JLDG - HPCI共用ストレージ 連携システム 利用の手引き (第1版)

JLDG チーム

2014年4月23日 第1版 第1刷

目 次

1 概要

JLDGでは、HPCI共用ストレージとJLDGを同時にFUSEマウントし、両グリッドファイルシステム間で、ファイルを並列に（高速に）コピーすることを可能とするシステムを提供しています。（以下、連携システムと呼びます。）連携システムは、HPCI共用ストレージの利用者で、かつ、JLDGの利用者(新規利用も含む）であれば、誰でも利用できます。

本手引きは、既にHPCI共用ストレージを利用している方が、連携システムを利用する際の手順・方法をまとめたものです。

連携システムでは、HPCIの電子証明書に基づく認証をJLDGの認証に利用します。既にJLDGを利用している（JLDG発行の証明書を持っている）場合、

- JLDG発行の証明書サブジェクトに紐付けられた既存のグローバルユーザー名とは別に、HPCI電子証明書サブジェクトに紐付けられたグローバルユーザー名を発行する
- 既存のグローバルユーザー名に対応するJLDG発行の証明書サブジェクトをHPCI電子証明書サブジェクトに置き換える

のどちらかを選択できます。HPCI電子証明書に基づく認証で、JLDGを新たに利用する事も可能です。

図1に、連携システムの利用イメージを示します。ユーザーはログイン元端末から、HPCI連携システムホストに、HPCI電子証明書に基づく認証でログインし、HPCI共用ストレージとJLDGをマウントし、`gfpcopy`等で、ファイルを操作します。

2 利用資格の確認

2.1 新たにJLDGを利用される方

『Japan Lattice Data Grid 利用の手引き』(資料[1])を参照し、JLDGの概要を理解して下さい。次に、所属グループを決め、所属グループの連絡責任者に、以下の書類・情報を伝え、JLDGの利用資格の確認を受けて下さい。

- HPCIへの登録情報: HPCI-ID照会フォーム (資料 [2]) のページをpdf化したもの(照合番号は伏せていただいても構いません)
- JLDG仮想組織へ登録する情報: HPCIへの登録情報と同じものを英文（ローマ字）にしたもの
  - Given name
  - Family name
  - Institution
  - Phone number
  - Address
  - Email address

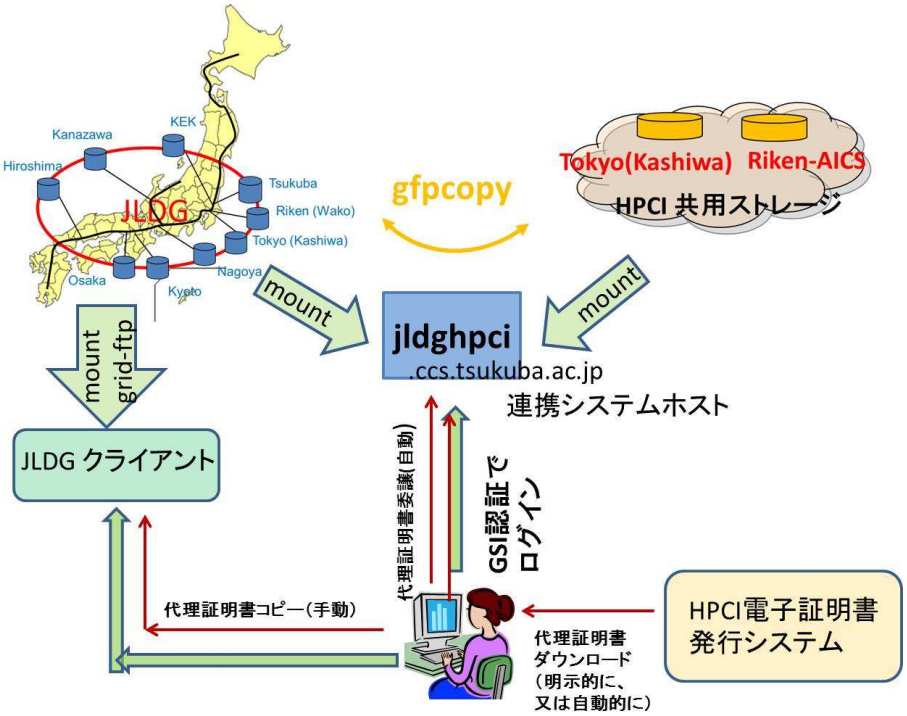

図 1: 連携システム利用イメージ

- HPCI 電子証明書のサブジェクト (HPCI 電子証明書発行システムで電子証明書を発行していない場合は、発行してください。)

