印刷・グラフィックサービス工業における　個人情報保護指針

公益社団法人　東京グラフィックサービス工業会
制定　2004 年(平成 16 年)8 月 23 日　第 4 回理事会
改定　2022 年(令和 4 年)9 月 6 日　第 2 回理事会

序　文

公益社団法人　東京グラフィックサービス工業会（以下、当会という）は、東京都における印刷・グラフィックサービス工業の事業者団体として個人情報保護の重要性を認識し、認定個人情報保護団体として対象事業者（当会正会員）である当会会員の個人情報保護への自主的な取組みを促進・支援するため、当会正会員への本指針の普及・啓発を図るとともに、消費者の個人情報保護に取り組む。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）は、認定個人情報保護団体に対して、当会正会員に個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとることを求めており、当会正会員は、本指針を守らなければならない。当会は、正会員に対し、本指針を遵守させるために必要な指導、勧告その他の措置をとることとする。又、消費者保護の観点から、当会は関連法令及び本指針を遵守することを約束する。

個人情報の適切な保護について、令和２年、３年に個人情報保護法が改正され、これまでに行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（通称：マイナンバー法)、特定個人情報の適正な取扱いに関するガイドライン（事業者編）が制定されている。令和４年４月より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)、同（外国にある第三者への提供編)、同（第三者提供時の確認・記録義務編)、同（仮名加工情報・匿名加工情報編)、同（認定個人情報保護団体編）が改正・施行された。加えて、対象事業者が体系的で経営活動全般を統合した個人情報保護マネジメントシステムを策定するための規範として、日本産業規格「個人情報保護マネジメントシステム-要求事項」(JIS Q 15001：2017）も考慮し、ジャグラ個人情報保護ガイドライン第６版（令和４年３月発行）及び令和４年４月、プライバシーマークにおけるＰＭＳ構築・運用指針が（一財）日本情報経済社会推進協会（ＪＩＰＤＥＣ）より公表されたので当会では、同指針も参考に本指針を改定した。
対象事業者は、個人情報を含む多種多様な情報を大量に取り扱う者の責務として個人情報の適切な保護に努めなければならないが、そのためには、本指針に準拠した対応を検討し、方針・ルール（内部規程、手順等）を策定し、それを実施し、維持し、及び継続的に改善していくことが必要である。
なお、対象事業者は、それぞれの事業活動の実態に照らし、個人情報との係わりを的確に把握した上で、本指針に規定した事項のほかに必要な項目を追加することができる。

本指針は、対象事業者が自由かつ公正な競争を阻害したり、法的義務を増大又は変更するために用いられることを意図したものではない。
対象事業者は、自由な情報流通の確保を前提とした高度情報通信社会の進展に資するため、個人情報の保護の必要性と個人情報の利活用等の有用性を共に認識し、両者を調和させるよう努めなければならない。

2022 年 9 月 6 日

公益社団法人東京グラフィックサービス工業会　会長　原 田 大 輔

第 1 章 適用範囲

（適用範囲）

第 1 条　本指針は、個人情報を事業の用に供している、対象事業者（当会正会員）に適用できる。対象事業者は、自らの事業の用に供している全ての個人情報の取扱いを個人情報保護マネジメントシステムの適用範囲として定め、その旨を文書化すること。
対象事業者は、次の事項を行う場合に、本指針を用いることができる。本指針は、当会が消費者に対して個人情報保護に対する有効な方針となることを約束する。

1. 本指針に基づき自社の個人情報保護方針を確立し、具体的に定めたルール（内部規程、手順等）に沿って運用を実施し、維持し、かつ、改善すること。
2. 本指針と自社で定める方針、ルールを確認し、適合していることを自ら表明すること。
3. 対象事業者は、組織内部、外部及び消費者に対して、本指針を遵守すること。

第 2 章 用語及び定義

（定義）

第 2 条 本指針で用いる用語の定義は、次による。

1. 個人情報：個人に関する情報であって、当該情報に含まれる、氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、ある個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わないもののうち、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それによって特定の個人を識別できるものを含む。）。本定義は、個人情報保護ガイドライン（通則編）等に準じ、齟齬のないように見直す。対象事業者が取り扱う個人情報としては、委託されて製作する印刷物（名刺、各種名簿、挨拶状、個人出版物、等）、発送の宛名等、従業者等の情報、各種情報処理関連データ等がある。

2. 個人識別符号：文字、番号、記号その他の符号のうち、以下に定めるものをいう。

（1）特定の個人の身体の一部の特徴を電子計算機の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（例：顔認証データ、指紋識別データ等）。個人情報保護法政令第 1 条 1 号に準じる。

（2）対象者ごとに異なるものとなるように役務の利用、若しくは商品の購入又は個人に発行されるカードその他の書類に付される符号（例：旅券番号、免許証番号等）。個人情報保護法政令第１条 2 号以下に準じる。

3. 要配慮個人情報（特定な機微情報を含む）：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個人情報保護法政令で定める記述等が含まれる個人情報。

4. 個人情報データベース等：個人情報を含む情報の集合物であって、次に掲げるもの（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個人情報保護法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）前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして個人情報保護法政令で定めるもの。

5. 個人データ：個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報をいう。なお、法第 16 条第 1 項及び政令第 4 条第 1 項に基づき、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ため、個人情報データベース等から除かれているもの（例：市販の電話帳・住宅地図等）を構成する個人情報は、個人データに該当しない。

