



つかえるITを、世界から。

SSLサーバー証明書の実用手順

株式会社オーシャンブリッジ

SSL-211012

- ISL Conference Proxyの初期設定ではISL側で発行した自己証明書（SSLサーバー証明書）が適用されています。
- ISL Conference Proxyをインターネット上に公開し、外部のユーザーが利用する際は、第三者機関が作成したSSLサーバー証明書の適用をお勧めいたします。

※SSLサーバー証明書：認証局(CA：Certificate Authority)が発行するもので、通信しようとする相手の身元を発行元の認証局に照会し、確認することができます。証明書の内容はSSL通信を開始する際にWebブラウザで表示することができ、相手の身元を表す情報と、照会した認証局の情報を確認できます。

1. SSLサーバー証明書を発行する会社を決めます（セコムトラストシステムズ社、シマンテック社など）
2. 発行会社の手順に沿った形でCSRファイルを作成し、発行会社に送付します
その後、発行会社から証明書が送られてきます
3. ISL Conference ProxyにSSLサーバー証明書を適用します
4. SSLサーバー証明書が適用されていることを確認します

※CSRとは「Certificate Signing Request」の頭文字を取ったもので、認証局に対し、SSLサーバ証明書への署名を申請する内容です。
CSRファイルには「公開鍵」とその所有者情報、及び申請者が対応する秘密鍵を持っていることを示すために申請者の署名が記載されています。

※SSLサーバー証明書は発行会社によって作成手順が異なります

1. SSLサーバー証明書を発行する会社について

- SSLサーバー証明書を発行できる会社であれば、どの会社を選んでいただいても構いません。
- ISL Onlineのクラウドライセンスでは、以下の証明書を使用しています。
 - COMODO社 : <https://comodo.jp/>
- オンプレミスライセンスのSSLサーバー証明書の適用実績がある会社は以下の通りです
 - セコムトラストシステムズ社 : <https://www.secomtrust.net/service/pfw/>
 - COMODO社 : <https://comodo.jp/>

2. 証明書の作成までの流れ（その1）

- SSLサーバー証明書を発行する会社の手順に沿った形でCSRファイルを作成して、証明書を受領してください。
- セコムトラストシステムズ株式会社の場合、以下のような流れになります。

▼お申し込みの流れ

<https://www.secomtrust.net/service/pfw/apply/sr/>



2. 証明書の作成までの流れ（その2）

- セコムトラストシステムズ株式会社の場合の流れをご説明いたします。（2019/02/14時点）
 - OpenSSLのインストールを実行してください。
▼OpenSSL
<https://slproweb.com/products/Win32OpenSSL.html>
※ご利用のOS（32bit版/64bit版）対応の完全版（Lightと記載のないもの）を選択してください
※ISL Conference ProxyをインストールしたPC以外でもCSRファイルの作成は可能です
 - OpenSSLを使用して、CSRファイルの作成を行ってください。手順については以下のWEBページをご参照ください。
▼セコムトラストシステムズ社の場合
https://www.secomtrust.net/service/pfw/apply/ev/1_2_openssl.html
 - お申し込みを行ってください。（申し込みの中で手順2で作成したCSRファイルを使用します）
※SHA-2に対応した「セコムパスポート for Web SR 3.0」の購入をお勧めしております
▼お申し込みの流れ
<https://www.secomtrust.net/service/pfw/apply/sr/>

※申込時のサーバタイプは「Apache」、
サーババージョンは「2.2」を選択してください

証明書新規申請 基本情報入力画面

お申込の基本情報を入力してください。
複数の証明書をお申込いただく場合、2通目以降の証明書も同様の方法でお申込ください。
この背景色の項目は入力必須です。

▶ 申込区分	新規
▶ 有効期間	<input type="text"/>
▶ サーバタイプ	Apache
▶ サーババージョン	2.2

サーバのバージョンを入力してください。
サーバタイプが「その他」の場合は、サーバタイプも入力してください。

3. SSLサーバー証明書の適用方法について（その1）

1. ISL Conference Proxyの管理画面（http://localhost:7615/conf）にログインします
2. 左側メニューの[Advanced]-[File storage]を選択します
3. [Private]タブを選択します
4. [Upload file]横の[ファイルを選択]ボタンから鍵ファイル、SSLサーバー証明書ファイル、（中間証明書ファイル）を選択し、[Upload]をクリックします
※ファイルの回数分繰り返してください
※証明書ファイルは、文字コードは「UTF-8」、改行コードは「LF」を選択してください
※ISL Conference Proxyのインストールフォルダ以下のフォルダ[objects]内にアップロードされます

File storage

Public **Private** Private (local) Programs Plugins Actions Translations Mod...

