情報・システム研究機構情報セキュリティ対策規程

（令和３年１０月１８日
制　　定）

（目的）

第１条　この規程は，情報・システム研究機構情報セキュリティ基本方針に基づき，大学共同利用機関法人情報・システム研究機構（以下「機構」という。）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に関する基本的な事項を定め，もって機構の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

（定義）

第２条　この規程において使用する用語は，情報・システム研究機構情報セキュリティ基本方針において使用する用語の例による。

（最高情報セキュリティ責任者）

第３条　機構に最高情報セキュリティ責任者（以下「最高責任者」という。）を置き，機構長が指名した理事をもって充てる。

２　最高責任者は，機構内の情報セキュリティ対策に関する事務を統括するとともに，その責任を負う。

３　最高責任者は，代理を指名し，権限を一時委譲することができる。

（最高情報セキュリティアドバイザー）

第４条　機構に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最高情報セキュリティアドバイザー（以下「アドバイザー」という。）を置き，最高責任者が指名した者をもって充てる。

２　アドバイザーは，最高責任者を補佐するとともに，情報セキュリティポリシー（以下「ポリシー」という。）の運用，評価及び見直しについて専門的な助言を行うものとする。

（情報セキュリティ監査責任者）

第５条　機構に，情報セキュリティ監査責任者（以下「監査責任者」という。）を置き，最高責任者が指名した者をもって充てる。

２　監査責任者は，最高責任者の指示に基づき，機構における情報セキュリティの監査に関する事務を統括する。

（各研究所等の情報セキュリティ責任者）

第６条　各研究所等に情報セキュリティ責任者（以下「各研究所等責任者」という。）を置き，最高責任者が指名した者をもって充てる。

２　各研究所等責任者は，機構における情報セキュリティ対策に関する事務について最高

責任者を補佐するとともに，当該研究所等における情報セキュリティ対策に関する事務を統括する。

3　最高責任者は，各研究所等責任者の代理を指名することができる。

（情報システムセキュリティ責任者）

第７条　各研究所等責任者は，所管する情報システムごとに情報システムセキュリティ責任者（以下「システム責任者」という。）を置かなければならない。

2　システム責任者は，所管する情報システムにおける情報セキュリティ対策に関する事務を統括する。

3　各研究所等責任者は，システム責任者を置いたとき及び変更したときは，最高責任者に報告する。

4　最高責任者は，機構のすべてのシステム責任者に対する連絡網を整備する。

5　各研究所等責任者は，システム責任者の代理を指名することができる。

（情報システムセキュリティ管理者）

第 8 条　システム責任者は，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セキュリティ管理者（以下「システム管理者」という。）を置く。

2　システム管理者は，所管する情報資産の管理業務における情報セキュリティ対策を実施する。

3　前項の実施に当たっては，システム責任者が定めた手順及び判断した事項に従って行うものとする。

4　システム責任者は，システム管理者を置いたとき及び変更したときは，各研究所等責任者を通じて，最高責任者に報告する。

5　最高責任者は，各研究所等のすべてのシステム管理者に対する連絡網を整備するものとする。

6　システム責任者は，システム管理者の代理を指名することができる。

（課室等情報セキュリティ責任者）

第９条　各研究所等責任者は，その所管する各課室等に課室等情報セキュリティ責任者（以下「課室等責任者」という。）を置き，原則として各課室等の長をもって充てる。

2　課室等責任者は，その所管する課室等における情報セキュリティ対策に関する事務を統括する。

3　最高責任者は，すべての課室等責任者に対する連絡網を整備する。

4　各研究所等責任者は，課室等責任者の代理を指名することができる。

（情報セキュリティ委員会）

第１０条　機構の情報セキュリティ対策に関する事項は，機構情報セキュリティ委員会において審議し，重要事項の決定等を行う。

２　各研究所等に，各研究所等の情報セキュリティ対策全般を審議するための委員会を置く。
３　前項の委員会には，機構情報セキュリティ委員会において各研究所から選出されている委員を含まなければならない。

