［学　長　裁　定
２０２５年４月２２日］

北陸先端科学技術大学院大学におけるサイバーセキュリティ基本計画

基本方針

サイバーセキュリティ等を取り巻く情勢の変化やサイバー攻撃のさらなる複雑化・巧妙化により，本学に求められる対策・対応も高度化・増大している．多様な構成員によって構成され，先端的研究に関する情報資産や，ネットワークに接続した教育・研究・業務をはじめとする多様なシステムの利用実態を有する本学の特性を踏まえると，実空間における情報の機密性・完全性・可用性の確保のために行われる情報セキュリティ対策に加えて，端末側やクラウド利用時のサイバーセキュリティ対策も重要となっている．

このような状況において，本学が教育・研究・社会貢献といった役割を今後も果たしていくためには，以下に示す，(1) 任務保証の考え方に基づいた取り組み，(2) リスクと利便性のバランスがとれた対策，(3) 参加・連携・協働の推進の 3 つの方針に基づいて，セキュリティ水準の維持・向上を絶えず図っていくことが必要である．　2025 年 4 月から 3 年間 を計画期間とし，サイバーセキュリティ対策の目標及び実施方針等を記載した「サイバーセキュリティ基本計画」を策定し，これを推進する．

(1) 任務保証の考え方に基づいた取り組み

- 世界最高水準の教育・研究を行う大学院大学としての役割を着実に遂行するために，必要なリソースを確保し，安全かつ持続的な業務・サービスの提供に関する責任を全うできる情報環境及びその管理運用体制の構築を推進する．
- サイバーセキュリティ対策は法人トップである学長が強いリーダシップを発揮し，CISO が中心となりサイバーセキュリティ対策の組織への浸透とセキュリティインシデントへの対応を効果的に行うために組織全体として計画的に取り組む．
- 個人情報の適切な管理に加えて，本学が保有する先端的な科学技術情報についても，競争力の維持及び強化や安全保障貿易管理，外部からの信頼確保等の点から適切な管理を行う．

(2) リスクと利便性のバランスがとれた対策

- サイバーセキュリティ対策を講じるにあたり，役員，教職員及び学生（以下「構成員」という．）の活動が円滑に行えるようセキュリティを維持しつつ，組織として得られる効果が最大化されるように実効性を重視した，高い利便性や性能を有する情報環境の構築を推進する．
- 限りある資源を有効に活用し，効率的にサイバーセキュリティ対策等を推進するため，法人として保護すべき重要な業務・サービスとそうでないものに分け，前者については優先順位を付けつつ重点的に対策を行い，後者については各種ガイドライン等に基づき必要となる対策を濃淡をつけて実施する．
- 本基本計画については，定期的に進捗状況を評価し，その結果やサイバーセキュリティ等を取り巻く状況の変化を踏まえ，必要に応じて見直しを行う．

(3) 参加・連携・協働の推進

- 全ての構成員がサイバーセキュリティ対策の重要性について認識し，主体的にサイバーセキュリティ等の確保に取り組むよう教育研修を実施する．なお，教育研修内容については，過去のインシデント事例の知見が引き継がれるよう検討する．
- 大学組織において共通性があるサイバーセキュリティ上の課題に対しては，他機関との連携・協力を積極的に検討する．

なお，以下の「個別方針」で示す取組の実施予定時期については，別紙「北陸先端科学技術大学院大学サイバーセキュリティ基本計画工程表」の通りである．

個別方針

1　インシデント対応体制

1.1　インシデント対応体制 (CSIRT) の運用と見直し

インシデントに対処する組織としての CSIRT を継続的に維持，運用する．運用にあたり，インシデント発生時の対処をより迅速かつ正確に行えるよう，学内の関係各部門だけでなく，外部機関との連携・協働を含めた体制やサービスの優先度付け等の見直しを定期的に実施する． 特に, 重大なインシデント発生時に原因や被害状況の把握のための調査を迅速に行うえるよう，あらかじめ外部の専門的な業者と NDA（秘密保持契約）を締結するなど体制の強化を検討する．また，インシデント対応における適切な対応を実施するために必要な手順書及び緊急連絡網を CSIRT 内及び関係各部門において共有する．

