

Microsoft Azure Web Apps 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

【！】 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」の「Web Apps」でサイバートラストのSSL/TLS サーバー証明書を設定する手順について解説するドキュメントです。
2. 本手順は、2019年3月時点の「Microsoft Azure」の「Web Apps」および「IIS10.0」の環境下で動作確認をしております。
3. 「Microsoft Azure」の「Web Apps」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。
4. 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、「Microsoft Azure」の「Web Apps」サービス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。
5. 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。
6. 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。

目次

1. <u>ご利用の前に</u>	…P4
2. <u>CSR作成</u>	…P5
3. <u>証明書のお申し込み</u>	…P6
4. <u>証明書のダウンロード</u>	…P7
5. <u>証明書のインストール</u>	…P9
6. <u>pfxファイルの作成</u>	…P10
7. <u>pfxファイルのアップロード</u>	…P18
8. <u>カスタムドメインの設定</u>	…P22
9. <u>SSL バインディングの設定</u>	…P25
10. <u>SSL/TLS通信の確認</u>	…P27

サイバートラストのSSL/TLS サーバー証明書を「Microsoft Azure」の「Web Apps」でご利用の場合、以下の点にご注意ください。

- 「Web Apps」で利用する「***.azurewebsites.net」は、Microsoft 社が管理しているドメインのため、SSL/TLS サーバー証明書を取得できません。CSR作成前にお客様独自のドメインを事前に取得のうえ、DNSサーバーで「Aレコード」もしくは「CNAME」のレコードを登録してください。
- お客様独自のドメインは、Basic、Standard、Premium、Isolatedのサービス プランで利用可能です。

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-----  
.....  
MIIEnhDCCA2wCAQAwYkxCzAJBgNVBAYTAkpQM4wDAYDVQQIDAVUb2t5bzESMBAG  
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKBDIDeWJlcnRydXN0IEphcGFuIENvLixM  
dGQuMRIwEAYDVQQLEDAIUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJ0cnVz  
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyIIEST  
.....  
-----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/TLS 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/TLS 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

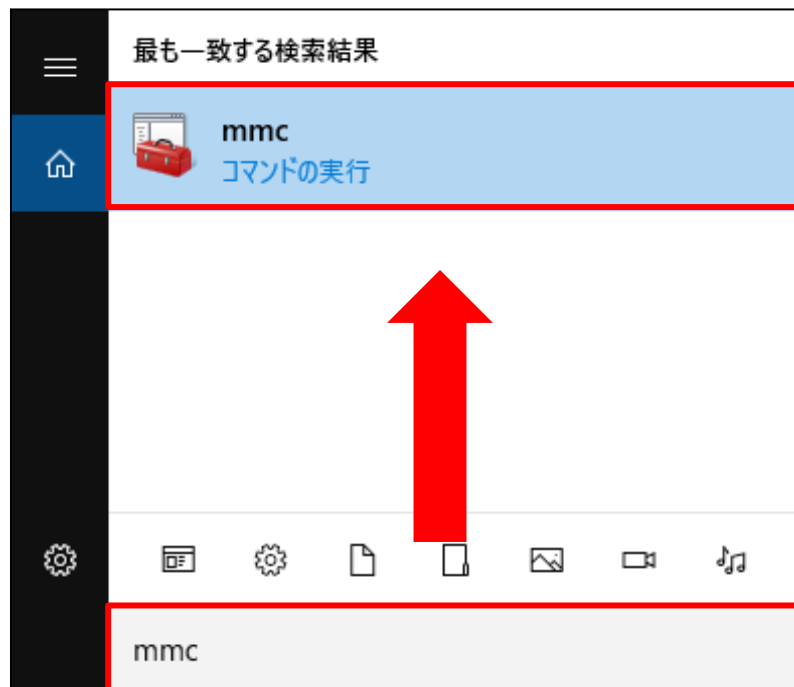
インストールした中間CA証明書、サーバー証明書と秘密鍵ファイルを1つのpfxファイルとして、エクスポートします。

