民間部門における電子商取引に係る
個人情報保護に関するガイドライン（Ver.4.0）

平成１８年１月１６日

次世代電子商取引推進協議会

目　次

第1章　総則

第1条（目　的）

このガイドラインは、電子商取引において個人情報を取り扱う事業者に対し、個人情報の保護に関する指針を示すことにより、インターネット等の情報ネットワーク上の個人情報の有用性と個人情報保護の必要性との調和のとれた適正な商慣行を形成し、もって高度情報通信社会の健全な進展に寄与することを目的とする。

（解説）

1.　電子商取引の健全な発展のためには、電子商取引において個人情報を取り扱うすべての企業や個人事業者が、消費者の個人情報を適切に保護する必要がある。

2.　一方で、One to One Marketing や CRM（Customer Relationship Management）に代表されるように個人情報はその業務において積極的に活用されている。このガイドラインでは、事業者に対し、顧客に対するサービスや利便性の向上あるいは事業拡大や業務効率向上を図る上で有効に個人情報を利用しながらも、個人の権利利益を適切に保護することを求めている。そして、それらをバランスよく調和させることにより電子商取引が更に健全に普及し、高度情報通信社会の進展に寄与するものと考える。

3.　個人情報の保護に関する法律（以下「個人情報保護法」という。）においても高度情報通信社会の進展の上で個人情報の有用性に配慮した個人の権利利益を保護することが目的として掲げられており、その精神は本ガイドラインと一致するものである。

参考　個人情報保護法第 1 条

第 2 条（適用範囲）

このガイドラインは，電子商取引を行うに際し情報ネットワーク上で個人情報を取り扱う事業者に適用する。

（解説）

1.　このガイドラインは、電子商取引を行うにあたりインターネット等の情報ネットワークを利用して個人情報を取得し、又は利用する事業者を対象とする。

2.　事業者は、このガイドラインを用いて次の事項を行うこととする。

(1)　個人情報の取扱いについて、適切に行われていることを確認すること。

(2)　個人情報保護推進体制を構築すること。

(3)　このガイドラインと個人情報保護推進体制が適合しているかを確認し、適合していることをウェブ画面等により社内外に表明する。

3.　このガイドラインは、上記に該当する事業者が自発的に採用するものであり、法的な拘束性を

持つものではないので、その取り扱う個人情報の量や利用方法により事業者等を限定しない。
4.　このガイドラインは、事業者が取り扱う個人情報を適用の対象とするが、その事業者の従業員の人事管理、福利厚生等のために保有する雇用管理情報（いわゆる「インハウス情報」）については、「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」（厚生労働省告示第259号）に従い、別途社内規程等を定めることが望ましい。
5.　電子商取引はグローバル化が進んでいるが、このガイドラインは国境を越えた商取引に伴う個人情報保護にも適用される。

第3条（定　義）

このガイドラインにおける用語の定義は、当該各号に定めるところによる。

(1)　電子商取引

インターネット等の情報ネットワーク上で、商取引及びこれを誘引するための宣伝･広告、その他の事業活動の全部又は一部を行うことをいう。

(2)　情報ネットワーク

電子商取引に限定されず、より幅広い業務や用途において利用されるインターネット等によるネットワークをいう。

(3)　個人情報

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

(4)　個人情報データベース等

個人情報を含む情報の集合物であって、特定の個人情報を電子計算機を用いて検索できるように体系的に構成したもの、及び個人情報を一定の規則にしたがって整理することにより特定の個人情報を容易に検索できるように体系的に構成し、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。

(5)　個人データ

個人情報データベース等を構成する個人情報をいう。

(6)　保有個人データ

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をいう。ただし、その存否が明らかになることにより公益その他の利益が害されるものとして以下のものに該当する場合及び 6 ヶ月以内に消去するものは除く。

①本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

②違法又は不当な行為を助長し、又は誘発するおそれがあるもの

③国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

④犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

(7) 本人

個人情報によって識別される特定の個人をいう。

(8) 事業者

電子商取引又はインターネット等の情報ネットワーク上で個人情報を取り扱う法人その他の団体又は個人であって、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。

(9) 個人情報保護管理者

事業者の代表者によって指名された者であって、個人情報保護体制の実施・運用を行う責任を有する者をいう。但し、個人事業者又は小規模事業者においては、代表者自らが個人情報保護体制の実施・運用を行う責任を有することもできる。

(10) 個人情報保護推進体制

事業者が保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメント・システムをいう。

(解説)

1. 電子商取引、インターネット等の情報ネットワークの定義について

(1) 「電子商取引」については、契約に係る商行為だけに限定せず、宣伝・広告という契約の誘引に当たる行為等その他の事業活動全般についてもインターネット等の情報ネットワーク上で行われる場合には、これに含めることとし、広くとらえている。すなわち、アンケート、抽選、懸賞への応募等により取得した個人情報、新製品やイベントの案内、マーケティングのために取り扱われる個人情報等についてもその対象としている。

(2) 「インターネット等の情報ネットワーク」は、上記の電子商取引の概念を一般的にイメージできる語句としてこのガイドラインを通じて使用している。前項に示すようにインターネット上で電子商取引が行われるネットワーク環境もそれに該当するが、BtoC (Business to Consumer) だけでなく、BtoB (Business to Business) などクローズドなユーザー間で使うエクストラネット、イントラネット等も含む。また、採用募集、雇用関連等の場面でもこのような経路で個人情報を取得する場合があり、それら全般を含むものとして表現している。

2. 個人情報の定義について

(1) 「個人情報」に関する定義については基本的に個人情報保護法に準じることとした。個人情報保護法では「個人情報データベース等」として (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構成したもの、(2) その他、特定の個人情報を容易に検索できるように体系的に構成したものとして政令で定めるもの、の 2 点が個人情報を含む情報の集合物としてあげられていた。(2) については、その後政令により、対象となるマニュアル (手作業) 処理情報としては、これに含まれる個人情報を一定の規則にしたが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と定められた。例えば、医療カルテのように体系的に整理され、すぐに検索可能なものがこれに相当すると考える。

(2)　購入履歴を基にした消費者個人の嗜好も識別性がある場合には「個人情報」に該当する。但し、商品の売れ筋の把握、将来開発する商品のために行うマーケティング調査等の統計目的で個人を特定しない形で収集し、取り扱う情報はこれに該当しない。

(3)　「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、暗号化されているかどうかを問わない。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）。

(4)　個人情報保護法は、「個人情報」、「個人データ」及び「保有個人データ」の語を使い分けており、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。

(5)　「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、当該事業者内部でも取扱部門が異なる場合等であって照合が困難な状態を除く。

【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)　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 4)　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 5)　雇用管理情報（会社が従業員を評価した情報を含む。）

事例 6)　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)　特定の個人を識別することができない統計情報

3.　個人データ・保有個人データの定義関係

(1)　企業が管理する「個人情報データベース等」を構成する個人情報を個人データと定義し、その中で企業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、利用停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する個人データを「保有個人データ」と定義している。なお、政令により、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ガイドライン 3. 定義（6）の①から④に示されるもの及び短期間（6 ヶ月以内）に消去されるものは除外される。

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）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

(2)　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、何ら取り決めがなく、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者であって、受託者ではない。

【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) キャンペーン、イベント等の実施にあたりウェブ画面を通して申し込みを受け付けた場合の申込者リストを検索できる状態にしている場合
事例 4) ウェブ画面を通じて行った、個人情報を含むアンケート結果そのものを保存した電子ファイルを検索できる状態にしている場合
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) 従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いていても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合
事例 2) アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

【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

(3) 本ガイドラインでは、ある程度の規模を持つ企業だけでなく、個人レベルで事業を営むケースも多いことから両者を総称する意味で「事業者」とした。このガイドラインを通じて、その適用対象である「個人情報の全部又は一部をインターネット等の情報ネットワークによって取り扱う事業者」を指す。なお、第2条（適用範囲）（解説)3に示すように、このガイドラインは、適用対象の事業者に対して法的な拘束性を持つものではないので、個人情報保護法における「個人情報取扱事業者」の範囲と異なり、その取り扱う個人情報の量や利用方法により適用除外となる事業者等を規定しない。なお、政令では、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ヶ月以内のいずれの日においても5000を超えない者は個人情報取扱事業者から除外されるとされている。さらに、他人の作成したカーナビや電話帳などの個人情報データベース等で個人情報として氏名、住所若しくは居所又は電話番号のみが含まれる場合であって、これを編集し、又は加工することなくその事業の用に供するときは、これ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、個人情報取扱事業者の範囲を画する際の個人情報によって識別される特定の個人の数に算入しないとされている。

(4) 「個人情報保護管理者」とは、個人情報保護体制の実施・運用を行う責任を負う者をいう。ある程度の規模を持つ企業においては、事業者の代表者によって指名されるが、個人事業者及び小規模事業者においては代表者自らがその任を負うこともある。ちなみに近年欧米の多くの大手

企業及びIT関連企業においては「チーフ・プライバシー・オフィサー（CPO＝最高個人情報保護責任者）」が任命されている。

参考　個人情報保護法第2条・政令第1条・第2条・第3条・第4条

第2章　規程・方針等

第4条（規程・方針等の策定）

事業者は，個人情報を保護するための規程を策定し、その代表者は事業の特性及び規模を考慮し、個人情報保護方針を定めるとともに、これらを実行し、維持することとする。

（解説）

1.　個人情報保護を適切に行うためには、全社に通用する基本的な内部規程が必要となる。これを基に、さらに細則的な規程類（各部門における業務について個人情報保護のための具体的対応を示す手順書なども含む）を策定し、従業者全員が同じ行動を取ることができるような構成にしておく必要がある。基本的な内部規程に一般的に含まれるべき事項としては、次に掲げる（1）から（15）までの内容が考えられる。

