JPRS サーバー証明書発行サービス ACME 対応版

Posh-ACME ご利用マニュアル

Version 1.2

株式会社日本レジストリサービス（JPRS）

目次

更新履歴

日付	Version	
2022/03/02	1.0	初版リリース
2022/04/11	1.1	OCSP に関する注意書きを更新
2022/12/15	1.2	更新に関する Windows の設定を変更

1 本資料について

本資料では、JPRS サーバー証明書発行サービス ACME 対応版（以下、本サービス）でご利用可能な ACME クライアントの一つである、Posh-ACME のご利用方法について説明します。

1.1 ACME について

ACME（アクミー）は、Automatic Certificate Management Environment（自動証明書管理環境）に由来する、証明書の管理を自動化するためのプロトコル（取り決め）です。証明書の管理者が ACME に対応することで、サーバー証明書をほぼ全自動で管理できます。

ACME に対応する場合、ACME のサービスを利用するためのソフトウェアである、ACME クライアントを使用できます。

1.2 Posh-ACME について

Posh-ACME は Windows PowerShell 向けのモジュールです。無償で利用可能です。

※ 本資料の執筆時点において、Posh-ACME は日本語のメッセージ表示に対応していないため、エラーメッセージの表示が文字化けします。エラーメッセージは英語と日本語で表示されますので、英語のメッセージを参照してください。

1.3 本資料における前提条件について

本資料は、以下の前提条件で記述しています。

- ✓ Windows Server 2019 及び IIS 10 をご利用中のものとします。
- ✓ Administrator 権限でコマンドを実行できるものとします。
- ✓ OS の設定については、本資料の対象外とします。
- ✓ モジュールのインストール方法については、本資料の対象外とします。
- ✓ ワイルドカード証明書を含む、DNS 認証（dns-01）を利用したサーバー証明書の発行・更新につきましては、ご利用中の DNS プロバイダーとの連携に対応したプラ

グインが必要となるため、本資料の対象外とします。恐れ入りますが、DNS 認証プラグインの利用方法につきましては、ご利用者様にてご確認ください。

2 事前準備

2.1 Posh-ACME のインストール

以下の参考 URL に記載された公式ドキュメント等をご参照のうえ、ご利用の環境に PowerShell から Posh-ACME モジュールと Posh-ACME.Deploy モジュールをインストールしてください。

なお、インストール方法については本資料では扱いませんので、予めご了承ください。

参考 Posh-ACME https://github.com/rmbolger/Posh-ACME

Posh-ACME.Deploy https://github.com/rmbolger/Posh-ACME.Deploy

2.2 指定事業者を経由した本サービスの利用申し込み

本サービスのご利用には、指定事業者を経由した申し込みが必要になります。

お手続き方法等は、指定事業者により異なります。申し込みやお手続きなどの詳細につきましては、ご利用の指定事業者にお問い合わせください。

2.3 ACME アカウントの発行に必要な EAB 認証情報の受領

本サービスのご利用には、EAB（認証情報）が必要です。

ご利用の指定事業者から EAB（認証情報）を受け取ってください。

※ EAB（認証情報）の有効期間は、EAB 認証情報の発行から 14 日間です。
この期間内に、手順 3.1「ACME アカウントの発行する」を行ってください。

※ EAB（認証情報）の有効期間が終了した場合や、EAB（認証情報）を失くした場合には、指定事業者へ EAB（認証情報）の発行を依頼してください。

3 初回の証明書発行を行う

3.1 ACME アカウントを発行する

本サービスを利用するための ACME アカウントの発行が必要になります。ご利用中の指定事業者から受領した EAB（認証情報）をご用意ください。

なお、ACME アカウント発行にあたり、JPRS からの緊急連絡を受信するメールアドレスの登録が必要になります。

Set-PAServer コマンドで、JPRS の ACME サーバーを接続先に指定します。

```
PS C:¥ > Set-PAServer https://acme.amecert.jprs.jp/DV/getDirectory
```

PS C:¥ >の表示は、ご利用の環境により異なります。また、この部分の入力は不要です。

New-PAAccount コマンドで EAB（認証情報）を利用し、ACME アカウントを発行します。

・-ExtAcctKID（必須）：指定事業者から受領した MAC 鍵識別子を入力します。

・-ExtAcctHMACKey（必須）：指定事業者から受領した MAC 鍵を入力します。

・-Contact（必須）：JPRS からの緊急連絡を受信するメールアドレスを登録します。

・-AcceptTOS（必須）：ご利用条件に同意します。

```
PS C:¥ > New-PAAccount -ExtAcctKID
62lYPavZWyE2MkzARtx_vxi7hmyFDG9GwOG8AlN_AAA -ExtAcctHMACKey
7O2PTsLwGNcr9bn3ImOD5-vlKE750bytPwjApnWcAAA -Contact info@jprs.jp -
AcceptTOS
```

