個人情報保護法に対応する

組合のリスクマネジメント

平成１７年5月

全国中小企業団体中央会

はしがき

コンピュータの処理能力の向上により、顧客・取引先データ、組合員名簿等の大量の個人情報をデータベース化し、各種の条件で検索、集計、抽出することが可能となりました。さらには、コンピュータシステムをインターネットとつなげることで、より詳細な個人情報をさまざまな目的のために利用することが可能となっています。

しかし、その一方では、情報の漏えいによる各種問題が表面化し、個人情報の取扱いに対して、慎重さが求められてきています。個人情報は、氏名、生年月日、住所、電話番号等個人を特定する項目を扱うという性質上、誤った取扱いをされると、個人に取り返しのつかない被害を及ぼすおそれがあります。

企業からの顧客情報等の大規模な流出や個人情報の売買等の事件が発生し、損害賠償の請求、特定個人への集中的攻撃等が発生し社会問題化してきています。それに伴い、個人のプライバシーをどのように保護していくか、安全管理等企業の個人情報保護の取組みが求められています。

このような状況のもと、「誰もが安心して高度情報通信社会の便益を享受するための制度的基盤として、官民を通じた個人情報保護の基本理念等を定めた基本法に相当する部分と民間事業者の遵守すべき義務等を定めた一般法に相当する部分から構成される」、個人情報の保護に関する法律（以下「個人情報保護法」といいます。）が、平成１５年５月３０日に公布、一部施行され、平成１７年４月１日より２年間の猶予をもって完全施行されました。

そこで本会では、組合等の中小企業連携組織がそれぞれに保有する組合員名簿や取引先データ等の個人情報の取扱いについて、同法の完全施行により、どのような点に留意し、組織として取り組んでいったらよいか、その方向性をとりまとめることと致しました。

組合等の中小企業連携組織は、業種・業態、組織規模、内部の業務処理等千差万別で異なっており、本書に掲載した様式等がすべての組合等中小企業連携組織にそのまま当てはまるものではありませんが、個人情報保護法にそってどのように実行していけばよいか検討するに当たって参考となれば幸甚です。

平成１７年５月

全国中小企業団体中央会

目　　次

第１章　個人情報保護法について

１．全体構造

個人情報保護法は、「高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護すること」を目的として制定されました。

同法は、「第１章　総則」から「第６章　罰則」まで全５９条と附則から構成されています。「第１章　総則」、「第２章　国及び地方公共団体の責務等」及び「第３章　個人情報の保護に関する基本方針」については、事業者の自律的な取組みに関して、行政機関等の支援が重要であり、国が事業者等への支援、苦情処理のための措置を講ずべきことを定めるとともに、個人情報の保護のための措置が整合的に実効性をあげていくためには、事業者、地方公共団体、国の行政機関等が協力し、連携を確保していくことが重要であることから、平成１５年５月３０日に公布・施行されました。そして、「第４章　個人情報取扱事業者の義務等」から「第６章　罰則」については、個人情報を取り扱う事業者にとっては、個人情報の適正な取扱いを強いられるため、２年間の猶予をもって平成１７年４月１日から施行されました。

国、地方公共団体及び独立行政法人以外の個人情報取扱事業者が取り扱う個人情報の利用目的等を定める「第４章　個人情報取扱事業者の義務等」が本法の中心となりますが、これを分類してみると、

① 個人情報の取得、取扱い関連事項（第１５条　利用目的の特定」から「第１８条　取得に際しての利用目的の通知等」まで）

② 個人データの管理関連事項（「第１９条　データ内容の正確性の確保」から「第２３条　第三者提供の制限」まで）

③ 本人の対応と苦情処理関連事項（「第２４条　保有個人データに関する事項の公表等」から「第３１条　個人情報取扱事業者による苦情の処理」まで）

の概ね三つに分けられます。

このうち、「個人データの管理関連事項」では、個人情報取扱事業者に対し、安全管理措置、従業者の監督、個人データの取扱いを委託する場合の委託者の監督及び第三者提供の制限等を定めています。この取組みを組織において具体化すると、個人情報保護方針、個人情報保護規程等各種規程類の整備や、個人情報を保護するために必要な事項を検討する個人情報保護委員会の設置など、従来にはない体制等の確立を図ることが求められています。

２．個人情報取扱事業者

個人の氏名や住所、電話番号等の個人情報を収集し、営利、非営利を問わず事業のために取扱う者は、規模の大小をとわず、個人情報の量や取扱う内容によって「個人情報取扱事業者」とされ、個人情報保護法の適用を受けることになりました。

協同組合や商工組合等の組合をはじめとした中小企業連携組織についても、保有する情報量によっては、当然に個人情報取扱事業者となり、同法を遵守し、適切な対応を行わないと、主務大臣から勧告、命令、さらには、罰則を受けることもあります。

「個人情報取扱事業者」（法第２条第３項関連）とは、その事業の用に供する個人情報データベース等を構成する、個人情報によって識別される特定の個人の数の合計が、過去６カ月以内に５，０００人を超えた者をいいます（国の機関、地方公共団体、独立行政法人等は除きます。）。また、「事業の用に供している」の「事業」とは、一定の目的を持って反復継続して遂行される同種の行為であって、かつ、一般社会通念上事業と認められるものをいい、営利、非営利を問いません。法人格のない任意団体や個人であっても、個人情報取扱事業者に該当します。

なお、特定の個人の数については、電話会社の電話帳や電話帳ＣＤ－ＲＯＭのように個人情報データベース等を他人が作成したもの、カーナビゲーションシステムのように、すでに氏名、住所、電話番号が入っているもので、新たに個人情報を加えたり、他の個人情報を付加したり、個人情報データベース等そのものを変更するようなことをせずに、事業の用に供しているものは算入しません。

組合等の中小企業連携組織が、個人情報保護法に基づく個人情報取扱事業者に該当する場合には、組織の体制や規程類の整備など、現状をとりまとめ整理することから取り組まなければなりません。

３．個人情報保護法で使用する基礎的用語の整理

ここでは、まず、個人情報保護法でよく使用される用語等の定義について、簡単に説明をします。

同法で使用されるわかりにくい用語の定義、解説につきましては、５１ページ以下に参考として掲載しました「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。以下「ガイドライン」といいます。）を参照して頂くのがわかりやすいと思いますので、以下に記載した用語以外の解説は、ガイドラインに委ねることとします。

①　「個人情報」（法第２条第１項関連）

「個人情報」とは、“生存する個人に関する情報”であって、氏名、生年月日その他の記述等により特定の個人を識別することができるものをいいます。これには、映像、音声による情報も含まれ、また、暗号化されていても対象と

なります。生存する個人には、日本国民だけでなく、外国人も含まれますが、法人その他の団体は「個人」に該当しません。

② 「個人情報データベース等」（法第２条第２項関連）

「個人情報データベース等」とは、特定の個人情報をコンピュータ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、個人情報を含む情報の集合物、又は、コンピュータを用いていない場合であっても、カルテや指導要録等、紙面で処理した個人情報を一定の規則（例えば、五十音順、年月日順等）に従って整理・分類し、“特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いている”ものをいいます。

