環境医学研究所における保有個人情報の保護及び管理の方法に関するマニュアル

名古屋大学個人情報保護規程（平成16年度規程第313号。以下「規程」という。）、名古屋大学個人情報保護規程施行細則（平成17年度細則第11号。以下「細則」という。）及び名古屋大学環境医学研究所個人情報保護内規により、環境医学研究所長は、環境医学研究所（以下「研究所」という。）における保有個人情報の取扱いに関するマニュアルを、次のとおり定める。

１　職員の責務

(1) 基本的な責務

イ 職員は、関連する法令、規程等（このマニュアルを含む。以下同じ。）の定めるところに従い、保有個人情報を取り扱わなければならない。

ロ 職員は、職務上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てはならない。その職を退いた後も、同様とする。

ハ 職員は、虚偽の利用目的を告げる等の不正な手段により個人情報を取得してはならない。

ニ 職員は、個人情報の保有に当たっては、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。

ホ 職員は、業務の達成に必要な範囲を超えて、個人情報を保有してはならない。

ヘ 職員は、法令に基づく場合を除き、利用目的以外に保有個人情報を利用し、又は提供してはならない。

(2) 情報セキュリティ対策

職員は、情報セキュリティ対策においては、次に掲げる事項に留意し、「名古屋大学情報セキュリティガイドライン」を遵守しなければならない。

イ 職員は、職務目的以外で名古屋大学（以下「本学」という。）の情報設備を利用してはならない。

ロ 職員は、保有個人情報を取り扱う情報システム等の起動に当たっては、ＩＤ・パスワードを設定し、取扱い権限を有する者でなければ利用できないようにしなければならない。

ハ 職員は、自らが情報システム等を利用するためのＩＤ・パスワードを他人に使用させ、貸与し、公開してはならない。

ニ 職員は、他人のＩＤ・パスワードを盗用する等により、アクセス権限のない情報システム等へアクセスしてはならない。

ホ 職員は、離席時には、パソコンをシャットダウン又は休止状態にし、あるいは利用再開時にパスワード入力が必要なスクリーンセーバーを作動させる等、保有個人情報が第三者に閲覧されないようにしなければならない。

ヘ 職員は、当該システム管理者の許可を得ることなく、本学の情報設備にソフトフェアをインストール又はアンインストールをしてはならない。

ト 職員は、自らが使用するパソコンにウィルス対策ソフトウェアをインストールして、常に有効な状態に保たなければならない。

チ 職員は、保有個人情報が完全性を保持する必要性の高いものである場合には、必ずバックアップのためのデータを作成しなければならない。

リ 職員は、保有個人情報を保存した記録媒体を修理又は廃棄する場合には、当該保有個人情報をデ

ータ消去ソフト等により完全に消去しなければならない。

(3) その他の留意事項

イ 職員は、保有個人情報について、業務に不必要な複写を行ってはならない。

ロ 職員は、個人情報が記録されている文書を印刷又は複写した場合は、プリンタや複写機から原本と複写物を直ちに回収しなければならない。

ハ 職員は、不要となった個人情報は、速やかに適切な方法により廃棄し、長期に保有してはならない。

ニ 職員は、職員不在時・退庁時には執務室を施錠しなければならない。

2 保有個人情報の取扱い方法

(1) 保有個人情報の管理

職員は、研究所における保有個人情報の管理について、名古屋大学環境医学研究所個人情報保護内規に基づくこととする。

(2) 持出し等のルール

イ　外部への送信

(ｲ) 保有個人情報を送信する場合は、ファクシミリ又は電子メールを利用することが適切かどうか、必要以上の情報が含まれていないか及びファクシミリ送信をする場合は、番号が正しいことを確認のうえ、送信する。

(ﾛ) 外部（行政機関、独立行政法人等を除く。）へ電子メールを送信する際、複数のアドレス宛に一括送信する場合は、ＢＣＣ等を利用して他のアドレスが判明しないようにする。

