別添資料１

「ＨＰＣＩの基本仕様に関する調査検討」

２２年度　委託業務研究成果報告書

平成２３年３月

国立大学法人東京大学情報基盤センター　　センター長　　石川　裕

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
学術基盤推進部　　部長　　安達　淳

本報告書は、文部科学省の科学技術試験研究委託事業による委託業務として、国立大学法人東京大学及び大学共同利用機関法人情報・システム研究機構が実施した、平成２２年度の「ＨＰＣＩの基本仕様に関する調査検討」の成果を取りまとめたものです。

（添付資料 1）

HPCI 基本仕様

― ストレージ資源利用のための基本仕様 ―

目次

1　概要

本基本仕様書は、ストレージ資源利用のための基本仕様である。本仕様策定に当たっては、「準備段階におけるコンソーシアム」での検討を踏まえ、HPCI の整備に必要な機能を明確にし、HPCI の基礎的な仕様をまとめたものである。開発項目は、2011 年 3 月時点で詳細仕様が決められるもののみとし、詳細仕様が作れない開発項目は研究開発項目としている。本基本仕様書は、ストレージ共有について基本仕様を定めている。

・ストレージ共有

平成 22 年度最先端研究基盤事業「e-サイエンス実現のためのシステム統合・連携ソフトウェアの高度利用促進」により東京大学情報基盤センターおよび理化学研究所計算科学研究機構に設置される大規模ストレージ、さらに今後各資源提供機関から提供されるストレージあるいはポータルシステムや各ユーザコミュニティとの連携に必要とされるストレージの共有方法の調査検討、およびそれに伴うソフトウェアの整備など、ストレージ共有に関する基本仕様を検討した。また、共有ストレージの運用に向けての整備計画、運用体制ならびに運用経費について検討した。

本仕様書は、スーパーコンピュータ施設を有し共同利用・共同研究拠点として活動している東京大学および SINET を運営している国立情報学研究所が主幹し、共同利用・共同研究拠点である北海道大学、東北大学、東京工業大学、名古屋大学、京都大学、大阪大学、九州大学、筑波大学、および京速コンピュータ「京」運用機関である理化学研究所計算科学研究機構と連携して、HPCI 構築に関する基本仕様について調査検討した結果に基づいて作成されている。

2　ストレージ共有の利用シナリオ

東京大学情報基盤センターおよび理化学研究所計算科学研究機構に設置される大規模ストレージ、各資源提供機関から提供されるストレージ、ポータルシステムやユーザコミュニティとの連携に必要とされるストレージなど、HPCI に供出される予定のストレージはネットワーク的に広域に分散して設置される。これらのストレージ群は広域分散ファイルシステム Gfarm により単一のファイルシステムのように束ねられ、複数の拠点から複数の研究者がシームレスにデータを共有して利用するストレージ基盤としてサービス提供を行う。

ストレージ共有の利用シナリオは平成 23 年度中に整備することが可能な機能を基本仕様とし、平成 23 年度に改めて詳細検討を行う機能は拡張仕様とした。各々の利用シナリオは、ユーザ視点、管理者視点、資源提供視点、事務局視点、共通視点に分け、本章で説明する。

ストレージ共有の基本仕様は 3 章に、資源提供機関のストレージ仕様は 4 章に説明する。

2.1 共有ストレージの目的

[ユーザ視点（管理者視点）]

HPCI で整備する共有ストレージ（以下、「HPC ストレージ」）は、HPCI の各資源提供機関に属する国内の研究者間、研究グループ内で効率よくデータ共有することで、研究業務の効率化や利便性の向上、ストレージ資源の有効利用を図ることを目的とする。共有ストレージ基盤は持続的なシステム増強が図られることを念頭に、提供するサービスの目標は以下とする。

- HPCI 上のどの拠点からでも利用可能な大容量ストレージ基盤の提供
- HPCI 上のスパコン間での効率的なファイル共有機能の提供
- 常に安定して稼働するための高い RAS 性を備えた共有ファイルシステムの提供

（高信頼、高可用、常時安定して稼働する共有ストレージの提供）

2.2 HPC ストレージの位置づけ

[ユーザ視点]

HPC ストレージは拠点スパコンのローカルストレージとは用途の異なるファイルシステムと位置付ける。一般的に拠点スパコンのローカルストレージは、ジョブ一時領域としての超高速/小容量のローカルファイルシステム（第一階層）と、データ保存領域としての高速/大容量のグローバルファイルシステム（第二階層）に分かれる。サービス提供する HPC ストレージはグローバルファイルシステムの更に下位層にある、拠点スパコン間のデータ共有領域の位置づけ（第三階層）とする。HPC ストレージの位置づけ（ファイル階層、ファイル特性）を図 2-1 に示す。

[管理者視点]

複数拠点に跨る HPC ストレージの利用において、利用者や利用形態によってもデータフロ

ー(データの生成、解析、格納、共有方法)は異なるが、Gfarm ファイルシステムの特性や利点が活きるのは拠点スパコンからデータ共有用途でアクセスされるケースであると考える。そのため、共有の仕組みや信頼性の確保、セキュリティ面での考慮は特に重要となる。また、多数の利用者が利用することから、公平な容量制限や容易な利用(アクセス方法)の整備も求められるが、HPC ストレージに格納されるファイルの種類には特に制限を設けず、コミュニティ(グループ)単位にファイル容量制限を行うことが望ましいと考える。

平成 23 年度に提供する HPC ストレージは東西拠点に設置される大規模ストレージを中心に整備を行うものとする。

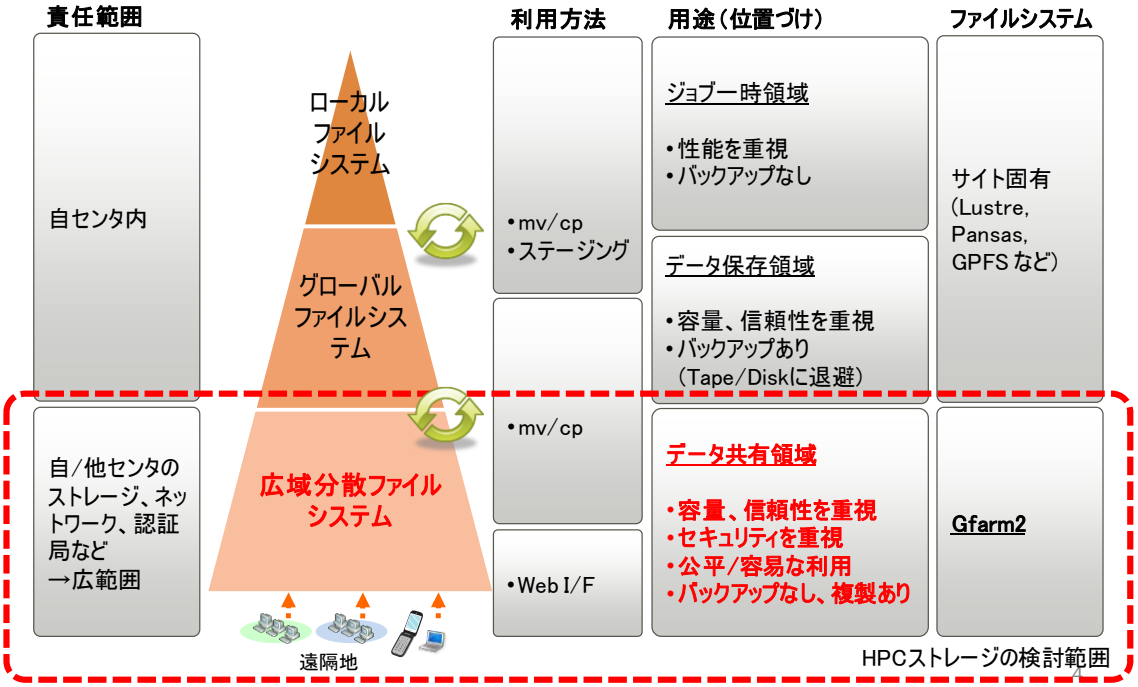


図 2-1 HPC ストレージの位置づけ

2.3 HPC ストレージの運用イメージ

[ユーザ視点]

HPC ストレージで利用する Gfarm ファイルシステムは、分散共有ファイルシステムとして以下の特長を有する。

- 複数の物理ノード(ストレージ)を単一のファイルシステムに束ねて運用できる。
- 複数のクライアントから同一ファイルシステムビューでアクセスできる。

[管理者視点]

HPC ストレージは東京大学情報基盤センターおよび理化学研究所計算科学研究機構に設置される大規模ストレージを中心に、各資源提供機関から提供されるストレージ群を Gfarm で単一のファイルシステムのように束ね、運用を行う。

（注記）

以降には全てのストレージ群を 1 組のメタデータサーバで束ね、HPC ストレージを単一のファイルシステムとして運用することを想定しているが、この集中管理運用について、各運用機関、資源提供機関の合意には至っていない。これまでに検討したメタデータの管理方法の違いによる問題点、影響を表 2-6 に示す。

具体的なメタデータの管理方法は平成 23 年度の検討継続課題とする。なお、シンボリックリンク設定などにより、ユーザビューとしては単一のファイルシステムのように見せて運用することが可能であることは検討をしている。

ユーザは各々の物理ノード（ストレージ）を意識する必要はなく、複数の拠点からシームレスにデータ共有できる。この際のデータアクセスは、物理的にも複数のストレージに分散してアクセスされる。HPC ストレージの運用イメージを図 2-2 に示す。

なお、単一のファイルシステムとして運用するためには、メタデータ（ファイルシステムのメタ情報）を管理するメタデータサーバは 1 組で運用することとなる。メタデータサーバを独立して運用する場合、メタデータサーバを追加設置することになるが、これは実質的に HPC ストレージを分割することを意味する。

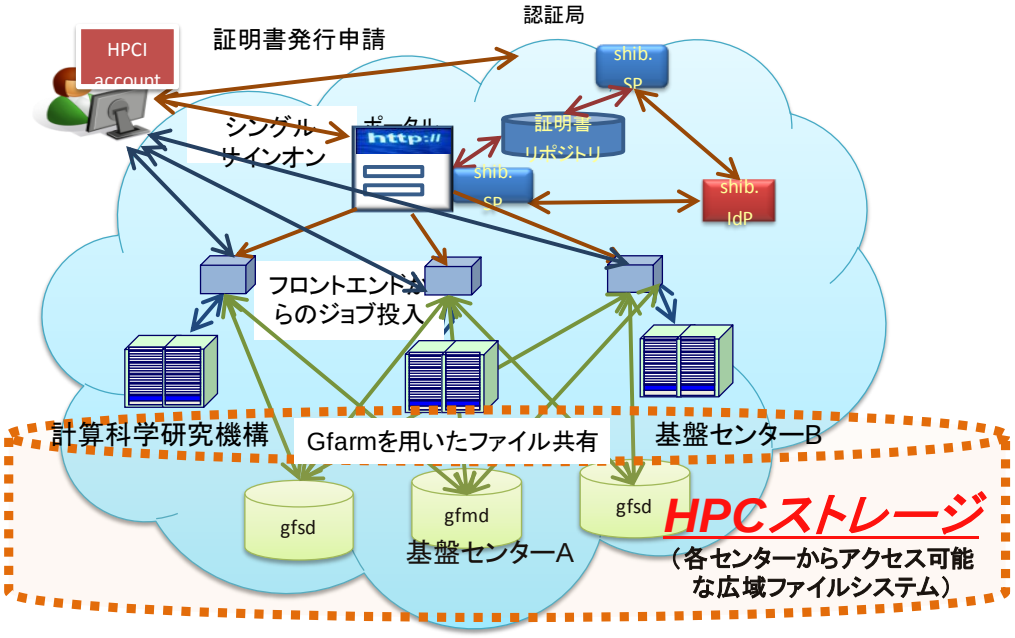


図 2-2 HPC ストレージの運用イメージ

2.4 利用シナリオ概要

HPC ストレージを利用する上で、各資源提供機関の既存システムにおいても最低限の環境変更や HPC ストレージの運用に則った運用ポリシーの見直しが必要となる。ただし、それによって HPC ストレージの利用が阻害されることのないよう、既存システムへの影響は最小限とする利用シナリオを検討する。

HPC ストレージを利用する上で拠点内に HPC ストレージ資源を設置し、1 組のメタデータサーバで管理することで、自動的にファイル複製が作成され、拠点内のローカルストレージと同等性能でファイルアクセスが行える。すなわち、拠点内に HPC ストレージ資源を設置することで HPC ストレージのメリットを最大限に享受できるが、試行的に利用したいケースも想定し、自拠点にストレージ資源を配備しなくても利用可能なシナリオ（クライアント利用）についても検討する。

2.4.1 ユーザ視点での利用シナリオ概要

ユーザ視点で HPC ストレージの利用シナリオをまとめたものを表 2-1 に示す。HPC ストレージのユーザ視点での利用シナリオとして 4 つのシナリオを検討した。シナリオ 1～3 はファイル共有の目的の異なる利用シナリオと言えるが、アクセス方法は共通である。

シナリオ 1「データ共有」は限られた研究グループ内に閉じたファイル共有のシナリオである。どの拠点のログインノードからでもユーザ自身で HPC ストレージをマウントし、名前空間も同じパス名でファイルアクセスすることを想定する。このファイルアクセスは、ローカルアカウント権限ではなく、HPCI アカウント権限で行われるため、どの拠点のログインノードから異なるローカルアカウント/グループでログインした場合でも、HPCI アカウントで一意にアクセスできる。ここでの限られた研究グループとは HPCI 課題グループを指す。HPCI 資源の利用はプロジェクト課題毎に資源利用が認可されるが、HPC ストレージもこの課題グループのグループメンバシップによりユーザ（HPCI アカウント）の管理を行う。ファイル共有、複製に関して、ユーザで意識する必要はなく、ファイルシステムレベルで最適なファイル複製、配置が行われる（ユーザにより近いストレージにファイル複製が作成されることで、ローカルストレージと変わらないファイルアクセスが可能となる）。

シナリオ 2「データアーカイブ」は広く一般的なファイル共有のシナリオである。従来の Anonymous FTP に代わるものとし、長期的に蓄積されるデータのストアを想定する。扱うデータの種類も利用人数も他のシナリオとは異なる。多拠点から利用される価値の高いデータであれば、全ての拠点にファイル複製が置かれるべきと言えるが、アクセス方法や共有方法について、他のシナリオとの違いはない。

シナリオ 3「セキュアストレージ」は機密性の高いデータのファイル共有のシナリオである。基本仕様では GSI によるユーザ認証、ACL によるユーザ/グループ単位のより細かなアクセス制限（ACL）、ユーザレベルでのファイル暗号化によるデータストアを想定する。

シナリオ 4「ファイルカタログ」は計算ノードから HPC ストレージ上のファイルカタログ（ファイル所在情報）を参照するシナリオである。計算ノードから HPC ストレージ上のファイルそのものにアクセスする機能を提供する訳ではないが、バッチジョブから HPC ストレージへファイルステージングしたいなどの利用シナリオと併せて検討を行う。

上記で説明した利用シナリオのうち、以下の具体的な実現方法は実装を含め未検討であるため、拡張仕様として平成 23 年度の検討継続課題とする。

- ユーザ PC の Web ブラウザからファイルアクセスする。
- ユーザ PC から WebDAV/CIFS プロトコルにより、ファイルアクセスする。
- ログインノードでメタ情報をブリッジするような機能を提供する。

表 2-1 ユーザ視点でのストレージ利用シナリオ概要

No.	利用シナリオ	アクセス方法	認証方法	ファイル共有、 複製方法
1	[データ共有] スパコンで解析された実行結果ファイルのデータ共有保管庫として利用する。（限られた研究グループ内でのファイル共有）	・ 拠点スパコンのログインノードに FUSE でマウントして、アクセスする。 ・ ユーザ PC の Web ブラウザからファイルアクセスする。[拡張仕様] ・ ユーザ PC から、WebDAV/CIFS プロトコルにより、ファイルアクセスする。[拡張仕様]	・ gsi_auth 認証を行う。ユーザ認証は暗号化されるが、データ通信は平文で行われる。（HPC ストレージへのアクセスは HPCI アカウント権限で行われる）	・ ファイルシステムレベルで、自動的に異なるノード/拠点にファイル複製が作成される。
2	[データアーカイブ] 巨大加速器の実験データ、天文データ、Bio-Mirror のゲノムデータなど、長期的に蓄積されるデータのアーカイブ領域として利用する。（広く一般的なファイル共有、Anonymous FTP の代替）			
3	[セキュアストレージ] 取り扱いの厳しいデータ、機密性の高いデータをコミュニティ内で安全にファイル共有する。		・ GSI 認証を行う。（ユーザ認証もデータ通信も暗号化される。）	・ ACL により、特定ユーザ/グループ単位にファイルアクセス設定を行う。 ・ ユーザ自身でファイルを暗号化してストアする。（付録 3.参照）
4	[ファイルカタログ] ファイル実体ではなく、ファイル所在を示すカタログ情報を共有する。（計算ノードからのメタデータ参照）	・ ログインノードでメタ情報をブリッジするような機能が必要だが、具体的な実現方法は実装を含め、未検討。[拡張仕様]		

※平成 23 年度以降に検討する利用シナリオ（拡張仕様）は下線で示す部分である。

2.4.2 管理者視点での利用シナリオ概要

管理者視点での HPC ストレージの利用シナリオについて、それぞれの管理者の役割や作業範囲を定義の上、管理作業シナリオを説明する。

(1) 管理者の位置づけ

HPC ストレージの管理者は、拠点管理者(メタデータ管理者、ストレージ提供機関、クライアント提供機関)とする。拠点管理者のそれぞれは HPC ストレージの運用方法やメタデータ管理ポリシーの違いにより、管理すべき資源の対象も異なり、管理作業シナリオも変わる。運用パターン毎の HPC ストレージ管理者の管理資源の違いを表 2-2 に示す。

運用パターン 1～3 は一拠点のメタデータサーバを共同利用する方法である。

運用パターン 1 では拠点内にメタデータサーバ/ストレージ/クライアントを設置、運用パターン 2 では拠点内にストレージ/クライアントを設置、運用パターン 3 では拠点内にクライアントのみを設置する方法である。各々、自拠点に設置されたストレージ資源の管理作業が必要であり、他拠点の資源については他拠点の管理者に管理を委ねることになる。

運用パターン 4 はメタデータを独立して運用する方法である。

運用パターン 1 と同様、拠点内にメタデータサーバ/ストレージ/クライアントが設置されるため、これらのストレージ資源の管理作業が必要となる。また、他の運用パターンと異なり、ファイルシステム空間は独立した運用となるため、他拠点との相互接続性を保証するにはシンボリックリンク設定など、個別の管理が必要となる。これは実質的に HPC ストレージを分割することを意味し、ファイルシステムの管理負担も増えることから、本運用パターンの利用は推奨しない(もしくは慎重に行う必要があると考える)。

表 2-2 ストレージ管理者の管理資源

ストレージ運用による分類		運用パターン 1	運用パターン 2	運用パターン 3	運用パターン 4
メタデータ管理ポリシー		共同利用 (一拠点でメタデータを集中管理)			独立 (拠点内で管理)
HPC ストレージの運用方法		クライアント利用 (メタ+ストレージあり)	クライアント利用 (ストレージあり)	クライアント利用 (ストレージなし)	独自利用
管理資源	メタデータサーバ	○自拠点で管理	他拠点に管理移譲	他拠点に管理移譲	○自拠点で管理
	ストレージ	○自拠点で管理	○自拠点で管理	他拠点に管理移譲	○自拠点で管理
	クライアント	○自拠点で管理	○自拠点で管理	○自拠点で管理	○自拠点で管理

※平成 23 年度の基本シナリオでは主に運用パターン 1～3 の利用を想定する。

(2) 管理作業シナリオ概要

管理者視点でHPCストレージの管理作業シナリオ概要をまとめたものを表2-3に示す。管理作業シナリオは以下8つに分類し、拠点管理者(メタデータ管理者、ストレージ提供機関、クライアント提供機関)に対応する管理作業として定義を行う。

管理作業シナリオ1: 初期設定
管理作業シナリオ2: ファイアウォールの設定変更
管理作業シナリオ3: ユーザ/グループ管理
管理作業シナリオ4: ファイルシステム管理
管理作業シナリオ5: ハードウェア管理
管理作業シナリオ6: 運用管理
管理作業シナリオ7: 運用監視
管理作業シナリオ8: 障害時対応

ユーザ視点での利用シナリオ(データ共有、データアーカイブ、セキュアストレージ、ファイルカタログ)に対する管理作業内容に大きな違いはないと考えられることから、日常的に想定される管理作業について、各管理者の立場での管理作業シナリオを定義した。

なお、定義した管理作業シナリオのうち、以下の具体的な実現方法は実装を含め未検討であるため、拡張仕様として平成23年度の検討継続課題とする。

- メタデータ、スプールディレクトリのバックアップ(バックアップ頻度、バックアップ方法、外部バックアップ先の決定)
- 利用統計情報のレポーティング
- HPCストレージの稼働確認、稼働監視、性能監視(ツール整備)

表 2-3 管理者視点でのストレージ管理作業シナリオ概要

No.	管理作業シナリオ	拠点管理者		
		メタデータ管理者	ストレージ提供機関	クライアント提供機関
1	初期設定 (拠点追加時)	・ ハード現調、OS、Gfarm、関連ソフトウェアのインストール ・ メタデータサーバの初期設定 ・ 管理者権限、root 権限のユーザ登録 ・ ファイルシステムノードのホスト登録	・ ハード現調、OS、Gfarm、関連ソフトウェアのインストール ・ ファイルシステムノードの初期設定	・ Gfarm、関連ソフトウェアのインストール ・ クライアントの初期設定
2	ファイアウォールの設定変更	・ TCP ポートのインバウンド許可設定	・ TCP ポートのインバウンド, アウトバウンド許可、UDP ポートのインバウンド許可設定	・ TCP ポートのアウトバウンド許可、UDP ポートのアウトバウンド許可設定
3	ユーザ/グループ管理	・ アカウントの登録、変更(grid-mapfile の編集) ・ ユーザ/グループディレクトリの作成、変更 ・ パーミッション、拡張 ACL の設定、変更	・ アカウントの登録、変更(grid-mapfile の編集)	-
4	ファイルシステム管理	・ クォータ設定 ・ グループディレクトリに対するシンボリックリンク設定(メタデータの分散管理時には必要) ・ 利用失効ユーザのアクセス権変更(書き込み禁止)、一定期間経過後のファイル強制削除(要検討)	-	-
5	ハードウェア管理	・ メタデータサーバノードの起動、停止	・ ファイルシステムノードの起動、停止	・ クライアントノードの起動、停止

No.	管理作業シナリオ	拠点管理者		
		メタデータ管理者	ストレージ提供機関	クライアント提供機関
6	運用管理	・ メタデータのバックアップ、リストア[拡張仕様] ・ ログファイルの退避 ・ 利用統計情報のレポーティング[拡張仕様]	・ スプールディレクトリのバックアップ[拡張仕様] ・ ログファイルの退避	・ ログファイルの退避
7	運用監視	・ メタデータサーバノードの稼働確認、監視	・ ファイルシステムノードの稼働確認、監視	・ HPC ストレージの稼働確認、稼働監視、性能監視[拡張仕様]
8	障害時対応	・ HPC ストレージ、メタデータサーバノードの障害切り分け、復旧対応	・ ファイルシステムノードの障害切り分け、復旧対応	・ クライアントノードの障害切り分け、復旧対応

※平成 23 年度以降に提供する機能(拡張仕様)は下線で示す部分である。

2.5 ユースケース

以下 5 つのユースケースより扱うデータの種類(機密性/秘匿性、データ価値、ファイルサイズ/ファイル数など)を抽出し、具体的な HPC ストレージの利用用途やユーザニーズ、利用シナリオの妥当性検討を行った。

1) 格子 QCD(アンサンブルデータ)

次世代スーパーコンピュータ戦略プログラムである格子 QCD において、様々の解析に用いられるアンサンブルデータはデータ生成に膨大な計算機資源が必要とされ、非常に貴重なデータとされる。データサイズは 100TB 規模の大きさで、複数の研究機関の研究者がデータを共有して解析を進めたいニーズが挙げられている。

格子 QCD における共有データフローを図 2-3 に示す。

格子 QCD では京コンピュータや拠点スパコンで長時間実行して得られたゲージ配位アンサンブルデータを HPC ストレージに格納する。全ての QCD 計算はゲージ配位アンサンブルデータを入力に行われるが、研究者が各々の興味で自由に生成するにはかなりの計算資源を要するため、研究者間で合意の元で決定されたパラメタで一通りを生成し、共有されるべきデータとされる。

HPC ストレージに格納した配位データは複数拠点にデータ複製され、冗長性が確保される。配位データはそれぞれの拠点スパコンのローカルストレージにコピーされ、解析が進められる。

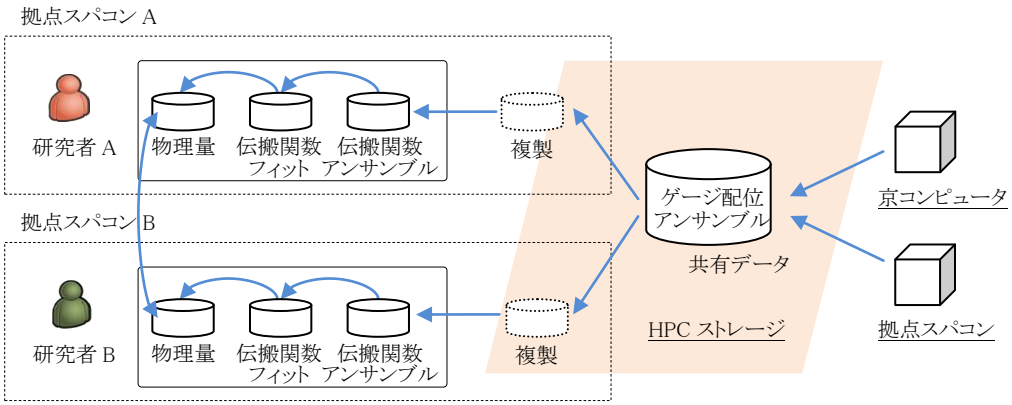


図 2-3 格子 QCD における共有データフロー

2) ライフサイエンス(シークエンスデータ)

ゲノムシークエンスデータは数 TB 規模の大きさが想定される。また、Bio-Mirror.net のような DNA データバンクを利用するニーズもある。また、一時的に特定ユーザにのみデータアクセスを許可したい、許可したユーザからのファイルアクセスがあったことを監査したいなど、セキュリティの固有ニーズが挙げられている。

ライフサイエンスにおける共有データフローの一例を図 2-4 に示す。

ライフサイエンスのシークエンスデータをそれぞれの拠点スパコンのローカルストレージにコピーした上で解析が進められる。扱うデータは DNA データバンクのような共有データもあれば、取り扱いが厳しく、公開範囲が限定されるデータも含まれる。ライフサイエンスの種類によってはアセンブリング後のデータを共有するニーズもある。

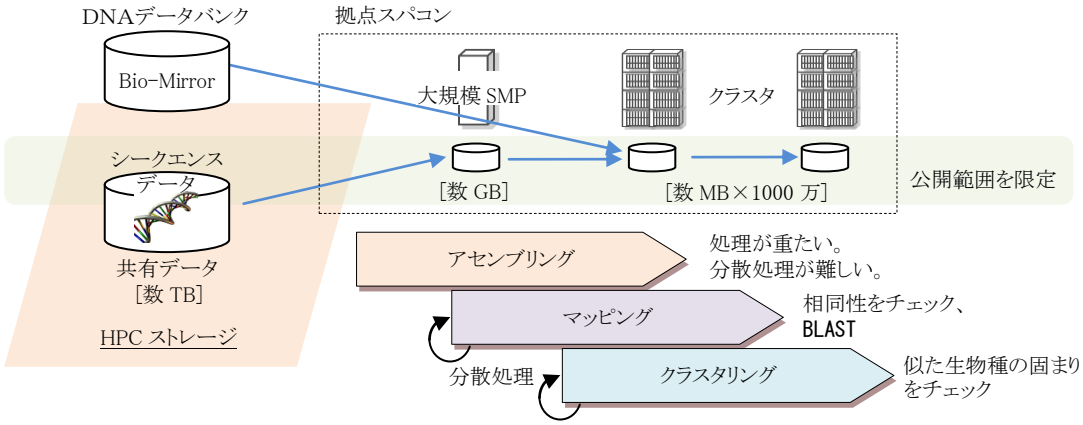


図 2-4 ライフサイエンスにおける共有データフローの一例

3) スパコンでのシミュレーション解析（大規模解析データ、実験データ）

大規模シミュレーションの解析結果のデータ保管庫としの利用ニーズがある。データサイズは 1PB 規模の大きさが想定される。ログインノードだけではなく、計算ノードからもファイルアクセスしたい、どの拠点からでも同じパス名でアクセスしたいなどのニーズが挙げられている。

ログインノードでメタ情報をブリッジするような機能の提供については、拡張仕様として検討する。

4) セキュアストレージ（医学・製薬系コミュニティの個人データ）

データの取り扱いに特に厳しいポリシーを持つ"コミュニティ"において、利用者自身で段階的にアクセスコントロールする仕組みを設けることにより、安全かつ容易に利用可能なセキュアストレージの利用ニーズが挙げられている。

ユーザ自身でファイルを暗号化してストアする方法について、付録にファイルの暗号化方法をまとめる。より強度なセキュリティ対策として、データ通信も暗号化する GSI 認証のサポートを行う。

5) 拠点外からのデータアクセス

スパコンのログインノードからだけではなく、CIFS/WebDAV などで PC からも容易にデータアクセスしたいニーズが挙げられている。これらアクセス方法の拡充については、拡張仕様として検討する。

2.6 平成 23 年度の利用シナリオ

平成23年度のHPCストレージの利用シナリオの前提条件を、運用実績があり、新規開発を必要としないものとする。平成 23 年度に先行して整備する HPC ストレージの利用シナリオについて、ユーザ視点、管理者視点、資源提供視点、事務局視点、共通視点の観点で以下に説明する。

2.6.1 ユーザ視点での利用シナリオ

平成 23 年度のユーザ利用シナリオを以下に説明する。

いずれのシナリオも HPC ストレージへのアクセス方法やユーザ認証方法は共通であるため、共通の利用シナリオとして説明する。

- データ共有　　（限られた研究グループ内でのファイル共有）
- データアーカイブ　　（広く一般的なファイル共有、Anonymous FTP の代替）
- セキュアストレージ　　（機密性の高いデータのファイル共有）

なお、利用開始までの流れとして、HPCI アカウントやユーザ証明書の取得が必要であるが、これらの申請方法についての説明は割愛する。

(1)　ローカルアカウントとストレージアカウントの関係

HPC ストレージの利用者は、HPC ストレージの利用に先立ち、HPCI 事務局に対して利用申請を行う。課題審査や本人確認に問題ない場合、HPCI 事務局から HPCI アカウントが発行される。

HPC ストレージへのアクセスはログインノードのローカルアカウント権限ではなく、HPCI アカウント権限で行う。拠点のログインノードから HPC ストレージにアクセスする場合、同一ユーザであっても拠点毎にユーザ名が同じとは限らないが、Gfarm ファイルシステムでグローバルなユーザ、グループ名を管理することで、各拠点から HPC ストレージ上のファイルにこのグローバルユーザ名で一意にアクセスする。

ローカルアカウントと HPCI アカウントの関係を図 2-5 に示す。ユーザ A、ユーザ B は各々のアカウント権限でローカルファイルにアクセスするが、HPC ストレージに対しては共通のグローバルアカウント(HPCI アカウント C)でファイルにアクセスする。

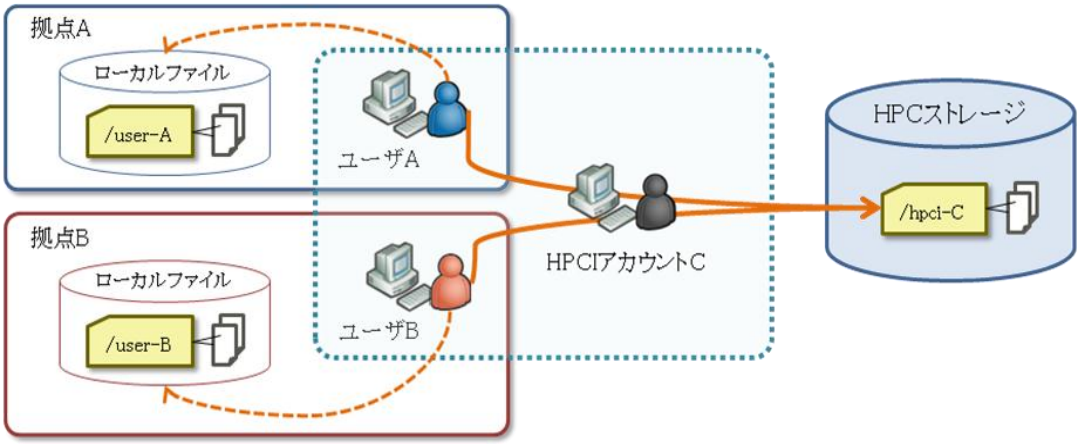


図 2-5 ローカルアカウントと HPCI アカウントの関係

(2)　認証方法

HPC ストレージを利用するには、HPCI アカウントでユーザ認証が必要である。HPC ストレージ(Gfarm ファイルシステム)のユーザ認証方式は、sharedsecret 認証、GSI(Grid Security Infrastructure)を用いた gsi_auth 手法、gsi 認証の 3 種類をサポートしている。

HPC ストレージでは特に性能を重視することから、gsi_auth 手法によるユーザ認証を基本とする。gsi_auth 手法はユーザ認証時に GSI 認証を用い、その後のデータ通信はデータに対する署名や暗号化保護のない生データの転送を行うため、セキュリティ的に強固とは言えない半面、高速なデータ転送が可能である。

gsi_auth 手法によるユーザ認証イメージを図 2-6 に示す。

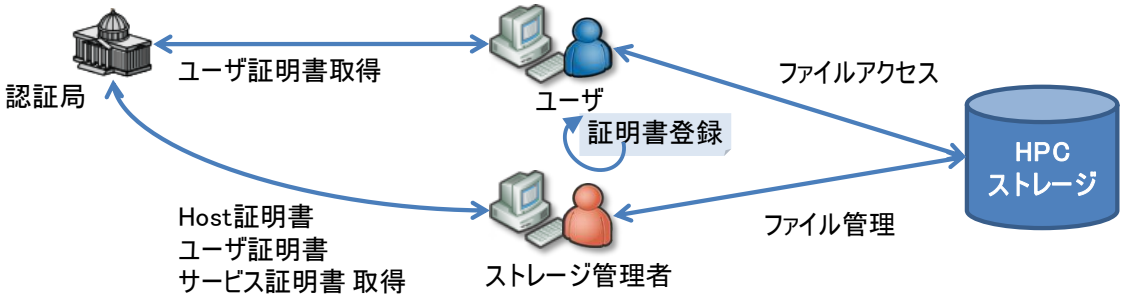


図 2-6 gsi_auth 手法によるユーザ認証イメージ

なお、セキュアストレージの目的であれば GSI 認証を利用することを推奨する。GSI 認証により、ユーザ認証もデータ通信時にも暗号化通信が可能となる。どちらの認証を行うかはクライアントノード単位の設定となるが、セキュアストレージを利用したい利用者は自身のホームディレクトリに Gfarm 設定ファイル(~/.gfarm2rc)を作成することで、ユーザ個々に認証方法を切り替え、利用することが可能である。