以下のメッセージが表示されましたら、ACME アカウントの発行は完了です。

```
id                    status    contact                  alg      KeyLength
--                    ------    -------                  ---      ---------
mk8NmSN--MQB8JCPR... valid      {mailto:info@jprs.jp}    ES256    ec-256
```

※マニュアルへの記載の都合上、一部表示内容を省略しております。

3.2 サーバー証明書を発行する

本サービスではサーバー証明書発行時のドメイン名利用権の確認方法として、ACME のファイル認証（http-01）または DNS 認証（dns-01）を利用できます。

本マニュアルではファイル認証を利用し、IIS に証明書を設定する場合の例を記載します。

> ご注意
>
> ※ DNS 認証を利用する場合、ご利用中の DNS プロバイダーとの連携に対応したプラグインが必要になります。DNS 認証用のプラグインの利用方法につきましては、恐れ入りますがご利用者様にてご確認ください。

New-PACertificate コマンドで、証明書の発行申請をします。

・-Plugin WebRoot：ファイル認証に利用するプラグインを指定します。
（本プラグインはデフォルトでインストールされています）

・-PluginArgs ： ウェブサイトのルートディレクトリを入力します。

```
New-PACertificate example.jp -Plugin WebRoot -PluginArgs @{WRPath =
'C:¥inetpub¥wwwroot'}
```

複数の FQDN を指定する場合、example.jp,www.example.jp のようにコンマで区切って指定します。複数の FQDN を指定することで、それらの FQDN が SAN（そのサーバー証明書を設定・使用するドメイン名）に記載された、1 枚の証明書が発行されます。

> ご注意
>
> ※ この状況において指定した FQDN の一つを利用終了した場合、その証明書自体が失効され、結果として他の FQDN が使用中であった場合も、指定したすべての FQDN の証明書が無効となることにご注意ください。
>
> 当該状況を回避するため、複数の FQDN を指定する場合、同じ利用期間を持つ FQDN とすることを推奨します。

当該コマンドを実行した際、以下のエラーメッセージが表示されます。

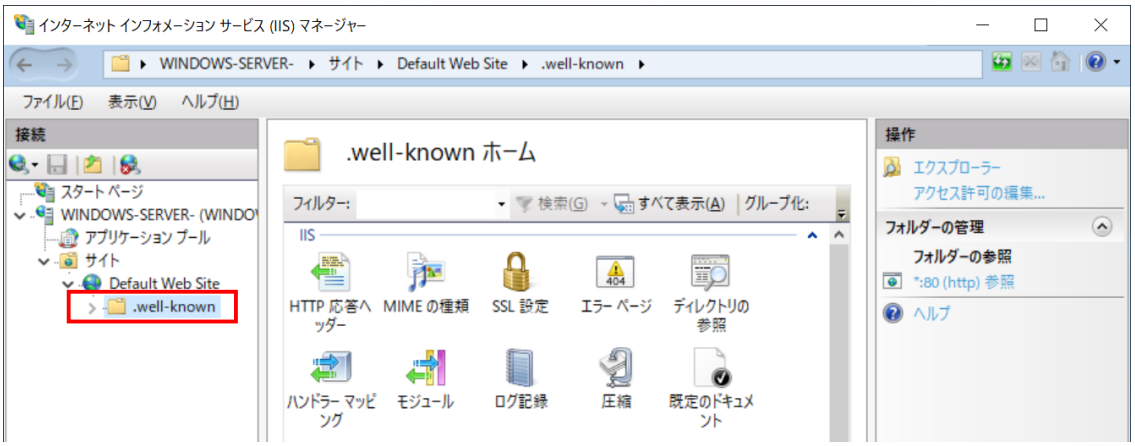
```
Exception: C:¥Program Files¥PowerShell¥Modules¥Posh-
ACME¥4.12.0¥Public¥New-PACertificate.ps1:238
Line |
```



```
238 |             Submit-ChallengeValidation
    |             ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    | Authorization invalid for (指定した FQDN):
```