(1)　目的、適用範囲、定義に関する規定

その内部規程の目的、適用する業務範囲、使用する用語の定義の規定。

(2)　個人情報保護管理者及び管理体制に関する規定

個人情報保護を具体的に実施するために社内管理体制を整備するに当たり、具体的に各担当者の役割、責任及び権限を規定する。

(3)　個人情報保護方針及び法定公表事項等に関する規定

個人情報保護方針は個人情報保護の取組み及び個人情報の取り扱いに関する基本的事項についての宣言であり、法定公表事項とは、個人情報保護法により公表等を義務付けられた事項をいう。個人情報保護方針は個人情報保護に関する取組みを社内外に示す手段であり、その決定のプロセスや内容、公表の仕方等について規定する。

(4)　法令及びその他の規範の特定、個人情報の特定

事業者は、自己の個人情報の取扱いに関わる業務について法令その他の規範がある場合についてそれを遵守する必要がある。そのために適用される法令その他の規範を特定し、かつそれを参照できる手順を定めた規定を設ける。また、計画段階では、事業者が現段階で自ら保有するすべての個人情報を特定することが必要であるが、個人情報保護体制整備後においても新たに発生する業務、プロジェクト等に対応する必要から、新たに取得し保有する個人情報を特定するための手順を確立しておくことが重要である。

(5)　個人情報の利用目的の特定、利用目的の制限、適正な取得、取得に際しての利用目的の通

知、取得の制限等に関する規定

このガイドラインの第6条から第16条までに従って規定されるべきである。

(6) 個人データの内容の正確性の確保及び安全管理措置（情報セキュリティ）に関する規定

このガイドラインの第17条と第23条に従って規定されるべきである。

(7) 従業者の監督、委託先の監督、及び第三者提供の制限等個人データの管理等に関する規定

このガイドラインの第24条から第29条までに従って規定されるべきである。

(8) 情報管理技術及び個人情報保護管理技術の採用等に関する規定

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

(9) 保有個人データに関する事項の公表等及び保有個人データの開示、訂正等、利用停止等並びにその手数料等に関する規定

このガイドラインの第30条から第36条までに従って規定されるべきである。

(10) 苦情の処理等に関する規定

このガイドラインの第37条に従って規定されるべきである。

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

事業者が取り扱う個人情報に関する具体的なリスクを明確にした上で、そのような事態が起こったときの対応及びその是正措置を規定する。このガイドラインの第38条を参照して規定されるべきである。

(12) 個人情報保護の管理に関する規定

このガイドラインの第39条及び第40条を参照して規定されるべきである。

(13) 個人情報保護に関する監査等に関する規定

このガイドラインの第41条及び第42条を参照して規定されるべきである。

(14) 個人情報保護体制の見直しに関する規定

個人情報保護体制は、監査報告書及びその他の経営環境に照らして、最適な状況に 維持されなければならない。そのために個人情報保護体制の見直しに関する措置について規定する。

(15) 内部規程に違反した場合の罰則に関する規定

一般的には社員の就業規則における罰則の条項を適用する。

2. 事業者の代表者は、内部規程に基づき、事業や業務の特性及び事業者の規模を考慮し、個人情報保護方針を定め、役員及び従業者に周知しなければならない。

第 5 条（個人情報保護方針及び法定公表事項等の公表）

事業者は、個人情報保護方針及び法定公表事項等を外部向けに文書化し、自らのウェブ画面等のわかりやすい場所に公表することとする。

(解説)

事業者は、一般の人がその企業の個人情報保護方針及び法的公表事項等を入手･閲覧できるように、外部向けに文書化し、ウェブ画面等のわかりやすい場所に公表することとする。個人情報護保護方針及び法的公表事項等はトップページにリンクボタンを設置し一度のクリックでその概要を参照できることが望ましい。また、文書化にあたっては、関係法令等の遵守、個人情報の利用目的、第三者提供の有無、開示等個人情報の取り扱いに関する諸手続きなど必要な事項と内容を選定し、一般にもわかりやすく記述するものとする。なお、法定公表事項等のモデルは巻末資料を参照のこと。

第 3 章　運用

第1節　個人情報の取得等

第 6 条 (利用目的の特定)

1　事業者は、個人情報を取り扱うにあたっては、本人が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判断できる程度に可能な限り具体的にその利用の目的 (以下「利用目的」という。) を特定しなければならない。

2　事業者は、利用目的を変更する場合には, 変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

(解説)

1.　事業者は, 利用目的をできる限り特定しなければならない。

利用目的の特定に当たっては, 利用目的を単に抽象的, 一般的に特定するのではなく, 事業者において最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定する必要がある (電話帳、カーナビゲーションシステム等の取り扱いについての場合を除く。)。利用する個人情報の種類及び入手先の事業者名等を特定することまで求めているわけではない。

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

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。

2.　雇用管理情報の利用目的の特定に当たっても，単に抽象的，一般的に特定するのではなく，労働者等（事業者に使用されている労働者，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。

【具体的に利用目的を特定している事例】
事例 1)「ネット販売業における商品の発送、代金決済、新商品・サービスに関する情報の通知のために利用する。」
事例 2)「××サービスの提供にあたりサービス内容の確認、代金決済、サービスご提供後の満足度調査のお願いのために利用する。」
事例 3)「お客様向けメール・マガジンの送付先として使用する。」
事例 4)「お客様からの相談に関する回答のためにのみ利用する。」

【具体的に利用目的を特定していない事例】
事例 1)「当社の事業活動に供するため」
事例 2)「弊社が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」

3.　(2)において利用目的の変更は，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としているが、事業者が取得した個人情報の利用目的を変更しようとするときは、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ができる。
　利用目的において特定され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が、例えば，利用目的において一連の個人情報の取り扱いの典型例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を電子メールにより送信することがあります。」とした利用目的において、「郵便によりお知らせすることがある」旨追加することは、許容される。

参考　個人情報保護法第 15 条

第 7 条（利用目的による制限）

1　事業者は、あらかじめ本人の同意を得ないで、第 6 条により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
2　事業者は、合併その他の事由により他の事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。
3　前 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
②　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
③　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
④　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(解説)
1.　一旦取得した個人情報について当初の利用目的の達成に必要な範囲を超えて取り扱うときには、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。

【同意が必要な事例】
事例 1)　苦情受付のためのお客様相談センターにて収集された情報をもとに、自己商品の販売促進のために試供品を送る場合
事例 2)　就職のための求職者からの履歴書情報をもとに、自己商品の販売促進のために自己販売サイトの案内メールを送る場合

2.　「本人の同意」とは、本人が個人情報の取り扱いに関する情報を与えられたうえで、本人の個人情報が、事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう。ネットワーク上で行う場合には、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、本人からの同意する旨のメールの受信等がこれにあたる。
3.　(3)①～④の適用除外の具体的事例は次のとおり。
(1)　法令に基づく場合((3)①関連)
　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), 地方税法第72条の63(事業税に係る質問検査権、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、回答が義務づけられているため、一律これに該当する。
事例）　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
　一方、刑事訴訟法第197条第2項（捜査に必要な取調べ）等のような、個人情報の提供が任意協力の場合についても対象となり得ると考えられるが、個別の判断が必要とされる。すなわち、無条件で個人情報の提供が可能だということはなく、提供することによる公共的利益と個人情報保護との比較衡量により、提供すべきかどうかについて案件ごとに慎重に判断すべきである。
事例 1)　商法第274条の3（新会社法第 381 条 3 項･4 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 2)　株式会社の監査等に関する商法の特例に関する法律第2条（新会社法第 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
(2)　人の生命、身体又は財産の保護（(3)②関連）
　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
(3)　公衆衛生の向上等（(3)③関連）
　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
(4)　国の機関等への協力（(3)④関連）
　国の機関等が法令の定める事務を実施するうえで、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
4.　個人情報保護法の施行前に第 6 条 1 項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旨の同意に相当するものがある場合は本項の同意があったものとみなされる。

参考　個人情報保護法第 16 条　附則第 2 条

第 8 条（適正な取得）

事業者は、偽りその他不正の手段により個人情報を取得してはならない。

（解説）

1.　個人情報の取得に際し、事業者は本人に対し、個人情報の利用目的を偽るなど不正な手段を用いて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、詐欺等により取得したり、使用・開示した者には不正競争防止法（平成 5 年法律第 47 号）第14条により刑事罰（3年以下の懲役又は300万円以下の罰金）が科され得る。

2.　偽りその他不正な手段（騙す、脅す、盗むなどをいう。）により取得した第三者から、不正な手段の介在を知りながら間接的に取得してはならない。また，個人情報保護法で規定されている第三者への提供の措置を行っていない第三者からその事実を知りながら間接的に取得してはならない。

3.　住民基本台帳法の改正により運用の始まった「住民票コード」のように法令により取得を禁止されているものは取得してはならない。

【不正な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供から、取得状況から考えて関係のない親の収入事情などの家族の個人情報を（情報ネットワークを通して）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

参考　個人情報保護法第 17 条

第 9 条（取得に際しての利用目的の通知等）

事業者は、個人情報を取得する場合は，あらかじめその利用目的を公表していることが望ましい。事業者は、取得する個人情報の利用目的を公表していない場合は、取得後速やかに、その利用目的を本人に通知するか、又は公表しなければならない。

（解説）

1.　個人情報保護法第 18 条第1項では、個人情報取扱事業者は、直接的・間接的に関わらず個

人情報を取得したときの措置としてあらかじめその利用目的を公表している場合を除き、速やかにその利用目的を本人に通知又は公表することが義務づけられている。

2. 近年の電子的ネットワーク技術の急速な発展、多様化する顧客のニーズに対応するために個人情報を利用した事業活動が重要になっていることに伴い、個人情報は直接的に本人から取得される場合に加えて、本人以外から間接的に取得される場合も急激に増えてきている。このように本人の知らない間に当該個人情報が流通することによって、本人の権利利益が侵害されないよう, 特に慎重に対応する必要がある。このガイドラインにおいては、本人以外から間接的に取得する場合を含めて、個人情報保護法に準じ、原則的に本人に対し利用目的を通知又は公表することとする。

