サイバーセキュリティ対策等基本計画

－第４期（2025～2027年度）－

２０２５年３月２７日

大学共同利用機関法人

自然科学研究機構

はじめに

大学共同利用機関法人自然科学研究機構は、多様な研究員によって研究の場が構成され、技術職員と事務職員が協働している。そして、活動により蓄積される知的資産や利用するシステムは多様である。このような環境において、サイバーセキュリティ対策は、外部からの信頼確保等の観点から重要な事項であり、これを失うことは、大学共同利用機関法人としての運営に重大な支障を及ぼす。

また、先端的な研究技術情報とともに、組織運営上の重要情報は、我々自身はもとより、我が国の科学技術競争力の維持・強化や、経済安全保障等の点から極めて重要な事項である。

以上の認識のもと、大学共同利用機関法人自然科学研究機構は、サイバーセキュリティインシデントの発生防止及びインシデント発生時の影響範囲を最小限に止めるため、自然科学研究機構情報セキュリティポリシー※1のもと、機構長及び情報担当理事のリーダーシップにより、関係役職員が連携し、必要な体制の整備と財源確保を行い、機構全体として組織的・計画的にサイバーセキュリティ対策に取り組み、安全・安心な研究・教育環境を確保する。

この目的を達成するため、最高情報セキュリティ責任者（以下「CISO」という。）は、文部科学省の「大学等におけるサイバーセキュリティ対策等の継続的な取組について(通知)」（令和６年12月25日６文科高第1551号）に基づき、情報セキュリティ対策基準2.1(2)①(f)に規定する「サイバーセキュリティ対策等基本計画」を、第１期（2016～2018年度）、第２期（2019～2021年度）及び第３期（2022～2024年度）に引き続き、第４期（2025～2027年度）としてここに策定し、実施する。

※１　自然科学研究機構セキュリティポリシーは、
・大学共同利用機関法人自然科学研究機構情報セキュリティ確保基本方針
・大学共同利用機関法人自然科学研究機構情報セキュリティ対策に関する基本規程
・大学共同利用機関法人自然科学研究機構情報セキュリティ対策基準
から構成される。

大学共同利用機関法人自然科学研究機構（以下「機構」という。）における「サイバーセキュリティ対策等基本計画－第４期（2025～2027年度）－」（以下「本計画」という。）を次のとおり定める。

１．情報セキュリティインシデントに対する的確な対応と予防

① 機構で働く役職員、共同利用・共同研究者、学生等全ての構成員が、常に情報セキュリティに関する自覚と認識を持ち、サイバーセキュリティインシデントの発生の防止及びインシデント発生時の影響範囲を最小限に止めるよう努める。

② 情報セキュリティインシデントが発生した場合、又はその恐れがある場合は、速やかに機関統一窓口及び情報セキュリティ責任者（又は副情報セキュリティ責任者）に報告・相談する。

③ 情報セキュリティインシデントが発生した場合、機構事務局及び当該機関のCSIRT等が連携し、インシデントの発生から被害拡大防止、インシデント解消のための的確な対応を行う。

④ 情報セキュリティインシデントに至らない事態（ヒヤリハット）については、情報セキュリティインシデントの防止に資するため、機構事務局及び各機関は機密情報を除いて共有する。

⑤ 各機関[※2]は、引き続き、CSIRT等インシデント対応体制の充実を図るとともに、必要により見直しを行う。

⑥ 各機関のCSIRT等が連携し、最新のセキュリティ脅威等の情報を把握・分析し、情報システム機器の更新や必要なソフトウェアの更新・導入等のインシデント予防措置を共有し実施する。

⑦ 機関における情報ネットワークセキュリティの向上を図るため、情報機器の脆弱性に関する情報収集と診断、グローバルIPアドレスを付与しているサーバ及び各機関で管理しているDNSや外部公開サーバ等の棚卸・点検を年１回以上行う。

⑧ 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の適時の更新はもとより、端末機器の暗号化等のセキュリティ対策、盗難対策を行うなどにより、テレワークや所外勤務時のインシデント対応の徹底を図る。

⑨ 研究者データベースや自然科学共同利用・共同研究統括システム（NOUS）など、各機関が運用しているデータベース等、個々の情報セキュリティの状況を常時又は一定期間ごとに確認する。

