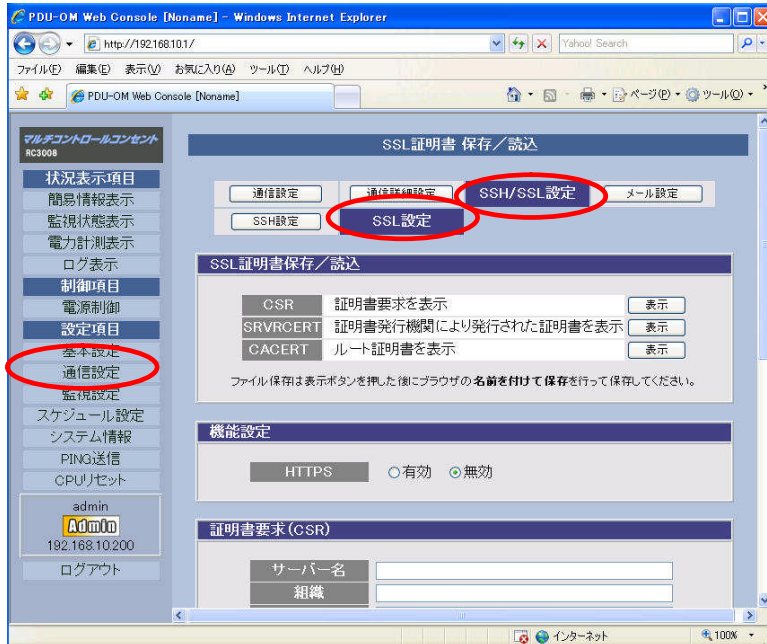


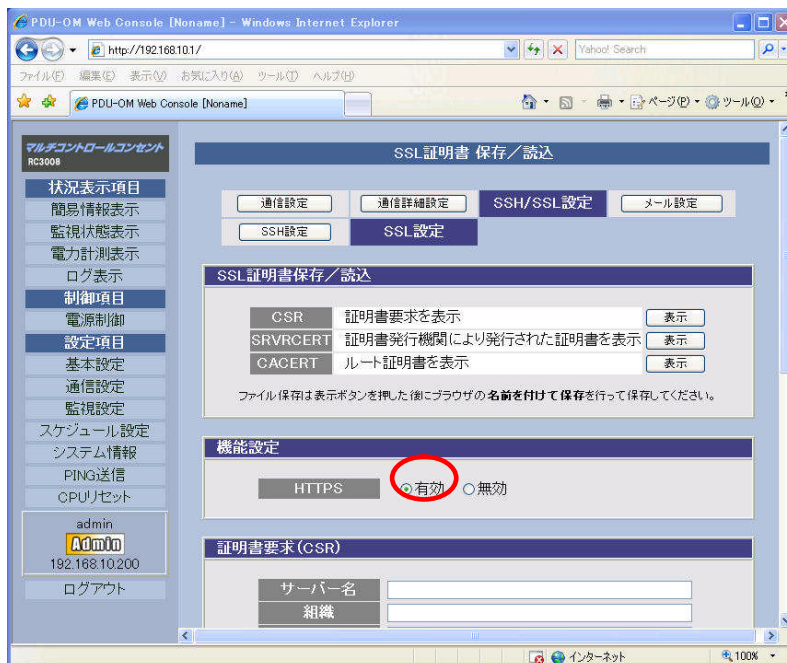
【RC3008 HTTPS 使用時の設定方法について】

Internet Explorer7 または 8 を使用し、HTTPS で RC3008 にアクセスする場合、最初にルート証明書をインストールする必要があります。以下の手順を行ってください。

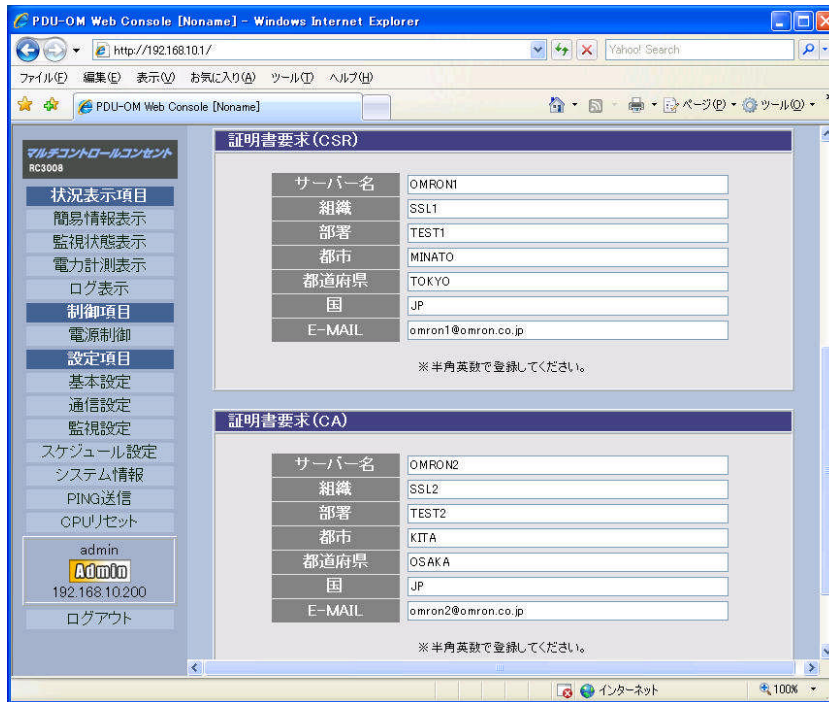
1. ブラウザで RC3008 の設定画面を開き、左側メニューの[通信設定]をクリック、[SSH/SSL 設定]の画面を開き、[SSL 設定]をクリックします。[SSL 証明書 保存/読込]画面が開きます。