そのため、電子メールで活用しているメールアドレス帳、ユーザーＩＤとユーザーが利用した取引についてのログ情報が保管されている電子ファイルなども対象となります。

また、職員、社員等の名刺については、パソコン以外でも体系的に整理され、他の職員、社員等も検索できる状態にしている場合は、該当しますので注意が必要です。

つまり、“他人により容易に検索できる状態になっているか否か”がポイントとなります。

③ 「個人データ」（法第２条第４項関連）

「個人データ」とは、個人情報取扱事業者が管理する“個人情報データベース等を構成する個人情報”をいいます。他の媒体に格納したバックアップ用の個人情報やコンピュータ処理による個人情報データベース等から出力された帳票等は個人データに該当します（個人情報データベース等を構成する前の入力帳票に記載されている個人情報は個人データにはなりません。）。

④ 「保有個人データ」（法第２条第５項関連）

「保有個人データ」とは、個人情報取扱事業者が、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すべてを行うことができる権限を有する個人データです（受託して処理しているものは除きます。）。

なお、その存否が明らかになることで、公益その他の利益が害されるもの、６カ月以内に消去する（更新は除きます。）ものは、保有個人データから除かれます。

⑤ 「本人」（法第２条第６項関連）

「本人」とは、個人情報によって識別される特定の個人をいいます。

第２章　個人情報取扱事業者の責務等

１．個人情報の取得、取扱い関連事項

（１）利用目的の特定（第１５条～第１６条）

個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」といいます。）をできる限り特定しなければなりません。

利用目的の特定に当たっては、利用目的を「当組合の事業活動」、「組合員や取引先へのサービスの向上」等抽象的、一般的に特定するのではなく、「組合員が取り扱う○○品の共同販売事業の商品の発送、新商品情報のお知らせ」など「可能な限り具体的に特定するとともに、個々の処理の目的を特定するにとどめるのではなく、あくまで個人情報取扱事業者において最終的にどのような目的で個人情報を利用するかを特定する必要があります。

また、あらかじめ個人情報を第三者に提供することを想定している場合には、利用目的において、その旨を特定しなければなりません。

なお、具体的な○○品や事業の特定に当たっては、日本標準産業分類の中分類から小分類程度の分類など、社会通念上、本人から見てその特定に資すると認められる範囲に特定することが望ましいとされます。

（２）利用目的の変更（第１５条第２項、第１８条第３項）

個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはなりません。

また、個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければなりません。

（３）利用目的による制限（第１６条第１項）

個人情報取扱事業者は、あらかじめ本人の同意を得ないで、特定された利用目的（例えば、就職のための履歴書の個人情報をもとに、組合員の取扱商品の販売促進のために商品カタログと購入申込書を送る場合など）の達成に必要な範囲を超えて、個人情報を取り扱ってはなりません。

（４）事業の承継による個人情報の取得（第１６条第２項）

個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前におけるその個人情報の利用目的の達成に必要な範囲を超えて、本人の個人情報を取り扱ってはならないとされます（承継前の利用目的の達成に必要な範囲内で取り扱う場合は、目的外利用にはならず、本人の同意を得る必要はありません。）。

（５）適正な個人情報の取得（第１７条関連）

個人情報取扱事業者は、親の同意もなく、十分な判断能力のない子供などから、親の収入状況や家族の個人情報などを、偽ったり、いろいろな不正の手段を使って個人情報を取得してはなりません。

（６）利用目的の通知、公表（第１８条第１項関連）

個人情報取扱事業者は、個人情報を取得する場合は、あらかじめその利用目的を公表する必要があります。あらかじめ利用目的を公表していない場合は、取得後速やかに、その利用目的を本人に通知するか、又は公表しなければなりません。

ガイドラインでは、

ａ．インターネット上で本人が自発的に公表している個人情報を取得する場合

ｂ．インターネット、官報、職員録等から個人情報を取得する場合

ｃ．電話による問合せやクレームのように本人により自発的に提供される個人情報を取得する場合

ｄ．個人情報の第三者提供を受ける場合

などを掲げています。

なお、個人情報保護法の施行前から保有している個人情報については、本条は適用されませんので、本人に通知又は公表をする義務はありませんが、「本人に知り得る状態」（Ｗｅｂページへの掲載、パンフレット、本人の要求に応じて回答を行うなど、本人が知ろうと思えば知ることができる状態）におくことをが必要です。

（７）書面やインターネットのＷｅｂ画面から入力するアンケート調査や応募等での個人情報の収集（第１８条第２項関連）

個人情報取扱事業者は、書面等による記載やインターネットのＷｅｂ画面から打ち込み等により入力する方法など、直接本人から個人情報を取得する場合には、あらかじめ、本人に対し、その利用目的を明示（本人に明確に示すことをいいます。）しなければなりません。

なお、口頭で行う個人情報の取得にまでは、本人への利用目的を明示する義務はありません。

２．個人データの管理関連事項

（１）データ内容の正確性の確保（第１９条関連）

個人情報取扱事業者は、個人情報データベース等への個人情報の入力時の照合や確認、誤りを発見した場合の訂正をする場合、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で、個人データを正確かつ最新の内容に保つよう努めなければなりません。入力、照会、訂正を行った場合には、記録等をつけることが必要で、不明確なデータ入力、更新、削除等を行うことなどは好ましくあり

ません。
　この場合、保有する個人データを一律に又は常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すればよいこととされています。

（２）安全管理措置（第２０条関連）
　個人情報取扱事業者は、個人データの漏えい、滅失又はき損の防止、その他の個人データの安全管理のため、①組織的、②人的、③物理的及び④技術的な、安全管理措置を講じなければなりません。
　この安全管理措置を行うための取決め等の準備、組織内へ如何に浸透させていくかが、最も重要な課題になるといえます。
　なお、個人データが漏えい、滅失又はき損等をした場合に、個人データの本人が被る権利利益の侵害の大きさを考慮し、個人データの取扱い等によるリスクに応じ、“必要かつ適切な措置を講じる”ものとします。その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましいとされます。“必要かつ適切な安全管理措置を講じていない場合”の例をガイドラインでは次のような例をあげています。
　ａ．公開されることを前提としていない個人データが事業者のホームページ上不特定多数に公開されている状態を個人情報取扱事業者が放置している場合
　ｂ．組織変更が行われ、個人データにアクセスする必要がなくなった従事者が個人データにアクセスできる状態を個人情報取扱事業者が放置していた場合で、その従事者が個人データを漏えいした場合
　ｃ．本人が継続的にサービスを受けるために登録していた個人データが、個人情報取扱事業者による不適切な取扱いにより滅失又はき損し、本人がサービスの提供を受けられなくなった場合
　ｄ．個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合
　ｅ．個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合
　以下に、①組織的、②人的、③物理的及び④技術的な、安全管理措置についての概略を記載しますが、ガイドラインに詳細な内容が記載されているので、参照して下さい。
　しかし、ガイドラインに記載されている項目をすべて取り入れ、規程等に掲げ、一挙に導入しようとしても、実現性の乏しい言葉だけの内容になってしまうことが予想されます。組合等中小企業連携組織の業種・業態や事務局組織の状態、コンピュータの設置形態、規模に応じた、個人情報が漏えい等しないよう、現実的で段階的な組織独自の規程類と実行体制を整備していくことが肝要であります。

