# 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

2012/3/30

国立情報学研究所

改版履歷				
版数	日付	内容	担当	
V.1.0	2009/5/15	初版	NII	
V.1.1	2009/6/4	誤植の修正	NII	
V.1.2	2009/7/13	旧プロジェクトからの移行に伴う補足の追加	NII	
		ルート CA 証明書インストール方法の修正		
		誤植の修正		
V.1.3	2009/8/6	誤植の修正	NII	
V.1.4	2009/9/11	誤植の修正	NII	
V.1.5	2009/10/13	DN 使用可能文字拡張	NII	
		誤植の修正		
V.1.6	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	NII	
		を追加		
		DNのルール記載変更		
		誤植の修正		
V.1.7	2011/6/3	文言を統一	NII	
V.1.8	2012/03/30	暗号アルゴリズムのセキュリティ対応に伴いサーバ証	NII	
		明書および CSR の鍵長 1024 ビット記載削除		

# <u>目次</u>

1.はじめに1
1-1.CSR とは1
1-2.OpenSSL の利用について1
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2
1-4.本書の範囲
2.IIS5.0 によるサーバ証明書の利用4
2-1.前提条件
2-2.事前準備
2-3.鍵ペアの生成と CSR の作成
2-3-1 鍵ペアの生成
2-3-2 CSR の生成
<b>2-4</b> .証明書の申請から取得まで11
2-5.証明書のインストール12
2-5-1 事前準備12
2-5-2 ルート CA 証明書のインストール14
2-5-3 中間 CA 証明書のインストール
2-5-4 サーバ証明書のインストール
2-6.サーバ証明書の置き換えインストール
2-7.起動確認

# 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 IIS5.0 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、[本プロジェクト])から発行された証明書を IIS5.0 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。

BEGIN CERTIFICATE REQUEST MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCS AxEDAOBgNVBAcTBOFjYWR bWUxKjAo BgNVBAoTIU5hdG vbmFsIE uc3RpdHVOZSBvZiBJbmZvcm1hdG jczEiMCAGA1UE  IGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkz 8TUF	CSR の例
MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCS AxEDAOBgNVBAcTBOFjYWR bWUxKjAo BgNVBAoTIU5hdG vbmFsIE uc3RpdHVOZSBvZiBJbmZvcm1hdG jczEiMCAGA1UE 	BEGIN CERTIFICATE REQUEST
BgNVBAoTIU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczEiMCAGA1UE IGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzl8TUF	MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCSIAxEDAOBgNVBAcTBOFjYWRIbWUxKjAo
lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzl8TUF	BgNVBAoTIU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczEiMCAGA1UE
lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzl8TUF	
BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzl8TUF	lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze
	BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzI8TUF
END CERTIFICATE REQUEST	END CERTIFICATE REQUEST

#### 1-2.OpenSSL の利用について

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 OpenSSL を利用することができます。 OpenSSL のインストール方法等は OpenSSL Project (http://www.openssl.org)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。 OpenSSL は最新版を使用することを強く推奨致します。

## 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	0	-	-
Apache2.0 系+mod_ssl	0	-	_
Apache-SSL	0	I	_
Tomcat	-	0	_
IBM HTTP Server	_	-	0
IIS5.0	0	-	-
IIS6.0	0	I	_
IIS7.0	0	-	-
IIS7.5	0	_	_

#### 【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	-	0	0
Apache2.0 系+mod_ssl	-	0	0
Apache-SSL	-	0	0
Tomcat	0	0	0
IBM HTTP Server	0	0	0
IIS5.0	0	0	0
IIS6.0	-	0	0
IIS7.0	-	0	0
IIS7.5	-	0	0

# 1-4.本書の範囲

本書では以下の(e、f)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.IIS5.0 によるサーバ証明書の利用

#### 2-1.前提条件

IIS5.0 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 Windows2000 Server、OpenSSL0.9.8k で CSR を作成し、Windows2000server ヘインストールする方法での実行例を記載しております)

前提条件	

- 1. 鍵ペア及び CSR を生成する端末に OpenSSL がインストールされていること。
- 2. 証明書をインストールする端末に IIS5.0 がインストールされていること

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.	乱数生成用ファイルの準備(200KB 程度のファイルであればどんなものでもかまいません)
	本マニュアルではファイル名を randfile1.txt、randfile2.txt、randfile3.txt とします。
2.	サーバ鍵ペア用私有鍵パスフレーズ <b>&lt;<u>PassPhrase</u>&gt;([2-3-1、2-3-2</b> で使用])
3.	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
	k))

