1.適用範囲

【規程】

1.人的範囲

当社の個人情報保護マネジメントシステム(以下 PMS と略す)を当社の全従業者（3.42 に定義する。）に対して適用する。

2.適用対象とする個人情報

事業の用に供する全ての個人情報を PMS の適用対象とする。

【要点】

1.下記従業者も人的範囲に含まれ，教育等の対象者である。

①非常勤役員

②監査役

③社外取締役，社外監査役

④実習生

⑤ボランティア

⑥組織内の従業者と変わりがない個人情報の取扱いに従事する委託先担当者

2.下記個人情報も適用対象に含める必要がある。

①委託先が委託業務遂行のために取り扱っている個人情報

例：代行取得を委託している個人番号

②客先で受託業務を行っている場合に取り扱う個人情報

例：客先サーバ中の個人情報，客先で目に触れる個人情報

③受託業務で遠隔から取り扱う客先サーバ中の個人情報

例：リモート保守受託業務で取り扱う客先サーバ中の個人情報

2.引用規格

【規程】

1. “JIS Q 15001:2017 ”が引用する規格はない。

3.用語および定義

【規程】

当社 PMS で使用する用語を“JIS Q 15001:2017 の 3（用語及び定義）”および“個人情報の保護に関する法律”に準じて，以下に定義する。

1)“JIS Q 15001:2017 の 3（用語及び定義）”による定義

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。

3.3 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。

3.4 マネジメントシステム

方針，目的およびその目的を達成するためのプロセスを確立するための，相互に関連する又は相互に作用する，組織の一連の要素。

3.5 トップマネジメント

最高位で組織を指揮し，管理する個人又は人々の集まり。当社のトップマネジメントは，代表取締役とする。

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。

3.7 方針

トップマネジメントによって正式に表明された組織の意図及び方向付け。

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。

3.11 文書化した情報

組織によって，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。

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。

3.13 パフォーマンス

測定可能な結果。

3.14 監視

システム，プロセス又は活動の状況を明確にすること。

3.15 測定

値を決定するためのプロセス。

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。

3.17 適合

要求事項を満たしていること。

3.18 不適合

要求事項を満たしていないこと。

3.19 是正処置

不適合の原因を除去し，再発を防止するための処置。

3.20 継続的改善

パフォーマンスを向上するために繰り返し行われる活動。

3.21 分析モデル

一つ以上の基本測定量及び/又は導出測定量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の特性又は特徴。

3.23 基本測定量

単一の属性とそれを定量化するための方法とで定義した測定量。

3.24 結果

目的に影響を与える事象の結末。

3.25 管理策

リスクを修正する対策。

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，閾値，目標又はパターン。

3.27 導出測定量

複数の基本測定量の値の関数として定義した測定量。

3.28 事象

ある特有な状況の出現又は変化。

3.29 起こりやすさ

何かが起こる見込み。

3.30 測定量

測定の結果として値が割り当てられる変数。

3.31 測定の関数

複数の基本測定量を結合するために遂行するアルゴリズム又は計算。

3.32 測定方法

特定の尺度に関して属性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。

3.33 対象物

属性の測定を通して特徴付けられるもの。

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，それに属性を対応付けるもの。

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，望ましくない事象の潜在的な原因。

3.36 ぜい弱性

一つ以上の脅威によって付け込まれる可能性のある，資産又は管理策。

3.37 残留リスク

リスク対応後に残っているリスク。

3.38 リスク対応

リスクを修正するプロセス。

3.39 本人（法　第2条　第8項と同一）

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の内部に属する者の中から指名された者であって，PMSの計画・実施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の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，実習生、ボランティアなど）も含まれる。

なお、組織の指揮監督を受けない業務委託された従業者であっても，個人情報の取扱いが組織内の従業者と変わりがない場合は，従業者に含めて適用する。

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の脅威が顕在化した状況。

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。

2)個人情報保護法による定義：()内に引用元法の条項等を記述する。

3.47 個人情報(第 2 条　第 1 項)

生存する個人に関する情報であって，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よって特定の個人を識別することができることとなる情報および個人識別符号を含む。

3.48 個人識別符号(第 2 条　第 2 項)

政令で定めるものであって，顔認識・指紋データ等の生体情報等，特定の個人を識別することができるもの。もしくは，個人に発行されるカード等に記載され，若しくは電磁的方式により記録された文字，番号，記号その他の符号であって，特定の本人を識別することができるものをいう。

3.49 要配慮個人情報(第 2 条　第 3 項)

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をいう。以下に主要関連法令等を記載する。

a) 施行規則　第 5 条（要配慮個人情報）

b) 政令　第 2 条（要配慮個人情報）

3.50 個人情報データベース等(第 2 条　第 4 項)

個人情報を含む情報の集合物であって，検索することができるように体系的に構成したもの。

3.51 個人情報取扱事業者(第 2 条　第 5 項)

個人情報データベースを事業の用に供している事業者をいう。

3.52 個人データ(第 2 条　第 6 項)

個人情報データベースを構成する個人情報をいう。

3.53 保有個人データ(第 2 条　第 7 項)

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を行うことのできる権限を有する個人データであって,その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のものをいう。

3.54 本人(第 2 条　第 8 項)：3.39 本人に前出

3.55 匿名加工情報(第 2 条　第 9 項)

個人情報に含まれる記述等の一部を，個人情報委員会規則に従って，復元することの

できない方法により削除，あるいは他の記述等に置き換え，もしくは，個人識別符号の全部を削除することにより，特定の本人を識別することができないようにしたものをいう。

3.56 匿名加工情報取扱事業者(第 2 条　第 10 項)

匿名加工情報を事業の用に供している事業者をいう。

3)その他の定義

3.57 個人情報保護マネジメントシステム(PMS と略す。)

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。

PMS は“Personal information protection Management System”の略称

3.58 本人の同意

本人が個人情報の取扱いに関する情報を与えられた上で，自己に関する個人情報の取扱いについて承諾する意思表示のこと。本人が子ども又は事理を弁識する能力を欠く者の場合は，法定代理人等の同意も得なければならない。

3.59 代理人

法律で定められた親権者，又は家庭裁判所で認められた後見人，本人が選定した任意代理人などをいう。

3.60 目的外利用

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。

3.61 提供

提供には以下の概念がある。

a)委託

委託業務遂行目的で，委託元が委託先に個人情報を受け渡す。個人情報の管理責任は委託元にある。

b)第三者提供

あらかじめ本人の同意を得てから，第三者に個人情報を受け渡す。個人情報を渡した後の管理責任については受け取った第三者が負う。

c)共同利用

複数の組織が個人情報を共同で利用する。

A.3 管理目的及び管理策

A.3.1 一般

A.3.1.1 一般

【規程】

A3.2 から A3.8 の管理策については，トップマネジメントによって権限を与えられた者が，当社が定めた手段に従って承認を行う。

【要点】

1.PMS 上の管理策の承認手順を定めて確実に実行する。

A.3.2 個人情報保護方針

A.3.2.1 内部向け個人情報保護方針

【規程】

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る。

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)PMS 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る。

【要点】

1.内部向け個人情報保護方針を規程文書として定め，全従業者に周知徹底させ，必要に応じて，利害関係者が入手可能にする。利害関係者には，委託先，協業などの取引先が含まれる。

2. “A.3.2.1”と“A.3.2.2”を満たした個人情報保護方針を定め，内部向けと外部向けで兼用することができる。

【手順】

1.以下の内容を盛り込んだ規程文書としての個人情報保護方針を作成し，トップマネジメントの承認を得て制定する。

①事業内容

②個人情報保護の理念

③a)～f)の事項

④制定日

⑤最終改正日：改正した場合のみ

2.規程文書と同一内容の個人情報保護方針を従業者に周知徹底させる。

(1)以下のいずれかの方法を組み合わせて，従業者が容易に入手できるようにする。

①サーバ上の共有フォルダに個人情報保護方針を掲載

②個人情報保護方針を載せた印刷物を常備し，随時閲覧可能にする。

③社内に掲示

(2)教育の中で繰り返し，説明し，充分に理解させる。

3.以下のいずれかの方法を組み合わせて，利害関係者が容易に入手できるようにする。

(1)個人情報保護方針を載せた印刷物を常備し，随時，閲覧および配布を可能にする。

(2)社内に常駐する利害関係者への教育で、個人情報保護方針を配布して説明する。

A.3.2.2 外部向け個人情報保護方針

【規程】

トップマネジメントは 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，次の事項も明記した，個人情報保護方針を文書化する。

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る。

【要点】

1.内部向け個人情報保護方針に問合せ先を追加して公表する。

2.制定年月日及び最終改正年月日については内部向け個人情報保護方針にも記載する。

【手順】

1.個人情報保護方針に関する問合せ窓口として「個人情報ご相談窓口」を設置する。外部向け個人情報保護方針には，「個人情報ご相談窓口」の連絡先情報を掲載する。

2.一般の人から要求があった場合には、個人情報保護方針を速やかに印刷して配布する。

3.当社 Web サイトを構築する際には、保有する全ての Web サイトのトップページから容易に到達できる位置に個人情報保護方針を掲載する。

4. 一般の人が訪れるオフィスを構えた際には、オフィス入口付近に個人情報保護方針を掲載する。

A.3.3 計画

A.3.3.1 個人情報の特定

【規程】

事業の用に供するすべ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，保管期限等を記載した個人情報を管理するための台帳を整備し，少なくとも年一回，適宜に確認し，最新の状態に維持する。

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。

【要点】

1. 個人情報を特定する目的

①事業の用に供するすべての個人情報を一覧にして管理対象を明確にする。

②個人情報の利用目的と取扱い方法を一覧にして周知徹底させる。

③リスク分析を行う対象を明確にする。

2. 事業の用に供する個人情報を特定する上での注意点

①取扱いを委託している個人情報も対象である。

自社内に保管していない場合でも委託先を管理監督する責任を負っている。

②常駐する客先で取り扱う個人情報及びリモートから取り扱う客先サーバ中等の個人情報等も対象である。

③閲覧あるいは目に入るだけであっても，目的外利用発生のリスクが想定される場合には特定する対象にする。

3. 個人情報の種類毎に特定する上での考慮事項

①全く取扱いが同じである個人情報は纏めて特定することは可能である。ただし，そこに含まれる個人情報が明確になっている必要がある。

②個人情報の個々の記録媒体を棚卸する等の個体管理には，「個人情報管理台帳」とは別の台帳等で管理する。

【手順】

1. 「個人情報調査表」の作成，更新

(1)「個人情報調査表」の内容(下表の通りとする)

No.	欄	記入内容
1	分類	“従業者情報”等の個人情報のカテゴリ
2	個人情報名	「個人情報管理台帳」に登録する個人情報名
3	定義	個人情報名の定義
4	書類名	総称する個人情報名中に含まれる具体的な帳票名，ファイル名
5	取得媒体	取得する媒体(紙，電子媒体，画面，メール等)
6	利用，保管媒体	利用，保管する媒体(紙，サーバ，PC，電子媒体等)
7	備考	特記事項(新規取得禁止等)

(2)「個人情報管理台帳」を新規作成する場合

①事業の用に供する全ての個人情報を記録する帳票名，ファイル名を洗い出す。

②洗い出した帳票名，ファイル名を「個人情報調査表」上に整理する。

(3)新規の種類の個人情報，書類を取得する場合

①既存の“個人情報名”に該当するものが無ければ，新たに“個人情報名”を決めて，各欄に所定の項目を記入する。

②既存の“個人情報名”に該当するものがあれば，該当する“個人情報名”の“書類名”欄に新規に取得する“書類名”を追加する。

(4)特定済の個人情報の特定内容を変更又は削除する場合

①「個人情報調査表」の特定内容に変更が必要な場合に変更する。

②特に新規利用禁止，新規取得禁止にする場合は備考欄にその旨を記入する。

2. 「個人情報取扱申請書」の作成，更新

(1)「個人情報調査表」に追加された“個人情報名”について，下表の項目を「個人情報取扱申請書」上に特定する。

(2)「個人情報調査表」で変更された“個人情報名”について，下表の項目を「個人情報取扱申請書」上で変更，削除する。

No.	欄	記入内容
1	個人情報名	「個人情報調査表」の“個人情報名”
2	取扱業務	個人情報を取り扱う業務名
3	媒体	記録する媒体（紙，サーバ，PC，電子媒体等該当するもの全て）
4	個人情報の項目	個人情報に含まれる具体的項目全て　*1
5	要配慮個人情報	含まれる要配慮個人情報名と取得根拠
6	利用目的	個人情報の具体的かつ明解な利用目的　*2
7	取得方法	“直接書面”，“書面以外”，“受託”，“提供受”を区別
8	開示対象	開示等の請求等に応じる場合に“開示”と記入
9	件数（概数）	保有している累積件数の概数　*3
10	利用権限者	利用権限を与えられる者の所属部門，職位，PMS 上の役割等
11	利用期間	利用する期間(期間計算の起点を明確にすること)
12	保管場所	媒体を保管するキャビネット，データを保管する機器名等
13	保管方法	施錠，アクセス権限設定等
14	保管期間	保管する期間(期間計算の起点を明確にすること)*4
15	提供元/委託元	“間接取得”する場合の提供元/委託元
16	連絡又は接触	本人への連絡又は接触方法と根拠
17	提供先	第三者提供がある場合の提供先
18	委託先	委託がある場合の委託先
19	廃棄・返却方法	具体的廃棄方法又は返却先

*1:氏名，住所，電話番号，年齢を基本情報とする。

*2:ここに記入されていない目的での利用は目的外利用に該当する。

*3:保管期間が短い場合は（目処として 1 年以内）期間内発生件数（/月，/年等）で記述する。

*4:利用しないが，法定期間保管する義務がある場合に注意する。

(3)「個人情報取扱申請書」を個人情報保護管理者に提出して承認を得る。

3.「個人情報管理台帳」の作成，更新と周知

(1)個人情報保護管理者は承認した「個人情報取扱申請書」に基づいて、「個人情報管理台帳」を PMS 事務局に作成又は更新させる。個人情報保護管理者は作成又は更新された「個人情報管理台帳」を承認する。

