金沢大学情報セキュリティ方針

1　主旨

今日、コンピュータネットワークはその利便性のゆえに、人間が社会生活を営む上で必要不可欠のシステムとなった。金沢大学（以下「本学」という。）においても、教育・研究・社会貢献及び運営のすべてにおいて、積極的に活用されている。

しかしながら、システムへの依存度が高まるとともに、不正アクセス、情報漏洩といった情報セキュリティに関する問題が多発するようになり、情報資産の損失のみならず、営々として築いてきた信用すらある日突然崩壊するなど、深刻な事態に陥る組織をしばしば目の当たりにするようになった。特に、学外とのネットワーク接続は、本学における活動の効率向上をもたらす反面、インターネット上の脅威にさらされる可能性もある。

こうした状況から、本学の構成員である我々が学習すべき点は、ネットワークシステムを利用する際、その利便性を享受するだけに留まらず、被害を受けない・与えない利用の仕方や情報管理技術を身につけ実行していくことではないだろうか。

加えて、ネットワークへの接続にあたっては、接続そのものの企画から、管理・運用まで慎重に行わなければならない。

これらのことに鑑み、我々が情報資産を扱うとき、個人においては法令を守り、適切な情報リテラシー・マナーを身につけ、自身の情報管理を強化すること、又組織においては金沢大学情報セキュリティに関する規程（以下「規程」という。）に則し、ネットワークシステムを管理・運用していく必要がある。

この情報セキュリティ方針は、以上の主旨の下に、本学の有する情報資産の保護及び活用に関する方針を定めるものである。

2　情報セキュリティポリシーの適用者

情報セキュリティポリシーにおいては、規程第 2 条 7 号でいう「利用者」を次のとおり細分化し、適用する。

（1）構成員

- 国立大学法人金沢大学規則等で定める役員、職員（出向者を含む）等（以下「職員等」という。）
- 金沢大学学則で定める学生、研究生、科目等履修生、特別聴講学生及び外国人留学生（以下「学生等」という。）

（2）準構成員

- 派遣職員・学外研究員等、職員等から委託や許可等を受け、構成員と同等に教育・研究又は大学運営に従事する者

（3）業務受託者

・ 職員等から業務を受託し、業務上の情報資産の利用や扱いに関する許可等を受けた者

（4）旧構成員

・ 過去に本学の構成員であった者（名誉教授を除く。）

（5）名誉構成員

・ 名誉教授、名誉博士等

（6）外来者

・ 本学に入構した上記以外の者

2.1 利用者の責務

利用者は、本学の教育・研究・社会貢献・運営及びそれらの支援活動（以下「教育・研究等」という。）のため情報資産を利用することができるが、私的利用を行うことで、これら教育・研究等の円滑な遂行を阻害することがあってはならない。

情報資産を扱うにあたり、利用者は情報セキュリティポリシーを遵守しなければならず、これに違背した者は、その結果について責任を負わなければならない。

加えて、情報セキュリティポリシー遵守意思の有無を問わず、結果として情報セキュリティ侵害等が発生したときは、学外への影響を最小限に抑え、かつ、本学の社会的信用や情報資産の損失を防ぐため、当該行為をなした者の利用制限を行い、場合によっては関係するネットワークを切断する等の措置も有りうる。更に、情報セキュリティ侵害等の程度によっては、利用制限・切断等といった措置に留まらず、学則等に基づく本学の懲戒処分、司法による刑罰等の社会的制裁、被害者からの損害賠償請求等の不利益を受ける可能性も有りうる。

以上の措置・処分等の可能性については、日頃から十分留意するよう要請するところである。

2.2 準構成員、受託業務者に対する本学の対応

準構成員、受託業務者に情報資産の利用や扱いに関する委託や許可等を与える者は、情報セキュリティポリシーで定める遵守事項及び違背時における責任に関し事前説明を行わなければならない。

2.3 外来者に対する本学の対応

外来者による本学の情報資産の利用は、原則として制限される。ただし、その利便性に配慮してのネットワーク環境の提供等、目的が適正であると判断できる場合については、情報セキュリティ対策が十分であることを条件に認める場合がある。

