「サーバ証明書の発行・導入における評価・啓発研究プロジェクト」および「UPKI オープンドメイン証明書自動発行検証プロジェクト」の変更点について（加入者編）

「サーバ証明書の発行・導入における評価・啓発研究プロジェクト」(以下、旧プロジェクト)に参加し、サーバ証明書の発行を受けていた加入者の方が、「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、新プロジェクト)から発行されたサーバ証明書へ移行するにあたって、新プロジェクトでの改善点や注意すべき事項について以下に記します

1. 旧プロジェクトからの改善点

新プロジェクトでは、発行・更新・失効申請の効率化を実現するために証明書自動発行支援システム(以下、「支援システム」)を導入しました。これにより、改善された主要な項目について以下に記します。

(ア) 申請様式が Excel 形式から TSV 形式になりました

新プロジェクトでは、Excel 形式の申請書を廃止して、TSV(タブ区切り) 形式の申請ファイルを使用することになりました。この申請 TSV ファイルは、加入者ご自身で作成していただくことを基本としていますが、実際の運用については機関によって異なる場合がありますので、詳細は機関の登録担当者の方にご確認ください。

⇒Web: TSV ツール（Web アプリ版）の使い方

https://upki-portal.nii.ac.jp/docs/odcert/software/tsvtool

(イ) 加入者が直接証明書をダウンロードできるようになりました

新プロジェクトでは、支援システムにアップロードされた発行・更新申請にもとづきサーバ証明書を発行した後、証明書取得 URL が記載されたメールを事務局から加入者の方に通知します。加入者の方は、この証明書取得 URL にアクセスすることで、登録担当者を介さずに直接サーバ証明書をダウンロードすることができるようになりました。

(ウ) 同一 FQDN で複数のサーバを利用している場合、証明書が 1 枚で済むようになりました

新プロジェクトでは証明書の使用許諾条件が変更になり、負荷分散や冗長化等の理由によって同一 FQDN で複数のサーバを利用している場合には、必要とする複数のサーバにコピーしてご利用いただくことができるようになりました。これ

は、負荷分散や冗長構成の場合は同一 FQDN の複数サーバはいずれも鍵ペア漏洩リスクが同等とみなすことができるためです。

ただし、同一 FQDN であっても設置場所が異なるなど鍵ペア漏洩リスクが同等とは言えない場合は、被害を最小にとどめるためにも、旧プロジェクト同様サーバ毎に異なる鍵ペア・証明書をご利用いただくようお願いいたします。

2. 新プロジェクトへの移行のお願い

旧プロジェクトは平成 21 年 6 月 30 日を以て終了となりました。引き続き NII から発行されるサーバ証明書の利用を希望される場合は、新プロジェクトから発行されるサーバ証明書へ移行していただくようお願いいたします。**現在ご使用頂いているサーバ証明書は平成 21 年 9 月 30 日を過ぎると失効します**ので、それまでの間に加入者サーバのサーバ証明書を、新プロジェクトから発行される新しい証明書に置き換えていただくことになります。新プロジェクトで証明書の発行を受けるためには、加入者の所属する機関が新プロジェクトに継続参加いただいていることが前提となります。

3. 新プロジェクトでの新しい証明書の申請方法

旧プロジェクトで証明書発行済の加入者サーバに対して、新プロジェクトから証明書の発行を受ける場合であっても、**新プロジェクトでは新規の発行になりますので更新申請ではなく「発行申請」を行っていただく**必要があります。

「更新申請」は、新プロジェクトで証明書発行を受けた後に、証明書の再発行や記載事項の変更を行う際の手続きとなります。

なお、新プロジェクトでは「1 旧プロジェクトからの改善点.」(ア)で述べた通り Excel 形式の申請書を廃止し、TSV(タブ区切り形式)ファイルによる申請となります。

⇒Web: 利用の手引き→加入者編→「新規証明書発行申請手続き」
https://upki-portal.nii.ac.jp/docs/odcert/howto/ee#case1

⇒PDF: 利用の手引き　p.18 「5. 発行申請手続(登録担当者、加入者向け)」
https://upki-portal.nii.ac.jp/docs/files/odcert_tebiki.pdf

