北陸先端科学技術大学院大学
情報セキュリティポリシー

改正 令和 8 年 7 月 22 日

1　情報セキュリティ基本方針

1.1　趣旨

北陸先端科学技術大学院大学（以下「本学」という.）は，開学当初から，FRONT 計画に基づいて構築される情報ネットワーク環境を FRONTIER（FRONT Information EnviRonment）と称し，本学の教職員及び学生に先端科学技術分野に関わる教育研究を行うための情報環境を提供しており，学内全ての情報ネットワークの管理運営を情報基盤センター（旧「情報科学センター/情報社会基盤研究センター」）が集中的に行うという他大学にはない特色ある体制をとっている.

こうした状況のもとで，本学の根幹を支える情報資産の価値は非常に増加しており，情報環境を適切に管理・運用し，学内外の不正なアクセスから情報資産を守るための情報セキュリティ対策を構築することが，リスク管理上極めて重要な地位を占めるに至った.

そこで,「情報セキュリティポリシーに関するガイドライン（平成 12 年 7 月 18 日情報セキュリティ対策推進会議決定)」における「政府の情報セキュリティの基本的な考え方」を踏まえ，情報セキュリティ対策の包括的なマニュアルとして，北陸先端科学技術大学院大学情報セキュリティポリシー（以下「ポリシー」という.）が平成 15 年 7 月 15 日に策定された．また,「政府機関の情報セキュリティ対策のための統一規範（平成 23 年 4 月 21 日情報セキュリティ対策推進会議決定)」及び「北陸先端科学技術大学院大学における情報セキュリティ基本計画（平成 29 年 3 月 30 日学長裁定)」を踏まえ，変化する社会の状況に対応するため，ポリシーは平成 29 年 3 月 30 日に改訂され更新した.

ポリシーは，本学の情報セキュリティ対策の強化・拡充を図る際の指針を示す．本学の情報環境を利用する全ての者は，高いレベルの情報セキュリティを実現するため，ポリシーを尊重し遵守しなければならない．ポリシーは，本学情報資産を対象とする．本学は，ポリシーを基に，　情報セキュリティ委員会 を中心として情報セキュリティの全学的な確保に取り組む.

1.2　定義

ポリシーで使用する用語を以下のとおり定義する.

1. 情報機器

- 情報処理（通信を含む.）の用に供する機器で，次に掲げるもの.
  (a) 端末機器：パーソナルコンピュータ，スマートフォン，タブレット端末等
  (b) サーバ装置：メールサーバ，Web サーバ，ファイルサーバ，DNS サーバ等
  (c) 通信装置：ルータ，スイッチ，ファイアウォール等
  (d) 入出力装置：複合機，プリンタ，画像スキャナ等
  (e) 電磁的記録媒体：ハードディスク，USB メモリ，CD/DVD 等
  (f) 特定用途機器：テレビ会議システム等の特定用途に使用されるシステムを構成する機器等

2. 情報環境

- 教育，研究，事務処理等に利用する情報機器，ソフトウェア及び情報処理サービスのうち，次に掲げるものの総称.
  (a) 本学が所有又は管理するもの
  (b) 本学との契約又は他の協定に従って提供されるもの
  (c) 本学キャンパスネットワークに接続する情報機器

3. 情報

- 次に掲げるもの．ただし，個人が所有する情報機器に電磁的に記録されたデータのうち，職務上取り扱うもの以外は除く.
  (a) 情報環境に電磁的に記録されたデータ
  (b) プリンタ等により情報環境から出力された文書等
  (c) 画像スキャナ等により情報環境に入力された文書等
  (d) 情報環境の開発，運用及び保守のための文書等
- 情報のうち，法人文書に分類されるものを法人文書情報という.

4. 情報資産

- 情報環境及び情報の総称.

5. 情報セキュリティ

- 情報資産の機密性，保全性及び可用性を維持すること.

6. 情報環境管理責任者（以下「管理責任者」という.）

- 情報環境の担当情報機器及び担当情報処理サービスの情報セキュリティに対する責任を負う者.

7. 情報環境利用者（以下「利用者」という.）

- 情報環境を利用する全ての者．本学の構成員に加えて，共同研究員，学会等による来学者，学外からネットワーク経由で情報環境を利用する者等を含む.

8. 情報セキュリティガイドライン（以下「ガイドライン」という.）

- 情報環境において遵守すべき行為及び判断基準を具体的に定めたもの．管理責任者を対象とした北陸先端科学技術大学院大学情報環境管理ガイドライン（以下「管理ガイドライン」という.），利用者を対象とした北陸先端科学技術大学院大学情報環境利用ガイドライン（以下「利用ガイドライン」という.）及び本学で取り扱う情報に対する格付け及び取扱制限に係る北陸先端科学技術大学院大学情報格付けガイドライン（以下「格付けガイドライン」という.）から成る.

