【参考資料4】

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

（平成２６年１２月１２日厚生労働省・経済産業省告示第４号）

平成２６年１２月
経済産業省

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

目次

１．目的及び適用範囲

このガイドラインは、個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）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方針」（平成２０年４月一部変更）を踏まえ、また、法第８条に基づき法に定める事項に関して必要な事項を定め、経済産業省が所管する分野及び法第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るものである。

本ガイドラインは、経済産業大臣が法を執行する際の基準となるものであるが、従業員の個人情報（雇用管理に関するもの）に関する部分については、雇用管理分野における個人情報保護に関するガイドライン（平成２４年厚生労働省告示第３５７号）との整合性に留意した（「従業員」及び「従業者」の用語については、「2-2-3-3.従業者の監督（法第２１条関連）」参照。）。このため、本ガイドラインのうちこれらの部分については、厚生労働大臣及び経済産業大臣の共同で作成し、両大臣が共同して法を執行する。

本ガイドライン中、「しなければならない」と記載されている規定については、それに従わなかった場合は、経済産業大臣により、法の規定違反と判断され得る。一方、「望ましい」と記載されている規定については、それに従わなかった場合でも、法の規定違反と判断されることはない（３．参照）。しかし、「望ましい」と記載されている規定についても、個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに配慮して適正な取扱いが図られるべきとする法の基本理念（法第３条）を踏まえ、個人情報保護の推進の観点から、できるだけ取り組むことが望まれるものである。もっとも、個人情報の保護に当たって個人情報の有用性に配慮することとしている法の目的（法第１条）の趣旨に照らし、公益上必要な活動や正当な事業活動等までも制限するものではない。

なお、本ガイドライン中に事例として記述した部分は、理解を助けることを目的として、該当する事例及び該当しない事例のそれぞれにつき、典型的な例を示すものであり、すべての事案を網羅することを目的とするものではない。実際には個別事案ごとに検討が必要となる。また、幾つかの業種の例を取り上げたもので、すべての業種の例を網羅しているわけではない。

このほか、経済産業分野に該当するもののうち、個人情報の性質及び利用方法又は事業実態の特殊性等にかんがみ、特別に個人情報の適正な取扱いを確保する必要がある場合には、経済産業大臣が、別途更なる措置を講ずることもあり得る。また、認定個人情報保護団体（法第３７条第１項の認定を受けた団体をいう。以下同じ。）が、法第４３条第１項に規定する個人情報保護指針を策定することもあり得る。さらに、事業者団体等が、当該事業の実態を踏まえ、当該団体傘下企業を対象とした自主的ルールである、事業者団体ガイドラインを策定又は改正することもあり得る。これらの場合、それらに該当する個人情報を取り扱うに当たっては、当該更なる措置、個人情報保護指針及び事業者団体ガイドラインに沿った対応を行う必要がある。

本ガイドラインは、経済産業分野における事業者等のうち、法が適用対象とする個人情報取扱事業者（※2-1-3 参照。）に該当する事業者等を対象として適用する。

また、経済産業分野において個人情報取扱事業者でない事業者等についても、「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。」（法第３条）という法の基本理念を踏まえ、このガイドラインに規定されている事項を遵守することが望ましい。

２．法令解釈指針・事例

2-1. 定義（法第２条関連）

2-1-1.「個人情報」（法第２条第１項関連）

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

「個人情報」※1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※2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、「2-2-3-2.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）。

※１法は、「個人情報」、2-1-4.「個人データ」及び 2-1-5.「保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。

※２「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等であって照合が困難な状態を除く。

【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（事業者が労働者等（個人情報取扱事業者に使用されている労働者、個人情報取扱事業者に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個人情報取扱事業者に使用されていた者。以下同じ。）の雇用管理のために収集、保管、利用等する個人情報をいい、その限りにおいて、病歴、収入、家族関係等の機微に触れる情報（以下「機微に触れる情報」という。）を含む労働者個人に関するすべての情報が該当する。以下同じ。）

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る。）

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@xyzisp.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

2-1-2.「個人情報データベース等」（法第２条第２項関連）

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。

1　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
2　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

個人情報の保護に関する法律施行令（平成１５年政令第５０７号。以下「政令」という。）第１条
法第２条第２項第２号の政令で定めるものは、これに含まれる個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。

「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。

【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、他の従業者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が、氏名、住所等により分類整理されていない状態である場合

2-1-3.「個人情報取扱事業者」（法第２条第３項関連）

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。ただし、次に掲げる者を除く。

１　国の機関

２　地方公共団体

３　独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成１５年法律第５９号）第２条第１項に規定する独立行政法人等をいう。以下同じ。）

４　地方独立行政法人（地方独立行政法人法（平成１５年法律第１１８号）第２条第１項に規定する地方独立行政法人をいう。以下同じ。）

５　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ものとして政令で定める者

政令第２条

法第２条第３項第５号の政令で定める者は、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の数を除く。）の合計が過去６月以内のいずれの日においても５０００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

「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、政令第２条では、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※の合計が過去６か月以内のいずれの日においても５０００人を超えない者とする。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の総和により判断する。ただし、同一個人の重複分は除くも

のとする。

ここでいう「事業の用に供している」の「事業」とは、一定の目的をも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個人情報取扱事業者に該当し得る。

※「特定の個人の数」について

個人情報データベース等が、以下の要件のすべてに該当する場合は、そ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は、上記の「特定の個人の数」には算入しない。

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。

【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（ただし、委託元の指示等によって個人情報を含む情報と認識できる場合は算入する。）

【個人情報取扱事業者に該当する事例】

事例）電子媒体及び紙媒体（以下「媒体」という。）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の総和が５０００人を超え

ている事業者

2-1-4.「個人データ」（法第２条第４項関連）

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。

「個人データ」※とは、個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報をいう。

※法は、2-1-1.「個人情報」、「個人データ」及び 2-1-5.「保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。

【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

＊電話帳、カーナビゲーションシステム等の取扱いについて

個人情報データベース等が、以下の要件のすべてに該当する場合であっても、その個人情報データベース等を構成する個人情報については、個人データとなる可能性も否定できない。しかしながら、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ことから、個人情報取扱事業者の義務（2-2.個人情報取扱事業者の義務等）を課されないものと解釈する。

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。
②その個人情報データベース等を構成する個人情報として氏名、住所（居所を含み、地図上又はコンピュータの映像面上において住所又は居所の所在場所を示す表示を含む。）又は電話番号のみを含んでいる。
③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、識別される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変更するようなことをしていない。

2-1-5.「保有個人データ」（法第２条第５項関連）

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。

政令第３条

法第２条第５項の政令で定めるものは、次に掲げるものとする。

１　当該個人データの存否が明らかになることにより、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

２　当該個人データの存否が明らかになることにより、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　当該個人データの存否が明らかになることにより、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　当該個人データの存否が明らかになることにより、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

政令第４条

法第２条第５項の政令で定める期間は、６月とする。

「保有個人データ」※1とは、個人情報取扱事業者が、本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する※2「個人データ」をいう。

※１法は、2-1-1.「個人情報」、2-1-4.「個人データ」及び「保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。

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

ただし、次の①又は②の場合は、「保有個人データ」ではない。

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※3。

②６か月以内に消去する（更新することは除く。）こととなるもの。

※３「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」とは、以下の場合を指す。

①その個人データの存否が明らかになることで、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

②その個人データの存否が明らかになることで、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、悪質なクレー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

③その個人データの存否が明らかになることで、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

④その個人データの存否が明らかになることで、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。

事例１）警察からの捜査関係事項照会や捜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

2-1-6.「本人」（法第２条第６項関連）

法第２条第６項

この法律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。

2-1-7.「本人に通知」

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。

その他、法第１８条第３項・第４項第１号～第３号等に記述がある。

「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状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【本人への通知に該当する事例】

事例１）面談においては、口頭又はちらし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。

2-1-8.「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。

その他、法第１８条第３項・第４項第１号～第３号等に記述がある。

「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。

特に雇用管理情報は、機微に触れる情報を含むため、事業者は、自らの置かれた状況に応じ、労働者等に内容が確実に伝わる媒体を選択する等の配慮を行うものとする。

【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。

2-1-9.「本人に対し、その利用目的を明示」

法第１８条第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（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。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。

「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。

【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述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。）

2-1-10.「本人の同意」

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。

法第２３条第１項

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。

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。

その他、法第１６条第２項・第３項第２号～第４号等に記述がある。

「本人の同意」とは、本人の個人情報が、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（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個人情報取扱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、子どもが判断能力を有していないなどの場合は、法定代理人等から同意を得る必要がある。

【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

2-1-11.「本人が容易に知り得る状態」

法第２３条第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。

法第２３条第４項第３号

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。

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、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

その他法第２３条第３項等に記述がある。

「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。

特に雇用管理情報は、機微に触れる情報を含み、第三者に容易に提供しないことを前提に収集されている可能性が高いことから、本人が定期的に閲覧すると想定されるウェブサイトへの継続的な掲載、事業所内において広く頒布されている刊行物における定期的な掲載等により、本人が確実に知り得ると想定される状態に置くものとする。

【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。

2-1-12.「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

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。

「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、2-1-11.「本人が容易に知り得る状態」及び 2-1-12.「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」の両者の趣旨に合致する方法である。

【本人の知り得る状態に該当する事例】

事例１）問い合わせ窓口を設け、問い合わせがあれば、口頭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。

2-1-13.「提供」

法第２３条第１項

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。

その他、法第２３条第２項等に記述がある。

「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。

2-2.個人情報取扱事業者の義務等

2-2-1.個人情報の利用目的関係（法第１５条～第１６条関連）

（1）利用目的の特定（法第１５条第１項関連）

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。

個人情報取扱事業者は、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。

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、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できる限り具体的に特定する必要がある（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

具体的には、「○○事業※における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられる。定款や寄附行為等に想定されている事業の内容に照らして、個人情報によって識別される本人からみて、自分の個人情報が利用される範囲が合理的に予想できる程度に特定している場合や業種を明示することで利用目的の範囲が想定される場合には、これで足りるとされることもあり得るが、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らない。また、単に「事業活動」、「お客様のサービスの向上」等のように抽象的、一般的な内容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らない。

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ましい。

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、その旨特定しなければならない。

雇用管理情報の利用目的の特定に当たっても、事業者において雇用管理情報が最終的にどのような事業の用に供され、どのような目的で利用されるかが本人にとって一般的かつ合理的に想定できる程度に具体的であることが望ましく、個別具体的な利用目的を詳細に列挙するまでの必要はないものの、抽象的であっても雇用管理情報の取扱いが利用目的の達成に必要な範囲内か否かを実際に判断できる程度に明確にするものとする。つまり、利用目的の達成に必要な範囲内か否かをめぐって、事業者と本人との間で争いとならない程度に明確にするものとし、当該争いの発生を未然に防止するためには、雇用管理分野における個人情報保護に関するガイドライン第 10 に定めるところにより、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しい。

