文書番号	ICS－M－007
制定日	２０１０．４．１．
改定日	２０２０．１０．１．
改訂版数	第６版
主管部署	管理部

個人情報保護規定

㈱イカイコントラクト

配布先：第二管理本部（原本）
社長　（ビズシステム）
専務　（ビズシステム）
各部　（ビズシステム）
各事業所　（ビズシステム）
各課　（ビズシステム）

承認	確認	作成
社長 '20/10/01 小山	専務 '20/10/01 林	管理部 '20/10/01 田中

目次

ご注意：文中の □ で囲った部分は JIS 規格の要求事項で、修正することはできません。

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 JIS Q15001:2017「個人情報保護マネジメントシステムー要求事項」に準拠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。

A.1 適用範囲

(1) 本規程の適用範囲は、当社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、改善するため業務上取扱う全ての個人情報とする。
(2) 本規程の適用範囲は、全従業者とする。

A.2 用語および定義

本規程で用いる主な用語及び定義は次の通りとする。

(1) 個人情報： 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など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)。又、下記の個人情報保護委員会規則で定められた個人識別符号①、②も個人情報に含まれる。
   ① 特定の個人の身体の一部の特徴を電子計算のために変換した指紋データ、虹彩データ、顔解析データ、手のひら等の静脈データ、声帯解析データ、歩容解析データ DNA を構成する塩基の配列等。
   ② 対象者ごとに異なるものとなるように役務の利用、商品の購入に際し割り当てられ、また、個人に発行されるカードやその他の書類に記載され、若しくは電磁的方式により記録された文字、番号で、その他の公的な符号である、旅券番号、基礎年金番号、運転免許証番号、マイナンバー、住民票コード、国民健康保険被保険者証の記号番号など。
(2) 個人データ：個人情報を検索することができるように体系的に構成した情報の集合物又は一定の規則に従って整理,分類し,目次,索引,符合などを付すことによって特定の個人情報を容易に検索できるように体系的に構成した情報の集合物（「個人情報データベース」という）を構成する個人情報をいう。いわゆるコンピュータシステムのデータベース、パソコンやスマートフォン、携帯電話の電話帳、検索可能な紙情報の集合体（名簿、名刺入れ）に格納された個人情報をいう。
(3) 保有個人データ：本人などから開示、訂正などの求めがあった場合に応じる権限を持つ個人データ（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を除く）

※法では、6 ヶ月以内に消去予定のものは、保有個人データから除くとされているが、当社においては当該例外は適用しない。

(4) 本人：個人情報によって識別される特定の個人

(5) 個人情報保護管理者：代表者によって当社の内部から指名された者であって、個人情保護マネジメントシステムの実施及び運用に関する責任及び権限を持つ者。

(6) 部門管理者：当社の各部門の管理者で、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を持つ者。但し、部門が存在しない場合設定は不要。

(7) 個人情報保護監査責任者：代表者によって当社の内部の者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。

(8) 個人情報保護教育責任者：個人情報保護管理者が任命し、全従業者に対するＰＭＳ教育を計画、実行する責任及び権限をもつ者。個人情報保護管理者が兼務することができる。

(9) 苦情相談窓口責任者：保有個人データに関する利用目的の通知、開示、追加、訂正、削除、利用又は提供の拒否、消去、及び苦情相談への対応について責任と権限を持つ者。

個人情報保護管理者が兼務することができる。

(10) 個人番号・特定個人情報管理責任者：個人番号・特定個人情報に関する責任及び権限を持つ者で、個人番号・特定個人情報を特定された利用目的の範囲で取り扱い、特定された担当者以外の取扱い・閲覧を防止するよう管理監督する。

(11) 個人番号・特定個人情報事務取扱担当者：個人番号・特定個人情報管理責任者のもと、個人番号及び特定個人情報の取扱いを行うことができる担当者(部門名でも可)。

(12) 従業者：当社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、派遣社員など）も含まれる。

(13) 監査員：個人情報保護監査責任者によって任命され、個別監査計画を立案し、運用監査を実施することができる。但し、自己の所属する部門の監査は実施できない。

(14) 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本人に明示し、本人の承諾を得る意思表示。

また、本人の同意によって生ずる結果について判断能力がない場合（未成年、成年被後見人、被保佐人、被補助人等）は、親権者や法定代理人から同意を得ることとする。

(15) 個人情報保護マネジメントシステム：当社が、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、監査及び見直しを含むマネジメントシステム。「ＰＭＳ」と略して使用することがある。

(16) 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をいう。

(17) 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をいう。

(18) 適合：要求事項を満たしていること。

(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をいう。

(20) 管理策：リスクを修正する対策をいう。

(21) 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。

(22) 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の弱点をいう。

(23) 残留リスク：リスク対応後に残っているリスクをいう。

(24) リスク対応：リスクを修正するプロセスをいう。（リスクの回避、リスク源の除去、起こりやすさの変更、結果の変更、リスクの共有、リスクの保有など）

(25) 緊急事態：個人情報保護リスクの脅威が顕在化した状態をいう。

A.3 管理項目及び管理策

A.3.1 一般

当社は、当社規程に定める A.3.2 から A.3.8 は、代表者によって権限を与えられた者によって、当社が定めた手段に従って承認されなければならない。

(1)A.3.2 から A.3.8 の承認手順は、各条項において定める。

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

(1) 代表者は､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、国が定める指針及び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の継続的改善に関すること。

f) 組織名及び代表者役職名・氏名

(2) 代表者は、内部向け個人情報保護方針を会議等で組織内に周知させるとともに、必要に応じて利害関係者が入手可能な措置（ホームページへの掲載や店頭等での掲示等）を講じなければならない。

A.3.2.2 外部向け個人情報保護方針

(1) 代表者は、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

(2) 代表者は、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（ホームページへの掲載や店頭等での掲示等）を講じなければならない。

A.3.3 計画

A.3.3.1 個人情報の特定

(1) 当社は、当社が自らの事業の用に供する全ての個人情報を特定するための手順を確立し、かつ、維持しなければならない。
(2) 当社は、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しなければならない。
(3) 当社は、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わなければならない。

(4) 個人情報の特定は、以下の要領にて実施する。

① 個人情報の取扱い担当者は、**「P-02 個人情報の特定とリスク分析の手引き」**に従って業務の流れの中で使用する帳票類を考慮し、**「PF-701 個人情報管理台帳」**に(2)の項目等を記載する。

② 部門管理者は、上記**「PF-701 個人情報管理台帳」**に特定漏れがないかを確認の上、個人情報保護管理者の承認を得る。

③ 新種の個人情報は、**「PF-111 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、**「PF-701 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。

④ **「PF-701 個人情報管理台帳」**は、*毎年６月*及び必要に応じて随時、部門管理者が見直しを行い、個人情報保護管理者の承認を得る。見直しを行なう際は、個人情報の利用目的、アクセス権限者、利用期限、保管期限等の各記載事項が適切かに留意する。

A.3.3.2 法令、国が定める指針及びその他の規範(以下法令等という)

(1) 個人情報保護管理者は、個人情報の取扱に関する法令、国が定める指針その他の規範を特定して参照できる手順を確立し、維持しなければならない。

(2) 法令等の特定は以下の要領にて行う。

① 対象とする法令等は、個人情報保護法、マイナンバー法、個人情報保護委員会や一部の関係省庁が示す基準、ガイドライン、及び業界が示す指針等、並びに自治体からの業務を受注する場合には当該自治体の個人情報保護条例等を、個人情報保護管理者が**「PF-103 個人情報保護に関する法令・規範一覧表」**に特定するものとする。

② 特定した法令等は**「PF-103 個人情報保護に関する法令・規範一覧表」**の URL に基づいて全従業者が閲覧可能な状態とする。

③ ①で特定した法令等は、個人情報保護管理者が、*毎年 6 月*及び必要に応じて随時、(1)項に示す法律、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**「PF-103 個人情報保護に関する法令・規範一覧表」**を改訂するものとする。

A.3.3.3 リスクなどの認識、リスクアセスメント及びリスク対策

(1) 個人情報保護管理者は、A.3.3.1 におい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、維持しなければならない。
(2) 個人情報保護管理者は、A.3.3.1 において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、維持しなければならない。
(3) 当社は、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、管理しなければならない。
(4) 当社は、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、適宜に見直さなければならない。

(5) 個人情報の取扱いの各局面におけるリスクとは、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、本人への影響などの恐れ等を含み、それらを分析し必要な対策を講じる手順を確立し、維持しなければならない。

(6) リスクの認識、リスクアセスメント、リスク対策は**「P-02 個人情報の特定とリスク分析の手引き」**に従って、以下の要領で行い、**「PF-702 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が承認した後に個人情報保護責任者が承認する。
これは、リスク対策には、人･物･金等の経営資源を必要とする場合があるので、個人情報保護責任者の承認を得る。

① 個人情報の業務の流れの類型化を図る
「PF-701 個人情報管理台帳」に特定した個人情報ごとに以下の手順でリスク分析を行なう。この際、業務の流れ（ライフサイクル局面）が同じ個人情報についてグループ化しリスク分析を集約することができる。

