大学共同利用機関法人自然科学研究機構情報システム運用基準

平成２０年４月１日
情報化統括責任者決定

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。）における情報システムの運用については，この運用基準の定めるところによる。

（適用範囲）

１．この運用基準は，情報システムを運用・管理・利用するすべての者に適用する。

（定義）

２．この運用基準において，次の各号に掲げる用語は，それぞれ当該各号の定めるところによる。

一　情報システム

機構における情報処理及び情報ネットワークに係るシステムをいう。

二　情報ネットワーク

情報ネットワークとは次のものをいう。

（１）機構により，所有又は管理されているすべての情報ネットワーク

（２）機構との契約又は協定に従って提供されるすべての情報ネットワーク

三　情報

情報とは次のものをいう。

（１）情報システム内部に記録された情報

（２）情報システム外部の電磁的記録媒体に記録された情報

（３）情報システムに関係がある書面に記載された情報

四　ポリシー

機構が定める情報システム基本方針及び本運用基準をいう。

五　実施規程

ポリシーに基づいて策定される規程及び計画をいう。

六　手順

実施規程に基づいて策定される具体的な手順やマニュアルをいう。

七　各機関等

機構本部，国立天文台，核融合科学研究所及び岡崎地区（基礎生物学研究所，生理学研究所，分子科学研究所，岡崎共通研究施設及び岡崎統合事務センター）のことをいう。

八　役職員

機構に勤務する役員及び職員（派遣職員を含む。）をいう。

九　学生等

機構の規程等に定める大学院学生，研究生，研究員，研修生及び研究者等をいう。

十　利用者

役職員及び学生等で，情報システムを利用する許可を受けて利用するものをいう。

十一　臨時利用者

役職員及び学生等以外の者で，情報システムを臨時に利用する許可を受けて利用するものをいう。

十二　情報セキュリティ

情報資産の機密性，完全性及び可用性を維持することをいう。

十三　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，コンピュータによる情報処理の用に供されるものをいう。

十四　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，機構の定める規程又は法律に反する事故又は事件をいう。

（情報化統括責任者）

３－１．情報システムの運用に責任を持つ者として，機構に情報化統括責任者（以下「ＣＩＯ」（Chief Information Officer）という。）を置き，機構長が指名する理事又は副機構長をもって充てる。

３－２．ＣＩＯは，以下の各号に定める業務を行う。

一　ポリシー，実施規程及び手順（以下「ポリシー等」という。）の策定や情報システム上での各種問題に対する処置を行う。

二　機構内で行う情報システムに関する教育を統括する。

三　ＣＩＯに事故があるときは，ＣＩＯがあらかじめ指名する者が，その職務を代行する。

四　必要に応じて，情報セキュリティに関する専門的な知識及び経験を有した専門家を，情報システムに関して助言を行える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。

（情報化・セキュリティ連絡会）

４－１．ＣＩＯは，情報システムの円滑な運用・管理に関する事項（以下「各事項」という。）について，情報化・セキュリティ連絡会に諮った上で，各事項について判断をしなければならない。

４－２．情報化・セキュリティ連絡会に関し必要な事項については，別に定める。

（情報化責任者）

５－１．各機関等に置く情報化責任者（以下「機関ＣＩＯ」という。）は，各機関等の長

の推薦を受け（岡崎地区においては，基礎生物学研究所，生理学研究所，分子科学研究所の長が推薦する１名），ＣＩＯが指名した者をもって充てる。

５－２．機関ＣＩＯは，以下の各号に定める業務を行う。

一　ＣＩＯの指示により，情報システムの整備と運用に関し，ポリシー等の実施を行う。

二　各機関等において，情報システムの運用に携わる者及び利用者に対して，情報システムの運用及び利用並びに情報セキュリティに関する教育を企画し，ポリシー等の遵守を確実にするための教育を実施する。

三　各機関等の情報セキュリティに関する連絡と通報において当該情報システムを代表する。

四　各機関等における運用方針の決定や情報システム上での各種問題に対する処置を担当する。

五　機関ＣＩＯの業務を補佐させるため，情報化責任者補佐（機関ＣＩＯ補佐）を指名することができる。

（情報セキュリティ監査責任者）

６－１．適正な情報セキュリティを確保するために，情報セキュリティ監査責任者を置き，ＣＩＯが指名する者をもって充てる。また，必要に応じて，各機関等にそれぞれ情報セキュリティ監査責任者を置くことができる。

６－２．情報セキュリティ監査責任者は，ＣＩＯの指示に基づき，監査に関する事務を統括する。

（事務部署）

７－１．情報システムの事務部署は，事務局企画連携課とする。

７－２．事務部署は，ＣＩＯの指示により，以下の各号に定める事務を行う。

一　各機関等における情報システムの運用と利用におけるポリシー等の実施状況の取りまとめ

二　講習計画，リスク管理及び非常時行動計画等の実施状況の取りまとめ

三　各機関等における情報セキュリティに関する連絡と通報

（各機関等の情報セキュリティに関する委員会）

８－１．各機関等に情報セキュリティに関する委員会を置く。

８－２．各機関等の情報セキュリティに関する委員会は，以下の各号に掲げる事項を実施する。

一　各機関等におけるポリシー等の遵守状況の調査及び周知徹底

二　各機関等におけるリスク管理及び非常時行動計画の策定及び実施

三　各機関等におけるインシデントの再発防止策の策定及び実施

四　各機関等における技術担当者向け教育の計画及び企画

８－３．各機関等の情報セキュリティに関する委員会に関し必要な事項については，別に定める。

（各機関等の技術担当者）

９－１．機関ＣＩＯは，複数の技術担当者を指名して実務を担当させることができる。

９－２．技術担当者は，機関ＣＩＯの指示により，各機関等の情報システムの運用の技術的実務を担当し，利用者への教育を補佐する。

（役割の分離）

１０．情報セキュリティ対策の運用において，以下の役割を同じ者が兼務しないこと。

一　承認又は許可事案の申請者とその承認者又は許可者

二　監査を受ける者とその監査を実施する者

（情報の格付け）

１１．ＣＩＯは，情報システムで取り扱う情報について，電磁的記録については機密性，完全性及び可用性の観点から，書面については機密性の観点から当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備する。

（機構外の情報セキュリティ水準の低下を招く行為の禁止）

１２－１．ＣＩＯは，機構外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規程を整備する。

１２－２．情報システムを運用・管理・利用する者は，原則として，機構外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

（情報システム運用の外部委託管理）

１３．ＣＩＯ又は機関ＣＩＯは，情報システムの運用業務のすべて又はその一部を第三者に委託する場合には，当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

（監査）

１４．情報セキュリティ監査責任者は，情報セキュリティ対策が手順に従って実施されていることを監査する。監査に関しては，別に定める監査規程に従う。

（見直し）

１５－１．ポリシー等を整備した者は，ポリシー等の見直しを行う必要性の有無を適時検討し，必要があると認めた場合にはその見直しを行う。

１５－２．情報システムを運用・管理・利用する者は，自ら実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には，当該事項の見直しを行う。