|  |
| --- |
|  |
| 操作チュートリアル  SSL証明書設定管理者編 |
| Ver5.74以上対象 |



|  |
| --- |
| 第1版  2025/09/11 |

目次

[1. はじめに 1](#_Toc208483310)

[2. SSL証明書設定について 1](#_Toc208483311)

[3. SSL証明書設定を行う 2](#_Toc208483312)

[3.1. 秘密鍵を生成して証明書登録 4](#_Toc208483313)

[3.1.1. CSRの作成、確認 5](#_Toc208483314)

[3.1.1.1. CSRの作成 6](#_Toc208483315)

[3.1.1.2. CSRの確認 8](#_Toc208483316)

[3.1.2. 認証局に証明書発行依頼 9](#_Toc208483317)

[3.1.3. 中間証明書のインポート 9](#_Toc208483318)

[3.1.4. サーバー証明書のインポート 12](#_Toc208483319)

[3.1.5. サーバー証明書の適用 14](#_Toc208483320)

[3.1.6. サーバー証明書適用後の確認 16](#_Toc208483321)

[3.1.7. ファイル認証を設定する 16](#_Toc208483322)

[3.1.8. 中間証明書の更新を行う場合 20](#_Toc208483323)

[3.1.9. 自己署名証明書の設定 20](#_Toc208483324)

[3.2. 秘密鍵とサーバー証明書をインポートして証明書登録 22](#_Toc208483325)

[3.2.1. 秘密鍵とサーバー証明書のペアをインポート 23](#_Toc208483326)

[3.2.2. PKCS#12形式のファイルをインポート 27](#_Toc208483327)

[3.3. バックアップからサーバー証明書を適用する 30](#_Toc208483328)

# はじめに

本書はProself Ver5.74以上を対象としたサーバー証明書設定方法について記載しております。

Proself Ver5.73以下をご利用中の場合は、以下URL内の「Proself Ver.5 - 操作チュートリアルSSL証明書設定管理者編」をご参照ください。

<https://www.proself.jp/manualtutorial/list/>

* Proselfのバージョン確認方法につきましては以下FAQをご参照ください。  
  <https://www.proself.jp/support/faq465/>

# SSL証明書設定について

Proselfでは管理画面からSSL証明書(サーバー証明書、中間証明書)の設定を行うことができます。

Proselfは標準出荷状態で「CN=www.proself.jp」の自己署名証明書を同梱しているため、そのままの状態でもHTTPS接続による通信の暗号化が可能ですが、コモンネーム不一致等の理由でWebサイトとしての実在証明ができず、アクセスした際に警告が表示されてしまいます。

Proselfを安全に利用するためにも、インターネットに公開する場合は本設定を実施いただくことを強くお勧めいたします。

* サーバー証明書はSectigo、GlobalSign、DigiCert等の認証局から発行してもらう必要がありますが、発行には別途費用が発生いたします。証明書の発行にかかる費用や発行の手続きにつきましては各認証局にご確認ください。

また、Ver5.74より画面上で作成したCSRを認証局に送付し発行されたサーバー証明書をインポートする従来の方法に加えて、Proself以外で作成した秘密鍵とサーバー証明書のペアのインポートにも対応しています。

# SSL証明書設定を行う

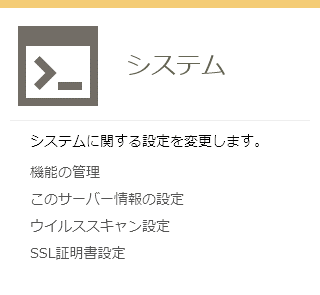
SSL証明書設定を行うための手順を記載します。

Proselfに管理者ユーザーでログイン後、管理画面にて「システム設定」をクリックします。



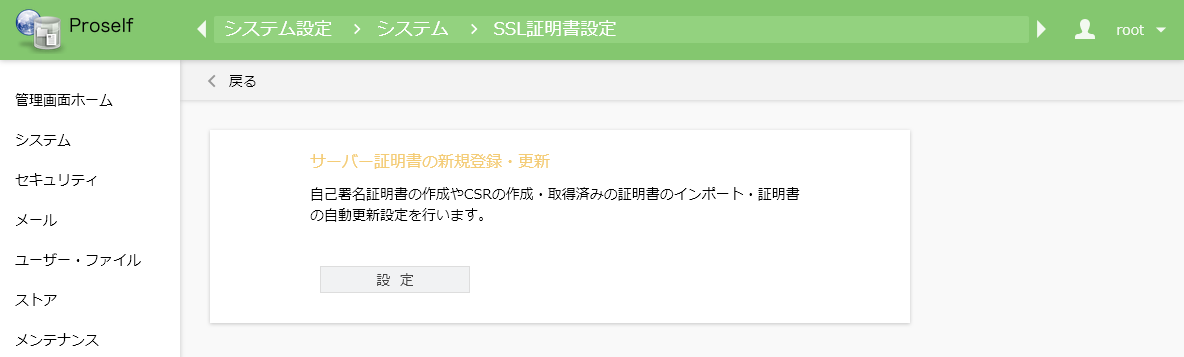
**管理画面ホーム**

システム内の「SSL証明書設定」をクリックします。



**システム設定 - システム**

「サーバー証明書の新規登録・更新」より「設定」をクリックします。



**SSL証明書設定**

「サーバー証明書の新規登録・更新」画面より、「秘密鍵を生成して証明書登録」「秘密鍵とサーバー証明書をインポートして証明書登録」のいずれかで設定を行います。



**サーバー証明書の新規登録・更新**

各機能に関する概要は以下の通りです。

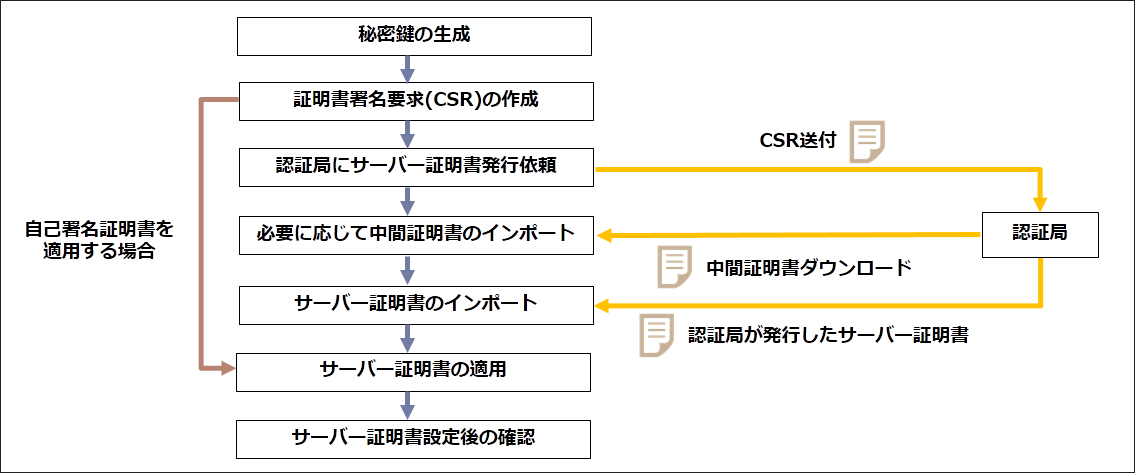
| 機能名 | 説明 |
| --- | --- |
| 秘密鍵を生成して証明書登録(※) | Proselfで秘密鍵の生成とCSRの作成を行い、そのCSRを使用して発行されたサーバー証明書をインポートする方法です。また、自己署名証明書を作成することもできます。  詳細につきましては「[3.1.秘密鍵を生成して証明書登録](#_秘密鍵を生成して証明書登録)」をご参照ください。 |
| 秘密鍵とサーバー証明書をインポートして証明書登録 | Proself以外で生成した秘密鍵とサーバー証明書のペアをインポートします。  詳細につきましては「[3.2.秘密鍵とサーバー証明書をインポートして証明書登録](#_秘密鍵とサーバー証明書をインポートして証明書登録_1)」をご参照ください。 |

* Ver5.73以下のバージョンでSSL証明書設定を行う場合と同じ方法です。

## 秘密鍵を生成して証明書登録

Proselfで秘密鍵を生成して証明書署名要求(CSR)の作成および認証局で発行されたサーバー証明書のインポートを行います。

サーバー証明書設定の流れは下図のようになります。



**サーバー証明書設定の流れ**

「サーバー証明書の新規登録・更新」画面内の「秘密鍵を生成して証明書登録」より「設定」をクリックします。



**サーバー証明書の新規登録・更新**

「秘密鍵を生成して証明書登録」画面内に各種メニューが表示されます。



**秘密鍵を生成して証明書登録**

サーバー証明書を新規設定、更新を行う場合はそれぞれ以下の設定を順に実施します。

手順の詳細につきましては各セクションをご参照ください。

* 「[3.1.1. CSRの作成](#_証明書署名要求(CSR)の作成)、確認」
* 「[3.1.2.認証局に証明書発行依頼](#_認証局に証明書発行依頼)」
* 「[3.1.3.中間証明書のインポート](#_中間証明書のインポート)」
* 「[3.1.4.サーバー証明書のインポート](#_SSL証明書のインポート)」
* 「[3.1.5.サーバー証明書の適用](#_SSL証明書の適用)」
* 「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」

### CSRの作成、確認

認証局に送付するための証明書署名要求(CSR)の作成、確認を行います。

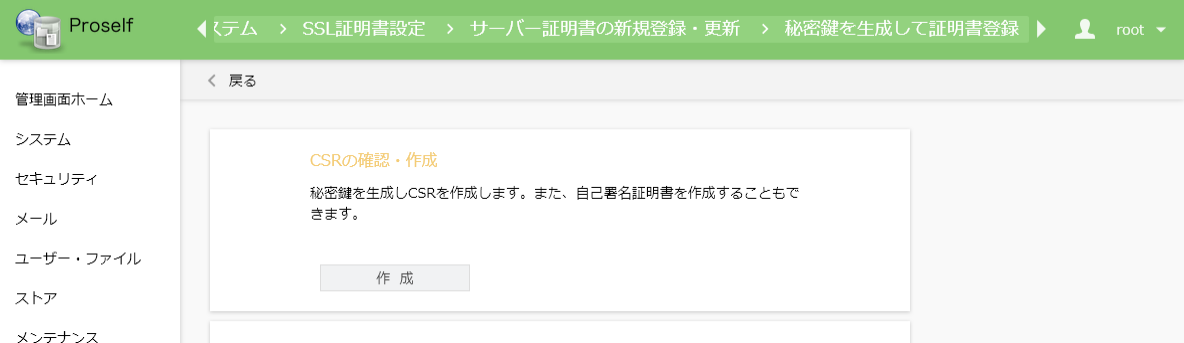
CSRが作成済みかどうかによって手順が異なります。

* CSR作成時はProself内部で秘密鍵が自動生成されます。

初めてCSRを作成する場合は「[3.1.1.1.CSRの作成](#_CSRの作成_1)」を、すでにCSR作成済みの場合は「[3.1.1.2.CSRの確認](#_CSRの確認)」をご参照ください。

#### CSRの作成

「CSRの確認・作成」より「作成」をクリックします。



**秘密鍵を生成して証明書登録**

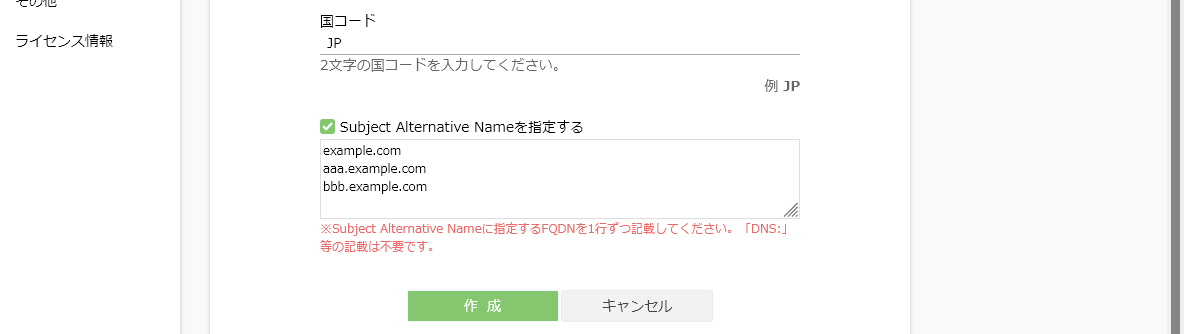
「CSRの作成」画面で各項目に入力をおこない「作成」をクリックします。

* 入力する値には日本語は使用できません。必ず英数字のみを入力してください。



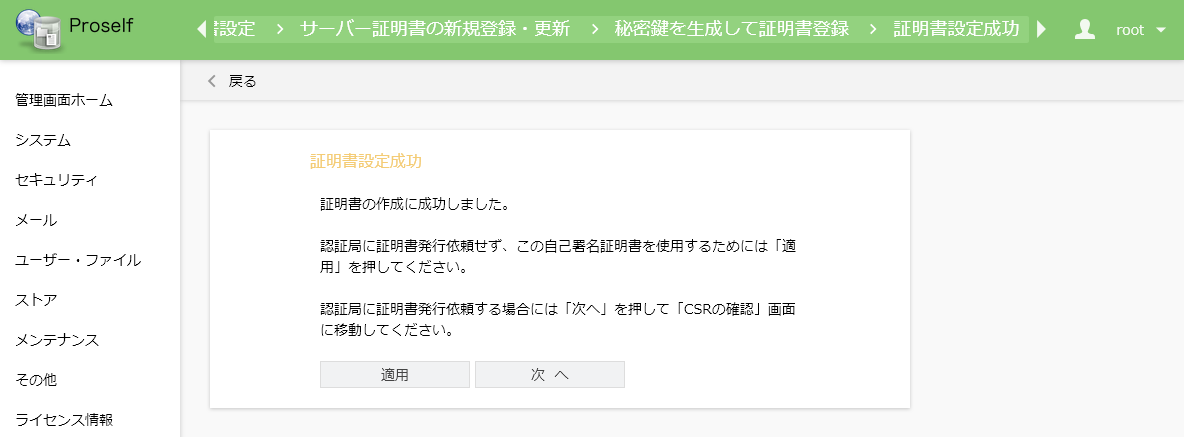
**CSRの作成**

なお、マルチドメイン証明書の利用に伴いCSRにSubject Alternative Namesを含める必要がある場合は、証明書署名要求(CSR)作成画面内の「Subject Alternative Nameを指定する」にチェックを入れ、入力欄にSubject Alternative Name(サブジェクトの別名) に指定するFQDNを1行ずつ記載します。



