JIS Q 15001:2006 をベースにした
個人情報保護マネジメントシステム実施のための
のガイドライン
－第２版－

一般財団法人日本情報経済社会推進協会
プライバシーマーク推進センター

はじめに

1980 年 9 月、OECD（経済協力開発機構）においてプライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告が採択され、そこで個人情報の保護に関する 8 原則が示された。以下に示すこの 8 原則は個人情報保護に関する実質的な標準となっており、世界各国の個人情報保護に関する法令はこれに準拠しているといっても過言ではない。当然、「個人情報保護法［個人情報の保護に関する法律（平成 15 年法律第 57 号）］」も JIS Q 15001 もこれに準拠した内容になっている。

① 収集制限の原則（Collection Limitation Principle）：
個人情報の収集には限度があり、かつ収集は適法かつ公正な手段によらなければならない。場合によっては、本人の認識又は同意が必要である。

② データ内容の原則（Date Quality Principle）：
個人情報は、利用目的の達成に必要な範囲内において、正確で完全で最新のものでなければならない。

③ 目的明確化の原則（Purpose Specification Principle）：
個人情報の収集目的は、遅くとも収集時には特定されていなければならず、その利用は収集目的（又は当該収集目的に反しない範囲で変更した利用目的）を達成する範囲内に限られる。

④ 利用制限の原則（Use Limitation Principle）：
個人情報は、特定された収集目的を超えて開示、提供又は利用されてはならない。ただし本人の同意がある場合又は法令に基づく場合はこの限りではない。

⑤ 安全保護の原則（Security Safeguards Principle）：
個人情報の保護のために、紛失、無権限でのアクセス、破壊、利用、改ざん又は漏えいといったリスクに対し合理的な安全対策を講じなければならない。

⑥ 公開の原則（Openness Principle）：
個人情報の取扱いについては公開するという基本方針がなければならない。個人情報の存在や種類、その主要な利用目的、その管理者及び所在地を明確にする手段が容易に利用できなければならない。

⑦ 個人参加の原則（Individual Participation Principle）：
本人は次の権利を有する。

(a) 個人情報の管理者等から、当該本人に関する情報を有しているか否か確認を得る。

(b) 当該本人に関する情報についての本人からの求めに回答を得る（個人情報の管理者は、合理的な期間内に、手数料を定めた場合は合理的な金額で、合理的な方法で、かつ当該本人に容易に理解できる形式で応じなければならない）

(c)　本人の求めに応じない場合にその理由の説明を求め異議を唱える

(d)　当該本人に関する情報の正当性について異議を唱え、もしその主張が正しければ、当該情報は消去又は訂正される

⑧　責任の原則（Accountability Principle）：

個人情報の管理者は、上記①～⑦の原則を定めたルールに準拠する責任を負う。

この OECD 8 原則に対応するため、1989 年、通商産業省（当時）が「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ついて（指針）」を公表した。

その後、1995 年 10 月には個人情報保護の取組みに関して大きな転換点となった、いわゆる「個人データ保護指令」が EU（European Union：欧州連合）で採択され、EU 加盟各国は 1998 年 10 月 24 日までに同指令に適合した国内法を整備するよう義務づけられた。また、同指令には EU 域内から個人データの保護水準が低い第三国への個人データの移転禁止が規定されていたため、他地域・諸国にも大きな影響を与えることとなった。国際的なビジネスを展開している事業者にとって、これは死活問題になると考えられたからである。

これに対応するため、通商産業省（当時）は上記指針を改定し、1997 年、「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」（平成 9 年 3 月 4 日通商産業省告示第 98 号）を策定した。さらに 1999 年 3 月、そのガイドラインを基に、個人情報の保護に関するマネジメントシステム規格として、「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（JIS Q 15001：1999）」が制定された。

個人情報保護を JIS のマネジメントシステム規格とした意義は、第三者認証制度の普及により、日本の個人データの保護水準を高めることが意図されたといえる。

- 民間部門の自主的取組みの促進
- 第三者認証の認証基準とすることにより取組みへのインセンティブを確保
- 認証基準の明確化により認証制度に対する社会的信頼性を確保
- JIS 化することによる業種業態を超えた対応の確保

第三者認証制度であるプライバシーマーク制度は 1998 年 4 月に創設され、その当時は 1997 年に公表された通商産業省（当時）の上記ガイドラインを認証基準としていたが、その JIS 化に伴い、認証基準を JIS Q 15001 に変更し現在に至っている。

JIS Q 15001:1999 は、2005（平成 17）年 4 月 1 日の個人情報保護法の全面施行を受けて 2006（平成 18）年 5 月に改正され JIS Q 15001:2006 として公表された。それに伴い、プライバシーマークの認証基準も JIS Q 15001:2006 に移行した。

この資料は、JIS Q 15001:2006 により個人情報保護マネジメントシステムを構築し運用するためのガイドライン、及びプライバシーマーク審査の基準となることを意図して作成したものである。

「第一部　個人情報保護マネジメントシステム作成指針」では、個人情報保護マネジメ

ントシステム構築にあたっての要点を述べ、「第二部　JIS Q 15001 各要求事項についてのプライバシーマーク付与適格性審査の基準」では、JIS Q 15001:2006 の要求事項ごとに、文書審査及び現地審査の項目と各々の審査における着眼点をリスト形式で記述した。個人情報保護マネジメントシステムの構築と審査の際の基準の両面における参考資料として、関係諸氏のお役に立てていただければ誠に幸いである。

目　次

第一部
個人情報保護マネジメントシステム作成指針

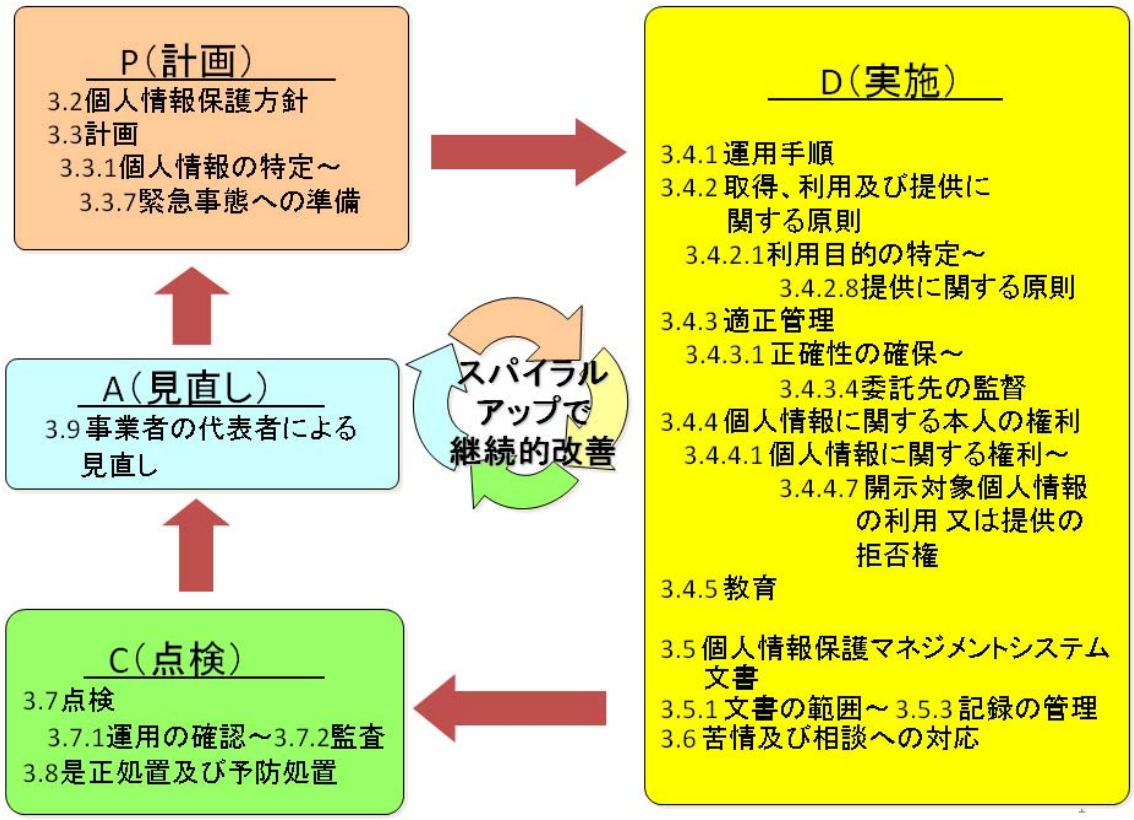
１．個人情報保護マネジメントシステムについて
２．JIS Q 15001:2006 に適合した個人情報保護マネジメントシステムを構築するメリット
３．JIS Q 15001:2006 での配慮
４．個人情報保護マネジメントシステム構築の具体的な進め方

１．個人情報保護マネジメントシステムについて

個人情報保護マネジメントシステム規格である JIS Q 15001:2006 は、マネジメントシステム規格を作成する場合の国際規約である ISO Guide 72:2001（マネジメントシステム規格の正当性及び作成に関する指針 ）に従って作成されている。したがって、品質マネジメントシステムや環境マネジメントシステムと共通のマネジメントシステム原則を採用している。

マネジメントシステム原則の趣旨は、方針を作成し、それに基づいて計画を作成し（Plan）、実施し（Do）、点検し（Check）、見直し（Act）を行うという、いわゆる PDCA サイクルをスパイラル的に継続することにより、事業者の管理能力を高めていくことにある。この仕組みを採用することで、事業者は個人情報の保護レベルを維持し、又は向上させていくことが期待される。

図 JIS Q 15001:2006 におけるＰＤＣＡサイクル



２．JIS Q 15001:2006 に適合した個人情報保護マネジメントシステムを構築するメリット

JIS Q 15001:2006 は、個人情報保護法を取込むことを最大の目標として、旧規格である JIS Q 15001:1999 から 2006 年 5 月 20 日に改正された。したがって、JIS Q 15001: 2006 に適合した個人情報保護マネジメントシステムを構築し、それを適正に運用していれば、個人情報保護法を遵守しているものと考えてよく、個人情報保護法に違反しないためにどのようにすればよいか分からないという事業者にとって、この JIS Q 15001:2006 は、非常に有効な指針といえる。

また、JIS Q 15001:2006 は、個人情報保護法を取り込んだだけでなく、個人情報保護法よりも高いレベルを求めている。したがって、個人情報保護法上は適法ではあっても規格上では不適合となる場合がある。個人情報保護法を遵守することは事業者としての当然の義務であるが、さらに一段高いレベルの保護水準を確立していることを対外的にアピールすることは、事業者にとって大きなメリットになるはずである。

さらに、2006 年 5 月に施行された会社法では、大会社や委員会設置会社に対して、法令や定款を遵守する体制の整備が義務づけられている。JIS Q 15001: 2006 が個人情報保護法の遵守を内容として含むことを考慮すると、JIS Q 15001:2006 が求める体制の整備は、会社法が求める法令遵守のための体制の整備に参考になるものと思われる。

３．JIS Q 15001:2006 での配慮

JIS Q 15001:2006 では、なるべくマネジメントシステム初心者にも分かりやすいようにしようという配慮がなされ、規格本体に可能な限りなすべきことを記述するとともに、規格に付属する解説で、できるだけ具体的に適用場面を記述してある。

規格本体と解説とを併せて読むことで、理解を深めることができる。

４．個人情報保護マネジメントシステム構築の具体的な進め方

前述のように、品質マネジメントシステム規格及び環境マネジメントシステム規格と共通の原則が採用されている。したがって、そのようなマネジメントシステムを既に運用している事業者は、それを基礎としてこの個人情報保護マネジメントシステムを構築することが可能である。

個人情報保護マネジメントシステム（以下、「PMS」という。）は、以下の手順で構築し、運用することができる。

ステップ 1 ：個人情報保護方針を定め文書化する
ステップ 2 ：PMS 策定のための組織を作る
ステップ 3 ：PMS 策定の作業計画を立てる
ステップ 4 ：個人情報保護方針を組織内に周知する
ステップ 5 ：個人情報を特定する
ステップ 6 ：法令、国が定める指針その他の規範を特定する
ステップ 7 ：個人情報のリスクを認識し、分析し対策を検討する
ステップ 8 ：必要な資源を確保する
ステップ 9 ：PMS の内部規程を策定する
ステップ 10 ：PMS を周知するための教育を実施する
ステップ 11 ：PMS の運用を開始する
ステップ 12 ：PMS の運用状況を点検し改善する
ステップ 13 ：PMS の見直しを実施する

ステップ１ ： 個人情報保護方針を定め文書化する

事業者の代表者は、個人情報の収集、利用、提供等に関する保護方針を定めなければならない。個人情報保護方針に定めなければならないことは、以下の内容である。

① 何のために個人情報保護活動を行うのか

② 個人情報保護のためにどのようなことをするのか

「何のために個人情報保護活動を行うのか」とは、規格本体 3.2 でいう「個人情報保護の理念」であり、個人情報保護に取り組む姿勢や基本的な考え方である。それには当然事業内容が絡んでくるであろう。その上で、「個人情報保護のためにどのようなことをするのか」の内容として、以下の事項を定める必要がある。

a) 個人情報の取得、利用及び提供に関すること（目的外利用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。）

b) 個人情報に関する法令、国が定める指針その他の規範の遵守に関すること
事業者の事業に関する法令等の中で個人情報の保護に関する事項が規定されている場合、又は行政機関等が特に定めた個人情報保護に関する規範等がある場合、これを遵守する必要がある。

c) 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

d) 苦情及び相談への対応に関すること

e) 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

そして、以上のように宣言したことについて、事業者の責任を明確にするために、以下の表示が求められるのである。

f) 代表者の氏名

PMS は、マネジメントシステムであることから、事業者が取り扱う個人情報とその扱い

方の変化、また事業者を取り巻く環境の変化等に対応することが求められる。したがって、事業者の代表者自らが継続的改善を明確に示しておくことは重要である。

なお、事業者の代表者は、この方針を文書化し、内外に公表しなければならない。したがって、一般に入手可能なように、例えば、事業者のホームページに掲載したり、リーフレット等に印刷したりする等の措置を講じる必要があるし、また社内にも周知徹底する必要がある。

以下のステップの実施は、この個人情報保護方針に記述したことの具体化であると理解しなければならない。

ステップ２ ： PMS 策定のための組織を作る

事業者の代表者は、組織の役員及び従業者等で構成するプロジェクトチーム（以下、「PMS 策定チーム」という。）を組織し、個人情報保護方針に基づいて個人情報保護マネジメントシステムの構築を推進させる。また、事業者の代表者は、各部門に対して、PMS 策定チームへの協力を指示する。

☞ **ポイント** 新しいことを実施する時は現場の負荷が増える。代表者が PMS 策定チームに丸投げしただけでは、PMS 策定チームは現場の協力を得られないため、作業が計画通りに進まなかったり、出来上がった PMS が現場の業務と乖離したものになったりすることが懸念される。代表者は、PMS 策定チームをバックアップする意思を明確に示す必要がある。また、外部コンサルタント等の協力を得る場合もあるが、この場合も外部コンサルタント等に丸投げするのでは自社の身の丈にあった PMS とはならない。事業者の従業者についても、PMS 策定チームと一体となり自社の PMS 構築にあたって積極的に関与する必要がある。

ステップ３ ：PMS 策定の作業計画を立てる

PMS 策定チームは、今後の作業スケジュールを立て、関係者に通知するとともに、協力を要請する。作業スケジュールは、以下のステップを考慮して立案する必要がある。

ステップ４ ：個人情報保護方針を組織内に周知する

PMS 策定チームは、事業者の代表者が定めた個人情報保護方針について、組織のすべての従業者に周知しなくてはならない。個人情報保護方針の周知は、事業者の代表者自らが行うことで、従業者の理解と PMS 策定チームへの協力への認識を高めることができ、より効果的である。

周知に当たっては、個人情報を保護することの重要性、利点及び個人情報が漏えい等した場合に予想される結果等を説明し、理解させることも必要である。

ここで、すべての従業者とは、事業者内で直接間接に事業者の指揮監督を受けて業務に

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、派遣社員等を含んでいる。

なお、すべての従業者に周知する意味は、直接に個人情報の取扱いに従事していない場合でも、組織内で個人情報に接する可能性があり、組織の方針を理解させておく必要があるからである。

ステップ５ ：個人情報を特定する

PMS 策定チームは、関係者の協力を得て自社内で取扱っている個人情報を特定する。

特定の対象となる個人情報は、事業者が事業で実際に活用している（これを「事業の用に供している」と呼ぶ）個人情報である。

個人情報の特定作業の意味は、このマネジメントシステムにおいて保護の対象となるものを明確にし、漏れのないようにすることである。各業務の中から個人情報を洗い出す方法には、主に(a)業務フロー図などを活用し、業務の流れに沿って個人情報を洗い出す方法と、(b)保管している帳票、保存データに注目して個人情報を洗い出す方法がある。(a)は、一時的に負担とはなるが、業務の流れを整理した上で特定するため、「特定漏れ」は生じにくい。また(b)は既存の帳票等を活用できるので取り組みやすいが、日常業務の観点で特定作業を行うため「特定漏れ」が生じやすくなる。

特定した結果は、当該個人情報の利用目的、入手経路、社内での取扱い経路（取扱い部署）、保管（一時保管も含む。）場所、保管形態（電子媒体、紙等）、保管期間、廃棄方法等について台帳等にまとめると、ステップ 7 のリスクの認識、分析・対策が行いやすくなる。

☞ **ポイント** PMS はリスクマネジメントシステムの一種である。まず、リスクマネジメントの対象となるものを洗い出し、明確にすることが出発点になる。

☞ **ポイント** 事業の用に供する個人情報は「事業者が商品やサービスを提供する業務において取り扱う個人情報」「従業者の採用や雇用管理で取り扱う個人情報」及び「PMS を運用することによって取り扱う個人情報」のいずれかに含まれることから、これを手掛かりにすることで「特定漏れ」をチェックすることも有効である。

ステップ６ ： 法令、国が定める指針その他の規範を特定する

事業者は、自身の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関連規範の有無について確認する。

事業者の個人情報の取扱いは、当該事業に関連する法令や国が定める指針等に規定がある場合には、JIS Q 15001 : 2006 に優先して適用されなければならないからである。なお、その他の規範として考えられる、いわゆる業界ガイドライン等に関しては、これも JIS と併せて遵守する必要があるが、JIS の要求事項のレベルよりも下回っている場合には当然のことながら JIS が優先されなければならない。

ステップ 7 ：個人情報のリスクを認識し、分析し対策を検討する

ステップ 5 で個人情報を特定する作業が終了した後、PMS 策定チームは、業務内容とそこに存在する個人情報の取扱いの流れを明確化し、個人情報が自社に入ってから出ていくまで（いわゆる個人情報のライフサイクル）を明らかにし、そのライフサイクルの局面（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄）ごとに、想定されるリスクを洗い出す。なおステップ 5 の個人情報の特定の段階から、業務フロー図などを活用して業務の流れを整理しておくと、ステップ 7 での作業が行いやすい.

想定されるリスクとして JIS Q 15001 では以下のようなものを挙げている。

- 漏えい（外に漏れること）
- 滅失（なくなってしまうこと）
- き損（壊れること、正確でなくなること）
- 目的外利用
- 関連する法令、国が定める指針その他の規範への違反
- 想定される経済的な不利益や社会的な信用の失墜の発生
- 本人への影響の発生

リスクを具体的に認識するには、誰が、どこで、どんなときに、何をすることによって、どんなリスクが現実のものとなるかを明らかにすればよい。単に「漏えいや滅失のリスクがある」との記載だけでは、具体的でなく、リスク対策を検討する上で十分とは言えない。

なお、社内にある情報資産をいかに守るか、という観点からのみのリスクの認識、分析及び対策では足りないことに注意する必要がある。個人情報は、例えば、取得や利用の局面において、本人の同意が得られていないことによる法令違反というリスクが想定されるが、これは情報資産の保護という観点からのみでは認識できないリスクである。このように、個人情報の保護においては、「守る」だけでなく適切な取扱いも求められる点に注意する必要がある。

洗い出して認識したリスクについては、リスクのもととなる原因（脅威）、発生の可能性と発生した場合の影響を分析・評価し、その結果に応じた合理的な対策を検討することになる。なお、「合理的」という言葉の解釈が非常にあいまいなために、事業者においてどの程度のリスク対策が「合理的」と判断できるかという問題がある。「合理的なリスク対策」とは、個人情報の取扱いに関するリスクが明確に認識・分析・評価されており、そのリスクに対するさまざまな予防処置を検討して、その中で当該事業者が取り得る最良の措置を講じることであり、予算を度外視した対策を講ずることではない。予算を度外視したリスク対策を計画しても、それが実行できなければ意味がない。「機械的なシステムを導入したいが、資金的な余裕がないから当面は人的な運用でカバーする」ということも、それは事業者の事情によるわけであるから、当然あり得る選択である。

また「事業者が取り得る」とするのは、検討したさまざまな対策の中から、費用、構築の容易さ、運用の容易さ、効果等の観点から総合的に検討して事業者自身が最適と判断し

た対策が実効性等の面からも効果的と考えられるからである。また、一つのリスクへの対策は、いくつかの対策を組み合わせることによって対応できるものが多いことから、技術的対策、物理的対策、人的管理的対策から多方面の検討が必要である。具体的には、「第二部　JIS Q 15001 各要求事項についてのプライバシーマーク付与適格性審査の基準」の「**3.4.3.2** 安全管理措置」に示す内容を参考にして対策を検討するとよい（93 ページを参照）。

このように策定されたリスク対策は、想定リスクとリスク対策とを一対にして管理し、「ライフサイクルのどの局面でどのようなリスクを認識し、どのような対策を講じたのか」との観点でそれぞれ関連づけを明確にしておく必要がある。リスクは常に変動するものであり、定期的かつ必要に応じた随時の見直しが必要であるが、この関連づけが明確でなければ、それぞれの業務内容や環境の変化に応じた見直しが出来ないおそれがあるからである。

なお、リスクへの対策を講じたとしてもすべてのリスクがなくなるわけではない。現状で可能な限りの対策を講じた上で、未対応部分については「残存リスク」として把握し、管理することが重要である。

また、講じたリスク対策を社内の関連規程（例えば、入退管理規程や情報システム管理規程などの安全管理措置規程、業務手順書など）に反映させリスクと関連付けた上で、関係者がいつでも参照できるようにしておくと社内でリスクに対する意識を高める効果が見込める。

このステップ 7 が確実に実施されていれば、講じることとした対策をまとめることで内部規程ができあがるはずである。

☞ **ポイント** ステップ 5～7 は、リスクマネジメントシステムとしての PMS の根幹である。ここが適正に実施されれば策定チームの作業のピークは乗り越えたといえる。逆にこの作業に抜けがあれば、PMS に従って個人情報を適正に取り扱ったとしても個人情報保護に対する十分性は確保できていないことになる。

ステップ 8 ：必要な資源を確保する

PMS 策定チームは、ステップ 7 の実施により、PMS 構築のために必要な経営資源（ヒト、モノ、カネ、情報）が判断できるはずである。それに基づき、各部門及び階層における個人情報を保護するための体制の整備を計画し、事業者の代表者に提示する。なお、資源を確保する段階で、計画の見直しが発生し、それがリスク対策にフィードバックされることもあり得る。事業者の代表者は、体制の整備計画に基づき、経営資源を配分し人事発令等を指示する。同時に、運用の開始時期を定め全従業者に周知する。

ステップ 9 ：PMS の内部規程を策定する

この作業の目的は、ステップ 8 までの手順で、実施すると決めたことを内部規程として

まとめることである。PMS は自社のマネジメントシステムであり、事業者の業種や規模や既存の他のシステムとの整合性が確保された実効性のある、身の丈に合ったものでなければならない。したがって、あらゆる事業者に適用できる内部規程としての「雛型」は存在しない。内部規程ができてからそれに実体を合わせるのではなく、実体を踏まえて内部規程化するのが順序である。内部規程は事業者にとって最も運用しやすい構成で作成するとよい。

PMS の実施にあたっては、最低限、以下の規定が必要である。すべての従業者が内部規程を遵守して個人情報の保護を実現するためには、具体的な手順、手段等が詳細に規定されていなければならない。

a) 個人情報を特定する手順に関する規定
b) 法令、国が定める指針その他の規範の特定、参照及び維持に関する規定
c) 個人情報に関するリスクの認識、分析及び対策の手順に関する規定
d) 事業者の各部門及び階層における個人情報を保護するための権限及び責任に関する規定
e) 緊急事態（個人情報が漏えい、滅失又はき損をした場合）への準備及び対応に関する規定
f) 個人情報の取得、利用及び提供に関する規定
g) 個人情報の適正管理に関する規定
h) 本人からの開示等の求めへの対応に関する規定
i) 教育に関する規定
j) 個人情報保護マネジメントシステム文書の管理に関する規定
k) 苦情及び相談への対応に関する規定
l) 点検に関する規定
m) 是正処置及び予防処置に関する規定
n) 代表者による見直しに関する規定
o) 内部規程の違反に関する罰則の規定

これらの規定は、共通的な部分（基本規程）と担当部署に依存する部分（詳細規程）があると考えられる。担当部署に依存する詳細な部分は、当該担当部署に協力要請して規定させることが PMS の実効性を高めるためには望ましい。その際には、事前に担当部署に対して個人情報保護方針、基本規程を十分に説明し理解させておくことが必須である。当該部署により規定された部分については、PMS 策定チームが個人情報保護方針、基本規程との整合性を十分に確認し、不整合がある場合は担当部門の間で協議して改善していかなければならない。なお、担当部署を巻き込んで詳細規程を作成することにより、PMS 策定の過程において、関係部門に個人情報保護方針、基本規程を周知することができるという効

果も期待できる。

なお、詳細規程については、既存の規程（例えば、罰則を規定した就業規則等）を参照して適用することも可能である。また、上記以外にも当該事業者の実情に応じて必要な事項を規定することが望ましい。事業者が所属する業界団体等が定めた個人情報保護に関するガイドライン、及び事業を規定した業法等法令や国が定める指針も参考にすることが必要である。ステップ 6 にも述べたとおり、業法等の法令に個人情報の取扱いに関する規定がある場合は JIS に優先するため、規程に反映しておくことが求められる。

策定した内部規程は、詳細規程を含め、JIS の要求事項に適合していることを評価しておかなければならない。内部規程が JIS の要求事項に反していたのでは、その後の運用が規定どおり実施されたとしても意味がないからである。

なお、策定した内部規程は、組織において決裁権限を有する者によって承認を受けなければならない。

a) 個人情報を特定する手順に関する規定

個人情報を特定する詳細手順を規定する。ステップ 5 で実施した手順を参考にするとともに、新しく取得する個人情報を特定する場合についても漏れがないように手順を定める必要がある。また、個人情報保護管理者が、個人情報の特定に関する最新状況をできる限り速やかに把握できる仕組みが必要である。

b) 法令、国が定める指針その他の規範の特定、参照及び維持に関する規定

自身の事業に関連する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特定し、特定した法令等について常に最新版を参照し維持する手順を規定する。この手順の目的は、特定した法令、国が定める指針その他の規範を参照し、必要に応じてその制定改廃の内容を PMS に反映させることである。

ステップ 6 で特定した法令等が運用開始時の基本になるが、これらは改定される性質のものであるから、最新版であるか、新たに加えるべきものはないか、不要になったものはないか等、定期的に確認することも手順として定める必要がある。

c) 個人情報に関するリスクの認識、分析及び対策の手順に関する規定

ステップ 7 で実施した手順を規定化すればよい。注意すべきことは、リスクは環境の変化や技術の進展等により常に変動することである。したがって、定期的な見直しは必須であり、また必要に応じて随時見直しを行うことも規定化する必要がある。ある部署で顕在化したリスクが他の部署でも当てはまる場合がある。その場合は、顕在化した部署内での見直しに止まるのではなく、全社的な見直しを実施する手続きとしなければならない。

d) 事業者の各部門及び階層における個人情報を保護するための権限及び責任に関する規定

詳細規程には、個人情報保護管理者の管理の下で個人情報の取扱いを担当する各部門のレベルで、部門管理者、権限及び責任を明確に規定しなければならない。支店、営業所等が全国に点在している場合においては、これらの場所についても同様に規定する必要がある。

e) 緊急事態（個人情報が漏えい、滅失又はき損をした場合）への準備及び対応に関する規定

万が一の緊急事態の発生に備え、それに対応するための手順を定め、社内の連絡手順、緊急事態の特定手順、被害・影響の把握、被害の拡大防止手順等、必要な事項を規定化する必要がある。どのような場合に緊急事態が発生し得るかは、ステップ 7 のリスクの認識、分析及び対策の手順を実施すれば明らかになるはずである。いかに被害を最小限に食い止めるかという観点から、対応策を定めなければならない。いうまでもないが、緊急時の対応手順は、緊急時に実施可能でなければならない。なお、緊急事態が起こったときの本人（消費者）への対応、関係機関への対応、マスコミ等への対応等の規定も必要である。

f) 個人情報の取得、利用及び提供に関する規定

個人情報の取得、利用、提供に関する関連部署の詳細手続きを規定する。

個人情報の取得に関しては、業務のそれぞれの現場で対応すべき事項について詳細に規定する必要がある。たとえば直接書面による取得とそれ以外の場合に分ける方法、業務フローに沿って実施すべきことを規定する方法などがある。

