サーバ証明書発行・導入における啓発・評価プロジェクト オープンドメイン認証局

サーバ証明書インストールマニュアル

Ver1.05 2008年8月26日

国立情報学研究所

	改訂履歴			
版数	日付	内容		
V1.0	2007/05/22	初版(配布開始)		
V1.01	2007/10/31	鍵生成時の openssl コマンド引数を 0S 別に記述		
V1.02	2007/11/30	鍵生成時の 512bit 鍵長に関する注意事項を記述		
V1.03	2008/2/21	CSR プロファイルの追加、modssl 中間 CA 証明書インストール方法修正		
V1.04	2008/4/24	「1.3 証明書の種類」のテーブルフォーマットを変更		
V1.05	2008/8/26	IIS6.0証明書更新方法の記述		

1. はじめに	1
1.1 サポートする SSL/TLS サーバ	1
1.2 OPENSSL の利用	1
1.3 証明書の種類	1
2. 鍵ペアと CSR の生成	3
2.1 CSR とは	3
2.2 DN のルール	3
2.3 CSR プロファイル	4
2.4 鍵ペア生成及び CSR 作成前の準備	4
2.5 OPENSSL での鍵ペア生成と CSR 作成	5
2.5.1 鍵ペアの生成	5
2.5.2 CSR の生成	6
2.6 JAVA KEYTOOL での鍵ペアと CSR 生成	8
2.6.1 Tomcat と JRE のバージョンによる注意点	8
2.6.2 DN 情報入力時の注意点	9
2.6.3 鍵ペアの生成	9
2.6.4 CSR の生成	11
2.6.5 SSL の有効化	12
3. 証明書のインストール	16
3.1 事前準備	16
3.1.1 証明書の取得	16
3.1.2 IIS 利用の場合 openss1 による PKCS#12 ファイルの作成	16
3.1.3 IIS 利用の場合 Security Communication RootCA1 認証局の自己署名証明書の	削除
	16
3.2 APACHE-SSL	17
3.2.1 中间 UA 証明者の1ノストール方法	18
3.2.2 リイト証明者(SSL/ILS リーハ証明者)のインストール方法	18
3.3 APACHE (MOD_SSL)	19
3.3.1 中间 UA 証明者の1ノストールガス	19
3.3.2 ソ1ト証明者(SSL/ILS ソーハ証明者)の1ノストール力法	20
5.4 JAKAKIA IUMUAI	20
5.4.1 証明音の1ノストールカム	01
J. J. 110J	Z I

	3.5.1 中間 CA 証明書のインストール方法	22
	3.5.2 サイト証明書(SSL/TLS サーバ証明書)のインストール方法	25
3.	6 IIS6	34
	3.6.1 中間 CA 証明書のインストール方法	34
	3.6.2 サイト証明書(SSL/TLS サーバ証明書)のインストール方法	37
	3.6.3 サイト証明書(SSL/TLS サーバ証明書)の更新時のインストール方法	41

1. はじめに

1.1 サポートする SSL/TLS サーバ

サポートする SSL/TLS サーバは以下となっています。

SSL/TLS サーバ	記載章節	章節題
各サーバ共通	1	はじめに
	2.1	CSRとは
	2.2	DNのルール
	2.4	鍵ペア生成及び CSR 作成前の準備
Apache-SSL	2.5	Openssl での鍵ペア生成と CSR 作成
	3.2	Apache-SSL
Apache+mod_ss1	2.5	Openssl での鍵ペア生成と CSR 作成
	3.3	Apache (mod_ssl)
Tomcat (4, 5.0), JRE1.4.2	2.6	Java keytool での鍵ペアと CSR 生成
	3.4	Jakarta Tomcat
IIS (Internet Information Server) 5	2.5	Openssl での鍵ペア生成と CSR 作成
	3.1	事前準備
	3.5	IIS5
IIS6	2.5	Openssl での鍵ペア生成と CSR 作成
	3.1	事前準備
	3.6	IIS6

表 1-1 サポートする SSL/TLS サーバと各サーバの記載章節

動作確認済みのブラウザについては、プロジェクトウェブサイトをご覧下さい。 https://upki-portal.nii.ac.jp/cerpj/

1.2 Openss1 の利用

証明書を申請する際に必要となる鍵の作成やCSRの生成には Tomcat を除く SSL/TLS サーバ で openss1 を利用します。

OpenSSL Project (<u>http://www.openssl.org</u>) では UNIX で動作するモジュールだけでなく、 Windows 版のバイナリモジュールも提供されています。Windows 版の OpenSSL は、OpenSSL binaries (<u>http://www.openssl.org/related/binaries.html</u>) ページで、EXE 形式のインスト ーラファイルをダウンロードしてインストールすることが可能です。また、Cygwin (<u>http://www.cygwin.com</u>)をインストールすることで UNIX のような操作で openssl を利用す ることができます。

ほとんどの UNIX システムでは、コンパイル可能なソースコード形態でも提供されています。 Openss1 のインストール方法等は OpenSSL Project (<u>http://www.openss1.org</u>) 等のインタ ーネット上のサイトやダウンロードしたファイルに付属しているインストールマニュアルを 参照してください。

1.3 証明書の種類

NII が運用するオープンドメイン認証局を利用するために必要となる証明書には以下の種類の証明書が必要となります。次の証明書は、インストールしていただく必要があります。

1

名称	役割		ファイル名
SecurityCommunicationRootCA1 証 明書(中間 CA 証明書)	WebTrust for CA 規準の認定を取得 に「信頼できるルート認証機関」 ート認証局の SECOM Trust. net Ro 間 CA 証明書です。SECOM Trust. net 認定を取得しています。	scrootl.crt	
	https://repol.secomtrust.net/s	ppca/NII/ODCA/index.html	
NII オープンドメイン認証局証明 書(中間 CA 証明書)	SecurityCommunicationRootCA1 CA 証明書です。NII オープンドス り、この認証局からサイト証明書 されます。この証明書はSSL/TLS して登録する必要があります。	&証局から発行された中間 メイン認証局の証明書とな (SSL/TLS 証明書)が発行 サーバに中間 CA 証明書と	niica.crt
	https://repol.secomtrust.net/s	ppca/NII/ODCA/index.html	
SSL/TLS (サイト) 証明書	SSL/TLSサーバに対してNIIオー プンドメイン認証局が発行した 証明書です。証明書が有効であ る場合には、そのサーバが間違 いなくサーバ証明書サブジェク ト(発行対象)によって運用管理 されているものであることが、 NII オープンドメイン認証局に よって証明されています。	SSL/TLS (サイト) 証明 書については、所属組織 のプロジェクトご担当 者にお問い合わせくだ さい。	Example.crt

表 1-2証明書の種類

<u>注</u>:上記のファイル名は本文書内の各手順で証明書を表す際に使うファイル名を示しています。

2. 鍵ペアと CSR の生成

2.1 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。

2.2 DN のルール

DN (Distinguished Name) とは SSL/TLS サーバの名称を表す識別名です。加入者が管理する SSL/TLS サーバの組織名、Common Name (サーバの FQDN) を一意に示す情報です。 CSR を作る際の DN 情報入力時の注意点を以下に示します。

• SSL/TLS サーバの識別名(DN) に、別紙1に記載の文字は使用できませんので、ご注意 ください。

※&が含まれる場合は、半角英語の and 等に置き換えてください。

- 各項目において、スペースのみの入力は控えてください。
 スペースのみの入力項目がある場合、証明書が発行されません。
- Common Name (コモンネーム)からドメイン名を省略したり、接続する URL に表示されるサーバ名とコモンネームが一致しない場合、ブラウザがサイトへの安全な接続を拒否する場合があります。
- Common Name (コモンネーム) に、プロトコル特定子(http://)、ポート番号、パス名は 使用しないでください。また、「*」や「?」のワイルドカード文字や、IP アドレスは使 用しないでください。

項目	指定内容の説明と注意点	必須	文字数
Country Name	本認証局では必ず「 <u>JP</u> 」と入力してくだ	\bigcirc	JP 固定
	さい。		
State or Province Name	<u>本認証局では使用しないでください。</u>	\times	省略
	<u>「.」(ドット)を入力することで省略で</u>		
	<u>きます。</u>		
Locality Name	本認証局では必ず「 <u>Academe</u> 」と入力し	\bigcirc	Academe 固定
	てください。		
Organization Name	大学名または研究所名等を示します。こ	\bigcirc	半角の英数字、別紙1
	の情報は、登録担当者の方にお問い合わ		記載文字以外で 64 文
	せください。この項目を省略すること		字以内
	は、できません。		
Organizational Unit Name	証明書を使用する部局等の名前になり	\bigtriangleup	半角の英数字、別紙1
	ます (この項目は省略可能です)。		記載文字以外で 64 文
			字以内
Common Name	サーバの URL に表示されるウェブ・サー	\bigcirc	FQDN の規格に則った
	バの名前を FQDN で入力してください。		文字で 64 文字以内
	例えば、 SSL/TLS を行うサイトの URL が		
	https://www.nii.ac.jp/ の場合にはコ		
	モンネームの値は「 <u>www.nii.ac.jp</u> 」と		
	なります。		