(2) PMS 事務局は共有サーバ上の「個人情報管理台帳」を最新状態に更新し，全従業者にアナウンスして周知徹底させる。

＜参照＞A.3.3.3 リスクアセスメント及びリスク 対策，A.3.4.2.6 利用に関する措置

4.「個人情報管理台帳」の見直し

(1)個人情報保護管理者は毎年「年間計画書」に定める時期に，必要に応じて適宜に，PMS 事務局に「個人情報管理台帳」の見直しを指示し，その結果を承認する。

A.3.3.2 法令，国が定める指針その他の規範

【規程】

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。

【要点】

1. 事業内容，業務内容により必要になる法令等がある。

【手順】

1.法令等の特定手順

(1)事業内容とは無関係に必要となる法令等

「法令等管理台帳」の雛型に記載済なので削除しない。

(2)事業内容に関係する法令等の洗出し

①地方公共団体から個人情報取扱い業務を受託している場合には当該地方公共団体の条例等を特定して追加する。

②事業分野（下記例参照）に関連して必要になる法令等を特定する。

労働者派遣事業

通信販売事業

保険医療福祉分野　等

④業務内容（下記例参照）に関連して必要になる法令等を特定する。

モバイル機器利用
クラウドサービス，ホスティングサービス利用
DM 発送
メルマガ送信　　等

(3)新たな事業に開始するときの法令等の追加

上記(2)の手順で，新たな事業で必要となる法令等を「法令等管理台帳」に追加する。

2.法令等の見直し手順

個人情報保護管理者は毎年「年間計画書」に定める時期に，必要に応じて適宜に，PMS 事務局に「法令等管理台帳」の見直しを指示する。

3.法令等の承認手順と社内周知

個人情報保護管理者は「法令等管理台帳」を作成及び更新の都度，承認する。承認後，PMS 事務局は全従業者が閲覧できる共有サーバ上の「法令等管理台帳」を最新状態に更新し，全従業者にアナウンスする。

A.3.3.3 リスクアセスメント及びリスク対策

【規程】

特定した個人情報について，目的外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。

特定し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，必要な対策を講じる手順を確立し，かつ， 維持する。

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。

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。

【要点】

1.目的外利用を行わないため必要な対策の具体的手順

A.3.3.1 で利用目的の特定と周知に関連して手順を定める。

A.3.4.2.6 で，目的外利用の禁止と利用目的変更の手順を定める。

2.リスク分析の基本的な考え方

個人情報を取り扱う業務の流れに沿ってリスクを洗い出して，必要な対策を洗い出し，各リスクに対する講じるべき対策を定める。

3.リスク分析を行う上での注意点

(1)残留リスク

講じるべき対策の中で，コスト的あるいは技術的に実施が困難であるため保留するものが出てくる場合が起こり得る。その時は，保留にした対策に対応するリスクが残留リスクとなり，運用の確認や内部監査で残留リスクの顕在化の兆候有無を確認する。

(2)グルーピング

業務の流れの中で取扱いが全く同じであれば,一つのグループに纏めてリスク分析を行うことは可能である。取扱いが異なる個人情報（データ化する個人情報とデータ化しない個人情報，移送・送信局面の有無が異なる等。）を一つのグループにするとリスク分析は極めて困難になる。また分析結果が大変理解し辛い内容になる。

(3)局面の流れ

実際の業務の流れに沿って記述すべきである。取扱いが複雑な個人情報の場合は同一局面が複数回現れることがあるが，その場合にもそのまま記述する。関係者が共通の認識を持てるように流れに沿って判り易く記述することが肝要である。

【手順】

1.リスク分析の実施手順

(1)個人情報を取り扱う業務フローを整理する。

個人情報を取り扱う当事者間での授受と利用，保管，廃棄の流れを整理する。

DFD(Data Flow Diagram)のような様式が望まれるが様式は規定しない。

(2)業務フローに従って，各局面での想定されるリスクを洗い出す。

個人情報を取り扱う各局面で想定されるリスクを洗い出し,「リスク分析表」の“想定されるリスク”欄に記入する。

(3)想定されるリスクに対して講じる対策と残留リスクを整理する。

想定されるリスクに対し，有効な対策を洗い出す。

実際に実施すると定めた対策を「リスク分析表」の“講じる対策”欄に記入する。

リスクの発生確率が充分低く,経済的あるいは技術的理由等で対策を保留する場合には，当該リスクを“残留リスク”欄に記入し，保留した対策を“残留リスク顕在化の兆候発生時の対策案”に記入する。なお，リスクに対する有効な対策案が出てこなかった場合にも当該リスクを“残留リスク”欄に記入する。この場合には“残留リスク顕在化の兆候発生時の対策案”は空欄にする。

2.リスク分析の追加，更新と見直し

(1)新しい種類の個人情報が追加されたとき

新しい種類の個人情報についてリスク分析を実施する。

(2)個人情報の特定内容に変更が生じたとき

変更した個人情報についてリスク分析を見直して更新する。

(3)定期的見直し

個人情報保護管理者は毎年「年間計画書」に定める時期に，必要に応じて適宜に，PMS事務局に「リスク分析表」の見直しを実施するように指示する。

3.リスク分析結果の承認と規程への反映

(1)リスク分析結果の承認

「リスク分析表」が作成あるいは更新される都度，トップマネジメントによって権限を与えられた個人情報保護管理者の承認を得る。

(2)リスク分析結果の規程への反映

「リスク分析表」で講じると定めた主要な対策を規程上に反映する。

規程上の反映した箇所の項番を「リスク分析表」の“関連規程”欄に記入する。

A.3.3.4 資源，役割，責任及び権限

【規程】

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，JIS Q 15001:2017 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当社の内部の者から指名し，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，業務を行わせる。

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 の運用状況を報告する。

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当社の内部の者から指名し，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，業務を行わせる。

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する。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する。

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。

【要点】

1. 役割，責任及び権限を組織規程等で定めることも可能である。

【手順】

1.PMS 体制における各責任者及び担当者の役割，責任及び権限を【PMS 体制における各責任者及び担当者の役割，責任及び権限】に定める。

2.PMS 体制上の要員の配置を定め，「PMS 体制図」として文書化する。

3.個人情報保護管理者は教育・訓練の実施により，従業者に「PMS 体制図」を周知させる。

【PMS 体制における各責任者及び担当者の役割，責任及び権限】

1.トップマネジメント

①全ての PMS 活動に関する最終責任を負う。

②個人情報保護方針を制定及び改正する。

③個人情報保護管理者を指名し，PMS の実施，運用に関する権限を付与する。

④個人情報保護監査責任者を指名し,PMS 監査計画の立案,実施に関する権限を付与する。

⑤「年間計画書」,「教育計画書」,「監査計画書」を承認する。

⑥少なくとも年一 回，適宜に PMS 全体を見直し，維持・改善を指示する。

⑦リスク対策についての承認を個人情報保護管理者に委任する。

2. 個人情報保護管理者（個人情報保護監査責任者との兼任不可）

①PMS の制定及び運用を指揮し，全従業者に対する管理及び監督の権限と責任を有する。

②PMS の運用状況を定期的にトップマネジメントに報告する。

③PMS 事務局を構成し，PMS 全体運用に関する事務，安全管理措置全般の推進，苦情相談窓口，従業者教育を担当させる。

④情報システム管理者を指名し，情報システムに関する安全管理措置の推進を担当させる。

⑤特定個人情報事務取扱担当者を指名し，特定個人情報の取扱いを担当させる。

⑥PMS 運用の記録を承認する。

3. PMS 事務局

①個人情報保護管理者の指揮下で，PMS 運用の事務処理を行う。

②開示等の請求及び苦情相談の受付窓口となり，対応を行う。

③全社の安全管理状況を定期的に確認する。

④全従業者に対する教育の実施計画を立案し，実施する。

4. 情報システム管理者

①個人情報保護管理者の指揮下で，全社の情報システムに関する安全管理措置ルールの制定と実施を行う。外部データセンタ利用も対象に含める。

②情報システムの構成と，利用者のアクセス権限を管理する。

③情報システムに関する安全管理措置の実施状況を点検し，個人情報保護管理者に報告する。

5. 特定個人情報事務取扱担当者

①個人情報保護管理者の指揮下で，個人番号及び特定個人情報を独占的に取り扱う。

6. 部門責任者

①各部門の PMS 活動を指導し，その推進についての責任を負う。

7. 個人情報保護監査責任者（個人情報保護管理者との兼任不可）

①PMS 監査計画を立案する。

②監査員を指名し，育成を行う。

③内部監査を指揮し，実施結果をトップマネジメントに報告する。

8. 監査員

①個人情報保護監査責任者の指揮下で，監査の実行手順を計画し，必要なチェックリストを作成する。

②内部監査を実施し，個人情報保護監査責任者に報告する。

③監査員については，コンサルタント会社社員等に代行を委託することは可能である。

9. 従業者

①PMS の意義と内容を理解して遵守する。

②PMS の推進に協力する。

A.3.3.5 内部規程

【規程】

次の事項を含む内部規程を文書化し，かつ，維持する。

a)個人情報を特定する手順に関する規定

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

c)個人情報に関する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

d)当社の各部門及び階層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

e)緊急事態（個人情報が漏えい，滅失又はき損をした場合）への準備及び対応に関する規定

f)個人情報の取得，利用及び提供に関する規定

g)個人情報の適正管理に関する規定

h)本人からの開示等の求めへの対応に関する規定

i)教育に関する規定

j)PMS 文書の管理に関する規定

k)苦情及び相談への対応に関する規定

l)点検に関する規定

m)是正処置に関する規定

n)マネジメントレビューに関する規定

o)内部規程の違反に関する罰則の規定

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。

【要点】

1.事業内容，取り巻く社会環境の変化等に対応して，規程を維持・改善する必要がある。

2.罰則規程は「就業規則」等に明示されていることが望ましい。

【手順】

1.内部規程の文書化

(1)a)～o)については本「個人情報保護規程」で規定する。

2.内部規程の制定，改廃

A.3.5.2 項に定める手順により制定及び改廃を行う。

3.内部規程の維持

事業内容，事業環境の変化，法令等の改正に対応して，内部規程を改正，維持していく。

4.内部規程の周知徹底

従業者が随時閲覧できるように印刷して常備する，従業者が常時閲覧できるように共有フォルダに掲載する，のいずれか，あるいは両方の措置を行う。

A.3.3.6 計画策定

【規程】

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の立案及びその文書化

【要点】

1.計画書に必須な事項が定められた。(2017 年度版)

a)実施事項

b)必要な資源

c)責任者

d)達成期限

e)結果の評価方法

2.計画に対する進捗管理も当然必要である。

【手順】

1.計画書の策定

(1)計画書の種類と概要

①「年間計画書」

下記 PMS の主要活動の実施計画を策定し，進捗管理する。

年間計画策定

「個人情報管理台帳」の見直し

「法令等管理台帳」の見直し

「リスク分析表」の見直し

委託先評価基準の見直しと再評価

教育

運用の確認

内部監査

マネジメントレビュー

②「教育計画書」

前年「教育報告書」等を考慮して，以下の事項を含む計画を策定する。

a)実施事項

教育の目的と狙い

教育内容

実施方法

b)必要な資源

c)責任者

d)達成期限

e)結果の評価方法

理解度確認方法

レビュー実施計画

③「監査計画書」

前年「監査報告書」等を考慮して，以下の事項を含む計画を策定する。

a)実施事項

監査の狙いと目的

教育内容

実施方法

b)必要な資源

c)責任者を含む監査体制

d)達成期限

e)結果の評価方法

(2)計画書の策定時期と承認

①「年間計画書」「教育計画書」

毎年 3 月に個人情報保護管理者が次年度の計画を策定してトップマネジメントの承認を得る。年度の途中で計画を修正した場合にもトップマネジメントの承認を得る。

②「教育計画書」

毎年「年間計画書」に定める時期に個人情報保護管理者が次年度の計画を策定してトップマネジメントの承認を得る。年度の途中で計画を修正した場合にもトップマネジメントの承認を得る。

③「監査計画書」

毎年「年間計画書」に定める時期に個人情報保護監査責任者が次年度の計画を策定してトップマネジメントの承認を得る。年度の途中で計画を修正した場合にもトップマネジメントの承認を得る。

2. 計画管理

(1)進捗管理

毎月末迄に個人情報保護管理者は「年間計画書」に実施結果を記録し，次月の計画を確認し，関係者に実施を指示する。

(2)計画変更

「年間計画書」を変更しなければならない事態になった場合は，「年間計画書」を変更し，トップマネジメントの承認を得る。

A.3.3.7 緊急事態への準備

【規程】

緊急事態を特定するための手順，また，それら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。

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，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。

【要点】

1. 受託業務で事故が発生した場合には，委託元に速やかに連絡して，委託元の指示に基づいて対応する。
2. 事故発生時(事故とすべきかどうか判断に迷う場合も含む)には，審査機関に報告して，アドバイスを得る。
3. 事故発生時は噂が飛び交いやすい傾向があるので，確認情報と未確認情報を明確に区別し，未確認情報については“緊急対策本部”内限りとする。

