公立大学法人秋田県立大学情報セキュリティポリシー

平成19年 2月 7日
改正　平成26年 3月 5日

Ⅰ　情報セキュリティの基本方針

１．基本方針

高度情報化社会の中で公立大学法人秋田県立大学の学生、教職員等が教育や研究、社会活動、大学運営を安全に行うためには、大学の情報資産の安全性を確保することが重要である。本学の学生、教職員等のすべてが、情報資産の価値を認識し、自身の情報を守るだけでなく、他者の情報資産も侵してはならないものとして行動しなければならない。

本学は、情報の公開性と利便性を確保するために安全な情報システムを整備し、学生、教職員等はこれを正しく利用するものとする。また、本学からの不正な情報提供や不正アクセスをなくし、学外に対しても本学の情報システムの信頼性を高めていくものとする。

本学の学生、教職員等のすべてが、情報システムを正しく利用していけるよう、情報システムの運用、利用についての指針として、情報セキュリティポリシーを制定する。

情報セキュリティポリシーの目指すところは

（ａ）本学の情報セキュリティに対する侵害を阻止すること
（ｂ）学内外の情報セキュリティを損ねる加害行為を抑止すること
（ｃ）情報システムで取り扱う電磁的記録情報に関して、重要度に見合った管理を行うこと
（ｄ）情報セキュリティに関する情報の取得を支援すること

である。

２．用語の定義

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、ポリシーとする）で使用する用語の定義については、平成12年7月18日に情報セキュリティ対策推進会議が決定した「情報セキュリティポリシーに関するガイドライン」に定める定義と同様とする。

（http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html）

３．対象範囲

ポリシーの対象範囲は、本学の情報資産のうち情報システム上で取り扱う文書、電磁的に記録された情報、並びに本学のネットワークに一時的にあるいは永続的に接続された全ての情報システムとする。

ポリシーの対象者は、本学の全構成員（大学生、大学院生、研究生、科目等履修生、聴講生、役員、教員、職員、委託業者など）および情報システムを利用する来学者とする。

４．情報セキュリティ基本規程の作成

公立大学法人秋田県立大学セキュリティ基本規程を定めて、情報セキュリティ管理体制その他必要な事項を規定する。

II　対策基準

１．組織・体制

本学に、情報セキュリティ及び情報システムに関する意思決定及び学内外に対する責任を負う最高情報責任者を置く。

最高情報責任者を長とする情報セキュリティ委員会を設置する。

情報セキュリティ委員会はポリシーを策定し、情報セキュリティ対策に関する重要事項を審議する。

情報セキュリティの管理と運用を実施するために総合情報セキュリティ管理者を置く。

総合情報セキュリティ管理者を補佐する情報セキュリティ管理者を置く。

部局内の情報システムについて管理する部局情報システム管理者を置く。

また、各々の情報システムごとに情報システム管理者を置く。

情報システム管理者は情報システムごとに情報セキュリティポリシー実施手順を策定し、これを実施する。

２．情報の分類と管理

２．１．情報の管理

情報資産は、管理の権限を有する者によって管理される。管理の権限については実施手順に規定する。情報システム管理者は管理する上で必要な範囲を超えて情報にアクセスしてはならない。

情報システムを利用する者は、自己の管理する情報へのアクセスのためであっても、情報システム管理者から許可を得ていない者に情報システムを使用させてはならない。

２．２．情報の分類

情報システム管理者は、ポリシーの対象となる情報システムで取り扱う電磁的記録情報について、閲覧できる者を限定した非公開情報と、情報の利用者すべてに閲覧を許す公開情報に分類しなければならない。

(a)　非公開情報

情報システム管理者から許可された者以外がコンピュータに非公開情報を保管してはならない。

情報システム管理者は情報の機密性や重要度に応じた適切なセキュリティ対策を施して情報を管理しなければならない。

非公開情報へのアクセスを許可する者の範囲は情報を管理する者が定める。

(b)　公開情報

公開情報は情報の改ざんや偽情報の流布への対抗策と、個人情報の漏洩、プライバシーや著作権の侵害への防止策が講じられなければならない。

情報発信を行う場合は、正規の発信者であることを証明する必要が生ずることに留意しなければならない。

２．３．情報の作成、保守、システム開発

情報を作成、保守、システム開発する際は、著作権などの他者の知的財産権を侵していないことを確認しなければならない。外部委託などのために、非公開情報を限定された第三者に開示する必要がある場合は、開示の都度、守秘義務契約を結ばなければならない。

２．４．情報機器および記憶媒体の処分

情報機器および記憶媒体を廃棄する場合は、その処分方法に注意しなければならない。情報機器および記憶媒体を保守契約により交換する場合、またはレンタル機器の撤去を行う場合など撤去後の記憶媒体の処理方法については実施手順に規定する。

３．物理的セキュリティ

３．１．パソコン端末機器とネットワーク設備

情報システム管理者から許可を得ていないものが機器や設備を使えないような方策を整えるよう努めなければならない。

パソコンや、ネットワークについては認証と使用の記録を残すように努めなければならない。

端末機器とネットワーク設備には、災害、事故および情報機器の盗難への対策を講じるよう努めなければならない。

３．２．サーバ機器

サーバ機器は、その重要度に応じたセキュリティ対策が施された管理場所に設置されなければならない。停止したときに大学内の業務遂行に重大な支障をきたす重要なサーバ機器に対しては、認証と入退室の記録を残すよう努めなければならない。

