国立大学法人奈良先端科学技術大学院大学
情報セキュリティポリシー

令和５年２月１日

改正履歴

改正日	改正内容
平成１８年６月２２日	初版策定
平成２２年８月１日	総合情報基盤センター設置に伴う改正
平成２４年４月１日	組織名称の変更に伴う改正
平成２５年１２月１日	緊急時の連絡体制の追加に伴う改正
平成２６年１２月１日	ポリシーの対象範囲の追加に伴う改正
平成２８年９月２０日	情報セキュリティインシデントの対応体制の整備に伴う改正
平成２９年４月１日	最高情報セキュリティ責任者の要件の変更に伴う改正
平成２９年１２月１９日	情報の格付けに伴う改正
令和元年７月１６日	情報セキュリティ管理・運用体制の変更及びパブリッククラウドサービス利用ガイドライン策定に伴う改正
令和４年４月１９日	総合情報戦略会議の設置に伴う改正
令和５年２月１日	聴講生制度の創設に伴う改正

目次

Ⅰ　情報セキュリティ基本方針

１　趣旨

国立大学法人奈良先端科学技術大学院大学（以下「本学」という。）が、高度情報社会において学術研究活動、教育活動及び社会貢献活動を展開するためには、情報基盤の整備を行うとともに、本学の情報資産のセキュリティを確保し、サイバーセキュリティを取り巻く情勢の変化に応じて求められる対策を着実かつ継続的に実施することが不可欠である。本学では、情報セキュリティ水準の維持及び向上を図り、セキュリティ対策を実効性のあるものとするため、「政府機関等の情報セキュリティ対策のための統一基準（平成３０年度版）」（平成３０年７月２５日内閣サイバーセキュリティセンターサイバーセキュリティ戦略本部策定）を踏まえ、国立大学法人奈良先端科学技術大学院大学情報セキュリティポリシーを定める。

２　目的

本学は次に定める事項に取り組み、もって情報資産の保護及び活用並びに情報環境の維持及びその適正な利用を促進する。

（１）情報セキュリティに対する侵害の防止
（２）情報セキュリティを損ねる加害行為の防止
（３）情報資産の重要度による格付けとその管理
（４）情報セキュリティに関する情報取得支援

ただし、少数のシステム管理者が情報システムを提供し、特定の利用者が使用する一般の省庁と大学は異なるため、次の事項を斟酌するものとする。

（１）教職員だけでなく、学生が利用者として含まれていること。
（２）本学で開催される学会、講演会、シンポジウムその他行事へ持ち込まれる情報機器も対象となりうること。

３　定義

このポリシーにおいて、次の各号に掲げる用語の定義は、それぞれ当該各号の定めるとおりとする。

（１）情報システム　　ハードウェア、ソフトウェア及び記録媒体で構成されるものであって、これら全体で業務処理を行うもの
（２）情報資産　　情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称
（３）利用者　　役員、教職員（常勤及び有期契約の教職員、研究員及び非常勤講師並びに派遣職員（外部委託を含む。））、学生（特別聴講学生、特別研究学生、科目等履修生、聴講生、研究生及び特別学修生を含む。）その他本学において教育研究又は事務若しくは技術業務に従事する者で、本学の情報ネットワークを利用するも

の
（４）システム管理者　　総合情報基盤センター長その他本学の情報システムを管理する者

４　適用範囲

このポリシーの適用範囲は、次の各号に規定する情報システム及び情報資産とする。

（１）本学が所有又は管理する情報システム（システム構成図等の文書を含む。）
（２）前号に規定する情報システムに接続された情報機器（本学のネットワークに一時的に接続された本学以外が所有又は管理する情報機器を含む。）で、前号に規定する情報システム以外のもの
（３）前２号に掲げる情報システムに電磁的に記録された情報

５　適用対象者

このポリシーの適用対象者は、本学の情報システム又は情報資産を運用、管理又は利用する全ての者とする。

II　対策基準

６　組織・体制

6.1　管理・運用組織の構成

6.1.1　最高情報セキュリティ責任者

（１）最高情報セキュリティ責任者（CISO: Chief Information Security Officer）は、全学の情報セキュリティに関する総括的な意思決定を行い、学内及び学外その他組織に対し責任を負う。また、本学における情報セキュリティ対策を推進する。
（２）最高情報セキュリティ責任者は、国立大学法人奈良先端科学技術大学院大学における総合情報戦略会議に関する規程（令和４年規程第２号）第３条第３項に規定する総合情報戦略会議の議長をもって充てる。

