

HPCI 基本仕様

— 先端ソフトウェア運用基盤基本仕様 —

目次

1. 概要	1
2. 利用シナリオ	2
2.1. 登録フェーズ.....	3
2.1.1. 先端ソフトウェア運用基盤利用申請.....	3
2.2. 運用フェーズ.....	4
2.2.1. 利用者シナリオ	4
2.2.2. ヘルプフロー	6
3. 基盤構築・運用基本仕様.....	8
3.1. 必要要件	8
3.2. 平成 23 年度テストベッド	9
3.3. 機能	10
3.3.1. 分散開発環境ホスティングの機能	10
3.4. 運用・保守	12
3.4.1. ホスティングサーバ導入・運用・保守	13
3.4.2. ホスティング管理サービス導入・運用・保守	15
3.4.3. VPN ゲートウェイサーバ導入・運用・保守	17
3.4.4. ヘルプデスク運用	18
3.4.5. HPCI 事務局	19
3.5. 追加仕様	19
3.5.1. 機能	19
3.5.2. 運用・保守	21
3.6. 検討項目	22
4. 資源提供基本仕様	23
4.1. ホスティングサーバ	23
4.1.1. ハードウェア構成	23
4.1.2. ソフトウェア構成	24
4.2. ホスティング管理サービス実行サーバ	25
4.2.1. ハードウェア構成	25
4.2.2. ソフトウェア構成	26
4.3. VPN ゲートウェイサーバ	27
4.3.1. ハードウェア構成	27
4.3.2. ソフトウェア構成	27
4.4. ネットワーク	28
4.5. 資源提供利用規則必須項目	28
5. ドキュメント&システム開発整備（発注仕様）	29

5.1.	ユーザ利用手引き発注仕様	29
5.1.1.	先端ソフトウェア運用基盤利用の手引き	29
5.2.	資源提供運用手引き発注仕様	29
5.2.1.	ホスティングサーバ運用の手引き	29
5.2.2.	ホスティング管理サービス実行サーバ運用の手引き	30
5.2.3.	VPN ゲートウェイサーバ運用の手引き	30
5.2.4.	ヘルプデスク運用の手引き	30
5.3.	利用細則発注仕様	31
5.4.	導入手順書発注仕様	31
5.4.1.	ホスティングサーバ導入手順書	31
5.4.2.	ホスティング管理サービス実行サーバ導入手順書	32
5.4.3.	VPN ゲートウェイサーバ導入手順書	32
5.5.	ヘルプデスク詳細設計発注仕様	33
5.6.	実証評価用ソフトウェア発注仕様	33
5.7.	追加仕様詳細調査検討のための役務発注仕様	34
5.8.	追加仕様開発発注仕様	37
6.	整備計画	38
6.1.	平成 23 年度実施項目	38
6.2.	平成 24 年度実施項目	38
6.3.	平成 24 年度後半 ～ 平成 25 年度実施項目	39
7.	必要経費	40
7.1.	ドキュメント整備費用	40
7.2.	実証評価用ソフトウェア開発費用	40
7.3.	追加仕様検討費用	40
7.4.	追加仕様開発費	40
7.5.	資源整備費用	40
7.6.	運用・保守費用	40
[付録]		42
1.	運用・保守シナリオ	42
1.1.	ホスティングサーバおよび仮想マシン登録フロー	42
1.2.	障害フロー	42
1.2.1.	ホスティング管理サービス実行サーバでの障害発生・保守フロー	42
1.2.2.	ホスティングサーバでの障害発生・保守フロー	43
1.2.3.	OS イメージの存在する共有ストレージでの障害発生時フロー	44
1.2.4.	仮想マシン動作環境での障害発生・保守フロー	45
1.2.5.	ホスティングサーバでのセキュリティインシデント発覚時フロー	46

2. 調査結果	47
2.1. 現状情報基盤センター群ネットワーク機能設定状況	47
2.2. 現状情報基盤センター群ホスティングサービス提供状況	48
3. 用語集	50

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。本策定にあたっては、「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。本基本仕様書は先端ソフトウェア運用基盤について基本仕様を定めている。

・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。仮想マシン(VM : Virtual Machine)技術を利用して実運用環境と隔離した開発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 HPCI 利用研究者が使えるようなソフトウェア・サービス・環境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。

本仕様書は、スーパーコンピュータ(以降、スパコンと表記)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

HPCI 利用形態は「表 1 HPCI 利用想定シナリオ」に示すように、スパコン利用のためのバッチキューへのジョブ投入だけにとどまらず、各種ポータルサービスのためのウェブサーバ運用(表の①)や、通常の運用環境では動作させられないコンピュータサイエンス(以降、CS と表記)系研究の開発環境(表の②)など、様々な利用シナリオが想定される。このような利用形態では、従来は個々の利用者が個別にサーバ・クラスタを用意し環境構築を行っていた。

先端ソフトウェア運用基盤は、通常のスパコン利用以外の利用目的を持つユーザに対し仮想マシン環境および各種サービスのホスティング環境を提供する。これにより、従来は個別に行っていた物理サーバの管理作業から利用者が解放されること、必要以上の権限を持たずに利用者がサービスを利用できる利点がある。一方で資源提供側にとっても、利用者にはサーバ・サービスに対しての管理者権限を与えつつもファームウェア更新等のハードウェア管理が行え、運用の安全性が確保できること、また Many Core かつ大容量メモリを搭載したサーバの普及に伴い、多数の利用者環境を少数のサーバに集約することが可能となる。

表 1 HPCI 利用想定シナリオ

HPCI 利用者区分	利用シナリオ	要求環境
応用 HPC 研究者	HPC リソースを用いた大規模計算（データ解析・シミュレーション等）を実行	HPCI 拠点リソース（スパコン）を利用
	特定 OS・ライブラリに依存するアプリケーションを実行	高信頼なサーバでのホスティングが求められる(①)
	HPC リソースにアクセスするためのポータルサービスを実行	
	成果公開・プロジェクトメンバー内情報共有のための WEB ポータル運用	
CS 系研究者	root 権限を必要とする OS 研究開発	管理者権限を持ったサーバからなる、必要に応じて分散配備可能な開発環境が求められる(②)
	開発したライブラリの、複数種 OS 上での検証	
	多拠点にグローバル IP を必要とする分散システムの開発	

先端ソフトウェア運用基盤は表の①、②で示す環境の提供を目標に、平成 23 年度は、表の②にあたる開発環境の実証実験とし、実証環境に資源供出可能な拠点間で環境を構築しサービスを試験的に提供する。以下、②の環境を利用者に提供することを「分散開発環境ホスティング」と呼ぶ。各地に配置したサーバ上で利用者が使用する環境を仮想マシン（VM）で提供するシステムである。利用者にはその VM に対する root アクセス権限が与えられる。平成 24 年度では、分散開発環境ホスティングの本格的運用、および、①で示す環境を分散開発環境ホスティング上で実現する。ただそのためにはシステムの堅牢性と、VM と HPC リソース間でネットワーク等の一部リソースを共通する必要があるが出てくる可能性があり、運用の堅牢性・セキュリティ等の検証、運用ポリシーの策定を平成 23 年度から平成 24 年度にかけて行う。

先端ソフトウェア運用基盤の分散開発環境ホスティング機能を用いることで、HPCI の追加機能の実証環境を構築することができる。例えば、HPCI で複数の拠点スーパーコンピュータに対して

ジョブ投入管理を行う Super Scheduler (Resource Broker)を導入する場合、あるいは、ストレージや認証の新しい機能を導入する場合に、事前テスト環境として使用することを検討している。

分散開発環境ホスティングは、分散リソース連携のためのサービスホスティング環境であり、仮想マシン (VM) 環境を利用してホスティングを実現する。各資源提供機関より分散開発環境ホスティング用に提供されたリソースをホスティングサーバ (VM が動作するサーバ) とし、それらを管理するホスティング管理サービスを先端ソフトウェア運用基盤運営局が運用する。ホスティング管理サービスは専用のサーバで動作する。

2.1. 登録フェーズ

2.1.1. 先端ソフトウェア運用基盤利用申請

HPCI 利用者が先端ソフトウェア運用基盤によって提供される環境を利用して開発を行う際には、課題申請時にその旨を申請する。

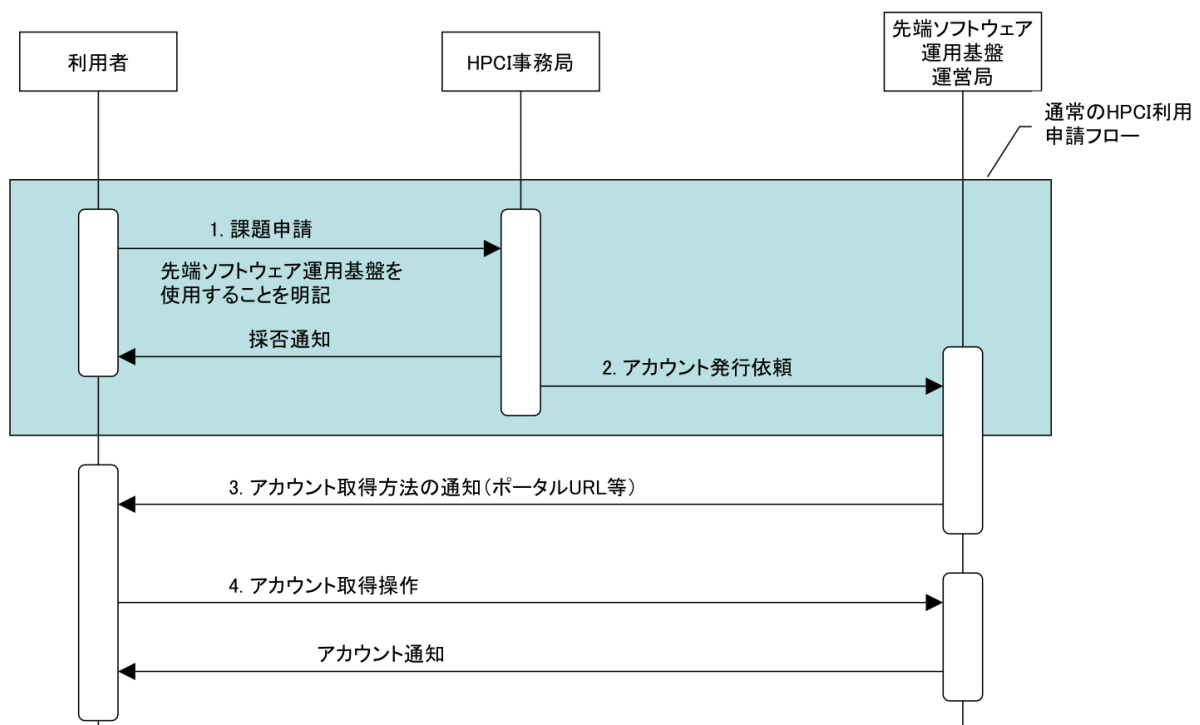


図 1 先端ソフトウェア運用基盤利用申請フロー

先端ソフトウェア運用基盤を利用する際の申請フローを「図 1 先端ソフトウェア運用基盤利用申請フロー」に示す。利用者は通常の HPCI 利用申請のフローに則り申請を行う (1. 課題申請)。申請を受けた HPCI 事務局も通常の申請にフローに則り、利用者に申請の採否を通知するとともに、先端ソフトウェア運用基盤運営局にアカウント発行を依頼する (2. アカウント発行依頼)。アカウント発行依頼を受けた先端ソフトウェア運用基盤運営局は、利用者に分散開発環境ホスティング機能利用のためのアカウント取得方法を通知する (3. アカウント取得方法の通知)。利用者は通知されたアカウント取得方法に従い、ポータルにてアカウント取得操作を行い (4. アカウント取得操作)、アカウントを得る。

2.2. 運用フェーズ

2.2.1. 利用者シナリオ

(1) VM 操作フロー

先端ソフトウェア運用基盤、分散開発環境ホスティング機能を使用する利用者のシナリオを「図 2 分散開発環境ホスティング機能利用フロー」に示す。

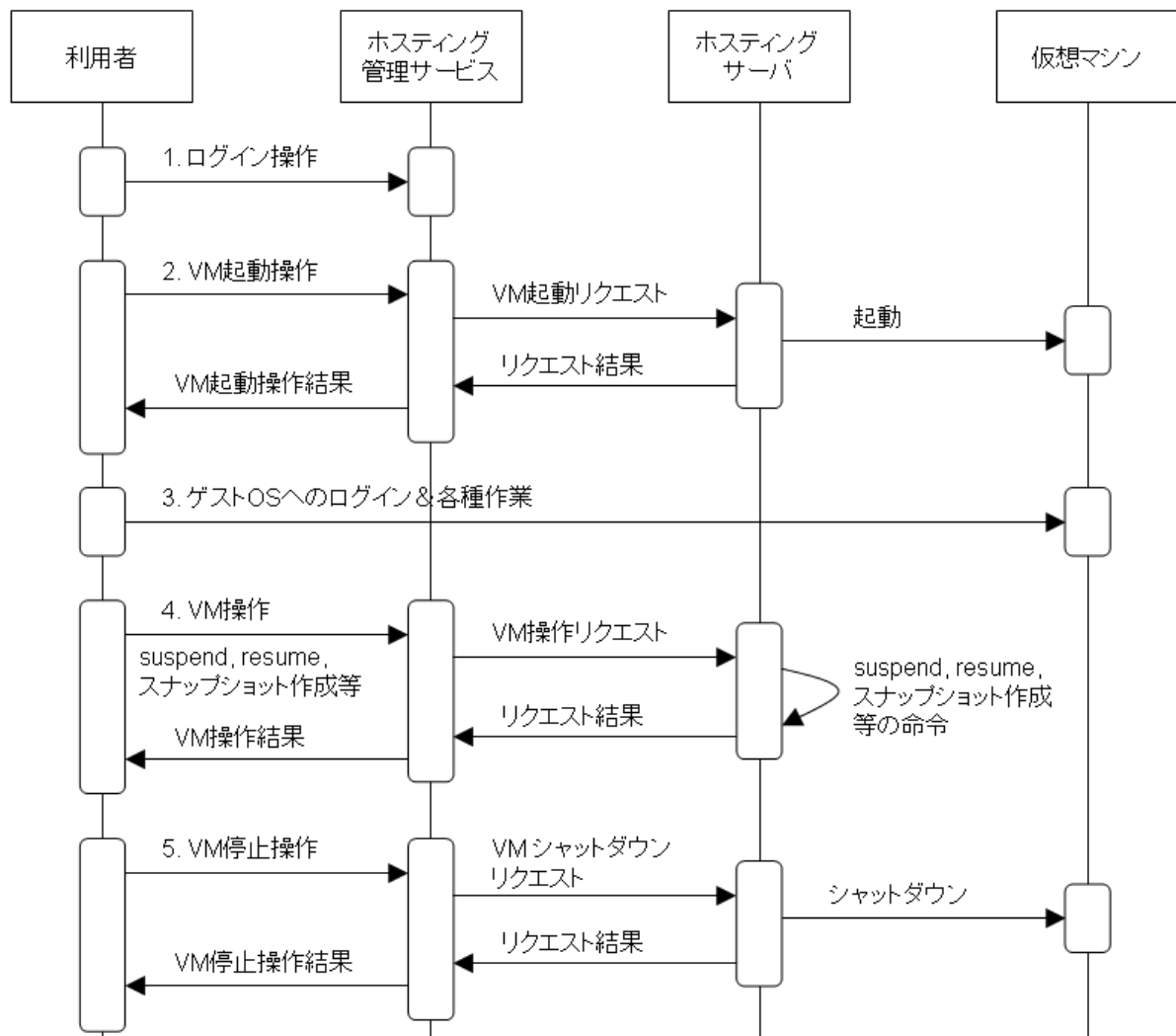


図 2 分散開発環境ホスティング機能利用フロー

分散開発環境ホスティング機能を使用する場合、利用者はまずホスティング管理サービスにログインする(1. ログイン操作)。ログイン時に使用するアカウントは、「2.1.1 先端ソフトウェア運用基盤利用申請」で取得したアカウントである。ホスティング管理サービスには HPCI 認証基盤で提供される GSI 認証による ssh ログインが可能である。以降の仮想マシンに対する操作はホスティング管理サービスにログインした状態で行う。

利用者はまずホスティング管理サービス上で VM 起動操作を行う(2. VM 起動操作)。この操作はホスティング管理サービスから適切なホスティングサーバに対して VM 起動リクエストとして要求され、共有ストレージに登録されている OS イメージを使って仮想マシン(ゲスト OS)が起動される。VM 停止操作についても同様である(5. VM 停止操作)。

動作中の仮想マシンを suspend させたり、suspend 中の仮想マシンを resume させたり、動作中の仮想マシンのスナップショットを取るといった操作を行う場合も、利用者はホスティング管理サービス上でそれぞれの操作を行う(4. VM 操作)。各操作は該当するホスティングサーバに要求され処理される。

仮想マシン起動後のゲスト OS 上での作業は、ゲスト OS に直接ログインして行う。ゲスト OS 上での操作の責任は利用者に一任される(3. ゲスト OS へのログイン&各種作業)。

(2) OS イメージ操作フロー

仮想マシン起動時に必要となる OS イメージは、事前に共有ストレージに登録しておく必要がある。OS イメージの操作フローを「図 3 OS イメージ操作フロー」に示す。



図 3 OS イメージ操作フロー

OS イメージの操作を行う場合にも、利用者はまずホスティング管理サービスにログインする(1. ログイン操作)。各操作はログインした状態で行う。OS イメージを登録する場合、利用者はホスティング管理サービス上で OS イメージの登録を行う(2. OS イメージ登録操作)。この操作では、利用者が用意した OS イメージがアップロードされ、共有ストレージに書き込まれる。

仮想マシン上で動作中の OS イメージを保存する場合、利用者はホスティング管理サービス上で

まず VM 状態保存の要求を行い(3. VM 状態保存要求)、その後に VM 停止操作を行う(4. VM 停止操作)。この操作がホスティング管理サービスからホスティングサーバに対して要求され、ホスティングサーバ上で共有ストレージへの OS イメージの書き込みが行われる。

分散開発環境ホスティング機能で使用中の OS イメージを他の環境に持っていくには共有ストレージに保存された OS イメージをダウンロードする必要がある。この場合、利用者はホスティング管理サービス上で OS イメージ取得操作を行う(5. OS イメージ取得操作)。この操作によりホスティング管理サービスによって共有ストレージから OS イメージが読み込まれ利用者の環境(PC 等)へダウンロードされる。

登録あるいは保存した OS イメージを削除する場合、利用者はホスティング管理サービス上で OS イメージ削除操作を行う(6. OS イメージ削除操作)。この操作によりホスティング管理サービスによって共有ストレージ上の OS イメージが削除される。

2.2.2. ヘルプフロー

分散開発環境ホスティング機能利用に際して不明点があれば、利用者はまず公開されている FAQ 等で確認を行う。FAQ 等の公開された情報では解決できない場合は、先端ソフトウェア運用基盤の問い合わせ先にメールで問い合わせる。問い合わせ先となるヘルプデスクは先端ソフトウェア運用基盤運営局が兼ねても良い。問い合わせ対応のフローを「図 4 ヘルプフロー」に示す。

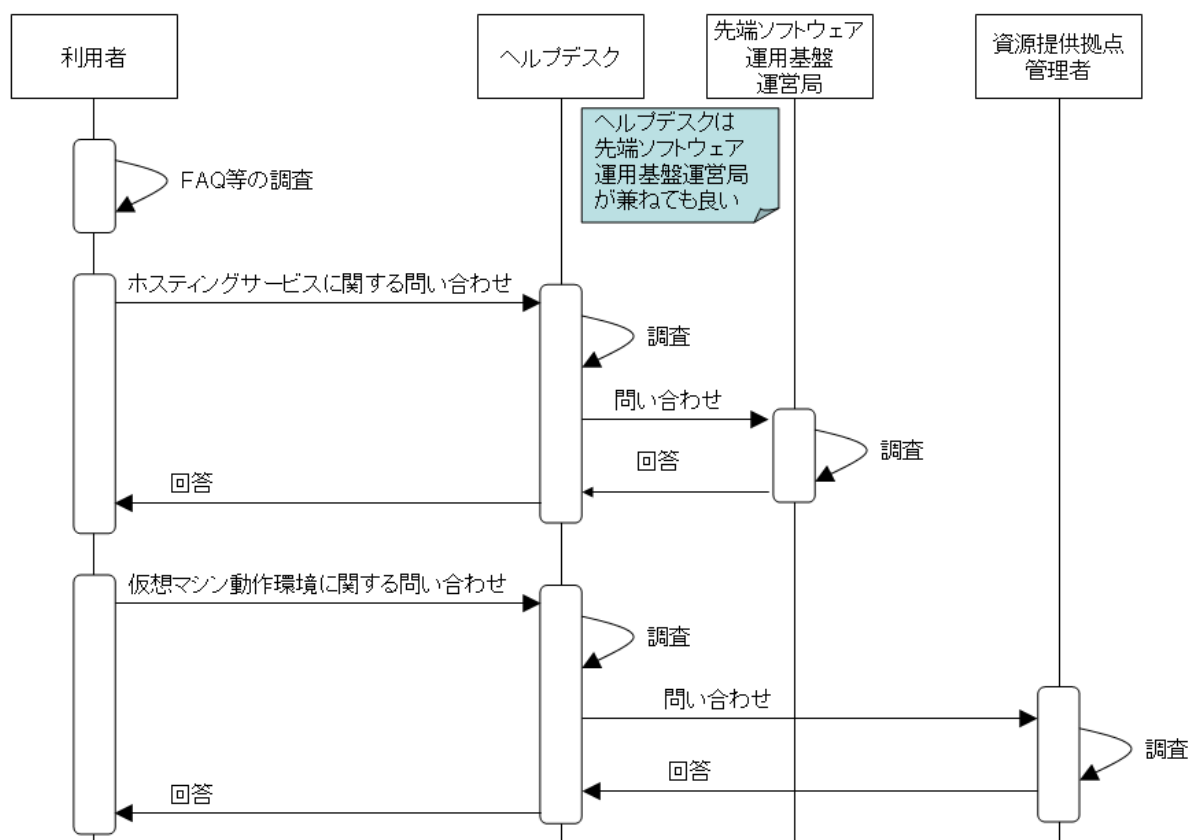


図 4 ヘルプフロー

利用者からの問い合わせ内容がホスティングサービスに関するものであれば、ヘルプデスク担当者は過去の問い合わせを確認し同じ内容があればその際の回答内容を利用者に返す。過去に問い合わせがなければ先端ソフトウェア運用基盤運営局に調査を依頼し、先端ソフトウェア運用基盤運営局からの調査結果を利用者に回答する。問い合わせ内容が仮想マシンの接続しているネットワーク等の動作環境に関するものであれば、ヘルプデスク担当者は過去の問い合わせを確認し同じ内容があればその際の回答内容を利用者に返す。過去に問い合わせがなければ該当仮想マシンの動作しているホスティングサーバの管理者（資源提供拠点管理者）に利用者からの問い合わせに対する調査を依頼し、資源提供拠点管理者からの調査結果をヘルプデスク経由で利用者に回答する。

3. 基盤構築・運用基本仕様

3.1. 必要要件

HPCI 利用者には応用 HPC 研究者と CS 系研究者の 2 種類に大別できると想定している。それぞれに以下のような利用シナリオを想定し、そのシナリオに沿った利用が可能な計算機環境を提供する必要がある。

- 応用 HPC 研究者の利用シナリオ
 - － HPC リソースを用いた大規模計算（データ解析・シミュレーション等）を実行したい
 - － 特定 OS・ライブラリに依存するアプリを利用したい
 - － HPC リソースにアクセスするためのポータルサービスを実行したい
 - － 成果公開・プロジェクトメンバー内情報共有のための Web ポータルがほしい
- CS 系研究者の利用シナリオ
 - － root 権限が必要な、OS レベルの研究開発をしたい
 - － ライブラリの開発をしたので、複数種の OS で検証したい
 - － 分散システムの開発をするため、多拠点にグローバル IP を持つサーバがほしい
 - － 成果公開・プロジェクトメンバー内情報共有のための Web ポータルがほしい

HPC 研究者の利用シナリオにある HPC リソースを用いた大規模計算は HPCI 拠点スパコンがサポートするが、スパコンでは所有拠点の定めた管理規則に従った一般利用者権限の作業スペースを提供するだけであり、root 権限や特定ポートを用いた通信などの特殊権限を要するそれ以外のシナリオをサポートすることができない。これらシナリオでは、高信頼なサーバ・サービスによる OS レベルからアプリケーションレベルにわたる多彩なホスティングが求められる。特に CS 系研究者の利用シナリオでは、管理者権限を持ったサーバからなる、必要に応じて分散配備可能な開発環境が求められる。HPCI として多岐にわたる研究者の要望・要求に応え、発展していくためには拠点スパコンを連携させるだけでは不十分であり、スパコンでは実現し得ないこれら利用シナリオをサポートする基盤が必要である。

高信頼なサーバでのホスティングや分散配備可能な開発環境は、従来、利用者が個別にサーバ・クラスタを購入して構築していたが、先端ソフトウェア運用基盤は研究者からの個々の要求に対し、再利用可能な共通サービスにより必要とされるプログラム実行環境を提供する。具体的には、頻繁に利用されるソフトウェアを導入した仮想マシン（VM）・サービスのホスティングを行う。先端ソフトウェア運用基盤は以下の理由から実機ではなく、VM・サービスレベルでのホスティングを採用した。

- 運用の安全性
 - 物理サーバによる提供は、ファームウェアの更新も利用者が可能となるため、管理・運用上困難
- 権限の委譲の制限

サーバ単位での提供は利用者に必要以上の権限を与えることもある。例えば、Web 系のコンテンツホスティングサービスを利用する際には、利用者にはサーバ root 権限は不要であり、逆に root 権限を持つことを嫌う者もいる。

- 資源の有効活用

Many Core 化、大容量メモリを搭載したサーバの普及により、多数の利用者の要求を少数サーバに集約可能

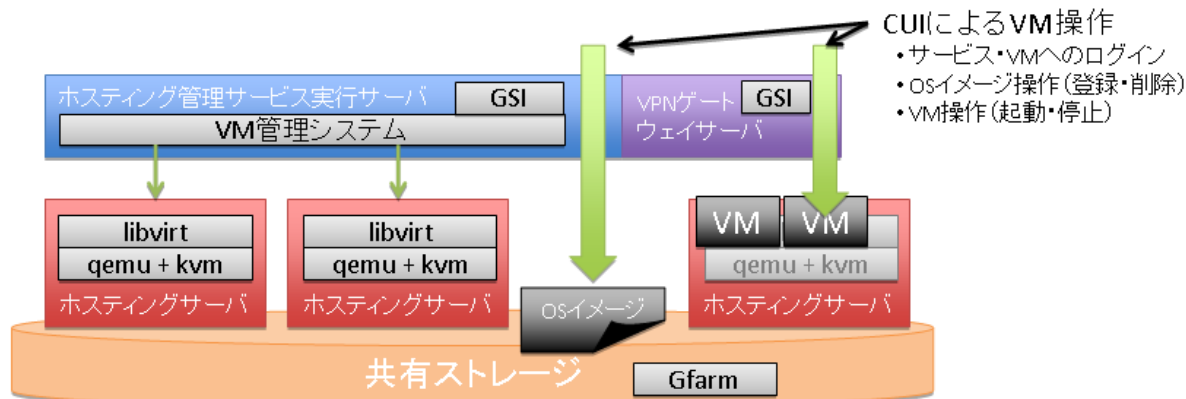
基盤センター群に対して、利用者に提供しているホスティングサービスのアンケートを行ったところ（付録 2.2 参照）、実機によるホスティング、VM によるホスティング、Web ホスティングに多くの利用者がいることがわかった。また、センターによっては有償アプリケーションのライセンスサーバホスティングや、DNS 登録のホスティングを行っている場所もあった。ライセンスサーバや DNS 登録のホスティングは拠点内部の運用と深く関わるため先端ソフトウェア運用基盤での提供は行わないが、以下のホスティング機能の提供を検討する。

- VM によるサーバホスティング
 - － プロジェクトサーバホスティング
申請課題プロジェクトごとに目的別サーバを提供
 - － 分散開発環境ホスティング
OS、分散システム開発のための環境を広域配備
- Web サービスホスティング
課題申請プロジェクトごとの情報公開用 Web スペース（Apache ディレクトリ、blog サービスなど）のホスティング

3.2. 平成 23 年度テストベッド

平成 23 年度は、平成 24 年度以降の HPCI 本格運用時に求められる、OS・分散システム等の研究開発環境構築のため、先行試験システムとして配備が進んでいる RENKEI-PoP による VM ホスティング環境をベースに設計した環境での実験を行う。環境は、実証実験用に資源を供出可能な拠点の資源より構成される。この実験により、HPCI 先端ソフトウェア運用基盤で提供する分散開発環境ホスティングとして求められる機能の精査、運用体制を勘案し、平成 24 運用システムの詳細仕様検討を行う。

平成 23 年度の実証実験の環境を「図 5 分散開発環境ホスティング機能実験環境」に示す。



実証実験に参加する拠点は VM 実行の処理を担うホスティングサーバを最低 1 台供出する。ホスティングサーバ間では、そのローカルストレージの一部を集約して共有ストレージを構成し、利用者が起動する VM で用いるベース OS イメージを格納する。ホスティングサーバは共有ストレージより OS イメージをローカルディスクにコピーした後に、その OS イメージを使用する VM を実行する。

利用者の VM 実行・停止等の操作は、ホスティング管理サービスにログインした後に、コマンドラインにて行う。ホスティング管理サービスは VM 操作命令・OS イメージ操作命令を利用者より受け付け、該当処理を行う。ホスティング管理サービスを実行するホスティング管理サービス実行サーバを 1 拠点に配備する。その拠点には、VM が接続されているネットワークに利用者から接続するためのログインゲートウェイである VPN ゲートウェイサーバも配備する。

実証実験では、RENKEI プロジェクト (<http://www.e-sciren.org/>) で東工大が中心に進めている RENKEI-PoP の成果も活用予定である。

3.3. 機能

3.3.1. 分散開発環境ホスティングの機能

分散開発環境ホスティングは以下の機能を提供する。

(1) 多拠点に配備したホスティングサーバ上での VM 実行

利用者はポータルサーバにログインして、VM 起動・停止、OS イメージ登録・削除を行う。この機能を実現するために、RENKEI-PoP 用に開発している VM 管理システムを利用する。

(2) 利用可能な仮想マシンイメージ

利用者には VM の root 権限を付与し、ゲスト OS 上での各種の設定を可能にする。また、グローバル IP アドレスを割り当て、異なる拠点の VM 間での連携を可能にする。VM の標準構成は 1 CPU コア、4GB メモリ、100GB ディスク、1000Mbps ネットワークインターフェースとする。

(3) 共有ストレージの利用

VM の OS イメージはホスティングサーバ間のグローバル共有ストレージ上で保存・管理する。ホスティングサーバはこの共有ストレージからローカルディスクに

OS イメージをコピーした後に、VM を実行する。共有ストレージには Gfarm を利用する。

(4) VM 管理機能

「図 6 VM 管理モデル」に VM 管理のための機能モデルを示す。

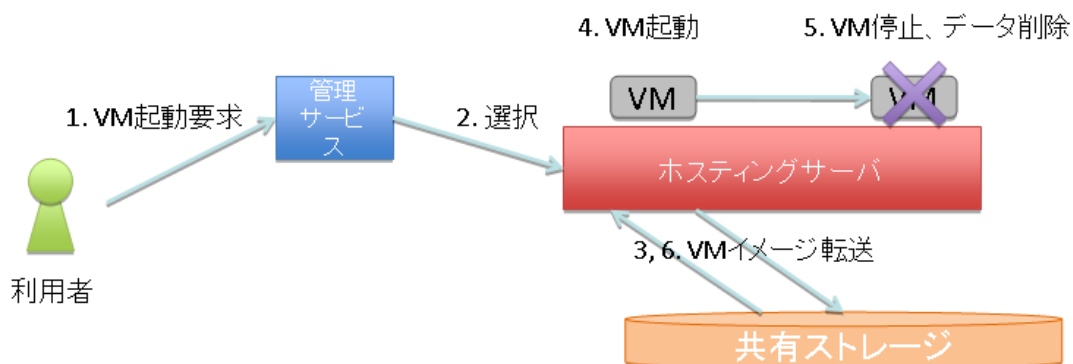


図 6 VM 管理モデル

0. 利用者はホスティング管理サービスにログイン
 1. 利用者はホスティング管理サービスに VM 起動を要求
 2. ホスティング管理サービスは適切なホスティングサーバを選択
 3. 共有ストレージから OS イメージをホスティングサーバに Import
 4. ホスティングサーバ上で必要な設定を施し、VM を起動
 5. VM shutdown 時には、ホスティングサーバから関連ファイルを削除
 6. 任意のタイミングで、OS イメージを共有ストレージに Export 可能
- 上記の操作・動作を可能とする VM 管理機能を提供する。

(5) ネットワーク

SINET VPN による多拠点接続されたネットワークセグメントを提供する。このネットワークに、ホスティング管理サービス実行サーバ、ホスティングサーバ、VM が接続しており、全ポートでの通信可能である。VPN であるため、インターネット等別ネットワークから直接アクセスすることはできない。

インターネットに接続可能なネットワークセグメントを提供する。ホスティング管理サービス実行サーバはこのネットワークに接続している。ホスティングサーバおよび仮想マシンをこのネットワークに接続させることも可能である。サーバ・VM へのアクセスは「表 2 インターネット接続ネットワークセグメントの必須ファイアウォール設定」に示す設定のファイアウォールにより、制限されている。

上記 VPN へのゲートウェイとして、ホスティング管理サービス実行サーバを保有する拠点では双方のネットワークセグメントに接続可能なログインサーバ(VPN ゲートウェイサーバ)を提供する。ホスティング管理サービス実行サーバが VPN ゲートウェイサーバを兼ねる場合もある。

「図 7 分散開発環境ホスティング機能のネットワーク環境」に分散開発環境ホスティング機能で使用するネットワーク環境を示す。

表 2 インターネット接続ネットワークセグメントの必須ファイアウォール設定

	inbound	outbound
ホスティング管理サービス実行サーバ	ANY => 22/tcp	=> ANY: 22/tcp
VPN ゲートウェイサーバ	ANY => 22/tcp	=> ANY: 22/tcp => ANY: 80/tcp => ANY: 443/tcp

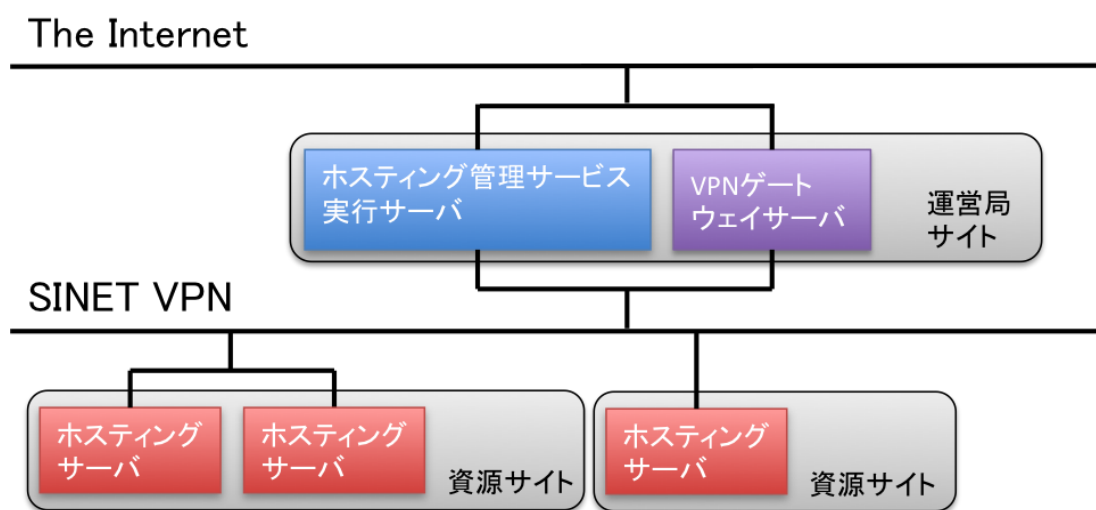


図 7 分散開発環境ホスティング機能のネットワーク環境

3.4. 運用・保守

運用・保守体制については、平成 23 年度の試験運用を元に平成 24 年度以降のシステムに求められる詳細仕様を検討する。

平成 23 年度では運用主体として以下の三者を想定している。

- 資源提供拠点管理者
- 先端ソフトウェア運用基盤運営局
- HPCI 事務局

それぞれの管理対象を以下に定義する。詳細は次節以降にまとめる。

- 資源提供拠点管理者
 - ホスティングサーバを管理
- 先端ソフトウェア運用基盤運営局
 - ホスティング管理サービスを管理
 - VPN ゲートウェイサーバを管理
 - 試験運用環境ヘルプデスクを管理
- HPCI 事務局
 - 先端ソフトウェア運用基盤を使用する課題の審査

平成 23 年度は、先端ソフトウェア運用基盤運営局は東京工業大学に設置することを計画して

いる。

3.4.1. ホスティングサーバ導入・運用・保守

資源提供拠点管理者は、ホスティングサーバ設置拠点ごとに存在し以下の運用・保守業務を実施する。

(1) ホスティングサーバの設置

- ホスティングサーバとなるサーバを 1 台以上用意する。
- ホスティングサーバを搭載可能なラックスペース、および電源設備を確保すること。
 - 電源は UPS による無停電対策されていると良い。
- ホスティングサーバを「3.3.1 (5) ネットワーク」に示したネットワークに接続させるために必要なルータ・スイッチポートを確保すること。
- ホスティングサーバの設置、電源・ネットワーク配線を行うこと。
- 必要に応じてコンソール入出力配線を行うこと。

(2) ホスティングサーバの導入・接続設定

- 拠点ネットワーク管理者に「3.3.1 (5) ネットワーク」に示したネットワークセグメントに属す IP アドレス割当て、およびファイアウォール設定を依頼すること。可能であれば、SINET VPN セグメントでは IDS 等のフィルタサービスを止めることを依頼すること。
- BIOS あるいは EFI 等システム設定ツールにて仮想化支援機能を有効にすること。
- 搭載するストレージデバイスを、最低限以下の 4 種類のパーティションに分割すること。
 - システム領域用 (マウントポイント: /)
 - ユーザホーム領域用 (マウントポイント: /home)
 - ローカルデータ領域用 (マウントポイント: /work)
サイズは、1 台のホスティングサーバ上で同時実行される標準 VM の数と標準 VM の最大ディスクサイズ (100GB) を掛け合わせた値以上であること。
 - 共有ストレージ供出領域用 (マウントポイント: /share)
サイズは、ローカルデータ領域用ストレージデバイスと同等程度が望ましい。
- OS・ソフトウェア群を導入すること。
- SELinux は無効にして良い。
- SINET VPN 接続インターフェースはブリッジとして構成すること。
- 適切な NTP サーバと時刻同期を行うこと。
- ホスティング管理サービス実行サーバからの ssh ログインを受け入れること。
 - パスワード認証は無効にすること。
 - root ログインは無効にすること。

- 共有ストレージ供出領域用ストレージデバイスをデータ格納用スプールとして Gfarm FileServer (gfsd) を構成すること。
 - gfarm 設定ファイルは先端ソフトウェア運用基盤運営局に問い合わせ入手すること。
 - gfsd 情報を先端ソフトウェア運用基盤運営局に通知すること。
 - VM 管理者アカウントを作成すること。
 - virsh(libvirt) で SINET VPN にブリッジ接続する VM を起動できること。
 - 先端ソフトウェア運用基盤運営局より受け取った、VM 管理システム管理者用 ssh 公開鍵を設定すること。
 - 先端ソフトウェア運用基盤運営局にサーバ情報 (ホスト名、IP アドレス) を通知すること。
- (3) VM ホスティングのための準備
- VM 用のホスト名・IP アドレスを決め、DNS サーバに登録すること。
 - 先端ソフトウェア運用基盤運営局に以下の情報を通知すること。
 - VM 用ネットワーク環境 (ネットワーク情報、ntp サーバ、dns サーバ)
 - VM のホスト名、IP アドレス
- (4) 通常管理
- ソフトウェアパッケージの定期的なアップデートを行うこと。
 - 停電を伴う保守時の停止・起動を行うこと。
- (5) 障害対応
- ハードウェアの障害については、各資源提供機関の障害対応手順に従う。
 - 共有ストレージにて障害が発生した場合は、先端ソフトウェア運用基盤運営局と連携して復旧作業を行うこと。
- (6) セキュリティインシデント発生時の対応
- ① VM におけるインシデント発生時
 - 該当 VM を即刻停止すること。
 - 該当 VM ホスティングサービス利用者、先端ソフトウェア運用基盤運営局に通知すること。
 - ホスティングサーバへの侵入がないか調査し、侵入痕跡があった場合は②の対処を行うこと。
 - ② ホスティングサーバにおけるインシデント発生時
 - ホスティングサーバ設置拠点の運用ポリシーに従いインシデント対応を行うこと。
 - root 権限が奪われた場合、実行中であった VM の OS イメージは、可能であればホスティングサーバから取り出し、先端ソフトウェア運用基盤運営局がアクセスできるネットワーク環境に置くこと。
 - root 権限が奪われた場合、共有ストレージに供出している、該当ホスティングサーバ上のファイルはすべて削除して良い。
- (7) セキュリティインシデント発生時の対応

