Japan Lattice Data Grid 利用の手引き (第6版)

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
2011 年 1 月 10 日 第 3 版 第 1 刷
2013 年 9 月 30 日 第 4 版 第 1 刷
2014 年 4 月 23 日 第 5 版 第 1 刷
2014 年 9 月 05 日 第 5 版 第 2 刷
2014 年 11 月 17 日 第 5 版 第 3 刷
2016 年 4 月 07 日 第 5 版 第 4 刷
2021 年 4 月 21 日 第 6 版 第 1 刷
2022 年 3 月 09 日 第 6 版 第 2 刷

目 次

1 JLDG の概要 **4**
1.1 JLDG の目的 4
1.2 システムとその利用の概要 4
1.3 利用資格 6
1.4 利用形態 7
1.4.1 一般公開データの利用 7
1.4.2 グループ内データ共有 8

2 利用開始までの流れ **8**
2.1 証明書発行の為のアカウント取得 8
2.2 グループ責任者への連絡 8
2.3 ライセンス ID の取得 9
2.4 ユーザ証明書の取得 10
2.5 証明書の管理とコピー 12
2.6 JLDG 仮想組織への登録 12
2.6.1 ユーザ証明書のブラウザへのインポート 12
2.6.2 仮想組織 (VOMS) への登録 15
2.6.3 情報の更新 15

3 利用法 **16**
3.1 代理証明書の作成 16
3.2 uberftp による利用 17
3.3 Gfarm コマンド 19
3.4 JLDG ファイルシステムのマウント 22
3.4.1 データのコピー 23
3.4.2 ファイルの複製について 24
3.5 証明書の失効と再発行 25
3.5.1 有効期限が経過した場合 26
3.5.2 ユーザ証明書を紛失した (パスフレーズが漏洩した) 場合 27
3.5.3 JLDG 認証局更新による証明書世代の更新 27

4 困ったときの連絡先 **28**

5 JLDG チームからのお願い **28**

A 各拠点の環境 **30**
A.1 筑波大学計算科学研究センター 30
A.1.1 クライアント 30
A.2 高エネルギー加速器研究機構計算科学センター 30

A.2.1 クライアント 30
A.2.2 グリッド ftp サーバ 31
A.3 大阪大学核物理研究センター 31
A.4 広島大学理学部物理学科 31
A.5 東京大学情報基盤センター 31
A.6 京都大学基礎物理学研究所 31
A.6.1 クライアント 31
A.6.2 グリッド ftp サーバ 31
A.7 理化学研究所仁科加速器科学研究センター 32
A.7.1 クライアント (仁科 NW 上) 32
A.7.2 クライアント (HOKUSAI スパコン NW 上) 32
A.7.3 グリッド ftp サーバ 32
A.8 理化学研究所計算科学研究センター 32

B JLDG 管理サーバへのアクセス 33
B.1 クライアントネットワーク 33
B.2 仮想組織管理サーバへのアクセス 33
B.2.1 筑波大計算科学研究センター 34
B.2.2 大阪大学核物理研究センター 35
B.2.3 理化学研究所仁科加速器科学研究センター 35
B.2.4 理化学研究所計算科学研究センター (富岳) 35
B.2.5 ブラウザの socks-v5 proxy 設定 36

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

2022 年 1 月現在、8 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 (KEK)、大阪大学核物理研究センター (RCNP)、広島大学理学部物理学科、東京大学情報基盤センター (柏キャンパス) [1]、京都大学基礎物理学研究所、理化学研究所仁科加速器科学研究センター (和光)、理化学研究所計算科学研究センター (神戸) が JLDG に接続しています (図 1)。

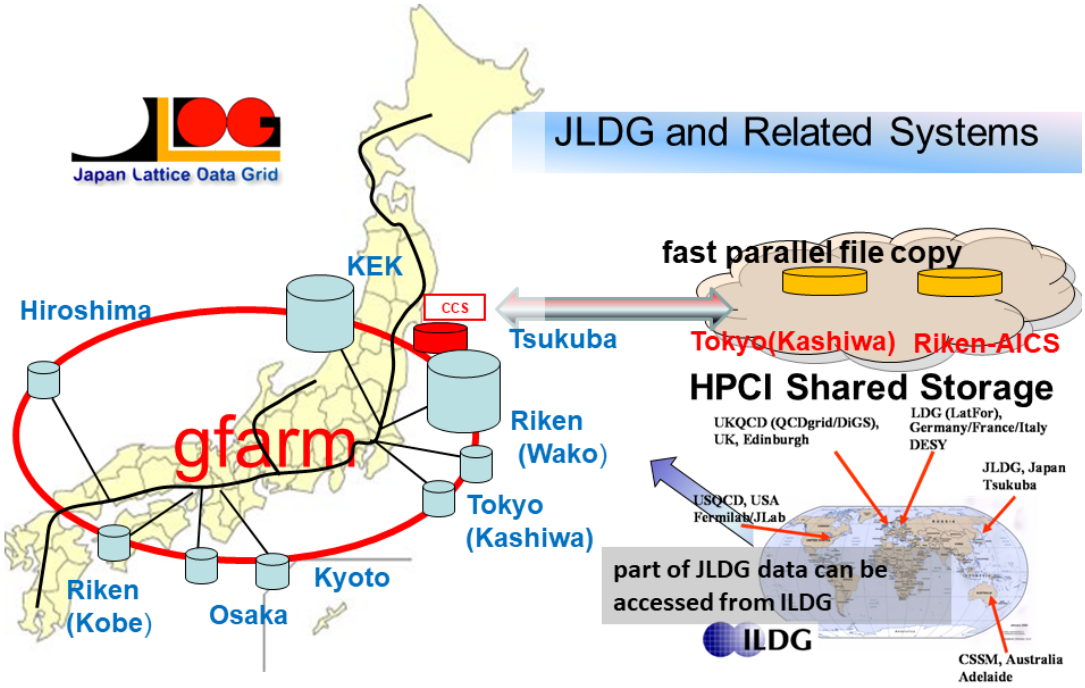

図 1: システム概念図

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 SINET5 上の L3-VPN (バーチャルプライベートネットワーク) Hepnet-J/sc に接続されています。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

[1] サーバのみ。クライアント設置は未定。

られており、ユーザからは、あたかも単一の（パーティションの区切りがない）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。

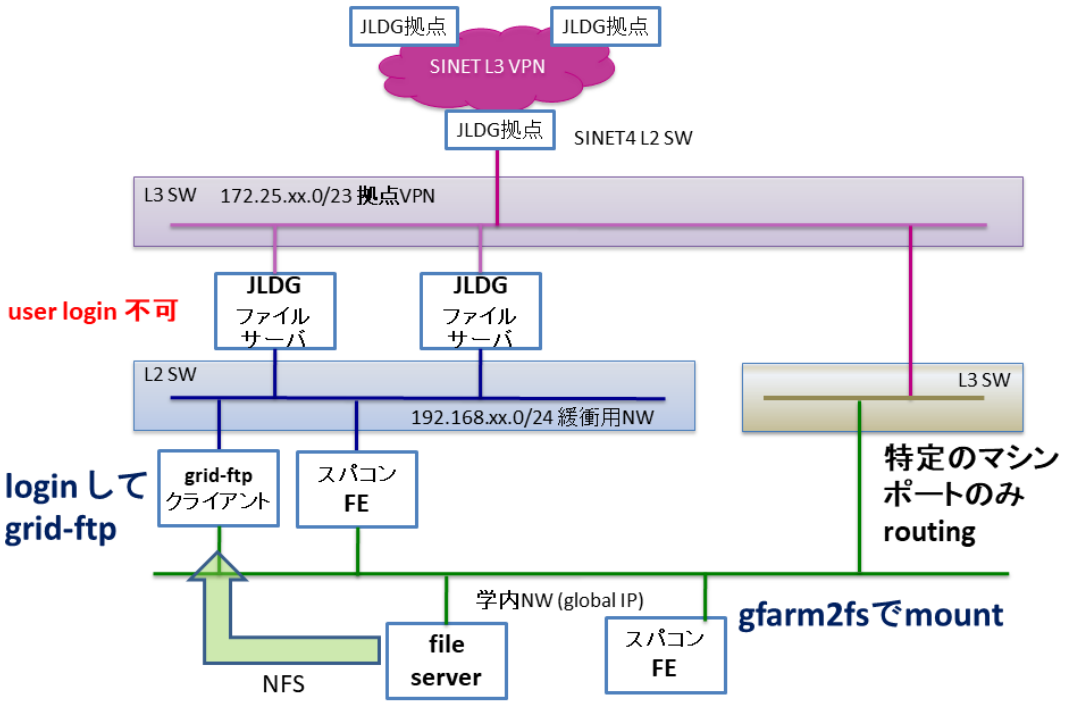

図 2: 各拠点のネットワーク概念図

各拠点にはクライアントが設置されています (図 2)。クライアントは、

- その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 マウントしている
- その拠点のスーパーコンピュータのフロントエンドである
- その拠点のデータ解析用ワークステーションである

