個人情報保護指針

平成 29 年 5 月 30 日制定

Ver3.00

1　目的

本指針は、個人情報の保護に関する法律(以下、「個人情報保護法」という)、関連する政令及び個人情報保護委員会規則、並びに個人情報の保護に関する法律についてのガイドライン(通則編)(以下、「保護法ガイドライン(通則編)」という。)、個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編)(以下、保護法ガイドライン(外国にある第三者への提供編))という。)、個人情報の保護に関する法律についてのガイドライン(第三者提供時の確認・記録義務編)(以下、「保護法ガイドライン(第三者提供時の確認・記録義務編)」という。)、個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)(以下、「保護法ガイドライン(匿名加工情報編)」という。)、及びその他特定の分野に関するガイドライン(以下、これらのガイドライン全てを総称して、「保護法ガイドライン」という。)に基づき、一般社団法人日本個人情報管理協会(以下「当法人」という)の正会員である認定個人情報保護団体の事業の対象となる対象事業者(以下、「対象事業者」という)が、その規模に応じ、事業活動を行う上で、個人の人格尊重の下で、お客様、従業者及び関係者等の個人情報を適正に取扱い、適切な安全管理を実施することにより、調和のとれた本人の権利利益の保護と個人情報の利活用が達成できるようにすることを目的とします。当法人は対象事業者が、本指針を遵守するよう、周知、徹底し、指導いたします。

なお、匿名加工情報の作成、取扱い、安全管理及びその提供についての指針は、匿名加工情報に関する指針として別途定めますので、本指針には含みません。

2　適用範囲

本指針は、個人情報を取り扱う当法人の全ての対象事業者に適用いたします。

3　対象事業者の責務

対象事業者は、個人情報を取り扱うにあたり、本指針を遵守しなければなりません。

1) 個人情報保護法及び関連する法令並びに保護法ガイドラインを遵守し、個人情報の適正な取扱いと、適切な安全管理を行うこと
2) 個人情報保護方針(プライバシーポリシー)を策定し、適切な方法で公表すること
3) 本指針を遵守するために必要となる取扱いの規程等(以下、「規程等」という。)を定め、運用し、点検し、改善を行うこと
4) 規程等には、個人情報の取扱いの各段階、すなわち、利用目的の特定、取得、保管、

利用、提供、廃棄の各段における手順、責任者、担当者等を含めること

5) 本指針を遵守するために必要となる個人情報の適切な安全管理のための対策についての実施計画を整備し、運用し、点検し、改善を行うこと

6) 本人及び代理人からの苦情及び相談に対して、本指針に従い、体制と手順等を定め、可能な限り迅速、かつ、適切に対処すること

7) 事故、外部からの攻撃、又は、違反等により個人情報の漏えい、き損及び滅失等の問題が発生した場合には、本指針に従い、速やかに適切な対応をとること

8) 個人情報に関する苦情処理の解決先として、当法人の窓口を法令に従い適切な方法で公表すること

9) 上記事項を、従業者が認識できるよう周知徹底すること

4 本指針で用いる用語の定義

本指針における用語の定義は、以下のとおりとします。なお、具体例は別表 1 に記載しましたので、必要に応じて参照してください。

1) 個人情報

個人に関する情報であって、以下の①、②のいずれかに該当するもの(個人情報保護法では、生存する個人に関する情報としていますが、本指針ではより安全に個人情報の取扱いが行えるよう、生死の区別を設けません。(本指針において、より安全な個人情報の取扱いと管理を行うために定めた事項を「本指針適用事項」という。以下において同じ。))

① 当該情報に含まれる氏名、生年月日その他の記述等(文書、図画若しくは電磁的記録に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項(個人識別符号を除く。)をいう。以下同じ。)により特定の個人を識別することができるもの(他の情報と容易に照合することで特定の個人を識別できることとなるものを含む)

② 個人識別符号を含むもの

2) 個人識別符号

次の①、②のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるもの

① 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

② 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカード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、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

③　個人識別符号の概要

ⅰ）①に該当する個人識別符号(個人情報保護委員会規則で定める基準に適合するもの)

- 細胞から採取されたデオキシリボ核酸(別名 DNA)を構成する塩基の配列(人の DNA 情報)
- 顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌(顔認証)
- 虹彩の表面の起伏により形成される線状の模様(虹彩認証)
- 発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化によって定まる声の質(声紋認証)
- 歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様(歩容認証)
- 手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状(手の静脈認証)
- 指紋又は掌紋
- 上記の組み合わせ

ⅱ）②に該当する個人識別符号

- 政令及び個人情報保護委員会規則で指定された文字、番号、記号その他の符号(旅券番号、基礎年金番号、免許証の番号、住民票コード、個人番号、公的保険の被保険者証の記号、番号及び保険者番号、並びに、特別永住者証明書の番号等)

