JLDG ユーザー各位

JLDG 証明書の一斉更新について

JLDG 管理者グループ
2021/10/04

JLDG 管理サーバの更新に伴い、『JLDG ユーザー証明書』の一斉更新を実施します。更新期間内に下記手順で更新下さい。期限後は、現証明書での JLDG 利用ができなくなります。また、期限後の証明書の発行は、新規ユーザー登録と同じ手続きが必要になります。現在有効な証明書をお持ちのユーザーの皆様は、期間中に必ず更新をお願いします。

(資料)
JLDG のユーザー証明書及び仮想組織管理関連事項の参考資料として『利用の手引き』の改訂版原稿の一部を添付しています。以下の、証明書更新の各手順での操作の詳細の確認にご利用下さい。

(更新の要否確認)
現証明書の確認：現在ご利用中の証明書のサブジェクトを確認してください。(資料の 3.5)
今回は、第 2 世代証明書を失効させ、第 3 世代の証明書に切り替えます。 第 3 世代証明書をご利用の方は、更新する必要はありません。更新の手順の概要は（資料の 3.5.3)を参照ください。

（更新期間）
更新は 2 回に分けて行います。どちらか、ご都合の良い期間に更新手続きをお願いします。
第 1 期：　更新依頼期間:10 月 8 日から 10 月 22 日、新証明書承認・設定変更日 10 月 25 日
第 2 期：　更新依頼期間:11 月 8 日から 11 月 22 日、新証明書承認・設定変更日 11 月 25 日

(更新手順)
更新依頼期間中に、(資料 3.5.3)の『手順 1:ライセンス ID 発行依頼』から『手順 5:証明書の追加』までを実行してください。システム側作業『手順 6: 新証明書承認・設定変更』は、更新依頼期間内に依頼があった更新依頼に対して、まとめて作業します。翌日からは、新証明書が有効になります。
(ご注意)
（資料の 3.5.3）の『手順 7:新証明書の有効化』までは、現証明書のみが有効です。『手順 2:新証明書の発行』後、新証明書を格納したディレクトリ $HOME/.globus を rename し、現証明書を格納してあるディレクトリを標準名に戻しておく、事をお勧めします。または、代理証明書発行の際に、現証明書を明示的に指定するなど、適宜、対応をお願いします。

資料

JLDG のユーザー証明書及び仮想組織管理関連事項

（利用の手引き改訂 6.2 版用原稿より）

2　利用開始までの流れ

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

を実行してください。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: ← 確認のため再入力。
```

PKCS12 形 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ください。

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ください。『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ください。

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、前でインポートした証明書を提示してください。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[1]。「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、各項目を記入してください。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ください。入力内容に問題がない場合、Confirmation required 云々を書かれたページが表示されます。

4. 本人確認のため、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（月ー金）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。

[1] 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。

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。

3　利用法

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　(現在有効、新規発行は停止)

     `/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

ユーザー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ください。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 の発行を依頼してください。

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ください。その際、所属グループ、ユーザー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 をお使いください。

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ください。

   - 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。

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纏めます。

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。

Site	network-name	ip-range
Tsukuba	Tsukuba-LAN110	130.158.110.0/24
	Tsukuba-SC	130.158.53.0/24
KEK	KEK-CRC	130.87.253.0/24
Riken-Wako	Riken-Wako-Nishina	134.160.38.0/24
	Riken-Wako-SC	134.160.228.0/24
Riken Kobe	Riken-Kobe	134.160.188.0/24
Kyoto	Kyoto-YITP	130.54.107.0/24
Osaka	Osaka-RCNP	133.1.86.0/24
Hiroshima		
Tokyo		

表 1: 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など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。

JLDD 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および 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 RCNP

『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 理研和光

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ようなモードで ssh ログインしてください。(ssh に ”-X” option (X11 forwarding を可能にする option) を付けてログインするなど)

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 理研神戸（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、次のよう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ください。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。

Internet Explorer 及び Google Chrome
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。

Firefox

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。