

ドメイン/Webサービス

SSLサーバ証明書（SureServer）

設定の手引き

2021年4月版

<https://dw.alpha-prm.jp/support/ssl/>

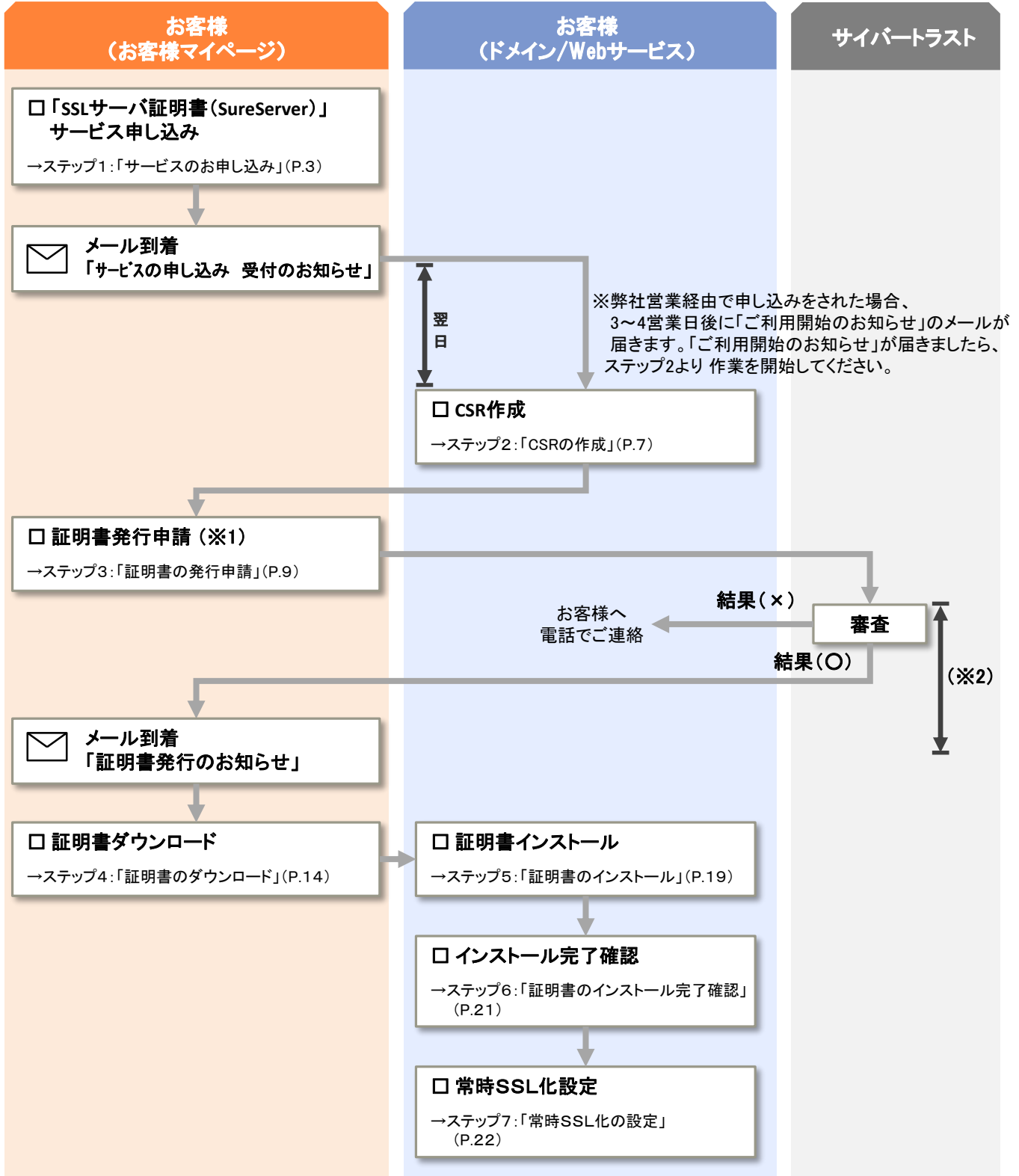
作業手順	2
ステップ 1 : サービスのお申し込み	3
ステップ 2 : CSRの作成	7
ステップ 3 : 証明書の発行申請	9
ステップ 4 : 証明書のダウンロード	14
ステップ 5 : 証明書のインストール	19
ステップ 6 : 証明書のインストール完了確認	21
ステップ 7 : 常時SSL化の設定（事前確認）	22
ステップ 7 : 常時SSL化の設定（.htaccessなし）	25
ステップ 7 : 常時SSL化の設定（.htaccessあり）	27

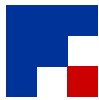
- 本書は2021年4月時点での情報を元に作成しています。
- 本書の内容の一部または全部を無断転載することは禁止されています。
- 本書の内容の複製または改変などを当社の許可なく行うことは禁止されています。
- 本書の内容に関しては、将来予告なく変更することがあります。
- 本書で取り上げたソフトウェアの変更、ホームページの構成・デザイン・内容の変更、それに伴って発生する損失、逸失利益に関し、当社はいかなる責任も負いかねます。
- 本書に記載されている社名および商品名は、各社の商標または登録商標です。



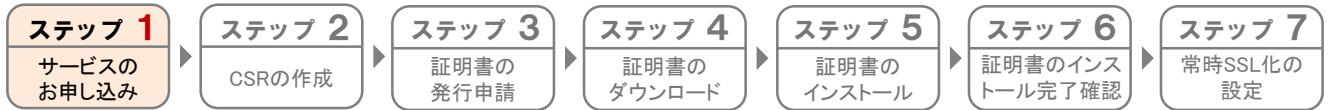
作業手順

「SSLサーバ証明書(SureServer)」をご利用される場合、以下の作業が必要になります。
お客様の作業が終わりましたら、チェックボックスにチェックを入れてください。





ステップ1: サービスのお申し込み



お客様マイページから「SSLサーバ証明書(SureServer)」を申し込みます。

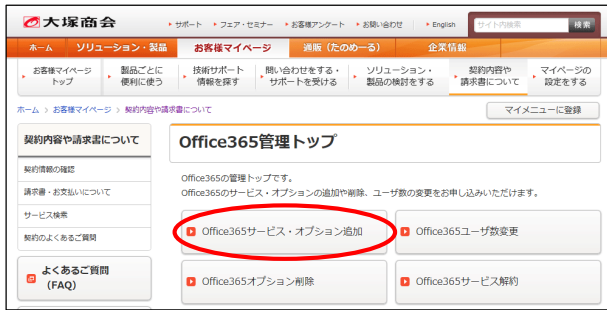
1 ブラウザを起動し、以下URLにアクセスします。
<https://mypage.otsuka-shokai.co.jp/keiyaku>

2 必要事項を入力し、「ログイン」をクリックします。

ログインID	ドメイン/Webサービスの「お客様番号(旧契約マイページのID)」を入力
パスワード	「お客様マイページ(旧契約マイページ)のパスワード」を入力

3 「Office365管理」をクリックします。

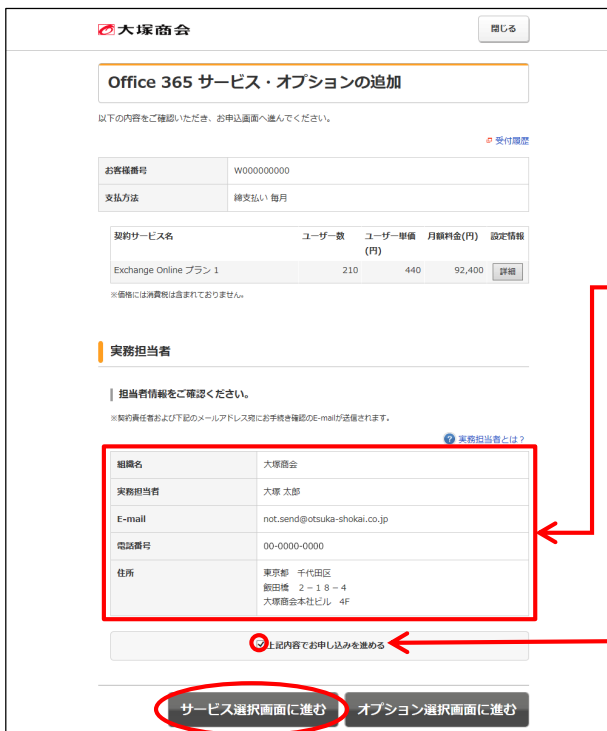
4 「Office365サービス・オプション追加」をクリックします。



5 「サービス・オプションを追加する」をクリックします。



6 以下を確認・選択し、「サービス選択画面に進む」をクリックします。



契約責任者および実務担当者メールアドレス宛にお手続き確認のE-mailが送信されます。

表示された内容を確認し、「上記内容でお申し込みを進める」をチェックします。

大塚商会

閉じる

Office 365 サービス追加

追加サービス選択

ユーザー追加

確認

完了

こちらからサービスの追加ができます。

お客様情報

※ 画面省略 ※

追加するサービス・オプション

サービス名	月額料金(円)
☐ Exchange Online プラン 2	870
☐ Exchange Online Kiosk	220
☐ Office 365 ProPlus	1,480
☐ Office 365 ProPlus サポートなし	1,310

