 提供先において、その従業員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。

第5節：開示・変更・利用停止等の求めに関する措置

第21条（保有個人データに関する事項の公表等）

事業者は、保有個人データに関し、次の各号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。

- (1) 当該事業者の氏名又は名称
- (2) すべての保有個人データの利用目的（個人情報保護法第18条第4項第1号から第3号までに該当する場合を除く。）
- (3) 保有個人データの利用目的の通知及び開示に係る手数料の額（ただし、定めた場合に限る。）並びに保有個人データの開示、訂正・追加又は削除（以下、訂正等という）、利用停止又は消去（以下、利用停止等という）、第三者提供の停止の手續
- (4) 当該事業者が行う保有個人データの取扱いに関する苦情の申出先
- (5) 当該事業者が認定個人情報保護団体の対象事業者である場合には、当該認定個人情報保護団体の名称及び苦情の解決の申出先

2 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、次の各号のいずれかに該当する場合は、この限りでない。

- (1) 前項の規定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) 第12条(1)から(3)までに該当する場合

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ない。

＜解説＞

- 1) 事業者が誤った個人情報を保有してしまうと、それを事業の用に供することで本人の利益が侵害されるおそれがあります。そのような場合に備え、事業者は本人が自己の利益を保護する手段として、自己の個人データに関しての開示、訂正等、利用停止等、第三者提供の停止の求めを容易に行える体制を確保しておかなければなりません。個人情報保護法では、第24条で、こうした体制の確保に関して規定していますが、このガイドラインもそれに準じ、この第21条第1項で(1)から(5)の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みます。）に置くことを義務づけています。
- 2) 「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。）」については、第2条（ガイドラインにおける用語の定義）第1項第15号及び同条の解説11）を参照してください。
- 3) 個人情報保護法の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いため、同法18条（取得に際しての利用目的の通知等）の規定は適用されませんが、それが法施行後も「保有個人データ」として取り扱われる場合は、同法第24条に基づく公表等の義務が課されることとなり、即ち、この第21条に定める措置を講じることが必要となります。
- 4) 「認定個人情報保護団体」制度について
苦情処理業務等、個人情報の適正な取扱いの確保を目的として業務を行う民間団体に対し、主務大臣が認定する制度であり、この制度の設置により、当該業務の信頼性を確保し、民間団体による個人情報の保護の推進を図ろうとするものです（個人情報保護法第37条以下参照）。
- 5) 事業者は、以下の場合を除いて、本人から、自己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、遅滞なく、本人に通知しなければなりません。なお、通知しない旨を決定したときも、遅滞なく、本人に通知しなければなりません。
 - i) この第21条第1項に定める措置により、自己が識別される保有個人データの利用目的が明らかである場合
 - ii) 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
 - iii) 利用目的を本人に通知し、又は公表することにより当該事業者の権利又は利益が侵害されるおそれがある場合
 - iv) 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り、協力する民間企業等が国の機関等から受け取った保有個人データの利用

目的を本人に通知し、又は公表することにより、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

第22条（開示）

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。）を求められたときは、本人に対し、書面の交付による方法（ただし、開示の求めを行った者が同意した他の方法がある場合は、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次のいずれかに該当する場合は、その全部又は一部を開示しないことができる。その場合はその旨を本人に対して遅滞なく通知しなければならない。

- （１）本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- （２）当該事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
- （３）他の法令に違反することとなる場合

<解説>

- 1) 前条の解説に示すように、誤った情報により本人の権利が侵害されることがあるため、本人は事業者に対し、保有個人データの開示を求めることができます。
- 2) 事業者は本人からの開示の求めに対し、この第22条(1)～(3)の場合を除き、遅滞なく開示しなければならない。また、この(1)～(3)の場合に該当し、開示しないことを決定したときでも、その旨を遅滞なく通知しなければなりません（「本人に通知」については、第2条（ガイドラインにおける用語の定義）第1項10号及び同条の解説6）を参照してください。）。

