Microsoft Exchange 2010

サーバ証明書と中間証明書をダウンロードし、次の手順を実行します。

1. [スタート] メニューの **[ファイル名を指定して実行]** をクリックします。
2. 「mmc」と入力し、**[OK]** をクリックします。Microsoft 管理コンソール画面が表示されます。
3. コンソール画面で、**[ファイル]→[スナップインの追加と削除]** の順にクリックします。[スナップインの追加と削除] 画面が表示されます。
4. **[証明書]** を選択し、**[追加]** をクリックします。
5. **[コンピュータ 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]** を選択し、**[完了]** をクリックします。
7. **[OK]** をクリックします。
8. コンソール画面で、左側にある **[証明書]** フォルダを展開します。
9. **[中間証明機関]** を右クリックし、**[すべてのタスク] → [インポート]** の順にクリックします。
10. 証明書のインポートウィザードで、**[次へ]** をクリックします。
11. **[参照]** をクリックして中間証明書ファイルを探します。ファイル拡張子フィルタを **[PKCS #7 証明書 (*.spc;*.p7b)]** に変更し、中間証明書ファイルを選択して **[開く]** をクリックします。
12. **[次へ]** をクリックします。
13. **[証明書をすべて次のストアに配置する]** を選択します。
14. **[参照]** をクリックし、**[中間証明機関]** を選択して **[次へ]** をクリックします。
15. **[完了]** をクリックしてコンソール画面を閉じます。
16. **[スタート]** メニューで、**[プログラム] → [Microsoft Exchange 2010]** の順にクリックし、**[Exchange 管理コンソール]** をクリックします。
17. **[データベースを管理する]** をクリックし、**[サーバーの構成]** をクリックします。
18. **[Exchange 証明書]** で証明書を選択します。
19. 右側にある **[操作]** パネルで、**[保留中の要求の完了]** をクリックします。
20. **[参照]** をクリックして証明書ファイルを探します。ファイル拡張子は .cer ではなく、.txt または .crt です (すべてのファイルを検索してください)。
21. **[開く]** をクリックし、**[完了]** をクリックします。「ソース データが壊れているか、Base64 で正しくエンコードされていません。」というエラーが表示される場合は、[自己署名] を確認してください。「True」と表示されている場合は、キーを押してコンソールを更新します。更新しても「True」と表示される場合は、新しい CSR を作成してから証明書を再生成します。
22. **[完了]** をクリックします。
23. **[操作]** メニューの **[サービスの証明書への割り当て]** をクリックします。
24. サーバを選択し、**[次へ]** をクリックします。
25. 証明書に割り当てるサービスを選択し、**[次へ]** をクリックします。
26. **[割り当て]** をクリックし、**[完了]** をクリックします。

Microsoft Exchange 2007

サーバ証明書と中間証明書をダウンロードし、次の手順を実行します。

1. **[スタート]** メニューの **[ファイル名を指定して実行]** をクリックします。
2. 「mmc」と入力し、**[OK]** をクリックします。Microsoft 管理コンソール画面が表示されます。
3. **[ファイル]** メニューの **[スナップインの追加と削除]** をクリックします。
4. **[証明書]** を選択し、**[追加]** をクリックします。
5. **[コンピュータ 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]** を選択し、**[完了]** をクリックします。
7. **[OK]** をクリックして [スナップインの追加と削除] を閉じます。
8. コンソール画面で、**[証明書]** フォルダを展開します。
9. **[中間証明機関]** を右クリックし、**[すべてのタスク]** → **[インポート]** の順にクリックします。
10. 証明書のインポートウィザードで、**[次へ]** をクリックします。
11. **[参照]** をクリックして証明書ファイルを探します。右下隅のオプションでファイル拡張子フィルタを **[PKCS #7 証明書 (*.spc;*.p7b)]** に変更します。証明書ファイルを選択し、**[開く]** をクリックします。
12. **[次へ]** をクリックします。
13. **[証明書をすべて次のストアに配置する]** を選択します。
14. **[参照]** をクリックし、**[中間証明機関]** を選択して **[次へ]** をクリックします。
15. **[完了]** をクリックします。
16. **[スタート]** メニューの **[Microsoft Exchange Server 2007]** を選択し、**[Exchange 管理シェル]** をクリックします。
17. プロンプトで、次のコマンドを入力して証明書をインポートします。

    Import-ExchangeCertificate -Path ＜証明書ファイルのパス＞
18. 証明書のサムプリントをコピーします。
19. 次のコマンドを入力して証明書を有効にします。

    Enable-ExchangeCertificate -Thumbprint **paste_thumbprint_here** -Services “SMTP, IMAP, IIS”

