

独立行政法人労働安全衛生総合研究所 情報セキュリティ管理規程

第1章 総則

(目的)

第1条 この規程は、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。）の情報セキュリティポリシー（以下「基本方針」という。）に基づき、研究所において情報セキュリティ対策を講ずるための組織及び体制の整備、情報セキュリティの分類と対策、その他基本となる事項について定めることを目的とする。

(定義)

第2条 この規程において使用する用語は、基本方針の「2 用語の定義」に定める用語の例によるほか、次の各号による。

- 一 「職務従事者」とは、研究所職員及び研究所職員の指揮、命令に服している者のうち、研究所の管理対象である情報及び情報システムを取り扱う者をいう。
- 二 「研究所外」とは、研究所が管理する組織又は研究所の施設の外をいう。
- 三 「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄等をいう。
- 四 「明示」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示に含むものとする。
- 五 「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。
- 六 「要機密情報」とは、研究所文書管理規程第46条に規定する秘密文書（以下、「秘密文書」という。）に相当する機密性を要する情報及び秘密文書には相当しないが、その漏洩により、国民の権利が侵害され、又は研究所の業務の遂行に支障を及ぼすおそれがある情報をいう。
- 七 「要保全情報」とは、職務で取り扱う情報（書面を除く。）のうち、その改ざん、誤謬又は破損により、職務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
- 八 「要安定情報」とは、職務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、職務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

第2章 組織と体制の整備

(最高情報セキュリティ責任者)

第3条 研究所に最高情報セキュリティ責任者を置く。

- 2 最高情報セキュリティ責任者は、研究所における情報セキュリティ対策に関する事務を統括する。
- 3 最高情報セキュリティ責任者は、理事長とする。

(統括情報セキュリティ責任者)

第4条 研究所に統括情報セキュリティ責任者を置く。

- 2 統括情報セキュリティ責任者は、最高情報セキュリティ責任者の補佐を行う者として、情報セキュリティ責任者を統括する。
- 3 統括情報セキュリティ責任者は、理事（総務担当）とする。
- 4 統括情報セキュリティ責任者は、全ての情報セキュリティ責任者、情報セキュリティ管理者及び情報システムセキュリティ責任者に対する連絡網を整備する。

(情報セキュリティ責任者)

第5条 総務部、研究企画調整部、災害調査分析センター及び国際情報・研究振興センター（以下「部等」という。）に情報セキュリティ責任者をおく。

- 2 情報セキュリティ責任者は、所管する部等（研究企画調整部の情報セキュリティ責任者にあっては、それぞれの地区の研究グループを含む。）における情報セキュリティ対策に関する事務を統括する。
- 3 情報セキュリティ責任者は、総務部長、総務課長、研究企画調整部長、同部首席研究員、労働災害調査分析センター長及び国際情報・研究振興センター長とする。

(情報セキュリティ管理者)

第6条 部等に情報セキュリティ管理者をおく。

- 2 情報セキュリティ管理者は、情報セキュリティ責任者の指示を受けて、所属する部等における情報セキュリティ対策に関する事務を行う。
- 3 情報セキュリティ管理者は、情報セキュリティ責任者が指名するものとする。

(情報システムセキュリティ責任者)

第7条 研究所における情報システム（一の部等において限定的に使用される情報システム（以下、「個別情報システム」という。）を除く。）ごとに、情報システムセキュリティ責任者を置く。

- 2 情報システムセキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務を統括する。
- 3 情報システムセキュリティ責任者は、最高情報セキュリティ責任者が指名するものとする。

(情報セキュリティ監査責任者)

第8条 研究所に、情報セキュリティ監査責任者を置く。

- 2 情報セキュリティ監査責任者は、最高情報セキュリティ責任者の指示に基づき、情報セキュリティ監査に関する事務を統括する。
- 3 情報セキュリティ監査責任者は、監事（業務担当）とする。

（情報セキュリティ委員会）

第9条 研究所に情報セキュリティ委員会を置く。

- 2 情報セキュリティ委員会は、研究所における情報セキュリティ対策の推進に関する重要な事項について調査審議を行う。
- 3 情報セキュリティ委員会の委員は、最高情報セキュリティ責任者、統括情報セキュリティ責任者及び情報セキュリティ責任者とする。
- 4 情報セキュリティ委員会の委員長（以下「委員長」という。）は、最高情報セキュリティ責任者とする。
- 5 情報セキュリティ委員会の庶務は、総務部が処理する。
- 6 その他情報セキュリティ委員会の運営に必要な事項については、別に定める。

