乙第32号証

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）

平成１１年４月２日

【 留意事項】

- 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）の掲載に当たっては、原案作成団体である財団法人日本規格協会の承認を得ています。
- 他に、転載することを禁じます。

【 お願い】

- 日本工業規格は工業標準化法第１５条の規定によって、少なくとも５年を経過するまでに改正等が行われることになっています。そのための参考とするため、この規格についてご意見・ご質問のある方は、下記までお願いいたします。

財団法人日本情報処理開発協会 （ プライバシーマーク事務局）	〒105-0011 東京都港区芝公園３-５-８　機械振興会館 電話：03-3432-9387　Fax：03-3432-9417 E-mail：info-privacy@jipdec.or.jp

【 規格の入手先】

- JIS Q 15001 は、製本されて下記にて頒布しています。入手を希望される方は、下記までお願いいたします。

財団法人日本規格協会 （ 普及業務課）	〒107-8440 東京都港区赤坂４-１-２４ 電話：03-3583-8002　Fax：03-3583-0462

日 本 工 業 規 格　　JIS

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

Q 15001：1999

Requirements for compliance program on personal information protection

0. **序文**　近年における情報処理技術の著しい発展は，電子計算機による大量，かつ，迅速な情報処理を可能とし，個人指向のクレジットローンなどの消費者信用取引，ダイレクトマーケティングなどにおいて，ニーズの多様化・個性化に対応した効率的な事業活動の展開を容易にしている。しかし一方で，こうした情報化の急速な進展に伴って，様々な事業者が情報システムを利用して個人情報を取り扱うことが可能となった結果，個人情報が分散した形で蓄積・利用される可能性が高まり，情報の不適切な利用，改ざんなどが行われるおそれが強まってきている。このため，個人情報の適切な利用と保護が極めて重要となってきており，国際的にも個人情報保護の強化に向けた取組が行われてきている。

個人情報を保護するためには，各事業者の自主的な取組が重要であり，こうした取組を進めるに当たって，体系的で全経営活動に統合されたマネジメントシステムであるコンプライアンス・プログラムを策定し，実施し，維持し，及び継続的に改善していくことが必要である。

この規格は，そのようなコンプライアンス・プログラムの最小限の要求事項を規定している。事業者は，個人情報の適切な保護の目的の範囲内において，個人情報の特性及びその活動の実態に応じて定められた特別な規範を適用することができる。

事業者は，この規格との適合性を，自己による評価，顧客による評価及び第三者機関による評価によって利害関係者に示すことができ，利害関係者の理解を得ることに使用できる。

この規格は，自由，かつ，公正な競争を阻害したり，事業者の法的な義務を増大又は変更するために用いられることを意図したものではない。

コンプライアンス・プログラムの基本モデルを，**図 1** に示す。このコンプライアンス・プログラムの成功は，すべての階層及び部門の関与，特に事業者の代表者の関与のいかんにかかっている。

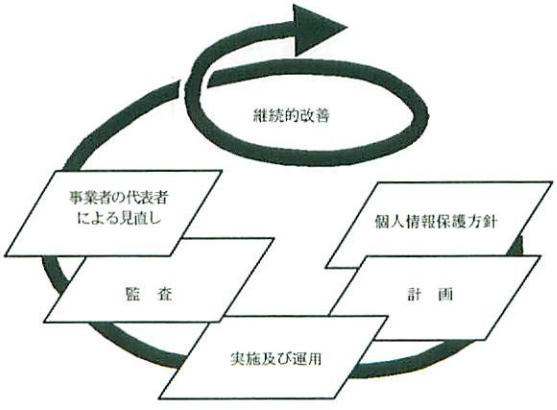


図 1　コンプライアンス・プログラムの基本モデル

この規格は，品質システム規格のJIS Z 9900シリーズ及び環境マネジメントシステムのJIS Q 14001と共通のマネジメントシステム原則を採用している。

このマネジメントシステム原則の趣旨は，方針を作成し，それに基づき計画し，実施し，監査し，及び見直しをスパイラル的に継続することによって，事業者の管理能力を高めていくことにある。

したがって，この規格によって，事業者の個人情報を管理する能力を高めていくことが期待できる。

事業者は，コンプライアンス・プログラムの基礎として，JIS Z 9900シリーズやJIS Q 14001に合致した既存のマネジメントシステムを使用してもよい。

この規格に規定するコンプライアンス・プログラムの要求事項は，既存のマネジメントシステム要素と独立に設定される必要はない。場合によっては，既存のマネジメントシステム要素を当てはめることによって，要求事項を満たすことも可能である。

