JIS Q 15001：2006

個人情報保護マネジメントシステム－要求事項
解　説（2011 年改訂）

この解説は，次の理由により 2006 年発行時に掲載した解説を改訂した。

個人情報保護法の施行後，個人情報保護への取り組みに関しては，本規格に基づく，より充実な取り組みが浸透しつつある。本規格の要求事項については，既に各要求事項に基づくマネジメントシステムの構築に当たって参照がなされている一方で，個人情報保護への取り組みにかかる対応においては，法及び本規格の解釈に関し，より一層の精緻化が求められてきたところである。これらのことから，本規格の要求事項の解釈に関し，法の施行への取り組み等の関係において疑義が生じているとしてきたことについて，要求事項本体の改正ではなく，解説の加除修正及び別表の追加による明確化を図ったものである。

この解説は，規格に規定・記載した事柄を説明するもので，規格の一部ではない。

この解説は，財団法人日本規格協会が編集・発行するものであり，これに関する問合せ先は，財団法人日本規格協会である。

I　改正の趣旨及び経緯

旧規格は，**JIS Q 15001**:1999（個人情報保護に関するコンプライアンス・プログラムの要求事項）であり，この規格は，コンピュータの使用による情報技術の進展及びインターネットなどのネットワークの普及に伴い，事業者が大量の個人情報を扱い，それを容易に加工・蓄積・流通することができる状況が出現し，個人情報の適切な利用と保護が極めて重要となるなか，各事業者におけるマネジメントシステムによる個人情報保護の取組みを促進し，高度情報通信社会の健全な発展と消費者保護を目的として，通商産業省（現在の経済産業省）が作成した“民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン”を基礎として，平成 11 年に制定された。

その後，情報技術はますます発展し，個人情報の保護の必要性が一層高まった。また，“個人情報の保護に関する法律”（平成 15 年 5 月 30 日法律第 57 号。以下，個人情報保護法という。）が平成 15 年に制定され，平成 17 年 4 月から全面施行を迎え，規格の取り巻く環境は大きく変化した。このような状況の変化を踏まえ，平成 18 年には，旧規格を，個人情報保護法に基づく個人情報保護ルール及びマネジメントシステムを併せもった規格に改正し，**JIS Q 15001**:2006（個人情報保護マネジメントシステム－要求事項）とした。

平成 18 年の改正以来，更に 5 年が経過したところ，個人情報保護法の施行後，個人情報保護への取組みに関しては本規格に基づく高度な取組みが浸透しつつある。本規格の要求事項については，既に各要求事項に基づくマネジメントシステムの構築に当たって参照がなされている一方で，個人情報保護への取組みに係る対応においては，個人情報保護法及び本規格の要求事項の解釈に関し，より一層の精緻化が求められてきたところである。

このような状況を踏まえ，この度，本規格の要求事項の解釈に関し，個人情報保護法の施行後の取組みとの関係においてより明確化が求められてきた部分について，要求事項本体の改正ではなく，高度で精緻な取組みに求められる解説の修正及び別表の追加による充実化を図ったほか，併せて，“個人情報の保護に関する基本方針”（平成 21 年 9 月 1 日一部変更閣議決定）や“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 21 年 10 月 9 日厚生労働省・経済産業省告示第 2 号）等の改正に対応した解説の修正を行った。

なお，本規格は，個人情報保護法の施行後にあっても，以下のような意義を有するものと考えられる。

－ 個人情報保護法を遵守し，より高い水準の保護を確立するための要求事項を定めるものであること
－ 個人情報保護のためのマネジメントシステムを構築するに当たっての基準であること
－ 個人情報の適正な取扱いと保護への取組みを行うことによって，本人と事業者，又は事業者相互の信頼関係構築に必要な事項について定めていること
－ 個人情報保護への取組みを行う者が参照し，その取組みを行うに当たって，有用な情報を提供するものであること

II 規定項目の内容

箇条ごとの規定項目の内容を，次に示す。

1 適用範囲（本体の箇条 1）

個人の住所録など個人が自己のために個人情報を取り扱っている場合はこの規格の対象とはしない。

“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，営利事業だけを対象とするものではない。従業者の個人情報は，事業の用に供している個人情報である。

なお，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は，その情報の中に含まれる個人情報については，事業の用に供していないといえる。

2 用語及び定義（本体の箇条 2）

この規格で別段の定めがある場合を除き，個人情報保護法の第 2 条に定義があるものについては，それを準用する。

2.1 個人情報（本体の 2.1）

“個人情報”には，死者の情報も含まれるが，歴史上の人物まで対象とするものではない。死者の情報も対象としている理由は，故人の個人情報が遺族の個人情報として解されることがあり，また，その利用目的との関係において，生死の別を厳格に管理しない場合もあるからである。さらには，事業活動においては，契約により取得している個人情報も多く，その一方当事者の死亡をもって，即時に個人情報保護マネジメントシステムの対象情報から除外するというものでもないからである。

2.2 事業者（本体の 2.3）

“事業者”には，取り扱う個人情報の量及び利用方法にかかわらず，個人情報を事業の用に供しているすべての事業者が含まれる。

2.3 個人情報保護管理者（本体の 2.4）

“個人情報保護管理者”は，個人情報の取扱いに関する安全管理面だけではなく，組織全体のマネジメントを含む全体の管理者である。

2.4 本人の同意（本体の 2.6）

“取扱いに関する情報”とは，本体の **3.4.2.4**，**3.4.2.6**，**3.4.2.7** 又は **3.4.2.8** において要求されている明示又は通知の項目である。同意は，本人の署名，同意欄へのチェック，ウェブサイト上での同意ボタンの押下などの明示的な方法によって本人の意思が表示されていることが原則である。当該通知項目が明示され

た書面に本人が記入したからといって，同意があったものとみなすべきではない。また，通知後一定期間内に本人の応答が無い場合に同意があったものとみなすことも原則として不適切である。

法定代理人等の同意を要する子どもとは，本体の **3.4.2.4** の **a)**～**h)**の内容を理解できない年齢の子どものことである。一般に，12 歳から 15 歳までの年齢以下が対象になると考えられる。また，“事理を弁識する能力を欠く者”とは，同様に本体の **3.4.2.4** の **a)**～**h)**の内容について，判断力に懸念があると考えられる成人を指し，成年被後見人［民法（明治 29 年法律第 89 号。以下同じ。）第 7 条］だけでなく，被保佐人（民法第 11 条）及び被補助人（民法第 15 条第 1 項）等で，本体の **3.4.2.4** の **a)**～**h)**の内容について，判断力に懸念がある状態にある場合も含む。

法定代理人等の同意の必要性については，あらゆる場合に，本人が子ども又は事理を弁識する能力を欠く者に当たるか否かを確認することが求められるのではなく，事業者において，個人情報の取得時に，子ども又は事理を弁識する能力を欠く者であることが明らかな場合若しくは合理的に知り得る状態にある場合，又は，取得後に知った場合に，法定代理人等の同意を得ることが求められる。

