情報・システム研究機構 情報セキュリティポリシー

平成３０年１月２６日　役員会決定

（前文）

昨今，Ｗｅｂサーバー等への攻撃，ファイル共有ソフトの利用やコンピュータウィルス等に起因する情報漏洩，スパイウェアによる不正アクセス等のサイバー犯罪等が発生している中で，政府としては官民における統一的・横断的な情報セキュリティ対策を推進するため，「第１次情報セキュリティ基本計画」（2006 年 2 月 2 日，情報セキュリティ政策会議決定）を策定し，さらに，政府機関の情報セキュリティ対策の強化・拡充を図るため「政府機関の情報セキュリティ対策のための統一基準」（2005 年 12 月 13 日同会議決定）を策定し，政府関係機関の情報セキュリティ水準の斉一的な引き上げを図ることが必要であるとされている。

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。）は，国立極地研究所，国立情報学研究所，統計数理研究所及び国立遺伝学研究所の４つの研究所が，極域科学，情報学，統計数理，遺伝学のナショナルセンターとしての使命に加えて，生命，地球，環境，社会などに関わる複雑な問題を情報とシステムという観点から総合的に捉え，実験・観測による多種・大量のデータからの情報の抽出，真理の発見，データベースの構築とその活用方法の開発などの諸課題に関して，分野の枠を超えた総合科学としての融合的な研究を通して，新分野の開拓を図ろうとしている。このような機構の使命を果たしていくためには，機構が保有する情報と情報システム（以下「情報資産」という。）は必要不可欠な基盤となっており，その安全性及び信頼性を確保することは極めて重要な責務である。

Ⅰ．情報セキュリティの基本方針

（目的）

第１条　機構における研究・教育活動に資する情報資産の安全性及び信頼性を確保するとともに，未来に向けてより高度で自由な情報通信の開発と利用を実践するため，機構に「情報・システム研究機構情報セキュリティポリシー」（以下「本ポリシー」という。）を策定するものである。

（法令等の遵守）

第２条　情報資産の取扱いに関しては，法令及び規制等（以下「関連法令等」という。）においても規定されているため，情報セキュリティ対策を実施する際には本ポリシーのほか関連法令等を遵守しなければならない。

（適用範囲）

第３条　本ポリシーは，機構の役員，職員及び客員教員，並びに外部委託業者，及び学生等で機構の情報資産を利用する者（以下「利用者」という。）に適用される。

（利用者の義務）

第４条　利用者は，本ポリシーに沿って利用し，各研究所等で定める実施手順等を遵守しなければならない。

（用語の定義）

第５条　本ポリシーにおいて，次の各号に掲げる用語は，当該各号の定めるところによる。

一　各研究所等

機構に置く各研究所，データサイエンス共同利用基盤施設及び本部をいう。

二　課室等

各研究所等において，情報セキュリティ対策を組織的に実施する課，室，研究系及びセンター等の最小限の組織の単位をいい，当該組織の単位については，各研究所等において，それぞれ別に定める。

三　情報システム

情報処理及び情報ネットワークに係わるシステムをいう。

四　情報ネットワーク

情報ネットワークには次のものを含むものとする。

（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）　機構との契約あるいは他の協定に従って提供されるすべての情報ネットワーク

五　情報

情報には次のものを含むものとする。

（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

２　前項で定めた用語のほかは，「政府機関の情報セキュリティ対策のための統一基準（平成２８年度版)」の用語の定義を準用するものとする。

Ⅱ．組織と体制

（最高情報セキュリティ責任者）

第６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，機構長が指名する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７条　機構に，情報システムに関する技術や事案に対する対処等の専門的な知見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，最高責任者が指名する者をもって充てる。

２　アドバイザーは，最高責任者を補佐するとともに，本ポリシーの運用，評価，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８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。）１名を置き，最高責任者が指名する者をもって充てる。

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９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。）をそれぞれ１名置き，最高責任者が指名する者をもって充てる。

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１０条　各研究所等責任者は，所管する情報システム毎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対する情報セキュリティ対策の管理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時及び変更した時は，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ものとする。

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１１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毎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。）を置くものとする。

２　システム管理者は，所管する管理業務における情報セキュリティ対策を実施する。なお，実施に当たってはシステム責任者によって定められた手順や判断された事項に従って行うものとする。

