Ver.1.6

証明書自動発行支援システム

サーバ証明書

インストールマニュアル

Tomcat(JavaKeytool)編

2012/3/30

国立情報学研究所

改版履歴			
版数	日付	内容	担当
V.1.0	2009/5/15	初版	NII
V.1.1	2009/7/13	誤植の修正	NII
V.1.2	2009/9/11	誤植の修正	NII
V.1.3	2009/10/13	DN 使用可能文字拡張 誤植の修正	NII
V.1.4	2011/2/28	サーバ証明書インストールマニュアルに IIS7.0・IIS7.5 を追加 DN のルール記載変更	NII
V.1.5	2011/6/3	文言の統一	NII
V.1.6	2012/3/30	暗号アルゴリズムのセキュリティ対応に伴いサーバ証明書および CSR の鍵長 1024 ビット記載削除	NII

目次

1.はじめに

証明書自動発行支援システムサーバ証明書インストールマニュアル Tomcat(JavaKeytool)編（以下、「本マニュアル」）は、UPKI オープンドメイン証明書自動発行検証プロジェクト（以下、「プロジェクト」）から発行された証明書を Tomcat で使用するための CSR の作成方法、発行したサーバ証明書をインストールする方法について記載します。

1-1.CSR とは

CSR（証明書発行要求：Certificate Signing Request）は証明書を作成するための元となる情報で、その内容には、加入者が管理する SSL/TLS サーバの組織名、Common Name（サーバの FQDN）、公開鍵などの情報が含まれています。NII では、加入者に作成いただいた CSR の内容を元に、証明書を作成します。CSR ファイルは通常 PEM 形式で表示されます。CSR を PEM 形式で表示したフォーマットは以下のようなものとなります。