1.2　インシデント対応に係る人材の育成と拡充

CISO，CISO 補佐，インシデント対応担当者，関連部局の職員等に対し外部の研修・演習やカンファレンス等への参加を推奨し，知識・技術の取得や人脈の構築を促進するとともに，資格試験の受験やセミナー受講の費用を援助するなど積極的な人材育成に取り組む． また，関連資格保有者等の任用や一時受け入れ，学内におけるキャリアパスの確立など， インシデント対応に係る中長期的に本学の情報セキュリティ業務を担える若手人材の拡充について検討を進める．

2　制度設計

2.1　PDCA サイクル　の維持

本基本計画は定期的な見直しを行い，必要に応じて更新する．更新にあたり，自己点検・監査結果等を踏まえ，最終的に大学全体でサイバーセキュリティにおける PDCA サイクルが持続的に行える体制を　維持する．

2.2　　データ管理指針の整理と運用

情報サービスの境界が利用者から見てあいまいになりつつある現状に対応するため，これまでに整備してきた情報の格付けや研究データ管理，外部クラウド指針などを一体的に運用することを目指す．本指針は，研究データだけでなく大学で扱われる様々なデータの適切な取扱いや管理手順を明確にし，組織全体の整備と保護を実現するための包括的なガイドラインを提供する．

- データ管理指針の整理：リスク評価と情報格付け，取扱制限の確認，国内外の法令適用リスク，新型コロナ禍による環境変化や生成 AI の普及を考慮し，学内外のクラウドを利用する際の指針を合わせて整理する．
- データ管理指針の運用：保護すべき研究情報や機器管理についての調査や，機密性の高い情報のアクセス制限や暗号化，外部記録媒体の利用可否に関する情報取扱マニュアルの作成などを進める．

2.3　　業務 継続計画の策定

大学全体の業務継続計画を踏まえ，情報セキュリティインシデントの発生および大規模地震や風水害等の各種災害を踏まえた IT システムの業務継続計画 (IT-BCP) を策定し，周知する．

3　技術的対策

3.1　機器に対する対策

3.1.1　機器対策の継続と発展

情報管理の信頼性を高め，リスクを軽減するために従来から対策してきた，重要情報を取り扱う機器や学外からのアクセス可能な機器，外部公開サーバ機器に対する対策を継続するとともに，効率的かつ包括的に発展させる．

- 重要情報を取り扱う機器への対策：リスク評価に基づき，標的型攻撃を踏まえた多層防御等の対策を検討・実施.
- 学外からの直接アクセス可能な機器への対策：当該機器の IP アドレスと利用者の管理を効率的に行い，ネットワーク構成の見直しでトラブル時に迅速に対応.
- 外部公開サーバ機器への対策：外部公開している情報機器・サービスの管理と有事対応手順の整備.

3.1.2　マイクロセグメンテーションの推進とゼロトラストアーキテクチャの検討

情報セキュリティインシデント発生時の影響範囲を限定的にするため，情報システムで取り扱う情報の格付け及び取扱制限に応じて、そのリスクと利便性のバランスがとれたマイクロセグメンテーション化を進める．また，ゼロトラストアーキテクチャの考え方に基づくネットワーク構成の検討や試行を通じて段階的に導入を推進する．また，全学向け情報環境として情報社会基盤研究センターが管理し貸与する端末において，盗難，紛失，不正プログラムの感染等による情報漏洩/改竄を防止するために導入しているエンドポイント対策 (MDM，EDR，AV 等) を，研究科や研究室等が管理する大学資産端末や接続が認可された個人資産端末に拡張することを検討する．