Ver.1.8

CSR に記述する DN のルールは以下のとおりとなります	F。
-------------------------------	----

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。	0	JP 固定	
	例) C=JP			
State or Province	本認証局では使用しないでください。	×		
Name (ST)				
Locality Name(L)	本認証局では必ず「Academe2」と設定してく	0	Academe2 固定	
	ださい。			
	例)L=Academe2			
Organization Name(O)	プロジェクト参加申請時の機関名英語表記を	0	半角の英数字 64 文字	
	設定してください。この情報は各所属機関の		以内	
	登録担当者にお問い合わせください。		(記号は「'(),/:=」	
	例)0=National Institute of Informatics		と半角スペースのみ	
			使用可能〉	
Organizational	証明書を使用する部局等の名前を設定してく	Δ	・半角の英数字 64 文	
Unit Name(OU)	ださい。		字以内	
	(この値は省略可能です)		(記号は「'(),/:=」	
	(この値は複数設定することが可能です。複		と半角スペースのみ	
	数指定する方法につきましては、CSR 作成時ご		使用可能〉	
	使用のアプリケーションのマニュアルをご確		<ul> <li>複数 0U を指定する</li> </ul>	
	認ください。)		場合は、全体で 64 文	
	例 )OU=Cyber Science Infrastructure		字以内	
	Development Department			
Common Name (CN)	サーバ証明書 URL に表示されるウェブ・サー	0	証明書をインストー	
	バの名前を FQDN で設定してください。例えば		ルする対象サーバの	
	SSL/TLS を行うサイトが		FQDN で 64 文字以内	
	<u>https://www.nii.ac.j</u> p の場合には、		半角英数字、"."、"-"	
	「www.nii.ac.jp」となります。FQDN にはプロ		のみ使用可能。また、	
	ジェクト参加申請時に登録いただいた対象ド		先頭と末尾に"."と	
	メイン名を含む FQDN のみ、証明書発行が可能		"-"は使用不可	
	となります。			
	例)www.nii.ac.jp			
Email	本認証局では使用しないでください。	×		
	鍵長			

○···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2-6をご確認ください。

#### 2-3.鍵ペアの生成と CSR の作成

#### 2-3-1 鍵ペアの生成

以下に鍵ペアの生成方法を記述します。

	鍵ペアの作成
1.	鍵ペアを生成するため、「2-2.事前準備」の手続き1で用意したファイル(200 KB 程度)を3 つ選んでくださ
	い。この手続きでは、 選択したファイルの名前を「randfile1.txt」、「randfile2.txt」、「randfile3.txt」と
	して表記します。
2.	用意したファイルを、秘密鍵を保存するフォルダに移動してください
[	c:¥>COPY randfile1.txt c:¥work¥randfile1.txt
	c:¥>COPY randfile2.txt c:¥work¥randfile2.txt
	c:¥>COPY randfile3.txt c:¥work¥randfile3.txt
2	舞ぶアの佐武を始めるため、次のコマンバを入力) アノゼヤい(た唐いのブラウザによってけり 行り上で美子
э.	
	f)     f)
	[Servermanie.key]Cv.)/HHIV//////////////////////////////////
	C:¥> od c:¥work ← <u>作業フォルダへ移動してください</u>
	C:¥work>openss  genrsa -des3 -rand < <i>randfile1.txt&gt;</i> ; < <i>randfile2.txt&gt;</i> ; < <i>randfile3.txt&gt;</i> 2048
	> servername. key
	Generating RSA private key, 2048 bit long modulus
	······ ******
	unable to write 'random state'
	e is 65537 (0x10001)
	Enter pass phrase: < <u>PassPhrase</u> > ← <u>私有鍵パスフレーズ入力</u>
	Verifying - Enter pass phrase: < <u>PassPhrase</u> > ← <u>私有鍵パスフレーズ再入力</u>
重	要: この鍵ペア用私有鍵パスフレーズは、証明書のインストール時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。証明
書	のインストール後、サーバ停止・起動時にパスフレーズは求められません。
4.	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。

# 2-3-2 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。

に従い、DN 情報を入力してください。

	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 釒	旔
	ペアの生成]の手続き3で作成した私有鍵のパスフレーズを入力してください	
	C:¥work>openssl req -new -key servername.key -sha1 -out servername.csr← <u>CSR ファイル名</u>	
	Enter pass phrase for servername.key: 〈PassPhrase〉 ← <u>私有鍵パスフレーズ入力</u>	
L		
2.	パスフレーズの入力に成功すると DN 情報の問い合わせが行われますので、[2-2. 事前準備]の[DN ルール	レ]

	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 ( <u>"JP"を入力</u>	
	State or Province Name (full name) [Some-State]:. ← <u>[.」ドットの入力</u>	
	Locality Name (eg, city) []: <mark>Academe2 ←<u>Academe2 を入力</u></mark>	
	Organization Name (eg, company) [Internet Widgits Pty Ltd]:	
	National Institute of Informatics ← <u>組織名を入力</u>	
	Organizational Unit Name (eg, section) []:Cyber Science Infrastructure Development	
	Department ← <u>部局名を入力</u>	
	Common Name (eg, YOUR name) []: <mark>www.nii.ac.jp ← <u>サーパ名 FQDN を入力</u></mark>	
	Email Address []:. ← <u>[.」ドットを入力</u>	
	Please enter the following 'extra' attributes	
	to be sent with your certificate request	
	A challenge password []:.← <u>[.」ドットを入力</u>	
	An optional company name []:.← <u>[.」ドットを入力</u>	
		1
3.	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	一で
	は、[servername.csr])に保存されます。[BEGIN CERTIFICATE REQUEST]から[F	END
	CERTIFICATE REQUEST]で囲まれた部分が CSR となります。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-----

 ${\tt MIIBhDCB7gIBADBFMQswCQYDVQQGEwJKUDEQMA4GA1UEBxMHQWNhZGVtZTEMMAoG}$ 

例

UmOE3vq8Ajg=

-----END CERTIFICATE REQUEST-----

4. 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。

```
C:¥work>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) <u>←鍵長が 2048bit であることを確認してください。</u>
              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:
```

# 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証明書発行申請 TSV ファイルを作成し申請します。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。

サーバ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。このメールは、電子署名されています。

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 ヘアクセスし、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/~

