目　次

まえがき

この規格は，工業標準化法に基づき，日本工業標準調査会の審議を経て，経済産業大臣が改正した日本工業規格である。

これによって，**JIS Q 15001**:1999 は改正され，この規格に置き換えられた。

この規格は，著作権法で保護対象となっている著作物である。

この規格の一部が，技術的性質をもつ特許権，出願公開後の特許出願，実用新案権，又は出願公開後の実用新案登録出願に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本工業標準調査会は，このような技術的性質をもつ特許権，出願公開後の特許出願，実用新案権，又は出願公開後の実用新案登録出願にかかわる確認について，責任をもたない。

日本工業規格（案）　　JIS
Q 15001：2006

個人情報保護マネジメントシステム―要求事項

Personal information protection management systems—Requirements

1　適用範囲

この規格は，個人情報を事業の用に供している，あらゆる種類，規模の事業者に適用できる個人情報保護マネジメントシステムに関する要求事項について規定する。

事業者は，次の事項を行う際に，この規格を用いることができる。

a) 個人情報保護マネジメントシステムを策定し，実施し，維持し，及び改善する。

b) この規格と個人情報保護マネジメントシステムとの適合性について自ら確認し，適合していることを自ら表明する。

c) 外部組織又は本人に，この規格と個人情報保護マネジメントシステムとの適合性について確認を求める。

2　引用規格

現時点では，引用規格はない。

3　用語及び定義

この規格で用いる主な用語及び定義は，次による。

3.1

個人情報

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

3.2

本人

個人情報によって識別される特定の個人。

3.3

事業者

事業を営む法人，その他団体又は個人。

3.4

管理者

事業者の内部において代表者から指名された者であって，個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限をもつ者。

3.5

監査責任者

事業者の内部において代表者から指名されたものであって，公平，かつ，客観的な立場にあり，監査の実施及び報告を行う責任及び権限をもつ者。

3.6

本人の同意

本人が，取得，利用又は提供に関する情報を与えられた上で，自己に関する個人情報の取得，利用又は提供について承諾する意思表示。本人が子どもの場合は，保護者の同意も得るべきである。

3.7

個人情報保護マネジメントシステム

事業者が，自らの事業の用に供する個人情報を保護するための方針，体制，計画，実施，監査及び見直しを含むマネジメントシステム。

3.8

不適合

要求事項を満たしていないこと。

3.9

是正処置

検出された不適合の原因を除去するための処置。

4　要求事項

4.1　一般要求事項

事業者は，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，及び改善しなければならない。その要求事項は，箇条 **4** 全体で規定する。

4.2　個人情報保護方針

事業者の代表者は，個人情報保護の理念を明確にした上で，次の事項を含む個人情報保護方針を定めるとともに，これを実行し維持しなければならない。

a) 事業の内容及び規模を考慮した適切な個人情報の取得，利用及び提供に関すること（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下，“ 目的外利用 ” という。）を行わないこと及びそのための措置を講じることを含む。）。

b) 個人情報への不正アクセス，個人情報の漏えい，滅失又はき損の防止並びに是正に関すること。

c) 苦情対応に関すること。

d) 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を遵守すること。

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。

f) 代表者の氏名

事業者の代表者は，この方針を文書（電子的方式，磁気的方式その他人の知覚によっては認識できない方式で作られる記録を含む。以下，同じ。）化し，従業者に周知させるとともに，一般の人が入手可能な措置を講じなければならない。

4.3　計画

4.3.1　個人情報の特定

事業者は，自らの事業の用に供するすべての個人情報を特定するための手順を確立し，維持しなければ

ならない。

4.3.2 法令，国が定める指針及びその他の規範

事業者は，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を特定し参照できる手順を確立し，維持しなければならない。

4.3.3 リスクなどの認識・分析及び対策

事業者は，**4.3.1** によって特定した個人情報について，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，維持しなければならない。

事業者は，**4.3.1** によって特定した個人情報について，その取扱いの各局面におけるリスク（個人情報の漏えい，滅失又はき損，関連する法令及びその他の規範に対する違反，想定される経済的な不利益及び社会的な信用の失墜などのおそれなど）を認識し，分析し，必要な対策を講じる手順を確立し，維持しなければならない。

4.3.4 資源，役割，責任及び権限

事業者の代表者は，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，改善するために不可欠な資源を用意しなければならない。