表 2-1 DN の要素と注意事項

2.3 CSR プロファイル

本認証局で作成する CSR プロファイルは以下のとおりです。CSR を作成する前にご確認ください。

基本領域		設定内容	補
Version		Version 1(0)	_
Subject	Country	C=JP (固定值)	1
	Locality	L=Academe(固定值)	1
	Organization	0="主体者組織名"	1
		* 機関毎に任意に指定	
		例) o= National Institute of	
		Informatics	
	Organizational Unit	OU="主体者組織単位名"	1
		* 証明書毎に任意に指定	
		例) ou= NII Open Domain CA	
	commonName	CN="サーバ FQDN"	1
		*証明書毎に任意に指定	
		例) cn=www.nii.ac.jp	
SubjectPubli	cKeyInfo	主体者の公開鍵 1024 ビット以上	2
		(ただし、例外を認める)	
attrobites		原則 Null 値とする	3
		(ただし、例外を認める)	
SignatureAlg	gorithm	SHA1 with RSAEncryption	
1.	上記指定以外の属性を利用	用する必要がある場合には事前相談するこ	こと。少な
	くとも ST (state or prov	vince name) 属性は使用しないこと。また	こ、例えば
	加入者メールアドレスなと	ビ本プロジェクトの確認項目対象外の情報	最を含めな
	いこと。		
2.	RSA1024bit 以上とする。 鍋	健長 1024bit 未満の場合には事前に登録層	司へ相談す
	ること。		

3. 任意の属性を含めても構わないが、必ずしも証明書に反映されるわけではない。また、含めた属性によっては受理不能とし、当該属性を除いて証明書発行要求の再生成を登録局から求める場合がある。少なくともSubjectAltName.rfc822Name属性は使用しないこと。

2.4 鍵ペア生成及び CSR 作成前の準備

以下の項目を準備しておいてください。

- 乱数生成用ファイル(200KB 程度で少なくとも3つ)
- サーバ鍵ペアファイル名
- サーバ鍵ペア用私有鍵パスフレーズ
- サーバ DN (「2.2 DN のルール」に従った DN)
- CSR ファイル名

2.5 0penss1 での鍵ペア生成と CSR 作成

Apache-SSL、Apache (mod_ssl)、IIS をお使いの加入者は openssl を利用して下記の手順で 鍵ペアと CSR を生成してください。

CSR 作成時には、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、必ず鍵ペアおよび CSR を新たに作成してください。

鍵ペアの鍵長は原則 1024bit 以上としてください。1024bit 未満の鍵を使用しなければならない場合、サーバ証明書申請前に本研究所まで連絡をください。

2.5.1 鍵ペアの生成

- 鍵ペアを生成するため、お使いのハード・ディスクから、無作為データ元になるファイル (200 KB 程度)を3 つ選んでください。この手順では、3 つのファイルの名前を 「<u>randfile1</u>」、「<u>randfile2</u>」、「<u>randfile3</u>」として表記します。
- 2. 鍵ペアの作成を始めるため、次のコマンドを入力してください(お使いのブラウザによっては2行以上で表示、印字されるかもしれませんが、実際は1行です)。
 今回のコマンド例では、1024 ビットの RSA 鍵ペアを生成し、「<u>servername. key</u>」という名前のファイルに保存することを示しています。

注) openssl コマンドの-rand 引数で指定するファイル名が複数の場合、セパレータとして使用する文字が OS により異なります。

■UNIX の場合-セパレータ文字':'(コロン)

openssl genrsa -des3 -rand *randfile1:randfile2:randfile3* 1024 > *servername.key*

■Windows の場合-セパレータ文字が';'(セミコロン)

openssl genrsa -des3 -rand *randfile1;randfile2;randfile3* 1024 > *servername.key*

 プロンプトが表示されたら、鍵ペアを保護する私有鍵パスフレーズ(以下「鍵ペア用私 有鍵パスパスフレーズ」とします)を決めて、入力してください。確認のため、2度入 力してください。(以下のは UNIX の場合の例です。2の注の通り、Windows の場合はセ パレータがセミコロンとなります)

重要: この鍵ペア用私有鍵パスフレーズは、サーバの再起動時および証明書のインスト ール等に必要となる重要な情報です。鍵ペア利用期間中は忘れることがないよう、また、 情報が他人に漏れることがないよう、安全な方法で管理してください。

 作成した鍵ペアの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、安全な場所に保存してください。鍵ペア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。従って保存する鍵ペ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、鍵ペア用私有鍵パスフレーズの管理も、確実に行ってください。鍵ペアファイル の紛失、鍵ペア用私有鍵パスフレーズ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。

2.5.2 CSR の生成

鍵ペアが作成されたことを確認後、 CSR を生成します。

1. 次のコマンドを入力し、 CSR の生成を開始してください。

openssl req -new -key servername.key - out servername.csr

と入力し、CSR の生成を開始します。ここで「*servername. key*」は、「2.5.1 鍵ペアの生成」で作成した鍵ペアのファイルの名前です。「*servername. csr*」は、CSR が保存されるファイルの名前です。

※現在利用中の鍵ファイルに上書きしないようご注意ください。

- 2. プロンプトが表示されたら、「2.5.1 鍵ペアの生成」で入力した鍵ペア用私有鍵パスフ レーズを入力してください。
- 3. プロンプトが表示されたら、証明書内に組み込む SSL/TLS サーバ識別名 (DN)情報を入 力してください。 更新用 CSR 生成時に指定する DN 情報は、前回申請した内容(現在利用中の証明書の DN) と同一にしてください。サイト名変更等により、DN 情報が変更になる場合は、新規の お申込となります。

\$ openssl req -new -key servername.key -out servername.csr Enter pass phrase for servername.key: ← 鍵ペア私有鍵パス フレーズ入力 You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [AU]: JP ← "JP"を入力 ← 「.」ドットの入力 State or Province Name (full name) [Some-State]:. ← "Academe"を入力 Locality Name (eg, city) []:Academe Organization Name (eg, company) [Internet Widgits Pty Ltd]:National Institute of Informatics ← 組織名を入力 Organizational Unit Name (eg, section) []:UPKI ← 部局名を入力 Common Name (eg, YOUR name) []:www.nii.ac.jp ← サーバ名 FQDN を入力 Email Address []:. ← 「.」ドットを入力 Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:. ← 「.」ドットを入力 ← 「.」ドットを入力 An optional company name []:. \$

4. 要求された情報の入力が完了すると CSR が生成され、-out 引数で指定した名前のファ イル(今回の例では、「<u>servername. csr</u>」)に保存されます。ファイルの内容には、次 の例のような部分があります。この部分が CSR です。

尚、CSR 生成時に入力した内容が記載されておりますので、証明書が発行され受け取る までは、このファイルもバックアップを取って、別途保管するようお勧めします。

5. 次のコマンドを入力し、CSRの内容をご確認ください。

ここで「*servername. csr*」は、CSR を保存したファイルの名前です。

```
$ openssl req -noout -text -in <u>servername.csr</u>
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=JP, L=Academe, 0=National Institute of Informatics, 0U=UPKI,
CN=www.nii.ac.jp
CN=ww
```

```
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: shalWithRSAEncryption
       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:
        cl:cc
$
```

6. ここで生成した CSR は、登録担当者に提出いただきます。

※重要

作成した CSR および鍵ペアのファイルは、必ずバックアップを取っていただき安全な場所 に保管してください。また、鍵ペアのファイル生成時に指定した鍵ペア用私有鍵パスフレー ズの管理も、確実に行ってください。鍵ペアのファイルの紛失、鍵ペア用私有鍵パスフレー ズ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。この場合は、新たに 鍵ペアを生成して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。

2.6 Java keytool での鍵ペアと CSR 生成

2.6.1 Tomcat と JRE のバージョンによる注意点

※Jakarta Tomcat および JRE は、最新版に更新しておくことをおすすめします。

Jakarta Tomcat 4 で PureTLS をインストールしている場合には、JSSE を使うために server.xml ファイルで Factory 要素の SSLImplementation 属性の値を 「org.apache.tomcat.util.net.JSSEImplementation」と明示的に指定するか、PureTLS をア ンインストールするか、どちらかにしてください。