開示の方法は、原則として書面の交付による方法としますが、開示を求めた者が同意した他の方法があるときは、その方法でもかまいません。

また、消費者等、本人の権利利益保護の観点から、事業活動の特性、規模及び実態を考慮して、個人情報の取得元又は取得方法（取得源の種類等）を、可能な限り具体的に明記し、本人からの求めに一層対応していくことが望まれます。

- 3) 「開示の求めを行った者が同意した他の方法がある場合は、その方法」とは、開示の方法としては、求めを行った者が同意している場合には電子メール、電話等様々な方法が可能であり、書面の交付による方法は同意がなくても可能ということを意味しています。

また、開示の求めを行った者から開示の方法について特に指定がなく、事業者が提示した方法に対して異議を述べなかった場合（電話での開示の求めがあり、必要な本人確認等の後、そのまま電話で問い合わせに回答する場合を含みます。）は、当該方法について同意があったものとみなすことができます。開示の求めがあった者からの同意の取り方として、事業者が開示方法を提示して、その者が希望する複数の方法の中から当該事業者が選択することも考えられます。

- 4) 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ります。
- 5) 雇用管理情報の開示の求めに応じる手続については、事業者は、あらかじめ、労働組合等と必要に応じ協議した上で、本人から開示を求められた保有個人データについて、その全部又は一部を開示することによりそ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に該当するとして、非公開とすることが予想される保有個人データの開示に関する事項を定め、労働者等に周知させるための措置を講ずるよう努めなければなりません。
- 6) この第22条の(1)に掲げる事項の具体的な例としては、次のような事例を挙げることができます（経済産業省ガイドラインより。）。
- 事例1：医療機関等において、病名等を開示することにより、本人の心身状況を悪化させるおそれがある場合
- 7) この第22条の(2)に掲げる事項の具体的な例としては、次のような事例を挙げることができます（経済産業省ガイドラインより。）。
- 事例1：試験実施機関において、採点情報のすべてを開示することにより、試験制度の維持に著しい支障を及ぼすおそれがある場合
- 事例2：同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなる等、業務上著しい支障を及ぼすおそれがある場合
- 8) この第22条の(3)に掲げる事項の具体的な例としては、次のような事例を挙げることができます（経済産業省ガイドラインより。）。
- 事例1：金融機関が「犯罪による収益の移転防止に関する法律」第9条第1項に基づいて、主務大臣に取引の届出を行っていたときに、当該届出を行ったことが記録されている保有個人データを開示することが同条第2項の規定に違反する場合
- 事例2：刑法第134条（秘密漏示罪）や電気通信事業法第4条（通信の秘密の保護）に違反することとなる場合

第23条（訂正等）

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等を求められたときは、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、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。

2 事業者は、前項の規定に基づき求められた保有個人データの内容の全部若しくは一部について訂正等を行ったとき、又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。

＜解説＞

- 1) 事業者の保有する個人データの内容が事実でない場合、本人はそれを理由として事業者の定める手続きに基づいて訂正等（訂正・追加又は削除）を求めることができます。
- 2) 開示請求の場合と同じように、本人の求めに対し、事業者は遅滞なくその事実関係を調査し、それが正当な申し出の場合は、遅滞なくその訂正等を行い、その内容を本人に通知しなければなりません。

利用目的から見て訂正等が必要ではない場合や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ありません。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りません。なお、他の法令の規定により特別の手続が定められている場合には、当該特別の手続が優先されます。

訂正を行う必要がない場合の具体的事例としては、次のようなものを挙げることができます（経済産業省ガイドラインより。）。

【訂正を行う必要がない事例】

事例1：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

- 3) 調査や訂正は「利用目的の達成に必要な範囲内において」行うこととしており、事業者の利用上、保有する個人データの厳密さが、さほど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事業者に過度な負担を強いる可能性があるため、限定的にそのように定めています。
- 4) 「本人に通知」については、第2条（ガイドラインにおける用語の定義）第1項10号及び同条の解説6）を参照してください。