また、雇用管理情報は、機微に触れる情報を含むとともに項目ごとに利用目的が異なることも想定されるため、可能な限り個人情報の項目ごとに利用目的を特定することが望ましい。

※○○事業の特定に当たっては、社会通念上、本人からみてその特定に資すると認められる範囲に特定することが望ましい。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場合がある。

【具体的に利用目的を特定している事例】

事例１）「○○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いたします。」

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」

（2)利用目的の変更（法第１５条第２項、法第１８条第３項関連）

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。

上記（1)により特定した利用目的は、社会通念上、本人が想定することが困難でないと認められる範囲内で変更することは可能である。変更された利用目的は、本人に通知※1するか、又は公表※2しなければならない。

なお、本人が想定することが困難であると認められる変更を行う場合は、法第１６条に従って本人の同意を得なければならない。

※１「本人に通知」については、2-1-7.参照。

※２「公表」については、2-1-8.参照。

＊本人が想定することが困難でないと認められる範囲内の基準

利用目的で示した個人情報を取り扱う事業の範囲を超えての変更は、あらかじめ本人の同意なく行うことはできない。

利用目的において、一連の個人情報の取扱いの典型を具体性をもって示していた場合は、その典型例から推測できる範囲内で変更することができる。

【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○○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。

（3）利用目的による制限（法第１６条第１項関連）

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。

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、個人情報を取り扱う場合は、あらかじめ本人の同意※を得なければならない。

同意を得るために個人情報を利用すること（メールの送付や電話をかけること等）は、当初の利用目的として記載されていない場合でも、目的外利用には該当しない。

※「本人の同意」については、2-1-10.参照。

【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

（4）事業の承継（法第１６条第２項関連）

法第１６条第２項

個人情報取扱事業者は、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。

個人情報取扱事業者が、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ならず、本人の同意を得る必要はない。

（5）適用除外（法第１６条第３項関連）

以下のような場合には、上記（3）及び(4)において本人による同意を得ることが求められる場合でも、その適用を受けない。

（ｉ）法令に基づく場合（法第１６条第３項第１号関連）

法第１６条第３項第１号
　前２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

法令に基づいて個人情報を取り扱う場合は、その適用を受けない。

上記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、その他各種税法に類似の規定あり。）等が考えられる。これらについては、強制力を伴っており、一律これに該当する。

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（捜査に必要な取調べ）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する。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るが、提供に当たっては、同照会制度の目的に則した必要性と合理性が認められるかを考慮する必要がある。

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、消費生活用製品安全法第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

（ⅱ）人の生命、身体又は財産の保護（法第１６条第３項第２号関連）

法第１６条第３項第２号

前２項の規定は、次に掲げる場合については、適用しない。

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。

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、その適用を受けない。

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師に提供する場合

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）製品事故※1が生じたため、又は、製品事故は生じていないが、人の生命若しくは身体に危害を及ぼす急迫した危険が存在するため、製造事業者等が消費生活用製品をリコール※2する場合で、販売事業者、修理事業者又は設置工事事業者等が当該製造事業者等に対して、当該製品の購入者等の情報を提供する場合

※１製品事故とは、消費生活用製品の使用に伴い生じた事故のうち、
①一般消費者の生命又は身体に対する危害が発生した事故、あるいは、
②消費生活用製品が滅失し、又はき損した事故であって、一般消費者の生命又は身体に対する危害が発生するおそれのあるもの、
のいずれかであって、消費生活用製品の欠陥によって生じたものでないことが明らかな事故以外のものをいう（消費生活用製品安全法第２条第４項）。

※２リコールとは、消費生活用製品による事故の発生の拡大可能性を最小限にするための事業者による対応をいう。具体的には、①消費者への注意喚

起（消費者に対する製品事故のリスクに関する適切な情報提供）、②流通及び販売段階からの回収、並びに③消費者の保有する製品の交換、改修（点検、修理及び部品の交換等）又は引き取りを実施することをいう。

（ⅲ）公衆衛生の向上等（法第１６条第３項第３号関連）

法第１６条第３項第３号

前２項の規定は、次に掲げる場合については、適用しない。

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。

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。）は、その適用を受けない。

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

（ⅳ）国の機関等への協力（法第１６条第３項第４号関連）

法第１６条第３項第４号

前２項の規定は、次に掲げる場合については、適用しない。

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。

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、その適用を受けない。

事例１）事業者等が、税務署の職員等の任意調査に対し、個人情報を提出する場合

事例２）事業者等が警察の任意の求めに応じて個人情報を提出する場合

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

2-2-2.個人情報の取得関係（法第１７条～第１８条関連）

（1）適正取得（法第１７条関連）

> 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。

個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはならない。

なお、不正の利益を得る目的で、又はその保有者に損害を加える目的で、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１，０００万円以下の罰金、又はその併科。法人に対する３億円以下の罰金）が科され得る。

また、第三者からの提供（法第 23 条第１項各号に掲げる場合並びに個人情報の取扱いの委託、事業の承継及び共同利用に伴い、個人情報を提供する場合を除く。）により、個人情報（政令第２条第２号に規定するものから取得した個人情報を除く。）を取得する場合には、提供元の法の遵守状況（例えば、オプトアウト、利用目的、開示手続、問合わせ・苦情の受付窓口を公表していることなど）を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、例えば、取得の経緯を示す契約書等の書面を点検する等により、当該個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。

【個人情報取扱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）親の同意がなく、十分な判断能力を有していない子どもから、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）又は上記事例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）利用目的の通知又は公表（法第１８条第１項関連）

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。

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※1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※2するか、又は公表しなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

法施行前から保有している個人情報については、法施行時に個人情報の取得行為がなく、法第１８条の規定は適用されない。ただし、保有個人データに関する事項の本人への周知については、法施行時に法第２４条第１項の措置を講ずる必要がある（2-2-5-1.参照）。

※１「公表」については、2-1-8.参照。
※２「本人に通知」については、2-1-7.参照。

【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

（３）直接書面等による取得（法第１８条第２項関連）

法第１８条第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（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。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。

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らない。また、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も、あらかじめ、本人に対し、その利用目的を明示する必要はないが、その場合は法第１８条第１項に基づいて、取得後速やかにその利用目的を、本人に通知し、又は公表しなければならない。

※「本人に対して、その利用目的を明示」については、2-1-9.参照。

【あらかじめ、本人に対し、その利用目的を明示しなければならない場合】

事例１）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

（４）利用目的の変更（法第１８条第３項関連）

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。

個人情報取扱事業者は、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※1するか、又は公表※2しなければならない（2-2-1.(2)参照）。

※１「本人に通知」については、2-1-7.参照。
※２「公表」については、2-1-8.参照。

（５）適用除外（法第１８条第４項関連）

以下の場合においては、上記（2)、(3)及び(4)はその適用を受けない。

（ｉ）本人又は第三者の権利利益を害するおそれ（法第１８条第４項第１号関連）

法第１８条第４項第１号
前３項の規定は、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

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は、その適用を受けない。

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

（ⅱ）当該個人情報取扱事業者の権利等を害するおそれ（法第１８条第４項第２号関連）

法第１８条第４項第２号

前３項の規定は、次に掲げる場合については、適用しない。

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個人情報取扱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

利用目的を本人に通知し、又は公表することにより企業秘密に関すること等が他社に明らかになり、当該個人情報取扱事業者の権利又は利益が侵害されるおそれがある場合は、その適用を受けない。

事例１）通知又は公表される利用目的の内容により、当該個人情報取扱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かか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

（ⅲ）国の機関等への協力（法第１８条第４項第３号関連）

法第１８条第４項第３号

前３項の規定は、次に掲げる場合については、適用しない。

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。

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個人情報の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場合は、その適用を受けない。

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個人情報取扱事業者に限って提供する場合、警察から受け取った当該個人情報取扱事業者が、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

（ⅳ）利用目的が自明（法第１８条第４項第４号関連）

法第１８条第４項第４号

前３項の規定は、次に掲げる場合については、適用しない。

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

個人情報が取得される状況から見て利用目的が自明であると認められる場合は、その適用を受けない。

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。）

2-2-3.個人データの管理（法第１９条～第２２条関連）

2-2-3-1.データ内容の正確性の確保（法第１９条関連）

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。

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らない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

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、その必要な範囲内で正確性・最新性を確保すれば足りる。

2-2-3-2.安全管理措置（法第２０条関連）

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。

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、物理的及び技術的な安全管理措置を講じなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失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。その際には、特に、中小企業者（中小企業基本法（昭和３８年法律第１５４号）第２条第１項各号に掲げる中小企業者をいう。以下同じ。）においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。また、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。なお、クレジットカード情報については、別添の「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ましい。

【必要かつ適切な安全管理措置を講じているとはいえない場合】

事例１）公開されることを前提としていない個人データが事業者のウェブ画面上で不特定多数に公開されている状態を個人情報取扱事業者が放置している場合

事例２）組織変更が行われ、個人データにアクセスする必要がなくなった従業者が個人データにアクセスできる状態を個人情報取扱事業者が放置していた場合で、その従業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（従業者の監督及び委託先の監督の義務違反ともならない場合）】

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、シュレッダー等による処理を行わずに廃棄し、又は、廃品回収に出した場合

組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】

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
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

【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「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

・従業者の役割・責任の明確化
＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。
・個人データの安全管理の実施及び運用に関する責任及び権限を有する者として、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））を設置し、原則として、役員を任命すること
・個人データの取扱いを総括する部署の設置、及び個人情報保護管理者（ＣＰＯ）が責任者となり、社内の個人データの取扱いを監督する「管理委員会」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
・個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者が社内の対応を確認すること（必要に応じ、外部の知見を有する者を活用し確認することを含む）などによる、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づいた場合の、代表者等への報告連絡体制の整備
・個人データの漏えい等（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（法第３１条を参照）。
・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
・漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備

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示
・個人データの取扱いに関する規程等の整備とそれらに従った運用
・個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用
＊なお、これらについてのより詳細な記載事項については、下記の【個人データの取扱いに関する規程等に記載することが望まれる事項の例】を参照。
・個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
・個人データの取扱いを委託する場合における委託先の選定基準、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切に行われたことを示す監査証跡※の保持
※保持しておくことが望まれる監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかの記録）、教育受講者一覧表等が考えられる。