(3) HPC ストレージへのアクセス方法

HPC ストレージへのアクセス方法を図 2-7 に示す。

HPC ストレージはまずはログインノードからの利用を前提とする。HPC ストレージにアクセスしたい HPCI 上のスパコンのログインノードにログインし、HPC ストレージをマウントすることで、ローカルストレージと同様に透過的にファイルアクセスを行う。または、Gfarm が提供するコマンドを利用し、ファイルアクセスを行う。

何れの方法もログインノードからのアクセスであり、計算ノードから HPC ストレージに直接アクセスはしない。HPC ストレージのマウントはユーザ自身で gfarm2fs コマンドを実行することでマウントされる。このマウント操作はユーザ権限で行われ、システム側で予め静的にマウントしておくことはできないが、一度マウントすれば、ユーザ PC からもログインノードを介し、HPC ストレージにデータ転送できる。

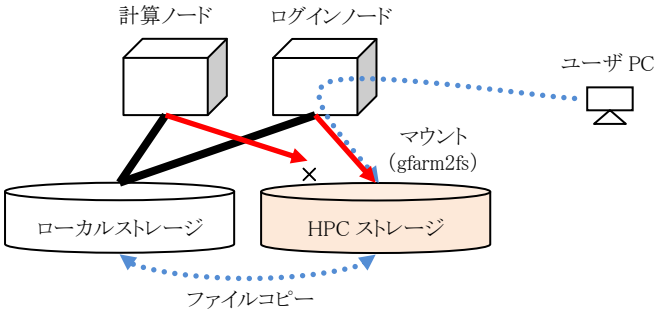


図 2-7HPC ストレージへのアクセス方法

(4) ファイル容量制限

HPC ストレージはユーザ/グループ単位にファイル数、ファイルサイズを制限することが可能である。ファイル容量制限等を行う場合、この制限値は HPCI 利用申請時にユーザが申告するものとし、申告どおりの制限容量で利用できるかも含め、利用審査されることが望ましいと考えるが、具体的な申請フローについては今後の検討課題とする。

(5) ファイル共有、データアーカイブ、ファイル複製方法

HPC ストレージ(Gfarm ファイルシステム)は複数ストレージを束ねた分散ファイルシステムであるため、HPC ストレージ上に置かれたファイルは HPCI 上のどのログインノードからでもファイル共有できる。実際には、どこかのファイルシステムノードにファイル複製が作成、格納されるが、ユーザ(アプリケーション)では格納場所を意識することなく、ファイル共有が可能となっている。

データアーカイブの一例として FTP によるファイル同期が考えられる。例えば Bio-Mirror などの Anonymous FTP の特定ディレクトリにあるファイルを HPC ストレージに lftp により同期(ミラー)することで、HPCI 上のスパコンからアーカイブされたデータに効率良くアクセスできる。

ファイル複製は拠点内の HPC ストレージ(自拠点のファイルシステムノード)が優先的に利用されるため、ユーザは意識することなく、最適な(高速な)ファイルアクセスが行えるが、どこにファイル複製が作成されるのか、ファイル複製の基本ルール(ロジック)はユーザでも認識すべき事項のため、以下に補足する。

- 新規ファイルを作成する場合、自拠点のファイルシステムノードに十分な空きがあれば書き込む。十分な空きがないと判断された場合、よりネットワーク的にアクセス元に近く、負荷の低いファイルシステムノードに書き込む(自拠点にファイルシステムノードが設置されていない場合も同様)。
- 既存ファイルへアクセスする場合、ファイル複製があれば自拠点のファイルシステムノードへアクセスする(アクセス元により近い)。近くのファイルシステムノードにファイル複製がない場合、ファイル複製を持つ、よりネットワーク的にアクセス元に近く、負荷の低いファイルシステムノードへアクセスする。

ファイル複製に関して、ユーザ自身でファイル複製を操作することも可能である。任意ファイルの複製を、指定されたホスト群に、指定された複製の数だけ、作成することができる。また、このファイル複製はファイル容量制値以下になるように制限も働く。それ以外に、ファイル複製数、どのファイルシステムノードに複製が存在するかなどを確認するコマンドも利用できる。

(6) アクセス制限

セキュアストレージなどの機密性の高いデータについて、コミュニティ内で安全にファイ

ル共有するためのアクセス制限機能として、アクセス制御リスト（ACL）を利用する。ACL エントリには所有者（owner）、指定ユーザ（named user）、所有グループ（group）、指定グループ（named group）、その他（other）があり、これらを組み合わせたアクセス権（rwx）を設定することで、セキュアストレージとして利用を行う。ACL の設定変更は所有者自身で行うものとする。

更に取り扱いの厳しいデータについては、ユーザ自身でファイルを暗号化して HPC ストレージに格納するものとする。ファイル暗号化の方法は付録にまとめる。ユーザが暗号化したファイルはパスワードや鍵が漏れない限り、管理者であっても復号化することは困難である。

2.6.2 管理者視点での利用シナリオ

平成 23 年度の管理作業シナリオを以下に説明する。

(1) 初期設定

初期設定は HPC ストレージの初期導入時および拠点追加時の管理作業シナリオである。これは HPC ストレージを構成するハードウェアの現調、OS や Gfarm ファイルシステムおよび関連ソフトウェアのインストール作業、メタデータサーバ/ファイルシステムノード/クライアントの Gfarm 初期設定作業を指す。Gfarm の管理者権限、root 権限のユーザ登録、追加されたファイルシステムノードの登録も本作業シナリオで行う。

HPC ストレージ(Gfarm ファイルシステム)の導入にあたり、メタデータサーバ、ファイルシステムノード、クライアントのハードウェア現調、OS、Gfarm、関連ソフトウェアのインスト―ルを行う必要がある。

次に、メタデータサーバ、ファイルシステムノード、クライアントの Gfarm 初期設定を行う必要がある。

次に、メタデータサーバに対し、管理者権限、root 権限を持つユーザ登録を行う必要がある。ここでのユーザ登録とは、Subject DN のユーザ証明書を持つユーザを Gfarm 管理者権限(gfarmadm)、root 権限(gfarmroot)のグループに登録することを指す。各管理者には一人ではなく、複数ユーザを登録することができる。

次に、ファイルシステムノードのホスト登録を行う必要がある。ファイルシステムノードが追加された場合、その都度、メタデータ管理者がメタデータサーバに対して追加されたファイルシステムノードのホスト登録を行う必要がある。

(2) ファイアウォール設定変更

ファイアウォールの設定変更はメタデータサーバ、ストレージ、クライアントが導入(または撤去)された場合に、互いの通信ポートを許可(または禁止)する管理作業シナリオである。将来的に数台のメタデータサーバ、数百台のストレージ、クライアントの相互接続性を許可しなければならない可能性がある。その他、転送バッファサイズなどのパラメタ調整が必要になることも考えられる。ファイアウォール設定変更は、メタデータ管理者および拠点管理者からファイアウォール管理者に必要な設定情報を通知の上、変更を依頼しなければならないと考える。。

HPCI 事務局と管理者、ユーザの関係図、連絡フローを図 2-8 に示す。メタデータ管理者は HPCI 事務局から通知される変更内容を確認の上、メタデータサーバ、ストレージ提供機関、クライアント提供機関で必要となる変更手順を確認し、変更手順を連絡する。一般的に資源提供サイトや機器の増減があった場合、拠点 F/W 管理者に対し、ファイアウォールの設定変更が必要となる。

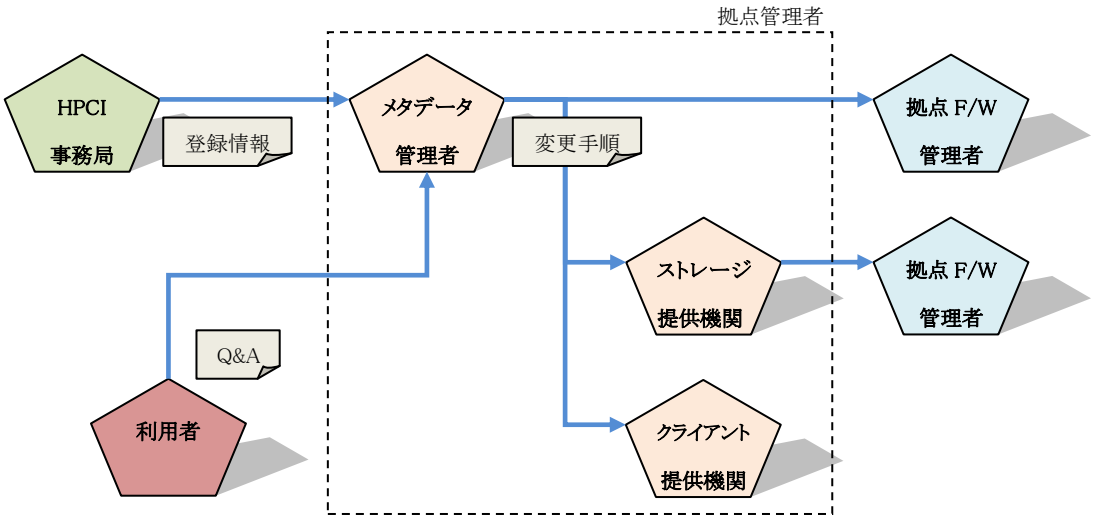


図 2-8 管理者間の関係図、連絡フロー

(3) ユーザ/グループ管理

ユーザ/グループ管理は HPC ストレージへのアカウント登録を行う管理作業シナリオである。本作業に先立ち、登録内容は HPCI 事務局から Gfarm の管理者に何らかの方法で登録情報が通知されるものと仮定する。HPC ストレージの利用認可がなされた場合、HPCI 事務局から通知される HPCI アカウント情報(ユーザ/グループ名)に基づき、Gfarm 管理者が Gfarm 管理コマンドを用いてストレージユーザ/グループの登録、ユーザディレクトリの作成、作成したユーザディレクトリの所有者/パーミッションの変更、必要に応じて拡張 ACL の設定などを行う。主なユーザ管理コマンドを表 2-4 に示す。なお、日常的に行われるユーザ登録作業の自動化/簡易化について、新たにツール群を整備する予定である(今後検討)。

表 2-4 ユーザ管理コマンド

管理作業	管理コマンド
ユーザ登録	$ gfuser -c hpci_user realname /hpci/group/user gsi_dn
FUSE ユーザ登録	# usermod -G fuse hpci_user
グループ登録	$ gfgroup -c hpci_group hpci_user
ユーザディレクトリ作成	$ gfmkdir /hpci/hpci_group/hpci_user
所有者変更	$ gfchown hpci_user:hpci_group /hpci/hpci_group/hpci_user
grid-mapfile 設定	自動生成ツールを提供予定(認証基盤)
quota 設定	$ gfquota -g hpci_group -S softspc -H hardspc

(4) ファイルシステム管理

ファイルシステム管理は HPCI ストレージのクォータ制限値等の変更などを行う管理作業シナリオである。また、必要に応じて、異なるメタデータサーバ間のグループディレクトリに対するシンボリックリンク設定、利用失効したユーザのアクセス権変更（書き込み禁止）、失効期限後に一定期間（今後検討）を経過したファイルの強制削除などを行う。具体的なファイルシステム管理手順については、管理者向けマニュアルとして整備を行うものとする。

(5) ハードウェア管理

ハードウェア管理は拠点内に設置されるノード、ストレージなどの機器の起動/停止を行う管理作業シナリオである。機器の起動/停止は計画停電や活性保守できないハードウェア障害が発生した場合に対応が必要である。なお、Gfarm ファイルシステムは一部のファイルシステムノード（ストレージ）が停止しても他のファイルシステムノードにファイル複製が置かれる前提であることから、運用影響は軽微で局所的なものとなる。具体的なハードウェア管理手順については、管理者向けマニュアルとして整備を行うものとする。

(6) 運用管理

運用管理はメタデータやスプールディレクトリ、ログファイルの退避などを行う管理作業シナリである。メタデータのバックアップは必須であると考える（バックアップ頻度、バックアップ方法、外部バックアップ先などは今後検討）。スプールディレクトリのバックアップは、他ファイルシステムノードに自動的にファイル複製が作成されることからも、バックアップは任意と考える（今後検討）。また、ユーザ単位、グループ単位、ストレージ全体の利用統計情報のレポーティングについても運用管理作業（定常作業）に含まれる。利用統計情報のレポーティングは拡張仕様とする（今後整備化を検討）。具体的な運用管理手順については、管理者向けマニュアルとして整備を行うものとする。

(7) 運用監視

運用監視は拠点内に設置されるノード、ストレージの稼働確認、監視を行う管理作業シナリオである。Gfarm ファイルシステムには PDS である ZABBIX の監視プラグインが整備されていることから、ZABBIX を用いた運用監視が可能である。Gfarm の監視機能（ハードウェア異常監視機能、ソフトウェア異常監視機能）は PDS の ZABBIX をベースに作成されているため、拠点毎に HPC ストレージ監視用の ZABBIX サーバが別に必要となる。また、メタデータサーバ、ファイルシステムノード、クライアントに監視プラグイン（ZABBIX エージェント）のインストールも必要となる。HPC ストレージにおける ZABBIX 監視構成を図 2-9 に示す。

また、I/O 性能に劣化はないかなど、各拠点のクライアントノード上で I/O 性能の監視

を行う。性能監視ツールは拡張仕様とする(今後整備化を検討)。稼働監視と性能監視は新たにツール群を整備する予定である。具体的な運用管理手順については、管理者向けマニュアルとして整備を行うものとする。

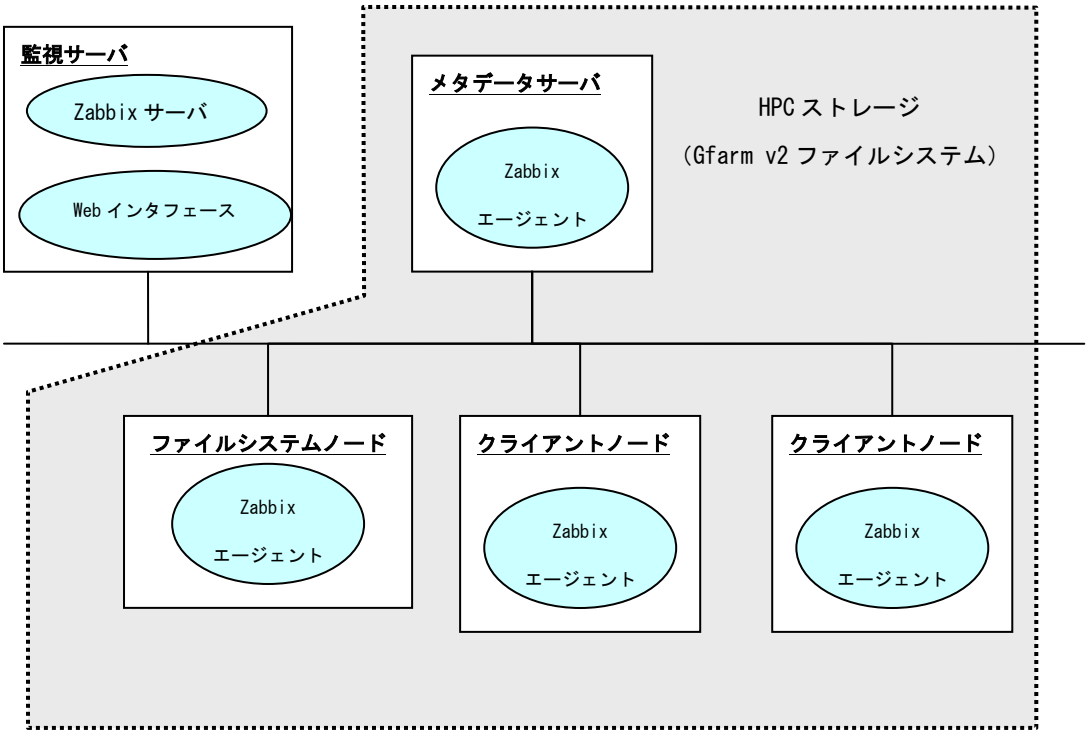


図 2-9 HPC ストレージにおける ZABBIX 監視構成

(8) 障害時対応

障害時対応はHPC ストレージを構成するハードウェア/ソフトウェアに何らかの障害(ハード・ソフト)が発生した場合のトラブルの一時切り分けと、復旧対応(暫定対処、恒久対処)を行うものである。トラブル対応手順は HPC ストレージの運用開始までにドキュメント整備し、本ドキュメントに基づき、対応を行うものとする。具体性に想定されるトラブル対応シナリオは別章で説明する。ストレージ障害は運用影響が非常に大きいため、データ分散冗長化や耐故障性の向上を図る一方、仮にストレージ障害が発生した場合も即座に復旧可能なよう、トラブル対応フローマニュアルとして整備を行うものとする。

2.6.3 資源提供視点でのシナリオ

平成 23 年度の資源提供視点でのシナリオを以下に説明する。

(1) ストレージ資源提供の検討

HPCI にストレージ資源を提供するかを検討する。

拠点側で共有ストレージを用意することで、ファイルアクセスはローカルアクセスとなり、拠点に共有ストレージを用意しない場合に比べ、より高速にファイル共有、複製が可能となる(ユーザメリット)。すぐにはストレージを整備できない場合や試行的に利用したい場合には、自拠点にストレージを用意せず、クライアント的に利用することも可能である。

資源提供機関が提供すべきストレージ資源を以下に示す。

・ストレージ(自拠点に HPC ストレージ用のファイルサーバを設置)

・メタデータサーバ(自拠点でファイルシステムを管理したい場合に設置)

(2) ストレージ資源管理ポリシーの検討

メタデータサーバを共同利用するか、独立して運用するか(自拠点でファイルシステムを管理するか)の管理ポリシーを検討する。

メタデータサーバを独立して運用する場合、メタデータサーバを追加設置することになるが、これは実質的に HPC ストレージを分割することを意味する。これによりストレージ拠点の管理負担が増え、利用効率も悪くなるため、追加は推奨しない(もしくは慎重に行う必要があると考える)。

(3) ストレージ資源の供出、管理

HPC ストレージの性能は主にネットワーク性能に律速されるため、HPC ストレージを快適に利用のための前提条件を提示することで高速ファイル共有を実現する。

具体的な接続条件は以下である。

- 拠点内スパコンのログインノードと HPC ストレージは同一ネットワーク(10Gbps 以上が望ましい)で直接、接続すること。
- ログインノードは HPC ストレージ専用の経路および帯域が確保できることが望ましい。
  ここでの帯域保障とは、通常のログインノードへのアクセスとは別に、ログインノードと HPC ストレージ間のアクセスを、別経路(専用アクセス経路)を用意することを指す。

なお、資源提供側が供出するストレージスペック詳細は別章で説明する。資源提供側で供出したストレージの管理は、管理者視点でのシナリオを参照のこと。

2.6.4 事務局視点でのシナリオ

平成 23 年度の事務局視点でのシナリオを以下に説明する。

(1) アカウント発行

HPC ストレージ利用者からHPC ストレージの利用申請を受け付ける。課題審査や本人確認等を行い、申請内容に問題なければ HPC ストレージ利用者に HPCI アカウントを通知する。HPC ストレージの変更/廃止申請もHPCI 事務局で受付を行い、変更/廃止内容を HPC ストレージ利用者に通知する。

HPC ストレージの利用に際して、申請時に必要と考えられる情報(申請書に取り込まれるべき情報)を表 2-5 に示す。なお、利用申請情報の詳細は今後検討とする。

表 2-5 HPC ストレージ利用申請情報

項目	内容
申請種類	□新規 □変更 □終了
利用用途	□一般利用 □特別利用(ex. 先端ソフト共有)
利用期間(開始～終了日)	開始日～終了日
申請者情報(代表者)	所属、氏名、連絡先
HPCI アカウント名	
HPCI 所属グループ名	(今後検討)
希望ファイルパス名	(今後検討)
希望容量(Group Quota)	●GB 単位(最大●GB)
メイン利用拠点	□プライマリサイト □セカンダリサイト
その他(利用機能)	□ACL □User Quota(filenum)
注意事項、免責	□データ無保証(ベストエフォートでの保障)への同意 □利用期限終了後のデータ破棄への同意

(2) アカウント変更

利用申請、変更/廃止申請のあった HPC ストレージの利用者情報(HPCI アカウント)について、HPCI 事務局からメタデータ管理者に通知する。

2.6.5 共通視点でのシナリオ

平成 23 年度の共通視点でのシナリオを以下に説明する。

(1) メタデータの管理

ファイルシステムの名前空間や容量制限を行う上で、メタデータを 1 式のサーバで集中管理する運用、拠点毎にメタデータサーバを配置して分散管理する運用が考えられる。集中管理と分散管理の何れの管理方法においてもユーザビリティが犠牲にならないよう、ファイルシステムの名前空間は一意とする(ファイルパスに拠点名などの文字列を含めることはしない)。

メタデータの集中管理と分散管理における問題点(長所・短所)を表 2-6 に示す。

表 2-6 メタデータの集中管理/分散管理における問題点

管理方法	長所	短所
集中管理	・ HPC ストレージ全体を1つのストレージとして利用可能なため、空き領域が有効に利用できる。 ・ ユーザ登録や容量制限など、1 回の設定で済む。 ・ 拠点ストレージはインクリメンタルに増設できる。	・ 1 つのファイルシステムで構成するので、障害時の影響が全体に及ぶ可能性あり(1 つの大容量のファイルシステムを作成できる)。
分散管理	・ 複数のファイルシステムで構成するので、障害時の影響を局所化できる。	・ HPC ストレージを事実上複数に分割するため、空き容量が有効に利用できない。 ・ ユーザ、グループ登録、容量制限は、メタデータサーバを提供する全ての拠点で設定が必要となる。 ・ ストレージを提供する拠点は、メタデータサーバを提供する拠点の数分のストレージの設定が必要となる(インクリメンタルに増設できない)。

両者の違いを以下に整理する。

- メタデータを拠点毎に分散管理すると、拠点毎に管理が必要な分、HPC ストレージ全体で管理工数は増える。
- HPC ストレージを事実上分割して利用することとなるため、空き領域が有効に利用できない。

- 拠点ストレージが追加された場合、分散管理ではインクリメンタルに増設できない（拠点分のストレージサーバが必要となること、各拠点のメタデータサーバ上でファイルシステムノードの設定が必要となる）。

(2) 名前空間と容量制限

HPC ストレージの名前空間（パス名）は「/hpci/グループ名/ユーザ名」のファイル階層とするのが望ましいと考える。第二階層を課題グループ名とすることから、複数の課題グループに属するユーザの場合、ユーザ自身で各々の課題グループ配下にあるユーザ自身のディレクトリを意識して使い分けることになる。これ以外にも先端基盤ソフトウェアの OS イメージなど、HPCI 共通のファイル格納先として利用する。HPCI の共有ディレクトリは第二階層に HPCI 管理者が希望する名前で作成する。HPC ストレージの名前空間の案を図 2-10 に示す。

容量制限（quota）はグループまたはユーザ単位に、ファイルサイズまたはファイル数で制限できる。

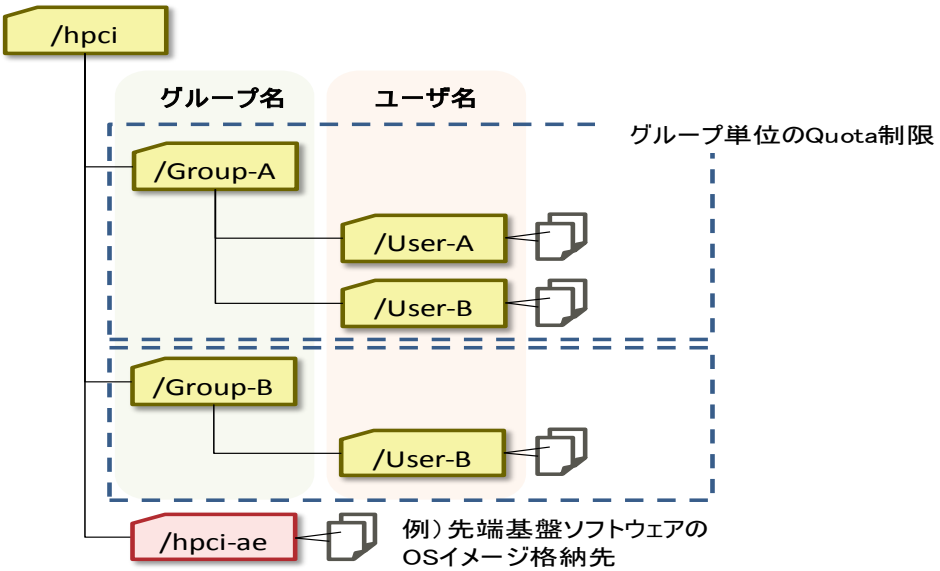


図 2-10 HPC ストレージの名前空間の案

メタデータサーバを各拠点に設置し、メタデータを分散管理する運用も可能である。複数メタデータサーバ構成で運用する場合、メタデータサーバ毎に名前空間は独立したものになるが、Gfarm URL のシンボリックリンク機能を利用すれば、複数メタデータサーバ構成で運用する場合も、同一の名前空間として利用者に透過的に見せることが可能である。ただし、異なる Gfarm 間でのファイル複製はできず、また同一の名前空間に見せるため、グループ追加の際に全拠点でシンボリックリンクの設定が必要となる。分散管理運用時の HPC ストレージの名前空間の案を図 2-11 に示す。

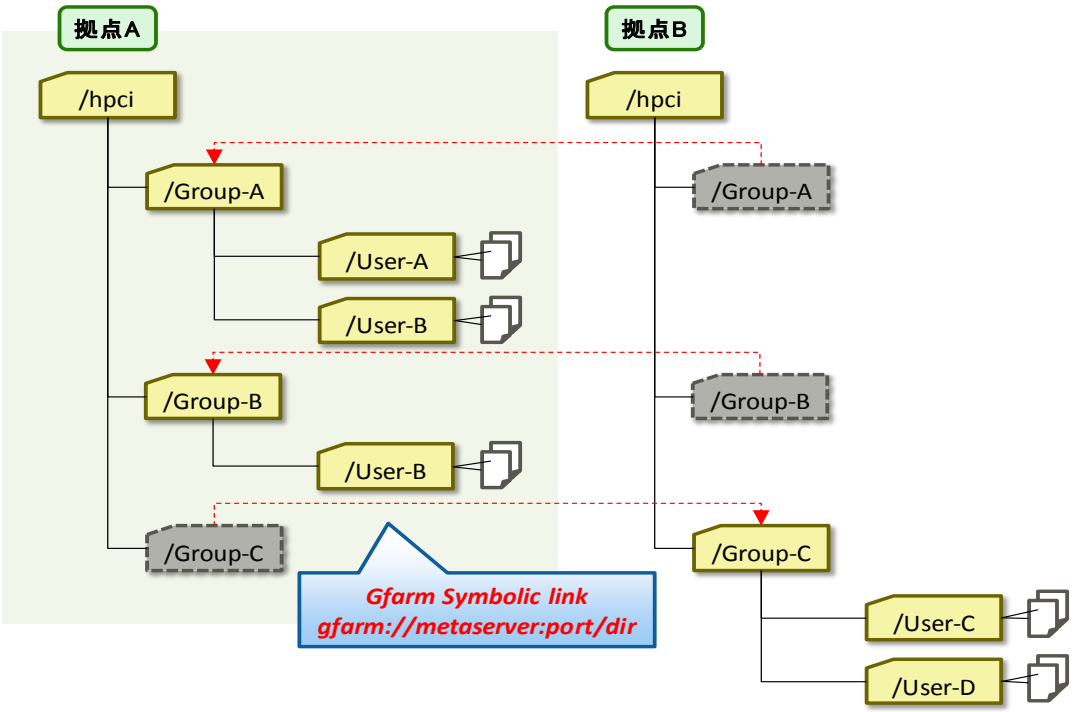


図 2-11 分散管理運用時の HPC ストレージ資源の名前空間の案

2.7 平成 24 年度以降の利用シナリオ

2.7.1 ユーザ視点での利用シナリオ

平成 24 年度以降のユーザ利用シナリオを以下に説明する。

(1) Web ブラウザからのファイルアクセスサポート

ユーザ PC から Web アクセスにより、HPC ストレージ上のファイルに容易にアクセスできる機能を提供する。また、ユーザ PC の Web ブラウザから、UNIX の一般的なファイルの操作(cp,mv,rm 等)、ファイルの表示、ファイルのアップロード/ダウンロード等の操作がより簡単に行えるポータルサービスの提供についても検討継続とする。

(2) ユーザ PC からのファイルアクセスサポート

ユーザ PC から HPC ストレージに対するファイルアクセス方法を拡充する。具体的には WebDAV/CIFS でのファイルアクセスをサポートする。技術的課題として、Web アクセス時のユーザ認証をどうするか、認証されたユーザ権限でどのように Gfarm ファイルシステムにアクセスするかを検討継続とする。

(補足)HPC ストレージへの Web アクセス(WevDAV サポート)は GSI 認証が課題である。秘密鍵を用いた sharedsecret 認証であれば基本仕様としてサービス提供できるが、GSI 認証が必要であれば新規開発が必要となる。なお、GSI 認証での Web アクセスは Gfarm 本来の機能ではないが、ユーザニーズや費用対コストも含めた実現可否の検討が必要であると考える。

(3) ファイルカタログ機能のサポート

計算ノードから HPC ストレージ上のファイルカタログ(ファイル所在情報)を参照する機能、計算ノード～HPC ストレージ間のファイルステージング機能、計算ノードから直接、HPC ストレージ上のファイルにアクセスする機能、拠点スパコンと HPC ストレージ間の自動ファイル同期機能など、多様なユーザニーズが挙げられているが、これらのユーザニーズの強さ、実現可否、費用対コスト、実現する上での課題有無など、検討継続とする。

2.7.2 管理者視点での利用シナリオ

平成 24 年度以降の管理作業シナリオを以下に説明する。

(1) Gfarm エンハンス対応

HPC ストレージの信頼性や性能向上、拠点管理者やユーザの利便性向上を目的とし、平成 23 年度、平成 24 年度に段階的に Gfarm ファイルシステムのエンハンスを行う予定である。Gfarm ファイルシステムのエンハンス予定機能を表 2-7 に示す。

拠点管理者はエンハンスされた Gfarm ファイルシステムの再インストール(必要に応じて再設定)などの作業が必要になる。

表 2-7 Gfarm ファイルシステムのエンハンス予定機能

No.	機能概要	開発予定機能
1	メタデータサーバ冗長化 (ホットスタンバイ)	- スレーブメタデータサーバへの管理データ同期機能の実装 - 障害発生時におけるフェイルオーバ機能の実装
2	高速ファイルコピー、複製作成機能 (ステージング＋複製)	- スパコンのファイルシステムとの間の高速コピーの実装 - 拠点間での高速複製作成の実装
3	監視機能の高度化	- チケットシステムとの連携 - メタデータサーバ異常検出時のフェイルオーバ支援
4	メタデータサーバ冗長化の信頼性向上 (ホットスタンバイの信頼性向上)	- Gfarm 自動ファイル複製機能の高度化

2.8 HPC ストレージの利用フロー

主な HPC ストレージの利用フローを以下にまとめる。

[利用者視点]

（初回利用時）

- ✧ HPCI 利用申請
- ✧ 証明書発行申請

（通常時）

- ✧ 拠点システムへのログイン（シングルサインオン）
- ✧ HPC ストレージのマウント（ユーザが必要に応じてマウントする、システムで静的にマウントしておくことはできない）
- ✧ HPC ストレージ上のファイル、ディレクトリ操作
- ✧ HPC ストレージ上のファイル、ディレクトリに対するパーミッションの設定、変更
- ✧ ファイルステージング（拠点スパコンのストレージ～HPC ストレージ間）
- ✧ HPC ストレージのアンマウント
- ✧ HPC ストレージのファイル複製（自動再複製）、複製場所の表示
- ✧ HPC ストレージ全体、拠点毎の稼働状況、使用量の表示

[拠点管理者（メタデータ管理者）視点]

（稼働開始前/非定形作業）

- ✧ Gfarm メタデータサーバの初期設定

（通常運用/定型作業）

- ✧ Gfarm メタデータサーバノードの起動、停止
- ✧ Gfarm メタデータサーバノードのハードウェア管理
- ✧ Gfarm メタデータサーバノードのユーザ/グループの登録、変更
  （利用を許可するユーザを登録する、未登録のユーザは利用できないので、拠点のメタデータサーバ毎に利用者を制限することも可能）
- ✧ メタデータのバックアップ、リストア
- ✧ ログファイルのバックアップ
- ✧ ユーザ/グループディレクトリの作成、変更（メタデータの集中管理時）
- ✧ グループディレクトリに対するシンボリックリンクの作成（メタデータの分散管理時）
- ✧ ユーザ/グループパーミッションの設定、変更
- ✧ ユーザ/グループの quota 設定、変更
- ✧ メタデータサーバの稼働確認、稼働監視
- ✧ HPC ストレージの利用統計

- ✧ Gfarm メタデータサーバノード障害時の調査、復旧
- ✧ 定期保守（パッチ適用）
- ✧ セキュリティチェック、脆弱性対応
- ✧ ウィルススキャン（要検討）
- ✧ 利用失効ユーザのアクセス権変更（書き込み禁止）、一定期間経過後のファイル強制削除（要検討）

（環境変更/非定形作業）

- ✧ 拠点ストレージの変更（増設、リプレース、撤去）
- ✧ ネットワーク変更
- ✧ ソフトウェアレベルアップ

［拠点管理者（ストレージ提供機関）視点］

（稼働開始前/非定形作業）

- ✧ Gfarm ファイルシステムノードの初期設定

（通常運用/定型作業）

- ✧ Gfarm ファイルシステムノードの起動、停止
- ✧ Gfarm ファイルシステムノードのハードウェア管理
- ✧ Gfarm ファイルシステムノードのユーザ/グループの登録、変更
  （利用を許可するユーザを登録する、未登録のユーザは利用できないので、拠点のファイルシステムノード毎に利用者を制限することは可能）
- ✧ ログファイルのバックアップ
- ✧ メタデータサーバの稼働確認、稼働監視
- ✧ Gfarm ファイルシステムノード障害時の調査、復旧
- ✧ 定期保守（パッチ適用）
- ✧ セキュリティチェック、脆弱性対応
- ✧ ウィルススキャン（要検討）
- ✧ 拠点内外の HPC ストレージに対するネットワーク疎通確認
- ✧ 拠点内のストレージに対する性能監視、調査
- ✧ スプールディレクトリのファイルバックアップ（必要に応じて）

（環境変更/非定形作業）

- ✧ 拠点ストレージの変更（増設、リプレース、撤去）
- ✧ ネットワーク変更
- ✧ ソフトウェアレベルアップ（メタデータ管理者より手順を提供）
- ✧ 拠点内のストレージ上のファイル転送（ストレージ撤去）