6.1.2　最高情報セキュリティ責任者補佐

（１）最高情報セキュリティ責任者補佐は、全学の情報セキュリティ対策の実施に関し、最高情報セキュリティ責任者を補佐するとともに、情報システム管理の実施に関し、緊急時の連絡など、総括的な対応にあたる。
（２）最高情報セキュリティ責任者補佐は、総合情報基盤センター長をもって充てる。

6.1.3　部局情報セキュリティ責任者

（１）部局情報セキュリティ責任者は、部局内の情報セキュリティ対策及び情報システム管理の実施に関し、最高情報セキュリティ責

任者補佐との連絡調整の対応にあたるとともに、部局内のシステム管理者を統括する。

（２）部局情報セキュリティ責任者は、各部局の長（事務局にあっては事務局長）又は当該部局の長が指名する者をもって充てる。

6.1.4　総合情報戦略会議

（１）国立大学法人奈良先端科学技術大学院大学における総合情報戦略会議に関する規程（令和４年規程第２号）に規定する総合情報戦略会議は、情報セキュリティポリシーの策定、情報セキュリティに関する基本計画の策定、情報セキュリティに関する啓発及び教育方策の決定その他重要事項の決定及び対外的な対応を行う。

（２）総合情報戦略会議は、情報資産に対する学外からの攻撃や学内からの加害行為に対する必要な措置、実施体制、組織及び手順を定める。

6.1.5　サイバーセキュリティインシデント対応チーム

（１）最高情報セキュリティ責任者のもとにサイバーセキュリティインシデント対応チーム(Cyber Security Incident Response Team（以下「NAIST CSIRT」という。）)を設置する。

（２）NAIST CSIRT は、本学において情報セキュリティインシデントが発生したときに、迅速かつ円滑に対応するものとする。

（３）このポリシーに定めるもののほか、NAIST CSIRT に関し必要な事項は、総合情報戦略会議が別に定める。

6.2　情報セキュリティインシデントへの対応

NAIST CSIRT は、情報セキュリティインシデントを認知した場合、情報セキュリティインシデント対応手順書に従い、関連する通信の遮断又は該当する情報機器の切り離しその他必要な措置を行う。最高情報セキュリティ責任者は、当該情報機器の復旧の判断を当該システムのシステム管理者及びNAIST CSIRTの報告を踏まえ行う。このとき、必要に応じて総合情報戦略会議に諮ることができる。

6.3　緊急時の連絡体制

緊急時の連絡体制は、本学の「危機管理マニュアル」類型Ⅲ不祥事等第２編情報管理に定めるとおりとし、被害を受けたサイバー攻撃に係る情報については最高情報セキュリティ責任者の判断のもと、可能な限り速やかに文部科学省その他必要な機関に連絡する。

6.4　組織体制図

本学の情報セキュリティ管理・運用組織体制は別図のとおりとする。

6.5　実施手順書の作成

このポリシーに沿った具体的な実施手順については、各部局において定めるものとする。

7　情報の格付け及び管理

7.1　アクセス制限

システム管理者は、情報の内容に応じて、当該情報にアクセス権限を有する者をその利用目的を達成するために必要な最小限に限定しなければならない。

利用者は、アクセス権限のない情報システム及び情報資産にアクセスしてはならない。

7.2　情報の格付け及び管理

本学で扱われるすべての電磁的記録情報について、情報の重要度による格付け、情報の管理方法及び管理責任を明確にする。重要度による格付けと、改ざん又は破壊によるリスク分析を、すべての部局で実行する。

部局情報セキュリティ責任者は、それぞれの情報における格付けが適切に行われるよう必要な措置を講ずるものとする。

7.3　情報の限定公開

システム管理者は、特定の利用者に特定の情報を公開する場合において、情報の登録又は閲覧は、許可された操作だけを行えるよう、認証及びアクセス制限機能を設けなければならない。

システム管理者は、異常な情報登録又は閲覧の状況を定期的に確認しなければならない。

7.4　重要情報の特定

最高情報セキュリティ責任者は、先端的な技術及びこれに係る研究成果その他学術研究活動に有用な情報の漏えいを防止するため、本学が保有するこれらの重要情報を特定しなければならない。