第24条（利用停止等）

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、その利用目的の制限に違反して取り扱われているという理由、若しくは適正な取得に違反して取得されたものであるという理由、又は第三者への提供の制限に違反して第三者に提供されてい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等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。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。

2 事業者は、前項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は前項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への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ない。

＜解説＞

1) 個人情報保護法第27条は、本人が事業者に対し、同法第16条の利用目的の制限に違反して取り扱われる場合及び同法第17条の適正な取得に違反して取得した場合に、その保有個人データの利用の停止等（利用の停止又は消去）を求めることができること、さらに同法第23条第1項の第三者提供の制限に違反して第三者提供がされている場合に、第三者提供の停止を求めることができることを規定しています。

2) 本人からの利用停止又は消去の求め又は第三者への提供の停止の求めに対し、事業者はその事実関係を調査し、それが正当な求めであることが判明した場合は、遅滞なくそれに応じなければなりません。

ただし、個人情報保護法では、これらの求めに応ずる際に、その実施に多額の費用を要したり、実施が困難な場合、例えば保有するデータベース内で当該本人の個人情報のみを利用停止すると、データベース全体が長期間使用できなくなり、業務上大きな支障を生ずる場合は、そのことに代えて本人の権利利益を保護する他の措置が取られるのであれば、その限りでないとしており、このガイドラインもそれに準拠することとしています。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りません。

なお、本人からの指摘（同意のない目的外利用、不正な取得、又は同意のない第三者提供である旨の指摘）が正しくない場合には、利用の停止等を行う必要はありませんが、この場合においても、遅滞なく、利用の停止等を行わない旨の通知を本人に行わなければなりません。

3) 保有個人データの全部について消去を求められた場合、「消去」とは保有個人データをそれとして使えなくすることで、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ものであることから、利用停止によって手続違反（同意のない目的外利用、不正な取得、同意のない第三者提供をいいます。）を是正できる場合は、そのような措置を講ずることによって義務を果たしたことになります。

また、消費者等、本人の権利利益保護の観点から、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の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、本人からの求めに一層対応していくことが望まれます。

4) 「本人に通知」については、第2条（ガイドラインにおける用語の定義）第1項10号及び同条の解説6）を参照してください。

第25条（理由の説明）

事業者は、保有個人データの公表、開示、訂正等及び利用停止等（以下、開示等という。）の規定により、本人から求めら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。

＜解説＞

- 1) 個人情報保護法第28条は、本人から求められた措置を取らなかった場合や異なる措置を取った場合の本人への理由の説明について、「努めなければならない」との表記で努力規定としています。このガイドラインにおいても個人情報保護法に準じた措置を求めることとします。
- 2) 理由の説明手段としては書面、電子メール、電話、面談などの方法が考えられますが、ケースに応じた説明手段を用いて、消費者に対し十分に説明し、納得が得られる方法を用いることが必要です（「本人に通知」については、第2条（ガイドラインにおける用語の定義）第1項第10号及び同条の解説6）を参照してください。）。

第26条（開示等の求めに応じる手続き）

事業者は、保有個人データについて本人からの開示等の求め（個人情報保護法第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をいう。）に関し、その受付方法として以下に掲げる事項について定めることができる。この場合において、事業者は、当該方法に従って行われる本人による開示等の求めを受け付けることとする。

- （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式
- （3）開示等の求めをする者が本人又は本条第4項に規定する代理人であることの確認方法
- （4）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

2 事業者は、前項に従って定められた開示等の求めを受け付ける方法及び手数料を定めた場合の手数料の額について、本ガイドライン第21条第1項（3）により、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。）に置かななければならない。

3 事業者は、本人からの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、当該本人に対し求めることができる。この場合において、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。

