

Japan Lattice Data Grid 利用の手引き

JLDG チーム

2008年 5月23日 第1版 第1刷
2010年 7月16日 第2版 第1刷

目次

1	JLDG の概要	3
1.1	JLDG の目的	3
1.2	システムとその利用の概要	3
1.3	利用資格	4
1.4	利用形態	4
1.4.1	一般公開データの利用	5
1.4.2	グループ間データ共有	5
2	利用開始までの流れ	5
2.1	クライアントマシンのアカウント取得	5
2.2	グループ連絡責任者への連絡	5
2.3	ライセンス ID の取得	6
2.4	ユーザー証明書の取得	6
2.5	証明書のブラウザへのインポート	8
2.6	仮想組織 (VOMS) への登録	10
3	日常の利用	10
3.1	grid-proxy-init	10
3.2	uberftp	11
3.3	証明書の再取得	12
4	困ったときの連絡先	12

1 JLDG の概要

1.1 JLDG の目的

Japan Lattice Data Grid (JLDG) は、国内の格子 QCD 及び関連分野の研究者・研究グループが、QCD 配位等の貴重なデータを大域的かつ効率的に共有し、研究の格段の促進と計算資源の有効活用を図る事を目的に構築されたデータグリッドです。

1.2 システムとその利用の概要

2010 年 5 月現在、6 つの研究拠点、筑波大計算科学研究センター、高エネルギー加速器研究機構計算科学センター、京都大学基礎物理学研究所¹、大阪大学核物理研究センター、広島大学理学部物理学科、金沢大学自然科学研究科² が JLDG に接続しています(図 1)。

各拠点にはファイルサーバが置かれ、国立情報学研究所が提供する SINET3 上のプライベートネットワーク Hepnet-J/sc に接続されています(図 2)。ファイルサーバ群は、産業技術総合研究所・筑波大学で開発された Gfarm システムにより束ねられており、ユーザーからは、あたかも単一の(パーティションの区切りがない)Unix 的なファイルシステム(以降、JLDG ファイルシステムと呼びます)に見えます。各拠点にはクライアントマシンが設置されており、ユーザーはクライアントマシンの一つにログインして、grid ftp (gftp) で JLDG ファイルシステムにアクセスします。クライアントマシンは各拠点のスーパーコンピュータや基幹のファイルサーバのファイルシステムを NFS マウントしています。どのクライアントから JLDG ファイルシステムにアクセスしても同一のディレクトリ構造やファイルが見えるので、スーパーコンピュータで生成した貴重な計算結果ファイルを JLDG ファイルシステムに置いておけば、それを任意の拠点から取り出し、その拠点のスーパーコンピュータで解析するといった作業を、効率よく行うことができます。

複数の研究拠点に所属する複数の研究者が共同研究を行う場合、JLDG ファイルシステムにデータを蓄積する事によって、データ共有の為にファイルを研究者自身が遠隔地に複製したり、複製間での煩雑な世代管理に煩わされることなく、ファイルを共有することができます。JLDG は、複数拠点間の自動ファイル複製機能を備えているので、複数の拠点で同一のデータに高速にアクセスする事も可能です。

JLDG では、研究グループ内でのデータ共有のみならず、国内の研究者にとって有用と想われるデータを一般に公開することもできます。

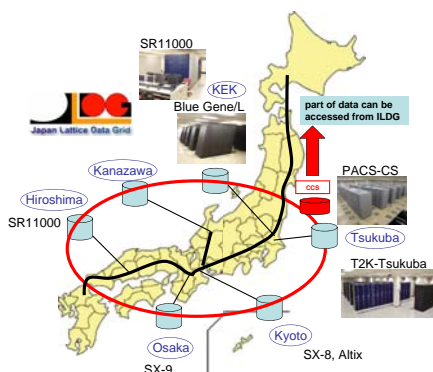


図 1: システム概念図 : 1

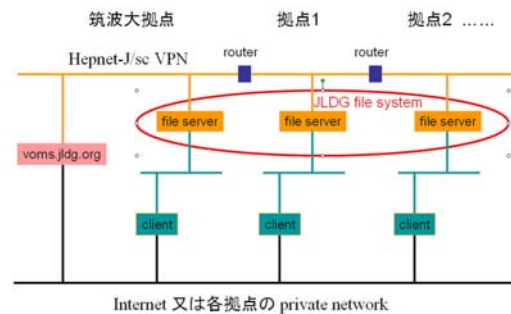


図 2: システム概念図 : 2

¹ 管理者不在の為現在停止しています。
² 現在システムアップグレード作業中です。

JLDG ファイルシステムへのアクセスは、クライアントのユーザー ID とは全く別の『ユーザー証明書』を用いて行います。ユーザー証明書は JLDG 内で共通であり、どの拠点から JLDG ファイルシステムにアクセスする場合も同一です。この様な、組織に依存しない仮想組織は、EDG (European Data Grid) で開発された VOMS (Virtual Organization Management System) によって管理されています。