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る。

(ア)事実調査、原因の究明

(イ)影響範囲の特定

(ウ)再発防止策の検討・実施

(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望ましい。

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る。

・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。）

(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業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）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る。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。

ただし、以下の場合は、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望ましい。

・機微にわたる個人データ（(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等）を漏えいした場合

・信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、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）に報告を行う。

ｃ．関係機関への報告

認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。

なお、ａ．及びｂ．のいずれの場合も、事業者は次の事例について、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る。

・ファクシミリやメールの誤送信（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、報告する必要はない（2-2-3-2.【安全管理措置の義務違反とはならない事例（従業者の監督及び委託先の監督の義務違反ともならない場合）】参照）。

(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、個人データ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重要である。

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る。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しい。

・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等に記載することが望まれる事項の例】

以下、(１)取得・入力、(２)移送・送信、(３)利用・加工、(４)保管・バックアップ、(５)消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。

(１)取得・入力

①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。）

②手続の明確化と手続に従った実施
・取得・入力する際の手続の明確化
・定められた手続による取得・入力の実施
・権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という。）での入力作業の実施
・個人データを入力できる端末の、業務上の必要性に基づく限定
・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）

③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

④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
①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

②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機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

③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

④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

①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

②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とともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）

③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

④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

①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

②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

③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

④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

①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

②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。）

③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

④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

人的安全管理措置

人的安全管理措置とは、従業者（「個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。）に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】
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
なお、管理者が定めた規程等を守るように監督することについては、法第２１条を参照。

【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「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しい。
＊個人情報に関する非開示の義務を、就業規則等の社内規程に規定することも考え

られる。なお、社内規程に個人情報に関する非開示の義務を規定する場合には、特に、労働基準法第８９条及び第９０条などの労働関連法規を遵守する必要がある。

＊個人情報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）ことが望ましい。

・非開示契約に違反した場合の措置に関する規程の整備

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

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

物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

【物理的安全管理措置として講じなければならない事項】

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

【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 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

・入退館（室）の記録
・個人データを取り扱う業務の、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によるのぞき見等の防止
・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
・入退館（室）の際における業務上許可を得ていない記録機能を持つ媒体及び機器の持ち込み及び持ち出しの禁止と検査の実施
・カメラによる撮影や作業への立ち会い等による記録又はモニタリングの実施

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

技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】

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

【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】

※技術的安全管理措置については、①から⑧までの各項目を遵守するとともに、複数の手法を組み合わせ、個人データ及びそれを取り扱う情報システム全体の安全性を確保することが重要である。各項目を実践するための各手法については、以降の①～⑧において、項目ごとに例示する。また、技術的安全管理措置の典型的な手法には例えば次のような方法がある。

「②個人データへのアクセス制御」
典型的手法）ファイアウォール、ルータ、サーバ等の設定
「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」
典型的手法）ウイルス対策ソフトウェアの導入

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正当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、ワンタイムパスワードによる認証、物理的に所持が必要な認証デバイス（ＩＣカード等）による認証、生体認証等）の実施

＊識別と認証においては、複数の手法を組み合わせて実現することが望ましい。

＊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。

＊生体認証を利用する場合には、当該識別と認証の方法を実施するために必要な情報（例えば、指紋、静脈）が、特定の個人を識別することができることから、個人情報に該当する場合があることに留意する。

・個人データへのアクセス権限を有する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る。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施

・アクセス権限を有する者に付与する権限の最小化

・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）

＊個人データを格納するためのデータベースを構成要素に含む情報システムを構築する場合には、当該情報システム自体へのアクセス制御に加えて、情報システムの構成要素であるデータベースへのアクセス制御を別に実施し、それぞれにアクセス権限を設定することが望ましい。

＊アクセス権限の設定を情報システム全体と別に実施する場合にあっては、無権限アクセスからの保護に係る機器等の設定として、特に不要アカウントの無効化や初期設定されている標準アカウントのパスワード変更を実施することが望ましい。

・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しい。

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

・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ＯＳ・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。）

＊個人データにアクセスできる者を許可する権限については、情報システム内において当該権限を含む管理者権限を分割する等して、不正利用を防止することが望ましい。

・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及び不正が疑われる異常な記録の存否の定期的な確認

＊個人データへのアクセスや操作の成功と失敗の記録については、情報システムを構成する各システムへのアクセスや操作の成功と失敗等の記録を組み合わせ、各個人データへのアクセスや操作の失敗を全体として記録することが考えられる。

・採取した記録の漏えい、滅失及びき損からの適切な保護

＊採取した記録を漏えい、滅失及びき損から保護するためには、当該記録を適切に管理された外部記録媒体ないしログ収集用のサーバ等に速やかに移動することが望ましい。

＊システム管理者等の特権ユーザーのアクセス権限を用いても、採取した記録を改ざん・不正消去できないよう、対策することが望ましい

＊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。

⑤「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及び当該ソフトウェアの有効性・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）

・端末及びサーバ等のオペレーティングシステム（ＯＳ）、ミドルウェア（ＤＢＭＳ等）、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

・組織で許可していないソフトウェアの導入防止のための対策

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

・個人データの移送時における紛失・盗難に備えるための対策（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）による個人データの送信（例えば、本人及び従業者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）時における、個人データの暗号化等の秘匿化（例えば、ＳＳＬ、Ｓ／ＭＩＭＥ等）

＊暗号を利用する場合には、復号に必要な鍵についても十分注意して管理する必要がある。

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（正確な動作確認を要する等、個人データの利用が不可欠な場合であっても、動作確認に影響のない範囲で、個人データの一部を他のデータに置き換える等の措置を講じることが考えられる。）

・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

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場合があることに留意する。

＊特権ユーザーによる個人データへのアクセス状況については、特に注意して監視することが望ましい。

・個人データを取り扱う情報システムへの外部からのアクセス状況の監視（例えば、ＩＤＳ・ＩＰＳ等）

＊監視システムを利用する場合には、事業者等が業務で行う送受信の実態に合わせ、当該装置について適切に設定し、定期的にその動作を確認することが必要になる。

2-2-3-3.従業者の監督（法第２１条関連）

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。

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（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失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。また、特に、中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。

【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】

事例１）従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、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録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

【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。

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しい。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しい。

なお、本ガイドライン及び雇用管理分野における個人情報保護に関するガイドライン第 10 に規定する雇用管理に関する個人情報の取扱いに関する重要事項とは、モニタリングに関する事項等をいう。

・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。

2-2-3-4.委託先の監督（法第２２条関連）

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。

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、委託を受けた者に対し必要かつ適切な監督をしなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、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た、必要かつ適切な措置を講じるものとする。特に、中小企業者においては、自ら又は委託先の事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第２０条に基づく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が含まれる。

なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。

①委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第２０条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行った上で、個人情報保護管理者（ＣＰＯ）等が、適切に評価することが望ましい。

（ア）組織的安全管理措置
- 個人データの安全管理措置を講じるための組織体制の整備
- 個人データの安全管理措置を定める規程等の整備と規程等に従った運用
- 個人データの取扱状況を一覧できる手段の整備
- 個人データの安全管理措置の評価、見直し及び改善
- 事故又は違反への対処

（イ）人的安全管理措置
- 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
- 従業者に対する内部規程等の周知・教育・訓練の実施

（ウ）物理的安全管理措置
- 入退館（室）管理の実施
- 盗難等の防止
- 機器・装置等の物理的な保護

（エ）技術的安全管理措置

・　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

②委託契約の締結

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、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を合理的に把握することを盛り込むことが望ましい。

③委託先における個人データ取扱状況の把握

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ためには、定期的に、監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者（ＣＰＯ）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

委託元が委託先について「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、再委託する場合は注意を要する。

このため、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先から事前報告又は承認を求める、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が法第２０条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。

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」を行うことが望ましい。

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、委託処理の透明化を進めることが望ましい。

【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】

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

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

・委託元及び委託先の責任の明確化
  ･委託先において、個人データを取り扱う者（委託先で作業する委託先の従業者以外の者を含む）の氏名又は役職等（なお、委託の実態に応じて、例えば、契約書とは別に、個人データを取り扱う者のリスト等により、個人データを取り扱う者を把握するなど、適切な対応を行うことが望ましい。）
・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事前報告又は承認
・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（例えば、安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項も含まれる。）
・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

2-2-4.第三者への提供（法第２３条関連）

（1）原則（法第２３条第１項関連）

法第２３条第１項

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。

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。

個人情報取扱事業者は、あらかじめ※1、本人の同意を得※2ないで、個人データを第三者に提供してはならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。同意の取得に当たっては、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示すこと。

※１「あらかじめ」とは、「個人データの第三者への提供に当たりあらかじめ」をいう。
※２「本人の同意を得（る）」については、2-1-10.参照。

【第三者提供とされる事例】（ただし、法第２３条第４項各号の場合を除く。）
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】（ただし、利用目的による制限がある。）
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、以下の場合は本人の同意なく第三者への提供を行うことができる。

（ⅰ）法令に基づいて個人データを提供する場合

（事例は、2-2-1(5)（ⅰ）と同様。）

【追加事例】
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

（ⅱ）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。）

（事例は、2-2-1(5)（ⅱ）と同様。）

(ⅲ)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。）

（事例は、2-2-1(5)(ⅲ)と同様。）

(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

（事例は、2-2-1(5)(ⅳ)と同様。）

(2)オプトアウト（法第２３条第２項関連）

法第２３条第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。

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。

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※1を行っている場合には、前項の規定にかかわらず、本人の同意なく、個人データを第三者に提供することができる。

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ない。

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、名簿等の入手元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元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しい。

【オプトアウトの事例】

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

事例２）データベース事業者（ダイレクトメール用の名簿等を作成し、販売）

※１「第三者提供におけるオプトアウト」とは、提供に当たりあらかじめ、以下の①から④までの事項すべてを、本人に通知※２し、又は本人が容易に知り得る状態※３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。
※２「本人に通知」については、2-1-7.参照。
※３「本人が容易に知り得る状態」については、2-1-11.参照。

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

事例１）氏名、住所、電話番号
事例２）氏名、商品購入履歴

③第三者への提供の手段又は方法

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本人の求めに応じて第三者への提供を停止すること。

（３）第三者に該当しないもの（法第２３条第４項関連）

以下の（ⅰ）から（ⅲ）までの場合については、個人情報取扱事業者とは別の主体として形式的には第三者に該当するものの、本人との関係において提供主体である個人情報取扱事業者と一体のものとして取り扱うことに合理性がある場合には、第三者に該当しないものとすべきとの考え方に基づき、第三者に該当しないとしており、このような要件を満たす場合には、本人の同意又は第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができる。

（ⅰ）委託（法第２３条第４項第１号関連）

法第２３条第４項第１号
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。
１　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。

