JISQ15001:2006 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１版—

2006 年 8 月

(財) 日本情報処理開発協会

プライバシーマーク推進センター

はじめに

1980 年 10 月、プライバシーの保護及び個人データの越境流通に関する OECD 勧告が公表され、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という場合に必ず引用されるもので、以後、世界の全ての個人情報保護に関する法令等はこれに準拠しているといっても過言ではない。当然、個人情報保護法も JISQ15001 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正確性の原則(Data 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収集目的特定の原則(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目的内利用の原則(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安全対策の原則(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本人関与の原則(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 OECD8 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処理に係わ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、個人情報保護について大きな転換点となることが起きた。EU が、個人データ保護に関するガイドラインを採択し、加盟各国に 1998 年 10 月 24 日までに国内法を整備するよう義務付けたことである。特に、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動を禁止した点が、他地域・諸国に大きな影響を与えた。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処理に係わ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、そのガイドラインを基に、個人情報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 JISQ15001:1999」が策定された。

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、以下の点が挙げられる。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言える。

・民間部門の自主的取組の促進
・第三者認証の認証基準とすることにより取組へのインセンティブを確保
・認定基準の明確化により認定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 規格化に伴い、認証基準を JISQ15001 に変更し現在に至っている。

JISQ15001:1999 は、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平成 18 年 5 月に改訂され JISQ15001:2006 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 JISQ15001:2006 に移行した。

この資料は、JISQ15001：2006 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 JISQ15001:2006 各要求事項についてのポイント」では、2006 年版 JISQ15001 の各要求事項毎に、文書の作成及び運用のポイントをリスト形式で記述している。また、付録として、1999 年版をベースにした内部規程に 2006 年版を取込む際の注意点をまとめた。

関係諸氏の参考となれば幸いである。

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..... 5

第二部 JISQ15001:2006 各要求事項についてのポイント.....17

付録 JISQ15001:1999 をベースにして作成した内部規程に
JISQ15001:2006 を取込む際の注意点 67

第一部
個人情報保護マネジメントシステム作成指針

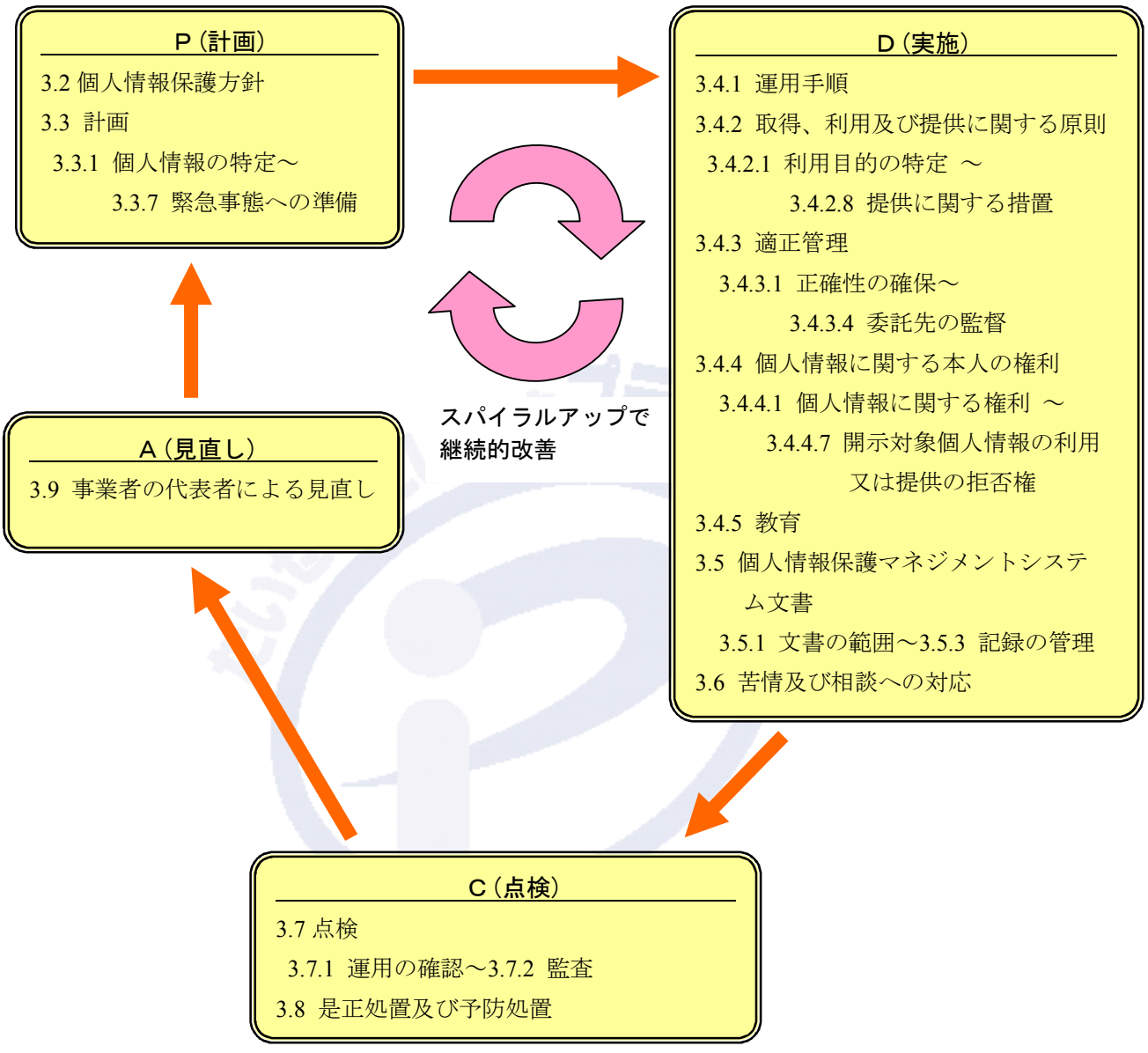
1. 個人情報保護マネジメントシステムについて
2. JISQ15001:2006 に適合した個人情報保護マネジメントシステムを構築するメリット
3. JISQ15001:2006 での配慮
4. 個人情報保護マネジメントシステム構築の具体的な進め方

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 JISQ15001:2006 は、マネジメントシステムを作成する場合の国際規約である ISO Guide 72（「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（2001）」）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上げていくことが期待される。