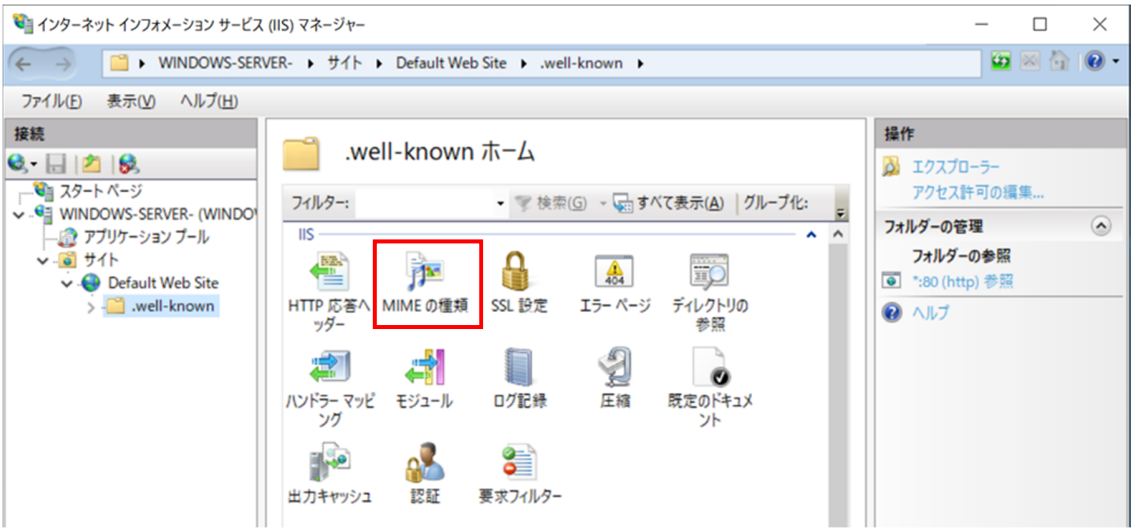
このエラーは以下の手順により「インターネットインフォメーションサービス（IIS）マネージャー」に、MIME の種類を設定することで解消できます。

① インターネットインフォメーションサービス（IIS）マネージャーを起動し、サーバー証明書を設定するサイトを選択し、配下の.well-known フォルダーをダブルクリックします。

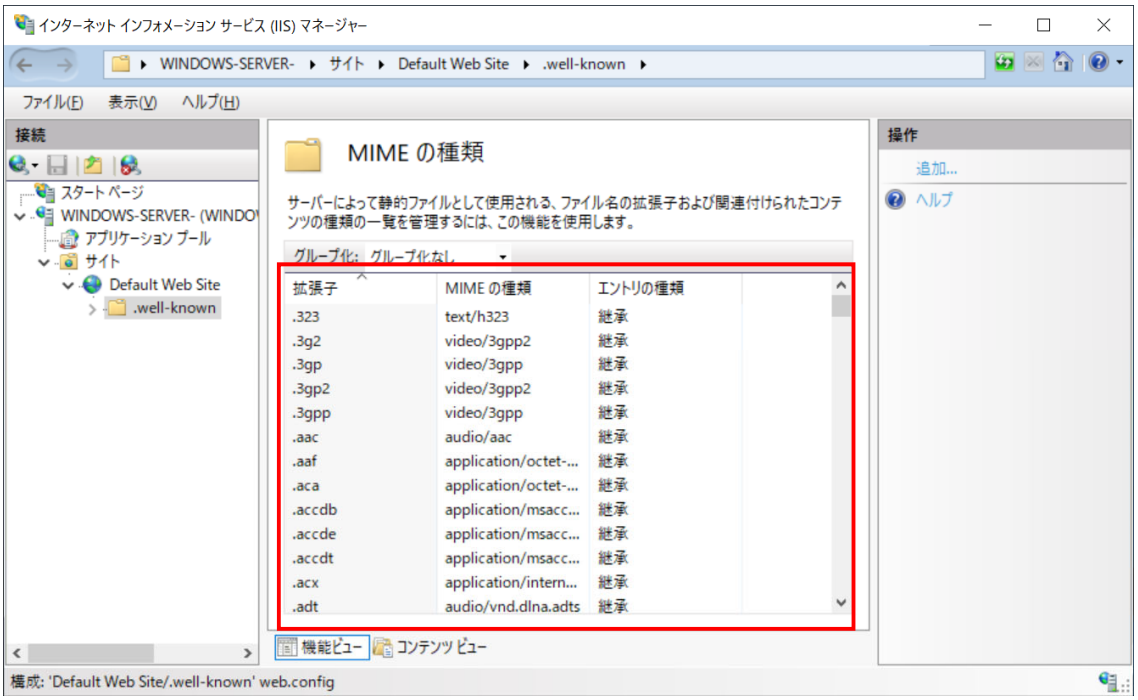


※ New-PACertificate コマンドを一度も実行していない場合、.well-known フォルダーは作成されていませんのでご注意ください。

② 「MIME の種類」をダブルクリックします。



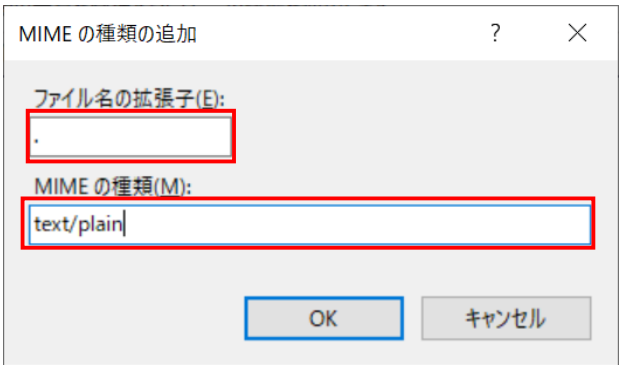
③　MIME の種類が表示されている部分で右クリックし、「追加」をクリックします。