この文書では、Unix版のJRE での操作例を掲載します。Windows版では、実際の表記が異なります。

プラット	変数置換	パス名	プロンプト	拡張子	ファイル連結
ホーム					コマンド
Unix	\${変数名}	/ディレクトリ名/ファイ	#や\$	Sh	cat
		ル名			
DOS	%変数名%	ドライブ名:¥ディレクト	ドライブ名>	Bat	type
		リ名¥ファイル名			

表 2-2 Unix と Windows の環境による違い

鍵ストアや鍵ペアの生成には、keytool というコマンドを使用して行います。

これは\${JAVA_HOME}/bin ディレクトリにインストールされているはずです(\${JAVA_HOME} は、JRE 1.4.2を導入したディレクトリです)。 鍵ストアや鍵ペアを生成するには、次の手順に従い行なってください。

更新時も、必ず鍵ペアや CSR を新たに生成してください。

2.6.2 DN 情報入力時の注意点

「2.2 DN のルール」を参照してください。

2.6.3 鍵ペアの生成

1. 鍵ペアの生成を始めるため、次のようなコマンドを入力してください。

\$ keytool -genkey -alias tomcat -keyalg RSA -keysize 1024 -keystore
/your/keystore/filename -dname "CN=www.nii.ac.jp, OU=UPKI, O=National
Institute of Informatics, L=Academe, C=JP"

上のコマンド例では、「<u>tomcat</u>」という名前をつけて 1024 ビットの RSA 鍵ペアを生成し、「<u>/your/keystore/filename</u>」という名前の鍵ストア・ファイルに、「CN=www.nii.ac.jp, OU=UPKI, O=National Institute of Informatics, L=Academe, C=JP」というDN で保存することを示しています。

ここで、「-dname」の後には、CSR に含む DN を指定します。「=」文字の後に指定する 値については、「2.2 DN のルール」を参照してください。

更新用 CSR 生成時に指定するディスティングィッシュネーム(DN)情報は、前回申請 した内容(現在利用中の証明書 DN)と同一にしてください。情報の入力にあたっては、 次の点にご注意ください。

注意:現在利用中の鍵ストアの鍵ペアに上書きしないよう、ご注意ください。

2. プロンプトが表示されたら、tomcatの鍵ストア用パスワードを入力してください。

言語環境	プロンプト(出力文字)
英語	Enter keystore password: <u>changeit</u>
日本語	キーストアのパスワードを入力してください: <u>changeit</u>

上のコマンド例では、「*changeit*」という鍵ストア用パスワードをつけたことを示して います。

<u>注意</u>:入力した鍵ストア用パスワードは、エコーバックで表示されます。周囲に他人がいる場合、不用意にのぞかれたりしないよう、ご注意ください。

※重要: このパスワードは、証明書のインストールに必要となる重要な情報です。鍵 ペア利用期間中は忘れることがないよう、また、他人に漏洩することがないよう、安全な 方法で管理してください。 3. プロンプトが表示されたら、私有鍵のパスワードの入力を促されますので、鍵スト アのパスワードと同じにするなら、そのままリターンキーを、鍵ストアのパスワー ドと異なるパスワードを設定する場合はそのパスワードを入力してください。

言語環境	プロンプト(出力文字)
英語	Enter key password for < <u>tomcat</u> >
	(RETURN if same as keystore password):
日本語	〈 <u>tomcat</u> 〉の鍵パスワードを入力してください。
	(キーストアのパスワードと同じ場合は RETURN を押してください):

4. 生成した鍵ストアを確認するため、次のコマンドを入力してください。

\$ keytool -list -v - keystore /your/keystore/filename

上のコマンド例では、「<u>/your/keystore/filename</u>」という名前のファイルに保存した鍵ストアを確認することを示しています。

5. プロンプトが表示されたら、鍵ストア用パスワードを入力してください。

言語環境	プロンプト(出力文字)
英語	Enter keystore password: <u>changeit</u>
日本語	キーストアのパスワードを入力してください:
	<u>changeit</u>

<u>注意</u>:入力したパスワードは、エコーバックで表示されます。周囲に他人のいる場合、不用意にのぞかれたりしないよう、ご注意ください。

6. 鍵ストアのファイルの情報が表示されます。

Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: tomcat
Creation date: Mar 9, 2007
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=www.nii.ac.jp, OU=UPKI, O=National Institute of Informatics, L=Academe, C=JP
Issuer: CN=www.nii.ac.jp, OU=UPKI, O=National Institute of Informatics, L=Academe, C=JP
Serial number: 45f167e9
Valid from: Fri Mar 09 22:58:01 JST 2007 until: Thu Jun 07 22:58:01 JST 2007
Certificate fingerprints:
MD5: 03:41:88:91:A3:44:D7:42:B8:38:6F:7A:C9:5B:5C:64
SHA1: 1A:6E:CB:66:5E:79:7A:0D:88:17:3B:BB:25:3C:AE:1D:A2:F1:36:05
Signature algorithm name: SHA1withRSA
Version: 3

7. 鍵ストアのバックアップはフロッピーディスク等に保存し、安全な場所に保存してください。鍵ストアの中の鍵ペアを利用すれば、お使いの SSL/TLS 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。従って保存する鍵ペア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、鍵ストアのファイル生成時に指定したパスワードの管理も、確実に行ってください。鍵ストアのファイルの紛失、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。

2.6.4 CSR の生成

CSR の生成には、keytool コマンドを使用して行います。

これは ${JAVA_HOME}/bin ディレクトリにインストールされているはずです(<math>{JAVA_HOME}$ は、JRE 1.4.2を導入したディレクトリです)。

CSR を生成するには、次の手順に従い行なってください。更新時も、必ず CSR を新たに生成してください。

鍵ペアが生成できたことを確認後、CSR を生成します。

1. 次のコマンドを入力し、CSRの生成を開始してください。

\$ keytool -certreq -sigalg SHA1withRSA -alias tomcat -file servername.csr -keystore
/your/keystore/filename

と入力し、CSR の生成を開始します。ここで上記の文字は以下を示します。

文字列	意味
<u>Tomcat</u>	「2.6.3 鍵ペアの生成」で指定した指定した鍵ペアの名前
/your/keystore/filename	「2.6.3 鍵ペアの生成」で指定した鍵ストアのファイルの名前
<u>Servername. csr</u>	CSR が保存されるファイルの名前

2. プロンプトが表示されたら、鍵ストア用パスワードを入力してください。

Enter keystore password: changeit

<u>注意</u>:入力したパスワードは、エコーバックでそのまま端末に表示されます。周囲に他人のいる場合、パスワードを不用意にのぞかれたりしないよう、ご注意ください。

3. CSR が生成され、手順1で指定した名前のファイル(今回の例では、「<u>servername.csr</u>」) に保存されます。ファイルの内容には、次の例のような部分があります。この部分が CSR です。 MIIBsjCCARsCAQAwcjELMAkGA1UEBhMCS1AxEDAOBgNVBAcTBOFjYWR1bWUxKjAoBgNVBAoTIU5h dG1vbmFsIE1uc3RpdHV0ZSBvZiBJbmZvcm1hdG1jczENMAsGA1UECxMEVVBLSTEWMBQGA1UEAxMN : 何列 : p09wBoF1r5fEK16VCFC0qzfDQsKMKjbA0QJ0C+2wIHR84NBxmse0A6d1ret+Tk/RvM/gX2Mrg+9E dKyJUY41fTpLkX1sFyKBimGN8Y/PHsPr6rnL6IeVip63yu1Eiwxf -----END NEW CERTIFICATE REQUEST-----

尚、CSR 生成時に入力した内容が記載されておりますので、証明書が発行され受け取るまでは、この CSR を保存したファイルもバックアップをとって、別途保管するようお勧めいたします。

4. openssl コマンドをインストールされている場合には、次のコマンドの入力で、CSR の 内容が確認できます。

\$ openssl req -noout -text -in <u>servername.csr</u>

----BEGIN NEW CERTIFICATE REQUEST-----

ここで「*servername.csr*」は、CSRを保存したファイルの名前です。

5. ここで生成した CSR は、登録担当者に提出いただきます。

※重要

鍵ストアと CSR のバックアップはフロッピーディスク等に保存し、安全な場所に保存して ください。鍵ストアの中の鍵ペアを利用すれば、お使いの SSL/TLS サーバーが 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。従って保存する鍵ペアへのアク 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。

鍵ストアのファイル生成時に指定したパスワードの管理も、確実に行ってください。鍵ストアのファイルの紛失、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。