**CSRの作成**

「証明書設定成功」画面が表示されます。認証局に証明書発行依頼する場合には「次へ」をクリックします。



**証明書設定成功**

「CSRの確認」画面が表示され、「CSRの作成」画面で設定した各項目の情報、作成されたCSRが表示されます。

* 設定内容の誤り等により再度CSRを作成したい場合は、「再作成」をクリックしてCSRの作作成を実施ください。



**CSRの確認**

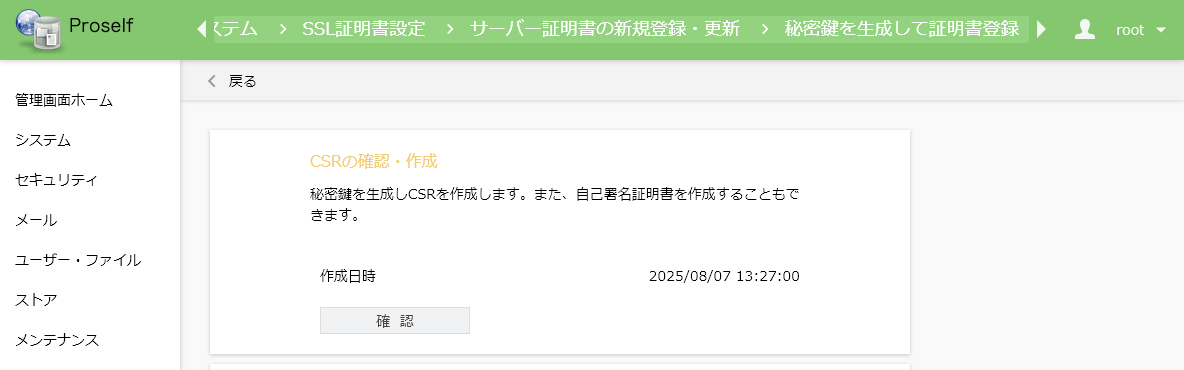
認証局から発行された証明書を使用する場合は、「[3.1.2.認証局に証明書発行依頼](#_認証局に証明書発行依頼)」、「[3.1.3.中間証明書のインポート](#_中間証明書のインポート)」、「[3.1.4.サーバー証明書のインポート](#_SSL証明書のインポート)」、「[3.1.5.サーバー証明書の適用](#_SSL証明書の適用)」、「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」を実施します。

「CSRの確認」画面内「生成されたCSR」のテキストエリアに表示されている「-----BEGIN NEW CERTIFICATE REQUEST-----」から「-----END NEW CERTIFICATE REQUEST-----」までの行は、「[3.1.2.認証局に証明書発行依頼](#_認証局に証明書発行依頼)」で認証局に送付する際に必要です。

#### CSRの確認

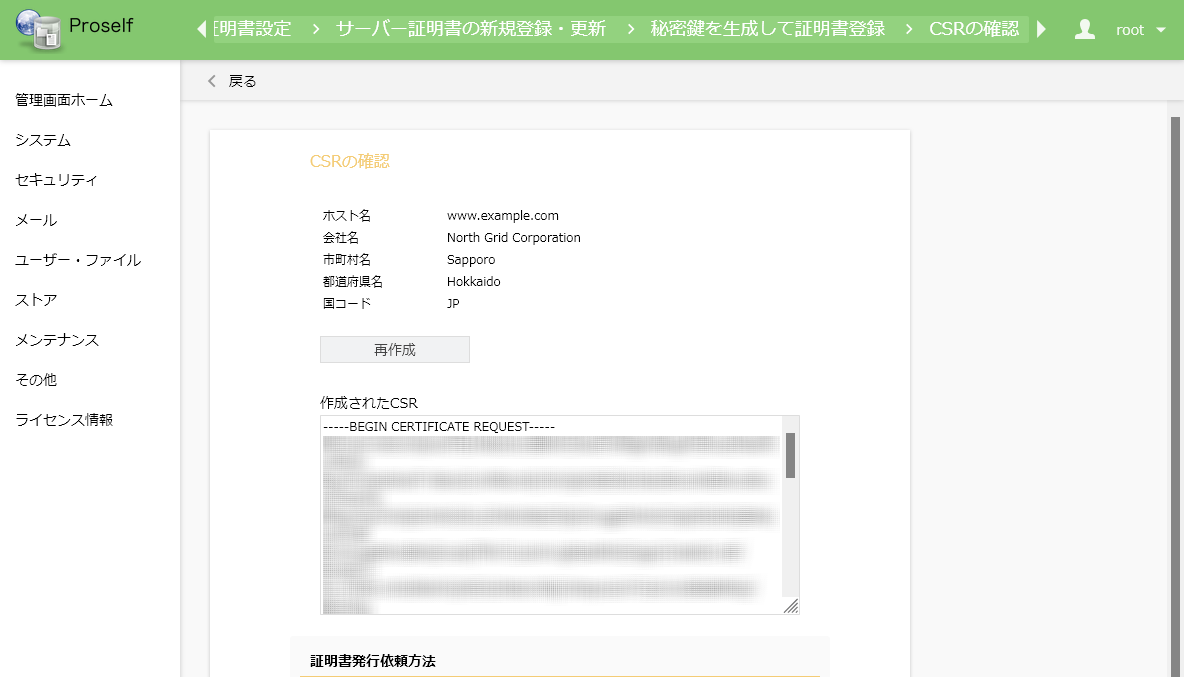
「[3.1.1.1.CSRの作成](#_CSRの作成_1)」でCSRを作成済みの場合は、本画面にCSRの作成日時が表示されます。

「CSRの確認・作成」より「確認」をクリックします。



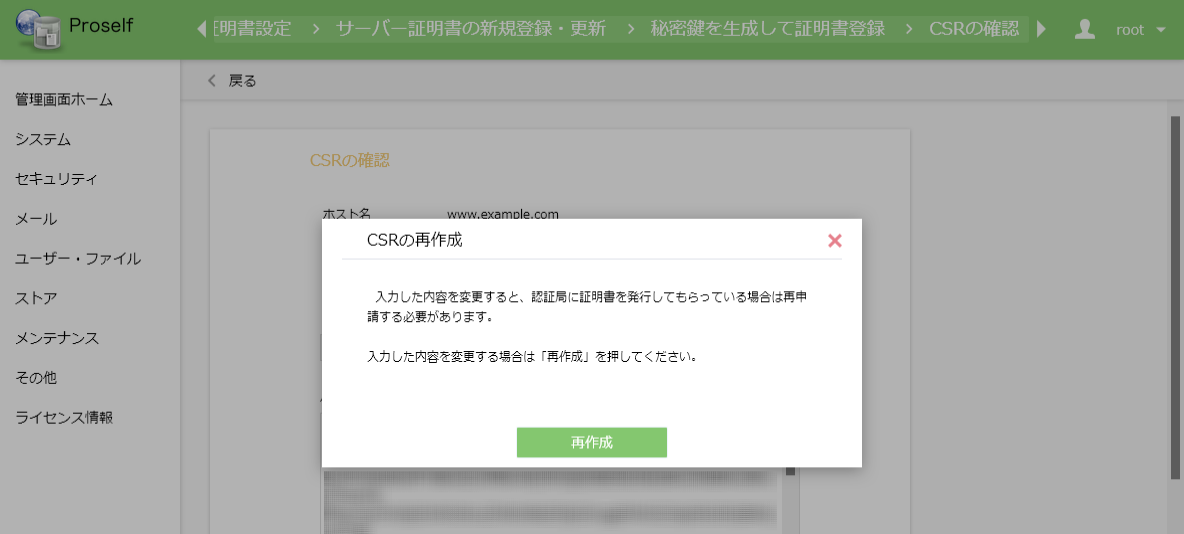
**秘密鍵を生成して証明書登録**

CSRの確認画面が表示されます。CSRを再作成する場合は「再作成」ボタンをクリックし、CSRを再作成せず前回のCSRを使用する場合は「作成されたCSR」の内容を取得ください。



**CSRの確認**

CSRの確認画面で「再作成」ボタンをクリックした場合は以下のような確認画面が表示されますので、「再作成」をクリックします。



**CSRの再作成**

以降は「[3.1.1.1.CSRの作成](#_CSRの作成_1)」と同様の手順でCSRの作成を行います。

* CSRの作成画面には前回作成時の内容が表示されます。入力内容に変更が無い場合でも「設定」をクリックする必要があります。

### 認証局に証明書発行依頼

「[3.1.1.CSRの作成](#_証明書署名要求(CSR)の作成)、確認」で作成、確認したCSRを認証局に送付し、サーバー証明書の発行を申請します。

* CSRの送付方法については認証局の指示に従ってください。

その後、認証局よりサーバー証明書が送付されましたら、「[3.1.3.中間証明書のインポート](#_中間証明書のインポート)」「[3.1.4.サーバー証明書のインポート](#_SSL証明書のインポート)」を実施します。

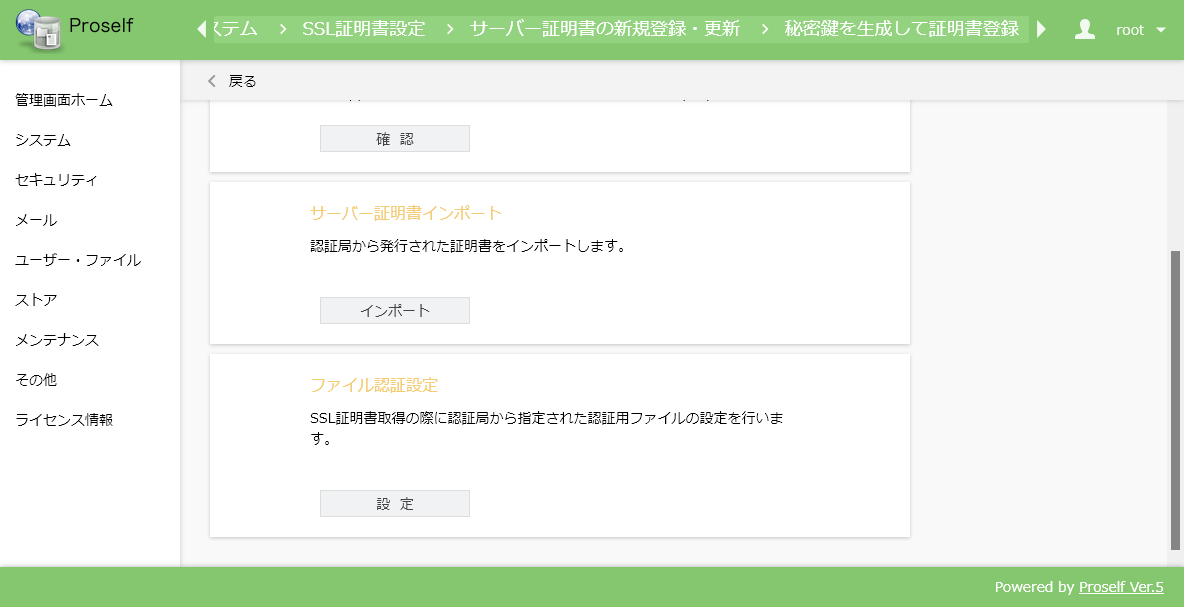
なお、サーバー証明書発行の申請時にファイル認証方式を選択した場合は、「[3.1.7.ファイル認証を設定する](#_ファイル認証を設定する)」を実施する必要がございます。