（兼務の禁止）

第10条 次に掲げる者は、相兼ねることができない。

- 一 この規程において定める承認又は許可の申請者とその承認権限者又は許可権限者
- 二 監査を受ける者とその監査を実施する者

第3章 情報の取扱いの原則

（情報の作成と入手、利用）

第11条 業務従事者は、研究所の業務の遂行以外の目的で、情報を作成し、又は入手してはならない。

- 2 業務従事者は、研究所の業務の遂行以外の目的で、情報を入手してはならない。

（重要度に応じた情報の取扱い）

第12条 情報の取扱いは、その情報の重要度に応じた適切な措置が講じられなければならない。

- 2 前項の重要度は第13条の情報の格付けにより分類する。

第4章 情報セキュリティ対策基準等の整備

（情報セキュリティ対策基準）

第13条 最高情報セキュリティ責任者は、基本方針に基づき、情報の分類と対策、情報のライフサイクルにわたる対策、情報セキュリティの明確化に基づく対策、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等に関する個別事項に係る情報セキュリティ対策に関して遵守すべき事項を情報セキュリティ対策基準（以下「対策基準」という。）として別に定める。

- 2 情報セキュリティ責任者は、個別情報システムについて、この規程及び対策基準で定める事項のほか、必要がある場合は、基本方針に従い、情報セキュリティ対策に関する事項を独自に定めることができる。
- 3 情報システムセキュリティ責任者は、自らが所管する情報システムについて、この規程及び対策基準で定める事項のほか、必要がある場合は、基本方針に従い、情報セキュリティ対策に関する事項を独自に定めることができる。

（情報の格付け）

第14条 最高情報セキュリティ責任者は、研究所の業務で取り扱う情報について、電磁的記録については、機密性、完全性及び可用性の観点から、書面については、機密性の観点から、当該情報の格付け及び取扱制限の明示等の基準を整備する。

（その他の基準等）

第15条 統括情報セキュリティ責任者は、次の各号に示す情報セキュリティ対策に関する事項について必要な基準等を整備する。

- 一 情報システムに係る機器等の選定基準及び購入する機器等の確認・検査、その他機器等の購入に関する手続きに関する事項
- 二 ソフトウェア開発、情報処理、情報システムの開発・保守・運用等を研究所外の機関に委託し、又は請け負わせる場合における当該機関の選定基準に関する事項
- 三 その他情報セキュリティの確保について必要な事項

第5章 例外措置

（例外措置）

第16条 基本方針、本規程及び本規程に基づき定められる基準等（以下「情報セキュリティ関係規程」という。）にそぐわない例外的な措置（以下「例外措置」という。）の適用を審査する者（以下「許可権限者」）は、情報セキュリティ責任者又は情報システムセキュリティ責任者（情報システムに関する違反にあっては、情報システムセキュリティ責任者。両者を併せて以下「情報セキュリティ責任者等」という。）とする。

- 2 許可権限者は、例外措置の適用の申請の審査手続きを別に定めるものとする。
- 3 業務従事者は、例外措置の適用を希望する場合には、定められた審査手続きに従い、許可権限者に例外措置の適用を申請しなければならない。ただし、業務の遂行に緊急を要する等の場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること、又は規定を実施しないことが不可避のときは、事後速やかに申請を行うものとする。

- 4 許可権限者は、業務従事者からの例外措置の適用の申請を、定められた手続きに従って審査し、許可の可否を決定する。
- 5 業務従事者は、例外措置の適用について許可を受け、例外措置を適用した場合には、それを終了したときに、許可権限者にその旨を報告する。ただし、許可権限者が報告を要しないとした場合は、その限りではない。
- 6 許可権限者は、例外措置の適用に係る申請、審査及び報告についての記録台帳を整備するものとする。

(違反に対する措置)

- 第17条 業務従事者は、情報セキュリティ関係規程への重大な違反を知った場合には、情報セキュリティ責任者等にその旨を報告しなければならない。
- 2 情報セキュリティ責任者等は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、統括情報セキュリティ責任者を通じて最高情報セキュリティ責任者にその旨を報告するとともに、違反者及び関係する者に情報セキュリティを確保するために必要な措置を講じさせる。

第6章 障害対応

(障害等の対応に備えた事前準備)

- 第18条 最高情報セキュリティ責任者は、情報セキュリティに関する事故及び障害（以下「障害等」という。）が発生した場合において、被害の拡大を防ぐとともに、障害等から復旧するための体制を整備しなければならない。
- 2 統括情報セキュリティ責任者は、障害等が発生した際の被害拡大防止及び関係者への連絡等に関する対処手順の整備を行わなければならない。
 - 3 統括情報セキュリティ責任者は、障害等について研究所外からの報告を受けるための窓口を設置しなければならない。