2.6.5 SSL の有効化

SSL/TLS を有効にするため、次の作業をしていただきます。

- 1. 次のような Connector 要素を、server. xml ファイルに指定してください。
 - Tomcat 4 の場合

```
<!- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
-->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
    port="8443" minProcessors="5" maxProcessors="75"
    enableLookups="true"
    acceptCount="100" debug="0" scheme="https" secure="true"
    useURIValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="/your/keystore/filename" keystorePass="<u>changeit</u>"
    clientAuth="false" protocol="TLS"/>
/Connector>
<!--</pre>
```

● Tomcat 5.0 の場合

```
<!- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
-->
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
keystoreFile="/your/keystore/filename" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS"/>
<!--
-->
```

ここで上記内の文字列は以下を示します。

文字列	意味
8443	Jakarta Tomcat 4が待ち受けるポートの番号
<u>Changeit</u>	「2.6.3 鍵ペアの生成」で指定した鍵ストアのパスワード
/your/keystore/filename	「2.6.3 鍵ペアの生成」で指定した鍵ストアのファイル名

注意: 鍵ストアのパスワードは、server.xml ファイルに平文で指定します。パスワードや 私有鍵が他人に漏洩しないよう、このファイルや conf ディレクトリの許可モードなどにご注 意ください。

2. Jakarta Tomcat 4 を(再) 起動してください。

\$TOMCAT_HOME/bin/catalina.sh run

または

\$TOMCAT_HOME/bin/startup.sh

<u>注意</u>: 待ち受けるポート番号によっては、スーパーユーザー特権の不必要な場合もあります。

- 3. 「https://コモンネーム:ポート番号/」の URL で閲覧できることを、ウェブ・ブラウザ でご確認ください(この時点では、SSL のサーバ証明書が自己署名になっていますので、 ブラウザによっては、警告のダイアログなどの出る場合もあります)。
- 4. Admin サーブレットにアクセスできるよう設定してから、「https://コモンネーム:ポート番号/admin/index.jsp」のURLで、ログイン画面にアクセスできることを、ご確認ください。

● Tomcatサーバー管理コンソール - Microsoft Internet Explorer _ □ □ ファイル(E) 編集(E) 表示(M) お気に入り(A) ツール(E) ヘルブ(E)	×
TOMCAT WEB SERVER	•
ADMINISTRATION	
TOOL	
ユーザ名	
パスワード	
	-
· · · · · · · · · · · · · · · · · · ·	•

5. 適切なユーザ名とパスワードを入力して、Admin サーブレットにログインしてください。

■ Tomeatサーバー管理コンソール - Microsoft Intern 」ファイル(E) 編集(E) 表示(V) お気に入り(A)	et Explorer ツール① ヘルプ	9 1 0 ×
TOMCAT WEB SERVER ADMINISTRATION TOOL	変更を反映	ログアウト
 ♥ ₩ Tomcat Server ● ♥ サービス (Catalina) ♥ ⊡リソース □ データソーフ 		
 □ メールセッション △ 環境エントリ ● ユーザデータベース ● コーザ定義 		
☆ ユーザ ☆ グループ 兼 ロール		

6. 「サービス」の下にある Connector (8443)を選択してから、指定した鍵ストアのファイ ルが読み込まれていることを、ご確認ください。 ここで「8443」は、Jakarta Tomcat 4 が待ち受けるポートの番号です。



※重要

鍵ストアのパスワードを指定する server. xml ファイルや、そのファイルのある conf ディ レクトリのアクセス管理を、必要最小限のユーザ、プロセスのみに限定するよう確実に行って ください。鍵ストアのファイルや、パスワードの紛失等が発生した場合、証明書のインストー ルが行えなくなります。この場合、新たに鍵ペアを生成して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。 3. 証明書のインストール

3.1 事前準備

3.1.1 証明書の取得

NII オープンドメイン認証局の証明書を利用する際に必要となる証明書の取得方法に関しては、「1.3 証明書の種類」を参照してください。

3.1.2 IIS 利用の場合 openss1 による PKCS#12 ファイルの作成

IIS を利用する場合、事前に鍵ペアとサイト証明書(SSL/TLS 証明書)を連結した PKCS#12 ファイルを作る必要があります。PKCS とは RSA Security 社が提唱した仕様で公開鍵/私有鍵 や証明書を利用するほとんどのシステムでサポートされています。その中に PKCS#12 があり、 鍵ペアと証明書等を PKCS#12 の仕様で決められたフォーマットに従い暗号化された状態で 1 つのファイルとすることができるものです。

以下のコマンドで openssl を使って鍵ペアとサイト証明書 (SSL/TLS 証明書) を連結した PKCS#12 ファイルを作ることができます。

openssl pkcs12 -export -inkey <u>servername.key</u> -in <u>Example.crt</u> -out <u>servername.pfx</u>

コマンドを実行すると、以下のようなプロンプトが順次表示されます。最初に鍵ペア用私 有鍵パスフレーズを入力します。次に PKCS#12 ファイルを開くためのパスフレーズを 2 回入力 します。後者を PKCS#12 保護パスフレーズと呼ぶことにします。

Enter pass phrase for <u>servername.key</u> :	
Enter Export Password:	← PKCS#12 保護パスフレーズ入力
Verifying - Enter Export Password:	← PKCS#12 保護パスフレーズ再入力

これで鍵ペアとサイト証明書(SSL/TLS 証明書)を連結した PKCS#12 の「<u>servername. pfx</u>」が作成されます。

3.1.3 IIS 利用の場合 Security Communication RootCA1 認証局の自己署名証明書の削除

WindowsのバージョンやWindows Updateの時期によってはSecurity Communication RootCA1 認証局の自己署名証明書が登録されています。この自己署名証明書が登録された状態では SSL/TLSの通信の際にSecurity Communication RootCA1認証局の中間 CA 証明書が利用されな い状態となってしまい、接続不能のブラウザ等がでてしまいます。従って、Security Communication RootCA1認証局の自己署名証明書を削除する必要があります。

サーバの「コントロールパネル」を開いて「インターネットオプション」を開いて、「コン テンツ」タグを開いた後、「証明書」のボタンより「信頼されたルート証明機関」をクリック してください。

次の証明書の有無を確認してください。

発行先:Security Communication RootCA1 発行者:Security Communication RootCA1 有効期限:2003/09/30 から 2023/09/30

発行先		発行者	有効期限	フレンドリ名	^
🔛 SecureSign	RootCA2	SecureSign RootCA2	2020/09/15	Japan Certificati	1
SecureSign	RootCA3	SecureSign RootCA3	2020/09/15	Japan Certificati	
SecureTrust	CA	SecureTrust CA	2030/01/01	SecureTrust Cor	
🔛 Security Cor	mmunication	Security Communication	2023/09/30	Security Commu	
🔛 Serasa Certi	ificate Authori	Serasa Certificate Author	2024/11/21	Serasa Certificat	
🔛 Serasa Certi	ificate Authori	Serasa Certificate Author	2024/11/21	Serasa Certificat	
🔛 Serasa Certi	ificate Authori	Serasa Certificate Author	2024/11/21	Serasa Certificat	
		SERVICIOS DE CERTIFI	2009/03/10	SERVICIOS DE	~
ンポート(D) (エクスポート(<u>E</u>)…	削除(<u>R</u>)		[詳細設定)	(<u>A</u>)

図 3-1 Windows に登録されている Security Communication RootCA1 認証局の自己署名証明書

上記証明書が確認できない場合は削除作業は不要です。 対象の証明書が選択された状態で「削除(R)」をクリックします。

※誤って別の証明書を削除することがないようご注意ください。※証明書を削除する前に、エクスポートすることによって証明書をバックアップできま

す。

削除確認のダイアログがでますので、「はい」を選択して削除完了です。

<u>※重要</u>

本作業の後、WindowsUpdate 等により Security Communication RootCA1 の自己署名証明 書を インストールすることのないようにご注意ください。

3.2 Apache-SSL

証明書のインストールにあたり、1.3節で示した2種類の証明書を以下の手順に準じてイン ストールしていただく必要があります。

- 1. 中間 CA 証明書をインストールします。
- 2. 中間 CA 証明書をインストール後、サイト証明書 (SSL/TLS サーバ証明書) をインストー ルします。
- 3. Apache サーバのデーモン・プロセスを再起動します。

以下の SSLCACertificatePath、SSLCertificateFile、SSLCertificateKeyFile 等のエント リは、Apache の立ち上げファイルの中にあります。

デフォルトの立ち上げファイル名は「httpd.conf」です。

立ち上げファイルでは、「#」文字で行内コメントが始まります。以下で使用する各種のエントリの前に「#」文字のないことを確認してください。

3.2.1 中間 CA 証明書のインストール方法

以下の手順に従って、SSLCACertificatePath エントリによって指定されるディレクトリに、 中間 CA 証明書をインストールしてください。 **※SSLCACertificateFile は設定しないでください。**