3　情報セキュリティポリシーの公開範囲

本文書である情報セキュリティ方針（以下「方針」という。）は、学内外に開示する。

情報セキュリティ対策基準（以下「対策基準」という。）及び情報セキュリティ対策実施手順書（以下「手順書」という。）は、構成員及び準構成員に開示する。

なお、上記該当者以外に開示しなければ業務を遂行できない場合に限り、情報セキュリティポリシーのうち当該部分の開示を認めることがある。

4　情報セキュリティ対策の実施体制

規程に定める情報セキュリティ対策部会、ネットワークシステム管理部会等の役割等については、次のとおりとする。

4.1　情報セキュリティ対策部会

情報セキュリティ対策部会（以下「対策部会」という。）は、本学の情報セキュリティの維持及び向上を図るため、次の事項を所掌する。

- 情報セキュリティポリシーの点検・評価
- 情報セキュリティポリシーに基づく情報機器等の監査
- 上記の点検・評価、監査の結果に基づく改善策の立案
- 情報セキュリティインシデントに関する対応策の立案

対策部会は、最高情報セキュリティ責任者（CISO：Chief Information Security Officer）（以下「最高情報セキュリティ責任者」という。）が指名する部会長及び部会員で構成される。

4.2　学術メディア創成センター

学術メディア創成センターは、本学のネットワークシステムに接続された情報機器の包括的な管理責任を有し、全学的な情報セキュリティ対策を実施する部署である。

学術メディア創成センターは、本学に関係する情報セキュリティに関する情報の収集・分析を行い、学内の情報セキュリティ対策に反映するとともに、必要に応じて対策部会に報告するものとする。

4.3　ネットワークシステム管理部会

ネットワークシステム管理部会（以下「管理部会」という。）は、規程に定めるもののほか、情報セキュリティ対策について検討しその改善を担うものとする。

管理部会長は、学術メディア創成センター長（以下「センター長」という。）をもって充て、管理部会員は、最高情報セキュリティ責任者が指名する者をもって充てる。

4.4　部局ネットワークシステム管理者

部局ネットワークシステム管理者（以下「部局管理者」という。）は、規程の定めるもののほか、当該部局内における情報機器及びネットワークシステムの管理運用、情報セキュリティに関する情報の収集及び啓発を行い、収集した情報を管理部会に報告するものとする。

部局管理者として、学術メディア創成センターを除く各部局等に教職員１名を置くものとする。

4.5　情報セキュリティ管理者

部局等あるいは研究室等が保有する情報機器に対して情報セキュリティ対策を実施するため、情報セキュリティ管理者を置くものとする。

情報セキュリティ管理者は、部局管理者が指名する。

4.6　技術担当者

情報セキュリティ管理者は、情報セキュリティ作業等を行うに当たり、必要に応じて当該部局等の学生を含む構成員の中から、技術担当者を置くことができる。

5　情報セキュリティポリシーの点検・評価体制

本学の情報資産の円滑な運用に資するため、また、情報セキュリティポリシーが不正アクセス行為の禁止等に関する法律、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、著作権及び学内規程等の関連規則に違背することがないよう情報セキュリティポリシーに関する点検・評価及び改善等の体制を、次のとおり設けることとする。

5.1　リスク分析

対策部会の主導の下に、本学の情報資産に対するリスク分析を行う。

5.2　情報セキュリティポリシーの点検・評価

情報セキュリティポリシーの点検・評価の実施に関し、方針及び対策基準については対策部会、手順書については管理部会がこれを行うものとする。

5.3　点検・評価結果の反映

方針及び対策基準に関する点検・評価の結果、実施又は改善等の必要が生じた場合は、手順書の定めるところにより措置するものとする。

6　教育・啓発

本学は、情報資産を扱うすべての者に対し、意識向上と技術レベルの向上の両面から、

情報セキュリティに関する教育の一層の充実を図るものとする。

また、学生等は、部局等で行われる情報関連科目を積極的に受けるものとする。

7　講習受講の義務

職員等は、学内にて行う情報セキュリティ関連講習を必ず受講するものとする。

附　則

本方針は、平成１７年４月１日より施行する。

附　則

本方針は、平成２８年４月１日より施行する。

附　則

本方針は、平成２９年４月１日より施行する。

附　則

本方針は、令和３年４月１日より施行する。