複数計算資源の連携・
次世代HPCIのセキュリティ

竹房あつ子
国立情報学研究所
2025年6月26日

資源管理

NII

リーダー：竹房@NII
NII: 佐賀、田中、高倉、坂根、合田、栗本、政谷、吉田
東工大：坂本、大阪大：伊達、九州大：大島、南里、
産総研：滝澤、東大：塙、理研：山本、他、運用FSの皆様
協力：アルテアエンジニアリング様、日本オラクル様、日本マイクロソフト様

目的：次期フラッグシップシステム、国内主要スパコン＋リアルタイムデータ・蓄積データ基盤＋それらを接続する学術情報ネットワークSINET

クラウドとの連携

一体的に運用される基盤の構築・運用に必要とされる技術的要件を検討
- 利用効率、高可用性や耐故障性
- 電力需給バランス調整によるスパコン・クラウド間連携によるカーボンニュートラル化への貢献
- セキュリティリスク

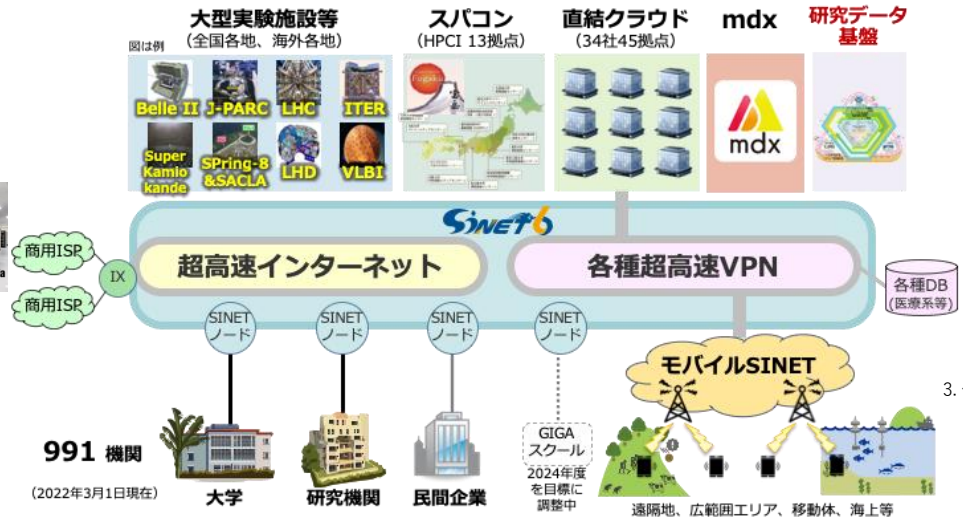
評価指標：ジョブ充填率、待ち時間、利用率、稼働率

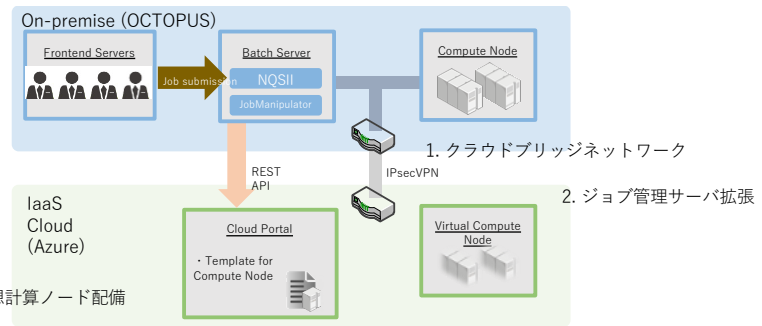
検討項目:
A)「フラッグシップシステム」と国内主要スパコンの資源管理連携
- システム間でジョブやデータを高効率で融通する技術

B)「フラッグシップシステム」他とリアルタイムデータ・蓄積データ基盤との連携
- 高度なデータ連携について Society 5.0運用調査検討、データ利活用調査検討グループとともに検討

C)「フラッグシップシステム」他とクラウドとの連携
- 連携する際の性能、可用性、ユーザビリティ、セキュリティの点で課題抽出（クラウドバースティングを例に）

D)上記連携を可能にするためのネットワーク技術
- 学術情報ネットワークSINETに求められる性能・機能要件を調査





クラウドバースティングの例(大阪大学)

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

R4年度成果（1/2）

NII

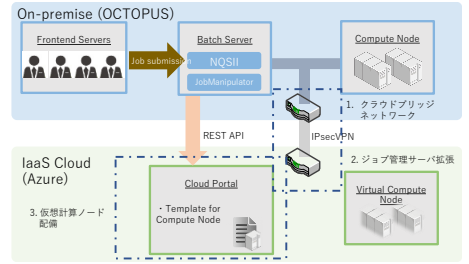
A)「フラッグシップシステム」と国内主要スパコンの資源管理連携

1.情報共有，運用制御技術に関する現状把握

- **海外動向調査**(学会: HotCarbon, SC, 計算基盤: ACCESS, EGI等 の論文, Web調査)
  - 低カーボンフットプリント運用の標準的手法ない. 資源の潜在的炭素排出量対応, 電力グリッド内の需給状況に応じた連携等も検討中
  - 米国: ACCESS, 欧州: EGIでは, 複数計算センターの一体的資源利用, データ基盤連携, 人的連携等が既に実現されている
- **国内主要基盤センター運用制御技術把握** (富岳, 9基盤センター, ABCI, HPCI共有ストレージ, SINETへのヒアリング)
  - 各基盤センターは同様の運用制御技術・情報を有しているが,
    制御方法, 運用情報の共有, 共通情報の追加, 調整等，**連携運用には課題多い**

2.利用者に対する統一I/F調査，一部動作検証

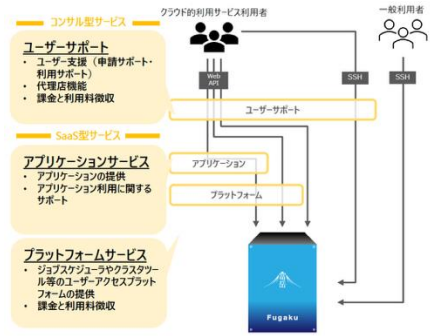
- 利用者環境: GakuNin RDM, Open OnDemand+Jupyterなど．スパコンとのファイル共有など課題
- I/F: RESTful I/F, S3ベース I/F, 既存スケジューラ I/F
  - RESTful I/F: 理研が富岳用に NEWT実装, 公開． S3ベース I/F: 多く採用されており, ABCI クラウドストレージも採用



クラウド資源利用(阪大)

C)「フラッグシップシステム」他とクラウドとの連携

- **資源利用**: クラウドバースティング(阪大, 九大, 産総研), ホスティング(東北大), ストレージ(理研)
  - 資源不足時の補完に効果的であるが, センターのビジネスモデルが難しい
- **スパコンのクラウド的提供**: 計算(理研, 九大, 産総研), ストレージ(産総研)
  - 計算資源提供は, SaaS型からバッチ＋コンテナ実行まで様々でWebベース (I/F仕様は様々)での提供が主
  - ストレージ資源提供はオブジェクトストレージ(S3互換)である



クラウド的提供(理研)

R4年度成果（2/2）

NII

C’) セキュリティ課題抽出

– クラウドデータセンター セキュリティアセスメントを理研, 東大のスパコンに適用, 課題を抽出
（外部コンサルと共同で実施）

- 性能重視の構成, データの責任分界点の違いなどから, 一般システムとは一部異なるアセスメントが必要なことを抽出.
- HPC固有の脅威や一体的運用のための安全なセンター間連携などを考慮したアセスメントの検討が必要である