- ホスティングサーバの障害・保守・セキュリティインシデント発生を先端ソフトウェア運用基盤運営局、利用者に通知すること。

3.4.2. ホスティング管理サービス導入・運用・保守

ホスティング管理サービスは HPCI 先端ソフトウェア運用基盤、分散開発環境ホスティング機能実現システムに唯一存在し、以下の運用・保守業務を必要とする。

- (1) ホスティング管理サービス実行サーバの設置
 - ホスティング管理サービス実行サーバを設置可能なラックスペース、および電源設備を確保すること。
 - 電源は UPS による無停電対策されていると良い。
 - ホスティング管理サービス実行サーバを「3.3.1 (5) ネットワーク」に示したネットワークに接続するために必要なルータ・スイッチポートを確保すること。
 - ホスティング管理サービス実行サーバの設置、電源・ネットワーク配線を行うこと。
 - 必要に応じてコンソール入出力配線を行うこと。
- (2) ホスティング管理サービス実行サーバの導入・接続設定
 - 拠点ネットワーク管理者に「3.3.1 (5) ネットワーク」に示したネットワークセグメントに属す IP アドレス割当て、およびファイアウォール設定を依頼すること。
 - 搭載するストレージデバイスを、最低限以下の 3 種類のパーティションに分割すること。物理的に異なるストレージデバイスを 2 つ以上搭載している場合、データ領域用に 1 つのストレージデバイスを専用に割り当てること。
 - システム領域用 (マウントポイント: /)
 - ユーザホーム領域用 (マウントポイント: /home)
 - データ領域用 (マウントポイント: /work)
 - OS・ソフトウェア群を導入すること。
 - SELinux は無効にして良い。
 - 適切な NTP サーバと時刻同期を行うこと。
 - 認証局よりホスト証明書を取得し、gsi 認証用に配置すること。
 - 任意のサーバからの ssh ログインを受け入れること。
 - 公開鍵認証、gsi 認証を有効にし、パスワード認証は無効にすること。
 - root ログインは無効にすること。
 - データ領域用ストレージデバイス上にメタデータ用 DB を設定し、Gfarm Metadata Server (gfmd) を構成すること。
 - VM 管理者アカウントを作成すること。このアカウントでホスティング管理サービスを実行すること。
- (3) VM ホスティングのための準備
 - 各ホスティングサーバの VM・ネットワーク情報 (VM 用ホスト名・IP アドレス、ネットワーク) をホスティング管理サービスに登録すること。

- ベース OS イメージ群を作成し、ホスティング管理サービスに登録すること。
 - イメージの複製を 3 つ以上作成すること。
- VM 構成を定義・作成し、ホスティング管理サービスに登録すること。
- (4) 共有ストレージの準備
 - ホスティングサーバを共有ストレージのファイルシステムサーバ (Gfarm File Server) として登録すること。
- (5) 通常管理
 - ソフトウェアパッケージの定期的なアップデートを行うこと。
 - 年 1 回のホスト証明書の更新をすること。
 - 月 1 回の CRL のアップデートをすること。
 - ホスティング管理サービス状態保存 DB の定期的なバックアップを行うこと。
 - 停電を伴う拠点全体メンテナンス時の停止・起動を行うこと。
- (6) 障害対策
 - ホスティング管理サービス状態保存 DB 障害発生時には、バックアップ DB を用いてリストアすること。
 - ホスティングサーバのローカルストレージ枯渇時の対応を行うこと。
 - 枯渇したホスティングサーバ上の gfarm スプールデータを他のホスティングサーバに移動すること。
 - データ移動だけでは解決しない場合、データの削除を利用者に依頼すること。
 - 共有ストレージ障害対策
 - ストレージを構成するハードウェアに対する対応は、各資源提供機関の障害対策手順に従うこと。
 - 障害の影響調査および復旧を gfarm 等のストレージソフトウェア管理者、実際にストレージの領域を使用しているホスティングサーバの管理者と協力して行うこと。なお、平成 23 年度の実証実験では、ストレージソフトウェア管理者は先端ソフトウェア運用基盤運営局が担う。
 - 障害調査手順は、ストレージソフトウェアが定める手順に従って行うこと。
- (7) 利用者アカウント管理
 - 利用者からの申請に対して許可を与える。
 - アカウントの作成・削除を行う。
 - grid-mapfile の更新を行う。
- (8) セキュリティインシデント発生時の対策
 - ① ホスティング管理サービス実行サーバにおけるインシデント発生時
 - ホスティング管理サービス実行サーバ設置拠点の運用ポリシーに従いインシデント対応を行うこと。
 - ② 他サーバ (VM、ホスティングサーバ、VPN ゲートウェイサーバ) におけるインシデント発生時
 - 進入痕跡の有無の調査を行い、侵入があった場合には①の対処を行う。
 - 全利用者・全資源提供拠点管理者に通知し、進入痕跡の有無の調査を依頼す

ること。

- VM イメージへのインシデントの場合、問題 VM が使用していた OS イメージを利用者に提供すること。

(9) 情報通知

- 各ホスティングサーバの障害・保守・セキュリティインシデント発生を利用者に通知
- ホスティング管理サービスの障害・保守・セキュリティインシデント発生を利用者、資源提供拠点管理者に通知

3.4.3. VPN ゲートウェイサーバ導入・運用・保守

VPN ゲートウェイサーバは、HPCI 先端ソフトウェア運用基盤、分散開発環境ホスティング機能実現システム全体で一つ以上存在し以下の運用・保守業務を必要とする。VPN ゲートウェイサーバの機能を、ホスティング管理サービス実行サーバが兼ねても良い。

(1) VPN ゲートウェイサーバ設置

- VPN ゲートウェイサーバとなるサーバを 1 台以上用意する。
- VPN ゲートウェイサーバを設置可能なラックスペース、および電源設備を確保すること。
 - 電源は UPS による無停電対策が実施されていると良い。
- VPN ゲートウェイサーバを「3.3.1 (5) ネットワーク」に示したネットワークに接続するために必要なルータ・スイッチポートを確保すること。
- VPN ゲートウェイサーバの設置、電源・ネットワーク配線を行うこと。
- 必要に応じてコンソール入出力配線を行うこと。

(2) VPN ゲートウェイサーバの導入・接続設定

- 拠点ネットワーク管理者に「3.3.1 (5) ネットワーク」に示したネットワークセグメントに属す IP アドレス割当て、およびファイアウォール設定を依頼すること。
- 搭載するストレージデバイスを、最低限以下の 2 種類のパーティションに分割すること。
 - システム領域用（マウントポイント：/）
 - ユーザホーム領域用（マウントポイント：/home）
- OS・ソフトウェア群を導入すること。
- SELinux は無効にして良い。
- 適切な NTP サーバと時刻同期を行うこと。
- 認証局よりホスト証明書を取得し、gsi 認証用に配置すること。
- 任意のサーバからの ssh ログインを受け入れること。
 - 公開鍵認証、gsi 認証を有効にし、パスワード認証は無効にすること。
 - root ログインは無効にすること。
- SINET VPN に属すサーバの http proxy、参照 DNS サーバとしての機能を有すること。

(3) 通常管理

- ソフトウェアパッケージの定期的なアップデート
- 年 1 回のホスト証明書の更新
- 月 1 回の CRL のアップデート
- 利用者のホーム領域の定期的なバックアップ
- 停電を伴う拠点全体メンテナンス時の停止・起動

(4) 障害対策

- ソフトウェア、サービス障害が起きた場合には調査を行い、適切な対応を行うこと。
- ハードウェア障害が起きた場合は、問題コンポーネントを特定し、修理・交換を行うこと。
- ストレージデバイスを交換する際は、必要に応じてバックアップしておいた利用者ホーム領域データをリストアすること。

(5) 利用者アカウント管理

- 利用者からの申請に対して許可を与える。
- アカウントの作成・削除を行う。
- grid-mapfile の更新を行う。

(6) セキュリティインシデント発生時の対策

- ① VPN ゲートウェイサーバにおけるインシデント発生時
 - VPN ゲートウェイサーバ設置拠点の運用ポリシーに従いインシデント対応を行うこと。
- ② 他サーバ (VM、ホスティングサーバ、ホスティング管理サービス実行サーバ) におけるインシデント発生時
 - 進入痕跡の有無の調査を行い、侵入があった場合には①の対処を行う。

(7) 情報通知

- VPN ゲートウェイサーバの障害・保守・セキュリティインシデント発生を利用者に通知すること。

3.4.4. ヘルプデスク運用

平成 23 年度は実証実験を目的とした試験運用であるため、利用者が限られると考えられるので、小規模なヘルプデスク運用を先端ソフトウェア運用基盤運営局が行うこととする。平成 24 年度以降の本格運用時には Web インターフェースを持ったチケット管理システム等の導入を検討しているが、詳細仕様策定は平成 24 年度に行う。

平成 23 年度の試験運用環境ヘルプデスクは以下の通りに運用する。

- 利用者からの質問窓口用電子メールアドレスを用意すること。
- 上記電子メール受取者として、先端ソフトウェア運用基盤運営局担当者の電子メールアドレスを登録すること。
- 先端ソフトウェア運用基盤運営局担当者は質問に回答すること。
- 平成 24 年度以降の詳細仕様・追加仕様策定のための参考情報として利用者との質

疑応答を利用できるように、アーカイブすること。

3.4.5. HPCI 事務局

(1) 通常の HPCI 公募課題と同様に審査

- － 先端ソフトウェア運用基盤を HPCI の 1 リソースとして扱うこと。

3.5. 追加仕様

3.5.1. 機能

先端ソフトウェア運用基盤における平成 24 年度およびそれ以降に実現する追加機能は、平成 23 年度の実験運用の結果を基に明らかにしていく。現状分散開発環境ホスティング機能の追加機能として、以下の機能を段階的に実現していくことを想定している。

(1) 資源提供拠点供出リソースのクラスタ構成

- － クラスタハードウェアの構成定義

平成 24 年度では本格運用のためにホスティング資源の追加が求められるため、拠点供出資源のクラスタ構成を検討している。VM ホスティングサーバ、ネットワーク構成、クラスタローカルの共有ストレージの構成について必須構成、奨励構成を策定する。

- － クラスタ内部ネットワーク、および外部接続ネットワークの論理構成設計

拠点資源をクラスタ構成とした場合、各ホスティングサーバへの VM 操作命令を送出する管理ネットワークは、クラスタのフロントエンドサーバを除き、プライベートネットワークにすることを検討している。また、利用者ごとのネットワークセグメント分断、VM が各種外部ネットワークに接続できる環境の提供を検討している。そのためには VLAN 等でネットワークを論理的に分割することが必要となり、また、帯域保証が求められるだろう。管理ネットワーク、共有ストレージ用ネットワーク、VM 間通信用ネットワークについての構成設計を行う。

- － クラスタソフトウェアの構成定義

クラスタ構成にすることにより、単一のホスティングサーバでの構成に加えて追加で必要となるソフトウェア項目について調査検討し、推奨構成を策定する。

- － VM 配置スケジューラの機能

拠点ごとのホスティング用資源をクラスタ構成にすることにより、平成 23 年度実験システムで想定している、全ホスティングサーバがネットワーク的にフラットに配置されている構成を対象とした VM 配置スケジューリングポリシーへの変更が必要となる可能性もあり、調査検討を行った後に、必要項目の開発を行う。

- － ホスティング管理サービスの構成定義

VM 配置スケジューラも含め、プライベートネットワーク構成となり得るホステ

イング用クラスタが拠点資源として供出されうるので、その構成に対応したホスティング管理サービスの構成について調査検討を行った後、必要項目の開発を行う。

(2) VM 用ネットワーク環境の構成変更

－ VM へのプライベート IP アドレス割当て

VM を利用する際に、一意のアドレスで VM を指定できれば利便性は向上する。一方、大勢の利用者の VM 環境をホストする際に、すべての VM にグローバル IP アドレスを割り当てることは困難である。利用者の増加に伴い、グローバル IP アドレスの消費削減のために、グローバル IP アドレスが不要なサーバにはプライベート IP アドレスのみを割り振るシステムとして構成する必要がある。これにより、1 拠点内部で複数 VM を実行する場合、プライベート IP アドレスを割り当てた VM クラスタとして構成可能である。実現のためにはグローバル IP とプライベート IP の両方を持つマルチホーム VM や、ポートフォワードが構成できる必要がある。仮想ルータや、仮想スイッチによる実現可能性、構成方法の調査検討を行う。

－ 申請課題ごとの VM ネットワークの分断機能

セキュリティ向上、およびブロードキャストのドメイン分割のため、特にプライベート IP アドレスが割り振られた VM クラスタの場合、申請課題ごとの VM ネットワークの分断が機能として求められる。拠点内部では仮想ルータや、仮想スイッチによる実現可能性、構成方法の調査検討を行う。拠点間では、主に通信の機密性保護を目的とし、SINET オンデマンド VPN 等の利用を検討していく。

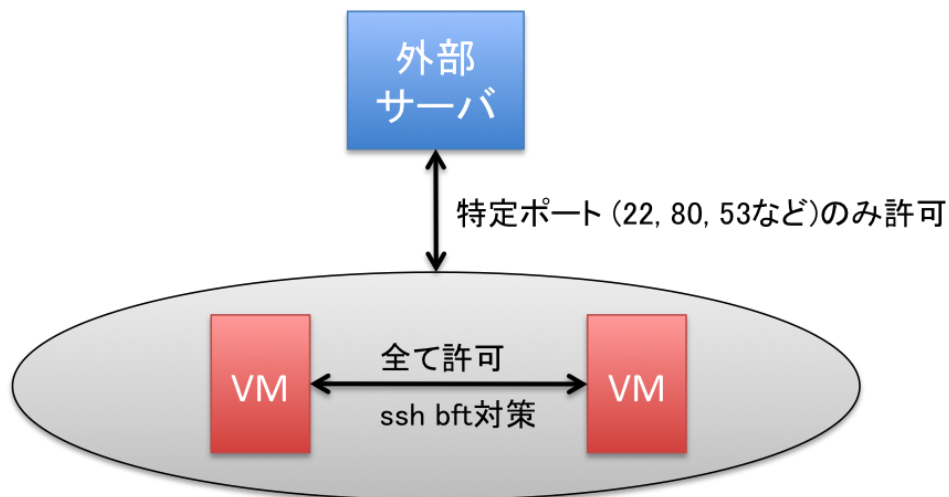
－ Internet Reachable ネットワークを VM ネットワークに使用

利用者の VM アクセスの利便性を考慮すると、SINET VPN ではなく、Internet Reachable ネットワークの IP アドレスを VM に割り振る方が良い。この場合に要求されるファイアウォール、IDS のセキュリティモデルの調査検討を行う。

平成 24 年度以降に想定している VM ネットワークを「図 8 平成 24 年度以降の先端ソフトウェア運用基盤 VM ネットワーク案」に示す。VM が動作する拠点資源を拠点ファイアウォールの外側に設置し、拠点資源管理者が独自に設定を行うことができることを想定している。ファイアウォールは拠点ごとに設定され、特定のポート(ポート 22 など)を使った通信のみを通す。また VM の通信に対して、検知フィルタは可能であれば解除するものとする。

－ IPv6 対応

先端ソフトウェア運用基盤として、IPv6 対応ソフトウェアの研究開発を希望する課題申請が想定されるため、提供を検討していく。



先端ソフトウェア運用基盤用グローバルIPネットワーク

図 8 平成 24 年度以降の先端ソフトウェア運用基盤 VM ネットワーク案

(3) Web GUI 環境の提供

利用者の利便性向上のため、最低限 VM、OS イメージ操作に関する Web GUI を備えた利用者用インターフェースを提供する。Web GUI で提供すべき機能の精査、実装方法についての検討を行う。

(4) Pre-Configured OS イメージの提供

研究者の利用環境を迅速に構築するために、Web サーバ機能、CMS サーバ機能、データベース機能等を実現するためのソフトウェアが予め導入された VM 用の OS イメージを提供する。提供すべき OS イメージの種類の調査を行う。

3.5.2. 運用・保守

先端ソフトウェア基盤における平成 24 年度およびそれ以降の運用・保守に関する追加仕様は、平成 23 年度の実証実験の結果を基に明らかにしていく。現状は以下の機能を段階的に実現していくことを想定している。

(1) ホスティングクラスタの運用・保守仕様策定

分散開発環境ホスティングで使用するハードウェアの追加、ネットワーク・ソフトウェア構成の追加・変更が行われるため、対応する運用・保守仕様の策定を行う。

(2) HPC ストレージとの連携

分散開発環境ホスティング機能実現のための共有ストレージとして、HPC ストレージの一部を使用する。HPC ストレージで定める運用・保守規則との仕様調整を行う。

3.6. 検討項目

平成 23 年度以降の検討項目として、以下の項目を挙げる。

(1) 仮想マシンと拠点ローカル資源との連携

分散開発環境ホスティング機能を用いて、複数のジョブスケジューラを統合管理するスーパースケジューラのようなソフトウェアの開発・評価を行う場合、仮想マシンと HPCI 参加拠点のローカル資源（スケジューラ、ネットワーク、アカウント）を連携・接続することが求められる場合がある。技術的には可能であるが、このようなシナリオを実現するための HPCI 拠点間の運用協定について調査検討を行う必要がある。

(2) 各種サービスホスティングの提供

「表 1 HPCI 利用想定シナリオ」に示す、利用者の「特定 OS・ライブラリに依存するアプリケーションを実行」、「HPC リソースにアクセスするためのポータルサービスを実行」、「成果公開・プロジェクトメンバー内情報共有のための WEB ポータル運用」利用シナリオを実現するための運用方針の策定を行う。上記(1)とも関連するが、拠点ごとに持つこれらシナリオを実現できるホスティングサービスの供出も含めた運用方針の検討を行う。

(3) 利用申請様式

先端ソフトウェア運用基盤利用のための利用申請様式、継続利用申請様式として必要な項目の洗い出しを行う。

(4) 課金

実運用に向けた課金方針の検討を行う。分散開発環境ホスティング機能においては VM 単価 × VM 実行時間での課金を行うことを検討しているが、その他必要項目の精査を行う。

4. 資源提供基本仕様

4.1. ホスティングサーバ

先端ソフトウェア運用基盤の分散開発環境ホスティングでは、ホスティングサーバとなるハードウェアを資源提供機関から提供を受ける。以下にホスティングサーバの構成仕様を示す。

4.1.1. ハードウェア構成

以下にホスティングサーバとして資源を提供する際のハードウェア必須構成と、推奨構成、RENKEI-PoPにおける参考構成を示す。

(1) 必須構成

- Intel 64bit 拡張された x86 系かつ、仮想化支援機能(Intel VT 等)を有すマルチコア CPU を 1 基以上搭載していること。動作周波数は 2.9GHz 以上であること。
- メモリ容量 4GB の VM を 1 台以上実行する際に全 VM メモリをオンメモリに搭載するために十分な DDR3 1333 メモリ容量を有すること。
- システム領域用、ホーム領域用ストレージデバイスとして、500GB 以上の HDD を有すること。
- ローカルデータ領域用ストレージデバイスとして、500GB 以上の HDD を有すること。サイズは、同時実行される標準 VM の数と標準 VM の最大ディスクサイズ (100GB) を掛け合わせた値以上であること。
- 共有ストレージ供出領域用ストレージデバイスとして、ローカルデータ領域用ストレージデバイスと同等程度のサイズのデバイスを有すること。
- 以上の 4 種類のストレージデバイスについて、単一のストレージデバイスを共有しても良い。
- 1000BASE-T イーサネットインターフェースを有すること。
- VGA または DVI 出力を有すること。

(2) 推奨構成

- Intel 64bit 拡張された x86 系かつ、仮想化支援機能(Intel VT 等)を有すマルチコア CPU を 2 基以上搭載していること。動作周波数は 2.9GHz 以上であること。
- メモリ容量 4GB の VM を 1 台以上実行する際に全 VM メモリをオンメモリに搭載するために十分な DDR3 1333 メモリ、24GB 以上の容量を有すること。
- システム領域用、ホーム領域用ストレージデバイスとして 500GB 以上の HDD、または SSD を有すること。システム領域用、ホーム領域用ストレージデバイスは同一デバイスを共有しても良い。
- ローカルデータ領域用ストレージデバイスとしてディスクドライブ 4 台以上から構成される RAID 装置を有すること。
- ディスクドライブ 1 台あたりの容量は HDD の場合は 2TB 以上、SSD の

場合は 200GB 以上有すること。

- ストレージデバイス全体で、同時実行される標準 VM の数と標準 VM の最大ディスクサイズ (100GB) を掛け合わせたサイズ以上の容量を持つこと。
- HBA は RAID0, 1, 5, 6, 10, 50, 60, JBOD に対応すること。
- HBA と全ディスクドライブはダイレクト接続されること。
- 共有ストレージ供出領域用ストレージデバイスとしてディスクドライブ 4 台以上から構成される RAID 装置を有すること。
- ディスクドライブ 1 台あたりの容量は HDD の場合は 2TB 以上、SSD の場合は 200GB 以上有すること。
- ストレージデバイス全体で、ローカルデータ領域用ストレージデバイス以上の容量を持つこと。
- HBA は RAID0, 1, 5, 6, 10, 50, 60, JBOD に対応すること。
- HBA と全ディスクドライブはダイレクト接続されること。
- ローカルデータ領域用ストレージデバイスと、共有ストレージ領域用ストレージデバイスは同一デバイスを共有しても良い。
- 1000BASE-T イーサネットインターフェースを 1 基有すること。
- 上記 1000BASE-T イーサネットインターフェースとは別に専用ポートにて IPMI 2.0 に対応したポートを 1 基有すること。
- 10Gbit Ethernet (10GBASE-T, SR, LR 等)イーサネットインターフェースを 1 基有すること。
- PXE によるネットワークブートが可能であること。
- VGA または DVI 出力を有すること。
- 19 インチラックに搭載可能であること。

(3) RENKEI-PoP 参考構成

CPU		Intel Xeon W3565 (3.2GHz 4core)
メモリ		24GB (DDR3 1333/4GB/ECC 6 枚構成)
ネットワーク インタフェース	1000BASE-T インターフェース Intel 82574L Gigabit Ethernet Controller 2 ポート	
	10Gbit Ethernet インターフェース Myricom 10GBASE-SR	
	IPMI 2.0 専用インターフェース Realtek RTL8201N	
ストレージ	システム領域用	2.5 インチ SATA HDD 500GB
	データ量域用	3.5 インチ SATA HDD 2TB 16 基 HBA: Adaptec RAID 51645
筐体		3U, 19 インチラック搭載可能

4.1.2. ソフトウェア構成

- OS には x86_64 対応 CentOS 5.5 相当を使用すること。

- libvirt+kvm による VM 実行機能を有すること
- gfarm バージョン 2.3.2 以上の以下のコンポーネントを導入すること
 - gfsd, client, gfarm2fs
- 以下のソフトウェアを導入すること
 - bridge-utils
 - fuse
 - iptables
 - openssh
 - ruby バージョン 1.8.7 以上
 - vnc
 - RENKEI-PoP 管理ツール群

4.2. ホスティング管理サービス実行サーバ

先端ソフトウェア運用基盤の分散開発環境ホスティングでは、ホスティングサーバを管理するホスティング管理サービスが存在し、このホスティング管理サービスが動作する専用サーバを必要とする。以下にホスティング管理サービス実行サーバの構成仕様を示す。

4.2.1. ハードウェア構成

以下にホスティング管理サービス実行サーバのハードウェア必須構成と、推奨構成、RENKEI-PoP 管理サーバにおける参考構成を示す。

(1) 必須構成

- Intel 64bit 拡張された x86 系 CPU を 1 基以上搭載していること。
- DDR3 1333 メモリ 4GB 以上の容量を有すること。
- システム領域用、ホーム領域用ストレージデバイスとして、500GB 以上の HDD を有すること。
- データ領域用ストレージデバイスとして、500GB 以上の HDD を有すること。同一のストレージデバイスをシステム領域用、データ領域用に共有しても良い。
- 1000BASE-T イーサネットインターフェースを 2 基以上有すること。
- VGA または DVI 出力を有すること。

(2) 推奨構成

- Intel 64bit 拡張された x86 系マルチコア CPU を 1 基以上搭載していること。動作周波数は 2.9GHz 以上であること。
- DDR3 1333 メモリ、12GB 以上の容量を有すること。
- システム領域用ストレージデバイスとして 500GB 以上の HDD、または SSD を有すること。
- データ領域用ストレージデバイスとして 160GB 以上の SSD 4 台以上から構

成される RAID 装置を有すること。

- HBA は RAID0, 1, 5, 6, 10, 50, 60, JBOD に対応すること。
- HBA と全 SSD はダイレクト接続されること。
- 1000BASE-T イーサネットインターフェースを 1 基有すること。
- 上記 1000BASE-T イーサネットインターフェースとは別に専用ポートにて IPMI 2.0 に対応したポートを 1 基有すること。
- 10Gbit Ethernet (10GBASE-T, SR, LR 等)イーサネットインターフェースを 1 基有すること。
- PXE によるネットワークブートが可能であること。
- VGA または DVI 出力を有すること。
- 19 インチラックに搭載可能であること。

(3) RENKEI-PoP 管理サーバ参考構成

CPU		Intel Corei7 965 Extreme (3.2GHz)
メモリ		12GB (DDR3 1333/2GB 6 枚構成)
ネットワーク インタフェース	1000BASE-T インターフェース	Realtek 8111C 2 ポート
	IPMI 2.0 専用インターフェース	Myricom 10GBASE-SR
ストレージ	システム領域用	1500GB
	データ量域用	SSD 32GB 8 基 HBA : Adaptec RAID 5085
筐体		ATX タワー mimiSAS ケーブルにてディスクエンクロ ージャと接続

4.2.2. ソフトウェア構成

- OS には x86_64 対応 CentOS 5.5 相当を使用すること。
- Globus Toolkit バージョン 4.2.1 以上の以下のコンポーネントを導入すること。
 - gsi, gridftp, data management, gsi-openssh, myproxy, proxy-utils
- gfarm バージョン 2.3.2 以上の以下のコンポーネントを導入すること
 - gdmd, client, gfarm2fs, gfarm_gridftp_dsi
- 以下のソフトウェアを導入すること
 - apache バージョン 2.2 以上
 - fuse
 - gxp バージョン 3.07 以上
 - iptables
 - OpenNebula バージョン 2.0.1 以上
 - openssh
 - ruby バージョン 1.8.7 以上

- sqlite バージョン 3.3 以上
- RENKEI-PoP 管理ツール群

4.3. VPN ゲートウェイサーバ

先端ソフトウェア運用基盤の分散開発環境ホスティングでは、VM が接続している SINET VPN に利用者がアクセスするためのサーバとなる VPN ゲートウェイサーバを必要とする。以下に VPN ゲートウェイサーバの構成仕様を示す。なお、ホスティング管理サービス実行サーバが VPN ゲートウェイサーバを兼ねても良い。

4.3.1. ハードウェア構成

以下に VPN ゲートウェイサーバのハードウェア必須構成と、推奨構成、RENKEI-PoP における参考構成を示す。

(1) 必須構成

- Intel 64bit 拡張された x86 系 CPU を 1 基以上搭載していること。
- DDR3 1333 メモリ 4GB 以上の容量をすること。
- システム領域用ストレージデバイスとして、500GB 以上の HDD を有すること。
- データ領域用ストレージデバイスとして、500GB 以上の HDD を有すること。同一のストレージデバイスをシステム領域用、データ領域用に共有しても良い。
- 1000BASE-T イーサネットインターフェースを 2 基以上有すること。
- VGA または DVI 出力を有すること。

(2) RENKEI-PoP 参考構成

RENKEI-PoP 管理サーバが VPN ゲートウェイサーバを兼ねる。構成は 4.2.1 (3)に示す通りである。

4.3.2. ソフトウェア構成

- OS には x86_64 対応 CentOS 5.5 相当を使用すること。
- Globus Toolkit バージョン 4.2.1 以上の以下のコンポーネントを導入すること。
 - gsi, gridftp, data management, gsi-openssh, myproxy, proxy-utils
- gfarm バージョン 2.3.2 以上の以下のコンポーネントを導入すること
 - client, gfarm2fs
- http proxy の機能を有すること
- 以下のソフトウェアを導入すること
 - fuse
 - iptables

- openssh

4.4. ネットワーク

先端ソフトウェア運用基盤の分散開発環境ホスティングで必要とするネットワーク環境を以下に示す。

(1) SINET VPN

- グローバル IP アドレスを持つ SINET VPN により多拠点接続されたネットワークセグメントであること。
- ホスティング管理サービス実行サーバはこのネットワークに接続すること。
- ホスティングサーバはこのネットワークに接続すること。
- ホスティングサーバ上の VM はこのネットワークに接続すること。
- ホスティングサーバ設置拠点ごとに二つ以上の IP アドレスを持つこと。
- VPN に接続しているサーバ・VM 間では全ポート通信可能であること。

(2) Internet Reachable Network

- グローバル IP アドレスを持つ Internet Reachable なネットワークセグメントであること。
- ホスティング管理サービス実行サーバはこのネットワークに接続すること。
- ホスティングサーバ、VM はともにこのネットワークに接続しても良い。
- 利用者のポート開放要求に対して応じられる運用体制を有すること。
- このネットワークは上記 SINET VPN と同一ネットワークセグメントとして提供しても良い。

4.5. 資源提供利用規則必須項目

先端ソフトウェア運用基盤は HPCI で新規に定義された資源であるため、管理拠点となるホスティング管理サービス提供拠点は以下に示す仕様の利用細則を有すること。

- 以下、全項目にて HPCI 利用細則に準拠すること。
- 先端ソフトウェア運用基盤を利用可能な利用目的が記載されていること。
- 先端ソフトウェア運用基盤の利用資格が記載されていること。
- 利用申請方法、継続申請方法が記載されていること。
- 利用者アカウント発行対象者、有効期限、失効基準が記載されていること。
- 先端ソフトウェア運用基盤利用者の責任範囲について記載されていること。
 - 特に、先端ソフトウェア運用基盤利用者が VM 上でサービスを構築した場合に、そのサービスの運用・管理責任は VM を所有するものに属することを明記すること。

5. ドキュメント&システム開発整備(発注仕様)

5.1. ユーザ利用手引き発注仕様

先端ソフトウェア運用基盤の利用者向けに、操作方法を記載した以下のマニュアルを作成すること。各操作方法是、「2 利用シナリオ」を参照のこと。

5.1.1. 先端ソフトウェア運用基盤利用の手引き

以下の内容をマニュアルに記載すること。操作例とその結果も記載すること。

- 概要
先端ソフトウェア運用基盤の概要を示す。
- ホスティング管理サービスへのログイン・ログアウト
- VM の起動
- VM のサスペンド
- VM のレジューム
- VM の状態保存
- VM の停止
- VM へのログイン・ログアウト
- OS イメージの登録
- OS イメージの取得
- OS イメージの削除
- OS イメージの作成方法
- 障害発生時対処

FAQ のありかや問い合わせ先メールアドレス、問い合わせフォーマットを記載する。

5.2. 資源提供運用手引き発注仕様

ホスティング管理サービスおよび VPN ゲートウェイサーバ、ホスティングサーバの管理者向けに、それぞれの運用法を記載した以下のマニュアルを作成すること。記述内容は「3.4 運用・保守」および「付録 1 運用・保守シナリオ」を参照のこと。

5.2.1. ホスティングサーバ運用の手引き

以下の内容をマニュアルに記載すること。操作例とその結果も記載すること。

- 概要
先端ソフトウェア運用基盤の概要を示す。
- ホスティングサーバ用ソフトウェアのインストール方法
- ホスティングサーバの起動／停止方法
- 仮想マシン設定手順
- 仮想マシンのホスティング管理サービスへの登録手順
- 障害発生時の対応手順
- セキュリティインシデント発生時の対応手順

5.2.2. ホスティング管理サービス実行サーバ運用の手引き

以下の内容をマニュアルに記載すること。操作例とその結果も記載すること。

- 概要
先端ソフトウェア運用基盤の概要を示す。
- ホスティング管理サービス用ソフトウェアのインストール方法
- ホスティング管理サービスの起動／停止方法
- ホスティングサーバ登録操作方法
- 利用者アカウント操作方法
- VM ホスティングのための情報登録方法
- 共有ストレージ操作方法
- ベース OS イメージ作成方法
- ベース OS イメージ登録方法
- VM 構成の作成・登録手順
- ホスト証明書更新手順
- CRL 更新手順
- ホスティング管理サービス状態保存 DB バックアップ手順
- ホスティング管理サービス状態保存 DB リカバリ手順
- 障害発生時の対応手順
- セキュリティインシデント発生時の対応手順

5.2.3. VPN ゲートウェイサーバ運用の手引き

以下の内容をマニュアルに記載すること。操作例とその結果も記載すること。

- 概要
先端ソフトウェア運用基盤の概要を示す。
- VPN ゲートウェイサーバ用ソフトウェアのインストール方法
- VPN ゲートウェイサーバの起動／停止方法
- 利用者アカウント操作方法
- ホスト証明書更新手順
- CRL 更新手順
- 障害発生時の対応手順
- セキュリティインシデント発生時の対応手順

5.2.4. ヘルプデスク運用の手引き

以下の内容をマニュアルに記載すること。

- 概要
先端ソフトウェア運用基盤の概要を示す。
- ヘルプデスク機能提供ソフトウェアのインストール・設定方法
- ヘルプデスク機能提供ソフトウェアの利用方法
- ヘルプデスク質疑応答データのアーカイブ方法

- ヘルプデスク質疑応答データのアーカイブからの検索方法

5.3. 利用細則発注仕様

以下の内容を記載した先端ソフトウェア運用基盤の利用細則を作成すること。

- 先端ソフトウェア運用基盤を利用可能な利用目的を列举
- 先端ソフトウェア運用基盤の利用資格を列举
- 利用申請方法

HPCI の利用申請に従うことを記述

- アカウント発行対象者
- アカウント有効期限
- アカウント継続申請方法
- アカウント失効基準

5.4. 導入手順書発注仕様

先端ソフトウェア運用基盤はホスティングサーバ、ホスティング管理サービス実行サーバ、VPN ゲートウェイサーバの3つのサーバから成る。これらのサーバの導入手順書を作成すること。

5.4.1. ホスティングサーバ導入手順書

以下の内容を記載したホスティングサーバ導入手順書を作成すること。

- 先端ソフトウェア運用基盤にホスティングサーバを接続する手順の概要
- 先端ソフトウェア運用基盤にホスティングサーバに接続する場合の制約事項
開放すべきポート等の条件を記載する。
- 設置場所・電源設備の確保
- ホスティングサーバの準備
 - ホスティングサーバに求められるハードウェア仕様
 - ホスティングサーバを運用するためにインストールすべきソフトウェア
 - ホスティングサーバを運用するために行うべき設定
- 先端ソフトウェア運用基盤にホスティングサーバを接続するために必要となるネットワークの準備
 - ネットワークへのホスティングサーバの接続とポートの開放
 - ホスティング管理サービス実行サーバとホスティングサーバの接続
- 接続と動作の確認
 - ホスティング管理サービス実行サーバからホスティングサーバ上に VM を生成し、プログラムを実行、停止、さらに VM の停止が行えることを確認する。
- 先端ソフトウェア運用基盤への参加
 - 先端ソフトウェア運用基盤への参加の通知
 - 先端ソフトウェア運用基盤上でのプログラムの実行確認
 - 導入完了の通知

5.4.2. ホスティング管理サービス実行サーバ導入手順書

以下の内容を記載したホスティング管理サービス実行サーバ導入手順書を作成すること。

- ・ ホスティング管理サービス実行サーバを導入する手順の概要
- ・ 先端ソフトウェア運用基盤にホスティング管理サービス実行サーバに接続する場合の制約事項
 - 既存のホスティング管理サービス実行サーバとの競合を未然に防ぐための条件等を記載する。
- ・ 設置場所・電源設備の確保
- ・ ホスティング管理サービス実行サーバの準備
 - － ホスティング管理サービス実行サーバに求められるハードウェア仕様
 - － ホスティング管理サービス実行サーバを運用するためにインストールすべきソフトウェア
 - － ホスティング管理サービス実行サーバに行うべき設定
- ・ 先端ソフトウェア運用基盤にホスティング管理サービス実行サーバを接続するために必要となるネットワークの準備
 - － ネットワークへのホスティング管理サービス実行サーバの接続とポートの開放
 - － ホスティング管理サービス実行サーバとホスティングサーバの接続
- ・ 接続と動作の確認
 - － ホスティング管理サービス実行サーバからホスティングサーバ上に **VM** を生成し、プログラムを実行、停止、さらに **VM** の停止が行えることを確認する。
- ・ 先端ソフトウェア運用基盤への参加
 - － 先端ソフトウェア運用基盤への参加の通知
 - － ホスティング管理サービス実行サーバ上での管理者権限の設定
 - － 先端ソフトウェア運用基盤上でのプログラムの実行確認
 - － 導入完了の通知

5.4.3. VPN ゲートウェイサーバ導入手順書

以下の内容を記載したホスティングサーバ導入手順書を作成すること。

- ・ VPN ゲートウェイサーバを導入する手順の概要
- ・ 先端ソフトウェア運用基盤に VPN ゲートウェイサーバを接続する場合の制約事項
- ・ 設置場所・電源設備の確保
- ・ ホスティング管理サービス実行サーバの準備
 - － VPN ゲートウェイサーバに求められるハードウェア仕様
 - － VPN ゲートウェイサーバを運用するためにインストールすべきソフトウェア
 - － VPN ゲートウェイサーバに行うべき設定
- ・ 先端ソフトウェア運用基盤に VPN ゲートウェイサーバを接続するために必要となるネットワークの準備
 - － ネットワークへの VPN ゲートウェイサーバの接続とポートの開放
- ・ 接続および動作の確認

VM への VPN 接続ができることを確認する。

- ・ 先端ソフトウェア運用基盤への参加
 - － 先端ソフトウェア運用基盤への参加の通知
 - － 先端ソフトウェア運用基盤上でのプログラムの実行確認
 - － 導入完了の通知

5.5. ヘルプデスク詳細設計発注仕様

以下の要員およびシステムを持つヘルプデスクの詳細設計を行うこと。

- ・ 利用者からの問い合わせをメールおよび Web で受け、回答を行う。
- ・ 問い合わせ内容および回答内容の記録を蓄積する。
- ・ 問い合わせに対して番号を採番し、問い合わせ状況(調査中/クローズ等の状況)の管理・検索ができるシステムを持つ (Request Tracker のようなチケット管理システムを想定)
- ・ 質問の多い内容を FAQ として公開する。

5.6. 実証評価用ソフトウェア発注仕様

平成 23 年度の先端ソフトウェア運用基盤、分散開発環境ホスティング機能の実証評価を行い、平成 24 年度以降のシステムにおいて運用時のテストを行うためのプログラム群を提供すること。

- ・ 動作確認テスト用プログラム
 - 以下の各種サーバ・サービスについて、動作確認を行うためのツールを提供すること。
このツールはシステム動作確認のために定期的に実行されうる。
 - － ホスティングサーバ
 - ◇ ホスティングサーバ上で VM を 1 つ以上実行するプログラムを提供すること。
 - － 共有ストレージ
 - ◇ データの新規書き込み、読み出しの確認をするプログラムを提供すること。
 - ◇ 対象ノードを指定した複製書き込みの確認をするプログラムを提供すること。
 - － ホスティング管理サービス
 - ◇ 各種 VM 操作の動作確認をするプログラムを提供すること。以下の機能について実装すること。
 - VM 起動
 - VM 停止
 - VM サスペンド
 - VM レジューム
 - VM スナップショット作成
 - VM 情報取得
 - OS イメージ登録
 - OS イメージ情報取得
 - OS イメージの公開・非公開設定
 - OS イメージ取得

- OS イメージ削除

- ・ 負荷テスト用プログラム

以下の各種サーバ・サービスについて、負荷テストを行うためのツールを提供すること。
このツールはサーバの調達、サービスへの組み込み時に性能ボトルネック解析を行うときなどに使われる。

- ホスティングサーバ

- ◇ 指定した数の VM を 1 つのホスティングサーバ上で実行するプログラムを提供すること。各 VM にて CPU、メモリを使い切る高負荷をかけるジョブを指定した時間実行する。ジョブとしては HPL を用いること。

- ◇ 指定した数の VM を 1 つのホスティングサーバ上で実行するプログラムを提供すること。各 VM にて、ランダムに IO を行うジョブを指定した時間実行する。ジョブとしては iozone ランダム R/W を用いること。

- ホスティング管理サービス

- ◇ ホスティング管理サービスが提供する機能ごとに、指定した数のクエリを同時発行するプログラムを提供すること。以下の機能について実装すること。

- VM 起動
 - VM 停止
 - VM サスペンド
 - VM レジューム
 - VM スナップショット作成
 - VM 情報取得
 - OS イメージ登録
 - OS イメージ情報取得
 - OS イメージの公開・非公開設定
 - OS イメージ取得
 - OS イメージ削除

- ・ セキュリティテスト用プログラム

以下の各種サーバについて、インターネット接続ネットワークセグメントにおいて、必要なポートのみ Open となっていることを確認するためのプログラムを提供すること。

- ホスティング管理サービス実行サーバ
 - VPN ゲートウェイサーバ

5.7. 追加仕様詳細調査検討のための役務発注仕様

平成 24 年度の前端ソフトウェア運用基盤追加仕様策定のため、分散開発環境ホスティング機能の追加機能について、以下の項目の技術的検討を行うこと。

- ・ 資源提供拠点供出リソースのクラスタ構成化についての調査検討
 - クラスタハードウェアの構成定義

平成 24 年度では本格運用のためにホスティング資源の追加が求められるため、拠点
供出資源のクラスタ構成を検討している。以下の項目について、定性的・定量的根拠
を付けて、必須ハードウェア構成、推奨構成の 2 種類を提示すること。

- ◇ VM ホスティング用サーバの CPU、メモリ、ローカルディスクについての種類、
および、量
- ◇ クラスタ内部結合網のネットワーク機器の種類、帯域
- ◇ クラスタと外部ネットワーク接続用機材の種類、およびルーティング・ファイア
ウォール等の要求機能
- ◇ クラスタローカルの共有ストレージ構成

－ クラスタ内部ネットワーク、および外部接続ネットワークの論理構成設計

拠点資源をクラスタ構成とした場合、各ホスティングサーバへの VM 操作命令を送出
する管理ネットワークは、クラスタのフロントエンドサーバを除き、プライベートネ
ットワークにすることを検討している。また、利用者ごとのネットワークセグメント
分断、VM が各種外部ネットワークに接続できる環境の提供を検討している。そのた
めには VLAN 等でネットワークを論理的に分割することが必要となり、また、帯域保
証が求められるだろう。以下の種類のネットワークについて、上記ネットワークハー
ドウェアを用いた論理構成についての調査検討を行うこと。

- ◇ クラスタ内ホスティングサーバの管理ネットワーク構成
- ◇ クラスタローカル共有ストレージ用ネットワーク構成
- ◇ 拠点内 VM 間通信用ネットワーク構成
- ◇ 拠点間 VM 間通信用ネットワーク構成

－ クラスタソフトウェアの構成定義

クラスタ構成にすることにより、単一のホスティングサーバでの構成に加えて追加で
必要となるソフトウェア項目について調査検討、推奨構成を提示すること。

－ VM 配置スケジューラの機能

拠点ごとのホスティング用資源をクラスタ構成にすることにより、平成 23 年度実験
システムで想定している、全ホスティングサーバがネットワーク的にフラットに配置
されている構成を対象とした VM 配置スケジューリングポリシーへの変更が必要となる
可能性もある。上記ハードウェア・ネットワーク環境上で要求される VM 配置スケ
ジューリングについての要件の調査検討を行うこと。