直接書面による取得の場合は、本人に通知すべき事項を書面により明示し、本人の同意を得るための詳細な手続きが重要である。直接書面による取得には、ウェブサイトからの入力も含まれる。事業者は、事業の推進に最適な方法を採用して手続き規定に反映しなければならない。

直接書面による取得以外の場合は、利用目的を本人に通知又は公表する必要がある。詳細については、第二部 3.4.2.1～3.4.2.8 を参照のこと。

g) 個人情報の適正管理に関する規定

個人情報の適正管理に関する規定には、正確性の確保に関する規定と安全性を確保するための規定が含まれる。

正確性の確保に関する規定には、データ処理システムの運用（オペレーション）に関する規定、データ更新手続きの規定、処理結果の確認規定等、個人情報取扱担当者のミ

スによる誤りを防止するための手続きを規定しなければならない。

安全性を確保するための規定には、合理的な安全対策に関して規定する必要がある。安全対策措置の内容等については、ステップ 7 において講じることとした対策をそのまま規定化すればよいはずである。一般的には、「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」（経済産業省、平成 16 年 10 月制定、以後原則として毎年改定）の法第 20 条関連として記載されている措置を参考に、事業者の業務内容や規模に応じた合理的な安全対策を規定化することが考えられ、それには以下のものが含まれる。

- 入退館（室）の管理、個人情報の盗難の防止等の措置に関する規定
- 個人情報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の措置に関する規定
- 個人情報の保管、廃棄、バックアップ等に関する個人情報管理規定
- 個人情報の取扱いの委託に関する委託先の選定基準、契約の基準等を定めた個人情報の委託先の監督に関する規定

h) 本人からの開示等の求めへの対応に関する規定

開示対象個人情報に関しては、当該本人に開示等を求める権利が認められているが、本人からの開示等の求めに、いかに対応するべきかを詳細に規定しておく必要がある。

本人とのトラブルは、これらの求めに的確に対応しなかったことによるものが多いことから、そのことを考慮した規定とするべきである。

なお、開示への対応時には、成りすましなどによって個人情報の漏えいに結び付く危険もあるので、本人確認を適正に実施する手順も忘れてはならない。

i) 教育に関する規定

事業者は、PMS に関して周知・徹底を図るだけでなく、従業者に、PMS を適切に運用する力量を身に付けさせなければならない。規定すべき内容は、下記の事項が考えられる。

- 目的
- 時期、期間、対象（従業者すべてを含む。）
- 内容、方法、場所
- 体制（担当者）
- 通知手続き
- 受講者管理の方法（出欠確認や補習実施）
- 教育効果の確認方法
- 実施記録の内容、保管方法等

j) 個人情報保護マネジメントシステム文書の管理に関する規定

PMS の内容を規定した文書、運用によって発生した記録類を適正に管理するための手続きを規定する。少なくとも、個人情報保護方針、内部規程、計画書及び記録は、PMS を構成する文書として管理しなければならない。PMS の運用が開始されると、さまざまなタイミングで実施記録を確保しておくことが、監査のための証拠を確保する意味から必要となる。文書管理の手順については、既存の規定があるのであれば、それを準用すればよい。

k) 苦情及び相談への対応に関する規定

事業者は、本人からの苦情及び相談に対しては、迅速に対応しなければならない。開示等の求めへの対応と同じく、初期の段階で的確に対応しなかったことが事案をこじらせる原因となるので、そのことを考慮した規定とすべきである。なお、本人からの苦情は、不適合を発見する端緒となる場合もあるし、それに至らなくとも、PMS の見直しにあたっての貴重な意見となる場合もある。したがって、その重要度に応じ、代表者に報告することを定めている必要がある。

l) 点検に関する規定

点検には、運用の確認と監査が含まれる。

運用の確認とは、各部門及び各階層において、日常的に個人情報の取扱い状況について確認を実施し、その結果、ルールに不適合な事項、是正・改善の必要のある事項について対処する活動である。

また、ステップ 7 により把握した残存リスクが顕在化していないかを確認するといったことも含まれる。不適合の早期発見につながるような運用を考えて規定を作成するとよい。

監査は、PMS の整備状況、PMS に基づく体制整備状況、運用状況及び是正・改善や見直しの結果 PMS 文書に JIS との不整合が発生していないかについて、定期的かつ必要に応じて随時点検し評価する。規定すべき内容は、下記の事項が考えられる。

- 目的
- 対象、時期（期間）
- 実施体制
- 監査担当者の責務と権限、倫理、守秘義務
- 計画（基本計画、個別計画、事業者の代表者による計画の承認）
- 被監査部門への通知手続き
- 実施の手続き
- 監査報告書（提出先、報告会）

・フォローアップ
・監査記録の方法、内容、保管等

なお、各年度の監査は原則として事業者の全ての部門を対象とするように計画して実施すべきであるが、大規模な事業者等部門の数が多い場合には、複数年度にまたがって実施することも可能である。その場合でも、必要に応じて不定期な監査を実施する配慮が求められる。

m) 是正処置及び予防処置に関する規定

不適合は、外部機関の指摘、緊急事態の発生、点検（運用の確認及び監査）の結果、外部からの苦情等により発見される。それらの不適合に対しての是正処置及び予防処置手順を定める必要がある。是正処置は発生した不具合に対処することであるが、予防処置は不適合の発生した事項を踏まえ、類似の不適合が他の個所等にも発生する可能性はないかを確認し、必要に応じて事前に予防的に措置することである。是正処置及び予防処置に関しては、再発を防止するよう以下の手順を含めて規定しなければならない。

・不適合の内容を確認する
・不適合の原因を特定し、是正処置及び予防処置を立案する
・期限を定め、立案された処置を実施する
・実施された是正処置及び予防処置の結果を記録する
・実施された是正処置及び予防処置の有効性をレビューする

n) 代表者による見直しに関する規定

発見された不適合を改善することのみが、代表者による見直しではない。PMS をより良いものにしていくために、場合によっては、現在の PMS のフレームワークを根本的に見直す作業が必要になる。したがって、そのための手順を定めておくことが必要である。

見直しにあたっては、以下の事項が考慮されなければならない。

・監査及び PMS の運用状況に関する報告
・苦情を含む外部からの意見
・前回の見直しの結果に対するフォローアップ
・個人情報の取扱いに関する法令、国の定める指針その他の規範の改正状況
・社会情勢の変化、国民の認識の変化、技術の進歩などの諸環境の変化
・事業者の事業領域の変化
・内外から寄せられた改善のための提案

o) 内部規程の違反に関する罰則の規定

個人情報の取扱いについて、PMS の定めに違反した場合の措置を規定する。実際の罰

則規定は、就業規則等に既に定められているものを適用することでもよいが、その場合には、本規定の中で適用する規則等を明示する必要がある。

ステップ 10：PMS を周知するための教育を実施する

教育に関する規定に定めた手順に従い、研修担当者が教育を実施する。研修担当者は、研修計画に基づき、PMS 策定チームの協力を得て研修を実施する。研修後は研修効果の確認を行うとともに研修記録を残し、次回以降の研修に反映する資料とする必要がある。

ステップ 11 ：PMS の運用を開始する

計画が立てられ、実施手順が定められ、必要な資源が用意され、担当者の責任・権限が定められかつその責任・権限に見合う力量を備えさせた段階で、初めて PMS の運用が可能になる。

ステップ 12 ：PMS の運用状況を点検し改善する

監査責任者は、PMS 運用開始後一定期間を経過した時点で、個人情報保護の状況について点検し評価する。ここでの監査は、PMS 運用開始後に効果的な運用ができる体制及び PMS となっているかについて確認するために実施するものであるから、事業者の全ての部門を対象とする必要がある。監査責任者は、評価の結果を監査報告書に取りまとめ、事業者の代表者に報告する。

PMS 策定チームは、監査の結果を受けて代表者から出された見直し指示に従い、PMS の改善を実施する。必要な改善措置の後、PMS 文書に改善内容を反映し、また、改善の内容、改善日を改善履歴として記録する必要がある。

ステップ 13 ：PMS の見直しを実施する

代表者による見直しに関する規定に定められた手順に従い、現状の PMS で適切であるかを検討し、必要に応じて改善を実施する。

プライバシーマークの認定申請においては、申請時にこのステップ 13 まで実施していることが必要である。

第二部
JIS Q 15001 各要求事項についての
プライバシーマーク付与適格性審査の基準

第二部「JISQ15001 各要求事項についてのプライバシーマーク付与適格性審査の基準」は、JIS Q 15001:2006 の要求事項ごとの審査の項目と各々の審査での着眼点を挙げている。
事業者各位においては，個人情報保護マネジメントシステムの構築にあたっても、これら留意点を参考として役立てていただきたい。

目　　次

注 1. 第二部は、規格本体に付属する解説と重複する記述は省いている。規格本体付属の解説と併せて読むことが望ましい。

注 2. 第二部で使用している略語は以下のとおりである。

① 個人情報保護法 :「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）

② 施行令 :「個人情報の保護に関する法律施行令」（平成 15 年 12 月 10 日政令第 507 号、平成 20 年 5 月 1 日一部改正）

③ 経済産業分野ガイドライン :「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」（厚生労働省・経済産業省告示第 1 号 平成 16 年 10 月制定、以後原則として毎年改定）

④ 管理者 : 個人情報保護管理者

⑤ 監査責任者 : 個人情報保護監査責任者

⑥ JIS : JIS Q 15001：2006

⑦ PMS : 個人情報保護マネジメントシステム

注 3. 規格本文のウェブサイトでの転載･公表は著作権者の許諾が得られない。したがって、対応する項番と項目名のみを記載している。

第二部の記述の見方

※第二部では、JIS Q 15001:2006 の各項目番号ごとに、以下に例示するような解説が付与されている。

1 適用範囲

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

この要求事項についての簡単な説明を記述する。

1 概要

この規格の適用範囲を定めたものである。ここで重要なことは「事業の用に供している」個人情報が対象となることである。事業の用に供している個人情報とは、経済産業分野ガイドラインや規格本体の解説にもあるように、必ずしも営利事業のみを対象としない。

この要求事項全体について注意すべき事項を補足して記述する。プライバシーマークの審査での注意事項も含む。

2 注意事項

従業者の個人情報は事業の用に供する個人情報であるから、実質的には全ての事業者がこの規格の対象となる。

個人情報と認識せず当該情報を預かっている事業者は、当該情報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言える。ただし、これらの事業者に対する一般消費者及び取引先の期待を考慮すれば、これらの事業者であっても、それらの情報を個人情報として特定する必要はないが、事業の用に供する個人情報と同等に位置づけ、リスクの認識、分析及び対策を実施することが当然望ましい。プライバシーマーク付与を受けようとする事業者の場合は必要である。

個人情報保護法と対応している要求事項については、該当する条項について記述する。

3 個人情報保護法との対応

①個人情報保護法第 2 条第 3 項（「個人情報取扱事業者」の定義）
②施行令第 2 条（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）※ただし施行令第 2 条は本規格では適用なし。

プライバシーマークの審査での「文書審査の項目」、「現地審査の項目」及び「審査の着眼点」を表形式で記述する。

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 全従業者を適用対象に定めていること。	(1) 全従業者を適用対象にしていること。	【文書審査】 ① 全従業者を適用対象とする旨を記述していること。 ※1 「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**、**3.4.3.3** 及び **3.4.5** で用いている「従業者」についても同じ。）。 【現地審査】 ① この運用が適切かどうかは、教育（**3.4.5**）、監査（**3.7.2**）の実施状況で判断される。 運用確認のためのエビデンス ・管理者の承認を得ていることが確認できる記録 ・個人情報を管理する台帳等

各審査項目における注意事項を記述する。

「....こと。」と書いてある事項は、実施していない場合、原則としてプライバシーマークの審査では不適合である。

審査員が運用状況を確認するために有用な記録類を、参考のために例示する。そこに記述されているものに限られるわけではない。また、この項目が記述されている場合だけエビデンスを確認するという意味ではない。

1 適用範囲

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

この規格の適用範囲を定めたものである。ここで重要なことは「事業の用に供している」個人情報が対象となることである。事業の用に供している個人情報とは、経済産業分野ガイドラインや規格本体の解説にもあるように、必ずしも営利事業のみを対象としない。

2 注意事項

従業者の個人情報は事業の用に供する個人情報であるから、実質的には全ての事業者がこの規格の対象となる。個人情報保護法でいう「個人情報取扱事業者」に該当するかどうかは関係ない。

個人情報と認識せず当該情報を預かっている（例えば、倉庫業、データハウジング、廃棄業など）事業者は、当該情報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言える。ただし、これらの事業者に対する一般消費者及び取引先の期待を考慮すれば、個人情報として認識している場合と同等に保護することが望ましい。したがって、プライバシーマーク制度としては、これらの事業者がプライバシーマーク付与を受けようとする場合、それらの情報を個人情報として特定することは求めないが、事業の用に供する個人情報と同等に位置付けて、リスクの認識、分析及び対策を実施することを求める。

3 個人情報保護法との対応

①個人情報保護法第 2 条第 3 項（「個人情報取扱事業者」の定義）

②施行令第 2 条（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）※ただし施行令第 2 条は本規格では適用なし。

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 全従業者を適用対象として定めていること。	(1) 全従業者を適用対象にしていること。	【文書審査】 ①全従業者を適用対象とする旨を記述していること。 ※1 「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、JIS の **3.2**、**3.3.4**、**3.4.3.3** 及び **3.4.5** で用いている「従業者」についても同じ。）。 ※2 出向社員は、出向元の事業者及び出向先の事業者の双方にとって従業者である。

文書審査の項目	現地審査の項目	審査の着眼点
		※3 派遣社員は、派遣事業者及び派遣先事業者の双方にとって従業者である。 ※4 一般派遣業の場合、登録しているだけの者については、雇用契約関係が発生していないため、従業者ではない。 【現地審査】 ① 全従業者を適用対象としていること。この項目についての運用が適切かどうかは、教育（**3.4.5**）、監査（**3.7.2**）の実施状況で審査される。 ※ 監査役は事業者の構成員であるから、事業者が定めたルールを守る必要がある。その意味で従業者に含まれる。ただし、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。したがって、監査役が教育(**3.4.5**)や監査(**3.7.2**)を受けていなくても不適合ではない。
2. 事業の用に供している個人情報を適用対象とするよう定めていること。	(1) 事業の用に供している個人情報を適用対象としていること。	【文書審査】 ①「事業の用に供している」個人情報を対象とすることが読み取れること。必ずしも同一の表現である必要はないが、適用対象が限定的と読み取れることは望ましくない。 【現地審査】 ① 事業の用に供している個人情報を適用対象としていること。ただし**2 注意事項**を参照。この項目についての運用が適切かどうかは、個人情報の特定（**3.3.1**）の実施状況の審査で判断される。

2 用語及び定義

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

JIS の中で使用する用語及び定義について規定している。JIS に合わせて内部規程の用語を統一する必要はない。大切なことは、JIS の要求事項に実態が適合していることであって、事業者内で使う用語が JIS と異なっていても全く関係ない。

2 注意事項

個人情報の定義が個人情報保護法とは異なることに注意する必要がある。個人情報保護法では原則として生存する個人に関する情報であり、例外的に死者の情報を含む。一方、この規格では、原則として死者の情報も個人情報であるが、歴史上の人物までは含まない。

個人情報保護法と定義が異なる理由は、事業者の実務に配慮したからである。事業者は個人情報保護法の義務のみに従えばよいのではなく、業法や契約法など、種々の規制の下にある。例えば、契約により取得している個人情報について、その一方の当事者が死亡したからといって、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してよいものではなかろう。民事責任を負わないようにするためのリスク管理も必要である。個人情報保護法という一つの法律だけを守っていればよいといったマネジメントシステムの構築は適切ではない。したがって、JIS の定義では死者の情報も含むものとなっている。

「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事業者であれば全て該当する。なお、プライバシーマーク付与は、従業者二人以上から対象となる（従業者には役員を含む）。従業者一人の事業者を対象としないのは、個人情報保護管理者と個人情報保護監査責任者を同一人物が兼務する場合、チェック機能が有効に働くと評価できないからである。

3 個人情報保護法との対応

① 個人情報保護法第 2 条第 1 項～第 6 項（定義）
② 施行令第 1 条（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）
③ 施行令第 2 条（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）※ただし施行令第 2 条は JIS では適用なし。

4 審査の項目とその着眼点

定義どおり理解しているかどうかは、個人情報保護マネジメントシステムの運用の全体において審査される。

3 個人情報保護マネジメントシステム要求事項

3.1 一般要求事項

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報保護マネジメントシステムを確立し，実施し，維持し，かつ，改善しなければならない旨を規定している。つまり、**PDCA** サイクルによりマネジメントシステムを適切に運用することを求めており、そのための要求事項を箇条 **3** に記述していることを明らかにしている。

2 注意事項

特になし。

3 個人情報保護法との対応

特になし。

4 審査の項目とその着眼点

この要求事項が実施されているかどうかは、箇条 **3** の実施状況の審査によって判断される。

3.2 個人情報保護方針

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

事業者における個人情報保護に関する取組みを文書化し、内外に宣言するよう求めている。何のために個人情報保護活動を行うのか（「個人情報保護の理念」）、個人情報保護のためにどのようなことを行うのか［**a**)～**e**)］、及び **f**) を記述しなければならない。☞第一部４.ステップ１及びステップ４。

2 注意事項

a)～**e**)の事項をこのとおりの順番に分けて書く必要はない。記載内容に **a**)～**e**)の事項が含まれていればよい。

公開している個人情報保護方針と規定文書の個人情報保護方針に不整合があれば、不適合となる。

3 個人情報保護法等との対応

①「個人情報の保護に関する基本方針」（平成16年4月2日閣議決定）

6 (1)①事業者が行う措置の対外的明確化

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 個人情報保護の理念を明確にしていること。	(1) 内容が適切であること。	【文書審査】 ① 個人情報保護に取り組む姿勢や基本的考え方を、事業の内容と絡めて記述していること。 ※ 「個人情報保護の理念」とは、何のために個人情報保護活動を行うかであり、それは当然事業内容に絡むはずである。例えば「○○事業を行うために、△△に努める」という関係があるであろう。
2. **a**)について記述していること。	(1) 内容が適切であること。	【文書審査】 ① 個人情報保護方針の文面に、目的外利用を行わない旨を記述していること。 ② 目的外利用を行わないための措置を講じる旨を記述していること。 ※ 「事業の内容及び規模を考慮した」とは、事業者に考慮することを求めているのであって、個人情報保護方針の文面にこのとおり記述することを要求しているのではない。
3. **b**)について記述していること。	(1) 内容が適切であること。	【文書審査】 ① 個人情報保護方針の文面に、「個人情報保護に関する法令、国が定める指針その他の規範を遵守する」主旨の記述があること。

文書審査の項目	現地審査の項目	審査の着眼点
4. **c)**について記述していること。	(1) 内容が適切であること。	【文書審査】 ① 安全管理措置を講じることを宣言する項である。安全管理措置の面で、個人情報の漏えい，滅失又はき損を防止し是正を行う旨を記述していること。 ※ この項に、目的外利用を含めて「防止及び是正」する旨を記述している場合は不適合である。なぜなら、目的外利用はしてはならないことであり、安全管理措置における是正と同列に論じることはできないからである。
5. **d)**について記述していること。	(1) 内容が適切であること。	【文書審査】 ① 個人情報保護方針の文面に、苦情や相談に対して対応する旨を記述していること。
6. **e)**について記述していること。	(1) 内容が適切であること。	【文書審査】 ① 個人情報保護方針の文面に、個人情報保護マネジメントシステムを継続的に見直し改善する旨を記述していること。
7. **f**）を表示していること。	(1) 内容が適切であること。	【文書審査】 ① 個人情報保護方針の文面に代表者の氏名を表示していること。 【現地審査】 ① 代表権を持つ者を代表者として表示していること。 ※ 代表者とは代表権を持つ者として登記されている者をいう。表見代表取締役は認められない。 運用確認のためのエビデンス ・公開している個人情報保護方針 ・登記事項証明書等
8. 制定日を表示していること。	(1) 公開（ウェブサイトなど）又は頒布している個人情報保護方針に、制定年月日（及び最終改訂年月日）を明示していること。	【文書審査】 ① 個人情報保護方針の文面に制定日、改訂日を表示していること。 ※1 個人情報保護方針は、文書の範囲（**3.5.1**）に含まれており、文書管理（**3.5.2**）の対象として、文書の発行及び改訂に関することを明示することが要求されているため、制定年月日や改訂年月日を明らかにする必要がある。 ※2 代表者名のみの変更を改訂に含めることは要求しない。 運用確認のためのエビデンス ・公開している個人情報保護方針

文書審査の項目	現地審査の項目	審査の着眼点
9. 従業者及び一般の人が入手可能な措置を講じるよう規定していること。	(1) 従業者及び一般の人が入手可能な措置を講じていること。	【文書審査】 ① 従業者及び一般の人が入手できるための手段を、具体的に定めていること。 【現地審査】 ① 従業者及び一般の人が入手できるための具体的な手段を整えていること。 ※1 従業者が入手可能な措置としては、イントラネットでの掲示、規程集の配布、社内の掲示等が考えられる。 ※2 一般の人が入手可能な措置としては、ウェブサイトに掲示することが考えられる。ウェブサイトがない場合、事業者の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、問合せに対しては要望に応じてすぐ送付する体制を整えておく等の措置が想定できる。従業者しか閲覧できないような社内掲示のみでは不適合になるので注意が必要である。 運用確認のためのエビデンス ・一般の人が入手可能な措置 ・従業者が入手可能な措置
	(2) ウェブサイトに掲載している場合、トップページにリンクがあること。	【現地審査】 ① 分かりやすく目に付きやすい場所にリンクを表示していること。 ※ トップページでなければ不適合ということではない。トップページには事業者イメージのみ表示している場合等は、少なくとも次の階層のページに個人情報保護方針へのリンクを配するなど、「分かりやすく目に付きやすい」よう配慮している必要がある。 運用確認のためのエビデンス ・ウェブサイトのトップページ
	(3) 公表している個人情報保護方針に、個人情報保護方針に関する問合せ先を明示していること。	【現地審査】 ① 問合せ先を明示していること。 ※1 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、当該方針の内容に関して一般の人からの質問に答えられるよう、問合せ先を明示している必要がある。 ※2 個人情報の取扱い一般に関する問合せ先と兼ねても良い。

文書審査の項目	現地審査の項目	審査の着眼点
		※3 ウェブサイトでは、問合せ先を一つのページにまとめ、リンクを明示している形態でも可である。 運用確認のためのエビデンス ・公開している個人情報保護方針
	(4) 公開している個人情報保護方針と規定文書の個人情報保護方針は同一であること。	【現地審査】 ① 公開している個人情報保護方針と規定文書としての個人情報保護方針が同一であること。 ※ 公表している問合せ先を、規定文書としての個人情報保護方針の一部として認識する必要はない。 運用確認のためのエビデンス ・公開している個人情報保護方針 ・規定文書としての個人情報保護方針

3.3 計画

3.3.1 個人情報の特定

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

事業の用に供しているすべての個人情報を漏れなく把握できる手順を確立し、維持することを求めている。

☞第一部４．ステップ５

特定した個人情報については、リスクを管理するという目的が果たせるように、その取扱状況が把握できるような手段を整備する必要があり、そのために作成するのが個人情報を管理するための台帳である。

個人情報を管理する台帳等は紙媒体である必要はなく、電子ファイル形式等、事業者にとって最も管理しやすい手段を利用すればよい。

2 注意事項

個人情報を特定することと個人情報を台帳管理することとは別であって、特定した個人情報すべてを台帳管理する必要はない。

例えば、「○○社の××さんから電話がありました」という伝言メモ、仕事で使っている手帳に記入した「○○さんとの打合せ」予定、ホワイトボードに書いた「○○さんのところに外出」といったものも、事業の用に供する個人情報かと問われればそのとおりであるが、そういったものまで台帳管理できるものではない。こういったものは、リスク対策としてのルールは必要であるにしても、取扱いは個々の従業者にゆだねるのが適切であろう。

また、事業者内には、守らなければならない大事な情報が多く存在し、個人情報はそのうちの一つに過ぎない。事業者の情報管理ルールの一環として、個人情報の取扱いに関するルールも存在するというのが本来のあり方である。

もし個人情報の取扱いに関するルールとは別に、すでに確立されたルール（例えば決裁書の管理に関する規程、契約書の管理に関する規程、経理規程など）があり、そのルールが個人情報の取扱いに関するルールと何ら矛盾することがないのであれば、それに従って取り扱っていればそれで良いのであって、個人情報だからといって、台帳で一括管理しなければならないものではない。

台帳管理することは、手段であって目的ではない。何を台帳管理の対象とするかもリスク対策の一つである。

なお、監視ビデオや電話音声の録音、業務の中で二次的に作成する管理資料（データベース等）、マネジメントシステムの運用において発生する記録類（同意書、誓約書、教育理解度把握のためのテスト、アンケート等）、バックアップなどは特定から漏れる例が多いので注意が必要である。

3 個人情報保護法との対応

① 個人情報保護法第２条第３項（「個人情報取扱事業者」の定義）

② 施行令第２条（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）※ただし施行令第２条は本規格では適用せず。

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 全ての個人情報を特定する手順が明確であること。	(1) 定めた手順に従い、個人情報を特定していること。	【文書審査】 ① 個人情報を特定する者を定めていること。 ② 個人情報を特定する方法を定めていること。これには、個人情報を特定するために使用する台帳等の様式を定めていることを含む。 ③ 個人情報保護マネジメントシステムの構築時や新規の種類の個人情報の取扱いが発生したとき等、個人情報を特定する作業が必要になるタイミングを明確にしていること。 【現地審査】 ① 定めた手順に従い、個人情報を特定していること。 ② 個人情報の特定に漏れがないこと。 運用確認のためのエビデンス ・個人情報を管理する台帳等
	(2) 管理者の承認を得ていること。	【文書審査】 ① 特定した個人情報について管理者の承認を得る手順を定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・個人情報を管理する台帳等

文書審査の項目	現地審査の項目	審査の着眼点
	(3) 個人情報を特定した台帳等を作成していること。	【文書審査】 ① 個人情報を管理する台帳等の作成手順を記述していること。 【現地審査】 ① 主要な個人情報を台帳に登録していること。 ② 台帳等は一覧形式である必要はないが、管理対象としての個人情報を全て把握できるものであること。 ③ 台帳等には、少なくとも以下の項目が含まれていること。 － 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 － 件数 ※ 件数は概数でよい。台帳管理の主旨は、1件残らず漏れなく管理していることの証明ではなく、組織内での個人情報の取扱状況を把握することにある。 運用確認のためのエビデンス ・個人情報を管理する台帳等
2. 個人情報を管理する台帳等の更新及び定期的な見直しに関する手順を定めていること。	(1) 定めた手順に従い、個人情報を管理する台帳等の更新及び定期的な見直しを実施していること。	【文書審査】 ① 個人情報の取扱いが変更、終了したときに台帳等を更新する手順を定めていること。 ② 具体的な時期を定めて定期的に台帳等を見直す手順を定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。特に新たに発生した個人情報、取扱いが変更・終了になった個人情報は、適時、台帳等に反映していること。 ※ 台帳の更新、定期的な見直し時期に合わせ、個人情報の棚卸しを必要とする場合がある。 運用確認のためのエビデンス ・個人情報を管理する台帳等

3.3.2 法令，国が定める指針その他の規範

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

法令、国が定める指針その他の規範に、個人情報の取扱いについて特別の定めがある場合、そちらが優先する。事業者は、**3.2** の **b)**で宣言したように、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しなければならない。したがって、事業者の自らの業務に関連のある範囲で、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の制定・改廃状況に注意し、常に最新版を維持・参照する手順を定め、それを実施している必要がある。☞第一部 4.　ステップ 6

2 注意事項

事業者は、自らの業務に関連のある範囲で、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特定し、それを遵守することが求められている。JIS は個人情報の取扱いに関する個々の法令等への違反について規定しているわけではないが、もし過失によりそれら法令等に違反した事業者は、必要な法令等が特定されていなかった、あるいは特定していても適切に管理されていなかったということになり、この要求事項に反して不適合ということになる。

