

## SSL 証明書作成手順例（ご参考）

### 参考

[https://kb.swivelsecure.com/wiki/index.php/SSL\\_Certificate\\_PINsafe\\_Appliance\\_How\\_to\\_Guide](https://kb.swivelsecure.com/wiki/index.php/SSL_Certificate_PINsafe_Appliance_How_to_Guide)

証明書に利用するホスト名は VIP の NAT として登録している「userportal.xxxx.co.jp」を利用する。

Webmin 用の SSL 証明書は別物で、自己証明書を継続利用する。

キーストアは JKS であり、DER で作成され、X.509 でのインポートとする。

### 内容

1. ログイン .....	2
2. ローカル証明書の作成 .....	2
3. CSR の発行 .....	3
4. SSL 証明書の発行 .....	4
5. SSL 証明書のアップロード .....	7
6. 証明書のインポート .....	8
7. インポートの確認 .....	11
8. 古い証明書の削除 .....	12
9. Tomcat の再起動 .....	13
10. 証明書の確認 .....	13
11. Standby サーバへの証明書のインストール .....	13
12. インポートの確認 .....	14
13. Tomcat の再起動 .....	14
14. 確認 .....	15
15. 不要ファイルの削除及びクローズ .....	15

## 1. ログイン

1.1. SSH で AP-Primary へ接続する

## 2. ローカル証明書の作成

2.1. Tomcat -> 4.Certificate Management -> 1.Create a local Certificate を選択する。

```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 1
```

2.2. 鍵長を 2048bit とするために、2.2048 を選択する。

```
Swivel Maintenance (c) 2012 Primary
Create Local certificate
Certificate Key size
1. 1024
2. 2048
3. 4096
0. Exit
Select: 2
```

2.3. 下記情報を入力する。

Domain Name:\*\*\*

Company Name: \*\*\*

Department: \*\*\*

City: \*\*\*

County: \*\*\*

Country Code: \*\*\*

2.4. キーストアを確認するために 4.View keystore を選択する。

```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 4
```

- 2.5. 作成したキーストアのエイリアス「swivel」を入力し、入力項目に間違いがないことを確認する。

### 3. CSR の発行

- 3.1. Generate CSR を選択する。

```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 2
```

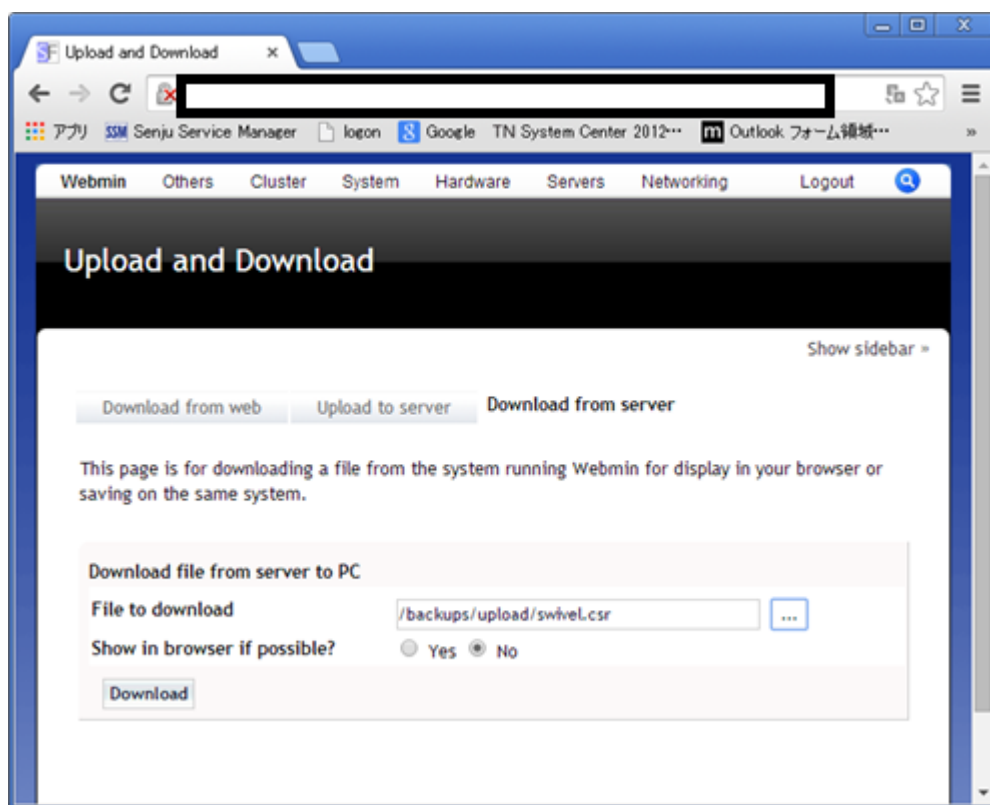
- 3.2. 先ほど作成した証明書エイリアス「swivel」を入力し、CSR が「/backup/upload/」配下に作成されたことを確認する。

```
Swivel Maintenance (c) 2012 Primary
Generate CSR
Alias name: swivel
Alias name: selfsigned

Enter Certificate name to create CSR for: swivel
CSR created in /backups/upload/swivel.csr

Press Return to Continue
```

