

## Microsoft Exchange 2010

1. [スタート] → [プログラム] → [Microsoft Exchange 2010] → [Exchange 管理コンソール] の順にクリックします。
2. [データベースを管理する] リンクをクリックします。
3. 左側にあるメニューで、[サーバーの構成] をクリックします。右側にある [操作] メニューで、[Exchange 証明書の新規作成] をクリックします。
4. フレンドリ名を入力するよう求められたら、この証明書を後から識別するのに役立つ名前を入力します。
5. ワイルドカード証明書の CSR を生成する場合は、[ドメインスコープ] の下にあるチェックボックスをオンにします。
6. [Exchange 構成] メニューで、実行の際にセキュリティで保護するサービスを選択します。表示される指示に従って、これらのサービスに接続する場合に使用する名前を入力します。
7. 次の画面では、証明書要求に含める名前が Exchange 2010 によって指定されます。名前を確認し、必要に応じて名前を追加します。
8. [参照] をクリックし、CSR を .req ファイルとして保存します。[次へ] → [新規作成] → [終了] の順にクリックします。
9. CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
10. AffirmTrust ポータルにログオンし、証明書の発行を行います。

## Microsoft Exchange 2007

1. Exchange 管理シェルコマンドラインを開き、次のテキストを 1 行で入力します。

```
New-ExchangeCertificate -GenerateRequest -KeySize 2048 -Path c:certificate.txt -  
SubjectName "c=country, l=locality, s=state, o=company, cn=yourdomain" -  
DomainName otherdomain.com, nextdomain.com -PrivateKeyExportable:$true
```

各項目の詳細は次のとおりです。

- **country** : 2 文字の ISO 3166 国コードです。たとえば、日本のコードは「JP」です。その他の国については、[ISO の国コードのリスト](#)を参照してください。
- **locality** : 本社がある地域または市区町村の正式名称。「Shibuya (渋谷区)」などです。
- **state** : 本社がある都道府県の正式名称。「Tokyo (東京都)」などです。
- **company** : 会社の正式名称。

**yourdomain** : SSL 証明書を要求する対象となる完全修飾ドメイン名 (FQDN) です。ワイルドカード証明書の CSR を生成する場合、コモンネームは \* で始まりません (例: \*.yourcompany.com)。

最初のドメイン名は、-SubjectName の中の cn= の後に表示されます。追加のドメ

イン名は、-DomainName パラメータの後に表示されます。各ドメイン名はカンマで区切られます。ドメイン名は必要な数だけ追加できます。

2. Cドライブ (c:) のルートに CSR ファイル (certificate.txt) が作成されます。このファイルをテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
3. AffirmTrust ポータルにログオンし、証明書の発行を行います。

## Microsoft Exchange 2003

1. [スタート] → [プログラム] → [Microsoft Exchange] → [システム マネージャ] の順にクリックします。
2. [管理グループを表示する] オプションが選択されている場合は、[管理グループ] を展開し、管理グループの名前を展開します。注意: 管理グループを表示するには、[<組織>] を右クリックし、[プロパティ] をクリックします。[管理グループを表示する] チェックボックスをオンにして、[OK] を2回クリックし、Exchange システムマネージャを再起動します。
3. [サーバー] を展開し、設定する Exchange Server コンテナを展開し、[プロトコル] コンテナを展開します。
4. 設定する各プロトコルを展開し、[既定の <プロトコル名> 仮想サーバー] オブジェクトを右クリックして、[プロパティ] をクリックします。
5. [アクセス] タブをクリックし、[証明書] をクリックします。
6. Web サーバー証明書ウィザードで、[次へ] をクリックし、[証明書の新規作成] をクリックし、[次へ] をクリックします。
7. [証明書の要求を作成して後で送信する] をクリックし、[次へ] をクリックします。
8. [名前] ボックスに証明書の適切な名前を入力するか、[既定の <プロトコル名> 仮想サーバー] の初期設定のままにします。[ビット長] リストで、使用するビット長を選択し、[次へ] をクリックします。
9. [組織] ボックスに、証明書を要求する CA の組織情報を入力し、[次へ] をクリックします。
10. [一般名] に、サイトのコモンネームを入力し、[次へ] をクリックします。