なお、事業者が従うべき規範は法令関係だけではない。「その他の規範」には、業界ガイドラインや顧客の要求なども含まれる。

3 審査の項目と着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 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特定し、参照し、維持する手順を定めていること。	(1) 参照すべき法令、国が定める指針その他の規範を、定めた手順に従い、特定していること。	【文書審査】 ①　法令等を特定する手順を定めていること。 【現地審査】 ①　定めた手順に従い、実施していること。 運用確認のためのエビデンス ・特定された法令等が明確になっていることを確認できる記録
	(2) 特定した法令、国が定める指針その他の規範について、管理者の承認を得ていること。	【文書審査】 ① 特定した法令、国が定める指針その他の規範について管理者の承認を得る手順を定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・特定した法令、国が定める指針その他の規範について管理者の承認を確認できる記録
	(3) 参照すべき法令、国が定める指針その他の規範を、必要に応じて更新していること。	【文書審査】 ① 参照すべき法令、国が定める指針その他の規範を更新する手順を記述していること。 ※ 情報を収集する担当者を定め、特定した法令等の制定改廃状況を、随時及び具体的な時期を定めて定期的に見直しを行うことが考えられる。 【現地審査】 ① 定めた手順に従い、必要に応じて、参照すべき法令、国が定める指針その他の規範を更新し、最新版を参照するよう管理していること。 運用確認のためのエビデンス ・参照すべき法令等を特定した記録の更新履歴
	(4) 特定している法令、国が定める指針その他の規範が適切であること。	【現地審査】 ① 事業者によって参照すべき法令等は異なる。事業者は、必要に応じて業界の関連法令やガイドライン等を特定していること。 なお、以下の 1)～6)は必須とする。 1)「個人情報の保護に関する法律」（平成 15 年 5 月、改正有） 2)「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」（厚生労働省・経済産業省、平成 16 年 10 月制定、改正有） 3)「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」（厚生労働省、平成 16 年 7 月制定、改正有） 4)「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項」（厚生労働省、平成 16 年 10 月制定、改正有） 5)「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成 25 年 5 月、改正有） 6)「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（特定個人情報保護委員会、平成 26 年 12 月制定、改正有） 運用確認のためのエビデンス ・特定された法令等が明確になっていることを確認できる記録

文書審査の項目	現地審査の項目	審査の着眼点
	(5) 特定している法令、国が定める指針その他の規範が、必要に応じて参照できること。	【文書審査】 ① 特定した法令等を組織内で参照する方法を定めていること。 【現地審査】 ① 法令等をそのまま内部規程の一部として位置づけるような文書体系をとっている場合、従業者全員が法令等を参照できるようにしていること。 ② 法令等が改訂されたとき、その内容を内部規程に反映するよう管理している場合は、内部規程を改定する立場の者が参照できるようになっていること。そのときは、法令等の改訂内容を、関連する文書にも確実に反映させていること。 運用確認のためのエビデンス ・社内での参照方法

3.3.3 リスクなどの認識，分析及び対策

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

3.3.1 により保護の対象としたものについて、想定される全てのリスクを管理することを求めている。リスクを漏れなく洗い出すためには、個人情報の取得から廃棄・消去までの取扱いの一連の流れ（いわゆる個人情報のライフサイクル）の全ての局面ごとに検討する必要がある。大変な作業であるが、この作業により、自社内での個人情報の取扱状況が明確になり、業務管理もやり易くなるはずである。

☞第一部 4.ステップ 7

2 注意事項

3.3.3 でいう対策には、**3.4.2.1**～**3.4.2.8** の要求事項に違反しないことも含まれるが、それらはそれぞれの要求事項において個別に審査されるため、ここでは安全管理措置面についての注意事項を述べる。

すべてのリスクについて可能な対策をすべて講じることができれば理想であるが、リスク対策を実施すべきであっても、対策ができない又は対策が不十分とならざるを得ない場合がある。対策が実施できない理由としては、経費面での制約、人的制約、技術的制約などがあり得るであろう。また、部門ごとの部分最適の対策の集合は必ずしも組織にとっての全体最適とはならず、業務効率が犠牲となることを避けるために、特定のリスクについては厳密な対策を取りえないといったこともあるであろう。

そのような場合は、現状で取り得る対策を講じた上で、当面必要と考えられる未対応部分を残存リスクとして把握し管理することが必要である（事業者にとって対策不可能なことまで残存リスクとして把握し管理する必要はない）。なお、残存リスクを管理（例えば、「個人情報リスク管理表」に記載）する目的の一つは、関係者が意識を共有し注意することにある。残存リスクは、運用の確認（**3.7.1**）の対象として認識し、日常的に点検するなどの措置が必要になるであろう。

なお、ISMS（ISO/IEC 27001）で採用している手法を利用してもよいが、その場合でも、個人情報のライクサイクルに沿ってリスクを認識し、分析し、対策を講じ、残存リスクを把握していることが必要である。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 目的外利用を行わないため、必要な対策を講じる手順を確立し，かつ，維持するよう規定していること。	(1) 目的外利用を行わないための手順を実施していること。	この項についての審査は、利用目的の特定(**3.4.2.1**)及び利用に関する措置(**3.4.2.6**)で行う。
2. 洗い出された個人情報について､ライフサイクルに応じてリスクを洗い出し､リスク分析を実施し、リスクに応じた対策を講じ、残存リスクを把握する手順が明確であること。	(1) 定めた手順に従って、リスクを認識し、分析し、対策を講じていること。	【文書審査】 ① リスクの認識、分析及び対策を確実に実施できるよう、手順を明確に記述していること。 手順には、以下の４点を明確に記述していること。 1) **3.3.1** により特定した個人情報のリスクをライフサイクルごとに洗い出すこと。 2) リスク分析を実施すること。 3) リスク分析に基づいて対策を講じること。 4) 残存リスクを把握すること。 【現地審査】 ① 定めた手順に従い実施していること。 運用確認のためのエビデンス ・リスク分析表等、リスクの認識、分析及び対策を実施した記録
	(2) 個人情報ごとにライフサイクルに沿って(ライフサイクルが同じものはグルーピング可)リスクを認識し、分析し、対策を講じ､残存リスクを把握していること。	【現地審査】 ① 個人情報を取り扱う業務の流れが明らかになっており、取扱いの局面におけるリスクを具体的に認識していること。 ② 立案した安全対策や把握した残存リスクをリスク分析表等に反映させ、かつ運用面で確認できること。 ③ 認識したリスクと対策との関連付けが明確であること。明確でなければ見直しができない。 ④ 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。単に情報資産を守るという観点からのみのリスクの認識、分析及び対策となっていないこと。

文書審査の項目	現地審査の項目	審査の着眼点
		⑤　個人情報の漏えい、滅失、毀損のほかに法令・国が定める指針等に対する違反なども必要に応じてリスクとして認識していること。 ※1 リスクの数値評価は必要でない。ただし、数値評価によるリスクの把握も一つの手法であり、これを否定するものではない。 ※2 現状で取り得る対策を講じた上で、当面必要と考えられる未対応部分を残存リスクとして把握し管理することが必要である。 運用確認のためのエビデンス ・リスクの認識、分析及び対策を実施した記録
	(3)リスク対策は事業者の代表者の承認を得て決定していること。	【文書審査】 ①　講じることとしたリスク対策について、事業者の代表者（又は代表者としての権限を委任されている者）の承認を得て決定する手順を定めていること。 ※ どこまで対策を講じるかは、費用対効果等を総合的に勘案し、事業者の代表者が経営判断として決定する事項であり、担当者レベルで決める問題ではない。ただし現場の判断に任せる範囲の対策もあろう。**3.3.4** の**2注意事項**を参照。 【現地審査】 ① 定めた手順に従い、実施していること。
	(4) 講じることとした対策は、規定に反映させていること。	【現地審査】 ①　講じることとした対策は規定化していること。 ※ 規定化しないこともリスクの一つである。なお、規定化は条文形式でなくてもよい。例えば実施すべきリスク対策をまとめたもの（リスク対策表等）について、遵守しなければならないものとして従業者に認識させているのであれば、規定化していると言える。**3.3.5** の**2注意事項**を参照。 運用確認のためのエビデンス ・リスク分析表等、リスクの認識、分析及び対策を実施した記録と規定との対応

文書審査の項目	現地審査の項目	審査の着眼点
3. 定期的な見直し、及び必要に応じた随時の見直しの手順が明確であること。	(1) 定めた手順に従い、リスクの見直しを実施していること。	【文書審査】 ① 具体的な時期を定めた定期的な、または必要に応じた随時の見直しを確実に実施するよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い実施していること。 ② リスクの見直しを定期的及び随時実施していること。 ※1 リスク分析表等を単に形式的に見直すのではなく、認識されたリスク、対策、残存リスクが適切であることを確認しているかが重要である。例えば、プライバシーマーク付与適格性審査の申請後、事務所を移転しているケースがあるが、これも環境の変化の一つであり、リスクの見直しが臨時に実施されていない場合、現地審査において不適合となる。 ※2 個人情報の取扱いに関する事故を起こした事業者においては、リスクの見直しを実施していることは必須であり、現地審査のときに確認する。 <u>運用確認のためのエビデンス</u> ・リスク分析表等、リスクの認識、分析及び対策を実施した記録及びその更新履歴

3.3.4 資源，役割，責任及び権限

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報保護マネジメントシステムを実施するための体制整備を求めている。☞第一部 4.ステップ 8

この規格上、少なくとも以下に挙げる担当者は必要であろう。名称はこれに合わせる必要はない。

－個人情報保護管理者

－個人情報保護監査責任者

－教育担当者

－監査員

－問合せ担当者

－苦情及び相談担当者

－開示等の担当者

この他にも、組織の実態に合わせて部門別担当者などを定めると良いであろう。これら担当者の兼務は認められるが、個人情報保護管理者は、個人情報保護監査責任者を兼務できない。また、小規模事業者で体制上やむを得ない場合を除き、個人情報保護管理者は、監査員についても兼務できない。

2 注意事項

個人情報保護マネジメントシステムの実施は業務執行の一場面であり、かつ継続的な活動である。したがって、会社法上の監査役が体制の一部を占める場合、継続的に代表者の監督下に入ることになるため、会社法第 335 条違反になると考えられる（この趣旨は、委員会設置会社における監査委員、非公開会社における会計参与も同様であり、それぞれ会社法第 400 条第 4 項、同第 333 条第 3 項第 1 号に監査役の場合と同じ趣旨の制限規定がある。なお、会計参与は同第 324 条により役員に含まれているため従業者である。）。ただし、だからといって監査役はこのマネジメントシステムの実施に関与してはならないというのではない。このマネジメントシステムが個人情報保護法の遵守を内容として含んでいることを考慮すれば、監査役に取締役会への出席・意見陳述義務があるのと同様、例えば、個人情報保護に関する社内の委員会や、監査報告会、代表者による見直し会議等が開催される時に、監査役が出席し意見を述べることは、業務監査（適法性監査）という観点からはむしろ望ましいと言える。

もし社外取締役を体制の一部に任命した場合、その取締役は当該事業者の業務執行者の一人となり、社外取締役ではなくなる（つまり、社内の取締役が一人増えて、社外取締役が一人減る。）ことになる。

なお、本書において、事業者の代表者による承認又は管理者による承認を求めるよう記述している場面が多いが、以下のように組織内での権限委任を前提に記述している。JIS Q 15001 の場合だけ事業者内での通常の承認ルールから外れた特別の運用をするよう求めているのではない。

JIS でいう事業者の代表者、個人情報保護管理者又は個人情報保護監査責任者（以下、ここでは「代表者等」という。）の権限を誰が行使するかは事業者のコーポレートガバナンスの問題であって、つまるところ、代表者等としての決裁権限を誰に与えるかという話である。例えば、10 万円以下の物品の購入であれば部長決裁であるがそれ以上は役員決裁であるといったように、案件の軽重に従って事業

者内で決裁権限が分配されているのが通常であろう。

それと同様に、JIS でいう代表者等の権限についても、案件の軽重に従って、しかるべき者を決裁権限者とすることについて、適正な手続により社内規程として定めているのであれば、それは事業者のコーポレートガバナンスにかかわる事項であって、審査では問題とはならない（もっとも、実質的な経営判断が求められる事項については経営層が決裁権限をもたなければならず、権限の委任といってもそこには自ずと限界はあろう。）。ただし、個人情報保護管理者と個人情報保護監査責任者の権限が同一人物に帰するような権限委任は、マネジメントシステムの趣旨に反するため認められない。

プライバシーマークの審査の際には、代表者等としての決裁権限が与えられている旨が確認できる根拠（包括的な委任状や決裁権限表、内部規程で決裁権限を規定している該当箇所など）を示してもらえればよい。

なお、以上のことはあくまで事業者の内部的な運用に過ぎず、代表者については、対外的な文書を代表権のない者の名義で出すべきでないのは当然である。代表権のない者が個人情報保護方針の代表者の氏名として記載されるのは不適合であり、プライバシーマーク付与適格性審査の申請も代表権のある者の名義でなければ受け付けない。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 各担当者の役割・権限を明確に定め、文書化していること。	(1) 各担当者の役割、責任及び権限を明確に定めていること。	【文書審査】 ① 各担当者の役割・権限を明確に定め、文書化していること。 ② 体制整備状況（教育責任者、問合せ対応責任者、システム担当者、部門毎の個人情報管理者、委員会、事務局など）に応じて、各担当者の責任及び権限を明確にすること。 【現地審査】 ① 従業者にとって、各担当者の役割、責任及び権限が明確であること。 運用確認のためのエビデンス ・各担当者の役割、責任及び権限が確認できる文書 ・各担当者に任命している者を確認できる文書
	(2) 個人情報保護管理者と個人情報保護監査責任者が同一人物でないこと。	【現地審査】 ① 同一人物が個人情報保護管理者と個人情報保護監査責任者を兼任していないこと。両者兼任の場合、マネジメントシステムが機能しないため、不適合となる。 運用確認のためのエビデンス ・各担当者の役割、責任及び権限が確認できる文書 ・各担当者に任命している者を確認できる文書

文書審査の項目	現地審査の項目	審査の着眼点
	(3) 個人情報保護管理者は、代表者によって内部から指名していること。	【現地審査】 ① 個人情報保護管理者は、代表者により内部から指名していること。 運用確認のためのエビデンス ・各担当者の役割、責任及び権限が確認できる文書 ・各担当者に任命している者を確認できる文書
	(4) 個人情報保護監査責任者は、代表者により内部から指名していること。	【現地審査】 ① 個人情報保護監査責任者は、代表者により内部から指名していること。 運用確認のためのエビデンス ・各担当者の役割、責任及び権限が確認できる文書 ・各担当者に任命している者を確認できる文書
	(5) 会社法上の監査役が、体制の一部を占めていないこと。	【現地審査】 ① 会社法上の監査役が体制の一部を占めていないこと。 ※ 会社法上の監査役が体制の一部（例えば監査責任者）を占める場合、継続的に代表者の監督下に入ることになるため、会社法第 335 条違反になる。これはコーポレートガバナンス自体ができていないことになり、マネジメントシステム以前の問題であって不適合となり、注意が必要である。 運用確認のためのエビデンス ・各担当者の役割、責任及び権限が確認できる文書 ・各担当者に任命している者を確認できる文書 ・登記事項証明書
	(6) 各担当者の役割・権限を周知させていること。	【現地審査】 ① 各担当者の役割・権限を周知させていること。 ※ 体制図を作成する場合、誰を示すのか社内的に明確であれば、氏名を入れる必要はない（いたずらに個人情報を増やす必要はない）。 運用確認のためのエビデンス ・各担当者の役割、責任及び権限が確認できる文書 ・各担当者に任命している者を確認できる文書

文書審査の項目	現地審査の項目	審査の着眼点
2. 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の見直し及び改善の基礎として，事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならない旨を規定していること。	(1) 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の見直し及び改善の基礎として，事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告していること。	【文書審査】 ① 個人情報保護マネジメントシステムの見直し及び改善の基礎として，事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならない旨を個人情報保護管理者の義務として記述していること。 【現地審査】 ① 個人情報保護管理者が個人情報保護マネジメントシステムの見直し及び改善の基礎として、事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告していること。 ※ この項は事業者の代表者による見直し(**3.9**)において審査される。

3.3.5 内部規程

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

確立した手順を内部規程として文書化することを求めている。☞第一部 4.ステップ 9

2 注意事項

内部規程は、基本となる規程の下に、必要に応じ、細則、マニュアル、チェックリストなどを作成するとよい。

内部規程だからといって法律の条文の書き方をまねる必要もない。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、従業者が具体的に理解できるよう、様式の記入例、図、イラストなどを活用するのも一つの方法である。例えば、手順をフローチャートで図示し、それを内部規程と位置付けることも何ら制限されない。内部規程は紙媒体である必要はない。従業者にとって分かり易くメンテナンスもしやすい方法が、その事業者にとって最も良い方法である。

内部規程は、必ずしも形式的に一本化された規程でなくてもよい。例えば、内部規程の違反に関する罰則は、就業規則を準用することでもよい。

ここに列挙されている a)～o)の 15 の規程を作成することが求められているのではない。小規模事業者であれば一つの規程に全ての規定を盛込むことも可能であろう。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. a)～o)に該当する、具体的な手順書レベルの規定があること。	(1) 取締役会の決議を経るなど一定の手続を経て定めていること。	【文書審査】 ① 規格と同程度の抽象的な規定があるだけでは足りない。具体的な手順レベルの規定を作成していること。 【現地審査】 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ていること。 運用確認のためのエビデンス ・一定の手続きを経て定めたことを示す記録

文書審査の項目	現地審査の項目	審査の着眼点
	(2) **a**)～**o**)を含む規程を、従業者が参照できること。	【現地審査】 ① 従業者にとって、どこに何があるか分かり、容易に参照できる環境であること。 ※1 規程集として一冊になっている必要はない。また、紙媒体である必要もない。 ※2 規程は、従業者にとって必要な範囲で参照できるようにしてあれば良い。例えば、個人情報を取り扱う業務に携わらない者が、詳細な手順書レベルの規程を参照できる必要はない。 運用確認のためのエビデンス ・従業者が参照できる措置
2. 文書化した内部規程の維持について規定していること	(1)文書化した内部規程を維持していること。	※ この項は文書管理(**3.5.2**)において審査される。
3. 内部規程の改正について規定していること。	(1)必要に応じて内部規程を改正していること。	※ この項は文書管理(**3.5.2**)及び監査(**3.7.2**)において審査される。

3.3.6 計画書

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報保護マネジメントシステムの実施にあたって、必要な計画書の策定を求めている。計画書の作成には事業者の代表者による承認が必要である。

2 注意事項

3.3.6 では「...教育や監査などの計画...」と規定されており、教育計画と監査計画のみを対象として限定しているのではなく、例として挙げてあるに過ぎない。計画とは一般に目標を含むものであって、それは事業者の代表者が全社的な事情を考慮して行う経営判断の一つである。管理者は、事業者の代表者が個人情報保護のために決定した事項についての執行責任者であって、自ら計画を決定する立場ではない。したがって、計画は原則として事業者の代表者による承認が必要である。ただし、その承認権限を他の者に委任すること（例えば、教育計画書の承認権限を個人情報保護管理者に委任すること）は、事業者のコーポレートガバナンスの問題であって、適正手続により権限が委任されていれば問題はない（**3.3.4** の**2注意事項**を参照）。

事業者は、少なくとも、教育計画書と監査計画書は策定しなければならない。計画書は、実施可能な程度に具体的に記述されている必要がある。必要に応じて、年間計画や個別計画等を作成すれば良い。

なお、プライバシーマーク制度では、教育や監査については少なくとも年 1 回以上の実施を要求している。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 事業者の代表者の承認を受けて、教育計画書を作成するよう規定していること。	(1) 事業者の代表者の承認を受けて、教育計画書を作成していること。	【文書審査】 ① 教育計画書を確実に作成できるよう、手順を明確に記述していること。 ② 教育計画書を事業者の代表者（または代表者から権限を委任された者）が承認していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・教育計画書

文書審査の項目	現地審査の項目	審査の着眼点
	(2) 作成した教育計画書の内容が適切であること。	【現地審査】 ① 研修名、開催日時、場所、講師、受講対象者及び予定参加者数、研修の概要等、実施可能な程度に具体的に記述していること。 運用確認のためのエビデンス ・教育計画書
2. 事業者の代表者の承認を受けて、監査計画書を作成するよう規定していること。	(1) 事業者の代表者の承認を受けて、監査計画書を作成していること。	【文書審査】 ① 監査計画書を確実に作成できるよう、手順を明確に記述していること。 ② 監査計画書を事業者の代表者（または代表者から権限を委任された者）が承認していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・監査計画書
	(2) 作成された監査計画書の内容が適切であること。	【現地審査】 ① 監査テーマ、監査対象、目的、範囲、手続、スケジュール等、実施可能な程度に具体的に記述していること。 運用確認のためのエビデンス ・監査計画書

3.3.7 緊急事態への準備

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報が漏えい、滅失又はき損をした場合に、被害を最小限に抑えるための手順をあらかじめ定めておくことを求めている。損害を被るのはそのような事故を起こした事業者だけでなく、取引先、グループ企業、そしてその個人情報によって特定される本人である。事故が起きた場合にそれら利害関係者全体に及ぼす影響を最小限にすることが、個人情報を取り扱う事業者としての社会的責任である。

緊急事態が発生したからといって、常に **a)**～**c)**全ての措置の実施が要求されるわけではない。法令や国が定める指針その他の規範で義務付けられていることは実施する必要があるが、それ以外の場合は、経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、どういう場合にどのような措置を講じるか定めておく必要がある。 ☞第一部 4.ステップ 9 **e)**

2 注意事項

実際に事故がおきた場合に、必ずしも事前の想定どおりに進むものではなかろう。確実に対策が実施される仕組みとすることが有用である。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 緊急事態を特定するための手順，また，それらにどのように対応するかの手順を定めていること。	(1) 定めた手順に従い、緊急事態を特定し、対応していること。	【文書審査】 ① 緊急事態の特定及び対応が確実に実施できるよう、手順を明確に記述していること。 なお、「緊急事態を特定するための手順」として、以下が考慮されている必要がある 1) 各事業者において想定される「緊急事態」の定義 2) 従業者が 1) の「緊急事態」発生に気がついた場合に、事態の判断ができる管理者等への情報伝達をはじめとする初期対応手順 【現地審査】 ① 定めた手順に従って実施していること。 運用確認のためのエビデンス ・緊急事態を特定し対応した記録

文書審査の項目	現地審査の項目	審査の着眼点
2. 個人情報が漏えい，滅失又はき損をした場合に想定される経済的な不利益及び社会的な信用の失墜，本人への影響などのおそれを考慮し，その影響を最小限とするための手順を定めていること。	(1) 定めた手順に従い、個人情報が漏えい，滅失又はき損をした場合に想定される経済的な不利益及び社会的な信用の失墜，本人への影響などを最小限にするよう意図された措置を実施していること。	【文書審査】 ① 確実に実施できるよう、手順を明確に記述していること。 ② 社内の連絡体制が従業者にとって明確であること。 ③ 手順を定めるにあたっては、以下の事柄を考慮していること。 1) 緊急事態及び事故が最も起こりやすい場面 2) 予想される被害の規模 3) 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 4) 再発防止処置を実施する手順 5) 緊急時対応についての教育訓練 【現地審査】 ① 定めた手順に従って実施していること。 ※ 一次的な対処により緊急事態が沈静化した後は、是正処置及び予防処置（**3.8**）により、原因を特定して事故の原因を根本的に除去する処置を取る必要がある。 運用確認のためのエビデンス ・緊急事態が発生したことがある場合、影響を最小限とするために実施した記録
3. 緊急事態が発生した場合に備え、**a)**漏えい，滅失又はき損が発生した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手順を定めていること。	(1) 定めた手順に従い、漏えい，滅失又はき損が発生した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いたこと。	【文書審査】 ① 確実に実施できるように、手順を明確に記述していること。 ② 緊急事態が発生した場合、常に **a)**～**c)**の全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、対処方針を定めていること。 【現地審査】 ① 手順は、緊急時に確実に実行可能であること。 運用確認のためのエビデンス ・緊急事態が発生したことがある場合、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いたことが確認できる記録

文書審査の項目	現地審査の項目	審査の着眼点
4. 緊急事態が発生した場合に備え、**b)**二次被害の防止，類似事案の発生回避などの観点から，可能な限り事実関係，発生原因及び対応策を，遅滞なく公表する手順を定めていること。	(1) 定めた手順に従い、二次被害の防止，類似事案の発生回避などの観点から，可能な限り事実関係，発生原因及び対応策を，遅滞なく公表していること。	【文書審査】 ① 確実に実施できるように、手順を明確に記述していること。 ② 緊急事態が発生した場合、常に **a)**～**c)**の全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、対処方針を定めていること。 【現地審査】 ① 手順は、緊急時に確実に実行可能であること。 運用確認のためのエビデンス ・緊急事態が発生したことがある場合、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表した記録
5. 緊急事態が発生した場合に備え、**c)**事実関係，発生原因及び対応策を関係機関に直ちに報告する手順を定めていること。	(1) 定めた手順に従い、事実関係，発生原因及び対応策を関係機関に直ちに報告していること。	【文書審査】 ① 確実に実施できるように、手順を明確に記述していること。 ② 緊急事態が発生した場合、常に **a)**～**c)**の全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、対処方針を定めていること。 【現地審査】 ① 手順は、緊急時に確実に実行可能であること。 運用確認のためのエビデンス ・緊急事態が発生したことのある場合、事実関係、発生原因及び対応策を関係機関に直ちに報告した記録
	(2) 緊急事態が発生した場合の連絡先が、従業者にとって明確であること。	【文書審査】 ① 関係機関及びその連絡先を特定していること。 ※1 「関係機関」とは公的機関という意味ではなく、報告すべき利害関係を有している機関（人を含む。）を指す。例えば、受託者が事故を起こした場合、最も重要な関係機関は委託者であろう。また、事業者が企業グループの一員であれば、企業グループ全体に影響する可能性があるため、他の企業グループ各社も関係機関になるであろう。 ※2 直ちに報告すべき関係機関の範囲は事業者の判断による。ただし、プライバシーマーク付与を受けている事業者は、次に掲げる機関も関係機関に含め、報告する必要がある。 1) 審査を受けた機関（JIPDEC または各指定審査機関） 2) 主務大臣、または認定個人情報保護団体に所属している場合は

文書審査の項目	現地審査の項目	審査の着眼点
		その団体（認定個人情報保護団体に所属している場合、通常は認定個人情報保護団体が事業者に代わって主務大臣に報告するが、重大事故のときは事業者から主務大臣へ直接報告する必要がある。） ※3 一般に、地方自治体は個人情報の取扱いについての事故報告を事業者に対して求めておらず、ここでいう関係機関には含まれない（個人情報の取扱いの委託をしている等の利害関係者である場合を除く）。 【現地審査】 ① 従業者が関係機関の連絡先を容易に知り得る環境であること。 運用確認のためのエビデンス ・緊急連絡網等の参照環境

3.4 実施及び運用

3.4.1 運用手順

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

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には、運用の手順を明確にすることが不可欠である旨を定めたものである。プライバシーマークの審査において各要求事項の実施のための運用の手順について明確化を求めるのも、この要求事項に基づく。

2 注意事項

特になし。

3 個人情報保護法との対応

特になし。

4 審査の項目とその着眼点

運用の手順が明確であるかどうかは、該当するそれぞれの要求事項において審査される。

3.4.2 取得，利用及び提供に関する原則

3.4.2.1 利用目的の特定

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報の取得は、利用目的をできる限り具体的に特定した上で、その目的の達成に必要な限度において行わなければならない。

2 注意事項

目的外利用にならないよう想定できる限りの利用目的をあらかじめ多数列挙している例があるが、目的外利用があり得ないほどに多くの利用目的が特定されていると、最終的にどの目的で個人情報が利用されるのかわからなくなり、利用目的を厳格に特定するよう求めている要求事項の意味がなくなる。事業目的の達成に必要な限度で特定する必要がある。

3 個人情報保護法との対応

①個人情報保護法第 15 条第 1 項（利用目的の特定）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 個人情報の取得に当たっては、利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない旨を規定していること。	(1) 利用目的をできる限り特定していること。	【文書審査】 ① 個人情報の取得に当たっては、利用目的をできる限り特定し、その目的の達成に必要な限度において行う旨を記述していること。 【現地審査】 ① 利用目的は、公序良俗に反しないこと。 ② 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していること。 ③ 消費者等、本人の権利利益の保護の観点から、必要な場合は、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特定していること。 ※1 「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足りない。「事業活動に用いるため」、「提供するサービスの向上のため」、あるいは「マーケティング活動に用いるため」といった表現は、利用目的を特定したことにならない。

