



# Riverbed® Stingray Traffic Manager CSR作成/証明書インストール手順書

# はじめに

## **【！】本手順書をご利用の前に必ずお読みください**

1. 本ドキュメントは、「Riverbed®/Stingray Traffic Manager」の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のCSR作成とサーバー証明書のインストールについて解説するドキュメントです。
2. 本ドキュメントは、図研ネットウェイブ株式会社のご協力の元、作成しております。
3. 実際の手順はお客様の環境により異なる場合があり、「Stingray Traffic Manager」の動作を保証するものではございません。あらかじめご了承ください。
4. このドキュメントは予告なく変更される場合があり、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。
5. 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。

# はじめに

## 目 次

1. CSRの作成 --- P4～
2. 証明書のお申し込み --- P9～
3. 証明書のダウンロード --- P10
4. 証明書のインストール --- P11～
5. 証明書インストール後の設定(例) --- P17～
6. SSL通信の確認 --- P21

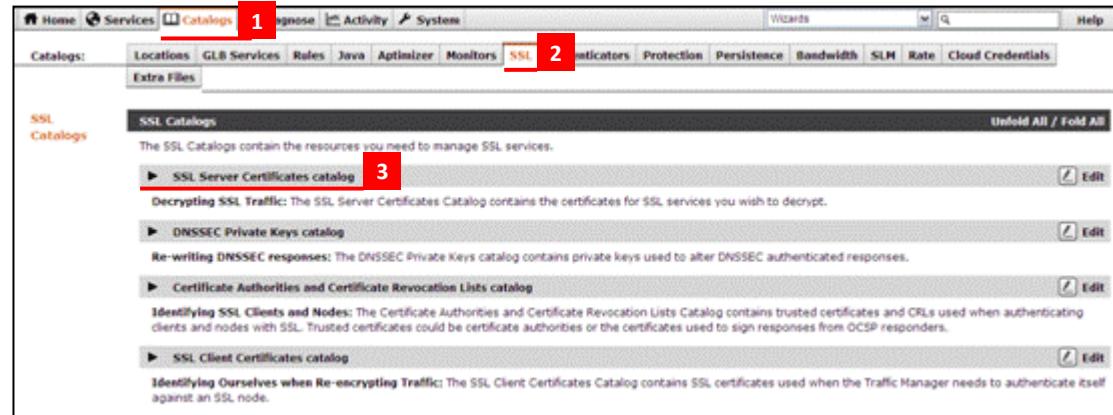
# 1. CSRの作成

## ■CSRを作成します。

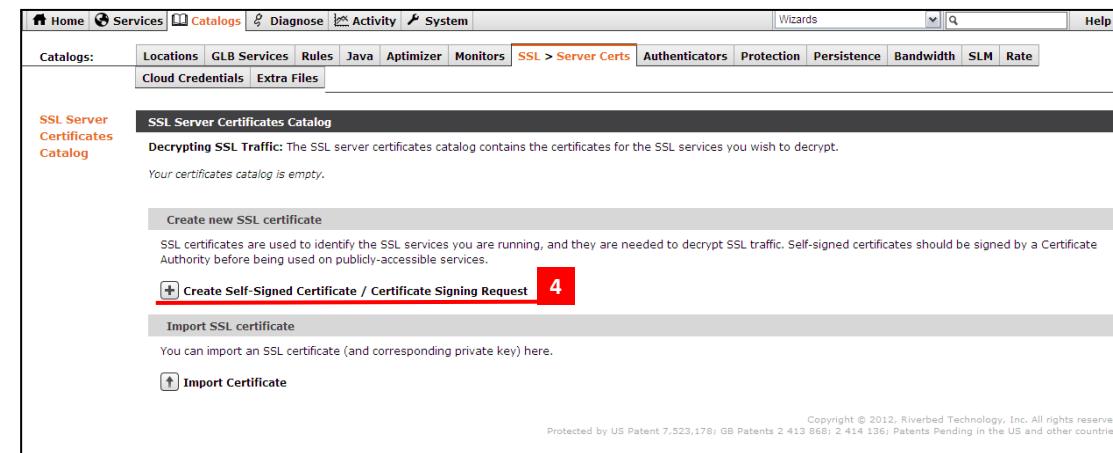
※CSRの作成方法は、以下のWebページもご参照下さい。

<https://www.cybertrust.co.jp/ssl/support/csr.html>

1. Administration interface ヘログイン後、Home画面から[Catalogs]タブをクリックします。
2. [SSL]タブをクリックします。
3. [SSL Server Certificates catalog]をクリックします。
4. [Create new SSL certificate]の「Create Self-Signed Certificate / Certificate Signing Request」をクリックします。



The screenshot shows the CyberTrust Administration interface. The top navigation bar includes Home, Services, Catalogs (highlighted with a red box labeled '1'), Diagnose, Activity, System, Wizards, Help, and a search bar. The Catalogs menu bar has tabs for Locations, GLB Services, Rules, Java, Optimizer, Monitors, SSL (highlighted with a red box labeled '2'), Authenticators, Protection, Persistence, Bandwidth, SLM, Rate, and Cloud Credentials. The main content area is titled 'SSL Catalogs' and contains a list of catalogs: 'SSL Server Certificates catalog' (highlighted with a red box labeled '3'), 'DNSSEC Private Keys catalog', 'Certificate Authorities and Certificate Revocation Lists catalog', and 'SSL Client Certificates catalog'. Each catalog entry includes a brief description and an 'Edit' link.



