

文書番号	
制定日	
改訂日	
改訂版数	1

# 個人情報保護基本規程

SAMPLE

承認	作成

株式会社〇〇〇〇〇

# 個人情報保護基本規程

文書番号

改訂版数

1

## 【目次】

0. 目的	1
1. 適用範囲	1
2. 適用基準	1
3. 用語及び定義	1
4. 個人情報保護マネジメントシステム	3
J.1 組織の状況	3
J.1.1 組織及びその状況の理解	3
J.1.2 利害関係者のニーズ及び期待の理解	3
J.1.3 法令、国が定める指針その他の規範	3
J.1.4 個人情報保護マネジメントシステムの適用範囲の決定	4
J.1.5 個人情報保護マネジメントシステム	4
J.2 リーダーシップ	4
J.2.1 リーダーシップ及びコミットメント	4
J.2.2 個人情報保護方針	4
J.2.3.1 組織の役割、責任及び権限	5
J.2.3.2 個人情報保護管理者と個人情報保護監査責任者	5
J.2.4 管理目的及び管理策(一般)	6
J.3 計画	6
J.3.1.1 個人情報の特定	6
J.3.1.2 リスク及び機会に対処する活動(一般)	6
J.3.1.3 個人情報保護リスクアセスメント	7
J.3.1.4 個人情報保護リスク対応	10
J.3.2 個人情報保護目的及びそれを達成するための計画策定	10
J.3.3 計画策定	11
J.4 支援	11
J.4.1 資源	11
J.4.2 力量	11
J.4.3 認識	12
J.4.4.1 コミュニケーション	12
J.4.4.2 緊急事態への準備	13
J.4.5.1 文書化した情報(一般)	14
J.4.5.2 文書化した情報の管理	15
J.4.5.3 文書化した情報(記録を除く)の管理	16
J.4.5.4 内部規程	16
J.4.5.5 文書化した情報のうち、記録の管理	18
J.5 運用	18
J.5.1 運用	18

個人情報保護基本規程	文書番号	
	改訂版数	1

J.6 パフォーマンス評価	19
J.6.1 監視、測定、分析及び評価	19
J.6.2 内部監査	19
J.6.3 マネジメントレビュー	21
J.7 改善	22
J.7.1 不適合及び是正処置	22
J.7.2 継続的改善	22
J.8 取得、利用及び提供に関する原則	23
J.8.1 利用目的の特定	23
J.8.2 適正な取得	23
J.8.3 要配慮個人情報	23
J.8.4 個人情報を取得した場合の措置	24
J.8.5 J.8.4のうち本人から直接書面によって取得する場合の措置	25
J.8.6 利用に関する措置	26
J.8.7 本人に連絡又は接触する場合の措置	27
J.8.8 個人データの提供に関する措置	28
J.8.8.1 外国にある第三者への提供の制限	29
J.8.8.2 第三者提供に係る記録の作成など	30
J.8.8.3 第三者提供を受ける際の確認など	31
J.8.8.4 個人関連情報の第三者提供の制限など	32
J.8.9 匿名加工情報	33
J.8.10 仮名加工情報	34
J.9 適正管理	35
J.9.1 正確性の確保	35
J.9.2 安全管理措置	36
J.9.3 従業者の監督	36
J.9.4 委託先の監督	36
J.10 個人情報に関する本人の権利	38
J.10.1 個人情報に関する権利	38
J.10.2 開示等の請求等に応じる手続	38
J.10.3 保有個人データ又は第三者提供記録に関する事項の周知など	39
J.10.4 保有個人データの利用目的の通知	39
J.10.5 保有個人データ又は第三者提供記録の開示の開示	40
J.10.6 保有個人データの訂正、追加又は削除	41
J.10.7 保有個人データの利用又は提供の拒否権	41
J.11 苦情及び相談への対応	42
J.11.1 苦情及び相談への対応	42
改訂歴表	43

個人情報保護基本規程

文書番号

改訂版数

1

SAMPLE

## 0. 目的

- (1) 本規程は、株式会社〇〇〇〇〇〇（以下、当社という）の個人情報保護に関する取組み及び考  
え方並びに遵守すべき事項を、JIS Q 15001:2017(個人情報保護マネジメントシステム-要求  
事項)に基づいた「プライバシーマークにおける個人情報保護マネジメントシステム構築・  
運用指針」の要求事項を満たすよう規定したものである。
- (2) 本規程は、当社の個人情報保護に関する管理レベルの維持・向上、本人への安心感の提供  
と満足度の向上を図ることを目的とする。

## 1. 適用範囲

- (1) 当社の個人情報保護マネジメントシステムは、当社の事業の従事する全ての従業者(役  
員、監査役、正社員、派遣社員、契約社員、嘱託社員、パート社員、アルバイト社員等)を  
対象とする。
- (2) 当社の個人情報保護マネジメントシステムは、当社の事業の用に供する全ての個人情報  
に適用する。

## 2. 適用基準

- (1) 当個人情報保護基本規程は、当社における個人情報保護を規定する最高位の文書であっ  
て、以下の基準の要求事項を適用し作成している。
- ① JISQ15001:2017(個人情報保護マネジメントシステム—要求事項)
  - ② プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針
- (2) 当個人情報保護基本規程および関連文書は、基準が改訂された場合、あるいはより信頼  
性を高めるために、必要な場合に改訂する。

## 3. 用語及び定義

- (1) 本規程で使用する用語は、以下の基準に準拠する。  
JISQ15001:2017(個人情報保護マネジメントシステム—要求事項)
- (2) 主な用語の定義

個人情報 (個人情報保護法の定義)	生存する個人に関する情報であって、以下のいずれかに該当するもの。 ・当該情報に含まれる氏名、生年月日その他の記述等によって特定の個人を識別できるもの(他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む)。 ・個人識別符号が含まれるもの。
個人番号	番号法の規定により、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。
特定個人情報	個人番号をその内容に含む個人情報をいう。
本人	個人情報によって識別される特定の個人。
組織	責任及び権限を持つトップマネジメントが存在し、自らの目的を達成するため、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。
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。
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。
従業者	個人情報取扱事業者の組織内にあつ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、アルバイト社員など)だけでなく、雇用関係にない従事者(取締役、執行役、理事、監査役、監事、派遣社員など)も含まれる。
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・通信、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。
個人情報保護マネジメントシステム(PMS)	事業者が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。
個人番号関係事務	番号法に規定される個人番号の利用範囲(税・社会保障及び災害対策)に関して、行われる他人の個人番号を必要な限度で利用して行う事務。
個人番号関係事務実施者	個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託をうけた者。
要配慮個人情報	本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないように、その取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報。
匿名加工情報	特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であつて、当該個人情報を復元することができないようにしたもの。
仮名加工情報	他の情報と照合しない限り特定の個人を識別できないように個人情報を加工して得られる個人に関する情報。
適合	要求事項を満たしていること。
不適合	要求事項を満たしていないこと。

#### 4. 個人情報保護マネジメントシステム

注記：以降の項目番号は、「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」の項目番号と一致させている。

##### J.1 組織の状況

###### J.1.1 組織及びその状況の理解

- (1) トップマネジメント及び個人情報保護管理者は、個人情報を取り扱う当社事業に関して、個人情報保護マネジメントシステムに影響を与えるような外部及び内部の課題を特定すること。
- (2) 特定する際には、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、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(人員・組織基盤・資金)、セキュリティ対策等の観点から、現状のみならず、将来実施するであろう事業を踏まえて洗い出すこと。
- (3) 特定した結果は、「外部及び内部の課題一覧表」に記録すること。

###### J.1.2 利害関係者のニーズ及び期待の理解

- (1) トップマネジメント及び個人情報保護管理者は、次の事項を特定すること。
  - ① 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(本人及び個人情報保護マネジメントシステムに関連する個人、事業者及び団体(委託元及び委託元の顧客)、委託先等)
  - ② その利害関係者の、個人情報保護に関連する要求事項(法令、官公庁等のガイドライン、当社の所属団体による自主規制、商慣習に基づき遵守が求められる事項、取引先等との間の契約上の義務等のニーズ及び期待)
- (2) 特定した結果は、「利害関係者からのニーズ及び期待一覧表」に記録すること。

###### J.1.3 法令、国が定める指針その他の規範

- (1) 個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し、参照(遵守)すること。
- (2) 法令、国が定める指針その他の規範の特定
  - ① 個人情報保護管理者は、個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し、「個人情報の取扱いに関する法令、指針及び規範の一覧表」に登録し、承認すること。
  - ② 「個人情報の取扱いに関する法令、指針及び規範の一覧表」は、公布年月日、最終改正日、URL等を記載し、参照と改正状況が明確になるようにすること。
- (3) 法令、国が定める指針その他の規範の見直し
  - ① 個人情報保護管理者は、年1回(4月)に、特定した法令、国が定める指針その他の規範に関する最新情報をインターネット等を利用して確認し、改正の有無を確認すること。
  - ② 改正が当社事業に関係する場合には、「個人情報の取扱いに関する法令、指針及び規範の一覧表」を修正し、承認すること。