※ 画面省略 ※

☐ トライアル Power BI Pro	0
☐ Office 365 プランE5	3,590
☒ SSLサーバ証明書	

※ サービスの設定時間は、9時から21時となります。21時以降のお申し込みにつきましては、翌日9時以降に設定処理が行われます。

※ サービスの設定は、お申し込み後30分で完了しますが、サーバーの状態などによっては遅れる場合があります。

※ 価格には消費税は含まれておりません。

戻る

次へ

7 以下を確認・選択し、「次へ」をクリックします。

「SSLサーバ証明書」を選択します。

大塚商会

閉じる

サービスの契約

サービスの選択

確認

完了

こちらからオプションの追加ができます。

お客様番号

W0000000000

新しく契約するサービス

サービス名

SSLサーバ証明書月額サービス

サービス	初期費用(円)	月額料金(円)
☒ SSLサーバ証明書 (SureServer)	---	3,800
☐ EV SSLサーバ証明書 (SureServer)	---	4,800

ドメイン

必須

daodao.jp

※ 価格には消費税は含まれておりません。

※ 価格はお問い合わせください。

戻る

次へ

8 契約するサービスを選択し、「次へ」をクリックします。

大塚商会 閉じる

サービスの契約

追加オプション選択 確認 完了

こちらからオプションの追加ができます。

お客様情報

お客様番号: W000000000

新しく契約するサービス

サービス名: SSL証明書月課サービス

追加するサービス

契約サービス名: SSLサーバ証明書 (SureServer)

ドメイン

ドメイン名: demodemo.jp

今回の追加金額(税別)	(初期費用)	0円
	(月額料金)	3,800円

※価格には消費税は含まれておりません。

約款の表示

☒ 約款・重要説明事項に同意する※

※お客様にて証明書の申請・更新が必要であること、相場によってお申し込み可能なメニューが異なるなど、本サービスには重要な案内がございますので、重要説明事項を必ずご確認ください。
また、お申し込み後、利用開始までの流れなど記載した受付メールを送付しますのでご確認ください。

変更申込時、受付完了メールが
ご契約責任者の連絡先E-mailアドレス not.send@otsuka-shokai.co.jp
実務担当者の連絡先E-mailアドレス not.send@otsuka-shokai.co.jp に送信されます。
※大塚ID管理者にも送付されます。

戻る 申し込み

9 表示された内容を確認し、「申し込む」をクリックします。

表示された内容を確認し、「約款・重要説明事項に同意する」をチェックします。

大塚商会 閉じる

SSL証明書の申込

入力 確認 完了

 サービス追加のお申し込みを受け付けました。
お申込番号は20170303000001です。

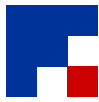
確認のため、ご契約責任者の連絡先E-mailアドレス not.send@otsuka-shokai.co.jp と
実務担当者の連絡先E-mailアドレス not.send@otsuka-shokai.co.jp へメールを配信しております。
※大塚ID管理者にも送付されます。

サービスの追加登録をありがとうございました。

ウィンドウを閉じる

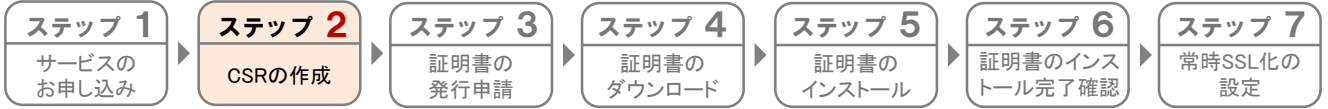
10 申し込みの完了画面が表示されます。
「ウィンドウを閉じる」をクリックし、お客様マイページからログアウトします。

以上で、ステップ1の作業は終了です。



ステップ2:CSRの作成

❗ こちらの作業は、ステップ1:「サービスのお申し込み」(P.3)を行った翌日以降に開始してください。



ドメイン/Webサービスの管理者機能からCSRを作成します。



1 ブラウザを起動し、ドメイン/Webサービス会員サイトにアクセスします。

<https://dw.alpha-prm.jp/>

「ログイン」をクリックします。



2 必要事項を入力し、「ログイン」をクリックします。

メールアドレス	「管理者メールアドレス(ログインID)」を入力
パスワード	「管理者パスワード」を入力



3 「管理者機能」をクリックします。

[illegible]

4 「Web」タブをクリックし、「独自SSL管理」→「CSR作成」をクリックします。

！ サーババージョン2環境へ切替え中のお客様
以下の手順で、サーババージョン2環境にて、CSRを作成してください。

「Web」タブをクリックし、「サーババージョン2」→「独自SSL管理」→「CSR作成」をクリックしてください。

CSR情報

公開経路 2048bit RSA
☒ https://www.aveb-pr.m.p
☐ https://aveb-pr.m.p

※ コモンネーム (Common Name)
 ※ 組織名 (Organizational Name) OTSUKA CORPORATION
 部門名 (Organizational Unit) Public Relations Dept
 ※ 国名 (Country) JP
 ※ 都道府県名 (State or Province) Tokyo
 ※ 市区町村名 (Locality) Chiyoda-ku

※ は必須入力項目です。

- ・ コモンネーム
 ・ 契約されたサブドメインなどでコモンネームに“www”を付与しない場合は、下記の「契約ドメイン名」を選択してください。
 設定可能なSSLサーバ証明書は、どちらか一方のコモンネームのみとなります。
 (例)https://sub.example.com
- ・ 組織名
 2文字以上44文字以下で指定してください。
 証明書が対応している場合、日本語での表記も可能です。(※)
 (例)OTSUKA CORPORATION (例)株式会社 大塚商会
- ・ 部門名
 84文字以下で指定してください。
 証明書が対応している場合、日本語での表記も可能です。(※)
 (例)Public Relations Dept (例)広報部
- ・ 国名
 国名(ISO国別記号)を指定してください。日本の国別記号は“JP”です。
- ・ 都道府県名/市区町村名
 128文字以下で指定してください。
 証明書が対応している場合、日本語での表記も可能です。(※)
 (例)Tokyo/Chiyoda-ku (例)東京都/千代田区

(※)日本語表記について
 日本語表記は44文字以下で指定してください。
 日本語表記が可能な対象項目や登録方法が各認証局の証明書により異なります。
 詳しくはお客様がご利用の各認証局にご確認ください。

作成

5 必要事項を入力し、「作成」をクリックします。

公開鍵長	公開鍵長 (2048bitRSA) が表示されます。
コモンネーム (Common Name)	コモンネームを選択します。
組織名 (Organizational Name)	組織の正式名称を入力します
部門名 (Organizational Unit)	部門名を入力します。
国名 (Country)	日本のISO国別記号「JP」が表示されます。
都道府県名 (State of Province)	都道府県名を入力します。
市区町村名 (Locality)	市区町村名を入力します。

！ 組織名などは日本語での表記も可能です

組織名、部門名、都道府県名、市区町村名は日本語での表記も可能です。

[illegible]

6 生成されたCSRが表示されます。

以上で、ステップ2の作業は終了です。
画面は閉じずに、ステップ3に進みます。

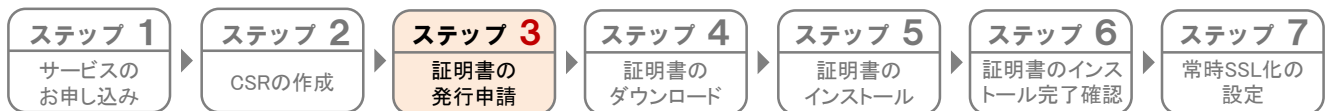
！ 画面は閉じないでください

画面に表示された赤枠内の情報は、次の設定で必要になります。画面を閉じないよう、ご注意ください。

※画面に表示されたCSRは次の設定で使います

ステップ3: 証明書の発行申請

! サイバートラスト社のメンテナンス実施中は、申請をお受けできずにエラーとなります。サイバートラスト社では、毎月第4水曜日の20:00～翌8:00に定期メンテナンスを実施しておりますので、ご注意ください。



お客様マイページから「SSLサーバ証明書 (SureServer)」の発行申請を行います。

1 ブラウザを起動し、以下URLにアクセスします。
<https://mypage.otsuka-shokai.co.jp/keiyaku>

2 必要事項を入力し、「ログイン」をクリックします。

ログインID	「お客様番号(旧契約マイページのID)」を入力
パスワード	「お客様マイページ(旧契約マイページ)のパスワード」を入力

! 弊社営業よりお申込書でSSLサーバ証明書をご契約いただいたお客様

SSLサーバ証明書専用のログインID・パスワードをお送りしておりますのでそちらを入力し、手順3に進みます。

3 「契約内容の確認」をクリックします。

4 SSLサーバ証明書の「契約内容を確認する」をクリックします。

大塚商会

[サポート](#) [フェア・セミナー](#) [お客様アンケート](#) [お問い合わせ](#) [English](#)

ホーム

ソリューション・製品

お客様マイページ

通販（たのめーる）

企業情報

お客様マイページトップ

製品ごとに便利に使う

技術サポート情報を探す

問い合わせをする・サポートを受ける

ソリューション・製品の検討をする

契約内容や請求書について

マイページの設定をする

ホーム

お客様マイページ

契約内容や請求書について

契約情報の確認

マイメニューに登録

契約内容や請求書について

契約情報の確認

請求書・お支払いについて

サービス検索

契約のよくあるご質問

よくあるご質問 (FAQ)