→ セキュリティ対策強化の追加調査研究

R5年度成果

NII

A)～D) **一体的に運用される基盤**の構築・運用に必要とされる技術的要件を検討

I) 一体的運用として**目指す姿の検討開始（図１）**

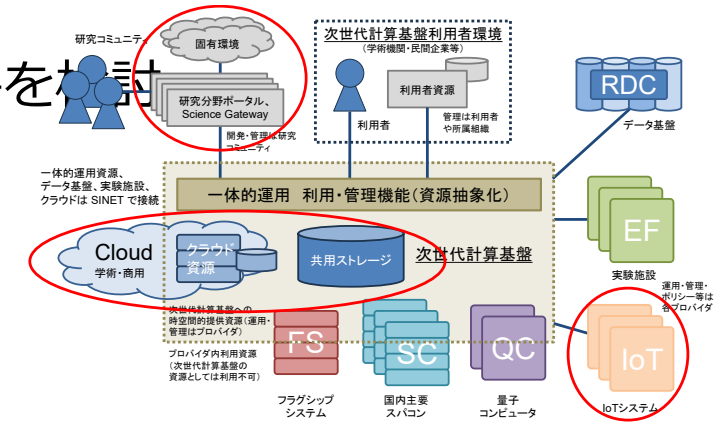
- 柔軟でシームレスな計算資源の利用
- 運用主体が異なる資源の一部をまとめ一体的運用するための前提と課題
- 既存の研究環境と一体的運用計算基盤の連携による研究加速

II) 既存の**国内外の一体的運用計算基盤等の調査**

- HPC系として米国のACCESS、日本のHPCI、HTC系として欧州のEGI、
  データ基盤として欧州のEOSC(一部機能)、参考としてグリッド研究のNAREGIを調査し、機能や課題を抽出した
- 欧米における実験施設とスパコンとの連携，スパコンと量子コンピュータのハイブリッド計算について調査

III)上記検討項目毎のユースケース等から**必要機能の抽出（図２）**，**一体的運用のたたき台を作成**し、チーム内で議論

- 必要機能について、既存の一体的運用計算基盤でのサポート状況、利用可能ソフトウェアを調査した



○:「次世代計算基盤検討部会のポスト「富岳」時代に目指すべき姿」との違い

図１　目指す姿

C') **セキュリティ対策強化**

II) HPCデータセンター向けセキュリティガイドライン ドラフト作成

- NIST の Cyber Security Framework を基にした
  HPC システム用セキュリティガイドラインのドラフトを作成した

→ R6年度はこれらの調査をさらに詳細化

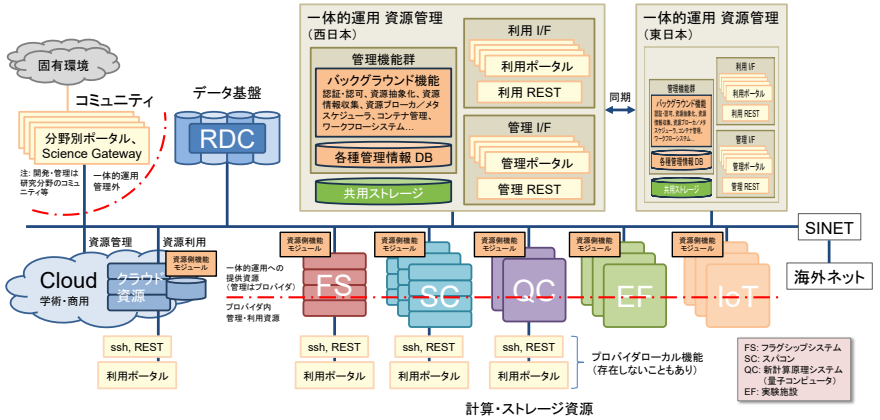


図２　一体的運用計算基盤の構成例

概要

- 複数計算資源の連携（一体的運用される計算基盤）
  1. 公募要領が求める調査研究項目（資源管理関連）
  2. 欧米の計算基盤の調査
  3. 利用方法検討
  4. 機能検討
  5. 構成検討
  6. まとめ
- 資源スケジューラのイベント駆動型ワークロードへの対応状況調査
- 次世代HPCIのセキュリティの検討

概要

- 複数計算資源の連携（一体的運用計算基盤）
  1. 公募要領が求める調査研究項目（資源管理関連）
  2. 欧米の計算基盤の調査
  3. 利用方法検討
  4. 機能検討
  5. 構成検討
  6. まとめ
- 資源スケジューラのイベント駆動型ワークロードへの対応状況調査
- 次世代HPCIのセキュリティの検討

1. 公募要領が求める調査研究項目（資源管理関連）

NII

- 踏まえるべき、これまでの文部科学省における検討（役割、機能の方向性）
  - p1:　国内主要計算基盤、データ基盤、ネットワークを一体的に運用、持続的に機能
  - p2:　最先端のシミュレーション、AI用学習データの生成、大量データ処理
  - p3:　実験系の研究者も利用しやすい計算環境
  - p4:　ジョブと計算資源のアロケーション最適化
  - p5:　他のシステムとの連携・融合を可能とする機能拡張性
  - p6:　ジョブを最適に実施するメタスケジューラ

- 本調査研究の事業の概要： 調査研究内容
  - p7:　Society5.0推進
  - p8:　SDGsの達成貢献
  - p9:　一体的運用に伴うセキュリティリスクへの対策
  - p10:　機密性の高いデータの安全な処理
  - p11:　仮想化と資源管理
  - p12:　クラウド連携
  - p13:　高可用性
  - p14:　リアルタイム処理

※ 類似の項目は集約、番号は独自に採番

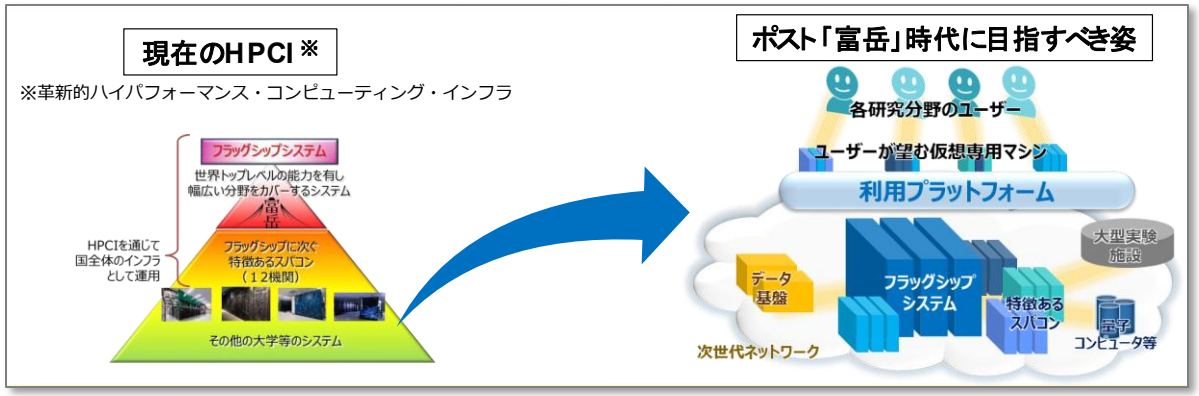

令和４年度

「次世代計算基盤に係る調査研究」

公　募　要　領

文部科学省
MEXT
MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY-JAPAN

令和４年５月



次世代計算基盤検討部会による「ポスト「富岳」時代に目指すべき姿」

1. 調査研究項目のポイント（資源管理関連）

NII

1. 他基盤との連携機能（異なる基盤の資源との連携）
   - データ基盤との連携
   - 分野別研究基盤（っ 実験施設）との連携　…

2. 高度な計算資源管理・ワークロード実行管理機能（同じ基盤内の資源の高度な連携）
   - ワークロードと資源配置の最適化
   - 資源操作の抽象化
   - ワークロードのポータビリティ（仮想化、コンテナ化、実行形式プログラム管理）
   - 資源、プロバイダを跨るワークロードの実行管理
   - 緊急ジョブ等イベント駆動型ワークロードのサポート　…