3)　要配慮個人情報

本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報

①　人種
②　信条
③　社会的身分
④　病歴
⑤　犯罪の経歴
⑥　犯罪により害を被った事実
⑦　身体障害、知的障害、精神障害(発達障害を含む。)その他の個人情報保護委員

会規則で定める心身の機能の障害があること

⑧ 本人に対して医師その他医療に関連する職務に従事する者により行われた疾病の予防及び早期発見のための健康診断その他の検査の結果

⑨ 健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと

⑩ 本人を被疑者又は被告人として、逮捕、捜査、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと(犯罪の経歴を除く。)

⑪ 本人を少年法に基づく少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと

4) 本人

個人情報によって識別される特定の個人

5) 個人情報データベース等

個人情報を含む情報を集めたもの(集合物)であって、次の①及び②に掲げるもの(利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。)

① 特定の個人情報を、電子計算機を用いて検索することができるように体系的に構成したもの

② 特定の個人情報を容易に検索することができるように索引等を付加し体系的に構成したもの

③ 政令で定める個人情報データベース等から除くものは、以下ⅰ)～ⅲ)の全てに当てはまるもの

ⅰ) 不特定かつ多数の者に販売することを目的として発行されたもので、かつその発行が法又は法に基づく命令の規定に違反して行われたものでないこと

ⅱ) 不特定かつ多数の者により随時に購入することができ、又はできたものであること

ⅲ) 生存する個人に関する他の情報を加えることなくその本来の用途に供しているものであること

6) 個人データ

個人情報データベース等を構成している個人情報

7) 保有個人データ

以下の①～④に該当するもの

① 個人データであること

② 6カ月以内に消去することとしていないもの

③ 対象事業者が自らの権限で、個人データの内容を訂正、追加、削除、開示(内容を本人に知らせること)をできること

④ 対象事業者が自らの権限で、利用停止、消去(該当する一連の個人データを消すこと)、第三者提供の停止を行うことができること

なお、上記に該当していても、以下の①～④に当てはまる個人データは、保有個人データにはなりません。

① その個人データの有無が分かると、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があるもの

② その個人データの有無が分かると、違法又は不当な行為を助長し、又は誘発するおそれがあるもの

③ その個人データの有無が分かると、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があるもの

④ その個人データの有無が分かると、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

8) 個人情報取扱事業者

個人情報データベース等を事業の用に供している者をいいます。ただし、次の①～④に掲げる者を除きます。

① 国の機関

② 地方公共団体

③ 独立行政法人等(独立行政法人等の保有する個人情報の保護に関する法律(平成15年法律第59号)第2条1項に規定する独立行政法人等をいう。以下同じ。)

④ 地方独立行政法人(地方独立行政法人法(平成15年法律第118号)第2条第1項に規定する地方独立行政法人をいう。以下同じ。)

9) 認定個人情報保護団体

個人情報保護法第47条の規定により、対象事業者による個人情報の適正な取扱いの確保を目的として個人情報保護委員会の認定を受けた者

① 対象事業者の個人情報の取扱いに関する苦情の処理

② 個人情報の適正な取扱いの確保に寄与する事項についての情報の提供

③ 対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

5　個人情報の適正な取扱い

1)　利用目的の特定

(個人情報保護法第 15 条第 1 項)

個人情報の取扱いを行うに当たり、以下の①～④に従い、利用目的を特定する(具体的に決める)こと

① 個人情報の持ち主である本人にとって分かり易いものであること

② 各種法令や公序良俗に反するような利用目的でないこと

③ 個人情報を取得する場合には、取得に先立ち利用目的の特定を行うこと

④ 第三者に個人情報を提供することが想定される場合は、必ず利用目的に加えること

2)　利用目的の遵守

(個人情報保護法第 16 条)

対象事業者は、以下の①～④の場合を除き、特定した利用目的以外で個人情報の利用を行わないこと(合併、事業統合、事業買収等の事業承継で取得した個人情報は、事業承継前の利用目的に従うこと)

① 法令に基づく場合

② 人の生命、身体又は財産の保護のために必要があり、本人の同意を得ることが困難である場合

③ 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り、本人の同意を得ることが困難である場合

④ 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り、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがある場合

3)　利用目的の範囲を超えた利用又は利用目的の変更

(個人情報保護法第 15 条第 2 項及び個人情報保護法第 16 条)

対象事業者は、個人情報を利用目的の範囲を超えて利用する場合、又は、利用目的を変更することが認められている範囲を超えて変更する場合には、あらかじめ、本人の明確な同意を得ること

4)　個人情報の適正取得

(個人情報保護法第 17 条)

対象事業者は、個人情報を取得する場合には、適法かつ公正な手段により行い、以下①～④に示す不正な取得を行わないこと

① 取得時の状況が不適正であると容易に理解できる個人情報の取得
② 取得時の状況が不明確である個人情報の取得
③ 事実を偽り、他者を騙す、脅す等して取得
④ 他者に不正な取得を強要して取得

