Vol.2011-HPC-130 No.69
2011/7/29

広域分散環境を提供するHPCIネットワーク・認証・ユーザ管理支援基盤の設計

合田憲人[†1] 東田学[†2] 漆谷重雄[†1]
天野浩文[†3] 坂根栄作[†1] 小林克志[†4]
青木道宏[†1] 柴山悦哉[†5] 石川裕[†5]

本稿では，HPCI 基本仕様として検討されているネットワーク基盤，認証基盤およびユーザ管理支援について報告する．ネットワーク基盤については，HPCI を構成する広域ネットワークに必要とされる機能や所要帯域に関する仕様の検討結果を報告する．認証基盤については計算機やストレージを利用するための認証・認可のための機能とソフトウェア仕様，またユーザ管理支援については，アカウンティング，障害対応，ヘルプデスクなどの機能や事務手続きフローについての検討結果を報告する．

Network, Authentication and User Support Infrastructure in HPCI Wide-Area Distributed Environment

Kento Aida,[†1] Manabu Higashida,[†2]
Shigeo Urushidani,[†1] Hirofumi Amano,[†3]
Eisaku Sakane,[†1] Katsushi Kobayashi,[†4]
Michihiro Aoki,[†1] Etsuya Shibayama[†5]
and Yutaka Ishikawa[†5]

This paper presents specifications of the high-performance computing infrastructure (HPCI) focusing on the network infrastructure, the authentication infrastructure and the user support. The specification of the network infrastructure defines services and bandwidth required in WAN organizing HPCI. The specification of the authentication infrastructure defines mechanisms and software architecture, which enable authentication and authorization for accessing computing/storage resources; and that of the user support defines accounting, trouble shooting and help desk services and their procedures.

1. はじめに

高性能計算技術やネットワーク技術の発展により，ネットワーク上に分散した大規模データの高速転送や共有，またこれらのデータを利用した高性能計算が可能となり，様々な研究分野で利用されている．これに伴い，従来は別々の研究分野で扱われていた実験データや大量のセンシングデータなどを融合して処理することにより，新たな科学的発見や融合研究領域を作り出すための研究手法として，e-サイエンス[1)]が注目されている．e-サイエンスを実現するためには，従来のように個々の高性能計算機やストレージを利用者が独立に利用するのではなく，これらの資源を共有できる高性能計算基盤を構築することが必要となる．

このような背景のもと，開発中の次世代スーパーコンピュータ（京コンピュータ）[2)]と国内のスーパーコンピュータや大規模ストレージを連携して利用するための革新的ハイパフォーマンス・コンピューティング・インフラ (HPCI)[3)]の構築が計画されており，HPCI の機能や基礎的な仕様をまとめた HPCI 基本仕様の策定が行われている．HPCI 基本仕様では，HPCI の機能をネットワーク基盤，認証基盤，ユーザ管理支援，共有ストレージ，先端ソフトウェア運用基盤に分け，それぞれについて利用シナリオやソフトウェアアーキテクチャ，およびシステム整備計画が検討されている．

本稿では，HPCI 基本仕様として検討されているネットワーク基盤，認証基盤およびユーザ管理支援について報告する．HPCI 基本仕様の検討では，それぞれの機能について利用シナリオの検討を行い，検討したシナリオを実現するためのネットワークやソフトウェアの仕様，運用管理方法などについての仕様を作成した．このうちネットワーク基盤については，主に広域ネットワークに必要とされる機能や所要帯域，認証基盤については計算機やストレージを利用するための認証・認可のための機能やソフトウェア仕様，ユーザ管理支援につ

†1 国立情報学研究所
National Institute of Informatics
†2 大阪大学
Osaka University
†3 九州大学
Kyushu University
†4 理化学研究所
RIKEN
†5 東京大学
The University of Tokyo

いては，アカウンティング，障害対応，ヘルプデスクなどの機能や事務手続きフローについて検討を行った．

以後，2 節では，ネットワーク基盤，認証基盤およびユーザ管理支援を中心とした HPCI の概要について述べる．次に 3 節では，HPCI のネットワーク基盤に関する仕様について述べ，4 節および 5 節では，認証基盤とユーザ管理支援に関する仕様についてそれぞれ述べる．最後に 6 節では，本稿の議論をまとめ，今後の整備計画について述べる．

