大学共同利用機関法人　高エネルギー加速器研究機構

J-PARC センター情報セキュリティポリシー

平成 18 年 12 月 27 日
制定

改訂　平成 23 年 5 月 18 日

第 1 章　総則

（目的）

第1条　このセキュリティポリシーは、J-PARC センターの情報システムを J-PARC センター内外の脅威から防御し、J-PARC センターの管理する情報資産を守るために、情報システムのセキュリティ管理に関する取扱い等の基本的事項を定めることを目的とする。

（定義）

第2条　このセキュリティポリシー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（アクセス記録等を含む。）、情報システム外部の電磁的記録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う。ハードウェア及びソフトウェア、ネットワーク並びに記録媒体で構成される。

(3)　情報資産とは、前二号に定める情報及び情報システムをいう。

(4)　機密性とは、アクセスを許可された者だけが、対象の情報にアクセスできる状態を確保することをいう。

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

(6)　可用性とは、情報へのアクセスを許可された者が、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。

(7)　脅威とは、情報資産に影響を与え、損失を発生させる直接の要因をいう。不正アクセスによる情報の改ざんや破壊、ウイルスによる感染事故、自然災害による情報インフラの停止や、過失による情報の漏洩や破壊などを含む。

(8)　情報セキュリティ事象とは、J-PARC センター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)　要機密情報とは、J-PARC センターで取扱う情報（情報システムに関する書面を含む。）のうち、J-PARC センター職員等以外の者に開示することにより J-PARC センターの業務の的確な遂行に支障（軽微なものを除く。）を及ぼすおそれのあるものであり、大学共同利用機関法人高エネルギー加速器研究機構（以下「高エネ機構」という。）の文書処理規程の定めにより秘密文書に区分される情報をいう。

(10)　要保全情報とは、J-PARC センターで取り扱う情報（書面を除く。）のうち、改ざんや破損

等により、J-PARC センターの業務の的確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

(11) 要安定情報とは、J-PARC センターで取り扱う情報（書面を除く。）のうち、滅失や当該情報が利用不可能であること等により、J-PARC センターの業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。

(12) 機器等とは、情報機器又はソフトウェア若しくは情報機器とソフトウェアの総称をいう。

(13) 記録媒体とは、情報機器から取り外しすることが可能な記録装置（磁気テープ、磁気ディスク、光ディスク、カセットテープ、MO、フロッピーディスク、USB メモリ等）をいう。

(14) J-PARC とは、「大強度陽子加速器施設の運営に関する基本協力協定」第２条第１号に規定する施設群をいう。

(15) J-PARC センター職員等とは、J-PARC センターに属する職員、技術開発協力員、嘱託、外来研究員、博士研究員、常用用員等及び派遣労働者をいう。

(16) 高エネ機構の職員等とは、高エネ機構の職員及び職員に準ずる者で J-PARC センター職員等を除く者をいう。

(17) J-PARC 利用者とは、J-PARC センターの管理する情報資産を取り扱う高エネ機構の職員等並びに J-PARC を契約又は協定等の手続により利用する者及び運営に協力する者をいう。

(18) 外部請負業者等とは、高エネ機構との契約及び J-PARC センターとの協定に基づく契約で J-PARC センターの情報資産を取り扱う者をいう。

(19) 情報システム使用者とは、J-PARC に関わる情報システムを使用する J-PARC センター職員等、J-PARC 利用者及び外部請負業者等をいう。

(20) 一時来訪者とは、研究会参加等の目的で J-PARC 及び関連施設に一時的に来訪する者をいう。

(21) JLAN とは、J-PARC センターの管理する基幹ネットワークをいう。

（適用範囲）

第3条 このセキュリティポリシーの適用対象は、J-PARC センターの管理する（賃借、保管を含む。）情報資産とし、人的範囲は J-PARC センター職員等、J-PARC 利用者、外部請負業者等及び一時来訪者とする。また、J-PARC センターが管理する以外の機器等であっても JLAN 及び J-PARC 内にあるネットワークに接続した場合等はこのセキュリティポリシーの対象とする。

（基本方針）

第4条 J-PARC センターにおける情報セキュリティ管理の基本方針は次のとおりとする。

(1) 情報セキュリティと利便性の両立

J-PARC は国際公共財として、研究開発の効率化、利用成果の普及及び産学連携等の推進に必要な情報システムとしての利便性を確保しつつ、J-PARC が原子力の平和利用に関する研究開発の中核的拠点である原子力機構敷地に設置されていることから、国民の安全と信頼に応える情報セキュリティを確保する。

(2)　体制の構築

J-PARC センター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。

(3)　情報セキュリティ意識の共有化と実施

J-PARC センターの管理する情報資産を扱う全ての者が情報セキュリティの重要性について共通の認識を持つとともに、J-PARC の運営及び利用に当たって情報セキュリティに関する法令、規程等を遵守するものとする。また、J-PARC センター職員等は J-PARC 利用者及び外部請負業者等にこれを遵守させる義務を負うものとする。JLAN セキュリティ責任者は一時来訪者に緊急対応手順を遵守させる義務を負うものとする。

