# 個人情報リスク管理規定

～ 目 次 ～

# 1. 個人情報の特定

事業の用に供している個人情報が、どこに、どんな状態であるか、すべての個人情報を調査し洗い出す。これには、番号利用法の定める特定個人情報等を含む。
洗い出された個人情報を適正化し、管理する個人情報を**「個人情報管理台帳」**に特定する。これらの手順を次に示す。

## 1) 個人情報の調査(洗い出し)

個人情報の洗い出し(PMS構築時、新たな業務開始時、業務の変更時等)
事業の用に供している個人情報を下記の手順で調査し洗い出す。
<洗い出し手順>

(1) 部門又は業務(洗い出しの単位)毎に取りまとめ者(部門又は業務個人情報責任者)を置く。
(2) 下記の点に留意し個人情報を洗い出す
① 従業者全員(役員、理事、監査役、社員、契約社員、嘱託社員、パート社員、アルバイト社員、派遣社員等)を対象とする。
② 業務が各部門を横断して行われる等、個人情報の取扱いが複雑な場合、業務フローを作成して、取扱っている個人情報を洗い出す。
③ この際、連絡メモ等、担当者間の連絡に利用され、すぐに不要となるものは、速やかに廃棄、または消去することを条件に、また、請求書、領収書等の利用目的が明らかで、所属、氏名程度のみである場合は、この洗い出し作業から除くことができる。他に、同等のものがあった場合は、個人情報管理責任者の判断による。

## 2) 個人情報の取扱いの適正化

取りまとめ者(部門又は業務個人情報責任者)は、洗い出された個人情報に対して、JIS Q 15001規格の要求事項とのギャップを分析し、適正な取扱いに改める。その結果を個人情報管理台帳に記入し、個人情報管理責任者に報告する。

(1) 利用目的及び取得内容(項目)を特定する(A.3.4.2.1 利用目的の特定)

取りまとめ者は、洗い出された個人情報に対して、利用目的及び取得内容(項目)を特定する。利用目的の特定に当っては、抽象的、一般的な表現でなく、本人が何に利用されるかが具体的に分かるように特定する。また、取得内容(項目)は、特定された利用目的の達成に必要のない過度なものまで取得していないかを検討し、過度なものがあれば削除する。その結果を個人情報管理台帳の**「利用目的」**及び**「取得内容(項目)」**欄に登録する。尚、マイナンバーの利用目的は、番号利用法の定める利用目的以外に利用してはならない。

(2) 適正な取得方法を決める(A.3.4.2.2 適正な取得)

洗い出された個人情報は、法令、国が定める指針、及びその他の規範を特定した「外部文書一覧表(法令・指針・規範等)」に違反した取得をしていないか、また、第三者が不正に入手した個人情報の取得、利用目的を通知しないで取得、嘘、偽り、誤解を生むような表現を使用しての不正な取得、強要・不正取得を指示する等の不正な取得をしていないかを確認する。不正な取得があった場合、取得をとり止め、適正な取得をしているものを個人情報管理台帳に登録する。

（3） 要配慮個人情報の取得を制限する（A.3.4.2.3 要配慮個人情報）

取得内容の中に、要配慮個人情報の有無を確認する。取得の必要がある場合、あらかじめ本人に明示し、書面による同意を得た上で行う。これら明示し、同意を得たもの、及び「個人情報新規取り扱い申請書」で承認された個人情報に関して、個人情報管理台帳の「取得内容（項目）」欄に記入し、要配慮個人情報が含まれることは符号をつける等で識別する。運用に伴って取扱う必要が生じた場合（例：人の生命に係る場合で、要配慮個人情報を取扱う必要が生じた場合等）は、「個人情報新規取り扱い申請書」で個人情報管理責任者の承認を得た上で行う。

（4） 個人情報取得時の明示・通知・公表、及び同意の方法を明確にする

個人情報を取得する方法を個人情報管理台帳の「取得方法」欄に登録する。この取得方法に対応した明示・通知・同意・公表、及び同意方法を個人情報管理台帳の「明示・通知・公表、同意方法」欄に登録する。（参照：「A.3.4.2.4 個人情報を取得した場合の措置」、「A.3.4.2.5 上記 A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置」）