【手順】

1. 緊急事態を特定する手順と初期対応手順

(1)以下の事態を緊急事態と定義する。

①目的外利用をしてしまった時

②個人情報の漏えい，滅失，毀損が発生した時

③その他，個人情報保護管理者が緊急事態と判断した時

(2)緊急事態発生時の社内通報・連絡

①緊急事態の発見者は直ちに個人情報保護管理者(不在時はPMS事務局)に報告する。

②個人情報保護管理者は直ちにトップマネジメントに報告し，指示を仰ぐ。

③トップマネジメントと個人情報保護管理者は緊急事態に対応するメンバーを選任し，“緊急対策本部”を設置する。

(3)初期対応

①個人情報保護管理者は“緊急対策本部”メンバーを招集し，初期対応を指示する。

②初期対応の内容には必ず以下を含める。

a)緊急事態に関する情報の収集

緊急事態の内容

影響範囲

【補記】未確認情報も収集するが，未確認情報として管理し，確認が完了するま

では原則として口外禁止

b)被害の拡大を防ぐ応急処置

個人情報の漏えい，滅失またはき損をした場合に，想定される影響を最小限とするための措置（サーバの停止，ネットワークの遮断等）の実施

c)受託業務での緊急事態の場合の委託元への通報

2. 本人に速やかに通知し，又は本人が容易に知り得る状態に置く手順

(1)本人への速やかな通知：原則

①“緊急対策本部”の担当者が本人に電話又はメールで緊急事態の内容を伝えると共に謝罪する。

②差出人をトップマネジメント又は個人情報保護管理者とする正式書面で緊急事態の通知と謝罪を行う。

(2)本人が容易に知り得る状態に置く：対象者が多数で個別通知が困難な場合等

①個人情報保護管理者がホームページにて公表する。

②本人からの問い合わせに応じる体制を準備する。

3. 二次被害の防止，類似事案の発生回避の観点から事実関係，発生原因及び対応策を，遅滞なく公表する手順

(1)受託業務の場合

委託元の指示に基づいて公表する。

(2)受託業務ではない場合

①個人情報保護管理者が二次被害の防止，類似事案の発生回避の観点から事実関係，発生原因及び対応策についての公表文書を作成する。

②公表することにより本人に迷惑が掛からないこと等を考慮した上で，トップマネジメントが公表すること及び公表文書の内容を承認する。

③個人情報保護管理者がホームページにて公表する。

4. 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手順

(1)報告内容

①「個人情報の取扱いに関する事故等の報告書」の様式で報告書を作成する。

②受託業務の場合には，報告書の内容について委託元の承諾を得る。

(2)報告先

①審査機関

②個人情報保護委員会

③その他の報告先については，審査機関のアドバイスに基づいて行う。

5. 再発防止（是正・予防処置）

(1)緊急事態が発生した個人情報について，以下の観点で「リスク分析表」を見直す。

①緊急事態が発生した局面事態が「リスク分析表」から漏れていないか？

②緊急事態が発生した原因が想定リスクから漏れていなかったか？

③類似のリスクが漏れていないか？

④「講じる対策」の内容が充分であったか？　等

(2)見直した「リスク分析表」を元に“A.3.8 是正処置及び予防処置”の手順を実施する。

A.3.4 実施及び運用

A.3.4.1 運用手順

【規程】

PMS を実施するために，運用の手順を本規程で明確にする。

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

【規程】

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限度において行う。

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。

【要点】

1. 利用目的（提供の範囲を含む。）を明確に記述する。
   利用目的の記述が不明確であると，解釈を誤って目的外利用を犯すリスクが生じる。
2. 本人が利用目的を明確に認識できる措置を講じる。

【手順】

1. 新たな種類の個人情報を取得する際には，“A.3.3.1 個人情報の特定”の手順で，利用目的を可能な限り具体的に特定する。
2. 特定した利用目的を本人に通知するか，又は公表する。

A.3.4.2.2 適正な取得

【規程】

適法，かつ，公正な手段によって個人情報を取得する。

【要点】

1. 本人から書面で個人情報を直接取得する場合
   優越的な地位を利用して同意を得ることは公正でない点に注意する。
2. 委託，第三者提供又は共同利用で個人情報を取得する場合
   委託元，提供元及び共同利用者が適切に取得していることを確認する必要がある。

【手順】

1. 本人から書面で個人情報を直接取得する場合には，A.3.4.2.5 の手順で同意を得る。
2. 委託，第三者提供又は共同利用で個人情報を取得する場合には，A.3.4.2.8.3. の手順で，委託元，提供元及び共同利用者が適切に取得していることを確認する。

A.3.4.2.3 要配慮個人情報

【規程】

新たに要配慮個人情報(用語の定義“2.3”を参照)を取得する場合，あらかじめ書面による本人の同意を得る。ただし，次に掲げるいずれかに該当する場合には，本人の同意を得ることを省略できる。

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)その他，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，又は政令で定められた要配慮個人情報であるとき

要配慮個人情報の利用又は提供，さらに要配慮個人情報のデータを提供する場合についても，同様の同意手順を実施する。

【要点】

1.あらかじめ書面による本人の同意を得，その証跡を残す必要がある。

2.就業規則に記述してある場合は，従業者から明示的な同意を得ていると判断して良い。

【手順】

1.要配慮個人情報を含む個人情報の特定時に,「個人情報取扱申請書」の“要配慮個人情報”欄に要配慮個人情報を含むこと及び要配慮個人情報名を記入し,「例外承認申請書」に要配慮個人情報を取得する根拠を記入する。

2.「個人情報取扱申請書」と「例外承認申請書」を個人情報保護管理者に提出して，承認を得る。

3.本人から同意を得る場合には，紙面に A.3.4.2.5 の a)～g)事項を明示して，本人から同意の署名を得る。

A.3.4.2.4 個人情報を取得した場合の措置

【規程】

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

【要点】

1.個人情報の取得方法によって，利用目的の通知又は公表方法が異なる。

取得方法		主な個人情報取得例	通知又は公表
取得元	手段		
本人	書面	A.3.4.2.5 参照	書面で本人に明示*1
	書面以外	監視カメラ映像，写真 電話録音	通知の場合が多い*2
第三者	受託	システム開発 DM 等の発送代行 メルマガ配信代行	公表の場合が多い*3
	第三者受け	ハローワークからの紹介者 就職サイト経由採用応募者 購入した名簿	
	共同利用	顧客情報を提携先と共同利用 顧客情報をグループ内で共同利用 グループ人事管理	

*1：書面で同意を得るために，書面で本人に明示する。

*2：通知が容易で無い場合には公表でも可

*3：第三者から取得する場合は本人に通知することが通常は困難であることによる。

2.本人から書面で個人情報を直接取得する以外の方法で取得する場合は，本人の同意を得るのが困難なので，本人に通知する，本人に通知することも困難である場合には公表することが求められている。

【手順】

1.本人から書面で個人情報を直接取得する場合は，A.3.4.2.5 の手順で，書面で本人に明示して，書面で同意を得る。

2.本人から書面で個人情報を直接取得する以外の方法で取得する場合は，利用目的を，本人に通知するか，又は公表する。

(1)本人に通知する手順

①口頭通知

電話録音，写真撮影等の場合には，開始直前に口頭で伝える。

②表示

本人が気付きやすい場所に表示する。“監視カメラ作動中”等

③その他

通常は上記のいずれかの手段で行われるが，他の手段でも本人に伝わる行為を実施すれば通知したことになる。

(2)公表する手順

①公表文書作成

PMS 事務局は直接書面以外の方法で取得した個人情報の利用目的を記載した「個人情報に関する公表事項」を作成し，個人情報保護管理者の承認を得る。

②公表方法

PMS 事務局は「個人情報に関する公表事項」を求められた時には速やかに印刷して渡す。ホームページ構築後は「個人情報に関する公表事項」を掲載する。

3.ただし書き a)～d)を適用する場合の承認手順

(1)「例外承認申請書」に適用するただし書きの項番，ただし書き適用の根拠を記入する。

(2)個人情報の特定時に，上記「例外承認申請書」を「個人情報取扱申請書」と共に提出して，個人情報保護管理者の承認を得る。

(3)ただし書き d)の適用は契約書あるいは見積り書に記載される個人情報，名刺等に限定し，乱用してはならない。

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

【規程】

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)当社の名称

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)本人が容易に認識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，身体又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。

【要点】

1. 証跡が残るので，同意を得るための明示文書が記載された紙面に本人が同意の署名をする手順が最も確実である。
2. Web 入力フォームでは同意を得るための文書を明示して同意の入力(チェックボックスのクリック等)がなければ，エラーにする等の手順で同意を確認するが，証跡を残すことが困難である点に注意すべきである。
3. 第三者提供については，漏れなく明示されていなければならない。第三者提供先については当社が管理監督できないからである。委託先については管理監督責任を負っているので委託することがある旨を明示するだけでよい。

【手順】

1. 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手順

(1)a)～h)の事項を満たした同意書に本人の同意の署名を得る。

①従業者の場合

「個人情報取扱同意書（従業者用)」に同意の署名を得る。

②採用応募者の場合

「個人情報取扱同意書（採用応募者用)」に同意の署名を得る。

③委託先個人事業主の場合

委託先として契約する時点で「個人情報取扱同意書（個人事業主用)」に同意の署名を得る。

④その他，顧客あるいは取引先等から対面で取得する場合

「個人情報取扱同意書」を作成し，個人情報保護管理者の承認を得てから，「個人情報取扱同意書」に同意の署名を得る。

⑤対面でない場合

個人情報保護管理者の承認を得た「個人情報取扱同意書」を郵送又はメール添付で送付し，本人が同意の署名した「個人情報取扱同意書」を送付して貰う。

(2)Web 入力フォームでは以下の手順で同意を得る。

①a)～h)の事項を満たした「個人情報取扱同意書」を作成し，個人情報保護管理者の承認を得る。

②「個人情報取扱同意書」を Web 入力フォームに掲載し，同意入力後に送信する手順

にする。(“「個人情報取扱同意書」に同意します”のチェックボックスがチェックされ無ければエラーとする等)

2. 書面による本人の同意を得ないで，本人から書面で取得する場合の承認手順

(1)「例外承認申請書」に適用するただし書きの項番，ただし書き適用の根拠(法令名等)を記入する。

(2)個人情報の特定時に，上記「例外承認申請書」を「個人情報取扱申請書」と共に提出して，個人情報保護管理者の承認を得る。

A.3.4.2.6 利用に関する措置

【規程】

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，本人の同意を得る。ただし，A.3.4.2.3 の a)～d)のいずれかに該当する場合は，この限りではない。

【要点】

1. 目的外利用と利用目的の変更は同じではない。

(1)目的外利用：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

(2)利用目的の変更：特定した利用目的を変更すること

利用目的の変更手続前に，当該目的で利用すると目的外利用になる。

2. 利用目的として特定されていない,本人への連絡又は接触或いは第三者提供を行うことは目的外利用である。ただし，本人から同意を得るために個人情報を利用することは許される。

3. 利用目的を変更する場合の同意を得る手順は,本人から書面で個人情報を直接取得する場合の同意を得る手順より条件が緩められている。(A.3.4.2.7，A.3.4.2.8 も同様)

(1)本人から書面で個人情報を直接取得する時の同意

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。

(2)利用目的の変更時の同意

本人に通知して同意を得る。

つまり口頭同意でも要求事項を満たしている。但し，口頭同意では証跡が残らないので，重要な利用目的変更では書面で明示して同意を得ることが望ましい。

4. Web 入力フォームで利用目的の変更，本人への連絡又は接触，第三者提供についての同意を得る場合には，通知して同意を得た証跡を残すことが必要になる。

【手順】

1. 利用目的の確認手順及び目的外利用に該当するか否かの判断手順

(1)利用目的の確認手順

個人情報を利用する際に「個人情報管理台帳」に特定されている利用目的を確認する。

(2)目的外利用に該当するか否かの判断に迷う場合の措置

個人情報保護管理者に判断を求める。

2.ただし書き A.3.4.2.3 の a)～d)を適用する場合の承認手順

(1)個人情報特定時に適用する場合

個人情報の特定時に，例外適用の事項と理由を記載した「例外承認申請書」を「個人情報取扱申請書」と共に提出して，個人情報保護管理者の承認を得る。

“法令に基づく場合”に該当する“建設業法に基づく委託元への作業員名簿の提出”等は，この手順で行うことも可能である。

(2)事象の発生都度，適用する場合

「例外承認申請書」に例外適用の事項と理由を記入して，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必要がある場合”等，緊急性のある場合には事後承認もやむを得ないが速やかに承認手続を実施する。

3.利用目的の社内変更手順

(1)「個人情報取扱申請書」の更新と同意書作成

①「個人情報取扱申請書」上の該当する特定内容を変更し，変更理由と通知して同意を得る手順を“補記”欄に記入する。

②A.3.4.2.5 の a)～f)を満たした「利用目的変更同意書」を作成する。

③「個人情報取扱申請書」と「利用目的変更同意書」を個人情報保護管理者に提出し，承認を得る。

(2)「個人情報管理台帳」の更新

個人情報保護管理者は「個人情報管理台帳」を PMS 事務局に更新させ，承認してから全従業者に周知させる。

4.利用目的を変更する場合に本人へ通知し，同意を得る手順

(1)同意書に本人の署名を得る手順

「利用目的変更同意書」を明示して，本人の署名を得る。

対面でない場合は，「利用目的変更同意書」を郵送する，メール添付で送信する，ホームページからダウンロードさせる等の方法を検討する。この場合の郵送料等は本人に負担させない配慮をする。

(2)口頭で同意を得る。

「利用目的変更同意書」の内容を読み上げて口頭で同意を得る。この場合，本人が同意した証跡が残らない点に注意すること。

A.3.4.2.7 本人に連絡又は接触する場合の措置

【規程】

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，次に示すいずれかに該当する場合は，この限りではない。

a)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，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，共同利用者が既に 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，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，本人に通知し，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
- 取得方法

e)A.3.4.2.4 のただし書き 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

【要点】

1. “本人に連絡又は接触する”には，訪問，電話，FAX，電子メール送信，DM 送付，ポスティング等の手段で本人に連絡又は接触することが含まれる。
2. 本人に連絡又は接触する場合に本人から同意を得る手順については,A.3.4.2.5 の場合より条件が緩められている。(A.3.4.2.6 項要点参照)
3. 共同利用については d)項の他に全ての共同利用者間で共同利用に関する取決めを行う必要がある。