のいずれかです。ユーザはクライアント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。拠点によっては、JLDG ファイルシステムをマウントし、あたかも通常のファイルシステムであるかの様に使用できる環境を提供しています。

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等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、それを任意の拠点の任意のクライアントから取り出し、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 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。

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 ID とは独立の『ユーザ証明書』を用いて行います。ユーザ証明書は 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、OSG (Open Science 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。

JLDG は、2012 年に開始された HPCI (High Performance Computing Infrastructure) (https://www.hpci-office.jp/) が提供する HPCI 共用ストレージとの連携システムも提供しています。別途提供されている手引きを参照して下さい。

1.3 利用資格

JLDG は国内の格子 QCD 及び関連分野の研究者と、国内の研究グループに属し JLDG のグループ管理者の許可を得た研究者（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。
幾つかのグループには、研究・利用形態に則して、小グループが組織されています[2]。

ユーザは、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の何れかのユーザアカウントが必要です[3]。通常利用する（最もよく利用する）クライアントを管理する拠点を、ユーザの所属サイトと呼びます。

従って、JLDG を利用するユーザは、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。

[2]新たな研究グループ･小グループの作成を希望される場合は、JLDG 仮想組織管理者 voadmin[AT]jldg.org に相談下さい。
[3]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、クライアントのいずれにもアカウントを持つ必要はありません。

グループ名	グループの説明
pacscs	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。
kek	高エネルギー加速器研究機構を拠点とするユーザの研究用。
rcnp	大阪大学核物理研究センターを拠点とするユーザの研究用。
kmi	名古屋大学素粒子宇宙起源研究機構を拠点としていたユーザの研究用。
npftqcd	npftqcd グループの研究用。
wmfqcd	wmfqcd グループの研究用。
yitp	京都大学基礎物理学研究所を拠点とするユーザの研究用。
riken	理化学研究所仁科加速器科学研究センターを拠点とするユーザの研究用。
astrosnx	超新星爆発シミュレーションを研究するユーザの研究用。
jldg	一般公開データへのアクセスだけを必要とするユーザ用。
public	一般公開用データ (ILDG 用等) を作製する為のグループ。 一般ユーザは所属できない。

表 1: JLDG のグループ

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
- グループ内データ共有

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 SINET5 of NII.

等の謝辞を含めて下さい。また、JLDG web page https://www.jldg.org/ にて成果リストを公開しておりますので、新たに成果を公開した際は、report[AT]jldg.org までご報告下さい。JLDG を今後も維持・発展させていく為には、JLDG の有用性をアピールすることが不可欠ですので、ご協力宜しくお願い致します。

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 等）を定め、JLDG web page https://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 グループ内データ共有

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[4]。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）が可能です。さらに、特定のユーザ・グループを指定してアクセス許可を設定することもできます。

グループ内に小グループがある場合、小グループのトップディレクトリは次の通りです。

`/gfarm/グループ名/小グループ名/`

2 利用開始までの流れ

2.1 証明書発行の為のアカウント取得

JLDG ファイルシステムにアクセスするには、ユーザ証明書を発行できるクライアントにアカウントが必要です。表 2 を参照し、管理者にアカウントを申請して下さい。各拠点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、管理者からアカウントが発行されます。所属サイト（JLDG を最もよく利用する拠点）のクライアントで証明書を発行するのが望ましいですが、他の拠点で証明書を発行しても構いません。

2.2 グループ責任者への連絡

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責任者（表 3）に、以下の情報をお知らせ下さい。

- 氏名 (漢字氏名、及びローマ字綴り)
- 所属 (研究機関名)
- 所属機関住所
- 電話番号 (オフィス等)
- e-mail アドレス
- 所属サイト名
- 所属グループ名
- 証明書を発行する拠点名と、証明書を発行するクライアント上のアカウント名

[4]設定は変更可能です。グループの責任者から voadmin[AT]jldg.org 宛、連絡下さい。

拠点	管理者	クライアント
筑波	吉江友照 yoshie[AT]ccs.tsukuba.ac.jp 大野浩史 hohno[AT]ccs.tsukuba.ac.jp	flare25.ccs.tsukuba.ac.jp cygnus.ccs.tsukuba.ac.jp (詳細は『筑波大 Cygnus での JLDG 利用: 規定・手順』参照。証明書の発行は不可)
KEK	松古栄夫 hideo.matsufuru[AT]kek.jp	jldgfe01, jldgfe02 (KEKSC ネットワーク内, VPN 経由)
大阪	外川浩章 togawa[AT]rcnp.osaka-u.ac.jp 石井理修 ishiin[AT]rcnp.osaka-u.ac.jp 土居孝寛 takahiro.doi[AT]rcnp.osaka-u.ac.jp	front01, front04 （ログインサーバ経由で利用） (詳細は、『RCNP サイトでの JLDG 利用マニュアル』参照)
広島	石川健一 ishikawa[AT]theo.phys.sci.hiroshima-u.ac.jp	theohpc.phys.sci.hiroshima-u.ac.jp
京都	青木慎也 saoki[AT]yukawa.kyoto-u.ac.jp	jldg-yitpin (login ゲートから login）
理研 (和光)	土井琢身 doi[AT]ribf.riken.jp	jldgfe (仁科 NW 上)
理研 (神戸)	中村宣文 nakamura[AT]riken.jp	クラウドストレージゲートウェイ: csgw1, csgw2 (詳細は、『富岳での JLDG 利用マニュアル』参照。証明書の発行は不可)

表 2: 各拠点の管理者とクライアント

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。

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。

2.3 ライセンス ID の取得

グループの責任者（jldg グループの場合は所属サイトの管理者）は、当該ユーザがグループのメンバーであること（jldg グループの場合、所属サイトのユーザであること）を確認した後、ユーザからの登録情報を 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 のユーザ証明書を発行する際に必要になる一回限りの ID で、次の様な大文字のアルファベットと数字の列です。

```
JLDG-CJN4SP-7O458F-1FOZYK
```

グループ	責任者
pacscs	吉江友照 (yoshie[AT]ccs.tsukuba.ac.jp) 大野浩史 (hohno[AT]ccs.tsukuba.ac.jp)
jlqcd kek	松古栄夫 (hideo.matsufuru[AT]kek.jp)
rcnp	外川浩章, 石井理修, 土居孝寛 申請先 Email: apply-jldg[AT]rcnp.osaka-u.ac.jp
kmi	青木保道 (yasumichi.aoki@riken.jp)
npftqcd	駒佳明 (koma[AT]numazu-ct.ac.jp)
wmfqcd	吉江友照 (yoshie[AT]ccs.tsukuba.ac.jp)
yitp	青木慎也 (saoki[AT]yukawa.kyoto-u.ac.jp)
riken	土井琢身 (doi[AT]ribf.riken.jp)
astrosnx	住吉光介 (sumi[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: 各グループの責任者等