［拠点管理者（クライアント提供機関）視点］

（稼働開始前/非定形作業）

- ✧ FUSE、GSI ライブラリ/クライアント、Gfarm クライアントのインストール
- ✧ Gfarm の初期設定
- ✧ 認証局の登録

（通常運用/定型作業）

- ✧ メタデータサーバ、ファイルシステムノードとの疎通確認
- ✧ HPC ストレージの稼働確認、稼働監視、性能監視
- ✧ HPC ストレージの障害時調査、復旧
- ✧ 定期保守（パッチ適用）
- ✧ セキュリティチェック、脆弱性対応

2.9 障害フロー

［管理者視点］

共有ストレージとして利用する Gfarm ファイルシステムは、メタデータサーバノード、ファイルシステムノード、クライアントノードから構成される。想定される障害とその運用影響、復旧対応等を以下にまとめる。なお、具体的な障害復旧手順については管理者向けマニュアルとして整備を行うものとする。

1）メタデータサーバノード障害

運用影響	ファイルのオープン/クローズやディレクトリ参照など、メタデータのアクセスを伴うファイルアクセスは不可（ファイルアクセスがブロックされる）。但し、書き込みオープン中のファイルを除き、メタデータサーバノードの復旧を待ち、運用継続可能。
対応者	メタデータ管理者
復旧対応	冗長構成（コールドスタンバイ）のため、基本的に復旧対応は不要。ホットスタンバイは将来サポート予定（拡張仕様）

2）ファイルシステムノード障害

運用影響	他のファイルシステムノードにファイル複製が存在すれば、運用継続可能。ダウンしたファイルシステムノードにしかファイルが存在しない場合、ファイルアクセスは不可（ファイルアクセスがブロックされる）。
対応者	メタデータ管理者、拠点管理者
復旧対応	ノード障害の復旧が必要。 バックアップがなく、データロストした場合、メタデータサーバ管理者でメタデータ複製情報の消去が必要。

3) ネットワーク障害

運用影響	クライアントから、メタデータサーバノード、ファイルシステムノードへアクセスできるかで影響範囲が異なる。上記 1)、2)を参照。
対応者	メタデータ管理者、拠点管理者
復旧対応	特になし、ネットワーク障害の復旧を待つ。

4) 認証局障害

運用影響	証明書が取得できない（初期登録できない）。
対応者	メタデータ管理者
復旧対応	特になし、認証局障害の復旧を待つ。

5) Gfarm 障害

運用影響	全系ダウンなど、影響は広範囲に及ぶ可能性あり。
対応者	メタデータ管理者
復旧対応	調査資料採取後に再起動で復旧

6) 停電対応

運用影響	メタデータサーバとネットワーク機器は UPS 保護するため、長時間の停電でなければ運用影響なし。ファイルシステムノードはUPS保護しないため、他拠点にファイル複製があれば運用継続可能だが、ファイル複製がなければファイルアクセス不可）
対応者	メタデータ管理者、拠点管理者
復旧対応	特になし、復電を待つ。

7) その他の不具合

その他、以下にあげる日常的に発生すると考えられる不具合について、切り分け方法や復旧手順について、管理者向けマニュアルとして整備を行う。

例）ファイルにアクセスできない理由

・証明書の有効期限切れ

・時刻同期とれていない

3 基盤構築・運用基本仕様

3.1 HPC ストレージ

本節ではストレージ共有のための HPC ストレージの基盤構築・運用の基本仕様を定義する。HPCI コンソーシアム（ストレージサブ WG）で検討されたストレージに関する要求事項は機能面、運用面、整備面に渡っている。これを整理し、要求が満たされるように、分散ファイルシステム機能として必須とする機能、将来の分散ファイルシステム機能として提供する機能、運用体制・運用方法として提供する機能、今後の整備として必要とされるものに分類する。

3.1.1 一般要求事項、付帯事項

HPCI コンソーシアム ストレージサブ WG で検討を行った共有ストレージ（HPC ストレージ）に関する一般要求事項を以下に示す。

- 大容量のデータを格納でき、場所を気にせずにアクセスする機能を有すること。
- 大量のデータを格納でき、コミュニティでのデータ共有、アーカイブする機能を有すること。
- 複製やバックアップなどによる高信頼性の保持、継続的な保守とシステム増強へ対応可能なこと（ファイルシステム容量はスケールアウトすること）。

上記の一般要求事項に対する付帯事項を以下に示す。付帯事項も一般要求事項と同じく、基本仕様に反映する。

- 各拠点にHPCI用の大規模ストレージを整備する上で、資源提供機関で必要な要件、スペックをまとめること。
- 最先端研究基盤事業で整備されたストレージの活用を検討すること。
- 必要に応じて、基盤センターや戦略機関等のストレージの整備、増強を検討すること。

3.1.2 HPC ストレージ基盤構築基本仕様

平成 23 年度の HPC ストレージ基盤構築の基本仕様を以下に示す。なお、平成 24 年度の HPC ストレージ基盤構築作業については、次年度に作業内容を検討する。

(1) 利用するストレージ資源

基本仕様では平成 22 年度最先端研究基盤事業「e-サイエンス実現のためのシステム統合・連携ソフトウェアの高度利用促進」により、東京大学情報基盤センターおよび理化学研究所計算科学研究機構に設置される大規模ストレージのうち、東京大学情報基盤センターに設置される大規模ストレージの一部を HPC ストレージとして整備する。理化学研究所計算科学研究機構に設置されるストレージについては、理化学研究所計算科学

研究機構との広域ネットワークが未整備なこと、京コンピュータの運用開始に向け、平成24 年 1 月以降でネットワーク網も順次整備されていく計画であることから、当面は実験的な部分利用に留め、HPC ストレージ運用には組み込まない。

東京大学情報基盤センターに設置される大規模ストレージの一部を HPC ストレージとして利用する上で、利用可能な資源（ディスク容量）は今後の調整とする。なお、HPC ストレージで利用するスプール領域は、ext3/ext4/xfs の何れかのファイルシステムで初期化した上で利用する。

(2) メタデータの管理方法

メタデータサーバの設置場所はメタデータの管理方法を調整した上で決定することとする。メタデータは 2 台のメタデータサーバ（冗長構成）で管理する。なお、基本仕様では東京大学情報基盤センターに HPC ストレージ全体を管理するメタデータサーバ一式を設置することとし、資源提供機関側でストレージを用意する場合も資源提供側にメタデータサーバを配置することはしない。

(3) ネットワーク接続

メタデータサーバ、ファイルシステムノード、クライアントは 10Gbps の帯域でネットワークに接続できることが望ましい。サーバのハードウェア仕様は別章で定義する。

HPC ストレージを利用する全てのクライアント（拠点スパコンのログインノード）はメタデータ（どのファイルがどこに格納されているか）を参照する際、メタデータサーバに問い合わせが必要なため、全クライアント～メタデータサーバ間でネットワーク接続が許可されている必要がある。また、実際のデータ通信はクライアントとファイルシステムノード間で直接通信を行うため、クライアント～全ファイルシステムノード間でネットワーク接続が許可されている必要がある。

一般的に拠点スパコンのログインノードは Firewall に守られた内部ネットワークに接続され、メタデータサーバ、ファイルシステムノードも同様に東京大学の Firewall 内に接続されるため、拠点の Firewall で通信相手毎に通信ポートへのアクセスを許可する必要がある。HPC ストレージ（Gfarm ファイルシステム）で利用する TCP port 番号は以下のとおり。

- メタデータサーバの port 番号：600/tcp
- ファイルシステムノードの port 番号：601/tcp+udp

(4) 運用開始時期

平成 23 年度中に HPC ストレージの仮運用を開始する。なお、運用開始に先立ち、HPCI 認証基盤の整備も必要であることから運用開始時期については今後調整とする。

3.1.3 HPC ストレージ基本ハードウェア/ソフトウェア仕様

HPC ストレージを構成する各サーバノードの基本ハードウェア/ソフトウェア仕様を以下に示す(●は今後検討)。

(1) ハードウェア仕様

HPC ストレージ(Gfarm ファイルシステム)は、メタデータサーバノード、ファイルシステムノード、クライアントノード、アレイディスク装置、管理用サーバ、ネットワークスイッチから構成される。

1) メータデータサーバは、以下の仕様を満たす同一構成のサーバ●台で構成すること。

- Intel 64bit 拡張された x86 系 CPU で、●コア以上の CPU コア(動作周波数は●GHz 以上)を●CPU 以上搭載すること。
- メモリ容量●GB(DDR● ●MHz)以上を有すること。
- システムディスクは●GB 以上の容量を持つ内蔵 SAS/SSD ディスクを●台以上有し、RAID1 で構成すること。
- メタデータディスク、Gfarm ジャーナルの格納ディスクは●GB 以上の容量を持つ外部 SAS/FC/SSD ディスクを RAID●で構成すること。
- 外部ディスクとサーバ間は●Gbps の FC/SAS インターフェース、●本以上で接続し、パス障害時にも自動的にパスを切り替えての運用継続が可能なこと。
- IPMI2.0 に対応したリモート監視およびシステム制御機能を有すること。
- 冗長電源を有すること。
- メタデータ応答時間短縮のため、メタデータ用データベース(PosugreSQL)の SSD または RAM ディスク格納については今後検討とする。

2) ファイルシステムノードは、以下の仕様を満たす同一構成のサーバ●台で構成すること。

- 上記 1)と同じ。

3) アレイディスク装置は、以下の仕様を満たす同一構成のディスク装置●台で構成すること。

- RAID6(7D+2P あるいは 8D+2P)構成で、物理データ領域(フォーマット後の論理容量)は最低●PB であること。
- 一部のワーク領域(テンポラリ領域)は RAID5(8D+1P あるいは 9D+2P)構成で、物理データ領域(フォーマット後の論理容量)は最低●PB であること。
- サーバ～アレイディスク装置間の接続パスは冗長化すること。
- ディスクアレイ装置全体のディスクコントローラは冗長性を有し、その物理性能は

●GB/s 以上であること。

- 冗長電源を有すること。
- コントローラ、ディスクドライブ、電源、ファンの活性保守が可能であること。また、各部品の予兆通知、異常通知が可能であること。
- 各種設定ツールは日本語・英語に対応していること。

4) 管理用サーバは、以下の仕様を満たす同一構成のサーバ●台で構成すること。

- 上記 1)と同じ。

5) ネットワークスイッチは、データ系と保守系のスイッチに分け、上記のサーバを接続すること。

- データ系スイッチは、10G インターフェースを●ポート以上有すること。

(2) ソフトウェア仕様

1) 各ノードの OS は、64 ビット版 RHEL6 相当であること。
2) 各ノードは NTP で時刻同期できること。
3) 分散ファイルシステムとして、Gfarm v2 最新版をインストールすること。

- ファイルシステムノード、クライアントノードは、運用中でも追加可能であること。
- メタデータサーバはコールドスタンバイ構成の冗長メタデータサーバ構成であること。
- quota 機能が利用できること。quota 機能はユーザおよびグループ毎に、ファイル複製も考慮した容量制限が行えること。また、ユーザ自身でファイル利用量を確認できること。(コマンドレベル)
- システムによる自動ファイル複製、利用者によるファイル複製操作、削除ができること。(コマンドレベル)
- ACL により、ファイルアクセス権を設定できること。(コマンドレベル)
- GSI 認証機能を有し、シングルサインオン機能を用いたシームレスなアクセスができること。パスワードを打ち込むことなく、アクセスすることができること(コマンドレベル)。

3.1.4 運用保守、ツール仕様

平成 23 年度に稼働開始する HPC ストレージの運用・保守のためのツール、運用保守支援体制、マニュアルに関する要件を以下に示す。

(1) 運用・保守のためのツール

1) Gfarm v2 ファイルシステムの運用管理機能

- 一部のワーク領域（テンポラリ領域）上にある長期未参照のファイルに対し、ファイル所有者にファイル削除を予告し、自動的にファイル削除できる機能を有すること。
- Gfarm ファイルシステムのハードウェア、ソフトウェア異常を監視する機能を有すること。ハードウェア異常監視機能は Gfarm v2 ファイルシステムを構成するメタデータサーバノード、ファイルシステムノード、クライアントノードを含むハードウェアコンポーネントに関して、異常を監視できること。ソフトウェア異常監視機能は Gfarm v2 ファイルシステムを構成するソフトウェアコンポーネント（メタデータサーバ、ファイルシステムサーバ、クライアント）に関して、異常を監視できること。

2) 拠点間の疎通をテストする運用ツールの作成（今後検討）

- 全てのファイルシステムノードに任意ファイル（任意ファイル数、任意ファイルサイズ）を作成、削除可能か、要した時間を含めて確認する管理者コマンドを提供すること。（運用ツール）
- 各拠点（クライアント）から、定期的にファイルアクセスできることを確認、アクセスできない場合には通知する管理者コマンドを提供すること。（運用ツール）
- 各拠点(クライアント)から定期的にファイルアクセス（メタ参照、ファイル作成、削除）を行い、I/O 性能を蓄積、ZABBIX でグラフ化すること。
- ダウンノードのみに存在するファイル（現在、利用できないファイル）を確認するコマンドを提供すること。

3) 稼働監視

- Web ビューでのメタデータサーバ、ファイルシステムノードのダウン監視、システム性能監視を行う環境を用意すること。（ZABBIX を利用）
- ファイルシステムノードの稼働状態を確認できること。（コマンドレベル）

4) 性能監視

- 過負荷 I/O ツール（細粒度 I/O や大規模ファイル作成）での試験ツールを提供すること。

(2) 運用・保守支援体制

- 本ストレージシステムを構成する機器に発生した自動検知可能な障害について、自動的にリモート保守センターに異常を通知できること。異常通知後、必要に応じ

て障害切り分け等の支援、リモート保守を行うこと。リモート保守に必要な機器等は必要に応じ、供給者が整備すること。

- ハードウェア及びソフトウェアの Q&A、トラブル対応について、平日（8:30～19:00）の保守支援体制をとること。
- 障害が発生した場合、当日または翌営業日（但し、夜間・休日の場合）に復旧作業に着手すること。障害状況は速やかにシステム管理者に途中経過や最終報告を行うこと。必要に応じ、発生障害の切り分け、原因究明を行い、障害部品の交換やバグ修正の適用を行うこと。
- 障害発生を未然に防ぐため定期保守（ソフトウェアのバージョンアップ）を実施すること。定期保守は原則として土曜日または日曜日に実施すること。
- 定期的にセキュリティ脆弱性テストを実施し、結果を報告すること。
- 運用保守に関する定期的な報告会を月 1 回開催すること。また、ストレージシステムの利用方法について、導入前後に利用講習会を開催すること。
- 1PB 以上の実容量を持つ大規模システムを有するスーパーコンピュータ(TOP500 リストに掲載されている規模)の導入及び運用実績を有すること。

(3) マニュアルに関する要件

1) メタデータ管理者用者向けに具体的な運用管理方法を記載した運用手引書、設定パラメタ等を記載したシステム環境設定書を作成し、電子媒体で提供すること。メタデータ管理者向けの運用手引書には以下の内容を記載すること。

- 起動、停止方法
- 稼働状況の確認、監視方法
- 定型作業手順
  ソフトウェアアップデート方法
  拠点管理（拠点追加、拠点ストレージの増設、拠点ストレージの停止）
  ユーザ管理（ユーザ/グループの新規登録・削除、quota 制限、統計情報採取）
  バックアップ（メタデータ、ログ、設定ファイル）
- トラブル対応方法
  トラブル発生時の切り分けフロー
  発生が想定されるトラブルとその復旧手順（認証/ネットワーク/ストレージ障害）

2) ストレージ提供機関、クライアント提供機関の管理者向けに具体的な操作方法を記載した運用手引書を作成し、電子媒体で提供すること。ストレージ提供機関、クライアント提供機関の管理者向けの運用手引書には以下の内容を記載すること。

- 起動、停止方法
- 稼働状況の確認、監視方法
- 定型作業手順

- トラブル対応方法

  トラブル発生時の切り分けフロー

  発生が想定されるトラブルとその復旧手順（認証/ネットワーク/ストレージ障害）

3) 利用者向けに具体的な利用方法を記載した手引書を作成し、電子媒体で提供すること。利用手引書には以下に内容を記載すること。

- 利用申請方法
- 利用方法

  アクセス方法（拠点スパコンへのマウント、Web アクセス）

  操作方法（一般コマンド、ファイル複製、QUOTA/ACL、並列検索）
- 留意事項

4) システム構成やソフトウェア環境の設定変更に伴う改版があった場合は、速やかに運用手引書、システム環境設定書、利用手引書の修正版を提供すること。

4　事務局、資源提供基本仕様

本節では、事務局および提供組織が提供しなければならない計算機環境仕様、提供資源連携のための委員会仕様を決める。資源提供組織は、資源提供連携ネットワーク委員会（仮称）の一員とする。

4.1 ストレージ資源提供環境必須項目

1）ネットワーク環境の変更
- 東京大学、拠点側の F/W 両端でポートオープン設定が必要である。
  （ポートオープン: gfsd/600、gfmd/601）

2）クライアント利用（ログインノードの環境変更）
- FUSE、GSI ライブラリ/クライアントのインストール、gfarm クライアントのインストール
  （具体的なバージョンは別途、基本的には最新版のインストール要）
- ホスト証明書の取得、登録
- 認証局の登録
- Gfarm クライアントの初期設定
- ログインノードは HPC ストレージ専用の経路および帯域が確保できることが望ましい。

3）ストレージ提供機関
- ストレージ資源提供機関が用意するメタデータサーバ、ファイルシステムノード、ストレージの具体的なスペック(ノード性能、ディスク容量)は次年度検討とする。
- 拠点内スパコンのログインノードと HPC ストレージは同一ネットワーク（10Gbps 以上が望ましい）で直接、接続すること。

5 ドキュメント&システム開発整備（発注仕様）

5.1 共有ストレージ導入、保守作業仕様

(1) 導入作業

共有ストレージの以下の導入作業を実施すること。

- 東京大学情報基盤センターに設置される大規模ストレージに Gfarm ファイルシステムを新規インストールし、HPC ストレージとして整備すること。理化学研究所計算科学研究機構に設置されるストレージは平成 24 年 1 月以降のネットワーク整備後に実施すること。（利用可能なストレージ資源は次年度検討）
- クライアント側は拠点スパコンの運用管理者が環境構築を行う。クライアント側で必要な作業手順を詳細にドキュメント化し、提供すること。
- 利用者向けマニュアル、管理者（メタデータ管理者、ストレージ提供機関、クライアント提供機関の管理者向け）マニュアルを作成すること。管理者向けマニュアルには発生が想定されるトラブルの復旧手順についても記載すること。システム構成やソフトウェア環境の設定変更に伴う改版があった場合は、速やかに運用手引書、システム環境設定書、利用手引書の修正版を提供すること。

(2) 保守作業

共有ストレージの以下の保守作業を実施すること。

- ハードウェア及びソフトウェアの Q&A、トラブル対応について、平日（8:30～19:00）の保守支援体制をとること。
- 障害が発生した場合、当日または翌営業日（但し、夜間・休日の場合）に復旧作業に着手すること。障害状況は速やかにシステム管理者に途中経過や最終報告を行うこと。必要に応じ、発生障害の切り分け、原因究明を行い、障害部品の交換やバグ修正の適用を行うこと。
- 障害発生を未然に防ぐため定期保守（ソフトウェアのバージョンアップ）を実施すること。定期保守は原則として土曜日または日曜日に実施すること。
- 定期的にセキュリティ脆弱性テストを実施し、結果を報告すること。
- 運用保守に関する定期的な報告会を月 1 回開催すること。また、ストレージシステムの利用方法について、導入前後に利用講習会を開催すること。

5.2 共有ストレージ運用ツール群発注仕様

共有ストレージの運用ツールにおいて、以下の機能を実現するソフトウェアの開発作業を発注する。発注するソフトウェア機能、作業内容を以下に説明する。

(1) 共通仕様

本作業は以下に示す機能を実現するために必要な機能を実装するのものである。Gfarm v2 に関する概要、インタフェース仕様、およびソースコードは以下にあるので、参照のこと。

http://datafarm.apgrid.org/

http://sf.net/projects/gfarm/

各作業における納入物件は以下とする。

- 作業報告書 一式
- Gfarm V2 ファイルシステムソースコード 一式
- gfarm2fs ソースコード 一式
- 修正ログ 一式
- 検査仕様書 一式
- 検査結果報告書 一式

本開発作業においては、Gfarm v2 のコーディングスタイルを守り、コードの可読性、モジュラリティを損なわないようにすること。また、コード中で共通部分はなるべく一ヶ所にくくり出し、メンテナンシビリティを損なわないようにすること。リテラルはなるべくマクロを利用するなどコード内で直接利用しないようにすること。checkpatch.pl によるチェックを実施すること。

(2) Gfarm メタデータサーバ冗長化(ホットスタンバイ)

メタデータサーバは、Gfarm ファイルシステムの管理データを管理するサーバである。メタデータサーバは 1 サーバで動作するため、このサーバに障害が発生すると新たなファイルシステムの利用ができなくなる。そのため、メタデータサーバの予備サーバ(以降スレーブメタデータサーバ、予備ではないサーバをマスターメタデータサーバと呼ぶ)を準備し、障害発生時にスレーブメタデータサーバに切り替えること(以降フェイルオーバ)により、ファイルシステムの利用を継続する。Gfarm バージョン 2.4.1 におけるフェイルオーバは、スレーブメタデータサーバをマスターメタデータサーバと同一の IP アドレスで起動するものであるが、この方式ではスレーブメタデータサーバの起動に数分～数十分かかることがあり、ファイルシステムを利用できない時間が長くなってしまう。本作業では、スレーブメタデータサーバを、マスターメタデータサーバと常に最新の状態で同期させ、メタ

データサーバに障害が発生したときに、スレーブメタデータサーバに即座に切り替えることにより停止時間を数秒程度にする。

具体的には以下の項目について、設計および開発作業を行うこと。

- スレーブメタデータサーバへの管理データ同期機能の実装
  スレーブメタデータサーバに対し、マスターメタデータサーバの管理データを同期するための機能を実装する。同期とは、必要な全管理データの転送、その後更新された管理データの転送を行い、マスターメタデータサーバと同一の管理データをもたせることである。同期後はいつどのような状態でも同一の管理データを保持することを保証すること。また、同期操作によるマスターメタデータサーバの処理低下を最小限とするよう考慮すること。

- 障害発生時におけるフェイルオーバ機能の実装
  マスターメタデータサーバの障害発生時に、スレーブメタデータサーバの中の１サーバをマスターメタデータサーバに昇格させ、そちらに接続を切り替えることにより、以降のファイルシステム操作を続行させる機能を実装する。マスターメタデータサーバの選出は自動ではなくても手動でもよいが、選出後は自動的にマスターメタデータサーバに昇格することが可能なようにすること。フェイルオーバ発生時にオープン中のファイルについては、できるだけ処理の続行が可能なようにすること。フェイルオーバは、クライアントからは透過的に実現すること。

(3)　高速ファイルコピー、複製作成機能（ステージング＋複製）

Gfarm ファイルシステムとスパコンのファイルシステムの間で多数ファイルを高速にコピーするための機能、複数拠点間で多数ファイルを効率的 に共有するために Gfarm ファイルシステムにおける複製を高速に作成する機能を設計、実装する。Gfarm ファイルシステム上の多数ファイルのアクセスは、物理的に異なるファイルシステムノードに格納されているファイルを並列にアクセスすることにより性能をスケールアウトさせることができる。高速化にあたり、その特性を利用し、スパコンのファイルシステムに対する高速コピー、拠点間での高速複製作成を実現すること。

具体的には以下の項目について、設計および開発作業を行うこと。

- スパコンのファイルシステムとの間の高速コピーの実装
  スパコンのファイルシステムと Gfarm ファイルシステムの間で、多数ファイルを高速にコピーするための機能を設計、実装する。物理的に異なるファイルシステムノードに格納されているファイルについては並列にアクセスすることにより性能がスケールアウトすることを利用し、まず、指定された多数ファイルの転送スケジューリン

グを検討すること。転送スケジューリング作成にあたり、ファイル複製も考慮し、適切なファイル複製を選択すること。決定した転送スケジューリングに従い、スパコンのファイルシステムと Gfarm ファイルシステムの間で多数ファイルの並列コピーを実装すること。

- 拠点間での高速複製作成の実装
  複数拠点間で多数ファイルを効率的に共有するため、Gfarm ファイルシステムにおける複製を高速に作成する機能を設計、実装する。スパコンのファイルシステムと Gfarm ファイルシステム間の高速コピーと同様に、転送スケジューリングを作成し、それに従いファイル複製を作成すること。ファイル複製作成において、空き容量の確認を行い、容量が溢れることのないようにすること。

(4) Gfarm ファイルシステム監視機能の高度化

Gfarm ファイルシステムは分散システムであり、多くのサーバ、ハードウェアにより構成されている。Gfarm ファイルシステムは、サーバやハードウェア障害についての耐故障性機能を有しているが、一方で障害の発生を検知するための監視機能は、障害を修復するためには重要である。また、Gfarm ファイルシステム的には正常に動作しているようでも、ハードウェア的には時々断などたまに発生するの障害により、性能に問題が出る場合もあり、監視機能を別途備えることは重要である。監視機能の高度化作業では、異常の検出に対し、チケットシステムなどと連動し異常の管理、メール発送などを可能とする。また、メタデータサーバの障害については必要であればシャットダウンを行うなど、スレーブメタデータサーバへの安全なフェイルオーバを可能とする。

具体的には以下の項目について、設計および開発作業を行うこと。

- チケットシステムとの連携
  監視機能によりソフトウェア、ハードウェアに異常が検出されたとき、チケットシステムに自動的に登録を行い、関係者にメール送付などを自動的に行うシステムを構築する。チケットシステムを含めパッケージ化を行い、導入作業を容易にすること。

- メタデータサーバ異常検出時のフェイルオーバ支援
  マスターメタデータサーバ、スレーブメタデータサーバに障害が発生した場合、障害をチケットシステムに登録するとともに、マスターメタデータサーバの障害に対しては安全にフェイルオーバができるよう、スレーブメタデータサーバの障害に対しては、必要な冗長性が保たれるよう支援を自動的に行う。具体的には、障害を起こしたマスターメタデータサーバのネットワークインターフェースを落とす、プロセスを安全に落とすなど、フェイルオーバが安全にできるよう支援する。スレーブメタデ

ータサーバの障害に対しては、予備のスレーブメタデータサーバを立ち上げるなど、必要な冗長性を保つよう支援する。

(5) Gfarm メタデータサーバ冗長化の信頼性向上(ホットスタンバイの信頼性向上)

フェイルオーバ発生時にオープン中のファイルについて、書き込みアクセスについても該当ファイルシステムノードに障害が発生しない限りは処理の続行を可能とする。さまざまなマスターメタデータサーバの障害に対しフェイルオーバを行えるよう負荷試験を行い、品質向上を図る。マスターメタデータサーバの障害時、スレーブメタデータサーバの中からマスターメタデータサーバに昇格するサーバを選出する必要あるが、その選出の自動化を行う。マスター選出の自動化を行うことにより、フェイルオーバの際の新しく書き込みアクセスを行うプロセスのブロック時間の短縮を図る。

具体的には以下の項目について、設計および開発作業を行うこと。

- Gfarm 自動ファイル複製機能の高度化
  Gfarm バージョン 2.4.1 における自動ファイル複製作成では、作成先のファイルシステムノードに障害が発生した時などは、自動ファイル複製作成をあきらめ、必要な数のファイル複製が作成されない。また、自動ファイル複製作成先のノードについて、何も指定することはできず、どこに作成されるか分からない。また、ファイルシステムノードに障害が発生した場合など、そのノードに格納されているファイル複製は失われるため、必要な数のファイル複製がない状態となってしまう。これらの問題を解決するための設計と実装を行い、自動ファイル複製機能の高度化を行う。

(6) その他の運用ツール

上記以外に整備検討が必要な利用者ツール、インターオペラビリティをテストする運用ツールを以下に示す。これらのツールについては次年度以降に実現可否を含め、再検討を行う。

- 利用者の Web ブラウザから、UNIX の一般的なファイル操作(cp,mv,rm 等)、ファイルの表示、ファイルのアップロード/ダウンロード等の操作が容易に行えること。また、これらの処理はユーザアカウント権限で実行できること。
- ファイル監査機能(ファイルごとのアクセス件数の取得、アクセス履歴の取得)
- 一クライアントからの一定量のアクセス要求に対し、全系スローダウンしない仕組みの検討(キーワード:アクセス量制限[QoS]、フローコントロール)
- ユーザ操作ミスで削除したファイルの復旧(アーカイブ、スナップショット)

6　整備計画

平成 23 年度、平成 24 年度の HPC ストレージ整備計画を表 6-1 に示す。

平成 23 年度は試験評価期間（仮運用期間）と考え、まずは東京大学の大規模ストレージを中心に HPC ストレージの整備、運用ドキュメント類の充足化を図る。

平成 24 年度は仮運用期間の課題フィードバックと必要に応じて是正処理を施した上、平成 24 年 11 月の HPC ストレージ本運用までに Gfarm ファイルシステムの機能エンハンスを行う。各基盤センタ（資源提供サイト）からのストレージ資源提供も順次受け付け、HPC ストレージを拡張していく計画である。

表 6-1 HPC ストレージ整備計画

	H23/1Q	2Q	3Q	4Q	H24/1Q	2Q	3Q	4Q
マイルストーン	--------▽仕様検討							
		----------▽基盤整備						
								----------▽仮運用
								△本運用
基本仕様	--------▽基本設計							
		--------▽東大整備（インフラ、マニュアル）					段階的に追加	
					拠点追加 --▽▽▽▽▽▽			
拡張仕様		----------▽Gfarm エンハンス						
			----------▽運用ツール整備					
					▽ホットスタンバイサポート			
					----------▽評価、調整			

7　必要経費

HPC ストレージのドキュメント整備、運用・保守に関する経費について、参考見積もりをベースに以下に記載する。

7.1 導入、保守作業費用

(1)　平成 23 年度

平成 23 年度の HPC ストレージの導入、保守作業費用を以下に示す。

HPC ストレージ構築では東京大学の大規模ストレージを中心とした HPC ストレージの構築作業を行う。また、ここでのマニュアル整備は HPC ストレージを構築する前提での費用見積りとなる。HPC トレージの構築作業とは別にマニュアル整備などのドキュメント作成のみを対応することは難しいため、発注仕様では構築作業とマニュアル整備を一式で発注する必要があると考える。

作業項目	期間	費用	備考
HPC ストレージ構築	2011/8～2011/10	¥5,534,000	一括
マニュアル整備	2011/8～2011/10	¥1,845,000	一括
運用保守	2011/11～2012/3	¥2,306,000	一括

平成 23 年度（小計）¥9,685,000

(2)　平成 24 年度

平成 24 年度の HPC ストレージの導入、保守作業費用を以下に示す。

HPC ストレージ再構築には平成 23 年度～平成 24 年度に実施する Gfarm エンハンス版の再インストールと、各基盤センタ（資源提供サイト）からのストレージ資源提供の伴う HPC ストレージの拡張作業が含まれる。

作業項目	期間	費用	備考
HPC ストレージ再構築	2012/8～2012/10	¥7,200,000	一括
マニュアル改版	2012/8～2012/10	¥2,400,000	一括
運用保守	2012/4～2013/3	¥600,000	月額

平成 24 年度（小計）¥16,800,000

7.2 運用ツール群の開発

運用ツール群として、平成 23 年度と平成 24 年度に段階的に Gfarm ファイルシステムのエンハンスを予定している。以下に開発を予定する機能、費用を示す。

作業項目	期間	費用	備考
メタデータサーバ冗長化 (ホットスタンバイ)	平成 23 年度	¥13,835,000	スレーブメタデータサーバへの管理データ同期、障害発生時の自動フェールオーバ
高速ファイルコピー、複製作成機能(ステージング＋複製)	平成 24 年度	¥10,000,000	スパコンのファイルシステム間との高速ファイルコピー、拠点間での高速複製作成
監視機能の高度化		¥10,000,000	チケットシステムとの連携、メタデータサーバ異常検出時のフェールオーバ支援
性能評価ツール一式		¥10,000,000	
ホットスタンバイの信頼性向上		¥15,000,000	
自動ファイル複製機能の高度化		¥15,000,000	自動ファイル複製の作成先ポリシー追加、FS 障害時の複製データを自動配布

平成 23 年度(小計) ¥13,835,000

平成 24 年度(小計) ¥60,000,000

[付録]

1 用語集

[1] HPCI 事務局
HPCI 利用の課題審査を行う組織

[2] HPCI アカウント IdP 運用機関
HPCI 環境に(シングル)サインオンするためのアカウントを発行・管理する組織(例:情報基盤センター, 国研, 商用プロバイダ)

[3] 資源提供機関
HPCI のユーザに対して計算機やストレージ等の資源を提供する組織(例:情報基盤センター, 国研)

[4] 認証ポータル運用機関
HPCI 環境に(シングル)サインオンするための認証ポータルを運用する組織(例:情報基盤センター, 国研)

[5] 認証局運用機関
HPCI 環境上で利用される電子証明書を発行する組織

[6] HPCI ID
HPCI 利用者に配布されるユニークな ID 番号。HPCI 上の資源を利用するためのアカウントではない。HPCI を利用するユーザ毎に発行されるユニークな ID。所属組織が変わっても HPCI ID は変わらない.