また、申請は、HPCI に登録した電子メールアドレスから、電子メールで行って下さい。

2.2 既に JLDG を利用されている方

所属グループの連絡責任者に、以下の書類・情報を伝え、利用資格の確認を受けて下さい。

- HPCI への登録情報: HPCI-ID 照会フォーム (資料 [2]) のページを pdf 化したもの (照合番号は伏せていただいても構いません)
- HPCI 電子証明書のサブジェクト (HPCI 電子証明書発行システムで電子証明書を発行していない場合は、発行してください。)
- JLDG グリッド証明書のサブジェクトと、JLDG グリッド証明書サブジェクトを HPCI 電子証明書サブジェクトで置き換えるか否か

申請は、HPCI に登録した電子メールアドレスから、電子メールで行って下さい。

2.3 連絡責任者・仮想組織管理者の作業

連絡責任者は、申請者がグループに所属できる（している）事、書類・手続きに不備がないことを確認の上、申請者に承諾の旨の返事をし、申請者からの情報を仮想組織管理者に連絡します。仮想組織管理者は、連絡責任者からの情報を確認し、連携システムホストにアカウントを作成、仮想組織へ登録、JLDG でのユーザー作成を実施し、申請者に完了の連絡をします。

3 連携システム利用環境のセットアップ

HPCI ログインマニュアル (資料 [3]) を参照して、HPCI 計算機資源に GSI 認証でログインできる環境を準備して下さい。HPCI 共有ストレージをお使いであれば、この作業は済んでいるハズです。同じ環境を連携システムへのログインに利用できます。また、これから環境構築される方は、アペンディクス A も参照下さい。

連携システムホストは、KEK CA 局発行のホスト証明者を用いています。KEK CA 局の CA 証明書を http://gridca.kek.jp/ からダウンロードして、所定の場所に格納して下さい。格納場所は、HPCI CA 証明書の格納場所と同一です。openssl のバージョンを確認 (コマンド openssl version) し、バージョンが 1.0.0 以降の場合、証明書のハッシュ値がダウンロードしたものと異なりますので、

```
2f2f573f.* -> 617ff41b.*
```

のシンボリックリンク (または、リネーム) を行って下さい。失効リストを定期的に更新したい場合は、適当なスクリプトを作成し、cron で実行して下さい。

連携システムホストは、

```
jldghpci.ccs.tsukuba.ac.jp
```

です。HPCI 計算機資源に GSI 認証でログインする方法と同一の手順で、ログインできることを確認します。ただし、接続先 port 番号は、標準の 22 を用います。（HPCI で使われている 2222 ではありません。）ログイン後、`grid-proxy-info` で、代理証明書が移譲されている事を確認して下さい。

連携システムホストは、パスワード認証、公開鍵認証は禁止しています。連携システムホストには、ssh の鍵や、JLDG グリッド証明書、HPCI 電子証明書（本手引きでは解説していません）を置くことは、禁止します。

globus 関係のコマンドは、システムの標準の場所にインストールされています。gfarm 関係のコマンドは、

```
/usr/local/gfarm/bin
```

にあります。コマンドパスに入れて下さい。

4 連携システム使用法

HPCI 共用ストレージと JLDG をマウントするには、mount.gfarm2fs を使います。

```
% mount.gfarm2fs /etc/gfarm2.conf-hpci ~/HPCI gfarmfs_root=/
Update proxy certificate for gfarm2fs
Mount GfarmFS on /home/yoshie/HPCI
% mount.gfarm2fs /etc/gfarm2.conf-jldg ~/JLDG gfarmfs_root=/
Mount GfarmFS on /home/yoshie/JLDG
% df -H
Filesystem             Size   Used  Avail Use% Mounted on
......
gfarm2fs                23P    15P   8.1P  65% /home/suzuki/HPCI
gfarm2fs               4.6P   2.1P   2.6P  45% /home/suzuki/JLDG
```