4 事業者は、次に掲げる代理人による開示等の求めに応じなければならない。

- （1）未成年者又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 事業者は、前四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。

6 本人の求めに対する利用目的の通知及び開示を行う場合は、その実施に関し、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定められた手数料を徴収することができる。

＜解説＞

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、追加又は削除、保有個人データの利用の停止又は消去、保有個人データの第三者への提供の停止の求めをいいます。

2) 事業者は個人情報保護法第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ます。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。）に置かなければなりません。なお、事業者が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ますが、開示等の求めについて特段の受付方法を定めていない場合は、自由な申請を認めることとなりますので注意してください。

3) 開示等の求めの受付方法には、郵送、FAX等がある。

4) 「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。）」については、第2条（ガイドラインにおける用語の定義）第1項15号及び同条の解説11）を参照してください。

5) 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ます。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役立つ情報の提供その他本人の利便性を考慮しなければなりません。また、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りません。

6) 事業者が保有個人データの開示を行う場合は、当該開示等を求める者が、真正な本人又はその代理人であることを十分に確認したうえで行わなくてはならず、その確認が十分にできない場合は安易に開示等の求めに応じるべきではありません（ただし、代理人であることの確認の方法は、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ず、事業者が保有している個人データに比して過剰な情報を求めるなど、本人確認のために必要以上に多くの情報を求めているではありません。）。なお、以下に経済産業省のガイドラインで示されている本人等の確認方法の具体的事例を記しておきますので、参考にしてください。

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（親権者が未成年者の法定代理人であることを示す場合は、本人及び代理人が共に記載され、その続柄が示された戸籍謄抄本、住民票の写し）

7) 利用目的の通知及び開示の求めについては、個人情報保護法第30条により、実費を勘案して合理的であると認められる範囲において手数料を定め、それを徴収することができるかとされていますが、そのとき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。）に置かれなければなりません。なお、個人情報保護法では訂正等及び利用停止等について事業者が手数料を徴収することについて規定を設けていません。このガイドラインもそれに準じて、これらの手続きに関して手数料を徴収することができるとはしていません。

8) 政令第8条（開示等の求めをすることができる代理人）により、未成年者又は成年被後見人の法定代理人及び開示の求めをすることについて本人が委任した代理人は、本人に代わって開示等の求めを行うことができることとなっています。これらの代理人が開示等の求めを行ってきた場合には、例えば未成年者であればその親権者であることの確認を、また本人の委任による代理人であれば当該代理人が真に本人の委任を受けた代理人であることを確認することができるように、あらかじめ確認手続きについて定めておく必要があります（確認方法の具体的事例については、上記6）の事例6を参照してください。）。)

第6節：苦情対応に関する措置

第27条（苦情への対応）

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対応に努めなければならない。

2 事業者は、前項の目的を達成するため、受付窓口の設置、対応マニュアルの作成等必

要な体制の整備に努めなければならない。

＜解説＞

- 1) 個人情報保護法第31条は、個人情報の取扱いに関する苦情の対応について、事業者の努力義務を規定しています。このガイドラインもそれに準じ、苦情の適切かつ迅速な対応に努めるため、事業者の事業活動の範囲、事業規模、顧客数等に応じ必要な体制の整備に努めるものとし（日本工業規格 JISQ10002「品質マネジメント—顧客満足—組織における苦情対応のための指針」を参考にすることができます。）。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ありません。
- 2) 苦情対応窓口の電話番号、メールアドレス等の連絡先は、契約書面、商品パンフレット又はホームページ等に掲載して明示することが考えられますが、いずれの場合においても消費者の目につきやすいところに表示しておくことが望まれます。
- 3) なお、個人情報保護法第42条は、本人等が認定個人情報保護団体に対して、苦情の解決を申し出ることができることと規定しています。この場合、当該認定個人情報保護団体は、構成員である当該事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることがあります。事業者側は正当な理由なくこれを拒むことができないと規定しています。
- 4) ダイレクトセリング業界のように、店舗以外の場所において対面による勧誘を行うケースが多い営業形態では、個人情報の取扱いに関するトラブルといった場合には、個人情報保護法の守備範囲だけではなく、プライバシーの侵害といった問題であるケースが少なくないと予測されます。このような場合は個人情報保護法での処理だけでは解決が難しいと考えられますが、そのような場合でも自主的な取組みによって解決に導くよう、あらかじめプライバシー保護といった視点での苦情対応について、必要な措置を講じておくことが肝要です。