#### 2-5.証明書のインストール

本章では IIS5.0 へのサーバ証明書のインストール方法について記述します。

※サーバ証明書発行・導入における啓発・評価研究プロジェクト(以下、旧プロジェクト)より発行したサーバ証明書 を利用しているサーバへ導入する場合は、事前に、別冊「証明書自動発行支援システム旧プロジェクトからの移行 補足」を読み、設定の変更をお願いします。

#### 2-5-1 事前準備

事前準備として、サーバ証明書、中間 CA 証明書を取得してください。また、ルート CA 証明書がインストールされているか確認を行ってください。

※別冊「証明書自動発行支援システム旧プロジェクトからの移行補足」で、ルート CA 証明書のインストールを終 えている場合は、ルート CA 証明書の確認、ルート CA 証明書のインストールは不要となります。

	事前準備		
1.	[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 という名前で任意の場所に保存して		
	ください。(本マニュアルではローカルディスクの work ディレクトリ[C:¥work]に保存しています。)		
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リポジトリにアクセスすることが可能です)		
	リポジトリ: <u>https://repo1.secomtrust.net/sppca/nii/odca2/</u>		
	BEGIN CERTIFICATE		
MII	EVDCCAzygAwIBAgIEErmwxzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJK		
UDE	YMBYGA1UEChMPU0VDT00gVHJ1c3QubmV0MScwJQYDVQQLEx5TZWN1cml0eSBD		
b21	tdW5pY2F0aW9uIFJvb3RDQTEwHhcNMDkwMzI3MDMxMzUxWhcNMTkwMzI3MDMx		
MzU	lxWjB9MQswCQYDVQQGEwJKUDERMA8GA1UEBxMIQWNhZGVtZTIxKjAoBgNVBAoT		
IU5	IU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczENMAsGA1UECxMEVVBL		
STE	gMB4GA1UECxMXTklJIE9wZW4gRG9tYWluIENBICOgRzIwggEiMAOGCSqGSIb3		
DQE	BAQUAA4IBDwAwggEKAoIBAQDgFG0JGEjnMbJg14i00KK4qPNr1gw0IZwJRIdh		
4L3	cYh6+sKhn/ISvIiCcbKFsGas9bj27d9N4dnzhyQaaurVmLFyFYtYdv8feyKcm		
SN7	UYUM4SoeAeq6990CPTLIQw2aehkPSGHy7ecH1JX6UYw/40pmFNc+ITIDjqf0+		
mwJ	ITRM8CtTwvegL7k5fZYinXXtXnh0aiho91/mqDErWOw+AIpPTCDoQBnq1BJzSJ		
h+9eMBqj1BrjcXULOpqBvzVz5IBXgrUq3zmVg3yjTGNErLnBg3xGxRwxgfCSo6vZ			
e6MpUePb7YarCGJ99L2ENGd0p53A0m8rXyWOK9WSLdbQ9h4jAgMBAAGjggEHMIIB			
AzAdBgNVHQ4EFgQUewoH9xjKjA7W2rxQgGwsRwLRDfswHwYDVROjBBgwFoAUoHNJ			

mWjchVtI45soL1efvT08B0gwEgYDVR0TAQH/BAgwBgEB/wIBADA0BgNVHQ8BAf8E BAMCAQYwSQYDVR0fBEIwQDA+oDyg0oY4aHR0cDovL3JlcG9zaXRvcnkuc2Vjb210 cnVzdC5uZXQvU0MtUm9vdDEvU0NSb290MUNSTC5jcmwwUgYDVR0gBEswSTBHBgoq gwiMmxtkhwUBMDkwNwYIKwYBBQUHAgEWK2h0dHBz0i8vcmVwb3NpdG9yeS5zZWNv bXRydXN0Lm5IdC9TQy1Sb290MS8wDQYJKoZIhvcNAQEFBQADggEBAKoqogcGLHdD lkXmNjCkI9kXn9I8zHNn7x03YdMYkgsIkYSAic9+HwWHJPV12/ba0xigpGKkY2vc SEDwAiHqSsVTHrzY6QyERVSaalk+C74+sxjxw1JG5LcH+wgt+ExA4mZPAS7v0fgD kni+7IP9YrILR19E6K2AQW6G3Df8zhnk0f2+kl+lavDvT74Krh0FojYZTGF6DFIo kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2IfP/rWbg2J1Ige zZc6shCn3VdrL2douVFjaAX1c8zwys/KIpLzNSx00GwJdKxFTaIzH/emcqKj93Jd DC1rrFMhoPE=

-----END CERTIFICATE-----

 ルートCA証明書を確認します。Internet Explorerを立ち上げ、[ツール(T)]→[インターネットオプション(O)]で 表示されるインターネットオプション画面より[コンテンツタブ]を選択し、[証明書(C)]ボタンを押して証明書スト アを表示してください。証明書画面で[信頼されたルート証明機関]のタブを選択し、発行先[Security Communication RootCA1]、発行者[Security Communication RootCA1]の証明書がある場合は、ルート CA 証明書の取得は不要となります。無い場合は、以下、「2-5-2 ルート CA 証明書のインストール手続き」に 従い、ルート CA 証明書の取得、インストールを実施してください。

#### 2-5-2 ルート CA 証明書のインストール

以下の手続きに従って、ルート CA 証明書のインストールを行ってください。

※別冊「証明書自動発行支援システム旧プロジェクトからの移行補足」で、ルート CA 証明書のインストールを終 えている場合、また[2-5-1 事前準備]でルート CA 証明書が存在した場合は、本手続きは不要となります。次の 「2-5-3 中間 CA 証明書のインストール」へ進んでください。

