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 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3章 個別取組

3.1 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。

3.2 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。

3.3 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 3.1、3.2 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。