2. 欧米の計算基盤

欧州：EGI、EOSC（EU Node）、米国：ACCESS、DOE HPC計算資源群など、主流の基盤を調査

- EGI、ACCESS:
  グリッド時代から機能更新、世代交代を続ける一体的運用計算基盤
  - DataGrid (HTC) → EGEE (HTC) → EGI (HTC, Cloud, HPC)
  - TeraGrid (HPC) → XSEDE (HPC) → ACCESS (HPC, HTC, Cloud)
- EOSC:
  様々なデータ基盤、計算基盤、研究基盤、クラウド等を統合する総合研究基盤
  - EOSC EU Node: EOSC の計算基盤（一部 EGI が資源提供）
- DOE HPC:
  DOE の計算資源群。単体運用であり、一体的運用はしていない

2. 調査研究項目のポイントと欧米の計算基盤

NII

1. 他基盤との連携（異なる基盤の資源との連携）

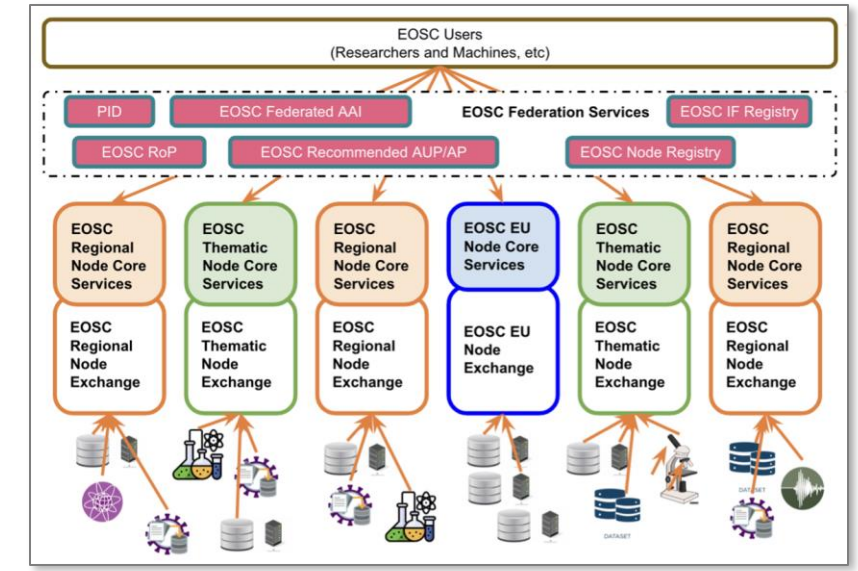
– データ基盤との連携

- 欧米とも利用するデータ転送機能が連携をサポート（例：EGI が利用する OneData）

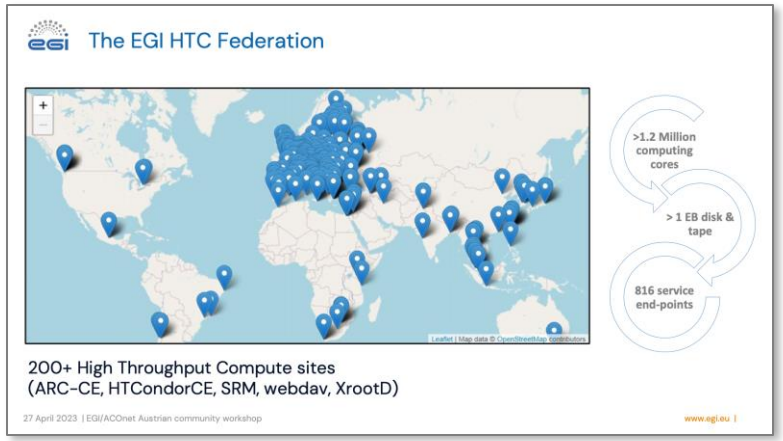
– 分野別研究基盤（実験施設含む）との連携

- 欧州: EOSC（総合研究基盤）が、欧州の様々な分野別研究基盤、計算基盤を Node として連携
  EGI も計算基盤として連携
- 米国: 分野別研究環境である Science Gateway 毎に ACCESS と連携、
  DOE Integrated Research Infrastructure (IRI) フレームワークにより実験施設毎に DOE HPC 計算資源と連携

– 連携機能: EOSC ＞ DOE IRI ＞ EGI, ACCESS



EOSC



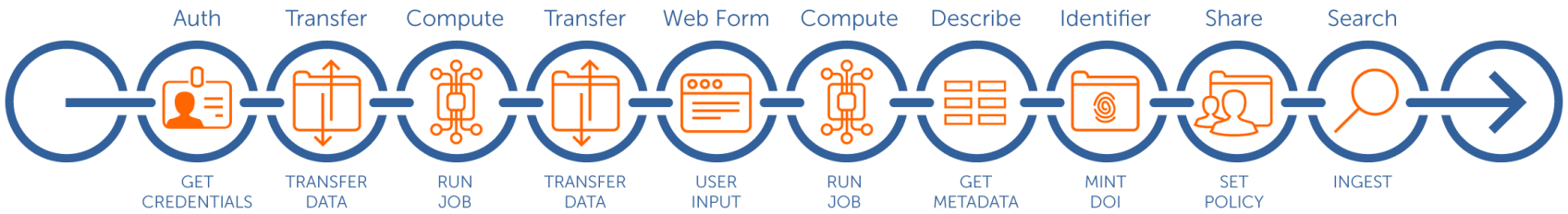
EGI e-infrastructure: Advanced computing services for science より

EGI

2. 調査研究項目のポイントと欧米の計算基盤（続）

NII

2. 高度な計算資源管理・ワークロード実行管理機能（同じ基盤内の資源の高度な連携）
   - 欧州: EGI は内部にメタスケジューラやワークフローなど資源間の計算連携機能を持つ**機能一体型**
   - 欧州: EOSC は連携する Node の機能に依存
   - 米国: ACCESS は内部には計算連携機能を持たず、ACCESS を利用する分野別研究環境である Science Gateway に計算連携機能を持つ**機能分散型**
   - 米国: DOE HPC は資源の単体利用であり、資源やプロバイダ間の標準的な連携機能はないが、IRI を実現する Globus（以前の Tool Kit とは異なる）等により、**資源間の計算連携**が可能
   - 機能: EGI ＞ DOE IRI （Globus） ＞ ACCESS



Globusのワークフロー例

3. 利用方法検討

- 利用形態
  - **計算のみ**
    - 入力データ: 無し（引数のみ）、stdin、予め計算資源の一時ストレージなどに転送
    - 出力データ: 無し（終了コードのみ）、stdout と stderr、一時ストレージなどに出力し転送
  - **外部の基盤と連携した計算**
    - 入出力データは、上記のデータに加え、実験装置、IoTシステム、データリポジトリ等のデータ

- 利用機能
  - **従来互換機能**
    - 利用者が選択した資源単位に直接利用するための機能
  - **新機能（公募要領が求める従来機能以外の機能）**
    - 利用者やシステムが選択した任意の資源をシームレスに利用可能な機能

