○東京藝術大学情報セキュリティ対策基本規程

（令和５年３月23日
制　　定）

改正　　令和７年７月17日

（目的）

第１条　本規程は、本学における情報及び情報システムの情報セキュリティ対策について基本的な事項を定め、もって本学の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

（適用範囲）

第２条　本規程において適用対象とする者は、全ての教職員、並びに本学の情報システムの利用者及び臨時利用者とする。

２　本規程において適用対象とする情報は、以下の情報とする。

（１）教職員等が職務上使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

（２）その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報

（３）前２号のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報

３　本規程において適用対象とする情報システムは、本規程の適用対象となる情報を取り扱う全ての情報システムとする。

（用語定義）

第３条　本規程及び関連規則等において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）外部サービス　学外の者が一般向けに情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において本学の情報が取り扱われる場合に限る。

（２）外部サービス管理者　外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。

（３）外部サービス提供者　外部サービスを提供する事業者をいう。外部サービスを利用して本学に向けて独自のサービスを提供する事業者は含まれない。

（４）外部サービス利用者

外部サービスを利用する本学の利用者等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう。

（５）学生等　学生、生徒、研究生、研究員、研修員並びに研究者等、その他、部局総括責任者が認めた者をいう。

（６）機器等　情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

（７）教職員等　本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職員を含む。）その他、部局総括責任者が認めた者をいう。教職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。
（８）業務委託　本学の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において本学の情報を取り扱わせる場合に限る。
（９）記録媒体　情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R等の外部電磁的記録媒体がある。
（10）サーバ装置　情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。
（11）CSIRT（シーサート）　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対処するため、本学に設置された体制をいう。Computer Security Incident Response Teamの略。
（12）実施手順　対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。
（13）情報　第２条第２項に定めるものをいう。
（14）情報システム　ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を業務委託しているシステムを含む。）をいう。
（15）情報セキュリティインシデント　JIS Q 27000:2019における情報セキュリティインシデントをいう。
（16）情報セキュリティ関係規程　対策基準及び実施手順を総称したものをいう。
（17）情報セキュリティ対策推進体制　本学の情報セキュリティ対策の推進に係る事務を遂行するため、学内に設置された体制をいう。
（18）対策基準　本学における情報及び情報システムの情報セキュリティを確保するための対策の基準として定める「東京藝術大学情報セキュリティ対策基準」をいう。
（19）端末　情報システムの構成要素である機器のうち、利用者等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体

として扱われるキーボードやマウス等の周辺機器を含む。)をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、本学が調達又は開発するもの以外を指す「本学支給以外の端末」がある。また、本学が調達又は開発した端末と本学支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。

(20) 通信回線　複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。)の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

(21) 通信回線装置　通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

(22) ポリシー　本学が定める「東京藝術大学情報セキュリティ対策基本方針」及び本規程をいう。

(23) モバイル端末　端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

(24) 要管理対策区域 本学の管理下にある区域（学外組織から借用している施設等における区域を含む。)であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。

(25) 利用者　教職員等及び学生等で、本学情報システムを利用する許可を受けて利用するものをいう。

(26) 臨時利用者　教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用するものをいう。

(27) 部局　美術学部（大学院美術研究科を含む。)、音楽学部（大学院音楽研究科及び大学別科を含む。)、大学院映像研究科、大学院国際芸術創造研究科、附属図書館、大学美術館、社会連携センター、未来創造継承センター、言語・音声トレーニングセンター、演奏芸術センター、保健管理センター、芸術情報センター、藝大アートプラザ、事務局及び情報セキュリティ対策上これらに準じると学長が認めた組織をいう。

(28) 管理運営部局　本学の学内ネットワークや学内共同利用の情報システムの管理運営を行う部局をいう。

（全学総括責任者）

第４条　本学における情報セキュリティに関する事務を統括する全学総括責任者１人を置き、理事（経営改革・財務担当）をもって充てる。

２　全学総括責任者は、全学総括責任者を助けて本学における情報セキュリティに関する事務を整理し、全学総括責任者の命を受けて本学の情報セキュリティに関する事務を統括する全学総括副責任者１人を、必要に応じて置くことができる。