【手順】

1. 本人への連絡又は接触の可否判断

「個人情報取扱申請書」の“連絡又は接触”欄が“可”となっている場合にのみ，本人に連絡又は接触できる。

2.本人への連絡又は接触する場合の承認手順

(1)個人情報取得時に本人への連絡又は接触の同意を得ている場合

個人情報の特定時に「個人情報取扱申請書」で個人情報保護管理者の承認を得る。

(2)初回連絡又は接触時に同意を得る手順を定めている場合

個人情報の特定時に「個人情報取扱申請書」で個人情報保護管理者の承認を得る。

(3)新たに個人情報を利用して本人に連絡又は接触する必要が生じた場合

本人への連絡又は接触を開始する前に「個人情報取扱申請書」で個人情報保護管理者の承認を得る。

3.本人に連絡又は接触する場合に本人へ通知し，同意を得る手順

(1)同意書作成

取得方法と A.3.4.2.5 の a)～f)を記述した「連絡又は接触同意書」を作成し，「個人情報取扱申請書」に添付して個人情報保護管理者の承認を得る。

(2)同意書に本人の署名を得る手順

①対面の場合

本人に「連絡又は接触同意書」を明示して，同意の署名を得る。

②DM 発送の場合

初回 DM 発送時に「連絡又は接触同意書」と返信用封筒を同封して，同意の署名をして送り返すように依頼する。

返信がなかった場合にも，DM 発送を継続できるが，拒否の意志表示がされた場合には二度と送ってはならない。

③その他の場合

「連絡又は接触同意書」を郵送する，メール添付で送信する，ホームページからダウンロードさせる等の方法を検討する。この場合の郵送料等は本人に負担させない配慮をする。

(3)口頭で同意を得る。

「連絡又は接触同意書」の内容を読み上げて口頭で同意を得る。この場合，本人が同意した証跡が残らない点に注意すること。

4.ただし書き b)～f)を適用する場合の承認手順

(1)個人情報特定時に適用する場合

個人情報の特定時に，例外適用の事項と理由を記載した「例外承認申請書」を「個人情報取扱申請書」と共に提出して，個人情報保護管理者の承認を得る。

特にただし書き b)，d)，e)を適用する場合は，個人情報の特定時にする。

ただし書き f)適用の場合については A.3.4.2.6【手順】2 を参照

(2)事象の発生都度，適用する場合

「例外承認申請書」に例外適用の事項と理由を記入して，個人情報保護管理者の承認を得る。

ただし書き c)，ただし書き f)の一部が該当する。

5.共同利用する場合の手順：本項は A.3.4.2.8 の共同利用と共通である。

(1)共同利用者との間で必要事項について取り決めの手順

共同利用者との間で以下の 10 項目について取り決めた契約書を交わす。

1)共同して利用する個人情報の項目

2)共同して利用する者の範囲

3)共同して利用する者のすべての利用目的

4)共同して利用する個人情報について責任を有する者の氏名又は名称

5)共同利用者の要件

6)各共同利用者の個人情報取扱責任者，問合せ担当者及び連絡先

7)共同利用する個人情報の取扱いに関する事項

・個人情報の漏えいと防止に関する事項

・目的外の加工，利用，複写，複製等の禁止

・共同利用終了後の個人情報の返還，消去，廃棄に関する事項

8)共同利用する個人情報に関する事件・事故が発生した場合の報告・連絡に関する事項

9)共同利用する個人情報の取扱いに関する取決めが遵守されなかった場合の措置

10)共同利用を終了する際の手続

(2)共同利用について本人への通知，公表の手順

①公表文書作成

ただし書き d)項に定める事項を「個人情報に関する公表事項」に記載し，個人情報保護管理者の承認を得る。

②公表方法

PMS 事務局は「個人情報に関する公表事項」を求められた時には速やかに印刷して渡す。ホームページ構築後は「個人情報に関する公表事項」を掲載する。

A.3.4.2.8 個人データの提供に関する措置

【規程】

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)の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，次に示すいずれかに該当する場合は，この限りではない。

a)A.3.4.2.5 又は 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明示又は通知し，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≪第三者提供に関する事項≫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

≪第三者提供に関する事項≫

・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個人情報の項目

・第三者への提供の手段又は方法

・本人の請求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

・取得方法

・本人からの請求などを受け付ける方法

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，法令に基づき又は本人若しく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，b)で示す≪第三者提供に関する事項≫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情報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)個人データを共同して利用する場合であって，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)のいずれかに該当する場合

【要点】

1.第三者に提供する場合に本人から同意を得る手順については，A.3.4.2.5 の場合より条件が緩められている。(A.3.4.2.6 項要点参照)

2.ただし書き b)に“通知し，又はそれに代わる同等の措置”について

(1)ホームページ公表等の容易に知り得る状態に置くだけの措置では不充分である。

“通知”と異なり，公表だけでは本人に伝わらない場合がある。

(2)“通知し，又はそれに代わる同等の措置”の例

本人が所属する組織を通して本人に伝えて貰う等の最大限の努力が必要である。

【手順】

1.提供の可否判断と承認手順

(1)提供の可否判断

①「個人情報取扱申請書」の“提供先”に記入されている提供先にだけ提供できる。

②「個人情報取扱申請書」の“委託先”に記入されている委託先にだけ委託できる。

(2)個人情報特定時の承認手続

以下の場合には，個人情報の特定時に「個人情報取扱申請書」で個人情報保護管理者の承認を得る。

①直接書面取得時に本人から第三者提供或いは委託の同意を得ている場合

②本人から第三者提供の同意を得る手順を定めている場合

③受託契約書あるいは再委託申請書等で委託元から再委託が承認されている場合

(3)第三者提供する直前に行う承認手続

新たに個人情報を第三者提供する必要が生じた時は，第三者提供する前に「個人情報取扱申請書」で個人情報保護管理者の承認を得る。

2.第三者提供する場合に本人へ通知し，同意を得る手順

(1)同意書作成

取得方法とA.3.4.2.4 のa)～d)を記述した「第三者提供同意書」を作成し，「個人情報取扱申請書」に添付して個人情報保護管理者の承認を得る。

(2)同意書に本人の署名を得る手順

「第三者提供同意書」を明示して本人の署名を得る。

対面でない場合は，「第三者提供同意書」を郵送する，メール添付で送信する，ホームページからダウンロードさせる等の方法を検討する。この場合の郵送料等は本人に負担させない配慮をする。

(3)口頭で同意を得る。

「第三者提供同意書」の内容を読み上げて口頭で同意を得る。この場合，本人が同意した証跡が残らない点に注意すること。

3.ただし書きb)～g)を適用する場合の承認手順

(1)個人情報特定時に適用する場合

個人情報の特定時に，例外適用の事項と理由を記載した「例外承認申請書」を「個人情報取扱申請書」と共に提出して，個人情報保護管理者の承認を得る。

特にただし書きb)，c)，d) ，f)を適用する場合は，個人情報の特定時にする。

ただし書きg)適用の場合についてはA.3.4.2.6【手順】2を参照

(2)事象の発生都度，適用する場合

「例外承認申請書」に例外適用の事項と理由を記入して，個人情報保護管理者の承認を得る。

ただし書きe)，ただし書きg)の一部が該当する。

4.ただし書きb)を適用する場合の措置

≪第三者提供に関する事項≫を本人が所属する組織を通して本人に伝えて貰う等の措置内容と個人情報保護委員会への届け出手順を「例外承認申請書」に記述して個人情報保護管理者の承認を得てから，実施する。特にホームページ公表だけでは不充分である点に注意すること。

5.ただし書きc)を適用する場合の措置

≪第三者提供に関する事項≫をホームページで公表する。

6.共同利用する場合の手順

A.3.4.2.7 の【手順】5 に定める手順を実施する。

A.3.4.2.8.1 外国にある第三者への提供の制限

【規程】

法令等の定めに基づき，外国にある第三者に個人データを提供する場合には，あらかじめ外国にある第三者への提供を認める旨の本人の同意を得る。ただし，A.3.4.2.3 の a)～d)のいずれかに該当する場合及びその他法令等によって除外事項が適用される場合は，この限りではない。

【要点】

1. 外国にある第三者に個人データを提供する場合には，あらかじめ本人の同意を得る。
2. 外国にある第三者に個人データを提供しておらず，計画も無い場合には，その旨を定めるだけでよい。

【手順】

1. 当社は外国にある第三者に個人データを提供しておらず，計画も無い。
2. 外国にある第三者への個人データ提供を開始する前に，別途，規程を定める。

A.3.4.2.8.2 第三者提供に係る記録の作成など

【規程】

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，保管しなければならない。ただし，A.3.4.2.3 の a)～d)のいずれかに該当する場合，又は次に掲げるいずれかに該当する場合は，この限りではない。

a) 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ことに伴って当該個人データが提供される場合

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が提供される場合

c) 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって，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

【要点】

1. 記録の作成方法は，当社の実情に合わせて選択することができる。
2. 安全管理措置における授受の確認手順とも密接な関係がある。

【手順】

1. “A.3.4.3.2 安全管理措置 B.技術的安全管理措置 4.個人情報の移送時の対策(4)，(5)”に定める手順に従って，個人データを第三者に提供したときの記録を作成し，保管する。

A.3.4.2.8.3 第三者提供を受ける際の確認など

【規程】

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わなければならない。ただし，A.3.4.2.3 の a)～d)のいずれかに該当する場合，又はA.3.4.2.8.2 の a)～c)のいずれかに該当する場合は，確認を要しない。

法令等の定めるところによって確認の記録を作成，保管しなければならない。

【要点】

1. 受託や第三者提供を受ける場合及び共同利用者が取得した個人データを利用する場合には，提供元が適正に取り扱っていることを確認しなければならない。個人情報名が同じであっても，複数の提供元がある場合には，提供元毎に確認を行う必要がある。運用が可能であれば，提供を受ける都度，確認することを検討する。
2. 受託業務で取り扱う個人データについては，委託元が本人から適切に取得して，取り扱っていることを確認する。なお，当社が再委託先になる場合は，委託元の委託元から当社への再委託が禁止されていないことを確認する必要がある。
3. 第三者提供で取得した個人データについは，提供元が当社に提供することに本人が同意していなければならない。名簿等で提供が繰り返し行われている場合には，トレーサビリティも必要である。

【手順】

1. 委託元及び提供元の適正な取扱いを以下の手順で確認する。
   (1)受領の都度，「個人情報授受記録(引渡し記録)」上で委託元，提供元と確認する。
   (2)委託元，提供元から「個人情報授受記録(引渡し記録)」による確認を拒否された場合には，年に 1 回以上，委託元，提供元の個人情報保護方針を確認する，あるいは Web 入力画面での同意取得方法と内容を確認する等の可能な方法で確認する。
   (3)確認結果を「委託元・提供元一覧表」に記入し，個人情報保護管理者の承認を得る。
2. 共同利用者の適正な取扱いについては，共同利用に関する取り決めを締結する際に，確認する。

A.3.4.2.9 匿名加工情報

【規程】

匿名加工情報の取扱いを行うか否かの方針を定める。

匿名加工情報を取り扱う場合には，本人の権利利益に配慮し，かつ，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確立し，かつ，維持する。

【要点】

1. 匿名加工情報の取扱いを行う場合には，その手順を確立して，実施する必要がある。
2. 匿名加工情報の取扱いを行う場合には，その旨を定めるだけでよい。

【手順】

1.当社は，匿名加工情報取扱事業者ではない。

2.匿名加工情報を取り扱う場合は，別途，規程を定める。

A.3.4.3 適正管理

A.3.4.3.1 正確性の確保

【規程】

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。

個人データを利用する必要がなくなったときは，当該個人デ ータを遅滞なく消去する。

【要点】

1.バックアップ取得要否の決定

(1)障害発生時にバックアップが無いと復元できない場合に必須となる。

(2)以下のような場合にはバックアップ取得は不要である。

①紙媒体から合理的な時間内に復元できるデータ

②委託元又は提供元から再提供を受ければ復元できるデータ

2.バックアップ取得方法を定める上での考慮事項

(1)DB の場合は DBMS（データベース管理システム）の仕様を考慮して手順を定める。

①DBMS の機能の中にバックアップ取得機能が含まれていることがある。

②勝手に DB 中のデータを複写してもバックアップとして使用できない場合がある。

(2)バックアップ取得対象の装置とは独立した装置にバックアップを取得する。

同一装置上であれば，同時に読めなくなってしまう。

(3)RAID(Redundant Arrays of Inexpensive Disks)のミラーリング機能はバックアップとは基本的に異なる。

RAID は多重化して，ハードウェア障害で一つのディスクが使用不能になっても，残りのディスクでシステムのサービスを続行できる仕組みであり，ソフトウェアによる不正更新，誤入力があった場合に復元を可能にする手段ではない。バックアップは，障害発生時に，データをバックアップ取得時点の状態に復元することを可能にする。

(4)外部データセンタを利用（ホスティング，クラウド等のサービス利用）するときは，バックアップの取得責任を利用規約等で必ず確認する。

(5)大規模災害対策としては，遠隔バックアップも検討する。

遠隔バックアップはコストが掛かること，遠隔バックアップによるリスク増加要素（バックアップ媒体の移送上のリスク，遠隔バックアップ先での保管上のリスク等）を考慮する必要がある。

