個人情報保護規程

文書番号	PA01
版数	第 1 版
発行者	個人情報保護管理者
制定日	2023 年 12 月 1 日
最終改訂日	2023 年 12 月 1 日
承認者	理事長　服部　一史

改訂履歴

改訂日	版数	内容	承認	作成
2023 年 12 月 1 日	1.0	新規制定	服部 一史	大丸 一

目　次

個人情報保護規程（基本文） 1
目的 1
１．　適用範囲 1
２．　引用規格 1
３．　用語及び定義 1
３．１ 組織 1
３．２ 利害関係者 1
３．３ 要求事項 1
３．４ マネジメントシステム 1
３．５ トップマネジメント 1
３．６ 有効性 1
３．７ 方針 1
３．８ 目的 2
３．９ リスク 2
３．１０ 力量 2
３．１１ 文書化した情報 2
３．１２ プロセス 2
３．１３ パフォーマンス 2
３．１４ 監視 2
３．１５ 測定 2
３．１６ 監査 2
３．１７ 適合 2
３．１８ 不適合 2
３．１９ 是正処置 2
３．２０ 継続的改善 3
３．２１ 分析モデル 3
３．２２ 属性 3
３．２３ 基本測定量 3
３．２４ 結果 3
３．２５ 管理策 3
３．２６ 判断基準 3
３．２７ 導出測定量 3
３．２８ 事象 3
３．２９ 起こりやすさ 3
３．３０ 測定量 3

３．３１ 測定の関数. 3
３．３２ 測定方法 4
３．３３ 対象物 4
３．３４ 尺度 4
３．３５ 脅威 4
３．３６ ぜい弱性 4
３．３７ 残留リスク. 4
３．３８ リスク対応. 4
３．３９ 本人 4
３．４０ 個人情報保護管理者. 4
３．４１ 個人情報保護監査責任者. 4
３．４２ 従業者 4
３．４３ 個人情報保護リスク. 5
３．４４ 緊急事態 5
３．４５ 個人情報保護. 5
３．４６ リスク所有者. 5
４． 組織の状況 5
４．１ 組織及びその状況の理解（J.1.1）. 5
４．２ 利害関係者のニーズ及び期待の理解（J.1.2）. 5
４．３ 個人情報保護マネジメントシステムの適用範囲の決定（J.1.4）. 5
４．４ 個人情報保護マネジメントシステム（J.1.5）. 6
５． リーダーシップ 6
５．１ リーダーシップ及びコミットメント（J.2.1）. 6
５．２ 方針 6
５．２．１ 内部向け個人情報保護方針（J.2.2） 6
５．２．２ 外部向け個人情報保護方針（J.2.2） 6
５．３ 組織の役割、責任及び権限（J.2.3.1）. 7
６． 計画 7
６．１ リスク及び機会に対処する活動. 7
６．１．１ 一般（J.3.1.2） 7
６．１．２ 個人情報保護リスクアセスメント 7
６．１．３ 個人情報保護リスク対応(J.3.1.4) 8
６．２ 個人情報保護目的及びそれを達成するための計画策定(J.3.2) 8
７ 支援 8
７．１ 資源(J.4.1) 8
７．２ 力量(J.4.2) 9

７．３ 認識(J.4.3) 9
７．４ コミュニケーション(J.4.4.1) 9
７．５ 文書化した情報 9
７．５．１ 一般(J.4.5.1) 9
７．５．２ 作成及び更新(J.4.5.3) 9
７．５．３ 文書化した情報の管理(J.4.5.2) 9
８ 運用 10
８．１ 運用の計画及び管理(J.5.1) 10
８．２ 個人情報保護リスクアセスメント 10
８．３ 個人情報保護リスク対応 10
９ パフォーマンス評価 10
９．１ 監視、測定、分析及び評価（J.6.1） 10
９．２ 内部監査（J.6.2） 11
９．３ マネジメントレビュー（J.6.3） 11
１０ 改善 12
１０．１ 不適合及び是正処置(J.7.1) 12
１０．２ 継続的改善(J.7.2) 12
個人情報保護規程（付属書Ａ） 13
A.3 管理目的及び管理策 13
A.3.1 一般 13
A.3.1.1 一般(J.2.4) 13
A.3.2 個人情報保護方針 13
A.3.2.1 内部向け個人情報保護方針(J.2.2) 13
A.3.2.2 外部向け個人情報保護方針(J.2.2) 13
A.3.3 計画 14
A.3.3.1 個人情報の特定(J.3.1.1) 14
A.3.3.2 法令、国が定める指針その他の規範(J.1.3) 14
A.3.3.3 リスクアセスメント及びリスク対策(J.3.1.3、J.3.1.4) 14
A.3.3.4 資源、役割、責任及び権限(J.2.3.2) 15
A.3.3.5 内部規程(J.4.5.4、J.8.8.4、J.8.10) 16
A.3.3.6 計画策定(J.3.3) 17
A.3.3.7 緊急事態への準備(J.4.4.2、J.8.10) 17
A.3.4 実施及び運用 21
A.3.4.1 運用手順(J.5.1) 21
A.3.4.2 取得、利用及び提供に関する原則 21
A.3.4.2.1 利用目的の特定(J.8.1、J.8.10) 21

A.3.4.2.2 適正な取得(J.8.2) 21
A.3.4.2.3 要配慮個人情報(J.8.3) 21
A.3.4.2.4 個人情報を取得した場合の措置(J.8.4) 22
A.3.4.2.5 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(J.8.5) 23
A.3.4.2.6 利用に関する措置(J.8.6、J.8.10) 24
A.3.4.2.7 本人に連絡又は接触する場合の措置(J.8.7) 25
A.3.4.2.8 個人データの提供に関する措置(J.8.8、J.8.8.4、J.8.10) 26
A.3.4.2.8.1 外国にある第三者への提供の制限(J.8.8.1) 28
A.3.4.2.8.2 第三者提供に係る記録の作成など(J.8.8.2) 29
A.3.4.2.8.3 第三者提供を受ける際の確認など(J.8.8.3) 30
A.3.4.2.9 匿名加工情報(J.8.9) 31
A.3.4.3 適正管理 31
A.3.4.3.1 正確性の確保(J.9.1) 31
A.3.4.3.2 安全管理措置(J.8.10、J.9.2) 31
A.3.4.3.3 従業者の監督(J.9.3) 40
A.3.4.3.4 委託先の監督(J.9.4) 41
A.3.4.4 個人情報に関する本人の権利 42
A.3.4.4.1 個人情報に関する権利(J.10.1) 42
A.3.4.4.2 開示等の請求等に応じる手続(J.10.2) 42
A.3.4.4.3 保有個人データに関する事項の周知など(J.10.3) 43
A.3.4.4.4 保有個人データの利用目的の通知(J.10.4) 44
A.3.4.4.5 保有個人データの開示(J.10.5) 44
A.3.4.4.6 保有個人データの訂正、追加又は削除(J.10.6) 45
A.3.4.4.7 保有個人データの利用又は提供の拒否権(J.10.7) 46
A.3.4.5 認識(J.4.3) 46
A.3.5 文書化した情報 47
A.3.5.1 文書化した情報の範囲(J.4.5.1) 47
A.3.5.2 文書化した情報（記録を除く。）の管理(J.4.5.3) 47
A.3.5.3 文書化した情報のうち記録の管理(J.4.5.5) 48
A.3.6 苦情及び相談への対応(J.8.10、J.11.1) 48
A.3.7 パフォーマンス評価 49
A.3.7.1 運用の確認(J.6.1) 49
A.3.7.2 内部監査(J.6.2) 49
A.3.7.3 マネジメントレビュー(J.6.3) 50
A.3.8 是正処置(J.7.1) 51

個人情報保護規程（基本文）

目的

本規程は、業務上取扱う個人情報の適切な使用と保護のため、日本産業規格 JISQ15001:2017「個人情報保護マネジメントシステムー要求事項」に合致した個人情報保護マネジメントシステムを策定し、実施し、維持し、及び改善するために必要な基本的事項を定めることを目的とする。

１． 適用範囲

この規程は、財団が、自らの事業の用に供している個人情報に関する、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、改善するための要求事項について規定する。

２． 引用規格

この規程が引用する規格はない。

３． 用語及び定義

この規程で用いる主な用語及び定義は、個人情報保護法による。その他の主な用語及び定義は、次による。

３．１ 組織

責任及び権限をもつトップマネジメントが存在し、自らの目的（ 3.8）を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。

３．２ 利害関係者

ある決定事項若しくは活動に影響を与え得るか、その影響を受け得るか、又はその影響を受けると認識している、個人又は組織（ 3.1)。(JIS Q 27000:2014 の 2.41 参照)

３．３ 要求事項

明示されている、通常暗黙のうちに了解されている又は義務として要求されている、ニーズ又は期待。(JIS Q 27000:2014 の 2.63 参照)

３．４ マネジメントシステム

方針（ 3.7)、目的（ 3.8）及びその目的を達成するためのプロセス（ 3.12）を確立するための、相互に関連する又は相互に作用する、組織（ 3.1）の一連の要素。

３．５ トップマネジメント

最高位で組織（ 3.1）を指揮し、管理する個人又は人々の集まり。

３．６ 有効性

計画した活動を実行し、計画した結果を達成した程度。(JIS Q 27000:2014 の 2.24 参照)

３．７ 方針

トップマネジメント（ 3.5）によって正式に表明された組織（ 3.1）の意図及び方向付け。(JIS Q

27000:2014 の 2.60 参照）

３．８ 目的

達成する結果。

３．９ リスク

目的に対する不確かさの影響。

３．１０ 力量

意図した結果を達成するために、知識及び技能を適用する能力。（ JIS Q 27000:2014 の 2.11 参照）

３．１１ 文書化した情報

組織（ 3.1） によって、 管理及び維持されるように要求されている情報、 並びにそれが含まれている媒体。（ JIS Q 27000:2014 の 2.23 参照）

３．１２ プロセス

インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動。（ JIS Q 27000:2014 の 2.61 参照）

３．１３ パフォーマンス

測定可能な結果。（ JIS Q 27000:2014 の 2.59 参照）

３．１４ 監視

システム、プロセス（ 3.12）又は活動の状況を明確にすること。（ JIS Q 27000:2014 の 2.52 参照）

３．１５ 測定

値を決定するためのプロセス（ 3.12)。

３．１６ 監査

監査基準が満たされている程度を判定するために、 監査証拠を収集し、 それを客観的に評価するための、体系的で、独立し、文書化したプロセス（ 3.12)。（ JIS Q 27000:2014 の 2.5 参照）

３．１７ 適合

要求事項（ 3.3）を満たしていること。（ JIS Q 27000:2014 の 2.13 参照）

３．１８ 不適合

要求事項（ 3.3）を満たしていないこと。（ JIS Q 27000:2014 の 2.53 参照）

３．１９ 是正処置

不適合（ 3.18）の原因を除去し、再発を防止するための処置。（ JIS Q 27000:2014 の 2.19 参照）

３．２０ 継続的改善

パフォーマンス（ 3.13）を向上するために繰り返し行われる活動。（ JIS Q 27000:2014 の 2.15 参照）

３．２１ 分析モデル

一つ以上の基本測定量（ 3.23）及び／又は導出測定量（ 3.27）をそれに関連する判断基準と結合するアルゴリズム又は計算。

３．２２ 属性

人手又は自動的な手段によって、定量的又は定性的に識別できる対象物（ 3.33）の特性又は特徴。（ JIS Q 27000:2014 の 2.4 参照）

３．２３ 基本測定量

単一の属性（ 3.22）とそれを定量化するための方法とで定義した測定量（ 3.30）。（ JIS Q 27000:2014 の 2.10 参照）

３．２４ 結果

目的（ 3.8）に影響を与える事象（ 3.28）の結末。（ JIS Q 27000:2014 の 2.14 参照）

３．２５ 管理策

リスク（ 3.9）を修正する対策。（ JIS Q 27000:2014 の 2.16 参照）

３．２６ 判断基準

アクション若しくは追加調査の必要性を決めるため又は与えられた結果の信頼度のレベルを記述するために使う、しきい（閾）値、目標又はパターン。（ JIS Q 27000:2014 の 2.21 参照）

３．２７ 導出測定量

複数の基本測定量（ 3.23）の値の関数として定義した測定量（ 3.30）。（ JIS Q 27000:2014 の 2.22 参照）

３．２８ 事象

ある特有な状況の出現又は変化。（ JIS Q 27000:2014 の 2.25 参照）

３．２９ 起こりやすさ

何かが起こる見込み。（ JIS Q 27000:2014 の 2.45 参照）

３．３０ 測定量

測定（ 3.15）の結果として値が割り当てられる変数。（ JIS Q 27000:2014 の 2.47 参照）

３．３１ 測定の関数

複数の基本測定量（ 3.23）を結合するために遂行するアルゴリズム又は計算。（ JIS Q 27000:2014 の 2.49 参照）

３．３２ 測定方法

特定の尺度（ 3.34）に関して属性（ 3.22）を定量化するために使う一連の操作の論理的な順序を一般的に記述したもの。（ JIS Q 27000:2014 の 2.50 参照）

３．３３ 対象物

属性（ 3.22）の測定（ 3.15）を通して特徴付けられるもの。（ JIS Q 27000:2014 の 2.55 参照）

３．３４ 尺度

連続的若しくは離散的な値の順序集合又は分類の集合で、それに属性（ 3.22）を対応付けるもの。（ JIS Q 27000:2014 の 2.80 参照）

３．３５ 脅威

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。（ JIS Q 27000:2014 の 2.83 参照）

３．３６ ぜい弱性

一つ以上の脅威（ 3.35）によって付け込まれる可能性のある、資産又は管理策（ 3.25）の弱点。（ JIS Q 27000:2014 の 2.89 参照）

３．３７ 残留リスク

リスク対応（ 3.38）後に残っているリスク（ 3.9)。（ JIS Q 27000:2014 の 2.64 参照）

３．３８ リスク対応

リスク（ 3.9）を修正するプロセス（ 3.12)。（ JIS Q 27000:2014 の 2.79 参照)。

３．３９ 本人

個人情報によって識別される特定の個人。

３．４０ 個人情報保護管理者

トップマネジメントによって組織内部に属する者の中から指名された者であって、個人情報保護マネジメントシステムの計画及び運用に関する責任及び権限をもつ者。

３．４１ 個人情報保護監査責任者

トップマネジメントによって組織内部に属する者の中から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責任及び権限をもつ者。

