

J-PARC MLF BL11 における リモートデスクトップ接続を用いたリモート解析環境の構築

一般財団法人総合科学研究機構(CROSS) 中性子科学センター,
^A 国立研究開発法人日本原子力研究機構(JAEA) J-PARC センター
岡崎 伸生, 服部 高典 ^A

Development of Remote Analysis Environment using Remote Desktop Connection at J-PARC MLF BL11

Neutron Science and Technology Center, Comprehensive Research Organization for Science and Society (CROSS), ^A J-PARC Center, Japan Atomic Energy Agency (JAEA)
Nobuo Okazaki, Takanori Hattori ^A

e-mail: n_okazaki@cross.or.jp

Published online: 14 February 2025

要約

大強度陽子加速器施設(J-PARC)の物質・生命科学実験施設(MLF)のBL11に設置されているビームラインPLANETでは、これまで測定したデータをリモート解析したいという要望があったが、それを定常的に行える仕組みが整備されていなかった。この要望に応えるため、リモートデスクトップ接続環境として広く使われているNoMachineを用い、リモート解析が行える仕組みを構築した。このシステムはクラウド上に構築されており、ユーザーはNoMachineクライアントを利用することで、インターネット環境さえあればどこからでも解析することが可能となった。

Abstract

There have been requests for remote analysis of measured data at the beamline PLANET installed at BL11 of the Materials and Life Science Experimental Facility (MLF) of the Japan Proton Accelerator Research Complex (J-PARC), but a system to perform this analysis on a regular basis has not been established. In order to meet this demand, a system for remote analysis was established using *NoMachine*, which is widely used as a remote desktop connection environment. This system is built on the cloud, and users can analyze data from anywhere with an Internet environment by using the *NoMachine* client.

Keywords

リモートデータ解析、リモートデスクトップ環境、NoMachine

Remote analysis、Remote desktop environment

1 緒言

茨城県東海村に位置する大強度陽子加速器施設(J-PARC¹)の物質・生命科学実験施設(MLF²)では、実験ユーザーが遠隔地から実験状況の監視やデータ解析を行える環境の構築が望まれており、各ビームライン(BL)において、それぞれの状況に合わせた遠隔化が様々な形で行われている。ここでいう遠隔地とはJ-PARCサイトで利用できるイントラネットワーク(JLAN)に接続されていないネットワーク環境のことを指す。MLFにおいて、遠隔地から実験の進行状況を確認する手段として、IROHA2³による仕組みや、BL11 PLANET⁴において導入したスクリーンショットによる測定状況確認システム[1]が存在する。また、BL17写楽⁵では、Webを介した実験状況モニタリングおよび解析システム[2]が稼働しており、BL18千手⁶では解析プログラムをWeb化したSTARGazer Online[3]が導入されるなど、遠隔利用の整備は進捗しつつある。

一方、「各装置(BL)にある解析環境をそのまま使いたい」というニーズもあり、それを可能とするリモートデスクトップの利用が検討されてきた。現在、いくつかのBLでJLANのSSL-VPN⁷の機能を用いてMLFサイト内の解析環境に接続する方法[4]が試験的に運用されている。一方、SSL-VPNを利用する場合、申請手続きの煩雑さやリモートデスクトップを安定して使うための帯域が確保しにくいといった制約がネックとなり、一般のユーザーに広く開放するのは難しいのが現状である。また、物理的に計算リソースを用意する場合、状況に合わせて増強するなどの弾力的な運用は困難である。

このような問題を解決するため、本開発ではパブリッククラウドサービスであるAmazon Web Services(AWS)上に解析環境を構築し、リモートデスクトップとして広く使われているNoMachine⁸を使い接続する環境を開発することにした。コストや使い勝手の検証は、BL11ユーザーの協力を得て、実際の解析操作を行うことで確認した。

2 システム実装

2.1 全体構成

全体構成をFig. 1に示す。本システムは、1) クラウド上のリモートデスクトップ環境(Fig. 1a; ネットワークロードバランサー、コンテナ実行環境、解析環境)、および、2) クラウドとオンプレミスにまたがるイベントデータ転送システム(Fig. 1b)からなる。

