

SSL/TLS サーバー証明書

Java 実行環境(keytool)

CSR 作成/証明書インストール手順書

(新規・更新用)

Version 1.0

PUBLIC RELEASE

2026/08/27

改訂履歴

日付	バージョン	内容
2026/08/27	1.0	初版リリース

目次

はじめに	4
サーバー証明書お申込みフロー	5
CSR の作成	6
1. CSR 作成前のご確認事項	7
1.1. 公開鍵長のご指定について	7
1.2. CSR 作成時に指定する項目 (DN)について	7
1.3. 本手順の設定例について	7
2. キーストアファイル・キーペアファイル・CSR の作成	8
2.1. キーストアファイルとキーペアファイルの作成方法	8
2.2. CSR の作成方法	11
3. キーストアファイルのバックアップ	11
4. 証明書のお申し込み	12
証明書のインストール	13
5. 証明書のダウンロード	14
5.1. ルート・中間 CA 証明書のダウンロード	14
5.2. サーバー証明書のダウンロード	14
» SSL/TLS サーバー証明書のダウンロードについて	14
6. 証明書のインストール	15
6.1. ルート証明書のインストール	15
6.2. クロスルート証明書のインストール	16
6.3. 中間 CA 証明書のインストール	17
6.4. サーバー証明書のインストール	18
7. キーストアファイルのバックアップ	19
8. ご参考までに	19
8.1. エイリアスの確認方法	19
8.2. エイリアスの削除方法	20

はじめに

【！】本手順書をご利用の前に必ずお読みください

本ドキュメントは、Java 実行環境(JRE/JDK)が導入された各種サーバー環境下で、サイバートラストのサーバー証明書をご利用いただく際に必要となる、keytool コマンドを使用したキーストアおよび CSR の作成、各種証明書のインポート手順について解説するドキュメントです。

本手順は、「Windows OS」および「Linux OS」上の「Java SE 17」「Java SE 21」環境下で動作確認をしております。また、Java 実行環境(path 設定を含む)がすでに設定されており、コマンドプロンプトまたはターミナル上での keytool コマンドが実行できる事を前提としております。

実際の手順はお客様の環境やご使用中のシステム、アプリケーションサーバーにより異なる場合があります。keytool コマンドの動作および証明書の設定を保証するものではありません。あらかじめご了承ください。

なお、このドキュメントは予告なく変更される場合があります。サイバートラスト株式会社はその内容に対して責任を負うものではありません。

また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。

このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。

ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。

サーバー証明書お申込みフロー

サーバー証明書のご購入については、以下のお申込みフローをご確認ください。

本手順では、**赤枠**で囲まれた部分のフローをご案内しています。



CSR の作成

1. CSR 作成前のご確認事項

CSR 作成前に以下についてご確認ください。

1.1. 公開鍵長のご指定について

公開鍵長は「2048bit」「3072bit」「4096bit」をご指定ください。

1.2. CSR 作成時に指定する項目(DN)について

詳細は以下をご確認ください。

≫ [CSR 作成時に指定する項目について](#)

1.3. 本手順の設定例について

本手順では以下の設定を例としてご案内しております。

種類	名称
キーストアのファイル名	server.keystore
サーバー証明書のエイリアス名	cybertrust
CSR のファイル名	server.csr

【！】注意事項

- ・お客様の環境によりファイルやパスが異なりますので、環境に合わせてお読み替えてください。
- ・既存のファイルと同名で作成した場合、既存のファイルへ新しいファイルが上書きされますので、別名をご指定ください。

2. キーストアファイル・キーペアファイル・CSR の作成

Java 実行環境下では、コマンドプロンプトやターミナル上で keytool を用いてキーストアファイルを作成・エイリアスをご指定のうえ、キーペアファイル(公開鍵・秘密鍵のペア)と CSR を作成します。

※証明書の更新や他社からのお乗換えの際も同様の手順です。

2.1. キーストアファイルとキーペアファイルの作成方法

キーストアファイルとキーペアファイルを作成します。

- A) コマンドプロンプトで以下のコマンドを入力し、キーストアファイルとキーペアファイルを作成します。

■ コマンド入力

```
keytool -genkey -alias 「サーバー証明書のエイリアス名(任意)」 -  
keyalg RSA -keysize 2048 -keystore 「キーストアファイル名(任意)」
```

