# 高性能分散計算環境のための認証基盤の設計

合田憲人[†1] 東田学[†2] 坂根栄作[†1]
天野浩文[†3] 小林克志[†4] 棟朝雅晴[†5]
江川隆輔[†6] 建部修見[†7] 鴨志田良和[†8]
滝澤真一朗[†9] 永井亨[†10]
岩下武史[†11] 石川裕[†8]

本稿では，現在文部科学省により整備が進められている革新的ハイパフォーマンス・コンピューティング・インフラ（HPCI）のための認証基盤の設計について述べる．本認証基盤では，グリッド上の認証技術である Grid Security Infrastructure (GSI)，および認証連携技術である Shibboleth を用いることにより，HPCI を構成する計算機や共用ストレージに対するシングルサインオンを実現する．本稿ではまた，本認証基盤の設計を検証するために構築した実験環境上での実証実験についても報告する．

# Design of Authentication System for High Performance Distributed Computing Environment

Kento Aida,[†1] Manabu Higashida,[†2] Eisaku Sakane,[†1]
Hirofumi Amano,[†3] Katsushi Kobayashi,[†4]
Masaharu Munetomo,[†5] Ryusuke Egawa,[†6] Osamu Tatebe,[†7]
Yoshikazu Kamoshida,[†8] Shin'ichiro Takizawa,[†9] Toru Nagai,[†10]
Takeshi Iwashita[†11] and Yutaka Ishikawa[†8]

This paper presents design of an authentication system for the High Performance Computing Infrastructure (HPCI), which is currently deployed by the Ministry of Education, Culture, Sports, Science and Technology. The presented authentication system enables single sign-on to computers and shared storages on HPCI by utilizing the authentication mechanism on the Grid, "Grid Security Infrastructure (GSI)", and the identity federation mechanism, "Shibboleth". This paper also presents the experiments conducted on the testbed for the presented authentication system.

†1 国立情報学研究所
National Institute of Informatics
†2 大阪大学
Osaka University
†3 九州大学
Kyushu University
†4 理化学研究所
RIKEN
†5 北海道大学
Hokkaido University
†6 東北大学
Tohoku University
†7 筑波大学
University of Tsukuba
†8 東京大学
The University of Tokyo
†9 東京工業大学
Tokyo Institute of Technology
†10 名古屋大学
Nagoya University
†11 京都大学
Kyoto University

## 1. はじめに

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

るのではなく，これらの資源を共有できる高性能分散計算環境が必要となる．このような背景のもと，米国の TeraGrid（現在 XSEDE）[2] や欧州の PRACE[3] といった高性能計算基盤が構築されているほか，日本でも，現在開発中の京コンピュータ[4] と国内のスーパーコンピュータや高性能ストレージを連携して利用するための革新的ハイパフォーマンス・コンピューティング・インフラ（HPCI）[5] の構築が進められている．

これらの高性能分散計算環境の運用では，複数の異なる組織が運用する資源（計算機やストレージ）を一度の認証手続きで利用可能とするシングルサインオンを実現することが重要な課題となる．分散計算環境上でシングルサインオンを実現する要素技術は従来より提案されている．しかし，実運用サービスを既に提供している組織の資源間でシングルサインオンを実現するためには，各組織の異なる運用方法や既存ユーザの利用方法に適した要素技術の選択，組織間の運用ポリシーの調整が必要であり，認証基盤の設計やシステム配備，運用方法を確立することは難しい．従って，実運用サービスを提供する分散計算環境上での認証基盤の設計事例を公開し，情報共有を行うことは，今後の認証基盤の設計や運用技術を確立するために重要である．

本稿では，HPCI のための認証基盤の設計について述べる．HPCI では，シングルサインオンにより HPCI 上のスーパーコンピュータへの遠隔ログインおよび共用ストレージへのアクセスを可能とすることを目指している[5]．これを実現するため，本認証基盤でシングルサインオンを実現するための機構は，グリッド技術を用いたシングルサインオン技術である Grid Security Infrastructure[6],[7] および分散したアカウント管理システムを連携するための技術である Shibboleth[8],[9] を用いて設計されている．ユーザは，HPCI 上の一組織（情報基盤センター等）から発行される HPCI を利用するためのアカウント（HPCI アカウント）を用いて，HPCI 上の資源にシングルサインオンすることが可能である．本認証基盤の設計を検証するため，認証基盤のプロトタイプシステムを構築し，実証実験を行った．本稿では実証実験についても報告する．

以後，2 節では HPCI のシステム概要について述べる．3 節では認証基盤の設計を示し，4 節では実証実験について報告する．5 節では関連研究を示し，最後に 6 節ではまとめと今後の計画について述べる．

## 2. HPCI の概要

HPCI では，京コンピュータと全国のスーパーコンピュータセンターを高速ネットワークでつなげるとともに共用ストレージを導入し，透過的アクセスを提供することによりユーザの利便性を高めることを目的としている．現在，HPCI 運用開始時に以下の環境を提供するための整備が進められている．なお，これらの環境については運用開始後に拡張されることも検討されている．