The screenshot shows the 'SSL Server Certificates Catalog' screen. The top navigation bar is identical to the previous screenshot. The Catalogs menu bar has tabs for Locations, GLB Services, Rules, Java, Optimizer, Monitors, SSL (highlighted with a red box labeled '2'), Authenticators, Protection, Persistence, Bandwidth, SLM, Rate, and Cloud Credentials (highlighted with a red box labeled '1'). The main content area is titled 'SSL Server Certificates Catalog' and contains a message: 'Decrypting SSL Traffic: The SSL server certificates catalog contains the certificates for the SSL services you wish to decrypt. Your certificates catalog is empty.' Below this, there are two buttons: '+ Create Self-Signed Certificate / Certificate Signing Request' (highlighted with a red box labeled '4') and 'Import SSL certificate'. A note below the buttons says: 'You can import an SSL certificate (and corresponding private key) here.' At the bottom of the page, there is a copyright notice: 'Copyright © 2012, Riverbed Technology, Inc. All rights reserved. Protected by US Patent 7,523,178; GB Patents 2 413 868; 2 414 136; Patents Pending in the US and other countries.'

# 1. CSRの作成

5. [Name:]に任意の登録名を指定します。  
この値は、証明書の設定時などに使用します。  
※空欄の場合は、【6】の値が使用されます。
6. [Common Name (CN):]に、「実際に接続するURLのFQDN」を指定します。  
例) <https://www.cybertrust.ne.jp/index.html>  
⇒ www.cybertrust.ne.jp
7. [Organisation (O):]に「申請組織の名称(英名)」を指定します。
8. [Organisational Unit (OU):]に任意の値(部署名など)を指定します。  
※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。  
※この値は空欄でも構いません。
9. [Location (L):]に申請組織の事業所住所の「市町村名(英名)※」を指定します。  
※東京 23 区は区名を指定します。

**Create New SSL Certificate**

This form lets you create a new, self-signed certificate. You will then be able to create a Certificate Signing Request for this certificate.

Enter a short name to identify your certificate. If you leave this blank, the 'Common Name' field will be used.

**Name:**  5

The public DNS address of your server, such as 'secure.yourcompany.com':

**Common Name (CN):**  6 www.cybertrust.ne.jp

The name of your organisation, such as 'Your Company':

**Organisation (O):**  7 Cybertrust Japan Co.,Ltd.

The unit within your organisation, such as 'Sales':

**Organisational Unit (OU):**  8 Technical Division (tional)

Your location (town or city), such as 'Anytown':

**Location (L):**  9 Minato-ku

Your state or province, such as 'Somestate':

**State (S):**  10 Tokyo (required for US only)

Your two-letter country code, such as 'US', 'GB' or 'FR':

**Country (C):**  11 JP

How long should this certificate be valid for:

**Expires in:**  1 year ▾

Private key size (1024 bits recommended):

**Key size:**  12 2048 bits ▾

**Create certificate**

# 1. CSRの作成

10. [State (S):]に申請組織の事業所住所の「都道府県名(英名)」を指定します。
11. [Country (C):]に申請組織の「国名(JP固定)」を指定します。
12. [Expires in:]はCSRと同時に作成される自己署名用の証明書の有効期限を設定します。  
CSRや弊社から発行される証明書には影響がないため、デフォルトで構いません。
13. [Key size:]は「2048 bits」を指定します。
14. すべての入力が終わったら、「Create certificate」ボタンをクリックします。

**Create New SSL Certificate**

This form lets you create a new, self-signed certificate. You will then be able to create a Certificate Signing Request for this certificate.

Enter a short name to identify your certificate. If you leave this blank, the 'Common Name' field will be used.

**Name:**

The public DNS address of your server, such as 'secure.yourcompany.com':

**Common Name (CN):**

The name of your organisation, such as 'Your Company':

**Organisation (O):**

The unit within your organisation, such as 'Sales':

**Organisational Unit (OU):**  (optional)

Your location (town or city), such as 'Anytown':

**Location (L):**

Your state or province, such as 'Somestate':

**State (S):**  10 required for US only

Your two-letter country code, such as 'US', 'GB' or 'FR':

**Country (C):**  11

How long should this certificate be valid for:

**Expires in:**  12

Private key size (1024 bits recommended):

**Key size:**  13

**Create certificate** 14

# 1. CSRの作成

15. 「Your configuration has been updated.」と表示され、指定した値が表示されます。  
ご指定の値にお間違いがないか、確認してください。
16. 「Export CSR / Sign Certificate」をクリックします。

The screenshot shows the Cybertrust SSL Certificate Catalog interface. A red box highlights the top message bar and the 'Edit certificate' form. The message bar says 'Your configuration has been updated.' The 'Edit certificate' form shows the following details for the SSL Certificate: www.cybertrust.ne.jp. The form fields are as follows:

Certificate Name:	www.cybertrust.ne.jp
Common Name (CN):	www.cybertrust.ne.jp
Organisation (O):	Cybertrust Japan Co.,Ltd.
Organisational Unit (OU):	Technical Division
Location (L):	Minato-ku
State (S):	Tokyo
Country (C):	JP
Valid for:	1 year
Key size:	2048 bits
Notes (not public):	(empty text area)

Below the form are three buttons: 'Update Certificate', 'Copy certificate', and 'Export CSR / Sign Certificate'. The 'Export CSR / Sign Certificate' button is highlighted with a red box and the number 16. The 'Copy certificate' section asks for a short name and has 'Save As: www.cybertrust.ne.jp (c)' and 'Copy Certificate' buttons. The 'Delete certificate' section notes that the certificate is not used by any virtual servers and has 'Delete certificate' and 'Confirm' buttons.