[7] HPCI アカウント
HPCI 環境に(シングル)サインオンするためのアカウント(OpenID や Shibboleth など)

[8] ローカルアカウント
資源提供機関の資源を利用するためのローカルアカウント(UNIX アカウント)

[9] クライアント証明書
ユーザ毎に認証局から発行される証明書(GSI 認証を行う場合に必要)NAREGI-CA

[10] HPC ストレージ
HPCI で整備する共有ストレージ(分散ファイルシステム)を指す

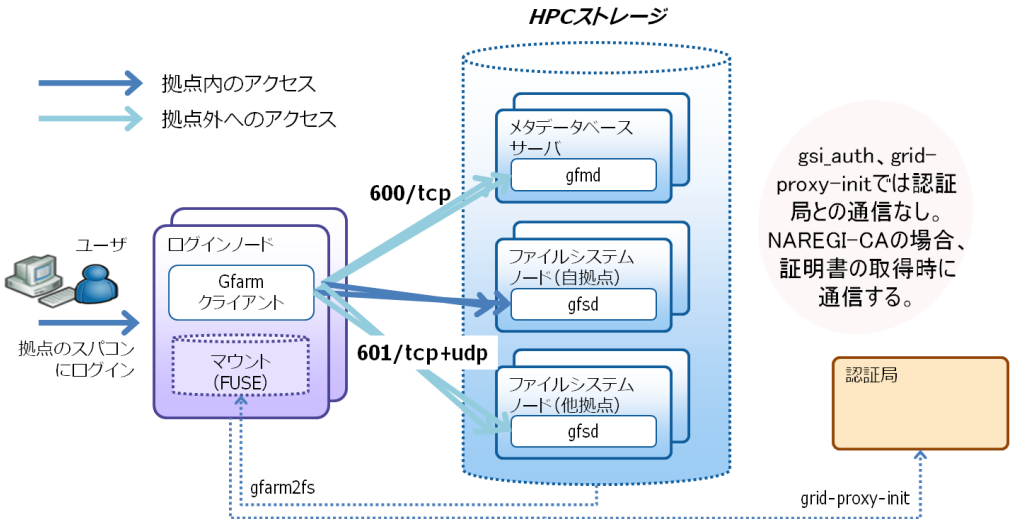
[11] ログインノード
各拠点スパコンにユーザがログインするノード(会話処理部)を指す。

2　利用 TCP ポート、UDP ポート

HPC ストレージ（Gfarm ファイルシステム）で利用する TCP/UDP ポートを以下に示す。

ポート番号	用途	備考
600/tcp	gfmd（Gfarm メタデータデーモン）	拠点 F/W 間での通信
601/tcp 601/udp	gfsd（Gfarm ファイルシステムデーモン）	拠点 F/W 間での通信

各拠点に設置される共有ストレージ群（Gfarm メタデータサーバノード、ファイルシステムノード、クライアント）は、各々の拠点リソースにアクセス可能な広域ネットワーク網（SINET4)に接続しなければならない。また、全てのログインノード（Gfarm クライアント）と、メタデータベースサーバノード、ファイルシステムノード間でファイル共有のための通信が行われるため、他拠点の共有ストレージ群との通信用に、自拠点のファイアウォール設定変更が必要となる。



3　ファイル暗号化

ファイルを暗号化する方法を以下に紹介する。HPC ストレージ上のファイルの暗号化は、ログインノード上で実行されることから、以下のコマンド実行は拠点ログインノードの環境に準ずる。

No.	コマンド	暗号化	復号化
1	zip パスワード設定	○パスワード設定 $ zip -m -e secret.txt.zip secret.txt	○パスワード設定解除 $ unzip secret.txt.zip
2	openssl 共通鍵暗号	○AES 暗号化 $ openssl enc -e -aes256 -in secret.txt -out secret.enc	○復号 $ openssl enc -d -aes256 -out secret.txt -in secret.enc

3	openssl
	公開鍵暗号
		○秘密鍵の作成
		$ openssl genrsa -out private.key
		○公開鍵の作成
		$ openssl rsa -in private.key -pubout -out public.key
		○公開鍵で暗号化
		$ openssl rsautl -pubin -inkey public.key -in secret.txt -encrypt -out secret.rsa.txt
			○秘密鍵で復号
			$ openssl rsautl -inkey private.key -in secret.rsa.txt -decrypt -out secret.txt
			※

4	gpg（GnuPG）
	公開鍵暗号
		○秘密鍵の作成
		$ gpg --gen-key
		○鍵のリスト表示
		$ gpg --list-key
		○公開鍵の作成
		$ gpg -a -o yyoshi_public.key --export yyoshi
		○公開鍵の信用証明の作成
		$ gpg --export-ownertrust > yyoshi_trust
		○公開鍵のインポート
		$ gpg --import yyoshi_public.key
		○公開鍵の信用証書のインポート
		$ gpg --import-ownertrust yyoshi_trust
		○ファイル暗号化
		$ gpg -e -a -r yyoshi@jp.fujitsu.com secret.txt
		→暗号化されたファイル（secret.txt.asc）が作成される。
			○ファイルを復号化
			gpg secret.txt.asc
			
			※ファイルサイズが大きいと、キーサイズ大きすぎると言われ、暗号化できない。
			回避策が不明。
			RSA operation error
			3740:error:0406D06E:rsa routines:RSA_padding_add_PKCS1_type_2:data too large for key size:rsa_pk1.c:151:

（添付資料 2）

HPCI 基本仕様

― ユーザ管理支援編 ―

1 目次

1　概要

本基本仕様書は，計算・ストレージ資源利用のための基本仕様である。本策定に当たっては，「準備段階におけるコンソーシアム」での検討を踏まえ，HPCI の整備に必要な機能を明確にし，HPCI の基礎的な仕様をまとめたものである。開発項目は，2011 年 3 月時点で詳細仕様が決められるもののみとし，詳細仕様が作れない開発項目は研究開発項目としている。本基本仕様書は，ストレージ共有，ユーザ管理支援，先端ソフトウェア運用基盤，認証基盤の 4 項目のうち，ユーザ管理支援について基本仕様を定めている。他の 3 項目については，それぞれ別の文書としてまとめられている。

- ストレージ共有

  平成 22 年度最先端研究基盤事業として「e-サイエンス実現のためのシステム統合・連携ソフトウェアの高度利用促進」で，東京大学情報基盤センターおよび理化学研究所計算科学研究機構に設置される大規模ストレージ，さらに今後各資源提供機関から提供されるストレージあるいはポータルシステムとの連携に必要とされる共通システムソフトウェア基本仕様を決め，運用に向けての整備計画，運用体制ならびに運用経費について検討した。

- ユーザ管理支援

  計算資源群の利用認可に必要となる事務手続きフロー，アカウンティング，障害対応などのユーザ利用管理支援に必要となるソフトウェア整備および運用に関して調査検討した。本仕様書を策定するにあたって，既にテスト運用されているグリッド連携の経験を元に事務手続きフロー策定手順およびスケジュール，さらに運用に必要とされる費用を検討した。また，各資源のアカウンティング情報集約機構や迅速な障害発見対応に帰するソフトウェアの必要性について検討し，運用に向けての整備計画，運用体制ならびに運用経費について検討した。

- 先端ソフトウェア運用基盤

  計算資源群が共通先端ソフトウェアを共有して運用できる基盤に必要となるソフトウェア整備および運用に関して調査検討した。平成 24 年度の本格運用時までに成熟していないミドルウェアに関しては，開発のための環境が必要になると予想される。VM(Virtual Machine)技術を利用して実運用環境と隔離した実験環境を提供する環境を基本仕様とした。また，平成 24 年度以降の本格運用後にも適時新しい先端ソフトウェアを各計算資源群で利用できるようにソフトウェアの配布機構も必要である。これら環境の詳細設計計画，整備計画，運用体制ならびに運用経費について検討した。

- 認証基盤

HPCI 上の資源を利用するユーザの認証および認可を実現するための認証基盤の利用シナリオ，システム整備および運用について調査検討した。HPCI を利用するコミュニティは多岐にわたることが予想されるため，複数の利用シナリオを想定し，これらの実現に必要なシステムや運用体制を検討した。次にこれらの検討結果より，平成 23 年度に運用開始可能な利用シナリオを決定し，これを実現するための認証基盤として Shibboleth および GSI 認証（※用語集参照）を用いた認証基盤アーキテクチャのシステム整備および運用体制について検討した。

本仕様書は，スーパーコンピュータ施設を有し共同利用・共同研究拠点として活動している東京大学および SINET を運営している国立情報学研究所が主幹し，共同利用・共同研究拠点である北海道大学，東北大学，東京工業大学，名古屋大学，京都大学，大阪大学，九州大学，筑波大学，および京速コンピュータ「京」運用機関である理化学研究所計算科学研究機構と連携して，HPCI 構築に関する基本仕様について調査検討した結果に基づいて作成されている。

2 利用シナリオ

2.1 HPCI 利用の概要

ここでは利用者が HPCI 環境を利用する際の手続きの概要について述べる。まず，予備知識として HPCI 環境における各種のアカウント，利用課題および各機関の役割の概要について述べ，次いで HPCI-ID の取得，利用課題申請から利用終了までの HPCI 利用の流れについて示す。

2.1.1 HPCI-ID と各種アカウント

まず以降の議論を正しく理解するために必要な HPCI-ID (利用者に対して一意に割り当てられる識別番号)，HPCI アカウント (HPCI 環境にサインオンするためのアカウント)，ローカルアカウント (HPCI に提供された資源にアクセスするための UNIX アカウント)，証明書の概念と，相互の関係を整理する(図 2.1)。

アカウント	発行元	ユーザ毎の取得数	備考
HPCI ID	HPCI事務局	1個／1ユーザ	HPCI事務局から1個取得.
HPCIアカウント	HPCIアカウントIdP運用機関	m個／1ユーザ	HPCIアカウントの種別（Shibboleth, OpenID等）毎に取得，HPCI IDにひも付けられる.
ローカルアカウント	資源提供機関	n個／1ユーザ	資源提供機関毎に取得，HPCIアカウントにひも付けられる.
証明書	認証局運用機関	1個／1ユーザ	認証局から1個取得. HPCI IDにひも付けられる.

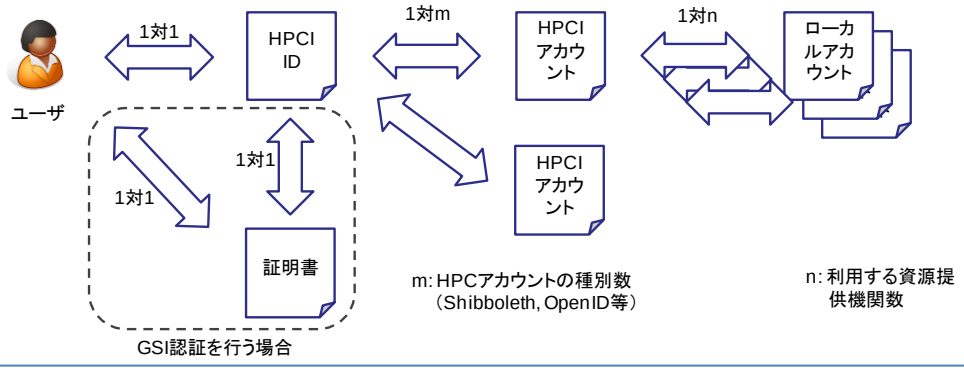


図 2.1: HPCI-ID, HPCI アカウント, ローカルアカウント, 証明書の相互の関係

【共通視点】

- 一人の HPCI 利用者(ユーザ)に対して一個の HPCI-ID が割り当てられ，その HPCI-ID にひも付けられた証明書が認証局から発行される。
- ユーザは Shibboleth や OpenID など異なる認証方式ごとに HPCI アカウントを取得することができ，それらの HPCI アカウントはユーザの HPCI-ID にひも付けられて管理される。
- 資源提供機関の資源を利用するためのローカルアカウントは HPCI アカウントにひも付けられるが，一人のユーザが複数の HPCI アカウントを所持しているとき，それぞれの HPCI

アカウントにより利用可能となる資源は異なっているものとし，同じ資源を異なる認証方式でサインオンして利用することは想定しない。

- ユーザが複数の HPCI 利用課題に属している場合，どのようにローカルアカウントを割り当てるかについては，各資源提供機関におけるグループ管理方式を踏まえてさらに検討する必要がある。

平成 23 年度検討事項

- HPCI-ID が一人の利用者にただひとつ割り当てられることを保証するための詳細な業務手順を決定する必要がある。この業務を簡素化するためには，HPCI-ID の交付申請にあたって，個人の識別が可能な番号を援用することが考えられる。本文書では e-Rad 研究者番号を用いることを想定しているが，詳細に関しては引き続き検討を行う。また，そのような個人識別番号をまだ取得していない者・雇用条件などにより取得が制限される者に対しては代替の個人識別番号が利用できるようにするなどの配慮も必要である。
- HPCI 利用資格の有無を確認する方法，および HPCI-ID の申請時に登録した個人識別番号が確かに申請者の所有するものであることを確認する方法についてもさらに検討が必要である。
- e-Rad 研究者番号の取得が制限される者が，その代替個人識別番号を用いて HPCI-ID を取得し，その後 e-Rad 研究者番号を取得した場合，あるいは e-Rad 研究者番号を所有しているときに HPCI-ID を取得し，その後 e-Rad 研究者番号を失効させ，代替個人識別番号を用いる場合の取り扱いに関しても検討が必要である。
- HPCI の提供する資源を利用する資格を失った者や，HPCI を利用しなくなったまま長期間経過したため当該 HPCI-ID を存続させることが適切かどうかの判断が困難となった者などに対する失効処理の手続きも，決定する必要がある。
- 本文書では HPCI-ID を取得した者が，有効期間（10 年を想定）が経過した後も継続して HPCI 環境を利用するには HPCI-ID の更新を行うものと想定している。また，HPCI-ID 取得時に登録した属性に変更が生じた時には，HPCI-ID を取得した本人が適切に属性変更の手続きを行うものと想定している。これらのような HPCI-ID を取得した者の責務に関しても検討が必要である。
- HPCI-ID の具体的な形式や生成規則なども平成 23 年度に検討を行う。
- HPCI-ID に関するこれらの検討内容は後述する HPCI-ID 運用規定（案）に反映されるものとする。

2.1.2 HPCI 利用課題

HPCI 環境を利用するには，課題審査委員会により利用を承認された HPCI 利用課題のいずれかに，課題実施者として登録されている必要がある。ここでは HPCI において公募される利用課題の概要を述べる。

【共通視点】

- HPCI 事務局が行う利用課題公募の要項に従って**HPCI 利用課題申請**を行う。表 2.1 に申請の種別を示す。

表 2.1 HPCI 利用課題の代表者が行う申請の種別

区分	内容	時期
新規課題申請	HPCI が提供する資源を用いて行う研究開発を実施するための初回の申請(通常の利用期間は当該年度末まで)	HPCI 事務局が利用課題の公募を行う期間
継続課題申請	すでに採択され利用していた課題を利用期間の終了後(通常は翌年度)も継続するための申請	HPCI 事務局が利用課題の公募を行う期間
課題変更申請	その課題に所属する課題実施者の変更を行うための申請	採択された利用課題による利用が終了する前まで

- 本文書では，利用課題申請に当たりあらかじめ代表者，副代表者(少なくとも 1 名)，連絡責任者の選出を行い(副代表者，連絡責任者は代表者が兼務しても良い)，代表者が申請を行うことを想定している。
- 新規・継続申請の場合，HPCI 事務局(あるいはそれが諮問する課題審査委員会)による審査の結果，利用が承認される。
- 利用が承認された場合に，各資源が利用できる期間は，当該年度末(ただし，資源の提供機関が別途期限を定めたときはその期限)までとする。
- HPCI で公募される利用課題の区分は運営規則等で別途定められることになる。本文書では，表 2.2 に示すような区分を想定し，その処理に必要となる申請・審査・利用登録等の業務について記述する。

表 2.2 本文書で想定する HPCI 利用課題の区分

区分	利用負担金	備考
無償型	全額免除	従量制利用負担金を採用している資源提供機関における利用の場合には上限額が定められることがある。また，HPCI 事務局(あるいはそれが諮問する課題審査委員会)による審査の結果，下に述べる利用負担金減免型あるいは全額有償型での利用を条件とした採択と判定されることがある。
利用負担金減免型	一部免除	免除されない金額もしくは授与された利用枠を超過

		して利用した場合の利用負担金は，課題の代表者が負担するものとする。ただし，HPCI 事務局（あるいはそれが諮問する課題審査委員会）による審査の結果，次に述べる全額有償型での利用を条件とした採択と判定されることがある。
全額有償型	すべて代表者が負担	

- 利用を承認された場合でも，課題区分に関する審査結果が受け入れられない場合に利用申請を取り下げることもできる。
- 一人の利用者が同時に複数の利用課題に所属することがあってもよい。

2.1.3 HPCI 環境の運用に関わる各機関の役割

ここでは，HPCI 環境の運用に関わる機関のうち HPCI 事務局，資源提供機関，プライマリセンター，資源提供連携ネットワーク委員会についてそれぞれの役割の概要を示す。この他に認証局運用機関や認証ポータル運用機関などがあるが，それらについては巻末の用語集および HPCI 基本仕様書「認証基盤編」を参照すること。

2.1.3.1 HPCI 事務局の役割

【共通視点】

- **HPCI 事務局**は，以下の役割を果たさなければならない。
  - HPCI-ID の発行・管理
  - 別途定められる失効の要件に基づく HPCI-ID の失効処理と，関係先への通知
  - HPCI 利用課題申請の公募
  - HPCI 利用課題の審査（利用負担金減免の審査を含む）
  - 申請者に対する，採否・利用の可否・利用負担金減免の可否の通知
  - 採択された各課題に関する情報の認証局運用機関・資源提供機関への通知
  - 各利用課題の代表者が提出する利用報告書の取りまとめと情報公開
  - HPCI の活動のために必要な広報活動
  - ヘルプデスク業務
  - 情報共有 CMS の運用

2.1.3.2 資源提供機関の役割

【共通視点】

- **資源提供機関**は，以下の役割を果たさなければならない。
  - 提供する資源の決定と HPCI 事務局への通知

・ 採択された利用課題の利用者に対するローカルアカウントの発行と，資源の提供
・ 利用統計情報の採取とHPCI 事務局への報告
・ HPCI 利用者に対する支援活動（利用の手引きの整備，利用に関する問い合わせへの対応など）

2.1.3.3 プライマリセンターの役割

【共通視点】

- 平成 23 年度は，Shibboleth 認証連携を用いたシングルサインオン環境が提供される。この認証連携方式においては，個々の利用課題ごとに，資源提供機関のいずれかがHPCI アカウント IdP 運用機関と認証ポータル運用機関の役割も果たす。ただし，これは当該利用課題に資源を提供する機関でなくともよい。この機関を当該利用課題の**プライマリセンター**と呼ぶ。プライマリセンターは，その利用課題とその利用者に関し，以下の役割を果たさなければならない。
  - ・ HPCI アカウント IdP 運用機関として，当該課題の利用者に対する電子証明書発行のための本人確認。本人確認の手続きに関しては後述する(2.3.1 節)。
  - ・ HPCI アカウント IdP 運用機関として，当該課題の利用者に対する HPCI アカウントの発行
  - ・ 認証ポータル運用機関として，認証ポータルの運用

2.1.3.4 資源提供連携ネットワーク委員会

【共通視点】

- 資源提供連携ネットワーク委員会は以下の役割を果たす。
  - ・ HPCI に提供する資源の運営責任を持つ。
  - ・ 各資源提供機関が提供する提供資源リストを管理する。
- 詳細に関しては平成 23 年度に検討する。

2.1.3.5 その他

【共通視点】

- HPCI 環境の運用に参画する各機関は以下の役割を果たす
  - ・ インシデント・レスポンス・チーム担当者を割り当て，HPCI 全体としてのセキュリティ・インシデントの対応を行う。
- 以下の役割を果たす機関に関しては，平成 23 年度に検討する。
  - ・ 開発チームの組織・運営

2.1.4　HPCI 利用の流れ

初めて HPCI 環境を利用しようとする者が実際に HPCI 環境の資源を利用可能となるために必要な手続きの概要を図 2.2 に示す。

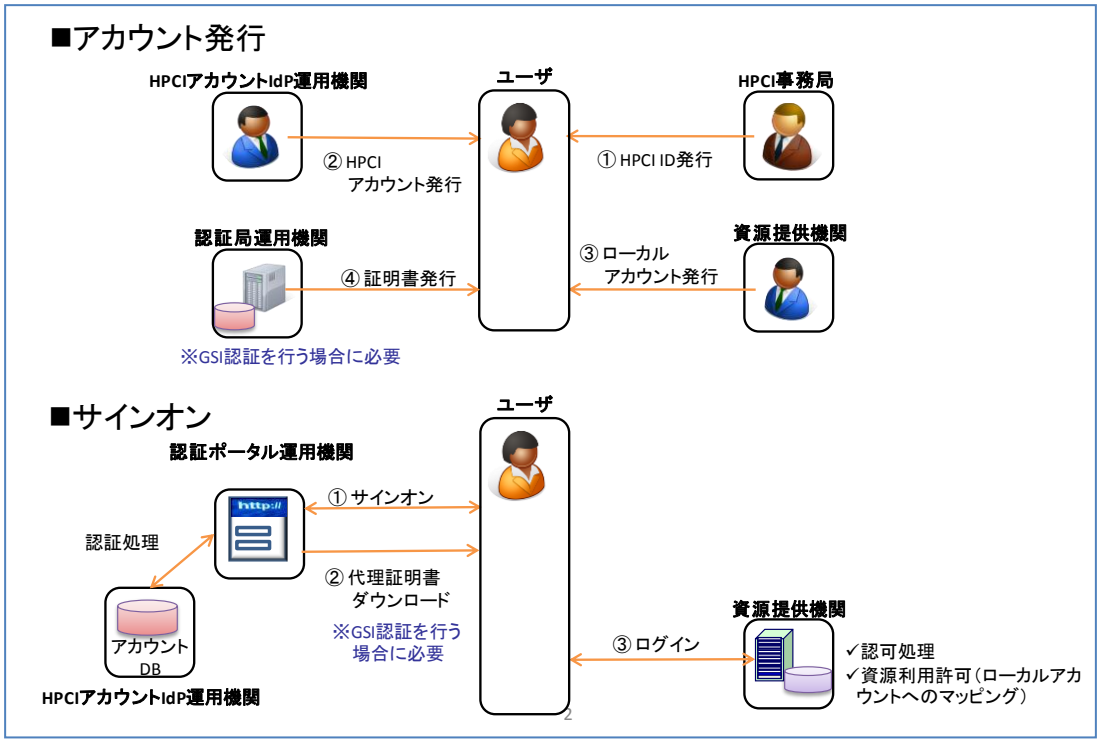


図 2.2 HPCI 利用に必要な手続きの概要

アカウント発行に関する諸手続きについては，2.1.4.1，2.2 および 2.3 節で，サインオンの詳細に関しては HPCI 基本仕様書「認証基盤編」を参照すること。

2.1.4.1　　利用課題申請から利用終了までの流れ

【共通視点】

- HPCI 環境の利用を希望する者が，申請に先立って HPCI-ID を準備し，HPCI 利用課題申請を行い，提供される資源を利用し，その利用を終了するまでの流れの概要を，図 2.3 に示す。

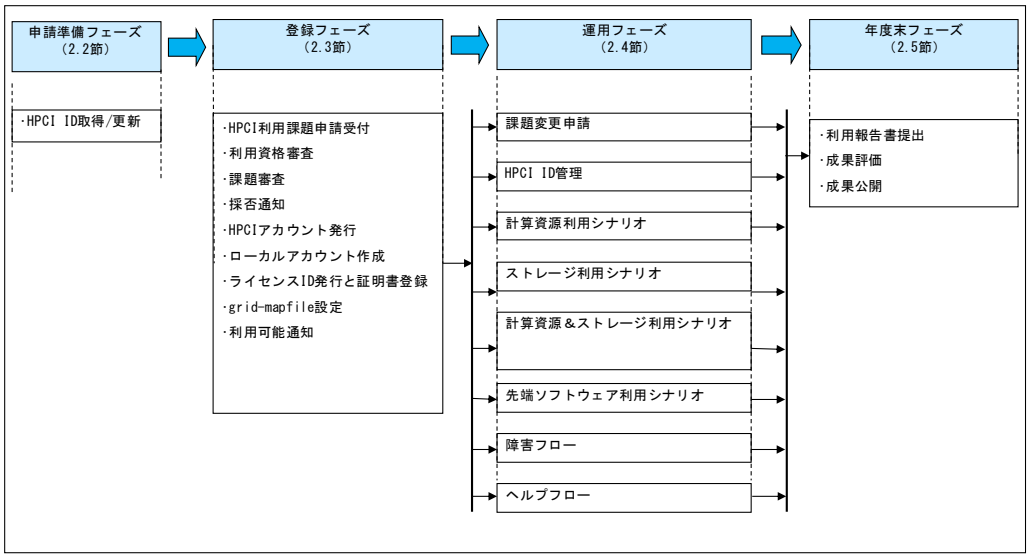


図 2.3 利用課題申請から利用終了までの大まかな流れ

- 図 2.3 における申請準備・登録・運用・年度末の4つのフェーズは，この順序で直列に進行する。
- 登録フェーズ内で行われる処理は，図 2.3 に示した順序で直列に進行する。この詳細は，2.3 節で述べる。2.1.2 節の表 2.1 に示した申請区分のうち，新規課題申請・継続課題申請はこのフェーズにおいて受理され処理される。
- 運用フェーズ内で行われる処理は，それぞれが並列に進行する。この詳細は 2.4 節で述べる。図 2.3 のそれぞれのシナリオは，2.4.1 節から 2.4.6 節に対応している。2.1.2 節の表 2.1 に示した申請区分のうち，課題変更申請はこの運用フェーズにおいて受理され処理される。
- 年度末フェーズ内で行われる処理は，図 2.3 に示した順序で直列に進行する。この詳細は，2.5 節で述べる。

2.2 申請準備フェーズ

HPCI で提供される計算機資源・ストレージ資源を利用しようとする者は，利用課題申請に先立って，申請する利用期間の終了まで有効な HPCI-ID を所有している必要がある。これらの処理はそれぞれの利用者が個人単位で行う。申請により発行された HPCI-ID と申請者の属性情報は HPCI-ID 管理簿により管理される。

申請準備フェーズでの処理の流れを図 2.4 に示す。図中の各ステップについての詳細は 2.2.1 および 2.2.3.2 節で説明する。

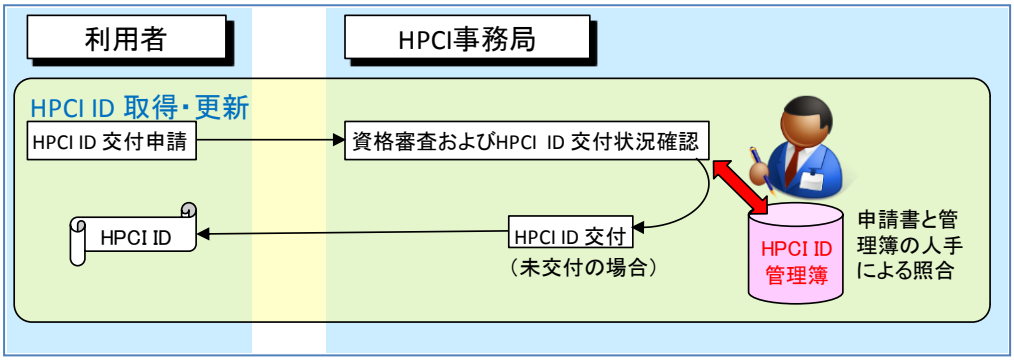


図 2.4 申請準備フェーズの処理の流れ

また，HPCI 事務局の作業量を軽減するために，HPCI-ID の申請処理を自動化する方式案の検討も行った。この案では HPCI-ID の新規発行や有効期間の更新は Web ポータル(HPCI ポータル)を介して行い，HPCI-ID 管理簿との照合作業などを自動化する。詳細に関しては平成 23 年度に引き続き検討を行う。図 2.5 に Web ポータルによる申請処理の省力化案での処理の流れを示す。

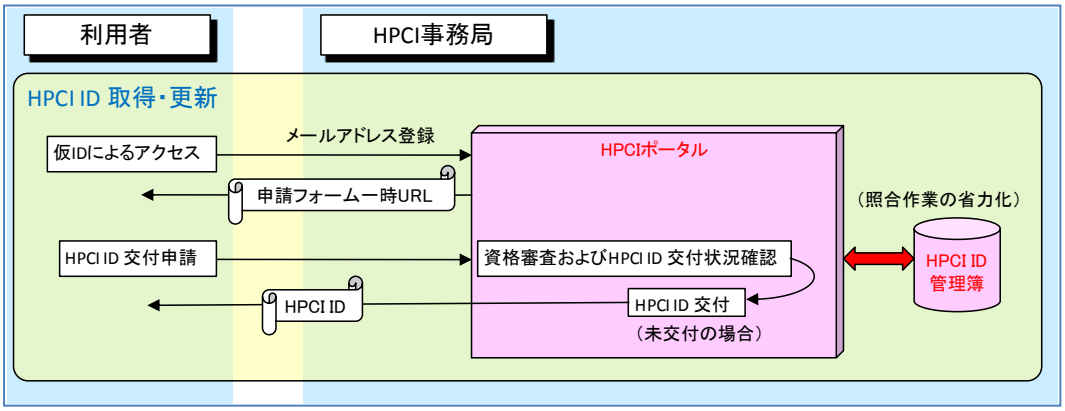


図 2.5 Web ポータルによる申請処理の省力化案

2.2.1 HPCI-ID の新規登録申請

【利用者視点】

- 申請に必要な e-Rad 研究者番号あるいはその代替個人認識番号を準備する。

- 申請用 Web フォームの URL にアクセスし，HPCI-ID 新規発行申請処理を実行する。

【HPCI 事務局視点】

- 入力された内容をチェックし，必須入力項目に未入力または形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力された内容をチェックし，e-Rad 研究者番号あるいはその代替個人認識番号に未入力あるいは形式エラーを検出したら，エラー表示を行い，再実行を促す
- HPCI-ID 管理簿を参照し，入力された e-Rad 研究者番号あるいはその代替個人認識番号の重複を検出したら，重複先の HPCI-ID を含めて検証を行う
- 入力内容に問題がなければ，資格審査および HPCI-ID 交付状況の確認を行い，未交付の場合は新しい HPCI-ID の発行を行い，申請者に通知する。

2.2.2 HPCI-ID の属性変更・更新申請

【利用者視点】

- 所有する HPCI-ID の有効期限を延長する，あるいは HPCI-ID 取得時に登録した所属・連絡先などの属性が変更になった場合，HPCI-ID の変更申請を行う。
- 申請用 Web フォームの URL にアクセスし，HPCI-ID 変更申請処理を実行する。

【HPCI 事務局視点】

- 入力された内容をチェックし，必須入力項目に未入力または形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力された内容をチェックし，e-Rad 研究者番号あるいはその代替個人認識番号に未入力あるいは形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力された HPCI-ID と e-Rad 研究者番号あるいはその代替個人認識番号が HPCI-ID 管理簿に登録されている情報との不一致を検出したら，入力された HPCI-ID，e-Rad 研究者番号あるいは代替個人識別番号を含めて検証を行う
- 入力内容に問題がなければ HPCI-ID 管理簿の内容を入力値で更新する
- 更新した結果を申請者に通知する

【共通視点】

- 属性変更申請の場合に，本人による申請であることを確認する方法についてはさらに検討が必要である。

2.2.3 Web ポータルによる自動化案

Web ポータルを用いた自動化案における HPCI-ID の新規申請および変更・更新申請は以下の通りとなる。

2.2.3.1 HPCI-ID の新規登録申請

【利用者視点】

- 利用者は HPCI 事務局が HPCI ポータルへのサインオンに使用することを認めた認証プロバイダのアカウントを必要に応じて取得する。ここで使用できるアカウントとしては，情報基盤センターの全国共同利用アカウントや学認連携アカウントなどの Shibboleth IdP のアカウント，あるいは HPCI 事務局より認定された商用の OpenID IdP のアカウントを想定している。

- 上記のアカウントを用いて HPCI 事務局が提供する HPCI ポータルにサインオンし，申請用 Web フォームの一時 URL の送付先メールアドレスを当該アカウントの属性として登録する

【HPCI 事務局視点】

- 申請者が入力した IdP，当該 IdP でのアカウント，メールアドレスを HPCI-ID 管理簿に登録する
- 申請用 Web フォームの一時 URL を生成し，その URL が記載されたメールを入力されたメールアドレスに送付する

【利用者視点】

- 受信したメールに記載された申請用 Web フォームの一時 URL にアクセスし，HPCI-ID 新規発行申請処理を実行する。

【HPCI 事務局視点】

- 入力された内容をチェックし，必須入力項目に未入力または形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力された内容をチェックし，e-Rad 研究者番号あるいはその代替個人認識番号に未入力あるいは形式エラーを検出したら，エラー表示を行い，再実行を促す
- HPCI-ID 管理簿を参照し，入力された e-Rad 研究者番号あるいはその代替個人認識番号の重複を検出したら，重複先の HPCI-ID を含めて検証を行う
- 入力内容に問題がなければ新しい HPCI-ID および照合コード(利用課題申請時の HPCI-ID 入力を補助するために使用する)の発行を行い，Web 表示とともに，連絡先メールアドレスに HPCI-ID および照合コードが記載されたメール送信を行う。
- 一時 URL を生成後，一定時間が経過したら当該 URL を無効化する

2.2.3.2 HPCI-ID の属性変更・更新申請

【利用者視点】

- 所有する HPCI-ID の有効期限を延長する，あるいは HPCI-ID 取得時に登録した所属・連絡先などの属性が変更になった場合，HPCI-ID の変更申請を行う。
- 利用者は有効な HPCI アカウントを所有している場合は HPCI アカウントにより HPCI ポータルへサインオンする。有効な HPCI アカウントを所有していない場合，HPCI 事務局が HPCI ポータルへのサインオンに使用することを認めた認証プロバイダのアカウントを必要に応じて取得する。ここで使用できるアカウントとしては，HPCI-ID 新規発行申請時と同様に，情報基盤センターの全国共同利用アカウントや学認連携アカウントなどの Shibboleth IdP のアカウント，あるいは HPCI 事務局により認定された商用の OpenID IdP のアカウントを想定している。
- 上記のアカウントを用いて HPCI 事務局が提供する HPCI ポータルにアクセスし，申請用 Web フォームの一時 URL の送付先メールアドレスを登録する

【HPCI 事務局視点】

- 申請者が入力した IdP，当該 IdP でのアカウント，メールアドレスを HPCI-ID 管理簿に登録する
- 申請用 Web フォームの一時 URL を生成し，その URL が記載されたメールを入力されたメールアドレスに送付する

【利用者視点】

- 受信したメールに記載された申請用 Web フォームの一時 URL にアクセスし，HPCI-ID 変更申請処理を実行する。

【HPCI 事務局視点】

- 入力された内容をチェックし，必須入力項目に未入力または形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力された内容をチェックし，e-Rad 研究者番号あるいはその代替個人認識番号に未入力あるいは形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力された HPCI-ID と e-Rad 研究者番号あるいはその代替個人認識番号の不一致を検出したら，入力された HPCI-ID，e-Rad 研究者番号あるいは代替個人認識番号を含めて検証を行う
- 入力内容に問題がなければ HPCI-ID 管理簿の内容を入力値で更新する
- 一時 URL を生成後，一定時間が経過したら当該 URL を無効化する

【共通視点】

- 属性変更申請の場合に，本人による申請であることを確認する方法についてはさらに検討が必要である。

2.3 登録フェーズ

登録フェーズでの処理の流れを図 2.6 に示す。図中の 1: HPCI 利用課題申請受付から，9: 利用可能通知までの各ステップについての詳細は 2.3.1 節で説明する。

