

大学共同利用機関法人自然科学研究機構情報セキュリティ対策に関する基本規程

平成28年9月23日

自機規程第111号

目次

- 第1章 総則（第1条－第4条）
- 第2章 組織（第5条－第19条）
- 第3章 情報資産の保護（第20条）
- 第4章 情報システムのライフサイクル（第21条）
- 第5章 インシデントへの対処（第22条）
- 第6章 ネットワークの監視等（第23条－第24条）
- 第7章 情報セキュリティ監査・点検（第25条－第26条）
- 第8章 情報セキュリティポリシー等の見直し（第27条）
- 第9章 雑則（第28条）

第1章 総則

（目的）

第1条 この規程は、大学共同利用機関法人自然科学研究機構（以下「機構」という。）情報セキュリティ確保基本方針（平成28年役員会決定。以下「基本方針」という。）に基づき、機構における情報セキュリティを確保し、もって機構の情報資産の円滑な運用と保護に資することを目的とする。

（情報セキュリティ対策方針）

第2条 機構は、基本方針の目的を達するため、以下の情報セキュリティ対策方針を遵守し、対策を行う。

- 一 情報セキュリティ管理体制の構築及び整備
- 二 情報セキュリティ対策の実施に必要な経費の確保
- 三 情報資産及び個人情報の保護
- 四 役職員等、情報システム利用者に対する情報セキュリティ教育、訓練及び啓発活動の実施
- 五 情報セキュリティポリシーや関連規程の組織への浸透
- 六 情報システムのセキュリティの維持及び向上
- 七 情報セキュリティインシデント対応体制及び手順書等の整備
- 八 ネットワークの監視及び利用情報の取得

- 九 情報機器の管理状況の把握及び必要な措置の実施
- 十 情報セキュリティ対策に係る自己点検，監査の実施及びその結果に基づく情報セキュリティポリシーの見直し等
- 十一 その他機構を取り巻く情報セキュリティ上の脅威等に応じた対策
(定義)

第3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。

- 一 ネットワーク 通信回線，ルータ等の通信機器をいう。
- 二 情報システム ハードウェア及びソフトウェアから成るシステムであつて，情報処理又は通信の用に供するもの（スーパーコンピュータ，サーバ，パソコン，モバイル端末，汎用機，ソフトウェア等（オペレーティングシステムを含む。），情報の作成，利用及び管理等のためのハードウェア及びソフトウェア等）をいい，特に断りのない限り，機構が調達又は開発するもの（管理を外部委託しているシステム及び外部サービスを含む。）をいう。
- 三 情報施設・設備 コンピュータ室，通信分岐盤，配電盤，電源ケーブル，通信ケーブル等をいう。
- 四 電磁的記録媒体 サーバ装置，端末，通信回線装置等に内蔵される内蔵電磁的記録媒体と，USBメモリ，外付けハードディスク，光学ドライブ，磁気テープ等の外部電磁的記録媒体をいう。
- 五 ネットワーク及び情報システムで取り扱う情報 ネットワーク，情報システムで取り扱うデータ（これらを印刷した文書を含む。）をいう。
- 六 システム関連文書 システム設計書，プログラム仕様書，オペレーションマニュアル，端末管理マニュアル，ネットワーク構成図等をいう。
- 七 情報資産 ネットワーク，情報システム，情報施設・設備，電磁的記録媒体，ネットワーク及び情報システムで取り扱う情報及びシステム関連文書をいう。
- 八 情報セキュリティ 別表第1に定める情報資産の分類に基づき，機密性，完全性及び可用性を維持することをいう。
- 九 情報セキュリティポリシー 基本方針，本規程及び第5条第3項に基づき最高情報セキュリティ責任者（Chief Information Security Officer。以下「CISO」という。）が定める大学共同利用機関法人自然科学研究機構セキュリティ対策基準（以下「対策基準」という。）をいう。
- 十 実施規則 情報セキュリティポリシーに基づきCISOが定める規則及び計画をいう。
- 十一 インシデント 情報セキュリティに関し，意図的又は偶発的に生じる，機構の諸規程又は法律に違反する事故若しくは事件をいう。

