OceanBridge

つかえるITを、世界から。

SSLサーバー証明書の適用手順

株式会社オーシャンブリッジ
2017年4月4日

SSL-170404

SSLサーバー証明書について

- 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。

© 2017 OceanBridge Inc. All Rights Reserved.

SSLサーバー証明書の適用までの流れ

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

© 2017 OceanBridge Inc. All Rights Reserved.

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/

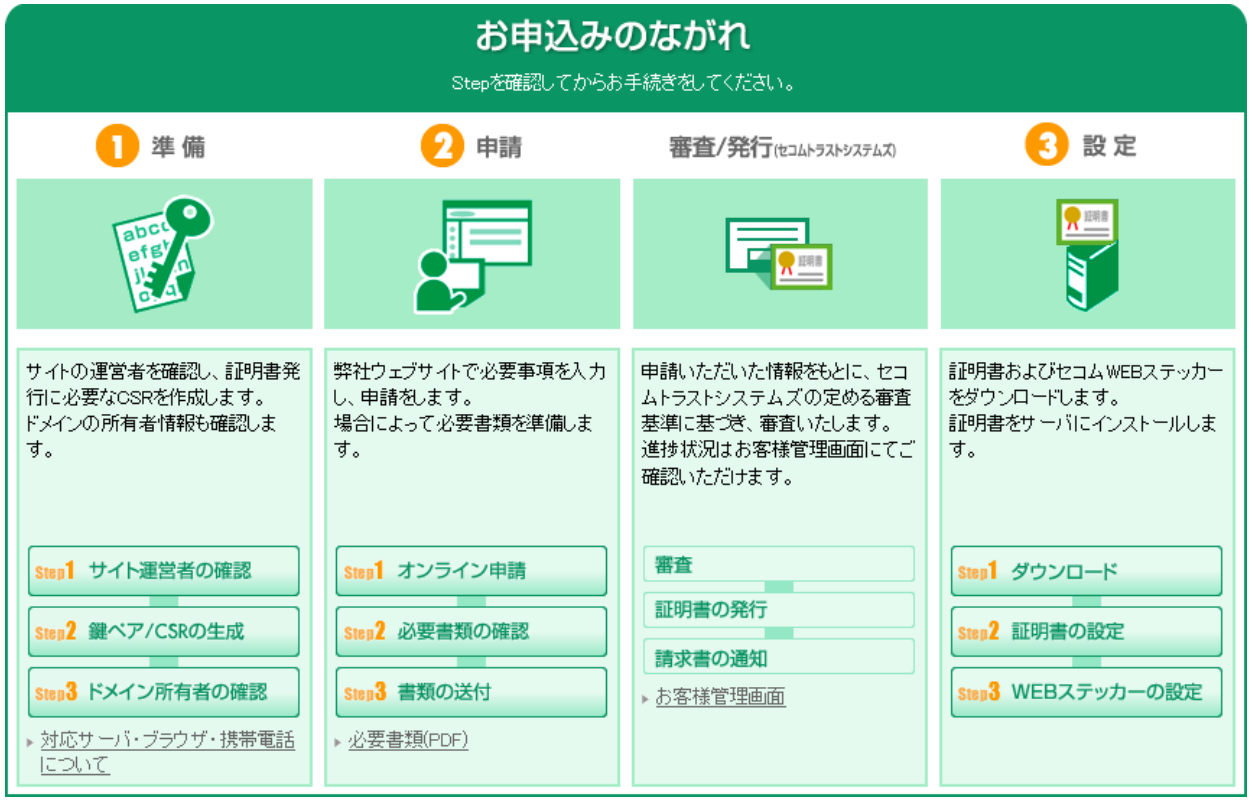
- オンプレミスライセンスのSSLサーバー証明書の適用実績がある会社は以下の通りです
  - セコムトラストシステムズ社：https://www.secomtrust.net/service/pfw/
  - COMODO社：https://comodo.jp/

© 2017 OceanBridge Inc. All Rights Reserved.