３．４２ 従業者

個人情報取扱事業者の組織内にあって直接間接に組織の指揮監督を受けて組織の業務に従事してい

る者などをいい、雇用関係にある職員（職員、期限付職員、非常勤職員、契約非常勤職員、短期臨時職員など）だけでなく、雇用関係にない従事者（理事、監事、評議員、派遣職員など）も含まれる。

３．４３ 個人情報保護リスク

個人情報の取扱いの各局面（個人情報の取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄に至る個人情報の取扱いの一連の流れ）における、個人情報の漏えい、滅失又はき損、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、本人の権利利益の侵害など、好ましくない影響。

３．４４ 緊急事態

個人情報保護リスク（ 3.43）の脅威（ 3.35）が顕在化した状況。

３．４５ 個人情報保護

組織が、自らの事業の用に供する個人情報について、その有用性及び個人の権利利益に配慮しつつ、保護すること。

３．４６ リスク所有者

リスク（ 3.9）を運用管理することについて、アカウンタビリティ及び権限をもつ人又は主体。

４． 組織の状況

４．１ 組織及びその状況の理解（J.1.1）

財団は、組織の目的に関連し、かつ、その個人情報保護マネジメントシステムの意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を決定する。

４．２ 利害関係者のニーズ及び期待の理解（J.1.2）

財団は、次の事項を決定する。

a） 個人情報保護マネジメントシステムに関連する利害関係者

b） その利害関係者の、個人情報保護に関連する要求事項

４．３ 個人情報保護マネジメントシステムの適用範囲の決定（J.1.4）

財団は、個人情報保護マネジメントシステムの適用範囲を定めるために、その境界及び適用可能性を決定する。

この適用範囲を決定するとき、財団は、次の事項を考慮する。

a） 4.1 に規定する外部及び内部の課題

b） 4.2 に規定する要求事項

c） 財団が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係

個人情報保護マネジメントシステムの適用範囲は、文書化した情報として利用可能な状態にしておく。

カテゴリー	対　象
組織	公益財団法人堺市文化振興財団
所在地	全ての事業拠点

対象個人情報	事業の用に供する全ての個人情報 ※「個人情報管理台帳」にて別途定義
技術	自社管理システム全般

４．４ 個人情報保護マネジメントシステム（J.1.5）

財団は、JISQ15001 の要求事項に従って、 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、継続的に改善する。

５． リーダーシップ

５．１ リーダーシップ及びコミットメント（J.2.1）

トップマネジメントは、次に示す事項によって、個人情報保護マネジメントシステムに関するリーダーシップ及びコミットメントを実証しなければならない。

a) 内部向け個人情報保護方針及び個人情報保護目的を確立し、それらが財団の戦略的な方向性と両立することを確実にする。

b) 財団のプロセスへの個人情報保護マネジメントシステム要求事項の統合を確実にする。

c) 個人情報保護マネジメントシステムに必要な資源が利用可能であることを確実にする。

d) 有効な個人情報保護マネジメント及び個人情報保護マネジメントシステム要求事項への適合の重要性を利害関係者に伝達する。

e) 個人情報保護マネジメントシステムがその意図した成果を達成することを確実にする。

f) 個人情報保護マネジメントシステムの有効性に寄与するよう人々を指揮し、支援する。

g) 継続的改善を促進する。

h) その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する。

５．２ 方針

５．２．１ 内部向け個人情報保護方針（J.2.2）

トップマネジメントは、次の事項を満たす内部向け個人情報保護方針を確立しなければならない。

a) 組織の目的に対して適切である。

b) 個人情報保護目的（ 6.2 参照）を含むか、又は個人情報保護目的の設定のための枠組みを示す。

c) 個人情報保護に関連する適用される要求事項を満たすことへのコミットメントを含む。

d) 個人情報保護マネジメントシステムの継続的改善へのコミットメントを含む。

内部向け個人情報保護方針は、次に示す事項を満たさなければならない。

e) 文書化した情報として利用可能である。

f) 組織内に伝達する。

g) 必要に応じて、利害関係者が入手可能である。

５．２．２ 外部向け個人情報保護方針（J.2.2）

トップマネジメントは、次の事項を満たす外部向け個人情報保護方針を文書化し、一般の人が知り得るようにしなければならない。

a）5.2.1 で確立した内部向け個人情報保護方針に対して矛盾しない。

５．３ 組織の役割、責任及び権限（J.2.3.1）

トップマネジメントは、個人情報保護に関連する役割に対して、責任及び権限を割り当て、利害関係者に伝達することを確実にしなければならない。

トップマネジメントは、次の事項に対して、責任及び権限を割り当てなければならない。

a） 個人情報保護マネジメントシステムが、JISQ15001 の要求事項に適合することを確実にする。

b） 個人情報保護マネジメントシステムのパフォーマンスをトップマネジメントに報告する。

６． 計画

６．１ リスク及び機会に対処する活動

６．１．１ 一般（J.3.1.2）

個人情報保護マネジメントシステムの計画を策定するとき、財団は、 4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し、 次の事項のために対処する必要があるリスク及び機会を決定する。

a）個人情報保護マネジメントシステムが、その意図した成果を達成できることを確実にする。

b）望ましくない影響を防止又は低減する。

c）継続的改善を達成する。

財団は、次の事項を計画する。

d）上記によって決定したリスク及び機会に対処する活動

e）次の事項を行う方法

1）その活動の個人情報保護マネジメントシステムプロセスへの統合及び実施

2）その活動の有効性の評価

６．１．２ 個人情報保護リスクアセスメント

財団は、 次の事項を行う個人情報保護リスクアセスメントのプロセスを定め、 適用する。

a）次を含む個人情報保護のリスク基準を確立し、維持する（J.3.1.3）。

1）リスク受容基準

2）個人情報保護リスクアセスメントを実施するための基準

b）繰り返し実施した個人情報保護リスクアセスメントに、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にする。

c）次によって個人情報保護リスクを特定する。

1）個人情報保護マネジメントシステムの適用範囲内における個人情報の不適切な取扱いに伴うリスクを特定するために、個人情報保護リスクアセスメントのプロセスを適用する。

2）これらのリスク所有者を特定する。

d）次によって個人情報保護リスクを分析する。

1）6.1.2 c） 1） で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。

2）6.1.2 c） 1） で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。

3）リスクレベル（リスクの大きさ）を決定する。

e）次によって個人情報保護リスクを評価する。

1）リスク分析の結果と 6.1.2 a） で確立したリスク基準とを比較する。

2）リスク対応のために、分析したリスクの優先順位付けを行う。

財団は、個人情報保護リスクアセスメントのプロセスについての文書化した情報を保持する。

６．１．３ 個人情報保護リスク対応(J.3.1.4)

財団は、 次の事項を行うために、 個人情報保護リスク対応のプロセスを定め、 適用する。

a)リスクアセスメントの結果を考慮して、適切な個人情報保護リスク対応の選択肢を選定する。

b）選定した個人情報保護リスク対応の選択肢の実施に必要な全ての管理策を決定する。

c）6.1.3 b） で決定した管理策を附属書 A に示す管理策と比較し、必要な管理策が見落とされていないことを検証する。

d）個人情報保護リスク対応計画を策定する。

e）個人情報保護リスク対応計画及び残留している個人情報保護リスクの受容について、リスク所有者の承認を得る。

財団は、個人情報保護リスク対応のプロセスについての文書化した情報を保持する。

６．２ 個人情報保護目的及びそれを達成するための計画策定(J.3.2)

財団は、関連する所属において、個人情報保護目的を確立する。

個人情報保護目的は、次の事項を満たさなければならない。

a）内部向け個人情報保護方針と整合している。

b）(実行可能な場合）測定可能である。

c）適用される個人情報保護要求事項、 並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。

d）伝達する。

e）必要に応じて、更新する。

財団は、個人情報保護目的に関する文書化した情報を保持する。

財団は、個人情報保護目的をどのように達成するかについて計画するとき、次の事項を決定する。

f）実施事項

g）必要な資源

h）責任者

i）達成期限

j）結果の評価方法

７ 支援

７．１ 資源(J.4.1)

財団は、 個人情報保護マネジメントシステムの確立、 実施、 維持及び継続的改善に必要な資源を決定し、提供する。

７．２ 力量(J.4.2)

財団は、次の事項を行う。

a) 財団の個人情報保護パフォーマンスに影響を与える業務をその管理下で行う人々に必要な力量を決定する。

b) 適切な教育、訓練又は経験に基づいて、それらの人々が力量を備えていることを確実にする。

c) 該当する場合には、必ず、必要な力量を身につけるための処置をとり、とった処置の有効性を評価する。

d) 力量の証拠として、適切な文書化した情報を保持する。

７．３ 認識(J.4.3)

財団の管理下で働く人々は、次の事項に関して認識をもたなければならない。

a) 内部向け個人情報保護方針及び外部向け個人情報保護方針

b) 個人情報保護パフォーマンスの向上によって得られる便益を含む、個人情報保護マネジメントシステムの有効性に対する自らの貢献

c) 個人情報保護マネジメントシステム要求事項に適合しないことの意味

７．４ コミュニケーション(J.4.4.1)

財団は、次の事項を含め、個人情報保護マネジメントシステムに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。

a) コミュニケーションの内容（何を伝達するか。）

b) コミュニケーションの実施時期

c) コミュニケーションの対象者

d) コミュニケーションの実施者

e) コミュニケーションの実施プロセス

７．５ 文書化した情報

７．５．１ 一般(J.4.5.1)

財団の個人情報保護マネジメントシステムは、次の事項を含める。

a) JISQ15001 が要求する文書化した情報

b) 個人情報保護マネジメントシステムの有効性のために必要であると組織が決定した、文書化した情報

７．５．２ 作成及び更新(J.4.5.3)

文書化した情報を作成及び更新する際、財団は、次の事項を確実にする。

a) 適切な識別及び記述（例えば、タイトル、日付、作成者、参照番号）

b) 適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）

c) 適切性及び妥当性に関する、適切なレビュー及び承認

７．５．３ 文書化した情報の管理(J.4.5.2)

個人情報保護マネジメントシステム及び JISQ15001 で要求されている文書化した情報は、次の事

項を確実にするために、管理しなければならない。

a）文書化した情報が、必要な時に、必要な所で、入手可能かつ利用に適した状態である。

b）文書化した情報が十分に保護されている（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。

文書化した情報の管理に当たって、財団は、該当する場合には、必ず、次の行動に取り組む。

c）配付、アクセス、検索及び利用

d）読みやすさが保たれることを含む、保管及び保存

e）変更の管理（例えば、版の管理）

f）保持及び廃棄

個人情報保護マネジメントシステムの計画及び運用のために組織が必要と決定した外部からの文書化した情報は、必要に応じて、特定し、管理しなければならない。

8 運用

8．1 運用の計画及び管理(J.5.1)

財団は、個人情報保護要求事項を満たすため、及び 6.1 で決定した活動を実施するために必要なプロセスを計画し、実施し、かつ、管理する。また、財団は、 6.2 で決定した個人情報保護目的を達成するための計画を実施する。

財団は、プロセスが計画通りに実施されたという確信をもつために必要な程度の、文書化した情報を保持する。

財団は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。

財団は、外部委託したプロセスが決定され、かつ、管理されていることを確実にする。

8．2 個人情報保護リスクアセスメント

財団は、 あらかじめ定めた間隔で、 又は重大な変更が提案されたか若しくは重大な変化が生じた場合に、6.1.2 a） で確立した基準を考慮して、個人情報保護リスクアセスメントを実施する。

財団は、個人情報保護リスクアセスメント結果の文書化した情報を保持する。

8．3 個人情報保護リスク対応

財団は、個人情報保護リスク対応計画を実施する。

財団は、個人情報保護リスク対応結果の文書化した情報を保持する。

9 パフォーマンス評価

9．1 監視、測定、分析及び評価（J.6.1）

財団は、個人情報保護パフォーマンス及び個人情報保護マネジメントシステムの有効性を評価する。

財団は、次の事項を決定する。

a）必要とされる監視及び測定の対象。これには、個人情報保護プロセス及び管理策を含む。

b）該当する場合には、必ず、妥当な結果を確実にするための、監視、測定、分析及び評価の方法

c）監視及び測定の実施時期

d）監視及び測定の実施者

e）監視及び測定の結果の、分析及び評価の時期

f）監視及び測定の結果の、分析及び評価の実施者

財団は、監視及び測定の結果の証拠として、適切な文書化した情報を保持する。

９．２ 内部監査（J.6.2）

財団は、個人情報保護マネジメントシステムが次の状況にあるか否かに関する情報を提供するために、あらかじめ定めた間隔で内部監査を実施する。

a） 次の事項に適合している。

1） 個人情報保護マネジメントシステムに関して、組織自体が規定した要求事項

2） JISQ15001 の要求事項

b） 有効に実施され、維持されている。

財団は、次に示す事項を行う。

c）頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持。監査プログラムは、関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない。

d）各監査について、監査基準及び監査範囲を明確にする。

e）監査プロセスの客観性及び公平性を確保する監査員を選定し、監査を実施する。

f）監査の結果を関連する管理層に報告することを確実にする。

g）監査プログラム及び監査結果の証拠として、文書化した情報を保持する。

９．３ マネジメントレビュー（J.6.3）

トップマネジメントは、組織の個人情報保護マネジメントシステムが、引き続き、適切、妥当かつ有効であることを確実にするために、あらかじめ定めた間隔で、個人情報保護マネジメントシステムをレビューしなければならない。

マネジメントレビューは、次の事項を考慮しなければならない。

a）前回までのマネジメントレビューの結果、とった処置の状況

b）個人情報保護マネジメントシステムに関連する外部及び内部の課題の変化

c）次に示す傾向を含めた、個人情報保護パフォーマンスに関するフィードバック

1）不適合及び是正処置

2）監視及び測定の結果

3）監査結果

4）個人情報保護目的の達成

d）利害関係者からのフィードバック

e）リスクアセスメントの結果及びリスク対応計画の状況

f）継続的改善の機会

マネジメントレビューからのアウトプットには、継続的改善の機会、及び個人情報保護マネジメントシステムのあらゆる変更の必要性に関する決定を含めなければならない。財団は、マネジメントレビューの結果の証拠として、文書化した情報を保持する。

１０ 改善

１０．１ 不適合及び是正処置(J.7.1)

