HPCI のためのネットワーク・認証基盤

合田 憲人，坂根 栄作，本山 一隆，青木 道宏，漆谷 重雄

国立情報学研究所

aida@nii.ac.jp

概要：本稿では，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）を構成するネットワークおよび認証基盤について報告する．HPCI では，全国のスーパーコンピュータおよび共用ストレージを学術情報ネットワーク SINET4 が提供する高速ネットワークにより接続するとともに，これらの計算資源やウェブサービスに対するシングルサインオンを可能としている．本稿ではこれらの基盤の運用状況についても報告する．

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，京コンピュータを中核として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）の運用が開始されている[4].

本稿では，HPCI を構成するネットワークおよび認証基盤について報告する．HPCI では，全国のスーパーコンピュータおよび共用ストレージを高速ネットワークにより接続するとともに，これらの計算資源に対するシングルサインオンを可能としている．高速ネットワークについては，国立情報学研究所（NII）が運営する学術情報ネットワーク SINET4[5]が用いられ，全国に分散した計算資源間の高速通信を可能としている．またシングルサインオンを実現するため，NII と計算資源を提供する機関（HPCI システム構成機関）との間で Shibboleth[6] および Grid Security Infrastructure（GSI)[7]を用いた認証基盤が運用されている．本稿では，これらの仕様について述べるとともに，現在の運用状況についても報告する．

以後，2 節では HPCI の概要について述べる．3 節および 4 節では，ネットワークおよび認証基盤の仕様と運用状況についてそれぞれ報告する．最後に 5 節では，まとめと今後の課題について述べる．

2. HPCI の概要

HPCI では，京コンピュータと全国に分散したスーパーコンピュータ群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．HPCI の計算資源は，2013 年 10 月時点で，京コンピュータ，9 大学の情報基盤センター（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）および海洋研究開発機構が運用するスーパーコンピュータから構成されている．また，理化学研究所および東京大学が運用する共用ストレージは，Gfarm ファイルシステム[8]を介して，上記のスーパーコンピュータ群からの透過的なアクセスを可能としている．これらの計算資源は，NII が運用する SINET4 により高速に接続されているほか，計算資源へのシングルサインオンが可能である．さらに，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）も運用されている[9].

HPCI 上の資源を利用するためには，HPCI を

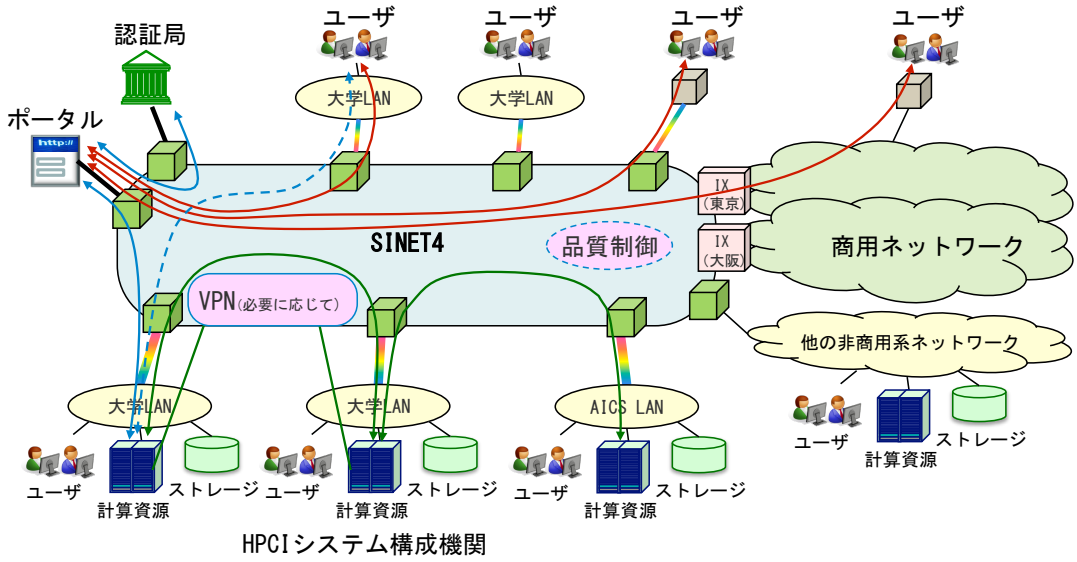

図 1 HPCI ネットワーク基盤

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（ユーザ）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ウェブサービス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，取得した電子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．また，HPCI ではユーザ支援を目的として，HPCI の利用申請やヘルプデスク等のシステムがウェブサービスとして提供されているほか，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ウェブサービス経由で提供している．ユーザは，これらのウェブサービスの利用も 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. ネットワーク基盤