2.2 リモートデスクトップ環境

本システムは、AWSクラウド上にTable 1に示したサービスを使用して構成した(Fig. 1a)。ユーザーが使用するデスクトップ環境はEC2で構成されており、NoMachine Workstation(以降、Workstation)によりリモートデスクトップ接続を行うことができる。インターネットからの接続は以下の経路で行われる。インターネット側ゲートウェイからの接続はElastic Load Balancing(ELB)の一つであるNetwork Load Balancer(NLB)を使用し、接続先ターゲットは、内部的なサービスアドレス解決によりAWS Fargateで稼

¹ Japan Proton Accelerator Research Complex

² Material and Life science Experimental Facility

³ IROHA2 ポータルサイト <https://mlfinfo.jp/groups/comp/ja/iroha2.html>

⁴ J-PARC MLF 超高圧中性子回折装置 BL11 PLANET <https://mlfinfo.jp/ja/bl11/>

⁵ J-PARC MLF 偏極中性子反射率系 BL17 写楽 <https://mlfinfo.jp/ja/bl17/>

⁶ J-PARC MLF 特殊環境微小単結晶中性子構想解析装置 BL18 千手 <https://mlfinfo.jp/ja/bl18/>

⁷ Secure Socket Layer(SSL)を活用した Virtual Private Network(VPN)プロトコル

⁸ NoMachine Remote Desktop <https://nomachine.com>

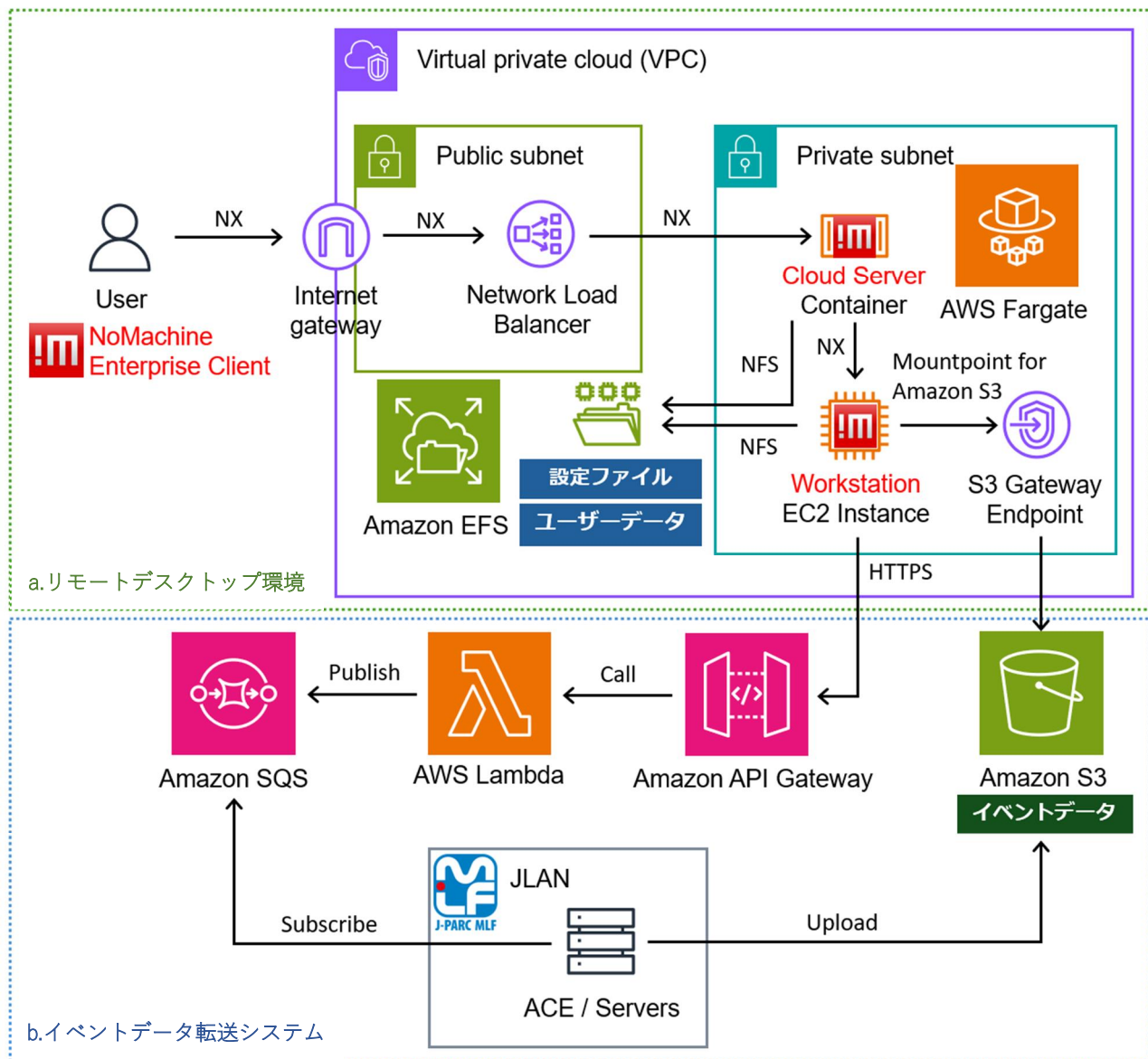


Fig.1 全体構成 a.リモートデスクトップ環境 b.イベントデータ転送システム

働しているNoMachine Cloud Server⁹(以降、Cloud Server)に接続される。この、Cloud Serverではユーザーの認証および最終的に接続するデスクトップ環境(Workstationノード)への振り分けが行われる。Cloud Serverでの認証はSSH公開鍵認証¹⁰を利用しており、それによりパスワードによる認証よりも強固なセキュリティを確保している。加えて、このような構成を採ることで、インターネットから直接接続可能なサーバーはCloud Serverのみとなる。それにより、外部からの攻撃にさらされる可能性のあるサービスを最低限にしている。