1. **適用範囲** この規格は，個人情報の全部若しくは一部を電子計算機などの自動処理システムによって処理している，又は自動処理システムによる処理を行うことを目的として書面などによって処理している，あらゆる種類，規模の事業者に適用できる。

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) コンプライアンス・プログラムを策定し，実施し，維持し，及び改善する。

b) この規格とコンプライアンス・プログラ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) 外部組織又は情報主体に，この規格とコンプライアンス・プログラ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. **定義** この規格で用いる主な用語の定義は，次による。

a) **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，又は個人別に付けられた番号，記号その他の符号，画像若しくは音声によって当該個人を識別できるもの(当該情報だけでは識別できないが，他の情報と容易に照合することができ，それによって当該個人を識別できるものを含む。)。

b) **情報主体** 一定の情報によって識別される，又は識別され得る個人。

c) **事業者** 事業を営む法人，その他の団体又は個人。

d) **管理者** 事業者の内部において代表者によって指名された者であって，コンプライアンス・プログラムの実施及び運用に関する責任と権限をもつ者。

e) **受領者** 個人情報の提供を受ける法人，その他の団体又は個人。

f) **監査責任者** 事業者の代表者によって指名された者であって，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権限をもつ者。

g) **情報主体の同意** 情報主体が，収集，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収集，利用又は提供について承諾する意思表示。情報主体が子供の場合は，保護者の同意も得るべきである。

h) **コンプライアンス・プログラム**(CP) 事業者が，自ら保有する個人情報を保護するための方針，組織，計画，実施，監査及び見直しを含むマネジメントシステム。

i) **収集目的** 個人情報の利用及び提供の範囲を定め，情報主体の同意の対象となるもの。

j) **利用** 事業者が当該事業者内で個人情報を処理すること。

k) **提供** 事業者が，当該事業者外のものに自ら保有する個人情報を利用可能にすること。

l) **預託** 事業者が，当該事業者外のものに情報処理を委託するなどのために自ら保有する個人情報を預けること。

4. コンプライアンス・プログラム要求事項

4.1 **一般要求事項** 事業者は，コンプライアンス・プログラムを策定し，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，この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，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くてはならない。事業者の代表者は，この方針を文書化し，役員及び従業員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くてはならない。

a) 事業の内容及び規模を考慮した適切な個人情報の収集，利用及び提供に関すること。

b) 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予防並びに是正に関すること。

c) 個人情報に関する法令及びその他の規範を遵守すること。

d) コンプライアンス・プログラムの継続的改善に関すること。

4.3 計画

4.3.1 **個人情報の特定** 事業者は，自ら保有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。事業者は，特定した個人情報に関するリスク(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)を認識しなければならない。

4.3.2 **法令及びその他の規範** 事業者は，個人情報に関する法令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 **内部規程** 事業者は，個人情報を保護するための内部規程を策定し，維持しなければならない。

内部規程は，次の事項を含まなければならない。

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) 個人情報の収集，利用，提供及び管理の規定。

c) 情報主体からの個人情報に関する開示，訂正及び削除の規定。

d) 個人情報保護に関する教育の規定。

e) 個人情報保護に関する監査の規定。

f) 内部規程の違反に関する罰則の規定。

事業者は，事業の内容に応じて，コンプライアンス・プログラ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。

4.3.4 **計画書** 事業者は，内部規程を遵守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。

4.4 実施及び運用

4.4.1 **体制及び責任** コンプライアンス・プログラ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，個人情報に関連のある業務にかかわる役員及び従業員に周知しなければならない。

事業者の代表者は，コンプライアンス・プログラムの実施及び管理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，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，コンプライアンス・プログラ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。

4.4.2 個人情報の収集に関する措置

4.4.2.1 **収集の原則** 個人情報の収集は，収集目的を明確に定め，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 **収集方法の制限** 個人情報の収集は，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収集の禁止** 次に示す内容を含む個人情報の収集，利用又は提供は行ってはなら

