国立研究開発法人　理化学研究所
情報セキュリティ対策規程

（平成３０年９月１３日規程第６９号）

目次

第１章　総則（第１条－第３条）
第２章　体制（第４条－第１６条）
第３章　情報セキュリティ委員会（第１７条－第２３条）
第４章　情報セキュリティ部会（第２４条－第３１条）
第５章　情報、情報システム及び研究所ネットワークの利用（第３２条・第３３条）
第６章　情報及び情報システムの管理（第３４条－第３９条）
第７章　緊急時の対応（第４０条－第４２条）
第８章　情報セキュリティの運用（第４３条－第５０条）
附　則

第１章　総則

（目的）

第１条　この規程は、国立研究開発法人理化学研究所（以下「研究所」という。）における情報セキュリティ対策を実施するために、政府機関の情報セキュリティ対策のための統一規範（平成２８年８月３１日サイバーセキュリティ戦略本部決定）に基づき、研究所における情報セキュリティの確保に関する基本的な事項を定めることにより、研究所の有する情報資産の保護と活用を図ることを目的とする。

２　この規程に定めるもののほか、この規程を実施するために必要な事項は、情報セキュリティポリシーに基づき情報セキュリティ委員会（以下「委員会」という。）が定める「情報セキュリティ対策基準」及び「情報セキュリティ実施手順」の定めるところによる。

（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、それぞれ当該各号に定めるところによる。

（１）　「情報セキュリティポリシー」とは、研究所における「情報セキュリティ基本方針」及びこの「情報セキュリティ対策規程」（以下「規程」という。）をいう。

（２）　「情報セキュリティ対策基準群」とは、委員会が定めた「情報セキュリティ対策基準」及び「情報セキュリティ実施手順」をいう。

（３）　「部門」とは、別に定める情報セキュリティ対策に係る管理の組織単位をいう。

（４）　「部署」とは、情報セキュリティ対策に係り、部門が定める管理の組織最小単位をいう。

（５）　「役職員」とは、役員及び職員（研究所との間で雇用契約を締結し研究所の業務に従事する者）をいう。

（６）　「外部人材」とは、役職員以外の者をいう。
（７）　「利用者」とは、次号で定める情報、第１０号で定める情報システム及び第１３号で定める研究所ネットワークを利用する役職員及び外部人材をいう。
（８）　「情報」とは、研究所の業務において作成し、収集し、又は取得した情報をいう。
（９）　「情報サービス」とは、情報の加工、蓄積、授受等を行い、利用者に提供することをいう。
（１０）　「情報システム」とは、情報サービスの提供を行うシステム、ハードウェア及びソフトウェアで、研究所の業務に供するものをいう。
（１１）　「所外情報システム」とは、研究所の資産でない情報システムをいう。
（１２）　「ネットワーク」とは、複数のシステムを接続し、協調動作させるための配線、ルータ及びスイッチ等のハードウェア並びにアドレス、プロトコル及びプログラム等のソフトウェアをいう。
（１３）　「研究所ネットワーク」とは、研究所が情報システムを接続し、制御し、及び運用する業務に供するネットワークをいう。
（１４）　「情報セキュリティ」とは、情報、情報システム及び研究所ネットワークが備えるべき次に掲げる性質を健全に保つことをいう。
イ　機密性（アクセスを許可された者だけがこれにアクセスできる状態が確保されていることをいう。）
ロ　完全性（処理方法の正確さ及び完全さが確保されていることをいう。）
ハ　可用性（必要時に中断することなくアクセスできる状態が確保されていることをいう。）
（１５）　「情報セキュリティインシデント」とは、情報の流失、漏えい、改ざん、破壊、障害等により情報、情報システム及び研究所ネットワークの情報セキュリティが損なわれることをいう。

（適用範囲）
第３条　この規程の適用対象とする者は、前条第７号で定める利用者とする。
２　この規程の適用対象とする情報は、前条第８号で定める情報とする。
３　この規程の適用対象とする情報システムは、前条第１０号で定める情報システムとする。
４　この規程の適用対象とするネットワークは、前条第１３号で定める研究所ネットワークとする。