HPCI のネットワークは汎用の広域ネットワークであり，国立情報学研究所が運用する SINET4[10] が利用される．計算機は，京コンピュータおよび 9 大学（北海道大学，東北大学，筑波大学，東京大学，東京工業大学，名古屋大学，京都大学，大阪大学，九州大学）の情報基盤センターが運用するスーパーコンピュータが利用されるほか，これらの計算機群からアクセス可能な共用ストレージとして，理化学研究所および東京大学が運用するストレージ[11] が提供される．また，特殊な OS やライブラリを必要とするアプリケーションの実験や，管理者権限を必要とするような実験を行うことを目的として，VM 環境（先端ソフトウェア運用基盤）も運用される計画である[12]．

**図 1** は HPCI 運用開始時点の環境をユーザが利用する手順を示している．HPCI 上の資源を利用するためには，HPCI を利用する研究課題の申請を行い，利用が認められる必要がある．課題申請は，研究を進めるグループ毎に行われ，採択された課題の参加者には HPCI を利用するためのアカウント（HPCI アカウント）が発行される．HPCI アカウントを取得したユーザは，本アカウントを用いて認証ポータル上でサインオン手続きを行うことにより，電子証明書の取得や，取得した証明書を用いた計算機群へのログイン，計算機群からの共用ストレージへのアクセスが可能となる．

図中には示されていないが，HPCI ではユーザ管理支援を目的として，HPCI の利用申請やヘルプデスク等のシステムが Web ポータル上で提供される予定である[13]．また，先端ソフトウェア運用基盤では，ユーザが VM の起動や制御を行う機能を Web ポータル経由で提供する予定である．ユーザは，これらの Web ポータル上のサービスの利用も HPCI アカウントを用いたシングルサインオンにより利用可能である．

## 3. 認証基盤の設計

HPCI の認証基盤の目的は，HPCI 上の資源へのシングルサインオンを実現する認証・認可サービスを提供することである．本節では，2 節であげた HPCI を構成する組織が運用する資源に対してシングルサインオンを実現するための認証基盤への要求要件を定義し，

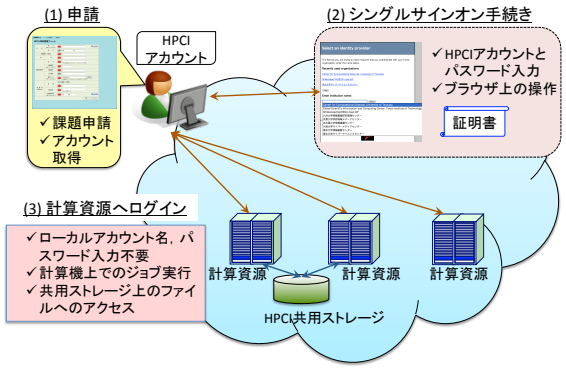


**図 1** HPCI の利用手順

次にこの要求要件を満足するために採用した要素技術，さらに認証基盤アーキテクチャについて述べる．

### 3.1 要求要件

HPCI の認証基盤では，シングルサインオンを実現する機能だけでなく，基盤を安定かつ継続して，ユーザに使いやすい方法で提供することが必要である．そのため，認証基盤は，以下に示す機能性，運用性，利便性に関する要件を満足して設計される必要がある．

(1) 機能性

(a) **シングルサインオン**：HPCI を構成する資源はそれぞれ独立して運用されており，現在，ユーザは資源毎に異なるユーザアカウント（ローカルアカウント）やパスワードを用いて，計算機に SSH を用いてログインして利用している．これに対して HPCI では，HPCI 上で有効な共通アカウント（HPCI アカウント）を用いることにより，全ての計算機に SSH を用いてログインすることや共用ストレージ上のファイルへのアクセスができる必要がある．

(b) **委譲**：HPCI では，ユーザが複数の資源を連携させて利用することが想定される．そのため，ユーザがある計算機にログイン後，さらに別の計算機へログインすることや共用ストレージ上のファイルへアクセスすることを認証手続き（ローカルアカウントやパスワードの入力）を行うことなく実現できる必要がある．

(2) 運用性

(a) **認可**：HPCI 上で提供される資源は，HPCI のユーザに占有されるわけではなく，資源を運用する組織の多くのローカルユーザからも利用される．そのため，HPCI 上で認証されたユーザが資源を利用するための認可については，資源を運用する組織が制御できる必要がある．

(b) **アカウント管理負荷分散**：HPCI のユーザ数は単一組織内のユーザ数に比べて多いため，HPCI のためのアカウント管理システムを新たに構築して運用することは多くの運用コストを必要とする．そのため，アカウント管理を複数組織に分散することにより，管理負荷の分散を図る必要がある．

(c) **安定運用**：HPCI の認証基盤には，HPCI に提供されるスーパーコンピュータの運用と同等の安定性および継続性が求められる．そのため，認証基盤を実現する要素技術やソフトウェアは，成熟した技術，かつ可能な限り利用実績のあるソフトウェアである必要がある．またアカウント管理システムは，既に安定運用されているシステムを最大限に活用する必要がある．

(d) **国際連携**：現在，HPCI と海外の計算基盤との連携運用については検討段階であるが，将来的に HPCI 上で認証を受けたユーザが海外の資源を利用することも想定される．そのため，HPCI の認証基盤は，海外の主要な計算基盤での認証技術との相互運用が技術的に容易である必要がある．

(3) 利便性

(a) **ユーザインタフェース**：HPCI のユーザが持つ分散計算環境を利用するための知識のレベルは多岐にわたることが想定されるため，シングルサインオン手続きは，高度な知識や技術を持たないユーザにとっても簡便である必要がある．