2. [機能設定]の[HTTPS]の[有効]をチェックします。



3. [証明書要求(CSR)]と[証明書要求(CA)]に必要な情報を入力します。



サーバー名 : サーバ名を入力します。63 文字以内の半角英数文字で任意のサーバ名を入力します。

組織 : 組織名を入力します。63 文字以内の半角英数文字で任意の名称を入力します。

部署 : 部署名を入力します。63 文字以内の半角英数文字で任意の名称を入力します。

都市 : 都市名を入力します。63 文字以内の半角英数文字で任意の名称を入力します。

都道府県 : 都道府県名を入力します。63 文字以内の半角英数文字で任意の名称を入力します。

国 : 国名を 2 桁のコードで入力します。あらかじめ「JP」が入力されているので変更する必要はありません。

E-MAIL : メールアドレスを入力します。63 文字以内の半角英数文字で任意のメールアドレスを入力します。

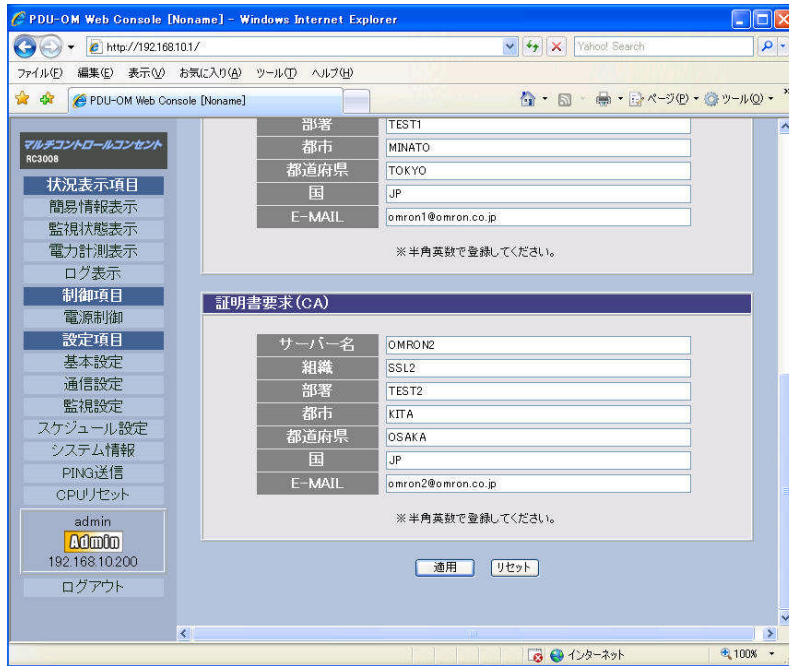
【入力時の留意点】

① CSR と CA のサーバー名は同じものにしないでください。同じものにした場合は、HTTPS 接続ができません。

② CSR のサーバー名と RC3008 の IP アドレスが一致しない場合は、ブラウザで[証明書のエラー]が表示される場合がありますが、このままご使用いただいても問題はありません。

