11-IS03

学術グリッド基盤の構築・運用技術に関する研究

合田 憲人（国立情報学研究所）

本研究では，我が国における e-サイエンスを活用した研究を促進することを目指し，学際大規模情報基盤共同利用・共同研究拠点に設置された計算機システム，およびこれらを接続する学術情報ネットワークである SINET4 から構成される実用的なグリッド基盤を構築・運用する技術を確立することを目的とする．平成 23 年度は，グリッド基盤上の計算機やストレージを連携して利用するために重要な技術のひとつである認証基盤技術に焦点を当て，平成 22 年度までの研究成果を活用し，グリッド認証基盤の設計，構築，実証実験を行う．具体的には，グリッド基盤として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）を想定し，本研究参加機関の情報基盤センターで管理されるユーザアカウント管理システムと国立情報学研究所が運用するグリッド認証システムを Shibboleth 認証連携技術により連携し，さらに Grid Security Infrastructure (GSI)を用いて，グリッド基盤にシングルサインオンする認証基盤を構築する．また，認証基盤の本格運用に向けた検証を行うため，認証基盤の実用性を重視した実証実験を行う．

1. 研究の目的と意義

ネットワーク上に分散した様々な研究データを融合して処理することにより，未知の問題解決や科学的発見を行う新たな研究手法（e-サイエンス）が注目されている．e-サイエンスを実現するためには，ネットワーク上に分散した様々なデータを連携し，かつ高性能計算機群を用いてこれらのデータを高速に処理するための基盤が必要となる．このような背景のもと，1990 年代よりグリッド技術の研究が世界的に進められ，国内においても多くの基礎研究の成果が報告されている．また現在，理化学研究所で開発されている京コンピュータおよび情報基盤センター等のスーパーコンピュータやストレージから構成され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）を構築する計画が文部科学省により進められており，e-サイエンスの基盤となる実用的な高性能分散計算基盤の実現が期待されている．しかし，このような分散計算基盤を構築・運用する技術については，未だ確立されていない部分も多く，解決しなければならない問題も残されている．

本研究では，我が国における e-サイエンスを活用した研究を促進することを目指し，学際大規模情報基盤共同利用・共同研究拠点に設置された計算機システム，およびこれらを接続する学術情報ネットワークである SINET4 から構成される実用的なグリッド基盤を構築・運用する技術を確立することを目的とする．申請者らは，平成 22 年度学際大規模情報基盤共同利用・共同研究拠点公募型共同研究の採択課題の中で，情報基盤センターへのグリッドミドルウェアの配備・運用技術やグリッド環境上でのユーザ管理技術に関する研究を進めてきた．平成 23 年度は，グリッド基盤上の計算機やストレージを連携して利用するために重要な技術のひとつである認証基盤技術に焦点を当て，平成 22 年度までの研究成果を活用し，本格的なグリッド認証基盤の設計，構築，実証実験を行う．具体的には，グリッド基盤として HPCI を想定し，本研究参加機関の情報基盤センターで管理されるユーザアカウント管理システムと国立情報学研究所が運用するグリッド認証システムを Shibboleth 認証連携技術により連携し，さらに Grid Security Infrastructure (GSI)を用いてグリッド基盤にシングルサインオンする認証基盤を構築する．また，認証基盤の本格運用に向けた検証を行うため，認証基盤の実用性を重視した実証実験を行う．