5) 要配慮個人情報の取得
(個人情報保護法第 17 条第 2 項)
要配慮個人情報を取得する場合は、以下の①～⑥に当てはまる場合を除きあらかじめ本人の同意を得ること
① 法令に基づく場合
② 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
③ 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
④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき
⑤ 当該要配慮個人情報が、本人、国の機関、地方公共団体、個人情報保護法第 76 条第 1 項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合
⑥ その他前各号に掲げる場合に準ずるものとして政令で定める場合

6) 利用目的の通知又は公表
(個人情報保護法第 18 条第 1 項)
特定した個人情報の利用目的を、本人に対して速やかに適切な方法で通知又は公表すること

7) 書面等で直接個人情報を取得する場合
(個人情報保護法第 18 条第 2 項)
契約書、申込書、懸賞の応募葉書等に記入した、あるいは、WEB 上や専用の申込画面等に入力した個人情報を直接取得する場合には、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を除き、確実に本人に利用目的が伝わるよう、あらかじめ特定した利用目的を明示すること

8) 利用目的を変更した場合の通知又は公表
(個人情報保護法第 18 条第 3 項)

利用目的の変更を行った場合は、速やかに、本人に通知又は公表すること

9) 利用目的の通知又は公表を行う必要がない場合

(個人情報保護法第 18 条第 4 項)

以下①～④に当てはまる場合は、利用目的の通知又は公表の義務は適用されません

① 利用目的を本人に通知又は公表することにより、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

② 利用目的を本人に通知又は公表することにより、対象事業者の権利又は正当な利益を害するおそれがある場合

③ 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り、利用目的を本人に通知又は公表することにより当該事務の遂行に支障を及ぼすおそれがある場合

④ 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

10) 個人情報の第三者への提供

(個人情報保護法第 23 条第 1 項)

個人情報を第三者に提供する場合は、以下の①～④の場合を除き、あらかじめ、本人が判断することが可能な情報を通知あるいは明示し、本人の明確な同意を得ること

① 法令に基づく場合

② 人の生命、身体又は財産の保護のために必要があり、本人の同意を得ることが困難である場合

③ 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り、本人の同意を得ることが困難である場合

④ 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り、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがある場合

11) オプトアウトによる個人情報の第三者提供

(個人情報保護法第 23 条第 2 項)

本人の求めにより個人情報の第三者提供を停止することを条件とすることにより、オプトアウトによる要配慮個人情報を除く個人情報の第三者提供が可能ですが、この場合は、個人情報保護委員会の定めに従い、あらかじめ、以下の①～⑤を、本人に通知するか本人が容易に知り得る状態に置くこと。また、個人データを当該第三者提供の対象とする場合には、個人情報保護委員会に届け出ること

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・方法
④ 本人の求めに応じて、第三者への提供を停止すること
⑤ 第三者提供の停止について本人の求めを受け付ける方法

12) オプトアウトに関する事項の変更
(個人情報保護法第 23 条第 3 項)
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・方法及び第三者提供の停止について本人の求めを受け付ける方法を変更する場合は、変更する内容について、個人情報保護委員会規則で定めるところにより、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くこと。また、当該変更が個人データについて行われる場合には、変更する内容について、個人情報保護委員会規則で定めるところにより、あらかじめ、個人情報保護委員会に届け出ること

13) 委託に伴う個人情報の提供
(個人情報保護法 23 条第 5 項第 1 号)
利用目的の達成に必要な範囲内で委託する事項を実施するために必要な範囲内で、個人情報を提供する場合は第三者提供には該当しません。

14) 事業承継に伴う個人情報の提供
(個人情報保護法第 23 条第 5 項第 2 号)
合併、事業統合、事業買収等の事業承継に伴い、当該事業に係る個人情報が提供される場合は、第三者提供に該当しませんが、事業承継前に特定した個人情報の利用目的に従うこと

15) 共同利用
(個人情報保護法第 23 条第 5 項第 3 号)
個人情報を特定の者との間で共同利用する場合は、第三者提供に該当しませんが、以下の①～⑤に示す事項を、あらかじめ、本人に通知するか、あるいは、本人が容易に知り得る状態に置くこと
① 特定の者との間で共同利用すること
② 共同利用される個人情報の項目
③ 共同して利用する者の範囲
④ 利用する者の利用目的
⑤ 個人情報の管理責任者の氏名あるいは名称
なお、個人情報の共同利用を行う場合は、法律で定められた上記の事項に加え、

以下の①～⑥に関して、あらかじめ明確にしておくこと(本指針適用事項)

① 共同利用者として認められる者の範囲

ⅰ） グループ会社(団体)

ⅱ） 特定のキャンペーン事業の一員

ⅲ） 特定の製品の販売等を共同して行う者(フランチャイズ等)