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（法第２２条関連）。

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

（ⅱ）事業の承継（法第２３条第４項第２号関連）

法第２３条第４項第２号
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。
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

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。

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らない。

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

（ⅲ）共同利用（法第２３条第４項第３号関連）

法第２３条第４項第３号
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。
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、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

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①から④まで

の情報をあらかじめ※1本人に通知※2し、又は本人が容易に知り得る状態※3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ときには、当該個人データの提供を受ける事業者は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性があると考えられることから、第三者に該当しない。また、既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合には、既に取得している事業者が法第１５条第１項の規定により特定した利用目的の範囲で共同して利用しなければならない。

また、事業者が共同利用を実施する場合には、共同利用者における責任等を明確にし円滑に実施する観点から、①から④までの情報のほか、以下に掲げる（ア）から（カ）までの事項について、あらかじめ取り決めておくことが望ましい。

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る。

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らない。

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わけでもない。

例えば、グループ企業でイベントを開催する場合において、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ときには共同利用となるが、自社でイベントを開催する場合において、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ときには、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、共同利用とはならない。

※１「あらかじめ」とは、「個人データの共同利用に当たりあらかじめ」をいう。
※２「本人に通知」については、2-1-7.参照。
※３「本人が容易に知り得る状態」については、2-1-11.参照。

【共同利用を行うことがある事例】

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１５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内で個人データを共同利用する場合

①共同して利用される個人データの項目

個人データの項目について、本人に通知し、又は本人が容易に知り得る状態に置

いていなければならない。

事例１）氏名、住所、電話番号
事例２）氏名、商品購入履歴

②共同して利用する者の範囲

「共同利用の趣旨」は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で当該個人データを共同して利用することである。

したがって、共同利用者の範囲については、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある。

なお、当該範囲が明確である限りにおいては、事業者の名称等を個別にすべて列挙する必要がない場合もある。

事例）本人がどの事業者まで利用されるか判断できる程度に明確な形で示された「提携基準」及び「最新の共同利用者のリスト」等を、共同利用者の全員が、本人が容易に知り得る状態に置いているとき

③利用する者の利用目的

共同して利用する個人データについて、その取得時の利用目的をすべて、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なければならない。

利用目的が個人データの項目によって異なる場合には区別して記載することが望ましい。

④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

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について、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なければならない。

ここでいう「責任を有する者」とは、共同して利用するすべての事業者の中で、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いい、共同利用者のうち一事業者の内部の担当責任者をいうものではない。

【上記①から④までの事項のほかに取り決めておくことが望ましい事項】

（ア）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）
（イ）各共同利用者の個人情報取扱責任者、問い合わせ担当者及び連絡先
（ウ）共同利用する個人データの取扱いに関する事項
・個人データの漏えい等防止に関する事項
・目的外の加工、利用、複写、複製等の禁止
・共同利用終了後のデータの返還、消去、廃棄に関する事項
（エ）共同利用する個人データの取扱いに関する取決が遵守されなかった場合の措置
（オ）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
（カ）共同利用を終了する際の手続

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③及び④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※1で変更することができ、変更する前に、本人に通知※2又は本人が容易に知り得る状態※3に置かなければならない。

また、上記①及び②については原則として変更は認められないが、次の場合、引き続き共同利用を行うことができる。

【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※4が行われた場合

※１「本人が想定することが困難でないと認められる範囲内」については、2-2-1.(2)参照。

※２「本人に通知」については、2-1-7.参照。

※３「本人が容易に知り得る状態」については、2-1-11.参照。

※４「事業の承継」については、2-2-4.(3)(ⅱ)参照。

(４)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（法第２３条第１項第１号から第４号までに該当する場合を除く。）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。その際、事業の性質及び雇用管理に関する個人データの取扱状況等に応じ、必要かつ適切な措置を講じるものとする。

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。

2-2-5.保有個人データに関する事項の公表、保有個人データの開示・訂正・利用停止等（法第２４条～第３０条関連）

2-2-5-1.保有個人データに関する事項の公表等（法第２４条関連）

（1）保有個人データに関する事項の本人への周知（法第２４条第１項関連）

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。

1　当該個人情報取扱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（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　次項、次条第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に応じる手続（第３０条第２項の規定により手数料の額を定めたときは、その手数料の額を含む。）
4　前３号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

政令第５条

法第２４条第１項第４号の政令で定めるものは、次に掲げるものとする。

1　当該個人情報取扱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
2　当該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ある場合にあっては、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

個人情報取扱事業者は、保有個人データについて、以下の①から④までの情報を本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）※1に置かなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

法施行前から保有している個人情報については、法施行時に個人情報の取得行為がなく、法第１８条の規定が適用されないので、法施行時に法第２４条第１項の措置を講ず

る必要がある。

※１「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、2-1-12.参照。

①個人情報取扱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（ただし、一定の場合※２を除く。法第１５条以下で用いられる個人情報に関する「利用目的」に同じ。）

※２「一定の場合」とは、以下をいう。

ア）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（事例は 2-2-2.(5)(ⅰ)と同様。）

イ）利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は利益が侵害されるおそれがある場合（事例は 2-2-2.(5)(ⅱ)と同様。）

ウ）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個人情報の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場合（事例は 2-2-2.(5)(ⅲ)と同様。）

③保有個人データの利用目的の通知及び保有個人データの開示に係る手数料の額（定めた場合に限る）※３並びに開示等の求め※４の手続

※３行政機関の保有する情報の公開に関する法律（平成１１年法律第４２号）第１６条及び同法施行令（平成１２年政令第４１号）第１３条第１項第１号に基づく開示請求に係る手数料は３００円である（開示実施手数料は別途発生）。

※４「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う。

④保有個人データの取扱いに関する苦情及び問い合わせの申出先（個人情報取扱事業者が認定個人情報保護団体※５に所属している場合は、その団体の名称及び申出先も含む。）

※５「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ある（法第３７条以下参照）。

（参考）

法第３７条第１項

個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人（法人でない団体で代表者又は管理人の定めのあるものを含む。次条第３号ロにおいて同じ。）は、主務大臣の認定を受けることができる。

１　業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）の個人情報の取扱いに関する第４２条の規定による苦情の処理

２　個人情報の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供

３　前２号に掲げるもののほか、対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

法第３７条第２項

前項の認定を受けようとする者は、政令で定めるところにより、主務大臣に申請しなければならない。

法第３７条第３項

主務大臣は、第１項の認定をしたときは、その旨を公示しなければならない。

法第４２条第１項

認定個人情報保護団体は、本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならない。

法第４２条第２項

認定個人情報保護団体は、前項の申出に係る苦情の解決について必要があると認めるときは、当該対象事業者に対し、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できる。

法第４２条第３項

対象事業者は、認定個人情報保護団体から前項の規定による求めがあったときは、正当な理由がないのに、これを拒んではならない。

（２）保有個人データの利用目的の通知（法第２４条第２項、第３項関連）

法第２４条第２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１８条第４項第１号から第３号までに該当する場合

法第２４条第３項

個人情報取扱事業者は、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。

個人情報取扱事業者は、以下の（ⅰ）から(ⅳ)までの場合を除いて、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※しなければならない。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らない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

※「本人に通知」については、2-1-7.参照。

(ⅰ)上記（1)の措置により、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

（事例は 2-2-2.(5)(ⅰ)と同様。）

(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個人情報取扱事業者の権利又は利益が侵害されるおそれがある場合

（事例は(2-2-2.(5)(ⅱ)と同様。）

(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

（事例は 2-2-2.(5)（iii）と同様。）

2-2-5-2.保有個人データの開示（法第２５条関連）

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。ただし、開示することにより次の各号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。

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　当該個人情報取扱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

政令第６条

法第２５条第１項の政令で定める方法は、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、当該方法）とする。

個人情報取扱事業者は、本人から、自己が識別される保有個人データの開示（存在しないときにはその旨を知らせることを含む。）を求められたときは、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法があるときはその方法※1）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（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

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しい。

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

雇用管理情報の開示の求めに応じる手続については、個人情報取扱事業者は、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開示とすることが想定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らない。

※１「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」について

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の意味である。

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、個人情報取扱

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む。）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る。開示の求めがあった者からの同意の取り方として、個人情報取扱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る。

ただし、開示することにより下記の（ⅰ）から(ⅲ)まで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が、この場合は、その旨を本人に通知※２しなければならない。

※２「本人に通知」については、2-1-7.参照。

（ⅰ）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

事例）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

（ⅱ）個人情報取扱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

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

（ⅲ）他の法令に違反することとなる場合

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

2-2-5-3.保有個人データの訂正等（法第２６条関連）

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、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。

法第２６条第２項

個人情報取扱事業者は、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。

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※1として、訂正等※2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（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

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ることとなる。

※１「原則」…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ない。ただし、その場合には、遅滞なく、訂正等を行わない旨を本人に通知※3しなければならない。

※２「訂正等」とは、保有個人データの内容の訂正、追加又は削除※4をいう。

※３「本人に通知」については、2-1-7.参照。

※４「削除」とは、不要な情報を除くことをいう。

【訂正を行う必要がない事例】

事例）訂正等の対象が事実でなく評価に関する情報である場合

2-2-5-4.保有個人データの利用停止等（法第２７条関連）

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。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。

法第２７条第２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２３条第１項の規定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第三者への提供の停止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、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

法第２７条第３項

個人情報取扱事業者は、第１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。

個人情報取扱事業者は、本人から、手続違反※1の理由により保有個人データの利用の停止等※2が求められた場合には、原則※3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※4しなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。

※１「手続違反」とは、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をいう。

※２「利用の停止等」とは、保有個人データの利用の停止、消去※5又は第三者への提供の停止をいう。

※３「原則」…違反を是正するための必要な限度を超えている場合や手続違反である旨の指摘が正しくない場合には、利用の停止等を行う必要はない。ただし、その場合には、遅滞なく、利用の停止等を行わない旨を本人に通知しなければならない。　なお、保有個人データの全部消去を求められた場合であっても、利用停止によって手続違反を是正できる場合であれば、そのような措置を講ずることにより、義務を果たしたことになり、必ずしも、求められた措置をそのまま実施する必要はない。

※４「本人に通知」については、2-1-7.参照。

※５「消去」とは、保有個人データを保有個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等を含む。

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しい。

2-2-5-5.理由の説明（法第２８条関連）

法第２８条
個人情報取扱事業者は、第２４条第３項、第２５条第２項、第２６条第２項又は前条第３項の規定により、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。

個人情報取扱事業者は、保有個人データの公表・開示・訂正・利用停止等において、その措置をとらない旨又はその措置と異なる措置をとる旨を本人に通知※する場合は、併せて、本人に対して、その理由を説明するように努めなければならない。