(b) **複数クライアント環境**：HPCI のユーザの利用環境（OS 等）は多岐にわたるため，より多くの環境からシングルサインオンが可能である必要がある．

### 3.2 要素技術

HPCI では，HPCI 上の計算機へのログイン，共用ストレージへのアクセス，ユーザ管理支援や先端ソフトウェア運用基盤の Web ポータルの利用に必要な認証が，3.1 節で示した要求要件を満たしつつ，シングルサインオンにより実現される必要がある．HPCI 認

証基盤の設計では，これらの要求要件を満足するために，Grid Security Infrastructure (GSI)[6),7)] および Shibboleth[8),9)] を用いて認証基盤を実現することとした．具体的には，GSI は HPCI 上の計算機へのログインや共用ストレージへのアクセス時の認証に用いられる．また，Shibboleth は，分散管理される HPCI アカウントを用いてユーザ管理支援や先端ソフトウェア運用基盤の Web ポータルを利用する際の認証に用いられる．また，GSI で必要となる証明書の発行や操作も Web ポータル上で提供されており，このための認証にも Shibboleth が用いられる．

本節では，以後，HPCI の認証基盤を実現するために用いられた要素技術として，GSI，Shibboleth，ユーザインタフェースについて述べるとともに，これらの要素技術と 3.1 節に示した要求要件との対応を**表 1** にまとめて示す．

#### 3.2.1 GSI

GSI は，Public Key Infrastructure (PKI)[14)] 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から作成される代理証明書を用いて，複数の資源に対するシングルサインオンを実現する．代理証明書は，新たに作成された秘密鍵と公開鍵を含み，ユーザの秘密鍵により署名されている．認証時には，代理証明書の秘密鍵を除いた部分が遠隔資源に送付され，PKI に基づく認証処理が行われる．ユーザは，代理証明書を生成する際に一度だけユーザの秘密鍵を復号化するためのパスフレーズを入力するが，代理証明書中の秘密鍵は暗号化されていないため，その後の認証ではパスフレーズを入力する必要がない．また GSI では，ユーザが GSI 認証を経て遠隔資源にログインした際に，遠隔資源上に新たな代理証明書（ログイン元の代理証明書によって署名された代理証明書）を生成することができる．この新たな代理証明書を用いることにより，さらに別の資源での認証をパスフレーズを入力することなく行うことができる．

以上のように GSI を用いることにより，3.1 に示した機能性に関する要件のシングルサインオンおよび委譲を満足することができる．GSI の認可処理はユーザのクライアント証明書の Subject DN と資源のローカルアカウントをマッピングすることにより実現されるが，マッピング処理は資源を提供する組織が制御できるため，3.1 の運用性に関する要件のうち，認可を満足することができる．また GSI は，グリッドミドルウェアとして長い実績を持つ Globus Toolkit 上に実装されている[7)] だけでなく，XSEDE[2)] や PRACE[3)] 等の実用サービスを提供する基盤上で既に採用されている．また，GSI のように PKI を用いた分散計算環境の国際的な相互認証に関して，その運用ポリシーを議論する組織である International Grid Trust Federation (IGTF)[15)] が 2003 年より活動を行っている．以上の理由により，GSI を用いることで運用性の安定運用および国際連携に関する要件も満たすことができる．

#### 3.2.2 Shibboleth

HPCI の認証基盤を実現する上で，HPCI アカウントの管理方法は重要な課題である．HPCI 上の計算機や共用ストレージを利用するためのローカルアカウントは，各資源の運用組織のアカウント管理システムにより管理されているため，これらの他にさらに HPCI アカウント用のアカウント管理システムを運用することは効率が悪い．そのため，本認証基盤では，HPCI に資源を提供する組織が運用する既存のアカウント管理システム上に HPCI アカウントを登録するとともに，これらのアカウント管理システムは分散して存在するため，Shibboleth 認証連携技術を用いて分散したアカウント管理システムを連携させる．

Shibboleth は Security Assertion Markup Language (SAML)[16)] を用いて Web 認証処理を連携させる技術である．Shibboleth では，ネットワーク上でサービスを提供するサービスプロバイダ（SP）それぞれがユーザアカウントを管理するのではなく，ユーザが SP 上でサインオンする際に，SP がユーザのアカウントを管理するアイデンティティプロバイダ（IdP）に認証処理を依頼することで複数の組織間で連携した認証を実現している．

LDAP や Kerberos などによる組織ごとに異なるアカウント管理システムを Shibboleth の IdP として統一的に連携運用することにより，3.1 の運用性に関する要件のうち，アカウント管理負荷分散を満足することができる．また，Shibboleth は Internet2 で開発され[9)]，米国の研究教育機関間の認証連携サービスを提供している InCommon[17)] において利用されている実績をもつため，運用性の安定運用に関する要件を満足する．

#### 3.2.3 ユーザインタフェース

ユーザの利便性を向上させるためには，より使い易いユーザインタフェースを提供することが重要である．HPCI の認証基盤では，HPCI 上の資源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．ユーザは，認証ポータル上でクライアント証明書の発行や代理証明書の生成を行うことができる．本認証基盤では，クライアント証明書を保管する証明書リポジトリを提供することにより，PKI に精通してないユーザでも