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

2.4 ユーザ証明書の取得

ユーザ証明書取得の作業は、証明書が発行可能なクライアント（表 2）上で行います。

ユーザ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 のユーザ証明書のサブジェクトは以下のいずれか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
/C=JP/O=Japan Lattice Data Grid/OU=所属グループ名/CN=フルネーム
/C=JP/O=JLDG3/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
/C=JP/O=Japan Lattice Data Grid/OU=jldg/CN=Ichiro Suzuki
/C=JP/O=JLDG3/OU=jldg/CN=Ichiro Suzuki
```

です。

ユーザ証明書を取得する為に `jldg-user-req.sh` を実行して下さい。

(実行例: 表示されるグループ名・番号、証明書の Organization 名 (O=...) は以下と異なる場合があります)

```
$ /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
7) kmi
8) wmfqcd
9) astrosnx
10) yitp
11) riken
12) kek
Input group number : 1          ←グループ名を選択
Please input your full name...
Ex). John Smith : Ichiro Suzuki ←ユーザ名を入力 (この様にフルネームで)
------You are requesting below content ------
"C=JP/O=JLDG3/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-CJN4SP-7O458F-1FOZYK ←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 user subject information --------
* email can be omitted by putting a char of '.'

------- please confirm your inputs ------------
GROUP   : JLDG user
SUBJECT : OU=jldg, CN=Ichiro Suzuki

trying to connect RA server : voms.jldg.org (11412) ... ok.
request for issuing a new certificate ... ok.
save a CA certificate file : /home/LATTICE/suzuki/.globus/ca-22655.cer
save a certificate file : /home/LATTICE/suzuki/.globus/usercert.pem
save a private key file : /home/LATTICE/suzuki/.globus/userkey.pem
Input PASS Phrase:              ←証明書のパスフレーズを設定 (忘れない様に)
Verifying - Input PASS Phrase:  ←チェックの為、再度パスフレーズを入力
The following files are generated:
-rw-r--r-- 1 yoshie LATTICE 1265 Jun  2 04:31 /home/LATTICE/suzuki/.globus/e2e582ef.0
-rw-r--r-- 1 yoshie LATTICE 1123 Jun  2 04:31 /home/LATTICE/suzuki/.globus/usercert.pem
-rw------- 1 yoshie LATTICE  963 Jun  2 04:33 /home/LATTICE/suzuki/.globus/userkey.pem
---------- 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 (e2e582ef.0 又は 32d10593.0)

2.5 証明書の管理とコピー

発行されたユーザの証明書（ユーザ秘密鍵）は、他人に見られない様に厳重に管理して下さい。因みに、証明書関係のファイル・ディレクトリのパーミッションは、

```
jldg-fr3[113]% ls -ld .globus
drwx------ 2 suzuki LATTICE 60 Jun  2 04:33 .globus/
jldg-fr3[114]% ls -l .globus
total 12
-rw-r--r-- 1 suzuki LATTICE 1265 Jun  2 04:31 e2e582ef.0
-rw-r--r-- 1 suzuki LATTICE 1123 Jun  2 04:31 usercert.pem
-rw------- 1 suzuki LATTICE  963 Jun  2 04:33 userkey.pem
```

となっています。これを変更しないで下さい。（変更すると、JLDG 関係のコマンドが動作しない場合があります。）

JLDG を複数のクライアントから使用する為には、ユーザ証明書を、証明書を発行したクライアントから別のクライアントにコピーする必要があります。安全な方法 (scp を使用する等）でコピーして下さい。その際、コピー先のファイル・ディレクトリのパーミッションが上記の通りになる様にして下さい。

2.6 JLDG 仮想組織への登録

JLDG ではユーザ情報を『JLDG 仮想組織』に登録し、所属するグループやメールリストの管理に利用しています。仮想組織への登録は、 1) JLDG ユーザ証明書をブラウザにインポートし、2) JLDG 仮想組織管理サーバにアクセスして必要事項を入力し、3) Email address の確認と 4) 仮想組織管理者の作業を経て、完了します。

2.6.1 ユーザ証明書のブラウザへのインポート

発行済みのユーザ証明書の形式を pem から PKCS12 に変換します。証明書を発行したクライアントの証明書を格納したディレクトリ (通常 ~/.globus) で、

```
$ openssl pkcs12 -export -in 証明書 -inkey 秘密鍵 -out PKCS12 形式のファイル名
```

を実行して下さい。

具体例:

```
$ cd ~/.globus
$ openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out usercert.p12
Enter pass phrase for userkey.pem: ←ユーザ証明書取得時の pass phrase
Enter Export Password:             ← PKCS12 形式のパスワード
Verifying - Enter Export Password: ←確認の為、再入力。
```

PKCS12 形式の証明書 usercert.p12 は秘密鍵が含まれていますので、漏洩しない様に管理して下さい。

仮想組織管理サーバへは、各拠点の『JLDG クライアントネットワーク』内の IP アドレスからのみ、アクセス可能です。JLDG クライアントでのブラウザの利用に不都合がある場合、ユーザ個人で、条件を満たすブラウザを準備して下さい。『クライアントネットワーク』とブラウザ準備に関する Tips は Appendix B を参照下さい。

必要に応じて、PKCS12 形式の証明書をブラウザが稼働している端末にコピーし、インポートします。証明書インポートの手順の詳細は、ブラウザの種類やバージョンによって異なりますので、詳細はブラウザのマニュアル等を参照して下さい。

Internet Explorer

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、「コンテンツ」「証明書」の順にクリックします。
2. 証明書ウィンドウが表示されるので、「インポート」を選択すると、「証明書のインポートウィザード」が起動します。「次へ」をクリックします。
3. 「参照」をクリックし、「usercert.p12」を選択し、「次へ」をクリックします。PKCS12 形式のファイルが表示されない場合は、選択メニューで「Personal Information Exchange」 か、「すべてのファイル」に切り替えます。
4. PKCS12 形式変換時に設定したパスワードを入力します。
5. 「次へ」→「次へ」→「完了」とクリックしていきます。
6. 「正しくインポートされました」と表示されるので「OK」をクリックします。終了です。
7. 「個人」の証明書欄に、『発行先:お名前 (証明書の DN)、発行者: JLDG3 CA』の証明書が表示されている事を確認して下さい。

Firefox

1. 「アプリケーションメニューを開きます」ボタンから「設定」、「プライバシーとセキュリティ」メニュー内の、「セキュリティー」:「証明書」の項目内の『証明書の表示』をクリックします。

2. 証明書マネージャが開くので、「あなたの証明書」が選択されていることを確認し、「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. 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. 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。

Google Chrome

1. 「Google Chrome の設定」ボタンから「設定」を選択、「プライバシーとセキュリティ」メニュー内の、「セキュリティー」を開きます。

2. 「セーフブラウジング」項目内の『証明書の管理』をクリックします。

3. 証明書ウィンドウが表示されるので、「インポート」を選択すると、「証明書のインポートウィザード」が起動します。「次へ」をクリックします。

4. 「参照」をクリックし、「usercert.p12」を選択し、「次へ」をクリックします。PKCS12 形式のファイルが表示されない場合は、選択メニューで「Personal Information Exchange」 か、「すべてのファイル」に切り替えます。

5. PKCS12 形式変換時に設定したパスワードを入力します。

6. 「次へ」→「次へ」→「完了」とクリックしていきます。

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

8. 「個人」の証明書欄に、『発行先:お名前 (証明書の DN)、発行者: JLDG3 CA』の証明書が表示されている事を確認して下さい。

2.6.2 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下さい。

1. 証明書を読み込んだブラウザで、次の URL にをアクセスします。

   `https://vomsrv7.jldg.org:8443/voms/jldg`

   認証の為、個人証明書の選択（または確認）が求められますので、前節でインポートした証明書を提示して下さい。また、セキュリティー証明書関係の警告が出た場合は、「原因がユーザ側ブラウザの設定にあり、安全性（暗号化）に問題がない」と確信できる場合は、「一時的に証明書を受け入れる」等を選び、接続を試みても結構です[5]。「voms admin for jldg」 という表題の登録ページが表示されます。