（ＲＯＩＳ　ＣＳＩＲＴ）
第１１条　組織運営規則第２８条の６に定めるＲＯＩＳ　ＣＳＩＲＴは，各研究所等のＣＳＩＲＴと連携して次の各号に掲げる業務を行う。
一　情報セキュリティインシデントの発生又はその疑いがある場合における，重篤性及び緊急性の判断
二　重篤性及び緊急性のあるインシデントが発生又はその疑いがある場合における，該当研究所等への連絡及び初動指示
三　重篤性及び緊急性のあるインシデントが発生又はその疑いがある場合における，本部危機管理室への連絡等
四　インシデントの状況等に応じた，関係者への被害拡大の防止・復旧・再発防止にかかる技術的支援及び助言
五　文部科学省への連絡
六　外部専門機関等からの情報セキュリティインシデントに係る情報の収集
七　他機関等への情報セキュリティインシデントに係る情報の共有
八　情報セキュリティインシデント発生状況の定期的とりまとめ及び機構情報セキュリティ委員会への報告
２　ＲＯＩＳ　ＣＳＩＲＴは次の各号に掲げる者をもって組織する。
一　各研究所等責任者が推薦する者
二　本部事務部主幹（情報基盤担当）
三　本部事務部総務課情報基盤係長
３　前項のほか，ＲＯＩＳ　ＣＳＩＲＴに専門的な助言を行うＲＯＩＳ　ＣＳＩＲＴアドバイザーを置くことができる。
４　前項までに定めるもののほか，ＲＯＩＳ　ＣＳＩＲＴについて必要な事項は別に定める。

（リスク評価と対策）
第１２条　最高責任者は，保有する情報及び利用する情報システムに係る脅威の発生の可能性及び顕在時の損失等を分析し，リスクを評価するものとする。
２　最高責任者は，前項の評価結果を踏まえ，次の各号に掲げる事項を含む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「対策等基本計画」という。）を定めなければならない。
一　情報セキュリティに関する教育・研修計画

二　情報セキュリティ対策の自己点検計画
三　前各号に掲げるもののほか，情報セキュリティ対策に関する重要な取組
3　各研究所等責任者は，前項の対策等基本計画に基づき情報セキュリティ対策を実施するとともに，実施状況を評価し，その結果を最高責任者に報告するものとする。
4　最高責任者は，第１項の評価に変化が生じた場合や，情報セキュリティに係る重大な変化が生じた場合には，情報セキュリティ対策及び対策等基本計画の見直しを行わなければならない。

（実施手順書の作成）
第１３条　ポリシーに基づき，情報セキュリティ対策を実施するに当たり，各研究所等においては，実施手順書及び関連する資料（以下，「実施手順書等」という。）を作成するものとする。

（違反行為への対処）
第１４条　利用者は，情報セキュリティ関係規程への重大な違反を知った場合には，各規程の実施に責任を持つ各研究所等責任者に報告するものとする。
2　各研究所等責任者は，情報セキュリティ関係規程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には，速やかに調査を行い，事実を確認するものとする。ただし，事実の確認に当たっては，可能な限り当該行為を行った者の意見を聴取しなければならない。
3　調査によって違反行為が判明したときは，各研究所等責任者は次の各号に掲げる措置を講ずることができる。
一　当該行為者に対して当該行為の中止命令
二　システム責任者に対して当該行為に係る利用の遮断命令
三　システム責任者に対して当該行為者のアカウント停止命令，又は削除命令
四　機構情報セキュリティ委員会への報告
五　その他法令に基づく措置
4　各研究所等責任者は，前項の措置を講じたときは，遅滞なく最高責任者に報告しなければならない。

（例外措置）
第１５条　ポリシーを含む情報セキュリティ関係規程の適用が機構の研究教育及び業務の適正な遂行を著しく妨げる等の理由により，情報セキュリティ関係規程の定めとは異なる代替の方法を採用する場合又は規程を実施しないことを認めざるを得ない場合については，予め定められた例外措置のための手続により，行うものとする。
2　前項に規定する例外措置のための手続については，各研究所等で別に定める。
3　各研究所等責任者は，利用者による例外措置の適用の申請を，各研究所等で定めた審査手続に従って審査し，許可の可否を決定する。

4　各研究所等責任者は，前項の例外措置の適用を決定する際には，次の各号に掲げる事項を含む例外措置の適用審査記録を整備するものとする。

一　審査した者の情報（氏名，役割名，所属，連絡先）

二　申請内容

三　審査結果の内容

5　各研究所等責任者は，例外措置の適用審査記録の台帳を整備し，例外措置の適用審査記録の参照について，情報セキュリティ監査を実施する者からの求めに応じて提出するものとする。

6　各研究所等責任者は，例外措置の申請状況を踏まえ，第１３条に定める実施手順等の見直しの検討を行う。

（教育・研修）

第１６条　最高責任者は，利用者が情報セキュリティ関係規程に関する理解を深め，情報セキュリティ対策を適切に実践できるよう，情報セキュリティ対策の教育を実施するものとする。

