# NAREGI-CA UPKI Web 使用手引書 (利用者ガイド)

2006年10月13日

国立情報学研究所

Copyright© 2004-2006 National Institute of Informatics, Japan. All rights reserved.

This file or a portion of this file is licensed under the terms of the NAREGI Public License, found at <a href="http://www.naregi.org/download/">http://www.naregi.org/download/</a>. If you redistribute this file, with or without modifications, you must include this notice in the file.

"This product includes software developed by Akira Iwata Laboratory,

Nagoya Institute of Technology in Japan (http://mars.elcom.nitech.ac.jp/)."

## 目次

1.	はじ	めに		. 1
2.	RA	アド	ミニストレータ	.4
3.	RA	オペ	レータ	.6
3	.1.	RA	アドミニストレータ操作画面	. 6
3	.2.	RA	オペレータ証明書発行	. 8
	3.2	.1.	RA オペレータ ―証明書申請―	10
	3.2	.2.	RA アドミニストレータ ―申請許可・証明書作成―	13
3	.3.	RA	オペレータ更新処理	17
	3.3	.1.	RA オペレータ —更新申請—	19
	3.3	.2.	RA アドミニストレータ —更新許可・証明書作成—2	22
3	.4.	RA	オペレータ失効処理	25
	3.4	.1.	RA オペレータ ―失効申請―2	27
	3.4	.2.	RA アドミニストレータ —失効許可—	30
3	.5.	RA	オペレータ申請検索	32
3	.6.	RA	オペレータ申請リスト表示	33
3	.7.	RA	オペレータ検索	34
3	.8.	RA	オペレータリスト表示	35
	3.8	.1.	RA オペレータ情報表示・変更	36
4.	エン	ドユ	ーザ	37
4	.1.	RA	オペレータ操作画面	37
4	.2.	그-	- ザ証明書発行	39
	4.2	.1.	ユーザ ―証明書申請―	41
	4.2	.2.	RA オペレータ ―申請許可―	14
	4.2	.3.	ユーザ ―証明書生成―	46
4	.3.	그-	- ザ証明書更新	50
	4.3	.1.	ユーザ —更新申請—	52
	4.3	.2.	RA オペレータ ―申請許可―	55
	4.3	.3.	ユーザ ―証明書生成―	57
4	.4.	고-	−ザ証明書失効	30
	4.4	.1.	ユーザ ―失効申請―	32
	4.4	.2.	RA オペレータ ―失効許可―	34
4	.5.	証明	月書申請検索	36

4.6.	証明書申請リスト表示	67
4.7.	ユーザ検索	68
4.8.	ユーザリスト表示	69
4.8.	1. ユーザ情報表示・変更	71
5. 自重	b承認発行(IC カード連携)	72
5.1.	事前準備	73
5.2.	ユーザ証明書取得処理	74

## 1. はじめに

本ドキュメントでは、NAREGI-CA の Challenge PIN/LicenselD 発行モード(authmode=4)を ベースとした RA 権限分離と証明書発行の流れについて説明します。また、ユーザ管理 WEB イ ンタフェースの解説も行います。

RA アドミニストレータへの証明書発行を2章で説明し、3章では RA オペレータが証明書を取 得・更新・失効を行う方法と RA アドミニストレータ操作画面について、4章ではユーザが証明書 を取得・更新・失効する方法と RA オペレータ操作画面について、5章では学内認証局等と連携 し、既に発行されている証明書から新しい証明書の発行を承認する「自動承認発行」について説 明します。

アクター	備考
CA アドミニストレータ	CA サーバの管理者
	CA サーバの運用
	RA アドミニストレータに証明書の配布を行う
RA アドミニストレータ	RA サーバの管理者
	RA サーバの運用
	RA オペレータの審査および証明書の配布を行う
RA オペレータ	ユーザの審査および証明書の配布を行う。
ユーザ	証明書を利用するユーザ

図 1-1,1-2,1-3 に利用手順概要を示します。

※本手順書で利用しているブラウザは Microsoft Internet Exploler(以下 IE)であり、それ以外の ブラウザには対応しておりません。



図 1-1 RA オペレータ証明書取得手順(概要)



図 1-2 ユーザ証明書取得手順(概要)



図 1-3 学内認証局から発行された IC カードを利用したユーザ証明書取得手順(概要)

## 2. RA アドミニストレータ

CA アドミニストレータは、CA サーバの管理を行うとともに、RA アドミニストレータ証明書の発行も行います。RA アドミニストレータ証明書を発行するには、CA サーバマシン上で直接 aica コマンドを使用して、鍵ペアの生成と証明書の発行を行います。

