○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）

**改正** 令和２年３月１１日規程第２４６号　令和３年３月２４日規程第３８０号
令和３年３月２９日規程第３９９号　令和４年３月２４日規程第５０７号
令和５年１０月３１日規程第１０８号　令和６年８月２９日規程第１８５号
令和７年３月３１日規程第１４３号　令和７年４月２４日規程第１８１号

目次



## 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、政府機関等のサイバーセキュリティ対策のための統一基準群に基づき、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。

（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）　部門　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。

（２）　部署　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。

（３）　役職員　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。

（４）　外部人材　役職員以外の者をいう。

（５）　情報　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。

（６）　情報サービス　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。

（７）　情報システム　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。

（８）　所外情報システム　研究所の資産でないPC、サーバ、スマートフォン、タブレット端末、USBメモリ等の情報システムをいう。

（９）　ネットワーク　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。

（１０）　研究所ネットワーク　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。

（１１）　利用者　情報、情報システム及び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。

（１２）　情報セキュリティ　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。）

（１３）　情報セキュリティインシデント　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。

（１４）　外部サービス　研究所外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において研究所の情報が取り扱われる場合に限る。

## 第２章　体制

（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（Chief Information Security Officer。以下「CISO」という。）を置き、理事長が指名する者をもって充てる。

２　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。

３　CISOは、研究所の情報セキュリティ対策推進計画を定め、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。

４　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。

（情報セキュリティ技術統括者）

第４条　研究所に、情報セキュリティ技術統括者（Chief Information Security Technical Officer。以下「CISTO」という。）を置き、理事長が指名する者をもって充てる。

２　CISTOは、研究所における情報セキュリティ対策に関する理事長及びCISO の技術的業務を、専門的観点から補佐する。

３　CISTOは、CISOと協議の上、情報セキュリティインシデントの重大度を判断し、重大度に応じて理事長及びCISOと密に連携し、被害拡大防止に向けた対応にあたる。

（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。）を置き、CISOが指名する者をもって充てる。

２　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、最高情報セキュリティ責任者補佐（以下「CISO補佐」という。）を置き、情報セキュリティに関する専門的知見を有する者のうちからCISOが指名する。

２　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、情報セキュリティに関する専門的知見を有する者のうちから、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　内部監査室長は、情報セキュリティ監査責任者として、研究所の情報セキュリティ対策の監査を行い、CISOに報告する。
（統括情報セキュリティ担当部署）
第９条　情報セキュリティ・システム部（以下「情シス部」という。）は、統括情報セキュリティ担当部署として、研究所の情報セキュリティ対策に関する業務を行う。
（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の運営に係る事務は、情シス部が行う。
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。
（CSIRTの組織）
第１１条　CSIRTは、次に掲げる構成員５名以上で組織する。
（１）　情シス部の職員のうちから情報セキュリティ・システム部長が指名する者
（２）　その他CISOが指名する者
（CSIRT責任者、副責任者）
第１２条　CSIRTにCSIRT責任者及びCSIRT副責任者を置き、それぞれCISOが指名する者をもって充てる。
２　CSIRT責任者に事故があるときは、CSIRT副責任者が、その職務を代行する。
（CSIRTの職務）
第１３条　CSIRTは、次の各号に掲げる活動を行う。
（１）　情報セキュリティインシデント発生に際し、情報を収集し事象を正確に把握する。
（２）　被害拡大の防止、復旧、再発の防止に係る技術的支援や助言を行う。
（３）　研究所内及び関係各機関との連絡、調整、情報セキュリティインシデントに関する情報の共有を行う。
（４）　研究所内で発生した情報セキュリティインシデントを取りまとめ、対策及び予防策に関する支援を行う。
（５）　情報セキュリティインシデントへの対処能力を向上させるため、必要に応じてCSIRT構成員に対し研修や訓練などを実施する。
２　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。
３　CSIRTは、その活動に関し、必要となる専門部署に意見を求めることができる。
（部門情報セキュリティ責任者）
第１４条　部門に、部門情報セキュリティ責任者を置き、CISOが指名する者をもって充てる。

２　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し、監督する。

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１５条　部門に、部門情報セキュリティ担当者を置き、部門情報セキュリティ責任者が CISO と協議して指名する。

２　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１６条　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し、監督する。

２　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１７条　部署に、情報セキュリティ担当者を置き、情報セキュリティ責任者が指名する者をもって充てる。

２　情報セキュリティ担当者は、情報セキュリティ対策に関し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１８条　利用者に情報サービスを提供する情報システム及び所管する外部サービスごとに、情報システム管理者を置き、情報セキュリティ責任者が指名する者をもって充てる。

２　情報システム管理者は、所管する情報システム及び外部サービスにおける情報セキュリティ対策を講じる。

（区域情報セキュリティ責任者）

第１９条　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。）に対応して、区域情報セキュリティ責任者を置く。