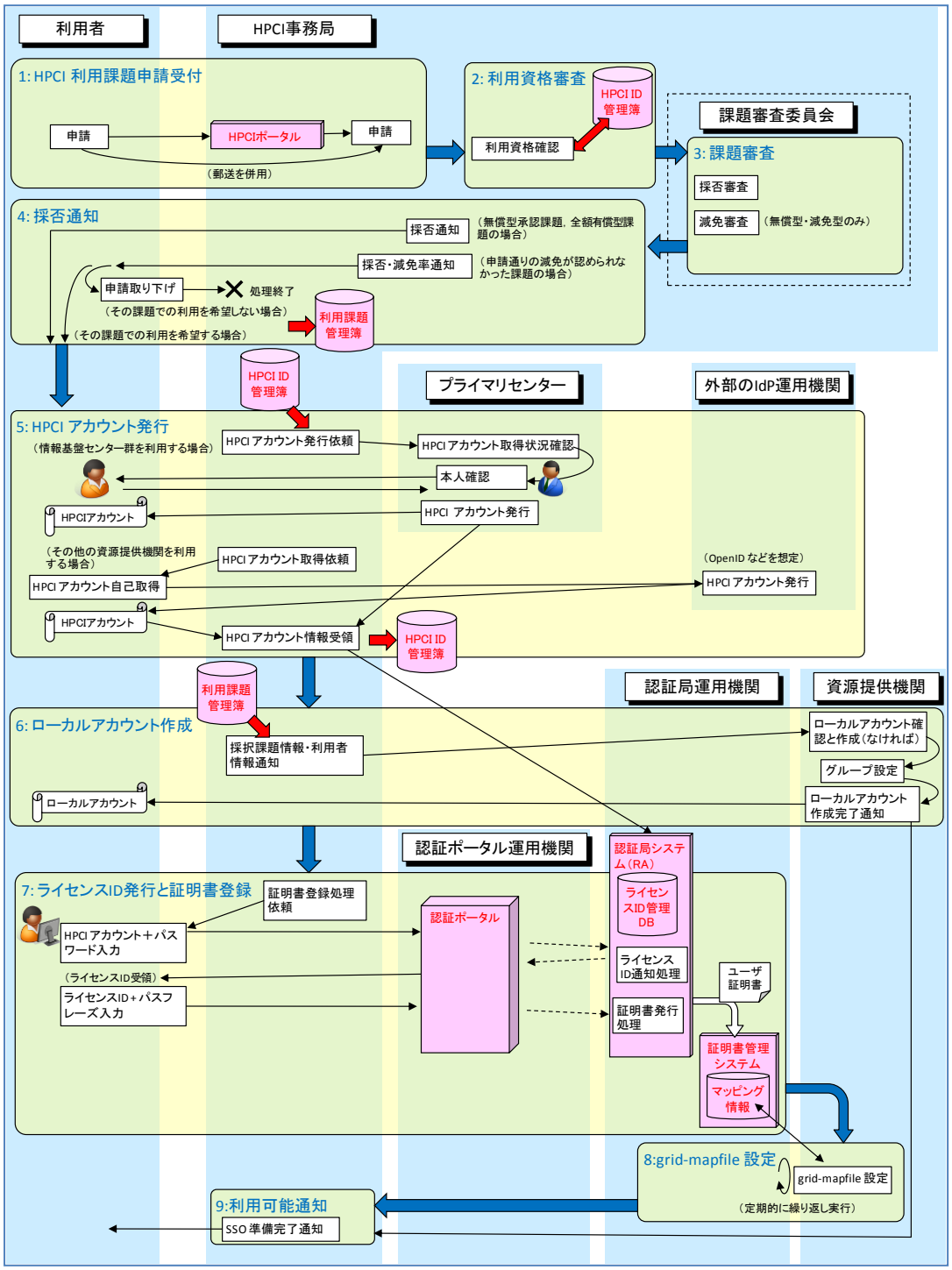


図 2.6 登録フェーズの処理の流れ

図中の 5: HPCI アカウント発行と 6: ローカルアカウント作成に関しては以下に示すような，資源ごとの HPCI アカウントおよびローカルアカウントの状況を考慮することとする。

【共通視点】

- HPCI 利用課題申請に先立ち，すべての課題実施者は，それぞれ事前に申請する利用期間を通して有効な HPCI-ID を保有していなければならない。申請時点でのそれぞれの課題実施者の HPCI アカウントおよびローカルアカウントについては，利用を希望する資源ごとに表 2.3 のような状況を想定する。

表 2.3 資源ごとの HPCI アカウント，ローカルアカウントの状況

	有効な HPCI アカウントを有している	有効な HPCI アカウントを有していない
有効なローカルアカウントを有している	以前に採択された利用課題の課題実施者として当該資源を利用しており，そのアカウントがまだ存続している。	当該資源を HPCI とは関係なく直接利用申請を行って利用しており，そのアカウントがまだ存続している。
有効なローカルアカウントを有していない	以前に採択された利用課題の課題実施者であるが，当該資源を利用していない。	当該資源を利用していない。

2.3.1 新規課題申請の処理

新規課題申請の処理は，以下の 1～9 の順序で進行する。申請された利用課題に関する情報は HPCI 利用課題管理簿により管理される。

1. HPCI 利用課題申請受付

【共通視点】

- 利用者は，HPCI 事務局が公表した公募要項に従って，利用課題申請書を提出する。申請書には以下の情報が含まれる。
  - 公募区分（無償型／負担金減免型／全額有償型の区別）
  - 申請区分（新規／継続の区別）
  - 課題代表者の氏名と HPCI-ID
  - 課題副代表者の氏名と HPCI-ID（最低 1 名）
  - 連絡責任者の氏名と HPCI-ID，連絡先
    （住所，電子メールアドレス，電話およびファックス番号）

・ 課題実施者の氏名とHPCI-ID，役割・担当分野
外国籍の実施者が含まれる場合は，国籍と現居住地と勤務年数（1 年未満の場合は月数）を補記
・ 研究課題名
・ 概要（研究目的，研究計画，これまでの業績・成果，準備状況など）
・ 利用を希望する資源提供機関（複数選択可），および，その機関が複数の資源を提供する場合には利用を希望する資源
・ 採択された場合のプライマリセンター（Shibboleth 認証を行う資源提供機関を利用しない場合は不要）
・ 利用負担金の一部もしくは全額を代表者が負担する場合の，経理手続きに必要な情報
・ 募集要項と記載内容への誓約確認
・ 課題実施者の本人確認情報

- Web ポータル上での申請処理自動化案では HPCI-ID は照合コードを用いて申請時に入力が正しいことを確認し，誤った HPCI-ID で申請が行われないようにする。

【利用者視点】

- 代表者は課題実施者全員の HPCI-ID を入手する。Web ポータル上での申請処理自動化案ではさらに，課題実施者全員の照合コードも入手する。
- 申請にあたっては，Web ポータルの課題申請ページ（重要事項の入力と所定の書式に従って作成した PDF ファイルの添付を併用する）を用いて申請書類のアップロードを行うとともに，押印したハードコピーを HPCI 事務局に送付する。

【HPCI 事務局視点】

- 利用者がアップロードしたデータと郵送された書類の照合を行い，次の利用資格審査および課題審査の処理に必要な準備を行う。

2. 利用資格審査

【HPCI 事務局視点】

- 当該申請課題のすべての課題実施者が利用資格を満たしていることを，HPCI-ID 管理簿によってチェックする。
・ この段階でのチェックは当該利用者の身分等を形式的に確認するものとなる。
・ HPCI-ID 管理簿に登録されている情報が正しいものであることは，本人性確認のための書類を提出できることにより判断できることとする。本人性確認のための書類には利用資格の有無を判定するための情報も含まれることとする。書類に不備があれば申請者に差し戻す。必要書類の詳細は平成 23 年度に検討する。
・ Web ポータル上での申請処理自動化案では HPCI-ID は申請時に照合コードによ

って正しく入力されているものとみなす。

3. 課題審査

【HPCI 事務局視点】

- 受理されて利用資格審査を経た利用課題申請を集約し，それらの審査を**課題審査委員会**に付議する。
- 課題審査委員会は，各利用課題の評点や順位などを判定し，採否を決定する。審査については別途運営規則等で定められるものとし，本文書では，以下のような判定が行われるものと想定する。
  - 無償型／利用負担金減免型の申請課題については，負担金減免の可否，および，申請通りの減免を認めない場合の利用者の負担割合または支払い金額も合わせて決定する。
  - 全額有償型課題については，採否の判定のみ。

4. 採否通知

【HPCI 事務局視点】

- 課題審査の結果を，代表者に通知する。
  - 無償型／利用負担金減免型の申請課題について，その希望が申請通りに認められなかった場合には，課題審査によって決定された利用者負担を受け入れるかどうかの意思を合わせて照会する。利用しない旨の回答があった課題は取り消しとして扱い，これ以降の処理は行わない。
  - 無償型または利用負担金減免型で申請通り承認された課題については，採否の通知のみ。
  - 全額有償型で承認された課題については，採否の通知のみ。

【利用者視点】

- 申請した公募区分のうちの無償型／利用負担金減免型がその申請通りに承認されなかった場合，代表者は，HPCI 事務局からの照会に対して，想定される利用負担金の支払いを行って利用する意思の有無を回答する。

【事務局視点】

- 課題審査の結果および申請者の利用意思の回答に基づき，利用課題管理簿を更新する。採択された課題に関しては，付与された統一グループ名，利用を承認された資源提供機関および資源の一覧を登録する。

5. HPCI アカウント発行

【HPCI 事務局視点】

- 当該課題が Shibboleth 認証を行う資源提供機関を利用する場合は，その課題のプライマリセンターに HPCI アカウントの発行処理を依頼すると同時に，課題連絡責任者にプライマリセンターにおいて本人確認の手続（後述）をするように連絡する。
- 当該課題が OpenID などを認証に用いる資源提供機関を利用する場合は，利用者に HPCI アカウントの自己取得を依頼する。

【プライマリセンター視点】（Shibboleth 認証の場合）

- 当該利用者の HPCI アカウント取得状況を HPCI 事務局から通知された情報に基づいて確認し，必要な処理を行う。
  - 本人確認の手続きとしては，身分証と利用資格を有することが確認できる書類（身分証で確認できる場合は身分証のみで良い）の複写を提示することを要件とする。
  - 有効な HPCI アカウントを保有している場合は，本人確認の手続きのみ行う。
  - 有効な HPCI アカウントを保有していない場合は，HPCI アカウントの発行と本人確認の手続きを行う。
  - 新規に発行した HPCI アカウントの情報を当該利用者に通知する。
  - HPCI アカウント IdP として提供する情報（英字氏名，HPCI-ID，eduPersonPrincipalName など）を更新する。
- 各利用者の HPCI-ID と HPCI アカウントを，HPCI 事務局に通知する。

【利用者視点】（OpenID などを用いる場合）

- HPCI 事務局からの依頼に応じて，外部の IdP 運用機関が発行する ID（アカウント）を用意する。すでに取得済みであれば，それを利用してよい。
- 自分の HPCI-ID と，取得した ID（当該利用者の HPCI アカウントとなる）を HPCI 事務局に報告する。
- OpenID などを用いる場合の利用資格を確認する手順については，さらに検討が必要である。

【HPCI 事務局視点】

- HPCI アカウントを HPCI-ID 管理簿に登録する。

【共通視点】

- 同一の利用者が複数の課題の新規メンバーとして同時に HPCI アカウントの発行を受ける場合，各課題のプライマリセンターが異なっていると，当該利用者に複数の HPCI アカウントが交付される可能性がある。このような場合でも証明書は1通しか交付されないような認証基盤を構築する必要がある。

6. ローカルアカウント作成

【HPCI 事務局視点】

- 各採択課題について，当該課題で利用する資源提供機関に，必要な情報を通知する。
  - その課題に付与された統一グループ名

・ その課題が利用を承認された資源提供機関およびその資源の一覧
・ 参加している全利用者の一覧(HPCI-ID, HPCI アカウント含む)

【資源提供機関視点】

- HPCI 事務局から送付された情報に基づき，各利用者に必要なローカルアカウントを用意する。
  ・ 当該利用者が，すでに有効なローカルアカウントを保持している場合には，それを流用してもよい。
  ・ ただし，その利用者が当該利用課題の経費負担によってその資源を利用できるよう，必要なグループ設定等を行う。
- ローカルアカウントが用意できたら，その旨を HPCI 事務局および課題連絡責任者に連絡する。
- ローカルアカウントと利用者の HPCI-ID の対応付けを行い，管理する。

7. ライセンス ID 発行と証明書登録

【HPCI 事務局視点】

- HPCI-ID と HPCI アカウント情報を認証局運用機関に通知する。

【認証局運用機関視点】

- 各利用者の HPCI アカウントに基づき，証明書の発行に必要な処理を行う。
- 証明書発行準備ができたら，HPCI 事務局にその旨を通知する。

【HPCI 事務局視点】

- 利用者に対し，認証ポータルにアクセスして証明書発行の手続きを実行するように通知する。

【利用者視点】

- HPCI 事務局からの通知に従い，認証ポータルにアクセスして，HPCI アカウントとパスワードを入力する。
- ライセンス ID がオンラインで通知されるので，認証ポータルにアクセスして証明書発行依頼手続きを実行する。

【認証局運用機関視点】

- HPCI アカウント IdP より，入力された HPCI アカウントに関する属性情報を取得し，ユーザ証明書を発行し，grid-mapfile 生成のためのマッピング情報とともに証明書管理システムに登録する。

8. grid-mapfile 設定

【資源提供機関視点】

- 認証局運用機関が生成した grid-mapfile 作成に必要なマッピング情報を取得し，自らが

管理する HPCI-ID とローカルアカウントの対応づけとあわせて，grid-mapfile を生成する処理を定期的に実行し，各提供資源の grid-mapfile を自動更新する。

9. 利用可能通知

【HPCI 事務局視点】

- 各利用者について，対象となる資源提供機関からのローカルアカウント作成完了通知を集約し，すべてがそろった時点で，利用を承認された資源の利用が可能となったことを通知する。

【利用者視点】

- 利用可能通知を受け取ったら，資源提供機関における grid-mapfile 更新サイクルを見計らってシングルサインオンによる資源利用が可能となったことを確認する。

2.3.2 継続課題申請の処理

継続課題申請の処理は，2.3.1 節の新規課題申請の処理と同様である。ただし，当該利用課題の各メンバーに対し，前年度に交付された証明書を失効させた後に翌年度の証明書が交付されるような仕組みを構築する必要がある。

2.4 運用フェーズ

2.4.1　課題変更申請の処理

課題変更申請の処理は，以下の各ステップからなる。

1. 申請受付

【共通視点】

課題変更申請には，以下の情報が含まれる。

- すでに利用を承認された課題実施者の情報の修正・変更を行う場合には，その内容
- 新たな課題実施者を追加する場合には，当該課題実施者の氏名，HPCI-ID，役割，担当分野

【利用者視点】

- 申請にあたっては，Web ポータルの課題変更申請ページ（重要事項の入力と所定の書式に従って作成した PDF ファイルの添付を併用する）を用いて申請書類のアップロードを行うとともに，押印したハードコピーを HPCI 事務局に送付する。

【HPCI 事務局視点】

- 利用者がアップロードしたデータと郵送された書類の照合を行う。すでに利用を承認された課題実施者の情報の修正・変更のみの場合には，利用課題管理簿等の修正を行い，変更申請の処理を終了する。
- 新たな課題実施者を追加する場合には，次の利用資格審査の処理に必要な準備を行う。

2. 利用資格審査

【HPCI 事務局視点】

- 当該メンバーの HPCI-ID が正当なものであるかを，HPCI-ID 管理簿を参照し，チェックする
- HPCI-ID を保有することが確認できないメンバーの場合は，申請者に差し戻す。

3. 新規課題申請の処理のステップ 5 に進む。

2.4.2　HPCI-ID の変更申請（変更）

2.2.3.2 HPCI-ID の属性変更・更新と同様の処理を実行する

2.4.3　HPCI-ID の廃止申請

【利用者視点】

- 申請用 Web フォームの URL にアクセスし，HPCI-ID 廃止申請処理を実行する。

【HPCI 事務局視点】

- 入力された内容をチェックし，必須入力項目に未入力または形式エラーを検出したら，エラー表示を行い，再実行を促す

- 入力された内容をチェックし，e-Rad 研究者番号あるいはその代替個人認識番号に未入力あるいは形式エラーを検出したら，エラー表示を行い，再実行を促す
- HPCI-ID 管理簿を参照し，入力された HPCI-ID と e-Rad 研究者番号あるいはその代替個人認識番号の不一致を検出したら，入力された HPCI-ID と e-Rad 研究者番号あるいは代替個人識別番号を含めて検証を行う
- 入力内容に問題がなければ廃止処理を実行し HPCI-ID 管理簿の内容を更新する
- 廃止された HPCI-ID は一定の保持期間（3 年間を想定）経過後，完全にデータを削除する

【共通視点】
- 廃止申請が本人による申請であることを確認する手順についてはさらに検討が必要である。

2.4.3.1 Web ポータルによる自動化案の場合

【利用者視点】
- 利用者は有効な HPCI アカウントを所有している場合は HPCI アカウントにより HPCI ポータルへサインオンする。有効な HPCI アカウントを所有していない場合，HPCI 事務局が HPCI ポータルへのサインオンに使用することを認めた認証プロバイダのアカウントを必要に応じて取得する。ここで使用できるアカウントとしては，情報基盤センターの全国共同利用アカウントや学認連携アカウントなどの Shibboleth IdP のアカウント，あるいは商用の OpenID IdP のアカウントを想定している。
- 上記のアカウントを用いて HPCI 事務局が提供する HPCI ポータルにアクセスし，申請用 Web フォームの一時 URL の送付先メールアドレスを登録する

【HPCI 事務局視点】
- 申請者が入力した IdP，当該 IdP でのアカウント，メールアドレスを HPCI-ID 管理簿に登録する
- 申請用 Web フォームの一時 URL を生成し，その URL が記載されたメールを入力されたメールアドレスに送付する

【利用者視点】
- 受信したメールに記載された申請用 Web フォームの一時 URL にアクセスし，HPCI-ID 廃止申請処理を実行する。

【HPCI 事務局視点】

- 入力された内容をチェックし，必須入力項目に未入力または形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力された内容をチェックし，e-Rad 研究者番号あるいはその代替個人認識番号に未入力あるいは形式エラーを検出したら，エラー表示を行い，再実行を促す
- 入力内容に問題がなければ廃止処理を実行し HPCI-ID 管理簿の内容を更新する
- 一時 URL を生成後，一定時間が経過したら当該 URL を無効化する
- 廃止された HPCI-ID は一定の保持期間（3 年間を想定）経過後，完全にデータを削除する

【共通視点】
- 廃止申請が本人による申請であることを確認する手順についてはさらに検討が必要である。

2.4.4 HPCI-ID の緊急時対応

ここでは，ユーザが HPCI-ID を忘れてしまった時の対処方法として検討した内容について述べる。詳細については引き続き検討する必要がある。

【利用者視点】
- ヘルプデスクの問い合わせフォームに e-Rad 研究者番号あるいはその代替個人識別番号とともに，HPCI-ID の送付を依頼する

【HPCI 事務局視点】
- HPCI-ID 管理簿を参照し，入力された e-Rad 研究者号あるいは代替個人識別番号に対応する HPCI-ID を，その HPCI-ID の属性として登録されている連絡先に連絡する

Web ポータルによる申請処理の省力化案により HPCI-ID 管理を行う場合には，HPCI-ID 申請時に登録した IdP のアカウントおよびパスワードにより当該 Web ポータル(HPCI ポータル)にサインオンすることにより，HPCI-ID の確認が可能となる。

【利用者視点】
- HPCI-ID 申請時に登録した IdP のアカウントおよびパスワードで HPCI ポータルにサインオンする。
- HPCI-ID 管理画面にアクセスすることにより，HPCI-ID を確認することができる

上記で，HPCI-ID 申請時に用いた IdP のアカウントおよびパスワードも忘れてしまった場合や，当該アカウントが失効している場合などにより HPCI ポータルにサインオンできない場合は，ヘルプデスクに問い合わせて対応を依頼する。

【利用者視点】

- ヘルプデスクの問い合わせフォームに e-Rad 研究者番号あるいはその代替個人識別番号とともに，HPCI-ID を確認するための手続きを依頼する

【HPCI 事務局視点】

- HPCI-ID 管理簿を参照し，入力された e-Rad 研究者番号あるいはその代替個人識別番号に該当する HPCI-ID を検索する
- 検索された HPCI-ID の属性として登録されている連絡先メールアドレスに HPCI ポータルの一時 URL を送付する

【利用者視点】

- 送付された一時 URL にアクセスし，IdP の再登録と HPCI-ID の確認を行う
- 一時 URL が記載されたメールが届かない場合，連絡先として登録されているメールアドレスが不達になっている可能性があるので，ヘルプデスク経由で HPCI 事務局に対応を依頼する

【HPCI 事務局視点】

- 一定時間経過した後，一時 URL を無効化する
- 一時 URL を記載したメールが不達であった場合などは，個別に対応する。但し，この場合にどのように本人確認を行うかなどの検討が必要である。

2.4.5　障害フロー

ここでは，HPCI 環境において障害が発生した場合にどのように対処が行なわれるかに関して記す。

障害対応フローとしては，以下のシナリオを考える。

1. 接続できない，資源が使えない
   HPCI 環境に参加する各機関の運用管理者の対応が必要になる案件の処理フロー
2. バグ報告
   開発者の対応が必要になる案件の処理フロー
3. パスワードを忘れた
   ユーザレベルのインパクトがある案件の処理フロー
4. システムの脆弱性を発見した
   システムレベルのインパクトがある案件の処理フロー

1. シナリオ1

このシナリオでは利用者が HPCI 環境を使用する際に必要となる認証ポータル，ログインノードなどに接続できない，あるいは HPCI 環境に提供されている資源が使えないなどの各資源の運用管理者の対応が必要になる事象が発生した場合を想定している。

シナリオ１に対する処理は以下の各ステップからなる。

【HPCI 事務局視点】

- ヘルプデスクを設置し，運用する。
- HPCI 環境に参加する各機関の運用状況を一覧することができるWeb ページ(HPCI 運用情報ページ)を設置し，運用する。

【資源提供機関視点】

- 資源提供機関は HPCI に提供している資源に関して，予め周知しておくべき運用情報（計画停止スケジュールなど）を HPCI 運用情報ページに登録する。

【利用者視点】

- 利用者は HPCI 環境を利用していて資源に接続できない，あるいは資源が使えないなどの事象に遭遇したときに，まず HPCI 運用情報ページを参照して当該事象に関連する運用情報（計画停止スケジュール，障害情報など）を確認する。
- 該当する情報が確認できなければ，ヘルプデスクのチケット一覧ページを参照し，同様な事象が報告されていないか確認する。
- 同様な事象が報告されていなければ，ヘルプデスクに遭遇した事象を登録する。

【HPCI 事務局視点】

- ヘルプデスクから新規案件が登録された旨の通知を受けたら，ヘルプデスク担当者は速やかに案件の内容を確認し，障害報告の場合は全ての利用者が参照できるように処理を行なう。
- ヘルプデスク担当者は必要に応じて登録者に問い合わせを行い，障害発生部位の切り分けを行なう。

【利用者視点】

- 案件を登録した利用者はヘルプデスク担当者からの問い合わせがあれば，速やかに回答する。

【HPCI 事務局視点】

- 障害発生部位の切り分けにより，登録された案件に関する対応依頼先機関を決定し，当該機関の HPCI 対応窓口に対してチケットの担当を割り当てる。
- ヘルプデスク担当者はチケットの進捗管理を行い，処理が滞留しないようにする。

【共通視点】

- チケットの担当を割り当てられた HPCI 対応窓口の担当者は，チケットの内容を確認して自機関における対応を行なう。
- 自機関における障害の場合は HPCI 運用情報ページに状況を登録し，適宜更新する。
- 対応が終了したら，HPCI 事務局に対してチケットを返却する。

【HPCI 事務局】

- ヘルプデスク担当者は返却されたチケットの内容を確認し，担当を割り当てた機関の対応によって案件が解決したかどうかを判定する。
- 案件が解決していなければ，再度対応依頼先機関を決定し，当該機関の HPCI 対応窓口に対してチケットの担当を割り当てる。
- 案件が解決していれば，案件の登録者に対して遭遇した事象が解決したか問い合わせる。

【利用者視点】

- 案件を登録した利用者は遭遇した事象が解決したかどうかを確認し，回答する。

【HPCI 事務局】

- 事象が解決したことが確認されたら，チケットのクローズを行なう。

- 事象が解決していなければ，再度対応依頼先機関を決定し，当該機関の HPCI 対応窓口に対してチケットの担当を割り当てる。

2. シナリオ2

このシナリオでは利用者が HPCI 環境を使用する際に，利用の手引き等に示されているものと異なる結果が得られるなど，HPCI が提供するソフトウェアの不具合が疑われる事象に遭遇した場合を想定している。

シナリオ２に対する処理は以下の各ステップからなる。

【共通視点】

- HPCI が提供するソフトウェアはそれぞれ保守を担当する開発チームが組織されていて，HPCI 事務局からの作業依頼に対応可能な体制が整えられていること。

【HPCI 事務局視点】

- ヘルプデスクを設置し，運用する。

【利用者視点】

- HPCI 環境を使用中に想定外の動作や結果が得られる事象に遭遇したら，ヘルプデスクに遭遇した事象を登録する。

【HPCI 事務局視点】

- ヘルプデスクから新規案件が登録された旨の通知を受けたら，ヘルプデスク担当者は速やかに案件の内容を確認し，HPCI が提供するソフトウェアの不具合が疑われる場合は必要に応じて登録者に問い合わせを行い，事象の発生原因であると疑われる部位の特定を行なう。

【利用者視点】

- 案件を登録した利用者はヘルプデスク担当者からの問い合わせがあれば，速やかに回答する。

【HPCI 事務局視点】

- 事象の発生原因であると疑われる部位が特定できたら，当該部位を担当する開発チームにチケットの担当を割り当て，調査を依頼する。
- ヘルプデスク担当者はチケットの進捗管理を行い，処理が滞留しないようにする。

【開発チーム視点】

- 割り当てられたチケットに対応し，事象の発生原因を調査する。
- 必要に応じて登録者に調査のための情報採取などを依頼する。

【利用者視点】

- 調査のための情報採取の依頼に対し，回答する。

【開発チーム視点】

- 必要に応じて調査用環境の使用を HPCI 事務局に依頼する。

【HPCI 事務局視点】

- 調査用環境提供のための調整を行ない，開発チームに回答する。

【開発チーム視点】

- 調査状況を適宜ヘルプデスクに登録する。
- 調査が終了したら，調査結果とともに，チケットを HPCI 事務局に返却する。調査結果には原因が特定できたか否か。原因が特定できた場合にはその発生原因，対処方法（暫定的・恒久的）が含まれる。

【HPCI 事務局視点】

- 返却されたチケットの内容を確認し，原因が特定された場合にはその内容を確認し，暫定的対処方法を登録者に回答する。
- 原因が特定できない場合には，調査担当者を再割り当てし調査を継続する。
- 開発を伴う対処方法を採用するかどうかを検討し，採用する場合は当該チケットに関連づけられた開発案件を起案し，開発チームにチケット担当を割り当てる。

【利用者視点】

- 暫定的対処方法により，事象の発生が回避できることを確認し回答する。

【HPCI 事務局視点】

- 情報共有 CMS に当該事象とその暫定対策について登録する。
- 不具合の報告に関するチケットはクローズ処理を行なう。

3. シナリオ3

このシナリオでは利用者が HPCI アカウントのパスワードを忘れてしまった，証明書のパスフレーズを忘れてしまった，などユーザレベルのインパクトが発生する場合を想定している。

シナリオ３に対する処理は以下の各ステップからなる。

【HPCI 事務局視点】

- セキュリティ専用のヘルプデスクを設置し，運用する。

【利用者視点】

- HPCI アカウントのパスワードあるいはユーザ証明書のパスフレーズを忘れてしまった場合には，セキュリティ専用のヘルプデスクに報告する。

【HPCI 事務局視点】

- 利用者が HPCI アカウントのパスワードを忘れた場合には，当該利用者のプライマリセンターである IdP 運用機関に対し，対応を依頼する。
- 利用者がユーザ証明書のパスフレーズを忘れてしまった場合には，新たな証明書を発行する手順を利用者に回答し，当該処理の終了とする。

【IdP 運用機関視点】

- 当該利用者に対し，パスワード再発行処理を実施する。
- 処理が完了したことを HPCI 事務局に連絡する。

【HPCI 事務局視点】

- IdP 運用機関から処理が完了した旨の連絡を受けたことをもって，当該処理の終了とする。

4. シナリオ4

このシナリオではシステムの脆弱性を発見した，などシステムレベルのインパクトが発生する場合を想定している。

シナリオ４に対する処理は以下の各ステップからなる。

【共通視点】

- HPCI 環境に参加する各機関は HPCI 向けのセキュリティ・インシデント・レスポンス・チームを組織している。

【HPCI 事務局視点】

- セキュリティ専用のヘルプデスクを設置し，運用する。

【共通視点】

- システムの脆弱性を発見した場合，速やかにセキュリティ専用のヘルプデスクに報告する。

【HPCI 事務局視点】

- インシデント・レスポンス・チームに対応を依頼する。

【インシデント・レスポンス・チーム】

- 各 HPCI 環境参加機関の自組織におけるインシデントの場合，自組織内のインシデント・レスポンスを実施すると共に，HPCI 事務局および他組織に当該インシデントを報告する。
- 自組織内のインシデント・レスポンスの結果を HPCI 事務局および他組織に報告する。
- 各 HPCI 環境参加機関の他組織におけるインシデントの場合，当該組織の資源を切り離し，フォレンジックを実施，解除待機する。
- 全てのインシデント・レスポンスが完了したことを HPCI 事務局に報告する。

【HPCI 事務局視点】

- インシデント・レスポンス・チームからの報告をもって当該処理の終了とする。

2.4.6　ヘルプフロー

ここでは，HPCI 事務局が設置するヘルプデスクについて，どのように処理が行なわれるかに関して記す。ヘルプデスクの運用を支援するためのソフトウェアとしてチケット管理システムを採用することを想定している。チケット管理システムを用いることで HPCI 環境における様々な問い合わせに対する対応状況を追跡し管理することが容易になる。

チケット管理システムによるヘルプデスクの業務フローの概要を以下に示す。

1. 案件の登録
2. チケットの新規発行
3. チケットのオープン
4. チケットの担当割り当て
5. チケットの処理と処理内容の記録
6. チケットのステータス変更(必要に応じて)
7. チケットの担当再割り当て
   （処理が完了するまで 5. ～7. を繰り返し）
8. チケットの完了承認
9. チケットのクローズ

これらの業務フローの各ステップの処理の詳細に関しては，平成 23 年度に検討し決定することとするが，現段階で想定しているシナリオは以下の通りである。

【HPCI 事務局視点】

- ヘルプデスクを設置し，チケット発管理システムにより案件管理を行なう。
- ヘルプデスクは問い合わせの内容別に案件の管理ができる。

【利用者視点】

- Web インターフェース経由あるいはメール経由でヘルプデスクに対する問い合わせ案件を登録する。
- Web インターフェース経由で案件を登録する場合にはユーザ認証が必要となる。

【HPCI 事務局視点】

- 登録された問い合わせに対して，チケットを新規発行する。
- チケットをオープンし，担当者を割り当てる。

【共通視点】

- チケットを割り当てられた担当者は，チケットの内容を確認し適切に対応する。

- チケットに対する対応内容を登録する。
- 自分に割り当てられたチケットの処理が完了したら，HPCI 事務局に担当を戻す。

【利用者視点】
- チケット発行システムに対しサインオンし，自分が登録した案件に対する対応内容を確認する。あるいは処理内容（の一部）をメールで受け取る。

【HPCI 事務局視点】
- HPCI 事務局はチケットに対する対応内容を確認し，必要ならば担当者を再割り当てする。
- チケットに対する対応が完了したと判断した場合には，案件登録者に問い合わせた内容が解決したかどうか確認する。

【利用者視点】
- 案件が解決したかどうかの問い合わせに回答する。

【HPCI 事務局視点】
- 案件が解決していれば，チケットのクローズ処理を行なう。
- 案件が解決していなければ，チケットの担当者を再割り当てする。

また，利用方法に関する問い合わせなど，同じような問い合わせが繰り返される場合にはその内容を FAQ として公開することも想定している。

【HPCI 事務局視点】
- 繰り返しヘルプデスクに登録される案件に対して，FAQ 管理を行なう。

【利用者視点】
- 利用方法などについてヘルプデスクに問い合わせる前に，FAQ に自分の問い合わせたい内容が登録されていないか確認する。

2.5 年度末フェーズ

採択された HPCI 利用課題の代表者の，利用報告書提出義務の有無・報告書の内容・成果評価の有無・成果公開の有無・公開の形態については，運営規則等で別途定められることになる。本文書では，各課題の代表者に一定の報告が求められ，無償型・利用負担金減免型の課題には成果評価が行われるものと仮定して，年度末に行われる業務を以下のようにまとめる。

【共通視点】

1. 利用報告書提出
   - HPCI 事務局からの請求に基づき，各利用課題の代表者は，当該利用期間の HPCI 利用にかかる報告書を提出する。
2. 成果評価
   - 無償型・利用負担金減免型の課題については，HPCI 事務局（あるいはそれが諮問する課題審査委員会）において，成果の評価を行う。
3. 成果公開
   - HPCI 事務局は，運営規則等の定めるところにより，成果公開の業務を行う。

3 基盤構築・運用基本仕様

3.1 ユーザ管理支援

3.1.1 マニュアル体系

HPCI 事務局は以下のマニュアルを整備・保守し，Web で公開する。特に，資源提供機関ごとの使い方に関しては，記述レベルや内容にバラつきがない様に，統一したフォーマットでまとめられていること。

3.1.1.1 ユーザ向け

(1) クイックスタートガイド

(2) 各種ユーザマニュアル

- HPCI ポータルユーザマニュアル
- 認証局ユーザマニュアル
- 認証ポータルユーザマニュアル
- Proxy 証明書リポジトリユーザマニュアル
- ヘルプデスクユーザマニュアル(一般ユーザ向け)
- 情報 CMS ユーザマニュアル(一般ユーザ向け)
- GSI-SSH システムユーザマニュアル
- 資源提供機関ごとのユーザマニュアル
- 先端ソフトウェア運用基盤ユーザマニュアル
- 緊急時対応ユーザマニュアル

3.1.1.2 運用管理者向け

3.1.1.2.1 資源提供機関向け

(1) 管理者マニュアル

- GSI-SSH システム管理マニュアル
- ヘルプデスクユーザマニュアル(管理者向け)
- 障害対応マニュアル
- HPCI 向けネットワーク・セキュリティ監査基準

(2) セキュリティ・インシデント対応マニュアル

3.1.1.2.2 HPCI 事務局向け

(1) 管理者マニュアル

- HPCI ポータルシステム管理マニュアル
- ヘルプデスクシステム管理マニュアル
- 情報共有 CMS 管理マニュアル

(2) ヘルプデスク対応マニュアル

- 障害対応マニュアル
- バグ報告対応マニュアル
- セキュリティ報告対応マニュアル
- その他の問い合わせ対応

(3) セキュリティ・インシデント対応マニュアル

(4) ユーザマニュアル

- HPCI ポータルシステムユーザマニュアル(管理者向け)
- ヘルプデスクユーザマニュアル(管理者向け)
- 情報共有 CMS ユーザマニュアル(管理者向け)