- ホスティング管理サービスの構成定義

VM 配置スケジューラも含め、プライベートネットワーク構成となり得るホスティング用クラスタが拠点資源として供出されるので、その構成に対応したホスティング管理サービスの構成について調査検討を行うこと。ホスティング管理サービスの構成としては以下が考えられるが、それぞれについて、平成 23 年度実験システムからへの追加機能項目を調査すること。

- ◇ 管理サービスから直に個々のホスティングサーバに対して VM 操作を要求（フラットモデル）
- ◇ ホスティング管理サービスからの VM 操作要求を個々のホスティングサーバに転送する、管理サービスのサブコンポーネントを拠点ごとに配置（階層型モデル）

- ・ VM 用ネットワーク環境についての調査検討

- VM へのプライベート IP アドレス割当て

利用者の増加に伴い、グローバル IP アドレスの消費削減のために、グローバル IP アドレスが不要なサーバにはプライベート IP アドレスのみを割り振るシステムとして構成する必要がある。これにより、1 拠点内部で複数 VM を実行する場合、プライベート IP アドレスを割り当てた VM クラスタとして構成可能である。実現のためにはグローバル IP とプライベート IP の両方を持つマルチホーム VM や、ポートフォワードが構成できる必要がある。仮想ルータや、仮想スイッチによる実現可能性、構成方法の調査検討を行うこと。

- 申請課題ごとの VM ネットワークの分断機能

セキュリティ向上、およびブロードキャストのドメイン分割のため、特にプライベート IP アドレスが割り振られた VM クラスタの場合、申請課題ごとの VM ネットワークの分断が機能として求められる。仮想ルータや、仮想スイッチによる実現可能性、構成方法の調査検討を行うこと。

- Internet Reachable ネットワークを VM ネットワークに使用

利用者の VM アクセスの利便性を考慮すると、SINET VPN ではなく、Internet Reachable ネットワークの IP アドレスを VM に割り振る方が良い。この場合に要求されるファイアウォール、IDS のセキュリティモデルの調査検討を行うこと。

- IPv6 対応

先端ソフトウェア運用基盤として、IPv6 対応ソフトウェアの研究開発を希望する課題申請が想定される。IPv6 対応 VM を提供するために必要な VM、ホスティングサーバ、ホスティング管理サービスに求められる追加機能の調査検討を行うこと。

- ・ Web GUI 開発についての調査検討

利用者の利便性向上のため、最低限 VM、OS イメージ操作に関する Web GUI を備えた利用者用インターフェースの提供を検討している。Web GUI で提供すべき機能の精査、実装方法についての調査検討を行うこと。

- ・ 提供すべき Pre-Configured OS イメージの調査

研究者の利用環境を迅速に構築するために、Web サーバ機能、CMS サーバ機能、データベース機能等を実現するためのソフトウェアが予め導入された VM 用の OS イメージの提供を検討している。提供すべき OS イメージの種類の調査を行うこと。

5.8. 追加仕様開発発注仕様

「5.7 追加仕様詳細調査検討のための役務発注仕様」の発注成果物を元に、必要機能を追加実装するための仕様書を作成すること。

6. 整備計画

先端ソフトウェア運用基盤の整備計画を「表 3 先端ソフトウェア運用基盤整備計画」に示す。

表 3 先端ソフトウェア運用基盤整備計画

	H23/1Q	2Q	3Q	4Q	H24/1Q	2Q	3Q	4Q
マイルストーン	>-----▽H23 試験運用仕様検討		>-----▽試験環境整備		>-----実証評価運用-----▽			> 本運用
基本仕様			>-----▽ドキュメント整備		>-----▽試験環境整備			
					>-----実証評価運用-----▽			
					>-----▽追加仕様詳細検討			
追加仕様			実証評価ソフトウェア開発 >-----▽					
			追加仕様開発(1, 2)>-----▽					
			ヘルプデスク仕様策定 >-----▽					
					ドキュメント修正 >-----▽			
					課金検討 >-----▽			
					運用環境整備 >-----▽			
								> 本運用
			追加仕様開発(3, 4)・ドキュメント作成（順次導入）>-----					

6.1. 平成 23 年度実施項目

まず基本仕様の実施について述べる。「ドキュメント整備」として、5.1 ～ 5.4 に示す各種書類を作成する。「試験環境整備」として、参加機関を募り、作成されたドキュメントを基に環境を構築する。平成 24 年第 1 クオータ以降に「実証評価運用」を行う。

平成 24 年度以降の本格運用のための追加仕様として、「追加仕様詳細検討」として、5.7 に示す仕様の調査検討を平成 23 年第 4 クオータから平成 24 年第 1 クオータにかけて行う。

6.2. 平成 24 年度実施項目

実証評価、および本格運用時の動作検証用に用いるソフトウェア群を 5.6 に仕様を示す「実証評価ソフトウェア開発」として開発を行う。平行して、追加仕様で記述した内容の開発、整備を行う。表 3 の「追加仕様開発(1,2)」として、詳細検討の結果作成した仕様書を元に、主に 3.5.1 (1) 資源提供拠点供出リソースのクラスタ構成、(2) VM 用ネットワーク環境の構成変更に記述した内容を実現するソフトウェアの開発を行う。

平成 24 年度秋（第 4 クオータを想定）以降の本格運用のため、「ヘルプデスク仕様策定」として、5.5 に示す仕様に従いヘルプデスク仕様策定を行う。「ドキュメント修正」として、「追加仕様開発(1,2)」の成果物を導入した環境利用・管理のために、各種書類（5.1 ～ 5.4 に相当）を更新

する。「課金検討」として先端ソフトウェア運用基盤の課金方針についての検討を行う。「ヘルプデスク仕様策定」で策定したヘルプデスクの構築も含め「運用環境整備」を行い、「本運用」を開始する。

6.3. 平成 24 年度後半 ～ 平成 25 年度実施項目

表 3 の「追加仕様開発(3, 4)・ドキュメント作成」として、平成 23 年度実施項目の「追加仕様詳細検討」の結果作成した仕様書を元に、主に 3.5.1 (3) Web GUI 環境の提供、(4) Pre-Configured OS イメージの提供に記述した内容を実現するソフトウェアの開発を行う。開発成果物は順次運用環境に導入し、必要なドキュメントも随時更新する。

7. 必要経費

ドキュメント整備、資源供出、運用・保守に関する経費について参考見積りをベースに記載する。

7.1. ドキュメント整備費用

5.1～5.5 に示した資料を作成するための費用の概算値を表 4 に示す。平成 23 年度の費用は 5 章に示した資料の内容からドキュメントのページ数を求め、ページ単価を乗じることによって算出した。ドキュメントの内容に依存する要素もあるが、250 ページ程度のマニュアルを作成する予定である。平成 24 年度は平成 23 年度に作成したドキュメントを改版する費用を見積もった。

7.2. 実証評価用ソフトウェア開発費用

5.6 に示した実証評価ソフトウェアを平成 24 年度に開発完了させる。この開発費用の概算値を表 4 に示す。

7.3. 追加仕様検討費用

3.5 に示した追加機能について、機能を実現するための方式に関する調査と、方式の比較検討を行う。検討に基づき基本仕様を策定する。調査と基本仕様書の作成のために必要とする開発費の概算値を表 4 に示す。

7.4. 追加仕様開発費

平成 24 年度の本格運用に向けて、平成 24 年度に 3.5 に示した追加機能の開発が必要となる。7.3 で作成する追加仕様検討結果にもとづき、この機能の開発のために必要とする開発費の概算値を表 4 に示す。本格運用開始以降の実現でも十分な追加機能分については、平成 25 年度以降の開発・導入を行うとし、この費用を見積もった。

7.5. 資源整備費用

平成 23 年度にテスト環境（VPN ゲートウェイサーバを兼ねるホスティング管理サービス実行サーバ）を構築するために計算機資源の整備が必要である。この資源を整備するために必要とする費用の概算値を表 4 に示す。なお平成 24 年度以降は実運用で使用するサーバ数に応じた資源整備費用が発生する。具体的な構成は平成 23 年度の試験運用を元に策定するが、負荷分散・耐故障性向上のために冗長構成、DB 機能の分割が求められることを想定すると、最低でもサーバ 4 台、サーバ間を接続するための 10Gbit Ethernet スイッチ 1 台が必要になり、1,000 万円の費用が発生すると考えられる。

7.6. 運用・保守費用

テスト環境を運用するために必要とする保守・運用費用の概算値を表 4 に示す。平成 23 年度は 7.5 で調達したシステムの保守費用を 1 件/3 ヶ月として算出した。平成 24 年度以降にはホスティング管理サービスおよび VPN ゲートウェイサーバの管理者 1 名の人件費が発生し、年間 1,500 万円の費用が発生する。

表 4 必要経費一覧(単位:千円)

費用項目	金額		
	平成 23 年度	平成 24 年度	平成 25 年度
ドキュメント整備費用	4,612	5,000	—
実証評価用ソフトウェア開発費用	—	20,000	—
追加仕様検討費用	4,612	5,000	—
追加仕様開発費用	—	39,000	5,000
資源整備費用	2,767 (1 ノード分)	平成 23 年度に明らかにする	
運用・保守費用	3,459	15,000	15,000
合計	15,450	84,000	20,000

[付録]

1. 運用・保守シナリオ

本編にて提示していない運用・保守のシナリオを付録としてここに示す。

1.1. ホスティングサーバおよび仮想マシン登録フロー

資源提供機関が持つサーバリソースをホスティングサーバとして登録する際のシナリオを「図 9 仮想マシン登録フロー」に示す（ただし、ハードウェアの設置や、OS およびネットワークの設定、必要ソフトウェアのインストールは割愛する）。

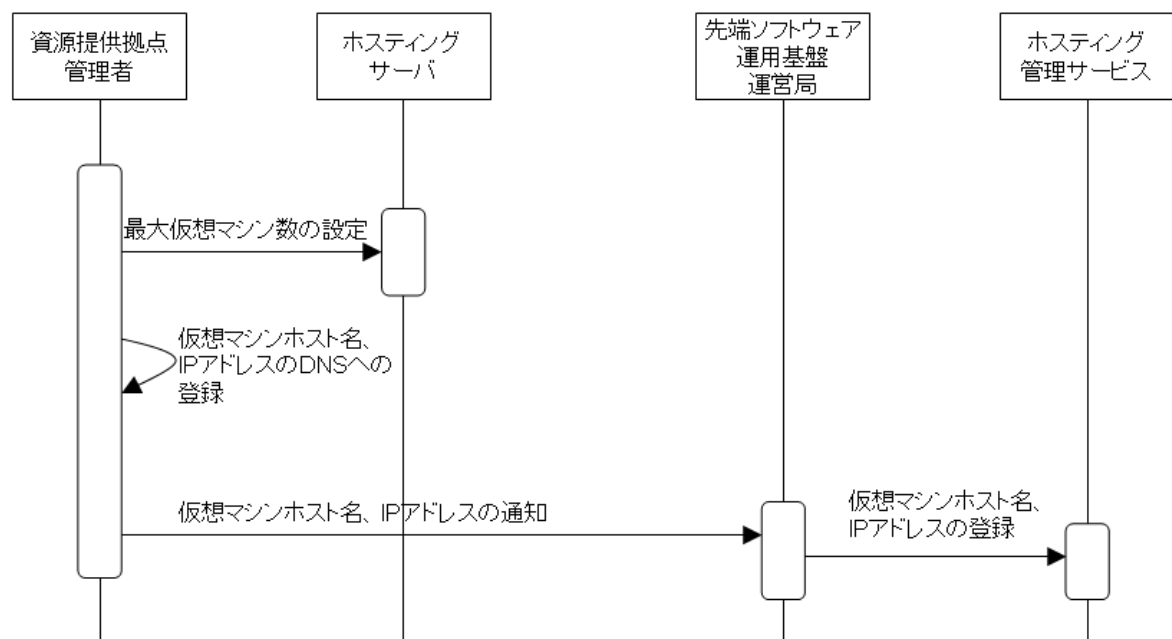


図 9 仮想マシン登録フロー

資源提供拠点管理者は、ホスティングサーバ上で動作させる最大仮想マシン数を定めホスティングサーバに設定する。さらに各仮想マシンのホスト名・IP アドレスをそれぞれの資源提供機関で運営している DNS サーバに登録する（実際には DNS 管理者に登録を依頼する）。登録したホスト名が参照可能になれば、資源提供拠点管理者は先端ソフトウェア運用基盤運営局に各仮想マシンのホスト名・IP アドレスを通知する。通知を受けた先端ソフトウェア運用基盤運営局は、通知された仮想マシンのホスト名・IP アドレスをホスティング管理サービスに登録する。

1.2. 障害フロー

1.2.1. ホスティング管理サービス実行サーバでの障害発生・保守フロー

ホスティング管理サービスの動作しているサーバでの障害発生およびサーバ保守実施時のフローを「図 10 ホスティング管理サービス実行サーバ障害・保守フロー」に示す。

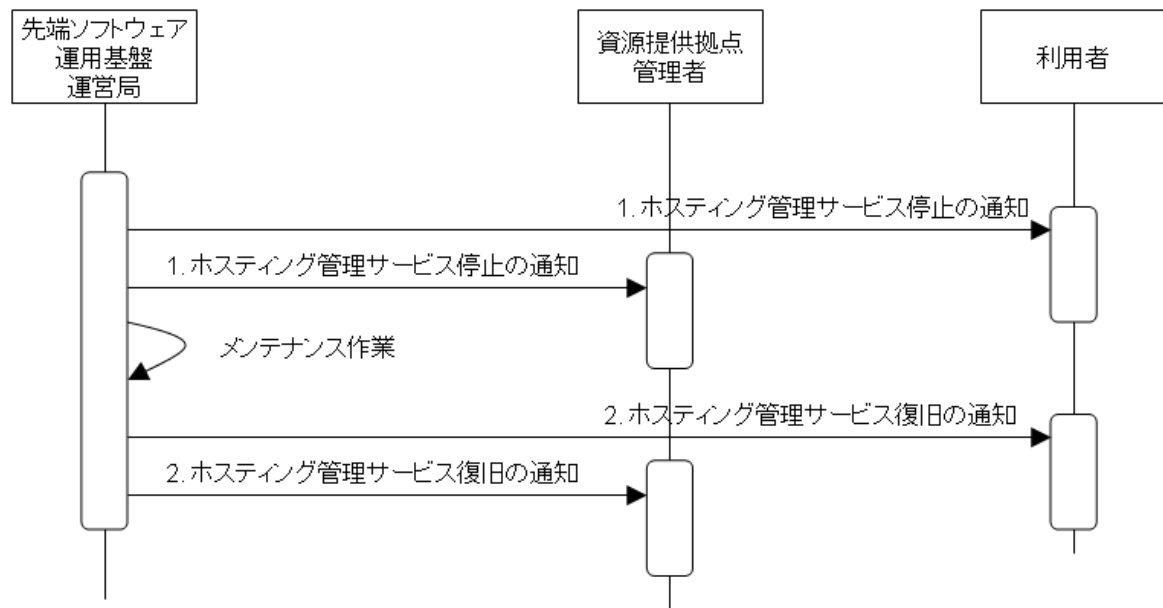


図 10 ホスティング管理サービス実行サーバ障害・保守フロー

ホスティング管理サービスが動作しているサーバで障害が発生した場合あるいはサーバの定期保守を行う場合、先端ソフトウェア運用基盤運営局は、分散開発環境ホスティング機能の全利用者および全資源提供拠点管理者に対し、ホスティング管理サービスが利用不可であることを通知する（1. ホスティング管理サービス停止の通知）。通知はメールでの連絡あるいはポータルでのアナウンスによって行う。

障害からの復旧あるいは保守作業終了後に、先端ソフトウェア運用基盤運営局は、ホスティング管理サービスが復旧したことを通知する（2. ホスティング管理サービス復旧の通知）

1.2.2. ホスティングサーバでの障害発生・保守フロー

資源提供機関から提供されたリソースのうちで分散開発環境ホスティング機能にてホスティングサーバとして使用しているサーバでの障害発生およびサーバ定期保守実施時のフローを「図 11 ホスティングサーバ障害発生・保守フロー」に示す。

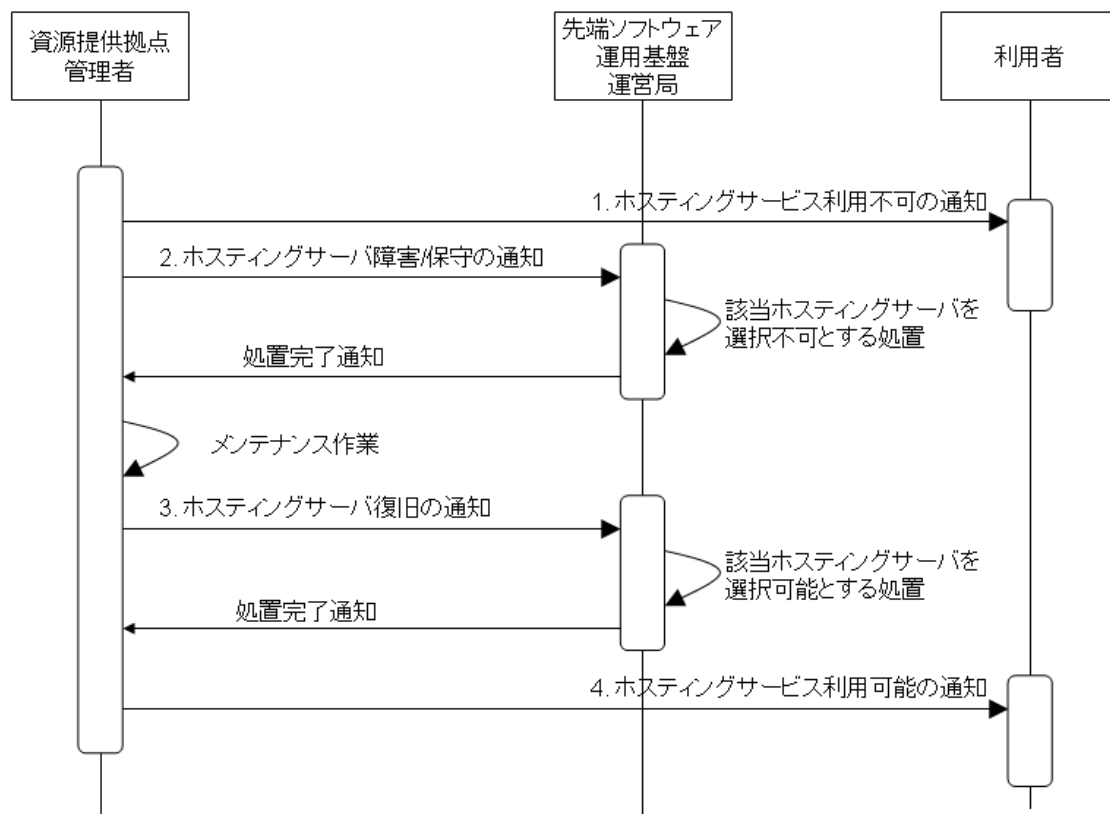


図 11 ホスティングサーバ障害発生・保守フロー

保守対象あるいは障害の発生したホスティングサーバの管理者（資源提供拠点管理者）は、該当サーバ上に存在する仮想マシンの利用者（VM ホスティングサービス利用者）にホスティングサービスが利用できないことを通知する（1. ホスティングサービス利用不可の通知）。さらに、先端ソフトウェア運用基盤運営局に該当ホスティングサーバで障害発生あるいは保守を行うことを通知し（2. ホスティングサーバ障害/保守の通知）、利用者がホスティング管理サービスから該当ホスティングサーバを選択できないようにしてもらう。

障害からの復旧あるいは保守作業終了後に、資源提供拠点管理者は先端ソフトウェア運用基盤運営局に該当ホスティングサーバが復旧したことを通知し（3. ホスティングサーバ復旧の通知）、利用者がホスティング管理サービスから該当ホスティングサーバを選択できるようにしてもらう。さらに、該当サーバ上の VM ホスティングサービス利用者に対しホスティングサービスが利用可能になったことを通知する（4. ホスティングサービス利用不可の通知）。

1.2.3. OS イメージの存在する共有ストレージでの障害発生時フロー

共有ストレージで障害が発生した場合、ほとんどはハードウェア側で障害を検出し復旧処置がとられるが、共有ストレージ管理用ソフトウェア（平成 23 年度の実証実験では **gfarm** を想定）での調査/復旧作業も必要となる場合がある。ストレージ管理用ソフトウェア上での調査/復旧には、ストレージ管理者と先端ソフトウェア運用基盤運営局が協力して作業を進める必要がある。

「図 12 共有ストレージ障害フロー」にストレージ管理ソフト上での調査/復旧の必要な共有ストレージ障害フローを示す。

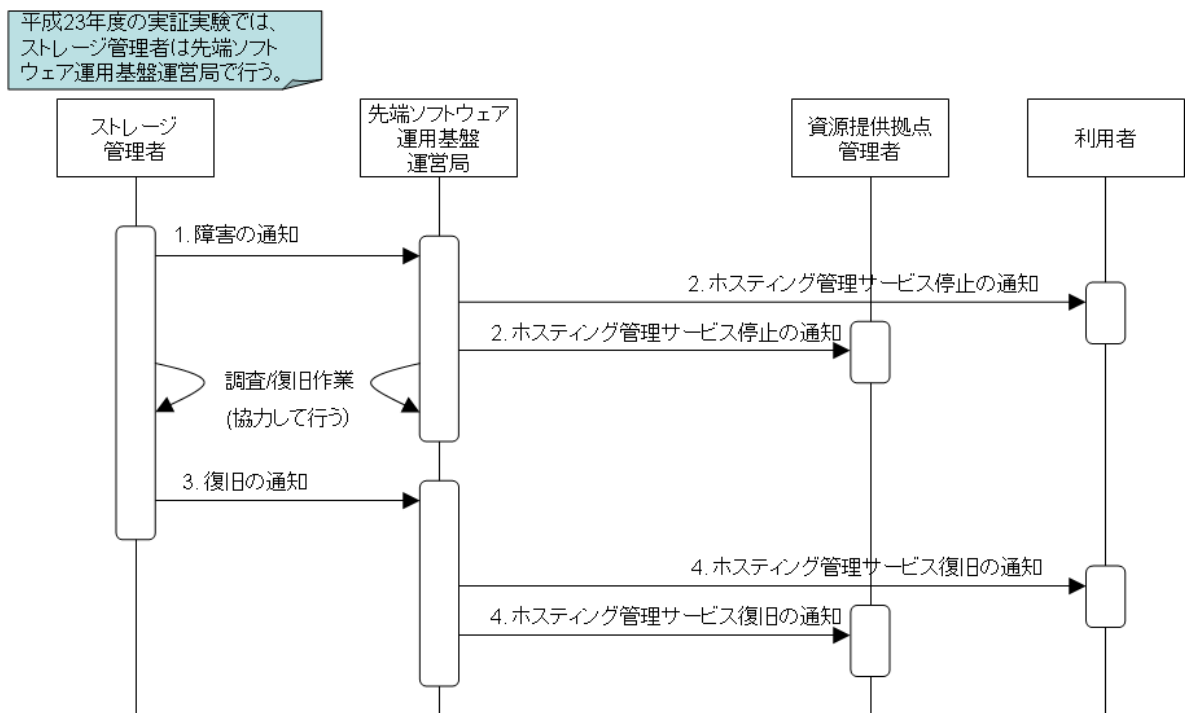


図 12 共有ストレージ障害フロー

先端ソフトウェア運用基盤運営局はストレージ管理者から障害を通知される(1. 障害の通知)と、共有ストレージの障害によりホスティング管理サービスが使用できないことを資源提供拠点管理者と利用者に通知する(2. ホスティング管理サービス停止の通知)。その後にストレージ管理者と協力して障害の原因/影響を調査し復旧作業を行う。ストレージ復旧の連絡を受けると(3. 復旧の通知)、先端ソフトウェア運用基盤運営局は、サービス再開の通知を資源提供拠点管理者と利用者に通知する(4. ホスティング管理サービス復旧の通知)。

1.2.4. 仮想マシン動作環境での障害発生・保守フロー

仮想マシン環境で使用するネットワークの保守など、特定の仮想マシン動作環境に関連する保守および障害発生時のフローを「図 13 仮想マシン動作環境での障害発生・保守フロー」に示す。

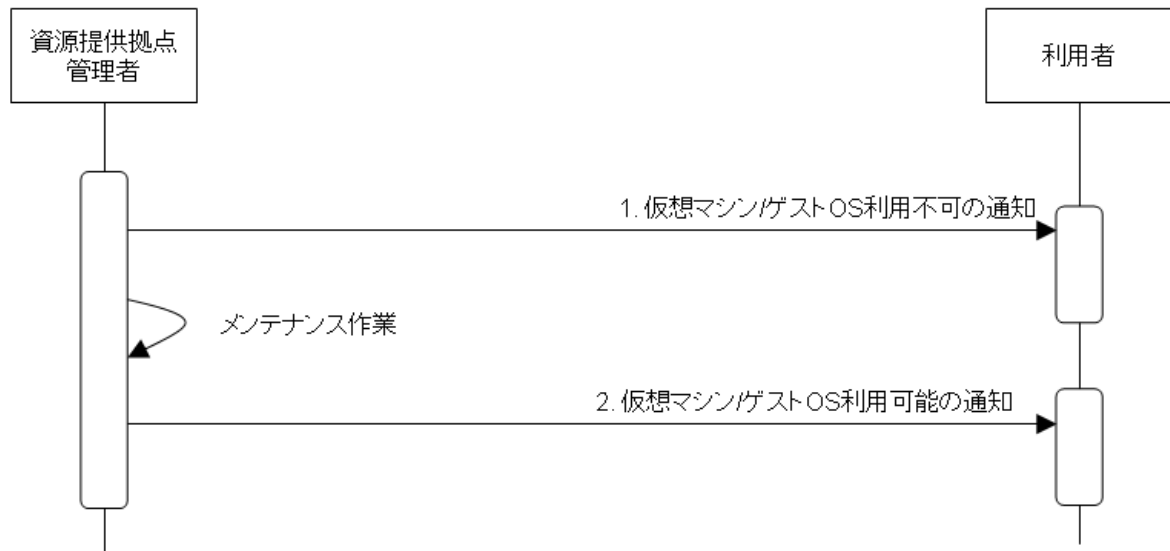


図 13 仮想マシン動作環境での障害発生・保守フロー

保守あるいは障害発生時に、資源提供拠点管理者は該当 VM ホスティングサービス利用者に対し仮想マシンあるいは仮想マシン上のゲスト OS を使用できないことを通知する(1. 仮想マシン/ゲスト OS 利用不可の通知)。

障害からの復旧あるいは保守作業終了後に、資源提供拠点管理者は該当 VM ホスティングサービス利用者に対し仮想マシンあるいは仮想マシン上のゲスト OS が使用可能となったことを通知する(2. 仮想マシン/ゲスト OS 利用可能の通知)。

1.2.5. ホスティングサーバでのセキュリティインシデント発覚時フロー

分散開発環境ホスティング機能で使用しているホスティングサーバに対するセキュリティインシデントが発覚した場合のフローを「図 14 ホスティングサーバでのセキュリティインシデント発覚時フロー」に示す。

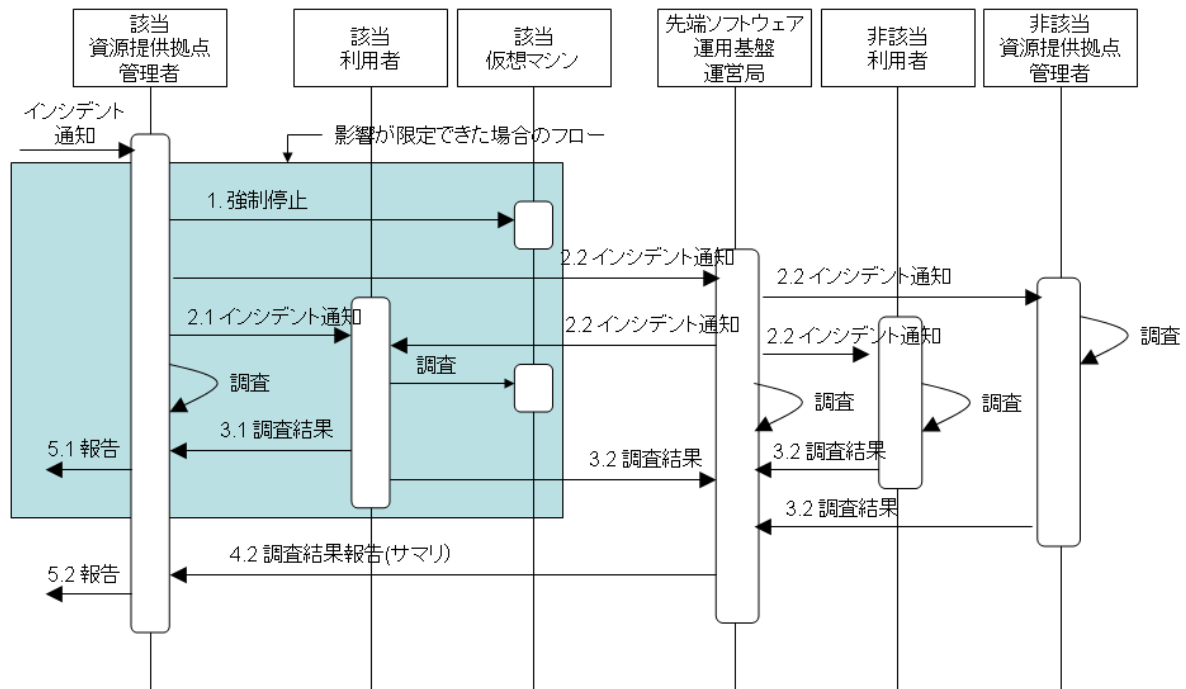


図 14 ホスティングサーバでのセキュリティインシデント発覚時フロー

セキュリティインシデント発生のお知らせを受けた資源提供拠点管理者は、インシデントに該当するサービスを運用/使用している仮想マシンを強制停止させ(1. 強制停止)、その仮想マシンの利用者(VM ホスティングサービス利用者)に対しインシデント発生を通知する(2.1 インシデント通知)。通知を受けた利用者は該当仮想マシン上での調査を行い、結果を資源提供拠点管理者に報告する(3.1 調査結果)。資源提供拠点管理者は、ホスティングサーバに対する調査を行い、該当利用者からの調査結果と合わせて資源提供機関のしかるべき部門に報告する(5.1 報告)。

インシデントの内容が他のホスティングサーバにも影響する場合、資源提供拠点管理者は先端ソフトウェア運用基盤運営局に対しセキュリティインシデント発生を通知し(2.2 インシデント通知)調査を依頼する。通知を受けた先端ソフトウェア運用基盤運営局は、他の資源提供拠点管理者および分散開発環境ホスティングの全利用者に対しインシデント発生を通知し(2.2 インシデント通知)、調査を依頼する。個々の利用者および資源提供拠点管理者は調査を行い、結果を先端ソフトウェア運用基盤運営局に報告する(3.2 調査結果)。先端ソフトウェア運用基盤運営局はそれぞれの調査結果を取りまとめ、インシデントの発生した資源提供拠点管理者に報告する(4.2 調査結果報告(サマリ))。当該資源提供拠点管理者は自サーバでの調査結果と合わせて資源提供機関のしかるべき部門に報告する(5.2 報告)。

2. 調査結果

2.1. 現状情報基盤センター群ネットワーク機能設定状況

先端ソフトウェア運用基盤、分散開発環境ホスティング機能で必要となるネットワーク機能について、各情報基盤センターの状況を調査した。結果を以下に示す。

(1) ファイアウォール設定

	解除可	個別設定	解除不可
ネットワークセグメントごと、あるいはIPアドレスごとの個別のファイアウォール設定変更	4 拠点	4 拠点	1 拠点

	可能	可能 (審査付)	不可
送信元ネットワークを絞れば、1025 番以上のポート宛の任意の受信を許可する設定が可能	6 拠点	2 拠点	0
送信元ネットワークを絞れば、Well Known Port への受信を許可する設定が可能	6 拠点	2 拠点	0
任意の送信元からの、一部の Well Known Port(ssh, http, https などごく少数)への受信を許可する設定が可能	6 拠点	2 拠点	0
宛先ネットワークを絞れば、1025 番以上のポート宛の任意の送信を許可する設定が可能	7 拠点	1 拠点	0
宛先ネットワークを絞れば、一部の Well Known Port(ssh, http, https, dns, ntp)宛の送信を許可する設定が可能	7 拠点	1 拠点	0

(2) 検知フィルタ設定

	導入	未導入
P2P 検知、ポートスキャン検知等の検知フィルタサービスの有無	8 拠点	1 拠点

	解除可	個別対応	解除不可
検知フィルタの解除可否	2 拠点	4 拠点	2 拠点

(3) DNS 登録

	可	不可
DNS 逆引き登録への対応状況	8 拠点	1 拠点
拠点所有サーバの IP アドレスを、学外管理の DNS サーバ(xxx.hpci.jp など)に登録ことの可否(運用上許可されているか)	6 拠点	3 拠点

(4) IPv6 対応状況

	対応	対応予定	未対応
IPv6 への対応状況	3 拠点	1 拠点	5 拠点

2.2. 現状情報基盤センター群ホスティングサービス提供状況

各情報基盤センターに対し、ホスティングサービスおよび WEB 等のサービス提供状況を調査

した。結果を以下に示す。

(1) サービス提供状況

サービス	提供拠点数	総利用者数
VM ホスティング	4	136
実機ホスティング	1	68
Web・メールサービス	4	319
DNS 登録サービス	1	214

(2) サービス提供対象

学内利用者にも提供	5 拠点
学外利用者にも提供	1 拠点

(3) サービス内容詳細

ホスティングサービス

- サイト B
 - － 利用者による OS・ソフトウェア等の選択が可能、自由管理（～8 コア、～16GB メモリ、～500GB ディスク）
- サイト D
 - － Vmware vSphere による、仮想マシンによるホスティングサービス。
 - － 学内業務システムや各種研究プロジェクト共用サーバとして利用（2 コア、～4GB メモリ、～数 TB ディスク）
- サイト E
 - － サーバ 1 台占有型の利用
 - － ホスティングサーバ：root 権限はセンターが所有し、HDE Controllerにより利用者がサーバ運用を行う
 - － プロジェクトサーバ：root 権限を利用者に与える
- サイト F
 - － 汎用コンピュータとして、スパコンとは独立した運用。
 - － 占有 VM を提供。2 コア、2GB メモリ、200GB ディスク
 - － 利用者へ root 権限を付与
- サイト G
 - － Xenserver による仮想専用サーバホスティングサービス（平成 23 年 4 月から提供開始予定）
 - － 1 CPU、～4GB メモリ、～100GB ディスク、これを越える場合別途相談

Web・メールサービス

- サイト A
 - － HDS コントローラを使って Web・メールホスティング環境を提供

- サイト B
 - － Web ホスティングサービス（試行）
- サイト D
 - － DNS(コンテンツ) サーバ代行サービス
 - － センターが管理する DNS サーバに、利用者が管理するサーバの DNS 情報を登録するサービス
 - － 利用者用 Web インターフェースが提供されており、A,CN,NX,NS レコードの編集が可能
- サイト F
 - － ホームページサービス、独自ドメイン名でのホームページの公開とメール転送環境を提供
- サイト G
 - － Web コンテンツの公開スペースを提供

3. 用語集

[1] HPCI 事務局

HPCI 利用の課題審査を行う組織

[2] 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）

[3] 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

[4] 分散開発環境ホスティング

地理的に分散したサーバ上で、利用者の要求に応じて必要な場所に必要な数の仮想マシンを実行し、それらから構成される開発環境を提供するサービス。OS への root 権限、グローバル IP アドレスが付与されるため、OS の研究や、分散システムの研究などコンピュータサイエンスの研究支援環境としての利活用を想定している。

[5] RENKEI-PoP

RENKEI プロジェクト (<http://www.e-sciren.org/>) にて配備運用を進めている仮想マシン実行機能を持つストレージサーバ。拠点スパコン間のデータ転送支援、グリッド技術を利用したリソース連携サービスのホスティングを行う。

[6] ホスティング管理サービス

利用者からの VM・OS イメージ操作を受け付け、ホスティングサーバに対して VM 操作命令を発行する。システム内で唯一の存在。

[7] ホスティング管理サービス状態保存 DB

ホスティング管理サービスが持つデータベース。VM 構成情報、OS イメージ情報、ネットワーク情報、VM 稼働時間等を記録する。

- [8] ホスティング管理サービス実行サーバ
 ホスティング管理サービスを実行するサーバ
- [9] ホスティングサーバ
 VM を実行するサーバ。資源提供先機関に最低 1 台設置
- [10] VPN ゲートウェイサーバ
 VPN により構成される仮想マシンネットワークへのゲートウェイ
- [11] 共有ストレージ
 ホスティングサーバ間での OS イメージ共有を実現する広域分散ストレージ
- [12] OS イメージ
 VM 実行時に使用される任意の OS が導入されているディスクイメージ。
- [13] 先端ソフトウェア運用基盤運営局
 先端ソフトウェア運用基盤の運営を行い、ホスティング管理サービスおよびホスティング管理サービス実行サーバ、VPN ゲートウェイサーバの運用・保守を担う組織および担当者
- [14] 資源提供拠点管理者
 資源提供機関から提供されたホスティングサーバの運用・保守を担う管理者

HPCI 基本仕様

— 認証基盤に関する基本仕様 —

目次

1	概要	4
2	利用シナリオ	5
2.1	認証と認可	5
2.2	認証基盤利用シナリオ概要.....	5
2.2.1	ユーザ視点での利用シナリオ.....	6
2.2.2	運用者視点での利用シナリオ.....	8
2.3	平成 23 年度利用シナリオ	11
2.3.1	クライアント証明書取得.....	11
2.3.2	シングルサインオン	12
3	認証基盤構築・運用基本仕様	13
3.1	必要要件およびアーキテクチャ概要.....	13
3.1.1	必要要件.....	13
3.1.2	認証基盤構築の方針	14
3.1.3	ユーザ認証アーキテクチャ	14
3.1.4	平成 23 年度認証基盤.....	15
3.2	平成 23 年度認証基盤アーキテクチャ.....	15
3.2.1	運用機関.....	16
3.2.2	ソフトウェアアーキテクチャ.....	16
3.2.3	HPCI 事務局との連携.....	19
3.2.4	ユーザ仕様.....	20
3.2.5	クライアント証明書取得.....	20
3.2.6	シングルサインオン	20
3.3	認証局運用機関仕様.....	21
3.3.1	認証局システム.....	22
3.3.2	証明書管理システム	32
3.3.3	Shibboleth DS.....	35
3.3.4	運用.....	37
3.4	認証ポータル運用機関仕様.....	38
3.4.1	認証ポータル	39
3.4.2	Proxy 証明書リポジトリ	42
3.4.3	運用.....	44

3.5	HPCI アカウント IdP 運用機関仕様	45
3.5.1	HPCI アカウント IdP	46
3.5.2	運用	49
3.6	資源提供機関仕様	50
3.6.1	GSI-SSH	52
3.6.2	Gfarm	54
3.6.3	grid-mapfile 自動生成ツール	54
3.6.4	運用	54
3.7	今後の検討課題	55
3.7.1	シナリオ検討	55
3.7.2	クライアント証明書発行	56
3.7.3	簡易ファイルアクセスのための認証基盤アーキテクチャ	56
3.7.4	グループ管理	56
4	ドキュメント&システム開発整備(発注仕様)	56
4.1	認証基盤導入および運用手引き仕様	56
4.1.1	認証局運用機関におけるシステムおよびドキュメント整備に関する仕様	57
4.1.2	認証ポータル運用機関におけるドキュメント整備に関する仕様	59
4.1.3	HPCI アカウント IdP 運用機関におけるドキュメント整備に関する仕様	61
4.1.4	資源提供機関におけるドキュメント整備に関する仕様	62
4.2	システム開発仕様	62
4.2.1	認証ポータル開発仕様	62
4.2.2	証明書管理システム開発仕様	64
5	整備計画	65
6	必要経費	66
1	利用 TCP ポート・UDP ポート	69
1.1	認証基盤において利用される通信ポート	69
1.1.1	認証局運用機関における利用ポート	71
1.1.2	認証ポータル運用機関における利用ポート	71
1.1.3	HPCI アカウント IdP 運用機関における利用ポート	71
1.1.4	資源提供機関における利用ポート	71
2	調査結果	71
2.1	情報基盤センター群グループ管理	71
3	用語集	74

1 概要

本基本仕様書は、HPCI における認証基盤の基本仕様を定めている。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 認証基盤の整備に必要な機能を明確にし、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。

・ 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

認証基盤では、HPCI 上の資源を利用するユーザの認証および認可のためのサービスを提供する。本節では、HPCI 上の資源を利用するための認証サービスを提供する認証基盤の利用シナリオを定義する。以後、本節では、ユーザが事前に HPCI を利用するためのアカウントを取得していることを前提とする。アカウント取得に関わるシナリオについては、ユーザ管理支援編で説明している。

HPCI 上の資源提供機関やユーザコミュニティは多岐にわたることが予想される。これらの組織やコミュニティでは、既存の計算機システム等を利用するために既に認証基盤が運用されている場合が多く、ユーザの視点では、現在利用しているシステムと同様の認証方法で HPCI 上の資源を利用できることが望ましい。そのため、本仕様では、HPCI 上でニーズが想定される認証基盤について複数の利用シナリオを想定するとともに、このうち平成 23 年度に運用を開始することが可能なシナリオについて平成 23 年度利用シナリオとして詳細を検討した。残りの利用シナリオについては、平成 23 年度以降に詳細を検討する予定である。

2.1 認証と認可

ユーザは、HPCI 上の資源を利用するためにその資源にアクセスするためには、アクセスするユーザの本人性を証明する処理を行う必要がある。この処理を「認証」と呼ぶ。認証は、ユーザが HPCI アカウント IdP から発行された HPCI アカウントとパスワードを HPCI 上の認証ポータルに入力することにより行われる。(後述の GSI 認証を用いる場合は、認証局から発行されるクライアント証明書も用いられる。)