文書審査の項目	現地審査の項目	審査の着眼点
		※2 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。 1) 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。 2) 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。 3) 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。 4) 利用目的を特定するにあたっては、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。 運用確認のためのエビデンス ・利用目的を特定した記録
2. 利用目的の特定に関する手順を定めていること。	(1) 利用目的を特定するにあたっては管理者の承認を得ていること。	【文書審査】 ① 目的外利用を行わないため、新たに取得した個人情報の利用目的を特定するにあたっては、管理者の承認を得ていること。 ※1 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的で良い。 ※2 承認は、個人情報の特定(**3.3.1**)や、新規の種類の個人情報の取得(**3.4.2.4** 及び **3.4.2.5**)で定める承認と一括で行うのが便宜であろう。なお、複数箇所で手順を定めている場合、手順の不整合があれば不適合とする場合がある。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・利用目的の特定に関する内部的な承認の記録
	(2) 個人情報を取り扱う従業者は、その利用目的を明確に認識していること。	【現地審査】 ① 当該個人情報を取り扱う従業者が、その利用目的を明確に認識し得る仕組みがあること。 ※ 個人情報を取り扱う従業者が、その利用目的を知り得ない環境にあるのでは意味がない。個人情報の取得・利用申請書や台帳等により、利用目的を知る機会がなければならない。 運用確認のためのエビデンス ・個人情報を管理する台帳、様式等の参照環境

3.4.2.2 適正な取得

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報の取得は、適法、かつ、公正な手段によって行わなければならない。個人情報保護法第 17 条では、「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。」とある。同じ意味と考えて良いが、法律と同じ表現でない理由は、不正ではないが公正ではない手段（優越的な地位の利用など）による取得も認められない旨を明確にするためである。

2 注意事項

提供又は委託を受けて取得した場合であっても、提供者又は委託者が適正な取得をしていなかった場合は、提供又は委託を受けた者は結果として不適正な取得及び利用を助長したことになる。それは JIS の趣旨に反する。したがって、提供又は委託を受けて個人情報を取得する者は、提供者又は委託者が法令や国が定める指針等に違反していないことを確認するよう努めなければならない。不適正な取得であると知りながら提供又は委託を受けた場合は、この要求事項を満たしていないことになる。

3 個人情報保護法との対応

①個人情報保護法第 17 条（適正な取得）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 個人情報の取得は、適法、かつ、公正な手段により行わなければならない旨を規定していること。	(1) 個人情報の取得を、適法、かつ、公正な手段により行っていること。	【文書審査】 ① 個人情報の取得は、適法、かつ、公正な手段により行う旨を記述していること。 【現地審査】 ① 適法，かつ，公正な手段により個人情報を取得していること。 ※ 適法，かつ，公正な手段により個人情報を取得しているかどうかは、個々の要求事項の運用において審査される。
2. 本人以外から個人情報を取得する場合（受託による取得を含む）、提供元又は委託元が個人情報を適正に取り	(1) 定めた手順に従い、提供元又は委託元の個人情報の取扱いについて確認していること。	【文書審査】 ① 提供元又は委託元が個人情報を適切に取り扱っていることを確認する旨を記述していること。 【現地審査】 ① 定めた手順に従い、提供元又は委託元の個人情報の取扱いについて確認していること。

文書審査の項目	現地審査の項目	審査の着眼点
扱っていることを確認するよう規定していること。		※1 事実確認は、提供元又は委託元と事業者との間の力関係もあるため不可能な場合もある。事業者なりに確認する努力をしているのであれば不適合ではない。なお、「確認する努力」として、例えば、当該提供元又は委託元が個人情報保護法でいう個人情報取扱事業者であるときは、少なくとも、個人情報保護法上の義務を果たしているかどうか、ウェブサイト等を閲覧することは可能なはずである。 ※2 行政機関や地方自治体等からの提供又は委託は、法令に基づいて適正に取り扱われているものと考えて良く、確認する必要はない。 ※3 提供者又は委託者が明らかに法令等に違反している場合には、提供又は委託を受けてはならない。 運用確認のためのエビデンス ・提供元又は委託元の適正な取扱いを確認している記録

3.4.2.3 特定の機微な個人情報の取得の制限

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。 ***

1 概要

a)～e)に定めるような特定の機微な個人情報の取扱いについては、特段の配慮が求められる。したがってこれらの個人情報の取得、利用及び提供は原則として禁止し、例外的に認めるものとする。

2 注意事項

個人情報保護法には特定の機微な個人情報に関する特別の規定はない。**3.4.2.3** は JIS 独自の規定である。ただし、所管省庁が策定しているガイドラインには特定の機微な個人情報の取得を制限している例がある。

指紋や虹彩など、一生変わらない身体の一部の情報は生体認証などに利用されているが、それ自体は **a)～e)**でいう「特定の機微な個人情報」には該当しない。ただし、もし漏えい等をした場合、犯罪に悪用されたり、自己の身体情報でありながら認証手段として使うことが一生できなくなる等の重大な不利益が本人に発生する可能性があるため、「特定の機微な個人情報」と同等に取り扱うことが望ましい。

また、身長や体重、スリーサイズなども、**a)～e)**でいう「特定の機微な個人情報」には該当しない。ただし、業務上の必要もないのに従業者からこのような情報を取得することは、適正な取得（**3.4.2.2**）に反する可能性があるし、不法行為となる可能性もある。

国籍は原則として「特定の機微な個人情報」に該当しないが、国籍により容易に人種、民族が特定され、社会的差別を受ける可能性がある場合は、「特定の機微な個人情報」に該当し得るであろう。

なお、従業者の健康情報については、「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項」（厚生労働省、平成 27 年 11 月 30 日）の第 3 の 8 に、「... 以下に掲げる事項について事業場内の規程等として定め、これを労働者に周知するとともに、関係者に当該規程に従って取り扱わせることが望ましい。...」として、下記の項目が掲げられていることに注意する必要がある。

(a) 健康情報の利用目的に関すること
(b) 健康情報に係る安全管理体制に関すること
(c) 健康情報を取り扱う者及びその権限並びに取り扱う健康情報の範囲に関すること
(d) 健康情報の開示、訂正、追加又は削除の方法（廃棄に関するものを含む。）に関すること
(e) 健康情報の取扱いに関する苦情の処理に関すること

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. **a)**～**e)**の特定の機微な個人情報を取得、利用、提供しない旨を規定していること。	(1) **a)**～**e)**の特定の機微な個人情報が、**3.4.2.3** のただし書きの場合を除き、取得, 利用又は提供されていないこと。	【文書審査】 ① 特定の機微な個人情報は、**3.4.2.3** のただし書きの場合を除き、取得、利用又は提供しない旨を記述していること。 【現地審査】 ① 特定の機微な個人情報は、**3.4.2.3** のただし書きの場合を除き、取得、利用又は提供していないこと。 運用確認のためのエビデンス ・個人情報を管理する台帳等
2. 例外的に機微な個人情報を取得、利用、提供する場合は、**3.4.2.3** に定めるただし書きのときのみに限定していること。	(1) **a)**～**e)**の特定の機微な個人情報を取得している場合は、ただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を、過不足なく記述していること。 【現地審査】 ① **a)**～**e)**の特定の機微な個人情報は、ただし書きの場合のみ取得していること。 ※ JIS では適用除外と明文化されていないが、受託による取得も適用除外と考えて良い。委託元が適正に取得していればそれで良い。 運用確認のためのエビデンス ・個人情報を管理する台帳等 ・ただし書きを適用する場合の承認に関する記録
3. ただし書きにより例外的に機微な個人情報を取得、利用、提供する場合、承認手順を定めていること。	(1) 定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① ただし書きにより例外的に機微な個人情報を取得、利用、提供することについて、管理者の承認を得る手順を定めていること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的で良い。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きを適用する場合の承認に関する記録 ・個人情報を管理する台帳等

文書審査の項目	現地審査の項目	審査の着眼点
4. 本人から同意を得て、特定の機微な個人情報を取得、利用、提供する場合、本人から同意を得る手順を具体的に定めていること。	(1) 本人の同意を得て特定の機微な個人情報を取得、利用、提供している場合、具体的な手順に従って本人の明示的な同意を得ていること。	【文書審査】 ① 本人からの同意取得を確実に実施するよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 書面により本人の同意を得ていること。明示的な同意とは書面による同意であり、黙示の同意は認められない。 ※1 社員については、採用後の健康診断書、ストレスチェック制度における面接指導の結果の取得は法令（労働安全衛生法）に基づくものであるから、本人の同意は不要である。なお、採用選考の資料として健康診断書の提出を求めることは、応募者の適性と能力を判断する上で必要のない事項を把握する可能性があり、結果として、就職差別につながるおそれがあるとして、原則として禁止されている（平成 5 年 5 月 10 日付け労働省職業安定局業務調整課長補佐及び雇用促進室長補佐から各都道府県職業安定主管課長あて事務連絡「採用選考時の健康診断について」及び平成 13 年 4 月 24 日付け厚生労働省職業安定局雇用開発課長補佐から都道府県労働局職業安定主務課長あて事務連絡「採用選考時の健康診断に係る留意事項について」）。 ※2 JIS では適用除外と明文化されていないが、受託による取得も適用除外と考えてよく、本人の同意は不要である。委託元が適正に取得していればそれでよい。 ※3 特定の機微な個人情報の取得は、書面による取得に限定されない。 ※4 書面により取得する場合、**3.4.2.4** の要件を満たせばそれでよい。 <u>運用確認のためのエビデンス</u> ・本人の同意書

3.4.2.4 本人から直接書面によって取得する場合の措置

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報保護法では、本人から直接書面により個人情報を取得する場合、利用目的を明示するだけでよく、本人の同意は不要である。**JIS** では **a)～h)**の事項を明示し、かつ、本人の同意を得なければならず、個人情報保護法より厳格である。

差し出された記入用紙に本人が黙って書き始めたからといって、本人の同意があったとみなしてはならない。書面によって明示された事項に本人が同意したことが明確でなければならない。本人の同意は書面による同意であることが原則である。☞**3.4.2.5** も参照のこと。

2 注意事項

規格本体にある書面についての説明で明らかなように、書面による取得には、ウェブサイトからの入力も含む。電子メールも書面であり、電子メールによる明示及び同意の取得も可能である。

「明示し」と言えるためには、どこに書いてあるかを明確に指し示す必要がある。例えば、会員規約や契約約款などを明示するための書面とする場合に、文字が小さくてどこに書いてあるか分からないとか、長すぎてどこに書いてあるか分からないというのでは、たとえ内容が **a)～h)**の事項を満たしていたとしても、「明示し」ているとは言えない。またウェブサイトから取得する場合、小さなウインドウでスクロールして見なければ分からないというのも「明示し」ているとは言えない。

会員規約や契約約款を明示する書面として使うのであれば、例えば、個人情報の取扱いの部分を切り出すとか、字の大きさや色調を変えるなど、個人情報の取扱いについて記載した部分を何らかの方法により強調し、本人が容易に認識できるような措置を講じる必要がある。

なお、本人が話すことを書き取るのは、直接書面による取得ではない。

3 個人情報保護法との対応

①個人情報保護法第 18 条第 2 項（直接書面による取得）
②個人情報保護法第 18 条第 1 項（取得に際しての利用目的の通知又は公表）
③個人情報保護法第 18 条第 4 項（利用目的の通知又は公表の例外）
④個人情報保護法第 16 条第 3 項（利用目的による制限についての適用除外）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 直接書面により、新規の種類の個人情報を取得する場合、その承認手順を定めていること。	(1) 新規の種類の個人情報を直接書面により取得する場合、定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① 新規の種類の個人情報の取得は新たなリスクの発生である。取得することについて管理者の承認を得る手順を定めていること。 ※1 承認は、個人情報の特定(**3.3.1**)、利用目的の特定(**3.4.2.1**)、個人情報の取得(**3.4.2.4** 又は **3.4.2.5**)について一括で行うのが便宜であろう。なお、複数箇所で手順を定めている場合、手順の不整合があれば不適合とする場合がある。 ※2 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・直接書面により個人情報を取得する場合の承認に関する記録
2. 本人に対し、取得する手段毎に手順を定め、**a)**～**h)**の必要事項を書面により明示して同意を得るように規定していること。	(1) 直接書面により取得する個人情報は、**a)**～**h)**の事項を書面により本人に明示し、書面により同意を得ていること。	【文書審査】 ① 単に「**a)**～**h)**の必要事項を明示する」「同意を得る」と記載するだけでは不十分である。直接書面により個人情報を取得する手段毎（ウェブサイト、手渡し等）に書面により本人に明示する手順、書面により同意を得る手順を具体的に記述していること(どのような書面か、本人から同意を得る方法は何か、等。具体例は【現地審査】の項参照)。 【現地審査】 ① 定めた手順に従い、取得手段毎（ウェブサイト、手渡し等）に、書面により本人に **a)**～**h)**の事項を明示し、書面により同意を得ていること。 ② ウェブサイトで入力フォーマットにより取得する場合、確実に同意を得る仕組みになっていること。例えば、明示の画面に同意しなければ、入力フォームの画面に進めないとか、入力フォームに明示文が掲示されていて、「同意して送信」ボタンを押すようになっている等の方法が考えられる。

文書審査の項目	現地審査の項目	審査の着眼点
		③　ウェブサイトで履歴書の送付を求めている場合、書面を表示するかまたは書面へのリンクを明示し、同意した上で送付するように注意書きを記述していること。この場合でも、面接時に書面により同意を得ること。なお、次の④も参照のこと。 ④　人材募集広告で履歴書の送付を求めている場合、スペースが限られているため、全ての項目を明示することはできないことがあり得る。この場合、最低限、利用目的は明示すること。また、自社ウェブサイトがある場合、ウェブサイトに採用における明示書面を掲示した上で、ウェブサイトのアドレス（トップページのアドレスで良い）を明示すること。いずれの場合も、本人の面接時に、改めて書面による同意を得ること。ハローワークを通じた求人の場合、現行の所定の求人票には個人情報の取扱いについて記述する欄がない。この場合も、本人の面接時に、書面による同意を得ること。なお、面接前に書類のみで合否判定をする場合は、必ず連絡用の電子メールアドレスを履歴書に記載するよう本人に要求し、書類選考に入る前に、電子メールにより **a)**～**h)**の事項について同意を求めること（電子メールも書面である）。 ⑤　**a)**～**h)**の事項がどこに書いてあるか明確であること（**2 注意事項**を参照）。 ※1 明示する書面は、本人が何に同意したか分かるよう、本人の手もとに残る（あるいはウェブサイトであればいつでも見ることができる）ようにすることが望ましい。 ※2 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明示したり、本人の選択により利用目的の限定ができるようにしたり等、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。 ※3 中・高校生の採用選考において本人から提出を求めることができる書面及び書式については、厚生労働省の規則により全国一律に定められており、それ以外の書面（例えばここでいう同意書）の提出を求めることは禁止されている。したがって、この場合は **3.4.2.6** のただし書き **a)**に該当し、書面による本人の同意を取得しなくても不適合ではない。 運用確認のためのエビデンス ・本人に明示する書面（手段毎） ・本人の同意書（手段毎）

文書審査の項目	現地審査の項目	審査の着眼点
	(2) 直接書面取得時に本人に明示する書面の内容が **a)**～**h)**の事項を満たしていること。	【文書審査】 ① 本人に明示する書面に **a)**～**h)**の事項を、明確に記載していること。 【現地審査】 ① 直接書面取得する場合について、取得手段毎に書面の内容が **a)**～**h)**の事項を満たしていること。 ② 「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、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。**d)**が該当する場合、本人に懸念を抱かせないよう各項目を具体的に明らかにしていること。「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、持株会社等）を指す。 ③ 共同利用する場合、共同利用についても明示し、同意を得ていること。 ④ クレジットカード情報を取得する場合、クレジットカード情報の利用目的、取得者、提供先名、保存期間等を明示していること。 ⑤ 「本人が容易に認識できない方法により個人情報を取得する」とは、例えば cookie 情報の取得等が挙げられるが、その場合、当該方法により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していること。 ※1 **d)**、**e)**、**f)**、**h)**は、該当しない場合、記載する必要はない。 ※2 「本人が個人情報を与えることの任意性」とは、例えば、申込書への記載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す。 ※3 「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考えられる結果（例えば、結婚紹介申込書の年収の欄を記入しなければ、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等）を指す。 ※4 特定電子メール又は電子メール広告を送信する場合、その旨を **c)**の「利用目的」の中に明示しておかなければ、特定電子メール法又は特定商取引法違反になる可能性があるので注意を要する。 <u>運用確認のためのエビデンス</u> ・直接書面取得の際に本人に明示する書面（取得手段毎）

文書審査の項目	現地審査の項目	審査の着眼点
3. 直接書面による取得において、本人の同意を不要とするのは、ただし書きの場合のみに限定していること。	(1) 直接書面による取得において、本人の同意を得ていないのは、ただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を、過不足なく記述していること。 【現地審査】 ① 直接書面による取得において、本人の同意を得ていないのは、ただし書きの場合のみであること。 運用確認のためのエビデンス ・利用目的を特定した記録 ・個人情報を管理する台帳等
4. ただし書きを適用する場合の承認手順を定めていること。	(1) ただし書きを適用する場合、定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① ただし書きを適用する場合について管理者の承認を得る手順を定めていること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的で良い。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きを適用する場合の内部的な承認の記録

3.4.2.5 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

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報の取得は本人の同意を得ることが原則であるが、すべての場合に本人の同意が必要であるというのは現実的でない。例えば、受託した事業者が取得したことについて本人の同意を得なければならないとするのは無理であるし、直接取得の場合にすべて **3.4.2.4** の **a)**～**h)**の事項を明示し同意を得なければならないとするのも、口頭で取得する場合や監視ビデオで取得する場合等を考えると無理がある。従って、**3.4.2.4** と **3.4.2.5** は、取得の現実に合わせて規定されたものである。

2 注意事項

ただし書きの **a)**～**d)**については、規格本体付属の解説や経済産業分野ガイドライン等を参考に、適用基準を定める必要がある。

この要求事項で注意することは、本人への通知又は公表をしたくがないために、安易にただし書き **d)**に該当すると判断するような運用をしてはならないということである。このただし書き **a)**～**d)**は直接書面で取得する場合のただし書きとしても適用されるが、例えば、「『アンケート』と書いてある用紙に書いてもらうのだから、取得の状況からみて利用目的は明らかであり、ただし書き **d)**に該当するから明示・同意は必要ない」とか、「採用募集で履歴書を出してもらうのだから採用目的に利用するのは当たり前であり、ただし書き **d)**に該当するから明示・同意は必要ない」などというのは誤った理解である。そのような理解が許されるのであれば、**3.4.2.4** の要求事項はほとんど空文化してしまう。アンケートに回答したらダイレクトメールが送られてきたなどという事例は世の中には多いのであって、取得の状況と利用目的は必ずしも一致しない。ただし書き **d)**はあくまで例外であると認識しなければならず、ただし書き **d)**を適用する場合の適用基準は厳格に定めている必要がある。

受託者の場合、「取得者（例えば委託者）が本人に明示又は通知していれば、すでに本人にとって利用目的は明らかであるから、受託の場合は **d)**に該当する」と誤って理解しているケースが多く見られるので注意しなければならない。受託の場合でも、受託者としての利用目的を本人に通知又は公表する義務がある。

経済産業分野ガイドラインによれば、例えば、以下のように記述していれば、受託者は利用目的を公表していると言えることになる。

> 「給与計算サービス、宛名印刷サービス、伝票の印刷・発送サービス等の情報処理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。」

どこから受託したかについてまで、通知又は公表する必要はない。

なお、言うまでもないが、適正な取得(**3.4.2.2**)に反して取得した個人情報について、**3.4.2.5** の措置を講じれば洗浄されてクリーンになると理解してはならない。

3 個人情報保護法との対応

①個人情報保護法第 18 条第 1 項（取得に際しての利用目的の通知又は公表）

②個人情報保護法第 18 条第 4 項（利用目的の通知又は公表の例外）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 直接書面以外の方法により、新規の種類の個人情報を取得する場合、その承認手順を定めていること。	(1) 新規の種類の個人情報を、直接書面以外の方法により取得する場合、定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① 新規の種類の個人情報の取得は新たなリスクの発生である。取得することについて管理者の承認を得る手順を定めていること。 ※1 承認は、個人情報の特定(**3.3.1**)、利用目的の特定(**3.4.2.1**)、個人情報の取得(**3.4.2.4** 又は **3.4.2.5**)について一括で行うのが便宜であろう。なお、複数箇所で手順を定めている場合、手順の不整合があれば不適合とする場合がある。 ※2 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 取得の場面に応じてあらかじめその利用目的を公表している、又は取得後速やかにその利用目的を本人に通知又は公表していること。 運用確認のためのエビデンス ・**3.4.2.4** 以外の方法により個人情報を取得する場合の承認に関する記録

文書審査の項目	現地審査の項目	審査の着眼点
2. 個人情報を **3.4.2.4** 以外の方法によって取得する場合に、あらかじめその利用目的を公表する手順、又は取得後に速やかにその利用目的を，本人に通知し，又は公表する手順を定めていること。	(1) 定めた手順に従い、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，又は公表していること。	【文書審査】 ① 単に「利用目的を公表する」「取得後に速やかにその利用目的を，本人に通知し，又は公表する」等と記述するだけでは不十分である。利用目的の通知又は公表を確実に実施するよう、手順や手段を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 受託により取得した個人情報についても、受託者としての利用目的を通知又は公表していること。 ③ 音声を録音している場合、その利用目的を通知又は公表していること。 ④ 防犯カメラを設置している場合は、隠し撮りとならないために、例えば「防犯カメラ監視中」や「防犯カメラ設置中」等の表示をすること。なお、防犯目的以外で利用する場合は、当該利用目的を通知又は公表すること。 ⑤ 提供する場合は「提供する」こと自体、共同利用する場合は「共同利用する」こと自体も、利用目的として通知又は公表していること。 ※1 「通知」とは、本人に直接知らしめることをいい、事業の性質及び個人情報の取扱い状況に応じ、内容が本人に認識される合理的かつ適正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り個人情報を取得する場合などは、通知も書面によらず口頭で行っても良い。 ※2 「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いの状況に応じ、合理的かつ適切な方法によらなければならない。 <u>運用確認のためのエビデンス</u> ・利用目的を記述しているウェブサイト又は一般に頒布している公表物
	(2) 通知又は公表に漏れがないこと。	【現地審査】 ① 本人から直接取得する場合（例えば監視カメラにより取得する場合、口頭により取得する場合等）であっても、書面によらない限り、**3.4.2.5** の対象として、利用目的を通知又は公表していること。

文書審査の項目	現地審査の項目	審査の着眼点
		※1 委託を受ける場合、第三者から提供を受ける場合、公開情報から取得する場合など、**3.4.2.4** 以外による個人情報の取得には、すべて **3.4.2.5** が適用される。 したがって、例えば法令に基づく取得であるために本人の同意が不要の場合であっても、それが **3.4.2.5** のただし書き **a)**～**d)**のいずれにも該当しないときは、利用目的の通知又は公表が必要である。 ※2 ただし書き **d)**により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、**3.4.2.5** のただし書き **d)**に該当せず、通知又は公表の対象となる。 運用確認のためのエビデンス ・個人情報を管理する台帳等 ・利用目的を特定した記録 ・利用目的を記述しているウェブサイト又は一般に頒布している公表物
3. 本人に通知又は公表しないのは、ただし書き **a)**～**d)**の場合のみに限定していること。	(1) 本人に通知又は公表しないのは、ただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を過不足なく記述していること。 【現地審査】 ① 本人に通知又は公表をしないのは、ただし書き **a)**～**d)**の場合のみであること。 運用確認のためのエビデンス ・利用目的を特定した記録 ・個人情報を管理する台帳等
4. ただし書き **a)**～**d)**を適用する場合の承認手順を定めていること。	(1) ただし書きを適用する場合、定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① ただし書きを適用する場合の管理者の承認手順を定めていること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的で良い。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きを適用する場合の承認に関する記録

文書審査の項目	現地審査の項目	審査の着眼点
5. ただし書き **d)**に該当する場合、適用を限定するよう規定していること。	(1) ただし書き **d)**に該当するものとして取得している個人情報は、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のみであること。	【文書審査】 ① 利用目的の通知又は公表をしたくがないために、安易にただし書き **d)**に該当すると判断するようなことがあってはならない。ただし書き **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り、極力限定的に解釈する必要がある。具体的な例を挙げる等により、適用を限定するよう記述していること。 【現地審査】 ① 事業者内には、ただし書き **d)**に該当するものが必ず存在する。ただし、通知又は公表したくがないために、安易にただし書き **d)**に該当すると判断するような運用をしていないこと。 ※ **3.4.2.5** のただし書き **d)**に該当すると考えられるものの例示（直接書面により取得する場合も含む。）は、次のとおりである。 1) 一般の慣行としての名刺交換 2) クリーニング店やデリバリーサービス等で受取人を特定するために個人情報を取得すること 3) 入退管理のためであることが明らかな状況において来訪者に氏名を記入してもらうこと 4) 配達などで受取確認のためにサインをもらうこと 5) 見積書、請求書等の伝票に記載された担当者名や捺印など 運用確認のためのエビデンス ・利用目的の特定に関する記録 ・個人情報を管理する台帳等

3.4.2.6 利用に関する措置

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報は、特定した利用目的の範囲内で利用しなければならない。個人情報保護法第 15 条第 2 項による利用目的の変更も、JIS では目的外の利用に該当することに注意する必要がある。

2 注意事項

企業の合併等では顧客データベースを統合することが考えられるが、それぞれが取得した際の利用目的が必ずしも一致しない場合がある。利用目的が重ならない部分は相互に目的外となるから、重なる範囲で利用するにとどめるか、あるいは重ならない部分について改めて本人の同意を得て利用するか、対応が必要であろう。

ただし書き **b)**～**d)**については、規格本体付属の解説や経済産業分野ガイドライン等を参考に、適用基準を定める必要がある。なお、**3.4.2.6** 項に限ったことではないが、「当社では運用を厳格にする方針であるため、ただし書きは適用しない。したがって文書にもただし書きは規定していない。」という事業者がある。それはそれで一つの考え方ではあるが、特にこの **3.4.2.6** 項のただし書きのように、ただし書きの中には事業者の社会的責任を定めているものがある。そのようなものさえも適用しないというのは個人情報保護に偏った過剰反応であって、社会的責任を放棄していると言わざるを得ない。各要求事項のただし書きはそれなりの合理的な理由があって定められているのであるから、適用すべきである。

なお、同意を得るために個人情報を利用することは、目的外利用には該当しない。

3 個人情報保護法との対応

①個人情報保護法第 15 条第 2 項（利用目的の変更）

②個人情報保護法第 16 条第 1 項（利用目的による制限）

③個人情報保護法第 16 条第 3 項（利用目的による制限の適用除外）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 特定した利用目的の達成に必要な範囲内で個人情報を利用しなければならない旨を明確に規定していること。	(1) 特定した利用目的の達成に必要な範囲内で個人情報を利用していること。	【文書審査】 ① 特定した利用目的の達成に必要な範囲内で個人情報を利用しなければならない旨を記述していること。 【現地審査】 ① 特定した利用目的の範囲内で個人情報を利用していること。 ※1 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。 ※2 個人情報保護法では、本人が想定できる範囲であれば、第 16 条第 2 項により、利用目的の変更は可能であるが、JIS では、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。 ※3 企業の合併等で顧客データベースを統合することが考えられるが、それぞれが取得した際の利用目的が必ずしも一致しない場合がある。統合して区別することなく利用するときは、重ならない部分は目的外利用になるから、改めて事前に本人の同意を得る必要がある。 ※4 利用目的は、最終的にどのような目的で利用するのか、可能な限り具体的に特定している必要がある。 ※5 利用目的の範囲を超えて提供することは目的外利用であり、**3.4.2.8** でなく **3.4.2.6** により同意を得る必要がある。 運用確認のためのエビデンス ・利用目的を特定した記録
2. 利用目的を変更する場合の承認手順を定めていること。	(1) 定めた手順に従い、管理者の承認を得て利用目的が変更されていること。	【文書審査】 ① 利用目的を変更する場合の管理者による承認手順を定めていること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的で良い。 【現地審査】 ① 定めた手順に従い、実施していること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・利用目的の変更に関する内部的な承認の記録
3. 利用目的を変更する場合、**3.4.2.4** の **a)**～**f)** に示す事項又はそれと同等以上の内容の事項を本人に通知して同意を得る手順を定めていること。	(1) 定めた手順に従い、本人に通知し同意を得ていること。	【文書審査】 ① 単に「**3.4.2.4** の **a)**～**f)** に示す事項又はそれと同等以上の内容の事項を本人に通知して同意を得る」等と記載するだけでは不十分である。利用目的を変更する場合に、本人への通知及び同意が確実に実施されるよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ※ 通知及び同意は書面によることが望ましいが、状況に応じた方法でもよい（口頭での通知及び口頭での同意）。 運用確認のためのエビデンス ・本人に通知した内容 ・本人の同意書
	(2) 通知する内容が **a)**～**f)**の要求事項を満たしていること。	【現地審査】 運用確認のためのエビデンス ・本人に通知した内容 ・本人の同意書
4. 目的外利用で本人の同意を必要としないのは、ただし書きの場合のみに限定して規定していること。	(1) 目的外利用で本人の同意を必要としないのは、ただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を過不足なく記述していること。 【現地審査】 ① 目的外利用で本人の同意を必要としないのは、ただし書きの場合のみであること。 運用確認のためのエビデンス ・利用目的を特定した記録 ・個人情報を管理する台帳等
5. ただし書き **a)**～**d)**を適用する場合の承認手順を定めていること。	(1) ただし書き **a)**～**d)**を適用する場合、定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① ただし書き **a)**～**d)**を適用することについての管理者の承認手順を明確に記述していること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。