第２章　体制

（最高情報セキュリティ責任者）
第４条　研究所に、最高情報セキュリティ責任者（Chief Information Security Officer。以下「CISO」という。）を置く。
２　CISOは、理事長が指名する。
３　CISOは、研究所における情報セキュリティ対策に関する業務を統括する。

４　CISOは、研究所の情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めなければならない。
５　CISOは、対策推進計画に基づき情報セキュリティ対策を実施しなければならない。
６　CISOは、情報セキュリティ対策に係る管理の単位となる部門を定める。

（最高情報セキュリティ副責任者）
第５条　研究所に、最高情報セキュリティ副責任者（以下「副CISO」という。）を置く。
２　副CISOは、CISOが指名する。
３　副CISOは、CISOを補佐し、CISOに事故等があるときは、その職務を代行する。

（最高情報セキュリティ責任者補佐）
第６条　研究所に、情報セキュリティに関する専門的知見を有する最高情報セキュリティ責任者補佐（以下「CISO補佐」という。）を置く。
２　CISO補佐は、CISOが指名する。
３　CISO補佐は、CISOを補佐し、CISOの命により、その職務の一部を代行する。

（情報セキュリティアドバイザー）
第７条　研究所に、情報セキュリティに関する専門的知見を有する情報セキュリティアドバイザーを置くことができる。
２　情報セキュリティアドバイザーは、CISOが指名又は委嘱する。
３　情報セキュリティアドバイザーは、CISOに情報セキュリティ対策等に関して助言する。

（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、情報化統括責任者（Chief Information Officer。以下「CIO」という。）が指名する。
３　情報セキュリティ監査責任者は、研究所の情報セキュリティ対策の監査を実施し、CIOに報告する。

（統括情報セキュリティ担当部署）
第９条　研究所に、統括情報セキュリティ担当部署を置く。
２　統括情報セキュリティ担当部署は、情報システム部サイバーセキュリティ課とする。
３　統括情報セキュリティ担当部署は、研究所の情報セキュリティ対策に関する業務を行い、各事業所情報システム室は当該業務を補佐する。

（情報セキュリティインシデント対策チーム）
第１０条　研究所に、情報セキュリティインシデント対策チーム（Computer Security Incident Response Team。以下「CSIRT」という。）を置く。
２　CSIRTの構成等については、別に定める。

３　CSIRT は、緊急時の対応において、CISO の業務（情報、情報システム及び研究所ネットワークの利用停止、必要な情報の開示請求並びに協力要請等）を代行する。
４　CSIRT は、研究所で情報セキュリティインシデントが発生又は発生が想定される場合、その対応にあたる。
５　利用者は、CSIRT の情報セキュリティインシデント対応に協力しなければならない。

（部門情報セキュリティ責任者）
第１１条　部門に、部門情報セキュリティ責任者を置く。
２　部門情報セキュリティ責任者は、CISO が指名する。
３　部門情報セキュリティ責任者は、所管部門の情報セキュリティ対策に関する業務を統括する。
４　部門情報セキュリティ責任者は、所管部門の情報セキュリティ責任者、情報セキュリティ担当者及び情報システム管理者に対する連絡網を整備し、CISO に報告する。

（部門情報セキュリティ担当者）
第１２条　部門に、部門情報セキュリティ担当者を置く。
２　部門情報セキュリティ担当者は、CISO と協議の上で部門情報セキュリティ責任者が指名する。
３　部門情報セキュリティ担当者は、部門情報セキュリティ責任者の業務を補佐する。

（情報セキュリティ責任者）
第１３条　部署に、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、部署の長とする。
３　情報セキュリティ責任者は、所管部署の情報セキュリティ対策に関する業務を統括する。
４　情報セキュリティ責任者は、情報セキュリティ担当者又は情報システム管理者を指名又は変更したときは、部門情報セキュリティ責任者に報告する。