３　全学総括責任者は、以下の各号の事務を統括するものとする。

（１）情報セキュリティ対策推進のための組織・体制の整備

（２）情報セキュリティ対策基準の決定、見直し

（３）対策推進計画の決定、見直し
（４）情報セキュリティインシデントに対処するために必要な指示その他の措置
（５）前各号に掲げるもののほか、情報セキュリティに関する重要事項
（全学情報セキュリティ委員会の設置）
第５条　情報セキュリティ対策に関する重要事項を審議するため、全学情報セキュリティ委員会を置く。次項及び第３項に定めるものの他、全学情報セキュリティ委員会に関し必要な事項は、全学総括責任者が別に定める。
２　全学情報セキュリティ委員会の委員長は全学総括責任者とし、以下の各号に掲げる者を委員として組織する。
（１）全学総括副責任者
（２）全学実施責任者
（３）管理運営部局長
（４）部局総括責任者
（５）その他全学総括責任者が必要と認める者
３　全学情報セキュリティ委員会は、以下の各号の事項を審議するものとする。
（１）情報セキュリティ対策基準
（２）対策推進計画
（３）前各号に掲げるもののほか、情報セキュリティに関し必要な事項
（情報セキュリティ監査責任者）
第６条　全学総括責任者の指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置き、監事のうち全学総括責任者が指名する者をもって充てる。次項に定めるものの他、情報セキュリティ監査責任者及びその業務に関し必要な事項は、全学総括責任者が別に定める。
２　情報セキュリティ監査責任者は、全学実施責任者の命により次の事務を統括するものとする。
（１）監査実施計画の策定
（２）監査実施体制の整備
（３）監査の実施指示及び監査結果の全学総括責任者への報告
（４）前各号に掲げるもののほか、情報セキュリティの監査に関する事項
（管理運営部局）
第７条　管理運営部局は、芸術情報センターとする。
（管理運営部局が行う事務）
第８条　管理運営部局は、全学実施責任者の指示により、以下の各号に定める事務を行うものとする。
（１）本学の情報システムの運用と利用におけるポリシーの実施状況の取りまとめ
（２）講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
（３）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
（４）全学総括責任者及び全学実施責任者の支援
（５）部局技術責任者の支援
（全学実施責任者・部局総括責任者の設置）
第９条　部局ごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置き、各部局の長をもって充てる。部局総括責任者を統括

し、全学総括責任者及び全学総括副責任者を補佐する者として、全学実施責任者１人を置き、部局総括責任者のうち、事務局長をもって充てる。
２　全学実施責任者は、全学総括責任者及び全学実施副責任者の命を受け、以下の各号の事務を統括するものとする。
（１）要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定
（２）情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ
（３）情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備
（４）例外措置の適用審査記録の台帳整備等
（５）情報セキュリティインシデントに対処するための緊急連絡窓口の整備等
（６）前各号に掲げるもののほか、情報セキュリティ対策に係る事務
３　部局総括責任者は、全学総括責任者、全学総括副責任者及び全学実施責任者の命を受け、部局における情報セキュリティ対策を推進するため、以下の各号の事務を統括するものとする。
（１）定められた区域ごとの区域情報セキュリティ責任者の設置
（２）部局の職場情報セキュリティ責任者の設置
（３）情報システムごとの部局技術責任者の設置
（４）情報セキュリティインシデントの原因調査、再発防止策等の実施
（５）情報セキュリティに係る自己点検計画の策定及び実施手順の整備
（６）前各号に掲げるもののほか、部局の情報セキュリティ対策に関する事務
（区域情報セキュリティ責任者の設置）
第１０条　部局総括責任者は、前条第２項第１号の規定に基づき全学実施責任者が定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者１人を置かなければならない。
２　区域情報セキュリティ責任者は、部局総括責任者の命を受け、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を統括する。
（職場情報セキュリティ責任者の設置）
第１１条　部局総括責任者は、学科、専攻、センター、事務部、室、係等の管理組織単位を部局の状況に応じて適切に定め、各管理組織単位の長を職場情報セキュリティ責任者に指名するものとする。
２　職場情報セキュリティ責任者は、部局総括責任者の命を受け、管理組織単位における情報の取扱いその他の情報セキュリティ対策に関する事務を統括する。
（部局情報セキュリティ委員会）
第１２条　各部局に部局情報セキュリティ委員会を置く。次項並びに次条及び第１４条に定めるもののほか、部局情報セキュリティ委員会に関し必要な事項は部局総括責任者が別に定める。
２　部局情報セキュリティ委員会は、以下の各号の事項を実施するものとする。
（１）部局におけるポリシーの遵守状況の調査と周知徹底
（２）部局におけるリスク管理及び非常時行動計画の策定及び実施
（３）部局における情報セキュリティインシデントの再発防止策の策定及び実施
（４）部局における部局技術担当者向け教育の計画と企画