- 十二 個人情報 大学共同利用機関法人自然科学研究機構個人情報保護規程（平成17年自機規程第54号）に規定する個人情報をいう。
- 十三 各機関 大学共同利用機関法人自然科学研究機構組織運営通則（平成16年通則第1号。以下「組織運営通則」という。）第2条第1項に定める大学共同利用機関をいう。
- 十四 各機関等 別表第2に掲げる機関等区分をいう。
- 十五 役職員等 役員及び機構が定める就業規則に基づき雇用されている全ての者をいう。
- 十六 共同利用・共同研究者等 機構の情報資産を利用する前号に掲げる者以外の全ての者をいう。
- 十七 電磁的記録 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。
- 十八 研究情報 第5号及び第6号に掲げる情報等のうち、研究活動（分析等を含む。）により生じた情報をいう。

（対象範囲）

- 第4条 情報セキュリティポリシーの適用範囲は、次の各号に規定する範囲とする。ただし、CISOが対策基準で定めるものを除く。
- 一 機構が所有又は管理する情報資産
 - 二 機構が所有又は管理するネットワーク及び情報システムに接続された情報機器で、前号に該当しないもの
 - 三 機構との契約又は協定に基づき提供される情報資産
 - 四 第1号若しくは前号に規定する情報資産又は第2号に規定する情報機器を利用する者（役職員等及び共同利用・共同研究者等以外の者を含む。以下同じ。）が、機構の研究、教育その他の業務のために作成又は取得した情報で、当該情報システム又は情報機器に記憶させたもの
 - 五 役職員等及び共同利用・共同研究者等が、機構の研究、教育その他の業務のために作成又は取得した情報で、前2号に該当しないもの
- 2 前項各号に規定する情報資産を運用、管理又は利用する者は、情報セキュリティポリシーを遵守しなければならない。

第2章 組織

（最高情報セキュリティ責任者）

- 第5条 機構にCISOを置き、情報担当理事又は情報担当副機構長をもって充てる。

- 2 C I S Oは、機構の情報資産の開発、管理、運用及び情報セキュリティ対策（以下「情報セキュリティ対策等」という。）に関する総括的な権限及び責任を有する。
- 3 C I S Oは、基本方針及び本規程に定める事項を適切に実施するため、対策基準に関する全権を有し、これを制定しなければならない。
- 4 C I S Oの職務及び職責については、対策基準で定める。

（機関最高情報セキュリティ責任者）

第6条 別表第2のとおり機関最高情報セキュリティ責任者（以下「機関C I S O」という。）を置く。

- 2 機関C I S Oは、所掌する組織における情報セキュリティ対策等の実施に関し総括する。
- 3 機関C I S Oの職務及び職責については、対策基準で定める。

（情報セキュリティ監査室）

第7条 機構における情報セキュリティポリシーの遵守を監査するため、機構に情報セキュリティ監査室を置き、次の各号の者をもって組織する。

- 一 情報セキュリティ監査責任者
- 二 情報セキュリティ監査実施者

- 2 情報セキュリティ監査責任者を情報セキュリティ監査室長とする。
- 3 情報セキュリティ監査室の職務は、次の各号に掲げるものとする。
 - 一 機構における情報セキュリティ監査手順及び監査計画を策定すること。
 - 二 機構における情報セキュリティ監査を実施すること。
 - 三 情報セキュリティ監査の結果を報告書としてまとめること。
 - 四 その他機構における情報セキュリティ監査に関すること。

- 4 その他情報セキュリティ監査室に関する必要な事項は、情報セキュリティ監査室長が定める。

（情報セキュリティ監査責任者）

第8条 情報セキュリティ監査責任者は、機構の役職員等のうちから、機構長が指名する。

- 2 情報セキュリティ監査責任者は、第25条に定める情報セキュリティ監査に関し統括する。

（情報セキュリティ監査実施者）

第9条 情報セキュリティ監査実施者は、役職員等のうちから、情報セキュリティ監査責任者が指名する。

- 2 前項の規定にかかわらず、情報セキュリティ監査責任者が必要と認めた場合は、機構長の承諾を得て、民間の専門家等機構外部の者を情報セキュリティ監査実施者としてとることができる。
- 3 情報セキュリティ監査実施者は、被監査部門から独立した者でなければならない。