サーバ機器に記録される情報資源は、サーバ機器の重要度に応じて定期的にバックアップを行うこととする。

情報資源を保存するサーバ機器や、情報をバックアップしたメディアには、火災、地震等の災害や盗難等の犯罪から守るためセキュリティエリアを分けるような対策を施さなければならない。

重要なサーバ機器については、故障や停電などの事故の際、迅速に保守、回復ができるような体制を整えておかなければならない。

４．人的セキュリティ

ポリシーの対象者は、ポリシーを遵守しなければならない。

情報システム管理者は、責任を持って個々の情報システムの維持に努めなければならない。

４．１．教育・研修

本学の全構成員は、研修会や説明会または講義等を通じてポリシーおよび実施手順を理解し、情報セキュリティ上の問題が生じないように努めなければならない。

情報セキュリティ委員会は、利用者向けのセキュリティに関する教育・研修の支援を行うものとする。

４．２．パスワード管理

自己のパスワードは秘密としなければならない。また、十分なセキュリティを維持できるよう、自己のパスワードの設定および変更に配慮しなければならない。

他の利用者のアカウントを使用してはならない。

４．３．利用範囲

情報機器やネットワーク設備は利用が許可される際に、利用目的が限定されていなければならない。許された目的以外で機器や設備を使用してはならない。

アクセス権のない情報システムや情報に入り込もうとしてはならない。意図的ではなく入り込んだときは、速やかに退出しなければならない。

４．４．システム管理

情報システム管理者は、利用資格を有する者以外に情報端末のアカウントを発行してはならない。また、利用資格を失った利用者のアカウントを速やかに除去しなければならない。

情報システム管理者は、いかなる場合にも利用者からのパスワードの聞き取りを行ってはならない。

ログ情報および通信内容の解析等にあたっては、利用者のプライバシーに配慮し、業務上、閲覧解析が必要な場合のみ行うものとする。

４．５．外部委託

本学の業務を請け負う事業者（委託業者）はポリシーの対象者に含まれる。

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委託業者に発注する場合は、契約書面にポリシーおよび実施手順の遵守を明記しなければならない。

５．技術的セキュリティ

情報システムを不正なアクセス等から保護するため、情報機器へのアクセス制御についての対策を講ずることとする。

この対策によって課される制限が教育研究上の利便性を過剰に損なうことは避けられなければならない。

５．１．ネットワーク設備およびパソコン、サーバの運用基準

情報システム管理者は、許可を得ていない者が機器や設備を使えないような方策を整えるように努めなければならない。

情報システム管理者は、管理する情報機器のアクセス記録を、盗難、改ざんや消去等を防止する処置を施して一定期間保存しなければならない。また、定期的にそれらを確認、分析しなければならない。情報システム管理者の管理する情報機器が不正使用されて学内外に被害を及ぼしているときは、最高責任者または最高責任者に指名を受けた者が、対策に必要なアクセス記録の提出を求めることがある。情報システム管理者はこれに協力しなければならない。

５．２．コンピュータウィルス、スパイウェア対策

情報システム管理者は、不正アクセス、コンピュータウィルスやスパイウェア等情報システムの運用を妨害し、情報を漏洩しようとする攻撃行為から情報資産を守るために必要な対策を講じなければならない。

５．３．非公開情報流出への対策

情報を管理する者の許可を得た場合を除いて、非公開情報の学外への持ち出し、あるいは、非公開情報への学外からのアクセスをしてはならない。

許可を得て非公開情報を学外に持ち出し、あるいは学外からアクセスするときは、情報を暗号化するなど盗難、紛失や盗聴による情報流出を防ぐための対策を講じなければならない。

６．事故・犯罪と発生時の対処

６．１．事故、故障

ポリシーの対象者は、情報セキュリティに関する事故、情報システム上の障害を発

見した場合には、情報システム管理者に直ちに報告しなければならない。
　情報システム管理者は、報告のあった事故等について必要な措置を直ちに講じなければならない。また、部局情報システム管理者へ報告することとする。
　情報システム管理者は、発生した事故等に関する記録を一定期間保存し、情報セキュリティ委員会に報告するとともに、重大な事故に対しては、迅速な再発防止のための対策を講じなければならない。

６．２．不正使用及び情報資産への侵害

　情報セキュリティ委員会は、情報システム管理者に対し、情報機器の不正使用及び情報資産への侵害が発生した場合の緊急時対応計画を、実施手順として定めさせる。
　情報システム管理者は、学内、学外からの報告や依頼を受けて、情報機器の不正使用の調査を早急に行う。不正使用が確認されたときは、手順に従って、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。
　あらかじめ定めのない行為によって情報セキュリティが阻害されたときは、最高情報セキュリティ責任者の判断で緊急に対処する。
　本学の構成員が不正使用を行ったときは、学則、就業規則、懲戒規程、その他の諸規則に従って処分を受けることがある。

７．点検・評価

　情報セキュリティ委員会は、ポリシーに関する点検と評価のために以下のような情報を収集して必要に応じて検討する。

（ａ）本学の構成員からのポリシー遵守に関する意見と実施運用上の要望、クレーム
（ｂ）事故、故障、不正行為の事例、対策の成功事例、システム管理者からの意見や要望
（ｃ）ポリシーの実施状況についての点検・監査結果
（ｄ）情報システムの機密性、完全性および可用性ならびに犯罪予防の観点からの情報セキュリティ診断結果

　情報セキュリティ委員会は、これらの情報をもとに、ポリシーの実効性を評価し、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。