（部局情報セキュリティ委員会の構成員）
第１３条　部局情報セキュリティ委員会は、委員長及び次の各号に掲げる者を委員として組織する。
（１）部局技術責任者
（２）部局技術担当者
（３）その他部局総括責任者が必要と認める者
（部局情報セキュリティ委員会の委員長）
第１４条　部局情報セキュリティ委員会の委員長は、部局総括責任者をもって充てる。
（部局技術責任者の設置）
第１５条　部局総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局技術責任者を、当該情報システムの企画に着手するまでに選任しなければならない。
２　部局技術責任者は、部局総括責任者の命を受け、情報システムにおける情報セキュリティ対策に関する事務を担う。
３　部局技術責任者は、所管する情報システムの管理業務において必要な単位ごとに部局技術担当者を置くものとする。
（全学情報セキュリティアドバイザーの設置）
第１６条　情報セキュリティ対策への助言、支援等を行うため、全学情報セキュリティアドバイザーを置く。全学総括責任者が、情報セキュリティについて専門的な知識及び経験を有する者として指名した者をもってこれに充てる。
２　全学情報セキュリティアドバイザーは、以下の各号の業務を行うものとする。
（１）全学の情報セキュリティ対策の推進に係る全学総括責任者及び全学総括副責任者への助言
（２）情報セキュリティ関係規程の整備に係る助言
（３）対策推進計画の策定に係る助言
（４）教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援
（５）情報システムに係る技術的事項に係る助言
（６）情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言
（７）利用者に対する日常的な相談対応
（８）情報セキュリティインシデントへの対処の支援
（９）前各号に掲げるもののほか、情報セキュリティ対策への助言又は支　　援
（情報セキュリティ対策推進体制の整備）
第１７条　全学総括責任者は、情報セキュリティ対策推進体制を整備するため、以下の各項に定めるもののほか、必要な事項を別に定めなければならい。
２　情報セキュリティ対策推進体制に責任者を置き、全学実施責任者をもってこれに充てる。
３　情報セキュリティ対策推進体制は、以下の各号の役割を担うものとする。
（１）情報セキュリティ関係規程及び対策推進計画の策定に係る事務
（２）情報セキュリティ関係規程の運用に係る事務
（３）例外措置に係る事務

（４）情報セキュリティ対策の教育の実施に係る事務
（５）情報セキュリティ対策の自己点検に係る事務
（６）情報セキュリティ関係規程及び対策推進計画の見直しに係る事務
（７）全学情報セキュリティ委員会の運営に関する事務

（情報セキュリティインシデントに備えた体制の整備）

第１８条　全学総括責任者は、CSIRTを整備し、以下の各項に定めるもののほか、必要な事項を別に定めなければならない。

２　全学総括責任者は、教職員等のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任しなければならない。そのうちから、本学における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置くものとする。また、CSIRT内の業務統括及び外部との連携等を行う教職員等を定めなければならない。

３　全学総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備しなければならない。

４　全学総括責任者は、以下を含むCSIRTの役割を規定しなければならない。

（１）本学に関わる情報セキュリティインシデント発生時の対処の一元管理
ア　全学における情報セキュリティインシデント対処の管理
イ　情報セキュリティインシデントの可能性の報告受付
ウ　本学における情報セキュリティインシデントに関する情報の集約
エ　情報セキュリティインシデントの全学総括責任者等への報告
オ　情報セキュリティインシデントへの対処に関する指示系統の一本化

（２）情報セキュリティインシデントへの迅速かつ的確な対処
ア　情報セキュリティインシデントであるかの評価
イ　被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
ウ　文部科学省への連絡
エ　外部専門機関等からの情報セキュリティインシデントに係る情報の収集
オ　他の機関等への情報セキュリティインシデントに係る情報の共有
カ　情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

５　全学総括責任者は、実務担当者を含めた実効性のあるCSIRT体制を構築しなければならない。

６　全学総括責任者は、情報セキュリティインシデントが発生した際に、全学総括責任者が、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築しておかなければならない。

７　全学総括責任者は、全学における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定しなければならない。

（全学BCPとの整合）

第１９条　全学実施責任者は、情報セキュリティ関係規程の整備又は見直しを指示するに際し、当該規程が満たすべき要件として東京藝術大学事業継続計画（全学

ＢＣＰ）との整合性の確保を含めなければならない。

（兼務を禁止する役割）

第２０条　教職員等は、情報セキュリティ対策の運用において、以下の役割を兼務してはならない。

（１）承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う者

（２）監査を受ける者とその監査を実施する者

２　教職員等は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得なければならない。

（対策基準の策定）

第２１条　全学総括責任者は、全学情報セキュリティ委員会における審議を経て、サイバーセキュリティ戦略本部決定「政府機関等のサイバーセキュリティ対策のための統一基準群」に準拠した対策基準を定めなければならない。また、対策基準は、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めるものとする。

附　則

この規程は、令和５年４月１日から施行する。

附　則

この規程は、令和７年８月１日から施行する。