④　MIME の種類の追加が表示されたら以下の通り入力し、OK をクリックします。

・ファイル名の拡張子（E）:.　※ドット（.）のみ

・MIME の種類（M）:text/plain



⑤　インターネットインフォメーションサービス（IIS）マネージャーを閉じます。

再度、New-PACertificate コマンドで、証明書の発行申請をします。

```
New-PACertificate example.jp -Plugin WebRoot -PluginArgs @{WRPath =
'C:¥inetpub¥wwwroot'}
```

以下のメッセージが表示されれば、証明書の発行は完了です。

```
Subject          NotAfter               KeyLength Thumbprint AllSANs
-------          --------               --------- ---------- -------
CN=example.jp 2022/04/21 14:59:59 2048        36C4211B5E {example...
```

ご注意

※ ワイルドカード証明書はファイル認証では発行できません。DNS 認証をご利用ください。

※ DNS 認証では、証明書の発行対象となる FQDN のゾーンを管理する権威 DNS サーバーに、ドメイン名利用権確認用の認証文字列が記載された TXT レコードを所定の方式で設定・更新する必要があります。そのため、DNS 認証を利用して証明書の発行・更新を自動化する（TXT レコードの設定・更新を自動化する）場合、ご利用の DNS プロバイダーが ACME クライアントとの API 連携に対応している必要があります。詳細につきましては、ご利用中の DNS プロバイダーにご確認ください。

※ Posh-ACME には主な DNS プロバイダーとの API 連携に対応したプラグインが用意されています。詳細は Posh-ACME 公式の Web サイト(*)をご確認ください。

(*) https://poshac.me/docs/v4/Plugins/

3.3 サーバー証明書をインストールする

Get-PACertificate | Set-IISCertificate コマンドを実行し、証明書を IIS にインストールします。

・SiteName：IIS のサイトネームを指定します。

・Port：IIS のポート番号を指定します。

```
PS C:¥ > Get-PACertificate | Set-IISCertificate -SiteName example.jp -Port 443
```

ご注意

現時点における本サービスの仕様により、証明書の発行から OCSP（証明書のステータス情報をオンラインで提供するプロトコル）サーバーへの情報登録までに、最大 10 分程度のタイムラグが存在します。

これにより、アクセス時に OCSP の情報を確認する一部 Web ブラウザーにおいて、OCSP に関するエラーメッセージが表示される場合があります。当社では Firefox ブラウザーにおいて、この状況を確認しています。

証明書の更新と Web サーバーへの読み込みの間に所定の待機時間を設定することで、エラーの発生を回避できます。

4 証明書の更新

4.1 更新を行う

Submit-Renewal コマンドを実行し、サーバー証明書を更新します。

```
PS C:¥ > Submit-Renewal example.jp
```

4.2 サーバー証明書をインストールする

Get-PACertificate | Set-IISCertificate コマンドを実行し、サーバー証明書を IIS にインストールします。

・SiteName：IIS のサイトネームを指定します。

・Port：IIS のポート番号を指定します。

```
PS C:¥ > Get-PACertificate | Set-IISCertificate -SiteName example.jp -Port 443
```

ご注意

現時点における本サービスの仕様により、証明書の発行から OCSP（証明書のステータス情報をオンラインで提供するプロトコル）サーバーへの情報登録までに、最大 10 分程度のタイムラグが存在します。

これにより、アクセス時に OCSP の情報を確認する一部 Web ブラウザーにおいて、OCSP に関するエラーメッセージが表示される場合があります。当社では Firefox ブラウザーにおいて、この状況を確認しています。

証明書の更新と Web サーバーへの読み込みの間に所定の待機時間を設定することで、エラーの発生を回避できます。

4.3 更新とインストールを自動化する

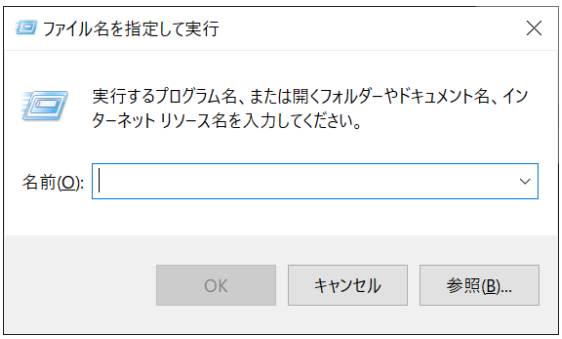
更新とインストールを自動化したい場合、タスクスケジューラと PS1 ファイルを利用します。