HPCI を構成するネットワーク基盤は，幅広いユーザの利用を考慮し，計算資源への制限のないアクセス環境を提供する必要がある．このような環境を実現するため，HPCI のネットワーク基盤は，図 1 に示すように SINET4 を用いて構成されている．本節では，本ネットワーク基盤について述べる．

3.1. ネットワーク基本構成

SINET4 では，レイヤ 1 からレイヤ 3 の各レイヤで多様なサービス（インターネット接続サービス，L3VPN，L2VPN/VPLS，QoS，リソースオンデマンド等）を提供している．現在 SINET4 では，サービス毎の通信プロトコルや高信頼化技術の違い等を考慮して，5 つのサービス論理網を形成してサービスを提供しているが，HPCI では SINET4 のインターネット接続サービスを利用している．

HPCI システム構成機関は，10Gbps から 40Gbps のネットワークにより SINET4 に接続されている．また SINET4 内では 40Gbps の基幹ネットワークにより各拠点が接続されるとともに，特に高い需要が見込まれる東京・大阪間の基幹ネットワークは 80Gbps の帯域を持つ．

3.2. 商用ネットワーク接続

HPCI では，産業界からの計算資源利用環境を整備することも重要な課題である．SINET4 は，東京と大阪に設置された接続拠点（IX）を介して商用ネットワークと接続されている．具体的には，東京 IX では 123 の商用ネットワークが 30Gbps の帯域で，大阪 IX では 22 の商用ネットワークが 11Gbps の帯域で SINET と接続されている．

3.3. 運用ポリシ

HPCI の本格運用では，スーパーコンピュータや共用ストレージ資源間の大容量ファイル転送が行われるため，計算資源を提供する HPCI システム構成機関の間で高速なネットワーク環境が必須となる．一方，各 HPCI システム構成機関は，各々

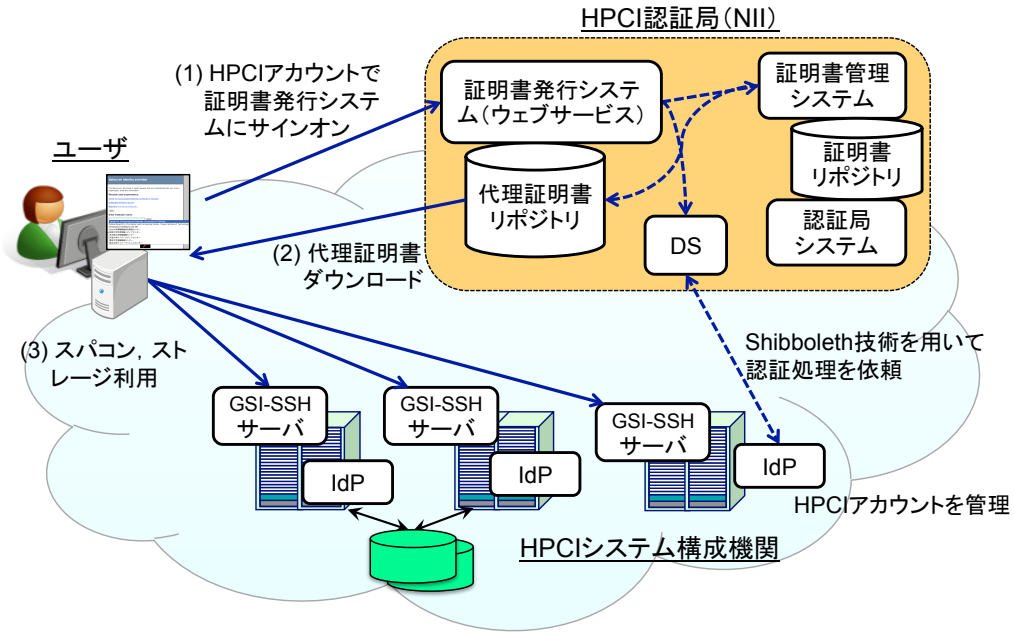

図 2 HPCI 認証基盤

異なるセキュリティポリシを持ち，そのポリシに基づいて計算資源等に対するアクセス管理を行っている．HPCI では，それぞれの組織のセキュリティポリシを尊重し，全ての通信に SINET4 の汎用ネットワークを使用している．この際に必要となる各拠点におけるファイアウォール設定については，HPCI 上の各種サービスの運用に必要な最小の要求要件を策定し，各拠点で運用している．