図 JISQ15001:2006 におけるＰＤＣＡサイクル



2. JISQ15001:2006 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

改訂前の JISQ15001:1999 は、個人情報保護に関する法律（以下、「個人情報保護法」という。）よりも前に策定されたため、個人情報保護法によって新しく導入された概念に対応していないところがあった。また、個人情報保護法と用語が異なるため、法への適合状況が分かりづらい面があった。JISQ15001:2006 は、個人情報保護法を取込むことを最大の目標にして改訂されたものである。したがって、JISQ15001:2006 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良く、個人情報保護法に違反しないためにどのようにすれば良いか分からないという事業者にとって、この JISQ15001:2006 は、非常に有効な指針となると言える。

また、JISQ15001:2006 は、個人情報保護法を取込んだだけでなく、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付けられている。JISQ15001:2006 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、JISQ15001:2006 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．JISQ15001:2006 での配慮

今回の JIS 規格の改訂に当たっては、原案作成協力者として当協会も名を連ねているように、当協会のこれまでの審査経験が反映されている。

JISQ15001：2006 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共に、規格本体として書きにくいことは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。これは審査基準の明確化にもつながる。

規格本体と解説とを合わせて読むことで、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策定の作業計画をたてる
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、

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

である。「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、また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、滅失又は毀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、たとえば、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取扱いの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** 新しいことをや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、作業が進まず、下からは突き上げられ上からは押し付けられ、という窮状に陥る。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。

ステップ３：PMS 策定の作業計画をたてる

PMS 策定チームは、今後の作業スケジュールをたて、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、組織の全ての従業者に周知しなくてはならない。

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。

なお、全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ることから、組織の方針を理解させておく必要からである。

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。この作業の意味は、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することである。特定にあたっては、当該個人情報の利用目的、入手経路、社内での取扱経路（取扱部署）、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良い。

☞**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出し、明確にすることが出発点になる。

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、JISQ15001（以下、「JIS」という。）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

PMS 策定チームは、ステップ５により特定した個人情報について、その個人情報が自社に入ってから出て行くまで（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各局面（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全て洗い出す。想定されるリスクには、個人情報への不正なアクセス、個人情報の紛失、破壊、改ざん及び漏えいなどだけでなく、ステップ６で認識した個人情報の取扱いに関する法令、国が定める指針及びその他の規範に対する違反や、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などが含まれる。ライフサイクルが同じものはパターン化してまとめれば良い。

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、たとえば、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というリスクがあるが、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分析し、評価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曖昧なために、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されており、そのリスクに対するさまざまな予防措置を検討して、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る。したがって、プライバシーマーク制度においても、合理的なリスク対策について、各事業者に共通な一律の基準を特に示していない。事業者の規模や事業内容に応じ、経済的に実行可能な範囲の対策を検討すれば良い。「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。

“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、幾つかの対策を組合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。このような過程を経て作り上げたリスク対策は、十分に合理的である。

なお、リスクへの対策を講じたとしても全てのリスクが無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、管理する必要がある。残存リスクは認識していることが重要である。

それから、『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』という関連付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、この関連付けが明確でなければ、メンテナンスができなくなるからである。

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半分以上はできたようなものである。逆にここに抜けがあれば、後が適正に実施されても何にもならない。

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までの経過に基づき、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あって実効性のある、身の丈に合ったものでなければならない。したがって、内部規程には定められた構成（雛型）は存在しない。内部規程ができてからそれに実体をあわせるのではなく、実体ができてからそれを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良い。

PMSの実施にあたっては、最低限、以下の規定が必要である。全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だ詳細規程の作成方法を採ることによって、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も参考にすることが必要である。先にも述べたとおり、業法等の法令がある場合は 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。

内部規程は、詳細規程を含め、JIS の要求事項との合致について監査を実施しなければならない。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、策定した詳細規程についても、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かぎ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ベースになるが、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良い。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あてはまる場合がある。そのような時は、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、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うるかは、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。また、漏えい等が起こったときの本人（消費者）への対応、主務官庁・JIPDEC プライバシーマーク推進センター・指定機関・認定個人情報保護団体等関係機関への対応、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、直接書面による取得とそれ以外の場合に分けて、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。

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、更新手続きの規定、処理結果の確認規定等、個人情報取扱い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において講ず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）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。

①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
②個人情報及びそれを取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
③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
④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因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。

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（従業者全てを含む）
・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）
・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

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、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あるから、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、日常的に気がついた点があれば是正･予防していくものであり、監査は計画書に基づき組織全体で定期的かつ必要に応じて随時実施するものである。

運用の確認は大げさなものでなくて良い。ルールどおり実施されているか、見回って確認するといったことが求められる。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であろう。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良い。

監査は、PMS の整備状況、PMS に基づく体制整備状況、運用状況を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

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であろう。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（初回は除く）
・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共に研修記録を残し、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。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 の見直しを行う

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
JISQ15001:2006 各要求事項についてのポイント

目　次

1 適用範囲 20
2 用語及び定義 21
3 個人情報保護マネジメントシステム要求事項 22
3.1 一般要求事項 22
3.2 個人情報保護方針 23
3.3 計画 24
3.3.1 個人情報の特定 24
3.3.2 法令，国が定める指針その他の規範 25
3.3.3 リスクなどの認識，分析及び対策 26
3.3.4 資源，役割，責任及び権限 27
3.3.5 内部規程 28
3.3.6 計画書 29
3.3.7 緊急事態への準備 30
3.4 実施及び運用 31
3.4.1 運用手順 31
3.4.2 取得，利用及び提供に関する原則 32
3.4.2.1 利用目的の特定 32
3.4.2.2 適正な取得 33
3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限 34
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 35
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 36
3.4.2.6 利用に関する措置 38
3.4.2.7 本人にアクセスする場合の措置 39
3.4.2.8 提供に関する措置 41
3.4.3 適正管理 43
3.4.3.1 正確性の確保 43
3.4.3.2 安全管理措置 44
3.4.3.3 従業者の監督 47
3.4.3.4 委託先の監督 49
3.4.4 個人情報に関する本人の権利 51
3.4.4.1 個人情報に関する権利 51