ない。ただし，これらの収集，利用又は提供について，明示的な情報主体の同意，法令に特別の規定がある場合，及び司法手続上必要不可欠である場合は，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(所在都道府県に関する情報を除く。)，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 情報主体から直接収集する場合の措置 情報主体から直接に個人情報を収集する場合には，情報主体に対して，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書面若しくはこれに代わる方法によって通知し，情報主体の同意を得なければならない。

a) 事業者の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名，及び所属並びに連絡先。

b) 収集目的。

c) 個人情報の提供を行うことが予定される場合には，その目的，当該情報の受領者又は受領者の組織の種類，属性及び個人情報の取扱いに関する契約の有無。

d) 個人情報の預託を行うことが予定される場合には，その旨。

e) 情報主体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情報主体に生じる結果。

f) 個人情報の開示を求める権利，及び開示の結果，当該情報が誤っている場合に訂正又は削除を要求する権利の存在，並びに当該権利を行使するための具体的な方法。

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 情報主体以外から間接的に個人情報を収集する場合には，情報主体に対して，少なくとも，4.4.2.4 の a)～d)及び f)に示す事項を書面又はこれに代わる方法によって通知し，情報主体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，この限りでない。

a) 情報主体からの個人情報の収集時に，あらかじめ自己への情報の提供を予定している旨 4.4.2.4 の c)に従い情報主体の同意を得ている提供者から収集を行う場合。

b) 情報処理を委託するなどのために個人情報を預託される場合。

c) 情報主体の保護に値する利益が侵害されるおそれのない収集を行う場合。

4.4.3 個人情報の利用及び提供に関する措置

4.4.3.1 利用及び提供の原則 個人情報の利用及び提供は，情報主体が同意を与えた収集目的の範囲内で行わなければならない。

なお，次に示すいずれかに該当する場合は，情報主体の同意を必要としない。

a) 法令の規定による場合。

b) 情報主体及び・又は公衆の生命，健康，財産などの重大な利益を保護するために必要な場合。

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 情報主体が同意を与えた収集目的の範囲外で個人情報の利用及び提供を行う場合は，少なくとも，4.4.2.4 の a)～d)及び f)に示す事項を書面又はこれに代わる方法によって情報主体に通知し，事前の情報主体の同意の下に行わなければならない。

4.4.4 個人情報の適正管理義務

4.4.4.1 個人情報の正確性の確保 個人情報は，収集目的に応じ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。

4.4.4.2 個人情報の利用の安全性の確保 個人情報に関するリスク(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)に対して，合理的な安全対策を講じなければならない。

4.4.4.3 個人情報の委託処理に関する措置 事業者が，情報処理を委託するなどのために個人情報を預託する場合は，十分な個人情報の保護水準を満たしている者を選定する基準を確立しなければならない。また，契約によって，次に示す内容を規定し，その保護水準を担保しなければならない。

a) 個人情報に関する秘密保持。

b) 再委託に関する事項について。

c) 事故時の責任分担。

d) 契約終了時の個人情報の返却及び消去。

当該契約書などの書面又はこれに代わる記録を，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。

4.4.5 個人情報に関する情報主体の権利

4.4.5.1 個人情報に関する権利 情報主体から自己の情報について開示を求められた場合は，合理的な期間内にこれに応じなければならない。また，開示の結果，誤った情報があり，訂正又は削除を求められた場合は，合理的な期間内にこれに応じるとともに，訂正又は削除を行った場合は，可能な範囲内で当該個人情報の受領者に対して通知を行わなければならない。

4.4.5.2 個人情報の利用又は提供の拒否権 事業者が保有している個人情報について，情報主体から自己の情報についての利用又は第三者への提供を拒まれた場合は，これに応じなければならない。

4.4.6 教育 事業者は，役員及び従業員に，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員に，次の事項を自覚させる手順を確立し維持しなければならない。

a) コンプライアンス・プログラムに適合することの重要性及び利点。

b) コンプライアンス・プログラムに適合するための役割及び責任。

c) コンプライアンス・プログラムに違反した際に予想される結果。

4.4.7 苦情及び相談 事業者は，個人情報及びコンプライアンス・プログラムに関して，情報主体からの苦情及び相談を受け付けて対応しなければならない。

4.4.8 コンプライアンス・プログラム文書 事業者は，書面又はこれに代わる方法で，コンプライアンス・プログラムの基本となる要素を記述しなければならない。

4.4.9 文書管理 事業者は，この規格が要求するすべての文書を管理しなければならない。

4.5 監査 事業者は，コンプライアンス・プログラムがこの規格の要求事項と合致していること，及びその運用状況を定期的に監査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。