3. 利用エンドポイント

NII

利用形態と利用機能を組合せた４種類の利用エンドポイント

- EP1: 計算のみ／新機能

  次世代計算基盤ポータルから任意の計算資源の利用

- EP2: 連携計算／新機能

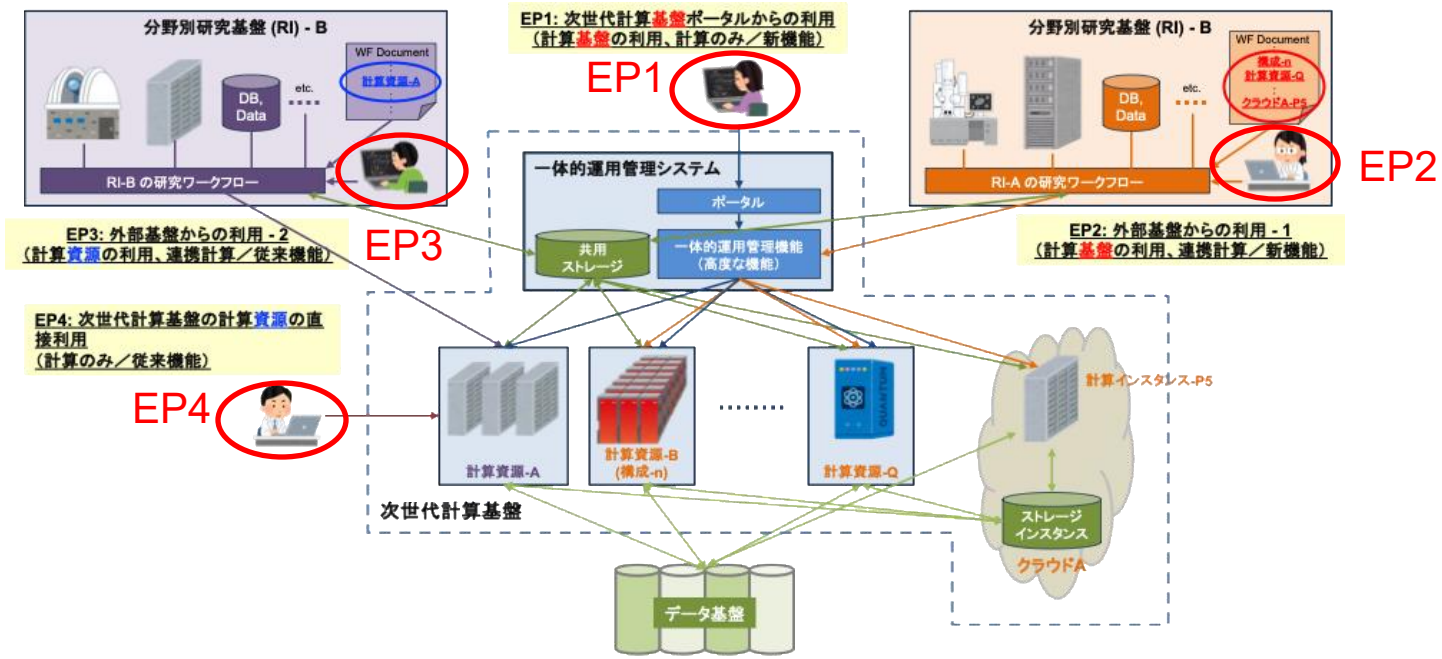
  外部基盤から次世代計算基盤の様々な機能、計算資源を利用

- EP3: 連携計算／互換機能

  外部基盤のジョブスケジューラベースの計算資源を次世代計算基盤の計算資源に置き換え

- EP4: 計算のみ／互換機能

  – 従来方法（スクリプト等）での次世代計算基盤の計算資源利用（小改編要）



4. 機能検討

以下の検討項目に対してユースケースを設定し、必要となる機能を検討

- 計算基盤としての基本機能
- 公募要領の調査検討項目に対する検討項目
  - A) 「フラッグシップシステム」と国内主要スパコンの資源管理
    システム間でジョブやデータを高効率で融通する技術
  - B) 「フラッグシップシステム」他とリアルタイムデータ・蓄積データ基盤との連携
    高度なデータ連携についてSociety 5.0運用調査検討、データ利活用調査検討グループとともに検討
  - C) 「フラッグシップシステム」他とクラウドとの連携
    連携する際の性能、可用性、ユーザビリティ、セキュリティの点で課題抽出（クラウドバースティングを例に）
  - D) 上記連携を可能にするためのネットワーク技術
    学術情報ネットワークSINETに求められる性能・機能要件を調査
- その他

4. ユースケースと必要機能

NII

機能分類	ユースケース		必要機能	公募要領との関係
	目的	操作・動作		
基本機能	資源選択～実行	利用者が選択した任意の資源でシンプルなワークロードを実行	1. 統一されたID、アカウントの管理	p1
			2. 全ての資源、サービスに対応する認証・認可	p1, p4, p7, p8, p11, p14
			3. 全資源、全プロバイダ等の静的、動的な情報の管理、表示等	p1, p4, p6, p7, p8, p11, p14
			4. 実行形式プログラム管理	p1, p4, p7, p8, p11
			5. 抽象化されたWL実行管理	p1, p4, p7, p8
			6. 共用ストレージ	p1, p4, p7, p8, p14
			7. 大規模データ、大量ファイルの高性能・セキュアなデータ転送	p1, p4, p7, p8, p14
			8. 統一的なアカウンティング管理	p1, p4
			9. 一体的運用ポータル	p1, p3
A	最適資源選択	WL実行要件、利用者要件、資源状況などから、利用者が使用する資源を選択	基本機能(#3)	
		利用者毎に異なる利用可能資源から、実行に最適な資源をシステムが選択	10. 資源ブローカ／メタスケジューラ	p3, p4, p6, p7, p8, p13
	実行	複数の資源に渡るWF実行	11. 複数プロバイダ対応WFシステム	p2, p3
		複数の資源のコンテナオーケストレーション	12. コンテナオーケストレータ	p3, p11
		実行するWLの管理	基本機能(#4)	
		WL投入・管理操作	基本機能(#5)	
		複数の従来型計算資源による連成計算、システム分散計算	13. 従来型計算機資源間での連成計算のための実行開始時刻同期	p2
		HPC・QC ハイブリッド計算	14. HPC・QCハイブリッド計算制御	p2

