

# 公立大学法人島根県立大学情報セキュリティ対策基本計画(2026年度版)

## 第1章 目的

情報セキュリティ対策基本計画(以下、「基本計画」という。)は、公立大学法人島根県立大学(以下、「本学」という。)の自己点検として行う情報セキュリティ監査(以下、「内部監査」という。)、及び、外部組織による監査(以下、「外部監査」という。)の指摘に基づき、本学に存在する情報セキュリティリスク(以下、「リスク」という。)を適切に評価し、中長期的な視点をもって当該リスクを制御することを目的とする。

## 第2章 用語の定義

公立大学法人島根県立大学情報システム運用基本規程第3条(用語の定義)に準ずる。

## 第3章 対象とする脅威

以下の脅威を想定し、情報セキュリティ対策を実施する。

- (1)不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報漏えい・破壊・改ざん・消去、重要情報の搾取、内部不正等
- (2)情報資産の無断持ち出し、無許可ソフトウェアの仕様等の規定違反、操作・設定ミス等の人為的  
要因による情報漏えい・破壊・消去等
- (3)設計・開発の不備、プログラム上の欠陥、メンテナンス不備、機器故障等のシステム要因による情報漏えい・破壊・消去等
- (4)内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥等の統制上の要因による情報漏えい・破壊・消去等

## 第4章 適用範囲

公立大学法人島根県立大学情報システム運用基本規程第4条(適用範囲)に準ずる。

## 第5章 職員等の遵守義務

公立大学法人島根県立大学情報システム運用基本規程第5条(管理者及び利用者の義務)に準ずる。

## 第6章 全体方針

情報セキュリティ対策の全体方針として、内部監査・外部監査によって指摘された内容を元に、情報システムの技術的な構成や、情報資産を取り扱う体制を改善するための施策を行うと共に、「情報セキュリティ講習に関する規程」に従い、学生・教職員への利用者教育を行う。その後、再度、内部監査・外部監査にて対策の実施状況の確認と、新たなリスクの洗い出しを行い、監査と改善を繰り返すことにより、本学情報セキュリティの向上を図る。

## 第7章 個別取組

### 7.1 体制の整備／技術的な施策

- (1)情報資産の重要性と利用者を明確にし、情報システムにて制御を行うことで機密性を確保する。
- (2)情報の持出し・持込みに利用するパソコン機器、外部記憶媒体、電子メールに安全な仕組みを

整備した上で、運用ルールを徹底させる。

(3)前年度の内部監査・外部監査での指摘事項・セキュリティ診断への対処を行う。

## 7.2 教育・訓練

(1)学生・教職員に対し、情報セキュリティ関連規程を理解、遵守させるため、情報セキュリティ教育（集合研修、オンライン研修、アンケート等）を行う。

(2)情報システム担当者が最新の情報セキュリティ対策を行うことができるよう、一般企業の情報セキュリティ研修に参加する。

(3)最新の情報セキュリティ情報を収集し、全学学生・教職員に周知・注意喚起する。

## 7.3 自己点検・監査

(1)内部監査、外部監査、専門家によるセキュリティ診断等により、上記 7.1、7.2 が適切に行われていることを確認する。

(2)内部監査、外部監査での指摘事項、及び、最新の情報セキュリティ状況にあわせ、情報セキュリティ関連規程の見直しを検討・改正する。

(3)内部監査、及び、外部監査により、関連規程に従っていないものや改善が必要なものの指摘を受け、次期情報セキュリティ基本計画に反映する。

(目的)

**第1条** この規程は、公立大学法人島根県立大学（以下「法人」という。）並びに法人が設置する島根県立大学及び島根県立大学短期大学部（以下「大学」という。）における情報セキュリティ確保のため、大学の教育研究活動の支援のための基盤として整備される情報システムの管理及び運用について基本的な事項を定め、法人及び大学が管理する情報資産を適切に保護することを目的とする。

(運用の基本方針)

**第2条** 前条の目的を達するため、大学の情報システムは、この規程及び関連する規程等の定めるところにより、優れた秩序と安全性をもって安定的かつ効率的に運用し、全学に安全かつ安定した利用環境を供用する。

(用語の定義)