第一引数は、gfarm の configuration_file で、上記の通り指定して下さい。第二引数は mount point です。mount point は、予め local file system 上に mkdir で作成しておいて下さい。mount point は NFS でマウントされたファイルシステム上に作らないで下さい。(連携システムホストでは、NFS は使用していません。) 第三引数は、gfarm file system の root directory をマウントする指定です。この引数をつけないと、gfarm の home directory がマウントされますが、JLDG では、home directory にユーザーファイルを置かない事としているので、引数は必ずつけて下さい。特定のディレクトリ以下のみ参照する予定の場合、そのディレクトリを指定しても構いません。例えば、

```
% mount.gfarm2fs /etc/gfarm2.conf-jldg ~/JLDG gfarmfs_root=/gfarm/public
```

mount.gfarm2fs は、自動で、移譲された代理証明書を正規の場所にコピーし、それを各データグリッドの認証に使用します。ファイル操作コマンドをバックグランドで実行後、連携システムホスト上からログアウトした後も、ファイルシステムはマウントされたままとなります。

gfarm command (gfdf や gfls など) は、どちらの gfarm file system に対する操作かを指定する必要があります。必要に応じて、環境変数GFARM_CONFIG_FILE に /etc/gfarm2.conf-hpci か/etc/gfarm2.conf-jldg をセットして下さい。

マウントした２つのファイルシステム間で、gfpcopy を用いて並列コピーができます。ログアウト後も gfpcopy の処理が継続される様、環境変数X509_USER_PROXY を unset した後、gfpcopy を起動して下さい。
sh や bash をお使いの場合、HPCI 共用ストレージから JLDG にディレクトリをまとめてコピーするには、以下のコマンドを用います。

```
% export GFARM_CONFIG_FILE=/etc/gfarm2.conf-hpci
% unset X509_USER_PROXY
% cd ~/HPCI/home/hp130027/hpci000151
% gfpcopy -P -j 16 ConfData-128 ~/JLDG/gfarm/pacscs/hpci
          < /dev/null > ~/hpci2jldg.log 2>&1 &
```

この例では、HPCI共用ストレージの (初期) 課題ID hp130027 HPCI-ID hpci000151 のディレクトリにある ConfData-128 というディレクトリ以下を、JLDG の /gfarm/pacscs/hpci に 16 並列でコピーします。ログファイルは、ホームディレクトリの hpci2jldg.log に書き出します。コマンド実行後、ログアウトしても、処理は継続されます。処理終了後、エラーが無いか、正しく処理されなかったファイルが無いか、次の様なコマンドで確認する事をお勧めします。

```
% grep ERROR ~/hpci2jldg.log
% grep '^\[NG\]' ~/hpci2jldg.log
```

アンマウントは、umount.gfarm2fs を使います。引数無しで２回実行すると、両 gfarm file system が アンマウントされます。

5 HPCI代理証明書の他のクライアントでの利用

連携システムホスト以外のJLDGクライアントは、(現在) GSI認証に基づくログインをサポートしていません。利用されたい場合は、HPCIの代理証明書をダウンロードし、安全な方法 (ssh の公開鍵認証等) で、クライアントにコピーして下さい。クライアント上の代理証明書は、/tmp/x509up_uUID (UIDは、クライアント上の user id 番号) で、permission を 600 として下さい。代理証明書の有効期間内、JLDGを利用できます。(grid-proxy-init は不要。)

6 問い合わせ先

本連携システムに関する問い合わせは、JLDG 管理者グループ (jldgop[AT]jldg.org) にお願いします。本システムは、HPCI の資源ではありませんので、HPCI ヘルプデスクへの問い合わせは、しないで下さい。

7 謝辞

本連携システムの構築は、HPCIシステム利用研究課題『HPCI共用ストレージ・JLDG連携』(課題番号 hp120108) により行われました。また、システムの機器設置・維持管理に、文部科学省 HPCI 戦略プログラム分野５「物質と宇宙の起源と構造」の課題「計算科学推進体制構築　研究支援体制による高度化支援利用」(hp120287,hp130027)、および計算基礎科学連携拠点のサポートを受けています。ここに記して、感謝します。

A　ログイン環境の構築

連携システムホストにログインする環境を新たに構築する場合、対象ホストが RedHat 系で、管理者権限をお持ちであれば、HPCI ログインマニュアルに書かれた方法より簡便に、環境構築できます。

A.1　時計合わせ

ログイン元計算機の時刻が正確でないと、GSI 認証で不具合が生じる場合があります。ntp 等を導入して下さい。

A.2　Globus Toolkit のインストール

Globus のリポジトリをインストールします。

```
http://toolkit.globus.org/toolkit/downloads/latest-stable/
```

の “Globus repository configuration files” から、お使いの OS に対応したリポジトリをインポートして下さい。CentOS 6 の場合

```
# rpm -Uvh http://toolkit.globus.org/ftppub/gt5/5.2/5.2.5/installers/repo/
                  Globus-5.2.stable-config.centos-6-1.noarch.rpm
```