3.1.1.2.3 認証局運用機関向け

(1) 管理者マニュアル

- 認証局システム管理者マニュアル
- 証明書管理システム管理者マニュアル(UMS, MyProxy)
- Shibbeoleth DS 管理者マニュアル

3.1.1.2.4 認証ポータル運用機関向け

(1) 管理者マニュアル

- 認証ポータル管理者マニュアル
- Proxy 証明書リポジトリ管理者マニュアル

(2) 障害対応マニュアル

3.1.1.2.5 HPCI アカウント IdP 運用機関向け

(1) 管理者マニュアル

- HPCI アカウント IdP 管理者マニュアル

(2) 障害対応マニュアル

3.1.2 セキュリティ・ポリシー

- HPCI としてのセキュリティ・ポリシーに関しては，基本的には HPCI 環境に参加する各機関のセキュリティ・ポリシーに従うこととする。
- 各資源提供機関内で発生したセキュリティ・インシデントについては各機関が責任を持って対処しなければならない。
- 各資源提供機関のセキュリティ・ドメインは独立しており，以下の要件を満たしているものとする。
    - セキュリティ・ポリシーやインシデント・レスポンスは各機関の内規に従う。
    - 管理者権限（root パスワード）は複数機関に跨って共有しない。
    - HPCI 利用者は有効期限の制約されたクレデンシャルで各資源提供機関の資源を利用するものとし，個人情報漏洩につながる操作（パスワード入力など）は行わない。
    - 同一グループに属さないユーザからの情報アクセスを制限できる。
- HPCI 全体としてのセキュリティ・インシデント対応のため，HPCI 事務局，資源提供機関，認証局運用機関など HPCI 環境の運用に参画するすべての機関は，それぞれ主担当・副担当・事務補佐を選出して，インシデント・レスポンス・チームを組織する。
- セキュリティ・インシデントが発生したときの情報伝達や対応の手順は別途定めることとする。
- 全ての資源提供機関において，パブリック・ネットワークに接続されるサーバに対して適用される，HPCI としてのネットワーク・セキュリティ監査基準を平成 23 年度に検討し策定する。ネットワーク・セキュリティ監査基準に含まれる内容としては以下に示すものを想定している。
    - 設定すべき ACL（公開ポートや通信ホスト制限，およびそれらの組み合わせ）
    - 不正アクセス検知システムの設置基準
    - セキュリティ・モニタ（マルウェア検出）の設置基準
    - 監査すべきログとその保全基準および監査内容と頻度

3.1.3 課題およびアカウント区分

3.1.3.1 利用課題について

利用者が HPCI で提供される計算機資源・ストレージ資源を利用する者は利用を承認された HPCI 利用課題のいずれかに課題従事者として属している必要がある。

2.1.2 節で述べたように，本文書では利用課題は表 2.2 に示したような資源利用にかかる負担金の支払い条件により 3 種類に区分されるものと想定し，利用課題の区分の詳細については運営規則等で別途定められるものとする。

HPCI 事務局は，利用課題を識別し管理するため，それぞれの利用課題には一意に決まる HPCI 利用課題 ID を付与する。HPCI 利用課題 ID の付与に関する規則は平成 23 年度に検討し定めるものとする。

また，利用課題は資源利用にかかる経費負担の集計単位でもあるため，各資源提供機関は利用者がどの利用課題の経費負担によって資源を使ったかについて記録し，集計できる必要がある。

3.1.3.2 グループ名について

GSI 認証を前提とする平成 23 年度の利用シナリオにおいては，ユーザが複数の利用課題に含まれる場合でも，ユーザの証明書に対応付けられるローカルアカウントは 1 個に限られるため，GSI-SSH によるログインではユーザは証明書に対応づけられたローカルアカウントおよびそのデフォルトグループでログインすることとなる。この制約の下での利用方法として，ユーザが資源を利用する際にどの利用課題の従事者として利用するのかを，上述した HPCI 利用課題 ID に対応付けられた何らかの識別番号により明示的に指定してジョブ投入を行うなどが考えられる。この識別番号として，Unix のグループ名を対応づけることを想定しているが，このグループ名が資源提供機関ごとに不統一となった場合には，ユーザに煩雑な記憶を強いることになるため，統一グループ名の可能性を検討するためのアンケート調査を行った（調査結果は付録に示す）。このアンケート調査の結果に基づき，グループ名に関する検討を平成 23 年度に実施する。

3.1.3.3 アカウント区分について

2.1.1 節に示したように，HPCI を利用するために以下のような各種アカウント (HPCI-ID を含む)を取得する

- 一人の HPCI 利用者(ユーザ)に対して一個の HPCI-ID が割り当てられ，その HPCI-ID にひも付けられた証明書が認証局から発行される。

- ユーザは Shibboleth や OpenID など異なる認証方式ごとに HPCI アカウントを取得することができ，それらの HPCI アカウントはユーザの HPCI-ID にひも付けられて管理される。
- 資源提供機関の資源を利用するためのローカルアカウントは HPCI アカウントにひも付けられる。
- ユーザが複数の HPCI 利用課題に属している場合，どのようにローカルアカウントを割り当てるかについては，各資源提供機関におけるグループ管理方式を踏まえてさらに検討する必要がある。

3.1.4 HPCI-ID 運用規約 (案)

HPCI-ID の運用に関する規約(案)を示す。引き続き検討し，平成 23 年度に決定する。

3.1.4.1 (定義)

- 「HPCI-ID」は，「HPCI 利用課題申請」に先立ち，「HPCI-ID 登録申請」に係る手続きに則って HPCI-ID 取得有資格者に発行される一意的な ID である。

3.1.4.2 (資格)

- e-Rad における研究者番号を取得可能なものを HPCI-ID 取得の有資格者とする。
- e-Rad における研究者番号を取得できないもののうち，HPCI 利用資格を有するものは HPCI-ID 取得の有資格者とする。HPCI 利用資格は別途定められているものとする。e-Rad 研究者番号を代替する識別番号として何を用いるかなど，その取り扱いは平成 23 年度に検討する。

3.1.4.3 (一意性と重複の排除)

- 「HPCI-ID 登録申請（交付)」においては，申請者を識別可能な個人識別番号（e-Rad 研究者番号およびその代替個人識別番号）によって重複発行を抑止する。
- 重複した HPCI-ID を保持していることが判明した場合は，速やかに「HPCI-ID 登録申請(廃止)」が行われるものとする。
- 「HPCI 利用課題申請」に際して，重複した HPCI-ID を保持している課題実施者)が含まれている場合は，当該申請を受理しない。

3.1.4.4 (利用者の識別と用途の限定)

- 「HPCI-ID 登録申請（変更，更新，廃止)」や緊急時対応の申込にあたっては，HPCI-ID によって利用者を識別する。
- 申請時に記載される「英文氏名」と HPCI-ID を電子証明書発行時に CN（Common Name）として電子証明書に記載し，GSI（Grid Security Infrastructure）認証によるサインオン時にローカルアカウント名との対応付けに用いる。
- ローカルアカウント名そのものに用いてよいか，などの詳細については HPCI-ID のフォーマットとともに平成 23 年度に検討する。
- 上記以外の用途に HPCI-ID を用いない。

3.1.4.5 (有効期間)

- HPCI-ID の有効期間は発行から 10 年間経過した日からその当日を含む最初の年度末とする。ここで，パスポートと同様な 10 年の有効期間が妥当であるかなどは引き続き検討する。

- 「HPCI 利用課題申請」に際して，課題従事者のすべてが課題実施期間内で有効な HPCI-ID を取得しているものとする。
- 課題実施期間内に HPCI-ID の有効期間が終了する場合は，申請に先立って「HPCI-ID 登録申請（更新)」が行われるものとする。

3.1.4.6　(変更登録と登録情報の一貫性の維持)

- HPCI-ID 登録時に申請した情報が変更された場合は，速やかに「HPCI 登録申請（変更)」が行われるものとする。
- 「HPCI 利用課題申請」に際して，申請代表者および副代表者は課題従事者の本人性確認を身分証明書と照らして行い，その記録として身分証明書類の複製を提出することが要請される。提出される証明書類の複製に記載されている情報が登録されている情報と一致しない場合は，HPCI-ID の失効処置を行う。また，当該申請は受理しない。

3.1.4.7　(失効と利用停止)

- HPCI-ID は一時的な失効処理と失効からの復帰が可能である。
- HPCI-ID が失効すると，HPCI-ID に対応づけられたローカルアカウントの利用が翌営業日までに停止される。
- HPCI-ID が失効から復帰すると，HPCI-ID に対応づけられたローカルアカウントの利用が翌営業日までに再開される。
- HPCI-ID は有効期間を過ぎても更新申請が行われていない場合は，即時失効処置を行ない，猶予期間内に「HPCI-ID 登録申請（更新)」あるいは「HPCI-ID 登録申請（廃止)」を行なうよう，HPCI-ID 保持者に書面で通知する。
- 「HPCI 利用課題申請」時に，HPCI-ID 取得資格を失っていることが判明した場合は，HPCI-ID の失効処置を行う。その際は，当該課題従事者が含まれる利用課題申請は受理せず，その旨を HPCI-ID の保持者と HPCI 利用課題代表者および連絡責任者に書面で通知する。
- 資源提供機関がローカルアカウントを発行する際に，課題実施者が HPCI 利用資格を有していないことが判明した場合は，HPCI-ID の失効処置を行う。既に採択されている他の利用課題に当該課題従事者が含まれる場合は，HPCI-ID が失効された翌営業日までにすべてのローカルアカウントの利用停止措置をおこない，それらの処置を行った旨を HPCI-ID の保持者と HPCI 利用課題代表者および連絡責任者に電子メールおよび書面で通知する。HPCI-ID の失効処理において他の課題に含まれて
- 課題代表者の HPCI-ID が失効した場合は，課題副代表者に業務を代行させ，すみやかに体制の復帰を促す。課題副代表者および連絡責任者の HPCI-ID が失効した場合は，すみやかに体制の復帰を促す。1 ヶ月以内に体制が整わない場合は，利用課題実施の実施停止措置を行う。

3.1.4.8　(廃止)

- HPCI-ID は恒久的な廃止処理が可能である。
- HPCI-ID が廃止されると，当該 HPCI-ID に対応づけられた電子証明書は失効される。
- HPCI-ID を保持しているものが HPCI-ID 取得資格を失った場合は，速やかに「HPCI-ID 登録申請（廃止）」が行われるものとする。
- HPCI-ID は有効期間を過ぎても更新申請が行われず，さらに猶予期間内に更新申請が行われない場合は，即時廃止処置を行ない，HPCI-ID 保持者に書面で通知する。
- HPCI-ID が廃止された場合，再発行時は異なる HPCI-ID を発行する。

3.1.4.9　(照合コード)

- 「HPCI 利用課題申請」の Web ポータル上での自動申請処理案では入力フォームにおいて，課題従事者の HPCI-ID を入力する際に，誤入力を防止するための照合コード(4 桁数字を想定)を発行する。当該フォームにおいて，HPCI-ID と照合コードを入力することによって英文氏名(displayName)を呼び出すことができる。
- それ以外の用途に照合コードを用いない。
- HPCI 利用課題申請に先立って，課題に従事する HPCI-ID 保持者が課題申請を行う課題代表者に照合コードを伝達する。
- 照合コードは，HPCI-ID 保持者が随時更新することが出来る。また，公募期間ごとに自動的に更新される。
- 同じ英文氏名を持つ複数の HPCI-ID 保持者に対しては，異なる照合コードが発行されることを保証する。

3.1.5 HPCI-ID に関わる申請窓口業務

HPCI 事務局は，随時，「HPCI-ID 取得有資格者」からの「HPCI-ID 登録申請」を受け付け，HPCI-ID の交付，変更，更新および廃止処置を行う。HPCI 運用に際して，HPCI-ID の一時的な失効が必要となった際は，失効処置を行ない，その旨を関係者に通知する。

3.1.5.1 HPCI-ID 運用規約

- HPCIコンソーシアムが定める「HPCI-ID 運用規約」に則って「HPCI-ID 登録申請」に係る運用業務を行う。

3.1.5.2 HPCI-ID 登録申請

- 「HPCI-ID 登録申請」は，Web ポータルで随時受け付ける。

3.1.5.2.1 交付申請

・ 次の属性情報を記載可能な「HPCI-ID 登録申請（新規）」用 Web 入力フォームを作成し，「HPCI-ID 管理簿」と連動させること。

- 氏名（和文，英文）
  英文氏名は，電子証明書発行時に CN（Common Name）として参照する
- 申請時の属性情報
  所属，職名・身分，連絡先（住所，電子メールアドレス，電話およびファックス番号）
- 所属組織が変わっても個人を識別可能な番号：e-Rad の研究者番号
  なお，一部の利用有資格者は，e-Rad の研究者番号を取得できないことが想定される。その場合に代替となる個人識別番号を記載できること。
- その他，プライマリセンターの指定をどこで行うかなどの画面設計の詳細は平成 23 年度に検討する。

・ HPCI-ID 登録申請用 Web フォームの画面案を図 3.1 に示す。この画面案では，登録，変更，廃止のそれぞれの申請を同一画面上で行うようになっている。

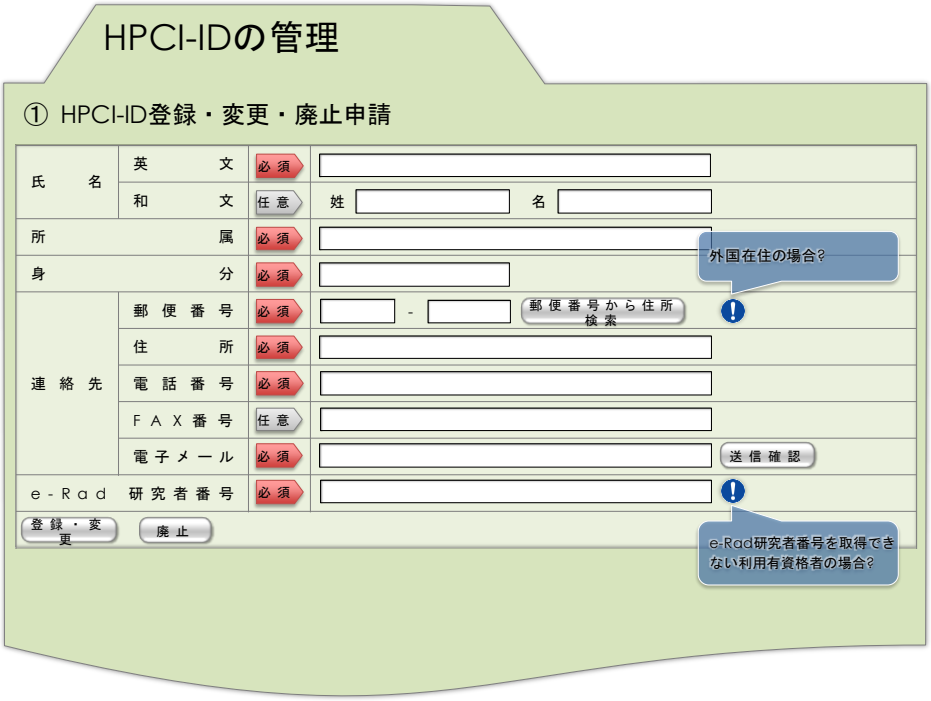


図 3.1 HPCI-ID 登録申請用 Web フォーム画面(案)

- 入力フォームは必要に応じて改版すること。その場合は「HPCI-ID 管理簿」と連動を維持すること。
- 次の場合, HPCI-ID は発行されない:
  - 必須入力項目 (和文氏名, 英文氏名, 所属, 職名・身分, 連絡先 (住所) が未入力または形式エラー
  - e-Rad 研究者番号あるいはその代替となる個人識別番号が未入力または形式エラー
  - e-Rad 研究者番号あるいはその代替となる個人識別番号の重複
- e-Rad 研究者番号あるいはその代替となる個人識別番号の重複が検出された場合は, 重複先の HPCI-ID を含めて検証を行う。
- HPCI-ID の発行段階では, HPCI-ID 取得者が HPCI 利用有資格者か否かの確認は行わない。
  - e-Rad 研究者番号による当該研究者の属性情報の参照はできない(本人確認など)ため, 利用有資格者か否かの確認は「HPCI 利用課題申請」時に身分証明書類の複写が添付されるのでその時点で照合することとする。また, 採択された「HPCI 利用課請」に対し, 資源提供機関においてローカルアカウントを登録処理する際に各資源提供機関の登録窓口により確認されることとする。その照合・確認方法などについての詳細は平成 23 年度に検討を行う。

- 利用資格の確認処理において不適正と判断された HPCI-ID は失効する。

・ 本人からの申請であることを確認する方法に関してはを引き続き検討する必要がある。

3.1.5.2.2 属性変更申請

・ 次の属性情報を記載可能な「HPCI 登録申込書（変更）」Web 入力フォームを作成し，「HPCI-ID 管理簿」と連動させること。

- HPCI-ID
- 氏名（和文，英文）
  英文氏名は，電子証明書発行時に CN（Common Name）として参照する
- 変更する属性情報
  所属，職名・身分，連絡先（住所，電子メールアドレス，電話およびファックス番号）

・ 次の場合，属性変更処理は行わない:

- 必須入力項目（和文氏名，英文氏名，所属，職名・身分，連絡先（住所）が未入力または形式エラー
- e-Rad 研究者番号あるいはその代替となる個人識別番号が未入力または形式エラー
- e-Rad 研究者番号あるいはその代替となる個人識別番号が HPCI-ID 管理簿に登録されている情報と一致しない

・ e-Rad 研究者番号あるいはその代替となる個人識別番号の HPCI-ID 管理簿との不一致が検出された場合は，入力された e-Rad 研究者番号あるいは代替個人識別番号，HPCI-ID を含めて検証を行う。

・ 本人からの申請であることを確認する方法に関してはを引き続き検討する必要がある。

3.1.5.2.3 更新申請

・ 次の属性情報を記載可能な「HPCI 登録申込書（更新）」Web 入力フォームを作成し，「HPCI-ID 管理簿」と連動させること。

- HPCI-ID
- 氏名（和文，英文）
  英文氏名は，電子証明書発行時に CN（Common Name）として参照する

・ 次の場合，更新処理は行わない:

- 必須入力項目（和文氏名，英文氏名，所属，職名・身分，連絡先（住所）が未入力または形式エラー

- e-Rad 研究者番号あるいはその代替となる個人識別番号が未入力または形式エラー
- e-Rad 研究者番号あるいはその代替となる個人識別番号が HPCI-ID 管理簿に登録されている情報と一致しない

・ e-Rad 研究者番号あるいはその代替となる個人識別番号の HPCI-ID 管理簿との不一致が検出された場合は，入力された e-Rad 研究者番号あるいは代替個人識別番号，HPCI-ID を含めて検証を行う。
・ 本人からの申請であることを確認する方法に関してはを引き続き検討する必要がある。

3.1.5.2.4 廃止申請

・ 次の属性情報を記載可能な「HPCI 登録申込書（廃止）」Web 入力フォームを作成し，「HPCI-ID 管理簿」と連動させること。
  - HPCI-ID
  - 氏名（和文，英文）
    英文氏名は，電子証明書発行時に CN（Common Name）として参照する

・ 次の場合，廃止変更処理は行わない:
  - 必須入力項目（和文氏名，英文氏名，所属，職名・身分，連絡先（住所）が未入力または形式エラー
  - e-Rad 研究者番号あるいはその代替となる個人識別番号が未入力または形式エラー
  - e-Rad 研究者番号あるいはその代替となる個人識別番号が HPCI-ID 管理簿に登録されている情報と一致しない
・ e-Rad 研究者番号あるいはその代替となる個人識別番号の HPCI-ID 管理簿との不一致が検出された場合は，入力された e-Rad 研究者番号あるいは代替個人識別番号，HPCI-ID を含めて検証を行う。
・ 本人からの申請であることを確認する方法に関してはを引き続き検討する必要がある。

3.1.5.3 緊急時対応

- HPCI-ID を忘れた場合の他，どのようなケースを想定すべきか，引き続き検討が必要。

3.1.5.4 Web ポータル上での各種申請処理の自動化(案)

Web ポータル上での各種申請の処理を自動化し，HPCI 事務局の作業コストを削減するための方式として以下に示す案を検討した。

- 有効な HPCI アカウントを持たない利用者は，HPCI 事務局によって承認された IdP のア

カウントによってWebポータルの初回認証を行うことで，HPCI-IDの交付申請や変更・更新・廃止申請を行うことができる。

・ Webポータルは，次の二段階の操作で申請者からの各種申請を受け付ける:

- 第一段階として，既存の IdP（情報基盤センターが提供する Shibboleth IdP や，認定された商用 OpenID プロバイダ）に認証を移譲し，電子メールアドレスの登録と IdP 毎の ID 識別子（Shibboleth の場合は IdP から提供される ePPN: eduPersonPrincipalName，OpenID の場合は個人識別用 URL）の対応付けを行う（図 3.2）。
- この対応付けは複数可能とし，特に，HPCI アカウントが Shibboleth IdP 運用機関に登録された場合は，その ePPN でも認可されるよう自動登録する。
- 第二段階として，登録された電子メールアドレスに対して申請用 Web フォームの一時 URL を送付し，申請情報の登録を受け付ける。一時 URL は，libuuid によって自動生成された uuid を含み，1 時間で無効化する。
- HPCI-ID 交付申請においては，3.1.5.2.1 節に示した形式的なエラーがなければ自動的に HPCI-ID を発行する。

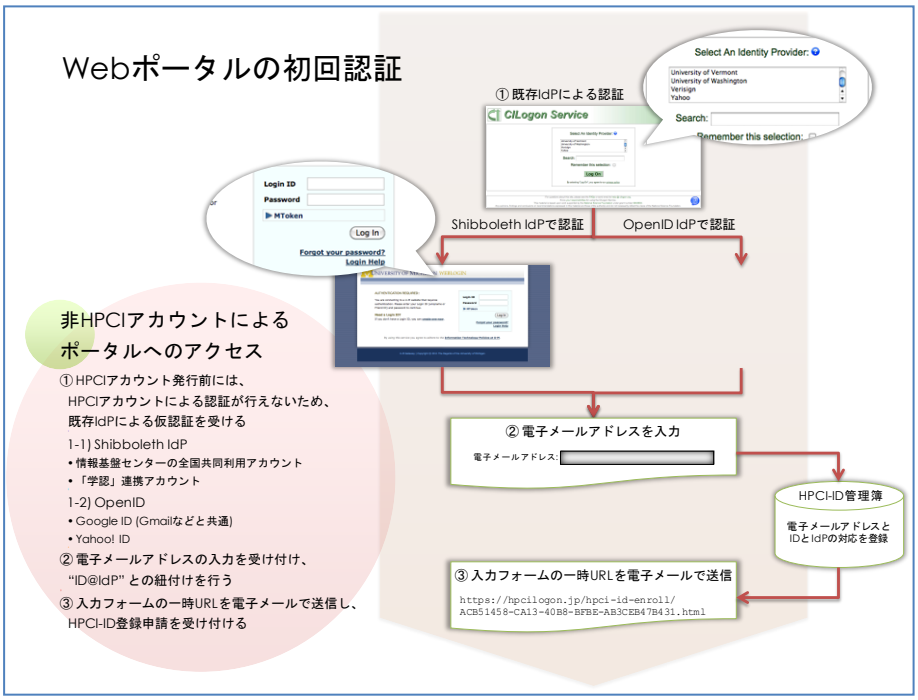


図 3.2 Web ポータルの初回認証

- 有効な HPCI アカウントを持つ利用者は直接 Web ポータルにサインオンすることで自分の HPCI-ID に関する変更・更新・廃止申請を行うことができる。
- HPCI アカウントでサインオンした場合と非 HPCI アカウントでサインオンした場合では，図

3.3 に示すようにポータル上で利用できる機能に差がある(この図では後述するようにポータル上からHPCI利用課題の申請，HPCIアカウントの管理も行うことを想定している)。すべての機能を利用するためにはHPCIアカウントでサインオンしなければならない。

		非HPCIアカウント	HPCIアカウント
HPCI-IDの管理	登録・変更・廃止	○	○
	照合コードの参照と再生成	○	○
	IdPの追加と削除	○	○
HPCI利用課題の申請	新規	○	○
	変更・継続	×	○ (代表者のみ)
HPCIアカウントの管理	アカウント発行状況の確認	○	○
	電子証明書の発行と更新	×	○
	代理証明書のダウンロード	×	○

図 3.3 HPCI アカウント/非 HPCI アカウントによる認証と認可

- 利用課題申請 Web フォームなどで HPCI-ID の入力する際に，入力ミスを事前に防止する機能があると，HPCI 事務局が HPCI-ID の正当性を確認するための労力を削減することができる。そのための仕組みとして HPCI-ID 照合コードを用いる方法を検討した。図 3.4 に示すように，Web フォームに入力した HPCI-ID が正しいことを照合コードにより照会して確認することが可能となる。

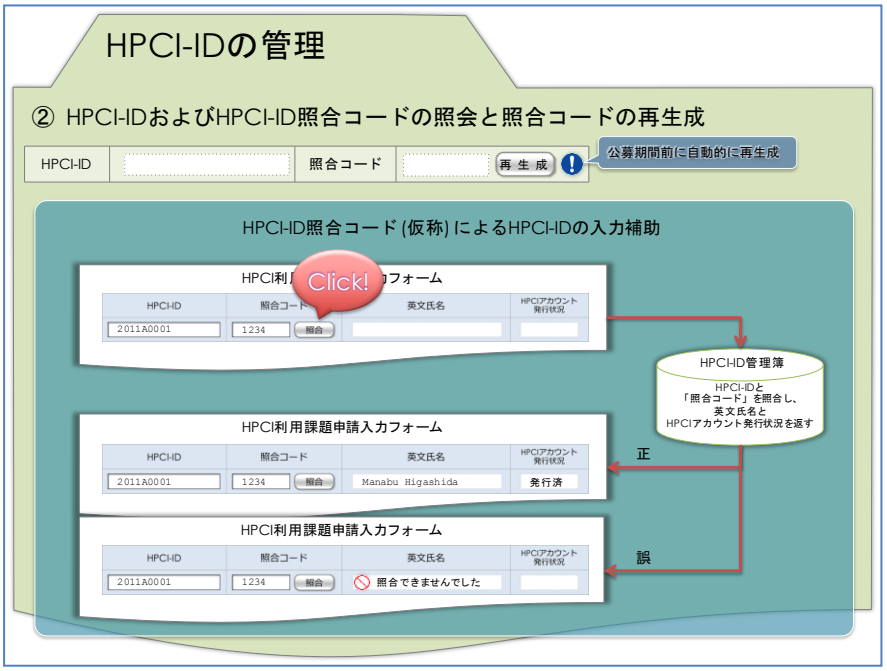


図 3.4 HPCI-ID 照合コード

- 本案については平成 23 年度に引き続き検討を行うこととする。

3.1.5.5 HPCI-ID 管理簿の操作

3.1.5.5.1 登録処理

- HPCI-ID は,「HPCI-ID 管理簿」に「HPCI-ID 登録申請」Web 入力フォームから属性情報とともに登録され, HPCI-ID の有効期間(10 年間を想定)満了後, 一定の保持期間 (3 年間を想定) 保持する。
- e-Rad 研究者番号または代替個人識別番号によって重複登録を抑止する。
- 更新履歴を残し, 遡って閲覧が可能であること。
- 「HPCI 利用課題管理簿」から HPCI-ID をキーとして属性情報を参照することが可能であること。
- Shibboleth IdP 運用機関に対して, HPCI-ID をキーとして英文氏名を提供可能であること。
- HPCI-ID が登録された場合は, 翌営業日までにローカルアカウントへの対応付けが開始されること。

3.1.5.5.2 失効処理と失効からの復帰処理

- 一時的な失効処理と失効からの復帰処理が可能であること。
- 失効・復帰処理を行った場合に,「HPCI 利用課題管理簿」と「HPCI 提供資源管理簿」から関連する「HPCI 利用課題 ID」と「HPCI 提供資源名」を抽出できること。
- HPCI-ID が失効した場合は, 翌営業日までにローカルアカウントへの対応付けを停止できること。
- HPCI-ID が失効から復帰した場合は, 翌営業日までにローカルアカウントへの対応付けを再開できること。

3.1.5.5.3 廃止処理

- 恒久的な廃止処理が可能であること。
- HPCI-ID が廃止された場合は, 証明書の失効処理を行うこと。
- HPCI-ID が廃止された場合は, 一定の保持期間 (3 年間を想定) 経過後, 完全にデータが削除されること。

3.1.6 提供資源管理業務

HPCI 事務局は，課題審査委員会，資源提供連携ネットワーク委員会(仮称)および個々の資源提供機関の業務窓口と連絡し，資源提供連携ネットワーク委員会(仮称)が取りまとめる提供資源リストを管理する。資源リストの更新頻度と更新時期に関しては別途運営規定等で定められるものとするが，ここでは年 2 回を想定する。課題審査委員会は提供資源リストから資源割り当てを行う。資源割り当ての頻度と時期は別途運営規定等で定められるものとするがここでは年 2 回を想定する。HPCI 事務局は，割り当てられた資源を資源提供連携ネットワーク委員会(仮称)に通知すると同時に，個々の資源提供機関との連携用データベースを更新する。提供資源管理業務に関しては平成 23 年度に引き続き検討する。

3.1.6.1 HPCI 提供資源管理簿

- 資源提供連携ネットワーク委員会（仮称）が年 2 回（1 月末, 6 月末）に作成する提供資源リストを「HPCI 提供資源管理簿」で管理すること。提供資源リストは，各資源提供機関から提供される以下の情報を含む。「HPCI 提供資源管理簿」は，これらの情報を格納可能であること。
    - 提供資源名
    - ハードウェアおよびソフトウェア仕様
    - AUP/SLA
    - 割当て単位と割当て可能量
    - 提供可能期間

- 「HPCI 提供資源管理簿」は，提供資源の割当て単位ごとに割当て可能量と提供可能期間を予約管理できること。課題審査委員会で資源割当ての検討できるようにオンラインで予約マップを表示し，予約割当てが可能であること。

- 「HPCI 提供資源管理簿」を元に，HPCI 利用課題募集要項と HPCI 利用課題申込書を更新し，年 2 回（2 月，7 月の 1 ヶ月間を想定），HPCI 利用課題公募を行うこと。

- 「HPCI 提供資源管理簿」を元に，課題審査委員会に対して，割当て可能な提供資源リストを提出すること。

- 課題審査委員会が各利用課題に割り当てた資源量と課題実施期間を「HPCI 提供資源管理簿」に反映し，資源提供連携ネットワーク委員会（仮称）に通知すると同時に，個々の資源提供機関との「連携用データベース」(後述)を更新すること。

- 課題審査委員会によって利用課題に対して資源の割り当てが行われた後に，未割当て

になっている資源の取り扱いに関しては，資源提供機関が回収し一般利用に組み込むなどが検討されたが，HPC ストレージの扱いなども含め平成 23 年度に引き続き検討を行う。

3.1.6.2 連携用データベース

- 「連携用データベース」は，資源提供機関 / 提供資源 / 利用課題 (HPCI 利用課題 ID = グループ・ニックネーム)という階層で情報を保持すること。

- 利用課題に対して次の属性情報を保持できること
  - 割当てられた資源量
  - 課題実施期間
  - 課題実施者の HPCI-ID のリスト
  - HPCI-ID と英文氏名の対応リスト（IdP 運用機関のみ）

- 資源提供機関毎にホストベースのアクセス制限を設定し，公開鍵による認証と，通信を暗号化して閲覧が可能であること。

- 履歴管理が可能であること。

- 資源提供機関が自動的なスクリプト処理によって定期的に grid-mapfile を自動生成可能なように配慮されていること。

3.1.6.3 Web ポータル上での各種処理の自動化(案)

- 資源提供機関に対し，Web ポータル上から提供資源の登録が行えるようなインターフェースを提供する(図 3.5)。
- 詳細に関しては平成 23 年度に検討する。

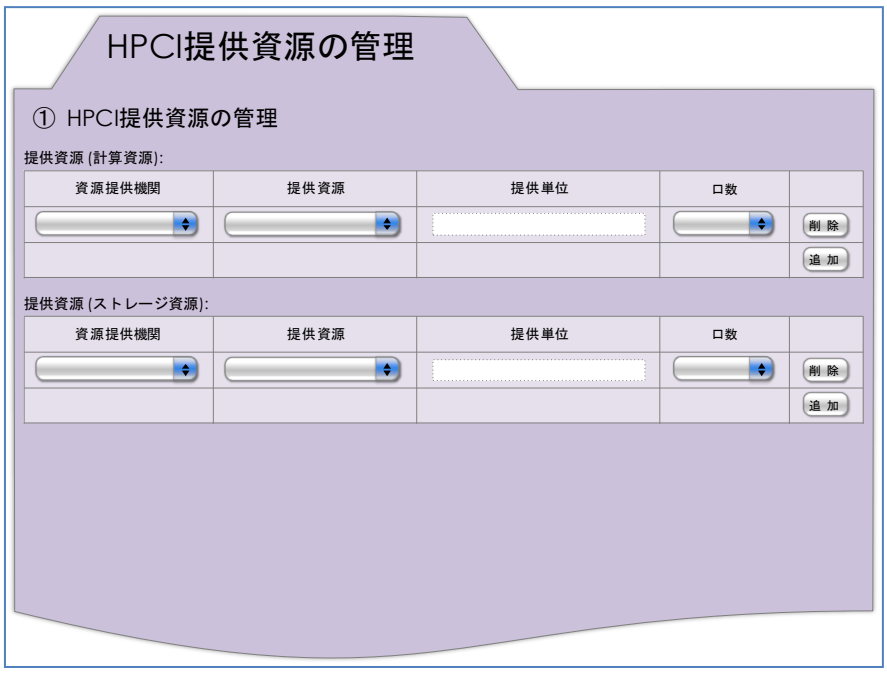


図 3.5 提供資源の登録インターフェース(案)

3.1.7　アカウント申請および作成手続き

ここでは，2.2 節および 2.3 節の利用シナリオにもとづいて，アカウント申請および作成手続きに関する以下の処理フェーズごとに HPCI に参加する各機関に対する基本仕様をまとめる。

想定する処理：

1. HPCI 利用申請受付
2. 利用資格審査
3. 課題審査
4. 審査結果通知
5. HPCI アカウント発行
6. ローカルアカウント作成
7. クライアント証明書(ユーザ証明書)発行
8. grid-mapfile 設定
9. 利用可能通知
10. HPCI 利用課題管理簿の操作

3.1.7.1　HPCI 利用申請受付

HPCI 事務局は，別途運営規定等で定められる HPCI 課題公募期間に，HPCI 利用有資格者からの HPCI 利用申請を受け付ける。

(1) 前提条件

- HPCI の利用資格は別途定められていることとする。
- 利用課題公募に関する規約が別途定められていること。規約には公募スケジュールなどが定められているものとする。
- 「HPCI 利用課題申請」は，課題名と概要，課題代表者と副代表者，連絡責任者および課題実施者，利用を希望する資源を記載し，所属機関長の職印を伴って HPCI 事務局へ電子メールおよび郵送で申請する。

(2) HPCI 事務局に対する要件

- 利用課題公募に関する規約に基き，利用課題公募の要項を作成し，公表すること。
- 利用課題申請に関する情報を管理するため，「HPCI 利用課題管理簿」を作成・保守すること。
- 「HPCI 利用課題申請」は，課題公募期間ごとに受け付けを行う。
- 次の属性情報を記載可能な「HPCI 利用課題申請」用 Web フォームを作成し，「HPCI 利用課題管理簿」と連動させること。
  - 課題代表者の氏名と HPCI-ID

- 課題副代表者の氏名とHPCI-ID（最低1名）
- 連絡責任者の氏名とHPCI-ID，連絡先（住所，電子メールアドレス，電話およびファックス番号）
- 課題実施者の氏名とHPCI-ID，役割・担当分野
- 外国籍の実施者が含まれる場合は，国籍と現居住地と勤務年数（1年未満の場合は月数）を補記
- 課題名
- 概要（目的・意義・必要性，利用計画，これまでの業績・成果）
- 希望する資源と割当量，それらの利用計画
- 所属機関長の職・氏名と職印
- 募集要項と記載内容への誓約確認
- 課題実施者の本人性確認情報