JLDG は 筑波大学計算科学研究センターにて International Lattice Data Grid (ILDG) と接続しています(図 1)。ILDG は国際規模での QCD 配位共有の為に構築されたデータグリッドです。国内の研究グループが ILDG に公開する配位は、全て JLDG ファイルシステム上に置かれるので、それらの配位を国内で利用する際は、ILDG 経由ではなく、直接 JLDG からダウンロードする事ができます。

1.3 利用資格

JLDG は国内の格子 QCD 及び関連分野の研究者(大学院生を含む)であれば、原則誰でも利用できます。ユーザーは JLDG 仮想組織内の何れかのグループに所属しなければなりません。現在、JLDG には表 1 に示したグループが用意されています³。

pacses	筑波大学計算科学研究センターを拠点とする PACS-CS Collaboration の研究用。
jlqcd	高エネルギー加速器研究機構を拠点とする JLQCD Collaboration の研究用。
rcnp	大阪大学核物理研究センターを拠点とするユーザーの研究用。
npftqed	npftqed グループの研究用。
jldg	上記の何れにも属さないユーザー用。
public	一般公開用データ (ILDG 用等) を作製する為のグループ。一般ユーザーは所属できない。

表 1: JLDG のグループ

ユーザーは、さらに、JLDG ファイルシステムにアクセスする為にクライアントマシンの何れかのユーザーアカウントが必要です⁴。通常利用する(最もよく利用する)クライアントマシンを管理する拠点を、ユーザーの所属サイトと呼びます。

従って、JLDG を利用するユーザーは、所属グループと所属サイトを決め、利用を開始することとなります。

1.4 利用形態

JLDG ファイルシステムは、

- 一般公開データのダウンロード
- グループ間データ共有

の 2 つの方法で利用する事を想定しています。

JLDG を利用した研究の成果を論文等で公開する際は、例えば、

This work is supported by the JLDG constructed over the SINET3 of NII.
等の謝辞を含めて下さい。

³ 新たな研究グループ作成を希望される場合は、voadmin[AT]jldg.org に相談下さい。

⁴ ILDG 経由で JLDG から ILDG に公開しているゲージ配位を取得する場合は、クライアントマシンのいずれにもアカウントを持つ必要はありません。

1.4.1 一般公開データの利用

一般公開データは、JLDG ファイルシステムの /gfarm/public 以下にストアされています。特に ILDG に公開されている QCD 配位は

```
/gfarm/public/ILDG/JLDG/Collaboration 名/
```

以下に置かれています。ここで、"Collaboration 名" は配位を生成した Collaboration の名称です。各 Collaboration は、配位公開のポリシー(利用範囲、配位を利用した結果を論文等で公開する場合の Acknowledge など)を定め、JLDG web page <http://www.jldg.org/ildg-data/> に掲載しているので、そのポリシーに従う事が求められます。また、JLDG から取得したデータは共同研究の範囲内で複数ユーザが利用して構いませんが、再配布はしないで下さい。

1.4.2 グループ間データ共有

研究グループのトップディレクトリは

```
/gfarm/グループ名/
```

です。当該ディレクトリは、グループに所属する全ユーザが書き込み権を有し、それ以外のユーザはアクセスできない (unix の記法で 770) 設定で提供されます⁵。トップディレクトリ以下の利用法は、各グループにまかされます。必要に応じて、Unix と同様のアクセス制御(ファイルやディレクトリの user/group/other のパーミッション設定)が可能で