- 3.3. CSR をダウンロードするために Webmin (<https://AP-Primary:10000>)へログインする。
- 3.4. Others -> Upload and Download をクリックする。
- 3.5. Download from server を選択し、File to download の...から先ほど作成された CSR ファイルを選択し、Download をクリックして CSR を保存する。



- 3.6. File to download の...から/home/swivel と辿り、.keystore ファイルが存在していることを確認する。

Directory of /home/swivel/

..	4 kB	27/May/2011	11:26
<a href="#">.bash_logout</a>	24 bytes	21/Feb/2012	01:55
<a href="#">.bash_profile</a>	191 bytes	21/Feb/2012	01:55
<a href="#">.bashrc</a>	124 bytes	21/Feb/2012	01:55
<a href="#">.canna</a>	5.49 kB	21/Feb/2012	01:55
<a href="#">.keystore</a>	3.58 kB	24/Jun/2014	20:45
<a href="#">.keystore.240614.1403610299</a>	1.35 kB	24/Jun/2014	20:44
<a href="#">swivel</a>	4 kB	02/Jun/2014	20:43
<a href="#">swivelportal</a>	4 kB	04/Jun/2014	17:20

Ok /home/swivel

#### 4. SSL 証明書の発行

- 4.1. SSL 発行 Web 画面にアクセスし、新規作成の「進む」をクリックする。



ヘルプ

新規申請 証明書の選択:

**更新** ご利用中の証明書の更新については、事前に有効期限の90日前から更新が可能です

**再発行** 秘密鍵がなんらかの理由で使用できなくなった場合、申請のミスなどにより証明書の記載情報に誤りがある場合には、再発行が可能です

**失効** 証明書の危険化が発生した場合には証明書の失効を行います

**検索** 申請者の電子メールアドレスか、証明書のコモンネームにより証明書の検索が可能です

**FAQ** マネージドPKI for SSLについてはこちら

管理画面 | メール | Copyright © Symantec Corporation. All rights reserved.



- 4.2. 申請者情報を入力する。
- 4.3. サーバソフトウェアおよび CSR で「サーバソフトウェアを選択してください」で IIS 以外のサーバを選択し、「CSR ファイルのアップロード」を選択した後、先ほどダウンロードした CSR ファイルを選択する。
- 4.4. 証明書署名アルゴリズムで「SHA-1 with RSA」を選択する。

#### 証明書署名アルゴリズム

証明書の署名の作成に使うアルゴリズムを選択します。アカウントの設定によっては、この証明書に別の鍵の種類と署名アルゴリズムが含まれる複数のバージョンを要求できることがあります。