2　各研究所等責任者は，第１２条第２項に定める対策等基本計画に基づき，利用者に対して教育・研修を実施するものとする。

3　課室等情報セキュリティ責任者は，当該課室等の職員に対し，情報セキュリティ対策のために，各研究所等責任者の実施する教育・研修への参加の機会を付与する等の必要な措置を講じなければならない。

4　利用者は，対策等基本計画に従って，適切な時期に研修を受講する。

（情報セキュリティインシデントの対応）

第１７条　情報セキュリティインシデント発生時には，各研究所等において別に定める情報セキュリティインシデントの対応手順に基づき，対処する。

2　各研究所等責任者は，前項の情報セキュリティインシデントの対応手順を整備するとともに，情報セキュリティインシデントが発生した場合には，当該対応手順に基づき，被害の拡大を防ぐとともに，情報セキュリティインシデントから復旧するための体制を整備する。

3　各研究所等責任者は，情報セキュリティインシデントについて利用者から各研究所等責任者への報告手順を整備し，当該報告手順を利用者に周知する。

4　各研究所等責任者は，情報セキュリティインシデントに備え，研究教育・業務の遂行のため特に重要と認めた情報システムについて，そのシステム責任者及びシステム管理者の緊急連絡先，連絡手段，連絡内容を含む緊急連絡網を整備する。

5　最高責任者は，情報セキュリティインシデントについて関係行政機関等の外部から報告を受けるための窓口を設置し，その窓口への連絡手段を外部に対して公表する。

6　利用者は，情報セキュリティインシデントの発生を知った場合には，それに関係する者

に連絡するとともに，各研究所等責任者が定めた報告手順により，各研究所等のＣＳＩＲＴ及び課室等責任者に報告する。

7　各研究所等責任者は，情報セキュリティインシデントが発生した場合には，その原因を調査するとともに再発防止策を策定し，その結果を報告書として最高責任者に報告する。

8　最高責任者は，前項の報告を受けた場合には，その内容を確認し，再発防止策を実施するために必要な措置を講ずるものとする。

（利用者が保有する情報の閲覧等）

第１８条　機構の情報資産を利用することにより，当該利用者が保有することとなった情報については，情報システムの運用に不可欠な範囲又は情報セキュリティインシデントの対応に不可欠な範囲において，当該情報システムを所管する各研究所等責任者が閲覧，複製又は提供（以下「閲覧等」という。）できるものとする。

2　閲覧等を行う手続及び範囲等については，各研究所等で別に定める。

（情報セキュリティ対策の自己点検）

第１９条　各研究所等責任者は，第１２条第２項に定める対策等基本計画に基づき，情報セキュリティ対策について，自己点検票及び自己点検の実施手順を整備し，自己点検を実施する。

2　各研究所等責任者は，自らが実施した自己点検の結果に基づき，自己の権限の範囲において改善を行い，その結果を最高責任者に報告する。

3　最高責任者は，各研究所等責任者からの報告に基づき，自己点検の結果を評価し，必要があると判断した場合には各研究所等責任者に対して改善を指示し，改善結果の報告を受ける。

（情報セキュリティ対策の監査）

第２０条　監査責任者は，ポリシー及びポリシーに基づく手順が確実に遵守され，問題点が改善されることを目的として，定期に，又は随時に監査を行い，その結果を最高責任者に報告するものとする。

2　前項の監査は，情報・システム研究機構内部監査規程に準じて行うものとする。

3　最高責任者は，監査責任者からの報告に基づき，監査結果を評価し，必要があると判断した場合には各研究所等責任者に対して改善を指示する。

（ポリシー等の見直し）

第２１条　最高責任者は，第１２条第３項に定める情報セキュリティ対策実施状況評価の結果，第１９条第２項に定める自己点検の結果及び第２０条第１項に定める監査の結果等を総合的に評価するとともに，情報セキュリティに係る重大な変化等を踏まえ，機構情報セキュリティ委員会の審議を経て，ポリシー及び情報セキュリティ関係規程等について必要な見直しを行う。

２　各研究所等責任者は，第１２条第３項に定める情報セキュリティ対策実施状況評価の結果，第１９条第２項に定める自己点検の結果及び第２０条第１項に定める監査の結果等に基づき，各研究所等で定める実施手順書等について適時見直し，見直し結果について最高責任者に報告するものとする。

（雑則）

第２２条　ポリシーに定めるもののほか，情報セキュリティ対策に関して必要な事項は，実施手順書等のほか，必要に応じて，各研究所等において別に定める。

附　則

１　この規程は，令和３年１０月１８日から施行する。