2 利用開始までの流れ

2.1 クライアントマシンのアカウント取得

JLDG ファイルシステムにアクセスするには、JLDG に接続している筑波大学計算科学研究センター (筑波)、高エネルギー加速器研究機構 (KEK)、京都大学基礎物理学研究所 (京都)、大阪大学核物理研究センター (大阪)、広島大学理学部 (広島)、金沢大学自然科学研究科 (金沢) のいずれかのサイトの JLDG クライアントマシン (表 2) のユーザである必要があります。通常利用するサイトを所属サイトと呼びます。希望する所属サイトの管理者にクライアントマシンのアカウントを申請してください。各サイトで設けている計算機システムの利用規定に合致していれば、サイトの管理者からクライアントマシンのアカウントが発行されます。

2.2 グループ連絡責任者への連絡

各ユーザは JLDG 仮想組織の何れかのグループ (表 1) に所属します。所属するグループの連絡責任者 (表 3) に、JLDG を利用する旨と、氏名、所属 (研究機関名)、e-mail アドレス、所属サイト名、所属サイトのクライアントマシンのアカウント名、所属するグループ名、の情報をお知らせ下さい⁶。特定の研究グループに所属しないユーザは 仮想グループ jldg に所属することになります。この場合は、所属サイトの管理者に連絡して下さい。連絡は e-mail で構いません。

⁵ 設定は変更可能です。グループの連絡責任者から voadmin@jldg.org 宛、連絡下さい。

⁶ ユーザは複数のグループに所属する事もできます。ユーザ証明書を取得後、追加で所属するグループの連絡責任者に連絡して下さい。その際、証明書のサブジェクト (後述) もお知らせ下さい。

サイト	管理者	クライアントマシン
筑波	浮田尚哉 (ukita[AT]ccs.tsukuba.ac.jp)	jldg-fr1.ccs.tsukuba.ac.jp jldg-fr2.ccs.tsukuba.ac.jp
KEK	松古栄夫 (hideo.matsufuru[AT]kek.jp)	scfe.kek.jp
京都	現在管理者不在です。	現在利用できません。
大阪	外川浩章 (togawa[AT]rcnp.osaka-u.ac.jp)	gftp.rcnp.osaka-u.ac.jp
広島	石川健一 (ishikawa[AT]theo.phys.sci.hiroshima-u.ac.jp)	theoipc.phys.sci.hiroshima-u.ac.jp
金沢	武田真滋 (takeda[AT]hep.s.kanazawa-u.ac.jp)	現在利用できません。
全体	吉江友照 (yoshie[AT]ccs.tsukuba.ac.jp)	

表 2: 各サイトの管理者とクライアントマシン

グループ	連絡責任者
pacscs	浮田尚哉 (ukita[AT]ccs.tsukuba.ac.jp)
jlqcd	松古栄夫 (hideo.matsufuru[AT]kek.jp)
rcnp	外川浩章 (togawa[AT]rcnp.osaka-u.ac.jp)
npftqcd	駒佳明 (koma[AT]numazu-ct.ac.jp)
jldg	所属サイトの管理者
仮想組織管理者	voadmin[AT]jldg.org

表 3: グループの連絡責任者等

2.3 ライセンス ID の取得

グループの連絡責任者 (jldg グループの場合は所属サイトの管理者) は、当該ユーザーがグループのメンバーであること (サイトのユーザーであること) を確認した後、ユーザーからの登録情報を JLDG 仮想組織管理者に e-mail にて連絡、登録依頼をします。

ユーザーは、e-mail を通じて仮想組織管理者からライセンス ID を受け取ります。ライセンス ID とは、JLDG のユーザー証明書を発行する際に必要になる一回限りの ID で、次のような大文字のアルファベットと数字の列です。

JLDG-CJ08SU-STUF2S-NH1ZCA

グループの連絡責任者 (所属サイトの管理者) はユーザーが JLDG を利用する際のコンタクトパーソンです。今後、所属の変更等異動があった場合は、グループの連絡責任者 (所属サイトの管理者) にその旨連絡下さい。

2.4 ユーザー証明書の取得

ユーザー証明書取得の作業は、所属サイトのクライアントマシン (表 2) 上でおこないます。(所属サイトが KEK の場合、証明書発行までの手順が他の拠点と異なります。KEK ではシステムの構成上クライアントマシンから直接証明書を取得することができないためです。KEK を所属サイトとして登録を希望される方は、管理者にご相談ください。)

まず、クライアントマシンにログインし、login shell に応じて次の様に環境設定を行います。

- login shell が bash の場合、~/ .bashrc に次の行を付け加えてください。

```
export GLOBUS_LOCATION=/usr/gt4
. $GLOBUS_LOCATION/etc/globus-user-env.sh
```

