国立大学法人東京学芸大学
情報セキュリティポリシー

令和５年４月

Ⅰ情報セキュリティの基本方針

１．基本方針

国立大学法人東京学芸大学（以下「本学」という。）は，「豊かな人間性と科学的精神に立脚した学芸諸般の教育研究活動を通して，高い知識と教養を備えた創造力・実践力に富む有為の教育者を養成すること」を基本理念としている。また，「教員養成の基幹大学としての社会的責任を果たすべく幅広い教育情報の収集発信基地となる」ことを基本方針のひとつとしている。

これらの理念・目標を達成するためには，質の高い情報資源と高度な情報基盤・システムの整備が必要なことは言うまでもないが，同時に利便性の向上に伴う情報の拡散性に起因する重大な危機の発生が予測される中で，本学に帰属する情報資産に対する情報セキュリティの確保は必要不可欠である。特に，平成17年４月１日から施行された「個人情報保護法」及び平成28年１月からの「社会保障・税番号制度（マイナンバー）」の取扱いと併せて，情報セキュリティ対策は本学を挙げて取り組むべき重要課題である。

また，東日本大震災等の自然災害を教訓に，近年，防災・減災対策として災害発生時の緊急避難情報の発信や安否確認等に最大限の情報通信技術の利活用が求められ，さらには自然災害や大事故等による突発的な環境の変化や不測の事態に対し重要な事業を中断させない，もしくは短期間での業務復旧が求められている。本学においても，大学情報資産の保護及び事業継続計画に関し，情報資産の学内外バックアップ体制や大学間連携の検討・整備を図っていく。

本学は，「情報セキュリティポリシーに関するガイドライン」（平成12年７月18日情報セキュリティ対策推進会議決定）及び「独立行政法人等の保有する個人情報の保護に関する法律」（平成15年法律第59号）を踏まえ，情報セキュリティの重要性を，本学の役員，職員（役員及び職員には非常勤を含む。以下「教職員」という。）及び学生等，本学の構成員全てに周知してその責任を明確にするとともに，情報資産の安全性を確固たるものにするために「国立大学法人東京学芸大学情報セキュリティポリシー」を定める。

このポリシーによって，目指すものは以下のとおりである。

(1) 本学の情報セキュリティに対する侵害の阻止
(2) 学内及び学外の情報セキュリティを損ねる加害行為の抑止
(3) 情報資産に関して，重要度による分類とそれに見合った管理
(4) 情報セキュリティに関する情報取得の支援

２．用語の定義

用語については，「情報セキュリティポリシーに関するガイドライン」（平成12年７月18日情報セキュリティ対策推進会議決定）の定義と同様とし，附録１に示す。なお，一部の用語については，本学用に再定義したものもある。

３．対象範囲

３．１　対象となる情報資産

このポリシーの対象となるものは，本学が保有する全ての情報資産，機器であるが，本学以外のコンピュータで本学のネットワークに一時的に接続されたコンピュータも含まれる。

３．２　対象者

このポリシーの対象者は，本学の構成員である教職員，学生，研究生，附属学校の幼児，児童，生徒，受託業者及び学外者（本学の施設等を利用する者）等，本学の情報資産を利用する者全てを含むものとする。

４．情報セキュリティガイドライン，情報セキュリティインシデント対応手順書等の作成

基本方針，管理運用及び対策基準の具体的な実施手順については，別に国立大学法人東京学芸大学情報セキュリティガイドライン，情報セキュリティインシデント対応手順書等（以下「規程・手順等」という。）を定める。

特に重要な情報資産を運用する部局においては，規程・手順等のほか，それぞれの情報資産について個別にガイドラインを作成する必要がある。個別に作成したガイドライン（以下「個別ガイドライン」という。）は，情報セキュリティ会議に報告するものとする。

５．情報資産に対する脅威

規程・手順等の策定に当たっては，情報資産への以下のような脅威が発生した場合の影響を考慮する。

(1) 物理的脅威：侵入，破壊，故障，停電，災害等
(2) 人的脅威：誤操作，無断持ち出し，不正行為，パスワードの不適切管理等
(3) 技術的脅威：不正アクセス，盗聴，コンピュータウイルス，改ざん，消去，DoS攻撃（Denial of Services：サービス拒否攻撃），DDoS攻撃（Distributed Denial of Service attack：分散DoS攻撃），なりすまし等