DNS サーバを使用している環境にて[サーバー名]から RC3008 の IP アドレスを参照できる場合は、上記事象は発生しません。

4. [適用]ボタンをクリックします。これで設定に必要な情報が RC3008 に書き込まれました。



5. 設定した情報を使用して、証明書を作成します。証明書は、コマンドを実行して作成します。

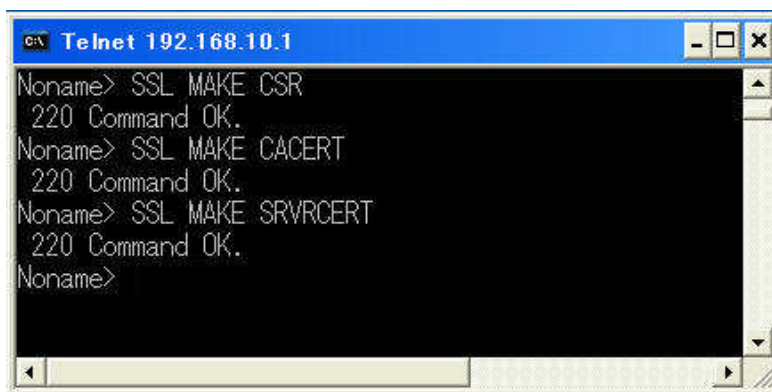
RC3008 と PC を COM で接続、コマンドプロンプトやターミナルソフトで RC3008 に以下の 3 つのコマンドを順番に実行してください。

```
SSL MAKE CSR  
SSL MAKE CACERT  
SSL MAKE SRVCERT
```

【コマンド実行時の留意点】

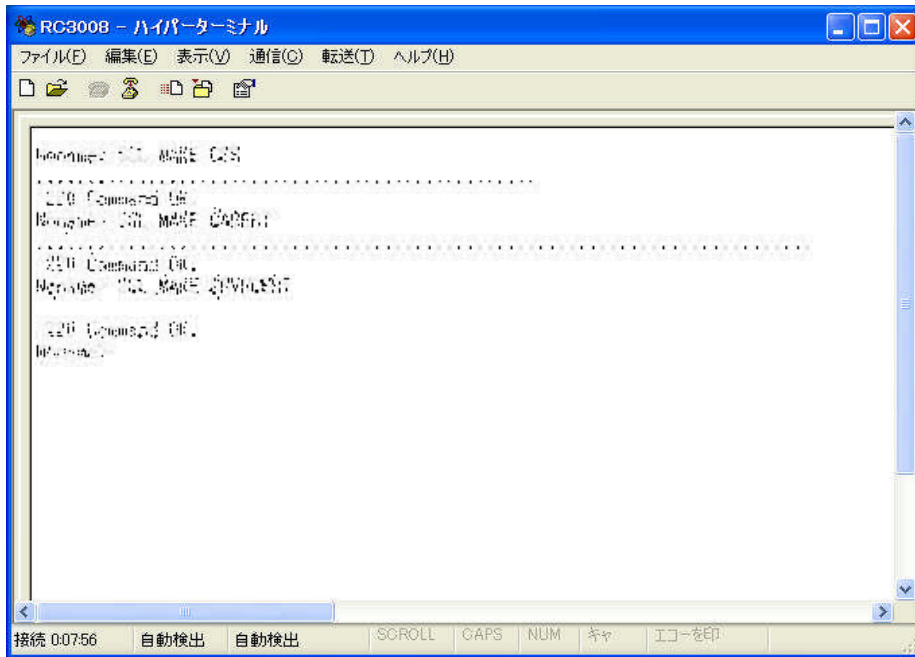
「SSL MAKE CSR」および「SSL MAKE CACERT」の実行には数分の時間がかかります。「220 Command OK.」と表示されるまで、そのままお待ちください。