# 1. CSRの作成

17. [Certificate Signing Request (CSR)]にCSRの内容が表示されますので、「-----BEGIN NEW CERTIFICATE REQUEST-----」から「-----END NEW CERTIFICATE REQUEST-----」の部分までを全てコピーし、テキストファイルへ貼り付けて任意の名前で保存してください。
- ※右記のCSRはサンプルです。ご申請にはご利用いただけません。

以上で、CSRの作成は完了です。

※サーバー証明書のインストールができないため、[SSL Server Certificates Catalog]に表示されている右記を削除しないよう、ご注意ください。

SSL Certificate: [www.cybertrust.ne.jp](http://www.cybertrust.ne.jp)

This form helps you to sign your certificate.

**Certificate Signing Request (CSR)**

Your Certificate Authority will use this Certificate Request text to create and issue a trusted certificate, based on this certificate.

17

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIC1zCCAb8CAQAwgZExCzAJBgNVBAYTAKpQMq4wDAYDVQQIEwVUb2t5bzESMBAG  
A1UEBxMjTWluYXRVrLw1MSIwIAYDVQQKEx1DeWJlcnRydXN0IEphcGFuIEhvLixM  
dGQuMRswGQYDVQQLExJUZWNobmljYWWgRG12aXNpb24xHTAbBgNVBAMTFHd3dy5j  
eWJlcnRydXN0Im5lLmpwMIIIBjJANBgkqhkiG9w0BAQEFAAOCAQ8AMIBcGKCAQE  
zorQ2201VG00GVD/GJemVb+fd9vvGz0Hac7J9yHkTgtdPe5z0XO33nBEKyp82A60  
uUfw1EjpYZIAkSr87prGTEmIj1Tm71OAc1PCiEYIV0wrvKobamOMRp4Rxi0rNF  
b6UII6432Cy83R5eY+ee2kyJTiQvpCwsHtSS7rljhviCc0cu9Y5e9GyLE19cqPC9  
vLM2eaH77hQN0ICgqE6F7Roea6BeQFC3RYBRb8XYb+0F1j3McibhAbx/lnRnLd7  
mX03/kakkcTMsFzaYeUNgBDUHn5Qpm+gc91kZiu8/xFnDZ/4cG0Hjs9dg/8cSQL  
xCeoQOINF2qPuKDoJKGVQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAKV1nmnA  
34xTpZ8g1PZCa12e5Tw4fcGpbYr2Jtbr/kr94KRg7xvttXctbDYKqf1v8bwOZ2Qt  
hmb802OA0cvpb9Xjb1PazwRm5H4gyZ1Fek5Yzr3QXzyF15GYbYxvjE8Yklwvkk  
yJdk+AgGfOFQBakcirSNGq+QIyaf0I2UFk0874q3Ggmqgogosjjg7ngi6m8+RNnP  
DhJQot6Jeb2jwArGMPhxkLshsCJBjmTIn8esBmVV9ttMgxD1LZvTMhs+yWHJ1Qz3
```

SSL Server Certificates Catalog

Unfold All / Fold All

Decrypting SSL Traffic: The SSL server certificates catalog contains the certificates for the SSL services you wish to decrypt.

www.cybertrust.ne.jp (www.cybertrust.ne.jp, self-signed, expires: 29 Jul 2014) Edit

Create new SSL certificate

SSL certificates are used to identify the SSL services you are running, and they are needed to decrypt SSL traffic. Self-signed certificates should be signed by a Certificate Authority before being used on publicly-accessible services.

Create Self-Signed Certificate / Certificate Signing Request

Import SSL certificate

You can import an SSL certificate (and corresponding private key) here.

Import Certificate

## 2.証明書のお申し込み

### ■証明書のお申し込みを行います。

作成した CSR をテキストエディタで開いて「-----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、WEB の申請サイト(※)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。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。

※WEBの申請サイトは以下よりご利用いただけます。

#### ▼SureBoard

<https://sstra.cybertrust.ne.jp/IRA/loginSb/>

#### ▼SureHandsOn

<https://sstra.cybertrust.ne.jp/IRA/loginSho/>

<CSRサンプル> ※お申し込みにはご利用いただけません。

-----BEGIN NEW CERTIFICATE REQUEST-----

.....

MII EhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG  
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM  
dGQuMRIwEAYDVQQLDlAUZXN0IFVuaxQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz  
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyIEST

.....

-----END NEW CERTIFICATE REQUEST-----

弊社にてお申し込み内容の審査を行い、すべてのお手続き完了後にサーバー証明書を発行いたします。(発行はメールにてお知らせいたします。)

サーバー証明書が発行されたら、次のステップへお進みください。

### 3.証明書のダウンロード

■インストールが必要となるサーバー証明書と中間CA証明書を事前にダウンロードします。

#### 【1】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事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

※サーバー証明書のダウンロードについては、以下をご参考ください。

<https://www.cybertrust.co.jp/ssl/support/download.html>

#### 【2】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、お使いの機器へ中間CA証明書のインストールが必要となります。

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、以下弊社ホーム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

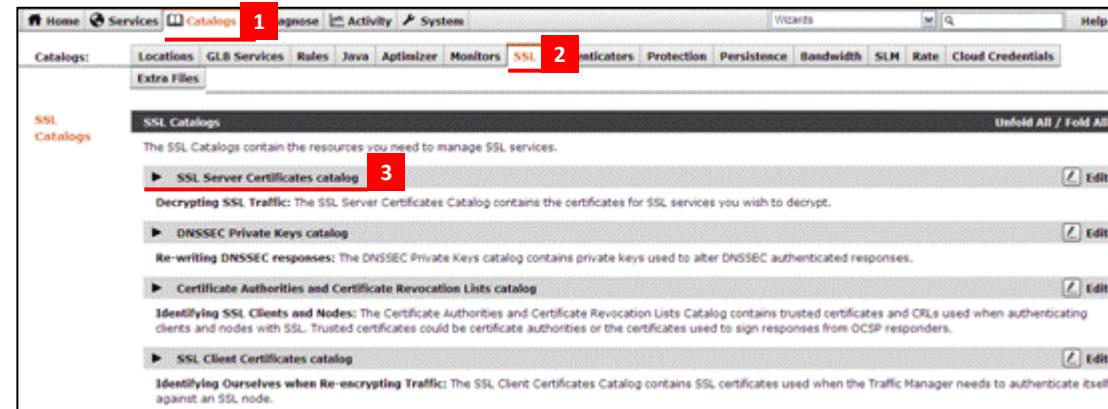
<https://www.cybertrust.ne.jp/ssl/download-ca/>

