（参考資料としての利用に限る）

Apache2.2.12～ の SNI 機能について

SNI とは Server Name Indication の略で SSL プロトコルの拡張機能。名前ベースの SSL サイトが設定を実現します。　つまり、同一筐体サーバ内で 1 IP 配下で、複数の SSL サイトを構築できることになる。 従来は、IP ベースと呼ばれ、SSL サイト毎必ず 1IP の割当が必須でありました。 SNI ではクライアントがサーバに対してサーバのホスト名を伝える事が定義されております。

利用条件

- **Apache が 2.2.12 以降**
- OpenSSL が 0.9.8f 以降で TLS 拡張オプションを指定(configure enable-tlsext shared)
- Apache が上記 OpenSSL でビルド
- ブラウザが SNI 対応

設定

Apache の設定ファイルは通常通りの設定で問題ありません。 SNI 用の設定としては冒頭の **SSLStrictSNIVHostCheck** のみ（これも Optional であり必須ではありません）です。

```
Listen 443

NameVirtualHost *:443

SSLStrictSNIVHostCheck off

<VirtualHost *:443>

DocumentRoot /srv/www/example1.com/

ServerName www.example1.com

...

</VirtualHost>
```

（以下 SNI 対象 Virtual Host を繰り返して設定）

<VirtualHost *:443>

DocumentRoot /srv/www/example2.com/

ServerName www.example2.com

…

</VirtualHost>

ここで SSLStrictSNIVHostCheck off と設定されておりますが、これは SNI 未対応ブラウザの挙動を制御する設定となり off であれば Default Virtual Host へリダイレクトされ、on であれば、接続自体を拒否します。

また Default Virtual Host に on が設定されている場合、IP/Port が同一の他の名前ベースの Virtual Host 接続は拒否されます。

SSLStrictSNIVHostCheck 自身は Server ディレクティブか VirtualHost ディレクティブに設定可能。

ブラウザ対応状況

注意すべきは、ブラウザは対応しているバージョンであっても、OS 側が対応していないって組み合わせがあることです。

ブラウザ名	バージョン、その他
IE	7 以降、Vista 以降 IE8 でも XP はダメ
FireFox	2.0 以降
Opera	8.0 以降
Opera Mobile	10.1 以降 Android 版
Chorome	6.??以降 XP でも OK、OS X 10.5.7 以降は Chrome 5.0.342.1 以降
Safari	2.1 以降、MaxOSX 10.5.6 以降、Vista 以降
Mobile Safari	iOS 4.0 以降
Windows Phone	7 以降

【補足】SNI を活用し、マルチドメイン証明書&ワイルドカード証明書の 2 枚を 1IP 配下で apache に設定する方法。

１．マルチドメイン証明書

Common Name：www.jcert.co.jp

SAN2: www.test1.jcertco.jp

SAN2: www.test2.jcert.co.jp

２．ワイルドカード証明書：*.jcert.jp

（これで、以下サブドメインを暗号化する）

- www1.jcert.jp
- www2.jcert.jp

```
<VirtualHost *:443>
DocumentRoot "/var/www/www.jcert.co.jp"
ServerName www.jcert.co.jp:443
SSLEngine on
SSLCertificateFile /etc/pki/multidomain.crt
SSLCertificateChainFile /etc/pki/multidomain.ca-bundle
SSLCertificateKeyFile /etc/pki/multidomain.key
(略)
</VirtualHost>

<VirtualHost *:443>
DocumentRoot "/var/www/www.test1.jcertco.jp"
ServerName www.jcert.co.jp:443
ServerAlias www.test1.jcertco.jp
SSLEngine on
SSLCertificateFile /etc/pki/multidomain.crt
SSLCertificateChainFile /etc/pki/multidomain.ca-bundle
SSLCertificateKeyFile /etc/pki/multidomain.key
(略)
</VirtualHost>
```

<VirtualHost *:443>
DocumentRoot "/var/www/www.test2.jcertco.jp"
ServerName www.jcert.co.jp:443
ServerAlias www.test2.jcertco.jp
SSLEngine on
SSLCertificateFile /etc/pki/multidomain.crt
SSLCertificateChainFile /etc/pki/multidomain.ca-bundle
SSLCertificateKeyFile /etc/pki/multidomain.key
(略)
</VirtualHost>

<VirtualHost *:443>
DocumentRoot "/var/www/www1.jcert.jp"
ServerName www1.jcert.jp:443
SSLEngine on
SSLCertificateFile /etc/pki/wildcard.crt
SSLCertificateChainFile /etc/pki/wildcard.ca-bundle
SSLCertificateKeyFile /etc/pki/wildcard.key
(略)
</VirtualHost>

<VirtualHost *:443>
DocumentRoot "/var/www/www2.jcert.jp"
ServerName www2.jcert.jp:443
SSLEngine on
SSLCertificateFile /etc/pki/wildcard.crt
SSLCertificateChainFile /etc/pki/wildcard.ca-bundle
SSLCertificateKeyFile /etc/pki/wildcard.key
(略)
</VirtualHost>

上記設定では、**SSLStrictSNIVHostCheck** を言及しておりませんので、SNI 非対応のクライアントに対しては、最上位の VirtualHost を返します。

されている情報に従ってユーザーが操作を行った結果、ユーザーが被る損害については、ジェイサートでは一切責任を負いません。ユーザーは自己責任においてのみ、この文書を使用するものとします。