※本手順ではIIS10.0を例にご説明します。

1. 【Windowsを検索】 ボタンをクリックします。

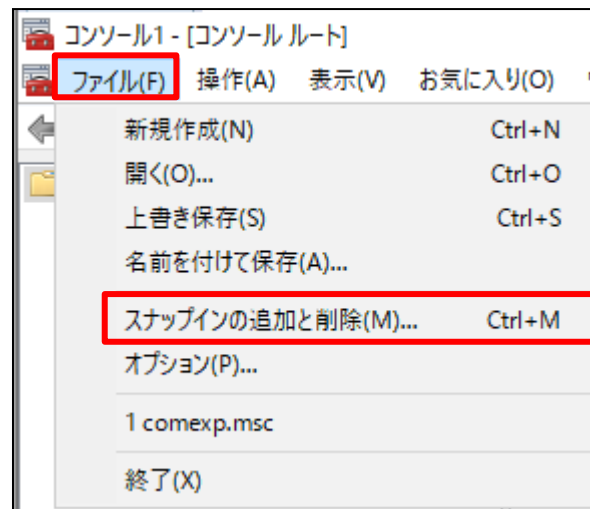


2. テキストボックスに「mmc」と入力し、検索結果の【mmc】をクリックして、「Microsoft 管理コンソール (MMC) 」を起動します。

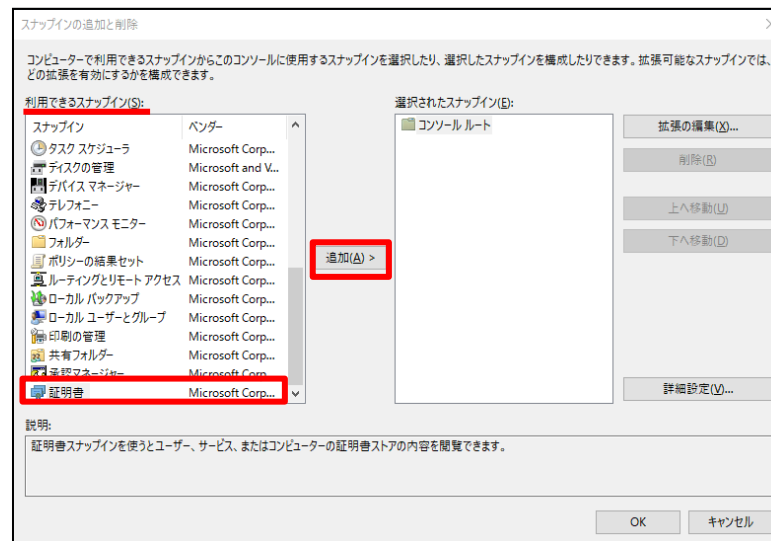


6. pfxファイルの作成

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。

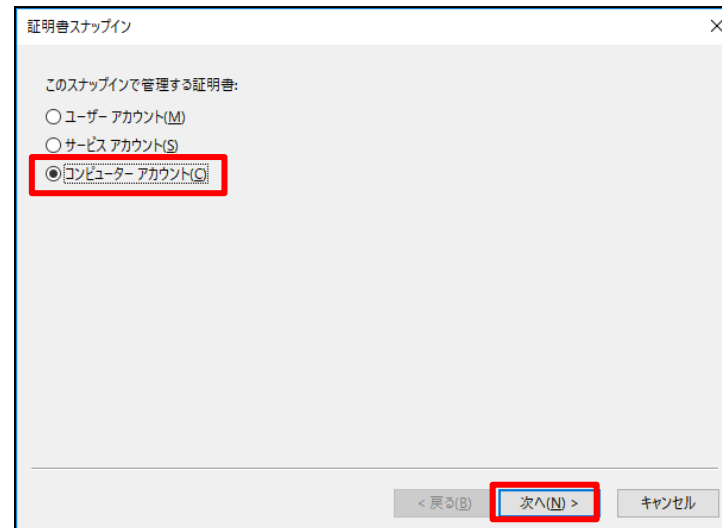


4. 【利用できるスナップイン】の【証明書】を選択し、【追加】をクリックします。

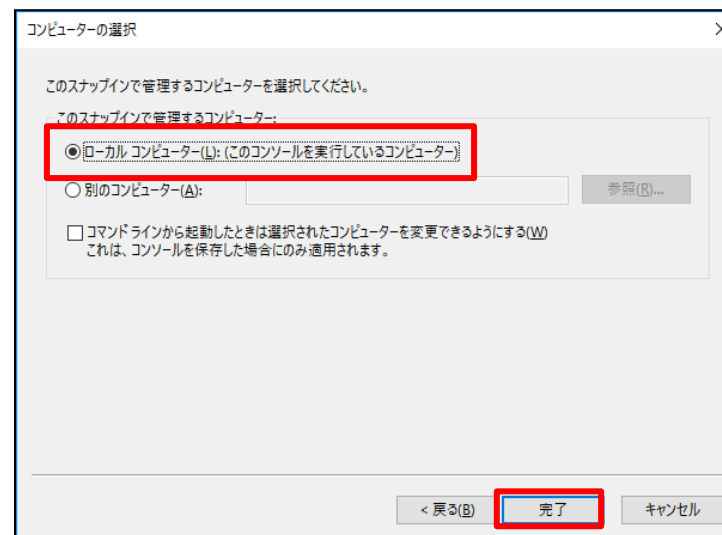


6. pfxファイルの作成

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。