（5） 利用に関しての取扱いを明確にする（A.3.4.2.6 利用に関する措置）

個人情報管理責任者は、個人情報管理台帳の「利用目的」欄に特定された利用目的を明示、通知し、同意を得る等の際に使用する案内文「個人情報の取扱い及び同意書」等に定める。これを取得時の明示や通知及び同意を得る際に使用する。この案内文は、業務毎の個人情報管理規程に添付する。また、当社が取扱う個人情報は、「個人情報の取扱いについて」公表する。ここに特定された利用目的、及び取得内容の範囲を超えて、利用及び取得してはならない（参照：「個人情報保護基本規程 A.3.4.2.6 利用に関する措置」）。マイナンバーに関しては、番号利用法の定める提供先にしか提供してはならない。また、本人の同意があっても提供することはできない。

（6） 本人に連絡又は接触する場合の処置を明確にする

個人情報を利用して、本人に連絡又は接触する場合、取得方法（本人から直接書面にて取得した場合、口頭や第三者等から取得した場合）によっては、「即時連絡又は接触する場合」と改めて明示し、同意を必要とする場合がある。これら連絡又は接触する場合の措置について、適正な方法を個人情報管理台帳「本人への連絡又は接触」欄に記入する。また、業務別の個人情報管理規定に定める。（参照：「A.3.4.2.7 本人に連絡又は接触する場合の措置」）

（7） 提供に関しての措置を明確にする

個人データの第三者への提供及び外国にある第三者への提供について、提供、委託、共同利用等の有無や有の場合、適切な提供先を個人情報管理台帳の「提供」欄に記入する。マイナンバーに関しては、番号利用法の定める提供先にしか提供してはならない。また、本人の同意があっても提供することはできない。（参照：「A.3.4.2.8.1 外国にある第三者への提供の制限」）

（8） 匿名加工情報を明確にする

当社は、匿名加工情報は取り扱わない。

（9） 保有個人データを明確にする

個人情報管理台帳に登録された個人情報が保有個人データに該当するか否かを確認し、該当するものを「保有個人データ」欄に特定する。（参照：「A.3.4.4.1 個人情報に関する権利」）

（10）管理者、保存・廃棄方法等を明確にする

個人情報の管理部門・責任者、個人情報へのアクセス権限、保管形態、保管場所、保管方法、保存期間、利用期限、バックアップ、及び廃棄方法について、「個人情報管理台帳」の「保管・廃棄」欄に登録する。マイナンバーは、番号利用法の定める保存期間とする。

## 3) 個人情報の特定（個人情報管理台帳の作成と維持）

洗い出された個人情報に対して、上記手順で適正化し、今後、管理すべき個人情報、管理すべき項目を**「個人情報管理台帳」**に特定する。

また、適正化によって必要となった新たな個人情報（例：個人情報取扱い案内及び同意書等）、及びリスク対策で必要となった新たな個人情報（例：お客様来社記録等）についても同様に個人情報管理台帳に特定する。

特定された**「個人情報管理台帳」**は、個人情報管理責任者が承認する。

**「個人情報管理台帳」**は、次の時に見直しを行い、新規作成及び改定が必要であれば、4章（個人情報の新規・変更時の取扱い）により維持管理をする。

⑴ 新たに個人情報の取扱う業務を開始、又は現状の取扱いを変更する時

⑵ 関連する法令、国が定める指針、及びその他の規範が制定又は改廃された時

⑶ マネジメントレビュー時（参照：「マネジメントレビュー規定」）

## 2. リスク認識、分析及び対策

個人情報管理台帳に特定された個人情報の目的外利用を防止する手順、及び個人情報保護リスクを特定し、分析し、必要な対策を講じる手順を次に示す。

### 1) 目的外利用防止の手順

個人情報の目的外利用を防止するために以下の手順を講じる。

(1) 個人情報を利用する際は、この**「個人情報管理台帳」**、及び案内文「個人情報の取扱い及び同意書」等や公表文「個人情報の取扱いについて」に特定されている「利用目的」の範囲内で取扱う。これ以外の目的で利用したり、取得内容を超えて個人情報を取扱ってはならない。また、ここに特定されていない個人情報、及び利用目的を定められていない個人情報を取扱ってはならない。