② 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想定リスクとして記述する。

③ リスク対策を記述する
想定リスクごとにリスクに対する対策を記入する。

④ 関連する規程類の記入

リスク対策を参照できるよう、関連する規程類の規程名と項番を記入する。

⑤ 残留リスクの記述

対策後においても人・物・金等の制約でリスクを完全には回避できない未対応部分を「残留リスク」として記述する。

但し、ヒューマンエラーや従業者の悪意によるリスクはなかなかゼロには出来ないと思われるため、これらに配慮した教育や監査・点検などの対策が実施されている場合は、残留リスクは記載しないものとする。

(7) **「PF-702 個人情報リスク分析対策表」**の更新

① 利用目的変更・取扱い方法変更の場合

ｱ) 部門管理者は、変更する前の**「PF-702 個人情報リスク分析対策表」**を参考に、当該部門の個人情報の想定リスク、リスク対策、リスク対策の規程、残留リスク等のリスク分析の見直しを行う。

ｲ) 個人情報保護管理者の承認の後に個人情報保護責任者の承認を受ける。

② 個人情報を削除する場合

ｱ) **「PF-702 個人情報リスク分析対策表」**から当該個人情報を削除する。この際、削除履歴が残るようにしておく。

ｲ) 個人情報保護管理者の承認の後に個人情報保護責任者の承認を受ける。

(8) **「PF-702 個人情報リスク分析対策表」**の見直し

「PF-702 個人情報リスク分析対策表」は、*毎年６月*に、部門管理者が見直しを行い、個人情報保護管理者の承認の後に個人情報保護責任者の承認を受ける。

随時見直しは部門管理者が新業務の追加や既存業務の変更などからリスクの見直しを実施することを決め、実施し、個人情報保護管理者の承認の後に個人情報保護責任者の承認を受ける。

A.3.3.4 資源、役割、責任及び権限

(1) 代表者は、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
(2) 代表者は、この規格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、個人情報保護マネジメントシステム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。
(3) 個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならない。
(4) 代表者は、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。
(5) 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、代表者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。
(6) 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。

(7) 個人情報保護に関する主たる責任と権限は以下の通りとする。各責任者の氏名は**「PF-104 個人情報保護体制図」**に記述する。

① 代表者
当社ＰＭＳの最高責任者として、個人情報保護管理者、個人情報保護監査責任者を指名し、ＰＭＳを実施、監査させる。
代表者の承認権限に関しては、個人情報保護方針の策定・改定以外は個人情報保護責任者に委譲する。

② 個人情報保護責任者
代表者からの権限移譲を受け、当社ＰＭＳの運用結果を確認し、承認する。

③ 個人情報保護管理者
当社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。(公表は、氏名または役職名で行う)
また、全てのＰＭＳ文書の改廃、及び記録を管理する。

④ 個人情報保護監査責任者
全部門の監査を計画、実行し、報告する。

⑤ 個人情報保護教育責任者
全従業者に対するＰＭＳ教育を計画、実行し、個人情報保護管理者に報告する。

⑥ 苦情相談窓口責任者
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。

⑦ 個人番号・特定個人情報事務取扱担当者
個人番号・特定個人情報の事務取扱担当者で、これ以外の者は個人番号・特定個人情報の取扱いができない。

A.3.3.5 内部規程

(1) 個人情報保護責任者は、下記の事項を含む内部規程を文書化し、かつ、維持しなければならない。
(2) 当社は、事業の内容に応じて、個人情報保護マネジメントシステムが確実に適用されるように内部規程を改正しなければならない。
(3) (1)により文書化する規定は以下の通り。

文書化すべき規定	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 「個人情報特定とリスク分析の手引き」
b) 法令、国が定める指針及び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 「個人情報特定とリスク分析の手引き」
d) 組織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	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.3.7.1、A.3.7.2
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(3) 就業規則

A.3.3.6 計画策定

(1) 当社は、個人情報保護マネジメントシステムを確実に実施するために、少なくとも年1回、次の事項を含めて、必要な計画を立案し、文書化し、かつ、維持しなければならない。

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

(2) 教育計画

① 個人情報保護教育責任者は、**A.3.4.5（認識）**に規定する事項を踏まえた**「PF-105 個人情報保護教育計画書」**を作成し、個人情報保護責任者に提出し、承認を得なければならない。

② **「PF-105 個人情報保護教育計画書」**には、実施日、場所、講師、実施方法、結果の評価方法、対象者を記載する。

③ 臨時の教育を行う際にも**「PF-105 個人情報保護教育計画書」**の作成を要する。

(3) 監査計画

① 個人情報保護監査責任者は、**A.3.7.2(内部監査)**に規定する事項を踏まえた**「PF-106 内部監査計画書」**を作成し、個人情報保護責任者の承認を受けなければならない。

② 個人情報保護監査責任者は、**「PF-106 内部監査計画書」**に基づき、監査時期等を監査対象部門に通知しなければならない。

③ 臨時の監査を行う際にも**「PF-106 内部監査計画書」**の作成を要する。

(4) PMS 年間計画

個人情報保護管理者は**「PF-107-1PMS 業務年間計画書」**を作成する。

「PF-107-1PMS 業務年間計画書」には(2)、(3)の項目以外に年 1 回以上見直しすべき項目として、個人情報管理台帳の見直し、リスク分析対策表の見直し、法令等の見直し、委託先管理台帳の見直し、マネジメントレビュー等の年間スケジュール、及び、運用の確認の実施月の年間スケジュールを作成するものとする。

A.3.3.7 緊急事態への準備

(1) 当社は、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、維持しなければならない。

(2) 当社は、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、維持しなければならない。

当社は、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、維持しなければならない。

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。

(3) 緊急事態の特定

緊急事態とは以下の場合を指すものとする。

① 個人情報の漏えい、紛失、滅失又はき損の発生
② 個人情報の改ざん、正確性の未確保状態の発生
③ 不正・不適正取得の発生
④ 目的外利用・提供の発生
⑤ 不正利用の発生
⑥ 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
⑦ システム上もしく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、システム管理責任者が判断した場合
⑧ 個人情報に関連する脅迫行為が行われた場合

(4) 緊急時の組織体制

緊急時における組織体制は、以下の通りとする。

① 緊急連絡

緊急事態又はその疑いがあることを発見した従業者は、出来る限り緊急事態を把握し、すみやかに部門管理者に連絡し、部門管理者は個人情報保護管理者に報告する。

② 緊急事態対策会議

関係役員、個人情報保護管理者、部門管理者等を構成メンバーとし、個人情報保護管理者が議長となる。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。

(5) 基本的な対応方針

① 対応は、緊急事態又はその疑いのあるとき、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。
② 緊急対応後の全ての対応は、緊急事態対策会議の決定に基づいて行う。
③ 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。
④ 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当たり、個人や特定部署での対応を禁ずる。

(6) 緊急時の一次対応

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、経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し以下の手順で行う。

① 緊急事態の類型による初期対応

ｱ) 警察への通知（盗難、強盗などの事件の場合）
ｲ) 対象となった個人情報、被害規模、範囲の特定（全ての場合）
ｳ) システム停止等の応急措置（システム障害の場合）
ｴ) 受託業務の場合は委託元への報告と協議し、委託元の指示に従う。

② 緊急事態対策会議の開催

ｱ) 対応方針決定

ｲ) 対応策の実施と記録

③ 本人への通知

ｱ) 特定された本人に対し電話やメール等で連絡を行い、事実関係及び、具体的な対応策を説明し、了承を得る。

ｲ) 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。

ｳ) 連絡がつかない場合、及び本人特定ができない場合は、ホームページでの公表など内容を本人が容易に知りうる状態に置く。

④ 公表

ｱ) 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、当社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。

ｲ) 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。

ｳ) 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。

⑤ 関係機関への報告

ｱ) 緊急事態対策会議における決定に基づき、当社の審査機関及び、認定個人情報保護団体に加入している場合は認定個人情報保護団体に報告を行う。認定個人情報保護団体に加入していない場合は「個人情報保護委員会」に報告を行う。その際、指定の事故報告書等の書式等がある場合は、それに従う。

番号法に定められた特定個人情報の安全の確保に係る「重大な事態」が生じたときは、緊急事態対策会議の承認を得て、個人情報保護委員会の HP に掲載されている様式に入力して報告すること。

「重大な事態」(その恐れのある事案を含む)

・情報提供ネットワークシステム又は個人番号利用事務を処理するシステムで管理される特定個人情報の漏えい等が発生した。

・漏えい等した特定個人情報の本人の数が 101 人以上である。

・電磁的方法によって、不特定多数の人が閲覧できる状態となった。

・従業者等が不正の目的で利用し、又は提供した。

(7) 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。

連絡先	電話番号
((審査機関): ・JIPDEC プライバシーマーク推進センター事故報告担当 〒106-0032 東京都港区六本木 1-9-9 六本木ファーストビル内 (認定個人情報保護団体):	TEL:03-5860-7565

当社が加入している認定個人情報保護団体は無い	
個人情報保護委員会 漏えい等の対応（個人情報） ・報告先の概要等 （個人番号・特定個人情報に関して） 個人情報保護委員会事務局 特定個人情報漏洩等報告窓口（報告フォーム） （個人情報に関して） 個人情報保護委員会事務局 個人データ漏洩等報告窓口 （報告フォーム）	https://www.ppc.go.jp/personalinfo/legal/leakAction/ https://roueihoukoku.ppc.go.jp/?top=mynumber https://roueihoukoku.ppc.go.jp/?top=kojindatahttps://roueihoukoku.ppc.go.jp/?top=mynumber