6. 保有個人データ：個人情報取扱事業者が、 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。（例：自社の事業活動に用いている顧客情報、従業員等の人事管理情報）

7. 個人関連情報：生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいう。「個人に関する情報」とは、ある個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報である。「個人に関する情報」のうち、氏名、生年月日その他の記述等により特定の個人を識別することができるものは、個人情報に該当するため、個人関連情報には該当しない。また、統計情報は、特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」に該当するものではないため、個人関連情報にも該当しない。

8. 匿名加工情報：個人情報に措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたもの。

9. 匿名加工情報を取扱う事業者：匿名加工情報を含む情報の集合物であって、特定の匿名加工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、その

他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして、個人情報保護法政令で定めるもの（以下「匿名加工情報データベース等」という。）を事業の用に供している者。

10.仮名加工情報：個人情報を、その区分に応じて次に掲げる措置を講じて他の情報と照合しない限り、特定の個人を識別することができないように加工して得られる個人に関する情報をいう。

当該個人情報に含まれる記述等の一部を削除すること。

「削除すること」には、「当該一部の記述等」又は「当該個人識別符号」を「復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む」とされている。

「復元することのできる規則性を有しない方法」とは、置き換えた記述等から、置き換える前の特定の個人を識別することとなる記述等、又は個人識別符号の内容を復元することができない方法である。

「特定の個人を識別することができる」とは、情報単体又は複数の情報を組み合わせて保存されているものから社会通念上そのように判断できるものをいい、一般人の判断力又は理解力をもって生存する具体的な人物と情報の間に同一性を認めるに至ることができるかどうかによるものである。

11. 本人：個人情報によって識別される特定の個人。

12. 対象事業者：当会会員で事業を営む法人その他団体又は個人。

13. 個人情報保護管理者：代表者によって事業所の内部の者から指名された者であって、個人情報保護マネジメ ントシステムの実施及び運用に関する責任と権限をもつ者 。

14. 個人情報保護監査責任者：代表者によって事業者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権限をもつ者。

15. 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。本人が未成年又は事理を弁識する能力を欠く者の場合は、法定代理人の同意も得なければならない 。

第 3 章 個人情報保護方針

（個人情報保護方針）

第 3 条　代表者は、個人情報保護の理念を明確化した上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなければならない。

a)事業の目的に対して適切であること

b)対象事業者が定めた個人情報保護目的を含むか、又は個人情報保護目的の設定のための枠組みを示すこと

c)個人情報保護に関連して適用される要求事項を実施すること

d)個人情報保護マネジメントシステムの継続的改善を実施すること

個人情報保護方針を文書化した情報には、次の事項を含むこと。

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その他の規範の遵守
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事項
d)苦情及び相談への対応に関する事項
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事項
f)代表者の氏名
g)制定年月日及び最終改正年月日
h)個人情報保護方針の内容についての問合せ先
代表者は、個人情報保護方針を文書化した情報を、事業者内に周知するとともに、一般の人が入手可能な措置を講じること。

第 4 章 計画

（個人情報の特定）
第 4 条 対象事業者は、自らの事業の用に供している全ての個人情報を特定するための手順を内部規程として文書化すること。
個人情報を管理するための台帳を整備すること。
台帳には、少なくとも次の項目を含むこと。
・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
台帳の内容は少なくとも年一回、適宜に確認し、最新の状態で維持すること。

（法令，国が定める指針その他の規範）
第 5 条 対象事業者は、個人情報の取扱いに関する法令、国が定める指針その他の規範（以下、「法令等」という。）を特定し、参照する手順を内部規程として文書化すること。法令等を特定し参照すること

（リスク及び機会に対処する活動）
第 6 条 対象事業者は、個人情報保護マネジメントシステムの計画の策定にあたって、第

１条で把握した課題及び 利害関係者の要求事項を考慮し、次の事項を実現できるよう個人情報保護リスクアセスメント及び個人情報保護リスク対応を行うこと。

a)事業者が意図した成果を達成できるようなマネジメントシステムの策定

b)望ましくない影響の防止

c)個人情報保護マネジメントシステムの継続的な改善

事業者は、個人情報保護マネジメントシステムの計画の策定にあたって、次の事項を含むこと。

d)リスクに対する対策の内容

e) d)の対策を個人情報保護マネジメントシステムの手順に含めて実施する方法

f) d)の対策の評価

（個人情報保護リスクアセスメント）

第７条　対象事業者は、個人情報に関するリスクについて、次の事項を踏まえて、個人情報保護リスクアセスメント（リスクを特定、分析及び評価）をするための手順を定め、かつ実施すること。手順及び実施した内容については、少なくとも年一回及び必要に応じて適宜に見直すこと。

a)次の観点を、個人情報保護のリスク基準とする

1)本指針に定める事項

2)法令及び国が定める指針その他の規範に関する事項

3)個人情報の漏えい、滅失又はき損等に関する事項

b)繰り返し実施した個人情報保護リスクアセスメントに、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にする

