InterMail Post.Office 4.2.1J 補遺マニュアル

マニュアル・バージョン4.2.1

2011年11月

Open
Technologies

目次

1. 新機能について

InterMail Post.Office 4.2.1J では、次の機能が追加されました。本マニュアルでは、この機能と設定方法に説明します。

- SSL 機能

2. SSL 機能について

2.1. SSL 通信がサポートされているプロトコル

Post.Office が、サポートしている SSL 通信可能なプロトコルとデフォルトのポート番号は次のとおりです。

対応プロトコル	ポート番号（デフォルト）	備考
SMTP	25 番	STARTTLS 利用
SMTPS	485 番	
POP3S	995 番	
IMAP4S	993 番	
HTTPS	443 番	Post.Office 管理画面

※　Post.Office サーバから外部に送信されるメールについては、SSL 通信を行うことはできません。
※　POP3 プロトコルの拡張コマンドである「STLS」には、対応しておりません。POP3S をご利用ください。

2.2. SSL 機能の設定

2.2.1. 自己署名の証明書と CA 発行のサーバ証明書について

Post.Office の SSL 機能では、自己署名のサーバ証明書、あるいは CA（Certificate Authority：認証局）が発行したサーバ証明書を設定することができます。

自己署名のサーバ証明書は、認証局によって認証されている証明書ではありませんので、メーラーやブラウザから SSL 接続をした場合、信頼できる証明書ではない等、その旨の注意が表示されます。（ご利用になっているアプリケーションによっては、SSL 接続時に証明書のエラーになることがありますが、証明書を承認する／例外として追加する、あるいは閲覧を続行することでご利用いただくことができます）

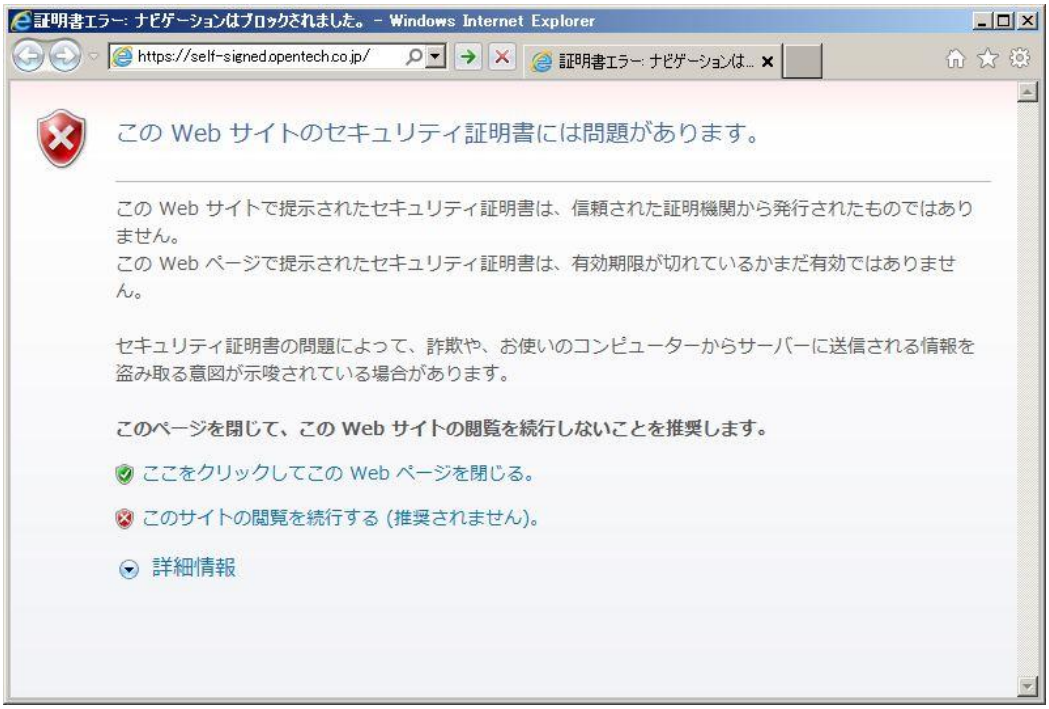

図１：自己署名のサーバ証明書を使っているサーバに接続した場合（IE）

CA 発行のサーバ証明書を設定する場合は、まず、証明書を発行してもらうための認証局を決めていただき、その認証局の手続きに従って、認証されたサーバ証明書を取得します。

