

個人情報保護規則

平成27年4月1日

規則第27号

改正 平成28年1月1日規則第33号

平成28年4月1日規則第50号

平成29年6月30日規則第89号

平成30年10月10日規則第106号

令和2年3月27日規則第33号

令和4年3月24日規則第18号

目次

第1章 総則

第1節 通則(第1条～第4条)

第2節 保有個人情報等の管理体制等(第5条～第8条)

第2章 個人情報等の取扱い

第1節 個人情報等の取得、利用等(第9条～第18条の4)

第2節 保有個人情報等の取扱い(第19条～第23条の4)

第3節 情報システムにおける安全の確保等(第24条～第38条の2)

第4節 情報システム室等の安全管理(第39条・第40条)

第3章 個人情報ファイル簿の作成及び公表等(第41条～第44条)

第4章 事案の報告及び再発防止措置(第44条の2～第50条)

第5章 点検及び監査等(第51条～第53条)

第6章 行政機関等匿名加工情報の提供等(第53条の2)

第7章 補則(第54条・第55条)

附則

第1章 総則

第1節 通則

(目的)

第1条 この規則は、国立研究開発法人日本医療研究開発機構(以下「機構」という。)の保有する個人情報について、その適切な管理に必要な事項を定めることにより、機構の業務の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

(定義)

第2条 この規則において、用語の定義は、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。)第2条、第16条及び第60条並びに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(平成25年法律第27号。以下「番号法」という。)第2条の定めるところによるほか、次の各号に定めるところによる。

- (1) 部室 組織規程(平成27年規程第4号)第10条に定める部室をいう。
- (2) 課 組織規程第11条から第17条に定める課をいう。
- (3) 役職員等 機構の役員、職員及びこの規則を遵守すべきものとして総括個人情報保護管理者が認めた者をいう。
- (4) 海外事務所 組織規程第15条の3第2号に定める海外事務所をいう。
- (5) 海外事務所の長 海外事務所の主たる担当地域等に関する達(平成28年達第23号)第4条に定める者をいう。

(適用の範囲)

第3条 機構の保有する個人情報、特定個人情報、個人情報ファイル及び特定個人情報ファイルの取扱いは、法、番号法及びこの規則の定めるところによる。

(役職員等の責務)

第4条 役職員等は、法及び番号法の趣旨に則り、関連する法令及び例規等の定め並びに総括個人情報保護管理者、副総括個人情報保護管理者及び個人情報保護管理者の指示に従い、保有個人情報及び保有特定個人情報(以下「保有個人情報等」という。)を取り扱わなければならない。

第2節 保有個人情報等の管理体制等

(総括個人情報保護管理者等)

第5条 機構に、総括個人情報保護管理者1名を置き、理事をもって充てる。

- 2 副総括個人情報保護管理者1名を置き、総務部長をもって充てる。また、副総括個人情報保護管理者補佐1名を置き、総務課長をもって充てる。
- 3 部室に主任個人情報保護管理者1名を置き、部室の長をもって充てる。
- 4 課及び海外事務所に、個人情報保護管理者1名を置き、当該課及び海外事務所の長をもって充てる。
- 5 課及び海外事務所に個人情報保護担当者1名を置き、個人情報保護管理者が指名した総括管理を担当する職員をもって充てる。個人情報保護管理者は、個人情報保護担当者を指名後、速やかに副総括個人情報保護管理者にその氏名、役職等を報告しなければならない。
- 6 機構に、個人情報監査責任者を置き、監査室長をもって充てる。

(総括個人情報保護管理者等の任務)

第6条 総括個人情報保護管理者は、機構における保有個人情報等の管理に関する事務を総括する。

2 副総括個人情報保護管理者は、総括個人情報保護管理者の命を受けて、総括個人情報保護管理者が行う事務を補佐する。また、副総括個人情報保護管理者補佐は、副総括個人情報保護管理者が行う事務を補佐する。