2. ネットワーク・認証・ユーザ管理支援基盤の概要

「革新的ハイパフォーマンス・コンピューティング・インフラ (HPCI) とこの構築を主導するコンソーシアムのグランドデザイン（平成 22 年 5 月 26 日文部科学省）」に基づき，同年 7 月に計算資源提供機関 25 機関とユーザコミュニティ機関 13 機関の計 38 機関からなる HPCI 準備段階コンソーシアムが発足した．HPCI では，次世代スパコン「京コンピュータ」と全国に存在するスーパーコンピュータセンターを高速ネットワークでつなげるとともに大規模ストレージシステムを導入し，透過的資源アクセスを提供することによりユーザの利便性を高めることを目的としている．現在このコンソーシアムが主導して，平成 24 年 11 月の運用開始を目途に HPCI の構築とコンソーシアムの形成に向けた検討と準備が進められている．これに平行して，東京大学が代表機関となり，情報・システム研究機構国立情報学研究所，北海道大学，東北大学，筑波大学，東京工業大学，名古屋大学，京都大学，大阪大学，九州大学，理化学研究所計算科学研究機構と共に HPCI のシステムソフトウェアに関する基本仕様の設計を行っている．

図 1 は，本 HPCI 基本仕様の中で，本稿が対象とする HPCI のネットワーク，認証，ユーザ管理支援基盤の概要を示している．ただし，本稿が対象とする基盤は，H22 年度に策定された HPCI 基本仕様の初期環境に基づいており，今後，環境を拡張することも検討されている．本基盤は，ネットワークに接続された計算資源をユーザが共有利用するためのサービスを提供する．ネットワーク基盤は汎用の広域ネットワークであり，国立情報学研究所が運用する SINET4[4] が利用される予定である．計算資源は，理化学研究所計算科学研究機構で開発中の京コンピュータ，および 9 大学（北海道大学，東北大学，筑波大学，東京大学，東京工業大学，名古屋大学，京都大学，大阪大学，九州大学）の情報基盤センターが運用するスーパーコンピュータが利用されるほか，これらの計算機群からアクセス可能な共有ストレージとして，理化学研究所計算科学研究機構および東京大学が運用する HPCI ストレージ[5] が提供される予定である．これらの計算資源を利用するための認証基盤では，計算機

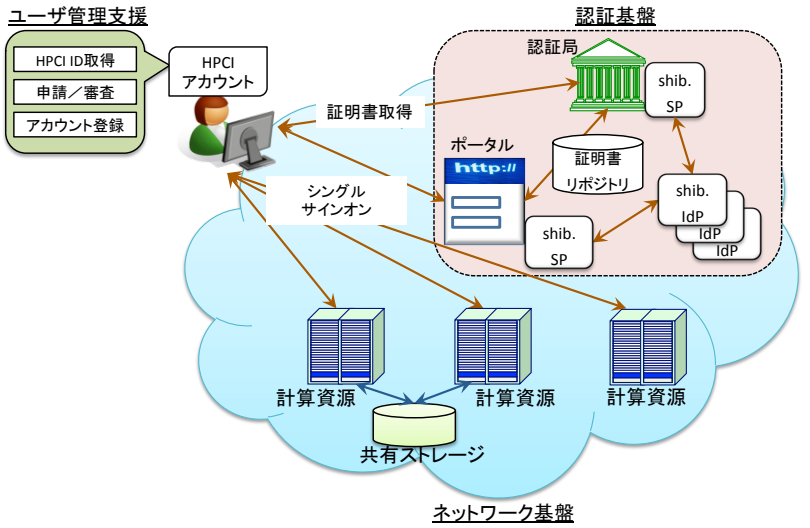

図 1 HPCI ネットワーク・認証・ユーザ管理支援基盤

や共有ストレージを利用するためのシングルサインオン認証を可能とする．共有ストレージの詳細については 5) を参照されたい．

HPCI 上の計算資源を利用するためには，HPCI を利用する研究課題に関する申請を行い，利用が認められる必要がある．課題申請は，研究を進めるグループ毎に行われ，採択された課題の参加者には HPCI を利用するためのアカウント（HPCI アカウント）が発行される．HPCI アカウントを取得したユーザは，本アカウントを用いて認証ポータル上でシングルサインオン処理を行うことにより，計算機群へのログインや計算機群からの共有ストレージ上のファイルへのアクセスが可能となる．

3. ネットワーク

本節では，HPCI におけるネットワーク基盤について述べる．ネットワーク基盤に関する検討では，HPCI のユーザおよび資源提供機関の観点でネットワーク利用シナリオを描き，課題の洗い出しとアーキテクチャの明確化を行った．

3.1 ネットワーク基盤の課題

ネットワーク基盤は，まず第一に，幅広いユーザの利用を考慮し，計算資源へのアクセス制限のない環境を整備する必要がある（**図 2** 参照）．HPCI の計算資源が SINET4 に収容されている場合，ユーザの計算資源へのアクセスとして，(1)SINET4 のみを用いてアクセス，(2) 商用ネットワーク等を経由して SINET4 に接続してアクセス，(3) 指定された拠点に出向いてアクセスという形態が考えられる．(1) は学術系ユーザの一般的なケースであり，機能および帯域として最も望ましいが，HPCI を企業にも活用してもらうよう，SINET4 の利用規定を整備することとした．(2) は商用ネットワークと SINET4 との相互接続環境が重要となるが，現時点で, 東京で合計 30Gbps の帯域で 134 の商用ネットワークと，大阪で合計 11Gbps の帯域で 22 の商用ネットワークと IX を介して相互接続されている．これらの接続について，現状 SINET 側で輻輳はみられないことから今後の利用動向をみながら増速を検討することとした．(3) は SINET4 としての課題はなく，拠点における協力により可能となる形態である．