【手順】

1.個人情報の入力

(1)入力担当者の限定と責任者の明確化

①個人情報毎に入力担当者を限定し，担当者の ID をパスワードで認証する。

②個人情報毎に責任者を明確にし，責任者は入力担当者を管理，指導する。

(2)入力後の再確認

入力担当者は入力後に再表示して入力原票と照合する。

重要な個人情報の入力後には，他の入力担当者又は責任者が確認する。

可能であれば、合理性チェック実施，チェックデジット付与等のシステムによるチェック機能強化も検討する。

2.個人情報の保存期間管理と廃棄手順

(1)「個人情報管理台帳」による管理

個人情報の保存期間と廃棄手順を「個人情報取扱申請書」で定め，「個人情報管理台帳」で周知させる。

特に受託業務で取り扱う個人情報と委託先で取り扱わせる個人情報については，契約内容に基づいて定める。

(2)保存期間を経過した個人情報の廃棄

個人情報毎の責任者の管理，指導下で，「個人情報管理台帳」に定めた手順で，入力担当者が廃棄を行う。

廃棄の記録が定められている場合は廃棄の記録を作成して保管する。特に採用応募者の個人情報は不採用者から苦情・問合せに対応できるように「採用応募書類廃棄記録」に記録して保管する。

システムからデータを消去する際の入力は， 1.(2)に定める手順で行う。可能であれば、システムによる自動削除も検討する。

3.バックアップの取得

(1)サーバ毎にあるいはフォルダ毎にバックアップ手順を制定

情報システム管理者は以下の内容を定めて運用と管理を行う。

①バックアップ取得責任者

②バックアップ取得先媒体

③バックアップの取得周期と保存世代数

(2)バックアップ取得先媒体の盗難防止措置

特に外付けハードディスク等の電子媒体に取得した場合は施錠保管等の盗難防止措置を講じる。

A.3.4.3.2 安全管理措置

【規程】

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。

【要点】

1. 本項に定めるルールと手順は A.3.3.3 の「講じる対策」と密接に関わっており，リスク分析が見直された際には，本項に反映されなければならない。
2. 物理的なオフィスを構えずにバーチャルオフィスだけを利用する事業者は全従業者がテレワークを行っているものして規定する。

【手順】

A. 物理的安全管理措置

1. オフィス出入口の施錠管理

(1) 出入口が物理錠と電子錠併用のオフィス

①出入口の物理錠を最初入室者が解錠し，最終退出者が施錠する。

②当該オフィスに出入りする全従業者は入室の都度カードキーで電子錠を解錠して入室する。

③出入口の物理鍵とカードキーの所持者を PMS 事務局が「鍵管理台帳」で管理し，貸借を禁止する。退職者等資格喪失者からは速やかに回収する。

④複製困難な仕様の物理鍵を使用する。

⑤カードキーには ID を付けて紛失等があった場合には直ちに当該カードを無効化する。

(2) 出入口が物理錠だけのオフィス

①出入口の物理錠を最初入室者が解錠し，最終退出者が施錠する。

②出入口の物理鍵の所持者を PMS 事務局が「鍵管理台帳」で管理し，貸借を禁止する。退職者等資格喪失者からは速やかに回収する。

③複製困難な仕様の物理鍵を使用する。

(3) 出入口が電子錠だけのオフィス

①当該オフィスに出入りする全従業者は入室の都度カードキーで電子錠を解錠して入室する。

②出入口のカードキーの所持者を PMS 事務局が「鍵管理台帳」で管理し，貸借を禁止する。退職者等資格喪失者からは速やかに回収する。

③カードキーには ID を付けて紛失等があった場合には直ちに当該カードを無効化する。

2. 最初入室及び最終退出の管理

(1) 最初入室者及び最終退出者は許可された役員又は正社員に限定する。

(2) 最初入室者は，以下の事項を「最初入室・最終退出確認表」に記入する。

①最初入室者名

②最初入室時刻

③最初入室時異常有無確認結果

(3)最終退出者はチェックした結果と最終退出者名及び最終退出時刻を「最初入室・最終退出確認表」に記録する。チェック事項には執務環境の実態に合わせて以下の事項等を含める。

①人が残っていないこと

②施錠確認（キャビネット，書庫，郵便箱，窓等）

③媒体の放置がないこと（机上，ローキャビネットの上，会議スペース等）

④電源(エアコン・照明)

⑤火元確認（灰皿，ポット）

(4)PMS 事務局は毎月初めに前月分の「最初入室・最終退出確認表」を確認する。

①記入漏れの有無

②異常な休日出勤

③機械警備システムあるいは電子錠システムログ等の最初入室･最終退出情報と照合（取得できる場合に限定）

(5)機械警備システムが導入されているオフィス

①最終退出者は機械警備を開始し，開始されたことを確認してから退出する。

②最初入室者は機械警備が作動中であることを確認してから解除する。作動中でなかった場合には，オフィス内に倒れている者がいるあるいは侵入者がいる事態を想定して警戒しながら入室して確認する。

②機械警備の開始，解除に使用するカードキーの所持者を PMS 事務局が「鍵管理台帳」で管理し，貸借を禁止する。退職者等資格喪失者からは速やかに回収する。

(6)機械警備システムが導入されていないオフィス

①最終退出者は出入口の施錠を再確認（ノブを引く等）する。

②最初入室者は解錠前に出入口が施錠されていることを確認する。出入口が施錠されていなかった場合には，オフィス内に倒れている者がいるあるいは侵入者がいる事態を想定して警戒しながら入室して確認する。

3.事務所内スペース管理と入場制限

(1)事務所内のスペース区分別入場可能者

レベル	スペース区分	入場可能者
0	受付スペース	入場制限なし
1	会議及び打ち合わせスペース	従業者及び受付済来訪者
2	執務スペース	従業者及び従業者が同行する来訪者
3	特定個人情報取扱スペース	特定個人情報事務取扱担当者
3	サーバ設置スペース	特に許可された従業者

(2)入場制限の運用手順

①来訪者の取扱い

・オフィス内の受付スペース以外のスペースに入場する来訪者には，応対者が来訪者に単票形式の「ご来訪記録」への記入と「ご来訪者カード」の着用を依頼する。来訪者の退室時に応対者が「ご来訪者カード」の返却を求め，「ご来訪記録」に退室時刻を記入し，PMS 事務局に提出する。

・PMS 事務局は「ご来訪記録」を都度，確認して受取り，2 年間保管する。

・来訪者をレベル 2 以上のスペース内に招く場合は，従業者が常時同行する。

②レベル 2 以上のスペースの管理

・個人情報の取扱いはレベル 2 以上のスペースで行う。

・壁で仕切られた独立した室を執務スペースにする。または衝立や棚等を適切に配置して，会議スペースから机上が見えないようにする。

・特定個人情報事務取扱担当者が特定個人情報を取り扱っている間は，他の従業者が特定個人情報取扱スペースに入ることを禁止し，特定個人情報事務取扱担当者が使用する机上や PC 画面を覗きこめない対策を講じる。

・サーバを収納するサーバ設置スペースには，情報システム管理者及び情報システム管理者が許可した者以外には入場させない。サーバは常時施錠するサーバ室又はサーバラックに収納し，情報システム管理者が鍵を管理する。

4. オフィスを共用する場合の措置

(1)オフィス共用の定義

①以下のケースをオフィス共用とする。

・当社のオフィス内に他組織が事業所を構えている。

・他組織の事業所は別室になっているが，他組織の室への出入りする際に当社が入退制限しているスペースを通過する必要がある。

②ただし，以下のケースはオフィス共用としない。

・同居する組織にプロパー社員等がおらず，全従業者が当社の従業者を兼任している。

・協力会社社員が常駐作業しているが，当社従業者が不在時には入退室できないようにしている。

(2)オフィス共用時の措置

①ゾーン分離

・当社と同居組織の領域を明確に区別する。(例：机の島を分離する。パーティションでゾーンを分離する。)

②個人情報を記録した媒体を保管する什器，機器，ネットワーク，情報システム

・それぞれ調達し，共用しないことを原則とする。

・複合機等の機器の共用時は，相互に相手側の資料が目に入らないように下記処置を講じる。

a)印刷要求したデータは個人別フォルダに一度格納し，印刷機のパネル操作で

印刷が開始され,印刷完了まで待機し,完了したら直ちに自席まで持ち帰る。

b)受信 FAX の番号を別々にし，受信時にはそれぞれのフォルダに保管し，印刷は a)と同一手順で行う。

・ネットワーク及びサーバの共用時は，セグメント，メールアドレスの分離，サーバ中のフォルダのアクセス権限分離の措置を行う。

③最初入室及び最終退出の管理

・当社としての最初入室及び最終退出の管理に加えて，同居する組織との共同でオフィス全体としての最初入室及び最終退出の管理を行う。

・当社社員が必ず最初入室と最終退出を行い同居組織はオフィス出入口を解錠するための鍵やカードキーを所持していない場合は,共同での最初入室及び最終退出の管理を省略できる。

④相互守秘義務の契約締結

・以下の内容を盛り込んだ契約を締結する。

a)双方の占有場所の明確な定義

b)共用するオフィスの最初入室及び最終退室の管理手順

c)やむを得ずオフィス内で目にした相手方の所有する個人情報を自ら利用するあるいは第三者に提供することを一切行わないこと

d)機器，什器・備品等をそれぞれに調達し，共用しないこと

e)共用する機器，什器・備品がある場合は，共用する手順

f)違反した場合の賠償責任

・事業に関して締結する契約書に上記趣旨の内容を盛り込む方法でも良いが，盛り込まれた契約が存在しない場合には，雛型“オフィス共用に関する守秘義務覚書”を参考に契約書または覚書等を作成して締結する。

5. 盗難の防止

(1)終業時の措置

①クリアデスクを徹底する。

②個人情報を記録した媒体（電子媒体，紙）を所定キャビネット又は机の抽斗に施錠保管する。特定個人情報については特定個人情報事務取扱担当者専用キャビネットに施錠保管する。電子媒体については PMS 事務局が「機器・媒体管理台帳」で管理し，毎月，棚卸する。

③キャビネットの鍵の施錠責任者を PMS 事務局が「鍵管理台帳」で管理する。

④PC をシャットダウンする。

⑤ノート型 PC 及び外付けハードディスクを所定キャビネット又は机の抽斗に施錠保管するか，セキュリティワイヤで固定する。

(2)執務中の措置

①来訪者から覗き見されないように PC を設置する，又は来訪者から覗き見できない

ように画面にスクリーンフィルタを貼付する。

②離席時にクリアデスクし，PC をログオフする。ログオフ忘れ対策として，5 分以内のパスワード付きスクリーンセーバ起動又は自動ログオフを設定する。

③紙媒体の廃棄時にはシュレッダで細断してから廃棄する。大量廃棄する場合には廃棄業者に委託してマニフェストを保管する。

④電子媒体の廃棄時は，物理破壊するか，データを全て削除してから専門業者に完全消去と廃棄を委託しマニフェストを保管する。

⑤PC 及びハードディスクの廃棄時は，ハードディスクを物理破壊するか，専用ソフトウェアで完全消去してから廃棄する。当社内での処置が困難な場合は，データを全て削除してから専門業者に完全消去と廃棄を委託しマニフェストを保管する。

(3)機器・装置等の物理的な保護

①フロア又はオフィス内に消火器を用意する。

②サーバは常時施錠するサーバ室又はサーバラックに収納し，情報システム管理者が鍵を管理する。

③サーバには無停電電源装置（UPS）を接続する。

④サーバラックの床への固定等の措置を行い，サーバ等の機器の倒壊を防ぐ。

⑤サーバ設置スペースでは飲食及び水の使用を禁止する。

B. 技術的安全管理措置

1. 情報システムの利用者の制限とアクセス権限管理

(1)個人情報にアクセスできる利用者を必要最小限に制限する。

(2)利用者の ID を個人単位に割り当て，共用させない。

(3)情報システム管理者は情報システムの利用者とアクセス権限を「アカウント管理台帳」で管理する。「アカウント管理台帳」上に利用者毎にアクセスできる情報システム名，フォルダ名を定めて実装する。

(4)情報システム管理者は退職した従業者，不要となった利用者 ID を速やかにシステム上から抹消する。

(5)情報システム管理者は「アカウント管理台帳」を毎年「年間計画書」に定める時期に，必要に応じて随時に，見直し，利用者毎のアクセス権限範囲とレベルを確認する。

(6)情報システム管理者と情報システム管理者が指名した情報システム担当者だけがサーバシステム(クラウドサービスも含む)の管理者権限を保有する。

2. 情報システム利用者の識別と認証

(1)利用者 ID をパスワードで認証する。

(2)パスワードは 8 文字以上とし，英数記号の混在を必須にする。

(3)パスワードを 6 ヶ月ごとに変更する。

3. 不正ソフトウェア対策

(1)クラウドサービス，ホスティングサービスの利用

①利用規約を確認し，不正ソフトウェア対策を含む安全管理措置が講じられていることを確認する。

(2)社内サーバ

①導入できない特別な事情がある場合を除き，ウイルス対策ソフトを導入する。業務に支障が生じないことを検証後に，パターンファイル，プログラムを更新して最新状態に維持する。定期的にウイルススキャンを実施する。

②業務に支障が生じないことを検証後に，OS やアプリケーション等のセキュリティパッチを適用して最新状態に維持する。

(3)端末及びPC

①ウイルス対策ソフトを導入し，パターンファイル，プログラムが自動更新されるように設定する。定期的にウイルススキャンを実施する。

②OSやアプリケーション等のセキュリティパッチが自動適用されるように設定する。

③新規のソフトウェアを利用する場合は情報システム管理者の許可を得る。特にファイル交換ソフトウェア（Winny，Share 等）の導入を禁止する。

④情報システム管理者は不正ソフトウェアが導入されていないことを毎月サンプリングで確認し，その結果を「運用確認チェックリスト」に記録する。全員が 1 年間に 1 回以上確認されるようにサンプリングする。