（情報セキュリティ担当者）
第１４条　部署に、情報セキュリティ担当者を置くことができる。
２　情報セキュリティ担当者は、情報セキュリティ責任者が指名する。
３　情報セキュリティ担当者は、情報セキュリティ責任者の業務を補佐する。

（情報システム管理者）
第１５条　利用者に情報サービスを提供する情報システムごとに、情報システム管理者を置く。
２　情報システム管理者は、情報セキュリティ責任者が指名する。
３　情報システム管理者は、所管する情報システムにおける情報セキュリティ対策を講じる。

（承認、許可、監査の適正性の確保）

第１６条　役職員は、情報セキュリティ対策の運用において、次に掲げる役割を兼務してはならない。

（１）　承認又は許可（以下「承認等」という。）の申請者と当該承認等を行う者（以下「承認権限者等」という。）

（２）　監査を受ける者とその監査を実施する者

２　役職員は、承認等を申請する場合において、承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得るものとする。

第３章　情報セキュリティ委員会

（委員会の設置）

第１７条　研究所に、情報セキュリティ委員会を設置する。

（職務）

第１８条　委員会は、次に掲げる事項を審議する。

（１）　研究所の情報セキュリティに関する重要事項

（２）　その他委員会が必要と認めた事項

（委員長及び副委員長）

第１９条　委員長は、CISO をもって充てる。

２　委員長は、委員会を代表し、会務を総理する。

３　副委員長は、副 CISO をもって充てる。

４　副委員長は、委員長を補佐し、委員長に事故等あるときは、その職務を代行する。

（委員）

第２０条　委員は、次に掲げる者をもって構成する。

（１）　部門情報セキュリティ責任者

（２）　研究コンプライアンス本部長

（３）　経営企画部長

（４）　総務部長

（５）　情報システム部長

（６）　人事部長

（７）　その他委員長が指名する者

（会議）

第２１条　委員会は、委員長が必要に応じて招集する。

２　委員会は、委員の過半数の出席により成立する。

３　委員長は、必要があると認める場合には、委員以外の者を出席させることができる。

４　前項の出席者は、検討事項につき意見を述べることができる。

（事務局）

第２２条　委員会の事務は、統括情報セキュリティ担当部署が、情報システム部情報化戦略・基盤課の協力を得て行う。

（その他）

第２３条　この規程に定めるもののほか、委員会の運営に必要な事項は、委員長が委員会に諮って定める。

第４章　情報セキュリティ部会

（情報セキュリティ部会の設置）

第２４条　委員会に、委員会の命を受け必要な事項の検討、審議を行わせるために、情報セキュリティ部会（以下「部会」という。）を設置する。

（職務）

第２５条　部会は、委員会の命を受け次に掲げる事項を審議する。

（１）　研究所の情報セキュリティに関する事項

（２）　その他委員会が必要と認めた事項

（部会長及び副部会長）

第２６条　部会長は、CISO をもって充てる。

２　部会長は、部会を代表し、会務を総理する。

３　副部会長は、副 CISO をもって充てる。

４　副部会長は、部会長を補佐し、部会長に事故等あるときは、その職務を代行する。

（委員）

第２７条　委員は、次に掲げる者をもって構成する。

（１）　部門情報セキュリティ責任者のうちから、部会長が指名する者

（２）　総務部長

（３）　研究コンプライアンス本部長

（４）　安全管理部長

（５）　情報システム部長

（６）　その他部会長が指名する者

（会議）

第２８条　部会は、部会長が必要に応じて招集する。

２　部会は、委員の過半数の出席により成立する。

３　部会長は、必要と認める場合には、委員以外の者を部会に出席させることができる。

４　前項の出席者は、検討事項につき意見を述べることができる。

（事務局）

第２９条　部会の事務は、統括情報セキュリティ担当部署が、情報システム部情報化戦略・基盤課の協力を得て行う。

（その他）

第３０条　この規定に定めるもののほか、部会の運営に必要な事項は、部会長が部会に諮って定める。

（作業部会）