適切なアルゴリズムが何か不明ですか? 詳しくは[ここをクリック](#)してください。

- SHA-1 with RSA - **重要:**2017 年 1 月 1 日より前に期限切れにする必要があります。
- SHA-256 with RSA 暗号化
- DSA with SHA-256

- 4.5. 証明書の取得オプションでサーバライセンス数 2、有効期限 1 年とする。

#### 証明書の取得オプション

この証明書をホストするサーバの数を入力して下さい。

サーバライセンス数

有効期間:  1年  2年  3年  4年

**重要:**業界標準では SHA-1 SSL 証明書を 2017 年 1 月 1 日より前に終了させる必要があります。

- 4.6. チャレンジフレーズで「\*\*\*」と入力する。

**チャレンジフレーズ**

チャレンジフレーズを入力してください。チャレンジフレーズとは更新／再発行の際に利用するパスワードになります。チャレンジフレーズは半角英数で入力してください。以下の条件を満たす強力なチャレンジフレーズを入力してください。

- 8文字以上であること。
- 大文字・小文字が混在すること。
- 数字を1文字以上使用すること。
- 少なくとも以下の特殊文字を1つ使用すること。( !~!@#%&\*()\_+`{|}~<.>?:;/ )

\* チャレンジフレーズ:  strength: strong

\* チャレンジフレーズの再入力:

4.7. 証明書利用規約で「同意する」をクリックする。

**証明書利用規約**

印刷向け

利用者は、本規約の定義によるところの再販業者からサービスを受けようとする場合、再販業者に証明書の申請、受領、インストール、管理、更新および必要に応じて失効を代行する許可を与えていることを表明し、保証することとします。再販業者に利用者の証明書の使用許可を与えることにより、本規約の条件に拘束されることとなります。本規約の条件に同意しない場合は、下記の第24条に記載されたペリサインの連絡先にすぐに連絡してください。ペリサインにより証明書は失効される場合があります。利用者が、顧客から証明書の代理申請の許可を受けた再販業者である場合、第8.2条および第8.3条に従って、表明および保証を行います。利用者が、自らの証明書を申請する再販業者である場合は、第8.2条および第8.3条に従って、表明および保証を行います。

4.8. 完了画面を確認し、メールが来るのを待つ。


**Net One Systems Co., Ltd. - Information Technology Department**  
 ペリサイン マネージドPKI for SSL サービス

日本語 ▾

---

**申請が完了しました**

Net One Systems Co., Ltd. 向け サーバIDの申請が完了いたしました。確認メールが届きますのでご確認ください。

管理者は申請情報に基づき承認を行います。承認作業が完了いたしますとメールにて サーバIDとインストールに関する案内が届きます。

ご質問がありましたら、[管理者](#)にご連絡ください。

管理者 | ニュース | Copyright © Symantec Corporation. All rights reserved.

  
 powered by Symantec

4.9. <https://www.verisign.co.jp/repository/intermediate.html> へアクセスし、セキュア・サーバ ID 用中間 CA 証明書、クロスルート設定用証明書をコピーし、ファイル化する。

### Class 3 中間CA証明書

#### サーバID・EV SSL証明書

	中間CA証明書 (三階層目・各製品専用)	クロスルート設定用証明書 (二階層目・製品共通)
グローバル・サーバID EV	グローバル・サーバID用中間CA証明書	クロスルート設定用証明書
セキュア・サーバID EV	セキュア・サーバID用中間CA証明書	
グローバル・サーバID	グローバル・サーバID用中間CA証明書	
セキュア・サーバID	セキュア・サーバID用中間CA証明書	

