

個人情報保護規程

第1章 総則

(目的)

- 第1条 本規程は、特定非営利活動法人育て上げネット（以下、「当法人」という。）の保有する。個人情報の適切な管理のために必要な事項を定めることにより、この法人の役職員等が遵守すべき事項を定め、当法人の業務の適正かつ円滑な運営を図るとともに、個人の権利利益を保護・管理することを目的とする。
- 2 当法人における個人情報の取扱いに関しては、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）その他関係法令の定めるもののほか、情報セキュリティ・管理規程（以下「管理規程」という。）及び本規程に定めるところによる。

(定義)

- 第2条 本規程において、次の各号に掲げる用語の定義は、次のとおりとする。なお、本規程に定義の定めのない用語は、法その他の関係法令の定めに従うものとする。

① 個人情報

「個人情報」とは個人情報保護法第2条第1項に規定する生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）及び個人識別符号が含まれるものをいう。

② 要配慮個人情報

「要配慮個人情報」とは、個人情報保護法第2条第3項に規定する個人情報であって、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法令で定める記述等が含まれるものをいう。

③ 個人番号

「個人番号」とは、行政手続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（以下「番号法」という。）第7条第1項又は第2項の規定により、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

④ 特定個人情報

「特定個人情報」とは、個人番号をその内容に含む個人情報をいう。

⑤ 特定個人情報等

「特定個人情報等」とは、特定個人情報及び個人番号をいう。

⑥ 保有個人情報

「保有個人情報」とは当法人の職員（⑧のとおり。以下同じ。）が職務上作成し、又は取得した個人情報であって、当法人の職員が組織的に利用するものとして、当法人が保有しているものをいう。

⑦ 保有個人情報データベース等

「保有個人情報データベース等」とは、個人情報を含む情報の集合で、次に掲げるものをいう。

ア 一定の事務の目的を達成するために特定の保有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。

イ ア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であって、目次、索引その他検索を容易にするためのものを有するものをいう。

⑧ 匿名加工情報

特定の個人を識別することができないよう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して特定の個人を再識別することができないようにしたものをいう。

⑨ 職員

理事、役員、職員、フェロー、インターン、支援員・ボランティア等名称や雇用条件にかかわらず、当法人の業務及び活動にかかわるすべての者をいう。

第2章 個人情報保護体制

（個人情報保護体制）

第3条 個人情報保護体制は、当法人の上位の「管理規程」に順ずる。

（情報セキュリティ責任者）

第4条 当法人に、情報セキュリティ責任者1名を置き、事務局長をもって充てる。

2 情報セキュリティ責任者は、当法人における保有個人情報の管理に関する事務を総括する。

（情報セキュリティ管理者）

第5条 当法人に情報セキュリティ管理者1名を置き、情報セキュリティ担当執行役員をもって充てる。

- 2 情報セキュリティ責任者の指揮、監督の下で情報セキュリティ事業所責任者と連携を取り、保有個人情報保護管理の維持および充実に努める。

(情報セキュリティ事業(所)責任者)

第6条 保有個人情報を取り扱う事業所に情報セキュリティ事業(所)責任者1名を置き、当該事業所のプロジェクトマネージャーをもって充てる。

情報セキュリティ事業(所)責任者は、事業所における保有個人情報を適切に管理する。

- 2 情報セキュリティ事業(所)責任者は、自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について、点検を行いその結果を点検・監査責任者に報告する。
- 3 点検・監査責任者は、情報セキュリティ事業所責任者からの報告を検証し必要に応じて情報セキュリティ委員会に報告する。

(点検・監査責任者)

第7条 当法人に点検・監査責任者1名を置き、プロジェクトサポートオフィス管理担当プロジェクトマネージャーをもって充てる。

- 2 点検・監査責任者は、年1回定期的に全事業所の保有個人情報の管理の状況について点検・監査を行い、また必要に応じて点検・監査を行う。
- 3 前項の点検・監査結果を情報セキュリティ委員会に報告する。
- 4 点検・監査責任者は、点検・監査の実施方法、内容、時期など監査実施計画書を作成する。

(教育責任者)

第8条 当法人に教育責任者1名を置き、人事担当執行役員をもって充てる。

- 2 教育責任者、情報セキュリティに関する教育計画を事業年度ごとに立案する。
- 3 前項の教育計画には事業(所)で行う研修を含む。

(インシデント対応責任者)

第9条 当法人にインシデント対応1名を置き、プロジェクトサポートオフィス管理担当プロジェクトマネージャーをもって充てる。

- 2 インシデント対応責任者は保有個人情報の漏えい・流出、改ざん・消失・データの破壊等の事案・事故発生時の対応に責任を負う。
- 3 上記に該当する事案・事故発生時には情報セキュリティ管理者、情報セキュリティ事業(所)責任者と協力の上で、再発防止策を含め必要な措置を講ずる。