(1) Telnet 接続の場合

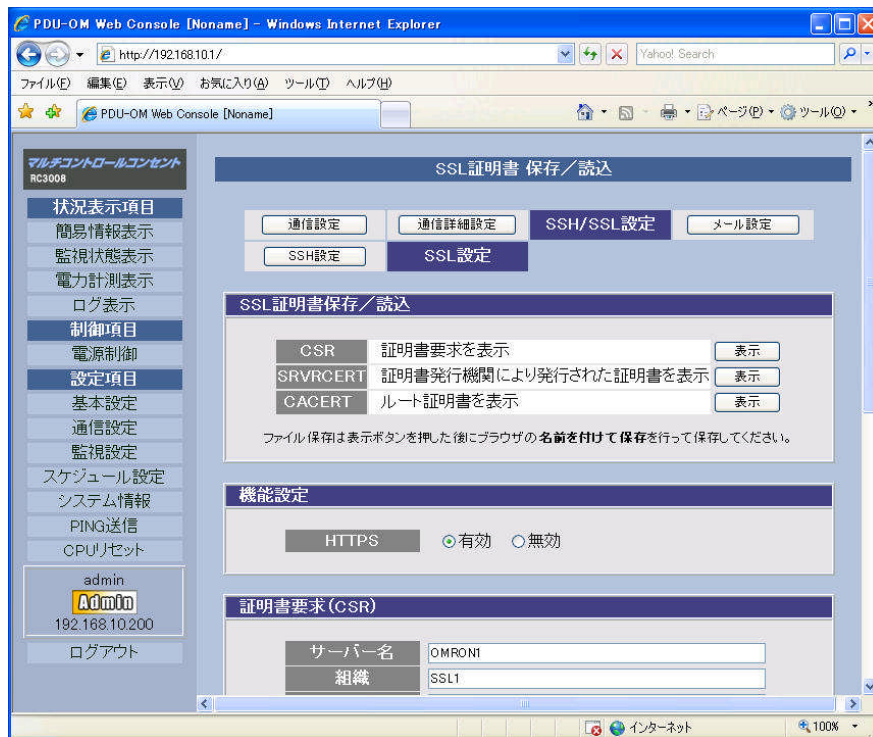


(2) COM 接続の場合

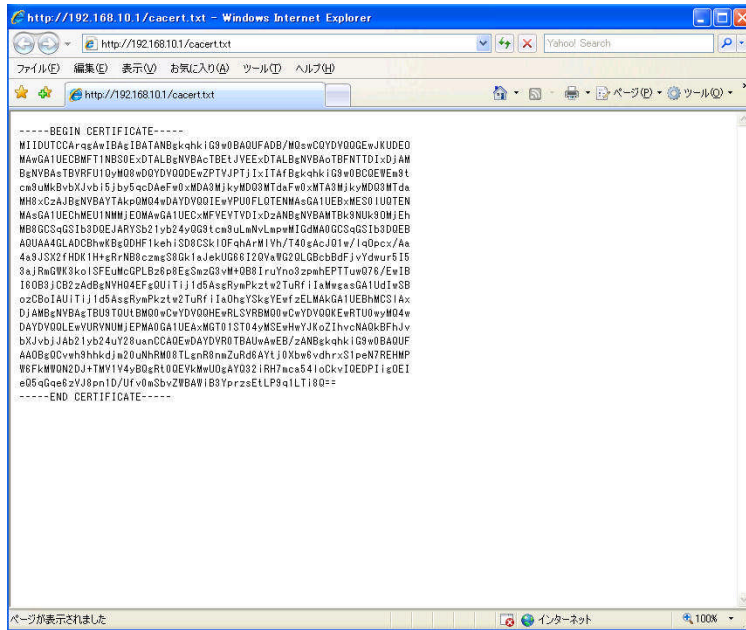
COM 接続の場合は、コマンド実行の進捗状況が表示されます。



6. ルート証明書をファイルに保存します。[CACERT]の[表示]をクリックしてください。

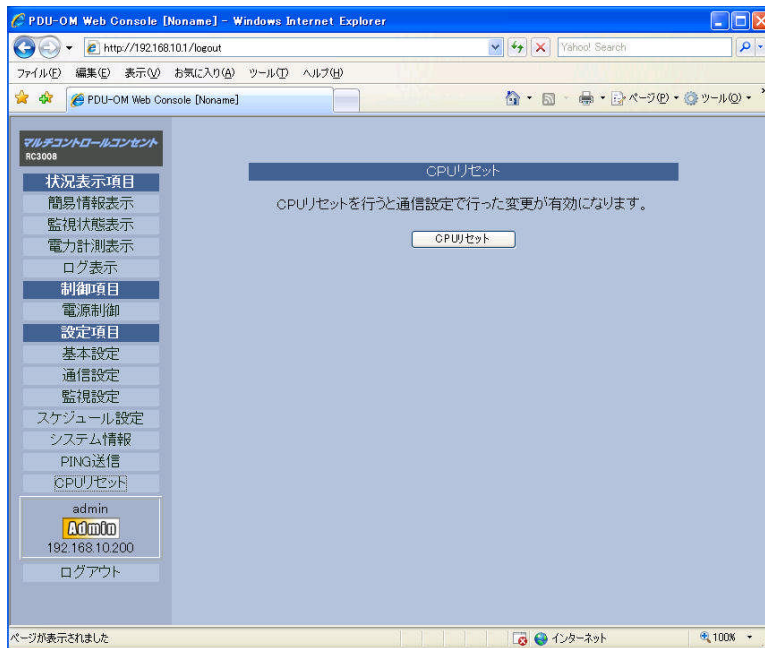


7. ルート証明書が表示されますので、ブラウザの[ファイル] ⇒ [名前を付けて保存]で任意の場所に保存してください。



8. RC3008 の CPU リセットを実行してください。

