公立大学法人秋田県立大学情報セキュリティ基本規程

平成２６年　３月　５日
規程第４４号
改正　令和３年３月１７日
改正　令和４年２月２２日

目　次

第１章　総則

（目的）

第１条　この規程は、公立大学法人秋田県立大学情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）に基づき、公立大学法人秋田県立大学の情報セキュリティ管理体制その他必要な事項を定めることを目的とする。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

一　情報システム　本学において、ハードウェア、ソフトウェア、ネットワーク及び記録媒体等で構成され、これらで業務処理を行うものをいう。

二　利用者　本学の教職員、学生その他本学に在籍するすべての者、委託業者及び情報システムを利用する来学者をいう。

三　教職員　本学に勤務する常勤若しくは非常勤の教職員（派遣を含む。）又は本学においてこれに準ずるものと認めた者をいう。

四　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、運用及び保守に関する資料等）の総称をいう。

五　情報セキュリティ　情報資産が備えるべき次に掲げる性質を保つことをいう。

イ　機密性　権限を持つ者だけがアクセスできること。

ロ　完全性　情報及びその処理方法の正確さ並びに完全さが保護されていること。

ハ　可用性　許可された利用者が必要な時に情報及び情報システムへアクセスすることが保証されていること。

六　情報セキュリティの侵害　情報資産が、流出、漏洩、改ざん、破壊、障害及び災害等により、前項に掲げた性質が侵害されることをいう。

第２章　組織・体制

（組織）

第３条　情報セキュリティ及び情報システムの管理・運用を行うため、本学に次のものを置く。

一　最高情報責任者（以下「最高責任者」という。）

二　情報セキュリティ委員会（以下「委員会」という。）

２　情報セキュリティの管理・運用を行うため、本学に次のものを置く。

一　総合情報セキュリティ管理者（以下「総合セキュリティ管理者」という。）

二　情報セキュリティ管理者（以下「セキュリティ管理者」という。）

三　情報セキュリティ担当者（以下「セキュリティ担当者」という。）

３　情報システムの開発・管理・運用を行うため、本学に次のものを置く。

一　部局情報システム管理者

二　情報システム管理者

（最高情報責任者）

第４条　最高責任者は、副理事長をもって充てる。

２　最高責任者は、情報システムの管理及び情報セキュリティ対策に関する最終決定権限及び責任を有し、情報システムの運用に携わる者及び利用者に対する教育を統括する。

３　最高責任者は、情報セキュリティに関する専門的な知識及び経験を有する外部の専門家を情報セキュリティアドバイザーとして置くことができる。

４　最高責任者がその職務を遂行できないときは、最高責任者があらかじめ指名する者がその職務を代行する。

（情報セキュリティ委員会）

第５条　委員会は、次の各号に掲げる委員をもって構成する。

一　最高責任者

二　総合セキュリティ管理者

三　セキュリティ管理者

四　部局情報システム管理者

五　その他最高責任者が認めた者

２　委員会は次の事項について審議し、かつ、実施する。

一　情報システムの運用、利用若しくは管理、並びに情報セキュリティに関する教育等に関すること
二　情報システムの運用リスク管理に関すること
三　情報セキュリティに係る教育計画及び実施計画に関すること
四　情報セキュリティポリシーの点検、評価並びに更新に関すること
五　情報セキュリティの検証と改善に関すること
六　その他必要な事項
3　委員会の委員長は最高責任者をもって充て、副委員長は総合セキュリティ管理者をもって充てる。
4　委員長は、委員会を招集し、その議長となる。
5　副委員長は、委員長を補佐し、委員長に事故があるときは、その職務を代理する。
6　委員会の議事は、出席した委員の過半数によって決し、可否同数のときは、委員長の決するところによる。

（総合情報セキュリティ管理者）
第6条　総合セキュリティ管理者は、最高責任者が指名する。
2　総合セキュリティ管理者は、最高責任者の指示に基づき次の業務を行う。
一　情報システムの運用に携わる者及び利用者に対するセキュリティに関する教育の企画
二　緊急時等の円滑な情報共有を図るための連絡体制の整備
三　情報セキュリティの遵守状況について確認及び問題を認めた場合の最高責任者への報告

