

# 独立行政法人労働安全衛生総合研究所 情報セキュリティポリシー（基本方針）

平成22年3月1日決定

## 1. 基本的な考え方

独立行政法人労働安全衛生総合研究所（以下「研究所」という。）は、職場における労働者の安全及び健康の確保に資することを目的とした独立行政法人である。研究所の取り扱う情報は、個人情報に関するもの、疫学情報や遺伝子情報等を含むもの、事業者の営業上又は技術上の権利に関するもの、国の行政運営上重要なもの等を多く含み、外部への漏えい、改ざん、消失等が発生した場合には、極めて重大な結果を招くおそれがある。したがって、適切な情報セキュリティ対策を講じることにより情報資産を様々な脅威から守ることは、研究所の社会的信頼及び事業継続の確保に必要であり、ひいては国民生活、事業者の事業活動及び行政の安定的運営に資するものである。

以上のことから、研究所における情報セキュリティ対策を体系的に構築するため、情報セキュリティ対策の目標、対象、対策の要点、役職員等の責務等を内容として、研究所の情報セキュリティに関する基本的な考え方を示す情報セキュリティ基本方針を定めることとする。

## 2. 用語の定義

(1) この基本方針における用語の意義は、以下のとおりとする。

ア 「情報セキュリティ」とは、情報の機密性、完全性及び可用性をいう。

イ 「情報セキュリティ対策」とは、情報セキュリティを確保するために必要な措置をいう。

ウ 「情報」とは、以下の（ア）から（エ）をいい、作成中の文書等も含まれる。

（ア）情報システム内部に記録された情報

（イ）情報システム外部の電磁氣的記録媒体に記録された情報

（ウ）情報システムに関係がある書面に記載された情報

（エ）研究所文書（研究所の役職員（非常勤職員及び派遣職員を含む。以下同じ。）が職務上作成し、又は取得した文書、図面、データ、電磁的記録（電子的方式、磁氣的方式その他人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た記録をいう。以下同じ。）であつて、研究所の役職員が組織的に用いるものとして、研究所が保有しているものをいう。）

エ 「情報システム」とは、情報処理及び通信に係るシステムをいう。

オ 「機密性」とは、情報に関して、認可された者だけがこれにアクセスできる状態を確保することをいう。

カ 「完全性」とは、情報が破壊、改ざん又は消去されていない状態を確保することをいう。

キ 「可用性」とは、認可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

ク 「情報資産」とは、情報及び情報を管理する仕組み（情報システム及び事務室、保管庫その他の情報を保管するための施設設備（情報システムを除く。）（以下「情報システム等」という。）の総称をいう。

- ケ 「主体認証」とは、識別コードを提示した主体が、その識別コードを付与された主体、すなわち、正当な主体であるか否かを検証することをいう。
- コ 「役職員等」とは、研究所の役員、職員、非常勤職員、派遣職員、客員研究員、フェロー研究員及び各種委員会委員（ただし、委嘱状が交付された者に限る。）をいう。
- サ 「委託事業者」とは、研究所との委託、請負付託、役務等の契約行為により研究所の業務を行う者をいう。
- シ 「情報セキュリティ関係規程等」とは、この基本方針、5.（1）の情報セキュリティ管理規程、同規程に基づき制定される情報セキュリティ対策基準その他の規程及びその実施手順その他の情報セキュリティ対策の実施に必要な規程類をいう。

### 3. 基本方針の対象

この基本方針の対象は、次に掲げるとおりとする。

- （1） 研究所の情報資産
- （2） 役職員等、委託事業者、共同研究先の当該共同研究従事者（以下「共同研究従事者」という。）及び共同事業先の当該事業従事者（以下、「共同事業従事者」という。）