4. 旧プロジェクトでの古い証明書の失効方法

新プロジェクトへの移行期限である平成 21 年 9 月 30 日以降、旧プロジェクト認証局(NII オープンドメイン認証局)では以下の閉局作業を行います。

- 旧プロジェクト認証局が発行した全ての証明書の一括失効
- 上位 SC-Root1 による旧プロジェクト認証局証明書の失効

旧プロジェクトでは通常、新しい証明書への置き換えが完了した際には、旧証明書を失効するために置き換え完了通知を、登録担当者経由でプロジェクト事務局に通知する必要がありました。しかしながら、今回の新プロジェクトへの移行にあたっては上記閉

局作業において失効申請の有無にかかわらず一括失効しますので、新プロジェクトの証明書へ置き換えが完了した際に**旧プロジェクトの証明書について失効申請していただく必要はございません**。

ただし、移行期間終了までの間に鍵ペアの危殆化(紛失・漏洩等)した場合など急ぎ失効する必要がある場合には、上記に関わらず直ちに失効申請を行っていただくようお願いいたします。

⇒Web: 各種手続き→失効手続き

https://upki-portal.nii.ac.jp/docs/server/5

5. CSR 生成手順の変更

新プロジェクトでは、旧プロジェクトとの識別のため、主体者 DN 中の L (Locality Name)の値が**”Academe”から”Academe2”へと変更**になります。このため、新プロジェクトでの発行申請の際に生成する CSR においても、DN 中の L の値を新しい値にて生成していただく必要がございます。旧プロジェクトでの L の値のままの CSR では、新プロジェクトから証明書を発行することができませんのでご注意ください。

旧プロジェクトの主体者 DN 例: CN=www.example.com, O=example, L=Academe, C=JP

新プロジェクトの主体者 DN 例: CN=www.example.com, O=example, L=Academe2, C=JP

⇒別添 1: サーバ証明書インストールマニュアル変更点一覧

6. DN 使用可能文字の変更

新プロジェクトでは、DN に使用可能な文字が変更になりました。なお、使用不可能となっている一部の文字については見直しを検討しており、近々に対応する予定です。

1) サーバ証明書の CN に使用できる文字

FQDN として使用可能な文字だけに制限しました。英数字の他に使用可能な文字はハイフン、ピリオドのみになります。

2) O,OU に使用できる文字

現状では旧プロジェクトと比較して左括弧および右括弧が追加されましたが、アポストロフィ、プラス、カンマ、イコールの 4 種類の文字が使用できなくなっています。近々に改修を行い互換性確保を図る予定ですが、プラスに限ってはシステム上の制約で使用することができませんのでご了承ください。

表 1　サーバ証明書の DN 使用可能文字に関する変更点

			英字	数字	空白	アポストロフィ	左括弧	右括弧	プラス	カンマ	ハイフン	ピリオド	スラッシュ	コロン	イコール	クエスチョン
			A－z	0-9		'	(	)	+	,	-	.	/	:	=	?
旧	O,OU,CN		○	○	○	○	×	×	○	○	○	○	×	○	○	×
新	CN		○	○	×	×	×	×	×	×	○	○	×	×	×	×
	O,OU	現状	○	○	○	×	○	○	×	×	○	○	×	○	×	×
		改修後	○	○	○	○	○	○	×	○	○	○	○	○	○	×

7.　中間 CA 証明書の変更

新プロジェクトでは、NII が運用する中間 CA について、新たにオープンドメイン認証局 2 として構築しました。すなわち、証明書チェーンが異なります。新旧プロジェクトの証明書チェーンの違いについては、図 1 および図 2 をご参照ください。

このため、サーバ証明書を新プロジェクトから発行されたものに置き換えていただく際には、併せて**中間 CA 証明書も新プロジェクトのオープンドメイン認証局 2 証明書に置き換え**ていただく必要がございます(新プロジェクトでは、中間 CA 証明書は、このオープンドメイン認証局 2 の 1 枚のみになります)。

中間 CA 証明書を置き換えない場合、サーバによってはサーバプロセスを正しく起動することができなかったり、あるいは利用者がサーバ証明書を検証することができず、サーバ認証に失敗する場合がありますのでご注意ください。