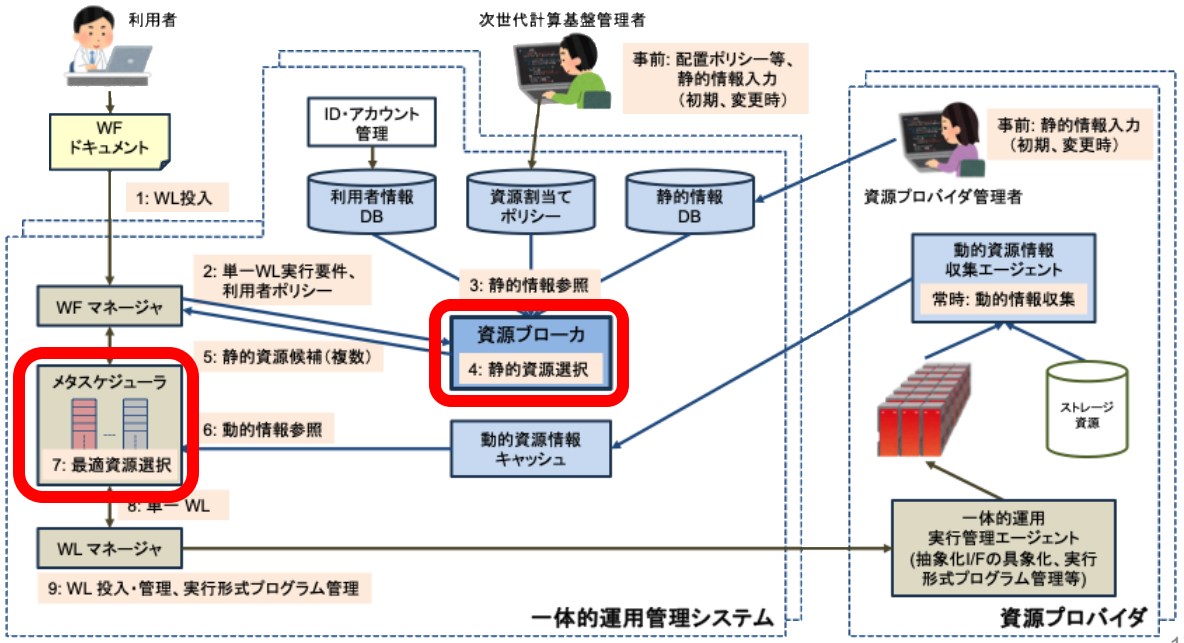
機能分類	ユースケース		必要機能	公募要領との関係
	目的	操作・動作		
A (続)	状況変化対応	WL実行待ち時の資源や環境の状況変化への対応	15. 実行待ちWLの時空間的移動	p8
	防災・減災	災害時における緊急WL優先実行	16. チェックポイント／リスタート	p7
			17. スポットWL	p7
B	データ利用・蓄積	一体的運用環境からデータ基盤の利用	18. データ基盤I/Fのサポート	p2, p5, p7
			19. データ蓄積用メタデータのサポート	p5, p7
	計算機資源提供	データ基盤など外部基盤から次世代計算基盤の計算機資源の利用	20. 計算基盤I/F	p5, p7, p14
	研究加速	実験施設、IoTシステム連携のための低遅延WL起動・再開(リアルタイム処理、ストリームデータ処理等)	21. プリエンプティブWL	p2, p7, p14
			22. ギャングスケジューラと同期型のWL高速切替え	p2, p7, p14
C	クラウド資源利用	クラウドインスタンス(IaaS)の管理	23. インスタンス管理の抽象化	p4, p5, p7, p12
			24. 秘匿情報管理	p4, p5, p7, p12
	資源提供	クラウドから一体的運用資源の利用	基本機能＋#20	p5. p7, p12
D	データ転送	計算データと計算結果の転送	基本機能(#7)	
		データ転送時間保証	25. ネットワークのバンド幅保証と保証時間管理	p2, p4, p7, p8, p14
その他	セキュリティ	一体的運用としてのセキュリティ	26. プロバイダセキュリティと一体的運用セキュリティ	p4, p7, p9, p10
	高可用性	一体的運用環境の 24/7 の利用	27. 一体的運用管理システムの高可用化	p4, p13
	資源プロバイダ構築	資源プロバイダ環境の構築作業	28. 資源プロバイダ機能のコンテナ化／アプライアンス化	

24ユースケースから必要機能28項目を抽出

4. 特徴的な機能: メタスケジューリング

NII

- 資源ブローカ
  - 利用者が利用可能な全資源から、静的情報（資源割当てポリシー、資源の静的情報、ワークロード実行要件など）をもとに利用優先順位を決定
  - 緊急ワークロードの場合、緊急時用のポリシーを使用
- メタスケジューラ
  - 上記利用優先順位順に常時収集の動的情報（資源状況、利用者ポリシーなど）から最適資源を選択、ワークロード投入
  - 緊急ワークロードの場合は、高速性、安定性などを重視して資源を決定
- 実行形式プログラム管理
  - コンテナや資源毎のビルド・配布の管理



WF: ワークフロー
WL: ワークロード

4. 特徴的な機能: イベント駆動型ワークロード

NII

- イベント駆動型ワークロード

  緊急ワークロード、実験施設連携ワークロード、リアルタイムデータワークロード、
  ストリーミングデータワークロード、LLM推論ワークロード、など
- 資源利用効率の観点から、イベント検出処理を小資源で常時実行、データ処理はHPC資源でイベント発生時に起動もしくは再開
- イベント検出からデータ処理開始までに許容されるレイテンシにより、利用者が実行方法を選択

許容レイテンシ	資源獲得方法	停止WLの停止・再開方法	備考
数分～	他WLの一時停止	チェックポイント／リスタート	
100m秒～数分	スポットWLのキャンセル	再開なし	スポットWL：キャンセルされる危険性があるがコストが低いWL
	プリエンプティブWLの一時停止	プリエンプション	同期型の高速切替え機構が必要
～100m秒	切替え不可のため、あらかじめ常時起動	停止WLなし	

定量的な評価は別途説明

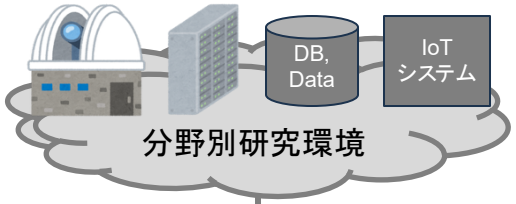
4. 必要機能の配置

NII

次世代計算基盤外
（一体的運用管理外）

次世代計算基盤

分野別研究基盤・研究コミュニティ



研究分野ポータル
(Science Gateway)

<# 20 (クライアント)>

注: 開発・管理は研究分野やコミュニティ

一体的運用 管理サイト
（西日本）

<# 1 - 5, 7, 8, 10 - 15, 18, 23, 25(クライアント), 26, 27>

管理機能群

バックグラウンド機能
認証・認可、情報管理、資源ブローカ／メタスケジューラ、WF、コンテナ管理、資源抽象化、…

<# 3, 24> 各種情報 DB

<# 2, 6> 共用ストレージ

利用・管理環境

利用ポータル <# 9>

計算基盤 I/F (利用I/F) <# 20>

管理ポータル <# 9>

管理 REST

フォアグラウンド機能
認証・認可、情報検索、WF、コンテナ管理、秘匿情報管理、…

<# 1 - 4, 7, 8, 11, 19, 24, 27>

同期

一体的運用 管理サイト
（東日本）

管理機能群

バックグラウンド機能
認証・認可、情報管理、資源ブローカ／メタスケジューラ、WF、コンテナ管理、資源抽象化、…

各種情報 DB

共用ストレージ

利用・管理環境

利用ポータル

計算基盤 I/F (利用I/F)