左側メニューの[CPU リセット]を繰り返クリックすると[CPU リセット]画面が表示されますので[CPU リセット]をクリックします。



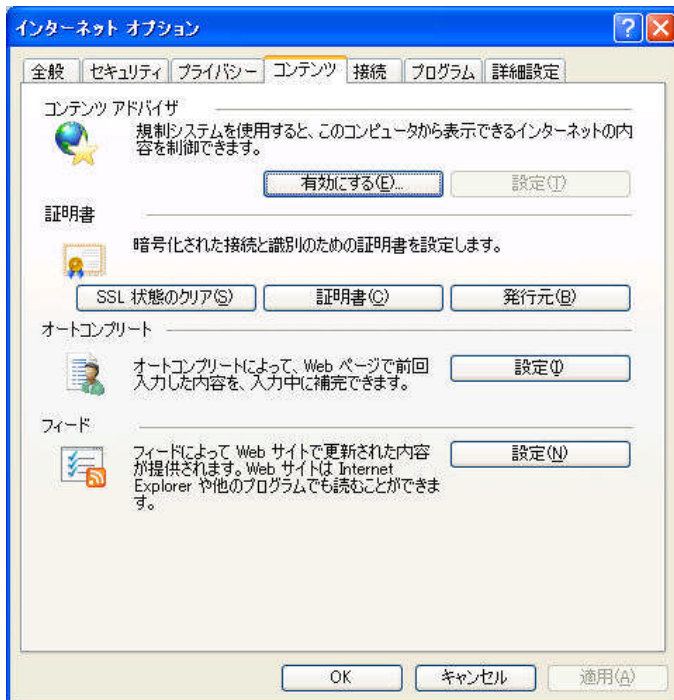
9. 確認のダイアログが表示されますので、[OK]をクリックしてください。RC3008 が再起動します。



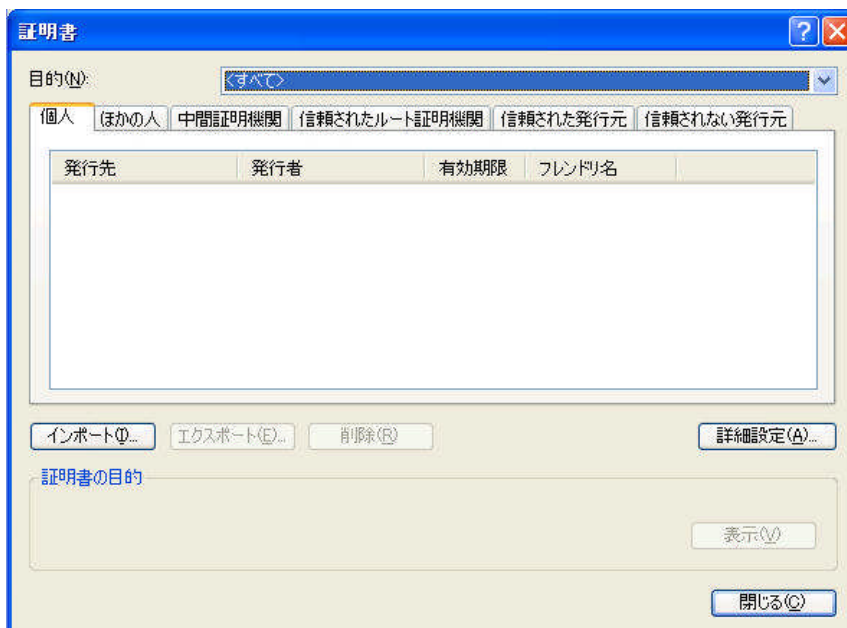
10. ブラウザへの証明書のインストール

ブラウザのメニューの[ツール] ⇒ [インターネットオプション]を選択してください。

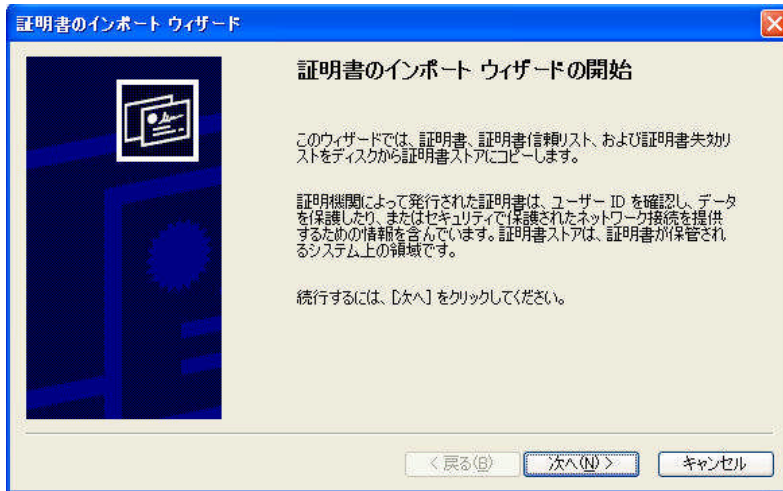
[インターネットオプション]の画面が表示されますので、[コンテンツ]タブにある[証明書]をクリックします。



