開発技術全般 - 報告書 #1216
SSL更新手順書

2017/11/27 17:13 - 匿名ユーザー

ステータス:	新規	**開始日:**	2017/11/27
優先度:	通常	**期日:**	
担当者:		**作業時間の記録:**	0.00時間
カテゴリ:			

説明

SSL更新手順書
（更新：20171127）

（※新規購入と更新購入に作業の差は無い）
（※けれどSSLストア上での管理のしやすさ的に更新の方が良さそう）

root権限で行う

「作業ディレクトリを作って入る」
? cd /etc/httpd/conf.d/
? mkdir ssl_2
? cd ssl_2

「keyファイルを作る」
PWはそのサイトのrootパスワード（下）
? openssl genrsa -des3 -out XXXXX.com.key 2048

keyファイルが作られたことを確認する
? ls

「XXXXX.comでのメールの受信確認」
→自分のThunderbirdからadmin@XXXXX.comに送る
? vim /var/spool/mail/adminを確認
? vim /home/admin/Maildir/new（の可能性もある）

・上記の二つがダメな場合
\ cd /var/log
\ cat maillog ¦ grep "from=<送信元メールアドレス>"

「keyファイルからcsrファイルを作る」
? openssl req -new -key XXXXX.com.key -out XXXXX.com.csr
（keyファイル作成時に設定したパスワードを入れる）
（以下を入力していく）
:JP
:Tokyo(◆HS:Okinawa)
:Musashino-shi(◆HS:Naha-shi)
:i-hearts Inc.(◆HS:HS, Inc.)
:(空欄Enter)
:XXXXX.com
:admin@XXXXX.com

:(空欄Enter)

:(空欄Enter)

.keyと.csrファイルがあることを確認する
? ls -l

csrをコピーしておく
? more XXXXX.com.csr

「SSLストアでアクティベートする」
コモンネーム : XXXXX.com
サーバの種類 : ApacheOpenSSL

承認メールアドレス
myoffice@i-hearts.jp
office@happysmartphone.jp
（admin@XXXXX.comじゃない方が一元管理できる）

CSR
（先程コピーしたものを貼り付ける）

[ドメイン所有者情報]

（アイハーツ名義の場合）----------
I-HEARTS INC.
NODA
NORICHIKA
JP
180-0004
TOKYO
MUSASHINO-SHI
1-12-9 KICHIJOJI-HONCHO
0422-28-1600
●サポートサービスを利用する

（エイチエス名義の場合）----------
HS , INC
YAMAMOTO
YOSHIHARU
JP
902-0071
OKINAWA
NAHA-SHI
5-1-24 HANTAGAWA
098-831-7070
●サポートサービスを利用する

「確認メールを受け取る」
（※英語メールなので迷惑メールに分類されている可能性あり）
（※メール容量いっぱいで受け取れない可能性あり。そういう場合は削除して容量を空け、再送する）
→中のURLから英語サイトに飛ぶ
→メール内の文字列をコピペして、申請を完了させる

「数十分後?（まれに2営業日後）に届くメールからcrtとcerファイルを作る」

（※メール文面に書かれている場合と、添付ファイルの場合があるらしい）

-----BEGIN CERTIFICATE-----
（中略）
-----END CERTIFICATE-----

これが1ブロックと3ブロック繋がってるもの、2つのまとまりになっているはず。
上をXXXXX.com.crtファイルとして保存。
下3ブロックをまとめてそのままXXXXX.com.cerとして保存する。

「秘密鍵からパスフレーズを外しておく」（apache再起動時にpassフレーズの入力を求められないように）
openssl rsa -in XXXXX.com.key -out XXXXX.com.nopass.key

「リネームで反映作業をする」
? cd ..
? pwd （→/etc/httpd/conf.dなど、sslとssl_2フォルダがある階層だと確認）
? mv ssl ssl_20171031
? mv ssl_2 ssl

「Apacheを再起動して反映させる」
/etc/init.d/httpd restart

・restartが失敗した場合
/etc/httpd/conf.dの直下にあるssl.confの設定が以下のようになっているか確認する

SSLCertificateFile /etc/httpd/conf.d/ssl/XXXXX.com.crt
SSLCertificateKeyFile /etc/httpd/conf.d/ssl/XXXXX.com.nopass.key
SSLCertificateChainFile /etc/httpd/conf.d/ssl/XXXXX.com.cer
SSLCACertificateFile /etc/httpd/conf.d/ssl/XXXXX.com.cer

・restartが成功した場合
「WebとAndroidからSSLがあることを確認（期限も確認）」

↓
矢野さんに確認して頂いて完了！

「Aipo更新」
SSL期限を更新する。
（※注意！開始日から変更しないと、肝心の有効期限が大幅にずれてしまう）
（※開始日を有効期限の3週間前にして、終了日を有効期限の日にする）