※「本人に通知」については、2-1-7.参照。

2-2-5-6.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。

政令第７条

法第２９条第１項の規定により個人情報取扱事業者が開示等の求めを受け付ける方法として定めることができる事項は、次に掲げるとおりとする。

１　開示等の求めの申出先

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方式

３　開示等の求めをする者が本人又は次条に規定する代理人であることの確認の方法

４　法第３０条第１項の手数料の徴収方法

政令第８条

法第２９条第３項の規定により開示等の求めをすることができる代理人は、次に掲げる代理人とする。

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

（１）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（ⅰ）から（ⅳ）までの事項を定めることができる。また、その求めを受け付ける方法を定めた場合には、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）※2に置いておかなければならない（上記(2-2-5-1.参照）。なお、個人情報取扱事業者が、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る。

※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う。

※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、2-1-12.参照。

（ⅰ）開示等の求めの受付先

（ⅱ）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）

（ⅲ）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ず、本人確認のために事業者が保有している個人データに比して必要以上に多くの情報を求めないようにするなど、本人に過重な負担を課すものとならないよう配慮しなくてはならない。）

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）

(ⅳ)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。

(２)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。

(３)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。

2-2-5-7.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。）※に置いておかなければならない（上記 2-2-5-1.参照）。

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（2-2-5-1.(1)③参照）。

※「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、2-1-12.参照。

2-2-6.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。

なお、必要な体制の整備に当たっては、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る。

2-2-7.経過措置（法附則第２条～第５条関連）

（本人の同意に関する経過措置）
法附則第２条
この法律の施行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１５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１６条第１項又は第２項の同意があったものとみなす。

法附則第３条
この法律の施行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２３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。

（通知に関する経過措置）
法附則第４条
第２３条第２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、この法律の施行前に、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。

法附則第５条
第２３条第４項第３号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、この法律の施行前に、本人に通知されているときは、当該通知は、同号の規定により行われたものとみなす。

2-2-1.(3)、2-2-1.(4)及び 2-2-4.(1)の「本人の同意」については、法施行前に得たものであっても、法に基づく同意があったものとみなされる。

また、2-2-4.(2)及び 2-2-4.(3)(ⅲ)の「本人に通知」については、法施行前に本人に通知していても、法に基づき、本人に通知したものとみなされる。

なお、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（2-2-2.(2)参照）。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る（2-2-5-1.(1)参照）。

2-3.民間団体付属の研究機関等における個人情報の取扱いについて

法第５０条第１項第３号
個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。

３　大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者　学術研究の用に供する目的

民間団体付属の研究機関等における研究活動についても、個人情報を取り扱う場面があるが、当該機関が学術研究を主たる目的とするものであって、当該活動が学術研究の用に供する目的である場合には、法第５０条第１項第３号により、法の適用除外となる。そのため、個人情報の取扱いを含む研究活動を行う、経済産業分野における民間団体付属の研究機関等について、法第５０条第１項第３号の考え方を整理する。

民間企業の研究機関等、「○○研究所」との名称を有している機関であっても、単に製品開発を目的としているものについては、学術研究を主たる目的として活動しているものとはいえないことから、本法の「学術研究を目的とする機関又は団体」には該当しない。

＊法第５０条第１項第３号の考え方

法第５０条第１項第３号に規定する「大学その他の学術研究を目的とする機関」とは、学術研究（新しい法則や原理の発見、分析や方法論の確立、新しい知識やその応用方法の体系化、先端的な学問領域の開拓等）を主たる目的とする機関である。

そのような機関において、個人情報を取り扱う目的の全部又は一部が、学術研究の用に供する目的である場合には、個人情報取扱事業者としての義務を課されない。

【適用除外となる場合】

事例）学術研究を主たる目的とする団体付属の研究機関において、個人情報を利用する目的の全部又は一部が学術研究である場合

【適用除外とならない場合】

事例１）学術研究を主たる目的とする団体付属の研究機関において、個人情報を利用する目的が商品開発情報の分析のみ（学術研究目的を含まない。）である場合

事例２）学術研究を主たる目的としない団体付属の研究機関

３．「勧告」、「命令」及び「緊急命令」についての考え方

法第３４条第１項

主務大臣は、個人情報取扱事業者が第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

法第３４条第２項

主務大臣は、前項の規定による勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者に対し、その勧告に係る措置をとるべきことを命ずることができる。

法第３４条第３項

主務大臣は、前２項の規定にかかわらず、個人情報取扱事業者が第１６条、第１７条、第２０条から第２２条まで又は第２３条第１項の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

法第５６条

第３４条第２項又は第３項の規定による命令に違反した者は、６月以下の懲役又は３０万円以下の罰金に処する。

法第５８条第１項

法人（法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項において同じ。）の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、前２条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。

法第５８条第２項

法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行為につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に関する法律の規定を準用する。

法第３４条に規定される経済産業大臣の「勧告（第１項）」「命令（第２項）」及び「緊急命令（第３項）」については、個人情報取扱事業者が本ガイドラインに沿って必要な措置等を講じたか否かにつき判断して行うものとする。

すなわち、本ガイドライン中、「しなければならない」と記載されている規定について、それに従わなかった場合は、法第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定違反と判断され得る。違反と判断された際、実際、「勧告」を行うこととなるのは、個人の権利利益を保護するため必要があると認めるときである。一方、本ガイドライン中、「望ましい」と記載されている規定については、それに従わなかった場合でも、法第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定違反と判断されることはないが、個人情報保護の推進の観点から個人情報取扱事業者においては、できるだけ取り組むことが望まれる。

「命令」は、単に「勧告」に従わないことをもって発することはなく、正当な理由なくその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切

迫していると認めるときに限られる。なお、「勧告」に従わなかったか否かを明確にするため、経済産業大臣は、「勧告」に係る措置を講ずべき期間を設定して「勧告」を行うこととする。

「緊急命令」は、個人情報取扱事業者が法第１６条、第１７条、第２０条から第２２条まで又は第２３条第１項の規定に違反した場合において、個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときに、「勧告」を前置せずに行う。

なお、「命令」及び「緊急命令」に従わなかったか否かを明確にするため、経済産業大臣は、「命令」及び「緊急命令」に係る措置を講ずべき期間を設定して「命令」及び「緊急命令」を行い、当該期間中に措置が講じられない場合は、「罰則（法第５６条、第５８条）」を適用される。

４．ガイドラインの見直し

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。

５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格

（１）個人情報保護のためのマネジメント体制の確立

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マネジメントシステムを確立し、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 JIS Q 15001「個人情報保護マネジメントシステムー要求事項」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 JIS X 5070「セキュリティ技術ー情報技術セキュリティの評価基準」、日本工業規格 JIS Q 27001「情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステム―要求事項」、日本工業規格 JIS Q 27002「情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」、独立行政法人情報処理推進機構（ＩＰＡ）の「組織における内部不正防止ガイドライン」、総務省・経済産業省の「電子政府における調達のために参照すべき暗号のリスト （ＣＲＹＰＴＲＥＣ暗号リスト）」、ISO/IEC 18033（暗号アルゴリズム国際規格）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る。

（２）個人情報保護を推進する上での考え方や方針の策定等

個人情報取扱事業者は、「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、消費者等本人との信頼関係を構築し事業活動に対する社会

の信頼を確保するために重要である。

個人情報取扱事業者は、一定の事項に関して公表しなければならないが（2-1-8 参照）、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である。

●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。）

(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)問い合わ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。

※「認定個人情報保護団体の対象事業者」とは、認定個人情報保護団体の構成員である個人情報取扱事業者（傘下企業）、又は団体が苦情処理等の業務を行うことについて当該団体と契約関係等にある事業者等

（３）消費者等本人に対する分かりやすい説明の実施

個人情報取扱事業者は、消費者等本人との信頼関係を構築する観点から、消費者等本人に対して､個人情報取扱事業者の個人情報保護を推進する上での考え方や方針等について、以下に掲げる基準を参考にして、冗長で分かりにくい表現を避け、消費者等本人に誤解を与えることなく分かりやすい表現で表示することが望ましい。

分かりやすい説明の実施に際して参考とすべき基準

１．記載事項

（１）必要十分な記載事項

１　個人情報の取扱いに関する情報として、以下の７項目が記載されていること
１）提供するサービスの概要
２）取得する個人情報と取得の方法
３）個人情報の利用目的
４）個人情報や個人情報を加工したデータの第三者への提供の有無及び提供先
５）消費者等本人による個人情報の提供の停止の可否、訂正及びその方法
６）問合せ先
７）保存期間、廃棄

２．記載方法

（１）取得する個人情報とその取得方法に係る記載方法

２　取得する個人情報の項目とその取得方法について、可能な限り細分化し、具体的に記載していること

３　取得する個人情報の項目やその取得方法のうち、消費者等本人にとって分かりにくいものを明確に記載していること

（２）個人情報の利用目的に係る記載方法

４　取得する個人情報の利用目的を特定し、具体的に記載していること
５　個人情報の利用目的が、取得する個人情報の項目と対応して記載されていること
６　取得する個人情報の利用目的のうち、消費者等本人にとって分かりにくいものを明確に記載していること

（３）第三者への提供の有無及び個人情報や個人情報を加工したデータの提供先に係る記載方法

７　個人情報取扱事業者が取得する個人情報や個人情報を加工したデータを第三者に提供する場合、その提供先（事後的に提供先を変更する場合は提供先の選定条件を含む）及び提供目的が記載されていること
８　個人情報取扱事業者が取得した個人情報を加工したデータを第三者に提供する場合、その加工方法が記載されていること

（４）消費者等本人による個人情報の提供の停止の可否及びその方法に係る記載方法

９　消費者等本人が個人情報取扱事業者による個人情報の取得の中止又は利用の停止が可能であるかが記載され、可能である場合には取得の中止方法又は利用の停止方法を明示して記載していること

上記の「参考とすべき基準」は、個人情報を含む「パーソナルデータ」を利活用してサービスを行う事業者が、消費者から「パーソナルデータ」を取得し利用する際に、消費者に対して行う情報提供や個人情報保護を推進する上での考え方や方針等を分かりやすく説明した文書等の内容の適切性を第三者が事前に評価する際のツールとして経済産業省が策定した「評価基準」を基に作成したものである。

同評価基準の評価方法等については、経済産業省ホームページの「個人情報保護」のページ中に掲載されている。

（経済産業省ホームページの「個人情報保護」のページ）
http://www.meti.go.jp/policy/it_policy/privacy/index.html