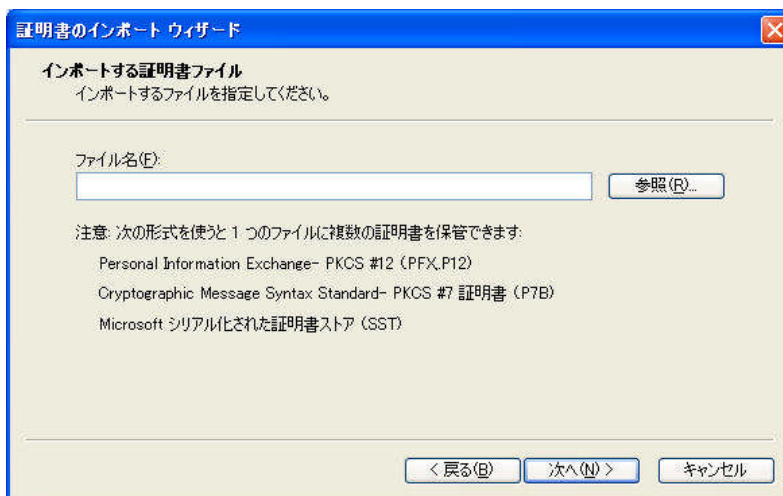
11. [証明書]の画面が表示されますので、[インポート]をクリックします。



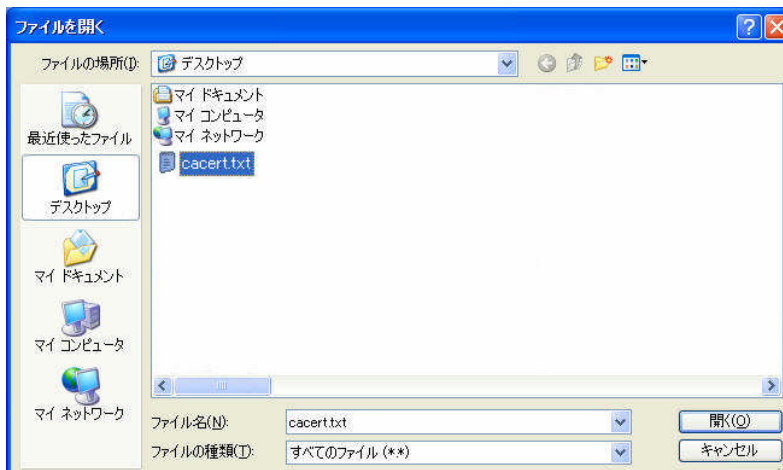
12. [証明書のインポートウィザード]が始まります。[次へ]をクリックしてください。



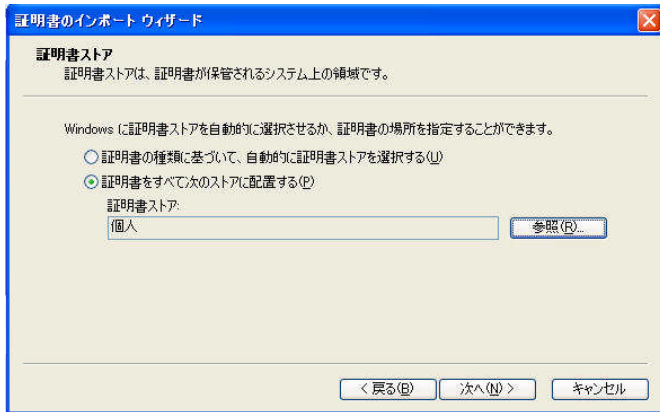
13. インポートの画面が表示されます。[参照]をクリックしてください。



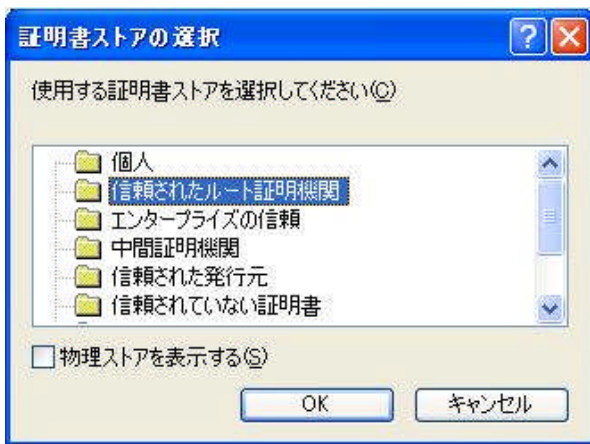
14. [ファイルを開く]のダイアログが表示されますので、8. で保存したルート証明書を選択してください。