一方，HPCI 用の先端ソフトウェア機能の性能検証等においては，汎用ネットワークとは分離した環境が必要になることが予想されるため，SINET4 が提供する L3VPN や L2VPN/VPLS サービス等の利用を検討することとしている．また，汎用ネットワーク内での高性能データ転送を目的とした品質制御については，今後の利用形態を見ながら検討する予定である．

4. 認証基盤

HPCI の認証基盤は，HPCI 上の計算資源およびウェブサービスに対するシングルサインオンを実現している．本節では，本認証基盤について述べる．

4.1. 認証基盤アーキテクチャ

HPCI の認証基盤は，要素技術として Shibboleth および GSI を用いて実装されている．具体的には，HPCI 上のウェブサービスへのサインオン時には HPCI アカウントを用いた Shibboleth 認証が行われ，計算資源の利用時には電子証明書を用いた GSI 認証が行われる．

図 2 は，HPCI の認証基盤アーキテクチャおよびユーザが計算資源にシングルサインオンする手順を示している．本認証基盤の主要部分は，NII が運用する HPCI 認証局と HPCI システム構成機関が運用する IdP および GSI-SSH サーバから構成されている．

ユーザは，計算資源にログインするために，まず証明書発行システム（ウェブサービス）に HPCI アカウントを用いてサインオンする．証明書発行システム上でのユーザ認証は Shibboleth 認証により行われる．即ち，認証処理は，DS を介して当該ユーザのアカウントを管理する組織のサーバ（IdP）にリダイレクトされ，IdP での認証に成功すると，当該ユーザの属性情報が証明書発行システムに通知される．

証明書発行システムは，クライアント証明書発行および代理証明書発行の 2 つのサービスを提供する．クライアント証明書は，HPCI のユーザに発行される 1 年間有効な電子証明書であり，発行された電子証明書は，通常の利用では NII 内の証明書リポジトリに保存される．一方，代理証明書

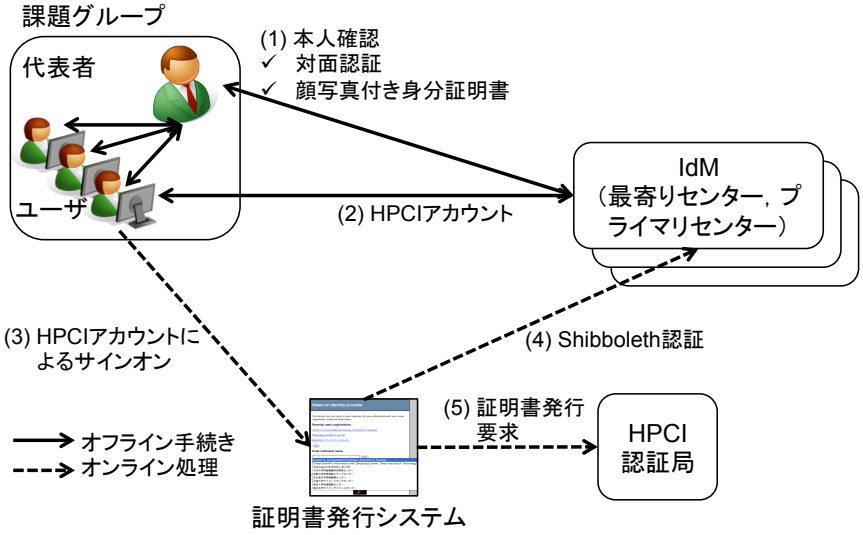

図 3 クライアント証明書発行手順

は，ユーザのクライアント証明書から作成される有効期間の短い（最長 1 週間）電子証明書である．ユーザは，証明書発行システム上で自分のクライアント証明書から代理証明書を作成し，代理証明書をローカル端末内に保存することができる．本代理証明書は，HPCI 上の計算資源にアクセスする際のクレデンシャルとして用いられる．具体的には，代理証明書が保存されたローカル端末からは，HPCI 上の計算資源にパスワード等を入力することなく，ログインできる．ユーザは，スーパーコンピュータへ GSI-SSH[10]を用いてログインすることができる．GSI-SSH は，GSI 認証が可能なリモートログインプログラムである．