(8) 緊急事態発生時における作業記録

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**「PF-201 緊急事態対応記録」**で個人情報保護責任者に報告し、その記録を保管するものとする。

① 外部からの問い合わせ、クレームの内容など

② 対外連絡、報告、協議に関する事項

③ 社内における連絡、報告、協議に関する事項

(9) 緊急事態への恒久的対応

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個人情報保護管理者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、以下の対応を行う。

① 原因の究明

② 原因が不適合などによる場合は、本規程 A3.8 に基づく、是正処置の実施

③ 必要に応じて臨時の教育、及び監査を行う。

(10)緊急事態対策会議の解散

個人情報保護管理者は、(4)～(6)の緊急事態対策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

個人情報保護管理者は、個人情報保護マネジメントシステムを確実に実施するために、運

用の手順を明確にしなければならない。

A.3.4.2 取得・利用及び提供に関する原則

A.3.4.2.1 利用目的等の特定

(1) 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わなければならない。 (2) 利用目的等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しなければならない。

(3) 利用目的等の特定手順

① 個人情報の特定手順は**「P-02 個人情報特定とリスク分析の手引き」**を参照すること。

② 既存の個人情報は、個人情報の特定時に**「PF-701 個人情報管理台帳」**に利用目的を明記し、個人情報保護管理者の承認を得る。

③ 新種の個人情報は、**「PF-111 新規個人情報取得申請書」**に利用目的を明記し、個人情報保護管理者の承認を得た後、**「PF-701 個人情報管理台帳」**に記録する。

④ 利用目的を変更する際の手順は、**A.3.4.2.6(3)**に定める。

A.3.4.2.2 適正な取得

(1) 個人情報の取得は、適法、かつ、公正な手段によって行われなければならない。

(2) 個人情報を直接書面取得以外の方法で取得する場合で、委託・提供・共同利用により個人情報を取得する場合は、委託元・提供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の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し、**「PF-111 新規個人情報取得申請書」**の「適法性」について記載する。

A.3.4.2.3 要配慮個人情報

(1) 当社は、新たに要配慮個人情報を取得、利用する場合、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てはならない。ただし、次に掲げるいずれかに該当する場合には、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、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

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

(2) 当社は、要配慮個人情報の利用についても、前項と同様に実施しなければならない。さらに、要配慮個人情報のデータの提供についても、同様に実施しなければならない。

(3) 要配慮個人情報は以下を言う。

① 人種

② 信条

③ 社会的身分

④ 病歴（病歴に準ずるもの）

診療情報、調剤情報、健康診断の結果、保健指導の内容、障害（身体障害、知的障害、精神障害（含む発達障害））

⑤ 犯罪の経歴（犯罪の経歴に準ずるもの）

・被疑者又は被告人として刑事手続きを受けた事実

・非行少年として承認保護事件の手続きを受けた事実

⑥ 犯罪により害を被った事実

⑦ JIS Q15001:2006 で規定する「特定の機微な個人情報」に該当する事項も「要配慮個人情報」と同様に扱う。

(4) 原則禁止と取得する場合の承認と同意の手順

要配慮個人情報の取得、利用又は提供は行ってはならない。なお、新規取得の場合は**「PF-111 新規個人情報取得申請書」**で、変更の場合は**「PF-112 個人情報の取扱い変更申請書」**で、利用目的等を明示し個人情報保護管理者の承認を得た後にその目的を示し、要配慮個人情報の取得、利用又は提供について、明示的な本人の同意を取得した場合は、要配慮慮情報の取得、利用及び提供等を行うことができる。

(5) ただし書き適用の承認手順

取得、利用の場合は**(1)a)～e)**のただし書きを、提供の場合は**a)～d)**をただし書きの適用範囲とし、個人情報保護管理者の承認を得る。

(6) 上記（1）のただし書きの例

また、上記（1）のただし書き e)の例は下記のｱ)ｲ) ｳ) 等があり、書面による本人の同意を得ることを要しない。

ｱ) 要配慮個人情報が、本人、国の機関、地方公共団体、報道機関などによって公開されている場合

ｲ) 身体に障害を抱えていることが意図せずに映りこんだ場合など

ｳ) 受託、事業継承、共同利用の場合

A.3.4.2.4 個人情報を取得した場合の措置

(1)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

(2) 社内承認の手続き

a) 新種の個人情報を取得する場合、取得にあたる部門の責任者は**「PF-111 新規個人情報取得申請書」**に必要事項を記入の上、自部門の部門管理者を経由して、個人情報保護管理者の承認を得る。

b) (1)のただし書き a)～d)に該当するため本人の同意を要しない場合は、自部門の部門管理者を経由して、個人情報保護管理者の承認を得る。

(3) (1)について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

① 予め公表する方法

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、当社ホームページ上で公表する。

② 取得後速やかに通知又は公表する方法

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、以下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。

ｱ) 文書での連絡

ｲ) 電話又は面談による口頭通知

ｳ) 当社ホームページ上での公表とする。

(4) (1)の d)を適用する場合は以下の場合に限定する。

① 名刺交換により取得した個人情報

② 見積書・請求書等に記載された個人情報

(5) 個人情報を直接書面以外の方法で取得する場合で、委託・提供・共同利用により個人情

報を取得する場合は、委託元・提供元またはその他の共同利用者が個人情報保護法及個人情報保護委員会の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。確認の方法としては、委託元・提供元・共同利用者のホームページや契約時に口頭で確認し、**「PF-111 新規個人情報取得申請書」の**「適法性」欄に記載するものとする。

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

(1) **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なければならない。

a) 組織の名称又は氏名

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) 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

(2) 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 (1)** 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。

(3) 社内承認の手続き

① 新種の個人情報を取得する場合、取得にあたる部門の責任者は**「PF-111 新規個人情報取得申請書」**に必要事項を記入の上、個人情報の利用目的等を明記した書面を添付し、自部門の部門管理者を経由して、個人情報保護管理者の承認を得る。

② 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 (1)** のただし書き **a)～d)** に該当するため本人の同意を要しない場合は、自部門の部門管理者

を経由して、個人情報保護管理者の承認を得る。

(4) 本人からの同意取得方法

本人から同意を取得する際は、(3)①で承認を得た明示事項を以下の方法で本人に提示し、本人の同意を得る。

① 顧客から紙媒体で取得する場合は、書面で明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。

② Web のフォームに入力させることにより取得する場合は、画面上で同意文面を読んだ上で「同意欄」をクリックした後、入力フォームに入力して送信する方式とする。

③ 当社従業者から個人情報を取得する際は、**「PF-110 従業者用同意書」**により本人の同意を取得する。

④ 採用応募者から個人情報を取得する際は、**「PF-109 採用応募者用同意書」**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

(1) 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しなければならない。

(2) 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(1)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、本人の同意を得なければならない。ただし、A.3.4.2.3 (1)a)～d)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。

(3) 社内承認の手続き

① 利用目的を変更する場合、**「PF-112 個人情報の取扱い変更申請書」**に必要事項を記入の上、文案を添付し、自部門の部門管理者を経由して、個人情報保護管理者の承認を得る。

② A.3.4.2.3(1)ただし書き a)～d)に該当するため本人の同意を要しない場合は、自部門の部門管理者を経由して、個人情報保護管理者の承認を得る。

(4) 本人からの同意取得方法

A.3.4.2.5(4)と同様の手順で同意を取得する。

(5) 目的外利用に該当するかどうか疑わしい場合には、個人情報保護管理者に相談し、指示を仰がなければならない。

A.3.4.2.7 本人に連絡又は接触する場合の措置

(1) 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(1)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(1)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(1) 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 A.3.4.2.5 (1) 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
- 取得方法

e) A.3.4.2.4(1) 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(1) のただし書き a)～d) のいずれかに該当する場合

(2) 社内承認の手続き

① 新規取得の場合は**「PF-111 新規個人情報取得申請書」**で、変更の場合は**「PF-112 個人情報の取扱い変更申請書」**に必要事項を記入し、利用目的の変更内容及び取得方法を明記した書類を添付し、当該個人情報を用いて本人に連絡又は接触することを個人情報保護管理者の承認を得る。

② (1)のただし書き 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、個人情報保護管理者の承認を得る。

(3) 本人からの同意取得方法

本人に文書等により、当該個人情報を用いて連絡又は接触する必要が生じたことを説明する書面を送付。同意文書を返送により取得する。

(4) (1)の d)を適用する場合

共同利用する必要が生じた場合には、共同利用に関する必要事項を記載して当社ホームページに掲載し、本人が容易に知りうる状態におく。

A.3.4.2.8 個人データの提供に関する措置

(1) 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(1)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　又はA.3.4.2.7の規定によって、 既にA.3.4.2.5(1)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) 第三者への提供を利用目的とすること

2) 第三者に提供される個人データの項目

3) 第三者への提供の手段又は方法

4) 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

5) 取得方法

6) 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、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、b)の1)～6)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(1)のただし書き a)～d)のいずれかに該当する場合

