JCCH・セキュリティ・ソリューション・システムズ

プライベート認証局Gléas ホワイトペーパー

Nginxでのクライアント証明書認証

Ver.1.0.1
2019 年 10 月

目次

1. はじめに

1.1. 本書について

本書では弊社製品「プライベート認証局Gléas」で発行した電子証明書を使って、Nginx Basic HTTP serverで証明書認証を行う環境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、ご参照いただけますようお願いいたします。

弊社では試験用証明書の提供も行っております。検証などで必要な場合は、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。

- CentOS 7.6-1810 ※以下「CentOS」と記載します
- Nginx Basic HTTP server 1.17.3 ※以下「Nginx」と記載します
- OpenSSL 1.1.1d
- PHP 5.4.16
- JS3 プライベート認証局Gléas （バージョン2.1.3）※以下「Gléas」と記載します
- クライアント：Dell XPS 12 (Windows 10 Pro) / Google Chrome

※以下「Windows」「Chrome」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。

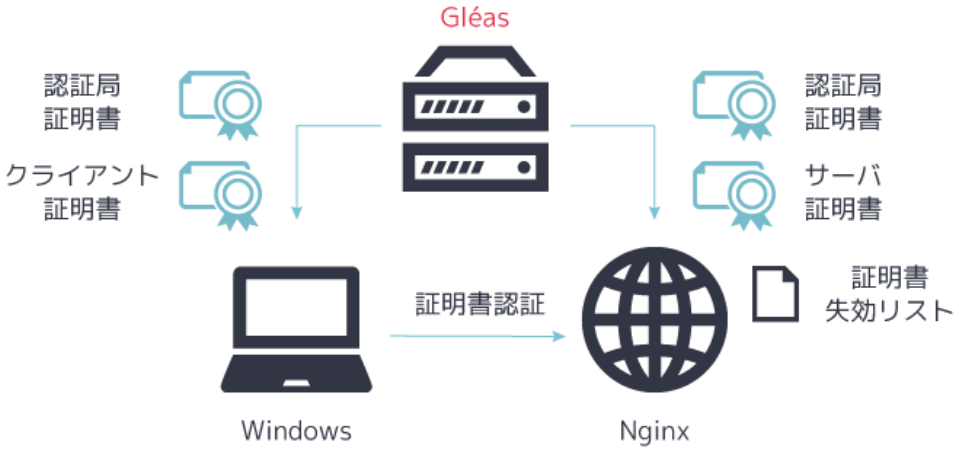
- CentOSの基本設定、ネットワーク設定、ファイヤウォール設定
- Nginx、OpenSSL、PHPのインストール
- Gléasの基本設定、サーバ証明書の発行
- Windowsの基本設定

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。

iOS13、macOS 10.15ではTLSサーバ証明書に対するセキュリティ要件がアップデートされています。サーバ証明書の有効期限や、鍵長、ハッシュアルゴリズムなどが条件を満たさないサーバには接続できません。詳しくはAppleのウェブサイトをご確認ください。
https://support.apple.com/ja-jp/HT210176

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



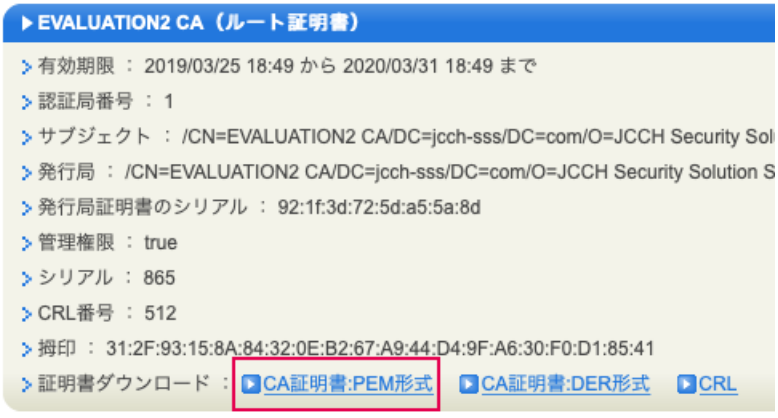
2. Nginxの設定

2.1. 証明書認証用ファイルのアップロード

下記のファイルをサーバにアップロードします。ファイル名とディレクトリはサンプルです。
本書では下記のファイル名とディレクトリであることを前提とします。

	ファイル名	ディレクトリ
認証局証明書	cacert.pem	/etc/pki/tls/certs/
サーバ証明書	nginx.crt	/etc/pki/tls/certs/
サーバ秘密鍵	nginx.key	/etc/pki/tls/private/
証明書失効リスト	crl_ia1.pem	/etc/pki/CA/crl

