

SSL をはじめよう

証明書の発行からトラブルシューティングまで

mochikoAsTech 著

2020-02-29 版 mochikoAsTech 発行

はじめに

2020 年 2 月 mochikoAsTech

この本を手にとってくださったあなた、はじめまして。「SSL をはじめよう」の筆者、mochikoAsTech です。

想定する読者層

本著は、こんな人に向けて書かれています。

- よく分からないけど言われるがままに SSL の設定をしている人
- SSL 証明書がいったい何を証明しているのか知らない人
- SSL は聞いたことがあるけど TLS は知らないという人
- これからシステムやプログラミングを学ぼうと思っている新人
- ウェブ系で開発や運用をしているアプリケーションエンジニア
- 「インフラがよく分からないこと」にコンプレックスのある人
- 証明書の購入や設置はしたことがあるけど SSL はあまり分かっていない人
- サイトを HTTPS 化しなきゃと思っている人

マッチしない読者層

本著は、こんな人が読むと恐らく「not for me だった…（私向けじゃなかった）」となります。

- SSL/TLS の通信を C 言語で実装したい人
- 「プロフェッショナル SSL/TLS」を読んで理解できた人

本著の特徴

本著では実際にサーバを立てて SSL 証明書の設置を行い、HTTPS のサイトを作ってみます。手を動かして試しながら学べるので理解がしやすく、インフラ初心者でも安心して読み進められる内容です。

また実際にありがちなトラブルをとり上げて、

- こんな障害が起きたら原因はどう調べたらいいのか？
- 問題をどう解決したらいいのか？
- どうしたら事前に避けられるのか？

を解説するとともに、実際にコマンドを叩いて反復学習するためのドリルもついています。

本著のゴール

本著を読み終わると、あなたはこのような状態になっています。

- SSL 証明書がどんな役割を果たしているのか説明できる
- 証明書を買うときは何に注意してどんな手順で買ったらいいか分かっている
- 意図せず「保護されていない通信」と表示されてしまったときの対処法が分かる
- 障害が起きたときに原因を調査できる
- 読む前より SSL が好きになっている

免責事項

本著に記載されている内容は筆者の所属する組織の公式見解ではありません。

また本著はできるだけ正確を期すように努めました。が、筆者が内容を保証するものではありません。よって本著の記載内容に基づいて読者が行った行為、及び読者が被った損害について筆者は何ら責任を負うものではありません。

不正確あるいは誤認と思われる箇所がありましたら、必要に応じて適宜改訂を行いますので GitHub の Issue や Pull request で筆者までお知らせいただけますと幸いです。

<https://github.com/mochikoAsTech/startSSL>

目次

はじめに	3
想定する読者層	3
マッチしない読者層	3
本著の特徴	4
本著のゴール	4
免責事項	4
 第 1 章 SSL のサイトを作ってみよう	 9
1.1 Alibaba Cloud でアカウント登録	9
1.1.1 無料でアカウントを作成	9
1.1.2 作ったアカウントでサインインする	16
1.2 Alibaba Cloud でサーバを立てよう	23
1.3 ドメイン名の設定	23
1.4 まずは HTTP でサイトを公開	23
1.5 証明書を取得しよう	23
1.5.1 秘密鍵を作ろう	23
1.5.2 CSR を作ろう	23
1.5.3 証明書の取得申請	23
1.5.4 取得した証明書をサーバに置こう	23
1.6 HTTPS でサイトを公開	23
 第 2 章 基本	 25
2.1 SSL ってなに?	26
2.2 TLS ってなに?	26
2.3 SSL と TLS の違いは?	26
2.4 SSL と SSH って似てる? 何が違うの?	26