3　要求事項

3.1　個人情報保護方針（本体の **3.2**）

“代表者”とは，代表権をもつ者をいう。

個人情報保護方針は，事業者の個人情報保護に関する取組みを内外に宣言する公式文書と位置づけられるものであり，個人情報保護の理念及び経営責任等を明確にするため，取締役会の決議を経るなど一定の手続を経て定める必要があるとともに，当該方針を公表するに当たっては，制定年月日及び最終改訂年月日を表示する必要がある。また，当該方針には，単に“事業内容及び規模を考慮して適切に取り扱います”などと記載したり，本体の **3.2** の **a)**～**e)**の各事項の文言をそのまま個人情報保護方針として記載することは望ましくなく，本体の **3.2** の **a)**～**e)**の各事項に関する各事業者ごとの方針を具体的に記載しなければならない。

“個人情報保護の理念”とは，当該事業者が個人情報保護に取り組む姿勢や基本的考え方である。個人情報保護方針は，一般の人に公開することを前提とするものである以上，容易に理解できる表現であることが望ましく，当該方針の内容についての問合せに応じられるよう，公開に当たっては問合せ先を明示しなければならない。また，個人情報保護方針は，**文書の範囲**（本体の **3.5.1**）に含まれており，**文書管理**（本体の **3.5.2**）の対象として，文書の発行及び改訂に関する情報を管理しなければならない。

なお，本体の **3.2** の **a)**，**c)**，**d)**については，個人情報保護法及び個人情報の保護に関する基本方針を踏まえたものである。“国が定める指針”とは，個人情報保護法に基づいて各所管省庁が作成したガイドライン・指針などである。

3.2 a)においては，“特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下，目的外利用という）を行わないこと及びそのための措置を講じることを含む”とされているが，これは本体の **3.4.2.6** を遵守した対応を求めているものである。

“一般の人が入手可能な措置”としては，例えば，ウェブサイトによる公開が考えられる。ウェブサイトをもたない場合は，例えば，会社パンフレットに記載し，受付カウンターに自由に持ち帰ることができるように用意しておくとともに，遠方からの問合せに対しては，要望があればすぐに送付する体制を整えておくといった手段が考えられる。

3.2　計画

3.2.1　個人情報の特定（本体の **3.3.1**）

事業者は，社内で事業の用に供している個人情報としてどのようなものがあるかを知らずして個人情報保護のための対策を取ることはできない。そのためには，まず，個人情報を漏れなく特定できる手順を検討し，その手順をルールとして確立させなければならない。

具体的に，ある情報が個人情報に該当するかどうかは，個人情報保護法に基づいて各所管省庁が作成したガイドライン・指針等を参考にするとよい（ただし，この規格では，個人情報に死者の情報も含まれる）。

次に，特定した個人情報については，その取扱状況を一覧できる手段を整備する必要がある。事業者は，個人情報の項目，利用目的，保管場所，保管方法，アクセス権限を有する者，利用期限等を記載した個人情報を管理するための台帳を整備するとともに，当該台帳の内容を定期的に確認し，最新の状態で維持されるようにしなければならない。

ただし，事業において利用するすべての個人情報について台帳整備を強いるのではなく，個人情報を含む文書の取扱いについては，その個人情報の利用目的を特定したうえで，その利用目的の範囲内で個々の従業者にゆだねるなど，柔軟な取扱いでよい場合もある。

3.2.2　法令，国が定める指針その他の規範（本体の **3.3.2**）

個人情報保護法，行政機関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 58 号），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），各地方自治体が制定している個人情報保護条例，その他の法令，行政機関が制定している個人情報の保護に関する指針（ガイドライン），認定個人情報保護団体が定めた個人情報保護指針，各業界が定めたガイドライン等がある。事業者は，事業に関連する個人情報の取扱いの法令，国が定める指針及びその他の規範の制定・改廃状況に注意し，必要に応じて速やかに個人情報保護マネジメントシステムに反映できる手順を確立しなければならない。

3.2.3　リスクなどの認識，分析及び対策（本体の **3.3.3**）

“目的外利用を行わないため，必要な対策を講じる手順”には，例えば，利用目的が定められていない個人情報については利用することができない旨の手順も含まれる。

“リスクを認識”とは，特定した個人情報の取得・入力，移送・送信，利用・加工，保管・バックアップ，消去・廃棄に至る個人情報の取扱いの一連の流れの各局面において，適正な保護措置を講じない場合に想定されるリスクを洗い出すことであり，リスクを“分析”するとは，洗い出したリスクを定性的な評価などによって評価することである。事業者は，洗い出したリスクに対し，その評価に相応した合理的な対策を講じなければならない。

“合理的な対策”とは，事業者の事業内容や規模に応じ，経済的に実行可能な最良の技術の適用に配慮することである。すべてのリスクをゼロにすることは不可能であるから，現状で取り得る対策を講じた上で，未対応部分を残存リスクとして把握し，管理しなければならない。

なお，個人情報は，取得及び利用面での適正な取扱いも求められる点で，単に情報資産として守るという観点からだけのリスクの認識，分析及び対策では足りない。

個人情報に関するリスクとは，人的及び物理的リスクだけでなく，個人情報の取扱いに関する法令，国が定める指針及びその他の規範に対する違反，想定される経済的な不利益及び社会的な信用の失墜等のおそれも含まれる。

リスクは，技術の進展や環境の変化等によって常に変動するものであり，リスクの認識・分析及び対策は，一度だけ実施すればよいものではない。事業者は，講じた対策が十分であるかを検証し，定期的に見直さなければならない。

3.2.4　資源，役割，責任及び権限（本体の **3.3.4**）

個人情報保護管理者は，個人情報保護マネジメントシステムを理解し，実施・運用できる能力をもった

者でなければならない。個人情報保護管理者は，当該事業者に係る個人情報の管理の責任者である性格上，いたずらに指名する者を増やし，責任が不明確になることは避けなければならない。したがって，事業部が複数あり個人情報保護管理者を複数名指名する場合には，当該者間での役割分担を明確にすることが求められる。

個人情報保護管理者は，社外に責任をもつことができる者（例えば，役員クラス）を指名することが望ましい。

個人情報保護管理者は，代表者による個人情報保護マネジメントシステムの見直しに資するため，定期的に，又は適宜に，代表者にその実施状況を報告しなければならない。

“資源”とは，人員，組織の基盤（規程，体制，施設・設備等）や資金などを意味するが，事業者の状況に応じて，適宜，不可欠な資源を判断し，用意することが求められる。

3.2.5　内部規程（本体の **3.3.5**）

手順として確立したルールは，文書化しておくことによって担当者が変わっても個人情報保護水準の継続性が保たれる。ルールが明文化されていないこともリスクの一つであると認識すべきである。

内部規程には，個人情報を保護するための組織規程を含む。事業者の各部門及び階層における権限と責任の明確化を図ることが重要である。

内部規程の整備は，本体の **3.3.3** によって実施したリスクの認識・分析及び対策がベースになるはずであり，リスクの認識が十分になされていればその対策を規定化する作業は容易であるはずである。内部規程の整備は，基本となる規程を形式的に定めるだけでなく，それを受けて細則，マニュアル，チェックリストなどを作成し，どのような行為をなすべきか，又はなすべきではないのか，従業者が具体的に規範に直面するよう構成する必要がある。内部規程は，必ずしも形式的に一本化される必要はなく，例えば，内部規程の違反に関する罰則は，就業規則で規定すればよい。

