

I 基本方針

1 趣旨

電動モビリティシステム専門職大学（以下「本学」という。）における教育研究活動は、情報の収集、保管、活用の上で成り立っている。情報管理が徹底していなければ、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、学生及び全ての関係者が不断の努力をもって、知り得た情報の機密性、完全性及び可用性に配慮し、保護しなければならない。本学が提供する情報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、権限のないアクセスや改ざん、複写、破壊、漏洩等をしてはならない。

- (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当該情報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、改ざん又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。

2 目的

本学は、本学の理念と使命を実現するため、本学で扱う情報及び情報システムを対象に情報セキュリティ対策を実施する。

この目的を達成するため、情報セキュリティ対策規程（以下「対策規程」という。）及びその他の規程等の定めるところにより、次に掲げる対策を行う。

- (1) 情報セキュリティ対策の実施体制の整備
- (2) 情報及び情報システムの保護
- (3) 情報システムや情報サービスの管理・運用
- (4) インシデントへの対処
- (5) 利用者への啓発・教育
- (6) その他情報セキュリティマネジメントの実施

3 対象範囲及び対象者

本ポリシーの対象範囲は、本学が組織として管理・運用すべき情報及びそれを管理する仕組みをいい、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であっても、本学保有の情報として認められるものは対象となる。

本ポリシーは、本学の情報を利用する教職員、学生等のほか、利用を許可され

た全ての者を対象とする。

4 利用者の義務

本学の情報及び本学で扱う情報システムを利用する者並びに管理・運用の業務に携わる者は、本ポリシー、対策規程その他の情報セキュリティに関する規程等を遵守しなければならない。

5 ポリシー違反に対する措置

本ポリシーに基づき定められる規程等に違反した場合の利用の制限及び罰則は、本学学則及び本学就業規則に則って行うほか、それぞれの規程に定めるところによる。

II 情報セキュリティ対策基準

1 実施体制

情報セキュリティを組織的に管理運用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

本学に、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「最高責任者」という。）を置き、学長をもって充てる。

最高責任者は、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最高責任者の解釈を持って最終決定とする。

(2) 情報セキュリティ委員会

本ポリシー及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、評価及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。

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

利用者は、学内外を問わず、あらゆる組織、団体、個人等の情報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 情報の分類と管理

本学において取り扱う情報について、重要情報を管理するため、重要度に応じた情報分類の定義、情報の管理責任及び管理方法等を定める。

4 物理的セキュリティ

情報システムの設置場所について、安全性を保ち、不正な立入りを阻止する対策を講じる。また、持ち運びを前提とした情報を保護するための対策にも十分に配慮する。

5 人的セキュリティ

情報セキュリティに関する権限や責任を定め、利用者に本ポリシーの内容を周知徹底するなど、十分な教育及び啓発が行われるよう、必要な対策を講じる。

6 技術的セキュリティ

本学の情報を学外又は学内からの不正なアクセスなどから適切に保護するため、情報へのアクセス制御、ネットワーク管理等の必要な対策を講じる。

7 運用

本ポリシーの実効性を確保するため、ポリシーの遵守状況の確認、ネットワークの管理等の運用面に関して必要な措置を講じる。

緊急事態が発生した際の迅速な対応を可能とするため、緊急時の対応計画を定める。

8 評価・見直し

本ポリシー、情報セキュリティ対策の評価、情報システムの変更及び新たな脅威などを踏まえ、定期的に本ポリシーの評価・見直しを実施する。

9 個人情報の保護

個人情報の保護に関する関係法令及び個人情報の取扱いに関する各種ガイドライン等を遵守しなければならない。また、業務上の権限を有しない者は、許可なく個人情報を閲覧してはならない。