2.5	HTTPS で始まるページで鍵のマークが壊れて表示された	26
2.6	種類	26
2.6.1	SSL サーバ証明書	26
2.6.2	SSL クライアント証明書	26
2.7	どんなシーンで使われている？	26
2.8	SSL 証明書は全然違う 2 種類の仕事をしている	26
2.8.1	Web サイトで送受信する情報を暗号化すること	26
2.8.2	Web サイト運営者の身元を証明すること	26
2.9	鍵マークが壊れるケース	26
2.9.1	すべて HTTP で通信しているとき	26
2.9.2	HTTPS だけど一部が HTTPS じゃないとき	26
2.10	ウェブページが表示されるまで	26
2.10.1	1 往復で表示されるわけじゃない	26
2.11	SSL 証明書は何を証明してくれるのか？	26
2.11.1	ネットバンクの事例	26
2.12	認証局事業者の身元は誰が証明する？	26
2.12.1	身元保証の連鎖をつなぐ中間 CA 証明書とルート証明書	26
2.13	SSL 証明書はどうしてあんなに値段に差があるの？	26
2.14	同じ「SSL 証明書」という名前でも 3 つの種類がある	26
2.14.1	EV 証明書	26
2.14.2	OV 証明書	26
2.14.3	DV 証明書	26
2.14.4	3 つの違いは何か？	26
2.14.5	ブラウザベンダーによる EV 証明書の扱いの変化	26
2.15	その他の証明書	26
2.15.1	中間証明書	26
2.15.2	クロスルート証明書	26
2.16	どの証明書を買えばいい？	26
2.16.1	ワイルドカード証明書	26
2.16.2	www ありにリダイレクトしたいだけなのに www なしの証明書 もいるの？	26
2.16.3	コモンネームが*.example.com の証明書は example.com で使え る？	26
2.16.4	Let'sEncrypt	26
2.17	CDN と証明書	26

2.17.1	CDN を使ったら古い端末でサイトが見られなくなった	26
2.17.2	同じサーバで複数サイトを HTTPS 化したら古い端末で別サイ トが表示された	26
2.17.3	SNI Server Name Indication	26
あとがき		27
	PDF 版のダウンロード	27
	Special Thanks:	27
	レビュアー	27
	参考文献	27
著者紹介		29

第 1 章

SSL のサイトを作ってみよう

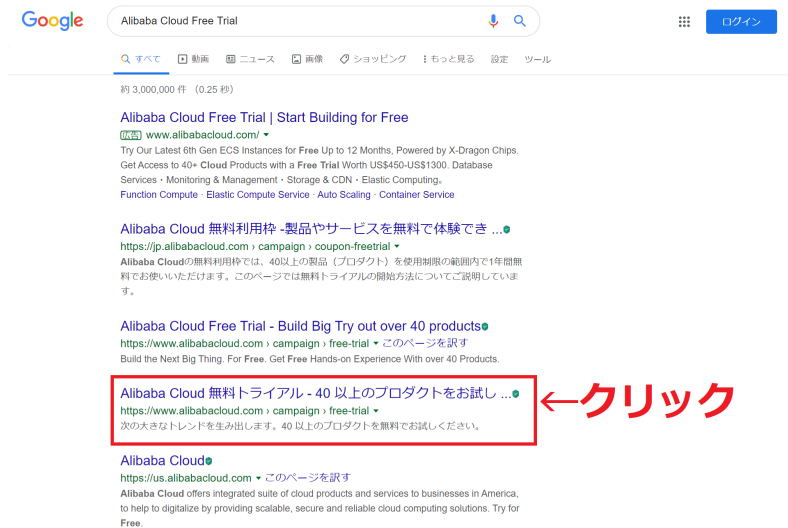
1.1 Alibaba Cloud でアカウント登録

1.1.1 無料でアカウントを作成

Google で [Alibaba Cloud Free Trial] を検索 (図 1.1)。したら、上から 4 つめの [Alibaba Cloud 無料トライアル - 40 以上のプロダクトをお試し ...] をクリックします。2 つめにもよく似た [Alibaba Cloud 無料利用枠 - 製品やサービスを無料で体験でき ...] がありますが、そちらはまた別のサイト^{*1}なので、ぐっところえて <https://www.alibabacloud.com/campaign/free-trial> と書いてある 4 つめの方をクリックしてください。

^{*1} jp.alibabacloud.com は SB クラウド (ソフトバンク株式会社とアリババグループの合併会社) が日本国内向けに提供している Alibaba Cloud で、www.alibabacloud.com はアリババグループがグローバルに提供している Alibaba Cloud である (という理解を筆者はしています)。今回はグローバル向けの後者を使います。