ⅳ） その他、特定の事業を共同して行う者として、明確に範囲を定めること

② 各共同利用者の責任者の明確化と情報の管理

ⅰ） 各共同利用者は、各々個人情報取扱責任者を決めること

ⅱ） 個人情報の管理責任者は、各個人情報取扱責任者の氏名、部署、連絡先を管理すること

ⅲ） 個人情報の管理責任者は、各共同利用者が問い合わせ担当者を設けている場合は、その氏名、部署、連絡先を管理すること

③ 共同利用する個人情報の取扱い

ⅰ） 個人情報の漏えい等防止

各共同利用者は、本指針と同様の安全管理措置を実施することが必要で、安全管理措置の実施が不十分な場合は、①に含まれる者であっても共同利用者にしないこと

ⅱ） 目的外の加工、利用、複写、複製等の禁止

各共同利用者は、共同利用の利用目的の範囲内でのみ加工、複写、複製等を行うことができ、それ以外での利用は禁止とすること

ⅲ） 共同利用終了後の個人情報の返還、消去、廃棄

共同利用が終了した場合は、当該共同利用者は速やかに共同利用していた個人情報を、個人情報の管理責任者に返還するか、速やかに安全な方法で消去あるいは廃棄することとし、個人情報の管理責任者は、消去あるいは廃棄したことを、書面をもって確認すること

④ 共同利用する個人情報の取扱いに関する取り決めが遵守されなかった場合

ⅰ） いずれかの共同利用者が、共同利用の利用目的以外に使用した場合、個人情報の管理責任者は、違反状態が解消されるまで当該者に対する他の共同用者からの個人情報の提供を中止させること

ⅱ） いずれかの共同利用者が、不正な第三者への提供を行った場合、個人情報の管理責任者は、直ちに当該者に対する他の共同利用者からの個人情報の提供を中止させること

ⅲ） 重大な違反があった場合には、直ちに共同利用者から除外し、速やかに当該者に対して他の共同利用者から提供された個人情報を消去し、個人情報の管理責任者は確認をとること

⑤ 共同利用する個人情報に関する事件・事故への対応

ⅰ） 共同利用者間での報告連絡体制の整備
ⅱ） 個人情報保護委員会への報告連絡の責任者
ⅲ） 原因の究明、影響範囲の把握、本人への連絡方法に関する取り決め
ⅳ） 再発防止策の公表等に関する取り決め

⑥ 共同利用を終了する際の手続
ⅰ） 共同利用を終了する場合は、個人情報の管理責任者がそのことを本人に通知するか本人が容易に知り得る状態に置くこと
ⅱ） 各共同利用者が、共同利用されていた個人情報を継続して利用する場合は、第三者提供に該当するため、あらかじめ本人の同意を得ること
ⅲ） 共同利用されていた個人情報を委託による提供に、移行する場合は、必要な契約をあらかじめ結び、適法に対応すること

16) 外国にある第三者に個人データを提供する場合
(個人情報保護法第 24 条)

外国にある第三者に個人データを提供する場合は、以下の①～③の場合を除きあらかじめ本人の同意を得ること

① 当該第三者が、日本と同等の水準にあると認められる個人情報保護制度を有している国として個人情報保護委員会規則で定める国にある場合
② 当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として個人情報保護委員会規則で定める基準に適合する体制を整備している場合
④ 個人データの第三者提供の制限が除外される場合
個人情報保護法第 23 条第 1 項第 1 号～第 4 号 (本指針 5 の 10)～④)

17) 個人データを第三者に提供した場合、第三者から取得した場合の確認と記録
(個人情報保護法第 25 条及び第 26 条)

個人データを第三者に提供する場合及び第三者から提供を受ける場合には、提供する場合は①を除き、提供を受ける場合は①及び②を除き、保護法ガイドライン(第三者提供時の確認・記録義務編)に従い、取得の経緯の説明及び確認を実施し、必要とされる事項を記録し、定められた期間を満たすまで保管すること

① 提供者、提供を受ける者の双方が確認・記録を行わなくて良い場合
ⅰ） 個人データの第三者提供の制限が除外される場合
ⅱ） 個人データの第三者提供に該当しない場合
ⅲ） 本人による提供と認められる場合
ⅳ） 本人に代わって提供される場合
ⅴ） 本人の代理人又は家族等、本人と一体と評価できる関係にある者に対し提