### 中間証明書のインポート

一部の認証局は中間証明書のインポートが必要です。中間証明書が必要かどうかは認証局ごとに異なりますので、ご不明な場合は認証局にお問い合わせください。

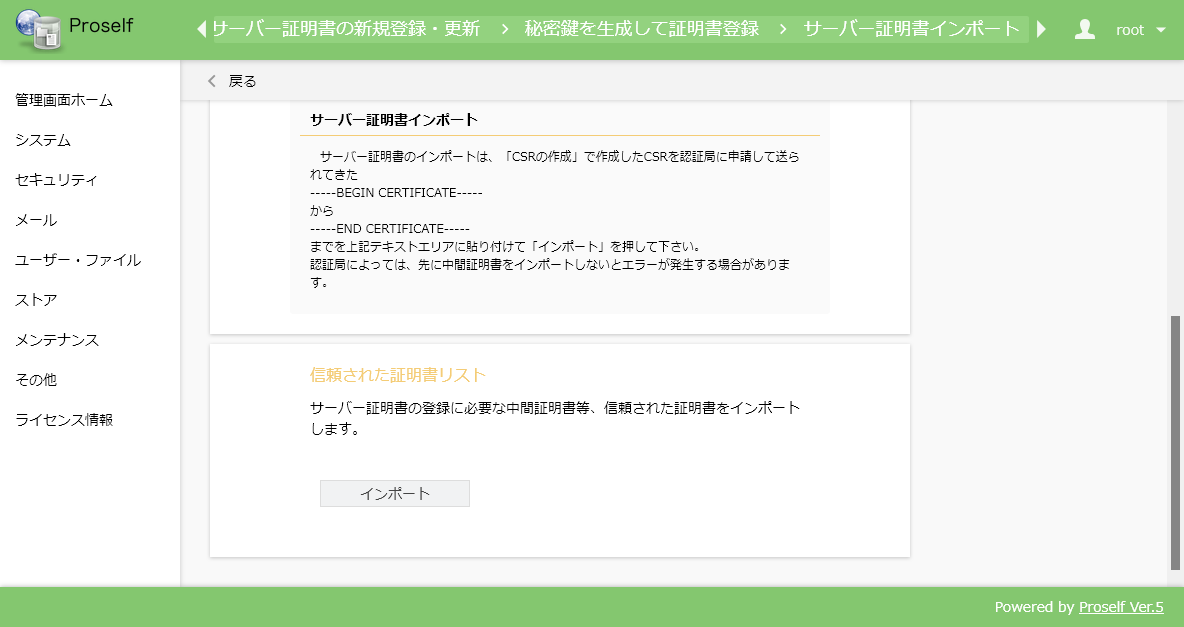
中間証明書が不要の場合は「[3.1.4.サーバー証明書のインポート](#_SSL証明書のインポート)」に進みます。

中間証明書が必要な場合は認証局から中間証明書をダウンロード後、「秘密鍵を生成して証明書登録」画面内の「サーバー証明書インポート」より「インポート」をクリックします。



**秘密鍵を生成して証明書登録**

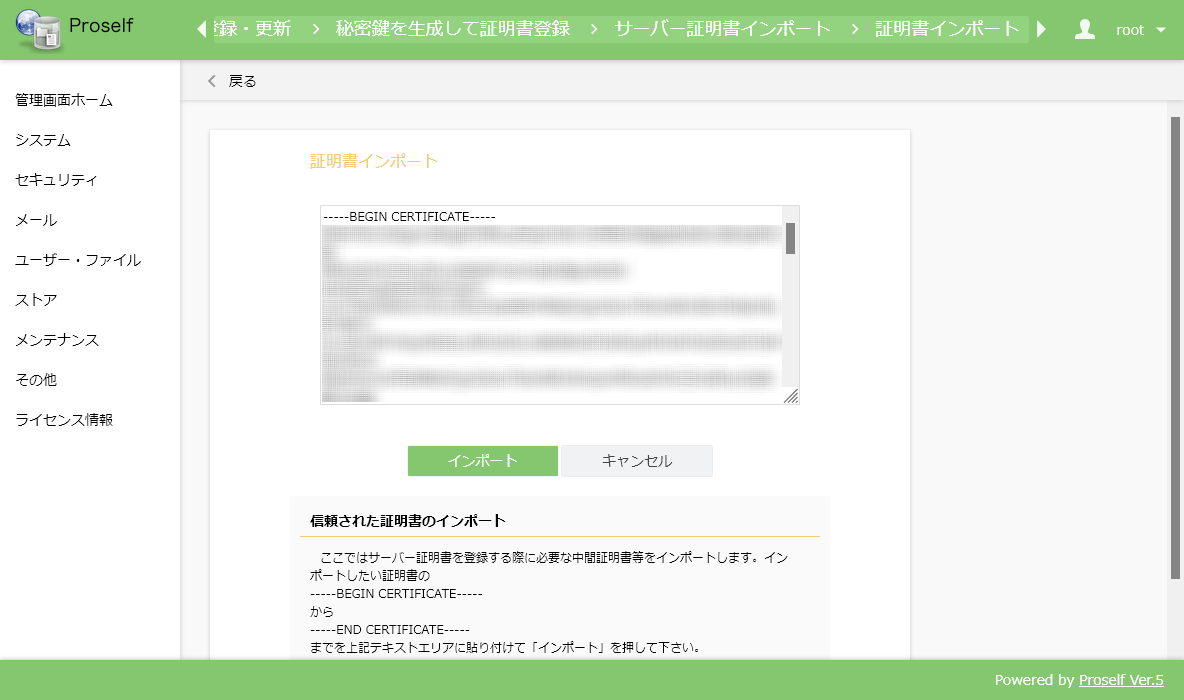
「サーバー証明書インポート」画面内の「信頼された証明書リスト」より「インポート」をクリックします。



**サーバー証明書インポート**

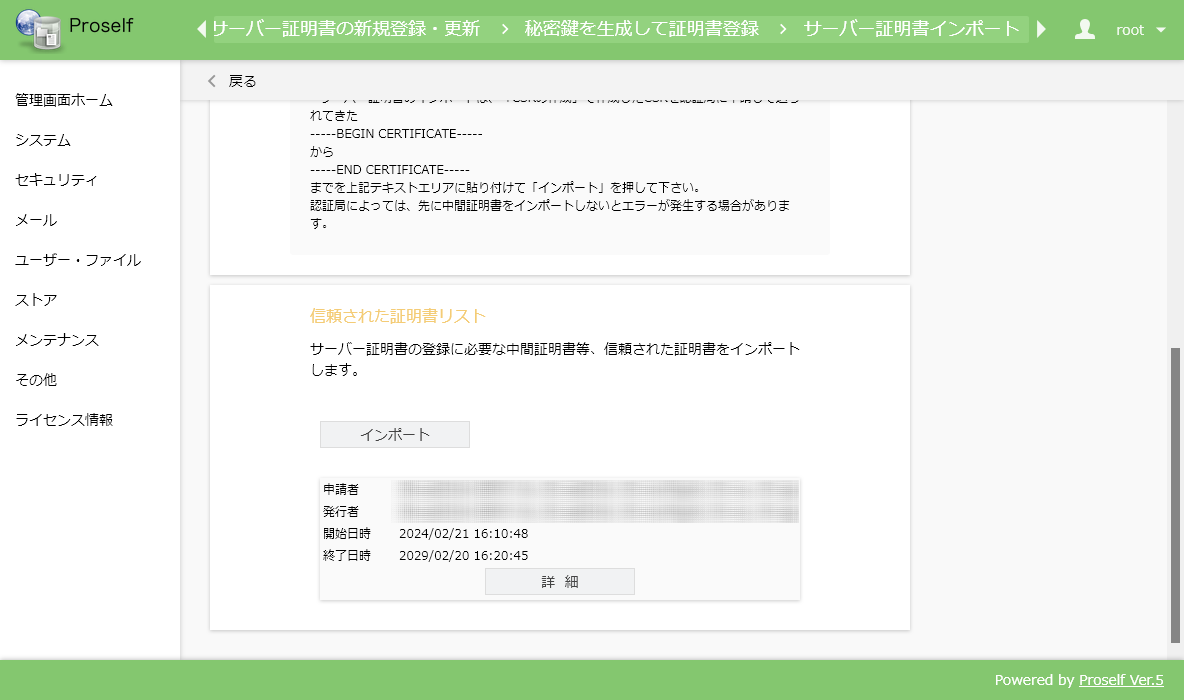
ダウンロードした中間証明書をテキストエディタで開き、中に記述されているテキストを「証明書インポート」画面内のテキストエリアにコピーして貼り付けます。

「インポート」をクリックすると中間証明書のインポートが行われます。



**信頼された証明書のインポート**

インポート完了後は「サーバー証明書」画面内の「信頼された証明書リスト」に証明書情報が表示されます。



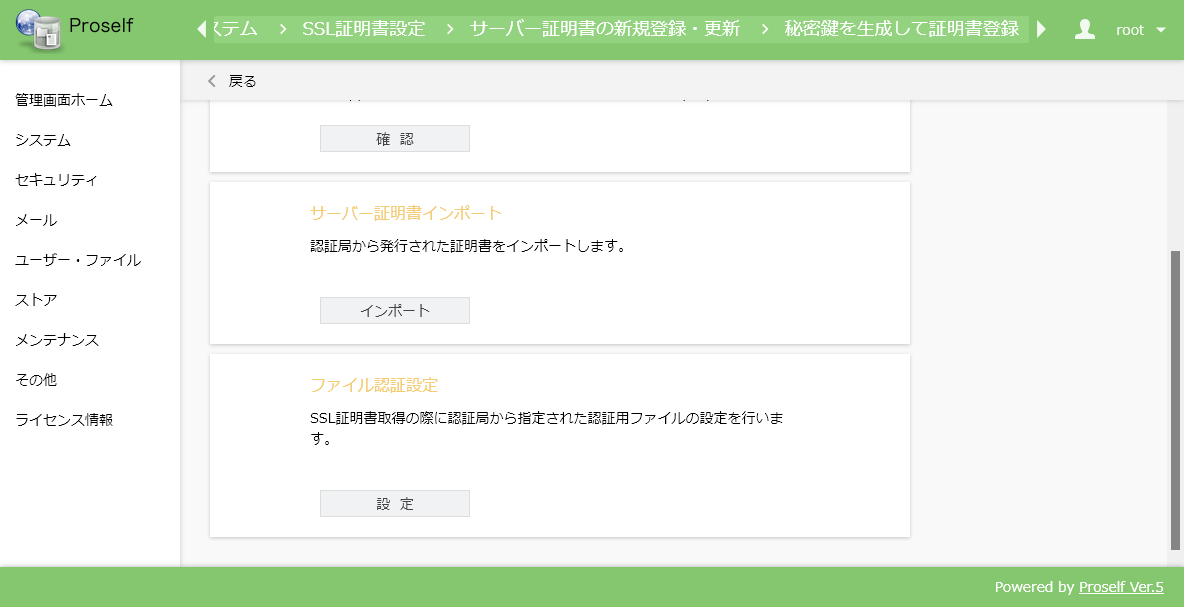
**サーバー証明書インポート**

さらに中間証明書をインポートする場合は、「信頼された証明書リスト」に表示されている「インポート」をクリックして上記手順を繰り返し実施ください。

### サーバー証明書のインポート

認証局より送付されてきたサーバー証明書をインポートします。

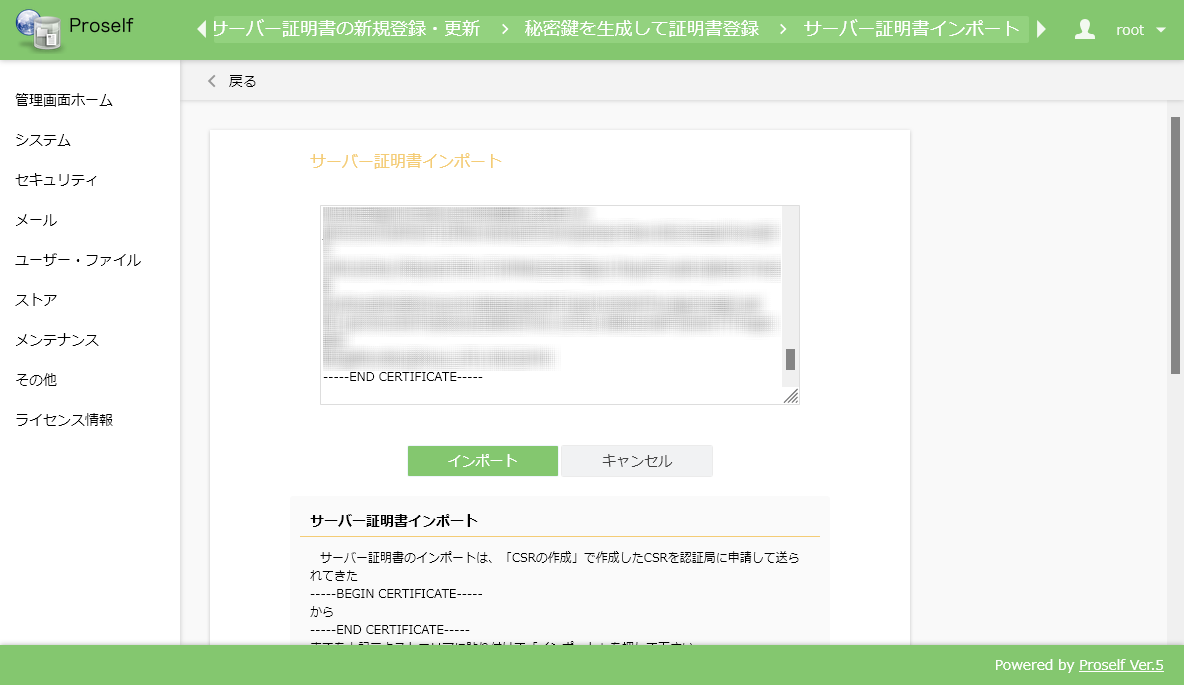
「秘密鍵を生成して証明書登録」画面内の「サーバー証明書インポート」より「インポート」をクリックします。