次に，HPCI の本格展開においては，計算資源やストレージ資源の間で大容量のファイルの転送が行われるため，資源提供機関間で高速なネットワーク環境が必須となる．一方で，各資源提供機関は，各々異なるセキュリティポリシーを持ち，そのポリシーに基づき，ファイヤーウォールで計算資源等に対するアクセス管理を行っている．HPCI では，それぞれの組織のセキュリティポリシを尊重し，計算資源やストレージ間の通信を含めて，全ての通信は汎用ネットワークを使用することとした．ただし，HPCI 用の先端ソフトウェア機能[6]の性能検証等においては，汎用ネットワークとは分離した環境（VPN 環境等）が必要な場合があり，開発者側でネットワーク環境を自由に選択して利用できる環境を整備することとした．また，汎用ネットワーク内で高性能にデータ転送を行うための品質制御については，今後の利用形態等を鑑み判断を行うこととした．

3.2 ネットワーク基盤のアーキテクチャ

SINET4 ではレイヤ 1〜レイヤ 3 の各レイヤで，多様なサービス（インターネット接続サービス，L3VPN，L2VPN/VPLS，QoS，リソースオンデマンド等）を提供している．現時点では，サービス毎の通信プロトコルや高信頼化技術の違い等を考慮して，5 つのサービス論理網を形成してサービスを提供している．HPCI では，SINET4 のインターネット接続サービスを利用することとした．組織毎に異なるファイウォールポリシの問題に関しては，HPCI に必要なサービス（認証，ストレージ，CPU アクセス）を絞った上で，組織毎に調整することとした．ここで，IP パケットの優先制御が必要となる場合には，IP アドレスやポート番号等の識別により実施が可能である．また，先端ソフトウェア機能等の性能検証においては，開発者が必要に応じてプロジェクト毎に L3VPN や L2VPN/VPLS を設定することが想定されることから，SINET4 上でそのための別論理網を形成することを予定している．

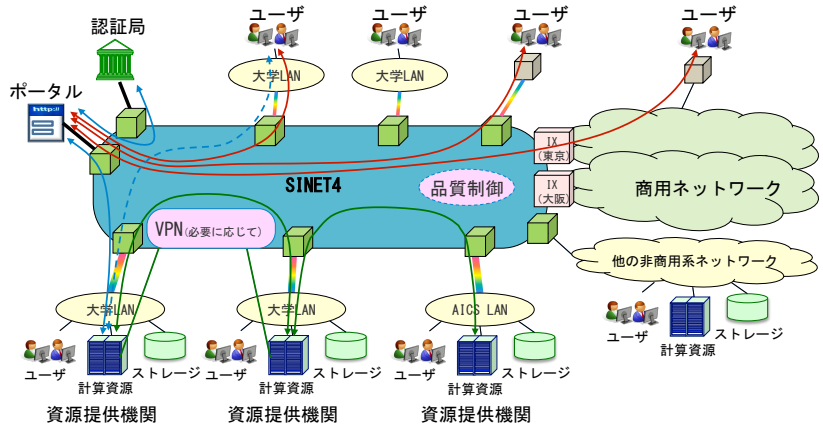

図 2 ネットワーク基盤のイメージ

また，必要なネットワーク帯域に関しては，HPCI 準備段階コンソーシアム加盟者に転送対象となるデータセット量を中心にヒアリング，それをもとに所要帯域を試算した．その結果，SINET4 のバックボーン整備が計画通りに平成 23 年度に東阪 80Gbps になれば，問題のない範囲であることが確認された．ただし，HPCI ストレージは現在設計途上でありこれに必要な帯域は本試算には含まれていない．このため，帯域需要については今後も十分に検討する必要がある．ヒアリング結果および所要帯域の試算の詳細については，A.1 を参照されたい．

4. 認　　証

本節では，HPCI における認証基盤について述べる．認証基盤に関する検討では，HPCI 上の計算機や共有ストレージへのシングルサインオンを実現する認証・認可サービスの利用シナリオを検討し，これを実現するための認証基盤アーキテクチャの設計を行った．

4.1 認証基盤の課題

認証基盤の目的は，HPCI 上の計算機や共有ストレージへのシングルサインオンを実現する認証・認可サービスを提供することである．**図 3** は，本認証基盤の利用シナリオを示している．本シナリオでは，ユーザが認証ポータルに HPCI アカウントを用いてサインオンし，シングルサインオン処理を行う．認証ポータルは耐故障性を向上させるために複数の組織で運用されるが，ユーザはどの認証ポータルからもサインオンすることができる．その後ユーザは，アカウントやパスワード等の入力を行うことなく，複数の計算機へのログインや共有ストレージ上のファイルへのアクセスを実行することができる．