① 組織的安全管理措置

組織的安全管理措置とは、安全管理について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（以下「規程等」といいます。）を整備運用し、その実施状況を確認することをいいます。組織的安全管理措置には以下の事項が含まれます。

- 個人データの安全管理措置を講じるための組織体制の整備
- 個人データの安全管理措置を定める規程等の整備と規程等に従った運用
- 個人データ取扱台帳の整備
- 個人データの安全管理措置の評価、見直し及び改善
- 事故又は違反への対処

② 人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいいます。

人的安全管理措置には以下の事項が含まれます。

- 雇用及び契約時における非開示契約の締結
- 従業者に対する教育・訓練の実施

なお、従業者には含まれませんが、個人データを保有する建物や情報システムにアクセスする可能性がある者（情報システムの開発・保守関係者、清掃担当者、警備員等）についても、アクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することが望ましいとされます。

③ 物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいいます。物理的安全管理措置には以下の事項が含まれます。

- 入退館（室）管理の実施
- 盗難等に対する対策
- 機器・装置等の物理的な保護

④ 技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいいます。技術的安全管理措置には、以下の事項が含まれます。

- 個人データへのアクセスにおける識別と認証
- 個人データへのアクセス制御、アクセス権限の管理、記録
- 個人データを取り扱う情報システムに対する不正ソフトウェア対策
- 個人データの移送・通信時の対策
- 個人データを取り扱う情報システムの動作確認時の対策、情報システムの監視

（３）従業者の監督（第２１条関連）

個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、その個人データの安全管理を図るため、従業員に対し「安全管理措置」を遵守させるよう必要かつ適切な監督をしなければなりません。ガイドラインでは、従業者とは、「個人情報取扱事業者の組織内にあって、直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。」とされています。

適切な監督をしていない例として、ガイドラインでは、

ａ．従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、予め定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合

ｂ．内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出し、それを放置した結果、紛失し、個人データが漏えいした場合

を例示しているので注意が必要です。

また、従業者に対し必要かつ適切な監督を行うに際し、「従業者のモニタリングを実施する」ことも考えられます。その際には、モニタリングの目的は何であるか、モニタリングの実施に関する責任者とその権限などを社内規程にとどめ、取得する個人情報の利用目的をあらかじめ特定し、重要事項として労働組合等に通知するとともにし、必要に応じて協議を行い、それを定めたときは、労働者等に周知することが望ましいとされます。

（４）委託先の監督（第２２条関連）

個人情報取扱事業者は、個人データの取扱いを業者等に委託、請負わせる場合、安全管理措置を遵守させるよう、受託する者に対し必要かつ適切な監督をしなければなりません。この“必要かつ適切な監督”には、委託者である個人情報取扱事業者が定める安全管理措置の内容（責任の明確化、個人データ漏えい防止、盗用禁止事項、委託契約範囲外の複写、複製の禁止、委託処理期間、個人データの返還・消去・廃棄に関する事項等）に盛り込むとともに、正しく遵守されていることを、定期的に確認することも含まれます。

特に委託された業者が再委託をする場合、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得ますので、注意が必要です。

（５）第三者への提供　――（原則）（第２３条関連）

個人情報取扱事業者は、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはなりません。親子兄弟会社、グループ会社間で個人データを交換したり、同業者間やフランチャイズ組織の本部と加盟店の間で個人データを交換する場合などは、第三者提供に当たります（同一事業者内で他部門へ個人データを提供すること第三者提供ではありません。）。

（６）第三者への提供　――（オプトアウト）（第２３条第２項関連）

個人情報取扱事業者は、第三者への提供に当たり、あらかじめ利用目的、氏名、住所、電話番号等の個人データ項目や、書籍として出版したり、インターネットに掲載する等第三者に提供する手段又は方法、本人が第三者への提供を停止してほしいと申し出た場合、いつでも停止できるとの情報を、本人に通知し、又は本人が容易に知り得る状態に置いておくことを行っている場合（オプトアウト）には、本人の同意なく、個人データを第三者に提供することができます。

ガイドラインでは、表札を調べて住宅地図を作成し、販売する住宅地図業者やダイレクトメール用の名簿等を作成し、販売するデータベース事業者をオプトアウトの例として掲げています。

（７）委託（第２３条第４項第１号）

個人情報取扱事業者が、利用目的の達成に必要な範囲内において、個人データの取扱いの全部又は一部を委託する場合は、第三者提供に該当しません。これは、個人情報取扱事業者が、委託先に対して、厳重な監督責任が課されるからです。

（８）承継（第２３条第４項第２号）

合併、分社化、営業譲渡等により事業が承継され、個人データが移転される場合で、承継後も個人データが譲渡される前の利用目的の範囲内で利用されるのであれば、その個人データの提供を受ける者は、第三者に該当しません。

（９）共同利用（第２３条第４項第３号関連）

個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、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場合は、第三者に該当しないことになっています。

（10）雇用管理に関する個人データ関連（第２３条関連）

従業員を子会社等へ出向させた際に、出向先にその従業員の人事考課情報等の雇用管理に関する個人データを提供することを行うことが多いと思います。出向元から出向先にその個人の個人データが提供された場合、出向先の役員及び従業員は、出向してきたその従業員の雇用管理に関する個人データを第三者へ提供したり、複写・複製、漏えいしたり、又は盗用してはなりません。

３．本人の対応と苦情処理関連事項

（１）保有個人データに関する事項の公表（第２４条関連）

個人情報取扱事業者は、保有している個人データについて、Ｗｅｂページへの掲載、パンフレットの配布等、以下の情報を本人の知り得る状態に置かなければなりません。

- 当該個人情報取扱事業者の氏名又は名称
- すべての保有個人データの利用目的
- 個人データの取扱いに関する苦情の申出先、個人データの開示、訂正、利用停止、及び、保有個人データの利用停止の求めに応じる手続（手数料の額を定めたときは、その手数料の額を含みます。）

（２）利用目的の通知（第２４条第２項、第３項関連）

個人情報取扱事業者は、本人から、本人の保有個人データの利用目的の通知を求められたときは、遅滞なく、本人に通知しなければなりません。

なお、通知しない旨を決定したときも、遅滞なく、本人に通知しなければなりません。

（３）保有個人データの開示（第２５条関連）

個人情報取扱事業者は、本人から、その本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含みます。）を求められたときは、本人に対し、書面の交付による方法（開示を求めた本人が、電子メール等でもよいと同意した場合には、電子メール等も可。）で、遅滞なく、当該保有個人データを開示しなければなりません。

（４）保有個人データの訂正等（第２６条関連）

個人情報取扱事業者は、本人から、その本人が識別される保有個人データの内容が事実でないと、その本人の個人データの内容の訂正、追加又は削除を求められた場合には、個人データの内容の訂正、追加又は削除に関して、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、その結果に基づき、当該保有個人データの内容の訂正等を行わなければなりません。

