

共用実験データシステムに関する細則

2025年4月1日制定

共用実験ネットワーク運用責任者

第1条（本細則の目的）

セキュリティを確保するため、共用実験ネットワークに接続する利用者は一定の制限を受ける。この制限のため利用者は、実験データの管理・活用のための各種サービスなどのサービスを構築することが出来ない。そこで共用実験データシステムを定義し、本細則に定める運用体制と運用ルールを遵守した場合について、運用について一定の裁量を認め、成果創出の加速・利便性向上とセキュリティ担保を両立させることを可能とする。本細則は共用実験データシステムの運用に関わるルールを定める。

第2条（ガイドラインとの関係）

本細則は、大型放射光施設ならびにX線自由電子レーザー施設における共用実験ネットワーク利用対策基準（SPring-8/SACLA共用実験ネットワーク利用ガイドライン）」（令和2年10月30日、SPring-8データ・ネットワーク委員会）第6条（細則の制定と見直し）の定めるところに基づき、共用実験データシステム（以下「データシステム」）が共用実験ネットワークに接続する際に求められる事項を、共用実験ネットワーク運用責任者が定める。

第3条（データシステムの運営体制）

データシステムを運用しようとするものはデータシステム責任者（以下「責任者」）とデータシステム担当者（以下「担当者」）を定め共用実験ネットワーク運用責任者に報告しなければならない。担当者は、主担当者を1人、副担当者を1人以上置くこと。

第4条（データシステムの運営時に遵守すべき事項）

責任者及び担当者は以下を遵守すること。ただし、SPring-8/SACLAの運営・高性能化・高度化のために必須でかつ他に代替方法がない等の場合で、責任者が共用実験ネットワーク運用責任者に申請し許可を得た場合に限り、例外を認めるものとする。

(1) 共用実験ネットワークへの接続に関する情報の報告

責任者は、共用実験ネットワークに接続しようとするデータシステムについて、次に掲げる項目を共用実験ネットワーク運用責任者に報告しなければならない。

- (a) データシステムの基本情報（システム構成の概要等）
- (b) データシステムと共用実験ネットワークとの接続を利用する者の範囲
- (c) 共用実験ネットワークに接続する機器の情報（製品名、MACアドレス等）
- (d) 共用実験ネットワークへの接続の情報及び物理的な接続箇所が特定できる情報（接続するネットワークゾーン名、固定IPアドレス、接続期間、建物名、部屋番号、情報コンセント番号等）

(2) 緊急時の対応体制の構築

責任者は、次に掲げる項目を実施し、緊急時における共用実験ネットワークとデータシステムの間での連携した対応の実現を図らなければならない。緊急時の定義は別途定める。

- (a) 主担当者及び副担当者はデータシステムでの一次対応の実務を行うものとする。責任者は、この主・副担当者を選任し、共用実験ネットワーク運用責任者に報告しなければならない。
- (b) 出張や病気等を理由として(a)の主担当者及び副担当者がともに兵庫県播磨地域に不在となり、緊急時の対応の体制確保が困難な場合には、共用実験ネットワークへのデータシステムの接続を休止する等の必要な処置を講じなければならない。
- (c) 共用実験ネットワーク運用責任者が緊急と判断した場合で、かつ(a)の主担当者及び副担当者のいずれとも連絡が取れない場合に限り、共用実験ネットワーク運用責任者はデータシステムにおける緊急の一次対応を代

行することができるものとする。この場合に代行できる内容を、あらかじめ共用実験ネットワーク運用責任者に報告しなければならない。

(3) 接続許可の申請

責任者は、本細則で定める共用実験ネットワーク運用責任者への報告を年度ごとの申請書により行うこと。この申請書は別に定める様式により行うものとする。

(4) セキュリティ対策の実施

担当者は、次に掲げる項目を実施し、データシステムにおける情報セキュリティの適切な維持を図らなければならない。

- (a) データシステムで使用する情報機器のオペレーティングシステムやその他のソフトウェアは、メーカーや開発元によりセキュリティ対策が継続されているバージョンを使用すること。
- (b) データシステムを管理するためのアカウントと、データシステムのサービスを利用するためのアカウントは異なるものを使用すること。
- (c) データシステムのサービスを利用するための認証情報（パスワード等）は他のシステムやサービスと異なるものを使用することを、サービスの利用者に指示すること。
- (d) データシステムで提供するサービスの重要度（機密性、完全性、可用性）に応じて、認証手順の多要素化を検討すること。
- (e) データシステムで提供するサービスの重要度に応じて、セキュリティインシデント発生時の原因究明に必要となる動作履歴（ログ）を記録すること。なお、このログは最低6ヶ月保持すること。
- (f) データシステムで使用する計算機について、共用実験ネットワークからの監査要求に対応すること。なお、監査の時期及び項目は、計算機の重要度を考慮して担当者と協議した上で決定する。
- (g) データシステムの中に無線LANのアクセスポイント機能を有するネットワーク機器を独自に設置してはならない。
- (h) データシステムの中の1台の情報機器を用いて共用実験ネットワークの複数のネットワークゾーンに同時に接続してはならない。ただし、やむを

得ないと共用実験ネットワーク運用責任者が判断する場合は許可することがある。

- (i) データシステムの中に独自のVPN装置の設置は原則禁止とする。ただし、やむを得ないと共用実験ネットワーク運用責任者が判断する場合は許可することがある。

第5条（改善勧告）

共用実験ネットワークの運用責任者は、ガイドラインおよび本細則に適合しないと認めるときは、当該データシステムの責任者に対し、期限を定めて、改善を勧告することができる。

2

共用実験ネットワークの運用責任者は、前項の規定による勧告を受けた責任者がその勧告に従わないときは、当該データシステムを共用実験ネットワークから予告なく切断することができる。

第6条（共用実験ネットワークからの切断）

共用実験ネットワーク運用責任者がセキュリティ担保の観点から必要と認める場合、共用実験ネットワークの運用責任者は、当該データシステムを共用実験ネットワークから予告なく切断することができる。

附則

この細則は、2025年4月15日から施行する。