4. 個人情報の移送時の対策

(1)USB メモリ等の電子媒体での移送

①個人情報の移送に使用する電子媒体にはパスワードを設定する。

②総当たり対策として，パスワード入力ミスが 5 回連続あった場合には読み出し不可となるように設定する。

(2)ノートPC，タブレット端末，外付けハードディスクでの移送

①持出し時は電源をオフにする。

②別の PC を使用してディスクから個人情報等を読み出せないように，ディスク起動パスワードを設定する又はディスク全体に暗号化措置を適用する。

(3)当社からの個人情報を含む媒体の発送

①書留，特定記録郵便，宅配便等の追跡できる手段で発送し，配送伝票等の控えを記録として保管する。

②封入，封緘時に封入物と宛先ラベルを再確認する。特に重要な個人情報の発送時には、封入者が宛先ラベルを読み上げ，立会人が封入物と宛先ラベルを確認する。

(4)委託元及び委託先との授受

①授受の記録は返却又は廃棄の 3 年後まで保管する。

②引渡しの確認を「個人情報授受記録(引渡し記録)」で行う。

③返却の確認を「個人情報授受記録(返却記録)」で行う。

④廃棄する場合は，「個人情報授受記録(廃棄報告)」で廃棄報告する。

⑤委託元及び委託先と合意した場合には，追跡できる手段で発送した配送伝票等の控えを記録として保管することで代替することも可能とする。

(5)提供元及び提供先との授受

①「個人情報授受記録(引渡し記録)」に授受(返却)を記録し，授受後 3 年間保管する。

②提供元及び提供先と合意した場合には，追跡できる手段で発送した配送伝票等の控えを記録として保管することで代替することも可能とする。

(6)個人情報を記録した媒体及び機器の持運び

①媒体及び機器を入れた鞄から手を離さないようにして持ち運ぶ。道路を歩くときは車道と反対側の手に持つ。

②個人情報を記録した媒体及び機器の持運びは当社から行き先まで直行し，当社まで直行で持ち帰ることを原則とする。特に酒席に持っていくことは厳禁である。

5. ネットワーク利用及び個人情報の送受信時の対策

(1)業務以外での利用禁止

①業務目的以外でのネットワーク利用(Web サイト閲覧等を含む。)を禁止する。

②特に安全性の確認ができていないサイトへのアクセスは厳禁である。

(2)電子メールの利用

①個人情報は平文ではなく，記録したファイルにパスワードを設定して，メール添付で送信する。パスワードの連絡は電話等の別手段で行いメールアドレスの思い込み間違いによるリスクを回避する。ただし，委託元等から強く別メールでの連絡を求められた場合は，その限りではない。

②同報通信は，全て Bcc でアドレスを設定する。

③送信前にアドレスを再確認する。特に重要なメールについては，空メールを一度送信し，返信を受けたメールへの返信で送信する。メールアドレスのオートコンプリート機能を使用しない。

④電子メールのアドレス帳には氏名だけでなく，社名等も入れ，同姓同名あるいは類似氏名等による宛先ミスを防止する。

⑤出所不明で悪意が含まれる危険性のあるメールの受信時は絶対に開かないで削除し、情報システム管理者に通報する。

(3)FAX の利用

①送信ボタンを押す前に宛先 FAX 番号を再確認する。特に重要な書類の場合には空 FAX を送信し，到着確認してから本文を送信する。

②送信後速やかに送信先に FAX 送信の通知をする。

③FAX を受信する場合は送信元から FAX 送信の通知を依頼し，長時間放置しない。可能であれば，受信時にはフォルダに保管し印刷を手動で行う方式にする。

(4)外部との接続(ファイル転送，ダウンロード，アップロード等)

①社外にあるサーバとの通信で個人情報を取り扱う場合には，VPN 回線利用，暗号化

等の盗聴防止措置を講じる。

(5)リモートアクセス

①リモートアクセスは原則禁止であり，必要な場合には個人情報保護管理者の承認の元に，情報システム管理者の指示に従って安全管理措置を講じて行う。

②特に自宅作業等で使用する場合には作業環境と作業条件を確認する。

(6)無線 LAN

①無線 LAN を使用する場合には，WPA2-AES 以上の強度を持つ暗号化を適用し，接続を ID とパスワードで制限する。ESSID のステルス化を適用する。

6.個人情報を取り扱う情報システム構築及び変更時の対策

(1)Web 入力フォーム

①個人情報を取得する Web 入力フォームには SSL を適用する。

(2) 個人情報を取り扱う情報システムの脆弱性対策

①SQL インジェクション，クロスサイトスクリプティング等の攻撃に対する脆弱性の構築手順を定め，それに従って構築する。

②情報システムの開発及び保守を委託する場合には，要求仕様に脆弱性対策を盛り込む。

③保守等で情報システムを変更した時には，リリース前に脆弱性対策が損なわれていないことを確認する。

④特にリスクの高い情報システムについては専門業者にペネトレーションテスト等を委託して確認する。

7.個人情報を取り扱う情報システムの監視

(1)情報システム管理者はサーバへのアクセスログを取得し，1 年分を保管する。

(2)情報システム管理者は毎月 1 回，保管されているアクセスログから，不正アクセスの兆候有無等を確認し「運用確認チェックリスト」に記録する。

8.モバイル機器の安全管理措置

(1)当社から貸与したモバイル機器

①当社が定めたマルウェア対策ソフトをインストールし，最新状態に維持する。ただし，フィーチャフォン，PHS 等はその限りでない。

②アプリケーションを情報システム管理者の許可なく搭載しない。

③社内ネットワークに接続しない。社内ネットワーク接続が必要な場合は上長経由で情報システム管理者の許可を得る。

④個人情報の登録は必要最小限にし，不要になったアドレス情報，メール，留守録を速やかに削除する。

⑤使用時は覗き見，傍聴に注意する。

⑥紛失，盗難を防ぐため，手から離さないようにする。

⑦ナンバーロックの設定をする。可能な機種についてはリモートワイプ機能の設定を

する。

⑧紛失，盗難にあった場合については，直ちに個人情報保護管理者に連絡する。

⑨廃棄時は物理的に破壊する又は購入先に持ち込んで完全消去を依頼する。リース/レンタルの場合には返却時に完全消去をさせる。

(2)私用モバイル機器の業務利用

①当社から貸与したモバイル機器に準じて利用する。

②業務利用で発生した事件や事故に該当する，あるいは該当する可能性のある事態が発生した場合には直ちに個人情報保護管理者に連絡する。

9. リース，レンタル機器の返却

(1)返却時には機器内のメモリから個人情報を完全消去する。

(2)当社内での完全消去が困難な場合には，リース，レンタルの契約時に契約先が完全消去する契約を締結する。あるいは返却時に契約し，証明書を受け取って保存する。

C.テレワーク時の安全管理措置

1. 作業場所施設（自宅等）の入退室管理

(1)出入口は入退室の都度，施錠する。

テレワーク作業者，家族等の同居人，及び来訪者が出入りするたびに開錠し、出入り後に施錠する。

(2)出入口の鍵等（物理鍵または ID カード）の管理

鍵等の所持者をテレワーク作業者，家族等の同居人に限定する。

鍵等の紛失時には，拾得者が侵入することができない対策を講じる。少しでも，そのリスクがある場合は，錠と鍵を新しいものに交換する。

(3)テレワーク作業者の外出時の安全確認

テレワーク作業者毎に、各自作業環境の実情に配慮したチェックリスト「外出時確認チェックリスト」を作成し，個人情報保護管理者に提出する。

テレワーク作業者は，自身の「外出時確認チェックリスト」でクリアデスク，施錠,クリアスクリーン等を確認してから外出する。

2. 作業上の安全確保

(1)作業開始前

テレワーク作業者が作業する机上が同居人や来訪者から覗きこまれない状況を整備する。可能であれば別室で作業する。

(2)作業中

印刷物が同居人や来訪者の目に触れないに印刷後、直ちに回収する。

業務上の連絡は同居人や来訪者に漏れないメール等の手段で行う。

どうしても電話等での連絡が必要になる場合には、会話の内容が同居人や来訪者に伝わらないような措置を講じる。

FAX で受信する場合にはフォルダに一時保管し，印刷時に直ちに回収する。受信

FAX のフォルダ保管ができない場合は、送信者に送信直前に連絡を受けて印刷機の前で待機する等の措置を講じる。

離席時にはクリアデスクし，PC をログオフする。ログオフ忘れ対策として，5 分以内のパスワード付きスクリーンセーバ起動又は自動ログオフを設定する。

紙媒体の廃棄時にはシュレッダで細断してから廃棄する。

電子媒体の廃棄時は，物理破壊するか，データを全て削除してから専門業者に完全消去と廃棄を委託しマニフェストを保管する。

PC 及びハードディスクの廃棄時は，ハードディスクを物理破壊するか，専用ソフトウェアで完全消去してから廃棄する。あるいはデータを全て削除してから専門業者に完全消去と廃棄を委託しマニフェストを保管する。

(3)作業終了時

①クリアデスクの徹底

特に個人情報を記録した媒体（電子媒体，紙）を所定キャビネット又は机の抽斗に施錠保管する。

②端末及び PC の不正使用と盗難防止

業務で使用する端末及び PC をシャットダウンする。

ノート型 PC 及び外付けハードディスクを所定キャビネット又は机の抽斗に施錠保管するか，セキュリティワイヤで固定する。

3.テレワーク先で使用する情報システムの安全管理措置

(1)業務利用の端末や PC を私用と分離

原則として業務で使用する端末や PC を私用（同居人による利用を含む）で利用しない。

どうしても機器の共用が必要になる場合はアカウントを別にし，アカウント間でファイルを共用しない。

4.その他の情技術的安全管理措置

“B.技術的安全管理措置”の“2.情報システム利用者の識別と認証”以降の既定内容をテレワークの場合にも基本的に適用する。

A.3.4.3.3 従業者の監督

【規程】

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，従業者に対し必要，かつ，適切な監督を行う。

【要点】

1.「誓約書」の提出を求める対象者

(1)受入派遣社員以外の従業者には雇用契約又は委託契約時に「誓約書」の提出を求める。

(2)受入派遣社員については不要

派遣元企業と秘密保持契約を締結する。

2.「誓約書」の内容に関する不可欠な事項

(1)個人情報の非開示契約になっていること

(2)退職（契約終了）後も一定期間有効であること

3.罰則適用については就業規則等に基づいて行う必要がある。(原則)

【手順】

1.従業者の監督

従業者には本規程を周知徹底させ，遵守させるように管理及び監督する。

2.従業者との非開示契約締結

(1)受入派遣社員以外の従業者には雇用契約又は委託契約時に「誓約書」の提出を求める。

(2)「誓約書」には，個人情報の非開示契約と退職（契約終了）後も一定期間有効であることを盛り込む。

3.PMS 違反者への処置

PMS に違反した場合は「就業規則」の罰則事項適用の対象になる。

4.ビデオ及びオンラインによる従業者のモニタリング

(1)モニタリング実施責任者

モニタリング実施責任者は個人情報保護管理者とする。

(2)従業者へのモニタリングの目的の明示

モニタリング実施責任者はモニタリングを開始する前に,全従業者にモニタリングの内容，方法，目的を文書で明示する。

(3)モニタリングに対する監査

個人情報保護監査責任者はモニタリングした個人情報が定めた利用目的の範囲内だけで使用されていることを内部監査時に点検する。

A.3.4.3.4 委託先の監督

【規程】

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。

個人データの取扱いの全部又は一部を委託する場合は，十分な個人情報の保護水準を満たしている者を選定する。このため，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。

個人データの取扱いの全部又は一部を委託する場合は，委託する個人情報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。

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

当該契約書などの書面を少なくとも個人情報の保有期間にわたって保存する。

【要点】

1. 全ての委託先を評価して選定すべきである。

国家資格を保有しかつ法律により守秘義務を課されている者，プライバシーマーク取得業者といえども，評価すべきである。これらは当社が必要としている個人情報の保護水準を保証するものではない。

2. 評価基準を毎年見直し，委託先を再評価すべきである。

世の中の動向，技術進歩等により評価基準，手順は見直されるべきである。

委託先の状況も日々変化する。

【手順】

1. 委託先選定基準の制定と見直し

(1)個人情報保護管理者は委託先選定基準を定め，委託先を評価する記録「委託先評価表」を制定する。

(2)個人情報保護管理者は，毎年「年間計画書」に定める時期に，必要に応じて適宜に，委託先選定基準を見直し，その結果で「委託先評価表」を改正する。

2. 委託先の評価と定期的再評価

(1)新規委託先の評価と選定

①委託先候補を「委託先評価表」で評価して合否判定を行い，個人情報保護管理者の承認を得る。個人情報保護管理者は承認後に当該委託先候補を「委託先管理台帳」に登録する。

②不合格となった委託先候補には委託しない。ただし，他に候補が無い場合等については，当該委託先候補に対し是正を求め，是正完了までの残留リスクを認識した上で，トップマネジメントの承認が得られた場合には例外的に委託できる。

(2)委託先の再評価

①「委託先管理台帳」に登録されている全委託先を毎年「年間計画書」に定める時期に，及び適宜に最新の「委託先評価表」で再評価し，個人情報保護管理者の承認を得る。

②再評価の結果で不合格となった場合の措置は(1)②の措置を行う。

3. 委託先との個人情報保護に関する契約

(1)下記いずれかの使用する様式で委託先と締結する。

①a)～g)の事項が盛り込まれた業務委託契約書

②「委託個人情報の保護に関する覚書」

(2)締結できない委託先については下記の代替措置を行う。

①利用規約，利用約款等を確認する。

②ホームページ等に公表されている個人情報保護方針を確認する。

③上記経緯を「委託先管理台帳」に記録し，個人情報保護管理者の承認を得る。

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

【規程】

保有個人データに関して，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，次の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と秩序維持に支障が及ぶおそれのあるもの