供される場合

vi） 誰でも容易に取得できる公開されている個人情報の授受

② 提供を受ける者が確認・記録を行わなくて良い場合

ⅰ） 受領者にとって個人データに該当しない場合

ⅱ） 受領者にとって個人情報に該当しない場合

ⅲ） 閲覧のみや一方的に個人データの送付を受ける等、受領者にとって提供を受けたことにならない場合

③ 記録の保管期間

ⅰ） 本人が行った契約等に基づく提供の場合は、契約書等を 1 年間

ⅱ） 繰り返し同様の提供をする又は提供を受ける場合は、一括して記録が可能で最後の授受が行われた日から 3 年間

ⅲ） それ以外の場合は、3 年間

④ 記録する必要事項

ⅰ） 本人の同意により提供する場合

第三者の氏名等、本人の氏名等、個人データの項目、本人の同意

ⅱ） オプトアウトにより提供する場合

提供した年月日、第三者の氏名等、本人の氏名等、個人データの項目

ⅲ） 本人の同意により提供を受ける場合

第三者の氏名等、取得の経緯、本人の氏名等、個人データの項目、本人の同意

ⅳ） オプトアウトにより提供を受ける場合

提供を受けた年月日、第三者の氏名等、取得の経緯、本人の氏名等、個人データの項目、個人情報保護委員会による公表

⑤ 記録方法及び記録を保管する方法

文書、電磁的記録又はマイクロフィルムを用いて記録を作成する

6 正確性の確保及び廃棄

(個人情報保護法第 19 条)

個人情報は、利用目的に照らして必要となる正確性を確保し、必要がなくなった場合は、速やかに安全な方法で廃棄するように努めなければなりません。

7 安全管理措置

(個人情報保護法第 20 条)

個人情報に対する不正アクセス、漏えいや滅失、毀損等を防止するために、個人情報保護法及び関連する保護法ガイドラインに従い、規律を定め、組織的、人的、物理的、技術的安全管理措置(安全管理のための対策)を実施し、定期的かつ計画的に点検、見直

しを行い、改善しなければなりません。

安全管理措置は、個人情報が漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人情報の取扱状況(取り扱う個人情報の性質及び量を含む。)、個人情報を記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければなりません。

1) 個人情報の取扱いについての規律の整備

個人情報の漏えい等の防止その他の個人情報の安全管理のために、具体的な取扱いについての規律を整備すること

2) 組織的安全管理措置

① 組織体制の整備

安全管理措置を講ずるための組織体制を整備すること

ⅰ) 個人情報の取扱いに関する責任者を任命し役割、責任及び権限を明確にすること(本指針適用事項)

ⅱ) 対象事業者の事業規模に応じ、教育、情報システム、相談及び苦情処理について責任を持つ者、並びに必要に応じて部門責任者等を任命する(各役割は兼務可能)(対応方法例)

ⅲ) 個人情報を取り扱う従業者及びその役割の明確化と従業者が取り扱う個人情報の範囲の明確化すること(対応方法例)

ⅳ) 個人情報の取扱いについて規律に違反している事実又はその兆候を把握した場合の責任者への報告連絡体制を確立すること(本指針適用事項)

ⅴ) 個人情報の漏えい等の事案の発生又は兆候を把握した場合の責任者への報告連絡体制を確立すること(本指針適用事項)

② 個人情報の取扱いに係る規律に従った運用

次に掲げるような事項についての記録を整備すること等により、あらかじめ整備された個人情報の取扱いに係る規律に従った個人情報の取扱いを確保すること

ⅰ) 個人情報データベース等の利用・出力状況(対応方法例)

ⅱ) 個人情報が記載又は記録された書類・媒体等の持ち運び等の状況(対応方法例)

ⅲ) 個人情報データベース等の削除・廃棄の状況(委託した場合の削除・廃棄を証明する記録を含む。)(対応方法例)

ⅳ) 個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況(ログイン実績、アクセスログの収集・確認)(対応方法例)

③ 個人情報の取扱状況を確認する手段の整備

個人情報の取扱状況を確認するための手段を整備すること

ⅰ） 個人情報データベース等の種類、名称、個人情報の項目、利用目的、責任者・取扱部署、利用部署・アクセス権を有する者等を洗い出し、個人情報台帳を作成する(対応方法例)

ⅱ） 洗い出した個人情報のリスクを分析し、実施すべき対策を決めること(対応方法例)

④ 漏えい等の事案に対応する体制の整備

漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備すること

ⅰ） 漏えい等の緊急性の高い事案が発生した場合は、以下の事項について適切に対応すること(本指針適用事項)

- 事実関係の調査及び原因の究明
- 影響を受ける可能性のある本人への連絡
- 個人情報保護委員会等への報告
- 再発防止策の検討及び決定
- 事実関係及び再発防止策等の公表等

⑤ 取扱状況の把握及び安全管理措置の見直し

個人情報の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない

ⅰ） 個人情報の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する(対応方法例)

ⅱ） 外部の主体による監査活動と合わせて、監査を実施する(対応方法例)

ⅲ） 点検や監査の責任者を任命し、代表者や組織の責任者に点検監査の状況を報告する(対応方法例)

ⅳ） 代表者、責任者は、様々な状況を踏まえ、改善、見直しを実施(対応方法例)

3) 人的安全管理措置

① 従業者に、個人情報の適正な取扱いを周知徹底するとともに適切な教育を行うこと

② 従業者との雇用契約、派遣契約等の締結時に非開示契約の締結(誓約書、確認書等の差入れも可)を可能な限り実施すること(本指針適用事項)