    ※ paste_thumbprint_here は、前の手順でコピーしたサムプリントです。この証明書で保護するサービスを引用符で囲んで指定します。有効なサービス識別子は、SMTP、POP、IMAP、UM、および IIS です。使用していないサービスは有効にしないでください。

20. Exchange 管理シェル画面を閉じます。

Microsoft Exchange Server 2003

1. インターネット インフォメーション サービス マネージャー、またはインターネット インフォメーション サービスのスナップインを含むカスタム MMC を開きます。

2. 左側にあるツリー構造で、**[インターネット インフォメーション サービス]** を展開し、保留中の証明書要求を含む Web サイトを参照します。
3. サイト名を右クリックし、**[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]** タブを選択します。
5. **[セキュリティで保護された通信]** の **[サーバー証明書]** 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]** をクリックします。
7. **[保留中の要求を処理し、証明書をインストールする]** を選択し、**[次へ]** をクリックします。
8. 証明書応答ファイルの場所を入力し、**[次へ]** をクリックします。
9. 概要の画面で、正しい証明書を処理しているかどうかを確認し、**[次へ]** をクリックします。
10. 確認画面に表示される情報を確認し、**[次へ]** をクリックします。
11. インターネット サービス マネージャを使用して、Exchange 仮想ディレクトリのプロパティを開きます。
12. **[ディレクトリ セキュリティ]** タブを選択し、**[セキュリティで保護された通信]** の **[編集]** ボタンをクリックします。
13. [セキュリティで保護された通信] 画面で、**[保護されたチャンネル (SSL) を要求する]** チェックボックスまたは **[128 ビット暗号化を要求する]** チェックボックスをオンにします。[128 ビット暗号化を要求する] チェックボックスをオンにした場合は、128 ビット暗号化をサポートするブラウザからのみ OWA に接続できます。

ユーザが「http://www.yourdomain.com/exchange」と入力すると、「HTTP 403.4 - 許可されていません: インターネット インフォメーション サービスを使用するには SSL が必要です」という内容のエラーメッセージが表示されます。これは、SSL を要求するように OWA が設定されているためです。SSL では HTTPS プロトコルを使用するため、ユーザは「https://www.yourdomain.com/exchange」という URL を入力する必要があります。

Microsoft IIS 7.x

サーバ証明書と中間証明書をダウンロードし、次の手順を実行します。

1. **[スタート]** メニューの **[ファイル名を指定して実行]** をクリックします。
2. 「mmc」と入力し、**[OK]** をクリックします。Microsoft 管理コンソール画面が表示されます。
3. コンソール画面で、**[ファイル]** → **[スナップインの追加と削除]** をクリックします。[スナップインの追加と削除] 画面が表示されます。
4. **[証明書]** を選択し、**[追加]** をクリックします。
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]** を選択し、**[完了]** をクリックします。
7. **[OK]** をクリックします。
8. コンソール画面で、左側にある **[証明書]** フォルダを展開します。
9. **[中間証明機関]** を右クリックし、**[すべてのタスク]** → **[インポート]** をクリックします。
10. 証明書のインポートウィザードで、**[次へ]** をクリックします。

11. **[参照]** をクリックして中間証明書ファイルを探します。ファイル拡張子フィルタを **[PKCS #7 証明書 (*.spc;*.p7b)]** に変更し、中間証明書ファイルを選択して **[開く]** をクリックします。
12. **[次へ]** をクリックします。
13. **[証明書をすべて次のストアに配置する]** を選択します。
14. **[参照]** をクリックし、**[中間証明機関]** を選択して **[次へ]** をクリックします。
15. **[完了]** をクリックしてコンソール画面を閉じます。
16. **[スタート]** メニューで、**[管理ツール]** に移動し、**[インターネット サービス マネージャ]** をクリックします。
17. 左側にあるサーバ名をクリックします。
18. **[サーバー証明書]** をダブルクリックします。
19. 右側にある **[操作]** パネルで、**[証明書の要求の完了]** をクリックします。
20. 証明書ファイルの場所を指定します。ファイル拡張子は .cer ではなく、.txt または .crt です。
21. 証明書ファイルのフレンドリ名を入力し、**[OK]** をクリックします。
22. [インターネット インフォメーション サービス マネージャー] 画面で、証明書をインストールしたサーバの名前を選択します。
23. **[サイト]** で、SSL 証明書で保護するサイトを選択します。
24. 右側にある [操作] パネルで、**[バインド]** をクリックします。
25. **[追加]** をクリックします。
26. **[サイト バインドの追加]**で、**[種類]** を **[https]** に設定し、**[IP アドレス]** として、**[未使用の IP アドレスすべて]** またはサイトの IP アドレスを選択し、**[ポート]** を「**443**」に設定します。インストールした SSL 証明書を選択して **[OK]** をクリックします。
27. **[閉じる]** をクリックし、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。