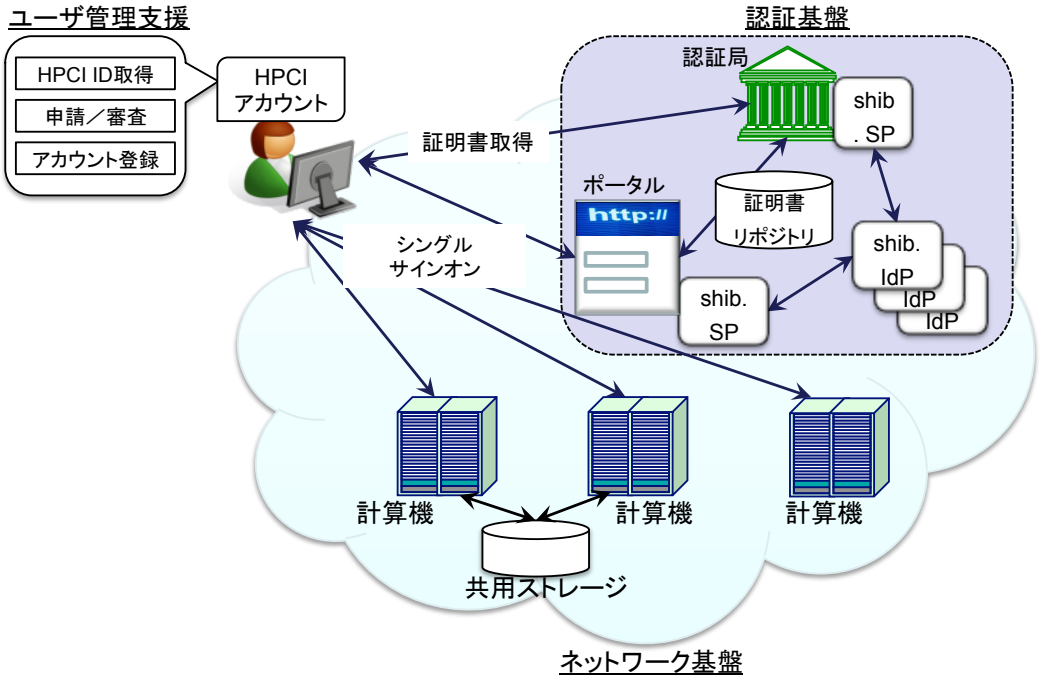

図 1 学術グリッド基盤

2. 当拠点公募型共同研究として実施した意義

(1) 共同研究を実施した大学名と研究体制

本研究は，課題連絡責任者の所属する国立情報学研究所（NII）がとりまとめ機関となり，当拠点を構成する北海道大学，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，九州大学との共同研究として実施している．

(2) 共同研究分野

本研究は，「大規模情報システム関連研究分野」における研究として実施している．

(3) 当公募型共同研究ならではという事項など

本研究が目指すグリッド環境の構築および運用では，共同研究を希望する大学の計算機上へのミドルウェアのインストールや設定作業が必要であり，各拠点の研究者や技官の協力が必要となる．また，実証実験では認証基盤を運用するための業務フローについても検討を行うため，各拠点の全国共同利用担当者の協力が必要となる．さらに本研究を進めるにあたり，グリッドミドルウェア技術に関して深い知見を持つ九州大学，大阪大学，筑波大学，東京工業大学の研究者の協力が必要である．また，実証実験に参加するユーザコミュニティとして九州大学の研究者の協力も必要である．

3. 研究成果の詳細と当初計画の達成状況

本研究では，学際大規模情報基盤共同利用・共同研究拠点に設置された計算機，およびこれらを接続する SINET4 から構成される実用的なグリッド基盤を構築・運用するための技術に関する研究を行うことを目的としている．本節では，最初に本研究が対象とする学術グリッド基盤について概説する．次に平成 23 年度に実施した認証基盤の設計および構築，実証実験の内容について報告する．

3.1. 学術グリッド基盤

図 1 は，本研究が対象とする学術グリッド基盤の概要を示している．本グリッド基盤は，文部科学省が進め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）[1]の基本仕