内部規程は，経営責任等を明確にするため，取締役会の決議を経るなど一定の手続を経て定める必要がある。

3.2.6　計画書（本体の **3.3.6**）

教育計画書は，個人情報保護研修の年間カリキュラム，個別の研修プログラム（研修名，開催日時，場所，講師，受講対象者及び予定参加者数，研修の概要，使用テキスト，任意参加か否かの別など）及び予算などによって構成する。

監査計画書は，当該年度に実施する（個人情報に関する）監査テーマ，監査対象，目的，範囲，手続，スケジュールなどによって構成する。

なお，教育計画書と監査計画書以外にどのような計画書を作成するかについては，本体の **3.9** の個人情報保護マネジメントシステムの見直しで把握された課題も踏まえ，事業者の置かれた状況等を勘案して，個別に必要性を検討することが望ましい。例えば，中長期的な視点も踏まえた安全管理（情報セキュリティ対策）計画書などが考えられる。

3.2.7　緊急事態への準備（本体の **3.3.7**）

緊急事態の特定手順及び対応手順の策定に当たっては，次のような事項を考慮するとよい。

－　緊急事態及び事故が最も起こりやすい場面
－　予想される被害の規模
－　被害を最小限に抑えるための一次的な対処方法
－　社内の緊急連絡網及び社外への報告手順の確立
－　再発防止処置を実施する手順

－　緊急時対応についての教育訓練

緊急事態が発生した場合，常に本体の **3.3.7** の **a)**～**c)**のすべてを実施しなければならないというものではない。どのような場合にどのような手順になるか，法令，国が定める指針その他の規範に従って対処方針を定め，その対処方針に従い実施すれば足りる。

なお，本体の **3.3.7 b)**の事案の公表に際しては，公表によって本人などへの二次被害を招かないように，公表する内容，手段及び方法を考慮することが必要である。また，個人情報の取扱いの全部又は一部を受託している受託者については，委託契約において何ら取り決めがない場合は，委託者と相談のうえ実施することが必要である。

3.4　実施及び運用

3.4.1　利用目的の特定（本体の **3.4.2.1**）

利用目的は，当然公序良俗に反しないことが求められる。

“利用目的をできる限り特定し”とは，利用目的を単に抽象的，一般的に特定するのではなく，事業者が最終的にどのような目的で個人情報を利用するのかを可能な限り具体的に特定することである。単に“事業活動に用いるため”，“提供するサービスの向上のため”，又は“マーケティング活動に用いるため”と表現することは，利用目的を特定したことにならない。

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特定して示したり，本人の選択によって利用目的の特定ができるようにしたりするなど，本人にとって利用目的がより明確になるような取組みが望ましい。

利用目的の特定に当たっては，次のことに配慮する必要がある。

a) 本人から取得する場合，利用目的は，本人との契約などにおいて明示的に了解されるか，又は本人との契約類似の信頼関係の中で黙示的に了解されること。

b) 本人以外の者から取得する場合も，取得する者が利用目的を設定し，取得の相手方との契約などにおいて明示すること。

c) 公開された資料などから取得する場合も，取得する者が公開された目的の範囲内で利用目的を設定すること。

d) 利用目的を特定するに当たっては，取得した情報の利用及び提供によって本人の受ける影響を予測できるように，利用及び提供の範囲を可能な限り具体的に明らかにすること。

3.4.2　適正な取得（本体の **3.4.2.2**）

利用目的を偽るなど不公正な手段によって個人情報を取得することは許されない。また，優越的な地位を利用して取得することも許されない。

なお，個人情報保護法第 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や，十分な判断能力を有していない子どもから親の収入事情などの家族の個人情報を取得する場合なども，適正な取得とは認められない。

3.4.3　特定の機微な個人情報の取得，利用及び提供の制限（本体の **3.4.2.3**）

“明示的な本人の同意”とは，書面による本人の同意をいう。黙示的な同意は認められない。機微な個人情報としては，最低限，本体の **3.4.2.3** の **a)**～**e)**に示す内容を含む個人情報が挙げられるが，これに加え，各事業者の事業の実態，個人情報の取扱状況等によって，一定の範囲を各事業者で定めることができる。

3.4.4　本人から直接書面によって取得する場合の措置（本体の **3.4.2.4**）

同意は，書面による同意が原則である。

本体の **3.4.2.4** の“明示”とは，本人に対して，本体の **3.4.2.4** の **a)**～**h)**の事項又はそれと同等以上の内容

の事項が書面によって明確に示されることをいい，例えば，本体の **3.4.2.4** の **a)**～**h)**の事項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や，本人がアクセスした自社のウェブ画面上に本体の **3.4.2.4** の **a)**～**h)**の事項を明記するなど，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。

“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，個人情報保護法第 18 条第 2 項のただし書きを踏まえて規定している。

本体の **3.4.2.5** のただし書き **a)**～**d)**は，個人情報保護法第 18 条第 4 項第 1 号～第 4 号を踏まえて規定している。

本体の **3.4.2.6** のただし書き **a)**～**d)**は，個人情報保護法第 16 条第 3 項第 1 号～第 4 号及び第 23 条第 1 項第 1 号～第 4 号を踏まえて規定している。

“個人情報を第三者に提供することが予定される場合”については，個人情報の第三者への提供は，本人が直接関与しないことが多いため，本人に懸念を抱かせないよう，本体の **3.4.2.4 d)**に定める事項を具体的に明らかにすることが必要である。“組織の種類，及び属性”とは，個人情報の提供を受ける組織（企業）の業種と提供元である企業との関係（関連会社，持株会社など）を指す。

“本人が個人情報を与えることの任意性”とは，申込書への記入が義務的なものなのか，任意（アンケート的なもの）であるかについての情報を指し，“当該情報を与えなかった場合に本人に生じる結果”とは，記入欄に回答しなかった場合に起こり得る結果（例えば，結婚紹介申込書の年収の欄に記入しなければ，年収を考慮した相手を紹介しないことや，中途採用に応募する場合に履歴書に職歴を記入しなければ選考対象とならないことなど）を指す。

“本人が容易に認識できない方法によって個人情報を取得する”とは，例えば，クッキー情報の取得等が挙げられるが，その場合には，当該方法によって個人情報を取得している旨及び取得する個人情報の内容を開示することが求められる。

3.4.5　個人情報を 3.4.2.4 以外の方法によって取得した場合の措置（本体の **3.4.2.5**）

本人から直接書面によって取得する場合以外は，本体の **3.4.2.5** の要求事項が適用される。したがって，委託を受けた場合，第三者として提供を受けた場合，公開情報から取得した場合等だけでなく，本人から直接取得した場合であっても，書面によらずに取得した場合（例えば，監視カメラによって取得した場合，口頭によって取得した場合など）には，本体の **3.4.2.5** の対象となる。

本体の **3.4.2.5** の“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。例えば，面談又は電話のように口頭によって個人情報を取得する場合などは，通知も書面によらずに口頭で行ってもよい。

本体の **3.4.2.5** の“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。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。

