

立正大学情報セキュリティポリシー

第1章 情報セキュリティ基本方針

1. 目的

高度情報社会において、立正大学（以下「本学」という。）が研究教育及び事務管理等の大学運営に必要な情報環境の安全性を高めるためには、情報基盤の整備に加えて、情報資産のセキュリティ確保が不可欠である。

情報セキュリティの大切さを本学の全構成員が十分に認識し、情報資産を守るため、「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 首相官邸・高度情報通信ネットワーク社会推進本部（IT戦略本部）情報セキュリティ対策推進会議策定）」を踏まえ、本学は「立正大学情報セキュリティポリシー（以下「ポリシー」）を定める。

本ポリシーによって目指すものは、次のとおりである。

- ア 本学の情報セキュリティに対する侵害の阻止
- イ 本学内外の情報セキュリティを損ねる加害行為の抑止
- ウ 情報資産の分類とその重要度に見合った管理
- エ 本学構成員の情報セキュリティ対策実施に関する支援

2. 定義

用語の定義は、首相官邸・高度情報通信ネットワーク社会推進本部情報セキュリティ対策推進会議が定めた「情報セキュリティポリシーに関するガイドライン」にあるものと同様とする。

3. 対象範囲

本ポリシーの対象範囲には、本学の情報資産に加えて、下記の対象者が本学の情報資産に一時的にアクセスするための情報システムを含む。また、本ポリシーの対象者（以下「対象者」）は、教職員（非常勤・契約職員等を含む。）、大学院生、学部学生、研究生、科目等履修生、留学生、共同研究者、公開講座受講生、委託業者、来学者等とする。

4. 実施体制の整備

本ポリシーに基づいて、本学が保有する情報資産に対する統一的な情報セキュリティ対策を推進するための全学的な組織体制を整備する。

5. 情報セキュリティ実施手順の作成

本ポリシーの具体的な実施手順は、第2章の情報セキュリティ対策基準に基づいて、情報セキュリティ委員会が全学的に定め、部局の具体的な実施手順は、必要に応じて各部局が別途定めるものとする。

6. 研修と情報提供

対象者へ本ポリシーの趣旨の浸透を図り、対策の円滑な実施を進めるため、研修等を適宜実施するとともに、情報セキュリティに関する情報提供を随時行う。

7. 評価及び見直し

本ポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、見直しを適宜行う。

8. 遵守

対象者は、本ポリシー、情報セキュリティ実施手順（以下「実施手順」という。）及びその他情報セキュリティに関する関係法令等を遵守しなければならない。

第2章 情報セキュリティ対策基準

9. 趣旨

この基準は、情報セキュリティ基本方針（以下「基本方針」という。）に基づき、情報セキュリティ対策を講ずるに当たり遵守すべき行為及び判断等の基準を統一するため、必要となる基本的な要件を定めるものである。

10. 組織

情報セキュリティ管理上の役割と権限を明確にするため、情報セキュリティ管理運営組織を次のとおり構成する。

10.1 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、全学の情報セキュリティに関する総括的な意思決定及び学内外に対する責任を負う。（情報メディアセンター担当副学長）

10.2 全学システム管理責任者

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、緊急時の連絡などの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。（情報メディアセンター長）

10.3 情報セキュリティ委員会

情報セキュリティ委員会は、全学的なセキュリティポリシーの策定及び情報セキュリティに関する事項の企画立案を行う。

10.4 部局等システム管理責任者

部局等システム管理責任者は、部局内の情報システムの管理に関し、システム管理者を統括する。（事務局長、事務副局長、各事務局部長、各学部長、各センター長（情報メディアセンター長を除く））

10.5 システム管理者

システム管理者は、部局等システム管理責任者の下で、システム担当者との連絡調整を行い、当該部局システム及びセキュリティを管理する。（各部局課長（事務長））

10.6 システム担当者

システム担当者は、個々の情報機器、ソフトウェア及び情報を具体的に管理し、セキュリティを維持するための責任を負う。（各部局システムの担当者等）

注）情報機器とはパソコン、サーバ等のコンピュータ本体及びディスプレイ、プリンタ等の周辺機器をさす。

11. 情報の分類と管理

システム担当者は、情報をその内容に応じて、公開・非公開等に分類し、その重要度に応じた情報セキュリティ対策を講じなければならない。

12. 情報セキュリティ対策

システム管理者は、物理的・人的・技術的セキュリティの全ての観点から、適切な情報セキュリティ対策を講じなければならない。

12.1 物理的セキュリティ

12.1.1 サーバ機器の設置場所

サーバ機器は、管理する情報の重要度に従ってそれぞれ設定された管理区域内に設置し、許可された者以外が使用できないように、必要に応じて入退室の認証・記録や警備システムの設置など物理的なセキュリティ確保に努めなければならない。