**第3条** この規程及びこの規程に基づいて策定する実施規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- (1) 情報システム サーバ、パソコン、モバイル機器、記憶媒体、システムソフトウェア、アプリケーションソフトウェア等、情報を取り扱う仕組みのうち、次のものをいう。
  - ア 法人により、所有又は管理されているもの
  - イ 法人との契約あるいは他の協定に従って提供されるものまた、広義には、情報システムが提供するサービスを実現するための、情報ネットワークを含めて情報システムという。
- (2) 情報ネットワーク 通信回線、ルータ等通信機器、ネットワークソフトウェア等、情報システム間を接続する仕組みのうち、次のものをいう。
  - ア 法人により、所有又は管理されているもの
  - イ 法人との契約あるいは他の協定に従って提供されるものまた、広義には、情報ネットワークを管理する情報システムを含めて情報ネットワークという。
- (3) 情報 情報には次のものを含む。
  - ア 情報システム内部に記録された情報
  - イ 情報システム外部の電磁的記録媒体に記録された情報
  - ウ 情報システムに係る文書に記載された情報
  - エ その他業務上必要な文書
- (4) 実施規程等 この規程に基づいて策定される規程、基準及び計画をいう。
- (5) 手順 実施規程等に基づいて策定される具体的な手順及びマニュアルをいう。
- (6) ガイドライン 実施規程等に基づいて策定される具体的な指針をいう。
- (7) 情報セキュリティポリシー この規程及びこの規程に基づいて策定される実施規程をいう。
- (8) 情報セキュリティ関連規程 情報セキュリティポリシー、手順及びガイドラインをいう。
- (9) 職員等 大学に勤務する常勤又は非常勤の教職員（派遣職員及び嘱託職員を含む）、役員、その他最高情報責任者が認めた者をいう。
- (10) 学生等 大学に在籍する学生、科目等履修生、聴講生、研究生、研究員、研究者及び最高情報責任者が認めた者をいう。
- (11) 利用者 職員等、学生等及び臨時利用者で、情報システムを利用する許可を受けて利用する者をいう。

- (12) 臨時利用者 職員等及び学生等以外の者のうち、大学情報システムを臨時に利用する許可を受けて利用する者をいう。
- (13) 情報セキュリティ 情報資産の機密性、完全性及び可用性を確保することをいう。
- (14) 電磁的記録 電子的方式、磁氣的方式、その他人の知覚によっては認識することができない方式で作られる記録で、コンピュータによる情報処理の用に供されるものをいう。
- (15) インシデント 情報セキュリティに関し、意図的若しくは偶発的に生じる法令、法人若しくは大学諸規程に違反する事故又は事件をいう。
- (16) 明示 情報を取り扱うすべての者が当該情報の分類について共通の認識となるように措置することをいう。
- (17) アカウント 正当な利用者であるか判別を行う必要がある情報システムにおいて、利用者又は電子計算機に付与された権限をいう。また、狭義には、利用者又は電子計算機に付与された識別符号(ユーザ ID)及び主体認証情報(パスワード)の組み合わせ、若しくはそれらのいずれかを指す。
- (18) 情報資産 情報並びに情報ネットワークに接続された情報ネットワーク機器及び電子計算機をいう。
- (19) 全学情報システム 大学として統合的に整備し、運用する情報システムをいう。
- (20) アカウント管理責任者 情報システムのアカウントを発行・停止・削除する権限を持った者であり、第7条及び第13条に定める。

(適用範囲)

**第4条** この規程は、情報システムを運用、管理及び利用するすべての者に適用する。

(管理者及び利用者の義務)

**第5条** 情報システムの運用、管理業務に携わる者及び利用する者は、情報セキュリティ関連規程、関係する法令及び条約を遵守しなければならない。

(最高情報セキュリティ責任者)

**第6条** 法人に、最高情報セキュリティ責任者(以下「最高情報責任者」という。)を置き、理事長をもって充てる。

2 最高情報責任者は、大学における情報セキュリティ確保に関する事務を総括する。

3 最高情報責任者がその職務を遂行できない場合には、最高情報責任者があらかじめ指名する者が、その職務を代行する。

(全学システム管理責任者)