c)個人情報保護リスクを特定する

1)事業者において、事業毎に、個人情報の取扱いを特定する

2)個人情報の取得、保管、利用及び消去等に至る各局面において、適正な保護措置を講じない場合に想定されるリスクを特定する

3)上記で特定したリスクのリスク所有者を特定する

d)個人情報保護リスクを分析・評価する

1) c)で特定したリスクと、a)のリスク基準とを比較する

2)リスク対応の優先順位を明らかにする

事業者は、個人情報保護のリスクを特定、分析及び評価をするための手順を内部規程として文書化すること。

（個人情報保護リスク対応）

第８条　対象事業者は、次の事項について、個人情報保護リスクへの対応手順を内部規程として文書化し、かつ実施すること。

手順及び実施した内容については、適宜見直すこと。

a)個人情報保護リスクへの対応にあたっては、個人情報保護リスクアセスメントの結果を考慮して、必要な対応策（本指針及び事業者が必要であると決定した、個人情報保護に関するリスクを修正する対策を含む。）を策定すること

b) a)を踏まえて、個人情報保護リスクへの対応計画を策定し、実施すること

c)個人情報保護リスクへの対応計画及び実施した内容（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、管理することを含む。）について、原則として、トップマネジメントの承認を得ること

対象事業者は、a)～c)を実施した記録を保持すること。

（個人情報保護目的及びそれを達成するための計画策定 ）

第 9 条　対象事業者は、次の事項を含めて、個人情報保護目的を達成するために計画すること。

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

（計画策定）

第 10 条　対象事業者は、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、次の事項を含めて、少なくとも年一回及び必要に応じて適宜に必要な計画を立案し、文書化すること。

a)教育実施計画

b)内部監査実施計画

第 5 章　支援

（認識：教育）

第 11 条　対象事業者は、従業者に対して、少なくとも年一回及び必要に応じて適宜に教育を実施する手順（教育の理解度を確認する手順を含む）を内部規程として文書化すること。

事業者は、従業者に対して、次の事項を認識させること。

a)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

（緊急事態への準備）

第 12 条　対象事業者は、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内部規程として文書化すること。

緊急事態への準備及び対応に関する規定には、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含むこと。

緊急事態への準備及び対応に関する規定には、緊急事態が発生した場合に備え、次の事項を対応手順に含むこと。

a)漏えい、滅失又はき損等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)緊急事態が発生した場合、定めた手順に従って緊急事態への対応を実施する

事実関係、発生原因及び対応策を個人情報保護委員会に報告すること。個人の権利利益を害するおそれが大きいものが発生した場合（特定個人情報：マイナンバー、要配慮個人情報、クレジットカード情報、不正アクセス事故、1，000 人を超える場合等）は、個人情報保護委員会へ事故発覚後 3～5 日以内に「速報」をその後、事故報告書の「確報」を個人情報保護委員会へ報告すること

d)当会への報告は、個人情報保護委員会への報告後、速やかに行うこととする

報告内容は、事故の概要（発生日・発覚日含む)、事故対象者の個人情報の媒体、項目及び件数、事故に係る経緯、事故発生元、事故対象となった個人情報等の本人への対応等とする。

（文書化した情報）

第 13 条　対象事業者は、個人情報保護マネジメントシステムの基本となる次の要素に対応する書面を作成すること。

a)個人情報保護方針

b)内部規程

c)内部規程に定める手順上で使用する様式

d)計画書

e)本指針が要求する記録

f)その他、事業者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文書（記録を含む。）

（文書化した情報の管理）

第 14 条　対象事業者は、個人情報保護マネジメントシステム及び本指針で要求されてい

る文書化した情報は、次の事項を確実にするために管理すること。
a)必要な時に、必要な所で、入手可能かつ利用に適した状態である
b)十分に保護されている（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）
文書化した情報の管理にあたっては、次の事項を実施すること。
c)配付、アクセス、検索及び利用
d)読みやすさが保たれることを含む、保管及び保存
e)変更の管理（例えば、版の管理）
f)保持及び廃棄
個人情報保護マネジメントシステムに必要となる外部からの文書化した情報は、必要に応じて特定し、管理すること。

（文書化した情報（記録を除く）の管理）
第 15 条　対象事業者は、本指針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、次の事項を含む内部規程として文書化すること
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
d)適切性及び妥当性に関する、適切なレビュー及び承認を行うこと
文書化した情報（記録を除く。）の管理を実施すること。

（内部規程）
第 16 条　対象事業者は，次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。
次の事項を含む内部規程を文書化すること。
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
d)事業者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請求等への対応に関する規定
i)教育などに関する規定
j)文書化した情報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、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すること。

（文書化した情報のうち、記録の管理 ）

第 17 条　対象事業者は、個人情報保護マネジメントシステム及び本指針で要求されている記録の管理についての手順を内部規程として文書化すること。
次の事項を含む必要な記録を作成すること。
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

第 6 章　パフォーマンス評価

（監査、測定、分析及び評価）

第 18 条　各部門及び階層の管理者が定期的に、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ことを確認する手順を内部規程として文書化すること。
対象事業者は、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かどうかを確認するために、次の事項を決定すること。
a)対象とする個人情報保護マネジメントシステムの運用状況
b) a)で対象とした運用状況の監視、測定、分析及び評価の方法
c) a)で対象とした運用状況の監視及び測定の実施時期

d) a)で対象とした運用状況の監視及び測定の実施者
e) a)で対象とした運用状況の分析及び評価の時期
f) a)で対象とした運用状況の分析及び評価の実施者
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、その是正処置を行うこと。
対象事業者は、監視及び測定の結果の証拠として、文書化した情報を保持すること。
個人情報保護管理者は、定期的に、及び適宜にトップマネジメントに運用の確認の状況を報告すること。