- この手順は、SSLCACertificatePath が立ち上げファイルで<u>〈SSLTOP〉</u>/CA に設定されていることを前提としています。
 ここで、<u>〈SSLTOP〉</u>は Apache-SSL で SSL を設定する各種ファイルのトップディレクトリを示しています。異なるパスを使用している場合は、正しいパスに適宜読み替えてください。
- 2. テキストファイルで中間 CA 証明書を保存していることを確認します。
- 3. SecurityCommunicationRootCA1の証明書ファイルをディレクトリ<u>〈SSLTOP〉</u>/CA/に移動し ます。SecurityCommunicationRootCA1の中間 CA 証明書ファイルのパス名は、 /tmp/<u>scroot1.crt</u>としています。

mv /tmp/*scroot1.crt <SSLTOP>*/CA/a3896b44.0

4. NII オープンドメイン認証局の証明書ファイルをディレクトリ<u>〈SSLTOP〉</u>/CA/に移動しま す。NII オープンドメイン認証局の中間 CA 証明書ファイルのパス名は、/tmp/<u>miica. crt</u> としています。

mv /tmp/<u>niica.crt</u> <u><SSLTOP></u>/CA/957e1f22.0

3.2.2 サイト証明書(SSL/TLS サーバ証明書)のインストール方法

以下の手順に従って、サイト証明書(SSL/TLS サーバ証明書)をインストールしてください。

- この手順では、SSLCertificateFile が立ち上げファイルで <u>〈SSLTOP〉</u>/conf/ssl.crt/server.crt に設定されていることを、前提としています。また、SSLCertificateKeyFile が立上げファイルで<u>〈SSLTOP〉</u>/conf/ssl.key/server.key に設定されていることを、前提としています。 ここで、<u>〈SSLTOP〉</u>は、SSLのトップディレクトリです。異なるパスを使用している場合、 正しいパスに適宜読み替えてください。またサイト証明書(SSL/TLSサーバ証明書)フ ァイルのパス名は、/tmp/<u>Example.crt</u>としています。
- 2. サイト証明書 (SSL/TLS サーバ証明書) をテキストファイルで保存していることを確認 してください。
- 3. サイト証明書 (SSL/TLS サーバ証明書)を、<u>〈SSLTOP〉</u>/conf/ssl.crt/server.crtのファ イルに移動してください。

mv /tmp/*Example.crt <SSLTOP*>/conf/ssl.crt/server.crt

- 4. 2.5.1で作成した、サイト証明書(SSL/TLS サーバ証明書)に対応する鍵ペアのファイ ルを、<u>〈SSLTOP〉</u>/conf/ssl.key/server.keyのファイルに移動してください。
- 5. 立上げファイル内に設定されている SSLCertificateKeyFile が、鍵ペアのファイルを指していることを確認してください。

証明書のインストールは、以上で完了です。

3.3 Apache (mod_ssl)

証明書のインストールにあたり、1.3節で示した2種類の証明書を以下の手順に準じてイン ストールしていただく必要があります。

- 1. 中間 CA 証明書をインストールします。
- 2. 中間 CA 証明書をインストール後、サイト証明書 (SSL/TLS サーバ証明書) をインストー ルします。
- 3. Apache サーバのデーモン・プロセスを再起動します。

以下の SSLCertificateChainFile、SSLCertificateFile、SSLCertificateKeyFile 等のエン トリは、Apache の立ち上げファイルの中にあります。 デフォルトの立ち上げファイル名は「httpd. conf」です。

立ち上げファイルでは、「#」文字で行内コメントが始まります。以下で使用する各種のエントリの前に「#」文字のないことを確認してください。

3.3.1 中間 CA 証明書のインストール方法

以下の手順に従って、SSLCertificateChainFile エントリによって指定されるファイルに中間 CA 証明書をインストールしてください。

- この手順では、SSLCertificateChainFile が立上げファイルで <u>〈SSLTOP〉</u>/conf/ssl.crt/ca.crtファイルに設定されていることを、前提としています。 ここで、<u>〈SSLTOP〉</u>は、Apache(mod_ssl)でSSLを設定する各種ファイルのトップディレクトリを示しています。トップディレクトリの下で異なるパスを使用している場合、正しいパスに適宜読み替えてください。
- 2. 中間 CA 証明書をテキストファイルで保存していることを確認してください。
- SecurityCommunicationRootCA1 認証局証明書ファイルをディレクトリ <u>〈SSLTOP〉</u>/conf/ssl.crt/に移動し、ファイル名をリネームします。 SecurityCommunicationRootCA1 認証局の中間 CA 証明書ファイルのパス名は、 /tmp/scroot1.crtとしています。

mv /tmp/*scroot1.crt <u><SSLTOP></u>*/conf/ssl.crt/ca.crt

4. NII オープンドメイン認証局の中間 CA 証明書ファイルを <u>〈SSLTOP〉</u>/conf/ssl.crt/ca.crtというファイルに追加してください。NII オープンドメ イン認証局の中間 CA 証明書ファイルのパス名は、/tmp/<u>niica.crt</u>としています。 cat /tmp/*niica.crt* >> *<SSLTOP>*/conf/ssl.crt/ca.crt

3.3.2 サイト証明書 (SSL/TLS サーバ証明書) のインストール方法

以下の手順に従って、 サイト証明書 (SSL/TLS サーバ証明書) をインストールしてください。

- この手順では、SSLCertificateFile が立上げファイルで <u>〈SSLTOP〉</u>/conf/ssl.crt/server.crt に設定されていることを、前提としています。また、SSLCertificateKeyFile が立上げファイルで<u>〈SSLTOP〉</u>/conf/ssl.key/server.key に設定されていることを、前提としています。 ここで、<u>〈SSLTOP〉</u>は、SSLのトップディレクトリです。トップディレクトリの下で異なるパスを使用している場合、正しいパスに適宜読み替えてください。 またサイト証明書 (SSL/TLS サーバ証明書)ファイルのパス名は、/tmp/<u>Example.crt</u>としています。
- 2. サイト証明書 (SSL/TLS サーバ証明書) をテキストファイルで保存していることを確認 してください。
- 3. サイト証明書 (SSL/TLS サーバ証明書)を、<u>〈SSLTOP〉</u>/conf/ssl.crt/server.crtのファ イルに移動してください。

mv /tmp/*Example.crt* <u><SSLTOP></u>/conf/ssl.crt/server.crt

- 4. 2.5.1で作成した、サイト証明書(SSL/TLS サーバ証明書)に対応する鍵ペアのファイ ルを、<u>〈SSLTOP〉</u>/conf/ssl.key/server.keyのファイルに保存してください。
- 5. 立上げファイル内に設定されている SSLCertificateKeyFile が、鍵ペアのファイルを指していることを確認してください。

証明書のインストールは、以上で完了です。

3.4 Jakarta Tomcat

3.4.1 証明書のインストール方法

証明書をインストールするため、次の作業をしていただきます。

1. 次のコマンドを入力し、1.3節で示した中間 CA 証明書とサイト証明書の 3 枚の証明書を つないでください。

\$ cat <u>Example.crt</u> <u>niica.crt scroot1.crt</u> > <u>combined-chain-and-webcert</u>

2. 次のコマンドを入力し、つないだ証明書をインストールしてください。

\$ keytool -import -alias <u>tomcat</u> -file <u>combined-chain-and-webcert</u> -keystore
/your/keystore/filename - trustcacerts

ここで上記のコマンド内にある文字列の意味は以下の通りです。

文字列	意味
<u>Tomcat</u>	「2.6.3鍵ペアの生成」で作成した鍵ペアの名前
<u>combined-chain-and-webcert</u>	上記手順1 でつないだ中間 CA 証明書とサイト証明書のファイ
	ルの名前
/your/keystore/filename	「2.6.3鍵ペアの生成」で指定した鍵ストアのファイルの名前

表 3-1 keytool コマンドの文字列の意味

3. プロンプトが表示されたらパスワードを入力してください。

Enter keystore password: *changeit*

ここで「*changeit*」は、「2.6.3鍵ペアの生成」で指定した鍵ストアのパスワードです。

<u>注意</u>:入力したパスワードは、エコーバックでそのまま端末に表示されます。周囲に他 人のいる場合、パスワードを不用意にのぞかれたりしないよう、ご注意ください。