[1] http://hpcic.riken.jp/

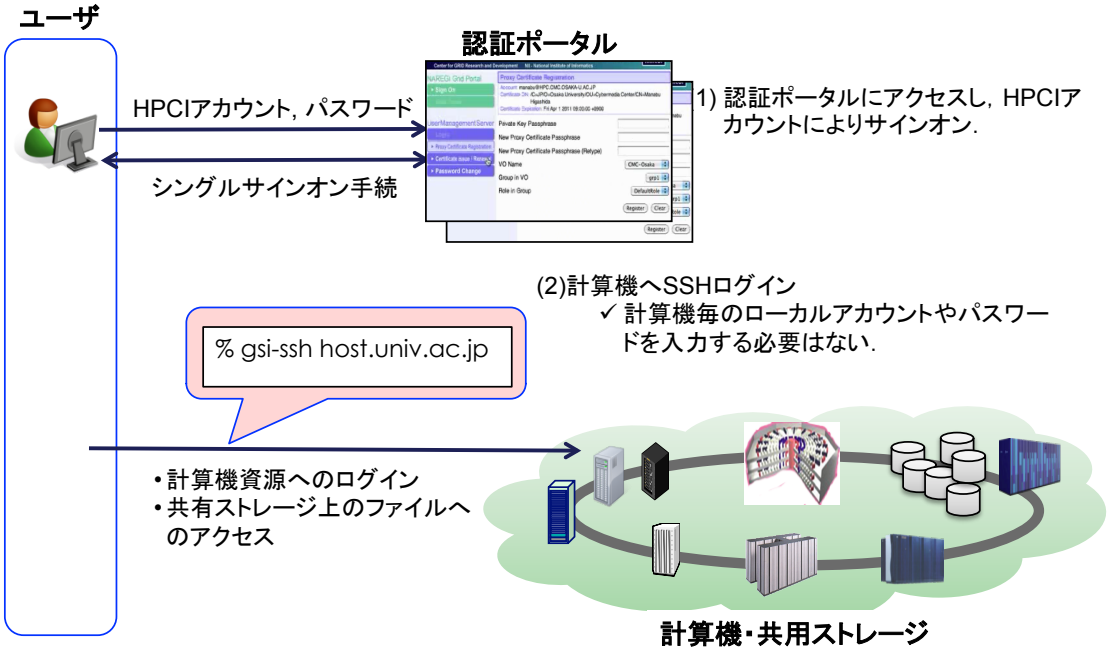

図 2 認証基盤の利用シナリオ

様に従って設計されており，ネットワークに接続された計算機や共用ストレージをユーザがシングルサインオンで利用可能な環境を提供する．

グリッド基盤上の計算資源は，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，九州大学の各情報基盤センターが運用するスーパーコンピュータから構成されており，HPCI の運用ではこれらに加えて理化学研究所計算科学研究機構（AICS）の京コンピュータも利用される予定である．また図中の共用ストレージは，本研究実施時には接続されていないが，HPCI の運用時には接続される予定である．これらの資源を接続するネットワーク基盤は，国立情報学研究所が運用する SINET4[2]が利用される．

計算機や共用ストレージへのシングルサインオンは，国立情報学研究所が中心となって運用する認証基盤により実現される．ユーザは，本認証基盤が提供する認証ポータル上でサインオン処理を行うことにより，本グリッド基盤上の（複数の）計算機や共用ストレージを個別の認証処理なしで利用することができる．認証ポータル上でのサインオンに用いるユーザアカウント（以後，HPCI アカウントと表記）の登録や利用中のユーザ支援等のユーザ管理支援については，業務を一括して担当する独立した組織が運用されることを想定している．

3.2. 認証基盤の設計

本研究では，学術グリッド基盤上の計算機や共用ストレージへのシングルサインオンを実現する認証・認可サービスの利用シナリオを検討し，これを実現するための認証基盤アーキテクチャの設計を行った．

認証基盤の目的は，学術グリッド基盤上の計算機や共用ストレージへのシングルサインオンを実現する認証・認可サービスを提供することである．図 2 は，本認証基盤の利用シナリオを示している．本シナリオでは，ユーザが認証ポータルに HPCI アカウントを用いてサインオンし，シングルサインオン処理を行う．認証ポータルは耐故障性を向上させるために複数の組織で運用されるが，ユーザはどの認証ポータルからもサインオンすることができる．その後ユーザは，アカウントやパスワード等の入力を行うことなく，複数の計算機への