資源提供機関では、認証されたユーザが自らの機関の提供する資源を利用可能かどうかを判断する処理が必要となる。この処理を「認可」と呼ぶ。資源提供機関は、自らの運用ポリシーに基づいて、資源を利用可能なユーザを決定することができる。認可は、認可用のソフトウェアがユーザの HPCI アカウントまたはクライアント証明書の DN (Distinguished Name) の持つ属性を取得し、取得した属性に基づいて資源利用の可否を判断することに相当する。

2.2 認証基盤利用シナリオ概要

本節では、HPCI の認証基盤上で想定される利用シナリオについて、ユーザおよび運用者の視点でそれぞれ説明する。

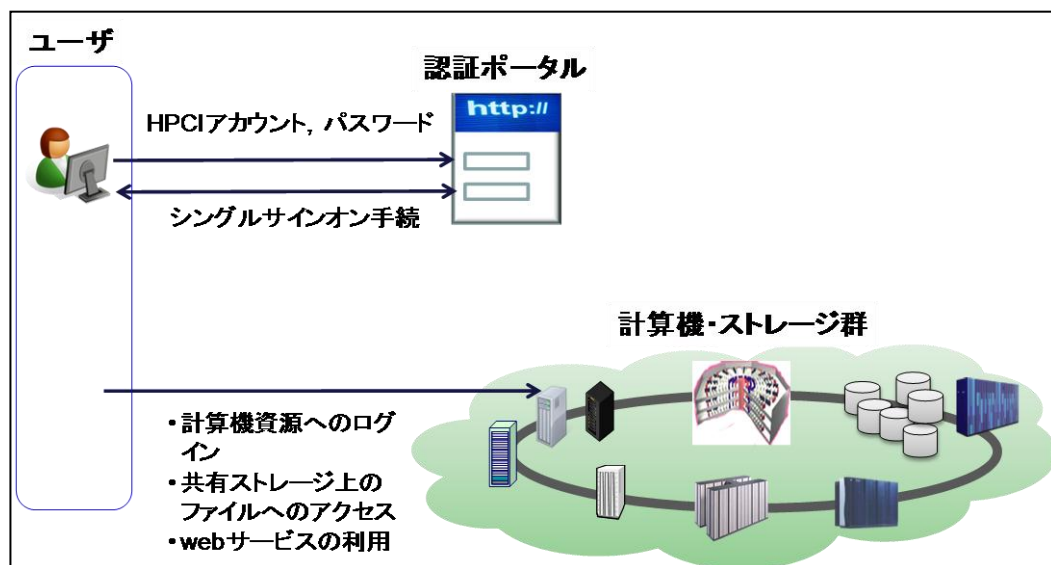


図 2.1 認証基盤利用シナリオ

HPCI の認証基盤では、図 2.1 に示すようなシングルサインオン環境を提供する。ユーザは、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のための手続きを行うことにより、HPCI 上の計算機へのログイン、ストレージ上のファイルアクセス、その他の Web サービスの利用を行うことができる。現在、認証ポータルを利用するためのアカウントやサービスの違いにより、表 2.4.1 および表 2.4.2 に示す 4 種類のシナリオ（シナリオ A～D）を想定している。このうち、シナリオ A および B は、HPCI 上の複数の資源を連携利用するためのシングルサインオン環境を提供することを目的としており、それぞれ HPCI アカウントとしてシナリオ A では Shibboleth、シナリオ B では OpenID を用いることを想定している。シナリオ C は、HPCI 上の特定の資源提供機関のサービスや計算機を利用するためのサインオン環境を提供することを目的としており、HPCI アカウントとして OpenID を想定している。最後にシナリオ D は、HPCI アカウントを利用して HPCI 外部のサービス（例えば電子ジャーナルや eduroam 等の利用）を利用することを目的としており、HPCI アカウントとして Shibboleth を想定している。

2.2.1 ユーザ視点での利用シナリオ

表 2.4.1 は、ユーザの視点で見た認証基盤の利用シナリオを示す。シナリオ A では、ユーザは、HPCI アカウント IdP が発行する Shibboleth アカウントを用いてサインオンすることにより、HPCI 上の複数の資源提供機関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が可能となる。ユーザは、利用申請のため、ユーザ管理支援編が定める手続きに従って表中の「ID/アカウント発行」に示される ID またはアカウントを取得する必要がある。資源の利用は、認証ポータル上でのサインオン処

理後、利用する計算機へログインすることにより可能となる。シナリオ B では、HPCI アカウントとして OpenID を利用すること以外は、シナリオ A と同じである。シナリオ C では、ユーザは、商用プロバイダ等が発行する OpenID アカウントを用いてサインオンすることにより、資源提供機関が提供するサービス（Web サービス）や計算機を利用することが可能となる。ただしシナリオ C では、シナリオ A や B と異なり、利用する資源毎にサインオンすることは可能ではあるが、複数資源ヘシングルサインオンすることはできない。シナリオ D は、他のシナリオと異なり、HPCI アカウントを持つユーザが、HPCI 外のサービスも利用する場合を想定している。ユーザは、HPCI アカウント IdP が発行する Shibboleth アカウントを用いてサインオンすることにより、電子ジャーナルや eduroam 等のサービスを利用することが可能となる。

表 2.1 ユーザ視点での HPCI 認証基盤利用シナリオ

シナリオ	認証基盤サービス	ユーザができること	ID/アカウント発行	サインオン
A	HPCI アカウント IdP が発行する Shibboleth アカウントを用いて、資源提供機関の計算機およびストレージを連携して利用するための GSI によるシングルサインオン環境を提供する。	✓ 資源提供機関の計算機へのログイン ✓ 資源提供機関の共有ストレージ上のファイルへのアクセス	✓ HPCI 事務局からの HPCI ID の発行 ✓ HPCI アカウント IdP からの HPCI アカウント (Shibboleth) の発行 ✓ 資源提供機関からのローカルアカウントの発行 ✓ 認証局からのクライアント証明書の発行	✓ HPCI アカウントを用いて認証ポータルにサインオン ✓ 資源へのログイン
B	商用プロバイダ等が発行する OpenID アカウントを用いて、資源提供機関の計算機およびストレージを		✓ HPCI 事務局からの HPCI ID の発行 ✓ HPCI アカウント IdP からのアカウ	

	連携して利用するための GSI によるシングルサインオン環境を提供する。		ント (OpenID) の発行 ✓ 資源提供機関からのローカルアカウントの発行 ✓ 認証局からのクライアント証明書の発行	
C	商用プロバイダ等が発行する OpenID アカウントを用いて、資源提供機関で提供されるサービス (Web サービス) や計算機を利用するためのサインオン環境を提供する。	✓ 資源提供機関で提供される Web サービスの利用 ✓ 資源提供機関の計算機へのログイン	✓ HPCI 事務局からの HPCI ID の発行 ✓ HPCI アカウント IdP からのアカウント (OpenID) の発行 ✓ 資源提供機関からのローカルアカウントの発行	✓ HPCI アカウントを用いて認証ポータルにサインオン ✓ Web サービスの利用、または資源へのログイン
D	HPCI 外のサービスを利用するための認証連携サービスを提供する。	✓ HPCI 外のサービス (電ジャーナル、eduroam 等) の利用。	✓ HPCI 事務局からの HPCI ID の発行 ✓ HPCI アカウント IdP からの HPCI アカウント (Shibboleth) の発行	✓ HPCI アカウントを用いて認証ポータルへサインオン

2.2.2 運用者視点での利用シナリオ

表 2.2 は、HPCI の運用者である資源提供機関、HPCI アカウント IdP 運用機関、認証ポータル運用機関、認証局運用機関 (※各機関の役割については用語集を参照) の視点で見た HPCI 認証基盤の利用シナリオを示す。シナリオ A から D が提供するサービスは、表 2.4.1 と同じである。

シナリオ A では、シングルサインオンの仕組みとして GSI 認証を用いるため、資源提供機関は、証明書の DN (Distinguished Name) と計算機上のローカルアカウント (UNIX アカウント) をマッピングする grid-mapfile や、信頼する認証局の証明書および証明書失効リスト (CRL) の管理を行う。HPCI アカウント IdP 運用機関および

認証ポータル運用機関は、Shibboleth IdP と認証ポータルをそれぞれ運用する。認証局運用機関は、認証局システムと発行された証明書管理のためのシステムを運用する。また、シナリオ A が想定する認証サービスは、グリッド配備・運用タスクフォースのグリッド基盤上で運用されている認証ポータルをベースとして認証ポータルを開発する必要があるほかは、既存のソフトウェアを用いて運用することが可能である。

シナリオ B では、資源提供機関が GSI 認証のための管理を行う点はシナリオ A と同じであるが、HPCI アカウント IdP 運用機関と認証ポータル運用機関が、Shibboleth に代わって OpenID に対応した IdP および認証ポータルをそれぞれ運用する点が、シナリオ A と異なる。また、OpenID に対応した認証ポータルは開発されていないため、シナリオ B ではこれを新規開発する必要がある。また、シナリオ B では商用 OpenID プロバイダが IdP となることも想定しているため、HPCI として信頼できる商用 OpenID プロバイダのセキュリティ要件に関する規定や、認証局運用規定の策定を新たに行う必要がある。

シナリオ C では、資源提供機関が OpenID のアカウントとローカルアカウントとのマッピングを行う必要があり、そのためのソフトウェアを新たに開発する必要がある。HPCI アカウント IdP 運用機関と認証ポータル運用機関については、シナリオ B と同じである。シナリオ C では、GSI 認証を用いないため、認証局運用機関は不要である。

シナリオ D では、HPCI アカウント運用機関が発行する Shibboleth のアカウントを用いて、HPCI 外のサービスをユーザが利用することを想定している。そのため、HPCI アカウント IdP 運用機関が Shibboleth IdP を運用すること以外、運用業務はない。

表 2.2 運用者視点での HPCI 認証基盤利用シナリオ

	認証基盤サービス	システム運用			
		資源提供機関	HPCI アカウント IdP 運用機関	認証ポータル運用機関	認証局運用機関
A	HPCI アカウント IdP が発行する Shibboleth アカウントを用いて、資源提供機関の計算機およびストレージを連携して利用するための GSI によるシングルサインオン環境を提供する	✓ ローカルアカウントへのマッピング (grid-map file の管理) ✓ 認証局証明	✓ Shibboleth IdP の運用	✓ 認証ポータルの運用 ※Shibboleth SP 対応認証ポータルの開発 (グリ	✓ 認証局システムの運用 ✓ 証明書管理システムの運用

	る。	書・CRL の管理		ット配備・運用タスクフォース版をベースに改変) が必要	
B	商用プロバイダ等が発行する OpenID アカウントを用いて、資源提供機関の計算機およびストレージを連携して利用するための GSI によるシングルサインオン環境を提供する。	✓ ローカルアカウントへのマッピング (grid-map file の管理) ✓ 認証局証明書・CRL の管理	✓ OpenID IdP の運用 ※OpenID プロバイダのセキュリティレベルに関する規定策定が必要	✓ 認証ポータル の運用 ※OpenID 対応認証ポータル の新規開発が必要	✓ 認証局システムの運用 ✓ 証明書管理システムの運用 ※認証局運用規定の策定が必要
C	商用プロバイダ等が発行する OpenID アカウントを用いて、資源提供機関で提供されるサービス (Web サービス) や計算機を利用するためのサインオン環境を提供する。	✓ ローカルアカウントへのマッピング (OpenID → ローカルアカウント) ※OpenID をローカルアカウントにマッピングするソフトウェアの新規開発が必要	✓ OpenID IdP の運用 ※OpenID プロバイダのセキュリティレベルに関する規定策定 が必要	✓ 認証ポータル の運用 ※OpenID 対応認証ポータル の新規開発が必要	—

D	HPCI 外のサービスを利用するための認証連携サービスを提供する。	—	✓ Shibboleth IdP の運用	—	—
---	-----------------------------------	---	----------------------	---	---

2.3 平成 23 年度利用シナリオ

平成 23 年度シナリオの決定にあたっては、以下の点に留意し、シナリオ A を平成 23 年度利用シナリオとすることとした。

- ✓ 関連する技術について、情報基盤センター等での利用実績があること。
- ✓ シナリオを実現するソフトウェアについて、既存のソフトウェア、または既存ソフトウェアをベースに開発したソフトウェアを利用可能であること。（新規ソフトウェア開発を必要としないこと。）

シナリオ A では、HPCI 認証基盤はユーザに対して、資源提供機関の計算機およびストレージを連携して利用するためのシングルサインオン環境を提供する。ユーザの認証は、ユーザが認証ポータル上で Shibboleth のアカウントおよびパスワードを入力することにより行われる。また、複数の資源提供機関の資源へのシングルサインオンを実現するために、証明書を利用した GSI 認証が行われる。以下では、平成 23 年度の利用シナリオにおいて、ユーザが認証基盤を利用する手順を説明する。

2.3.1 クライアント証明書取得

GSI 認証は、PKI (Public Key Infrastructure) 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。そのため、ユーザはまず、クライアント証明書を取得する必要がある。平成 23 年度の認証基盤利用シナリオでは、ユーザがオンライン処理よりクライアント証明書を取得できることを想定しており、図 2.2 はそのための手順を示す。クライアント証明書発行手順は、以下の 2 段階の操作から成る。初めにユーザは、認証局運用機関のポータルにアクセスし、ライセンス ID の発行を受ける。次に、ユーザは、認証ポータルにアクセスし、ライセンス ID を入力することにより、クライアント証明書が発行される。発行されたクライアント証明書は、証明書用のリポジトリに保管されるが、クライアント証明書をユーザのローカルマシンにダウンロードすることも可能である。上記の 2 つのポータルにアクセスする際の認証には、ユーザの HPCI アカウントを用いる。

クライアント証明書には有効期間（例：1 年間）が定められており、その有効期間内であれば、次節で示す手順により複数資源へのシングルサインオンが可能である、即ち、有効期間内は新たなクライアント証明書を取得する必要はない。クライアント証

明書の有効期間が終了した場合、または何らかの理由によりクライアント証明書が失効された場合は、図 2.2 の手順で新たなクライアント証明書を取得する必要がある。

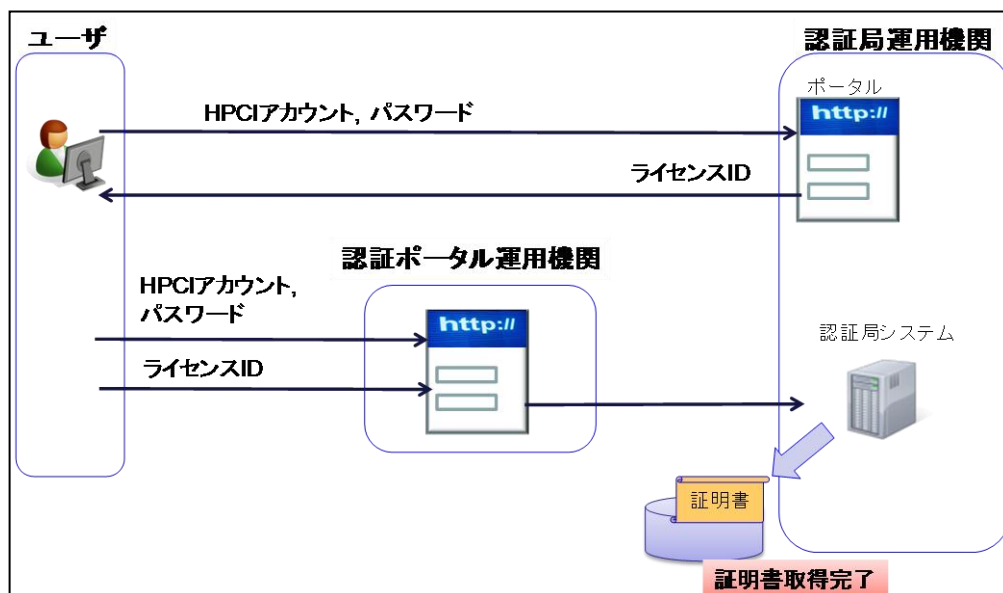


図 2.2 利用シナリオ A におけるクライアント証明書取得手順

2.3.2 シングルサインオン

GSI 認証では、ユーザの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）を用いてシングルサインオンが実現される。図 2.3 は、ユーザが HPCI 上の資源にシングルサインオンするための手順を示す。ユーザは、認証ポータル上で HPCI アカウントを用いてサインオンし、Proxy 証明書を生成する。生成された Proxy 証明書は、Proxy 証明書用リポジトリに保管され、複数資源へのアクセス権限を移譲するために用いられる。ただし、ユーザが利用するソフトウェアによっては、必要に応じてユーザのローカルマシンに Proxy 証明書をダウンロードする。

Proxy 証明書には有効期間（例：1 週間）が定められており、その有効期間内であれば、ユーザは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、即ち、有効期間内は Proxy 証明書を再生成する必要はない。Proxy 証明書の有効期間終了後は、図 2.3 の手順で新たな Proxy 証明書を生成する必要がある。

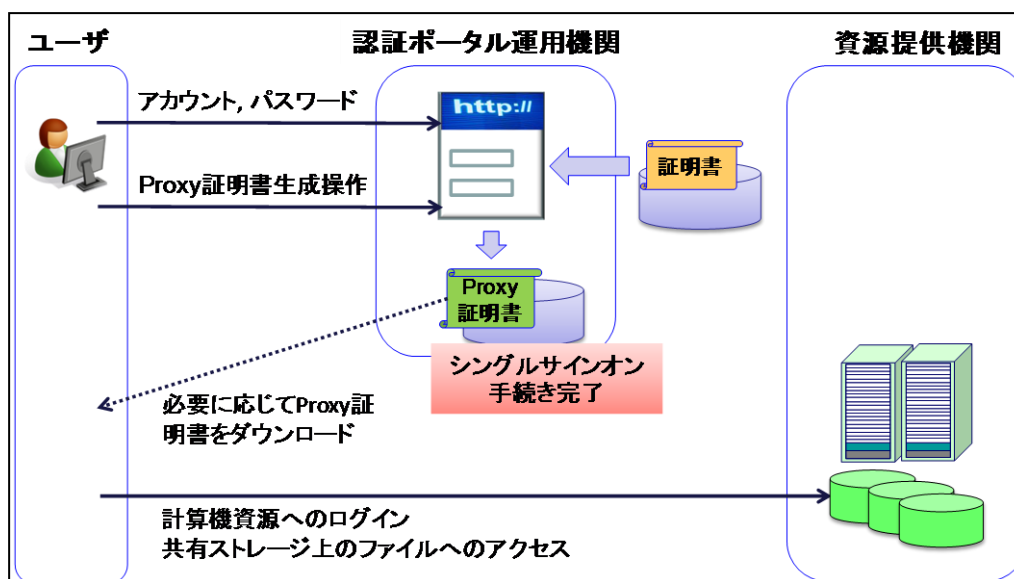


図 2.3 シナリオ A におけるシングルサインオン手順

3 認証基盤構築・運用基本仕様

本節では、HPCI 認証基盤を構成するシステムの仕様について説明する。初めに、HPCI 認証基盤の必要要件およびアーキテクチャ概要を示し、平成 23 年度に実現する認証基盤のアーキテクチャおよびユーザ仕様を説明する。次に、HPCI 認証基盤を構成する運用機関毎の詳細仕様を説明する。また、平成 24 年度以降の実現に向けた検討事項についても述べる。

3.1 必要要件およびアーキテクチャ概要

3.1.1 必要要件

認証基盤の目的は、「2.2 認証基盤利用シナリオ概要」に記載されている下記の A～D)を実現することである。

- A) HPCI アカウント IdP 運用機関が発行する Shibboleth アカウントを用いて、HPCI 認証局でのクライアント証明書の発行が可能であること。発行したクライアント証明書を使用し、資源提供機関の計算機やストレージ等を連携して利用するための GSI 認証によるシングルサインオン環境を提供すること。
- B) 商用プロバイダ等が発行する OpenID アカウントを用いて、HPCI 認証局でのクライアント証明書の発行が可能であること。発行したクライアント証明書を使用し、資源提供機関の計算機やストレージ等を連携して利用するための GSI 認証によるシングルサインオン環境を提供すること。
- C) 商用プロバイダ等が発行する OpenID アカウントを用いて、資源提供機関で提供されるサービス(Web サービス)や計算機を利用するためのサインオン環

境を提供すること。

- D) HPCI アカウント IdP 運用機関が発行する Shibboleth アカウントを用いて、HPCI 外のサービスを利用するための認証連携サービスを提供すること。

3.1.2 認証基盤構築の方針

HPCI におけるユーザへのサービス提供方法は、単純なターミナルによる直接ログイン、ミドルウェアを介してのジョブ投入やファイル操作、Web サービスによるアプリケーション実行の3種類が考えられる。HPCI 認証基盤は、その全てに対応可能とする。

また全国規模で分散された情報資源の安全性を一定のレベルで確保し、かつ広範囲なユーザに対して効率的な認証サービスを行うことを前提条件として、実証済みの技術で実用的な認証基盤を作ることを目指す。そのために PKI(public Key Infrastructure:公開鍵暗号基盤)を採用し、統合的な認証基盤を構築する。

3.1.3 ユーザ認証アーキテクチャ

認証基盤の実現に必要な基本的な機能とプロトコルは、図 3.1 に示す HPCI 認証基盤におけるユーザ認証アーキテクチャに示す通りである。全てのセキュリティ基盤の基礎となるのは、セキュリティ・モデルとセキュリティ・ポリシーである。また認証基盤の構造は、ユーザインターフェース層と認証機能層の2層からなる。

ユーザインターフェース層には、端末機能、ミドルウェア機能、Web サービスのためのサービスプロバイダ機能の3つがある。端末およびミドルウェアからの認証には GSI(Grid security Infrastructure)のプロトコルを用いる。また SAML プロトコルは、Web サービスの他、ミドルウェアに実装されて利用されることも想定している。

認証機能層には、Web サービス系と GSI 系の2系統の機能がある。

Web サービス系としては、サービスプロバイダに対して、SAML による認証サービスを行う IdP(Identity Provider)機能があり、Shibboleth や OpenID 等のプロトコルを使用する。

GSI 系としては、信頼の起点としての CA(認証局)、端末のための SSH、ミドルウェアのための仮想組織 (VO) やクレデンシャル・レポジトリという機能がある。例えば、SSH は GSI SSH、クレデンシャル・レポジトリは MyProxy、VO は VOMS のプロトコルを用いることが想定できる。クレデンシャル・レポジトリと VO を統合して利用するためのプロトコルとしては、GAMA や UMS(User Management Service)が想定できる。

Grid Pack for HPCI は、HPCI のために開発される、人の手続きを含むプロトコルであり、Web サービスの IdP を用いて認証局の本人確認を行い、直接本人に証明書を発行することを可能とする。 GAKUNIN/UPKI は、現在 NII が行っている電子ジ

ジャーナル購読等のための個人認証や汎用サーバの正当性証明のサービスであり、将来的には HPCI 認証基盤との連携を考慮する。

以上の機能やプロトコルの内、H23 年度に運用を開始する予定の部分をピンク色と赤字で示す。

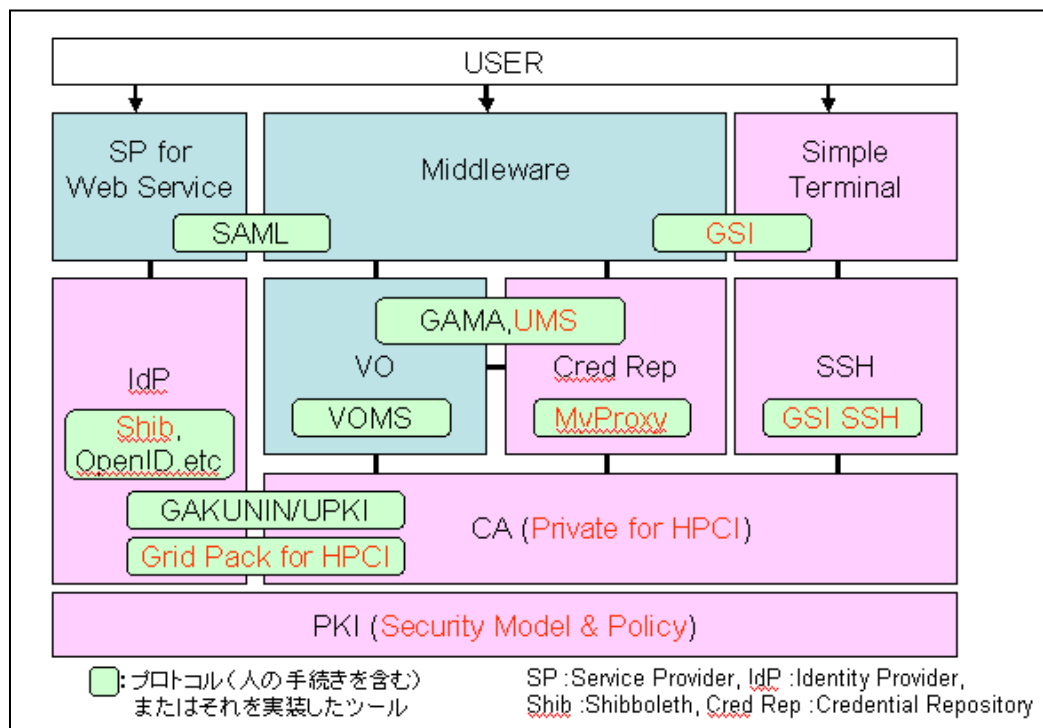


図 3.1 認証基盤におけるユーザ認証アーキテクチャ

3.1.4 平成 23 年度認証基盤

尚、2.4.3 節で述べたように、平成 23 年度に実現する認証基盤では、シナリオ A を実現することを目的とする。認証基盤を構成する組織（運用機関）については、平成 23 年度に運用する認証基盤に参加可能な具体的な運用機関を想定する。また、認証基盤を構築するためのソフトウェアは、原則として既に情報基盤センター等での利用実績があるソフトウェア、またはこれを改変したソフトウェアを使用することとする。

以降では シナリオ A を対象とした仕様について説明する。B～D においては平成 24 年度以降での実現に向けた目標とし、平成 23 年度中にソフトウェア仕様、運用規定、運用開始時期について検討することとする。

3.2 平成 23 年度認証基盤アーキテクチャ

本節では、平成 23 年度に実現する認証基盤を構成する運用機関およびソフトウェアアーキテクチャの仕様について説明する。

3.2.1 運用機関

平成 23 年度に実現する認証基盤は、HPCI 事務局、認証局運用機関、認証ポータル運用機関、HPCI アカウント IdP 運用機関、資源提供機関の 5 機関から構成される。(※各機関の役割については用語集を参照)また平成 23 年度は、これらの運用機関として、具体的に表 3.1 に示す機関を想定している。

表 3.1 運用機関(登場人物)

運用機関	運用予定サイト
HPCI 事務局	第三者機関※未定
認証局運用機関	NII
認証ポータル運用機関	情報基盤センター、NII
HPCI アカウント IdP 運用機関	情報基盤センター、理研（神戸）※検討中
資源提供機関	情報基盤センター、理研（神戸）※検討中

3.2.2 ソフトウェアアーキテクチャ

平成 23 年度に実現する認証基盤は、以下の 6 つのソフトウェアコンポーネントから構成される。また図 3.2 は、以下のコンポーネント間の関係を示す。

1. 認証ポータル

認証ポータルはユーザが認証基盤システムを利用する為に最初にアクセスする必要のある Web ポータルサービスである。ユーザは HPCI アカウント IdP 運用機関で発行された Shibboleth アカウントのアカウント名、パスワードを入力することで認証を行い、後述の「認証局システム」コンポーネントと連携し、ユーザの属性値をもとにクライアント証明書の発行操作や発行されたクライアント証明書を用いたシングルサインオン操作を行うためのインターフェイスを提供する。

2. 認証局システム

認証局システムは、「認証ポータル」コンポーネントと連携し、ユーザの要求を受け付けクライアント証明書発行用のライセンス ID の発行、及びクライアント証明書の発行を行う。認証局システムは、その役割から CA サーバ部と RA サーバ部に分かれ、認証局の管理者は、RA サーバ部を操作することで

CA サーバ部上でクライアント証明書、ホスト証明書、サービス証明書の発行処理・失効処理を行うことができる。

また、認証局の CA 証明書や CRL、および、CP/CPS 等の認証局運用に必要な情報の公開を行う。

3. 証明書管理システム

証明書管理システムは、「認証ポータル」コンポーネント及び「認証局システム」コンポーネントと連携し、発行されたクライアント証明書を格納、管理する。また、ユーザの操作による認証ポータルからの要求を受け、格納しているクライアント証明書から Proxy 証明書を作成し、Proxy 証明書リポジトリへ格納する。

4. Proxy 証明書リポジトリ

Proxy 証明書リポジトリは、「証明書管理システム」コンポーネントからの操作により、作成された Proxy 証明書を格納管理する。

5. GSI 認証機能を持つミドルウェア

GSI 認証機能を持つミドルウェアとしては、Globus Tool Kit に含まれる GSH-SSH と Gfarm を使用することを想定する。GSI-SSH は、Proxy 証明書を使用し、GSI 認証による SSH ログインが可能である。ストレージアクセスのためのミドルウェアである Gfarm も同様に、Proxy 証明書を使用し、GSI 認証によるストレージ共有が可能である。

6. 認証連携用ミドルウェア

認証連携用ソフトウェアとしては Shibboleth 使用する。Shibboleth は、Shibboleth IdP(以下 IdP)、認証ポータルおよび認証局で動作する Shibboleth SP (以下 SP)、Shibboleth DS (以下 DS) の 3 つのソフトウェアコンポーネントが必要である。

IdP は、ユーザの Shibboleth アカountのアカウント名、パスワードの入力による認証を行う。認証は HPCI アカount IdP 運用機関のアカウント DB に登録された認証情報を元に実施する。SP は、IdP で認証されたユーザの属性情報を取得し、アプリケーションやサービスに情報伝播及びアクセス制御を行うためのサービスプロパイダとして機能する。DS は複数ある IdP の中からユーザが認証に必要な IdP を選択するためのサービスである。

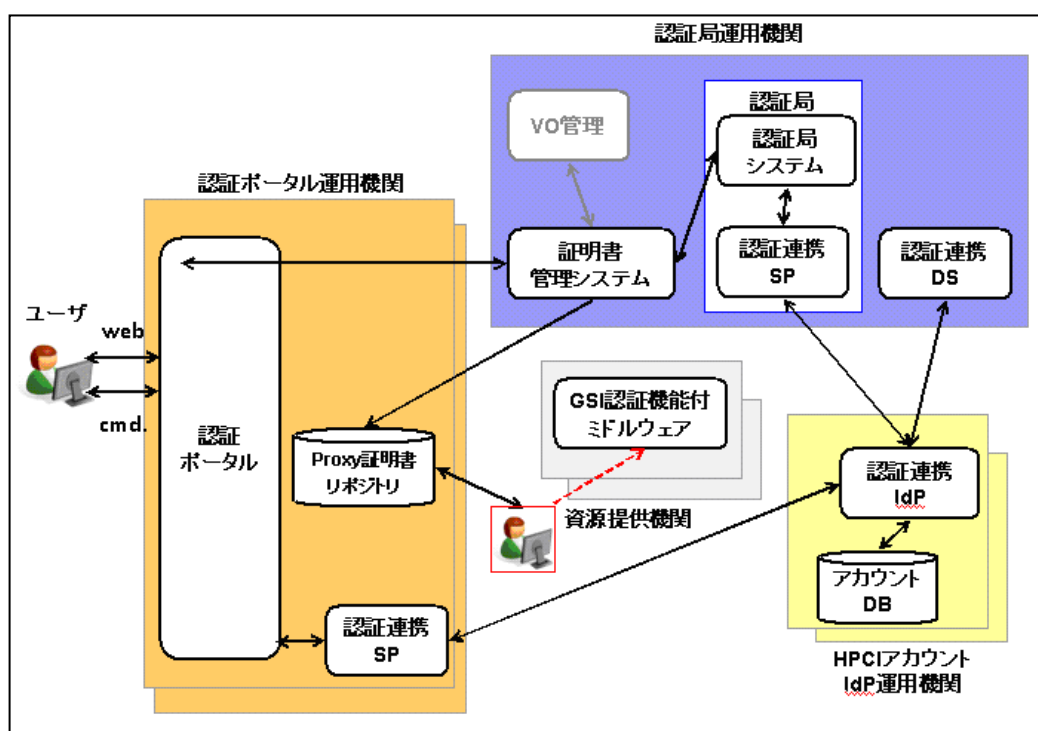


図 3.2 H23 年度運用機関連携図

図 3.2 のシステムを構築するためのソフトウェアは、原則として、既に情報基盤センター等での利用実績があるものを利用する。具体的には、表 3.2 のソフトウェアを利用する。

表 3.2 利用ソフトウェア

コンポーネント	ソフトウェア
認証局システム	NAREGI-CA
認証ポータル	グリッド配備・運用タスクフォースで使用されているポータルをベースに開発
証明書管理システム	UMS、MyProxy
Proxy 証明書リポジトリ	MyProxy
GSI 認証機能を持つミドルウェア	Globus(GSI-SSH)、Gfarm
認証連携用ソフトウェア	Shibboleth IdP Shibboleth DS Shibboleth SP

3.2.3 HPCI 事務局との連携

認証基盤システムにおいては、HPCI 事務局にて運用する HPCI ポータルで管理する 3 つのデータベース、

- ・ HPCI-ID 管理簿
- ・ HPCI 利用課題管理簿
- ・ HPCI 提供資源管理簿

と、業務自動化のため密接に連携する必要がある。具体的には各データベースの情報を参照し CN の重複チェックの自動化、grid-mapfile の生成の自動化を実現する。図 3.3 は、これら連携機関のネットワーク概念図を示す。

各データベースはプライベートネットワーク（または VPN）上に設置し、HPCI 事務局運用の HPCI ポータルおよび認証局運用機関運用の証明書管理システムからのみ接続を許可する。HPCI ポータルおよび証明書管理システムは、認証ポータル等との連携のためグローバルネットワークとプライベートネットワークの両方にインターフェースを持つ。HPCI ポータルと証明書管理システムのグローバルネットワーク側のインターフェースは認証ポータルとの連携で使用し、認証ポータルからのみの接続を許可する。

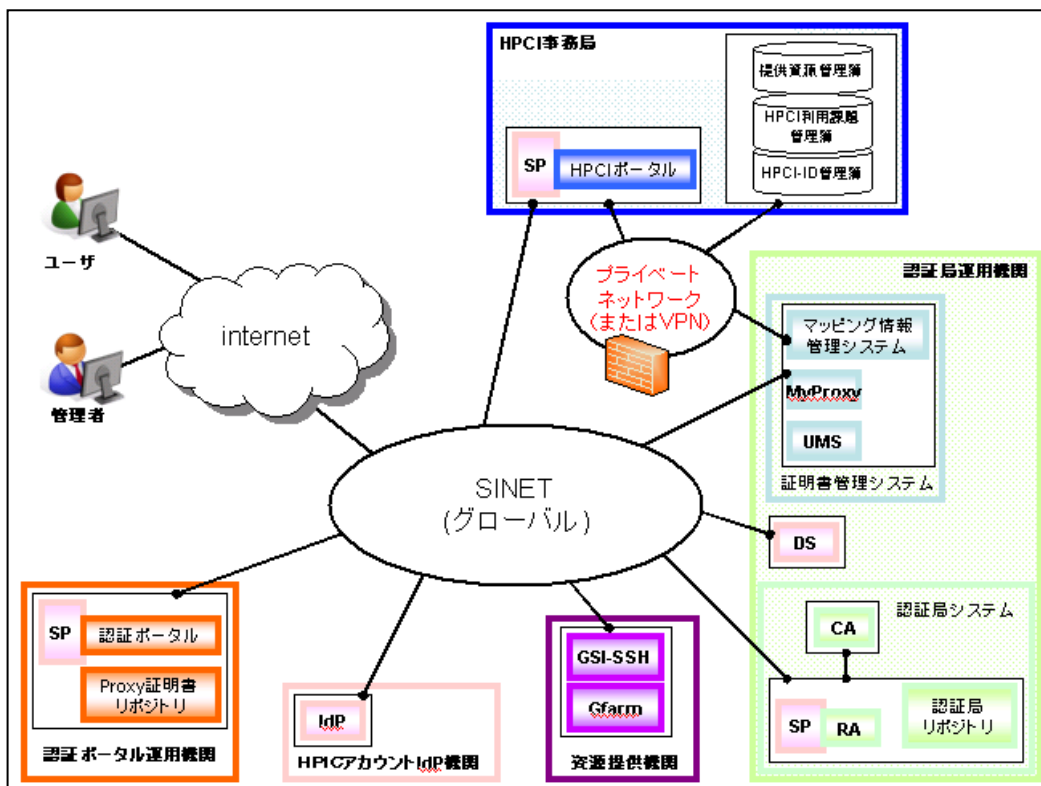


図 3.3 ネットワーク概念図

3.2.4 ユーザ仕様

本節では、平成 23 年度認証基盤アーキテクチャにおけるユーザが整備すべきソフトウェアに関する仕様を説明する。ユーザの認証基盤の利用は、2.3 節に示したように GSI 認証のためのクライアント証明書取得、および取得したクライアント証明書を用いたシングルサインオン（Proxy 証明書生成と資源へのログイン）の 2 種類が想定される。それぞれの利用において必要となるソフトウェアの仕様を表 3.3 に示すとともに、以下に説明する。

表 3.3 認証基盤におけるユーザソフトウェア

利用内容	ソフトウェア	例
クライアント証明書取得	Web ブラウザ	IE, FireFox 等
シングルサインオン	Web ブラウザ	IE, FireFox 等
	Proxy 証明書管理 (クライアントソフトウェア)	MyProxy, Certificate Management Wizard
	GSI-SSH (クライアントソフトウェア)	GSI-OpenSSH, GSI-SSHTerm

3.2.5 クライアント証明書取得

ユーザは、図 2.2 に示す手順で認証局運用機関および認証ポータル運用機関のポータル上でオンライン処理を行うことにより、クライアント証明書を取得することができる。ここでユーザが必要なソフトウェアは、ポータルにアクセスするための Web ブラウザ（Internet Explorer や FireFox 等）のみである。

3.2.6 シングルサインオン

ユーザは、図 2.3 に示す手順で認証ポータル運用機関が運用する認証ポータル上でオンライン処理を行うことにより、シングルサインオンが可能となる。具体的には、ユーザはまず認証ポータル上で Proxy 証明書の生成と MyProxy への格納を行う。Proxy 証明書生成後はその有効期限内であれば、ユーザは HPCI 上の資源へ認証処理なしでログインすることができる。ここでユーザが必要なソフトウェアは、認証ポータルにアクセスするための Web ブラウザ、Proxy 証明書を管理するためのソフトウェア（クライアントソフトウェア）、資源へログインするための GSI-SSH（クライアントソフトウェア）である。

このうち、Proxy 証明書を管理するためのソフトウェアの例は、MyProxy (<http://grid.ncsa.illinois.edu/myproxy/>) や Certificate Management Wizard (<http://www.ngs.ac.uk/tools/certwizard>) が想定される。また、GSI-SSH の例としては、

GSI-OpenSSH (<http://www.globus.org/toolkit/docs/4.0/security/openssh/>) や GSI-SSHTerm (<https://security.ncsa.illinois.edu/gsi-sshterm/>)が想定される。ただし本仕様では、これらについて特定のソフトウェアに限定することはない。

3.3 認証局運用機関仕様

本節では、平成 23 年度に認証局運用機関が整備すべきシステムとその運用に関する仕様（認証局運用体制も含む）を説明する。

認証局運用機関は以下の 3 つのコンポーネントで構成し、運用する。

- ・ 認証局システム
- ・ 証明書管理システム
- ・ Shibboleth DS

以下に、認証局運用機関について、ユーザ視点と管理者視点での概念図を示す。

【ユーザ視点】

ユーザは、認証局運用機関に対して、ライセンス ID の発行要求（図中 1-* の処理）、およびクライアント証明書の発行要求（図中 2-* の処理）を行う。

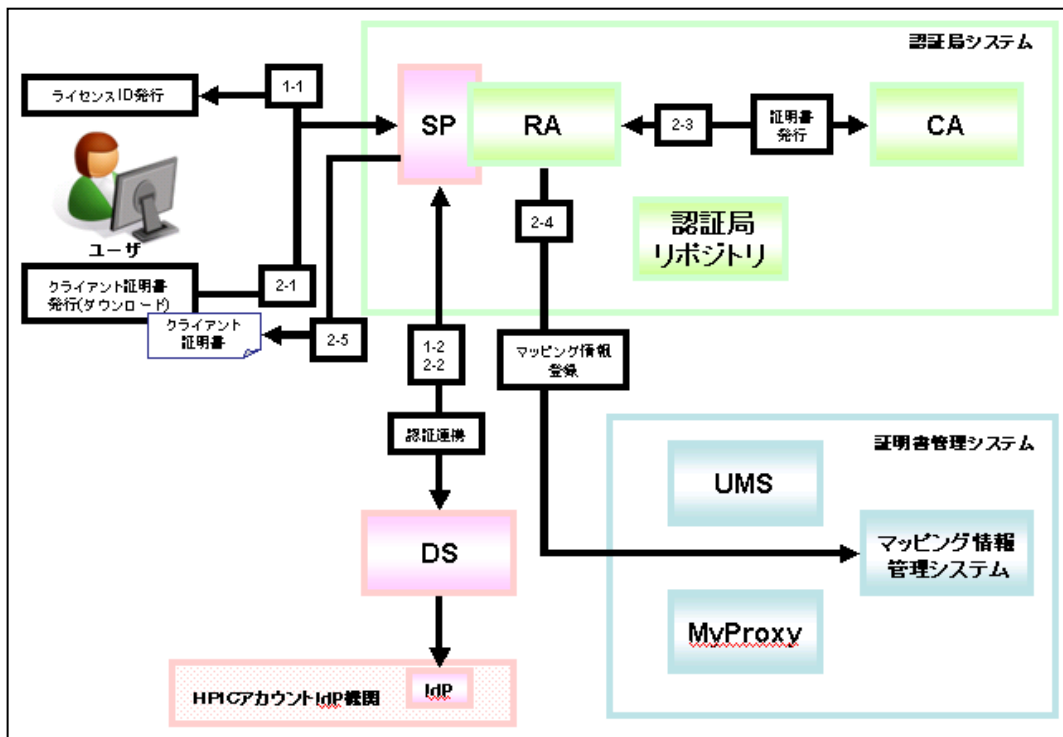


図 3.4 認証局運用機関 概念図（ユーザ視点）

【管理者視点】

認証局運用機関の管理者は、証明書の発行・失効処理（図中 1-*の処理）、データのバックアップ（図中 2-*の処理）、Shibboleth DS のメタデータ更新（図中 3-*の処理）、grid-mapfile 情報の管理（図中 4-*の処理）を行う。