（４）その他参考となる事項

本ガイドラインで取り上げた典型的な事例のほか、より具体的な事例は「個人情報保護ガイドライン等に関するＱ＆Ａ」で取り上げる。ただし、同Ｑ＆Ａの事例も、すべての事例を網羅することを目的とするものではなく、実際には個別事案ごとの検討が必要となる。

同Ｑ＆Ａは、経済産業省ホームページの「個人情報保護」のページ中に掲載され、随時更新する予定である。

（経済産業省ホームページの「個人情報保護」のページ）
http://www.meti.go.jp/policy/it_policy/privacy/index.html

別添

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。

また、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か月以内のいずれの日においても５０００人を超えない者であっても、クレジット販売関係事業者等であれば、クレジットカード情報等の保護の観点から、以下の措置を講じることも含め、本ガイドラインに規定されている事項を遵守することが望ましい。

なお、クレジットカード会社は「経済産業分野のうち信用分野における個人情報保護ガイドライン（平成１６年経済産業省告示第４３６号）」に定めがある場合には、その例による。

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

【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スキミング防止のためのセキュリティ機能（漏えい防止措置等）を搭載する等）
・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

・インターネット取引においてクレジットカード情報等を本人から直接取得するなど、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

「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」改正案の新旧対照表

（傍線部分は改正部分）

○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

改　正　案	現　行
１．目的及び適用範囲 （略） 本ガイドラインは、経済産業大臣が法を執行する際の基準となるものであるが、従業員の個人情報（雇用管理に関するもの）に関する部分については、雇用管理分野における個人情報保護に関するガイドライン（平成２４年厚生労働省告示第３５７号）との整合性に留意した（「従業員」及び「従業者」の用語については、「2-2-3-3.従業者の監督（法第２１条関連）」参照。）。このため、本ガイドラインのうちこれらの部分については、厚生労働大臣及び経済産業大臣の共同で作成し、両大臣が共同して法を執行する。 （略） 2-1-1.「個人情報」（法第２条第１項関連） 法第２条第１項 （略） （略） 【個人情報に該当する事例】 事例１）～５）　（略） 事例６）雇用管理情報（事業者が労働者等（個人情報取扱事業者に使用されている労働者、個人情報取扱事業者に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個人情報取扱事業者に使用されていた者。以下同じ。）の雇用管理のために収集、保管、利用等する個人情報をいい、その限りにお	１．目的及び適用範囲 （略） 本ガイドラインは、経済産業大臣が法を執行する際の基準となるものであるが、従業員の個人情報（雇用管理に関するもの）に関する部分については、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）との整合性に留意した（「従業員」及び「従業者」の用語については、「2-2-3-3.従業者の監督（法第２１条関連）」参照。）。このため、本ガイドラインのうちこれらの部分については、厚生労働大臣及び経済産業大臣の共同で作成し、両大臣が共同して法を執行する。 （略） 2-1-1.「個人情報」（法第２条第１項関連） 法第２条第１項 （略） （略） 【個人情報に該当する事例】 事例１）～５）　（略） 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。）

いて、病歴、収入、家族関係等の機微に触れる情報（以下「機微に触れる情報」という。）を含む労働者個人に関するすべての情報が該当する。以下同じ。） 事例７）・８）　（略）	事例７）・８）　（略）
（略）	（略）
2-1-8.「公表」 法第１８条第１項 （略） 「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。 特に雇用管理情報は、機微に触れる情報を含むため、事業者は、自らの置かれた状況に応じ、労働者等に内容が確実に伝わる媒体を選択する等の配慮を行うものとする。	2-1-8.「公表」 法第１８条第１項 （略） 「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。
（略）	（略）
2-1-11.「本人が容易に知り得る状態」 法第２３条第２項 （略） 法２３条第４項第３号 （略） 「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。 特に雇用管理情報は、機微に触れる情報を含み、第三者に容易に提供しないことを前提に収集されている可能性が高いことから、本人が定期的に閲覧すると想定されるウェブサイトへの継続的な掲載、事業所内に	2-1-11.「本人が容易に知り得る状態」 法第２３条第２項 （略） 法２３条第４項第３号 （略） 「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。

おいて広く頒布されている刊行物における定期的な掲載等により、本人が確実に知り得ると想定される状態に置くものとする。	
（略）	（略）
2-2-1. 個人情報の利用目的関係（法第１５条～第１６条関連）	2-2-1. 個人情報の利用目的関係（法第１５条～第１６条関連）
（1）利用目的の特定（法第１５条第１項関連） 法第１５条第１項 （略）	（1）利用目的の特定（法第１５条第１項関連） 法第１５条第１項 （略）
個人情報取扱事業者は、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。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、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できる限り具体的に特定する必要がある（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。 具体的には、「○○事業※における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられる。定款や寄附行為等に想定されている事業の内容に照らして、個人情報によって識別される本人からみて、自分の個人情報が利用される範囲が合理的に予想できる程度に特定している場合や業種を明示することで利用目的の範囲が想定される場合には、これで足りるとされることもあり得るが、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らない。また、単に「事業活動」、「お客様のサービスの向上」等のように抽象的、一般的な内容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らない。 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ましい。 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	個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。個人情報取扱事業者は、利用目的をできる限り具体的に特定しなければならない。利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、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できる限り具体的に特定する必要がある（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。 具体的には、「○○事業※における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられる。定款や寄附行為等に想定されている事業の内容に照らして、個人情報によって識別される本人からみて、自分の個人情報が利用される範囲が合理的に予想できる程度に特定している場合や業種を明示することで利用目的の範囲が想定される場合には、これで足りるとされることもあり得るが、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らない。また、単に「事業活動」、「お客様のサービスの向上」等のように抽象的、一般的な内容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らない。 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

る場合には、利用目的において、その旨特定しなければならない。 雇用管理情報の利用目的の特定に当たっても、事業者において雇用管理情報が最終的にどのような事業の用に供され、どのような目的で利用されるかが本人にとって一般的かつ合理的に想定できる程度に具体的であることが望ましく、個別具体的な利用目的を詳細に列挙するまでの必要はないものの、抽象的であっても雇用管理情報の取扱いが利用目的の達成に必要な範囲内か否かを実際に判断できる程度に明確にするものとする。つまり、利用目的の達成に必要な範囲内か否かをめぐって、事業者と本人との間で争いとならない程度に明確にするものとし、当該争いの発生を未然に防止するためには、雇用管理分野における個人情報保護に関するガイドライン第 10 に定めるところにより、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しい。 また、雇用管理情報は、機微に触れる情報を含むとともに項目ごとに利用目的が異なることも想定されるため、可能な限り個人情報の項目ごとに利用目的を特定することが望ましい。	な取組が望ましい。 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、その旨特定しなければならない。 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（個人情報取扱事業者に使用されている労働者、個人情報取扱事業者に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個人情報取扱事業者に使用されていた者。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らない。
（略）	（略）
2-2-2.個人情報の取得関係（法第１７条～第１８条関連） （１）適正取得（法第１７条関連） 法第１７条 （略） 個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはならない。 なお、不正の利益を得る目的で、又はその保有者に損害を加える目的で、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１，０００万円以下の罰金、又はその併科。法人に対する３億円以下の罰金）が科され得る。 また、第三者からの提供（法第 23 条第１項各号に掲げる場合並びに個人情報の取扱いの委託、事業の承継及び共同利用に伴い、個人情報を提供する場合を除く。）により、個人情報（政令第２条第２号に規定する	2-2-2.個人情報の取得関係（法第１７条～第１８条関連） （１）適正取得（法第１７条関連） 法第１７条 （略） 個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはならない。 なお、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１，０００万円以下の罰金、又はその併科。法人に対する３億円以下の罰金）が科され得る。

ものから取得した個人情報を除く。）を取得する場合には、提供元の法の遵守状況（例えば、オプトアウト、利用目的、開示手続、問合せ・苦情の受付窓口を公表していることなど）を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、例えば、取得の経緯を示す契約書等の書面を点検する等により、当該個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。	
（略）	（略）
2-2-3-2.安全管理措置（法第２０条関連） 法第２０条 （略） 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、物理的及び技術的な安全管理措置を講じなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の程度を考慮し、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。その際には、特に、中小企業者（中小企業基本法（昭和３８年法律第１５４号）第２条第１項各号に掲げる中小企業者をいう。以下同じ。）においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。また、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。なお、クレジットカード情報については、別添の「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ましい。	2-2-3-2.安全管理措置（法第２０条関連） 法第２０条 （略） 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、物理的及び技術的な安全管理措置を講じなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失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。その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。なお、クレジットカード情報については、別添の「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ましい。
（略）	（略）
組織的安全管理措置 組織的安全管理措置とは、安全管理について従業者（法第２１条参照）	組織的安全管理措置 組織的安全管理措置とは、安全管理について従業者（法第２１条参照）

の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。 （略） **【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　「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 ・従業者の役割・責任の明確化 ＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。 ・個人データの安全管理の実施及び運用に関する責任及び権限を有する者として、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））を設置し、原則として、役員を任命すること ・個人データの取扱いを総括する部署の設置、及び個人情報保護管理者（ＣＰＯ）が責任者となり、社内の個人データの取扱いを監督する「管理委員会」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 ・個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者が社内の対応を確認すること（必要に応じ、外部の知見を有する者を活用し確認することを含む）などによる、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づいた場合の、代表者等への報告連絡体制の整備 ・個人データの漏えい等（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	の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。 （略） **【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「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 ・従業者の役割・責任の明確化 ＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。 ・個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））の設置 ・個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定 ・個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定 ・個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化 ・監査責任者の設置 ・監査実施体制の整備 ・個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備 ・個人データの漏えい等（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（法第３１条を参照）。 ・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 ・漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備	通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第３１条を参照）。 ・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 ・漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備
②～⑤　（略）	②～⑤　（略）
【個人データの取扱いに関する規程等に記載することが望まれる事項の例】 以下、(１)取得・入力、(２)移送・送信、(３)利用・加工、(４)保管・バックアップ、(５)消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。 (１) 取得・入力 ①　（略）	【個人データの取扱いに関する規程等に記載することが望まれる事項の例】 以下、(１)取得・入力、(２)移送・送信、(３)利用・加工、(４)保管・バックアップ、(５)消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。 (１) 取得・入力 ①　（略）
②手続の明確化と手続に従った実施 ・(略) ・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）	②手続の明確化と手続に従った実施 ・(略) ・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。）
(２)　（略）	(２)　（略）
(３)利用・加工 ①　（略）	(３)利用・加工 ①　（略）
②　手続の明確化と手続に従った実施 ・（略） ・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	②　手続の明確化と手続に従った実施 ・（略） ・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、個人データを閲覧だけできる端末では、CD-R、

