

大川広域行政組合個人番号及び特定個人情報の取扱いに関する規程

〔平成30年 3月28日〕
訓 令 第 2 号

(趣旨)

第1条 この規程は、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(平成25年法律第27号。以下「番号法」という。)及び大川広域行政組合個人情報保護条例(平成18年大川広域行政組合条例第3号。以下「条例」という。)に基づき、大川広域行政組合(以下「組合」という。)における個人番号及び特定個人情報(実施機関が保有するものに限る。以下「特定個人情報等」という。)の適正な取扱いの確保に関し必要な事項を定める。

(用語の定義)

第2条 この規程において使用する用語は、条例において使用する用語の例による。

(個人番号を取り扱う事務の範囲)

第3条 組合において個人番号を取り扱う事務は、次の各号に掲げる事務に限定する。

- (1) 職員等の健康保険及び厚生年金届出等事務
- (2) 職員等の雇用保険関係事務
- (3) 職員等の香川県市町村職員共済組合への届出等に関する事務
- (4) 職員等の源泉徴収関係事務

(総括責任者)

第4条 組合に、特定個人情報保護総括責任者(以下「総括責任者」という。)を置くこととし、事務局長をもって充てる。

2 総括責任者は、組合における特定個人情報等の管理に関する事務を総括する任に当たる。

(保護責任者)

第5条 特定個人情報等を取り扱う部署及びこれに相当する組織(以下「部署等」という。)に特定個人情報保護責任者(以下「保護責任者」という。)を置くこととし、事務局にあっては特定個人情報等を取り扱う副主幹をもって充てる。

2 保護責任者は、部署等における特定個人情報等を適切に管理する任に当たる。

3 保護責任者は、特定個人情報等を取り扱う職員(以下「事務取扱担当者」という。)及びその役割を指定する。

4 保護責任者は、各事務取扱担当者が取り扱う特定個人情報等の範囲を指定する。

5 保護責任者は、次の各号に掲げる組織体制を整備する。

- (1) 事務取扱担当者がこの規程等に違反している事実又は兆候を把握した場合の総括責任者への報告連絡体制
- (2) 特定個人情報等の漏えい、滅失又は毀損等(以下「情報漏えい等」という。)事案の発生又は兆候を把握した場合の職員から総括責任者への報告連絡体制
- (3) 特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化
- (4) 特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合の対応体制

(監査責任者)

第6条 組合に、監査責任者を置くこととし、事務局次長をもって充てる。

2 監査責任者は、特定個人情報等の管理の状況について監査する任に当たる。

(事務取扱担当者)

第7条 組合における特定個人情報等を取り扱う事務については、第3条に規定する事務ごとに事務取扱担当者を明確にするものとする。

2 事務取扱担当者は、特定個人情報等を取り扱う情報システム及び機器等を適切に管理し、利用権限のない者に使用させてはならない。

(特定個人情報の適切な管理のための会議)

第8条 総括責任者は、特定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、関係職員を構成員とする会議を開催することができる。

(教育研修)

第9条 保護責任者は、特定個人情報等の取扱いに従事する職員に対し、特定個人情報等の取扱いについて理解を深め、特定個人情報等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ものとする。

2 保護責任者は、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定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ものとする。

(職員の責務)

第10条 職員は、番号法及び条例の趣旨に則り、関連する法令及びこの規程並びに総括責任者及び保護責任者の指示に従い、特定個人情報等を取り扱わなければならない。

2 職員は、情報漏えい等の事案の発生又は兆候を把握した場合及びこの規程等に違反している事実又は兆候を把握した場合は、速やかに保護責任者に報告しなければならない。

(アクセス制限)

第11条 保護責任者は、特定個人情報等の秘匿性等その内容に応じて、当該特定個人情報等にアクセスする権限を有する者を、その利用目的を達成するために必要最小限の職員に限らなければならない。

2 アクセス権限を有しない職員は、特定個人情報等にアクセスしてはならない。

3 職員は、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特定個人情報等にアクセスしてはならない。

(作成等の制限)

第12条 職員は、業務上の目的で特定個人情報等を取り扱う場合であっても、次の各号に掲げる行為については、保護責任者の指示に従い行わなければならない。

(1) 特定個人情報等の複製

(2) 特定個人情報等の送信

(3) 特定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ち出し

(4) その他特定個人情報等の適正な管理に支障を及ぼすおそれのある行為

(誤りの訂正)