3. 通知の方法としては、電子メールの利用等があり、公表についてはウェブ画面上への掲載や自己の店舗･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･配布等が考えられる。なお、法定公表事項等のモデルは巻末資料を参照のこと。

【本人に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) 官報、職員録等から個人情報を取得する場合

事例 3) 電子メール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) 第三者から個人情報の提供を受ける場合

参考 個人情報保護法第 18 条第1項

第 10 条（情報ネットワーク上又は書面で本人から直接に取得する場合の措置）

事業者は、インターネット等の情報ネットワーク上又は書面で本人から直接当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

（解説）

1. 個人情報保護法第 18 条第2項では、本人との間で契約書等の書面で個人情報を直接に取得する場合に、あらかじめ本人に対しその利用目的を明示することを義務として課している。このガイドラインでも、第 9 条で個人情報取得時の原則的な措置を定めたうえで、とりわけインターネット等の情報ネットワーク上又は書面で本人から直接当該本人の個人情報を取得する場合等の措置として、あらかじめ本人に対しその利用目的を明示することと定めた。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。

2. 「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、情報ネットワーク上においては、申込者の入力画面のように本人がアクセスした自己のウェブ画面上、又は本人の端末装置上にその利用目的を明記することがこれにあたる。この場合申込者本人が入力する以前、送信ボタン等をクリックする以前等にその利用目的を認識できるように配慮するする必要がある。また、利用目的を明示するだけでなく、本人の同意を取得する措置（同意ボタンの設置等）を推奨する。

3.　アンケート等により取得する個人情報を基にイベントや新商品等の情報のダイレクトメールを行うことについては、本人は個人情報を入力する際にそこまでの認識を有していない場合があるので、そのようなダイレクトメール等を発信することを予定している場合は、事前に本人にその利用目的を明示しなければならない。

【あらかじめ、本人に対し，その利用目的を明示しなければならない場合の事例】

事例 1)　ウェブ画面より本人から個人情報を直接取得する場合

事例 2)　お客様カード等に記載された個人情報を（直接本人から）取得する場合

参考　個人情報保護法第 18 条第2項

第 11 条（利用目的の変更時の措置）

事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

（解説）

事業者は、社会通念上、本人が想定することが困難でないと認められる範囲内で利用目的を変更した場合は、変更された利用目的について，本人に通知するか、又は公表しなければならない。

参考　個人情報保護法第 18 条第 3 項

第 12 条（取得時及び利用目的の変更時の措置の適用除外）

前第 9 条から第 11 条の規定は、次に掲げる場合については適用しない。

①　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

②　利用目的を本人に通知し、又は公表することにより当該事業者の権利又は正当な利益を害するおそれがある場合

③　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及

ぼすおそれがあるとき。
④　取得の状況からみて利用目的が明らかであると認められる場合

（解説）
1. 個人情報保護法第 18 条第4項において、上記の4項目は、取得に際しての利用目的の通知等の原則的な規定の適用が除外される事項として記されている。
2. (1)から(3)における「おそれ」、(4)における「明らかであると認められる」については事業者において判断されるにあたり、客観的な基準でなされなければならない。

【本人又は第三者の権利利益を害するおそれがある場合の事例((1)関連)】
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おそれがある場合

【当該事業者の権利等を害するおそれがある場合の事例((2)(関連)】
事例）通知又は公表される利用目的の内容により、当該事業者が行う新商品等の開発内容、営業ノウハウ等の企業秘密にかかわるようなものが明らかになる場合

【国の機関等への協力がある場合の事例((3)関連)】
事例）公開手配を行わないで、被疑者に関する個人情報を，警察から被疑者の立ち回りが予想される事業者に限って提供する場合、警察から受け取った当該事業者が利用目的を本人に通知し、又は公表することにより、捜査活動に重大な支障を及ぼすおそれがある場合

【利用目的が自明の場合の事例((4)関連)】
事例 1) 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）。

参考　個人情報保護法第 18 条第 4 項

第 13 条（インターネット等の情報ネットワーク上で自動的に個人情報を取得する場合の措置）
事業者は、インターネット等の情報ネットワーク上でその付随する機能を用いて、本人から自動的

に個人情報を取得することとなるときは、その事実と利用目的を通知し、又は公表しなければならない。

(解説)

1.　インターネット上では本人の知らない所で個人情報が取得されている場合がある。特に、電子商取引の場面では、クッキーに代表される個人履歴情報取得技術を使って、

(1)　訪問者がそのページに何回訪れたかを記録したり、それを表示したりする

(2)　通常モード、フレームモード等、訪問者の好みを記録しておき、次回訪問時にその好みのモードで表示する

(3)　掲示板やチャットで入力したユーザー名を記録しておき、次回訪問時にユーザー名の入力を省略する

といったことがすでに実施されている。これは本人の知らないところで、本人のパソコンのブラウザーの中にクッキーが送信され、また、再度そのページに訪れた際、本人のパソコンから蓄積したクッキーのデータが事業者側のサーバーに自動的に提供される仕組みによるものである。

2.　クッキーのデータは常に個人情報に該当するわけではない。またその利用において個人情報として使わないこともあるが、特定個人を識別する形で利用するクッキーについてはその事実と利用目的を通知又は公表しなければならない。なお、本人に対し安心感を与える意味で、クッキーを個人情報と結び付けて利用しないケースでもその旨をわかりやすく示したり、クッキーの使用を説明した上でなおかつ本人が利用停止を望んだ場合に備えクッキーを無効にする操作手続きを明示することが望まれる。

3.　また、クッキーと同様の目的でウェブ･ビーコン(ビーコンとは標識、信号灯の意)が利用される場合もあるが、これについても事前に利用目的と実際にどのように利用しているかを「個人情報保護方針」等にわかりやすく記載し、ウェブ利用者の不安感を払拭することが望ましい。

参考　個人情報保護法第 18 条

第 14 条（子どもから個人情報を取得する場合の措置）

　事業者は、子どもから個人情報を取得する場合には、子どもが理解できる平易な表現で利用目的を明示するものとする。また、事業者は、子どもに個人情報の入力を求める場合は、保護者の了解を得るようにその子どもを促すものとする。

（解説）

1.　パソコンの操作性の向上に伴い、子どもでも簡単にインターネット等の情報ネットワーク上で商品･サービスの売買やアンケートへの回答を行うことが可能となった。こうした状況を利用し、例えば、子どもに人気の高いゲーム等を景品として提供することと引き換えに、子どもから、子ども自身や保護者の個人情報を取得する事例が生じている。子どもは必ずしも個人情報の取得及び利用につ

いての認識が十分ではないことから、なぜ情報が必要なのかをわかりやすく誤解を生じない表現で説明する等の慎重な取扱いが必要である。例えば、情報の提供はあくまでも任意で、必ずしも必須ではない場合には、「名前を入れなくてもゲームはできます。」等はっきり知らせなければならない。

2.　子どもやその保護者が、自分の知らないところで不利益を被る懸念があることから、「子どもに個人情報の入力を求める場合」は、取得する前に保護者に事情を説明し了解を得る機会を設定するなど、より慎重に配慮する必要がある。

3.　ここで「子ども」とは、必ずしも全ての未成年者をいうものではなく、取り扱う商品やサービスにより、対象となる年齢層が定まることを想定した用語である。「JIS Q15001」では一般に12歳から15歳までの年齢以下を対象としている。事業者は、それらを参考にし、かつ個人情報を取り扱う業務の内容を考慮し、対象となる「子ども」の年齢を定め、適正な取得方法に配慮するものとする。

また、子どもから取得状況から考えて関係のない両親、家族、友人等に関する個人情報を不当に取得してはならない。

第 15 条（取得の制限）

事業者は、その事業の遂行に必要と判断した場合に限り個人情報を取得するものとする。また、事業者は、思想、信条、宗教、健康状態その他人種、門地等社会的差別につながる個人情報の取得又は保有に際しては厳格な取り扱いに努めなければならない。

（解説）

事業者は、個人情報の取得にあたり明確な指針を策定し、事業の遂行に必要な個人情報を特定することが望まれるが、その際、思想、信条、宗教、健康状態その他人種、門地等社会的差別につながるおそれのある機微な（センシティブ）個人情報について格段の配慮を払う必要がある。事業者は、事業の遂行上、止むを得ず取得する場合には、本人の同意を得る、又はより厳格な安全管理措置を施す、さらには、第三者提供を行わないなど取扱いに特に留意しなければならない。

第 2 節　ダイレクトメールにおける個人データの利用

第 16 条（ダイレクトメールにおける個人データの利用）

事業者は、自己が取得した個人情報を用いて商用のダイレクトメールを発信する場合は当該個人情報をどのようにして取得したかを明示するとともに、受信者が今後配信を望まない際には容易に配信停止手続きを取ることができるよう配慮することが望ましい。

（解説）

1.　事業者は自己が取得した個人情報を用いて商用のダイレクトメールを発信する場合は当該個

人情報をどのようにして取得したかをメール文の冒頭に明示することが望ましい。
2.　配信先が今後当該ダイレクトメールの配信継続を望まない場合に備え、メール文の末尾に配信先が容易に取りうる配信停止手続を記載することが望ましい。
3.　当該個人情報の取得、利用に関する照会先を明示し、問合わせがあった場合には誠実に対応するものとする。
4.　「特定商取引に関する法律」及び「特定電子メールの送信の適正化等に関する法律」において、事業者が自己の営業について広告宣伝の手段として送信先の承諾に基づかないで電子メールを送信する場合、メール件名欄の冒頭に「未承諾通知※」の表示、事業者ないし送信者の指名・名称及び受信拒否（オプトアウト）の通知を受けるための電子メールアドレスの表示等を義務付けている（あらかじめその送信について同意する旨を送信者に対して通知している者を除く）が、ここでは受信者からの信頼を一層確かなものとするためその入手経路を明らかにすることが望ましいとした。