⑩ 政府等関係機関の情報や外部専門家の知見を活用し、情報セキュリティポリシーや関連規程の点検と必要な見直しや、これに連動したインシデント対応手順書等の更新・整備を行う。

⑪ 緊急時においては、機構の事業継続計画（BCP）に従って、ネットワーク環境・サーバ等の被害状況の把握と復旧に努めるとともに、可能な範囲でのデータのバックアップを行う。

⑫ 各機関において、年１回以上、実態に即したインシデント対応訓練を行う。

⑬ 情報セキュリティインシデントの影響範囲を限定的にするため、ネットワーク構成については、適切なセグメント分け、適正なアクセス制御の観点で、機関の現状を確

認し、必要に応じ変更する。

⑭　重要度の高い情報端末やサーバ装置を監視し、不正プログラム等の検知や対処のため、EDR（Endpoint Detection and Response）等の導入を進める。

⑮　情報セキュリティインシデント発生後の迅速な調査を行うため、あらかじめフォレンジング調査を行う外部機関を選定し、NDA（秘密保持契約）を締結する。

※２　本計画における機関とは、情報ネットワーク等の基盤が構築されている
・機構事務局等
・国立天文台
・核融合科学研究所
・岡崎３機関等
をいう。

２．情報セキュリティポリシーや関連規程、手順書の普及啓発・教育活動の実施

①　情報セキュリティポリシーや関連規程、手順書の普及啓発を行うため、職務・職階別の教育訓練を行う。教育訓練にあたっては、内製の研修資料の他、文部科学省、大学共同利用研究教育アライアンス（IU-REAL）及び民間機関教育機関の知見や資料等を活用し、効率的・体系的に実施する。

・機構の役職員、派遣職員、共同利用・共同研究員及び学生への共通的教育訓練の実施
・情報セキュリティ関係者（CISO、情報セキュリティ管理者、情報システム管理者及びCSIRT等）への専門的教育訓練の実施

②　機構において、年１回以上、標的型攻撃メールの訓練を実施する。

③　教育訓練の実施管理を効率的・効果的に行うため、e-Learning研修システムの導入を図る。

④　インシデントが発生した時は、その事態が終息した後速やかに、再発防止のための注意喚起や対策等の周知徹底を図る。

⑤　生成AIの業務利用等については、「ChatGPT等の生成AIの業務利用に関する申合せ（第２版）」（2023 年（令和５年）９月15日デジタル社会推進会議幹事会申合せ）に準拠するとともに、生成AIの進展に伴い、業務利用等について必要なガイドラインを策定する。

３．情報セキュリティ対策に係る自己点検、情報セキュリティ監査の実施

①　機構の役職員、派遣職員、共同利用・共同研究員及び学生に対し、情報セキュリティ対策の状況を確認するため、年１回以上、自己点検を実施する。

②　情報セキュリティ関係者（CISO、情報セキュリティ管理者、情報システム管理者及びCSIRT等）に対し、所掌するネットワーク・サーバ等の情報セキュリティ対策に係る自己点検を年１回以上実施する。

③　機関の情報セキュリティ責任者を監査責任者とした情報セキュリティ監査室を編成し、年１回、機構事務局等及び各機関を対象に以下の計画で情報セキュリティ監査を実施する。