(4)　情報資産の分類と管理

情報資産をその内容に応じて分類し、その重要度に応じたセキュリティ管理対策を行うものとする。一時来訪者は、統括情報セキュリティ責任者が利用を認めた情報資産のみ使用できるものとする。

(5)　情報セキュリティ対策

J-PARC センターの管理する情報資産を損傷、妨害等から保護するための物理的な対策、情報セキュリティに関する権限や責任を定め、情報システム使用者に情報セキュリティ対策の内容を周知徹底し、情報システムの監視及び情報セキュリティ対策の遵守状況の確認を実施するものとする。システム開発等を外部委託した場合は、運用面の対策、情報システムの管理・運用等の技術的な対策、情報資産へのアクセス制御、システムの開発及び保守面での対策等を実施するものとする。

(6)　対策基準の策定

情報システムのセキュリティ対策を講ずるに当たって、情報システム使用者及び一時来訪者が遵守すべき行為及び判断の基準を統一的なレベルで定めた基本的な要件を明記した情報システムセキュリティ対策基準を策定するものとする。

(7)　実施手順の策定

情報システムに関するセキュリティ対策を確実に実施していくために、情報システムセキュリティ対策基準の基本的な要件に基づき、情報システムセキュリティ実施手順を策定するものとする。

(8)　緊急対応手順の策定

情報システムに関するセキュリティ障害の発生時に従うべき情報システムセキュリティ緊急対応手順を策定するものとする。

(9)　監査の実施

情報セキュリティに関する法令、規程等が遵守されていることを検証するため、定期的に監査を実施するものとする。

(10)　評価及び見直しの実施

情報セキュリティ監査の結果等及び情報セキュリティを取り巻く状況の変化に鑑み、情報セキュリティ対策の評価を実施するものとする。また、必要に応じ情報セキュリティに関する規程等の見直しを実施するものとする。

第２章　管理体制の構築と運用

（最高情報セキュリティ責任者）

第5条　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者として J-PARC センター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、J-PARC センター長をもって充てる。

3　最高情報セキュリティ責任者は、必要に応じ、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を最高情報セキュリティアドバイザーとして置くことができる。

（J-PARC センター情報セキュリティ委員会）

第6条　J-PARC センターに J-PARC センター情報セキュリティ委員会（以下「委員会」という。）　を置く。

2　委員会は、次の各号に掲げる事項について審議する。また、必要に応じて最高情報セキュリティ責任者に意見具申することができる。

(1) 情報セキュリティ確保のための計画、実施、監査、見直しに関する重要事項

(2) その他 J-PARC センターの情報セキュリティに関する基本的事項

（情報セキュリティ監査責任者）

第7条　情報セキュリティに関する法令、規程等が遵守されていることを検証するため、J-PARC センター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が指名又は委嘱する。

3　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業務を統括する。

（統括情報セキュリティ責任者）

第8条　J-PARC センター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又は委嘱する。

3　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を補佐し、J-PARC センター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、情報システム使用者及び一時来訪者に対する指揮に当たる。

4　統括情報セキュリティ責任者は、情報セキュリティ対策の実施に必要な連絡体制を整備する。情報システム使用者は連絡体制の運用に協力しなくてはならない。

（情報セキュリティ責任者）

第9条　最高情報セキュリティ責任者は、情報セキュリティ対策の運用に係る管理を行う単位を定め、その単位毎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、最高情報セキュリティ責任者が指名又は委嘱する。

3　情報セキュリティ責任者は、所管する単位における情報セキュリティ対策の実施に関して業務を統括し、実施責任を有する。

4　情報セキュリティ責任者は、所管する単位の情報資産を守るために必要と判断したときは、当該情報システムの緊急停止、ネットワークからの遮断等の緊急措置をとることができる。

(JLAN セキュリティ責任者)

第10条　J-PARC センターに JLAN セキュリティ責任者を置く。

2　JLAN 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又は委嘱する。

3　JLAN セキュリティ責任者は、統括情報セキュリティ責任者を補佐し、JLAN の情報セキュリティ対策の実施に当たる。

4　JLAN セキュリティ責任者は、J-PARC センターの情報資産を守るために必要と判断したときは、JLAN の緊急停止措置又は JLAN に接続する情報システムの JLAN からの遮断措置を講ずることができる。

(情報システムセキュリティ責任者)

第11条　情報セキュリティ責任者は、所管する情報システム毎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の管理に関する業務を統括し、当該情報システムのセキュリティ対策の管理責任を有する。

3　情報システムセキュリティ責任者は、所管する単位における情報資産を守るために必要と判断したときは、当該情報システムの緊急停止、ネットワークからの遮断措置等の緊急措置をとることができる。

(情報システム運用管理者)

第12条　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の管理業務において必要な単位ごとに情報システム運用管理者を置く。

2　情報システム運用管理者は、情報システムセキュリティ責任者の指示により、当該情報システムの情報セキュリティ対策を実施する。

(役割の分離)