**表 1** 要求要件に対する対応

| 分類 | 要求要件 | GSI | Shibboleth |
|---|---|---|---|
| 機能性 | シングルサインオン | 計算機ログイン，共用ストレージアクセス | Web ポータル利用 |
| | 委譲 | 計算機ログイン，共用ストレージアクセス | - |
| 運用性 | 認可 | grid-mapfile による資源毎の認可 | Shibboleth 属性による Web サーバ毎の認可 |
| | アカウント管理負荷分散 | - | 複数 IdP による HPCI アカウント管理および Shibboleth 認証連携 |
| | 安定運用 | 運用実績多 | 運用実績多 |
| | 国際連携 | 海外での運用実績多，IGTF による国際連携活動 | 海外での運用実績多 |
| 利便性 | ユーザインタフェース | Web ブラウザ／コマンドライン | Web ブラウザ |
| | 複数クライアント環境 | Windows, MacOS, Linux | Web ブラウザ |

証明書をより安全に管理することを可能としている．ユーザは認証ポータルにサインオン後，証明書リポジトリ内のクライアント証明書の操作が可能である．また，PKI に精通したユーザがクライアント証明書をローカル計算機に保管することも可能である．

本認証ポータルにより，3.1 に示す利便性のユーザインタフェースおよび複数クライアント環境に関する要件を満たすことができる．また，本インタフェースは，既存の CUI や，NGS[18] が Java ベースで開発した Cert Wizard との親和性も高い．さらに，後述の GSI-SSH 等，GSI 認証に対応したクライアントソフトウェアには，Linux，MacOS，Windows に対応したものが既に開発されているため，複数クライアント環境から HPCI 上の資源にアクセス可能である．

### 3.3 認証基盤のアーキテクチャ

HPCI 認証基盤は，**表 2** に示す組織が運用するシステムから構成されている．**図 2** は，各機関が運用するシステムの関係を示す．HPCI 認証基盤では，課題申請から審査・選定を経て，認証のためのアカウント発行や資源利用の認可のための構成情報を一元管理している．この構成情報を元に，要素技術を連携させる枠組みを適宜開発し，HPCI アカウント IdP 運用機関に業務負荷を分散させることで，より多くの利用者を支援可能な体制を整備している。

#### 3.3.1 認証局運用機関

認証局運用機関は，GSI において必要となるクライアント証明書およびサーバ証明書を発行する組織である．図中の証明書管理システムは，ユーザからの証明書の発行・失効等の申請を受け付け，認証局システムに処理を依頼するソフトウェアである．認証局システムから発行されたクライアント証明書は，証明書リポジトリに保管される．認証局システムは，Shibboleth SP[9] として実装されており，証明書申請時のユーザの認証を Shibboleth IdP に依頼する．また，Shibboleth DS[9] は，認証を受けるアカウントを管理する Shibboleth IdP[9] に認証処理を転送する役割を持つ．認証局運用機関では，認証局システム用ソフトウェアとして NAREGI-CA[19]，証明書リポジトリとして MyProxy[20] を用いる．Shibboleth を用いた認証連携には，Internet2 で公開されているソフトウェアパッケージ[9] を用いる．証明書管理システム用ソフト

**表 2** 認証基盤運用機関

| 運用機関 | 役割 |
|---|---|
| 認証局運用機関 | HPCI 環境上で利用される電子証明書を発行する． |
| 認証ポータル運用機関 | HPCI 環境にシングルサインオンするための認証ポータルを運用する． |
| HPCI アカウント IdP 運用機関 | HPCI 環境にシングルサインオンするためのアカウントを発行・管理する． |
| 資源提供機関 | HPCI のユーザに対して計算機やストレージ等の資源を提供する． |

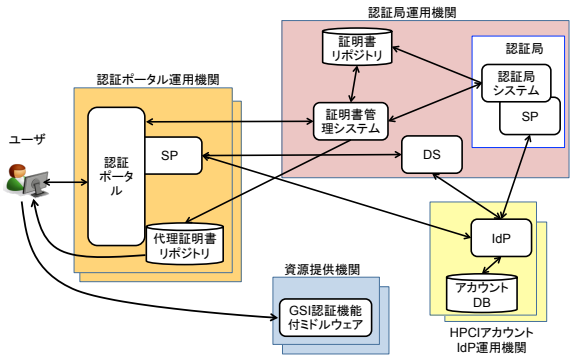


**図 2** 認証基盤のアーキテクチャ

ウェアについては，HPCI 上でのユーザ管理向けに特化した機能が必要なため，新たに開発したものを用いる．また，これらのソフトウェアを実行するサーバには，認証局が発行するサーバ証明書が設置され，サーバ間の通信時には適切にホスト認証が行われる．

認証局は，IGTF で定められた国際基準である MICS（Member Integrated X.509 Credential Services）プロファイル[21] に基づいて証明書を発行する．MICS プロファイルでは，ユーザの本人性確認を他の信頼できるアカウント管理システム上のデータを用いて行う．即ち，ユーザが信頼できる組織のアカウントを所有していることをもって，ユーザの本人性確認を行う．従ってユーザは，後述の HPCI アカウントを管理する組織から発行された HPCI アカウントを用いてポータルにサインオンすることにより，クライアント証明書をオンライン処理のみで取得することができる．また，クライアント証明書を証明書リポジトリで集中管理することが可能であるが，この場合は，証明書リポジトリをアクセスするための認証手段を別途提供する必要が生じる．本認証基盤では，Shibboleth による Web 認証連携によってこのための認証が実現される．