#### セキュア・サーバID用中間CA証明書

ツイートする いいね! 0



#### 注意

- 以下は、2010年10月10日の仕様変更以降に申請されたセキュア・サーバIDでご利用いただく中間CA証明書です。  
(ストアフロント、マネージドPKI for SSL共通)  
携帯電話端末を含め、より幅広いSSL接続クライアントからのアクセスを可能とするために、[クロスルート設定用証明書](#)を併せてインストールしてください。
- 証明書仕様**  
公開鍵鍵長: 2048bitRSA  
署名アルゴリズム: SHA-1  
有効期限: 2020年2月7日(GMT)  
Subject:  
CN = VeriSign Class 3 Secure Server CA - G3  
OU = Terms of use at https://www.verisign.com/rpa(c)10  
OU = VeriSign Trust Network  
O = VeriSign, Inc.  
C = US  
Serial Number: 6e cc 7a a5 a7 03 20 09 b8 ce bc f4 e9 52 d4 91  
Certificate SHA1 Fingerprint: 5d eb 8f 33 9e 26 4c 19 f6 68 6f 5f 8f 32 b5 4a 4c 46 b4 76

#### 全て選択

```
-----BEGIN CERTIFICATE-----
MIIF7DCCBNSgAwIBAgIQbsx8pacDIAm4zrz06VLUKTANBghkhiG9wOBAOUFADCB
yIELMAKGA1UEBhMCVWxZAVBgnVBAoTDIzIcmITaWduLCEBjbmMuMR9wHOYDVOQL
EzZlZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZj
U21nbWVzZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZj
ZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZk
aG9yaXR5IENBZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZj
MAKGA1UEBhMCVWxZAVBgnVBAoTDIzIcmITaWduLCEBjbmMuMR9wHOYDVOQLExZ
ZXJpU21nbWVzZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZj
aHR0cHM6Ly93ZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZj
aYNoZ24gQ2xhc3MgYm90ZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZjZkZj
DEBAQIAA41BDwAwggEKAoIBAQCxh40fWgxF9byrJZenral+nLr2wTm418rCrFbG
5bt1jkrPtc5v70IKIK9OEJxoiy8Ve4mbEBrINDTBR1vzSxt1g01BdNGIeGwGU/m8
fDMv1gzgzsChewDEBRJK2GfWQ63HRKNKEdCuqWHQsV/KNL085jIND4LQyUlhDK
tpo3yus3nABINyYpUHjorWPNGUFP9Zxse5jUxHGzUL4os4+guVoc9cosI6n9FAbo
GLSa6Dxugf3kzT2s1HTaewSuI Zub5tXxYsU5w7Hn01KWGrJTCw/EbGuHGeBy0RV
M51/JJs/UVV/hhrzPPptf4H1uErT8YU3HLWm0AnkGHs4TvoPAGMBAAGIggHfMIIB
2zA0BgggrBGFEBQcBAQQoMcywJAYIKwYBBQUHMAAGGgGh0dHABLy9vY3NwLnZlcmIz
aWduLnNvbTASBgNVHRMBAf8ECDAGAQH/AgEAMHAGA1UdIARpMGcwZQVLYlZlAYb4
```

4.10. SSL 証明書管理者からメールでサーバ証明書が届くので、保存する。

## 5. SSL 証明書のアップロード

5.1. Webmin 上で Others -> Upload and Download をクリックする。

5.2. Upload to server を選択し、File to upload よりメールできたサーバ証明書、セキュア・サーバ ID 用中間 CA 証明書、クロスルート設定用証明書を選択し、File or directory to upload to に「/backups/upload」と入力し、Upload をクリックする。

5.3. アップロードが完了した画面を確認する。

## 6. 証明書のインポート

中間証明書より先にサーバ署名書を入れないようにする。

サーバ証明書インストール時、下記のエラーが出ても既存のエイリアスを削除しては  
いけない。

"Please delete the existing certificate, before generating a new one"