4.2. HPCI 認証局

HPCI 認証局は，HPCI の認証基盤の中核となるものであり，ユーザ認証のために用いられるクライアント証明書のほか，ホスト証明書およびサービス証明書などのサーバ証明書を発行する．これらのサーバ証明書は HPCI 上で運用されるホスト（具体的には GSI-SSH サーバ）とサービス（具体的には Gfarm）の認証のために用いられ，これらのホストやサービスの管理者が発行申請を行なうものである．認証局のソフトウェア実装としては，NAREGI-CA[11]が採用されており，証明書の発行，証明書失効リストの発行などを行っている．

HPCI 認証局では，内閣官房セキュリティセンターによる「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」[12]ならびに世界的な暗号アルゴリズムの移行情勢を鑑み，HPCI の供用開始からハッシュ関数 SHA-256 と 2048 ビット長の RSA 公開鍵暗号を組合せた電子証明書を全ての対象に発行することに決定し，全システムへの展開準備並びに必要な開発を行なった．これにより，供用開始以降での電子証明書移行作業を回避できるとともに，現在のところ高度な強度を担保する電子証明書の提供が可能となっている．

認証局運用では，電子証明書発行時に申請者の本人確認を確実に行うことが重要である．HPCI 認証局では，図 3 に示すように，採択された課題のユーザへ HPCI アカウントを発行する際に本人確認が実施される．具体的には，採択された課題の代表者は，課題に参加するユーザの本人確認を実施し，さらに最寄りセンターで自身の本人確認を受ける．本人確認では，申請者の顔写真付き身分証および対面審査での確認を行う．対面認証完了後，各ユーザに対してプライマリセンターから HPCI アカウントが発行される．プライマリセン