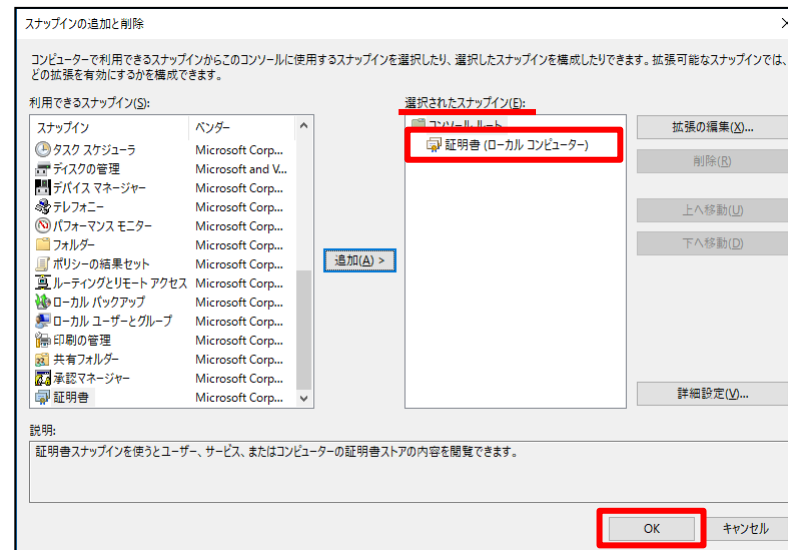


6. 【ローカルコンピューター】を選択し、【完了】をクリックします。

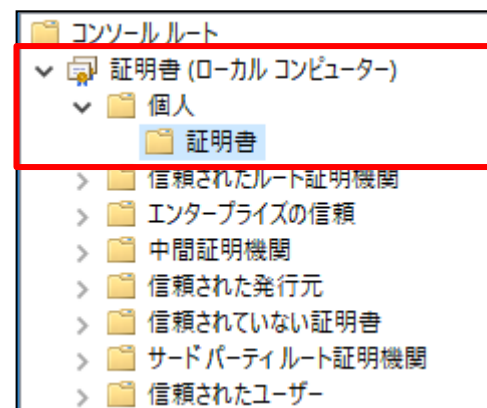


6. pfxファイルの作成

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。

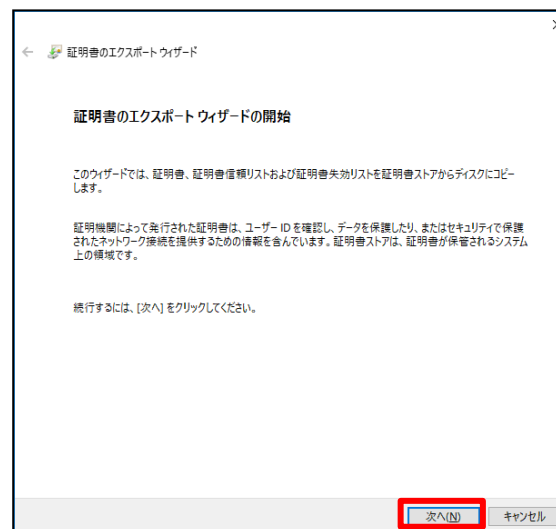


6. pfxファイルの作成

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。

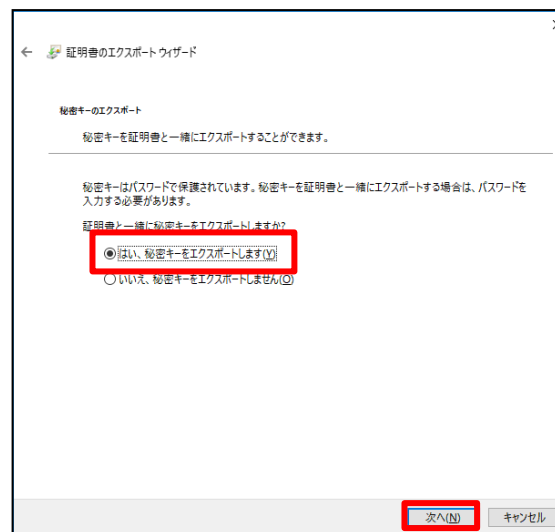


10. 【証明書のエクスポートウィザード】が起動したら、【次へ】をクリックします。



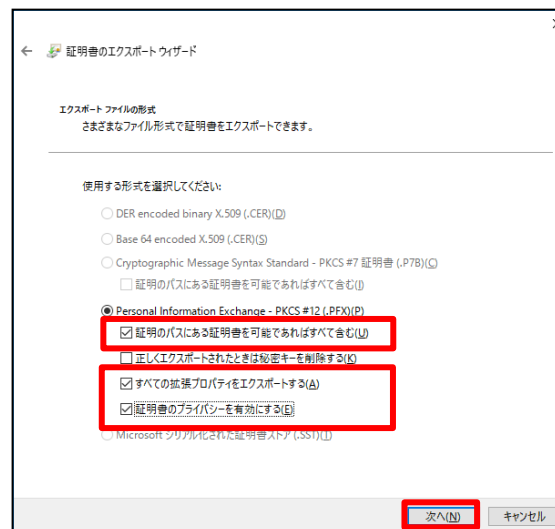
6. pfxファイルの作成