4) 物理的安全管理措置

① 個人情報を取り扱う区域の管理

個人情報データベース等を取り扱うサーバーやメインコンピュータ等の重要な

情報システムを管理する区域(以下「管理区域」という。)及びその他の個人情報を取り扱う事務を実施する区域(以下「取扱区域」という。)について、それぞれ適切な管理を行うこと

ⅰ) 管理区域での対策(対応方法例)

- 入退室管理及び持ち込む機器等の制限等
- IC カード、ナンバーキー等による入退室管理システムの設置
- 物理的破壊からの防止

ⅱ) 取扱区域での対策(対応方法例)

- 壁又は間仕切り等の設置、座席配置の工夫
- のぞき込みを防止する措置の実施
- 権限を有しない者による個人情報の閲覧等の防止

② 機器及び電子媒体等の盗難等の防止

個人情報を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために適切な管理を行うこと

ⅰ) 個人情報を取り扱う機器、個人情報が記録された電子媒体又は個人情報が記載された書類等を、施錠できるキャビネット・書庫等に保管(対応方法例)

ⅱ) 個人情報を取り扱う情報システムが機器のみで運用されている場合は盗難防止のために固定(対応方法例)

ⅲ) 監視装置の設置、警報装置の設置、監視サービスの導入等(対応方法例)

③ 電子媒体を持ち運ぶ場合の漏えい等の防止

個人情報が記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人情報が判明しないよう、安全な対策を行うこと

ⅰ) 持ち運ぶ個人情報の暗号化、パスワードによる保護等を行った上で電子媒体に保存(本指針適用事項)

ⅱ) 封緘、目隠しシールの貼付けを行う(対応方法例)

ⅲ) 施錠できる搬送容器を利用(対応方法例)

④ 個人情報の削除及び機器、電子媒体等の廃棄

個人情報を削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元できない手段で行うこと

ⅰ) 個人情報が記載された書類等を廃棄する方法(本指針適用事項)

- 焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用

ⅱ) 個人情報を削除し、又は、個人情報が記録された機器、電子媒体等を廃棄する方法(本指針適用事項)

- 情報システム(パソコン等の機器を含む。)内の個人情報を削除する場合、容易に復元できない手段を採用

・ 個人情報が記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウエアの利用又は物理的な破壊等の手段を採用

5) 技術的安全管理措置

① アクセス制御

担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない

ⅰ) 個人情報を分類し、誰が仕事をする上で必要としているかを確認し、個人情報毎に利用者を決め、個人情報を取り扱えるかどうかの設定を行う(対応方法例)

ⅱ) アクセス権の設定は、個々の個人情報を収納する場所(ディレクトリー)を決め、どのディレクトリーに対して誰が(どの人が)見る(READ)、修正する+追加する(Write)、消す(Delete)できるかの権限を設定する(対応方法例)

ⅲ) 退職、職場の変更、異動により職務が変わった場合には、設定したアクセス権をできるだけ早く変更すること(本指針適用事項)

② アクセス者の識別と認証

個人情報を取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない

ⅰ) 各担当者が使用する情報システムや機器(PC、サーバー、ファイルサーバー)等の機器や個人情報を取り扱う業務システム等で、個人情報を取り扱うことが許可された利用者であるかを確認し、使用許可を与えるようにすること(本指針適用事項)

・ 利用者の ID を決め、利用者の USER Name を決める
・ 利用者を確認する方法を決める
・ 各自のパスワードを設定する

ⅱ) パスワードの使い回しは危険であるため禁止すること(本指針適用事項)

ⅲ) パスワードが見破られないように、単純なものは避ける(対応方法例)

ⅳ) 生体認証を用い、成すましを防ぐ(対応方法例)

ⅴ) PIN Code の利用(対応方法例)

ⅵ) IC カードの利用(対応方法例)

③ 外部からの不正アクセス等の防止

個人情報を取り扱う情報システムを外部からの不正アクセス又は不正ソフトウエアから保護する仕組みを導入し、適切に運用しなければならない

ⅰ) 事業者内のネットワークへの出入りを制限し、外部からの不正な侵入を防止するために以下の対策を行うこと(本指針適用事項)

・ ファイアウォール、UTM、あるいは、ファイアウォール機能のあるルーター等を設置する等し、事業規模に応じた適切な対策を行うこと

ⅱ） 情報機器そのものが不正プログラムにより汚染されないようにし、脆弱性(攻撃に対する弱点)がないように以下の対策を実施すること(本指針適用事項)

・ サーバー、PC、モバイルの各機器にウイルス対策ソフトを導入し最新状態を保つこと

・ ソフトウエアの更新を迅速に実施し脆弱性を排除すること

ⅲ） 情報機器の監視ソフトにはアクセスログを残す機能があるので利用する(対応方法例)