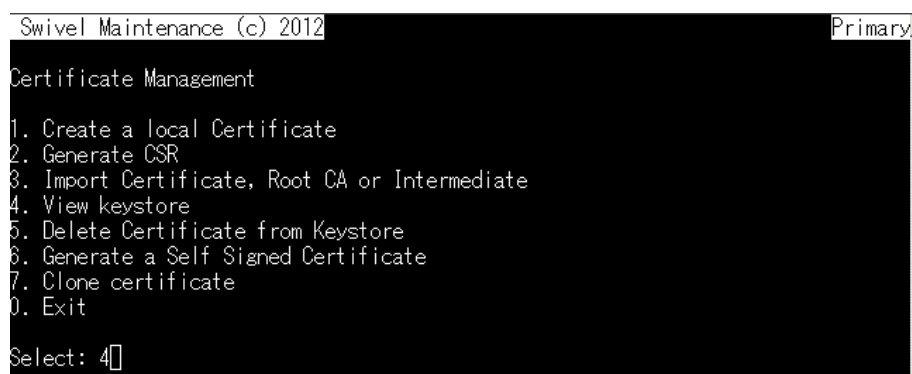
上記エラーが発生した場合はコマンドラインから下記のコマンドを入力する。

```
keytool -importcert -keystore /home/swivel/.keystore -alias swivel -file  
/backups/upload/response.txt -trustcacerts
```

詳細は下記 URL の 4. Import the Certificate に記載があるため、必ず確認する。


[https://kb.swivelsecure.com/wiki/index.php/SSL\\_Certificate\\_PINsafe\\_Appliance\\_How\\_to\\_Guide](https://kb.swivelsecure.com/wiki/index.php/SSL_Certificate_PINsafe_Appliance_How_to_Guide)

- 6.1. SSH 接続した AP-Primary 上で、1.Tomcat ->4.Certificate Management -> 4.View keystore を選択する。



```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 4
```

- 6.2. 既存のエイリアスを確認し、Enter キーを押して Certificate Management 画面まで戻る。



```
Swivel Maintenance (c) 2012 Primary
View Keystore
Alias name: swivel
Alias name: selfsigned
Enter Certificate name to view, or Return for all Certificates:
```

- 6.3. Import Certificate, Root CA or Intermediate を選択する。



```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 3
```

- 6.4. アップロードしたクロスルート証明書のファイル名を入力する。

```
Swivel Maintenance (c) 2012 Primary
Import Certificate
#####
## Upload your Certificate response, Root CA or Intermediate file ##
## to /backups/upload ##
#####
Enter the filename of the file you uploaded: cross-root.cer
```

- 6.5. 先に確認したエイリアス以外のエイリアスを任意で入力し、Yes と入力し、証明書がキーストアに追加されたことを確認する。

```
Swivel Maintenance (c) 2012 Primary
Import Certificate
#####
## Upload your Certificate response, Root CA or Intermediate file ##
## to /backups/upload ##
#####
Enter the filename of the file you uploaded: cross-root.cer
Enter a unique alias name: veri-cr-140625
Are you sure? (Yes/No): Yes
Certificate was added to keystore
Press Return to Continue.
```

- 6.6. Import Certificate, Root CA or Intermediate を選択する。

```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 3
```

- 6.7. アップロードしたセキュア・サーバ ID 用中間 CA 証明書のファイル名を入力する。

```
Swivel Maintenance (c) 2012 Primary
Import Certificate
#####
## Upload your Certificate response, Root CA or Intermediate file ##
## to /backups/upload ##
#####
Enter the filename of the file you uploaded: secure-server-id.cer
```

- 6.8. 先に確認したエイリアス及び先ほど入力した以外のエイリアスを任意で入力し、Yes と入力し、証明書がキーストアに追加されたことを確認する。

```
Swivel Maintenance (c) 2012 Primary
Import Certificate
#####
## Upload your Certificate response, Root CA or Intermediate file ##
## to /backups/upload ##
#####
Enter the filename of the file you uploaded: secure-server-id.cer
Enter a unique alias name: veri-ss-140625
Are you sure? (Yes/No): Yes
Certificate was added to keystore
Press Return to Continue.
```

- 6.9. 3.Import Certificate, Root CA or Intermediate を選択する。

```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 3
```