	ルート CA 証明書のインストール
1.	InternetExprorerを開始して、次のサイトに接続してください。
	URL : https://repository.secomtrust.net/SC-Root1/index.html
	「Security Communication RootCA1 Certificate(SCRoot1ca.cer)」と記述されたリンクを選択してく
	ださい
	③ Security Communication Root/OA1 Repository - Microsoft Internet Explorer ライルシ 編集の 表示の お知(ス)(4) シールの ハル749
	▲ # # > れら安心を 北会へ、
	Security Communication RootCA1 Repository
	Security Communication RootCA CP/CPS最新パージョン - Certificate Policy and Certification Practice Statement -
	日本超級 - Japanese -  • 逻Certification Practice Statement(SCRootCPS aff) version 400 2009-5-29 release (2009年5月29日 公表)
	■ <u> 下位CA用, Certificate Policy(SCRootCP1 ad1) version 400</u> 2009-5-29 release (2009年5月29日 公表)
	・ 医タイムスケンブ用 Cartificate Policy(SCRootCP2 pdf) version 3.00 2009-5-29 releases (2008年5月29日 公表)
	Security Communication RootCA1 証明書 - Security Communication RootCA1 Certificate -
	Security Communication RootCA1 Certificate(SCRoot1ca.cer)
	Fingerprint(SHA1) = 3681 2849 F981 9ED7 4C9E BC38 0FC6 568F 5DAC B2F7 Fingerprint(SHA1) = 518C 636A 54F0 F527 F5CD F71A F34D 6F4A
	■スタート) ● ③ ① ) 9 マイ コンビューク / Gr CV Grindrustsecontrus. ] _ CVM000KStrysten22.   自1 Security Communica. 9
2.	ファイルのタリンロード - セキュリアイ警告ワインドワか表示されますので、[保存(5)]を選択してくたさい。
	ファイルのダウンロード - セキュリティの警告
	このファイルを開くか、または保存しますか?
	名前: SUFWORTLEACEY 種類: セキュリティ証明書, 862 バイト
	発信元 repository.secomtrust.net
	インターネットのファイルは役に立ちますが、このファイルの種類はコンピュータに問題 を起こす可能性があります。発信を元が最新できない場合は、このソフトウェアを開 においたりますのでは、「ありません」は考古し、このソフトウェアを開
	◆ いだりまけつだりしないていたという」 <u>にためまれ合われて</u>
L	





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( <u>C</u> )
□ □ □ 信頼されたルート証明機関 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
● 物理ストアを表示する(S) OK キャンセル
9. 証明書ストアが[信頼されたルート証明機関¥ローカルコンピュータ]であることを確認し、[次へ(N)]を選択して ください。
IPIB書のインボート ウィザード       区         IEIの目書ストア       IEIの目書太小Pな、IEIの目書太小Pを違かです。         Windows (IEIの目書ストアを違かでよこのは気できるとかできます。       ・         ・       IEIの目書なんア         ・       IEIの目書なんでなのストアに配置する(P)         「PI目書なったア       ●照(R)         ・       IEIの目書の場所開開(#10 - カルコンピューダ)         ●照(R)
10. セキュリティ警告画面が表示されますので、拇印が「Fingerprint (SHA-1) = 36 b1 2b 49 f9 81 9e d7 4c 9e
bc 38 0f c6 56 8f 5d ac b2 f7]であることを確認して、[はい(Y)]を選択してください。
11. [正しくインポートされました]が表示されたら、インストールが終了です。[OK]を選択し、証明書インポートウィザ ードを終了してください。

証明書のインポートウィザード × 正しくインポートされました。 OK
19 インストールされた証明書を確認するために 東前進備と同様の方注で発行生「Security Communication
RootCA1 路行考[Security Communication RootCA1] [Fingerprint (SHA-1) = 36 b1 2b 49 f9 81
$20 d7 da 00 ba 28 0f a6 56 8f 5d og b2 f71 (55.5 \times 10^{-5})$
13 上記を確認後 証明書の利用方法の変更を実施します 証明書画面上り 当該の証明書を選択しダブルクリッ
$\frac{10}{7} + \frac{10}{7} + \frac{10}{10} + \frac{10}{$
個人   ほかの人   中間証明機関 (言頼されたルート証明機関) 信頼された発行元   信頼されない発行元
発行先 第二日本
インポートФ     「町除(R)       詳細設定(A)
証明書の目的
表示①
 閉じる(©)
14. 証明書詳細画面が表示されますので、[詳細]のタブを選択し、[プロパティの編集(E)]を選択してください。

	ごりお       2 ×         全般       11900/12         東市会       (オペア)         アールド       値         「パールド       値         「パールド」       0         三方・フジュン       V3         ジリアル番号       00         三素行手者       Security Communication Root         「オガル開影の終す       2023年9月30日 132049         「サブジェクト       Security Communication Root         「パール・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・
15. 証明書プロパティ画面で[4	全般]タブを選択してください。
[次の目的だけを有効にす	-る(O)]のラジオボタンにチェックを入れると、下部の証明書の目的部分のチェック
ボックスの編集が可能とな	ります。 <u>以下の項目以外のチェックボックスをすべて外してください。</u>
<ul> <li>(ア) サーバー認証</li> <li>(イ) クライアント認証</li> <li>(ウ) 電子メールの保護</li> <li>(エ) コード署名</li> <li>(オ) タイムスタンプ</li> <li>(カ) 1.3.6.1.5.5.7.3.9</li> </ul>	