本体の **3.4.2.5** のただし書き **a)**～**d)**は，個人情報保護法第 18 条第 4 項第 1 号～第 4 号を踏まえて規定している。

本体の **3.4.2.5 a)**の場合とは，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，当該総会屋の個人に関する情報を取得し，企業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って，当該総会屋等の逆恨みによって，第三者たる情報提供者が被害を被るおそれがある場合などをいう。

本体の **3.4.2.5 b)**の場合とは，例えば，通知又は公表される利用目的の内容によって，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などをいう。

本体の **3.4.2.5 c)**の場合とは，例えば，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された場合，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って，捜査活動に重大な支障を及ぼすおそれがある場合などをいう。

本体の **3.4.2.5 d)**の場合であるかどうかは，条理又は社会通念による客観的判断によって，極力限定的に解釈する必要がある。商品やサービスの販売・提供において住所・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やサービス等の販売・提供だけを確実に行うためという利用目的であるような場合（クリーニング店やデリバリーサービスなどで受取人を特定するために個人情報を取得するなど）や，一般の慣行としての名刺交換（ただし，ダイレクトメール等の目的に名刺の個人情報を用いることは，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。）の場合などはこれに該当する。また，請求書や見積書等の伝票に記載された担当者名，捺印等もこれに該当する。ただし，本体の **3.4.2.5 d)**によって取得した個人情報であっても，その取扱いの委託を受けた場合は，本体の **3.4.2.5 d)**に該当しない。

3.4.6　利用に関する措置（本体の **3.4.2.6**）

企業内のある部門が，本人の同意を得て取得した個人情報を他の部門が利用する場合には，本人の同意を得た当初の目的の範囲内である場合と範囲外の場合の両方があり得る。後者の場合には，たとえ同一企業内であっても，改めて事前の本人の同意を得ることが必要である。

なお，本人が想定できる範囲であっても，同意を得た範囲を超えて利用目的を変更することは目的外利用に該当する点に注意する必要がある。

利用目的を特定した日以降に利用目的を変更した場合で，本体の **3.4.2.4** 又は **3.4.2.5** によって既に利用目的を明らかにしているときは，本体の **3.4.2.6** によって本人の同意を得る必要がある。

本体の **3.4.2.6** のただし書き **a)～d)**は，個人情報保護法第 16 条第 3 項第 1 号～第 4 号及び第 23 条第 1 項第 1 号～第 4 号を踏まえて規定している。

本体の **3.4.2.6 a)**は，法令に基づいて個人情報を取り扱う場合をいう。例えば，刑事訴訟法第 218 条の令状による捜査に基づき，個人情報を取り扱う場合，少年法第 6 条の 5 の令状による触法少年の調査の場合，所得税法第 234 条の所得税に係る税務職員の質問検査権の行使の場合，地方税法第 72 条の 7 の事業税に係る徴税吏員の質問検査権行使の場合などをいう。

本体の **3.4.2.6 b)**は，人（法人を含む。）の生命又は財産といった具体的な権利利益が侵害されるおそれがあり，これを保護するために個人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（他の方法によって，当該権利利益の保護が十分可能である場合を除く。）をいう。例えば，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，製品事故が生じたため，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などをいう。

本体の **3.4.2.6 c)**は，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（他の方法によって，当該権利利益の保護が十分可能である場合を除く。）をいう。例えば，不登校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などをいう。

本体の **3.4.2.6 d)**は，国の機関等が法令の定める事務を実施する上で，民間企業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をいう。例えば，事業者が，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などをいう。

b)～**c)**の場合に該当するかどうかについては，当事者のし（恣）意的な判断ではなく，条理又は社会通念による客観的判断のもとで，極力限定的に解釈する必要がある。

d)の場合に国の機関等による任意の求めに応じるかどうかについては，当事者のし（恣）意的な判断ではなく，条理又は社会通念による客観的判断のもとで，限定的に解釈する必要がある。

3.4.7　本人にアクセスする場合の措置（本体の **3.4.2.7**）

本体の **3.4.2.7** の“本人にアクセスする”とは，個人情報の利用目的の達成に当たり，本人に対し，郵便，電話，又はメールなどで連絡する又は接触することである。

本体の **3.4.2.7** の“取得方法”については，“同窓会名簿”及び“官報”等の取得源の種類並びに“書店から購入”等の取得経緯を通知する。

本体の **3.4.2.7** の同意は，例えば，ダイレクトメールの場合，最初に出すダイレクトメールに通知文書を同封して送付し，本人の同意が得られれば，継続して本人にアクセスできることになる。

なお，回答が無い場合に黙示の同意があったものとみなすことは原則として不適切である。

本体の **3.4.2.7** のただし書き **b)**～**d)**は，個人情報保護法第 23 条第 4 項第 1 号～第 3 号を踏まえて規定している。

本体の **3.4.2.7 b)**によって個人情報の取扱いの委託を受けた者は，個人情報の取扱いに際し，委託の本旨に反して利用及び提供をすることは当然に許されないことであり，また，この規格に従い，個人情報を適正に管理する必要がある。

なお，委託を受けた者が，自身は適正に業務を実施するとしても，結果として個人情報の不適正な利用を助長することになれば，それもまた当然望ましいことではない。したがって，委託を受ける者は，委託を受けた個人情報が適正に取得されたものかどうか，委託者に確認するよう努めるべきであり，委託する者が明らかに法令に違反している場合には，委託を受けてはならない。

本体の **3.4.2.7 d)**の“共同して利用する者の範囲”は，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でない場合もある。例えば，最新の共同利用者のリストを本人が容易に知り得る状態に置いているときなどが該当する。

本体の **3.4.2.7 d)**の“共同して利用する個人情報の管理について責任を有する者の氏名又は名称”とは，開示等（本体の **3.4.4.1** 以下を参照。）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，個人情報の内容等について，開示，訂正，利用停止等の権限を有し，安全管理等個人情報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。）をいう。

本体の **3.4.2.7 d)**に規定する共同利用を実施する際には，共同利用する者の間で，共同利用者の要件，各共同利用者の個人情報取扱責任者・問合せ担当者及び連絡先，共同利用する個人情報の取扱いに関する事項（漏えい防止に関する事項，目的外加工，利用，複写，複製等の禁止など），共同利用する個人情報の取扱いに関する取り決めが遵守されなかった場合の措置，共同利用する個人情報に関する事件・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などを取り決めておくことが望ましい。

3.4.8　提供に関する措置（本体の **3.4.2.8**）

個人情報を第三者に提供する場合には本人の同意を得ることが原則である。ただし，個人情報を直接取得する時点で，情報の提供について，本人から再提供を含めて同意を得ている提供者から取得した場合は，

本人が同意した利用目的の範囲内で提供する限り，改めて本人の同意を得る必要はない。例えば，本人の同意を得て作成されている名簿は，販売時に改めて同意を得る必要はない。

なお，特定した利用目的の達成を必要な範囲を超えて個人情報を提供することは，利用目的の達成に必要な範囲を超えた利用に該当するため，本体の **3.4.2.6** によって，本人の同意を得る必要がある。

本体の **3.4.2.8 b)**の“大量の個人情報を広く一般に提供するため，本人の同意を得ることが困難な場合”に該当するかどうかについては，広く一般に提供することの公共的な有益性と本人の不利益とを比較し，条理又は社会通念による客観的判断のもとで，極力限定的に解釈する必要がある。

