Microsoft Azure Cloud Services
CSR作成/証明書インストール手順書

サイバートラスト株式会社

2025年6月1日

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、「Microsoft Azure Cloud Services」の利用時にCSRの作成、および、サイバートラストのSSLサーバー証明書をインストールする手順について解説するドキュメントです。本手順は、「Windows 7」「IIS7.0」「Visual Studio Express 2015 RC for Web」の環境下で2015年6月に動作確認をしております。
2. 「Microsoft Azure Cloud Services」 のサービスお申し込みや、設定がすでに完了しており、単独での動作確認ができている事を前提としております。実際の手順はお客様の環境により異なる場合があり、「Microsoft Azure Cloud Services」サービス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。
3. 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、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。
4. 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。

cybertrust

目次

1. ご利用の前に

サイバートラストのSSLサーバー証明書を「Microsoft Azure Cloud Services（以下、クラウドサービス）」でご利用の場合、
以下の点にご注意ください。

- 「クラウドサービス」で利用する「***. cloudapp.net」は、Microsoft 社が管理しているドメインのため、SSLサーバー証明書を取得できません。そのため、CSR作成前にお客様独自のドメインを事前に取得してください。
- FQDNと「***.cloudapp.net」を関連付けるため、DNSサーバーに「CNAME」の設定が必要です。実際に接続を行うURLは「CNAME」に登録されたFQDNです。

例）別名として「www.cybertrust.ne.jp」を登録した場合
エンドユーザーが接続する際のURL：www.cybertrust.ne.jp
↓DNS
接続先：https:// ***.cloudapp.net/
↓DNS
紐付いているIPアドレス

2. CSR作成

CSRは「Microsoft Azure」の管理ポータルサイトではなく、お客様のローカル環境で作成します。

※「IIS」を利用したCSRの作成は以下の手順書の「CSR作成」の項目をご覧ください。

▼Microsoft IIS7.0/7.5 CSR作成/証明書インストール手順書（新規・更新用）
https://www.cybertrust.co.jp/ssl/support/files/iis7.pdf

▼Microsoft IIS8.0/8.5 CSR作成/証明書インストール手順書（新規・更新用）
https://www.cybertrust.co.jp/ssl/support/files/iis8.pdf

▼Microsoft IIS10.0 CSR作成/証明書インストール手順書（新規・更新用）
https://www.cybertrust.co.jp/ssl/support/technical/iis10.html