第1章 SSL のサイトを作ってみよう



▲図 1.1 「Alibaba Cloud Free Trial」を検索

「Alibaba Cloud 無料トライアル」*²のページを開いたら、「無料アカウントの作成」(図 1.2) をクリックします。

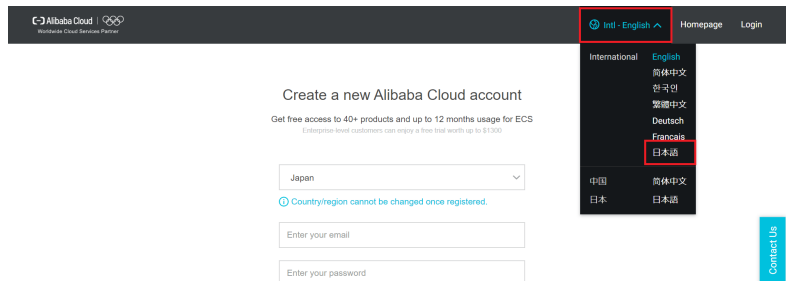


▲図 1.2 「無料アカウントの作成」をクリック

「Create a new Alibaba Cloud account」と書かれた英語のページが表示されます。右

*² <https://www.alibabacloud.com/ja/campaign/free-trial>

上の [Intl - English] から言語選択を開いて、[International] の [日本語]*3を選択します。

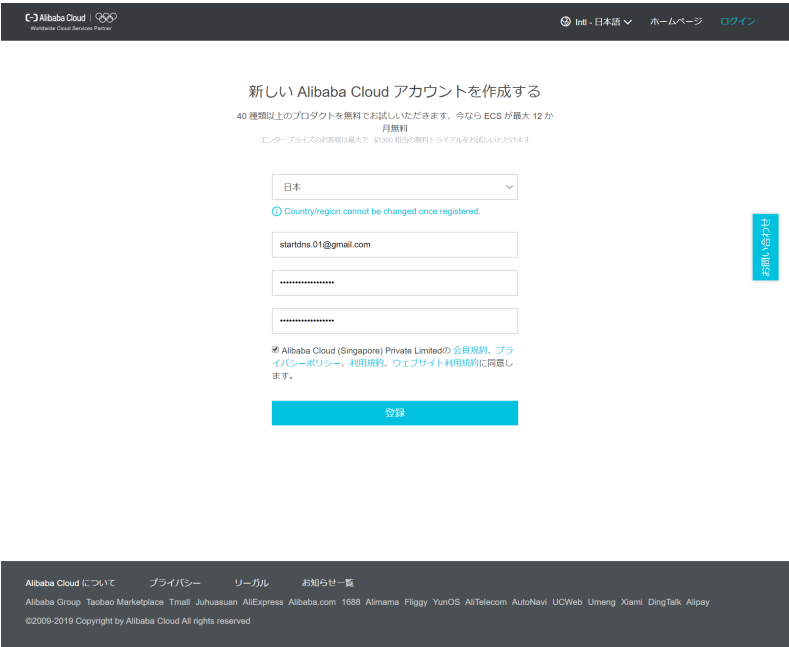


▲図 1.3 「無料アカウントの作成」をクリック

「新しい Alibaba Cloud アカウントを作成する」と書かれた日本語のページになりました。それでは次の情報を入力して、会員規約やプライバシーポリシー等を確認した上でチェックボックスにチェックを入れたら「登録」をクリックしましょう。後で分からなくならないように、登録した項目をメモしておきましょう。(表 1.1)

*3 ちなみに「日本」の「日本語」を選ぶと、前述した SB クラウドの方の Alibaba Cloud でのアカウント作成ページに遷移してしまうのでご注意ください。