3 主任個人情報保護管理者は、当該部室における個人情報の管理に関する事務を総括する。

4 個人情報保護管理者は、当該課及び海外事務所における保有個人情報等を適切な管理を確保する任に当たる。保有個人情報等を情報システムで取り扱う場合、当該情報システムの管理者と連携して、その任に当たる。

5 個人情報保護担当者は、個人情報保護管理者の命を受けて、個人情報保護管理者を補佐し、当該課及び海外事務所における保有個人情報等の管理に関する事務を担当する。

6 個人情報監査責任者は、保有個人情報等の管理の状況について監査する任に当たる。

7 個人情報保護管理者は、個人番号及び特定個人情報(以下「特定個人情報等」という。)を取扱う職員(以下「事務取扱担当者」という。)を指定し、その役割及び各事務取扱担当者が取扱う特定個人情報等の範囲を指定する。

(保有個人情報等の適切な管理のための委員会)

第7条 総括個人情報保護管理者は、機構の保有個人情報等の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるときは、関係役職員等を構成員とする委員会を設け、定期に又は随時に開催するものとする。

(教育研修)

第8条 総括個人情報保護管理者は、保有個人情報等の取扱いに従事する役職員等に対し、保有個人情報等の取扱いについて理解を深め、個人情報及び特定個人情報(以下「個人情報等」という。)の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。

2 総括個人情報保護管理者は、保有個人情報等を取扱う情報システムの管理に関する事務に従事する役職員等に対し、保有個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

3 総括個人情報保護管理者は、個人情報保護管理者及び個人情報保護担当者に対し、課及び海外事務所の現場における個人情報等の適切な管理のための教育研修を実施する。

4 個人情報保護管理者は、当該課及び海外事務所の役職員等に対し、保有個人情報等の適

切な管理のために、総括個人情報保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講じなければならない。

第2章 個人情報等の取扱い

第1節 個人情報等の取得、利用等

(利用目的の特定)

第9条 役職員等は、個人情報を取り扱うに当たっては、法令の定める業務を遂行するため必要な場合に限り、かつ、その利用の目的をできる限り特定しなければならない。

2 役職員等は、前項の規定により特定された利用の目的(以下「利用目的」という。)の達成に必要な範囲を超えて、個人情報等を保有してはならない。

3 役職員等は、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ってはならない。

(利用目的による制限)

第10条 役職員等は、あらかじめ本人の同意を得ないで、前条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、個人情報を取り扱ってはならない。

2 役職員等は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3 前2項の規定は、法第18条第3項に掲げる場合については、適用しない。

(不適正な利用の禁止)

第10条の2 役職員等は、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方法により個人情報を利用してはならない。

(適正な取得)

第11条 役職員等は、偽りその他不正の手段により個人情報等を取得してはならない。

2 役職員等は、法第20条第2項に掲げる場合を除くほか、あらかじめ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。

3 事務取扱担当者は、特定個人情報取扱事務を処理するため必要があるときは、本人に対して個人番号(当該本人と同一の世帯に属する者の個人番号を含む。)の提供を求めることができるものとする。

4 事務取扱担当者は前項により本人より個人番号の提供を受けるときは、法令の定めるところにより本人確認を行わなければならない。

5 事務取扱担当者は第3項の場合を除き、本人に個人番号の提供を求めてはならない。

(取得に際しての利用目的の通知等)

第11条の2 役職員等は、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、又は公表しなければならない。

2 役職員等は、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(電磁的記録を含む。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しなければならない。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 役職員等は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

4 前3項の規定は、法第21条第4項第1号から第4号までに掲げる場合については、適用しない。

(データ内容の正確性の確保等)

第12条 役職員等は、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内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう行わなければならない。

(安全管理措置)

第13条 役職員等は、この規則に定めるところにより、保有個人情報の漏えい、滅失又は毀損の防止その他の保有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。

(職員の監督)