文書審査の項目	現地審査の項目	審査の着眼点
		【現地審査】 ①　定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きを適用する場合の承認に関する記録 ・国の機関等が発行した照会状等の書面
6. 目的外利用に該当するかどうか判断に迷う場合、管理者の判断を求めるよう規定していること。	(1) 目的外利用に該当するかどうか判断に迷う場合、管理者の判断を求めていること。	【文書審査】 ①　目的外利用の場合の承認手順のことではなく、ここでは、目的外利用かどうか判断に迷う場合をいっている。派生的に新たな利用をする場合、明らかな目的外利用であれば文書で定めた手順に従うが、目的内の利用かどうかグレーゾーンで、従業者が判断に迷うことがあり得る。こういった場合も必ず最終的には管理者の判断を求めるようにしていること。 【現地審査】 ①　定めた手順に従い、実施していること。 運用確認のためのエビデンス ・従業者への質問

3.4.2.7 本人にアクセスする場合の措置

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

「本人にアクセスする」とは、ダイレクトメール、電話、FAX、電子メール等で本人に接触することをいい、個人情報の利用の一場面である。個人情報保護法には本人にアクセスするために利用することについての特別な規定はなく、この要求事項は JIS 独自の規定である。

個人情報の利用においては、身に覚えのない事業者からの電話やダイレクトメールに対する苦情が多い。一方、個人情報は適切に利用すれば効果的なサービスを提供できる重要な情報である。個人情報保護法も JIS も、個人情報の保護と個人情報の有効活用のバランスをとることを意図しているが、この要求事項は、その性格が端的に現れている場面であると言える。

消費者としては、自分の情報がどこからどのように取得されたのかを知りたい。それに応えるため、事業者は、**3.4.2.4** の **a)～f)** に示す事項又はそれと同等以上の内容の事項だけでなく、「取得方法」を本人に通知し、同意を得なければならない。取得方法も通知しなければならないことがこの要求事項のポイントである。取得方法には、その個人情報の出所は何か（卒業生名簿、電話帳、登記事項証明書等の「取得源」）、どのように取得したのか（書店から購入した、提供を受けた等の「取得の経緯」）の両方を記述しなければならない。

言うまでもないことであるが、適正な取得(**3.4.2.2**)を満たしていない個人情報を利用して本人にアクセスすることは許されない。取得方法を通知すれば不適正に取得された個人情報が洗浄されてクリーンになると理解してはならない。これは **3.4.2.8** でも同様である。

2 注意事項

3.4.2.7 では「あらかじめ」の同意を求めていない。したがって、例えばダイレクトメールを郵送する場合、最初に送るときに通知文と返送用の同意書を同封してもよい。

この **3.4.2.7** は、「本人にアクセスすること」を利用目的としてあらかじめ特定していることが前提であることに注意する必要がある。利用目的として特定していなかった場合、本人にアクセスすることは目的外利用になるため、**3.4.2.6** に従い、あらかじめ同意を得る必要がある。ここで、**3.4.2.7** における通知及び同意の手順を、目的外利用についての通知及び同意の手順と兼ねることができると考えるのは誤りである。個人情報保護法第 16 条では目的外利用についてあらかじめ同意を求めることを義務付けており、本人にアクセスする場合だけ、同意はあらかじめでなくてもよいという解釈が許されるのであれば、**3.4.2.7** は個人情報保護法に違反していることになってしまう。「本人の同意なく取得（**3.4.2.5** により取得）した個人情報により本人にアクセスする場合、本人にアクセスすることを利用目的として特定し通知又は公表しているときでも、なおかつ、その利用について本人の同意が必要」というのが **3.4.2.7** の規定の主旨である。だからこそ個人情報保護法よりも厳しい上乗せ規制なのである。

電子メール広告や特定電子メールを送る場合は、特定商取引法や特定電子メール法の規定により、原則として事前の同意を得ていなければならないことに注意を要する。

3 個人情報保護法との対応

①個人情報保護法第 23 条第 4 項（第三者提供に該当しない場合）

②個人情報保護法第 16 条第 3 項（利用目的による制限についての適用除外）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 本人にアクセスすることについての承認手順を定めていること。	(1) 定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① 本人にアクセスする手段毎に管理者の承認を得る手順を定めていること。 ※1 承認は、個人情報の特定(**3.3.1**)、利用目的の特定(**3.4.2.1**)、個人情報の取得(**3.4.2.4** 又は **3.4.2.5**)などと共に一括で行うのが便宜であろう。なお、複数箇所で手順を定めている場合、手順の不整合があれば不適合とする場合がある。 ※2 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・本人にアクセスすることについての承認に関する記録
2. 本人に対し、**3.4.2.4** の **a)**～**f)** に示す事項又はそれと同等以上の内容の事項, 及び取得方法を通知し、本人の同意を得る手順を規定していること。	(1) 定めた手順に従い、本人の同意を得る手順を実施していること。	【文書審査】 ① 単に「**3.4.2.4** の **a)**～**f)** に示す事項又はそれと同等以上の内容の事項, 及び取得方法を通知し、本人の同意を得る」等と記述するだけでは不十分である。手順は、アクセスの手段（ダイレクトメール、電話、FAX、電子メール等）毎に記述していること。 ※ 特定電子メールまたは電子メール広告を送信する場合、**3.4.2.7** の規定にかかわらず、取引関係にある者への送信など一定の場合を除き、あらかじめ同意を得る手順を規定している必要がある。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 本人から同意を得ていること。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

文書審査の項目	現地審査の項目	審査の着眼点
		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、本人からの明示的な同意を得ることが原則であるが、同意の意思があっても本人から同意する旨の回答が返ってくることは期待しにくい現実を考慮し、本人が心理的負担や経済的負担を感じることなく明示的に回答できる措置を講じている場合は、継続して本人にアクセスしてよいものとする。これは **3.4.2.7** に限り認める特例であって、他の要求事項でいう「同意」には適用されない。 ※1 通知及び同意は書面によることが望ましいが、状況に応じた方法でもよい（口頭での通知及び口頭での同意）。 ※2 特定電子メールまたは電子メール広告を送信する場合、**3.4.2.7** にかかわらず、取引関係にある者への送信など一定の場合を除き、あらかじめ同意を得ることが必須である。なお、名刺交換で取得したメールアドレスに特定電子メールや電子メール広告を送信する場合、取得の状況から判断される利用目的の範囲内であることが必要である。 運用確認のためのエビデンス ・通知内容（手段毎） ・本人の同意書（手段毎） ・本人が心理的負担や経済的負担を感じることなく回答できるよう講じている措置
	(2) 本人に通知する書面が、**3.4.2.4** の **a)**～**f)** に示す事項又はそれと同等以上の内容の事項, 及び取得方法を満たしていること。	【現地審査】 ① 「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していること。 運用確認のためのエビデンス ・通知内容（手段毎）
3. 本人の同意を必要としないのは、ただし書きの場合のみであるように規定していること。	(1) 本人の同意を必要としないのは、ただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を過不足なく記述していること。 【現地審査】 ① 本人の同意を必要とせず本人にアクセスしているのは、ただし書きに該当する場合のみであること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・利用目的を特定した記録 ・個人情報を管理する台帳等
4. ただし書き **b)**～**f)**を適用する場合の承認手順を定めていること。	(1) 定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① ただし書き **b)**～**f)**を適用する場合の管理者による承認手順を明確に記述していること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きの適用についての承認に関する記録
5. ただし書き **d)**を適用する場合、その手順を定めていること。	(1) 定めた手順に従い、共同利用者との間で必要事項について取り決めていること。	【文書審査】 ① 以下の事項を共同利用者との間で取り決める手順を明確に定めていること。 1) 共同して利用する個人情報の項目 2) 共同して利用する者の範囲 3) 共同して利用する者のすべての利用目的 4) 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 5) 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み） 6) 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 7) 共同利用する個人情報の取扱いに関する事項 － 個人情報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 － 共同利用終了後の個人情報の返還、消去、廃棄に関する事項 8) 共同利用する個人情報の取扱いに関する取決めが遵守されなかった場合の措置 9) 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 ※1 ただし書き **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

文書審査の項目	現地審査の項目	審査の着眼点
		個別列挙が必要でない場合もある。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ことでもよい。 ※2 すでに特定の事業者が取得している個人情報を他の事業者と共同利用する場合、すでに取得している事業者が特定した利用目的の範囲内で共同利用しなければならない。 ※3 ただし書き **d)**の「当該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（**3.4.4.1**～**3.4.4.7** 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。 【現地審査】 ① 定めた手順に従い、実施していること。 ※1 グループ企業間での共同利用について、十分認識せず行っているケースがよくあるので確認する必要がある。 ※2 共同利用と考えていても実態は委託の場合がある。その場合は **3.4.3.4** の対象となるので、実態を正しく把握する必要がある。 <u>運用確認のためのエビデンス</u> ・共同利用者間の契約書
	(2) 定めた手順に従い、ただし書き d)の小項目を、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こと。	【文書審査】 ① 本人に通知し，又は本人が容易に知り得る状態に置く手順を明確に定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② どのように「あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いている」のかを、具体的に示すことができること。 <u>確認のためのエビデンス</u> ・ただし書き **d)**の小項目を、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措置

3.4.2.8 提供に関する措置

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

「提供」とは、個人情報を利用可能な状態に置くことをいう。個人情報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情報を利用できる状態にあれば、「提供」に当たる。

個人情報を第三者に提供する場合は、あらかじめ本人の同意を得ることが原則である。

取得方法を通知すれば不適正に取得された個人情報が洗浄されてクリーンになると理解してはならない。

2 注意事項

ただし書き **b)**は、個人情報保護法第 23 条第 2 項に定める第三者提供の際のオプトアウトに似ているが、同じではない。法と異なり、「通知に代わる同等の措置を講じている」ことを要求している。これは、通知と同等と言えるだけのできる限りの措置を講じることが求められているのであって、個人情報保護法でいう「公表」又は「本人が容易に知り得る状態に置く」だけでは足りない。また、ただし書き **b)**は安易に適用してはならず、適用基準を定める必要がある。

3.4.2.8 は、「第三者に提供すること」を利用目的としてあらかじめ特定していることが前提である。利用目的として特定していなかった場合に第三者に提供することは目的外利用になるため、**3.4.2.6** に従い、あらかじめ同意を得ることが原則であるが、**3.4.2.8** による同意取得の手続と兼ねても良い。

ただし書き **d)**については、「取得したときは委託する予定がなかったため委託する旨を本人に明示していなかったが、分社化や業務の拡大等により、事後的に委託せざるを得なくなった場合」を含む。

ただし書き **e)**については、事業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、自社の個人情報を相手会社へ提供する場合も含む。その際は、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、事業承継が不調に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に必要な契約を締結しなければならない。

なお、第三者提供によって取得した個人情報が、開示対象個人情報に該当する場合は、**3.4.4.1**～**3.4.4.7** が適用されることに注意する必要がある。

3 個人情報保護法との対応

① 個人情報保護法第 23 条（第三者提供の制限）

② 個人情報保護法第 16 条第 3 項（利用目的による制限についての適用除外）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 第三者に提供する場合、承認手順を定めていること。	(1) 定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① 第三者に提供することについての管理者の承認を得る手順を記述していること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。 【現地審査】 ① 定めた手順に従い、実施していること。 ※1 法令に基づいて役所等（市町村、ハローワーク、社会保険事務所、年金基金、健康保険組合等）に従業者の情報を提供する場合も第三者提供に該当するが、**3.4.2.6** のただし書き **a)**に該当するため、本人の同意は不要である。 ※2 例えば、受託開発ソフトウェア事業者が従業者のスキルシートを委託元に提供する場合は第三者提供に該当する。 運用確認のためのエビデンス ・第三者に提供することについての承認に関する記録
2. 第三者に提供する場合、あらかじめ本人に対して，取得方法及び **3.4.2.4** の **a)**～**d)** の事項又はそれと同等以上の内容の事項を通知し，本人の同意を得る手順を定めていること。	(1) 定めた手順に従い、本人に通知し同意を得る手順を実施していること。	【文書審査】 ① 単に「あらかじめ本人に対して，取得方法及び **3.4.2.4** の **a)**～**d)** の事項又はそれと同等以上の内容の事項を通知し，本人の同意を得る」等と記載するだけでは不十分である。本人への通知及び同意の取得を確実に実施するよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い実施していること。 ※ 通知及び同意は書面によることが望ましいが、状況に応じた方法でもよい（口頭での通知及び口頭での同意）。 運用確認のためのエビデンス ・本人への通知内容 ・本人の同意書

文書審査の項目	現地審査の項目	審査の着眼点
	(2) 本人への通知内容が、少なくとも取得方法及び **3.4.2.4** の **a)** ～**d)**の事項を満たしていること。	【現地審査】 ① 本人に、少なくとも取得方法及び **3.4.2.4** の **a)** ～**d)**の事項を満たしている内容を通知していること。 運用確認のためのエビデンス ・本人への通知内容 ・本人の同意書
	(3) 特定した利用目的の達成に必要な範囲を超えて個人情報を提供する場合、**3.4.2.6** により、目的外利用の手順により同意を得ていること。	【現地審査】 ① 特定した利用目的の達成に必要な範囲を超えて個人情報を提供する場合、**3.4.2.6** により、目的外利用の手順により同意を得ていること。 運用確認のためのエビデンス ・目的外利用についての承認に関する記録 ・本人への通知内容 ・本人の同意書
3. 本人の同意を必要としないのは、ただし書きの場合のみであるように規定していること。	(1) 本人の同意を必要としないのは、ただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を過不足なく記述していること。 【現地審査】 ① 本人の同意を必要としないのは、ただし書きの場合のみであるように運用していること。 運用確認のためのエビデンス ・利用目的を特定した記録 ・個人情報を管理する台帳等
4. ただし書き **b)**～**g)**を適用する場合の承認手順を定めていること。	(1) 定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① ただし書き **b)**～**g)**を適用する場合について、管理者の承認を得る手順を定めていること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きの適用についての承認に関する記録

文書審査の項目	現地審査の項目	審査の着眼点
5. ただし書き **b)**を適用する場合、各小項目をあらかじめ，本人に通知し，又はそれに代わる同等の措置を講じる手順を定めていること。	(1) 定めた手順に従い、ただし書き **b)**の各小項目をあらかじめ，本人に通知し，又はそれに代わる同等の措置を講じていること。	【文書審査】 ① ただし書き **b)**を適用する場合の必要な措置が確実に講じられるよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② どのように「あらかじめ、本人に通知し、又はそれに代わる同等の措置を講じている」のかを、具体的に示すことができること。 ※1 ただし書き **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。 ※2 ただし書き **b)**の小項目は、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、ただし書き **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り、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、企業の総務担当者から個人情報を取得する場合に、ただし書き **b)**の小項目を、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、通知と同等と言えるだけのできる限りの措置を講じることを要し、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。 <u>運用確認のためのエビデンス</u> ・本人に通知又はそれに代わる同等の措置を講じていることを証明できる記録
6. ただし書き **c)**を適用する場合、**b)**で示す事項又はそれと同等以上の内容の事項を，あらかじめ，本人に通知し，又は本人が容易	(1) 定めた手順に従い、**b)**で示す事項又はそれと同等以上の内容の事項を，あらかじめ，本人に通知し，又は本人が容易	【文書審査】 ① ただし書き **c)**を適用する場合の必要な措置を確実に実施するよう、手順を明確に記述している必要がある。 【現地審査】 ① 定めた手順に従い、実施していること。 ② どのように「あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いている」のかを、具体的に示すことができること。

文書審査の項目	現地審査の項目	審査の着眼点
に知り得る状態に置く手順を定めていること	に知り得る状態に置いていること	※1 ただし書き 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、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。 ※2「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。 運用確認のためのエビデンス ・b) で示す事項又はそれと同等以上の内容の事項を，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措置
7. ただし書き f)を適用する場合、その手順を定めていること。	(1) 定めた手順に従い共同利用者との間で必要事項について取り決めていること。	【文書審査】 ① 以下の事項を共同利用者との間で取り決める手順を明確に定めていること。 1) 共同して利用する個人情報の項目 2) 共同して利用する者の範囲 3) 共同して利用する者のすべての利用目的 4) 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 5) 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み） 6) 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 7) 共同利用する個人情報の取扱いに関する事項 － 個人情報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 － 共同利用終了後の個人情報の返還、消去、廃棄に関する事項 8) 共同利用する個人情報の取扱いに関する取決めが遵守されなかった場合の措置 9) 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 ※1 ただし書き f)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

文書審査の項目	現地審査の項目	審査の着眼点
		も個別列挙が必要でない場合もある。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ことでもよい。 ※2 すでに特定の事業者が取得している個人情報を他の事業者と共同利用する場合は、すでに取得している事業者が特定した利用目的の範囲で共同利用しなければならない。 ※3 ただし書き f)の「当該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（**3.4.4.1**～**3.4.4.7** 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。 【現地審査】 ① 定めた手順に従い、実施していること。 ※1 グループ企業間での共同利用について、十分認識せず行っているケースがよくあるので確認する必要がある。 ※2 共同利用と考えていても実態は委託の場合がある。その場合は **3.4.3.4** の対象となるので、実態を正しく把握する必要がある。 <u>運用確認のためのエビデンス</u> ・共同利用者間の契約書
	(2) 定めた手順に従い、ただし書き f)の小項目を、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こと。	【文書審査】 ① ただし書き f)の小項目を、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く手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② どのように「本人が容易に知り得る状態」に置いているかを、具体的に示すことができること。 <u>運用確認のためのエビデンス</u> ・ただし書き f)の小項目をあらかじめ，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措置

3.4.3 適正管理

3.4.3.1 正確性の確保

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報は、利用目的の達成に必要な範囲内において、正確、かつ、最新の状態で管理しなければならないことを要求している。☞第一部 4.ステップ 9 **g)**

2 注意事項

個人情報に誤りがあることが分かった場合、本人から訂正の要求がなくても、事業者はこの要求事項に基づき自ら訂正できる。本人の死亡により当該本人の個人情報が不要になった場合、当然のことであるが本人の要求がなくても消去できる。

3 個人情報保護法との対応

①個人情報保護法第 19 条（データ内容の正確性の確保）

4 審査の項目とその着眼点

事業者は、利用目的の達成に必要な範囲内において、正確、かつ、最新の状態で管理するために、以下の事項について対策を講じなければならない。

① 個人情報の入力時の照合・確認の手続の整備
② 訂正の手続の整備
③ 個人情報が正確かつ最新であることを検証する手順の整備
④ 記録事項の更新
⑤ 保存期間の設定

ただし、事業者が取り扱う個人情報の量や内容により対策は異なるため、ここではそれぞれの講じなければならない事項について、望ましい手法を例示する。

取り扱う個人情報の量や内容は事業者ごとに異なるため、講じなければならない事項を実施する手法も事業者の判断により異なって当然であり、**ここに示されている手法を一律に実施するよう求めるものではない。**事業者はここに示されている手法を参考に、必要に応じて、自らに合った方法で実施すればよい。

なお、講じることとした対策は、内部規程(**3.3.5**)の **g)**（個人情報の適正管理に関する規定）の一つとしてとりまとめなければならない。

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
1. 個人情報の入力時の照合・確認の手続の整備	(1) 個人情報を入力する際の作業責任者を明確化していること	① PMS の体制整備の一環として、個人情報を入力する際の作業責任者の責任及び権限を内部規程に明確に定めている。 ② 作業責任者が誰かを明確にしている。

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(2) 入力した個人情報の照合及び確認の手順を明確化していること	① 入力した個人情報の照合及び確認の手順を確立し、内部規程に明確に定め、維持している。 ② 作業手順書を作業者に配布する等により、周知徹底している。
	(3) 定めた手順により照合及び確認作業を実施していること	① 作業の実施状況をモニタリングしている。 ② 定めた手順により作業者が照合及び確認作業を実施していることを定期的に確認している。 運用確認のためのエビデンス ・作業状況を確認している記録
2. 訂正の手続の整備	(1) 個人情報を訂正する際の作業責任者を明確化していること	① PMS の体制整備の一環として、個人情報を訂正する際の作業責任者の責任及び権限を内部規程に明確に定めている。 ② 作業責任者が誰かを明確にしている。
	(2) 個人情報の誤りや不整合を発見する手順を明確化していること	① 個人情報の誤りや不整合を発見する手順を確立し、内部規程に明確に定め、維持している。 ② 作業手順書を作業者に配布する等により、周知徹底している。
	(3) 訂正した個人情報の照合及び確認の手順を明確化していること	① 訂正した個人情報の照合及び確認の手順を確立し、内部規程に明確に定め、維持している。 ② 作業手順書を作業者に配布する等により、周知徹底している。
	(4) 定めた手順により訂正作業を実施していること	① 作業の実施状況をモニタリングしている。 ② 定めた手順により作業者が訂正作業を実施していることを定期的に確認している。 運用確認のためのエビデンス ・作業状況を確認している記録
3.個人情報が正確かつ最新であることを検証する手順の整備	(1) 個人情報が正確かつ最新であることを検証する作業責任者を明確化していること	① PMS の体制整備の一環として、個人情報が正確かつ最新であることを検証する作業責任者の責任及び権限を内部規程に明確に定めている。 ② 作業責任者が誰かを明確にしている。
	(2) 個人情報が正確かつ最新であることを検証し、必要に応じて訂正する手順を明確化していること	① 個人情報が正確かつ最新であることを検証し、必要に応じて訂正する手順を確立し、内部規程に明確に定め、維持している。 ② 登録している個人情報については、本人が自らいつでも訂正できる仕組み（本人確認についての措

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
		置を講じた上でのウェブサイトからの修正など）を提供している。 ③ 作業手順書を作業者に配布する等により、周知徹底している。
	(3) 定めた手順により作業を実施していること	① 作業の実施状況をモニタリングしている。 ② 定めた手順により作業者が個人情報が正確かつ最新であることを検証する作業を実施していることを定期的に確認している。 運用確認のためのエビデンス ・作業状況を確認している記録
4. 記録事項の更新	(1) 作業実施記録を維持する責任者を明確化していること	① PMS の体制整備の一環として、作業実施記録を維持する責任者の責任及び権限を内部規程に明確に定めている。 ② 責任者が誰かを明確にしている。
	(2) 作業実施記録を更新する手順を明確化していること	① 作業記録を更新する手順を確立し、内部規程に明確に定め、維持している。 ② 作業手順書を作業者に配布する等により、周知徹底している。
	(3) 作業記録を保管する手順を明確化していること	① 作業記録を保管する手順を確立し、内部規程に明確に定め、維持している。 ② 作業手順書を作業者に配布する等により、周知徹底している。
	(4) 定めた手順により記録事項の更新を実施していること	① 作業実施記録の更新を確認している。 ② 定めた手順により記録事項の更新を実施していることを定期的に確認している。 運用確認のためのエビデンス ・作業実施記録及びその更新状況
5. 保存期間の設定	(1) 保存期間を設定する責任者を明確化していること	① PMS の体制整備の一環として、保存期間を設定する責任者の責任及び権限を内部規程に明確に定めている。 ② 責任者が誰かを明確にしている。

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(2) 保存期間を設定する基準を明確化していること	① 保存期間を設定する基準を内部規程に明確に定めている。 ※ 保存期間は事業者がリスクを負って設定するものであり、永久保管と定めたからといって不適合ではない。
	(3) 定めた手順により保存期間を設定していること	① 設定した保存期間が保存期間を設定する基準と整合性があることを確認している。 ② 期限前に廃棄したり、期限終了後も漫然と保存してリスクを抱え込んだりすることのないよう、ラベルを貼るなど保存期間がすぐに分かるようにしている。 ※ 保存期間が過ぎたからといって機械的にその都度廃棄することが（技術的に又は業務上煩雑になるために）難しい場合もある。ある程度まとまった段階で廃棄するといった方法もあろう。そういうやり方を否定するものではない。 運用確認のためのエビデンス ・個人情報を管理する台帳等 ・個人情報の保存状況

3.4.3.2 安全管理措置

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

事業者は、取り扱う個人情報のリスクに応じて合理的な安全管理措置を講じなければならない旨を規定している。これは当然、リスクなどの認識、分析及び対策(**3.3.3**)と連動する。**3.3.3** において講じることとした対策が、安全管理措置となるはずであり、全事業者一律の対策が求められているわけではない。

☞第一部 4. ステップ 7 及びステップ 9 **g)**

なお、言うまでもないが、セキュリティ度を高めたいからといって、例えば消防法等の法令に違反する設備を構築するようなことがあってはならない。

2 注意事項

個人情報保護法では、安全管理の対象は個人データであって、個人情報ではない。一方、JIS では個人情報を安全管理の対象としている。ここにこそ、安全管理についての JIS の思想が現れていると言える。個人情報は、そのライフサイクルの過程で、記録媒体が変わったり増えたり個人データになったりと形を変えていく。そういった状況に応じてリスクを認識し、分析し、対策を講じることを JIS では求めているのである。

3.3.3 において講じることとする対策の具体的な考え方については、経済産業分野ガイドラインが参考になる。ただし、事業者は、リスクなどの認識、分析及び対策（**3.3.3**）により講じることとした対策をルールとして定め運用しているはずであり、事業者の規模や業務内容により安全管理措置のレベルが異なって当然である。事業者によっては、これでは多すぎる場合もあるし、不足する場合もある。事業者は、規模や業務内容に応じ、必要かつ十分な措置を講じる必要がある。

なお、個人情報保護法第 20 条の安全管理措置には、内容として、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置が含まれると解されているが、JIS では他の要求事項においてすでに組織的安全管理措置と人的安全管理措置については言及されているため、この **3.4.3.2** 項でいう安全管理措置では、物理的安全管理措置及び技術的安全管理措置が対象となる。

3 個人情報保護法との対応

①個人情報保護法第 20 条（安全管理措置）

4 審査の項目と着眼点

事業者は，リスクなどの認識，分析及び対策(3.3.3)に基づき，個人情報のライフサイクルの観点から，以下に例示するような対策を決定することとなろう。

取扱いの局面	対策（例）
1. 取得・入力	**(1) 作業責任者の明確化** ① 個人情報を取得する際の作業責任者の明確化 ② 取得した個人情報を情報システムに入力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 ① 取得・入力する際の手続の明確化 ② 定められた手続による取得・入力の実施 ③ 権限を与えられていない者が立ち入れない建物，部屋での入力作業の実施 ④ 個人情報を入力できる端末の，業務上の必要性に基づく限定 ⑤ 個人情報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，個人情報を入力できる端末では，CD-ROM，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) 作業担当者の識別，認証，権限付与 ① 個人情報を取得・入力できる作業担当者の，業務上の必要性に基づく限定 ② 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 ③ 作業担当者に付与する権限の限定 ④ 個人情報の取得・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 ① 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 ② 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** ① 個人情報を移送・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 ① 個人情報を移送・送信する際の手続の明確化 ② 定められた手続による移送・送信の実施 ③ 個人情報を移送・送信する場合の個人情報の暗号化等の秘匿化（例えば，公衆回線を利用して個人情報を送信する場合） ④ 移送時における宛先確認と受領確認（例えば，簡易書留郵便その他個人情報が含まれる荷物を郵送する特定サービスの利用） ⑤ FAX 等における宛先番号確認と受領確認 ⑥ 個人情報を記した文書を FAX 等に放置することの禁止 ⑦ 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 ① 個人情報を移送・送信できる作業担当者の，業務上の必要性に基づく限定 ② 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 ③ 作業担当者に付与する権限の限定（例えば，個人情報をコンピューターネットワークを介して送信する場合，送信する者は個人情報の内容を閲覧，変更する権限は必要ない。） ④ 個人情報の移送･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 ① 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 ② アクセスの記録，保管と権限外作業の有無の確認