認証局の運用では，ユーザにクライアント証明書を発行するための業務負荷が課題となる．課題審査・選定を経て利用資格を得たユーザは，いずれかの HPCI アカウント IdP 運用機関の窓口で対面認証に相当する本人性確認を受ける．これが済むと利用許可を受けた計算資源を有する資源提供機関のアカウント発行処理が行われ，Shibboleth 認証が可能となり，Web 認証連携が行われている認証ポータルから電子証明書の発行が可能となる．このような枠組みによって，認証局の業務負荷が軽減される．

#### 3.3.2 認証ポータル運用機関

認証ポータル運用機関は，HPCI にユーザがシングルサインオンするための Web ポータル（認証ポータル）を提供する組織である．認証ポータルは，Shibboleth による Web 認証フェデレーションから GSI 認証への認証ブリッジを行うための Web インターフェースを提供する．具体的には，認証ポータルは Shibboleth SP として実装されており，ユーザ認証をユーザの HPCI アカウントを管理する Shibboleth IdP に依頼する．ポータル上でサインオンしたユーザは，代理証明書を生成することができ，生成された代理証明書は代理証明書リポジトリに保存される．代理証明書は生成時に有効期間を設定することにより万一漏出した場合の影響範囲を限定することができる．ユーザは，認証ポータル上で 1 時間単位で最大 168 時間 (1 週間) まで有効期間を設定できる．例えば，有効期間を 24 時間と指定した場合，24 時間以内は認証手続きなしで遠隔計算機にログインできる．

認証ポータル用ソフトウェアは，HPCI 向けに特化したインタフェースが必要なため，新たに開発したものを用いる．また，代理証明書リポジトリには MyProxy を用いる．認証ポータルは，冗長性を確保するために複数の組織が運用することが可能であり，ユーザはどの認証ポータル上でもシングルサインオンを行うことができる．また，別途，Shibboleth の ePPN (eduPersonPrincipalName) 属性とクライアント証明書の Subject DN を対応付けるためのユーザ管理支援システムが構築されており，このシステムと認証ポータルを組み合わせることにより，MICS プロファイル[21] に基づいた半自動的な認証局運用を可能にしている．本認証基盤では，このような枠組みによって，認証におけるアカウント管理の負荷分散が実現されている．

#### 3.3.3 HPCI アカウント IdP 運用機関

HPCI アカウント IdP 運用機関は，HPCI アカウントの認証機能を提供する組織である．本機関では，自らが運用するアカウント管理システム（アカウント DB）に HPCI アカウントを登録する．アカウント DB は Shibboleth IdP と連携しており，Shibboleth IdP は，Shibboleth SP から要求された HPCI アカウントの認証を行い，認証結果を Shibboleth SP に返す．

#### 3.3.4 資源提供機関

資源提供機関は，HPCI に対して計算機や共用ストレージを提供する組織である．これらの資源を利用するためのミドルウェアについては，GSI 認証を用いて計算機に SSH でログインするために GSI-SSH[22]，共用ストレージ上のファイルアクセスのために Gfarm2[23] を用いる．資源提供機関は HPCI アカウント IdP 運用機関の機能も持つことが想定されるが，本稿では，認証基盤の機能を明確に分類するために両者を分けて定義している．

資源提供機関では，GSI の認可処理を実現するため，各ユーザのクライアント証明書の Subject DN とユーザのローカルアカウントを対応づける grid-mapfile を作成する．Subject DN は証明書発行時に認証局運用機関が決定するため，資源提供機関は認証局運用機関から Subject DN を入手し，ローカルアカウントに対応づける必要がある．HPCI 上のユーザには HPCI の利用を申請する以前に HPCI-ID と呼ばれる番号が割り当てられており[13]，認証局運用機関および資源提供機関に HPCI-ID が通知されている．資源提供機関で

は，この HPCI-ID を用いることにより，Subject DN とローカルアカウントの対応付けを行うことができる．具体的には，以下の手順で対応付けが行われる．

(1) 認証局運用機関は，ユーザからのクライアント証明書発行申請時にユーザの HPCI-ID を申請情報として得ることにより，HPCI-ID と Subject DN の対応情報を作成し，サブバージョン（SVN）を用いて資源提供機関に公開する．

(2) 資源提供機関は，ローカルアカウント作成時にユーザの HPCI-ID を申請情報として得るため，同様に HPCI-ID とローカルアカウントの対応情報を作成する．

(3) 資源提供機関は，定期的に認証局運用機関の SVN から HPCI-ID と Subject DN の対応情報をダウンロードし，手元の HPCI-ID とローカルアカウントとの対応情報と照合することにより，grid-mapfile を作成する．

これらの処理は，スクリプトを用いた自動処理が可能であり，資源提供機関における grid-mapfile 管理に要する負荷を抑えることができる．以上のように，課題審査・選定を経て割り当てられる資源配分に対応した gird-mapfile 情報を配信することによって，認可におけるアカウント管理の負荷分散が実現されている．