第13条の2 総括個人情報保護管理者は、職員に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該職員に対する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13条の3 役職員等は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された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。

(第三者提供の制限)

第14条 役職員等は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

(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) 当該第三者が学術研究機関等である場合であって、当該第三者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。)

2 役職員等は、第三者に提供される個人データについて、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、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くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。ただし、第三者に提供される個人データが要配慮個人情報又は第11条第1項の規定に違反して取得されたもの若しくは他の個人情報取扱事業者からこの項本文の規定により提供されたもの(その全部又は一部を複製し、又は加工したものを含む。)である場合は、この限りでない。

(1) 機構の名称、住所及び理事長の氏名

(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) 第三者に提供される個人データの取得の方法

(5) 第三者への提供の方法

(6) 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。

(7) 本人の求めを受け付ける方法

(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

3 個人情報取扱事業者は、前項第1号に掲げる事項に変更があったとき又は同項の規定による個人データの提供をやめたときは遅滞なく、同項第3号から第5号まで、第7号又は第8号に掲げる事項を変更しようとするときはあらかじめ、その旨について、個人情報保護委員会規則で定めるところにより、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出なければならない。

4 次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。

(1) 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

(2) 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

(3) 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並びに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及び住所並びに法人にあっては、その代表者の氏名について、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。

5 個人情報取扱事業者は、前項第3号に規定する個人データの管理について責任を有する者の氏名、名称若しくは住所又は法人にあっては、その代表者の氏名に変更があったときは遅滞なく、同号に規定する利用する者の利用目的又は当該責任を有する者を変更しようとするときはあらかじめ、その旨について、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

(特定個人情報の提供の制限)

第15条 役職員等は、番号法で限定的に明記された場合を除き、特定個人情報を提供してはならない。

(特定個人情報の利用の制限)

第16条 事務取扱担当者は番号法に定められた事務以外のために特定個人情報を自ら利用してはならない。

2 前項の規定にかかわらず、事務取扱担当者は、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、本人の同意があり、又は本人の同意を得ることが困難であると認められるときで、かつ、当該特定個人情報を利用目的以外の目的のために自ら利用する

ことによって、本人又は第三者の権利利益を不当に侵害するおそれがないと認められるときは、利用目的以外の目的のために特定個人情報を自ら利用することができる。

3 前項の規定は、特定個人情報の利用を制限する法令の適用を妨げるものではない。

(外国にある第三者への提供の制限)

第17条 役職員等は、外国(本邦の域外にある国又は地域をいう。以下この条及び第18条の3第1項第2号において同じ。)(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と認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条及び同号において同じ。)にある第三者(個人データの取扱いについてこの節の規定により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(第3項において「相当措置」という。)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を除く。以下この項及び次項並びに同号において同じ。)に個人データを提供する場合には、法第14条第1項各号に掲げる場合を除くほか、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。この場合においては、同条の規定は、適用しない。

2 役職員等は、前項の規定により本人の同意を得ようとする場合には、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、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない。

3 個人情報取扱事業者は、個人データを外国にある第三者(第1項に規定する体制を整備している者に限る。)に提供した場合には、個人情報保護委員会規則で定めるところにより、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ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない。

(第三者提供に係る記録の作成等)

第18条 役職員等は、個人データを第三者(法第16条第2項各号に掲げる者を除く。以下この条及び次条(第18条の3第3項において読み替えて準用する場合を含む。)において同じ。)に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。ただし、当該個人データの提供が第14条第1項各号又は第4項各号のいずれか(第14条第1項の規定による個人データの提供に

あつては、第14条第1項各号のいずれか)に該当する場合は、この限りでない。

- 2 役職員等は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

(第三者提供を受ける際の確認等)

第18条の2 役職員等は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が法第14条第1項各号又は第4項各号のいずれかに該当する場合は、この限りでない。