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/



© 2017 OceanBridge Inc. All Rights Reserved.

2. 証明書の作成までの流れ（その2）

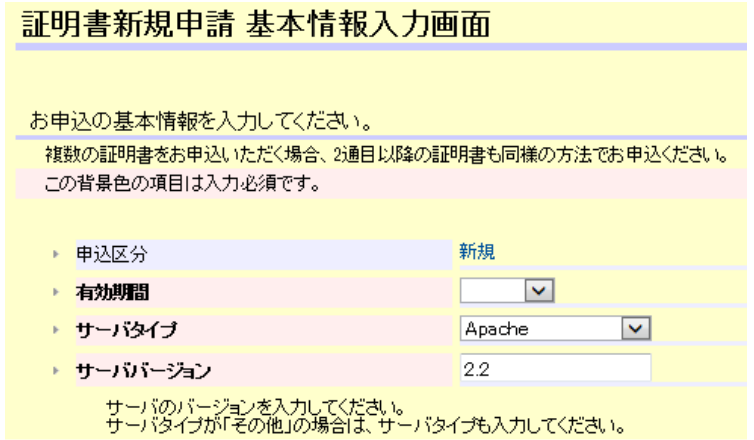
■ セコムトラストシステムズ株式会社の場合の流れをご説明いたします。（2017/03/28時点）

1. OpenSSLのインストールを実行してください。
   ▼OpenSSL
   http://slproweb.com/products/Win32OpenSSL.html
   ※64bit OSの場合、 Win64 OpenSSL v1.1.0e（33MB Installer）をご利用ください
   ※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

2. 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

3. 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



© 2017 OceanBridge Inc. All Rights Reserved.

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

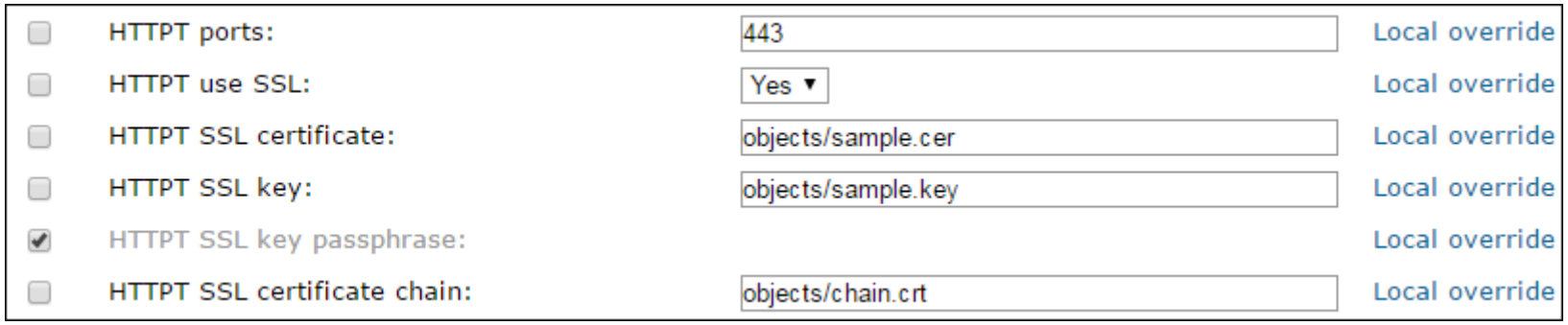
4. [Upload file]横の「参照」ボタンから鍵ファイル、SSLサーバー証明書ファイル、（中間証明書ファイル）を選択し、「Upload」をクリックします
   ※ファイルの個数分繰り返してください
   ※証明書ファイルは、文字コードは「UTF-8」、改行コードは「LF」を選択してください
   ※ISL Conference Proxyのインストールフォルダ以下のフォルダ[objects]内にアップロードされます

© 2017 OceanBridge Inc. All Rights Reserved.

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、画面右下の「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



© 2017 OceanBridge Inc. All Rights Reserved.