- 6.10. アップロードしたサーバ証明書のファイル名を入力する。

```
Swivel Maintenance (c) 2012 Primary
Import Certificate
#####
## Upload your Certificate response, Root CA or Intermediate file ##
## to /backups/upload ##
#####
Enter the filename of the file you uploaded: _____ .cer
```

- 6.11. **CSR 発行時に利用したエイリアス swivel を入力**し、Yes を入力し、証明書がキーストアにインストールされたことを確認する。

```
Swivel Maintenance (c) 2012 Primary
Import Certificate
#####
## Upload your Certificate response, Root CA or Intermediate file ##
## to /backups/upload ##
#####
Enter the filename of the file you uploaded: _____ .cer
Enter a unique alias name: swivel
Are you sure? (Yes/No): Yes
Certificate reply was installed in keystore
Press Return to Continue.
```

## 7. インポートの確認

- 7.1. View keystore を選択する。

```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 4
```

- 7.2. 先ほど作成したエイリアス名をそれぞれ入力する。

```
Swivel Maintenance (c) 2012 Primary
View Keystore
Alias name: veri-cr-140625
Alias name: veri-ss-140625
Alias name: swivel
Alias name: selfsigned
Enter Certificate name to view, or Return for all Certificates: swivel
```

- 7.3. サーバ証明書の場合、Entry type が PrivateKeyEntry、Certificate chain length がインポートした証明書数+1(今回の場合、3つの証明書をインポートしたので4)とな

っていることを確認する。

```
Enter Certificate name to view, or Return for all Certificates: swivel
Alias name: swivel
Creation date: 25-Jun-2014
Entry type: PrivateKeyEntry
Certificate chain length: 4
```

- 7.4. セキュア・サーバ ID 用中間 CA 証明書、クロスルート設定用証明書のエイリアスの場合は、Entry type が trustedCertEntry となっていることを確認する。

```
Enter Certificate name to view, or Return for all Certificates: veri-cr-140625
Alias name: veri-cr-140625
Creation date: 25-Jun-2014
Entry type: trustedCertEntry
```

## 8. 古い証明書の削除

前のエイリアス名の証明書が新しい証明書より先に読み込まれる場合があるので、前のエイリアス名の証明書は必ず削除する。

- 8.1. Webmin より、Others -> Upload and Download をクリックする。  
8.2. File to download の...から/home/swivel と辿り、.keystore のバックアップファイルが存在していることを確認する。

Directory of /home/swivel/

Icon	File Name	Size	Modified	Permissions
Folder	..	4 kB	27/May/2011	11:26
File	<a href="#">.bash_logout</a>	24 bytes	21/Feb/2012	01:55
File	<a href="#">.bash_profile</a>	191 bytes	21/Feb/2012	01:55
File	<a href="#">.bashrc</a>	124 bytes	21/Feb/2012	01:55
File	<a href="#">.canna</a>	5.49 kB	21/Feb/2012	01:55
File	<a href="#">.keystore</a>	10.03 kB	25/Jun/2014	18:08
File	<a href="#">.keystore.250614.1403655951</a>	1.35 kB	25/Jun/2014	09:25
File	<a href="#">.keystore.250614.1403686203</a>	3.58 kB	25/Jun/2014	17:50
File	<a href="#">.keystore.250614.1403686546</a>	4.83 kB	25/Jun/2014	17:55
File	<a href="#">.keystore.250614.1403687303</a>	6.35 kB	25/Jun/2014	18:08

Ok /home/swivel

- 8.3. SSH 上の AP-Primary で、5.Delete Certificate from Keystore を選択する。

```
Swivel Maintenance (c) 2012 Primary
Certificate Management
1. Create a local Certificate
2. Generate CSR
3. Import Certificate, Root CA or Intermediate
4. View keystore
5. Delete Certificate from Keystore
6. Generate a Self Signed Certificate
7. Clone certificate
0. Exit
Select: 5
```