- (1) 当該第三者の氏名又は名称及び住所並びに法人にあつては、その代表者の氏名
- (2) 当該第三者による当該個人データの取得の経緯

- 2 前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない。

- 3 役職員等は、第1項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。

- 4 役職員等は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

(個人関連情報の第三者提供の制限等)

第18条の3 役職員等は、第三者が個人関連情報(個人関連情報データベース等を構成するものに限る。この節において同じ。)を個人データとして取得することが想定されるときは、第14条第1項各号に掲げる場合を除くほか、次に掲げる事項について、あらかじめ個人情報保護委員会規則で定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。

- (1) 当該第三者が役職員等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。
- (2) 外国にある第三者への提供にあつては、前号の本人の同意を得ようとする場合において、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、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報が当該本人に提供されていること。

- 2 第17条第3項の規定は、前項の規定により役職員等が個人関連情報を提供する場合について準用する。この場合において、第17条第3項中「講ずるとともに、本人の求めに

応じて当該必要な措置に関する情報を当該本人に提供し」とあるのは、「講じ」と読み替えるものとする。

- 3 前条第2項から第4項までの規定は、第1項の規定により役職員等が確認する場合について準用する。この場合において、同条第3項中「の提供を受けた」とあるのは、「を提供した」と読み替えるものとする。

(苦情の処理)

第18条の4 役職員等は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

- 2 個人情報保護管理者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

第2節 保有個人情報等の取扱い

(アクセス制限)

第19条 個人情報保護管理者は、保有個人情報等の秘匿性等その内容(特定の個人の識別の容易性の程度、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを考慮する。以下同じ。)に応じて、当該保有個人情報等にアクセスする役職員等の範囲と権限の内容をその利用目的を達成するために必要最小限の範囲に限らなければならない。

- 2 アクセス権限を有しない役職員等は、保有個人情報等にアクセスしてはならない。
- 3 役職員等は、アクセス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等にアクセスしてはならない。

(複製等の制限)

第20条 役職員等が、業務上の目的で保有個人情報等を取扱う場合であっても、個人情報保護管理者は次に掲げる行為については、当該保有個人情報等の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、役職員等は個人情報保護管理者の指示に従い行うものとする。

- (1) 保有個人情報等の複製
- (2) 保有個人情報等の送信
- (3) 保有個人情報等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等の適切な管理に支障を及ぼすおそれのある行為

(誤りの訂正等)

第21条 役職員等は、保有個人情報等の内容に誤り等を発見した場合には、当該誤り等が

明らかに軽微であると認められる場合を除き、個人情報保護管理者の指示に従い、訂正等を行わなければならない。

(媒体の管理等)

第22条 役職員等は、個人情報保護管理者の指示に従い、保有個人情報等が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは耐火金庫への保管、施錠等を行わなければならない。また、保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、原則として、パスワード等(パスワード、ICカード、生体情報等をいう。以下同じ。)を使用して権限を識別する機能(以下「認証機能」という。)を設定する等のアクセス制御のために必要な措置を講じなければならない。

(誤送付等の防止)

第22条の2 役職員等は、保有個人情報を含む電磁的記録又は媒体の誤送信・誤送付、誤交付、又はウェブサイト等への誤掲載を防止するため、個別の事務・事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認やチェックリストの活用等の必要な措置を講ずる。

(廃棄等)

第23条 役職員等は、保有個人情報等又は保有個人情報等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、個人情報保護管理者の指示に従い、当該保有個人情報等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わなければならない。特に、保有個人情報の消去や保有個人情報が記録されている媒体の廃棄を委託する場合(二以上の段階にわたる委託を含む。)には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取るなど、委託先において消去及び廃棄が確実に行われていることを確認しなければならない。

(外的環境の把握)

第23条の2 役職員等は、保有個人情報が、外国において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有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。

(個人情報の取扱いに係る業務を外部に委託する場合の措置)

第23条の3 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、必要な措置を講ずる。また、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及び業務従事者の管