（内部監査）

第 19 条　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内部規程として文書化すること。
対象事業者は、個人情報保護マネジメントシステムが次の事項の状況にあるか否かについて、少なくとも年一回及び必要に応じて適宜に内部監査を実施すること。
a)事業者が規定した要求事項及び本指針の要求事項に適合している
b)個人情報保護マネジメントシステムが有効に実施され、維持されている
個人情報保護監査責任者は、次の事項を行うこと。
c)内部監査実施計画を策定、確立、実施及び維持する。その内部監査実施計画は、関連するプロセスの重要性及び前回までの監査の結果を考慮する
d)各監査について、監査基準及び監査範囲を明確にする
e)監査プロセスの客観性及び公平性を確保する監査員を選定し、内部監査実施計画に従って、監査を実施する
f)監査の結果を監査報告書としてまとめ、管理層及び代表者に報告する
g)内部監査実施計画及び監査結果の証拠として、文書化した情報を保持する
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。

（対象事業者の代表者による見直し：マネジメントレビュー）

第 20 条　対象事業者の代表者は、マネジメントレビューを実施する手順を内部規程として文書化すること。
事業者の個人情報保護マネジメントシステムが、引き続き、適切、妥当かつ有効であることを確実にするために、少なくとも年一回及び必要に応じて、適宜にマネジメントレビューを実施すること。
マネジメントレビューの実施にあたっては、次の事項を考慮すること。
a)前回までのマネジメントレビューの結果を踏まえた見直しの状況
b)個人情報保護マネジメントシステムに関連する外部及び内部の問題点の変化

c)以下の状況を踏まえた、現在の個人情報保護マネジメントシステムの運用状況の評価
1)不適合及び是正処置
2)確認及び点検の結果
3)監査結果
4)個人情報保護目的の達成
d)利害関係者からのフィードバック
e)リスクアセスメントの結果及びリスク対応計画の状況
f)継続的改善の機会
マネジメントレビューからのアウトプットには、継続的改善の機会及び個人情報保護マネジメントシステムのあらゆる変更の必要性に関する決定を含めること。
事業者は、マネジメントレビューの結果の証拠として、文書化した情報を保持すること。

第 7 章 改善

（不適合及び是正処置）

第 21 条 対象事業者は、次の事項を含めて、不適合に対する是正処置を実施するための責任及び権限を定める手順を内部規程として文書化すること。
a)その不適合に対処し、該当する場合には、必ず、次の事項を行う
1)その不適合を管理し、修正するための処置をとる
2)その不適合によって起こった結果に対処する
b)次の事項によって、その不適合の原因を除去するための処置を検討する
1)その不適合を調査及び分析する
2)その不適合の原因を特定する
3)類似の不適合の有無、又はそれが発生する可能性を検討する
c)是正処置を計画し、計画された処置を実施する
d)実施された全ての是正処置の有効性を調査、分析及び評価する
e)必要な場合には、個人情報保護マネジメントシステムの改善を行う
不適合が明らかとなった場合、a)～e)の事項を実施すること。
a)～e)の実施結果について、文書化した情報を保持するとともに、原則として、トップマネジメントが承認すること。

（継続的改善）

第 22 条 対象事業者は、個人情報保護マネジメントシステムの適切性、妥当性及び有効性を継続的に改善すること。

第 8 章 取得、利用及び提供に関する原則

（利用目的の特定）

第 23 条　個人情報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取扱いを行うこと。
利用目的は、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こと。

（適正な取得）
第 24 条　対象事業者は、適法かつ公正な手段によって個人情報を取得すること。

（要配慮個人情報）
第 25 条　新たに要配慮個人情報を取得、利用又は提供並びに要配慮個人情報のデータを提供する場合、あらかじめ書面による本人の同意を得ること。
要配慮個人情報を取得、利用する際、書面による本人の同意を得ることを要しないときとは、以下の場合に限定すること。
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)当該要配慮個人情報が、法令等により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であるとき
f)本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得又は利用する場合
g)個人情報保護法二十七条第五項各号に掲げる場合において、個人データである要配慮個人情報の提供を受けるとき
h)個人情報取扱事業者が学術研究機関等である場合であって、当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）
i)学術研究機関等から当該要配慮個人情報を取得し、利用する場合であって、当該要配慮個人情報を学術研究目的で取得し、利用する必要があるとき（当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（当該個人情報取扱事業者と当該学術研究機関等が共同して学術研究を行う場合に限る。）

要配慮個人情報を提供する際、書面による本人の同意を得ることを要しないときとは、第25条のa)～d)又は、以下の場合に限定すること。
j)個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）
k)個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限る。）
l)第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

（個人情報を取得した場合の措置）
第 26 条　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し、又は公表すること。
本人に利用目的を通知し、又は公表を要しないのは、以下の場合に限定すること。
a)利用目的を本人に通知し、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し、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し、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

（第26条のうち本人から直接書面によって取得する場合の措置）
第27条 本人から、書面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こと。
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)第 44 条～第 47 条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

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いのは、以下の場合に限定すること。

・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
・以下のいずれかに該当し、第 26 条の措置を要しない場合