テキストエディタ（メモ帳など）で以下の内容を記載し、拡張子を ps1 として保存します。

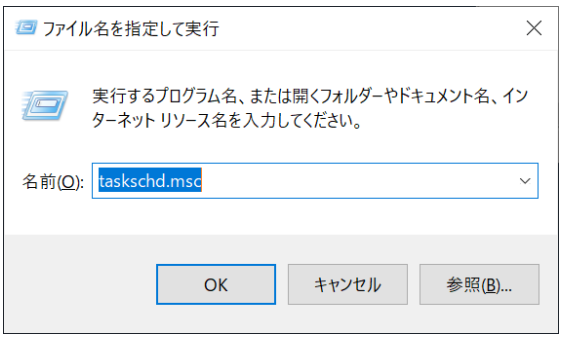
```
Start-Transcript acme_log.txt

Set-PAOrder example.jp -Verbose

if ($cert = Submit-Renewal) {

  Start-Sleep 600

  $cert | Set-IISCertificate -SiteName example.jp -Port 443 -Verbose

}

Stop-Transcript
```

※ログファイル名、ドメイン名、サイトネーム、ポート番号は環境に応じて書き換えてください。

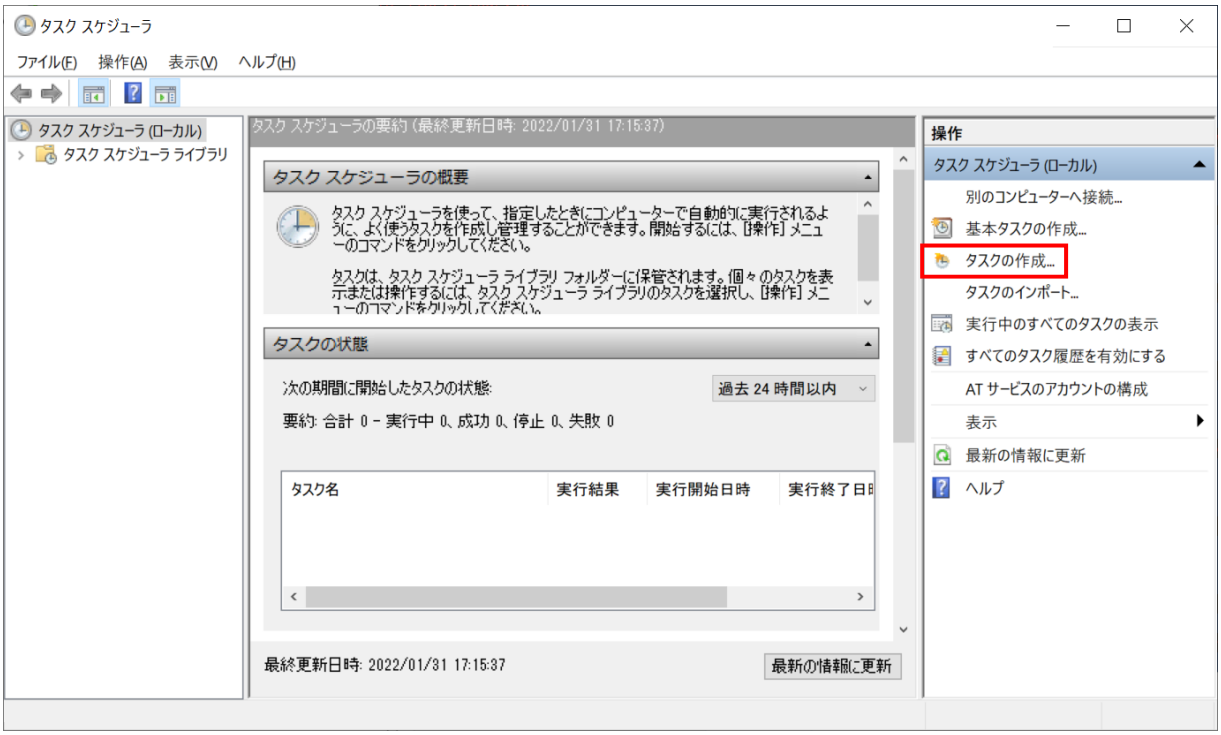
キーボードの「Windows」キーを押しながら「R」キーを押し、「ファイル名を指定して実行」を表示します。