第 1 章 SSL のサイトを作ってみよう

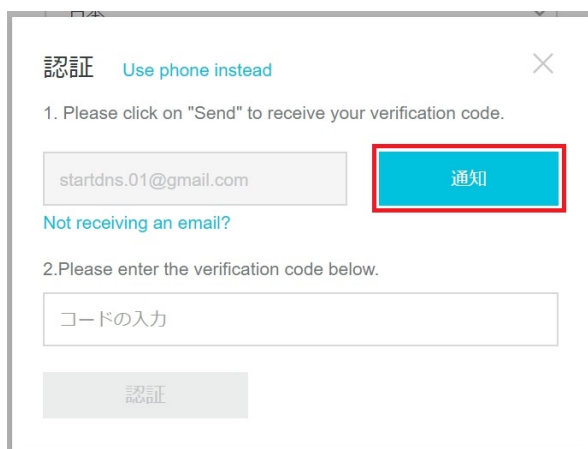


▲図 1.4 入力してチェックを入れたら「登録」をクリック

▼表 1.1 Alibaba Cloud に登録した情報

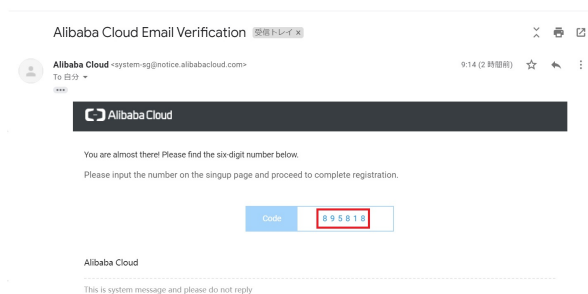
項目	例	あなたが登録した情報
国	日本	
メールアドレス	startdns.01@gmail.com	
パスワード	自作のパスワード	

登録したメールアドレス宛てに確認コードを送信するよう書いてあるので「通知」をクリックします。



▲図 1.5 メールアドレスを確認して「通知」をクリック

「Alibaba Cloud Email Verification」という件名でメールが届きます。メールの本文に書かれている Code をコピーしましょう。



▲図 1.6 Alibaba Cloud からメールが届いたら Code をコピー

メールからコピーした Code を、「2.Please enter the verification code below.」の下の欄にペーストします。「認証」をクリックしてください。

認証 Use phone instead

1. Please click on "Send" to receive your verification code.

startdns.01@gmail.com 通知

Not receiving an email?

2. Please enter the verification code below.

895818

認証

▲図 1.7 メールからコピーした Code をペーストして [認証] をクリック

もし迷惑メールフィルタなどが原因でメールが届かないときは、[Use phone instead] をクリックすれば、メールアドレスの代わりに携帯電話の番号を登録して、SMS で確認コードを受信する方法でも認証できます。

認証 Use email instead

1. Please enter your mobile phone number and click "Send Message".

+81 090*****

SMSで通知

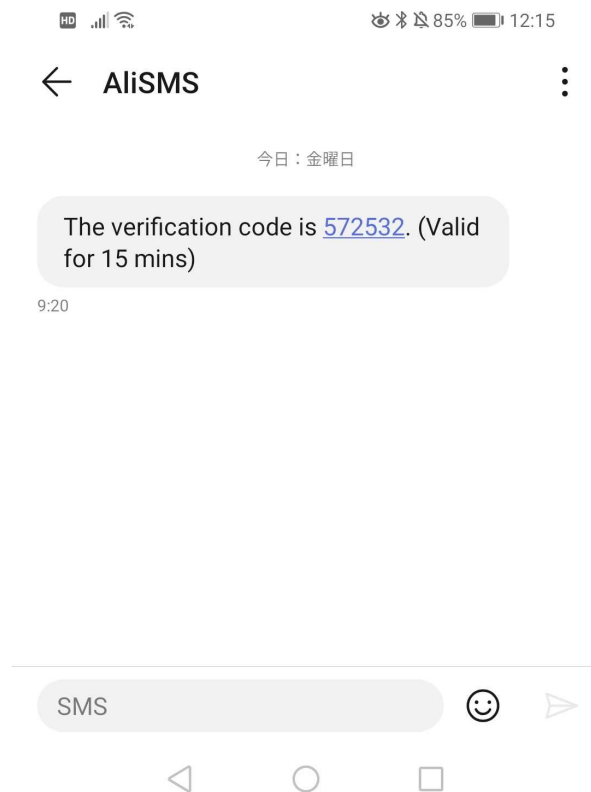
Not receiving messages?

