（学　長　裁　定
平成２９年３月３０日）

北陸先端科学技術大学院大学における情報セキュリティ対策基本計画

１．全体方針

・世界最高水準の教育・研究を行う大学院大学として、それに必要な情報セキュリティ対策を講じた情報環境の構築を推進する。

・情報セキュリティ対策を講じるにあたり、役員、教職員及び学生（以下「構成員」という。）の活動が円滑に行えるようセキュリティを維持しつつ、高い利便性や性能を有する情報環境の構築を推進する。

・情報セキュリティ対策の組織への浸透とセキュリティインシデントへの対応を効果的に行うための組織体制を整備する。

・全ての構成員が情報セキュリティ対策の重要性について認識し、それを順守するよう教育研修を実施する。

２．個別取組の方針・重点

（１）情報セキュリティインシデント対応体制及び手順書等の整備

・学内 CSIRT の整備

学内情報セキュリティ対策チーム（(Computer Security Incident Response Team）以下「CSIRT」という。）を構築し、情報セキュリティインシデント（以下「インシデント」という。）が発生した際に、迅速に報告・連絡、被害拡大防止等の対応ができる体制を整備し、これを学内外に明示的に周知する。CSIRT はインシデント対応だけではなく、インシデント発生を未然に防ぐため最新の情報セキュリティの動向を収集し、学内 Web ページ、メール、SNS 等を活用した広報活動を行う。また、学内における教育研修の実施及び新規採用等により、業務を担える高い情報セキュリティ技術を有する人材の確保に努める。

・監視体制の整備

インシデントに迅速に対応するため、外部の研究機関や民間組織と連携し、常時監視する体制の構築を行う。

・手順書の整備

インシデント発生時の手順書を整備し、CSIRT、情報社会基盤研究センター及び事務局の担当者間で共有する。手順書には、緊急時に停止可能な情報機器と業務継続のために継続稼働が求められる情報機器を記載する。

（２）情報セキュリティポリシーや関連規程の組織への浸透

・情報セキュリティポリシーの見直し

昨今の情報セキュリティの動向や基準に基づき情報セキュリティポリシー及び関連規程等の見直しを行う。英語版についても必要に応じて整備を行う。

・情報の格付けや取扱区分の周知と徹底

情報ファイル及び情報システムの格付けや取扱区分について明確化し、これを周知する。併せて構成員がこれを遵守できるよう標準的かつ簡易的な、情報取扱いマニュアルを作成する。必要に応じて「JAIST 事務マニュアル」等、既存の業務マニュアルにも反映を行う。

（３）情報セキュリティ教育・訓練及び啓発活動

・標的型メール対策訓練の実施

本学の情報を狙う標的型メールによる攻撃を想定し、訓練を実施する。機密情報を取り扱う教職員だけではなく、構成員全員が訓練に参加するよう必要な対策を講じる。

・インシデント訓練の実施

インシデント発生時に、迅速かつ的確に対応できるよう、CSIRT 及び関係職員で年１回程度のインシデント対応訓練を実施する。

・リテラシー教育の実施

構成員の役職に応じたオフライン教育を毎年実施する。部局毎の実施や複数回の実施、未受講者へのフォローを行うとともに、オフライン教育の受講が困難な者への対応や理解を深めることを目的として e-learning 環境を整備する等、リテラシー教育の受講率を 100％とするべく取り組む。外国人研究者及び外国人学生が必要な情報リテラシーを習得できるよう、情報セキュリティに関するパンフレットの英語版を作成する。

（４）情報セキュリティ対策に係る自己点検・監査の実施

・重要システムの外部監査の実施

外部公開を行うサーバ及び高い機密性を持つシステムについては定期的（毎月～四半期毎）に情報社会基盤研究センターによる脆弱性調査を実施し、不備がある場合には改善を行う。

また、年に１回、外部情報セキュリティ専門機関又は監査法人等によるセキュリティ診断又は監査を実施する。

・全学での自己点検、外部監査の実施

機密性の高い情報ファイル及び情報システムについて優先的に自己点検及び外部監査を行い、それ以外においても順次実施する。最終的に大学全体で情報セキュリティにおける PDCA サイクルが持続的に行える体制を構築する。

・進捗状況の自己点検、外部監査の実施

本計画の進捗状況については自己点検及び外部監査を毎年実施する。

（５）情報及び情報機器管理状況の把握及び必要な措置

・IP アドレス管理の徹底

学内 LAN に接続する際の利用申請を徹底し、学内 LAN で利用する IP アドレスを適切に管理する。また、未申請の端末は学内 LAN に接続できないネットワーク環境を整備する。

・ウィルス、マルウェア監視の強化

ウィルスやマルウェアに感染し、不審な振る舞いをした端末を早期に検知し、学内ネットワークから迅速に隔離する体制を整備する。

・モバイルデバイスの管理の徹底

外部に持ち出す可能性がある情報機器の管理を徹底し、紛失やウィルス、マルウェア感染による情報漏洩が発生しない体制を目指す。

・ネットワーク設計の見直し

頻繁に出入りする外部利用者のネットワーク接続を許容しつつ、適切にアクセス制限を行う。また、インシデントが発生してもその被害の拡大を最小化できるよう、ネットワークの細分化等のゾーン設計の見直しを行う。あわせて、外部公開が目的の情報セキュリティポリシー除外申請について、申請、承認、適用等の管理を強化する。

・アクセス制限及び暗号化

情報ファイル及び情報システムの格付けに基づき、アクセス制限や暗号化、外部との情報の受け渡しにあたっての取扱いを徹底するため、情報ファイルの共有方法及び取扱い手順の見直しを行う。また、情報の管理者や構成員が円滑かつ適切に管理できるよう仕組みを構築する。

・アカウント管理及び認証基盤の強化

アカウントの作成や削除などのアカウント管理業務の見直しを行い、構成員の身分に応じて適切な範囲の情報環境が利用できるよう生涯 ID の運用を踏まえたアカウント及び保有データの管理の強化を行う。

また、必要に応じて、統合 ID 管理システムの導入を検討する。さらに、認証基盤を強化し、パスワードの複雑さの向上やパスワード以外の要素を組み合わせる二要素認証への対応を推進する。

・物理セキュリティの強化及び外部データセンタ/クラウド事業者の利用推進

学内システムを収容するサーバ室や各端末等について自己点検や外部監査に基づく改善を行うと共に、より物理セキュリティの高い外部クラウド事業者、データセンタの利用を推進する。

３．個別の取組の実施時期（工程表）

「２．個別の取組の方針・重点」で示した個別の取組の実施予定時期を別紙「北陸先端科学技術大学院大学大学情報セキュリティ対策基本計画工程表」に示す。

別　紙

北陸先端科学技術大学院大学大学情報セキュリティ対策基本計画工程表