(2) 社内承認の手続き

① 個人データを第三者へ提供する場合で、新規取得の場合は**「PF-111 新規個人情報取得申請書」**で、変更の場合は**「PF-112 個人情報の取扱い変更申請書」**に必要事項を記入し、取得方法及び第三者提供の要領を明記した書面を添付し、当該個人情報を用いて第三者に個人データを提供することを個人情報保護管理者の承認を得る。

② (1)のただし書き b)～g)に該当するため通知と同意を要しない場合は**「PF-112 個人情報の取扱い変更申請書」**に適用するただし書きを記載し、個人情報保護管理者の承認を得る。

(3) 本人からの同意取得方法

(1)のただし書き a)～g)に該当しない場合は、A.3.4.2.5(4)の方法で本人の同意を得る。

(4) (1)のただし書き b)（オプトアウトによる個人データの提供）を適用する場合は、第三者に提供する個人データ（要配慮個人情報を除く）は、本人の求め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としている場合であって、次に掲げる事項について個人情報保護委員会規則で定めるところにより、予め本人に通知し、又は当社ホームページに掲載し、本人が容易に知り得る状態に置くと共に、個人情報保護委員会に届け出たときは、前項の規定にもかかわらず、当該個人データを第三者に提供することができるものとする。

① 第三者への提供を利用目的としていること
② 第三者に提供される個人データの項目
③ 第三者への提供の方法
④ 本人の求めに応じて当該本人が識別される個人データの提供を停止すること
⑤ 取得方法
⑥ 本人の求めを受け付ける方法

(5) 当社はただし書き c)を適用することはない。

もし、ただし書き c)を適用する必要が生じた場合には、第三者提供に関する必要事項を記載して当社ホームページに掲載し、本人が容易に知りうる状態におく。

(6) 共同利用する必要が生じた場合には、共同利用に関する必要事項を記載して当社ホームページに掲載し、本人が容易に知りうる状態におく。

また、共同利用会社間で A.3.4.2.7 d) に規定されている共同利用に関する事項について契約を締結すること。

A.3.4.2.8.1 外国にある第三者への提供の制限

(1) 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及びその他法令等によって除外事項が適用される場合には、本人の同意を得ることを要しない。

(2) 社内承認の手続き

① 個人データを外国の第三者へ提供（個人情報を委託、共同利用、事業継承を含む）する場合は予め新規取得の場合は**「PF-111 新規個人情報取得申請書」**で、変更の場合は**「PF-112 個人情報の取扱い変更申請書」**に必要事項を記載し、取得方法並びにA.3.4.2.5(1)の明示事項 a)～d)を明記した文面の案を添付し、個人情報保護管理者

の承認を得る。

② A.3.4.2.3 のただし書き a)～d)に該当するため通知と同意を要しない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、個人情報保護管理者の承認を受ける。

③ 上記②のその他法令等によって除外事項が適用される場合とは、「個人情報の保護に関する法律施行規則（平成 28 年 10 月 5 日個人情報保護員会規則第 3 号)」第 11 条に定める次のｱ)、ｲ)のいずれかが適用出来る場合である。

ｱ) 個人情報保護委員会が認めた国･地域　(現時点では該当はない)

ｲ) 個人情報保護委員会が認めた国際認証（例：APEC GBPR）を取得している事業者

④ 外国にある第三者に個人情報を委託する場合も(1)を適用する。

(3) 本人からの同意取得方法

A.3.4.2.3 のただし書き a)～d)に該当しない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、(2)の①で承認を得た文面を通知し、A.3.4.2.5(4)の方法で本人の同意を得る。

A.3.4.2.8.2 第三者提供に係る記録の作成など

(1) 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 (1) 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、記録の作成を要しない。

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。

(2) 第三者提供の記録の保持

第三者提供の際には、提供の都度、記録を作成するなどを実施し、個人情報保護管理者の承認を受け保管するものとする。

なお、「個人情報の保護に関する法律施行規則」第 12 条第 2 項に、継続的に若しくは反復して提供した時は、一括して作成することも出来る。また、同第 3 項に該当する場合は、当該提供に関して作成された契約書その他の書面をもって記録に代えることができる。また、記録媒体、記録事項、保存期間などは同規則の第 12 条～14 条によるものとする。

(3) A.3.4.2.3 のただし書き a)～d)に該当するため通知と同意を要しない場合及び

A.3.4.2.8.2のただし書きa) ～c)に該当する場合は、個人情報保護管理者の承認を得る。

A.3.4.2.8.3 第三者提供を受ける際の確認など

(1) 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(1) a)～d) のいずれかに該当する場合、又はA.3.4.2.8.2(1)a)～c) のいずれかに該当する場合は、確認を要しない。
また、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。

(2) 社内承認の手順
個人データを第三者から受領する場合で、新規取得の場合は**「PF-111 新規個人情報取得申請書」**で、第三者提供の目的、相手企業名、相手責任者名、提供データ名、共同利用か否か、等必要事項を記入し、個人情報保護管理者の承認を受ける。

(3) A.3.4.2.3(1) ただし書き a)～d) のいずれかに該当する場合、又はA.3.4.2.8.2(1) ただし書きa)～c) のいずれかに該当する場合は、個人情報保護管理者の承認を得る。

(4) 第三者提供受領の記録の保持
第三者提供受領の都度、記録を作成し、個人情報保護管理者の承認を受け保管するものとする。
なお、「個人情報の保護に関する法律施行規則」第16条第2項に、継続的に若しくは反復して提供した時は、一括して作成することも出来る。また、同第3項に該当する場合は、当該提供に関して作成された契約書その他の書面をもって記録に代えることができる。また、確認方法、記録媒体、記録事項、保存期間などは同規則の第15条～18条によるものとする。

A.3.4.2.9 匿名加工情報

(1) 匿名加工情報の取扱いを行うか否かの方針を定めなければならない。
(2) 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、維持しなければならない。

(3) 個人データを単にマスキングしただけで、法令に定める適切な加工を行っていない場合は、匿名加工情報ではなく個人データである。(システム技術者のスキルシートなど)

(4) 当社では当面の間、匿名加工情報の取扱いを行わない。
但し、当社で匿名加工情報の取扱いを開始する際は、(5)～(7)の遵守事項等の対処方法を社内で定められた稟議書等に記載して、個人情報保護責任者の承認を得るものとする。

(5) 匿名加工を行う場合は下記の事項を遵守しなければならない。
① 匿名加工情報を作成する場合は下記(6)の適正な加工を行わなければならない。
② 匿名加工情報を作成したときは加工方法等の情報の安全管理措置を講じなければな

らない。

③ 匿名加工情報を作成したときは、当該情報に含まれる情報の項目を公表しなければならない。

④ 匿名加工情報を第三者提供するときは、提供する情報の項目及び提供方法について公表すると共に、提供先に当該情報が匿名加工情報である旨を明示しなければならない。

⑤ 匿名加工情報を自ら利用するときは、元の個人情報に係る本人を識別する目的で他の情報と照合することを行ってはならない。

⑥ 匿名加工情報を作成したときは、匿名加工情報の適正な取扱いを確保するため、安全管理措置、苦情の処理などの措置を自主的に講じて、その内容を公表するように努めなければならない。

(6) 匿名加工情報を作成する場合は下記の手順を実施すること

① 特定の個人を識別することの出来る記述（例：氏名）等の全部又は一部を削除すること。

② 個人識別符号（マイナンバー、運転免許証番号等）の全部を削除すること。

③ 個人情報と他の情報との連結する符号（例：委託先に渡すために分割したデータとひも付ける ID）を削除すること。

④ 特異な記述(例：年齢 116 歳や極少病歴など)を削除すること。

⑤ 以上のほか、個人情報とデータベースの内の他の個人情報との差異等の性質を勘案し適切な措置を講ずること。

(7) 匿名加工情報データベース等を事業の用に供している匿名加工情報取扱事業者が遵守すべき義務等

① 匿名加工情報を第三者提供する時は提供する情報の項目及び提供方法について公表すると共に、提供先に当該情報が匿名加工情報である旨を明示しなければならない。

② 匿名加工情報を利用するときは、元の個人情報に係る本人を識別する目的で、加工方法等の情報を取得し、又は他の情報と照合することを行ってはならない。

③ 匿名加工情報の適正な取扱いを確保するため、安全管理措置、苦情の処理などの措置を自主的に講じて、その内容を公表するように努めなければならない。

A.3.4.3 適正管理

A.3.4.3.1 正確性の確保

当社は、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しなければならない。 当社は、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を含む管理を、規定に基づいて適切に行っていること。

(1) 個人データの入出力管理

① 情報システムへの個人データの入力処理を行う者は、業務責任者の説明と指導を受ける。

② 入力の際は誤りの無いよう入力者又は別の担当者が入力データを見直し、誤入力チェックを行い、常に正確性の確保に努める。

③ 情報システムからの出力情報の正確性を確保するとともに、出力情報の不正使用を防止し、出力データの取扱いについて適正かつ厳重な管理を行う。

(2) 個人情報・個人データの保管期限

① 既存の個人情報・個人データは**「PF-701 個人情報管理台帳」**に、新種の個人情報・個人データは**「PF-111 新規個人情報取得申請書」**に保管期限を記入し、個人情報保護管理者の承認を得る。