⇒別添 1: サーバ証明書インストールマニュアル変更点一覧

図 1　旧プロジェクトの証明書チェーン

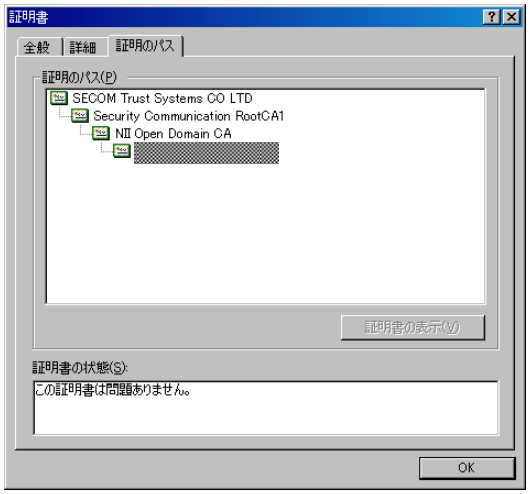
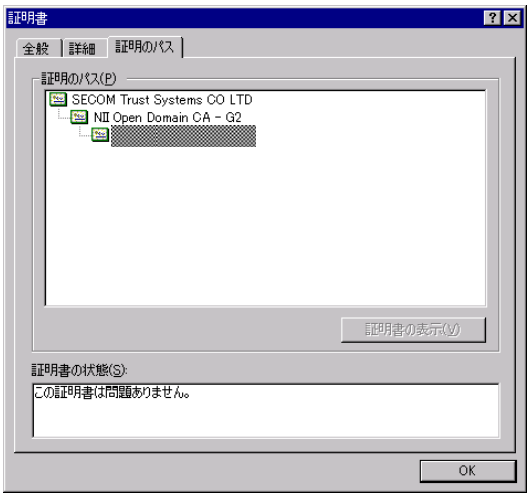


図 2　新プロジェクトの証明書チェーン



8. ルート CA 証明書の変更(加入者サーバが IIS の場合のみ)

ご要望の多かった携帯電話対応を実現するため、新プロジェクトではルート認証局を SECOM Trust.net Root1 CA(以下、STN-Root1)から Security Communication RootCA1(以下、SC-Root1)へと変更しました。IIS をご利用の加入者の方は旧プロジェクトにおいては、SC-Root1 が「信頼されたルート証明機関」に登録されていた場合に、「信頼されたルート証明機関」から SC-Root1 の自己署名証明書を削除していただく必要がありましたが、新プロジェクトにおいては、SC-Root1 を「信頼されたルート証明機関」として扱うため、**削除いただいた SC-Root1 の自己署名証明書を「信頼されたルート証明機関」に再登録**する必要があります。

SC-Root1 の自己署名証明書を「信頼されたルート証明機関」に再登録するためには別添の手順「Security Communication RootCA1 認証局の自己署名証明書の再登録」を実行してください。

SC-Root1 が「信頼されたルート証明機関」に登録されていない状態ですと、携帯電話等新プロジェクトがサポートする Web ブラウザで検証できない場合がございますのでご注意ください(旧プロジェクトがサポート範囲としている Web ブラウザでしか検証できません)。

⇒別添 2: Security Communication RootCA1 認証局の自己署名証明書の再登録

以上

別添 1: サーバ証明書インストールマニュアル変更点一覧

旧プロジェクトマニュアル章節	変更箇所	変更対象							新プロジェクトマニュアル章節	変更内容
		Apache 2 + mod_ssl 編	Apache 1.3 + mod_ssl 編	Apache-SSL 編	Microsoft IIS 6.0 編	Microsoft IIS 5.0 編	Tomcat (JavaKeytool) 編	IBM HTTP Server 編		
1.3節　表1-2	Security Communication RootCA1証明書(中間CA証明書)	○	○	○	○	○	○	○		削除
1.3節　表1-2	NIIオープンドメイン認証局証明書(中間CA証明書)	○	○	○	○	○	○	○	2-5-1節　手順2	認証局証明書URLおよびファイル名
2.2節　表2-1 および2.3節	Locality Name	○	○	○	○	○	○	○	2-2節	旧: Academe 新: Academe2
2.5.2節　手順3	Locality Name	○	○	○	○[1]	○[1]	○	○	2-3-2節　手順2 [1]	
2.6.3節　手順1	L (Locality Name)						○		2-3-1節　手順1	
3.1.3節	SC-Root1自己署名証明書の削除				○	○				手順廃止
3.2.1節　手順3	SC-Root1(中間CA)証明書のインストール			○						手順廃止
3.2.1節　手順4	NIIオープンドメインCA(中間CA)証明書のインストール			○					2-5-2節	中間CA証明書およびファイル格納パ
3.3.1節　手順3	SC-Root1(中間CA)証明書のインストール	○	○							手順不要
3.3.1節　手順4	NIIオープンドメインCA(中間CA)証明書のインストール	○	○						2-5-2節	中間CA証明書およびファイル格納パ
3.4.1節　手順1～2	中間CA証明書のインストール						○		2-5-2節 および2-5-3節	ルートCA証明書(scroot1.crt)および 中間CA証明書(nii-odca2.crtのみ)を それぞれインストール
3.5.1節	中間CA証明書のインストール					○			2-5-2節 および2-5-2節	ルートCA証明書(scroot1.crt)および 中間CA証明書(nii-odca2.crtのみ)を それぞれインストール
3.6.1節	中間CA証明書のインストール				○				2-5-2節	nii-odca2.crtのみをインストール