理体制及び実施体制、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しなければならない。

(1) 個人情報に関する秘密保持、目的外利用の禁止等の義務

(2) 再委託(再委託先が委託先の子会社(会社法(平成17年法律第86号)第2条第1項第3号に規定する子会社をいう。)である場合も含む。本号及び同条同項第4号において同じ。)(委託先との契約書に、再委託に際して再委託先に求める事項は、再委託先が子会社である場合も、同様に求めるべきことを明記すること。)の制限又は事前承認等再委託に係る条件に関する事項

(3) 個人情報の複製等の制限に関する事項

(4) 個人情報の安全管理措置に関する事項

(5) 個人情報の漏えい等の事案の発生時における対応に関する事項

(6) 委託終了時における個人情報の消去及び媒体の返却に関する事項

(7) 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項

(8) 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項(再委託先の監査等に関する事項を含む。)

2 役職員等は、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、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。

3 役職員等は、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、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認しなければならない。

4 役職員等は、委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に前1号の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前3号の措置を実施しなければならない。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

5 役職員等は、保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記しなければならない。

6 役職員等は、保有個人情報を提供又は業務委託する場合には、漏えい等による被害発生

のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講じなければならない。

(派遣労働者の派遣を受ける場合の措置)

第23条の4 個人情報保護管理者は、保有個人情報等の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記しなければならない。

第3節 情報システムにおける安全の確保等

(アクセス制御)

第24条 個人情報保護管理者は、保有個人情報等(情報システムで取扱うものに限る。)の秘匿性等その内容に応じて、パスワード等(パスワード、ICカード、生体情報等をいう。以下同じ。)を使用して権限を識別する機能(以下「認証機能」という。)を設定する等のアクセス制御のために必要な措置を講じなければならない。

2 個人情報保護管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備(その定期又は随時の見直しを含む。)するとともに、パスワード等の読取防止等を行うために必要な措置を講じなければならない。

(アクセス記録)

第25条 個人情報保護管理者は、保有個人情報等(情報システムで取扱うものに限る。)について、秘匿性等その内容に応じて、当該保有個人情報等へのアクセス状況を記録し、その記録(以下「アクセス記録」という。)を一定の期間保存し、及びアクセス記録を定期的に又は随時に分析するために必要な措置を講じなければならない。

2 個人情報保護管理者は、アクセス記録の改ざん、窃取又は不当な消去の防止のために必要な措置を講じなければならない。

(アクセス状況の監視)

第26条 個人情報保護管理者は、保有個人情報等(情報システムで取り扱うものに限る。)の秘匿性等その内容及びその量に応じて、当該保有個人情報等への不適切なアクセス監視のため、保有個人情報等を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該機能の定期的確認等の必要な措置を講じなければならない。

(管理者権限の設定)

第27条 個人情報保護管理者は、保有個人情報等(情報システムで取扱うものに限る。)の秘

匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講じなければならない。

(外部からの不正アクセス防止)

第28条 個人情報保護管理者は、保有個人情報等を取扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講じなければならない。

(不正プログラムによる漏えい等の防止)

第29条 個人情報保護管理者は、不正プログラムによる保有個人情報等(情報システムで取扱うものに限る。)の漏えい、滅失又は毀損の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置(導入したソフトウェアを常に最新の状態に保つことを含む。)を講じなければならない。

(情報システムにおける保有個人情報等の処理)

第30条 役職員等は、保有個人情報等について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。個人情報保護管理者は、当該保有個人情報等の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認するものとする。

(暗号化)

第31条 個人情報保護管理者は、保有個人情報等(情報システムで取り扱うものに限る。)の秘匿性等その内容に応じて、暗号化のために必要な措置を講じなければならない。

2 役職員等は、次に掲げる行為については、保有個人情報等(情報システムで取扱うものに限る。)の暗号化を行わなければならない。

- (1) 保有個人情報等の共有ドライブへの保存
- (2) 保有個人情報等が記録されている媒体の外部への持ち出し
- (3) その他保有個人情報等の適切な管理に支障を及ぼすおそれのある行為

