

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ます、「Stingray Traffic Manager」の動作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。
4. 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。
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 |

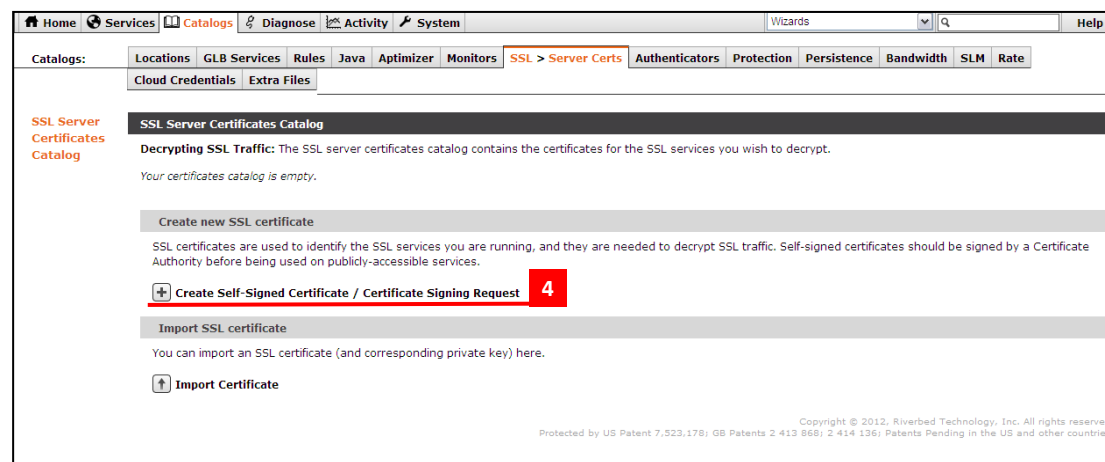
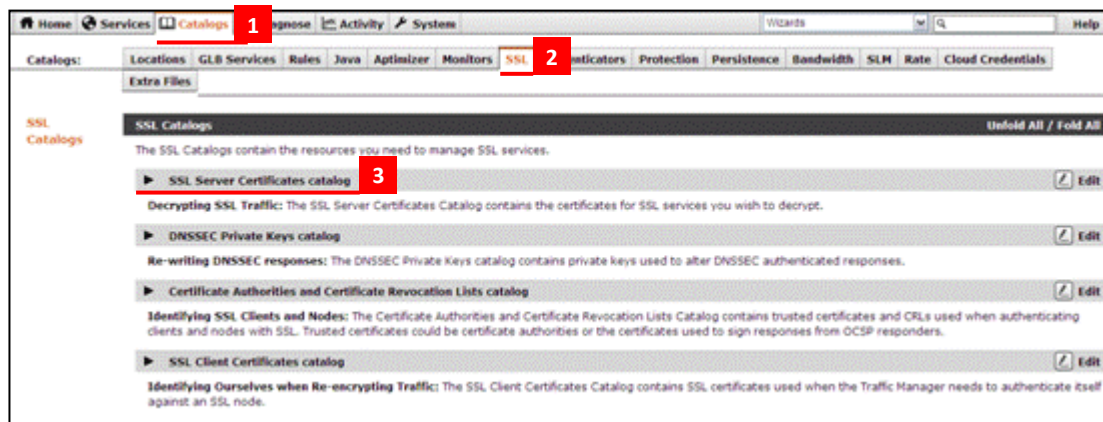
1. CSRの作成

■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 へログイン後、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。



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

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

Organisation (O): 7

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

Organisational Unit (OU): 8 tional)

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

Location (L): 9

Your state or province, such as 'Somestate':

State (S): (required for US only)

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

Country (C):

How long should this certificate be valid for:

Expires in: ▼

Private key size (1024 bits recommended):

Key size: ▼

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。

SSL Certificates Catalog

✓ Your configuration has been updated.

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

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):

Update Certificate

Copy certificate

Enter a short name to identify your new certificate:

Save As: www.cybertrust.ne.jp 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 16

Delete certificate

This certificate is not used by any virtual servers.