お知らせ

お問い合わせ

マイメニュー

トップ (マイメニュー)

マイメニューの編集

マイメニューとは

お客様マイページの使いかた

旧QQ-Webをご利用のお客様へ

旧契約マイページご利用のお客様へ

お客様マイページとは

各マークとは

お客様マイページ内検索

契約情報の確認

現在登録されている契約内容を確認するために、ご利用先を契約情報一覧から選択します。
多数の契約を持っているお客様は、絞り込み条件を入力して対象となる契約を取り込むことができます。

ご契約内容をご確認いただけます

契約情報一覧

絞り込み条件を開く

全1件中 1 - 1件表示

No	: 1	ご利用先	: 大塚商会
契約申込書No	: 0000000000	ご利用先	: 大塚商会
申込日	: 2015年10月23日	契約開始日	: 2015年10月26日
お客様番号	: 000000	会員番号	: -
設置先管理番号	: 0000000000	状況	: 契約中
契約額	: 12,600円 (月額)		
<契約お客様情報>			
契約責任者	: 大塚 太郎 様	ご利用先担当者	: 大塚 太郎 様
実務担当者	: 大塚 太郎 様		
サービス			
91.15.01	アルファメールプレミアム 100G	サービス内容	
91.59.95	SSLサーバ証明書 (SureServer)	サービス内容	

契約内容を確認する

5 「SSL証明書発行」をクリックします。

大塚商会

閉じる

契約内容の確認

契約申込書No	0000000000	ご利用先	大塚商会
ご利用先	大塚商会		
申込日	2015年10月23日	契約開始日	2015年10月26日
お客様番号	000000	会員番号	-
設置先管理番号	0000000000	契約状況	契約中
契約額	12,600円 (月額)		

[サービス申込履歴](#) [受付履歴](#) [お問い合わせ窓口](#)

ご契約中のサービスや利用料金の確認などができます。

[受付履歴](#)

契約サービス

契約サービス	月賦料金(円)
SSLサーバ証明書 (SureServer)	3,800

※価格には消費税は含まれておりません。

お客様番号	0000000000
支払方法	納金払い 毎月
利用開始日	
支払開始月	
契約期間	2016/10/17~
利用終了日	

ドメイン名	demodemo.jp
契約ID	000000

契約オプション

オプションの追加はこちら

オプションの削除はこちら

サービスの解約はこちら

SSL証明書発行

10

6 「SSL申請法人情報」に必要事項を入力します。

❗入力項目は、お申込みのサービスによって異なります。
(こちらは、EV SSLサーバ証明書をお申し込みのお客様向けの画面です)

画面下「SSL申請情報」の入力については、
次の手順で説明します。

申請法人名	法人格も入力してください。 例)株式会社 大塚商会
ビル・マンション名	全角40文字以内で入力してください。 無い場合は、「なし」と入力してください。 例)本社ビル
会社法人等番号	申請組織のカテゴリで「民間組織」を選択された場合は、会社法人等番号の入力が必須となります。 登記簿に記載されている12桁の会社法人等番号です。マイナンバーの法人番号(13桁)の先頭1桁を除いた12桁が、会社法人等番号になります。 例) 1234-00-123456
登記住所(都道府県)	申請組織のカテゴリで「行政機関(市区町村)」を選択された場合のみご入力ください。 (例) 東京都=Tokyo、埼玉県=Saitama、大阪府=Osaka

大塚商会

閉じる

SSL証明書の申請

入力確認完了

SSL申請法人情報

申請法人名

必須

株式会社 大塚商会

※全角55文字以内

法人格

必須

株式会社

※個人事業主のお客様は「その他法人」を選択してください。

法人代表者(最高責任者)

必須

姓 大塚

名 太郎

郵便番号

必須

102-8573

住所検索

※ハイフン(-) 付き、半角数字
例) 102-8573
郵便番号を入力し、「住所検索」ボタンを押すと住所を自動表示します

住所

必須

都道府県 東京都

※都道府県を一覧より選択してください

市区町村 千代田区

※全角40文字以内
例) 千代田区

丁目・番地 飯田橋

※全角40文字以内
例) 飯田橋2-18-4

ビル・マンション名

必須

本社ビル

※全角40文字以内
例) 本社ビル

申請責任者氏名(かな)

必須

姓 おおつか

名 たろう

申請責任者氏名(漢字)

必須

姓 大塚

名 太郎

部署名

必須

業務部

役職

必須

課長

申請組織カテゴリ

必須

民間組織

会社法人等番号

任意

1234 - 00 - 123456

※申請組織のカテゴリで「民間組織」を選択された場合のみご入力ください。

法人設立機関

必須

法務局

※民間組織の場合は、「法務局」とご入力ください。
行政機関の場合は、自身の上位団体がある場合はその行政機関名、それ以外の場合は自身の組織名を入力して下さい。

申請法人名(英名)

必須

OTSUKA CORPORATION

登記住所(都道府県:英名)

任意

※(例) 東京都=Tokyo、埼玉県=Saitama、大阪府=Osaka
※申請組織カテゴリで「行政機関(市区町村)」を選択された場合は必須です。

登記住所(国:英名)

必須

JP

代表電話番号

必須

03 - 1234 - 5678

申請責任者電話番号

必須

03 - 1234 - 5678

SSL申請情報

契約ドメイン

xxx.co.jp

本サービスでお申し込みいただいたドメイン名のコンテンツのみ証明書の申請・発行が可能です。
誤ったドメインのコンテンツで申請された場合は、無効となりますのでご注意ください。
※サブドメインsub.example.jpなど申請される場合は、sub.example.jpでサービス契約が必要となります。

CSR

必須

-----BEGIN CERTIFICATE-----
MIIDdzCQA+gawIBAgEAAQANANBqskqhkiGBvUBAQIFADBaMNs
oCZDVVODAJJ
PTENCAgAUUECNMUoaFsdGlttk3UjNWRMcOYDVOQLfemDeWJclir
ydxNOMSivlAYD
VUDUeXicYwfoadflvcuUagQI1ZXJUcnYzdsBSz29WB4XDtAWdu
MIc1ANDVwzd
DTT1MOUMJ1zktkvWfovYjELMAAGAEUEBMCSUUeJAQBgaMYBAo
TCOLHofRfuys
ZTEPESGAUECNMGSI1ZXJUcnYzdsEIMOGAIEUAzMZomFsdGI
UbSJ1JENSlyv
WkL13dudhvdyDOCASTv0DYJKoZIhvcNAQEBBgAzgEPADCCAgQ
CgeARCBgcwYwK

Webサーバ/クライアントに生成したCSRを貼り付けてください。
貼り付けの際、-----BEGIN CERTIFICATE REQUEST-----から-----EN
D
CERTIFICATE REQUEST-----を含めたすべての行をコピーして上の欄
に貼り付けてください。

※アルファメールプレミアたよれるOffice365Webサービスオプション
をご利用のお客様は、管理者機能ページの独自SSL管理「CSR作成」
メニューから出力できます。
※アルファメール2をご利用のお客様は、管理者機能ページの独自SSL
メニュー「CSRの作成」ボタンから出力できます。

通知メールアドレス1

not.send@otsuka-shokai.co.jp

通知メールアドレスを登録してください。通知メールアドレスには、
サイトトラスト社から審査に関する内容や更新期などの重要なメールが配信されま
す。
メールのお落着としないようグループアドレスの通知を推奨します。
※通知メールアドレス1は、本契約にご登録中の実務担当者メールアドレスが固定で
指定されます。

通知メールアドレス2

not.send@suka-shokai.co.jp

通知メールアドレス3

not.send@tsuka-shokai.co.jp

申請法人名の言語選択

必須

●日本語 ○英語

※ブラウザのアドレスバーに表示される法人名を日本語もしくは英語で
表示するかを選択できます。

コモンネーム

解除 必須

※CSRの入力を完了しましたら、上のボタンを押してしてください。
[www.demodemo.jp](#)

☐ demodemo.jp のコモンネームにもSSL証明書を対応させる。

■申請にあたっての留意事項（必ずご確認ください）

・ 「ご記入いただいた個人情報の取り扱い・利用目的」の内容についてご確認ください、ご同意の上でご入力ください。

・ サイバートラスト株式会社(以下、サイバートラスト社)のSureServerに関する利用規約は、下記サイトに
掲載しておりますのでご確認ください。
[サイバートラスト社約款](#)
※「SureServer証明書加入契約書」「SureServerEV証明書加入契約書」「SureServer証明書およびSureMail証明書CPS」
「SureBoard利用規約」
「EVC認証運用規定」の最終バージョンが該当します。

・ 本画面で入力いただいた個人情報および本サービスにご登録の実務担当者情報（組織名、氏名、電話番号、部署名、メールアドレス）は、
SSLサーバ証明書・発行・管理のためサイバートラスト社に提供されます。
提供された個人情報はサイバートラスト社の利用目的に基づいて取り扱います。