- 8.4. selfsigned と入力し、Yes と入力する。

```
Swivel Maintenance (c) 2012 Primary
Delete Keystore

Alias name: veri-cr-140625
Alias name: veri-ss-140625
Alias name: swivel
Alias name: selfsigned

Enter certificate Alias to delete: selfsigned

Are you sure? (Yes/No): Yes

Press Return to Continue
```

- 8.5. 4.View keystore を選択し、エイリアスに self-signed が無いことを確認し、Enter を押す。

```
Swivel Maintenance (c) 2012 Primary
View Keystore

Alias name: veri-cr-140625
Alias name: veri-ss-140625
Alias name: swivel

Enter Certificate name to view, or Return for all Certificates: 
```

## 9. Tomcat の再起動

- 9.1. Exit->2.Restart と進み、Yes と入力する。

```
Swivel Maintenance (c) 2012 Primary
Tomcat : Running

1. Stop
2. Restart
3. HTTPS/HTTP
4. Certificate Management
0. Main Menu

Select: 2

Are you sure? (Yes/No): Yes
```

- 9.2. 再起動後、Tomcat が Running となっていることを確認する。

```
Swivel Maintenance (c) 2012 Primary
Tomcat : Running

1. Stop
2. Restart
3. HTTPS/HTTP
4. Certificate Management
0. Main Menu

Select: 
```

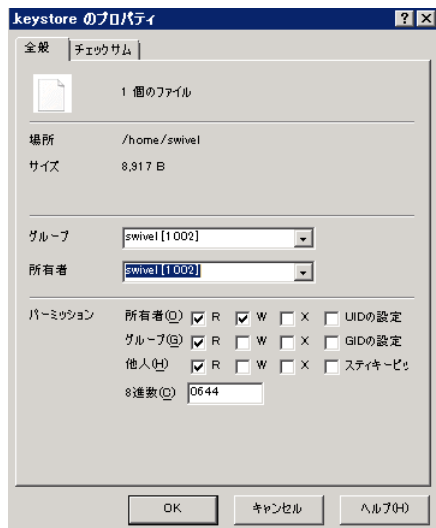
## 10. 証明書の確認

- 10.1. 社外より <https://userportal.xxxx.co.jp:8443/proxy/SCImage?username=test> へアクセスし、証明書が正しくインストールされていることを確認する。

## 11. Standby サーバへの証明書のインストール

- 11.1. WinSCP を開き、AP-Primary へ接続する。

- 11.2. /home/swivel/.keystore ファイルをローカルにコピーする。
- 11.3. WinSCP を開き、AP-Standby へ接続する。
- 11.4. AP-Standby 上の.keystore ファイルをリネームする。
- 11.5. 先ほどローカルにコピーした.keystore ファイルを/home/swivel/へコピーする。
- 11.6. AP-Standby 上の.keystore ファイルを右クリックし、プロパティを開き、グループおよび所有者を swivel とする。



## 12. インポートの確認

- 12.1. SSH で AP-Standby へログインする。
- 12.2. Tomcat -> 4.Certificate Management -> 4.View keystore を選択し、AP-Primary と同じエイリアスがあることを確認する。

```
Swivel Maintenance (c) 2012 Standby
View Keystore
Alias name: veri-cr-140625
Alias name: veri-ss-140625
Alias name: swivel
Enter Certificate name to view, or Return for all Certificates: []
```

## 13. Tomcat の再起動

- 13.1. Tomcat -> 2.Restart を選択し、Yes と入力する。

```
Swivel Maintenance (c) 2012 Standby
Tomcat : Running
1. Stop
2. Restart
3. HTTPS/HTTP
4. Certificate Management
0. Main Menu
Select: 2
Are you sure? (Yes/No): Yes[]
```

## 14. 確認

14.1. 社内より <https://AP-Standby:8080/pinsafe> を開き、証明書を確認する。

## 15. 不要ファイルの削除及びクローズ

15.1. AP-Primary を開いている WinSCP で、「/backups/upload」ディレクトリを開き、CSR、サーバ証明書、セキュア・サーバ ID 用中間 CA 証明書、クロスルート設定用証明書を削除する

以上