(ﾊ) 電子情報をメールで送信するときは、ファイルへのパスワードの設定、暗号化等を行う。

ロ　外部への送付

(ｲ) 封入作業は、個人の作業机とは別の場所で行い、封入作業スペースの周辺は、整理整頓する。

(ﾛ) 封入前に、封筒と内容物の数を合わせておき、封入後に、封筒と内容物の残数が一致するかを確認する。

(ﾊ) 複数人の個人情報を一括して送付する際は、紛失や書類混入を速やかに発見できるよう、送付状に封書内の個人情報の件数等を記載する。

(ﾆ) 個人情報の含まれる書類を郵送する際は、簡易書留等通常の郵便とは別の郵送ルートが確認できる方法を利用する。

ハ　外部への持出し

保有個人情報は、外部へ持ち出してはならない。ただし、職務遂行上必要な場合は、保護管理者の許可を得ること。

(ｲ) 持ち出すときは、

①持ち出す情報は、職務遂行に必要な最小限の量とする。

②持ち運びには、必要に応じて施錠可能なカバン等を使用する。

③電子情報には、ファイルへのパスワードの設定、暗号化等を行う。

(ﾛ) 持出し中は、

①ひったくり、車上狙い等の犯罪を意識しながら、手元から離さないよう常に携行する。

②必要に応じて、持ち出した情報を失っていないか確認する。

(ﾊ) 持出し先では、

ウィニー等のファイル共有ソフトがインストールされたパソコンで記録媒体（ＵＳＢメモリ等

）を取り扱わない。

３　パソコンや記録媒体（ＵＳＢメモリ等）の取扱い方法

(1) パソコンの管理

職員は、研究所におけるパソコン等の取扱い、管理等について、保護担当者の指示に従うこととする。

イ　外部持出し

本学内で利用するパソコン等については、原則として持出しを認めない。ただし、職務遂行上必要な場合は、【持出用】のパソコン等を設定し、それを使用すること。

(ｲ) 【持出用】と設定されたパソコン等には、保有個人情報を含む電子情報を保存しない。

(ﾛ) 持ち出すときは、

①持ち出す情報は、職務遂行に必要な最小限の量とする。

②持ち運びには、必要に応じて施錠可能なカバン等を使用する。

③電子情報には、ファイルへのパスワードの設定、暗号化等を行う。

(ﾊ) 持出し中は、

①ひったくり、車上狙い等の犯罪を意識しながら、手元から離さないよう常に携行する。

②必要に応じて、持ち出した情報を失っていないか確認する。

ロ　共有サーバ

(ｲ) 共有サーバ上の共有フォルダのアクセス権は、必要最小限の職員にのみ付与することとする。

(ﾛ) 共有サーバ上に保有個人情報が含まれるフォルダを置く場合は、ＩＤ・パスワードを設定し、取扱い権限を有する者でないと利用できないようにしなければならない。

ハ　その他

(ｲ) 持ち運びしないノートパソコンは、盗難防止ワイヤーで机等に固定する。

(2) 電子記録媒体の管理

イ　保管

研究所内で利用する電子記録媒体は、使用しない時には、鍵のかかるキャビネット等に保管し、施錠する。

ロ　外部持出し

研究所内で利用する電子記録媒体については、原則として持出しを認めない。ただし、職務上必要な場合は、【持出用】のUSBメモリ等を設定し、それを使用すること。

(ｲ) 【持出用】と設定されたUSBメモリ等は、使用後は、その都度、記録された電子情報を完全に消去する。

(ﾛ) 持ち出すときは、

①持ち出す情報は、職務遂行に必要な最小限の量とする。

②持ち運びには、必要に応じて施錠可能なカバン等を使用する。

③電子情報には、ファイルへのパスワードの設定、暗号化等を行う。

(ﾊ) 持出し中は、

①ひったくり、車上狙い等の犯罪を意識しながら、手元から離さないよう常に携行する。

②必要に応じて、持ち出した情報を失っていないか確認する。

(ﾆ)　持出し先では、ウィニー等のファイル共有ソフトがインストールされたパソコンで記録媒体（USBメモリ等）を取り扱わない。

ハ　廃棄

(ｲ) 研究所内で利用する電子記録媒体を廃棄する際は、機密の保持を可能とする次の処理方法から選択し、廃棄する。

①物理的破壊による方法

研究所事務部のディスクシュレッダーを使用する場合は、経理課用度掛（内線5264）へ連絡する。

②データ消去ソフトによる方法

(3) パスワードの管理

イ　アカウント作成時に付与されたパスワードは、使用しない。

ロ　桁数8桁以上で、英数字、大文字、小文字、特殊記号が混在したパスワードを設定する。

・人名、地名、辞書に記載されている等の一般的な単語・用語は避ける。

・性、名、誕生日、アカウント等から容易に推測されるものは避ける。

・キーボードの並び順等で設定することは避ける。

ハ　パスワードは、1年に1回以上変更する。

ニ　作業机周辺、マニュアル等の他人に知られる可能性が高い場所にパスワードを記載しない。

以上