1 aica user オペレーションにより RA アドミニストレータ向けの証明書を発行します。コマンドの形式は次のとおりです。この操作は、CA アドミニストレータが CA サーバマシン上で直接行います。

aica user はプシ	านไ
オプション:	]
-add	:オペレータを追加します
-del	:オペレータを削除します
-mod	: オペレータの情報を更新します
-cpw	:オペレータのパスワードを更新します
オプション(オフラー	<b>(ンの</b> み):
-addop	:SSL 認証用のオペレータを追加します
-addraop	:RA アドミニストレータ証明書を発行します
-smlib	: PKCS#11 ライブラリを指定(RA アドミニストレータ用)
-smlabel	: PKCS#11 ラベル名(RA アドミニストレータ用)
ー般オプション:	
-sv path	: "サーバ名:CA 名"を指定します
-ssl	: リモート CA 接続に SSL を使用します
-clid name	: SSL クライアント証明書の ID を指定します
-u loginid	: CA ユーザ名を指定します(非 SSL 接続)
-p passwd	: CA ユーザパスワードを指定します(非 SSL 接続)

**2** RA アドミニストレータ証明書発行は以下のように行います。-smlib と-smlabel オプションを 指定することで、IC カードで直接鍵ペアの生成も可能です。

bash\$ aica user –addraop CA PKCS#12 file open
Input PKCS#12 Password: (パスワードを入力)
Issuing a new RA operator(admin) certificate.
generate private key (size 1024 bit) oo
00
Input PASS Phrase: (パスワードを入力)
Verifying - Input PASS Phrase: (パスワードを入力)
RA operator certificate has been issued. (sn=1996)
success to modify CA user.

**3** 証明書発行後、PKCS#12 ファイルの出力を行います。下記コマンドにより、newcert.p12 ファイルが出力されます。(IC カードで鍵ペアを生成した場合は、この操作は必要ありません)

bash\$ aica export -sn 1996 -p12 CA PKCS#12 file open Input PKCS#12 Password: (パスワードを入力) get private key file from CA key store. Input PASS Phrase: (パスワードを入力) save PKCS#12 file. input new password. Input Export Password: (パスワードを入力) Verifying - Input Export Password: (パスワードを入力) success to export a pkcs#12 (sn: 1996)

上記操作を行った後、PKCS#12 ファイルを Windows マシンにインストールするか IC カードを使用することで、InternetExplorer にて WEBの RA アドミニストレータ操作画面に接続することが可能になります(SSL クライアント認証が行われます)。

## 3. RA オペレータ

本章ではRAオペレータの証明書申請、更新、失効の手順とRAアドミニストレータ操作画面について説明します。

#### 3.1. RA アドミニストレータ操作画面

https://サイト名/CA 名\_ra/airaadmin にアクセスすることで、RA アドミニストレータの操作画 面を表示することができます。この画面を表示するには、SSL クライアント認証が必要であり、あ らかじめ Windows に RA アドミニストレータ証明書のインストールもしくは、IC カードを使用する 必要があります。

NAREGI-CA Certification Authority Server Powered by AlCrypto Library		Security post the Street of				
National Research Grid Initiative		1 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				
NAREGI CA - RAオペレータ管理サイト	操作者名 鍵ID	CN=RAAdmin003, e8f49984eb5b08e416b081c60fb31b8dc08cb30a				
サイト操作 RA管理者操作 RAオペレータ操作						
▶ RAアドミニストレータ情報						
○ RAアドミニストレータ証明書詳細 / RAアドミニスト」	レータ証明書ダウンロ	<u>1-r</u>				
○ <u>RA CGI設定表示</u>						
○CA証明書詳細 / CA証明書ダウンロード / CRLダウンロード						
▶ RAオペレータ操作一覧						
© <u>RAオペレータ新規申請</u>						
◎ RAオペレータ申請検索 / RAオペレータ申請一覧 / RAオペレータ更新申請一覧 / RAオペレータ失効申請一覧						
○ RAオペレータ検索 / RAオペレーター覧						
) 2006 National Research Grid Initiative		NAREGLCA RA Managama				

それぞれのメニューの内容は以下の通りです。

RA アドミニストレータ証 明書詳細	RA アドミニストレータ証明書の内容を表示します。
RA アドミニストレータ証	RA アドミニストレータ証明書をダウンロードします。秘密鍵はダウン
明書ダウンロード	ロードできません。
RA CGI 設定表示	RA サーバの CGI 設定を表示します。表示だけであり、修正を行う 場合は、RA サーバ上で直接 aica.cnf を編集してください。
CA 証明書詳細	CA 証明書の内容を表示します。
CA 証明書ダウンロード	CA 証明書をダウンロードします。

CRL ダウンロード	最新の CRL をダウンロードします。
RA オペレータ新規申請	RA オペレータ証明書を新規に申請します。 申請ページを新たに開きます。
RA オペレータ申請検索	RA オペレータ証明書の申請を検索します。
RA オペレータ申請一覧	RA オペレータ証明書の申請の一覧を表示します。
RA オペレータ更新申請 一覧	RA オペレータ証明書の更新申請の一覧を表示します。
RA オペレータ失効申請 一覧	RA オペレータ証明書の失効申請の一覧を表示します。
RA オペレータ検索	証明書発行済の RA オペレータを検索します。
RA オペレーター覧	証明書発行済の RA オペレータの一覧を表示します。
トップページ (サイト操作メニュー)	トップページを表示します。
ログアウト (サイト操作メニュー)	ログアウト操作を行い、セッションをクリアします。