(2行目の先頭は"."(ピリオド)です。)

- login shell が tcsh の場合、~/ .cshrc に次の行を付け加えてください。

```
setenv GLOBUS_LOCATION /usr/gt4
source $GLOBUS_LOCATION/etc/globus-user-env.csh
```

ユーザー証明書のユニークな ID を 証明書の”サブジェクト”と呼びます。JLDG のユーザー証明書のサブジェクトは以下の形式になっています。

```
/C=JP/O=JLDG/OU=所属グループ名/CN=フルネーム
```

例えば、

```
/C=JP/O=JLDG/OU=jldg/CN=Ichiro Suzuki
```

です。ユーザー証明書を取得する為に jldg-user-req.sh を実行してください。

(実行例)

```
$ /usr/local/naregi-ca/bin/jldg-user-req.sh
--- Construct certificate request contents ---
Please select your group
1) jldg
2) pacscs
3) jlqcd
4) rcnp
5) public
6) npftqcd
Input group number : 1          グループ名を選択
Please input your full name...
Ex.) John Smith : Ichiro Suzuki   ユーザー名を入力 (この例のようにフルネームを入力)
-----You are requesting below content -----
"C=JP/O=JLDG/OU=jldg/CN=Ichiro Suzuki"
-----
Is it OK? (Y/N) : Y          証明書のサブジェクトを確認し、OKなら"Y"を入力
Please input one time LicenseID for CA...
Ex.) ABCD-EFGHIJ-KLMNOP-QRSTUV : JLDG-CJM8S0-I7M9TS-6R4RV0   交付のライセンス ID を入力

----- Start to access JLDG CA service -----
```

```

-----
creating a certificate signing request
-----
generate private key (size 1024 bit)
.....oo
.....oo
input Distinguished Name (DN).
select directory tag (input number)
(1.C, 2.ST, 3.L, 4.O, 5.OU, 6.CN, 7.UID, 8.Email, 9.Quit)[1]:Country [JP]: select dir ((略))
(1.C, 2.ST, 3.L, 4.O, 5.OU, 6.CN, 7.UID, 8.Email, 9.Quit)[2]:Organization [nitech.ac. ((略))
(1.C, 2.ST, 3.L, 4.O, 5.OU, 6.CN, 7.UID, 8.Email, 9.Quit)[6]:Organization Unit []: se ((略))
(1.C, 2.ST, 3.L, 4.O, 5.OU, 6.CN, 7.UID, 8.Email, 9.Quit)[6]:Common Name [test]: sele ((略))
(1.C, 2.ST, 3.L, 4.O, 5.OU, 6.CN, 7.UID, 8.Email, 9.Quit)[8]:trying to connect RA ser ((略))
request for issuing a new certificate ... ok.
save a CA certificate file : /home/ichiro/.globus/9fac2951.0
save a certificate file : /home/ichiro/.globus/usercert.pem
save a private key file : /home/ichiro/.globus/userkey.pem
Input PASS Phrase:          証明書のパスフレーズを設定(忘れないように)
Verifying - Input PASS Phrase:   チェックのため再度パスフレーズを入力
----- END OF jldg-user-req.sh -----

```

この作業を終えると、\$HOME/.globus 以下に次の 3 つのファイルが生成されます。

- ユーザ証明書 (usercert.pem)
- ユーザ秘密鍵 (userkey.pem)
- CA 証明書 (9fac2951.0)

2.5 証明書のブラウザへのインポート

JLDG 仮想組織への登録はブラウザを用いて行います。そのために、まず、openssl コマンドを使って次の要領で証明書を PKCS12 形式のファイルに変換します。

```
$ openssl pkcs12 -export -in ユーザー証明書 -inkey ユーザー証明書の秘密鍵 \
-out PKCS12形式のファイル名
```

具体例:

```
$ openssl pkcs12 -export -in $HOME/.globus/usercert.pem \
-inkey $HOME/.globus/userkey.pem -out $HOME/.globus/usercert.p12
Enter pass phrase for /home/ichiro/.globus/userkey.pem: ユーザ証明書取得時の pass phrase
Enter Export Password:          web browser で使うパスワードを設定する。
Verifying - Enter Export Password: 確認のため再入力。
```