また、個人情報取扱事業者は、保有個人データの内容の全部若しくは一部について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正等を行ったときは、その内容を含みます。）を通知しなければなりません。

（５）保有個人データの利用停止等（第２７条第１項、第２項）

個人情報取扱事業者は、本人から個人データが、利用目的の達成に必要な範囲を超えたり、不正により個人情報を取得し、その保有個人データの利用の停止又は消去（「利用停止等」といいます。）を要求された場合や、あらかじめ本人の

同意を得ないで第三者に提供されているという理由で、その保有個人データの第三者への提供の停止を要求された場合、その要求に理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければなりません。ただし、当該保有個人データの利用停止等に多額の費用を要する場合やその他の利用停止等を行う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、この限りではありません。

また、個人情報取扱事業者は、保有個人データの全部若しくは一部について、ａ．利用停止等を行ったとき、ｂ．利用停止等を行わない旨の決定をしたとき、ｃ．第三者への提供を停止したとき、ｄ．第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければなりません。

（６）理由の説明（第２８条関連）

個人情報取扱事業者は、保有個人データの、ａ．利用目的を通知しない決定をしたとき、ｂ．全部又は一部について開示しない決定をしたとき、ｃ．全部又は一部について訂正、追加又は削除（訂正等）を行ったとき、又は訂正等を行わない決定をしたとき、ｄ．全部又は一部について利用停止等を行ったとき、又は利用停止等をしないことを決定したときは、本人に対し、その理由を説明するよう努めなければなりません。

（７）開示等の求めに応じる手続（第２９条関連）

個人情報取扱事業者は、本人から保有個人データについて、ａ．利用目的の通知を要求されたとき、ｂ．開示を要求されたとき、ｃ．内容の訂正、追加又は削除（訂正等）を要求されたとき、ｄ．利用の停止又は消去（利用停止等）を要求されたとき（「開示等の求め」といいます。）は、その手続方法を本人の知り得る状態においておかなくてはなりません。

（８）手数料（第３０条関連）

個人情報取扱事業者は、利用目的の通知又は開示を求められたときは、当該措置の実施に関し、手数料を徴収することができます。また、手数料を徴収する場合には、実費を勘案して合理的であると認められる範囲内で、その手数料の額を定めなければなりません。

（９）苦情の処理（第３１条関連）

個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければなりません。また、苦情の処理を図るため、必要な体制の整備に努め、苦情の適切かつ迅速な処理を行うに当たっては、苦情処理窓口の設置や苦情処理の手順を定める等必要な体制の整備に努めなければなりません。

第３章　個人情報取扱事業者が取り組む手順

１．「コンプライアンス・プログラム（ＣＰ）」とは

組合等の中小企業連携組織が、個人情報保護法に基づく個人情報取扱事業者になる場合には、その事業規模及び活動に応じた、個人情報の保護のための「コンプライアンス・プログラム（ＣＰ）」を作成する必要があります。

コンプライアンス・プログラムとは、ＪＩＳ　Q15001の前身である「個人情報保護ガイドライン」から使われている言葉で、方針（ポリシー）、規程（スタンダード）、細則（プロシージャー）、手順書（マニュアル）が含まれます。教育に関する計画書、システム関係の報告書、さらには、就業規則、安全管理などの規程類、安全管理委員会の書類、議事録など、いわば組織全体の仕組み、コンセンサスを示すことになります。

このように組織、グループ等を網羅したコンプライアンス・プログラムは、個人情報保護に関わる全社的、組織的な活動といえます。コンプライアンス・プログラムを効果のあるものにしていくためには、実現性のある具体的な計画立案と実行体制づくりが重要です。

２．現状把握＜第１段階＞

（１）個人情報の把握

現在、組織内にどのような個人情報が、どのくらいのデータ量を有しているか、保管形態は紙媒体、電子媒体のいずれか、そこにアクセスすることができるのは、どのような方法で、だれが可能なのかなど、まず現状の把握に努めます。目次や索引がつけられていて個人情報の検索が可能であれば、紙媒体なども該当しますので漏れがないように整理を行うことが必要です。

個人情報保護法により、個人情報が漏えいした場合には、勧告、命令、さらには罰則といった行政処分だけでなく、本人からの求めに応じ、情報を開示したり、訂正や削除に応じなければならなくなります。そのためには、組織内にどのような個人情報がどのくらいあるか把握する必要があります。

（２）利用目的の明確化

個人情報を収集する際、又は、すでに収集した個人情報データについては、利用目的を明確にし、本人に通知・公表したり、目的以外で利用する場合には、本人の同意を得ないといけなくなります。また、本人に容易に知り得る状態におかなければなりません。

従来、個人情報をデータベース化し、代表者宛にダイレクトメールやパンフレットを顧客や取引先、組合員へ送付したり、マーケティング等のさまざまな戦略

に使用している組織にとって、利用目的を具体的に定めることは、範囲が定まらず難解な業務であるといえます。例えば、利用目的を追加、変更する場合などは、個別に本人から同意をとる必要が生じ、今まで実施したことのない手数のかかる作業になります。利用目的をすべてに該当するように抽象的に記載したいものですが、具体的に示していなければ、クレームが発生することにもなりかねません。そのため、考えられる個人情報の利用目的を具体化、明確化し、今後どのような利用目的で個人情報を取得していくのかを検討していく必要があります。

３．各種規程、体制等の段階的な整理、整備＜第２段階＞

（１）方針、規程、規則類の作成、整備

個人情報保護方針、個人情報保護規程の作成、各部門・部署の責任の範囲、業務委託先との覚書、教育研修プログラムなど、業種・業態、組織の状況に応じた各種規程等の段階的な整理、整備を行い、体系的なコンプライアンス・プログラム（ＣＰ）を構築していくことになります。

このとき、コンプライアンス・プログラムを検討していくと、従来の作業、業務の流れ、慣行・慣習等を変更しなくてはならないことも少なくないことから、無理のない計画で、かつ、法律が要求している項目を網羅した実効性のある整備をしていくことが必要です。

組合等中小企業連携組織において、作成する必要がある文書は、次の三つから構成されます。

イ．個人情報保護方針

組合等中小企業連携組織それぞれの個人情報保護に対する取組みの方針を示す文書です。すべての職員等は、この方針に従って行動する必要があります。

ロ．個人情報保護規程

個人情報保護方針に従い、それを実践するための具体的な仕組みや規則を文書化したものです。

ハ．規則、細則、覚書き、手順、台帳等

個人情報保護規程に準じて、具体的な運用するために定めた手順等を定型化、あるいは文書化したものです。組織の状況に応じて、さまざまな種類が考えられますので、段階的に整備する必要があります。

- 個人情報ファイル等管理台帳
- ソフトウェア管理台帳
- メールアドレス及びアクセス権限一覧
- 情報機器管理室（サーバルーム）入室・作業記録
- 外部の委託業者との覚書き