#### 3.2. RA オペレータ証明書発行

RA オペレータが証明書を取得する場合、RA オペレータ操作画面から新規に申請を行います。 申請を受け取ったRA アドミニストレータは、申請内容を確認しRAアドミニストレータ向けの証明 書(IC カード)を発行します。その後、IC カードを RA オペレータに配布します。



#### RA オペレータ処理の流れ

RA アドミニストレータ処理の流れ



#### 3.2.1. RA オペレータ --証明書申請--

- 1 RA オペレータは RA オペレータ操作メニューサイト(https://サイト名/CA 名\_ra/airaregist) にアクセスし、「オペレータ証明書新規申請」を選択します。
  - ※ アクセスは https であるが、SSL クライアント認証は不必要です。ただし、メニューから ユーザ管理サイトにログインする場合、ブラウザの実装上あらかじめ RA オペレータ証 明書で認証しておく必要があります。

NAREGI CA - オペレータ操作メニュー ▶操作メニュー 電子証明書に関する操作を行います。 操作メニューをクリックして操作を実行してください。 ユーザ管理サイトにログインし、ユーザ証明書の申請処理を行ないます。 なお、下記サイトにアクセスするためにはRAオペレータ証明書を使用して、SSLクライアント認証を行な う必要があります。 ユーザ管理サイトにログイン 0 新規に電子証明書を申請します、SSLクライアント認証は必要ありません。 オペレータ証明書新規申請 0 既に証明書を取得している場合、オペレータ証明書の更新と失効の申請が可能です。 また、Challenge PIN の変更も下記メニューにて行ないます。 オペレータ証明書更新申請 / オペレータ証明書失効申請 / Challenge PIN 変更 0 CA証明書の表示とCA証明書のダウンロードを行ないます。 また、最新のCRLのダウンロードを行ないます CA証明書詳細 / CA証明書ダウンロード / CRLダウンロード 0 (c) 2006 National Research Grid Initiative NAREGI-CA RA Management

図 3-1 オペレータ操作メニュー画面

2 RA オペレータレジストレーションのページが表示されるので、RA オペレータの情報を入力します(氏名・E-mail・Challenge PIN の入力は必須です)。項目を入力した後、画像認証のための文字列を入力し「証明書情報の確認」ボタンをクリックします。

NAREGI-CA Certification Authority Server Powered by AlCrypto Library National Research Grid Initi	iative	(margaret	n este	<b>19</b> 2			
NAREGI CA - RAオペレータレジストレーション							
新しくRAオペレータ証明書の申請を行ないます。							
	ト記の項目を記入し、「中前情報の確認」 ホメノをクリックしてください。						
項目名	項目内容						
氏名:	(姓)	(名)	0				
Email :				0			
Email(確認用):				0			
Challenge PIN :		• *1					
Challenge PIN (確認用) :		• *1					
所属:							
所属番号:							
職位:							
電話番号1:							
電話番号 2:							
FAX 1 :							
FAX 2 :							
郵便番号:							
住所:							
関連URL:							
その他・備考:							
●は必須項目です。							
*1 Challenge PIN は証明書の取得、更新、失効に必要で:	*1 Challenge FIN は証明書の取得、更新、失効に必要です。忘れにくいFIN文字列を指定してください。						
・画像認証							
フォーム入力が正しく行われているか確認するために、画像認証を行ないます。 下記の画像の数字5ケタを入力してください。							
文字列:0	90658	128 500 h to to to	۹. ۱۰				
	申請情報の確	112					
c) 2006 National Research Grid Initiative	and the second second		NAREC	GI-CA RA Management.			

図 3-2 RA オペレータレジストレーション画面

**3** 表示される情報を確認し、入力内容に誤りがなければ、「証明書の申請」ボタンをクリックします。

しくRAオペレー 切証明書の中部 力項目を確認し、問題が悪けれ	春を行ないます。 れば江明寺を中観日 ボタンを クリックしてください。 1977年7月 1991 - 1992 - 1992 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995
RAオペレータ情報を思	TVLK-0J IN 97 E 1999D CLICEON
<b>AB6</b>	项目内容
<b>6.6</b> :	те 3т
Email :	test@wall.com
Challenge PDI :	3ddddd:
<b>新展</b> :	
所英者号:	
華査:	
電話書号 1:	
電話書号 2:	
FAX 1:	
FAX 2 :	
野祝香号:	
<b>佳所</b> :	
間違URAL:	