**秘密鍵を生成して証明書登録**

認証局から送られてきたサーバー証明書をテキストエディタで開き、中に記述されているテキストを「サーバー証明書インポート」画面内のテキストエリアに貼り付けます。

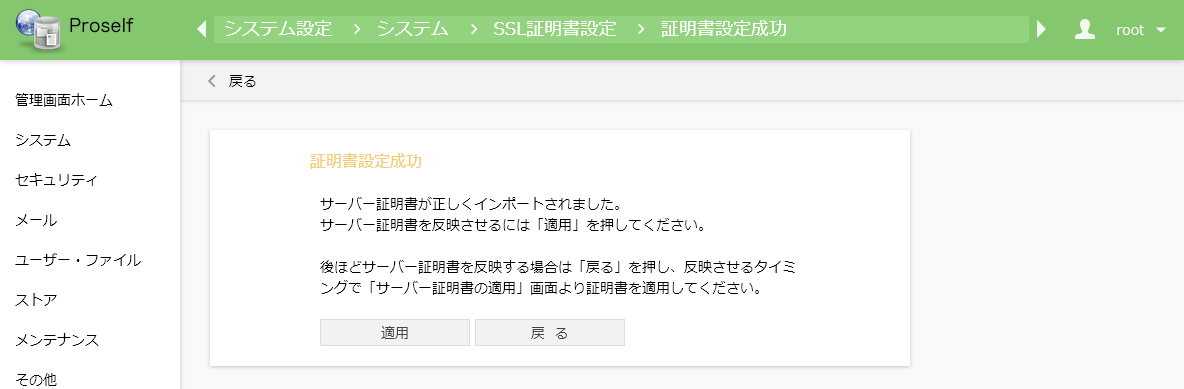
「インポート」をクリックするとサーバー証明書のインポートが行われます。



**サーバー証明書インポート**

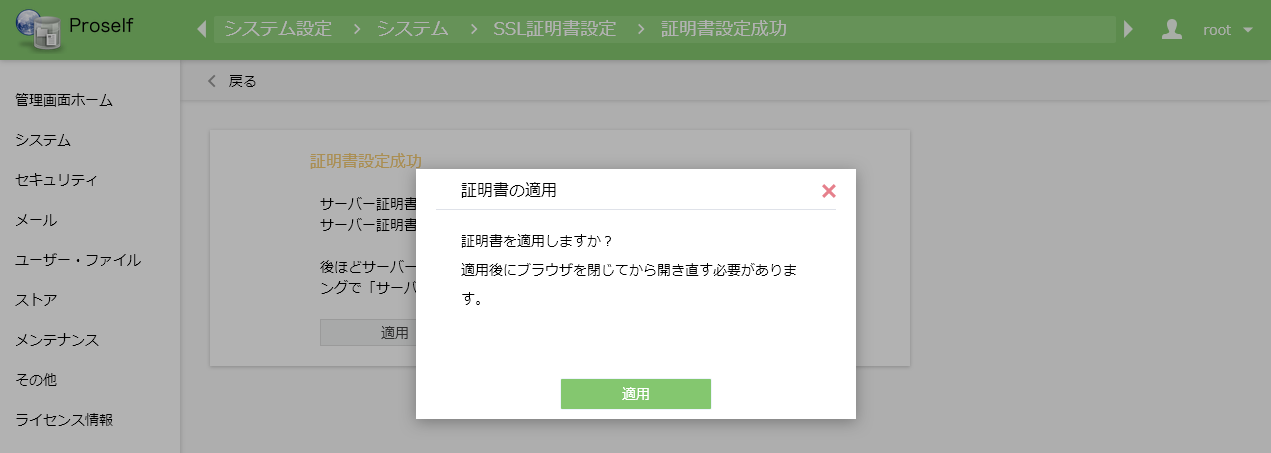
インポートが正しく行われた場合は「証明書設定成功」画面が表示されます。直ちに証明書を反映させる場合は「適用」をクリックし、証明書を後日反映させる場合は「戻る」をクリックします。

* 後日反映の手順については「[3.1.5.サーバー証明書の適用](#_SSL証明書の適用)」をご参照ください。



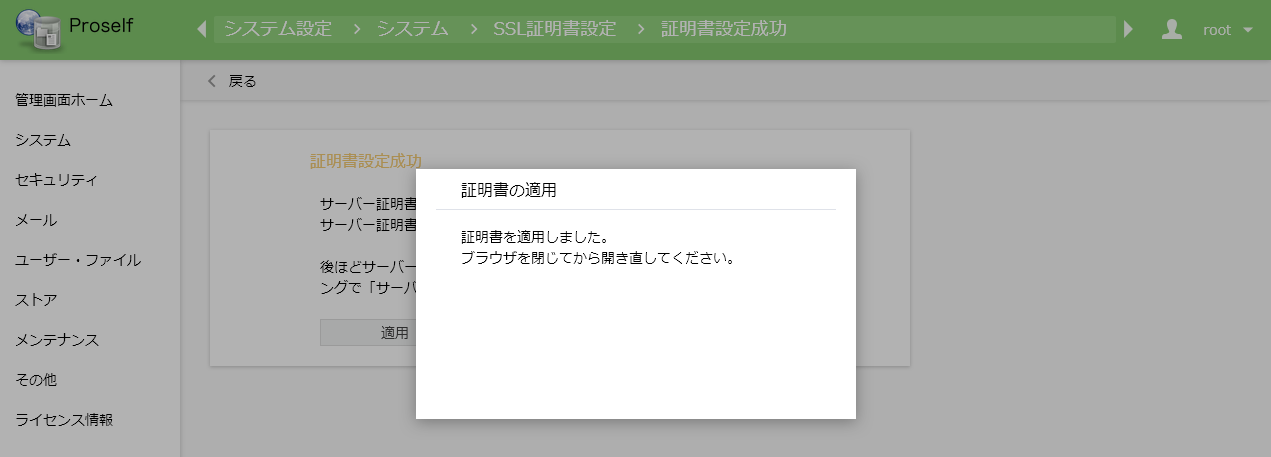
**証明書設定成功**

確認ダイアログが表示されますので、「適用」をクリックします。



**証明書の適用**

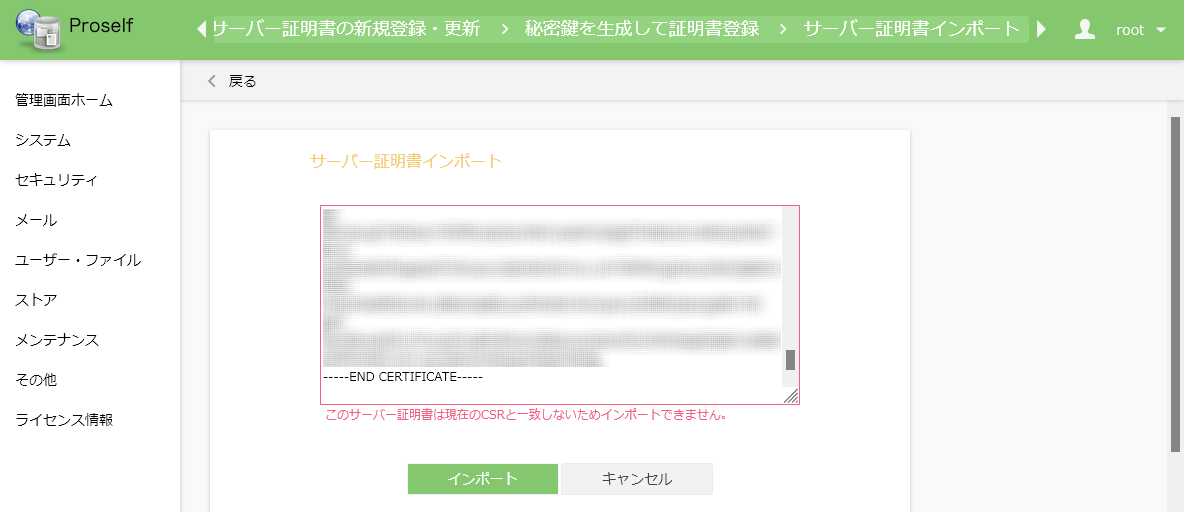
証明書の適用が完了した旨の画面が表示されますので、指示に従いブラウザを開きなおします。



**証明書の適用**

適用後は「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」を実施します。

* 「[3.1.1.CSRの作成](#_証明書署名要求(CSR)の作成)、確認」で作成したCSRと異なるCSRで発行されたサーバー証明書をインポートした場合は以下のようなエラーが表示されます。インポートするサーバー証明書に誤りが無いかご確認ください。



**サーバー証明書インポート**

### サーバー証明書の適用

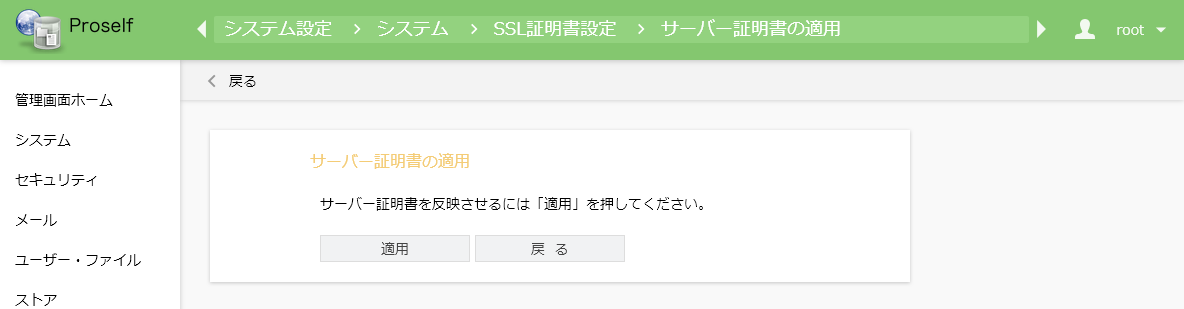
「[3.1.4.サーバー証明書のインポート](#_SSL証明書のインポート)」で適用しなかったインポート済みのサーバー証明書を適用します。

「サーバー証明書設定」画面内の「サーバー証明書の適用」に表示されている「適用予定のサーバー証明書」の内容を確認し、「適用」をクリックします。



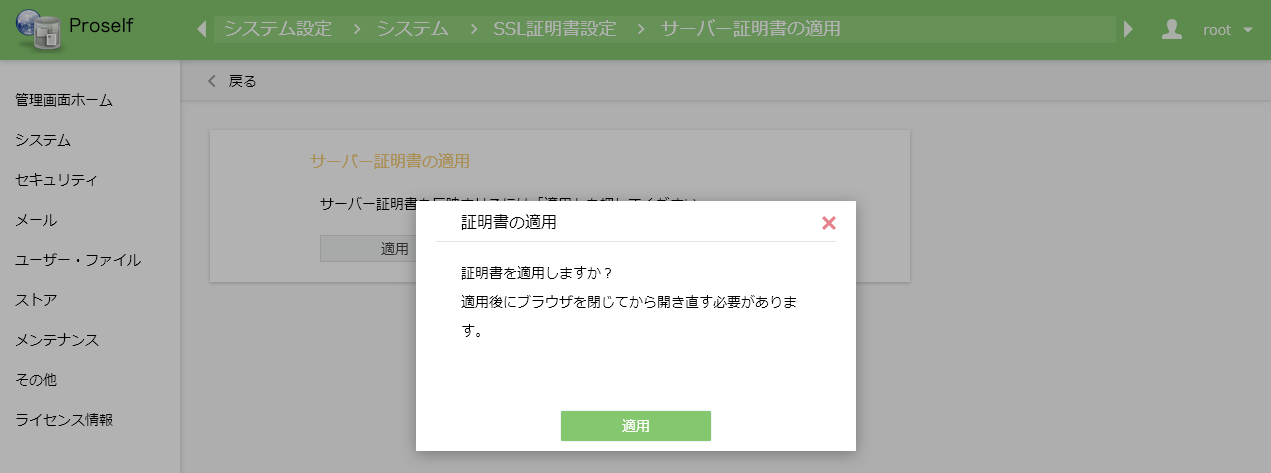
**SSL証明書設定**

「サーバー証明書の適用」画面内の「適用」をクリックします。



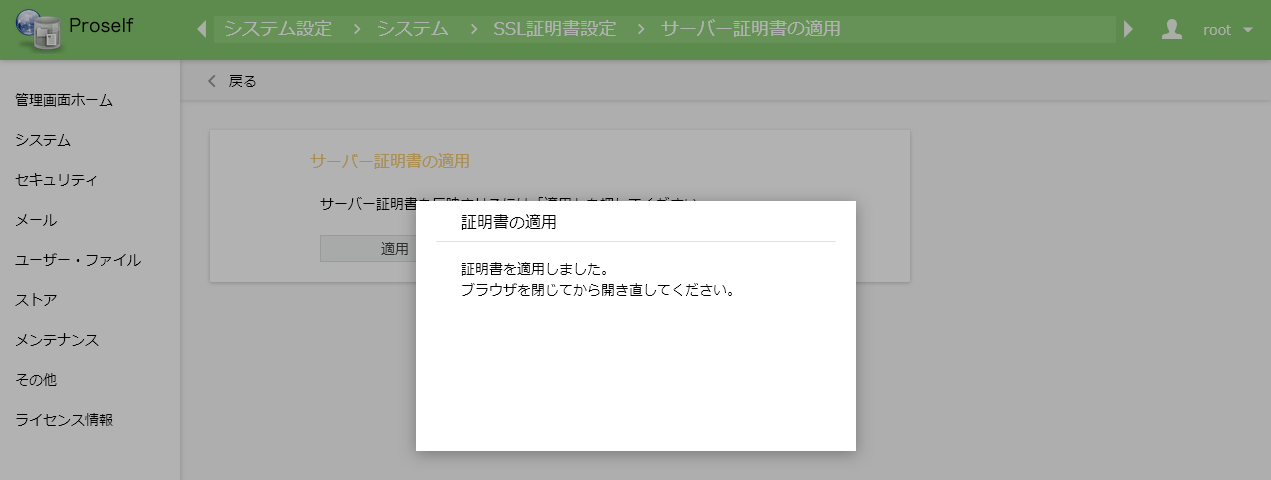
**サーバー証明書の適用**

確認ダイアログが表示されますので、「適用」をクリックします。



**証明書の適用**

証明書の適用が完了した旨の画面が表示されますので、指示に従いブラウザを開きなおします。



**証明書の適用**

適用後は「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」を実施します。

### サーバー証明書適用後の確認

サーバー証明書適用後は、ProselfにHTTPS接続できること、「SSL証明書設定」画面内に表示される「現在適用されているサーバー証明書」よりインポートしたサーバー証明書が反映されていることを確認します。