### 4. 情報セキュリティ対策の目標等

- （1） 研究所の情報セキュリティ対策は、研究所の情報資産に対する次に掲げる研究所内外からの脅威を考慮するものとする。
  - ア 外部からの意図的な攻撃による障害（不正侵入、コンピューターウイルス、盗聴、盗難、改ざん、破壊、消去、漏えい等）
  - イ 内部の意図的な不正使用等による障害（不正使用、改ざん、破壊、消去、漏えい、持出し等）
  - ウ 非意図的要因による障害（次号に掲げるものを除く。）（ハードウェア障害、ソフトウェア障害、ネットワーク障害、設備の故障、誤った使用・運用、過失等）
  - エ 災害による障害（落雷、火災、水害、地震等）
  - オ 研究所の情報資産を用いた外部の情報資産への加害行為（非意図的なものを含む。）（コンピューターウイルスの送信、不正侵入等）
- （2） 研究所の情報セキュリティ対策は、情報セキュリティの確保について必要かつ適切な措置を講じることにより、次に掲げる事項を目標とする。
  - ア 上記（1）のアからウまでに掲げる脅威に関して、被害を受けず、若しくは当該情報資産に係る外部の関係者に損害を与えず、又は被害若しくは損害を最小限に食い止め、もって実務上、法務上、財務上又は社会的信頼の上で研究所の存続又は業務の継続に甚大な悪影響を受ける事態を起こさないこと。
  - イ 上記（1）のエに掲げる脅威に関して、研究所の受ける被害及び当該情報資産に係る外部の関係者に与える損害を可能な範囲で小さくし、もって研究所の社会的信頼を獲得し及び保持すること。
  - ウ 上記（1）のオに掲げる脅威に関して、外部に損害を与えず又は損害を最小限に食い止め、

もって実務上、法務上、財務上又は社会的信頼の上で研究所の存続又は業務の継続に甚大な悪影響を受ける事態を起こさないこと。

## 5. 情報セキュリティ対策の要点

### (1) 組織及び体制の確立

情報セキュリティの確保に必要な組織及び体制を整備し、責任と権限を明確にする。

### (2) 情報の格付けに応じた対策

情報を機密性、完全性及び可用性の観点から格付けを行い、当該格付けに応じて対策を講じる。

### (3) 情報のライフサイクルにわたる対策

情報の作成、入手、利用、保存、移送、提供、消去、廃棄等の情報のライフサイクルの各段階において必要な対策を講じる。

### (4) 情報セキュリティ要件の明確化に基づく対策

主体認証、アクセス制御、権限管理等の基本的なセキュリティ機能及び主要な脅威を防ぐために遵守すべき事項に関する必要な対策を講じる。

### (5) 情報システム及び保管施設設備の構成要素についての対策

情報システム等に係る装置、設備、ソフトウェア、施設・環境面等について必要な対策を講じる。

### (6) 情報システムに係るその他の対策

ア 情報システム等の調達及び開発に係る仕組み及び手続き、研究所外での情報処理の制限等について必要な対策を講じる。

イ (4) 及び (5) の対策は、委託事業者、共同研究従事者及び共同事業従事者における情報セキュリティ確保の観点を併せて考慮するものとする。

### (7) 教育

ア 役職員の着任時及び定期的に、情報セキュリティに関する必要な教育を行うものとする。

イ 客員研究員、フェロー研究員、委託事業者、共同研究従事者及び共同事業従事者に対しても、アの教育に準じた教育を実施するように努めるものとする。

### (8) 評価と見直し

情報セキュリティ対策について自己点検及び監査を行い、それらの結果により、情報セキュリティ関係規程に定められた事項及び対策を評価し、必要に応じ見直す。

## 6. その他

(1) 関係規程類の体系

ア 4に基づく情報セキュリティ対策の基本的かつ具体的な枠組みを規定するため、情報セキュリティ管理規程（以下「管理規程」という。）を定めることとする。

イ 管理規程の規定する枠組みを実施するのに必要な具体的な対策基準その他の規程（以下「対策基準等」という。）及び対策基準等に定められた対策の内容を具体的な業務又は情報システムにおいて実施するための実施手順並びに監査を実施するための基準及び実施手順は、それぞれ別途定めることとする。

ウ この基本方針及び管理規程以外の規程類（(1)イの規程類を除く。）において、情報セキュリティの確保に係る部分は、この基本方針及び管理規程に矛盾のないよう、又は、当該部分とこの基本方針及び管理規程とは相互に矛盾のないよう規定するものとする。

(2) 基本方針等の公表

この基本方針及び管理規程は、制定又は改定したときは、これを公表するものとする。

(3) 周知及び徹底

役職員は、委託事業者、共同研究従事者及び共同事業従事者にこの基本方針及び情報セキュリティ関係規程等の周知及び徹底を図るものとする。

(4) 役職員の責務

ア 役職員は、情報セキュリティ関係規程等に定める事項の実施に責任を負うとともに、それらを遵守する。

イ 役職員は、情報セキュリティ関係規程等に定める事項を委託事業者、共同研究従事者及び共同事業従事者に遵守させるものとする。

(5) 法令遵守

ア 役職員等、委託事業者、共同研究従事者及び共同事業従事者は、研究所の情報資産を使用するに当たって関係する法令及び規則等を遵守する。

イ アの関係する法令及び規則等には、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、不正アクセス行為の禁止等に関する法律、著作権法、不正競争防止法、刑法及び国家公務員法が含まれる。