・　文書管理に関する規則
・　入退室管理手順
・　教育研修プログラム
など。

（２）個人情報保護体制

個人情報保護方針、個人情報保護規程、規則等の規程類の整備とあわせ、個人情報を安全、かつ、適切に取り扱うため必要な個人情報保護体制を実効あるものとして組織することが必要です。

そのためには、個人情報保護に関する目標、計画の策定、諸規程類の作成、改訂、教育、事故対応、情報セキュリティ対策等の全般的実務、円滑な運用について責任を負う「個人情報保護委員会」を組合等中小企業連携組織内に設置します。「個人情報保護委員会」は、最高責任者としての委員長、部門別の個人情報管理責任者、教育責任者、苦情対応責任者、情報システム管理者等の委員から構成されます。また、監査役を置き、定期的に個人情報保護規程等に定められた事項が適切かつ有効に実効されているか評価・確認を行います。

（個人情報保護委員会を構成する各種の責任者、委員については、組合等中小企業連携組織それぞれの実情に応じて設置して下さい。）

（３）職員教育

個人情報の「内部からの流出」を防止するためには、職員に対し教育・研修を行って、個人情報保護に関する知識レベル、均質化するために均質化するなど、組織的な取組みが必要です。

職員のセキュリティに関する認識の甘さにより情報が流出してしまうというケースも多くみられます。入退管理、施錠管理、データのバックアップ、データの破棄等のルール化にあわせ、社員リテラシーの向上も含め、計画的な社員教育を徹底して行うことが必要です。

（４）委託業者の監督責任

組合等中小企業連携組織が保有する個人情報データベースに接触する可能性のためコンピュータ機器の保守業者や印刷業者など、外部の委託業者に業務を預託する場合は、預託する業務を厳選したり、個人情報やデータ項目を必要最低限のものに絞り込んだりする必要があります。また、業務を委託した業者が別の事業者に再委託することは、原則禁止する必要があります。

なお、委託契約書や細則、覚書き等に秘密保持義務規定を盛り込むなど、外部の委託先についても、個人情報の漏えい等がないよう監視をしていく必要があります。

４．危険分散と対外的信用力の維持に向けて＜第３段階＞

（１）個人情報を取得する際の通知や事前同意

組合等中小企業連携組織は、通常総会、各種委員会、○○記念式典などの諸会議を開催し、出欠通知を組合員等から受領する場合が少なくありません。その際には、氏名、住所、電話番号等個人情報に係わるデータが収集されることになるため、「本出欠票及び委任状により収集される氏名、住所、電話番号の個人データは、平成○○年度通常総会に関する議案審議、議事録送付、賦課金徴収通知以外には使用しません。」等の利用目的を具体化した文面を入れて通知しておくことが必要です。

また、第三者に個人情報を提供する場合には、事前に同意をとっておくことが得策です。個人情報取得後に第三者提供を行うことも可能ですが、第三者提供の場合は、取扱いが厳格で、それぞれに通知するだけでなく、それぞれに同意を得る必要があるので、コスト等を考えると取得時に同意を得ておく必要があります。

（２）監視体制の構築

コンピュータウィルスやワームの侵入を監視、第三者のなりすましによる不正なアクセス、インターネットや持ち込み機器からの進入を防ぐため、３６５日・２４時間監視体制の構築の方法等実現可能なシステムを検討します。

また、ソフトウェアのバグなどによって生じた、システムのセキュリティ上の弱点であるセキュリティーホール対策を検討します。

（３）個人情報の安全性の確保（電子認証制度の活用）

事務所入り口、サーバルームへの入退出やデータベースへのアクセス制限などの対策について、限られた人間にしかアクセスを許可しないことで、第三者による個人情報の閲覧や持ち出しを防止することができます。また、アクセスログを一定期間保管し、個人情報などが流出した場合でもアクセスログを追跡することで被害を最小限に押さえることも重要です。

特に、個人情報の安全性の確保の観点からは、全国中央会の電子認証制度等個人認証技術を用いて、“なりすまし、漏えい、改ざん、否認等”の危険性を低下させていく必要があります。

（４）個人情報保護の取組みに関する第三者機関による認定

個人情報保護の取り組みに対する第三者機関による認定があり、代表的なものとしては、「プライバシーマーク制度」があります。これは、個人情報保護の取組みに対する第三者機関による認定を取得することで、個人情報の取扱に関する社内体制やセキュリティシステムを整備できるほか、個人情報保護やセキュリティに対する積極的な姿勢を対外的にアピールすることができます。

（５）「中央会の個人情報漏えい賠償責任保険」への加入

情報漏えいが起きてしまうと、企業の信頼と利益を失うことになります。漏えい事件が起こってしまった場合、対応によっては組織の存続が左右されます。情報流出の疑いが生じた場合、調査開始の公表から結果報告までには、あまり時間的に余裕はありません。万が一、情報漏えい事故が起きてしまった場合に備え、「中央会の個人情報漏えい賠償責任保険」に加入するなど、補償の用意や専門家と相談できる体制等を準備しておくことが必要です。

第４章　コンプライアンス・プログラム参考例

ここでは、組合等中小企業連携組織がコンプライアンス・プログラムを構築していくための、最初に取り組む必要のある代表的な方針、規程を参考として掲載します。

なお、以下の規程類は、参考例であり、組合等の組合等中小企業連携組織の業種・業態、組織の状況等に応じて、改訂・改良等を加えて作成して下さい。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

＜個人情報保護方針＞（例）

制定　平成１７年　　月　　日

○○○協同組合（以下「本組合」という。）は、本組合の事業活動を通じて得た個人情報の保護に努めることを社会的責務と認識し、以下の方針に基づき個人情報の保護に努めます。

１．個人情報の取得について

本組合は、適法かつ公正な手段によって、個人情報（氏名、性別、生年月日、住所、電話番号、ＦＡＸ、メールアドレス、所属組合、役職、その他の記述により当該本人を識別できるもの）を取得致します。

２．個人情報の利用について

本組合は、本組合の事業活動やサービス提供の過程で収集した個人情報を本組合事業活動及びサービス提供とこれに付随する業務を行う目的の範囲内で利用させて頂きます

上記以外の目的で利用する必要がある場合には、あらかじめご本人の承諾を得ることを前提と致します。

また、収集した個人情報の取扱いを外部に委託する場合には、委託先について厳正な調査を行ったうえ、個人情報の漏えい等の事故が発生しないよう適正な監督を行います。

３．個人情報の第三者提供について

本組合は、下記の場合を除き、個人情報を、事前に本人の同意を得ることなく、第三者に提供致しません。

（１）法令に定める場合

（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得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り当該事務の遂行に支障を及ぼすおそれがあるとき。

４．個人情報の管理について
（１）本組合は、個人情報の正確性を保ち、これを安全に管理致します。
（２）本組合は、個人情報の紛失、破壊、改ざん及び漏えい等を防止するため、不正アクセス、コンピュータウィルス等に対する適正な情報セキュリティ対策を講じます。
（３）本組合は、個人情報を持ち出し、外部へ送信する等によりこれを漏えいさせません。