Gléas の認証局証明書は管理画面で、認証局→発行局と進んだ画面でダウンロードできます。



[CA 証明書:PEM 形式]をクリックします。

あらかじめ Gléas でサーバ証明書を発行しておきます。Gléas の管理画面で当該の証明書の詳細を表示し、[ダウンロード]をクリックします。ダウンロードした証明書ファイルは PKCS#12 形式のファイルです。Nginx の仕様に合わせるため、証明書を PEM 形式に変換し、秘密鍵を抽出します。

PKCS#12 ファイルから PEM 形式の証明書を作成
```
openssl pkcs12 -in [filename] -clcerts -nokeys -out nginx.crt
```

PKCS#12 ファイルから秘密鍵を抽出
```
openssl pkcs12 -in [filename] -nocerts -nodes -out nginx.key
```

サーバ秘密鍵は root をオーナーにし、パーミッションを 400 にすることをお勧めします。

Gléas の証明書失効リストは、ブラウザで下記 URL へアクセスしてダウンロードできます。
http://serverurl/crl/crl_ia1.pem

2.2. nginx.conf の編集

Nginx の設定ファイル nginx.conf を編集します。本環境では /etc/nginx/ に配置されています。

4.2.項で、失効済み証明書でアクセスした場合のエラー内容を確認するため、error_log のレベルを info あるいは debug に設定します。
```
error_log /var/log/nginx/error.log info;
```

4.1.項でのアクセスログ確認のため、log_format に暗号プロトコルと暗号スイートを加えます。
```
log_format main '$remote_addr - $remote_user [$time_local] '
                        '$ssl_protocol/$ssl_cipher '
                        '"$request" $status $body_bytes_sent '
                        '"$http_referer" "$http_user_agent"';

access_log /var/log/nginx/access.log main;
```

2.3. default.conf の編集

nginx.conf は外部の設定ファイルを読み込むことができます。本環境では /etc/nginx/conf.d/default.conf を読み込んでいます。default.conf を編集します。

リッスンするポートを 443 番の SSL にします。
```
listen 443 ssl;
```

2.1.項で設定したサーバ証明書と秘密鍵のパスを指定します。サーバ名は環境に合わせた名前を指定します。
```
ssl_certificate /etc/pki/tls/certs/nginx.crt;
ssl_certificate_key /etc/pki/tls/private/nginx.key;
server_name nginx.jcch-sss.local;
```

SSL のプロトコルを TLSv1.2 と TLSv1.3 を指定します。
```
ssl_protocols TLSv1.2 TLSv1.3;
```

Nginx が指定する暗号スイートをクライアントの指定より優先させます。
```
ssl_prefer_server_ciphers on;
```

暗号スイートを指定します。本環境では Mozilla が推奨する設定にしています。
```
ssl_ciphers
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK;
```

PEM 形式で Gléas の認証局証明書を設定します。
```
ssl_client_certificate /etc/pki/tls/certs/cacert.pem;
```

PEM 形式で CRL を設定します。
```
ssl_crl /etc/pki/CA/crl/crl_ia1.pem;
```

クライアント証明書認証を有効化します。
```
ssl_verify_client on;
```

証明書チェーンの段階の上限値を設定します。
```
ssl_verify_depth 1;
```

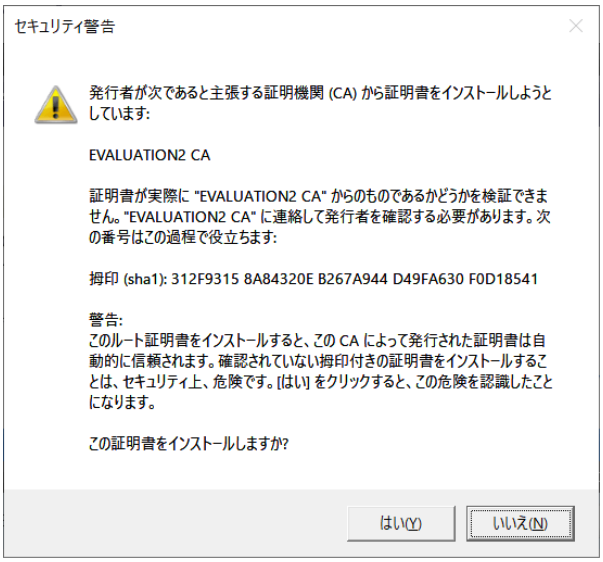
default.conf を保存したら、Nginx を再起動します。
```
systemctl restart nginx
```