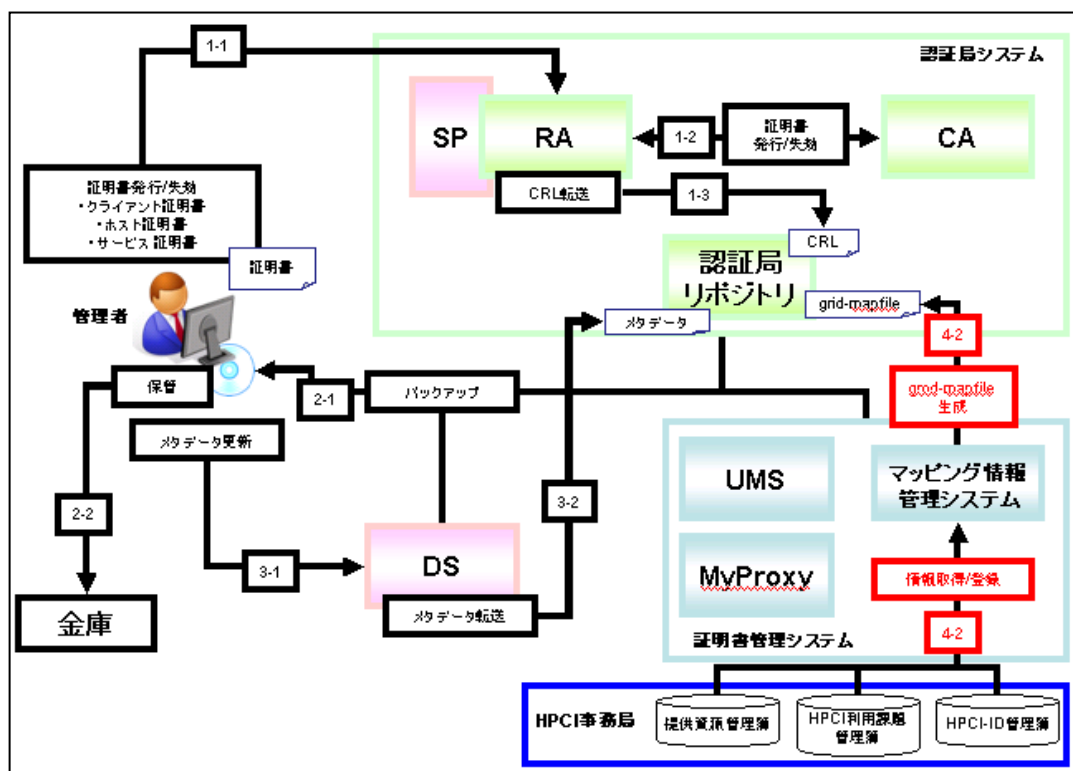


図 3.5 認証局運用機関 概念図（管理者視点）

3.3.1 認証局システム

認証局運用機関は、HPCI で利用するための、

- ・ クライアント証明書
- ・ ホスト証明書
- ・ サービス証明書

の発行業務を行う。

クライアント証明書の発行では、HPCI アカウント IdP 運用機関、および商用プロバイダ等のユーザ管理機関と連携することで、証明書発行におけるユーザの利便性向上、運用工数の削減を目指す。ただし、HPCI アカウント IdP 運用機関、商用プロバイダ等が管理するアカウントの認証レベル、および属性の保証レベルに対応した認証局の構成、運用、および発行するクライアント証明書の保証を行う。

平成 23 年度には、HPCI アカウント IdP 運用機関が発行する Shibboleth アカウントを用いた連携を行い、HPCI アカウント IdP 運用機関が管理する HPCI アカウントの

保証レベルへの対応とすることで、できる限り MICS プロファイルに対応した保証レベルを目指すものとする。以下では、平成 23 年度に構築、運用開始する認証局運用機関に求められる要件を示す。

認証局システムの構成およびその役割は下記のとおりである。

1. CA サーバ
 - ・ 3 種類の証明書の発行、失効を行う。
 - ・ 定期的に CRL を発行して認証局リポジトリにこれを送信する。
2. RA サーバ
 - ・ 3 種類の証明書の発行登録、失効登録を行う。
 - ・ 証明書発行のためのライセンス ID 管理機能を備える。
 - ・ クライアント証明書の登録用ポータルを備える。
 - ・ クライアント証明書の登録用ポータルは、HPCI アカウント IdP 運用機関が運用する IdP と連携する。
 - ・ クライアント証明書の登録用ポータルは、認証ポータル運用機関が運用する認証ポータルと連携する。
 - ・ HPCI 事務局と連携し、HPCI 事務局からの申請により、クライアント証明書の失効を行う。
3. 認証局リポジトリ
 - ・ CP/CPS を公開する。
 - ・ CA 証明書、および、フィンガープリントを公開する。
 - ・ CRL を公開する。
 - ・ HPCI 認証局の各種情報を公開する。

3.3.1.1 ソフトウェア仕様

認証局システムのソフトウェアの仕様は以下の通りである。

1. CA サーバ
 - 1-1 ソフトウェアとして NAREGI-CA をベースとして使用し構築すること。
 - 1-2 CA サーバは、RA サーバとは物理的な別サーバとして構築すること。
 - 1-3 オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザ数無制限のサーバライセンスであること。
 - 1-4 RA と連携しクライアント証明書の発行が出来ること。
 - 1-5 RA と連携しホスト証明書の発行が出来ること。
 - 1-6 RA と連携しサーバ証明書の発行が出来ること。

- 1-7 RA と連携し、クライアント証明書の失効ができること。
- 1-8 RA と連携し、ホスト証明書の失効ができること。
- 1-9 RA と連携し、サーバ証明書の失効ができること。
- 1-10 1 万人を超えるユーザが利用可能であり、200 回／分のトランザクションがあってもボトルネックにならないこと。

2. RA サーバ

- 2-1 ソフトウェアとして NAREGI-CA をベースとして使用し構築すること。また、認証局リポジトリと同じサーバ上に構築しても良い。
- 2-2 RA サーバは、CA サーバとは物理的な別サーバとして構築すること。
- 2-3 オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザ数無制限のサーバライセンスであること。
- 2-4 SAML による認証連携ができること。ソフトウェアは Shibboleth SP を使用すること。
- 2-5 学術認証フェデレーションのメタデータを自動ダウンロードして、利用できること。
- 2-6 ユーザが Web アクセスし、クライアント証明書を発行する際に使用するライセンス ID を取得するためのインターフェースを有すること。
- 2-7 ユーザが Web アクセスしライセンス ID を入力し、クライアント証明書を取得するためのインターフェースを有すること。
- 2-8 ユーザが Web アクセスし、発行した証明書をダウンロードするためのインターフェースを有すること。
- 2-9 ユーザが取得可能なライセンス ID の数が制限できること。
- 2-10 ユーザが同時に保持できるライセンス ID の数が制限できること。
- 2-11 ユーザがクライアント証明書を発行した際、自動的に証明書発行通知メールを送信する機能を有すること。
- 2-12 証明書発行通知メールの送信先は認証局管理者が任意に設定できること。証明書発行通知メールの送信先はドメイン単位での設定ができること。
- 2-13 Shibboleth の機能により受け取った属性を使用し、クライアント証明書の発行を申請したユーザの英字名、英字性、HPCI-ID を含む CN が自動反映される設定とすること。
- 2-14 Shibboleth の機能により受け取った属性値を参照し、認証局の利用における認可判定を自動的に行う機能を有すること。

- 2-15 認可判定で使用する Shibboleth の属性とその値は、認証局管理者が任意に設定できること。
- 2-16 SSL によるユーザからのアクセスに対応していること。
- 2-17 1 万人を超えるユーザが利用可能であり、200 回／分のトランザクションがあってもボトルネックにならないこと。
- 2-18 CA と連携しホスト管理者によりホスト証明書が発行できること。
- 2-19 CA と連携しサービス管理者によりサービス証明書が発行できること。
- 2-20 CA と連携し証明書を失効する機能を有すること。

3. 認証局リポジトリ

- 3-1 **grid-mapfile** を公開する機能を有すること。
- 3-2 認証局システムの証明書を公開する機能を有すること。
- 3-3 認証局システムのフィンガープリントを公開する機能を有すること。
- 3-4 証明書失効リスト(CRL)を公開する機能を有すること。
- 3-5 CP/CPS を公開する機能を有すること。
- 3-6 仮想化環境上に構築、もしくは RA サーバと同サーバ上に構築しても良い。
- 3-7 オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザ数無制限のサーバライセンスであること。
- 3-8 仮想化環境上に構築する場合は、サーバに実装された CPU・主記憶装置・ストレージ・ネットワークを全て認識する仮想化基本ソフトウェアおよびライセンスを導入すること。尚、ゲスト OS は仮想化基本ソフトウェア上でサポート及び動作確認が行われている日本語対応のサーバ用 OS であること。

3.3.1.2 ハードウェア仕様

認証局システムを構成するサーバのハードウェア仕様は以下のとおりである。

1. CA サーバ (1 台)

- 1-1. 物理サーバとし、CA システムのみ稼動させること。
- 1-2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。また、プロセッサは冗長化すること。
- 1-3. ECC 機能に対応した 4GB 以上の容量のメモリを有すること。
- 1-4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で

接続されたドライブを有すること。

- 1-5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
- 1-6. 1000Base-T 規格の Ethernet インターフェースを 2 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
- 1-7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID5 相当のアレイ構成とすること。
- 1-8. ディスク装置を活線挿抜によって交換できること。
- 1-9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
- 1-10. 電源ユニットおよびファンは冗長化すること。
- 1-11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
- 1-12. VGA モニタおよび USB キーボード・マウスを接続できること。
- 1-13. 本体はラックに収容すること。
- 1-14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。
- 1-15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
- 1-16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
- 1-17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
- 1-18. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
- 1-19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
- 1-20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

2. HSM (1 台)

- 2-1. FIPS 140-2 level 3 以上相当の機能を有すること。

2-2. 秘密鍵をバックアップ可能であること。

3. RA サーバ（1台）

- 3-1. 物理サーバとすること。
- 3-2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。また、プロセッサは冗長化すること。
- 3-3. ECC 機能に対応した 12GB 以上の容量のメモリを有すること。
- 3-4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
- 3-5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
- 3-6. 1000Base-T 規格の Ethernet インターフェースを 4 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
- 3-7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID5 相当のアレイ構成とすること。
- 3-8. ディスク装置を活線挿抜によって交換できること。
- 3-9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
- 3-10. 電源ユニットおよびファンは冗長化すること。
- 3-11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
- 3-12. VGA モニタおよび USB キーボード・マウスを接続できること。
- 3-13. 本体はラックに収容すること。
- 3-14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。
- 3-15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
- 3-16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
- 3-17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
- 3-18. 復電時には、切断時に稼働していたオペレーティングシステムを再起

動し、運用状態を復元できること。

- 3-19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
- 3-20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

4. 認証局リポジトリ（1台）

- 4-1. 物理サーバとする場合は下記の内容に従うこと。仮想サーバとして構築しても良いが、下記の内容と同等の性能を満たす環境とすること。
また、RA サーバと同じサーバ上に構築する場合は、RA サーバのハードウェア仕様に従うこととするが、ストレージ容量とメモリサイズは十分に考慮すること。
- 4-2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。また、プロセッサは冗長化すること。
- 4-3. ECC 機能に対応した 8GB 以上の容量のメモリを有すること。
- 4-4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
- 4-5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
- 4-6. 1000Base-T 規格の Ethernet インターフェースを 4 回線有すること。
また、トランク機能によって論理的に単一インターフェースとして稼働できること。
- 4-7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID0 もしくは RAID 1 相当のアレイ構成とすること。
- 4-8. ディスク装置を活線挿抜によって交換できること。
- 4-9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
- 4-10. 電源ユニットおよびファンは冗長化すること。
- 4-11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
- 4-12. VGA モニタおよび USB キーボード・マウスを接続できること。
- 4-13. 本体はラックに収容すること。
- 4-14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。

- 4-15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
- 4-16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
- 4-17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
- 4-18. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
- 4-19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
- 4-20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

3.3.1.3 セキュリティ仕様

認証局システムのセキュリティ管理仕様は以下の通りである。

1. セキュリティについては、平成 23 年度に作成する CP/CPS に従うこと。
2. マシンへの物理的アクセス方法について、CPS で定めるアクセス権限者のみが可能とすること。
3. 設置場所は、十分な防火対策、水害対策、地震対策が可能であること。
4. CA サーバは隔離されたネットワークに設置し、RA サーバとのみ通信可能とすること。
5. RA サーバにおいてはファイアウォールによる通信ポート制限を行うこと。
6. RA サーバにおいてはアクセスログの採取が可能であること。
7. 認証局リポジトリは、公開する内容のセキュリティを考慮して利用プロトコルを決定すること。特に、フィンガープリントの公開にあたっては https のみを利用することとする。

3.3.1.4 認証局運用仕様

(ポリシー管理)

1. HPCI 認証局ポリシー管理委員会（HPCI 認証局 PMA）を置く。
2. HPCI 認証局 PMA は、CP/CPS の維持管理を行う。
3. PMA の組織構成、各種手続きについては別途定める

(運用ポリシー)

1. HPCI 認証局では、CP/CPS (Certificate Policy and Certification Practice Statement) を定める
2. CP/CPS は、HPCI 全体のセキュリティ要件、HPCI 認証局としてのセキュリティ要件と運用要件、および、HPCI の他の運用機関との連携機能要件を満たし、できる限り IGTF が定める MICS プロファイルを満たすよう作成する
(添付資料 1 HPCI 認証局運用規定 Draft Ver1.0 を参照)
3. 運用体制と担当者の人数は表 3.4.4 の通りとする。

表 3.4 運用体制

構成要素		主な役割
認証局運用者	認証局責任者 (1 名、 認証局の他業務との 兼務不可)	・ 認証業務統括 ・ CA 秘密鍵管理 ・ IdP 連携申請承認
	CA 運用者 (2 名、認 証局の他業務との兼 務不可)	・ CA 秘密鍵の活性化／非活性化 ・ CA サーバ、RA サーバの管理 ・ 認証局システムの操作・保守管 理
	ログ管理者 (1 名、認 証局の他業務との兼 務不可)	・ バックアップ媒体、ログ／アーカ イブ媒体の管理
	認証局ヘルプデスク (1 名以上、認証局の 他業務との兼務可)	・ HPCI ヘルプデスクからの証明書 利用に関する問い合わせ窓口
HPCI アカウン ト IdP 運用者	HPCI 利用者受付 (3 名)	・ 利用者の申請受付、登録 ・ 申請責任者の審査
	申請責任者 (*)	・ ユーザの審査・承認
利用者	ユーザ (*)	・ HPCI 認証局発行の証明書ユーザ
	ホスト管理者 (*)	・ 証明書を利用する資源提供機関に おけるホストの管理者
	サービス管理者 (*)	・ 証明書を利用する資源提供機関に おけるサービスの管理者

*人数は規定しない。

4. 業務担当と業務を行う人数は表 3.4.5 の通りとする。

表 3.5 認証局業務

業務	要員（要員数） ※表 3.4.4 で定める人数の内数
認証業務統括	認証局責任者（1 名）
CA 秘密鍵操作と管理	認証局責任者（1 名）、CA 運用者（1 名）
CA 秘密鍵の活性化/非活性化	CA 運用者（2 名）
CA サーバ、RA サーバの管理	CA 運用者（2 名）
認証局システムの保守管理	CA 運用者（2 名）
監査ログ/アーカイブ媒体の管理	ログ管理者（1 名）
認証局ヘルプデスク	認証局ヘルプデスク（1 名以上）
申請責任者からの申請受付・審査・承認	利用者受付（3 名）
ユーザからの申請受付・審査	申請責任者（*）

*人数は規定しない。

5. CA 秘密鍵は下記とする。
 アルゴリズム、鍵長： RSA 2048bit
 有効期間： 10 年
 利用目的（KeyUsage）： keyCertSign, cRLSign
 秘密鍵管理： HSM で管理
 バックアップ： バックアップを安全な場所で管理
6. HPCI 認証局の CA 鍵ペア生成にあたっては、キーセレモニーを実施すること。
7. クライアント証明書発行における利用者の本人審査は、利用者の HPCI アカウント IdP による認証により行うこととする。
8. クライアント証明書発行における利用者の資格審査は、利用者が HPCI アカウント IdP による認証により有効な HPCI アカウントを保持していることを確認することにより行うこととする。
9. ライセンス ID の発行時には、HPCI ID が一意であることを確認する。
10. クライアント証明書の発行は、1 つの HPCI ID に対し証明書 1 枚のみを発行する。
11. クライアント証明書、ホスト証明書、サービス証明書の 3 種類の証明書の発行、失効を行うこと。
12. 発行する証明書の主なプロファイルは下記とすること。

- (1) クライアント証明書
アルゴリズム、鍵長： RSA 2048bit
有効期間： 13 ヶ月
利用目的： digitalSignature, keyEncipherment
commonName： ユーザ氏名（ヘボン式ローマ字）（スペース） HPCI ID
 - (2) ホスト証明書
アルゴリズム、鍵長： RSA 2048bit
有効期間： 13 ヶ月
利用目的： digitalSignature, keyEncipherment
commonName： ホスト名（FQDN）
 - (3) サービス証明書
アルゴリズム、鍵長： RSA 2048bit
有効期間： 13 ヶ月
利用目的： digitalSignature, keyEncipherment
commonName： サービス名
13. 認証局リポジトリにより、下記を公開すること。
 - ・ CP/CPS
 - ・ CA 証明書、および、フィンガープリント
 - ・ CRL
 - ・ HPCI 認証局の各種情報
 14. CRL 発行は下記の通りとすること。
有効期間： 30 日
発行時期： 有効期限の 7 日前まで
 15. 監査ログの保管期間は 3 年間、ただし、CA ログ、HSM ログは 10 年間とすること。
 16. 認証局責任者は、学術認証フェデレーションに SP の登録を行うこと。この際、認証局ポータルが HPCI アカウント IdP との SAML 連携で利用する証明書を用いたメタデータを提出すること。
 17. 学術認証フェデレーションに参加する SP として、学術認証フェデレーション システム運用基準にしたがった運用を行うこと。

3.3.2 証明書管理システム

認証局運用機関は、ユーザが利便性良く、且つ柔軟なクライアント証明書利用を目指し、証明書の管理業務を行う。また、クライアント証明書と資源提供機関におけるローカルアカウントをマッピングするための元情報を管理し、資源提供機関に対し提供することで、HPCI 認証基盤システムの運用における業務工数の削減を目指す。

平成 23 年度には、ユーザのクライアント証明書利用における利便性の向上、柔軟性の維持のため、

- ・ UMS
- ・ MyProxy

の 2 種類の証明書リポジトリに対応する。また、クライアント証明書と資源提供機関におけるローカルアカウントをマッピングするための情報としては、

- ・ クライアント証明書の SubjectDN
- ・ UMS、MyProxy におけるローカルアカウント名
- ・ HPCI アカウントの eduPersonPrincipalName(以下 ePPN)

を管理するマッピング情報管理システムを構築する。以下では、平成 23 年度に構築、運用開始する証明書管理システムに求められる要件を示す。

証明書管理システムの構成およびその役割は下記のとおりである。

1. UMS

- ・ クライアント証明書の保管、管理を行う。
- ・ 認証局システムのクライアント機能を備え、クライアント証明書の取得においては認証局システムと連携する。また、クライアント証明書の発行要求の受付については、認証ポータルと連携する。
- ・ マッピング情報管理システムのクライアント機能を備え、マッピング情報登録においてはマッピング情報管理システムと連携する。

2. MyProxy

- ・ クライアント証明書の保管、管理を行う。
- ・ 認証局システムのクライアント機能を備え、クライアント証明書の取得においては認証局システムと連携する。また、クライアント証明書の発行要求の受付については、認証ポータルと連携する。
- ・ マッピング情報管理システムのクライアント機能を備え、マッピング情報登録においてはマッピング情報管理システムと連携する。

3. マッピング情報管理システム

- ・ クライアント証明書と資源提供機関におけるローカルアカウントをマッピングするための情報を保持、管理する。
- ・ 管理情報の取得においては、UMS サーバ、MyProxy サーバと連携する。
- ・ 資源提供機関に対しマッピング情報を提供する機能を備える。

3.3.2.1 ソフトウェア仕様

証明書管理システムのソフトウェア仕様は、以下のとおりである。

1. 証明書を格納するリポジトリとして、UMS と MyProxy の 2 つを構築すること。
2. ユーザの操作による認証ポータルから要求を受け、CA サーバに対しクライアント証

明書の発行要求が行えること。

3. 発行したクライアント証明書が保管できること。
4. ユーザの操作による認証ポータルから要求を受け、Proxy 証明書の発行が行えること。
5. 発行した Proxy 証明書を Proxy 証明書リポジトリに格納できること。
6. クライアント証明書を保管するための UMS 上のローカルアカウント名、EPPN、SubjectDN を紐付けした名寄せ情報が管理できること。
7. ユーザがクライアント証明書を発行した際、自動的に証明書発行通知メールを送信する機能を有すること。
8. 証明書発行通知メールの送信先は認証局管理者が任意に設定できること。
9. 証明書発行通知メールの送信先はドメイン単位での設定ができること。
10. 1 万人を超えるユーザが利用可能であり、全ユーザのクライアント証明書が格納できること。
11. HPCI 事務局が管理するデータベースを参照し、grid-mapfile の雛形となるファイルを作成できること。

3.3.2.2 ハードウェア仕様

証明書管理システムを運用するサーバのハードウェア仕様は以下のとおりである。

1. 物理サーバとすること。
2. UMS、MyProxy、マッピング情報管理システムは証明書管理システムとして同一サーバ上に構築すること。
3. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。また、プロセッサは冗長化すること。
4. ECC 機能に対応した 8GB 以上の容量のメモリを有すること。
5. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
6. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
7. 1000Base-T 規格の Ethernet インターフェースを 4 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
8. SAS 規格のストレージ接続インターフェースを有し、RAID5 相当のアレイ構成とすること。
9. ディスク装置を活線挿抜によって交換できること。
10. 実行容量が 500GB 以上の容量を持つストレージを内蔵し、ディスクの 15000rpm 以上のディスクを使用すること。

11. 電源ユニットおよびファンは冗長化すること。
12. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
13. VGA モニタおよび USB キーボード・マウスを接続できること。
14. 本体はラックに収容すること。
15. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。
16. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
17. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
18. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
19. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
20. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
21. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

3.3.2.3 セキュリティ仕様

1. ファイアウォールによる通信ポート制限を行うこと。
2. 最新の OS セキュリティパッチを適用すること。
3. アクセスログの採取が可能であること。

3.3.3 Shibboleth DS

Shibboleth DS は、HPCI アカウントを利用した認証時にユーザが HPCI アカウント IdP 運用機関を選択する機能を提供する。Shibboleth DS は、ユーザに表示する IdP 一覧にて、HPCI 内で利用可能な全ての HPCI アカウント IdP 運用機関のみを表示し、ユーザはこの中から利用する1つの運用機関を選択する。また、この選択は一定の日数の間、キャッシュされ、この期間内は IdP 一覧の表示は行わず、自動選択される。

3.3.3.1 ソフトウェア仕様

Shibboleth DS のソフトウェア仕様は以下のとおりである。

1. オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上

の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザー数無制限のサーバライセンスであること。

2. 仮想化環境上に構築する場合は、サーバに実装された CPU・主記憶装置・ストレージ・ネットワークを全て認識する仮想化基本ソフトウェアおよびライセンスを導入すること。尚、ゲスト OS は仮想化基本ソフトウェア上でサポート及び動作確認が行われている日本語対応のサーバ用 OS であること。
3. 将来的な Shibboleth DS の冗長化を考慮した設計とすること。
4. ソフトウェアとしては Shibboleth DS を使用し SAML による認証連携ができること。
5. 学術認証フェデレーションのメタデータを自動ダウンロードして、利用できること。
6. メタデータに登録されている IdP から、IdP 一覧に表示する IdP を選択できること。
7. 1 万人を超えるユーザが利用可能であり、200 回／分のトランザクションがあってもボトルネックにならないこと。

3.3.3.2 ハードウェア仕様

Shibboleth DS を運用するサーバのハードウェア仕様は以下のとおりである。

1. 物理サーバとする場合は下記の内容に従うこと。仮想サーバとして構築しても良いが、下記の内容と同等の性能を満たす環境とすること。
2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。また、プロセッサは冗長化すること。
3. ECC 機能に対応した 8GB 以上の容量のメモリを有すること。
4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
6. 1000Base-T 規格の Ethernet インターフェースを 4 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID0 もしくは RAID 1 相当のアレイ構成とすること。
8. ディスク装置を活線挿抜によって交換できること。
9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
10. 電源ユニットおよびファンは冗長化すること。
11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
12. VGA モニタおよび USB キーボード・マウスを接続できること。
13. 本体はラックに収容すること。

14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。
15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
18. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

3.3.3.3 セキュリティ仕様

1. ファイアウォールによる通信ポート制限を行うこと。
2. 最新の OS セキュリティパッチを適用すること。
3. アクセスログの採取が可能であること。

3.3.4 運用

認証局運用機関における運用体制および業務は以下の通りである。

3.3.4.1 体制仕様

1. 認証局システムにおける運用体制については、「3.3.1.4 認証局運用仕様」に記載している通りの体制とする。
2. その他、証明書管理システムおよび Shibboleth DS の管理者を一名以上用意すること。証明書管理システムと Shibboleth DS の管理者は同じ人物でも良い。また、認証局システムにおける認証局運用者と同じ人物でも良い。

3.3.4.2 業務仕様

1. 認証局システムにおける運用業務については、「3.3.1.4 認証局運用仕様」に記載している通りの業務とする。
2. 管理者は、証明書管理システムおよび Shibboleth DS を構築する際は、認証局運用者と連携しホスト証明書の取得を行うこと。

3. 管理者は、ホスト証明書の有効期限が切れる際には、認証局運用者と連携し、ホスト証明書の再取得を行うこと。

3.4 認証ポータル運用機関仕様

本節では、平成 23 年度に認証ポータル運用機関が整備すべきシステムとその運用に関する仕様を説明する。

認証ポータル運用機関は以下の 2 つのコンポーネントで構成し、運用する。

- ・ 認証ポータル
- ・ Proxy 証明書リポジトリ

以下に、認証ポータル運用機関について、ユーザ視点と管理者視点での概念図を示す。

【ユーザ視点】

ユーザは、認証ポータルに対して、ライセンス ID 発行要求（図中 1-* の処理）、クライアント証明書発行要求（図中 2-* の処理）、Proxy 証明書発行要求（図中 3-* の処理）を行う。また、Proxy 証明書リポジトリに対して Proxy 証明書のダウンロード（図中 4-* の処理）を行う。

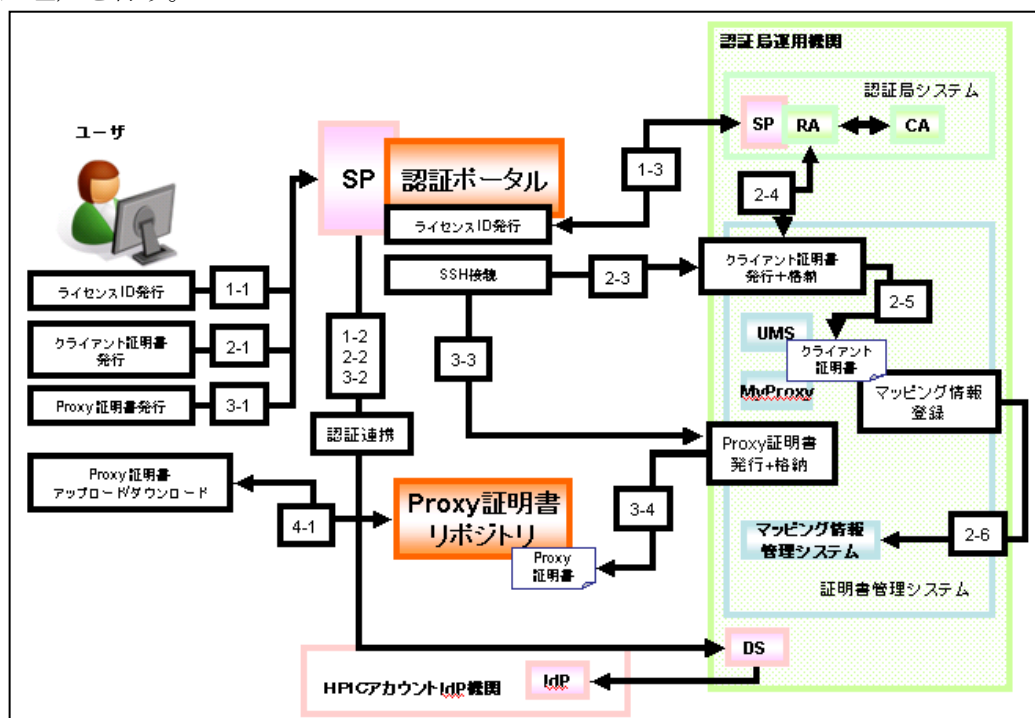


図 3.6 認証ポータル運用機関 概念図（ユーザ視点）

【管理者視点】

認証ポータル管理者は、データのバックアップ（図中 1-* の処理）、Shibboleth SP のメタデータの取得（図中 2-*）の処理を行う。

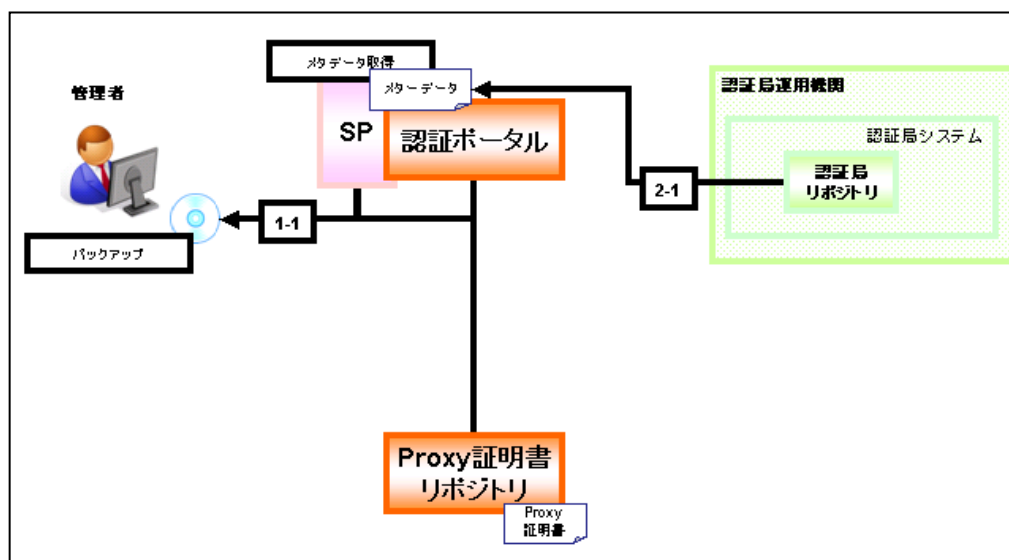


図 3.7 認証ポータル運用機関 概念図（管理者視点）

3.4.1 認証ポータル

認証ポータル運用機関は、ユーザがライセンス ID 発行、クライアント証明書発行、プロキシ証明書発行における Web インターフェースとして利用する認証ポータルサービスの運用業務を行う。

認証ポータルの利用では、HPCI アカウント IdP 運用機関、および商用プロバイダ等のユーザ管理機関と連携することで、認証ポータルの利用におけるユーザの利便性向上、運用工数の削減を目指す。ただし、HPCI アカウント IdP 運用機、商用プロバイダ等が管理するアカウントの認証レベル、および属性の保証レベルに対応した認証局の構成、運用の保証を行う。

平成 23 年度には、HPCI アカウント IdP 運用機関が発行する Shibboleth アカウントを用いた連携を行い、HPCI アカウント IdP 運用機関が管理する HPCI アカウントの保証レベルへの対応とする。以下では、平成 23 年度に構築、運用開始する認証ポータルに求められる要件を示す。

認証ポータルの構成およびその役割は下記のとおりである。

1. 認証ポータルサーバ

- ・ ユーザが Web アクセスし、ライセンス ID の発行、クライアント証明書の発行、Proxy 証明書を取得するためのインターフェースを備える。
- ・ 認証局システムと連携し、認証局システムに対しライセンス ID の発行要求を行う機能を備える。

- ・ 証明書管理システムと連携し、証明書発行システムに対して証明書発行要求や Proxy 証明書発行要求を行う機能を備える。
- ・ HPCI アカウント IdP 運用機関が運用する IdP と連携し、HPCI アカウントによる認証、および Shibboleth 属性値による認可を行う機能を備える。

3.4.1.1 ソフトウェア仕様

認証ポータルソフトウェア仕様は以下のとおりである。

1. ソフトウェアにグリッド配備・運用タスクフォースで使用されている Portal をベースとして改変したものを使用し、構築すること。
2. 仮想化環境上に構築、もしくは Proxy 証明書リポジトリと同サーバ上に構築しても良い。
3. オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザ数無制限のサーバライセンスであること。
4. 仮想化環境上に構築する場合は、サーバに実装された CPU・主記憶装置・ストレージ・ネットワークを全て認識する仮想化基本ソフトウェアおよびライセンスを導入すること。尚、ゲスト OS は仮想化基本ソフトウェア上でサポート及び動作確認が行われている日本語対応のサーバ用 OS であること。
5. SAML による認証連携ができること。ソフトウェアは Shibboleth SP を使用すること。
6. 学術認証フェデレーションのメタデータを自動ダウンロードして、利用できること。
7. ユーザが Web アクセスし、クライアント証明書を発行する際に使用するライセンス ID を取得するためのインターフェースを有すること。
8. ユーザが Web アクセスしライセンス ID を入力し、クライアント証明書を取得するためのインターフェースを有すること。
9. ユーザが Web アクセスし、発行したクライアント証明書をダウンロードするためのインターフェースを有すること。
10. Shibboleth の機能により受け取った属性を使用してクライアント証明書の発行を申請したユーザの英字名、英字性、HPCI-ID を含む CN が自動反映される設定とすること。
11. ユーザが Web アクセスしクライアント証明書を発行する際に、証明書の保管先に UMS もしくは MyProxy を任意に選択できること。
12. ユーザが Web アクセスし、証明書管理システムに保管した証明書を使用して Proxy 証明書を発行するためのインターフェースを有すること。
13. ユーザが Web アクセスし、発行した Proxy 証明書をダウンロードする機能を

有すること。

14. Shibboleth の機能により受け取った属性値を参照し、認証ポータルの利用における認可判定を自動的に行う機能を有すること。
15. SSL によるユーザからのアクセスに対応していること。
16. 1 万人を超えるユーザが利用可能であり、200 回／分のトランザクションがあってもボトルネックにならないこと。

3.4.1.2 ハードウェア仕様

認証ポータルを運用するサーバのハードウェア仕様は以下の通りである。

1. 物理サーバとする場合は下記の内容に従うこと。仮想サーバとして構築しても良いが、下記の内容と同等の性能を満たす環境とすること。また Proxy 証明書リポジトリと同一サーバ上に構築しても良い。
2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。
3. ECC 機能に対応した 8GB 以上の容量のメモリを有すること。
4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
6. 1000Base-T 規格の Ethernet インターフェースを 2 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID0 もしくは RAID 1 相当のアレイ構成とすること。
8. ディスク装置を活線挿抜によって交換できること。
9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
10. 電源ユニットおよびファンは冗長化すること。
11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
12. VGA モニタおよび USB キーボード・マウスを接続できること。
13. 本体はラックに収容すること。
14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。
15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、

同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。

17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
18. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

3.4.1.3 セキュリティ仕様

1. ファイアウォールによる通信ポート制限を行うこと。
2. 最新の OS セキュリティパッチを適用すること。
3. アクセスログの採取が可能であること。

3.4.2 Proxy 証明書リポジトリ

認証ポータル運用機関は、ユーザが Proxy 証明書を発行した際の保管先として Proxy 証明書リポジトリの運用業務を行う。

平成 23 年度には、ユーザによる認証ポータルの操作による Proxy 証明書の格納と、Globus Tool Kit 等を利用したローカル環境へのダウンロードおよびアップロードにも対応した環境とする。以下では、平成 23 年度に構築、運用開始する Proxy 証明書リポジトリに求められる要件を示す。

Proxy 証明書リポジトリの構成およびその役割は下記のとおりである。

1. MyProxy サーバ
 - ・ ユーザが認証ポータルを操作し発行した Proxy 証明書を格納する機能を備える。
 - ・ ユーザがローカル環境等に Proxy 証明書をダウンロードできる環境を備える。
 - ・ ユーザがローカル環境等で発行した Proxy 証明書を格納できる環境を備える。

3.4.2.1 ソフトウェア仕様

Proxy 証明書リポジトリのソフトウェア仕様は以下のとおりである。

1. ソフトウェアとしては MyProxy を使用すること。
2. 証明書管理システムで発行した Proxy 証明書が保管できること。
3. 仮想化環境上に構築、もしくは認証ポータルと同サーバ上に構築しても良い。

4. オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザー数無制限のサーバライセンスであること。
5. 仮想化環境上に構築する場合は、サーバに実装された CPU・主記憶装置・ストレージ・ネットワークを全て認識する仮想化基本ソフトウェアおよびライセンスを導入すること。もしくは認証ポータルと同一サーバ上に構築しても可とする。尚、ゲスト OS は仮想化基本ソフトウェア上でサポート及び動作確認が行われている日本語対応のサーバ用 OS であること。
6. 1 万人を超えるユーザーが利用可能であり、全ユーザーのクライアント証明書が格納できること。

3.4.2.2 ハードウェア仕様

Proxy 証明書リポジトリを運用するサーバのハードウェア仕様は以下のとおりである。

1. 物理サーバとする場合は下記の内容に従うこと。また認証ポータルと同一サーバ上に構築しても良い。仮想サーバとして構築しても良いが、下記の内容と同等の性能を満たす環境とすること。
2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。
3. ECC 機能に対応した 8GB 以上の容量のメモリを有すること。
4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
6. 1000Base-T 規格の Ethernet インターフェースを 2 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID0 もしくは RAID 1 相当のアレイ構成とすること。
8. ディスク装置を活線挿抜によって交換できること。
9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
10. 電源ユニットおよびファンは冗長化すること。
11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
12. VGA モニタおよび USB キーボード・マウスを接続できること。
13. 本体はラックに収容すること。
14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。

15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
18. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

3.4.2.3 セキュリティ仕様

1. ファイアウォールによる通信ポート制限を行うこと。
2. 最新の OS セキュリティパッチを適用すること。
3. アクセスログの採取が可能であること。

3.4.3 運用

認証ポータル運用機関における運用体制および業務は以下の通りである。

3.4.3.1 体制仕様

1. 認証ポータルの管理者、および Proxy 証明書リポジトリ管理者を一名以上用意すること。認証ポータルと Proxy 証明書リポジトリ管理者は同じ人物でも良い。

3.4.3.2 業務仕様

1. 管理者は、認証ポータルを構築する際には認証局運用機関に連絡し、ホスト証明書の取得を行うこと。
2. 管理者は、認証局運用機関から取得したホスト証明書を使用し、認証ポータルで使用する Shibboleth メタデータファイルを作成し、認証局運用機関に提出すること。
3. 管理者は、ホスト証明書の有効期限が切れる際には、認証局運用機関に対しホスト証明書の再取得を行うこと。
4. ホスト証明書を再取得した際、管理者は認証ポータルで使用するメタデータファイルも再作成し、再度認証局運用機関に提出すること。

3.5 HPCI アカウント IdP 運用機関仕様

本節では、平成 23 年度に HPCI アカウント IdP 運用機関が整備すべきシステムとその運用に関する仕様を説明する。

HPCI アカウント IdP 運用機関は以下の 1 つのコンポーネントで構成し、運用する。

- ・ HPCI アカウント IdP

以下に、HPCI アカウント IdP 運用機関について、ユーザ視点と管理者視点での概念図を示す。

【ユーザ視点】

ユーザは認証ポータル上でサインオンの手続きを行う。認証処理は、ユーザの HPCI アカウントを管理する HPCI アカウント IdP において行われる。

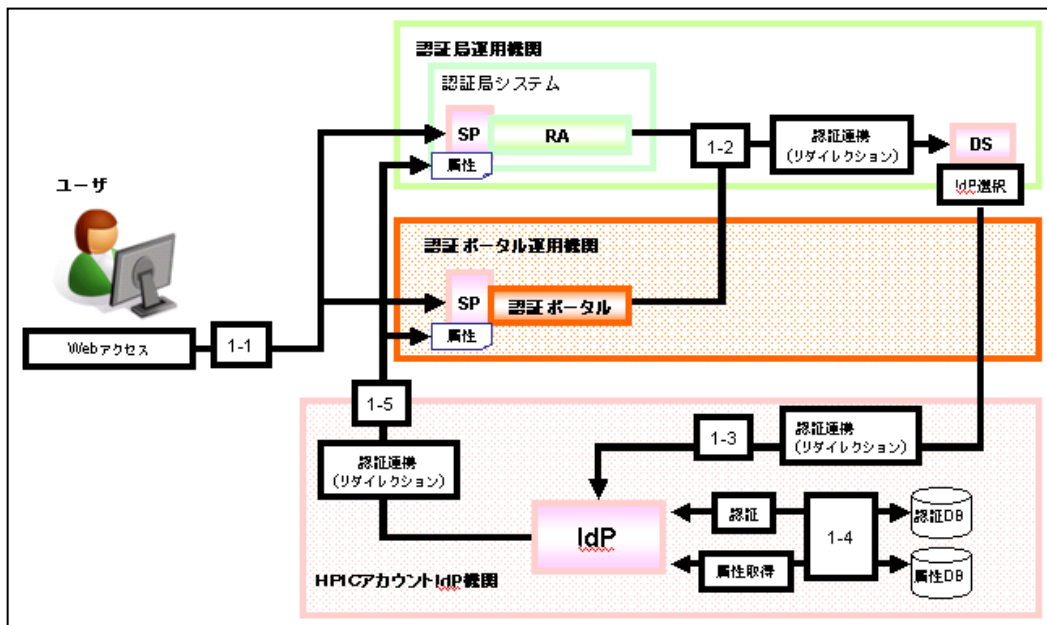


図 3.8 HPCI アカウント IdP 運用機関 概念図 (ユーザ視点)