第 3 節　個人データの管理

第 17 条（個人データの全体把握）

事業者は、自己が取得した個人情報について、その保有状況を定期的に点検し、個人データならびに個人データベースの内容及び件数の正確な把握に努めなければならない。

（解説）
1.　事業者は、情報ネットワーク上又は書面にて取得した個人情報について6ヶ月に一度は全社規模で点検（棚卸し）を行い、安全に管理すべき個人データの全体を把握することが望ましい。
2.　事業者は、データベース化されたファイルについては、その利用目的、データベースを構成する項目、個人データ件数、管理責任者、保管場所、安全対策実施状況等を適時点検、更新する。
3.　さらに、事業者は、各個人データベースの活用状況を精査し必要に応じて随時スクラップアンドビルドを行うものとする。

第 18 条（個人データの正確性の確保）

事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

（解説）
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（電話帳、カーナビゲーションシステム等の取り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。

参考　個人情報保護法第 19 条

第 19 条（安全管理措置）

事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理（情報セキュリティ）のために、その規模に応じた必要かつ適切な措置を講じなければならない。

（解説）

1. 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（電話帳、カーナビゲーションシステム等の取り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。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。

【必要かつ適切な安全管理措置を講じているとはいえない場合の事例】

事例 1)　公開されることを前提としていない個人データ（購買履歴、顧客嗜好・属性情報、決済関連情報等）が事業者のウェブ画面上で不特定多数に公開されている状態を事業者が放置している場合

事例 2)　組織変更が行われ、個人データにアクセスする必要がなくなった従業者が個人データにアクセスできる状態を事業者が放置していた場合で，その従事者が個人データを漏えいした場合

事例 3)　本人が継続的にサービスを受けるために登録していた個人データが、システム障害により破損したが、採取したつもりのバックアップも破損しており、個人データを復旧できずに滅失又はき損し、本人がサービスの提供を受けられなくなった場合

事例 4)　個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合

事例 5)　個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

事例 6)　情報システム更新時に実データをシステム・テストに利用しその後のデータ回収・管理を怠った場合

2.組織的安全管理措置とは、安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認することをいう。
3.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。
4.物理的安全管理措置とは入退館（室）の管理、個人情報の盗聴の防止等の措置をいう。
5.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。
6.組織的、人的、物理的、技術的安全管理措置の具体的事項については巻末資料1に記載した。

第 20 条（物理的盗難・紛失対策）
事業者は、事業活動に即して、事業所内外での個人データの盗難、紛失その他の事故防止策を講じなければならない。

（解説）
1. 個人情報保護漏洩事案のうち相当数は個人情報入りＰＣ、記録媒体等の盗難、紛失によるものであり、事故後発見されたり、返却されるケースはきわめて稀である。事業者はかような状況を重く受け止め、自己の事業活動に即した盗難紛失事故防止策を講じなければならない。従業者に対する注意喚起は言うまでもないが、それでも不注意による盗難、紛失の完全防止は不可避との前提にたち、事故発生時における緊急対応策を講じる必要がある。
2. 盗難・紛失リスクの高い個人使用クライアント端末の運用について下記の措置が講じられることが望ましい。
(1) 個人データベースのクライアント端末への格納禁止（但し、メールアドレス・電話番号など連絡用に用いる個人データを除く）
(2) 社外等への持出し制限と台帳管理の徹底
(3) 退社時、移動時の起動ロック、データファイル暗号化、鍵のあるロッカーへの格納
3. 個人データベースのサーバー集約に伴い、サーバー本体の物理的、技術的安全対策が一層重要となるので相応の手段が講じなければならない。
4. 紙媒体などの非電子媒体についてもその取扱手順を文書にて明確に定め、関係者に周知徹底する。

第 21 条（不正アクセス・ウィルス対策）
事業者は、自己の保有する個人情報データベース等について最新の技術を踏まえながら必要かつ適切な方法により不正アクセス及びウィルス侵入に対する防衛策を講じなければならない。

（解説）
事業者の取るべき不正アクセス・ウィルス対策の具体例として、以下のようなものがある。

(1)　常時不正アクセスの有無、ウィルスの進入を監視し、異状を発見した場合は直ちにシステム全体の稼動停止若しくはその一部をネットワークから切り離しその安全を確認するものとする。
(2)　アクセス制限の実施の際には必ず詳細アクセスログを採取し、事故発生の原因究明に供する。アクセスログは6ヶ月以上保有することが望ましい。
(3)　責任者の承諾のない私用PC・未検疫PCのネットワーク接続を禁止する。
(4)　暗号化を施すことなく、インターネット上で個人情報を含んだファイルの送信、交換を行わない。

第 22 条（人的安全管理措置の推進）
事業者は、人的安全管理措置として、雇用契約時及び委託契約時における非開示契約を締結し、また、従業者に対して教育及び訓練を実施するものとする。

（解説）
1. 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や個人情報取扱いに関する教育・訓練等を行うことを指すが、組織的あるいは技術的安全管理措置などに比べ対応の遅れを指摘する事業者が多い。個人情報を取り扱うのはつまるところ「人」であることを再認識し、社内ルールを真に定着させるために絶えざる教育・訓練が重要である。
2.　事業者は、従業者の教育・訓練実施にあたっては事前に自己の個人情報保護に関する考え方とルールを文書化し、周知徹底を図ることが重要である。教育の実施については e ラーニングシステムの活用などにより極力広範な従業員が教育を受けることができるようにし、教育受講歴、理解度結果の保存に努めるものとする。
3.　個人情報保護の観点から人事制度、就業規則との整合を図り、故意、重大な過失・違反行為については懲戒処分を含めた罰則規定を明確にする。

第 23 条（安全廃棄の徹底）
事業者は、自己が保有するPC、個人情報が記録された電子媒体の廃棄に際し、個人情報が意図せず流出することがないことを確認しなければならない。

（解説）
1.　PC類の処分にあたっては完全消去ソフトウェアなどを利用することにより内蔵されていたすべての情報を消去する（若しくは信用のある事業者に委託する）。
2.　記録媒体についてはシュレッダーによる破砕処理などにより完全消去を徹底する。

第 24 条（従業者の監督）
1　事業者は、その従業者に個人データを取り扱わせるにあたっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

2　事業者は、前項の監督にあたっては少なくとも次の事項を行わなければならない。
① 規程類を策定し従業者に周知徹底すること。
② 従業者に対して定期的に個人情報の保護に関する教育･訓練を実施すること。
③ 個人データが適切に取り扱われているかを必要に応じて確認すること。

（解説）
1.　個人情報保護法第 21 条では、従業者に対する事業者の監督責任が義務として課されている。個人情報の処理を実際に担当する従業者は、まさに直接に個人情報を取り扱う者として、その意識を高く持つことが求められる。なお、「従業者」とは、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、委託社員、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。
2.　実際，個人情報が漏えいする事件の原因の1つに内部関係者の介在が指摘されている。内部関係者の行為による漏えいは、それが公になることにより、企業イメージは大きく損なわれ、場合によっては企業の存続に関わる問題ともなる。したがって、事業者は、役員をはじめすべての従業者に対し、不断の啓発活動や個人情報保護についての教育･訓練を実施することが望まれる。
3.　教育の実施にあたっては e ラーニングの活用等により対象者の履修履歴、理解度を把握･記録することが望ましい。
4.　また，個人情報保護法第 58 条では，事業者は従業者が業務において違反行為を犯した場合、行為者とともに事業者にも罰則を科するとされていることも十分に認識されるべきことである。
5.　規程類を定め、教育･訓練を通じ従業者の意識浸透を図るとともに、必要に応じて個人データが適切に取り扱われているかどうかの現場監査や従業者に誓約書の提出を求めること等の措置を講ずる必要がある。

【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の事例】
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】
　個人データの取り扱いに関する従業者及び委託先の監督，その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング（以下「モニタリング」という。）を実施する場合は、次の点に留意する。
　その際，雇用管理に関する個人情報の取り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,「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16年10月22日厚生労働省経済産業省告示第4号）Ⅱ.2.(3)3)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7月1日厚生労働省告示第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。

・ 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。

参考 個人情報保護法第21条

第25条（委託先の監督）

1 事業者は、個人データの取り扱いの全部又は一部を委託する場合は、その取り扱いを委託した個人データの安全管理が図られるよう、受託者に対する必要かつ適切な監督を行わなければならない。

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

① 委託先の選定基準を策定すること。

② 前号の基準に照らして委託先の評価を行うこと。

③ 個人情報の保護に関する事項を契約書に明記すること。

④ 前号の契約の内容が遵守されていることをあらかじめ定めた間隔で定期的に確認すること。

（解説）

1. 近年の情報化の進展に伴い、企業における情報処理業務がますます多様化、複雑化していることから経営の効率化や顧客サービスの向上等のために情報処理業務を外部に委託するケースも多くなっている。外部委託の増加に伴い、情報処理の委託先における個人情報の処理に関してトラブルが生じることがないよう必要な措置を講ずるべきとの観点から本項が定められた。

2. 個人情報の処理を委託している場合において、本人からの開示･訂正･削除等の求めに応ずる責任を負うのは、直接的には委託元の事業者である。ただし、委託の業態に応じて、委託先に対し、開示･訂正･削除等の請求を受ける窓口事務や、場合によっては、求めに応じて開示･訂正･削除等を行うこと自体を委託契約のなかで定めることもできる。

3.　委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取り扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要する。
4.　委託者が優越的地位にある場合、その地位を利用して一方的に受託者に不当な負担を課すことがないよう配慮する。業務委託契約における個人情報漏えい事故に係る損害賠償の範囲（逸失利益、情報主体に対するお詫び料等を含む）については事前に委託者、受託者双方が協議し同意をとることが望ましい。

【受託者に必要かつ適切な監督を行っていない場合の事例】
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定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合
事例 2)　個人データの取り扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合
事例 3)　再委託の条件に関する指示を受託者に行わず，かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し，結果，再委託先が個人データを漏えいした場合

【個人データの取り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】
○　委託者及び受託者の責任の明確化
○　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者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者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