CSR の例

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCSlAxEDAOBgNVBAcTB0FjYWRlbWUxKjAo
BgNVBAoTIU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczEiMCAGA1UE
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze
BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG7ORkIss4ST6PDF+RQw+TRdkzl8TUF
-----END CERTIFICATE REQUEST-----
```

1-2.キーストアとは

キーストア（Key Store）は鍵と証明書を保管するためのデータベースファイルです。ファイル全体がパスワードによって暗号化されており、また鍵の保管区域である エントリと呼ばれる領域も個別のパスワードで保護することができます。キーストア内のすべての鍵と証明書は alias という別名で管理されています。

1-3.他のサーバ証明書インストールマニュアルとの比較について

本マニュアルでは、各サーバで使用する鍵ペア、CSR生成ツールとして、【鍵ペア生成時の共通事項】に記述したツールを使用して説明します。

また、各サーバへインストールする必要がある証明書を【サーバ証明書インストールに必要となる証明書一覧】に記述します。

【鍵ペア生成時に利用するツール】

○・・・該当する　　-・・・該当しない

	Openssl	JavaKeytool	iKeyman
Apache1.3 系+mod_ssl	○	-	-
Apache2.0 系+mod_ssl	○	-	-
Apache-SSL	○	-	-
Tomcat	-	○	-
IBM HTTP Server	-	-	○
IIS5.0	○	-	-
IIS6.0	○	-	-
IIS7.0	○	-	-
IIS7.5	○	-	-

【サーバ証明書インストールに必要となる証明書一覧】

○・・・該当する　　-・・・該当しない

	ルート CA 証明書	中間CA証明書	サーバ証明書
Apache1.3 系+mod_ssl	-	○	○
Apache2.0 系+mod_ssl	-	○	○
Apache-SSL	-	○	○
Tomcat	○	○	○
IBM HTTP Server	○	○	○
IIS5.0	○	○	○
IIS6.0	-	○	○
IIS7.0	-	○	○
IIS7.5	-	○	○

1-4.本書の範囲

本書では以下の(f、g)の作業について記述をします。

マニュアル名	内容
操作手順書（加入者用）	a. 加入者が実施する本システムへのサーバ証明書発行申請・取得について（2 章に記載） b. 加入者が実施する本システムへのサーバ証明書更新申請・取得について（3 章に記載） c. 加入者が実施する本システムへのサーバ証明書失効申請について（4 章に記載） d. 本システムへの証明書アップロードフォーマットについて(５章に記載)
サーバ証明書インストールマニュアル※1	e. ＣＳＲと鍵ペアの作成方法について f. サーバ証明書のインストール方法について

※1 以下のマニュアルを総称して「サーバ証明書インストールマニュアル」と呼びます。

- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IBM HTTP Server 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Tomcat(JavaKeytool)編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache-SSL 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache2.0 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache1.3 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS7.0・IIS7.5 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS6.0 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS5.0 編

2.Tomcat(JavaKeytool)によるサーバ証明書の利用

2-1.前提条件

Tomcat(JavaKeytool)でサーバ証明書を使用する場合の前提条件について記載します。適時、サーバ証明書をインストールする加入者様の環境により、読み替えをお願いします。(本マニュアルでは Redhat Enterprise Linux ES release4、Java 2 Runtime Environment、Standard Edition(build 1.4.2)、Tomcat5.0 での実行例を記載しております。

前提条件
1. Tomcat(JavaKeytool)がインストールされていること(対応:4.0～6.0)
2. 使用中の Tomcat(JavaKeytool)に最適な J2SE がインストールされていること(J2SE1.4 以降を前提とする)]
3. tomcat の設定ファイル server.xml ファイルまでの絶対パス:$CATALINA_HOME/conf/server.xml
※Tomcat6.0 系でサポートしているサーブレット 2.5 に対応するためには、J2SE5.0 以上が必要です

CSR 作成時は既存の鍵ペアは使わずに、必ず新たに CSR 作成用に生成した鍵ペアを利用してください。更新時も同様に、鍵ペアおよび CSR を新たに作成してください。鍵ペアの鍵長は2048bit にしてください。

2-2.事前準備

鍵ペア・CSR を生成する前に、事前に以下の項目の準備をしてください。

事前準備
1. キーストアファイル名:<*server_yyyymmdd.keystore*>(「2-3-1、2-3-2、2-5-2、2-5-3、2-5-4」で使用) 例)server_20090401.keystore
2. サーバ DN(※サーバ DN については、本プロジェクト証明書ポリシまたは、下記 DN のルールをご確認ください):<*サーバ DN*>(「2-3-1」で使用) 例)CN=www.nii.ac.jp, OU=Cyber Science Infrastructure Development Department, O=National Institute of Informatics, L=Academe2, C=JP
3. 鍵ペア alias 名:<*tomcat*>(「2-3-1、2-3-2、2-5-4」で使用) 例)tomcat
4. 鍵ストア・パスワード:<*keystore_pass*>(「2-3-1、2-3-2、2-5-2、2-5-3、2-5-4」で使用) 例)changeit ※tomcat の設定ファイルの初期値で changeit と記述されているため changeit を設定することにより、設定ファイルの変更を省略することができます。
5. 鍵のパスワード:<*key_pass*>(「2-3-1 キーストアの生成」で使用) 例)changeit

6. CSR ファイル名：<***servername.csr***>（「2-3-2 CSR の生成」で使用）

CSR に記述する DN のルールは以下のとおりとなります。

DN のルール			
項目	指定内容の説明と注意	必須	文字数および注意点
Country(C)	本認証局では必ず「JP」と設定してください。 例） C=JP	○	JP 固定
State or Province Name(ST)	本認証局では使用しないでください。	×	
Locality Name(L)	本認証局では必ず「Academe2」と設定してください。 例)L=Academe2	○	Academe2 固定
Organization Name(O)	プロジェクト参加申請時の機関名英語表記を設定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例)O=National Institute of Informatics	○	半角の英数字 64 文字以内 (記号は「' (),-./:=」と半角スペースのみ使用可能)
Organizational Unit Name(OU)	証明書を使用する部局等の名前を設定してください。 （この値は省略可能です） （この値は複数設定することが可能です。複数指定する方法につきましては、CSR 作成時ご使用のアプリケーションのマニュアルをご確認ください。） 例)OU=Cyber Science Infrastructure Development Department	△	・半角の英数字 64 文字以内 (記号は「' (),-./:=」と半角スペースのみ使用可能) ・複数 OU を指定する場合は、全体で 64 文字以内
Common Name(CN)	サーバ証明書 URL に表示されるウェブ・サーバの名前を FQDN で設定してください。例えば SSL/TLS を行うサイトが https://www.nii.ac.jp の場合には、「www.nii.ac.jp」となります。FQDN にはプロジェクト参加申請時に登録いただいた対象ドメイン名を含む FQDN のみ、証明書発行が可能となります。 例)www.nii.ac.jp	○	証明書をインストールする対象サーバの FQDN で 64 文字以内 半角英数字、”.“、“-”のみ使用可能。 また、先頭と末尾に“.”と“-”は使用不可
Email	本認証局では使用しないでください。	×	
鍵長			

RSA 2048bit

○・・・必須　×・・・入力不可　△・・・省略可

注意：証明書の更新を行う場合は、先に 2-7 をご確認ください。

2-3.鍵ペアの生成と CSR の作成

2-3-1 キーストアの生成

以下に鍵ペアの生成方法を記述します。

鍵ペアの作成

1. キーストアを作成するため、以下のコマンドを実施してください。 -dName の引数に関しましては、「2-2.事前準備」の「DN ルール」に従い DN 情報を入力してください。