【管理者視点】

HPCI アカウント IdP の管理者は、データのバックアップ (図中 1-*の処理)、HPCI アカウントの登録 (図中 2-*の処理) を行う。

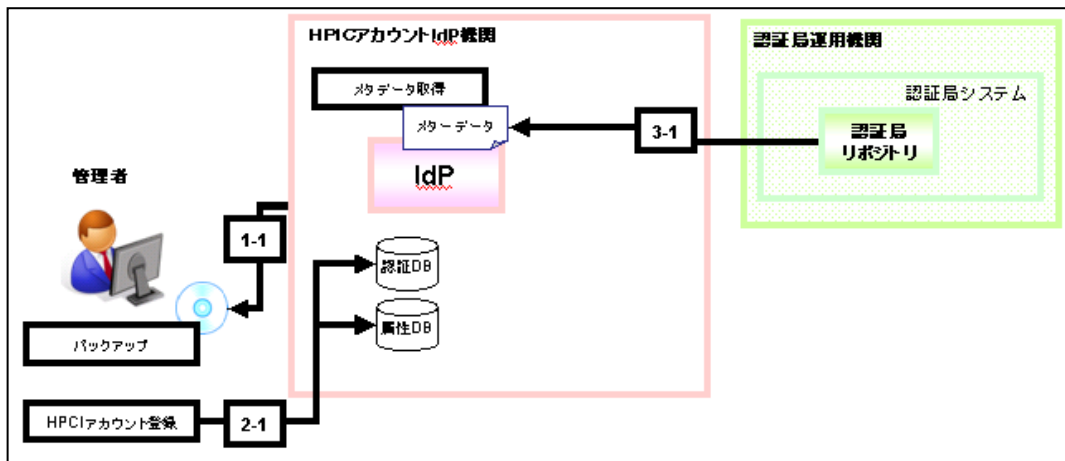


図 3.9 HPCI アカウント IdP 運用機関 概念図（管理者視点）

3.5.1 HPCI アカウント IdP

HPCI アカウント IdP 運用機関は HPCI で利用するための HPCI アカウントにおける

- ・ 登録
- ・ 変更
- ・ 失効
- ・ 削除

などの HPCI アカウント管理業務を行う。また、HPCI アカウント管理のための HPCI アカウント IdP の運用業務を行う。また、HPCI アカウント IdP の認証 DB および属性 DB の運用業務を行う。認証 DB としては LDAP、Windows ADS、Kerberos のいずれか、属性 DB としては LDAP、Windows ADS、リレーショナル DB のいずれか、を運用する必要がある。

平成 23 年度には、認証局システムおよび認証ポータルと連携し、IdP に登録した HPCI アカウントを利用時のシングルサインオン環境を実現する。以下では、平成 23 年度に構築、運用開始する HPCI アカウント IdP に求められる要件を示す。

HPCI アカウント IdP の構成およびその役割は下記のとおりである。

1. HPCI アカウント IdP サーバ

- ・ 認証局システムと連携し、認証 DB に登録された HPCI アカウントによる認証を行う機能を備える。また、属性 DB に登録された属性情報を受け渡す機能を備える。
- ・ 認証ポータルと連携し、認証 DB に登録された HPCI アカウントによる認証を行う機能を備える。また、属性 DB に登録された属性情報を受け渡す機能を備える。

2. 認証 DB サーバ

- ・ HPCI アカウント IdP と連携できる、LDAP/Windows ADS/Kerberos/の

いずれかの機能を備える。

- HPCI アカウントの認証情報を管理する。
- 尚、既に同様のシステムを運用している場合は既存システムを利用しても良い。

3. 属性 DB サーバ

- HPCI アカウント IdP と連携できる、LDAP/Windows ADS/リレーショナル DB のいずれかの機能を備える。
- HPCI アカウントの属性情報を管理する。
- 尚、既に同様のシステムを運用している場合は既存システムを利用しても良い。ただし、その場合にも必要な属性を全て管理していること。

3.5.1.1 ソフトウェア仕様

HPCI アカウント IdP のソフトウェア仕様は以下のとおりである。

1. ソフトウェアとして Shibboleth IdP を使用し、SAML による認証連携が行えること。
2. オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザー数無制限のサーバライセンスであること。
3. 仮想化環境上に構築する場合は、サーバに実装された CPU・主記憶装置・ストレージ・ネットワークを全て認識する仮想化基本ソフトウェアおよびライセンスを導入すること。尚、ゲスト OS は仮想化基本ソフトウェア上でサポート及び動作確認が行われている日本語対応のサーバ用 OS であること。
4. 認証 DB として LDAP、ADS、Kerberos のいずれかが利用できること。
5. 属性 DB として LDAP、ADS、リレーショナル DB のいずれかが利用できること。
6. 学術認証フェデレーションからメタデータ情報が自動で取得できること。
7. Shibboleth SP である認証局および認証ポータルに対し、
 - ”英字姓”
 - ”英字名”
 - ”HPCI-ID”
 - ”eduPersonPrincipalName”
 - ”eduPersonEntitlement”の情報を受け渡せること。
8. 1 万人を超えるユーザーが利用可能であり、200 回／分のトランザクションがあってもボトルネックにならないこと。
9. 学認と連携する同組織内の IdP と異なるセキュリティ・ドメインを設定すること。
10. 当面、下記の属性を送信しないこと。

- (1) organizationName “o”
- (2) jaOrganizationName “jao”
- (3) organizationalUnitName “ou”
- (4) jaOrganizationalUnitName “jaou”

3.5.1.2 ハードウェア仕様

Shibboleth IdP を運用するサーバのハードウェア仕様は以下のとおりである。

1. 物理サーバとする場合は下記の内容に従うこと。仮想サーバとして構築しても良いが、下記の内容と同等の性能を満たす環境とすること。
2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。
3. ECC 機能に対応した 8GB 以上の容量のメモリを有すること。
4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
6. 1000Base-T 規格の Ethernet インターフェースを 2 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID0 もしくは RAID 1 相当のアレイ構成とすること。
8. ディスク装置を活線挿抜によって交換できること。
9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
10. 電源ユニットおよびファンは冗長化すること。
11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
12. VGA モニタおよび USB キーボード・マウスを接続できること。
13. 本体はラックに収容すること。
14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。
15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。

18. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

3.5.1.3 セキュリティ仕様

1. ファイアウォールによる通信ポート制限を行うこと。
2. 最新の OS セキュリティパッチを適用すること。
3. アクセスログの採取が可能であること。

3.5.2 運用

HPCI アカウント IdP 運用機関における運用体制および業務は以下の通りである。

3.5.2.1 体制仕様

1. HPCI アカウント IdP の管理者を一名以上用意すること。

3.5.2.2 業務仕様

1. 管理者は、HPCI アカウント IdP を構築する際には認証局運用機関に連絡し、ホスト証明書の取得を行うこと。
2. 管理者は、認証局運用機関から取得したホスト証明書を使用し、HPCI アカウント管理 IdP で使用する Shibboleth メタデータファイルを作成し、認証局運用機関に提出すること。
3. 管理者は、ホスト証明書の有効期限が切れる際には、認証局運用機関に対しホスト証明書の再取得を行うこと。
4. ホスト証明書を再取得した際、管理者は HPCI アカウント IdP で使用するメタデータファイルも再作成し、再度認証局運用機関に提出すること。
5. 管理者は、HPCI アカウント IdP の認証 DB として、LDAP、ADS、Kerberos のいずれかを準備、運用すること。認証 DB として、既存のシステムを利用することも可とする。
6. 管理者は、HPCI アカウント IdP の属性 DB として、LDAP、ADS、リレーショナル DB のいずれかを準備、運用すること。属性 DB として、既存のシステムを利用することも可とする。ただし、既存のシステムを利用する場合にも HPCI 環境の利用に必要な属性項目は全て管理すること。
7. 管理者は、HPCI 基本仕様が定める運用フローに従い、HPCI 事務局からの連

絡を受け、HPCI アカウントの登録処理を行うこと。

8. 管理者は HPCI アカウントの登録処理が完了した際には、ユーザに HPCI アカウント情報を通知すること。
9. 管理者は、HPCI 基本仕様が定める運用フローに従い、HPCI 事務局からの連絡を受け、HPCI アカウントの失効処理を行うこと。
10. 管理者は HPCI アカウントの失効処理が完了した際には、ユーザに HPCI アカウントの失効を通知すること。
11. 管理者は、HPCI 基本仕様に定められる運用フローに従い、HPCI 事務局からの連絡を受け、HPCI アカウントの削除処理を行うこと。
12. 管理者は HPCI アカウントの削除処理が完了した際には、ユーザに HPCI アカウントの削除を通知すること。
13. 学術認証フェデレーションに参加する IdP として、学術認証フェデレーション システム運用基準にしたがった運用を行うこと。

3.6 資源提供機関仕様

本節では、平成 23 年度に資源提供機関が整備すべきシステムとその運用に関する仕様を説明する。

資源提供機関は GSI 認証機能を持つミドルウェアで構成し、運用する。ミドルウェアとしては、下記の 2 つを想定する

- ・ GSI-SSH
- ・ Gfarm

以下に、資源提供機関について、ユーザ視点と管理者視点での概念図を示す。

【ユーザ視点】

ユーザは、認証ポータル上でのシングルサインオン後、資源提供機関の計算機に GSI-SSH を用いてログインする（図中 1-* の処理）。

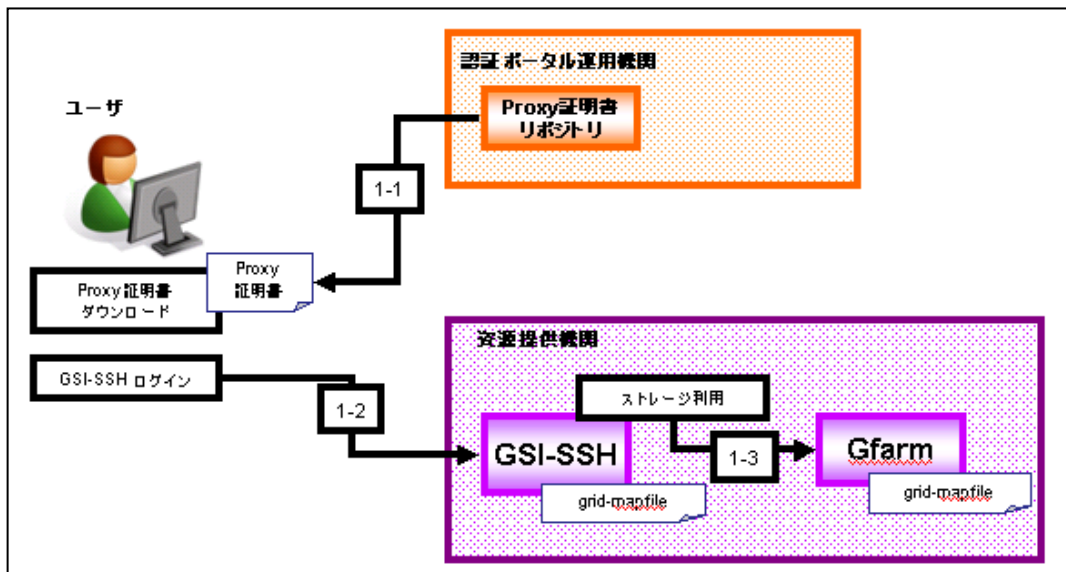


図 3.10 資源提供機関 概念図（ユーザ視点）

【管理者視点】

資源提供機関の管理者は、データのバックアップ（図中 1-*の処理）、ローカルアカウントの登録および grid-mapfile 管理（図中 2-*の処理）を行う。

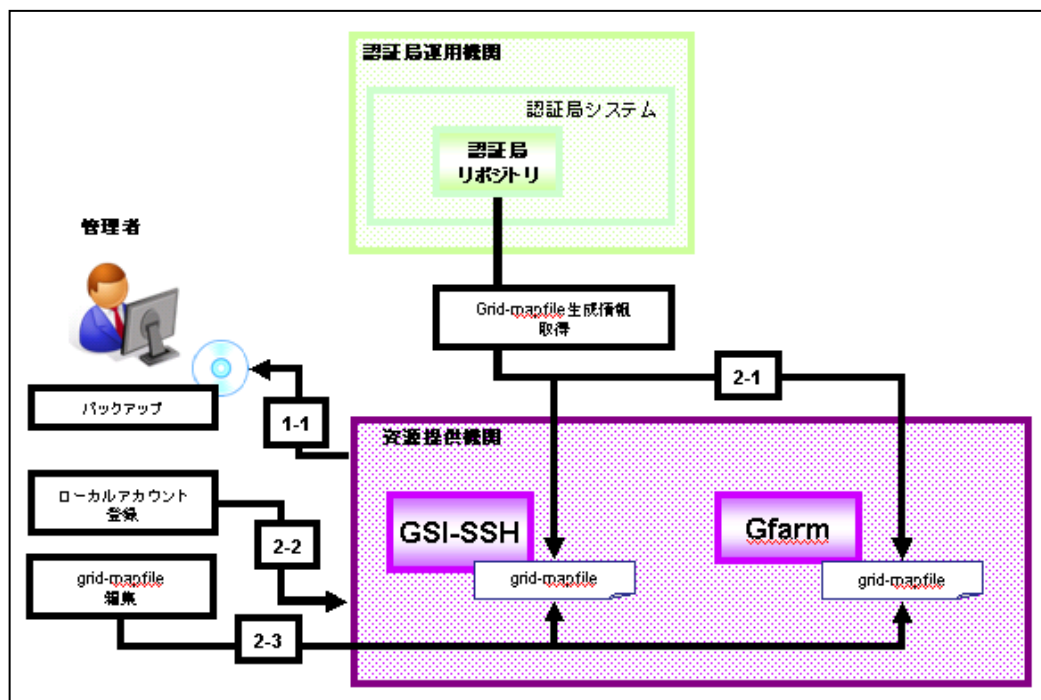


図 3.11 資源提供機関 概念図（管理者視点）

3.6.1 GSI-SSH

資源提供機関は認証ポータルで発行した Proxy 証明書を利用した SSH ログインが可能な GSI-SSH の運用業務を行う。

平成 23 年度には、GSI-SSH 環境の整備と、GSI-SSH でログイン後に使用されるローカルアカウントの管理、証明書の SubjectDN とローカルアカウントをマッピングするための grid-mapfile の管理を行う。grid-mapfile の管理においては、認証局運用機関の証明書管理システムより提供される情報を元に行う。以下では、平成 23 年度に構築、運用開始する GSI-SSH に求められる要件を示す。

GSI-SSH の構成およびその役割は下記のとおりである。

1. GSI-SSH サーバ

- Proxy 証明書を使用した GSI 認証による SSH ログイン機能を備える。
- 証明書の SubjectDN とローカルアカウントをマッピングするための grid-mapfile を有する。
- 証明書管理システムと連携し、マッピング情報を自動で取得する機能を備える。

3.6.1.1 ソフトウェア仕様

GSI-SSH のソフトウェア仕様は以下のとおりである。

1. ソフトウェアとしては GSI-SSH を使用し、GSI 認証による SSH ログインができること。
2. オペレーティングシステムは、Red Hat Enterprise Linux 6 for Server 相当以上の機能を有すると判断され、日本語対応であること。併せて、ライセンスは、ユーザー数無制限のサーバライセンスであること。
3. 仮想化環境上に構築する場合は、サーバに実装された CPU・主記憶装置・ストレージ・ネットワークを全て認識する仮想化基本ソフトウェアおよびライセンスを導入すること。もしくは認証ポータルと同一サーバ上に構築しても可とする。尚、ゲスト OS は仮想化基本ソフトウェア上でサポート及び動作確認が行われている日本語対応のサーバ用 OS であること。
4. 1 万人を超えるユーザが利用可能あり、200 回／分のトランザクションがあってもボトルネックにならないこと。

3.6.1.2 ハードウェア仕様

GSI-SSH を運用するサーバのハードウェア仕様は以下のとおりである。

1. 物理サーバとする場合は下記の内容に従うこと。仮想サーバとして構築しても良いが、下記の内容と同等の性能を満たす環境とすること。
2. Intel 社のマルチコア Xeon E5503 2GHz 相当以上の性能・機能を有すると判断されるプロセッサを搭載していること。

3. ECC 機能に対応した 8GB 以上の容量のメモリを有すること。
4. CD-ROM および DVD-ROM を利用可能な、内蔵もしくは USB2.0 で接続されたドライブを有すること。
5. USB メモリを USB2.0 インターフェースを介して接続し、起動および BIOS のアップデートが可能であること。プラグアンドプレイに対応していること。
6. 1000Base-T 規格の Ethernet インターフェースを 2 回線有すること。また、トランク機能によって論理的に単一インターフェースとして稼働できること。
7. SATA または SAS 規格のストレージ接続インターフェースを有し、RAID0 もしくは RAID 1 相当のアレイ構成とすること。
8. ディスク装置を活線挿抜によって交換できること。
9. 実行容量が 300GB 以上の容量を持つストレージを内蔵すること。
10. 電源ユニットおよびファンは冗長化すること。
11. BIOS の設定は、商用電源喪失後も 60 日間以上維持されること。
12. VGA モニタおよび USB キーボード・マウスを接続できること。
13. 本体はラックに収容すること。
14. ラックに収容可能な、画面サイズが対角 15 インチ、1,024×768 ピクセル以上のカラー液晶ディスプレイ、JIS 配列 109 キーボードおよび 3 ボタン式マウスを有すること。
15. 同じラックにマウントされるサーバは、KVM 切り替え装置によってモニタ、キーボードおよびマウスを共用すること。KVM 切り替え機に遠隔から接続できる機能を有すること。
16. ラックマウント型の無停電電源装置を有し、瞬電対応が可能であること。尚、同じラックにマウントされるサーバは、無停電電源装置を共有してもよい。
17. 停電時には稼働中のオペレーティングシステムにシャットダウンを促し、BIOS が電源切断を行うまで、電源供給ができること。
18. 復電時には、切断時に稼働していたオペレーティングシステムを再起動し、運用状態を復元できること。
19. スケジュール機能により、自動的にシャットダウン、再起動する機能を有すること。
20. 冗長化されている構成要素がある場合、それぞれの構成要素に故障が発生した場合に、管理者にメールを送信するなど外部に報告する機能を有すること。

3.6.1.3 セキュリティ仕様

1. ファイアウォールによる通信ポート制限を行うこと。
2. 最新の OS セキュリティパッチを適用すること。
3. アクセスログの採取が可能であること。

3.6.2 Gfarm

ストレージ利用のための基本仕様編にて定める。

3.6.3 grid-mapfile 自動生成ツール

資源提供機関は、GSI-SSH および Gfarm の運用で必要となる grid-mapfile の管理業務を行う。grid-mapfile の管理は、認証局運用機関の証明書管理システムで提供される情報を元に行う。

平成 23 年度には、証明書管理システムで提供される情報を自動で取得し、grid-mapfile の雛形として利用できるファイルとして設置するための grid-mapfile 自動生成ツールを提供する。当該ツールを、grid-mapfile が必要なサーバ上に設置し実行することで grid-mapfile の管理を行う。尚、最終的なローカルアカウントとの紐付けによる grid-mapfile の作成は、各資源提供機関の手法に委ねる。

以下では、平成 23 年度に使用する grid-mapfile 自動生成ツールに求められる要件を示す。

grid-mapfile 自動生成ツールの機能は下記のとおりである。

1. grid-mapfile 自動生成ツール

- ・ 証明書管理システムに接続し、SubjectDN と ePPN の情報を取得する機能を備える。
- ・ 証明書管理システムから取得した情報を grid-mapfile と同じフォーマットのファイルとして設置する機能を備える。

3.6.4 運用

資源提供機関における運用体制および業務は以下の通りである。

3.6.4.1 体制仕様

1. 資源提供機関の管理者として一名以上用意すること。

3.6.4.2 業務仕様

1. 管理者は、GSI-SSH 環境を構築する際には認証局運用機関に連絡し、ホスト証明書の取得を行うこと。
2. 管理者は、Gfarm 環境を構築する際には認証局運用機関に連絡しホスト証明書とサービス証明書の取得を行うこと。
3. 管理者は、ホスト証明書の有効期限が切れる際には、認証局運用機関に対しホスト証明書の再取得を行うこと。
4. 管理者は、サービス証明書の有効期限が切れる際には、認証局運用機関に対しサービス証明書の再取得を行うこと。

5. 管理者は、HPCI 基本仕様が定める運用フローに従い、HPCI 事務局からの連絡を受け、ローカルアカウントの登録処理を行うこと。
6. 管理者は、ローカルアカウントの登録処理が完了した際には、ユーザにアカウント情報を通知すること。
7. 管理者は、ローカルアカウントの登録処理が完了した際には、HPCI アカウントとローカルアカウントをマッピングするため情報を `grid-mapfile` へ追加すること。
8. 管理者は、HPCI 基本仕様が定める運用フローに従い、HPCI 事務局からの連絡を受け、ローカルアカウントの失効処理を行うこと。
9. 管理者はローカルアカウントの失効処理が完了した際には、ユーザにローカルアカウントの失効を通知すること。
10. 管理者は、HPCI アカウントとローカルアカウントをマッピングするため情報を `grid-mapfile` から削除すること。
11. 管理者は、HPCI 基本仕様が定める運用フローに従い、HPCI 事務局からの連絡を受け、ローカルアカウントの削除処理を行うこと。
12. 管理者は HPCI アカウントの削除処理が完了した際には、ユーザにローカルアカウントの削除を通知すること。
13. 管理者は、構築したサーバ上に認証局証明書の配置を行うこと。
14. 管理者は、認証局運用機関が公開する CRL を定期的にダウンロードすること。

3.7 今後の検討課題

本節では、平成 24 年度以降での実現に向け、平成 23 年度中に検討すべき事項について記載する。

3.7.1 シナリオ検討

本仕様書で示したシナリオ B、C および D については、平成 24 年度以上の実現に向けて、各シナリオの認証方法に対するユーザからのニーズおよび実装技術に関する調査を進めるとともに、実現のためのアーキテクチャおよびスケジュールに関する検討を行う予定である。各シナリオに関する主要な検討項目は、以下のとおりである。

➤ シナリオ B

- ・ ソフトウェア仕様の検討(OpenID 対応認証ポータル)
- ・ 運用規定(OpenID プロバイダ、認証局)
- ・ 運用開始時期

➤ シナリオ C

- ・ ソフトウェア仕様の検討(OpenID 対応認証ポータル、OpenID からローカルアカウントへのマッピング)

- ・ 運用規定(OpenID プロバイダ)
- ・ 運用開始時期

➤ シナリオ D

- ・ 運用規定(学認経由で利用可能なサービスプロバイダ、課金など)
- ・ 運用開始時期

3.7.2 クライアント証明書発行

本仕様書が示す仕様では、ユーザがクライアント証明書を発行するために図 2.4.2 に示す 2 段階の操作を行う必要がある。この仕様は、クライアント証明書発行におけるセキュリティをより強固にできる一方で、ユーザの手間が増えるという問題もある。技術的には、1 回の操作（例えばワンクリック操作）でクライアント証明書発行を実現することは可能であるが、セキュリティ強度は低下する。以上の点を考慮し、クライアント証明書発行方法については、セキュリティ面での検討を開始し、ユーザの利便性とセキュリティのトレードオフを考慮した方法を策定する予定である。

3.7.3 簡易ファイルアクセスのための認証基盤アーキテクチャ

HPCI 基本仕様の検討段階において、Samba や http 経由でユーザがファイルへアクセスする機能へのニーズが示されている。平成 23 年度に実現する GSI 認証を用いた実装では、このニーズに直接対応することはできないため、現在、ファイルアクセスのためのアクセスポイントを設け、本アクセスポイント経由でファイルアクセスを実現する方法を検討している。今後、この案を含む対応案を検討するとともに、先端ソフトウェア運用基盤上で実証実験を行う予定である。

3.7.4 グループ管理

HPCI では、利用が承認された課題に基づいてユーザが決定されるため、資源へのアクセス制御等の認可処理を課題毎に行うことが必要である。これを実現するため、ユーザのグループ管理のモデルやグループ毎の資源の利用方法(ストレージアクセス制御や計算ジョブ実行時のグループ指定の方法等)について、付録に示す情報基盤センター群グループ管理の結果を考慮しながら、検討を進める予定である。

4 ドキュメント&システム開発整備（発注仕様）

4.1 認証基盤導入および運用手引き仕様

本節では、認証基盤におけるドキュメント整備に関する仕様を示す。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、改版内容について報告し、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。

4.1.1 認証局運用機関におけるシステムおよびドキュメント整備に関する仕様

認証局運用機関におけるシステム導入および運用に必要なドキュメントとして、以下を作成すること。

1. 認証局システム構成仕様書
 - 1-1. CA システムハードウェア構成情報を記載すること。
 - 1-2. CA システムソフトウェア構成を記載すること。
 - 1-3. RA システムハードウェア構成を記載すること。
 - 1-4. RA システムソフトウェア構成を記載すること。
 - 1-5. 認証局システムに関連するネットワーク構成を記載すること。
 - 1-6. 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。
2. 認証局運用規定(以下、CP/CPS)
 - 2-1 HPCI 基本仕様書に基づいて、関係者との協議・調整し、MICS プロファイルに対応した CP/CPS を作成すること。
 - 2-2 詳細な内容については発注者と協議の上、決定すること。

- 2-3 関連する機関との調整全般を全て行うこと。
- 2-4 CP/CPS 作成に関わる会議には全て出席し報告を行うこと。
- 2-5 CP/CPS 作成までに使用する下記の資料を合わせて納入すること。

要件定義書
会議議事録
課題管理表

3. 認証局システム管理者マニュアル

- 3-1 管理者が短時間で構成と機能およびそれら进行操作する方法が把握できる内容となっていること。
- 3-2 認証局システム（ソフトウェア）の導入方法について記載すること。
- 3-3 クライアント証明書の発行および失効など、クライアント証明書の管理業務について記載すること。
- 3-4 ホスト証明書の発行および失効など、ホスト証明書の管理業務について記載すること。
- 3-5 サービス証明書の発行および失効など、サービス証明書の管理業務について記載すること。
- 3-6 年度更新処理の業務について記載すること。
- 3-7 システムバックアップや障害発生時の復旧手順など保守業務について記載すること。
- 3-8 バックアップ等の保管業務について記載すること。
- 3-9 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。

4. 証明書管理システム構成仕様書(UMS, MyProxy)

- 4-1 UMS サーバハードウェア構成情報を記載すること。
- 4-2 UMS サーバソフトウェア構成を記載すること。
- 4-3 MyProxy サーバハードウェア構成を記載すること。
- 4-4 MyProxy サーバソフトウェア構成を記載すること。
- 4-5 マッピング情報管理システムハードウェア構成を記載すること。
- 4-6 マッピング情報管理システムサーバソフトウェア構成を記載すること。
- 4-7 証明書管理システムに関連するネットワーク構成を記載すること。
- 4-8 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. 証明書管理システム管理者マニュアル(UMS, MyProxy)

- 5-1 管理者が短時間で構成と機能およびそれら进行操作する方法が把握できる内容となっていること。

- 5-2 証明書管理システム（ソフトウェア）の導入方法について記載すること。
- 5-3 証明書の発行業務について記載すること。
- 5-4 証明書の失効業務について記載すること。
- 5-5 年度更新処理の業務について記載すること。
- 5-6 システムバックアップや障害発生時の復旧手順など保守業務について記載すること。
- 5-7 バックアップ等の保管業務について記載すること。
- 5-8 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。

6. Shibboleth DS 管理者マニュアル

- 6-1. 管理者が短時間で構成と機能およびそれら进行操作する方法が把握できる内容となっていること。
- 6-2. Shibboleth DS（ソフトウェア）の導入方法について記載すること。
- 6-3. メタデータの更新業務について記載すること。
- 6-4. 年度更新処理の業務について記載すること。
- 6-5. システムバックアップや障害発生時の復旧手順など保守業務について記載すること。
- 6-6. バックアップ等の保管業務について記載すること。
- 6-7. 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。

7. 認証局ユーザマニュアル

- 7-1 利用者が短時間で機能およびそれら进行操作する方法が把握できる内容となっていること。
- 7-2 ライセンス ID の発行操作方法について記載すること。
- 7-3 クライアント証明書の発行操作について記載すること。
- 7-4 HPCI アカウントにおける認証方法について記載すること。
- 7-5 属性値による認可についてもユーザに分かり易く説明を記載すること。

4.1.2 認証ポータル運用機関におけるドキュメント整備に関する仕様

認証ポータル運用機関におけるシステム導入および運用に必要なドキュメントとして、以下を作成すること。

1. 認証ポータル構成仕様書

- 1-1 認証ポータルハードウェア構成情報を記載すること。

- 1-2 認証ポータルソフトウェア構成を記載すること。
- 1-3 認証ポータルに関連するネットワーク構成を記載すること。
- 1-4 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。

2. 認証ポータル管理者マニュアル

- 2-1 管理者が短時間で構成と機能およびそれら进行操作する方法が把握できる内容となっていること。
- 2-2 認証ポータル（ソフトウェア）の導入方法について記載すること。
- 2-3 メタデータの更新業務に発行業務について記載すること。
- 2-4 年度更新処理の業務について記載すること。
- 2-5 システムバックアップや障害発生時の復旧手順など保守業務について記載すること。
- 2-6 バックアップ等の保管業務について記載すること。
- 2-7 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。

3. Proxy 証明書リポジトリ構成仕様書

- 3-1 Proxy 証明書リポジトリハードウェア構成情報を記載すること。
- 3-2 Proxy 証明書リポジトリソフトウェア構成を記載すること。
- 3-3 Proxy 証明書リポジトリに関連するネットワーク構成を記載すること。
- 3-4 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。

4. Proxy 証明書リポジトリ管理者マニュアル

- 4-1 管理者が短時間で構成と機能およびそれら进行操作する方法が把握できる内容となっていること。
- 4-2 Proxy 証明書リポジトリ（ソフトウェア）の導入方法について記載すること。
- 4-3 Proxy 証明書の管理業務について記載すること。
- 4-4 年度更新処理の業務について記載すること。
- 4-5 システムバックアップや障害発生時の復旧手順など保守業務について記載すること。
- 4-6 バックアップ等の保管業務について記載すること。
- 4-7 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. 認証ポータルユーザマニュアル

- 5-1 利用者が短時間で機能およびそれら进行操作する方法が把握できる内容となっていること。

- 5-2 ライセンス ID の発行操作方法について記載すること。
- 5-3 クライアント証明書の発行操作方法について記載すること。
- 5-4 Proxy 証明書の発行操作方法について記載すること。
- 5-5 HPCI アカウントにおける認証方法について記載すること。
- 5-6 属性値による認可についてもユーザに分かり易く説明を記載すること。

6. Proxy 証明書リポジトリユーザマニュアル

- 6-1 利用者が短時間で機能およびそれら进行操作する方法が把握できる内容となっていること。
- 6-2 Proxy 証明書のダウンロード方法について記載すること。
- 6-3 Proxy 証明書のアップロード方法について記載すること。

4.1.3 HPCI アカウント IdP 運用機関におけるドキュメント整備に関する仕様

HPCI アカウント IdP 運用機関におけるシステム導入および運用に必要なドキュメントとして、以下を作成すること。

1. HPCI アカウント IdP 構成仕様書

- 1-1 HPCI アカウント IdP ハードウェア構成情報を記載すること。
- 1-2 HPCI アカウント IdP ソフトウェア構成を記載すること。
- 1-3 HPCI アカウント IdP に関連するネットワーク構成を記載すること。
- 1-4 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。

2. HPCI アカウント IdP 管理者マニュアル

- 2-1 管理者が短時間で構成と機能およびそれら进行操作する方法が把握できる内容となっていること。
- 2-2 HPCI アカウント IdP の導入方法について記載すること。
- 2-3 HPCI アカウントの発行業務について記載すること。
- 2-4 HPCI アカウントの失効業務について記載すること。
- 2-5 HPCI アカウントの削除業務について記載すること。
- 2-6 メタデータの更新業務に発行業務について記載すること。
- 2-7 年度更新処理の業務について記載すること。
- 2-8 システムバックアップや障害発生時の復旧手順など保守業務について記載すること。
- 2-9 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。

4.1.4 資源提供機関におけるドキュメント整備に関する仕様

資源提供機関におけるシステム導入および運用に必要なドキュメントとして、以下を作成すること。

1. GSI-SSH システム構成仕様書

- 1-1 GSI-SSH システムハードウェア構成情報を記載すること。
- 1-2 GSI-SSH システムソフトウェア構成を記載すること。
- 1-3 GSI-SSH システムに関連するネットワーク構成を記載すること。
- 1-4 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。

2. GSI-SSH システム管理者マニュアル

- 2-1 管理者が短時間で構成と機能およびそれら进行操作する方法が把握できる内容となっていること。
- 2-2 GSI-SSH 環境（ソフトウェア）の導入方法について記載すること。
- 2-3 grid-mapfile の管理業務について記載すること。
- 2-4 CRL の取得、管理業務について記載すること。
- 2-5 システムバックアップや障害発生時の復旧手順など保守業務について記載すること。
- 2-6 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。

3. GSI-SSH システムユーザマニュアル

- 3-1 利用者が短時間で機能およびそれら进行操作する方法が把握できる内容となっていること。
- 3-2 Proxy 証明書のダウンロード方法について記載すること。
- 3-3 Proxy 証明書のアップロード方法について記載すること。
- 3-4 GSI-SSH によるログイン方法について記載すること。
- 3-5 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。

4.2 システム開発仕様

本節では、認証基盤におけるソフトウェア開発に関する仕様を示す。

4.2.1 認証ポータル開発仕様

認証ポータルは、認証局システムおよび証明書管理システムと連携し、ライセンス ID 発行、クライアント証明書発行、プロキシ証明書発行をユーザが行うための Web サービスである。また、Shibboleth 認証に対応し、ユーザが HPCI アカウントによる

認証、属性値による認可を行うための機能を備える。以下に、認証ポータルの開発における要求要件について記載する。

1. ソフトウェアにグリッド配備・運用タスクフォースで使用されている Portal をベースとして改変したものを使用すること。
2. 認証ポータルに必要な機能を明確化し、5.7.5.1 に示す要求仕様に基づいて詳細設計および開発を行うこと。
3. 認証ポータルと連携が必要な認証局システム、証明書管理システム、Proxy 証明書リポジトリの機能や動作を十分に考慮し設計を行うこと。
4. 画面設計等は十分に発注者と協議し、ユーザが利用し易いインターフェースにすること。
5. 不明な点がある場合は発注者と協議の上、決定すること。
6. 協議の上、確定した設計および利用する技術の実現性においては、事前に同等環境を構築し、評価を行うこと。このとき、評価環境は受託業者側で用意すること。

4.2.1.1 要求仕様

1. SAML による認証連携ができること。ソフトウェアは Shibboleth SP を使用すること。
2. Shibboleth の機能により受け取った属性値を参照し、認証ポータルの利用における認可判定を自動的に行う機能を有すること。尚、認可に使用する属性と値は管理者が任意に設定できること。
3. SSL によるユーザからのアクセスに対応していること。
4. 認証局システムと連携しライセンス ID を取得するためのインターフェースを有し、認証局システムとの連携機能を備えること。
5. クライアント証明書を取得するためのインターフェースを有し、認証局システムおよび証明書管理システムとの連携機能を備えること。
6. クライアント証明書発行には、下記の入力を必須とすること。
 - ・ ライセンス ID
 - ・ 秘密鍵パスフレーズ
 - ・ 秘密鍵パスフレーズ（確認用）
7. 4 の項目と合わせて、クライアント証明書の保存先として UMS もしくは MyProxy、download のいずれかを任意にユーザが選択できること。
8. Shibboleth の機能により受け取った属性を使用し、クライアント証明書の CN として設定する値を自動生成する機能を備えること。ただし、CN の自動生成に使用する属性の値に不足があった場合はクライアント証明書が発行できないこと。

9. 証明書管理システムと連携し、自動生成した CN が既に使用されていなか重複チェックを自動で行なう機能を備えること。CN が重複していた場合はクライアント証明書が発行できないこと。
10. 自動生成した CN の値は、ユーザが確認できるようクライアント証明書発行前に表示する機能を備えること。
11. CN 自動生成に使用する属性とフォーマットは管理者が任意に設定できること。
12. 自動的に設定された CN 情報は 4 の項目と合わせて表示できること。
13. 証明書管理システムに保管した証明書を使用して **Proxy** 証明書を発行するためのインターフェースを有し、**MyProxy** との連携機能を備えること。
14. **Proxy** 証明書発行には、下記の入力を必須とすること。
 - ・ 秘密鍵パスフレーズ
 - ・ **Proxy** 証明書格納パスフレーズ
 - ・ **Proxy** 証明書格納パスフレーズ（確認用）
 - ・ (VO 名)
 - ・ (グループ名)
 - ・ (ロール名)
15. アクセスログを出力し、下記の情報が確認できること。
 - ・ 接続ユーザの HPCI-ID
 - ・ 接続ユーザの ePPN
 - ・ 接続ユーザの認可判定結果
 - ・ ライセンス ID を発行した場合の記録
 - ・ クライアント証明書を発行した場合の記録
 - ・ **Proxy** 証明書を発行した場合の記録
 - ・ 各処理の時刻と処理結果
16. 1 万人を超えるユーザが利用可能であり、200 回／分のトランザクションがあってもボトルネックにならないこと。

4.2.2 証明書管理システム開発仕様

認証ポータルの開発および証明書リポジトリとして **MyProxy** を使用するにあたって、証明書管理システムにおいても **MyProxy** に対し証明書を格納する機能を備える必要がある。以下に、証明書管理システムの開発における要求要件について記載する。

1. ソフトウェアにグリッド配備・運用タスクフォースで使用されている **UMS** をベースとして改変したものを使用すること。

2. 証明書管理システムに必要な機能を明確化し、5.7.6.1 に示す要求仕様に基づいて詳細設計および開発を行うこと。
3. 証明書管理システムと連携が必要な認証局システム、認証ポータル、証明書リポジトリとしての MyProxy の機能や動作を十分に考慮し設計を行うこと。
4. 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. 協議の上、確定した設計および利用する技術の実現性においては、事前に同等環境を構築し、評価を行うこと。このとき、評価環境は受託業者側で用意すること。

4.2.2.1 要求仕様

1. 認証ポータルとの連携し、クライアント証明書を MyProxy に格納する機能を備えること。
2. クライアント証明書を MyProxy に格納した場合にも、マッピング情報管理システムに対し以下の値を格納する機能を備えること。
 - ・ クライアント証明書の SubjectDN
 - ・ UMS、MyProxy におけるローカルアカウント名
 - ・ HPCI アカウントの ePPN

5 整備計画

本節では、認証基盤における整備計画について記載する。平成 23 年度および平成 24 年度は、図 5.1 に示すように整備を進める予定である。整備計画詳細について、以下に説明する。

1. 平成 23 年度
 - 利用シナリオ A を実現するため、以下の整備を行う。また、利用シナリオ A 以外の仕様について検討を行う。
 - 1-1. システム整備
 - 認証局システム、証明書管理システム、Shibboleth DS、認証ポータル、Proxy 証明書リポジトリを運用するためのハードウェアおよびソフトウェア環境を構築する。
 - 1-2. ドキュメント整備
 - 認証局運用機関、認証ポータル運用機関、HPCI アカウント IdP 運用機関、資源提供機関向けのドキュメントを作成する。
 - 1-3. ソフトウェア設計・開発
 - 認証ポータルおよび HPCI 事務局向けのソフトウェアの設計・開発を行う。

1-4. 認証基盤の運用開始

認証基盤の運用を開始する。

1-5. 仕様検討

平成 23 年度に実現しなかった利用シナリオを実現するためのソフトウェア仕様、運用規定、運用開始時期の検討を行う。

2. 平成 24 年度

平成 23 年度に開始した認証基盤の運用を継続する。また、平成 23 年度に行った利用シナリオ A 以外についての仕様検討結果に基づき、システム整備、ドキュメント整備、ソフトウェア設計・開発を行う。

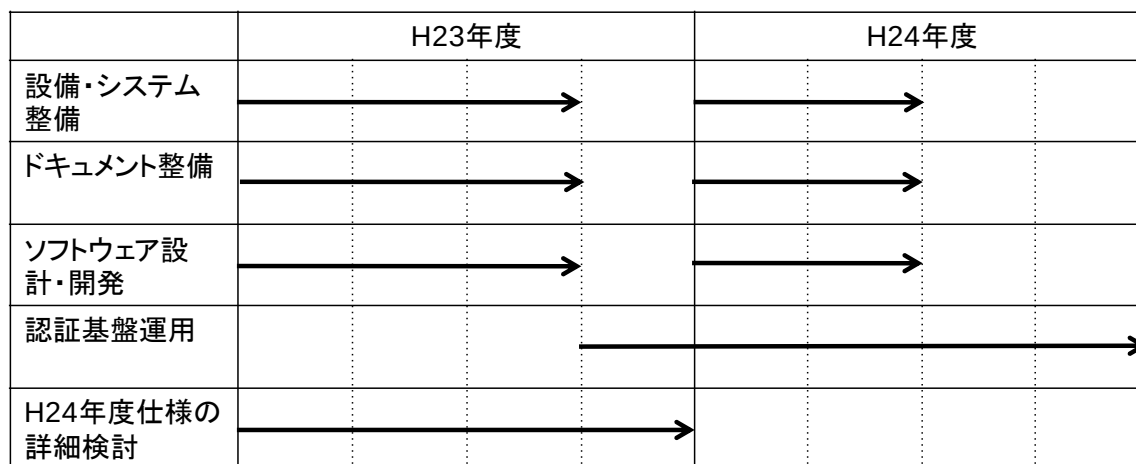


図 5.1 認証基盤 整備計画ロードマップ

6 必要経費

本仕様を実現するための必要経費見積を表 6.1 および表 6.2 に示す。

表 6.1 認証基盤構築・運用のための必要経費（平成 23 年度）

		費用見積[千円]
システム整備	認証局システム構築 証明書管理システム構築 Shibboleth DS 構築 認証ポータル構築	6,502

	Proxy 証明書リポジトリ構築	
ドキュメント整備	認証局運用機関向け 認証ポータル運用機関向け HPCI アカウント IdP 運用機関向け 資源提供機関向け	9,223
認証基盤ソフトウェア 設計・開発	認証ポータル	9,223
HPCI 事務局ソフトウェア 設計・開発	HPCI-ID 発行・管理システム HPCI 課題申請・管理システム 資源提供機関との情報連携	9,223
認証基盤運用	認証局運用・システム運用 (H24 年 1 月~H24 年 3 月)	14,019
資源設備費用	認証局運用機関用サーバ, HSM 認証ポータルサーバ	15,218
合計		63,408