② 保管期限を決める際は、下表を参考にする。法令によるものはそれに従う。

保存期限終了後、当該個人情報・個人データは遅滞なく消去・廃棄するものとする。

記入例	内容（選択の基準と例）
退職後速やかに	マイナンバー申請書類
６ヶ月間以内	アンケート等イベント的に取得した個人情報等
１年間	定めのないもので、１年間を目途に見直すもの等
３年間	労働関係に関する重要な書類等
５年間	勤務評定や教育訓練に関する書類等
５年間	健康診断書、ストレスチェック
５年間	身元保証書
７年間	源泉徴収票、支払調書
退職後３年	従業員の履歴書等
契約更新後３年間	取引先との契約書等

(3) バックアップの取得

個人データファイルに破損・障害等が発生した場合に備え、個人データファイルのバックアップを行う。バックアップの頻度や世代管理は業務の実施サイクル等によるものとする。

A.3.4.3.2 安全管理措置

個人情報保護責任者は、個人情報保護管理者を通じて、その取り扱う個人情報のリスクに応じて、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、適切な措置を講じなければならない。

(1) 入退管理

① 管理者

ｱ) 入退管理責任者：全社の入退管理について、その任を負う。

ｲ) 入退管理担当者：各場所における管理の実務を実行させるため、入退管理責任者によって指名された者。

② 入退資格

入退を行う対象者に対して、入退資格を設け、資格のない者の立ち入りを禁ずる。なお、必要となる場合は、ＩＤカードまたはこれに代わるもの等を交付することにより付与する。

③ 社員証・許可証等の着用義務

入退資格を有する者は、社員証または別に定める許可証などが定められている場合は、常に他者から見えるところに着用する。

④ 施錠の原則

ｱ) 各事業場は原則として常時施錠可能とし、入退資格のない者の立ち入りを禁ずる。やむを得ず施錠可能でない事業場においては、個人情報をはじめとする機密情報または重要情報は、必ず施錠可能なキャビネット等に収納するなど厳重な管理を行う。

ｲ) 施錠、開錠は、原則として従業者が行う。

⑤ 入退者の記録

ｱ) 入退の際は、**「PF-302 入退室管理簿」**への記入または入退管理装置により、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の記録を残す。

ｲ) 外来者の訪問は、原則として、**「PF-301 訪問受付票」**に記録する。**「PF-301 訪問受付票」**は、原則として１人又は１社につき１葉の用紙を用い、それに氏名、身元、入退時刻を記入し、原則として面談者が面会の確認印の押印または署名を行う。

ｳ) 入退管理責任者は、**「PF-302 入退室管理簿」**が適切に記録されているかどうかを月に１度確認する。

ｴ) ｱ)、ｲ)の記録は２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。

⑥ 物品の持込み・持出し

ｱ) 入退管理担当者は、持込み・持出し物品に関して不審な点を発見した場合は、速やかに入退管理責任者に報告する。

ｲ) 当社の資産および顧客からの預かり資産を入退管理責任者の許可なく無断で持ち出すことを禁ずる。

⑦ 入退場所の制限

ｱ) 入退管理責任者は、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する。

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

⑧ 休日・夜間の入場

役員、従業員および外部要員が休日、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部門長の許可を受け、入退管理責任者または入退管理担当者に届け出る。

⑨ 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者は、その行動を監視し、必要と認めるときは入退管理担当者または入退管理責任者に報告する。

⑩ 入退管理に関する運用の確認

入退管理責任者は、入退管理が有効かつ適切に実施されていることを毎月定期的に確認し、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。

⑪ 社内ビデオモニタリング監視

社内の安全管理のためにビデオによるモニタリングをする場合は、モニタリングの目的を特定し従業者に明示すること。

(2) 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記憶媒体を机上やその周辺に放置してはならない。

② 個人データの複製

個人データの複製は、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。

個人データは、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。

ｱ) 個人データファイルは、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。

ｲ) 個人情報が記された書類および個人情報が入った記憶媒体（USB、CD-ROM 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。

ｳ) 重要な個人情報が記された書類のファイル、バインダ、記憶媒体の容器、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。

ｴ) 個人情報が記された書類および個人データが入った記憶媒体（USB、CD-ROM 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。

ｵ) 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、消火器等を設置する。

④ 個人情報の移送・送信・受信

ｱ) 個人情報を外部へ持ち出す際は、自部門の部門管理者の許可を得ることとし、目的地以外へ立ち寄らず、手放さない、車中に放置しないよう徹底する。
また、必要に応じて持ち物検査を行う。

ｲ) 紙や記憶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、誤配、紛失等の危険を最小限にするため、私書箱の利用、書留の利用、セキュリティ便の利用等の措置を講じる。また、防犯対策のために郵便ポストへは施錠する。

ｳ) 個人データをインターネット経由で送受信する際は、SSL 等の暗号化対策やパスワード設定等の措置を講じる。

ｴ) 個人情報の入った FAX を送信する際は、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。

ｵ) 個人情報の入った FAX を受信する際は、定期的に回収を行い長時間 FAX 機に放置しない。

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。

ｱ) 紙や記憶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。

ｲ) 電子メールにより個人データ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。

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。

ｱ) 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。

ｲ) 記憶媒体（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データの廃棄は、以下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。

・記憶媒体そのものを物理的な破壊方法により処分する。

ｳ) 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。

ｴ) 個人情報の記された書類は再利用しないこと。

ｵ)　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。

(3) 情報システムの管理

①　サーバの安全対策

システム管理責任者は、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、以下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

システム管理責任者は、社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以下の点に努める。

ｱ)　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。

ｲ)　ネットワーク障害に備え、バックアップ回線の確保や復旧手順を備える。

ｳ)　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。

ｴ)　利用者の故意、過失により情報の漏洩、き損、滅失が起こらないよう、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洩やデータの破壊を防ぐため、システム管理責任者は以下の対策を施す。

ｱ)　社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。

ｲ)　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。

ｳ)　ファイル共有ソフト（ファイル交換ソフト）など、システムの脆弱性を高めるソフトウェア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。

④　アクセス記録の管理

システム管理責任者は、重要な情報資産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が必要な場合は取得し、定期的にチェックを行わなければならない。
常時取得の必要がない場合は、アラートが上がった場合にチェックを行う。

⑤　機器・装置等の物理的な保護

システム管理責任者は、重要な情報資産を取り扱う機器・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）から以下に従って物理的に保護する。

ｱ)　社外クラウドやサーバ室など隔離されたエリアへの設置

ｲ)　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

ｳ)　耐震性、防火性、防水性を考慮した設置

ｴ)　無停電電源装置の設置

⑥　ソフトウェア使用の原則

ｱ)　クライアントパソコンで使用するソフトウェアは、原則システム管理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。

ｲ)　ファイル共有ソフト（ファイル交換ソフト）など、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。

⑦　ID、パスワードの付与管理

ｱ)　システム管理責任者は、以下のアカウントについて、ID 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。

・クライアントパソコンのユーザ ID

・ネットワークユーザーID

・業務用Ｅメールアカウントの ID

・業務システム、グループウェアその他のユーザ ID

・上記における管理者 ID

ｲ)　アカウントは業務上必要な範囲で社員等に付与され、部門管理者によって承認される。

ｳ)　社員等が退職した場合は、所属部門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

ｱ)　ユーザ ID のパスワードは、利用者が厳重に管理し、容易に破られない文字種類と長さ(英数 8 桁以上)の文字列を設定しなければならない。また個人情報から類推可能なパスワードは設定しない。

ｲ)　各システムにおける管理者 ID のパスワードは、システム管理責任者において厳重に管理しなければならない。

ｳ)　利用者およびシステム管理責任者は、パスワードの代替若しくは補完のために、静脈などの生体認証、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。

⑨　アクセス権と認証管理

ｱ) 利用者のアクセス権は、個人情報などの重要情報に対しては必要最小限の者がアクセスするという原則のもとに、システム管理責任者が検討し、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部門の責任者を経由して、システム管理責任者の許可によりおこなうものとする。

ｲ) 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の許可を必要とする。

⑩ パソコン利用者の義務

パソコンは、私用や部外者に使わせてはならない。パソコン利用者はパソコンの管理について以下の義務を負う。

ｱ) パソコンの盗難防止

ｲ) 不正ソフトウェアからの保護

ｳ) 障害や事故の発生、又はそのおそれのあるときのシステム管理責任者への報告

⑪ 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以下のいずれかの対策を施すものとする。

ｱ) ワイヤーチェーン等による固定

ｲ) 帰宅時等不使用時の施錠保管

ｳ) 外部に持ち出す際の BIOS パスワード等による起動制限

⑫ パソコンの持ち出しと持ち込み

ｱ) パソコンの持ち出し、持ち込みおよび私物パソコンの業務上の利用については原則として禁止とし、**「PF-303 機器持出・持込申請書」**にて該当部門の長およびシステム管理責任者が認めた場合にのみこれを許可する。

ｲ) 持ち出しの際には以下の保護対策を行う。

・持ち出しパソコンには、必要な情報以外を保存しない。
・⑪のｳ)に従い、第三者による起動制限措置をとる。
・重要な情報は暗号化またはパスワード付きとする。

ｳ) 持ち込みおよび私物パソコン利用の場合は、以下の保護対策を行う。

・社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、システム管理責任者が指定するソフトウェアによりウィルスチェックを行う。
・前項と同様の盗難防止対策をとる。
・許可されていないソフトウェアを無断でインストールしない。