```
$keytool -genkey -alias <tomcat> -keyalg RSA -keysize 2048 -keystore
<server_yyyymmdd.keystore> -dname "<サーバ DN>"
鍵ストア・パスワードを入力してください：<keystore_pass> ←changeit を推奨
<tomcat>の鍵パスワードを入力してください
        （鍵ストア・パスワードと同じ場合には Enter を押してください）：←鍵のパスワードを入力
```

注意：入力したパスワードは画面に表示されます。

重要：このパスワードは証明書のインストールに必要な情報となります。鍵ペア利用期間中は忘れることが無いよう、また、他人に知られることの無いよう、安全な方法で管理してください。

重要：更新時、キーストアファイルを上書きすることの無いように、キーストアファイルに日付等のファイル名をつけることを推奨します。

2. 作成したキーストアの情報は以下のコマンドで確認することができます。

```
$keytool -list -v - keystore < server_yyyymmdd.keystore >
鍵ストア・タイプ: JKS
・・・
別名: tomcat
・・・
所有者: CN=www.nii.ac.jp, OU=UPKI, O=National Institute of Informatics, L=Academe2, C=JP
発行者: CN=www.nii.ac.jp, OU=UPKI, O=National Institute of Informatics, L=Academe2, C=JP
```

3. 作成したキーストアファイルを保存します。バックアップはフロッピーディスク等に保存し、安全な場所に保管してください。キーストアファイルの中の私有鍵を利用すれば、お使いのウェブ・サーバが SSL/TLS で保護して送受信したデータを、解読することができてしまいます。従って保存するキーストアファイルへのアクセス権は加入者自身と SSL/TLS サーバのプロセス等必要最小限になるよう設定してください。またバックアップを保存したフロッピーディスク等も加入者のみまたは同じ権限のある方のみ利用できる場所へ保管してください。また、キーストアファイル作成時のパスワードの管理も、確実に行ってください。キーストアファイルの紛失、パス

ワード忘れ等が発生した場合、証明書のインストールが行えなくなります。この場合、新たに証明書を申請しなおしていただくことになりますので、ご注意ください。

2-3-2 CSR の生成

キーストアが作成されたことを確認後、CSR を生成します。

CSR の作成

1. 次のコマンドを入力し、CSR の作成を開始してください。パスフレーズの入力が求められますので、「2-3-1 キーストアの生成」の手順 1 で作成したキーストアのパスワードを入力してください。

```
$keytool -certreq -sigalg SHA1withRSA -alias <tomcat> -file <servername.csr> -keystore
<server_yyyymmdd.keystore>
鍵ストア・パスワードを入力してください：<keystore_pass>
```

注意：入力したパスワードは画面に表示されます。

2. パスワードの入力が成功すると CSR が生成され、要求された情報の入力が完了すると CSR が生成され、servername.csr に保存されます。なお、このファイルも、バックアップをとって、証明書を受領するまでは別途保管することをお勧めします。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBhDCB7gIBADBFMQswCQYDVQQGEwJKUDEQMA4GA1UEBxMHQWNhZGVtZTEMMAoG
                                        例
UmOE3vq8Ajg=
-----END CERTIFICATE REQUEST-----
```

3. 以下のコマンドを入力することにより、CSR の内容を確認することができます。

```
$ openssl req -noout -text -in servername.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=JP, L=Academe2, O=National Institute of Informatics, OU=Cyber Science
Infrastructure Development Department, CN=www.nii.ac.jp          ←CSR 生成時に入力した DN
と一致していることを確認してください。
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit) ←鍵長が 2048bit であることを確認してください。
                Modulus (2048 bit):
                    00:c9:0e:99:5c:8a:4a:e3:b2:e2:0d:3d:60:4d:30:
                                :
                               例
                                :
                    ca:2e:56:f7:66:bd:01:44:ea:f3:ca:d2:f6:e0:5e:
                    6c:57:4b:65:e4:e7:f7:ca:dd
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption←署名アルゴリズムが sha1 であることを確認し
                                                てください。

        88:44:e5:27:06:02:ec:85:6c:29:6a:0f:a3:92:87:4e:e2:f1:
                               :
                              例
                               :
        9c:3c:0b:7e:1c:55:3d:c3:b3:7a:3a:36:d1:f6:3a:97:78:1a:
        c1:cc
```