管理ポータル

管理 REST

フォアグラウンド機能
認証・認可、情報検索、WF、コンテナ管理、秘匿情報管理、…

SINET

<# 25>

海外ネット

研究データ管理

データ基盤

計算資源

インスタンス管理

資源利用

Cloud
学術・商用

資源側管理機能

クラウド資源

ssh, REST

利用ポータル

FS: フラグシップシステム
SC: スパコン
QC: 新計算原理システム（量子コンピュータ）

資源側管理機能 <base + #13> FS

資源側管理機能 <base + #13> SC

資源側管理機能 <base + #14> QC

一体的運用への提供資源（管理は資源プロバイダ）

資源プロバイダ内利用資源
時空間的に一体的運用と分離

ssh, REST

ssh, REST

ssh, REST

プロバイダローカル機能（存在しないこともあり）

base = <# 2 - 5, 7, 8, 12, 15 - 18, 20 - 22, 25, 26, 28>

5. 一体的運用計算基盤の構成検討

NII

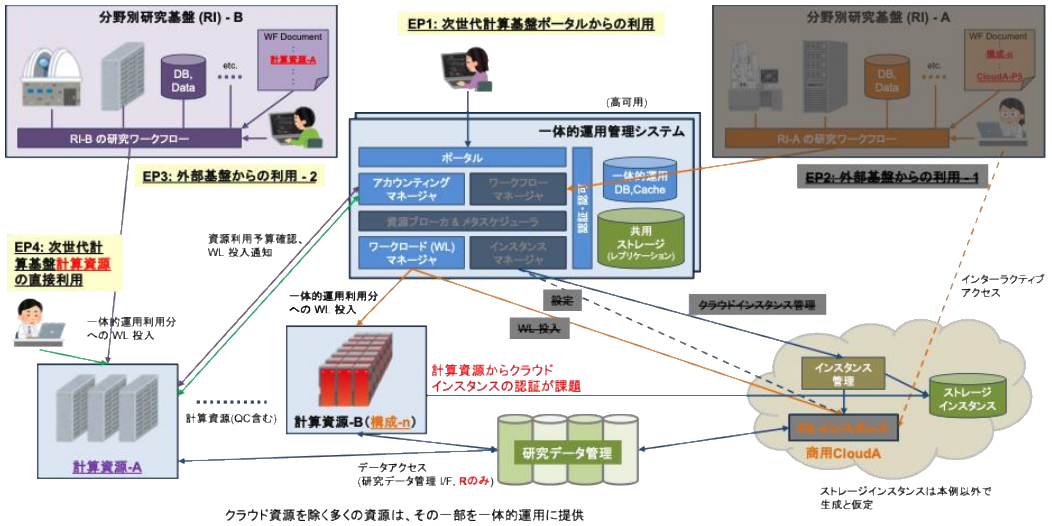
- 一体的運用計算基盤の機能を段階的にサポートする構成を検討
  - 欧米の計算基盤は、「ポスト「富岳」時代に目指すべき姿」に近い機能を持つ
  - これら基盤の OSS を利用しても、運用レベルの計算基盤の開発には多くの工数が必要
  - EGI, ACCESS は長期間に渡る機能追加や更新により現在の形になった。現在も進化中

1. 基本構成
   - ポータルや外部基盤から計算資源単体を利用
2. 資源連携構成
   - 基本構成の機能に加え、ワークフローツールなどで複数資源を連携して利用可能
3. 高機能構成
   - 資源連携構成の機能に加え、ポリシーによるワークロードや資源のアロケーション最適化が可能

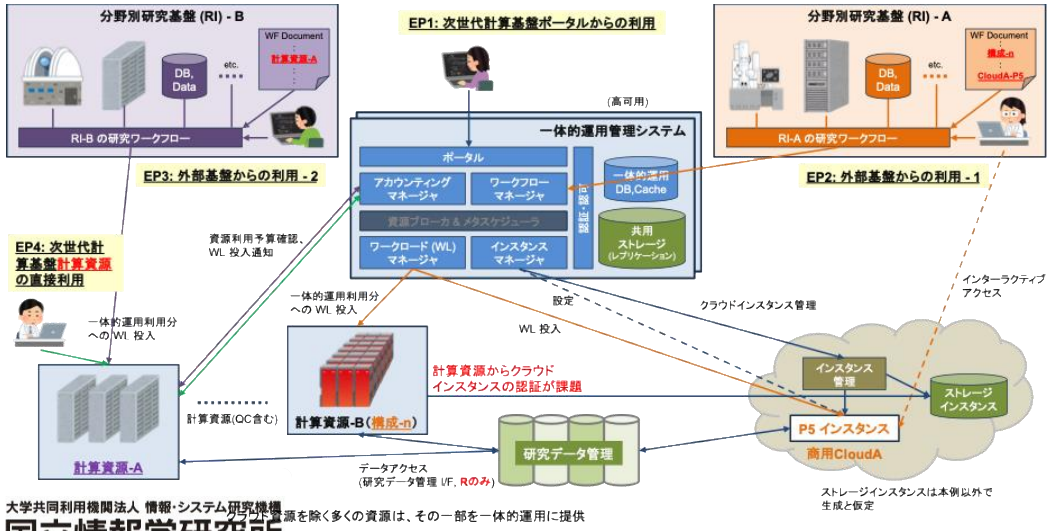
5. 一体的運用計算基盤の構成検討

NII

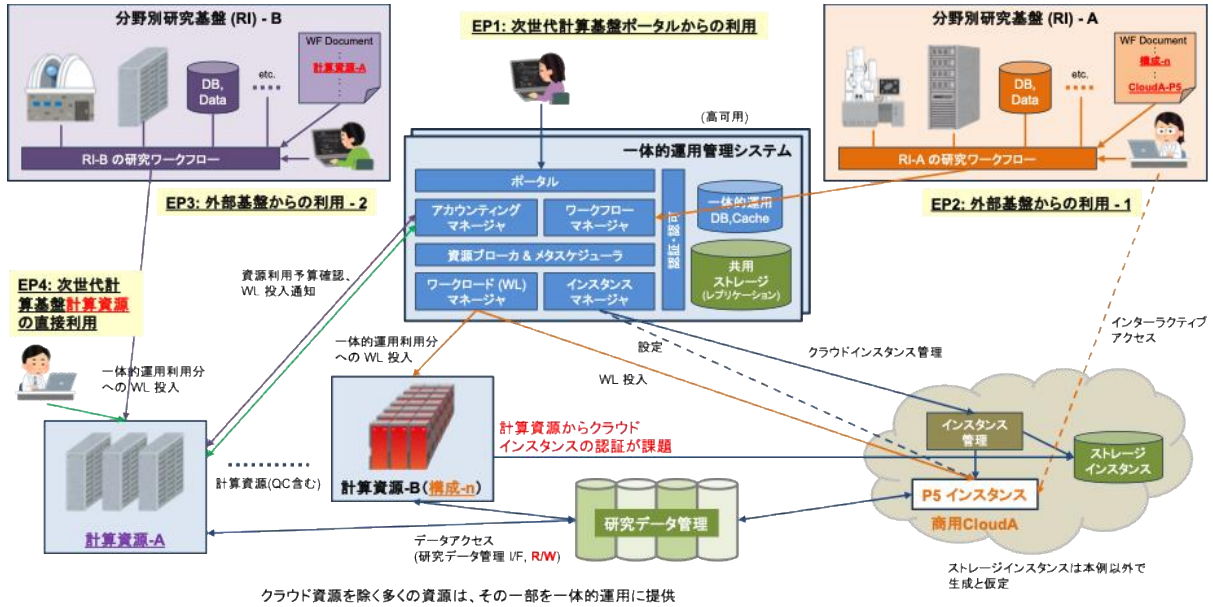
1. 基本構成：ポータルや外部基盤から計算資源単体を利用



2.資源連携構成：基本構成＋WFなどで複数資源を連携利用



3. 高機能構成：資源連携構成＋ポリシーによる資源最適化



6. 複数計算資源の連携のまとめ

- 欧米の計算基盤の調査
  - 欧州のEGIは内部に様々な連携機能を持つ機能一体型
  - 米国のACCESS、DOE HPC は計算に特化し連携機能を外部に持つ機能分散型
- 機能検討
  - 24ユースケースから28の必要機能を抽出
  - 特徴的な機能の検討
    - メタスケジューリングの検討
    - イベント駆動型ワークロードの検討
- 構成検討
  - 機能分散型から機能一体型へ段階的に拡大する構成を検討

概要

- 複数計算資源の連携
  1. 公募要領が求める調査研究項目（資源管理関連）
  2. 欧米の計算基盤の調査
  3. 利用方法検討
  4. 機能検討
  5. 構成検討
  6. まとめ
- 資源スケジューラのイベント駆動型ワークロードへの対応状況調査
- 次世代HPCIのセキュリティの検討