第３１条　部会に、特定の事項について検討させるために、作業部会を置くことができる。

２　作業部会に作業部会長を置き、部会長の指名する者をもって充てる。

３　作業部会長は、作業部会の事務を掌理する。

４　作業部会に属すべき者は、部会長が指名する。

第５章　情報、情報システム及び研究所ネットワークの利用

（基本事項）

第３２条　利用者は、情報、情報システム及び研究所ネットワークの利用に際し、関係法令、規程及び情報セキュリティ対策基準群を遵守しなければならない。

２　利用者は、情報セキュリティ責任者が定める情報セキュリティ対策を実施し、情報セキュリティインシデントの発生を防がなければならない。

３　利用者が情報、情報システム及び研究所ネットワークを業務以外の目的で用いること及び不正に用いることは禁止する。

４　利用者は、情報、情報システム及び研究所ネットワークを破損及び亡失してはならない。

（情報の格付けと取扱い）

第３３条　利用者は、情報の作成、更新、収集、取得等に際し、別に定める情報の格付け及び取扱制限を遵守しなければならない。

２　情報セキュリティ責任者は、所管部署における情報の格付け及び取扱制限の運用を監督しなければならない。

３　部門情報セキュリティ責任者は、所管部門における情報の格付け及び取扱制限の運用を監督しなければならない。

第６章　情報及び情報システムの管理

（情報及び情報システムを扱う範囲）

第３４条　情報セキュリティ責任者は、所管の居室、サーバ室等の施設に係る情報セキュリティ対策が必要な範囲（以下「管理区域」という。）及びその特性に応じた情報セキュリティ対策を定め、利用者に周知し、並びに遵守させなければならない。

２　情報セキュリティ責任者は、所管部署の管理区域における情報セキュリティ対策を運用し監督しなければならない。

３　部門情報セキュリティ責任者は、所管部門の管理区域における情報セキュリティ対策を監督しなければならない。

（情報及び情報システムの管理）

第３５条　情報セキュリティ責任者は、所管の情報及び情報システムにおける情報セキュリティ対策を定め、運用し、並びに監督しなければならない。

２　情報セキュリティ責任者は、情報及び情報システムにおける情報セキュリティインシデントの発生を防がなければならない。

３　情報セキュリティ責任者及び情報システム管理者は、管理者権限を不正に用いてはならない。

４　情報セキュリティ責任者及び情報システム管理者は、情報及び情報システムの運用に係る記録を保持しなければならない。

５　部門情報セキュリティ責任者は、所管部門における情報及び情報システムの情報セキュリティ対策を監督しなければならない。

（情報及び情報システムの利用終了）

第３６条　情報セキュリティ責任者は、情報及び情報システムの利用を終了、廃棄、返却、譲渡等する場合は、情報の漏えい等を防ぐための措置を講じなければならない。

（外部情報サービスの利用）

第３７条　利用者が、外部情報サービスを研究所の業務に供する場合は、情報セキュリティ責任者の許可を受け、この規程を遵守し情報セキュリティインシデントの発生を防がなければならない。

２　情報セキュリティ責任者は、外部情報サービスを研究所の業務に供する場合は、統括情報セキュリティ担当部署に報告しなければならない。

（情報システムの持ち出し）

第３８条　利用者は、情報システムを管理区域外に持ち出す場合は、情報セキュリティ責任者の許可を受け、管理区域外においてもこの規程を遵守しなければならない。

（所外情報システムの業務利用）

第３９条　利用者は、所外情報システムにおいて研究所の情報を取り扱う場合は、この規程を遵守しなければならない。

２　情報セキュリティ責任者は、利用者に所外情報システムを管理区域に持ち込ませ、研究所ネットワークを利用させる場合は、別に定める手続きにより、この規程を遵守していることを確認しなければならない。

３　情報セキュリティ責任者は、研究所の情報を取り扱う所外情報システムの利用を終了する場合は、当該情報システムに記録された研究所の情報が消去されていることを確認しなければならない。ただし、情報セキュリティ責任者の許可を受けた場合及び別の定めがある場合を除く。