4. 次のようなプロンプトの表示される場合は「yes」と入力してください。

Top-level certificate in reply: Owner: OU=Security Communication RootCA1, O=SECOM Trust.net, C=JP Issuer: CN=http://www.valicert.com//emailAddress=info@valicert.com, OU=ValiCert Class 1 Policy Validation Authority, O=ValiCert, Inc., L=ValiCert Validation Network Serial number: 10002 Valid from: Tue Mar 16 11:34:42 JST 2005 until: Mon Mar 11 11:34:42 JST 2015 Certificate fingerprints: MD5: BC:88:BB:D7:36:2C:63:8C:F3:F6:CB:D9:69:B3:DC:83 SHA1: AB:A0:A6:0A:3B:A7:D2:2C:0D:CF:77:41:D8:F5:5C:B3:C1:24:1D:F0

... is not trusted. Install reply anyway? [no]: yes

5. 次のように表示されることを、ご確認ください。

Certificate reply was installed in keystore

6. この確認がとれれば不要になりますので、つないだ証明書のファイルは、次のようなコ マンドの入力で削除できます。

\$ rm - f <u>combined-chain-and-webcert</u>

<u>※ 重要</u>

証明書のインストール後、鍵ストアのファイルは、必ずバックアップをとり、鍵ペア利用 期間中はパスワードの保管場所と別の安全な場所に保管してください。

3.5 IIS5

証明書のインストールにあたり、必要な証明書に関しては「1.3 証明書の種類」を参照してください。

3.5.1 中間 CA 証明書のインストール方法

- 中間 CA 証明書の SecurityCommunicationRootCA1 認証局証明書(scroot1.crt)と NII オープンドメイン認証局証明書(niica.crt)を順番にインストール作業を行います。
- 2. 証明書ダイアログボックスが表示されます。「全般」タブの[証明書のインストール]をクリックします。

証明書 ?▼ 全般 】詳細設定 】証明のパス 】
証明書の情報
この証明書の目的: ・電子メールを保護する ・リモート コンピュータの ID を保証する
*詳細は、証明機関のステートメントを参照してください。
発行先 : Security Communication RootCA1
発行者: http://www.valicert.com/
有効期間 2005/03/16 から 2015/03/16
ОК

3. 証明書マネージャインポートウィザードが表示されますので、「次へ」をクリック してください。

証明書のインポートウィザード		×
	証明書のインボート ウィザードの開始	
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リ ストをディスクから証明書ストアにコピーします。	
	証明機関によって発行された証明書は、ユーザー ID を確認し、データ を保護したり、またはセキュリティで保護された接続を提供するための情 報を含んでいます。証明書ストアは、証明書が保管されるシステム上 の領域です。	
	1元1丁9つには、レスヘ」をソリックしていたさい。	
	く戻の国にないいろううキャンセル]

4. [証明書をすべて次のストアに配置する]を選択し、[参照]をクリックします。

週月書のインボート ウィザード
証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。
Windows (ご証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。
○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
● 証明書をすべて次のストアに配置する(P)
証明書ストア:
参照(R)
< 戻る(B) 次へ(N) > キャンセル

証明書ストア選択ダイアログボックスが表示されますので、[物理ストアを表示する]を選択します。
 ダイアログボックス内の項目[中間証明機関]のそばにある[+]マークをクリックして拡張し、[ローカルコンピュータ]を選択し、[0K]をクリックします。

証明書ストアの選択	? ×
使用する証明書ストアを選択してください	
□□□ レンストラ □□□ グループ ポリシー	
□・□ 1言親された発行元 □・□ 信頼されていない言語明書	
▶ 初理ストルを表示する心	
OK ++>>t	ZJU

6. 証明書ストアに「中間証明機関¥ローカルコンピュータ」が表示されている事を確認し、「次へ」をクリックしてください。

証明書のインポートウィザード	×
証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。	
Windows (ご証明書ストアを自動的に選択させるか、証明書の場所を指定すること	ができます。
○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)	
◎ 証明書をすべて次のストアに配置する(P)	
証明書ストア:	
中間証明機関¥ローカル コンピュータ	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●
< 戻る(<u>B</u>) 次へ(<u>N</u>)> キャンセル

- 7. 「証明書のインポートウィザードの完了」が表示されたら、「完了」をクリックしてください。
- 8. 証明書のインポートウィザードが表示されます。[OK]をクリックします。

証明書の	(ンポート ウィザード	×
į	正しくインボートされま	した。
	OK	

SecurityCommunicationRootCA1 認証局証明書及び NII オープンドメイン認証局証明書のインストールが終了したら、サイト証明書(SSL/TLS サーバ証明書)をインストールします。

3.5.2 サイト証明書 (SSL/TLS サーバ証明書) のインストール方法

- 「3.1.2 IIS 利用の場合 openss1 による PKCS#12 ファイルの作成」を参照して 「<u>servername. pfx</u>」ファイルを準備します。
- 2. 「ファイル名を指定して実行」より「MMC」と入力し MMC コンソールを立ち上げま す

ארעכב 🕅 רעכב 🕼 🕕 ראיז אולא 🗐 🗈 😂 🔚 💷	
「油コンソールルート 「油コンソールルート 「快作仏) 表示(い) お気に入り(E) ← → 前回 12 「記 23	
ツリー お気に入り 名前 コンソール ルート	

- 3. MMC コンソールより「コンソール」メニューの「スナップインの追加と削除」を選 択します。
- 4. 追加をクリックします。

スナップインの追加と削除	? ×
スタンドアロン 拡張	
このページを使ってコンソールにスタンドアロン スナップインを追加または削除しま	:च.
スナップインの追加先(S): 🏾 📾 🖬 ンソール ルート	•
追加(D) 削除(R) パージョン情報(B)	
OK	キャンセル

5. 「証明書」を選択し、「追加」をクリックします。

スタンドアロン スナップインの追加		? ×
利用できるスタンドアロン スナップイン:		
スナップイン	ベンダ	
	Microsoft Corporation	
📓 パフォーマンス ログと警告	Microsoft Corporation	
ロ フォルダ		
ようしたしていたいには、していたいでは、	HighGround Systems, Inc.	
重ルーティングとリモート アクセス	Microsoft Corporation	
🕵 ローカル ユーザーとグループ	Microsoft Corporation	
	Microsoft Corporation	
	Microsoft Corporation	
きょう数ファイル システム	Microsoft Corporation	-
		Ľ
証明書スナップインを使うとユーザー、サービ	どス、またはコンピュータの証明書ストア	0
内容を表示できます。		
	j自to(A) PBL*2	5

6. 「コンピュータアカウント」を選択し、「次へ」をクリックします。

証明書スナップイン	X
このスナップインで管理する証明書:	
○ ユーザー アカウント(M)	
	〈戻る(8) (次へ(12) > キャンセル

「ローカルコンピュータ」を選択し、「完了」をクリックします。「スタンドアロンスナップインの追加」のウィンドウは「閉じる」にて Close してください。

コンピュータの選択	×
このスナップインで管理するコンピュータを選択してください。 このスナップインで管理するコンピュータ ・ ローカル コンピュータ(L): このコンソールを実行しているコンピュータ)	
○別のコンピュータ(A):	
□ コマンド ラインから起動したときは、選択されたコンピュータを変更できるようにする(W) これは、コンソールを保存した場合にのみ適用されます。	
< 戻る(B) 完了 キャンセル	

- 8. 「スナップインの追加と削除」のウィンドウにて「OK」をクリックし、ウィンド ウを閉じます。
- 9. 「証明書 (ローカルコンピュータ)」の+を展開し、「個人」ストアをマウスの右 ボタンでポイントし、「すべてのタスク」から「インポート」を選択します。



10. 「証明書のインポートウィザード」が起動します。「次へ」をクリックします。

証明書のインボートウィザード		×
	証明書のインポート ウィザードの開始	
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リ ストをディスクから証明書ストアにコピーします。	
	証明機関によって発行された証明書は、ユーザー ID を確認し、データ を保護したり、またはセキュリティで保護された接続を提供するための情 報を含んでいます。証明書ストアは、証明書が保管されるシステム上 の領域です。	
	続行するには、D欠へ] をクリックしてください。	
	< 戻る(B) (次へ(N)) キャンセル	

 「参照」クリックし、手順1で準備した「<u>servername. pfx</u>」を指定し、「次へ」を クリックします。

明書() イン)インボート ウィザード ボートする証明書ファイル
	インボートするファイルを指定してください。
	ጋァイル名(Ε):
	C¥tmp¥servername.pfx
	注意: 次の形式を使うと1 つのファイルに複数の証明書を保管できます:
	Personal Information Exchange- PKCS #12 (PFX,P12)
	Cryptographic Message Syntax Standard- PKCS #7 証明書(P7B)
	Microsoft シリアル化された証明書ストア(SST)
	< 戻る(B) (次へ(N) >) キャンセル