Microsoft 信頼リストの署名         Microsoft なり、28'77         目的の追加(P)         0K       キャンセル         道用(A)         16. (手続き 15 項目(力))が利用目的の一覧に表示されていない場合は、[目的の追加(P)]を選択し、[ユーザ定
義の目的]画面に「1.3.6.1.5.5.7.3.9」の値を入力し、[OK]を選択してください。
ユーザー定義の目的       ▼         追加する証明書の目的のオブジェクト ID (OID) を入力         してください。         OK       キャンセル         17. 証明書プロパティ画面に戻り[適用(A)]を選択後、[OK]を選択してください。

証明書のプロパティ
全般   クロス証明書
フレンドリ名(E): SECOM Trust Systems CO LTD 説明(D):
<ul> <li>○ この証明用書の目的をすべて有効にする(E)</li> <li>○ この証明用書の目的をすべて無効にする(Q)</li> </ul>
○ 次の目的だけを有効にする(型) 注意:証明のパスで許可された証明書の目的しか編集できない場合があります。
▼ サーバーI228正 ▲
✓ クライアント認証     ✓ コード署名
マ 電子メールの保護
□ [microsoft 137#)/人の43-25 □ Microsoft タイム スタンプ
 OK キャンセル 適用( <u>A</u> )
18. 証明書詳細画面に戻るので、[OK]を選択し、画面を閉じてください。
<b>証明書</b>
全般 [詳新冊]] 証明のパス
表示(S): 〈すべて〉 🔽
フィールド 値 ■バージョン V3
<ul> <li>マリアル番号 00</li> <li>著名アルゴリズム sha1RSA</li> </ul>
三発行者     Security Communication Root       三有効期間の開始     2003年9月30日       1320.49
■有効期間の終了 2023年9月30日 13:20:49 ■サブジェクト Security Communication Root
ブロバティの編集(型)ファイルにコピー(型)
OK
19. 証明書画面に戻るので、証明書の目的の欄に以下の項目が表示されていることを確認し[閉じる(C)]を選択し
てください。
(ア) サーバー認証
(イ)クライアント認証
(ウ) 雷子メールの保護
(エ)コード者名
(オ) タイムスタンプ

(力) 1.3.6.1.5.5.7.3.9	
記明書 目的(N): 「 個人 (ほかの人) 中間証明機関 (信頼されたルート証明機関 ) 信頼された発行元 ) 「 第行先 第行者 有効期限 ] フレンドジ名   第GTE CyberTrust GL。GTE CyberTrust Glob 2018/08/ GTE CyberTrust 岡 Microsoft Root Aut Microsoft Root Autho 2020/12/ Microsoft Root ■Security Communic Security Communicati 2023/09/ SECOM Trust Sy	
インボートの エクスボート(E) 削除(B) 詳細設定(A) 「証明書の目的 1.361.55.73.9、タイム スタンプ、電子メールの保護、コード署名、クライアント認証、サーバー認証 表示(い) 閉じる(C)	
以上で、ルートCA証明書のインストールは終了となります。	

#### 2-5-3 中間 CA 証明書のインストール

以下の手続きに従って、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
1.	「2-5-1.事前準備」で取得した中間CA証明書 nii-odca2.cer をダブルクリックしてください。
2.	[証明書]ダイアログが表示されます。発行先と発行者を確認した後、[全般]タブの[証明書のインストール( <u>1</u> )]
	ボタンをクリックします。
	発行先:NII Open Domain CA-G2
	発行者:Security Communication RootCA1
	証明書     ? ×
	全般  詳細  証明のパス
	証明書の情報
	この証明書の目的::       ・リモート コンピュータの ID を保証する         ・リモート コンピュータに ID を証明する         ・電子メールを保護する         ・型子ンールを保護する         ・ソフトウェアがソフトウェア発行者の送信であるか確認する         *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:       NII Open Domain CA - G2         発行者:       Security Communication RootCA1         有効期間       から
3.	[証明書インポートウィザード]が表示されますので、[次へ( <u>N</u> )]ボタンをクリックします。 <sup>評明804/2ポートウィザード</sup> 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、証明表 証明長常(鮮リスト、および証明書)失効り 入をさくれたから証明者な下ルにごとします。 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 好な話しの情報を含んではす。証明者が保留され さうスエム上の情報です。 続行するには、Dた人)をカリックして(ださい。
4.	└訨明書をすべて次のストンに配置する( <u>P)</u> 」を択一し、└参照( <u>R</u> )」ホタンをクリックします。

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。

証明書のインボート ウィザード

証明書ストア:

5. [証明書ストアの選択]ダイアログが表示されますので、[物理ストアを表示する(<u>S</u>)]をチェックしてください。 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、[OK]ボタンをクリックしてください。

\_\_\_\_\_\_参照(<u>R</u>)...