不適合が発生した場合、財団は、次の事項を行う。

a）その不適合に対処し、該当する場合には、必ず、次の事項を行う。

1）その不適合を管理し、修正するための処置をとる。

2）その不適合によって起こった結果に対処する。

b）その不適合が再発しないように又は他のところで発生しないようにするため、次の事項によって、その不適合の原因を除去するための処置をとる必要性を評価する。

1）その不適合をレビューする。

2）その不適合の原因を明確にする。

3）類似の不適合の有無、又はそれが発生する可能性を明確にする。

c）必要な処置を実施する。

d）とった全ての是正処置の有効性をレビューする。

e）必要な場合には、個人情報保護マネジメントシステムの変更を行う。

是正処置は、検出された不適合のもつ影響に応じたものでなければならない。

財団は、次に示す事項の証拠として、文書化した情報を保持する。

f）不適合の性質及びとった処置

g）是正処置の結果

１０．２ 継続的改善(J.7.2)

財団は、個人情報保護マネジメントシステムの適切性、妥当性及び有効性を継続的に改善する。

個人情報保護規程（付属書Ａ）

A.3 管理目的及び管理策

A.3.1 一般

A.3.1.1 一般(J.2.4)

この管理策に規定する A.3.2 から A.3.8 は、個人情報保護管理者によって、財団が定めた手段に従って承認されなければならない。

承認は本規程が組織内で承認を受けていることを示す記録によって認めるものとする。

A.3.2 個人情報保護方針

トップマネジメントは、個人情報保護目的を説明できなくてはならない。

財団の個人情報保護目的は次の通りとする。

a）財団の事業の用に供する個人情報で特定できる本人の権利を保護する。

b）個人情報に関する法的・社会的要求事項を尊重し遵守する。

c）個人情報に係る事故を未然に防ぎ、事故の脅威から財団の事業を保護する。

A.3.2.1 内部向け個人情報保護方針(J.2.2)

トップマネジメントは、5.2.1e）に規定する内部向け個人情報保護方針を文書化した情報には次の事項を含めなければならない。

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

b）個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守すること。

c）個人情報の漏えい、滅失又はき損の防止及び是正に関すること。

d）苦情及び相談への対応に関すること。

e）個人情報保護マネジメントシステム（以下「PMS」という。）の継続的改善に関すること。

f）トップマネジメントの氏名

トップマネジメントは、内部向け個人情報保護方針を文書化した情報を、組織内に伝達し、必要に応じて、利害関係者が入手可能にするための措置を講じなければならない。具体的な措置は、本項要求事項を満たす「個人情報保護方針」を策定し、財団ホームページに掲載することとする。

A.3.2.2 外部向け個人情報保護方針(J.2.2)

トップマネジメントは、外部向け個人情報保護方針を文書化した情報には、A.3.2.1 に規定する内部向け個人情報保護方針の事項に加えて、次の事項も明記しなければならない。

a）制定年月日及び最終改正年月日

b）外部向け個人情報保護方針の内容についての問合せ先

トップマネジメントは、外部向け個人情報保護方針を文書化した情報について、一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない。具体的な措置は、本項要求事項を満たす「個人情報保護方針」を策定し、財団ホームページに掲載することとする。

A.3.3 計画

A.3.3.1 個人情報の特定(J.3.1.1)

財団は、自らの事業の用に供している全ての個人情報を特定するための手順を確立し、かつ、維持する。

個人情報の特定は、次の要領にて行う。

a) 個人情報の取扱い担当者は、業務の流れの中で使用する帳票類を考慮し、「個人情報管理台帳」に個人情報を特定する。

b) 個人情報保護管理者は、上記「個人情報管理台帳」に特定漏れがないかを確認の上、承認する。

c) 新種の個人情報は、「新規個人情報取得申請書」によって個人情報保護管理者の承認を得た後、「個人情報管理台帳」に遅滞なく記録し管理するものとする。

d) 既に取得した個人情報の利用目的や取扱い方法が変更された場合には、「個人情報取扱変更等申請書」によって個人情報保護管理者の承認を得た後、「個人情報管理台帳」を更新しなければならない。

財団は、個人情報の項目、利用目的、保管場所、保管方法、アクセス権を有する者、利用期限、保管期限などを記載した、個人情報を管理するための台帳を整備するとともに、当該台帳の内容を少なくとも年一回、適宜に確認し、最新の状態で維持されるようにする。

「個人情報管理台帳」は、毎年 4 月及び必要に応じて随時、各所属長が見直しを行い、個人情報保護管理者の承認を得る。見直しを行なう際は、個人情報の件数、アクセス権者や管理者、保管期間が適切かに留意する。

財団は、特定した個人情報については、個人データと同様に取り扱う。

A.3.3.2 法令、国が定める指針その他の規範(J.1.3)

財団は、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 (以下、“法令等” という。) を特定し参照できる手順を確立し、かつ、維持する。

法令等の特定は次の要領にて行う。

a) 対象とする法令等は、個人情報保護法、各省庁が示す基準、ガイドライン及び業界が示す指針等並びに自治体から業務を請け負う場合は当該自治体の個人情報保護条例等とし、個人情報保護管理者が特定し、個人情報保護管理者が承認するものとする。

b) 特定した法令等は「個人情報保護に関する法令規範一覧」として全職員が閲覧可能な状態とする。

c) 法令等は、個人情報保護管理者が、毎年 4 月及び必要に応じて随時、(a) 項に示す法律、基準、ガイドライン、指針、条例等の告示、改訂等を確認し、必要に応じて改訂するものとする。

A.3.3.3 リスクアセスメント及びリスク対策(J.3.1.3、J.3.1.4)

財団は、A.3.3.1によって特定した個人情報について、利用目的の達成に必要な範囲を超えた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、維持する。
財団は、A.3.3.1によって特定した個人情報の取扱いについて、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確立し、かつ、維持する。
財団は、現状で実施し得る対策を講じた上で、未対応部分を残留リスクとして把握し、管理する。
財団は､個人情報保護リスクの特定､分析及び講じた個人情報保護リスク対策を少なくとも年一回、適宜に見直す。

リスクの認識、分析、対策は次の要領で行い、「個人情報リスク分析対策表」に記述し、個人情報保護管理者の承認を経てトップマネジメントが承認する。

a）個人情報の類型化を図る
「個人情報管理台帳」を参考に、業務内容や媒体単位等の類似した個人情報を集約する。

b）ライフサイクル局面ごとのリスクを記述する
個人情報のライフサイクル（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄）それぞれについて考えられるリスクを認識する。

c）リスク対策を記述する
リスクに対する対策を記入する。

d）関連する規程類の記入
リスク対策を参照できるよう、関連する規程類の項番を記入する。

e）残留リスクの記述
十分な対策を講じられない場合や､対策後においてもリスクを完全には回避できない部分を残留リスクとして把握する。

個人情報リスク分析対策表の更新は、次の要領で行う。

ｆ）新規取得・利用目的変更・取扱い方法変更の場合
ｱ）各所属長は、既存のリスク分析シート等も参考に、当該個人情報のリスク分析を行う。
ｲ）個人情報保護管理者の承認を経てトップマネジメントの承認を受ける。

ｇ）個人情報を削除する場合
ｳ）リスク分析表から当該個人情報を削除する。
ｴ）個人情報保護管理者の承認を経てトップマネジメントの承認を受ける。

個人情報リスク分析対策表の見直しは、次の要領で行う。
「個人情報リスク分析対策表」は、毎年４月に、各所属長が見直しを行い、個人情報保護管理者の承認を経てトップマネジメントの承認を受けた上、必要に応じて変更を行う。また、個人情報の保管場所が変わる等、取り扱い方法に変更が生じた場合には、随時見直しを行う。

A.3.3.4 資源、役割、責任及び権限(J.2.3.2)

トップマネジメントは、少なくとも、次の責任及び権限を割り当てなければならない。

a）個人情報保護管理者
b）個人情報保護監査責任者

トップマネジメントは、JISQ15001 及び PMS 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組織内部に属する者の中から指名し、PMS 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。
個人情報保護管理者は、PMS の見直し及び改善の基礎として、トップマネジメントに PMS の運用状況を報告しなければならない。
トップマネジメントは、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組織内部に属する者の中から指名し、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らない。
個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、トップマネジメントに報告しなければならない。監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しなければならない。
個人情報保護監査責任者と個人情報保護管理者とは異なる者でなければならない。

個人情報保護に関する主たる責任と権限は次の通りとする。各責任者の氏名または役職は「個人情報保護体制図」に記述する。個々の特定個人情報の特定個人情報等事務取扱担当者は、「個人情報管理台帳」のアクセス権を有する者欄に記述する。

c) トップマネジメント（理事長）
財団 PMS の最高責任者として、管理責任者、監査責任者を指名し、PMS を実施させる。

d) 個人情報保護管理者（事務局長）
財団 PMS の統括責任者として、PMS の構築、維持および個人情報取扱いの管理全般について責任を負う。

e) 個人情報保護監査責任者（副理事長）
全所属の監査を計画、実行し、トップマネジメントに報告する。

f) 苦情相談窓口責任者（総務課長）
保有個人データに関する問合せや各種依頼への対応、及び個人情報取扱についての苦情相談等に対応する。

g) 情報セキュリティ責任者（総務課長）
情報セキュリティに関して、PMS を維持するための安全管理対策を実施する。

h) 特定個人情報取扱責任者（総務課長）
個人番号を含む個人情報の取扱いについて、特定個人情報取扱いの管理全般について責任を負う。

i) 特定個人情報取扱担当者（総務課の人事・給与・報酬・福利厚生に関する担当者）
個人番号を含む個人情報の取扱いについて、特定個人情報等事務取扱責任者の指示を受けて適切な取得、利用、保管を実施する。

A.3.3.5 内部規程(J.4.5.4、J.8.8.4、J.8.10)

財団は、次の事項を含む内部規程を文書化し、かつ、維持する。

文書化する事項	本規程の項番及び関連文書
a) 個人情報を特定する手順に関する規定	A.3.3.1
b) 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	A.3.3.2

c)個人情報保護リスクアセスメント及びリスク対策の手順に関する規定	A.3.3.3
d)組織の各所属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	A.3.3.4 個人情報保護体制図
e) 緊急事態への準備及び対応に関する規定	A.3.3.7
f) 個人情報の取得、利用及び提供に関する規定	A.3.4.2
g) 個人情報の適正管理に関する規定	A.3.4.3
h) 本人からの開示等の請求等への対応に関する規定	A.3.4.4
i) 教育などに関する規定	A.3.4.5
j) 文書化した情報の管理に関する規定	A.3.5
k) 苦情及び相談への対応に関する規定	A.3.6
l) 点検に関する規定	A.3.7
m) 是正処置に関する規定	A.3.8
n) マネジメントレビューに関する規定	A.3.7.3
o) 内部規程の違反に関する罰則の規定	A.3.4.3.3 公益財団法人堺市文化振興財団職員就業規則（以下「就業規則」という。）

財団は、事業の内容に応じて、PMS が確実に適用されるように内部規程を改正する。

財団は、仮名加工情報を取り扱う場合には、法令等の定めるところによって、適切な取扱いを行う手順を内部規程として文書化する。

財団は、個人関連情報を取り扱う場合には、法令等の定めるところによって、適切な取扱いを行う手順を内部規程として文書化する。

A.3.3.6 計画策定(J.3.3)

財団は、PMS を確実に実施するために、少なくとも年一回、次の事項を含めて、必要な計画を立案し、文書化し、かつ、維持する。

a) A.3.4.5 に規定する事項を踏まえた教育実施計画の立案及びその文書化

b) A.3.7.2 に規定する事項を踏まえた内部監査実施計画及びその文書化

PMS を確実に実施するために必要な計画に、次の事項を含んでいることとする。

c) 実施事項

d) 必要な資源

e) 責任者

f) 達成期限

g) 結果の評価方法

計画の詳細については、本規程 A.3.4.5 及び A.3.7.2 に定める。

A.3.3.7 緊急事態への準備(J.4.4.2、J.8.10)

財団は、緊急事態を特定するための手順、及び、特定した緊急事態にどのように対応するかの手順

を確立し、実施し、かつ、維持する。
財団は、個人情報保護リスクを考慮し、その影響を最小限とするための手順を確立し、かつ、維持する。
また、財団は、緊急事態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、維持する。

a）漏えい、滅失又はき損等が発生した個人情報の内容を本人に速やかに通知するか、又は本人が容易に知り得る状態に置くこと。
b）二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表すること。
c）事実関係、発生原因及び対応策を関係機関に直ちに報告すること。

緊急事態とは次の場合を指すものとする。

d）個人情報の取り扱いにおいて、下記の事象が発生した場合(個人情報保護委員会による「漏えい等」)
漏えい、滅失又は毀損
e）個人情報の取り扱いにおいて、下記の事象が発生した場合(プライバシーマーク審査機関による「事故等」)
①漏えい、②紛失、③滅失・き損、④改ざん、正確性の未確保、⑤不正・不適正取得、⑥目的外利用・提供、⑦不正利用、⑧開示等の求め等の拒否、⑨①～⑧のおそれ
f）火災や地震等により、個人情報を取り扱う業務に重大な支障をきたすと思われる場合
g）システム上又はネットワーク上に重大な障害が発生し、個人情報の適正管理に支障をきたすと、情報セキュリティ責任者が判断した場合
h）個人情報に関連する脅迫行為が行われた場合
i）その他、トップマネジメント又は個人情報保護管理者が、個人情報に係る緊急事態であると判断した場合

緊急時における組織体制は、次の通りとする。

j）緊急事態対策会議
トップマネジメント、役員、個人情報保護管理者、関係所属長を構成メンバーとし、トップマネジメント又はトップマネジメントが選任した者が議長となる。また必要に応じて、その他の要員及び外部の専門家を加えることもある。
k）緊急連絡網
緊急事態が発生した場合の組織内連絡は、「緊急連絡網」に基づいて行う。「緊急連絡網」は個人情報保護管理者が作成し、保管する。