取扱いの局面	対策（例）
3. 利用・加工	**(1) 作業責任者の明確化** ① 個人情報を利用・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 ① 個人情報を利用・加工する際の手続の明確化 ② 定められた手続による利用・加工の実施 ③ 権限を与えられていない者が立ち入れない建物，部屋での利用・加工の実施 ④ 個人情報を利用・加工できる端末の，業務上の必要性に基づく限定 ⑤ 個人情報を利用・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，個人情報を閲覧だけできる端末では，CD-ROM，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) 作業担当者の識別，認証，権限付与 ① 個人情報を利用・加工できる作業担当者の，業務上の必要性に基づく限定 ② 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 ③ 作業担当者に付与する権限の限定（例えば，個人情報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，個人情報の複写，複製を行う権限は必要ない。） ④ 個人情報の利用・加工業務を行う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）の記録
	(4) 作業担当者及びその権限の承認 ① 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 ② 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** ① 個人情報を保管・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 ① 個人情報を保管・バックアップする際の手続の明確化 ② 定められた手続による保管・バックアップの実施 ③ 個人情報を保管・バックアップする場合の個人情報の暗号化等の秘匿化 ④ 暗号鍵やパスワードの適切な管理 ⑤ 個人情報を記録した媒体を保管する場合の施錠管理 ⑥ 個人情報を記録している媒体の遠隔地保管 ⑦ 個人情報を入力できる端末の，業務上の必要性に基づく限定 ⑧ 個人情報のバックアップから迅速に個人情報が復元できることのテストの実施 ⑨ 個人情報のバックアップに関する各種事象や障害の記録 ※ 情報システムで個人情報を処理している場合は，個人情報のみならず，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。
	(3) 作業担当者の識別，認証，権限付与 ① 個人情報を保管・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 ② 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 ③ 作業担当者に付与する権限の限定（例えば，個人情報をバックアップする場合，その作業担当者は個人情報の内容を閲覧，変更する権限は必要ない。） ④ 個人情報の保管・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）の記録
	(4) 作業担当者及びその権限の確認 ① 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 ② アクセスの記録，保管と権限外作業の有無の確認

取扱いの局面	対策（例）
5. 消去・廃棄	**(1) 作業責任者の明確化** ① 個人情報を消去する際の作業責任者の明確化 ② 個人情報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 ① 個人情報を消去・廃棄する際の手続の明確化 ② 定められた手続による消去・廃棄の実施 ③ 権限を与えられていない者が立ち入れない建物，部屋での消去・廃棄作業の実施 ④ 個人情報を消去できる端末の，業務上の必要性に基づく限定 ⑤ 個人情報が記録された媒体や機器をリース会社に返却する前の，個人情報の完全消去（例えば，意味のない情報を媒体に 1 回又は複数回上書きする。） ⑥ 個人情報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 ① 個人情報を消去・廃棄できる作業担当者の，業務上の必要性に基づく限定 ② 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 ③ 作業担当者に付与する権限の限定 ④ 個人情報の消去・廃棄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 ① 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 ② アクセスの記録，保管と権限外作業の有無の確認

事業者が講じることとした具体的な対策が適切に実施されているかどうかが審査の対象となる。講じることとした対策は、内部規程(3.3.5)の g)（個人情報の適正管理に関する規定）の一つとしてとりまとめなければならない。

なお、経済産業分野ガイドラインに記述されているように、対策には、必ず実施することが求められる事項がある。

以下のⅠ.及びⅡ.に、実施しなければならない事項と、それを実施するために望ましい手法を例示する。

取り扱う個人情報の量や内容は事業者ごとに異なるので、講じなければならない事項を実施する手法も事業者の判断により異なって当然であり、**ここに示されている手法を一律に実施するよう求めるものではない。**

事業者はここに示されている手法を参考に、必要に応じて、自らに合った方法で実施すればよい。

Ⅰ．物理的安全管理措置として講じなければならない事項と望ましい手法の例示

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
1.入退館（室）管理の実施	(1) 建物、室、サーバー室、個人情報の取扱い場所への入退を制限していること。	① IC カード認証や生体認証など、機械的なシステムによる認証を導入しており、それぞれの場所について、業務上必要な者のみに入退の権限を与えている。また、人事異動や退職者等に合わせ、遅滞なく設定を見直している。 ② ナンバーキーにより入退を制限している。ナンバーキーは、定期的及び随時（人事異動や退職者が出た場合等）にキー番号を変更している。 ③ ID カードの提示により入退を制限している。 ④ 通常は施錠し、必要な都度、鍵管理者の承認を得て鍵を開けている。 ⑤ 予備の鍵（IC カード等含む）を適正に管理している。 ⑥ 非常口は内部から施錠している。 ⑦ 従業者には、ID カードを常時携帯（着用）させている。 ⑧ 来訪者には、来訪者であることが一目で分かるような入館証を着用（携帯）させている。 ⑨ 監視カメラを作動させている。 ⑩ 従業者と事前の約束のない来訪者は受け入れない。 ⑪ 来訪者を受け入れる場合は、必ず従業者が帯同する。 ⑫ 来訪者を受け入れる場合は、あらかじめ定めた区域内のみを案内する。 ⑬ 来訪者をセキュリティ度の高い区域に案内する必要がある場合は、守秘義務についての誓約書を取得する。 ※ 一つの室に複数の事業者が同居しているからといって不適合ではない。同居することのリスクをどのように評価し対策を講じているかが問われる。例えば、パーティションで区切るという措置も、必要性を判断した上で実施の採否を決定すればよい。 運用確認のためのエビデンス ・入退館（室）の制御機構 ・従業者の ID カード ・外来者に貸与する入館証 ・鍵（IC カード等含む。）を貸与している者を管理している記録
	(2) 建物、室、サーバー室、個人情報の取扱い場所への入退の記録を取り、保管していること。	① 個人情報を取り扱うそれぞれの場所に関し、従業者、来訪者それぞれについて記録を取り、保管している。 ② 従業者の入退については、最低限、最初と最後の記録は残している。24 時間記録している場合には不要である。 ③ 最終退出時の社内点検（施錠、防火確認等）を実施している。24 時間開いている事業所では不要である。 運用確認のためのエビデンス ・来訪者の入退記録 ・従業者の入退記録 ・最終退出時の社内点検の記録

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(3) 建物、室、サーバー室、個人情報の取扱い場所への入退の記録を定期的にチェックしていること。	① 個人情報を取り扱うそれぞれの場所に関し、従業者、来訪者それぞれについて入退記録を定期的にチェックしている。 ② 最終退出時に施錠、防火等の確認を実施した記録を保管し、定期的にチェックしている。 運用確認のためのエビデンス ・来訪者の入退記録 ・従業者の入退記録 ・最終退出時の社内点検の記録
2.盗難等の防止	(1) 離席時に個人情報を記した書類、媒体、携帯可能なコンピュータ等を机上に放置していないこと。	① 離席時は、机上に個人情報を記録した媒体（紙、電子媒体）や携帯可能なコンピュータ等を放置せず、引出しやキャビネット等に施錠保管する。 運用確認のためのエビデンス ・個人情報を取り扱う室内の状況
	(2) 個人情報を取り扱うコンピュータの操作において、離席時は、パスワード付きスクリーンセーバーの起動又はログオフを実施していること。	① 個人情報を取り扱うコンピュータの操作において離席時は、ログオフやパスワード付きスクリーンセーバーの起動を行っている。 ② スクリーンセーバー起動までの時間は、業務の内容に応じ合理的な範囲で定めている。 ③ USB キーがなければコンピュータを操作できないよう設定しており、離席時は必ず USB キーを抜いている。 運用確認のためのエビデンス ・コンピュータの設定 ・個人情報を取り扱う室内の状況
	(3) 個人情報を記録した媒体（紙、外部記録媒体）は施錠保管していること。	① 個人情報を記録した紙媒体や USB メモリ、CD-ROM 等の外部記録媒体は、施錠保管している。 ② 施錠保管では、あるべきものが全てそこにあるかについて管理している。例えば、外部記録媒体を保管している場合において、何か無くなっても容易に気がつかないような管理状況ではない。 ③ 個人情報を施錠保管しているキャビネット等は、中が見えないようになっており、また内容物を表示するラベル等を貼付していない。表示する場合は、従業者にしか分からない記号にする等の措置を講じている。 運用確認のためのエビデンス ・個人情報を記録している媒体を施錠保管している保管庫等 ・現在保管しているものを把握している記録
	(4) 個人情報を記録した媒体の保管場所の鍵は特定者が管理していること。	① 鍵は特定者が管理している。 ② 特定者の数は最小限である。 ③ 予備の鍵についても、適切な管理を行っている。 運用確認のためのエビデンス ・鍵を貸与している者を管理している記録

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(5) 個人情報を記録した媒体（紙、外部記録媒体）の廃棄は、再利用できない措置を講じていること。	① 保管期間が経過した個人情報を確実に消去・廃棄・返却している。 ② 個人情報を記録した媒体は、媒体の種類ごとに確実に消去・廃棄・返却している。 ③ 個人情報を記録した外部記録媒体を物理的に破壊しない場合、完全消去の措置を取っており、その方法が明示できる。 ④ 個人情報を消去・廃棄・返却した記録を取り、その記録を一定期間保管している。 ⑤ 委託先等、外部の者に消去・廃棄させる場合、廃棄証明等を取得している。 ⑥ 個人情報が記録された機器（コンピュータ、コピー機等）や媒体をリース業者やレンタル業者等へ返却するとき、データを完全消去しており、その方法が明示できる。契約によりリース業者等による完全消去義務を定めることでもよい。 ⑦ 保管している個人情報を誤廃棄しないための手順があり、遵守している。 ⑧ 法令等で保管期間が定められた個人情報を誤って保管期間満了前に消去・廃棄しないための対策がある。 ⑨ 個人情報が記載された書類の裏面を使用していない。 運用確認のためのエビデンス ・シュレッダーの存在 ・個人情報を管理する台帳等に登録している個人情報についての廃棄の記録 ・廃棄を委託している場合、廃棄証明書等
	(6) 個人情報を記録した携帯可能なコンピュータ等について、盗難防止措置を講じていること。	① 携帯可能なコンピュータや外付けハードディスクに個人情報を保管している場合、チェーンロック又は帰宅時のキャビネット等への施錠保管を行っている。 ② 業務で使用する携帯電話については、取扱いルールを定め、ルールを遵守している（肌身離さない携行、落下防止ストラップの装着等の紛失防止策、ナンバーロックの実施、リモートロック等）。 ※ 私物の携帯電話を業務に使うことを認めている場合は、事業者と従業者間で取扱いのルールについて合意していることが望ましい。ルールを作るに当っては、事業者は従業者のプライバシーに配慮する必要がある。 運用確認のためのエビデンス ・携帯可能なコンピュータ等の盗難防止措置の状況 ・携帯電話の取扱い手順等

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(7) 携帯可能なコンピュータや USB メモリ、CD-ROM 等の外部記録媒体の利用についてルールを定め、それを遵守していること。	① 携帯可能なコンピュータや USB メモリ、CD-ROM 等の外部記録媒体の利用、持出し、持込みの際のルールを定め、遵守している。 ② 外部記録媒体を社外へ持ち出すときや社内に持ち込む（持出しの返却を含む。）ときは、必要に応じて暗号化等の秘匿化やウイルスチェック等を実施することもルールに含め、遵守している。 ③ 外部記録媒体を利用できる端末を限定している。 運用確認のためのエビデンス ・個人情報を取り扱う室内の状況 ・携帯可能なコンピュータ、USB メモリや CD-ROM 等の外部記録媒体の取扱い手順等 ・外部記録媒体を利用できる端末
	(8) 個人情報を取り扱う情報システムの操作マニュアルを机上に放置していないこと。	① 個人情報を取り扱う情報システムの操作マニュアルを保管する場所を定め、使用後は必ずそこに返却している。 ② 個人情報を取り扱う情報システムの操作マニュアルは電子化している。 運用確認のためのエビデンス ・個人情報を取り扱う室内の状況

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
3.機器・装置等の物理的な保護	(1) 個人情報を取り扱う機器・装置等について、安全管理上の脅威（盗難、破壊、破損等）や環境上の脅威（漏水、火災、停電、地震等）から物理的に保護する装置を導入していること。	① 個人情報を取り扱う機器・装置等は、サーバー室やサーバーラック等に施錠保管し、物理的に保護している。 ② 個人情報を取り扱う機器・装置等には無停電電源装置（UPS）を設置している。 ③ 個人情報を取り扱う機器・装置等を保管する部屋には、耐火（消火）設備を用意している。 ④ 個人情報を取り扱う機器・装置等を保管する部屋について、室温管理を実施している。 ⑤ 具体的な期間を定め、定期的にバックアップを保管している。 ⑥ バックアップは、数世代を保管している。 ⑦ バックアップする場合、暗号化等の秘匿化の措置を講じている。 ⑧ バックアップした媒体は施錠保管している。 ⑨ バックアップした媒体は、遠隔地に保管している。 ⑩ 情報システムの OS やアプリケーションのバックアップも保管している。 ⑪ バックアップから迅速に個人情報が復元できることのテストを実施している。 ⑫ バックアップに関する各種事象や障害について記録している。 ※1 個人情報を取り扱う機器・装置等は、サーバー室やサーバーラック等に施錠保管していることが必要であるが、事業者の規模、取り扱う個人情報の量や質、あるいはオフィスそのものの高い機密性の確保といったことを総合的に勘案し、サーバー室やサーバーラックが必要でない場合もある。ただし、そのような場合であっても、安全管理上の脅威（盗難、破壊、破損等）や環境上の脅威（漏水、火災、停電、地震等）からの物理的な保護装置が必要であることに変わりはない。 ※2 サーバー室を事務消耗品などをストックしておく倉庫として利用し、情報システムの管理に関係のない者が頻繁に入退室する環境は好ましくない。 ※3 バックアップの要否は、復旧の容易性やコスト等を勘案して事業者で判断することである。 運用確認のためのエビデンス ・個人情報を取り扱う機器・装置等の保護状況 ・バックアップを保管している媒体 ・バックアップを保管している媒体の保管状況 ・バックアップの実施記録 ・バックアップの復元テストの記録

Ⅱ．技術的安全管理措置として講じなければならない事項と望ましい手法の例示

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
1.個人情報へのアクセスにおける識別と認証	(1) 個人情報へのアクセスにおいて、識別情報（ID、パスワード等）による認証を実施していること。	① 個人情報へのアクセスにおいて、識別情報（ID、パスワード、生体情報等）による認証を実施している。 運用確認のためのエビデンス ・アクセス権限表 ・個人情報を取り扱うコンピュータ、サーバー等の設定
	(2) 個人情報を格納した情報システムについて、デフォルトの設定を必要に応じて適切に変更していること。	① 個人情報を格納した情報システムについて、デフォルトの設定を必要に応じて適切に変更している（例えば、パスワードや SNMP コミュニティ文字列の変更、不要なアカウントの削除）。 ② 不要な付加機能（スクリプト、ドライバーなど）を無効にしている。 ※ ここでいう「デフォルトの設定」とは、メーカー出荷時の初期状態のままという意味である。 運用確認のためのエビデンス ・個人情報を取り扱うコンピュータ、サーバー等の設定
	(3) 識別情報の発行・更新・廃棄は、ルールに従っていること。	① 識別情報（ID、パスワード等）の発行・更新・廃棄は、ルールに従って行っている。 ② 人事異動や退職時等、アカウントの発行・更新・廃棄は適時実施している。 ※ 識別情報の対象としては、クライアントコンピュータ起動、ネットワーク接続、電子メール、グループウェア、ファイルサーバー、業務処理システム等のアカウント等がある。 運用確認のためのエビデンス ・識別情報（ID、パスワード等）の発行や廃棄の申請書等の記録
	(4) 識別情報を平文で記録していないこと。	① 識別情報は暗号化等の秘匿化の措置を講じて保管している。 ② 識別情報を平文で記録している場合、施錠保管する等の措置を実施している。 運用確認のためのエビデンス ・識別情報（ID、パスワード等）の保管状況

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(5) 識別情報の設定及び利用は、ルールに従っていること。	① パスワードの有効期限を設定している。 ② 同一又は類似パスワードの再利用を制限している。 ③ 最低パスワード文字数を設定している。 ④ パスワードの設定方法（文字、数字、記号を必ず混ぜて設定する等）を定めている。 ⑤ 一定回数以上ログインに失敗した ID の停止等の措置を講じている。 運用確認のためのエビデンス ・個人情報を取り扱うコンピュータ、サーバー等の設定 ・個人情報へのアクセス状況に関する記録
	(6) 個人情報へのアクセス権限を有する従業者が使用できる端末又はアドレス等について制限していること。	① 個人情報へのアクセス権限を有する従業者が使用できる端末又はアドレス等について、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により制限している。 運用確認のためのエビデンス ・個人情報を取り扱うコンピュータ、サーバー等の設定 ・個人情報へのアクセス状況に関する記録 ・ネットワーク構成図等
2.個人情報へのアクセス制御	(1) 個人情報にアクセスできる従業者の数は必要最小限にしていること。	① 個人情報にアクセスできる従業者の数を必要最小限にしている。 ※ 小規模事業者の場合、従業者全員がアクセス権をもたなければ業務が成り立たないこともあろう。それを否定するものではない。 運用確認のためのエビデンス ・アクセス権限表等
	(2) 個人情報にアクセスできる識別情報を複数人で共用していないこと。	① 個人情報にアクセスできる識別情報を複数人で共用することを禁止している。 ② 個人情報にアクセスできる識別情報を複数人で共用することが必要な場合は、共用者を最小限に特定し、利用状況を把握している。 運用確認のためのエビデンス ・アクセス権限表等
	(3) 従業者に付与するアクセス権限は必要最小限にしていること。	① 従業者に付与するアクセス権限は必要最小限である。 ※ 小規模事業者の場合、従業者全員が完全なアクセス権を持たなければ業務が成り立たないこともあろう。それを否定するものではない。 運用確認のためのエビデンス ・アクセス権限表等

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(4) 個人情報を格納した情報システムの同時利用者数を制限していること。	① 個人情報を格納した情報システムの同時利用者数を制限している。 ※ 情報システムへの負荷を問題とする必要がないのであれば不要である。 運用確認のためのエビデンス ・情報システムへのアクセスの記録等
	(5) 個人情報を格納した情報システムの利用時間を制限していること。	① 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などの措置を講じている。 ※ 24 時間年中無休で稼働させている場合は不要である。 運用確認のためのエビデンス ・情報システムへのアクセスの記録等
	(6) 個人情報を格納した情報システムを無権限アクセスから保護していること。	① ファイアウォール、ルーター等の設定を行い、個人情報を格納した情報システムを無権限アクセスから保護する措置を講じている。 ② 個人情報データベースを公開セグメント（DMZ）に配置していない。 運用確認のためのエビデンス ・社内ネットワーク図等
	(7) 個人情報にアクセス可能なアプリケーションの無権限利用を防止していること。	① アプリケーションシステムに認証システムを実装している。 ② 担当者ごとに業務上必要なソフトウェアのみインストールしている。 ③ 担当者ごとに業務上必要な機能のみメニューに表示させている。 ④ 個人情報の入力や利用･加工を行う端末を限定している。 ⑤ 個人情報を取り扱う端末には、必要以上の機能を付加しない。 運用確認のためのエビデンス ・個人情報を取り扱う室内での業務の状況
	(8) 個人情報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を検証していること。	① 個人情報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を検証している。 ② ウェブアプリケーションの脆弱性の有無を検証している。 運用確認のためのエビデンス ・導入したアクセス制御機能の有効性を検証した記録

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
3.個人情報へのアクセス権限の管理	(1) 個人情報にアクセスできる者を許可する権限管理を適切かつ定期的に実施していること。	① 個人情報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定期的に十分に審査し、その者だけが行えるようにしている。 ② 個人情報にアクセスする者の登録を行う作業担当者が自分のために設定したアクセス権について、定期的に第三者が点検している。 運用確認のためのエビデンス ・作業担当者を審査した記録
	(2) 個人情報を取り扱う情報システムへのアクセスは必要最小限であるよう制御していること。	① 個人情報を取り扱う情報システムへのアクセスは必要最小限にしている。 ※1 例えば、個人情報を移送･送信する作業を行うだけの者には、個人情報の内容を閲覧、変更する権限を付与しない。 ※2 例えば､個人情報を閲覧することのみが業務上必要とされる者には、個人情報の複写、複製を行う権限を付与しない。 ※3 例えば､個人情報をバックアップする作業を行うだけの者には、個人情報の内容を閲覧、変更する権限を付与しない。 ※4 例えば、個人情報を入力する作業を行うだけの者には、個人情報の内容を出力する権限を付与しない。 運用確認のためのエビデンス ・アクセス権限表等 ・個人情報を取り扱う情報システムにアクセスできる端末 ・情報システムの利用者による実際の操作
4.個人情報へのアクセスの記録	(1) 個人情報へのアクセスや操作の成功と失敗の記録を取得し､保管していること。	① 個人情報へのアクセスや操作の成功と失敗についての記録を取得し、保管している。 ② 情報システムのアクセスログについては、利用者の人数や利用状況、情報システムで取り扱う個人情報を考慮して取得している。個人情報へのアクセスや操作を記録できない場合は、情報システムへのアクセスの成功と失敗の記録を取得している。 ③ 漏えいは内部犯行である場合が多い。また、発覚するまで数ヶ月以上を要することがある。したがって、正当なアクセスの記録について、ある程度の期間は保管している（ただし期間は一概には定められない)。 ④ 個人情報を保管している情報システムやネットワークへのアクセスログを定期的にチェックしている。 ⑤ 情報システムのアクセスログから内部の異常アクセス（例えば、休業日、業務時間外のアクセス、ログインエラー等）をチェックしている。 ⑥ ウェブサーバーのアクセスログから外部の不正アクセスをチェックしている。 運用確認のためのエビデンス ・個人情報へのアクセスや操作の成功と失敗の記録（または情報システムへのアクセスの成功と失敗の記録) ・アクセスログの項目、保管期間の記録

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
	(2) 取得した記録について、漏えい、滅失及びき損から適切に保護していること。	① 取得した記録は、施錠保管している。 ② 取得した記録は、暗号化やパスワードロック等の秘匿化等の措置を講じて保管している。 ※ 個人情報を取り扱う情報システムへのアクセス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。 運用確認のためのエビデンス ・個人情報へのアクセスや操作の成功と失敗の記録（または情報システムへのアクセスの成功と失敗の記録）の保管状況
5.個人情報を取り扱う情報システムに関する不正ソフトウェア対策	(1) ウイルス対策ソフトウェアを導入していること。	① 個人情報を取り扱う情報システム（コンピュータ、サーバー等）にはウイルス対策ソフトウェアを導入している。 ② ウイルス対策ソフトウェアは、常に最新のパターンファイルを適用している。 運用確認のためのエビデンス ・個人情報を取り扱うコンピュータ、サーバー等
	(2) OSや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）を適用していること。	① OS や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）を適用している。 ※1 システムによっては、パッチを適用することで動作がおかしくなることがある。必要性を判断した上で適用/不適用を実施すれば良い。 ※2 メーカーがサポートを終了した OS（Windows98 等）やアプリケーションを使用することはリスクが大きい。 運用確認のためのエビデンス ・個人情報を取り扱うコンピュータ、サーバー等
	(3) 不正ソフトウェア対策の有効性・安定性を確認していること。	① どのような不正ソフトウェアが存在するか、状況を把握している。 ② パターンファイルや修正ソフトウェアによる更新後に、有効性や動作の安定性を確認している。 ※ 不正ソフトウェア及びその対策についての最新情報は、独立行政法人情報処理推進機構（**IPA**）のウェブサイト等を参考にすると良い。 運用確認のためのエビデンス ・個人情報を取り扱うコンピュータやサーバー等について、有効性・安定性を確認した記録
	(4) 個人情報にアクセスできる端末にファイル交換ソフトウェア（Winny、Share、Cabos 等）をインストールしていないこと。	① 個人情報にアクセスできる端末の利用者に、ソフトウェアをインストールする権限を与えていない。 ② 自宅での作業を認めている場合、自宅のコンピュータについてもファイル交換ソフトウェア（Winny、Share、Cabos 等）をインストールしていないことを条件としている。

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
		運用確認のためのエビデンス ・個人情報を取り扱うコンピュータ、サーバー等の点検記録
6.個人情報の移送・通信時の対策	(1) 個人情報の受渡しには授受の記録を残していること。	① 個人情報を記録した媒体を社外（顧客、委託先等）や社内の遠隔地事業所と手渡ししたり、郵便、宅配便等で授受するとき、責任の所在の明確化や紛失した場合の追跡等のため、授受記録を取り保管している。 ※ 授受の記録は互いの責任範囲を明確にするものであるから、双方が確認した記録であることが望ましい。 運用確認のためのエビデンス ・受渡しの際の授受の記録
	(2) 個人情報を媒体で移送するときに、移送時の紛失・盗難が生じた際の対策を講じていること。	① 個人情報を記録した媒体を郵便、宅配便、社用車等で送付するとき、宛先記載ミス、誤封入、誤送付等を防止するため、宛先や送付物を確認している。 ② 送付する個人情報の重要度に応じて、適切な送付手段（社用車、セキュリティ便、書留、配達証明、本人限定受取郵便等）を採用している。 ③ 個人情報が記録された媒体を社用車その他の交通機関を利用して運搬するとき（自宅に持ち帰る場合を含む）は、運搬ルールを遵守している。 ④ 個人情報が記録された媒体の運搬時（自宅に持ち帰る場合を含む）に紛失、車上荒し、置引き、ひったくり等の予防策を個人情報の重要度に応じて実施している。例えば、専用かばんの使用、運搬車両の施錠、肌身離さない携行、運搬途中立寄らないことを励行しているなど。 ⑤ 個人情報の重要度やリスクに応じて、暗号化やパスワードロック等の秘匿化の措置を講じている。 運用確認のためのエビデンス ・移送される媒体 ・運搬ルールの実施状況 ・授受確認のルールの実施状況（授受記録の確認）
	(3) 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）で個人情報を送信する際に、個人情報の暗号化又はパスワードロック等の秘匿化の措置を講じていること。	① ウェブサイトで本人に個人情報を入力させる場合、SSL、SQL インジェクション、クロスサイトスクリプティング対策等の措置を実施している。 ② SSL 等の措置を取っている場合、cookie も暗号化している。 ③ ウェブサイトで個人情報を送受信する場合、電子メールの添付ファイルで送受信する場合や、FTP でファイル転送する場合は、それぞれ暗号化やパスワードロック等の秘匿化の措置を講じている。 ④ パスワードロックを行う場合、パスワードの設定方法（文字数や文字・記号・数字の使用等）やパスワードの通知方法についてルールを定め、それを遵守している。 ⑤ 個人情報を電子メールで送信するとき、誤送信を防止するため、宛先や送信内容を確認するルールを定め、遵守している。 ⑥ 電子メールを社外の複数宛先に同時に送信するときは、その宛先は BCC を使用したり、宛先を伏せて送信できるようにするシステムやツールを利用するなどの対策を

講じなければならない事項		望ましい手法の例示（具体的な対策の例）
		実施している。 運用確認のためのエビデンス ・個人情報を取り扱うコンピュータ、サーバー等 ・本人の個人情報入力を受け付けているウェブサイト画面 ・複数宛先に同時送信する場合の対策
7.個人情報を取り扱う情報システムの動作確認時の対策	(1) 情報システムの動作確認時のテストデータとして個人情報を利用していないこと。	① 情報システムの動作確認時のテストデータとして個人情報を利用することを禁止している。 ② やむを得ず個人情報をテストデータとして利用する場合、利用できる条件が明確であり、それに従っている。 運用確認のためのエビデンス ・テストデータの取扱状況 ・個人情報をテストデータに利用する条件を満たしている記録
	(2) 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を検証していること。	① 情報システムの変更時に、情報システム又は運用環境のセキュリティが変更前と同等以上に維持されていることを検証している。 ② 不要になったシステム機能が残存していないか確認している。 ③ システム変更によりウェブサイトやモバイルサイトに公開すべきでない個人情報が閲覧できるようになっていないか公開前に確認している。 運用確認のためのエビデンス ・本格運用前に検証した記録
8.個人情報を取り扱う情報システムの監視	(1) 個人情報を取り扱う情報システムの使用状況を定期的にチェックしていること。	① 個人情報を取り扱う情報システムの使用状況を定期的にチェックしている。 ※ 個人情報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。 運用確認のためのエビデンス ・個人情報を取り扱う情報システムの使用状況を定期的にチェックしている記録
	(2) 個人情報へのアクセス状況（操作内容を含む。）を定期的にチェックしていること。	① 個人情報へのアクセス状況（操作内容を含む。）を定期的にチェックしている。 ※ 個人情報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。 運用確認のためのエビデンス ・個人情報へのアクセス状況を定期的にチェックしている記録

3.4.3.3 従業者の監督

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報を取り扱う業務に携わる従業者に対する適切な監督を求めている。

従業者との雇用契約時又は委託契約時に非開示契約を締結している必要がある。従業者の場合、就業規則（雇用契約の内容である）に盛込まれて規定されていれば、非開示契約を締結していることになる。通常、就業規則では非開示の対象は「個人情報」に限られず業務上知り得た機密情報一般が対象になっていると思われるが、非開示の対象に個人情報が含まれる旨が認識されていれば、特に「個人情報」と明示されていなくてもよい。