参考　個人情報保護法第 22 条

第 26 条（サイバーモール運営者の対応）
　事業者のうちサイバーモールを運営する者は、サイバーモールを運営するに当たり、直接個人情

報を取得するオンラインショッピング業者等（以下「ショップ等」という。）が適正な個人情報保護管理を行うように適切な対策を講じることとする。

（解説）

1. 本条は、サイバーモール運営者がそこに出店するショップ等の個人情報の取扱いについて、一定の対策を施すよう努めることを奨励するものである。

2. 実際には、サイバーモール運営者はショップ等における個々の取引や契約について消費者と直接的な関係を持つものではない。 したがって、万一、ショップ等から個人データが漏洩した場合、消費者に対する責任は、本来、ショップ等が負うこととなる。しかしながら、消費者からみると、そのショップ等の責任を追及するにとどまらず、ショップ等が加入しているサイバーモール運営者に苦情が寄せられることも考えられる。

そうした事態が発生し、マスコミ報道等により社会的信頼を損なうこととなりうる点も考慮すると、ショップ等に対し、個人情報の取得や個人データの安全管理措置等について、責任の所在を明らかにする等の適切な対策を施すことが望ましい。

3. サイバーモール運営者がショップ等に対して、契約の中で、取得や安全管理についての必要かつ適切な措置を施すことを義務づけることにより、顧客の不安は解消され、いくらかのトラブルが回避でき、サイバーモール運営者自体のリスクも回避される。

4. また、事業者は、消費者がサイバーモールを利用し、個人情報の入力をする際に、個人情報の取扱い上の責任がサイバーモール運営者とショップ等の間のいずれにあるかについて、ウェブ画面上に明示することが望まれる。

第 3 節　個人データの第三者への提供

第 27 条（第三者への提供の制限）

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

① 法令に基づく場合

② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（解説）

1. 個人情報保護法第 23 条第 1 項では、(1)から(4)の場合を除いて原則としてあらかじめ本人の同意を得ないで個人データを第三者に提供してはならないとしている。

2. ①～④の適用除外の具体的事例は、第 7 条 3 項①～④と同様である。

3. 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（①～④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ものとする。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、従業者の子会社への出向に際して、出向先に当該従業者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、派遣契約の締結に際して、契約締結前に、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。

・ 提供先において、その従業者に対し当該個人データの取り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。

【第三者への提供とされる事例】（ただし、本条①～④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

【第三者への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。

4. 個人情報保護法の施行前に第三者提供を認める旨の同意に相当するものがある場合は本条の同意があったものと認められる（個人情報保護法附則第 3 条）。

参考 個人情報保護法第 23 条第 1 項

第 28 条（第三者提供におけるオプトアウト）

1　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、次の各号に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前条の規定にかかわらず、当該個人データを第三者に提供することができる。

① 第三者への提供を利用目的とすること。

② 第三者に提供される個人データの項目

③ 第三者への提供の手段又は方法

④ 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

2　事業者は、前項②又は③に掲げる事項を変更する場合は、変更する内容について、あらかじめ, 本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

（解説）

1.　本条は、住宅地図業者やデータベース業者等第三者に個人データを提供する事業者の取るべき措置を規定した個人情報保護法第 23 条第 2 項に対応している。

2.　前条で原則として同意を得ないで個人データを第三者への提供をしてはならないとしたうえで、本条に示すように、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は、そのことを含む①から④について本人に通知するか本人が容易に知り得る状態に置くことにより、第三者への提供が許されるとする。

3.　「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アクセスできたり、認識できたりする状態をいう。例えば、ウェブ画面上の見えやすいところに、「個人情報の第三者への提供について」等と表記し、そこをクリックすることによりその内容が表示されるといったことが方法として考えられる。なお、第 30 条の解説 2.において説明されている「本人の知り得る状態」との違いに留意する。

4.　ここで定められる措置は, いわゆるオプトアウトの手続きである。

5.　インターネット等の情報ネットワーク上では、当該本人が識別される個人データの第三者提供の停止の求めを本人から受け付ける方法として、ウェブ画面からの入力や本人からの電子メールによる返信等の方法が可能である。

また、本条 2 項に定める措置についても、ウェブ画面上での告知や本人への電子メールで通知することができる。

【第三者に提供される個人データの項目】

事例 1)　氏名、住所、メールアドレス

事例 2)　氏名、商品購入履歴

【第三者への提供の手段又は方法】

事例 1)　電子媒体に変換して配布
事例 2)　インターネットに掲載
事例 3)　プリントアウトして交付等

6.　個人情報保護法の施行前に本人に通知されているときは当該通知は本条の規定により行われたものとみなされる（個人情報保護法附則第 4 条）。

参考　個人情報保護法第 23 条第 2 項･第 3 項　附則第 4 条

第 29 条（第三者に該当しない場合）
1　次の各号のいずれかに該当する場合は、当該個人データの提供を受ける者は、第 27 条及び第 28 条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　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り扱いの全部又は一部を委託する場合
②　合併その他の事由による事業の承継に伴って個人データが提供される場合
③　個人データを特定の者との間で共同して利用する場合であって、以下のことをあらかじめ，本人に通知し、又は本人が容易に知り得る状態に置いているとき。
ア　共同利用する旨
イ　共同して利用される個人データの項目
ウ　共同して利用する者の範囲
エ　利用する者の利用目的
オ　当該個人データの管理について責任を有する者の氏名又は名称
2　前条③号に規定する項目のうち、エ又はオを変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

（解説）
1.　個人情報の処理を外部に委託することは、個人情報を取得した事業者の目的の範囲内で行われる一般的な行為であるため、個人情報保護法でも委託先は第三者に該当しないとしている。典型的な例として、物流業者に対する商品配送業務、商品代金回収業務の委託などがあげられる。
2.　合併や分社化、事業譲渡等により、事業の承継が行われ、併せて同じ目的の範囲内で個人データが移転（提供）される場合についても、個人情報保護法では提供された事業者を第三者とはみなしていない。ただし、移転可能時期は事業承継が正式に決定した時点以降に限られる。

【事業の承継に伴って個人データが提供される場合の事例】
事例 1)　合併、分社化により、新会社に個人データを渡す場合

事例 2)　営業譲渡により、譲渡先企業に個人データを渡す場合

3.　本条 1 項③号については、複数の企業が個人情報を共有することでより効率的、一体的かつ円滑な事業展開を行うケース等が想定される。ただし，この共同利用はあらかじめ個人情報の利用目的にグループによる共同利用がある旨を本人に通知し、又は容易に知りうる状態に置くことが条件になっているので注意が必要である（この場合の複数の企業とは必ずしも資本関係の有無を条件としない。）。例として、旅行業界で顧客情報を共有する場合やクレジットカード利用に関する個人信用情報照会システムなどがあげられる。なお、事業者がこの共同利用を行うにあたっては、共同利用対象会社の個人情報保護推進部門と連携を取りつつ行うものとする。

【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利用目的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)　外国の会社と利用目的の範囲内で個人データを共同利用する場合

ア）　共同して利用される個人データの項目

事例 1)　氏名、住所、メールアドレス
事例 2)　氏名、商品購入履歴

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

ウ）　利用する者の利用目的（共同して利用する個人データの全ての利用目的）

エ）　開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称（共同利用者の中で、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。）

4.　個人情報保護法の施行前に本人に通知されているときは当該通知は本条 1 項の規定により行われたものとみなされる（個人情報保護法附則第 5 条）。

参考　個人情報保護法第 23 条第 4 項・第 5 項　附則第 5 条

第 4 節　開示･変更･利用停止等の求めへの対応

第 30 条（保有個人データに関する事項の公表等）

1　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　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

③　保有個人データの開示、訂正･追加･削除、利用停止･消去、第三者提供の停止の手続及び保有個人データの開示にかかる手数料

④　事業者が行う保有個人データの取り扱いに関する苦情の申出先

⑤　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

2　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である場合

②　第 12 条 1 号から 3 号までに該当する場合

3　事業者、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。

（解説）

1.　例えば、料金を既に支払っているにもかかわらず、支払われていないことになっている場合など誤った個人情報を保有し、その情報に基づいて業務処理を行う等により本人の利益が侵害されることも想定される。これについては、事業者は本人が自己の利益を保護する手段として開示、訂正･追加･削除、利用停止･消去、第三者提供の停止を容易に行える体制を確保しなくてはならない。

2.　「本人の知り得る状態に置く」とはウェブ画面にリンク先を継続的に掲示すること、問合せ先のメールアドレスをウェブ画面などに明記し問い合わせがあった場合には速やかに回答できる体制を構築しておくことなどがあげられる。

3.　事業者は、以下の（1）から（4）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。

(1)　本条 1 項の措置により，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

(2)　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

(3)　利用目的を本人に通知し、又は公表することにより当該事業者の権利又は利益が侵害されるおそれがある場合
(4)　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又は公表することにより、本人の同意を得ることが当該業務の遂行に支障を及ぼすおそれがある場合
4.　このガイドライン第 31 条から第 33 条にて表記される「遅滞なく」とは本人からの申し出に対して、その事実関係を調査し、それが正当な申し出の場合は、いたずらに時間をかけることなく速やかに行われることをいい、通常の場合は 2 週間以内が妥当と考えられる。

参考　個人情報保護法第 24 条･政令第 5 条

第 31 条（開　示）
1　事業者は、保有個人データについて、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。）を求められた場合は、本人確認のうえ遅滞なくこれに応じなければならない。ただし、事業者は、開示することにより、次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ものとし、開示ない旨の決定をしたときはその旨を本人に対して遅滞なく通知を行う。
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　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
2　事業者は、前項で定める開示にあたっては、書面を交付する方法により行うこととする。ただし，開示の求めを行った者が同意した方法があるときは、当該方法で行うことができる。