1)利用目的を本人に通知し、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
2)利用目的を本人に通知し、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
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る場合であって、利用目的を本人に通知し、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
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

（利用に関する措置）

第 28 条　個人情報を利用する場合には、本人の同意の有無に関わらず、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を除くこと。

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こと。

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、第 27 条の 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、本人の同意を得ること。

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に、本人の同意を得ることを要しないのは、以下のいずれかに該当する場合に限定すること。

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り当該事務の遂行に支障を及ぼすおそれがあるとき。
e)当該個人情報取扱事業者が学術研究機関等である場合であって、学術研究目的で取り扱う必要があるとき（当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）
f)学術研究機関等に個人データを提供する場合であって、当該学術研究機関等が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）

（本人に連絡又は接触する場合の措置）

第 29 条　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、第 27 条の 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、本人の同意を得ること。
個人情報を利用して本人に連絡又は接触する場合のうち、本人に通知し、本人の同意を得ることを要しない場合を、利用する個人情報が以下の場合に限定すること。
a）第 27 条の措置において、あらかじめ、利用目的として個人情報を利用して本人に連絡又は接触することを含め、第 27 条の 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、既に第 27 条の 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、共同して利用する者が、既に共同して利用することに関して、第 27 条の 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、以下の 1)～6)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。)
1)共同して利用すること
2)共同して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)共同して利用する者の利用目的
5)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及び住所及

び並びに法人にあっては、その代表者の氏名

6)取得方法

e) 第 26 条の d)に該当し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) 第 25 条の a)～d)のいずれかに該当する場合

（個人データの提供に関する措置）

第 30 条　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、当該個人データを第三者に提供することに関して、第 27 条の 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、本人の同意を得ること。

2. 個人データを第三者に提供する場合に、本人に通知し、本人の同意を得ることを要しない場合は、以下の場合に限定すること。

a) 第 27 条の規定によって、個人データを第三者に提供することに関して、既に第 27 条の 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し、本人の同意を得ているとき、又は第 29 条の規定によって、既に第 27 条の 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、本人に通知し、又はそれに代わる同等の措置を講じているとき

1) 事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

2)第三者への提供を利用目的とすること

3)第三者に提供される個人データの項目

4)第三者への提供の手段又は方法

5)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

6)取得方法

7)本人からの請求などを受け付ける方法

8)その他個人の権利利益を保護するために必要なものとして個人情報保護委員会規則で定める事項

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、法令等が定める手続に基づいた上で、b)の 1)～8)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、第 29 条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) 第 25 条の a)～d)のいずれかに該当する場合
3. 2 項 b)の適用にあたっては、以下の 1)～3)を除くこと。
1)要配慮個人情報
2)偽りその他不正の手段により取得された個人データ
3)個人情報保護法二十七条第二項、又は第 30 条の前項 b)により提供された個人データ(提供されたデータに対して、その全部又は一部を複製し、又は加工したものを含む)

(外国にある第三者への提供の制限)

第 31 条 1. 外国にある第三者に個人データを提供する場合、以下のいずれかを満たすこと。ただし、第 25 条の a)～d)、又は、第 25 条の j)～l)のいずれかに該当する場合はこれに限らない。
a)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がある場合
b)個人データの取扱いについて、個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なもの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者への提供をする場合
c)個人の権利利益を保護する上で我が国と同等の水準にある外国として個人情報保護委員会規則で定める国・地域にある第三者への提供をする場合
2. 1 項の a)によって外国にある第三者に個人データを提供する場合は、あらかじめ、法令等の定めるところによって、次に掲げる事項について、当該本人に必要な情報を提供すること。
d)当該外国の名称
e)当該外国における個人情報の保護に関する制度に関する情報
f)当該第三者が講ずる個人情報の保護のための措置に関する情報
g) d)～f)に定める事項が特定できない場合、その旨及びその理由
h) g)に該当する場合であって、d)～f)の事項に代わる本人に参考となるべき情報がある場合には、当該情報
i) g)及び h)に該当する場合について情報提供できない場合には、g)及び h)に定める事項に代えて、その旨及びその理由
3. 1 項の b)によって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、法令等の定めるところによって、次に掲げる事項について、必要な措置を講じること。
j)当該第三者による相当措置の実施状況、並びに相当措置の実施に影響を及ぼすおそれの

ある当該外国の制度の有無及びその内容について、適切かつ合理的な方法による定期的な確認
k)当該第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人データの当該第三者への提供の停止
l)本人の求めを受けた場合には、情報提供することにより当該組織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を除き、遅滞なく、以下の情報を提供する
1)当該第三者による体制の整備の方法
2)当該第三者が実施する相当措置の概要
3) j)による確認の頻度及び方法
4)当該外国の名称
5)当該第三者による相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその概要
6)当該第三者による相当措置の実施に関する支障の有無及びその概要
7)前号の支障に関して、k)により講ずる措置の概要
4. 3 項の l)で、本人の求めに係る情報の全部又は一部について提供しない旨の決定をしたときは、本人に対して、遅滞なく、その旨を通知するとともに、その理由を説明すること。