12. PKCS#12 ファイルを作る際に指定した PKCS#12 保護パスフレーズを入力し、「秘密 キーにエクスポート可能フラグを付ける」をチェックし、「次へ」をクリックしま す。

証明書のインポートウィザード	x
パスワード セキュリティを維持するために、秘密キーはパスワードで保護されていました。	
秘密キーのパスワードを入力してください。	
バスワード型: *******	
強力な秘密キーの(保護を有効にする(E) このオブションを有効にすると、秘密キーがアブリケーションで使われるたび に確認を求められます。	
▶ 秘密キーにエクスボート可能フラグを付ける(M)	
〈戻る(12) 〈次へ(12) 〉 キャンセル	J

13. 「証明書をすべて次のストアに配置する」を選択し、「次へ」をクリックします。

明書のインポートウ	ザード		
証明書ストア 証明書ストフ	は、証明書が保管されるシステム上の領域です。		
Windows (2	正明書ストアを自動的に選択させるか、証明書のナ	易所を指定することが	できます。
○ 証明	書の種類に基づいて、自動的に証明書ストアを選	択する(U)	
(ⓒ 罰明	書をすべて次のストアに配置する(P)		
EIB!	 書ストア:		
個人			参照(<u>R</u>)
	< 戻る	o(B) 🌔 次へ(N)	>) キャンセル

14. 「完了」をクリックします。

証明書のインポートウィザード	×
	証明書のインポート ウィザードの完了
	証明書のインポートウィザードが正常に完了しました。
	次の設定が指定されました。
	ユーザーが選択した証明書ストア 個人 内容 PFX
	ファイル名 C¥tmp¥servername.pfx
	< 戻る(B) (完了) キャンセル

15. 「OK」をクリックします。



16. 「インターネットサービスマネージャ」を起動し、サイトのプロパティを開きま す。 17. 「ディレクトリ セキュリティ」のタグより「セキュリティ保護された通信」の「サ ーバー証明書」を開きます。

既定の Web サイトのプロパティ 💦 🔀
Web サイト オペレータ パフォーマンス ISAPI フィルタ ホーム ディレクトリ ドキュメント ディレクトリ セキュリティ HTTP ヘッダー カスタム エラー ASP.NET Server Extensions
匿名アクセスおよび認証コントロール
┌ IP アドレスとドメイン名の制限
IP アドレスまたはインターネット ドメイン名を使用してこ のリソースへのアクセス許可を切り替えます。
編集型
セキュリティ保護された通信
このリソースへのアクセス時に、セキュリティ保護された通信 を要求し、クライアント証明書を有効にします。
記明書の表示(型)
編集(0)
OK キャンセル 適用(酒) ヘルプ

18. 「サーバ証明書ウィザード」が起動します。「次へ」をクリックします。



19. 「既存の証明書を使用」を選択し、「次へ」をクリックします。

サーバー証明書ウィザード	×
サーバー証明書 Web サイトに証明書を割り当てるには、3 種類の方法。	があります。
この Web サイトに使用する方法を選択してください:	
○ 証明書の新規作成(©)	
● 既存の証明書を使用(A)	
○ キー マネージャのバックアップ ファイルから証明書を	(ンポート(型)
	〈戻る(四) (次へ(11)) キャンセル

20. SSL/TLS サーバ証明書を選択し、「次へ」をクリックしてください。

ł	サーバー証明書ウィザー	-K				×
	使用可能な証明 Web サーバー	月書 -に使用可能な証明	書のリストは以下の	とおりです。		
	証明書を選択し	してください:				
	発行先	発行元	有効期限	使用目的	登録名	
	www.nii.ac.jp	NII Open Domai	2008/03/10	サーバー認証	くなし>	
	, 					
_						
				(夏5(B)	1/2 A (N) >	キャンクル
				THE P		11201

21. 証明書情報が表示されます。「次へ」をクリックします。

サーバー証明書ウィザード	×
証明書の概要 既存の証明書をインストー	มและสุด
以下の証明書が Web サーバー	-にインストール可能です。インストールするには、D欠ヘ]をクリックしてください。
証明書の詳細:	
発行先 発行元 有効期限 使用目的 登録名 国名/地域 市区町村 組織	www.nii.ac.jp NII Open Domain CA 2008/03/10 サーバー記記正 くなし> JP Academe National Institute of Informatics
	< 戻る(B) (二次へ(M)) キャンセル

22. 「完了」クリックします。IISを再起動してください。



設定したサイト証明書及び秘密鍵はバックアップを取って鍵ペア利用期間中は安全な場所 で保管してください。

3.6 IIS6

証明書のインストールにあたり、必要な証明書に関しては「1.3 証明書の種類」を参照してください。

3.6.1 中間 CA 証明書のインストール方法

- 中間 CA 証明書 (SecurityCommunicationRootCA1 認証局証明書:scroot1.crt と NII オープンドメイン認証局証明書:<u>niica.crt)</u>のファイルを開き、以下の作業を繰 り返します。
- 2. 証明書ダイアログボックスが表示されます。「全般」タブの[証明書のインストール]をクリックします。

証明書の)情報	
この証明書の目的	b :	
・電子メール	を保護する	
 リモートコン 12392200 	/ビューダ(J) IU を1未言止する ING1 1 NN GN1 1	
発行先: 発行者:	Security Communication RootCA1 http://www.valicert.com/	
有効期間	2005/03/16 から 2015/03/16	

3. 証明書マネージャインポートウィザードが表示されますので、「次へ」をクリック してください。



4. [証明書をすべて次のストアに配置する]を選択し、[参照]をクリックします。

			- 10	- 1 (1) 1 1
Windows (ご記明書ス	トアを目動的に選択る	させるか、証明書 (-ETBB寺コレフォ	の場所を指定する。 躍ってい	ことかできます。
● 副明書の種類	観と空りいし、目動的 7.ケハフトマ(「開業す	icallの日本人下がる 「ス7PNi	D∰1/(9@\ <u>U</u>)	
÷				

証明書ストア選択ダイアログボックスが表示されますので、[物理ストアを表示する]を選択します。
 ダイアログボックス内の項目[中間証明機関]のそばにある[+]マークをクリックし

タイプロクホックス内の項目[中間証明機関]のそはにある[+]マークをクリックして拡張し、[ローカルコンピュータ]を選択し、[0K]をクリックします。

証明書ストアの選択	? ×
使用する証明書ストアを選択してください(C)	
	-
レンストッ シンストッ 一一一 グループ ポリシー	
□ □ □ 信頼された発行元	_
□ □ □ □ 信頼されていない証明書	-
▼ 物理ストアを表示する(S)	
	- 1
<u> </u>	

6. 証明書ストアに「中間証明機関¥ローカルコンピュータ」が表示されている事を確認し、「次へ」をクリックしてください。

明書ストア 証明書ストアは、証明書が保管されるシ	ステム上の領域です。	
Windows に証明書ストアを自動的に選択	択させるか、証明書の場所を指注	定することができます。
○ 証明書の種類に基づいて、自動	的に証明書ストアを選択する(世)
● 証明書をすべて次のストアに配置	きする(<u>P</u>)	
証明書ストア:		
中間証明機関¥ローカル コンピ	ュータ	参照(<u>R</u>)

- 7. 「証明書のインポートウィザードの完了」が表示されたら、「完了」をクリックしてください。
- 8. 証明書のインポートウィザードが表示されます。[OK]をクリックします。

証明書の	(ンポートウィザード 🛛 🗙
i	正し、インボートされました。
	OK

SecurityCommunicationRootCA1認証局証明書とNIIオープンドメイン認証局証明書の インストールが終了したら、サイト証明書(SSL/TLS 証明書)をインストールします。

3.6.2 サイト証明書 (SSL/TLS サーバ証明書) のインストール方法

- 「3.1.2 IIS 利用の場合 openss1 による PKCS#12 ファイルの作成」を参照して 「*servername. pfx*」ファイルを準備します。
- 2. 「インターネットインフォメーションサービス (IIS) マネージャ」を起動し、サ イトのプロパティを開きます。
- 3. 「ディレクトリ セキュリティ」のタグより「セキュリティ保護された通信」の「サ ーバー証明書」を開きます。

定の Web サイトのプロパティ
Web サイト パフォーマンス ISAPI フィルタ ホーム ディレクトリ ドキュメント ディレクトリ セキュリティ HTTP ヘッダー カスタム エラー ASP.NET
認証とアクセス制御 医名アクセスを有効にし、このリソースの認証方法 を編集します。 編集(E)…
IP アドレスまたはインターネット ドメイン名を使用して このリソースへのアクセス許可を切り替えます。
編集型
このリソースへのアクセス時に、セキュリティで保護さ れた通信を要求し、クライアント証明書を有効に します。
単わらり 通用(日) へルフ