５．個人情報の開示・訂正・利用停止・消去等について
本組合は、本人が自己の個人情報について、開示・訂正・利用停止・消去等を求める権利を有していることを認識し、これらの要求がある場合には、誠実に対応致します。

６．組織・体制
（１）本組合は、個人情報保護管理責任者を置くとともに、個人情報を取り扱う部門ごとに部門責任者を置き個人情報の適正な管理を実施致します。
（２）本組合は、役職員に対し個人情報の保護及び適正な管理方法についての研修を実施し、日常業務及び退職後における個人情報の適正な取扱いを徹底致します。

７．個人情報保護コンプライアンス・プログラムの策定・実施・維持・改善
本組合は、この方針を実行するため、個人情報保護コンプライアンス・プログラム（本方針、個人情報保護規程その他の規程を含む。）を策定し、これを本組合役職員その他関係者に周知徹底させて実施し、維持し、継続的に改善致します。

○○○協同組合
理事長　○　○　○　○

＜お問い合わせ窓口＞
○○○協同組合
個人情報保護管理責任者
事務局長　○　○　○　○
連絡先　〒999-9999　東京都中央区新川9-9-9
Tel 03（9999）9999　　Fax 03(9999)9998

＜個人情報保護規程＞（例）

制定　平成１７年　月　日

○○○協同組合

１．目　的

本規程は、○○○協同組合（以下「本組合」という。）が取り扱う個人情報の適切な保護のための項目を定め、役員、職員をはじめとする従事者がその事業内容に応じた個人情報保護を遵守することを目的とする。

２．用語の定義

本規程における用語の定義は、下記のとおりとする。

（１）個人情報

「個人情報」とは、生存する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等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することがきるものを含む。）をいう。

（２）本人

「本人」とは、個人情報によって識別される特定の個人をいう。

（３）従事者

本組合内において業務に従事する役員、職員、派遣社員及びアルバイトなどをいう。

３．適用範囲

本規程は、コンピュータ・システムにより処理されているか否か、及び書面に記録されているか否か等を問わず、本組合において取り扱われるすべての個人情報を対象とする。

４．照会先

この規程に対する照会先は、○○○○協同組合個人情報保護委員会とする。

５．計　画

（１）個人情報の特定

取得、利用、保管など、取り扱う個人情報は、すべて特定する。

（２）個人情報に関するリスクの明確化

特定された個人情報は、必ずそのリスク（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）を明確にする。

（３）法令及びその他の規範

ａ．本組合における個人情報の取扱いに関わる業務に関する法令やその他の規

範は、「個人情報に関する法令及びその他の規範リスト」を作成し特定するとともに、法令及びその他の規範の本文をいつでも参照できるように整備する。リスト及び本文は、最新の状態で維持できるように定期的に見直す。

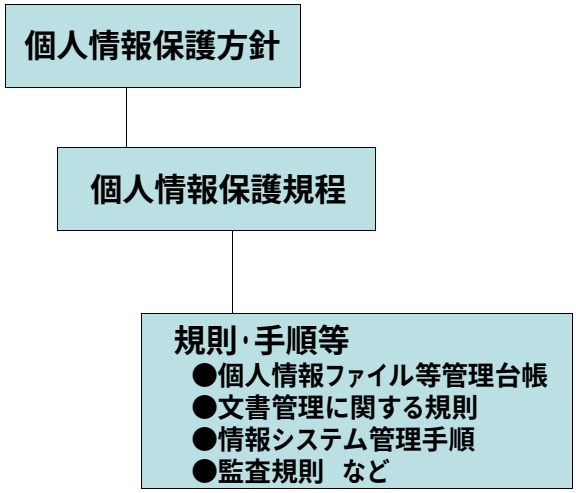
ｂ．法令及びその他の規範に改廃があった場合は、速やかにその改廃内容を本規程や関連規程類に反映する。

６．個人情報保護に関する文書

（１）文書の構成

本組合における個人情報保護に関する文書の体系は、下記のとおり３階層で構成される。

個人情報保護に関する文書の体系



①　個人情報保護方針

本組合の個人情報保護に対する取り組みの方針を示すもの。すべての従事者は、この方針に従って行動する必要がある。

②　個人情報保護規程

本規程のことで、個人情報保護方針を実践するための仕組み及び規則等を文書化したもの。

③　規則・手順等

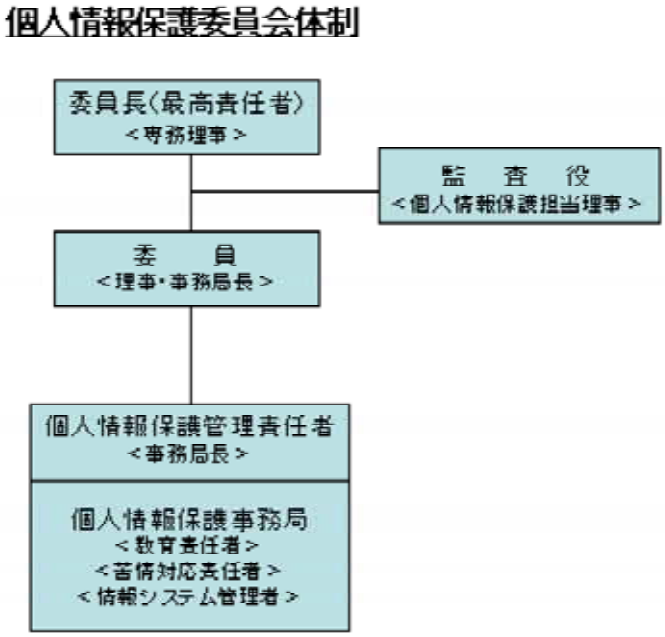
本規程に準じて、個人情報保護体制を運用するために定める具体的な規則・手順等を文書化したもの。

（２）文書の見直し

各文書を所管する部門は、本組合の組織変更、社会情勢の変化、関係法令・技術などに対して、個人情報保護関連文書が常に合理的かつ現実に即したものとなるよう、必要に応じて内容を見直す。

７．個人情報保護委員会の設置

本組合が保有する個人情報及び情報資産について、本組合全体として適切に取り扱い、それを保護するとともに、必要かつ適切な措置を講ずるため、個人情報保護委員会を設置する。



（１）本委員会の具体的役割

本委員会は、個人情報と情報資産全般に係る取扱方針を決定し、体制整備及びその維持改善に努める。また、必要に応じて個人情報保護管理責任者に対し、企画立案又は改善案策定、作業実施、状況又は結果報告等の指示を行い、報告内容を評価のうえ、判断又は承認を行う。

（２）本委員会の構成

本委員会は、以下のメンバーで構成する。

①　委員長（最高責任者）

ａ．理事長の名により、専務理事がこれにあたる。

委員長は、本組合における個人情報等情報資産全般に係る取扱いの最高責任者となるとともに、個人情報保護委員会を効果的に運用するために役割、責任及び権限を定め、文書化し、かつ、すべての従事者に周知させる。