- 利用課題申請用Webフォームの画面案を図 3.6～図 3.9に示す。図中の「照合コード」は3.1.5.4節で述べたWebポータル上での申請処理を自動化案で導入される，HPCI-IDの入力を支援するためのものである。

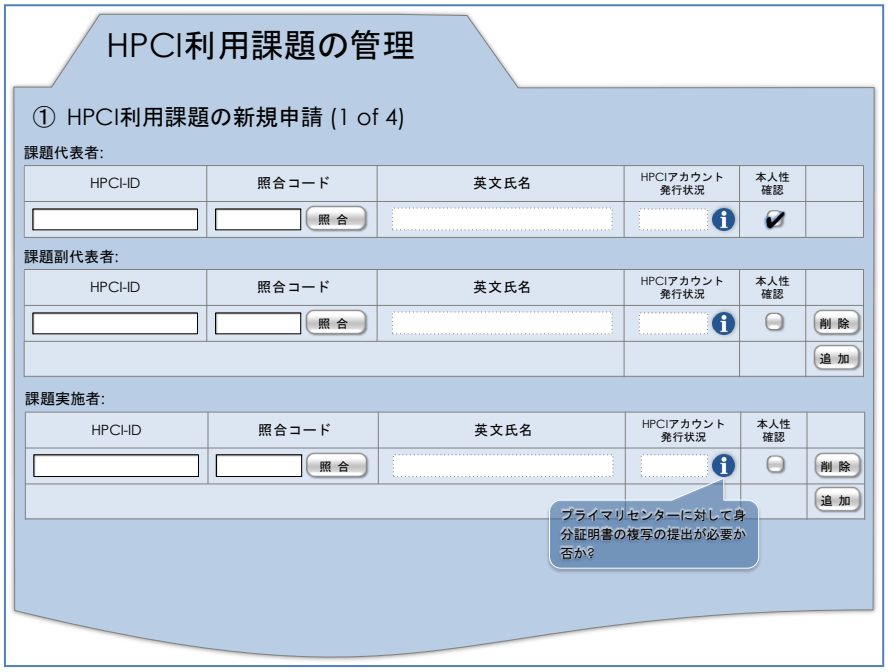


図 3.6 利用課題申請用Webフォーム画面(案) 1/4

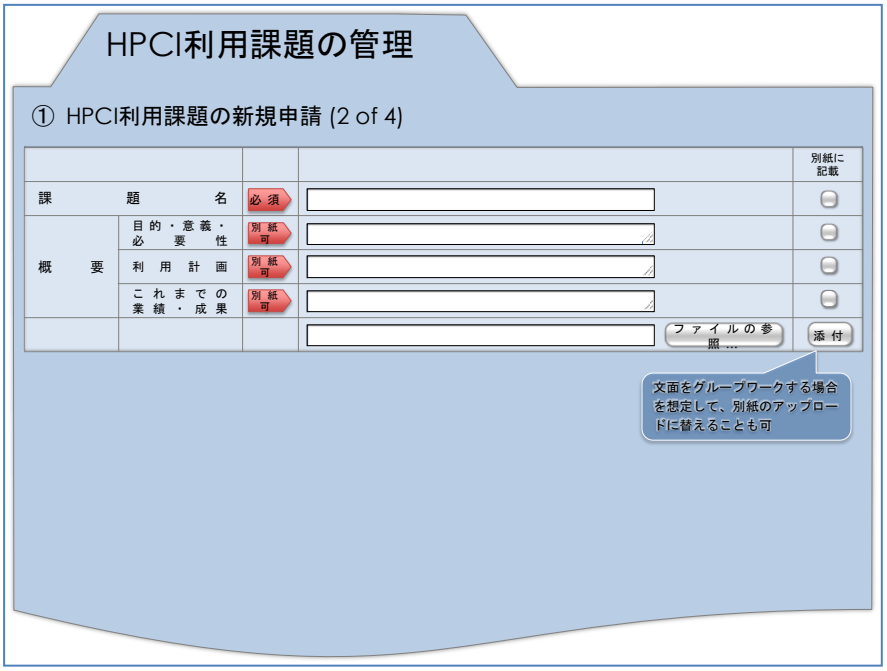


図 3.7 利用課題申請用 Web フォーム画面(案) 2/4

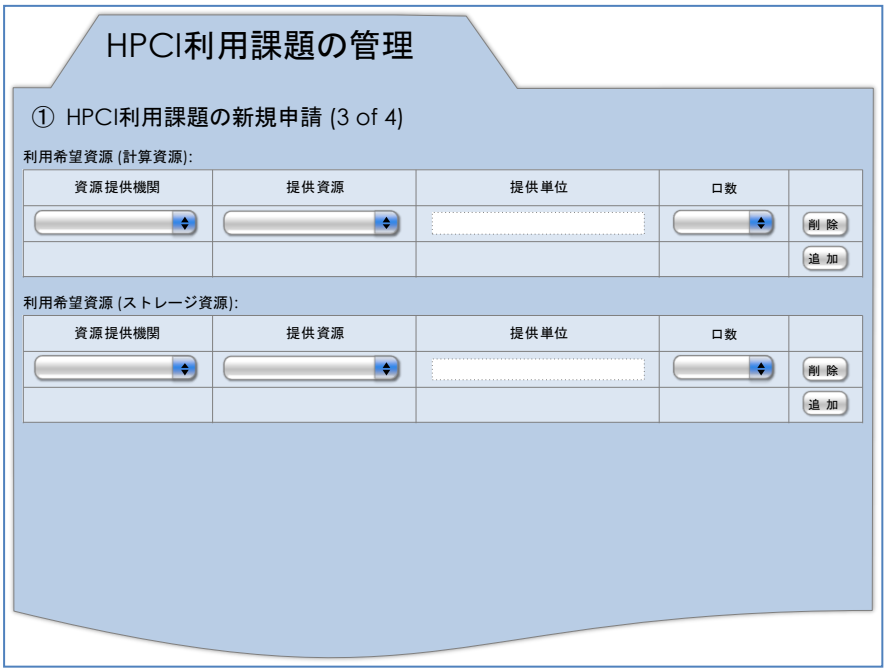


図 3.8 利用課題申請用 Web フォーム画面(案) 3/4

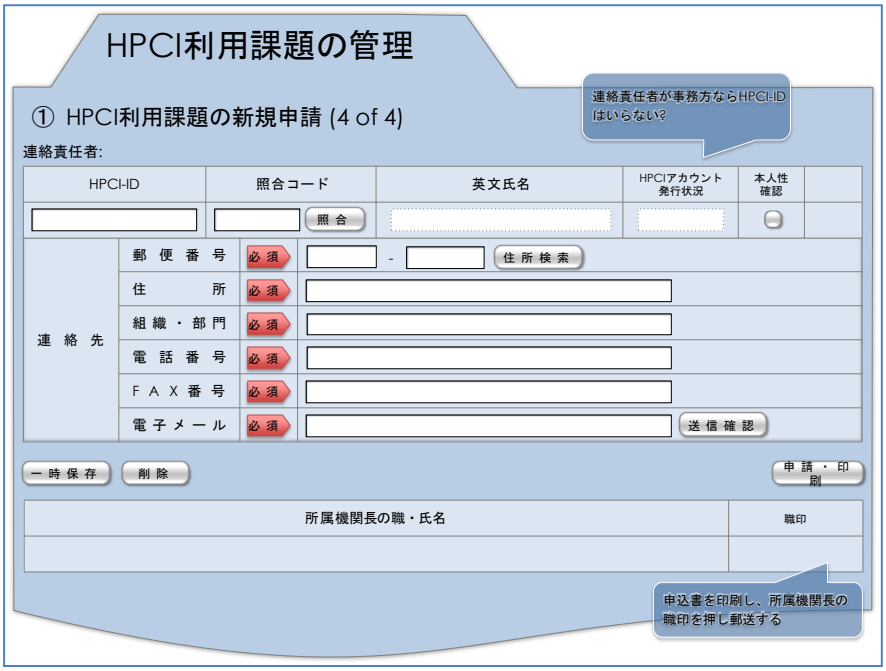


図 3.9 利用課題申請用 Web フォーム画面(案) 4/4

- 入力フォームは必要に応じて改版すること。その場合は「HPCI 利用管理簿」と連動を維持すること。
- 電子申請システムは重要事項を入力するための Web フォーム，入力された情報から所定の書式に従った申請書の PDF ファイルを作成し，それを申請者が保存できる機能を提供すること。
- HPCI 利用課題管理簿で管理される情報には Web フォームで入力された申請情報，申請者から郵送される押印された申請書，本人性確認情報が含まれる。
- HPCI 利用課題管理簿に登録された Web フォームで入力された情報，申請者から郵送された情報を照合し，内容が一致しない課題については，申請者に差し戻す。差し戻した申請の取り扱いについては別途定める必要がある。

(3) Web ポータル上での申請処理の自動化(案)

HPCI 利用課題申請に関しても，Web ポータル上での申請処理の自動化案を採用することを検討した。

- 3.1.5.4 節と同様に，有効な HPCI アカウントを持たない利用者は，HPCI 事務局によって承認された IdP のアカウントによって Web ポータルの初回認証を行うことで，HPCI 利用課題新規を行うことができる(図 3.3 参照)。
- 「HPCI 利用課題申請」Web 入力フォームに HPCI-ID を入力する際は，セキュリティコードと照合することで HPCI-ID 保持者の英字氏名 (displayName) を表示

し，誤入力を防止する。課題登録時に，課題従事者すべてに課題名を電子メールで通知する事で，HPCI-ID が参照され，課題に従事者として含まれたことを通知する。

- 概要などの長文は Word 文書の添付でフォーム入力に替えることができる。その場合は，添付文書に記載されていることをチェックボックスで確認できるように配慮する。
- 詳細は平成 23 年度に設計することとする。

3.1.7.2 利用資格審査

HPCI 事務局は，受け付けた利用課題のすべての課題従事者が HPCI 利用資格を満たしていることを確認する。

(1) 前提条件

- この段階での利用資格の確認は，形式的なものとなる。
- 本人性確認情報として提出される書類に，HPCI 利用資格を確認することができるものが含まれているものとする。
- HPCI 利用資格を確認するための書類としてどのようなものを採用するかなどの詳細については平成 23 年度に検討する。

(2) HPCI 事務局に対する要件

- 申請を受け付けた利用課題のすべての課題従事者に対し，本人性確認のための書類として指定されたものが提出されていることを確認する。
- 利用資格を確認できないメンバーが含まれる課題については，申請者に差し戻す。差し戻した申請の取り扱いについては別途定める必要がある。

3.1.7.3 課題審査

HPCI 事務局は，利用資格審査を経た利用課題申請を集約し，それらの審査を課題審査委員会に付議する。

(1) 前提条件

- 課題審査委員会の設置・運営について別途定められていることとする。
- 課題審査委員会に関する HPCI 事務局の役割についても規定されることとする。ここでは，課題審査委員会における審査のために必要な書類の準備と配布を行うものと想定する。

(2) HPCI 事務局に対する要件

- 課題審査委員会における審査のために必要な書類の準備と審査委員への配布を行う。

(3) Web ポータル上での申請処理の自動化(案)

- 課題審査委員会の各委員に対し，審査に必要な書類を Web ポータル上から取得することができるようなインターフェースを提供する(図 3.10)。
- 詳細に関しては平成 23 年度に検討する。

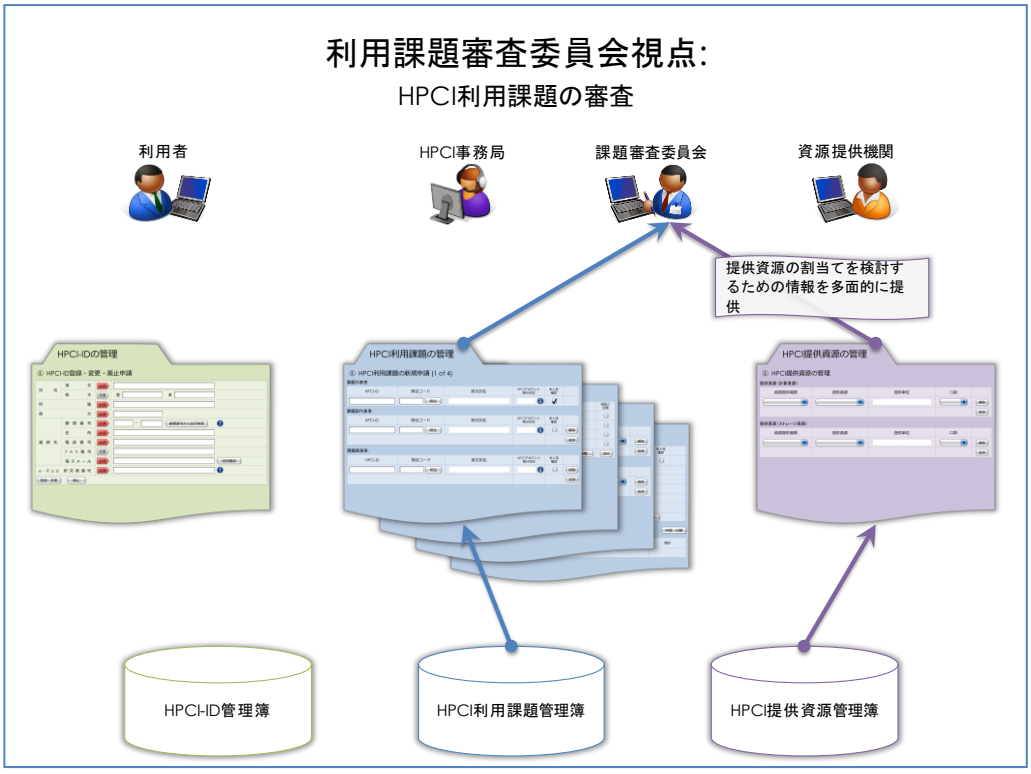


図 3.10 Web ポータルからの審査書類の配付(案)

3.1.7.4 採否通知

HPCI 事務局は課題審査委員会の審査結果を利用課題の連絡責任者に連絡する。申請通りの負担金減免が認められなかった課題については，審査結果を受け入れるかどうかの意思を確認する。

(1) HPCI 事務局に対する要件

- 課題審査委員会の審査結果を利用課題の連絡責任者に通知する。
- 無償型・利用負担金減免型の申請課題について，申請時の希望通りに採択さ

れなかった場合には課題審査によって決定された利用者負担を受け入れるかどうかを回答するよう連絡責任者に依頼する。審査結果を受け入れない場合には申請を却下する。

- 課題審査委員会の審査結果および利用意思の回答に基づき，それぞれの課題に対して HPCI 利用課題 ID を発行し(HPCI 利用課題 ID の発行規約は別途運営規則等で定められるものとする)，利用を許可された資源に関する情報とともに，利用課題管理簿に登録する。

3.1.7.5 HPCI アカウント発行

HPCI 事務局は，課題審査委員会の審査結果および申請者による利用意思の回答結果に基づき，HPCI アカウントの発行処理を依頼する。

(1) 前提条件

- HPCI アカウントの発行依頼は利用課題ごとに行なう。
- 資源提供機関として，Shibboleth 認証を行う機関と OpenID などを認証に用いる機関を想定する。
- Shibboleth 認証を用いる資源提供機関を利用する場合，HPCI アカウント発行時に，プライマリセンターにおいて，利用課題の課題従事者の本人性確認および利用資格の確認を行う。本人性確認の手続きとしては，当該課題従事者の身分証と利用資格を有することが確認できる書類の複写を提示することを要件とする。本人確認手続きの詳細についてはさらに検討を行う。
- OpenID などを認証に用いる資源提供機関のみを利用する利用課題の場合に，HPCI 利用資格を確認する手順については平成 23 年度に検討を行うものとする。
- 同一の利用者が複数の課題の新規メンバーとして同時に HPCI アカウントの発行を受ける場合，各課題のプライマリセンターが異なっていると，当該利用者に複数の HPCI アカウントが交付される可能性がある。このような場合でも証明書は 1 通しか交付されないような認証基盤を構築する必要がある。
- HPCI-ID 管理簿には，当該 HPCI-ID を所有する利用者の HPCI アカウント取得状況に関する情報も含まれているものとする。

(2) HPCI 事務局に対する要件

- 当該利用課題が Shibboleth 認証を行なう資源提供機関を利用する場合は，その課題のプライマリセンターに課題従事者の HPCI アカウントの発行処理およびその結果の連絡を依頼する。依頼時には課題従事者の HPCI-ID および HPCI アカウント取得状況情報を添付する。同時に，利用課題の連絡責任者に，

プライマリセンターにおいて課題従事者の本人確認手続きを行うよう連絡する。

- プライマリセンターから当該利用課題の課題従事者に関する HPCI アカウント発行結果の連絡を受けたら，その内容で HPCI-ID 管理簿を更新する。
- 当該利用課題が OpenID などを認証に用いる資源提供機関を利用する場合は，利用課題の連絡責任者に課題従事者が HPCI アカウントの自己取得を行い，その結果を HPCI 事務局に通知するよう依頼する。
- OpenID などを認証に用いる場合の HPCI アカウント取得結果の連絡を受けたら，その内容で HPCI-ID 管理簿を更新する。

(3) プライマリセンターに対する要件

- 当該利用課題のすべての課題従事者の HPCI アカウント取得情報を確認し，有効な HPCI アカウントを保有していない場合には，HPCI アカウントの発行手続きを行なう。
- 当該利用課題のすべての課題従事者の本人確認手続きを行ない，HPCI-ID と HPCI アカウント取得情報を HPCI 事務局に，発行した HPCI アカウントに関する情報を利用課題の連絡責任者にそれぞれ通知する。

3.1.7.6 ローカルアカウント作成

(1) 前提

- 利用課題ごとに統一グループ名が付与されているものとする。
- 統一グループ名に関する議論については，3.1.3.2 節を参照のこと。

(2) HPCI 事務局に対する要件

- 各採択課題について，HPCI アカウントの作成完了の通知を受けたあと，当該課題で利用する資源提供機関に，以下の情報を通知する。
  - 課題に付与された統一グループ名
  - 課題が利用を承認された資源提供機関およびその資源の一覧
  - 課題に参加している全利用者の一覧(HPCI-ID，HPCI アカウントを含む)

(3) 資源提供機関に対する要件

- HPCI 事務局から送付された情報に基づき，各利用者に必要なローカルアカウントを用意する。
- 当該利用者がすでに有効なローカルアカウントを保持している場合には，それを流用してもよい。但し，その利用者が当該利用課題の経費負担によってその資源を利用できるよう必要なグループ設定等を行なう。

- ローカルアカウントが用意できたら，その旨を利用課題の連絡責任者および HPCI 事務局に通知する。

3.1.7.7 クライアント証明書（ユーザ証明書）発行

(1) HPCI 事務局に対する要件

- HPCI-IDとHPCIアカウント情報を認証局運用機関に通知し，証明書発行のための準備を依頼する。
- 利用課題の連絡責任者に対し，認証ポータルにアクセスして証明書発行のための手続きを実施するように通知する。

3.1.7.8 grid-mapfile 作成

(1) HPCI 事務局に対する要件

- 資源提供機関が自動的なスクリプト処理によって定期的に grid-mapfile を自動生成可能なように，連携用データベースに必要な情報を保持すること。
- 連携用データベースについては 3.1.6.2 節を参照すること。

(2) 資源提供機関に対する要件

- HPCI 事務局が管理する利用課題管理簿より，grid-mapfile 生成に必要な情報を取得する。
- 認証局運用機関の証明書管理システムより，grid-mapfile 生成に必要なマッピング情報を取得する。
- 自らが管理する利用者の HPCI-ID とローカルアカウントのマッピング情報とあわせて，grid-mapfile を生成する処理を定期的に実行し，各提供資源の grid-mapfileを更新する。

3.1.7.9 利用可能通知

(1) HPCI 事務局に対する要件

- 各利用課題について，利用する資源提供機関からのローカルアカウント作成完了通知を集約し，すべてがそろった時点で，その旨を利用課題の連絡責任者に通知する。

3.1.7.10　HPCI 利用課題管理簿の操作

HPCI 事務局は，応募された HPCI 利用課題に対して「HPCI 利用課題 ID」を発行し管理する。HPCI 利用課題 ID は，資源提供機関においてグループ名として参照されることを想定している。HPCI 利用課題 ID として用いることができる文字数や文字種の制約に関しては調査・検討を要する。

- 申請を受け付けた HPCI 利用課題を，HPCI 利用課題管理簿に登録し，採択課題に関しては，課題実施期間終了後一定期間保持する。この保持期間は 10 年間を想定する。また，不採択課題に関しても一定期間保持するが，この保持期間は 3 年間を想定する。それぞれの保持期間については別途運営規則等で定められることとする。
- 「HPCI 利用課題管理簿」は次の仕様を満たして管理されること。
    - HPCI 利用課題 ID に対して「HPCI 利用課題申込書」に記載される情報を新規登録および更新登録が可能であること。
    - 更新登録では，利用課題の継続，変更（課題実施者）が行えること。
    - 割当て資源の変更は「HPCI 提供資源管理簿」で行う。HPCI 利用課題 ID から割当て資源を参照する機能を有すること。
    - 連絡責任者に対する課題の採否の通知，利用の意志確認などの業務フローの追跡管理が可能であること。
    - HPCI 利用課題 ID と課題実施者の HPCI-ID の対応表を，HPCI 提供資源管理簿と連動して資源提供機関に通知すること。この通知に連動して，資源提供機関のローカルアカウントの利用開始・停止措置が可能であること。
    - HPCI-ID が失効した課題従事者が含まれる利用課題を随時抽出し警告表示ができること。

3.1.8　ヘルプデスク基本仕様

HPCI 環境における各種の問い合わせに対応するために HPCI 事務局はヘルプデスクを設けることとする。また，各資源提供機関はヘルプデスクの業務を遂行するために必要な協力体制を整えることとする。

ヘルプデスクは，以下の要件を満たしていなければならない。

- Web インターフェースにより HPCI 環境に関する利用方法の問い合わせや障害報告，バグ報告が可能であること。
- メールによっても Web インターフェース経由と同様の問い合わせおよび報告が可能であること。
- セキュリティに関する問い合わせ・報告とその他の問い合わせ・報告はそれぞれ別々の受付窓口により受け付けられること。
- セキュリティに関する問い合わせや報告とその回答に関しては必要な関係者以外への閲覧を制限できること。
- セキュリティに関する問い合わせや報告以外では，問い合わせ内容やその回答が必要に応じて他の利用者に対しても公開されること。
- Web やメールによって受け付けられた問い合わせや報告はチケットとしてヘルプデスクに登録され，適切に処理が行われるよう管理されること。
- 問い合わせや報告の内容に応じて，それぞれの案件を処理する業務フローが明確になっていること。また，業務フローにおける各業務を処理する担当者の役割や権限が明確になっていること。
- HPCI 環境で用いられている各種ソフトウェア（ユーザアプリケーションは除く）のそれぞれに対して，報告された不具合に関する調査依頼先が明確になっていること。
- プログラム開発・修正が必要と判断された場合に，開発チームに作業依頼ができること。

HPCI 環境に参加する各機関は以下の要件を満たしていなければならない。

- ヘルプデスクを運用するために，HPCI 環境に参加する各機関（HPCI 事務局，各資源提供機関）は必要に応じて連携して作業を行なうこと。また，そのための体制を整えること。

3.1.9　情報共有 CMS 基本仕様

HPCI 事務局は HPCI 環境における情報共有のための CMS を設置し運用管理する。情報共有 CMS は以下に挙げる目的別に設置する。

- 運用管理者向け
- 研究者向け
- 開発者向け
- 利用者向け

- HPCI 事務局は情報共有 CMS を運用管理するための運用管理マニュアルを整備すること。

- 運用管理者向け，および研究者向けには HTML などの知識がなくても容易に Web ページを作成・管理できる CMS を提供すること。

- 開発者向け CMS はヘルプデスクに報告された不具合に対して開発チームが修正作業を行う場合などに利用するため，開発チームが利用可能なバージョン管理システムを運用し開発者向け CMS と連携させること。

- 利用者向け CMS では HPCI 環境の各資源の計画停止スケジュールや障害状況などの運用情報が参照できること。また，各資源提供機関の提供資源に関する情報を参照できること。

- 資源提供機関は提供する資源の保守や点検などの計画停止スケジュールを HPCI 事務局に通知し，情報提供 CMS により利用者に周知すること。

- 認証局運用機関は提供する資源の保守や点検などの計画停止スケジュールを HPCI 事務局に通知し，情報提供 CMS により利用者に周知すること。

- 認証ポータル運用機関は提供する資源の保守や点検などの計画停止スケジュールを HPCI 事務局に通知し，情報提供 CMS により利用者に周知すること。

- HPCI アカウント IdP 運用機関は提供する資源の保守や点検などの計画停止スケジュールを HPCI 事務局に通知し，情報提供 CMS により利用者に周知すること。

  - 書き込み操作を許可するために利用者の認証を必要とすること。

・　運用管理者向けのページはあらかじめ登録されたユーザのみが書き込み権限を持つようにアクセス制限を行うこと。

3.1.10 広報活動業務

3.1.10.1 申込書式の作成と配布

HPCI 事務局は,「HPCI-ID 登録申込」書式と「HPCI 利用課題申込」書式を作成し, Web サイトから電子的に公開する。

(1) 申込書式の作成と改版

- 申請書式の作成にあたっては,「学際大規模情報基盤共同利用・共同研究拠点」事業および「先端的大規模計算利用サービス」事業の申込書式を参考にすること。
- 課題申込書は様式番号と日付による版管理が行われること。
- 版毎の改訂を管理簿（データベース）と連動できるように配慮すること。

(2) 募集要項の作成と配布

- HPCI 事務局は, 募集要項と申込書記入要項を作成し, 申込書と共に, Web サイトから電子的に配布を行うこと。
- HPCI コンソーシアムが開催する公募説明会を支援すること。

3.1.11 障害対応フロー

HPCI 環境において障害が発生したときに，その障害対応に関して HPCI 事務局および各資源提供機関が果たすべき役割や実施すべき業務フローの詳細について平成 23 年度に検討を行う。そのための前提となる要件は以下のとおりである。

3.1.11.1 HPCI 事務局

- HPCI 事務局はヘルプデスクに登録された障害報告に対し，障害対応マニュアルに従ってチケットの処理を開始するものとする。
- そのために必要な障害対応マニュアルを整備すること。
- 障害対応マニュアルは以下の内容を含むこと。
  - マニュアル障害対応マニュアルにはチケットのオープンからクローズまでのライフサイクルの各段階での処理の進め方や，それぞれの段階における HPCI 事務局および資源提供機関の役割が明記されていること。
  - 障害対応マニュアルにはセキュリティ専用ヘルプデスクに登録すべき内容が登録された場合の対応についても明記されていること。
  - その他の詳細な記載内容については発注者と協議の上，決定すること
- HPCI 事務局は依頼したチケットの処理が滞留しないように，進捗管理を行うこと。
- HPCI 事務局は障害発生部位の切り分けの結果に基づき，チケットの処理を担当する機関を割り当て，処理を依頼すること。また，必要に応じてチケットの処理を担当する機関の再割り当てを行うこと。

- HPCI 事務局は実際に障害が発生していることが確認されたのちに，情報共有 CMS に障害状況を登録し，HPCI 利用者に対して周知すること。また，チケット処理の進捗に応じて情報共有 CMS に登録した障害状況を更新すること。
- HPCI 事務局は当該チケットの処理が完了したのち，障害対応マニュアルに従って，チケットのクローズ処理を行う。

- HPCI 事務局はヘルプデスクに登録されたバグ報告に対し，バグ報告対応マニュアルに従ってチケットの処理を開始するものとする。そのために必要なバグ報告対応マニュアルを整備すること。バグ報告対応マニュアルにはチケットのオープンからクローズまでのライフサイクルの各段階での処理の進め方や，それぞれの段階における HPCI 事務局および開発チームの役割が明記されていること。開発チームの作業に必要な環境の準備方法についてもバグ報告対応マニュアルに明記すること。

- HPCI 事務局は開発チームの組織についての規約を策定すること。

- HPCI 事務局はセキュリティ専用ヘルプデスクに登録されたセキュリティに関する報告・問い合わせに対し，セキュリティ報告対応マニュアルに従ってチケットの処理を開始するものとする。また，登録されたセキュリティに関する報告が重大なセキュリティ・インシデントであると判断した場合には，インシデント・レスポンス・チームへ対応を依頼する。そのために必要なセキュリティ報告対応マニュアルを整備すること。セキュリティ報告対応マニュアルにはチケットのオープンからクローズまでのライフサイクルの各段階での処理の進め方や，それぞれの段階における HPCI 事務局およびその他の HPCI 参加機関の役割が明記されていること。

3.1.11.2 資源提供機関

- 資源提供機関は HPCI 事務局から依頼された障害対応に関するチケットの処理を障害対応マニュアルに従って実施すること。そのために必要な体制を整備すること。
- 資源提供機関は提供資源における障害発生を HPCI 事務局に報告するとともに，情報共有 CMS により利用者に周知すること。障害対応・復旧後にも HPCI 事務局に報告するとともに，情報共有 CMS により利用者に周知すること。そのための障害対応マニュアルを整備すること。
- 資源提供機関は HPCI 事務局から依頼されたセキュリティ報告対応に関するチケットの処理をセキュリティ報告対応マニュアルに従って実施すること。そのために必要な体制を整備すること。
- 資源提供機関は，自組織においてセキュリティ・インシデントが発生したとき，HPCI 向けセキュリティ・インシデント対応マニュアルに従って対応すること。

3.1.11.3 認証局運用機関

- 認証局運用機関は HPCI 事務局から依頼された障害対応に関するチケットの処理を障害対応マニュアルに従って実施すること。そのために必要な体制を整備すること。
- 認証局運用機関は提供資源における障害発生を HPCI 事務局に報告するとともに，情報共有 CMS により利用者に周知すること。障害対応・復旧後にも HPCI 事務局に報告するとともに，情報共有 CMS により利用者に周知すること。
- 認証局運用機関は HPCI 事務局から依頼されたセキュリティ報告対応に関するチケットの処理をセキュリティ報告対応マニュアルに従って実施すること。そのために必要な体制を整備すること。

3.1.11.4 認証ポータル運用機関

- 認証ポータル運用機関はHPCI事務局から依頼された障害対応に関するチケットの処理を障害対応マニュアルに従って実施すること。そのために必要な体制を整備すること。
- 認証ポータル運用機関は提供資源における障害発生を HPCI 事務局に報告するととも

に，情報共有 CMS により利用者に周知すること。障害対応・復旧後にも HPCI 事務局に報告するとともに，情報共有 CMS により利用者に周知すること。そのための障害対応マニュアルを整備すること。

- 認証ポータル運用機関は HPCI 事務局から依頼されたセキュリティ報告対応に関するチケットの処理をセキュリティ報告対応マニュアルに従って実施すること。そのために必要な体制を整備すること。

3.1.11.5 HPCI アカウント IdP 運用機関

- HPCI アカウント IdP 運用機関は HPCI 事務局から依頼された障害対応に関するチケットの処理を障害対応マニュアルに従って実施すること。そのために必要な体制を整備すること。
- HPCI アカウント IdP 運用機関は提供資源における障害発生を HPCI 事務局に報告するとともに，情報共有 CMS により利用者に周知すること。障害対応・復旧後にも HPCI 事務局に報告するとともに，情報共有 CMS により利用者に周知すること。そのための障害対応マニュアルを整備すること。
- HPCI アカウント IdP 運用機関は HPCI 事務局から依頼されたセキュリティ報告対応に関するチケットの処理をセキュリティ報告対応マニュアルに従って実施すること。そのために必要な体制を整備すること。

3.1.12 ツール群

3.1.12.1 HPCI ポータルシステム

HPCI ポータルシステムは，2.2～2.4 節および 3.1.5～3.1.7 節において HPCI 事務局の作業工数を軽減するための案として示した，Web ポータル上での処理の自動化を実現する。利用者，HPCI 事務局，資源提供機関，認証局運用機関を含む業務フローの各ステップの遷移がなるべく人手を介さずに行われるような機能も含め，詳細に関しては平成 23 年度に検討を行う。

3.1.12.2 アカウンティング集計ソフトウェア

HPCI 環境に資源を提供する各機関において，それぞれ独自にアカウンティング情報を収集しているものと考えられる。それらの情報を HPCI 環境内で共通の意味と形式を持つ HPCI アカウンティング情報として収集および集計するために以下の各項目を平成 23 年度に実施する。

(1) HPCI 事務局において実施するもの

- 平成 23 年度において資源提供機関として想定される各情報基盤センターにおいて収集・集計しているアカウンティング情報について調査し，HPCI 環境内で共通に用いるための用語とその概念，および情報の表現形式を定義すること。

- HPCI アカウンティング情報としては，以下に例としてあげる各項目が考えられるが，各資源提供機関が HPCI 向けに提供可能なアカウンティング情報を調査し，HPCI アカウンティング情報として収集・集計する項目を決定すること。
  - セッションに関する情報
    - 利用時間，実行コマンド
  - 計算資源に関する情報
    - CPU 使用量，メモリ使用量
    - 実行コマンド単位，ジョブ単位
  - ストレージ資源に関する情報
    - ストレージ使用量
  - 収集する単位
    - アカウント毎，グループ毎

- HPCI アカウンティング情報を収集・集計・参照するための方式を検討し，必要なソフトウェアの仕様を決定すること。その際，アカウンティング情報がインターネット経由で受け渡しされることを想定し，セキュリティに関して考慮すること。

- HPCI アカウンティング情報を管理するために必要な機器の仕様を決定すること。

- HPCI アカウンティング情報として収集・集計する際に，それぞれの資源提供機関におけるローカルアカウントやグループ毎に収集・修正されている情報を HPCI における HPCI アカウントや HPCI 課題グループに関連付けることが望ましい。各資源提供機関において収集・集計しているアカウンティング情報を HPCI アカウントおよび HPCI 課題グループ毎に集計するための方式を検討すること。

(2) 各資源提供機関において実施するもの

・ HPCI アカウンティング情報の収集・集計に関して，各資源提供機関は以下の内容を満たすドキュメントを作成する。

- 各資源提供機関が独自に収集・集計しているアカウンティング情報について
  - HPCI 向けに提供できる情報項目の一覧とそれらの情報項目の定義を明確に説明したドキュメント
  - HPCI 向けに提供できる情報項目に関し，収集・集計した結果から利用者および管理者がそれらを取得するためのコマンドや API 等の使い方を説明したドキュメント

3.1.13 今後の検討課題

ユーザ管理支援に関する基本仕様として，ここまでに示した内容において今後の検討課題としたものを，ここにまとめておく。

3.1.13.1 HPCI-ID に関するもの

- HPCI-ID の一意性を確保するために用いる個人識別番号として，e-Rad 研究者番号を想定するが，e-Rad 研究者番号が取得できない場合の代替個人認識番号について検討する
- HPCI 利用資格の有無を確認する方法、および HPCI-ID の申請時に登録した個人識別情報が確かに申請者の所有するものであることを確認する方法について検討する
- e-Rad 研究者番号を取得しているときに，HPCI-ID を取得した者が e-Rad 研究者番号を失効させたときの取り扱い，および e-Rad 研究者番号を取得できない者が HPCI-ID を取得し，その後 e-Rad 研究者番号を取得した場合の取り扱いを検討する。
- HPCI-ID の失効処理に関する手続きについて検討する。
- HPCI-ID の有効期限と更新手続き，および有効期限内に HPCI-ID の属性情報に変更が生じた場合の手続きに関する規則の検討を行う。
- HPCI-ID の具体的なフォーマット・生成規則などの検討を行う。
- HPCI-ID の属性変更・更新・廃止申請において，本人による申請であることを確認する手順について検討を行う。
- HPCI-ID に関する緊急時対応について，さらに検討を行う。
- Web ポータル上での処理の自動化案の詳細について，さらに検討を行う。