図 3-3 RA レジストレーション確認画面

4 申請結果が表示されるので画面をプリントアウトし、RA アドミニストレータに送付します。

NAREGI CA - RAオペレータレジストレーション					
証明書の申請が完了し 必要であれば下記の5	しました。 フォームを印刷して管理者に提出してください。				
受付け番号: RAREG0219					
受付け日時: 2006/02/22 19:33:45					
申請者氏名:	test name				

図 3-4 申請結果画面

#### 3.2.2. RA アドミニストレータ —申請許可・証明書作成—

**1** RA オペレータ管理サイト(https://サイト名/CA 名\_ra/airaadmin)に RA アドミニストレータで ログインし、「申請一覧」を選択します。

National Research Grid Initiative	1				
NAREGI CA - RAオペレータ管理サイト	操作者名 鍵ID	CN=RAAdmin003. e8f49984eb5b08e416b081c60fb31b8dc08cb30a			
サイト操作 RA管理者操作 RAオペレータ操作					
新規申請					
RAアドミニストレータ情報					
申請一覧					
○ RAアドミニストレータ証明書詳細 更新申請一覧	証明書ダウンロ	<u>] -                                   </u>			
○ RA CGI設定表示					
○ <u>CA証明書詳細</u> / <u>CA証明書が</u> オペレータ検索 オペレーター覧	<u>1-F</u>				
▶RAオペレータ操作一覧					
○ <u>RAオペレータ新規申請</u>					
◎ RAオペレータ申請検索 / RAオペレータ申請一覧 / RAオペレータ更新申請一覧 / RAオペレータ失効申請一覧					
◎ RAオペレータ検索 / RAオペレーター覧					

図 3-5 RA オペレータ管理サイト画面

2 証明書発行申請している RA オペレータの申請番号を選択します。

Aオペレ	ータ管理サイ	Έ	操作者名 鍵ID	CN=RAAdmin e8f49984eb5l	003, b08e416b081c60fb3	1b8dc08cb30a
RA管理者	操作 RA才べ	レータ操作				
					最大表示	件数: 20 💊
	氏名	EMAIL			申請日時	
	Aオペレ (A管理者	Aオペレータ管理サイ A管理者操作 RAオペ ▲ ▼ 氏名	Aオペレータ管理サイト A管理者操作 RAオペレータ操作 ・ 氏名 EMAIL	Aオペレータ管理サイト 鍵ID A管理者操作 RAオペレータ操作 低名 EM AIL	Aオペレータ管理サイト 鍵ID e8f49984eb5t A管理者操作 RAオペレータ操作 ・ 氏名 EM AIL	Aオペレータ管理サイト 鍵ID e8f49984eb5b08e416b081c60fb3 (A管理者操作 RAオペレータ操作 最大表示

- 3 RA オペレータの申請内容を確認し、管理グループにチェックを入れて「発行を許可する」ボタンをクリックします。証明書発行許可の旨を申請者に通知したい場合は、「申請者に通知する」にチェックを入れます。
  - ※ 管理グループには注意が必要です。管理グループを指定しないと、RA オペレータがユ ーザを管理できなります)

-			0-6	
申請者に チェックを有	通知する 効にすると発行審員	直の結果をメールで申請者	こ通知します。	
発行許可能	制に有効にすると、新	#ベアの生成と証明書の取	得を申請者が行なうこ	とになります。
●は必須項目	です。			
●は必須項目	です。			

図 3-7 RA オペレータ申請確認画面

**4** RA オペレータ証明書発行画面にて下記項目を設定し「証明書を発行する」ボタンをクリック します。

設定項目	備考
CSP	証明書のインストール先。Microsoft ~ Cryptographic
	Providerを選択するとPCのハードディスクにインストールし
	ます。ICカードにインストールする場合は、対応する CSPを
	選択します。
秘密鍵の長さ	鍵長が長い程安全性が高くなります
秘密鍵のエクスポート	可能に設定すると、Windows の内部ストアから秘密鍵をエ
	クスポートすることが可能になります。
秘密鍵の保護レベル	「通常」を選択した場合、Windows で秘密鍵を用いる時にパ
	スワードの入力を簡略化できます。
	「強力な保護」を選択した場合、秘密鍵を利用する度にパス
	フレーズの入力が必要となります。

ーバに対し	て、電子証明書を申請しま	す。 ೧೯೮೫週期 いわードホカードリーダ/ニイターセット で
明書を発行す	あ」ボタンをクリックしてくた	さい。
明書要求	(CSR)情報	
-		
	フロファイル情報	
-	プロファイル名:	Operators
	フーザ坊報	
-	申請者名:	unitaro
	ON :	RAOP0162
	Email :	test@mail.com
1	秘密總於完	
	SP:	Microsoft Enhanced Cryptographic Provider v1.0 💌
	秘密鍵の長さ	© 512 bit @ 1024 bit © 2048 bit
	秘密鍵のエクスポート:	◎可能 ○不可
	秘密鍵の保護レベル:	<ul> <li>通常</li> <li>・ 強力な保護</li> </ul>
	will de la construction de la construction	11 - 18 11 - 18 18 - 18 - 18 - 18 - 18
	HAVE & O COP ILLOT IL.	長い難長の難の生成の行えないことがあります。
		1710-A+70-12-+1

