大学共同利用機関法人高エネルギー加速器研究機構
情報セキュリティ規程

（平成２２年１１月４日
規 程 第 ５０ 号）

改正 平成２９年3月２９日規程第１５号
改正 平成３０年3月２９日規程第２３号

（目的）

第１条　高エネルギー加速器研究機構（以下「機構」という。）は、国内外の多くの研究・教育活動を支えており、これらの活動は様々な情報資産の上に成り立っている。機構における研究・教育活動にとって、情報資産を活用することが不可欠であり、利用環境の利便性を保ちつつ、国内外の大学・研究機関を含む社会からの信頼に応える情報セキュリティを確保することが必須である。この規程は、情報セキュリティに関する管理・利用に係る事項を定め、機構業務の円滑な運営を図ることを目的とする。

（定義）

第２条　本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）　情報とは、情報システム内部に記録された情報、情報システム外部の電磁的記憶媒体に記録された情報、及び情報システムに関する書面情報をいい、特に定めがない限り機構が保有及び管理するものをいう。

（２）　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い、ハードウェア及びソフトウェア、ネットワーク並びに記憶媒体で構成されるものをいう。

（３）　情報資産とは、前二号の定める情報及び情報システムをいう。

（４）　機密性とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。

（５）　完全性とは、情報が破壊、改ざん又は消去されていない特性をいう。

（６）　可用性とは、情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。

（７）　情報セキュリティとは、情報資産の機密性、完全性、可用性を維持することをいう。

（８）　情報セキュリティインシデントとは、機構の情報セキュリティを侵そうとする事柄の発生事象をいう。

（９）　情報セキュリティ関係規程とは、本規程及び本規程に基づき定められるすべての規則類を総称したものをいう。

(10)　情報セキュリティ対策とは、情報セキュリティのために行う対策全般をいう。

(11)　一時来訪者とは、限定された機構の情報資産の利用を一時的に許可された者をいう。
(12)　情報システム利用者とは、機構の情報資産の利用を許可された者（一時来訪者を除く。）をいう。
(13)　J-PARC センターが管理する情報資産とは、J-PARC センターが J-PARC としての情報セキュリティポリシーに基づき、情報セキュリティを管理する情報資産をいう。

（適用範囲）
第３条　この情報セキュリティ規程の適用対象は機構が管理する（賃借、保管を含む。）情報資産とし、人的範囲は情報システム利用者及び一時来訪者とする。
２　J-PARC センターが管理する情報資産については、本規程の対象外とする。
３　機構が管理する以外の情報システム（J-PARC センターが管理する情報システムを含む。）であっても、機構の情報システムに接続した場合は、本規程の対象とする。

（方針）
第４条　機構は、第１条の目的を達成するため、以下の方針を定める。
（１）体制の構築
機構は、機構の情報セキュリティを確保するために必要な体制を構築する。
（２）リスク評価に基づく対策の実施
機構は、機構における情報セキュリティ上のリスクを評価し、必要となる情報セキュリティ対策を講じるための計画及び関係規程を整備した上で、情報セキュリティ対策を実施する。また、リスク評価に変化が生じた場合は、計画及び関係規程を見直す。
（３）教育の実施
機構は、情報セキュリティ対策の有効性を高めるために、情報システムを利用する全ての者に対して、情報セキュリティに関する教育を継続的に実施する。
（４）自己点検及び監査の実施
機構は、情報セキュリティ対策が有効に機能していることを確認及び検証するために、情報セキュリティに関する自己点検及び監査を実施する。
（５）情報セキュリティインシデントへの対応
機構は、情報セキュリティインシデントが発生した場合には、定めた体制及び措置に基づき適切に対応し、機構内外の情報資産を保全する。

（最高情報セキュリティ責任者）
第５条　機構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、機構の情報を担当する理事をもって充てる。
３　最高情報セキュリティ責任者は、機構における情報セキュリティに関する総括的な意

思決定及び責任を有する。
４　最高情報セキュリティ責任者は、自らが担当する業務の一部を、別に定める責任者等に担わせることができる。

（情報セキュリティ委員会）
第６条　機構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の組織は、別に定める。
３　情報セキュリティ委員会は、機構の情報セキュリティに関する最高審議機関として、次の各号に掲げる事項を審議する。
（１）　情報セキュリティ規程及び情報セキュリティ対策基準の策定及び運用に関すること。
（２）　情報セキュリティ確保のための計画、実施、監査、見直しに関連する重要事項の決定に関すること。
（３）　その他情報セキュリティに関連する基本的事項の決定に関すること。
４　この規程に定めるもののほか、情報セキュリティ委員会に関し必要な事項は、別に定める。

（情報セキュリティ監査責任者）
第７条　機構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、機構長が任命する。
３　情報セキュリティ監査責任者は、情報セキュリティに関する法令及び関係規程が遵守されていることを検証するなど、情報セキュリティ監査に関する業務を統括する。

（統括情報セキュリティ責任者）
第８条　機構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が指名する。
３　統括情報セキュリティ責任者は、機構における情報セキュリティ対策の実施に関する業務を統括する。

