JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

File Transfer Protocol（FTP）でのクライアント証明書認証

Ver.1.0

2014 年 6 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベートCA Gléas」で発行したクライアント証明書・を利用して、FTP通信で認証をおこなう環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- FTPサーバ：Ubuntu Server 14.04 LTS
  ProFTPD 1.3.5rc3 Server & mod_tls 2.4.5 / OpenSSL 1.0.1f
  （Ubuntuのパッケージを利用）
  ※以後、「FTPサーバ」と記載します
- JS3 プライベートCA Gléas （バージョン1.11）
  ※以後、「Gléas」と記載します
- クライアントPC：Windows 8.1 Pro 64bit
  GUIクライアント：SmartFTP 6.0.2024.0 評価版
  CUIクライアント：curl 7.36.0 (x86_64-pc-win32)
  ※以後、「PC」と記載します

以下については、本書では説明を割愛します。

- Ubuntu ServerやFTPサーバのセットアップ
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- PCでのネットワーク設定等の基本設定

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

2. FTPサーバの設定

2.1. ファイルのアップロード

次のファイルを FTP サーバにアップロードします。
ファイル名、アップロード先ディレクトリ共にサンプルとなります。本書では以下の名前であることを前提に記載します。

	ファイル名	アップロード先ディレクトリ名※
CA 証明書	ia1.pem	/etc/pki/tls/ca_certs/
サーバ証明書	ssl-server.crt	/etc/pki/tls/server/
秘密鍵	ssl-server.key	/etc/pki/tls/server/
証明書失効リスト（CRL）	crl_ia1.pem	/etc/pki/tls/crls/

※ 各ディレクトリが存在しない場合は新規に作成してください。

【CA 証明書】
Gléas では次の URL から取得できます。
http://{Gléas のホスト名 or IP アドレス}/crl/ia1.pem
ファイルのアップロード後、以下のコマンドで CA 証明書のハッシュリンクを作成しておきます。

```
c_rehash /etc/pki/tls/ca_certs/
```

※tls.conf で TLSCACertificatePath ディレクティブを使う場合。TLSCACertificateFile ディレクティブを使う場合は不要です

【サーバ証明書・秘密鍵】
Gléas からダウンロードしたサーバ証明書は PKCS#12 という形式になっているため、PEM 形式に変換・分離する必要があります。
1) PKCS#12 ファイルより証明書を取得

```
openssl pkcs12 -in ssl-server.p12 -clcerts -nokeys -out ssl-server.crt
```

2) PKCS#12 ファイルより秘密鍵を取得

```
openssl pkcs12 -in ssl-server.p12 -nocerts -nodes -out ssl-server.key
```

秘密鍵は root をオーナーにし、パーミッションを 400 にすることを変更します。

【証明書失効リスト（CRL）】
Gléas では CRL ファイルは次の URL から取得できます。
http://{Gléas のホスト名 or IP アドレス}/crl/crl_ia1.pem

ファイルのアップロード後、以下のコマンドで CRL ファイルのハッシュリンクを作成しておきます。

```
c_rehash /etc/pki/tls/crls/
```

※tls.conf で TLSCARevoatoinPath ディレクティブを使う場合。TLSCARevocationFile ディレクティブを使う場合は不要です

認証局で証明書を失効しても、FTP サーバ上の CRL が自動的に更新されることはありません。また、NextUpdate の日付を過ぎた CRL は無効な情報と判断され、ProFTPD は全ての接続を拒否します。
新たに証明書を失効した時や NextUpdate の日付が過ぎる前に、新しい CRL を取得して、既存の CRL と置き換える必要があります。
Gléas では、CRL は HTTP（または LDAP）を用いてダウンロード可能です。以下の処理を cron などで定期的に実施することを推奨します。
CRL 取得処理手順：
1) 認証局のリポジトリから wget 等で CRL ファイルを取得する
2) 正常にダウンロード出来たことを確認して、/etc/pki/tls/crls/のファイルを上書きコピーする
3) ProFTPD を再起動（もしくはリロード）する
※c_rehash を再度実行する必要はありません

2.2. proftpd.conf の編集

proftpd.conf（/etc/proftpd/proftpd.conf）ファイルを以下の通り編集します。

FTPS を有効にするため以下の行のコメントアウトをはずします。

```
Include /etc/proftpd/tls.conf
```

2.3. tls.conf の編集

tls.conf（/etc/proftpd/tls.conf）ファイルを以下の通り編集します。

以下のディレクティブのコメントアウトをはずして SSL を有効にします。

```
TLSEngine
TLSLog
TLSProtocol
```

TLSRSACertificateFile ディレクティブのコメントアウトをはずしてサーバ証明書ファイルをフルパスで指定します。

```
TLSCertificateFile              /etc/pki/tls/server/ssl-server.crt
```

TLSRSACertificateKeyFile ディレクティブのコメントアウトをはずしてサーバ証明書に対応する秘密鍵ファイルをフルパスで指定します。

```
TLSCertificateFile              /etc/pki/tls/server/ssl-server.key
```

TLSCACertificatePath ディレクティブを追加し、CA 証明書ファイルが置かれたディレクトリを指定します。

```
TLSCACertificatePath            /etc/pki/tls/ca_certs/
```

TLSCARevocationPath ディレクティブを追加し、証明書失効リストが置かれたディレクトリを指定します。

```
TLSCACertificatePath            /etc/pki/tls/crls/
```

クライアント証明書要求を有効化するために、TLSVerifyClient ディレクティブのコメントアウトをはずして、クライアント証明書要求を有効にします。

```
TLSVerifyClient                 on
```

FTP サーバへの接続を SSL のみに制限したい場合は、TLSRequired ディレクティブを有効にします。

```
TLSRequired                     on
```