認証に成功し、デスクトップに接続したユーザーは、そのデスクトップ上で解析プログラムを起動し、データの解析を行うことができる。イベントデータを配信する仕組みは後述するイベントデータ転送システムにより行う。ユーザーは解析結果などのファイルをNoMachineのファイル転送機能を用いて入手できる。Cloud Serverは、ユーザーごとに接続可能なWorkstationノードを管理者が指定可能であり、ユーザー単位で接続可能なデスクトップ環境を制限することができる。これはユーザーが使用できる環境を選択しやすくし、接続可能な期間を制限するなどして、計算リソースを配分することもできる。

⁹ NoMachine Cloud Server Family <https://www.nomachine.com/cloud-server-family>

¹⁰ Secure Shell(SSH)で認証に用いられる公開鍵基盤を利用した認証方式。秘密鍵を用い認証する

Table 1 AWSで利用している主なサービス

サービス名	機能
AWS Fargate ¹¹	NoMachine Cloud Serverコンテナの実行
Amazon EC2 ¹²	解析環境の実行(NoMachine Workstation)
Amazon EFS ¹³	設定ファイルやユーザーファイルの格納
Amazon SQS ¹⁴	シンプルなタスクキュー
AWS Lambda ¹⁵	イベントデータ転送システムの制御
Amazon S3 ¹⁶	イベントデータのストレージ
Amazon API Gateway ¹⁷	Webアクセスを受け入れる
Elastic Load Balancing (ELB) ¹⁸	インターネットからのアクセス受け入れる

2.3 イベントデータ転送システム

MLFで取得されたイベントデータはMLF先進計算環境(ACE¹⁹)[5]に格納されており、クラウド上にあるデスクトップ環境から直接アクセスすることはできない。そのため、ユーザーが希望するイベントデータ番号をリクエストすると、MLFからクラウド上に自動転送する仕組みを開発した(Fig. 1b)。

ユーザーはスクリプトによりイベントデータリクエストのWeb APIを介して希望するイベントデータ番号(測定Run No.)を指定する。この接続はクライアント証明書により保護されており、証明書で認証されないアクセスは拒否される。Web APIへのリクエストはメッセージとしてAmazon SQSに発行され、キューを購読しているMLFオンプレミスのノードに到達する。このノードはリクエストに従って、指定されたRun No.をAmazon S3の適切なパスにアップロードされる。このS3のパスはユーザーがアクセスするNoMachineにMountpoint for Amazon S3²⁰を介してマウントされており、ユーザーは通常のファイルと同様にイベントデータにアクセスすることができる。