2. このページの内容を熟読の上、各項目を記入して下さい。最下部の「Message for VO Administrator」の項を除く、全項目に記入が必要です。Email address 欄には、メールが受信できるだけでなく、送信もできるアドレスを記入して下さい。

3. 「Submit」ボタンをクリックして下さい。 入力内容に問題がない場合、Confirmation required 云々と書かれたページが表示されます。

4. 本人確認の為、上記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“ request by going to the following url: ”のページにアクセスすると本人確認が終了します。

5. その後、JLDG 仮想組織管理者の作業が行われます。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。仮想組織管理者の作業は、原則、平日（月–金）9:00-17:00 に行います。受付時間によっては、当日作業できない場合があります。

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。

2.6.3 情報の更新

仮想組織管理サーバに登録している事項に変更が生じた場合は、その都度、登録内容を更新して下さい。

1. 証明書をインポートしたブラウザで、`https://vomsrv7.jldg.org:8443/voms/jldg` にアクセスします。必要に応じて証明書の選択・確認を行います。

2. 表示された登録情報を更新し、項目 Email: の下の「Change personal Information」をクリックします。

[5] JLDG 側の設定に疑義がある場合は、拠点の管理者に連絡下さい。

3　利用法

JLDG では、二通りの利用法を提供しています。

- uberftp という grid-ftp ソフトを使って、JLDG に (から) ファイルをアップロード (ダウンロード) する方法。gfarm コマンドを用いて、ファイルやディレクトリを操作 (linux の ls や mv 等に相当する操作) することも可能です。
- JLDG ファイルシステムをクライアントの自分のディレクトリにマウントし、通常の linux (unix) コマンドでファイルを操作する方法。

拠点やクライアントによって、提供する機能が異なります。詳細は、Appendix A を参照して下さい。

どちらの方法で利用する時も、GSI 認証用の代理証明書の作成が必要です。

3.1　代理証明書の作成

まず、"`grid-proxy-init`" command を使って、GSI 認証用[6]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
Enter GRID pass phrase for this identity:
    ← 証明書作成時に入力したパスフレーズを入力します。
```

一部のクライアントでは、代理証明書の鍵長指定のオプション "`-bits 1024`" を付ける必要があります。どのクライアントでこのオプションが必要かは、付録 A を参照して下さい。

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。

  (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
  ```

[6]GSI: Grid Security Infrastracture の略

代理証明書は、/tmp/x509up_u<uid>というファイルに格納されます。これを読み出して、代理証明書の各種情報（有効期限等）を表示するには、

```
$ grid-proxy-info
```

を使います。

一部のクライアントには、代理証明書を自動更新する grid-proxy-agent が用意されています。

```
$ grid-proxy-agent
Enter your pass phrase: パスフレーズを入力
```

3.2 uberftp による利用

拠点のクライアントから uberftp という grid-ftp ソフトウエアを用いて、その拠点のグリッド ftp サーバに接続して利用します。各拠点のグリッド ftp サーバは、Appendix A を参照して下さい。以下の例では、グリッド ftp サーバを gftpserv と書きます。

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 等に書いておくと便利です。）

1. uberftp を起動します。

   ```
   $ uberftp gftpserv
   220 gftpserv GridFTP Server 3.41 (gcc64, 1330711604-80) ....
   230 User nobody logged in.
   UberFTP>
   ```

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、/ です。**)

   ```
   UberFTP> cd /gfarm/<グループ名>
   ```

3. “help” command で uberftp の command の概略を見られます。command は ftp とよく似ていますので、ftp を使った経験がある方は、とまどうことなく使えると思います。より詳しい情報は、次の URL を参照して下さい。

   ```
   https://github.com/gridcf/UberFTP
   ```

以下に、クライアントの current directory の Sample という directory 以下を、recursive に、JLDG の mygroup グループの SGROUP 小グループのトップディレクトリにコピーする例を示します。

```
$ uberftp gftpserv
220 gftpserv GridFTP Server 3.41 (gcc64, 1330711604-80) ...
230 User nobody logged in.
UberFTP> cd /gfarm/mygroup/SGROUP      ←小グループのトップ
UberFTP> put -r Sample                 ←recursive option を付けて put
Sample/RC32x48-005300: 905970592 bytes in 7.732109 Seconds (111.742 MB/s)
Sample/RC32x48-005310: 905970592 bytes in 7.688954 Seconds (112.369 MB/s)
Sample/RC32x48-005320: 905970592 bytes in 7.689116 Seconds (112.367 MB/s)
....
Sample/RC32x48-005390: 905970592 bytes in 11.065409 Seconds (78.081 MB/s)
UberFTP> ls Sample                     ←ls で表示
drwxrwxr-x 32000 suzuki89   mygroup            0 Jun  5 16:56 .
drwxr-x--- 32000 suzuki89   mygroup            0 Jun  5 16:55 ..
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 16:55 RC32x48-005300
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 16:55 RC32x48-005310
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 16:55 RC32x48-005320
....
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 16:56 RC32x48-005390
UberFTP> bye
221 Goodbye.
```

ls で表示されるユーザ名 (上の例では suzuki89) は、gfarm でユーザを識別するグローバル名です。これについては、”gfarm command” の項で解説します。

uberftp は、非対話的に使うこともできます。以下は、mygroup グループの直下に Sample というディレクトリを作成し、クライアントのカレントディレクトリ内の全てのファイルを、そこにコピーする例です。各コマンドの意味は、`uberftp -help` で参照して下さい。uberftp を非対話的に使うと、複雑なファイル操作を shell script に記述し、それをバックグラウンドで実行する、といった事ができます。

```
% uberftp -mkdir gsiftp://gftpserv/gfarm/mygroup/Sample
% foreach file (*)
foreach? uberftp file:$file gsiftp://gftpserv/gfarm/mygroup/Sample/$file
foreach? end
% uberftp -ls gsiftp://gftpserv/gfarm/mygroup/Sample
drwxrwxr-x 32000 suzuki89   mygroup            0 Jun  5 17:31 .
drwxrwx--- 32000 gfarmadm   mygroup            0 Jun  5 17:29 ..
```

```
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 17:30 RC32x48-005300
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 17:30 RC32x48-005310
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 17:30 RC32x48-005320
....
-rw-rw-r--   1 suzuki89   mygroup    905970592 Jun  5 17:31 RC32x48-005390
% uberftp -rm -r gsiftp://gftpserv/gfarm/mygroup/Sample
% uberftp -ls gsiftp://gftpserv/gfarm/mygroup/Sample
No match for /gfarm/mygroup/Sample
```

3.3 Gfarm コマンド

クライアントでは、uberftp で grid-ftp server に接続せずに、Gfarm コマンドを使用することができます。まず、Appendix A を参照して、パスの設定をして下さい。Gfarm コマンドを利用するには、”grid-proxi-init ” コマンドで生成した有効期限内の代理証明書が必要です。

表 4 に利用可能な Gfarm コマンドの一覧があります。ほとんどのコマンドにはマニュアルページがありますので、詳細はそちらを参照して下さい。ファイルの実体を操作することはできませんが、ファイルの mv (move)、ディレクトリの作成、パーミッションの変更といった、ファイルのメタデータの操作は、ほとんど Gfarm コマンドで行う事ができます。コマンド名は、対応する linux のコマンドの先頭に gf を付けたもの (ex. ls → gfls) が多く、よく似ています。但し、