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. 以下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。

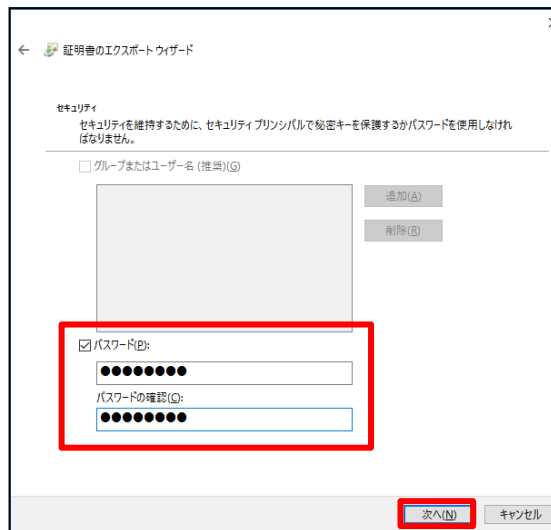
- ・ 証明書のパスにある証明書を可能であればすべて含む
- ・ すべての拡張プロパティをエクスポートする
- ・ 証明書のプライバシーを有効にする



6. pfxファイルの作成

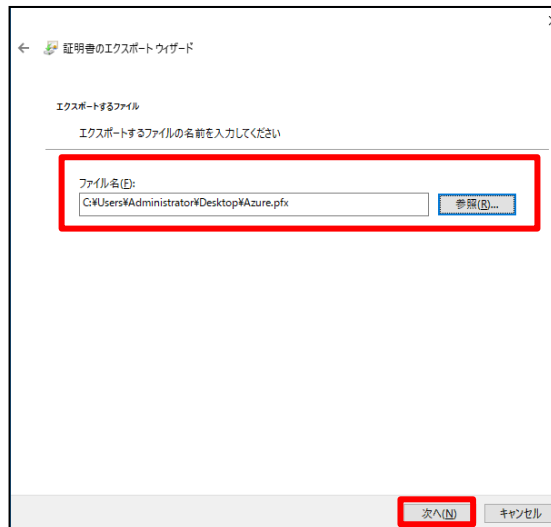
13. 【パスワード】にチェックを入れ、
【パスワード】の入力欄と【パス
ワードの確認入力】に任意のパス
ワードを入力し、【次へ】をクリッ
クします。

※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。



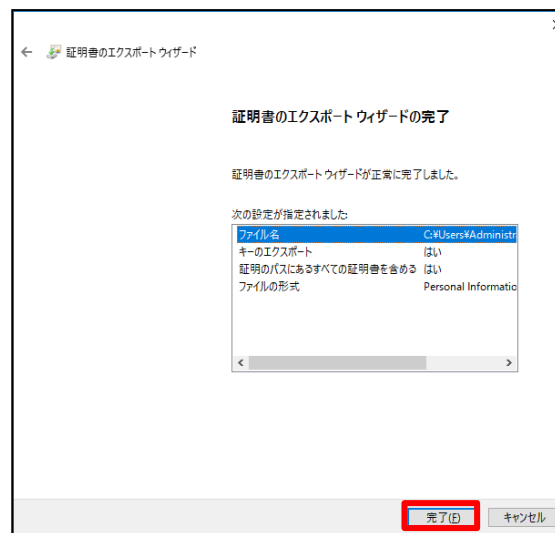
14. 任意のファイル名(拡張子は.pfx)を入
力して、【次へ】をクリックします。