「名前（O)」に taskschd.msc と入力して、OK をクリックします。

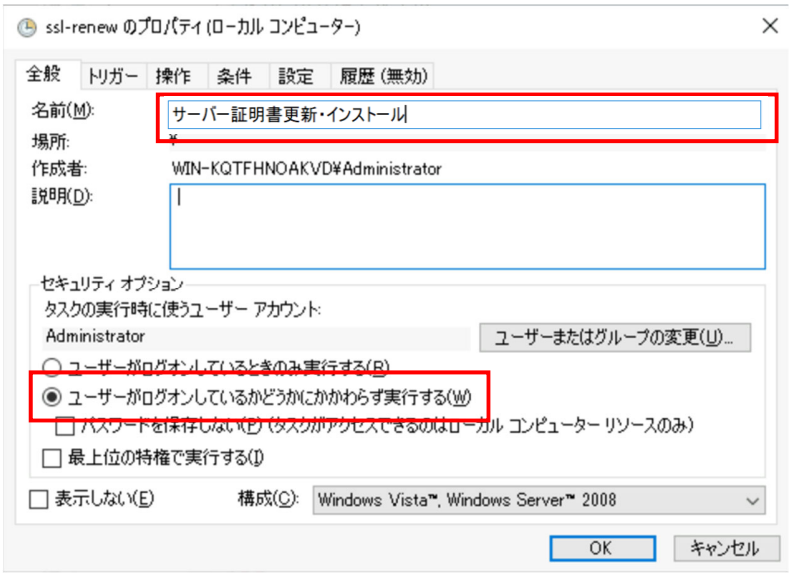


タスクスケジューラが起動しますので、「タスクの作成」をクリックします。

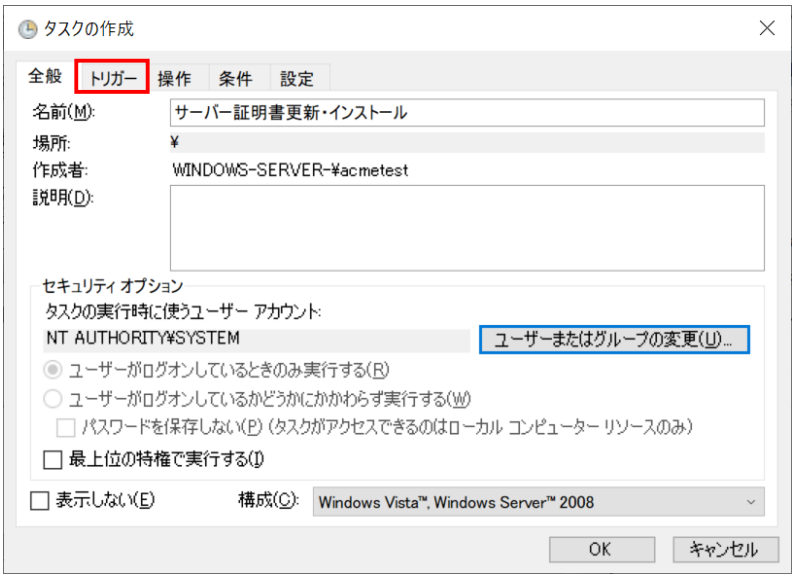


タスクの作成が表示されたら、「名前（M)」にタスクの名前を入力し、セキュリティオプションの「ユーザーがログオンしているかどうかに関わらず実行する（W)」をクリックします。

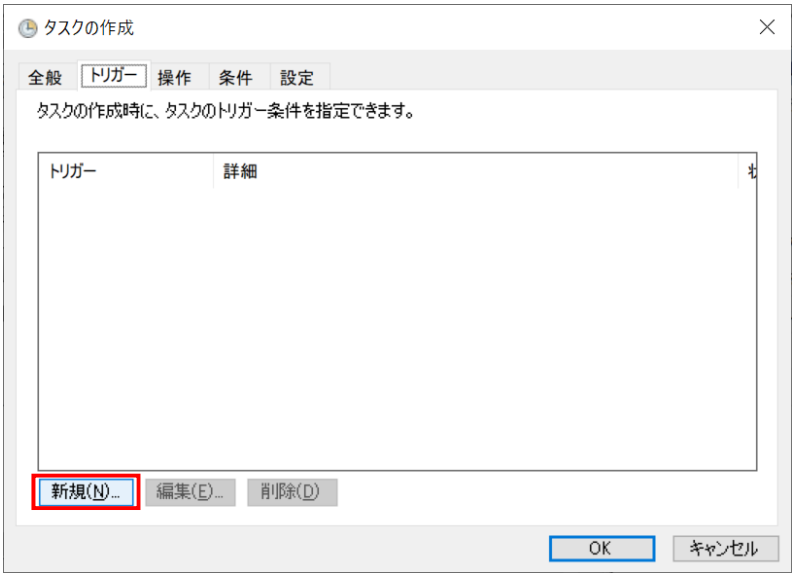
※名称には任意の名前を設定可能です。わかりやすい名前を入力しておくとよいでしょう。