（情報セキュリティ責任者）
第９条　次の各号に掲げる組織に情報セキュリティ責任者を置く。
２　情報セキュリティ責任者は、当該各号に定める者をもって充てる。
（１）　素粒子原子核研究所及び物質構造科学研究所 所長
（２）　加速器研究施設及び共通基盤研究施設 施設長
（３）　先端加速器推進部 部長
（４）　社会連携部及び機構組織規程第７条に定める室 社会連携部長

（５）　研究支援戦略推進部 部長
（６）　管理局 局長
（７）　上記以外の組織 統括情報セキュリティ責任者
３　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の下で、所管する組織における情報セキュリティ対策の実施に関する業務を統括し、実施責任を有する。
４　情報セキュリティ責任者は、自らが担当する業務の一部を、別に定める責任者等に担わせることができる。

（最高情報セキュリティアドバイザー）
第１０条　機構に最高情報セキュリティアドバイザーを置く。
２　最高情報セキュリティアドバイザーは、情報セキュリティに関する専門的な知識及び経験を有する専門家のうちから、最高情報セキュリティ責任者が指名する。
３　最高情報セキュリティアドバイザーは、最高情報セキュリティ責任者に対して専門的観点から機構の情報セキュリティ対策等について勧告する。

（情報セキュリティインシデント対応チーム　KEK CSIRT）
第１１条　機構に、情報セキュリティインシデント対応チーム（以下「KEK CSIRT」という。）を置く。
２　KEK CSIRT は、計算科学センターが主務を執る。
３　KEK CSIRT は、情報セキュリティインシデントについての機構内外に対する緊急対応窓口として機能するとともに、情報セキュリティインシデントが発生した場合には、被害の拡大を防ぎ、当該情報システムの復旧作業を技術的に支援する。

（リスク評価）
第１２条　最高情報セキュリティ責任者は、第１７条に定める自己点検及び第１８条に定める監査の結果等を勘案した上で、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し、定期的にリスクを評価する。

（情報セキュリティ対策基本計画）
第１３条　最高情報セキュリティ責任者は、機構の情報セキュリティ対策に係る基本的な計画（情報セキュリティ対策基本計画）を定める。

（情報セキュリティ対策基準）
第１４条　最高情報セキュリティ責任者は、情報セキュリティ委員会に諮り、リスク評価を考慮した上で、情報システムのセキュリティ対策を講ずるにあたって、遵守すべき行為及び判断基準を統一的に定めるために、情報セキュリティ対策基準（以下「対策基準」

という。）を策定し、必要に応じて見直す。

（情報セキュリティ対策の実施）

第１５条　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は、対策基準に基づき、情報セキュリティ対策を行う。

（教育）

第１６条　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は、情報システム利用者及び一時来訪者の情報セキュリティ関係規程への理解を深めるために、情報セキュリティに関する教育を行う。

（自己点検）

第１７条　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は、対策基準等の遵守状況等を把握・分析するために、情報セキュリティ対策の自己点検を行う。

（監査）

第１８条　情報セキュリティ監査責任者は、情報セキュリティに関する法令、情報セキュリティ関係規程が遵守されていることを検証するために、監査を実施する。

（情報セキュリティインシデントへの対応）

第１９条　統括情報セキュリティ責任者は、情報セキュリティインシデントに対処するために、適正な体制を構築するとともに、必要な措置を定め実施する。

２　情報セキュリティインシデントの可能性を認知した者は、前項で統括情報セキュリティ責任者が定める措置を実施しなければならない。

（通信の監視）

第２０条　最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、機構の通信回線を通じて行われる通信を監視することができる。ただし、監視で取得した情報は情報セキュリティ対策をする場合及び通信障害を解析する場合に限り利用できる。

２　情報セキュリティ責任者は、所掌する業務に関して、機構の通信回線を通じて行われる通信を監視することができる。ただし、監視で取得した情報は情報セキュリティ対策をする場合及び通信障害を解析する場合に限り利用できる。

（情報システム利用者及び一時来訪者の責務）

第２１条　情報システム利用者及び一時来訪者は、情報セキュリティの重要性について共通の認識をもち、情報セキュリティ関係法令及び情報セキュリティ関係規程を遵守しな

ければならない。
２　機構職員は、機構職員以外の情報システム利用者及び一時来訪者に対して、情報セキュリティ関係法令及び情報セキュリティ関係規程を遵守させるよう努めなければならない。

（例外措置）
第２２条　情報システム利用者は、情報セキュリティ関係規程の適用が、機構の業務の遂行を著しく妨げる場合には、別に定める手順により、最高情報セキュリティ責任者に例外措置の適用を申請することができる。

（雑則）
第２３条　この規程に定めるもののほか、機構の情報セキュリティに関し必要な事項は別に定める。

附 則
この規程は、平成２２年１１月４日から施行する。
附 則（平成２９年３月２９日規程第１５号）
この規程は、平成２９年３月２９日から施行する。
附　則（平成３０年３月２９日規程第２３号）
１．この規程は、平成３０年４月１日から施行する。
２．「大学共同利用機関法人高エネルギー加速器研究機構情報セキュリティポリシー」（平成２２年６月１７日情報セキュリティ委員会決定）は、廃止する。