4 情報セキュリティ監査実施者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

5 情報セキュリティ監査実施者は、情報セキュリティ監査責任者の指示に基づき、第25条に定める監査を実施する。

(情報セキュリティアドバイザー)

第10条 機構に、必要に応じて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識及び経験を有する機構職員のうちから、CISOが委嘱する。

3 前項の規定にかかわらず、CISOが必要と認めた場合は、機構長の承諾を得て、民間の専門家等機構外部の者を情報セキュリティアドバイザーとすることができる。

4 情報セキュリティアドバイザーの業務内容は、CISOが定める。

(情報セキュリティ責任者)

第11条 機関CISOの下に、情報セキュリティ責任者を置き、機関CISOが指名する者をもって充てる。

2 情報セキュリティ責任者の職務及び職責については、対策基準で定める。

(CSIRT)

第12条 機構に、CSIRT (Computer Security Incident Response Team) を置く。

2 CSIRTは、次項に定める機関CSIRTにより構成する。

3 機関CISOの下に、機関CSIRTを置き、機関CISOが指名する者をもって組織する。

4 機関CISOは、機関CSIRTとして、役職員等のほか、派遣、業務委託による者を指名することができる。ただし、役職員等の中から1名以上を指名しなければならない。

5 CSIRT及び機関CSIRTの職務及び職責については、対策基準で定める。

(情報システム管理者)

第13条 機関CISOの下に、情報システム管理者を置き、機関CISOが指名する者をもって充てる。

2 情報システム管理者は、複数置く事ができるが、1つの情報システムにおける情報システム管理者は1名としなければならない。ただし、機関CISOが必要と認めた場合はこの限りではない。

3 機関CISOは、ネットワーク、情報システム及び外部電磁的記録媒体(第4条第1項第1号及び第3号に該当するものに限る。以下「管理情報システム等」という。)を運用する場合は、情報システム管理者を指名しなければならない。

4 機関CISOは、前項に掲げる管理情報システム等以外のネットワーク、情報システム及び外部電磁的記録媒体等について、必要に応じて情報システム管理者を指名するこ

とができる。

5 情報システム管理者の職務及び職責については、対策基準で定める。

(情報システム担当者)

第14条 情報システム管理者の指示等に従い、情報資産の開発、設定の変更、運用、更新等の作業を行う者を、情報システム担当者とする。

2 情報システム担当者は、情報システム管理者が指名する者をもって充てる。

(技術責任者等)

第15条 機関CISOは、必要に応じて情報システム副管理者、情報セキュリティ技術責任者、情報セキュリティ副技術責任者等を置くことができる。

2 前項に必要な事項は、当該機関の機関CISOが定める。

(情報セキュリティ管理者)

第16条 機関CISOの下に、情報セキュリティ管理者を置き、大学共同利用機関法人自然科学研究機構法人文書管理規程（平成16年自機規程第50号）第5条に規定する文書管理者をもって充てる。

2 情報セキュリティ管理者は、その所掌する課室等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。

(情報セキュリティ委員会)

第17条 組織運営通則第12条の6に基づき、機構にCISOを委員長とする情報セキュリティ委員会を置き、情報セキュリティポリシー等機構全体の情報セキュリティ対策等に関する重要な事項、危機管理に関する事項及び倫理に関する事項を決定する。

2 前項に規定する委員会の組織運営に関し必要な事項については、別に定める。

(機関情報セキュリティ委員会)

第18条 各機関等における個別に対策すべき情報セキュリティ対策等を行うため、各機関等に機関CISOを委員長とする機関情報セキュリティ委員会を置き、機関等における情報セキュリティポリシー等の情報セキュリティ対策等に関する重要な事項を決定する。

2 前項に規定する委員会の組織運営に関し必要な事項については、機関CISOが別に定める。

(兼務の禁止)

第19条 情報セキュリティ対策の実施において、原則として以下の役割を同じ者が兼ねることができない。

一 承認又は許可を受ける者とその承認又は許可を行う者（ただし、機関CISOが認めた場合を除く。）

二 監査を受ける者とその監査を行う者

2 前項にかかわらず、CISOは情報セキュリティ監査責任者を兼務することができる。

第3章 情報資産の保護

(情報資産の分類・格付け及び取扱制限)