(記録機能を有する機器・媒体の接続制限)

第32条 個人情報保護管理者は、保有個人情報等(情報システムで取扱うものに限る。)の秘匿性等その内容に応じて、当該保有個人情報等の漏えい、滅失又はき損の防止のため、スマートフォン、USBメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限(当該機器への更新への対応を含む。)等の必要な措置を講じなければならない。

(入力情報の照合等)

第33条 役職員等は、情報システムで取り扱う保有個人情報等の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報等の内容の確認、既存の保有個人情報等との照合等を行わなければならない。

(バックアップ)

第34条 個人情報保護管理者は、保有個人情報等(情報システムで取扱うものに限る。)の重要度に応じて、バックアップを作成し、分散保管するため、必要な措置を講じなければならない。

2 役職員等は、個人情報保護管理者の指示に従い、保有個人情報等のバックアップを行わなければならない。

(情報システム設計書等の管理)

第35条 個人情報保護管理者は、保有個人情報等に係る情報システムの設計書及び構成図等の文書について外部に知られることがないように、その保管、複製及び廃棄等について必要な措置を講じなければならない。

(端末の限定)

第36条 個人情報保護管理者は、保有個人情報等(情報システムで取り扱うものに限る。)の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講じなければならない。

(端末の盗難防止等)

第37条 個人情報保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講じなければならない。

2 役職員等は、個人情報保護管理者が必要があると認めるときを除き、端末を外部へ持出し、又は外部から持込んではならない。

(第三者の閲覧防止)

第38条 役職員等は、端末の使用に当たっては、保有個人情報等(情報システムで取り扱うものに限る。)が第三者に閲覧されることがないように、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講じなければならない。

(サイバーセキュリティの確保)

第38条の2 役職員等は、個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法(平成26年法律第104号)第26条第1項第2号に掲げられたサイバーセキュリティに関する対策の基準等を参考として、取り扱う保有個人情報の性質等に照らして適正なサイバーセキュリティの水準を確保する。

第4節 情報システム室等の安全管理

(入退室の管理)

第39条 保有個人情報等を取扱う基幹的なサーバ等の機器を設置する室その他の区域(以下「情報システム室等」という。)を管理する課及び海外事務所の長(以下「情報システム室等の長」という。)は、情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の役職員等の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持出しの制限又は検査等の措置を講じなければならない。また、保有個人情報等を記録する媒体を保管するための施設を設けている場合も、必要があると認めるときは同様の措置を講じなければならない。

- 2 情報システム室等の長は、必要があると認めるときは、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講じなければならない。
- 3 情報システム室等の長は、情報システム室等及び保管施設の入退室の管理について、必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めを整備(その定期又は随時の見直しを含む。)、パスワード等の読取防止等を行うために必要な措置を講じなければならない。

(情報システム室等の管理)

第40条 情報システム室等の長は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置、監視設備の設置等の措置を講じなければならない。

- 2 情報システム室等の長は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講じなければならない。

第3章 個人情報ファイル簿の作成及び公表等

(個人情報ファイル簿の作成及び公表)

第41条 総括個人情報保護管理者は、政令で定めるところにより、当機構が保有している個人情報ファイルについて、それぞれ法第74条第1項第1号から第7号まで、第9号及び第10号に掲げる事項その他政令で定める事項を記載した帳簿(以下この章において「個人情報ファイル簿」という。)を作成し、公表しなければならない。

- (1) 個人情報保護管理者は、個人情報ファイルのうち個人情報ファイル簿として公表するものを保有した時は、遅滞なく、副総括個人情報保護管理者に通知しなければならない。

(2) 個人情報ファイル簿は、整備上必要な場合を除き、閲覧所に備え置き、一般の閲覧に供するものとする。

2 前項の規定は、次に掲げる個人情報ファイルについては、適用しない。

(1) 法第74条第2項第1号から第10号までに掲げる個人情報ファイル

(2) 法第74条第1項の規定による公表に係る個人情報ファイルに記録されている記録情報の全部又は一部を記録した個人情報ファイルであって、その利用目的、記録項目及び記録範囲が当該公表に係るこれらの事項の範囲内のもの