第7節：個人情報の適正管理義務に関する措置

第28条（個人情報保護管理者の設置）

事業者の代表者は、個人情報保護法及びその他の関係法令、並びに本ガイドラインについて、その内容を理解し実践する能力のある者を事業者の内部から1名以上指名し、個人情報の適正管理義務の遂行等、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。

＜解説＞

- 1) 個人情報保護管理者は、事業者の代表者により指名され、個人情報保護に係るマネジメントシステムの運営と施策の実施を行う責任者であって、個人情報の取扱いについて決定する権限を有します。いわゆる CPO（チーフ・プライバシー・オフィサー）はこれに該当しますが、対外的な責任という意味から、役員が指名されることが望まれます。
- 2) 事業者の代表者は個人情報保護管理者を1名以上指名し、個人情報の適正管理義務の

遂行等の任に就くことができるよう配置することとします。ただし、個人情報保護管理者を複数名とした場合は、責任を明確にし、当事者間での役割分担を明らかにしなければなりません。

第 29 条（個人情報保護管理者の責務）

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し、遵守するとともに、従業者に対しこれを理解させ、遵守させるために、内部規程を整備し、個人情報保護に係るマネジメントシステムの整備並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。

<解説>

1) 個人情報保護管理者は、個人情報の取扱について定めた内部規程を整備し、それに則したマネジメントシステムの整備のために以下のような措置を講じるものとします。

(1) 法令その他規範の特定：

個人情報に関する法令その他の規範を特定し、参照できる手順を確立し、維持する。

(2) 個人データの特定：

保有するすべての個人データを特定するための手順を確立し、特定する。さらに特定した個人情報に関するリスクを定期的に調査し、その予防及び是正等の措置に関する計画書を立案する。

(3) 細則の策定：

事業に関する個人情報、雇用管理に関する個人情報、その他の個人情報の種類、取り扱う個人情報の量、利用方法、部門の業務の特性、個人の権利利益を害するリスクの程度等に応じて内部規程の細則（帳票等を含む。）を定め、必要に応じてコンプライアンス・マニュアルを作成する。

(4) 計画書の策定：

内部規程を遵守するために必要なリスク調査、教育、監査等の計画を立案し、文書化し、かつ、維持する。また、必要に応じて詳細計画を立案する。事業者は、計画の達成のために必要な予算措置を講じる。

2) 個人情報に関係する業務に初めて就く者に対しては、あらかじめ個人情報保護に関する必要な教育訓練をしたうえで配置するなり、十分に教育訓練された者がサポートするといった体制を敷くことが必要です。

3) 個人情報の取扱いを外部の機関等に委託する場合は、当該委託先の個人情報に関する管理状況に関して適宜確認を行ってください。

4) 個人情報保護管理者は、その他、例えば十分な技術的保護措置を実施する等の責任も負います。

5) 個人情報保護管理者は、事業者におけるリスク管理の観点から、このガイドラインに定めるすべての事項について、書面又はこれに代わる方法で、適正に文書管理が行われ

るよう徹底することが望まれます。個人情報保護法第35条「報告の徴収」における主務大臣による要求により、その取扱いについての報告が求められたときや訴訟等の状況に陥ったときに、迅速かつ的確に対応できるよう、あるいは改ざんのそしりを受けないように、文章の記録・作成と管理を徹底しておくことで後日のトラブルに備える体制の整備が必要です。