(重要事項の決定等)

第10条 保有個人情報の管理に係る重要事項の審議は情報セキュリティ委員会にて行い、最

終的な決定及び変更は経営ボード会議にて行う。

- 2 前項の決定及び変更の通達等は情報セキュリティ責任者が情報セキュリティ委員会を通じて行う。

第3章 保有個人情報の取扱い

(職員の責務)

- 第11条 本規程は、全ての職員に適用する。職員は、法の趣旨に則り、関連する法令、管理規程及び本規程等の定め及び情報セキュリティ事業(所)責任者の指示に従い、保有個人情報を取り扱う。
- 2 職員は、その業務に関して知り得た個人情報の存否及び内容をみだりに他人に知らせ、又は不当な目的に利用しない。
 - 3 情報セキュリティ事業(所)責任者は、本規程の順守を確保するために必要な措置を講ずる。

(利用目的の特定)

- 第12条 個人情報の保有に当たっては、業務を遂行するため必要な場合に限り、かつ、その利用の目的（以下、「利用目的」という。）をできる限り特定する。
- 2 利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行わない。

(利用目的の通知等)

- 第13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。
- 2 前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示する。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。
 - 3 利用目的を変更する場合は、変更する利用目的について、事前に本人に通知し、同意を得る。
 - 4 前三項の規定は、次に掲げる場合については、適用しない。
 - (1) 利用目的を本人に通知し、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し、又は公表することにより当該個人情報取扱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り当該事務の遂行に支障を及ぼすおそれがあるとき

(適正な取得)

第14条 職員は、偽りその他不正の手段により個人情報を取得しない。また、事前に本人の同意を得ないで取得することができない。

(個人情報の保有の制限等)

第15条 職員は、個人情報を保有するに当たっては、業務を遂行するため必要な場合に限る。

- 2 職員は、前項の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を保有しない。
- 3 職員が利用目的を変更するに当たっては、変更前の利用目的と関連性を有すると情報セキュリティ事業(所)責任者に認められた範囲を超えて行わない。

(正確性の確保)

第16条 職員は、利用目的の達成に必要な範囲内で、保有個人情報が過去又は現在の実事と合致するよう努める。

- 2 職員は、保有個人情報の内容に誤り等を発見した場合には、情報セキュリティ事業所責任者の指示に従い、訂正等を行う。

(利用及び提供の制限)

第17条 職員は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は第三者に提供してはならない。但し、やむを得ず利用目的外に使用する場合は情報セキュリティ事業(所)責任者の許可及び本人の同意を得て行う。

- 2 情報セキュリティ管理者は、情報セキュリティ事業(所)責任者との協議の上、真にやむを得ないと判断した場合にのみ提供あるいは共有を許可する。
- 3 提供あるいは共有先は、社会通念上相当な事業活動を営む者であること。および個人情報の保護に関し、この規程と同様の規程を有し、かつその適正な運用及び実施をしている者であること。
- 4 保有個人情報を提供あるいは共有するときは、原則として、提供あるいは共有先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わす。
- 5 保有個人情報を提供あるいは共有する場合には、必要な安全確保の措置を要求し、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認して、その結果を記録するとともに改善要求等の措置を講ずること。

(業務の委託等)

第18条 保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないように、管理規程に基づき必要な措置を講ずること。

2 前項により外部に委託する場合には、当該契約書に、次に掲げる事項を明記するとともに、委託先における責任者等の管理体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認すること。

- (1) 個人情報に関する秘密保持等の義務
- (2) 再委託の制限又は条件に関する事項
- (3) 個人情報の複製等の制限に関する事項
- (4) 個人情報の漏えい等の事案の発生時における対応及び責任分担に関する事項
- (5) セキュリティ対策の実施状況に関する監査の方法とその権限
- (6) 委託終了時における個人情報の消去、廃棄及び媒体の返却に関する事項
- (7) 契約内容が遵守されない、もしくは違反した場合にける契約解除その他必要な措置
- (8) 事故発生時の報告方法

(取扱い制限)

第19条 情報セキュリティ事業(所)責任者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報を取り扱う権限を有する者をその利用目的を達成するために必要最小限の職員に限る。

2 取扱い権限を有しない職員は、保有個人情報を取り取り扱わない。

3 職員は、取扱い権限を有する場合であっても、業務上の目的以外の目的で保有個人情報を取り扱わない。

(複製等の制限)

第20条 職員は、業務上の目的で保有個人情報を取り扱う場合であっても、次に掲げる行為については、原則として禁止する。但し、やむを得ない場合は情報セキュリティ事業(所)責任者の指示に従って行う。