**第7条** 大学に全学システム管理責任者(以下「全学管理責任者」という。)を置く。全学管理責任者は、情報基盤推進室長をもって充てる。

2 全学管理責任者は、最高情報責任者の指示により、情報セキュリティ関連規程に基づく情報システムの整備及び運用を行う。

3 全学管理責任者は、情報システムの運用、管理に携わる者及び利用する者に対して、情報システムの運用、管理及び利用並びに情報システムのセキュリティに関する講習を企画し、情報セキュリティ関連規程の遵守を確実にするための講習を実施する。

4 全学管理責任者は、情報システムのセキュリティに関する連絡と通報において大学情報システムを代表する。

5 全学管理責任者は、全学情報システムについて管理責任を負い、アカウントを発行・停止・削除する権限を持つ。

6 全学管理責任者は、全学に係る情報ネットワークの管理責任を負う。

(全学情報セキュリティ委員会)

**第8条** 大学情報システムの円滑な運用に資する情報セキュリティ確保のための審議機関として、本学に全学情報セキュリティ委員会（以下「全学委員会」という。）を置く。

2 全学委員会は、次の事項について審議する。

- (1) 情報セキュリティ対策、講習及び監査の実施に関すること。
- (2) 情報システム非常時行動計画の策定及びその実施に関すること。
- (3) その他必要な事項  
(全学委員会の構成員)

**第9条** 全学委員会は、次の各号に掲げる委員をもって構成する。

- (1) 最高情報責任者
- (2) 全学管理責任者
- (3) 副理事長、副学長、事務局長、出雲キャンパス事務部長、松江キャンパス事務部長

2 全学委員会は、必要に応じて委員以外の者を出席させて意見を聞くことができる。

(全学委員会の委員長)

**第10条** 全学委員会の委員長は、最高情報責任者をもって充てる。

(全学委員会の運営)

**第11条** 全学委員会は委員長が招集し、その議長となる。

(キャンパス情報セキュリティ責任者)

**第12条** 各キャンパスにキャンパス情報セキュリティ責任者（以下「キャンパス責任者」という。）を置くこととし、各キャンパスのキャンパス責任者は副学長をもって充てる。

2 キャンパス責任者は、各キャンパスが独自に整備する情報システムを総括し、運用方針を決定する。

(キャンパスシステム管理責任者)

**第13条** 各キャンパスにキャンパスシステム管理責任者（以下「キャンパス管理責任者」という。）を置くこととし、各キャンパスのキャンパス管理責任者は浜田キャンパスにあつては教育研究支援部長を、出雲キャンパス及び松江キャンパスにあつては事務部長をもって充てる。

2 キャンパス管理責任者は、次の情報システムについて管理責任を負い、アカウントを発行・停止・削除する権限を持つ。

- (1) 全学システムにおいて、キャンパスごとの運用が認められている部分
- (2) キャンパスが独自に整備する情報システム

3 キャンパス管理責任者は、キャンパス独自に整備された情報ネットワークの管理責任を負う。

(キャンパス情報セキュリティ委員会)

**第14条** キャンパス内の情報セキュリティの連絡調整機関として、各キャンパスにキャンパス情報セキュリティ委員会（以下「キャンパス委員会」という。）を置く。

2 キャンパス委員会は、次の事項について審議及び実施する。

- (1) キャンパス固有の情報システムの運用、利用及び講習に係る手順並びにガイドラインの整備並びにその実施に関すること
- (2) キャンパス内の連絡調整
- (3) その他必要な事項

(キャンパス委員会の構成員)

**第15条** キャンパス委員会は、委員長及び次の各号に掲げる委員をもって構成する。

- (1) キャンパス責任者
- (2) キャンパス管理責任者

2 キャンパス委員会は、必要に応じて委員以外の者を出席させて意見を聞くことができる。

(キャンパス委員会の委員長)

**第16条** キャンパス委員会の委員長及び副委員長は、キャンパス責任者及びキャンパス管理責任者をもって充てる。

(情報セキュリティ監査責任者)