1「Microsoft IIS 6.0 編」および「Microsoft IIS 6.0 編」に限り、新プロジェクトマニュアル章節が「2-2-2節　手順2」になります。

別添 2: Security Communication RootCA1 認証局の自己署名証明書の再登録

旧プロジェクトで IIS5.0 または 6.0 を加入者サーバとしてご利用いただいていた加入者の方は、新プロジェクトが推奨する Web ブラウザに対応するために、以下の手順で Security Communication RootCA1 認証局(以下、SC-Root1)を「信頼するルート証明機関」として登録していただく必要があります。

1) 下記 URL の SC-Root1 リポジトリにアクセスして、SC-Root1 の自己署名証明書をダウンロードします。
https://repository.secomtrust.net/SC-Root1/index.html


信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

Security Communication RootCA1 Repository

Security Communication RootCA CP/CPS最新バージョン - Certificate Policy and Certification Practice Statement -

日本語版 - Japanese -

- Certification Practice Statement(SCRootCPS.pdf) version 4.00 2009-5-29 release (2009年5月29日 公表)
- 下位CA用 Certificate Policy(SCRootCP1.pdf) version 4.00 2009-5-29 release (2009年5月29日 公表)
- タイムスタンプ用 Certificate Policy(SCRootCP2.pdf) version 3.00 2009-5-29 release (2009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) = 36B1 2B49 F981 9ED7 4C9E BC38 0FC6 568F 5DAC B2F7

Fingerprint(MD5) = F1BC 636A 54E0 B527 F5CD E71A E34D 6E4A

証明書失効リスト - Certificate Revocation List -

- Certificate Revocation List(SCRoot1CRL.crl)

タイムスタンプ用証明書失効理由(ReasonCode)

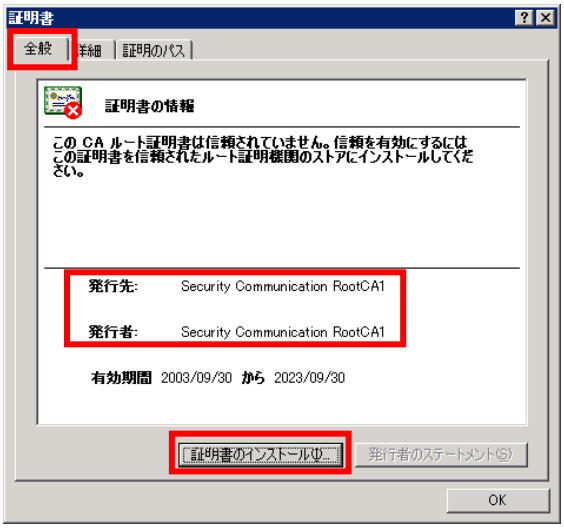
(注) 通信データの安全を確保するため、本ページのアドレスがhttps://repository.secomtrust.net/...で始まっていることをご確認ください。

最終更新日 2009年6月24日

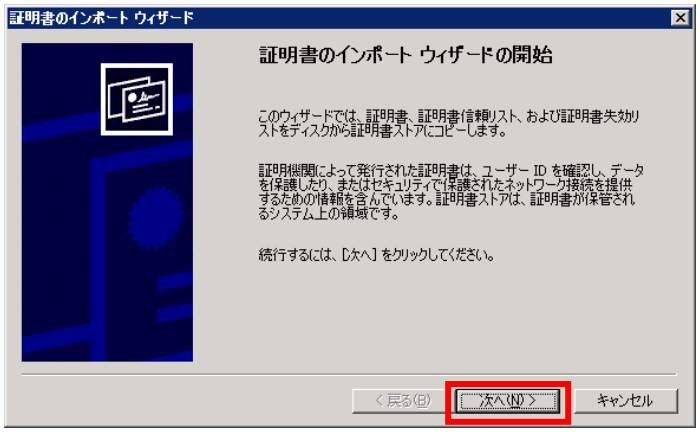
2) 1)で取得した SC-Root1 の自己署名証明書ファイルをダブルクリックして、[**全般**]タブが表示されている状態で発行先と発行者が以下の通りであることを確認した後、[**証明書のインストール(I)…**]ボタンをクリックします。