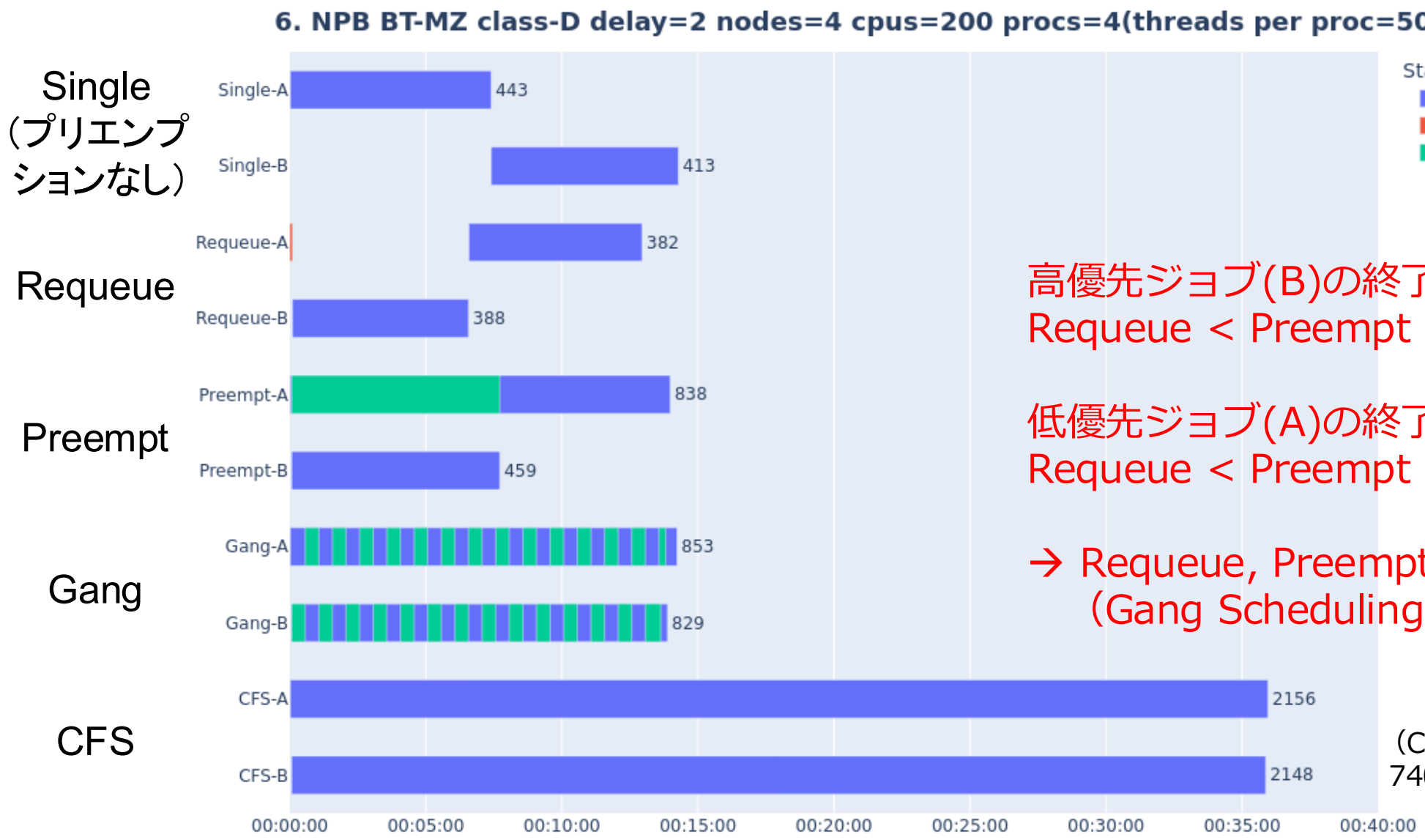
イベント駆動型ワークロードへの対応状況調査

NII

イベンド駆動型ワークロード（高優先ジョブ）への対応状況をSlurmで比較・調査

- スケジューリングポリシ
  - **Single**：プリエンプション無効，ジョブは順番にスケジュール
  - **Requeue**：先行（低優先）ジョブをCANCEL後リキュー，緊急（高優先）ジョブを素早く実行
  - **Preempt**：先行ジョブを停止し，高優先ジョブを素早く実行
  - **Gang**：Gang Scheduling．タイムスライスごとに先行ジョブと高優先ジョブを交互に実行
  - **CFS**： Completely Fair Scheduler．Linux標準スケジューラに実行を任せる
- 実験環境
  - 計算ノード構成：理研R-CCS Fujitsu A64FX (50 cores) x 4ノード
  - ソフトウェア：Slurm v23.11.6, Rocky v8.10，Open HPC v3.1
  - ベンチマークプログラム：NPB BT-MZ (NPB3.4-MZ-MPI)

NPB BT-MZ実行結果：スケジューリングポリシの比較



高優先ジョブ(B)の終了時間は
Requeue < Preempt < Gang < CFS

低優先ジョブ(A)の終了時間は
Requeue < Preempt < Gang < CFS

→ Requeue, Preemptが優位
（Gang Schedulingはメリット低）

（CFSはコアバインド等で
740秒程度に短縮可能）

イベント駆動型ワークロードへの対応状況調査 まとめ

NII

- 緊急（高優先度）ジョブを素早く実行するには，Requeue，Preemptのようなスケジューリングポリシが有効
  - **Gang Schedulingはメリット少ない**
  - ただし，**Preempt**では緊急ジョブが必要とする空きメモリがない場合，**緊急ジョブが起動できない**
- 必要とされるスケジューリングポリシ
  - **Requeueポリシ**を採用し，先行（低優先）ジョブは緊急時は停止しても構わない，スポットジョブとして扱うことで，**緊急ジョブの優先実行とメモリの有効活用**ができる
  - 先行ジョブの実行状態を残したい場合は，**チェックポイント（CP）＆リスタート**との組合わせも検討が必要
    - ただし，システム的なCPでは，並列ジョブのCPは難しく，メモリサイズが大きいとCPのオーバヘッドも大きい
    - アプリケーションレベルのチェックポイントの方が有効

概要

- 複数計算資源の連携
  1. 公募要領が求める調査研究項目（資源管理関連）
  2. 欧米の計算基盤の調査
  3. 利用方法検討
  4. 機能検討
  5. 構成検討
  6. まとめ
- 資源スケジューラのイベント駆動型ワークロードへの対応状況調査
- 次世代HPCIのセキュリティの検討

R4年度 セキュリティ評価結果概要

NII

- セキュリティ課題の抽出として，クラウドDCのセキュリティ評価を既存HPCシステムに適用
  - セキュリティ対策の考え方は、従来の**「境界防御」前提の考え方(ISMS)**から、侵入や内部不正を前提として被害を最小限に抑える**「サイバーレジリエンス」**が主流となっている
    - 従来のセキュリティ対策（ISMS）：機密性、完全性、可用性（情報のCIA）を保護するための対策を示す．侵入される前の「特定」、「防御」の対策を重視.
    - サイバーレジリエンス（CSF, Cybersecurity Framework*）：侵入される前の「**特定**」、「**防御**」に加え、侵入されても被害を最小限に抑えるため、「**検知**」、「**対応**」、「**復旧**」を強化
      - *https://www.nist.gov/cyberframework/framework
  - 従来のHPCシステムは性能を重視，隔離環境を前提にしてきたため，クラウドDCレベルのセキュリティ対策はなされていない
  - 次世代HPCIのセキュリティでは，レジリエンスを考慮した対策強化が必須であることが判明

共通してプロファイル値が低い傾向．HPCでは性能を最大化するように設計され，
セキュリティはその妨げにならないことを前提に運用されているためと考えられる

結果1

結果2

赤は特に対策が必要とされている項目

投影のみ

クラウドDCセキュリティ評価用CSF分析シート

NII

「CSF分析シート」でプロファイルや対象HPCのセキュリティ上の課題を特定する

CSFの機能・カテゴリ・サブカテゴリ（CSF コア*から抜粋）

要件の解釈・チェック項目

事前分析とアセスメント結果

CSF分析シート（システム名：　　）

機能	カテゴリー	サブカテゴリー	要件の解釈	チェック項目	チェック結果	プロファイル（AsIs）	プロファイル値（AsIs）	G列の判断理由	参照した情報
識別（ID）	資産管理（ID.AM）：目組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と目組織のリスク戦略における相対的な重要性に応じて管理されている。	ID.AM-1: 目組織内の物理デバイスとシステムが、目録作成されている。					#N/A		
識別（ID）		ID.AM-2: 目組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。							
識別（ID）		ID.AM-3: 組織内の通信とデータフロー図が、作成されている。							
識別（ID）		ID.AM-4: 外部情報システムが、カタログ作成されている。							
識別（ID）		ID.AM-5: リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。							
識別（ID）		ID.AM-6: 全労働力と利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。					#N/A		