※ファイル名はファイル出力先の
フルパスを入力もしくは【参照】か
ら指定します。

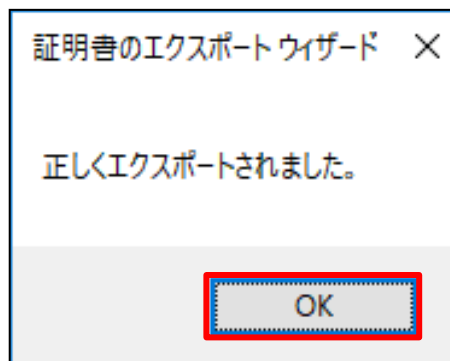


6. pfxファイルの作成

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を確認し、【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

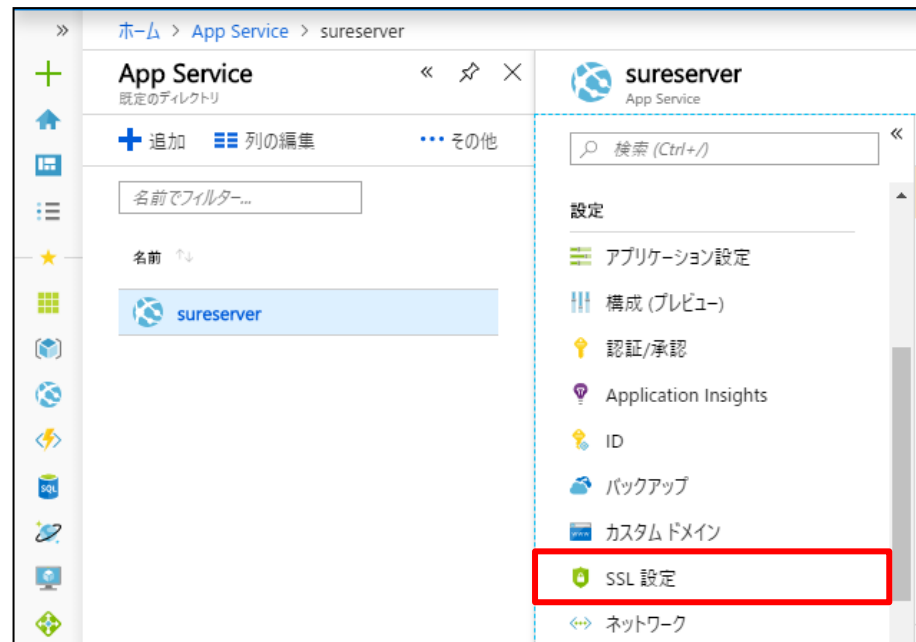
作成したpfxファイルを「Microsoft Azure」管理ポータルサイトへアップロードします。

1. 管理ポータルへログインし、左側のメニューより【Web Apps】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. 【SSL 設定】をクリックします。



7. pfxファイルのアップロード

3. 【プライベート証明書 (.pfx)】 タブをクリックし、【証明書のアップロード】をクリックします。





最新の情報に更新 ? よく寄せられる質問 | バインドを削除する

バインド プライベート証明書 (.pfx) 公開証明書 (.cer)

 **プライベート証明書**

プライベート証明書 (.pfx) は、SSL バインドのために使用したり、アプリで使用するために証明書ストアに読み込んだりすることができます。アプリで使用するために証明書を読み込む方法の詳細については、詳細情報リンクをクリックしてください。アップロードした証明書は、Azure 管理ポータルからの手動ダウンロードには利用できません。これらの証明書は、必要なアプリ設定を正しく設定した後に App Service でホストされたアプリで使用するか、SSL のために使用することのみが可能です。
[詳細情報](#)