例) keytool -genkey -alias cybertrust -keyalg RSA -keysize 2048 -keystore
server.keystore

※証明書の更新や他社からのお乗換えの際、**キーストアファイル名は既存のキーストアファイル名と別名**をご指定ください。

- B) 以下が表示されますので、キーストアファイルのパスフレーズとして任意の文字列(6 文字以上)を入力します。

キーストアのパスワードを入力してください:

- C) パスフレーズを再入力します。

新規パスワードを再入力してください:

D) DN 情報の入力

■ 姓名を入力してください。

入力必須項目です。

申請するサーバー証明書の FQDN 名(サーバ名+ドメイン名)を入力してください。

例) www.cybertrust.ne.jp

```
姓名を入力してください。  
[Unknown]: www.cybertrust.ne.jp
```

■ 組織単位名を入力してください。

任意入力項目です。

必要に応じて申請する組織の部署名を入力してください。

※2022 年 6 月 23 日以降に発行されるサーバー証明書には含まれません。

例) Technical Division

```
組織単位名を入力してください。  
[Unknown]: Technical Division
```

■ 組織名を入力してください。

入力必須項目です。

申請する英訳組織名を入力してください。

例) Cybertrust Japan Co.,Ltd.

```
組織名を入力してください。  
[Unknown]: Cybertrust Japan Co.,Ltd.
```

■ 都市名または地域名を入力してください。

入力必須項目です。

申請する組織の市町村名を入力してください。(東京 23 区は区名)

例) Minato-ku

```
都市名または地域名を入力してください。  
[Unknown]: Minato-ku
```

■ 州名または地方名を入力してください。

入力必須項目です。

申請する組織の都道府県名を入力してください。

例) Tokyo

```
州名または地方名を入力してください。
[Unknown]: Tokyo
```

■ この単位に該当する 2 文字の国番号を入力してください。

JPと入力します。

```
この単位に該当する 2 文字の国番号を入力してください。
[Unknown]: JP
```

E) 入力内容を確認し、誤りがなければ「y」と入力して、Enter キーを押します。

```
CN=www.cybertrust.ne.jp, OU=Technical Division, O="Cybertrust Japan Co.,Ltd.", L=Minato-ku,
ST=Tokyo, C=JP よろしいですか?
[no]: y
```

F) 何も入力せずに Enter キーを押します。

```
<cybertrust> の鍵パスワードを入力してください。
(キーストアのパスワードと同じ場合は RETURN を押してください):
```

以上でキーストアファイルとキーペアファイルの作成が完了します。

2.2. CSR の作成方法

- A) コマンドプロンプトで以下のコマンドを入力し、指定した秘密鍵ファイルから CSR を作成します。

※CSR は既存の CSR と同ファイル名を指定した場合、ファイルが上書きされますので、ご注意ください。

■ コマンド入力

keytool -certreq -alias 「サーバー証明書のエイリアス名」 -file 「CSR 名(任意)」 -keystore 「キーストアファイル名」

例) keytool -certreq -alias cybertrust -file server.csr -keystore server.keystore

- B) キーストアファイルに設定したパスワードを入力します。

キーストアのパスワードを入力してください:

以上で CSR の作成は完了です。

3. キーストアファイルのバックアップ

秘密鍵ファイルを含むキーストアファイル(server.keystore など)は、証明書の設定やサーバー復旧時に必要となる重要なデータです。

障害等による消失や破損に備え、安全な場所にバックアップを保管してください。

なお、弊社がお客様のキーストアファイルを受け取ることはございません。あらかじめご了承ください。

4. 証明書のお申し込み

作成した CSR をテキストエディタで開いて内容をコピーし、WEB の申請サイト ([SureBoard](#) / [SureHandsOn](#)) の申請フォームへ貼り付けて、弊社へお申し込みください。