[2] http://www.sinet.ad.jp/

ログインや共用ストレージ上のファイルへのアクセスを行うことができる．

学術グリッド基盤の資源提供機関やユーザコミュニティは多岐にわたり，これらのユーザが習得している認証方法も複数想定されるため，認証ポータルにサインオンするためのアカウント種別やユーザが利用するサービスにより，図 2 を実現するシナリオは複数考えられる．一方，本研究成果を平成24年度に運用開始が予定されているHPCIの構築に活用するためには，早急に安定した認証基盤の運用を開始する必要がある．本研究では，分散計算システム上の認証方式やその運用に関して国内外での動向調査を行った．これらの検討の結果，9 大学の情報基盤センターおよび国立情報学研究所による運用実験が行われた実績[3]のあるGrid Security Infrastructure (GSI)[4]およびShibboleth[5]を組み合わせる方式を採用し，認証基盤の設計を行った．

GSI は，Public Key Infrastructure (PKI)[6]に基づく認証技術であり，ユーザの持つクライアント証明書を使って複数の資源に対するシングルサインオンが実現される．ユーザは，自らのクライアント証明書を使ってサインオンすることにより，クライアント証明書から作成される一時的な証明書(Proxy 証明書)を生成することができる. Proxy 証明書は，新たに作成された秘密鍵と公開鍵を含み，ユーザの秘密鍵（または一世代前の Proxy 証明書に含まれる秘密鍵）により署名されている．認証時には，Proxy 証明書の秘密鍵を除いた部分が遠隔計算機やストレージに送付され，PKI に基づく認証処理が行われる．Proxy 証明書には有効期間が定められており，その有効期間内であれば，ユーザは新たなサインオン処理を行うことなく，複数の資源へのログインやファイルアクセスが可能となる．

GSI では，各ユーザが認証局からクライアント証明書の発行を受ける必要がある．本認証基盤におけるクライアント証明書の取得方法は，International Grid Trust Federation (IGTF)[7] で定められた国際基準である MICS プロファイル[8]に基づいて行われる．MICS プロファイルでは，ユーザの本人性確認を他の信頼できるアカウント管理システム上のデータを用いて行う．即ち，ユーザが信頼できる組織のアカウントを所有していることをもって，ユーザの本人性確認を行う．従ってユーザは，後述の HPCI アカウントを管理する組織から発行された HPCI アカウントを用いてポータルにサインオンすることにより，クライアント証明書をオンライン処理のみで取得することができる．

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

[3]合田憲人:学術グリッド基盤の構築・運用技術に関する研究,学際大規模情報基盤共同利 用・共同研究拠点第 3 回シンポジウム, 2011

[4] Welch,V. :Globus Toolkit Version4 Grid Security Infrastructure: A Standards Perspective, http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf, 2005

[5] http://shibboleth.internet2.edu/

[6]小松文子(編): PKI ハンドブック,ソフトリサーチセンター, 2004

[7] http://www.igtf.net/

[8] Murray, M.: Profile for Member Integrated X.509 Credential Services (MICS) with Secured Infrastructure Version 1.0, The Americas Grid Policy Management Authority, 2007