 App Service 証明書のインポート  **証明書のアップロード**

プライベート証明書

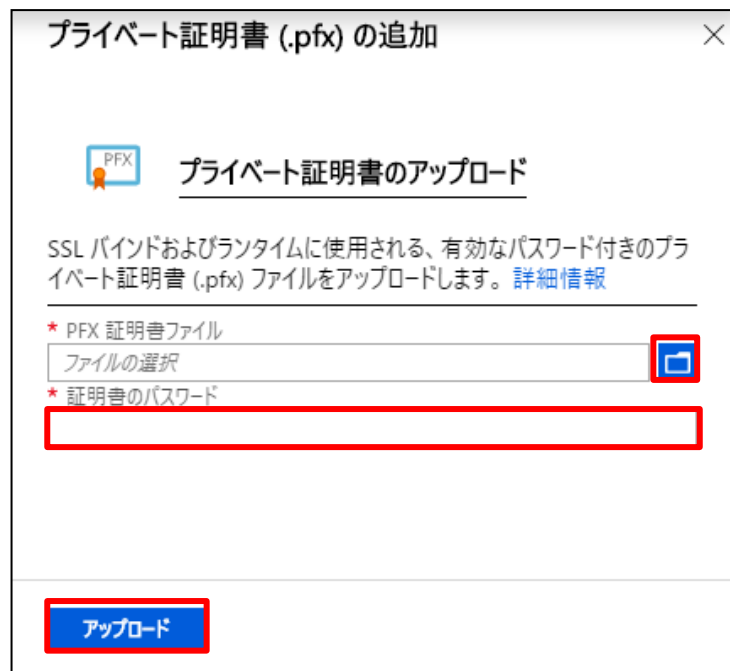
状態フィルター **すべて** 正常 警告 有効期限切れ

ヘルス状...	ホスト名	有効期限	サムプリント
---------	------	------	--------

アプリが使用できるプライベート証明書がありません。

7. pfxファイルのアップロード

4. 【PFX 証明書ファイル】のフォルダアイコンをクリックしてアップロードするpfxファイルを選択し、【証明書のパスワード】にpfxファイルの作成時に指定したパスワードを入力して、【アップロード】をクリックします。