2 注意事項

受入派遣社員等（受託により客先で勤務する者を含む。）は、すでに自らが所属する事業者と秘密保持の契約を締結し、また当該事業者は派遣を受入れる事業者との間で秘密保持の契約を締結していることが通常である。したがって、派遣元との間で非開示契約を締結することも、人的安全管理措置のひとつといえる。

また、ビデオ及びオンラインによる従業者のモニタリングを実施する場合、以下の事柄に留意して実施する必要がある。

- モニタリングの目的、すなわち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。

従業者の監督という点では、「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 27 年厚生労働省告示第 454 号）第 10 の 1 に規定する「雇用管理情報の取扱いに関する重要事項」に該当するものについては、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旨、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旨が記述されているので注意する必要がある。経済産業分野ガイドラインによれば、従業者のモニタリングの実施はこの指針でいう重要事項に該当する。

3 個人情報保護法との対応

①個人情報保護法第 21 条（従業者の監督）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 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旨を JIS に従い規定していること。	(1) 従業者に対し必要かつ適切な監督を行っていること。	【文書審査】 ① 従業者に対し必要かつ適切な監督を行う旨を記述していること。 【現地審査】 ① この項目はそれぞれの要求事項において審査される。
2. 従業者との雇用契約時又は委託契約時に、個人情報の非開示契約を締結するように規定していること。	(1) 従業者との雇用契約時又は委託契約時に、個人情報の非開示契約を締結していること。	【文書審査】 ① 従業者と個人情報の非開示契約を締結するように記述していること。または、就業規則に業務上知り得た情報の非開示の義務が規定していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 従業者の採用時に非開示契約を締結していること。ただし「誓約書」のような書面でなく、就業規則（雇用契約の内容）に盛込まれて規定されていれば、非開示契約を締結していることになる。 ※ 受入派遣社員等（受託により客先で勤務する者を含む。）は、すでに自らが所属する事業者と守秘義務の契約を締結し、また当該事業者は、派遣を受り入れる事業者との間で守秘義務の契約を締結していることが通常である。したがって、派遣を受け入れる場合には、更に受入派遣社員等個々人と守秘義務契約を締結する必要はない。 <u>運用確認のためのエビデンス</u> ・就業規則 ・非開示契約の締結を確認できる記録
3. 雇用契約または委託契約等を締結する場合、非開示条項は、契約終了後も一定期間有効とするよう規定していること。	(1) 雇用契約または委託契約等において､非開示条項は､契約終了後も一定期間有効であるように定め締結していること。	【文書審査】 ① 非開示契約において、非開示条項は、契約終了後も一定期間有効であるよう記述していること。または、就業規則に業務上知り得た情報の非開示の義務が一定期間有効であるよう記述していること。 【現地審査】 ① 雇用契約において、非開示条項は、契約終了後も一定期間有効であるように定め締結していること。 ※1 「誓約書」のような書面でなく、就業規則（雇用契約の内容である）に

文書審査の項目	現地審査の項目	審査の着眼点
		盛込まれて規定されていれば、締結していることになる。 ※2 秘密保持義務の存続期間については可能な限り期限を設定することが望ましい。 ※3 秘密保持義務の存続期間の設定が困難な場合は、（秘密性が失われるまで）無期限とすることも可能であるが、情報が公知になって秘密性を失ったときは、元従業者からの問合せがあれば誠実に回答するなどの対策を講じることが望ましい。 運用確認のためのエビデンス ・就業規則 ・非開示契約の締結を確認できる記録
4. 個人情報保護マネジメントシステムに違反した場合の措置に関する規程を整備していること。	(1) 個人情報保護マネジメントシステムに違反した場合､規程に従って措置を実施していること。	【文書審査】 ① 違反となる要件は、従業者が確実に理解できるよう明確に記述していること。 ② 措置の内容が、確実に実施できるよう明確に記述していること。 ※ 「就業規則」に定めた懲戒処分が適用される旨を規定していても良い。 【現地審査】 ① 規程に従い、措置を実施していること。 運用確認のためのエビデンス ・個人情報保護マネジメントシステムに違反した場合に措置を実施した記録
5. ビデオ及びオンラインによる従業者のモニタリングを実施する場合、その措置の実施について規定していること。	(1)モニタリングの目的をあらかじめ特定し、従業者に明示していること。	【文書審査】 ① モニタリングの目的をあらかじめ特定し､従業者に明示する手順を記述していること。 ※ モニタリングの目的とは､モニタリングによって取得する個人情報の利用目的のことである。 【現地審査】 ① 定めた手順に従い実施していること。 運用確認のためのエビデンス ・モニタリングの目的を従業者に明示しているもの

文書審査の項目	現地審査の項目	審査の着眼点
	(2) モニタリングの実施に関する責任者とその権限を定めていること。	※ この項は、資源、役割、責任及び権限(**3.3.4**)において審査される。
	(3) 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し、事前に社内に徹底していること。	【文書審査】 ① モニタリングの実施について定めた社内規程案を、モニタリングの実施前に、社内に徹底する手順を記述していること。 【現地審査】 ① 定めた手順に従い実施していること。 運用確認のためのエビデンス ・モニタリングの実施前に社内規程案を社内に徹底したことが分かる記録
	(4) モニタリングの実施状況について、適正に行われているか監査又は確認を行っていること。	※ この項は、運用の確認(**3.7.1**)又は監査(**3.7.2**)において審査される。

3.4.3.4 委託先の監督

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報を取り扱う業務を委託する場合に実施すべき事項を定めている。ただし、仮に委託先で漏えい等の事故が起きた場合、これらの措置を講じていたからといって、委託者は責任を免れるものではない。本人に対して責任を負うのは委託者である。

2 注意事項

人材派遣契約は個人情報の取扱いの委託には含まれず、**3.4.3.4**（委託先の監督）の要求事項の対象外である。

また、清掃事業者、機器のメンテナンス事業者、警備会社等との契約も、個人情報の取扱いを含まない限り、この **3.4.3.4**（委託先の監督）の要求事項の対象外である。ただし、これら清掃事業者等との契約も、広く **3.4.3.2**（安全管理措置）の対象には含まれるため、このような個人情報に触れる可能性がある契約先については、立ち入ることのできる範囲を定めたり、業務上知り得る情報（例えば入退制限の機構）についての守秘義務などを盛り込んだ契約を締結することが望ましい。

委託先が、個人情報が含まれるかどうかを認識することなく委託された情報を取り扱う場合は、契約書が必要であることはもちろんにしても、「個人情報」という文言を契約書に盛り込むことまで求めるものではない。

3 個人情報保護法との対応

①個人情報保護法第 22 条（委託先の監督）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 委託先選定基準を定める手順及び見直しの手順を定めていること。	(1) 定めた手順に従い、委託先選定基準を確立させていること。	【文書審査】 ① 委託先選定基準を定める手順を記述していること。 【現地審査】 ① 定めた手順に従い実施していること。 ※1 委託先選定基準は、委託する業務ごとに作成することが望ましい。 ※2 委託先選定基準は、委託する業務との関連でどのような観点から作成したか、説明できる必要がある。 ※3 個人に委託する場合も委託先選定基準が必要である。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・委託先選定基準
	(2) 委託先選定基準は具体的で運用可能なものであること。	【現地審査】 ① 委託先を選定する基準として、該当する業務については少なくとも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こと。 ※1 「プライバシーマーク申請中」、「プライバシーマーク付与事業者に準じた」、「セキュリティの体制が整備されている」といった文言だけでは具体的な基準とは言えない。 ※2 委託先選定基準について、点数評価による単純な合計点方式を採っている例があるが、零点が許されない必須項目がある場合もあり得る。 ※3 委託者が優越的地位にある場合、受託者に不当な負担を課すことがあってはならない。 運用確認のためのエビデンス ・委託先選定基準
	(3) 必要に応じて委託先選定基準の見直しを実施していること。	【文書審査】 ① 委託先選定基準を見直すタイミングと手順を定めていること。 ※ 委託先選定基準の見直しのタイミングとしては、委託契約の更新時、定期的な再評価の実施時、リスクの認識、分析及び対策を実施したとき等が考えられる。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・委託先選定基準の改訂状況

文書審査の項目	現地審査の項目	審査の着眼点
2. 委託先選定基準により委託先を評価するよう規定していること(定期的な再評価を含む)。	(1) 委託先選定基準により委託先を評価していること(定期的な再評価を含む。)	【文書審査】 ① 委託先の評価を確実に実施するよう、手順を明確に記述していること。 ② 選定した委託先について、具体的な時期を定め定期的な再評価を行う手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② このマネジメントシステム運用開始時の既存の委託先についても、委託先選定基準に従って評価していること。 ③ 委託先を定期的に再評価していること。 ※1 業務を行うためには国が定めた資格が必要で、かつ法律により守秘義務を課されている者(弁護士、社会保険労務士、公認会計士、医師等)は、それだけで選定基準を満たしていると評価でき、委託先選定基準による選定は必須ではない。 ※2 倉庫業、廃棄業、データセンター(ハウジング、ホスティング)等の事業者を委託先とする場合、それら委託先事業者は委託される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としても、委託する側は委託するものが個人情報であることを認識しているのであるから、委託先選定基準による選定が必要である。 <u>運用確認のためのエビデンス</u> ・委託先選定基準により委託先を評価した記録
	(2) 委託先の認識に漏れがないこと。	【現地審査】 ① 個人情報の取扱いを委託している委託先を漏れなく把握していること。 ※1 給与計算、廃棄、名刺の印刷、個人事業主への委託等が認識から漏れやすいので注意が必要である。 ※2 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、**3.4.3.4** の対象外である。これらは広く **3.4.3.2** に含まれるものであり、このような事業者とは、立ち入ることのできる範囲や守秘義務に関する事項を盛込んだ契約を締結することが望ましい。 ※3 健康保険組合や厚生年金基金への社員の個人情報の提供は、法令に基づく第三者提供であって、委託ではない。 ※4 全国銀行協会は、口座振替、給与振込、一般の振込、財形貯蓄制度を事業者から依頼されることについて、受託ではなく第三者提供であるとの統一見解を出しており、すべての銀行はその統一見解に基づき運用して

文書審査の項目	現地審査の項目	審査の着眼点
		いる。したがって、これら金融機関を委託先と認識する必要はない。 運用確認のためのエビデンス ・委託先の一覧表等、個人情報の取扱いを委託している事業者全てを把握していることが確認できる記録
3. a)～g)の内容を盛り込んだ契約書を締結する手順を定めていること。	(1) 定めた手順に従い、委託契約が特定した利用目的の範囲内であることを、あらかじめ管理者に確認していること。	【文書審査】 ① 委託契約の内容が特定した利用目的の範囲内であることについて管理者の承認を得る手順を定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。 ※ 実務的には、個人情報の取扱いの委託が含まれる契約の締結についての稟議が管理者を通るようになっていれば問題ない。 運用確認のためのエビデンス ・利用目的の特定に関する記録 ・契約書
	(2) 定めた手順に従い、a)～g)の内容が盛り込まれた契約書を締結していること。	【文書審査】 ① 個人情報の取り扱いを委託する場合、a)～g)の内容を契約書に盛り込むことを記述し、かつ、規定に基づく契約書雛形を用意していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 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ていること。 －個人情報の漏えい防止、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情報の返還・消去・廃棄に関する事項 ③ c)再委託 に関する事項には、以下の事項が含まれていること。 ・再委託を行うに当たっての委託者への文書による報告 ④ a)～g)の全ての項目が盛りこまれた契約を締結しているのが原則であるが、そうでないからといって即不適合というわけではない。約款によりサービスを提供し個別の契約には応じない受託者も多い。その場合は契約書が取交わせなくても事業者の責任ではない。また、相手が契約に応

文書審査の項目	現地審査の項目	審査の着眼点
		じないこともある。このようなときは、不足している項目があること又は契約が締結できなかったことを残存リスクとして把握し管理していること。 ※1 委託する業務の内容によっては、**a)～g)**の全ての項目を盛り込む必要がない場合がある（委託する業務の内容や業務の実施形態など、取り扱う個人情報のリスクに応じて変わり得る）。 ※2 「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。立入監査は必須ではない。 ※3 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のはもちろんであるが、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。 ※4 委託先が倉庫業、廃棄業、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、それら委託先事業者が、委託される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まで、「個人情報」に関する条項を契約書に盛込むことを要求するものではない。その場合は、「個人情報」という文言のない契約書でかまわない。 ※5 倉庫業、廃棄業、データセンター（ハウジング、ホスティング）等の事業者が約款以外の個別契約に応じない場合、約款に機密保持に関する事項が記載されているかどうか確認することが必要である。確認していなければ審査において不適合となり得る。 ※6 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のであれば、この要求事項の対象外である。ただし **3.4.3.2** の一環として、立ち入ることのできる範囲や守秘義務に関する事項を盛込んだ契約を締結することが望ましい。 ※7 業務を行うためには国が定めた資格が必要で、かつ法律により守秘義務を課され、守秘義務違反に対しては資格剥奪を含む罰則が科せられる者（弁護士、社会保険労務士、公認会計士、医師等）については、契約に基づく民事上の監督よりも厳しい国の監督をすでに受けている。従って、これらの者と **a)～g)**の内容が盛り込まれた契約書を締結することは必須ではない。 <u>運用確認のためのエビデンス</u> ・委託先との契約書

文書審査の項目	現地審査の項目	審査の着眼点
	(3) 契約書の内容を実行していること。	【現地審査】 ① 契約書に規定してある条項を、実施していること。 運用確認のためのエビデンス ・契約に定めた条項を実施していることを確認できる記録（再委託の際の事項等）
4. 当該契約書などの書面を個人情報の保有期間にわたって保存する手順を定めていること。	(1) 定めた手順に従い、当該契約書などの書面を個人情報の保有期間にわたって保存していること。	【文書審査】 ① 個人情報の取扱いを委託する場合、委託終了後も当該個人情報が事業上必要な期間は委託先選定の記録や契約書を保存するよう記述していること。 ※ 記録の管理（**3.5.3**）に対応する規程で規定していてもよい。 【現地審査】 ① 定めた手順に従い実施していること。

3.4.4 個人情報に関する本人の権利

3.4.4.1 個人情報に関する権利

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報を取り扱う事業者に対して本人が開示等を求められた場合、それに応じなければならないのが原則であるが、個人情報の取扱いの委託を受けているに過ぎない場合、本人からの求めがあっても応じる権限はないのが通常であろう。開示等の求めの「すべて」に応じる権限を有するものが対象となる。

2 注意事項

3.4.2.4 により直接書面取得したものだけが開示対象個人情報になると誤解している例が多いので、注意する必要がある。第三者提供により取得した個人情報や公開情報から取得した個人情報も、開示対象個人情報となり得る。

ただし書き **a)**～**d)**については、規格本体付属の解説及び経済産業分野ガイドライン等を参考に、適用基準を定める必要がある。

開示対象個人情報は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、消去までの期間は問わない点が異なる。この点について、「JIS では開示対象個人情報に該当する場合は消去してはいけない」という意味に誤解している事業者があるが、必要があって保有している間は開示等の求めに応じなければならないという主旨であって、不要なものは廃棄すればよい。廃棄したものについて開示等の義務はない。

3 個人情報保護法との対応

①個人情報保護法第 2 条第 5 項（「保有個人データ」の定義）
②施行令第 3 条（保有個人データから除外されるもの）
③施行令第 4 条（保有個人データから除外されるものの消去までの期間）
※ただし施行令第 4 条は本規格では適用せず。

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 開示対象個人情報について、規格のように開示等に応じる旨を規定していること。	(1) 開示等の求めに応じていること。	【文書審査】 ①「開示対象個人情報」の定義および「開示等」の範囲が JIS に定めるように明確であり、かつ、開示等に応じる旨を記述していること。 【現地審査】 ① 本人からの開示等の求めに適切に応じているかどうかは、**3.4.4.2**～**3.4.4.7** において審査される。

文書審査の項目	現地審査の項目	審査の着眼点
	(2) 開示対象個人情報に漏れがないこと。	【現地審査】 ① 開示対象個人情報を漏れなく認識していること。 ※ 開示対象個人情報は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、消去までの期間は問わない点が異なる。 運用確認のためのエビデンス ・開示対象個人情報を管理する台帳等（開示対象個人情報だけを抜き出した台帳は必要でなく、個人情報を管理する台帳等で、分かるように区別されていれば良い。）
2. 開示対象個人情報から除外されるものをただし書きに限定していること。	(1) 開示対象個人情報から除外されるものは、ただし書きに限定していること。	【文書審査】 ① JIS に定める要求事項を、過不足なく記述していること。 【現地審査】 ① 開示対象個人情報から除外されるものは、ただし書きに限定して運用していること。 運用確認のためのエビデンス ・開示対象個人情報を管理する台帳等（開示対象個人情報だけを抜き出した台帳は必要でなく、個人情報を管理する台帳等で、分かるように区別されていれば良い。）
3. ただし書きが適用される場合の承認手順を定めていること。	(1) 定めた手順に従い、管理者の承認を得ていること。	【文書審査】 ① ただし書きを適用する場合について、管理者から承認を得る手順を定めていること。 ※ 管理対象として同一の個人情報の場合、承認は本人毎でなく包括的でよい。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きの適用についての承認に関する記録

3.4.4.2 開示等の求めに応じる手続

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

開示対象個人情報について、本人からの開示等の求めに応じる手続を定めるよう求めている。

2 注意事項

本人から開示等の求めが 1 件もない場合は、「ない」と安心しているのではなく、定めた手順が機能していないために、責任ある立場の者まで本人からの求めが上がってきていないのではないかと疑ってみる必要がある。

確実を期するために本人からの開示等の求めにのみ応じ、代理人による求めには応じない例があるが、それは本人の権利利益を不当に阻害する行為であって許されない。

3 個人情報保護法との対応

①個人情報保護法第 29 条（開示等の求めに応じる手続き）

②施行令第 7 条（開示等の求めを受け付ける方法）

③施行令第 8 条（開示等の求めをすることができる代理人）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. **a**)～**d**)の事項について、応じる手順を、それぞれ規定していること。	(1) **a**) 開示等の求めの申出先について、適切に定めていること。	【文書審査】 ① 開示等の求めの申出先を定めていること。 【現地審査】 ① 本人にとって、申し出先が明確であること。 ② 定めた申出先で受け付けていること。 ③ 実際に誰がどのように行うのか、手順を一通り説明できること。 ※ 「受け付け例なし」の場合でも、手順が機能していないために、責任ある立場の者まで本人の求めが上がらず、結果として受付例がないものと誤認している可能性もあり得る。 運用確認のためのエビデンス ・本人にとって申し出先が明確であることを確認できる記録

文書審査の項目	現地審査の項目	審査の着眼点
	(2) **b)** 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について、適切に定めていること。	【文書審査】 ① 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について定めていること。 【現地審査】 ① 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、様式の整備・入手等、本人の利便を考慮した適切な方式を用意していること。 ② 回答の方法が公平であること。例えば、書面の提出を要求しておきながら回答は口頭で行うといった行為は公平性に反する。ただし、本人が同意した方法であればそれでもよい。 運用確認のためのエビデンス ・開示等の求めに際して提出すべき書面の様式等
	(3) **c)** 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について、適切に定めていること。	【文書審査】 ① 代理人又は本人であることの確認方法について具体的に定めていること。 【現地審査】 ① 代理人による開示等の求めを認めていること。 ② 定めた手順に従い、本人又は代理人であることを確認していること。 運用確認のためのエビデンス ・本人確認の方法
	(4) **d)** **3.4.4.4** 又は **3.4.4.5** による場合の手数料（定めた場合に限る。）の徴収方法について、適切に定めていること。	【文書審査】 ① **3.4.4.4** 又は **3.4.4.5** による場合について手数料を定めることは必須ではない。手数料を定める場合には、金額及び徴収方法について定めていること。 【現地審査】 ① 徴収方法は本人の負担にならないよう配慮していること。 ② 手数料は合理的な範囲であること。 ※ 開示等の求めを事実上断念させることを目的とする料金設定であることが明らかであると認められる場合は、不適合となり得る。

文書審査の項目	現地審査の項目	審査の着眼点
2. 本人からの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旨規定していること。	(1) 本人からの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ていること。	【文書審査】 ① 本人からの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旨を記述していること。 【現地審査】 ① 上記 **a)**～**d)**に関する運用において、本人に過重な負担を課すものになっていないこと。 ※1 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提示を求めるなど、必要以上の個人情報の提供を求めるべきではない。 ※2 例えば、インターネットや郵送などの通信手段によって取得した個人情報でありながら、開示等の求めに応じる手続については、事業者の特定の事業所の窓口を来訪する方法に限定するなど、本人に過重な負担を課すべきでない。

3.4.4.3 開示対象個人情報に関する周知など

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

事業者は、開示対象個人情報について、**a)～f)**の事項を本人の知り得る状態に置かなければならない。

2 注意事項

3.4.2.4 や **3.4.2.6～3.4.2.8** により、**a)～f)**の事項をすでに本人に明示又は通知している場合であっても、開示対象個人情報である限りは、この要求事項に沿って **a)～f)**の事項を本人の知り得る状態に置いておく必要がある。

「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、ウェブサイト画面への掲載、パンフレットの配布、要求に応じて遅滞なく回答を行う等、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う。常にその時点で正確な内容を本人が知り得る状態でなければならない。

3 個人情報保護法との対応

①個人情報保護法第 24 条第 1 項（保有個人データに関する事項の公表等）

②個人情報保護法第 37 条（個人情報保護団体の認定）

③施行令第 5 条（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）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. **a)～f)**の事項を本人の知り得る状態に置く具体的な手順を定めていること。	(1) 開示対象個人情報について、**a)～f)**の事項を本人の知り得る状態に置いていること。	【文書審査】 ① 開示対象個人情報について、**a)～f)**の事項を本人の知り得る状態に置くことが確実に実施されるよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 開示対象個人情報に該当する限り、**3.4.2.4～3.4.2.8** により **a)～f)**の事項を本人に明示又は通知しているときであっても、この要求事項に従い本人の知り得る状態に置いていること。 ③ どのように「本人の知り得る状態」においているかを明確に示すことができること。 ※1 ウェブサイトに掲載した個人情報保護方針、利用目的公表のページに問合せ先を記載するのも一つの方法である。 ※2 本人以外の家族から開示等を求められることもあり得る。そのような場

文書審査の項目	現地審査の項目	審査の着眼点
		合も含め、開示等の求めに対する対応方法（家族からの開示等の求めには応じないのであればその旨）の詳細についても、知り得る状態に置いておくことが望ましい。 運用確認のためのエビデンス ・開示対象個人情報について，a)～f)の事項を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。）に置いている措置 ・開示対象個人情報を管理する台帳等（開示対象個人情報だけを抜き出した台帳は必要でなく、個人情報を管理する台帳等で、分かるように区別されていれば良い。）
	(2) 開示対象個人情報について、本人の知り得る状態に置いている内容が、JIS の a)～f)の事項を満たしていること。	【文書審査】 ① a)～f)の事項を本人の知り得る状態に置くよう記述していること。 【現地審査】 ① a)～f)の事項を本人の知り得る状態に置いていること。 ※ 認定個人情報保護団体の対象事業者となっていない場合は、e)は不要である。 運用確認のためのエビデンス ・a)～f)を記載した書面等

3.4.4.4 開示対象個人情報の利用目的の通知

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

本人から、当該本人が識別される開示対象個人情報について、利用目的の通知を求められた場合、どのように対応しなければならないかを定めている。

2 注意事項

理由の説明は個人情報保護法では努力義務であるが、JIS では義務である。**3.4.4.5**～**3.4.4.7** も同様である。

3 個人情報保護法との対応

①個人情報保護法第 24 条第 2 項及び第 3 項（利用目的の通知）

②個人情報保護法第 28 条（理由の説明）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 本人から，当該本人が識別される開示対象個人情報について利用目的の通知を求められた場合、遅滞なくこれに応じるよう規定していること。	(1) 定めた手順に従い、本人の求めに応じていること。	【文書審査】 ① 本人の求めに応じて確実に利用目的を通知するよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・受け付ける様式等
	(2) 遅滞なく実施していること。	【文書審査】 ① 本人の求めに遅滞なく応じる旨を記述していること。 ※ 遅滞なく実施することが読み取れればよい。「遅滞なく」という文言が必須なのではない。 【現地審査】 ① 期間は一概に決められないが、本人の求めの程度との関連で、合理的な期間内で実施していること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・受け付けたときの記録 ・本人の求めに応じた記録（応じない場合を含む）
2. 本人への回答内容（求めに応じない場合を含む）に関する承認手順を定めていること。	(1) 定めた手順に従い、本人への回答内容（求めに応じない場合を含む）について、管理者の承認を得ていること。	【文書審査】 ① 管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・回答内容（求めに応じない場合を含む）の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）
3. 利用目的を通知しないのは、JIS が定めるただし書きの場合に限定していること。	(1) 利用目的を通知しないのは、JIS が定めるただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を過不足なく記述していること。 【現地審査】 ① 利用目的を通知しないのは、ただし書きの場合のみであること。 運用確認のためのエビデンス ・本人の求めに応じた記録（求めに応じない場合を含む）
4. ただし書きにより利用目的を通知しない場合の承認手順を定めていること。	(1) ただし書きにより利用目的を通知しない場合、管理者の承認を得ていること。	【文書審査】 ① 管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きを適用する場合の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）

3.4.4.5 開示対象個人情報の開示

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

本人から，当該本人が識別される開示対象個人情報の開示を求められたときの対応方法について定めている。

2 注意事項

ただし書き **b)**については、規格本体付属の解説及び経済産業分野ガイドライン等を参考に、適用基準を定める必要がある。**3.4.4.5** の手続の後に **3.4.4.6** 又は **3.4.4.7** の手続へと移行すると考えられるため、円滑に移行できるような仕組みにしておくのが望ましいであろう。

3 個人情報保護法との対応

①個人情報保護法第 25 条（開示）
②個人情報保護法第 28 条（理由の説明）
③施行令第 6 条（個人情報取扱事業者が保有個人データを開示する方法）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 本人から，当該本人が識別される開示対象個人情報の開示を求められた場合に、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，本人に対し，遅滞なく応じるよう規定していること。	(1) 定めた手順に従い、本人の求めに応じていること。	【文書審査】 ① 本人の求めに応じる手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・受け付ける様式等
	(2) 遅滞なく実施していること。	【文書審査】 ① 本人の求めに遅滞なく応じる旨を記述していること。 ※ 遅滞なく実施することが読み取れればよい。「遅滞なく」という文言が必須なのではない。 【現地審査】 ① 期間は一概に決められないが、本人の求めの程度との関連で、合理的な期間内に実施していること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・受け付けたときの記録 ・本人の求めに応じた記録（求めに応じない場合を含む）
2. 本人への回答内容（求めに応じない場合を含む）に関する承認手順を定めていること。	(1) 定めた手順に従い、本人への回答内容（求めに応じない場合を含む）について、管理者の承認を得ていること。	【文書審査】 ① 本人への回答内容について管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ※ 回答内容には、消費者等、本人の権利利益の保護の観点から、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を、可能な限り具体的に明記していることが望ましい。 運用確認のためのエビデンス ・回答内容（求めに応じない場合を含む）の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）
3. 開示の求めに応じないのは､JIS が定めるただし書きの場合のみに限定していること。	(1) 開示の求めに応じないのは、JIS が定めるただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項が、過不足なく記述してあること。 【現地審査】 ① 開示の求めに応じないのは、JIS が定めるただし書きの場合のみであること。 運用確認のためのエビデンス ・本人の求めに応じた記録（求めに応じない場合を含む）
4. ただし書きにより本人に開示しない場合の承認手順を定めていること。	(1) ただし書きにより本人に開示しない場合、管理者の承認を得ていること。	【文書審査】 ① ただし書きにより本人に開示しない場合について管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きを適用する場合の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）

3.4.4.6 開示対象個人情報の訂正，追加又は削除

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

本人から、当該本人が識別される開示対象個人情報の内容について、訂正等を求められた場合の対応方法を定めている。

2 注意事項

開示対象個人情報そのものの削除（消去）については、**3.4.4.7** の対象となる。

訂正等を行わない場合の適用基準は、経済産業分野ガイドライン等を参考に定める必要がある。

3 個人情報保護法との対応

①個人情報保護法第 26 条（訂正等）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 本人から，当該本人が識別される開示対象個人情報の訂正等を求められた場合、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，その結果に基づいて，当該開示対象個人情報の訂正等を行わなければならない旨を規定していること。	(1) 定めた手順に従い、本人の求めに応じていること。	【文書審査】 ① 本人の求めに応じる手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・受け付ける様式等
	(2) 遅滞なく実施していること。	【文書審査】 ① 本人の求めに応じて遅滞なく実施する旨を記述していること。 ※ 遅滞なく実施することが読み取れればよい。「遅滞なく」という文言が必須なのではない。 【現地審査】 ① 期間は一概に決められないが、本人の求めの程度との関連で、合理的な期間内で実施していること。 運用確認のためのエビデンス ・受け付けたときの記録 ・本人の求めに応じた記録（求めに応じない場合を含む）