本体の **3.4.2.8 b)**の各小項目は，本人に通知することが原則であるが，第三者から間接的に取得した個人情報である場合には，本人に通知することが困難な場合があり得る。この場合は，**b)**の小項目について，通知に代わる同等の措置を講じることによって，本人の同意を得ずに第三者に提供することができる。この場合の“それに代わる同等の措置を講じている”とは，例えば，データベース事業者等が，企業の総務担当者から従業員の個人情報を取得する場合に，**b)**の各小項目を，個人情報の取得者が本人に対して直接通知するのではなく，当該企業の総務担当者を通じて本人に通知するなど，通知と同等といえるだけのできる限りの措置を講じることを要する。

なお，個人情報保護法第 23 条第 2 項で規定する“第三者提供におけるオプトアウト”は，第三者提供に当たりあらかじめ，個人情報保護法第 23 条第 2 項各号に規定する内容を，本人に通知し，又は本人が容易に知り得る状態に置いておくとともに，本人の求めに応じて第三者への提供を停止することをいうが，本体の **3.4.2.8 b)**は，公表又は本人が容易に知り得る状態に置くことだけでは足りない。

本体の **3.4.2.8 c)**の“法人その他の団体の役員に関する情報”とは，株主総会などで配布される事業報告書など，株主や顧客に配布される書類などに記載されている役員の履歴，持株数など，法令又は本人若しくは当該法人その他の団体自らによって公表されているような情報を指す。個人が営業する屋号については，法人その他の団体の役員に関する情報と考えてよい。

“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。

なお，本体の **3.4.2.8 e)**の事業の承継のために，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，自社の個人情報を相手会社へ提供する場合は，当該個人情報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する必要がある。

3.4.9　正確性の確保（本体の 3.4.3.1）

事業者は，個人情報の正確性を確保するため，誤入力チェック，データのバックアップなどの手順を確立しなければならない。

なお，取得した個人情報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よい。

3.4.10　安全管理措置（本体の 3.4.3.2）

安全管理措置については，個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインをはじめとした，各所管省庁が作成したガイドライン・指針等を参考にした対策を講じる必要がある。

なお，安全管理措置は，個人情報が漏えい等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情報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ことが求められているのであって，すべての個人情報について一律な措置を求めるものではない。

“漏えい，滅失又はき損”とは，個人情報保護法第 20 条で規定する内容と同義であり，個人情報への不正アクセス，個人情報の紛失，破壊及び改ざんなども含む概念である。

“必要かつ適切”という意味は，経済的に実行可能な最良の技術の適用に配慮することである。“経済的に実行可能な最良の技術”は，事業者の事業内容や規模によって異なる。

個人情報の漏えい事例には，廃棄時の漏えいが多くみられることから，廃棄に当たっても，電子ファイルの消去，個人情報が打ち出された紙の破砕処理などによって，廃棄された個人情報が他者に流出することのないよう留意することが必要である。

3.4.11　従業者の監督（本体の **3.4.3.3**）

“従業者”とは，事業者の組織内で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（正社員，契約社員，嘱託社員，パート社員，アルバイト社員等）のほか，取締役，執行役，理事，監査役，監事，派遣社員等を含む（なお，本体の **3.2**，**3.3.4** 及び **3.4.5** で用いている“従業者”についても同じ。）。

なお，監査役に対する監督は，株主総会による選任権及び解任権を通じた監督によるべきであり，取締役等業務執行者による監督は，監査の独立性が害されるため許されない。

本体の **3.4.3.2** によって定めた安全管理措置を遵守させるよう，従業者に対し，必要，かつ，適切な監督を行わなければならない。

なお，本体の **3.4.5** の教育の要求事項は，従業者に，個人情報保護マネジメントシステムの運用を確実に実施できる力量を備えさせるための要求事項であり，従業者の監督とは意味合いが異なる。

3.4.12　委託先の監督（本体の **3.4.3.4**）

委託者は，個人情報の取扱いの全部又は一部を委託する場合，特定した利用目的の範囲内で委託契約を締結することが必要である。

なお，委託を行う場合においては，委託者は，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など，委託処理の透明化を進めることが望ましい。

委託先の監督の前提として，委託する業務内容に対して必要のない個人情報を提供しないようにすることは当然に求められることである。必要のない個人情報を提供した結果，委託先が個人情報を漏えいした場合には，必要かつ適切な安全管理措置を講じていたとはみなされないことにも留意すべきである。

委託先を選定する基準は，少なくとも委託する当該業務に関しては，自社と同等以上の個人情報保護の水準にあることを客観的に確認できるものでなければならない。個人に委託する場合であっても，委託先選定基準による選定が必要である。

委託先が倉庫業，データセンター（ハウジング，ホスティング）等の事業者であって，当該事業者に取り扱わせる情報に個人情報が含まれるかを認識させることなく預ける場合であっても，委託者は委託するものが個人情報であることを認識しているわけであるから，委託先選定基準による選定が必要である。ただし，“個人情報”に関する条項を契約書に盛り込むことを要求するものではない。

“必要，かつ，適切な監督”には，委託契約において，当該個人情報の取扱いに関して，必要，かつ，適切な安全管理措置として，委託者，受託者双方が同意した内容を契約に盛り込むとともに，同内容が適切に遂行されていることを，あらかじめ定めた間隔で確認することも含まれる。

なお，優越的地位にある者が委託者の場合，受託者に不当な負担を課すことがあってはならない。また，優越的地位にある者が受託者の場合も，委託者の権利を不当に制限することがあってはならない。

本体の **3.4.3.4** の **a)～g)**の事項は，いかなる場合にも契約によって規定することを要求するものではなく，

取り扱う個人情報のリスクに応じて規定する内容が変わり得るものである。

本体の **3.4.3.4 b)**個人情報の安全管理に関する事項には，以下の事項が含まれる。

－ 個人情報の漏えい防止，盗用禁止に関する事項
－ 委託範囲外の加工，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情報の返還・消去・廃棄に関する事項

本体の **3.4.3.4 c)**再委託に関する事項には，以下の事項が含まれる。

－ 再委託を行うに当たっての委託者への文書による報告

なお，人材派遣事業者との人材派遣契約，清掃事業者との契約，オフィスの賃貸借契約等は，個人情報の取扱いを含まない限り，本体の **3.4.3.4** の対象外である。これらは広く本体の **3.4.3.2** に含まれるものであり，このような事業者とは，守秘義務に関する事項を盛り込んだ契約を締結することが望ましい。

3.4.13 個人情報に関する権利（本体の 3.4.4.1）

“開示対象個人情報”は，原則として個人情報保護法でいう“保有個人データ”と同様の概念であるが，保有個人データと異なり，消去までの期間は問わない。この点，“開示対象個人情報”は法律上の用語ではないため，“開示対象個人情報”という用語を用いる場合には，本規格の用語である旨の注意書きを付すなど，混同を招かないように配慮することが望ましい。

本体の **3.4.4.1** のただし書き **a)～d)**は，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）第 3 条を踏まえて規定している。