# 4.証明書のインストール

## ■サーバー証明書と中間CA証明書をインストールします

### 【1】サーバー証明書のインストール

1. Administration interface ログイン後、Home画面から[Catalogs]タブをクリックします。
2. [SSL]タブをクリックします。
3. [SSL Server Certificates Catalog]をクリックします。
4. CSR作成時に[Name]で指定した値をクリックします。



Home Services Catalogs 1 Diagnose Activity Systems Wizards Q Help

Catalogs: Locations GLB Services Rules Java Optimizer Monitors SSL 2 Authenticators Protection Persistence Bandwidth SLIM Rate Cloud Credentials Extra Files

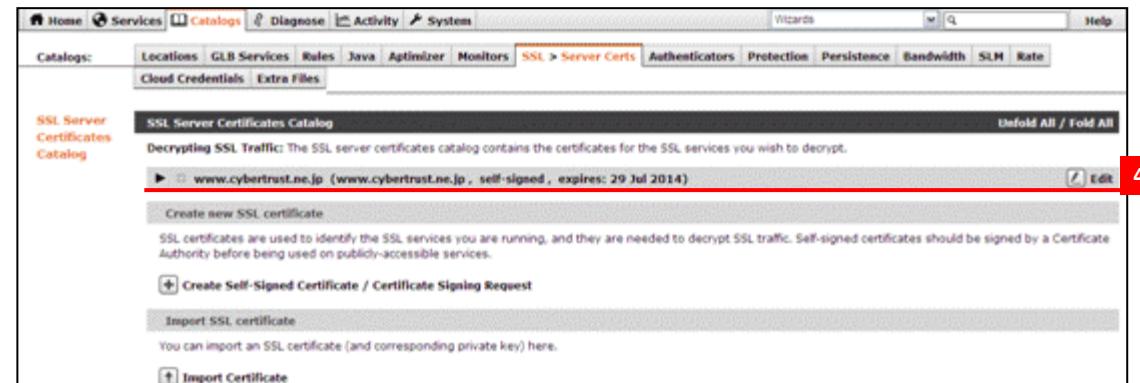
**SSL Catalogs** Unfold All / Fold All

The SSL Catalogs contain the resources you need to manage SSL services.

- SSL Server Certificates catalog 3 Edit
- DNSSEC Private Keys catalog Edit
- Certificate Authorities and Certificate Revocation Lists catalog Edit
- SSL Client Certificates catalog Edit

Identifying SSL Clients and Nodes: The Certificate Authorities and Certificate Revocation Lists Catalog contains trusted certificates and CRLs used when authenticating clients and nodes with SSL. Trusted certificates could be certificate authorities or the certificates used to sign responses from OCSP responders.

Identifying Ourselves when Re-encrypting Traffic: The SSL Client Certificates Catalog contains SSL certificates used when the Traffic Manager needs to authenticate itself against an SSL node.



Home Services Catalogs 4 Diagnose Activity Systems Wizards Q Help

Catalogs: Locations GLB Services Rules Java Optimizer Monitors SSL > Server Certs 4 Authenticators Protection Persistence Bandwidth SLIM Rate Cloud Credentials Extra Files

**SSL Server Certificates Catalog** Unfold All / Fold All

Decrypting SSL Traffic: The SSL server certificates catalog contains the certificates for the SSL services you wish to decrypt.

- www.cybertrust.ne.jp (www.cybertrust.ne.jp, self-signed, expires: 29 Jul 2014) Edit

Create new SSL certificate

SSL certificates are used to identify the SSL services you are running, and they are needed to decrypt SSL traffic. Self-signed certificates should be signed by a Certificate Authority before being used on publicly-accessible services.

+ Create Self-Signed Certificate / Certificate Signing Request

Import SSL certificate

You can import an SSL certificate (and corresponding private key) here.

+ Import Certificate

## 4. 証明書のインストール

5. 「Export CSR / Sign Certificate」をクリックします。

**SSL Certificate: www.cybertrust.ne.jp**

This form lets you edit, copy, sign or delete your SSL certificate.

Last Modified: 29 Jul 2013 10:51

**Edit certificate**

<b>Certificate Name:</b>	www.cybertrust.ne.jp
<b>Common Name (CN):</b>	www.cybertrust.ne.jp
<b>Organisation (O):</b>	Cybertrust Japan Co.,Ltd.
<b>Organisational Unit (OU):</b>	Technical Division
<b>Location (L):</b>	Minato-ku
<b>State (S):</b>	Tokyo
<b>Country (C):</b>	JP
<b>Valid for:</b>	1 year
<b>Key size:</b>	2048 bits
<b>Notes (not public):</b>	

**Update Certificate**

**Copy certificate**

Enter a short name to identify your new certificate:

**Save As:** www.cybertrust.ne.jp (c) **Copy Certificate**

**Certificate signing**

This is a self-signed certificate, so it is not suitable for a publicly-accessible service. For this purpose, you should obtain a certificate that has been signed by a trusted 'Certificate Authority'.

**Export CSR / Sign Certificate** 5

**Delete certificate**

This certificate is not used by any virtual servers.

**Delete certificate**  **Confirm**

# 4. 証明書のインストール

6. サーバー証明書をテキストエディタなどで開き、「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」まで、ハイフンを含めてすべてコピーして貼り付けます。
7. 「Update Certificate」ボタンをクリックします。

SSL Certificates Catalog

SSL Certificate: www.cybertrust.ne.jp

This form helps you to sign your certificate.

Certificate Signing Request (CSR)

Your Certificate Authority will use this Certificate Request text to create and issue a trusted certificate, based on this certificate.

