

独立行政法人消防研究所の保有する個人情報の適切な管理のための措置に関する規程

平成17年2月28日消研規程第71号

第1章 総則

(趣旨)

第1条 この規程は、独立行政法人消防研究所（以下「消防研究所」という。）における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。以下「法」という。）第7条の保有個人情報の適切な管理のための措置について必要な事項を定めるものとする。

(定義)

第2条 この規程における用語の意義は、法第2条の定めるところによる。

第2章 管理体制

(総括保護管理者)

第3条 消防研究所に、総括保護管理者1人を置く。

2 総括保護管理者は、理事をもって充てる。

3 総括保護管理者は、次に掲げる事務を行うものとする。

(1) 消防研究所における保有個人情報の管理に関する事務を総括すること。

(2) 保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うために必要があると認めるときは、保護管理者等関係職員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こと。

(3) 情報基盤委員会規程（平成14年4月1日理事長達第3号）に基づき設置された情報基盤委員会との連絡・調整等に関すること。

(4) 職員に対し、個人情報の保護に関する意識の高揚及び保有個人情報の適切な管理を図るために必要な教育研修等を行うこと。

(保護管理者)

第4条 各部課室に、保護管理者を1人置く。

2 保護管理者は、各部課室長をもって充てる。

3 保護管理者は、次に掲げる事務を行うものとする。

(1) 各部課室における保有個人情報を適切に管理すること。

(2) 当該部課室の職員に対し、保有個人情報の適切な管理のために、総括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ずること。

(保護担当者)

第5条 各部課室に、当該部課室の保護管理者が指定する保護担当者を1人又は複数人置く。

2 保護担当者は、保護管理者を補佐し、各部課室における保有個人情報の管理に関する事務を行う。

(監査責任者)

第6条 消防研究所に、監査責任者を置く。

2 監査責任者は、監事をもって充てる。

3 監査責任者は、保有個人情報の管理の状況について監査する。

第3章 職員の責務

(職員の責務)

第7条 職員は、法の趣旨に則り、関連する法令及び規程等の定め並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱わなければならない。

第4章 保有個人情報の取扱い

(アクセス制限)

第8条 保護管理者は、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定しなければならない。

2 アクセス権限を有しない職員は、保有個人情報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保有個人情報にアクセスしてはならない。

(複製等の制限)

第9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、保護管理者の指示に従い行う。

(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

(誤りの訂正等)

第10条 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、保護管理者の指示に従い、訂正等を行うものとする。

(媒体の管理等)

第11条 職員は、保護管理者の指示に従い、保有個人情報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施錠等を行うものとする。

(廃棄等)

第12条 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、保護管理者の指示に従い、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ものとする。

(保有個人情報の取扱い状況の記録)

第13条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有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するものとする。

第5章 情報システムにおける安全の確保等

(アクセス制御)

第14条 保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第5章（第19条を除く。）において同じ。）の秘匿性等その内容に応じて必要があると認めるときは、パスワード

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るものとする。

2 保護管理者は、1の措置を講ずる場合には、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ずるものとする。

（アクセス記録）

第15条 保護管理者は、保有個人情報の秘匿性等その内容に応じて必要があると認めるときは、当該保有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、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ずるものとする。

2 保護管理者は、アクセス記録の改ざん、窃取又は不正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。

（外部からの不正アクセスの防止）

第16条 保護管理者は、保有個人情報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17条 保護管理者は、コンピュータウイルスによる保有個人情報の漏えい、滅失又はき損の防止のため、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18条 保護管理者は、保有個人情報の秘匿性等その内容に応じて必要があると認めるときは、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。

（入力情報の照合等）

第19条 職員は、情報システムで取り扱う保有個人情報の重要度に応じて、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の内容の確認、既存の保有個人情報との照合等を行うものとする。

（バックアップ）

第20条 保護管理者は、保有個人情報の重要度に応じて、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ずるものとする。

（情報システム設計書等の管理）

第21条 保護管理者は、保有個人情報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22条 保護管理者は、保有個人情報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 2 3 条 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 職員は、保護管理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 2 4 条 職員は、端末の使用に当たっては、保有個人情報 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。

第 6 章 情報システム室等の安全管理

(入退室の管理)

第 2 5 条 保護管理者は、基幹的なサーバ等の機器を設置する室等 (以下「情報システム室等」という。) には、入室する権限を有する者を定めるものとする。

(情報システム室等の管理)

第 2 6 条 保護管理者は、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の設置等の措置を講ずるものとする。

2 保護管理者は、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ずるものとする。

第 7 章 保有個人情報の提供及び業務の委託

(保有個人情報の提供)

第 2 7 条 保護管理者は、法第 9 条第 2 項第 3 号及び第 4 号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、原則として、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ものとする。

2 保護管理者は、法第 9 条第 2 項第 3 号及び第 4 号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、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の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ずるものとする。

3 保護管理者は、法第 9 条第 2 項第 3 号の規定に基づき行政機関又は独立行政法人等に保有個人情報を提供する場合において、必要があると認めるときは、1 及び 2 に規定する措置を講ずるものとする。

(業務の委託等)

第 2 8 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、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ものとする。

(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に関する事項
 - (5) 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
 - (6) 違反した場合における契約解除の措置その他必要な事項
- 2 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するものとする。

第8章 安全確保上の問題への対応

(事案の報告及び再発防止措置)

- 第29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保護管理者に報告するものとする。
- 2 保護管理者は、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ものとする。
 - 3 保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告するものとする。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 総括保護管理者は、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、被害状況等を理事長に速やかに報告するものとする。
 - 5 保護管理者は、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ずるものとする。

(公表等)

- 第30条 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。

第9章 監査及び点検の実施

(監査)

- 第31条 監査責任者は、保有個人情報の管理の状況について、定期に又は随時に監査を行うものとする。
- 2 総括保護管理者は、監査の結果を踏まえ、適切な措置を講じなければならない。

(点検)

- 第32条 保護管理者は、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、定期に又は随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告するものとする。

(評価及び見直し)

- 第33条 保有個人情報の適切な管理のための措置については、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講ずるものとする。

附 則

この規程は、平成17年4月1日から施行する。