TLSUserName ディレクティブを利用すると、証明書の内容と FTP ログインに利用するユーザ ID との一致をチェックすることができます。
以下は証明書サブジェクトのコモンネーム（すなわち、Gléas でのアカウント名）と、FTP ログインで利用するユーザ名の一致をチェックする場合の例となります。
なお一致する場合は、FTP クライアントのパスワード入力は不要となります。

```
TLSUserName                     CommonName
```

2.4. ProFTPD の再起動

tls.conf ファイルの編集が完了したら、ProFTPD を再起動します。
「netstat –a | grep ftp」を実行して、以下の行が表示されれば正常に起動しています。何も表示されない場合、設定を確認してください。

```
tcp6       0      0       [::]:ftp        [::]:*          LISTEN
```

以上で、ProFTPD の設定は終了です。

3. Gléasの管理者設定

GléasのUA（申込局）より発行済み証明書をPCにインポートできるよう設定します。
※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

3.1. UA（ユーザ申込局）設定

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA（申込局）をクリックします。

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

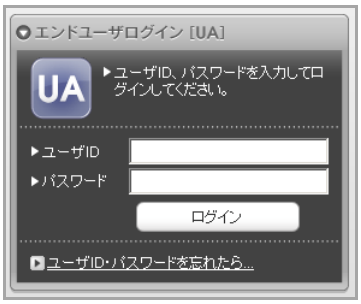
- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、 [保存]をクリックします。

4. PC での操作

4.1. クライアント証明書のインポート

Internet ExplorerでGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、Gléasでのユーザ IDとパスワードを入力しログインします。



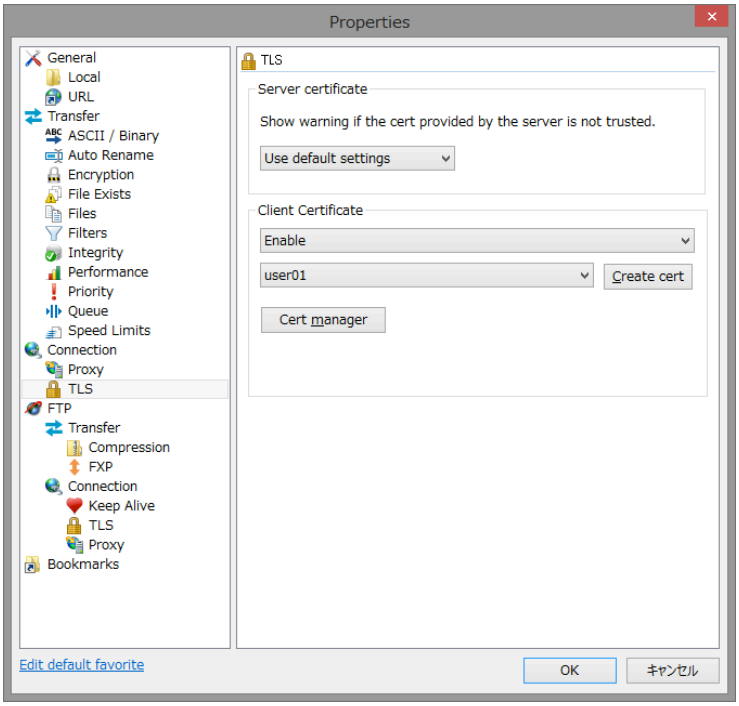
ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。
※初回ログインの際は、ActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。

4.2. FTP クライアントの設定・接続

SmartFTPでの接続設定では、ユーザ名のみとします。
（2.3項の通り、tls.confファイルでTLSUserNameディレクトリが設定されている前提）

[プロパティ] > [TLS]のClient Certificateで、クライアント証明書を[enable]にして接続に利用する証明書をドロップダウンリストより選択します。



その後、ログインをおこなうとクライアント証明書認証がおこなわれ、FTPサーバへのログインがおこなわれます。
その際に、tls.confファイルのTLSLogディレクティブで指定したファイルに認証ログが残ります（以下はその抜粋です）。

```
mod_tls/2.4.5[12345]: TLS/TLS-C requested, starting TLS handshake
mod_tls/2.4.5[12345]: CRL store present, checking client certificate against configured CRLs
mod_tls/2.4.5[12345]: CA CRL: Issuer: CN=demoCA, DC=COM, DC=JCCH-SSS, lastUpdate: May 30 05:30:36 2014 GMT, nextUpdate: Jun 29 05:30:36 2014 GMT
mod_tls/2.4.5[12345]: CRL store present, checking client certificate against configured CRLs
mod_tls/2.4.5[12345]: Client: CN = user01, DC = COM, DC = JCCH-SSS
mod_tls/2.4.5[12345]: TLSv1/SSLv3 connection accepted, using cipher DHE-RSA-AES256-GCM-SHA384 (256 bits)
mod_tls/2.4.5[12345]: matched client cert CommonName 'user01' to user 'user01'
mod_tls/2.4.5[12345]: TLS/X509 TLSUserName 'CommonName' check successful for user 'user01'
```

4.3. コマンドラインからの接続

以下、cURLを用いた接続確認例を記します。引数などの詳細はcURLのマニュアルをご参照ください。

```
curl --ssl ftp://fqdn/ --user username:password --cert username.cer --key username.key --cacert gleascert.cer --verbose
```

※本書の設定内容であれば、password部分は何を指定しても構いません
※証明書ファイル（.P12ファイル）をダウンロードして、証明書と秘密鍵を分けておく必要があります（2.1項のサーバ証明書を分割する手順と同じです）。

5. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや検証用の証明書に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ
Tel:　050-3821-2195
Mail:　sales@jcch-sss.com