○学校法人東京歯科大学情報セキュリティポリシー

平成17年３月25日

改正　令和６年１月１日

学校法人東京歯科大学における教育・研究・診療活動には、情報基盤の充実に加え、情報資産のセキュリティ確保が不可欠である。本法人では、文部科学省が定めた「教育情報セキュリティポリシーに関するガイドライン」および総務省が定めた「個人情報の保護に関する法律」を踏まえ、本ポリシーを制定した。

Ⅰ　情報セキュリティの基本方針

１　情報セキュリティの基本方針

情報は学校法人東京歯科大学（以下、本法人）にとつて重要な資産である。本法人における教育・研究・診療活動は、情報の収集、格納、伝達、報告といつた手段で行われている。情報資産が守られなければ、本法人の教育・研究・診療活動は停滞し、さらに本法人に対する信頼の喪失などといつた被害を受けることとなる。したがつて、教職員、学生、及びすべての関係者が不断の努力により、情報資産の保全を行うことが必要である。本法人が提供するネットワークサービスを利用する者は、情報セキュリティポリシー（以下、ポリシー）を遵守する責任があり、意図の有無を問わず、学内外の情報資産に対する権限のないアクセスや改竄、複写、破壊、漏洩等をしてはならない。東京歯科大学情報システム管理室（以下、管理室）は、利用者がポリシー、ガイドライン及び各種規程等を理解し、実施できるように教育、指導をする責任を持つ。

２　趣旨並びに位置付け

ポリシーは、下記のとおりの目的をもつて、本法人の管理するコンピュータ、ネットワーク等を利用し情報を扱うにあたつて遵守しなければならない最低限の事項をまとめたものである。詳細は、条約、関連法規、本法人の各種規程等に従うものとする。

- 本法人の情報セキュリティに対する侵害の阻止
- 学内外の情報セキュリティを侵害する行為の抑止
- 情報資産の分類と管理
- 情報セキュリティの評価と更新

３　定義

用語の定義は、文部科学省が定めた「教育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。

https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

情報資産の定義は、情報並びに情報を管理する仕組みとする。

4　対象範囲並びに対象者

本法人におけるポリシーの対象範囲は、本法人の管理する機器、ネットワーク、一時的にネットワークに接続された機器、及び情報資産である。ポリシーの対象者は本法人の情報資産を利用するすべての者とする。

5　実施手順

ポリシーの実施手順は、本法人の規程等によつて別途定めるものとする。関連する規程等は付録に示すとおりである。

Ⅱ　対策基準

1　組織・体制

管理室は、情報セキュリティに関する意見を総括する。理事長はこれを承認し、学内外に対する責任を負うものとする。

ポリシーの策定並びに重要事項の決定は、管理室が行うものとする。

管理室は、システム管理の実施、緊急時の対応等にあたるものとする。

情報セキュリティに関する啓発及び教育については、管理室が担当し、自主管理ドメイン等の管理者に対する教育を行うとともに、利用者に対する幅広い教育を行う。

2　情報セキュリティ侵害の阻止

(1)　不正アクセス等への対応

外部又は内部からの不正アクセスが検出された場合、管理室は、関連する通信の遮断又は該当する情報機器の切り放しを実施する。不正アクセスが継続する場合には、当該情報機器又はそれを接続するネットワークに対し、事態を警告、対策をとるよう勧告、定常的な利用を禁止するなどの抑止措置をとることができる。

(2)　アクセス制限

管理室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べく必要なアクセス制限を行わなければならない。利用者は、アクセス権限のない情報にアクセスしたり、許可されていない情報を利用したりしてはならない。

3　学内外の情報セキュリティを侵害する行為の抑止

学内外を問わず、あらゆる研究・教育機関、企業、組織、団体、個人等の情報資産を侵害してはならない。また、情報セキュリティに関連する条約、諸法規並びに本法人が定める規約等を遵守しなければならない。

4　情報資産の分類と管理

本法人の提供する情報に関しては、それが果たす役割と影響を十分認識し、常にその情報の正確性と健全性に配慮しなければならない。また、提供することによつて利用者が被害を受けるいかなる情報も扱つてはならない。情報提供の際には、関連する条約、諸法規並びに本法人が定める規約等を遵守しなければならない。

(1)　情報資産の管理者

本法人の管理する機器に保存された情報は、管理室が管理しなければならない。本法人の管理するネットワークに個人の機器、又は自主管理ドメインの機器を接続した場合、当該機器内の情報は、利用者、又は自主管理ドメインの管理者がセキュリティポリシーにしたがい管理しなければならない。また、必要に応じて機器を含めたアクセス権限の管理、不正プログラムの感染、当該人以外の閲覧防止に関する措置等を取らなければならない。

(2)　非公開情報資産

個人情報、事務、研究・教育等の非公開情報を不当に利用してはならない。情報は適切に管理されなければならず、権限のない情報に対してアクセスを行つたり利用したりしてはならない。情報の盗難・漏洩等を防止するため、非公開情報を扱うネットワークは、暗号化や盗聴防止策を講じることが望ましい。また、情報が記録された媒体は、適切に管理されなければならない。さらに、不正な登録、閲覧及び操作が行われていないか、定期的に調査・確認しなければならない。

(3)　限定公開情報資産

特定の利用者に特定の情報を公開する場合、その情報の登録・閲覧は、許可された者が許可された操作だけを行えるように、認証、アクセス制御等を実施しなければならない。非公開情報を扱う場合と同じく、ネットワークは、暗号化や盗聴防止策を講じることが望ましい。さらに、不正な登録、閲覧及び操作が行われていないか、定期的に調査・確認しなければならない。

(4)　公開情報資産

あらゆる公開情報を不当に利用してはならない。情報は故意、破壊されないように適切に管理されなければならない。また、非公開情報を公開する場合には、個人情報の漏洩、プライバシーや著作権の侵害に十分注意し、公開できる情報だけを抽出し、公開してよい形に加工しなければならない。情報が記録された媒体は、適切に管理されなければならない。

(5)　情報機器及び記憶媒体の処分

非公開・限定公開・公開を問わず、情報機器及び記憶媒体を破棄する場合は、その処分方法に注意しなければならない。

Ⅲ　実施手順

1　情報セキュリティ並びにポリシーの教育

管理室は、本法人内の利用者がポリシー、ガイドライン及び各種規程、また個人情報の保護に関する法律等の遵守を含めた情報セキュリティ教育を実施しなければならない。教育の具体的な内容については別途定める。

2　情報セキュリティ並びにポリシーの評価と更新

(1)　情報セキュリティの評価と更新

本法人の情報資産を守るためには、常に最新の情報を取得し、適切な物理的・技術的・人的セキュリティが実施されているか定期的に調査・評価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、速やかに情報セキュリティの更新を行わなければならない。また、大規模災害や事件・事故、サイバー攻撃などに遭遇した際のシステムなどの早期復旧を確保する計画（BCP）も併せて更新する。

(2)　ポリシーの評価と更新

情報セキュリティの調査とともに、ポリシーの実効性を定期的に評価し、改善が必要と認められた場合には、変更内容及び実施時期の決定を行い、セキュリティレベルの高い、かつ遵守可能なポリシーに更新しなければならない。

附　則

このポリシーは、平成17年４月１日から施行する。

附　則

このポリシーは、令和６年１月１日から施行する。

付録

教育情報セキュリティポリシーに関するガイドライン（文部科学省）

https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

国民のためのサイバーセキュリティサイト（総務省）

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/intro.html