3. 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＞

```
-----BEGIN CERTIFICATE REQUEST-----
.....
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyllEST
.....
-----END  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。

4. 証明書のダウンロード

証明書が発行されましたら、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。

- 中間CA証明書のダウンロード
  - 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サイト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/
  - 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？
    https://www.cybertrust.co.jp/ssl/support/faq/tmxwjqz2p3bq.html

4. 証明書のダウンロード

- 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。
▼SSLサーバー証明書のダウンロード
https://www.cybertrust.co.jp/ssl/support/download.html

5. 証明書のインストール

CSRを作成したローカル環境へ中間CA証明書とSSLサーバー証明書をインストールします。

※「IIS」への証明書インストールは以下の手順書の「証明書のインストール」の項目をご覧ください。

▼Microsoft IIS7.0/7.5 CSR作成/証明書インストール手順書（新規・更新用）
https://www.cybertrust.co.jp/ssl/support/files/iis7.pdf

▼Microsoft IIS8.0/8.5 CSR作成/証明書インストール手順書（新規・更新用）
https://www.cybertrust.co.jp/ssl/support/files/iis8.pdf

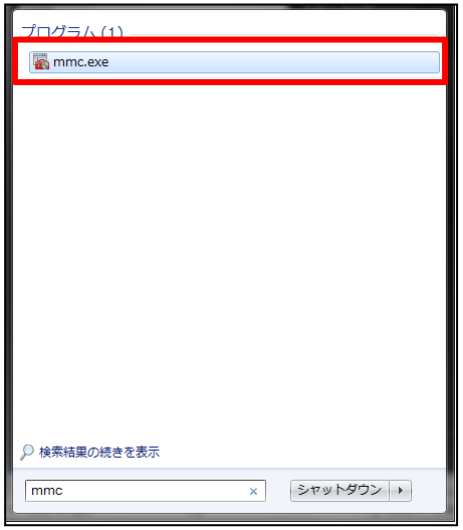
▼Microsoft IIS10.0 CSR作成/証明書インストール手順書（新規・更新用）
https://www.cybertrust.co.jp/ssl/support/technical/iis10.html

6. pfxファイルの作成

インストールした中間CA証明書、サーバー証明書と秘密鍵ファイルを1つのpfxファイルとして、エクスポートします。

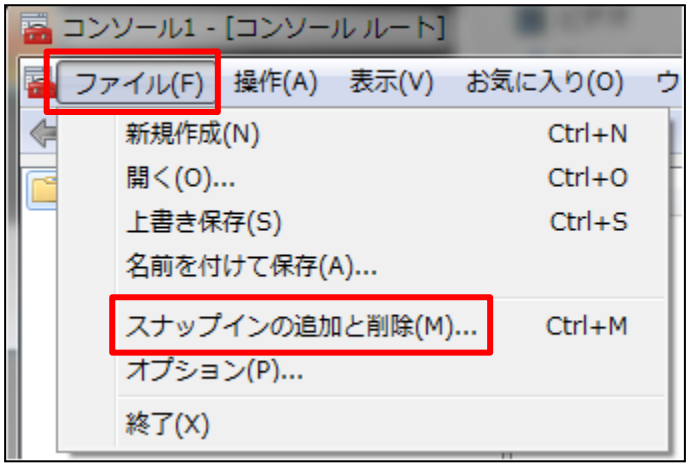
1. 【スタート】ボタンをクリックし、【プログラムとファイルの検索】のテキストボックスに「mmc」と入力します。

2. 検索結果として表示される【mmc.exe】をクリックし、「Microsoft 管理コンソール」を起動します。

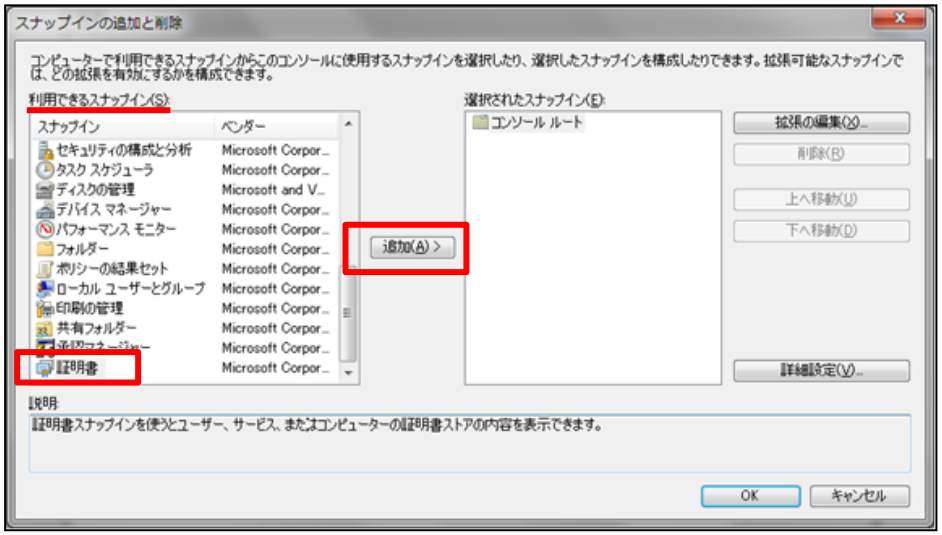


6. pfxファイルの作成

3. MMC起動後、画面上部のメニューの【ファイル】より、【スナップインの追加と削除】をクリックします。



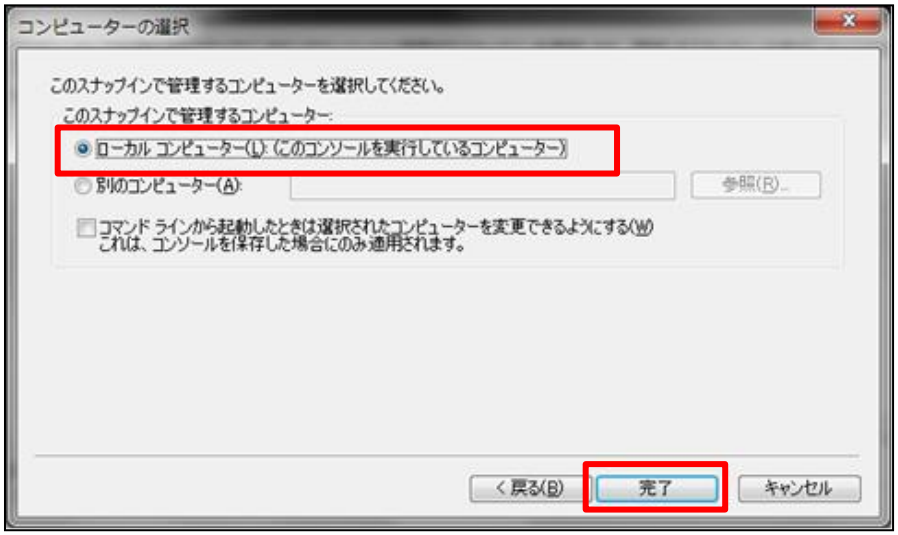
4. 【利用できるスナップイン】の【証明書】を選択し、【追加】をクリックします。



6. pfxファイルの作成

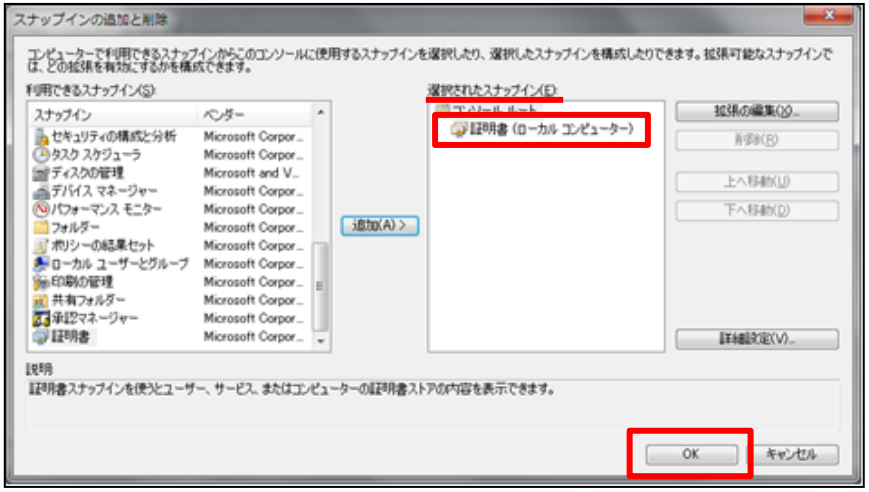
5. 【コンピューターアカウント】を選択し、【次へ】をクリックします。

6. 【ローカルコンピューター】を選択し、【完了】をクリックします。

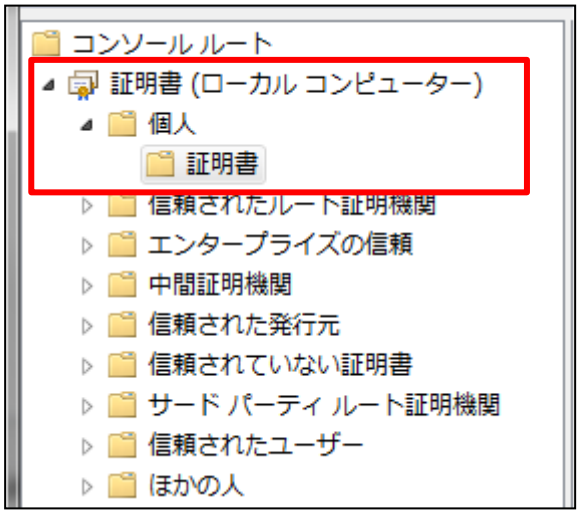


6. pfxファイルの作成

7. 【選択されたスナップイン】に【証明書（ローカルコンピューター）】が追加されたことを確認し、【OK】をクリックします。