注意: インターネットからのアクセスを許可する場合は、この名前を、外部から解決可能な完全修飾ドメイン名 (コモンネーム) にする必要があります。この完全修飾ドメイン名は、仮想サーバにリンクされる IP アドレスにマップする必要があります。

11. [国/地域] リストで、国または地域の名前をクリックします。
12. [都道府県] ボックスと [市区町村] ボックスに、組織に適した情報を入力し、[次へ] をクリックします。
13. [ファイル名] ボックスに、作成する証明書の名前とパスを入力するか、初期設定のファイル名のままにします。[次へ] をクリックします。
14. [要求ファイルの概要] 画面で、情報を確認します。正しくない情報がある場合は、[戻る] をクリックして修正が必要な画面を表示し、必要な修正を行います。[次へ] をクリックして [要求ファイルの概要] 画面に戻り、[次へ] をクリックします。

- 最後の画面には、指定されたファイル名で証明書が作成されたというメッセージが表示されます。初期設定では、ドライブ名:certreq.txt になります。
- [完了]** をクリックします。
- certreq.txt ファイルをテキストエディタで開きます。開始タグと終了タグを含めてテキストをコピーします。
- AffirmTrust ポータルにログオンし、証明書の発行を行います。

## Microsoft IIS 7.x

- [スタート]** → **[管理ツール]** → **[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]** をクリックします。
- サーバ名をクリックします。
- 中央の画面のメニューで、**[セキュリティ]** までスクロールし、**[サーバー証明書]** をダブルクリックします。
- 右側の画面にある **[操作]** メニューで、**[証明書の要求の作成]** をクリックします。証明書の要求ウィザードが表示されます。
- [識別名プロパティ]** 画面にて各情報を入力します。
- [次へ]** をクリックします。
- [暗号化サービス プロバイダーのプロパティ]** 画面で、初期設定 (Microsoft RSA SChannel と 2048) のままにして、**[次へ]** をクリックします。
- CSR の名前と場所を入力します。
- CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
- AffirmTrust ポータルにログオンし、証明書の発行を行います。

## Microsoft IIS 5.5 または 6.x

- コントロールパネルで、**[管理ツール]** → **[インターネット インフォメーション サービス]** をクリックします。
- 左側のパネルで、保護する Web サイトを右クリックし、**[プロパティ]** をクリックします。
- [ディレクトリ セキュリティ]** タブで、**[サーバー証明書]** をクリックします。**[次へ]** をクリックします。
- [証明書の新規作成]** を選択し、**[次へ]** をクリックします。注意: 既存の証明書を更新する場合は、更新のオプションを選択し、手順 10 に進みます。
- [証明書の要求を作成して後で送信する]** を選択し、**[次へ]** をクリックします。
- [名前]** ボックスに、この証明書を後から識別するのに役立つ名前を入力します。ビット長を 2048 に設定します。このパネルの他のチェックボックスはオフのままにして、**[次へ]** をクリックします。
- [組織]** ボックスに、会社の正式名称を入力し、**[次へ]** をクリックします。

8. **[コモンネーム]** ボックスに、サイトの完全修飾ドメイン名 (例: www.yourdomain.com) を入力し、**[次へ]** をクリックします。
9. 組織の所在地 (**[国]**、**[都道府県]**、および **[市区町村]**) を入力し、**[次へ]** をクリックします。
10. **[ファイル名]** ボックスに、ファイルの名前と SSL 証明書署名要求 (CSR) の保存先を入力します。ファイルの拡張子は .txt にします。**[次へ]** をクリックします。
11. **[要求ファイルの概要]** 画面で、**[次へ]** をクリックして CSR ファイルを生成します。
12. CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
13. AffirmTrust ポータルにログオンし、証明書の発行を行います。

