互助会契約及び施行に係る
個人情報保護ガイドライン

＜　解　説　書　＞

平成 11 年 5 月　　制定
平成 16 年 10 月　　改定
平成 18 年 9 月 21 日　　改定
平成25年 7月 17日　　改定

一般社団法人全日本冠婚葬祭互助協会

はじめに

1．　近年、パソコンの普及により一般家庭においてもインターネットを利用する人が急増しております。

インターネットは個人が様々な情報を瞬時に見られる一方で、個人のプライバシーまでもが本人の知らないうちに漏洩し、トラブルに巻き込まれたり、犯罪に悪用されるケースも増加しております。

また個人だけでなく、企業のコンピュータが不正侵入され個人情報を盗み出されたり、データを改ざんされたりする事件なども起こっています。

2．　世界的に見ると、欧米先進国では早くから個人情報を保護する対策に取り組んでおり、OECD では 1980 年(昭和 55 年)に、個人情報の収集・データ内容・目的明確化・利用制限・安全保護・公開・個人参加・責任の原則を規定した「8原則」を策定しており、EU・米国ではそれぞれ 1970 年代に立法措置が講じられています。

3．　日本においても 1988 年(昭和 63 年)に「行政機関の保有する電子計算機処理に係る個人情報保護に関する法律」が施行され、また民間分野の自主的な取り組みとして、平成 10 年 4 月から財団法人日本情報処理開発協会（JIPDEC）において個人情報を保護する体制が整備されている企業であることを第三者機関が評価し、認定するプライバシーマーク制度が開始されています。

また、平成 11 年 3 月に、JIS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（CP）の要求事項（JISQ 15001）（以下、JIS要求事項）が制定されています。

さらに、平成 17 年 4 月 1 日から、「個人情報の保護に関する法律（平成 15 年法律第 57 号）（以下、「法」という。）が全面施行されることになり、これに対応して、経済産業省は「法」の[個人情報取扱事業者の義務等]を中心に、平成 16 年 10 月に

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を作成しております。

4.　このような状況下で、互助会業界につきましては、「法」に定められた「個人情報保護の対象となる事業者」に該当すると考えられますので、正会員及び準会員代表者各位におかれては、全面施行された「法」の［個人情報取扱事業者の義務等］について、対策等を講じなければなりません。

総務委員会では、「互助会契約及び施行に係わる個人情報保護ガイドライン」＜解説書＞（平成 11 年 5 月発行）を経済産業省のガイドライン（平成 16 年 10 月）及びJIS要求事項を踏まえながら「法」に適合する内容に見直す作業を進め、個人情報を取り扱う互助会事業者が、いかなる対策を講じるか、社内における個人情報保護の実践遵守計画（コンプライアンス・プログラム）を策定する際における指針となるガイドライン（改訂版）＜解説書＞を平成17年2月に作成しました。その後、個人情報保護法で導入された概念の導入・明確化などのために、JIS 要求事項が平成 18 年 5 月 20 日に大幅に改正されたことから、本ガイドライン＜解説書＞（新訂版）を作成しました。

5.　個人情報の利用と保護は、「法」を遵守するための各事業者の積極的な取り組みが重要となります。各事業者におかれては、知り得た冠婚、葬祭に係る互助会加入者等の個人情報について、適切な取扱いをすることはもとより、漏洩、紛失、破壊、及び改ざん等を絶対起こさないようにし、業界全体の信頼の一層の向上を図るため、本ガイドライン＜解説書＞（新訂版）にしたがって個人情報保護マネジメントシステムを策定し、個人情報の適正な取扱いや安全管理などの体制整備を図るとともに、当協会が付与認定指定機関となりましたプライバシーマークを取得されるようにお願い致します。

互助会契約及び施行に係る個人情報保護ガイドライン

目　　次

第1章　ガイドラインの目的

（目　的）

第1条　このガイドラインは、一般社団法人全日本冠婚葬祭互助協会（以下「当協会」という。）加盟会員（以下「協会員」という。）が取り扱う個人情報の適正な保護の指針となる項目を定め、「協会員」がその活動の実態に応じた個人情報保護マネジメントシステムを策定することを支援し、及び促進することを目的とします。

【解説】

1．　本条は、「当協会員」が取り扱う個人情報保護マネジメントシステム策定の支援及び促進を目的とします。

2．　個人情報保護マネジメントシステムとは、「協会員」が保有し、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、点検、及び見直しを含むマネジメントシステムをいいます。

3．　一つの「当協会員」において、複数の業種の事業を行なうことがある場合には、関連している全ての業界ガイドラインを参照し、その趣旨を十分に踏まえながら、その「当協会員」にふさわしい個人情報保護対策を規定した個人情報保護マネジメントシステムを策定することになります。

4．　個人情報保護マネジメントシステムは、それ自体公表を前提としたものではありませんが、「当協会員」は、消費者に対して個人情報保護のために講じている対策について説明できるようにしておくことが望ましいです。

5．　「当協会員」とは、当協会の正会員及び準会員をいいます。

第2章　定　義

（定義）

第2条　このガイドラインにおいて、次の各号に掲げる用語の定義は、当該各号に定めるところとなります。

(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又は個人別に付された番号、記号その他の符号、画像若しくは音声により、特定の個人を識別できるもの（当該情報のみ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、それにより特定の個人を識別することができるものも含む。）をいいます。

(2)　互助会契約　消費者に対して「当協会員」が予め定めた冠婚葬祭に係るサービス（役務）の提供及びそれに関連する物品の給付のために交わした契約をいいます。

(3)　施行　「当協会員」があらかじめ互助会契約を交わした消費者又はその他の消費者に対し、冠婚葬祭に係るサービス（役務）の提供及びそれに関連する物品の給付を行うことをいいます。

(4)　本人　個人情報によって識別される特定の個人をいいます。

(5)　個人情報保護管理者　「当協会員」の内部において代表者により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持つ者をいいます。

(6)　個人情報保護監査責任者　「当協会員」の内部において代表者により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なう責任及び権限を持つ者をいいます。

(7)　受領者　個人情報の提供を受ける法人、その他団体又は個人をいいます。

(8)　従業者　役員及び従業員をいい、役員、正社員に限らず、契約社員、嘱託社員・パート・アルバイト、派遣社員等も含みます。

(9)　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をいいます。本人が子ども又は無能力者などの場合は、保護者、法定代理人などの同意も得なければなりません。

(10)　利用　「当協会員」が当該「当協会員」内で個人情報を処理することをいいます。

(11)　提供　「当協会員」が当該「当協会員」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をいいます。

(12)　委託　「当協会員」が、当該「当協会員」外のものに施行、会員募集、情報処理などのために、委託契約などにより、自ら保有する個人情報を利用可能にすることをいいます。

(13)　個人情報保護マネジメントシステム　「当協会員」が保有する自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステムをいいます。

(14)　不適合　本ガイドラインの要求を満たしていないこと。

【解説】

1.　上記(1)「個人情報」については、平成11年3月に制定されて、平成18年5月に改定された「個人情報保護マネジメントシステム要求事項」(JIS　Q　15001:2006)」における「個人情報」の定義を参考にしています。

又、「個人別に付された番号」とは、電話番号、銀行口座番号、保険証番号等や互助会加入者番号、世帯管理番号、受注番号等を指します。

2.　上記(5)「個人情報保護管理者」については、「当協会員」におい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持つ責任者として明確に規定し、責任の所在を明確にしておかなければなりません。上記(6)「個人情報監査責任者」についても、監査の実施及び報告を行なう責任及び権限を持つ責任者として明確に規定し、責任の所在を明確にしておくことがおかなければなりません。

3.　上記(7)「受領者」とは、情報を提供する者と対比して、個人情報の提供を受ける者を指しま

す。

4. 上記(8)「従業者」とは、「当協会員」の組織内で直接間接に「当協会員」の指導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、受入派遣社員等を含みます。

5. 上記(9)「取得、利用又は提供に関する情報」とは、本人から直接書面での取得、利用、本人へのアクセス又は提供において本ガイドラインで要求されている書面などによる明示又は通知をすべき事項です。同意は、本人の署名押印などの明示的な方法（ウェブサイト上での同意ボタンのクリックなども含む。）によって本人の意思が表示されていることが原則です。与えられた書面に本人が黙って記入したからといって、明示的な同意があったものとみなすことはできません。また、通知後一定期間内に本人の応答が無い場合に同意があったものとみなすことも不適切です。

JIS Q 15001:2006 2.

第3章　ガイドラインの適用範囲

（対象となる個人情報）

第3条　このガイドラインは、「当協会員」が扱う互助会契約及び施行とそれに関連する事業並びに「当協会員」内の人事などに係る個人情報を対象とし、電子計算機処理を行なうことを目的として書面等により処理されている個人情報及び手作業により直接処理されている個人情報の全てにこれを適用します。但し、従業者などの個人が「協会員」の業務と関係ない個人情報を、自己のために取得する場合については、この限りではありません。

【解説】

1. コンピュータ等による自動処理システムを用いて個人情報が処理される場合には、情報処理の迅速性、大量性等のため個人の利益が侵害される危険がマニュアル処理（手作業による処理）に比べ著しく大きいという観点から、取扱いには特に、十分な配慮が必要となります。

2. しかし、マニュアル処理による個人情報であっても、個人の利益の侵害が大きいことが懸念されるため、「加入者管理台帳」をはじめ、顧客管理等の目的で取得、保有されている「互助会加入申込書」「施行時の見積書」「施行時の発注伝票」等の情報や「ダイレクトメール用シール」「振替済通知書」「満期完納通知書」等、事業の用に供している全ての個人情報を本ガイドラインの対象に含めるものとします。

3. 個人の住所録等個人が業務に関係なく自己のために収集する個人情報についてはこの対象外とします。しかし、個人用であっても、外見的に「当協会員」の従業者として個人情報を取り扱っていると判断される場合（例えば、個人の住所録が、場合によっては、DM発送や営業活動に活用されること。）には、対象となりますので十分に注意してください。

4. また、本ガイドラインは、個人情報に関する取扱いについて定めるものですので、「当協会

員」がその従業者の人事管理、福利厚生、あるいは採用等のために保有する個人情報（いわゆる「インハウス情報」）についても、本ガイドラインの適用の対象とします。

5．本ガイドラインの人的適用範囲は役員、正社員、派遣社員、契約社員、パートタイマーも含めた「協会員」の全従業者になります。

JIS Q 15001:2006 1.