(障害等の発生時における報告と応急措置)

- 第19条 業務従事者は、障害等を知った場合には、情報セキュリティ責任者等を通じて統括情報セキュリティ責任者にその旨を通知しなければならない。
- 2 統括情報セキュリティ責任者は、障害等の報告を受けた場合及び自らが重大な障害等を知った場合には、最高情報セキュリティ責任者にその旨を報告するとともに、情報セキュリティ責任者等を通じて業務従事者に情報セキュリティを確保するために必要な措置を講じさせなければならない。
 - 3 業務従事者は、障害等が発生した際、当該障害について適用可能な対処手順がある場合には、その手順に従い対応しなければならない。
 - 4 業務従事者は、障害等が発生した際、当該障害について適用可能な対処手順がない場合には、情報セキュリティ責任者等から指示を受けるまで、障害等による被害の拡大防止に

努めなければならない。また、指示を受けた場合には、その指示に従い対応しなければならない。

(障害等の原因調査と再発防止対策)

第20条 情報セキュリティ責任者等は、障害等が発生した場合には、障害等の原因を調査し、再発防止対策を策定した上で、その結果を報告書として統括情報セキュリティ責任者を通じて最高情報セキュリティ責任者に報告しなければならない。

2 最高情報セキュリティ責任者は、情報セキュリティ責任者等からの障害等の原因調査等に係る報告を受けた場合は、その内容を検討し、再発防止策を実施するために必要な措置を講じる。

3 最高情報セキュリティ責任者は、必要と認めるときは、情報セキュリティ責任者等に障害等の原因調査及び再発防止対策の策定を指示するものとする。

第7章 教育

(情報セキュリティ対策の教育)

第21条 統括情報セキュリティ責任者は、新たに業務従事者になったものに対して、情報セキュリティ関係規程及び情報セキュリティ対策の実施に関する事項について、基礎的な教育を行わなければならない。

2 統括情報セキュリティ責任者は、業務従事者を対象に、原則として年1回以上、情報セキュリティ対策の実施に関する事項について、知識及び技能の向上を図るための教育を行わなければならない。

(情報セキュリティ対策の啓発)

第22条 統括情報セキュリティ責任者は、前条に規定する教育のほか、情報セキュリティ関係規程及び情報セキュリティ対策の実施について、業務従事者に対し、その啓発に努める。

第8章 評価及び見直し

(自己点検の実施)

第23条 最高情報セキュリティ責任者は、少なくとも年に1回以上、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システムセキュリティ責任者及び業務従事者（以下、「業務従事者等」という。）に対して、情報セキュリティに関する自己点検の実施を指示しなければならない。

2 業務従事者等は、最高情報セキュリティ責任者からの指示に従って、情報セキュリティに関する自己点検を実施しなければならない。

(自己点検の結果の評価)

第24条 業務従事者及び情報セキュリティ管理者は、自己点検の結果を情報セキュリティ責任者等に報告しなければならない。

- 2 情報セキュリティ責任者等は、業務従事者及び情報セキュリティ管理者から報告のあった自己点検の結果を評価し、この結果を統括情報セキュリティ責任者に報告しなければならない。
- 3 統括情報セキュリティ責任者は、情報セキュリティ責任者から報告のあった評価の結果を研究所全体の自己点検の結果として取りまとめ、この結果を最高情報セキュリティ責任者に報告しなければならない。

(自己点検に基づく改善)

第25条 業務従事者等は、自らが実施した自己点検の結果に基づき、自己の権限の範囲内で改善できると判断したことは改善しなければならない。

- 2 最高情報セキュリティ責任者は、統括情報セキュリティ責任者から報告のあった研究所全体の自己点検の評価結果を基に、改善の必要があると認めるときは、関係者に改善の指示を行わなければならない。

(監査の実施)

第26条 情報セキュリティ監査責任者は、少なくとも年に1回以上、情報セキュリティに関する監査を実施するものとする。

- 2 前項の監査の実施に当たっては、情報セキュリティ監査責任者は、予め監査の日時、対象者、監査する事項を定め、最高情報セキュリティ責任者の承諾を得ておくものとする。
- 3 情報セキュリティ監査責任者は、監査を実施した結果及び結果に基づく改善事項についての報告書を取りまとめ、最高情報セキュリティ責任者に提出するものとする。

(監査結果に基づく改善)

第27条 最高情報セキュリティ責任者は、情報セキュリティ監査責任者から提出された報告を踏まえ、情報セキュリティ関係規程等の見直し、又は関係者に対する改善の指示を行わなければならない。

附則

(施行期日)

第1条 本規程は、平成22年3月1日より適用する。