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

平成１８年　６月　２２日

目　　次

Ⅰ 情報セキュリティ基本方針

1　情報セキュリティ基本方針

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・教育活動・社会貢献を展開するためには情報基盤の整備に加えて大学の情報資産のセキュリティを確保することが不可欠である。情報セキュリティの重要性を本学の教職員および学生等の全ての構成員に熟知させ情報資産を確固として守るため、「情報セキュリティポリシーに関するガイドライン（平成 12 年 7 月 18 日情報セキュリティ対策推進会議決定)」を踏まえ情報セキュリティポリシーを定める。

本ポリシーによって目指すものは次の通りである。

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分類とその管理
④　情報セキュリティに関する情報取得支援

一方、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、次のような点を斟酌する。

・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。
・本学で開催される学会、講演会、シンポジウムなどへ持ち込まれる情報機器も対象となりうること。

本学においては、以下の対策によって情報セキュリティを確保する。

１）組織・体制

最高情報セキュリティ責任者は、情報セキュリティ委員会の委員長となり、大学における情報セキュリティ対策を推進する。また、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してネットワーク遮断等の措置を、どのような体制で、どの組織で、どのような手順で行うかを規定する。

２）情報の分類と管理

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分類、情報の管理方法、管理責任を規定する。重要度による分類と、改ざんや破壊によるリスク分析を、すべての部局で実行する。

３）物理的対策

情報システムの設置場所について、安全性を保ち、不正な立入りを阻止する対策を立てる。またデスク上のパソコンまたは持ち運びを前提としたノートパソコン等の情報資産を保護する

４）技術的対策
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・管理に対して必要な技術的対策を講ずる。
５）人的対策
全構成員に対して本ポリシーを周知徹底させるとともに、各員が情報資産に対してどのような権限と責任を持っているかを規定し、情報セキュリティを確保するための啓発活動や教育の対策を講ずる。
６）評価・見直し
情報技術の発展ならびに策定したポリシーの遵守度により、本ポリシーを定期的に見直してセキュリティレベルを絶えず上げるよう努力する。更に、セキュリティ監査についても措置をとる。

2　定義

このポリシーにおいて用いる用語の定義は次の通りとする。

2.1　情報システム

本学において、ハードウェア、ソフトウェア、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。

2.2　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。

2.3　利用者

役員、教職員、学生その他本学において教育研究または事務もしくは技術に従事する者で、本学の情報ネットワークを利用する者をいう。

2.4　システム管理者

情報科学センター長その他本学の情報システムを管理する者をいう。

3　対象範囲

ポリシーの対象範囲は、ハードウェア、ソフトウェア、記録媒体等の情報システム等（システム構成図等の文書を含む。）及びすべての情報のうち、情報システムに電磁的に記録される情報、ならびにこれらの情報に接するすべての者とする。このため、本ポリシーにおいて、「情報資産」の情報は、電磁的に記録されたものに限られる。さらに、本学以外のコンピュータで、本学のネットワークに一時的に接続されたコンピュータを含む。
ポリシーの対象者は役員、教職員（常勤および有期契約の教職員、非常勤講師ならびに派遣職員（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、研究生、留学生等を含む）および来学者等である。

4　実施手順の作成

この基本方針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こ

ととする。

II 対策基準

1 組織・体制

1.1 管理・運用組織の構成

1.1.1 最高情報セキュリティ責任者

最高情報セキュリティ責任者は全学の情報セキュリティに関する総括的な意思決定と、学内、他の組織および学外に対し責任を負う。情報管理を担当する理事をもって充てる。

1.1.2 全学システム管理責任者

全学の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り、最高情報セキュリティ責任者を補佐する。情報科学センター長をもって充てる。

1.1.3 部局システム管理責任者

部局内の情報システム管理の実施に関し、全学システム管理責任者との連絡などの対応にあたり、システム管理者を統括する。各部局の長（事務局にあっては事務局長）または当該部局の長が指名する者をもって充てる。

1.1.4 情報セキュリティ委員会

全学の情報セキュリティに関し、基本的なセキュリティポリシーの策定および重要事項の決定を行うとともに、対外的な対応等を行う。

情報セキュリティに関する啓発および教育について、部局システム管理責任者とシステム管理者に対するレベルの高い教育を行うとともに、一般の利用者に幅広く初心者教育を行う。最高情報セキュリティ責任者、部局システム管理責任者および全学システム管理責任者等で構成する。全学情報管理・個人情報保護委員会をもって充てる。