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とともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）	USB メモリ等の外部記録媒体を接続できないようにする。）
③・④　（略）	③・④　（略）
（４）・（５）　（略）	（４）・（５）　（略）
人的安全管理措置 人的安全管理措置とは、従業者（「個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。）に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。	人的安全管理措置 人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。
（略）	（略）
物理的安全管理措置 物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。	物理的安全管理措置 物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。
【物理的安全管理措置として講じなければならない事項】 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	【物理的安全管理措置として講じなければならない事項】 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
【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　「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 ・入退館（室）の記録 ・（略） ・（略）	【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　「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 （追加） ・（略） ・（略）
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	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によるのぞき見等の防止 ・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 ・入退館（室）の際における業務上許可を得ていない記録機能を持つ媒体及び機器の持ち込み及び持ち出しの禁止と検査の実施 ・カメラによる撮影や作業への立ち会い等による記録又はモニタリングの実施	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によるのぞき見等の防止 ・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（略）	③（略）
技術的安全管理措置 技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。 **【技術的安全管理措置として講じなければならない事項】** 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 **【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】** ※技術的安全管理措置については、①から⑧までの各項目を遵守する	技術的安全管理措置 技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。 **【技術的安全管理措置として講じなければならない事項】** 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 **【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】** （追加）

とともに、複数の手法を組み合わせ、個人データ及びそれを取り扱う情報システム全体の安全性を確保することが重要である。各項目を実践するための各手法については、以降の①～⑧において、項目ごとに例示する。また、技術的安全管理措置の典型的な手法には例えば次のような方法がある。 「②個人データへのアクセス制御」 典型的手法）ファイアウォール、ルータ、サーバ等の設定 「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」 典型的手法）ウイルス対策ソフトウェアの導入	
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正当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、ワンタイムパスワードによる認証、物理的に所持が必要な認証デバイス（ＩＣカード等）による認証、生体認証等）の実施 ＊識別と認証においては、複数の手法を組み合わせて実現することが望ましい。 ＊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。 ＊生体認証を利用する場合には、当該識別と認証の方法を実施するために必要な情報（例えば、指紋、静脈）が、特定の個人を識別することができることから、個人情報に該当する場合があることに留意する。 ・個人データへのアクセス権限を有する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、電子証明書等）の実施	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正当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しい。 ・個人データへのアクセス権限を有する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	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る。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施 ・アクセス権限を有する者に付与する権限の最小化 ・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） ＊個人データを格納するためのデータベースを構成要素に含む情報システムを構築する場合には、当該情報システム自体へのアクセス制御に加えて、情報システムの構成要素であるデータベースへのアクセス制御を別に実施し、それぞれにアクセス権限を設定することが望ましい。 ＊アクセス権限の設定を情報システム全体と別に実施する場合にあっては、無権限アクセスからの保護に係る機器等の設定として、特に不要アカウントの無効化や初期設定されている標準アカウントのパスワード変更を実施することが望ましい。 ・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しい。 ＊特権ユーザーに対するアクセス制御については、例えば、トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。 ・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ＯＳ・ウェブアプリケーションのぜい弱性	・識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施 ・アクセス権限を有する者に付与する権限の最小化 ・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しい。 ＊特権ユーザーに対するアクセス制御については、例えば、トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。 ・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の

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。） ＊個人データにアクセスできる者を許可する権限については、情報システム内において当該権限を含む管理者権限を分割する等して、不正利用を防止することが望ましい。 ・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及び不正が疑われる異常な記録の存否の定期的な確認 ＊個人データへのアクセスや操作の成功と失敗の記録については、情報システムを構成する各システムへのアクセスや操作の成功と失敗等の記録を組み合わせ、各個人データへのアクセスや操作の失敗を全体として記録することが考えられる。 ・採取した記録の漏えい、滅失及びき損からの適切な保護 ＊採取した記録を漏えい、滅失及びき損から保護するためには、当該記録を適切に管理された外部記録媒体ないしログ収集用のサーバ等に速やかに移動することが望ましい。 ＊システム管理者等の特権ユーザーのアクセス権限を用いても、採取した記録を改ざん・不正消去できないよう、対策することが望ましい。 ＊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。 ⑤「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及び当該ソフトウェアの有効性・	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する。 ⑤「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

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） ・端末及びサーバ等のオペレーティングシステム（ＯＳ）、ミドルウェア（ＤＢＭＳ等）、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 ・組織で許可していないソフトウェアの導入防止のための対策	・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 ・個人データの移送時における紛失・盗難に備えるための対策（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）による個人データの送信（例えば、本人及び従業者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）時における、個人データの暗号化等の秘匿化（例えば、ＳＳＬ、Ｓ／ＭＩＭＥ等） ＊暗号を利用する場合には、復号に必要な鍵についても十分注意して管理する必要がある。	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、本人及び従業者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（正確な動作確認を要する等、個人データの利用が不可欠な場合であっても、動作確認に影響のない範囲で、個人データの一部を他のデータに置き換える等の措置を講じることが考えられる。） ・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	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	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場合があることに留意する。 ＊特権ユーザーによる個人データへのアクセス状況については、特に注意して監視することが望ましい。 ・個人データを取り扱う情報システムへの外部からのアクセス状況の監視（例えば、ＩＤＳ・ＩＰＳ等） ＊監視システムを利用する場合には、事業者等が業務で行う送受信の実態に合わせ、当該装置について適切に設定し、定期的にその動作を確認することが必要になる。	＊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場合があることに留意する。
2-2-3-3. 従業者の監督（法第２１条関連） 法第２１条 （略） 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（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失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。また、特に、中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。 （略） 【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。 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しい。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しい。	2-2-3-3. 従業者の監督（法第２１条関連） 法第２１条 （略） 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（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失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。 （略） 【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。 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しい。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しい。

なお、本ガイドライン及び雇用管理分野における個人情報保護に関するガイドライン第10に規定する雇用管理情報の取扱いに関する重要事項とは、モニタリングに関する事項等をいう。	なお、本ガイドライン及び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）第三九（一）に規定する雇用管理に関する個人情報の取扱いに関する重要事項とは、モニタリングに関する事項等をいう。
（略）	（略）
2-2-3-4.委託先の監督（法第２２条関連）	2-2-3-4.委託先の監督（法第２２条関連）
法第２２条 （略）	法第２２条 （略）
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、委託を受けた者に対し必要かつ適切な監督をしなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、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た、必要かつ適切な措置を講じるものとする。特に、中小企業者においては、自ら又は委託先の事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。	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、委託を受けた者に対し必要かつ適切な監督をしなければならない（2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、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た、必要かつ適切な措置を講じるものとする。
「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第２０条に基づく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が含まれる。 なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。	「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第２０条に基づく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が含まれる。
① 委託先の選定 委託先の選定に当たっては、委託先の安全管理措置が、少なくとも	①委託先の選定 委託先を適切に選定するためには、委託先において実施される個人

法第２０条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行った上で、個人情報保護管理者（ＣＰＯ）等が、適切に評価することが望ましい。 （ア）組織的安全管理措置 ・ 個人データの安全管理措置を講じるための組織体制の整備 ・ 個人データの安全管理措置を定める規程等の整備と規程等に従った運用 ・ 個人データの取扱状況を一覧できる手段の整備 ・ 個人データの安全管理措置の評価、見直し及び改善 ・ 事故又は違反への対処 （イ）人的安全管理措置 ・ 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 ・ 従業者に対する内部規程等の周知・教育・訓練の実施 （ウ）物理的安全管理措置 ・ 入退館（室）管理の実施 ・ 盗難等の防止 ・ 機器・装置等の物理的な保護 （エ）技術的安全管理措置 ・ 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	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しい。また、委託先の評価は適宜実施することが望ましい。
② 委託契約の締結 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、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を合理的に把握する	② 委託契約の締結 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、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を合理的に把握する

ことを盛り込むことが望ましい。 （削除）	ことを盛り込むことが望ましい。 なお、本人からの損害賠償請求に係る責務を、安全管理措置に係る責任分担を無視して一方的に委託先に課すなど、優越的地位にある者が委託元の場合、委託先に不当な負担を課すことがあってはならない。
③　委託先における個人データ取扱状況の把握 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ためには、定期的に、監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者（ＣＰＯ）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。	③委託先における個人データ取扱状況の把握 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しい。
委託元が委託先について「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、注意を要する。このため、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先から事前報告又は承認を求める、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が法第２０条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。	委託元が委託先について「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、注意を要する。
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」を行うことが望ましい。 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、委託処理の透明化を進めることが望ましい。	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」を行うことが望ましい。 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、委託処理の透明化を進めることが望ましい。
（略）	（略）
【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】	【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

・委託元及び委託先の責任の明確化 ・委託先において、個人データを取り扱う者（委託先で作業する委託先の従業者以外の者を含む）の氏名又は役職等（なお、委託の実態に応じて、例えば、契約書とは別に、個人データを取り扱う者のリスト等により、個人データを取り扱う者を把握するなど、適切な対応を行うことが望ましい。） ・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事前報告又は承認 ・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（例えば、安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項も含まれる。） ・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 2-2-4.第三者への提供（法第２３条関連） （１）　（略） （２）オプトアウト（法第２３条第２項関連） 法第２３条第２項 （略） （略）	・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 2-2-4.第三者への提供（法第２３条関連） （１）　（略） （２）オプトアウト（法第２３条第２項関連） 法第２３条第２項 （略） （略）

（３）第三者に該当しないもの（法第２３条第４項関連） 以下の（ⅰ）から（ⅲ）までの場合については、個人情報取扱事業者とは別の主体として形式的には第三者に該当するものの、本人との関係において提供主体である個人情報取扱事業者と一体のものとして取り扱うことに合理性がある場合には、第三者に該当しないものとすべきとの考え方に基づき、第三者に該当しないとしており、このような要件を満たす場合には、本人の同意又は第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができる。 （ⅰ）～（ⅱ）（略） （ⅲ）共同利用（法第２３条第４項第３号関連） 法第２３条第４項第３号 （略） 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①から④までの情報をあらかじめ※1本人に通知※2し、又は本人が容易に知り得る状態※3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ときには、当該個人データの提供を受ける事業者は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性があると考えられることから、第三者に該当しない。また、既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合には、既に取得している事業者が法第１５条第１項の規定により特定した利用目的の範囲で共同して利用しなければならない。 また、事業者が共同利用を実施する場合には、共同利用者における責任等を明確にし円滑に実施する観点から、①から④までの情報のほか、以下に掲げる（ア）から（カ）までの事項について、あらかじめ取り決めておくことが望ましい。 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る。 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らない。	（３）第三者に該当しないもの（法第２３条第４項関連） 以下の（ⅰ）から（ⅲ）までの場合は、第三者に該当しないため、本人の同意又は第三者提供におけるオプトアウトを行うことなく、情報の提供を行うことができる。 （ⅰ）～（ⅱ）（略） （ⅲ）共同利用（法第２３条第４項第３号関連） 法第２３条第４項第３号 （略） 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①から④までの情報をあらかじめ※1本人に通知※2し、又は本人が容易に知り得る状態※3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。また、既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合は、既に取得している事業者が法第１５条第１項の規定により特定した利用目的の範囲で共同して利用しなければならない。 共同利用する場合、①から④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しい。 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る。 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らない。