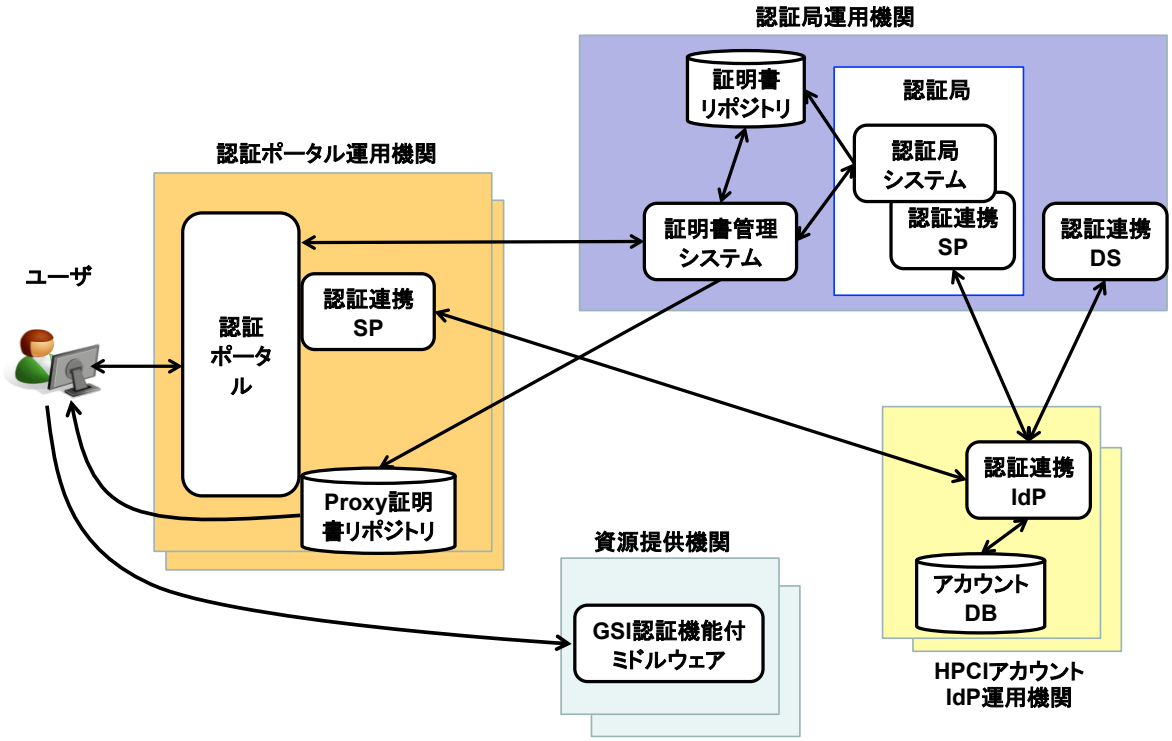

図 3 認証基盤アーキテクチャ

る．

3.3. 認証基盤のアーキテクチャ

本節では，認証基盤を構成するシステムとその運用組織について述べる．本認証基盤は，表 1 に示す組織が運用するシステムから構成されている．図 3 は，各機関が運用するシステムの関係を示す．

認証局運用機関は，GSI において必要となるクライアント証明書およびサーバ証明書を発行する組織である．図中の証明書管理システムは，ユーザからの証明書の発行・失効等の申請を受け付け，認証局システムに証明書の発行・失効依頼を行うソフトウェアである．認証局システムから発行されたクライアント証明書は，証明書リポジトリに保管される．認証局システムは，認証連携システムのサービスプロバイダ（SP）として実装されており，証明書取得処理におけるユーザの認証を認証連携システムのアイデンティティプロバイダ（IdP）に依頼する．また，認証連携 DS は，認証を受けるアカウントを管理する IdP の情報を検索するための役割を持つ．現在構築している実験環境では，認証局システムおよび証明書管理システムのソフトウェアとして，NAREGI-CA[9] と UMS[10]を用いている．

表 1 認証基盤運用機関

運用機関	役割
認証局運用機関	学術グリッド基盤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	学術グリッド基盤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	学術グリッド基盤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	学術グリッド基盤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．

[9] http://ca-dev.naregi.org/
[10] http://www.naregi.org/

証明書リポジトリの運用には，MyProxy[11]を利用している．また，認証連携システムには，Internet2 で公開されている Shibboleth のソフトウェアパッケージを用いている．

認証ポータル運用機関は，学術グリッド基盤にユーザがシングルサインオンするための Web インタフェースとしての機能を提供する組織である．認証ポータルは，ユーザが学術グリッド基盤にサインオンするための Web ポータルである．ユーザは HPCI アカウントを用いてサインオンするため，認証ポータルは Shibboleth SP として実装されており，ユーザ認証を HPCI アカウントの Shibboleth IdP に依頼する．ポータル上でサインオンしたユーザは，GSI によるシングルサインオンを行うための Proxy 証明書を生成することができ，生成された Proxy 証明書は Proxy 証明書リポジトリに保存される．認証ポータル用ソフトウェアは，現在，NAREGI Portal[10] をベースとしたプロトタイプが開発されている．また，Proxy 証明書リポジトリとして MyProxy を用いている．