「usercert.p12」ができあがった PKCS12 形式のファイルです。この例だと \$HOME/.globus 中にできます。(他の場所に生成してもよいのですが、決して他人から見える場所に置かないよう注意してください。)

次に、ブラウザに変換された証明書をインポートします。ブラウザの種類に応じて、次の要領で行ってください。

- Mozilla の場合

1. 「Edit」 「Preference」 「Privacy&Security」 「Certificate」の Manage Certificate を起動します。
2. 「Your Certificate」タブを選択し、「Import」をクリックします。
3. ファイル選択ウィンドウが開くので、「usercert.p12」を選択します。
4. この機能を初めて使う場合、Change Master Password ポップアップが表示されます。これは、ブラウザの証明書機能を使用するときに使われるパスワードを設定するものです。ブラウザの証明書の出し入れの他、ブラウザが覚えているパスワードの取り出しなどにも使われますので、忘れないようにしましょう。
5. Password Entry Dialog が開きます。PKCS12 形式に変換したときに使ったパスワードを入力します。
6. 「successfully restored your security certificate(s) and private key(s)」と表示されるので、「OK」をクリックします。
7. 続けて、「OK」 「OK」で完了です。

- Mozilla Firefox(日本語版) の場合

1. 「編集」 「設定」 「詳細」 「セキュリティー」タブ (Firefox 2.0 の場合は、「暗号化」タブ) 「証明書を表示」と選択していきます。
2. 証明書マネージャが開くので、「インポート」を選択します。
3. ファイル選択ポップアップが開くので、「usercert.p12」を選択します。
4. 先ほどの PKCS12 形式への変換時に使用したパスワードを入力します。
5. 「セキュリティー証明書と秘密鍵が正常に復元されました」と表示されるので「OK」を押します。
6. 証明書マネージャに JLDG の証明書の情報が表示されると終了です。

- Internet Explorer(日本語版) の場合

1. 「ツール」プルダウンメニューから「インターネットオプション」を選択します。
2. 「インターネットオプション」ポップアップが表示されるので、「コンテンツ」タブをクリックします。
3. 真中あたりの「証明書」ボタンをクリックします。
4. 証明書ウィンドウが表示されるので、「インポートを選択します。」
5. 「証明書のインポートウィザード」が表示されるので、これに従って進みます。「次へ」をクリックします。
6. 「参照」をクリックし、「usercert.p12」を選択し、「次へ」をクリックします。
7. PKCS12 形式変換時に設定したパスワードを入力します。
8. 「次へ」 「次へ」 「完了」とクリックしていきます。

9. 「正しくインポートされました」と表示されるので「OK」をクリックして終了です。

- 次の URL の「鍵対の WEB ブラウザへの組込み」により説明があります。

<http://www.icepp.s.u-tokyo.ac.jp/~sakamoto/education/atlasj/lcg/certificate>

2.6 仮想組織 (VOMS) への登録

以下の手順に従って、仮想組織への登録を行ってください。

1. 証明書を読み込んだブラウザで、次の URL をアクセスし、「Welcome to VOMS!」のページを表示します。

<https://voms.jldg.org:8443/voms/jldg>

必要に応じて先ほどインポートした証明書を提示してください。また、Web サイトのセキュリティー証明書関係で問題が出る可能性があります。「一時的に証明書を受け入れる」等を選び、お進みください。

2. 左にある「New user registration」をクリックします。「VO User Registration Request」のページに進入できました。このページの内容を熟読の上、必要事項を記入してください。その後、下にある二つのボタン「I have read and agree to the VO's Usage Rules」または「I DO NOT agree to the VO's Usage Rules」のいずれかをクリックしてください。
3. 本人確認のため「New user registration」のページで書き込んだメールアドレスにメールが送られてきます。そのメール中の“<https://voms...>”のページにアクセスすると本人確認が終了します。
4. VOMS 管理者の処理が終了すると、手続き終了を知らせるメールが届きます。

JLDG ファイルシステムの利用は、仮想組織管理者の処理終了後の翌日午前 4 時から可能です。

3 日常の利用

3.1 grid-proxy-init

JLDG ファイルシステムにアクセスするためには、まず、“grid-proxy-init” command を使って、GSI 認証用⁷ に一定時間 (default 値:12 時間) だけ有効なプロキシ証明書 (代理証明書) を作成します。

```
$ grid-proxy-init
```