2.2.2. CA 発行の証明書の取得手続きから設定までの流れ

CA 発行の証明書の手続きから Post.Office への設定までの概要は、次のとおりです。

- 秘密鍵と CA 申請用サーバ証明書（CSR：Certificate Signing Request）の生成（Post.Office にて行います）
  秘密鍵は、自動的に生成されます。
  ↓
- CA 申請用サーバ証明書の取得（Post.Office にて行います）
  ↓
- 認証局にて、CA 申請用サーバ証明書を提示（認証局にて手続きします）
  ↓
- 認証局が承認した CA 発行のサーバ証明書を取得（認証局より発行されます）
  ご契約される認証局によっては、中間 CA ルート証明書も必要になりますので、一緒に取得しておきます。
  ↓
- CA 発行のサーバ証明書の設定（Post.Office にて行います）
  中間 CA ルート証明書が必要な場合は、その証明書も設定します。

詳細は、ご契約される認証局のサーバ証明書の発行手順をご覧ください。

2.2.3. SSL 機能の設定方法

「SSL 機能の設定」画面は、次のようになっています。

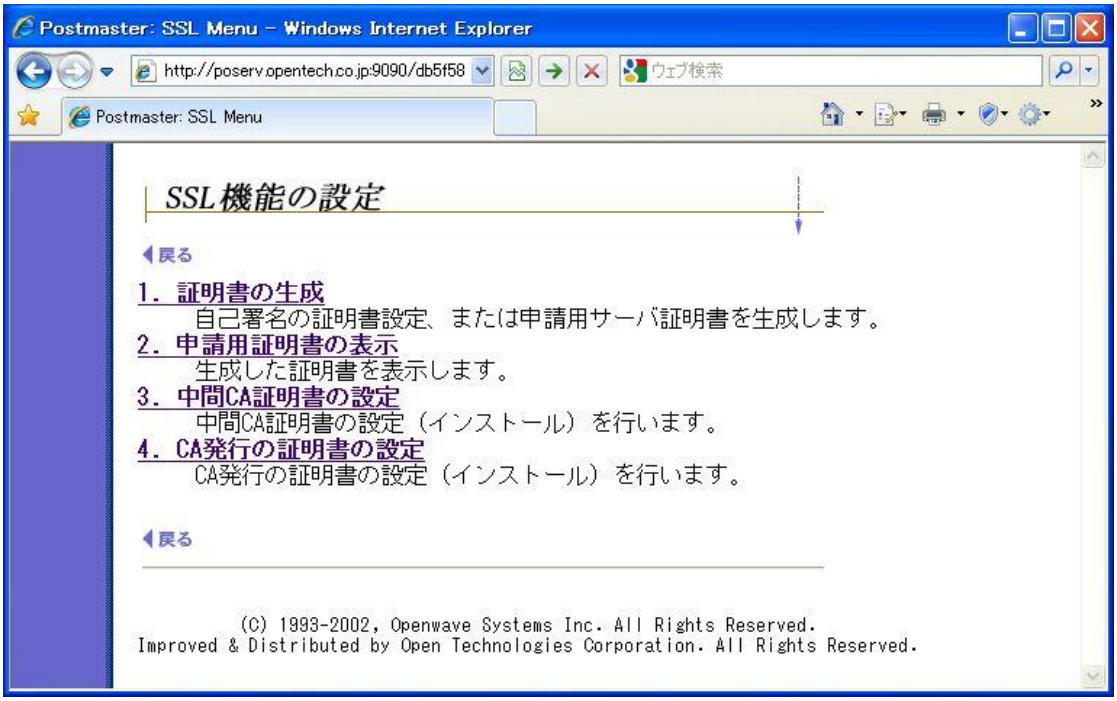

図２：SSL 機能の設定画面

画面に表示されている項目の順番どおりに、設定を行なっていきます。

※　自己署名の証明書を利用する場合は、「１．証明書の生成」だけを行います。

1. 証明書の生成

設定画面は、次のとおりです。

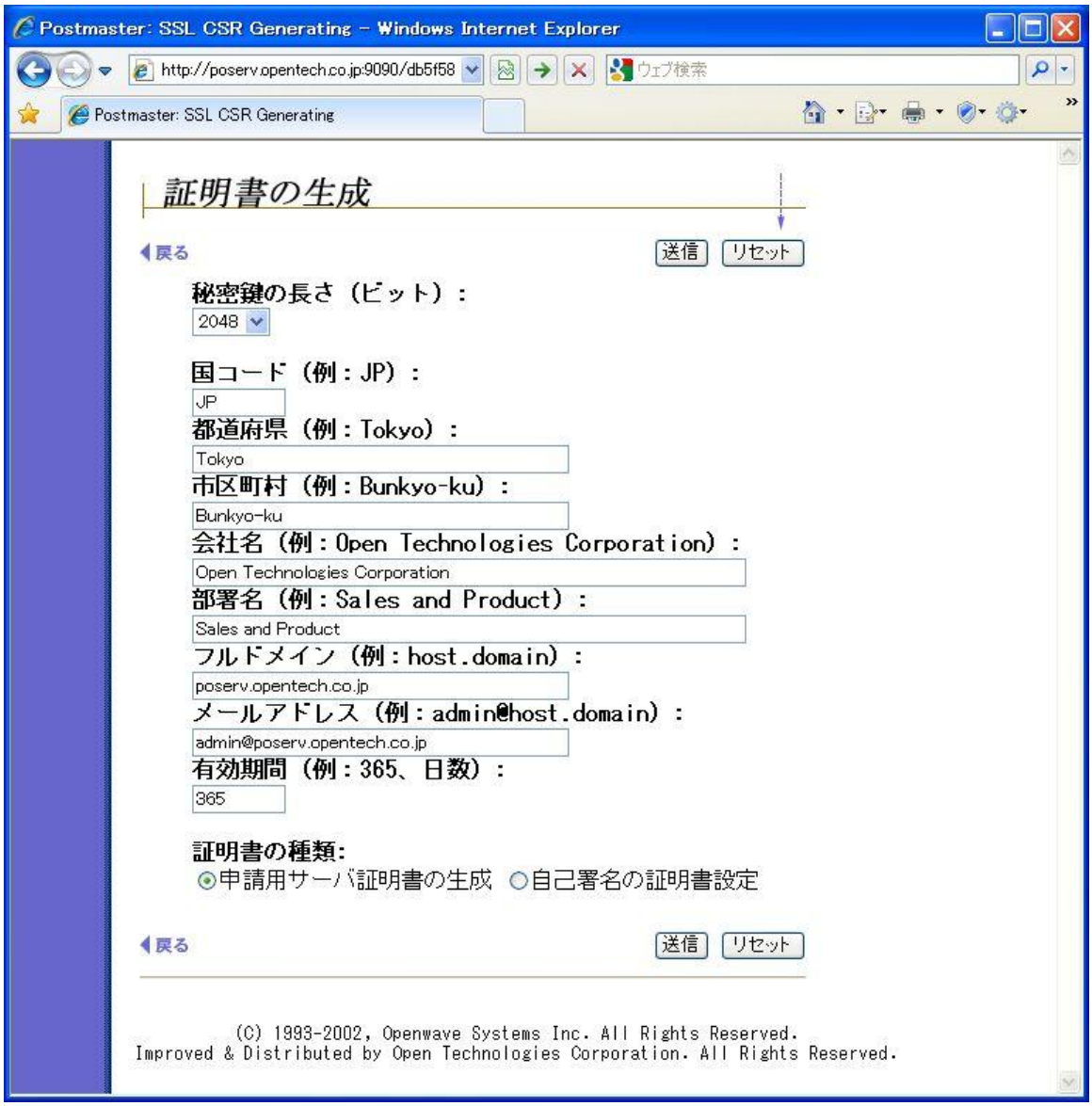

図３：証明書の生成

秘密鍵と証明書を生成するために必要な項目に入力し、［送信］ボタンをクリックします。入力可能な文字は半角英数文字になりますが、特殊文字を使った場合、認証局への申請用の証明書（CSR）の提示時にエラーにされてしまうことがあるため、都道府県、市区町村、会社名、部署名には、特殊文字をご利用にならないようお願いいたします。

項目への入力が終わりましたら、必要な「証明書の種類：」を選択していただき、［送信］ボタンをクリックします。

※　「証明書の種類：」にて、「自己署名の証明書」を選択（自己署名のサーバ証明書をご利用）した場合は、［送信］ボタンをクリックして、設定作業は終了になります。（この後の項目２～４を行う必要はありません）