図 3-8 RA オペレータ証明書発行画面

5 「電子証明書をインストール」ボタンをクリックし、発行した証明書をPCもしくはICカードにインストールします。



図 3-9 電子証明書インストール画面

6 インストールが正常に完了すると下記の画面が表示されます。

電子証明書のインストールが完了しました

ICカードをICカードリーダ/ライタから取り外し可能です。

RA管理者であれば、管理者用のICカードに入れ替えてください。 3秒後に自動で管理者画面に移動します。

図 3-10 電子証明書インストール結果画面

## 3.3. RA オペレータ更新処理

RA オペレータ証明書を更新する処理の流れは以下の通りです。

#### RA オペレータ処理の流れ



RA アドミニストレータ処理の流れ



#### 3.3.1. RA オペレータ —更新申請—

**1** RA オペレータは RA オペレータ操作メニューサイト(https://サイト名/CA 名\_ra/airaregist) にアクセスし、「オペレータ証明書更新申請」を選択します。



図 3-11 オペレータ操作メニュー画面

**2** ユーザ認証ページで Challenge PIN を入力し、「ログイン」ボタンをクリックします。

NA	AREGI-CA	tiative	and the second
NAREGI C	A - RAオペレータレジストレ 2日	ーション	
電子証明書 Challenge F	ーー Hに関する操作を行います。 PIN を入力してください。		
	Challenge PIN :		- i
		ログイン	

図 3-12 RA オペレータレジストレーション画面

3 RA オペレータの情報を確認し、「証明書の申請」ボタンをクリックします。

項目名	項目内容
氏名:	test name
Email :	test@mail.como
Challenge PIN :	
住所:	
関連URL:	
その他・備考:	

図 3-13 RA オペレータ情報確認画面

4 申請結果が表示されるので画面をプリントアウトし、RA アドミニストレータに送付します。

REGICA - RAZ	ペレータレジストレーション
月書の申請が完了!	しました。
econtia raco.	オームで印刷して管理者に提出してくたでい。
受付け番号:	RAREG0219
受付け日時:	2006/02/22 19:33:45
申請者氏名:	test name

図 3-14 RA オペレータレジストレーション結果画面

#### 3.3.2. RA アドミニストレータ — 更新許可・証明書作成—

**1** RAオペレータ管理サイト(https://サイト名/CA名\_ra/airaadmin)にRAアドミニストレータで ログインし、「更新申請一覧」を選択します。



図 3-15 RA オペレータ管理サイト画面

2 更新申請をしている RA オペレータの申請番号を選択します。

申請番号		氏名	EMAIL	申請日時	
RAREG0224		BUNKYO TARO	and the second second	2006/03/10 15:17:17	
B RAREG0223	>	aaa bbb		2006/03/07 20:19:19	
E RAREG0219		test name	1000	2006/02/22 19:33:45	

#### 図 3-16 申請一覧画面

- 3 RA オペレータの申請内容を確認し、管理グループにチェックを入れて「発行を許可する」ボタンをクリックします。申請者に通知したい場合は、「申請者に通知する」にチェックを入れます。
  - ※ 管理グループを指定しないと、RA オペレータがユーザを管理できなくなります)

管理グループ:	SMIME user	🔽 testerp2 hoge group	ample3 group	🔽 zyouhou kougakka
<ul> <li>申請者に</li> <li>チェックを有</li> <li>発行許可時</li> </ul>	<b>通知する</b> 効にすると発行審査 に有効にすると、鍵	の結果をメールで申請者に ペアの生成と証明書の取得	:通知します。 身を申請者が行なうこ	とになります。
●は必須項目	です。			
		発行を許可する 第	能行を拒否する	

図 3-17 RA オペレータ申請確認画面

**4** RA オペレータ証明書発行画面にて下記項目を設定し「証明書を発行する」ボタンをクリック します。

設定項目	備考
CSP	証明書のインストール先。Microsoft~Cryptographic
	Provider を選択すると PC のハードディスクにインストー
	ルします。ICカードにインストールする場合は、対応する
	CSP を選択します。
秘密鍵の長さ	鍵長が長い程安全性が高くなります
秘密鍵のエクスポート	可能に設定すると、Windows の内部ストアから秘密鍵
	をエクスポートすることが可能になります。
秘密鍵の保護レベル	「通常」を選択した場合、Windows で秘密鍵を用いる時
	にパスワードの入力を簡略化できます。
	「強力な保護」を選択した場合、秘密鍵を利用する度に
	パスフレーズの入力が必要となります。