ファイル・ディレクトリは、JLDG ファイルシステムの絶対パスで指定

しなければなりません。

以下に、特定のディレクトリのリストを表示し、ファイルのパーミッションを変更する例を示します。

```
% gfls -l /gfarm/mygroup/SGROUP/Sample
-rw-rw-r-- 1 suzuki89   mygroup    905970592 Jun  6 13:08 RC32x48-005300
-rw-rw-r-- 1 suzuki89   mygroup    905970592 Jun  6 13:08 RC32x48-005310
-rw-rw-r-- 1 suzuki89   mygroup    905970592 Jun  6 13:09 RC32x48-005320
....
-rw-rw-r-- 1 suzuki89   mygroup    905970592 Jun  6 13:09 RC32x48-005380
-rw-rw-r-- 1 suzuki89   mygroup    905970592 Jun  6 13:10 RC32x48-005390
% gfchmod 644 '/gfarm/mygroup/SGROUP/Sample/*'
% gfls -l /gfarm/mygroup/SGROUP/Sample
-rw-r--r-- 1 suzuki89   mygroup    905970592 Jun  6 13:08 RC32x48-005300
-rw-r--r-- 1 suzuki89   mygroup    905970592 Jun  6 13:08 RC32x48-005310
```

```
-rw-r--r-- 1 suzuki89   mygroup    905970592 Jun  6 13:09 RC32x48-005320
....
-rw-r--r-- 1 suzuki89   mygroup    905970592 Jun  6 13:09 RC32x48-005380
-rw-r--r-- 1 suzuki89   mygroup    905970592 Jun  6 13:10 RC32x48-005390
```

ワイルドカードを使う場合は、クライアントの shell に解釈されない様、エスケープして下さい。（上の gfchmod の引数の様に。）

Gfarm コマンド名	動作内容
gfarm.arch.guess	アーキテクチャ名を表示
gfchgrp	chgrp
gfchmod	chmod
gfchown	chown
gfdf	df
gfedquota	edquota
gfgroup	グループ名表示
gfhost	ホスト名表示，-M オプションのみ
gfkey	秘密鍵操作
gfln	ln
gfls	ls
gfmkdir	mkdir
gfmv	mv
gfquota	quota
gfquotacheck	quotacheck
gfrm	rm
gfrmdir	rmdir
gfstat	stat
gfstatus	状態表示
gfusage	利用状況表示
gfuser	ユーザ名表示
gfwhere	ファイル所在表示
gfwhoami	グローバル名表示
gfxattr	拡張属性操作

表 4: Gfarm コマンド一覧

Gfarm 特有のコマンドや、Gfarm 特有の情報を表示するコマンドがあります。以下に、普段の利用に有用なコマンドを紹介します。

gfwhoami: グローバルユーザ名を表示します。
Gfarm では、ユーザを" グローバルユーザ名" で管理しています。グローバルユーザ名は、メールアドレスの@以降を除いた個人を識別するユーザ名に何桁かの数字を付加したものになっています。uberftp の ls や gfls で表示されるユーザ名です。

```
% gfwhoami
suzuki89
```

ご自身のグローバルユーザ名を覚えていて下さい。JLDG では、グローバルユーザ名とユーザ証明書の組で仮想組織を管理しています。

```
% gfwhoami -v
suzuki89 /C=JP/O=JLDG3/OU=mygroup/CN=Ichiro Suzuki
```

gfusage: 現在の JLDG の使用状況を表示します。

```
% gfusage
#   UserName :       FileSpace     FileNum   PhysicalSpace PhysicalNum
    suzuki89 :   2456721043020      366992   5375933759291      887566
```

Gfarm では、ファイルの複製を作ることができます。JLDG では、ファイルの生成時に(put 時に)、自動的に、ひとつのサーバにオリジナルを、別のサーバに複製をつくる設定で運用しています。FileSpace, FileNum は、カタログ上の値を、PhysicalSpace PhysicalNum は、複製を含めた実数を表します。

gfwhere: ファイルが置かれている gfarm server を表示します。

```
% gfwhere -r /gfarm/mygroup/SGROUP/Sample
/gfarm/mygroup/SGROUP/Sample/RC32x48-005300:
jldg-fs6-sc jldg-fs10-sc

/gfarm/mygroup/SGROUP/Sample/RC32x48-005310:
jldgnagfs1-s jldg-fs10-sc
.....
/gfarm/mygroup/SGROUP/Sample/RC32x48-005340:
scjldgkek06 jldg-fs10-sc

/gfarm/mygroup/SGROUP/Sample/RC32x48-005350:
hn-oss46 jldg-fs10-sc
....
/gfarm/mygroup/SGROUP/Sample/RC32x48-005390:
jldghu02 jldg-fs10-sc
```

ホスト名の命名規則は、現在、筑波 (jldg-fs*-sc), KEK(scjldgkek*), 大阪 (rcnp-gf-*-ss), 広島 (jldghu*), 理研和光 (jldgriken*-sc), 理研神戸 (jldgkobe*)、東大 (jldgut*-sc) としています。

gfdf: Gfarm ファイルシステムのディスク使用状況を表示します。

```
% gfdf -H
1K-blocks   Used  Avail Use% Host
     235T  18.9T   216T   8% hn-oss45
     235T  19.6T   215T   8% hn-oss46
     114T   2.7T   111T   2% jldg-fs10-sc
    37.0T  37.0T      0 100% jldg-fs4-sc
    37.0T  37.0T   123M 100% jldg-fs5-sc
     126T  70.4T  55.6T  56% jldg-fs6-sc
     109T  48.3T  60.7T  44% jldg-fs7-sc
     100T  43.9T  56.1T  44% jldg-fs8-sc
     114T  66.4T  47.4T  58% jldg-fs9-sc
     114T  17.5T  96.3T  15% jldghu02
     114T  17.9T  95.9T  16% jldghu03
     153T  23.5T   129T  15% jldgnagfs0-s
     153T  20.8T   132T  14% jldgnagfs1-s
     7.0T   7.0T   1.0M 100% knzjldgs
     7.0T   7.0T      0 100% rcnp-gf-ss
     7.0T   7.0T      0 100% scjldgkek01
    54.0T  32.5T  21.5T  60% scjldgkek02
     261T  18.9T   242T   7% scjldgkek05
     261T  15.5T   245T   6% scjldgkek06
----------------------------
     2.2P   512T   1.7P  23%
```

3.4 JLDG ファイルシステムのマウント

クライアントで JLDG をマウントして利用できます。この機能を提供している拠点・クライアントについては、Appendix A を参照して下さい。

利用手順は、代理証明書を作成した後、

```
% mkdir /tmp/suzuki     ←マウントポイントを作成 (なければ)
% gfarm2fs /tmp/suzuki ←マウントする
% ls /tmp/suzuki        ←マウントポイントが JLDG の root directory です。
gfarm/home/  lost+found/  stress/  tmp/
```

```
% cd /tmp/suzuki/gfarm/mygroup/SGROUP/Sample/ ←任意のコマンド
% ls -l                                       ←任意のコマンド
total 8847370
-rw-r--r-- 1 suzuki 70001 905970592 Jun  6 13:08 RC32x48-005300
-rw-r--r-- 1 suzuki 70001 905970592 Jun  6 13:09 RC32x48-005370
-rw-r--r-- 1 suzuki 70001 905970592 Jun  6 13:09 RC32x48-005380
....
-rw-r--r-- 1 suzuki 70001 905970592 Jun  6 13:10 RC32x48-005390
% cp RC32x48-005390 ~/        ← cp も普通にできます
% cd                           ← JLDG の外にでる
% fusermount -u /tmp/suzuki   ←アンマウントする
```

です。上記の例の様に、ls 等で表示されるユーザ名はクライアント上のアカウント名です。また、マウントポイントは、local file system 上に作成して下さい。NFS マウントされた file system 上にマウントすると、不具合が生じる可能性があります。

JLDG をマウント利用している場合、Gfarm コマンドの引数に、相対パスを指定する事ができます。

```
% cd /tmp/suzuki/gfarm/mygroup/SGROUP/Sample/
% gfwhere RC32x48-005390
jldghu02 jldg-fs10-sc
```