Upload file:

Extract ZIP file: Yes

Select	File	Bytes	Download	Content	Ver. on -1
<input type="checkbox"/>	software_policy.xml	37477	Click	[<softwarePolicy> <scopes> ...]	3

3. SSLサーバー証明書の適用方法について（その2）

5. 左側のメニュー内から[General]を選択し、以下の項目のチェックボックスを外し、変更後、画面下の[Save]をクリックしてください

※使用するポートを変更した場合、ISL Conference Proxyの再起動が必要です

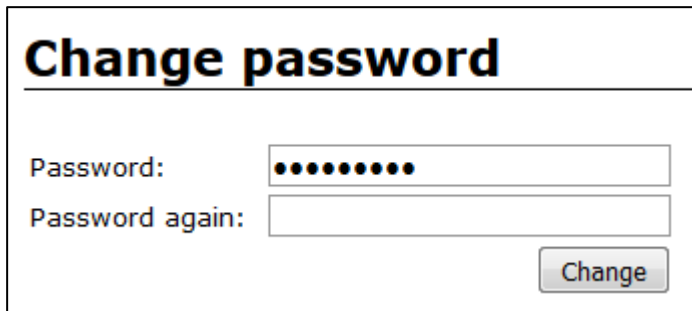
- [HTTPT ports] : 「443」 のみにする場合は変更してください
- [HTTPT use SSL] : 「Yes」 に変更してください
- [HTTPT SSL certificate] : 証明書ファイル（「objects/sample.cer」 など）を指定してください
- [HTTPT SSL key] : CSRファイルの作成時に使用した鍵ファイル（「objects/sample.key」 など）を指定してください
- [HTTPT SSL certificate chain] : 中間証明書ファイル（「objects/chain.crt」 など）がある場合、指定してください

※中間証明書ファイルがない場合、設定は不要です

<input type="checkbox"/>	HTTPT ports:	<input type="text" value="443"/>	Local override
<input type="checkbox"/>	HTTPT use SSL:	<input type="text" value="Yes"/>	Local override
<input type="checkbox"/>	HTTPT SSL certificate:	<input type="text" value="objects/sample.cer"/>	Local override
<input type="checkbox"/>	HTTPT SSL key:	<input type="text" value="objects/sample.key"/>	Local override
<input checked="" type="checkbox"/>	HTTPT SSL key passphrase:		Local override
<input type="checkbox"/>	HTTPT SSL certificate chain:	<input type="text" value="objects/chain.crt"/>	Local override

6. 左側のメニュー内から[General]を選択し、以下の項目のチェックボックスを外し、変更後、画面下の[Save]をクリックしてください（ISL Conference Proxyの再起動は不要です）