Ⅱ対策基準

１．組織・体制

このポリシーに基づく具体的事項について，企画，立案，実施，管理，評価及び継続的検討を行うために，情報セキュリティに係る組織を設置する。

（別紙１　情報セキュリティインシデント対応体制）

１．１　最高情報セキュリティ責任者

本学に最高情報セキュリティ責任者を置き，情報を所掌する副学長がこれに当たる。

最高情報セキュリティ責任者は，全学の情報セキュリティに関する総括的な意思決定と，学内，他の組織及び学外に対する責任を負う。

また，情報システムの円滑な運用に必要な措置をTGU-CSIRT責任者に指示するとともに，TGU-CSIRT責任者が行った緊急避難措置に対処する。

１．２　情報セキュリティ会議

本学に，全学の情報セキュリティに関し，ポリシー及びガイドライン等の策定・改訂並びに情報セキュリティに関する重要事項の審議を行うための組織として「情報セキュリティ会議」を置く。

情報セキュリティ会議は，最高情報セキュリティ責任者が委員長となる。

情報セキュリティ会議は，このポリシーの対象者に対して情報セキュリティに関する教育・啓発活動を行い，このポリシー及び規程・手順等（規程・手順等には，個別ガイドラインを含む。以下同じ。）の遵守を励行させる。

また，情報セキュリティ会議は，軽微なインシデント事案の対応を協議し，不正アクセス等，重大なセキュリティインシデント事案が発生したとき，最高情報セキュリティ責任者が召集する「緊急対策室」の構成員になり，対策を講じる。

１．３　全学システム管理責任者

全学システム管理責任者は，ＩＣＴ／情報基盤センター長がこれに当たる。

全学システム管理責任者は，全学の情報システム管理の実施に関し，緊急時の連絡等，総括的な対応に当たり，最高情報セキュリティ責任者を補佐する。

１．４　TGU-CSIRT責任者

TGU-CSIRT責任者は，ＩＣＴ／情報基盤センターの業務を担当する専任教員のうちから最高情報セキュリティ責任者が指名する。

TGU-CSIRT責任者は，TGU-CSIRT の業務を統括し，情報セキュリティインシデントの発生時に，あらかじめ最高情報セキュリティ責任者による承認を得た条件を満たす場合には，TGU-CSIRT責任者による判断に従って，本学情報ネットワークの緊急避難措置を行うことができる。

１．５　部局情報セキュリティ管理責任者

部局情報セキュリティ管理責任者は，各部局に配置し，部局の長がこれに当たる。

部局情報セキュリティ管理責任者は，部局システム管理責任者と協力し，情報セキュリティ会議の指示のもとに，部局の構成員に対して情報セキュリティに関する教育・啓発活動を行い，このポリシー及び規程・手順等の遵守を励行させる。

１．６　部局システム管理責任者

部局システム管理責任者は，部局情報セキュリティ管理責任者が指名する。

部局システム管理責任者は，部局内の情報セキュリティの実施に関し，TGU-CSIRT責任者との連絡等の対応に当たり，システム管理者を統括する。

また，部局内において情報セキュリティを守るために必要と判断したときは，部局情報セキュリティ管理責任者に連絡し，当該部局内の緊急避難措置をとることができる。

１．７　システム管理部会

全学システム管理責任者が主査となり，部局システム管理責任者で構成する。

システム管理部会は，全学の情報システムのセキュリティ管理を実施するための連絡調整を行う。

１．８　システム管理者

システム管理者は，当該部局の情報システムの管理者権限を有する者がこれに当たる。

システム管理者は，部局の情報システムごとの情報セキュリティを実施する。

２．情報資産の管理

２．１　情報コンテンツの管理責任

情報コンテンツの管理責任は，当該情報コンテンツを入手し，又は作成した部局の当該教職員（事務局にあっては，当該課長）が負う。

なお，本学が取り扱う電磁的に記録された情報コンテンツについては，システム管理者との間で，管理の範囲，責任及び権限を明確にする。

２．２　情報システムの管理責任

情報システムの管理責任は，当該情報システムを管理し，又は運用する部局のシステム管

理者が負う。

２．３　アクセス制限

情報コンテンツの内容に応じて，情報コンテンツにアクセス可能な利用者及び使用端末を定め，不正アクセス，情報の漏洩等が発生しないようにアクセス制限を行う。このポリシーの対象者は，アクセス権のない情報資産に入り込もうとしてはならない。

２．４　情報コンテンツの分類と管理方法

本学で取り扱う全ての情報コンテンツは，各部局において公開，非公開に分類し，それぞれ重要度（機密性，完全性及び可用性の要求度から判断）に応じた基準によって適切に管理する。