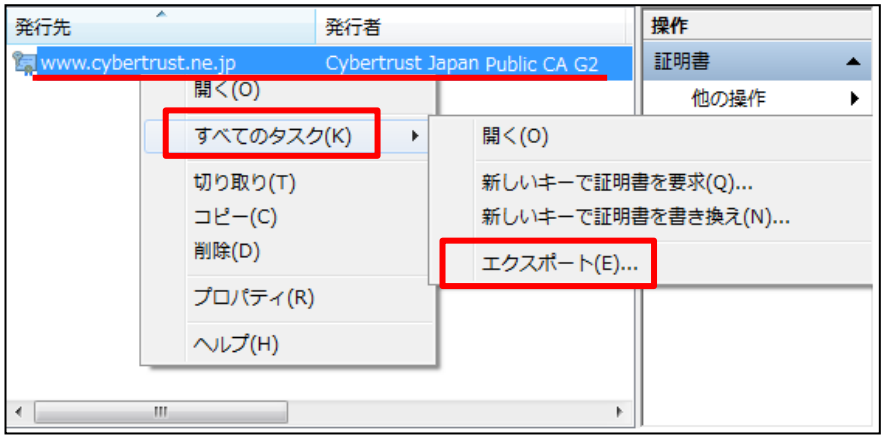


8. 【証明書（ローカルコンピューター）】→【個人】→【証明書】の順にクリックします。

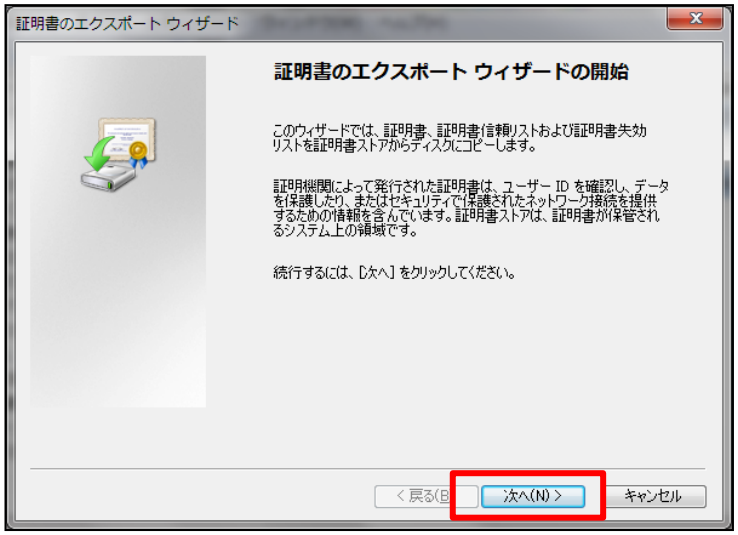


6. pfxファイルの作成

9. MMCの画面中央に表示されるインストールしたサーバー証明書を右クリックし、【すべてのタスク】へマウスカーソルを合わせ、表示された【エクスポート】をクリックします。

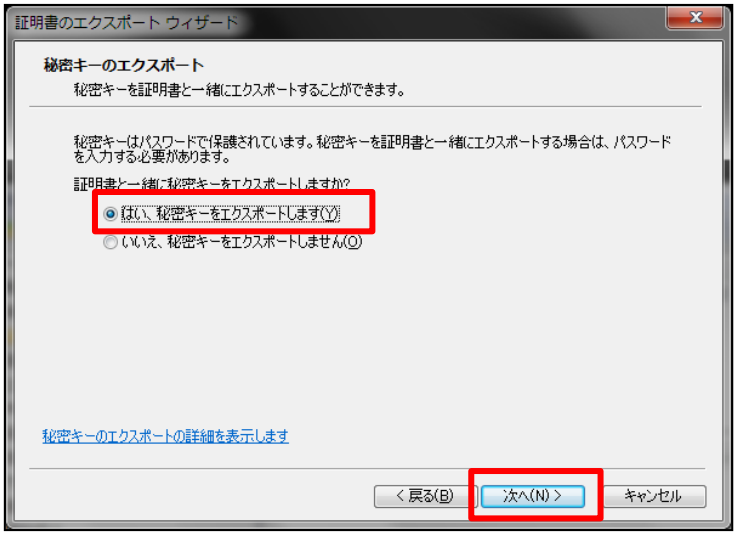


10. 【証明書のエクスポートウィザード】が起動しましたら、【次へ】をクリックします。

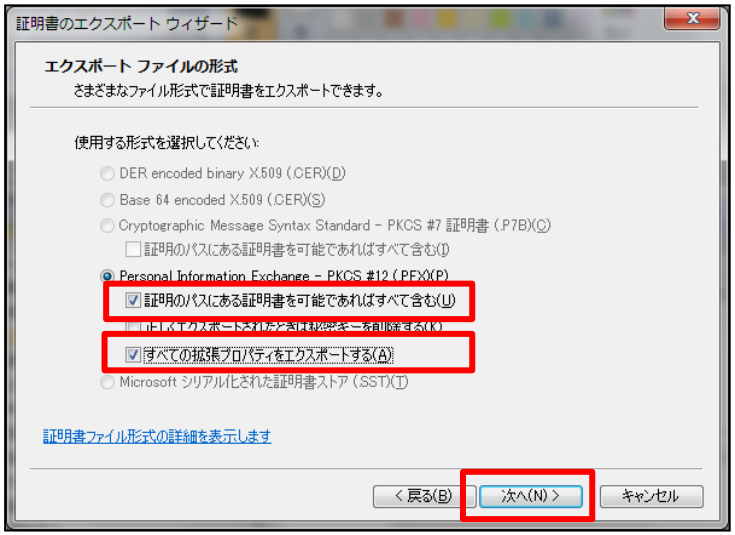


6. pfxファイルの作成

11. 【はい、秘密キーをエクスポートします】を選択し、【次へ】をクリックします。



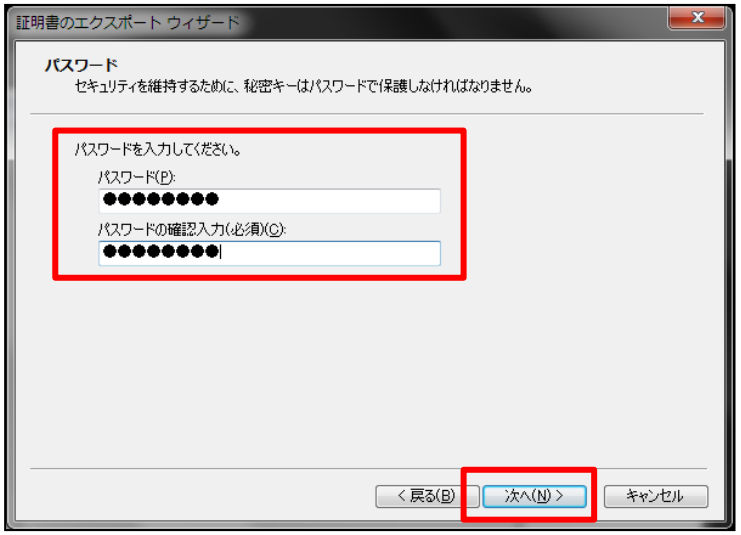
12. 【証明書のパスにある証明書を可能であればすべて含む】と【すべての拡張プロパティをエクスポートする】のチェックボックスにチェックを入れ、【次へ】をクリックします。



6. pfxファイルの作成

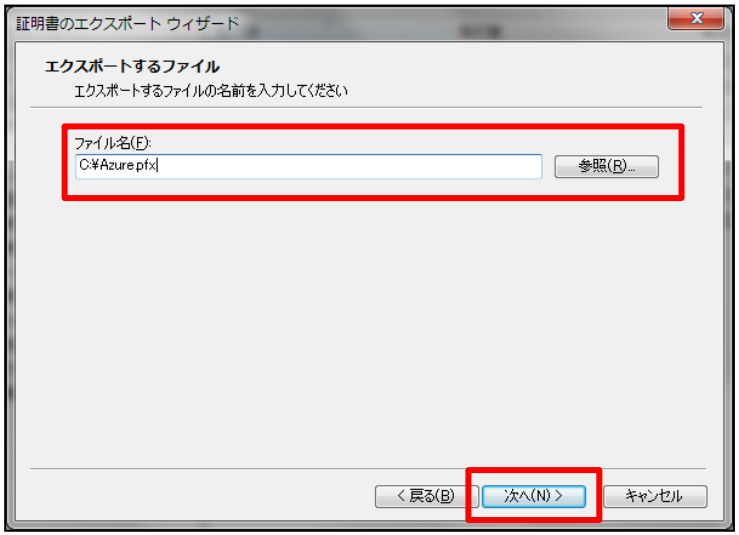
13. 【パスワード】、【パスワードの確認入力】に任意のパスワードを入力し、【次へ】をクリックします。

※パスワードはpfxファイルをインポートする際に必要です。



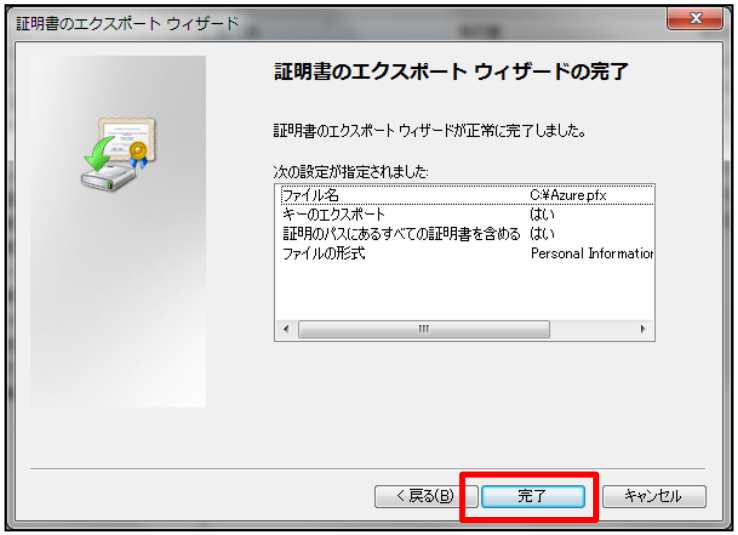
14. 任意のファイル名(拡張子は.pfx)を入力して、【次へ】をクリックします。

※ファイル名はファイル出力先のフルパスを入力します。

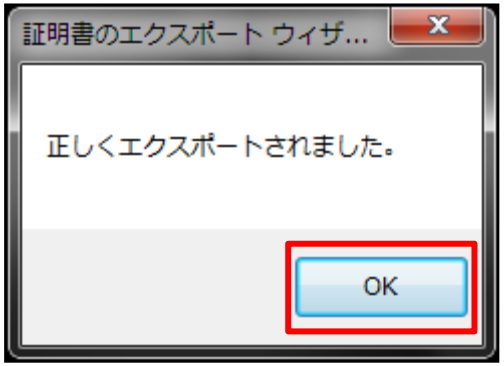


6. pfxファイルの作成

15. 証明書のエクスポートウィザードが正常に完了したことを確認し、【完了】をクリックします。