（ガイドラインの拡張）

第4条　「当協会員」は、本ガイドラインに基づき個人情報の適切な保護の目的の範囲内において、各々の活動の実態に応じた項目を追加又は修正し、「当協会員」各々の個人情報マネジメントシステムを策定することができます。

【解説】

1．　本ガイドラインは、個人情報の適切な保護のために、業界として必要な一般的な事項を定めたものでありますので、個人情報保護の実効性を高めるため、本ガイドラインに基づいて、「当協会員」が策定する個人情報マネジメントシステムに、「当協会員」の活動の実態に応じた項目を追加、修正することを妨げるものではありません。但し、これはあくまでも、「当協会員」各々の実態に合わせた実効性の高い個人情報マネジメントシステムを策定するためのものであり、個人情報保護の水準低下を容認するものではありません。

第4章　個人情報保護方針

（個人情報保護方針）

第5条　「当協会員」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、かつ、維持しなければなりません。

(1)　互助会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。また、特定された利用目的を公表することを含む。）。

(2)　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。

(3)　個人情報への不正アクセス、個人情報の紛失、破壊、改ざん又は漏えいなどの防止及び是正に関すること。

(4)　苦情及び相談への対応に関すること。

(5)　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。

(6)　代表者の氏名

(7)　制定・改訂年月日

(8)　問い合わせ先

また、「協会員」の代表者は、この方針を文書化（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。)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りません。

【解説】

1. 個人情報保護方針は、「協会員」の個人情報保護に関する取り組みを内外に宣言する公式文書と位置づけられるもので、経営責任を明確にするため、取締役会の決議を経るなど一定の手続きを定めておくことが重要です。

2. 個人情報保護方針は、「協会員」の代表者が個人情報保護の理念(個人情報保護に取り組む姿勢、経営責任や基本的な考え方)を互助会事業の内容と絡めて明らかにした上で策定し、個人情報保護マネジメントシステム全体に反映する内容としなければなりません。

   また、この方針はウェブなどにより一般の人に公開することを前提とする以上、容易に理解できる表現にするとともに制定年月日及び改訂年月日、代表者名に加えて、問い合わせに応じられるように、問い合わせ先を明示しなければなりません。

3. 「当協会員」の代表者が定めた個人情報保護方針については、互助会事業に従事する者全員に周知しなければなりません。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洩等した場合に予想される結果等を説明し、理解させることが必要です。

   従業者への周知方法としては、朝礼、社内会議での周知徹底、社内各部署への掲示、社内通知文書の配布、イントラネットによる公開などがあります。また、個人情報保護方針を一般の人が入手可能なように、「当協会員」のホームページへの掲載、会社案内、ポスター等への掲載やチラシなどへの挿入等の措置を講じなければなりません。

4. 「国が定める指針」とは、個人情報保護法に基づいて主務官庁(経済産業省など)が作成したガイドライン、指針などです。

5. 個人情報保護方針についても、監査結果等を踏まえ、見直し、改善を継続することによって、「当協会員」の管理能力を高めていくことが重要です。

6. 「当協会員」の代表者は、この方針の下に、個人情報保護マネジメントシステムの策定や見直しについて担当者を指名し、個人情報保護方針に沿った活動をさせることが重要です。

7. 個人情報を取扱う業務の従事者は、個人情報保護方針を理解したうえで、本ガイドラインに準拠した業務管理システムに基づき、個人情報保護を実施していくことになります。

8. 上記個人情報保護方針中に、開示対象個人情報に関する周知事項で上記(1)～(8)と重ならない事項も含めるようにしてください。(第29条の解説1.を参照のこと)

JIS Q 15001:2006 3.2

第5章　体制及び責任

（体制）

第6条　「当協会員」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、かつ、改善するために、不可欠な資源を用意しなければなりません。

「当協会員」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りません。

【解説】

1．　個人情報保護マネジメントシステムを有効なものとするには、従業者の役割と責任、権限を決めておく必要があります。特にJIS規格で明記されている役割には、「当協会員」の代表者、個人情報保護管理者、個人情報保護監査責任者、苦情・相談責任者があり、この四者に加えて、教育責任者の役割、責任、権限は最低限決めておかねばなりません。

2．　「当協会員」の代表者は、個人情報保護の理念を明確にした上で、個人情報保護方針を策定し従業者へ周知することや、個人情報を管理するために必要な資源（“人・物・金”など）の用意、個人情報保護マネジメントシステムを実施・運用するための責任者である個人情報保護管理者、個人情報保護マネジメントシステムの監査を行なわせるための個人情報保護監査責任者などの指名、並びに監査報告、苦情、法令改正、経営環境変化などから個人情報保護マネジメントシステムを見直すことなど、重要な役割を担っており、自ら積極的に活動する代表者であることが重要です。

個人情報保護管理者、個人情報保護監査責任者及び苦情・相談責任者などの役割については、第7条で説明します。

3．　個人情報保護マネジメントシステムを文書化し、全ての従業者に周知しなければなりません。互助会事業では、社内情報を含めて考慮すべき個人情報に関わらない業務はほとんどなく、かつ、個人情報管理の重要性を全従業者に十分に認識させることが重要ですので必ず、全ての従業者に周知しなければなりません。

JIS Q 15001:2006 3.3.4

（個人情報保護管理者、個人情報保護監査責任者、苦情・相談責任者及び教育責任者の指名）

第7条　「当協会員」の代表者は、このガイドラインの内容を理解し実践する能力のある個人情報保護管理者を内部から指名し、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関わりなく与え、業務を行わせなければなりません。

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、「当協会員」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りません。

2　「当協会員」の代表者は、このガイドラインの内容を理解し、個人情報保護管理者

から独立した公平かつ客観的な立場にある者を個人情報保護監査責任者として内部から指名し、個人情報保護マネジメントシステムの監査に関する責任及び権限を与え、監査を行わせなければなりません。

3　「当協会員」の代表者は、個人情報及び個人情報保護マネジメントシステムに関しての苦情・相談を受け付けて対応する苦情・相談責任者を指名し、また、苦情・相談窓口を常設し、この連絡先を公表しなければなりません。

4　「当協会員」の代表者は、従業者に個人情報保護に関する教育を行う教育責任者を指名し、教育訓練を行わせなければなりません。

【解説】

1．　個人情報保護管理者は、当該事業に係る個人情報の管理の責任者である性格上、いたずらに指名者数を増やし、責任の所在が不明確になることは避けなければなりません。従って、複数指名する場合には、当該者間での役割分担を明確にしなければなりません。個人情報保護管理者については、社内で対外的に責任の持てる者を指名しなければなりません。

2．　本ガイドラインにおいては、個人情報保護管理者は、特に「当協会員」における個人情報保護の意識の向上に資する個人情報保護マネジメントシステムの策定について、その策定、周知徹底等の措置を実施する責任を負うとともに、代表者による個人情報保護マネジメントシステムの見直し及び改善の基礎として、その実績（運用状況など）を代表者に定期的に、かつ、適宜、報告しなければなりません。

3．　「当協会員」の代表者は、公平かつ客観的な立場にあり、監査の実施及び報告の権限を持つ内部の者を個人情報保護監査責任者に指名しなければなりません。

4．　個人情報保護監査責任者は本ガイドラインに社内規定が合致しているか、社内規定通りに運用されているかなどを監査することを指揮し作成した監査報告書により、代表者に報告しなければなりません。

5．　苦情及び相談の受付は、苦情・相談責任者又は担当者を指名し、常設の対応窓口を設置しなければなりません。但し、個人情報保護管理者との兼任は妨げません。窓口又は担当者の連絡先は、公表しなければなりません。

6．従業者に対する教育訓練は個人情報保護の重要性について十分な認識を持ってもらうために必要不可欠ですので、そのための教育責任者を指名しなければなりません。

JIS Q 15001:2006	3.3.4	資源、役割、責任及び権限、
	3.7.2.	監査、
	3.6	苦情及び相談、
	3.4.5	教育

第6章　計　画

（個人情報の特定）

第8条 「当協会員」は、自らの事業の用に供する全ての個人情報を特定するための手順を

確立し、かつ、維持しなければなりません。

【解説】

1. 社内で事業の用に供している個人情報としてどのようなものがあるかを知らないで、個人情報保護のための対策をとることはできません。したがって、個人情報を保護管理するためには、取扱っている個人情報全てについて各部署毎に、漏れなく洗い出して、特定しておくことが極めて重要です。また、把握していない個人情報があった場合、その個人情報が漏洩したり、紛失したり、改ざんされたとしても、わからず、二次被害に発展してから気づく場合もありますが、これでは遅すぎます。万一、漏洩が発生してもすぐ気づき、迅速な対応を取ることが不可欠です。しかも、個人情報は日々変化する場合が多く、新たな個人情報を特定するための手順や仕組みを確立、維持しておかなければなりません。