事業者は，監査報告書を管理し，保管しなければならない。

4.6 事業者の代表者による見直し 事業者の代表者は，監査報告書及びその他の経営環境などに照らして，適切な個人情報の保護を維持するために，定期的にコンプライアンス・プログラムを見直さなければならない。

JIS Q 15001：1999

個人情報保護に関する コンプライアンス・プログラムの要求事項 解説

この解説は，本体に規定した事柄，及びこれに関連した事柄を説明するもので，規格の一部ではない。

I. **制定の趣旨** 昨今の情報処理技術の進歩は目をみはるものがあり，特にダウンサイジング，エンド・ユーザー・コンピューティングなどによって，従来の大型コンピュータを用いた大量・定型業務の処理に伴うものだけでなく，中小を含めた様々な事業者などが情報システムを利用して個人情報を取り扱うことが可能となった結果，個人情報が分散した形で蓄積・利用される可能性が高まり，正当な権限のないものによる情報の不当な利用，改ざん，加工などが行われるおそれも強まってきている。実際に，個人情報の漏えい事件は散見されてきており，個人情報保護に対する不安感の高まりから，消費者団体からも個人情報保護の強化が求められているところである。

また，最近のインターネットの爆発的な拡大に代表されるオープンなコンピュータ・ネットワークの世界的な発展などによって，いったんネットワーク上に乗せられた個人情報は，一瞬のうちに国境をも越えて広範囲に流通することが可能となっていることから，より大規模な個人情報の侵害事例の発生のおそれが強まるとともに，個人情報保護の国際的な調和が必要となってきている。

さらに，海外先進諸国においては，従来から，個人情報保護法が制定され，1980 年(昭和 55 年)に経済協力開発機構(OECD)が採択した“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”をもとに，その後も個人情報保護法が制定されている。さらに，近年の情報技術の進展に伴い，各国において個人情報保護の強化へ向けた取組が開始されている。

特に，EU においては，1995 年(平成 7 年)10 月に“個人データ処理に係る個人情報の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令”が採択され，域内各国は当該指令に適合するよう 3 年以内に法制化を含めた検討を行うよう求められている。当該指令によれば，個人情報の第三国への移転について，第三国が十分なレベルの保護措置を講じていない場合にはその移転が禁止されるほか，第三国が十分なレベルの保護措置を講じていないと EU 委員会が認定した場合には，第三国と交渉できることとなっており，我が国においても“個人情報の十分なレベルの保護”を確保することが求められているところである。

以上に述べたような状況の変化を踏まえ，通商産業省においては，平成元年に制定した“民間部門における電子計算機処理に係る個人情報の保護について(指針)”を改定し，“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)として告示した。

今回の個人情報保護に関する規格の制定は，この通商産業省のガイドラインを基礎として，関係事業者はもとより社会一般によって広く周知し問題意識を向上させることで，この規格を利用する事業者を社会的に認知し，高度情報化社会の健全な発展と適切な消費者保護を目的としたものである。

II. **規格の概要**

1. **適用範囲**(本体の 1.) 個人の住所録など個人が自己のために個人情報を取り扱っている場合はこの規格の対象とはしない。しかし，個人であっても，外見的に特定企業の従業員として個人情報を取り扱っていると判断される場合は，対象とすべきである。

自動処理システムによる処理には，一般的に入力，処理，出力が包含されている。

2. **定義**(本体の 3.)

2.1 **個人情報**[本体の 3. a)] “個人情報”には，法人その他の団体に関して記録された情報に含まれる当該法人その他の団体の役員に関する情報を含まない。“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。