3.4.4.2 開示等の求めに応じる手続 52
3.4.4.3 開示対象個人情報に関する事項の周知など 53
3.4.4.4 開示対象個人情報の利用目的の通知 54
3.4.4.5 開示対象個人情報の開示 55
3.4.4.6 開示対象個人情報の訂正，追加又は削除 56
3.4.4.7 開示対象個人情報の利用又は提供の拒否権 57
3.4.5 教育 58
3.5 個人情報保護マネジメントシステム文書 59
3.5.1 文書の範囲 59
3.5.2 文書管理 60
3.5.3 記録の管理 61
3.6 苦情及び相談への対応 62
3.7 点検 63
3.7.1 運用の確認 63
3.7.2 監査 64
3.8 是正処置及び予防処置 65
3.9 事業者の代表者による見直し 66

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。必ず規格本体付属の解説と併せて読むことが望ましい。

注 2. この資料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 年法律第 57 号）
② 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」（平成 16 年 10 月、経済産業省）
③ 1999 版＝JISQ15001：1999
④ 2006 版＝JISQ15001：2006
⑤ 管理者＝個人情報保護管理者
⑥ 監査責任者＝個人情報保護監査責任者

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。

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) この要求事項の目的

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、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。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かどうかは別にして、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。

(2) 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政令第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）※ただし政令第２条は本規格では適用せず。

(3) ポイント

	文書の作成	運用
1	全従業者を人的適用範囲に定めていること。	①全従業者を人的適用範囲にしていること。
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。

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)この要求事項の目的

この規格の中で使用する用語及び定義について規定する。言うまでもないことであるが、2006版への改訂により 1999 版と用語が変わったからといって、2006 版に合わせて用語を統一しなければならないものではない。大切なことは、規格が要求することに実体が適合していることであって、事業者内で使う用語が規格と異なっていても全く関係ない。

なお、個人情報の定義については、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。

(2)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政令第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政令第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）
※ただし政令第２条は本規格では適用せず。

(3)ポイント

	文書の作成	運用
1	「個人情報」を規格 2.1 のように定義していること。	
2	「本人」について規格 2.2 のように定義していること。	
3	「事業者」について規格 2.3 のように定義していること。	
4	「個人情報保護管理者」について規格 2.4 のように定義していること。	
5	「個人情報保護監査責任者」について規格 2.5 のように定義していること。	
6	「本人の同意」について規格 2.6 のように定義していること。	
7	「個人情報保護マネジメントシステム」について規格 2.7 のように定義していること。	
8	「不適合」について規格 2.8 のように定義していること。	
9	規格に無い用語を定義している場合、規格の内容に反する定義をしていないこと。	

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)ポイント

特になし。

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) この要求事項の目的

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) 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

(3) ポイント

	文書の作成	運用
1	個人情報保護の理念を明確にしていること。	
2	**a)**について記述していること。	
3	**b)**について記述していること。	
4	**c)**について記述していること。	
5	**d)**について記述していること。	
6	**e)**について記述していること。	
7	**f)**が記述されていること。	
8	制定日及び最終改訂年月日が表示されていること。	①公開(ウェブなど)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が明示されていること。
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。
		②ウェブに掲載している場合、トップページにリンクがあること。
		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い合わせ先が明示されていること。
		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。

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) この要求事項の目的

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

(2) 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政令第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）※ただし政令第２条は本規格では適用せず。

(3) ポイント

	文書の作成	運用
1	全ての個人情報を特定する手順及び承認手順が明確であること。	①定められた手順に従い、個人情報が特定されていること。
		②個人情報を特定した台帳等が作成されていること。
		③個人情報が漏れなく特定されていること。
2	個人情報を特定した台帳等の更新及び定期的な見直しに関する手順が定められていること。	①定められた手順に従い、個人情報を特定した台帳等の更新及び定期的な見直しが実施されていること。

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)この要求事項の目的

事業者の事業に関連のある法令、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。したがって、事業者の事業に関連のある法令、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・参照する手順が定められ、実施されている必要がある。☞第一部４.ステップ６

(2)ポイント

	文書の作成	運用
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、維持する手順が定められていること。	①参照すべき法令、国が定める指針その他の規範が、定められた手順に従い、特定されていること。
		②参照すべき法令、国が定める指針その他の規範が、必要に応じて更新されていること。
		③特定されている法令、国が定める指針その他の規範が適切であること。
		④特定されている法令、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。

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)この要求事項の目的

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、自社に入って来てから出て行くまで（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い状況が明確になり、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)ポイント

	文書の作成	運用
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。
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定められた手順に従って、リスクを認識し、分析し、対策を講じていること。
		②個人情報毎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)、リスクが認識され、分析され、対策がとられ、残存リスクが把握されていること。
		③講ずることとした対策は、規定に反映されていること。
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定められた手順に従い、リスクの見直しを実施していること。

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)この要求事項の目的

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

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、だからと言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、たと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。

(2)ポイント

	文書の作成	運用
1	各担当者の役割・権限が明確に定められ、文書化されていること。	①各担当者の役割、責任及び権限が明確に定められていること。
		②各担当者の役割・権限が周知されていること。
		③会社法上の監査役、監査委員、又は会計参与が、体制の一部を占めていないこと。
2	個人情報保護管理者は、代表者によって内部から指名するよう規定していること。	①個人情報保護管理者は、代表者によって内部から指名されていること。
		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。
3	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。

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) この要求事項の目的

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) ポイント

	文書の作成	運用
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られていること。
		②a)～o)を含む規程が、従業者に参照できるようになっていること。

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) この要求事項の目的

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。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の審査では、教育や監査については少なくとも年一回以上の実施を要求している（「プライバシーマーク制度設置及び運営要領」第 10 条参照)。

(2) ポイント

	文書の作成	運用
1	事業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。
		②作成された教育計画書の内容が適切であること。
2	事業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。
		②作成された監査計画書の内容が適切であること。

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)この要求事項の目的

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。緊急事態が発生したからと言って、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９e)

(2)ポイント

	文書の作成	運用
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が定められていること。	①定められた手順に従い、緊急事態が特定され、対応されていること。
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が定められていること。	①定められた手順に従い、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が実施されていること。
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が定められていること。	①定められた手順に従い、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。
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が定められていること。	①定められた手順に従い、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。
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が定められていること。	①定められた手順に従い、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。 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。

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)ポイント

この要求事項に対応する特別の審査は無い。手順が明確にされているかは、個々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) この要求事項の目的

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) 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）

(3) ポイント

	文書の作成	運用
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が規定されていること。	①利用目的ができる限り具体的に特定されていること。
2	利用目的の特定に関する手順が定められていること。	①定められた手順に従い、利用目的が特定されていること。
		②個人情報を取扱う従業者は、その利用目的を明確に認識していること。