※本見積には HPCI アカウント IdP 運用機関および資源提供機関における経費は含まない。
また、本見積には HPCI 事務局におけるシステム整備や運用経費等は含まない。

表 6.2 認証基盤構築・運用のための必要経費（平成 24 年度）

		費用見積[千円]
システム整備	OpenID プロバイダ対応 DS 冗長化	1,250
ドキュメント整備	認証局運用機関向け 認証ポータル運用機関向け HPCI アカウント IdP 運用機関向け 資源提供機関向け OpenID プロバイダ対応	15,250
認証基盤ソフトウェア 設計・開発	OpenID 対応認証ポータル OpenID-ローカルアカウントマッピング	5,000
HPCI 事務局ソフトウェア 設計・開発	HPCI-ID 発行・管理システム HPCI 課題申請・管理システム 資源提供機関との情報連携	15,000
認証基盤運用	認証局運用・システム運用 (H24 年 4 月~H25 年 3 月)	65,000
資源設備費用	HSM 保守	1,250

	DS 冗長化	
人件費	特任研究員×2 事務補佐員×1	18,500
合計		121,250

※本見積には HPCI アカウント IdP 運用機関および資源提供機関における経費は含まない。
また、本見積には HPCI 事務局におけるシステム整備や運用経費等は含まない。

付録

1 利用 TCP ポート・UDP ポート

1.1 認証基盤において利用される通信ポート

本節では、HPCI 認証基盤において利用する通信ポートについて説明する。

HPCI 認証基盤における利用ポートを表 付録 1.1 および図 付録 1.1、図 付録 1.2 に纏める。

表 付録 1.1 HPCI 認証基盤で利用する通信ポート

運用機関	コンポーネント	仕様ポート	通信相手
認証局運用機関	認証局システム	80/tcp(HTTP) 443/tcp(HTTPS)	ユーザ GSI-SSH 等(認証局リポジトリとして)
		11412/tcp(RA)	証明書管理システム
	証明書管理システム	22/tcp(SSH)	認証ポータル 認証局システム
		7512/tcp(MyProxy)	証明書管理システム
	Shibboleth DS	80/tcp(HTTP) 443/tcp(HTTPS)	ユーザ
認証ポータル運用機関	認証ポータル	80/tcp(HTTP) 443/tcp(HTTPS)	ユーザ
	Proxy 証明書リポジトリ	7512/tcp(MyProxy)	証明書管理システム ユーザ
HPCI アカウント IdP 運用機関	HPCI アカウント IdP	80/tcp(HTTP) 443/tcp(HTTPS)	ユーザ
資源提供機関	GSI-SSH	22/tcp(GSI-SSH)	ユーザ

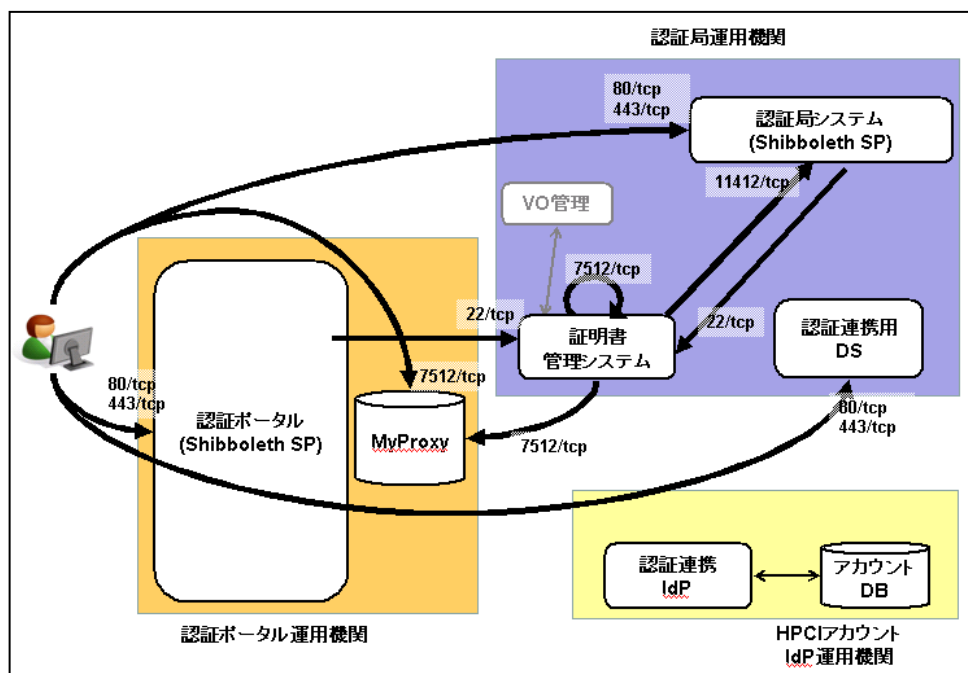


図 付録.1.1 認証局・認証ポータルから見た通信ポート

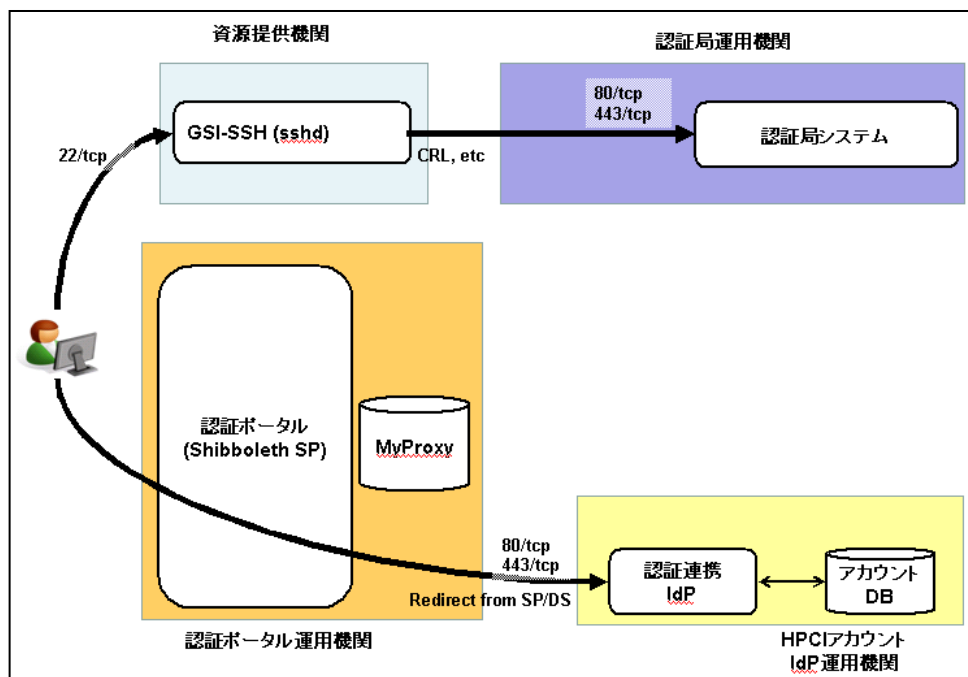


図 付録.1.2 資源提供機関・HPCI アカウント運用機関から見た通信ポート

1.1.1 認証局運用機関における利用ポート

認証局システムは 80/tcp、443/tcp、11412/tcp ポートを使用する。80/tcp および 443/tcp ポートはユーザから RA への Web アクセスおよび認証局リポジトリとしての HTTP/HTTPS として使用する。また、証明書管理システムからの証明書発行要求の受付のため 11412/tcp ポートを使用する。

証明書管理システムは、22/tcp、7512/tcp ポートを使用する。22/tcp ポートは、認証局システムと認証ポータルからの SSH 接続による連携のため使用する。7512/tcp ポートは MyProxy へのクライアント証明書格納のため使用する。

Shibboleth DS は、80/tcp、443/tcp ポートを使用する。80/tcp および 443/tcp ポートは Shibboleth による認証連携におけるユーザからの Web アクセスのための HTTP/HTTPS として使用する。

1.1.2 認証ポータル運用機関における利用ポート

認証ポータルは 80/tcp、443/tcp ポートを使用する。80/tcp および 443/tcp ポートはユーザから認証ポータルへの Web アクセスのための HTTP/HTTPS として使用する。

Proxy 証明書リポジトリは 7512/tcp ポートを使用する。7512/tcp ポートは、証明書管理システムもしくはユーザからの Proxy 証明書格納および取得のため使用する。

1.1.3 HPCI アカウント IdP 運用機関における利用ポート

HPCI アカウント IdP は 80/tcp、443/tcp ポートを使用する。80/tcp および 443/tcp ポートは Shibboleth による認証連携におけるユーザからの Web アクセスのための HTTP/HTTPS として使用する。

1.1.4 資源提供機関における利用ポート

GSI-SSH 環境は 22/tcp ポートを使用する。22/tcp ポートはユーザが Proxy 証明書を使用した GSI 認証による SSH ログインのための SSH として使用する。

2 調査結果

2.1 情報基盤センター群グループ管理

本節では、情報基盤センター群のグループ管理方法に関する調査結果を報告する。HPCI では、利用が承認された課題に基づいてユーザが決定されるため、資源へのアクセス制御等の認可処理を課題毎に行うことが必要となる。これを実現するためには、資源を利用するユーザのグループ管理を行う仕組みが必要となるため、情報基盤セン

ターにおけるグループ管理の現状を調査した。各情報基盤センターに対して以下の質問を行った結果を表 付録 2.1 に示す。

- (1) スパコン利用者を区分するグループ(以後、利用者グループと表記)を作成していますか？
- (2) どのような単位で利用者グループを作成していますか？(例:利用者の身分単位, 研究プロジェクト単位など)
- (3) 利用者グループは課金処理と関係していますか？(例:利用者グループ毎に課金が行われるなど)
- (4) 利用者グループは、計算機システム上ではどのように実装されていますか？(例:利用者グループ毎に UNIX GID を設定しているなど)
- (5) 利用者グループ毎に計算資源の CPU 利用制限やクォータ制限を行っていますか？
- (6) 同一の利用者が複数の利用者グループに属している場合で、利用者が特定の利用者グループ権限でジョブを実行したい場合、利用者はどのように利用者グループを指定しますか？
- (7) 利用者グループ単位でストレージ上のファイルへのアクセス制限の制御を行えますか？

表 付録 2.1 情報基盤センターにおけるグループ管理

	グループ管理	グループ分けの単位	課金	グループの実装	グループ毎の CPU, クォータ制限	ジョブ実行時のグループ指定方法	グループ毎のファイルアクセス制限
北大	有	研究室, 学科, 研究プロジェクト等	グループの代表者またはメンバに課金	グループ毎にユーザアカウントを発行し, グループ ID (UNIX GID) を設定.	有	指定するグループのユーザアカウントでログインする	有
東北大	無	—	—	—	—	—	—
筑波大	有	研究プロジェクト	グループの代	グループ毎に UNIX GID を設	有	qsub のオプション	有

			表者に課金	定.		ン	
東大	有	研究プロジェクト単位	グループの代表者に課金	グループ毎にユーザアカウントを発行し, グループ ID (UNIX GID) を設定	有	指定するグループのユーザアカウントでログインする	有
東工大	有	研究プロジェクト, 他(課金なしの場合)	グループの代表者に課金	グループ毎に UNIX GID を設定.	有	qsub のオプション	有
名大	有	センター、一般利用、グリッド利用、共同研究利用、機関利用、民間利用等	グループと課金処理は独立	グループ毎にユーザアカウントを発行し, グループ ID (UNIX GID) を設定	有	指定するグループのユーザアカウントでログインする	有
京大	有	研究プロジェクト, グループに属さないユーザも可.	グループの代表者に課金	グループ毎に UNIX GID を設定.	有	qsub のオプション	有 (ただし Large 領域のみ)
阪大	有	研究プロジェクト, 他	グループの代表者に課金	グループ毎にユーザアカウントを発行し, グループ ID (UNIX GID) を	有	指定するグループのユーザアカウント	有

				設定		トでログインする	
九大	有	資源共有型利用者のグループ1個，資源占有型は研究プロジェクト，研究室，共同研究利用等	資源共有型利用は利用者個人に課金，資源占有型はグループの代表者に課金	グループ毎にユーザアカウントを発行し，グループID（UNIX GID）を設定	有	指定するグループのユーザアカウントでログインする	有
京	有	研究プロジェクト	グループの代表者に課金	グループ毎にUNIX GIDを設定.	有	ジョブ投入時のオプション	有

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。
- [12] GSI (Grid Security Infrastructure)認証
PKI (Public Key Infrastructure)技術を用いて、グリッド上でシングルサインオンを実現するための技術
- [13] Shibboleth
複数の組織が運営する Web サービスへのシングルサインオンを実現するための仕組みを指す。
- [14] OpenID
一つのアカウントを用いて複数の Web サイト上の認証を行うための仕組みを指す。

HPCI 基本仕様

— ネットワーク基盤の基本仕様 —

目次

1	概要	3
2	ネットワーク基盤の利用シナリオ	4
2.1	全体利用イメージ	4
2.2	ユーザのネットワーク利用シナリオ	5
2.2.1	幅広いユーザのネットワーク利用	5
2.2.2	商用ネットワークと SINET4 との接続	7
2.2.3	企業の SINET4 への加入について	8
3	ネットワーク基盤の基盤構築・運用基本仕様	10
3.1.1	所要ネットワーク機能	10
3.1.2	ネットワーク構成	11
3.1.3	所要ネットワーク帯域	13
3.1.4	SINET4 上での実装案	15
3.1.5	ネットワーク保守運用体制	19
4	整備計画	20
4.1	ネットワーク整備計画(案)	20
4.1.1	ネットワーク機能・構成・帯域	20
4.1.2	アンケート結果に基づく所要帯域試算(一次分析)	22
5	必要経費	26
5.1	ネットワーク基盤経費	26
	用語集	27
	(参考1)学術情報ネットワーク加入規定	30
	(参考2)学術情報ネットワーク加入細則	32

1 概要

本基本仕様書は、ネットワーク基盤資源利用のための基本仕様である。HPCI を活用した各種研究活動の全国的な展開を推進するためには、ユーザや資源提供機関の間を結ぶ全国規模の高速で安定的なネットワーク基盤が不可欠である。このため、次期学術情報ネットワーク(SINET4)上にHPCI用のネットワークを形成することが「革新的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)に記載されている。同グランドデザインに基づき、ネットワークの利用シナリオ、ネットワーク機能と所要帯域、運用体制おならびに運用経費について検討を行った。

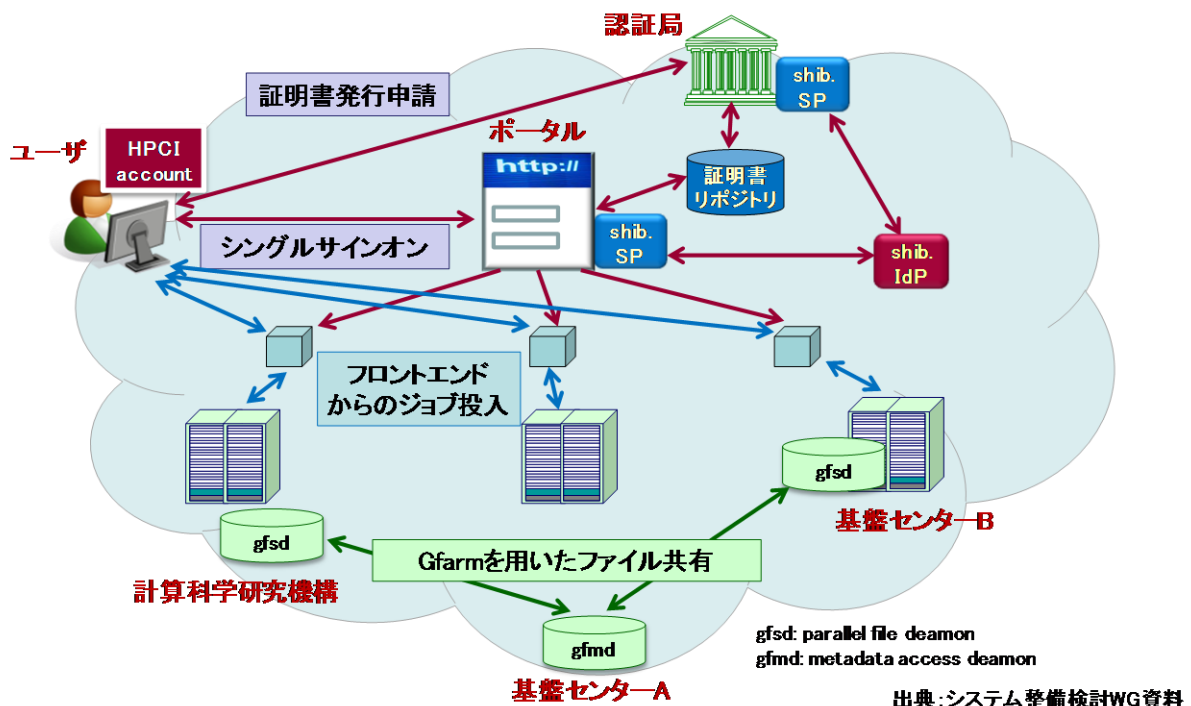
本仕様書は、スーパーコンピュータ施設を有し共同利用・共同研究拠点として活動している東京大学およびSINETを運営している国立情報学研究所が主幹し、共同利用・共同研究拠点である北海道大学、東北大学、東京工業大学、名古屋大学、京都大学、大阪大学、九州大学、筑波大学、および京速コンピュータ「京」運用機関である理化学研究所計算科学研究機構と連携して、HPCI構築に関する基本仕様について調査検討した結果に基づいて作成されている。

2 ネットワーク基盤の利用シナリオ

2.1 全体利用イメージ

ネットワーク利用に関わるプレーヤーとしては、資源を利用するユーザ、資源を提供する資源提供機関の他に、ユーザ認証において重要な役割を担う認証ポータル運用機関、認証局運用機関、を考慮する必要がある(図 1)。

ユーザは、資源提供機関の資源にアクセスするために、認証ポータルや認証局を通じてユーザ認証を受け、また、各資源に対するアクセスの認可を受ける必要がある。その後、ユーザから計算資源に対してジョブ投入が行われる。ジョブを実行するに当たっては、計算資源やストレージ資源の間で大容量のファイル転送やファイルの共有が行われる場合があり、高いジョブ実行性能を得るには、十分なネットワークの帯域が必要になる。



2.2 ユーザのネットワーク利用シナリオ

2.2.1 幅広いユーザのネットワーク利用

企業を含む幅広いユーザの利用を推進するために、様々なネットワーク(商用ネットワークを含む)から資源提供機関にアクセスできる環境を整備する必要がある。学術系ユーザにおいては、全国 700 以上の国公私立大学、研究機関等の学術情報基盤である SINET4 を主として活用することとし、学術系以外のユーザも資源提供機関へのアクセスに極力制限がでないように商用ネットワーク等との相互接続環境を整備することとする。(図 2)。

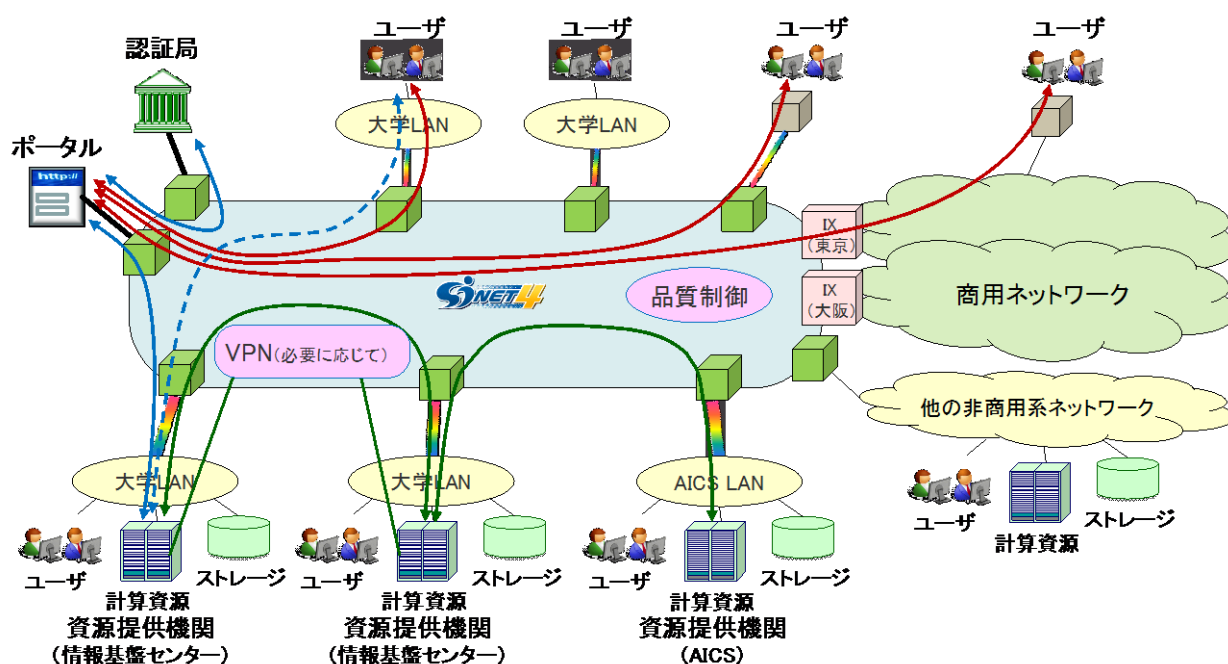


図 2. 幅広いユーザ収容を考慮したネットワークのイメージ

HPCI の資源提供機関が SINET4 に収容されている場合、HPCI ユーザの資源提供機関へのアクセスとしては、以下のケースが考えられる。

- ①ユーザが SINET4 のみを用いて資源提供機関にアクセス(専用線等で SINET4 の DC のノードに直接接続して SINET4 を利用)
- ②ユーザが商用ネットワークや他の非商用系ネットワーク経由で SINET4 に接続して資源提供機関にアクセス
- ③ユーザが資源提供機関の場所に出向いて直接アクセス(資源提供機関間のデータ転送は SINET4 を利用)

①のケースは学術系ユーザの一般的なケースであり、SINET4 内に閉じた形態となるため、SINET4 の多様なサービス(L3/L2/L1VPN、QoS、オンデマンドサービス等)を享受できる。ここで、企業のユーザがこの接続形態を望む場合には、企業は SINET の加入機関になる必要がある。SINET4 に直接接続するための専用線等の費用については企業の負担となるが、SINET 側で接続認可ポリシーを明確にする必要があり、これについては、2.2.3 項で詳細に説明する。

②のケースは、いわゆるインターネット的な利用形態であり、企業のユーザも現在でも可能である。また、ユーザが SINET の加入機関になる必要はなく、費用負担も発生しない。ここで、商用ネットワークと SINET4 とは、相互接続ポイント(IX)である JPNAP (Japan Network Access Point)や JPIX (JaPan Internet eXchange)により接続されており、SINET と JPNAP・JPIX との間の接続帯域は通信トラフィック量を見ながら適宜増速を行っており、性能上の問題はないと考えられる。これについては、2.2.2 を参照のこと。また、SINET4 は他の非商用系ネットワーク(地域の学術ネットワーク、WIDE, JGN 等)とも相互接続されており、十分なアクセス手段を有していると考えられる。

③のケースは、各提供資源機関の資源利用認可ポリシーに基づき可能となる形態であるが、SINET4の利用は提供資源機関が行っていることになるため、企業のユーザが利用している場合でも、その企業は SINET の加入機関になる必要はない。ちなみに、SINET 側では、提供資源機関のユーザの識別(教員、学生、企業等)は困難である。

2.2.2 商用ネットワークと SINET4 との接続

商用ネットワークと SINET4 とは、相互接続ポイントである JPNAP や JPIX 経由での接続が可能である(図 3)。この接続形態であれば商用ネットワークと SINET4 との間において自由に通信が可能であり、SINET4 側では何ら制限を設けていない。なお、SINET4 と JPNAP・JPIX と間の接続インターフェースおよび JPNAP・JPIX を介して接続されているネットワーク数は表1のとおりで、東京では合計 30Gbpsの帯域で 134 の商用ネットワークと、大阪では合計 11Gbpsの帯域で 22 の商用ネットワークと接続されている。SINET4 と JPNAP・JPIX との間の接続帯域は通信トラフィック量を見ながら適宜増速を行っており、性能上の問題は無いと考えられる。

表1. SINET4 と JPNAP・JPIX との接続帯域およびその接続ネットワーク数

IX	東京		大阪	
	帯域	接続 NW 数	帯域	接続 NW 数
JPNAP	10GE	47	10GE	16
JPIX	10GE×2	87	1GE	6

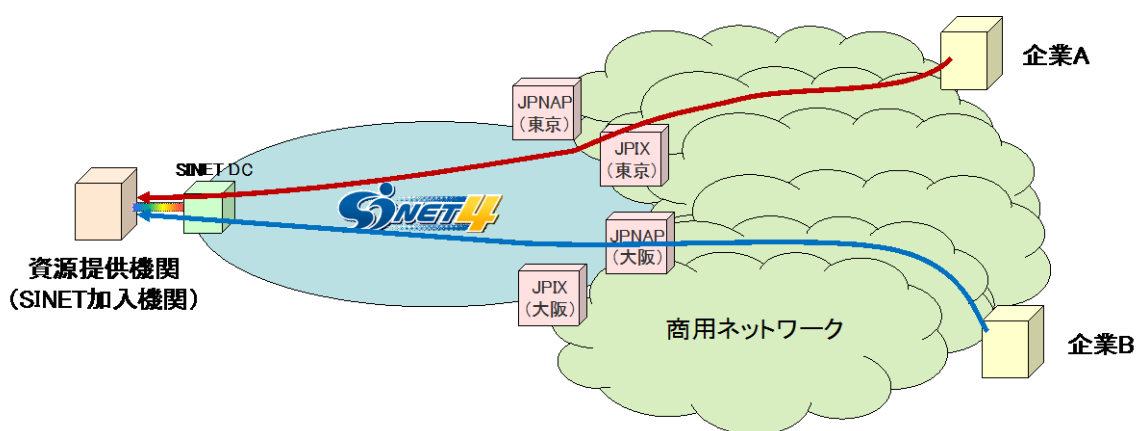


図 3. 商用ネットワークと SINET4 との接続

2.2.3 企業の SINET4 への加入について

企業が SINET4 に直接接続(DC のノードに接続;図 4)するためには、SINET の加入機関となる必要がある。すなわち、SINET 加入申請を行い、国立情報学研究所での審査・承認を得る必要がある。現在、『学術情報ネットワーク加入規程』において、「前 3 号(※)に定める機関と共同で研究等を行う機関」であれば、加入が認められる。(詳細は参考1を参照のこと)

国家プロジェクトである HPCI プロジェクトに参画する企業に対しては、その活動が「共同で研究等」に相当するととらえ、HPCI プロジェクトの参画期間内に限り、SINET に加入することは差し支えない。なお、HPCI プロジェクトの本格展開に向けて、この文脈がより明確に読みとれるよう、加入規定の改定についても検討を行っている。

(※)一 大学、短期大学、高等専門学校、大学共同利用機関等、二 研究所の事業に協力する機関、三 国公立試験研究機関並びに研究又は研究支援を目的とする独立行政法人及び特殊法人等

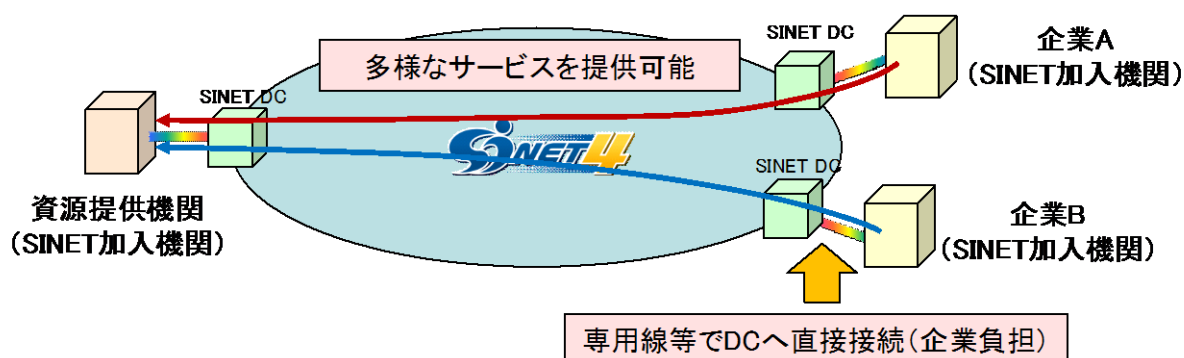


図 4. 民間企業の SINET への直接接続

2.3 資源提供機関のネットワーク利用シナリオ

HPCI の本格展開においては、資源提供機関の計算資源やストレージ資源間で大容量のファイルの転送が行われるため、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やストレージ資源に対するアクセス管理を行っている。HPCI ではセキュリティ面の強化を考慮して、計算資源やストレージ資源の間の通信を含めて、全ての通信は各資源提供機関のファイヤーウォールを必ず通すこととする。すなわち、ファイヤーウォールを通さない VPN は基本的に使用せず、全ての通信は共用のネットワーク(いわゆるインターネット)を使用することとする。ここで、HPCI では各資源提供機関のセキュリティリスクの増大を極力抑えるネットワークサービス設計をおこなうこととする。具体的には、HPCI が使用するプロトコル(ポート番号)を最小限とすることとする。注)

注)HPCIの構築にあたって必要なポート数は、暫定的に10 未満として設計を進めることとした。

ただし、HPCI の進展を加速させる先端ソフトウェア機能の性能検証等においては、資源提供機関間で共用ネットワークとは分離した環境(L3VPN やL2VPN などのVPN 環境)での検証実施等が必要な場合があり、先端ソフトウェア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ことが望ましい。

また、共用ネットワークを用いて高性能に大容量のファイル転送を行う必要があるが、ネットワーク内で品質制御を行うか否かは、今後の利用形態等を鑑み判断を行うこととする。

3 ネットワーク基盤の基盤構築・運用基本仕様

3.1 ネットワーク機能・構成・帯域

3.1.1 所要ネットワーク機能

HPCIとしては、基本的に、全ての利用形態において共用ネットワーク(いわゆるインターネット)を用い、各資源提供機関のファイヤーウォールで計算資源やストレージ資源へのアクセス制限等を行い、全体として高いセキュリティを確保する。すなわち、基本となるネットワーク機能は、IPv4 パケット転送機能である。ここで、将来の IPv6 への対応も考慮して、ネットワークとしては、IPv4/IPv6 dual stack 機能を提供することとする。

また、HPCI の進展を加速させる先端ソフトウェア機能の性能検証等のためには、先端ソフトウェア開発者側でネットワーク環境(共用ネットワーク、L3VPN、L2VPN 等)を自由に選択して利用することが望ましい。このため、HPCI 発展のために SINET4 上で特別な開発環境を提供する。

また、高性能に大容量のファイル転送を行う際に、ネットワーク内で品質制御が必要になる可能性があり、ネットワークの機能としては、事前に実装しておくこととする。(図 5)

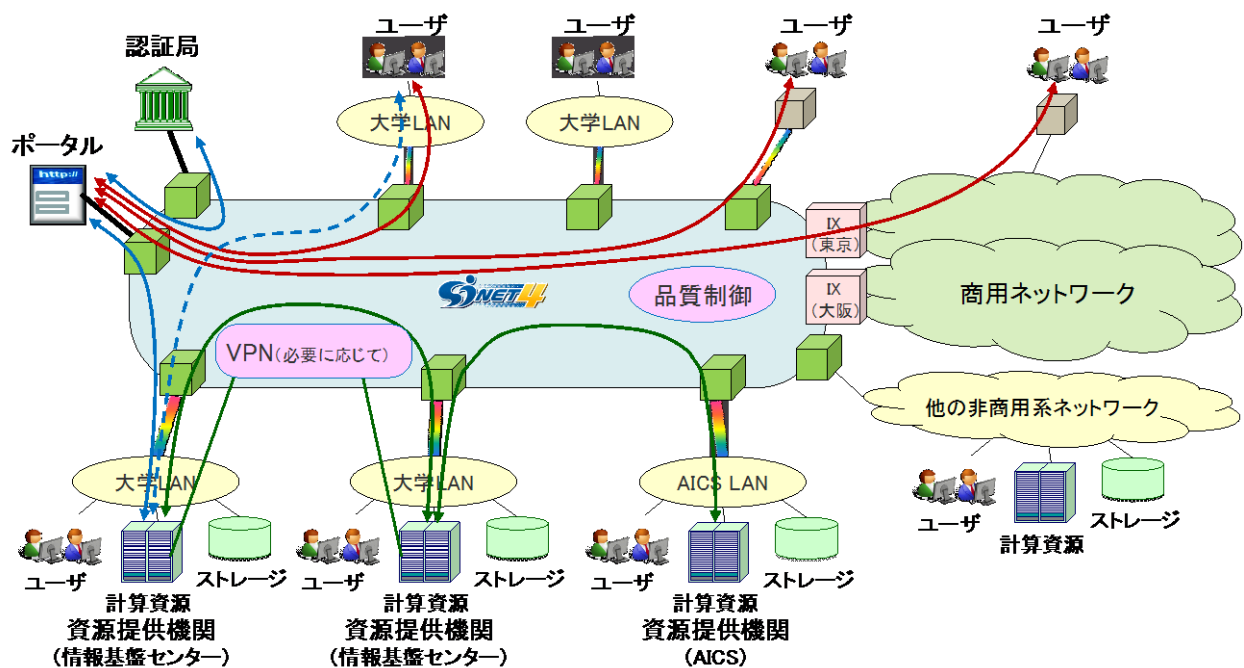


図 5. 所要ネットワーク機能

3.1.2 ネットワーク構成

平成 23 年 4 月より本格運用が開始される SINET4 は、国内最高帯域である 40Gbps の回線を全国面に採用している。ネットワーク構成の特徴としては以下の通りである(図 6)。

- ・ 加入機関(大学や研究機関等)を収容するエッジノードの数は 42、加入機関を収容しかつ中継機能を有するコアノードの数は 8 であり、全県でユーザを収容可能で、また、全てのエッジ・コアノードが商用の DC に設置される。
- ・ コア回線(コアノード間の回線)は 40Gbps を基本として冗長化を図っており、エッジ回線(エッジノードーコアノード間の回線)は 2.4Gbps～40Gbps、アクセス回線(エッジノードー加入機関間の回線)は 10Gbps～40Gbps(可変速)である。
- ・ 加入機関向けのノードインタフェースは、E/FE/GE (T)、GE (LX)、10GE (LR) の三種類の中から自由に選択できる。

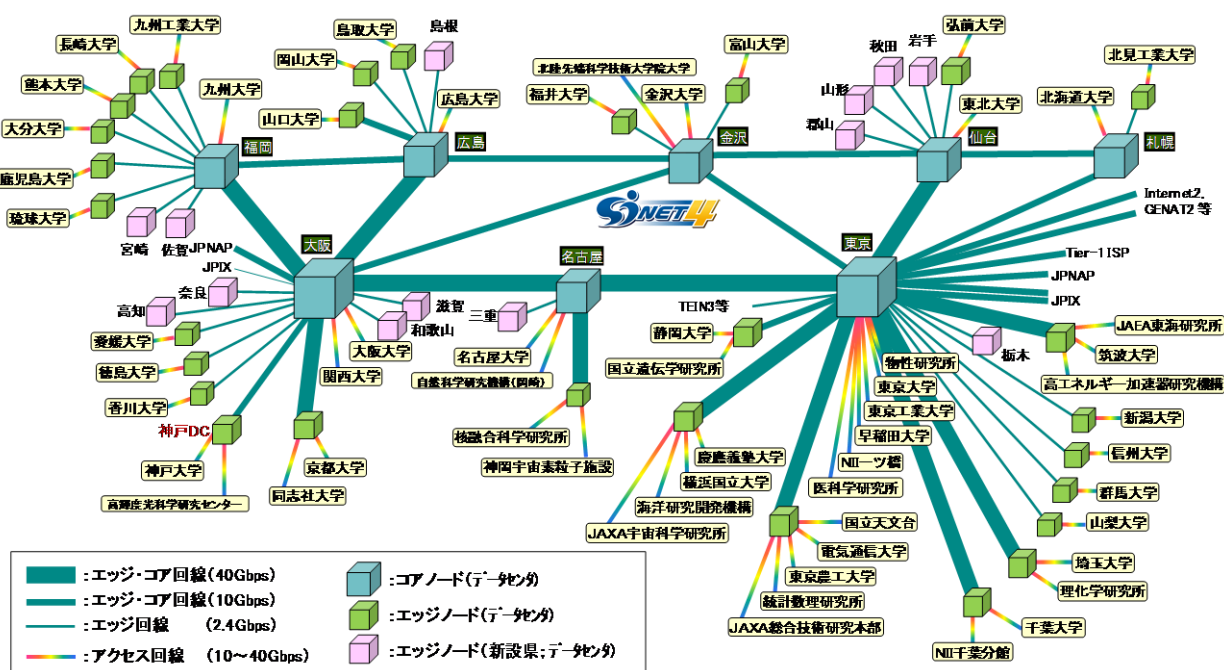


図 6. SINET4 のネットワーク構成(平成 23 年 4 月時点)

資源提供機関である北海道大学、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、九州大学を収容する DC は全て 40Gbps 回線で接続されており(札幌 DC は 23 年度)、ネットワーク構成上の問題はない。ここで、資源提供機関と SINET4 の DC との間は WDM 回線であり、増速は 10GE 単位で容易に可能である(図 7)。

理化学研究所計算科学研究機構(AICS)と SINET4 との接続形式は、神戸 DC/大阪 DC への収容、AICS/大阪 DC への PoP の設置有無など、多様な側面から検討を行っている。現時点では、平成 24 年 1 月から大阪 DC に 40Gbps で接続する方向で検討を進めている。

SINET4では全県にDCが設置されているため、全国の大学や研究機関等から計算資源やストレージ資源へアクセスする環境も整備されている。かつ、DCの環境は、計画停電による電源供給休止なし、停電時でも非常用電源供給装置から10時間以上継続して給電可能、阪神・淡路大震災クラスに耐える耐震性、24時間365日セキュアに入退館管理を実施、申請後2時間以内に担当者の緊急入館が可能、任意のキャリアの回線サービスの利用が可能、任意の事業者の各種機器類の設置が可能などを考慮しており、安定的にサービスを提供可能である。

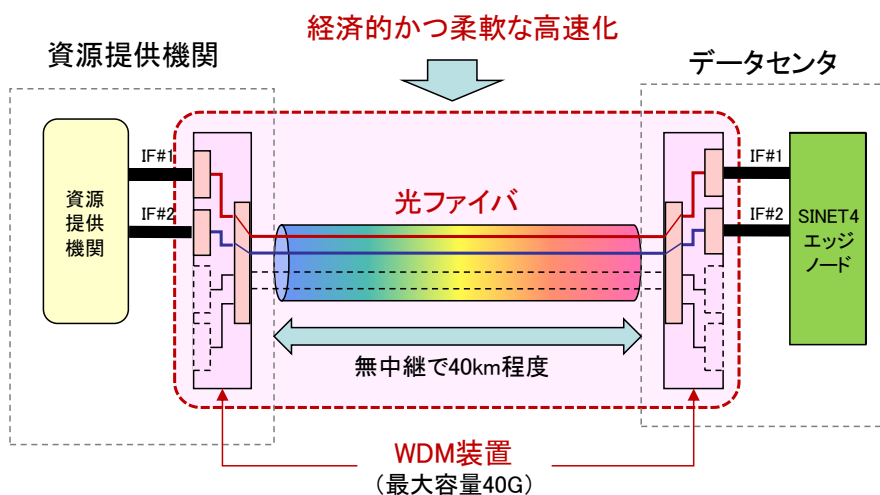


図 7. SINET4 における資源提供機関向けの回線

3.1.3 所要ネットワーク帯域

所要ネットワーク帯域としては、需要に応じて、バックボーン回線 (DC 間)、アクセス回線 (DC－加入機関間)、相互接続用回線 (JPNAP・JPIX 向け) の増速を検討する必要がある。例えば、図 8 のような理化学研究所・計算科学研究機構 (AICS) と各資源提供機関との接続を考慮する場合、東京 DC－大阪 DC 間と東京 DC－札幌 DC 間の回線の増速が必須であることがわかる。AICS が神戸 DC に接続する場合には、神戸 DC－大阪 DC 間の回線の増速も必要になる。

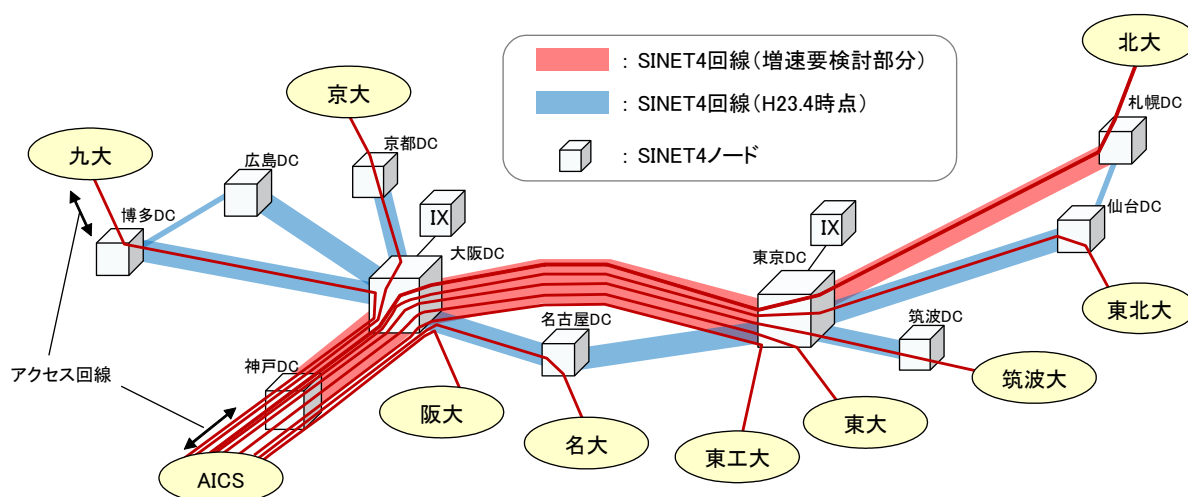


図 8. 所要ネットワーク帯域検討例(9 大学と AICS を接続する場合)