⑬ 離席時のモニター画面からの漏洩防止（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洩しないよう以下の措置を実施する。

ｱ) 離席と同時にパスワードの入力又は物理的キーによってのみ復帰できる方法で画面ロックを行う。

ｲ) ｱ)の処置をし忘れても問題が無いように、パスワード付きスクリーンセーバを設

定時間*１０分*以内とする。

ｳ) ログイン ID、パスワードを机上に貼付することは厳禁とする。

⑭ 社内ネットワークの利用

社内ネットワークの利用は、以下のルールに従って行う。

ｱ) 社内ネットワークへの接続は、システム管理責任者の承認と指示された手順に従う。

ｲ) 他人の ID、パスワードで、社内ネットワークに接続しないこと。

ｳ) 一旦、社内ネットワークから切り離したパソコン等は、ウィルスチェックなどの安全確認を行ってから再接続すること。

ｴ) 社内で新規に無線LANを設置する場合は、システム管理責任者が暗号レベル(WPA2以上）を設定し、必要によりドメイン設定や IP フィルタリングによる接続制限及びユーザの制限をして設置する。

ｵ) 社外から社内LANに公衆回線やインターネット経由でリモートアクセスすることは原則として禁止するが、やむをえない場合は、システム管理責任者の承認を得て、システム管理責任者の認める十分な安全対策の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、以下のルールに従って行う。

ｱ) インターネットを利用する場合は、情報システム管理者の指示に従うこと。
従業者の業務に関連のないWebサイトへのアクセスを制限するフィルタリングを実施することが出来る。

ｲ) インターネットは、社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。

ｳ) 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、部門管理者及びシステム管理責任者に速やかに連絡すること。

ｴ) インターネットへのアクセスは、社内ネットワークを経由してアクセスすること。

⑯ Ｅメールの利用

Ｅメールの利用は、以下のルールに従って行う。

ｱ) Ｅメールは会社所定のソフトを使用し、その利用は業務上必要な場合に限定すること。

ｲ) 個人情報を含む機密情報を送信する場合は、暗号化やパスワードで、盗聴等のリスクを回避すること。

ｳ) 社外メーリングリストへの参加は、原則禁止とする。

ｴ) Ｅメールによる攻撃（DOS 攻撃、ウィルス、傍受など）及びそのおそれを感知した場合は、遅滞なく部門管理者及びシステム管理責任者に報告する。

⑰ 外部記憶媒体の取扱

ｱ) CD、USB メモリなどの外部記憶媒体に、むやみに顧客情報や個人情報、会社の重

要情報を保存してはならない。

ｲ) 外部記憶媒体を机上や、棚上等に放置してはならない。

ｳ) 私用の外部記憶媒体を持ち込む場合、社有の外部記憶媒体を持ち出す場合は、**「PF-303 機器持出・持込申請書」**にて該当部門の長およびシステム管理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

ｱ) 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し、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。

ｲ) システム管理責任者は、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

ｱ) 利用者は、Ｅメールへの添付、FTP サーバや Web サーバを介する送受信、専用システムによるファイル伝送などでデータを送受信する場合は、データを暗号化する、パスワードをつけるなど通信中の漏洩防止対策をとらなければならない。
例えば、Web サーバからメールのプロバイダーが個人情報をメールテキストデータとして送信する場合は、SMTP over SSL または POP3 over SSL などの設定を行い、回線を暗号化していることを確認すること。

ｲ) また､OS が WINDOWS の場合､Web サーバを介して個人情報を受信する際は WINDOWS の脆弱性対策（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等）を実施すること。なお、脆弱性対策を実施した記録を個人情報保護管理者が確認し、承認すること。

ｳ) システム管理責任者は、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部門管理者と協議の上実施しなければならない。

⑳ 記憶媒体によりデータを受け渡しする場合

ｱ) CD-ROM、USB メモリなどの記憶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､以下のような受け渡し方法をとることとする。

・責任者または直接担当者間による手渡し
・自社便での配送
・書留や保険付き宅配便
・その他、配達記録の残る受け渡し方法

ｲ) データの受け渡しに際しては、授受記録を残し、部門管理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。

(4) 携帯電話・スマートフォン・タブレット端末の管理

① 管理者

ｱ) 会社所有の携帯電話・スマートフォン・タブレット端末（以下「社有携帯電話等」という）は個人情報保護管理者が管理する。

ｲ) 個人情報保護管理者は、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。

ｳ) 個人情報保護管理者は、社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

社有携帯電話等の使用を希望する者は、部門管理者を経由して個人情報保護管理者の承認を得なければならない。

③ 使用者の義務

ｱ) 社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。

ｲ) 社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。

ｳ) スマートフォンについては OS の最新版への更新や、ウィルス対策ソフトの導入を行うこと。

ｴ) 持ち歩く際は、ストラップを付ける等の盗難・紛失防止策を講じなければならない。

ｵ) 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見聞きされないよう十分配慮しなければならない。

ｶ) 社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。

ｷ) 社有携帯電話等を私用に用いてはならない。

ｸ) 業務に関係ないアプリケーションをインストールしないこと。
業務上必要なソフトでも、特にアンドロイド OS のスマートフォンについては安全なアプリケーションであることを確認すること。

④ 私用の携帯電話等を業務で使用する場合は、③使用者の義務を順守しなければならない。

(5) マイナンバー管理手順

① マイナンバーカード（含む通知カード）の取得の際は、従業者本人及びその家族以外の者の番号を取得することはできない。また、法律で定められた利用目的（社会保険、税金、災害対策）以外の目的で取得、利用することはできない。

② 個人番号、特定個人情報を取り扱う区域を設定し、個人番号・特定個人情報の取扱管理者及び個人番号・特定個人情報の取扱担当者以外は、個人番号、特定個人情報の取り扱いをしないようにすること。ただし、区域が設定できない場合は、机の位置など

を工夫して見られないようにすること。

③　個人番号については個人番号・特定個人情報事務取扱担当者は、手渡しでマイナンバーカード（含む通知カード）を原則本人から手渡しで受け取り、番号を照合する。その際本人確認資料や委任情報等が必要な場合は取得し確認を行うこと。

④　社内に保管している「マイナンバー情報」は、電子データの場合はパスワード付ファイルとして、紙媒体の場合は施錠保管し、退職後本人のデータはすみやかに廃棄・削除すること。

⑤　個人番号の記載された資料を、年金事務所や税務事務所、及びそれらの委託先に送付する際は、記録の残る「宅配便」等を利用する。又は「個人情報委託記録シート」を作成すること。

⑥　個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存すること。

⑦　委託した個人番号若しくは特定個人情報ファイルを削除した場合又は電子媒体等を廃棄した場合に、削除又は廃棄した証明書を確認すること。

⑧　本人の同意があったとしても、利用目的を超えて個人番号若しくは特定個人情報を利用してはならない。

⑨　個人番号若しくは特定個人情報ファイルは、法定保管期限が来たら廃棄・削除する。

A.3.4.3.3 従業者の監督

(1) 当社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はかられるよう、当該従業者に対し必要、かつ、適切な監督を行わなければならない。

(2) 当社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はかられるよう、当該従業者に対し必要、かつ、適切な監督を行わなければならない。

(3) 従業者との雇用契約時又は派遣社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。

(4) フィルタリングとオンラインモニタリング

従業者の業務に関連のないWebサイトへのアクセスを制限するフィルタリングを実施することが出来る。

また、社内の安全管理のためにオンラインモニタリングを実施することが出来る。その際は、モニタリングの目的を特定し、従業者に通知すること。

(5) 内部規程違反時の罰則

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、調査と確認を行う場合は従業者に通知した上で実施する。

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、懲戒等を行うものとする。

(6) 派遣社員等については、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。

A.3.4.3.4 委託先の監督

(1) 委託先の選定基準

当社は、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しなければならない。

また、当社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しなければならない。このため，当社は、委託を受ける者を選定する基準を確立しなければならない。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なければならない。

当社は、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わなければならない。

(2) 委託先との契約

当社は、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しなければならない。

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

当社は、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。

(3) 個人データの取扱いの全部又は一部を委託する場合に委託を受ける者を選定する基準を以下の手順で定める。

① 個人情報保護管理者は、委託業務担当部門の責任者と協議し、委託業務の性格、委託先の業種、必要性、および業者の信用度等を勘案し、評価項目を決定する。具体的な選定項目は**「PF-404 個人データ委託先審査票」**に定める。

② ①で定めた当社の取引先資格要件の水準は、個人情報の取扱いに関する法令等の改正状況や社会情勢の変化、技術の進歩等を考慮し、当該取引に関与する部門の責任者及び個人情報保護管理者の協議に基づき、*毎年６月*に見直す。

(4) 委託先の選定

① 個人データの取扱いの全部又は一部を委託する場合、業務委託部門の責任者は、委託先候補企業の管理体制について**「PF-404 個人データ委託先審査票」**で評価し、個人情報保護管理者の承認を得る。

評価の結果、基準点に達しない委託先でも、特別なノウハウを保持している委託先や、長年の実績で信用がある委託先については、例外として**「PF-404 個人データ委託先審査票」**の特記欄にその旨を記載し、個人情報保護管理者の承認を得れば委託することが出来る。