第13条 職員は、特定個人情報等の内容に誤り等を発見した場合には、保護責任者の指示に従い、

訂正等を行わなければならない。

(媒体の管理等)

第14条 職員は、保護責任者の指示に従い、特定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。

(廃棄等)

第15条 職員は、特定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、保護責任者の指示に従い、当該特定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削除又は当該媒体の廃棄を行わなければならない。

(特定個人情報等の取扱状況の記録)

第16条 保護責任者は、特定個人情報等の秘匿性等その内容及び必要に応じて、台帳等を整備して、当該保有特定個人情報の利用及び保管等の取扱いの状況について記録しなければならない。

(アクセス制御)

第17条 保護責任者は、特定個人情報等（情報システムで取り扱うものに限る。以下、第29条までにおいて同じ。）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。）を使用して権限を識別する機能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。

(アクセス記録)

第18条 保護責任者は、特定個人情報等の秘匿性等その内容及び必要に応じて、当該保養個人情報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なければならない。

2 保護責任者は、必要に応じてアクセス記録を分析するものとする。

3 保護責任者は、アクセス記録の改ざん、窃取又は不正な消去等の防止のために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19条 保護責任者は、特定個人情報等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限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ずる。

(外部からの不正アクセスの防止)

第20条 保護責任者は、特定個人情報等を取り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、ファイアー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。

(コンピュータウイルスによる漏えい等の防止)

第21条 保護責任者は、コンピュータウイルスによる特定個人情報等の漏えい、滅失又は毀損等の防止のため、コンピュータウイルスの感染防止等に必要な措置を講じなければならない。

(暗号化)

第22条 保護責任者は、特定個人情報等の秘匿性等その内容に応じて、その暗号化のために必要な措置を講じなければならない。

(バックアップ)

第23条 保護責任者は、特定個人情報等の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講じなければならない。

(情報システム設計書等の管理)

第24条 保護責任者は、特定個人情報等に係る情報システムの設計書、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、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25条 保護責任者は、特定個人情報等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しなければならない。

(端末の盗難防止等)

第26条 保護責任者は、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 職員は、保護責任者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んで서는ならない。

(第三者の閲覧防止)

第27条 職員は、端末の使用に当たっては、特定個人情報等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。

(記録機能を有する機器・媒体の接続制限)

第28条 保護責任者は、特定個人情報等の秘匿性等その内容に応じて、当該特定個人情報等の情報漏えい等の防止のため、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29条 職員は、情報システムで取り扱う特定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、処理前後の当該特定個人情報等の内容の確認、既存の特定個人情報等との照合等を行うものとする。

(特定個人情報等の提供)

第30条 保護責任者は、組合以外の者に特定個人情報等を提供する場合に必要なであると認めるときは、提供先における利用目的、利用する業務の根拠法令、利用する記録の範囲及び記録項目、利用形態等について書面を取り交わさなければならない。

2 保護責任者は、組合以外の者に特定個人情報等を提供する場合に安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地調査等を行い、措置状況を確認し、その結果を記録するとともに、改善要求等の措置を講じなければならない。

(事案の報告及び再発防止措置)

第31条 情報漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者がこの規程等に違反している事実又は兆候を把握した場合等、安全確保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、速やかに当該特定個人情報等を管理する保護責任者に報告しなければならない。

- 2 保護責任者は、被害の拡大防止又は復旧等のために必要な措置を講じなければならない。
- 3 保護責任者は、事案の発生した経緯、被害状況、内容等を調査し、総括責任者に報告しなければならない。
- 4 総括責任者は、前項の規定に基づく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、被害状況等を管理者に速やかに報告しなければならない。
- 5 保護責任者は、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なければならない。

(公表等)

第32条 保護責任者は、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、当該事案に係る本人への対応等の措置を講ずるものとする。

(監査)

第33条 監査責任者は、特定個人情報等の管理の状況について、定期的に又は随時に監査を行い、その結果を総括責任者に報告するものとする。

(点検)

第34条 保護責任者は、自ら管理責任を有する特定個人情報等の記録媒体、処理経路、保管方法等について、定期的に又は随時に点検を行い、必要があると認めるときは、その結果を総括責任者に報告するものとする。

(評価及び見直し)

第35条 特定個人情報等の適切な管理のための措置については、総括責任者は、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を行う。

(その他)

第36条 この規程に定めるもののほか、必要な事項は管理者が別に定める。

附 則

この訓令は、平成30年4月1日から施行する。