## 4. 実証実験

本稿で示した認証基盤の実証実験を行うため，9 大学の情報基盤センター，国立情報学研究所（NII）から構成される認証基盤実験環境を構築した．本節では，本環境上での実験結果について述べる．

### 4.1 動作試験

本実験環境では，**図 3** に示すように，NII が認証局運用機関および認証ポータル運用機関としての役割を持ち，認証局システム，証明書管理システム，証明書リポジトリ，認証ポータル，代理証明書リポジトリ，Shibboleth DS（DS）を運用する．また，他の情報基盤センター群は，HPCI アカウント IdP 運用機関および資源提供機関としての役割を持ち，各自が運用するユーザアカウント管理システム（アカウント DB）と連携した Shibboleth IdP（IdP），ユーザが計算機にログインするための GSI-SSH サーバを運用する．また，情報基盤センターでは，ユーザの利用環境として，Web ブラウザや GSI-SSH クライアントも運用する．**表 3** は，実証実験に用いたソフトウェアの一覧を示す．なお，証明書管理システム（証明書リポジトリ含む）および認証ポータルは，現在，HPCI 向けのソフトウェアを開発中のため，NAREGI Middleware

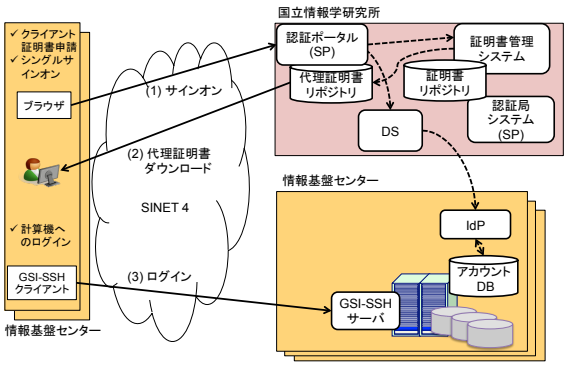


**図 3** 実証実験環境

**表 3** 認証基盤ソフトウェア一覧

| システム名 | ソフトウェア名 |
|---|---|
| 認証局システム | NAREGI-CA 2.3.4 (Shibboleth 対応版) |
| 代理証明書リポジトリ | MyProxy 4.2 |
| Shibboleth SP<br>Shibboleth DS<br>Shibboleth IdP | Shibboleth SP 2.4.3<br>Shibboleth DS 1.1.2<br>Shibboleth IdP 2.3.2 |
| GSI-SSH サーバ | Globus Toolkit 5.0.4 |

1.1[24] に含まれる UMS およびポータルを本実証実験向けに改編したプロトタイプソフトウェアを用いた．

本実証実験の結果，本環境上でユーザによる以下の操作が可能であり，本認証基盤により HPCI 上の計算機へのシングルサインオンが可能であることが確認された．

- Shibboleth 認証連携を用いた認証ポータル上でのサインオン
- 認証ポータル上でのクライアント証明書取得
- 認証ポータル上での代理証明書生成およびダウンロード
- GSI-SSH を用いた 9 大学情報基盤センターの計算機へのログイン

認証ポータルおよび代理証明書リポジトリを運用するサーバには，UPKI イニシアティブから発行されたサーバ証明書[25] が配置され，ユーザのクライアント環境と本サーバ間の通信は，SSL により安全に実現される．

Shibboleth に関する実験では，まず NII 内にテスト用の IdP を構築することにより，NII 内部で認証局運用機関，認証ポータル運用機関，HPCI アカウント IdP 運用機関間の連携動作を確認した．次に，各情報基盤センターに IdP を構築して NII 内のシステムとの連携試験を行ったが，NII と情報基盤センター間で

アカウント情報（属性）が適切に提供されていることを確認するため，提供された Shibboleth 属性を表示する Web サイトを NII 内に構築した．情報基盤センターの管理者は，本 Web サイトにアクセスすることにより自組織の IdP の設定を確認することができる．

GSI-SSH サーバに関する実験では，GSI-SSH サーバがデフォルトで用いる 22/tcp ポートが，OS 付属の ssh の利用ポートと衝突する不具合が一部で発生した．これに対して各情報基盤センターでは，OS 付属の ssh を停止する，または GSI-SSH で 22 番以外のポートを利用することにより対応した．HPCI の本運用では，GSI-SSH が用いるポート番号を別途定める予定である．

### 4.2 ユーザの利用例

図 3 は，ユーザの利用例として，シングルサインオンを行って計算機にログインするまでの手順を示している．図中，実線矢印はユーザの処理，点線矢印はシステムの処理を意味する．

(1) ユーザは Web ブラウザで NII の認証ポータルにサインオンする．この際，ユーザは，自分のアカウントを管理する HPCI アカウント IdP 運用機関を選択し，HPCI アカウントとパスワードを入力する．認証ポータルは，DS 経由でユーザが指定した HPCI アカウント IdP（情報基盤センター）にユーザの認証処理を依頼する．**図 4** は，ユーザが DS 上で HPCI アカウント IdP 運用機関を選択する画面（左図），および選択後の IdP での認証時の画面（右図）の例である．次にユーザは，認証ポータル上で代理証明書を生成する．具体的には，証明書リポジトリに保存されているクライアント証明書から代理証明書が生成され，代理証明書リポジトリに格納される．