HPCI の資源提供機関やユーザコミュニティは多岐にわたり，これらのユーザが習得している認証方法も複数想定されるため，認証ポータルにサインオンするためのアカウント種別やユーザが利用するサービスにより，図 3 を実現するシナリオは複数考えられる．一方，H24 年度の京コンピュータの運用開始にあわせて HPCI の運用開始も計画されているため，早急に安定した認証基盤の運用を開始する必要がある．HPCI 基本仕様の検討では，アカウント種別として Shibboleth[7),8)] や OpenID[9)]，およびシングルサインオンを実現する方式として Grid Security Infrastructure (GSI)[10),11)] を用いる方式について検討を行うとともに，これらの認証方式の運用に関して国内外での動向調査を行った．これらの検討の結果，9 大学の情報基盤センターおよび国立情報学研究所による運用実験が行われた実績[12)] のある GSI および Shibboleth を用いた方式を採用した．

GSI は，Public Key Infrastructure (PKI)[13)] に基づく認証技術であり，ユーザの持つクライアント証明書を使って複数の資源に対するシングルサインオンが実現される．ユーザは，自らのクライアント証明書を使ってサインオンすることにより，クライアント証明書から作成される一時的な証明書（Proxy 証明書）を生成することができる．Proxy 証明書には，クライアント証明書（または一世代前の Proxy 証明書）により署名された秘密鍵と公開鍵のペアが含まれており，これを利用する遠隔計算機やストレージに送付することにより，PKI に基づく認証が行われる．Proxy 証明書には有効期間が定められており，その有効期間内であれば，ユーザは新たなサインオン処理を行うことなく，複数の資源へのログインやファイルアクセスが可能となる．

GSI では，各ユーザが認証局からクライアント証明書の発行を受ける必要がある．本認証基盤におけるクライアント証明書の取得方法は，The International Grid Trust Federation (IGTF) で定められた国際基準である MICS プロファイル[14)] に基づいて行われる．MICS プロファイルでは，ユーザの本人性確認を他の信頼できるアカウント管理システム上のデータを用いて行う．即ち，ユーザが信頼できる組織のアカウントを所有していることをもって，ユーザの本人性確認を行う．従ってユーザは，後述の HPCI アカウントを管理する組織から発行された HPCI アカウントを用いてポータルにサインオンすることにより，クライアント証明書をオンライン処理のみで取得することができる．

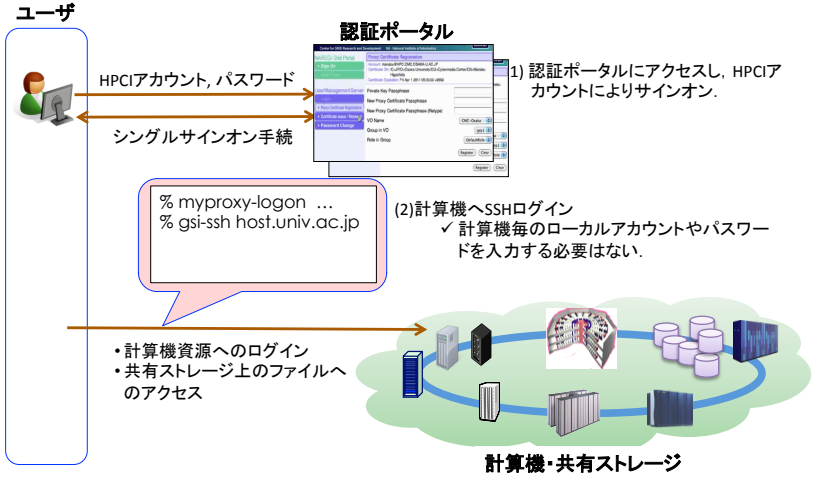

図 3 認証基盤の利用シナリオ

HPCI の認証基盤を実現する上で，HPCI アカウントの発行および管理方法は重要な課題である．資源提供機関の計算機や共有ストレージを利用するためには，各々の資源のローカルアカウントが必要となるため，これらローカルアカウントのアカウント管理システムの他に，さらに HPCI アカウント用のアカウント管理システムを運用することは効率が悪い．そのため，本認証基盤では，HPCI に参加する組織が運用する既存のアカウント管理システム上に HPCI アカウントを登録するとともに，これらのアカウント管理システムは分散して存在するため，Shibboleth 認証連携技術を用いて分散したアカウント管理システムを連携させる．従って，ユーザは，HPCI 上の一組織から発行された HPCI アカウントを用いて，シングルサインオンが可能である．

4.2 認証基盤のアーキテクチャ

本節では，認証基盤を構成するシステムとその運用組織について述べる．本認証基盤は，**表 1** に示す組織が運用するシステムから構成されている．**図 4** は，各機関が運用するシス