```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIC1zCCAb8CAQAwgZEKczAUBgNVBAYTAkpmQMQ4wDAYDVQQIEwVUb2t5bzESMBAG  
A1UEBxMjMTW1uXXRvLw1MSIwIAYDVQQREx1DeWJlcnRydXN0IEphcGFuIENvLixM  
dGQuMRSwGQYDVQQLExJU2ZNbmljYWwgR12aXNpb24xHTAbBgNVBAMTFd3dy5j  
eWJlcnRydXN0Lm51LmpwMIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMiIBcKCAQEA  
zorQz201VG00GVd/GJsmVb+fD9vgZo0Hac7J9yHkTgtde5z0Xo33nBEKyp82A60  
uUfWs1EjpYZIAkSr87prGTEmIj1Tm7IOAqlPCiEYIV0wrwKobam0Rp4Rxic0rNf  
b6UI6432cy83R5eY+ee2kyTiQvpCwsHt887rljhwic0cu9X5e9gyLE19cqPC9  
vLMzeaH77hQNoICgqE6F7RoBa6BeQFC3RYBrb8Xvb+02Flj3McibhAbx/lnRnLd  
mX03/kaKkcTMRsFzsYeUNgBDUHn5Qpm+gc91kziu8/xFDz/4g0Hjs9dg/8ccQL  
xCeoQOINf2qPuKDoJKGVIDAQABoAwDQYJKoZIhvCNQEFBQADgEBAKVlmmnA  
34xTpZ8g1PZCaI2e5Tw4fcGpbYr2Jtbr/kr94KRg7xvttXctbDYKqf1vSbw02Qt  
hm8S020A0cvpk9Xkzb1pazwRn5H4gYzFek5Xzr3QX2yF15gYbYXwjkB8YR1lwkk  
yJdk+Ag6fOFQBakc1rsNGg+0Iyaf0I2UFk0874q3Ggm8qgogsjg7ng16m+RwNfJ  
DQot6Jeb2jwArGMPHxkLhsCJBjmTyneesBmVv9ttMgx01LzvTMnS+yWHJiQz3
```

Replace certificate

Once you have received a new certificate, paste it here to replace your current certificate.