また、監査対象外の年度においては、監査指摘事項への対応状況に関する監査（フォ

ローアップ監査）を実施する。

【監査計画（対象機関）】

2025年度　機構事務局等及び核融合科学研究所

2026年度　国立天文台

2027年度　岡崎３機関等

４．情報資産の管理

① 機構として守るべき情報は、情報資産としての格付けを明確にし、重要情報のセキュリティマネージメントを行う。

また、格付けの際は、法人文書管理及び個人情報管理の整合性を取ることとする。

② 本計画期間中に、これまでの情報資産の棚卸を行う。特に情報格付けの見直し、未使用のサーバやデータベースの整理等を行う。

③ 情報資産の漏洩、棄損した場合のリスク分析・評価を実施するとともに、必要な情報セキュリティ対策を講じる。特に以下の事項について留意する。

・機密性２以上の情報資産を扱うシステムにおいては、多要素認証の導入や定期的なログ確認などの不正アクセス対策を強化する。

・ユーザーアカウントの定期的な棚卸を行い、退職者のアカウントは速やかに削除又は停止する。

・重要情報を扱う部門のActive Directory等の認証機能を有するサーバ等については、標的型攻撃に対する対策を行う。

・機関から貸与された情報端末の盗難、紛失や不正プログラムの感染等による情報漏洩を防止するため、多重認証ログインや情報の暗号化等のセキュリティ対策を行う。

・重要情報を扱う区域について、年１回以上点検し、区域の明示、入退室方法の確認を行う。

・重要な情報システムについては、ペネトレーションテスト又は脆弱性診断を実施する。

④ 安全保障貿易管理に関する法令を遵守するとともに、研究インテグリティ等の国の政策を注視し、機動的な対応を行う。

⑤ 本計画期間中に、機構及び各機関における業務用アプリケーションの認証機能を充実・強化することや、各種業務情報の集約による業務効率化を推進するため、機構全体の構成員のID管理システムを構築し、運用を開始する。

５．情報化（DX）の推進とクラウドサービスの活用

① 研究事業、事務管理等に関する機構共通の情報DXを引き続き推進する。

② 本計画期間中に、機構及び各機関における業務用アプリケーションの認証機能を充実・強化することや、各種業務情報の集約による業務効率化を推進するため、機構全体の構成員のID管理システムを構築し、運用を開始する。【再掲】

③ 各機関が運用するサーバ類は、予算との関係を考慮しつつ、適宜クラウド化することにより個別のサーバ類を減らし、情報セキュリティリスクを低減する。

④ クラウドサービスを活用するにあたり、ゼロトラストアーキテクチャを考慮した選

定・利用のためのマニュアルを定めるとともに、必要な事項は「クラウドサービス利用のための情報セキュリティマネジメントガイドライン(2013年度版)」(経済産業省)を準用する。

なお、クラウド提供事業者については、原則として「政府情報システムのためのセキュリティ評価制度（ISMAP)」(内閣サイバーセキュリティセンター）の認証を受けた事業者とする。

ただし、「ISMAP等クラウドサービスリスト」以外のサービスを利用するときは、セキュリティリスクを明らかにし、必要な対策等を明示して、機関CISOの許可を得る。

６．サプライチェーンリスクへの対応

① 情報システム・機器・役務等調達においては、情報セキュリティ上のサプライチェーンリスクを軽減するため、「情報セキュリティ上のサプライチェーンリスクに対応するための仕様書追加要件」(令和６年２月１日情報化推進委員会・情報セキュリティ委員会決定）に従う。

② ①の要件が追加されていない既存の外部サービスプロバイダを利用するシステムやデータ、あるいは情報ネットワーク、情報機器については、通信状態やデータ保護について、必要に応じて点検や調査を行う。

７．本計画の実施状況の把握と対応

① 機関CISOは、常に本計画の実施状況を把握し、そのPDCAを検討する。

また、年１回以上情報セキュリティ委員会に報告し、必要に応じて情報セキュリティポリシーや関連規程、手順書等の改定を行う。

② 原則、月１回開催する各機関の情報セキュリティ責任者、CSIRT責任者等によって構成する情報基盤連絡会を活用し、本計画の実施状況に関し情報交換を行うことで、PDCAの基礎的な検討を行う。

③ CISOは、常に最高情報責任者（CIO）と緊密に連携して本計画を実施する。

④ 情報基盤連絡会等を活用し、研究インテグリティ・研究セキュリティの関係部署との連携を強化する。

年間実施計画(目安)

タスク	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
情報セキュリティ委員会			○						○			
機関情報セキュリテイ委員会						○						○
採用時研修	随　時											
情報初任者研修		○										
情報セキュリティ管理者研修			○									
IU-REAL-CISO研修								○				
標的型メール訓練								○	○			
インシデント訓練								○	○			
自己点検				○	○				報告			
情報セキュリティテスト						○	○		報告			
情報セキュリティ監査							○	○	機構長報告			
機構全体情報基盤連絡会	○	○	○	○		○	○	○	○	○	○	○