② **「PF-404 個人データ委託先審査票」**の評価の項目は複数の選択が可能。また、Pマーク認定事業者、士業であっても契約の締結（「覚書」の取り交わし）をするものとする。

③ ①で選定した委託先は、**「PF-403 個人データ委託先管理台帳」**に記載し管理する。

④ ①で選定した委託先については*毎年 6 月*、及び必要に応じて随時再評価を行い、個人情報保護管理者の承認を得る。

(5) 委託先との覚書による契約

① 委託に際しては、次に示す事項を**「PF-405 個人データの取扱いの委託に関する覚書」**によって規定し、十分な個人情報の保護水準を担保しなければならない。

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

② 当該部門の部門管理者は、当該契約書などの書面を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。

③ マイナンバーに関する委託を行う際はマイナンバーの事業者ガイドラインに定められた下記の事項を**「PF-405-1 マイナンバーの委託に関する覚書」**上で明文化するものとする。

a) 秘密保持義務

b) 事業者内からの特定個人情報の委託業務以外での持ち出しの禁止

c) 特定個人情報の目的外利用の禁止

d) 再委託における条件

e) 漏えい事案等が発生場合の委託先の責任

f) 委託契約終了後の特定個人情報の返却または廃棄

g) 従業者に対する監督･教育

h) 契約内容の遵守状況について報告を求める規定

④ 委託先のサービス商品を利用するケースで、上記で定めた内容での契約や覚書を個々に締結できない場合には、当該委託先企業の利用するサービス約款、または、利用規約等で個人データの管理状況を確認し、**「PF-404 個人データ委託先審査票」**の特記欄にその旨を記載し、個人情報保護管理者の承認を得れば委託することが出来るものとする。

(6) 委託先との確認事項

① 委託前の確認事項

個人データを委託する場合、必要に応じ、下記内容を委託先との間で取り交わすものとする。

a) 委託する個人情報の内容

b) 個人データの利用条件

c) 授受と保管の方法

d) 返還又は廃棄の方法

② 個人データの授受記録

委託先との間で個人データの授受が発生する場合、必要に応じて授受記録を残すものとする。

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

(1) 当社は、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は，保有個人データには当たらない。

次のいずれかに該当する場合は、保有個人データではない。

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し、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

(2) 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。

(3) 上記(1)のただし書きに基づき、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、個人情報保護管理者の承認を受けるものとする。

A.3.4.4.2 開示等の求めに応じる手続き

(1) 当社は、開示等の求めに応じる手続きとして以下の事項を定める。

a) 開示等の請求等の申し出先

b) 開示等の求めに際して提出すべき書面の様式とその他の開示等の請求の方式

c) 開示等の請求をする者が、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

(2) (1)の手続きを定めるに当たっては、本人の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。

(3) 当社は、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、その額を定めるものとする。

(4) 開示等の求めに応じる詳細は以下の通りとする。

① 開示等の求めの申し出先

本人からの開示等の求めの申出先は、苦情・相談窓口責任者とする。

② 開示等の求めに際して提出すべき書面の様式その他の開示等の求めの方式

本人には、**「PF-113 保有個人データ開示等請求書」**を提出してもらう。

③ 本人又は代理人であることの確認方法

ｱ) 個人情報の開示等の求めに応じる場合の本人確認

以下の本人確認書類のいずれかの写しを同封することとする（本籍地の情報は都道府県のみとして、その他は黒塗りで収集するものとする)。

・ 運転免許証
・ パスポート
・ その他本人確認できる公的証明書

ｲ) 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 ｱ)に加えて、代理権が確認できる下記 a）の書類の写しいずれか及び代理人自身を証明する b）の書類の写しのいずれかを必要とする。

a) 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
・ 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

＜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

b) 代理人自身を証明する書類（本籍地の情報は都道府県のみとして、その他は黒塗りで収集するものとする。）

・ 運転免許証
・ パスポート
・ 住民基本台帳カード

・ 在留カード又は特別永住者証明書
・ マイナンバーカード（表面）
・ その他本人確認できる公的証明書

④ 開示等の求めの手数料および徴収方法
利用目的の通知又は開示請求の場合、１回の請求につき返信のための事務手数料・郵送費相当の手数料を徴収できる。

A.3.4.4.3 保有個人データに関する周知など

(1) 当社は、保有個人データに関し、次の事項を本人が知り得る状態（本人の請求などに応じて遅滞なく回答する場合を含む）に置かなければならない。
a) 当社の名称
b) 個人情報保護管理者（若しくは代理人）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(1)の a)～c)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) 当社の属する認定個人情報保護団体の対象事業社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き

(2) 本人が知り得る状態とする方法
① (1)の a)～f)の事項については個人情報保護管理者の承認を得た上で当社ホームページにて公表することとする。
② 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

(1) 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(1)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(1)の c)により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。

(2) 利用目的の通知を求められた際の処理手順
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**「PF-113 保有個人データ開示等請求書」**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。
① 保有個人データを調査の上、必要事項を確認する。

② 「PF-501 苦情・相談等受付処理票」に必要事項を記入する。

③ 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(1)の a)～c)に該当する場合、又は A.3.4.4.3(1) c)によって保有個人データの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。

④ ③について、個人情報保護管理者の承認を得る。

⑤ 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③で立案した理由の説明）は以下のいずれかの適切な方法を選択し行う。

ｱ) 登録されている本人住所に回答文面を郵送する。

ｲ) 登録されている本人の FAX 番号に回答文面を FAX する。

ｳ) 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。

ｴ) 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

(1) 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）を求められたときは、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（開示の求めを行った者が同意した方法があるときは、当該方法）によって開示しなければならない。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、理由を説明しなければならない。

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) 法令に違反することとなる場合

(2) 開示を求められた場合の処理手順

開示を求められた場合、原則として本人から「PF-113 保有個人データ開示等請求書」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。

① 保有個人データを確認の上、必要事項を確認する

② 「PF-501 苦情・相談等受付処理票」に必要事項を記入する。

③ 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、(1)のただし書き 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し、「PF-501 苦情・相談等受付処理票」に記入する。

④ ③の記入内容について、個人情報保護管理者の承認を得る。

⑤ 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③で立案し

た理由の説明）はA.3.4.4.4(2)の⑤に準じて行う。

A.3.4.4.6 保有個人データの訂正、追加又は削除

(1) 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わなければならない。

(2) 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しなければならない。

(3) 訂正等を行う際、及び訂正等を行わない旨を決定した際の手順

訂正等は、原則として本人から**「PF-113 保有個人データ開示等請求書」**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。

① 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。また、訂正等を行わないと決定した場合はその旨を確認する。

② **「PF-501 苦情・相談等受付処理票」**に必要事項を記入する。

③ 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（訂正等を実施しない場合を含む）を立案する。その際、法令の規定によって特別の手続きが定められている場合はその旨を記載し、また、訂正等を行わないと決定したときも、その旨及び理由を記載する。

④ ③について、個人情報保護管理者の承認を得る。

⑤ 訂正等についての本人への回答はA.3.4.4.4(2)の⑤に準じて行う。

A.3.4.4.7 保有個人データの利用又は提供の拒否権

(1) 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「利用停止等」という）を求められた場合は、これに応じなければならない。また、措置を講じた後は、遅滞なくその旨を本人に通知しなければならない。ただし、A.3.4.4.5(1)の 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もに、理由を説明しなければならない。

(2) 利用停止等を求められた場合の処理手順

利用停止等を求められた場合、原則として本人から**「PF-113 保有個人データ開示等請求書」**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。

① 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。
② 「PF-501 苦情・相談等受付処理票」に必要事項を記入する。
③ 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(1)のただし書き 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。
④ ③について、個人情報保護管理者の承認を得る。
⑤ 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③で立案した理由の説明）は、A.3.4.4.4(2)の⑤に準じて行なう。

A.3.4.5 認識

(1) 個人情報保護教育責任者は、従業者が下記の a)～d)についての認識を持つために、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、維持しなければならない。
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) 個人情報保護マネジメントシステムに適合することの重要性及び利点
c) 個人情報保護マネジメントシステムに適合するための役割及び責任
d) 個人情報保護マネジメントシステムに違反した際に予想される結果
当社は、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なければならない。

(2) また、マイナンバーに関しては、従業者に次の事項を理解させる手順を確立し、維持しなければならない。
a) マイナンバーとは何かなど基本的な知識
b) マイナンバーの利用範囲の制限
c) マイナンバーの社内での取扱い方法
d) 番号法に違反した場合の罰則

(3) 教育の詳細は以下の通りとする。
① 教育の対象範囲
教育の対象範囲は、全従業者とする。また、派遣会社の場合は派遣スタッフも実務に就く際に別途教育を行う。
② 個人情報保護教育責任者の責務
個人情報保護教育責任者は、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。
③ 教育計画の策定
個人情報保護教育責任者は A.3.3.6 により教育計画を作成する。
④ 教育の実施

ｱ) 教育は、教育計画に基づいて定期教育は*毎年９月*に、受入教育は随時に実施し、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。

