○学校法人東京電機大学情報セキュリティ基本規程

情報統括責任者
総合メディアセンター

第１章　総則

（目的）

第１条　本規程は、学校法人東京電機大学（以下「本法人」という。）情報セキュリティ基本方針に基づき、本法人が保有する情報資産を漏えい、改ざん、滅失、不正利用その他の脅威から保護するため、情報セキュリティの確保に関する管理体制及び基本的事項を定め、これにより、教育、研究及び管理運営の安全かつ継続的な実施を確保するとともに、本法人の信頼性を維持し、もって社会的責任を果たすことを目的とする。

（定義）

第２条　本規程において「情報資産」とは、本法人が保有し、教育、研究及び管理運営において利用する情報並びにこれを処理するために用いられる情報システム等であって、次に掲げるものをいう。

（１）情報ネットワーク及び情報処理・保存に係るシステム

（２）前号のシステムに接続され、又は当該システムの構成要素として用いられる情報機器

（３）前２号のシステム及び機器により生成、処理、保存、又は伝送される情報（電磁的記録を含む。）

（４）前各号のシステム及び機器に用いられるソフトウェア

（適用範囲）

第３条　本規程は、本法人の情報資産の管理・利用に適用する。

２　本規程は、本法人の役員、教職員、学生・生徒、研究員その他本法人の情報資産を利用するすべての者（以下「利用者」という。）に適用する。

３　本法人の情報資産の処理、管理又は取扱いを委託された者（以下「委託先」という。）及び情報資産の一部又はこれに関する情報を提供された者は、本規程を遵守しなければならない。また、委託先との契約においては、本規程の遵守及び情報セキュリティの確保に関し、必要な事項を定めることができる。

第２章　情報セキュリティ確保の基本原則

（基本原則）

第４条　本法人における情報セキュリティの確保は、次に掲げる基本原則に基づき実施す

るものとする。

（１）情報資産の保護

情報資産の機密性、完全性及び可用性を確保し、適切に保護すること。

（２）法令の遵守

情報資産の管理及び利用に当たっては、関係法令、本法人の諸規程及び契約上の義務を遵守すること。

（３）組織的な管理

情報セキュリティを確保するため、組織的かつ継続的な管理を行うこと。

第３章　情報セキュリティの管理体制

（管理責任者）

第５条　本法人は、情報セキュリティの確保及び推進を統括するため、次に掲げる管理責任者を置く。

（１）情報セキュリティ最高責任者及び情報セキュリティ最高責任者補佐

学校法人東京電機大学情報セキュリティ最高責任者に関する規程に基づき、本法人に情報セキュリティ最高責任者及び情報セキュリティ最高責任者補佐を置き、本法人における情報セキュリティに関する管理及び運営を統括する。

（２）情報セキュリティ実施責任者

本法人に情報セキュリティ実施責任者を置き、総合メディアセンター長をもって充てるものとし、本法人における情報セキュリティ対策の実施、運用及び維持を統括する。

（３）情報システム管理責任者

情報システムを設置し、又は運用する学部、学科、学系、系、研究室、中学校・高等学校及び各部署等に情報システム管理責任者を置くものとし、当該組織の長又はこれに準ずる者をもって充てる。

（情報セキュリティ戦略会議）

第６条　学校法人東京電機大学情報セキュリティ最高責任者に関する規程に基づき、本法人に情報セキュリティ戦略会議（以下「戦略会議」という。）を置き、情報セキュリティに関する基本方針、重要施策その他重要事項を審議する。

２　戦略会議の組織及び運営に関し必要な事項は別に定める。

（情報セキュリティ統括本部）

第７条　学校法人東京電機大学情報セキュリティ最高責任者に関する規程第８条に基づき、本法人に情報セキュリティ統括本部を置く。

２　情報セキュリティ統括本部は、戦略会議において決定された方針に基づき、本法人における情報セキュリティ対策が整合的かつ統一的に実施されるよう、必要な調整及び指

示を行う。

（セキュリティインシデント対応チーム（TDU-CSIRT））

第８条　本法人における情報セキュリティインシデントに迅速かつ適切に対応するため、セキュリティインシデント対応チーム（以下「TDU-CSIRT」という。）を置く。

２　TDU-CSIRTの組織及び運営に関し必要な事項は別に定める。

（情報セキュリティ統括実施機関）

第９条　本法人における情報セキュリティ対策の統括実施機関は、総合メディアセンターとし、戦略会議で決定された方針に基づき、具体的な企画、実施及び運用を統括して行う。

２　情報システムを設置し、又は運用する各部署は、前項に規定する統括実施機関からの指示に従い、また、本規程及び関連規程に基づき、当該部署における情報セキュリティ対策を適切に実施するものとする。

（情報セキュリティ関連規程）

第10条　本法人は、情報セキュリティを確実に確保するため、次に掲げる規程等を別に定める。

（１）情報セキュリティ対策規程

（２）情報セキュリティ確保のためのガイドライン

第４章　資産管理とアクセス権

（情報資産の分類と管理）

第11条　情報システム管理責任者は、所管する情報資産について、その重要性、機密性、完全性及び可用性の観点から適切に分類し、管理しなければならない。

２　情報システム管理責任者は、前項の分類に応じ必要な管理措置を講じなければならない。

３　利用者は、情報資産の分類に応じて適切に取り扱わなければならない。

４　情報資産の分類区分及び管理方法に関し必要な事項は別に定める。

（アクセス管理の原則）

第12条　情報資産の機密性、完全性及び可用性を確保するため、情報資産へのアクセス権を適切に管理しなければならない。

２　アクセス権は、利用者権限に基づき、必要な範囲に限り最小限を付与しなければならない。

３　利用者は、自己のアクセス権情報を適切に管理し、これを第三者に利用させ、又は開示してはならない。

第５章　事故・障害時の対応

（インシデントの報告及び対応）

第13条　本法人は、情報セキュリティインシデントに対しては、TDU-CSIRTを中心として、組織的かつ迅速に対応するものとする。

２　利用者は、情報セキュリティインシデント（そのおそれがある場合を含む）を認知したときは、速やかにTDU-CSIRTが定める窓口に報告しなければならない。

３　情報資産を利用する者及び関係部署等は、TDU-CSIRTの指示に従い、調査、拡大防止、復旧等に必要な措置に協力しなければならない。

第６章　啓発活動と点検

（啓発活動）

第14条　本法人は、情報セキュリティの確保及び向上を図るため、すべての利用者に対し、情報セキュリティに関する教育、訓練及び啓発活動を計画的かつ継続的に実施するものとする。

２　本法人は、情報セキュリティに関する意識の向上を図るため、必要な情報提供及び注意喚起を行うものとする。

３　利用者は、本法人が実施する教育及び啓発活動に協力しなければならない。

（点検）

第15条　本法人は、情報セキュリティ対策について定期的に点検を行い、必要に応じて改善を行うものとする。

第７章　措置

（違反者への措置）

第16条　本規程に違反し、本規程に基づく情報セキュリティの確保に重大な支障を及ぼすおそれがあると認められるときは、統括実施機関は、当該利用者に対し、情報セキュリティ確保のための措置を講ずることができる。

２　措置内容等は別に定める。

第８章　雑則

（雑則）

第17条　この規程に定めるもののほか、情報セキュリティに関し必要な事項は、別に定めることができる。

（改廃）

第18条　本規程の改廃は、戦略会議の議を経て、常任理事会において決定する。