アセスメント業者が定義

※フレームワークのカテゴリ及びサブカテゴリから組織が選択した、ビジネスニーズを基に期待される成果
（「重要インフラのサイバーセキュリティを改善するためのフレームワーク」より抜粋）

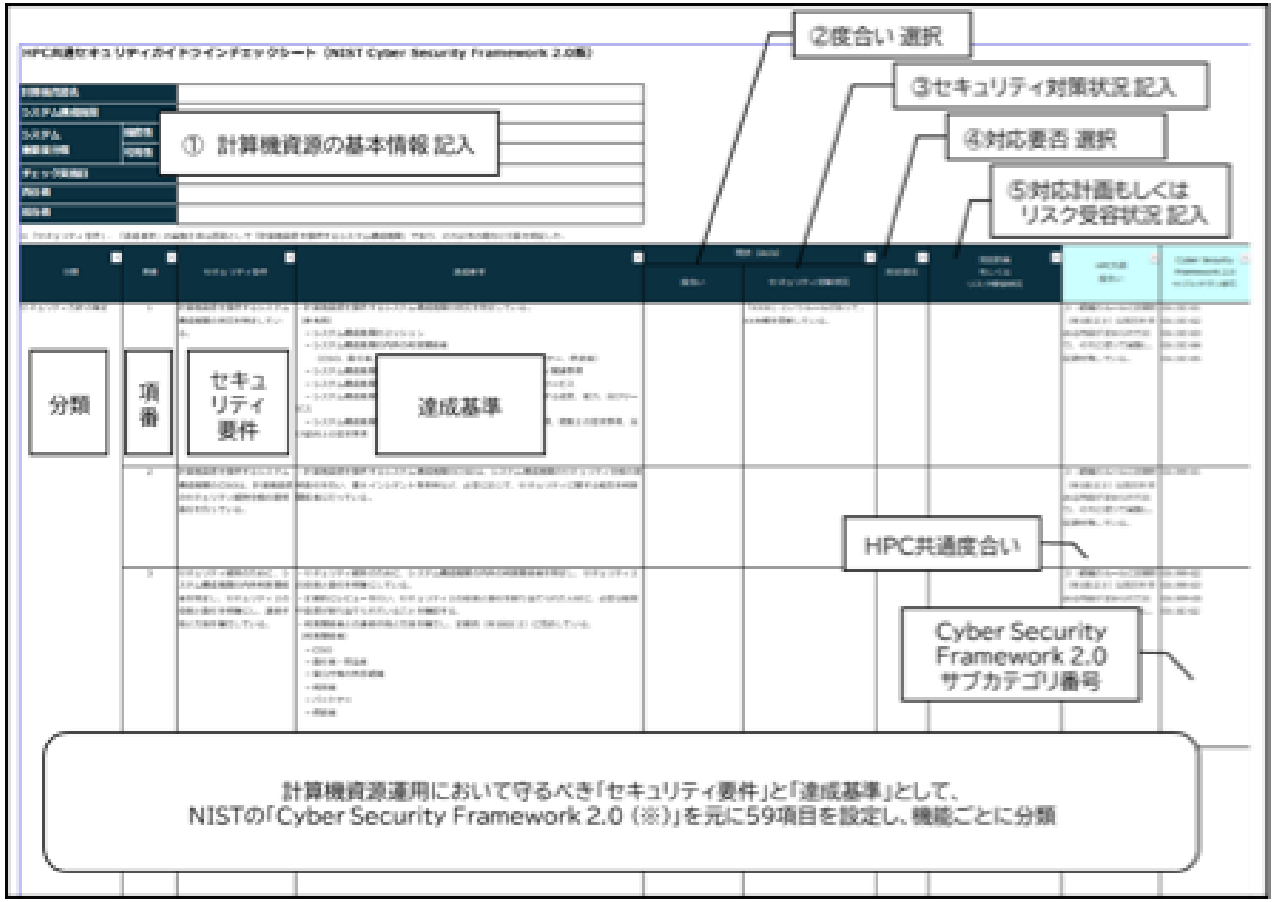
プロファイル	プロファイル値
対象外	N/A
実施を要求していないorルール・手順書がないorルール・手順書を知らない	0
ルール・手順書が存在し、部分的に準拠している。（10%～70%）	1
ルール・手順書が存在し、準拠している。（70%～）	2
ルール・手順書に準拠している。＋ 定期的に見直しを行いルールを更新している	3
ルール・手順書に準拠している。＋ 随時ルールの見直しを行い更新している	4

ルール/手順を規定して実行できているかどうか評価
ルール/手順自体を定義しているものではない

NTT-AT様報告資料より抜粋

HPCシステム用セキュリティガイドラインの作成（1/2）

1. HPCシステム用セキュリティガイドラインのドラフトを作成
   - NIST CSFを基にしたガイドライン
     - NII ストラテジックサイバーレジリエンス研究開発センターの協力
     - 境界防御型から侵入やミスを前提とするゼロトラスト型のセキュリティ
   - R6年2月にCSFが組織間連携を考慮したv2.0に更新されたため，R6年度ガイドラインも更新



HPC共通セキュリティガイドラインチェックシート

HPCシステム用セキュリティガイドラインの作成 (2/2)

2. CSF2.0対応ガイドラインドラフトについて，10の学術機関から意見を収集、反映
   - 機関によりセキュリティ基準や対策状況が異なる
     ISMS，NIIセキュリティポリシーサンプル規定集，他
   - ほぼ全ての機関でチェックシート，セキュリティ対策を実施するリソースが不足している

3. 「HPC 共通セキュリティガイドライン」策定
   - **ガイドラインドキュメント**と**チェックシート**で構成
   - チェックシートは「CSF分析シート」を**HPC向けに解釈**し，チェック項目を定義したもの
   - 現状のHPCの脅威のシナリオを作成し，CSFのどのカテゴリを強化すべきか検討した

「HPC 共通セキュリティガイドライン」

目次

次世代HPCIのセキュリティの検討 まとめ

- 「HPC 共通セキュリティガイドライン」策定
  - CSF2.0に基づくセキュリティガイドラインの作成
  - さらなるブラッシュアップが必要（ISMSとの比較等）
  - ほぼ全ての機関で，セキュリティ対策を実施するリソース不足が課題
  - 次世代HPCIでは，今後共通の**セキュリティポリシ**の策定も必要

- その他，ソフトウェアの安全性も必要
  - GitHub，Spackのようなautomatic checkの仕組み
    - SBOM：Software Bill of Materials, 使用したコンポーネント等のリストを一覧化
  - セキュリティ・プライバシに配慮したストレージ
  - TEE (Trust Execution Environment)によるセキュアな計算環境

まとめ

- 複数計算資源の連携（一体的運用計算基盤）
- 資源スケジューラのイベント駆動型ワークロードへの対応状況調査
- 次世代HPCIのセキュリティの検討

謝辞　以下のシステム構成機関の皆様にはヒアリングに際して多大なご協力を賜り誠にありがとうございました　(ヒアリング順(敬称略）)

東京科学大学　　理化学研究所　　産業技術総合研究所
名古屋大学　　京都大学　　大阪大学　　東北大学
東京大学　　北海道大学　　九州大学