1.1.5 システム管理部会

情報セキュリティ委員会のもとにシステム管理部会を設置し、全学の情報システムのセキュリティ管理を実施するための連絡調整および部局システム管理責任者への技術的助言等の支援を行う。

全学システム管理責任者および部局システム管理責任者の指名するシステム管理者等で構成する。

1.2 不正アクセス等への対応

システム管理部会は、外部または内部からの不正アクセスを検出した場合、情報セキュリティ委員会が定めた緊急措置手順に従い、関連する通信の遮断または該当する情報機器の切り離しを実施する。ただし、あらかじめ手順に定められていない状況には、最高情報セキュリティ責任者が判断する。

情報セキュリティ委員会は、不正アクセスが継続する場合に、当該情報機器またはそれを接続するネットワークについて、定常的な利用の停止などの抑止措置をとることができる。

2　情報の分類と管理

2.1　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必要最小限の利用者に限定しなければならない。
利用者はアクセス権のない情報システムや情報にアクセスしてはならない。

2.2　情報の分類

システム管理者はそれぞれの情報について、公開・非公開を定めること。

2.3　情報の公開化

非公開情報を公開化する場合は、個人情報の漏洩、プライバシーや著作権の侵害に十分注意し、公開できる情報だけを抽出する、あるいは統計処理等の加工をしなければならない。

2.4　情報の限定公開

特定の利用者に特定の情報を公開する場合において、情報の登録および閲覧は、許可された操作だけを行えるよう、認証およびアクセス制限機能を設けなければならない。さらに、異常な登録や閲覧が行われていないか、定期的に状況を確認しなければならない。

2.5　情報改ざんおよび偽情報流布の防止

非公開情報および公開情報の原本は、書き換え不能な記憶媒体に保存するなどにより原本性を保証しなければならない。また、それぞれの情報システムごとにシステム管理者をもうけなければならない。

2.6　情報機器および記憶媒体の処分

公開・非公開を問わず、情報機器および記憶媒体を破棄する場合は、その処分方法に注意しなければならない。

3　物理的対策

クライアント、サーバ、ネットワーク機器、ネットワークケーブルそれぞれにおいてセキュリティ侵害への物理的対策が施される必要がある。

4　人的対策

4.1　責務

すべての利用者は本ポリシーを遵守しなければならない。

4.2　教育研究上の利便性の配慮

教職員および学生は、情報システム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点、あるいは、遵守することが現実的に困難な点については、最高情報セキュリティ責任者に対して、ポリシーの実施手順の改善を求

めることができる。

4.3 教育・研修

情報セキュリティ委員会は、システム管理者等が行う教職員向けのポリシーに関する研修の支援をしなければならない。また、教員が行う学生向けのポリシーに関するオリエンテーションまたは講義に協力しなければならない。

4.4 教職員ならびに外部委託等

4.4.1 教務および事務系業務

教職員（外部委託事業者を含む）には、雇用契約等の際に、守るべきポリシーの内容を理解させ、実施および遵守させなければならない。

4.4.2 情報システムの開発ならびに保守ならびに管理業務

情報システムの開発および保守ならびにシステム管理業務を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受託する業者を含めて、ポリシーのうち外部委託事業者が守るべき内容の遵守を明記した契約を行わなければならない。

外部委託事業者との契約書には、責任所在の境界ならびにポリシーが遵守されなかった場合の規定を定めなければならない。

5 技術的対策

5.1 ネットワーク運営方針

情報セキュリティ委員会は、外部からの脅威や内部から外部への攻撃に対処できるようにネットワークの設計・構築・運営をする必要がある。

利用者は、設置されたネットワーク侵入検知システムやその他によるトラフィックの検査を受け入れなければならない。

5.2 端末機器等に関する基準

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ものは、セキュリティ対策を含む設定作業の完了していない装置を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、情報セキュリティ委員会の要請に応じて、ログ等の運用に関する情報を情報セキュリティ委員会に対して開示しなければならない。

6 評価・見直し

6.1 ポリシーの運用実態

全学システム管理責任者は、システム管理部会を定期的に開催し、収集した情報を分析・整理した上で、情報セキュリティ委員会に報告しなければならない。

情報セキュリティ委員会は、全学におけるポリシーの運用実態に基づいて、ポリシーの検討を行わなければならない。

6.2　セキュリティレベル向上策

情報セキュリティ委員会は、ポリシーの実効性を少なくとも年一回評価し、改善が必要な場合には内容の変更および実施時期の決定を行い、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しなければならない。
情報セキュリティ委員会は、評価・見直しの結果を踏まえ、情報セキュリティ計画および予算案の作成を行わなければならない。