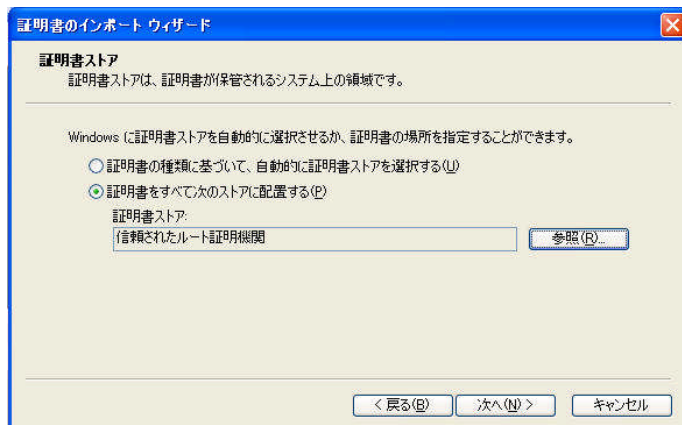
15. [証明書ストア]の画面が表示されるので、[証明書をすべて次のストアに配置する]をチェックしてから[参照]をクリックしてください。



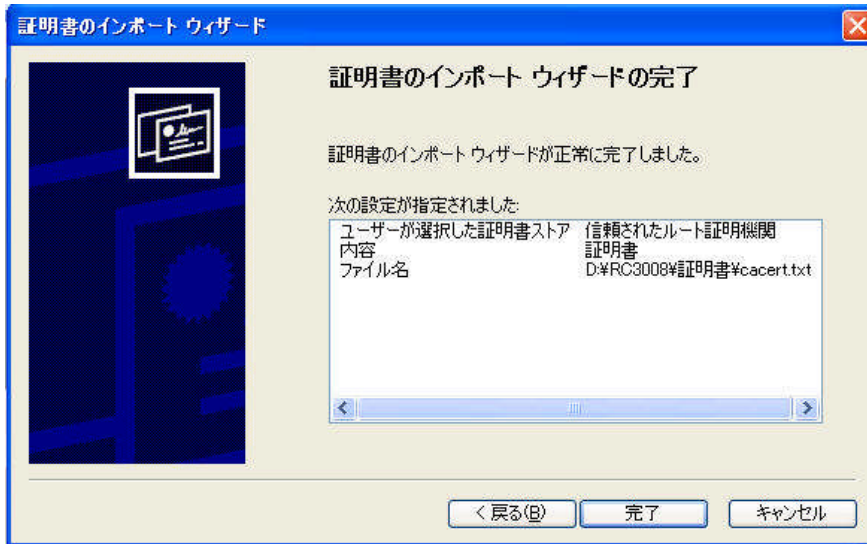
16. [証明書ストアの選択]が表示されるので、[信頼されたルート証明期間]を選択して[OK]をクリックしてください。



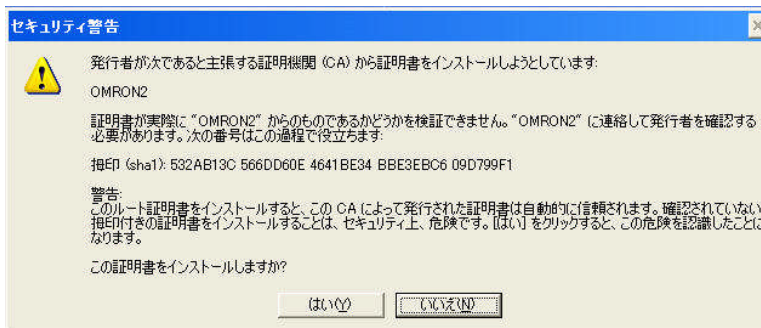
17. [証明書ストア]画面に戻ったら、[次へ]をクリックしてください。



18. [証明書のインポートウィザードの完了]画面が表示されたら、[完了]をクリックしてください。



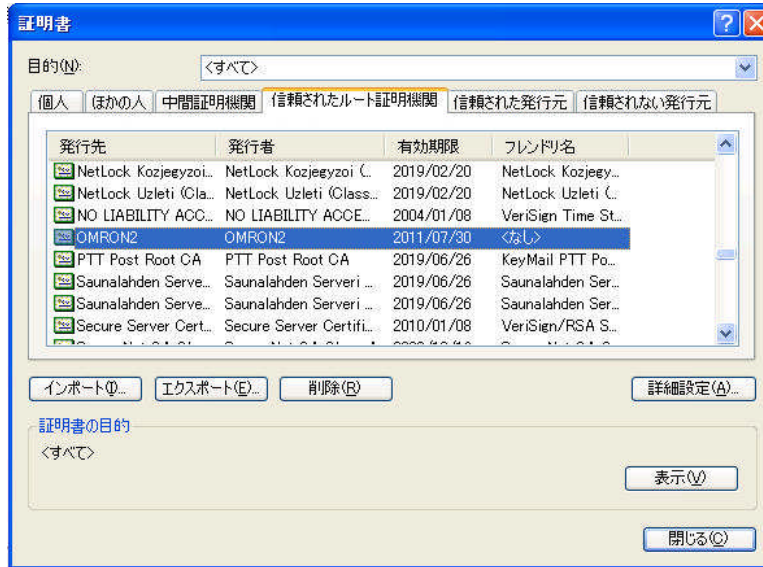
19. 下記のセキュリティ警告のポップアップ画面が表示されます。[はい]をクリックしてください。