書要求	(CSR)情報	
	ブロファイル 情報	
-	プロファイル名:	Operators
	ユーザ情報	
	申請者名:	uni taro
i	CN:	RAOP0162
	Email :	test@mail.com
	秘密教师完	
	SP:	Microsoft Enhanced Cryptographic Provider v1.0 💌
	秘密鍵の長さ	© 512 bit @ 1024 bit © 2048 bit
	秘密鍵のエクスポート:	<ul> <li>可能</li> <li>〇 不可</li> </ul>
	秘密線の保護レベル:	④ 通常 〇 砕力な保護

図 3-18 RA オペレータ証明書発行画面

**5**「電子証明書をインストール」ボタンをクリックし、発行した証明書をPCもしくはICカードにインストールします。



図 3-19 電子証明書インストール画面

6 インストールが正常に完了すると下記の画面が表示されます。





## 3.4. RA オペレータ失効処理

RA オペレータ証明書を失効する処理の流れは以下の通りです。

#### RA オペレータ処理の流れ



RA アドミニストレータ処理の流れ



3.4.1. RA オペレータ — 失効申請—

- **1** RA オペレータは RA オペレータ操作メニューサイト(https://サイト名/CA 名\_ra/airaregist) にアクセスし、「オペレータ証明書失効申請」を選択します。
  - ※アクセスは https ですが、SSL クライアント認証は不必要です。ただし、メニューからユー ザ管理サイトにログインする場合、ブラウザの実装上あらかじめ RA オペレータ証明書で 認証しておく必要があります。

NAREGI-CA
Powered by AlCrypto Library
National Research Grid Initiative
NAREGI CA - オペレータ操作メニュー
▶ 操作メニュー
電子証明書に関する操作を行います。 操作メニューをクリックして操作を実行してください。
ユーザ管理サイトにログインし、ユーザ証明書の申請処理を行ないます。 なお、下記サイトにアクセスするためにはRAオペレータ証明書を使用して、SSLクライアント認証を
◎ ユーザ管理サイトにログイン
新規に電子証明書を申請します。SSLクライアント認証は必要ありません。
◎ オペレータ証明書新規申請
既に証明書を取得している場合、オペレータ証明書の更新と失効の申請が可能です。 また、Challenge PIN の変更も下記メニューにて行ないます。
○オペレータ証明書更新申請 オペレータ証明書失効申請 Challenge PIN 変更
CA証明書の表示とCA証明書のダウンロードを行ないます。 また、最新のCRLのダウンロードを行ないます
© CA証明書詳細 / CA証明書ダウンロード / CRLダウンロード

図 3-21 オペレータ操作メニュー画面

**2** ユーザ認証ページで、Challenge PIN を入力し、「ログイン」ボタンをクリックします。

NA	REGI-CA Continuation Authority Server Preserved by AlCrypto Library	tiative
	A - RAオペレータレジストレ	ーション
電子証明書 Challenge P	に関する操作を行います。 IN を入力してください。	
	Challenge PIN :	
		ログイン

図 3-22 ユーザ認証ページ

**3** RA オペレータ証明書の情報を確認、失効理由を選択し「失効の申請」ボタンをクリックします。

(Aオペレータ証明	書を失効します !!	
オペレータ証明書を かを行なう場合 [失す	失効すると、該当するRAオペレ かの申請1ボタンをクリックしてく	ータによる操作が行なえなくなります。 ださい。
項目名	項目內容	
シリアル番号:	1931	
サブジェクト:	C=JP, O=my organization	OU=business unit, CN=RAOP0150,
開始日時:	2006/03/01 18:28:37	
終了日時:	2000/02/28 18:28:37	
地理中の設定		
● 特定しない		○ 鍵の破損
		-

図 3-23 RA オペレータ失効申請画面

**4** RA オペレータ失効申請結果画面が表示されるので、表示されたページをプリントアウトし、 RA アドミニストレータに送付します。

受付け日時:	2006/03/01 18:31:12
2110 11-1	
シリアル番号:	1931
サブジェクト:	C=JP, O=my organization, OU=business unit, CN=RAOP0150,
開始日時:	2006/03/01 18:28:37
終了日時:	2009/02/28 18:28:37
失効理由:	特定しない

図 3-24 RA オペレータ失効申請結果画面

3.4.2. RA アドミニストレータ — 失効許可—

**1** RAオペレータ管理サイト(https://サイト名/CA 名\_ra/airaadmin)に RA アドミニストレータで ログインし、「失効申請一覧」を選択します。



2 失効申請者のリストが表示されるので、失効申請者の「revoke」を選択します。

RAオペレーター覧	[ _							
						最大;	表示件数: 20	•
オペレータ名称		氏名	EMAIL	A ¥	状態		律作	
E RAOP0150		uni taro	test@mail.com		WAIT_REV	OKE	[revoke]	
						P	age 1 (Return	: 1)

