［学　長　裁　定
令和元年　9月27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．令和元年 10 月から令和 4 年 3 月を計画期間とし，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．なお，詳細な体制整備及び予算の確保については，2020 年度から始まる新執行部と策定の上，本計画を更新する．
- 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．
- 対策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，関係各部門・外部機関との連携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．

1.2　対応手順書及び緊急連絡網の整備と共有

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．手順書は，システム本体に加えてシステム間の依存関係等の資料を含むだけでなく，適切な時点での関係各部署への報告・連絡を含んだ，より実情に即したものとなるよう更新を行う．また，インシデント発生時の緊急連絡網に変更の必要が生じた場合，速やかに更新する．

1.3　インシデント対応に係る人材の育成

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年 1 回以上の参加を推奨し，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．

1.4　統括部門の整備，人材拡充

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，インシデント対応を含むセキュリティ統括部門の整備と人材拡充について検討を行う．

2　制度設計

2.1　PDCA サイクル体制の構築

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構築する．

2.2　情報の格付け及び取扱手順の策定

情報や情報システムの格付けについて， 作成した格付けガイドラインを構成員に周知し，浸透を図る．加えて格付けに応じた情報の取り扱い，特にアクセス制限や暗号化等を要求される機密性の高い情報の取り扱いの手順や，外部電磁的記録媒体の利用可否などを構成員が正しく認識できるよう，標準的かつ簡易な情報取扱マニュアルを作成し，必要に応じて既存の業務マニュアルにも反映する．

2.3　他機関との連携体制の構築

他大学等と連携し，インシデントや対処技術，機器やツールの情報や知見などの技術情報，また注意喚起文や教育・訓練コンテンツなどのサイバーセキュリティ対策等に係る各種リソースについて定期的に情報交換，共有するほか，監査やインシデント対応等における相互協力体制を段階的に構築する．その取り組みの中でインシデント発生時の相互協力，訓練・演習の実施，セキュリティ監査，セキュリティ機器やサービスの調達, 相互のバックアップの保管やバックアップサイトの構築が可能か検討を進める．国立情報学研究所 NII-SOCS と引き続きインシデント情報や脅威情報の共有を行う．

2.4 外部委託要件の標準化

新たな情報機器購入，情報システム構築，保守業務委託等の際に求める標準的なセキュリティ要件及びサプライチェーン・リスク管理体制を定め，調達・委託にあたっての契約条件とする．また，受注業者には定期的な遵守状況の報告及び，実作業にあたっての作業者の告知を義務付ける．

2.5 外部クラウド利用指針の策定

学外のクラウドサービスを利用する際の利用指針を策定し，周知する．策定にあたり，一般的なクラウドサービスにおいて情報の適切な取扱いが行われていることを直接確認し難いこと，国内法以外の法令が適用されるリスクがあることなどの特性を踏まえ，個々の利用者がクラウドサービスの利用を検討する際のリスク評価に資するよう，必要な情報をわかりやすく提供することに努める．

2.6 運用継続計画の策定

地震や豪雨等の大規模自然災害発生を想定した緊急事態等発生時の対応計画に加え，サイバー攻撃やその他大規模システム障害の可能性を踏まえた運用継続計画を策定し，周知する．

3 技術的対策

3.1 機器に対する対策

3.1.1 学外から直接アクセス可能な機器への対策

学外から直接アクセスできる情報機器について，IP アドレスと利用者の紐づけを容易にするとともに，紐づけの困難な場合についてはネットワークアクセスを制限・遮断できるネットワーク構成を検討し，段階的に整備を進める．

3.1.2 エンドポイント対策

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搾取を防止するエンドポイント対策 (MDM，EDR，AV 等) を引き続き運用する．また，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ついてもエンドポイント対策の強化を図る．

3.1.3 重要情報を取り扱う機器への対策

重要情報を取り扱う機器やそれらの資源を管理する機器（主要な ActiveDirectory サーバ等を含む.）については，取り扱われる情報の重要度，発生しうる脅威や発生可能性に基づくリスク評価を行った上で，必要に応じ標的型攻撃を踏まえた多層防御等の適切な対策を検討・実施する．

3.1.4 先端的研究情報を取り扱う機器の対策

本学として保護すべき先端的な研究情報について調査し，これを取り扱う機器については，項目 3.1.3 の内容に準じるとともに，学内外からのアクセスの制限・遮断や USB 等外部記憶媒体の取り扱いを制限するなど 十分な対策を検討する．

3.1.5　外部公開サーバの取扱手順の整備と共有

本学名で外部に公開している情報機器・サービスについて定期的に調査しリスト化する．このうち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，必要に応じてシステム停止・復旧の手順書を随時更新し，関係者間で共有する．また，研究科や研究室等が管理するその他の機器についても，有事における対応手順及びネットワーク遮断手順を継続的に更新する，

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，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．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．またより詳細な分析・検知を可能とするために，セキュリティ情報イベント管理システム（SIEM）等の導入を検討する．

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とともに，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を検討し，段階的に整備を進める．また，研究科，研究室等にも整備した管理ツールを提供し，運用支援を行う．

3.2.4　インシデント予防・早期発見活動の継続

外部公開サーバ等に対し，脆弱性診断を定期的に実施する．また，ログの分析，脆弱性情報の確認・評価やオープンソースインテリジェンス（OSINT）の活用等，インシデントの予防または早期発見につながる活動を継続して行う．