Delete certificate Confirm

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くなるため、[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

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-----
MIIC1zCCAB8CAQAwZExxOzA1UEBxMjUyYXRvLWt1MSIwIAAYDQYKKExlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRswGQYDVQQLExJUZWNobmljYWwgRG12aXNpb24xHTABBgNVBAMTFHd3dy5j
eWJlcnRydXN0Lm5lLmpwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
zorQZ201VG00GVD/GJsmVb+fd9vvGz0HaC7J9yHkTgtdPe5z0X033nBEKyps2A6O
uUfWslEjpYZIAKsr87prGTEmIj1Tm7IOAQ1PCiEYIV0wrvKobam0MRp4Rxic0rNF
b6UII6432Cy83R5eY+ee2kyJTiQvpCwsHtSS7rljhviCc0cu9Y5e9GyLE19cqPC9
vLMZeaH77hQNoICggE6F7RoEa6BeQFC3RYBRb8XYb+02Flj3McibhAbx/lnRnLd7
mX03/kakkcTMKsFzsYeUNGBDUhn5Qpm+gc91kZiu8/xFnDZ/4oG0HJs9dg/ScCQL
xCeooQOINF2qPuKDoJKGVQIDAQABoAAwDQYJKoZIhvcNAQEFBQDggEBAKVlnmNA
34xTpZ8glPZCaI2e5Tw4fcGpbYr2Jtbr/kr94KRg7xvttXCtbDYKqf1v8bwOZ2Qt
hmBS02OA0cvpb9Xjb1PazwRm5HJ4gyZIFek5Yzr3QXZyF15GYbYxvje8YK1wvkkx
yJdk+AgGfOFQBakclrSNGq+QIyafoIZUFk0874q3Ggm8qgogsjg7ngi6m8+RWnPJ
DhJQOt6Jeb2jwArGMPPhxkLshsCJBjmTYnesBmVV9ttMgxDDLZvTMns+yWHJiQz3
-----END NEW CERTIFICATE REQUEST-----
```

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-----  
.....  
MIIEhDCCA2wCAQAwYkxCzAJBgNVBAYTAkpQM4wDAYDVQQIDAVUb2t5bzESMBAG  
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBIDeWJlcnRydXN0IEphcGFuIEVnLixM  
dGQuMRlwEAYDVQQQLDAIUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz  
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyIIEST  
.....  
-----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ましたら、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

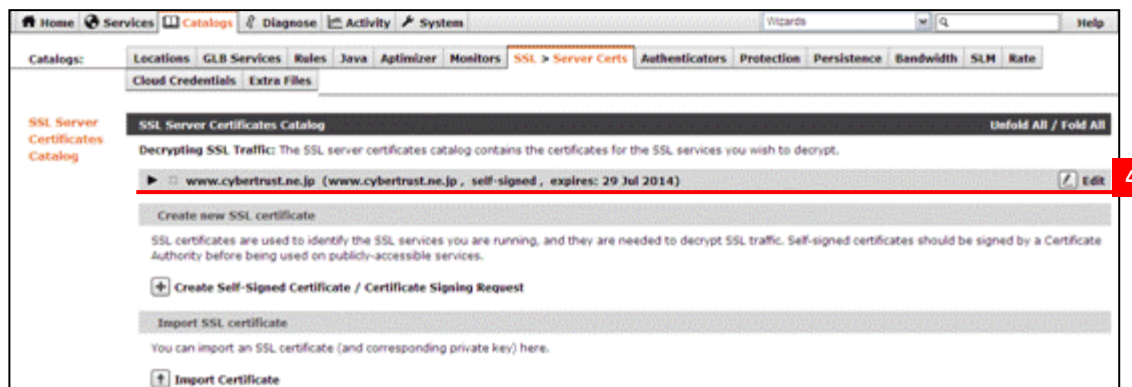
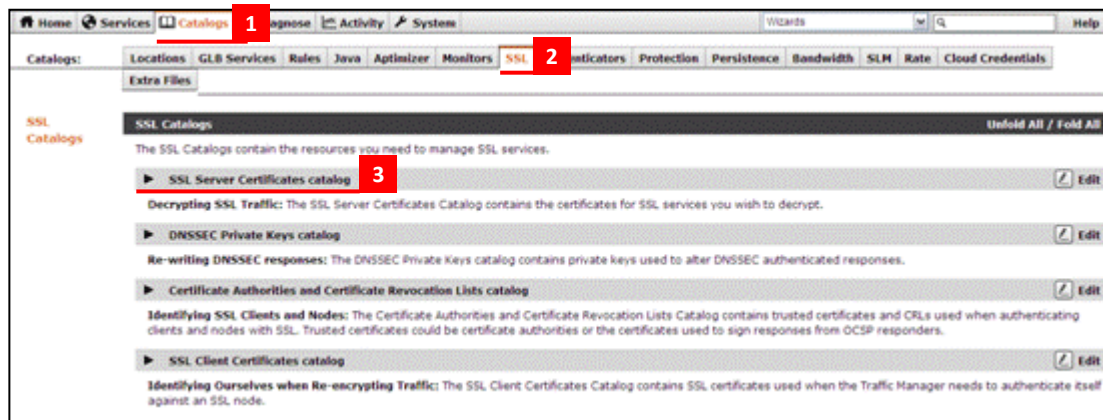
<https://www.cybertrust.ne.jp/ssl/download-ca/>

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 へログイン後、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。



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 Certificates Catalog

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

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):

Update Certificate

Copy certificate

Enter a short name to identify your new certificate:

Save As: www.cybertrust.ne.jp (or) 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。

[illegible]

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。

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

8

SSL Certificates Catalog

✓ Your configuration has been updated.

SSL Certificate: www.cybertrust.ne.jp

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

Last Modified: 29 Jul 2013 18:29