（第三者提供に係る記録の作成など ）

第 32 条　個人データを第三者に提供したときは、当該個人データの提供について必要な記録を作成すること。
個人データを第三者に提供したときに、当該個人データの提供に関する記録の作成を要しない場合を、以下の場合に限定すること。
a)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
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
c)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、第 29 条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
d)法令に基づく場合
e)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
f)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
g)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

h)個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）

i)個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（個人情報取扱事業者 と第三者が共同して学術研究を行う場合に限る。）

j)第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く）。

個人データを第三者に提供したことに関する記録を作成した場合、当該記録を必要な期間、保管すること。

個人データを提供したときに、提供先が実施する第三者提供を受ける際の確認等に対し、適切に応じること。

（第三者提供を受ける際の確認など）

第 33 条　第三者から個人データの提供を受けるに際しては、必要な確認を行うこと。

第三者から個人データの提供を受けるに際して、確認を要しないのは、以下の場合に限定すること。

a)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されたとき

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を提供される場合であって、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

c)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、第 29 条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

d)法令に基づく場合

e)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

f)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

g)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

h)個人情報取扱事業者が学術研究機関等である場合であって、個人データの提供が学術研

究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）
i)個人情報取扱事業者が学術研究機関等である場合であって、個人データを学術研究目的で提供する必要があるとき（個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（個人情報取扱事業者と第三者が共同して学術研究を行う場合に限る。）
j)第三者が学術研究機関等である場合であって、第三者が個人データを学術研究目的で取り扱う必要があるとき（個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）
第三者から個人データの提供を受けるに際して確認を行ったときは、必要な記録を作成すること。
第三者から個人データの提供を受けるに際して確認を行った記録は、必要な期間、保存すること。

（個人関連情報の第三者提供の制限など）

第 34 条　1. 個人関連情報を取り扱う場合には、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内部規程として文書化すること。
2. 第三者が個人関連情報を個人データとして取得することが想定される場合、当該個人関連情報を当該第三者に提供するに際しては、第 25 条の a)～d)、又は、第 25 条の j)～l)のいずれかに該当する場合を除き、あらかじめ、次に掲げる事項又はそれと同等以上の内容の事項について、法令等の定めるところによって、確認を行うこと。
a)当該第三者が個人関連情報取扱事業者から個人関連情報の提供を受けて本人が識別される個人データとして、取得することを認める旨の当該本人の同意が得られていること。
b)外国にある第三者への提供にあっては、a)の本人の同意を得ようとする場合において、法令等で定めるところによって、以下の 1)～3)に示す事項について、あらかじめ、当該本人に提供されていること。
1)当該外国における個人情報の保護に関する制度
2)当該第三者が講ずる個人情報の保護のための措置
3)その他当該本人に参考となるべき情報
3. 個人関連情報を外国にある第三者に提供した場合には、第 31 条で定めるところによって、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講じること。
4. 法令等の定めるところによって、以下の事項について、確認の記録を作成、保管すること。
《個人関連情報の提供元の確認の記録事項》
c) a)で本人の同意が得られていることを確認した旨及び外国にある個人情報取扱事業者にあっては、b)で本人に情報の提供が行われていることを確認した旨

d)個人関連情報を提供した年月日
e)当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
f)当該個人関連情報の項目
《個人関連情報の提供先の確認の記録事項》
g) a)で本人の同意が得られている旨及び外国にある個人情報取扱事業者にあっては、b)で本人に情報の提供が行われている旨
h)当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
i)当該個人データ（個人関連情報）によって識別される本人の氏名その他当該本人を特定するに足りる事項
j)当該個人関連情報の項目

（匿名加工情報）

第 35 条　匿名加工情報の取扱いを行うか否かの方針を定めること。

匿名加工情報を取り扱う場合には、法令等の定めるところによって、以下の事項に関する適切な取扱いを行う手順を内部規程として文書化すること。

a)適切な加工方法の決定、及び加工の実施
b)加工方法等情報の安全管理措置
c)匿名加工情報を作成、及び提供することに関する公表
d)匿名加工情報の取扱いにおいて識別行為を防止する措置
e)匿名加工情報の安全管理、苦情処理、その他の適正な取扱いのための措置、及び当該措置の公表

匿名加工情報を取り扱う場合には、定めた手順に従うこと。

（仮名加工情報）

第 36 条　1. 仮名加工情報を取り扱う場合には、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内部規程として文書化すること。
2. 仮名加工情報を作成する場合には、他の情報と照合しない限り特定の個人を識別することができないようにするために必要なものとして、個人情報保護委員会規則で定める基準に従い、個人情報を加工すること。
3. 仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等を取得したときは、削除情報等の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、削除情報等の安全管理のための措置を講じること。
4. 仮名加工情報を利用する場合には、以下を実施すること。
a)利用目的をできる限り特定し、法令に基づく場合を除くほか、その目的の達成に必要な範囲内において行うこと
b)あらかじめその利用目的を公表している場合及び法令に基づく場合を除き、速やかに、

その利用目的を公表すること

c)仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合しないこと

d)電話をかけ、郵便若しくは信書便により送付し、電報を送達し、ファクシミリ装置若しくは電磁的方法を用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用しないこと

5. 仮名加工情報を提供する場合には、以下の場合を除き、仮名加工情報である個人データを第三者に提供しないこと。

e)仮名加工情報の取扱いの全部又は一部を、第 40 条と同等の措置を講じたうえで委託する場合

f)仮名加工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、既に共同して利用する場合（第 27 条の 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、以下の 1)～6)に示す事項又はそれと同等以上の内容の事項を、本人が容易に知り得る状態に置く場合）