次に、必要なパッケージをインストールします。

```
# yum install gsi-openssh-clients
# yum install globus-proxy-utils
```

後者は必須ではありませんが、代理証明書の確認に使用するツールがインストールされますので、インストールしておく事をお勧めします。

A.3　HPCI CA 局証明書のインストール

HPCI ログインマニュアル (資料 [3])『3.2. Globus Toolkit のインストール手順』の『(4) 信頼できる CA の設定』に従って、HPCI CA 局証明書を所定の場所に格納します。マニュアルでは、`~/.globus/certificates` にインストールする様になっていますが、`/etc/grid-security/certificates` にインストールする事をお勧めします。(こうする事で、各ユーザーが、この作業をする必要がなくなります。) 手順は以下の通りです。web browser と端末ソフトを同時に立ち上げて作業して下さい。

```
# mkdir -p /etc/grid-security/certificates
# cd /etc/grid-security/certificates
```

web browser で、HPCI 認証局 https://www.hpci.nii.ac.jp/ca/ にアクセスし、ページ下部の『認証局情報』欄の『CA 証明書ダウンロード』をクリックします。一番下の hpcica.pem.zip にカーソルを合わせ、リンクの URL をコピーして下さい。

```
# wget https://www.hpci.nii.ac.jp/ca/hpcica.pem.zip
      (URL はペーストして下さい。)
# unzip hpcica.pem.zip
```

web browser で一つ戻って、『Signing Policy』をクリックし、hpcica.signing_policy.zip にカーソルを合わせ、リンクの URL をコピーして下さい。

```
# wget https://www.hpci.nii.ac.jp/ca/hpcica.signing_policy.zip
      (URL はペーストして下さい。)
# unzip hpcica.signing_policy.zip
```

web browser で一つ戻って、『CRL ダウンロード（PEM 形式)』にカーソルを合わせ、リンクの URL をコピーして下さい。

```
# wget https://www.hpci.nii.ac.jp/ca/hpcica.crl
      (URL はペーストして下さい。)
# mv hpcica.crl ‘openssl crl -in hpcica.crl -noout -hash‘.r0
```

失効リストを定期的に更新する為、下記のスクリプトを/etc/cron.daily/getHpciCrl.sh に作って下さい。

```
% cat /etc/cron.daily/getHpciCrl.sh
#! /bin/sh
CERTDIR=/etc/grid-security/certificates
SERVER=www.hpci.nii.ac.jp
CRL_CA=hpcica.crl

/usr/bin/wget -P $CERTDIR http://$SERVER/ca/$CRL_CA
HASH_CA=‘/usr/bin/openssl crl -in $CERTDIR/$CRL_CA -noout -hash‘
/bin/mv $CERTDIR/$CRL_CA $CERTDIR/${HASH_CA}.r0
```

A.4 HPCI 計算機資源へのログインテスト

ユーザー権限で、HPCI 計算機資源へのログインテストを行います。

A.4.1 HPCI 電子証明書の発行

HPCI 電子証明書を発行していない場合は、HPCI ログインマニュアル (資料 [3]) の『2.1. 電子証明書の発行手順』に従って、電子証明書を発行して下さい。以下は手順の概略です。(はじめて電子証明書を発行する際は、必ず HPCI ログインマニュアルを参照して下さい。以下は、再発行時のメモとして、参照下さい。)

https://portal.hpci.nii.ac.jp/ にアクセス
　HPCI 認証フェデレーション プライマリセンター選択画面 が表示される
プライマリセンターを選択する
プライマリセンターログインページで HPCI アカウントでログインする
　HPCI 証明書発行システムメニュー が表示される
電子証明書発行を選択する
電子証明書発行画面で、パスフレーズを入れ、発行ボタンを押す
　電子証明書の発行完了画面が表示される

A.4.2 代理証明書の発行とダウンロード

代理証明書は、有効期限の短い、電子証明書の写しです。HPCI 共用ストレージを利用したり、HPCI 計算機資源に GSI 認証でログインしたり、JLDG との連携システムを利用する際の認証に用いられます。電子証明書本体は使いません。代理証明書の有効期限が切れ、再度利用する際には、本節の手順を再度行う必要があります。

代理証明書の使いかたは幾つかありますが、ここでは、代理証明書をダウンロードして (ログイン元計算機に置いて) 利用する方法を示します。代理証明書のダウンロード法についても、HPCI ログインマニュアルを参照して下さい。以下は、手順の概略です。