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) この要求事項の目的

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。」と記述されている。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) 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）

(3) ポイント

	文書の作成	運用
1	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という原則を規定していること。	①個人情報の取得が、適法、かつ、公正な手段によって行われていること。

3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限

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) この要求事項の目的

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。

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について」（厚生労働省労働基準局長 平成 16 年 10 月 26 日）の第 3 の 4 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。

- 健康情報の利用目的に関すること
- 健康情報に係る安全管理体制に関すること
- 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
- 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
- 健康情報の取扱いに関する苦情の処理に関すること

(2) ポイント

	文書の作成	運用
1	a)～e)の特定の機微な個人情報を取得、利用、提供しないという原則を規定していること。	①a)～e)の特定の機微な個人情報が、規格 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。
2	例外的に機微な個人情報の取得、利用、提供する場合は、規格 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。	①a)～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。
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定められた手順に従い、管理者の承認を得ていること。
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。

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) この要求事項の目的

個人情報の取得は本人の同意を得ることが原則である。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。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。☞3.4.2.5 の説明も参照のこと。

「明示し」とは、どこに書いてあるかを明確に指し示す必要がある。たとえば、会員規約や契約約款などを通知書面とする場合に、小さな文字で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。そういったときは、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ずる必要がある。

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。

(2) 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）

(3) ポイント

	文書の作成	運用
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、その承認手順が定められていること。	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、定められた手順に従い、管理者の承認を得ていること。
2	本人に対し、取得する手段毎に手順を定め、a)～h)の必要事項を通知して同意を得るように規定してあること。	①直接書面により取得する個人情報は、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。
		②直接書面取得時に本人に明示する通知書面の内容が a)～h)を満たしていること。
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。
4	ただし書きを適用する場合の承認手順が定められていること。	①ただし書きを適用する場合、定められた手順に従い、管理者の承認を得ていること。

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) この要求事項の目的

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。たとえば、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。

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、何でも 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 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、たとえば、「『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、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、d) に該当するから明示・同意は必要ない」などというのは全く誤った理解である。そのような理解が許されるのであれば、3.4.2.4 の要求事項は殆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。d)はあくまで例外中の例外であると認識しなければならず、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、「大元の取得者（たとえば委託者）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する必要がある。受託の場合でも、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、たとえば、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扱います。」

どこから受託したかは企業秘密であるから通知又は公表する必要はない。

なお、言うまでもないが、要求事項「3.4.2.2 適正な取得」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。

(2) 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)

(3) ポイント

	文書の作成	運用
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、その承認手順が定められていること。	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、定められた手順に従い、管理者の承認を得ていること。
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,	①定められた手順に従い、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。

	文書の作成	運用
	又は公表する手順が定められていること。	②通知又は公表に漏れがないこと。
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。
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、定められた手順に従い、管理者の承認を得ていること。

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) この要求事項の目的

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、この規格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。

なお、企業の合併等では顧客 DB 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。

ただし書きの b)～d)については、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。

(2) 個人情報保護法との対応

①個人情報保護法第15条(利用目的の特定)

②個人情報保護法第16条第3項(目的外利用で同意が不要の場合)

(3) ポイント

	文書の作成	運用
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という原則を明確に規定していること。	①目的外利用をしていないこと。
2	利用目的を変更する場合の承認手順が定められていること。	①定められた手順に従い、管理者の承認を得て利用目的が変更されていること。
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が定められていること。	①定められた手順に従い、本人に通知し同意を得ていること。 ②通知内容が a)～f)の要求事項を満たしていること。
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。
5	ただし書き b)～d)を適用する場合の承認手順が定められていること。	①ただし書き b)～d)を適用する場合、定められた手順に従い、管理者の承認を得ていること。
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。

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) この要求事項の目的

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ツールである。個人情報保護法も JISQ15001 も、個人情報の保護と個人情報の有効活用とのバランスをとったものであるが、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、自分の情報をどこからどのように取得したのかを知りたい。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、住民基本台帳、電話帳、登記簿等の「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、要求事項「3.4.2.2 適正な取得」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。

なお、ただし書き b)により委託を受けた場合であっても、もし委託者が適正な取得をしていなかった場合は、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。それはこの規格の趣旨に反する。したがって、委託を受けた者は、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しなければならない。不適正な取得であると知りながら委託を受けた場合は、要求事項「3.4.2.2 適正な取得」を満たしていないことになる。

(2) 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(目的外利用で同意が不要の場合)

(3) ポイント

	文書の作成	運用
1	本人にアクセスすることについての承認手順が定められていること。	①定められた手順に従い、管理者の承認を得ていること。
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が規定されていること。	①定められた手順に従い、本人の同意を得る手順が実施されていること。
		②本人に通知する内容が、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。
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。
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定められた手順に従い、管理者の承認を得ていること。
5	ただし書き b)の場合、委託元が個人情報保護法及びガイドライン等に沿って適切に個人情報を取扱っていることを確認するよう規定していること。	①定められた手順に従い、委託元に確認していること。

	文書の作成	運用
6	ただし書き **d)**を適用する場合、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が定められていること。	①定められた手順に従い、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。

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)この要求事項の目的

個人情報を第三者に提供する場合は、本人の同意を得ることが原則である。

言うまでもないことであるが、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。

目的外の提供をする場合に同意を得る必要があることについて、1999 版では **4.4.3.2** に『収集目的の範囲外の利用及び提供に関する措置』の中に明記されているが、2006 版では明記されていない。明記されていない理由は、目的外の提供は、すなわち目的外利用であるため、当然、本体の **3.4.2.6** により、本人の同意を得る必要があると考えられているからである。

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」ことだけでは足りない。また、**b)**は安易に適用してはならないのであって、適用基準を定める必要がある。

ただし書き **d)**については、取得した時は委託する予定がなく、取得する時に委託する旨通知していなかったが、分社化や業務の拡大などにより、事後的に委託せざるを得なくなった場合、というのが含まれる。

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** の要求事項が適用されることに注意する必要がある。

(2)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(目的外利用で同意が不要の場合)

(3)ポイント

	文書の作成	運用
1	第三者に提供する場合、承認手順が定められていること。	①定められた手順に従い、管理者の承認を得ていること。
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定められた手順に従い、本人に通知し同意を得る手順を実施していること。
		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。
		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。
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。
4	ただし書き **b)**～**g)**を適用する場合の承認手順を定めてしていること。	①定められた手順に従い、管理者の承認を得ていること。
		②ただし書き **b)**の適用について、適用基準が定められていること。