< 戻る(B) 次へ(N) > キャンセル

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)	
● ● エンタープライズの信頼	-
□ □ □ 1 3// 1921 9 1 □ □ □ 信頼された発行元	-
▼ 物理ストアを表示する(S)	
OK **>	ยน

6. 証明書ストアに「中間証明機関¥ローカル コンピュータ」が表示されていることを確認し、[次へ(<u>N</u>)]ボタンをクリ ックします。

	<b>証明書のインポート ウィザード</b> X
	<b>証明書ストア</b> 証明書入トアは、証明書が保留されるシステム上の領域です。
	Windows(証証明書入トアを自動的に定確状をせるか、証明界書の場所を指定することができます。 ・ 「証明書の経境に基づいて、自動的に証明書入トアを選択する(型) 「証明界書入トア: 「中間証証明細関約ローカル・コンピュータ」 「中間証証明細関約ローカル・コンピュータ」
	〈 戻る(型 ) 次へ(型 ) キャンセル
7.	以下の確認画面が表示されたら、[完了]ボタン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が表示さ
	れます。[OK]ボタンをクリックします。

8. 証明書のインポートウィザードが表示されます。[OK]ボタンをクリックします。

#### 2-5-4 サーバ証明書のインストール

新規で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
1.	[2-5-1.事前準備]で取得したサーバ証明書と[2-3-1.鍵ペアの生成]で生成した私有鍵を PKCS#12 ファイル
	にします。サーバ証明書と私有鍵を同じフォルダ内に配置し、以下のコマンドを実行してください。カレントフ
	ォルダ内に、鍵ペアとサイト証明書(SSL/TLS 証明書)を連結した PKCS#12 の[servername.pfx]が作成されま
	す。
	C:¥work>openssl pkcs12 -export -inkey servername.key -in server.cer -out servername.pfx
	Enter pass phrase for servername.key: <b>〈PassPhrase〉</b> ← <u>2-3-1 で入力したパスフレーズを入力」</u>
	Enter Export Password: 〈PassPhrase〉
	Verifying - Enter Export Password: 〈 <b>PassPhrase</b> 〉 ← <u>PKCS#12 保護パスワード再入力</u>
2.	[ファイル名を指定して実行]より[mmc]と入力して、[OK]ボタンをクリックします。MMC コンソールが立ち上がり
	ます。
	7ァイル名を指定して実行 ?×
	実行するプログラム名、または開くフォルダやドキュメント名、インターネットリソース名を入力してください。
	名前②: mmc III
	OK 参照(B)
3.	メニュー・バーの[コンソール( <u>C</u> )]から[スナップインの追加と削除( <u>M</u> )]を実行してください。
	上書き1+45 名前を付けて保存( <u>A</u> )
	スナップインの追加と削I除( <u>M</u> ) Ctrl+M オプション(P)
	1 C-¥WINNT¥system32¥compmgmt
	2 C#WIINN i#System32#Inetsrv#iis 
4.	Lスナッフィンの追加と削除」ダイアログが表示されます。L追加( <u>D</u> )」ボタンをクリックします。

	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す。
	スナップインの 🚔 コンソール ルート 🗾 💼
	説明
5	「フタンドアロン、フナップインの追加]ダイアログがまことれまナ「訂明ま]を選択」「迫加(ハ)デタンクション
э.	レクシャティーン ヘノッノインの迫加リアイノークかる小されより。し証明者」を選択し、「迫加(A)」かタンをクリック
	利用できるスタンドアロンスナップイン: スナップイン インダ 風ルーティングとリモートアクセス Microsoft Corporation アローカル ユーザーとグループ Microsoft Corporation アロイヤレスモニタ Microsoft Corporation 同共有フォルダ Microsoft Corporation 回証明接関 Microsoft Corporation 回証明接関 Microsoft Corporation 回証明書ランプレート Microsoft Corporation 同証明書ランプレート Microsoft Corporation 同証明書フナップイルシステム Microsoft Corporation 又 説明 証明書スナップインを使うとユーザー、サービス、またはコンピュータの証明書ストアの内容 を表示できます。
6.	[証明書スナップイン]ダイアログが表示されます。[コンピュータ アカウント( <u>C</u> )]をチェックして、[次へ( <u>N</u> )>]ボタ
	ンをクリックします。
	ま9月客人 <b>ナッ</b> ブインで管理する証明書: C ユーザーアカウント(M) C 井ードス アカウント(S) C <u>コンピュータ アカウント(S)</u>

メカヘ(N) > キャンセル

	ウィンドウは「閉じろ(C)」ボタンをクリック」、閉じてください
	スクとコージの交換     スク     ス     スク     ス     スク     スク     スク     スク     スク     スク     スク     スク     ス     スク     ス     スク     ス
	〈戻る(2) 売7 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]ボタンをクリックし、ウィンドウを閉じます。証明書マネージャ
	が MMC にインストールされました。
9.	次にサーバ証明書を個人ストアにインポートします。
	[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
	( <u>K</u> )]から[インポート]を選択します。
10.	[証明書のインホートワイサード]か起動します。[次へ(N)>]ホタンをクリックします。 「明書のインホートウィサード」 「「「「」」」」 「「」」」」 「「」」」」 「「」」」」 「「」」」」 「「」」」」 「「」」」」 「」」、 「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」 「
11.	[参照( <u>R</u> )]ボタンをクリックし、手続き 1 で準備した[servername.pfx]を指定し、[次へ(N)>]ボタンをクリックしま

	す。
	IB明書のインボートウィザード     ×       インボートするEPH書ファイル インボートするファイル名信と     マアイル名信と       アイル名信と     学照(E)       「2WorkWservername.pfx     学照(E)       注意: 次の形式を使た:1 つのファイルに複数の証明書を(保管できます: Personal Information Exchange - PKOS #12 (PFX.P12)     Prisonal Information Exchange - PKOS #12 (PFX.P12)       Cryptographic Message Syntax Standard - PKOS #7 証明書 (P7B)     Microsoft シリアル化された証明書ストア (SST)
	(反る(位)) (次へ(位)) 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
	フクを付ける( <u>M</u> )」にナエックし、[次へ( <u>N</u> )]ホタンをクリックします。
	<b>パスワード</b> 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。
	総密キーのパスワードを入力してください。 パスワード(2): ★**** ■ ジェカルがの密キーの(発展を有り加速さん):
	に加えるないようめに、ものに、「カレートリン」フェントになっている。 「「「「総治キーにエクスポート可能フラグを付ける(W)」
13.	[証明書をすべて次のストアに配置する( <u>P)</u> ]を選択し、[次へ( <u>N</u> )>]ボタンをクリックします。
	正明書のインポートウィザード  正明書ストア  正明書ストアは、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。         ● 証明書の種類に送るいて、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・         (個人)
14.	[完了]ボタンをクリックします。