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わけでもない。 例えば、グループ企業でイベントを開催する場合において、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ときには共同利用となるが、自社でイベントを開催する場合において、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ときには、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、共同利用とはならない。 ※１「あらかじめ」とは、「個人データの共同利用に当たりあらかじめ」をいう。 ※２「本人に通知」については、2-1-7. 参照。 ※３「本人が容易に知り得る状態」については、2-1-11. 参照。	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わけでもない。 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るが、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、共同利用とはならない。 ※１「あらかじめ」とは、「個人データの共同利用に当たりあらかじめ」をいう。 ※２「本人に通知」については、2-1-7. 参照。 ※３「本人が容易に知り得る状態」については、2-1-11. 参照。
【共同利用を行うことがある事例】 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１５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内で個人データを共同利用する場合	**【共同利用を行うことがある事例】** 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１５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内で個人データを共同利用する場合
①共同して利用される個人データの項目 個人データの項目について、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なければならない。 事例１）氏名、住所、電話番号 事例２）氏名、商品購入履歴	**①共同して利用される個人データの項目** 事例１）氏名、住所、電話番号 事例２）氏名、商品購入履歴
②共同して利用する者の範囲	**②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**

「共同利用の趣旨」は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で当該個人データを共同して利用することである。 したがって、共同利用者の範囲については、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある。 なお、当該範囲が明確である限りにおいては、事業者の名称等を個別にすべて列挙する必要がない場合もある。	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。）
事例）本人がどの事業者まで利用されるか判断できる程度に明確な形で示された「提携基準」及び「最新の共同利用者のリスト」等を、共同利用者の全員が、本人が容易に知り得る状態に置いているとき	事例）最新の共同利用者のリストを本人が容易に知り得る状態に置いているとき
③利用する者の利用目的 共同して利用する個人データについて、その取得時の利用目的をすべて、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なければならない。 利用目的が個人データの項目によって異なる場合には区別して記載することが望ましい。	③利用する者の取得時の利用目的（共同して利用する個人データのすべての利用目的）
④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 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について、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なければならない。 ここでいう「責任を有する者」とは、共同して利用するすべての事業者の中で、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いい、共同利用者のうち一事業者の内部の担当責任者をいうものではない。	④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のではない。）
【上記①から④までの事項のほかに取り決めておくことが望ましい事項】 （ア）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	【上記①から④までの事項のほかに取り決めておくことが望ましい事項】 ●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）

枠組） （イ）各共同利用者の個人情報取扱責任者、問い合わせ担当者及び連絡先 （ウ）共同利用する個人データの取扱いに関する事項 ・個人データの漏えい等防止に関する事項 ・目的外の加工、利用、複写、複製等の禁止 ・共同利用終了後のデータの返還、消去、廃棄に関する事項 （エ）共同利用する個人データの取扱いに関する取決が遵守されなかった場合の措置 （オ）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 （カ）共同利用を終了する際の手続	●各共同利用者の個人情報取扱責任者、問い合わ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 ・個人データの漏えい等防止に関する事項 ・目的外の加工、利用、複写、複製等の禁止 ・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
法第２３条第５項 （略）	法第２３条第５項 （略）
上記③及び④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※1で変更することができ、変更する前に、本人に通知※2又は本人が容易に知り得る状態※3に置かなければならない。 また、上記①及び②については原則として変更は認められないが、次の場合、引き続き共同利用を行うことができる。	上記③及び④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※1で変更することができ、変更する前に、本人に通知※2又は本人が容易に知り得る状態※3に置かなければならない。 また、上記①及び②については原則として変更は認められないが、次の場合、引き続き共同利用を行うことができる。
【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※4が行われた場合	**【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※4が行われた場合
※１「本人が想定することが困難でないと認められる範囲内」については、2-2-1.(2)参照。 ※２「本人に通知」については、2-1-7.参照。 ※３「本人が容易に知り得る状態」については、2-1-11.参照。 ※４「事業の承継」については、2-2-4.(3)(ⅱ)参照。	※１「本人が想定することが困難でないと認められる範囲内」については、2-2-1.(2)参照。 ※２「本人に通知」については、2-1-7.参照。 ※３「本人が容易に知り得る状態」については、2-1-11.参照。 ※４「事業の承継」については、2-2-4.(3)(ⅱ)参照。

（略）	（略）
５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格 （１）個人情報保護のためのマネジメント体制の確立 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マネジメントシステムを確立し、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 JIS 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 JIS 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 JIS 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 JIS Q 27002「情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」、独立行政法人情報処理推進機構（ＩＰＡ）の「組織における内部不正防止ガイドライン」、総務省・経済産業省の「電子政府における調達のために参照すべき暗号のリスト（ＣＲＹＰＴＲＥＣ暗号リスト）」、ISO/IEC 18033（暗号アルゴリズム国際規格）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る。	**５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格** 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マネジメントシステムを確立し実施し、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 JIS 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 JIS 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 JIS 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 JIS 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」、ISO/IEC 18033（暗号アルゴリズム国際規格）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る。
（２）個人情報保護を推進する上での考え方や方針の策定等 個人情報取扱事業者は、「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、消費者等本人との信頼関係を構築し事業活動に対する社会の信頼を確保するために重要である。 個人情報取扱事業者は、一定の事項に関して公表しなければならないが（2-1-8 参照）、個人情報取扱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である。	また、個人情報取扱事業者は、「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重要である。 個人情報取扱事業者は、一定の事項に関して公表しなければならないが（2-1-8 参照）、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である。

●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。）	●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。） （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）問い合わ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。 ※「認定個人情報保護団体の対象事業者」とは、認定個人情報保護団体の構成員である個人情報取扱事業者（傘下企業）、又は団体が苦情処理等の業務を行うことについて当該団体と契約関係等にある事業者等 （３）消費者等本人に対する分かりやすい説明の実施 個人情報取扱事業者は、消費者等本人との信頼関係を構築する観点から、消費者等本人に対して、個人情報取扱事業者の個人情報保護を推進する上での考え方や方針等について、以下に掲げる基準を参考にして、冗長で分かりにくい表現を避け、消費者等本人に誤解を与えることなく分かりやすい表現で表示することが望ましい。 分かりやすい説明の実施に際して参考とすべき基準 １．記載事項 （１）必要十分な記載事項 １　個人情報の取扱いに関する情報として、以下の 7 項目が記載されていること	・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。） （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）問い合わ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。 ※「認定個人情報保護団体の対象事業者」とは、認定個人情報保護団体の構成員である個人情報取扱事業者（傘下企業）、又は団体が苦情処理等の業務を行うことについて当該団体と契約関係等にある事業者等

１）提供するサービスの概要 ２）取得する個人情報と取得の方法 ３）個人情報の利用目的 ４）個人情報や個人情報を加工したデータの第三者への提供の有無及び提供先 ５）消費者等本人による個人情報の提供の停止の可否、訂正及びその方法 ６）問合せ先 ７）保存期間、廃棄 ２．記載方法 （１）取得する個人情報とその取得方法に係る記載方法 ２　取得する個人情報の項目とその取得方法について、可能な限り細分化し、具体的に記載していること ３　取得する個人情報の項目やその取得方法のうち、消費者等本人にとって分かりにくいものを明確に記載していること （２）個人情報の利用目的に係る記載方法 ４　取得する個人情報の利用目的を特定し、具体的に記載していること ５　個人情報の利用目的が、取得する個人情報の項目と対応して記載されていること ６　取得する個人情報の利用目的のうち、消費者等本人にとって分かりにくいものを明確に記載していること （３）第三者への提供の有無及び個人情報や個人情報を加工したデータの提供先に係る記載方法 ７　個人情報取扱事業者が取得する個人情報や個人情報を加工したデータを第三者に提供する場合、その提供先（事後的に提供先を変更する場合は提供先の選定条件を含む）及び提供目的が記載されていること ８　個人情報取扱事業者が取得した個人情報を加工したデータを第三者に提供する場合、その加工方法が記載されていること （４）消費者等本人による個人情報の提供の停止の可否及びその方法に係る記載方法 ９　消費者等本人が個人情報取扱事業者による個人情報の取得の中止又は利用の停止が可能であるかが記載され、可能である場合には取得の中止方法又は利用の停止方法を明示して記載しているこ	

と 上記の「参考とすべき基準」は、個人情報を含む「パーソナルデータ」を利活用してサービスを行う事業者が、消費者から「パーソナルデータ」を取得し利用する際に、消費者に対して行う情報提供や個人情報保護を推進する上での考え方や方針等を分かりやすく説明した文書等の内容の適切性を第三者が事前に評価する際のツールとして経済産業省が策定した「評価基準」を基に作成したものである。 同評価基準の評価方法等については、経済産業省ホームページの「個人情報保護」のページ中に掲載されている。 （経済産業省ホームページの「個人情報保護」のページ） http://www.meti.go.jp/policy/it_policy/privacy/index.html （４）その他参考となる事項 本ガイドラインで取り上げた典型的な事例のほか、より具体的な事例は「個人情報保護ガイドライン等に関するＱ＆Ａ」で取り上げる。ただし、同Ｑ＆Ａの事例も、すべての事例を網羅することを目的とするものではなく、実際には個別事案ごとの検討が必要となる。 同Ｑ＆Ａは、経済産業省ホームページの「個人情報保護」のページ中に掲載され、随時更新する予定である。 （経済産業省ホームページの「個人情報保護」のページ） http://www.meti.go.jp/policy/it_policy/privacy/index.html	本ガイドラインで取り上げた典型的な事例のほか、より具体的な事例は「個人情報保護ガイドライン等に関するＱ＆Ａ」で取り上げる。ただし、同Ｑ＆Ａの事例も、すべての事例を網羅することを目的とするものではなく、実際には個別事案ごとの検討が必要となる。 同Ｑ＆Ａは、経済産業省ホームページの「個人情報保護」のページ中に掲載され、随時更新する予定である。 （経済産業省ホームページの「個人情報保護」のページ） http://www.meti.go.jp/policy/it_policy/privacy/index.html