	文書の作成	運用
5	ただし書き b)を適用する場合、必要な措置を講じる手順が定められていること。	①定められた手順に従い、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。
6	ただし書き c)を適用する場合、必要な措置を講じる手順が定められていること。	①定められた手順に従い、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、又は本人が容易に知り得る状態に置いていること
7	ただし書き f)を適用する場合、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が定められていること。	①定められた手順に従い、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。

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) この要求事項の目的

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９g)

(2) 個人情報保護法との対応

①個人情報保護法第19条(正確性の確保)

(3) ポイント

	文書の作成	運用
1	誤入力チェックを行うよう定められていること。	①定められた手順に従い、誤入力チェックが実施されていること。
2	個人情報の保存期間を定める手順が定められていること。	①定められた手順に従い、保存期間が定められていること。
3	個人情報のバックアップを実施する手順が定められていること。	①定められた手順に従い、バックアップが実施されていること。

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) この要求事項の目的

事業者は、取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、「3.3.3 リスクなどの認識、分析及び対策」と連動する。3.3.3 において講ずることとした対策が、安全管理措置に反映されるはずであり、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９g)

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、たと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) 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)

(3) ポイント

『個人情報保護に関する法律についての経済産業分野のガイドライン（平成 16 年 10 月)』に記述された安全管理措置が参考になる。ただし、事業者は、リスクの認識、分析及び対策（3.3.3）により講ず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って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。

安全管理措置	チェック項目
1. 物理的安全管理措置	
1.1 入退館（室）管理	①建物、室、マシン室、個人情報の取り扱い場所への入退の制限機構がある。
	②建物、室、マシン室、個人情報の取り扱い場所への入退が制限されている。
	③建物、室、マシン室、個人情報の取り扱い場所への入退の記録が取られ、保管されている。
	④建物、室、マシン室、個人情報の取り扱い場所への入退の記録は定期的にチェックされている。
1.2 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。
	②個人情報を取扱う PC 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。
	③個人情報を記録した媒体（記録媒体、紙）は施錠保管され、あるべきものが全てあることが把握されている。
	④個人情報を記録した媒体（記録媒体、紙）の保管場所の鍵は特定者が管理している。

安全管理措置	チェック項目
	⑤個人情報を記録した媒体（記録媒体、紙）の廃棄は、再利用できない措置を講じている。
	⑥個人情報を記録した携帯可能な PC 等の盗難防止措置が施されている。
	⑦FD、MO、CD、USB フラッシュメモリ等の外部記憶媒体の利用はルールに従っている。
	⑧個人情報を取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。
1.3 機器・装置等の物理的な保護	①個人情報を取扱う機器・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）からの物理的な保護装置がある。
2.技術的安全管理措置	
2.1 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）による認証が実施されている。
	②個人情報を格納した情報システムは、デフォルトの設定を残していない。
	③識別情報の発行・更新・廃棄は、ルールに従っている。
	④識別情報は平文で記録していない。
	⑤パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID の停止等の措置が講じられている。
	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は、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、制限されている。
2.2 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である。
	②個人情報にアクセスできる識別情報を複数人で共用していない。
	③従業者に付与するアクセス権限は必要最小限である。
	④個人情報を格納した情報システムの同時利用者数は制限されている。
	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。
	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。

安全管理措置	チェック項目
	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。
	⑧個人情報を取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。
2.3 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。
	②個人情報を取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。
2.4 個人情報へのアクセス記録	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。
	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。
2.5 個人情報を取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が導入され、常に最新版が適用されている。
	②OS 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。
	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。
	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 や Share など）をインストールしていない。
2.6 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が残されている。
	②個人情報を媒体で移送する時に、移送時の紛失・盗難が生じた際の対策が講じられている。
	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（例えば本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際に、個人情報の暗号化又はパスワードロック等を実施している。
2.7 個人情報を取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。
	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。
2.8 個人情報を取扱う情報システムの監視	①個人情報を取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。
	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。

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) この要求事項の目的

個人情報を取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。

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。なお、経済産業省が平成 17 年 10 月に公表した『営業秘密管理指針（改訂版）』pp. 34 では、次のように記述されている。

> 『...派遣先企業と派遣従業者とが直接秘密保持契約を締結することが直ちに法律違反になるわけではないが、労働者派遣事業制度の趣旨からは、派遣先は、派遣従業者と直接秘密保持契約を締結するよりもむしろ、雇用主である派遣元事業主との間で秘密保持契約を締結し、派遣元事業主が派遣先に対し派遣従業者による秘密保持に関する責任を負うこととすることが望ましいものである。...』

この趣旨は、派遣先企業は派遣契約に基づき派遣従業者に対する指揮命令権はあるが、派遣従業者とは雇用契約関係にはないため懲戒権はない、したがって、雇用関係にならない誓約書なら許されるが、懲戒処分（契約の打切り等）を定めるような誓約書は、派遣元と派遣先の二重雇用状態になり、職業安定法 44 条（労働者供給事業の禁止）に抵触し許されないということである。

したがって、事業者同士で秘密保持契約を締結しているのであれば、事業者は、受入派遣社員等の個々人と秘密保持契約を締結する必要はない。そういった場合に更に懲戒処分を含むような秘密保持契約の締結を求めることは違法であり、個人情報保護法への過剰反応である。

また、従業者の監督という点では、「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」（平成 16 年厚生労働省告示第 259 号）第三 九（一）に規定する「雇用管理に関する個人情報の取扱いに関する重要事項」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必要がある旨定めら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に関する事項は、上記指針でいう重要事項に該当する。

(2) 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）

(3) ポイント

	文書の作成	運用
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規格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。

	文書の作成	運用
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。
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であるように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されていること。
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定が整備されていること。	①個人情報保護マネジメントシステムに違反した場合、規定に従って措置が実施されていること。

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) この要求事項の目的

個人情報を取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。

なお、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は、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、これらの事業者との契約も、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契約書の中に盛り込んでおくことが望ましい。