・ 証明書の発行と審査は、サイバートラスト株式会社が行います。審査にあたりサイバートラスト社より、
申請責任者に発照確認などのため欠く連絡をさせていただきます。
※ご連絡までの目安 本申請の当日～翌営業日
※発行日数の目安
必要書類のやりとりを含めた平均的な日数です。
必要書類の有無、審査状況によって異なります。
・ SSLサーバ証明書 …… 1～5営業日
・ EV SSLサーバ証明書 …… 5～10営業日

・ 審査にあたり必要書類や申請内容のご確認をさせていただく場合は、サイバートラスト社より、
ご登録の実務担当者宛にご連絡させていただきます。（個人事業主のお客様、ドメイン名等々に確認が必要な場合など）

・ 審査の内容及ち結果について弊社は一切開示せず、お問い合わせ等にもお答え致しかねますので
あらかじめご了承ください。

・ 審査の結果、発行不可となった場合は、本サービスは自動解約とさせていただきます。
（ご利用料金や解約的金戻金は発生しません。）

上記のすべての内容について確認、同意しました。

戻る

次へ

7 「SSL申請情報」に必要事項を入力します。

CSR	「ステップ2: CSRの作成」手順6(P.8)で画面に表示されたCSR欄の、 -----BEGIN CERTIFICATE REQUEST----- から -----END CERTIFICATE REQUEST----- までをコピーし、こちらに貼り付けます。
通知 メール アドレス1	サイバートラスト社から証明書の発行や更新に関する期限通知など重要なメールがこちらのメールアドレスに配信されます。 通知先を追加される場合は、以下「通知メールアドレス2」「通知メールアドレス3」に通知先のメールアドレスを入力します。 ※メールの見落とし防止のため、部署などのグループアドレスのご登録を推奨します。 ※通知メールアドレスは一度登録すると変更することができませんのでご注意ください。
申請法人 名の言語 選択	ブラウザのアドレスバーに表示される法人名の言語を選択します。 ※EV SSLサーバ証明書をお申し込みのお客様のみ選択ができます。 [画面イメージ] 
コモン ネーム	CSRを貼り付けた後に、「解析」をクリックすると「ステップ2: CSRの作成」手順5(P.8)で選択したコモンネームが表示されます。 「https://www.契約ドメイン名」「https://契約ドメイン名」の両方でホームページを公開される場合は、チェックボックスにチェックを入れます。

表示された内容を確認し、「上記のすべての内容について確認、同意しました。」をチェックして「次へ」をクリックします。

SSL証明書申請

SSL申請法人情報

申請法人名	大塚商会
法人格	株式会社

※ 画面省略 ※

	3pqa1BdRtH5qcCy7XX1u8DMEBQZAmbl1rF8yvtDHYwCb /AgY/LN2Hw5Xa7cUgtszh7hCkZMTHTkpCp9BSXtZLeoS5Wk7E/w9UfuecdB11 fVnrlw5Hs0Lga5QV/HpC3a3PbZyBB1n1pU000+VmrntST0pLUYm+KYyZ591Ythw 95Df0zCTQUGIAwMqJMB6FeNTEZZKoaK07X0hcS41uXG2JFY9Yz5OrY2hop1X2CAIFZKmCvuBGKQY8tsaG2W545DofFah9vbbfVg7dKtXdrYqZ9pbjGSROrWNBQ Umpl -----END CERTIFICATE REQUEST-----
通知メールアドレス1	not_send@otsuka-shokai.co.jp
通知メールアドレス2	
通知メールアドレス3	

約数の表示

2

約数・ご確認事項に同意する

変更申請時、受付完了メールが
 貴社担当者の連絡先E-mailアドレス not_send@otsuka-shokai.co.jp に送信されます。
 ※大塚ID管理者にも送付されます。

8 表示された内容を確認し、「約款・ご確認事項に同意する」を選択して「申し込む」をクリックします。

大塚商会

閉じる

SSL証明書申請

入力

確認

完了



SSLサーバ証明書（SureServer）／EV SSLサーバ証明書（SureServer）の
「証明書発行申請」を受け付けました。

受付確認の通知メールを実務担当者様宛にお送りしました。
申請後の流れや注意事項などを記載しておりますので必ずご確認ください。

ウィンドウを閉じる

9 申請の完了画面が表示されます。
「ウィンドウを閉じる」をクリックし、お客様マイページからログアウトします。

The screenshot shows the AWS IAM console interface. On the left sidebar, under 'Groups', the 'AWS-ReadOnlyAccess' group is listed with a count of 1. The main content area is titled 'Groups' and shows details for the 'AWS-ReadOnlyAccess' group. The 'Name' is 'AWS-ReadOnlyAccess', the 'Type' is 'AWS managed', and the 'Permissions' section shows a list of permissions, including 'AWS-ReadOnlyAccess' and 'AWS-ReadOnlyAccess-ReadOnlyAccess'. The 'Permissions' section is expanded, showing a list of permissions with their names and descriptions.

10 「ステップ2：CSRの作成」手順6（P.8）で残した画面に戻り、「ログアウト」をクリックします。

以上で、ステップ3の作業は終了です。



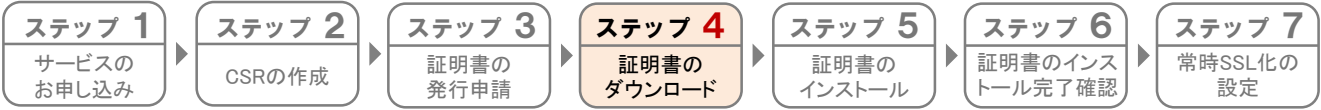
ステップ4: 証明書のダウンロード

! こちらの作業は、「証明書発行のお知らせ」というメールが到着してから開始してください。

サイバートラストのページは予告なく変更される場合があります。その場合は適宜指示に従って作業を進めてください。

メールは、サイバートラストからお客様マイページの実務担当者のメールアドレス宛てに送られます。「ステップ3: 証明書の発行申請」手順7(P.12)で通知先を追加された場合は、追加したメールアドレス宛てにもメールが送られます。

メールの送信日が2019年9月30日以降か、9月30日までかによって、「本ステップ」手順7(P.16)以降でダウンロードする中間証明書が異なりますのでご注意ください。



お客様マイページから証明書をダウンロードします。

1 ブラウザを起動し、以下URLにアクセスします。
<https://mypage.otsuka-shokai.co.jp/keiyaku>

お客様マイページ

ホーム > お客様マイページ > ログイン > お客様番号 (旧契約マイページのID) でログイン

お客様番号 (旧契約マイページのID) でログイン

ID、パスワードを入力してください。

ID欄にはお客様番号とログインIDのみが入力できます。

ログインID

必須 例) W123456789、123456

「」からIDの入力を省略する

パスワード

必須

パスワードをお忘れですか?

旧契約マイページでブラウザにIDとパスワードを記憶されている方へ

Webでのお問い合わせ

ログインページへ

ログイン

2 必要事項を入力し、「ログイン」をクリックします。

ログインID	「お客様番号 (旧契約マイページのID)」を入力
パスワード	「お客様マイページ (旧契約マイページ) のパスワード」を入力

! 弊社営業よりお申込書でSSLサーバ証明書をご契約いただいたお客様

SSLサーバ証明書専用のログインID・パスワードをお送りしておりますのでそちらを入力し、手順3に進みます。

大塚商会

サポート > フェア・セミナー > お客様アンケート > お問い合わせ > English

ホーム ソリューション・製品 お客様マイページ 通販 (たのめー) 企業情報

お客様マイページ トップ

製品ごとに
便利に使う

技術サポート
情報を探す

問い合わせをする・
サポートを受ける

ソリューション・
製品の検討をする

契約内容や
請求書について

マイページの
設定をする

ホーム > お客様マイページ > 契約内容や請求書について

マイメニューに登録

契約内容や請求書について

契約情報の確認

請求書・お支払いについて

サービス検索

契約のよくあるご質問

よくあるご質問
(FAQ)

お知らせ

お問い合わせ

マイメニュー

トップ (マイメニュー)

マイメニューの編集

契約内容や請求書について

ご契約内容、請求書に関する情報の確認をさせていただきます。

IBQQ-Webご利用のお客様へ

旧契約マイページご利用のお客様へ

契約を確認する・手続きする

ご契約いただいている内容の確認や更新ができます。

契約の確認

契約情報の確認

契約内容の確認

ご契約の明細や履歴などを確認できます。

ご契約されている契約情報のお客様情報の確認、変更申し込みができます。

請求情報の確認

3 「契約内容の確認」をクリックします。

4 SSLサーバ証明書の「契約内容を確認する」をクリックします。



5 「SSL証明書ダウンロード」をクリックします。



大塚商会

SSL証明書のダウンロード

お客様番号: 0000405039

オプション名: SSLサーバ証明書 (SureServer)

※ 画面省略 ※

通知メールアドレス1: not.send@otsuka-shokai.co.jp

通知メールアドレス2:

通知メールアドレス3:

ダウンロードされた証明書も、Webサーバにインストールされる際には、中間CA証明書が必要となります。下記のサイトよりダウンロードしてご利用ください。

SSLサーバ証明書(SureServer)をご契約のお客様: SureServer(SHA-2)