**第17条** 情報システムにおける情報セキュリティの監査に責任を持つ者として、情報セキュリティ監査責任者(以下「情報監査責任者」という。)を置く。情報監査責任者は副理事長をもって充てる。

2 情報監査責任者は、監査に関する事務を統括する。

(システム管理者)

**第18条** 第7条に定める全学システム管理責任者、又は、第12条に定めるキャンパスシステム管理責任者の指揮の下、情報システムの運用及び管理の実務にあたる者であって、アプリケーションソフトウェア、業務プロセスに関することを所掌する業務管理者と、サーバ、ネットワーク、システムソフトウェア等に関することを所掌する基盤管理者からなる。

2 業務管理者及び基盤管理者は、それぞれが所掌する領域において、利用者がサービスを利用するために必要な情報提供、情報システムの運用・保守、アカウント管理、情報セキュリティ対策等の実務を行い、情報システムを安定して利用できるように努める。

3 情報システムごとのシステム管理者は、表の通りとする。

(表 情報システムごとのシステム管理者)

| 情報システム                 | システム管理者   |                            |
|------------------------|-----------|----------------------------|
|                        | 業務管理者     | 基盤管理者                      |
| 全学情報システム               | 別に定める(注1) | 図書情報課長                     |
| 各キャンパスが独自に整備する情報システム   | 別に定める(注1) | 図書情報課長(浜田)、<br>管理課長(出雲、松江) |
| 研究室、ゼミが独自に整備する情報システム   | 担当教員      | 担当教員                       |
| 課又は室が独自に整備する情報システム     | 担当課室長     | 担当課室長                      |
| 全学にかかる情報ネットワーク         | 該当なし      | 図書情報課長                     |
| 各キャンパスが独自に整備する情報ネットワーク | 該当なし      | 図書情報課長(浜田)、<br>管理課長(出雲、松江) |

(注1) KENDAI DATA に定める担当課室長とする。

(役割の分離)

**第19条** 情報セキュリティ対策の運用において、同一の者が次に掲げる役割を担うことができない。

(1) 承認又は許可事案の申請者と、その承認者又は許可者

(2) 監査を受ける者と、その監査を実施する者

(情報の分類)

**第20条** 最高情報責任者は、情報の取扱いに関する規程を整備する。

2 情報システムで取り扱う情報は、重要性に基づき分類し、必要に応じて取扱制限の指定及び明示を行う。

(情報システム利用)

**第 21 条** 最高情報責任者は、情報システムの利用に関する規程を整備する。

(情報セキュリティ講習)

**第 22 条** 最高情報責任者は、情報セキュリティ講習に関する規程を整備する。

(情報システム非常行動計画)

**第 23 条** 最高情報責任者は、情報システム非常時行動計画に関する規程を整備する。

(情報システム運用・管理)

**第 24 条** 最高情報責任者は、情報システム運用及び管理に関する規程を整備する。

(情報セキュリティ監査)

**第 25 条** 情報監査責任者は、情報システムにおける情報セキュリティ監査に関する規程を整備する。

2 情報監査責任者は、情報システムのセキュリティ対策がこの規程に基づく実施規程等に従って実施されていることを監査する。

(見直し)

**第 26 条** 最高情報責任者は、この規程等の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。

2 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及び問題点が認められる場合には、当該事項の見直しを行う。

(利用制限)

**第 27 条** この規程に基づく実施規程等に違反した場合の利用制限は、当該規程等に定めることとする。

(事務)

**第 28 条** 全学委員会及びキャンパス委員会の事務は、事務局において処理する。

(実施)

**第 29 条** この規程の実施に関し必要な事項は、別に定める。

#### 附 則

- 1 この規程は、平成 27 年 4 月 1 日から施行する。
- 2 島根県立大学・島根県立大学短期大学部情報システム管理規程(平成 19 年 4 月 1 日規程第 41 号)は、廃止する。
- 3 この規程は、平成 31 年 4 月 1 日から施行する。

#### 附 則

この規程は、令和 3 年 4 月 1 日から施行する。