再び、タスクの作成が表示されますので、「トリガー」タブをクリックします。



トリガータブが表示されましたら、「新規（N)」をクリックします。



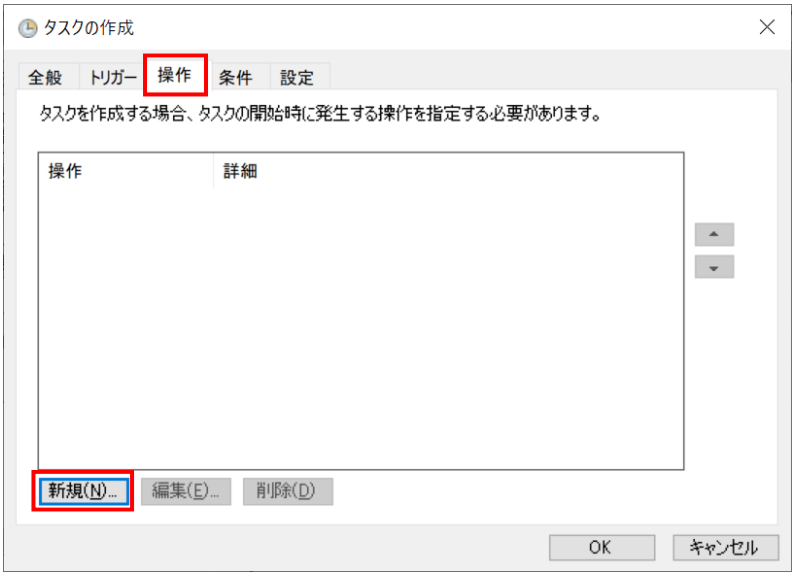
新しいトリガーが表示されたら以下の内容を選択・入力し、画面下の「OK」をクリックします。

・設定の「毎日（D)」を選択

・「開始（S)」の時刻欄に、毎日の更新チェックを開始したい時刻を設定

※任意の時刻を設定可能です。

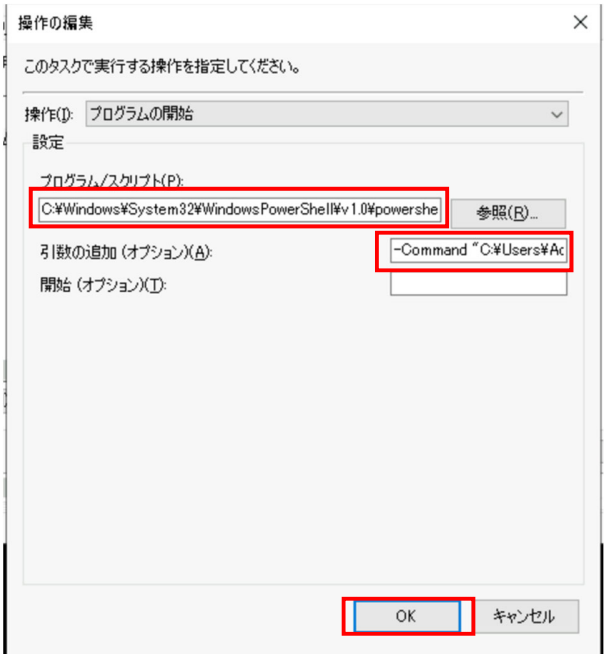
タスクの作成に戻りますので「操作」のタブをクリックし、「新規（N)」をクリックします。



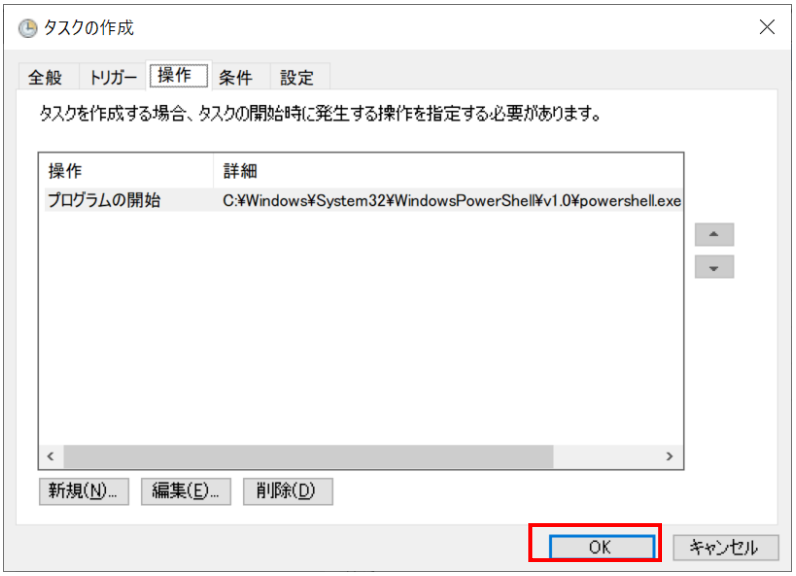
操作の編集が表示されますので、プログラム/スクリプト（P）に以下を入力します。

C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe

引数の追加（オプション）に作成した-Command “ps1 ファイルを保存したパス”を入力し、「OK」をクリックします（例：-Command "C:¥renew.ps1"）。