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込むことまで求めるものではない。

(2) 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）

(3) ポイント

	文書の作成	運用
1	委託先選定基準を定める手順及び見直しの手順が定められていること。	①定められた手順に従い、委託先選定基準が確立されていること。
		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。
		③必要に応じて委託先選定基準の見直しが実施されていること。
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）。
		②委託先の認識に漏れがないこと。
3	a)～g)の内容が盛り込んだ契約書を締結する手順が定められていること。	①定められた手順に従い、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。
		②定められた手順に従い、a)～g)の内容が盛り込まれた契約書を締結していること。
		③契約書の内容が実行されていること。

	文書の作成	運用
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定められた手順に従い、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。

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)この要求事項の目的

個人情報を取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。

ただし書き a)～d)については、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。

(2)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政令第3条(保有個人データに該当しない場合)

③政令第4条(保有個人データとなる期間)※ただし政令第４条は本規格では適用せず。

(3)ポイント

	文書の作成	運用
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が規定されていること。	①開示等の求めに応じていること。
		②開示対象個人情報に漏れがないこと。
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、ただし書きに限定されていること。
3	ただし書きが適用される場合の承認手順が定められていること。	①定められた手順に従い、管理者の承認を得ていること。

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)この要求事項の目的

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。なお、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来ていないのではないかと疑ってみる必要がある。

(2)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政令第7条(開示等の求めを受け付ける方法として定めることができる事項)
③政令第8条(開示等の求めをすることができる代理人)

(3)ポイント

	文書の作成	運用
1	規格のa)～d)の事項について、応じる手順が、それぞれ規定されていること。	①a)の事項が適切に定められていること。
		②b)の事項が適切に定められていること。
		③c)の事項が適切に定められていること。
		④手数料を徴収する場合、d)の事項が適切に定められていること。
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。

3.4.4.3 開示対象個人情報に関する事項の周知など

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)この要求事項の目的

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。3.4.2.4 や 3.4.2.6～3.4.2.8 により、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。

(2)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政令第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)

(3)ポイント

	文書の作成	運用
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が定められていること。	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。
		②開示対象個人情報について、本人の容易に知り得る状態に置いている内容が、規格の a)～f)の要求事項を満たしていること。

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)この要求事項の目的

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)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）

(3)ポイント

	文書の作成	運用
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定められた手順に従い、本人の求めに応じていること。 ②遅滞なく実施していること。
2	本人への回答内容（求めに応じない場合を含む）に関する承認手順が定められていること。	①定められた手順に従い、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。
3	利用目的を通知しないのは、規格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、規格が定めるただし書きの場合のみであること。
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が定められていること。	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。

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)この要求事項の目的

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。

ただし書き b)については、規格本体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。

(2)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政令第６条（保有個人データの開示を求められたときの方法）

(3)ポイント

	文書の作成	運用
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定められた手順に従い、本人の求めに応じていること。 ②遅滞なく実施していること。
2	本人への回答内容（求めに応じない場合を含む）に関する承認手順が定められていること。	①定められた手順に従い、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。
3	開示の求めに応じないのは、規格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、規格が定めるただし書きの場合のみであること。
4	ただし書きにより本人に開示しない場合の承認手順が定められていること。	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。

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)この要求事項の目的

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。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を、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定める必要がある。

(2)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）

(3)ポイント

	文書の作成	運用
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定められた手順に従い、本人の求めに応じていること。 ②遅滞なく実施していること。
2	本人への回答内容（求めに応じない場合を含む）に関する承認手順が定められていること。	①定められた手順に従い、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。
3	訂正等を行わない場合の承認手順が定められていること。	①訂正等を行わない場合、管理者の承認を得ていること。

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)この要求事項の目的

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。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）、本人同意無しの第三者提供（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。しかしこの規格では、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。

ただし書きで 3.4.4.5 の 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。

(2)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）

(3)ポイント

	文書の作成	運用
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定められた手順に従い、本人の求めに応じていること。
		②遅滞なく実施していること。
2	本人への回答内容（求めに応じない場合を含む）の承認手順が定められていること。	①定められた手順に従い、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。
3	利用停止等の求めに応じないのは、規格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、規格が定めるただし書きの場合のみであること。
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が定められていること。	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。

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) この要求事項の目的

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。

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（たとえば、従業者の情報、名刺の情報など）に接する可能性はあるからである。

なお、プライバシーマークの審査では、少なくとも年 1 回以上の教育の実施を求めている（「プライバシーマーク制度設置及び運営要領」第 10 条参照）。

(2) ポイント

	文書の作成	運用
1	全ての従業者に、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、教育が実施されていること。
		②全ての従業者に個人情報保護に関する適切な教育が実施されていること。
2	規定又は教育計画書に、少なくとも a)～c)の内容が含まれていること。	①教材に a)～c)の内容が含まれていること。
3	受講者の理解度確認を実施する手順が規定されていること。	①受講者の理解度確認を実施していること。
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が規定されていること。	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られ、実施されていること。

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)この要求事項の目的

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)ポイント

	文書の作成	運用
1	個人情報保護マネジメントシステム文書の範囲が明確であり、最低限、a)～d)が含まれていること。	①個人情報保護マネジメントシステムの基本となる要素を、a)～d)を含め書面で記述していること。

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)この要求事項の目的

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)ポイント

	文書の作成	運用
1	記録を除く文書の管理について、少なくともa)～c)の具体的な手順が定められていること。	①定められた手順にしたがって、文書が管理されていること。

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)この要求事項の目的

この規格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。なお、記録自体が個人情報である場合もあるから、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、この規格によって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、必要に応じて作成するようにしなければならない。

(2)ポイント

	文書の作成	運用
1	記録の管理手順が明確に定められていること。	①定められた手順に従い、記録が管理されていること。

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)この要求事項の目的

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。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来ていないのではないかと疑ってみる必要がある。

(2)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）

(3)ポイント

	文書の作成	運用
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が定められていること。	①苦情の宛先が、本人にとって明確であること。
		②定められた手順に従って受け付けられ、対応されていること。
		③対応が迅速であること。
		④受け付ける手順が機能していること。
2	本人に回答する対応内容に関する承認手順が定められていること。	①定められた手順に従い、対応内容について管理者の承認を得ていること。
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が定められていること。	②定められた手順に従い、代表者に報告されていること。

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)この要求事項の目的

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。日常的な運用の確認が実施されるために業務に支障がでるというのでは本末転倒であるから、この要求事項はそれほど大げさなものは想定していないと理解される。ルールどおり実施されているか見回って確認するといったことでも良い。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。たとえば、

a)最終退出時の社内点検（施錠確認等）の記録を残し、定期的に確認すること
b)最初に出社した人と最後に退社した人の記録を残し、定期的に確認すること
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、定期的に確認すること