2. Please enter the verification code below.

コードの入力

認証

▲図 1.8 携帯電話の番号を入力して [SMS で通知] をクリック



▲図 1.9 SMS で Code が届いた

無事に認証が完了したらログインページが表示されます。先ほど登録したメールアドレスとパスワードを入力したら、[サインイン] をクリックします。

第 1 章 SSL のサイトを作ってみよう



▲図 1.10 メールアドレスとパスワードを入力して [サインイン]

1.1.2 作ったアカウントでサインインする

サインインできたら、最上部の「Alibaba Cloud を始めるため、もう 1 つステップが必要です。請求先住所と支払い方法を追加してください。」の隣にある「進む >>」をクリックします。

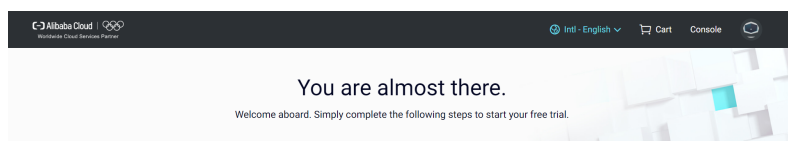


▲図 1.11 サインインできたら、最上部の「進む >>」をクリック

ここからは無料トライアルを使うために必要な情報を入力していきます。

Basic information

■ **Account Type (アカウントの種類)** このアカウントは業務用ではなく、個人的な勉強のために使うので、Account Type は「Personal account」を選択します。450 ドル相当のフリートライアルが可能だそうです。すごい。



Basic information

Account Type*

☐ Enterprise account
Get a free trial worth \$1,300 and the tax free in some countries/regions.

☒ Personal account
Sign up now to take advantage of a free trial worth \$450.

▲図 1.12 Account Type は「Personal account」を選択

■ **Billing address (請求先住所)** 続いて請求先の郵便番号、住所、氏名を入力します。*4

Billing address*

Account email*
startdms.01@gmail.com Verified

Address line 1*
港区東新橋1丁目9-2

Address line 2
汐留住友ビル 27F

City*
東京都

State/Province*
Kanto

Postal Code
105-0021

Country/Region*
Japan

Last Name*
藤村

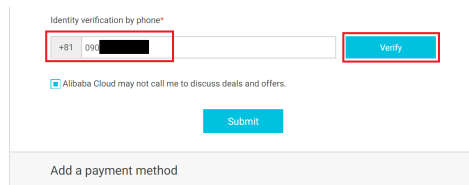
First Name*
もち子

▲図 1.13 郵便番号、住所、氏名を入力する

■ **Identity verification by phone (電話認証)** 最後に携帯電話の番号を入力したら、「Verify」をクリックします。

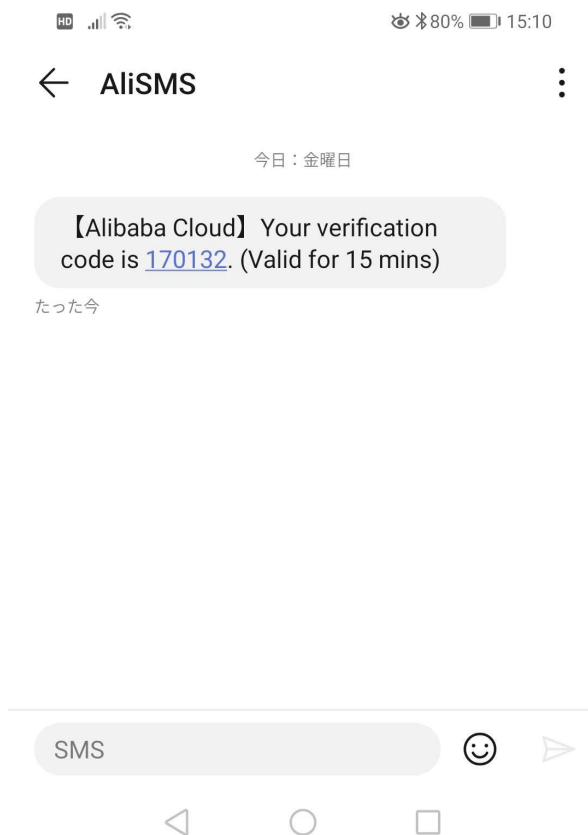
*4 キャプチャでは、郵便番号と住所はSBクラウドのオフィスをサンプルとして入力しています。実際はご自身の住所やお名前をきちんと登録してください。