ここで特定するための手順とは、コンピュータシステムにより個人情報を一元管理することまでを意図しているのではなく、個人情報管理台帳のような手作業での一元管理が一般的です。

2. 個人情報を特定し管理する単位は、管理が有効に働くレベルでなくてはなりません。例えば、“○○システム”の単位では、そのシステムの中に、どのような個人情報ファイルがあり、どのように使われているかが分らない場合もあります。一般的には、入会申込書といった個人情報ファイルが管理の単位として適切と思われます。例えば、個人情報管理台帳により、各部署毎に、個人情報を含んだ管理対象のファイル名(例えば入会申込書)毎に、登録日、利用目的、入手先、社内での取扱部門、責任者、保管場所、保管形態(電子媒体、紙)、保管期間、提供・委託の有無、廃棄の方法、アクセス権限を有する者・利用制限(複写、FAX・送信、mail送信、閲覧の可否)、累積保有件数などの項目を管理しなければなりません。また、個人情報管理台帳はその内容を定期的に確認し、最新の状態で維持できるような手続きを定めなければなりません。

JIS Q 15001:2006 3.3.1

(個人情報のリスク等の認識、分析及び対策)

第9条 「当協会員」は、第8条により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、かつ、維持しなければなりません。

「当協会員」は、第8条により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、関連する法令、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)を認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければなりません。また、その際、必要

な対策を講じても対処しきれないリスク(残存リスク)についても認識しなければなりません。

【解説】

1. 目的外利用は許されないので、目的外利用を起こさないような対策を講じなければなりません。例えば、利用目的が定められていない個人情報は利用することができないような手順を定めなければなりません。

2. 特定した個人情報ファイル単位(ただし、取扱いが同じものはグルーピングをして良い。)毎に、個人情報の取り扱いの流れの各段階(取得・入力、移送・送信、利用・加工、保管・バックアップ、委託・提供、消去・廃棄)ごとに、どのようなリスクがあるかを調査し、そのリスクに見合った必要な対策を講じなければなりません。「必要な」とは、「当協会員」の事業内容や規模に応じ、経済的に実行可能な最良の技術の適用と運用手順等の確立を含む合理的な対策を講じることであり、全てのリスクをゼロにすることは不可能ですから、各段階毎に、現状把握しているリスクを踏まえ、対策を実施すべき優先順位と取り得る最善の対策を定め、未対応部分を残存リスクとして把握しなければなりません。したがって、個人情報の取り扱いの流れの各段階毎に、リスク、対策及び残存リスクを一覧表にとりまとめ、一元管理しなければなりません。このリスク・対策・残存リスク一覧表は、個人情報の適切な安全管理対策を行う前提となりますので、この作成の善し悪しが安全管理対策の善し悪しに反映されることになりますので、時間をかけて確実に行わなければなりません。また、リスクは技術の進歩、環境変化等により常に変動するものであり、また、個人情報保護・安全対策の一層の改善を図るためにも、リスク評価・対策の継続的な改善が必要ですので、この一覧表は最初に一度だけ作成すればよいものではなく、手続き規定を整備し、定期的に見直し、改善をしなければなりません。

3. 個人情報に関する「リスク」とは、不正アクセス、個人情報の紛失、破壊、改ざん、漏えいなどの人的、物的リスクだけでなく、個人情報保護法などの法令違反(例えば、本人から個人情報を直接書面で取得する場合に本人への明示・同意が取られていないとか、目的外利用を本人への通知・同意をとらずに行うとか)、国が定める指針及びその他の規範に対する違反、想定される経済的な不利益や社会的な信用の失墜、本人への不利益、悪影響などのおそれも含まれます。

「必要な対策」の内容は、リスクを回避(事故を防止)するための様々な情報セキュリティ対

策及び法令違反などをなくすために必要な手順・様式などの整備をいい、「当協会員」の建物、事務室などの入退制限・安全管理、情報システムへのアクセス制限、記録媒体の施錠管理及び個人情報の取得、利用、提供などのための申請承認手続きの整備などがあります。

4. 事故によりもたらされる信用失墜は、その漏洩の規模にもよりますが、互助会にとって致命傷となります。さらに、損害賠償や対応・復旧費用の負担などの大きな直接的影響が出るほか、官公庁や報道機関への報告、株主代表訴訟への対応など様々な影響があることを十分に認識しなければなりません。

JIS Q 15001:2006 3.3.3

（法令、国が定める指針及びその他の規範）

第10条 「当協会員」は、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、参照できる手順を確立し、かつ、維持しなければなりません。

【解説】

1. 個人情報を保護するには、社内規定はもちろんのこと、個人情報保護法、経済産業省の個人情報保護ガイドライン、厚生労働省の雇用管理に関する個人情報指針、営業地域の条例、本ガイドラインなどの法令、指針や規範を守らなければなりません。そのため、個人情報に関する法令、指針や規範を特定し、従業者が参照できる手順を確立しておかなければなりません。また、その特定した法令やその他の規範などの制定、改廃状況を常にフォローし、最新の内容に見直すとともに、必要に応じて、個人情報保護マネジメントシステムに反映する手順を確立しなければなりません。

JIS Q 15001:2006 3.3.2

（内部規定）

第11条 「当協会員」は、次の事項を含む内部規程を文書化し、かつ、維持しなければなりません。

(1) 「協会員」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程
(2) 個人情報を特定する手順に関する規程
(3) 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程
(4) 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程
(5) 個人情報の取得、利用、及び提供に関する規程
(6) 個人情報の適正管理に関する規程
(7) 本人からの開示等の求めへの対応に関する規程
(8) 苦情及び相談への対応に関する規程
(9) 個人情報の教育に関する規程
(10) 個人情報保護の点検に関する規程

(11)　是正処置及び予防処置に関する規程
(12)　内部規程の違反に関する罰則の規程
(13)　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程
(14)　緊急事態(個人情報への不正アクセス、個人情報の漏えい、滅失又はき損をした場合)への準備及び対応に関する規程
(15)　代表者による見直しに関する規程
「当協会員」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りません。

【解説】

1.　全社内を統括した個人情報保護管理を行なうためには、手順として、確立したルールを文書化して担当者が変わっても個人情報保護の継続性が保たれるようにしておかなければなりません。ルールが明文化されていないこともリスクであることを認識しておく必要があります。その内容には、(1)～(15)の各号に掲げた事項を盛り込む必要があり、これらが個人情報保護マネジメントシステムの中核をなす基本規程となります。

基本規程の整備は、第9条により実施したリスクの認識、分析及び対策がベースになるので、リスク認識等を十分にしたうえで、作成しなければなりません。また、これらの基本規程のみを策定しただけで従業者が個人情報保護のためにどのような行為をなすべきか、なすべきでないか判断できないので、これらの基本規程に基づく行動細則やマニュアル、チェックリスト、様式などを策定し、全員が同じ行動を取ることができるようにしておかなければなりません。

第35条【解説】3.参照。

2.　基本規定などは必ずしも形式的に一本化された規定でなくても良いです。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ができます。

3.　基本規程は、全社内で共通に適用し、かつ、強制力を持たせるため、重要規程と位置づけ、これらの制定・改廃は、取締役会の決議事項あるいは代表者の承認事項にし、また行動細則、マニュアル等その他の内部規定類の制定・改廃についても社内承認手続きを決めておくなど規定体系を整備しておかなければなりません。

JIS Q 15001:2006 3.3.5

(計画書)
第12条　「当協会員」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、維持しなければなりません。

【解説】

1.　個人情報を保護するためには、内部規程の策定など個人情報を保護するためのルールの策定も重要ですが、そのルールを遵守して従業者に行動させるためには教育をしなければなりません.

また、定められたルール通りに実施しているかをチェックするためには監査をしなければなりません。

2. そのための教育や監査などは毎年、計画的に行なうのが効果的かつ効率的ですので、それらの計画書を策定し、それに従って実行していかなければなりません。

3. 個人情報保護研修計画書に必要な項目は以下が考えられます。

- 年間カリキュラム
- 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
- 全員参加か任意参加かの別
- 予算など

4. 個人情報保護監査計画書に必要な項目は以下が考えられます。

- 監査テーマ
- 監査対象
- 目的
- 範囲
- 手続き
- スケジュールなど

JISQ 15001:2006 3.3.6

（緊急事態への準備）

第13条 「当協会員」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、かつ、維持しなければなりません。

「当協会員」は、個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい等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確立し、かつ、維持しなければなりません。

また、個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい等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、かつ、維持しなければなりません。

(1) 当該個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい等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うる状態に置くこと。

(2) 二次被害の防止、類似事案の発生回避等の観点から、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。

(3) 事実関係、発生原因及び対応策を管轄している経済産業局に直ちに報告し、指示を受けること。また、全互協に報告書の写しを直ちに提出すること。

【解説】

1. 緊急事態の特定手順及び対応手順を規定として策定するにあたっては、次のような事項を考慮します。

・ 緊急事態に該当する事故・状況の特定　　・ 予想される被害の規模
・ 被害を最小限に抑えるための一次的な対応　　・ 再発防止措置を実施する手順
・ 社内の緊急連絡網及び社外への報告手順の確立　　・ 緊急時対応についての教育訓練

2.　二次被害を防止することが重要です。漏えいなどの緊急事態が発生した個人情報の内容を本人に速やかに説明し、お詫びすることは勿論ですが、さらに、類似事案の発生回避のために、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なければなりません。

