湘南工科大学
情報セキュリティポリシー

平成２９年４月１２日

湘南工科大学情報セキュリティ委員会

湘南工科大学情報セキュリティポリシー

1　目的

湘南工科大学（以下「本学」という。）における情報資産について、高度情報社会において本学が学術研究・教育活動を高め継続的かつ安定的な業務の遂行を確保するとともに、社会的信頼の下に情報化を推進するため情報セキュリティポリシーを策定し、本学の利用者（役員、教員、事務系職員、臨時職員、非常勤教職員、学生（保護者、大学院生等を含む。）、来学者、委託業者等をいう。以下「利用者」という。）は、セキュリティの重要性を認識し、次に掲げる目標を達成するため情報セキュリティポリシーを遵守しなければならない。

（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
（4）情報セキュリティの評価と更新

2　定義

情報セキュリティポリシーで使用する用語の定義は、つぎのとおりとする。

（1） 情報資産

情報（紙媒体を含む）及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称。

（2） 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維持すること。

（3） 情報システム

ネットワーク機器（ルータ、スイッチ、ファイアウォール、ハブ、ケーブルなど）、サーバ機器、メインフレームシステム、パーソナルコンピュータ、プリンター、基本ソフトウェア、応用ソフトウェア、システム設定情報（パスワード、ファイル等）、記憶媒体（ＵＳＢメモリ、磁気ディスク、光ディスクその他取り外しが可能で情報が保存できるもの。）、システム構成図、持ち込まれたノートパソコン等の総称。

（4）情報セキュリティ対策基準

本学の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめたもの。どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定。

（5）情報セキュリティ実施手順

情報セキュリティ対策基準に定められた内容を具体的な情報システムにおいて、どのような手順に従って実行していくのかを示すもの。

3　対象範囲ならびに対象者

本学における情報セキュリティポリシーの対象範囲は、本学の管理する機器、ネットワーク、一時的にネットワークに接続された機器および情報資産である。情報セキュリティポリシーの対象者は、本学の情報資産を利用するすべての者とする。

4　組織・体制

情報セキュリティの確保のための組織・体制は、本学教員、事務系職員（以下「職員」という。）が一体となって情報セキュリティ対策を推進するための組織・体制を定める。

本学の情報セキュリティを統括管理するために、最高情報セキュリティ責任者及び全学システム管理責任者を置く。 最高情報セキュリティ責任者には学長をあてる。また、全学システム管理責任者にはメディア情報センター長をあてる。

部局ごとに部局システム管理責任者を置く。 各部局の部局システム管理責任者は、その責任のもとにシステム管理者を置くことができる。 情報セキュリティ担当部局は、メディア情報センターとする。

5　情報セキュリティ対策基準

本学の情報資産の適切な保護を維持するため、情報資産の重要度に応じた分類、管理方法、管理責任を明確にした情報セキュリティ対策基準を定め、これに従って情報セキュリティ対策を行う。

6　情報セキュリティ対策

（1）人的セキュリティ

情報セキュリティ対策基準に規定した事項を的確に実行し、検証していくための組織・体制に対して責任と権限を定める。本学の情報資産を用いた業務に携わるすべての利用者に情報セキュリティポリシーを周知徹底させるとともに、各人がどのような権限と責任を持っているかを明らかにし、情報セキュリティポリシーに違反したときの対策を講じる。

（2）物理的セキュリティ

情報資産を事故ならびに不正な立ち入りによる損傷・盗難・妨害等から保護するため、情報システムの設置環境やシステム機器の管理方法について物理的な対策を講じる。また、机上のパソコンや持ち運びを前提としたノートパソコン等の情報資産を保護するための対策を講じる。

（3）技術的セキュリティ

情報資産を学外又は学内からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等に必要な対策を講じる。

7　運用

情報セキュリティポリシーの実効性の確保並びに不正アクセス及び不正アクセスによって他の情報システムに対する攻撃に悪用されることを防ぐため、情報セキュリティポリシーの遵守状況の確認、ネットワークの監視といった運用面に関して必要な措置を講じる。また、緊急事態が発生した際の迅速な対応を可能とするため、緊急時対応計画を講じる。

8　評価・見直し

情報システムの変更、情報技術の発展、新たな脅威及び情報セキュリティポリシーの遵守等を踏まえ、情報セキュリティ委員会で定期的に情報セキュリティポリシーの評価・見直しを実施し、必要な措置を講じる。

附　則

1　情報セキュリティポリシーは平成２９年４月１２日から施行する。