16. 【正しくエクスポートされました。】というメッセージが表示されましたら、【OK】をクリックします。



以上で、pfxファイルの作成は完了です。

7. pfxファイルのアップロード

作成したpfxファイルを「Microsoft Azure」管理ポータルサイトへアップロードし、証明書を設定します。

1. 管理ポータルへログインし、左側のメニューより【クラウドサービス】をクリックし、一覧から証明書を設定したいサービスをクリックします。

7. pfxファイルのアップロード

2. 上部メニューより【証明書】をクリックし、【→】ボタンをクリックします。

※更新の際は画面下部の【アップロード】ボタンをクリックします。

7. pfxファイルのアップロード

3. 【ファイル】よりアップロードするpfxファイルを選択し、pfxファイルの作成時に指定したパスワードを入力して、【✓】ボタンをクリックします。

4. pfxファイルがアップロードされます。

以上で、pfxファイルのアップロードは完了です。

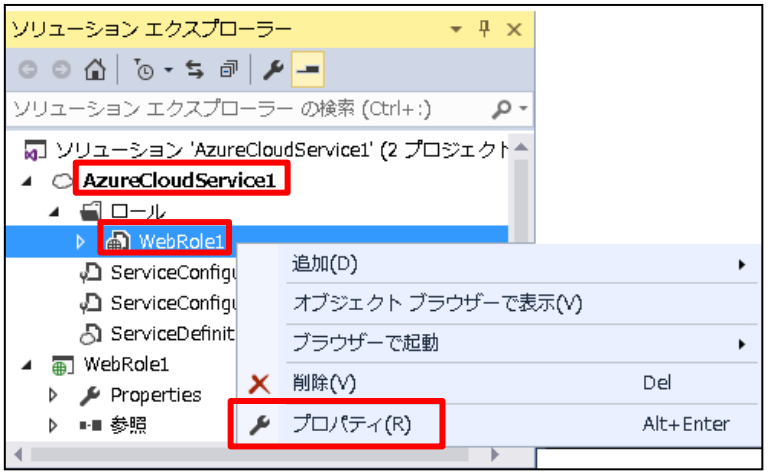
8. パッケージファイルとサービス構成ファイルの作成

開発環境でパッケージファイル（cspkgファイル）と、サービス構成ファイル（cscfgファイル）を作成します。

※本手順では「Microsoft Visual Studio Express 2015」を使用しております。

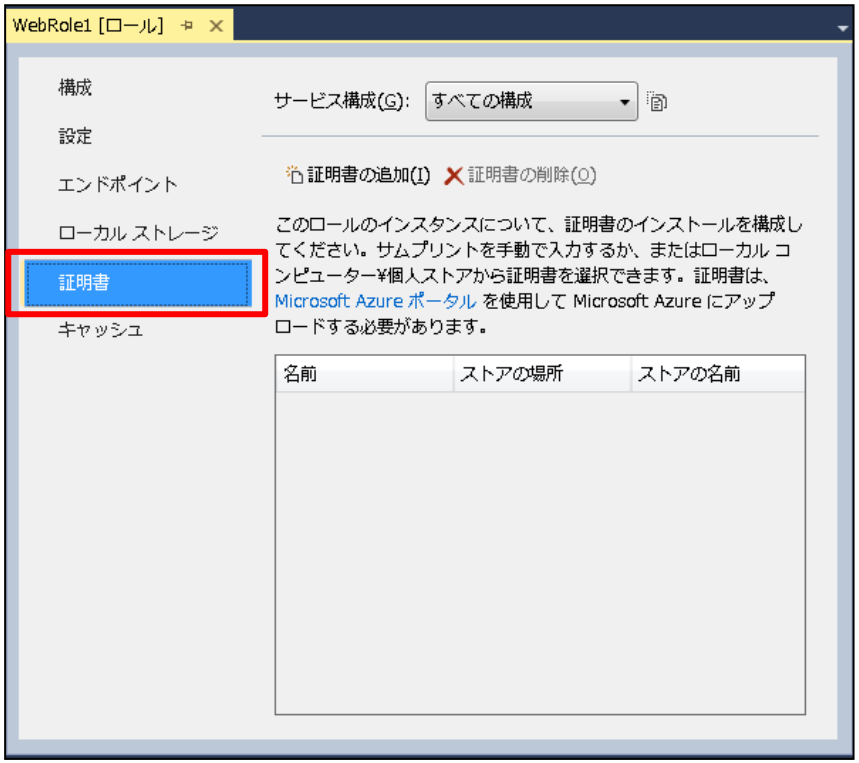
※「Microsoft Visual Studio」以外の開発環境をお使いのお客様の場合、操作が異なる可能性がございます。パッケージファイルの作成方法はお使いのソフトのマニュアルをご覧ください。

1. 開発環境のプログラムを起動し、証明書を適用するプロジェクトを開き、Webロールを右クリックして、【プロパティ】をクリックします。



8. パッケージファイルとサービス構成ファイルの作成

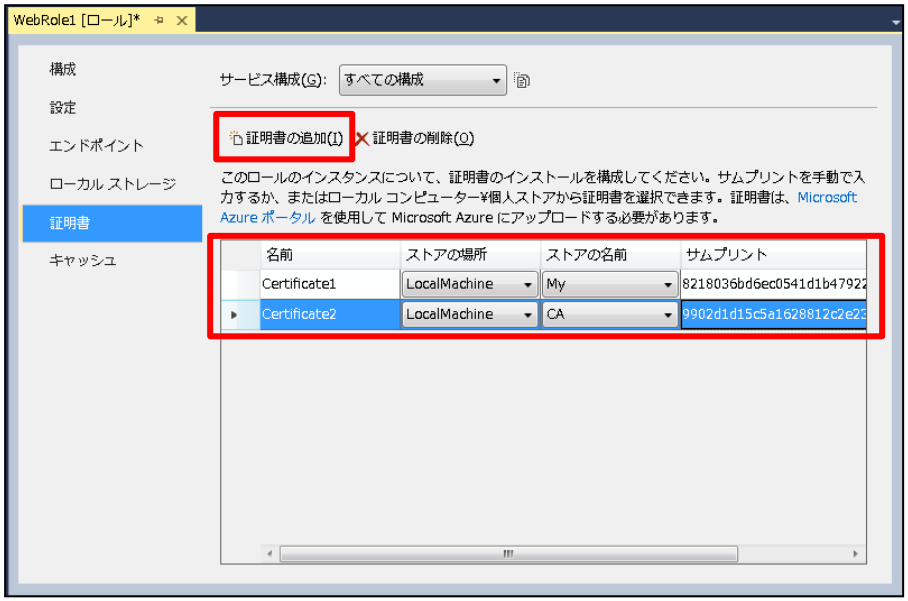