2. 申請用証明書の表示

項目１にて生成した申請用の証明書（CSR）を、コピー&ペーストするために表示させます。

図４：申請用の証明書（CSR）の表示

テキストボックス中の文字列「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までを含めて選択＋コピーし、認証局での申請手続きの中でペーストします。

3. 中間 CA 証明書の設定

認証局によっては、発行されたサーバ証明書の他に、中間 CA ルート証明書が必要になる場合があります。
中間 CA ルート証明書は、認証局の方で準備していますので、その取得手順に従って入手しておきます。

入手した中間 CA ルート証明書を、ノートパッド等を利用して、テキスト文字列として表示させた後、文字列「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」までを含めて選択＋コピーして、「中間 CA 証明書の設定（インストール）:」のテキストボックスに貼り付け、[送信] ボタンをクリックします。

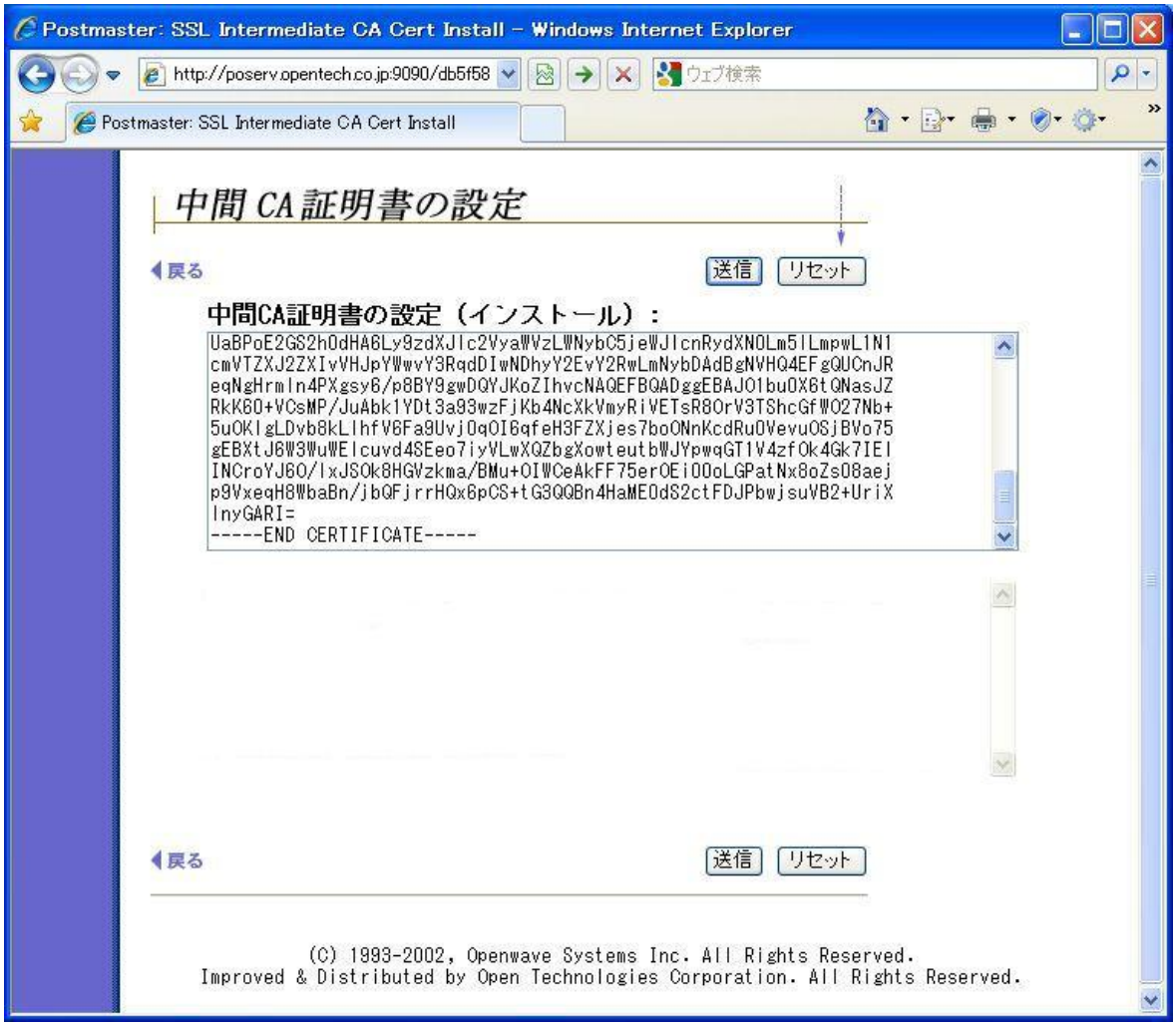

図５：中間 CA ルート証明書の設定

4. CA 発行の証明書の設定

認証局より発行されたサーバ証明書をノートパッド等を利用して、テキスト文字列として表示させた後、文字列「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」までを含めて選択＋コピーして、「CA 発行の証明書の設定（インストール）：」のテキストボックスに貼り付け、［送信］ボタンをクリックします。