ｂ．委員長は、公平かつ客観的な立場にある者を監査役として任命する。
ｃ．委員長は、個人情報保護管理責任者を任命し、管理責任者としての責任と権限を明確にし、業務を行わせる。

② 監査役

監査役は、「（７）個人情報保護に関する監査」に定める個人情報等情報資産の取扱いに関する監査を実施し、個人情報保護委員会に報告する。

③ 委　員

ａ．委員は、本会における個人情報等情報資産の取扱いに関する事項又は事務所内外で発生する情報セキュリティに関する事項を、個人情報保護委員会に議題として提示する。
ｂ．委員は、本規程に定められた事項を理解し遵守するとともに、従事者にこれを理解させ、安全対策の実施及び周知徹底等の措置を実施する責任を負う。

④ 個人情報保護管理責任者

ａ．個人情報保護管理責任者は、個人情報保護委員会を運営するうえで必要な事務並びに個人情報等情報資産の取扱い全般に関する文書等を管理する。
ｂ．個人情報保護管理責任者は、個人情報保護委員会で決定した事項の実施、状況の調査・報告、企画・改善案の策定等について、個人情報保護事務局を設置し、必要な指示を行い、その結果を判断したうえで個人情報保護委員会に報告する。

⑤ 個人情報保護事務局

ａ．個人情報保護管理全般を主管する組合事務局がこれにあたる。
ｂ．個人情報保護事務局は、個人情報保護管理責任者の指示に基づいて、本規程に定められた事項を理解し遵守するとともに、従事者にこれを理解させ、遵守させるための教育訓練、安全対策の実施及び周知徹底等の措置を実施する責任を負う。
ｃ．個人情報保護管理責任者は、前項の責務を果たすため、教育責任者、苦情対応責任者並びに情報システム管理者を定める。

⑥ 教育責任者の責務

ａ．教育責任者は、本規程に定められた事項を理解し遵守するとともに、個人情報に関連のある業務に関わる従事者に本規程を遵守させるための教育訓練を企画・運営する責任を負う。

⑦ 苦情対応責任者の責務

ａ．苦情対応責任者は、本規程に定められた事項を理解し遵守するとともに、組合員等からの個人情報に係る問い合わせ・苦情等を受け付けて対応するとともに、相談内容を分析し再発防止等を検討して本規程の運営に反映させる責任を負う。
ｂ．問い合わせ・苦情を受け付けた従事者は、問い合わせ･苦情の受付内容を苦情対応責任者に報告する。

⑧ 情報システム管理者の責務

情報システム管理者は、本規程に定められた事項を理解し遵守するとともに、

本会情報システムの安全管理と効果的かつ効率的な運用に努める責任を負う。

（３）個人情報の取扱い

①　利用目的の特定

ａ．利用目的は、本組合の正当な事業の範囲で、明確に定めること。

ｂ．利用目的は、できる限り具体的に特定すること。

ｃ．利用目的を変更する場合は、本規程に従い、新たに本人に通知又は公表すること。

②　取得に際しての利用目的等の通知

ａ．以下の事項を本組合Ｗｅｂページなどで公表するか又は本人に通知すること。

・　個人情報を収集、利用する事業名

・　利用目的

・　開示等の手続きにおいて手数料を取得する際は、手数料の額

・　個人情報の取扱いに関する苦情の申出先

ｂ．Ｗｅｂページなどで公表している場合でも、契約書その他の書面、インターネットの入力フォームなど、本人から直接に個人情報を収集する際には、利用目的を本人に通知すること。

ｃ．個人情報を他と共同して利用する場合は、その旨並びに共同して利用されるデータの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人情報の管理責任者名を、あらかじめ本人に通知するか、Ｗｅｂページなどで公表すること。

③　個人情報の収集と利用の原則

ａ．個人情報の収集は、適法かつ公正な手段によって行うこと。

ｂ．個人情報の取得と利用は、利用目的の達成に必要な範囲内で行うこと。

ｃ．合併その他の事由により他者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ない限り、個人情報の収集と利用は、承継前における当該個人情報の利用目的の範囲内で行うこと。

④　特定の機微な個人情報の取得、利用及び提供の禁止

次に示す社会的差別を助長するような内容を含む個人情報の収集、利用又は提供を行ってはならない。ただし、これらの取得、利用又は提供について、本人の明確な同意、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。

・　思想、信条及び宗教に関する事項

・　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

・　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

・　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

・　保健医療及び性生活

⑤　提供の制限

個人情報は、あらかじめ本人の同意を得ないで、第三者に提供してはならない。ただし、次に掲げる事項について、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は、当該個人データを第三者に提供することができる。

・　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データの項目
・　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

⑥　個人情報の委託処理に関する措置

ａ．業務を委託するなどのため個人情報を外部に預託する場合は、十分な情報セキュリティ水準を提供する者を選定すること。

ｂ．前項で選定した委託事業者とは、契約などの法律行為により、本会の指示の順守、個人情報に関する秘密の保持、再委託に関しての事項及び事故時の責任分担などを担保するとともに、当該契約書などの書面又は電磁的記録を個人情報の保存期間にわたり保存するものとする。

ｃ．前項の再委託に関しての事項において、委託事業者による再委託は原則禁止とし、必要な場合は、承諾を得る旨を盛り込むこと。

⑦　個人情報に関する本人の権利

ａ．本人又はその代理人（未成年者又は成年被後見人の法定代理人、及び開示等の求めをすることにつき本人が委任した代理人に限る。）から自己の情報について開示を求められた場合は、原則として合理的な期間内にこれに応ずること。

ｂ．ただし、法令が定める場合及び開示を求められた個人情報が、本人の評価、選考などに関するものであって、これを開示することにより業務の適正な実施に支障が生ずるおそれがあると認められる場合などには、その全部又は一部に応じないことができるものとする。

ｃ．開示の結果、誤った情報があった場合で、訂正又は削除を求められた場合には、原則として合理的な期間内にこれに応ずるものとし、訂正又は削除を行った場合には、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うこと。

ｄ．本会が既に保有している個人情報について、本人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、これに応ずること。

（４）個人情報の適正管理義務

①　個人情報の正確性の確保

個人情報は利用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すること。

②　個人情報利用時の安全性の確保

ａ．個人情報に関するリスク（個人情報への不当なアクセス又は個人情報の紛失、破壊、改ざん、漏えい等）に対して、技術面及び組織面において合理的な安全対策を講ずること。
ｂ．個人情報管理責任者は、少なくとも年１回リスク評価を行い、その評価結果及び対策を委員長に報告すること。
ｃ．個人情報の廃棄方法
本会が個人情報を廃棄する場合、その方法は次のとおりとする。
イ．書面に記録された個人情報
・　破砕機による破砕、溶解又は焼却
ロ．電磁的に記録された個人情報
・　記録媒体の破砕又は電子ファイルの完全消去（再利用不可能な方法）

（５）教　育
ａ．すべての従事者は、教育責任者の定める個人情報保護に関する教育を受けなければならない。
ｂ．教育には下記の事項を含むこととする。
・　個人情報保護の重要性及び利点
・　個人情報保護のための役割及び責任
・　本規程や関連法令の規定に違反した際に予想される結果と処置
ｃ．研修の内容及びスケジュールは、毎年教育責任者が定め、委員長の承認を得るとともに、スケジュール及び実績を整理する。