12.1.2 情報機器及び記録媒体の盗難対策

システム管理者は、情報機器及び記録媒体の盗難予防に努めなければならない。

注) 記録媒体とはCD、DVD、MO、フレキシブルディスク、フラッシュメモリ等をさす。

12.1.3 情報機器及び記録媒体の学外持ち出し

個人情報及び本学の重要なデータが入った情報機器及び記録媒体は、無断で学外へ持ち出してはならない。やむを得ず、情報機器及び記録媒体を学外へ持ち出す場合は、情報の漏えいが発生しないように情報セキュリティ対策を講じなければならない。

12.1.4 情報機器及び記録媒体の学内への持ち込み

情報機器及び記録媒体を学内へ持ち込む場合は、ウイルスチェックを行うなどの情報セキュリティ対策を講じなければならない。

12.1.5 情報の原本と完全性

完全性が求められる情報の原本は、必要に応じて書換不能な記録媒体に保存するなどにより、原本性を確保しなければならない。

12.1.6 情報のバックアップ

サーバ機器等に記録するデータは、必要に応じて定期的にバックアップしなければならない。

12.1.7 情報機器及び記録媒体の処分

情報機器及び記録媒体を破棄する場合は、残存情報が第三者に読みとられることのないよう対策を講じなければならない。

12.2 人的セキュリティ

12.2.1 教育・研修

最高情報セキュリティ責任者は、情報セキュリティに関する啓発や教育を実施するために必要な措置を講じなければならない。

12.2.2 セキュリティ事故・障害時の対応と報告

情報セキュリティに関する事故・障害及び公開情報の改ざん等を発見した場合には、部局等システム管理連絡担当者又は当該のシステム担当者に直ちに報告しなければならない。

部局等システム管理連絡担当者及び各システム管理者は、発生した事故・障害等について、迅速な対応を講じるとともに、部局等システム管理責任者及び全学システム管理責任者に報告し、必要に応じて支援を要請しなければならない。また、重大な被害が発生した場合は、部局等システム管理責任者及び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に報告し、その指示に従わなければならない。

部局等システム管理責任者及び全学システム管理責任者は、発生したすべての情報セキュリティ上の事故等に関する記録を一定期間保存し、情報セキュリティ委員会に報告し、再発防止のための対策を講じなければならない。

12.3 技術的セキュリティ

12.3.1 不正アクセス等への対応

全学システム管理責任者は、不正アクセスの防止並びに検出するための適切な手段を講じなければならない。不正アクセスが検出された場合は、関連する通信の遮断又は該当する情報機器の切り離しを実施する。

12.3.2 アクセス制限

システム管理者は、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

るために必要なアクセス制限を行わなければならない。

1 2 . 3 . 3 ネットワークの運用管理

本学の基幹ネットワークの管理は、全学システム管理責任者が行い、サブネットワークの管理は、全学システム管理責任者によりその設置が許可された者がこれを行う。また、基幹ネットワーク及び重要なサブネットワークについては、ファイアウォール及び侵入検知システムを設置し、それらのログを一定期間保存しなければならない。

1 2 . 3 . 4 バックドアの排除

情報メディアセンターの管理外で、バックドア（PPPサーバ、外部ネットワークへの物理的接続、VPN装置及びソフトウェア等）を設置することは原則として禁止する。

1 2 . 3 . 5 ネットワーク接続機器

本学のネットワークに接続する情報機器はウィルス対策ソフトを導入し、OSのセキュリティアップデートを行うなどのセキュリティ対策を講じたものでなければならない。また、システム管理者は、正当な利用者のみが情報機器を利用できるように、当該情報機器に物理的認証や電子的認証などの設定を行わなければならない。

1 2 . 3 . 6 利用記録の保存と提供

個人情報などの非公開情報を管理するサーバ及び必要とされるサーバについて、アクセス記録を取得し、これを一定期間保存し、定期的にそのアクセス記録を分析し、侵入の試みがなされていないかなどをチェックしなければならない。また、全学システム管理責任者等からアクセス記録の提供を求められた場合は、速やかに応じなければならない。

1 2 . 3 . 7 パスワードの管理

自己のアカウントのパスワードは秘密としなければならない。また、十分なセキュリティを維持できるように、自己のパスワードの設定及び変更配慮しなければならない。

1 3 . 違反者への対応

本ポリシー及び実施手順に違反した者に対しては、本学の構成員であるなしに関わらず本学の情報資産の利用制限を行うことがある。また重大な違反をした者で、本学の構成員である者に対しては、関係規程に基づき処分を行うことがある。

1 4 . 評価・見直し

1 4 . 1 情報セキュリティの評価と見直し

最高情報セキュリティ責任者は、適切な物理的・技術的・人的セキュリティ対策が実施されているか、定期的に評価、調査及び監査を実施しなければならない。改善が必要と認められた場合は、速やかに必要な財源を確保して、情報セキュリティ対策を実施しなければならない。

1 4 . 2 情報セキュリティポリシーの評価と更新

情報セキュリティの評価等を行う場合は、情報セキュリティポリシーの実効性の観点から検討を加え、改善が必要と認められた場合には、実効性の高いポリシーに更新しなければならない。

－以上－