Edit certificate

Your certificate has been signed by an external 'Certificate Authority'. You cannot edit the values in this certificate.

Certificate Name:

Subject:		Issuer:	
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):

Copy certificate

Enter a short name to identify your new certificate:

Save As:

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

Delete certificate

This certificate is not used by any virtual servers.

☐ Confirm

4. 証明書のインストール

2. [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。
3. 「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。
4. 「Upload Intermediate certificate」をクリックします。

The screenshot shows the 'SSL Certificates Catalog' interface. At the top, it says 'SSL Certificate: www.cybertrust.ne.jp'. Below this, a note explains that if a certificate isn't signed directly by the root, the intermediate certificate must be sent. The 'Intermediate Certificate' section contains a table for 'Certificate Issuer' information, which is highlighted with a red box and a '2' in a red square. The table lists: Site (CN): Cybertrust Japan EV CA G2, Company (O): Cybertrust Japan Co., Ltd., and Country (C): JP. Below the table, there is a section to 'Enter the location of the intermediate certificate file:' with a 'Certificate file:' input field and a '参照' (Reference) button, highlighted with a red box and a '3' in a red square. At the bottom, there is a blue button labeled 'Upload intermediate certificate', highlighted with a red box and a '4' in a red square.

SSL Certificates Catalog

SSL Certificate: www.cybertrust.ne.jp

When the certificate signed by a Certificate Authority isn't signed directly by the root certificate it may be necessary to send clients both the signed certificate and the Certificate Authority's intermediate certificate.

Intermediate Certificate

The intermediate certificate (if any) must match the following details:

2

Certificate Issuer:	
Site (CN):	Cybertrust Japan EV CA G2
Company (O):	Cybertrust Japan Co., Ltd.
Country (C):	JP

Enter the location of the intermediate certificate file:

Certificate file: 参照 3

Upload intermediate certificate 4

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、対象商品はありせん

The screenshot displays the 'SSL Certificates Catalog' interface. At the top, a green banner indicates 'Your configuration has been updated.' with a red '5' in a box. Below this, the 'SSL Certificate: www.cybertrust.ne.jp' is shown. The interface includes sections for 'Edit certificate', 'Expiry', 'Other details', 'Intermediate Certificate', 'Notes (not public)', 'Copy certificate', 'Certificate signing', and 'Delete certificate'. The 'Intermediate Certificate' section is highlighted with a red box and a red '6' in a box, showing details for the 'Cybertrust Japan EV CA G2' issuer.