5. pfxファイルがアップロードされます。

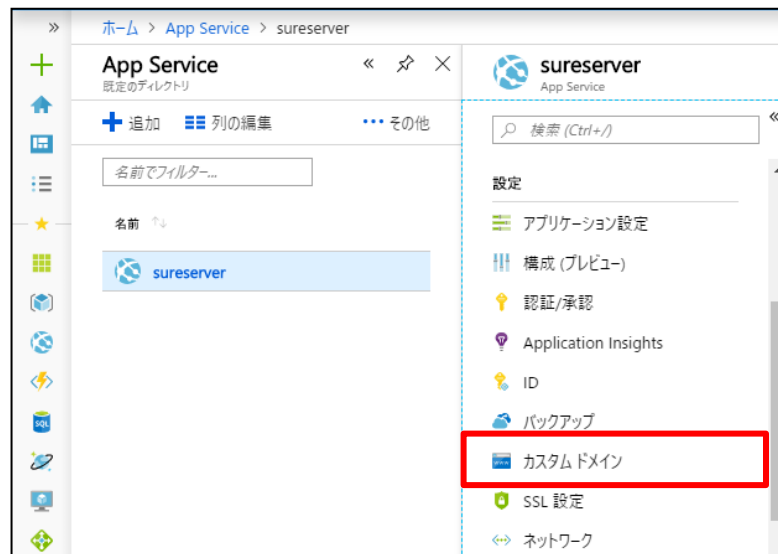


以上で、pfxファイルのアップロードは完了です。

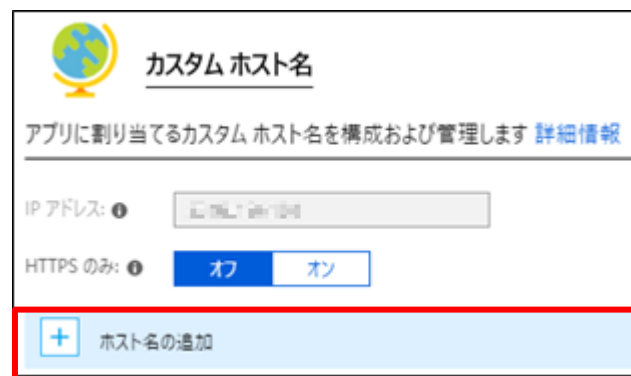
8. カスタムドメインの設定

「Aレコード」もしくは「CNAME」に設定したお客様独自のドメインをカスタムドメインとして設定します。

1. 【カスタム ドメイン】をクリックします。

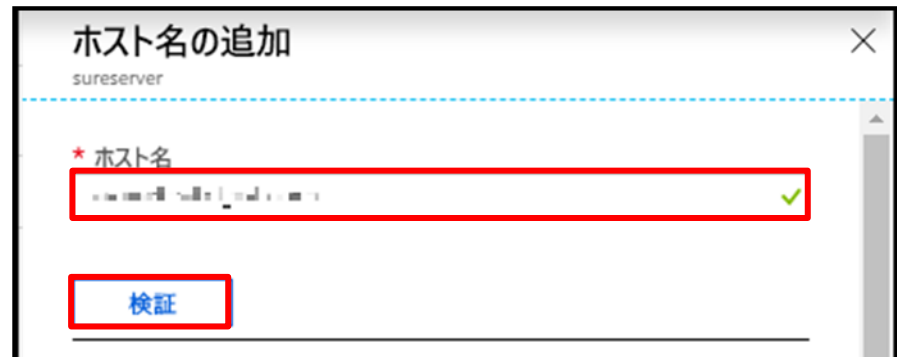


2. 【ホスト名の追加】をクリックします。

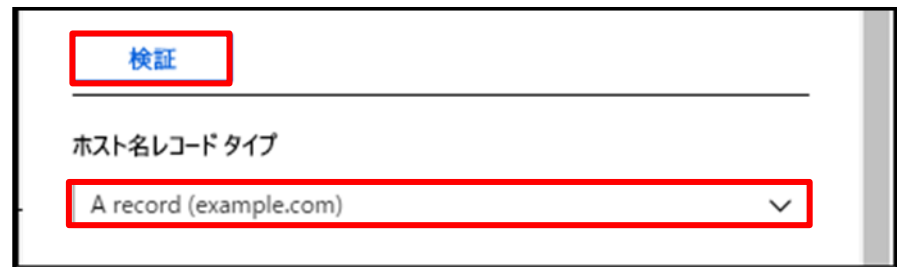


8. カスタムドメインの設定

3. 設定を行うお客様独自のドメインを【ホスト名】に入力し、【検証】をクリックします。



※ A レコードを使用する場合のみ、【ホスト名レコードタイプ】で【A record(example.com)】を選択し、再度【検証】をクリックします。



8. カスタムドメインの設定


4. 【ホスト名】の追加をクリックします。

ホスト名の追加

☒ ホスト名の利用可否


☒ ドメイン所有権

※右図のエラーが表示された場合は、【ホスト名レコードタイプ】に応じて、お客様独自のドメインのDNS設定を行ってください。

 **ドメイン所有権**

以下の構成を使用して、DNS プロバイダーで CNAME レコードを作成します。[詳細情報](#)

種類	ホスト	値
CNAME	www またはサブドメイン	...

 **ドメイン所有権**

ドメインの所有権を確認するには、以下の構成を使用して、DNS プロバイダーで TXT レコードおよび A レコードを作成します。[詳細情報](#)

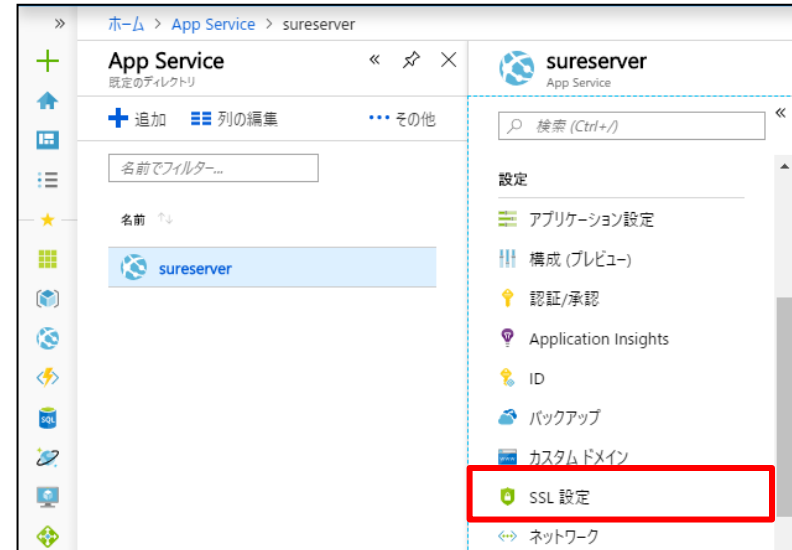
種類	ホスト	値
TXT	@	...
A	@	...