本体の **3.4.4.1 a)**の場合とは，例えば，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）を本人とする個人情報をもっている場合などをいう。

本体の **3.4.4.1 b)**の場合とは，例えば，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情報をもっている場合や，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情報を保有している場合などをいう。

本体の **3.4.4.1 c)**の場合とは，例えば，製造業者，情報サービス事業者等が，防衛に関する兵器・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情報を保有している場合や，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などをいう。

本体の **3.4.4.1 d)**の場合とは，例えば，警察からの捜査関係事項照会や捜査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情報を保有している場合などをいう。

3.4.14 開示等の求めに応じる手続（本体の 3.4.4.2）

事業者は，本人に対し，その開示対象個人情報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，当該開示対象個人情報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。

なお，開示等の求めをすることができる代理人は，以下の代理人とする。

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

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。ただし，本人確認に当たっては，例えば，通常業務において ID 及びパスワードで本人確認をしているにもかかわらず，開示等の求めに応じる手続について

は，一律，運転免許証又はパスポートの呈示を求めるなど，本人に必要以上の個人情報の提供を求めるべきではない。

3.4.15　開示対象個人情報に関する事項の周知など（本体の **3.4.4.3**）

事業者は，開示対象個人情報に関する事項を本人が知り得る状態におくことによって，開示等の対象となる個人情報を明確にしなければならない。“本人が知り得る状態(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，本人が知ろうと思えば知ることができる状態に置くことをいい，常にその時点で正確な内容を本人が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い状況に応じ，内容が本人に認識される合理的かつ適切な方法によらなければならない。

本体の **3.4.4.3** の **a)**～**f)**は，個人情報保護法第 24 条第 1 項を踏まえて規定している。

なお，事業者は，家族から開示等を求められることもあり得るため，そのような場合も含め，開示等の求めに対する対応方法の詳細を定めた上で，知り得る状態に置いておくことが望ましい。

また，本体の **3.4.4.3** の **d)**～**e)**は，苦情の申し出先について，本人の知り得る状態に置くことを求めているが，これは開示対象個人情報である場合についてのみ苦情及び相談への対応を求めている趣旨ではないことに留意が必要である。

3.4.16　開示対象個人情報の利用目的の通知（本体の **3.4.4.4**）

本体の **3.4.4.4** のただし書きは，個人情報保護法第 24 条第 2 項及び第 3 項を踏まえて規定している。

3.4.17　開示対象個人情報の開示（本体の **3.4.4.5**）

本体の **3.4.4.5** のただし書き **a)**～**c)**は，個人情報保護法第 25 条第 1 項を踏まえて規定している。

本体の **3.4.4.5 b)**の“当該事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合”とは，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って，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や，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返し開示の求めがあり，事実上問合せ窓口が占有されることによって他の問合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などをいう。

なお，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，問合せ等があった場合には本人からの求めに一層対応していくことが望ましい。

3.4.18　開示対象個人情報の利用又は提供の拒否権（本体の **3.4.4.7**）

個人情報保護法第 27 条では，本人の求めに応じる義務が発生するのは，事業者が同法第 16 条，第 17 条又は第 23 条に違反していることが前提になるが，この規格では，本人の同意を得た範囲内で事業者が取り扱う場合でも，本人が求めた場合は，事業者は原則としてそれに応じなければならないことに注意する必要がある。

なお，当該開示対象個人情報の第三者への提供の停止に著しく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。

3.4.19　教育（本体の **3.4.5**）

事業者は，従業者に，本体の **3.4.5** の **a)**～**c)**に定める事項を理解させ，自覚させ，個人情報保護体制における各々の役割・権限を確実に果たすことができるようにしなければならない。そのため，結果を報告する際には，単に教育実施の結果を報告するだけではなく，教育の有効性の確認を報告することが必要であ

る。すなわち，アンケートや小テストを実施するなどによって従業者の理解度を把握し，必要に応じて教育内容の見直しを図ることや，教育を受けたことを自覚させる仕組みを取り入れることが望ましい。欠席者にも漏れなく教育することが必要であり，従業者全員に教育を実施したことの記録を残さなければならない。

3.5　個人情報保護マネジメントシステム文書

3.5.1　文書の範囲（本体の 3.5.1）

個人情報保護マネジメントシステムとは，本体の **2.7** の定義にもあるように，実際に事業者内で機能している仕組みそのものをいい，内部規程だけでなく資源も含めた全体を指す。“マネジメントシステムの基本となる要素”とは，その個々の構成要素のことであり，それを明確に把握するために文書化しておくことが必要である。本体の **3.5.1** の **a)**～**d)**は，最低限，文書化しておくべきである。

3.5.2　文書管理（本体の 3.5.2）

文書管理とは，個人情報保護マネジメントシステム文書及び下位文書を保存し，常に最新の状態で維持しておくことである。記録は文書の一種ではあるが，本体の **3.5.3** に規定する要求事項に従って管理するものとする。

文書類は，個人情報保護マネジメントシステムを構成する要素が互いにどのように関係しているか，及び特定部分の運用についての詳細な情報がどこに記述されているかを，十分に示せる程度にあればよい。文書類は，事業者によって実施される他のシステムの文書類と統合されることがある。

当初は，個人情報保護マネジメントシステム以外の目的で作成した文書が，個人情報保護マネジメントシステムの一部として使用されることがある。そのような使い方をする場合は，それらの文書を個人情報保護マネジメントシステムの中で参照しておく必要がある。

なお，文書管理は，個人情報保護マネジメントシステムを確実に実施するための手段であって，目的ではない。手段と目的とを混同しないよう留意する必要がある。

3.5.3　記録の管理（本体の 3.5.3）

この規格で必要とする記録には，以下のものが含まれる。

a)　個人情報の特定に関する記録
b)　法令，国が定める指針及びその他の規範の特定に関する記録
c)　個人情報のリスクの認識，分析及び対策に関する記録
d)　計画書
e)　利用目的の特定に関する記録
f)　開示対象個人情報に関する開示等（利用目的の通知，開示，内容の訂正，追加又は削除，利用の停止又は消去，第三者提供の停止）の求めへの対応記録
g)　教育実施記録
h)　苦情及び相談への対応記録
i)　運用の確認の記録
j)　監査報告書
k)　是正処置及び予防処置の記録
l)　代表者による見直しの記録

記録は紙媒体である必要はなく，事業者内において運用しやすい合理的な方法で作成するとよい。事業者は，必要な記録を特定し，保管，保護，保管期間及び廃棄についての手順を確立し，実施し，維持しなければならない。記録自体も個人情報である可能性があるから，とりあえず何でも記録として残すという

姿勢ではなく，その必要性を判断すべきである。また，記録は，必要なときにすぐに検証できるように維持しておかなければならない。

3.6　苦情及び相談への対応（本体の 3.6）

苦情及び相談の受付は，常設の対応窓口の設置又は担当者の任命によって行う必要がある。ただし，個人情報保護管理者との兼任を妨げない。

必要な体制の整備に当たっては，日本工業規格 **JIS Q 10002**（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。

3.7　点検

3.7.1　運用の確認（本体の 3.7.1）

組織全体として実施する監査（本体の **3.7.2**）と異なり，各部門及び各階層において行われるものである。各部門及び各階層の管理者は，定期的にマネジメントシステムが適切に運用されているかを確認し，不適合が確認された場合は，その是正処置及び予防処置を行うことが必要である。