(2) ユーザは，代理証明書リポジトリから代理証明書をユーザが使用するローカル計算機にダウンロードする．代理証明書のダウンロードには，Linux や MacOS 環境上では MyProxy が提供する myproxy-logon コマンド，Windows 環境では NGS[18] で開発された MyProxy Uploader を利用可能である．

(3) ユーザは，GSI-SSH を用いることにより遠隔計算機にログインする．この時の認証は GSI 認証によって行われるため，ユーザは，遠隔計算機のローカルアカウント名やパスワードを入力する必要はない．GSI-SSH のクライアント環境は，Linux や MacOS 環境では Globus Toolkit が提供する gsissh[22]，Windows 環境では NGS[18] で開発された GSI-SSHTerm を利用可能である．

## 5. 関連研究

Web アプリケーションのためのシングルサインオンを実現する認証・認可のためのプロトコルとして OpenID[26] や OAuth[27] の仕様が策定されている．また，同様にシングルサインオンを実現するための Java ベースのソフトウェアとして，OpenSSO[28] が開発されている．これらのプロトコルやソフトウェアは Web アプリケーションのシングルサインオンを実現するための有効な手段といえるが，HPCI では，遠隔の計算機への SSH を用いたログインや共用ストレージへのアクセスもシングルサインオンで実現する必要がある．そのため，HPCI の認証基盤の設計では，GSI と Shibboleth を用い，認証ポータルで Shibboleth による Web 認証フェデレーションから GSI 認証への認証ブリッジを行うための Web インターフェースを提供する方式を採用した．

Shibboleth による Web 認証を Web アプリケーション以外へ連携させる取り組みに関しては，IETF の ABFAB (Application Bridging for Federated Access Beyond web) ワーキンググループ[29] における検討が始まっている．また，Project Moonshot[30] では，Kerberos へのブリッジや GSI へのブリッジを行う取り組みが行われているが，まだ試験段階であるため，HPCI の認証基盤への導入は見送った．

米国の TeraGrid で用いられた GridShib[31]，英国の NGS における ShibGrid[32] では，ともに Shibboleth と GSI を用いてシングルサインオンを実現するシステムを開発している．このうち米国では，Cyberinfrastructure を構成する TeraGrid や OSG (Open Science Grid) に対して認証ゲートウェイサービスを提供するために “CILogon” が開発されている[33]．CILogon では，Shibboleth フェデレーションである InCommon と Grid PKI をブリッジするために GridShib を用いており，LoA (Level of Assuarance) を階層的に規定することによって，OpenID 認証による証明書発行も受け付けている．しかしシステムの配備や運用方法にまでは言及されておらず，HPCI 上での認証基盤の実現には本稿で述べた議論や実証実験が必要であった．一方，HPCI の認証基盤は，GSI を用いた認証を行う点で GridShib や ShibGrid と共通しているため，これらのシステムを用いた海外の分散計算基盤と HPCI が連携することを技術的に容易にしている．

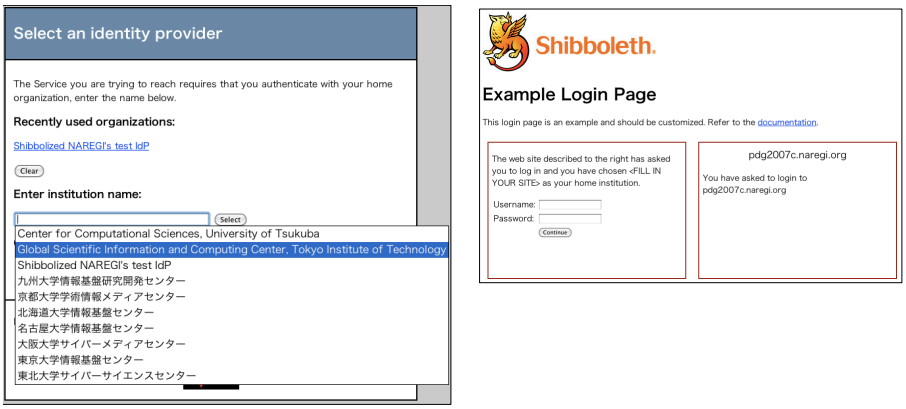


**図 4** 認証時のユーザ画面例

## 6. おわりに

本稿では，HPCI 上でシングルサインオンを実現するための認証基盤の設計およびプロトタイプシステムによる実証実験について述べた．HPCI は H24 年 9 月に本運用を開始する計画であり，基盤整備が進められている．認証ポータルについては，現在，新たに開発したソフトウェアの試験を実施している．また，証明書管理システムについては， 34) を参考にして証明書リポジトリに MyProxy を用いる実装を行い，ソフトウェアの試験を実施している．今後，これらのソフトウェアを用いて，本運用と同仕様のシステムを用いた運用試験を開始する予定である．また，認証局の運用については，将来的に IGTF での承認を受けるための準備を進めている．

**謝辞** 本稿をまとめるにあたり御議論頂いた「HPCI の詳細仕様に関する調査検討」および HPCI システム WG 委員の皆様に感謝します．本研究の一部は文科省委託「HPCI の詳細仕様に関する調査検討」，学際大規模情報基盤共同利用・共同研究拠点共同研究「学術グリッド基盤の構築・運用技術に関する研究」による．