3.1.13.2 HPCI 利用課題申請に関するもの

- 利用課題申請フローにおいて，HPCI 事務局，プライマリセンター，資源提供機関のそれぞれが行う利用資格審査・本人確認のために必要な書類，および具体的な確認内容について検討を行う(Shibboleth 認証を用いる資源提供機関の場合)。
- OpenID を認証に用いる資源提供機関の場合の，利用資格審査・本人確認手続きについて検討を行う。
- HPCI 利用課題 ID の付与，統一グループ名採用の可否，複数の利用課題に含まれる利用者に対するローカルアカウントとグループとの関係，についてそれぞれ検討を行う。
- Web ポータル上での処理の自動化案の詳細について，さらに検討を行う。

3.1.13.3　ヘルプフロー・障害フローに関するもの

- ヘルプデスクおよび情報共有 CMS を用いた障害あるいは問い合わせ対応に関する業務フローの詳細について検討を行う。
- セキュリティ・インシデントが発生したときの HPCI としての対応手順について検討を行う。
- HPCI としてのネットワーク・セキュリティ監査基準について検討する。
- 開発チームの組織・運営に関して検討を行う。

3.1.13.4　その他

- 提供資源管理業務について引き続き検討を行う。

4 事務局，資源提供基本仕様

本節では，事務局および提供組織が提供しなければならない計算機環境仕様，提供資源連携のための委員会仕様を決める。資源提供組織は，資源提供連携ネットワーク委員会（仮称）の一員とする。

4.1 事務局運用仕様

4.1.1 想定する利用者数，利用課題数，提供資源数

HPCI 事務局の運用仕様を検討するために, HPCI 利用者数, HPCI 利用課題数および HPCI 提供資源数として表 4.1 に示すものを想定した。

表 4.1 想定する HPCI 利用者数および HPCI 利用課題数

HPCI 利用者数	HPCI 利用課題数	HPCI 提供資源数
800 人	60 課題	20 資源

ここで, HPCI 利用者数および HPCI 利用課題数は平成 23 年当初の資源提供機関として想定される情報基盤センター群(9 機関)へのアンケート結果から見積もった数値である。平成 22 年度 2 月の実績で，9 機関の合計は 50 名未満の小規模グループが 662 件，50 名以上の大規模グループが 16 件であった。また，グループ当たりの平均登録者数は，中小規模グループが 7.1 名，大規模グループが 130.1 名であった。

「京」供用開始前の試行運用において，中小規模グループの内，複数センターに登録している割合を 3 割, さらにその内の 3 割が HPCI 経由での登録に移行することを想定すると，およそ 60 グループ，400 名の登録が見込まれる。また，大規模グループの内，2 割が応募すると想定すると，3 グループ，400 名の登録が見込まれる。これを合算して，当面の HPCI 利用課題数を 60 課題，HPCI 利用者数を 800 名と見積もっている。HPCI 提供資源数は 9 機関からそれぞれおよそ 2 個の資源が提供されるものとした。

また HPCI-ID 管理簿，HPCI 利用課題管理簿，HPCI 提供資源管理簿に登録し，管理するデータの件数は表 4.2 に示す件数を想定した。

表 4.2 各管理簿に登録される件数

HPCI-ID 管理簿	HPCI 利用課題管理簿	HPCI 提供資源管理簿
3000 件	120 件	20 件

ここで，HPCI-ID の有効期限を 10 年間，失効から 3 年間保存するものとし，毎年 20%程度の利用者が入れ替わると仮定して HPCI-ID 管理簿の件数を見積もった。また，HPCI 利用課題管理簿は年度末に旧年度分，新年度分それぞれ 60 件のデータを管理するものを仮定した。

4.1.2 構成要員

4.1.2.1 事務系職員

申請窓口業務を執り行う事務系職員の要員数を以下のように見積もっている。

- 申請期間を1ヶ月と想定して、HPCI-IDの申請数を800件と見積もると、平滑化して毎日40 件の処理（HPCI-ID 管理簿への入力、重複確認、発行通知）を行わなくてはならない。
- 書面による申請でも、専任して 2 名があたれば処理可能な業務量であるが、将来、HPCI-IDの申請数に応じた非常勤職員の手配が必要となることが予想される。
- さらに、HPCI-ID は、利用課題申請に先立って取得しておかなければならないので、実際は、より短期間に迅速に発行処理を行う必要がある。
- また、発行に際しては、e-Rad 研究者番号による重複確認を行うが、重複が検出された場合は、申請者に対する個別の確認業務が発生し、この例外対処にどれだけの要員を必要とするか、現時点で見積もることは非常に困難である。

利用課題申請を60件と見積もると、申請段階でHPCI-ID発行業務はほぼ完了していることが想定できるので、上述の専任2名の要員で、〆切日前後1週間ずつの期間があれば利用課題管理簿への入力を行う事が可能であると想定できる (3件/人日)。ただし、課題従事者がHPCI-IDを取得した有資格者か否かを逐一確認し、記載ミスや重複が検出された場合の例外対応業務が頻出した場合に、どれだけの要員が必要となるか、現時点で見積もることは非常に困難である。

採択後の通知業務は，1件当たり1人時とすれば60課題で60人時なので，2名の要員で1週間で処理可能な業務量である。

以上から、書面による申請を行うとすると、表4.1および表4.2で想定している応募数を処理するためには、登録受付期間内およびその後の2週間 (課題審査期間を除く) に、最低専任2名、予備1名の合計3名の事務職員で対応が可能であると推定できる。ただし、例外処理が起こったときの対応業務量を想定することは極めて難しく、また、HPCI-ID申請数や課題数に応じた要員が必要となり、想定する量を超える応募があった場合に遅延を見積もることも難しい。

これに対して、Web申請を導入すれば、管理簿への転記業務は必要なくなり、さらに申請時に申請者自身による例外対処を求めることで、例外対処要員数の不確定性を押さえることができる。表4.1および表4.2で想定している応募数を処理するためには、専任1名、

予備 1 名の合計 2 名の最低限の事務職員要員数で対応が可能であると推定でき、かつ、想定以上の申請があっても対応できると考えられる。

表 4.3 に上記の事務系職員の要員数に関する見積もり結果をまとめて示す。

表 4.3 事務系職員の要員数の見積もり

	800 名/60 件	1,600 名/120 件
書面申請の場合	専任 2 名, 予備 1 名	専任 4 名, 予備 2 名
Web 申請の場合	専任 1 名, 予備 1 名	専任 1 名, 予備 1 名

4.1.2.2 技術系職員

技術系職員の要員数の見積もりは以下の通り。

- SE 委託
  - 登録受付期間と課題審査期間は常時 1 名派遣
  - それ以外は遠隔対応で可

4.1.3 その他

- 個人情報の取扱基準を定め, 関連機関に遵守を促すこと。

4.2 計算機環境必須項目

4.2.1 事務局

本節では HPCI 事務局において HPCI-ID，HPCI 利用課題，HPCI 提供資源の管理，利用者向け Web サーバ，および資源提供計算資源との対応のために必要となるサーバ群一式の仕様を説明する。

4.2.1.1 管理簿サーバシステム

管理簿サーバシステムは HPCI-ID 管理簿，HPCI 利用課題管理簿，HPCI 提供機関管理簿を管理するためのシステムである。

以下の仕様をみたす管理簿サーバシステムを提供すること

1. 耐障害性を確保するため 2 台以上のサーバで冗長化し，Active･Stanby 構成とすること
2. サーバの障害時には必要に応じて自動的にフェールオーバーし，運用を継続できること
3. それぞれのサーバは Intel Xeon E5503 プロセッサ相当以上の性能･機能を有するプロセッサを搭載していること
4. それぞれのサーバは 16GB 以上の容量のメモリを有すること
5. それぞれのサーバは DVD-ROM を利用可能なドライブを 1 台以上有すること
6. それぞれのサーバは 2 ポート以上の 1000Base-T ネットワークインターフェースを有すること。
7. それぞれのサーバの内蔵ストレージは冗長化構成をサポートし，冗長化後の容量が 500GB 以上であること。
8. 管理簿データを格納するデータ用領域はサーバ間で共有あるいは常時複製され，それぞれのサーバ上で同一の内容となる設定とすること

4.2.1.2 利用者向け Web サーバシステム

利用者向け Web サーバシステムは，利用者向けの Web サーバを提供するためのシステムである。ヘルプデスクシステムおよび情報共有 CMS は利用者向けサーバシステム上で動作するものとする。また，DNS サーバとしても使用する。

以下の仕様をみたす利用者向け Web サーバシステムを提供すること

1. 耐障害性を確保するため 2 台以上のサーバで冗長化し，Active･Stanby 構成とすること
2. サーバの障害時には必要に応じて自動的にフェールオーバーし，運用を継続できること
3. それぞれのサーバは Intel Xeon E5620 プロセッサ×2CPU 相当以上の性能･機能を有するプロセッサを搭載していること

4. それぞれのサーバは 8GB 以上の容量のメモリを有すること
5. それぞれのサーバは DVD-ROM を利用可能なドライブを 1 台以上有すること
6. それぞれのサーバは 2 ポート以上の 1000Base-T ネットワークインターフェースを有すること。
7. それぞれのサーバの内蔵ストレージは冗長化構成をサポートし，冗長化後の容量が 300GB 以上であること。
8. Web コンテンツデータを格納するデータ用領域はサーバ間で共有あるいは複製され，それぞれのサーバ上で同一の内容となる設定とすること

4.2.1.3 資源提供機関向け連携サーバシステム

資源提供機関向け連携サーバシステムは，資源提供機関が HPCI アカウントの作成や grid-mapfile による認可情報を更新する際に必要となる情報を，管理簿サーバシステムに格納されている情報と連携しながら，適宜かつ安全に配信するためのシステムである。

以下の仕様をみたす資源提供機関向け連携サーバシステムを提供すること

1. 耐障害性を確保するため 2 台以上のサーバで冗長化し，Active･Stanby 構成とすること
2. サーバの障害時には必要に応じて自動的にフェールオーバーし，運用を継続できること
3. それぞれのサーバは Intel Xeon E5503 プロセッサ相当以上の性能･機能を有するプロセッサを搭載していること
4. それぞれのサーバは 16GB 以上の容量のメモリを有すること
5. それぞれのサーバは DVD-ROM を利用可能なドライブを 1 台以上有すること
6. それぞれのサーバは 2 ポート以上の 1000Base-T ネットワークインターフェースを有すること。
7. それぞれのサーバの内蔵ストレージは冗長化構成をサポートし，冗長化後の容量が 100GB 以上であること。
8. 資源提供機関の連携データを格納するデータ用領域はサーバ間で共有あるいは常時複製され，それぞれのサーバ上で同一の内容となる設定とすること

4.2.1.4 事務職員用端末システム

以下の仕様を満たす事務職員用端末システムを提供すること

4.2.1.4.1 事務職員用端末

以下の要件を満たす事務職員用端末を 3 台提供すること(←事務職員の人数分)

1. x86-64 アーキテクチャの CPU を搭載すること
2. 1 台あたりの CPU は 1 以上，コア数は 2 以上とし，2GHz 以上の性能を有すること。

3. メモリ容量は 4GB 以上であること。
4. 300GB 以上の容量を持つ内蔵ストレージを有すること。
5. DVD-ROM ドライブを有すること。
6. 日本語キーボードおよびマウスを有すること。
7. 1 台あたり 1 つ以上の 1000Base-T ネットワークインターフェースを有すること。
8. 1 台あたり 22 インチ以上で 1,920x1,080 以上の解像度を持つ液晶ディスプレイを有すること。
9. 端末のオペレーティングシステムとして Windows 7 Professional Edition 以上を提供すること。
10. マイクロソフト Office Home and Business 2010 相当以上を提供すること
11. ウィルス対策ソフトウェアを提供すること
12. 後述するカラープリンタのドライバを提供すること

4.2.1.4.2 カラープリンタ

以下の要件を満たすカラープリンタを 1 台提供すること

1. フルカラーモード毎分 30 枚以上の印刷が可能なこと
2. 両面印刷機能を有すること
3. A3, A4 自動切り替え機能を有すること
4. ネットワーク経由で IPP を利用して印刷可能なこと

4.2.1.5 ネットワークシステム

以下の仕様を満たすネットワークシステムを提供する

1. ネットワークシステムは,
   - 利用者へのインターフェースを提供する公開系,
   - 資源提供機関へのインターフェースを提供する公開系,
   - 認証局へのインターフェースを提供するプライベート系

   で構成される。
2. 公開系のネットワークにおいても個人情報が流通するために, SSL によって暗号化された通信を行う必要がある。
3. プライベート系のネットワークにおいては, 認証基盤サブシステムのマッピング情報管理システムがユーザ管理支援サブシステムの管理簿サーバシステムに格納された情報を参照する必要があり, より強固な秘匿性を提供できる VPN による通信が必要である。

詳細なネットワーク構成は, 事務局の開設場所が決まってから改めて検討する。

4.2.2　資源提供計算資源提供機関

資源提供機関における計算機環境や体制などに関する要件は，平成 23 年度に検討を行う。

4.3 資源提供利用規則必須項目

各資源提供機関より HPCI に提供される資源の利用規則は，各資源提供機関の利用規則を参考に平成 23 年度に検討する。

4.4 資源提供連携ネットワーク委員会基本仕様

4.4.1　資源提供ネットワーク委員会規則

資源提供連携ネットワーク委員会規則は，別途定めるが，以下の仕様を満たさなければならない。

- 定例委員会：年 1 回程度開催
- 臨時委員会：必要に応じて開催
- 委員の構成：資源提供機関の代表者（センター長），教員 1 名および職員
- 委員長：互選により決める
- 事務局：HPCI コンソーシアム事務局

4.4.2　ミッション

- HPCI に提供する資源の運営責任を持つ。
- 下部組織に資源提供連携ネットワーク運営・作業部会を設置し，当委員会で決定される方針に基づき，運営・作業部会に対して作業を依頼する。
- 運営・作業部会からの報告を受け，運営を決定する。

4.5 資源提供連携ネットワーク運営・作業部会基本仕様

4.5.1　資源提供連携ネットワーク運営・作業部会規則

資源提供連携ネットワーク運営・作業部会規則は，別途定めるが，以下の仕様を満たさなければならない。

- 定例委員会：定例委員会の開催回数については引き続き検討する
- 臨時委員会：不測の事態が生じた時に適宜開催する。
- 委員の構成：資源提供機関の教員若干名および職員
- 委員長：互選により決める
- 事務局：専任技術補佐員を 2 名程置き，HPCI 基盤運用に当たるとともに事務局も兼ねる。不測事態が生じた時は，不測事態が生じた機関が事務局をつとめる。詳細は引き続き検討する

4.5.2 ミッション

- 運用状況の把握
- 下記の議論に基づき規則を作成する
    - アカウント管理に関する議論
    - システム変更に関する議論
    - セキュリティに関する議論
    - HPCI ストレージ運用に関する議論

4.6 今後の検討課題

事務局，資源提供基本仕様に関する，今後の検討課題は以下の通り。

- HPCI 事務局の計算機環境におけるネットワーク構成は，事務局の開設場所が決定した後に，改めて検討する。
- 資源提供機関における計算機環境および体制に関する要件を検討する。
- 各資源提供機関よりHPCIに提供される資源の利用規則は，各資源提供機関の利用規則を参考に検討する。

5 ドキュメント＆システム開発整備（発注仕様）

以下に整備するドキュメントにおいての共通仕様を記載する。

1. ソフトウェアのバージョンアップ等によりマニュアルの改版があった場合にも，遅延なくそれぞれのマニュアルの改版を行い提供すること。また，改版内容につて報告し，承認を受けること。
2. 機能毎のマニュアルには機能を分かりやすく説明した機能概要の章を設けること。
3. 各マニュアルには目次および牽引をつけること。
4. 各マニュアルに用いる用語は統一されていなければならない。資源提供機関毎に用いる用語・概念に差異がある場合など，必要に応じて用語集を付録としてつけること。
5. マニュアルに記載されたそれぞれの処理を実行したときに発生しうるエラーについて漏れなく記載すること。エラー発生時の対処についても記載すること。
6. 利用シナリオに従い，それぞれの処理に対して使用例を示すこと。
7. 図表等を活用し，色使いにも配慮して視覚的に分かりやすい記述にすること。
8. 各マニュアルは極力外部参照を避け，当該マニュアル内で完結する記述とすること。
9. それぞれのマニュアルの構成，書式および記述レベルは統一されていること。
10. 各マニュアルは HTML 形式および PDF 形式で提供すること。

5.1 ユーザ利用手引き発注仕様

HPCI 基本仕様書の内容を踏まえ，以下の項目を含んだユーザ向け利用手引き書を作成すること。

5.1.1 クイックスタートガイド

利用者が短時間で HPCI 全体の構成と機能およびそれらを操作する方法を把握するために必要なドキュメントとしてクイックスタートガイドを作成する。

- 以下の内容を含むクイックスタートガイドを作成すること。
  - HPCI 環境の目的
  - HPCI 環境を利用するために理解しておかなければならない概念
  - HPCI 環境に含まれる以下の各機関とそれぞれの役割
    - HPCI 事務局
    - 資源提供機関
    - HPCI アカウント IdP 運用機関
    - 認証局運用機関
    - 認証ポータル運用機関
  - HPCI 環境の代表的な利用シナリオと実行例
  - HPCI 環境を利用するまでに必要な手続き

- その他の詳細な記載内容については発注者と協議の上，決定すること

5.1.2 各種ユーザーズマニュアル

以下の機能別ユーザマニュアルを作成する。

5.1.2.1 HPCI ポータルユーザマニュアル

- HPCI ポータルユーザマニュアルは以下の内容を記載すること。
    - HPCI ポータルの機能概要
    - 非 HPCI アカウントによる HPCI ポータルの初回認証について
    - HPCI ID の登録・変更・廃止申請について
    - HPCI ID および HPCI-ID 照合コードの照会と照合コードの再生成について
    - HPCI 利用課題の新規・変更・継続申請について
    - HPCI アカウントの管理について
- その他の詳細な記載内容については発注者と協議の上，決定すること

5.1.2.2 ヘルプデスクユーザマニュアル

- ヘルプデスクユーザマニュアルは以下の内容を記載すること。5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物の内容を反映すること。
    - ヘルプデスクで行う業務の概要について
    - 案件の登録について
    - 案件の状況確認について
    - 登録した案件に対する問い合わせ対応について
- その他の詳細な記載内容については発注者と協議の上，決定すること

5.1.2.3 情報共有 CMS ユーザマニュアル

- 情報共有 CMS ユーザマニュアルには以下の内容を記載すること。5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物の内容を反映すること。
    - 情報共有 CMS で行う業務の概要について
        - 運用管理者向け
        - 研究者向け
        - 開発者向け
        - 利用者向け
    - 情報共有 CMS への情報登録について
    - 情報共有 CMS へ登録した情報の変更について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.1.2.4　資源提供機関ごとのユーザマニュアル

- すべての資源提供機関についてユーザマニュアルを作成すること。
- 資源提供機関ごとのユーザマニュアルは以下の内容を記載すること。
    - システム構成の概要について
    - 利用できるハードウェア・ソフトウェア資源について
    - ユーザ利用環境について
    - GSI-SSH による GSI ログインについて
    - ローカルアカウントによる直接ログインについて
    - 利用課題とグループ管理について
    - プログラム開発環境について
    - ジョブ実行について
    - HPCI 共有ストレージの使い方について
    - 資源提供機関特有の環境（可視化ツールなど）の使い方
- ユーザマニュアルは各資源提供機関から提供された情報にもとづいて記載すること
- その他の詳細な記載内容については発注者と協議の上，決定すること

5.1.2.5　緊急時対応ユーザマニュアル

- 緊急時対応ユーザマニュアルは以下の内容を記載すること。
    - パスワード・パスフレーズを亡失した場合の手続きについて
        - HPCI アカウントのパスワードの場合
        - 資源提供機関ごとのローカルアカウントのパスワードの場合
        - 証明書のパスフレーズの場合
    - パスワード・パスフレーズの漏洩が疑われる場合の手続きについて
        - HPCI アカウントのパスワードの場合
        - 資源提供機関ごとのローカルアカウントのパスワードの場合
        - 証明書のパスフレーズの場合
    - システムの脆弱性やセキュリティ・インシデントの報告について
        - 報告手順について
        - 報告すべき内容について
        - 報告に必要な記録の作成について
        - 報告先について
- その他の詳細な記載内容については発注者と協議の上，決定すること

5.2 事務局，資源提供運用手引き発注仕様

HPCI 基本仕様書の内容を踏まえ，以下の項目を含んだ運用手引き書を作成する。

5.2.1 HPCI 事務局向け

5.2.1.1 HPCI ポータルシステム管理マニュアル

- HPCI ポータルシステム管理マニュアルには以下の内容を記載すること。
    - HPCI ポータルシステムで行う業務の概要について
    - HPCI ポータルシステムのシステム構成について
    - HPCI ポータルシステムの導入方法について
    - HPCI-ID 管理簿について
    - HPCI 利用課題管理簿について
    - HPCI 提供資源管理簿について
    - システムバックアップや障害発生時の復旧手順について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.1.2 ヘルプデスクシステム管理マニュアル

- ヘルプデスクシステム管理マニュアルには以下の内容を記載すること。5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物の内容を反映すること。
    - ヘルプデスクシステムで行う業務の概要について
    - ヘルプデスクシステムのシステム構成について
    - ヘルプデスクシステムの導入方法について
    - システムバックアップや障害発生時の復旧手順について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.1.3 情報共有 CMS 管理マニュアル

- 情報共有 CMS 管理マニュアルには以下の内容を記載すること。5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物の内容を反映すること。
    - 情報共有 CMS で行う業務の概要について
    - 情報共有 CMS のシステム構成について
    - 情報共有 CMS の導入方法について
    - システムバックアップや障害発生時の復旧手順について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.1.4 ヘルプデスク対応フローマニュアル

- ヘルプデスク対応フローマニュアルには以下の内容を記載すること。各対応フローの詳

細については5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物を反映すること。

- 障害対応について
- バグ報告対応について
- セキュリティ報告対応について
- FAQ について
- その他の問い合わせ対応について

- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.1.5 セキュリティ・インシデント対応マニュアル

- セキュリティ・インシデント対応マニュアルには以下の内容を記載すること。
  - セキュリティ・インシデントの発見について
    - チェックするログファイルについて
    - インシデントの検出方法について
  - セキュリティ・インシデントが発生したときの報告について
    - 報告すべき内容について
    - 連絡体制について
    - 連絡手順について
  - セキュリティ・インシデントが発生したときの対応手順について
    - 記録の作成について
    - 復旧作業について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.1.6 HPCI ポータルシステムユーザマニュアル（管理者向け）

- HPCI ポータルユーザマニュアル(管理者向け)は以下の内容を記載すること。
  - HPCI ポータルの機能概要
  - 非 HPCI アカウントによる HPCI ポータルの初回認証について
  - HPCI ID の登録・変更・廃止申請について
  - HPCI ID および HPCI-ID 照合コードの照会と照合コードの再生成について
  - HPCI 利用課題の新規・変更・継続申請について
  - HPCI アカウントの管理について
  - HPCI 提供資源の管理について
- その他の詳細な記載内容については発注者と協議の上，決定すること

5.2.1.7　ヘルプデスクユーザマニュアル（管理者向け）

- ヘルプデスクユーザマニュアル(管理者向け)は以下の内容を記載すること。5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物の内容を反映すること。
    - ヘルプデスクで行う業務の概要について
    - 案件の登録について
    - 案件に対する問い合わせ対応について
    - チケットの発行について
    - チケットの担当割り当てについて
    - チケットの処理と処理内容の記録について
    - チケットのステータス変更について
    - チケットのクローズについて
- その他の詳細な記載内容については発注者と協議の上，決定すること

5.2.1.8　情報共有 CMS ユーザマニュアル（管理者向け）

- 情報共有 CMS ユーザマニュアルには以下の内容を記載すること。5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物の内容を反映すること。
    - 情報共有 CMS で行う業務の概要について
        - 運用管理者向け
        - 研究者向け
        - 開発者向け
        - 利用者向け
    - 情報共有 CMS への情報登録について
    - 情報共有 CMS へ登録した情報の変更について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.2　資源提供機関向け

5.2.2.1　ヘルプデスクユーザマニュアル

- ヘルプデスクユーザマニュアルは以下の内容を記載すること。5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様に基づき発注された成果物の内容を反映すること。
    - ヘルプデスクで行う業務の概要について
    - 案件の登録について
    - 案件の状況確認について
    - 登録した案件に対する問い合わせ対応について
- その他の詳細な記載内容については発注者と協議の上，決定すること

5.2.2.2　障害対応マニュアル

- 障害対応マニュアルには以下の内容を記載すること。
    - 障害発生の報告について
    - 提供資源に対する障害調査依頼への対応について
    - 計画停止スケジュールの報告について
    - 復旧後の報告について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.2.3　セキュリティ・インシデント対応マニュアル

- セキュリティ・インシデント対応マニュアルには以下の内容を記載すること。
    - セキュリティ・インシデントの発見について
        - チェックするログファイルについて
        - インシデントの検出方法について
    - セキュリティ・インシデントが発生したときの報告について
        - 報告すべき内容について
        - 連絡体制について
        - 連絡手順について
    - セキュリティ・インシデントが発生したときの対応手順について
        - 記録の作成について
        - 復旧作業について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.3　認証局運用機関向け

5.2.3.1　障害対応マニュアル

- 障害対応マニュアルには以下の内容を記載すること。
    - 障害発生の報告について
    - 提供資源に対する障害調査依頼への対応について
    - 計画停止スケジュールの報告について
    - 復旧後の報告について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.4　認証ポータル運用機関向け

5.2.4.1　　障害対応マニュアル

- 障害対応マニュアルには以下の内容を記載すること。
    - 障害発生の報告について
    - 提供資源に対する障害調査依頼への対応について
    - 計画停止スケジュールの報告について
    - 復旧後の報告について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.2.5　HPCI アカウント IdP 運用機関向け

5.2.5.1　　障害対応マニュアル

- 障害対応マニュアルには以下の内容を記載すること。
    - 障害発生の報告について
    - 提供資源に対する障害調査依頼への対応について
    - 計画停止スケジュールの報告について
    - 復旧後の報告について
- その他の詳細な記載内容については発注者と協議の上，決定すること。

5.3 事務局，資源提供機関規則集発注仕様

HPCI 基本仕様書に基づいて，HPCI 事務局準備室（仮称）？による関係機関との協議・調整および事務局と資源提供機関に関する規則を明文化する作業を支援し，ドキュメントとしてまとめること。その他の詳細な記載内容については発注者と協議の上，決定すること。

5.3.1.1 HPCI-ID 運用規約
5.3.1.2 HPCI 利用課題番号およびグループについて
5.3.1.3 資源提供機関ごとの HPCI 向けアカウンティング情報について
5.3.1.4 HPCI 向けネットワーク・セキュリティ監査基準
5.3.1.5 障害発生時の対応について
5.3.1.6 セキュリティ・インシデント・レスポンスについて

5.4 ヘルプデスクおよび情報共有 CMS 詳細設計発注仕様

- HPCI 基本仕様の 3.1.8 ヘルプデスク基本仕様および 3.1.9 情報共有 CMS 基本仕様に基づき，ヘルプデスクの運用に関する詳細設計を行なうこと。
- ヘルプデスクの業務フローを詳細化し，それぞれの業務フローにおける HPCI 事務局，資源提供機関などが果たすべき役割を明確にすること。
- ヘルプデスクの運用に必要なハードウェア・ソフトウェアの仕様を明確にすること。
- 不明な点がある場合は発注者と協議の上，決定すること。

5.5 ユーザ管理支援ツール発注仕様

5.5.1　アカウンティング集計ソフトウェア詳細設計発注仕様

- HPCI 基本仕様の 3.1.12.2 アカウンティング集計ソフトウェアに基づき，アカウンティング集計ソフトウェアの詳細設計を行なうこと。

6 整備計画

本節では、ユーザ管理支援における整備計画について記載する。

1　平成 23 年度

1.1　HPCI 事務局ソフトウェアの設計と開発

1.1.1　HPCI-ID 発行・管理システム

1.1.2　HPCI 課題申請・管理システム

1.1.3　資源提供機関との情報連携

1.2　ヘルプデスクの詳細設計と構築

1.3　ドキュメント整備

1.3.1　ユーザマニュアル

1.3.2　HPCI 事務局・資源提供機関運用手引き

1.3.3　HPCI 事務局・資源提供機関規則

1.4　HPCI 事務局計算機環境整備

2　平成 24 年度

2.1　HPCI 事務局ソフトウェアの設計と開発 (継続)

2.1.1　HPCI-ID 発行・管理システム

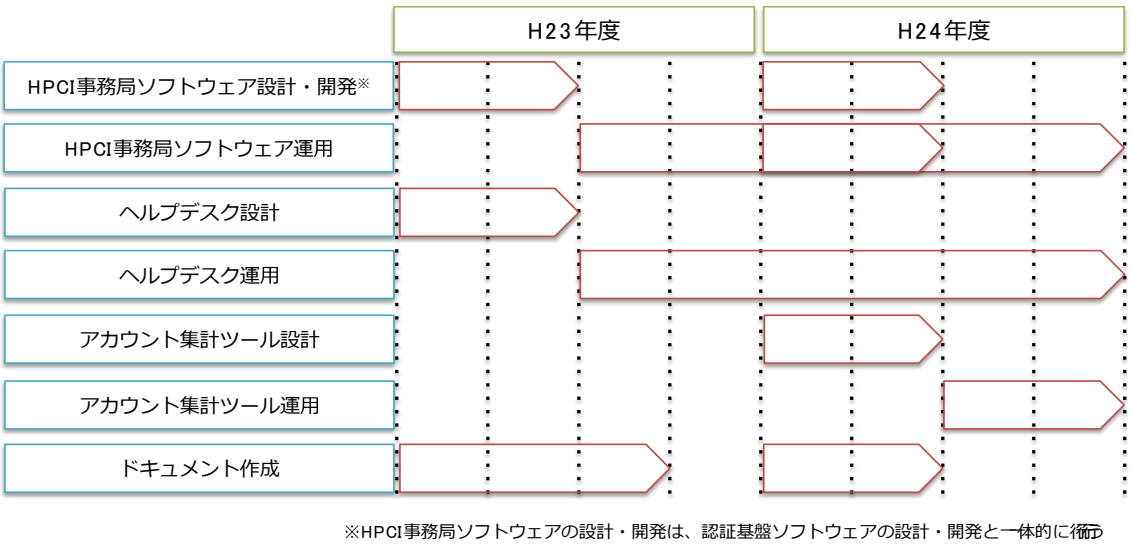
2.1.2　HPCI 課題申請・管理システム

2.1.3　資源提供機関との情報連携

2.2　ヘルプデスクの運用 (コンサル含む)

2.3　アカウンティング集計ツールの詳細設計と開発

HPCI 事務局の要員確保（非常勤事務補佐員と SE 常駐および派遣）



7 必要経費

7.1 ユーザ管理支援

ユーザ管理支援に関する必要費用について表 7.1 および表 7.1 に示す。

表 7.1 必要経費一覧 (H23 年度)

項目	費用見積 [千円]	備考
ドキュメント整備	13,835	
(内訳)		
ユーザマニュアル	6,289	5 人月
事務局・資源提供機関運用手引き	3,773	3 人月
事務局・資源提供機関規則	3,773	3 人月
詳細仕様検討	2,767	
(内訳)		
ヘルプデスク詳細設計	2,767	基本設計+運用設計 (既存 AP を想定)
設備	1,568	
(内訳)		
HPCI 事務局計算機環境	1,568	HPCI-ID 発行・管理システム、HPCI 課題申請・管理システム、ヘルプデスクシステム、アカウント集計ツールのサーバ構築 (H/W、S/W 費用別)
合計	**18,170**	

※HPCI 事務局ソフトウェアの設計・開発は、認証基盤ソフトウェアの設計・開発と一体的に行うため、認証基盤編にて計上

表 7.2 必要経費一覧 (H24 年度)

項目	費用見積 [千円]	備考
ドキュメント整備	5,000	
(内訳)		
ドキュメント整備	5,000	H23 年度分の改訂および追加
詳細仕様検討	4,300	
(内訳)		
アカウンティング集計ツール詳細設計	4,300	
開発	14,289	
(内訳)		
アカウンティング集計ツール開発	14,289	10 人月
導入，運用・保守	46,139	
(内訳)		
HPCI 事務局事務補佐員	4,639	2 人×12 ヶ月 非常勤事務補佐員雇用保険込み，交通費なし
ヘルプデスク運用 (コンサル含む)	34,000	2 人×12 ヶ月
HPCI 事務局計算機環境	7,500	HPCI-ID 発行・管理システム、HPCI 課題申請・管理システム、ヘルプデスクシステム、アカウント集計ツールのサーバ構築 (H/W 冗長化と保守)
合計	**69,728**	

1 利用 TCP ポート，UDP ポート

HPCI ポータルに関する利用ポートは HPCI 事務局のネットワーク構成も含め，平成 23 年に検討を行う。

2 調査結果

2.1 現状情報基盤センター群アカウント情報

別紙1を参照

2.2 E-Rad との連携

別紙2を参照

3 用語集

[1] HPCI 事務局

HPCI 利用の課題審査を行う組織

[2] HPCI アカウント IdP 運用機関

HPCI 環境に（シングル）サインオンするためのアカウントを発行・管理する組織（例：情報基盤センター，国研，商用プロバイダ）

[3] 資源提供機関

HPCI のユーザに対して計算機やストレージ等の資源を提供する組織（例：情報基盤センター，国研）

[4] 認証ポータル運用機関

HPCI 環境に（シングル）サインオンするための認証ポータルを運用する組織（例：情報基盤センター，国研）

[5] 認証局運用機関

HPCI 環境上で利用される電子証明書を発行する組織

[6] HPCI-ID

HPCI 利用者に配布されるユニークな ID 番号。HPCI 上の資源を利用するためのアカウントではない。HPCI を利用するユーザ毎に発行されるユニークな ID。所属組織が変わっても HPCI-ID は変わらない。

[7] HPCI アカウント

HPCI 環境に（シングル）サインオンするためのアカウント（OpenID や Shibboleth など）

[8] ローカルアカウント

資源提供機関の資源を利用するためのローカルアカウント（UNIX アカウント）

[9] クライアント証明書

ユーザ毎に認証局から発行される証明書（GSI 認証を行う場合に必要）NAREGI-CA

[10]HPCI ストレージ

HPCI で整備する共有ストレージ（分散ファイルシステム）を指す

[11]ログインノード

各拠点スパコンにユーザがログインするノード（会話処理部）を指す。