2. 【証明書】をクリックします。



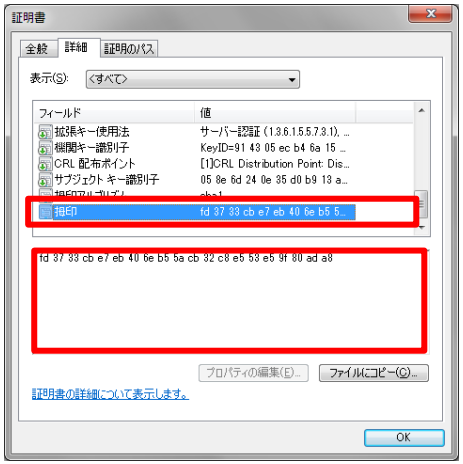
8. パッケージファイルとサービス構成ファイルの作成

3. 【証明書の追加】を2回クリックして、サーバー証明書と中間CA証明書を設定します。

項目	サーバー証明書	中間CA証明書
名前	任意の証明書名	
ストアの場所	LocalMachine	
ストアの名前	My	CA
サムプリント	各証明書の拇印	

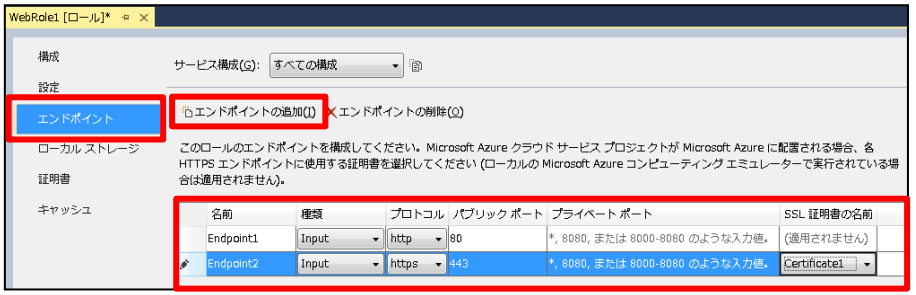


- 証明書の更新時は、サムプリントの値を更新後の証明書の値に変更してください。
- 【サムプリント】は証明書の拇印の値です。
  値を直接入力するか、【…】をクリックしてpfxファイルを選択してください。
  ※証明書をダブルクリックした際に表示される、「証明書の詳細タブ」 > 「拇印」より確認できます。



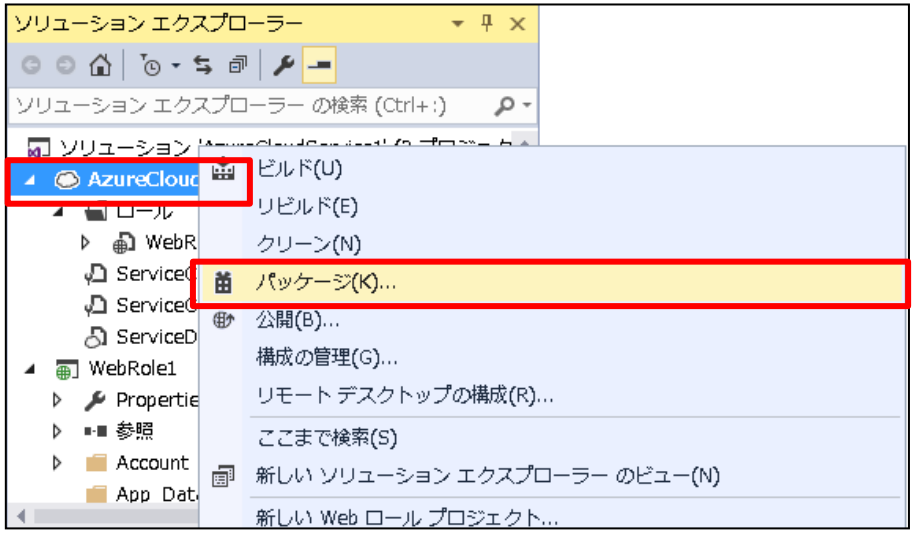
8. パッケージファイルとサービス構成ファイルの作成

4. 【エンドポイント】→【エンドポイントの追加】の順にクリックします。



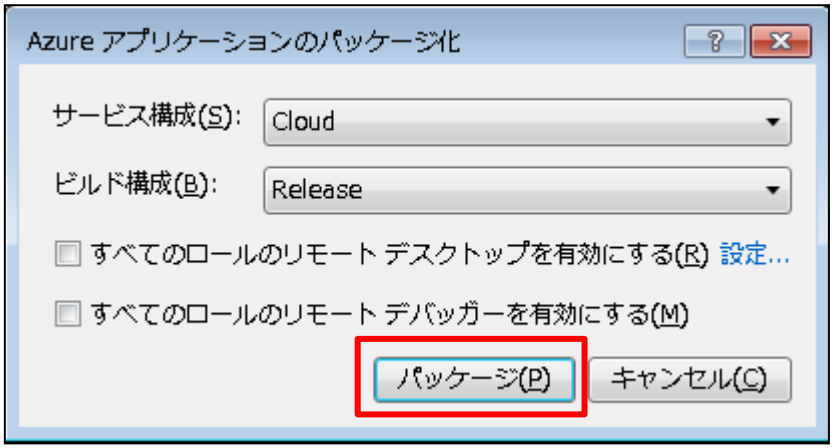
- 【名前】　：エンドポイントの名前（任意）
- 【種類】　：Input
- 【プロトコル】　：https
- 【パブリックポート】：SSL通信を行うポート（通常は443）
- 【SSL証明書の名前】：前頁で設定したサーバー証明書の名前

5. プロジェクト名を右クリックし、【パッケージ】をクリックします。



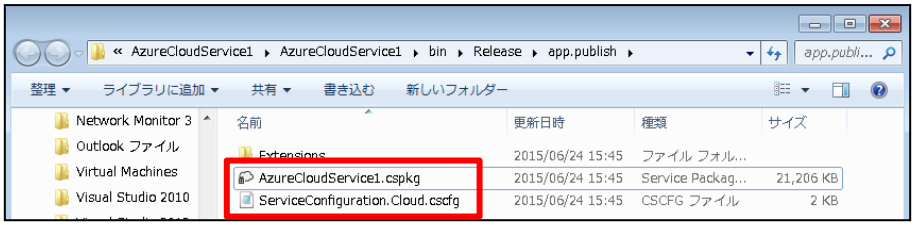
8. パッケージファイルとサービス構成ファイルの作成

6. 【パッケージ】をクリックします。



7. パッケージファイル（cspkgファイル）とサービス構成ファイル（cscfgファイル）が作成され、保存フォルダが表示されます。

※保存フォルダのパスを控えておくことを推奨します。