3.　また、互助会業界の主務大臣である経済産業大臣に所轄の経済産業局を通じて、指定様式に基づいて可及的速やかに報告し、指導を受けなければなりません。また、その報告書の写しを全互協に提出する必要があります。その際、発生原因を十分に調査し、今後、事故が発生しないように、十分な再発防止策を策定しなければなりません。

4.　個人情報の取扱いの全部又は一部を受託している場合には、上記2. の公表をするときは委託契約において公表について何ら取り決めがない場合は、委託元と相談の上、実施しなければなりません。

JIS Q 15001:2006 3.3.7

第7章　実施及び運用

第1節　運用手順

（運用手順）

第14条　「当協会員」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りません。

【解説】

手順として確立したルールは、内部規程（基本規程及び行動細則など）として文書化しておくことにより、担当者が変わっても個人情報保護水準を維持できるようにしておかねばなりません。ルールが明文化されていないこともリスクの一つであると認識すべきです。この要求事項は、運用全体に係わります。

JIS Q 15001:2006 3.4.1

第2節　個人情報の利用目的の特定に関する原則

（利用目的の特定）

第15条　「当協会員」は、個人情報を取得するにあたっては、その利用目的をできる限り特定し、互助会契約及び施行とそれに関連する事業並びに「当協会員」内の人事等を行うために必要な範囲内とし、その目的の達成に必要な限度において行わなければなりません。

【解説】

1.　利用目的は、当然のことながら、公序良俗に反しないことが求められます。

2.　「利用目的をできるだけ特定し」とは、利用目的を抽象的、一般的に特定するのではなく、「当協会員」が最終的にどのような目的で個人情報を利用するのかを可能な限り具体的に特定することです。「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「マーケテイ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はなりません。

利用目的を特定するに当たっては、次のことに配慮する必要があります。

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於いて明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於いて明示すること

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

3.　「互助会契約及び施行を行なうために必要な範囲内」とは、互助会契約を締結する際に必要な住所、氏名、生年月日、勤務先、取引先金融機関及び預金口座に係る個人情報等が該当し、冠婚関係の施行で必要な住所・氏名・出身地・勤務先・所属団体・社会的地位・招待者の氏名と社会的地位・交友関係・宗教等であり、葬祭関係では、故人及びその家族の出身地・勤務先・所属団体・社会的地位・宗教・寺院等と故人の病名・死因・死亡時刻等が該当すると考えられます。また、葬儀の生前予約では入院先・健康状態等も該当すると考えられます。なお、宗教、病名、死因、健康状態などは特定の機微な個人情報に該当しますので、第17条の規制対象となることに留意してください。

4.　「それに関連する事業を行なうために必要な範囲内」とは、顧客（互助会加入者及び一般施行者）との契約を履行するため、または事前の準備、アフターサービスとして、顧客の利便のために関連する事業として行なっている部門などによる営業販売活動や各種案内等を指します。例えば、顧客に対する新婚旅行・法事、盆のお返し品や料理・婚礼家具の情報提供及び衣裳展示会の案内状等が考えられます。

なお、医療介護用品等は必要な範囲内とは考えられません。これらの目的のために個人情報を取得し、利用・提供する際には別途予め本人の同意が必要となります。

5.　「当協会員」内の人事等を行なうために必要な範囲内」については、第3条【解説】4. を参照のこと。

JIS Q 15001:2006 3.4.2.1

第3節　個人情報の取得に関する措置

（適正な取得）

第16条　「当協会員」は、適法かつ公正な手段によって個人情報を取得しなければなりません。

【解説】

1.　「適法かつ公正な手段によって」とは、国内において規制されている法律を犯して取得したり、取得目的を詐る等の不公正な手段により取得することは許されないという意味です。また、優越的な地位を利用して取得することも許されません。

JIS Q 15001:2006 3.4.2.2.

（特定の機微な個人情報の取得、利用及び提供の制限）

第17条　「当協会員」は、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りません。但し、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第20条のただし書き(1)～(4)のいずれかに該当する場合は、この限りではありません。

(1) 思想、信条及び宗教に関する事項
(2) 人種、民族、門地、本籍地（所在都道府県に関する情報は除く。）身体・精神障害、犯罪暦、その他社会的差別の原因となる事項
(3) 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
(4) 集団示威行為への参加、請願権の行使、及びその他政治的権利の行使に関する事項
(5) 保健医療及び性生活に関する事項

【解説】

1.　上記(1)「宗教」については、「当協会員」が葬祭における施行を行なうときに必要な場合もありますが、本ガイドラインの対象としました。従いまして、これらを取得し、利用し、又は提供する場合には、明示的な本人の同意が必要です。「明示的な本人の同意」とは、書面による本人の同意をいいます。黙示的な同意は認められません。

2.　上記(2)「本籍地」について、本籍に関する全ての情報の収集を禁止すると、個人認証を必要とする業務に支障をきたすおそれがあることから、都道府県までの情報の収集については、禁止の対象外としました。但し、本籍地の情報（国籍を含む）は、時として、商行為において不当な差別につながる懸念もあることから、互助会契約の解約時の個人認証等、特に高度の個人認証を必要とする業務を除き、取得を行なわないことが望ましいと考えます。なお、本人確認において、免許証で確認する場合もそれには本籍地が記載されているため、特定の機微な個人情報に該当するので、確認に留め、その写しを求め、取得するのは望ましくありません。どうしても必要な場合には、明示的な本人の同意をとらなければなりません。

3.　上記(5)「保健医療」の典型的な例としては、個人の病歴が考えられます。遺伝性のある、又は、あると考えられる病気が存在することを勘案すれば、当該者の父母・兄弟・親類等の病歴についてもその例に含まれます。また、これに類似した情報で葬儀施行にて扱う病名・死因・

死亡時刻を当該施行以外に利用する目的で取得することは禁止します。

なお、社員の採用において、採用後の健康診断書の取得は労働安全衛生法に基づくものであることから、本人の同意は不要ですが、採用選考の資料として健康診断書の提出を求めるのは、法令に基づくものではないので、書面による同意が必要です。

JIS Q 15001:2006 3.4.2.3

（本人から直接書面により取得する場合の措置）

第18条　「当協会員」は、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、書面によって本人に明示し、本人の同意を得なければなりません。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、第19条のただし書き（1）～（4）のいずれかに該当する場合及び第20条のただし書き（1）～（4）のいずれかに該当する場合は、この限りではありません。

(1) 「協会員」の氏名又は名称

(2) 個人情報保護管理者（若しくはその代理人）の氏名又は職名、所属及び連絡先

(3) 利用目的

(4) 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、及び属性

・個人情報の取扱いに関する契約がある場合はその旨

(5) 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

(6) 第30条～第33条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

(7) 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

(8) 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

【解説】

1．本ガイドラインにおいては、本人自らの個人情報に対する権利を明確化することを目的の一つとしており、その一環として本人から直接書面により取得する際には、利用目的や開示、訂正、削除の求めに応じる旨などをあらかじめ書面によって明示し、原則として、書面により本人の同意を得なければなりません。これは、事後の紛争に備えた証拠としての役割も担うものです。

2．上記「書面によって明示」とは、互助会加入申込書、約款の裏面、又はパンフレット等に(1)～(8)までの内容について明確に記載し、当該個人情報の取得、利用又は提供に関する同意を得ることをいいます。

3．上記(2)「個人情報保護管理者（若しくはその代理人）の氏名又は職名、所属及び連絡先」の

「氏名、職名」については、責任者が容易に特定できるようにしなければなりません。また、「個人情報保護管理者（若しくはその代理人）」は、専任である必要はなく、実務的には、例えば、「お客様相談窓口」等個人情報以外についても消費者との対応窓口となる者が対応することも多いと考えられます。

4．上記(4)「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、個人情報の提供は、本人が直接関与することがないことが多いため、提供する目的、当該情報の提供を受ける者等に関する情報を、本人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となります。「組織の種類、属性」とは、個人情報の提供を受ける組織（企業の種類）と提供元の組織との関係（関連会社、持株会社等）を指します。

5．上記(7)「本人が個人情報を与えることの任意性」とは、当該申込書等の中の項目について、記載が義務的なものか、任意（アンケートのようなものか）なのかを書面の中で明らかにすることをいいます。

「当該情報を与えなかった場合に本人に生じる結果」とは、記載欄に回答しなかった場合に考えられる結果を指し、例えば、互助会加入申込書に月掛金の引き落とし口座等を記入しない等契約に係る必要な記載項目に記入がない場合、加入をお断りする場合もあるということ等が考えられます。

6．上記(8)「本人が個人情報を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、ホームページ上でのクッキー情報の取得等が挙げられますが、その場合には、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明示しなければなりません。

7．本条但し書きの事例に該当するかどうかは、当事者の恣意的な判断ではなく、条理又は社会通念による客観的な判断のもとで、極力限定的に解釈する必要があり、慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

8．互助会への加入あるいは冠婚葬祭の施行などの申込に際しては、申込時点において、本条の事項が記載されている申込書に本人が署名等により同意することが必要です。なお、別会社である代理店を通じた申込書の受付は、「当協会員」が本人から直接書面により取得する場合に該当し、本条が適用されると考えられますので、注意してください。

JIS Q 15001:2006 3.4.2.4.