	証明書のインボートウィザード
	証明書のインボートウィザードの完了         証明書のインボ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-8       C.\#work\#servername.pfx
15.	[OK]ボタンクリックします。
	証明書のインボートウィザード 正しくインボートされました。 OK
16.	次に、サーバ証明書をIIS5.0に設定します。[スタート]→[プログラム( <u>P</u> )]→[管理ツール]→[インターネットサー
	ビスマネージャ]を選択し、インターネットサービスマネージャを開いてください。Web 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]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(S)]を開きます。
	設定の Web サイトのプロパライ       2 ×         Web サイト       オペシーク       パフォーマンス       ISAPI フィルタ       ホーム ディレクトリ       ドキュジント         ディレクトリ セキュリティ       HTTP ヘッダー       カスタム エラー       Server Extensions         ご 個名 アクセスある(UZ) エントロール       ビネット       ビネット       第二       編集(ビー         ●       ビネックセスを有効にし、このリソースの認知法方法を編集       編集(ビー       編集(ビー         ●       アドレスとドメイン名の海豚
18.	[サーバ証明書ウィザード]が起動します。[次へ( <u>N</u> )>]ボタンをクリックします。

	サーバー証明書ウィザードへようこそ	×	
	the second se	ーバー証明書ウィサードへようこそ	
	U.	)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護された Web 通信に 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。	
	We	b サーバーの状態: b サーバーに証明書がインストールされておらず、保留中の要求もありません。サ <→証明書やパードが、の Web サーバーのかめの証明書の新規作成、ある()	
	it)	現存の証明書の添付のお手伝いをします。	
		◇】をクリックして続行してください。	
19.	[既存の証明書を使用(A)]を選択し、[次~	-(N)>]ボタンをクリックします。	
	サーバー証明書 サーバー証明書 いたサイバー証明書		
	web リコ PにJulie Public	- こしには、3 種実現(リカ)法が使ります。	
	C 証明書の新規作成(2)		
	○ 既存の証明書を使用(点)		
	C キー マネージャのバックアッ:	ブ ファイルから証明書をインポート(Q)	
		< 戻る(B) 次へ(N) > キャンセル キャンセル	
20	インポートした SSL/TLS サーバ証明書を	選択し、「次へ(N)>]ボタンをクリックしてくた	<i>*</i> さい
20.	サーバー証明書ウィザード	x	
	使用可能な証明書 Web サーバーに使用可能な証	明書のリストは以下のとおりです。	
	証明書を選択してください。		
	発行先   発行元  example.nii.ac.jp    NII Open Domain (	有効期限   使用目的   登録名 CA 2010/05/13 サーバー試証 <なし>	
	1		
		〈 戻る(日〉 (水へ(N) 〉 キャンセル	
91			
21.	証明者情報が衣小されます。[伏へ( <u>N</u> )/]ス	<i>▶७ ✓ 𝔄 У У 𝒴 𝒴 𝔅</i>	

サーバー証明書ウィザード	×
<b>証明書の概要</b> 既存の証明書をインストールします。	
トリアの770日本がいい。 は、 パーインコート オマがホナーノンコート オナスワイナ ひんえう ナトロートリーアノギン	
レス FOUREWH書か「Web リーハーにイリストールPJ REU 9。インストール 9 GUCは、レスペリ をジリタリしていたさ	· *•
ⅡⅢ28月書の01単4番 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
発行元 example nitac.pp 発行元 NII Open Domain CA 有分類開現	
使用首約 サーバー記録正 登録名 ない	
国名/地域 JP 市区町村 Academe2 組織 National institutes of inforantics	
部門名UPKI	
22. [完了]ボタンをクリックします。	
サーバー証明書ウィザード	X
サーバー証明書ウィザートの完了	
Web サーバー証明書ウィザードを完了しました。	
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 を再び使用してください。	ウィザード
[完了]をクリックしてウィザードを終了してください。	
< 戻る(但) <b>元7</b> キ	eンTZIL

#### 2-6.サーバ証明書の置き換えインストール

更新した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。

既に IIS5.0 に証明書をインストールしている場合は、インストールしている旧サーバ証明書の削除が必要となります。下記にサーバ証明書のエクスポート・削除方法を記述します。