以上で、パッケージファイルとサービス構成ファイルの作成は完了です。

9. ファイルのアップロード

作成したパッケージファイルとサービス構成ファイルを
「Microsoft Azure」管理ポータルサイトへアップロードします。

1. 管理ポータルへログインし、左側のメニューより【クラウドサービス】をクリックし、一覧から、証明書を設定したいサービスをクリックします。

- 作成したファイルのアップロードはご利用の環境に応じて、以下のいずれかの設定を行います。
  - 新規運用環境のデプロイ
  - 既存デプロイの構成変更

    ※証明書の更新時は「既存デプロイの構成変更」を行ってください。

10. 新規運用環境のデプロイ

■新規運用環境のデプロイ

1. 【デプロイの設定】の【新規運用環境のデプロイ】をクリックします。

2. 必要項目を入力・選択します。

項目	値
デプロイラベル	任意のラベル名
パッケージ	【ローカルから】cspkgファイル
構成	【ローカルから】cscfgファイル

3. 【デプロイの開始】にチェックを入れます。

4. 【✓】ボタンをクリックします。

以上で、新規運用環境のデプロイは完了です。

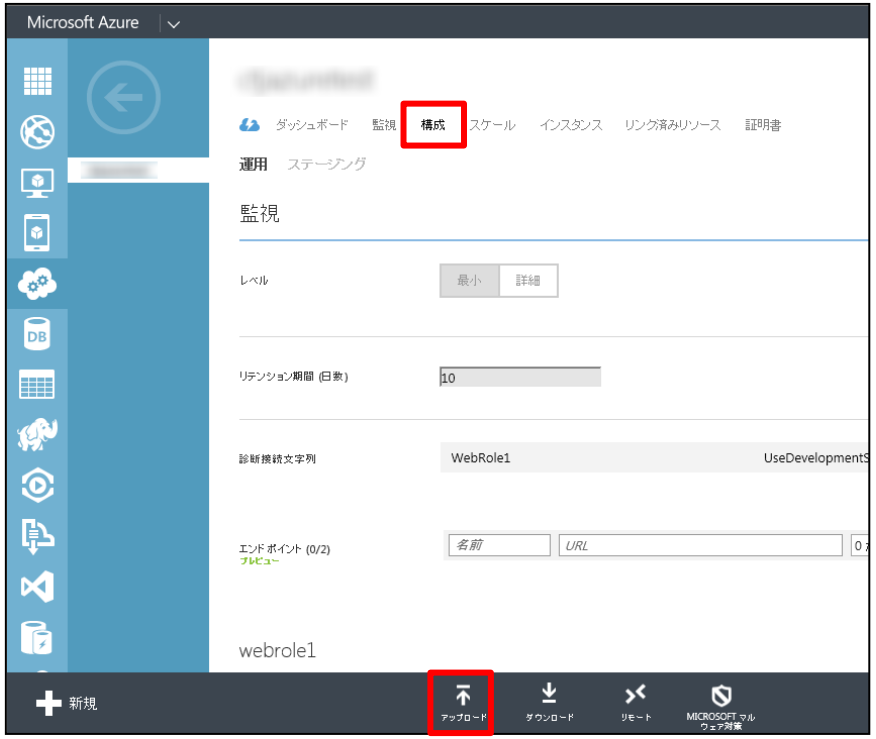
11.既存デプロイの構成変更

■既存デプロイの構成変更

A) 証明書階層の変更がない場合

※更新前と同じ商品をご利用の場合は本手順を行ってください。

1. 上部のメニューより【構成】をクリックし、画面下部の【アップロード】をクリックします。



11.既存デプロイの構成変更

2. cscfgファイルを指定します。

3. 【✓】ボタンをクリックします。

以上で、証明書階層の変更がない場合の既存デプロイの構成変更は完了です。

- 作成したpfxファイルなどは、万が一に備えて必ず別のメディア（CDやUSBメモリ等）にコピーして安全な場所に保管してください。
- 弊社がお客様の秘密鍵ファイルの情報が含まれたpfxファイルなどの情報を受け取ることはございません。

11.既存デプロイの構成変更