＜CSR サンプル＞ ※ こちらは申請にご利用いただけません。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
. . . . .
MIIEhDCCA2wCAQAwYkxCzAJBgNVBAYTAkpQM4wDAYDVQQIDAVU2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBIDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDA1UZXRNOIFVuaXQxHjAcBgNVBAMMFXRlc3QuY3IiZXJ0cnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4R0cFsgRk05FgeUCaeDFyIIEST
. . . . .
-----END NEW CERTIFICATE REQUEST-----
```

「-----BEGIN NEW CERTIFICATE REQUEST-----」から、「-----END NEW CERTIFICATE REQUEST-----」までをハイフンを含め、すべてコピーし申請画面に貼り付けてください。

なお、1 文字でも欠けると正しく解析できませんのでご注意ください。

【！】CSR 作成後の注意事項

発行されたサーバー証明書は CSR を作成したエイリアスと同一のエイリアスへインストールします。インストールを行う前にキーストアファイルやエイリアスの削除を行わないよう、ご注意ください。

証明書のインストール

【！】本手順はサーバー証明書の発行後に行います。

5. 証明書のダウンロード

インストールが必要な中間 CA 証明書・サーバー証明書をダウンロードします。

5.1. ルート・中間 CA 証明書のダウンロード

サーバー証明書をご利用の際、お使いの機器へルート証明書と中間 CA 証明書のインストールが必要です。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社 Web ページからダウンロードしてください。

≫ [ルート・中間 CA 証明書のダウンロード](#)

※ 2026 年 8 月 27 日以降に発行されるサーバー証明書を利用する場合は、「クロスルート証明書」と「中間 CA 証明書」をダウンロードしてください。

また、ご利用商品や必要な証明書の種類がご不明の場合は、以下をご覧ください。

≫ [どの中間 CA 証明書をダウンロードすればよいですか？](#)

5.2. サーバー証明書のダウンロード

サーバー証明書が発行されましたら、証明書発行のお知らせのメール内リンクよりダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

≫ [SSL/TLS サーバー証明書のダウンロードについて](#)

6. 証明書のインストール

ルート証明書、クロスルート証明書、中間 CA 証明書、サーバー証明書の順番でインストールします。

※本手順では以下の設定を例としてご案内しています。

項目	ファイル名	エイリアス名
ルート証明書	scrca2.txt	root
クロスルート証明書	tlrsarootca2024cross-pem.txt	cross
中間 CA 証明書	ovrsaca2025e1.txt	CA
サーバー証明書	servercert.cer	cybertrust
作成したキーストア	server.keystore	

6.1. ルート証明書のインストール

ルート証明書のインストールを行います。

A) コマンドプロンプトで以下のコマンドを入力し、ルート証明書をインストールします。

※「ルート証明書エイリアス名」は、他のエイリアス名と重複しないように異なるエイリアス名を指定してください。

■ コマンド入力

keytool -import -alias 「ルート証明書エイリアス名(任意)」 -keystore 「キーストアファイル名」 -file 「ルート証明書ファイル名」

例) keytool -import -alias root -keystore server.keystore -file scrca2.txt

B) キーストアファイルに設定したパスワードを入力します。

C) 「yes」と入力して Enter キーを押します。

D) 以上でルート証明書のインストールが完了します。

```
D:\Program Files\Java\jdk-17\bin>keytool -import -alias root -keystore server.keystore -file scrca2.txt
キーストアのパスワードを入力してください:
```

: (中略) :

```
この証明書を信頼しますか。[いいえ]: y
証明書がキーストアに追加されました
```

6.2. クロスルート証明書のインストール

※2026 年 8 月 27 日以降に発行されるサーバー証明書を利用する場合のみ、クロスルート証明書のインストールを行います。

A) コマンドプロンプトで以下のコマンドを入力し、クロスルート証明書をインストールします。

※「クロスルート証明書エイリアス名」は、他のエイリアス名と重複しないように異なるエイリアス名を指定してください。

■ コマンド入力

```
keytool -import -alias 「クロスルート証明書エイリアス名(任意)」 -  
keystore 「キーストアファイル名」 -file 「クロスルート証明書ファイ  
ル名」
```

例) `keytool -import -alias cross -keystore server.keystore -file
tlsrsarootca2024cross-pem.txt`

B) キーストアファイルに設定したパスワードを入力します。

C) 以上でクロスルート証明書のインストールが完了します。

```
C:\Program Files\Java\jdk-17\bin>keytool -import -alias cross -keystore server.keystore -file tlsrsarootca2024cross-pem.txt  
キーストアのパスワードを入力してください:
```