（個人情報を第18条以外の方法により取得した場合の措置）

第19条　「当協会員」は、個人情報を第18条以外の方法により取得した場合は、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りません。

ただし、次に示すいずれかに該当する場合は、この限りではありません。

(1) 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、財産その他の利益を害するおそれがある場合

(2) 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

(3) 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り当該事務の遂行に支障を及ぼすおそれがあるとき

(4) 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

【解説】

1. 本人から直接書面により取得する場合以外は、本条が適用されます。したがって、委託を受ける場合、第三者として提供を受ける場合、公開情報から取得する場合等だけでなく、本人から直接取得する場合であっても、書面によらない限り（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）、本条の対象となります。

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）をいいます。公表に当たっては、事業の性質及び個人情報の取得状況に応じ、合理的かつ適切な方法によらなければなりません。

3. 上記(2)の場合とは、通知又は公表される利用目的の内容により、「当協会員」が行う営業ノウハウ等の企業秘密に関わるようなものが明らかになる場合がありうります。

4. 上記(4)の場合とは、一般の慣行としての名刺交換（ただし、ダイレクトメール等の目的に名刺を用いることは、自明の利用目的に該当しない場合がありますので注意を要します。）などはこれに該当します。また、請求書や見積書等の伝票に記載された担当者名、捺印等もこれに該当します。 さらに、電話注文を受け、届け先に関する個人情報を配送のみに利用する場合もこれに該当すると考えられますが、その後、継続してカタログ等の発送に利用する場合、当初の利用目的と異なってくるため、アクセス時に、本人の同意を得なければなりません。

5. 上記3.及び4.の判断も含め、本条但し書きの事例に該当するかどうかは、当事者の恣意的な判断ではなく、条理又は社会通念による客観的な判断のもとで、極力限定的に解釈する必要があり、慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

6.「協会員」は利用目的を通知又は公表した日を明確にしておかなければなりません。これらの日が明確でなければ、「当協会員」は利用目的を都合のいいように変えることができ、目的外利用の場合の本人の同意の条文が死文化するからです。

JIS Q 15001:2006 3.4.2.5.

第4節　個人情報の利用に関する措置

（利用に関する措置）

第20条　「当協会員」は、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りません。 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、第18条(1)～(6)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、本人の同意を得なければなりません。

ただし、次に示すいずれかに該当する場合は、この限りではありません。

(1) 法令に基づく場合

(2) 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

(3) 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、本人の同意を取ることが困難であるとき

(4) 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

【解説】

1. 個人情報の利用は、当然に特定した利用目的の達成に必要な範囲内で利用しなければなりません。

2. 特定した利用目的の達成に必要な範囲を超えて、利用する場合には、あらかじめ、書面によって、本人に通知し、原則として、書面により、同意を得なければなりません。

第18条【解説】1.を参照のこと。

3. 「特定した利用目的の達成に必要な範囲を超えて」については、「当協会員」内のある部門が、本人の同意を得て取得した個人情報を「当協会員」内の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うります。後者の場合には、例え、同一企業内であっても改めて、あらかじめ、書面によって、本人の同意を得なければなりません。

4. 「当協会員」は利用目的を特定した日を明確にしておかなければなりません。第15条により利用目的を特定した日以降に利用目的を変更した場合で、第18条等で利用目的を明らかにしているときは、本人の同意を改めて得なければなりません。

5. 上記ただし書き(1)～(4)の場合に該当するときは本人の同意は必要としません。

ただし、これらの場合に該当するかは、当事者の恣意的な判断ではなく、条理又は社会通念による客観的な判断のもとで、極力限定的に解釈する必要があり、正式な書面により依頼された場合のみ対応する等の基準を定める必要があり、また、これらの事例に該当するかどうかは、慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

6. 合併等でデータベースを統合する場合は、取得した際の利用目的とずれてしまう場合があります。ずれている場合は目的外利用になるので、統合して利用するときは改めて本人の同意を得なければなりません。

JIS Q 15001:2006 3.4.2.6

（本人にアクセスする場合の措置）

第21条 「当協会員」は、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，第18条の(1)～(6) 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りません。

ただし，次に示すいずれかに該当する場合は，この限りではありません。

(1) 個人情報の取得時に，既に第18条(1)～(6) 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，既に本人の同意を得ているとき

(2) 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

(3) 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、個人情報を提供する事業者が、既に第18条の(1)～(6)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追加し、本人の同意を得ている場合であって、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

(4) 個人情報を特定の者との間で共同して利用され、共同利用者が、既に第18条の(1)～(6)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、又は本人が容易に知り得る状態に置いているとき

－ 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

－ 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

－ 取得方法

(5) 第19条のただし書き(4) 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

(6) 第20条 のただし書き(1)～(4) のいずれかに該当する場合

【解説】

1. 「本人にアクセスする」とは、個人情報の利用目的の達成にあたり、本人に対し、郵便、電話又はダイレクトメールなどで連絡したりすることです。

2. 「取得方法」については、同窓会名簿、官報等の取得源の種類並びに書店からの購入等の取得経緯について、該当するものを全て記載しなければなりません。ただし、具体的な提供元の名称等については必ずしも明らかにする必要はありません。なお、回答がない場合は、黙示の同意があったとみなす旨の通知は不適切であり、認められません。

3. 委託を受ける者は委託を受けた個人情報が適正に取得されたものであるかどうか、委託元に確認するように努めるべきであり、委託元が明らかに法令に違反している場合には、委託を受けてはなりません。

4. 上記ただし書き(5)の場合は、第19条【解説】4.参照。

5.　上記ただし書きの場合に該当するかどうかは、慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

JIS Q 15001:2006 3.4.2.7

第5節　個人情報の提供に関する措置

(提供に関する措置)

第22条　「当協会員」は、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、取得方法及び第18条(1)～(4) 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りません。ただし，次に示すいずれかに該当する場合は、この限りではありません。

(1) 第18条 又は第21条 の規定によって、既に第18条(1)～(4)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

(2) 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

(3) 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、(2)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

(4) 特定し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

(5) 合併その他の事由による事業の承継に伴って個人情報を提供する場合であって、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

(6) 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

－ 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

－ 共同して利用する者の利用目的

－ 共同して利用する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

(7) 第20条のただし書き(1)～(4)のいずれかに該当する場合

【解説】

1. 個人情報を第三者に提供する場合は、あらかじめ、本人の同意を得ていることが原則です。

2. 上記ただし書き(1)の場合とは、個人情報を直接書面で取得する時点、又は本人にアクセスする時点で、情報提供について本人から同意を得ている提供者から取得した場合には本人が同意した利用目的の範囲内で提供する場合に限り、改めて本人の同意を得る必要はありません。例えば、本人の同意を得て作成されている紳士録は、販売の時に改めて同意を取る必要はありません。

なお、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は、本人の同意を得なければなりません。

3. 上記ただし書き(2)の場合とは、データベース事業などにおいて、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な判断のもとで、極力限定的に解釈する必要があります。当然ながら、いわゆる名簿屋はこの(2)には該当しません。

4. 上記ただし書き(3)の「法人その他の団体の役員に関する情報」とは、株主総会などで配布される事業報告書など、株主や顧客に配布される書類などに記載されている役員の履歴、持株数など、法令又は本人若しくは当該法人その他の団体自らによって公表されているような情報を指します。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良いです。「本人が容易に知り得る状態」とは、本人が知ろうと思えば、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おいていることをいい、事業の性質及び個人情報の取扱いの状況に応じ、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いけません。

5. なお、「直接書面取得時には委託する予定がなかったため委託する旨を通知していなかったが、業務拡大等により、後日委託する必要が生じた」場合は、上記ただし書き(4)に該当することとなります。

6. 上記ただし書きの(1)～(7)の場合に該当するかどうかは、慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

JISQ 15001:2006 3.4.2.8.

第6節 個人情報の適正管理義務

(個人情報の正確性の確保)

第23条 「当協会員」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りません。

【解説】

1.　上記「必要な範囲内」とは、「互助会契約及び施行とそれに関連する事業」において業務上必要な範囲のことをいいます。第15条解説3. 及び4. を参照のこと。

2.　「当協会員」は、利用目的の達成に必要な範囲内において、個人情報の誤入力防止のための入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人情報を正確かつ最新の内容に保たなければなりません。

3.　上記「正確かつ最新の状態」とは、実務上、全ての個人情報を正確かつ最新の状態に保つことには限界がある他、取引密度や利用目的等によって必ずしも情報の更新を必要としない場合もあり得ます。そこで、正確性、最新性については個人情報の利用目的からみて、必要な範囲内で確保することとします。例えば、互助会契約は長期間に及ぶため、家族構成の変更等は顧客からの連絡があった時点で速やかに情報の更新を行なう等の対応が考えられます。

4.　個人情報の正確性、最新性を保つため、情報の種類に応じて個人情報の保存期間を定めるときには、慎重な配慮が必要です。例えば、互助会月掛金の掛金中の口座情報と満期完納となった口座情報はどちらも大切な情報ですが、本人との確認性の観点からいうと満期完納となった口座情報は、極めて確認頻度が少なく直ぐに確認を必要としない情報といえますが、集金管理だけではなく、施行でも使用される可能性がありますので、満期完納となった口座情報も一元管理する必要があります。

JISQ 15001:2006 3.4.3.1.