基本的な対応方針は次の通りとする。

l）対応は、事態の拡大防止等のための一次対応と再発防止のための恒久的対応に分けて行う。
m）全ての対応は、緊急事態対策会議の決定に基づいて行う。
n）被害の対象となる本人に対しては、誠意ある対応を第一とする。
o）マスコミ等外部への対応は緊急事態対策会議で決定した問合せ窓口があたり、個人や各所属での対応を禁ずる。

p）速報の対象となる事態である場合は、トップマネジメントに報告の上、必要な報告を行う。

緊急時における一次対応は、被害状況の把握及び被害の拡大防止、二次被害の防止の観点により、次の手順で行う。

q）緊急事態の類型による初期対応

1）警察への通知（盗難、強盗などの場合）

2）対象となった個人情報、被害規模、範囲の特定（全ての場合）

3）システム停止等の応急措置（システム障害の場合）

4）委託元への報告（受託した個人情報の場合）

r）緊急事態対策会議の開催

1）対応方針決定

2）対応策の実施と記録

s）本人への通知（受託した個人情報の場合は、委託元の指示に基づく）

1）特定された本人に対し、事実関係及び、具体的な対応策を説明し、了承を得る。

2）了承を得られない場合には、緊急事態対策会議にて改めて対応を協議の上、決定事項に基づいて本人への対応を行う。

3）連絡がつかない場合、及び本人特定ができない場合は、内容を本人が知りうる状態におく。

t）公表（受託した個人情報の場合は、委託元の指示に基づく）

1）緊急事態対策会議において公表が必要と判断した場合には、財団ホームページを通じて事実関係及び、発生原因、対応状況、再発防止策などを公表する。

2）影響範囲が広範囲かつ深刻な場合は、マスコミへの公表を行う。

3）公表を行う場合は、マスコミ等外部に対する問合せ窓口を設置する。

u）関係機関への報告（受託した個人情報の場合は、委託元の指示に基づく）

確報の対象となる事態である場合は、緊急事態対策会議の決定に基づき、必要な報告を行う。関係機関より、対応について指示のある場合は、すみやかにそれに従う。

《個人情報保護委員会への速報》

下記に該当する「漏えい等」が発生した場合は、発覚日から 3～5 日以内に、個人情報保護委員会に報告しなければならない。

1）要配慮個人情報が含まれる事故等が発生し、又は発生したおそれがある事態

2）不正に利用されることにより財産的被害が生じるおそれがある事故等が発生し、又は発生したおそれがある事態

3）不正の目的をもって行われたおそれがある事故等が発生し、又は発生したおそれがある事態

4）個人データに係る本人の数が 1,000 人を超える事故等が発生し、又は発生したおそれがある事態

5）不正の目的をもって行われたおそれがある特定個人情報の漏えい等が発生し、若しくは発生したおそれがある事態又は不正の目的をもって、特定個人情報が利用・提供され、若しくは利用・提供されたおそれがある事態

6）特定個人情報ファイルに記録された特定個人情報が電磁的方法により不特定多数の者に閲覧され、又は閲覧されるおそれがある事態

7) 漏えい等が発生し、若しくは発生したおそれがある特定個人情報又は番号法に反して利用・提供され、若しくは利用・提供されたおそれがある特定個人情報に係る本人の数が 100 人を超える事態

8) 情報提供ネットワークシステム等又は個人番号利用事務を処理するために使用する情報システム等で管理される特定個人情報の漏えい等が発生し、又は発生したおそれがある事態

《一般財団法人　関西情報センター プライバシーマーク審査グループへの速報》

下記に該当する「事故等」が発生した場合は、発覚日から 3～5 日以内に、一般財団法人　関西情報センター プライバシーマーク審査グループに報告しなければならない。

本項 1）～8）に該当する事態

9) その他、付与機関がプライバシーマーク付与適格性審査基準における重大な違反、又は重大な違反のおそれがあると認めた事態

《個人情報保護委員会への確報》

本項 1）～8）に該当する「漏えい等」が発生した場合は、発覚日から 30 日（本項 3）の場合は 60 日）以内に、個人情報保護委員会に報告しなければならない。

《一般財団法人　関西情報センター プライバシーマーク審査グループへの確報》

e）による「事故等」が発生した場合は、発覚日から 30 日（本項 3）の場合は 60 日）以内に、一般財団法人　関西情報センター プライバシーマーク審査グループに報告しなければならない。

連絡先	
個人情報保護委員会事務局 個人データ漏えい等報告窓口	個人データ漏洩時 https://roueihoukoku.ppc.go.jp/incident/?top=r2.kojindata 特定個人情報漏洩時 https://roueihoukoku.ppc.go.jp/incident/?top=r2.mynumber
KIIS　プライバシーマーク審査グループ	https://secure.kiis.or.jp/pe/jiko/index.html

個人情報保護管理者は、事後の係争への対処および業務改善のため、緊急事態発生時における、以下に関する事項の全てにつき「緊急事態対応記録」でトップマネジメントに報告し、その記録を保管するものとする。

v）外部からの問い合わせ、クレームの内容など

w）対外連絡、報告、協議に関する事項

x）組織内における連絡、報告、協議に関する事項

緊急事態における一次対応が収束し、被害の拡大がないとトップマネジメントが判断した場合には、緊急事態対策会議は、再発防止のため、次の対応を行う。

y）原因の究明

z）原因が不適合による場合は、本規程 A.3.8 に基づく、是正処置の実施

トップマネジメントは、上記、緊急事態における一次対応、及び再発防止のための対応が完了したことを確認し、緊急事態対策会議を解散する。

A.3.4 実施及び運用

A.3.4.1 運用手順(J.5.1)

財団は、PMS を確実に実施するために、運用の手順を明確にする。

A.3.4.2 取得、利用及び提供に関する原則

A.3.4.2.1 利用目的の特定(J.8.1、J.8.10)

財団は、個人情報を取り扱うに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な範囲内において行う。

財団は、利用目的の特定に当たっては、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よう配慮する。

財団は、仮名加工情報を利用する場合には、利用目的をできる限り特定し、法令に基づく場合を除くほか、その目的の達成に必要な範囲内において行う。

A.3.4.2.2 適正な取得(J.8.2)

財団は、適法かつ公正な手段によって個人情報を取得する。

本人以外の第三者からの提供、委託または共同利用により個人情報を取得する場合は、提供元・委託元またはその他の共同利用者が個人情報保護法及び個人情報保護委員会ガイドライン等に沿って適切に個人情報を取り扱っていることを確認する。

A.3.4.2.3 要配慮個人情報(J.8.3)

財団は、新たに要配慮個人情報を取得する場合、あらかじめ書面による本人の同意を得ないで、要配慮個人情報を取得しない。ただし、次に掲げるいずれかに該当する場合には、書面による本人の同意を得ることを要しない。

a) 法令に基づく場合

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

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

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

e) 当該要配慮個人情報が、法令等により個人情報取扱事業者の義務などの適用除外とされている者及び個人情報保護委員会規則で定めた者によって公開された要配慮個人情報であるとき

f) 本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得又は利用する場合

g) 個人情報保護法二十七条第五項各号に掲げる場合において、個人データである要配慮個人情

報の提供を受けるとき

h) 個人情報取扱事業者が学術研究機関等である場合であって、当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

i) 学術研究機関等から当該要配慮個人情報を取得し、利用する場合であって、当該要配慮個人情報を学術研究目的で取得し、利用する必要があるとき（当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（当該個人情報取扱事業者と当該学術研究機関等が共同して学術研究を行う場合に限る。）

財団は、要配慮個人情報の利用についても、前項と同様に実施する。さらに、要配慮個人情報を提供する際、書面による本人の同意を得ることを要しないときは、本項のただし書き a) ～d)、又は、以下の場合に限定する。

j) 個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）

k) 個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限る。）

l) 第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

あらかじめ書面による本人の同意を得る手順は、次の通りとする。

m) 要配慮個人情報に関して、A.3.4.2.5 のａ）～ｇ）の事項を含む文面を作成し、個人情報保護管理者の承認を得る。

n) m) の文面を直接提示し、本人の署名を得る。

A.3.4.2.4 個人情報を取得した場合の措置(J.8.4)

財団は、個人情報を取得した場合は、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、本人に通知するか、又は公表しなければならない。ただし、次に掲げるいずれかに該当する場合には、本人への利用目的の通知又は公表は要しない。

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

b) 利用目的を本人に通知するか、又は公表することによって当該組織の権利又は正当な利益を害するおそれがある場合

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

d) 取得の状況からみて利用目的が明らかであると認められる場合

本項に該当する個人情報は、財団では以下に限定する。

1）名刺交換により取得した個人情報、及びこれに準じる取引先担当者情報

2）入退管理のために来訪者から取得する個人情報

3）見積書・請求書・契約書等に記載された個人情報

4）受信メールに含まれるメールアドレス及びシグネチャー（署名）

予め利用目的を公表する方法及び取得後速やかに通知又は公表する方法は、次の通りとする。

e）予め公表する方法

直接書面以外の方法で取得する個人情報の利用目的を含む文面について個人情報保護管理者の承認を得た上で、財団ホームページ上で公表する。

f）取得後速やかに通知又は公表する方法

直接書面以外の方法で取得した個人情報の利用目的を含む文面について個人情報保護管理者の承認を得た上で、次のうち合理的かつ適切な方法を選択して通知又は公表を行う。

1）文書での連絡

2）電話又は面談による口頭通知

3）財団ホームページ上での公表

A.3.4.2.5 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(J.8.5)

財団は、A.3.4.2.4 の措置を講じた場合において、本人から、書面（電子的方式、磁気的方式など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、書面によって本人の同意を得る。

a）財団の名称

b）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

c）利用目的

d）個人情報を第三者に提供することが予定される場合の事項

－ 第三者に提供する目的

－ 提供する個人情報の項目

－ 提供の手段又は方法

－ 当該情報の提供を受ける者又は提供を受ける者の組織の種類、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

e）個人情報の取扱いの委託を行うことが予定される場合には、その旨

f）A.3.4.4.4～A.3.4.4.7 に該当する場合には、その請求等に応じる旨及び問合せ窓口

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

h）本人が容易に知覚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

ただし、人の生命、身体若しくは財産の保護のために緊急に必要がある場合、又はただし書き A.3.4.2.4 の a）～d）のいずれかに該当する場合は、本人に明示し、本人の同意を得ることを要しない。

新種の個人情報を取得する場合、取得にあたる所属長は「新規個人情報取得申請書」に必要事項を記入の上、ａ）～ｈ）の事項を含んだ「取得時の必要通知事項」の文案を添付し、各所属の所属長

を経由して、個人情報保護管理者の承認を得る。
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、A.3.4.2.4のａ）～ｄ）に該当するため本人の同意を要しない場合も「新規個人情報取得申請書」に必要事項を記入の上、各所属の所属長を経由して、個人情報保護管理者の承認を得る。

本人から同意を取得する際は、a）～h）の事項を含む文面を次の方法で本人に明示し、本人の同意を得る。

i）紙媒体で取得する場合は、同文面を直接提示した上で同意の署名若しくは同意欄へのチェックを必要とする。

j）ウェブのフォームに入力させることにより取得する場合は、画面上で同文面を読んだ上で「同意欄」をクリックした後、入力されたデータが送信される方式とする。

k）従業者から個人情報を取得する際は、「従業者個人情報の取扱いについて（同意書）」により本人の同意を取得する。

l）採用応募者から個人情報を取得する際は、「採用応募者の個人情報の取扱いについて」により本人の同意を取得する。

A.3.4.2.6 利用に関する措置(J.8.6、J.8.10)

個人情報を利用する場合には、本人の同意の有無に関わらず、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を除く。財団は、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する。
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、A.3.4.2.5のa）～f）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、A.3.4.2.5のi）～l）の方法で本人の同意を得る。ただし、以下のいずれかに該当する場合には、本人の同意を得ることを要しない。

a）法令に基づく場合

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

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

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

e）当該個人情報取扱事業者が学術研究機関等である場合であって、学術研究目的で取り扱う必要があるとき（当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

f）学術研究機関等に個人データを提供する場合であって、当該学術研究機関等が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

利用目的を変更する場合、「個人情報取扱変更等申請書」に必要事項を記入の上、利用目的を改訂した「取得時の必要通知事項」の文案を添付し、各所属長を経由して、個人情報保護管理者の承認

を得る。
A.3.4.2.3 のａ）～ｄ）に該当するため本人の同意を要しない場合は、「個人情報取扱変更等申請書」に不要な理由等必要事項を記入の上、各所属長を経由して、個人情報保護管理者の承認を得る。個人情報保護管理者の承認後に、「個人情報管理台帳」の利用目的を更新する。

財団は、仮名加工情報を作成する場合には、他の情報と照合しない限り特定の個人を識別することができないようにするために必要なものとして、個人情報保護委員会規則で定める基準に従い、個人情報を加工する。
財団は、仮名加工情報を取り扱う場合には、以下を実施する。

g）利用目的をできる限り特定し、法令に基づく場合を除くほか、その目的の達成に必要な範囲内において行う。

h）あらかじめその利用目的を公表している場合及び法令に基づく場合を除き、速やかに、その利用目的を公表する。

i）仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合しない。

j）電話をかけ、郵便若しくは信書便により送付し、電報を送達し、ファクシミリ装置若しくは電磁的方法を用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用しない。

A.3.4.2.7 本人に連絡又は接触する場合の措置(J.8.7)

財団は、個人情報を利用して本人に連絡又は接触する場合には、本人に対して、A.3.4.2.5 の a）～f）に示す事項又はそれと同等以上の内容の事項、及び取得方法を通知し、本人の同意を得る。ただし、次に掲げるいずれかに該当する場合は、本人に通知し、本人の同意を得ることを要しない。

a）A.3.4.2.5 の措置において、あらかじめ、利用目的として個人情報を利用して本人に連絡又は接触することを含め a）～f）に示す事項又はそれと同等以上の内容の事項を明示し、既に本人の同意を得ているとき

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

c）合併その他の事由による事業の承継に伴って個人情報が提供され、個人情報を提供する組織が、既に A.3.4.2.5 の a）～f）に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき

d）個人情報が特定の者との間で共同して利用され、共同して利用する者が、既に共同して利用することに関して、A.3.4.2.5 の a）～f）に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、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、本人に通知するか、又は本人が容易に知り得る状態に置いているとき（以下、“共同利用”という。）

－ 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及び住所並びに法人にあっては、その代表者の氏名
－ 取得方法

e) A.3.4.2.4 の d) に該当するため、利用目的などを本人に明示、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、本人に連絡又は接触するとき

f) A.3.4.2.3 のただし書き a) ～d) のいずれかに該当する場合

財団は、個人情報を利用して本人に連絡又は接触する場合には、「個人情報取扱変更等申請書」に当該個人情報を用いて本人に連絡又は接触することを記述し、個人情報保護管理者の承認を得る。ｂ）～ｆ）に該当するため本人への通知と同意を要しない場合は、「個人情報取扱変更等申請書」に不要な理由等を明記し、個人情報保護管理者の承認を得る。

本人からの同意取得方法は次の通りとする。

A.3.4.2.5 の a) ～f) の事項又は同等以上の内容及び取得方法を含む文面について個人情報保護管理者の承認を得た上で、以下の要領で通知し同意を取得する。