(2) 利用目的が複数(例:配達時に利用する、新商品、新サービスの案内をする等)ある場合、同意を得られた利用目的でのみ取扱うように管理する(利用目的の管理)。

(3) 同意を得られた範囲外の目的で利用する必要が生じた場合、本人に「個人情報の利用目的変更のご案内」で通知し、同意を得てから行なう。

尚、マイナンバーは、番号利用法の定める利用目的にのみ利用でき、本人の同意があっても目的外に利用することはできない。また、マイナンバーを利用して、番号利用法の定める利用目的以外の特定個人情報ファイルを作成してはならない(例:社員管理のためにマイナンバーを利用したファイルを作成する等)。

個人情報管理責任者は、これを従業者に周知し、従業者はこれを順守しなければならない。

### 2) 個人情報保護リスクの特定、分析、対策を講じる手順

特定された個人情報について、個人情報保護リスクを特定し、分析し、対策を講じる手順を以下に示す。

(1) 個人情報の取扱い方を特定する

特定された個人情報毎に、取得・入力から消去・廃棄に至る局面で、個人情報をどのように取扱っているかを特定する。取扱いの内容を、各局面別に**「リスク対策一覧表」**の「局面」、「取扱い内容」に、また取扱っている担当を「部門」欄に記入する。

その個人情報が記録されている媒体(紙媒体、電子媒体)を「媒体」欄に記入する。

これらは、**「個人情報管理台帳」**に特定された個人情報毎に行うが、取扱う局面、取扱い内容、媒体が同じで、同じリスクが想定され、結果的に対策が同じになる場合は、一つのリスク対策一覧表にまとめて記入することができる(グループ化)。

尚、局面は次の通りとする(他の表現も可)。

① 取得・入力

個人情報を本人から直接または間接的に入手することを取得するという。また、個人情報を利用・加工するためにPCに入力したり、紙媒体に書きこんだりすることを入力という。

② 移送・送信

取得した個人情報を、紙媒体、電子媒体で運搬、郵送、宅配便等によって、また、通信回線（e メール等）を利用して送ったり、受け取ったりすることをいう。

③ 利用・加工

個人情報を、利用目的に従って利用する（例：個人情報を利用して、新商品の案内をする）。利用しやすいように加工する（例：申込者一覧表から地域別一覧表を作成する等）。他の情報との結合する（例：今回の参加者と今までの参加者を合わせる）等のことをいう。

④ 保管・バックアップ

保管は、作業中断時の一時保管、ある期間利用しない時の保管（例：月 1 回しか利用しない間の保管）、ある期間（例：3 年）に渡って個人情報を維持するために保管することをいう。バックアップは、ハードウエアの破壊、消磁、劣化、損傷、盗難、またはデータの改ざん、消去、不正コピー等によって発生する個人情報の劣化、損傷、紛失が起きた際の原状回復をする手段（複製）のことをいう。

⑤ 消去・廃棄

個人情報の利用目的を達成した個人情報や保管期間を過ぎた個人情報を、PC、サーバから消去したりする等、紙媒体や電子媒体を電子的に、また物理的に読めなくすることを廃棄という。

(2) 個人情報保護リスクを特定し、分析し、対策を講じる

① 個人情報保護リスクを特定し、分析、対策を行う

- 個人情報を取扱う各局面で、個人情報に対する脅威とぜい弱性を考慮し、どのようなリスクがあるかを想定する（例：取得時のリスク―利用目的を案内しないで取得し法律違反となる、授受ミス等。持ち運び時のリスク―PC の紛失、盗難、漏えい等。利用時のリスク：不正アクセス、改ざん、ウィルス感染等）。
  想定されるリスクを**「リスク対策一覧表」の「想定リスク」欄**に記入する。
- 想定されたリスクに対して、現状の対策ではリスクが現実となり、本人への影響や会社への経済的な不利益、社会的な信用失墜等を与える可能性があるかを評価し、現状の対策では不十分な場合、組織的対策、人的対策、物理的対策、技術的対策を考慮して、経済的に実行可能なリスク対策を講じる。リスク対策の内容を、**「リスク対策一覧表」の「対策内容」欄**に記入する。
- 費用面ですぐに実施できない対策は、PMS 年間計画書に記入し、確実に実施できるように管理する。