20. 下記のポップアップ画面が表示されたらインポートは完了です。[OK]をクリックしてください。



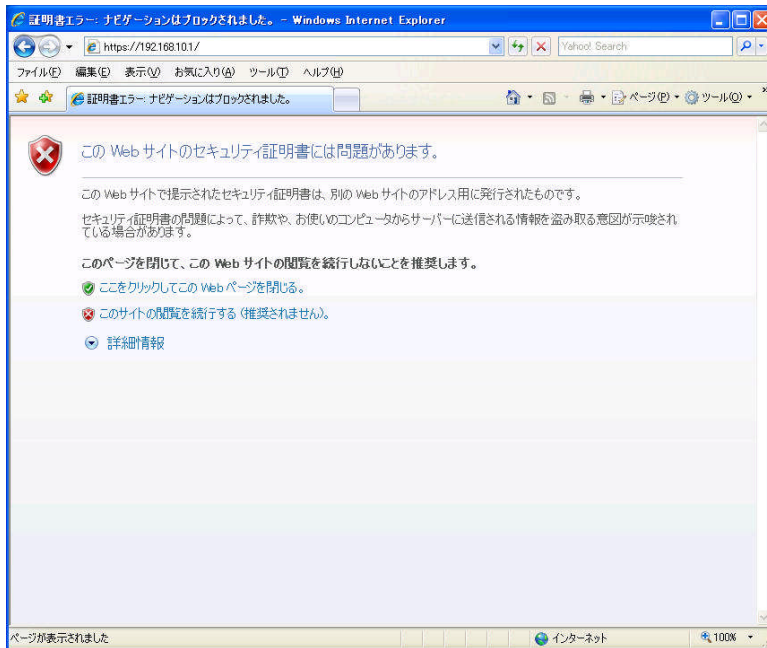
21. 正しくインポートできているかどうかを確認するためには、[証明書]画面の[信頼されたルート証明機関]タブをクリックしてください。[発行先]と[発行者]に、4. で入力した[証明書要求(CA)]のサーバ名が表示されていたら HTTPS で RC3008 にアクセス可能となります。



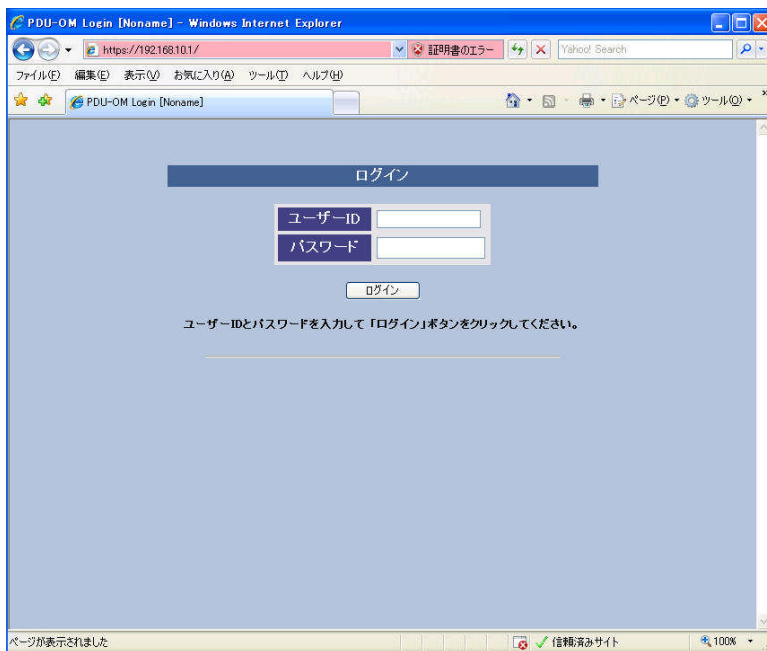
22. ブラウザで URL アドレスに「https://192.168.10.1/」(RC3008 の IP アドレスが 192.168.10.1 の場合)と入力して RC3008 にアクセスしてください。RC3008 の設定画面が表示されたら、HTTPS 接続できていることとなります。

備考

以下の画面が表示された場合は、[このサイトの閲覧を続行する(推奨されません)。] をクリックしてください。



RC3008 と https 接続した場合に、以下のように[証明書のエラー]が表示されますが、このままご使用いただき問題はありません。



RC3008 の IP アドレスと、[証明書要求(CSR)]で設定した[サーバ名]の IP アドレスが一致しない場合、上記事象となります。DNS サーバを使用している環境にて[サーバ名]から RC3008 の IP アドレスを参照できる場合は、上記事象は発生しません。

オムロン株式会社 K1L-D-10037A