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わなければならな い。

【要点】

1. 保有個人データには，直接書面以外で取得した個人情報も含まれることがある。

(1)写真，映像，録音等も開示等の請求等に応じることができる場合は保有個人データに含めるべきである。

(2)第三者提供で取得した個人情報も開示等の請求等に応じることができる場合は保有個人データに含めるべきである。ただし，当然ながら提供元の個人情報については請求等に応じることはできないし，不要である。

(3)受託業務で取得した個人情報は開示等の請求等に応じることも委託された場合を除

き，開示等の請求等に応じる権限が無いので，保有個人データとしない。

2.本項のただし書きは2時点で適用する。

(1)個人情報特定時

ただし書きに該当する場合には，個人情報を特定する際に保有個人データとしない。

(2)開示等の要求があった時

ただし書きにより保有個人データとしていない個人情報について開示等の要求があった場合に，請求等に応じないことの回答及び承認手続で使用する。

【手順】

1.個人情報特定時に保有個人データとするか否かを決定する。

(1)保有個人データとするか否かの判断

①保有個人データとするか否かを定める。

・本人から直接書面によって取得した個人情報は保有個人データである。

・本人から直接書面以外の方法で取得した個人情報については【要点】1.項を参考に定める。

②ただし書きa)～d)に該当する場合は，保有個人データとしない。

(2)承認手順

保有個人データとするか否かを「個人情報取扱申請書」の“開示対象”欄に記入して，個人情報特定時に個人情報保護管理者の承認を得る。

2.ただし書きa)～d)を適用して保有個人データとしない場合の承認手順

個人情報の特定時に，例外適用の事項と理由を記載した「例外承認申請書」を「個人情報取扱申請書」と共に提出して，個人情報保護管理者の承認を得る。

A.3.4.4.2 開示等の請求等に応じる手続

【規程】

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)開示等の請求等の申し出先

b)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)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（定めた場合に限る。）の徴収方法

本人から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する。A.3.4.4.4 又は A.3.4.4.5 によって本人からの請求等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，その額を定める。

【要点】

1.情報主体である本人は開示等を請求する権利を持っている。

ただし書きに該当する場合を除き，開示等の請求等に応じなければならない。

2.本人又は代理人以外に開示することは漏洩である。

(1)開示等を求める者（以下，請求者と記述）が本人又は正当な代理人であることの確認が必要である。

(2)本人又は代理人の確認手順を状況に応じて決めるべきである。

①本人確認手順を厳格に行う必要があるが，過剰な負担とならない配慮が必要である。

②ID/パスワードで本人確認するのはコンピュータシステム上の手順であり，開示等を求める者の本人確認でパスワードの提示を求めるべきでない。

③本人確認する証明書が“写真入り”であることが有効なのは対面で本人確認する場合だけである。

【手順】

1. 開示等の請求等の申し出先

(1)個人情報保護管理者は開示等の請求等の申し出先として，「個人情報ご相談窓口」を設置し，窓口責任者にPMS事務局を任命する。

(2)窓口責任者は，個人情報保護管理者の指揮下で開示等の請求等の受付，対応，請求者への回答及び個人情報保護管理者への報告を行う。

(3)「個人情報ご相談窓口」の連絡先情報をホームページ上の「個人情報保護方針」及び「個人情報に関する公表事項」に公表する。

2.開示等の請求等の受付手順

(1)窓口責任者は開示等の請求等の請求者に「個人情報開示等請求書」を郵送させて受け付ける。ただし請求者が従業者の場合は手渡しでも受け付ける。

①「個人情報開示等請求書」の様式をホームページ上からダウンロードできるようにする。

②請求者がホームページ上からダウンロードできない場合は，郵送等の措置を行う。

(2)窓口責任者は本人確認又は代理人の確認を行う。

①開示等の請求等を本人から受け付けた場合

・従業者から対面で受け付ける場合は，社員証の提示を求める。

・郵送で受け付けた場合にはコールバックして氏名，生年月日等を聞き，当社内で保有している個人情報と照合する。当社内で保有している個人情報であって，本人以外の者が知らない属性を選んで質問する。

・コールバックで確認できない場合は，本人確認書類（運転免許証等）の写しを郵送させ，確認する。

②法定代理人による場合

法定代理人であることを証明する公的証明書と代理人の本人確認書類の写しを「個人情報開示等請求書」と同封させて受取り，確認する。

③委任代理人による場合

委任状と印鑑登録証明書及び代理人の本人確認書類の写しを「個人情報開示等請

求書」と同封させて受取り，確認する。

(3)利用目的の通知と開示の請求等の場合には，PMS 事務局は手数料 1,000 円分の切手が同封されていることを確認する。

(4)窓口責任者は受付処理結果を「開示等対応記録」に記録し，個人情報保護管理者に報告する。

3.開示等の請求等への対応手順

(1)開示等の請求等に応じることの可否を判断し，「開示等対応記録」に記録する。

①「個人情報管理台帳」の“開示対象”欄に“保有個人データ”又は“開示”と記入されていない場合には請求等に応じられない。

②下記等の不備がある場合には応じられない場合がある。連絡できる場合は丁重に，追加資料，差替え資料等の提出を依頼する。

・請求資料(本人確認資料等を含む)が不備

・利用目的の通知又は開示の請求等の場合の手数料が不足　等

③A.3.4.4.4～A.3.4.4.7 のただし書きに該当する場合には応じられない場合がある。適用するただし書きを「開示等対応記録」に記入する。

(2)開示等の請求等に応じる手順の決定

①窓口責任者は開示等の請求等に応じる（応じない場合も含む）手順の詳細とスケジュールを定めて「開示等対応記録」に記入する。なお，本人への回答期限は 5 営業日以内を原則とする。5 営業日を超える場合には，事前に請求者に連絡して了承を得る。

②窓口責任者は「開示等対応記録」で個人情報保護管理者の承認を得る。

(3)窓口責任者は個人情報保護管理者の承認を得た「開示等対応記録」に基づいて対応し，その結果を「開示等対応記録」に記録する。

4.回答手順

(1)回答文書の作成（請求等に応じない場合も含む）

窓口責任者は対応結果について，「個人情報開示等回答書」を作成する。

(2)回答文書の承認と発送

窓口責任者は「個人情報開示等回答書」を「開示等対応記録」に添えて個人情報保護管理者に提出し，「開示等対応記録」に承認を得てから，配達を追跡できる方法で「個人情報開示等回答書」を請求者に送付する。

A.3.4.4.3 保有個人データに関する事項の周知など

【規程】

保有個人データに関し，次の事項を本人の知り得る状態（本人の請求等に応じて遅滞なく回答する場合を含む。）に置く。

a)当社の社名

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)すべ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し出先

e)当社が認定個人情報保護団体の対象事業者である場合には，当該認定個人情報保護団体の名称及び苦情の解決の申し出先

f)A.3.4.4.2 によって定めた手続

【手順】

1.公表文書の作成

PMS 事務局は a)～f)の事項を記載した「個人情報に関する公表事項」を作成し，個人情報保護管理者の承認を得る。

2.公表方法

PMS 事務局は「個人情報に関する公表事項」を求められた時には速やかに印刷して渡す。

ホームページ構築後は「個人情報に関する公表事項」を掲載する。

A.3.4.4.4 保有個人データの利用目的の通知

【規程】

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。

【手順】

1.利用目的の通知の請求等を受け付けた時は“A.3.4.4.2 開示等の請求等に応じる手続”に定める手順で対応する。

A.3.4.4.5 保有個人データの開示

【規程】

本人から当該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，当該保有個人データを書面（開示の請求を行った者が同意した方法があるときは，当該方法）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) 当社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

【手順】

1. 開示の請求等を受け付けた時は“A.3.4.4.2 開示等の請求等に応じる手続”に定める手順で対応する。

A.3.4.4.6 保有個人データの訂正，追加又は削除

【規程】

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，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。

【手順】

1. 訂正等の請求等を受け付けた時は“A.3.4.4.2 開示等の請求等に応じる手続”に定める手順で対応する。

A.3.4.4.7 保有個人データの利用又は提供の拒否権

【規程】

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。

【手順】

1. 利用停止等の求めを受け付けた時は“A.3.4.4.2 開示等の請求等に応じる手続”に定める手順で対応する。

A.3.4.5 認識

【規程】

従業者に以下の事項を認識させる。

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，PMS 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

従業者が 上記の認識をもつために，関連する各部門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

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。

【要点】

1.全従業者が教育の対象である。

非常勤役員，社外取締役も教育対象に加える必要がある。ただし，執務状況等の実態に即した教育内容及び教育方法で行うことは可能である。

2.以下の委託先社員も教育の対象にするのが望ましい。(契約上できない場合を除く。)

①当社内に常駐して作業する委託先社員

②当社社員と一緒に客先常駐で作業する委託先社員

3.新規要員については担当業務開始前に教育を行う。

【手順】

1.定期教育の実施（年 1 回以上）

(1)PMS 事務局は毎年「教育計画書」に基づいて，及び適宜に，全従業者を対象とする教育を実施する。

(2)委託先社員も当社又は客先常駐者については極力，教育に参加させる。

(3)教育終了後に「理解度確認テスト」を実施して理解度を確認する。PMS 事務局は不正解について不正解となった理由を説明し理解させる。正答率が 80%未満の受講者には再教育を行う。

(4)PMS 事務局は教育対象者の参加日付と「理解度確認テスト」の結果を「教育受講者名簿」に記録する。

2.新規要員教育の実施

(1)PMS 事務局は毎年「教育計画書」に基づいて，新規要員に対して担当業務開始前に教育を実施する。

(2)新規要員に対する教育実施手順は前項と同様とする。

3.教育結果の報告，レビューと次回計画への反映，記録の保管

(1)「教育実施報告書」の作成

PMS 事務局は教育の実施結果を「教育実施報告書」に記録して，個人情報保護管理者に報告する。

(2)教育実施結果のレビューと次回計画への反映

①個人情報保護管理者と PMS 事務局は「教育計画書」と「教育実施報告書」を対比し，

教育計画の達成度，改善すべき事項，今後の教育方針を整理して，「教育実施報告書」に記入する。なお，必要であれば関係者を招集してレビュー会議を実施する。

②個人情報保護管理者は「教育実施報告書」を承認してから，トップマネジメントに報告し，トップマネジメントの承認を得る。

(3)教育記録の保管

PMS 事務局は教育関連の全ての記録を 2 年以上保管する。

A.3.5 文書化した情報

A.3.5.1 文書化した情報の範囲

【規程】

次の PMS の基本となる要素を書面で記述する。

a)内部向け個人情報保護方針

b)外部向け個人情報保護方針

c)個人情報保護規程

d)個人情報保護規程に定める手順上で使用する様式

e)計画書：「年間計画書」，「教育計画書」，「監査計画書」

f)JIS 要求事項(JIS Q 15001:2017)が要求する記録及び PMS を実施する上で必要と判断した記録

A.3.5.2 文書化した情報（記録を除く。）の管理

【規程】

JIS 要求事項(JIS Q 15001:2017)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，維持する。文書化した情報の管理手順には，次の事項が含める。

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

【要点】

1.全従業者が 最新版の文書により PMS 活動することが目的である。これは記録についても同様である。

【手順】

1.文書の発行及び改正

(1)文書の発行

①個人情報保護方針，個人情報保護規程及び計画書の発行時にはトップマネジメントの承認を得る。

②初回発行時の版を第1版とし，発行日付も記入する。

③「PMS 文書・様式一覧表」に第1版の発行日付を記入する。

(2)文書の改正

①個人情報保護方針,個人情報保護規程及び計画書の改正時にはトップマネジメントの承認を得る。

②改正の都度，版数を1ずつ加算し，発行日付も記入する。但し，単なる字句の修正時は版数を変更しないことも可能とするが，発行日付は更新する。

③「PMS 文書・様式一覧表」に改正した版数と日付を記入する。

2.文書の閲覧と最新版の確認

(1)ファイルサーバの共有フォルダに最新版の PMS 文書と「PMS 文書・様式一覧表」を掲載し，全従業者が閲覧できるようにする。

(2)PMS 文書が最新であるか否かの確認は「PMS 文書・様式一覧表」中の版数と発行日付(改正日付)の照合で行う。

A.3.5.3 文書化した情報のうち記録の管理

【規程】

PMS 及び JIS 要求事項(JIS Q 15001:2017)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ことに伴って当該個人データが提供される場合

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

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。

【手順】

1.記録様式の制定と改正

(1)様式の制定

①a)～1)の事項を含む記録の体系を定める。

②様式の制定時には個人情報保護管理者の承認を得る。

③初回制定時の版を第1版とし，発行日付も記入する。

④「PMS 文書・様式一覧表」に第1版の制定日付を記入する。

(2)記録様式の改正，

①様式の改正時には個人情報保護管理者の承認を得る。

②改正の都度，版数を1ずつ加算し，発行日付も記入する。但し，単なる字句の修正時は版数を変更しないことも可能とするが，発行日付は更新する。

③「PMS 文書・様式一覧表」に改正した版数と日付を記入する。

2.様式の入手と最新版の確認

(1)ファイルサーバの共有フォルダに最新版の記録様式と「PMS 文書・様式一覧表」を掲載し，全従業者がダウンロードできるようにする。

(2)記録様式が最新であるか否かの確認は「PMS 文書・様式一覧表」中の版数と発行日付(改正日付)の照合で行う。

3.記録の作成，保管及び承認

(1)記録の作成者，保管者，承認者及び保管期限は「PMS 文書・様式一覧表」上に定める。

(2)記録の作成者は本規程に定める手順に従って記録を作成し，承認者に提出して承認を得る。

A.3.6 苦情及び相談への対応

【規程】

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。

上記の目的を達成するために必要な体制の整備を行う。

【要点】

1.苦情及び相談の対象は開示等の請求等と異なり，本人の個人情報の取扱いに関してだけでなく，以下の質問例のようにPMSの運用に関する場合もある。

(1)個人情報を取得するWeb入力フォームにSSLが適用されていないのでは？

(2)死亡した従業者の訃報を受け取ったが本人は同意しているのか？　等

2.本人の個人情報の取扱いに関する苦情及び相談の場合は本人確認をする必要があるが，その他の場合には匿名でも受け付けるべきである。匿名の場合には，苦情及び相談への対応結果を報告することができないことを考慮して対応する必要がある。