- 6) マネジメントシステムのもとに個人情報保護を推進するときには、法令、個人情報保護指針、内部規程、細則等と合致していること及びその運用状況を確認するために定期的な監査等を実施することが望まれます。

第8節：緊急時における連絡体制の確立に関する措置

第30条（関係機関への連絡）

事業者は、個人情報漏えいした事実、及び漏えいしたおそれがある事実を把握した場合は、当協会及び経済産業省等関係する機関に対し、即時に連絡を行わなければならない。

2 個人情報の漏えい事件等が発生した時は、事業者は、被害の拡大防止、類似事件の発生防止の観点や、本人個人が被る権利利益の侵害の大きさ等を考慮し、可能な限り当該事案に係る事実関係を公表するものとする。

<解説>

1) 経済産業省は、平成16年3月23日付けで当協会に対し、民間事業者による個人情報の安全管理の徹底に関して文書による要請を行いました。その内容は以下のとおりです。

- ①省内の業及び団体所管課に個人情報安全管理責任者を置きます。貴団体の個人情報安全管理責任者は、経済産業省商務情報政策局消費経済政策課長（商務流通グループ商取引・消費経済政策課消費経済企画室長）となります。
- ②貴団体及び傘下の企業等において、個人情報漏えい事件等が発生した場合は、当該企業等から、上記個人情報安全管理責任者に即時に連絡を行うよう徹底をお願いいたします。
- ③なお、近時の事案を踏まえ、貴団体及び傘下の企業等において、保有する個人情報のアクセス管理の徹底、個人情報の情報管理体制の整備、企業の内部関係者による個人情報の持ち出しの防止に係る対策、外部からの不正アクセスの防御等情報管理システムの堅牢化及び個人情報に関する従業者・委託先の監督体制の整備などを行うことにより、個人情報の情報管理の徹底を図るよう改めて周知及び指導いただきますようお願いいたします。
- ④また、平成17年4月1日に個人情報保護法が施行されますが、経済産業省では、内閣府が定める基本方針に沿って、当省所管企業、業界団体に対応を行う場合の具体的な対処方針を「個人情報の保護に関する法律に基づく経済産業省ガイドライン」として

作成、公表することとしております。貴団体及び傘下の企業等が個人情報の安全管理体制等の整備を行う際には、当該ガイドラインを参照するよう周知及び指導いただくとともに、必要に応じて、貴団体における自主的なガイドラインの策定・見直しも検討いただくなど、常に十分な個人情報の情報管理の徹底が図られるようお願いいたします。

- 2) このガイドラインでは、本条において、事業者における個人情報の漏えい等が発生した時の連絡体制の確立などについて規定しています。具体的には、漏えい等が発生した場合は、即時に当協会及び経済産業省等の関係機関に連絡を行うことを義務づけています。

なお、個人情報の漏えいが発生した場合等における対処の方法については、本ガイドライン第14条(安全管理措置)の解説(1)「組織的安全管理措置について」の⑤「事故又は違反への対処を実践するために講じることが望まれる手法の例示」を参考にすることができます。

- 3) 個人情報の漏えい事件などが発生した場合は、事業者がその事実関係を公表することで二次被害の発生を防止したり、類似の事件の発生を未然に防ぐことができます。このガイドラインでは、このような事案の発生に際しては、事業者は被害の拡大防止、類似事件の発生防止の観点や、本人個人が被る権利利益の侵害の大きさ等を考慮して、できる限り当該事案に係る事実関係を公表するものとしています。

第31条（報告等）

事業者は、個人情報の取扱いに関し、当協会及び経済産業省等関係機関から報告を求められた場合は、直ちに報告しなければならない。

<解説>

- 1) 個人情報保護法第32条では、主務大臣の権限として「報告徴収」について規定されています。主務大臣は、同法第4章第1節（個人情報取扱事業者の義務）の規定の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱いに関し報告をさせることができることを規定しています。