2-4.証明書の申請から取得まで

CSR を作成しましたら登録担当者へ送付するための証明書発行申請 TSV ファイルを作成し申請します。証明書発行申請 TSV ファイルの作成方法、申請方法等につきましては、「**証明書自動発行支援システム操作手順書(加入者用)**」をご確認ください。

証明書の発行が完了すると、本システムより以下のメールが送信されます。メール本文に記載された証明書取得 URL にアクセスし、証明書の取得を実施してください。

証明書取得 URL の通知

【件名】

Web サーバ証明書発行受付通知

・・・・・

#以下に証明書の取得先が記述されています。

貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。

本日から 1 ヶ月以内に以下の証明書取得 URL へアクセスし、サーバ証明書の取得を行ってください。

証明書取得 URL:https://scia.nii.ac.jp/～ **←左記 URL にアクセスし証明書の取得を行ってください。**

・・・・・

2-5.証明書のインストール

本章では Tomcat(JavaKeytool)への証明書のインストール方法について記述します。

2-5-1 事前準備

事前準備として、サーバ証明書、中間 CA 証明書、ルート CA 証明書を取得してください。

前提条件

1. サーバ証明書を準備します。「2-4.証明書の申請から取得まで」で受領したサーバ証明書を server.cer という名前で保存してください。

2. 中間 CA 証明書を準備します。以下の中間 CA 証明書の「-----BEGIN CERTIFICATE----- から -----END CERTIFICATE-----」までをコピーして、nii-odca2.cer という名前で保存してください。(次の URL にアクセスすることで同様のファイルが公開されているリポジトリへアクセスできます。)
   リポジトリ:https://repo1.secomtrust.net/sppca/nii/odca2/

```
-----BEGIN CERTIFICATE-----
MIIEVDCCAzygAwIBAgIEErmwxzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJK
UDEYMBYGA1UEChMPU0VDTO0gVHJ1c3QubmV0MScwJQYDVQQLEx5TZWN1cmlOeSBD
b21tdW5pY2FOaW9uIFJvb3RDQTEwHhcNMDkwMzI3MDMxMzUxWhcNMTkwMzI3MDMx
MzUxWjB9MQswCQYDVQQGEwJKUDERMA8GA1UEBxMIQWNhZGVtZTIxKjAoBgNVBAoT
IU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczENMAsGA1UECxMEVVBL
STEgMB4GA1UECxMXTklJIE9wZW4gRG9tYWluIENBIC0gRzIwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDgFGOJGEjnMbJg14iOOKK4qPNr1gwOIZwJRIdh
4L3cYh6+sKhn/lSvliCcbKFsGas9bj27d9N4dnzhyQaaurVmLFyFYtYdv8feyKcm
SN7UYUM4SoeAeq699OCPTLIQw2aehkPSGHy7ecH1JX6UYw/4OpmFNc+ITIDjqf0+
mwJTRM8CtTwvegL7k5fZYinXXtXnhOaiho91/mqDErWOw+AIpPTCDoQBnq1BJzSJ
h+9eMBqj1BrjcXULOpqBvzVz5lBXgrUq3zmVg3yjTGNErLnBg3xGxRwxgfCSo6vZ
e6MpUePb7YarCGJ99L2ENGdOp53AOm8rXyWOK9WSLdbQ9h4jAgMBAAGjggEHMIIB
AzAdBgNVHQ4EFgQUewoH9xjKjA7W2rxQgGwsRwLRDfswHwYDVR0jBBgwFoAUoHNJ
mWjchVtl45soL1efvTO8BOgwEgYDVR0TAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8E
BAMCAQYwSQYDVR0fBEIwQDA+oDygOoY4aHR0cDovL3JlcG9zaXRvcnkuc2Vjb210
cnVzdC5uZXQvUOMtUm9vdDEvUONSb29OMUNSTC5jcmwwUgYDVR0gBEswSTBHBgoq
gwiMmxtkhwUBMDkwNwYIKwYBBQUHAgEWK2h0dHBzOi8vcmVwb3NpdG9yeS5zZWNv
bXRydXNOLm5ldC9TQy1Sb29OMS8wDQYJKoZIhvcNAQEFBQADggEBAKoqogcGLHdD
lkXmNjCkI9kXn9I8zHNn7xO3YdMYkgsIkYSAic9+HwWHJPV12/baOxigpGKkY2vc
SEDwAiHqSsVTHrzY6QyERVSaalk+C74+sxjxw1JG5LcH+wgt+ExA4mZPAS7vOfgD
```

```
kni+7lP9YrlLR19E6K2AQW6G3Df8zhnkOf2+kl+lavDvT74KrhOFojYZTGF6DFIo
kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2lfP/rWbg2J1Ige
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSxOOGwJdKxFTaIzH/emcqKj93Jd
DC1rrFMhoPE=
-----END CERTIFICATE-----
```