4. 「サーバ証明書ウィザード」が起動します。「次へ」をクリックします。



5. 「pfx ファイルから証明書のインポート」をチェックし「次へ」をクリックします。

IS 証明書ウィザード	×
サーバー証明書	
以下は、Web サイトに証明書を割り当てる方法です。	
この Web サイトに使用する方法を選択してください:	
○ 証明書の新規作成(○)	
○ 既存の証明書を使用(A)	
○ キー マネージャのバックアップ ファイルから証明書をインボート(○)	
● iptyファイルから言止明書のインボート(M)	
○ リモート サーバーからこのサイトへの証明書のコピーまたは移動(ど)	
< 戻る(B) (次へ(N) > _	キャンセル

6. 「参照」クリックし、手順1で準備した「*servername. pfx*」を指定します。「証明 書をエクスポート可能に設定」をチェックし「次へ」をクリックします。

IIS 証明書ウィザード	×
証明書のインボート .pfx ファイルから証明書をインボートできます。	
証明書を含むファイルの名前とパスを入力してください。 パスとファイル名(P):	
C.¥tmp¥servername.pfx	参照(<u>R)</u>
インボートした証明書を、インボート後にエクスボート可能として設定するかどうか指定 ボート可能として設定すると、セキュリティ上のリスクは高くなりますが、バックアップ用に調 モタスボートすることができます。 ▼ 調明書をエクスボート可能に設定(M)	してください。エクス 正明書をファイルに
< 戻る(B) (次へ(N) >	*+>tell

7. PKCS#12ファイルを作る際に指定したPKCS#12保護パスフレーズを入力し、「次へ」 をクリックします。

IIS 証明書ウィザード		×
証明書インボートのパスワード 証明書をインボートするには、パスワード	フードを入力する必要があります。	
インポートする証明書のパスワード	を入力してください。	
	< 戻る(B) (次へ(N) >	キャンセル

8. SSL/TLS サーバの TCP ポート番号を入力し「次へ」をクリックします。

IIS 証明書ウィザード			×
SSL ポート この Web サイトが使用する TCP ポートを指定	してください。		
この Web サイトが使用する TCP ボート(L):			
	< 戻る(B) ((注へ(N) >)_	キャンセル

9. 証明書情報が表示されます。「次へ」をクリックします。

以下のインポートお	へん アンクロン アン・ション アン・ション アン・ション アン・ション しょう アン・ション しょう
ファイル名:	C:¥tmp¥servername.pfx
証明書の詳細: 発行元 発行元期限 使用目的 フレンドリ名 国人地域 市区職 組織	www.nii.ac.jp NII Open Domain CA 2008/03/10 サーバー認証 くなし> JP Academe National Institute of Informatics

10. 「完了」クリックします。IIS を再起動してください。

IIS 証明書ウィザード	凶 Web サーバー証明書ウィザードの完了
	Web サーバー証明書ウィザードを完了しました。 このサーバーに証明書がインストールされました。 将来、証明書を更新、置換、または削除する必要がある場合には、こ のウィザードを再び使用してください。
	ウィザードを終了するには、「完了」をクリックしてください。
	< 戻る(B) (元7) キャンセル

設定したサイト証明書及び秘密鍵はバックアップを取って鍵ペア利用期間中は安全な場所 で保管してください。

3.6.3 サイト証明書(SSL/TLS サーバ証明書)の更新時のインストール方法 既に対象のサーバに証明書をインストールしている場合は、事前にインストールしている 証明書の削除が必要となります。下記に登録された証明書の削除方法を記述します。 1. 「インターネットインフォメーションサービス (IIS) マネージャ」を起動し、サ イトのプロパティを開きます。

11.44.71	
ved サイト ディレクトリイ	ハノオーマンス ISAPI ノイルタ ホーム ナイレクトリ トキュメン セキュリティ HTTP ヘッダー カスタム エラー ASP NET
忍証とアクセン	1
k -5	第名アクセスを有効にし、このリソースの認証方法 を編集します。 編集します。 「「「「編集」」
של ויש בי מי	
P / P / AZ I	
	IF アトレスまたはインターネットトメイン名を使用して このリソースへのアクセス許可を切り替えます。
w.	得生/1
セキュリティで1	保護された通信
	このリソースへのアクセス時に、セキュリティで保護させていていますのアクセス時に、セキュリティで保護させています。
~	れた通信を要求し、クライアント語山明書を有効に
	编集(<u>D</u>)

Web サーバー証明書ウィサードの	^{演奏} Web サーバー証明書ウィザードの開 始
	このウィザードがサーバーとクライアントの間のセキュリティで保 譲された Web 通信に使用されるサーバー証明書の作成と 管理のお手伝いをします。 Web サーバーの状態: 選択されたサーバーに証明書がインストールされました。証明 書ウィザードで、証明書を管理することができます。
	続行するには、「次へ] をクリックしてください。
	< 戻る(B) () (1) キャンセル

2. 「サーバ証明書ウィザード」が起動します。「次へ」をクリックします。

3. 「現在の証明書を削除する」をチェックし「次へ」をクリックします。

現在、この Web サイトには、証明書がインストールされています。 現在インストールされている証明書をどのように処理しますか?	Eの証明書の割り当ての変更	29 (1910 (193)	
現在インストールされている証明書をどのように処理しますか?	現在、この Web サイトには、証明書がイン	バストールされています。	ŧ
 現在の証明書を更新する(W) 現在の証明書を削除する(R) 現在の証明書を置き換える(A) pfx ファイルに現在の証明書をエクスポートする(X) リモート サーバー サイトに現在の証明書をコピーまたは移動する(C) 	現在インストールされている証明書をどの。	ように処理しますか?	
 現在の証明書を削除する(E) 現在の証明書を置き換える(A) pfx ファイルに現在の証明書をエクスポートする(X) リモート サーバー サイトに現在の証明書をコピーまたは移動する(C) 	○ 現在の証明書を更新する(₩)		
 ○ 現在の証明書を置き換える(A) ○ pfx ファイルに現在の証明書をエクスポートする(X) ○ リモート サーバー サイトに現在の証明書をコピーまたは移動する(C) 	● 現在の証明書を削除する(R)		
○ pfx ファイルに現在の証明書をエクスポートする(X) ○ リモート サーバー サイトに現在の証明書をコピーまたは移動する(<u>C</u>)	○ 現在の証明書を置き換える(<u>A</u>)		
○ リモート サーバー サイトに現在の証明書をコピーまたは移動する(C)	○ pfx ファイルに現在の証明書をエクスオ	ং−->ব্র(४)	
	○ リモート サーバー サイトに現在の証明	書をコピーまたは移動する(<u>C</u>)	
		< 戻る(B) (次へ(N))	> ++>セル

4. 現在インストールされている証明書を確認し「次へ」をクリックします。

IS 証明書ウィザード	X
証明書の削除	
証明書を保存し、後でこのサ	ーバーあるいは他のサーバーで再使用することができます。
D次へ] をクリックすると、この証	明書がサーバーから削除され、後で使用するために保存されます。
証明書の詳細: 発行先 発行元 有効期限 使用目的 フレンドリ名 国/地域 吉に町は	www.nii.ac.jp NII Open Domain CA 2008/03/10 サーバー認証 くなし> JP
組織	National Institute of Informatics
	< 戻る(B) (ご次へ(N)>) キャンセル

IIS 証明書ウィザード	X
	Web サーハー証明書ウィサートの完了
	Web サーバー証明書ウィザードを完了しました。
	証明書はアンインストールされました。
	証明書をこのサーバーに添付するには、Web サーバー証明書ウィザード を再起動してください。新しい証明書を作成、または保存された証明書 を再使用することができます。
	ウィザードを終了するには、「完了」をクリックしてください。
	< 戻る(B) 元了 キャンセル

5. 「完了」をクリックします。

6. 「3.6.2 サイト証明書 (SSL/TLS サーバ証明書)のインストール方法」の手順に従い、新しい証明書をインストールする。

番号	禁則文字	文字名称
1	!	exclamation mark
2	"	double quote
3	#	number sign (hash)
4	\$	Dollar
5	%	Percent
6	&	ampersand
7	(open parenthesis
8)	close parenthesis
9	*	Asterisk
10	/	oblique stroke
1 1	;	SEMICOLON
1 2	<	less than
13	>	greater than
14	?	Question mark
15	@	commercial at
16	[open square bracket
1 7	¥	backslash
18]	close square bracket
19	^	Caret
2 0		underscore
2 1		back quote
2 2	{	open curly bracket
23		vertical bar
2 4	}	close curly bracket
2 5	~	Tilde

DN の禁則文字