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。

(2)ポイント

	文書の作成	運用
1	個人情報保護マネジメントシステムが適切に運用されていることが、事業者の各部門及び階層において、定期的に確認されるための手順が定められていること。	①個人情報保護マネジメントシステムが適切に運用されていることが、事業者の各部門及び階層において、定期的に確認されていること。

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)この要求事項の目的

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

個人情報保護マネジメントシステムのこの規格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、何にもならないからである。

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、特段の公的資格は必要でない。

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（たとえば、従業者の情報、名刺の情報など）に接する可能性はあるからである。

なお、プライバシーマークの審査では、少なくとも年1回以上の監査の実施を求めている（「プライバシーマーク制度設置及び運営要領」第10条参照）。

(2)ポイント

	文書の作成	運用
1	JIS 規格との合致及びその運用状況について監査するよう規定されていること。	①監査計画書に従って監査が実施されていること。
		②JIS 規格との合致について監査が実施されていること。
		③運用状況について監査が実施されていること。
		④全部門の監査が実施されていること。
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されていること。	①個人情報保護監査責任者は、代表者によって事業者の内部から指名されていること。
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されていること。	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。
4	監査員は、自ら所属する部門を監査しないよう規定されていること。	①監査員は、自ら所属する部門を監査していないこと。
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が定められていること。	①定められた手順に従い、監査の計画及び実施、結果の報告並びにこれに伴う記録が保持されていること。

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)この要求事項の目的

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。不適合が発見される場面としては、たとえば、1.d)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全て、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の原因を特定し対策を講じて再発を防止することであり、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。

(2)ポイント

	文書の作成	運用
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が実施されていること。
2	是正処置及び予防処置を確実に実施するための手順が、a)～e)の事項を含めて定められていること。	①定められた手順に従い、是正処置及び予防処置が、a)～e)の事項を含めて実施されていること。

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)この要求事項の目的

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、現状を前提とせず見直すことを要求している。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、経営判断が求められていると言える。したがって、この「3.9 事業者の代表者による見直し」は、日々の是正や 3.7.2 の監査に基づく改善とは次元が異なることに注意する必要がある。

(2)ポイント

	文書の作成	運用
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されていること。	①規定に従い、代表者による見直しが実施されていること。
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。

－付録－
JISQ15001:1999 をベースにして作成した内部規程に、JISQ15001:2006 を取込む際の注意点

2006 版項目	1999 版で対応する項目及び注意点
1. 適用範囲	1. 適用範囲
	①1999 版は 2006 版よりも対象範囲が狭い。適用される個人情報の範囲に、最低限、「事業の用に供しているもの」が含まれるよう修正する必要がある。
2. 用語及び定義	3. 定義
	①1999 版では無かった定義は、追加している必要がある。 ②個人情報保護監査責任者（以下、監査責任者という。）の定義に、内部からの指名を明確にする必要がある。 ③本人の同意について、「本人が子ども又は事理を弁識する能力を欠く者の場合は，法定代理人等の同意も得なければならない」趣旨を盛込む必要がある。 ④1999 版の定義が残っていても特段の問題はない。
3.1 一般要求事項	4.1 一般要求事項
	特段の対応は不要。
3.2 個人情報保護方針	4.2 個人情報保護方針
	①個人情報保護の理念を明確にした記述が必要である。 ②a)について、目的外利用に関する記述が必要である。 ③c)について、1999 版 b)では「個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの...」となっているが、その表現でも良い。 ③d)項に関する記述を追加する必要がある。 ④f)については、これまでの 1999 版での審査においても事実上要求項目に含まれるものとして指摘してきた。審査基準が明らかになったといえる。
3.3.1 個人情報の特定	4.3.1 個人情報の特定（前段）
	特段の対応は必要でない。
3.3.2 法令、国が定める指針その他の規範	4.3.2 法令及びその他の規範
	特段の対応は必要でない。
3.3.3 リスクなどの認識、分析及び対策	4.3.1 個人情報の特定（後段）
	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，維持しなければならない」旨の記述が追加されている必要がある。 ②2006 版の「個人情報の漏えい，滅失又はき損」の代わりに、1999 版の表現を維持し、「個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい」と記述してあっても良い。ただし、2006 版の「個人情報保護法との対応，国が定める指針その他の規範に対する違反，想定される経済的な不利益及び社会的な信用の失墜，本人への影響などのおそれな

2006 版項目	1999 版で対応する項目及び注意点
	ど」という記述は追加する必要がある。 ③2006 版により、ライフサイクルに従ったリスクの認識、評価及び対策を実施すべきことが明確になった。「その取扱いの各局面におけるリスク」という表現の趣旨を盛込む必要がある。
3.3.4 資源，役割，責任及び権限	**4.4.1 体制及び責任**
	①2006 版の最後の段落「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。」旨を追加する必要がある。
3.3.5 内部規程	**4.3.3 内部規程**
	確立した手順は文書化するというのがこの要求事項の趣旨であり、取組みやすいように規定名で例示してある。2006 版はその数が 1999 版よりも増えているだけで、趣旨に変更はない。
3.3.6 計画書	**4.3.4 計画書**
	特段の対応は不要。
3.3.7 緊急事態への準備	－
	2006 版において新設された要求事項であり、1999 版には該当するものがない。2006 版 3.3.7 に従って規定を追加する必要がある。
3.4 実施及び運用	**4.4 実施及び運用**
3.4.1 運用手順	－
	2006 版で新設された要求事項であり、1999 版に該当するものはないが、特段の対応は必要でない。
3.4.2.1 利用目的の特定	**4.4.2.1 収集の原則**
	1999 版では「収集」目的とあるが、それでも良い。また、1999 版では「収集目的を明確に定め」とあるが、これは解釈上、2006 版の「利用目的をできる限り特定し」と同義であり、1999 版の表現でも良い。特段の対応は必要でない。
3.4.2.2 適正な取得	**4.4.2.2 収集方法の制限**
	特段の対応は必要でない。
3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限	**4.4.2.3 特定の機微な個人情報の収集の禁止**
	①適用除外の場合が明確になった。2006 版 3.4.2.3 のただし書きを盛込む必要がある。
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	**4.4.2.4 情報主体から直接収集する場合の措置**
	1999 版と 2006 版では、取得に関する区分が異なることに注意する必要がある。1999 版では直接取得と間接取得に区分されるが、2006 版では、直接書面取得とそれ以外に区分され、間接収集という概念が無くなった。以下の対応が必要である。 ①2006 版では明示項目が増えているため、明示項目の修正が必要である。