なお，大学に帰属する情報コンテンツのうち，その取扱いについて，国立大学法人東京学芸大学法人文書管理規則（平成22年規則第４号），国立大学法人東京学芸大学におけるウェブサイト等の運営規程（平成24年規程第14号）又は共同研究若しくは受託研究等の契約等により規定されるもの，その他法令等の定めがあるものについては，それによるものとする。

また，個人情報の取扱いに関しては，国立大学法人東京学芸大学の保有する個人情報の保護に関する規程（平成17年規程第７号）又は国立大学法人東京学芸大学特定個人情報等に関する取扱規程（平成27年規程第28号）によるものとする。

２．５　利用の責任

情報資産を利用する者（利用者）は，情報コンテンツの分類に応じて利用責任を有する。

３．情報セキュリティ対策

３．１　物理的セキュリティ

情報システムを構成するクライアント機器，サーバ機器及びネットワーク機器については，設置場所の管理，情報の機密性及び完全性の保持，保守対応等，適切な物理的対策を講じるものとする。

３．２　人的セキュリティ

１）情報セキュリティ対策の遵守義務と加害行為の禁止

本学の情報資産を管理又は利用する者は，情報セキュリティに関連する諸法規，条約等はもとより，このポリシー及び規程・手順等記載されている内容を遵守しなければならない。

また，このポリシーの対象者は，学内外の機関，団体，個人等の情報資産を侵害してはならず，東京学芸大学情報倫理憲章（平成13年10月16日制定）を遵守しなければならない。

２）教育及び訓練

情報セキュリティに対する意識を醸成・維持するために，本学の全ての構成員が情報セキュリティ及び個人情報保護の重要性を認識するとともに，このポリシー及び規程・手順等を理解し，これを実践することができるように，情報セキュリティ会議は計画的に教育

及び訓練を実施するものとする。

３．３　技術的セキュリティ

学内外からの不正アクセス等による情報資産の盗難，流出，改ざん，破壊又はなりすまし等を阻止するために，アクセス記録の取得，適切なアクセス制御，情報の機密性・完全性の保持，運用管理及び保守対策を講じるものとする。

３．４　運用

１）情報セキュリティ情報の収集と対策

情報セキュリティに関する情報を恒常的に収集し，必要な対策を講じる。

２）情報セキュリティ侵害時の対応策（緊急時避難）

情報セキュリティが侵害された場合，又は侵害されるおそれがある場合等においては，情報セキュリティインシデント対応手順書，及び情報セキュリティ会議が定めた緊急時対応に従い，対処する。

４．評価・見直し

本学は，このポリシーの運用実態の把握，セキュリティ診断，セキュリティ監査等の方法により定期的に対策基準の評価・見直しを行い，情報セキュリティの向上に努める。

評価・見直しは，情報セキュリティ会議において少なくとも年１回以上行うものとする。このポリシーの評価・見直し結果は，適切に規程・手順等に反映させるものとする。

附則

このポリシーは，平成17年12月21日から施行する。

附則

このポリシーは，平成18年4月1日から施行する。

附則

このポリシーは，平成20年4月26日から施行する。

附則

このポリシーは，平成23年3月31日から施行する。

附則

このポリシーは，平成24年3月31日から施行する。

附則

このポリシーは，平成25年4月1日から施行する。

附則

このポリシーは，平成26年3月5日から施行する。

附則

このポリシーは，平成29年3月16日から施行する。

附　則

このポリシーは，平成31年４月26日から施行し，平成31年４月１日から適用する。

附　則

このポリシーは，令和２年４月１日から施行する。

附　則

このポリシーは，令和４年４月27日から施行し，令和４年４月１日から施行する。

附　則

このポリシーは，令和５年４月１日から施行する。

附録１　用語の定義

○　ネットワーク機器（端末機器）

情報ネットワークの接続のために設置され，コンピュータにより情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール，ルータ，ハブ，情報コンセント又は無線ネットワークアクセスポイントを含む。）をいう。

○　クライアント機器

主としてパーソナルな利用で用いられ，他の情報機器へアクセスすることで処理を進めていくものを指す。クライアント機器には，学内に設置されたパーソナルコンピュータだけではなく，教職員，学生等が学内外に携帯し，本学において利用するコンピュータ類を含む。

○　サーバ機器

複数のクライアント機器からアクセスされ，共同で利用される情報機器をいう。

○　情報コンテンツ

国立大学法人東京学芸大学が保有する教育・研究・事務処理に関わる紙媒体及び電磁媒体等に記録された情報。

○　情報資産

情報コンテンツ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）並びにそこで取り扱われる情報の総称。ただし，別に定める場合を除き，情報は電磁的記録（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た記録をいう。）に限るものとする。