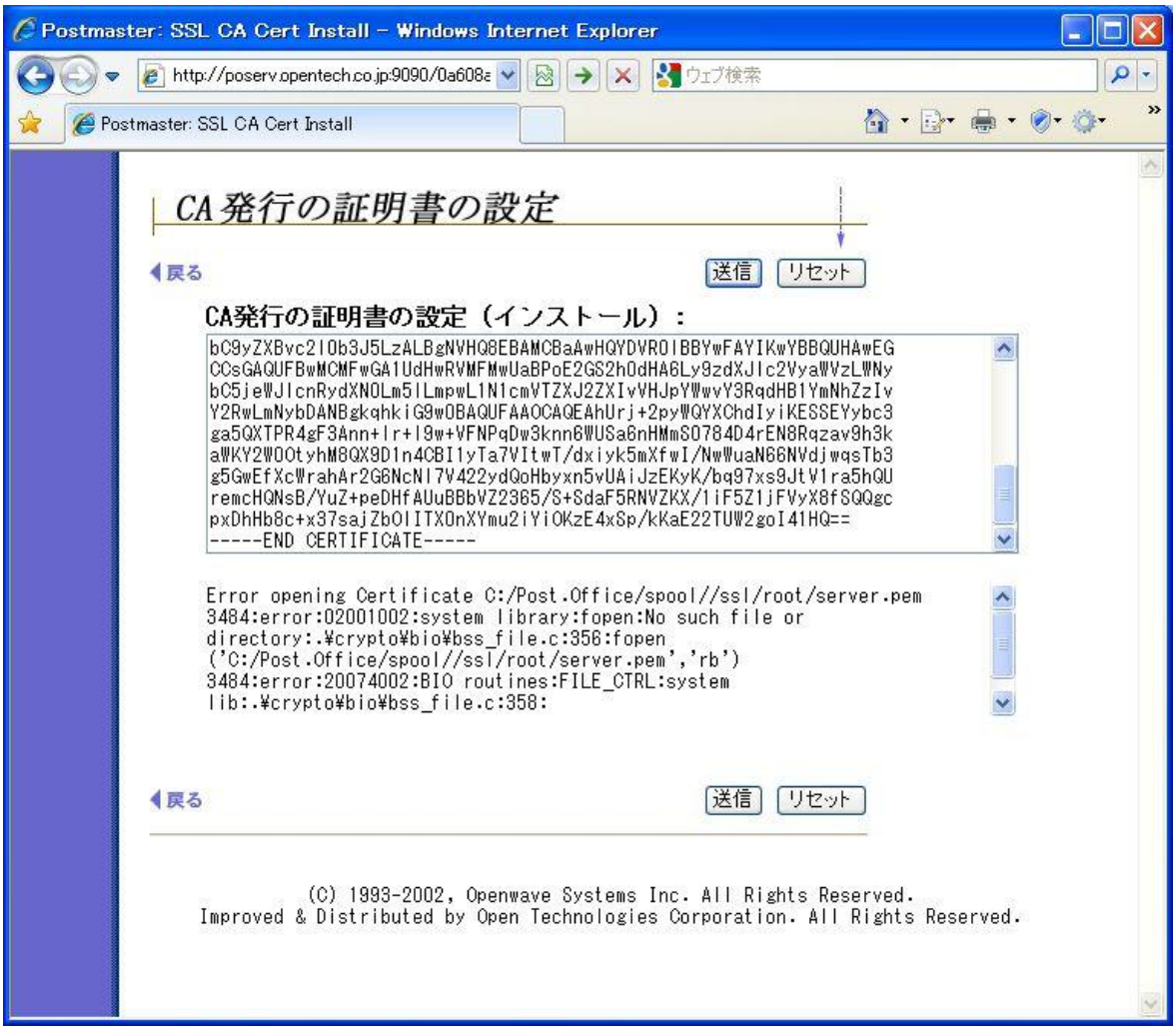

図６：CA 発行のサーバ証明書の設定

※ テキストボックスの下に「Error opening Certificate …」というエラーメッセージが表示されていますが、最初に SSL 設定を行う場合は、サーバ証明書等の設定ファイルが存在していないためエラーとなって表示されています。この設定操作を行うことで、テキストボックスに貼り付けた証明書がインストールされると、エラー表示は無くなります。

2.3. その他

2.3.4. SSL 機能のために追加されたパラメータ

SSL 機能に関連したパラメータは、Windows のレジストリキーに設定されています。次のとおりです。

- SSL 通信のポート番号を変更する場合
  - IMAP4S プロトコル
    - HKEY_LOCAL_MACHINE¥SOFTWARE¥Software.com¥Post.Office¥IMAPS-Server¥Config キー
    - Socket 値
      ポート番号を設定
  - POP3S プロトコル
    - HKEY_LOCAL_MACHINE¥SOFTWARE¥Software.com¥Post.Office¥POP3S-Server¥Config キー
    - Socket 値
      ポート番号を設定
  - SMTPS プロトコル
    - HKEY_LOCAL_MACHINE¥SOFTWARE¥Software.com¥Post.Office¥SMTPS-Accept¥Config キー
    - Socket 値
      ポート番号を設定
  - HTTPS プロトコル（Post.Office 管理画面）
    HKEY_LOCAL_MACHINE¥SOFTWARE¥Software.com¥Post.Office¥WWWS-Server¥Config キー
    - Socket 値
      ポート番号を設定

- SSL 機能のフラグ
  SSL 通信を機能させるためのフラグです。
  - HKEY_LOCAL_MACHINE¥SOFTWARE¥Software.com¥Post.Office¥SSL-Info¥Config キー
  - SSL-Enabled 値
    「yes」か「no」を設定

- SMTP プロトコルの「STARTTLS」コマンド対応のフラグ
  SMTP プロトコルにて「STARTTLS」コマンドを機能させるためのフラグです。
  - HKEY_LOCAL_MACHINE¥SOFTWARE¥Software.com¥Post.Office¥SMTP-Accept¥Config キー
