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

Apacheでのクライアント証明書認証

Ver.1.4
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、Apache 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
- Apache HTTP Server 2.4.41 (IUS)　※以下「Apache」と記載します
- mod_ssl 2.4.41
- OpenSSL 1.0.2k-fips
- 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
- Apache、mod_ssl、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

2. Apacheの設定

2.1. 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	apache.crt	/etc/pki/tls/certs/
サーバ秘密鍵	apache.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。Apache 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 apache.crt
```

PKCS#12 ファイルから秘密鍵を抽出

```
openssl pkcs12 -in [filename] -nocerts -nodes -out apache.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. ssl.conf の編集

ssl.conf を編集します。本環境では /etc/httpd/conf.d/ に配置されています。

サーバ証明書の指定
```
SSLCertificateFile /etc/pki/tls/certs/apache.crt
```

サーバ秘密鍵の指定
```
SSLCertificateKeyFile /etc/pki/tls/private/apache.key
```

認証局証明書の指定
```
SSLCACertificateFile /etc/pki/tls/certs/cacert.pem
```

クライアント証明書認証の有効化
```
SSLVerifyClient require
```

証明書の失効確認の有効化
```
SSLCARevocationCheck chain
```

証明書失効リストの指定
```
SSLCARevocationFile /etc/pki/CA/crl/crl_ia1.pem
```

以上の項目の変更後、Apache を再起動します。
```
apachectl restart
```

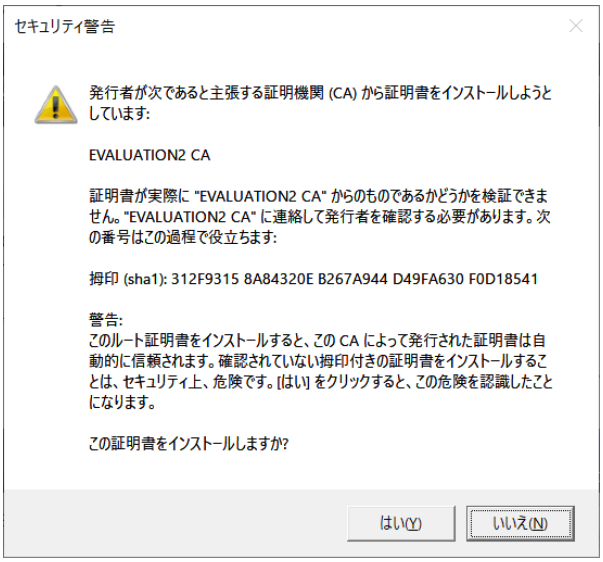
Apache の状況を確認します。
```
apachectl status
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running)
```

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。

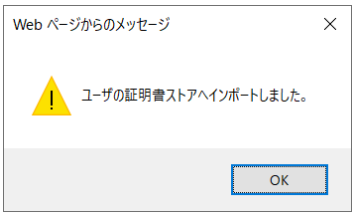
[証明書のインポート]をクリックすると下のセキュリティ警告が出ます。これは Windows が Gléas を信頼する証明機関と見なしていないためです。[はい]をクリックすることで、Windows は Gléas を信頼する証明機関と見なします。



※セキュリティ向上とめ、[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

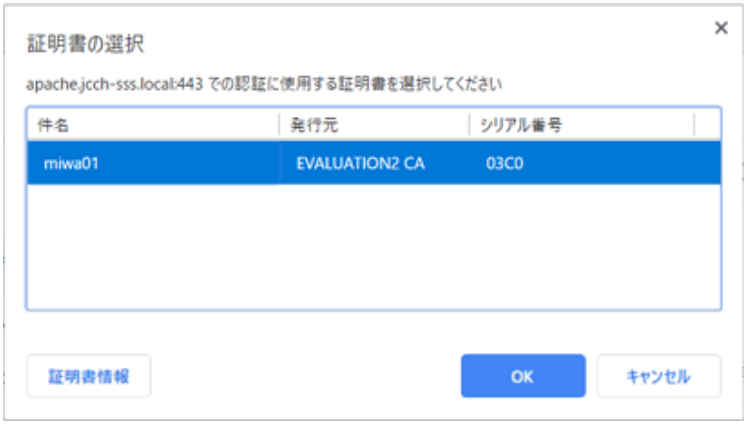
め、他のデバイスにコピーされる恐れはありません。



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Chromeを起動し、Apache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、Apacheへのアクセスが許可されます。



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Apacheに設定してから、同じ証明書でApacheにアクセスすると、接続できません。

Apacheのエラーログを確認します。本環境では /var/log/httpd/ssl_error_log にあります。

[Mon Sep 09 15:24:32.801650 2019] [ssl:error] [pid 26998:tid 140595913729792] [client 192.168.20.42:49915] AH02039: Certificate Verification: Error (23): certificate revoked

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サブジェクトによるアクセス制限

証明書のサブジェクトによって、アクセスできるディレクトリを制限できます。
OU=groupA の証明書を持つユーザだけに /groupA ディレクトリにアクセスを許可するため、ssl.conf に以下の記述を加えます。

```
<Directory "/var/www/html/groupA">
        Require expr %{SSL_CLIENT_S_DN_OU} = 'groupA'
</Directory>
```

OU=groupB の証明書で /groupA にアクセスした場合のエラーログ /var/log/httpd/ssl_access/log は以下のようになります。

[Fri Sep 27 17:44:42.606621 2019] [authz_core:debug] [pid 66468] mod_authz_core.c(820): [client 192.168.20.42:50810] AH01626: authorization result of Require expr %{SSL_CLIENT_S_DN_OU} = 'groupA': denied
[Fri Sep 27 17:44:42.606636 2019] [authz_core:debug] [pid 66468] mod_authz_core.c(820): [client 192.168.20.42:50810] AH01626: authorization result of <RequireAny>: denied
[Fri Sep 27 17:44:42.606641 2019] [authz_core:error] [pid 66468] [client 192.168.20.42:50810] AH01630: client denied by server configuration: /var/www/html/groupA/

4.4. クライアント証明書の情報をログに記載

Apache の Custom Log 機能を使って、クライアント証明書の情報をログに残すことができます。ssl.conf に以下の記述を加え、アクセスした時刻、クライアントの IP アドレス、証明書に記載された組織、所属、コモンネームをログに記録します。

```
CustomLog "logs/ssl_cert_log"
"%t %a   %{SSL_CLIENT_S_DN_O}x %{SSL_CLIENT_S_DN_OU}x %{SSL_CLIENT_S_DN_CN}x
"
```

4.5. PHP でクライアント証明書の情報を取得

SSL関連の環境変数を取得するため、ssl.conf に以下の記述を加えます。

```
SSLOptions +StdEnvVars
```

取得したクライアント証明書の情報（組織、所属、コモンネーム）をPHPで表示させる場合の例です。

```
<?php
echo 'Organization : '.$_SERVER['SSL_CLIENT_S_DN_O']."<br/>¥n";
echo 'Organization Unit : '.$_SERVER['SSL_CLIENT_S_DN_OU']."<br/>¥n";
echo 'Common Name : '.$_SERVER['SSL_CLIENT_S_DN_CN']."<br/>¥n";
?>
```

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