タスクの作成が表示されますので、「OK」をクリックし、設定を完了します。



ご注意

※　更新処理は、サーバー証明書の有効期限（発行から 90 日後）の 30 日前から可能です。更新可能なタイミングになりましたら、必ず更新処理が行われているかをご確認ください。

5 その他必要時にのみ行う作業（強制更新、失効）

5.1 強制的に更新を行う

- Force オプションを指定することで、証明書を強制的に更新できます。緊急に証明書の入れ替えが必要になったなどの場合に、本オプションを指定してください。

強制更新が完了しましたら、手順 4.2「サーバー証明書をインストールする」を参照し、サーバー証明書をインストールしてください。

※ 大量の証明書発行が継続して行われた場合、サーバー側で申請を制限する場合があります。

```
PS C:¥ Submit-Renewal example.jp -Force
```

5.2 （必要時）証明書を失効する

秘密鍵の危殆化など、証明書を失効する必要が生じた場合、次のコマンドを実行することで証明書を失効できます。

```
PS C:¥ Revoke-PACertificate example.jp
```


6 参考情報

6.1 Posh-ACME 公式サイト

様々な環境における Posh-ACME のインストール・証明書の設定方法が記載されています。

https://poshac.me/

6.2 ACME 対応版サービス - エラーの種別と発生条件

本サービスで出力するエラーの種別と発生条件は次の通りです。

エラー種別	HTTP ステータスコード	メッセージ文(英語)	発生条件
accountDoesNotExist	400	The request specified an account that does not exist	指定されたアカウントが存在しない場合
alreadyRevoked	400	The request specified a certificate to be revoked that has already been revoked: [%s]	失効対象の証明書が既に失効されている場合
badCSR	400	The CSR is unacceptable	CSR が受け付けられない場合(鍵長が短すぎるなど)
badNonce	400	The client sent an unacceptable anti-replay nonce	受理不能なノンスを受信した場合
badPublicKey	400	The JWS was signed by a public key the server does not support	アカウント公開鍵の情報に問題がある場合
badRevocationReason	400	The revocation reason provided is not allowed by the server: [%s]	送信された失効理由がサーバー側で許可されていない場合
badSignatureAlgorithm	400	The JWS was signed with an algorithm the server does not support: [%s]	サーバーがサポートしないアルゴリズムで JWS が署名されている場合
caa	403	CAA records forbid the CA from issuing a certificate	CAA レコードにより証明書の発行が許可されていない場合
connection	400	The server could not connect to validation target : [%s]	FQDN の審査対象のサーバーに接続できない場合
externalAccountRequired	400	The request must include a value for the externalAccountBinding field	リクエストに externalAccountBinding(*)が存在しない場合 (*)認証情報(MAC 鍵識別子・MAC 鍵)
invalidContact	400	A contact URL for an account was invalid: [%s]	コンタクトの URL の形式が不正である場合
malformed	400	The request information is invalid	必須項目チェックや形式チェックなどのリクエスト不正である場合
malformed	400	Unable to create account	EAB アカウントが不正である場合

malformed	400	The contact information is invalid:	・コンタクトメールアドレスが 7 件以上設定されている、もしくは、0 件である場合 ・コンタクトメールアドレスが重複して設定されている場合
malformed	400	Please agree to the term of service.	利用規約に同意していない場合
malformed	400	The FQDN is invalid: [%s]	発行できない FQDN である場合
malformed	400	Validity period of application has been expired	オーダーオブジェクトの有効期限切れの場合
malformed	400	Unable to accept order	オーダーオブジェクトのステータスが不正である場合
malformed	400	Validity period of application has been expired	認可オブジェクトが有効期限切れである場合
malformed	400	Unable to accept order	認可オブジェクトのステータスが不正である場合
malformed	400	The certificate does not exist: [%s]	失効対象の証明書が存在しない場合
malformed	405	The HTTP method is invalid: [%s]	リクエスト不正：許容されていない HTTP Method である場合
malformed	415	The content-type is invalid: [%s]	リクエスト不正：許容されていない ContentType である場合
orderNotReady	403	The request attempted to finalize an order that is not ready to be finalized	finalize の準備ができていない order に対して finalize した場合
rejectedIdentifier	400	The server will not issue certificates for the identifier	対象の識別子に対してサーバーが証明書を発行しない場合
serverInternal	500	The server experienced an internal error	サーバーで内部エラーが発生した場合
unauthorized	401	The client lacks sufficient authorization	ACME アカウントのステータスが不正である場合
unsupportedContact	400	A contact URL for an account used an unsupported protocol scheme: [%s]	コンタクト URL がサポートしないスキームである場合
unsupportedIdentifier	400	An identifier is of an unsupported type	識別子がサポートされていない場合

※[%s] や [%d] には、エラーの要因となった具体的な値が出力されます