○　情報システム

同一組織内において，ハードウエア，ソフトウエア，ネットワーク，記録媒体で構成されるものであって，これら全体で国立大学法人東京学芸大学の教育・研究・事務処理を行うもの。

○　情報セキュリティ

情報資産の機密性，完全性及び可用性（注）を維持すること。

（注）ISMS（Information Security Management System）認証基準Ver.2.0

・機密性（Confidentiality）：アクセスを認可された者だけが情報にアクセスできることを確実にすること。

・完全性（Integrity）：情報及び処理方法が正確であること及び完全であることを保護すること。

・可用性（Availability）：認可された利用者が必要なときに，情報及び関連する資産にアクセス及び使用できることを確実にすること。

○　情報セキュリティポリシー

所有する情報資産の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。情報セキュリティの基本方針及び情報セキュリティ対策基準からなる。

○　情報セキュリティ基本方針（以下「基本方針」という。）

情報セキュリティ対策に対する根本的な考え方を表すもので，どのような情報資産を，どのような脅威から，なぜ保護しなければならないかを明らかにし，情報セキュリティに関する取組姿勢を示すもの。

○　情報セキュリティ対策基準（以下「対策基準」という。）

「基本方針」に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準，つまり「基本方針」を実現するために何をやらなければならないかを示すもの。

○　情報セキュリティガイドライン（実施手順）等

情報セキュリティポリシーには含まれないものの，対策基準に定められた内容を具体的な情報システム又は業務において，どのような手順に従って実行していくのかを示すもの。

○　情報セキュリティポリシーに関するガイドライン

政府全体の情報セキュリティについての基本方針及び各省庁におけるポリシー策定のために参考とする手引きであるとともに，各省庁が最低限行うべき対策を示すもの。

○　部局

事務局，総合教育科学系，人文社会科学系，自然科学系，芸術・スポーツ科学系，大学院連合学校教育学研究科，附属図書館，大学教育研究基盤センター機構，現職教員支援センター機構，先端教育人材育成推進機構，教育インキュベーション推進機構，附属学校運営部及び各附属学校，その他（施設プロジェクト等を含む）

附録２　主な情報セキュリティ関連法令等

・不正アクセス行為の禁止等に関する法律
・行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
・行政機関の保有する情報の公開に関する法律
・独立行政法人等の保有する個人情報の保護に関する法律
・電子署名及び認証業務に関する法律
・著作権法
・不正競争防止法
・犯罪捜査のための通信傍受に関する法律
・刑法

第７条の２（定義）
第157条第1項（公正証書原本不実記載等）
第158条第1項（偽造公文書行使等）
第161条の2（電磁的記録不正作出及び供用）
第234条の2（電子計算機損壊等業務妨害）
第246条の2（電子計算機使用詐欺）
第258条（公用文書等毀棄）
第259条（私用文書等毀棄）

・特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律
・サイバーセキュリティ基本法
・特定電子メールの送信の適正化等に関する法律
・国立大学法人東京学芸大学文書管理規則（平成26年6月）
・国立大学法人東京学芸大学の保有する個人情報の保護に関する規程（平成27年1月）
・国立大学法人東京学芸大学特定個人情報等に関する規程（平成27年12月）
・東京学芸大学情報倫理憲章（平成13年10月）

附録３　参考資料

１．情報セキュリティポリシーに関するガイドライン（平成12年7月18日情報セキュリティ対策推進会議決定）
２．大学における情報セキュリティポリシーの考え方（平成14年3月29日大学の情報セキュリティポリシーに関する研究会）
３．独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（平成16年9月14日[一部改正] 平成27年8月25日）
４．コンピュータセキュリティインシデントへの対応（1999年12月9日JPCERT）
５．情報セキュリティマネジメントシステム適合性評価制度 ISMS 認証基準（Ver.2.0　JIS Q 27001：2014）（2014 年 3 月 20 日日本情報処理開発協会）
６．高等教育機関の情報セキュリティ対策のためのサンプル規程集（2015 年版補訂 NII）
７．国立大学法人等における情報セキュリティ強化について（通知）（平成 28 年 6 月 29 日文部科学省）
８．大学等におけるサイバーセキュリティ対策等の強化について（通知）（令和元年 5 月 24 日文部科学省）

東京学芸大学情報セキュリティ対応体制