図 3-26 失効申請一覧画面

**3** RA オペレータ証明書情報の確認を行い、失効理由にチェックを入れ、「証明書の失効」ボタンをクリックします。

▶ RAオペレータ証明	書情報
!! RAオペレータ証明	書を失効します !!
RAオペレータ証明書を 失効を行なう場合 [証明 [失効をキャンセルする]	失効すると、該当するRAオペレータによる操作が行なえなくなります。 月書の失効]ボタンをクリックしてください。  ボタンをクリックすると WAIT_REVOKE から ACTIVE 状態に復帰します。
項目名	项目内容
シリアル番号:	1931
サブジェクト:	C=JP, O=my organization, OU=business unit, CN=RAOP0150,
開始日時:	2006/03/01 18:28:37
終了日時:	2009/02/28 18:28:37
[証明書詳細を表示]	
失効理由の設定	
◎ 特定しない	鍵の破損
○ 証明書更新	○ 一時停止
	証明書の失効 失効をキャンセルする

図 3-27 RA オペレータ証明書失効画面

## 3.5. RA オペレータ申請検索

RAアドミニストレータの操作画面から「RAオペレータ申請検索」を選択することで、オペレータの申請を検索することができます。検索結果はリストで表示され、RA オペレータ申請一覧と同じように証明書の発行審査画面へリンク移動が可能です。

AJベレータ申請 検索条件を指定し	の検索を行ないます。 、「検索」ボタンをクリックしてください。
検索区分:	③ 氏名(部分一致)
	○ メールアドレス(部分一致)
	○ 申請番号(完全一致)
	○ 所属(部分一致)
	○ 電話番号(部分一致)
検索文字列:	

図 3-28 RA オペレータ申請検索画面

検索項目はそれぞれ以下の通りです。

氏名	氏名(属性型 CN)の一部を指定します。 例 suzuki
メールアドレス	メールアドレス(属性型 mail)の一部を指定します。 例. suzuki@
申請番号	申請番号(属性型 CN)の完全一致の値を指定します。 例. RAREG0011
所属	所属(属性型 OU)の一部を指定します。 例. science
電話番号	電話番号(属性型 telephoneNumber)の一部を指定します。 例. 090 1234
## 3.6. RA オペレータ申請リスト表示

「RAオペレータ申請検索」もしくは「RAオペレータ申請一覧」にて、現在 RAオペレータ証明書 申請中の申請リストを表示することができます。これらの表示項目について解説します。



図 3-29 RA オペレータ申請リスト画面

- 申請番号のリンクを表します。このリンクをクリックすることで、RA オペレータ申請の審 査画面に移行します。
- ② 最大表示件数を示すリストボックスです。10, 20, 50, 100 件を選択することができます。
- ③ ソートを行うためのアイコンです。「申請番号」「EMAIL」「申請日時」について昇順、降 順でソートが可能です。
- ④ 現在の表示ページとLDAPのリターン項目数を表します。最大表示件数を超えるリターン項目数がある場合、別ページへのリンクが表示されます。なお、最大リターン項目数は1000件となります。

# 3.7. RA オペレータ検索

RA アドミニストレータの操作画面から「RA オペレータ検索」を選択することで、RA オペレータ を検索することができます。検索結果はリストで表示され、RA オペレーター覧と同じように証明 書の更新や失効処理等が行えます。

NAREGICA -	RAオペレータ管理サイト	操作者名 鍵ID	CN=RAAdmin003, e8f49984eb5b08e416b081c60fb31b8dc08cb30a
サイト操作	RA管理者操作 RAオペレータ操作		
RAオペレータ	検索		
Aオペレータの検 検索条件を指定し	索を行ないます。 、[検索]ボタンをクリックしてください。		
検索区分:	<ul> <li>氏名(部分一致)</li> </ul>		
	○ メールアドレス(部分→致)		
	○ オペレータ名称(完全一致)		
	○ 所属(部分一致)		
	○ 電話番号(部分一致)		
	○ 状態(完全一致)		
検索文字列:			
		検索を実行	1

図 3-30 RA オペレータ検索画面

検索項目はそれぞれ以下の通りです。

丘夕	氏名(属性型 CN)の一部を指定します。
氏石	例. suzuki
メニルマドレフ	メールアドレス(属性型 mail)の一部を指定します。
<u> </u>	例. suzuki@
ナペレークタ 社	オペレータ名称(属性型 CN)の完全一致の値を指定します。
オハレージ石杯	例. RAOP0011
元度	所属(属性型 OU)の一部を指定します。
川周	例. science
委託圣旦	電話番号(属性型 telephoneNumber)の一部を指定します。
电动借方	例. 090 1234
	状態値(属性型 st)の完全一致の値を指定します。
	指定できる値は以下の通り。
	ACTIVE 現在有効な証明書を保持しています。
状態	REVOKED 証明書が無効なユーザです。
	WAIT_ISSUE 発行許可後、ユーザによる証明書発行待ちです。
	WAIT_REVOKE 失効申請中です。
	WAIT_UPDATE 更新申請中です。

