

公益財団法人九州先端科学技術研究所情報セキュリティ管理規程

(目的)

第1条 この規程は、公益財団法人九州先端科学技術研究所（以下、「本研究所」という。）が所管する情報資産の保護及び管理に関する基本的事項を定め、情報資産の漏洩及び不正使用など防止することを目的とする。

(定義)

第2条 この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- (1) 情報セキュリティ 情報資産の機密を保持し、情報資産の正確性及び完全性を維持し、並びに情報資産を定められた範囲で利用可能な状態で維持することをいう。
- (2) 情報資産 ネットワーク及び情報システム、これらに関する設備、これらで取り扱う情報、これらを印刷した文書、電磁的記録媒体並びにシステム構成図等の関連する文書をいう。
- (3) ネットワーク コンピュータ等を相互に接続するための通信網並びにその構成機器であるハードウェア及びソフトウェアをいう。
- (4) 情報システム コンピュータ、ネットワーク、電磁的記録媒体等で構成され、情報処理を行う仕組みをいう。
- (5) 職員 公益財団法人九州先端科学技術研究所就業規則、特任研究員就業規程、特別研究員就業規程、嘱託職員就業規程、研究補助職員就業規程、事務補助職員就業規程に規定する職員をいう。
- (6) 派遣労働者 労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）第26条第1項に規定する労働者派遣契約に基づき本研究所に派遣され、本研究所の業務に従事している者をいう。
- (7) 脅威 情報資産に何らかの障害又は影響を与える原因となるものをいう。

(適用範囲)

第3条 この規程は、本研究所が所管する情報資産を利用する全ての職員及び派遣労働者（以下「職員等」という。）に適用する。

(職員等の責務)

第4条 職員等は、情報セキュリティの重要性を認識し、業務の遂行に当たっては、この規則を遵守しなければならない。

2 職員等は、情報資産の取扱いに当たっては、次に掲げる法令等を遵守しなければならない。

(1) 著作権法(昭和45年法律第48号)

(2) 不正アクセス行為の禁止等に関する法律(平成11年法律第128号)

(3) 公益財団法人九州先端科学技術研究所個人情報保護管理規程、個人情報保護管理・運用基準

(情報セキュリティ対策)

第5条 脅威から情報資産を保護するための情報セキュリティに関する対策(以下「情報セキュリティ対策」という。)は、次に掲げるとおりとする。

(1) 災害、事故等に対する物理的セキュリティ対策

(2) 情報資産の無断持出し、操作ミス等に対する人的セキュリティ対策

(3) 不正アクセス、データ改ざん等に対する技術的セキュリティ対策

(管理体制)

第6条 情報セキュリティを確保するため、次の各号に掲げる職を置き、当該各号に定める職にある者をもって充てる。

(1) 情報セキュリティ最高責任者 研究所長

(2) 情報セキュリティ統括管理者 各部門の長

(3) ネットワーク管理者 研究所長が指定するもの

(4) 情報システム管理者 研究所長が指定するもの

(5) 情報セキュリティ管理者 研究所長が指定するもの

(情報セキュリティ最高責任者)

第7条 情報セキュリティ最高責任者は、情報セキュリティ対策に関する最終決定権限及び責任を有する。

2 情報セキュリティ最高責任者が欠けたときは、副所長が、その職務を代理する。

(情報セキュリティ統括管理者)

第8条 情報セキュリティ統括管理者は、情報セキュリティ対策全般について統括管理する。

(ネットワーク管理者)

第9条 ネットワーク管理者は、本研究所のネットワークの敷設、設定の変更、運用及び見直し（以下「敷設等」という。）並びに当該ネットワークの情報セキュリティ対策に関する権限及び責任を有する。

2 ネットワーク管理者は、本研究所のネットワークの敷設等に携わる職員等並びに当該ネットワークを利用する職員等を指導し、及び監督する。

(情報システム管理者)

第10条 情報システム管理者は、本研究所の情報システムの開発、設定の変更、運用及び見直し（以下「開発等」という。）並びに当該情報システムの情報セキュリティ対策に関する権限及び責任を有する。本研究所の所管する情報システムの開発等に携わる職員等及び当該情報システムを利用する職員等を指導し、及び監督する。

(情報セキュリティ管理者)

第11条 情報セキュリティ管理者は、本研究所の情報セキュリティ対策に関する権限及び責任を有する。

2 情報セキュリティ管理者は、本研究所の情報資産の利用について、本研究所の職員等を指導し、及び監督する。

(実施手順の策定)

第12条 情報セキュリティ最高責任者は、本研究所で行うべき情報セキュリティ対策の詳細を定めた情報セキュリティ実施手順（以下「実施手順」という。）を策定しなければならない。

(情報資産の管理)

第13条 情報セキュリティ管理者は、本研究所の情報資産について、この規程及び実施手順に従い適正な管理を行うよう、本研究所の職員等を指導し、及び監督しなければならない。

2 ネットワーク管理者、情報システム管理者及び情報セキュリティ管理者は、実施手順に従い本研究所の情報資産に応じた情報セキュリティ対策を実施しなければならない。

(情報資産の利用)

第 14 条 職員等は、業務以外の目的で情報資産を利用してはならない。

2 職員等は、情報資産を利用する場合には、実施手順に従い、適正に取り扱わなければならない。

(職員への周知等)

第 15 条 情報セキュリティ最高責任者は、情報資産を取り扱う全ての職員等を対象とした情報の提供や研修を実施し、情報セキュリティの重要性について周知し、及び啓発しなければならない。

(情報セキュリティ監査)

第 16 条 情報セキュリティ最高責任者は、情報セキュリティ対策の実施状況を検証するため、情報セキュリティに関する監査を実施しなければならない。

(侵害への対応)

第 17 条 情報セキュリティ最高責任者は、情報セキュリティに関する事故、障害及び違反行為による情報資産への侵害（以下「侵害」という。）が発生し、又はそのおそれがある場合の対応を定めた手順を策定しなければならない。

2 ネットワーク管理者及び情報システム管理者は、侵害が発生し、又はそのおそれがある場合の対応を定めた具体的な手順を策定しなければならない。

(委任)

第 18 条 この規程に定めるもののほか、この規程に関し必要な事項は、情報セキュリティ最高責任者が定める。

附則

本規程は、令和 2 年 4 月 1 日から施行する。