第 1 章 SSL のサイトを作ってみよう



▲図 1.14 携帯電話の番号を入力したら [Verify] をクリック

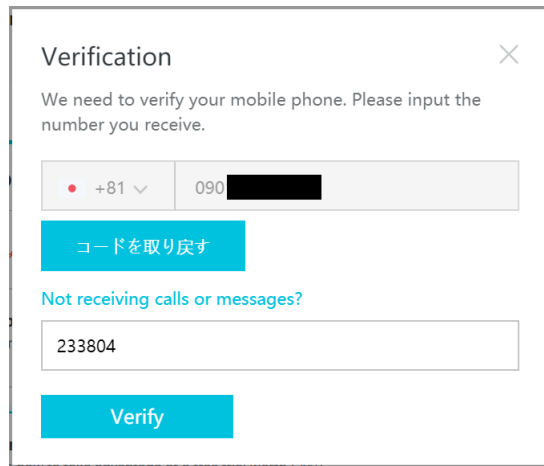
[Ali SMS] から SMS が届きます。



▲図 1.15 SMS で Code が届いた

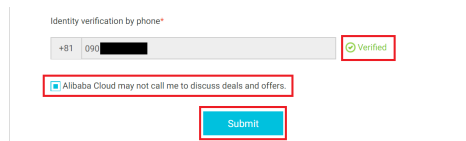
SMS に書いてあった Code を、[Verification] の下の欄に入力します。[Verify] をク

リックしてください。

A verification dialog box titled "Verification" with a close button (X) in the top right corner. The text inside says "We need to verify your mobile phone. Please input the number you receive." Below this is a phone number input field showing "+81" as a country code and "090" followed by a masked number. There is a blue button labeled "コードを取り戻す" (Get code). Below that is a link "Not receiving calls or messages?". Underneath is a text input field containing the code "233804". At the bottom is a large blue button labeled "Verify".

▲図 1.16 SMS に書いてあった Code を入力して [Verify] をクリック

[Verified] と表示されたら電話認証は完了です。もしこの番号で営業電話を受けたくないければ、[Alibaba Cloud may not call me to discuss deals and offers.] にもチェックを入れておきましょう。[Submit] をクリックします。

A screen titled "Identity verification by phone*". It shows the phone number "+81 090" followed by a masked number and a green "Verified" status. Below this is a checkbox labeled "Alibaba Cloud may not call me to discuss deals and offers." which is checked. At the bottom is a blue "Submit" button.

▲図 1.17 [Verified] と表示されたことを確認して [Submit] をクリック

■**Add a payment method (支払い方法の追加)** 続いて支払い方法を追加します。Alibaba Cloud では、AWS と同じように使った分だけ請求が来ます。本著では無料トライアルの範囲内で Alibaba Cloud を使っていきますが、支払い方法は登録しておく必要があります。

[Add] をクリックして、クレジットカードの情報を登録しましょう。

第 1 章 SSL のサイトを作ってみよう

The screenshot shows the Alibaba Cloud account setup interface. At the top, the header includes the Alibaba Cloud logo, 'Welcome to Alibaba Cloud', and navigation links for 'Intl - English', 'Cart', and 'Console'. Below the header, a message states 'You are almost there. Welcome aboard. Simply complete the following steps to start your free trial.' The main content area is titled 'Basic information' and contains a section 'Add a payment method'. This section has two options: 'Credit or Debit Card' with logos for Visa, MasterCard, and American Express, and an 'Add' button; and 'PayPal' with the PayPal logo and a 'Link' button. A note at the bottom of the section states: 'You will not be charged by Alibaba Cloud until you use cloud resources. You can manage payment methods in the Payment Methods module of the Billing Management console.'