２　区域情報セキュリティ責任者は、次の各号に掲げる場合に応じ、当該各号に掲げる者をもって充てる。

（１）　一つの管理区域を一つの部署で使用する場合　情報セキュリティ責任者

（２）　一つの管理区域を複数の部署で使用する場合　事業部長が指名する者

３　区域情報セキュリティ責任者は、管理区域の情報セキュリティ対策に関する業務を統括し、監督する。

（承認、許可、監査の適正性の確保）

第２０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

（設置）

第２１条　研究所に、情報セキュリティに関する重要事項等について検討、審議するため、情報セキュリティ委員会（以下「委員会」という。）を置く。

（委員）

第２２条　委員会は、次に掲げる委員で組織する。

（１）　CISO

（２）　副 CISO

（３）　情報統合本部長

（４）　情報セキュリティ・システム部長

（５）　総務部長

（６）　研究インテグリティ・経済安全保障部長

（７）　部門情報セキュリティ担当者のうち委員長が指名する者

（８）　その他委員長が指名する者

（委員長及び副委員長）

第２３条　委員会に委員長を置き、CISO をもって充てる。

２　委員長は、会務を掌理する。

３　委員会に副委員長を置き、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。

（会議等）

第２４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　情報セキュリティ監査責任者は、委員会に出席して意見を述べることができる。

４　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。

５　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。

６　委員会の事務は、情シス部が行う。

## 第４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２５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、この規程並びに委員会が定める情報セキュリティ対策基準群（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制限）

第２６条　利用者は、情報の作成、更新、収集、取得等に際し、情報セキュリティ実施手順で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。

## 第５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２７条　情報セキュリティ責任者及び区域情報セキュリティ責任者は、管理区域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。

（情報及び情報システムの管理）

第２８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、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。

（情報及び情報システムの利用終了）

第２９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。

（外部サービスの利用）

第３０条　利用者が、次項に規定する許可を得ずに外部サービスを研究所の業務に供することを禁止する。

２　情報セキュリティ責任者は、利用者に外部サービスの研究所業務への供用を許可するに当たっては、当該利用者が外部サービスの利用要件やこの規程を遵守することを確認するとともに、情シス部に事前相談し、許可後に利用登録をしなければならない。

（情報システムの持ち出し）

第３１条　利用者が、次項に規定する許可を得ずに情報システムを管理区域外に持ち出すことを禁止する。

２　情報セキュリティ責任者は、利用者に情報システムの管理区域外への持ち出しを許可するに当たっては、情報セキュリティ実施手順の手続きにより、利用者が当該持ち出す情報システムについて管理区域外においてもこの規程を遵守することを確認するとともに、情シス部に登録しなければならない。

（所外情報システムの業務利用）

第３２条　利用者が、次項に規定する許可を得ずに所外情報システムを業務に利用すること及び所外情報システムで研究所の情報を取り扱うことを禁止する。

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の業務利用及び所外情報システムでの研究所の情報の取り扱い、あるいは所外情報システムの管理区域への持ち込み及び研究所ネットワークへの接続を許可するに当たっては、情報セキュリティ実施手順の手続きにより、利用者がこの規程を遵守することを確認するとともに、許可後、情シス部に登録しなければならない。

３　情報セキュリティ責任者は、利用者が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、研究成果有体物取扱規程（平成１８年規程第１０号）及び研究成果有体物の提供及び受領について（平成１８年通達第８号）の規定に基づいて、情報を提供する場合及び転出に伴い外部機関に移転する場合は除く。

## 第６章　緊急時の対応

（緊急時の対応）

第３３条　利用者は、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、直ちに所属長及びCSIRT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しなければならない。

３　情報セキュリティ責任者及び情報システム管理者は、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３４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、委員会に再発防止計画を報告しなければならない。

３　委員会は、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７章　その他

（教育等）

第３５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を実施しなければならない。

２　利用者は、前項の情報セキュリティ教育を受けなければならない。

３　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３６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３７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３８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３９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。

（業務委託等）

第４０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、業務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業務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４１条　CISOは、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　CISOは、点検・評価の結果及び監査の結果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、情報セキュリティ対策の継続的な改善を図るものとする。

附　則

この規程は、平成３０年１０月１日から施行する。

附　則（令和２年３月１１日規程第２４６号）

この規程は、令和２年４月１日から施行する。

附　則（令和３年３月２４日規程第３８０号）

この規程は、令和３年４月１日から施行する。

附　則（令和３年３月２９日規程第３９９号）

この規程は、令和３年４月１日から施行する。

附　則（令和４年３月２４日規程第５０７号）

この規程は、令和４年４月１日から施行する。

附　則（令和５年１０月３１日規程第１０８号）

この規程は、令和５年１１月１日から施行する。

附　則（令和６年８月２９日規程第１８５号）

この規程は、令和６年９月１日から施行する。

附　則（令和７年３月３１日規程第１４３号）

この規程は、令和７年４月１日から施行する。

附　則（令和７年４月２４日規程第１８１号）

この規程は、令和７年５月１日から施行する。