	証明書のエクスポート ウィザード 🛛 🔀
	<b>秘密キーのエクスポート</b> ができょうますUPTのセレーンをJUTTのセレーンをJUTTのセレーン
	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
5.	[次へ( <u>N</u> )>]ボタンをクリックします。
	証明書のエクスポート ウィザード エカフォート フィイリの形式
	とおさまなファイル形式で証明書をエクスポートできます。 
	使用する形式を確択してください。
	DER, encoded binary X509 (OER)( <u>0</u> )     C Base 64 encoded (X509 (OER)(5)
	<ul> <li>Cryptographic Message Syntax Standard - PKOS #7 証明書 (P7B)(Q)</li> <li>「目明のパないた方言明書表面音が方針パズオズで含み(0)</li> </ul>
	C Personal Information Exchange - PKCS 創2 (PFX)(例) 「 ISTRID(パン)(本文目的日本の10年本の10年本の10日本の20日)
	■ ミローカル いえこのショニット者 マット RC C の いな タイ C E G () マ 強力な保護を有効にする (E 50, NT 40 SP4 またはそれ以上が必要)(E)
	□ 正し、エクスポートされたときは秘密キーを削除する(2)
6.	サーバ証明書を PKCS#12 にエクスポートします。 PKCS#12 の保護パスフレーズを入力してください。
	二度パスフレーズを入力したら、「次へ( <u>N</u> )」ボタンをクリックします。
	<b>パスワード</b> 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しなければなりません。
	パスワードを入力してください。
	パスワード(P):  **** パスワードの確認スカ(Q):  ****
	〈 戻る(B) 法へ(M) 〉 キャンセル
7.	エクスポートするサーバ証明書の保存先を指定します。「次へ( <u>N</u> )」ボタンをクリックします。

	証明書のエクスポートウィザード ▼						
	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー						
	·						
	C¥work¥servername_backup.pfx						
	〈戻る(B) 次へ(W) キャンセル						
8.	[完了]ボタンをクリックします。[証明書エクスボートウィザード]ダイアログが表示されるので、[OK]ボタンをクリ						
	ックします。						
	■昭明書のエクスポート ウィザード ×						
	証明書のエクスポート ウィザードの完了						
	証明書のエクス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。 ファイル名 C¥work¥servernami キーのロクスポート (ない)						
	i証明のパスにあるすべての証明書を含める (パパス ファイルの形式 Personal Information						
	_ 〈 戻る(B) <u> </u>						
9.	次に、更新対象の旧サーバ証明書を削除します。[スタート]→[プログラム( <u>P</u> )]→[管理ツール]→[インターネ						
	ットサービスマネージャ]を選択し、インターネットサービスマネージャを開いてください。Web サイトのプロパテ						
	ィを開きます。						
10.	[ディレクトリ セキュリティ]のタブより[セキュリティで保護された通信]の[サーバー証明書( <u>S</u> )]を開きます。						
	既定の Web サイト (停止)のプロパティ 😰 🗙						
	Web サイト オペレーカ 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 Server Extensions						
	田田名アクセスおよび認証エントロール・ 田名アクセスを有効にし、このリソースの認認証方法を編集 します。 (日本に)						
	編集 (0						
	セキュリティ保護された通信 このリントスへのアクセス時に、セキュリティ保護された通信 「サニアニ資格財産に」						
	を要求し、カライアン「証明書を有効にします。 証明書の表示・(ジー)						

11.	サーバ証明書ウィザード]が起動します。「次へ( <u>N</u> )」ボタンをクリックします。
12.	[現在の証明書を削除する( <u>R</u> )]をチェックし「次へ( <u>N</u> )」ボタンをクリックします。
	サーバー証明書ウィザード 💌
	現在の証明者の割り当ての変更 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と処理しますか? (*)現在の証明書を更新する(W)
	<ul> <li>○ 現在の証明書を削除する(£)</li> </ul>
	● 現在の証明書を選ぎ換える(2)
	< 戻る(型) 次へ(型) キャンセル
13.	削除するサーバ証明書を確認し「次へ(N)」ボタンをクリックします。
	サーバー証明書ウィザード
	計切まの的場合 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。
	じ欠へ」をクリックすると、この証理明書がサーバーから削減され、(後で使用するために(保存されます。 Ⅲ7回日書のⅡ半編
	1975年 example.niiac.jp 第17元 NIIOpen Domain CA 推行規程限
	使用自合う サーバー-記録 数45 イスレン 国法(地域 JP TOTAT Anadom?
	報題 11 Production And Advisor
	〈戻る(8) 「次へ(10)」 キャンセル
14.	完了]をクリックします。

サーバー証明書ウィザード () () () () () () () () () ()	▼ サーパー証明書ウィザードを完了しました。 証明書なかサーバー証明書なた。 証明書なのサーバーCインストールざれました。 証明書なのサーバーCインストールざれました。 証明書なのサーバーCインストールざれました。 証明書なたのサーバーCインストールざれました。 このサーバーCインストールざれました。 このサーバーCインストールざれました。 このサーバーCインストールざれました。 このサーバーCインストールざれました。 このサーバーCインストールざれました。 このサーバーCインストールざれました。 このサーバーETUP書では、または1年存された証明書で、 「売了」をグリックしてウィザードを終了してください。
15. [2-5-3 サーバ証明書のインストール方	(R36) <b>先7</b> キャンル (R36) (R7) キャンル

# 2-7.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.	[スタート]→[プログラム( <u>P</u> )]→[管理ツール ビスマネージャを開いてください。	√]→[インター	-ネットサービスマネージャ]をう	選択し、インターネットサー			
2.	[Web サイト]にカーソルをあわせ、マウスの <b>第409-494 42734-922 サービ</b> 第4年回 表示型 「 <del>年</del> → 1 97- 100-494 42734-932 サービ 日 供給 (100-494 42734-932) サービ 日 供給 (100-494 42744-934-944-944-944-944-944-944-944-944-9	D 右ボタンで 2 回 × □ 2 頃 Scripts	[開始]を実行してください。				
3.	当該のサーバに接続し、SSL 通信が行え	ることを確認	してください。				