1) ダイレクトメールの場合：最初に発送するダイレクトメールに通知文書を同封して同意を得る。

2) 電話の場合：最初に電話する際に、利用目的等を告げて同意を得る。

財団は d) に該当する本人への連絡又は接触をおこなわない。

A.3.4.2.8 個人データの提供に関する措置(J.8.8、J.8.8.4、J.8.10)

財団は、個人データを第三者に提供する場合には、あらかじめ、本人に対して、A.3.4.2.5 の a) ～d) 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、本人の同意を得る。ただし､次に掲げるいずれかに該当する場合は､本人に通知し､本人の同意を得ることを要しない。

a) A.3.4.2.5 の規定によって、個人データを第三者に提供することに関して、既に A.3.4.2.5 の a)～d)の事項又はそれと同等以上の内容の事項を本人に明示し､本人の同意を得ているとき、または A.3.4.2.7 の規定によって、既に A.3.4.2.5 の a)～d)の事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を得ているとき

b) 本人の同意を得ることが困難な場合であって、法令等が定める手続に基づいた上で、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、本人に通知するか、又はそれに代わる同等の措置を講じているとき

1) 財団の名称及び住所並びに代表者名

2) 第三者への提供を利用目的とすること

3) 第三者に提供される個人データの項目

4) 第三者への提供の手段又は方法

5) 本人の請求などに応じて当該本人が識別される個人データの第三者への提供を停止すること

6) 取得方法

7) 本人からの請求などを受け付ける方法

8) その他個人の権利利益を保護するために必要なものとして個人情報保護委員会規則で定め

る事項

c) 法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に関する情報であって、かつ、本人又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、法令等が定める手続きに基づいた上で、b) の 1) ～8) 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、本人に通知するか、又は本人が容易に知り得る状態に置いているとき

d) 特定した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とき

e) 合併その他の事由による事業の承継に伴って個人データ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データを取り扱うとき

f) 個人データを共同利用している場合であって、共同して利用する者の間で、A.3.4.2.7 に規定する共同利用について契約によって定めているとき

g) A.3.4.2.3 のただし書き a) ～d)、又は A.3.4.2.3 のただし書き j) ～l) のいずれかに該当する場合

財団では、b)、c) に該当する個人データの提供をおこなわない。

個人情報を第三者へ提供する場合は予め「個人情報取扱変更等申請書」に必要事項を記入し、取得方法並びに A.3.4.2.5 の a)～d)を明記した文面の案を添付し、個人情報保護管理者の承認を受ける。

ｅ)、ｇ）に該当するため通知と同意を要しない場合は、「個人情報取扱変更等申請書」に不要な理由等を明記し、個人情報保護管理者の承認を受ける。

本人からの同意取得方法は次の通りとする。

a) ～g) に該当しない場合は、A.3.4.2.5 の a) ～d) の事項又は同等以上の内容及び取得方法を含む文面について個人情報保護管理者の承認を得た上で、同文面を本人に通知し、A.3.4.2.5 の i) ～l) の方法で本人の同意を得る。

第三者が個人関連情報を個人データとして取得することが想定される場合、当該個人関連情報を当該第三者に提供するに際しては、A.3.4.2.3 の a) ～d)、又は、A.3.4.2.3 の j) ～l) のいずれかに該当する場合を除き、あらかじめ、次に掲げる事項又はそれと同等以上の内容の事項について、法令等の定めるところによって、確認を行う。

h) 当該第三者が個人関連情報取扱事業者から個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の当該本人の同意が得られていること。

i) 外国にある第三者への提供にあっては、a) の本人の同意を得ようとする場合において、法令等で定めるところによって、以下の 1)～3) に示す事項について、あらかじめ、当該本人に提供されていること。

1) 当該外国における個人情報の保護に関する制度

2) 当該第三者が講ずる個人情報の保護のための措置

3) その他当該本人に参考となるべき情報

個人関連情報を第三者に提供する場合、法令等の定めるところによって、以下の事項について、確

認の記録を作成、保管する。

《個人関連情報の提供元の確認の記録事項》

j) h) で本人の同意を得られていることを確認した旨及び外国にある個人情報取扱事業者にあっては、i)で本人に情報の提供が行われていることを確認した旨

k) 個人関連情報を提供した年月日

l) 当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

m) 当該個人関連情報の項目

《個人関連情報の提供先の確認の記録事項》

n) h)で本人の同意が得られている旨及び外国にある個人情報取扱事業者にあっては、i)で本人に情報の提供が行われている旨

o) 当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

p) 当該個人関連情報によって識別される本人の氏名その他の当該本人を特定するに足りる事項

q) 当該個人関連情報の項目

仮名加工情報を提供する場合には、以下の場合を除き、仮名加工情報である個人データを第三者に提供しないこと。

r) 仮名加工情報の取扱いの全部又は一部を、A.3.4.3.4 と同等の措置を講じた上で委託する場合

s) 仮名加工情報が特定の者との間で共同して利用され、共同して利用する者が、既に共同して利用する場合 (A.3.4.2.5 の a)～f)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、以下の 1)～6)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く場合)

1) 共同して利用すること

2) 共同して利用される仮名加工情報の項目

3) 共同して利用する者の範囲

4) 共同して利用する者の利用目的

5) 共同して利用する仮名加工情報の管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

6) 取得方法

t) 合併その他の事由による事業の承継に伴って仮名加工情報を提供する場合

u) 法令に基づく場合

A.3.4.2.8.1 外国にある第三者への提供の制限(J.8.8.1)

外国にある第三者に個人データを提供する場合、以下のいずれかを満たす。ただし、A.3.4.2.3 の a) ～d)、又は、A.3.4.2.3 の j) ～l) のいずれかに該当する場合はこれに限らない。

a) あらかじめ外国にある第三者への提供を認める旨の本人の同意がある場合

b) 個人データの取扱いについて個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者への提供をする場合

c) 個人の権利利益を保護する上で我が国と同等の水準にある外国として個人情報保護委員会規則で定める国・地域にある第三者への提供をする場合

a)によって外国にある第三者に個人データを提供する場合は、あらかじめ、法令等の定めるところによって、次に掲げる事項について、当該本人に必要な情報を提供する。

d) 当該外国の名称

e) 当該外国における個人情報の保護に関する制度に関する情報

f) 当該第三者が講ずる個人情報の保護のための措置に関する情報

g) d) ～f) に定める事項が特定できない場合、その旨及びその理由

h) g) に該当する場合であって、d) ～f) の事項に代わる本人に参考となるべき情報がある場合には、当該情報

i) g) 及び h) に該当する場合について情報提供できない場合には、g) 及び h) に定める事項に代えて、その旨及びその理由

本項 b) によって外国にある第三者に個人データを提供する場合には、あらかじめ、法令等の定めるところによって、次に掲げる事項について、必要な措置を講じる。

j) 当該第三者による相当措置の実施状況並びに相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその内容について、適切かつ合理的な方法による定期的な確認

k) 当該第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人データの当該第三者への提供の停止

l) 本人の求めを受けた場合には、情報提供することにより当該組織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を除き、遅滞なく、以下の情報の提供

1) 当該第三者による体制の整備の方法

2) 当該第三者が実施する相当措置の概要

3) j) による確認の頻度及び方法

4) 当該外国の名称

5) 当該第三者による相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその概要

6) 当該第三者による相当措置の実施に関する支障の有無及びその概要

7) 前号の支障に関して、k) により講ずる措置の概要

本項 l) で、本人の求めに係る情報の全部又は一部について提供しない旨の決定をしたときは、本人に対して、遅滞なく、その旨を通知するとともに、その理由を説明する。

個人関連情報を外国にある第三者に提供した場合には、本項で定めるところによって、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講じる。

A.3.4.2.8.2 第三者提供に係る記録の作成など(J.8.8.2)

財団は、個人データを第三者に提供したときは、法令等の定めるところによって記録を作成し、保管する。ただし、次に掲げるいずれかに該当する場合は、記録の作成を要しない。

a) 特定した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とき

b) 合併その他の事由による事業の承継に伴って個人データ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データを取り扱うとき

c) 個人データを共同利用している場合であって、共同して利用する者の間で、A.3.4.2.7 に規定する共同利用について契約によって定めているとき

d) 法令に基づく場合

e) 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

f) 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

g) 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

h) 個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）

i) 個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限る。）

j) 第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

第三者提供に係る記録の作成は、次の要領で実施する。

k) 個人データを第三者に提供した時の記録は、次の情報を含むこととする。

1) 当該個人データを提供した年月日

2) 当該第三者の氏名又は名称

3) その他の法令等で定められた事項

l) 本人の同意があった場合も、記録作成義務はなくならない。

m) 作成した記録は、法令等で定められた期間保存しなければならない。

A.3.4.2.8.3 第三者提供を受ける際の確認など(J.8.8.3)

財団は、第三者から個人データの提供を受けるに際しては、法令等の定めるところによって確認を行う。ただし、次に掲げるいずれかに該当する場合は、確認を要しない。

a) 特定した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されたとき

b) 合併その他の事由による事業の承継に伴って個人データを提供される場合であって、承継前の利用目的の範囲内で当該個人データを取り扱うとき

c) 個人データを共同利用している場合であって、共同して利用する者の間で、A.3.4.2.7 に規定する共同利用について契約によって定めているとき

d) 法令に基づく場合

e) 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

f）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

g）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

h）個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）

i）個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限る。）

j）第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

財団は、第三者から個人データの提供を受けるに際して確認を行ったときは、必要な記録を作成する。

第三者から個人データの提供を受けるに際して確認を行った記録は、必要な期間保存する。

第三者提供を受ける際に確認する内容は次の通りとし、法令等の定めに基づく記録を作成する。

k）提供元である第三者の氏名又は名称及び住所並びに法人などについては代表者の氏名

l）提供元である第三者による当該個人データの取得の経緯

A.3.4.2.9 匿名加工情報(J.8.9)

財団は匿名加工情報の取扱を行わない。

A.3.4.3 適正管理

A.3.4.3.1 正確性の確保(J.9.1)

財団は、利用目的の達成に必要な範囲内において、個人データを、正確、かつ、最新の状態で管理する。入力の際は誤りの無いよう誤入力チェックを行い、常に正確かつ、最新の状態である事を確認する。

財団は、個人データを利用する必要がなくなったときは、A.3.4.3.2b)6)の手順に従い当該個人データを遅滞なく消去するよう努める。

仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去する。

A.3.4.3.2 安全管理措置(J.8.10、J.9.2)

財団は、その取り扱う個人情報の個人情報保護リスクに応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じる。

財団は、本項に述べる安全管理策について必要性を検討し、策定し、実施する。

a）入退管理

1）入退資格

個人情報保護管理者は、入退を制限する場所の範囲を定め、入退資格を有さない者の立ち入りを制限し、制限を実現するための鍵管理等をおこなう。

2）職員証・許可証等の着用義務

従業者、来訪者、あるいは不審な侵入者の見分けが困難な執務スペースにおいては、制服や許可証など、識別するための施策を行う。

入退を許可された外来者に対しては、原則として職員が随行し、立入り場所の制限を行い、管理する。

3）施錠の原則

① 各事業場は常時施錠を原則とする。やむを得ず施錠可能でない事業場においては、個人情報を施錠可能なキャビネット等に収納するなどの管理を行う。

② 施錠、開錠は、原則として従業者が行う。

4）入退者の記録

① 各稼働日における従業者の最初の入場者の氏名と入場時刻および最後の退場者の氏名と退場時刻を「入退室管理簿」への記入またはそれに代わる装置等により記録する。

② 入退制限範囲内への来訪者の訪問時、原則として１組につき１葉の「来訪者入退受付票」またはそれに代わる装置等により記録する。来訪者に対応したものは退出時間を記載し、所定の場所に格納する。

③ ①、②の記録は１年間保存の上、必要な時はいつでも閲覧または検索できるように保管する。

5）物品の持込み・持出し

① 持込み・持出し物品に関して不審な点を発見した従業者等は、速やかに個人情報保護管理者に報告する。

② 財団の資産および顧客からの預り資産を入退管理の担当者の許可なく無断で持ち出すことを禁ずる。

6）休日・夜間の入場

従業者等が休日、夜間に入場する場合は、原則として、その日の前日までに所属長の許可を受けた者に届け出る。ただし、前日までに許可を得ることができない場合は事後の承認を得る。

7）不審者の監視

入退資格を有していない、または有していても不審な行動が察知される者を発見した従業者は、その行動を監視し、必要と認めるときは個人情報保護管理者に報告する。

8）入退管理に関する運用の確認

個人情報保護管理者は、入退管理が有効かつ適切に実施されていることを定期的に確認し、不備が発見された場合は速やかに是正の処置をとらなければならない。個人情報保護管理者は、従業者の入退記録が適切にとられているかどうかを月に１度確認する。

9）特定個人情報の取扱区域

特定個人情報は、特定個人情報等事務取扱担当者以外から見られることのない囲われた区域で、特定個人情報等事務取扱担当者だけが取り扱う。

b）個人情報の適正管理

1）クリアデスクの徹底

離席時や退社時には、個人情報を記した書類や電磁的記録媒体を机上やその周辺に放置してはならない。

2）個人情報の複製

個人情報の複製は、バックアップの必要上および業務上やむをえない場合の必要最小限の範囲にとどめるものとする。

3）個人情報の保管

個人情報の保管は、次に掲げる事項に従って行わなければならない。

① 個人情報のデータは、それを業務上取扱う必要のある者以外が閲覧や操作できる状態におかないこと。特定個人情報は、特定個人情報の管理区域を明確に定め、管理区域以外に保管せず、特定個人情報等事務取扱担当者以外の者が閲覧や操作できる状態におかないこと。

② 個人情報のデータファイルやデータベースは、必要に応じてアクセス権や、パスワード等を設定し、管理すること。

③ 個人情報が記された書類および個人情報が入った電磁的記録媒体（CD-R、USB メモリー等）は、業務終了時や長時間中断時には、紛失や盗難に備え鍵のかかる机やキャビネット等に施錠して保管する。

④ 重要な個人情報が記された書類のファイル、バインダ、電磁的記録媒体の容器、保管場所等には、部外者に内容が容易にわかる表示をしない。

⑤ 個人情報が記された書類および個人情報が入った電磁的記録媒体（CD-R、USB メモリー等）は、個人情報管理台帳に定められた保管期間に従って保管する。

⑥ 保管場所は火災による情報消失のリスクから保護するために、火気厳禁とし、必要に応じて消火器等を設置する。

4）個人情報の移送・送信

① 個人情報を外部へ持ち出す際は、個人情報保護管理者の許可を得ることとし、目的地以外へ立ち寄らず、電車の網棚に置かない、手放さない、車中に放置しないよう徹底する。