1)共同して利用すること

2)共同して利用される仮名加工情報の項目

3)共同して利用する者の範囲

4)共同して利用する者の利用目的

5)共同して利用する仮名加工情報の管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

6)取得方法

g)合併その他の事由による事業の継承に伴って仮名加工情報を提供する場合

h)法令に基づく場合

6. 仮名加工情報の取扱いに関する苦情の適切かつ迅速な対応を行うこと。

7. 仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去すること。

第 9 章　適正管理

（正確性の確保）

第 37 条　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こと。

個人データの管理（利用する必要がなくなった場合の消去を含む。）は、定めた手順に基づいて適切に行うこと。

（安全管理措置）

第 38 条　対象事業者は、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。当該措置は個人情報が漏えい等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等のリスクに応じて必要かつ適切な内容としなければならない。
取扱いに係る規律の整備として、取得、利用、保存、提供、削除、廃棄等の段階毎に、取扱い方法、責任者・担当者及びその任務について取扱い規程を策定すること。組織的、人的及び物理的安全管理措置の内容並びに情報システムを使用して個人情報を取り扱う場合（インターネット等を通じて外部と送受信する場合を含む）は、技術的安全管理措置の内容を盛り込むことが望ましい。

1. 組織的安全管理措置

対象事業者は、組織的安全管理措置として、次に掲げる措置を講じなければならない。
（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しなければならない。
（2）個人データの取扱いに係る規律に従った運用
あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。なお、整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、システムログ又は利用実績を記録すること。
（3）個人データの取扱状況を確認する手段の整備
個人データの取扱状況を確認するための手段を整備しなければならない。
（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しなければならない。なお、漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表すること。
（5）取扱状況の把握及び安全管理措置の見直し
個人データ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。
≪参考:注意事項≫
① 安全管理措置を講じるための組織体制の整備及び役割・責任の明確化
② 安全管理措置を定める規程等の整備と規程等に従った運用
③ 個人情報の取扱状況を一覧できる手段の整備
④ 安全管理措置の評価、見直し及び改善
⑤ 事故又は違反への対処

2. 人的安全管理措置

対象事業者は、人的安全管理措置として、次に掲げる措置を講じなければならない。また、対象事業者は、従業者に個人データを取り扱わせるに当たっては、個人情報保護法第24条に基づき従業者に対する監督をしなければならない。
従業者には、個人データ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わなければならない。

≪参考:注意事項≫

① 雇用契約時及び委託契約時における非開示契約の締結
② 従業者に対する教育・訓練の実施

3. 物理的安全管理措置

対象事業者は、物理的安全管理措置として、次に掲げる措置を講じなければならない。

（1）個人データ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。）及びその他の個人データ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わなければならない。

（2）機器及び電子媒体等の盗難等の防止

個人データを取り扱う機器、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、適切な管理を行わなければならない。

（3）電子媒体等を持ち運ぶ場合の漏えい等の防止

個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。なお、「持ち運ぶ」とは、個人データを管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、事業所内の移動等であっても、個人データの紛失・盗難等に留意すること。

（4）個人データの削除及び機器、電子媒体等の廃棄

個人データ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、復元不可能な手段で行わなければならない。また、個人データを削除した場合、又は個人データが記録された機器、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や、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認すること。

≪参考:注意事項≫

① 個人情報を加工、保管するセキュリティエリア及び機器の特定
② 建物及びセキュリティエリア等、場所の特性に応じた合理的な入退館（室）管理
オフィス、部屋及び施設のセキュリティ
③ 個人情報を保管する機器、媒体、個人情報を記載した出力用紙等の盗難に対する十分

な対策
④ 個人情報を加工・保管するセキュリティエリア及び機器の自然災害等からの物理的な保護
⑤　セキュリティを保つべき領域ごとの管理
⑥ 受渡場所の管理
⑦ 個人情報を保管する機器、媒体、個人情報を記載した出力用紙等の盗難に対する十分な対策
・機器及び電子媒体等の盗難等の防止
・電子媒体等を持ち運ぶ場合の漏えい等の防止
・個人データの削除及び機器、電子媒体等の廃棄

4.　技術的安全管理措置

対象事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。

（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。

（2）アクセス者の識別と認証

個人データ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。

（3）外部からの不正アクセス等の防止

個人データ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ェ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。

（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データ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。

≪参考:注意事項≫

① 個人情報へのアクセスにおける制限と管理
③　個人情報へのアクセスの記録（アクセスログの一定期間の保管）
③ 個人情報を取り扱う情報システムに対する不正ソフトウェア対策（ウィルス対策ソフトウェアの導入、いわゆるセキュリティパッチの適用等）
④ 個人情報を取り扱うソフトウェアに対する脆弱性対策（脆弱性診断ツールの適用等）
⑥ 個人情報の移送・通信時の暗号化等の漏えい防止対策
⑥ 個人情報を取り扱う情報システムの異常監視

（従業者の監督）

第 39 条　対象事業者は、その従業者に個人情報を取り扱わせるに当たっては、当該個人情報の安全管理が図られるよう、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。

（委託先の監督）

第 40 条　個人データの取扱いの全部又は一部を委託する場合、十分な個人データの保護水準を満たしている者を選定するための委託先選定基準を確立し、委託先を選定すること。