**SSL証明書設定**

なお、適用したサーバー証明書の問題等により過去に適用したサーバー証明書に差し戻す必要がある場合は、「[3.3.バックアップからサーバー証明書を適用する](#_バックアップからサーバー証明書を適用する)」を実施ください。

**＜補足＞**

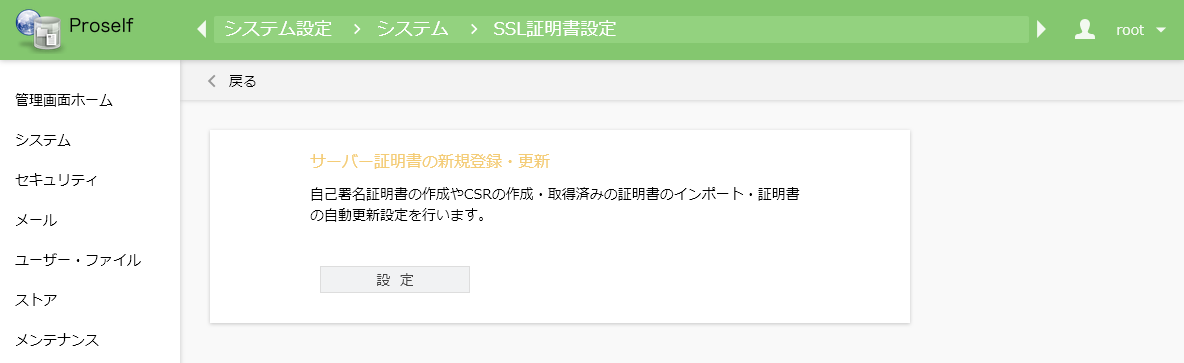
* サーバー証明書を設定後、HTTP経由のアクセスが必要ない場合の対応方法については以下FAQをご参照ください。  
  <https://www.proself.jp/support/faq427/>
* HTTPからアクセスがあった場合に、HTTPSへリダイレクトさせる方法もございます。詳細については以下FAQをご参照ください。  
  <https://www.proself.jp/support/faq331/>

### ファイル認証を設定する

ファイル認証とは、認証局より発行された認証用ファイルがサーバーのFQDN(コモンネーム)配下に配置されたことを認証局が検知すると、サーバー証明書が発行される仕組みです。

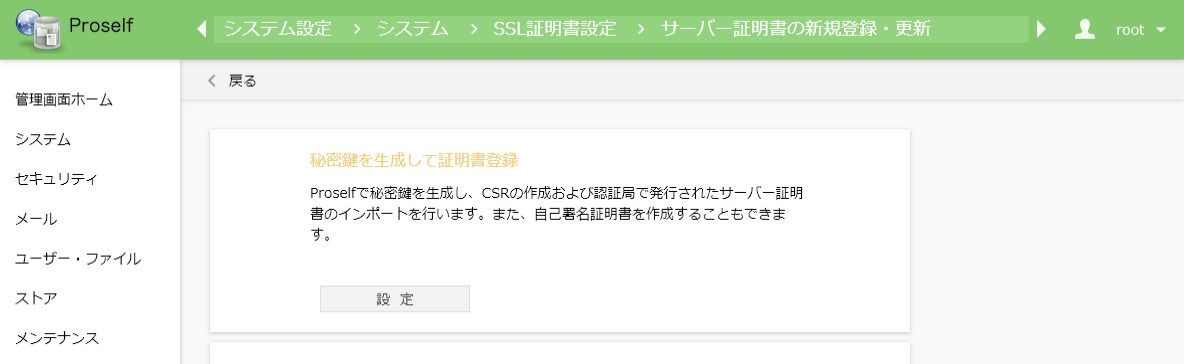
Proselfでファイル認証を利用する場合は以下の設定を行います。

「サーバー証明書の新規登録・更新」より「設定」をクリックします。



**SSL証明書設定**

「サーバー証明書の新規登録・更新」画面内の「秘密鍵を生成して証明書登録」より「設定」をクリックします。



**サーバー証明書の新規登録・更新**

「秘密鍵を生成して証明書登録」画面内の「ファイル認証設定」より「設定」をクリックします。



**秘密鍵を生成して証明書登録**

「ファイル認証設定」画面からご利用の認証局の設定方法に従い、認証用ファイル配置先を設定します。



**ファイル認証設定**

「認証用ファイルアップロード」下にあるエリア内に認証局から発行された認証用ファイルをドラッグ＆ドロップします。



**ファイル認証設定**

「認証用ファイルアップロード」下にあるエリア内にファイル名とアイコンが表示されていることを確認し、「設定」をクリックします。



**ファイル認証設定**

設定完了後、「秘密鍵を生成して証明書登録」画面内の「ファイル認証設定」に設定済みのファイル認証設定内容が表示されます。



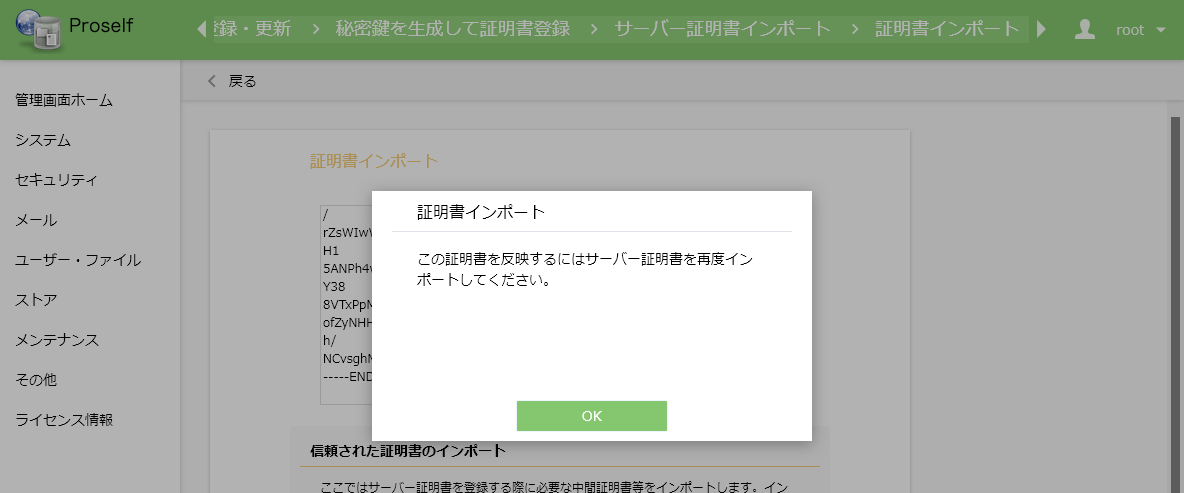
**秘密鍵を生成して証明書登録**

認証局によって認証用ファイルが検知されるとサーバー証明書が発行されます。

サーバー証明書が発行された後、「[3.1.4.サーバー証明書のインポート](#_SSL証明書のインポート)」を実施します。

### 中間証明書の更新を行う場合

「[3.1.5.サーバー証明書の適用](#_サーバー証明書の適用)」実施後に「[3.1.3.中間証明書のインポート](#_中間証明書のインポート)」で中間証明書のインポートを実施した場合は、以下のようなダイアログが表示されます。

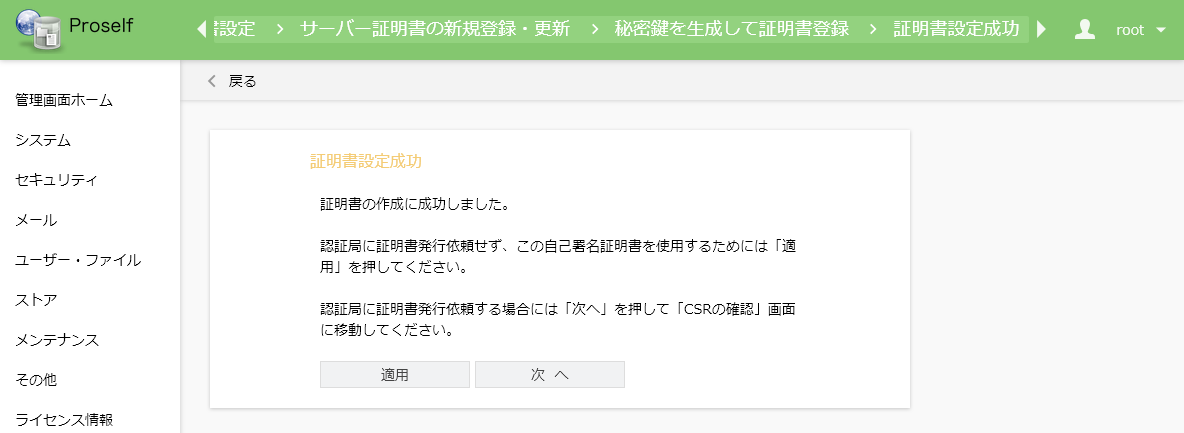


**信頼された証明書のインポート**

インポートした中間証明書を反映するには「[3.1.4.サーバー証明書のインポート](#_サーバー証明書のインポート)」の手順でサーバー証明書を再度インポートする必要がございます。

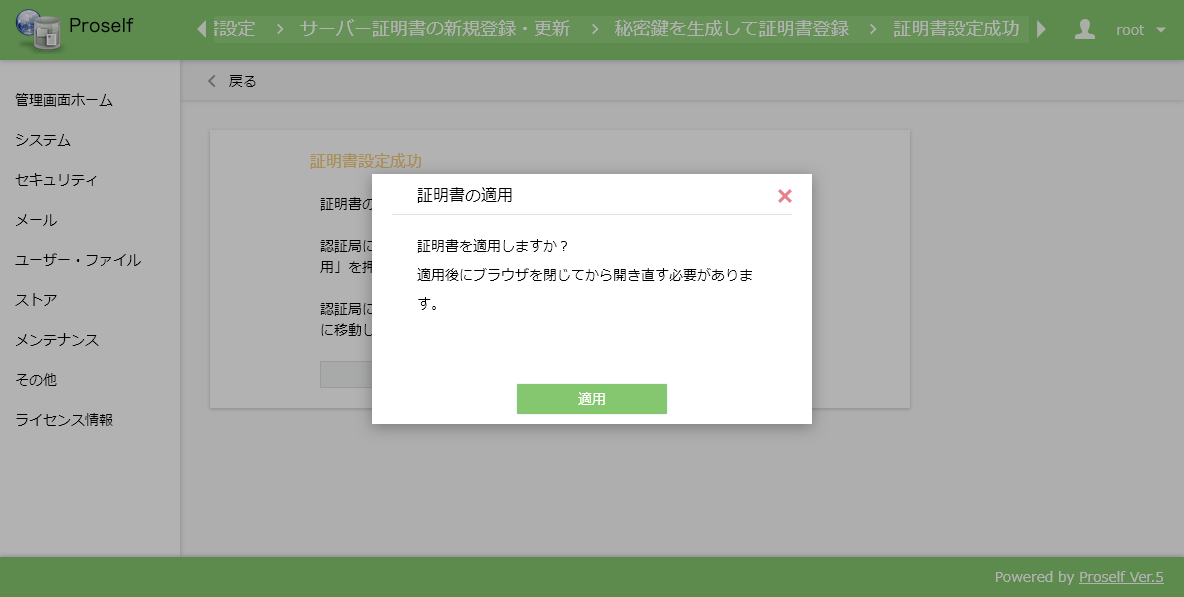
### 自己署名証明書の設定

「[3.1.1.1.CSRの作成](#_CSRの作成_1)」の手順で作成したCSRを自己署名証明書として使用する場合は、CSR作成後に表示される「証明書設定成功」画面で「適用」をクリックします。



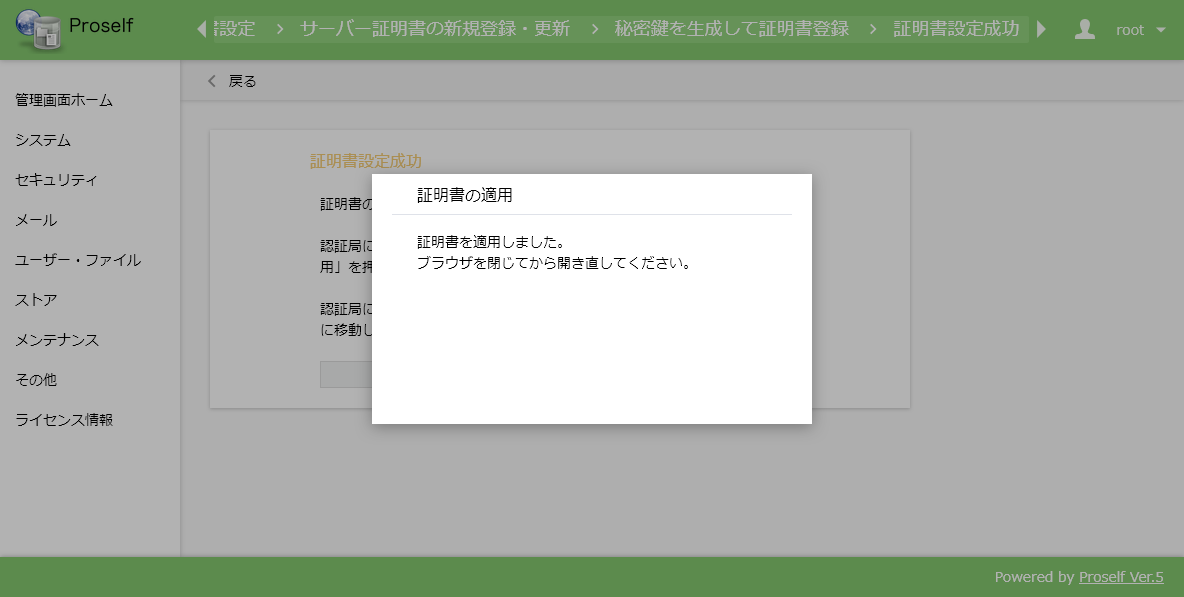
**証明書設定成功**

適用確認画面内の「適用」をクリックします。



**証明書の適用**

以下のような適用完了した旨のメッセージを確認後、画面の指示に従いブラウザを閉じて再度開き直し、「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」を実施します。