② 紙や電磁的記録媒体による個人情報を郵便や宅配便等により移送するときは、宛名の確認や封入物のダブルチェック等を行うなどして誤封入の防止に努めるとともに、授受における誤配、紛失等の危険を最小限にするため、ポストへの施錠、私書箱の利用、受け取り確認が可能な移送手段の選択等の措置を講じる。

③ 個人情報を含む電子データファイルをインターネット経由で送受信する際は、情報セキュリティ責任者が許可したストレージサービスを介しておこなう。やむを得ず電子メールに添付して送信する場合は、送信先や取り扱う情報等を踏まえ、必要かつ適切な安全管理措置を講じければならない。

④ 個人情報をインターネット経由で通信するシステムを利用する際は、SSL 等の暗号化対策やパスワード設定等の措置を講じる。

⑤ 個人情報の入った FAX を送受信する際は、必要に応じて短縮ダイヤルの利用、完了する

までの待機、完了後の相手先への電話連絡を行うこととする。また、送受信資料は直ちに回収し、放置することの無いように注意する。大量の個人情報やリスクの高い個人情報をFAX で受領する場合は、必要に応じて専用の受信 FAX をアクセス管理された場所に設置する。

5）個人情報の授受記録

個人情報の授受は、次に掲げる事項に従って行わなければならない。

① 紙や電磁的記録媒体による個人情報の授受に際しては、送付票や受領証等で授受の完了を確認するか、または授受簿を作成し記録すること。

② ストレージサービスを介した授受を行う際は、サービスの利用ログを授受記録とする。電子メールにより個人情報の授受を行う際には送信済みメールおよび、受領確認の返信メールの何れかまたは両方を授受記録とする。

③ 特定個人情報を従業者から取得する場合は、受領日時等を記録するものとする。

6）個人情報の廃棄

個人情報の廃棄は、次に掲げる事項に従って行わなければならない。

① 紙に記された個人情報の廃棄は、シュレッダーによる裁断、焼却、溶解いずれかの方法で処分する。また、廃棄前の一時保管場所からの紛失・盗難防止のため、重要書類は即廃棄する。

② 電磁的記録媒体（PC およびサーバ内等のハードディスクも含む）に記憶されている個人情報の廃棄は、次の何れかの廃棄方法で処分すること。

・データ消去用のソフトウェアを使用するなどし、記憶されている情報を復元できないように完全に消去する。

・電磁的記録媒体そのものを物理的な破壊方法により処分する。

③ 上記以外の方法により、処分する必要があると認められる場合、事前に個人情報保護管理者の承認を得ることを要するものとする。

④ 個人情報の記された書類は再利用しないこと。

⑤ 必要に応じてデータ消去簿や廃棄記録により、廃棄漏れを防止する。特定個人情報の廃棄、返却または行政等への提出の際は、その日時等を記録するものとする。

⑥ 契約解除等によりリース機器・レンタル機器等を返却する場合は、機器内に保存・記録されている情報を完全消去（復元できない状態にすることを含む）した上で返却するか、返却先で確実に完全消去（復元できない状態にすることを含む）させなければならない。

c）情報システムの管理

1）サーバの安全対策

① 情報セキュリティ責任者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、次のような安全対策を検討し、必要に応じて実施するものとする。

・システム及びデータのバックアップ

・ディスクの二重化など冗長構成

・ログの取得と管理および定期的なチェック

・電源の冗長化など、停電対策

・専用ツールや外部サービスによる定期的な脆弱性チェック

2）ネットワークの管理

情報セキュリティ責任者は、組織内ネットワークの運用とセキュリティの確保を適切に行い、データの正確性と安全性が維持されるよう次の点に努める。

① ネットワークにおける社外との境界にはファイアウォールを設けるなど、不正侵入対策を施す。

② ネットワーク障害に備え、必要に応じてバックアップ回線の確保や復旧手順を備える。

③ ネットワーク上の機器やデータに対する不正アクセスから重要な情報資産を保護するための対策をリスクに応じて実施する。

④ 利用者の故意、過失により情報の漏えい、滅失、き損が起こらないよう、利用者への操作手順の明示、教育の支援、その他の対策を実施する。

3) 不正ソフトウェアへの対策

コンピュータウィルスやスパイウェア等による情報漏えいやデータの破壊を防ぐため、情報セキュリティ責任者は次の対策を施す。

① 組織内ネットワークに接続する全てのパソコンにウィルス対策ソフトウェア等を導入し、当該ソフトウェアのアップデートおよびパターンファイルの更新が適時に行われるように管理する。

② オペレーティングシステム（OS）やアプリケーションには常に最新のセキュリティパッチを適用する。ただし、検証の結果、業務上支障があると認められる場合には、他の方法で不正ソフトウェア対策を実施する。

4) アクセス記録の管理

情報セキュリティ責任者は、必要に応じて個人情報が格納されているコンピュータのアクセス記録を常時取得し、定期的にチェックを行わなければならない。

5) 機器・装置等の物理的な保護

情報セキュリティ責任者は、重要な情報資産を取り扱う組織内の機器・装置類に対する安全管理上の脅威（盗難・破壊・破損等）や、環境上の脅威（地震、漏水、火災、停電等）から物理的に保護するため、必要に応じて次のような措置を講じる。

① サーバ室など隔離されたエリアへの設置

② 隔離されていないエリアに設置する場合は、常時施錠可能なラック等への収容

③ 耐震性、防火性、防水性を考慮した設置

④ 無停電電源装置の設置

6) ソフトウェア使用の原則

① クライアントパソコンで使用するソフトウェアは、原則情報セキュリティ責任者によって指定されたもののみとし、それ以外のソフトウェアを使用する場合は、事前に許可を得るものとする。

②ウィルス感染や不正アクセス等の原因となりやすいソフトの使用は、特に厳禁とする。

③ 情報セキュリティ責任者は、システムの脆弱性を高めるソフトウェア等がネットワーク上に不正に導入されないよう十分に注意喚起する。

7) ユーザ、パスワードの付与管理

① 情報セキュリティ責任者は、業務で使用する各種アカウントについて、ユーザおよびパスワードの付与と変更、削除の管理を行うものとする。

② アカウントは業務上必要な範囲で職員等に付与され、付与は原則として記録に残る方法にて申請し、情報セキュリティ責任者によって承認されることを要する。

③ 職員等が退職した場合は、各所属にて業務に支障がないよう調整し、速やかに該当アカウントを削除しなければならない。

8）パスワードの管理

① ユーザのパスワードは、利用者が厳重に管理し、必要に応じて変更しなければならない。その際、前回と同じパスワードは使用しないものとし、パソコン起動の際のパスワードは大小英数記号混合 8 文字以上の文字列を設定しなければならない。

② 各システムにおける特権アカウントのパスワードは、情報セキュリティ責任者において厳重に管理しなければならない。

③ 利用者および情報セキュリティ責任者は、パスワードの代替若しくは補完のために、指紋などの生体認証、ＩＣカード認証などの機器による認証方式を採用することもできるものとする。

④ パスワードを机上等に貼付してはならない。

⑤ 複数のサービスで同一のパスワードを使い回してはならない。

⑥ 漏えいした、または漏えいの恐れがあるパスワードは、速やかに変更しなければならない。

9）アクセス権と認証管理

① 利用者のアクセス権は、必要最小限の者がアクセスするという原則のもとに、情報セキュリティ責任者が検討し、設定を行う。利用者のアクセス権の変更は、当該利用者の属する所属長を経由して、情報セキュリティ責任者の許可によりおこなうものとする。

② 重要な個人情報および企業秘密などの情報に対するアクセス権の設定、変更は、個人情報保護管理者、またはトップマネジメントの許可を必要とする。

③ 特定個人情報については、当該情報の特定個人情報等事務取扱担当者だけがアクセスできるようアクセス権を設定し維持するものとする。

10）財団所有パソコン利用者の義務

利用者は、財団所有パソコンを自己の業務のためにのみ使用し、私用で使ったり、部外者に使わせてはならない。財団所有パソコン利用者はその管理について次の義務を負う。

① 財団所有パソコンの盗難防止

② 不正ソフトウェアからの保護

③ 障害や事故の発生、又はそのおそれのあるときの情報セキュリティ責任者への報告

11）財団所有パソコンの盗難防止対策

ノートパソコンは盗難防止のために、次のいずれかの対策を施すものとする。

① ワイヤーチェーン等による固定

② 不使用時の施錠保管

③ カバン等に入れて常時携帯

12）財団所有パソコンの持ち出しと持ち込み

① 財団所有パソコンの持ち出しは原則として禁止とするが、当該従業者の所属等の属性により持ち出しが認められている場合は、その限りではない。

② 財団が管理しないパソコンの持ち込みおよび業務上の利用については原則として禁止とするが、雇用形態の一環として私物パソコンの使用が認められている場合はこの限りではない。

③ ①②以外の場合で、財団所有情報機器類の持ち出し、私用情報機器類の持ち込みを行う

場合は、「パソコン持出申請書」またはそれに代わる管理方法により状況の把握を行う。

④ 財団所有情報機器類を持ち出す際は次の保護対策を行う。

・必要な情報以外を機器内部に保存しない。

・起動パスワードの設定等を行い、第三者による起動制限措置をとる。

・重要な情報を内部保存する場合は、ファイル自体を暗号化またはパスワード付与する。

⑤ 財団が管理しない情報機器類を利用する場合は、次の保護対策を行う。

・組織内ネットワークには接続しない。やむを得ず接続する場合は、接続と同時にソフトウェアによるウィルスチェックが働くよう設定する。

・前項と同様の盗難防止対策をとる。

・情報セキュリティ責任者が必要と判断した場合は、私用情報機器類の利用状況等に関して調査をおこなう。

13）離席時のモニター画面からの漏えい防止（クリアスクリーン）

利用者は、離席時にパソコンを他者に操作されたり、画面を覗かれたりすることにより情報が漏えいしないよう、不操作 10 分でスクリーンセーバが起動する、または OS がスリープし、かつ、再使用前にパスワードの入力を求めるよう設定する。

14）組織内ネットワークの利用

組織内ネットワークの利用は、次のルールに従って行う。

① 組織内ネットワークへの接続は、情報セキュリティ責任者の承認と指示された手順に従う。

② 他人の、パスワードで、組織内ネットワークに接続しないこと。

③ 各拠点内のネットワークは、有線 LAN による構築を優先する。やむを得ず無線 LAN を利用する場合は、情報セキュリティ責任者の承認を得た暗号化規格を採用し、財団が管理しない情報機器類の接続制限など、十分な安全対策を実施すること。

④ 社外から組織内 LAN にリモートアクセスする場合は、情報セキュリティ責任者の認める十分に安全対策が講じられた方法を用いること。

15）インターネットの利用

インターネットの利用は、次のルールに従って行う。

① インターネットを利用する場合は、情報セキュリティ責任者の指示に従うこと。

② インターネットは、組織内ネットワークに比べ様々なリスクがあることを認識し、業務上必要な範囲に限定して利用すること。

③ 事件・事故が発生した場合又はその可能性を認識した場合は、所属長及び情報セキュリティ責任者に速やかに連絡すること。

④ インターネットへのアクセスは、情報セキュリティ責任者の承認と指示された手段でアクセスすること。公衆回線を使ったインターネット接続をしてはならない。

16）メールの利用

メールの利用は、次のルールに従って行う。

① メールは財団所定のソフトウェアを使用し、その利用は業務上必要な場合に限定すること。

② 送信元、送信先以外の個人情報をメール本文に記載することのリスクを検討し、必要に応じて他の方法を選択すること。

③ 外部コミュニケーションサービスを利用する場合は、個人情報の委託先として管理をお

こなう。登録するメンバーや共有する情報については十分に配慮する。

④ メール送信に際しては、送信先のメールアドレスに間違いが無いかを確認してから送信すること。

⑤ 同報メールにより、多数を対象にメール送信する場合は、Bcc に送信先メールアドレスを設定するものとし、To や Cc に設定することによる漏えいを避けなければならない。

17）外部電磁的記録媒体の取扱

① CD-R や USB メモリなどの外部電磁的記録媒体の利用は、当該所属長が認めた用途に限定する。

② 外部電磁的記録媒体を机上や、棚上等に放置してはならない。

③ 私有の外部電磁的記録媒体を持ち込む場合、財団所有の外部電磁的記録媒体を持ち出す場合は、「USB メモリ持出管理台帳」にて当該所属長および情報セキュリティ責任者の許可を得なければならない。

18）バックアップデータの管理

① バックアップデータを記憶した媒体は、施錠可能な場所に保管し、地震、火災、水害等の事故を考慮したうえ、必要に応じてバックアップ元のハードウェアのある場所とは別の場所（遠隔地等）に保管するものとする。

② 情報セキュリティ責任者は、バックアップが確実に行われており、障害時に復元が可能かどうかを定期的にチェックしなければならない。

19）ネットワークを経由してデータを送受信する場合

① 拠点間ネットワークを構築する場合、情報セキュリティ責任者は VPN を採用など、安全性に十分注意したシステムを採用しなければならない。

② 情報セキュリティ責任者は、前項における対策が有効であるかどうかをチェックし、不十分と思われる場合は、適切な代替策を提示し、もしくは他の受け渡し方法に変更するなどの対策を当該所属長と協議の上実施しなければならない。

20）電磁的記録媒体によりデータを受け渡しする場合

① CD-R や USB メモリなどの電磁的記録媒体でデータを受け渡す場合は、データの内容に応じてセキュリティを確保できるよう、配達記録が残るサービス利用または従業者による手渡しなど、確実な受け渡し方法をとることとする。

② データの受け渡しに際しては授受記録を残し、情報セキュリティ責任者は定期的に授受記録をチェックし、受け渡し方法に問題があれば是正しなければならない。

d）携帯電話・スマートフォンの管理

1）管理者

① 財団所有の携帯電話・スマートフォン（以下「財団所有携帯電話等」という）は情報セキュリティ責任者が管理する。

② 情報セキュリティ責任者は、必要に応じて管理簿等を作成することにより、使用者や使用期間、使用状況等を記録するものとする。

③ 個人情報保護管理者は、財団所有携帯電話等の紛失等、事故発生時の対応を主管する。

2）使用手続き

財団所有携帯電話等の使用を希望する者は、所属長を経由してトップマネジメントの承認を得なければならない。

3）使用者の義務

① 財団所有携帯電話等を使用する者は、紛失、破損しないよう丁寧かつ慎重に扱わなければならない。

② 財団所有携帯電話等を使用する者は、使用者本人以外が操作できないよう、セキュリティロック等により保護しなければならない。必要に応じて、オプションサービス等による遠隔ロックや遠隔削除サービスを利用する。