■既存デプロイの構成変更

B) 証明書階層の変更がある場合

※他社お乗換えや商品変更、中間CA証明書の差し替えの場合などは本手順を行ってください。

1. クラウドサービスのトップページの【運用環境のデプロイを更新する】をクリックします。

11.既存デプロイの構成変更

2. 必要項目を入力・選択します。

項目	値
デプロイラベル	任意のラベル名
パッケージ	【ローカルから】cspkgファイル
構成	【ローカルから】cscfgファイル
ロール	変更対象のロール

3. 【✓】ボタンをクリックします。

以上で、証明書階層の変更がある場合の既存デプロイの構成変更は完了です。

- 作成したpfxファイルなどは、万が一に備えて必ず別のメディア（CDや、USB等）にコピーして安全な場所に保管してください。
- 弊社がお客様の秘密鍵ファイルの情報が含まれたpfxファイルなどの情報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。

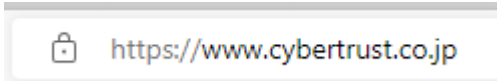
12. SSL通信の確認

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。

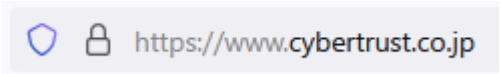
- SSL通信の確認は設定を行っているサーバー以外のWEBブラウザやスマートフォンなどの携帯端末、弊社「SSLサーバ証明書　導入サポートツール」のサーバ証明書の設定確認から行うことを推奨します。

■設定確認例

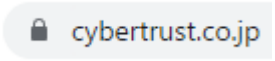
<Edge>



<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/

https://www.cybertrust.ne.jp

詳細は下記まで、お問い合わせください。
0120-957-975
電話受付時間 平日 9:00 ～ 18:00
servicedesk@cybertrust.ne.jp