**証明書の適用**

## 秘密鍵とサーバー証明書をインポートして証明書登録

Proself以外で生成した秘密鍵とサーバー証明書のペアをインポートすることができます。

* Proself以外で生成した秘密鍵、サーバー証明書に関するお問い合わせは弊社では対応いたしかねますため、発行元までお問い合わせください。

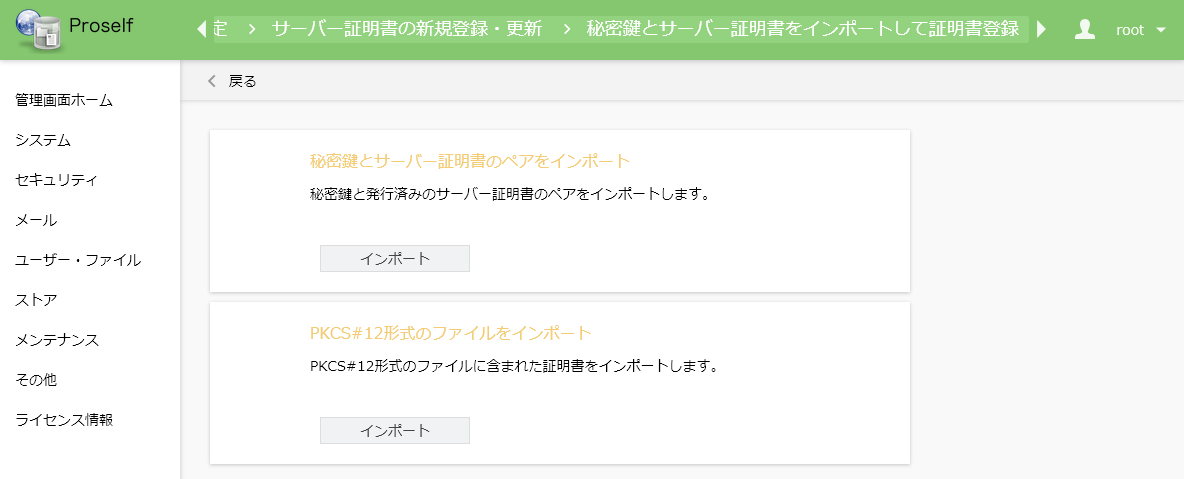
「サーバー証明書の新規登録・更新」画面内の「秘密鍵とサーバー証明書をインポートして証明書登録」より「設定」をクリックします。



**サーバー証明書の新規登録・更新**

「秘密鍵とサーバー証明書をインポートして証明書登録」画面より、目的に応じた機能ご利用ください。

手順詳細につきましては次項より記載しております。

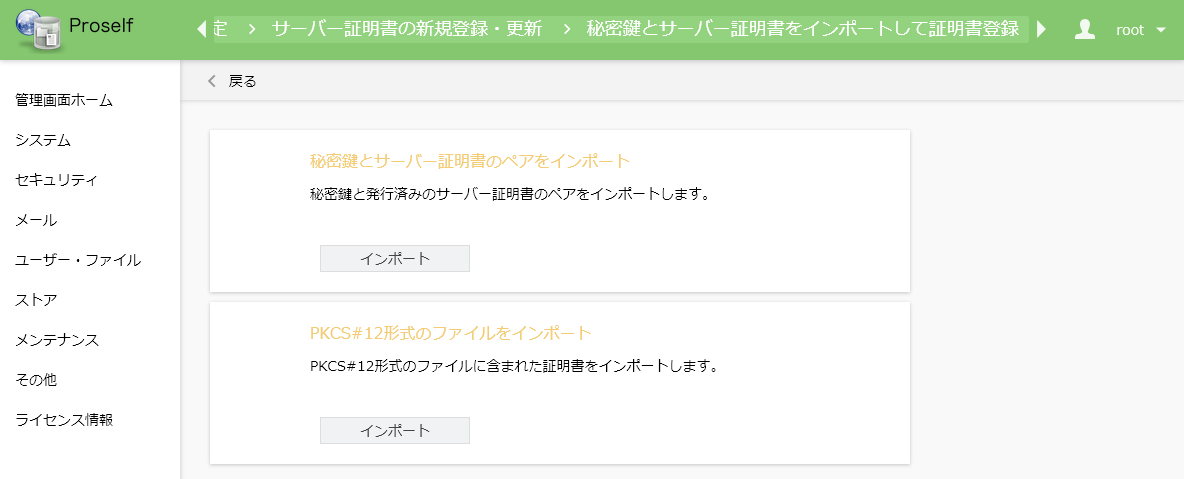


**秘密鍵とサーバー証明書をインポートして証明書登録**

### 秘密鍵とサーバー証明書のペアをインポート

Proself以外で生成した秘密鍵とサーバー証明書のペアをインポートすることができます。

「秘密鍵とサーバー証明書をインポートして証明書登録」画面内の「秘密鍵とサーバー証明書のペアをインポート」より「インポート」をクリックします。



**秘密鍵とサーバー証明書をインポートして証明書登録**

「秘密鍵とサーバー証明書をインポート」画面より各項目の設定を行い、「インポート」をクリックします。

* 秘密鍵にパスフレーズが設定されている場合は「パスフレーズ」欄の入力も必要です。



**秘密鍵とサーバー証明書をインポート**

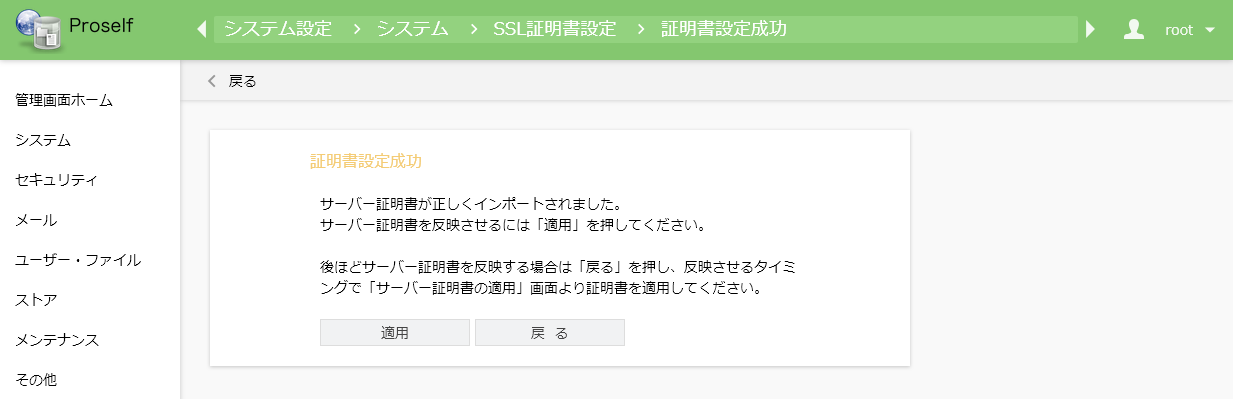
インポート内容に問題ない場合は、以下のようなダイアログが表示されますので、「インポート」をクリックします。



**証明書確認**

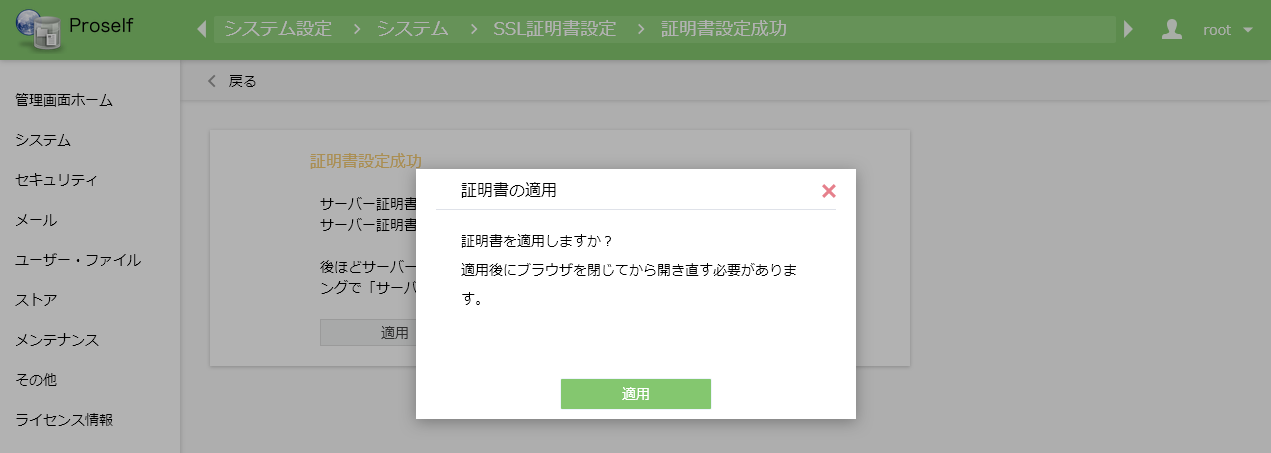
インポートが正しく行われた場合は「証明書設定成功」画面が表示されます。直ちに証明書を反映させる場合は「適用」をクリックし、証明書を後日反映させる場合は「戻る」をクリックします。

* 後日反映の手順については「[3.1.5.サーバー証明書の適用](#_SSL証明書の適用)」をご参照ください。



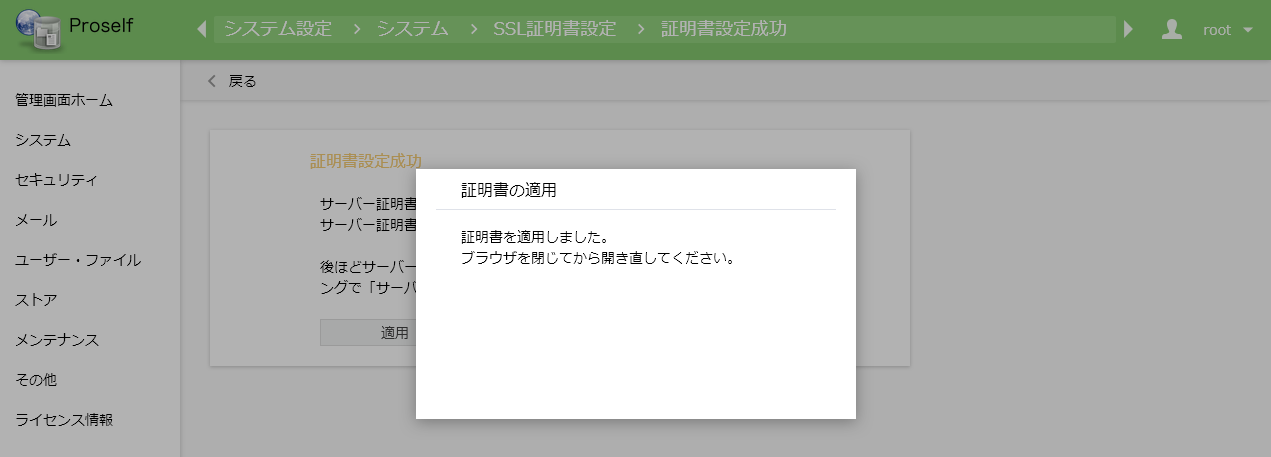
**証明書設定成功**

確認ダイアログが表示されますので、「適用」をクリックします。



**証明書の適用**

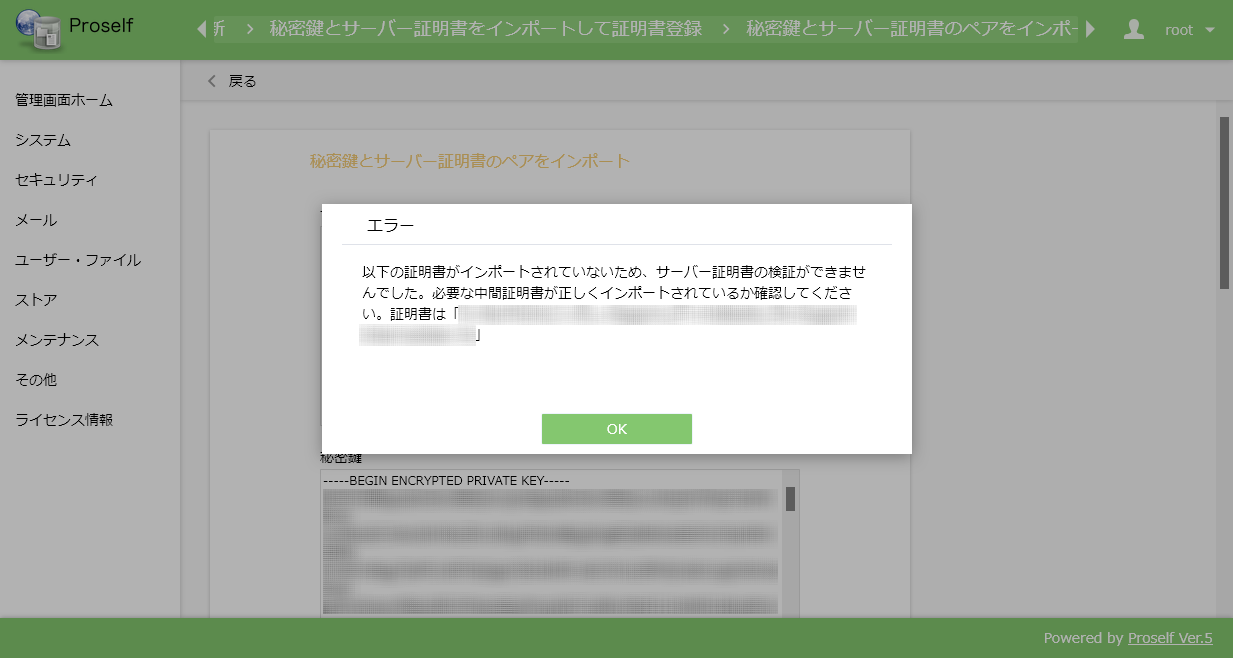
証明書の適用が完了した旨の画面が表示されますので、指示に従いブラウザを開きなおします。