2.2 **情報主体**[本体の 3. b)] “情報主体”とは，当該個人情報の本人をいう。

2.3 **受領者**[本体の 3. e)] “受領者”とは，情報を提供する者と対比して，直接又は間接的に個人情報の提供を受ける者を指す。

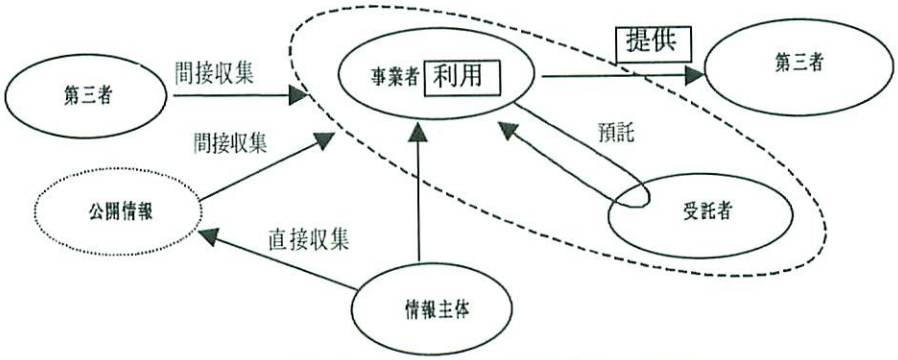
2.4 **情報主体の同意**[本体の 3. g)] 情報主体の署名押印，口頭による回答などの明示的方法による意思表示が原則である。ただし，例えば，次の場合においては，当該行為の手続において反対の意思を表明しないなどの黙示的方法による意思表示を含めることができるものと考える。

— 情報主体が既に必要な事項の通知を受けていることが明白である場合。
— 契約履行のために，金融機関の口座番号を記入した際にあって，与信機関に照合する場合。
— 情報主体によって不特定のものに公開された情報を収集する場合。
— 電気・ガスの供給契約など，書面の交付による契約手続を伴わない取引，申込み，加入などの行為の場合において，ポスター，ちらしなどによって必要な事項を告知する場合。

保護者の同意も得るべきであるとする子供とは，本体の 4.4.2.4 の a)～f)の内容を理解できない年齢の子供のことである。一般に，12 歳から 15 歳までの年齢以下が対象となると考えられる。また，同様に本体の 4.4.2.4 の a)～f)の内容について，判断力に懸念があると考えられる成人についても配慮すべきである。

2.5 **コンプライアンス プログラム**(CP) [本体の 3. h)] 法人である事業者が，複数の事業を営んでいる場合は，個人情報を取り扱う事業部門を明確に確定でき，かつ，個人情報の取扱いについて当該事業ごとの特性があるときは，当該法人の一事業部門だけ，又は事業部門ごとに CP を策定することもできる。ただし，当該法人内部の責任関係を明確化するとともに，CP に違反した場合の最終的な経営責任が当該法人の代表者にあることを明示する必要がある。

2.6 **利用及び提供**[本体の 3. j)及び k)] “利用”及び“提供”の関係を**解説図 1** に示す。



解説図 1 “利用”及び“提供”の関係

委託者が個人情報を預託する場合には，委託者は本体の 4.4.4.3 が，受託者は本体の 4.4.2.5 b)が適用される。

3. **コンプライアンス プログラム要求事項**(本体の 4.)

3.1 **個人情報保護方針**(本体の 4.2) 方針の文書化には，サーバーなどの電子的な方法も含む。“従業員”には正社員だけでなく，派遣社員，非常勤職員を含む(なお，本体の 4.4.1 及び 4.4.6 で用いている“従業員”についても同じ。)。

3.2 **個人情報の特定**(本体の 4.3.1) 個人情報を保護するためには，対象となる個人情報を具体的に把握するための手順を確立し，維持するとともに，適正な保護措置を講じない場合のリスクと影響を認識しなければならない。影響

には，事業者に直接的に与える影響のほか，社会的信用の喪失など間接的な影響もあることを認識する必要がある。

3.3 法令及びその他の規範(本体の 4.3.2) 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律，各地方自治体が制定している個人情報保護条例，その他の法令，行政機関が制定している個人情報保護ガイドライン，各業界が定めたガイドラインなどがある。

3.4 内部規程(本体の 4.3.3) 内部規程には，個人情報を保護するための組織規程を含む。事業者の各部門及び階層における権限と責任の明確化を図ることが重要である。

また，内部規程の整備は，基本となる規程を形式的に定めるだけではなく，それを受けて細則，マニュアル，チェックリストなどを作成し，どのような行為をなすべきか，又はなすべきではないか，従業員が具体的に規範に直面するよう構成する必要がある。内部規程は，必ずしも形式的に一本化された規程でなくともよい。内部規程の違反に関する罰則は，就業規則を準用するとよい。