また，一連のマネジメントシステムの実施結果を受けて行うものではなく，日常業務において気付いた点があればそれを是正及び予防していくものであるため，たとえ小規模な事業者であっても，**運用の確認**（本体の **3.7.1**）及び**監査**（本体の **3.7.2**）を行わなければならない。

3.7.2　監査（本体の 3.7.2）

監査は，個人情報保護マネジメントシステムの整備状況及び運用状況について行う。個人情報保護監査責任者は，内部の者から指名された適任者であることが要求されるが，個人情報保護管理者と異なる者でなければならず，かつ，社外に責任をもつことができる者（例えば，役員クラス）であって，個人情報保護管理者と同格又は上席者を指名することが望ましい。監査は，事業者内部からの要員によって，又は事業者のために働くように外部から選んだ者によって実施することができる。その際，監査を実施する監査員には，力量があり，公平かつ客観的に行える立場にある者をあてる。また，監査員は，自己の所属する組織の監査をしてはならない。ただし，小規模な事業者における個人情報保護監査責任者は，監査対象となる組織との兼務もやむを得ない。

運用状況の監査に当たっては，本体の **3.3.3** によって講ずることとした対策を，監査項目に設定して実施するとよい。

監査報告書には，監査実施の状況のほか，問題点として把握した指摘事項と，その中で改善すべき事項について区別して示す必要がある。

この規格は，他のマネジメントシステムと異なり，事業者単位で実施されることが前提になっている。したがって，監査結果の報告は事業者の代表者に行わなければならず，改善の指示も事業者の代表者から受けなければならない。

3.8　是正処置及び予防処置（本体の 3.8）

不適合は，点検の結果，緊急事態の発生及び外部機関の指摘等によって，事業者においてこの規格の要求を満たしていないと判断したものである。

不適合の原因が特定されなければ，根本的な解決にはならず，単なるもぐらたたきの改善で終わってしまい，再発を防げない。被監査部門は，指摘事項となった不適合の原因を特定した上で，再発防止のためのその是正処置及び予防処置を立案し，承認を受け，実施しなければならない。

是正処置を確実に実施させるために期限を区切ることは有効であるが，不適合の内容によっては，長期にわたることもあり得る。不適合の内容に相応した期限の設定が望ましい。

3.9　事業者の代表者による見直し（本体の 3.9）

監査は社内の現状のルールを前提に，それが守られているかを点検するものであり，それに基づく改善も現状の枠内に止まるものである。本体の **3.9** による代表者による見直しは，それに止まらず，外部環境も考慮した上で，現状そのものを根本的に見直すことがあり得る点で，監査による改善とは本質的に異なる。

常に，本体の **3.9** の **a)**～**g)**の事項をまとめて見直すという必要はない。見直しは，必要に応じて実施されることもある。

3.10　表示事項整理表

本規格における表示に関する要求事項を整理した表示事項整理表を，**解説表 1** に示す。

注記 1　要求事項として明らかなものだけを記載した。

注記 2　要求事項のただし書きにおける適用除外については，記載していない。

解説表 1－表示事項整理表

個人情報保護方針に関する事項				
	個人情報保護方針	本体の **3.2**	従業者に周知させるとともに，一般の人が入手可能な措置を講ずる。	□事業の内容及び規模を考慮した適切な個人情報の取得，利用及び提供に関すること
				□個人情報の取扱いに関する法令，国が定める指針その他の規範を遵守すること
				□個人情報の漏えい，滅失又はき損の防止及び是正に関すること
				□苦情及び相談への対応に関すること
				□個人情報保護マネジメントシステムの継続的改善に関すること
				□代表者の氏名
				□制定年月日及び最終改訂年月日（解説の **3.1** 参照）
				□個人情報保護方針の内容についての問合せ先（解説の **3.1** 参照）
緊急事態に関する事項				
	漏えい，滅失又はき損の発生	本体の **3.3.7**	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。	□当該漏えい，滅失又はき損が発生した個人情報の内容
			可能な限り遅滞なく公表する。	□事実関係，発生原因及び対応策

解説表 1－表示事項整理表（続き）

<table>
<tr><td colspan="5">個人情報の取得に関する事項</td></tr>
<tr><td></td><td rowspan="10">本人から直接書面による取得</td><td rowspan="10">本体の3.4.2.4</td><td rowspan="10">あらかじめ，書面によって本人に明示し，本人の同意を得る。</td><td colspan="2">□事業者の氏名又は名称</td></tr>
<tr><td colspan="2">□個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先</td></tr>
<tr><td colspan="2">□利用目的</td></tr>
<tr><td colspan="2">□個人情報を第三者に提供することが予定される場合は，</td></tr>
<tr><td></td><td>－第三者に提供する目的</td></tr>
<tr><td></td><td>－提供する個人情報の項目</td></tr>
<tr><td></td><td>－提供の手段又は方法</td></tr>
<tr><td></td><td>－当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性</td></tr>
<tr><td></td><td>－個人情報の取扱いに関する契約がある場合はその旨</td></tr>
<tr><td colspan="2">□個人情報の取扱いの委託を行うことが予定される場合には，その旨</td></tr>
<tr><td colspan="2">□開示対象個人情報に関する求めがあった場合には，その求めに応じる旨及び問合せ窓口</td></tr>
<tr><td colspan="2">□本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果</td></tr>
<tr><td colspan="2">□本人が容易に認識できない方法によって個人情報を取得する場合には，その旨</td></tr>
<tr><td></td><td>上記の方法以外の方法による取得</td><td>本体の3.4.2.5</td><td>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，本人に通知し，又は公表する。</td><td colspan="2">□利用目的</td></tr>
<tr><td colspan="5">個人情報の利用に関する事項</td></tr>
<tr><td></td><td rowspan="10">目的外利用</td><td rowspan="10">本体の3.4.2.6</td><td rowspan="10">あらかじめ，本人に通知し，本人の同意を得る。</td><td colspan="2">□事業者の氏名又は名称</td></tr>
<tr><td colspan="2">□個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先</td></tr>
<tr><td colspan="2">□利用目的</td></tr>
<tr><td colspan="2">□個人情報を第三者に提供することが予定される場合は，</td></tr>
<tr><td></td><td>－第三者に提供する目的</td></tr>
<tr><td></td><td>－提供する個人情報の項目</td></tr>
<tr><td></td><td>－提供の手段又は方法</td></tr>
<tr><td></td><td>－当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性</td></tr>
<tr><td></td><td>－個人情報の取扱いに関する契約がある場合はその旨</td></tr>
<tr><td colspan="2">□個人情報の取扱いの委託を行うことが予定される場合には，その旨</td></tr>
<tr><td colspan="2">□開示対象個人情報に関する求めがあった場合には，その求めに応じる旨及び問合せ窓口</td></tr>
</table>