3.2　包括的対策

3.2.1　不正ログイン対策の強化

学外からログイン可能なシステムについては， パスワードレス認証，二要素認証の導入及びパスワードの強化を継続して推進する と共に，学内システムについても SAML 認証によるシングルサインオンを推進する． また，アカウント情報は定期的に棚卸しを行うとともに，より効率的かつ正確に修了生や退職者等のロールに応じた削除・権限制御を行うため，ワークフローの見直し及びシステムの改善を図る．

3.2.2　ログ管理の徹底

不審な通信の疑いのある端末の特定作業等のインシデント対応の際に必要となるログの保存を継続する．ログ収集に不備がないようシステム等で監視しつつ，ログ収集の範囲についても定期的に見直しを行う．また セキュリティ情報イベント管理システム（SIEM） による分析を平時から行うと共に，製品トレーニングなどを行い高度な運用, 分析ができる要員を育成 する．

3.2.3　セキュリティアップデート・パッチ適用の徹底

全学向け情報環境として事務部局及び情報社会基盤研究センターの管理下にある機器については，ソフトウェアのサポート期間等のライフサイクルを考慮に入れた機器導入・運用方針を徹底する　. また，外部公開サーバや 認証システム，機密性の高い情報を保有するなどリスクが高いシステム 等に対し，脆弱性診断を定期的に実施すると共にサーバ管理者に　オペレーティングシステムやアプリケーション・ソフトウェア等についてアップデートの適用漏れを防ぐための技術的な管理ツール や脆弱性診断ツールなどのサービスを提供　し，大学全体でセキュリティアップデート・パッチ適用ができる環境を整備す る．

3.2.4　物理的インシデント防止策の推進

重要情報を含む機器を取り扱う区域において，区域の施錠，入退室管理等を徹底する．また，重要な書類や外部記録媒体，ノートパソコンその他適切な管理が必要な物品の管理徹底について，部局間での連携のもとで引き続き推進する．

3.2.5　IT 管理業務における DX の推進

IT 管理業務や情報セキュリティ関連業務について DX を推進し，効率的かつ正確に管理できる環境の整備を進める．人的な作業を減らすことで，人為的なミスによるセキュリティインシデントのリスクを軽減し，人的のリソース不足の問題を補う．

4　教育・啓発

構成員全体のセキュリティ意識を高め，組織全体のインシデントの予防と対応力を強化するために，以下に示す取り組みを行う．

- インシデント対応のための訓練：インシデント予防および発生後の対応力を向上させるため，過去のインシデント事例に基づいたインシデント対応訓練を CSIRT を含めて横断的に実施する．
- 構成員への教育啓発活動：構成員に対し，適切なタイミングでセキュリティ教育の実施，脆弱性情報やセキュリティ情報のアナウンス・注意喚起を行う．特に，入学・新規採用時には以下の手続きを徹底する．
- 重要情報を取り扱う担当者への教育啓発活動：重要情報やシステムを取り扱う担当者に対し，役職と役割，責任に応じた情報共有およびセキュリティ教育を実施する．

5　自己点検と監査

5.1　自己点検の実施

情報や情報システムの機密性，完全性，可用性及びインシデント発生状況等を考慮し，適切な目的や点検対象 (外部クラウドやホスティングを含む．)，実施時期，実施頻度を設定した年度ごとの自己点検計画を作成し，これに基づいた自己点検を実施する．

5.2　監査の実施

サイバーセキュリティ監査及び情報セキュリティポリシーや実施手順書等の遵守状況を監査対象とした情報マネジメント監査を定期的に実施する．実施にあたり，過年度に発生したインシデントを踏まえた監査内容とし，監査により得られた指摘事項に対する知見・対策は本基本計画に反映するなど，実効力のある監査体制を整備する．