③ 持ち歩く際は、ストラップを付ける等の盗難・紛失防止策を必要に応じて講じなければならない。

④ 電車やバスの中、その他公共の場所における使用は控え、個人情報やその他機密情報を他者に聞かれないよう十分配慮しなければならない。

⑤ 財団所有携帯電話等を紛失、破損した場合は、直ちに個人情報保護管理者に報告し、指示を受けなければならない。

⑥財団所有携帯電話等を私用に用いてはならない。

財団所有携帯電話等がスマートフォンである場合は、上記各項に加えて、下記の項についても留意する。

⑦ アプリ等ソフトウェアは最新の状態になるようにし、ウィルス対策アプリがインストールされており、パターンファイルの更新が適切に行われるよう設定されていることを確認しなければならない。

⑧ 業務に不要なアプリはインストールしてはならない。公式なサイト以外で公開されているアプリをインストールしてはならない。

⑨ 不要なデータをスマートフォン内に保存してはならない。一時的に保存した場合は、不要になり次第削除しなくてはならない。

e）個人情報を取り扱う情報システムの安全対策

1）情報システムの変更時の確認

個人情報を取扱う情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれていないことを、必要に応じて次の観点から検証するものとする。

① 情報システムの変更時に、情報システム又は運用環境のセキュリティが変更前と同等以上に維持されていること

② 不要になったシステム機能が残存していないこと

③ システムの変更によりウェブサイトやモバイルサイトに公開すべきでない個人情報が閲覧可能な状態になっていないこと

④ ウェブアプリケーションの安全対策

ウェブアプリケーションを利用して個人情報を取扱う場合は、次の事項に充分留意し、個人情報の取扱い内容に応じた安全対策を講じなければならない。

ｱ）ウェブアプリケーションのセキュリティ実装

・SQL インジェクション対策

・クロスサイトスクリプティング対策　　など

ｲ）ウェブサイト安全性向上のための取組み

・ウェブサーバのセキュリティ対策

・ネットワーク盗聴への対策　　など

これらの対策を講じるに際しては、独立行政法人情報処理推進機構（IPA）発行の「安全なウェブサイトの作り方」を参考にするものとする。

f）在宅勤務時の安全対策

1）情報セキュリティ責任者が実施すべき対策

①在宅勤務者の情報セキュリティに関する認識を確実なものにするために、定期的に教育・啓蒙活動を実施する。

②端末に必要な情報セキュリティ対策が施されている事を使用者に確認させる。

③ランサムウェアの感染に備え、重要な電子データのバックアップを組織内システムから切り離した状態で保存する。

④在宅勤務者がインターネット経由で組織内システムにアクセスする際のアクセス方法を定める。また、組織内システムとインターネットの境界線はファイアウォールやルータ等を設置し、アクセス状況を監視するとともに、不必要なアクセスを遮断する。

⑤ファイル共有サービスなどのパブリッククラウドサービスの利用ルールを整備し、情報漏洩につながる恐れのある利用方法を禁止する。

2）在宅勤務者が実施すべき対策

①定期的に実施される情報セキュリティに関する教育・啓蒙活動に積極的に取り組むことで、情報セキュリティに対する認識を高めることに務める。

②マルウェア感染を防ぐ為、OS やブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにアクセスしない。

③アプリケーションをインストールする際はその安全性を確認し、禁止されているものに該当しないか確認する。また、許可されているアプリケーションでも、安全性に疑いのある場合は管理者に確認を行う。

④作業開始前にウィルス対策ソフト及び OS、ソフトウェアについて最新の状態である事を確認する。

⑤無線 LAN を使用する場合、安全性の高い暗号化方式を使用する（WPA2 以上を推奨）

⑥第三者と共有する環境で作業を行う場合は、端末の画面にプライバシーフィルターを装着するか、作業場所を選ぶことにより、画面の覗き見防止に努める。

財団は、仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等を取得したときは、削除情報等の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、削除情報等の安全管理のための措置を講じる。

A.3.4.3.3 従業者の監督(J.9.3)

財団は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行う。

従業者の監督は、次の要領で実施する。

a）従業者との雇用契約時又は派遣職員等の受入時における派遣事業者との委託契約時には、個人情報の非開示契約を締結する。この契約には、雇用契約等の終了後においても非開示条項が一定期間有効である旨を定める。

b）内部規程違反時の罰則

1）A.3.3.5 の内部規程に対する違反の疑いが生じた場合には、個人情報保護管理者の指示の下、調査と確認を行う。

2）調査と確認の結果、違反の事実が明白となった場合には、その影響と損失の度合いに応じ、就業規則に則り、解雇を含む懲戒を行うものとする。また、財団が被った損害の一部又は全部を賠償させることがある。

3）派遣職員等については、派遣事業者との契約に基づいて責任を負わせるものとする。

c）安全管理に係るモニタリング

1）財団は、情報セキュリティ上の安全管理を目的としてビデオ及びオンラインよる従業者のモニタリングを実施する場合がある。モニタリングを実施する場合は、事前に従業者に周知徹底するものとする。

2）モニタリングの実施に関する責任は、個人情報保護管理者が負うものとし、個人情報保護管理者は前項の利用目的の範囲を超えて利用されないよう、モニタリング情報を厳重に管理するものとする。

3）モニタリングの実施状況が適正に行われていることを運用の確認又は監査において確認するものとする。

A.3.4.3.4 委託先の監督(J.9.4)

財団は、個人データの取扱いの全部又は一部を委託する場合、特定した利用目的の範囲内で委託契約を締結する。

財団は、個人データの取扱いの全部又は一部を委託する場合は、十分な個人データの保護水準を満たしている者を選定する。このため、財団は、委託を受ける者を選定する基準を確立する。委託を受ける者を選定する基準には、少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護の水準にあることを客観的に確認できることを含める。

財団は、個人データの取扱いの全部又は一部を委託する場合は、委託する個人データ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う。

財団は、次に示す事項を契約によって規定し、十分な個人データの保護水準を担保する。

a）委託者及び受託者の責任の明確化

b）個人データの安全管理に関する事項

c）再委託に関する事項

d）個人データの取扱状況に関する委託者への報告の内容及び頻度

e）契約内容が遵守されていることを委託者が、定期的に、及び適宜に確認できる事項

f）契約内容が遵守されなかった場合の措置

g）事件・事故が発生した場合の報告・連絡に関する事項

h）契約終了後の措置

財団は、当該契約書などの書面を少なくとも個人データの保有期間にわたって保存しなければならない。

委託先の監督は、次の要領で実施する。

i）個人情報保護管理者は毎年 4 月に委託先の選定基準を見直し、「個人情報委託先審査票」に定

める。

j）各所属長は、各所属において個人情報を委託する全ての委託先について、取引開始時、毎年4月、及び必要に応じて「個人情報委託先審査票」による評価を実施、個人情報保護管理者の承認を得る。

k）個人情報保護管理者は、各所属において個人情報を委託する全ての委託先について「個人情報委託先審査票」を作成し、維持する。

A.3.4.4 個人情報に関する本人の権利

A.3.4.4.1 個人情報に関する権利(J.10.1)

財団は、保有個人データ又は第三者提供記録に関して、本人から開示等の請求等を受け付けた場合は、A.3.4.4.4～A.3.4.4.7 の規定によって、遅滞なくこれに応じる。ただし、次に掲げるいずれかに該当する場合は、保有個人データには当たらない。

a）当該個人データ又は第三者提供記録の存否が明らかになることによって、本人又は第三者の生命、身体又は財産に危害が及ぶおそれのあるもの

b）当該個人データ又は第三者提供記録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する、又は誘発するおそれのあるもの

c）当該個人データ又は第三者提供記録の存否が明らかになることによって、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの

d）当該個人データ又は第三者提供記録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及び秩序維持に支障が及ぶおそれのあるもの

a)～d)に基づき、保有個人データでないと判断される個人情報を取扱うに際しては、「新規個人情報取得申請書」にて個人情報保護管理者の承認を受けるものとする。

財団は、保有個人データに該当しないが、本人から求められる利用目的の通知、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の請求などの全てに応じることができる権限を有する個人情報についても、保有個人データと同様に取り扱う。

A.3.4.4.2　開示等の請求等に応じる手続(J.10.2)

財団は、保有個人データ又は第三者提供記録の開示等の請求等に応じる手続として次の事項を定める。

a）保有個人データ又は第三者提供記録の開示等の請求等の申出先

b）保有個人データ又は第三者提供記録の開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等の方式

c）保有個人データ又は第三者提供記録の開示等の請求等をする者が、本人又は代理人であることの確認の方法

d）A.3.4.4.4 又はA.3.4.4.5 による場合の手数料（別に定める。）の徴収方法

財団は、本人からの保有個人データ又は第三者提供記録の開示等の請求等に応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。

財団は、A.3.4.4.4 又はA.3.4.4.5 によって本人からの請求などに応じる場合に、手数料を徴収するときは、実費を勘案して合理的であると認められる範囲内において、その額を定めなければならない。

開示等の請求等に応じる手続は、次の通りとする。本人から電磁的手続きによることの要望を受けた場合は、原則として本人の要望に合わせた対応を行う。

e）開示等の求めの申出先

本人からの開示等の求めの申出先は、原則として個人情報問合せ窓口とする。

f）開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等の方式

本人より「保有個人データ開示等請求書」の提出を必要とする。

g）本人又は代理人であることの確認方法

本人確認が可能な財団への登録情報の 2 項目程度を上記ｆ）の書面と同時に受け取るか、ｆ）の書面を受け取り後、問合せる等の手続きにより本人確認を行う。

h）代理人による開示等の求めの場合

代理人による開示等の求めの場合、前記 g）に加えて、代理権が確認できる下記 1）の書類の写しいずれか及び代理人自身を証明する 2）の書類の写しのいずれかを必要とする。

1）代理人である事を証明する書類

＜開示等の求めをすることにつき本人が委任した代理人の場合＞

・本人の委任状

＜代理人が未成年者の法定代理人の場合＞

・戸籍謄本

・住民票（続柄の記載されたもの　個人番号が記載されていないもの）

・その他法定代理権の確認ができる公的書類

＜代理人が成年被後見人の法定代理人の場合＞

・後見登記等に関する登記事項証明書

・その他法定代理権の確認ができる公的書類

2）代理人自身を証明する書類（本籍地の情報は都道府県以外を、個人番号は全桁を非表示としたうえで収集するものとする）

・運転免許証

・パスポート

・健康保険の被保険者証（被保険者等記号・番号等を全て非表示としたもの）

・住民票（個人番号が記載されていないもの）

i）開示等の求めに係る手数料等

1）手数料は、無料とする。

2）個人データの写しの交付を受ける者は、公益財団法人堺市文化振興財団個人情報の保護に関する法律施行規程に定める費用を負担する。

A.3.4.4.3 保有個人データに関する事項の周知など(J.10.3)

財団は、当該保有個人データ又は第三者提供記録に関し、次の事項を本人の知り得る状態（本人の請求などに応じて遅滞なく回答する場合を含む。）に置く。

a）財団の名称及び住所並びに代表者名
b）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
c）全ての保有個人データの利用目的［A.3.4.2.4 の a）～c）までに該当する場合を除く。］
d）保有個人データの取扱いに関する苦情の申出先
e）当該組織が認定個人情報保護団体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出先
f）A.3.4.4.2 によって定めた手続
g）保有個人データの安全管理のために講じた措置（本人の知り得る状態に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）

本人が知り得る状態とする方法は、次の通りとする。
h）a）～g）の事項については予め文書化し、個人情報保護管理者の承認を得た上で財団ホームページにて公表することとする。
i）本人からの求めがあった場合には苦情相談窓口責任者が応じることとし、遅滞なく文書にて送付することとする。

A.3.4.4.4 保有個人データの利用目的の通知(J.10.4)

財団は、本人から、当該本人が識別される保有個人データについて、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る。ただし、A.3.4.2.4 のただし書き a）～c）のいずれかに該当する場合、又は A.3.4.4.3 の c）によって当該本人が識別される保有個人データ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ないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明する。

保有個人データについて利用目的の通知を求められた場合、原則として本人から「保有個人データ開示申出書」を提出してもらい、その記載内容に基づいて以下の通り処理を実施する。
a）保有個人データを調査の上、必要事項を確認する。
b）「苦情・相談等受付処理票」に必要事項を記入する。
c）苦情相談窓口責任者と個人情報保護管理者で対応を協議し、本人への回答内容を立案する。但し、本規程 A.3.4.2.4 のａ）～ｃ）に該当する場合、又は A.3.4.4.3ｃ）によって利用目的が明らかであるという理由により、利用目的通知の求めに応じない場合、その理由の説明について立案する。
d）c）について、個人情報保護管理者の承認を得る。
e）利用目的についての本人への回答（求めに応じない場合はその旨の回答と c）で立案した理由の説明）は以下のいずれかの方法で行う。
1）登録されている本人住所に回答文面を郵送する。
2）登録されている本人の FAX 番号に回答文面を FAX する。
3）登録されている本人のＥメールアドレスに回答文面をメールする。
4）登録されている本人の電話番号に電話をかけ、口頭にて回答する。

A.3.4.4.5 保有個人データの開示(J.10.5)

財団は、本人から、当該本人が識別される保有個人データ又は第三者提供記録の開示（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む。）の請求を受けたときは、法令の規定によって特別の手続が定められている場合を除き、本人に対し、遅滞なく、電磁的記録の提供も含めて当該本人が指定した方法（当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法）によって開示する。ただし、開示することによって次の a）～c）のいずれかに該当する場合は、その全部又は一部を開示する必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明する。

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

b）当該組織の業務の適正な実施に著しい支障を及ぼすおそれがある場合

c）法令に違反する場合

開示を求められた場合、原則として本人から「保有個人データ開示申出書」を提出してもらい、その記載内容に基づいて以下の通り処理を実施する。

d）保有個人データ又は第三者提供記録を確認の上、必要事項を確認する

e）「苦情・相談等受付処理票」に必要事項を記入する。

f）苦情相談窓口責任者と個人情報保護管理者で対応を協議し、本人への回答内容を立案する。但し、ａ）～ｃ）に該当する場合で開示の求めに応じない場合、その理由の説明について立案する。

g）f）について、個人情報保護管理者の承認を得る。

h）開示についての本人への回答（求めに応じない場合はその旨の回答と A.3.4.4.5 の f）で立案した理由の説明）は A.3.4.4.4 の e）に従って行う。