事業者の代表者は，個人情報保護マネジメントシステムを効果的に実施するために役割，責任及び権限を定め，文書化し，かつ，従業者に周知しなければならない。

事業者の代表者は，この規格の内容を理解し実践する能力のある管理者を事業者の内部から指名し，個人情報保護マネジメントシステムの実施及び運用に関する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。

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実績を報告しなければならない。

4.3.5 内部規程

事業者は，次の事項を含む内部規程を文書化し，維持しなければならない。

a) 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の規定。

b) 個人情報を特定する手順に関する規定。

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) 法令，国が定める指針及びその他の規範の特定，参照及び維持に関する規定。

e) 個人情報の取得，利用，提供の規定。

f) 個人情報の適正管理に関する規定。

g) 本人からの開示など（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）の求めに関する規定。

h) 苦情対応に関する規定。

i) 個人情報保護に関する教育の規定。

j) 個人情報保護に関する内部監査の規定。

k) 内部規程の違反に関する罰則の規定。

l) 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。

m) 緊急事態への準備及び対応に関する規定。

n) 代表者による見直しに関する規定。

事業者は，事業の内容に応じて，個人情報保護マネジメントシステムが確実に適用されるように内部規

程を改定しなければならない。

4.3.6 計画書

事業者は，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に必要な教育，監査などの計画を立案し，文書化し，かつ，維持しなければならない。

4.3.7 緊急事態への準備

事業者は，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確立し，実施し，維持しなければならない。

事業者は，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確立し，維持しなければならない。

また，個人情報の漏えい，滅失又はき損が発生した場合に備え，次の事項を含む対応手順を確立し，維持しなければならない。

a) 当該漏えい，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こと。

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，遅滞なく公表すること。

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こと。

4.4 実施及び運用

4.4.1 運用管理

事業者は，個人情報保護マネジメントシステムが確実に実施されるように，運用の手順を明確にしなければならない。

4.4.2 取得・利用及び提供に関する原則

4.4.2.1 利用目的の特定

個人情報を取得するに当たっては，その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。

4.4.2.2 適正な取得

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。

4.4.2.3 特定の機微な個人情報の取得の制限

次に示す内容を含む個人情報の取得，利用又は提供は，行ってはならない。ただし，これらの取得，利用又は提供について，明示的な本人の同意がある場合及び **4.4.2.6** のただし書き **a)**～**d)** のいずれかに該当する場合は，この限りでない。

a) 思想，信条及び宗教に関する事項。

b) 人種，民族，門地，本籍地，身体・精神障害，犯罪歴，その他社会的差別の原因となる事項。

c) 勤労者の団結権，団体交渉及びその他団体行動の行為に関する事項。

d) 集団示威行為への参加，請願権の行使，及びその他の政治的権利の行使に関する事項。

e) 保健医療及び性生活。

4.4.2.4 本人から直接書面によって取得する場合の措置

本人から，書面（電子的方式，磁気的方式その他人の知覚によっては認識できない方式で作られる記録を含む。以下，同じ。）に記載された個人情報を直接に取得する場合には，少なくとも，次に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，書面によって明示し，本人の同意を得なければならない。ただし，人の生命，身体又は財産の保護のために緊急に必要がある場合及び **4.4.2.5** のただし書き **a)**～**d)** の

いずれかに該当する場合は明示及び同意を必要とせず，**4.4.2.6** のただし書き **a)**～**d)** のいずれかに該当する場合は同意を必要としない。

a) 事業者の氏名又は名称

b) 管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先。

c) 利用目的。

d) 個人情報を第三者に提供することが予定される場合の事項。

- 第三者に提供する目的
- 提供する個人情報の項目
- 提供の手段又は方法
- 当該情報の提供を受ける者又は提供を受ける者の組織の種類，属性
- 個人情報の取扱いに関する契約がある場合はその旨

e) 個人情報の取扱いの委託を行うことが予定される場合には，その旨。

f) **4.4.4.5**～**4.4.4.7** に該当する場合には，その求めに応じる旨及び問合せ窓口。

g) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果。

h) 本人が容易に認識できない方法によって個人情報を取得する場合には，その旨。

4.4.2.5 個人情報を 4.4.2.4 以外の方法によって取得した場合の措置

個人情報を **4.4.2.4** 以外の方法によって取得した場合は，あらかじめその利用目的を公表している場合を除き，速やかにその利用目的を，本人に通知し，又は公表しなければならない。ただし，次に示すいずれかに該当する場合は，通知又は公表を必要としない。