## 参 考 文 献

1) Hey, T., Tansley, S. and Tolle, K.(eds.): *The Fourth paradigm, Data-Intensive Scientific Discovery*, Microsoft Research (2009).
2) XSEDE: Extreme Science and Engineering Discovery Environment, https://www.xsede.org/.
3) PRACE: Partnership for Advanced Computing in Europe, http://www.prace-ri.eu/.
4) 理化学研究所: 次世代スーパーコンピュータの開発・整備, http://www.nsc.riken.jp/.
5) HPCI 準備段階コンソーシアム: ＨＰＣＩとその構築を主導するコンソーシアムの具体化に向けて-最終報告-, http://hpcic.riken.jp/ＨＰＣＩとその構築を主導するコンソーシアムの具体化に向けて-最終報告-.pdf (2012).
6) Welch, V., Siebenlist, F., Foster, I., Bresnahan, J., Czajkowski, K., Gawor, J., Kesselman, C., Meder, S., Pearlman, L. and Tuecke, S.: Security for Grid Services, *Proc. of the 12th IEEE International Symposium on High Performance Distributed Computing* (2003).
7) Welch, V.: Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective, http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf (2005).
8) Morgan, R. L., Cantor, S., Carmody, S., Hoehn, W. and Klingenstein, K.: Federated Security: The Shibboleth Approach, *EDUCAUSE Quarterly*, Vol. 27, No. 4 (2004).
9) Internet2: Shibboleth, http://shibboleth.internet2.edu/.
10) 国立情報学研究所: SINET4 学術情報ネットワーク, http://www.sinet.ad.jp/.
11) 實本英之, 建部修見, 佐藤仁, 石川裕: 広域分散環境を提供する HPCI システムソフトウェア基盤の設計概要と共有ストレージ構築, 情報処理学会研究報告 HPC-130 (2011).
12) 滝澤真一朗, 棟朝雅晴, 宇野篤也, 小林泰三, 實本英之, 松岡聡, 石川裕: 広域分散環境を提供する HPCI 先端ソフトウェア運用基盤の設計, 情報処理学会研究報告 HPC-130 (2011).
13) 合田憲人, 東田学, 漆谷重雄, 天野浩文, 坂根栄作, 小林克志, 青木道宏, 柴山悦哉, 石川裕: 広域分散環境を提供する HPCI ネットワーク・認証・ユーザ管理支援基盤の設計, 情報処理学会研究報告 HPC-130 (2011).
14) 小松文子 (編): PKI ハンドブック, ソフトリサー

チセンター (2004).
15) IGTF: International Grid Trust Federation, http://www.igtf.net/.
16) OASIS: Security Assertion Markup Language (SAML) Specification, http://www. oasis-open.org/committees/security/ (2005).
17) InCommon: InCommon, http://www.incommon.org/.
18) NGS: National Grid Service, http://www.ngs.ac.uk/.
19) National Institute of Informatics: NAREGI-CA development, http://ca-dev.naregi.org/.
20) Novotny, J., Tuecke, S. and Welch, V.: Initial Experiences with an Online Certificate Repository for the Grid: Myproxy, *Proc. of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10)* (2001).
21) Murray, M.: Profile for Member Integrated X.509 Credential Services (MICS) with Secured Infrastructure Version 1.0, *The Americas Grid Policy Management Authority http://www.TAGPMA.org/* (2007).
22) Globus Alliance: GSI-OpenSSH, http://globus.org/toolkit/docs/4.0/security/open ssh/.
23) Tatebe, O., Hiraga, K. and Soda, N.: Gfarm Grid File System, *New Generation Computing*, Vol. 28, No. 3, pp. 257–275 (2010).
24) NAREGI: National Research Grid Initiative, http://www.naregi.org/.
25) UPKI イニシアティブ: UPKI オープンドメイン証明書自動発行検証プロジェクト, https://upki-portal.nii.ac.jp/docs/odcert.
26) OpenID Foundation: OpenID, http://openid.net/.
27) Ed. E. Hammer-Lahav: The OAuth 1.0 Protocol, RFC 5849.
28) ORACLE: Opensso, http://java.net/projects/opensso/.
29) IETF: Application Bridging for Federated Access Beyond web (abfab), http://datatracker.ietf.org/wg/abfab/.
30) JANET: Project Moonshot, http://www.project-moonshot.org/.
31) Basney, J., Martin, S., Navarro, J., Pierce, M., Scavo, T., Str, L., Uram, T., Wilkins-diehr, N., Wu, W. and Youn, C.: The Problem Solving Environment of TeraGrid, Science Gateway, and the Intersection of the Two, *Proc. of the Fourth IEEE International Conference on e-Science and Grid Computing (e-Science'08)* (2008).
32) Spence, D., Geddes, N., Jensen, J., Richards, A., Viljoen, M., Martin, A., Dovey, M., Kang, M. N. T., Trefethen, A., Allan, D. W. R. and Meredith, D.: ShibGrid: Shibboleth Access for the UK National Grid Service, *Proc. of the Second IEEE International Conference on e-Science and Grid Computing (e-Science'06)* (2006).
33) CILogon Project: CILogon, http://www.cilogon.org/.
34) Yamamoto, N., Kojima, I. and Y. Tanaka, S.S.: VO-enabled Service Harmonization in the GEO Grid, *Proc. of the Fourth IEEE International Conference on e-Science and Grid Computing (e-Science'08)* (2008).