**証明書の適用**

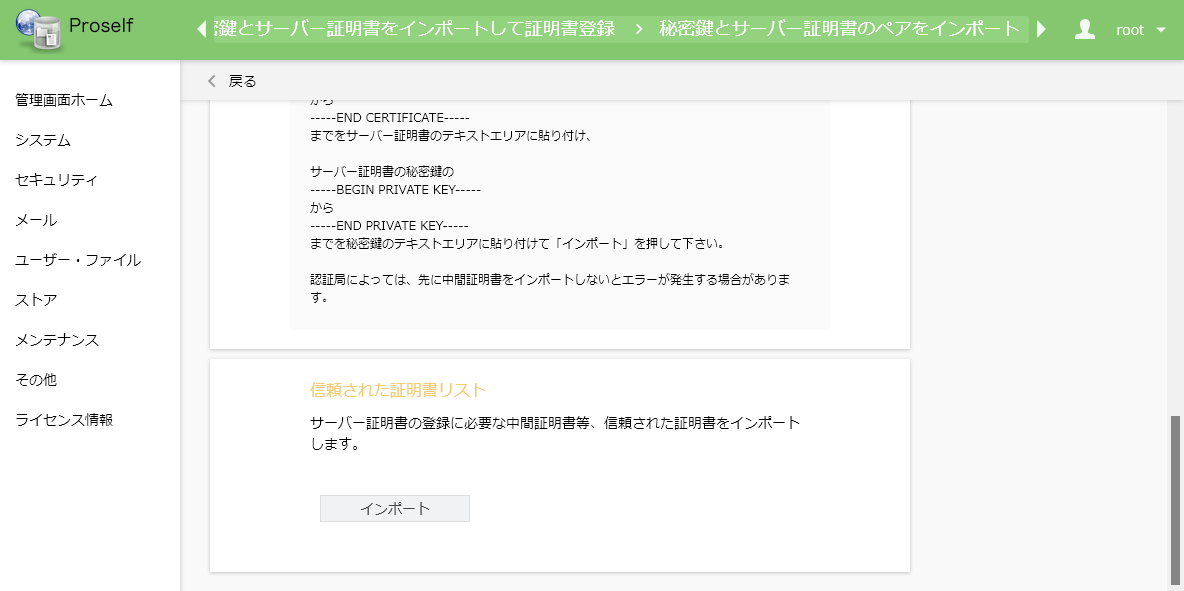
適用後は「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」を実施します。

秘密鍵とサーバー証明書のインポート実施時に以下のようなエラーが表示される場合は、中間証明書の設定が必要です。



**秘密鍵とサーバー証明書をインポート**

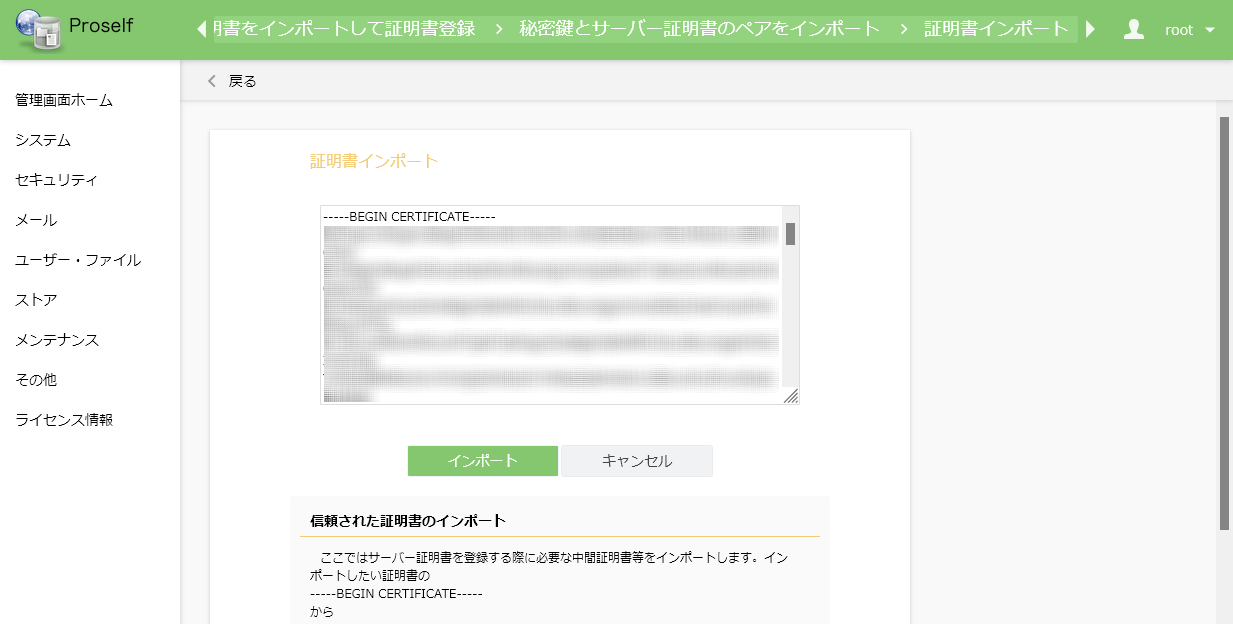
この場合は、「秘密鍵とサーバー証明書をインポート」画面内の「信頼された証明書リスト」より「インポート」をクリックします。



**秘密鍵とサーバー証明書をインポート**

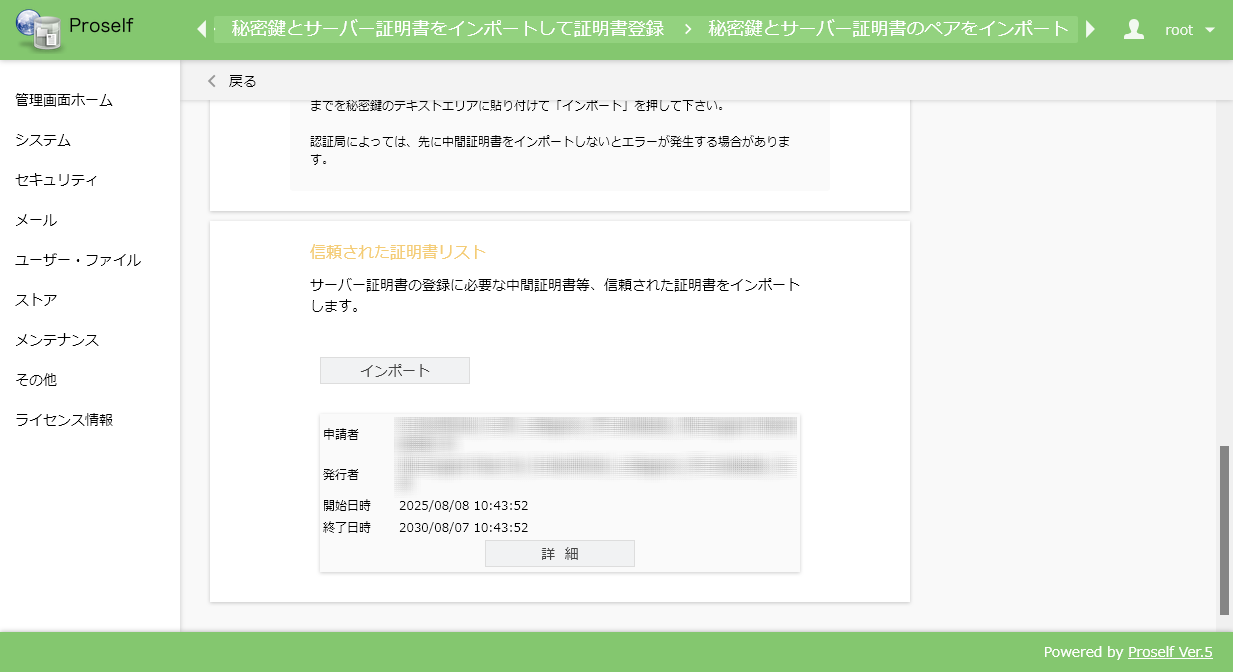
ダウンロードした中間証明書をテキストエディタで開き、中に記述されているテキストを「証明書インポート」画面内のテキストエリアにコピーして貼り付けます。

「インポート」をクリックすると中間証明書のインポートが行われます。



**信頼された証明書のインポート**

インポート完了後は「サーバー証明書」画面内の「信頼された証明書リスト」に証明書情報が表示されます。



**秘密鍵とサーバー証明書をインポート**

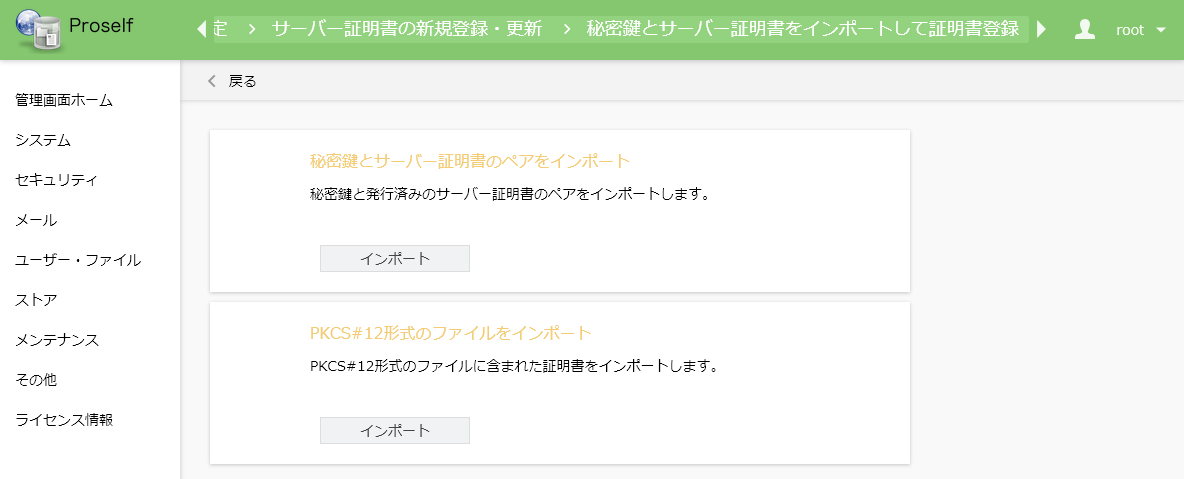
さらに中間証明書をインポートする場合は、「信頼された証明書リスト」に表示されている「インポート」をクリックして上記手順を繰り返し実施ください。