証明書作成時に入力したパスフレーズを入力します。

知っておくと便利なオプションをまとめました。

- default の有効時間の 12 時間は、“-valid” オプションを使って変更できます。

⁷ GSI: Grid Security Infrastructure の略

(例) `$ grid-proxy-init -valid 72:00` 72 時間有効なプロキシ証明書が生成される。

- `grid-proxy-init` は default では、`~/globus` 中の証明書を参照しますが、これらは“-cert” オプションと“-key” オプションを使って変更可能です。いくつか証明書を持っていて、それらを状況に応じて使い分けたいときに便利です。

(例) `$grid-proxy-init -cert .globus-KEK/usercert.pem \`
`-key .globus-KEK/userkey.pem`

3.2 uberftp

サイト名	ホスト名
筑波大学計算科学研究センター	jldg-fs1
KEK 高エネルギー加速器研究機構	scjldg01
京都大学基礎物理学研究所	yitpjldg01
大阪大学核物理研究センター (RCNP)	rcnp-gf-dmz-sc
広島大学理学部	jldghu01-local
金沢大学自然科学研究科	

表 4: 各サイトの FS ノード

JLDG ファイルシステムは、所属サイトのクライアントマシンから NCSA で開発された `uberftp` という `grid ftp` ソフトウェアを用いて、所属サイトのファイルサーバノード (以降 FS ノードとよびます) に接続して利用します。各サイトの FS ノードのアドレスは、表 4 を参照してください。

`uberftp` は 環境変数 `LANG` が設定されていると正しく動きません。環境変数 `LANG` を無効にするには、ログインシェルが `bash` の場合は、`unset LANG`、`tcsh` の場合は `unsetenv LANG` です。(`.basrc` `.cshrc` 等を書いておくと便利です。)

1. `uberftp` を起動します。

```
$ uberftp <FS ノード名>
220 FS ノード名 GridFTP Server 2.3 (gcc32, 1144436882-63) ready.
230 User nobody logged in.
```

2. JLDG ファイルシステムで共有されている `directory` へ `cd` します。(起動直後の `directory` は、Grid ファイルシステムで共有されていないので注意してください。)

```
uberftp> cd /gfarm/<グループ名>
```

3. JLDG から ILDG に公開されているゲージ配位は次以下にあります。

/gfarm/public/ILDG/

4. directory 構造を保ったまま、ダウンロードする場合は”get -r”を使います。
例えば、/gfarm/public/ILDG/JLDG/XX 以下を local の current directory に download する場合

(例)
uberftp> cd /gfarm/public/ILDG/JLDG
uberftp> get -r XX

5. “help” command で uberftp の command の概略を見られますが、もっと詳しい情報は、次の URL を参照してください。

<http://dms.ncsa.uiuc.edu/set/uberftp>

3.3 証明書の再取得

ユーザー証明書は発行時から3年間有効⁸です。失効後(失効時期が近づき)JLDGの継続利用を希望する場合は、登録されているメールアドレスから voadmin[AT]jldg.org 宛、証明書のサブジェクトを添えて、ライセンスIDの発行を依頼してください。ライセンスIDを受け取ったら、2.4節の手順で同じサブジェクトでユーザー証明書を取得し、以降、その証明書を用いてJLDGをご利用下さい。仮想組織への再登録の手続きは不要です。

4 困ったときの連絡先

お困りの点や疑問点等がございましたら、お気軽に各サイトの管理者(表3)までご相談ください。

謝辞

JLDGの開発、維持管理に、以下の外部資金の援助を受けています。ここに記して謝意を表します。

- 日本学術振興会先端研究拠点事業「計算素粒子物理学の国際研究ネットワークの形成」(平成16年度～平成17年度)
- 国立情報学研究所 CSI 委託事業「グリッド・認証技術による大規模データ計算資源の連携基盤の構築」
- 国立情報学研究所「e-science 研究分野の振興を支援する CSI 委託事業」の「計算素粒子物理学の高度データ共有基盤 JLDG の構築」
- 国立情報学研究所「e-Science 研究分野を支援する CSI 委託事業」の「計算素粒子物理学のデータ共有基盤 JLDG の高度化」
- 科学研究費補助金(新学術領域研究)「素核宇宙融合による計算科学に基づいた重層的物質構造の解明」の計画研究「分野横断アルゴリズムと計算機シミュレーション」(平成20年度～平成24年度)

⁸ 証明書の有効期限等の情報は、grid-cert-info コマンドで調べられます。