▲図 1.18 [Add] をクリックしてクレジットカードの情報を登録

カード情報を入力したら [Submit] をクリックします。

1.1 Alibaba Cloud でアカウント登録

The screenshot shows the Alibaba Cloud account registration process. At the top, a banner says "You are almost there. Welcome aboard. Simply complete the following steps to start your free trial." Below this is the "Basic information" section, which includes a "Add a payment method" form. The form is for a "Credit or Debit Card" and lists supported cards: JCB, VISA, MasterCard, and American Express. It includes two instructions: "1. A bank card can only be added to one Alibaba Cloud account at a time." and "2. Prepaid cards, virtual cards, and gift cards are not supported." The form fields are: Card Number (masked), Expiration Date (masked), CVV (masked), First Name (masked), Middle Name (empty), Last Name (masked), Company Name on Card (empty), and Billing Address (masked). A red "Submit" button is at the bottom of the form. Below the form is a "PayPal" section with a "PayPal" logo and a "Bind" button. At the bottom of the page, there is a footer with links for "About Us", "Privacy Policy", "Legal", and "Notice List", and a copyright notice: "© 2009-2019 Copyright by Alibaba Cloud All rights reserved."

Alibaba Cloud |

Intl - English | Cart | Console

You are almost there.

Welcome aboard. Simply complete the following steps to start your free trial.

Basic information

Add a payment method

Credit or Debit Card

Recommended to all customers.
Supports JCB, VISA, MasterCard, and American Express credit or debit cards.

1. A bank card can only be added to one Alibaba Cloud account at a time.
2. Prepaid cards, virtual cards, and gift cards are not supported.

Card Number *

Expiration Date * CVV *

First Name *

Middle Name

Last Name *

Company Name on Card

Billing Address * [Edit](#)

[Submit](#)

To verify that your card is valid, after you submit your card information, Alibaba Cloud will place a USD 1.00 pre-authorization hold on your bank card and will cancel the pre-authorization hold soon after you pass the verification.

PayPal

Associate your Alibaba Cloud account with your PayPal account. [Bind](#)

You will not be charged by Alibaba Cloud until you use cloud resources. You can manage payment methods in the Payment Methods module of the Billing Management console.

About Us | Privacy Policy | Legal | Notice List

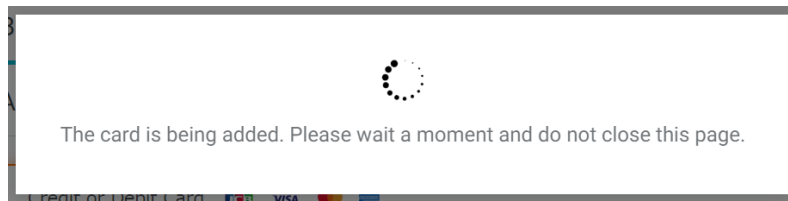
Alibaba Group Taobao Marketplace Tmall Juhuasuan AliExpress Alibaba.com 1688 Alimama Alltrip YunOS AliTelecom AutoNavi UCWeb Umeng Xiami DingTalk Alipay