さらに，内部規程は，取締役会の決議を経るなど従業員を正当に拘束するに足りる一定の手続を経て定める必要がある。

3.5 計画書(本体の 4.3.4) 教育計画書は，個人情報保護研修の年間カリキュラム，個別の研修プログラム(研修の名称，開催日時，場所，講師，受講対象者及び予定参加者数，研修の概要，使用テキスト，任意参加か否かの別など)及び予算などによって構成する。

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

3.6 体制及び責任(本体の 4.4.1) 管理者は，当該事業者に係る個人情報の管理の責任者である性格上，いたずらに指名する者を増やし，責任が不明確になることは避けなければならない。したがって，事業部が複数あり管理者を複数名指名する場合には，当該者間での役割分担を明確にすることが求められる。

管理者は，社外に責任のもつことができる者(例えば，役員クラス)を指名することが望ましい。

3.7 個人情報の収集に関する措置本体の 4.4.2)

3.7.1 収集の原則(本体の 4.4.2.1) 収集目的は，当然公序良俗に反しない範囲であることが求められる。

収集目的の明確化に当たっては，次のことに配慮する必要がある。

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

b) 本人以外の者から収集する場合も，収集する者が収集目的を設定し，収集の相手方との契約などにおいて明示すること。

c) 公開された資料などから収集する場合も，収集する者が収集目的を設定すること。

d) 収集目的を設定するに当たっては，収集した情報の利用及び提供によって情報主体の受ける影響を予測できるように，利用及び提供の範囲を可能な限り具体的に明らかにすること。

3.7.2 収集方法の制限(本体の 4.4.2.2) 個人情報の収集は，収集目的を偽るなど不公正な手段によって収集することは許されない。

3.8 情報主体から直接収集する場合の措置(本体の 4.4.2.4) “個人情報の提供を行うことが予定される場合”については，個人情報の提供は，情報主体が直接関与することがないことが多いため，提供の目的，当該情報の受領者などに関する情報を，情報主体に懸念を抱かせないよう具体的に明らかにすることが必要である。

“組織の種類，属性”とは，個人情報の受領者たる組織(企業)の業種と提供元である企業との関係(関連会社，持株会社など)を指す。

“情報主体が個人情報を与えることの任意性”とは，申込書など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し，“当該情報を与えなかった場合に情報主体に生じる結果”とは，記載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載しなければ，年収を考慮した相手を紹介しないことなど)を指す。

テレビショッピングの告知や雑誌の広告による通信販売のように，取引の時間又はスペースの関係などで申込みを受ける時点までに本体の 4.4.2.4 に示す事項を示すことが困難な場合には，カタログや商品の発送など，次に消費者などと連絡を取る際に，本体の 4.4.2.4 に示す事項を改めて通知し，同意を得るべきである。

“書面に代わる方法”とは，例えば，電子メールなどを送受信する方法である。

3.9　情報主体以外から間接的に収集する場合の措置本体の 4.4.2.5)　4.4.2.5 b)について情報処理の委託を受けた者は，個人情報の処理に際し，委託の本旨に反して利用及び提供をすることは当然に許されないことであり，また，この規格に従い，個人情報を適正に管理することが望ましい。

本体の 4.4.2.5 c)の“情報主体の保護に値する利益が侵害されるおそれのない収集を行う場合”とは，例えば，ガスの保安サービスを行う者が，顧客の安全を確保するために個人情報を収集するなどである。

本体の 4.4.2.5 c)の場合に該当するかどうかの判断についても，当事者のし意的判断ではなく，条理又は社会通念による客観的判断のもとで，極力限定的に解釈する必要がある。

3.10　収集目的の範囲外の利用及び提供の場合の措置(本体の 4.4.3.2)　企業内のある部門が，情報主体の同意を得て収集した個人情報を他の部門が利用する場合には，情報主体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，例え同一企業内であっても，改めて事前の情報主体の同意を得ることが必要である。

3.11　個人情報の適正管理義務(本体の 4.4.4)

3.11.1　個人情報の利用の安全性の確保(本体の 4.4.4.2)　“合理的”という意味は，経済的に実行可能な最良の技術の適用に配慮することである。

技術面での安全対策として，“情報システム安全対策基準(平成 7 年 8 月 29 日通商産業省告示第 518 号)”，“コンピュータ不正アクセス対策基準(平成 8 年 8 月 8 日通商産業省告示第 362 号)”などを参考にした対策，組織面での安全対策として，個人情報保護に関する社内基準や責任体制の確立などが必要とされる。