9. 情報セキュリティインシデント（以下「インシデント」という.）

- 情報セキュリティに関し，意図的又は偶発的に生じる，本学規程（ポリシー及びガイドラインを含む.）又は法令に反する事件若しくは事故．本学情報資産における，次に掲げるものを含む.
  (a) 物理的破損，不正利用，改ざん，漏えい，サービス妨害等
  (b) その疑いのある，又はそれに至る危険性をもつ事象

2 情報セキュリティ対策基準

2.1 組織体制

1. 最高情報セキュリティ責任者（Chief Information Security Officer，以下「CISO」という．）

   (a) CISO は，学長が指名する者をもって充てる．

   (b) CISO は，学内の全ての情報セキュリティに関する総括的な権限と責任を有する．

   (c) 情報セキュリティに関する学外からの苦情及び学外から受けた被害への対応のうち，損害賠償請求等法的対応部署との連携が必要となった場合及び被害回復請求といった重大な事態が生じた場合は，CISO がこれらの対応に当たる．

   (d) CISO は，情報セキュリティインシデント対応班の活動内容について助言又は指導を行う．

2. 最高情報セキュリティ責任者補佐（以下「CISO 補佐」という．）

   (a) CISO 補佐は，情報基盤センター長をもって充てる．

   (b) CISO 補佐は，情報セキュリティインシデント対応班の活動内容について助言又は指導を行う．

3. 情報セキュリティ委員会

   (a) 情報セキュリティ委員会は，教員，事務職員及び技術職員から全学的な見地により構成する．

   (b) 情報セキュリティ委員会に委員長を置き，CISO をもって充てる．

   (c) 情報セキュリティ委員会は，情報セキュリティに関し必要な事項を審議する．

4. 全学情報環境管理責任者（以下「全学管理責任者」という．）

   (a) 全学管理責任者は，CISO の指名する 情報基盤センターの教員をもって充てる．

   (b) 全学管理責任者は，情報環境における情報セキュリティの保持及び強化のための調査検討を行うとともに，緊急時の総括的な対応を行う．

5. 情報セキュリティインシデント対応班（Computer Security Incident Response Team，以下「CSIRT」という．）

   (a) CSIRT は，情報セキュリティに関する専門的な知識又は適性を有すると認められる教職員から構成する．

   (b) CSIRT には主査を置き，全学管理責任者をもって充てる．

   (c) CSIRT は，緊急時対応に必要な権限について，予め CISO から委譲を受けておくことができる．

   (d) CSIRT は，インシデントの通報を受け付け，分析及び情報収集により事象を正確に把握するとともに，必要に応じて被害拡大の防止，復旧，再発の防止に係る措置を実施し，また，管理責任者に対する技術的支援及び助言を行う．

   (e) CSIRT は，学内のインシデントの発生状況を定期的に取りまとめる．

6. 管理責任者

   (a) 情報環境の各情報機器及び各情報処理サービスに管理責任者を置く．

   (b) 管理責任者は，情報環境における情報セキュリティの保持及び強化のため，調査検討及び対策の実施に責任を負うとともに，担当情報機器及び担当情報処理サービスに関して管理運営を行う．

   (c) 管理責任者は，情報セキュリティに関する情勢及び傾向の把握に努め，ポリシー及びガイドラインの評価及び更新に必要な情報を CSIRT に提供する．

7. 格付け管理者

   (a) 本学で取り扱われる情報には格付け管理者を置く．

   (b) 法人文書情報の格付け管理者は，当該法人文書の文書管理者をもって充てる．

   (c) その他の情報の格付け管理者は，当該情報を作成又は取得した者をもって充てる．

   (d) 格付け管理者は，情報セキュリティ対策を適正に実施するため，担当情報の格付け及び取扱制限の管理を行う．

8. 総括文書管理者

   (a) 総括文書管理者は，法人文書情報に付される格付け及び取扱制限の管理を取りまとめる．

2.2 緊急時の対処

1. 利用者は，情報環境上のインシデントを発見した場合には，CSIRT 及び管理責任者に直ちに通報するとともに，その指示に従い，被害拡大の防止，復旧，証拠保全等の必要な措置を迅速にとらなければならない．

2. 管理責任者は，担当する情報機器又は情報処理サービス上で発生したインシデントを CSIRT に直ちに報告するとともに，その指示に従い，被害状況の把握，緊急避難措置，被害拡大の防止，復旧，証拠保全等に必要な措置を講じなければならない．また，その措置によって影響を及ぼすと判断される利用者に対しては，その事実を速やかに通知しなければならない．

3. CSIRT は，通報されたインシデントに対して，直ちにリスク分析を行い，必要に応じて被害拡大の防止，復旧，再発の防止に係る措置を実施し，また，関係する管理責任者に対する技術的支援や助言を行う．重大な事案については，直ちに CISO および CISO 補佐に報告する．

4. CISO 及び CSIRT は，必要な場合には，不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）第 9 条に基づき，石川県公安委員会に対し支援の要請を行う．

2.3 遵守義務

1. 利用者は，利用ガイドラインに定める各項目を遵守しなければならない．

2. 利用者は，情報の作成又は取得し，その管理を開始するときに，格付けガイドラインに定められた手順に従って当該情報の格付け及び取扱制限を指定し，それを認識できるようにしなければならない．

3. 利用者は，利用ガイドラインに基づき，次の情報セキュリティ対策に努める．

   (a) 意図的・偶発的にかかわらず情報環境を不正に利用することがないようにすること．

   (b) 情報環境を不正に利用されることがないようにすること．

   (c) 情報の内容に応じたアクセス対象の制限を行うこと．

   (d) 不要情報の処分等を行うこと．

   (e) 情報の取扱に当たっては，格付けガイドラインに基づき指定された取扱制限に従うこと．

4. 情報環境に接続するすべての情報機器に関して，情報セキュリティ上の問題等で全学管理責任者又はその指名する者，CSIRT 及び管理責任者から指示があるときには，利用者はその指示に従わなければならない．

2.4 管理責任

1. 管理責任者は，管理ガイドラインに定める各項目を遵守しなければならない．
2. 管理責任者は，担当情報機器又は担当情報処理サービスの情報セキュリティに対する責任を負う．
3. 管理責任者は，管理ガイドラインに定める各項目に基づき，次の運用管理を行う．
   (a) 担当情報機器について，記録されている情報の格付け及び取扱制限の把握に努める．
   (b) 担当情報機器について，記録されている情報の取扱制限に留意して管理方針を決め，その情報セキュリティが維持されるよう努める．
   (c) 管理体制を整備し，緊急時にも速やかに対応できるよう努める．
4. 管理責任者は，情報セキュリティ上の問題等で全学管理責任者又はその指名する者及び CSIRT から指示があるときには，その指示に従わなければならない．
5. 格付け管理者は，格付けガイドラインに定める各項目を遵守しなければならない．

2.5 教育・研修

1. 情報セキュリティ委員会 は，ポリシー及びガイドラインを Web 上で公開するとともに，要約を対象者に配布するものとする．
2. 情報セキュリティ委員会 は，新たに本学の構成員になった職員，学生等を対象に情報セキュリティ研修の機会を設けるものとする．
3. 情報セキュリティ委員会 は，来学者が学内の情報環境を一時的に使用する場合に，ポリシー及び利用ガイドラインを遵守させるよう適切な措置を講じるものとする．

2.6 評価及び見直し

2.6.1 情報セキュリティ評価

1. 情報セキュリティ委員会は情報セキュリティ対策の実施状況を評価する．
2. 情報セキュリティ委員会は全学管理責任者及び管理責任者に情報セキュリティ対策の見直しを提言する．
3. 全学情報管理責任者は，情報セキュリティ対策の実施状況評価に係る技術的支援を行う．
4. CSIRT は、インシデント発生状況を情報セキュリティ委員会に報告する．

2.6.2 ポリシー及びガイドラインの更新

1. 情報セキュリティに関する特に重大な情勢の変化を認めた場合には，ポリシー及びガイドラインの更新案を作成し， 情報セキュリティ 委員会に提案する．
2. ポリシー及びガイドラインの更新案は 情報セキュリティ 委員会において審議の上，CISO が決定する．ただし，ポリシーを更新する場合には， 情報セキュリティ委員会が 審議した後に教育研究評議会 に報告 の上，学長が決定する．
3. 更新したポリシー及びガイドラインの遵守を啓発するため，その要約を配布して全ての構成員に提示する．

3 例外事項

1. 教育，研究，事務処理等の都合によりポリシー及びガイドラインを遵守することができない状況が発生するおそれのある場合には， 管理責任者は予め情報セキュリティ委員会に申請し，ポリシー及びガイドラインの適用除外について承認を受けなければならない．
2. 情報セキュリティ委員会 は，適用除外の申請があった場合には速やかに適用除外についての審査を行う．
3. 独立行政法人等の保有する情報の公開に関する法律（平成 13 年法律第 140 号）又は 個人情報の保護に関する法律 （平成 15 年法律第 57 号） に基づく開示請求に関しては，学長が情報公開・個人情報保護委員会に諮問の上，必要な措置を判断し，その判断に基づいた情報の取り扱いを行うものとする．
4. ポリシー及びガイドラインに記載のない事項により問題が発生した場合，特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成 13 年法律第 137 号）に基づく開示請求があった場合，又はその他の法令に抵触する場合については， 情報セキュリティ委員会 がその取扱いについて判断する．その判断結果については検証を行い，ポリシー及びガイドラインの更新案に反映させることとする．

更新履歴

1. 平成 15 年 7 月 15 日: 初版（第 1 版）
2. 平成 25 年 3 月 31 日: 更新（第 2 版）
3. 平成 29 年 3 月 30 日: 更新（第 3 版）
4. 令和 2 年 4 月 1 日: 更新（第 4 版）
5. 令和 3 年 10 月 1 日: 更新（第 5 版）
6. 令和 4 年 10 月 31 日: 更新（第 6 版）
7. 令和 8 年 7 月 22 日: 更新（第 7 版）