テムの関係を示す．

認証局運用機関は，GSI において必要となるクライアント証明書およびサーバ証明書を発行する組織である．図中の証明書管理システムは，ユーザからの証明書の発行・失効等の申請を受け付け，認証局システムに証明書の発行・失効依頼を行うソフトウェアである．認証局システムから発行されたクライアント証明書は，証明書リポジトリに保管される．認証局システムは，Shibboleth SP[8] として実装されており，証明書取得処理におけるユーザの認証を Shibboleth IdP に依頼する．また，Shibboleth DS[8] は，認証を受けるアカウントを管理する Shibboleth IdP[8] の情報を検索するための役割を持つ．現在，認証局システム用ソフトウェアとして NAREGI-CA[15]，証明書管理システム用ソフトウェアとして UMS[15]，証明書リポジトリとして MyProxy[16),17)] を利用する予定である．また，Shibboleth を用いた認証連携には，Internet2 で公開されているソフトウェアパッケージ[8] を用いる予定である．

認証ポータル運用機関は，HPCI にユーザがシングルサインオンするためのインタフェースとしての機能を提供する組織である．認証ポータルは，ユーザが HPCI にサインオンするための web ポータルである．ユーザは HPCI アカウントを用いてサインオンするため，認証ポータルは Shibboleth SP として実装されており，ユーザ認証を HPCI アカウントの Shibboleth IdP に依頼する．ポータル上でサインオンしたユーザは，GSI によるシングルサインオンを行うための Proxy 証明書を生成することができ，生成された Proxy 証明書は Proxy 証明書リポジトリに保存される．認証ポータル用ソフトウェアは，現在，HPCI 向けに開発を行っている．また，Proxy 証明書リポジトリとして MyProxy を用いる予定である．

HPCI アカウント IdP 運用機関は，HPCI アカウントの認証機能を提供する組織である．本機関では，自らが運用するアカウント管理システム（アカウント DB）に接続する Shibboleth IdP を運用し，Shibboleth SP から要求された HPCI アカウントの認証を行い，認証結果を Shibboleth SP に返す．資源提供機関は，HPCI に対して計算機や共有ストレージを提供する組織である．これらの資源を利用するためのミドルウェアについては，現在，計算機に遠隔ログインするために GSI-SSH[18]，共有ストレージ上のファイルアクセスのために Gfarm2[19] を用いる予定である．HPCI アカウント IdP 運用機関と資源提供機関については同一組織が両方の機能を持つことが想定されるが，本稿では，認証基盤の機能を明確に分類するために両者を分けて定義している．

現在，本認証基盤の試行運用を開始するために，理化学研究所計算科学研究機構，9 大学情報基盤センター，国立情報学研究所が認証基盤の構築を進めている．9 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は資源提供機関および HPCI アカウント運用機関としての役割を持ち，国立情報学研究所が認証局運用機関を運用する予定である．また，認証ポータル運用機関は，国立情報学研究所と情報基盤センターの一部が運用することを予定している．

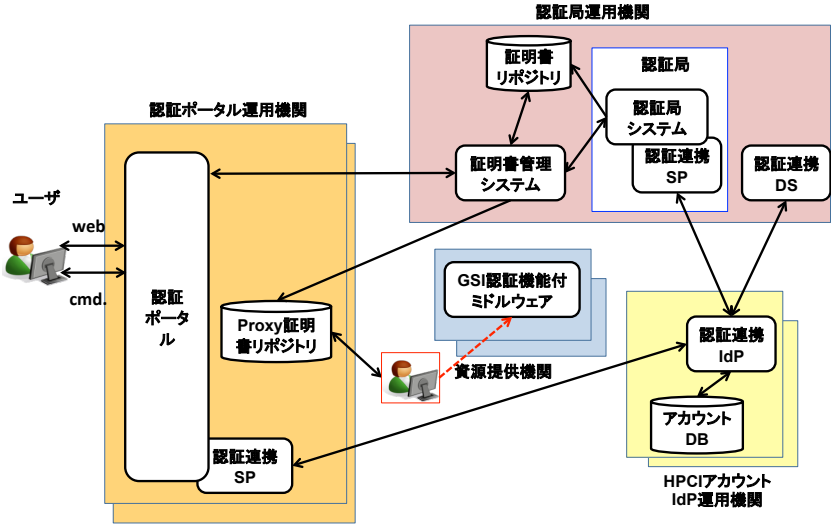

図 4 認証基盤のアーキテクチャ

表 1 認証基盤運用機関

運用機関	役割
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．
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．
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．
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．

5. ユーザ管理支援

本節では，HPCI におけるユーザ管理支援について述べる．ユーザ管理支援では，資源提供機関の従来のユーザ管理支援業務フローを考慮し，HPCI のユーザに対する管理および支