```
-----BEGIN CERTIFICATE-----  
MIIGJDCCBQygAwIBAgIU2caC2h8eVJP6n0288bD4PhdbVYkwDQYJKoZIhvCNQEF  
BQAwMjELMAkGA1UEBhMCS1axIzAhcgvNBVAcT5knM5YnVydHJlc3QgSmFwYh4gQ28u  
LCBMDGQuMSIwIAYDVQDEx1DeWJlcnRydXN0IEphcGFuIENBIEcyMB4XDTEz  
MDc0yTA3MjgxM1oXDETEzMDgyOTEUN0NMFowgejgxEzARBgzBqEAYIzPAIBaRMC  
SIAXrzAVBqGNVBAUTDjAxMDQ1MDETMDY1MDExMRswGQYDVQPFExJWMS4wLCBDbGF1  
c2UgNS4oYikxKzAJBgNVBAYTAkpmQRIwEAYDVQQIDAnmnbHkuqzpg70xDzAnBgNV  
BACMbu4rWMujeTMcsGA1UECwgk44K144Kk44Qc44084401440p44K544o15qCq  
5byPSly456s+MRswGQYDVQQLExJU2ZNbmljYWwgR12aXNpb24xHTAbBgNVBAMT  
FHd3dy5jewWJ1lcnRydXN0Lm51LmpwMIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMiIB  
CgKCAQEazorQz201VG00GVd/GJsmVb+fD9vgZo0Hac7J9yHkTgtde5z0Xo33nBE  
Kyp82A60uEjpeYzIAkSr87prGTEmIj1Tm7IOAqlPCiEYIV0wrwKobam0Rp4  
Rxic0rNf6UI6432cy83R5eY+ee2kyTiQvpCwsHt887rljhwic0cu9X5e9gyLE19  
cqPC9vLMzeaH77hQNoICgqE6F7RoBa6BeQFC3RYBrb8Xvb+02Flj3McibhAbx  
/lnRnLd7mX03/kaKkcTMRsFzsYeUNgBDUHn5Qpm+gc91kziu8/xFDz/4g0Hjs9  
dg/8ccQlxCeoQOINf2qPuKDoJKGVIDAQABo4ICVTCALewCQYDVRO7BAIwADCB  
ugYDVR0gBIGyMIGvMIGsBgorBqEEAbE+ANQBMIGdMFcGCCsGAQFBwICMEsa8U2v  
ciBtb3J1IGRldGfpbHms1HbsZWFzZB2aXNpdcBvdXigd2vici2102SSBdHrwzov  
L3d3dy5jewWJ1lcnRydXN0Lm51LmpwIc4wQgYIKwYBQUHagEWNh0dHBo18vd3d3  
LmN5imVydHJ1c3QubmUuanAvc3Nsl3J1cG9zaXrvenkvaW5kZXguaeHrbDCBpQYI  
KwYBBQUHAAQEEg2gwg2UwPgYIKwYBBQUHMGGMm0diHA6Ly9zdXJ1c2VyaWwzLW9j  
c3AuY3liZXJ0cnVzdC5u285qcC9PY3NwU2VydMvYMFMGCCsGAQFBzAChkdodHRw  
oi8ve3VvY2XN1cm1ly1jcmwuY31izXJ0cnVzdC5u285qcC9TdXJ1U2VydMvYzIw
```

Update Certificate 7

# 4.証明書のインストール

8

- 「Your configuration has been updated.」と表示され、設定したサーバー証明書の内容が表示されます。

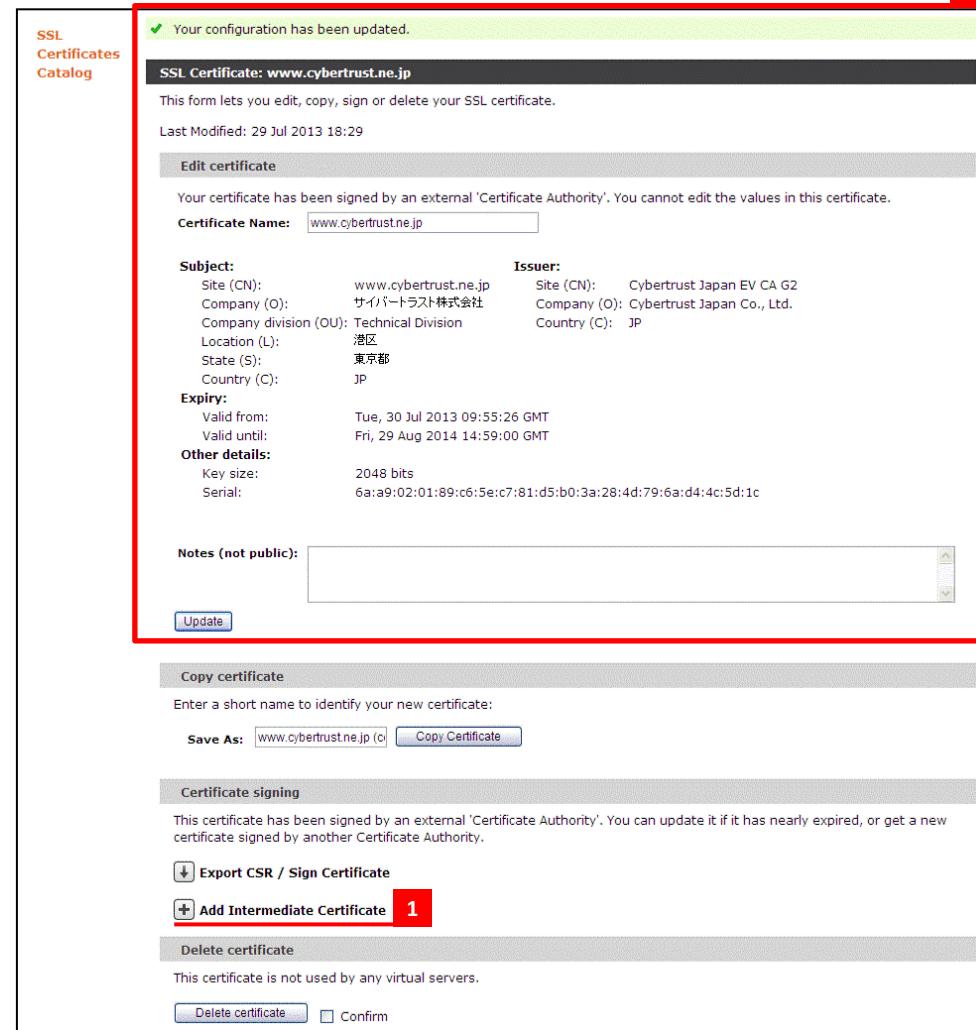
以上でサーバー証明書のインストールは完了です。

続いて、中間CA証明書のインストールを行います。

## 【2】中間CA証明書のインストール

※必要な中間CA証明書をすでにインストール済みの場合は、設定不要です。

- 「Add Intermediate Certificate」をクリックします。



The screenshot shows the 'SSL Certificates Catalog' interface. At the top, a green bar indicates 'Your configuration has been updated.' Below this, the 'SSL Certificate: www.cybertrust.ne.jp' is displayed. The certificate details are as follows:

<b>Subject:</b>	Site (CN): www.cybertrust.ne.jp	Site (CN): Cybertrust Japan EV CA G2
Company (O):	サイバートラスト株式会社	Company (O): Cybertrust Japan Co., Ltd.
Company division (OU):	Technical Division	Country (C): JP
Location (L):	港区	
State (S):	東京都	
Country (C):	JP	

**Expiry:**  
Valid from: Tue, 30 Jul 2013 09:55:26 GMT  
Valid until: Fri, 29 Aug 2014 14:59:00 GMT

**Other details:**  
Key size: 2048 bits  
Serial: 6a:a9:02:01:89:c6:5e:c7:81:d5:b0:3a:28:4d:79:6a:d4:4c:5d:1c

**Notes (not public):** [Text area]

**Update** button

**Copy certificate**  
Enter a short name to identify your new certificate:  
Save As: www.cybertrust.ne.jp (c)

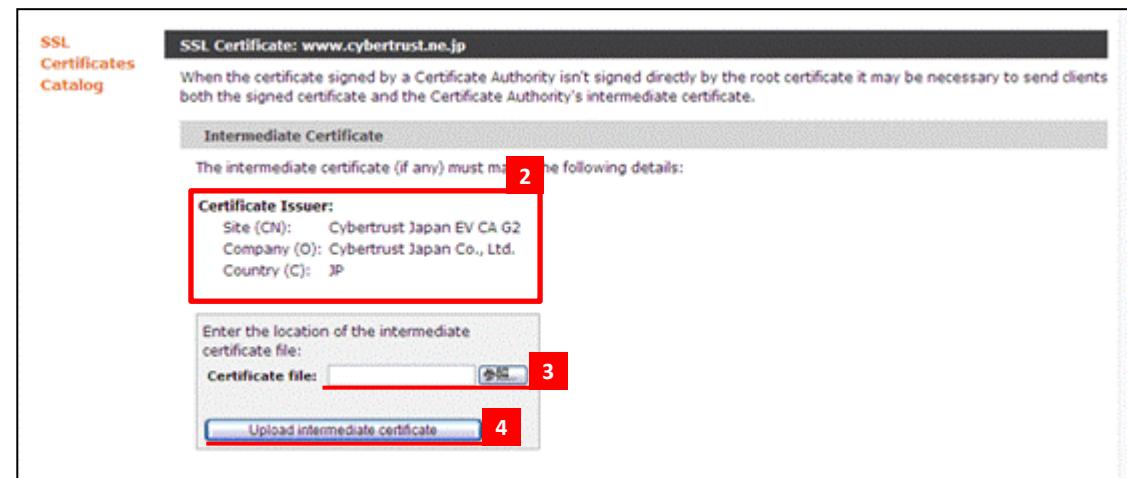
**Certificate signing**  
This certificate has been signed by an external 'Certificate Authority'. You can update it if it has nearly expired, or get a new certificate signed by another Certificate Authority.

1 1  
  Confirm

This certificate is not used by any virtual servers.

# 4.証明書のインストール

- [Certificate Issuer:]としてインストールが必要な中間CA証明書の情報が表示されますので、事前にダウンロードした中間CA証明書と一致していることを確認します。
- 「参照」ボタンをクリックして、設定する中間CA証明書を指定します。
- 「Upload Intermediate certificate」をクリックします。



# 4.証明書のインストール

5. 「Your configuration has been updated.」と表示されます。
6. [Intermediate Certificate 1 Issuer:]として、インストールした中間CA証明書の情報が表示されます。

以上で中間CA証明書のインストールは完了です。

## 【！】クロスルート方式をご設定の場合

クロスルート方式をご設定の場合は、『【2】中間CA証明書のインストール』- 1~6の手順を繰り返し行い、クロスルート用中間CA証明書をインストールします。

### ▼クロスルート方式の対象商品

2025年6月1日現在、対象商品はありません