別　紙

2025-2027

北陸先端科学技術大学院大学 サイバーセキュリティ基本計画工程表

					2025年度(令和7年度)				2026年度(令和8年度)				2027年度(令和9年度)			
					1期	2期	3 期	4期	1期	2期	3期	4期	1期	2期	3期	4期
1	1		インシデント対応体制(CSIRT)の運用と見直し	定期的な評価と見直し			体制の評価/見直し								体制の評価/見直し	
				緊急連絡網の更新		緊急連絡網の更新				緊急連絡網の更新				緊急連絡網の更新		
				手順書の整備/見直し		手順書見直し				手順書見直し				手順書見直し		
	2		インシデント対応に係る人材の育成と拡充	研修等参加	研修/セミナー等参加											
				人材拡充の検討			人材拡充の検討								人材拡充の検討	
2	1		PDCAサイクルの維持	基本計画見直し					基本計画見直し				基本計画見直し		次期計画検討	
				ポリシー/ガイドラインの更新			更新要否検討				更新要否検討				更新要否検討	
	2		データ管理指針の整理と運用	データ管理指針の整理と運用	データ管理指針の整理			マニュアルの作成			策定と周知		データ管理指針の運用			
				研究情報や機器管理についての調査	研究情報や機器管理の調査									更新の調査		
			ITシステムの業務継続計画(IT-BCP)の策定	IT-BCPの策定	IT システムの業務継続計画(IT-BCP) の策定											
3	1	1	機器に対する対策	重要情報を取り扱う機器への対策	多層防御等の対策を検討						構築	運用				
				学外からの直接アクセス可能な機器への対策	効率的な管理方法の検討						構築	運用				
				外部公開サーバ機器への対策	効率的な管理方法の検討						構築	運用				
		2	マイクロセグメンテーションの推進とゼロトラストアーキテクチャの検討	マイクロセグメンテーションの推進	検討				推進							
				ゼロトラストアーキテクチャの検討	検討						導入	運用				
	2	1	不正ログイン対策の強化	二要素認証の検討/拡充			対象システム検討/拡充				対象システム検討/拡充				対象システム検討/拡充	
				アカウント棚卸		アカウント棚卸				アカウント棚卸				アカウント棚卸		
				アカウント管理ワークフローの見直し			見直し				見直し				見直し	
		2	ログ管理の徹底	ログ収集範囲の見直し			見直し				見直し				見直し	
				ログ採取方針の見直し	現SEIMの評価・見直し		新SIEM導入		新SIEMの運用							
		3	セキュリティアップデート・パッチ適用の徹底	パッチ更新管理監視サービスの普及	サービスの提供と普及										評価と見直し	
				脆弱性診断ツールのサービス提供		検討・評価		導入	サービスの提供と普及							
		4	物理的インシデント防止策の推進	重要情報取り扱い区域指定と対策	対象部局の拡大											
				物品管理の徹底	物品管理徹底											
		5	IT 管理業務におけるDX の推進	DX の推進	ITSMの検討			ITSMの導入	運用				運用と対象システム拡充			
4			インシデント対応のための訓練	インシデント対応訓練						計画		実施				
			構成員への教育啓発活動	新構成員への教育啓発活動		新構成員向け		新構成員向け		新構成員向け		新構成員向け		新構成員向け		新構成員向け
				在校生セキュリティ研修			在校生向け研修				在校生向け研修				在校生向け研修	
			重要情報を扱う担当者への教育啓発活動	教職員向けセキュリティ研修			教職員向け研修				教職員向け研修				教職員向け研修	
				システム管理者向け研修		実施内容の検討、コンテンツ選定				システム管理者向け研修				システム管理者向け研修		
5	1		自己点検の実施	自己点検の実施		自己点検対象の検討	自己点検			自己点検対象の検討	自己点検			自己点検対象の検討	自己点検	
	2		監査の実施	外部監査の実施			外部監査対象の検討	外部監査			外部監査対象の検討	外部監査			外部監査対象の検討	外部監査