文書審査の項目	現地審査の項目	審査の着眼点
2. 本人への回答内容（求めに応じない場合を含む）に関する承認手順を定めていること。	(1) 定めた手順に従い、本人への回答内容（求めに応じない場合を含む）について、管理者の承認を得ていること。	【文書審査】 ① 本人への回答内容について管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・回答内容（求めに応じない場合を含む）の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）
3. 訂正等を行わない場合の承認手順を定めていること。	(1) 訂正等を実施しない場合、管理者の承認を得ていること。	【文書審査】 ① 訂正等を行わない場合について管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・ただし書きを適用する場合の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）

3.4.4.7 開示対象個人情報の利用又は提供の拒否権

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

本人から当該本人が識別される開示対象個人情報の利用停止等を求められたときの対応方法を定めている。

2 注意事項

個人情報保護法では、目的外利用（第 16 条違反）、不正な取得（第 17 条違反）、本人同意なしの第三者提供（第 23 条違反）といった法律違反を犯していない限り、事業者は、本人から利用停止等の求めがあっても応じる義務はない。しかし JIS では、本人の事前又は事後の同意の有無にかかわらず、本人からの求めがあれば、事業者は原則として無条件に応じなければならないことに注意を要する。

3.4.4.5 のただし書き **b)**を適用する場合については、規格本体付属の解説及び経済産業分野ガイドライン等を参考に、適用基準を定める必要がある。

3 個人情報保護法との対応

①個人情報保護法第 27 条（利用停止等）

②個人情報保護法第 28 条（理由の説明）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 本人から，当該本人が識別される開示対象個人情報の利用停止等を求められた場合、これに応じなければならないと共に，措置を講じた後は，遅滞なくその旨を本人に通知しなければならない旨を規定していること。	(1) 定めた手順に従い、本人の求めに応じていること。	【文書審査】 ① 本人の求めに応じる手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・受け付ける様式等
	(2) 遅滞なく実施していること。	【文書審査】 ① 遅滞なく実施する旨を記述していること。 ※ 遅滞なく実施することが読み取れればよい。「遅滞なく」という文言が必須なのではない。 【現地審査】 ① 期間は一概に決められないが、本人の求めの程度との関連で、合理的な期間内に実施していること。

文書審査の項目	現地審査の項目	審査の着眼点
		※「消去」とは、開示対象個人情報を開示対象個人情報として使えなくすることであり、当該情報を削除することのほか、当該情報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。 運用確認のためのエビデンス ・受け付けたときの記録 ・本人の求めに応じた記録（求めに応じない場合を含む）
2. 本人への回答内容（求めに応じない場合を含む）の承認手順を定めていること。	(1) 定めた手順に従い、本人への回答内容（求めに応じない場合を含む）について管理者の承認を得ていること。	【文書審査】 ① 本人への回答内容について管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・回答内容（求めに応じない場合を含む）の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）
3. 利用停止等の求めに応じないのは、JIS が定めるただし書きの場合のみに限定していること。	(1) 利用停止等の求めに応じないのは、JIS が定めるただし書きの場合のみであること。	【文書審査】 ① JIS に定める要求事項を過不足なく記述していること。 【現地審査】 ① 利用停止等の求めに応じないのは、JIS が定めるただし書きの場合のみであるように運用していること。 運用確認のためのエビデンス ・本人の求めに応じた記録（求めに応じない場合を含む）
4. ただし書きにより利用停止等を実施しない場合の承認手順を定めていること。	(1) ただし書きにより利用停止等を実施しない場合、管理者の承認を得ていること。	【文書審査】 ① ただし書きにより利用停止等を実施しない場合いについて管理者の承認を得る手順を明確に記述していること。 ※ 当該開示対象個人情報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、利用停止等の求めに応じないこともできる。ただし、その場合は、**3.4.4.5** のただし書き **b)**に該当する場合として、判断基準としてその旨を定めている必要がある。 【現地審査】 ① 定めた手順に従い、実施していること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・ただし書きを適用する場合の承認に関する記録 ・本人の求めに応じた記録（求めに応じない場合を含む）

3.4.5 教育

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

従業者に、個人情報保護マネジメントシステムを実施できるための力量を確実に身につけさせることが目的である。そのためには、受講者の理解度を把握し、理解が不十分である受講者に対しては、再度教育を実施するといった措置が必要である。

2 注意事項

教育は、全ての従業者に実施しなければならない。直接に個人情報の取扱いに従事しない部門であっても、個人情報（例えば、従業者の情報、名刺の情報）に接する可能性はあるからである。教育内容は、個人情報を取り扱うリスクの発生の可能性に応じて実施してよい。

教育は集合教育である必要はなく、e ラーニングなど事業者にとって合理的な方法で実施するとよい。

なお、プライバシーマーク制度では、少なくとも年 1 回以上の教育の実施を求めている。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. すべての従業者に、定期的に個人情報保護に関する適切な教育を実施するよう規定していること。	(1) 教育計画書に従い、教育を実施していること。	【文書審査】 ① 定期的な教育を確実に実施するよう手順を明確に記述していること。教育計画書もその手順と整合している必要がある。 【現地審査】 ① 定めた手順に従い、年 1 回以上の教育を実施していること。 ② 教育を実施した方法を記録していること。 ※ 更新審査においては、過去 2 年分の教育記録について確認する。 運用確認のためのエビデンス ・教育計画書 ・教育実施記録

文書審査の項目	現地審査の項目	審査の着眼点
	(2) すべての従業者に個人情報保護に関する適切な教育を実施していること。	【文書審査】 ① 適切な教育を確実に実施するよう手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 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していること。 ③ 新規採用時や中途採用時（派遣社員の受入れ時を含む。）には、必要に応じ、随時教育を実施していること。 ※1 人材派遣業を営む事業者は、雇用契約を締結している派遣スタッフ（実働者）への教育も必要である。ただし、当該事業者内で働くわけではないから、当該事業者の社員と同等である必要はない。 ※2 長期休暇中（例えば産休）のため受講できない従業者については、現地審査の時点で教育を実施している必要はない。それらの者については休暇明けに実施すればよい。 運用確認のためのエビデンス ・受講状況（出欠状況、欠席者への補講の実施等）が確認できる記録
2. 規定又は教育計画書に、少なくとも **a)**～**c)** の内容を含めていること。	(1) 教材に **a)**～**c)** の内容を含めていること。	【文書審査】 ① 規定又は教育計画書に、少なくとも **a)**～**c)** の内容を含めて記述していること。 【現地審査】 ① 使用した教材に **a)**～**c)** の内容を含んでいること。 運用確認のためのエビデンス ・使用した教材
3. 受講者の理解度確認を実施する手順を規定していること。	(1) 受講者の理解度確認を実施していること。	【文書審査】 ① アンケートや小テストの実施など、理解度確認を確実に実施するよう具体的な手順を定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 理解度が不十分な受講者へのフォローアップを実施していること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・受講者の理解度確認を実施した記録
4. 教育の計画及び実施，結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定める手順を規定していること。	(1) 教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定め、実施していること。	【文書審査】 ① 教育の実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持を確実に実施するよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 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していること。 運用確認のためのエビデンス ・教育の計画及び実施，結果の報告及びそのレビュー，計画の見直し並びにこれらに伴う記録

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

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報保護マネジメントシステムを構成している要素のうち、最低限 **a)**～**d)**は文書化する必要がある旨を定めたものである。

2 注意事項

書面は紙媒体である必要はない。

JIS で必要とする記録には、以下のものが含まれる。

- 個人情報の特定に関する記録
- 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
- 個人情報のリスクの認識、分析及び対策に関する記録
- 計画書
- 利用目的の特定に関する記録
- 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
- 教育実施記録
- 苦情及び相談への対応記録
- 運用の確認の記録
- 監査報告書
- 是正処置及び予防処置の記録
- 代表者による見直しの記録

3 審査の項目とその着眼点

この要求事項が実施されているかどうかは、個人情報保護マネジメントシステムの運用の全体において審査される。

3.5.2 文書管理

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

確立した手順を確実に実施するためには、その手順を文書化しておく必要がある。この要求事項は、作成した文書の管理手順を定めるよう求めている。なお、文書管理それ自体は個人情報保護マネジメントシステムの目的ではない。文書は、個人情報保護マネジメントシステムを確実に運用するための手段として、事業者にとって分かりやすいように作成し、管理されていれば足りる。

2 注意事項

文書は紙媒体である必要はなく、事業者にとって運用しやすいものであれば良い。

文書は、ISMS（ISO/IEC27001）や ISO9001、ISO14001 などの他のマネジメントシステム文書と統合してもよい。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 記録を除く文書の管理について、少なくとも **a)**～**c)**の具体的な手順を定めていること。	(1) 定めた手順に従い、文書を管理していること。	【文書審査】 ① **a)**～**c)**を確実に実施できるよう、手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 最新版、旧版等が明確であるように管理していること。 ※ ISO14001：2004 の文書管理についての解説では、「...しかし、組織が本来重視すべきことは、複雑な文書管理システムにあるのではなく、環境マネジメントシステムの効果的な実施及び環境パフォーマンスにある。」とわざわざ記述されており、文書管理に偏った審査の弊害が認識されている。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。従業者にとって明確であればそれで良い。 運用確認のためのエビデンス ・文書の更新履歴 ・文書の管理状況 ・文書を従業者が参照する環境

3.5.3 記録の管理

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

JIS への適合を実証するための記録の作成及び維持を要求している。記録は紙媒体である必要はなく、運用しやすい方法で作成すればよい。

2 注意事項

記録自体が個人情報の場合もあるから、個人情報の特定から漏れないように注意する必要がある。また、不必要に個人情報を増やすような記録の作成は避けるべきである。規格本体付属の解説には、JIS で要求される記録に含まれるものが列挙されているので、参考にすると良い。ただし、そこに列挙されているものだけを作成すれば良いと考えるのではなく、それ以外にも必要に応じて作成するようにしなければならない。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 記録の管理手順を明確に定めていること。	(1) 定めた手順に従い、記録を管理していること。	【文書審査】 ① 必要な記録の特定、保管、保護、保管期間及び廃棄についての手順を明確に記述していること。 ※ JIS で必要とする記録は、**3.5.1** を参照のこと。 【現地審査】 ① 定めた手順に従い、実施していること。 ※ 記録は紙媒体である必要はない。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良い。

3.6 苦情及び相談への対応

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切、かつ、迅速な対応を行うよう要求するものである。

2 注意事項

苦情は、不適合が発見される端緒にもなる。なお、苦情や相談が１件もない場合は、「ない」と安心しているのではなく、定めた手順が機能していないために、責任ある立場の者まで苦情及び相談が上がっていないのではないかと疑ってみる必要がある。

3 個人情報保護法との対応

①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）

②個人情報保護法第 37 条（個人情報保護団体の認定）

4 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 個人情報の取扱い及び個人情報保護マネジメントシステムに関して，本人からの苦情及び相談を受け付けて，適切，かつ，迅速な対応を行う手順を定めていること。	(1) 苦情の宛先が、本人にとって明確であること。	【現地審査】 ① 認定個人情報保護団体の対象事業者である場合、当該団体の苦情解決の申し出先も明示していること。 ※ 個人情報保護方針に関する問合せ先や個人情報の取扱いに関する問合せ先と併せて、苦情及び相談の受付窓口を記載するのも便宜であろう。 運用確認のためのエビデンス ・苦情申し出の宛先を本人に対し明確にしていることを確認できるもの
	(2) 定めた手順に従って受け付け、対応していること。	【文書審査】 ① 苦情及び相談を受け付ける手順を記述していること。 ※ 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り行う必要があり、個人情報保護管理者が兼任してもよい。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 「受け付け例なし」の場合には、受付ける手順を具体的に示すことができること。

文書審査の項目	現地審査の項目	審査の着眼点
		運用確認のためのエビデンス ・受付を記録する様式
	(3) 対応が迅速であること。	【文書審査】 ① 迅速に対応する旨を記述していること。 【現地審査】 ① 受け付けた日と対応した日、苦情及び相談者本人の要求の程度との関連で、合理的な期間内に対応していること。 運用確認のためのエビデンス ・受け付けた時の記録 ・対応した記録
	(4) 受け付ける手順が機能していること。	【現地審査】 ① 受け付ける手順を一通り説明できるようになっていること。 ※ 内部規程のどこに書いてあるかを答えるのみではなく、審査の場面で説明できることが肝要である。特に苦情及び相談の受付例がない場合、手順が機能していないために、責任者まで苦情及び相談が上がっていない可能性もあり得る。 運用確認のためのエビデンス ・苦情及び相談を受け付ける手順、様式等
2. 本人に回答する対応内容について承認手順を定めていること。	(1) 定めた手順に従い、対応内容について管理者の承認を得ていること。	【文書審査】 ① 本人に回答する対応内容について管理者の承認を得る手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・対応内容の承認に関する記録

文書審査の項目	現地審査の項目	審査の着眼点
3. 苦情や相談の内容及び対応結果を代表者に報告する手順を定めていること。	(1) 定めた手順に従い、代表者に報告していること。	【文書審査】 ① 代表者に報告する手順を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ※ すべての苦情を代表者に報告する必要はないが、管理者が重要と判断したことについては、随時、報告を行う必要があろう。 運用確認のためのエビデンス ・苦情の内容及び対応結果を報告したことが確認できる記録

3.7 点検

3.7.1 運用の確認

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

日常的な運用確認により、不適合を早期に発見し事故の芽を摘むことを想定した要求事項である。運用の確認(3.7.1)はその部門に所属する者が運用主体として自ら点検するものであり、監査(3.7.2)は、当該部門以外に所属する第三者が客観的に点検するものと言える。

2 注意事項

日常的な運用の確認を実施するために業務に支障が出るというのでは本末転倒である。業務に支障のない範囲で、ルールどおり実施されているか見回って確認する程度でもよい。また、3.3.3（リスクの認識、分析及び対策）において把握した残存リスクが顕在化していないかどうか、確認することも含まれるであろう。確認した記録を残すかどうかは、事業者が必要に応じて判断すれば良い。ただし、最低限の記録は必要であろう。例えば、

a)最終退出時の社内点検（施錠確認等）の記録を残し、定期的に確認する

b)最初に出社した人と最後に退社した人の記録を残し、定期的に確認する

c)個人情報を格納した情報システムへのアクセスログを取得し、定期的に確認する

といったことは、通常行われているものと考える。もっとも、これらは安全管理措置とも重なるので、そちらで定めておけばよい。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 個人情報保護マネジメントシステムの適切な運用について事業者の各部門及び階層において定期的に確認するための手順を定めていること。	(1) 個人情報保護マネジメントシステムの適切な運用について事業者の各部門及び階層において定期的に確認していること。	【文書審査】 ① 運用の確認を確実に行うように、確認を行う時期（月○回、等）を含めた手順（a)～c)を含む点検項目、点検者、点検記録方法）を明確に記述していること。 【現地審査】 ① 定めた手順に従い、実施していること。 ※ 確認した記録を残すという面では、以下の 1)～3)は必須である。しかし安全管理面の審査と重複するので、そちらで確認できれば良い。 1) 最終退出時の社内点検（施錠確認等） 2) 入退館（室）の記録の定期的な確認 3) アクセスログの定期的な確認 運用確認のためのエビデンス ・定期的に運用の確認を実施している記録

3.7.2 監査

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

個人情報保護マネジメントシステムの JIS への適合状況及びその運用状況を定期的に監査するよう求めている。

2 注意事項

個人情報保護マネジメントシステムの JIS への適合状況を監査した上で、個人情報保護マネジメントシステムの運用状況を監査する必要がある。適合していないものに基づいて運用しても無意味であるからである。

個人情報保護監査責任者は内部の者から指名しなければならないが、監査員は外部の者でも良い。監査責任者又は監査員になることについて、特段の資格は必要でない。なお、プライバシーマーク制度では、代表者が個人情報保護監査責任者を兼務することを認めていない。

監査は、全ての部門を対象に実施しなければならない。直接的に個人情報の取扱いに従事しない部門であっても、個人情報（例えば、従業者の情報、名刺の情報）に接する可能性はあるからである。

プライバシーマーク制度では、少なくとも年 1 回以上の監査の実施を求めている。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. JIS との適合状況及びその運用状況について監査するよう規定していること。	(1) 監査計画書に従い監査を実施していること。	【文書審査】 ① 定期的な監査を確実に実施するよう手順を明確に記述していること。監査計画書もその手順と整合している必要がある。 ② 定期的に行うために、具体的な時期（「○月」等）を定めていること。 【現地審査】 ① 監査計画書に従って監査を実施していること。 ② 年 1 回以上の監査を実施していること。 ※ 更新審査においては過去 2 年分の記録を確認する。 運用確認のためのエビデンス ・監査計画書 ・監査報告書

文書審査の項目	現地審査の項目	審査の着眼点
	(2) JIS との適合状況について監査を実施していること。	【文書審査】 ① JIS への適合状況について監査を行う手順を記述していること。 【現地審査】 ① 手順書レベルまでの全体を含めて、内部規程と JIS との適合状況を監査していること。 ※1 様々な外部文書を取り込んでいるうちに、ルールが JIS に適合しない内容になってしまう可能性がある。例えば、個人情報保護法のレベルにダウンすることによって JIS に適合しない内容に改変される。また、現場で JIS と適合しないルールが作られている可能性がある。したがって、最上位規程と JIS との対応を監査するだけでは不十分である。 ※2 内部規程の改正がない場合であっても、事業環境の変化、法令等の制定改廃、リスク状況の変化などにより、内部規程の改正漏れが生じていないか監査する必要がある。 運用確認のためのエビデンス ・監査報告書 ・監査チェックリスト等
	(3) 運用状況について監査を実施していること。	【文書審査】 ① 運用状況について監査を実施する手順を記述していること。 【現地審査】 ① 定められた手順に従い運用状況の監査を実施していること。 ② 運用状況の監査にあたっては、**3.3.3** のリスクなどの認識、分析及び対策により講じることとした対策を規定に反映させ、その規定に沿って監査項目を設定していること。 ※ 運用状況の監査のためのチェックリストは様式として定型化されている必要はなく、監査計画書を基に監査の都度作成してもよい。 運用確認のためのエビデンス ・監査報告書 ・監査チェックリスト等
	(4) 全部門の監査を実施していること。	【文書審査】 ① 全部門を監査の実施対象とするよう記述していること。

文書審査の項目	現地審査の項目	審査の着眼点
		【現地審査】 ① 全部門の監査を実施していること。 ※1 事業者内部で、個人情報の取扱いがないと判断している部門であっても、本当に個人情報の取扱いがないか、従業者の個人情報の取扱状況はどうか、個人情報保護マネジメントシステムが浸透しているか等を監査する必要がある。 ※2 受託業務を委託元の構内で実施している場合、受託業務である限りは事業者に管理責任があるため、監査の対象となる。ただし、委託元の許可が得られない場合は自主点検を行わせ、その結果を確認することで代替してもよい。 運用確認のためのエビデンス ・監査報告書
2. 事業者の代表者は、個人情報保護監査責任者を、事業者の内部の者から指名するよう規定していること。	(1) 個人情報保護監査責任者は、代表者が事業者の内部から指名していること。	【文書審査】 ① 事業者の代表者は、個人情報保護監査責任者を事業者の内部の者から指名する旨を記述していること。 【現地審査】 ① 事業者の代表者は、個人情報保護監査責任者を事業者の内部の者から指名していること。 ※ 個人情報保護監査責任者は、個人情報保護管理者と同等以上の役職にある者が望ましい。個人情報保護監査責任者となることに特別な資格は不要である。 運用確認のためのエビデンス ・体制図等
3. 個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、事業者の代表者に報告するよう規定していること。	(1) 個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、事業者の代表者に報告していること。	【文書審査】 ① 個人情報保護監査責任者は、監査を指揮し、監査報告書を作成しなければならない旨を記述していること。 ② 監査結果の報告を事業者の代表者（または代表者から権限委任された者）に対して行うよう記述していること。 ※ JIS Q 15001 は、ISO9001 や ISO14001 など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ため、それらのマネジメントシステムでいう組織の長は、事業者の代表者と一致する。

文書審査の項目	現地審査の項目	審査の着眼点
		【現地審査】 ①　定めた手順に従い、実施していること。 ※ 監査報告書は、監査を実施した状況のほか、問題点として把握した事項と、その中で改善すべき事項について区別して示すよう記述する。 運用確認のためのエビデンス ・監査報告書
4. 監査員は、自ら所属する部門を監査しないよう規定していること。	(1) 監査員は、自ら所属する部門を監査していないこと。	【文書審査】 ① 監査員は自ら所属する部門を監査してはならない旨を記述していること。 ※ 監査は、事業者内部からの要員により、又は事業者のために働くように外部から選んだ者により実施することができる。その際、監査を実施する者には、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必要があるが、特別な資格は不要である。 【現地審査】 ①監査員は、自ら所属する部門を監査していないこと。 運用確認のためのエビデンス ・監査報告書
5. 監査の計画及び実施，結果の報告並びにこれに伴う記録の保持に関する責任及び権限を定める手順を規定していること。	(1) 定めた手順に従い、監査の計画及び実施，結果の報告並びにこれに伴う記録を保持していること。	【文書審査】 ①　監査の計画及び実施，結果の報告並びにこれに伴う記録保持を確実に実施するよう、手順を明確に記述していること。 【現地審査】 ①　定めた手順に従い、実施していること。 ②　監査記録として、まとめた結果としての監査報告書だけでなく、実際に記入した監査チェックリスト等も保管していること。 運用確認のためのエビデンス ・監査計画書 ・監査報告書 ・監査チェックリスト等 ・是正処置及び予防処置を実施した記録

3.8 是正処置及び予防処置

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

不適合が発見された場合の是正処置及び予防処置を実施する手順について定めている。

2 注意事項

不適合が発見される場面としては、例えば、**1c)**の外部機関による審査、**3.3.3** のリスクなどの認識、分析及び対策、**3.3.7** の緊急事態の発生、**3.6** の苦情、**3.7.1** の運用の確認、**3.7.2** の監査などが考えられる。発見された不適合についてはすべて、この要求事項により是正処置及び予防処置が実施されることになる。

是正処置は発見された不適合を改善することであり、予防処置は不適合の発生を未然に防ぐことである。両者の意味は異なるが、きっかけが異なるだけで実施する内容は同じであるため、同じ要求事項に並べてまとめられている。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 発見された不適合については、この要求事項に基づき、是正処置及び予防処置を実施するという関係が明確であること。	(1) 発見された不適合について、是正処置及び予防処置を実施していること。	【文書審査】 ① 発見された不適合については、この要求事項により是正処置及び予防処置を実施するという関係が明確であること。 ※ 監査によって発見された不適合の是正のみが意識されている場合が多いので注意する。 【現地審査】 ① 発見された不適合については、この要求事項により是正処置及び予防処置を実施していること。
2. 是正処置及び予防処置を確実に実施するための手順を、a)～e)を含めて定めていること。	(1) **a)**不適合の内容を確認していること。	【文書審査】 ① 不適合の内容について事業者の代表者（または代表者としての権限を委任されている者）の承認を得る手順を定めていること。 ※ 不適合は、事業者の代表者が承認することにより初めて不適合になる。ただし、軽微な不適合まで事業者の代表者に報告されるとなると現場が萎縮してしまい、事実が隠されてしまう可能性がある。軽微な不適合については、是正処置及び予防処置の実施を含め承認権限を委任するのが現実的と考えられる（**3.3.4** の**2注意事項**参照）。

文書審査の項目	現地審査の項目	審査の着眼点
		【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・是正処置及び予防処置を実施した記録（処置した結果を含む）
	(2) b)不適合の原因を特定し、是正処置及び予防処置を立案していること。	【文書審査】 ① 不適合の原因を特定し是正処置及び予防処置を立案するのは、不適合が発見された部門である旨を記述していること。 ② 不適合の原因を特定し是正処置及び予防処置を立案する手順を定めていること。 ※1 不適合が発見された部門が、当該部門の業務内容を最も理解し把握しているので、業務内容に相応した是正処置及び予防処置を当該部門に立案させるべきである。 ※2 不適合の原因を特定していないと根本的解決にはならず、再発の予防にもならない。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・是正処置及び予防処置を実施した記録（処置した結果を含む）
	(3) c)期限を定め、立案した処置を実施していること。	【文書審査】 ① 立案された是正処置及び予防処置について、実施期限を含め、事業者の代表者（または代表者としての権限を委任されている者）の承認を得て、実施する手順を定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。 ② 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を設定していること。 運用確認のためのエビデンス ・是正処置及び予防処置を実施した記録（処置した結果を含む）

文書審査の項目	現地審査の項目	審査の着眼点
	(4) **d)**実施した是正処置及び予防処置の結果を記録していること。	【文書審査】 ① 実施した是正処置及び予防処置の結果を記録する手順を定めていること。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・是正処置及び予防処置を実施した記録（処置した結果を含む）
	(5) **e)**実施した是正処置及び予防処置の有効性をレビューしていること。	【文書審査】 ① 実施した是正処置及び予防処置の有効性をレビューする手順を定めていること。 ※1 想定された効果が得られているかどうかを確認するのが「レビュー」である。運用の確認（**3.7.1**）に含めてもよい。 ※2 不適合が改善されているか、フォローアップ監査を実施することが望ましい。 【現地審査】 ① 定めた手順に従い、実施していること。 運用確認のためのエビデンス ・是正処置及び予防処置を実施した記録（処置した結果を含む） ・実施した是正処置及び予防処置をレビューした記録

3.9 事業者の代表者による見直し

*** 著作権者の許諾が得られないため、ウェブサイトでは規格本文を表示できません。***

1 概要

より良い個人情報保護マネジメントシステムとするため、**a)**～**g)**の事項を材料に、現状を前提としないで見直すことを要求している。

2 注意事項

検討結果次第では経営資源の配分の見直しといった今後の事業計画への影響も考えられるため、実質的な経営判断が求められていると言える。したがって、**3.9**（事業者の代表者による見直し）は、日々の改善や **3.8** に基づく是正処置とは次元が異なることに注意する必要がある。

プライバシーマーク制度では、少なくとも年 1 回の見直しの実施を求めている。

3 審査の項目とその着眼点

文書審査の項目	現地審査の項目	審査の着眼点
1. 具体的な期間（時期）を明確にして個人情報保護マネジメントシステムを見直すよう規定していること。	(1) 規定に従い、代表者による見直しを実施していること。	【文書審査】 ① 確実に実施するよう、手順を明確に記述していること。 ② 具体的な時期（「○月」等）を定めていること。例えば、監査の時期が明確であれば、「監査終了後何ヶ月以内」等の定め方でもよい。 ③ 少なくとも年 1 回は実施するよう記述していること。 ※ 定期的に行うだけでなく、必要に応じて臨時に実施するよう記述していることが望ましい。 【現地審査】 ① 定めた手順に従い、実施していること。 ② **3.8** に基づく現状の延長線上での是正にとどまらず、**a)**～**g)**の社外環境も考慮した上で見直しを検討していること。 ※1 更新審査においては、過去 2 年分の記録を確認する。 ※2 **3.8** に基づく是正について事業者の代表者が承認することは、ここでいう事業者の代表者による見直しではない。**3.9** では実質的な経営判断が求められている。 <u>運用確認のためのエビデンス</u> ・事業者の代表者による見直しを実施した記録

文書審査の項目	現地審査の項目	審査の着眼点
2. 見直しのインプットとして、**a)**～**g)**を含めて規定していること。	(1) 見直しのインプットに**a)**～**g)**を含めていること。	【文書審査】 ① 見直しのインプットとして、**a)**～**g)**を含めて記述していること。 【現地審査】 ① **a)**～**g)**を含むインプットを材料にして見直しを実施していること。 ※ 常に**a)**～**g)**の事項すべてを見直しの材料にする必要はない。 運用確認のためのエビデンス ・事業者の代表者による見直しを実施した記録

改廃履歴

版	改定日	改定箇所・理由
１．０	平成２２年 ９月１７日	「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン－第 2 版－」公表に伴い 1.0 版とする。
１．１	平成２４年 ９月 ５日	平成 24 年 7 月「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」（変更前：「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対する指針」）公表に伴う変更を反映
１．２	平成２６年１月１４日	「3.4.4.3 開示対象個人情報に関する周知など」における記載内容の一部訂正を反映
１．３	平成２８年１月４日	平成 27 年 11 月「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」「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項」公表に伴う変更を反映 平成 27 年 5 月 19 日「特定個人情報の取扱いの対応について」(一般財団法人日本情報経済社会推進協会プライバシーマーク推進センター)公表に伴う変更を反映 平成 27 年 1 月「営業秘密管理指針」改訂に伴う変更の反映