3. ルート CA 証明書を準備します。以下 URL より Security Communication RootCA1 証明書 - Security Communication RootCA1 Certificate を取得して、scroot.cer という名前で場所に保存してください。本ファイルはデフォルトでは SCroot1ca.cer という名前でダウンロードされます。
   リポジトリ:https://repository.secomtrust.net/SC-Root1/index.html

2-5-2 ルート CA 証明書のインストール

以下の手順に従って、ルート CA 証明書のインストールを行ってください。

ルート CA 証明書のインストール

「2-5-1.事前準備」で取得したルート CA 証明書をキーストアにインストールしてください。

```
$ keytool -import -alias root -keystore <server_yyyymmdd.keystore> -file scroot.cer
←hash 値が表示されるので、リポジトリに公開された hash 値と等しいことを確認してください
Enter keystore password: <keystore_pass> ←キーストアのパスワードを入力してください
Trust this certificate? [no]: yes ←yes と入力してください
Certificate was added to keystore
```

2-5-3 中間 CA 証明書のインストール

以下の手順に従って、中間 CA 証明書のインストールを行ってください。

中間 CA 証明書のインストール

「2-5-1.事前準備」で取得した中間 CA 証明書をキーストアにインストールしてください。

```
$ keytool -import -alias niica2 -keystore < server_yyyymmdd.keystore > -file nii-odca2.cer
Enter keystore password: <keystore_pass>  ←キーストアのパスワードを入力してください
Trust this certificate? [no]:  yes     ←yes と入力してください
Certificate was added to keystore
```

2-5-4 サーバ証明書のインストール

サーバ証明書をインストールする場合は以下の手続きによりサーバ証明書のインストールを実施してください。

サーバ証明書のインストール

「2-5-1.事前準備」で取得したサーバ証明書をキーストアにインストールしてください。

```
$keytool -import -alias <tomcat> -keystore <server_yyyymmdd.keystore> -file server.cer
Enter keystore password: <keystore_pass>  ←キーストアのパスワードを入力してください
Trust this certificate? [no]:  yes     ←yes と入力してください
Certificate was added to keystore
```

2-6.Tomcat の設定変更

本章では Tomcat に証明書を適用するための設定方法について記述します。

Tomcat の設定変更

証明書のインストール終了後、「2-1. 前提条件」で記述した server.xml ファイルの編集を行ってください。証明書の更新を行った場合は新たに作成したキーストアファイルのファイルパスを **KeystoreFile** に、新たに作成したキーストアファイルのパスワードを **KeystorePass** に設定してください。

```
<Connector port="443"  ←SSL 通信を行うポート番号を指定
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
keystoreFile="[< server_yyyymmdd.keystore >までのパス]" keystorePass="<keystore_pass>"
↑キーストアファイルまでのパス                    ↑キーストアのパスワード
clientAuth="false" sslProtocol="TLS"/>
```

2-7.証明書の更新

証明書の更新時はキーストアを新たに作成して頂く必要がございます。本マニュアルに従い、キーストアを作成後、「2-6.Tomcat の設定変更」の keystoreFile、KeystorePass の値を新たに作成したキーストアに合わせて変更してください。

2-8.起動確認

本章ではインストールした証明書による SSL 通信に問題がないか確認する方法を記述します。

証明書の反映・確認

1. Tomcat を再起動し、変更した設定を反映させます。

```
$ /sbin/service tomcat5 stop
$ /sbin/service tomcat5 start
```

※ Tomcat の起動と停止は、ご使用の環境によって大きく異なりますので、適時読み替えてください。

2. ブラウザ経由で、当該のサーバへアクセスし、SSL 通信に問題がないことを確認してください。