© 2009-2019 Copyright by Alibaba Cloud All rights reserved

▲図 1.19 カード情報を入力したら [Submit] をクリック

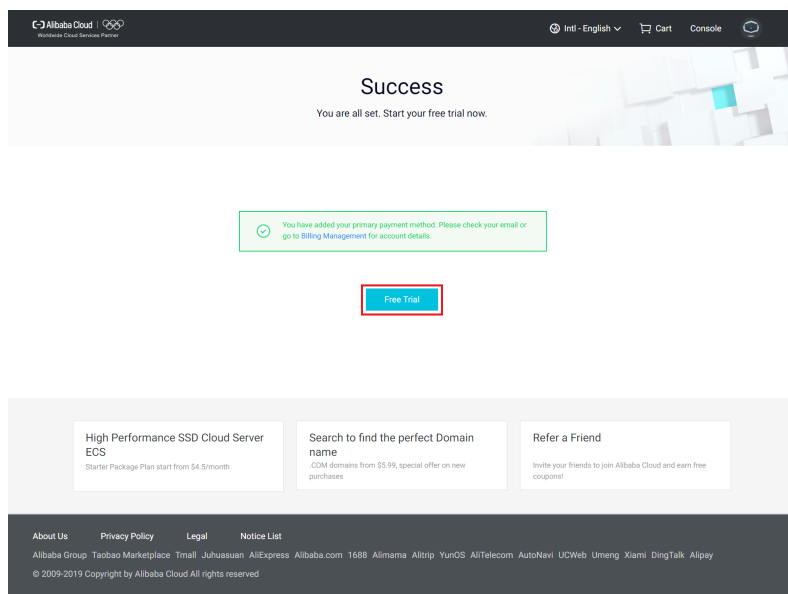
こんな感じで「ちょっと待ってね…」と表示されたのちに…

第 1 章 SSL のサイトを作ってみよう



▲図 1.20 ちょっと待ってね…の表示

[Success] と表示されたら、請求先住所と支払い方法の登録は完了です。これで無料トライアルが使えるようになりました！早速 [Free Trial] をクリックして、HTTPS のサイトを乗っけるサーバを立ててみましょう。



▲図 1.21 [Success] と表示されたら登録完了

1.2 Alibaba Cloud でサーバを立てよう

1.3 ドメイン名の設定

1.4 まずは HTTP でサイトを公開

1.5 証明書を取得しよう

1.5.1 秘密鍵を作ろう

1.5.2 CSR を作ろう

1.5.3 証明書の取得申請

1.5.4 取得した証明書をサーバに置こう

1.6 HTTPS でサイトを公開

第 2 章

基本

2.1 SSL ってなに？

2.2 TLS ってなに？

2.3 SSL と TLS の違いは？

2.4 SSL と SSH って似てる？ 何が違うの？

2.5 HTTPS で始まるページで鍵のマークが壊れて表示された

2.6 種類

2.6.1 SSL サーバ証明書

2.6.2 SSL クライアント証明書

2.7 どんなシーンで使われている？

2.8 SSL 証明書は全然違う 2 種類の仕事をしている

2.8.1 Web サイトで送受信する情報を暗号化すること

2.8.2 Web サイト運営者の身元を証明すること

2.9 鍵マークが壊れるケース

2.9.1 すべて HTTP で通信しているとき

2.9.2 HTTPS だけど一部が HTTPS じゃないとき

画像と CSS の指定が絶対パスだった

2.10 ウェブページが表示されるまで

あとがき

数ある技術書の中から「SSL をはじめよう」を手にとってくださったあなたに感謝します。

2020 年 2 月
mochikoAsTech

PDF 版のダウンロード

本著（紙の書籍）をお買い上げいただいた方は、下記の URL から PDF 版を無料でダウンロードできます。

- ダウンロード URL : <https://mochikoastech.booth.pm/items/xxxxxx>
- パスワード : xxxxxx

Special Thanks:

- ネコちゃん

レビューアー

- Takeshi Matsuba

参考文献

- ぶんけん
– ??

著者紹介

mochiko / @mochikoAsTech

元 Web 制作会社のシステムエンジニア。技術書典で出した本がきっかけで、テクニカルライターの仕事を始めた。モバイルサイトのエンジニア、SIer とソーシャルゲームの広報を経て、2013 年よりサーバホスティングサービスの構築と運用を担当したのち、再び Web アプリケーションエンジニアとしてシステム開発に従事。「分からない気持ち」に寄り添える技術者になれるように日々奮闘中。技術書典 4,5,6 で頒布した「DNS をはじめよう」「AWS をはじめよう」「技術をつたえるテクニック」「技術同人誌を書いたあなたへ」は累計で 7,800 冊を突破。

- <https://twitter.com/mochikoAsTech>
- <https://mochikoastech.booth.pm/>
- <https://note.mu/mochikoastech>
- <https://mochikoastech.hatenablog.com/>

Hikaru Wakamatsu

表紙デザインを担当。

Shinya Nagashio

挿絵デザインを担当。

SSLをはじめよう

証明書の発行からトラブルシューティングまで

2020年2月29日 技術書典8 初版

著 者 mochikoAsTech
デザイン Hikaru Wakamatsu / Shinya Nagashio
発行所 mochikoAsTech
印刷所 日光企画

(C) 2019 mochikoAsTech