2.4 NoMachine の構成

今回採用したのは、接続の入口となるNoMachine Cloud Serverと、ユーザーが操作するデスクトップ環境を提供するNoMachine Workstationを使用する構成である(Fig. 2)。Cloud Serverは管理サーバーおよびWorkstationノードへのハブとして機能し、ユーザーが接続する際の窓口となる。一方、WorkstationはCloud Serverのノードとして振る舞い、Cloud Serverからアクセス可能なネットワークに配置される必要がある。これにより、ユーザーはまずCloud Serverに接続し、それを経由してWorkstationノードにアクセスする。

¹¹ AWS Fargate <https://aws.amazon.com/jp/fargate/>

¹² Amazon Elastic Compute Cloud <https://aws.amazon.com/jp/ec2/>

¹³ Amazon Elastic File System <https://aws.amazon.com/jp/efs/>

¹⁴ Amazon Simple Queue Service <https://aws.amazon.com/jp/sqs/>

¹⁵ AWS Lambda <https://aws.amazon.com/jp/lambda/>

¹⁶ Amazon Simple Storage Service <https://aws.amazon.com/jp/s3/>

¹⁷ Amazon API Gateway <https://aws.amazon.com/jp/api-gateway/>

¹⁸ Elastic Load Balancing <https://aws.amazon.com/jp/elasticloadbalancing/>

¹⁹ Advanced Computing Environment: MLF から高速にアクセスできる共通ストレージ

²⁰ Amazon S3 バケットをローカルファイルシステムとしてマウントするためのクライアント

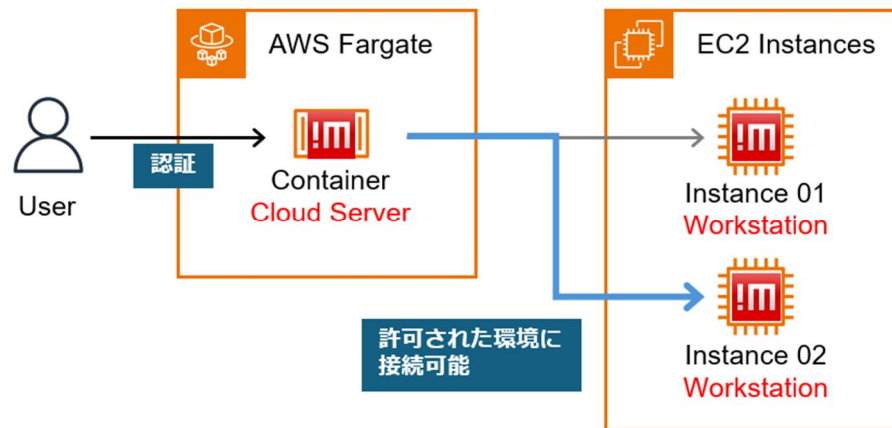


Fig.2 NoMachine の構成

NoMachine Cloud Server

Cloud Serverを使用する構成では、ユーザーはWorkstationに直接接続するのではなく、Cloud Serverに接続する。ユーザーはCloud Serverで認証を行い、その後、管理者により接続が許可されているWorkstationノードを選択し、接続する。Cloud Serverは管理の省力化のため、コンテナイメージをビルドし、サービスとしてAWS Fargate上で稼働させる。設定ファイルなどを保持するための永続ストレージとしてAmazon EFSを使用している。

NoMachine Workstation

WorkstationはCloud Serverの接続先ノードとして動作する。Workstationが動作するEC2は、インスタンス構成時にEC2のユーザーデータスクリプト²¹により自動的に初期化され、環境構築の省力化を図っている。また、EC2上で動作する解析プログラムなどはDocker²²コンテナとして動作するため、OS依存性を最小限に抑えるように設計されている。そのため、ユーザーが増えた場合でもEC2のOSの統一を図りながら様々な解析プログラム(場合によってはバージョン違い)への対応が可能である。