発行先：Security Communication RootCA1

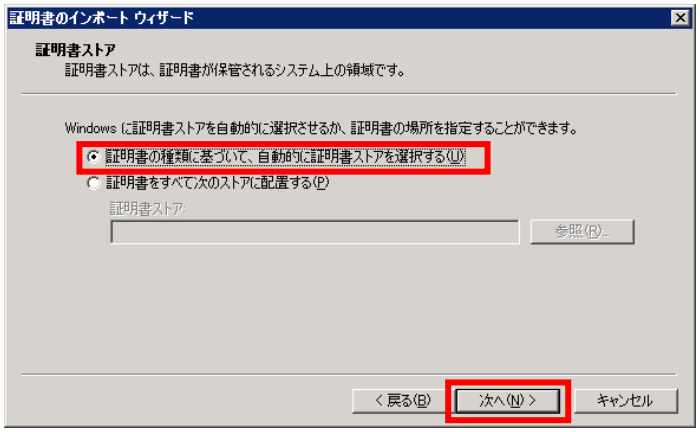
発行者：Security Communication RootCA1



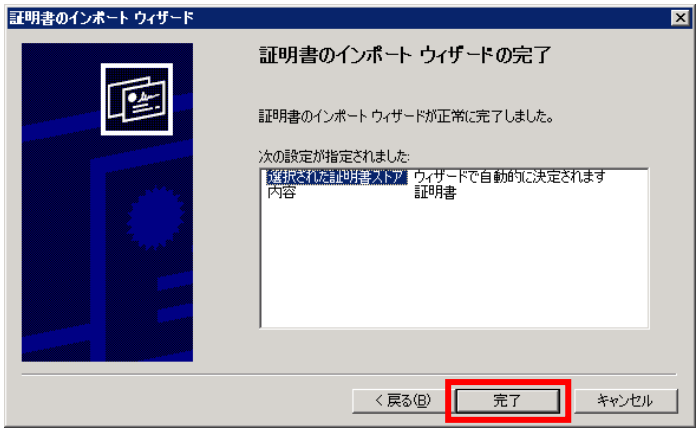
3) 「証明書のインポートウィザード」が開始するので、[次へ(N)]ボタンをクリックします。



4) [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)]を選択し、[次へ(N)]ボタンをクリックします。

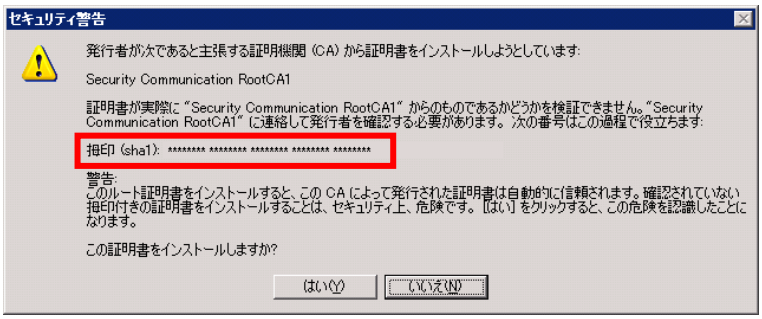


5) 以下の画面が表示されたら、[完了]ボタンをクリックします。



6) ルート証明書をインストールしようとするため、セキュリティ警告が表示されます。証明書が SC-Root1 からのものであることを検証するために、表示されている拇印(sha1)が、以下の値と一致することを確認した上で、[はい(Y)]ボタンをクリックします。

拇印(SHA1) : 36B1 2B49 F981 9ED7 4C9E BC38 0FC6 568F 5DAC B2F7



7) 以下の画面が表示されたら、証明書のインポートは完了です。[OK]ボタンをクリックすると証明書のインポートウィザードが終了します。

以上