

東京工科大学情報セキュリティ対策規程

(目 的)

第1条 この規程は、東京工科大学情報セキュリティに関する基本方針（以下「基本方針」という。）に基づき、東京工科大学（以下「本学」という。）が保有する情報資産を適切に保護し活用するため、本学における情報セキュリティ水準の維持及び向上に関し、必要な事項を定めることを目的とする。

(定 義)

第2条 この規程における用語の定義は、次の各号に定めるところによる。

- (1) 情報資産とは、情報システム及び情報システム内部に記録された情報並びに情報システム外部の電磁的記録媒体に記録された情報もしくは情報システムに関係がある書面に記載された情報をいう。
- (2) 情報システムとは、情報処理及び情報ネットワークに係るシステムで、本学により所有又は管理され、若しくは本学との契約あるいは他の協定に従って提供されるものをいう。
- (3) ガイドラインとは、基本方針及び本規程並びに関係諸規程（以下「基本方針等」という。）に基づいて策定される具体的な実施手順をいう。
- (4) 教職員等とは、本学の教職員（派遣職員、パートタイマー、外部機関に所属する本学常駐者を含む。）及び本学が委嘱する非常勤教育職員、特別研究員並びに片柳研究所等で外部機関等から参加する所員・研究員をいう。
- (5) 学生等とは、本学の学部学生、大学院学生、研究生、科目等履修生をいう。
- (6) 利用者とは、本学の教職員等及び学生等で、許可を受けて本学の情報システムを利用する者をいう。
- (7) 臨時利用者とは、利用者以外の者で、許可を受けて本学の情報システムを臨時に利用する者をいう。
- (8) 記録媒体とは、情報を記録した電磁的記録媒体あるいは情報を印刷した紙媒体等をいう。
- (9) 情報セキュリティインシデントとは、マルウェアの感染や不正アクセス、あるいは情報資産の流出など情報セキュリティ上の脅威となる事象をいう。

(適用範囲)

第3条 本規程は、本学の情報システムを管理する者及び利用者並びに臨時利用者に適用する。

(遵守義務)

第4条 本学の情報資産を利用する全ての者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたっては、基本方針等及びガイドライン並びにその他関連法令等を遵守しなければならない。

2. 本学の情報資産を利用する全ての者は、基本方針等の定めに従い、本学が保有する情報資産を保護するため、適切な情報セキュリティの確保に努めなければならない。

(最高情報セキュリティ責任者)

第5条 本学に情報セキュリティに関する業務の統括的な権限を有する者として、最高情報セキュリティ責任者(以下「CISO」という。)を置き、学長をもって充てる。

(CISOの職務)

第6条 CISOは、情報セキュリティ対策の推進責任者として、次の各号に掲げる職務を行う。

- (1) 情報セキュリティ対策組織の整備に関すること
- (2) 基本方針並びに情報セキュリティ対策推進計画の策定及び改廃に関すること
- (3) 情報セキュリティインシデントに対処するための指示及びその他の措置の実施に関すること
- (4) 情報セキュリティに関する教育に関すること
- (5) その他情報セキュリティ対策の推進に関すること

(全学情報システム責任者)

第7条 本学に全学情報システム責任者(以下、「システム責任者」という。)を置き、八王子キャンパス業務部長をもって充てる。

2. システム責任者は、本学の情報システムのセキュリティに関する連絡と通報に係る事項を総括し、CISOを補佐する。

(委員会)

第8条 本学の情報セキュリティの維持及び向上を図るため、東京工科大学情報セキュリティ委員会(以下「委員会」という。)を置く。

2. 委員会は、学長直属の委員会とする。
3. 委員会は、CISOを委員長、メディアセンター長を副委員長とし、次の委員をもって構成する。
 - (1) システム責任者
 - (2) CISOとシステム責任者が協議のうえ指名する教員 数名
 - (3) 大学事務局から委嘱される職員 若干名
4. 委員長は、必要に応じ委員以外の教職員及び情報セキュリティに関する専門的な知識や経験を有する有識者に出席を依頼することができる。

(審議事項)

第9条 委員会は、次に掲げる事項について審議する。

- (1) 基本方針等及びガイドラインの制定及び改廃に関すること
- (2) 本学において発生した情報セキュリティインシデントに関する措置及び再発防止策の策定に関すること
- (3) その他情報セキュリティに関すること

(教育)

第10条 CISO は、情報セキュリティ対策を推進するために必要と認める場合は、利用者に対し、適切な方法により情報セキュリティに関する教育を行わなければならない。

(点検)

第11条 システム責任者は、情報資産に係る物理的又は技術的若しくは人的セキュリティ対策について定期的な点検を実施し、その結果を CISO に報告しなければならない。

(情報セキュリティインシデント発生時の措置)

第12条 本学における情報資産を利用する全ての者は、情報セキュリティインシデントが発生したもしくは発生するおそれがある事実を知った場合には、その事実を速やかに大学事務局八王子キャンパス業務部業務課又は蒲田キャンパス事務部業務課（以下「業務課」という。）に報告しなければならない。

2. 前項の報告を受けた業務課は、システム責任者と協議のうえ、当該報告の内容を調査し、必要な措置について CISO に報告しなければならない。ただし、当該内容の調査の結果、緊急に措置を講ずる必要がある場合は CISO への報告を事後とすることができるものとする。
3. 前項の報告を受けた CISO は、委員会を開催し、当該事実が発生した原因を確定するとともに、必要な対応措置（緊急に措置を講じた場合を除く）及び再発防止策について検討するものとする。
4. CISO は、当該事実が発生した原因が第14条に該当すると判断した場合には、第14条に定める手続きをとらなければならない。

(利用制限)

第13条 CISO は、本学における情報資産を利用する全ての者が、故意又は重大な過失により基本方針等及びガイドライン並びに関係法令に違反した場合には、委員会の審議を経て本学情報システムの利用を制限することができる。

(懲戒)

第14条 CISO は、教職員等のうち就業規則又は嘱託職員就業規程（以下「就業規則等」

という。)に定める職員が故意又は重大な過失により基本方針等及びガイドライン並びに関係法令に違反し、それが就業規則等に定める懲戒事由に該当する疑いがある場合には、東京工科大学就業規則違反等に関する委員会にその事実を報告するものとする。

2. CISOは、学生等のうち本学の学生が故意又は重大な過失により基本方針等及びガイドライン並びに関係法令に違反し、それが学則又は大学院学則に定める懲戒に該当する疑いがある場合には、当該学生が所属する組織の長にその事実を報告するものとする。

(庶務)

第15条 この規程の庶務は、関係部署の協力を得て、業務課が行う。

(改廃)

第16条 この規程の改廃は、大学評議会の議を経て、学長が定める。

附 則

1. この規程は、令和2年9月1日から施行する。
1. この改正規程は、令和3年4月1日から施行する。