ｲ) 受講者は、教育受講時、理解度、自覚度を確認するために理解度テストやアンケートを受けなければならない。

ｳ) 個人情報保護教育責任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。また、理解度テストやアンケートの結果については、必要に応じて次回の計画へ反映させるものとする。

⑤ 実施報告

個人情報保護教育責任者は、**「PF-116-2 教育報告書」**で教育の実施記録を作成し、個人情報保護責任者に提出し、承認を得なければならない。

⑥ 記録の保持

個人情報保護教育責任者は、教育計画書、教育テキスト、受講者名簿、理解度テストやアンケート、教育報告書等の教育関係の記録を所定の期間保管することとする。

A.3.5 文書化した情報

A.3.5.1 文書化した情報の範囲

(1) 個人情報保護管理者は、次の個人情報保護マネジメントシステムの基本となる要素を書面で記述しなければならない。

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) 内部規程
d) 内部規程に定める手順上で使用する様式
e) 計画書
f) JIS Q15001:2017 が要求する記録及び当社が個人情報保護マネジメントシステムを実施する上で必要と判断した記録

(2) 文書の詳細は**「PF-118 個人情報保護マネジメントシステム文書体系表」**に示す。

A.3.5.2 文書化した情報（記録を除く）の管理

(1) 管理内容

当社は、JIS Q15001:2017 が要求する全ての文書（記録を除く）を管理する手順を確立し、実施し、維持しなければならない。文書管理の手順には、次の事項を含まれなければならない。

a）文書化した情報（記録を除く。）の発行及び改訂に関すること
b）文書化した情報（記録を除く。）の改訂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

(2) 文書管理は以下の手順にて行う。

① 文書の発行

ｱ）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、制定日、発行者を明記しておくものとする。ただし記録類を除く。

ｲ）発行の際は、事前に所定の承認を得なければならない。

② 文書の改訂

ｱ）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記載し、版番号を更新することとする。

ｲ）改訂は以下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

③ ＰＭＳ文書管理責任者は、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

(1) 管理内容

個人情報保護管理者は、個人情報保護マネジメントシステムおよび JIS Q15001:2017 の要求事項への適合を実証するために必要な記録を作成し、かつ、維持しなければならない。

ｱ）個人情報の特定に関する記録
ｲ）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
ｳ）個人情報のリスクの認識、分析及び対策に関する記録
ｴ）計画書
ｵ）利用目的の特定に関する記録
ｶ）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）の請求への対応記録
ｷ）教育などの実施記録
ｸ）苦情及び相談への対応記録

ヶ) 運用の確認の記録
ヨ) 内部監査報告書
サ) 是正処置の記録
シ) マネジメントレビューの記録

当社は、記録の管理についての手順を確立し、実施し、かつ、維持しなければならない。

(2) 個人情報保護管理者は、記録の取扱いについての手順を確立し、実施し、維持しなければならない。

① (1)の記録について具体的な書類、データ等を取りまとめ、保管期間、保管場所を決めて**「PF-119ＰＭＳ記録管理対象一覧」**で管理、維持する。

② 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。

③ 記録に特定の個人の情報を含む場合は、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

(1) 苦情相談窓口責任者は、個人情報の取扱い及び個人情報保護マネジメントシステムに関して、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、維持しなければならない。

(2) 個人情報保護管理者は、上記の目的を達成するために必要な体制の整備を行わなければならない。

(3) 苦情及び相談への対応の詳細は以下の通りとする。

① 体制

苦情及び相談には、苦情・相談窓口が対応する。苦情・相談窓口責任者は、苦情・相談窓口を統括する。

② 対応手順

ｱ) 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**「PF-501 苦情・相談等受付処理票」**に記入する。

ｲ) 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。

ｳ) 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個人情報保護管理者に報告する。

ｴ) 問合せ内容に応じて、苦情・相談窓口責任者並びに関連部門と協議を行い、回答方針案を作成する。

ｵ) 回答内容について、個人情報保護管理者の承認を得た上で、A.3.4.4.4(2)⑤ｱ)～ｴ)の方法で速やかに本人へ連絡する。

ｶ) 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に報告する。

③ 処理結果の記録

苦情・相談等の対応結果は、**「PF-501 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。

④ 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。

A.3.7 パフォーマンス評価

A.3.7.1 運用の確認

(1) 個人情報保護管理者は、個人情報保護マネジメントシステムが適切に運用されていることが当社の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，維持しなければならない。

(2) 運用の確認の手順

① 各部門及び各階層の管理者は、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。

② 個人情報保護管理者は，トップマネジメントによる個人情報保護マネジメントシステム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。

(3) 日常の業務で個人情報が部門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**「PF-120 個人情報保護運用チェックリスト」**により*四半期に一回*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。

(4) (3)の他、従業者の入退出及び毎日の戸締りや火の元等の確認については、A.3.4.3.2(1)⑤の**「PF-302 入退室管理簿」**により確認することとする。

A.3.7.2 内部監査

(1) 当社は、個人情報保護マネジメントシステムの JIS Q15001:2017 への適合状況及び個人情報保護マネジメントシステムの運用状況を少なくとも年 1 回、必要に応じて適宜に監査しなければならない。

(2) 個人情報保護監査責任者は、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と権限を定める手順を確立し、実施し、かつ、維持しなければな

らない。
(3) 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。

(4) 監査に関する詳細は以下の通りとする。

① 監査対象範囲

監査対象範囲は、当社の全ての事業所、部署、及び個人情報保護管理者とする。

② 監査計画

監査計画は A.3.3.6 により作成する。

③ 監査時期

監査の実施時期は、次のとおりとする。

ｱ) 個人情報保護マネジメントシステムの JIS Q15001:2017 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２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。

ｲ) 個人情報保護マネジメントシステム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。

ｳ) その他必要に応じて随時監査を実施する。

④ 監査実施

ｱ) 監査員は、個別監査計画に基づき、チェックリストを用い、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。

ｲ) 個人情報保護監査責任者は、監査チェックリストその他の監査実施記録を保管する。

⑤ 監査報告

個人情報保護監査責任者は、監査結果を**「PF-123 内部監査報告書」**に取りまとめ、個人情報保護責任者に報告し承認を得るとともに、承認結果の写しを被監査部門長に配布しなければならない。

A.3.7.3 マネジメントレビュー

(1) 個人情報保護責任者は、個人情報の適切な保護を維持するためのマネジメントレビューを少なくとも年 1 回実施し、適宜に個人情報保護マネジメントシステムを見直さなければならない。
(2) 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) 監査及び個人情報保護マネジメントシステム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、国の定める指針その他の規範の改正状況
e) 社会情勢の変化、国民の認識の変化、技術の進歩などの諸環境の変化
f) 当社の事業領域の変化
g) 内外から寄せられた改善のための提案

(3) マネジメントレビューは、原則として*毎年4月*に行うものとし、必要な場合には、その他の時期にも随時行うものとする。
(4) マネジメントレビューに際しては、上記の事項を考慮し、**「PF-124 マネジメントレビュー議事録」**に記載しなければならない。

A.3.8 是正処置

(1) 個人情報保護管理者は、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、維持しなければならない。その手順には、以下の事項を含めるものとする。
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、立案された適切な処置を実施する
d) 実施された是正処置の結果を記録する
e) 実施された是正処置の有効性をレビューする

(2) 是正処置の詳細は以下の通りとする。
① 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。
② 是正処置の入力情報は、以下の通りとする。
ｱ) 内部監査により発見した不適合
ｲ) 各部門における運用の確認において発見された不適合
ｳ) 緊急事態の原因となった不適合
ｴ) 外部機関、組織等の指摘による、不適合
ｵ) 苦情や相談により明らかになった不適合
③ 是正の実施手順
是正処置は、以下の手順に従い実施する。
ｱ) 是正処置の必要な事象を発見した者は、**「PF-601 是正処置計画・報告書」**により不適合発生部門に対して指摘する。指摘を受けた当該部署の部門責任者は、不適合の内容を確認の上、個人情報保護管理者に提出し承認を得る。
ｲ) 指摘を受けた当該部署の部門責任者は、指摘内容の根本原因を特定し、処置

計画を立案する。

当該部署の部門責任者は、不適合の内容、根本原因、処置計画が記入された**「PF-601 是正処置計画・報告書」**で個人情報保護責任者の承認を得る。

ｳ) 当該部署の部門責任者は、承認された処置計画に従って処置を実施する。

ｴ) 当該部署の部門責任者は、処置結果を記載した、**「PF-601 是正処置計画・報告書」**を個人情報保護管理者に提出し承認を得る。

ｵ) 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**「PF-601 是正処置計画・報告書」**に記載する。

A.4 雑則

A.4.1 改廃

本規程の改廃は、個人情報保護責任者によって承認されるものとする。

㈱イカイ コントラクト	個人情報保護規則	ICS-M-007	１／１０
		改定日 ２０２０．１０．１．	第６版

改　訂　履　歴			
版数	改訂日	ページ	改訂概要
1	２０１０．４．１．	全	新規制定
2	２０１２．９．１．	全	全面見直し改訂
3	２０１４．４．１．	P7～10	新規追加
4	２０１７．４．１	P5	新規追加（第１０条）
5	２０１８．４．１	１	配布先及び承認欄の変更
6	２０２０．１０．１．	全	全面見直し改訂（JIS Q 15001 対応）