（個人情報の利用の安全性の確保）

第24条　「当協会員」は，その取り扱う個人情報のリスクに応じて、個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい等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りません。

【解説】

1.　本条は、第8条で特定し、第9条でリスク等の認識、分析及び対策を講じた個人情報について、そのリスクに応じて安全管理措置を講じるべきであると定めており、全ての個人情報について一律に同等の安全管理措置を講じることを求めているわけではありません。

2.　安全管理措置は、「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（平成16年10月経済産業省）」の「2)安全管理措置（法第20条関連；23頁～33頁）」に従って、以下の項目について安全対策を講じなければなりません。

①　組織的な安全管理措置（従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備、運用し、その実施状況を確認すること。）

② 人的安全管理措置（従業者に対する、業務上秘密とされた個人情報の非開示契約の締結や教育訓練等を行うこと。）

③ 物理的安全管理措置（入退館（室）の管理、盗難防止のための紙・電子媒体の施錠管理、機器などの安全・環境上の脅威からの保護（、無停電電源装置、データのバックアップなど）を行うこと。）

④ 技術的安全管理措置（個人情報及びそれを扱う情報システムへのアクセス制限、不正ソフトウェア対策、情報システムの監視（アクセスログなど）、等個人情報に対する技術的な安全管理措置を講じること。）

3. さらに、「当協会員」においては、膨大かつ機微な個人情報を有していますので、以下の対策も講じてください。

① データサーバなどに保存されている会員情報などの個人情報については、漏えいなどを防止するため、データサーバなどへのアクセス可能者の制限をするのは勿論のこと、一定件数以上の個人情報を電子媒体などへのコピーしたり、プリントアウトする場合は個人情報保護管理者の事前承認を得る手順を整備するとともに、データサーバなどへのアクセスログを必ず取り、不可解なアクセスがないかどうかを頻度を決めてチェックすることが必要です。

② 個人情報が保存されたパソコンなどの社外での置き忘れや車上荒らしによる個人情報の漏洩あるいはファイル交換ソフトウィニーを介した個人情報の大量漏えいなどの事故を未然に防止するため、社内パソコンなどの外部持ち出しの原則禁止及び私物パソコンなどの社内持ち込みの原則禁止等の対策が必要です。

③ お客様の家から、事務所に戻るまでの間に、加入申込書などを電話ボックスに置き忘れたり、車上荒らしで紛失しないように自社及び代理店の営業関係者への教育を徹底するとともに、それらの漏洩リスクへの十分な対策を実施する必要があります。

④ 互助会や施行会社の本部・大きな拠点のみならず、出先の営業店、代理店においても、盗難などによる個人情報の漏洩などを避けるために、入退館（室）の管理のみならず、盗難防止のための建物、事務室などの施錠管理、紙・電子媒体の施錠管理はもとより、個々のパソコンなどに個人情報を保存しないなどの個人情報の安全管理を徹底してください。

4. 「必要かつ適切な措置」とは、経済的に実行可能な最良の技術の適用に配慮した上で実施する措置のことをいいます。

5. 個人情報の漏洩事例には、廃棄時の漏えいが多く見られることから、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等により、廃棄されたデータが他者に流出することのないように、廃棄方法の承認手続き、廃棄記録の保存などの廃棄取扱い規定の整備を行ってください。

JISQ 15001:2006 3.4.3.2.

（個人情報の安全管理に関する従業者の監督）

第25条　「当協会員」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りません。

【解説】

1．　「個人情報データベースへのアクセスが最も容易であり、個人情報の大量漏えい事故の原因になり易い情報処理関係者（委託先も含む。）、お客様との接点となり、申込書などを持ち運んでくる自社及び代理店の営業社員はもとより、「協会員」の全ての従業者（代理店の従業者も含む。）に対して、教育により個人情報保護の意識を向上させることが基本ですが、それとともに、個人情報の漏洩などに関する罰則規程の適用、雇用契約時における秘密保持に係る誓約書の提出に加えて、安全管理措置を遵守しているかの点検（運用の確認及び監査）を厳格に実施することにより、第24条で定めた安全管理措置を自社及び代理店の従業者に遵守させるように、必要かつ適切な監督を行わなければなりません。

JIS Q 15001:2006 3.4.3.3

（個人情報の委託先の監督）

第26条　「当協会員」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りません。このため、「協会員」は、委託を受ける者を選定する基準を確立しなければなりません。また、「協会員」は個人情報の取扱いの全部又は一部を外部に委託する場合は、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りません。さらに、「協会員」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りません。

(1) 委託者及び受託者の責任の明確化
(2) 個人情報の安全管理に関する事項
(3) 再委託に関する事項
(4) 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
(5) 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
(6) 契約内容が遵守されなかった場合の措置
(7) 事件・事故が発生した場合の報告・連絡に関する事項

「協会員」は，当該契約書などの書面を少なくとも個人情報の保有期間にわたって保存しなければなりません。

【解説】

1．　近年の情報化の進展に伴い、企業等における情報処理業務がますます多様化、複雑化していることから、経営の効率化や顧客サービスの向上等のために情報処理業務を外部へ委託する場合も多くなっています（いわゆるアウトソーシング）。これらアウトソーシングの増加に伴い、

情報処理などの委託先における個人情報の処理に関してトラブルが生じることのないよう必要な措置を講ずるべきであるという観点から、本条が設けられました。

2. 上記「個人情報の取扱いの全部又は一部を委託する場合」とは、例えば、代理店に対する会員募集・集金代行をはじめとして、社内の情報システム処理、互助会月掛金の口座振替処理、ダイレクトメールの発送、廃棄などの外、冠婚葬祭の施行に必要な衣裳、生花、仕出し、写真、マイクロバスの提供などの多岐に渡ります。

3. 委託先を選定する際の基準については、特に、会員募集、情報システム処理、口座振替処理、ダイレクトメールの発送、会員募集、廃棄などの「当協会員」が保有する大量の個人情報を委託する者については、プライバシーマークを取得しているか、それと同等以上の個人情報保護レベルを有していることを選定基準とすべきです。一方で、生花、仕出しなど少量の個人情報しか委託しない者については、この選定基準を適当なレベルまで緩和することも考えられます。個人に委託する場合であっても、委託先選定基準による選定が必要となります。なお、優越的な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りません。委託先が倉庫業、データセンター(ハウジング、ホステイング)等の事業者であって、当該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場合であっても、委託者は委託するものが個人情報であることを認識しているわけですから、委託先選定基準による選定が必要です。

なお、人材派遣事業者との人材派遣契約、清掃事業者との契約、オフィスの賃貸借契約等は、個人情報の取扱いを含まない限り対象外でありますが、このような事業者であっても、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。

4. 「必要かつ適切な監督」には、委託契約において、当該個人情報の取り扱いに関して、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監督内容を契約に盛り込むとともに、同内容が適切に実施されていることを、あらかじめ定めた間隔で確認することも含まれます。なお、優越的地位にある者が委託者の場合、受託者に不当な負担を課すことがあってはなりませんが、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りません。

5. 上記(1)～(7)の事項は、契約によって規定する必要がありますが、取り扱う個人情報の数量、リスクに応じて規定する契約内容は変わりうると考えます。

6. 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ます。

・個人情報の漏洩防止、盗用禁止に関する事項

・委託範囲外の加工、利用の禁止

・委託契約範囲外の複写、複製の禁止

・委託契約期間

・委託契約終了後の個人情報の返還・消去・廃棄に関する事項

・その他、個人情報の漏えいなどの防止のために必要な安全管理措置を講じる上で必要な取り決め

7. 再委託に関する事項には、以下の事項が含まれます。

・再委託を行うに当たっての委託者との協議

JISQ 15001:2006 3.4.3.4.

第7節　自己情報に関する本人の権利

(自己情報に関する権利)

第27条　「当協会員」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、符号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、「当協会員」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、第7節において"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，第30条 ～ 第33条の規定によって、遅滞なくこれに応じなければなりません。

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ありません。

(1) 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

(2) 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

(3) 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

(4) 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

【解説】

1. 「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」と同様の概念ですが、保有個人データよりやや広く、消去までの期間が6ヶ月以内のものも含みます。

2. 上記ただし書き(2)の場合とは、いわゆる総会屋等による不当要求被害を防止するため、「協会員」が総会屋等を本人とする個人情報を持っている場合や、不審者、悪質なクレーマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人情報を保有している場合などをいいます。

3. 上記ただし書き(1)～(4)の事例に該当するかどうかは、慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

4. 本人確認をすることに留意してください。第28条解説を参照。

(開示などの求めに応じる手続)

第28条 「当協会員」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りません。

(1) 開示などの求めの申し出先

(2) 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

(3) 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

(4) 第30条又は第31条 による場合の手数料(定めた場合に限る。)の徴収方法

「当協会員」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りません。

「当協会員」は、第30条の3又は第31条の4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りません。

【解説】

1. 「当協会員」は、本人に対し、その開示対象個人情報を特定するために必要な事項の提示を求めることができます。この場合において、「当協会員」は本人が容易かつ的確に開示等の求めができるよう、当該開示対象個人情報の特定に必要な情報の提供その他本人の利便性を考慮した適切な措置をとらなければなりません。

2. 開示などの求めをすることができるのは、プライバシー保護の見地から本人又は次の本人の代理人のみとします。

① 未成年者又は成年被後見人の法定代理人

② 開示等の求めをすることについて本人が委任した代理人

3. 「当協会員」が、開示等の求めを受け付ける方法を合理的な範囲で定めたときで、求めを行った本人又はその代理人がそれに従わなかった場合は、開示等を拒否することができます。ただし、開示等の求めに応じるにあたって本人確認をする際には、運転免許証又はパスポートの呈示だけに留めず、その写しを要求するなど、本人に必要以上の個人情報の提供を求めることには注意が必要です。ただし、一方で、本人確認を怠った場合は、個人情報の漏洩に繋がりますので、慎重に対応することが必要であり、例えば、電話での問い合わせにおいては、一定の登録情報(生年月日など)の確認及びコールバックすることなどが必要と考えられます。この点については経済産業省のガイドライン(ⅲ開示等の…の確認方法;51ページ)を参照してください。