なお、回線の増速検討にあたっては、以下の点を考慮して進める必要がある。

- ・ 現行の SINET4 の帯域増強計画は HPCI 利用を想定していなかった時点のものであり、HPCI の本格展開時に帯域が不足することのないよう、今後の帯域需要を十分に精査する必要がある。ただし、SINET では、実績を元にした予測値で計画を立てており、HPCI についても、何からの指標が必要と考える。
- ・ 故障時の迂回用帯域についても考慮の上、増速区間、帯域を決定する必要がある。

また、現時点では、HPCI プロジェクトと他のプロジェクトとでネットワークの帯域を共有することを想定している(図 9)。共有される帯域は、SINET4 の整備が「4. 整備計画」に記載する計画の通りに進めば、当面は問題のないレベルと想定される。今後、HPCI の利用が進み、トラフィック増に伴って専用帯域を HPCI プロジェクトの負担で追加する必要がある際には、SINET4 内の設定によりデータの優先度を高く変更したり、帯域を固定で割り当てるなどの対応も可能である。ただし、その場合にも、HPCI 用の帯域が空いている場合には、他のコミュニティにおいても活用が可能とすることが望ましい。

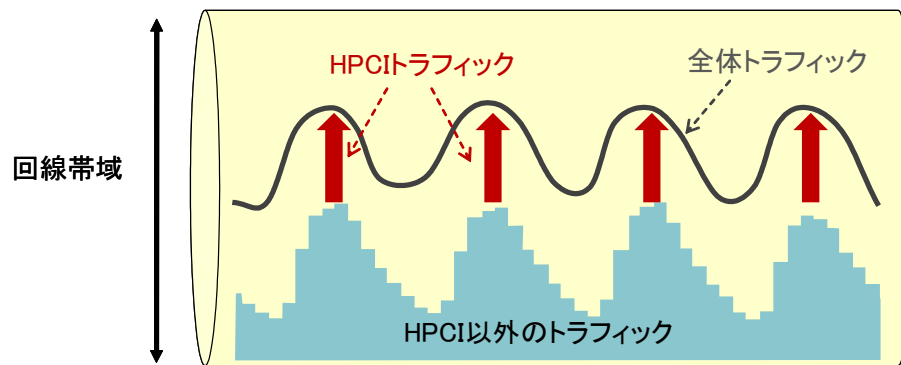


図 9. ネットワーク帯域の割り当て方法

3.1.4 SINET4 上での実装案

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、L1オンデマンド等)を提供している(表 2)。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構築することによりサービスを提供している(図 10)。

HPCI の利用においては、SINET4 は基本として、3.1.1 項に記載のとおり、IPv4/IPv6 dual stack 論理網上で IP パケット転送サービスを提供する。ここで、IP パケットの優先制御が必要となる場合には、SINET4 内では、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。

先端ソフトウェア機能等の性能検証においては、先端ソフトウェア開発者が、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 上でそのための別サービス論理網を設定して機能の提供を行う。

表 2. SINET4 の提供サービス一覧

サービスメニュー		SINET4	備考
提供インタフェース	E/FE/GE (T)	◎	
	GE (LX)	◎	
	10GE (LR)	◎	
L3サービス	インターネット接続	◎	
	IPv6	◎	native/dual stack/tunnel
	マルチホーミング	◎	
	フルルート提供	◎	
	IPマルチキャスト	◎	
	L3VPN	◎	
	アプリケーション毎QoS	◎	
	IPマルチキャスト (QoS)	◎	
	L3VPN (QoS)	◎	
	L3VPN (マルチキャスト)	予定	
L2サービス	L2VPN/VPLS	◎	
	L2VPN/VPLS (QoS)	◎	
	L2オンデマンド	予定	
L1サービス	L1オンデマンド	◎	
情報提供/ ユーザ支援サービス	パフォーマンス計測/改善	◎	スループット/RTT情報提供、性能改善ソフト提供(予定)
	トラフィック利用状況	◎	個別にSINET利用推進室にお問合せください

※ その他のサービスも検討中

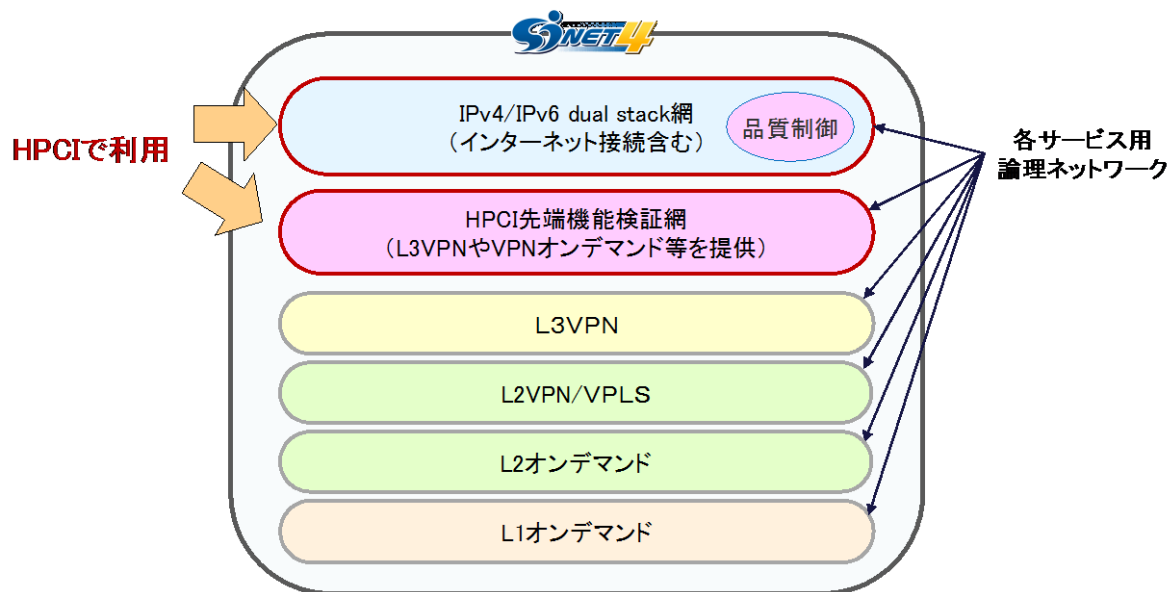


図 10. SINET4 上での HPCI 向けサービス

ここで、SINET4 上でオンデマンドで VPN を設定する機能は国立情報学研究所 (NII) において開発予定の機能であるが、先端ソフトウェア機能の開発者をターゲットとして、HPCI 専用の設定用画面を用意する方向で検討中である。本機能を利用することにより、web ページ上で開発者が必要時に対地 (複数対地間接続も可能) と VLAN ID などを選択して L2VPN を設定することが可能となる (図 11)。

SINET4 上でのより詳細な実装例を図 12 に示す。SINET4 で導入しているノードは、ハードウェアは市販品であるが、ソフトウェアはスペシャルコードを提供してもらっており、リソースオンデマンド等の独自の機能は NII で開発し、スペシャルコードと連携させることで独自のネットワークサービスを提供している。各サービスは VLAN やレイヤ1パスで分離・多重し、IP ルータでは各サービス用の論理ルータを設定することで多様なサービスを提供する。HPCI 用に、共用の IPv4/IPv6 dual stack 用の VLAN や論理ルータに加え、HPCI 先端用の VLAN や論理ルータも設定する。

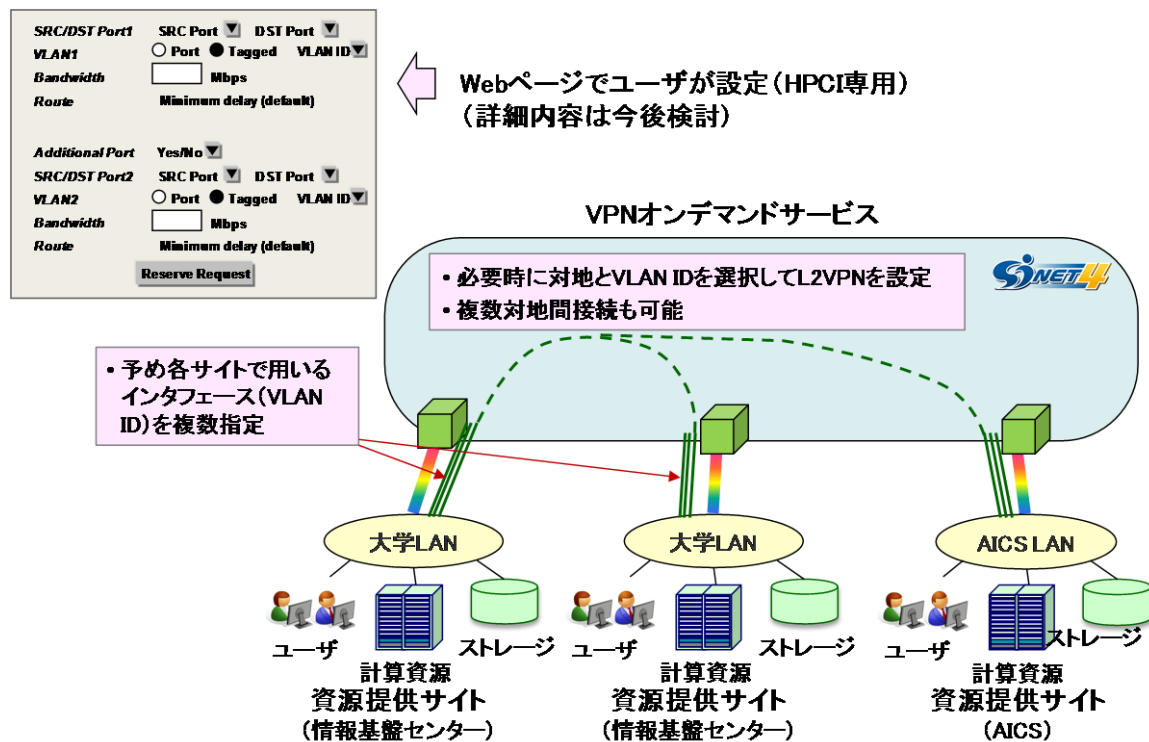


図 11. VPN オンデマンドサービスのイメージ

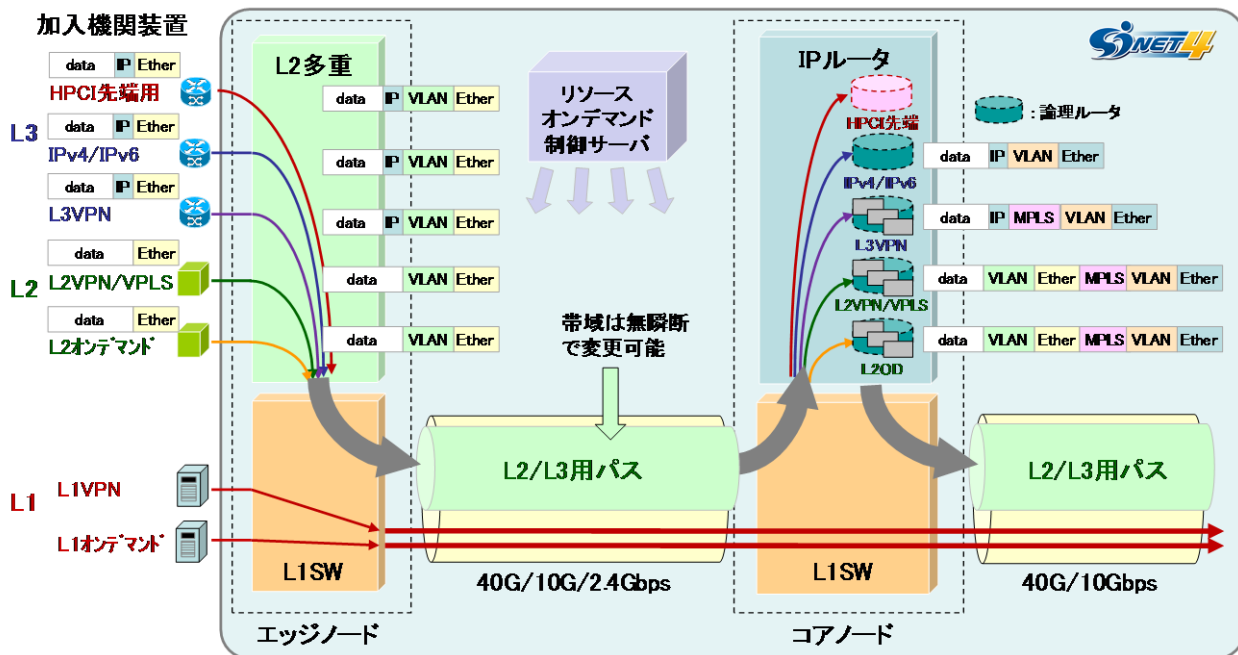


図 12. SINET4 上での具合的実装

その他の提供機能候補としては、高効率データ転送機能(確保した帯域を高効率に使いきるデータ転送機能:開発要)、トラフィック測定機能(VPN 内のトラフィック測定値を提示する機能:軽微な開発要)、SINET 内の特殊パッケージを用いた高精度なトラフィック分析機能:少し将来の実装)、利用者支援機能(ユーザ側で用意した計測装置(PerfSONAR 等)と SINET との連携:今後議論要)などが考えられる。

3.1.5 ネットワーク保守運用体制

SINET4 の運用保守対応は国立情報学研究所にて実施する(24 時間 365 日対応)。ここで、障害時には、共用ネットワークサービス、先端研究用サービスは同じ優先度で扱う。

SINET 以外も含めたネットワーク全体の運用保守、さらには、HPCI 全体の運用保守に関して特別な体制を整えるのかは議論が必要である。たとえば、HPCI 事務局が提供するヘルプデスクとのワークフロー、障害情報の共有などを今後検討する必要がある。

- バックボーン回線:
東京 DC－大阪 DC 間の更なる増速については需要次第
(例えば、今後のユーザ拡大の積極的な推進を前提として、100Gbps 回線(平成 24 年度にリリースが期待される)を東阪に追加、など)
- アクセス回線:
必要に応じて資源提供機関のアクセス回線を増速
(例えば、各資源提供機関のアクセス回線に 10G-IF を追加、など)
- 相互接続用回線:
必要に応じて帯域を増速
- ノードインタフェース:
上記に応じてノードインタフェースを追加

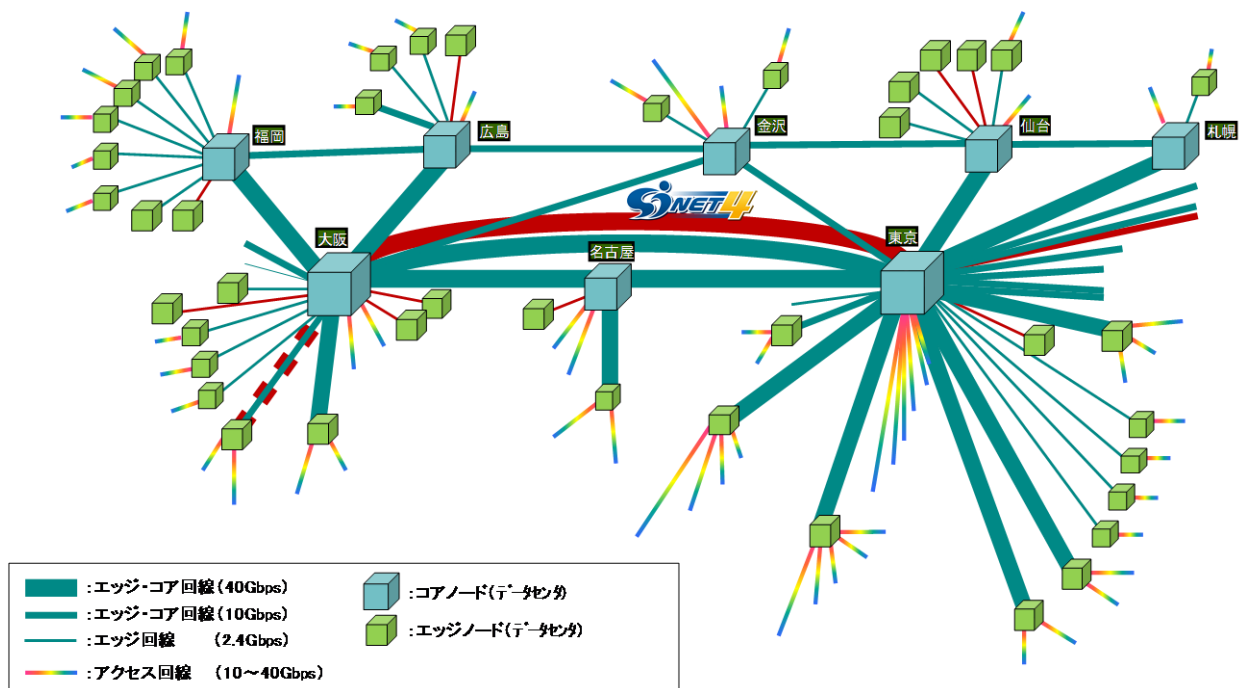


図 14. 平成 24 年度以降の SINET4 のネットワーク整備計画(時期未定)

4.1.2 アンケート結果に基づく所要帯域試算(一次分析)

平成 22 年 12 月～平成 23 年 1 月に行われた HPCI コンソーシアム加盟者を対象とした HPCI に関する利用者ニーズのアンケート結果(ネットワーク関連部分の抜き出しは表 3)を基に、必要な帯域を試算した。

まず、アンケート結果について確認を行ったところ、機関ごとに需要提示方法が区々であることが判明した。傾向を分類すると、以下のとおりとなった。

(1) 必要帯域を明確に指定している機関(7 機関)

名古屋大学太陽地球環境研究所、国立天文台、東京大学物性研究所、計算物質科学イニシアティブ(CMSI)などがこれにあたり、必要帯域が 1Gbps～100Gbps の間で明確に指定されている。

名古屋大学太陽地球環境研究所を例にとると、「(ア)電磁流体シミュレーション次世代スパコン: 81,920 ノード×300 時間、ストレージ:30PB×30 日、ネットワーク回線:名古屋大学との間で 1PB 規模×30 日(100Gbps ※実効性能で)。」との回答があり、明確に 100Gbps の帯域を要望している。また国立天文台の回答においても、「(中略～)1 兆粒子のシミュレーションを数回から数十回行くと、ストレージは 100PB 程度を数年間、ネットワークは次世代の神戸サイトと国立天文台他のいくつかのサイト間で 10GB/s 程度が必要になる。」と明記されている。

上記機関などは必要帯域を明示していることからデータ量と転送時間とを一定して関連付けている様子が伺えるが、現行において 40Gbps を超える帯域の回線サービスは存在せず、また SINET4 の中継面(コア・エッジ区間)においても、最大帯域は 40Gbps となっており、仮にアクセス区間において 40Gbps を超える需要があったとしても、コア・エッジ区間で帯域が他のトラフィックに重畳されてより細い帯域の確保しかできず、要望の実現可能性については懸念が残る。またこれらの機関から「京」の設置される計算科学研究機構(AICS)まで接続すると仮定した場合、AICS の必要とする帯域は各機関の必要帯域の総和となり、100Gbps をはるかに超える帯域が必要となる計算となる。こうした帯域を用意するのは実際には困難であるため、何らかの指標を持って各機関の需要を換算する必要があると考えられる。

(2) データ量および送信に要する時間を指定している機関(3 機関)

必要帯域をダイレクトに指定はしていないものの、データ量および送信に要する時間を指定している機関については、換算により必要帯域を算出することが可能である。計算基礎科学連携拠点、名古屋大学、スーパーコンピューティング技術産業応用協議会などの回答がこれに該当する。

計算基礎科学連携拠点の回答を例にとると、回答内容として「ネットワークとして『京』計算機や主要な研究所の間に 10GB/s 程度、が必要である」と記載しているが、 $10\text{GB/s} \approx 80\text{Gbit/s}$ であることから、同拠点が回答している必要帯域は 80Gbit/s 程度であると推察される。

(3) 必要データ量のみが提示され、送信に要する時間を指定しない機関(7 機関)

京都大学基礎物理学研究所、海洋研究開発機構などがこれにあたる。海洋研究開発機構の回

答を例にとると、「ネットワーク回線:20TB 規模×50 日 JAMSTEC ESC への転送のため」と記載されている。こうした記載方法をとっている場合においては、必要帯域の換算において、当該データの送信に要する時間を規定する必要がある。(一秒〜一日程度の間と想定される)

(4) 必要データ量自体を指定しない、あるいは推察が困難な機関(20 機関)

NPO 法人バイオグリッドセンター関西(回答:「具体的な仕様は決まっています。」)、財団法人計算科学振興財団(回答:「HPCI の数%を産業界の専用枠とする」)など、必要なデータ量そのものが指定されていない機関が複数見られた。また回答内容がスパコンのノード数と稼働時間のみ、あるいはストレージの帯域と日数のみの機関も多数あり、こうした機関については必要帯域の算出自体が困難であったため、帯域需要の算出対象外とした。

なお、この他一部機関の回答において「殆どの研究分野で、理想的に望ましい計算能力と実際に例えば次世代スパコンで現実的に利用可能と推測される資源量には何桁もの違いがあり、『どれだけ必要か』という問題設定は無意味」といった趣旨の指摘もあり、本分野における適切な帯域設定の難しさを伺わせる内容となった。

上記(1)～(4)の分類のうち、(3) 必要データ量のみが提示され、送信に要する時間を指定しない機関 について、提示されたデータ量を転送するための環境を松/竹/梅(6 分/1 時間/10 時間で転送)で表現し、必要帯域を試算した(表 4)。ここで、(1) 必要帯域を明確に指定している機関 について、ややオーバースペック気味と思われるもの(80Gbps や 100Gbps)は松の位置づけとした。

竹(1 時間)程度の転送環境を想定すると、特出した需要は京都大学基礎物理研究所(27.5Gbps)、海洋研究開発機構(44Gbps)などであるが、その他は概ね 10Gbps 以下であり、現時点では、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。

表 3. アンケート結果(平成 24 年度及び平成 29 年度の要望)

No	機関名	平成24年度(対地:要望)	平成29年度まで(対地:要望)
1	核融合科学研究所	次世代スパコン: 数TB規模のデータ転送 東京大学: 数10GB規模のデータ転送	次世代スパコン: 数TB規模のデータ転送 東京大学: 数10GB規模のデータ転送
2	計算物質科学イニシアティブ (CMSI)	次世代スパコン: 帯域保証ベースで1Gbps 物性研、分子研、金研スパコン: 帯域保証 ベースで1Gbps	次世代スパコン: 帯域保証ベースで1Gbps 物性研、分子研、金研スパコン: 帯域保証 ベースで10Gbps
3	東京大学 物性研究所	次世代スパコン: 帯域保証ベースで1Gbps 物性研スパコン: 帯域保証ベースで1Gbps	次世代スパコン: 帯域保証ベースで1Gbps 物性研スパコン: 帯域保証ベースで10Gbps
4	高エネルギー加速器研究機構	次世代スパコン、共同利用研、大学: 大容量 データのやり取りを円滑かつ高速に	
5	スーパーコンピューティング 技術産業応用協議会	次世代スパコン～利用者ローカル環境: 1TB×1日 (1モデルの結果を1日で転送) 次世代スパコン～拠点間: 10GB規模 ×100日	次世代スパコン～利用者ローカル環境: 10TB×1日 (1モデルの結果を1日で転送) 次世代スパコン～拠点間: 100GB規模×100 日
6	地球シミュレータセンタ	ネットワーク帯域として10Gbps以上必要	ネットワーク帯域として40Gbps以上必要
7	海洋研究開発機構	JAMSTEC ESC: 20TB規模×50日	JAMSTEC ESC: 40TB規模×60日
8	国立天文台	次世代スパコン: 10GB/s	
9	名古屋大学 太陽地球環境研究所	次世代スパコン: 各シミュレーションで1PB 規模×30日～60日(100Gbps)	次世代スパコン: 各シミュレーションで10PB 規模×30日～60日(1Tbps)
10	北海道大学 情報基盤センタ	次世代スパコン: 1TBを1時間以内に交換 可能な300MB/s以上が必要	
11	計算基礎科学連携拠点	次世代スパコン～主要な研究所間: 10GB/s程度	
12	大阪大学 臨床医工学融合研究センター	次世代スパコン: 128GB規模×10日	次世代スパコン: 128GB規模×10日
13	京都大学 基礎物理学研究所	次世代スパコン: 1Gbpsで50TB/4日より 早く	
14	東北大学 サイバーサイエンスセンター	次世代スパコン: 数値流体力学:10GB規 模×30日、気象学:1TB/1日	次世代スパコン: 数値流体力学:10GB規模 ×30日、気象学:1TB/1日
15	東京工業大学 学術国際情報センター	次世代スパコンや世界最高水準のスパコン、 1TB以上/1時間(10Gbps以上)	
16	東京大学 生産技術研究所	次世代スパコン: 10GB規模×100日	次世代スパコン:40GB規模×200日
17	名古屋大学	次世代スパコン、大学センター: 1TB/1時 間	次世代スパコン、大学センター: 5TB/1時間

表 4. アンケート結果に基づく所要帯域試算結果(一次分析)

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	核融合科学研究所	AICS～NIFS: 数TB 東京大学～NIFS: 数10GB	AICS～NIFS (3TB) 東京大学～NIFS (30GB)	0.67 0.067	6.7 0.67	67 6.7
2	計算物質科学イニシアティブ (CMSI)	AICS～CMSI: 1Gbps 分子研～CMSI: 10Gbps 金研～CMSI: 10Gbps	AICS～CMSI 分子研～CMSI 金研～CMSI	1 – –	– 10 10	– – –
3	東京大学 物性研究所	AICS～物性研: 1Gbps 物性研(～東京DC): 10Gbps	AICS～物性研 物性研(～東京DC)	1 –	– 10	– –
4	高エネルギー加速器研究機構					
5	スーパーコンピューティング 技術産業応用協議会	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	地球シミュレータセンタ	ESC(～横浜DC): 10Gbps	ESC(～横浜DC)	–	10	–
7	海洋研究開発機構	AICS～JAMSTEC: 20TB	AICS～JAMSTEC	4.4	44	440
8	国立天文台	AICS～NAOJ: 10GB/s	AICS～NAOJ	–	8	80
9	名古屋大学 太陽地球環境研究所	名大(～名古屋DC): 100Gbps	名大(～名古屋DC)	–	10	100
10	北海道大学 情報基盤センタ	北大(～札幌DC): 2.4Gbps	北大(～札幌DC)	–	2.4	24
11	計算基礎科学連携拠点	AICS～NAOJ～KEK/筑波大: 10GB/s	AICS～NAOJ～KEK/筑 波大	–	8	80
12	大阪大学 臨床医工学融合研究センター	AICS～阪大: 128GB/日	AICS～阪大	0.028	0.28	2.8
13	京都大学 基礎物理学研究所	AICS～京大: 50TB/4日以上	AICS～京大(12.5TB/1 日)	2.75	27.5	275
14	東北大学 サイバーサイエンスセンター	AICS～東北大: 10GB AICS～東北大: 1TB/1日	AICS～東北大 AICS～東北大	0.002 0.22	0.022 2.2	0.22 22
15	東京工業大学 学術国際情報センター	AICS～東工大: 10Gbps以上	AICS～東工大	–	10	–
16	東京大学 生産技術研究所	AICS～東大: 10GB	AICS～東大	0.002	0.022	0.22
17	名古屋大学	AICS-名大: 1TB/1時間	AICS-名大	0.22	2.2	22

5 必要経費

5.1 ネットワーク基盤経費

前項に記載のとおり、平成 23 年度は既存の設備計画にて対応を行うため、HPCI として必要な経費は無い。

平成 24 年度以降は、別途需要予測を精査し検討を行う。

以上

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] DC
Data center の略で、ネットワーク機器や管理サーバ等を設置するために 24 時間 365 日無停電の環境が維持されている場所のこと。データセンター側で、電源・空調の提供、入館管理等を行う。
- [12] IX
Internet Exchange の略で、複数のインターネットサービスプロバイダや学術ネットワークを相互に接続するインターネット上の相互接続ポイント。
- [13] JGN

Japan Gigabit Network の略で、独立行政法人情報通信研究機構(NICT)が運用する研究開発テストベッドネットワークのこと。JGN(平成 11 年度～平成 15 年度)、JGN2(平成 16 年度～平成 19 年度)、JGN2plus(平成 20 年度～平成 22 年度)を経て平成 23 年度より JGN-X が運用される。

※ テストベッド：技術の実運用のための実験・検証・評価を行う場のこと。

[14] JPIX

Japan Internet Exchange の略で、日本インターネットエクスチェンジ株式会社によって運営されている、インターネット上の相互接続点(IX)の名称である。

[15] JPNAP

Japan Network Access Point の略で、インターネットマルチフィード株式会社によって運営されている、インターネット上の相互接続点(IX)の名称である。

[16] PoP

Point of Presence の略で、インターネット利用者が、インターネットに接続する事業者へ最初に接続する拠点を差す。

[17] SINET

Science Information NETwork の略で、700 機関以上の日本全国の大学・研究機関を接続する基盤として、国立情報学研究所が構築・運用している学術情報ネットワークで、研究・教育環境の高度化のため、先進的で多様なネットワークサービスを提供している。さらに、海外の研究ネットワークとも相互接続し、国際学術情報ネットワークの一翼を担っている。平成 23 年度より SINET4 が運用開始する。

[18] VLAN

Virtual LAN の略で、LAN(local area network)において、実際のケーブルや機器間の接続構成とは関係なく、ネットワークに接続された特定の端末だけを仮想的にグループ化する方法のこと。

[19] VPN

Virtual Private Network(仮想閉域ネットワーク)の略で、多数で共用する通信回線の一部を、通信相手を特定したプライベートな専用回線であるかのように仮想的に利用するサービスのこと。

[20] VPLS

Virtual Private LAN Service の略で、ルーターで構築したネットワークで広域イーサネット・サービスを提供するための技術である。

[21] アクセス回線

各大学・研究機関等が学術情報ネットワークを利用するために、各機関からエッジノードまでを結ぶ回線のこと。

[22] エッジ回線

接続拠点であるエッジノードとコアノードを結ぶ回線のこと。

- [23] エッジノード
「ノード」を参照。
- [24] オンデマンド
ユーザの要求があった時にサービスを提供する方式。SINETでは回線帯域などのネットワーク資源を利用者の要求に応じて、必要な時に必要な分だけ確保し提供する。
- [25] コア回線
学術情報ネットワークにおけるコアノード間を接続する回線のこと。
- [26] コアノード
「ノード」を参照。
- [27] セキュリティポリシー
組織全体の情報セキュリティに関する基本方針。広義には、セキュリティ対策基準や個別具体的な実施手順などを含む。
- [28] 帯域
本来は通信で使用する信号の周波数の幅(帯域幅)を指すが、回線においては、単位時間に流すことができるデータ量(データ速度)の意味で用いられる。
- [29] トラフィック
ネットワークを流れるデータのこと。また、そのデータ量のこと。
- [30] ノード
学術情報ネットワーク用の通信機器、電源設備等を設置した施設のこと。
エッジノードは、エッジ回線及びアクセス回線を接続する通信機器等を置く拠点。
コアノードは、コア回線及びエッジ回線を接続する通信機器等を置く拠点。
- [31] ノードインタフェース
ノードに設置される通信機器の回線接続部。
- [32] バックボーン回線
ネットワーク回線における基盤となる部分。アクセス回線部分に対比して使用される。
- [33] ファイヤーウォール
組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステム。
- [34] 閉域網
インターネットをあたかもプライベートな専用回線として利用するネットワーク形態。
- [35] レイヤ
OSI 参照モデルで規定されたネットワーク対応機器の機能を7階層に分割したもので、個々の機器やソフトウェアの役割を規定している。レイヤが低いほど、電気信号の形式やケーブルなど物理的実体に近い仕様を規定しており、上位のレイヤは、データ形式や表示方式などソフトウェアや人間に近い仕様を規定する。

(参考1) 学術情報ネットワーク加入規定

(目的)

第1条 この規程は、国立情報学研究所(以下「研究所」という。)が整備する学術情報ネットワーク(以下「ネットワーク」という。)への加入に関し必要な事項を定めることを目的とする。

(加入者の資格)

第2条 ネットワークへ加入できる者は、次の各号の一に該当する機関若しくは機関の部局等(以下「加入者」という。)とする。

- 一 大学、短期大学、高等専門学校、大学共同利用機関等
- 二 研究所の事業に協力する機関
- 三 国公立試験研究機関並びに研究又は研究支援を目的とする独立行政法人及び特殊法人等
- 四 前3号に定める機関と共同で研究等を行う機関
- 五 学会、学術研究法人及び大学に相当する教育施設等
- 六 研究を目的とするネットワークの参加機関
- 七 その他国立情報学研究所長(以下「所長」という。)が適当と認めた機関

(加入の申請)

第3条 加入しようとする者は、所定の利用申請書により、所長に加入の承認を求めなければならない。

2 加入の申請は、機関の長が行うものとする。

(加入の承認)

第4条 所長は、前条の申請について適当と認めた場合には、これを承認し、接続すべきノード(研究所が電気通信設備を設置した機関)を設定するものとする。

(変更の申請承認)

第5条 加入者は、承認を受けた事項を変更しようとする場合には、所長に申請し、変更の承認を求めなければならない。

2 所長は、前項の申請について適当と認めた場合には、これを承認するものとする。

(加入の解除)

第6条 加入者は、加入の解除をしようとする場合は、速やかに所長に届け出なければならない。

(加入に当たっての遵守事項)

第7条 加入者は、次の各号に掲げる事項を遵守しなければならない。

- 一 研究・教育並びにその支援のための管理業務以外の目的にネットワークを利用しないこと。
- 二 営利を目的とした利用を行わないこと。
- 三 通信の秘密を侵害しないこと。
- 四 ネットワークの運用に支障を及ぼすような利用を行わないこと。
- 五 ネットワーク及び接続するコンピュータに対する不正行為等が発生しないよう最善の努力を払うこと。

六 その他所長が別に定める事項

(加入の取消し)

第8条 所長は、前条に違反したと認められる加入者に対して、加入の承認を取り消すことができる。

(調査・協力)

第9条 所長は、加入者に対して、ネットワークの利用状況、運用実態、障害時の対応、不正行為に対する情報収集等についての調査・協力を求めることができる。

(経費の負担)

第10条 加入に係る経費は、加入者の負担とする。ただし、その負担の内容については、加入者及び当該ノードの長と協議して所長が定める。

(雑則)

第11条 この規程に定めるもののほか、ネットワークの加入について必要な事項は、別に定める。

(参考2) 学術情報ネットワーク加入細則

(目的)

第1条 この細則は、国立情報学研究所学術情報ネットワーク加入規程第11条の規程に基づき、国立情報学研究所(以下「研究所」という。)が整備・運用する学術情報ネットワーク(以下「ネットワーク」という。)への加入及びネットワークが提供する接続等サービス(以下「サービス」という。)の利用を円滑に行うために必要な事項を定めることを目的とする。

(定義)

第2条 本細則における用語の定義は、次のとおりとする。

一 「加入」とは、第3条及び第4条の手続きを経てネットワークに加わることをいい、当該加入した機関等を「加入機関」という。

二 「管理者 ID」とは、加入が承認された機関の管理者に付与する識別符号をいう。

三 「利用」とは、第5条及び第6条の手続きを経て承認され、サービスを利用することをいう。

四 「利用サービス管理者」とは、利用を承認されたサービスを管理する者をいう。

五 「利用サービス ID」とは、利用サービス管理者に付与する識別符号をいう。

(加入の申請)

第3条 加入を申請する機関の長は、ネットワーク側の接続拠点が異なり、かつ、管理・運用主体が異なるキャンパスネットワーク毎に、別に定める加入申請書により、研究所の所長(以下「所長」という。)に申請するものとする。

(加入の承認)

第4条 所長は、前条の申請を審査し、加入を承認した場合、別に定める加入承認書を交付するとともに、加入機関の管理者に対し、管理者 ID を発行する。

2 研究所は、次の各号の一に該当する場合は、加入を承認しないことができるものとする。

一 第7条第5項の規定に基づき、過去に研究所から強制的に加入の解除処分を受けたことがある機関からの申請

二 加入申請書の内容に虚偽の記載が認められたとき。

三 その他、研究所が加入申請を承諾することが不適當であると判断したとき。

(利用の申請)

第5条 加入機関は、利用サービス管理者を指定して、希望するサービス毎に、別に定める利用申請書により、研究所に申請するものとする。

(利用の承認)

第6条 研究所は、前条の申請を審査し、利用を承認した場合、別に定める利用承認書を交付するとともに、1サービスごとに利用サービス ID を発行する。

2 前項にかかわらず、研究所が1利用サービス管理者に複数サービスの利用を認める場合は、同一の利用サービス ID で利用を承認することができるものとする。

3 次の場合は、利用を承認しないことができる。

一 加入機関以外からの申請

二 第7条第5項の規定に基づき、過去に研究所から強制的に利用の終了処分を受けたことがある者からの申請

三 利用申請書の内容に虚偽の記載が認められたとき。

四 その他、研究所が利用申請を承諾することが不適当であると判断したとき。

(加入の解除及び利用の終了)

第7条 加入機関がネットワークの加入を解除する場合は、所長に対し、研究所が別に定める加入解除届を提出しなければならない。この場合、届出に記載された日の翌日から解除の効力が生じるものとする。

2 利用サービス管理者がサービスの利用を終了する場合、加入機関は、研究所が別に定める利用終了届を提出しなければならない。この場合、届出に記載された日の翌日から終了の効力が生じるものとする。

3 加入機関が加入を解除した場合は、サービスの利用も終了するものとする。

4 第1項及び第2項により、加入解除又は利用終了を届け出た機関又は利用サービス管理者は、ノードに設置した通信回線を含む電気通信設備等を速やかに撤去しなければならない。

5 加入機関及び利用サービス管理者が、次の各号の一に該当する場合、研究所は、書面による通知により、強制的に加入の解除もしくは利用の終了させることができる。

一 サービスの利用期限が過ぎたとき。

二 申請書等に虚偽の記載があることが判明したとき。

三 第9条に規定する変更届の提出を遵守しなかった場合などによって、研究所から利用サービス管理者への連絡ができなくなったとき。

四 本細則に違反したとき。

五 ネットワーク上において、第三者の利益を損ねる行為が認められたとき。

六 その他、研究所が不適当と判断する相当の理由があるとき。

(ID 及びパスワードの管理)

第8条 加入機関は、研究所が発行する管理者 ID とそのパスワードについて、当該加入機関の管理者が指定する者以外に開示又は漏洩してはならない。

2 利用サービス管理者は、研究所が発行する利用サービス ID とそのパスワードについて、当該利用サービス管理者以外の者の開示または漏洩してはならないものとする。

3 管理者 ID 及び利用サービス ID とそのパスワードを紛失又は盗難にあった場合は、直ちに研究所に連絡するものとする。

4 管理者 ID 及び利用サービス ID とそのパスワードの再発行を希望する場合は、別に定める ID 再発行届により、研究所に届け出るものとする。

(申請の変更)

第9条 加入機関及び利用サービス管理者は、申請内容に変更があった場合、別に定める申請事項変更届により、速やかに研究所に届け出るものとする。

(責任の分界点)

第10条 加入機関及び利用サービス管理者と、研究所の責任分界点は、研究所が接続拠点(以下「ノード」という。)に設置した利用に係る接続用通信機器のインタフェースとする。

(障害申告)

第11条 加入機関及び利用サービス管理者は、障害等によりネットワークの利用ができなくなったときは、調査を行った上で、その障害部分が前条に規定されるところの研究所側にあると判断される場合には、研究所へ申告するものとする。

2 研究所は、前項の障害申告に対して、加入機関及び利用サービス管理者に障害対策のための協力を求めることができる。

(サービスの中止)

第12条 研究所は、緊急時のやむを得ない場合の他次の各号の一に該当する場合、ネットワークのサービスを一時中止することができる。サービスを一時中止する場合は、可能な限り速やかに、加入機関に通知するものとする。

- 一 設備の保守又は工事のとき。
- 二 災害等の不可抗力により、サービス提供が困難になったとき。
- 三 通信事業者の責により、サービス提供が困難になったとき。

(経費負担)

第13条 研究所の設置したノードへの加入機関または利用の接続及び接続のための設備の設置又は管理等の一切については、加入機関が自らの費用負担及び責任において行うものとする。

(個人情報等の取扱い)

第14条 個人情報の取扱いに関し必要な事項は、情報・システム研究機構個人情報保護規程において定めるものとする。

(ネットワーク利用情報の取扱い)

第15条 研究所は、ネットワークの運営に伴い研究所が取得し保有する情報(以下「ネットワーク利用情報」という。)について、運用支援又は研究目的で利用、改変又はその他のデータ操作等を行うことができるものとする。

2 研究所は、前項により、得られた研究成果又はネットワーク利用情報について、ネットワーク利用情報の主体又は、属性たる個人若しくは機関等が判別できない形に処理することに留意した上で、開示・公表等ができるものとする。

(加入機関及び利用サービス管理者の責任)

第16条 利用サービス管理者及び管理者の監督下で利用する者のネットワークに関する行為は、全て当該利用サービス管理者の所属する加入機関の責任による行為とみなされるものとする。

2 加入機関は、ネットワークの利用に伴い、加入機関又は利用サービス管理者の責めに帰すべき理由によって第三者に損害を与えたときは、直ちにこれを賠償する等自らこれを解決するものとする。

3 利用サービス管理者は、ネットワークの利用に伴い、利用サービス管理者の責めに帰すべき

理由によって第三者に損害を与えたときは、加入機関と協力して、直ちにこれを賠償する等自らこれを解決するものとする。

(細則の遵守)

第17条 加入機関及び利用サービス管理者は、この細則の内容を承諾したものとし、遵守しなければならない。

(研究所の免責)

第18条 研究所は次の各号の一に該当する場合、責任を負わないものとする。

- 一 サービスの利用による加入機関又は利用サービス管理者に発生する紛争・損害等
- 二 第12条の規定に基づくサービスの一時停止により発生する損害等
- 三 地域IP網等の通信事業者が管理するネットワーク等の障害

(細則の変更)

第19条 研究所が必要と認めた場合は、加入機関及び利用サービス管理者の承諾を得ることなく本細則を変更できるものとする。

(雑則)

第20条 この細則に定めるもののほか、ネットワークの運用に関し必要な事項は、別に定める。

以上