OceanBridge

3. SSLサーバー証明書の適用方法について（その3）

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、画面右下の「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

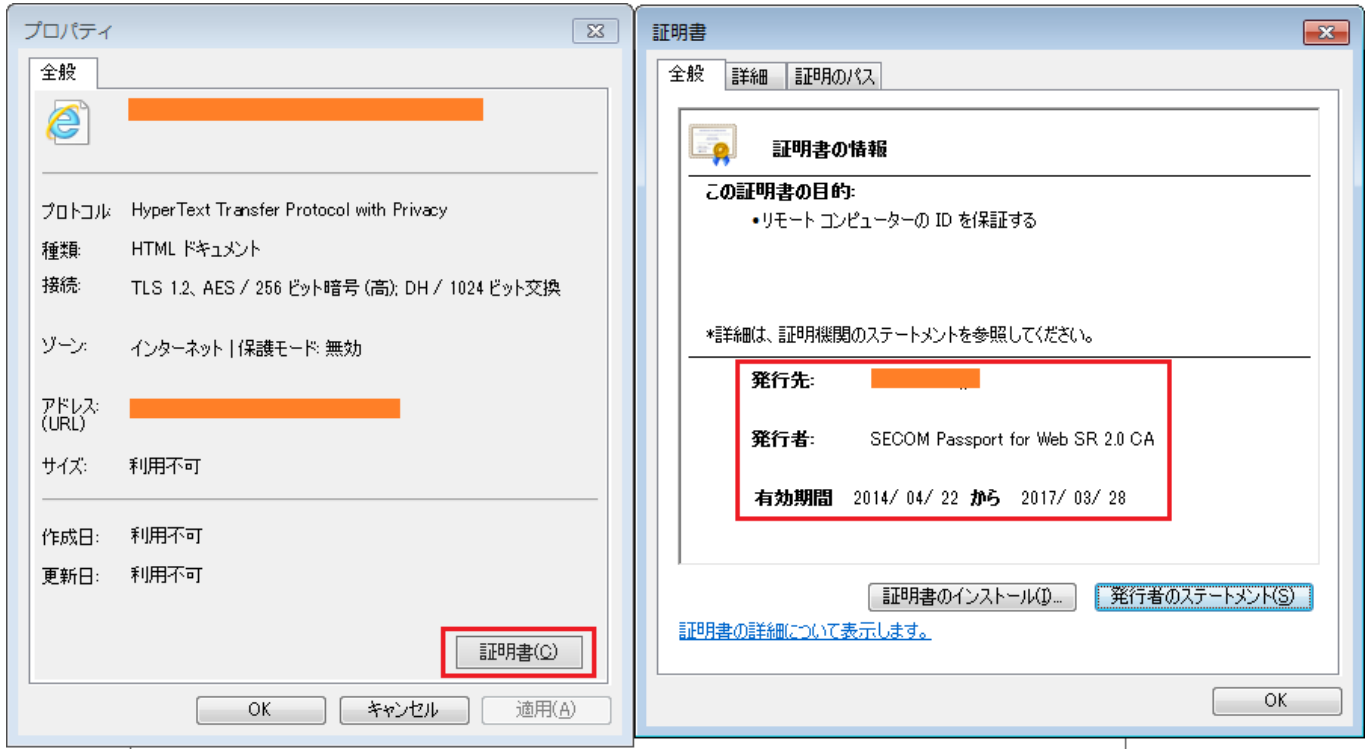
7. 左側メニュー内から[Security]を選択し、項目名「Force SSL for all user web pages:」のチェックボックスを外し、画面右下の「Save」をクリックしてください
   ※この設定を行うことで、プロダクトログインページへのアクセスは全てSSL通信となります

© 2017 OceanBridge Inc. All Rights Reserved.

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”/）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



© 2017 OceanBridge Inc. All Rights Reserved.

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

isl-support@oceanbridge.jp

株式会社オーシャンブリッジ

150-0043　東京都渋谷区道玄坂1-20-8　寿パークビル7F
www.oceanbridge.jp