第13条　情報セキュリティ対策の運用において、次の役割を同じ者が兼務しないものとする。

(1)　情報セキュリティに関し、承認又は許可を要する事案の申請者とその承認者又は許可者

(2)　監査を受ける者とその監査を実施する者

(違反への対応)

第14条　情報システム使用者は、情報セキュリティ関連規程等への重大な違反を知った場合には、当該規定等の実施に責任を持つ情報セキュリティ責任者にその旨　を報告するものとする。

2　各情報セキュリティ責任者は、情報セキュリティ関連規程等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は、違反者及び必要な者に対し、速やかに情報セキュリティの確保に必要な措置をとらせるものとする。

3　各情報セキュリティ責任者は、情報セキュリティ関連規程等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は、統括情報セキュリティ責任者に報告するものとする。

4　統括情報セキュリティ責任者は、必要に応じて違反した当事者の母組織に違反行為について報告する。

（例外措置）

第15条　J-PARC センター職員等は、情報セキュリティ関連規程等の遵守事項をやむを得ない事情により守れない状況が発生した場合は、最高情報セキュリティ責任者による例外の適用承認を受けなければならない。

2　例外措置の申請手続方法及び審査に必要な事項については、最高情報セキュリティ責任者が定める。

（教育）

第16条　統括情報セキュリティ責任者は、講習会の実施等により、情報システム使用者に対し情報セキュリティについて啓発するものとする。

2　情報セキュリティ責任者は、所管する単位における情報システム使用者に情報セキュリティ教育を受講する機会を与える等必要な措置を講ずるものとする。

（情報セキュリティ事象等への対応）

第17条　情報セキュリティ事象の発生時における対処として、以下の事項を実施するものとする。

(1)　情報システム使用者及び一時来訪者は、情報セキュリティ事象を認知した場合、速やかに緊急対応手順に基づきその旨を報告するものとする。

(2)　情報システム運用管理者は、情報セキュリティ事象等を認知した場合、緊急対応手順に基づき被害拡大防止に努めること。

(3)　最高情報セキュリティ責任者は、情報セキュリティ事象等について必要に応じて文部科学省等の関連機関へ報告を行うこと。

2　統括情報セキュリティ責任者又は JLAN セキュリティ責任者は情報セキュリティ事象の対処のため必要な措置をとることができるものとする。

（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、規程等が遵守されていることを検証するため監査を行う者を委嘱し、計画的に監査を行うものとする。

2　監査計画については、予め最高情報セキュリティ責任者の承認を得るものとする。

3　最高情報セキュリティ責任者は、監査の結果に基づき必要に応じて情報セキュリティ責任者　に改善を指示するものとする。

（規程等の見直し）

第19条　委員会は、監査結果や情報セキュリティを取り巻く状況の変化により新たな情報セキュリティ対策が必要となった場合、情報セキュリティ関連規程等の見直しを実施し、必要な見直し内容とその時期について審議するものとする。

第３章　情報の管理

（情報の分類）

第20条　当該情報の機密性、完全性及び可用性の観点(書面については機密性の観点のみ)から当該情報の分類を行うものとする。

2　情報の機密性については、文書管理規程及び文書処理規程の定めに従い分類するものとする。

3　情報の完全性及び可用性については、情報セキュリティ責任者が、当該情報に対する脅威が J-PARC センターの業務に与えるリスクとして勘案し、それぞれ以下のとおり分類するものとする。

(1) 要保全情報

(2) 要安定情報

(3) 一般情報（前二号以外のもの）

（情報の取扱制限）

第21条　要機密文書の取り扱いについては、文書処理規程の定めに従い適切な措置を行うものとする。

2　要保全情報の取り扱いについては、J-PARC センターの業務の的確な遂行に支障を及ぼすことがないように適切な措置を行うものとする。

3　要安定情報については、J-PARC センターの業務の安定的な遂行に支障を及ぼすことがないように適切な措置を行うものとする。

（情報の利用）

第22条　情報システム使用者は、J-PARC センターが管理する情報を、J-PARC の運営又は J-PARC の利用以外の目的で利用してはならない。

第４章　情報セキュリティ対策基準、実施手順及び緊急対応手順

（対策基準）

第23条　情報システムに関する対策を講ずるに当たって、遵守すべき行為及び判断の基準を統一的なレベルで定めた基本的な要件を明記した情報システムセキュリティ対策基準を策定するものとする。

2　情報システムセキュリティ対策基準は、委員会に諮問し、最高情報セキュリティ責任者が別に定める。

（実施手順）

第24条　情報システムに関する対策を確実に実施していくために、情報システムセキュリティ対策基準の基本的な要件に基づき、情報システムセキュリティ実施手順を策定するものとする。

2　情報システムセキュリティ実施手順は、原則として情報セキュリティ責任者が所管する情報システム毎に定める。

（緊急対応手順）

第25条　情報セキュリティ事象が発生した場合に緊急に従うべき、緊急対応手順を、第2章の管理体制に基づき策定するものとする。

2　緊急対応手順は、統括情報セキュリティ責任者が策定するものとする。

附則

このセキュリティポリシーは、平成19年3月20日より施行する。