中間証明書のインポート実施完了後は、再度秘密鍵、発行済みのサーバー証明書のインポートを実施ください。

### PKCS#12形式のファイルをインポート

Proself以外で生成済みのPKCS#12形式のファイルに含まれた証明書をインポートします。

「秘密鍵とサーバー証明書をインポートして証明書登録」画面内の「PKCS#12形式のファイルをインポート」より「インポート」をクリックします。



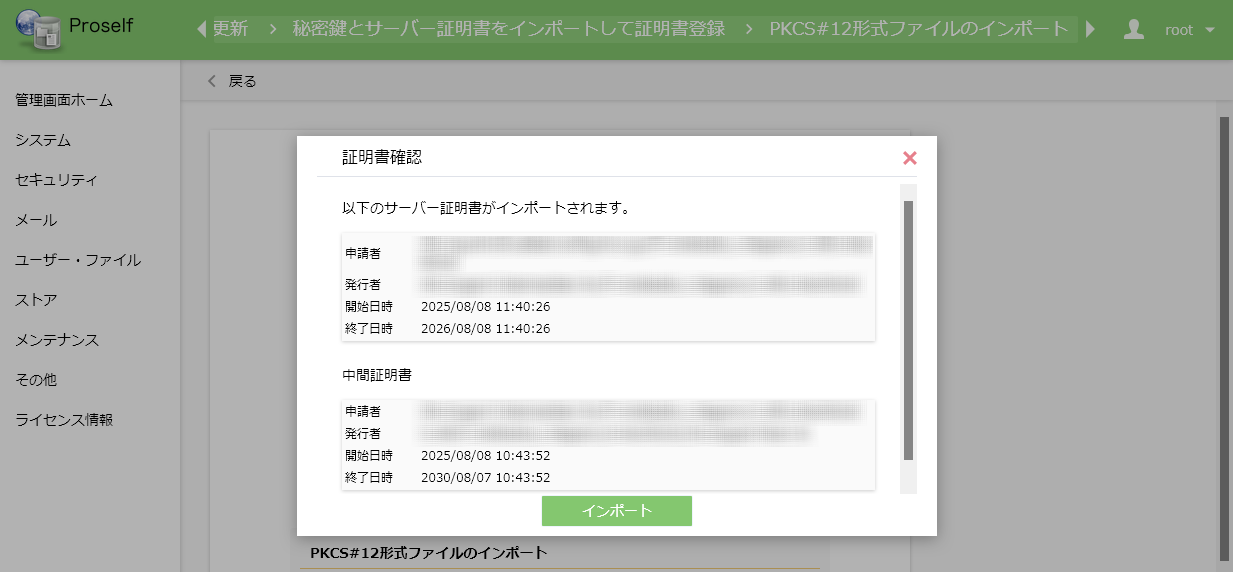
**秘密鍵とサーバー証明書をインポートして証明書登録**

「PKCS#12形式のファイルをインポート」画面より各項目の設定を行い、「インポート」をクリックします。



**PKCS#12形式のファイルをインポート**

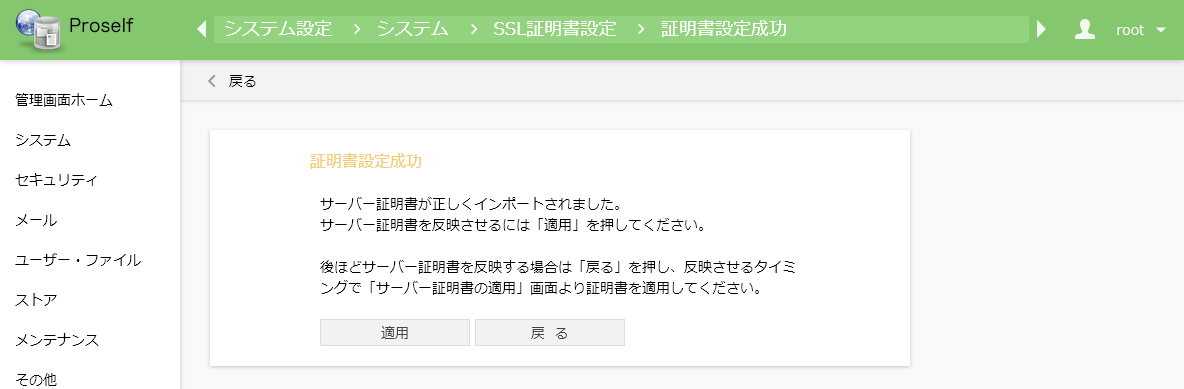
内容に問題が無い場合は以下のようなダイアログが表示されますので、「インポート」をクリックします。



**証明書確認**

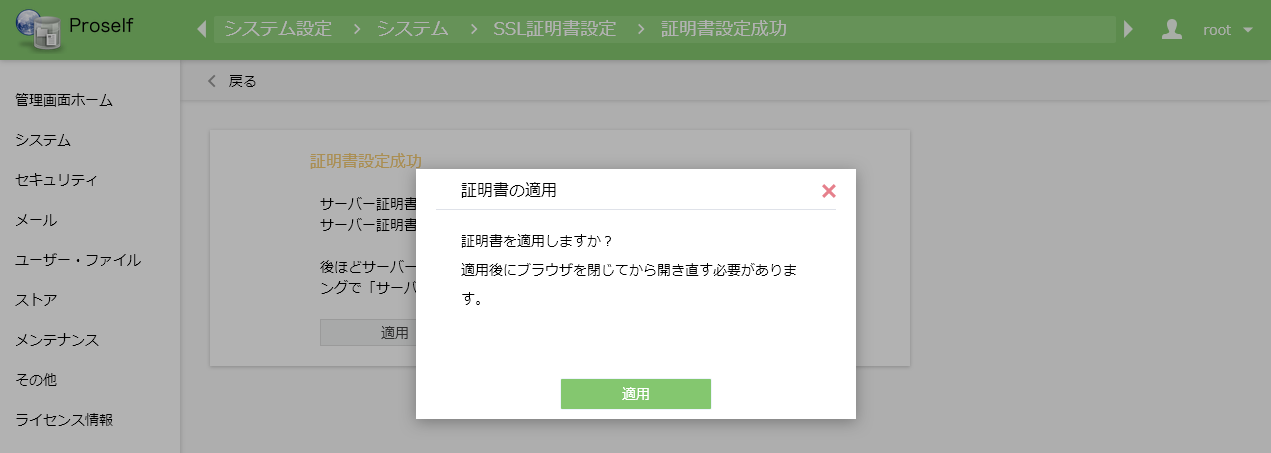
インポートが正しく行われた場合は「証明書設定成功」画面が表示されます。直ちに証明書を反映させる場合は「適用」をクリックし、証明書を後日反映させる場合は「戻る」をクリックします。

* 後日反映の手順については「[3.1.5.サーバー証明書の適用](#_SSL証明書の適用)」をご参照ください。



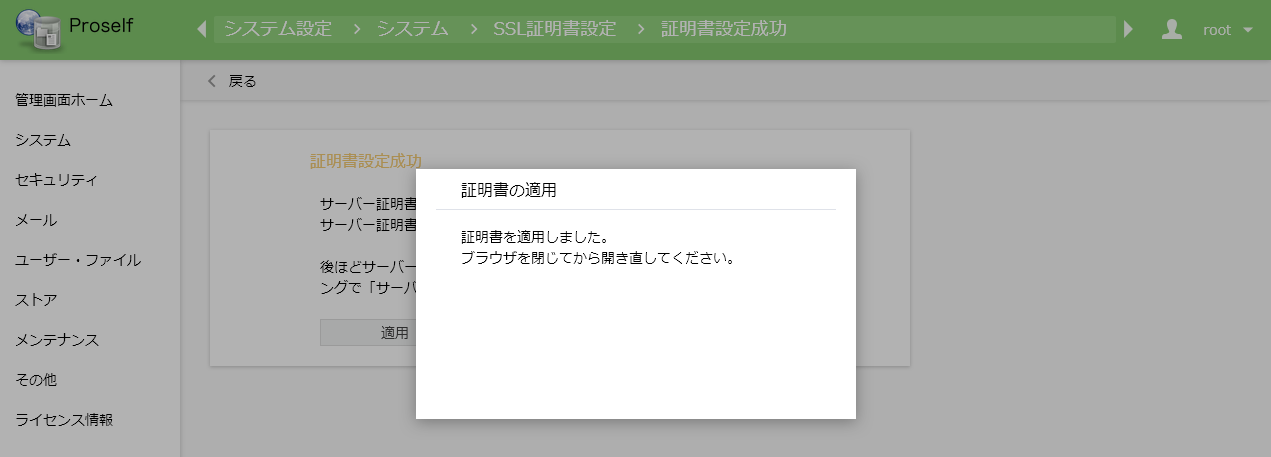
**証明書設定成功**

確認ダイアログが表示されますので、「適用」をクリックします。



**証明書の適用**

証明書の適用が完了した旨の画面が表示されますので、指示に従いブラウザを開きなおします。



**証明書の適用**

適用後は「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」を実施します。

## バックアップからサーバー証明書を適用する

過去にバックアップされたサーバー証明書を適用することができます。

* Proselfではサーバー証明書更新時に過去に適用したサーバー証明書を自動でバックアップしております。

「SSL証明書設定」画面内の「バックアップから証明書を適用」より「設定」をクリックします。



**SSL証明書設定**

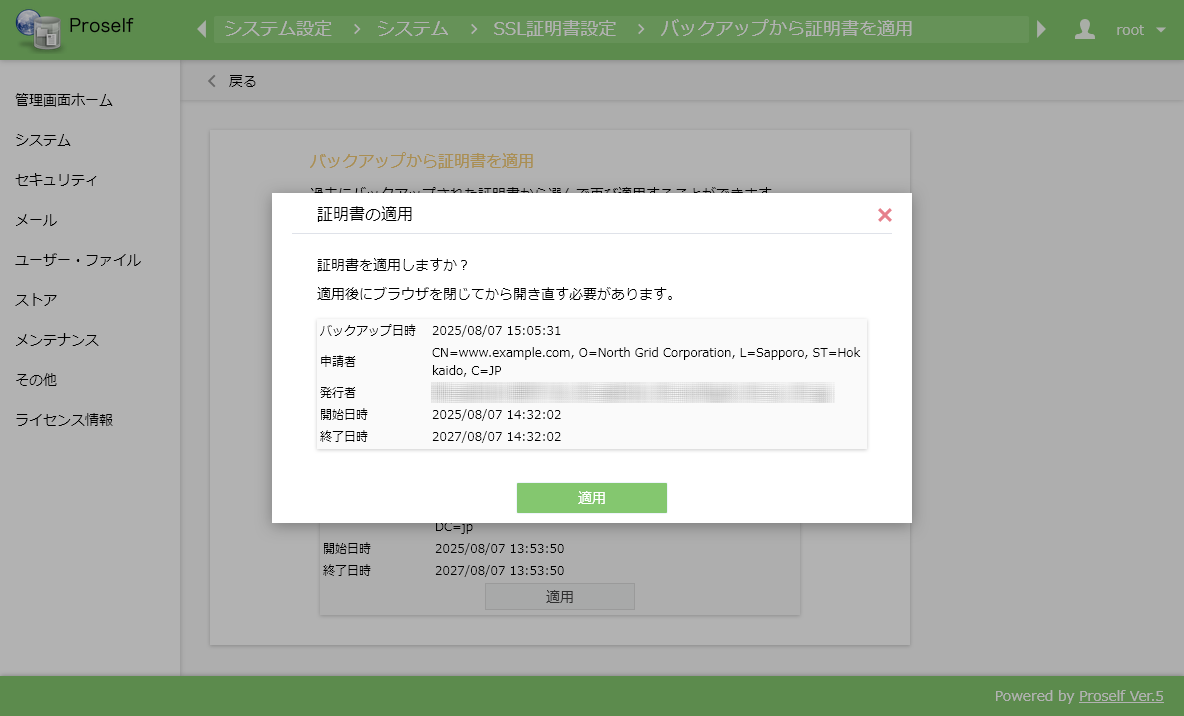
過去にバックアップされたサーバー証明書の一覧が表示されます。

適用したいサーバー証明書情報を確認の上、「適用」をクリックします。



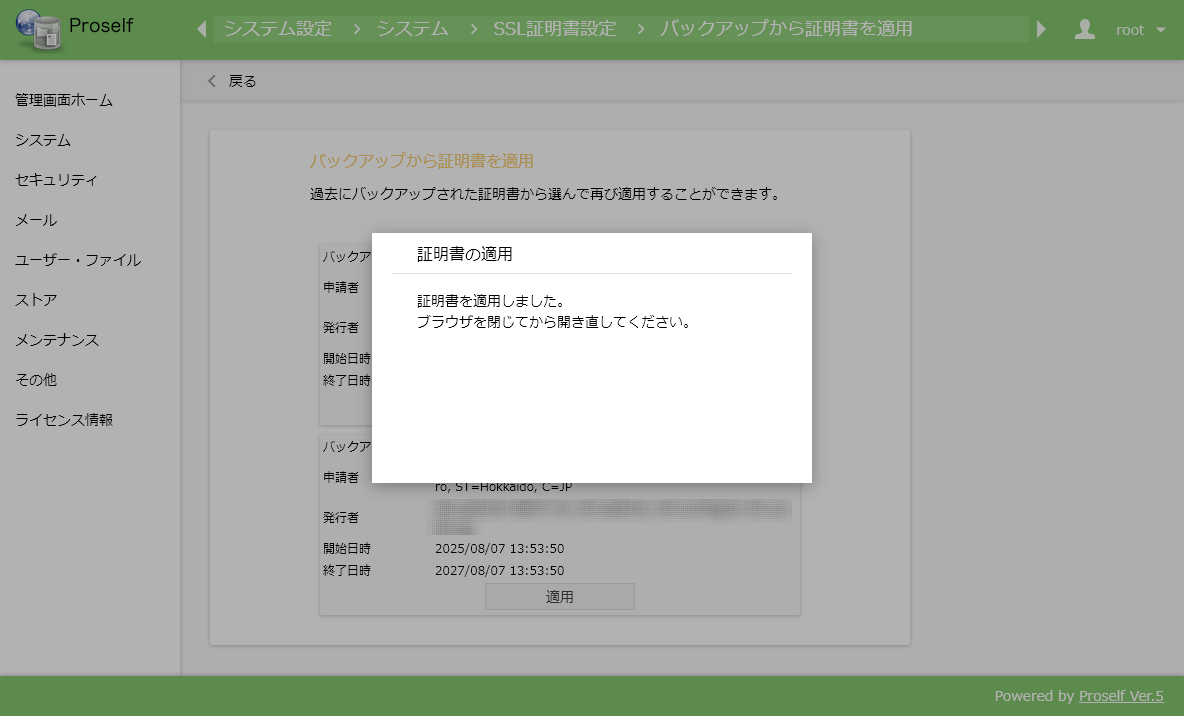
**バックアップから証明書を適用**

適用する証明書内容で問題ないことを確認後、「適用」をクリックします。



**証明書の適用**

適用後は以下のような画面が表示されますので、「[3.1.6.サーバー証明書設定後の確認](#_SSL証明書適用後の確認)」を実施します。



**証明書の適用**