- (1) 保有個人情報の複製
- (2) 保有個人情報の送信
- (3) 保有個人情報が記録されている媒体の外部への送付又は持出し
- (4) その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

(媒体の管理等)

第21条 職員は、情報セキュリティ事業(所)責任者の指示に従い、保有個人情報記録されている媒体を定められた場所に保管し、施錠等を行うこと。

- 2 職員は、保有個人情報又は保有個人情報が記録されている媒体(端末及びサーバに内蔵されているものを含む)が不要となった場合には、情報セキュリティ事業所責任者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により、当該情報の消去又は当該媒体の廃棄を行うこと。

(消去の義務)

第22条 職員は、保有個人情報を利用する必要が無くなったときは、遅滞なく消去すること。ただし、匿名加工情報については削除の対象としない。

第4章 情報システムにおける安全の確保等

(情報システムにおける安全の確保)

第23条 個人情報の情報システムにおける取扱いの安全確保・管理のための措置については、管理規程において別途定める。

- 2 情報セキュリティ管理者は、必要に応じて個人情報の安全管理のため、個人情報不正アクセス、漏洩、滅失又は既存の防止に努め、個人情報の取扱いを職員に遵守させる。

(点検・監査の実施)

第24条 事業(所)の個人情報の点検・監査は、別途定める「情報セキュリティ点検・監査規程」及び監査実施計画書に基づき点検・監査を行う。

(教育・研修の実施)

第25条 管理規程3.4に基づき、情報セキュリティ委員会は全職員を対象に、年度ごとに最低1回は個人情報の扱いに関する教育・研修を実施する。

- 2 教育・研修の実施結果は情報セキュリティ事業(所)責任者から教育責任者へ報告する。
- 3 個人情報の扱いに関する研修は1とは別に、入職時にも実施する。

第5章 開示等請求への対応等

(開示対象等)

第26条 個人情報の開示等の対象は、保有個人情報のうち、対象者本人の申告書面、職員の聞き取り等によって作成した書面及び保有個人データとする。但し、法第25条各号に該当する場合には、開示等を行わないことができる。

(開示方法・訂正等)

第27条 本人またはその代理人が個人情報の開示等を請求するときは、別紙「個人情報開示等請求書」を本部個人情報担当宛てに提出する。

- 2 開示の結果、誤った情報があり、訂正、追加又は削除を求められた場合は、原則として合理的な期間内にこれに応じるとともに、訂正、追加又は削除を行った場合は、当該保有個人情報の受領者に対して通知を行う。

第6章 問題への対応等

(安全確保上の問題への対応)

第28条 保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報を管理する情報セキュリティ事業所責任者に報告する。

- 2 情報セキュリティ事業(所)責任者は、被害の拡大防止又は復旧等のために必要な措置を講ずるとともに、事案の発生した経緯、被害状況等について調査し、速やかに情報セキュリティ管理者及びインシデント対応責任者に報告する。報告を受けたインシデント対応責任者は事実確認を行った上で情報セキュリティ責任者に報告する。
- 3 情報セキュリティ責任者は、前項の報告を受けたときは事案の内容等に応じて当該事案の内容、経緯、被害状況等について理事長に速やかに報告する。
- 4 情報セキュリティ責任者は事業(所)管理者及び点検・監査責任者と協力の上で、事案の発生した原因を分析し、再発防止のために必要な措置を講じる。
- 5 上記の実際の運用方法については別途「危機管理マニュアル」に定める。

(安全確保上の問題の報告・公表)

第29条 理事長は、前条の事案が発生したときは、事案の内容、影響等に応じて情報セキュリティ責任者の助言のもとに事実関係及び再発防止策を公表し、当該事案に係る本人への対応等の措置を講ずる。

- 2 理事長は、情報セキュリティ責任者の助言のもとにかかる事案について法令に基づく報告及び当該事案当事者本人への通知を行う。

(苦情処理)

第30条 情報セキュリティ事業(所)責任者は、個人情報の扱いに関する苦情又は意見があった

ときは、速やかにインシデント対応責任者に報告をし、適正かつ迅速に処理するよう努める。

- 2 インシデント対応責任者は事案の内容、対応及び処理について必要に応じて情報セキュリティ委員会に報告する。

(罰則)

第31条 本規程に違反した者は、「懲戒規程」に基づき処罰する。

(改廃)

第32条 本規程は、経営ボード会議の決議により、改廃することができる。

付 則

本規程は、平成26年8月1日から施行する。

平成26年10月1日 改定

平成28年11月1日 改定

平成31年4月1日 改定

令和5年7月1日 改定

令和5年9月22日 改定

令和6年11月30日 改定