（解説）
1.　第 30 条の解説 1.に示すように誤った情報により本人の権利が侵害されることがあるため、本人は事業者に対し、保有個人データの開示を求めることができる。
2.　事業者は本人からの開示の求めに対し、本条 1 項①から③の場合を除き、遅滞なく開示しなければならず、また、本条 1 項①から③の場合に該当し、開示しないことを決定したときもその旨を遅滞なく通知しなければならない。「遅滞なく」とは本人からの申し出に対して、いたずらに時間をかけることなく速やかに行われることをいい、通常の場合は 2 週間以内が妥当と考えられる。
3.　政令により、開示の方法としては、原則として、書面により交付することとし、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で行うことができる。これについては、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無く、事業者が提示した方法に対して異議を述べなかった場合（電話での開示の求めがあり，必要な本人確認等の後，そのまま電話で問い合わせ等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とみなすことができる。

4.　雇用管理情報の開示の求めに応じる手続については、事業者はあらかじめ労働組合等と必要に応じ協議したうえで、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を定め、従業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。

【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の事例】
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恐れがある場合

【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の事例】
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

【他の法令に違反することとなる場合の事例】
事例）　金融機関が「組織的な犯罪の処罰及び犯罪収益の規制等に関する法律」第54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

参考　個人情報保護法第 25 条･政令第 6 条

第 32 条（訂正等）
1　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「訂正等」という。）を求められたときは、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等に応じなければならない。
2　事業者は、前項の規定に基づき訂正等を行ったとき又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは，その内容を含む。）を通知しなければならない。

（解説）
1.　事業者の保有個人データの内容が事実でない場合，本人はそれを理由として事業者の定める手続きに基づき訂正、追加又は削除（「訂正等」という。）を求めることができる。

2.　開示請求の場合と同様に、本人の求めに対し、事業者はその事実関係を調査し、それが正当な申し出の場合は、いたずらに時間をかけることなく、原則として訂正等を行わなければならない。通常の場合、2 週間以内に作業を完了することが望ましい。
＊「原則」…利用目的から見て訂正等が必要でない場合や誤りである旨の指摘が正しくない場合に、訂正等を行う必要はない。ただし，その場合には、遅滞なく訂正等を行わない旨を本人に通知しなければならない。
3.　調査や訂正等は「利用目的の達成に必要な範囲内において」行うこととしているが、これは事業者においてその保有個人データを利用するうえで、利用目的の達成に必要のない訂正等についてまでその都度対応しなければならないとすると過度な負担となる可能性があるためである。

【訂正を行う必要がない事例】
事例）　訂正等の対象が事実でなく評価に関する情報である場合

参考　個人情報保護法第 26 条

第 33 条（利用停止等）
1　事業者は、本人から、当該本人が識別される保有個人データがその利用目的の制限に違反して取り扱われているという理由若しくは適正な取得に違反して取得されたものであるという理由又は第三者への提供の制限に違反して第三者に提供されているという理由によって当該保有個人データの利用の停止若しくは消去（以下「利用停止等」という。）又は第三者への提供の停止を求められた場合で、その求めに理由があることが判明したときには、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い、又は遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの利用停止等又は第三者への提供の停止に多額の費用を要する等、その実施が困難な場合であって、本人の権利利益を保護するために必要な代替措置をとるときは、この限りでない。
2　事業者は、前項の規定に基づき求められた保有個人データの全部又は一部について、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、本人に対し、遅滞なく、その旨を通知しなければならない。

（解説）
1.　個人情報保護法第 27 条にて本人は事業者に対し、同第 16 条の利用目的の制限に違反して取り扱われる場合及び同第 17 条の適正な取得に違反して取得した場合、その個人データの利用の停止又は消去を求めることができるとし、さらに同第 23 条第1項の第三者への提供の制限に違反して第三者への提供がされている場合、第三者への提供の停止を求めることができるとしている。

2.　開示請求，訂正等請求と同様に、本人の求めに対し、事業者はその事実関係を調査し、それが正当な求めであることが判明した場合は、いたずらに時間をかけることなく、原則として当該措置を行わなければならない。通常の場合、2 週間以内に作業を完了することが望ましい。
＊「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。
3.　ただし，個人情報保護法では、利用停止等に応ずる際、その実施に多額の費用を要する等によりその実施が困難な場合、あるいは、例えば事業者が保有するデータベース内でその本人の個人情報のみ利用停止することで、データベースが長期間使用できなくなり、業務上大きな支障が発生したりする場合は、そのことに代えて本人の権利利益を保護する措置が取れるのであればその限りでないとしており、本条においてもそれに従っている。

参考　個人情報保護法第 27 条

第 34 条（理由の説明）
　事業者は、開示，訂正等、利用停止等及び第三者への提供の停止の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。

（解説）
1.　個人情報保護法では措置を取らなかった場合や異なる措置を取った場合の本人への理由の説明について、「努めなければならない」との表記で努力義務が求められている。このガイドラインにおいても同様の措置を求めることとする。
2.　理由の説明の手段として電子メールを用いて行うこともできる。ただし、電子メールだけでは本人に対し、十分な説明ができないときや本人が納得しないケースも十分考えられる。その場合は、担当者による電話や面談等による説明を行うことが必要である。

参考　個人情報保護法第 28 条

第 35 条（開示等の求めに応じる手続）
1　事業者は、本人からの、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、開示、訂正等、利用停止等又は第三者への提供の停止の求め（以下「開示等の求め」という。）に関し、その求めを受け付ける方法として以下について定めることができ、当該方法に従って本人による開示等の求めを受け付けることとする。
①　開示等の求めの申し出先
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 開示の求めをする者が本人又は本条 5 項に規定する代理人であることの確認方法
④ 手数料の徴収方法（徴収する場合）
2 事業者は、前項にしたがって定められた開示等の求めを受け付ける方法及び手数料を定めた場合の手数料の額について第 24 条 1 項③により本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
3 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、事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。
4 事業者は、次に掲げる代理人による開示の求めに応じなければならない。
① 未成年者又は成年被後見人の法定代理人
② 開示等の求めをすることにつき本人が委任した代理人
5 事業者は、前 1 項、3 項及び 4 項の規定に基づき開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。
6 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及び開示を求められたときは、当該措置の実施に関し、実費を勘案して合理的であると認められる範囲において定められた手数料を徴収することができる。

（解説）
1. 個人情報保護法第 29 条により、本人からの開示等の求めに対し、それらを受け付ける手続きを定めることができる。なお、開示等の求めを受ける方法を定めない場合には、自由な申請を認めることになる。
2. 本人に対し自己の個人データの開示を行う場合、その目的等を本人に尋ねる等により、本人への開示範囲を確認することができる。
3. また、開示等の求めを主張する者が、真正な本人かどうか確認する必要がある。本人を確実に認証できない限り、安易に開示等の求めに応ずるべきではない。

【開示の求めをする者が本人又はその代理人であることの確認の方法】
事例 1) 本人の場合（オンライン）：ID とパスワード
事例 2) 本人の場合（電話）：一定の登録情報（生年月日号等）、コールバック
事例 3) 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 4) 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 5)　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

5.　保有個人データの利用目的の通知及び開示の求めについては、個人情報保護法第 30 条により、手数料を定めることができるが、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とされている。この手数料の額は、本人の知り得る状態に置かれなければならない（個人情報保護法第 24 条 1 項 3 号）。また、個人情報保護法においては、訂正等、利用停止等及び第三者への提供の停止については、手数料を徴収することができるとはしていない。

6.　政令により、未成年者又は成年被後見人の法定代理人及び開示の求めをすることにつき本人が委任した代理人が本人に代わって開示等の求めができることとなった。未成年者であれば、その親権者であることを確認すべきであり、委任を受けての代理を受け付けるにあたっては、本人の委任を受けた代理人であることを確認する手続き等を定め、その手続きに従って開示等に応ずることが必要である。

参考　個人情報保護法第 29 条･第 30 条･政令第 7 条･第 8 条

第 36 条（子どもの個人情報に関する保護者の求めへの対応）

事業者は、子どもである本人の保有個人データについて、その親権者等法定代理人から開示等の求めがあった場合は、子どものプライバシーに配慮し、第 31 条から第 35 条の規定に準じてこれに応じなければならない。

（解説）

1.　本条では、子どもが入力した個人情報の取扱いから子ども及び親権者等法定代理人である保護者が不利益を被らないようにするために、その保護者から子どもである本人の保有個人データの開示等の求めがあった場合、事業者には、本人からの開示等の求めと同等の対応が求められることを定めている。

2.　上記に該当する開示等の求めがなされた場合、取得した個人情報が、第 14 条（解説）3. にて事業者が定める「子ども」の年齢に該当する本人から取得したものであることを確認するとともに、開示等の求めをする者が親権者等法定代理人であることを確認しなければならない。

第 5 節　苦情処理

第 37 条（苦情への対応）

1　事業者は、個人情報の取り扱いに関する苦情の適切かつ迅速な対応に努めなければならな

い。
2　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。

（解説）
1.　本節は個人情報保護法第 31 条「個人情報取扱事業者による苦情の処理」に対応している。
2.　これは「個人情報保護法制に関する大綱案」で示された「私人間の関係である個人情報取扱事業者と本人との間に発生する問題は，基本的に当事者間で扱われるべきであり、また、迅速な解決を図るうえでも，そのほうが望ましい」とされていることによるものである。
3.　個人情報保護法においては当事者間で解決されない場合、認定個人情報保護団体に対して苦情についての解決を申し出ることができ（個人情報保護法第 42 条）、また，主務大臣は事業者に対して報告の徴収，助言，勧告，命令の権限を持っているので、それらが発動されることもありうる（個人情報保護法第 32 条から第 34 条）。
4.　苦情への対応については、個人情報保護法と同様に努力義務のレベルで体制の整備を求めるが、その事業領域、取り扱う個人情報の特性や対象となる個人情報の件数等に応じ、リスク管理の観点からも充実を図り、苦情に対して自主的取組みによって解決に導くことが望まれる。
5.　また、苦情への対応窓口のメールアドレス、電話番号等の連絡先はウェブ画面上の個人情報保護方針と併せ、個人情報の本人の目につきやすいところに常時表示しておくことが望ましい。