The screenshot shows the SSL Certificates Catalog interface. At the top, a green bar indicates 'Your configuration has been updated.' (5). Below it, the 'SSL Certificate: www.cybertrust.ne.jp' section shows the certificate details for 'www.cybertrust.ne.jp'. The 'Subject' section lists the site as 'www.cybertrust.ne.jp' and the company as 'サイバートラスト株式会社'. The 'Issuer' section shows the certificate is signed by 'Cybertrust Japan EV CA G2' (6). The 'Expiry' section shows the certificate is valid from Tuesday, July 30, 2013, 09:55:26 GMT to Friday, August 29, 2014, 14:59:00 GMT. The 'Other details' section shows a key size of 2048 bits and a serial number of 6a:9:02:01:89:c6:5e:c7:81:d5:b0:3a:28:4d:79:6a:d4:4c:5d:1c. A red box highlights the 'Intermediate Certificate' section, which lists 'Cybertrust Japan EV CA G2' as the issuer. The 'Notes (not public)' section is empty. Below it are buttons for 'Update' and 'Copy certificate'. The 'Save As' field is set to 'www.cybertrust.ne.jp (c)' with the 'Copy Certificate' button. The 'Certificate signing' section indicates the certificate is signed by an external authority and can be updated or renewed. The 'Delete certificate' section shows the certificate is not used by any virtual servers and includes 'Delete certificate' and 'Confirm' buttons.

# 5.証明書インストール後の設定(例)

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

## 【1】Virtual Serverの設定

1. Administration interface ヘログイン後、Home画面から[Services]タブをクリックします。
2. [Virtual Servers]タブをクリックします。
3. 設定を行う仮想サーバーの名称をクリックします。

The screenshot shows the Cybertrust Administration interface. The top navigation bar has tabs: Home, Services (highlighted in red), Catalogs, Diagnose, Activity, System, Wizards, and Help. Below the navigation bar, the 'Configuring' dropdown is set to 'Virtual Servers'. The main content area has a left sidebar labeled 'Virtual Servers' and a right panel titled 'Virtual Servers'. The right panel contains a brief description: 'A virtual server accepts network traffic and processes it. It normally gives each connection to a pool; the pool then forwards the traffic to a server node.' Below the description is a list with one item: '▶ ✓ test (HTTP, port 80)' (highlighted with a red box and number 3). At the bottom of the right panel is a 'Create a new Virtual Server' form with fields: 'Virtual Server Name:' (input field), 'Protocol:' (dropdown set to 'HTTP'), 'Port:' (input field '80'), and 'Default Traffic Pool:' (dropdown set to 'testx2048.cybertrust.ne.jp'). A 'Create Virtual Server' button is at the bottom of the form.

# 5.証明書インストール後の設定(例)

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

4. [SSL Decryption]をクリックします。

※以下の設定になっていることを確認してください。

[Enabled]: Yes

[Internal protocols]: HTTP (Internal のプロトコルを指定)

[Port]: 443

[Default Traffic Pool]: 使用したいPoolを選択

Virtual Server: test (HTTP, port 80)

Pools used by this virtual server:

discard Default

Last Modified: 25 Jul 2013 15:54

**Basic Settings**

The basic settings specify the internal virtual server protocol that is used for traffic inspection, the port and IP addresses the virtual server listens on along with the default pool for handling traffic.

Name: test

Enabled:  Yes  No

Internal Protocol:

Port: 443

Default Traffic Pool: test

Listening on:  All IP addresses  Traffic IP Groups ...  Domain names and IP addresses ...

Notes:

Update View traffic on World Map

**Rules** Edit

TrafficScript rules provide sophisticated traffic management functionality.

**SSL Decryption** Edit

SSL decryption can decrypt SSL connections before processing.

**Classes** Edit

Classes modify the operation of this virtual server. You can apply Service Protection, Bandwidth Management or Service Level Monitoring classes.

# 5.証明書インストール後の設定(例)

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

5. [ssl decrypt:] を「Yes」に変更します。
6. [Default Certificate:]に使用するサーバー証明書を選択します。
7. 「Update」ボタンをクリックします。

Virtual Server: test (HTTP, port 80)  
SSL Decryption  
Virtual server can decrypt and authenticate SSL connections. This offloads SSL processing from your nodes, and allows the virtual server to inspect and process the connection.

**SSL Decryption**

These settings control how SSL connections are decrypted.