３　システム責任者は，システム管理者を置いた時及び変更した時は，各研究所等責任者を通して，最高責任者に報告する。

４　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。

５　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１２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。）１名を置き，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　各研究所等責任者は，すべての課室等責任者に対する連絡網を整備するものとする。
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１３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，各研究所等が管理する情報システム及び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１３条の２　組織運営規則第２８条の６に定めるＲＯＩＳ　ＣＳＩＲＴは，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　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　第９条に定める各研究所等責任者が推薦する者
二　戦略企画本部ＵＲＡステーションマネージャー（情報基盤担当）
三　戦略企画本部ＵＲＡステーション情報基盤係長
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　この他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１４条　各研究所等責任者は，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　各研究所等責任者は，前項の評価の結果を踏まえ，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「対策推進計画」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年次自己点検計画

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　各研究所等においては，前項の対策推進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，各研究所等責任者は，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　各研究所等責任者は，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推進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１５条　本ポリシーに基づき，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，以下の事項に係る実施手順等を作成するものとする。

一　情報資産の運用管理

二　情報資産を利用する者の管理

三　情報資産の障害等の管理

（違反行為への対処）

第１６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に違反すると被疑される行為が認められるときは，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の利用停止命令，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，上記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１７条　本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こと又は規程を実施しないことを認めざる得ない場合につい

ては，あらかじめ定められた例外措置のための手続により，行うこととする。
２　前項で規定するあらかじめ定められた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　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　決定を審査した者の情報（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１５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１８条　最高責任者は，機構の利用者に対して，情報セキュリティ対策の教育を通じて，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にするものとする。
２　各研究所等責任者は，第１４条第２項に定める対策推進計画に基づき，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，対策推進計画に従って，適切な時期に研修を受講する。（障害等の対応）
第１９条　障害等発生時には，各研究所等において別に定める障害等の対応手順に基づき，対処する。
２　各研究所等責任者は，前項の障害等の対応手順を整備するとともに，障害等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，障害等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，障害等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，障害等に備え，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，障害等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，障害等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，課室等責任者に報告する。

７　各研究所等責任者は障害等が発生した場合には，障害等の原因を調査し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，その内容を検討し，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２０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障害等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２１条　各研究所等責任者は，第１４条第２項に定める対策推進計画に基づき，所管する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，自己の権限の範囲で改善できると判断したことは改善し，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，自己点検の結果を全体として評価し，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。

（情報セキュリティ対策の監査）

第２２条　監査責任者は，本ポリシーの実施状況を確認するために，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　前項の監査の実施に当たっては，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，監査結果を全体として評価し，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。

（本ポリシー等の見直し）

第２３条　機構情報セキュリティ委員会は，第１４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２１条第３項に定める自己点検の結果及び第２２条第１項に定める監査の結果等に基づき，本ポリシーの実効性を評価し，必要な部分を見直して内容の変更を行い，よりセキュリティレベルの高いかつ遵守可能なポリシーに更新する。

２　各研究所等責任者は，第１４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２１条第２項に定める自己点検の結果及び第２２条第１項に定める監査の結果等に基づき，情報セキュリティ対策，対策推進計画及び各研究所等で定める実施手順等

について適時見直しを行うものとする。

（罰則）

第２４条　利用者が故意若しくは重大な過失により著しく本ポリシー等に違反した場合，又はネットワークに関する法令等の遵守事項の違反行為に該当する場合において，処分を行う場合には次の各号に基づきこれを行うものとする。

一　行為者が研究教育職員の場合は，情報・システム研究機構懲戒規程及び情報・システム研究機構研究教育職員の就業の特例に関する規程に基づき行うものとする。

二　行為者が研究教育職員以外の職員の場合は，情報・システム研究機構懲戒規程に基づき行うものとする。

２　機構の職員以外で機構の情報資産を利用する者（学生及び外部委託業者を含む）については，関係法令，規程及び契約等に基づき，処分等を行うものとする。

（雑則）

第２５条　本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，第１５条において各研究所等で定めるとした実施手順のほか，必要に応じて，各研究所等において別に定める。

附　則

本ポリシーは，平成１９年６月２２日から施行する。

附　則

本ポリシーは，平成２６年５月２０日から施行する。

附　則

本ポリシーは，平成２６年１０月２９日から施行する。

附　則

本ポリシーは，平成２８年１２月１９日から施行し，平成２８年４月１日から適用する。

附　則

本ポリシーは，平成３０年４月１日から施行し，平成２９年６月１日から適用する。