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

3.12　個人情報の委託処理に関する措置本体の 4.4.4.3)　委託者は，預託に際し，情報主体の同意を得た範囲内で委託契約を締結することが必要である。

3.13　個人情報に関する情報主体の権利本体の 4.4.5)

3.13.1　個人情報に関する権利(本体の 4.4.5.1)　個人に関する特定の評価などの情報については，社会通念や慣行に照らし合わせて開示が適当と判断される場合もあると考えられる。

“合理的な期間”とは，企業内での個人情報の更新期間程度を指す。

3.13.2　個人情報の利用又は提供の拒否権(本体の 4.4.5.2)　第三者への提供を拒まれた場合などは，情報主体に不利益を与えないようにこれに応じなければならない。

本体の 4.4.3.1 のただし書き a)，b)のいずれかに該当する場合は，この限りではない。

3.14　苦情及び相談(本体の 4.4.7)　苦情及び相談の受付は，常設の対応窓口の設置又は担当者の任命によって行う必要がある。ただし，管理者との兼任を妨げない。

また，窓口又は担当者の連絡先は，情報主体に対して告知する必要がある。

3.15　文書管理(本体の 4.4.9)　文書管理とは，CP 文書及び下位文書を保存するだけでなく，常に最新の状態で維持しておくことである。

3.16　監査(本体の 4.5)　監査は，コンプライアンス・プログラムの整備状況，体制整備状況，及び運用状況について行う。

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

4. **原案作成委員会の構成表** 1998年に設置された原案作成委員会の構成表を，次に示す。

個人情報保護規格審議委員会 構成表

	氏名	所属
(委員長)	堀部政男	中央大学法学部
(副委員長)	松本恒雄	一橋大学法学部
(委員)	浅川敏郎	工業技術院標準部管理システム規格課
	安達正雄	トヨタ自動車株式会社国内業務部
	有明武美	東京ガス株式会社人事部
	五十嵐得郎	東日本旅客鉄道株式会社総合企画本部経営管理部
	伊藤仁	東京海上火災保険株式会社情報システム部
	上田宗央	株式会社パソナ
	氏兼裕之	通商産業省機械情報産業局情報処理システム開発課
	内布光	株式会社日立情報システムズ社長室法務統括センタ
	馬屋原久史	株式会社セブン・イレブン・ジャパン商品本部雑貨部
	岡田謙二	株式会社野村総合研究所法務部
	奥本晋也	株式会社東急ストアシステム開発部
	蟹江利彦	株式会社日立製作所情報システム管理本部
	鎌木伸一	株式会社日本交通公社総務部法務室
	嘉屋園江	大日本印刷株式会社知的財産権本部第二部
	河北博文	河北総合病院
	久賀淳一	日本航空株式会社法務部
	佐藤良治	日立クレジット株式会社社長室
	白石昭	株式会社三菱総合研究所情報事業センター
	新谷修次	株式会社ムトウ通販事業部販売企画部
	鈴木康史	富士通株式会社法務・知的財産権本部法務部ビジネス支援部
	鈴木隆一	保健医療福祉情報システム工業会
	関志郎	社団法人全国学習塾協会
	関本貢	財団法人日本情報処理開発協会情報セキュリティ対策室
	田中龍郎	株式会社オーエムエムジー
	照井恵光	工業技術院標準部標準認証課
	広畑寿一郎	株式会社西武百貨店営業企画部クラブオン課
	増井克吉	社団法人日本消費者生活アドバイザー・コンサルタント協会
	松尾廣志	電気事業連合会情報通信部
	丸橋透	ニフティ株式会社管理部
	山縣昭一	株式会社セントラルファイナンス経営企画部(東京)
	山本泉二	ソニー株式会社デジタルネットワークソリューションカンパニー
	若松修	日本コンパクトディスク・ビデオレンタル商業組合
(関係者)	高橋俊一	通商産業省機械情報産業局情報処理システム開発課
	山並憲司	通商産業省機械情報産業局情報処理システム開発課
	天野正喜	工業技術院標準部
	桑山広司	工業技術院標準部

	佐　草　幸　一	電子商取引実証推進協議会
	鈴　木　正　朝	社団法人情報サービス産業協会
(事務局)	吉　村　秀　勇	財団法人日本規格協会技術部
	井ノ口　和　好	財団法人日本規格協会技術部
	末　安　いづみ	財団法人日本規格協会技術部