

I 目的

大阪工業大学(以下「本学」という)の教育ならびに学術研究等の活動において、学生の個人情報等、電磁的方法によって管理された重要な情報(以下「情報資産」という)の活用は不可欠である。本学の情報資産を利用する者は、情報セキュリティの重要性を認識し、適切な対策と運用に努めなければならない。

本ポリシーは、本学の情報セキュリティ対策の基本姿勢となり、情報資産を機密性・完全性・可用性の面において適切に管理し、関連する法令および規則を遵守し、不正アクセス等情報資産に対する学内外からの脅威を未然に防止することを目的とする。

II 適用範囲

本ポリシーの適用範囲は、本学の情報資産と情報ネットワークシステムを使用する情報機器ならびにこれらの利用者を対象とする。利用者については別途、本学情報センター利用内規に定める。

III 組織・体制

情報セキュリティの運用・管理は、図1の体制で行う。

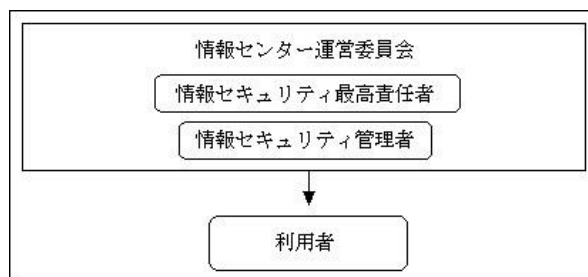


図1 情報セキュリティ組織・体制図

1 情報センター運営委員会

本ポリシーおよび各種ガイドラインの策定ならびに改訂、情報セキュリティ対策の実施、情報セキュリティ事案における対外的な対応等、情報セキュリティに関する重要な事項は情報センター運営委員会が執り行う。

また、本ポリシーの運用にあたり本委員会に情報セキュリティ最高責任者、情報セキュリティ管理者を設置する。

2 情報セキュリティ最高責任者

情報セキュリティ最高責任者は、全学的な見地に立ち、本学の情報セキュリティの維持・向上に努めなければならない。

情報セキュリティ最高責任者は、情報センター長がこの任にあたる。

3 情報セキュリティ管理者

情報セキュリティ管理者は、情報資産や情報機器を適切に維持・管理し、情報セキュリティの保護に努めなければならない。これらの管理を他に委託する場合は、責任と権限を明確にしなければならない。

情報セキュリティ管理者は、情報センター運営委員会内規第2条第1項ロ号からト号までの委員がこの任にあたる。

4 利用者

利用者は、本ポリシーはもとより、関連する法令を遵守しなければならない。

また、情報セキュリティ管理者から情報セキュリティ維持管理のために必要な措置を指示された場合、速やかに従わなければならない。

個人研究室および共同研究室ならびに事務部署等において特定の教職員が専有または所轄する情報資産については、当該教職員がその情報セキュリティについて責任を持って管理しなければならない。

IV 情報資産の管理

情報セキュリティ管理者は、情報資産を適切に管理しなければならない。

1 入退室管理

情報セキュリティ管理者は、情報資産を保存する情報機器等を設置した部屋への入退室を厳重に管理しなければならない。

2 情報機器の管理

情報セキュリティ管理者は、情報機器を適切に管理し、コンピュータウイルス対策や不正アクセス対策(ファイアウォールの設定、暗号化等)、機器の盗難・き損による情報漏洩や改ざん等の防止に努めなければならない。

3 アカウント(利用資格)の管理

情報機器にアカウントを付与する場合は、必要な利用者にも限定し、利用可能な機能も必要最低限としなければならない。

4 情報資産の管理

個人情報等の重要なデータを扱う場合は、暗号化やパスワードの設定等の措置を講じなければならない。

5 情報機器および記憶媒体の処分

情報機器および記憶媒体を廃棄する場合、情報資産が第三者に読み取られないようにした上で廃棄しなければならない。

V 違反時の罰則

本ポリシーに違反した者には、利用制限および利用資格停止等の措置をとる場合がある。

また、情報セキュリティ最高責任者は、重大な違反に対しては、他の学内意思決定組織と連携して必要な措置を講じる場合がある。

VI 事故・障害の報告

情報セキュリティに関する事故や障害等を発見した場合には、情報セキュリティ管理者または情報セキュリティ最高責任者へ速やかに報告しなければならない。

情報センター運営委員会は、発生した情報セキュリティ事案に関する記録を一定期間保存し、事案の影響度等に応じ、利用者への周知や啓蒙等迅速に再発防止策を講じなければならない。

本学からの不正アクセスによって学内外に被害を与え、その説明を被害者または第三者から求められた場合、情報セキュリティ最高責任者は関連部署と連携し対応しなければならない。

VII 教育

情報センター運営委員会は、情報セキュリティに関する啓発や教育等を全学的に実施するために必要な措置を講じなければならない。

また、利用者は、講習会および研修会等を通じて本ポリシーおよび実施手順を理解し、情報セキュリティの向上に努めなければならない。

VIII 評価・見直し

情報センター運営委員会は、本ポリシーが遵守されているか適宜、点検および評価を実施するものとする。

1 ポリシー運用実態の把握

情報センター運営委員会は、全学における本ポリシーの運用実態を適宜、調査しなければならない。

また、利用者から本ポリシーの遵守状況について意見を収集し、本ポリシーの運用が教育研究活動において利便性を著しく損なうことのないよう配慮しなければならない。

2 ポリシーの見直し

情報センター運営委員会は、本ポリシー運用実態の把握と利用者の意見等に基づき本ポリシーの実効性を評価しなければならない。また、情報セキュリティの動向等を踏まえ適宜、本ポリシーを見直さなければならない。

3 セキュリティ計画および予算措置

情報セキュリティ最高責任者は、評価・見直し等の結果を踏まえ、情報センター運営委員会の審議を経て、情報セキュリティ計画および予算措置等を講じなければならない。

4 報告義務

情報セキュリティ最高責任者は、必要に応じて他の学内意思決定組織に評価・見直し等の結果を報告しなければならない。また、その要約について全学の利用者に周知徹底しなければならない。

IX 適用時期

- 1 本ポリシーは、2014年9月17日より適用する。
- 2 この改正ポリシーは、2021年4月1日より適用する。