Whether or not the virtual server should decrypt incoming SSL traffic.  
ssl\_decrypt:  Yes  No **5**

Which SSL certificate(s) should this virtual server use?  
Additional certificates can be supplied to match different sites hosted by this virtual server. You can specify a different certificate for any hostname or IP address. The wildcard character '\*' can be used to match multiple hostnames. If none of the addresses or hostnames match the default certificate will be used.

Note: Hostname mappings require support of the TLS 1.0 'Server Name' extension, which is not supported by all browsers.

certificate: Default Certificate: www.cybertrust.ne.jp (www.cybertrust.ne.jp, Expires 29 Aug 2014) **6**

Add certificate mapping:  
IP Address / Host Name:   
Certificate:

**Manage SSL Certificates**

Whether or not the virtual server should add HTTP headers to each request to show the SSL connection parameters.

ssl\_headers:  Yes  No

If the traffic manager is receiving traffic sent from another traffic manager, then enabling this option will allow it to decode extra information on the true origin of the SSL connection. This information is supplied by the first traffic manager.

ssl\_trust\_magic:  Yes  No

Whether or not to send an SSL/TLS "close alert" when the traffic manager is initiating an SSL socket disconnection.

ssl\_send\_close\_alerts:  Yes  No

Whether or not to prefer SSLv3 over TLS when the client appears to support both. SSLv3 is slightly faster, but some clients don't allow SSLv3 but still send the ClientHello inside SSLv2 or SSLv3 records. The default option is to prefer TLS due to known vulnerabilities in the way block ciphers are used before TLSv1.1.

ssl\_prefer\_sslv3:  Yes  No

**SSL Client Authentication**

These settings control how clients are authenticated in SSL transactions.

**SSL Client Certificate OCSP Checking**

These settings control how the traffic manager checks the revocation of client certificates using OCSP.

Apply Changes  
**Update** **7**

# 5.証明書インストール後の設定(例)

※本項は、「Virtual server」と「Pool」が作成済みであることを前提としています。

9. 「Your configuration has been updated.」と表示されます。
10. [SSL Decryption]に有効状態を示す緑色のチェックがつきます。

SSL Decryption

Your configuration has been updated. 9

Virtual Server: test (HTTP, port 80, SSL-decrypt)

Unfold All / Fold All

SSL Decryption 10

These settings control how SSL connections are decrypted.

Whether or not the virtual server should decrypt incoming SSL traffic.

ssl\_decrypt:  Yes  No

Which SSL certificate(s) should this virtual server use?

Additional certificates can be supplied to match different sites hosted by this virtual server. You can specify a different certificate for any hostname or IP address. The wildcard character '\*' can be used to match multiple hostnames. If none of the addresses or hostnames match the default certificate will be used.

Note: Hostname mappings require support of the TLS 1.0 'Server Name' extension, which is not supported by all browsers.

certificate: Default Certificate: www.cybertrust.ne.jp (www.cybertrust.ne.jp, Expires 29 Aug 2014)

IP Address / Host Name	Certificate	Remove
210.189.211.57	www.cybertrust.ne.jp (www.cybertrust.ne.jp, Expires 29 Aug 2014)	<input type="checkbox"/>

Add certificate mapping:

IP Address / Host Name:   
Certificate:

以上で設定完了です。

サーバー証明書とマッピングしたIPアドレス、またはホスト名にhttps(443)のアクセスがあった場合、設定したサーバー証明書を利用した暗号化通信が行われます。

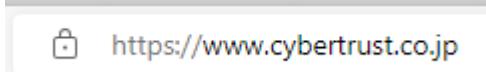
# 6. SSL通信の確認

サーバー証明書が正しく設定され、エラーやセキュリティ警告が表示されず、正常にSSL通信が可能であることを確認します。

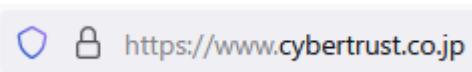
- SSL通信の確認は設定を行っているサーバー以外のWEBブラウザやスマートフォンなどの携帯端末、弊社「SSLサーバ証明書 導入サポートツール」のサーバ証明書の設定確認から行うことを推奨します。

## ■ 設定確認例

<Edge>



<Firefox>



<Chrome>



※接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL通信時のセキュリティ警告やエラーについて」をご参照ください。

<https://www.cybertrust.co.jp/ssl/support/faq/>