○金沢大学情報セキュリティに関する規程

平成17年4月1日

規程第374号

(目的)

第1条　この規程は，金沢大学(以下「本学」という。)における情報セキュリティの維持及び向上に関する事項を定めることにより,本学の有する情報資産の保護及び効率的な活用を図ることを目的とする。

(定義)

第2条　この規程において，次の各号に掲げる用語の意義は，当該各号に定めるところによる。

(1)　ネットワークシステム

情報の流れを制御するルータ等の機器及び有線又は無線ネットワークをいう。

(2)　情報資産

ネットワークシステム及びネットワークシステムに接続された情報機器並びにそれらで取り扱われる情報をいう。

(3)　情報セキュリティ

情報資産の機密性，完全性及び可用性を維持することをいう。

(4)　情報セキュリティポリシー

本学における情報セキュリティに係る基本方針を定めた情報セキュリティ方針(以下「方針」という。)，方針に基づき遵守すべき基準を定めた情報セキュリティ対策基準(以下「対策基準」という。)，及び対策基準に基づき具体的な対策手順を定めた情報セキュリティ対策実施手順書で構成された文書群をいう。

(5)　リスク分析

ネットワークシステムの脆弱性及び情報セキュリティを侵害された場合の影響の評価をいう。

(6)　部局等

ネットワークシステム管理上，次のとおり区分された組織等をいう。

人間社会研究域（附属学校を含む），理工研究域，医薬保健研究域，国際基幹教育院，附属病院，がん進展制御研究所，ナノ生命科学研究所，附属図書館，事務局，学術メディア創成センター及びその他の学内共同教育研究施設等

(7)　利用者

本学が管理する情報資産を扱うすべての者をいう。

(適用範囲)

第3条　情報セキュリティポリシーは，利用者及び次に掲げる情報資産等に適用する。

(1)　本学が管理するネットワークシステム

(2)　前号のネットワークシステムに接続された情報機器

(3)　利用者が，本学の教育，研究その他の業務のために作成し，又は取得した情報で第1号のネットワークシステム又は前号の情報機器に記憶させたもの

(4)　利用者が，本学の教育，研究その他の業務のため作成し，又は取得した情報で前号に該当しないもの

(5)　前各号に係る設備及び物品を収容する施設等

(最高情報セキュリティ責任者)

第4条　本学に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。）を置き，情報担当理事をもって充てる。

2　最高情報セキュリティ責任者は，本学の情報セキュリティに関する総括的な権限及び責任を有する。

3　最高情報セキュリティ責任者を補佐するため，副最高情報セキュリティ責任者（副CISO）を置き，学術メディア創成センター長をもって充てる。

(部局ネットワークシステム管理者)

第5条　部局等に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。)を置き，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。

2　部局管理者は，当該部局等の情報セキュリティに関する権限及び責任を有する。

(情報セキュリティ対策部会)

第6条　本学の情報セキュリティの維持及び向上を図るため，情報セキュリティ対策部会を置く。

2　情報セキュリティ対策部会の組織，運営等に関し必要な事項は，方針で定める。

(ネットワークシステム管理部会)

第7条　本学のネットワークシステムの管理・運用を行うため，ネットワークシステム管理部会を置く。

2　ネットワークシステム管理部会の組織，運営等に関し必要な事項は，方針で定める。

(情報資産の保護)

第8条　ネットワークシステム管理部会長(前条第1項に規定するネットワークシステム管理

部会の長をいい，以下「管理部会長」という。)及び部局管理者は，必要に応じ，利用者に対してリスク分析を求めることができる。

2　管理部会長及び部局管理者は，方針の定めるところにより，リスク分析の結果に基づいた適切な管理を実施しなければならない。

(情報セキュリティ侵害への対処)

第9条　本学の情報セキュリティに対する侵害が発生したとき又は本学から学外の情報セキュリティに対する侵害が発生したときは，最高情報セキュリティ責任者，管理部会長，部局管理者，利用者その他のネットワークシステム関係者は，対策基準の定めるところにより，適切に対処しなければならない。

(ネットワークの監視)

第10条　利用者は，ネットワークを通じて行われる通信を傍受してはならない。

2　最高情報セキュリティ責任者及び部局管理者は，セキュリティ確保のために，あらかじめ指名した者に，ネットワークを通じて行われる通信の監視(以下「監視」という。)を行わせることができる。

3　前項の指名を受けた者は，監視によって知り得た情報の内容を他の者に伝達してはならない。ただし，本学又は学外に対する重大な情報セキュリティ侵害を防止するために必要と認められる場合は，この限りではない。

4　第2項の監視の範囲及び手順，前項ただし書に該当した場合の伝達に係る手続及び要件，監視によって採取した記録の取扱いその他のネットワークの監視に必要な事項は，対策基準で定める。

(利用の記録)

第11条　情報機器の利用記録の採取及び取扱いについては，対策基準で定める。

(監査)

第12条　学術メディア創成センター長（以下「センター長」という。）は，情報セキュリティポリシーの実施状況に係る監査を行い，その結果を情報セキュリティ対策部会長に報告するものとする。

(点検)

第13条　部局管理者は，当該部局等における情報セキュリティポリシーの実施状況に関し，対策基準で定める点検を行い，センター長に報告するものとする。

(その他)

第14条　この規程に定めるもののほか，本学の情報セキュリティの維持及び向上に関し必

要な事項は，方針及び対策基準で定める。ただし，附属病院の診療業務に関する事項は別に定める。

附　則

この規程は，平成17年4月1日から施行する。

附　則

この規程は，平成20年4月1日から施行する。

附　則

この規程は，平成23年4月1日から施行する。

附　則

この規程は，平成26年4月1日から施行する。

附　則

この規程は，平成28年4月1日から施行する。

附　則

この規程は，平成30年8月1日から施行する。

附　則

この規程は，令和3年4月1日から施行する。