3.4.1 データのコピー

クライアントのローカルな（または NFS マウントされた）ファイルシステムと、JLDG ファイルシステムの間で、高速にデータをコピーすることができる並列コピーコマンド gfpcopy が用意されています。以下に、カレントディレクトリ（ローカルなファイルシステム）直下にあるディレクトリ以下をリカーシブに、ディレクトリ構造を保ったまま、JLDG ファイルシステムに並列コピーする例を示します。

```
% pwd                                  ←ローカルなファイルシステムにいます
/home/LATTICE/suzuki/TestDir
% ls                                   ←カレントディレクトリの ls
DataDir/  Sample2/
% ls /tmp/suzuki/gfarm/mygroup/SGROUP  ← Gfarm ファイルシステムを
Sample/                                    /tmp/suzuki にマウントしています。

% gfpcopy -p Sample2 /tmp/suzuki/gfarm/mygroup/SGROUP ←Sample2 以下をコピー

all_entries_num: 10
```

```
copied_file_num: 10
copied_file_size: 9059705920            ←コピー終了時のメッセージです
total_throughput: 26.375856 MB/s
total_time: 343.484817 sec.

% ls /tmp/suzuki/gfarm/mygroup/SGROUP/Sample2   ←コピーされました
RC32x48-005300RC32x48-005320RC32x48-005340RC32x48-005360RC32x48-005380
RC32x48-005310RC32x48-005330RC32x48-005350RC32x48-005370RC32x48-005390
```

上の例のコマンドオプションの -p は、コピー終了時に統計情報を表示させるオプションです。その他、並列度を指定する -j オプション等があります。詳細は man page をご覧下さい。

gfpcopy は、JLDG をマウントすることなく使う事もできます。その際は、

```
% gfpcopy -p Sample3 gfarm:///gfarm/mygroup/SGROUP
% gfls /gfarm/mygroup/SGROUP
Sample  Sample2 Sample3
```

の様に、url (gfarm:///... や file:///...) を指定します。

3.4.2 ファイルの複製について

JLDG では、ファイルのアップロード時にオリジナルとその複製を自動的に作成します。複製はオリジナルとは別のサーバに作られます。

ファイルの自動複製作成数は gfncopy コマンドで管理することができます。以下の様にオプションを付けない場合、現在設定されている自動複製作成数を表示します。

```
% gfncopy /gfarm/mygroup/SGROUP/Sample
3
```

また、-s オプションを付けることで、自動複製作成数を変更できます。以下に、自動複製作成数を 2 にする例を示します。

```
% gfncopy -s 2 /gfarm/mygroup/SGROUP/Sample
```

その他、詳細は man page をご覧下さい。

この様に、JLDG をマウントして利用できる環境では、ユーザ自身で複製を管理する事ができますが、大量のデータの複製を 3 つ以上作成すること（つまり、オリジナルと自動的に作成される複製以外に複製をつくること）は避けて下さい。

3.5 証明書の失効と再発行

JLDG ユーザ証明書は、種々の理由で失効します。本節では、失効する理由と証明書の再発行の手続きを案内します。証明書の再発行には、以下の情報が必要になります。

- 仮想組織に登録の Email address
  ユーザ本人からの依頼である事を確認する為、JLDG 管理者グループ宛ての Email は、仮想組織管理サーバに登録の Email address から送信して下さい。JLDG ユーザへのアナウンスを受信している address が登録アドレスです。ユーザ宛のアナウンスメールが一定回数配信エラーになると、アナウンスの配送が停止されます。その場合も、仮想組織管理サーバにアクセスして登録している Email address を確認することができます。異動等によって、登録 Email address からのメール送信ができず、仮想組織管理サーバへのアクセスもできない場合は、所属グループの管理者に『所属拠点と登録 Email address、勤務先住所 (ローマ字)、勤務先電話番号』の変更を依頼して下さい。所属グループの管理者による本人確認と、仮想組織管理グループによる登録情報の変更後、新 Email address 宛て『登情報変更済み』旨、連絡します。

- 失効した（あるいは、間もなく失効する）証明書のサブジェクト
  証明書のサブジェクトは、次のどちらかのコマンドで確認できます。

  ```
  % grid-cert-info [ -file ~/.globus/usercert.pem ] -s
  % openssl x509 -in ~/.globus/usercert.pem -noout -subject
  ```

  `[...]` は省略可。証明書の標準パス `~/.globus/usercert.pem` は適宜変更下さい。

  JLDG には、発行時期により 3 種類のサブジェクトのユーザ証明書があります。

  1. (第 1 世代) 2007〜2013 年 12 月 (現在無効)

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

  2. (第 2 世代) 2013 年 12 月〜2021 年 3 月 (現在無効)

     `/C=JP/O=Japan Lattice Data Grid/OU=`所属グループ`/CN=`ユーザフルネーム

  3. (第 3 世代) 2021 年 3 月〜

     `/C=JP/O=JLDG3/OU=`所属グループ`/CN=`ユーザフルネーム

- 証明書の有効期限

```
% grid-cert-info [ -file ~/.globus/usercert.pem ] -ed
% openssl x509 -in ~/.globus/usercert.pem -noout -enddate
```

3.5.1 有効期限が経過した場合

ユーザ証明書は発行時から 3 年間有効です。有効期限後も JLDG の継続利用を希望する場合は、以下の手順で更新して下さい。有効期限前に更新する事も可能です。(新証明書の有効期限は、新証明書発行時点から 3 年です。現証明書の有効期限が 1 カ月を切るころを目安に、更新する事を推奨します。)

1. 登録されているメールアドレスから、仮想組織管理者 voadmin[AT]jldg.org 宛、現証明書のサブジェクトを添えて、ライセンス ID の発行を依頼して下さい。

2. 現証明書を別所に保管 (eg. `mv ~/.globus ~/.globus-back`) した後、証明書の新規発行と同じ手順 (2.4 節参照) で証明書を発行して下さい。その際、所属グループ、ユーザフルネームは現証明書と同じにして下さい。第 3 世代の証明書が発行されます。

3. 失効する（した）現在の証明書が第 3 世代のものであれば、新証明書のサブジェクトは、現証明書のそれと同一です。この場合、手続きは完了です。新証明書で JLDG をお使い下さい。

4. 現証明書が第 2 世代のもの (`/C=JP/O=Japan Lattice...`) の場合、同じサブジェクトでの利用継続は出来ません。以下のどちらかの方法で、新証明書を仮想組織に登録して下さい。

   - 本手引き 2.6 節の手順で、新証明書をブラウザにインポートし、新規ユーザとして仮想組織に登録する。その際、氏名・所属等の個人情報を再入力すると共に、登録フォームの下部にある「Message for VO administrator」欄に、失効する現証明書のサブジェクトを記入して下さい。

   - 現証明書をインポートしてあるブラウザで仮想組織管理サーバにアクセスします。入力済の個人情報を確認・修正した後、「Certiicates」欄の 「Add an additional certificate」をクリックします。pem 形式の新証明書（あらかじめブラウザから参照できるファイルシステムにコピーしておく）を選択して、「Request cetificate」をクリック。

5. どちらの場合も、仮想組織管理者が確認し、問題が無ければ承認します。あわせて、gfarm の global name と証明書サブジェクトの紐付けを変更します。承認後の最初の午前 4 時以降、新証明書が有効になります。既存の JLDG ファイルシステム内のファイル等はアクセス制御情報を含めて変更されません。

3.5.2 ユーザ証明書を紛失した (パスフレーズが漏洩した) 場合

ユーザ証明書が紛失し利用できなくなった場合、又は証明書パスフレーズが漏洩した（その疑いがある場合も含む）は、その旨を速やかに、グループ管理者及び仮想組織管理者に連絡して下さい。事態を放置すると JLDG ファイルシステムへの不正アクセスの原因になりますので、早急の対応をお願い致します。

1. 仮想組織管理者は、現証明書を失効させます。
2. JLDG の利用を再開したい場合は、新規ユーザ登録と同一の手順で、証明書の発行から仮想組織への登録の手続きを行ないます。
3. 新証明書のサブジェクトが現証明書のそれと異なる場合（証明書の世代が違う場合）、gfarm global name と証明書サブジェクトの紐付け変更を行なう。