EV SSLサーバ証明書(SureServer)をご契約のお客様: SureServer EV(SHA-2)(連絡ファイルの増設をご利用ください)

SureServer 中間CA証明書ダウンロード

ダウンロードする

6 「ダウンロードする」をクリックし、ファイルを保存します。

※ステップ5で利用しますので、SSL証明書とわかるように保存してください。

次に「SureServer 中間CA証明書ダウンロード」をクリックします。

7 サイバートラストのダウンロードページが表示されます。

次の手順は、ご契約のサービスによって異なります。

■EV SSLサーバ証明書 (SureServer) をご契約のお客様

→手順8に進みます。

■SSLサーバ証明書 (SureServer) をご契約のお客様

→手順10に進みます。

cybertrust

企業情報 手続案内 お取引先 導入事例 検索ワードを入力

ルート・中間 CA 証明書 ダウンロード

SureServer / SureServer EV / SureMail

ルート・中間 CA 証明書 ダウンロード

SureServer EV Prime

SureServer EV Prime

(SHA-2 for クラウド利用)

ご利用のお客様はこちら

SureServer Prime

SureServer Prime

(SHA-2 for クラウド、デジタルカード利用)

ご利用のお客様はこちら

SureMail

ご利用のお客様はこちら

SureServer EV 中間 CA 証明書ダウンロード

SureServer 中間 CA 証明書ダウンロード

SureMail 中間 CA 証明書ダウンロード

！ 手順8の作業は、「EV SSLサーバ証明書 (SureServer)」をご契約のお客様向けの作業になります。

8 「SureServer EV中間CA証明書ダウンロード」をクリックします。

！ 「SureServer EV中間CA証明書ダウンロード」を必ず選択してください

誤って他の項目を選択すると、正常に設定が完了できません。

cybertrust

企業情報 手続案内 お取引先 導入事例 検索ワードを入力

ルート・中間 CA 証明書 ダウンロード

SureServer / SureServer EV / SureMail

ルート・中間 CA 証明書 ダウンロード

SureServer EV Prime

SureServer EV Prime

(SHA-2 for クラウド利用)

ご利用のお客様はこちら

SureServer Prime

SureServer Prime

(SHA-2 for クラウド、デジタルカード利用)

ご利用のお客様はこちら

SureMail

ご利用のお客様はこちら

SureServer EV 中間 CA 証明書ダウンロード

SureServer 中間 CA 証明書ダウンロード

SureMail 中間 CA 証明書ダウンロード

9 「クロスルートあり（4階層）」タブを選択します。

「連結ファイルの場合」にある「クロスルート用中間CA証明書+中間CA証明書」の「テキスト形式」を右クリックし、保存します。

※ステップ5で利用しますので、中間証明書とわかるように保存してください。

サイバートラストの画面を閉じます。

手順6（P. 16）の画面に戻り、「閉じる」をクリックし、画面を閉じます。お客様マイページからログアウトします。

以上で、ステップ4の作業は終了です。
ステップ5に進みます。

！左図は、2021年4月時点のダウンロードページです。
ダウンロードページは予告なく変更される場合があります。

ダウンロードページが変更されていた場合は、以下に該当する中間証明書をテキスト形式でダウンロードしてください。

「SureServer EV中間CA証明書」
→「クロスルートあり(4階層)」
→「連結ファイル」
→「クロスルート用中間CA証明書+中間CA証明書」

EV 認証証明書用 ルート・中間 CA 証明書 ダウンロード

2019 年 9 月 30 日以降に発行された SureServer EV Prime / SureServer EV をご利用のお客様用のルート・中間 CA 証明書

最新の提供開始日
中間 CA 証明書: 2019 年 9 月 30 日 9:00

一般的な構成での利用を想定されている場合、クロスルートなし (3 階層) をご利用ください。
幅広いクライアントパナリティをサポートする必要があるなど、特定のご要望がある場合はクロスルートあり (4 階層) をご利用ください。

クロスルートなし (3 階層) **クロスルートあり (4 階層)**

クロスルートの場合、個別インストールおよび連結ファイルのどちらをご選択いただくかは、お客様のご利用環境に応じて選択ください。

- IIS や IPanet Web Server, keytool(Tomcat) などをご利用のお客様
クロスルート用中間 CA 証明書と中間 CA 証明書を個別にダウンロードし、2 つともインストールしてください。
- Apache や BIG-IP などの OpenSSL ハンドル系のサーバーをご利用のお客様
クロスルート用中間 CA 証明書と中間 CA 証明書を連結して 1 つのファイルにしたものをインストールしてください。

個別インストールの場合

	コモンネーム (または OU の値)	設定	ダウンロード	プロファイル
ルート証明書	Security Communication RootCA1	不要※1	テキスト形式	詳細
クロスルート用 中間 CA 証明書	Security Communication RootCA2	必要	テキスト形式	詳細
中間 CA 証明書	Cybertrust Japan SureServer EV CA G3	必要	テキスト形式	詳細
サーバー証明書	お申込みの FQDN	必要	個別にご案内※2	

連結ファイルの場合

	コモンネーム (または OU の値)	設定	ダウンロード	プロファイル
ルート証明書	Security Communication RootCA1	不要※1	テキスト形式	詳細
クロスルート用 中間 CA 証明書 + 中間 CA 証明書	Cybertrust Japan SureServer EV CA G3	必要	テキスト形式	詳細
サーバー証明書	お申込みの FQDN	必要	個別にご案内※2	

※1 ルート証明書の設定が必要なサーバーソフトウェア・機器をご利用の場合のみ、設定してください (例: Keyman や Lotus Domino, Keytool(Tomcat) など)。
※2 「証明書発行のお知らせ」メールに記載の URL からダウンロードしてください。

「テキスト形式」を右クリックし、保存します。

！手順10の作業は、「SSLサーバ証明書(SureServer)」をご契約のお客様向けの作業になります。

10 「SureServer 中間CA証明書ダウンロード」をクリックします。

！「SureServer 中間CA証明書ダウンロード」を必ず選択してください

誤って他の項目を選択すると、正常に設定が完了できません。

ルート・中間 CA 証明書 ダウンロード

SureServer / SureServer EV / SureMail
ルート・中間 CA 証明書 ダウンロード

このページでは、SureServer シリーズおよび SureMail のルート証明書と中間 CA 証明書をダウンロードいただけます。なおご利用にあたり、最新の加入契約 (C/P/CPS) をご確認くださいませようお願いします。

SureServer EV Prime **SureServer Prime**

SureServer EV Prime
SureServer EV
(M1) for クラウド環境
ご利用のお客様はこちら

SureServer Prime
SureServer
(M1) for クラウド、クラウド/オンプレミス
ご利用のお客様はこちら

SureMail
SureMail
ご利用のお客様はこちら

SureServer EV 中間 CA 証明書ダウンロード **SureServer 中間 CA 証明書ダウンロード** SureMail 中間 CA 証明書ダウンロード

cybertrust

企業情報

事業内容

ニュース

導入事例

お問い合わせ

English

企業認証(OV)証明書用 ルート・中間 CA 証明書 ダウンロード

HOME > 保証・サポート > SSL/TLS サーバー証明書 SureServer > ルート・中間 CA 証明書 ダウンロード > 企業認証(OV)証明書用 ルート・中間 CA 証明書 ダウンロード

トップ SureServer 製品情報 お申込み手順 サポート情報 申請ツール

SureServer Prime / SureServer

ルート・中間 CA 証明書 ダウンロード

このページでは、SureServer Prime / SureServer (企業認証: OV) 用のルート・中間 CA 証明書がダウンロードできます。EV 証明書の SureServer EV Prime / SureServer EV をお使いの方は、EV 保証証明書用 ルート・中間 CA 証明書 ダウンロードページをご利用ください。
ご利用にあたり、最新の加入契約書、CP/PS をご確認くださいませようお願いいたします。

2019 年 9 月 30 日以降に発行された SureServer Prime / SureServer 用のルート・中間 CA 証明書

最新版の提供開始日
中間 CA 証明書: 2019 年 9 月 30 日 9:00

一般的な構成での利用を想定されている場合、クロスルートなし (3 階層) をご利用ください。
特定のクライアントがバレージをサポートする必要があるなど、特定の要望がある場合にはクロスルートあり (4 階層) をご利用ください。

クロスルートなし (3 階層) **クロスルートあり (4 階層)**

クロスルートの場合、個別インストールおよび連結ファイルのどちらをご選択いただくかは、お客様のご利用環境に応じて選択ください。

- IIS や iPlanet Web Server、keytool(Tomcat) などをご利用のお客様
クロスルート用中間 CA 証明書と中間 CA 証明書を個別にダウンロードし、かつともインストールしてください。
- Apache や BIG-IP などの OpenSSL バンドル系のサーバをご利用のお客様
クロスルート用中間 CA 証明書と中間 CA 証明書を連結して 1 つのファイルにしたものをインストールしてください。

個別インストールの場合

	コモンネーム (または OU の値)	設定	ダウンロード	プロファイル
ルート証明書	Security Communication RootCA1	不要 ^{※1}	テキスト形式	詳細
クロスルート用 中間 CA 証明書	Security Communication RootCA2	必要	テキスト形式	詳細
中間 CA 証明書	Cybertrust Japan SureServer CA G4	必要	テキスト形式	詳細
サーバー証明書	お申込みの FQDN	必要	個別にご案内 ^{※2}	

連結ファイルの場合

	コモンネーム (または OU の値)	設定	ダウンロード	プロファイル
ルート証明書	Security Communication RootCA1	不要 ^{※1}	テキスト形式	詳細
クロスルート用 中間 CA 証明書 + 中間 CA 証明書	Cybertrust Japan SureServer CA G4	必要	テキスト形式	詳細
サーバー証明書	お申込みの FQDN	必要	個別にご案内 ^{※2}	

※1 ルート証明書の発行者が必須のサーバーソフトウェア・機器をご利用の場合のみ、設定してください (例: Keyman や Lotus Domino、Keytool(Tomcat) など)。
※2 「証明書発行の案内書」メールの記載の URL からダウンロードしてください。

11 「クロスルートあり (4階層)」タブを選択します。

「連結ファイルの場合」にある「クロスルート用中間CA証明書+中間CA証明書」のダウンロードの「テキスト形式」を右クリックし、保存します。

※ステップ5で利用しますので、中間証明書とわかるように保存してください。

サイバートラストの画面を閉じます。

手順6 (P. 16) の画面に戻り、「閉じる」をクリックし、画面を閉じます。お客様マイページからログアウトします。

以上で、ステップ4の作業は終了です。
ステップ5に進みます。

!