HPCI アカウント IdP 運用機関は，HPCI アカウントの認証機能を提供する組織である．本機関では，自らが運用するアカウント管理システム（アカウント DB）に接続する Shibboleth IdP を運用し，Shibboleth SP から要求された HPCI アカウントの認証を行い，認証結果を Shibboleth SP に返す．資源提供機関は，HPCI に対して計算機や共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，計算機に遠隔ログインするために GSI-SSH[12]，共用ストレージ上のファイルアクセスのために Gfarm2[13]を用いる．HPCI アカウント IdP 運用機関と資源提供機関については同一組織が両方の機能を持つことが想定されるが，本稿では，認証基盤の機能を明確に分類するために両者を分けて定義している．

11 http://grid.ncsa.illinois.edu/myproxy/
12 http://globus.org/toolkit/docs/4.0/security/openssh/
13 http://datafarm.apgrid.org/

3.4. 実証実験

本研究で設計した認証基盤の実証実験を行うため，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，九州大学の各情報基盤センター，国立情報学研究所から構成される認証基盤実験環境を構築した．図 4 は，本実験環境の構成を示している．本実験環境では，国立情報学研究所（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，Proxy 証明書リポジトリ，Shibboleth DS（Shib. 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）と連動した Shibboleth IdP（Shib. 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している．

本実証実験の結果，本環境上でユーザが以下の操作が可能であり，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

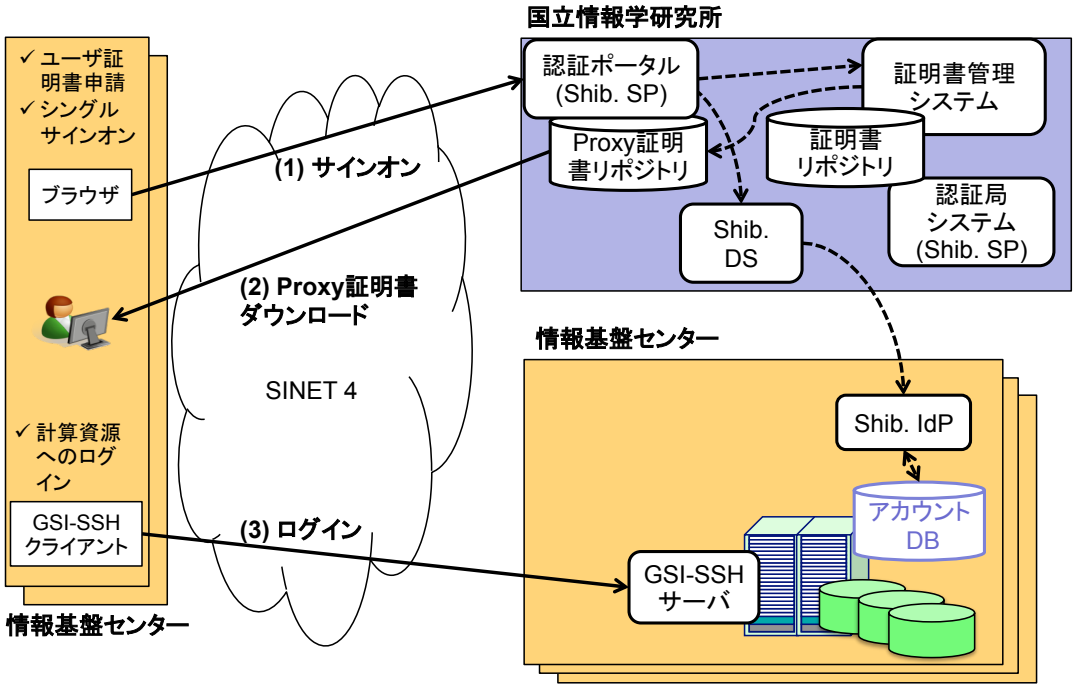

図 4 認証基盤実験環境

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．

図 4 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以下の手順も示している．図中，実線矢印やユーザの処理，点線矢印はシステムの処理を意味する．

(1) ユーザは web ブラウザ経由で 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 アカウントおよびパスワードを入力する．認証ポータルは，Shibboleth DS（Shib. DS）経由でユーザが指定した HPCI アカウント IdP 運用機関（情報基盤センター）の Shibboleth IdP（Shib. IdP）にユーザの認証処理を依頼する．図 5 は，ユーザが認証ポータル上で HPCI アカウント IdP 運用機関を選択する画面（左図），およびその後の認証時の画面（右図）の例である．次にユーザは，認証ポータル上で Proxy 証明書を生成する処理を行う．この処理により，事前に証明書リポジトリに保存されているユーザのクライアント証明書から Proxy 証明書が生成され，Proxy 証明書リポジトリに格納される．

(2) ユーザは，Proxy 証明書リポジトリから Proxy 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．Proxy 証明書のダウンロードには，UNIX や MacOS 環境上では MyProxy が提供する myproxy-logon コマンド，Windows 環境で

図 5 認証画面の例

は MyProxy Uploader[14]を利用する.