2006 版項目	1999 版で対応する項目及び注意点
	②「書面により明示し」を盛込む必要がある。 ③2006 版 3.4.2.4 のただし書きの内容を盛込む必要がある。
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	－
	この要求事項は 2006 版によって新設され、1999 版には該当する事項がない。2006 版 3.4.2.5 の要求事項に従った規定を追加する必要がある。
3.4.2.6 利用に関する措置	**4.4.3.1 利用及び提供の原則** **4.4.3.2 収集目的の範囲外の利用及び提供の場合の措置**
	①2006 版 3.4.2.4 は、1999 版 4.4.2.4 より通知事項が増えている。漏れがないよう修正する必要がある。 ②4.4.3.1 のなお書き b)は、2006 版 3.4.2.6 b)～d)に置き換え、内容を明確にする必要がある。
3.4.2.7 本人にアクセスする場合の措置	**4.4.2.5 情報主体以外から間接的に収集する場合の措置**
	①2006 版 3.4.2.4 では通知事項が増えている。漏れがないよう修正する必要がある。 ②2006 版 3.4.2.4 のただし書き b)～e)に該当する場合がないときは、追加する必要はない。 ③1999 版 4.4.2.5c)に該当するのは、2006 版 3.4.2.6 のただし書き a)～d) のいずれかに該当する場合であるから、その旨を明確に規定する必要がある。
3.4.2.8 提供に関する措置	**4.4.3.1 利用及び提供の原則** **4.4.3.2 収集目的の範囲外の利用及び提供の場合の措置**
	①2006 版 3.4.2.4 では通知事項が増えている。漏れがないよう修正する必要がある。 ②1999 版 4.4.3.1 b) は、2006 版 3.4.2.6 b)～d)に置き換え、内容を明確にする必要がある。 ③2006 版 3.4.2.8 のただし書き b)～f)に該当する場合が無いときは、追加する必要はない。
3.4.3.1 正確性の確保	**4.4.4.1 個人情報の正確性の確保**
	特段の対応は必要でない。
3.4.3.2 安全管理措置	**4.4.4.2 個人情報の利用の安全性の確保**
	2006 版の「個人情報の漏えい、滅失又はき損」の代わりに、1999 版の表現を維持し、「個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなど」と記述してあっても良い。特段の対応は必要でない。
3.4.3.3 従業者の監督	－
	2006 版において新設された要求事項であり、1999 版には該当する要求事項はない。2006 版 3.4.3.3 に従った規定を追加する必要がある。
3.4.3.4 委託先の監督	4.4.4.3 個人情報の委託処理に関する措置

2006 版項目	1999 版で対応する項目及び注意点
	2006 版では契約書に規定すべき事項が詳細になっている。2006 版にあわせる必要がある。
3.4.4.1 個人情報に関する権利 3.4.4.2 開示等の求めに応じる手続 3.4.4.3 開示対象個人情報に関する事項の周知など 3.4.4.4 開示対象個人情報の利用目的の通知 3.4.4.5 開示対象個人情報の開示 3.4.4.6 開示対象個人情報の訂正、追加又は削除	**4.4.5.1 個人情報に関する権利** 2006 版 3.4.4.1～3.4.4.6 は、1999 版 4.4.5.1 を詳細にしたものであり、基準が明確になったと言える。以下の対応が必要である。 ①2006 版によりなすべきことが明確になった。1999 版 4.4.5.1 に代え、2006 版 3.4.4.1～3.4.4.6 を取り込む必要がある。 ②1999 版 4.4.5.1 では、訂正等を行った場合、可能な限り受領者にも通知するようになっているが、これは共同利用の場合を想定している。2006 版では共同利用の場合の取扱いについて、3.4.2.7 や 3.4.2.8 等に定められ、また 3.4.4.1～3.4.4.6 の手続も整備されたのであるから、それに基づいて運用する必要がある。
3.4.4.7 開示対象個人情報の利用又は提供の拒否権	**4.4.5.2 個人情報の利用又は提供の拒否権** 2006 版 3.4.4.7 は、1999 版 4.4.5.2 を詳細にしたものであり、なすべきことが明確になったと言える。したがって、2006 版 3.4.4.7 の内容を盛込む必要がある。
3.4.5 教育	**4.4.6 教育** 2006 版 3.4.5 の後段の文章を追加する必要がある。
3.5.1 文書の範囲	**4.4.8 コンプライアンス・プログラム文書** 2006 版 3.5.1 によって、内容が明確になった。2006 版 3.5.1 の内容を盛込む必要がある。
3.5.2 文書管理	**4.4.9 文書管理** 2006 版 3.5.2 によって、内容が明確になった。2006 版 3.5.2 の内容を盛込む必要がある。
3.5.3 記録の管理	**4.4.9 文書管理** 2006 版 3.5.3 によって、内容が明確になった。2006 版 3.5.3 の内容を盛込む必要がある。
3.6 苦情及び相談への対応	**4.4.7 苦情及び相談** ①2006 版 3.6 の「迅速な対応」について、規定を追加する必要がある。 ②認定個人情報保護団体の対象事業者である場合、当該団体の連絡先も明示するよう規定する必要がある。
3.7.1 運用の確認	－ 2006 版で新設された要求事項であり、1999 版に該当するものは無い。2006 版 3.7.1 に対応する規定を新たに追加する必要がある。
3.7.2 監査	**4.5 監査**

2006 版項目	1999 版で対応する項目及び注意点
	①「事業者の代表者は、公平かつ客観的な立場にある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、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。」の趣旨を盛込む必要がある。 ②「監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しなければならない。」の趣旨を盛込む必要がある。
3.8 是正処置及び予防処置	－
	2006 版により新設された要求事項であり、1999 版には該当するものがない。以下の対応が必要である。 ①2006 版 3.8 に対応する規定を追加する必要がある。 ②発見された不適合と 3.8 との関係を明確にする必要がある。
3.9 事業者の代表者による見直し	4.6 事業者の代表者による見直し
	2006 版 3.9 により見直しの範囲が詳細に定められた。2006 版 3.9 の a)～g)を盛込む必要がある。

本ガイドラインの無断転載を禁じます