3.5.3 JLDG 認証局更新による証明書世代の更新

JLDG では、システムの安定稼働やセキュリティ維持の為、認証局を再構築する場合があります。切替開始日に、旧認証局での証明書発行は停止され、新認証局の証明書の発行が開始されます。切替終了日に、旧認証局発行の証明書は全て失効させます。JLDG で使用する証明書が一斉に更新される為、証明書の世代の更新、と呼びます。ユーザの皆様は、切替開始日から終了日の間に、新証明書の発行と仮想組織への登録が必要です。

1. 切替開始日以降、仮想組織管理サーバに登録されている Email address から、仮想組織管理者 `voadmin[AT]jldg.org` 宛て、ライセンス ID 発行依頼を出します。
2. 現証明書ディレクトリ `~/.globus` を rename して、jldg-user-req.sh を実行して新証明書を発行します。
3. 現証明書（新証明書ではありません）をインポートしてあり、仮想組織管理サーバにアクセス可能な端末に、新証明書 `~/.globus/usercet.pem` を安全な方法でコピーします。
4. 仮想組織管理サーバ `vomsrv7.jldg.org:8443/voms/jldg` にアクセスし、個人情報を確認・修正し、「Certificates」欄の「Add an additional certificate」をクリックする。
5. 表示される「証明書追加」ページで、新証明書ファイルを指定し、「Request cetificate」をクリック。ページ後半の「証明書サブジェクト、CA の組を指定」の方法は使用しないこと。
6. リクエストは、仮想組織管理者に送付されます。管理者は gfarm global name と紐付ける証明書のサブジェクトを、現証明書から新証明書のそれに変更し、リクエストを承認します。

7. 承認後、最初の午前 4 時に新証明書が有効となり、現証明書では JLDG を利用できなくなります。

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、お気軽に各拠点の管理者 (表 2) までご相談下さい。

5 JLDG チームからのお願い

JLDG は、その主旨に賛同する JLDG の構成拠点や研究グループの運営費や科研費等の外部資金からの資金支援やリソースの提供を受けて構築・拡充され、拠点や研究グループの構成員がボランティアベースで運用しています。一方、その利用については、運用開始時から、『計算素粒子物理研究者であれば、所属する組織・研究グループによらずに、無審査・無制限・無料で利用できる』ものとしてきました。JLDG が十数年にわたって規模を拡大し、このコミュニティの有用なインフラとして認知される様になった大きな理由は、この運用方針・形態にあると確信しています。

この『無償・無制限』の原則は、諸刃の剣です。実際、JLDG のファイルスペースの使用率は常に高い水準にあり、毎年、かなりの規模のストレージの増強を行っているにもかかわらず、実質 100% 使用されている為、他のデータが書けない状況がしばしば発生します。JLDG は、研究データの共有の為に運用しているシステムですが、JLDG に置かれたデータが再読み込みされることなく、長期間ファイルスペースを占有している例が多々見受けられます。また、昨今、研究プロジェクトが利用できる計算機・ストレージ資源が急激に大きくなっており、JLDG をプロジェクト移行時の研究データの一時退避に利用され、新プロジェクトに引き継ぎされないデータ、引き継がれても JLDG から消去されないデータ量も大きい様です。

この様な状況は、JLDG の可用性・有用性を著しく損ね、研究機関・研究グループへの支援依頼を困難にさせ、JLDG の運用を危機にさらす事になります。JLDG の精神を生かしつつ有効活用する為にも、データの整理 (古いデータの削除、複製数の縮減、外部システムへの引き上げ) を常に心がけて頂きます様、お願い致します。

謝辞

JLDG の開発・拡張・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）
- 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」（平成２３年度～平成２７年度）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)
- 文部科学省 ポスト「京」で重点的に取り組むべき社会的・科学的課題 (重点課題)(9)「宇宙の基本法則と進化の解明」 (2015 年 2 月～2020 年 3 月)
- 計算基礎科学連携拠点（JICFuS）

A　各拠点の環境

A.1　筑波大学計算科学研究センター

A.1.1　クライアント

flare25

- JLDG 利用の為の専用クライアント、センターの基幹ファイルサーバ等を NFS マウントしている。ユーザアカウントはセンターの NIS で管理している。
- uberftp、gfarm command、mount 利用、が可能。
- gfarm command と mount 利用時のパス設定: 以下をコマンドパスに追加 `/usr/local/gfarm/bin`
- uberftp 接続先 jldg-fs27

cygnus01, cygnus02, cygnus03 (代表名 cygnus)

- cygnus のフロントエンド。
- gfarm command、mount 利用、が可能。（uberftp は利用できない）
- gfarm command と mount 利用時のパス設定: 以下をコマンドパスに追加 `/usr/local/gfarm/bin`
- HPCI 共用ストレージとの同時マウント、gsissh による single sign-on 等の機能あり。詳細は『筑波大 Cygnus での JLDG 利用: 規則・手順』参照。

A.2　高エネルギー加速器研究機構計算科学センター

A.2.1　クライアント

jldgfe01, jldgfe02

- JLDG 利用の為のクライアント。SC ネットワーク上にあり、外部からは VPN 経由でアクセスする。
- uberftp、gfarm command が可能。
- gfarm command 利用時のパス設定: 以下をコマンドパスに追加 `/usr/local/gfarm/bin`

A.2.2 グリッド ftp サーバ

- 次の 2 台: scjldg16, scjldg17

A.3 大阪大学核物理研究センター

『RCNP サイトでの 利用マニュアル』(`https://www.jldg.org/jldg/`) を参照して下さい。RCNP に設置・運用されている JLDG のクライアント及びサーバを利用するうえで必要な情報がまとめられています。

A.4 広島大学理学部物理学科

現在、サーバのみで、ユーザが直接利用する環境はありません。

A.5 東京大学情報基盤センター

現在、サーバのみで、ユーザが直接利用する環境はありません。

A.6 京都大学基礎物理学研究所

A.6.1 クライアント

jldg-yitpin

- JLDG 利用の為の専用クライアント。YITP 大規模クラスタサーバのファイルシステムを NFS マウントしている。基研ログインゲート経由でログイン可能。
- uberftp、gfarm command が可能。
- gfarm command 利用時のパス設定: 以下をコマンドパスに追加
  `/usr/local/gfarm/bin`

A.6.2 グリッド ftp サーバ

- 次の 1 台: jldgyitp

A.7 理化学研究所仁科加速器科学研究センター

A.7.1 クライアント (仁科 NW 上)

jldgfe

- JLDG 利用の為の専用クライアント。仁科 NW 上にある。
- uberftp、gfarm command が可能。
- gfarm command 利用時のパス設定: 以下をコマンドパスに追加
  `/usr/local/gfarm/bin`

A.7.2 クライアント (HOKUSAI スパコン NW 上)

jldgfe-hgw

- JLDG 利用の為の専用クライアント。理研の HOKUSAI スパコン NW 上にある。(スパコンアカウント保持者のみ利用可能)
- uberftp、gfarm command が可能。
- gfarm command 利用時のパス設定: 以下をコマンドパスに追加
  `/usr/local/gfarm/bin`

A.7.3 グリッド ftp サーバ

- 次の 4 台: jldgriken01, jldgriken02, jldgriken03, jldgriken04

A.8 理化学研究所計算科学研究センター

『富岳での JLDG 利用マニュアル』(`https://www.jldg.org/jldg/`) を参照して下さい。

B　JLDG 管理サーバへのアクセス

JLDG では、セキュリティ向上の為、管理サーバへの接続制限を行っています。本 Appendix では、JLDG 利用の際、ユーザが明示的にアクセスする必要がある管理サーバの接続制限の概要と、推奨する接続方法をまとめます。

B.1　クライアントネットワーク

管理サーバの多くは、接続元 IP アドレスをクライアントネットワーク内のアドレスに制限しています。クライアントネットワークとは、JLDG 各拠点のクライアントが JLDG の管理サーバとの通信に使用するグローバル IP アドレスを含む、IP アドレスの範囲であり、各拠点の管理者が指定しています。