(3) ユーザは，gsissh コマンドを実行することにより，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.

3.5. 当初計画の達成状況

本研究が目標としていた認証基盤の設計および構築については，当初の計画通り達成することができた．本研究の成果である認証基盤の設計は HPCI で採用されるとともに，HPCI で利用される予定の証明書管理システムや認証ポータルは，本研究が用いたプロトタイプソフトウェアを参考にして現在開発中である.

実証実験では，認証基盤の動作確認を行うとともに，実証実験結果をもとにして，HPCI の本運用へ向けて提言を行うことができた．例えば，本実証実験で構築した IdP の設定確認のための環境は，現在進められている HPCI の試験運用でも利用されている．また， GSI-SSH が利用する通信ポートに関する問題については，本実験結果をもとにして，HPCI では GSI-SSH 用に統一した通信ポートを定めることが決定された.

一方，実証実験に参加したユーザは，情報基盤関係者に留まった．これらのユーザにはアプリケーション分野の研究者も含まれたが，HPCI の運用時には，多くのアプリケーション研究者からの意見をシステム運用に反映させることが重要である.

4. 今後の展望

本研究では，学術グリッド基盤の構築および運用技術の確立を目的として，学術グリッド基盤として HPCI を想定し，その認証基盤の設計および構築，実証実験を行った．HPCI では，現在，平成 24 年 9 月の供用開始を目指して，認証基盤の構築が行われ，試験運用が開始されている．本研究の成果は，HPCI 認証基盤の構築に大きく貢献しており，今後 HPCI の中で本研究成果が活用される予定である.

5. 研究成果リスト

(1) 学術論文

[1] 合田憲人，東田学，坂根栄作，天野浩文，小林克志，棟朝雅晴，江川隆輔，建部修見，

14 http://www.ngs.ac.uk/tools/certwizard

鴨志田良和, 滝澤真一朗, 永井亨, 岩下武史, 石川裕, 高性能分散計算環境のための認証基盤の設計, 情報処理学会論文誌コンピューティングシステム（投稿中）

(2) 国際会議プロシーディングス

[1] Eisaku Sakane, Kento Aida, Manabu Higashida, Taizo Kobayashi, Hirofumi Amano, Mutsumi Aoyagi, Grid Operational Supports for Middleware Deployment and User Administration, Proceedings of Science, The International Symposium on Grids and Clouds and the Open Grid Forum, 2011 年 9 月

(3) 国際会議発表

[1] Kento Aida, Authentication Mechanism for High Performance Computing Infrastructure in Japan, 32nd APAN Meeting, 2011 年 8 月

[2] Kento Aida, Towards a Unified Cyberinfrastructure, International Conference for High Performance Computing, Networking, Storage and Analysis (SC11), BOF, 2011 年 11 月

(4) 国内会議発表

［1］ 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，情報処理学会第130回ハイパフォーマンスコンピューティング研究会，2011 年 7 月

［2］ 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, HPCI のためのネットワーク・認証基盤，電子情報通信学会インターネットアーキテクチャ研究会／ADVNET2011，2011 年 10 月

［3］ 合田憲人，東田学，坂根栄作，天野浩文，小林克志，棟朝雅晴，江川隆輔，建部修見，鴨志田良和，滝澤真一朗，永井亨，岩下武史，石川裕，高性能分散計算環境のための認証基盤の設計，情報処理学会先進的計算基盤システムシンポジウム（SACSIS2012），2012 年 5 月（発表予定）

(5) その他（特許，プレス発表，著書等）