解説表 1－表示事項整理表（続き）

<table>
<tr><td colspan="5">個人情報の利用に関する事項</td></tr>
<tr><td></td><td rowspan="10">本人へのアクセス</td><td rowspan="10">本体の3.4.2.7</td><td rowspan="10">本人に対して通知し，本人の同意を得る。</td><td colspan="2">□事業者の氏名又は名称</td></tr>
<tr><td colspan="2">□個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先</td></tr>
<tr><td colspan="2">□利用目的</td></tr>
<tr><td colspan="2">□個人情報を第三者に提供することが予定される場合は，</td></tr>
<tr><td></td><td>－第三者に提供する目的</td></tr>
<tr><td></td><td>－提供する個人情報の項目</td></tr>
<tr><td></td><td>－提供の手段又は方法</td></tr>
<tr><td></td><td>－当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性</td></tr>
<tr><td></td><td>－個人情報の取扱いに関する契約がある場合はその旨</td></tr>
<tr><td colspan="2">□個人情報の取扱いの委託を行うことが予定される場合には，その旨</td></tr>
<tr><td colspan="5">個人情報の提供に関する事項</td></tr>
<tr><td></td><td rowspan="10">第三者への提供</td><td rowspan="10">本体の3.4.2.8</td><td rowspan="10">あらかじめ，本人に対して通知し，本人の同意を得る。</td><td colspan="2">□事業者の氏名又は名称</td></tr>
<tr><td colspan="2">□個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先</td></tr>
<tr><td colspan="2">□利用目的</td></tr>
<tr><td colspan="2">□個人情報を第三者に提供することが予定される場合は，</td></tr>
<tr><td></td><td>－第三者に提供する目的</td></tr>
<tr><td></td><td>－提供する個人情報の項目</td></tr>
<tr><td></td><td>－提供の手段又は方法</td></tr>
<tr><td></td><td>－当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性</td></tr>
<tr><td></td><td>－個人情報の取扱いに関する契約がある場合はその旨</td></tr>
<tr><td colspan="2">□取得方法</td></tr>
</table>

解説表 1－表示事項整理表（続き）

開示対象個人情報に関する事項				
	開示対象個人情報に関する事項の周知	本体の**3.4.4.3**	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。	□事業者の氏名又は名称
				□個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先
				□すべての開示対象個人情報の利用目的［本体の**3.4.2.5** の **a)**～**c)**までに該当する場合を除く。］
				□開示対象個人情報の取扱いに関する苦情の申し出先
				□個人情報保護法第 37 条第 1 項の認定を受けた者（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し出先
				□開示等の求めの申し出先
				□開示等の求めに際して提出すべき書面の様式その他の開示等の求めの方式
				□開示等の求めをする者が，本人又は代理人であることの確認の方法
				□本人から，利用目的の通知又は開示対象個人情報の開示を求められた場合の手数料（定めた場合に限る。）の徴収方法
	開示対象個人情報の利用目的の通知	本体の**3.4.4.4**	本人に遅滞なく通知する。	□利用目的
			本人に遅滞なく通知するとともに，理由を説明する。	□利用目的の通知をしないときは，その旨
	開示対象個人情報の開示（存在しないときにその旨を知らせることを含む）	本体の**3.4.4.5**	法令の規定によって特別の手続が定められている場合を除き，本人に対し，遅滞なく書面（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）によって開示する。	□当該開示対象個人情報（存在しないときにその旨）
			本人に遅滞なく通知するとともに，理由を説明する。	□全部又は一部を開示しないときは，その旨
	開示対象個人情報の訂正，追加又は削除（訂正等）	本体の**3.4.4.6**	本人に対し，遅滞なく通知する。	□訂正等を行ったときは，その旨及びその内容
				□訂正等を行わない旨の決定をしたときは，その旨及びその理由
	開示対象個人情報の利用の停止，消去又は第三者への提供の停止（利用停止等）	本体の**3.4.4.7**	本人に遅滞なく通知する。	□措置を講じた後は，その旨
			本人に遅滞なく通知するとともに，理由を説明する。	□利用停止等を行わないときは，その旨

III 原案作成委員会の構成表

原案作成委員会の構成表を，次に示す。

JIS Q 15001 改正原案作成委員会　構成表

	氏名	所属
(委員長)	堀　部　政　男	中央大学法科大学院
(幹事)	藤　原　静　雄	筑波大学大学院
(委員)	相　澤　直　行	財団法人医療情報システム開発センター
	足　立　和　朗	電気事業連合会
	岩　瀧　敏　昭	社団法人日本クレジット産業協会
	江　藤　　学	経済産業省産業技術環境局
	長　見　萬里野	財団法人日本消費者協会
	加　藤　洋　一	経済産業省商務情報政策局
	金　子　直　好	日本百貨店協会（株式会社小田急百貨店）
	佐　藤　厚　夫	社団法人情報サービス産業協会
	新　保　史　生	筑波大学大学院
	鈴　木　正　朝	国立大学法人新潟大学
	鈴　木　　靖	株式会社シーピーデザインコンサルティング
	関　　志　郎	社団法人全国学習塾協会
	関　本　　貢	財団法人日本情報処理開発協会
	高　芝　利　仁	高芝法律事務所
	高　柳　忠　明	社団法人日本マーケティング・リサーチ協会
	武　田　隆　男	社団法人日本病院会
	玉　本　雅　子	社団法人日本消費生活アドバイザー・コンサルタント協会
	長谷川　和　久	社団法人全日本冠婚葬祭互助協会
	松　尾　正　浩	株式会社三菱総合研究所
	松　田　雄　一	社団法人日本人材派遣協会
	万　場　　徹	社団法人日本通信販売協会
(関係者)	佐々木　啓　介	経済産業省商務情報政策局
	齊　藤　雄　一	経済産業省商務情報政策局
	太　田　克　良	経済産業省商務情報政策局
	矢　野　友三郎	経済産業省産業技術環境局
	小　田　宏　行	経済産業省産業技術環境局
	西　田　聖　道	財団法人日本情報処理開発協会
	江　口　正　裕	次世代電子商取引推進協議会
(事務局)	岡　本　　裕	財団法人日本規格協会
	朝　山　恒　男	財団法人日本規格協会

（文責　太田　克良）

JIS Q 15001 改正作業部会　構成表

	氏名	所属
(主査)	高　芝　利　仁	高芝法律事務所
(委員)	相　澤　直　行	財団法人医療情報システム開発センター 医療情報安全管理推進部
	小　堤　康　史	社団法人電子情報技術産業協会情報法規専門委員会
	新　保　史　生	慶應義塾大学総合政策学部
	鈴　木　　靖	株式会社シーピーデザインコンサルティング
	関　本　　貢	財団法人日本情報処理開発協会 プライバシーマーク推進センター
	松　尾　正　浩	株式会社三菱総合研究所
	松　田　治　男	財団法人日本データ通信協会
(関係者)	西　田　淳　二	経済産業省商務情報政策局
	篠　原　治　美	経済産業省商務情報政策局
	布　施　剛　之	経済産業省産業技術環境局
(事務局)	小　林　慎太郎	株式会社野村総合研究所
	水之浦　啓　介	株式会社野村総合研究所
	八　代　　拓	株式会社野村総合研究所
	伊　藤　智　久	株式会社野村総合研究所

財団法人日本規格協会
〒107-8440　東京都港区赤坂 4 丁目 1-24
平成 23 年 9 月 20 日発行