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

b) 利用目的を本人に通知し，又は公表することによって当該事業者の権利又は正当な利益を害するおそれがある場合。

c) 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって，利用目的を本人に通知し，又は公表することによって当該事務の遂行に支障を及ぼすおそれがあるとき。

d) 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。

4.4.2.6 利用に関する措置

個人情報の利用は，特定した利用目的の達成に必要な範囲内で行わなければならない。

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利用する場合は，あらかじめ，少なくとも，**4.4.2.4** の **a)**～**f)** に示す事項又はそれと同等以上の内容の事項を書面によって本人に通知し，本人の同意を得なければならない。ただし，次に示すいずれかに該当する場合は，本人の同意を必要としない。

a) 法令に基づく場合。

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

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

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

4.4.2.7 本人にアクセスする場合の措置

個人情報を利用して本人にアクセスする場合には，本人に対して，**4.4.2.4** 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，本人の同意を得なければならない。ただし，次に示すいずれかに該当する場合は，この限りではない。

a) 個人情報の取得時に，既に **4.4.2.4** の **a)**～**f)** に示す事項又はそれと同等以上の内容の事項を明示又は通知し，本人の同意を得ているとき。

b) 個人情報の取扱いの全部又は一部を委託された場合であって，当該個人情報を，その利用目的の達成に必要な範囲内で取り扱うとき。

c) 合併その他の事由による事業の承継に伴って個人情報が提供された場合であって，承継前の利用目的の範囲内で当該個人情報を取り扱うとき。

d) 個人情報を特定の者との間で共同して利用する場合であって，次に示す事項又はそれと同等以上の内容を，あらかじめ，本人に通知しているとき。

- 共同して利用すること
- 共同して利用される個人情報の項目
- 共同して利用する者の範囲
- 利用する者の利用目的
- 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
- 取得方法

e) **4.4.2.5** のただし書き **d)** に該当するため，利用目的などを明示，通知又は公表することなく取得した個人情報を利用して，本人にアクセスするとき。

f) **4.4.2.6** のただし書き **a)**～**d)** のいずれかに該当する場合

4.4.2.8 提供に関する措置

個人情報を第三者に提供する場合には，あらかじめ本人に対して、取得方法並びに **4.4.2.4** 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，本人の同意を得なければならない。ただし，次に示すいずれかに該当する場合は，この限りではない。

a) **4.4.2.4** 又は **4.4.2.7** の規定によって，既に **4.4.2.4** の **a)** ～**d)** の事項又はそれと同等以上の内容の事項を本人に明示又は通知し，本人の同意を得ているとき。

b) 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であって，次に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，又はそれに代わる同等の措置を講じているとき。

- 第三者への提供を利用目的とすること
- 第三者に提供される個人情報の項目
- 第三者への提供の手段又は方法
- 本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること
- 取得方法

c) 法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に関する情報であって，かつ，法令に基づき又は本人若しくは当該法人その他の団体自らによって公開又は公表された情報を提供する場合であって，**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とき。

d) 特定された利用目的の達成に必要な範囲内において，個人情報の取扱いの全部又は一部を委託すると

き。

e) 合併その他の事由による事業の承継に伴って個人情報が提供された場合であって，承継前の利用目的の範囲内で当該個人情報を取り扱うとき。

f) 個人情報を特定の者との間で共同して利用する場合であって，次に示す事項又はそれと同等以上の内容を，あらかじめ，本人に通知しているとき。

- 共同して利用すること
- 共同して利用される個人情報の項目
- 共同して利用する者の範囲
- 利用する者の利用目的
- 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
- 取得方法

g) **4.4.2.6** のただし書き **a)**～**d)** のいずれかに該当する場合

4.4.3 適正管理

4.4.3.1 正確性の確保

事業者は，利用目的の達成に必要な範囲内において，個人情報を，正確，かつ，最新の状態で管理しなければならない。

4.4.3.2 安全管理措置

事業者は，その取り扱う個人情報のリスクに応じて，漏えい，滅失又はき損の防止その他の個人情報の安全管理のために必要，かつ，適切な措置を講じなければならない。

4.4.3.3 従業者の監督

事業者は，その従業者に個人情報を取り扱わせるに当たっては，当該個人情報の安全管理が図られるよう，当該従業者に対し必要，かつ，適切な監督を行わなければならない。

4.4.3.4 委託先の監督

事業者は，個人情報の取扱いの全部又は一部を委託する場合は，十分な個人情報の保護水準を満たしている者を選定しなければならない。このため，事業者は，委託を受ける者を選定する基準を確立しなければなければならない。