3.2.5　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．

4　教育・啓発

4.1　インシデント対応のための訓練

インシデント予防及び発生後の対応力の向上のため，インシデント対応訓練を年 1 回以上実施する．なお，訓練対象に関係部門を含めるなど，横断的かつ現実に即した実践方法を検討する．

4.2 構成員への教育啓発活動

構成員に対し，各種脆弱性情報やセキュリティ情報等に関するアナウンス・注意喚起を適切なタイミングで実施する．特に入学・新規採用時には以下の手続きを徹底し，構成員の意識向上に努める．

- 情報セキュリティパンフレットの配布
- 情報セキュリティポリシーに関する講習の受講
- 情報セキュリティポリシーの理解と遵守について署名

4.3 重要情報を取り扱う担当者への教育啓発活動

重要情報，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及びセキュリティ教育を定期的に実施する．

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

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

				令和元年度				令和二年度				令和三年度			
				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	体制の継続運用	体制の継続運用(インシデント対応)									
			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		
	2	対応手順書および緊急連絡網の整備と共有	緊急連絡網の更新		緊急連絡網の更新				緊急連絡網の更新				
			手順書の見直し		手順書見直し				手順書見直し				
	3	インシデント対応に係る人材の育成	研修等参加	研修/セミナー等参加			研修/セミナー等参加				研修/セミナー等参加		
	4	統括部局の整備，人材拡充	検討および調整		新執行部との検討および調整				統括部局の整備、各人材の拡充				
2	1	PDCAサイクル体制の構築	PDCAサイクル実施状況			評価		改善案検討		評価		改善案検討	
			基本計画見直し					基本計画見直し					次期計画検討
	2	情報の格付け，取扱手順の策定	ガイドライン周知	格付けガイドライン周知，広報									
			取扱マニュアル作成					簡易取扱マニュアル作成					
	3	他機関との連携体制の構築	大学間での情報交換会の実施		実施		実施		実施			実施			実施
			相互協力体制の拡充		共同調達の検討、他大学と共同調達の可否の検討協議								
	4	外部委託要件の標準化	セキュリティ要件/サプライチェーンリスク回避要件の仕様書への反映		標準要件の作成/調達仕様への反映			一部部局による試行		仕様の見直し			
										全学調達仕様書への反映			
			定期報告の評価						定期報告評価				
	5	外部クラウド利用指針の策定と公開	簡易版の作成/周知		作成/公開		周知	評価					
			利用指針策定/周知						策定	周知			
	6	運用継続計画の策定	運用継続計画策定	緊急事態発生時の対応の見直し，運用継続計画の策定						運用継続計画の推進			
3	1	学外からアクセス可能な機器への対策	IPアドレス管理手法更新	ネットワーク接続申請システムへの移行		運用							
		エンドポイント対策 貸与機器	導入済対策の評価/見直し		評価，見直し				評価，見直し				評価，見直し
		エンドポイント対策 その他機器	エンドポイント対策の強化	強化策の検討			強化策の実施						
		重要情報を取り扱う機器への対策	防御方針検討	対象機器の洗い出し			リスク評価		防御方針検討/実装				
		先端的研究情報を取り扱う機器への対策	機器調査，対策検討	対象機器調査		機器の性質に応じた対策検討/実装							
		外部公開機器，サービスへの対策 全体	調査/リスト化				機器，サービスの調査/リスト化				機器，サービスの調査/リスト化		
		外部公開機器，サービスへの対策 全学向け情報環境	停止・復旧手順書の見直し・共有			整備/見直し				見直し			
		外部公開機器，サービスへの対策 その他機器	有事における対応の見直し		見直し				見直し				見直し
	2	不正ログイン対策の強化	二要素認証拡充			二要素認証適用対象拡充/システム見直し							
			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	アカウント管理ワークフロー見直し			システム検討		新ワークフロー移行	運用			
		ログ管理の徹底	ログ採取方針・管理手法の見直し	ログ採取方針・管理手法の見直し									
			新システムの導入の検討						SIEM等の導入の検討				
		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	技術的更新管理手法検討/整備	要更新管理機器リスト化									
					機器に応じた更新管理手法検討，整備								
		セキュリティアップデート/パッチ適用の徹底 その他機器	更新管理用プラットフォーム検討/整備	管理プラットフォーム導入検討				サーバ管理者向け更新管理監視インタフェース提供					
		インシデント予防，早期発見対策の継続	インシデント予兆調査・早期検知	インシデント予兆調査・早期検知									
			情報収集		脆弱性情報の確認/評価, OSINT								
			脆弱性診断の実施		脆弱性診断				脆弱性診断				
	3	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	一部部局での区域指定の試行									
								全学区域指定/対策					
			物品管理の徹底	物品管理徹底									
4	1	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				計画・実施			
	2	各構成員への教育啓発活動	構成員向けアナウンス啓発活動		アナウンス/注意喚起				アナウンス/注意喚起				アナウンス/注意喚起
			新規構成員への啓発活動				セキュリティセミナー企画/実施				セキュリティセミナー企画/実施		
	3	重要情報を扱う担当者への教育啓発活動	役員・管理職向け啓発活動				情報共有/セミナー				情報共有/セミナー		
			重要情報・システム管理者向け啓発活動				セミナー					セミナー	
5	1	自己点検の実施	自己点検の実施	自己点検				自己点検				自己点検	
	2	監査の実施	外部監査の実施		外部監査体制検討		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	