ⅳ） 情報機器に備え付けられた機能を利用しアクセスの記録を残す(対応方法例)

④ 情報システムの使用に伴う漏えい等の防止

情報システムの使用に伴う個人情報の漏えい等を防止するための措置を講じ、適切に運用しなければならない

ⅰ） 情報システムのテストを実施する際は、ダミーデータを使用すること(本指針適用事項)

ⅱ） 個人情報を含むファイルの送受信を行う場合は、暗号化やパスワード設定等による保護措置を講じること(本指針適用事項)

ⅲ） インターネットを介して個人情報の授受を行う場合は VPN(バーチャルプライベートネットワーク)を利用し、インターネット利用の安全性を確保する(対応方法例)

ⅳ） 電子メールのやり取りを安全な設定で行う(対応方法例)

ⅴ） 不正アプリケーションソフトウエアの起動防止、その他監視ソフトの導入(対応方法例)

ⅵ） 対象事業者の状況に応じて、個人情報取扱い状況が分かるよう適切な方法でアクセスログの収集、確認を実施し、併せて不正通信の監視サービス等を導入する(対応方法例)

8 従業者の監督

(個人情報保護法第 21 条)

従業者に対して個人情報の適正な取扱いと安全管理が徹底できるよう、適切な監督を計画的、定期的、継続的に実施しなければなりません。

1) 従業者の監督のために、監視等対策を行う場合は、従業者の権利保護のために、組合、職場代表者等と協議し合意した上で実施すること(本指針適用事項)

2) 可能な限り実施状況について記録を残すよう努めること(本指針適用事項)

9 委託先の監督

(個人情報保護法第 22 条)

個人情報の取扱いを含む業務の一部又は全部を委託する場合は、以下の事項に従い適切な監督を計画的、定期的、継続的に実施しなければなりません。

1) 委託先の選定においては、委託先における個人情報保護のための安全管理措置の実施状況を確認し、適切に選定すること

2) 個人情報が適正に取り扱われるよう必要事項を契約内容に含めること

3) 委託先における個人情報の取扱いに関して、定期的に確認し、必要があれば改善をも求めること

4) 再委託先等に関しても委託先と協調し、上記 1)～3)の事項が守られるようにすること

5) 可能な限り実施状況について記録を残すように努めること(本指針適用事項)

10 保有個人データの開示、訂正、削除、消去、利用停止等

対象事業者は、本人から保有個人データの利用目的の通知の求め又は個人情報の開示、訂正、追加、削除、利用停止、消去若しくは第三者への提供の停止(以下、「開示等」といいます)の請求があった場合は、確実に本人確認を行い、関連する法令及び該当する保護法ガイドラインに従って、速やかに対応しなければなりません。

1) 必要事項の公表等

(個人情報保護法第 27 条第 1 項)

保有個人データに関して、以下の①～⑤の事項を本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。以下、同じ。)に置くこと

① 対象事業者の氏名・名称
② すべての保有個人データの利用目的
③ 求め又は請求に応じる手続き(手続きを定めた場合)
④ 利用目的の通知及び開示についての手数料(手数料を定めた場合)
⑤ 政令で定めるもの

ⅰ） 保有個人データの取扱いに関する苦情の申出先
ⅱ） 当法人の苦情の解決の申出先

2) 利用目的の通知
(個人情報保護法第 27 条第 2 項及び第 3 項)
本人から、保有個人データの利用目的について通知を求められた場合(問い合わせを受けた場合)、以下の①～④の場合を除き、本人に対し遅滞なく通知すること
① 保有個人データの利用目的が明らかな場合
② 人の生命・身体・財産その他の権利利益が侵害されるおそれがある場合
③ 当該対象事業者の権利・正当な利益が侵害されるおそれがある場合
④ 国の機関・地方公共団体が法令の定める事務を遂行することに対する必要な協力に支障を及ぼすおそれがある場合
上記①～④に該当して利用目的の通知を行わないことを決めたときは、遅滞なくその旨を本人に通知すること

3) 開示
(個人情報保護法第 28 条)
本人から、保有個人データの開示(存在しないときにはその旨を知らせることを含む。以下同じ。)を請求された場合は、以下の①～③の場合を除き、本人に対し書面の交付による方法(請求を行った者が同意した場合他の方法も可能)により開示すること
① 人の生命・身体・財産その他の権利利益が侵害されるおそれがある場合
② 当該対象事業者の業務の適正な実施に著しい支障の生じるおそれがある場合
③ 他の法令に違反することとなる場合
上記①～③に該当して保有個人データの開示をしないことを決めたときは、遅滞なくその旨を本人に通知すること

