cybertrust

SureServer/SureServer EV

PEM⇔PKCS#12

ファイル形式変換手順書

Version 1.1

PUBLIC RELEASE

2016/12/15

改訂履歴

日付	バージョン	内容
2012/06/22	1.0	初版リリース
2016/12/15	1.1	「はじめに」の記述内容を修正

目次

はじめに

【！】本手順書をご利用の前に必ずお読みください

本ドキュメントは、サイバートラストの SSL サーバ証明書のファイル形式を変換する手順について解説するドキュメントです。

なお、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。

1. ファイル形式の変換手順について

OpenSSL を用いて PEM 形式(テキストファイル)⇔PKCS#12 形式(pfx ファイル)間の変換する手順について解説します。

1.1. PKCS#12 形式→PEM 形式

OpenSSL を用いて pfx ファイルから SSL サーバ証明書ファイルと秘密鍵ファイルを出力します。

A) OpenSSL で以下のコマンドを入力します。

※コマンド入力の際は、パスフレーズの入力が必要となるため、pfx ファイルのエクスポートの際に設定したパスフレーズを入力してください。

■ SSL サーバ証明書ファイル

openssl pkcs12 -in pfx ファイル名 -clcerts -nokeys -out 任意のサーバ証明書ファイル名

例)pfx ファイル「backup.pfx」から SSL サーバ証明書ファイル「SureServer.cer」を作成

openssl pkcs12 -in backup.pfx -clcerts -nokeys -out SureServer.cer

※指定するサーバ証明書ファイルの拡張子は、「txt」、「.pem」、「.cer」、「.crt」のいずれかとしてください。

※SSL サーバ証明書ファイルはダウンロードサイトや申請サイトより何度でもダウンロード可能です。

■ 秘密鍵ファイル

openssl pkcs12 -in pfx ファイル名 -nocerts -out 任意の秘密鍵ファイル名

例)pfx ファイル「backup.pfx」から秘密鍵ファイル「server.key」を作成

openssl pkcs12 -in backup.pfx -nocerts -out server.key

※指定する秘密鍵ファイルの拡張子は、「.txt」、「.pem」、「.key」、のいずれかとしてください。

【！】セキュリティ上の観点から秘密鍵ファイルの暗号化を推奨いたしますが、やむを得ない場合は、以下のコマンドで暗号化をせずに変換を行ってください。

■コマンド入力

openssl pkcs12 -in pfx ファイル名 -nocerts -nodes -out 任意の秘密鍵ファイル名

B) 指定したファイル名で SSL サーバ証明書ファイルと秘密鍵ファイルが作成されます。

以上で pfx ファイルから PEM 形式の SSL サーバ証明書ファイルと秘密鍵ファイルへの変換は完了です。

1.2. PEM 形式→PKCS#12 形式

OpenSSL を用いて PEM 形式の SSL サーバ証明書ファイルと秘密鍵ファイルから pfx ファイルへ変換を行います。

A) OpenSSL で以下のコマンドを入力します。

■ コマンド入力

openssl pkcs12 -export -inkey 秘密鍵ファイル名 -in SSL サーバ証明書ファイル名 -out 任意の pfx ファイル名

例）秘密鍵ファイル「server.key」と SSL サーバ証明書「SureServer.cer」から pfx ファイル「backup.pfx」を作成

openssl pkcs12 -export -inkey server.key -in SureServer.cer -out backup.pfx

※秘密鍵ファイル名、および、SSL サーバ証明書ファイル名はご利用のファイル名を指定してください。
※指定する pfx ファイルの拡張子は、「.pfx」としてください。
※事前に SSL サーバ証明書ファイルと秘密鍵ファイルのバックアップを行ってください。

B) 指定した pfx ファイル名で PKCS#12 形式の pfx ファイルが作成されます。

以上で PEM 形式の SSL サーバ証明書ファイルと秘密鍵ファイルから pfx ファイルへの変換は完了です。