以上で、カスタムドメインの設定は完了です。

9. SSL バインディングの設定

カスタムドメインとアップロードした証明書を紐づけるため、SSL バインディングの設定を行います。

1. 【SSL 設定】をクリックします。



9. SSL バインディングの設定

2. 【SSL バインディングの追加】をクリックします。

[最新の情報に更新](#) | [よく寄せられる質問](#) | [バインドを削除する](#)

バインド

プライベート証明書 (.pfx)

公開証明書 (.cer)



プロトコル設定

プロトコル設定はグローバルであり、アプリで定義されているすべてのバインディングに適用されます。

HTTPS のみ:

TLS の最小バージョン:

着信クライアント証明書:



SSL バインド

バインディングを使用すると、特定のホスト名に対して HTTPS で行われる要求にตอบสนองの際に使用する証明書を指定できます。SSL バインディングには、特定のホスト名に対して発行された、有効なプライベート証明書 (.pfx) が必要です。[詳細情報](#)

+

SSL バインディングの追加


<input checked="" type="checkbox"/> ホスト名	プライベート証明書の拇印	SSL の種類
SSL バインディングがアプリに対して構成されていません。		

9. SSL バインディングの設定

3. 【ホスト名】と【プライベート証明書の拇印】と【SSL の種類】をリストから選択し、【バインディングの追加】をクリックします。

- 【ホスト名】
「8. カスタムドメインの設定」で設定済みのドメインが表示されます。未設定のドメインは表示されません。
- 【プライベート証明書の拇印】
設定済みのカスタムドメインと同名の証明書が表示されます。別名の証明書の場合、pfx ファイルをアップロード済みであっても表示されません。
- 【SNI SSL】
任意で【SNI SSL】または【IP ベースの SSL】を選択します。

SSL バインディング



SSL バインド

SSL で保護するホスト名と、使用する証明書をドロップダウンから選択してください。Server Name Indication (SNI) と IP ベースの SSL のどちらを使用するかを選択することもできます。[詳細情報](#)

* ホスト名

* プライベート証明書の拇印

* SSL の種類:

SNI SSL

バインディングの追加

9. SSL バインディングの設定

4. 追加した【ホスト名】と【プライベート証明書の拇印】と【SSL の種類】が表示されます。



The screenshot shows the 'SSL バインド' (SSL Binding) configuration page. At the top, there are links for '最新の情報に更新' (Update latest information), 'よく寄せられる質問' (Frequently asked questions), and 'バインドを削除する' (Delete binding). Below this is a tabbed interface with 'バインド' (Binding) selected, showing options for 'プライベート証明書 (.pfx)' (Private certificate) and '公開証明書 (.cer)' (Public certificate). The 'プロトコル設定' (Protocol settings) section includes a gear icon and a description: 'プロトコル設定はグローバルであり、アプリで定義されているすべてのバインディングに適用されます。' (Protocol settings are global and apply to all bindings defined in the app). It contains three settings: 'HTTPS のみ' (HTTPS only) set to 'オン' (On), 'TLS の最小バージョン' (Minimum TLS version) set to '1.2', and '着信クライアント証明書' (Incoming client certificate) set to 'オフ' (Off). The 'SSL バインド' section has a lock icon and a description: 'バインディングを使用すると、特定のホスト名に対して HTTPS で行われる要求に応答する際に使用する証明書を指定できます。SSL バインディングには、特定のホスト名に対して発行された、有効なプライベート証明書 (.pfx) が必要です。詳細情報' (Using bindings allows you to specify the certificate used to respond to requests over HTTPS for specific host names. SSL bindings require a valid private certificate (.pfx) issued for the specific host name. See details). Below this is a '+ SSL バインディングの追加' (Add SSL binding) button. At the bottom, there is a table with columns: 'ホスト名' (Host name), 'プライベート証明書の拇印' (Private certificate thumbprint), and 'SSL の種類' (SSL type). The table contains one row with placeholder icons for each column, and the entire table area is highlighted with a red rectangle.

以上で、設定は全て完了です。

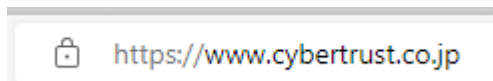
- 作成したpfxファイルは、万が一に備えて別のメディア（CDやUSB等）にコピーして安全な場所に保管してください。
- 弊社がお客様の秘密鍵ファイルの情報が含まれたpfxファイルの情報を受け取ることはございません。あらかじめご了承ください。

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。

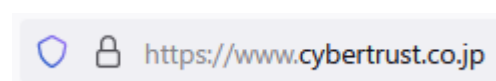
- SSL通信の確認は設定を行っているサーバー以外のWEBブラウザやスマートフォンなどの携帯端末、弊社「SSLサーバ証明書 導入サポートツール」のサーバ証明書の設定確認から行うことを推奨します。

■ 設定確認例

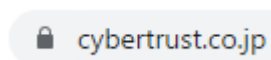
<Edge>



<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