HPCI 証明書発行システムメニューを表示する (上記の手順を参照)
メニュー画面で、代理証明書発行・ダウンロードを選択する
ダウンロードラジオボタンを選択し、パスフレーズ、有効期限を入力し、ダウンロード
　代理証明書を保存する。保存先は、
　/tmp/x509up_uUID　(UID はそのマシンの user id 番号)
代理証明書のパーミッションを 600 に変更する

代理証明書が正しくダウンロードできている事は、grid-proxy-info で確認できます。

A.4.3 HPCI 計算機資源へのログインテスト

ご自身の HPCI 利用課題で利用可能な計算機資源に、GSI 認証でログインできる事を確認します。

HPCI 共用ストレージを使える場合

```
% gsissh -p 2222 hpcieast-p01.cspp.cc.u-tokyo.ac.jp
```

K computer を使える場合

```
% gsissh -p 2222 k.aics.riken.jp
```

その他の HPCI シングルサインオンをサポートしている計算機資源へのログインテストでも構いません。

A.4.4 HPCI 共用ストレージの利用テスト

この時点で、HPCI 共用ストレージが利用できる事を確認しておく事をお勧めします。東京大学情報基盤センター提供クライアントにログインして、マウントしてみて下さい。

```
% gsissh -p 2222 hpcieast-p01.cspp.cc.u-tokyo.ac.jp   （クライアントへログイン）
% mount.hpci
% df
% umount.hpci
```

/gfarm/課題 ID/ユーザー名 で HPCI 共用ストレージがマウントされます。

HPCI 共用ストレージの利用については、『HPCI 共用ストレージ利用マニュアル』(資料 [4]) を参照して下さい。なお、HPCI 電子証明書を発行した後、HPCI 共用ストレージを利用できる様になるまで、1 日程度時間が掛かる場合があります。

A.5 KEK CA 局証明書のインストール

本連携システムのホスト jldghpci.ccs.tsukuba.ac.jp は、KEK CA 局発行のホスト証明書を用いています。この為、ログイン元計算機に、KEK CA 局証明書のインストールが必要です。KEK GRID CA Web Repository http://gridca.kek.jp/ から、ページ下部の『CA Certificate』、『CA Signing Policy』、『CRL』を /etc/grid-security/certificates に保存します。

```
# cd /etc/grid-security/certificates
# wget http://gridca.kek.jp/repository/617ff41b.0
# wget http://gridca.kek.jp/repository/617ff41b.signing_policy
# wget http://gridca.kek.jp/repository/617ff41b.r0
```

OpenSSL のバージョンを確認して下さい。`openssl version` で確認できます。バージョンが 1.0.0 以降の場合、証明書のハッシュ値（上の例では、`617ff41b`）がダウンロードしたものと異なります。以下を実行して下さい。

```
# ln -s 617ff41b.0 2f2f573f.0
# ln -s 617ff41b.signing_policy 2f2f573f.signing_policy
# ln -s 617ff41b.r0 2f2f573f.r0
```

失効リストの自動更新の為、以下のスクリプトを`/etc/cron.daily` に置いて下さい。

```
% cat /etc/cron.daily/getKEKCrl.sh
#! /bin/sh
CERTDIR=/etc/grid-security/certificates
KEKCA=617ff41b
CRLWGT=http://gridca.kek.jp/repository/617ff41b.r0

/usr/bin/wget -O $CERTDIR/$KEKCA.r0 $CRLWGT
```

A.6　連携システムホスト へのログインテスト

ユーザーとして作業して下さい。HPCI 電子証明書発行システムからご自身の代理証明書をダウンロードし、所定の場所に配置して下さい。（手順は、アペンディクス A.4.2 を参照。）

連携システムホストへログインしてみて下さい。

```
% gsissh jldghpci.ccs.tsukuba.ac.jp
```

さらに、連携システムホスト上で、

```
% grid-proxy-info
```

を実行して見て下さい。エラー無く代理証明書情報が表示されれば、連携システムホストへ、代理証明書が移譲されています。

資料

[1] http://www.jldg.org/jldg/Tebiki/tebiki.pdf

[2] https://www.hpci-office.jp/entry から、HPCI-ID 登録情報の確認へと進んで下さい。

[3] https://www.hpci-office.jp/ の『利用者のページ』の『マニュアル』にあります

[4] https://www.hpci-office.jp/ の『利用者のページ』の『マニュアル』にあります