第20条 情報セキュリティ管理者は、所掌する情報資産について、別表第1に規定する情報資産の分類・格付けと取扱制限に基づき、機密性、完全性及び可用性に分類するとともに適切な格付けを行い、取扱制限を実施しなければならない。

2 研究情報について、別表第1に規定する情報資産の分類・格付け及び取扱制限を行うことが著しく不合理であると機関CISOが認めるときは、機関CISOは別途これを規定することができるものとする。

3 第1項の規定の適用に関し必要な事項は、対策基準で定める。

第4章 情報システムのライフサイクル

(情報システムのライフサイクル)

第21条 機構が所有又は管理する情報システムの設置、運用及び廃棄に関し必要な事項は、対策基準で定める。

第5章 インシデントへの対処

(インシデントへの対処)

第22条 インシデントへの対処に関し必要な事項は、対策基準で定める。

第6章 ネットワークの監視等

(ネットワークの監視)

第23条 第4条第1項第1号若しくは第3号の情報資産又は同項第2号の情報機器を管理、運用又は利用する者は、ネットワークを通じて行われる通信を傍受してはならない。ただし、CSIRT、セキュリティ確保を目的として、CISO又は機関CISOがあらかじめ指名した者及びネットワークを管理する情報システム管理者（所掌範囲に限る。）（以下「ネットワーク監視者」という。）は、ネットワークを通じて行われる通信の監視（以下「監視」という。）を行うことができる。

2 前項のネットワーク監視者は、機構又は機構外に対する重大なセキュリティ侵害を防止するために必要として対策基準で定める場合を除き、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。

3 監視の範囲、手続及び監視によって採取した記録の取扱いその他必要な事項は、対策

基準で定める。

(利用の記録)

第24条 情報システムの利用記録の採取及び取扱いについては、対策基準で定める。

第7章 情報セキュリティ監査・点検

(監査)

第25条 情報セキュリティ監査責任者は、情報セキュリティポリシー、実施規則の実施状況及び情報資産に対する情報セキュリティ対策状況について、毎年度定期に、又は必要に応じて随時に監査を行うものとする。

2 外部委託事業者に委託している場合、情報セキュリティ監査責任者は外部委託事業者から下請けとして受託している事業者も含めて、必要に応じて情報セキュリティポリシーの遵守についての監査を行うものとする。

3 情報セキュリティ監査責任者は、監査を行うに当たっては、監査計画を策定し、機構長及びCISOの承認を得るものとする。

4 情報セキュリティ監査責任者は、監査を実施した場合は、監査結果を取りまとめ、機構長及びCISOに報告するものとする。

5 情報セキュリティ監査責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

(自己点検)

第26条 機関CISOは、年に1回以上、当該機関における情報セキュリティポリシー及び実施規則の実施状況について自己点検を行い、CISOに報告するものとする。

第8章 情報セキュリティポリシー等の見直し

(ポリシー及び実施規則の更新)

第27条 CISOは、第25条の監査及び前条の自己点検の結果並びに機構におけるインシデントを勘案し、定期的に情報セキュリティポリシー及び実施規則の見直しを行うものとする。

第9章 雑則

(その他)

第28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、対策基準で定める。

附 則

- 1 この規程は、平成28年9月23日から施行する。
- 2 大学共同利用機関法人自然科学研究機構業務の情報化及び情報セキュリティの確保に関する基本規程（平成19年自機規程第67号）は、廃止する。