3.苦情の場合は認定個人情報保護団体(JIPDEC 等)に申し出があり，認定個人情報保護団体から通知される場合もある。

【手順】

1. 苦情及び相談の受付窓口の設置と連絡先の公表

(1)個人情報保護管理者は苦情及び相談の申し出先問合せ窓口として，「個人情報ご相談窓口」を設置し，窓口責任者にPMS事務局○○を任命する。

(2)窓口責任者は，個人情報保護管理者の指揮下で苦情及び相談の受付，対応，相談者への回答及び個人情報保護管理者への報告を行う。

(3)「個人情報ご相談窓口」の連絡先情報をホームページ上の「個人情報保護方針」及び「個人情報に関する公表事項」に公表する。

2. 苦情及び相談の請求等の受付手順

(1)窓口責任者が苦情及び相談を受け付ける。

①窓口責任者以外の者が電話やメール等で受け付けた場合には，窓口責任者(不在時は個人情報保護管理者)に回し，自身では受け付けてはならない。

②書面以外の手段でも受け付ける。

(2)本人の個人情報の取扱いに関する苦情の場合は，窓口責任者は本人確認を行い，確認できない場合は対応しない。本人確認はA.3.4.4.2【手順】2.(2)の手順で行う。

(3)匿名で受け付けた場合には苦情及び相談への回答ができないので，回答が必要な場合には，“～日後に再度PMS事務局宛にお電話戴ければ，対応結果をお知らせ致します。”等を伝えて，再度の相談者からの連絡を依頼する。

(4)窓口責任者は受付内容と経緯を「苦情相談等対応記録」に記録し，個人情報保護管理者に報告する。

3. 苦情及び相談への対応手順

(1) 苦情及び相談に応じる手順の決定

①窓口責任者は苦情及び相談に応じる手順の詳細とスケジュールを定めて「苦情相談等対応記録」に記入する。なお，本人への回答期限は10営業日以内を原則とする。10営業日を超える場合には，事前に相談者に連絡して了承を得る。

②窓口責任者は「苦情相談等対応記録」で個人情報保護管理者の承認を得る。

(3)PMS事務局は個人情報保護管理者の承認を得た「苦情相談等対応記録」に基づいて対応し，その結果を「苦情相談等対応記録」に記録する。

4. 相談者への回答

(1)回答文書の作成

窓口責任者は対応結果について，「苦情相談等回答書」を作成する。

(2)回答文書の承認と発送

窓口責任者は「苦情相談等回答書」を「苦情相談等対応記録」に添えて個人情報保護管理者経由でトップマネジメントに提出し，「苦情相談等対応記録」に承認を得てから，配達を追跡できる手段で「苦情相談等回答書」を相談者に送付する。

A.3.7 パフォーマンス評価

A.3.7.1 運用の確認

【規程】

PMS が適切に運用されていることが，各部門及び階層において定期的に，及び適宜に確認されるための手順を確立し，実施し，かつ，維持する。

不適合が確認された場合は，各部門及び各階層の管理者は，その是正処置を行う。

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。

【要点】

1. 不適合を早期発見し，事故の芽を早期に摘む目的で行われる。発見された不適合への是正処置は必須である。他部門で同様不適合が発生しない予防にも活用すべきである。
2. 各部門が自主的に行う定期的点検であり，「運用確認チェックリスト」は部門の運用実態に即して作成，維持すべきである。

【手順】

1. 「運用確認チェックリスト」の作成
   (1) 各部門の責任者は，年度末に次年度の自部門の「運用確認チェックリスト」を作成し，個人情報保護管理者の承認を得る。
   (2) 「運用確認チェックリスト」の作成に際しては前年度の実績，部門を取り巻く環境の変化等を考慮する。
2. 運用の確認の実施と実施結果の報告
   (1) 各部門の責任者は，担当者に毎月初に「運用確認チェックリスト」を使用して自部門の前月の運用状況を点検させ，その結果を報告させる。
   (2) 各部門の責任者は，担当者から受け取った「運用確認チェックリスト」を確認して，個人情報保護管理者に提出する。
3. 運用の確認実施結果のレビューと是正・予防処置
   (1) 個人情報保護管理者は各部門から提出された「運用確認チェックリスト」を確認し，承認する。
   (2) 「運用確認チェックリスト」に不適合が発見された場合は，当該部門に是正処置を指示する。
   (3) 重大な不適合が発見された場合には，他部門にも警告を発し，同一不適合の発生を未然に防ぐように点検の強化を指示する。

A.3.7.2 監査

【規程】

JIS 要求事項(JIS Q 15001:2017)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。

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。

【要点】

1. 適合性監査と運用監査の 2 段階で内部監査を行う。
   (1)適合性監査
   PMS の規程類が JIS 要求事項(JIS Q 15001:2017)を満たしているかを監査する。
   (2)運用監査
   JIS 要求事項(JIS Q 15001:2017)を満たしている PMS の規程類に定めていることが遵守されているかを監査する。
2. 運用監査の対象は全部門である。個人情報の取扱いが無いと判断している部門であっても，個人情報の取扱いが無いことの確認は必要である。
3. 実際に監査を行う監査員は被監査部門に所属しない者から選ぶ。なお，個人情報保護監査責任者はトップマネジメントが内部の者から指名するが，監査員は外部の者から選任できる。
4. 客先常駐作業及び社外で行う業務(移送，送信等)も監査対象である。ただし，客先で内部監査を実施することが困難な場合には帰社日等にインタビュー方式で監査する等の方法で行う。

【手順】

1. 内部監査の計画
   (1)個人情報保護監査責任者は毎年「監査計画書」を作成し，「監査計画書」に基づいて，及び適宜に適合性監査と全部門を対象とする運用監査を実施する。
   (2)被監査部門の構成を計画時に決定する。
   ①業務組織とは独立した被監査部門
   以下の部門については，業務組織と独立して運用監査を行う。
   個人情報保護管理者及び PMS 事務局
   情報システム管理部門
   ②業務組織別被監査部門
   全業務組織が運用監査の対象に含まれる必要がある。事業部単位あるいは部単位で被監査部門を設定するかは，組織構成と業務内容を考慮して決める。

(3)内部監査を実施する監査員を個人情報保護監査責任者が指名するが,監査員は被監査部門に所属しない者を選ぶ。

2.監査員の養成

(1)監査員を内部から指名して自部門監査を回避するためには,少なくとも異なる2部門に監査員が必要である。コンサルタント会社等に監査員業務を委託する場合はこの限りではない。

(2)監査員はJIS要求事項(JIS Q 15001:2017)と当社のPMSを理解し,当社事業での個人情報の取扱い実態を把握していることが求められるが,個人情報保護監査責任者は監査員の養成計画を立案して実施する。

3.適合性監査の実施手順

(1)被監査部門は個人情報保護管理者及びPMS事務局とする。

(2)当社規程とJIS要求事項(JIS Q 15001:2017)を「規格適合性監査チェックリスト」で照合し,その結果を「規格適合性監査チェックリスト」に記入する。

(3)監査員は「規格適合性監査チェックリスト」を整理して「監査報告書(規格適合性監査編)」を作成し,チェックリストと共に個人情報保護監査責任者に提出する。

4.全部門を対象とする運用監査の実施手順

(1)個人情報保護監査責任者は運用監査用の下記チェックリストを監査員に用意させる。

①「運用監査チェックリスト(事務局)」

個人情報保護管理者及びPMS事務局を被監査部門として全社的PMS運用について監査するために使用する。

②「リスク分析表」の写し

個人情報保護管理者及びPMS事務局を被監査部門として,「リスク分析表」の“講じる対策”が実施されているか,また“残留リスク”に顕在化の兆候有無を監査するために使用する。

③「運用監査チェックリスト(情報システム)」

情報システム管理部門を被監査部門として,情報システム及びネットワークの運用状況について監査するために使用する。

④「運用監査チェックリスト(部門)」

各部門を被監査部門として,各部門でのPMS運用状況について監査するために使用する。

(2)監査員は監査を実施する。

①監査員はチェックリストに従って被監査部門の担当者に記録の提出を求めて確認する,現場で直接見る等の方法で監査を進め,監査結果をチェックリストに記入する。

②監査員は監査指摘する場合には,被監査部門担当者にその旨と理由を伝えて納得させる。

②監査員はチェックリストの内容を整理して「監査報告書(個別運用監査編)」を作成し，チェックリスト共に個人情報保護監査責任者に提出する。

5.内部監査結果の報告と承認及び記録の保管

(1)個人情報保護監査責任者は,監査員から提出された「監査報告書(規格適合性監査編)」,「監査報告書(個別運用監査編)」とチェックリストを確認してから承認し，監査結果全体を纏めて「監査報告書(総括編)」を作成する。

(2)個人情報保護監査責任者は「監査報告書(総括編)」でトップマネジメントに報告し，トップマネジメントの承認を得る。

(3)個人情報保護監査責任者は「監査計画書」を含めた全ての内部監査の記録を3年間保存する。

6.不適合に対する是正処置

監査指摘があった場合には，個人情報保護監査責任者は個人情報保護管理者経由で当該部門に是正処置の実施を指示する。

A.3.7.3 マネジメントレビュー

【規程】

トップマネジメントは個人情報の適切な保護を維持するために，少なくとも年一回，適宜にPMSを見直す。

マネジメントレビューにおいては，次の事項を考慮する。

a)内部監査及びPMSの運用状況に関する報告

b)苦情を含む外部からの意見

c)前回までの見直しの結果に対するフォローアップ

d)個人情報の取扱いに関する法令，国の定める指針及びその他の規範の改正状況

e)社会情勢の変化，国民認識の変化，技術の進歩などの諸環境の変化

f)事業領域の変化

g)内外から寄せられた改善のための提案

【要点】

1.マネジメントレビューは，PMSの維持，改善を継続する上での経営判断を求めている。

【手順】

1.マネジメントレビューの実施時期（年1回以上）

トップマネジメントは毎年「年間計画書」に基づいて，及び適宜に，マネジメントレビューの開催を個人情報保護管理者に指示する。

2.マネジメントレビューの必須参加者

トップマネジメント，個人情報保護管理者，個人情報保護監査責任者，PMS事務局及び情報システム管理者を必須参加者とし，その他の担当者を必要に応じて参加させる。

3.マネジメントレビューの実施

(1)参加者は自身の役割に関連する a)～g)の事項についてトップマネジメントに報告する。

(2)トップマネジメントは今後の PMS 運営の指針，及び改善すべき事項を指示する。

(3)個人情報保護管理者は議事録として「マネジメントレビュー実施記録」を作成し，トップマネジメントの承認を得る。

4.マネジメントレビュー結果に基づく改善

個人情報保護管理者は「マネジメントレビュー実施記録」に基づいて関連部門に改善を指示する。是正処置に該当する改善の場合は“A.3.8 是正処置”の手順で実施させる。

A.3.8 是正処置

【規程】

不適合に対する是正処置を確実に実施するための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。その手順には次の事項を含める。

a)不適合の内容を確認する。

b)不適合の原因を特定し，是正処置を立案する。

c)期限を定め，立案された処置を実施する。

d)実施された是正処置及の結果を記録する。

e)実施された是正処置及の有効性をレビューする。

【要点】

1.不適合が発見される場面の主なものには以下があり，内部監査や事故だけではない。

①外部機関による審査

②リスク分析

③緊急事態

④苦情

⑤運用の確認

⑥内部監査

⑦内部の者からの改善提案

2.是正処置には再発防止策及び類似不適合発生の予防策が必要であり，以下を必ず確認する。

①不適合発生の根本原因

②類似不適合の潜在有無

③他部門での同一あるいは類似不適合発生の潜在有無

【手順】

1.不適合発見時の報告と承認

(1)不適合発生部門の責任者は不適合の内容と状況を「不適合発生報告書」に記入し，個人情報保護管理者に提出する。

(2)個人情報保護管理者は,「不適合発生報告書」の内容を承認してから，トップマネジメントに報告して承認を得る。

(3)個人情報保護管理者は，トップマネジメントの承認に基づいて，不適合発生部門の責任者に是正処置の立案を期限期限付きで指示する。

2.是正処置の立案

(1)不適合発生部門の責任者は以下の内容を盛り込んだ是正処置案を作成し,「是正処置計画書」に記入する。

①発生した不適合の解消手順

②再発及び類似不適合の発生防止策の策定

・不適合発生の根本原因を究明する。

・不適合発生業務のリスク分析内容を見直す。

・改善案の候補を案出する。

③各改善案の効果とコストを纏めて比較評価

④部門としての推奨案の選択

⑤実施及び有効性確認の計画

(2)不適合発生部門の責任者は「是正処置計画書」を個人情報保護管理者に提出して承認を得る。

(3)個人情報保護管理者は「是正処置計画書」をトップマネジメントに提出して承認を得る。

3.是正処置の実施

(1)個人情報保護管理者は不適合発生部門の責任者に対し,「是正処置計画書」に基づいて是正処置の実施を指示する。

(2)不適合発生部門の責任者は「是正処置計画書」に従って，是正処置を実施し，その結果を「是正処置実施報告書」に記録し，個人情報保護管理者に提出して承認を得る。

4.有効性の確認

(1)不適合発生部門の責任者は「是正処置計画書」に示された時期に，実施した是正処置が定着し，計画通りの効果が実現できていることを確認し,「是正処置有効性確認報告書」に記録し，個人情報保護管理者に提出して承認を得る。