事業者は，個人情報の取扱いの全部又は一部を委託する場合は，委託する個人情報の安全管理が図られるよう，委託を受けた者に対する必要，かつ，適切な監督を行わなければならない。

事業者は，次に示す事項を契約によって規定し，十分な個人情報の保護水準を担保しなければならない。

a) 委託者及び受託者の責任の明確化

b) 個人情報の安全管理に関する事項

c) 再委託に関する事項

d) 個人情報の取扱状況に関する委託者への報告の内容及び頻度

e) 契約内容が遵守されていることを委託者が確認できる事項

f) 契約内容が遵守されなかった場合の措置

g) 事件・事故が発生した場合の報告・連絡に関する事項

事業者は，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なければならない。

4.4.4 個人情報に関する本人の権利

4.4.4.1 個人情報に関する権利

事業者は，電子計算機を用いて検索することができるように体系的に構成した情報の集合物又は一定の規則に従って整理，分類し，目次，索引，符合などを付すことによって特定の個人情報を容易に検索できるように体系的に構成した情報の集合物を構成する個人情報であって，事業者が，本人から求められる開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止の求めのすべてに応じることができる権限を有するもの（以下，**4.4.4** において“開示対象個人情報”という。）に関して，本人から利用目的の通知，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止（以下，“開示など”という。）を求められた場合は，**4.4.4.4** ～ **4.4.4.7** の規定によって，遅滞なくこれに応じなければならない。

ただし，次のいずれかに該当する場合は，開示対象個人情報ではない。

a) 当該個人情報の存否が明らかになることによって，本人又は第三者の生命，身体又は財産に危害が及ぶおそれのあるもの

b) 当該個人情報の存否が明らかになることによって，違法又は不当な行為を助長し，又は誘発するおそれのあるもの

c) 当該個人情報の存否が明らかになることによって，国の安全が害されるおそれ，他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの

d) 当該個人情報の存否が明らかになることによって，犯罪の予防，鎮圧又は捜査その他の公共の安全と秩序維持に支障が及ぶおそれのあるもの

4.4.4.2 開示などの求めに応じる手続

事業者は，開示などの求めに応じる手続として次の事項を定めなければならない。

a) 開示などの求めの申し出先

b) 開示などの求めに際して提出すべき書面の様式その他の開示などの求めの方式

c) 開示などの求めをする者が，本人又は代理人であることの確認の方法

d) **4.4.4.4** 又は **4.4.4.5** による場合の手数料（定めた場合に限る。）の徴収方法

事業者は，本人からの開示など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。

事業者は，**4.4.4.4** 又は **4.4.4.5** によって本人からの求めに応じる場合に，手数料を徴収するときは，実費を勘案して合理的であると認められる範囲内において，その額を定めなければならない。

4.4.4.3 開示対象個人情報に関する周知など

事業者は，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，当該開示対象個人情報に関し，次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。）に置かなければならない。

a) 事業者の氏名又は名称

b) 管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先

c) すべての開示対象個人情報の利用目的[**4.4.2.5** の **a)**～**c)** までに該当する場合を除く。]

d) 開示対象個人情報の取扱いに関する苦情の申し出先

e) 当該事業者が個人情報の保護に関する法律（平成 15 年法律第 57 号）第 37 条第 1 項の認定を受けた者（以下，“認定個人情報保護団体”という。）の対象事業者である場合にあっては，当該認定個人情報保護団体の名称及び苦情の解決の申し出先

f) **4.4.4.2** によって定めた手続

4.4.4.4 開示対象個人情報の利用目的の通知

事業者は，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には，遅滞なくこれに応じなければならない。ただし，**4.4.2.5** のただし書き **a)**～**c)** のいずれかに該当する場合は利用目的の通知を必要としないが，そのときは，本人に遅滞なくその旨を通知するとともに，理由を説明しなければならない。