4) 訂正、追加、削除
(個人情報保護法第 29 条)
本人から、保有個人データの内容に誤りがあり、事実でないという理由によって、訂正、追加又は削除(以下、「訂正等」という)を請求された場合は、以下の①～④に従い対応すること
① 「原則」訂正等を請求に対しては、利用目的の範囲内で遅滞なく調査し、対応すること
② 利用目的を達成するうえで訂正等をする必要がない場合や事実ではないという

理由が正しくない場合には、訂正等を行わなくてよい

③ 他の法律等で取り決めがある場合は、そちらを優先すること

④ 訂正等を行った場合も、行わなかった場合も本人に対し遅れることなく通知すること

5) 利用停止、消去

(個人情報保護法第 30 条第 1 項及び第 2 項)

本人から、保有個人データが以下の①及び②の違反があったとの理由によって、利用の停止、消去(以下、「利用停止等」という)を請求された場合は、その請求が妥当であり、かつ、その理由が事実である場合には、遅滞なく、利用停止等を行うこと

① 「利用目的による制限」に違反して取り扱われている場合(目的外利用)

② 「適正な取得」に違反している場合(不正な手段による取得)

ただし、以下の①及び②の場合には、本人の権利利益を保護するために必要となる他の方法により対応することが可能

① 利用停止等に多額の費用が掛かり、他の方法で本人の権利利益を保護することができる場合

② その他利用停止等が困難であり、他の方法で本人の権利利益を保護することができる場合

6) 第三者提供の停止

(個人情報保護法第 30 条第 3 項及び第 4 項)

本人から、同意していないのに保有個人データが第三者に提供されているという理由によって第三者への提供の停止を請求された場合は、その請求が妥当であり、かつ、その理由が事実である場合には、遅滞なく、第三者への提供の停止を行うこと

ただし、以下の①～②の場合には、本人の権利利益を保護するために必要となる他の方法により対応することが可能

① 第三者提供の停止に多額の費用が掛かり、他の方法で本人の権利利益を保護することができる場合

② その他第三者提供の停止が困難であり、他の方法で本人の権利利益を保護することができる場合

7) 利用の停止等(利用停止、消去、第三者への提供の停止)の通知

(個人情報保護法第 30 条第 5 項)

保有個人データの全部又は一部について利用の停止等を行った場合、利用の停止

を行わないことを決めた場合のいずれの場合においても、本人に対し遅滞なく実施した内容等又は請求に応じないことを通知すること

8) 理由の説明

(個人情報保護法第 31 条)

保有個人データの開示等において、請求への対応を通知する場合、あるいは請求と異なる対応を行うことを通知する場合は、その理由を本人に説明するよう努めること

9) 利用目的の通知の求め、開示等の請求に応じる手続き

(個人情報保護法第 32 条)

利用目的の通知の求め又は開示等の請求を受け付ける方法として、以下の①～④を含む手続きを定めることができますが、定めた場合には、その内容を本人の知り得る状態に置くこと

① 利用目的通知の求め、開示等の請求の受付先
② 利用目的通知の求め、開示等の請求に際して提出すべき書面の様式、その他の受付方法
③ 利用目的通知の求め、開示等の請求をする者が、本人又はその代理人であることの確認方法
④ 手数料の徴収方法

10) 手数料

(個人情報保護法第 33 条)

利用目的通知の求め及び開示等の請求については、実費を基に妥当性のある手数料を設定することができますが、その場合、設定した手数料を本人の知り得る状態に置くこと

11) 裁判上の訴えの事前請求

(個人情報保護法第 34 条)

本人が対象事業者に対して開示等の請求権を有することが明確化され、裁判上の訴えを提起できることが明確になりました。その場合、本人があらかじめ裁判外において当該請求を対象事業者に対し行い、かつ、当該請求が当該対象事業者に到達した日から 2 週間を経過した後でなければ、その訴えを提起することができません。但し、対象事業者が当該裁判外の請求を拒んだときは、2 週間を経過する前に訴えを提起することができます。当該裁判外の請求を拒んだときとは、以下の①～③が該当します。

① 対象事業者が本人に不開示等の通知を行った場合
② 対象事業者が請求に応じない態度を明らかにした場合
③ 本人が求める開示等の請求が一部しか認められなかった場合、その以外の部分について

11 苦情への対応

個人情報の取扱いに関する苦情又は相談がなされた場合は、可能な限り迅速に対処しなければなりません。そのために、対象事業者の責務及び組織的安全管理措置において示した、以下の①～③を実施しなければなりません。(本指針適用事項)

① 苦情相談の責任者の任命と窓口の設置及びその公表
② 苦情相談に対応するための手順の整備
③ 当法人の苦情解決窓口の公表等を行うこと

12 本指針が遵守されない場合

本指針が遵守されない事実が判明した場合は、対象事業者は遵守されていない事項に関して、改善策を実施しなければなりません。

改善策が実施されない場合、当法人は対象事業者に対して助言、指導及び勧告を行い、当該対象事業者はその内容を尊重し、適切に対応しなければなりません。

以上