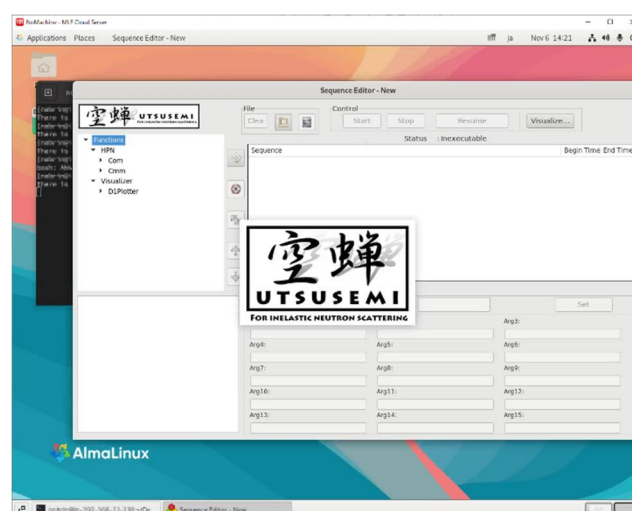


Fig.3 デスクトップのスクリーンショット(空蝉[6]を起動したところ)

²¹ ユーザーデータ入力を使用して EC2 インスタンスを起動するときにコマンドを実行する
https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/user-data.html

²² Docker <https://www.docker.com>

例えば、今回はBL11 PLANETでのデータ処理用としてのデスクトップ環境を用意しており、この環境ではPLANETでの測定データを処理するための空蟬およびTschues²³などがすでにインストールされており、ユーザーはBLでの環境と同じように使うことができる(Fig.3)。

2.5 検証に用いたシステム構成

今回、以下の環境で構築したシステムを用いて動作の確認を行い、リモートデスクトップとして使用可能なことが確認できた。なお、クラウド環境はAWS東京リージョン(ap-northeast-1)を使用した。

NoMachine Cloud Server

- AWS Fargate プラットフォームバージョン1.4.0
- NoMachine Cloud Server 8.13.1 (ベースイメージ: Docker Hub²⁴ almalinux:9.4)

EC2 デスクトップ環境

- Amazon EC2 T3.xlarge (CPU 4コア、RAM 16GB)
- AlmaLinux 9.4
- NoMachine Workstation 8.13.1
- Docker 27.3.1
- Python 3.9.18
- Mountpoint for Amazon S3 1.10.0

3 結果と考察

3.1 実行パフォーマンス

MLF BL11の構成と、2.5に示したシステム構成のパフォーマンスを比較するために、解析プログラム空蟬のCmm.GetNeunetHist()関数によりヒストグラム化にかかる時間を比較した。Table 2に解析環境のスペックと解析時間を示す。結果は、BL11解析環境において14秒かかる内容が、リモート環境では27秒かかった。CPU等のスペックが全く異なるため、単純な比較はできないが、最も大きな要因は、BL11においてはイベントデータへのアクセスが高速なのに対し、リモート環境ではMountpoint for Amazon S3を使用しており、イベントデータへのアクセス速度に時間がかかるためと考えられる。ストレージに関しては様々な選択肢があるため、今後の利用状況やコストメリットを見ながら改善を進めたい。

Table 2 解析にかかった時間の比較

	MLF BL11 HPN_ANA03	リモート環境
CPU	Intel Xeon Gold 6128 3.4GHz	Intel Xeon Platinum 8259L 2.5GHz
RAM	256GB	16GB
計算時間	14秒	27秒

²³ BL11 PLANET の解析用プログラム

²⁴ Docker Hub Container Image Library <https://hub.docker.com>

3.2 セキュリティ

本システムでは、Cloud Serverへの不正アクセスが最も警戒すべき点となる。Cloud Serverへの不正アクセスに対する保護手段は標準でいくつか用意されており、状況に応じてそれらを適切に組み合わせて適用定する。一般的な保護方法として、1) 認証方法の強化、2) NoMachine通信プロトコル(NXプロトコル)の保護の2種類が挙げられる。それぞれについて、内容と効果を示す。1) 認証方法の強化はユーザー名とパスワードの組み合わせによる認証ではなく、SSH公開鍵基盤を使った認証を行う。NXはRSA公開鍵認証²⁵に対応しており、4096ビットRSA(RSA4096)を使用する。RSA4096はセキュリティ強度が128ビット～196ビット程度と見積もられており、CRYPTREC²⁶の基準[7]では、この強度であれば2040年頃まで使用可能とされている。従って、当面の間は問題なく運用できると考えている。2) NXプロトコルの保護は、通信をTLS²⁷で保護し、クライアント認証を必須とする設定とし、実現する。この設定により、X.509²⁸クライアント証明書がインストールされている環境からのみ接続が許可されるため、さらに強力な保護を行うことが可能となる。