Microsoft IIS 5.5 または 6.x

注意 ： サーバ証明書をインストールする手順は、OV 証明書と EV 証明書のどちらをインストールするかによって異なります。適切な手順に従ってください。

OV サーバ証明書をインストールする

1. 保護する Web サーバにサーバ証明書をダウンロードします。
2. コントロールパネルで、**[管理ツール]** → **[インターネット サービス マネージャ]** をクリックします。
3. **[既定の Web サイト]** または CSR が作成された Web サイトを右クリックし、**[プロパティ]** をクリックします。証明書は、CSR を作成した Web サイトにインストールする必要があります。
4. [ディレクトリ セキュリティ] パネルで、**[サーバー証明書]** をクリックします。証明書ウィザードが起動します。**[次へ]** をクリックします。
5. **[保留中の要求を処理し、証明書をインストールする]** を選択し、**[次へ]** をクリックします。
6. **[参照]** をクリックし、SSL 証明書 (your_domain.cer) を探して **[次へ]** をクリックします。
7. ウィザードの残りの手順に従います。

8. Internet Explorer 以外のブラウザで、セキュリティで保護された URL にアクセスして証明書をテストします。Internet Explorer では、中間証明書がなくてもサイトが信頼されていることを確認できます。他のブラウザでサイトが信頼されていないことが検出された場合は、中間証明書をインポートします (以下の手順を参照)。ISA 2004 または 2006 を使用していて、サーバから中間証明書が送信されていない場合は、サーバを再起動する必要があります。サーバがまだ古い証明書を使用している場合や、https がサーバによってロードされない場合は、サーバをシャットダウンして再起動しなければならない可能性があります。
9. サーバがクラッシュする場合に備えて、証明書と秘密鍵のバックアップコピーを作成します。

Windows Server 2000 または 2003 に EV 証明書をインストールする

1. 保護する Web サーバにサーバ証明書をダウンロードします。
2. 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。
3. CSR を作成した Web サイトを右クリックし、**[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]** タブを選択し、**[サーバー証明書]** ボタンをクリックします。IIS 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. **[保留中の要求を処理し、証明書をインストールする]** を選択します。**[次へ]** をクリックします。
6. **[参照]** をクリックし、EV 証明書ファイル (your_domain_name.cer) を探して **[次へ]** をクリックします。
7. ウィザードの残りの手順に従います。
8. IIS を再起動し、新しい証明書を使用して IIS が起動されるようにします。正しく起動されない場合は、サーバをシャットダウンしてから再起動してください。

中間証明書をインポートする

この手順は、ほとんどのインストール環境では必要ありません。証明書がサーバに正しくインストールされている場合、ブラウザには証明書に関する警告は表示されません。ただし、信頼されていない会社から証明書が発行されたことを示す警告がクライアントに表示される場合は、次の手順に従って問題を修正してください。

1. 中間証明書 (.crt) をダウンロードしてサーバに保存します。
2. 証明書をダブルクリックします。[証明書] ダイアログボックスが表示されます。
3. **[全般]** タブの一番下にある **[証明書のインストール]** をクリックします。証明書のインポートウィザードが起動します。**[次へ]** をクリックします。
4. **[証明書をすべて次のストアに配置する]** を選択し、**[参照]** をクリックします。
5. **[物理ストアを表示する]** チェックボックスをオンにして、**[中間証明機関]** フォルダを展開し、**[ローカル コンピュータ]** フォルダを選択して、**[OK]** をクリックします。**[次へ]** をクリックし、**[完了]** をクリックします。
6. AffirmTrust_Commercial.crt で始まる中間証明書について上記の手順を実行し、その後サーバに適した中間証明書について上記手順を実行します。この中間証明書はサーバ証明書の種類に応じて、AffirmTrust_Certificate_Authority_OV1.crt 或いは AffrimTrust_Certificate_Authority_EV1.crt のいずれかになります。サーバの再起動が必要な場合があります。

複数の IIS サイトにユニファイドコミュニケーション証明書またはワイルドカード証明書をインストールする

複数の IIS Web サイトでワイルドカード証明書またはユニファイドコミュニケーション証明書を使用している場合は、証明書を使用する各サイトを割り当てるのではなく、SSL ホストヘッダを設定します。証明書を使用する各 IIS サイトの名前をユニファイドコミュニケーション証明書またはワイルドカード証明書に含める必要があります。