4. 開示できない事項として、例えば個人に関する特定の人事評価等、社会通念や慣行により開示が適切でないと認められるものは対象から除くことが可能ですが、この場合には慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

5.　本人からの開示請求については、実費を勘案して合理的であると認められる範囲内で手数料等の負担を求めることができます。なお、その場合、本人にあらかじめ所要の費用負担を求めることを知らせるべきであり、約款などにその旨及び手数料を明記しなければなりません。

JISQ 15001:2006 3.4.4.2

開示対象個人情報に関する事項の周知など)

第29条 「当協会員」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。）に置かなければなりません。

(1) 「当協会員」の氏名又は名称

(2) 個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先

(3) すべての開示対象個人情報の利用目的[第19条の(1)～(3)までに該当する場合を除く。]

(4) 開示対象個人情報の取扱いに関する苦情の申し出先

(5) 当該「当協会員」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

(6) 第28条 によって定めた手続

【解説】

1. 「当協会員」は、開示対象個人情報に関する事項を本人が知りうる状態におくことにより、開示等の対象となる個人情報を明確にしなければなりません。「本人が知りうる状態（本人の求めに応じて遅滞なく回答する場合を含む。）」とは、ウェブ画面への掲載、パンフレットの配布、本人の求めに応じて遅滞なく回答を行うこと等、本人が知ろうと思えば知ることができる状態に置くことをいい、常にその時点で正確な情報を本人が知りうる状態に置かなければなりません。この周知事項は、個人情報保護方針中に記載することが適切です。

2. 「当協会員」が開示等の求めを受け付ける方法を合理的な範囲内で定めたときで、求めを行った者がそれに従わなかった場合は、開示等を拒否することができます。ただし、本人確認にあたっては、必要以上の個人情報の提供を求めてはなりません。（第28条の【解説】3. を参照）

3. 開示対象個人情報に該当する場合は、第18条～第22条により、(1)～(6)の事項を本人に明示あるいは通知しているときであってもこの要求事項に従い、本人の知りうる状態に置いておかねばなりません。

「開示対象個人情報の取扱いに関する苦情の申し出先」については、「当協会員」が個人情報保護法第37条以下に定める認定個人情報保護団体の対象事業者であるときには、「当協会員」に対する苦情を当該外部組織に申出ることができる旨を周知することも求められま

す。

4．「協会員」は家族から開示等を求められることもあり得るため、そのような場合も含め、開示等の求めに対する対応方法（本人の委任状がない場合には、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、知りうる状態に置いておくことが望ましい。

JISQ 15001:2006 3.4.4.3

開示対象個人情報の利用目的の通知）

第30条 「当協会員」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りません。ただし、第19条 のただし書き(1)～(3)のいずれかに該当する場合、又は第29条(3)によって当該本人が識別される開示対象個人情報の利用目的が明らかな場合は利用目的の通知を必要としませんが、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りません。

【解説】

1． 「当協会員」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りません。

2． 本人確認をすることに留意してください。第28条【解説】3. を参照。

JISQ 15001:2006 3.4.4.4

（開示対象個人情報の開示）

第31条 「当協会員」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、法令の規定によって特別の手続きが定められている場合を除き、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りません。ただし、開示することによって次の(1)～(3)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ありませんが、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りません。

(1) 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

(2) 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

(3) 法令に違反することとなる場合

【解説】

1． 上記ただし書き(2)は、同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務ができなくなる場合、あるいは、人事などの評価といった社会通念や慣

行により開示が適切でない場合等が考えられますが、業務上著しい支障を及ぼすおそれがある場合などについて、慎重、かつ、限定的に対応しなければなりません。この場合には慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

２．　本人確認をすることに留意してください。第28条解説を参照。

JISQ 15001:2006 3.4.4.5

開示対象個人情報の訂正，追加又は削除）

第32条 「当協会員」は、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が、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、法令の規定によって特別の手続き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などを行わなければならない。また、「協会員」は訂正などを行ったときは、その旨及びその内容を、本人に対し、遅滞なく通知し、訂正などを行わない旨の決定をしたときは、その旨及びその理由を、本人に対し遅滞なく通知しなければなりません。

【解説】

１．「当協会員」は、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が開示の結果、誤っており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等を求められた場合は、当該開示対象個人情報の訂正等を行わなければなりません。

２．　本人確認をすることに留意してください。第28条【解説】3. を参照。

JISQ 15001:2006 3.4.4.6

（開示対象個人情報の利用又は提供の拒否権）

第33条 「当協会員」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，この条において“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りません。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りません。ただし、第31条のただし書き(1)～(3)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ありませんが、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りません。

【解説】

１．　本人による利用・提供の拒否を一般的な原則としたのは、近年個人情報の流通が頻繁に行なわれる中で、本来個人情報の利用・提供について本人の了解を取るべき場合にも、それが行なわれないという事態も起こり得るからです。また、本人の了解を得られた場合であっても、契約に際し約款等で包括的に行なわれるときには、本人が将来の利用・提供についてまであらかじめ的確に判断したとは限らないことも考えられます。したがって、本人の了解を得ることを

怠った場合はもちろん、本人の了解が一応得られた場合であっても、その後の状況に応じ本人は自己の情報の利用・提供を拒み得るので、原則として、本人が求めた場合には、それに応じなければなりません。

2. ただし、第31条のただし書き(2)に基づき、互助会契約及び施行に関する個人情報であって、顧客管理、月掛金、冠婚、葬祭に係る役務サービスの提供のために必要なものなどについては、拒否権の対象から除外することが考えられます。また、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、拒否権の対象から除外することが考えられます。ただし、除外する場合には慎重な判断を要しますので、個人情報保護管理者の承認を受ける手順を整備してください。

3. 本人確認をすることに留意してください。第28条【解説】3. を参照。

JISQ15001:2006 3.4.4.7

第8節 教育

(教育)

第34条 「当協会員」は、従業者に、定期的に適切な教育を行わなければなりません。

2 「当協会員」は、従業者に関連する各部門及び階層における次の事項を理解させる手順を確立し、かつ、維持しなければなりません。

(1) 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

(2) 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

(3) 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

「当協会員」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、かつ、実施し、かつ、維持しなければなりません。

【解説】

1. 「当協会員」に対し、その従業者に定期的に適切な教育を施す責務があり、①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・利点、②個人情報保護マネジメントシステムに適合するために必要とされる役割・責任、及び、③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について、理解させ、自覚させ、個人情報保護体制における各々の役割・権限を確実に果たすことができるようにする手順を確立し、維持していくことを定めなければなりません。「協会員」の代理店の従業者についても、同様な教育を行って下さい。

2. 個人情報保護マネジメントシステムに定められた事項を理解し、遵守するとともに、従業者にこれを理解させ、及び遵守するための教育訓練の企画・運営をする者を教育責任者として指名します。

3. 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なく、教育の有効性の確

認を報告することが必要です。すなわち、感想文・アンケート・小テストを実施するなどにより、従業者の理解度を把握し、必要に応じて、教育内容の見直し(教育用テキストの内容、教育研修の時間の確保も含む)を図ることや、教育を受けたことを自覚させる仕組みを取り入れることが必要です。教育研修の欠席者にも後日、漏れなく教育することが必要であり、従業者全員に教育を実施したことの記録を残さなければなりません。

JISQ15001:2006 3.4.5

第9節　文書範囲及び文書管理

(個人情報保護マネジメントシステム文書の範囲)

第35条 「当協会員」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りません。

(1)個人情報保護方針

(2)内部規程

(3)計画書

(4)本ガイドラインが要求する記録及び「当協会員」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

【解説】

1. 個人情報保護マネジメントシステムとは、実際に「協会員」内で機能している仕組みそのものをいい、内部規定だけでなく資源を含めた全体を指します。 個人情報保護マネジメントシステムの「基本となる要素」とは、その個々の構成要素のことで、それを明確に把握するために文書化しておくことが必要です。上記(1)～(4)は最低限、文書化しなければなりません。

2. 個人情報保護マネジメントシステム文書を作成することの目的及び意義は、以下のとおりです。

① 「協会員」内部の内部規程の一部として体系的に位置付け、監査、教育、違反の際の罰則などについて、円滑な対応措置を取ることができるようにすること。

② 「協会員」の従業者全員に周知徹底し、個人情報の保護水準を担保すること。個人情報保護方針については、対外的にもまた「協会員」の従業者全員に周知徹底することにより、規範化すること。

③ 「協会員」の個人情報保護管理者、個人情報保護監査責任者及び苦情・相談対応窓口責任者、教育責任者など一定の責務を担う者に対し、個人情報保護マネジメントシステムに則った措置をとらせること。

