OCSP stapling on nginx　設定手順書

サイバートラスト株式会社

2016年12月15日

はじめに

【！】本手順書をご利用の前に必ずお読みください

1. 本ドキュメントは「Linux OS」「nginx」の環境下でサイバートラストのサーバー証明書をご利用いただく際のOCSP staplingのご設定について解説するドキュメントです。
2. 本ドキュメントは「CentOS 6.3」「nginx 1.6.2」「OpenSSL 1.0.1e」の環境下で動作確認をしており、SSLの設定が完了していることを前提としております。
3. 実際の手順はお客様の環境により異なる場合があり、nginxの動作を保証するものではございません。あらかじめご了承ください。
4. このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
5. このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。

cybertrust

目　次

1. 設定ファイル編集（1/2）

cybertrust

➢ SSL設定ファイルに設定ディレクティブを記述します。

SSL設定ファイルを編集し、下記のディレクティブを{server section} の中に記述します。

- **ssl_stapling on;**
- **resolver *IPaddress [valid=time]*;**

※ SSL設定ファイルは、お客様がお使いのnginxにより異なる場合があります。
例）nginx1.6.2…example_ssl.conf
※ お客様の環境によりファイルやパスが異なりますので、環境に合わせてお読み替えください。
※ カレントディレクトリは任意のディレクトリとなります。
※ 本ドキュメントでは以下の設定を例としてご案内しております。

項目	ファイル名
サーバールート	/etc/nginx
秘密鍵ファイル・証明書ファイル保存ディレクトリ	/etc/nginx/ssl_certs
SSL設定ファイル保存ディレクトリ	/etc/nginx/conf.d/example_ssl.conf
サーバー証明書・中間CA証明書連結ファイル名	certs.pem
秘密鍵ファイル	server.key

```
# HTTPS  server
#
server {
   listen       443 ssl;
   server_name  www.example.com;

   ssl_certificate      /etc/nginx/ssl_certs/certs.pem;
   ssl_certificate_key  /etc/nginx/ssl_certs/server.key;

   ssl_stapling on;
   resolver XXX.XXX.XXX.XXX valid=300s;

   ssl_session_cache shared:SSL:1m;
   ssl_session_timeout  5m;

   ssl_ciphers  HIGH:!aNULL:!MD5;
   ssl_prefer_server_ciphers   on;


   location / {
      root   /usr/share/nginx/html;
      index  index.html index.htm;
}
}
```

1. 設定ファイル編集（2/2）

各ディレクティブの意味は下記を参考にしてください。

- **ssl_stapling on;**

  OCSP stapling を有効にします。

- **resolver *IPaddress [valid=time]*;**

  サーバーが名前解決に使用するDNSサーバーのIPアドレスを記述します。

  DNSサーバーは複数登録可能です。

  その際は半角スペースを空けて、続けてIPアドレスを記述します。

  例）resolver XXX.XXX.XXX.XXX valid=300s;

  「IPaddress」に適宜、お客様任意の内容を記述してください。

個別にOCSP staplingを無効にしたい仮想サイトには、対象の仮想サイトの{server section}内にOCSP staplingに関する内容を記述しません。

右記の例では仮想サイト＜www.example.com＞にはOCSP staplingを適用させ、仮想サイト＜www2.example.com＞ではOCSP staplingを無効にしています。

先頭の仮想サイト（デフォルトサーバー）にてOCSP staplingを無効にしていると、配下の仮想サイトでOCSP staplingが有効にならない場合があります。ご注意ください。

```
# HTTPS  server
#
server {
   listen       443 ssl;
   server_name  www.example.com;

   ssl_certificate      /etc/nginx/ssl_certs/certs.pem;
   ssl_certificate_key  /etc/nginx/ssl_certs/server.key;

   ssl_stapling on;
   resolver XXX.XXX.XXX.XXX valid=300s;

   ssl_session_cache shared:SSL:1m;
   ssl_session_timeout  5m;

   ssl_ciphers  HIGH:!aNULL:!MD5;
   ssl_prefer_server_ciphers   on;


   location / {
      root   /usr/share/nginx/html;
      index  index.html index.htm;
}
}


server {
   listen       443 ssl;
   server_name  www2.example.com;

   ssl_certificate      /etc/nginx/ssl_certs/certs2.pem;
   ssl_certificate_key  /etc/nginx/ssl_certs/server2.key;

   ssl_session_cache shared:SSL:1m;
   ssl_session_timeout  5m;

   ssl_ciphers  HIGH:!aNULL:!MD5;
   ssl_prefer_server_ciphers   on;

   location / {
      root   /usr/share/nginx/html;
      index  index.html index.htm;
}
}
```

2. nginxの再起動

cybertrust

➢ nginxを再起動します。

設定を有効にするため、nginxの再起動を行ってください。

- **サーバー停止：/etc/init.d/nginx stop**
- **サーバー起動：/etc/init.d/nginx start**

※ご利用の環境によりましては、コマンドが異なる場合があります。

※「nginx　restart」コマンドで再起動を行った場合、正しく反映されない場合があります。

OCSP staplingの設定は以上で完了です。

3. OCSP staplingの確認（1/3）

cybertrust

- **OpenSSLのコマンドを利用し、通信の確認を行います。**
  - **openssl s_client -connect *example.com*:443 –status**

- OCSPの応答が含まれている場合には、以下の「OCSP Response Data」が出力されます。

```
openssl s_client -connect example.com:443 -status
CONNECTED(00000003)
OCSP response:
======================================
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C5D35618C8049B52D1BF6BCBEE037045AD93F8A7
    Produced At: Feb 11 21:25:51 2015 GMT
    Responses:
```

OCSP Response Statusが
successfulとなっていれば、
設定は正しく行われています。

3. OCSP staplingの確認（2/3）

- OCSP staplingに非対応のバージョン、サーバーソフトウェアおよび本設定が正しくない場合、OCSPの応答が含まれず、以下の「OCSP response: no response sent」が出力されます。

```
openssl s_client -connect example.com:443 -status
Loading 'screen' into random state - done
CONNECTED(00000170)
OCSP response: no response sent
```

OCSP Response StatusがNo response sentとなっていれば、設定は正しく行われていません。

3. OCSP staplingの確認（3/3）

- nginxからサイバートラストのOCSPサーバーへ接続が必要なため、以下とhttp通信が可能であることを確認してください。

■SureServer[2048bit] / SureServer[SHA-2]

http://ocsp.cybertrust.ne.jp/OcspServer

■SureServer EV[2048bit] / SureServer EV[SHA-2]

http://sureseries-ocsp.cybertrust.ne.jp/OcspServer

https://www.cybertrust.ne.jp

詳細は下記まで、お問い合わせください。
0120-957-975
電話受付時間 平日 9:00 ～ 18:00
servicedesk@cybertrust.ne.jp