左図は、2021年4月時点のダウンロードページです。ダウンロードページは予告なく変更される場合があります。

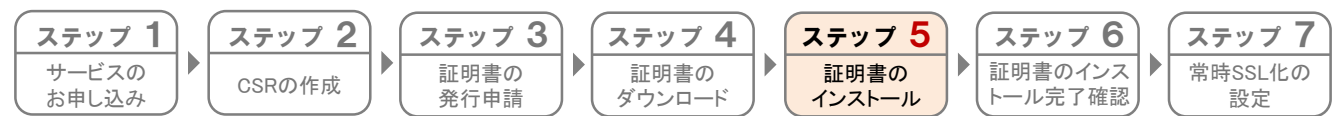
ダウンロードページが変更されていた場合は、以下に該当する中間証明書をテキスト形式でダウンロードしてください。

「SureServer EV中間CA証明書」
→「クロスルートあり(4階層)」
→「連結ファイル」
→「クロスルート用中間CA証明書+中間CA証明書」

「テキスト形式」を右クリックし、保存します。

18

ステップ5: 証明書のインストール



ドメイン/Webサービスの管理者機能から証明書をインストールします。

- 1 ブラウザを起動し、ドメイン/Webサービス会員サイトにアクセスします。
<https://dw.alpha-prm.jp/>
「ログイン」をクリックします。



- 2 必要事項を入力し、「ログイン」をクリックします。

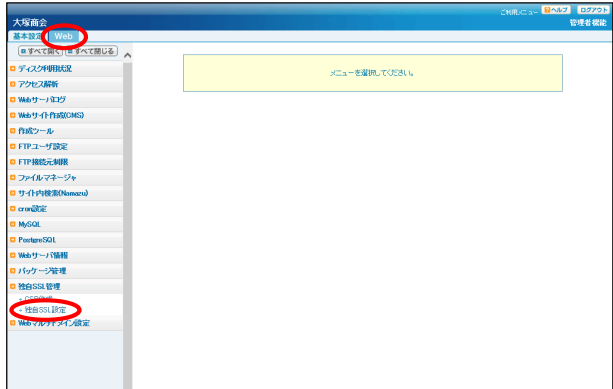
メールアドレス	「管理者メールアドレス(ログインID)」を入力
パスワード	「管理者パスワード」を入力



- 3 「管理者機能」をクリックします。



- 4 「Web」タブをクリックし、「独自SSL管理」→「独自SSL設定」をクリックします。



! サーババージョン2環境へ切替え中のお客様
以下の手順で、サーババージョン2環境に、SSL証明書を設定してください。
「Web」タブをクリックし、「サーババージョン2」→「独自SSL管理」→「独自SSL設定」をクリックしてください。

[illegible]

5 必要事項を入力し、「設定」をクリックします。

SSL サーバ 証明書	「ステップ4: 証明書のダウンロード」手順6 (P.15) でダウンロードしたファイルをメモ帳等で開きます。 -----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- を含めたすべての行をコピーして貼り付けます。
中間 認証局 証明書	「ステップ4: 証明書のダウンロード」でサイバートラストのダウンロードページからダウンロードしたファイルをメモ帳等で開きます。 -----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- を含めたすべての行をコピーして貼り付けます。

**！ 秘密鍵・クロスルート方式用中間認証局証明書は
入力しません**

▼をクリックすると入力欄が表示されますが、こちらの入力欄には何も入力しません。

中間型証明書証明書	<pre> XX XX XX XX XX XX XX XX XX XX -----END CERTIFICATE----- SSLサーバ証明書が中間型証明書証明書のインストールを必要とする場合、 証明書から発行された中間型証明書証明書の -----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- を含めたすべての行をゴースト上の欄に貼り付けてください。 ※連結ファイルをご利用の場合は証明書指定の順番で分割せずに貼り付け </pre>
▼秘密鍵を入力する	
▼クロスルート方式用中間型証明書証明書を入力する	

EV SSLサーバ証明書をご契約されたお客様

中間認証局証明書が1ファイルの中で、「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」までが2つ繋がっています。2つ繋がったままコピーし、ペーストしてください。

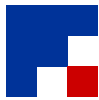
独自SSL設定

お客様のSSLサーバ証明書の設定が完了しました。

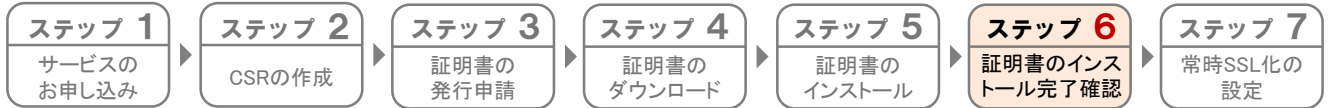
ブラウザで正しくSSL通信ができることも必ずご確認ください。

6 設定が完了すると左記画面が表示されます。
画面右上「ログアウト」をクリックします。

以上で、ステップ5の作業は終了です。
ステップ6に進みます。



ステップ6: 証明書のインストール完了確認



証明書のインストールが正常に完了されたか確認します。

- 1 ブラウザを起動し、以下URLにアクセスします。
https://sstool.cybertrust.ne.jp/support_tool/index01.php

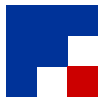
- 2 必要事項を入力し、「設定を確認する」をクリックします。

https	選択します。
FQDN 1	取得されたSSL証明書のコモンネームを入力します。 (例) www.alpha-prm.jp

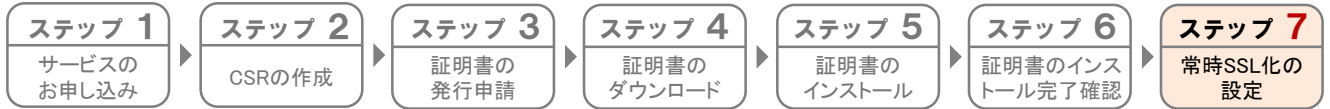
- 3 インストールが正常に完了された場合、証明書が正しく設定された旨の文言が表示されます。
※画面に表示される文言は、ご契約のサービスによって異なります。

併せてコモンネームとサーバ証明書の有効期限が正しいことを確認しましたら、画面を閉じます。

以上で、ステップ6の作業は終了です。
すべての作業が終了しましたので、SSLサーバ証明書をご利用いただけます。



ステップ7: 常時SSL化の設定 (事前確認)



! 本作業は、お客様任意の作業です。

お客様ホームページへHTTP(非SSL)でアクセスされた際に、HTTPS(SSL)でのアクセスへ遷移させる事で常にSSL通信とすることができます。ご利用の機能によっては、正常に動作しない等の影響がございますので、注意事項をご確認の上設定ください。

! お客様の環境によって、手順が異なります。

本作業では、Webサービス環境の最上位階層に.htaccessというファイルを置くことで、常時SSL化を実現します。お客様のホームページによっては、既に.htaccessが存在している場合もありますので、事前に.htaccessの有無を確認の上、手順に従って作業をお願いします。既に.htaccessが設置されている場合は、Webサービスの機能により設置された場合のみを想定した手順となっております。WordPressやMovableTypeをはじめとするツール類等、アルファメールプレミアの機能以外をご利用の場合は、弊社サポート対象外となりますので、ホームページを作成された方にお問い合わせください。