参考　個人情報保護法第 31 条

第 4 章 漏えい等が発生した場合の措置

第 38 条（漏えい等が発生した場合の措置）
1　事業者は、自己が取り扱う個人情報について漏えい等（紛失，き損を含む。以下同じ。）の事実を把握した場合は当該漏えい等に関する個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くものとする。
2　事業者は、自己が取り扱う個人情報について漏えい等の事実を把握した場合は二次被害の防止、類似事案の発生回避の観点から、可能な限り事実関係及び発生原因を遅滞なく公表するものとする。
3　事業者は、自己が取り扱う個人情報について漏えい等の事実を把握した場合は発生原因及び対応策を所管する省庁に直ちに報告するものとする。

（解説）
1.　事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、その個人情報の本人が適切に対応できるようにするため、事実関係を本人に速やかに通知又は容易に知りうる状態

に置くものとする。「本人が容易に知りうる状態」とは、ウェブ画面上のわかりやすい場所（トップページから 1 回程度の操作で到達できる場所）に継続的に表示することや、専用のフリーダイヤル設置などをいう。

2.　事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、二次被害の拡大、類似事故の発生回避のため可能な限り事実関係等を遅滞なく公表すべきである。

3.　事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、事実関係、発生原因、対応策を当該事業者の行う事業を所管する省庁へ届け出るものとする。

4.　事業者は事故発生に備え、あらかじめ緊急事態対応体制を構築し、事故発生時の対応業務につきマニュアルを整備するなど日頃から準備しておくことが重要である。

第 5 章 推進体制

第 39 条（個人情報保護管理者の指名）

事業者の代表者は、このガイドラインの内容を理解し実践する者を内部から1名以上指名し、個人情報保護管理者としての業務を行わせるものとする。但し、個人事業者又は小規模事業者においては、代表者自らが個人情報保護体制の実施･運用を行う責任を有することもできる。

（解説）

1.　本章は, このガイドラインの諸原則を遵守するための組織及びその実施責任について定めたものである。

2.　個人情報保護管理者は、事業者の代表者により指名され、個人情報保護推進体制の運営と施策の実施を行う責任者であって、個人情報の取り扱いについて決定する権限を有する。

3.　事業者は個人情報保護管理者を1名以上指名することとする。但し、個人事業者又は小規模事業者においては、代表者自らが個人情報保護体制の実施･運用を行う責任を有することもできる。管理者を複数名とした場合には、責任を明確にし、当事者間での役割分担を明らかにしなければならない。また, 個人情報保護管理者を含め各社の個人情報保護の体制については、役割、責任及び権限を定めたものを文書化し、従業者に周知する必要がある。

第 40 条（個人情報保護管理者の責務）

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

（解説）

1.　個人情報保護管理者は、内部で個人情報の取り扱いについて定めた規程類を整備し、それに則した個人情報保護推進体制の整備のためには、以下のような措置を講じることが有効である。

(1)　法令その他規範の特定

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

(2)　個人データの特定

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

(3)　規程類の策定

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

(4)　計画書の策定

規程類を遵守するために必要なリスク調査、教育、監査等の計画を立案し、文書化し、かつ、維持すべきである。また、必要に応じて詳細計画を立案する。

2.　初めて個人情報に関する業務に従事する者については、あらかじめ必要な教育訓練を行うか、十分に教育訓練された者がその者を支援するような体制を取る必要がある。

3.　個人情報の取り扱いを外部に委託する場合も、当該委託先における管理状況に関して適宜確認する。

4.　個人情報保護管理者は、十分な技術的保護措置を実施する等の責任も負う。

5.　個人情報保護管理者は、このガイドラインに定めるすべての事項について、適正に書面又はこれに代わる方法で文書管理がなされるよう徹底することが望まれる。また、個人情報保護法がに基づいて、事業者として守るべき義務が生じたことに伴い企業リスク管理の観点から、文書管理に関する規程類を策定し、監査等の証拠として、また後日のトラブルに備えることが必要となる。このガイドラインにて定められる本人からの開示等の求めへの対応や苦情への対応だけでなく、個人情報保護法第 35 条「報告の徴収」における主務大臣による要求により、その取り扱いについての報告が求められたときや訴訟等の状況に陥ったとき、迅速かつ的確に対応できるよう、あるいは改ざんのそしりを受けないように文章の記録･作成と管理を徹底しておくべきである。

6.　個人情報保護推進体制のもとに個人情報保護を推進するときには、法令, 所轄官庁の指針、規程等と合致していること及びその運用状況を確認する定期的な監査等を実施することが望ましい。

第 41 条（個人情報保護監査責任者の指名）

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

(解説)

1. 個人情報保護監査責任者は、事業者の代表者により指名され、各社の個人情報保護推進体制の整備がこのガイドラインの要求事項と合致していること及びその運用状況を定期的に監査することが望ましい。

2. 個人情報保護監査責任者は個人情報保護体制の妥当性、有効性及び実施状況を監査する立場にあるため、個人情報保護管理者がこれを兼務することはできない。

第 42 条(個人情報保護監査責任者の責務)

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

(解説)

1. 事業者の個人情報保護監査責任者は、あらかじめ決められたサイクルで事業者の個人情報保護推進体制を監査し、監査報告書を作成し、事業者の代表者に報告するものとする。

2. 事業者は監査状況を常時管理し、監査報告書を一定期間保管するものとする。

第 6 章 その他

第 43 条(見直し)

事業者の代表者は、個人情報保護の実施状況及びその他の経営環境等に照らして、適切な個人情報の保護を維持するために、少なくとも年 1 回以上保護推進体制を見直すこととする。

(解説)

事業者の代表者は、個人情報保護体制の監査等における報告書の指摘事項を必ず確認し、個人情報保護推進体制の改善点等について見直し案を作成させ、優先順位を付して実行させる必要がある。また、具体的な指示の内容は、それぞれの担当者宛に書面により行い、徹底することが重要である。

(平成18 年1月 16 日 改訂)

巻末資料 1

(ア)　　組織的安全管理

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個人データの取扱い状況を一覧できる手段の整備
④個人データの安全管理措置の評価，見直しおよび改善
⑤事故または違反への対処

【各項目について講じることが望まれる事項】

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する上で望まれる事項

・従業者の役割・責任の明確化

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

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

・個人データの取り扱い（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およ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および担当者（システム管理者を含む。）の限定

・個人データの取り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

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

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

※個人データの漏えい等についての情報は代表窓口、苦情対応窓口を通じ、外部からもたらされる場合もあるため、苦情の対応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およ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する上で望まれる事項
・個人データの取り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【個人データの取り扱いに関する規程等に記載することが望まれる事項】を参照。
・個人データの取り扱いに係る建物、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
・個人データの取り扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
・定められた規程等に従って業務手続が適切に行われたことを示す監査証跡※の保持
※保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば，だれがどのような操作を行ったかを記録）、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する上で望まれる事項
・個人データについて、取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取り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、見直しおよび改善をするうえで望まれる事項
・監査計画の立案と、計画に基づく監査（内部監査または外部監査）の実施
・監査実施結果の取りまとめと、代表者への報告
・監査責任者から受ける監査報告、個人データに対する社会通念の変化およ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および改善

⑤事故または違反への対処をするうえで望まれる事項
・事実関係、再発防止策等の公表

・その他、以下の項目等の実施

ア）事実調査、イ）影響範囲の特定、ウ）影響を受ける可能性のある本人および主務大臣等への報告、エ）原因の究明、オ）再発防止策の検討・実施

【個人データの取り扱いに関する規程等に記載することが望まれる事項】

以下、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、個人データの取り扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項を列記する。

①取得･入力

ア．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。）

イ．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。）

ウ．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

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、およ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

ア．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

イ．手続の明確化と手続に従った実施

・個人データを移送・送信する際の手続の明確化

・定められた手続による移送・送信の実施

・個人データを移送・送信する場合の個人データの暗号化（例えば，公衆回線を利用して個人データを送信する場合）移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用）

・ＦＡＸ等におけるあて先番号確認と受領確認

・個人データを記した文書をＦＡＸ等に放置することの禁止

・暗号鍵やパスワードの適切な管理

ウ．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

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、およ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

ア．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

イ．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）

ウ．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

エ．作業担当者およびその権限の確認
・手続の明確化と手続に従った実施、およ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

ア．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

イ．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
・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

ウ．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

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、およ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

ア．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

イ．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回または複数回上書きする。）

・個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）

ウ．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

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、およ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

(ｲ)　　人的安全管理

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】

①雇用契約時及び委託契約時における非開示契約の締結

②従業者に対する教育･訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、法第21条を参照。

【各項目について講じることが望まれる事項】

①雇用契約時及び委託契約時における非開示契約の締結をする上で望まれる事項

・従業者の採用時または委託契約時における非開示契約の締結

※雇用契約または委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。

・非開示契約に違反した場合の措置に関する規程の整備

※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲およ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従業者に対する周知･教育･訓練を実施する上で望まれる事項

・個人データおよび情報システムの安全管理に関する従業者の役割および責任を定めた内部規程等についての周知

・個人データおよび情報システムの安全管理に関する従業者の役割およ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

(ウ)　　物理的安全管理

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

【各項目について講じることが望まれる事項】

①入退館(室)管理を実施する上で望まれる事項

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

・個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理

的に保護された室内等への設置

②盗難等を防止する上で望まれる事項

・離席時の個人データを記した書類、媒体、携帯可能なコンピュータ等の机上等への放置の禁止

・離席時のパスワード付きスクリーンセイバ等の起動

・個人データを含む媒体の施錠保管

・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管

・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③機器･装置等を物理的に保護する上で望まれる事項

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

(エ)　技術的安全管理

技術的安全管理措置とは、個人データおよ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

【各項目について講じることが望まれる事項】

①個人データへのアクセスにおける識別と認証を行う上で望まれる事項

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

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

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

②個人データへのアクセス制御を行う上で望まれる事項

・個人データへのアクセス権限を付与すべき従業者数の最小化

・識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）

・従業者に付与するアクセス権限の最小化

・個人データを格納した情報システムへの同時利用者数の制限

・個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）

・個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）

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

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

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

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

③個人データへのアクセス権限の管理を行う上で望まれる事項

・個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）

・個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

④個人データへのアクセスの記録を行う上で望まれる事項

・ 個人データへのアクセスや操作の成功と失敗の記録（例えば，個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）