附 則

この規程は、平成28年12月22日から施行する。

附 則

この規程は、平成30年3月1日から施行する。

附 則

この規程は、平成30年4月1日から施行する。

附 則

この規程は、平成30年11月1日から施行する。

附 則

この規程は、令和元年12月1日から施行する。

附 則

この規程は、令和2年12月4日から施行する。

附 則

この規程は、令和4年11月24日から施行する。

附 則（令和5年2月16日改正）

この規程は、令和5年4月1日から施行する。

別表第1 情報資産の分類・格付けと取扱制限（第3条，第20条関係）

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性4 (極秘)	国の安全保障に関わるもの, 特定個人情報など, 内容が漏洩した場合, 機構の業務への影響が深刻かつ重大な情報資産	機密性3の取扱制限に加えて, 機関CISOの許可がある場合を除き下記の措置 <ul style="list-style-type: none"> 複製及び配付禁止 指定場所以外でのアクセスの禁止 運用は, スタンドアロン又は独立したネットワークの範囲に限定
機密性3 (秘密)	機構で取り扱う情報資産のうち, 秘密文書に相当する機密性を要する情報資産	機密性2の取扱制限(例外措置を除く。)に加えて, 機関CISOの許可がある場合を除き下記の措置 <ul style="list-style-type: none"> 機構の資産である情報システム端末以外での作業の原則禁止 必要以上の複製及び配付禁止 電磁的記録媒体の施錠可能な場所への保管
機密性2 (機構外秘)	機構の業務で取り扱う情報資産のうち, 秘密文書に相当する機密性は要しないが, 漏えいにより, 個人の権利が侵害され又は機構業務の遂行に支障を及ぼすおそれがある情報資産(本分類区分で取扱うことを本人が承諾した個人情報を含む。)	<ul style="list-style-type: none"> 保管場所の制限, 保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 情報の送信, 情報資産の運搬・提供時における暗号化・パスワード設定又は鍵付きケースへの格納 復元不可能な処理を施しての廃棄 信頼のできるネットワーク回線の選択 外部で情報処理を行う際の安全管理措置の規定

分類	分類基準	取扱制限
		<p>【例外措置】</p> <p>対策基準で例外措置の定めがある場合は、上記にかかわらず対策基準の例外措置を適用する。</p>
機密性 1 (公開)	公表済みの情報, 公表しても差し支えない情報等, 機密性 2 以上の情報資産以外の情報資産	

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性 3	破損, 改ざんにより, 復旧が困難な情報資産であり, かつ機構業務に深刻かつ重大な影響を与える情報資産	<p>完全性 2 の取扱制限に加えて下記の措置</p> <ul style="list-style-type: none"> ・保管地域を異にする複数バックアップ ・電子署名, ハッシュ値の保管, 時刻認証等による改ざん検出又は防止対策の実施
完全性 2	機構で取り扱う情報資産のうち, 改ざん, 誤びゅう又は破損により, 個人の権利が侵害される又は機構業務の適確な遂行に支障 (軽微なものを除く。) を及ぼすおそれがある情報資産で完全性 3 に該当しない情報資産	<ul style="list-style-type: none"> ・バックアップ ・電子署名, ハッシュ値の保管, 時刻認証等による改ざん検出又は防止対策の実施。¹ただし, 機関 C I S O が認めた場合を除く。 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性 1	完全性 2 以上の情報資産以外の情報資産	

¹ 改ざんできない媒体 (WORM メディアなど) を用いる場合における当該媒体にかかる改ざん防止対策は不要である。

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性 3	常時使用が可能でなければ機構業務に深刻かつ重大な影響を与える情報資産	可用性 2 の取扱制限に加えて下記の措置 <ul style="list-style-type: none"> ・フェイルオーバー，フェールセーフに基づくクラスタリング構成
可用性 2	機構で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が 1 時間から 24 時間程度利用不可能であることにより、個人の権利が侵害される又は機構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資産で可用性 3 に該当しない情報資産	<ul style="list-style-type: none"> ・バックアップ，指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性 1	可用性 2 以上の情報資産以外の情報資産	

別表第2（第6条関係）

機関等区分	機 関 等	機関C I S O
国立天文台	国立天文台	国立天文台長が指名する副台長
核融合科学研究所	核融合科学研究所	核融合科学研究所副所長
岡崎3機関等	基礎生物学研究所	3所長が一致して指名する副所長又は研究総主幹
	生理学研究所	
	分子科学研究所	
	岡崎3機関共通の研究施設及び組織等	
	生命創成探究センター	
事務局等	事務局並びに組織運営通則第2条の2第1項及び第3条に定める組織等のうち、上記に該当しない組織等	C I S Oが兼務

注：組織運営通則第2条の2第1号に掲げる共創戦略統括本部及び同条第2号に掲げるアストロバイオロジーセンターについて、機関等の施設に設置された研究室等については、当該機関等の機関C I S Oが所掌するものとする。