! 注意事項

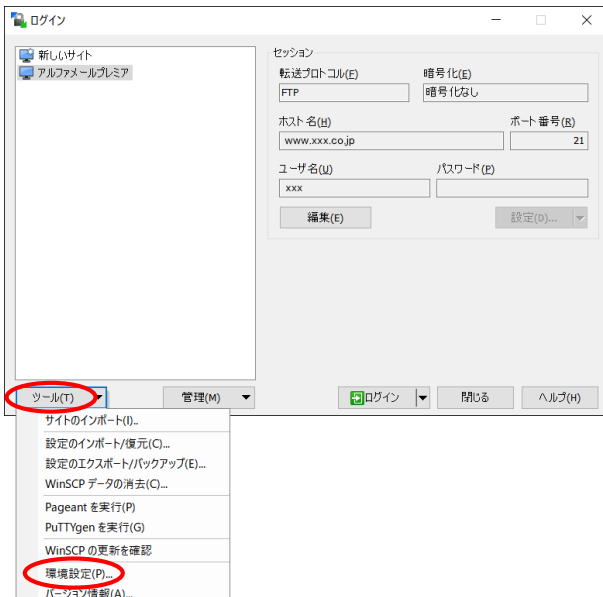
- Webマルチドメイン設定をご利用のお客様は、本作業は行わないでください。
外部ドメインでホームページにアクセスされた際に、URLがSSL証明書の共通ネームに変更されてしまいます。
- 本作業を行う事で、お客様ホームページへHTTPでアクセスされ場合、HTTPSへ遷移するようになります。HTTPSへ遷移する際、HTTPによるアクセスとHTTPSによるアクセスで、アクセスログが複数行出力されます。
- 共用SSLをご利用の場合、URLがSSL証明書の共通ネームに変更されます。
- 本作業後に、アクセス制限を設定しているページへHTTPでアクセスした場合、HTTPで認証を行った後にHTTPSで再度認証を求められるようになります。
- .htaccessの記載内容に不備等があった場合、お客様ホームページが表示できなくなる場合があります。作業を行う際は、十分ご注意ください。

お客様環境にて、.htaccessの有無を確認します。

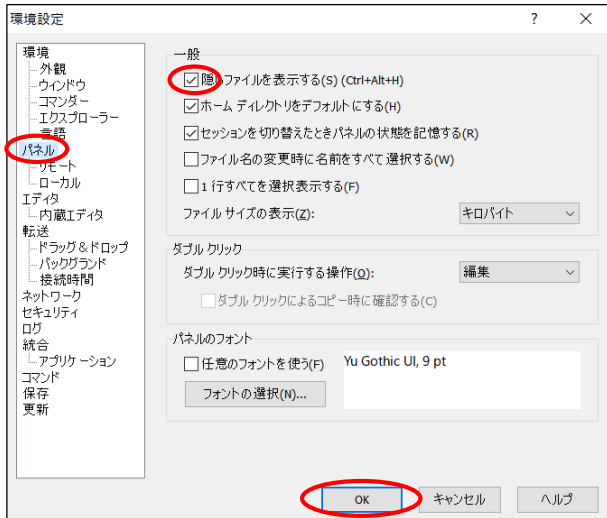


1 WinSCPを起動します。

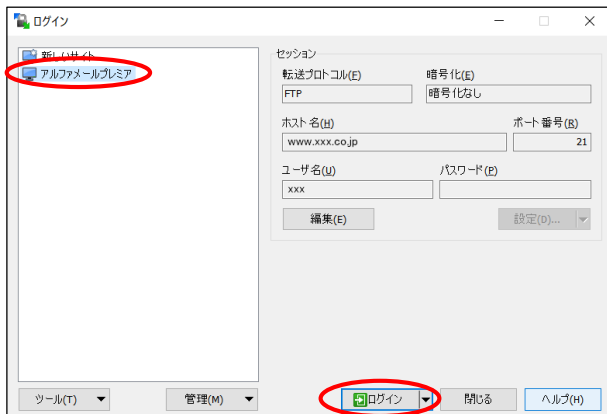
2 「ツール」から「環境設定」を選択します。



3 「パネル」を選択し、「隠しファイルを表示する」にチェックを入れ、「OK」をクリックします。



4 Webサービス用の設定名をクリックし、「ログイン」をクリックします。



❗ ドメイン/Webサービス用の設定が登録されていない場合は、以下のURLにアクセスし、FTPソフト設定マニュアルを参照の上、設定をお願いします。
<https://dw.alpha-prm.jp/support/ftp/index.html>



❗ 最上位の階層にアクセスする必要がありますので、管理者もしくは最上位の階層にアクセス可能なFTPユーザでログインしてください。

5 サーバに接続されます。

サーバの最上位階層に「.htaccess」というファイルが存在するか確認してください。

※ファイル名の先頭に「.」(ピリオド)が付いています

左側：ローカル（お客様のコンピュータ）
右側：サーバ（アルファメールプレミアム環境）

確認しましたら、引き続き以下のページに進み作業を行います。

.htaccessが存在しない場合

→ このまま「常時SSL化の設定(.htaccessなし)」へ進む

.htaccessが存在する場合

→ このまま「常時SSL化の設定(.htaccessあり)」へ進む

! ここからの作業は、.htaccessが存在しない場合と、.htaccessが存在する場合の作業に分かれます。

.htaccessが
存在しない場合

「常時SSL化の設定(.htaccessなし)」へ進む
→P.25

.htaccessが
存在する場合

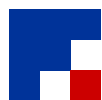
「常時SSL化の設定(.htaccessあり)」へ進む
→P.27

ご利用の機能に進みます

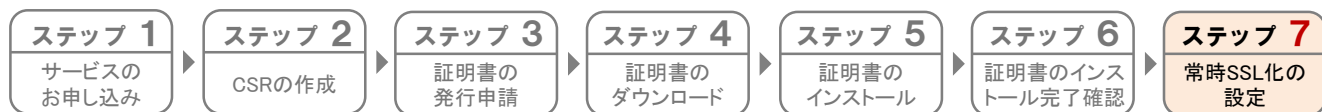
アクセス制限機能をご利用のお客様

エラーページ設定機能をご利用のお客様

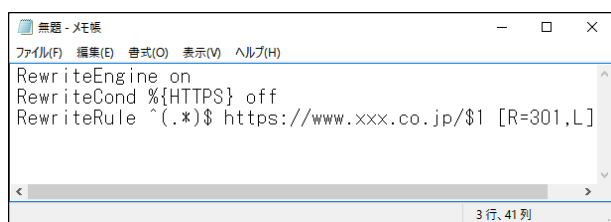
モバイルURL振り分け、Webサイト作成の
スマートフォンページ振り分け設定機能
をご利用のお客様



ステップ7: 常時SSL化の設定 (.htaccessなし)



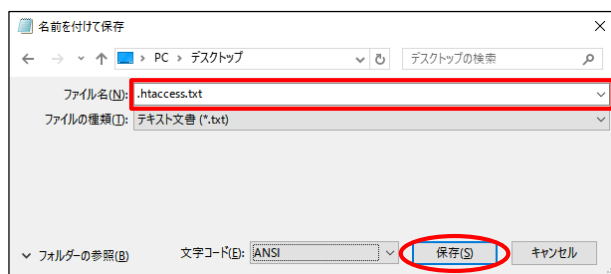
1 お客様のPCにて、メモ帳を起動します。



2 以下の内容をコピーし、メモ帳に貼り付けます。

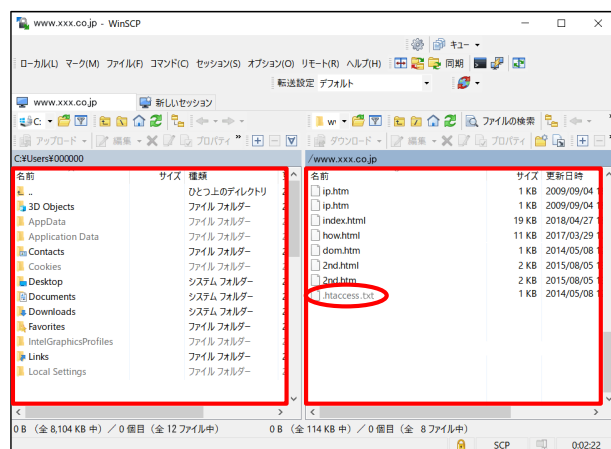
```
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://「コモンネーム」/$1 [R=301,L]
```

❗ 「コモンネーム」には、取得されたSSL証明書のコモンネームを指定してください

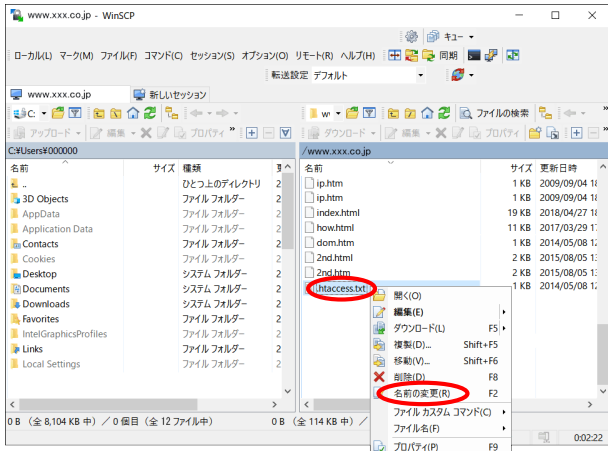


3 ファイル名「.htaccess.txt」にて、保存します。

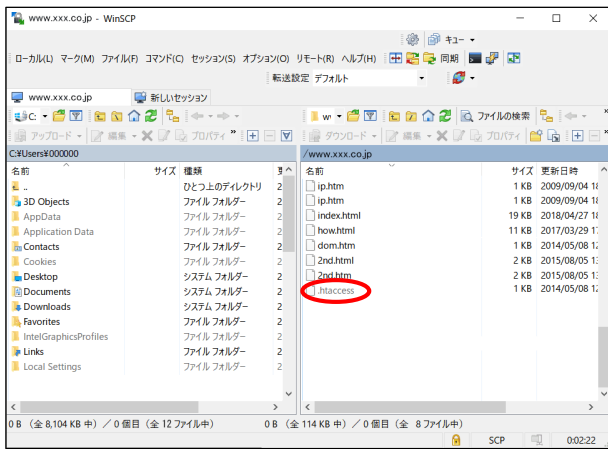
❗ ファイル名の先頭に「.」(ピリオド)が必要です。



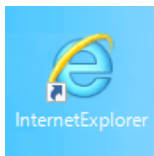
4 WinSCPにて、アルファメールプレミア環境の最上位階層に「.htaccess.txt」をアップロードします。