援方法の検討を行った．

5.1 ユーザ管理支援の課題

HPCI 環境は，2 節に述べられているような利用課題申請を行って利用を認められた課題のメンバーのみが利用することができる．一方，採択課題のメンバーであっても，HPCI に資源を提供している個々の機関でのローカルアカウントを交付されなければ，実際に HPCI 環境で提供される資源を利用できるようにはならない．しかし，各資源提供機関は HPCI に資源を供出するのとは別に従来の全国共同利用サービスの提供も継続するため，ローカルアカウント発行のために各資源提供機関が持っている作業手順は，HPCI 発足後も存続することになる．このため，課題が採択された後に個々のローカルアカウントが発行できるまでの作業手順は，各資源提供機関ごとの従来の業務フローをなるべく踏襲できることが望ましい．

また，HPCI 環境を利用して得られた成果は，HPCI ストレージを通じ，課題のメンバー (代表者が認める場合には研究コミュニティ全体) で共有することができる．同ストレージ上のデータは，課題終了後も一定期間保存され，前年度には採択されていなかったユーザが，それ以前に得た自分の成果を引き継ぐ形で新たな利用課題を申請することもできる．このユーザが新課題で採択された場合，休眠状態のまま保存されていたデータを再び元の所有者によって利用可能な状態に戻さなければならない．このようなことを可能にするために，HPCI 利用課題とも各サイトのローカルアカウントとも独立に，比較的長期間に渡り所属機関の壁を越えて個人を識別できることが必要になる．

さらに，サイトごとに異なる利用者認証手順を簡素化するために，4 節に述べたようなシングルサインオン環境が用意され，ユーザは，異なるサイトに分散する資源を透過的に利用できるようになる．その一方で，利用に関する質問への回答やシステム障害等の解決に実質的に関与しなければならない人員は，HPCI 環境の性質上，多数の機関に分散することとなる．しかし，ユーザが適切な回答者・管理者をピンポイントで予想して連絡をとることは非常に困難であると予想される．このため，ユーザの負担を軽減しながら，ユーザから寄せられた質問を適切な人員に的確に伝達するだけでなく，回答・対処の進捗状況を確実に追跡できるしくみも必要となる．

5.2 ユーザ管理支援の運用フロー

前節のような検討から，HPCI における利用課題申請から利用終了までのおおまかな流れは，**図 5** に示すような形にまとめられる．

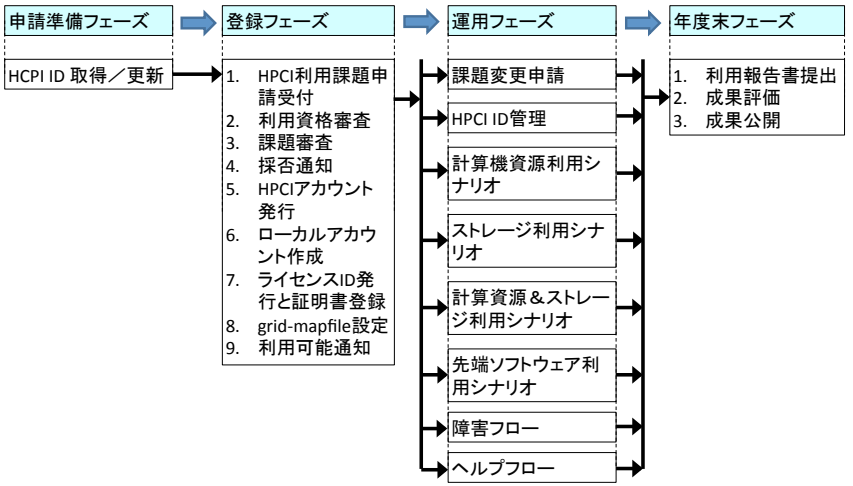

図 5 利用課題申請から利用終了までのおおまかな流れ

申請準備フェーズでは，HPCI 利用課題を申請しようとする者が，申請に先立ち，一意な **HPCI ID** を取得するものとする．

登録フェーズでは，利用申請から利用可能通知までのイベントが逐次的に進行する．ユーザから受け付けられた利用課題について，課題審査が行われる．採択された課題については，そのメンバーに対する HPCI アカウントが発行され，利用を承認された各資源提供機関は，従来の業務フローに基づいてローカルアカウントを用意する．この HPCI アカウントを用いてユーザが証明書の登録を行い，各資源提供機関でそのローカルアカウントに関連する必要な設定作業が終了すると，シングルサインオンによる HPCI の利用が可能となる．

運用フェーズでは，課題変更申請・HPCI ID 管理・計算資源利用等のシナリオが並行に進行する．

年度末フェーズでは，資源を提供された各利用課題の代表者が，利用期間終了後，所定の成果報告書を提出する．採択時の条件によっては，成果評価が行われることもある．

5.3 ユーザ管理支援を円滑に行うための体制

このような業務フローを円滑に運用するとともにユーザの負担を軽減するため，ユーザから見た，HPCI ID の交付・利用課題申請受付・採否通知・各資源の利用可能通知などの窓口は，**HPCI 事務局**に一本化される．また，ユーザが利用に関する質問や障害の通報を行