SSL Certificates Catalog

✓ Your configuration has been updated. 5

SSL Certificate: www.cybertrust.ne.jp

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

Last Modified: 29 Jul 2013 18:51

Edit certificate

Your certificate has been signed by an external 'Certificate Authority'. You cannot edit the values in this certificate.

Certificate Name: www.cybertrust.ne.jp

Subject:

Site (CN):	www.cybertrust.ne.jp	Issuer:	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

Intermediate Certificate:

Site (CN):	Cybertrust Japan EV CA G2	Issuer:	Site (CN): Cybertrust Global Root
Company (O):	Cybertrust Japan Co., Ltd.	Company (O):	Cybertrust, Inc
Country (C):	JP		

Notes (not public):

Copy certificate

Enter a short name to identify your new certificate:

Save As: www.cybertrust.ne.jp

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.

Delete certificate

This certificate is not used by any virtual servers.

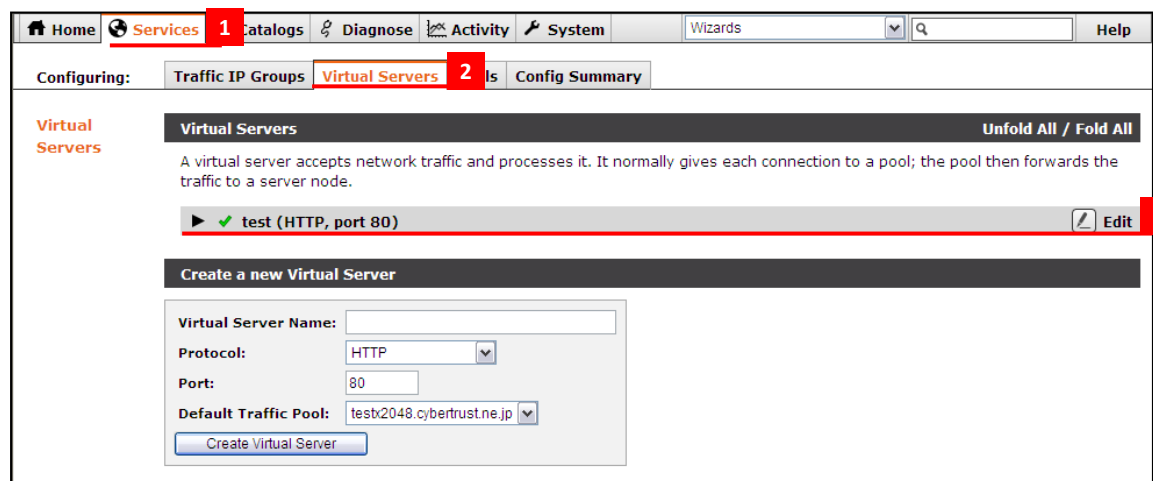
☐ Confirm

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 へログイン後、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。



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 Servers

Virtual Server: test (HTTP, port 80) Unfold All / Fold All

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: HTTP

Port: 443

Default Traffic Pool: test

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

Notes:

► **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。

SSL
Decryption

Virtual Server: test (HTTP, port 80) Unfold All / Fold All

Your 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

Your 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 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
210.169.211.57	www.cybertrust.ne.jp (www.cybertrust.ne.jp, Expires 29 Aug 2014) ▼	<input type="checkbox"/>

Add certificate mapping:

IP Address / Host Name:

Certificate:

Manage SSL Certificates

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。

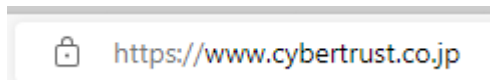
6.SSL通信の確認

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。

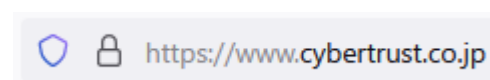
- SSL通信の確認は設定を行っているサーバー以外のWEBブラウザやスマートフォンなどの携帯端末、弊社「SSLサーバ証明書 導入サポートツール」の[サーバ証明書の設定確認](#)から行うことを推奨します。

■設定確認例

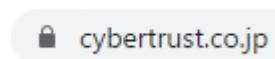
<Edge>



<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/>