# 湘南工科大学
# 情報セキュリティ対策基準

平成２９年７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対策基準

## 1　情報セキュリティに対する侵害の阻止

### （1）不正アクセス、コンピュータウィルス等への対応

外部または内部からの不正アクセスやコンピュータウィルスが検出された場合、全学システム管理責任者、部局システム管理責任者、システム管理者及び情報セキュリティ担当部局は、対策が完了するまで関連する通信の遮断または該当する情報機器の切り離し等を実施する。また速やかに関係する部局システム管理責任者、情報セキュリティ担当部局及び全学システム管理責任者に報告する。

不正アクセスが継続する場合には、当該情報機器またはそれを接続するネットワークについて、定常的な利用の停止などの抑止措置をとることができる。

### （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なう。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てはならない。

## 2　学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、あらゆる研究・教育機関、企業、組織団体、個人等の情報資産を侵害してはならない。また、情報セキュリティポリシーの他、情報セキュリティに関連する法令及び本学が定める規程等を遵守しなければならない。

## 3　情報資産の分類と管理、事故発生時の対応

### （1）分類と管理

すべての情報は、非公開情報・限定公開情報・公開情報といった情報の重要度による分類に応じ、それぞれ必要な情報セキュリティ保護対策を講じる。

### （2）事故発生時の対応

非公開情報・限定公開情報の入った USB メモリ、PC や紙媒体の紛失等、情報漏えいの恐れがある事故が発生した場合には、速やかに関係する部局システム管理責任者、情報セキュリティ担当部局及び全学システム管理責任者に報告しなければならない。

## 4　情報セキュリティ対策の実施

１、２及び３に掲げた基準を満たすため、物理的、技術的な情報セキュリティ対策手順を具体的に定め、実施する。また、情報セキュリティポリシーの対象となる利用者に、それぞれに応じた教育、研修、啓発等を行い、情報セキュリティの重要性を理解させる。

## 5　権限と責任

### （1）最高情報セキュリティ責任者

最高情報セキュリティ責任者は、本学のすべての情報セキュリティに関する総括的な権限と責任を有し、全学的見地から、本学の情報セキュリティの維持・強化に努める。

### （2）全学システム管理責任者

全学システム管理責任者は、最高情報セキュリティ責任者を補佐し、全学の情報資産が適正かつ安全に運用されるように、情報セキュリティの維持並びに情報セキュリティ対策の強化を推進する。

### （3）部局システム管理責任者

部局システム管理責任者は、全学システム管理責任者と協力し、当該部局の情報資産が適正かつ安全に運用されるように、情報セキュリティの維持及び情報セキュリティ対策を実施する。

（4）システム管理者

システム管理者は、情報セキュリティ担当部局と協力し、担当する情報資産の情報セキュリティの維持・強化に必要とされる物理的、技術的な対策を実施する。

（5）情報セキュリティ担当部局

情報セキュリティ担当部局は、全学システム管理責任者のもと、全学の情報セキュリティポリシーの維持及び情報セキュリティ対策の推進に関する企画、実施、情報発信に努める。

（6）利用者

利用者は、本学の情報資産の利用に際し、これらを管理運用するシステム管理者等に協力するとともに、自らも情報セキュリティポリシーを遵守して本学の情報セキュリティの維持・強化に努める。

6　例外事項

本学の情報セキュリティに対し脅威が発生し、または発生する恐れがあるとき、全学システム管理責任者、部局システム管理責任者及びシステム管理者が、その影響及び被害を最小化するために実施した措置に対し、情報セキュリティポリシー及び対策基準に掲げる遵守義務を免除することがある。 最高情報セキュリティ責任者は、脅威に対する影響及び被害を最小化するためにやむを得ないと判断したとき、必要な改善措置がなされるまで情報セキュリティポリシーについて時限的例外措置を設けることができる。 これらの措置が取られた場合、情報セキュリティ委員会に報告されなければならない。

附　則

1　情報セキュリティ対策基準は平成２９年７月１３日から施行する。