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こと。

次に示す事項が盛り込まれた契約を締結すること。

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

全ての委託先を漏れなく特定すること。

委託契約書は当該個人データの保有期間にわたって保存すること。

委託契約に基づき、委託先を適切に監督すること。

委託先選定基準には、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すること。

第 10 章　個人情報に関する本人の権利

（個人情報に関する権利）

第 41 条　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た場合、第 44 条～第 47 条の規定によって、遅滞なくこれに応じること。

第 32 条及び第 33 条で作成した第三者提供記録に関して、本人から開示等の請求等を受けた場合、第 45 条の規定によって、遅滞なくこれに応じること。

保有個人データ又は第三者提供記録に当たらないものとして、次に掲げるいずれかに限定すること。

a)当該個人データ又は当該第三者提供記録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)当該個人データ又は当該第三者提供記録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)当該個人データ又は当該第三者提供記録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)当該個人データ又は当該第三者提供記録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及び秩序維持に支障が及ぶおそれのあるもの

（開示等の請求等に応じる手続）

第 42 条　保有個人データ又は第三者提供記録の開示等の請求等に応じる手続として、次の事項を文書化すること。
a)開示等の請求等の申出先
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）第 44 条又は 第 45 条による手数料(定めた場合に限る。）の徴収方法
保有個人データ又は第三者提供記録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こと。
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、その額を定めること。

（保有個人データ又は第三者提供記録に関する事項の周知など）

第 43 条　保有個人データ又は第三者提供記録に関して、次の事項を本人の知り得る状態（本人の請求などに応じて遅滞なく回答する場合を含む。）に置くこと。
a)組織の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
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)全ての保有個人データの利用目的(第 26 条の 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出先
e)当該組織が認定個人情報保護団体（東京グラフィックサービス工業会）正会員であるので、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：(公社）東京グラフィックサービス工業会が認定個人情報保護団体である旨を明示すること
f）第 42 条によって定めた手続
g)保有個人データの安全管理のために講じた措置（本人の知り得る状態に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）

（保有個人データの利用目的の通知）

第 44 条　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、遅滞なくこれに応じること。
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であって、利用目的の通知を必要としないのは以下の場合に限定すること。
・第 26 条の a)～c)のいずれかに該当する場合
・第 43 条の 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
前 2 項の各事由のいずれかに該当する場合、本人に遅滞なくその旨を通知するとともに、理由を説明すること。

（保有個人データ又は第三者提供記録の開示）

第 45 条　1. 本人から、当該本人が識別される保有個人データ又は第三者提供記録の開示の請求を受けた場合、法令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、電磁的記録の提供も含めて当該本人が指定した方法（当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法）によって開示すること。

2. 本人から、当該本人が識別される保有個人データ又は第三者提供記録の開示の請求を受けた場合であって、全部又は一部の開示を必要としないのは以下の場合に限定すること。
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)当該組織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

3.　1.項の当該本人が指定した方法について、当該方法による開示が困難であるとして、書面での交付とした場合、もしくは、前 2. 項の各事由のいずれかに該当する場合、本人に遅滞なくその旨を通知するとともに、理由を説明すること。

（保有個人データの訂正、追加又は削除）

第 46 条　本人から、当該本人が識別される保有個人データの訂正等（訂正、追加又は削除）の請求を受けた場合、法令の規定により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こと。
本人から保有個人データの訂正等の請求を受けて訂正等を行った場合は、その旨及びその内容を本人に遅滞なく通知すること。
本人から保有個人データの訂正等の請求を受けたが応じなかった場合、その旨及びその理由を本人に遅滞なく通知すること。

（保有個人データの利用又は提供の拒否権）

第 47 条　本人から当該本人が識別される保有個人データの利用停止等（利用の停止、消去又は第三者への提供の停止）の請求に応じること。

本人からの当該本人が識別される保有個人データの利用停止等の請求に応じた場合、遅滞なくその旨を本人に通知すること。
本人からの当該本人が識別される保有個人データの利用停止等の請求に応じなかった場合は、第 45 条の a)～c)に該当する場合に限定すること。
第 45 条の a)～c)のいずれかに該当する場合、本人に遅滞なくその旨通知するとともに、理由を説明すること。

第 11 章 苦情及び相談への対応

（苦情及び相談への対応）

第 48 条 対象事業者は，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が内部規程として文書化すること。 苦情及び相談への対応を実施すること。
苦情の申立て先は、本人にとって明確にすること。 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ための体制を整備すること。
認定個人情報保護団体（公社）東京グラフィックサービス工業会の正会員は、当会を苦情解決の申し出先として明示する。
苦情申し立て先：（公社）東京グラフィックサービス工業会
〒103-0001 東京都中央区日本橋小伝馬町 7-16 電話 03-3667-3771 FAX03-3249-0377

第 12 章 罰則、勧告

（罰則）

第 49 条 対象事業者は、本指針第 16 条 o)項により策定した内部規程に違反した従業者に対して就業規則に基づき懲戒を行わなければならない。

（勧告）

第 50 条 対象事業者は、法令、本指針にそぐわない取扱いがあった場合、当会個人情報保護委員会において協議し、事案の公表、指導・勧告を行う。その方法は、当会個人情報保護委員会において決定する。

第 13 章 改廃

（改廃）

第 51 条 本指針の改廃は、当会個人情報保護委員会において起案し、当会理事会の承認を得るものとする。