3. クライアント証明書の取得

Windows で Internet Explorer を起動し、Gléas のユーザ用ウェブ画面にアクセスします。

ユーザ ID とパスワードを入力してログインします。

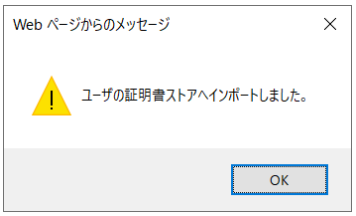
[証明書のインポート]をクリックすると下のセキュリティ警告が出ます。これは Windows が Gléas を信頼する証明機関と見なしていないためです。[はい]をクリックすることで、Windows は Gléas を信頼する証明機関と見なします。



※セキュリティ向上ため、[拇印]に表示された文字列と、システム管理者から伝えられた文字列が突合するかを確認する運用が推奨されます。

続いてクライアント証明書が証明書ストアへ直接インポートされます。証明書は秘密鍵のエクスポートができないようになっています。また証明書がファイル形式で Windows に残らないた

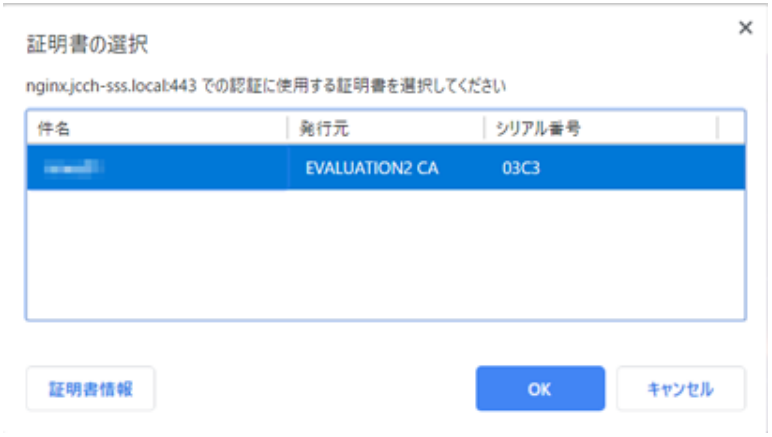
め、他のデバイスにコピーされる恐れはありません。



4. 動作確認

4.1. 有効な証明書の場合

クライアント証明書をインポートしたWindowsでGoogle Chromeを起動し、Nginxにアクセスします。Gléasからインポートした証明書が表示されたら[OK]をクリックし、Nginxへのアクセスが許可されます。



アクセスログ（本環境では /var/log/nginx/access.log）を確認します。

```
192.168.20.42 - - [18/Sep/2019:15:00:16 +0900] TLSv1.2/ECDHE-RSA-AES128-GCM-SHA256 "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36"
```

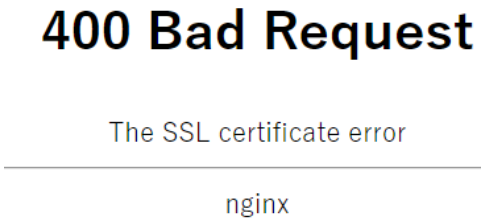
使われた暗号プロトコル、暗号スイートを確認できます。

4.2. 失効済み証明書の場合

Gléasの管理画面で当該のクライアント証明書を失効し、更新された証明書失効リストをNginxに設定して、Nginxを再起動します。

```
systemctl restart nginx
```

同じ証明書でNginxにアクセスすると、接続できません。



エラーログ（本環境では /var/log/nginx/error.log）を確認します。

```
2019/09/30 16:53:06 [info] 7803#7803: *3 client SSL certificate verify error: (23:certificate revoked) while reading client request headers, client: 192.168.20.42, server: nginx.jcch-sss.local, request: "GET / HTTP/1.1", host: "nginx.jcch-sss.local"
```

証明書の失効が原因で認証エラーが起こったことがわかります。

4.3. クライアント証明書の情報をログに記載

Nginxのログにクライアント証明書の情報を記録することができます。

nginx.conf に以下の記述を加えて、Nginxを再起動します。。

```
log_format ssl '$time_local $remote_addr '
                    '[$ssl_client_s_dn_legacy] '
                    '$ssl_protocol/$ssl_cipher '
                    '$request $http_user_agent';
access_log /var/log/nginx/access.log ssl;
```

アクセスログ /var/log/nginx/access.log を確認します。

```
02/Oct/2019:10:06:45 +0900 192.168.20.42 [/CN=user01/OU=groupA/O=JCCH Security Solution Systems Co., Ltd./DC=com/DC=jcch-sss] TLSv1.2/ECDHE-RSA-AES128-GCM-SHA256 GET / HTTP/1.1 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
```

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