3.3 運用とコストについて

本構成はAWS上に構築されているため、運用・保守に関してはAWSに関する知識が不可欠であり、インフラストラクチャの全体像を把握しておくことが求められる。日常的な運用業務が発生するポイントとしては、ユーザー管理、デスクトップ環境の管理が考えられる。現在の構成では、ユーザー認証の設定はCloud Serverのローカルアカウントで行っており、Cloud Server上でのユーザー管理および各デスクトップ環境でのローカルユーザーの設定が必要である。また、状況に応じてユーザーが接続可能なWorkstationノードを制限するなどの設定を行う。また、各デスクトップ環境の管理に関して、OSに関してはセキュリティアップデートの対応などを行う。解析プログラムはDockerコンテナによる整備を想定しているため、必要な解析プログラムのコンテナイメージを作成するために、コンテナイメージのビルド環境を整備しておく必要がある。

本システムの運用にかかる金銭的成本は、主に以下の4つの要素に分けられる。1) 計算リソース、2) ストレージ、3) データ転送、4) ソフトウェアライセンスである。それぞれの詳細を以下に示す。1) 計算リソース(EC2インスタンスやコンテナ)の稼働時間に応じた料金が発生し、運用コストの大半を占める。ユーザー数や使用時間、容量に比例し、利用拡大時には効率的な運用が必要になるかもしれない。2) データや解析結果を保持するストレージに利用料金が発生する。そのため、データの整理やライフサイクル管理(一定期間アクセスがないデータは自動で削除)などが必要になる。3) 外部へのデータ送信に費用が発生するが、MLFの解析環境ではデータ送信量は少なく、さほど考慮する必要はないと思われる。4) NoMachine Cloud ServerおよびWorkstationのサブスクリプション費用が定期的(1年ごと)に発生する。

3.4 今後の展開

現時点では、NoMachineクライアントからのみの接続を想定しているものの、NoMachineはWebブラウザによる接続も可能である。そのため、ユーザーの要望に応じてWebアクセスの導入も検討できる。その際にはApplication Load Balancer(ALB)の追加やWebアクセス保護などの追加設定が必要となる。また、

²⁵ RSA 暗号を用いた公開鍵基盤による認証

²⁶ Cryptography Research and Evaluation Committees: 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト <https://www.cryptrec.go.jp>

²⁷ Transport Layer Security: セキュリティを要求される通信を行うためのプロトコル

²⁸ 国際電気通信連合電気通信標準化部門(ITU-T)の公開鍵基盤(PKI)の規格

今後、利用ユーザーが増加した場合に、現在のローカルユーザー管理では運用が煩雑化する可能性がある。その場合はLDAP²⁹などの導入を視野に入れ、ユーザー管理方法の整備を進める必要がある。ただし、機能やユーザー数の拡大に伴い、保守範囲や管理コストも増加するため、導入の際には日常的な運用を想定した整備を進めることが重要である。

謝辞

本環境の検証は、東京大学大学院理学系研究科附属地殻化学実験施設 小松一生准教授に協力していただきました。深く感謝いたします。

参考文献

- [1] N. Okazaki and T. Hattori, CROSS Reports, **1** (2023) 1. DOI:10.57378/crossrep.2023001
- [2] S. Kasai *et al.*, CROSS Reports, **2** (2024) 2. DOI:10.57378/crossrep.2024002
- [3] T. Ohhara *et al.*, J-PARC Annual Report 2019, **2** (2020) 104-105.
- [4] Y. Inamura and N. Okazaki, J-PARC Annual Report 2021, **2** (2022) 131-134.
- [5] 稲村泰弘, 日本中性子科学会誌「波紋」, **31** (2021) 121-127.
- [6] Y. Inamura *et al.*, J. Phys. Soc. Jpn., **82** (2013) SA031-1-SA031-9.
- [7] CRYPTREC LS-0003-2022r1 暗号強度要件(アルゴリズム及び鍵長選択)に関する設定基準
<https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf>

²⁹ Lightweight Directory Access Protocol: ディレクトリサービスを認証に使うためのプロトコル