（情報セキュリティ管理者）
第7条　各キャンパスにセキュリティ管理者を置き、総合セキュリティ管理者が指名する。
2　セキュリティ管理者は、情報セキュリティポリシー及び関連規程に基づき、次の業務を行う。
一　情報システムのセキュリティ維持・管理状況についての点検・評価
二　情報システムのセキュリティに関する教育の実施
三　情報セキュリティポリシー及び関連規程の利用者への公表方法の検討・実施
3　セキュリティ管理者は、セキュリティ担当者を任命することができる。セキュリティ管理者及びセキュリティ担当者となるべき者が情報セキュリティに関する資格（システム監査技術者、ネットワークスペシャリスト、情報セキュリティスペシャリスト等）を有しないときは、当該資格又は当該資格に準ずる技術を有する者を情報セキュリティ専任員（以下「セキュリティ専任員」という。）として指名することができる。
4　セキュリティ専任員は、セキュリティ管理者及びセキュリティ担当者の業務について

も自ら率先して取り組むものとし、セキュリティ専任員は外部に委託することができる。

（部局情報システム管理者）

第８条　公立大学法人秋田県立大学事務組織規程（規程第２号）第２条に規定する本部並びに秋田県立大学学則（規程第１００号）に規定する学部、総合科学教育研究センター、地域連携・研究推進センター、アグリイノベーション教育研究センター及び木材高度加工研究所並びに秋田県立大学大学院学則（規程第１０１号）に規定する研究科（以下「部局」という。）に部局情報システム管理者を置き、当該本部及び部局の長をもって充てる。

２　部局情報システム管理者は、次の業務を行う。

一　情報システムの運用方針決定及び各種問題の処理

二　情報セキュリティに侵害が発生した場合又は侵害のおそれがある場合における総合セキュリティ管理者（不在時は最高責任者）への速やかな報告及び対応

（情報システム管理者）

第９条　本部及び部局に情報システム管理者を置き、部局情報システム管理者が情報システムごとに指名する。

２　情報システム管理者は、次の業務を行う。

一　情報システムの開発、設定の変更、運用、更新及び管理等

二　情報セキュリティポリシー実施手順の維持管理等

三　情報セキュリティに侵害が発生した場合又は侵害のおそれがある場合における部局情報システム管理者（不在時は総合セキュリティ管理者又は最高責任者）への速やかな報告及び対応

第３章　情報の分類と管理

（情報資産の分類と管理）

第 10 条　情報システム管理者は、別に定める基準に基づき、機密性、完全性及び可用性の観点から、情報資産の分類を行う。

２　情報資産を取り扱う者は、前項で定められた分類に応じ、適切な取り扱いをしなければならない。

３　情報資産を取得した者あるいは作成した者は、取得した情報資産の分類が不明な場合、情報システム管理者に判断を仰がなければならない。

４　情報資産を取り扱う者は、情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って取り扱わなければならない。

５　情報資産が複製又は伝送された場合、当該情報資産は本条の分類に基づき管理しなければならない。

第４章　情報セキュリティポリシー等の遵守状況の確認

（教職員の遵守事項）

第 11 条　教職員は、情報システムを取り扱う上で、次の事項を遵守し、業務を行わなければならない。

一　情報セキュリティポリシー及び関連規程を遵守し、情報セキュリティ対策について不明な点、遵守することが困難な点等ある場合は、速やかにセキュリティ担当者に相談し、指示を仰がなければならない。

二　情報セキュリティポリシー及び関連規程に対する違反行為を発見した場合、直ちに所属の部局情報システム管理者に報告し、違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると総合セキュリティ管理者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

三　異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

四　業務上必要のない情報を取り扱ってはならない。

五　業務・教育・研究目的以外での情報システムを使用してはならない。

第５章　侵害時の対応

（緊急時対応計画の策定）

第 12 条　最高責任者は、情報セキュリティに関する事故、情報セキュリティポリシー等の違反等により情報セキュリティの侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておかなければならない。

２　緊急時対応計画には次に掲げる内容を規定するものとする。

一　関係者の連絡先

二　発生した事案に係る報告すべき事項

三　発生した事案への対応措置

四　再発防止措置の策定

３　委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、最高責任者に対して緊急時対応計画の見直しを求めることができる。

第６章　点検

（点検）

第 13 条　最高責任者は、この規程及び本学情報セキュリティポリシーその他関連規程等の見直しを行う必要性の有無を適時検討し、必要があると認められる場合はその見直しを行う。

２　本学情報システムを運用、管理及び利用する者は、自らが実施した情報セキュリティ対策に関連する事項に、課題若しくは問題点が認められる場合には、当該事項の見直しを行わなければならない。

附　則

この規程は、平成２６年３月５日から施行する。

附　則（令和３年３月１７日改正）

この規程は、令和３年４月１日から施行する。

附　則

この規程は、令和４年２月２２日から施行する。