  - AllowSTARTTLS 値
    「yes」か「no」を設定

※ Windows Server 2008 R2 をご利用の場合は、「HKEY_LOCAL_MACHINE¥SOFTWARE¥Software.com」の箇所を「HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Software.com」に置き換えてキーを選択してください。

2.3.5. ログ出力フォーマットについて

Post.Office のログ出力フォーマットの中で、<モジュール名>を表記している箇所が、

<date-time>:<モジュール名>:……

次の文字列となります。

- IMAP4S-Server
- POP3S-Server
- SMTPS-Accept
- WWWS-Server

※　STARTTLS コマンドを使った SMTP アクセスの場合は、「SMTP-Accept」になります。

2.4. ご利用上の注意

- Post.Office サーバから外部に送信されるメール（SMTP-Delier モジュールが処理するメール）については、SSL 通信を行うことはできません。
- POP3 プロトコルの拡張コマンドである「STLS」には、対応しておりません。メーラーの設定では、POP3S をご利用ください。
- 自己署名のサーバ証明書を利用する場合は、「１．証明書の生成」だけを行います。項目２～４を行う必要はありません。
- 自己署名のサーバ証明書から、CA 発行のサーバ証明書に切り替える場合は、「１．証明書の生成」から設定をやり直してください。

(C) 1993-2002, Openwave Systems Inc. All Rights Reserved.
(C) 2002-2009 Open Technologies Corporation. All Rights Reserved.
Improved & Distributed by Open Technologies Corporation.

3. ライセンスおよび商標について

■ OpenSSL ソフトウェアについて

本製品には、弊社がその著作権者とのライセンス契約に基づき使用しているソフトウェアである「OpenSSL（「Original SSLeay」と称するライブラリーを含む）」を利用しています。

OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
   The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]