7.5　情報改ざん及び偽情報流布の防止

役員及び教職員は、情報の原本を書き換え不能な記憶媒体に保存その他方法により完全性を保証しなければならない。

7.6　情報機器及び記憶媒体の処分

情報機器及び記憶媒体を管理する者は、当該機器及び媒体を処分する場合、部外者が記録内容を解読できないように処分しなければならない。

8　物理的対策

システム管理者は、情報システムを構成する情報機器全てにおいて、設置場所の安全性を確保のうえセキュリティ侵害への物理的対策を実施し、不正な立入りを阻止するための対策を講じる。

9　人的対策

9.1　責務

総合情報戦略会議は、利用者の情報資産に対する権限及び責任を明

確にし、すべての利用者に対しこのポリシーを周知徹底する。すべての利用者は、このポリシーを遵守しなければならない。

9.2　教育研究上の利便性の配慮

教職員及び学生は、情報セキュリティ対策において、教育研究上の利便性を著しく損なう場合又は遵守することが現実的に困難な場合は、最高情報セキュリティ責任者にポリシーの改善を求めることができる。

9.3　教育・研修

総合情報戦略会議は、部局情報セキュリティ責任者等が行う教職員向けのセキュリティに関する研修の支援を講じなければならない。また、教員が行う学生向けのセキュリティに関するオリエンテーション及び講義に協力しなければならない。

9.4　教職員及び外部事業者

9.4.1　教務及び事務系業務

最高情報セキュリティ責任者は、教職員（外部事業者を含む）に、雇用契約その他必要と認める場合に、遵守すべきポリシーの内容を理解させ、及び遵守させなければならない。

9.4.2　情報システムの開発及び保守並びに管理業務

システム管理者は、情報システムの開発及び保守並びにシステム管理業務を外部事業者に委託する場合は、外部事業者が再委託する外部事業者を含め、ポリシーのうち外部事業者の遵守事項を明記した契約書の取り交わしをしなければならない。

外部事業者との契約書には、責任所在の境界及び遵守事項に違反した場合の規定を定めなければならない。

9.4.3　パブリッククラウドサービス利用に関する基準

本学は、外部事業者が運営するパブリッククラウドサービスを利用し、情報資産を管理及び運用しようとする場合は、別に定めるパブリッククラウドサービス利用ガイドラインを基準に、利用の是非について検討しなければならない。

１０　技術的対策

10.1　情報ネットワーク運営方針

本学は、外部からの不正アクセスによる情報資産の破壊を阻止するため、情報ネットワークのアクセス制御及び管理に対して必要な技術的対策を講ずるものとする。

総合情報戦略会議は、学外からの脅威又は学内から学外への攻撃に対処するため、総合情報基盤センターと連携し、安全な情報ネットワークの設計、構築及び運営を推進するため、情報ネットワークのアクセス制御及び管理に関して必要な技術的対策を行う。

利用者は、設置されたネットワーク侵入検知システムその他トラフィック検査及び情報セキュリティインシデント発生時の通信遮断措置

その他実施した措置を受け入れなければならない。

10.2　端末機器等に関する基準

情報ネットワークに接続する機器は、利用者を何らかの方法で認証できなければならない。機器を設置しようとする者は、セキュリティ対策を含む設定作業が完了していない機器を情報ネットワークに接続してはならない。システム管理者は、設置機器の利用者を特定可能でなければならない。

システム管理者は、総合情報戦略会議又はNAIST CSIRTの要請に応じて、ログ等の運用に関する情報を総合情報戦略会議又はNAIST CSIRTに対して開示しなければならない。

１１　評価・見直し

11.1　ポリシーの運用実態

部局情報セキュリティ責任者は、部局における情報セキュリティ対策に係る状況を各年度１回以上自己点検し、総合情報戦略会議に報告しなければならない。

総合情報戦略会議は、全学におけるセキュリティ対策に係る状況の変化に応じて、ポリシーの見直しその他必要な検討を行わなければならない。

11.2　セキュリティレベル向上策

総合情報戦略会議は、報告を受けた自己点検結果を各年度１回以上評価し、改善が必要な場合にはポリシー内容の変更を行い、より高度なセキュリティレベルの維持及び向上並びに遵守が可能なポリシーに更新しなければならない。

（別図）国立大学法人奈良先端科学技術大学院大学情報セキュリティ管理・運用組織体制図