

# SSL 登録手順 簡易マニュアル

独自 SSL 機能について解説します。

本機能は、お客様が作成した CSR 鍵を使用して取得された SSL サーバ証明書（独自 SSL）をサーバに設定し、Web サイトとサイト来訪者の通信を暗号化することができます。

独自 SSL ご利用までの大きな流れは以下となります。

## ① CSR の作成

### 共有ホスティング サイトマネージャー

TOP > サイトマネージャー > Web&FTP管理 > 独自SSL > CSR・秘密鍵の作成

すべて開く | すべて閉じる

インフォメーション

サイト管理

ドメイン  
ディスク容量  
adminアカウント管理  
サーバー情報

**WEB & FTP 管理**

Webユーザ管理  
アクセス制御  
CGI管理  
WordPress  
ログファイル  
独自SSL  
CSR・秘密鍵の作成  
SSLサーバ証明書の設定  
SSLサーバ証明書の削除  
SSLサーバ証明書のキーペア取得  
HTTP/HTTPSのディレクトリ統合  
AnonymousFTP  
Webメール管理  
MySQL管理

メール管理

メールユーザ管理  
メールリスト管理  
ウイルスチェック  
迷惑メールフィルタ管理  
メール送信状況確認

FTPソフト設定例

メールソフト設定例

オンラインマニュアル

お問い合わせ

## CSR・秘密鍵の作成

SSLに対応したホームページを作成する場合、CSR(証明書署名要求)を作成し、認証局にご提出いただけます。

すべての項目は**半角英数字**で入力してください。  
日本語や全角英数字は使用できません。

鍵長	2048ビット
コモンネーム (Common Name)	https:// (ドメイン名) / コモンネームとは、SSLで接続可能なホームページのURLの一部として使用される名前です。 WebブラウザでSSLのホームページにアクセスする時に、ドメイン名の前に www. を付ける場合は(例:https://www.example.com/)、コモンネームを www.example.com としたCSRを作成してください。 なお、ご申請のコモンネームにより、サーバー証明書の証明対象となるURLが異なります。 認証局によっては www. を先頭にも含むコモンネームを指定すると、www. を含まないURL (例:https://example.com/)もサーバー証明書の証明対象にできる場合があります。 事前にSSL認証局へご確認の上、コモンネームを指定ください。
組織名 (Organization)	(組織名) 会社・学校・その他の団体など、任意の組織名を入力してください。
部門名 (Organization Unit)	SSLの証明書を使用する部署またはグループの名前を入力してください。 この項目は入力しなくても問題ございません。
国名 (Country)	JP 選択する国名はISOの国別記号で表示されています。 日本の国別記号は「JP」ですので通常は変更する必要はございません。
都道府県名 (State or Province)	(都道府県名) 東京都の場合は Tokyo、神奈川県の場合は Kanagawa のように、「都」や「県」を省いた都道府県名を半角英字で入力してください。 ただし、北海道だけは「道」を省かず Hokkaido と入力してください。
地域名 (Locality)	(地域名) 千代田区の場合は Chiyoda-ku、川崎市の場合は Kawasaki-shi のように、市区町村名を半角英字で入力してください。

<注意>  
「作成」ボタンを押した後、ページの表示に時間がかかる可能性がございますが、ページを移動せずにそのままお待ちください。

作成 | リセット

- お客様の組織名、所在地、サーバの URL (コモンネーム) などを記入し、[作成ボタン] をクリックしてください。
- CSR は、ダウンロード時に指定したフォルダに保存されます。「メモ帳」などのテキスト・エディターで作成した CSR のファイルを開き、中身を確認してください。
- ここで作成した CSR (証明書署名要求) と受付番号の組み合わせは、SSL をサーバへ設定するとき必要となります。CSR ファイルは SSL の設定が完了するまで必ず大切に保管してください。



#### ④ 取得した証明書をサーバへ設定

共有ホスティング サイトマネージャー

TOP > サイトマネージャー > Web&FTP管理 > 独自SSL > SSLサーバ証明書の設定

### SSLサーバ証明書の設定

お客様にて取得されたSSL証明書を、サーバに設定します。  
既にサーバへSSLが設定されている場合は証明書情報を上書きします。

以下の入力欄にそれぞれ証明書の内容を貼り付けてください。  
証明書情報には「BEGIN CERTIFICATE」「END CERTIFICATE」の行も含めます。

入力例)

```
-----BEGIN CERTIFICATE-----
:
-----END CERTIFICATE-----
```

■SSL証明書:

※証明書は絶対に編集(加工)しないでください。  
念の為、余分な空白(半角/全角スペース)や改行が含まれていないことをご確認ください。

■中間証明書:

※証明書は絶対に編集(加工)しないでください。  
念の為、余分な空白(半角/全角スペース)や改行が含まれていないことをご確認ください。  
※中間証明書が正しく設定されていないと、SSL接続の際に【セキュリティの警告】が表示されます。  
中間証明書がない場合は、発行元認証局にご確認ください。  
※複数ある場合は続けて貼り付けてください。

例)

```
-----BEGIN CERTIFICATE-----
:
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

受付番号の登録 (サイトマネージャーでCSRを作成した場合)  
 秘密鍵を入力 (認証局において秘密鍵およびCSRを作成した場合等)

■受付番号:  
認証局に申請する時に「CSR・秘密鍵作成」で作成、ダウンロードした「csr.txt」に記載されている受付番号 (14桁の数字) 入力してください。

設定 入力内容をリセット

SSL 証明書と中間証明書をコピー＆ペーストでそれぞれの欄に入力します。

秘密鍵の入力については基本的に「受付番号から秘密鍵を登録する」を選択し、[ ■ 受付番号 ] 欄に受付番号を入力するようにしてください。

#### 【受付番号について】

受付番号は「CSR の作成」の段階で作成し、SSL サーバ証明書の申請時に利用した CSR のファイルから取得してください。

\* SSL サーバ証明書の申請時に利用した CSR と、その CSR ファイルに記載されている受付番号の組み合わせが一致している必要があります。

\* 受付番号 (CSR ファイル) を紛失された場合、お手数ではございますが今一度「CSR の作成」で新しい CSR と受付番号の組み合わせを取得し、新しい CSR で SSL サーバ証明書の「再発行」を行ってから証明書の設定に進んでください。