

はじめに

大阪河崎リハビリテーション大学における教育・研究・診療活動には多大な情報の発生と管理が伴うが、それらを情報資産ととらえて、その有効利用と管理・保全について以下にまとめ、本学における情報セキュリティポリシーとする。

1. 基本方針

情報は大阪河崎リハビリテーション大学(以下、本学)にとって重要な資産である。本学における教育・研究・診療活動は、情報の収集、格納、解析、伝達、報告といった手段で行われている。その情報資産には、積極的に開示し利用を図るべきものから、慎重にとり扱い遺漏や改竄の無いよう保全に努める情報まで各種ある。基本的には大学の扱う情報資産は有効活用を前提として、公開すべき性質のものが多いが、近年組織情報や個人情報等に関して非開示が望ましい種類の情報資産が、特にコンピューターネットワークを通じて改竄されあるいは遺漏する事件が相次いでいる。そこで、本ポリシーでは、本学における情報資産について、第一には、開示利用すべき情報資産は積極的にその公開に努めるものと確認し、第二に、内部利用のみに留めて遺漏流出等から守るべき情報資産の取扱いについて、あるいは本学情報資産を経由して外部情報への脅威となる事態が発生しないよう、教職員、学生、およ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と宣言する。本学において教育・研究・診療活動に関わり、媒体によらず学内情報資産を利用するものは、本情報セキュリティ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。本学情報セキュリティ委員会は、利用者が本ポリシー、情報セキュリティガイドラインおよび関連各種内規等を理解し、実施できるように教育、指導をする責任を持つ。具体的には、このポリシーの元に、情報セキュリティガイドラインを策定し、学内各施設の利用規程、各種内規を置くものとする。

2. 定義

情報資産の定義は、情報ならびに情報を管理する仕組みとする。

3. 対象範囲ならびに対象者

本学におけるポリシーの対象範囲は、本学の管理する情報機器、学内情報ネットワークおよびネットワークに接続された機器、および情報資産である、ポリシーの対象者は上記機器および情報資産を利用するすべての者とする(以下利用者という)。

4. 実施手順

ポリシーの実実施手順は、本学の規程、内規等によって別途定めるものとする。関連する規程、内規等は内規・ガイドラインに示すとおりである。

(別途ガイドラインや利用規程を作成)

5. 組織・体制

情報セキュリティ委員会委員長(以下、委員長)は、情報セキュリティに関する総合的な意思決定を行い、学長が承認し、学内外に対する責任を負うものとする。ポリシーの策定ならびに重要事項の決定は、委員会が行うものとする。委員会は、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および教育については、本委員会あるいは本学FD委員会が担当し、利用者に対する幅広い教育を行う。

1. 公開すべき情報に対するアクセスへの対応

外部または内部から正式な手続きを経て本学情報資産の開示を求められた場合、その公開について本委員会が審議の上決定し、学長に答申するものとする。また、学生の成績等の保護者への開示については本学教務委員会の方針に従い、広域災害等の緊急時における個人情報の取扱いについては、別に定める本学緊急災害時対策委員会(仮名)の基本方針に従い取り扱うものとする。公開に関しては、以下の4-(4)および(5)に従うものとする。

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

外部または内部からの不正アクセスが検出された場合、委員会は、緊急措置手順に従って関連する通信の遮断また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、所定の手続きに基づいて当該情報機器また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

委員会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、利用者はあらゆる研究・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、諸法規ならびに本学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

利用者は、本学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、提供することによって他の利用者が被害を受けるいかなる情報も扱ってはならない。情報提供の際には、関連する条約、諸法規ならびに本学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

本学の管理する機器に保存された情報は、委員会が管理しなければならない。本学の管理するネットワークに個人の機器を接続した場合、当該機器内の情報は、利用者、または当該機器の管理者がセキュリティポリシーに従い管理しなければならない。

(2)非公開情報資産

利用者は、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ない。権限のない情報に対してアクセスを行っ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。

(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、アクセス制御等が実施されなければならない。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、委員会は意図によらずシステムに影響を及ぼす異常な登録、閲覧およ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

情報資産の管理者を含む利用者は、あらゆる公開情報を不当に利用してはならない。情報は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、あるいは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)情報機器および記憶媒体の処分

非公開・限定公開・公開を問わず、情報機器およ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。

5. 情報セキュリティなら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

本学の情報資産を守るために、委員会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、定期的に評価・調査・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、速やかに情報セキュリティの更新を行わなければならない。

(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、変更内容とその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。