○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）

改正

（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。

⑴　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。

⑵　情報資産　ネットワークシステム及び本学が保有，管理又は運用している情報機器並びにそれらで取り扱われる情報をいう。ただし，別に定める場合を除き，情報は第11号に定める電磁的記録に限る。

⑶　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。

⑷　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。

⑸　情報セキュリティ事案　情報セキュリティ侵害，方針違反，あるいは管理策の不具合の可能性，又は情報セキュリティに関係し得る未知の状態を示すネットワークシステム，情報機器，又は情報サービスの状態に関連する事象をいう。

⑹　情報セキュリティインシデント　望まない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって，本学の事業運営又は利用者に悪影響を及ぼすもの（以下「インシデント」という。）をいう。

⑺　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。

⑻　部局等　金沢大学学則第22条第1項に定める部局（グローバル人材育成推進機構を除く。）のほか，事務局，学内共同利用施設，学則第16条に基づき置かれる組織及び人間社会学域学校教育学類附属学校（園）をいう。

(9)　部局長　前号に定める部局等の長（事務局にあっては事務局長を，人間社会学域学校教育学類附属学校にあっては各学校長及び園長をいう。以下同じ。）をいう。
(10)　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。
(11)　電磁的記録 電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。

(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及び副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（Chief Information Security Officer。以下「CISO」という。）を置き，情報担当理事をもって充てる。
2　CISO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　CISOを補佐するため，副最高情報セキュリティ責任者（以下「副CISO」という。）を置き，学術メディア創成センター長をもって充てる。
4　CISO及び副CISOは，本学の情報セキュリティ上のリスクが高くインシデントの発生を未然に防止する必要性が高いと認められる場合又はインシデント発生後の対応策として必要と認められる場合は，全学又は特定の部局等のネットワークシステムの全部又はその一部を停止することを命ずることができるものとする。

(部局情報システム利用責任者)

第5条　部局等に，情報システム利用責任者（以下「部局責任者」という。）を置き，当該部局の長をもって充てる。
2　部局責任者は，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。

(情報セキュリティの維持及び向上のための組織)

第6条　本学の情報セキュリティに係る重要事項（インシデント対応を除く。）の決定，連絡・調整等を行う必要があるときは，金沢大学情報戦略本部で審議する。

(情報セキュリティインシデント対応チーム)

第7条　本学におけるインシデントに対応する組織として，CISOのもとに金沢大学情報セキュリティインシデント対応チーム（Computer Security Incident Response Team。以下「CSIRT」という。）を置く。
2　CSIRTの組織，運営等に関し必要な事項は，別に定める。

（情報資産の保護）

第8条　CISO，副CISO及び部局責任者は，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　CISO，副CISO及び部局責任者は，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。

（情報セキュリティ事案への対処）

第9条　本学の情報セキュリティ事案が発生したときは，CISO，副CISO，部局責任者，情報システム利用者及びその他関係者は，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　CISO，副CISO及び部局責任者は，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　副CISO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CISOに報告するものとする。

（点検）

第13条　部局責任者は，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，CISO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，情報戦略本部が別に定める。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

この規定は，平成 28 年 4 月 1 日から施行する。

附　則

この規定は，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。

附　則

この規程は，令和 4 年 7 月 15 日から施行する。