うための一次窓口も，事務局内に併設された**ヘルプデスク**に一本化される．

HPCI 事務局は，HPCI ID の一意性を管理し，利用資格を喪失した者に対する失効処理なども行わなければならない．(潜在的な) ユーザの数が多くなるとこの業務の負荷は非常に大きくなるおそれがある．このため，e-Rad のような一意性が保証されている他の個人識別番号を援用する方式や，web ポータルによるアップロードを併用することにより，ユーザから提出された申請書と HPCI ID 管理簿データとの照合作業を省力化する方式などを検討している．

また，障害対応やヘルプのフローにおいても，HPCI 事務局は重要な役割を果たす．利用者から寄せられた障害通知・質問に対して，一次対応を行い，必要に応じて二次対応先を切り分け，対応を依頼する．特に，システムレベルの緊急対応を必要とするような障害に対処するため，各資源提供機関のセキュリティ担当者による**インシデントレスポンスチーム**を形成し，この種の事案については，事務局は同チームに対応を依頼するものとする．

さらに，ユーザから寄せられた障害通知や質問を適切な人員に的確に伝達し，回答・対処の進捗状況を確実に追跡するためには，チケット管理システムを利用する方針である．

6. おわりに

本稿では，HPCI 基本仕様として検討されているネットワーク基盤，認証基盤およびユーザ管理支援について，それぞれに求められる課題と課題を解決するための仕様検討結果を報告した．ネットワーク基盤については，H23 年度より既に SINET4 が稼働しており，HPCI 構築に向けた京コンピュータの接続およびバックボーンネットワークの帯域増強について検討中である．また，認証基盤とユーザ管理支援については，理化学研究所計算科学研究機構，9 大学情報基盤センター，国立情報学研究所が参加し，本稿で述べた基本仕様に基づく運用環境の構築が進められており，H23 年度中に試行運用が開始される予定である．

謝辞 本稿をまとめるにあたり御議論頂きました「HPCI の基本仕様に関する調査検討」委員の皆様，ならびに，HPCI システム WG 委員の皆様に感謝致します．本研究の一部は，文部科学省委託「HPCI の基本仕様に関する調査検討」および「HPCI の詳細仕様に関する調査検討」による．

参考文献

1) Hey, T., Tansley, S. and Tolle, K.(eds.): *The Fourth paradigm, Data-Intensive Scientific Discovery*, Microsoft Research (2009).
2) 理化学研究所：次世代スーパーコンピュータの開発・整備，理化学研究所（オンライン），入手先⟨http://www.nsc.riken.jp/⟩（参照 2011-06-23）.
3) 理化学研究所：革新的ハイパフォーマンス・コンピューティグ・インフラ (HPCI)，理化学研究所（オンライン），入手先⟨http://hpcic.riken.jp/⟩（参照 2011-06-23）.
4) 国立情報学研究所：SINET4 学術情報ネットワーク，国立情報学研究所（オンライン），入手先⟨http://www.sinet.ad.jp/⟩（参照 2011-06-23）.
5) 實本英之，建部修見，　佐藤仁，　石川裕：広域分散環境を提供する HPCI システムソフトウェア基盤の設計概要と共有ストレージ構築，情報処理学会研究報告 HPC-130 (2011).
6) 滝澤真一朗，棟朝雅晴，宇野篤也，小林泰三，實本英之，松岡　聡，石川　裕：広域分散環境を提供する HPCI 先端ソフトウェア運用基盤の設計，情報処理学会研究報告 HPC-130 (2011).
7) Morgan, R.L., Cantor, S., Carmody, S., Hoehn, W. and Klingenstein, K.: Federated Security: The Shibboleth Approach, *EDUCAUSE Quarterly*, Vol.27, No.4 (2004).
8) Internet2: Shibboleth, Internet2 (online), available from ⟨http://shibboleth.internet2.edu/⟩ (accessed 2011-06-23).
9) OpenID Foundation: OpenID, OpenID Foundation (online), available from ⟨http://openid.net/⟩ (accessed 2011-06-23).
10) Welch, V., Siebenlist, F., Foster, I., Bresnahan, J., Czajkowski, K., Gawor, J., Kesselman, C., Meder, S., Pearlman, L. and Tuecke, S.: Security for Grid Services, *Proc. of the 12th IEEE International Symposium on High Performance Distributed Computing* (2003).
11) Welch, V.: Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective, *http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf* (2005).
12) 合田憲人：学術グリッド基盤の構築・運用技術に関する研究，学際大規模情報基盤共同利用・共同研究拠点第 3 回シンポジウム http://jhpcn-kyoten.itc.u-tokyo.ac.jp/sympo/ (2011).
13) 小松文子（編）：PKI ハンドブック，ソフトリサーチセンター (2004).
14) Murray, M.: Profile for Member Integrated X.509 Credential Services (MICS) with Secured Infrastructure Version 1.0, *The Americas Grid Policy Management Authority http://www.TAGPMA.org/* (2007).
15) NAREGI: National Research Grid Initiative, 国立情報学研究所 (online), available from ⟨http://www.naregi.org/⟩ (accessed 2011-06-23).
16) Novotny, J., Tuecke, S. and Welch, V.: Initial Experiences with an Online Certificate Repository for the Grid: Myproxy, *Proc. of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10)* (2001).