このガイドラインでは、この第31条において、主務大臣が行う報告徴収や当協会からの求めに応じて行われる事業者の報告について規定しています。

- 2) 事業者は、主務大臣から報告徴収を受けた場合は、直ちにその内容を当協会に報告してください。ケースによっては、当協会から文書若しくは口頭による説明を求められ、または資料の提出を求められることがあります。正当な理由がないのにこれを拒んではなりません。

第9節：経過措置

第32条（本人の同意に関する経過措置）

本ガイドラインの実施前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第6条第1項の規定により特定される利用目的以外の目的で個人情報を取り扱うことを認める旨の同意に相当するものであるときは、第7条第1項又は第2項の同意があったものとみなす。

2 本ガイドラインの実施前になされた本人の個人情報の取扱いに関する同意がある場合において、その同意が第18条第1項の規定による個人データの第三者への提供を認める旨の同意に相当するものであるときは、同項の同意があったものとみなす。

<解説>

1) 個人情報保護法は、次の①から③に掲げる個人情報の取扱い及び提供を行う場合は、あらかじめ本人の同意を得なければならないことを規定していますが、同法の施行前にこの法律で求められる本人の同意に相当する同意がなされているときは、施行後に改めて本人の同意を得る必要はないことを規定しています。

①個人情報取扱事業者が法第15条第1項の規定により特定した個人情報の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こと（法第16条第1項）

②企業の合併等による事業の承継に伴って個人情報を取得した場合に、承継前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うこと（法第16条第2項）

③個人データを第三者に提供すること（法第23条第1項）

2) 本ガイドラインでは、本人の同意に関する経過措置については個人情報保護法に準ずる措置を実施することを本条に規定しています。

第33条（通知に関する経過措置）

本ガイドライン第19条第1項の規定により本人に通知し、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事項に相当する事項について、本ガイドラインの実施前に本人に通知されているときは、当該通知は、同項の規定により行われたものとみなす。

2 本ガイドライン第20条第1項(3)の規定により本人に通知し、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事項に相当する事項について、本ガイドラインの実施前に本人に通知されているときは、当該通知は、同項の規定により行われたものとみなす。

<解説>

1) 個人情報保護法において、一定事項について、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くことを求めている法第23条第2項（第三者提供ができる場合（本ガイドライン第19条）を参照）及び第4項第3号（個人データの共同利用（本ガイドライン第20条）を参照）について、個人情報保護法の施行前にこの法律に規定するものに相当する内容の通知が行われているときは、施行後に改めて通知を行う必要はありません。

2) 本ガイドラインは、通知に関する経過措置については個人情報保護法に準ずる措置を実施することを本条に規定しています。

第10節：個人情報保護体制の見直しに関する措置

第34条（事業者における個人情報保護体制の見直し）

事業者の代表者は、個人情報保護の実施状況及びその他の経営環境等に照らして、適切な個人情報の保護を維持するために定期的にコンプライアンス・プログラム等を見直すものとする。

＜解説＞

- 1) 事業者の代表者は、個人情報保護の実施状況について監査等を実施するときには、あわせて、マネジメントシステムについて、それ自体に改善点はないか見直しを行わせ、必要に応じて改善案の作成などを行わせたうえで優先順位を付して実行させる必要があります。また、具体的な指示の内容は、それぞれの担当者宛に書面により行い、徹底するとともに、その実施結果も含めて履歴を管理しておくことが重要です。
- 2) 個人情報保護のための体制整備に当たっては、日本工業規格 J I S Q 15001「個人情報保護マネジメントシステム—要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格 J I S X 5070「セキュリティ技術—情報技術セキュリティの評価基準」、日本工業規格 J I S Q 27001「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—要求事項」、日本工業規格 J I S Q 27002「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の実践のための規範」、CRYPTREC（暗号技術評価プロジェクト）の「電子政府推奨暗号リスト」等を、個人データの安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にすることができます。
- 3) 事業者は、「個人情報保護を推進する上での考え方や方針（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、それをウェブ画面への掲載又は店舗の見やすい場所への掲示等により公表し、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するためには重要です。事業者がそうした公表を行う場合には、事業者の個人情報保護を推進する上での考え方や方針には、消費者等、本人の権利利益の保護の観点から、以下に掲げる点を考慮した事項を盛り込み、本人からの求めに一層対応していくことも重要なことであると考えられます。