(3) 法第75条第2項第2号に掲げる個人情報ファイルに準ずるものとして政令で定める個人情報ファイル

3 第1項の規定にかかわらず、機構の長は、記録項目の一部若しくは法第74条第1項第5号若しくは第7号に掲げる事項を個人情報ファイル簿に記載し、又は個人情報ファイルを個人情報ファイル簿に掲載することにより、利用目的に係る事務又は事業の性質上、当該事務又は事業の適正な遂行に著しい支障を及ぼすおそれがあると認めるときは、その記録項目の一部若しくは事項を記載せず、又はその個人情報ファイルを個人情報ファイル簿に掲載しないことができる。

(課及び海外事務所における台帳の整備)

第42条 個人情報保護管理者は、当該課及び海外事務所の保有する個人情報ファイルについて台帳を整備して、当該保有個人情報等の利用及び保管等の取扱いの状況について記録及び更新しなければならない。

2 前項の台帳は、各課及び海外事務所ごとに、当該各課及び海外事務所の個人情報保護担当者が記録の事務及びその管理を行うものとする。

第43条 廃止

(保有個人情報等の取扱いの状況の記録)

第44条 副総括個人情報保護管理者は、第41条の規定により通知を受けた保有個人情報等について、台帳を整備し、当該保有個人情報等の利用及び保管等の取扱いについて記録しなければならない。

第4章 事案の報告及び再発防止措置

(個人情報の漏えい事案等の報告等)

第44条の2 総括個人情報保護管理者は、その取り扱う個人情報の漏えい、滅失、毀損その他の個人情報の安全の確保に係る事態であって個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会

規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。ただし、他の個人情報取扱事業者又は行政機関等から当該個人情報の取扱いの全部又は一部の委託を受けた場合であって、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を当該他の個人情報取扱事業者又は行政機関等に通知したときは、この限りでない。

- 2 前項に規定する場合には、総括個人情報保護管理者(同項ただし書の規定による通知をした者を除く。)は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

(個人情報の漏えい事案等の報告等及び措置等)

第45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又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した役職員等は、直ちに、当該保有個人情報を管理する個人情報保護管理者にその旨を報告しなければならない。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末の無線LANをオフにする又はLANケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行うものとする。

- 2 個人情報保護管理者は、前項の規定により役職員等から報告を受けたときは、被害の拡大防止及び復旧等のために必要な措置を速やかに講じなければならない。
- 3 個人情報保護管理者は、前項の措置を講じた後、速やかに、事案の発生した経緯、被害状況等を調査し、総括個人情報保護管理者及び副総括個人情報保護管理者に報告しなければならない。ただし、特に重大と認める事案が発生した場合には、直ちに総括個人情報保護管理者及び副総括個人情報保護管理者に当該事案の内容等について報告するものとする。
- 4 総括個人情報保護管理者は、前項の報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を理事長に速やかに報告しなければならない。
- 5 総括個人情報保護管理者は、事案の内容に応じて、事案の内容、経緯、被害状況等について、機構を所管する行政機関に対し、速やかに情報提供を行うものとする。

(個人情報の漏えい事案等の再発防止措置)

第46条 個人情報保護管理者は、保有個人情報の漏えいその他個人情報の管理に関して問題となる事案が発生した場合には、前条第3項の規定により調査した結果に基づき、当該

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とともに、同種の業務を実施している部室に再発防止措置を共有しなければならない。

(個人情報の漏えい事案等の公表等)

第47条 機構は事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応等の措置を講ずるものとする。

2 公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会に報告を行うものとする。

(特定個人情報の漏えい事案等の報告)