Microsoft IIS 4.x

1. AffirmTrust ポータルからルート証明書ファイル、中間証明書ファイル、およびサーバ証明書ファイルを取得します。
2. キーマネージャを開きます。
3. www ディレクトリの **[IIS プライマリ SSL 証明書]** キーをクリックし、**[キー証明書のインストール]** をクリックします。
4. パスワードを入力します。
5. バインドを要求されたら、IP アドレスとポート番号を追加します。Web サーバに他の IIS SSL 証明書がインストールされていない場合は、**[未割り当てすべて]** を選択できます。**注意 :**複数の証明書を同じ Web サーバにインストールする場合、SSL ではホストヘッダがサポートされないため、証明書ごとに個別の IP アドレスが必要になります。
6. **[コンピュータ]** → **[今すぐ変更を反映]** をクリックするか、キーマネージャを終了して変更を反映するかどうかの確認を求められたら **[はい]** をクリックします。これで、新しい IIS プライマリ SSL サーバ証明書が正常にインストールされました。
7. キーマネージャでキーをバックアップするには、**[キー]** → **[キーのエクスポート]** → **[バックアップ ファイル]** をクリックします。ハードドライブおよび別のサーバにバックアップファイルを保存します。
8. IIS 4 を実行しているサーバを再起動します。
9. Service Pack 3 を実行している場合:

   中間証明書とルート証明書を Internet Explorer にインストールします。そのためには、各証明書を開き、**[証明書のインストール]** をクリックします。次に、この IIS CA のバッチファイルを使用して、すべてのルート証明書を Internet Explorer から IIS 証明書ストアに転送できます。

   Service Pack 4 以降を実行している場合:

   ルート証明書をダブルクリックしてインストールウィザードを開き、**[証明書をすべて次のストアに配置する]** を選択し、**[参照]** をクリックします。**[物理ストアを表示する]** → **[信頼されたルート証明機関]** → **[ローカル コンピュータ]** をクリックします。**[OK]**、**[次へ]**、**[完了]** の順にクリックします。中間証明書についても上記の手順を繰り返しますが、[信頼されたルート証明機関] ではなく **[中間証明機関]** を使用してください。

10. サーバを再起動します。IIS を再起動しても SSL 証明書は更新されません。証明書を更新するには、サーバを再起動する必要があります。

Microsoft Office Communications Server (OCS) 2007

1. CSR を生成した Office Communications Server にサーバ証明書ファイルをダウンロードします。
2. サーバで、**[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。
3. Enterprise Edition Server に移動します。
4. CSR を生成した Office Communications Server を右クリックし、**[証明書]** をクリックします。**[次へ]** をクリックします。
5. **[保留中の要求を処理し、証明書をインストールする]** を選択します。
6. サーバ証明書ファイルを参照し、**[次へ]** をクリックします。これで、証明書がインストールされます。証明書を確認して証明書ウィザードを終了できます。

Microsoft Outlook Web Access (OWA)

1. 保護するサーバのデスクトップにサーバ証明書をコピーします。
2. [管理ツール] からインターネット サービス マネージャを開きます。**[既定の Web サイト]** または CSR が作成された Web サイトを右クリックし、**[プロパティ]** をクリックします。証明書は、CSR を作成した Web サイトに作成する必要があります。
3. [ディレクトリ セキュリティ] パネルに移動します。**[サーバー証明書]** ボタンをクリックします。証明書ウィザードが起動します。**[次へ]** をクリックします。
4. **[保留中の要求を処理し、証明書をインストールする]** を選択します。**[次へ]** をクリックします。
5. SSL 証明書を参照し、**[次へ]** をクリックします。ウィザードの残りの手順に従って、ウィザードを終了します。これで、証明書のインストールは完了です。
6. (オプション) 128 ビットで暗号化された接続のみ受け入れるように OWA サーバを設定できます。この設定は必須ではありませんが、セキュリティで保護された接続をサーバに適用する場合に役立ちます。
    1. インターネット サービス マネージャで、Exchange 仮想ディレクトリのプロパティを開きます。
    2. [ディレクトリ セキュリティ] タブで、[セキュリティで保護された通信] 領域の [編集] ボタンをクリックします。[セキュリティで保護された通信] パネルが表示されます。
    3. **[保護されたチャンネル (SSL) を要求する]** オプションを選択します。40 ビットで暗号化された古いブラウザと接続できないようにする場合は、**[128 ビット暗号化を要求する]** を選択します。証明書は 2048 ビット暗号化まで対応しますが、証明書はスケーラブルであるため、40 ビットと 56 ビットの接続が許可されます (ユーザが指定した場合)。また、これにより HTTP 接続は無効になり、128 ビットの HTTPS 接続だけが許可されます。
    4. HTTPS 接続を受け入れるようにファイアウォールが設定されていることを確認します (初期設定はポート 443 です)。