17) NCSA: MyProxy: Credential Management Service, the University of Illinois (online), available from ⟨http://grid.ncsa.illinois.edu/myproxy/⟩ (accessed 2011-06-23).
18) Globus Alliance: GSI-OpenSSH, Globus Alliance (online), available from ⟨http://globus.org/toolkit/docs/4.0/security/openssh/⟩ (accessed 2011-06-23).
19) Tatebe, O., Hiraga, K. and Soda, N.: Gfarm Grid File System, *New Generation Computing*, Vol.28, No.3, pp.257–275 (2010).

付　　録

A.1 HPCI ネットワークの所要帯域の分析

HPCI ネットワーク基盤において必要なネットワーク帯域に関して，HPCI 準備段階コンソーシアム加盟者に転送対象となるデータセット量を中心にヒアリングを行った．これに対して提示されたニーズ（特に転送データ量）を松/竹/梅（それぞれ 6 分/1 時間/10 時間）で実現するために必要な帯域を**図 6** に示す．この結果より，竹程度を想定するとバックボーンとしては特に問題のない範囲であると考えられる．

No	機関名	アンケートからの抜粋部分	換算帯域（Gbps）			
			対地	梅	竹	松
1	機関A	AICS～機関A：数TB 東京大学～機関A：数10GB	AICS～機関A（3TB） 東京大学～機関A（30GB）	0.67 0.067	6.7 0.67	67 6.7
2	機関B	AICS～機関B：1Gbps 研究所Y～機関B：10Gbps 研究所Z-機関B：10Gbps	AICS-機関B 研究所Y-機関B 研究所Z-機関B	1 - -	- 10 10	- - -
3	機関C	AICS～機関C：1Gbps 機関C(～東京DC)：10Gbps	AICS～機関C 機関C(-東京DC)	1 -	- 10	- -
4	機関D					
5	機関E	AICS～利用者ローカル環境：10TB/1日 AICS～拠点間：100GB	AICS～神戸DC AICS～神戸DC	2.2 0.022	- 0.22	- 2.2
6	機関F	機関F(～横浜DC)：10Gbps	機関F(～横浜DC)	-	10	-
7	機関G	AICS～機関G：20TB	AICS～機関G	4.4	44	440
8	機関H	AICS～機関H：10GB/s	AICS～機関H	-	8	80
9	機関I	機関I(～名古屋DC)：100Gbps	機関I(～名古屋DC)	-	10	100
10	機関J	機関J(～札幌DC)：2.4Gbps	機関J(～札幌DC)	-	2.4	24
11	機関K	AICS～機関H～機関D/機関K：10GB/s	AICS～機関H～機関D/機関K	-	8	80
12	機関L	AICS～機関L：128GB/日	AICS～機関L	0.028	0.28	2.8
13	機関M	AICS～機関M：50TB/4日以上	AICS～機関M（12.5TB/1日）	2.75	27.5	275
14	機関N	AICS～機関N：10GB AICS～機関N：1TB/1日	AICS～機関N AICS～機関N	0.002 0.22	0.022 2.2	0.22 22
15	機関O	AICS～機関O：10Gbps以上	AICS～機関O	-	10	-
16	機関P	AICS～機関P:10GB	AICS～機関P	0.002	0.022	0.22
17	機関Q	AICS-機関Q: 1TB/1時間	AICS-機関Q	0.22	2.2	22

図 6　HPCI ネットワーク基盤の所要帯域の分析

正誤表

4 ページ左段 22 行目（4.1 認証基盤の課題）

（誤）

Proxy 証明書には，クライアント証明書（または一世代前の Proxy 証明書）により署名された秘密鍵と公開鍵のペアが含まれており，これを利用する遠隔計算機やストレージに送付することにより，PKI に基づく認証が行われる．

（正）

Proxy 証明書は，新たに作成された秘密鍵と公開鍵を含み，ユーザの秘密鍵（または一世代前の Proxy 証明書に含まれる秘密鍵）により署名されている．認証時には，Proxy 証明書の秘密鍵を除いた部分が遠隔計算機やストレージに送付され，PKI に基づく認証処理が行われる．