④ 文書化することにより、その時点における個人情報保護マネジメントシステムの内容を明示的に特定し、恣意的な解釈・運用を許さないこと。

3. 個人情報保護マネジメントシステム文書の具体的イメージは次表のとおりです。

基本となる要素	個人情報保護マネジメントシステム文書の種類

	基本規程	下位文書
個人情報保護方針	・個人情報保護方針	
内部規程	・個人情報保護基本規程	
	・法令及びガイドライン	
	・個人情報を特定する手順に関する規定	・実施手順及び運用マニュアル、様式等
	・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	・実施手順及び運用マニュアル、様式等
	・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	・実施手順及び運用マニュアル、様式等
	・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 (例)・組織図 ・組織権限規程 ・職務分掌規程	・実施手順及び運用マニュアル、様式等
	・緊急事態(個人情報が漏えい、滅失又はき損した場合)への準備及び対応に関する規定	・実施手順及び運用マニュアル、様式等
	・個人情報の取得、利用及び提供に関する規定	・実施手順及び運用マニュアル、様式等
	・個人情報の適正管理に関する規定	・実施手順及び運用マニュアル、様式等
	・本人からの開示等の求めへの対応に関する規定	・実施手順及び運用マニュアル、様式等
	・教育に関する規定	・実施手順及び運用マニュアル、様式等
	・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	・実施手順及び運用マニュアル、様式等
	・苦情及び相談への対応に関する規定	・実施手順及び運用マニュアル、様式等
	・点検に関する規定	・実施手順及び運用マニュアル、様式等
	・是正処置及び予防処置に関する規定	・実施手順及び運用マニュアル、様式等
	・代表者による見直しに関する規定	・実施手順及び運用マニュアル、様式等
	・内部規定の違反に関する罰則の規程	・実施手順及び運用マニュアル、様式等
計画書		・教育計画書
		・監査計画書
記録類		・教育報告書
		・監査報告書
		・苦情相談結果報告書
		・個人情報の特定に関する記録
		・法令その他の規範の特定に関する記録
		・個人情報のリスク認識、評価及び対策に関する記録
		・利用目的の特定に関する記録

基本となる要素	個人情報保護マネジメントシステム文書の種類	
	基本規程	下位文書
		・安全管理に関する記録 ・開示対象個人情報に関する開示等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 ・運用確認の記録(点検の記録) ・是正措置及び予防措置の記録 ・代表者による見直しの記録など

JISQ15001:2006 3.5.1

(文書の管理)

第36条 「当協会員」は、本ガイドラインが要求する全ての文書(記録を除く。)を管理する手順を確立し、実施し、かつ、維持しなければなりません。文書管理の手順には、次の事項が含まれなければなりません。

(1) 文書の発行及び改訂に関すること。

(2) 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。

(3) 必要な文書が必要なときに容易に参照できること。

【解説】

1. 文書として管理するとは、単に保存するだけでなく、常に最新の状態で維持することを含みます。

2. 実施記録も文書の一種ではありますが、第37条に規定する要求に従って管理するものとします。

3. 文書類は、個人情報保護マネジメントシステムを構成する要素が互いにどのように関係しているか、及び特定部分の運用についての詳細な情報がどこに記述されているかを十分に示せる程度であれば良いです。文書類は「協会員」によって実施される他のシステムの文書類を使用することがあり、そのような使い方をする場合は、それらの文書を個人情報保護マネジメントシステム文書の中に入れておく必要があります。

4. 文書管理は個人情報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り、目的ではないことに留意する必要があります。

JISQ15001:2006 3.5.2

(記録の管理)

第37条「当協会員」は、個人情報保護マネジメントシステム及び本ガイドラインの要求事項へ

の適合を実証するために必要な記録を作成し、かつ、維持しなければなりません。

「協会員」は、記録の管理についての手順を確立し、実施し、かつ、維持しなければなりません。

【解説】

1. 必要とする記録には、以下のものが含まれます。

- 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
- 目標及び計画書
- 利用目的の特定に関する記録
- 安全管理に関する記録
- 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など

2. 記録は紙媒体である必要はなく、運用しやすい合理的な方法で作成すると良いです。

3. 「当協会員」は、必要な記録を特定し、保管、保護、保管期間及び廃棄についての手順を確立し、実施し、維持しなければなりません。「必要な記録を特定し」とは、記録自体も個人情報である可能性があるから、とりあえず何でも記録として残すという姿勢ではなく、その必要性を判断すべきという意味です。また、記録は必要なときに直ぐに検証できるように維持しておかなければなりません。

JISQ15001:2006 3.5.3

第10節　苦情及び相談

（苦情及び相談への対応）

第38条　「当協会員」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、迅速な対応を行う手順を確立し、かつ、維持しなければなりません。

「当協会員」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りません。

【解説】

1.　「当協会員」が、個人情報及び個人情報保護マネジメントシステムに関し本人からの苦情・相談を受け付け、適切、迅速に対応すべき義務を負うことを定めます。

2.　個人情報保護の問題は、個人情報の不適切な取扱い行為に起因するものであり、当事者間における事実上の対応等により解決することのできる場合も多いと推測され、又、迅速な解決も望まれることから、本人からの苦情・相談に対応することは、個人情報保護の実効性を確保するものといえます。

3.　苦情・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わなければなりません。ただし、個人情報保護管理者との兼任は妨げません。必要な体制の整備に当たっては、JISQ 10002「品質マネジメント－顧客満足－組織における苦情対応のための指針」を参考にして下さい。

JISQ15001:2006 3.6.

第8章　点　検

（運用の確認）

第39条　「当協会員」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「当協会員」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確立し、実施し、かつ、維持しなければなりません。

【解説】

1.　運用の確認とは、組織全体として実施される監査とは異なり、各部門、各階層において行われるものです。日常業務において気づいた点があればそれを是正、予防していくためのものであるため、各部門及び各階層の管理者は、定期的に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かを確認し、不適合が確認された場合は、その是正措置及び予防措置を行わなければなりません。自主点検はルール通り実施されているかどうかを見回って確認する程度でも良いです。

2.　確認した記録を残すという面では、以下の(1)～(3)は必須とします。

(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

JISQ15001:2006 3.7.1.

（監査）

第40条　「当協会員」は、個人情報保護マネジメントシステムのこのガイドライン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りません。

「当協会員」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「当協会員」の内部から指名し、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りません。

個人情報監査責任者は，監査を指揮し，監査報告書を作成し，「当協会員」の代表者に報告しなければなりません。監査員の選任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りません。

「当協会員」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及び権限を定める手順を確立し，実施し，かつ、維持しなければなりません。

【解説】

1. 監査すべき事項は、a．本ガイドラインとの適合性監査（個人情報保護マネジメントシステムが本ガイドラインの要求事項と合致していることの監査）、b．運用状況の監査（個人情報保護マネジメントシステムに従って運用されているかの監査であり、教育訓練が計画書どおりに行なわれているかどうかも監査の対象です。）であり、監査チェックリストを作成して実施すべきです。

2. 個人情報保護監査責任者は、内部の者から指名された適任者であることが要求されますが、個人情報保護管理者とは異なる者でなければならず、かつ、社外に責任を持つことができる者（例えば、役員クラス）であって、個人情報保護管理者と同等あるいは上席者を指名することが望ましい。監査員は「当協会員」内部からの要員によって、又は「当協会員」のために働くように外部から選んだ者によって実施することができます。その際、監査を実施する監査員には力量があり、公平かつ客観的に行える立場にある者をあてます。また、監査員は自己の所属する組織の監査をしてはいけません。

3. 運用状況の監査にあたっては、第9条により講じることとした対策を監査項目に設定して実施すべきです。

4. 監査報告書には、監査実施状況のほか、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区別して示す必要があり、また、「当協会員」の代表者に報告しなければならず、改善の指示も代表者から受けるようにしなければなりません。なお、監査報告書は、第42条で定める「当協会員」の代表者による見直しへのインプットとしても不可欠です。

JISQ15001:2006 3.7.2

是正処置及び予防処置）

第41条 「当協会員」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及び権限を定める手順を確立し、実施し、かつ、維持しなければなりません。その手順には，次の事項を含めなければなりません。

(1) 不適合の内容を確認する。

(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。

(3) 期限を定め、立案された適切な処置を実施する。

(4) 実施された是正処置及び予防処置の結果を記録する。
(5) 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。

【解説】

1. 不適合は、点検(運用の確認や監査)の結果、漏えいなどの緊急事態の発生及び外部からの指摘等により、「当協会員」が本ガイドラインの要求を満たしていないと判断したものです。不適合の原因が特定されなければ、根本的な解決にはならず、再発を防げません。被監査部門は、指摘事項となった不適合の原因を特定した上で、再発防止のための是正処置及び予防処置を立案し、承認を受け、実施しなければならなりません。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すが、不適合の内容によっては、長期に渡ることもあり得ます。不適合の内容に相応した期限の設定が望ましい。

JISQ15001:2006 3.8

第9章 見直し

(「当協会員」の代表者による見直し)

第42条 「当協会員」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りません。また、「当協会員」の代表者の見直しの記録(議事録)を取らなければなりません。

「当協会員」の代表者による見直しにおいては,次の事項を考慮しなければなりません。

(1) 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
(2) 苦情を含む外部からの意見
(3) 前回までの見直しの結果に対するフォローアップ
(4) 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
(5) 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
(6) 「当協会員」の事業領域の変化
(7) 内外から寄せられた改善のための提案

【解説】

1. 個人情報を適切に保護するため、「協会員」の代表者は、年に最低1回は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りません。

2. 監査は社内の現状のルールを前提に、それが守られているかを点検するものであり、それに基づく改善も現状の枠内に留まるものですが、代表者の見直しは、それに留まらず、外部環境も考慮した上で、現状そのものを根本的に見直すことがあり得る点で、監査による改善とは本質的に異なる点に注意する必要があります。

3. 上記(1)～(7)の事項をまとめて見直す必要はありません。見直しは随時実施されることもあります。

4. 代表者の見直しの記録(議事録)を取らなければなりません。 改善措置をとる必要があると

判断されたときは、必要な改善措置をした後、個人情報保護マネジメントシステム文書に改善内容を反映し、また、改善の内容、改善日と改善履歴を記録する必要があります。

JISQ15001:2006 3.9