A.3.4.4.6 保有個人データの訂正、追加又は削除(J.10.6)

財団は、本人から、当該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いう理由によって当該保有個人データの訂正、追加又は削除（以下、この項において“訂正等”という。）の請求を受けた場合は、法令の規定によって特別の手続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、当該保有個人データの訂正等を行う。また、財団は、訂正等を行ったときは、その旨及びその内容を、本人に対し、遅滞なく通知し、訂正等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、遅滞なく通知する。

訂正等を求められた場合、原則として本人から「保有個人データ開示申出書」を提出してもらい、その記載内容に基づいて以下の通り処理を実施する。

a）訂正内容、訂正目的、保有する現データとの違いを確認し、必要な訂正事項を確認する。

b）「苦情・相談等受付処理票」に必要事項を記入する。

c）苦情相談窓口責任者と個人情報保護管理者で対応を協議し、本人への回答内容を立案する。また調査の結果、訂正、追加、削除の求めに応じない場合は、その理由の説明について立案する。

d）c）について、個人情報保護管理者の承認を得る。

e）訂正等についての本人への回答は A.3.4.4.4 の e）に従って行う。

A.3.4.4.7 保有個人データの利用又は提供の拒否権(J.10.7)

財団が、本人から当該本人が識別される保有個人データの利用の停止、消去又は第三者への提供の停止（以下、この項において“利用停止等”という。）の請求を受けた場合は、これに応じる。また、措置を講じた後は、遅滞なくその旨を本人に通知する。ただし、A.3.4.4.5 のただし書き a）～c）のいずれかに該当する場合は、利用停止等を行う必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明する。

利用停止等を求められた場合、原則として本人から「保有個人データ開示申出書」を提出してもらい、その記載内容に基づいて以下の通り処理を実施する。

a）保有する現データと利用目的、提供先等を確認し、依頼の妥当性を確認する。

b）「苦情・相談等受付処理票」に必要事項を記入する。

c）苦情相談窓口責任者と個人情報保護管理者で対応を協議し、本人への回答内容を立案する。但し、A.3.4.4.5 のａ）～ｃ）に該当する場合で利用停止等の求めに応じない場合、その理由の説明について立案する。

d）c）について、個人情報保護管理者の承認を得る。

e）利用停止等についての本人への回答（求めに応じない場合はその旨の回答と c）で立案した理由の説明）は、A.3.4.4.4 の e）に従って行なう。

A.3.4.5 認識(J.4.3)

財団は、従業者が JISQ15001 7.3 に規定される認識をもつために、関連する各所属及び階層における次の事項を認識させる手順を確立し、かつ、維持する。

a）個人情報保護方針（内部向け個人情報保護方針及び外部向け個人情報保護方針）

b）PMS に適合することの重要性及び利点

c）PMS に適合するための役割及び責任

d）PMS に違反した際に予想される結果

財団は、認識させる手順に、全ての従業者に対する教育を少なくとも年一回、適宜に行うことを含める。

認識させる手順は、次の通りとする。

e）教育の対象範囲

教育の対象範囲は、財団の全従業者とする。

f）個人情報保護管理者の責務

個人情報保護管理者は、教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらの記録に関する責任と権限を有する。

g）教育計画の策定

個人情報保護管理者は、毎年 4 月に年間教育計画を作成し、トップマネジメントの承認を得なければならない。

h）教育の実施

1）教育は、教育計画に基づいて実施し、受講対象者が全て受講したことを記録しなければならない。

2）受講者は、教育受講時、理解度、自覚度を確認するために原則としてテスト等を受けなければならない。

3）個人情報保護管理者はテスト等にて受講者の理解度を把握する。その際、理解度の低い受講者に対しては再教育等を行い、所定の水準に達したことを確認するものとする。

i）実施報告

個人情報保護管理者は、教育の実施記録を作成し、トップマネジメントの承認を得なければならない。

A.3.5 文書化した情報

A.3.5.1 文書化した情報の範囲(J.4.5.1)

財団は、次の PMS の基本となる要素に対応する書面を作成する。

a）個人情報保護方針

b）内部規程

c）内部規程に定める手順上で使用する様式

d）計画書

e）プライバシーマークにおける PMS 構築・運用指針が要求する記録

f）その他、財団が PMS を実施する上で必要と判断した文書（記録を含む。）を書面で記述する。

A.3.5.2 文書化した情報（記録を除く。）の管理(J.4.5.3)

財団は、JISQ15001 が要求する全ての文書化した情報（記録を除く。）を管理する手順を確立し、実施し、かつ、維持しなければならない。

文書化した情報（記録を除く。）の管理の手順には、次の事項が含まれなければならない。

a）文書化した情報（記録を除く。）の発行及び改正に関すること

b）文書化した情報（記録を除く。）の改正の内容と版数との関連付けを明確にすること

c）必要な文書化した情報（記録を除く。）が必要なときに容易に参照できること

d）適切性及び妥当性に関する、適切なレビュー及び承認を行うこと

文書管理は次の手順にて行う。

e）文書の発行

1）新規に PMS 文書を発行するに際しては、原則として、文書番号、版番号又はそれに代わる識別情報、制定日、発行者を明記しておくものとする。ただし様式類、記録類を除く。

2）発行の際は、適切性及び妥当性に関する、適切なレビューを行い、事前に所定の承認を得なければならない。

f）文書の改訂

1）個人情報保護管理者は、PMS 文書を必要に応じて適宜改訂するものとする。改訂に際しては、改訂履歴に改訂日と改訂内容を残し、版番号を更新することとする。

2）改訂は次の要因を把握して行うものとする。

・本規程 A.3.7.3 に定めるマネジメントレビュー

・PMS の管理方法、手順に変更が生じた場合

・文書の正確性や文書間の整合性を維持するために必要な場合

g) 個人情報保護管理者は、必要に応じて関係者の誰もが PMS 文書にアクセスできるような手段を講ずる。また、PMS 文書は、常に最新版の閲読または入手可能な便宜を図り、旧版あるいは無効の PMS 文書の返却または廃棄の指示と管理を関係者に対して行う。

A.3.5.3 文書化した情報のうち記録の管理(J.4.5.5)

財団は、PMS 及び JISQ15001 の要求事項への適合を実証するために必要な記録として、次の事項を含む記録を作成し、かつ、維持する。

a) 個人情報の特定に関する記録
b) 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
c) 個人情報保護リスクの認識、分析及び対策に関する記録
d) 計画書
e) 利用目的の特定に関する記録
f) 保有個人データに関する開示等（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）の請求等への対応記録
g) 教育などの実施記録
h) 苦情及び相談への対応記録
i) 運用の確認の記録
j) 内部監査報告書
k) 是正処置の記録
l) マネジメントレビューの記録

財団は、記録の管理についての手順を確立し、実施し、かつ、維持する。

記録管理は次の手順にて行う。

m) 記録について具体的な書類、データ等を特定し、保管、保護、保管期間及び廃棄の手順を定めて「PMS 記録管理シート」で管理、維持する。
n) 記録類は、必要とするときにはすぐに検証できるようにしておく。
o) 記録に個人情報が含まれる場合は、当該記録は個人情報として特定し、関連規定に従って取り扱う。

A.3.6 苦情及び相談への対応(J.8.10、J.11.1)

財団は、個人情報の取扱い及び PMS 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、維持する。
財団は、上記の目的を達成するために必要な体制の整備を行う。

本人からの苦情及び相談に対応する手順は、次の通りとする。

a) 体制
苦情及び相談には、個人情報問合せ窓口が対応する。苦情相談窓口責任者は、個人情報問合せ窓口を統括する。
b) 対応手順
1) 苦情及び相談の受け付け

受付者は、苦情及び相談の内容を「苦情・相談等受付処理票」に記入する。

2）電話の場合、受付者は問い合わせ内容等を確認したら、一旦電話を切り、苦情相談窓口責任者に報告する。

3）苦情相談窓口責任者は、事業への影響度を含めて苦情等の内容をトップマネジメントと個人情報保護管理者に報告する。

4）問合せ内容に応じて、苦情相談窓口責任者並びに関連所属と協議を行い、回答方針案を作成する。

5）回答内容について、トップマネジメントと個人情報保護管理者の承認を得た上で、原則として書面により速やかに本人へ連絡する。

6）苦情相談窓口責任者は、苦情や相談の内容と対応結果を、個人情報保護管理者およびトップマネジメントに報告する。

c）処理結果の記録

苦情・相談等の対応結果は、「苦情・相談等受付処理票」に記録し、苦情相談窓口責任者が保管する。

d）苦情の処理が終わった後、本規程 A.3.8（是正処置）に基づき、再発防止のため苦情の根本原因を明確にし、必要に応じ是正処置を実施することとする。

仮名加工情報の取扱いに関する苦情の適切かつ迅速な対応を行う。

A.3.7 パフォーマンス評価

A.3.7.1 運用の確認(J.6.1)

財団は、PMS が適切に運用されていることが組織の各所属において定期的に、及び適宜に確認されるための手順を確立し、実施し、かつ、維持しなければならない。

各所属長は、定期的に、及び適宜に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、その是正処置を行わなければならない。

個人情報保護管理者は、トップマネジメントによる PMS の見直しに資するため、定期的に、及び適宜にトップマネジメントにその状況を報告しなければならない。

運用の確認は、次の手順で行う。

a）各所属長は、日常の業務で個人情報が所属内で規程通り取り扱われているか、また法令等に違反していないかを「個人情報保護運用チェックリスト」により 3 か月に 1 回、及び適宜に確認し、その結果を個人情報保護管理者に報告し、承認を得るものとする。

A.3.7.2 内部監査(J.6.2)

財団は、PMS の JISQ15001 への適合状況及び PMS の運用状況を少なくとも年一回、適宜に監査する。

財団は、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、維持する。

個人情報保護監査責任者は、監査員に、自己の所属する部署の内部監査をさせてはならない。

監査の手順は次の通りとする。

a）監査対象範囲

監査対象範囲は、財団の全ての部署、及び個人情報保護管理者とする。

b）監査時期

監査の実施時期は、次の通りとする。

1）PMS の JISQ15001 への適合状況及び運用状況の監査は年１回、原則として毎年 12 月にこれを実施する。なお、運用状況の監査には、リスク分析の結果、講じることとした対策の実施状況の監査も含める。

2）PMS の修正等が実施された場合は、それに即して適時に監査を実施する。

3）その他必要に応じて随時監査を実施する。

c）監査計画

個人情報保護監査責任者は、毎年 4 月に監査の実施についての「内部監査計画書」を作成し、トップマネジメントの承認を受ける。また、必要に応じて「個別監査計画書」を作成し、関係者のスケジュールを調整する。

d）監査実施

1）監査人は監査計画に基づき、チェックリスト等を用いて現場責任者へのヒアリング、文書記録類の確認、現場視察により監査を実施する。

2)個人情報保護監査責任者は､使用したチェックリスト等その他の監査実施記録を保管する。

e）監査報告

個人情報保護監査責任者は、監査結果を「内部監査報告書」に取りまとめ、トップマネジメントに報告し承認を受ける。

A.3.7.3 マネジメントレビュー(J.6.3)

トップマネジメントは、JISQ15001 9.3 に規定されるマネジメントレビューを実施するために、少なくとも年一回、適宜に PMS を見直さなければならない。

マネジメントレビューにおいては、次の事項を考慮しなければならない。

a）前回までのマネジメントレビューの結果を踏まえた見直しの状況

b）PMS に関連する外部及び内部の問題点の変化

c)以下の状況を踏まえた、現在の PMS の運用状況の評価

1）不適合及び是正処置

2）確認及び点検の結果

3）監査結果

4）個人情報保護目的の達成

d）利害関係者からのフィードバック

e）リスクアセスメントの結果及びリスク対応計画の状況

f）継続的改善の機会

マネジメントレビューからのアウトプットには、継続的改善の機会及び PMS のあらゆる変更の必要性に関する決定を含める。

マネジメントレビューを実施する手順は、次の通りとする。

g）マネジメントレビューは、原則として毎年 12 月、及び必要に応じて随時行う。

h）個人情報保護管理者は、マネジメントレビューの結果を「マネジメントレビュー記録」に取

りまとめ、トップマネジメントの承認を受ける。

A.3.8 是正処置(J.7.1)

財団は、次の事項を含めて、不適合に対する是正処置を実施するための責任及び権限を定める手順を内部規程として文書化する。

a) その不適合に対処し、該当する場合には、必ず、次の事項を行う。
   1) その不適合を管理し、修正するための処置をとる。
   2) その不適合によって起こった結果に対処する。
b) 次の事項によって、その不適合の原因を除去するための処置を検討する。
   1) その不適合を調査及び分析する。
   2) その不適合の原因を特定する。
   3) 類似の不適合の有無、又はそれが発生する可能性を検討する。

c) 是正処置を計画し、計画された処置を実施する。
d) 実施された全ての是正処置の有効性を調査、分析及び評価する。
e) 必要な場合には、PMS の改善を行う。

不適合が明らかとなった場合、a)～e)の事項を実施する。
a) ～e) の実施結果について、文書化した情報を保持するとともに、原則として、トップマネジメントが承認する。

是正処置を実施する手順は、次の通りとする。

f) 処置の基本
是正処置は、問題の大きさに対して適切な程度とし、考えられるリスクに釣り合う程度とすることが、処置の基本である。

g) 是正処置の入力情報は、次の通りとする。
1) パフォーマンス評価 (A.3.7) により明らかになった不適合
2) 緊急事態の原因となった不適合
3) 苦情や相談により明らかになった不適合
4) 外部機関の指摘により明らかになった不適合

h) 是正処置の実施手順
是正処置は、次の手順に従い実施する。
1)是正処置の必要な事象を発見した者は、「是正処置実施記録」により当該所属長の確認を得て、個人情報保護管理者およびトップマネジメントの承認を受ける。
2) 当該所属長は、指摘内容の根本原因を特定し、処置計画を立案する。
3) 当該所属長は、不適合の内容、根本原因、処置計画が記入された「是正処置実施記録」を提出し、個人情報保護管理者およびトップマネジメントの承認を受ける。
4) 当該所属長は、承認された処置計画に従って処置を実施する。
5) 当該所属長は、処置結果を記載した、「是正処置実施記録」を個人情報保護管理者に提出し、

承認を得る。

6）個人情報保護管理者は、処置結果についての有効性のレビュー（効果確認）を実施し、その結果を「是正処置実施記録」に記載し、トップマネジメントに報告する。