5 アップロードした「.htaccess.txt」を右クリックし、「名前の変更」を選択します。



6 ファイル名を「.htaccess」に変更します。



7 Internet Explorerを起動し、httpでお客様ホームページにアクセスします。
(例) <http://www.お客様ドメイン名>

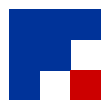


8 Internet Explorerで表示されているURLが、<https://>～に変更されることを確認します。

! お客様ホームページが表示されなくなった場合

6. で変更したファイル名を「.htaccess」から、元の「.htaccess.txt」へ戻してください。

9 WinSCPを終了します。



ステップ7: 常時SSL化の設定 (.htaccessあり)

ステップ 1

サービスの
お申し込み

ステップ 2

CSRの作成

ステップ 3

証明書の
発行申請

ステップ 4

証明書の
ダウンロード

ステップ 5

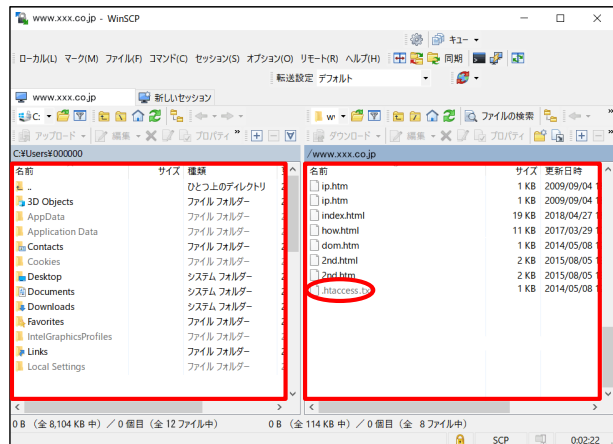
証明書の
インストール

ステップ 6

証明書のインス
トール完了確認

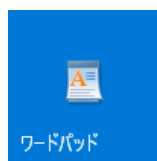
ステップ 7

常時SSL化の
設定



1 WinSCPにて、「.htaccess」をダウンロードします。

必ず、バックアップを取得した上で、以降の作業を実施してください。



2 ダウンロードした「.htaccess」をワードパッドで開きます。

※ご利用の機能により、記載されている内容が異なります。

ご利用の機能により、記載されている内容が異なります。
「アクセス制限機能」をご利用のお客様向けのご案内です。

アクセス制限機能をご利用のお客様

エラーページ設定機能をご利用のお客様

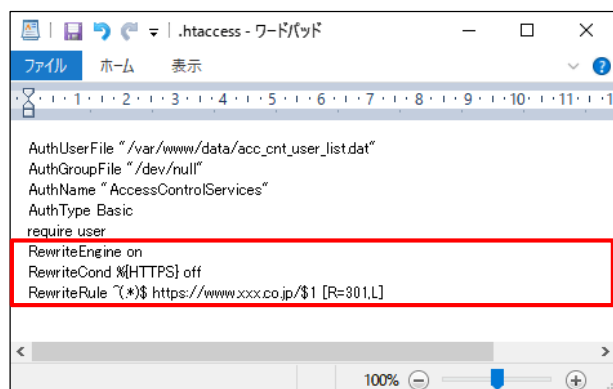
モバイルURL振り分け、Webサイト作成の
スマートフォンページ振り分け設定機能を
ご利用のお客様

```
AuthUserFile "/var/www/data/acc_cnt_user_list.dat"
AuthGroupFile "/dev/null"
AuthName "AccessControlServices"
AuthType Basic
require user
```

左記の内容が記載されておりますので、末尾
に以下の内容を追記してください。

```
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://「コモンネーム」/$1 [R=301,L]
```

「コモンネーム」には、取得されたSSL証明書の
コモンネームを指定してください



! ご利用の機能により、記載されている内容が異なります。
「エラーページ設定機能」をご利用のお客様向けのご案内です。

アクセス制限機能をご利用のお客様

エラーページ設定機能をご利用のお客様

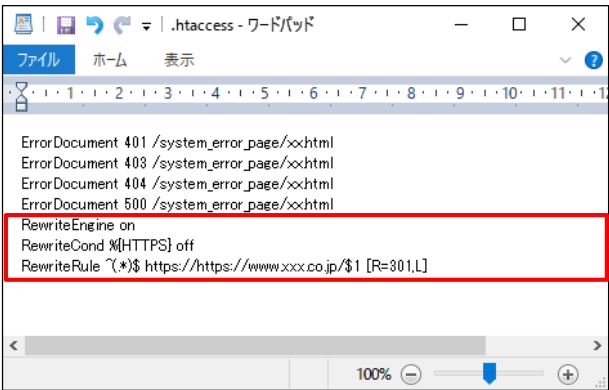
モバイルURL振り分け、Webサイト作成のスマートフォンページ振り分け設定機能をご利用のお客様

```
ErrorDocument 401 /system_error_page/xx.html
ErrorDocument 403 /system_error_page/xx.html
ErrorDocument 404 /system_error_page/xx.html
ErrorDocument 500 /system_error_page/xx.html
```

左記の内容が記載されておりますので、末尾に以下の内容を追記してください。

```
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://「コモンネーム」/$1 [R=301,L]
```

! 「コモンネーム」には、取得されたSSL証明書のコモンネームを指定してください



! ご利用の機能により、記載されている内容が異なります。
「モバイルURL振り分け」、「Webサイト作成のスマートフォンページ振り分け設定機能」をご利用のお客様向けのご案内です。

アクセス制限機能をご利用のお客様

エラーページ設定機能をご利用のお客様

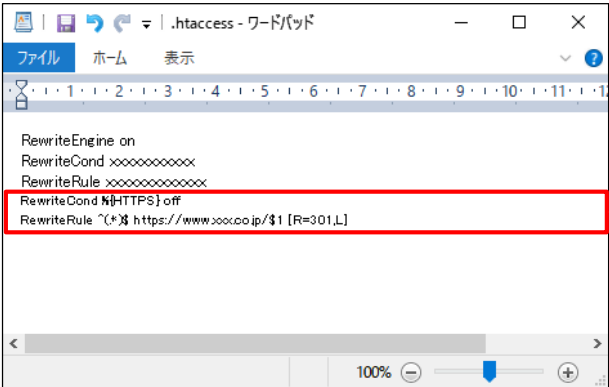
モバイルURL振り分け、Webサイト作成のスマートフォンページ振り分け設定機能をご利用のお客様

```
RewriteEngine on
RewriteCond xxxxxxxxxxxx
RewriteRule xxxxxxxxxxxxxx
```

左記の内容が記載されておりますので、最後のRewriteRuleの次の行に以下の内容を追記してください。

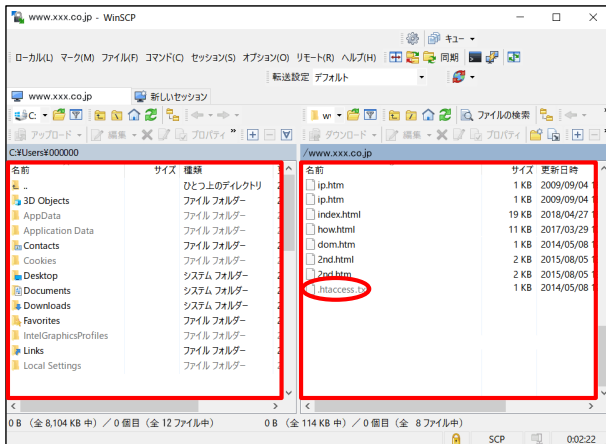
```
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://「コモンネーム」/$1 [R=301,L]
```

! 「コモンネーム」には、取得されたSSL証明書のコモンネームを指定してください



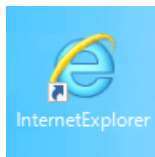
3 「.htaccess」を上書き保存します。

4 WinSCPにて、アルファメールプレミア環境の最上位階層に「.htaccess」をアップロードし上書きします。



5 Internet Explorerを起動し、httpでお客様ホームページにアクセスします。

(例) [http://www. お客様ドメイン名](http://www.お客様ドメイン名)



6 Internet Explorerで表示されているURLが、https://～に変更されることを確認します。



！ お客様ホームページが表示されなくなった場合

1. で取得いただいた「.htaccess」のバックアップを最上位階層にアップロードし、上書きしてください。

7 WinSCPを終了します。