4.4.4.5 開示対象個人情報の開示

事業者は，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（当該本人が識別される開示対象個人情報が存在しないときにその旨を知らせることを含む。）を求められたときは，本人に対し，遅滞なく，当該開示対象個人情報を書面（開示の求めを行った者が同意した方法があるときは，当該方法）によって開示しなければならない。ただし，開示することによって次の **a)**～**c)** のいずれかに該当する場合は，その全部又は一部を開示する必要はないが，そのときは，本人に遅滞なくその旨を通知するとともに，理由を説明しなければならない。

a) 本人又は第三者の生命，身体，財産その他の権利利益を害するおそれがある場合

b) 当該事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

c) 法令に違反することとなる場合

4.4.4.6 開示対象個人情報の訂正，追加又は削除

事業者は，**4.4.4.5** による開示の結果，事実でないという理由によって当該開示対象個人情報の訂正，追加又は削除（以下，この項において“訂正など”という。）を求められた場合は，利用目的の達成に必要な範囲内において，遅滞なく必要な調査を行い，その結果に基づいて，当該開示対象個人情報の訂正などを行うとともに，訂正などを行った後に，本人に対し，遅滞なく，その旨（訂正などの内容を含む。）を通知しなければならない。

4.4.4.7 開示対象個人情報の利用又は提供の拒否権

事業者が，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の停止，消去又は第三者への提供の停止（以下，この項において“利用停止など”という。）を求められた場合は，これに応じなければならない。また，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。ただし，**4.4.4.5** のただし書き **a)**～**c)** のいずれかに該当する場合は，利用停止などを行う必要はないが，そのときは，本人に遅滞なくその旨を通知するとともに，理由を説明しなければならない。

4.4.5 教育

事業者は，従業者に，定期的に適切な教育を行わなければならない。事業者は，関連する各部門及び階層において，その従業者に，次の事項を理解させる手順を確立し，維持しなければならない。

a) 個人情報保護マネジメントシステムに適合することの重要性及び利点。

b) 個人情報保護マネジメントシステムに適合するための役割及び責任。

c) 個人情報保護マネジメントシステムに違反した際に予想される結果。

事業者は，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と権限を定める手順を確立し，実施し，維持しなければならない。

4.5 個人情報保護マネジメントシステム文書

4.5.1 文書の範囲

事業者は，次の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書面で記述しなければならない。

a) 個人情報保護方針

b) 内部規定

c) 計画書

d) この規格が要求する記録及び事業者が個人情報保護マネジメントシステムを実施する上で必要と判断した記録。

4.5.2 文書管理

事業者は，この規格が要求するすべての文書（記録を除く。）を管理する手順を確立し，実施し，維持しなければならない。

文書管理の手順には，次の事項が含まれなければならない。

a) 文書の発行及び改訂に関すること。

b) 文書の改訂の内容と版数との関連付けを明確にすること。

c) 必要な文書が必要なときに容易に参照できること。

4.5.3 記録の管理

事業者は，個人情報保護マネジメントシステム及びこの規格の要求事項への適合を実証するために必要な記録を作成し，維持しなければならない。

事業者は，記録の取扱いについての手順を確立し，実施し，維持しなければならない。

4.6 苦情及び相談

事業者は，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，迅速な対応をしなければならない。

事業者は，上記の目的を達成するために必要な体制の整備を行わなければならない。

4.7 点検

4.7.1 運用の確認

事業者は，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を事業者の各部門及び階層において定期的に確認しなければならない。

4.7.2 内部監査

事業者は，自ら定めた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しなければならない。

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なければならない。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。

事業者は，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と権限を定める手順を確立し，実施し，維持しなければならない。

4.8 是正処置及び予防処置

事業者は，不適合に対する是正処置及び予防処置を確実に実施するための責任と権限を定める手順を確立し，実施し，維持しなければならない。その手順には，次の事項を含めなければならない。

a) 不適合の内容を確認する。

b) 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。

c) 期限を定め，立案された適切な処置を実施する。

d) 実施された是正処置及び予防処置の結果を記録する。

e) 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。

4.9 事業者の代表者による見直し

事業者の代表者は，個人情報の適切な保護を維持するために，定期的に個人情報保護マネジメントシステムを見直さなければならない。

事業者の代表者による見直しにおいては，次の事項が考慮されなければならない。

a) 内部監査及び個人情報保護マネジメントシステムの運用状況に関する報告。

b) 苦情を含む外部からの意見。

c) 前回までの見直しの結果に対するフォローアップ。

d) 個人情報の取扱いに関する法令，国の定める指針及びその他の規範の改正状況。

e) 社会情勢の変化，一般の認識の変化，技術の進歩などの諸環境の変化。

f) 改善のための提案。