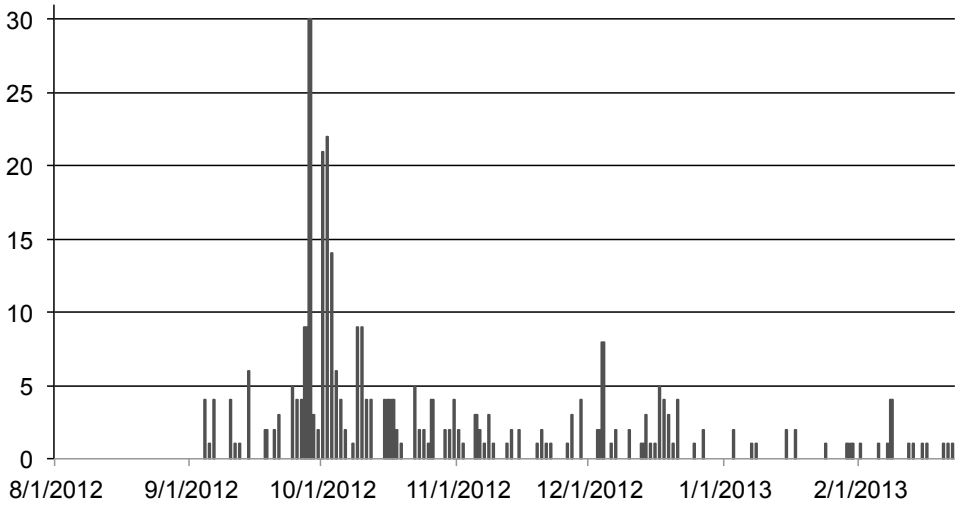

図 4 クライアント証明書発行数

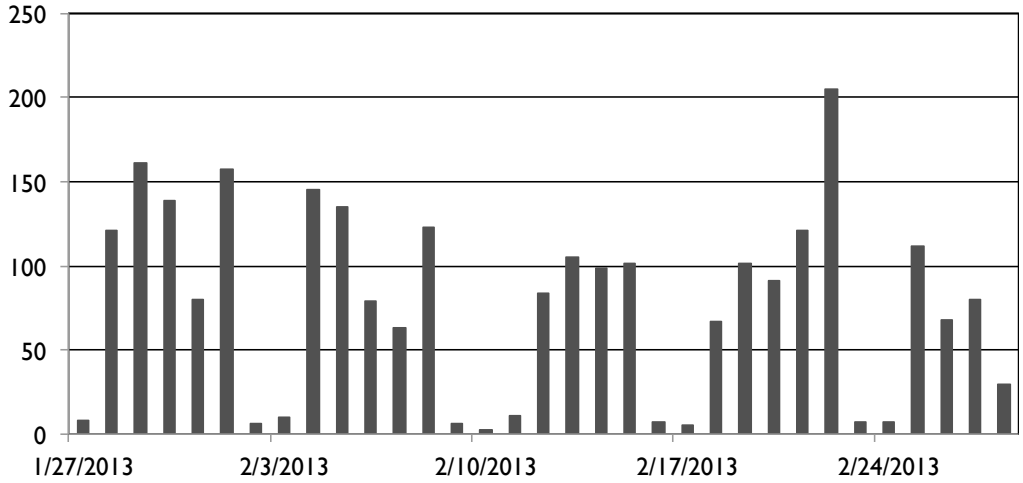

図 5 DS へのアクセス数

ターは,ユーザのHPCIアカウントを管理するIdPであり，現在の運用ではHPCIシステム構成機関がプライマリセンターも運用している．HPCIアカウントを取得したユーザは，オンライン処理により自身のクライアント証明書を取得できる．具体的には,ユーザは,証明書発行システムにHPCIアカウントを用いてサインオンし，証明書発行システム上の操作によりクライアント証明書の申請および取得を行う．

HPCI認証局は，2013年10月22日時点で，クライアント証明書649枚，サーバ証明書128枚，サービス証明書194枚を発行している．図4は，2012年9月4日から2013年2月28日までの1日当たりのユーザのクライアント証明書発行枚数を示している．図4では，HPCI運用開始直後に電子証明書発行数がピークに達していることを示しており，運用開始直後に多くのユーザが電子証明書を取得したことがわかる．

次に，図5は，2013年1月27日から2月28日までの1日当たりのDSへのアクセス数を示している．DSは，ユーザがShibboleth認証を行う際にアクセスされるサーバであり,図5の結果は,HPCIの認証基盤の利用状況を示す指標といえる．本結果より，平日は1日あたり100件以上のアクセスが行われていることがわかる．ただし，ユーザは代理証明書の有効期間中（最大1週間）は，Shibboleth認証なしで計算資源にログインできるほか，ウェブブラウザのキャッシュ機能により，

DS を介さずに Shibboleth 認証が行われる場合もあるため，認証基盤全体の実際の利用頻度は本結果より多いといえる．

5. おわりに

本稿では，HPCI を構成するネットワーク基盤および認証基盤の仕様を述べるとともに，運用状況を報告した．現在，これらの基盤は定常運用の段階に入っており，国立情報学研究所では，基盤の安定運用および強化を目的として，ネットワークや認証基盤の利用状況の分析を進めている．

現在，HPCI 認証局では，国内の HPCI 上の計算資源のみの利用を目的とした電子証明書を発行しているが，今後，海外の計算資源と連携した利用の需要も想定される．海外資源との連携のためには，グリッド認証局の運用方法を定める国際機関である International Grid Trust Federation（IGTF）[13]から HPCI 認証局が承認される必要があるため，承認に向けた準備を進めている．

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] 高度情報科学技術研究機，“High Performance Computing Infrastructure”, https://www.hpci-office.jp/

[5] 国立情報学研究所, “学術情報ネットワーク SINET4”, http://www.sinet.ad.jp/

[6] Morgan, R. L., Cantor, S., Carmody, S., Hoehn, W. and Klingenstein, K., “Federated Security: The Shibboleth Approach”, EDUCAUSE Quarterly, Vol. 27, No. 4, 2004

[7] Welch, V., Siebenlist, F., Foster, I., Bresnahan, J., Czajkowski, K., Gawor, J., Kesselman, C., Meder, S., Pearl- man, L. and Tuecke, S., “Security for Grid Services”, Proc. of the 12th IEEE International Symposium on High Performance Distributed Computing, 2003

[8] Tatebe, O., Hiraga, K. and Soda, N., “Gfarm Grid File System”, New Generation Computing, Vol. 28, No. 3, pp. 257–275, 2010

[9] 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

[10] Globus Alliance, “GSI-OpenSSH”, http://globus.org/toolkit/docs/4.0/security/openssh/

[11] NAREGI-CA, "NAREGI-CA development", http://ca-dev.naregi.org/

[12] 内閣官房セキュリティセンター, “政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針”, http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf

[13] IGTF, “International Grid Trust Federation”, http://www.igtf.net/