

環太平洋大学 情報セキュリティポリシー

環太平洋大学（以下、「本学」という。）における教育・研究活動には、情報基盤の充実に加え、情報資産のセキュリティ確保が不可欠である。今般、社会の高度な情報化に伴い、情報媒体の種類（電磁的媒体、光学的媒体、紙媒体など）を問わず、本学が管理するすべての情報資産を対象とする「環太平洋大学セキュリティポリシー」（以下、「本ポリシー」という。）を新たに制定する。

I. 情報セキュリティの基本方針

1. 目的

情報資産は本学にとって重要である。本学における教育・研究活動は、情報の収集、格納、伝達、報告といった手段に依存している。情報資産が守られなければ、本学の教育・研究活動の停滞、本学に対する信頼の喪失などといった被害を受ける可能性がある。したがって、教職員、学生、およびすべての関係者が不断の努力をもって、本学の情報資産を「機密性」「完全性」「可用性」に配慮し、保護しなければならない。本学の提供する情報資産に関連するサービスを利用する者は、本ポリシーを遵守する責任があり、意図の有無を問わず、学内外の情報資産に対する権限のないアクセスや改ざん、複写、破壊、漏えい等をしてはならない。

本ポリシーが目指すものは、次のとおりである。

- (1) 本学の情報セキュリティに対する侵害の阻止
- (2) 学内外の情報セキュリティを侵害する行為の抑止
- (3) 情報資産の分類と管理の徹底
- (4) 情報セキュリティ侵害の早期検出と迅速な対応の実現
- (5) 情報セキュリティの評価と更新

2. 対象範囲および対象者

本ポリシーの対象範囲は、本学の管理するすべての情報資産である。「情報資産」とは、本学が組織として管理すべき情報およびそれを管理する仕組みをいう。ここでいう「情報」は、媒体（電磁的媒体、光学的媒体、紙媒体など）の種類を問わない。本学以外に保管される情報資産であっても、本学保有の情報資産として認められるものは対象となる。

本ポリシーは、本学の情報資産を利用する教職員、学生等のほか、利用を許可されたすべての者を対象とする。

3. 実施方法

本学には、対象者が本ポリシーおよび各種内規等を理解し、実施できるように教育、指導する責任があり、また、本ポリシーを実施するための「対策基準」、「実施手順」は、本学の規約等によって別途定めるものとする。なお、必要があれば、各部門のそれぞれの事情に応じて、本ポリシーに反しない範囲で、独自に対策基準や実施手順を作成する。

II. 対策基準

1. 組織・体制

情報セキュリティを組織的に管理運営する体制を確立するために、その役割と責任を定める。

(1) 情報セキュリティ最高責任者

本学は情報セキュリティに関する総括的な意思決定を行う情報セキュリティ最高責任者（以下 CISO）を置く。CISO は情報セキュリティに関する施策を定め、それを本学全体に徹底させるため必要な措置を実施する権限を有する。また、本ポリシーの解釈については CISO の解釈をもって最終決定とする。

(2) 情報セキュリティの審議体制

教育経営会議において、本ポリシーおよび情報セキュリティに関する重要事項を決定し、遵守状況の確認、評価および見直しを行うとともに、情報セキュリティ上のインシデントが発生した場合の対応状況を確認し、必要に応じて助言・指導・勧告を行う。

(3) 情報セキュリティ責任者および担当者

本学事務局に情報セキュリティ責任者を置き、情報セキュリティ責任者は、本学において保有する情報資産に対して責任を持つ。また、事務局および必要な部署に情報セキュリティ担当者を置き、業務遂行上で必要な情報セキュリティ実施手順を策定し、維持するための活動を行う。

2. 情報セキュリティ侵害の阻止

(1) 内外の情報セキュリティを侵害する行為の抑止

学内外を問わず、あらゆる組織、団体、個人等の情報資産を侵害してはならない。

(2) アクセス制限

情報の内容に応じてアクセス可能な利用者を定め、不正なアクセスを阻止するべく必要なアクセス制限を行わなければならない。利用者は、アクセス権限のない情報にアクセスしたり、許可されていない情報を利用したりしてはならない。

3. 情報資産の分類と管理

本学の情報資産に関しては、それが果たすべき役割と影響を十分に認識し、常にその機密性、完全性、可用性に配慮して適切に分類し、管理しなければならない。

- (1)「機密性」とは、情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。
- (2)「完全性」とは、情報が破壊、改ざんまたは消去されていない状態を確保することをいう。
- (3)「可用性」とは、アクセスを認められた者が、必要時に中断することなく、情報にアクセスできる状態を確保することをいう。

4. 法令等の遵守および違反への罰則

情報資産の取り扱いに関しては、法令および規則等についても遵守する必要がある。本ポリシーおよびセキュリティに関連する諸法規、条約ならびに本学が定める規約等に対する違反があった場合、本学各規程等にしたがって対処する。

5. 情報セキュリティおよびポリシーの罰則

情報資産を守るためには、適切な情報セキュリティ対策が実施されているか定期的に評価し、改善が必要と認められた場合は、速やかに更新しなければならない。また、本ポリシーの実効性を定期的に評価し、改善が必要と認められた場合には、変更内容および実施時期の決定を行い、セキュリティレベルが高く、かつ遵守可能なポリシーに更新しなければならない。

以上