拠点	ネットワーク名	IP アドレス範囲
筑波	Tsukuba-LAN110	130.158.110.0/24
	Tsukuba-SC	130.158.53.0/24
KEK	KEK-CRC	130.87.253.0/24
大阪	Osaka-RCNP	133.1.86.0/24
京都	Kyoto-YITP	130.54.107.0/24
理研 (和光)	Riken-Wako-Nishina	134.160.38.0/24
	Riken-Wako-SC	134.160.228.0/24
理研 (神戸)	Riken-Kobe	134.160.188.0/24
広島	–	–
東京	–	–

表 5: 各拠点のクライアントネットワーク

B.2　仮想組織管理サーバへのアクセス

JLDG 管理サーバの多くは、HEPnet-J/sc 内の通信と各拠点の JLDG クライアントとのインターネット経由の通信のみ必要ですが、web 系のサーバは例外です。web 系のサーバはユーザのブラウザと通信しますが、ブラウザが稼働している端末は、例えば研究室や自宅等クライアントネットワーク外にあるのが通例です。一方で、web 系のアプリケーションは、不正侵入の為の攻撃の対象になりやすく、接続元 IP を制限して運用するのが通例です。

JLDG の web 系のサーバでは、公開のウェブサーバを除くと、仮想組織管理サーバが、ユーザの個々のブラウザとの通信を必要とする、唯一のサーバです。JLDG では、安全性と利便性の妥協点として、仮想組織管理サーバへのアクセス元 IP をクライアントネット

ワークに限定し、安全とされる方法でユーザ個々のブラウザからサーバにアクセスする方法を提示する事にしました。

JLDG の拠点のネットワーク構成や運用規則は、拠点毎に異なっている為、拠点毎に推奨するアクセス方法を示します。何れも、よく知られた方法（の組み合わせ）です。

B.2.1 筑波大計算科学研究センター

1. 個人利用端末 (後に、ブラウザを起動します) から、JLDG クライアントに openssh でログインする環境を整えて下さい。センタークライアント経由で JLDG を利用する為には、必須の設定です。センター内から:

   ```
   % ssh flare25.ccs.tsukuba.ac.jp
   ```

   センター外（学外含む）からは:

   ```
   % ssh -J charon.ccs.tsukuba.ac.jp flare25.ccs.tsukuba.ac.jp
   ```

   計算科学研究センターのサーバへのログインは公開鍵認証 ssh のみ許可されており、サーバに秘密鍵を置くことは禁止されています。端末には、クライアント (flare25) やアクセスサーバ (charon) の秘密鍵を置き、パスフレーズを ssh-agent で管理すると便利です。サーバ名の前に `user@` を付加できます。
   Windows 環境下の ssh クライアントは何種類かありますが、windows10 では openssh が標準で install されています。ssh-agent は無効になっているので、タスクマネージャで有効にし、起動して下さい。ssh コマンドは、PowerShell 内で CLI で使います。

2. 仮想組織管理サーバにアクセスする際は、ssh の dynamic port forwarding を用います。センター内外に応じて、

   ```
   % ssh -D 1080 flare25.ccs.tsukuba.ac.jp
   % ssh -D 1080 -J charon.ccs.tsukuba.ac.jp flare25.ccs.tsukuba.ac.jp
   ```

   で接続し、接続を維持したまま、証明書のインポート及び socksv5 proxy (ホスト: ポート localhost:1080) の設定が済んだブラウザを立ち上げ、

   ```
   https://vomsrv7.jldg.org:8443/voms/jldg
   ```

   にアクセスします。ポピュラーなブラウザに対する証明書のインポート方法は 2.6.1 を、proxy 設定は B.2.5 を参照して下さい。

   ssh の port forwarding と ブラウザの proxy 設定によって、localhost:1080 へのアクセスが JLDG クライアント flare25 に転送され、サーバからはあたかも、クライアントからアクセスされている様に見えます。

B.2.2 大阪大学核物理研究センター

『RCNP サイトでの JLDG 利用マニュアル』(https://www.jldg.org/jldg/) に具体的な方法を記載していますので、参照して下さい。

B.2.3 理化学研究所仁科加速器科学研究センター

1. 仁科 NW 上のクライアント (jldgfe) に ssh でログインします。この際、jldgfe 上で立ち上げたアプリケーションのウィンドウが手元の端末に表示される様なモードで ssh ログインして下さい。(ssh に "-X" option (X11 forwarding を可能にする option) を付けてログインする等)

2. 証明書をインポートしたブラウザを jldgfe 上で立ち上げ、以下の URL にて仮想組織管理サーバに接続します。

   `https://vomsrv7.jldg.org:8443/voms/jldg`

   ポピュラーなブラウザに対する証明書のインポート方法は 2.6.1 を参照して下さい。

B.2.4 理化学研究所計算科学研究センター (富岳)

1. ssh を使い、ローカルのポート (1080) をリモート先 (vomsrv7.jldg.org:8443) に転送します。

   - putty の場合、「富岳」ログイン用セッションの、[接続]→[SSH]→[認証]→[トンネル] の [フォワードするポートの追加] で、以下を記述/選択し、「追加」ボタンを押して、セッションを保存し、接続します。(保存は一度で十分です。)
     - 源ポートに `1080` を記述
     - 送り先に `vomsrv7.jldg.org:8443` を記述
     - ローカルを選択
     - 自動を選択
   - ssh の場合、次の様に富岳へログインします。
     `ssh user@login.fugaku.r-ccs.riken.jp -L 1080:vomsrv7.jldg.org:8443 -N`

2. 証明書をインポートしたブラウザで以下の URL にて仮想組織管理サーバに接続します。その際、SSL の証明書の警告が出る可能性がありますがそのまま接続して問題ありません。

   `https://localhost:1080/voms/jldg`

   ポピュラーなブラウザに対する証明書のインポート方法は 2.6.1 を参照して下さい。

B.2.5　ブラウザの socks-v5 proxy 設定

proxy 設定の手順の詳細は、OS の種類やバージョンによって異なりますので、詳細は OS のマニュアル等を参照して下さい。ここでは、windows10 を例に proxy 設定の手順を示します。

1. 「インターネットオプション」を開きます。「インターネットオプション」は Internet Explorer の「ツール」プルダウンメニューから、あるいは、スタートボタンをクリック後、「インターネットオプション」とキーボードで入力する等して開くことができます。
2. 「接続」「LAN の設定」の順にクリックします。
3. 「プロキシ サーバー」の項目にある、「LAN にプロキシ サーバーを使用する」のチェックボックスにチェックを付けます。
4. 「詳細設定」をクリックし、「サーバー」の項目にある、種類「Socks」に対し、以下の設定を入力します。
   - 使用するプロキシのアドレス: localhost
   - ポート: 1080
5. 「OK」→「OK」→「OK」とクリックして「インターネットオプション」ウィンドウを閉じれば設定完了です。

<u>Internet Explorer 及び Google Chrome</u>
以上の設定ができた状態でブラウザを立ち上げれば proxy 設定が適用されます。

<u>Firefox</u>

1. 右上のメニューボタン（横三本線）をクリックし、プルダウンメニューから「設定」をクリックします。
2. 「一般」パネルの「ネットワーク設定」の項目にある「接続設定」をクリックします。
3. 「インターネット接続に使用するプロキシーの設定」で、「システムのプロキシー設定を利用する」を選択します。（上記の様に「インターネットオプション」で proxy の設定をする代わりに、ここで「手動でプロキシーを設定する」を選択し、proxy を設定することも可能です。）
4. 「OK」をクリックし、設定を完了します。

なお、ここで設定した proxy が不要になった際は、再び「インターネットオプション」より「接続」→「LAN の設定」と進み、「LAN にプロキシ サーバーを使用する」のチェックを外せば、設定を解除できます。