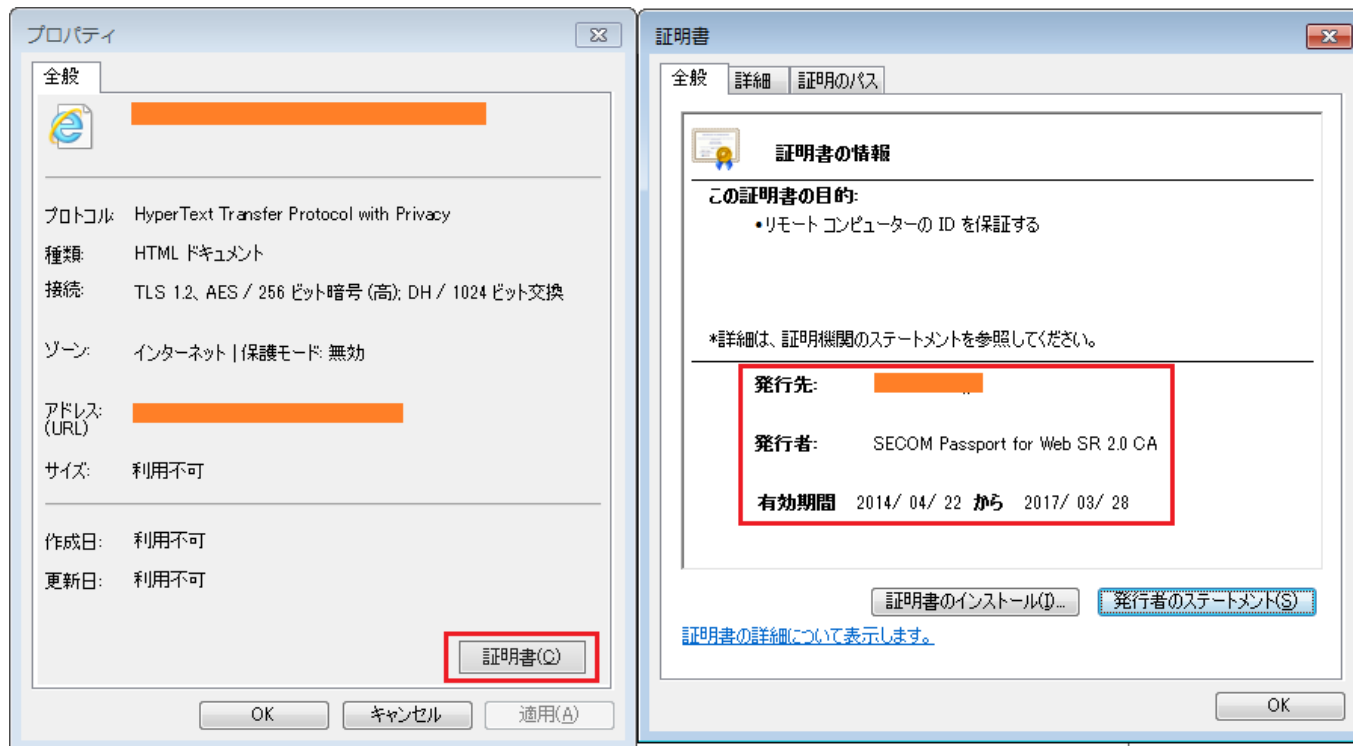
- [HTTPT SSL key passphrase]：鍵ファイル作成時にパスフレーズを指定した場合、パスフレーズを入力してください
※保護していない場合、設定は不要です



7. 左側メニュー内から[Security]を選択し、項目名「Redirect HTTP to HTTPS for all user web pages:」のチェックボックスを外し、画面下の[Save]をクリックしてください
※この設定を行うことで、オンラインページへのアクセスは全てSSL通信となります

4. SSLサーバー証明書の適用を確認する手順

1. ISL Conference Proxyのログインページ (https://<サーバーのIPアドレスまたはホスト名:ポート番号>/) にアクセスします
2. ページのプロパティを選択後、「証明書」をクリックして、発行先、発行者、有効期間が正しいことを確認してください



- ISL Conference Proxy 4.4.1947.98以降では、以下のようなSSLサーバー証明書の期限に関する通知メールを受信できます（メールサーバーの設定を行う必要があります）。
 - 2020-06-10T06:59:38Z [<サーバーのホスト名>/confproxy_server/4972] certificate expired AKV LOG_SEVERITY="alert" LOG_SUBSYSTEM="core_cert_expiry_check" CERTEXP_FILE="https_cert_expiry_check" CERTEXP_VALIDUTC="1" CERTEXP_VALIDFROM="2016-09-27" CERTEXP_VALIDTO="2018-02-15" CERTEXP_MSG_TXT="HTTPS certificate expiry warning"
- 通知メールは、以下のタイミングで送信されます。
 - 期限日の60日前
 - 期限日の30日前
 - 期限日の15日前より毎日
- 通知メールは、証明書の有効期間が1/3以下となるタイミングから有効になります。
例：
 - 証明書の有効期間が90日の場合： 「期限日の30日前」 から通知メールが送信されます
 - 証明書の有効期間が365日の場合： 「期限日の60日前」 から通知メールが送信されます



つかえるITを、世界から。

製品、サービス、その他ご質問やご不明な点などございましたら
下記までお問い合わせください

体験版ユーザー様はこちら : sales@oceanbridge.jp

ご購入ユーザー様はこちら : isl-support@oceanbridge.jp

株式会社オーシャンブリッジ

〒107-0051 東京都港区元赤坂一丁目5番12号 住友不動産元赤坂ビル7階

www.oceanbridge.jp