●事業の内容及び規模を考慮した適切な個人情報の取扱いに関すること。

（ア）取得する個人情報の利用目的（法第18条関係）

すべての利用目的を列記するのではなく、事業内容を勘案して顧客の種類ごとに利用目的を限定して示すなど、事業内容の特性、規模及び実態に応じ、本人にとって利用目的がより明確になるようにすることが望ましい。

(イ) ＜個人データの取扱いの委託を行う場合＞（法第22条関係）

事業内容の特性、規模及び実態に応じ委託処理の透明化を進めることを盛り込むことが望ましい。

- ・個人データの委託を行うこと。
- ・委託する事務の内容

(ウ) ＜本人の同意なく第三者提供する場合＞（法第23条第2項及び第3項関係）

- ・利用目的に第三者提供が含まれていること。
- ・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。

(エ) ＜共同利用する場合＞（法第23条第4項及び第5項）

- ・特定の者との間で共同利用すること。
- ・共同して利用される個人データの項目
- ・共同利用者の範囲
- ・共同して利用する者の利用目的
- ・共同して利用する者のうち、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

(オ) 以下の保有個人データに関すること（法第24条、第25条及び第27条関係）

個人情報の取得元又は取得方法（取得源の種類等）を可能な限り具体的に明記したり、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たりするなど、事業活動の特性、規模、実態を考慮して、本人からの求めに対応していくことを盛り込むことが望ましい。

- ・自己の氏名又は名称
- ・すべての保有個人データの利用目的
- ・「開示等の求め」に応じる手続（定めた場合に限る。）
- ・保有個人データの利用目的の通知及び開示に係る手数料の額（定めた場合に限る。）
- ・苦情の申出先（認定個人情報保護団体の対象事業者である場合には当該団体の名称及び苦情解決の申出先を含む。）

(カ) 開示等の求めに応じる手続に関すること（法第29条関係）

- ・申請書の様式（定めた場合に限る。）
- ・受け付ける方法（定めた場合に限る。）
- ・保有個人データの特定に役立つ情報の提供

(キ) 問合せ及び苦情の受付窓口に関すること（法第23条第5項、第24条第1項、第29条第1項及び第31条関係）

- 個人情報の保護に関する法律を遵守すること。
- 個人情報の安全管理措置に関すること。
- マネジメントシステムの継続的改善に関すること。

第5章：ガイドラインの見直し

第35条（ガイドラインの見直し）

本ガイドラインは、個人情報保護法の施行後における状況等諸環境の変化を踏まえて、見直しを行うこととする。

<解説>

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す。そこで、このガイドラインについては、経済産業省のガイドラインに準じて、個人情報保護法の施行後の状況等諸環境の変化を踏まえて見直しを行うこととします。

<附則>

附則：本ガイドラインは、平成17年4月1日から実施する。

附則：（平成20年1月8日）

本ガイドラインの改正規定は、理事会の議決日（平成20年1月8日）をもって実施する。

附則：（平成20年6月11日）

本ガイドラインの改正規定は、理事会の議決日（平成20年6月11日）をもって実施する。

附則：（平成22年1月7日）

本ガイドラインの改正規定は、理事会の議決日（平成22年1月7日）をもって実施する。

附則：

本変更規程は、一般社団法人及び一般財団法人に関する法律及び公益社団法人及び公益財団法人の認定等に関する法律の施行に伴う関係法律の整備等に関する法律第106条第1項に定める公益法人の設立の登記の日から施行する。

以上