・採取した記録の漏えい、滅失およ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施する上で望まれる事項

・ウイルス対策ソフトウェアの導入

・オペレーティングシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用

・不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）

⑥個人データの移送（運搬、郵送、宅配便等）・送信時の対策の上で望まれる事項

・移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化）

・盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）で個人データを送信（例えば、本人およ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

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の上で望まれる事項

・情報システムの動作確認時のテストデータとして個人データを利用することの禁止

・情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証

⑧個人データを取り扱う情報システムの監視を行う上で望まれる事項

・個人データを取り扱う情報システムの使用状況の定期的な監視

・個人データへのアクセス状況（操作内容も含む）の監視

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

巻末資料　2

「個人情報の保護に関する法律」に基づく公表事項（案）

○○○○株式会社

「個人情報の保護に関する法律」（以下「法」といいます。）に基づき，以下の事項を「公表」致します。（「本人が容易に知り得る状態に置いている」こと，及び，「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。）」に置くことを義務付けられている事項を含みます。）

１．利用目的の公表に関する事項（法 18 条 1 項）

（1）直接書面取得以外で取得する場合の「個人情報」の「利用目的」（法 18 条 1 項）

お客さまから直接書面に記載された個人情報を取得する場合（直接書面取得）は，その都度，お客さまに利用目的を明示させて頂きます（法 18 条 2 項）。それ以外で個人情報を取得する場合は，次の利用目的の制限の範囲内で取り扱わせて頂きます（法 18 条 1 項）。ただし，以下の（2），（3），２．の場合は除きます（法 23 条 4 項）。

	「個人情報」の類型	利用目的
a.		（変更前） （変更後）
b.		
c.		

（2）委託された「個人情報」の「利用目的」（法 18 条 1 項，法 23 条 4 項 1 号）

当社が取扱いを委託されている「個人情報（個人データ）」の「利用目的」は次のとおりです。

	「個人情報」の類型	利用目的
a.		（変更前） （変更後）
b.		

（3）合併，事業承継に伴い取得した「個人情報」の「利用目的」

（法 18 条 1 項，法 23 条 4 項 2 号）

平成〇年〇月〇日の当社と〇〇〇〇株式会社との（合併・事業承継）に伴い，旧〇〇〇〇株式会社の保有する「個人情報」を取得致しました。当該「個人情報（個人データ）」の「利用目的」は次のとおり，旧〇〇〇〇株式会社において特定した「利用目的」と同じものです。

	「個人情報」の類型	利用目的
a.	顧客名簿	
b.	労働者名簿	

２．「共同利用」に関する事項（法 23 条 4 項 3 号，法 23 条 5 項）

次のａに示した○○○に関する顧客情報（「個人データ」）を、ｂに示した者との間で共同して利用させて頂きます。

a.	**共同して利用される個人データの項目**
	① 氏名 ② 住所 ③ 電話番号 ④ FAX 番号 ⑤ 電子メールアドレス， ⑥ 注文内容（商品名・数量・対価）
b.	**共同して利用する者の範囲**
	① ○○○○株式会社（東京都○○区） ② ○○○○株式会社（東京都○○区） ③ ○○○○株式会社（東京都○○区） ④ ○○○○株式会社（東京都○○区） ⑤ ○○○○株式会社（東京都○○区） ⑥ ○○○○株式会社（東京都○○区）
c.	**利用する者の利用目的**
d.	**当該個人データの管理について責任を有する事業者の名称**
	○○○○株式会社 連絡先（個人情報保護対策室） 〒000-0000　東京都○○区○○○1-2-3　○○○ビル TEL　03-0000-0000　　FAX　03-0000-0000 e-mail

3．「保有個人データ」に関して「本人の知り得る状態」に置くべき事項

（法 24 条 1 項）

当社の保有する「個人情報（「保有個人データ」）の「利用目的」は次のとおりです。

	「保有個人データ」の類型	利用目的
a.		（変更前） （変更後）
b.		
c.		
d.		

４．「苦情」の受付窓口に関する事項

（法 24 条 1 項 4 号，施行令 5 条，法 31 条）

（1）個人情報の取扱いに関する苦情の申出先

当社の個人情報の取扱いに関する苦情については，下記までお申し出下さい。

●お電話による場合

〇〇〇〇株式会社　個人情報保護対策室　03-0000-0000

●お手紙による場合

〒000-0000

東京都〇〇区〇〇０丁目０番０号　〇〇〇〇ビル

〇〇〇〇株式会社　個人情報保護対策室

●電子メールによる場合

parsonaldata@ispisp.com

●ご来社について

直接ご来社頂いてのお申し出はお受けかねますので，その旨ご了承賜りますようお願い申し上げます。

（2）当社の所属する「認定個人情報保護団体」の名称及び苦情の申出先

財団法人日本データ通信協会　〇〇〇〇〇〇

●お電話による場合

03-0000-0000

●お手紙による場合

〒000-0000

東京都ＸＸ区ＸＸ０丁目０番０号　ＸＸＸＸＸビル

●電子メールによる場合

parsonaldata@ispisp.com

●面談によるご相談について

５．「開示等の求め」に応じる手続等に関する事項（法 29 条）

（１）開示の求めの対象となる項目（「保有個人データ」の特定に資する情報）

開示の対象としている個人情報（「保有個人データ」）の項目は以下のとおりです。

1．○○情報	2．○○情報	3．○○情報	4．○○情報
5．○○情報	6．○○情報	7．○○情報	8．○○情報
9．○○情報	10．○○情報	11．○○情報	12．○○情報

（２）「開示等の求め」の申出先

開示等の求めは下記宛，所定の申請書に必要書類を添付の上，郵送によりお願い申し上げます。なお，封筒に朱書きで「開示等請求書類在中」とお書き添え頂ければ幸いです。

〒000-0000
東京都ＸＸ区ＸＸ　Ｘ丁目Ｘ番Ｘ号　ＸＸＸＸＸビル
株式会社ＸＸＸＸＸ　個人情報保護対策室

（３）「開示等の求め」に際して提出すべき書面（様式）等

「開示等の求め」を行う場合は，次の申請書（A）をダウンロードし，所定の事項を全てご記入の上，本人確認のための書類（B）を同封し上記（２）宛ご郵送下さい。

A．当社所定の申請書

・「保有個人データ」開示申請書
・「保有個人データ」変更等申請書
・「保有個人データ」利用停止等申請書

B．本人確認のための書類

次のうちいずれかを同封して下さい。

・運転免許証（有効期限内のもので、各都道府県公安委員会発行のもの。国際運転免許証は除く。）の写し

・学生証の写し（有効期限内のもので、顔写真、生年月日、住所が記載されているもの。住所が記載されていない場合は、現住所が記載されている住民票、又は現住所が記載されている公共料金領収証・請求書の写しも併せて添付して下さい。）

・日本国の旅券（パスポート）（有効期限内のもので、現住所が記入されているもの。）の写し

・健康保険証の写し＋現住所が記載されている住民票、又は現住所が記載されている公共料金領収証若しくは請求書の写し

・障害者手帳又は療育手帳又は精神障害者保健福祉手帳の写し（現住所が記入されているもの。住所が記載されていない場合は、現住所が記載されている住民票、又は現住所が記載されている公共料金領収証・請求書も併せて添付して下さい。）

・外国人登録証明書の写し＋旅券（パスポート）の写し、又は公共料金領収証若しくは請求書の写し、又は米軍ＩＤカードの写し

（4）代理人による「開示等の求め」

「開示等の求め」をする者が本人又は未成年者又は成年被後見人の法定代理人若しくは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場合は，前項の本人確認のための書類に加えて，下記の書類を同封して下さい。

A．法定代理人の場合

・当社所定の申告書　１通

・法定代理権があることを確認するための書類（戸籍謄本，又は親権者の場合は扶養家族が記入された保険証の写しも可）　１通

・未成年者又は成年被後見人の法定代理人本人であることを確認するための書類（法定代理人の運転免許証，又は旅券（パスポート）の写し）　１通

B．委任による代理人の場合

・当社所定の委任状　１通

・本人の印鑑証明書　１通

（５）「開示等の求め」の手数料及びその徴収方法

１回の申請ごとに，ＸＸＸ円（税込）
ＸＸＸ円分の郵便切手を申請書類に同封して下さい。
＊手数料が不足していた場合，及び手数料が同封されていなかった場合は，その旨ご連絡申し上げますが，所定の期間内にお支払いがない場合は，開示の求めがなかったものとして対応させて頂きます。

（６）「開示等の求め」に対する回答方法

申請者の申請書記載住所宛に書面によってご回答申し上げます。

（７）開示等の求めに関して取得した個人情報の「利用目的」

開示等の求めにともない取得した個人情報は，開示等の求めに必要な範囲のみで取り扱うものとします。提出頂いた書類は，開示等の求めに対する回答が終了した後，２年間保存し，その後廃棄させて頂きます。

（８）個人データ」の不開示事由について

次に定める場合は，不開示とさせていただきます。不開示を決定した場合は，その旨，理由を付記して通知申し上げます。また，不開示の場合についても所定の手数料を頂きます。

・申請書に記載されている住所・本人確認のための書類に記載されている住所・当社の登録住所が一致しないときなど本人が確認できない場合
・代理人による申請に際して，代理権が確認できない場合
・所定の申請書類に不備があった場合
・開示の求めの対象が「保有個人データ」に該当しない場合
・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
・当社の業務の適正な実施に著しい支障を及ぼすおそれがある場合

・他の法令に違反することとなる場合