

公立大学法人青森公立大学
情報セキュリティポリシー

平成29年3月31日 策定

公立大学法人青森公立大学

1 情報セキュリティ基本方針

1-1 目的

公立大学法人青森公立大学（以下「本学」という。）の情報資産は、本学の重要な資産であり、漏えいや改ざん・遺失が生じた場合には、本学の教育研究活動の停滞、本学の社会的信用の失墜につながりかねず、更には社会に大きな混乱や障害をもたらすことも懸念される。

このことから、本学の情報資産に関する情報セキュリティ対策の統一かつ基本的な事項を定めることにより、本学の教育研究活動の適正かつ円滑な実践を図ることを目的とする。

1-2 用語の定義

公立大学法人青森公立大学情報セキュリティポリシー（以下「ポリシー」という。）で使用する用語の定義は、次のとおりとする。

（1）情報

本学の教育・研究・管理運営に関わる者が作成し、又は取得した内容が記録された電子情報。

（2）情報資産

- ①ネットワーク、情報システム及びこれらに関する設備及び電磁的記録媒体
- ②ネットワーク及び情報システムで取り扱う情報
- ③情報システムの仕様書及びネットワーク図等の情報システム関連文書

（3）情報セキュリティ

情報資産の機密性（アクセスを許可された者だけが情報資産にアクセスできることを確実にすること）、完全性（情報資産及び処理方法が正確であること及び完全であることを保護すること）、可用性（許可された利用者が必要な時に情報資源にアクセスできることを確実にすること）を維持すること。

（4）情報システム

ハードウェア、ソフトウェア、ネットワーク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。

1-3 対象範囲

本学が所有するすべての情報資産及び本学の情報資産を利用するすべての者を対象とする。

2 情報セキュリティ対策基準

2-1 管理体制及び審議機関

本学の情報資産に関する情報セキュリティ対策を推進・管理するため、以下の管理体制及び審議機関により責任及び権限を明確にする。

(1) 管理体制

① 情報セキュリティ総括責任者

本学の情報セキュリティを総括する責任者として情報セキュリティ総括責任者（以下「総括責任者」という。）を置き、理事長の職をもって充てる。総括責任者は情報セキュリティに関する総括的な意思決定を行い、学内外に対する最高責任を負うものとする。総括責任者に事故があるときは、総括責任者があらかじめ指名するものが、その職務を代行する。

② 情報セキュリティ総括管理者

本学の情報セキュリティを総括する管理者として情報セキュリティ総括管理者（以下「総括管理者」という。）を置き、学長の職をもって充てる。総括管理者は、情報セキュリティの適正な管理を指揮監督する。

③ 情報セキュリティ管理者

本学の情報セキュリティの適正な管理を指揮監督する者として情報セキュリティ管理者（以下「管理者」という。）を置き、事務局長の職をもって充てる。管理者は情報セキュリティの管理について責任を負うとともに、教職員等へ必要な指導及び調整を行う。

④ 情報セキュリティ担当者

管理者を補佐するとともに、情報セキュリティ対策を担当する者として情報セキュリティ担当者（以下「担当者」という。）を置き、事務局教務学事グループリーダーの職をもって充てる。担当者は、責任者を補佐するとともに、情報セキュリティに関する事務を行う。また必要に応じて自らが指名した者に情報セキュリティ対策のための事務を行わせることができる。

(2) 審議機関

青森公立大学情報システム委員会規程により設置される青森公立大学情報システム委員会は、以下の情報セキュリティに関する事項を所掌し、情報セキュリティ対策を推進する。

① 情報セキュリティ対策の見直しに関する事項

② 情報セキュリティ対策の遵守状況の確認に関する事項

③ 情報セキュリティ対策の有効性の検証に関する事項

④ その他情報セキュリティ対策実施に必要な事項

2-2 情報の区分と対策等

本学の情報資産は、これを非公開情報と公開情報（限定公開情報を含む。）に区分するものとする。また当該区分、情報セキュリティ対策並びに情報機器及び電磁的記録媒体の処分方法に関しては実施手順に定めるものとする。

2-3 評価・見直し

本ポリシー及び実施手順において定めた事項の遵守状況や新たな脅威等を踏まえた有効性の検証に基づく本ポリシー及び実施手順の見直しを必要に応じて行うものとする。

2-4 法令等の遵守

本学の情報資産を利用する者は、情報セキュリティに関する各種法令の規定を遵守する。