第７章　緊急時の対応

（緊急時の連絡）

第４０条　利用者が、情報セキュリティインシデントを発見し又は発生の連絡を受けた場合は、直ちに別に定める窓口に通報しなければならない。

２　利用者は、発見し又は発生の連絡を受けた情報セキュリティインシデントの被害拡大防止策を可能な限り実施すること。

（緊急時の対応）

第４１条　情報セキュリティ責任者及び情報システム管理者が、情報セキュリティインシデントを発見し又は発生の連絡を受けた場合は、被害拡大の防止処置を速やかに実施しなければならない。

（事後の対応）

第４２条　情報セキュリティ責任者及び情報システム管理者は、情報セキュリティインシデントの再発防止計画（以下「再発防止計画」という。）を策定、実施し、部門情報セキュリティ責任者に報告しなければならない。

２　部門情報セキュリティ責任者は、部会に再発防止計画を報告しなければならない。

３　部会は、報告された再発防止計画に基づいて、当該情報システムの運用、利用再開について審査する。

第８章　情報セキュリティの運用

（教育）

第４３条　CISO は、利用者に対し、対策推進計画で定める情報セキュリティ教育（以下「教育」という。）を実施しなければならない。

２　利用者は、CISO が実施する教育を受けなければならない。

（情報セキュリティに関する知見等の収集）

第４４条　CISO は、情報セキュリティに関する知見等を収集し、利用者に周知しなければならない。

（監視等）

第４５条　CISO は、研究所ネットワークにおいて情報セキュリティインシデントを検知、監視するための措置を講じなければならない。

２　CISO は、研究所の情報、情報システム及びネットワークを監視することができる。

（警告等）

第４６条　CISO は、この規程の遵守状況について利用者に報告を求めることができる。

２　CISO は、この規程に違反する利用者、利用者を監督する情報セキュリティ責任者及び部門情報セキュリティ責任者に対して、警告し、改善を求めることができる。

（利用等の制限）

第４７条　CISO は、この規程に違反する利用者、利用者を監督する情報セキュリティ責任者及び部門情報セキュリティ責任者に対し、情報、情報システム及び研究所ネットワークの運用及び利用を制限することができる。

（外部人材）

第４８条　情報セキュリティ責任者は、外部人材に情報、情報システム及び研究所ネットワークを利用させる場合は、この規程を遵守させ、監督しなければならない。

２　部門情報セキュリティ責任者は、所管部門の各部署が受け入れる外部人材における情報セキュリティ対策を監督しなければならない。

（外部委託等）

第４９条　利用者は、情報の作成、加工、集計等の業務、情報システムの開発、運用及び管理等の業務を研究所外に委託する場合は、予め情報セキュリティ責任者の承認を得なければならない。

２　情報セキュリティ責任者は、委託先における情報の漏えいや改ざん、破壊等を防止する情報セキュリティ対策に係る要件を定め、調達仕様に記載させるとともに、当該委託業務を適切に実施させなければならない。

３　情報セキュリティ責任者は、情報システムの調達において、既知の脆弱性の有無、不正な情報システムの納入を防止する等、情報セキュリティ対策に係る要件を定め、調達仕様に記載させるとともに、適切に実施させなければならない。

４　部門情報セキュリティ責任者は、所管部門の各部署が実施する外部委託及び情報システムの調達における情報セキュリティ対策を実施させなければならない。

（点検、監査の実施及び継続的改善）

第５０条　CISO は、第４条第５項に規定する情報セキュリティ対策の実施状況を点検・評価しなければならない。

２　CIO は、第８条第３項に規定する監査により判明した要改善事項について、CISO に勧告する。

３　CISO は、前項の要改善事項について、対策推進計画の見直しを行い、CIO に報告しなければならない。

４　CISO は、第１項に規定する点検・評価の結果及び第２項に規定する勧告並びに情報セキュリティに係る重大な変化等を踏まえて、必要に応じて対策推進計画の見直しを行う等、研究所の情報セキュリティ対策を改善しなければならない。

附　則

この規程は、平成３０年１０月１日から施行する。