（６）苦情及び相談
ａ．本組合は、苦情相談窓口を設置し、個人情報の取扱いに関して、情報主体からの苦情及び相談を受け付けて対応、整理する。
ｂ．是正・予防措置が必要な場合は、速やかに是正・予防措置を実施するとともに実施内容を記録する。

（７）個人情報保護に関する監査
＜監査の実施＞
ａ．監査は、「監査規則」に従い、実施する。
ｂ．監査役は、毎年、監査計画を立案し委員長の承認を得る。
ｃ．監査役は、監査計画に従って監査を行い、「監査報告書」を作成し、委員長に報告する。委員長は報告書を保管する。
ｄ．報告書に改善勧告が含まれていた場合、委員長は被監査部門に対し、改善活動の実施を命じるものとする。
ｅ．被監査部門は、改善勧告に従って改善活動を行わなければならない。
ｆ．監査役は、改善活動のフォローアップを行うとともに、改善状況を委員長に報告する。

（８）委員長による見直し

ａ．委員長は、監査報告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、定期的に個人情報保護体制を見直さなければならない。

ｂ．個人情報保護体制の見直しは定期監査の後に実施し、委員長は見直しの結果を個人情報保護管理責任者に指示する。

ｃ．個人情報保護管理責任者は、委員長の指示に基づき、必要な作業を実施する。

８．罰　則

本規程に故意又は過失によって違反した役員及び職員は、就業規則に基づき解雇を含む懲戒の対象となる。

９．その他

①　本規程は、平成１７年　月　日より施行する。

②　本規程の運用に必要な細則は、別に定める。

＜外部委託先との秘密保持に関する覚書＞

個人情報の秘密保持に関する覚書

○○○○協同組合（以下「甲」という。）と＿＿＿＿＿＿＿＿＿＿（以下「乙」という。） とは、業務委託契約書（以下「契約書」という。）に基づく、○○・○○・○○業務及びこれに付随する業務における個人情報の秘密保持に関し、次のとおり覚書を締結する。

（個人情報の秘密保持）

第１条　乙は、本件業務の遂行及び契約の履行に関して知り得た個人情報(※氏名、生年月日その他個人を特定できる項目を具体的に列挙する。）を契約期間中のみならず、基本契約解除後も複製、第三者に開示、漏えいし、本件業務の遂行以外のいかなる目的にも使用してはならない。

（業務遂行と管理業務）

第２条　乙は、本件業務の遂行に当たり、甲乙両者間で定められた個人情報に係る処理方法を遵守し、十分な配慮をもってこれを管理するとともに、迅速、かつ、誠実にこれを遂行するものとする。

２　乙は、甲より提供を受けた個人情報への不当なアクセス又は個人情報の紛失、破壊、改ざん、漏えい等の危険に対して、技術面及び組織面において合理的な安全対策を講じるものとする。

３　乙は、甲より提供を受けた個人情報について、本件業務の終了後、業務内容に定められた期間保管し、期間満了後には責任をもって削除を行うものとする。

（個人情報の開示･訂正･削除請求への対応）

第３条　乙は、情報主体である本人から、自己（本人）に関する情報開示の請求があった場合は、速やかに甲に報告しなければならない。

２　乙は、本人であることを確認したうえで、原則として可能な限りこれに応じるものとする。

３　乙は、個人情報に誤りがあって、情報主体である本人より訂正又は削除の請求を受けた場合は、速やかに甲に報告するとともに、遅滞なくその請求に応じるものとする。

（損害賠償等）

第４条　乙は、甲より提供を受けた個人情報への不当なアクセス又は個人情報の紛失、破壊、改ざん、漏えい等の事故が発生した場合は、速やかに甲に報告しなければな

らない。
2　甲及び乙は、第１項の個人情報への不当アクセス又は個人情報の紛失、破壊、改ざん、漏えい等の事故が発生した場合は、その原因について協議し、調査を行い、損害の拡大防止に必要な措置を講じるものとする。
3　前項の事故が乙の責に帰すべきものであると認められた場合は、乙は、事故調査、損害の拡大を防止するために講じた措置に要する合理的費用（損害賠償金を含む。）の負担を負うものとする。なお、当該求償権の行使は、甲の乙に対する損害賠償請求権の行使を妨げるものではない。
4　第１項の事故が乙の本覚書の違反に起因する場合は、乙は、前３項のほか、当該事故の拡大防止や収集のために必要な措置について、別途、甲からの指示に従うものとする。

（関係者への遵守徹底）
第５条　乙は、個人情報を知り得る可能性のある乙の従業員に、本覚書の内容を周知徹底のうえ、遵守させるものとする。

本覚書締結の証として本書２通を作成し、甲乙記名押印のうえ、各１通を保有する。

平成〇年〇月〇日

（甲）
〒〇〇〇－〇〇〇〇　東京都〇〇区××
×××協同組合
代表理事　△△△　△△

（乙）
〒〇〇〇－〇〇〇〇　東京都〇〇区××
×××株式会社
代表取締役　△△△　△△

第５章　個人情報保護に関する主なＵＲＬ

ここでは、個人情報保護に関して、組合等中小企業連携組織が参考となるＷｅｂサイトのＵＲＬを紹介します。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

平成１７年５月６日現在

○　首相官邸　個人情報の保護に関する法律
　http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

○　総務省　行政機関等個人情報保護法
　http://www.soumu.go.jp/gyoukan/kanri/kenkyu.htm

○　内閣官房情報セキュリティ対策推進室
　http://www.bits.go.jp/

○　警察庁　ハイテク犯罪対策
　http://www.npa.go.jp/cyber/

○　経済産業省　情報セキュリティに関する政策、緊急情報
　http://www.meti.go.jp/policy/netsecurity/

○　独立行政法人情報処理推進機構（ＩＰＡ）セキュリティセンター
　http://www.ipa.go.jp/security/

○　独立行政法人通信総合研究所　非常時通信グループ　不正アクセス関連情報
　http://www2.nict.go.jp/jt/a114/incident_top.html

○　財団法人日本情報処理開発協会　セキュリティ対策室
　http://www.jipdec.jp/security/security.html

○　財団法人日本情報処理開発協会　プライバシーマーク制度
　http://www.privacymark.jp/

○　財団法人日本規格協会
　　http://www.jsa.or.jp/

○　財団法人ニューメディア開発協会
　　個人情報保護とプライバシー情報管理システム
　　http://www.nmda.or.jp/enc/privacy/index.html

○　財団法人インタネット協会
　　電子ネットワーク運営における「個人情報保護に関するガイドライン」
　　http://www.iajapan.org/privacy/

○　財団法人日本データ通信協会　「個人情報保護登録センター」
　　http://www.dekyo.or.jp/hogo/center.htm

○　特定非営利活動法人日本ネットワークセキュリティ協会
　　http://www.jnsa.org/

○　個人情報ドットコム
　　http://www.kojinjoho.com/