第48条 役職員等は、番号法違反の事案又は番号法違反のおそれのある事案を把握した場合及び重大事案(個人番号を取り扱う情報システムから外部に情報漏えい等があった場合(不正アクセス又は不正プログラムによるものを含む。)、事案における特定個人情報の本人の数が101人以上である場合、不特定多数の人が閲覧できる状態になった場合、役職員等が不正の目的で持出した場合、その他機構において重大事案と判断される場合)又はそのおそれのある事案が発覚した場合には、直ちに、当該保有特定個人情報を管理する個人情報保護管理者にその旨を報告するとともに、被害の拡大を防止しなければならない。

2 個人情報保護管理者は、前項の規定により役職員等から報告を受けたときは、事実関係を調査し、その原因の究明を行うとともに、速やかに総括個人情報保護管理者及び副総括個人情報保護管理者に報告をしなければならない。

3 総括個人情報保護管理者は、前項の報告を受けた場合には、当該事案の内容、経緯、被害状況等を理事長に速やかに報告しなければならない。

4 総括個人情報保護管理者は、事実関係及び再発防止策等について速やかに(重大事案又はそのおそれのある事案については、直ちに)個人情報保護委員会に報告を行わなければならない。

(特定個人情報の漏えい事案等の再発防止措置)

第49条 個人情報保護管理者は、前条第2項の規定により把握した事案による影響の範囲を特定するとともに、究明した原因を踏まえ再発防止策を検討し、速やかに実施しなければならない。

(特定個人情報の漏えい事案等の公表等)

第50条 機構は、事案の内容等に応じて、二次被害の防止、類似事案に発生の回避等の観点から、事実関係等について、速やかに、本人へ連絡し、又は本人が容易に知り得る状態に置くとともに、事実関係及び再発防止策等について、速やかに公表しなければならない。

第5章 点検及び監査等

(点検)

第51条 個人情報保護管理者は、課及び海外事務所における保有個人情報等の記録媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括個人情報保護管理者に報告する。

(監査)

第52条 個人情報監査責任者は、保有個人情報等の適切な管理を検証するため、機構における保有個人情報等の管理の状況について、定期に及び必要に応じ随時に監査(外部監査を含む。以下同じ。)を行い、その結果を総括個人情報保護管理者に報告する。監査は保有個人情報等の秘匿性等その内容に応じて、実地監査を含めた重点的な監査として行うものとする。

(評価及び見直し)

第53条 副総括個人情報保護管理者は、保有個人情報等の適切な管理のための措置について、点検又は監査の結果等を踏まえ、実効性等の観点から保有個人情報等の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講じる。

2 副総括個人情報保護管理者は、前項の見直し等の結果を総括個人情報保護管理者に報告する。

第6章 行政機関等匿名加工情報の提供等

(行政機関等匿名加工情報の作成及び提供等)

第53条の2 匿名加工情報については、法第107条から第121条の規定に基づき適切に対応するものとする。

第7章 補則

(行政機関との連携)

第54条 機構は、「個人情報の保護に関する基本方針」(平成16年4月2日閣議決定)を踏まえ、機構を所管する行政機関と緊密に連携して、その保有する個人情報の適切な管理を行うものとする。

(規則の細目の策定)

第55条 この規則に定めるもののほか、機構の保有個人情報等の保護に関する必要な細目は、別に定める。

附 則

この規則は、平成27年4月1日から施行する。

附 則(平成28年1月1日規則第33号)

この規則は、平成28年1月1日から施行する。

附 則(平成28年4月1日規則第50号)

この規則は、平成28年4月1日から施行する。

附 則(平成29年6月30日規則第89号)

この規則は、平成29年7月1日から施行する。

附 則(平成30年10月10日規則第106号)

この規則は、平成30年10月10日から施行する。

附 則(令和2年3月27日規則第33号)

この規則は、令和2年4月1日から施行する。

附 則(令和4年3月24日規則第18号)

この規則は、令和4年4月1日から施行する。