② 対策を規定化する

講じた対策を確実に実施するために規定化する。規定の名称を「規定」欄に記入する。

(3) 残留リスクの把握と管理

リスク対策を実施する必要があっても、費用面や効率面で対策をすぐに実施できない、又は対策が不十分にならざるを得ない場合がある。このような場合、現状で取り得る対策を講じた上で、まだ残っているリスクを残留リスクとして特定し、認識する。これらの残留リスクを「リスク対策一覧表」の「残留リスク」欄に記入する。日常業務に当って、これらが顕在化しないように、残留リスクを十分認識し業務にあたるとともに、監督、点検（運用確認、内部監査）を行う。

### 3) リスク対策一覧表の作成と維持

最終的に定まったリスク対策は、**「リスク対策一覧表」**として、社長が承認する。また、次の時に見直しを行い、新規作成及び改定が必要であれば、4 章（個人情報の新規・変更時の取扱い）により、維持管理をする。

(1) 新たに個人情報の取扱う業務を開始、又は現状の取扱いを変更する時
(2) 関連する法令、国が定める指針、及びその他の規範が制定又は改正され、個人情報の取扱いに変更を及ぼす時
(3) 是正処置が実施され、リスク対策が変更される時
(4) 技術の進歩や環境の変化によって、リスク対策が変更される時
(5) マネジメントレビューを行う時（参照:「マネジメントレビュー規定」）

## 3. 業務別個人情報管理規定の作成と維持

個人情報を取扱う業務に関して、適正な取扱いを定めた業務別の**個人情報管理規定**を作成する（例:受託業務個人情報管理規定、取引先個人情報管理規定、従業者個人情報管理規定等）。

業務別の個人情報管理規定には、下記の内容を含める。

１．目的
　個人情報の利用目的、及び規定の作成目的を明確にする。
２．責任と権限
　本規定に係る者の責任と権限を明確にする。
３．適用業務及び適用範囲
　本規定が適用される業務内容と規定の適用範囲を明確にする。
４．個人情報の取得
　個人情報の取得にあたって、どのように明示、通知、公表するか、また必要な同意を得るかを明確にする。
５．個人情報の利用と提供
　取得した個人情報をどのように利用・提供するかを明確にする。また、利用目的、取得内容の範囲内で行うことを明確にする。
６．個人情報の適正管理
　個人情報の正確性の確保、安全性の確保、従業者の監督、委託する場合の措置を明確にする。
７．個人情報に関する本人の権利
　保有個人データに対して、本人から利用目的の通知、開示、訂正・追加、削除、利用停止、消去及び第三者への提供停止の要求があった場合の手順、手続きを明確にする。
８．苦情及び相談への対応
　個人情報に関する苦情・相談があった場合の窓口及びその対応手順を明確にする。

本規定の見直しは「リスク対策一覧表」の見直しと同じ要領で行い、発行は**文書・記録管理規定**によって行う。

## 4. 個人情報の新規・変更時の扱い

1) PMS の運用後、新たな個人情報を取扱う業務が生じた場合、業務開始前に個人情報の取扱いを、1～2章に沿って、個人情報を**「個人情報管理台帳」**に特定し、リスク対策を**「リスク対策一覧表」**で行い、3 章の業務別の「個人情報管理規定（案）」を作成する。作成後、**「個人情報新規取り扱い申請書」**により、許可願いを個人情報管理責任者に申請し、承認後、**「PP-C-002 文書・記録管理規定」**によって関連する個人情報管理規定を発行し、業務を開始する。

2) 現行の個人情報の取扱いに変更の必要性が生じた場合、変更部分に対して、上記と同様な検討を行い、既存部分と調整をした上で、個人情報管理規定を改定し、**「個人情報新規取り扱い申請書」**により個人情報管理責任者の承認後、**「PP-C-002 文書・記録管理規定」**によって関連する個人情報管理規定を発行し、業務を開始する。

以上