**注意：**この手順が完了すると、Web サイトに保留中の要求が作成されます。この保留中の要求は削除しないでください。証明書を受け取ったら、この保留中の要求に証明書をインストールする必要があります。

## Microsoft IIS 4.x

1. IIS の Microsoft 管理コンソール (MMC) を開きます。
2. **[Internet Information Server]** を展開し、保護するコンピュータ名を展開します。
3. 保護する Web サイトの名前を右クリックし、**[プロパティ]** をクリックします。
4. **[ディレクトリ セキュリティ]** フォルダを開きます。
5. **[セキュリティで保護された通信]** で、**[キー マネージャ]** をクリックします。**[新しいキーの作成]** 画面が表示されます。
6. **[証明機関に送信するファイルに要求を添付]** を選択してファイル名を指定するか、初期設定を受け入れます。
7. 会社の情報を入力します。
8. 最後の画面が表示されるまで **[次へ]** をクリックし、**[完了]** をクリックします。変更を保存するよう求められたら、**[はい]** をクリックします。
9. CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
10. AffirmTrust ポータルにログオンし、証明書の発行を行います。

## Microsoft Office Communications Server (OCS) 2007

1. **[スタート]** → **[プログラム]** → **[管理ツール]** → **[Office Communications Server 2007]** の順にクリックします。
2. インストールした Enterprise Edition Server に移動します。
3. サーバ名を右クリックし、**[証明書]** をクリックします。
4. 証明書ウィザードが表示されます。**[次へ]** をクリックします。
5. **[証明書の新規作成]** を選択し、**[次へ]** をクリックします。

6. **[証明書の要求を作成して後で送信する]** を選択し、**[次へ]** をクリックします。
7. **[名前]** に、この証明書を後から識別するのに役立つ名前を入力します。**[証明書をエクスポート可能にする]** を選択して、他のサーバに証明書をエクスポートできるようにします。**[次へ]** をクリックします。
8. **[組織]** に、会社の正式名称を入力し、**[次へ]** をクリックします。
9. **[サブジェクト名]** に、プールの完全修飾ドメイン名を入力します。**[ローカルコンピュータ名をサブジェクト代替名に自動的に追加]** を選択し、**[次へ]** をクリックします。
10. **[国]**、**[都道府県]**、および **[市区町村]** を入力し、**[次へ]** をクリックします。
11. 新しい証明書要求 (CSR) の場所とファイル名を選択します。ファイルの拡張子は.txt にします。**[保存]** をクリックします。
12. 設定を確認し、証明書ウィザードを終了します。これで、前の手順で入力した場所に CSR ファイルが保存されます。
13. CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
14. AffirmTrust ポータルにログオンし、証明書の発行を行います。

## Microsoft Outlook Web Access (OWA)

1. インターネットサービスマネージャを開き、**[既定の Web サイト]** (または OWA コンポーネントをホストするサイト) を右クリックして、**[プロパティ]** をクリックします。
2. **[ディレクトリ セキュリティ]** タブで、**[サーバー証明書]** をクリックします。**[次へ]** をクリックします。
3. **[証明書の新規作成]** を選択し、**[次へ]** をクリックします。
4. **[証明書の要求を作成して後で送信する]** を選択し、**[次へ]** をクリックします。
5. **[名前]** ボックスに、この証明書を後から識別するのに役立つ名前を入力します。**[ビット長]** を 2048 に設定します。他のチェックボックスはオフのままにします。**[次へ]** をクリックします。
6. **[組織]** ボックスに、会社の正式名称を入力し、**[次へ]** をクリックします。
7. **[一般名]** ボックスに、Outlook Web Access Server の完全修飾ドメイン名 (例: mail.yourdomain.com) を入力します。**[次へ]** をクリックします。
8. 組織の所在地 (**[国/地域]**、**[都道府県]**、および **[市区町村]**) を入力します。**[次へ]** をクリックします。
9. CSR のファイル名と場所を選択します。ファイルを .txt ファイルとして保存します。**[次へ]** をクリックしてファイルを生成します。
10. CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
11. AffirmTrust ポータルにログオンし、証明書の発行を行います。