```
証明書がキーストアに追加されました
```

6.3. 中間 CA 証明書のインストール

中間 CA 証明書のインストールを行います。

A) コマンドプロンプトで以下のコマンドを入力し、中間 CA 証明書をインストールします。

※「中間 CA 証明書エイリアス名」は、他のエイリアス名と重複しないように異なるエイリアス名を指定してください。

■ コマンド入力

```
keytool -import -alias 「中間 CA 証明書エイリアス名(任意)」 -keystore 「キーストアファイル名」 -file 「中間 CA 証明書ファイル名」
```

例)keytool -import -alias CA -keystore server.keystore -file ovrsaca2025e1.txt

B) キーストアファイルに設定したパスワードを入力します。

C) 以上で中間 CA 証明書のインストールが完了します。

```
C:\Program Files\Java\jdk-17\bin>keytool -import -alias CA -keystore server.keystore -file ovrsaca2025e1.txt
キーストアのパスワードを入力してください:
証明書がキーストアに追加されました
```

6.4. サーバー証明書のインストール

サーバー証明書のインストールを行います。

A) コマンドプロンプトで以下のコマンドを入力し、サーバー証明書をインストールします。

※「サーバー証明書エイリアス名」は、**キーペアファイル作成時に指定したエイリアス名を指定**してください。

■ コマンド入力

```
keytool -import -alias 「サーバー証明書エイリアス名」 -keystore  
「キーストアファイル名」 -file 「サーバー証明書ファイル名」
```

例)keytool -import -alias cybertrust -keystore server.keystore -file servercert.cer

B) キーストアファイルに設定したパスワードを入力します。

キーストアのパスワードを入力してください:

C) 以上でサーバー証明書のインストールが完了します。

証明書応答がキーストアにインストールされました。

以上でルート証明書、クロスルート証明書、中間 CA 証明書、サーバー証明書のインポートは完了です。

完成したキーストアファイルを、ご利用のシステム環境(各種サーバーやパッケージソフト等)に適用してご使用ください。

【システムへの適用について】

作成したキーストアファイルを Web サーバーやアプリケーションに紐付けるための設定手順(XML ファイルの編集や管理コンソールでの登録など)は、ご利用の環境によって異なります。

キーストアファイルのシステムへの設定方法につきましては、お使いのシステム(WebLogic、独自アプリケーション、または各種サーバー等)の取扱説明書やマニュアルに従って設定を行ってください。

7. キーストアファイルのバックアップ

秘密鍵ファイルを含むキーストアファイル(server.keystore など)は、証明書の設定やサーバー復旧時に必要となる重要なデータです。

障害等による消失や破損に備え、安全な場所にバックアップを保管してください。

なお、弊社がお客様のキーストアファイルを受け取ることはございません。あらかじめご了承ください。

8. ご参考までに

ご参考までに、エイリアスの内容確認や削除方法をご案内します。

8.1. エイリアスの確認方法

以下のコマンドにてキーストアファイルに登録されているエイリアスの内容を確認できます。

■ コマンド

keytool -list -v -alias 「エイリアス名」 -keystore 「キーストアファイル名」

コマンド例)keytool -list -v -alias cybertrust -keystore server.keystore

出力例)

別名: cybertrust

作成日: 2026/08/15

エントリ・タイプ: PrivateKeyEntry

証明書チェーンの長さ: 4

証明書[1]:

項目	内容
別名	エイリアス名
作成日	エイリアスを作成した日時
エントリ・タイプ	PrivateKeyEntry ⇒ 秘密鍵の含まれているエイリアス
	trustedCertEntry ⇒ 秘密鍵の含まれていないエイリアス
証明チェーンの長さ	エイリアスの中に登録されている証明連鎖の長さ 例)【1】ルート証明書、中間 CA 証明書、サーバー証明書で構成される 3 階層 ⇒「3」と表示されます。 【2】ルート証明書、クロスルート証明書、中間 CA 証明書、サーバー証明書で構成される 4 階層 ⇒「4」と表示されます。
証明書[n]	証明連鎖の番号

8.2. エイリアスの削除方法

以下のコマンドにてキーストアファイルに登録されている不要なエイリアスを削除できます。

■ コマンド

keytool -delete -alias 「削除したいエイリアス名」 -keystore 「キーストアファイル名」

例) keytool -delete -alias cybertrust -keystore server.keystore

キーストアファイルに設定したパスワードを入力後、指定したエイリアスが削除されます。

キーストアのパスワードを入力してください: