# 個人情報保護管理規程（PMS 規程）

## 第 1 章　総則

（目的）
第 1 条　本規程は、個人情報保護マネジメントシステム（PMS）を構築・運用・維持することによって、当社における個人情報の保護を確実に実施することを目的とする。

（適用範囲）
第 2 条　本規程は、当社が事業の用に供して取り扱うすべての個人情報及びその取扱いに関与する全役職員（正社員、契約社員、派遣社員、パートタイム社員等を含む）に適用する。

## 第 2 章　用語の定義

（定義）
第 3 条　本規程で使用する用語は、JIS Q 15001:2017 に準拠する。

【参考】JIS Q 15001:2017 における「個人情報」の定義
この JIS で用いられている主な用語の定義は、JIS 内で定義されているほか、個人情報保護法に定義されている用語を用いている。
「個人情報」は、個人情報保護法 2 条 1 項で以下のように定義されている。

> **第 2 条**　この法律において**「個人情報」**とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
>
> 一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第 2 号において同じ。）で作られる記録をいう。第 18 条第 2 項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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できることとなるものを含む。）
>
> 二　個人識別符号が含まれるもの

要約すると「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できることとなるものを含む）及び個人識別符号が含まれるものである。

具体例）

特定の個人を識別できる情報とは、氏名、生年月日、住所、電話番号、メールアドレス、顧客番号、会員 ID などである（他情報と照合することで識別できるものも含む）

個人識別符号を含む情報とは、身体的特徴などとしては顔画像、指紋データ、虹彩、声紋データ などであり、公的番号としてはマイナンバー（個人番号）、パスポート番号、運転免許証番号、保険証番号 などである。

## 第 3 章　組織体制

（個人情報保護管理責任者の任命と責任）
第 4 条　当社は、個人情報の管理を統括する責任者として個人情報保護管理責任者を任命する

（役割と責任）
第 5 条　当社の全役職員は、個人情報保護方針を理解・遵守し、個人情報保護管理責任者と共になって個人資産の保護に努めるものとする。

## 第 4 章　管理責任者の責務

（責務）
第 6 条　個人情報保護方針は、会社の定めた個人情報保護方針に基づき、PMS の確立、実施・運用、維持、継続的改善に関する責任を負う。

（教育）
第 7 条　個人情報保護管理責任者は、社員に対する教育・訓練を入社時および定期的に実施（年 1 回）する。
入社時の個人情報保護に関する教育実施後に、全ての社員に誓約書を提出させる。

（監査）
第 8 条　個人情報保護管理責任者は、内部監査を定期的に実施（年 1 回）し、PMS 運用状況を把握し、必要な対策、改善を継続的に行う。

（委託先の管理：選定・契約・監督）
第 9 条　個人情報保護管理責任者は、個人情報の取扱いを委託する際、個人情報保護に関する内容が記載されている秘密保持契約を締結し、適切な管理状況を確立する。

## 第 5 章　安全管理措置

（基本方針）
第 10 条　個人情報の漏えい、滅失、毀損等のリスクを特定し、必要な安全管理措置を講じる。

（物理的安全管理）
第 11 条　個人情報を保管する場所を特定・明確にし、個人情報を保管する区域へのアクセス制限を設け、施錠管理を行う。

（技術的安全管理）
第 12 条　個人情報を保管する媒体を特定・明確にし、パスワード管理、アクセス制御、ウイルス対策等を行う。

（人的安全管理）
第 13 条　誓約書の提出および定期教育を通じ、従業員の意識向上を図る。

（アンケート調査等における安全管理措置）
第 14 条　記名式のアンケート調査を実施するなど新たに個人情報を取得する場合は、チェックシート等を用いて個人情報の取り扱いに関する計画を立案し、個人情報保護管理責任者に相談し承認を得ること。そして、立案した計画に従って取得した個人情報の保護を確実に実施すること。

## 第 6 章　個人情報の取扱い

（利用目的の特定、通知・公表）
第 15 条　個人情報の取得にあたっては、その利用目的をできる限り特定し、本人に通知または公表する。

（取得・利用）
第 16 条　個人情報の取得にあたっては、必要最小限の個人情報に留め、本人の同意を得た上で適正に取得し、目的外利用を行わない。

（第三者提供）
第 17 条　法令に定める場合を除き、本人の同意なく第三者に提供しない。

## 第 7 章　苦情および相談への対応

（対応体制）
第 18 条　個人情報保護管理責任者は、苦情・相談受付窓口を設け、迅速かつ適切な対応を行う。





## 第 8 章　マネージメントレビュー

（マネジメントレビュー）
第 19 条　当社は、代表者によるマネジメントレビューを行い、内部監査結果を基に必要な改善措置を実施する。個人情報保護管理責任者は、PMS 運用状況、内部監査結果をマネジメントレビュー会議において報告をする。

## 第 9 章　附則

（規程の改定）
第 20 条　本規程は、必要に応じて見直しを行い、継続的に改善するものとする。

## Appendix

付属書類

- 個人情報保護に関するチェックシート
- 個人情報保護に関する教育実施記録
- 機密情報および個人情報取り扱いに関する誓約書
- 個人情報保護に関するリスク管理シート

# 個人情報取得に関するチェックシート

本チェックシートは、JIS Q 15001:2017 に基づき、個人情報の取得時に必要な手続きが適切に実施されているかを確認するためのものです。

個人情報保護に関する立案時、および監査時にチェックする項目

| チェック項目 | 確認（✓） | 備考・対応状況 |
|---|---|---|
| 1. 個人情報を取得する前に、利用目的を明確に特定しているか（第 15 条） | | |
| 2. 利用目的を、本人に対して書面または画面表示等により通知・公表しているか（第 15 条） | | |
| 3. 本人から個人情報を直接取得する場合、同意を得た上で取得しているか（第 16 条） | | |
| 4. 個人情報の取得にあたって、必要最小限の範囲に限定しているか（第 16 条） | | |
| 5. 本人の同意の取得方法（書面、同意ボタンなど）が記録として保存されているか（第 16 条） | | |
| 6. 本人が同意しなかった場合に、個人情報を取得・利用していないか（第 16 条） | | |
| 7. 個人情報を保管する場所・媒体を特定・明確にしているか（第 11、12 条） | | |
| 8. 個人情報の保管は、物理的・電子的なアクセス制限をする計画をしているか（第 11、12 条） | | |
| 9. 本人に対して、個人情報の利用目的、管理責任者、問い合わせ窓口等を明示しているか（第 18 条） | | |





| | | |
|---|---|---|
| 10. 個人情報の取得手段が公正かつ適法であることを確認しているか | | |

監査時にチェックする項目

| チェック項目 | 確認（✓） | 備考・対応状況 |
|---|---|---|
| 1. 目的外利用をしていないか（第 16 条） | | |
| 2. 法令に定める場合を除き、本人の同意なく第三者に提供しないか（第 17 条） | | |
| 3. 個人情報の保管は、物理的・電子的なアクセス制限をしているか（第 11、12 条） | | |

| 承認 | 審査 | 作成 |
|---|---|---|
| yy/mm/dd | yy/mm/dd | yy/mm/dd |
| | | |

※ 本チェックシートによるチェックを定期的に実施し、確実に個人情報の保護をすること（基本的には、内部監査前に実施することで少なくとも年１回のチェックを実施する）

社内文書

# 個人情報保護に関する教育実施記録

教育名：

実施日：　　年　　月　　日（　　）

実施場所：

講師名：

対象者：全社員／新入社員／その他（　　）

## 【教育内容の概要】

・個人情報保護法、JIS Q 15001 の概要
・社内規程の説明
・社内規定に従った安全管理措置の実務

## 【受講者記録】

| 氏名 | 所属 | 署名 | 備考 |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

以上



社内文書

# 機密情報および個人情報取扱いに関する誓約書

私は、会社の業務に従事するにあたり、職務上知り得た情報資産（機密情報および個人情報等）を適切に取扱い、以下の事項を遵守することを誓約します。

1. 在職中および退職後においても、業務上知り得た会社の営業上・技術上・業務運営上の機密情報および社員・お客様（顧客）・パートナー企業様等に関する一切の個人情報を、正当な理由なく第三者に漏えい・提供・開示しません。
2. その他の情報資産について、目的外利用、複製、改ざん、持ち出し、破棄等の不正行為を行いません。
3. 個人情報保護に関する法令、会社の個人情報保護管理規程および情報セキュリティ管理規程、その他関連する社内規程に従います。
4. 情報資産を取り扱う機器（PC、媒体等）の管理を徹底し、漏えいや紛失を防止します。
5. 業務終了後、取得した情報資産は、会社の指示または社内手続きに従って返却・削除します。
6. 退職・異動後も、在職中に知り得たすべての情報資産について、第三者に開示・使用しません。

私は、上記に違反した場合、就業規則その他の社内規程に基づく懲戒処分または法的責任を問われることがあることを承知します。

以上

年　　月　　日

所属：

氏名：　　（署名）

社内文書

# 個人情報保護に関するリスク管理シート

| 承認 | 審査 | 作成 |
|---|---|---|
| yy/mm/dd | yy/mm/dd | yy/mm/dd |
| 名前 | 名前 | 名前 |

| 項番 | 想定されるリスク | リスクが顕在化した時の影響 | 重大度（S） Severity | 発生頻度（O） Occurrence | 検出度（D） Detection | RPN（S×O×D） Risk Priority Number | 対策 | 対策後のS | 対策後のO | 対策後のD | 対策後のRPN |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | 0 | | | | | 0 |
| 2 | | | | | | 0 | | | | | 0 |
| 3 | | | | | | 0 | | | | | 0 |
| 4 | | | | | | 0 | | | | | 0 |
| 5 | | | | | | 0 | | | | | 0 |
| 6 | | | | | | 0 | | | | | 0 |
| 7 | | | | | | 0 | | | | | 0 |

説明

| | | | | |
|---|---|---|---|---|
| **S** | Severity | **重大度** | 発生した場合の影響の大きさ | 3点法で評価 |
| **O** | Occurrence | **発生度** | 発生する可能性（頻度） | 3点法で評価 |
| **D** | Detection | **検出度** | 事前に検出できる可能性 | 3点法で評価 |
| **RPN** | Risk Priority Number | **リスク優先度** | **S × O × D** によって算出されるリスクスコア（リスク評価） | RPNが10以上、または一つでも3がある場合に対策をする（ただし、重大度は下げられない場合もあるので、その場合はRPN9以下であれば良しとする） |

例）

| 指標 | 低（1） | 中（2） | 高（3） |
|---|---|---|---|
| S（重大度） | 重大問題に至る可能性の低い問題 | 重大問題に至る可能性のある問題<br>例）不正な複製など | 法令上の重大問題<br>例）個人情報の漏えい、目的外利用など |
| O（発生度） | 非常に稀れ | 年1回程度 | 月1回程度 |
| D（検出度） | ほぼ確実に検出可能 | 監査時に検出可能 | 全く検出困難 |

※　本リスク管理シートによるリスク管理を定期的に実施し、確実に個人情報の保護をすること（基本的には、内部監査前に実施することで少なくとも年１回のチェックを実施する）