## 3.8. RA オペレータリスト表示

「RAオペレータ検索」もしくは「RAオペレーター覧」にて、現在のRAオペレータリストを表示することができます。これらの表示項目について解説します。

RAオペレーター覧 ③				最7	(2)
月ペレータ名称 🔺	6 氏名	EMAIL	状態		<b>操作</b>
RAOP0171	test taro		ACTIVE		[update][revoke] [delete][view]
RAOP0170	aaa bbb		 ACTIVE		[update][revoke] [delete][view]
X <u>RAOP0168</u>	test desu	-	 WAIT_ISSI	UE	[delete]
X <u>RAOP0167</u>	test desu	-	 WAIT_ISSI	UE	[delete]
X <u>RAOP0166</u>			 WAIT_REV	OKE	[ <u>revoke</u> ] [ <u>delete][view]</u>
R <u>RAOP0165</u>	BUNKYO JIRO	1000	 ACTIVE	(4)	[ <u>update][revoke]</u> [delete][view]
区 <u>RAOP0164</u>	BUNKYO TARO		WAIT_ISSI	UE	[ <u>delete</u> ]
RAOP0163	popo taro		ACTIVE		[ <u>update][revoke]</u> [ <u>delete][view</u> ]
RAOP0162	unitaro		ACTIVE		[ <u>update][revoke]</u> [ <u>delete][view</u> ]
© <u>RAOP0161</u>	ume ume		 <b>S</b> YOKED	·	[update] [defeite][view]
	•			Page	1 <u>2</u> 3 (Return : 26)

図 3-31 RA オペレータリスト画面

- ① オペレータ名称のリンクを表します。このリンクをクリックすることで、RA オペレータ情報の表示と修正画面に移行します。
- ② 最大表示件数を示すリストボックスです。10, 20, 50, 100 件を選択することができます。
- ③ ソートを行うためのアイコンです。「オペレータ名称」「EMAIL」「状態」について昇順、降 順でソートが可能です。
- ④ RAオペレータに対する操作メニューです。操作内容は次の通りです。

	証明書の更新を行うメニューです。RA オペレータからの申請がな
update	くても、証明書の更新が可能です。
	状態が ACTIVE、REVOKED の場合に表示されます。
	証明書の失効を行うメニューです。RA オペレータからの申請がな
revoke	くても、証明書の失効が可能です。
	状態が ACTIVE の場合に表示されます。
	RA オペレータ情報の削除を行います。LDAP からエントリの削除
delete	を行うため、この操作を行うと、該当する RA オペレータへの一切
	の操作が行えなくなります。

	全ての状態で表示されます。
view	RA オペレータ証明書の詳細情報を表示します。 状態が ACTIVE、REVOKED の場合に表示されます。

⑤ 現在の表示ページとLDAPのリターン項目数を表します。最大表示件数を超えるリターン項目数がある場合、別ページへのリンクが表示されます。なお、最大リターン項目数は1000件となります。

#### 3.8.1. RA オペレータ情報表示・変更

RA オペレータリストのオペレータ名称をクリックすると、RA オペレータ情報の表示と修正画面を表示することができます。これらの表示項目について解説します。

▶RAオペレータ情報				
RAオペレータの情報を表示します。 項目を変更したい場合、項目名をクリックしてテキストを変更してください。 「update!」をクリックすると情報を更新します。				
	정모라☆			
項日名	項目內容			
<u>氏名</u> :	2 ひとなまえ			
<u>Email</u> :	jtest@localhost update!			
<u>所属</u> :	а			
<u>所属番号</u> :	Ь			
<u>豊位</u> :	c			
<u> 電話番号1</u> :	d			
<b>重話番号 2</b> :	e			
<u>FAX 1</u> :	f			
<u>FAX 2</u> :	g			
<u>郵便番号</u> :	h			
<u>住所</u> :	i			
<u>関連URL</u> :	j			
<u>その他・備考</u> :	8			
管理グループ:	SMIME user Architectonics Computer Science Economics			
状態:	ACTIVE			

図 3-32 RA オペレータ情報画面

- RA オペレータ情報の項目名です。修正したい項目をクリックすると、項目内容が編集 可能になります。
- ② RA オペレータ情報の項目内容です。編集可能な状態で「update!」をクリックすると該 当する LDAP エントリの属性値を更新します。
- ③ 管理可能なグループを表します。RA オペレータに管理してもらうグループ名のチェック ボックスを有効にして「update!」をクリックすることで修正が可能です。

# 4. エンドユーザ

本章ではユーザが Challenge PIN を使用して証明書申請、更新、失効を行うときの手順と RA オペレータ操作画面について説明します。

### 4.1. RA オペレータ操作画面

https://サイト名/CA 名\_ra/airaop にアクセスすることで、RA アドミニストレータの操作画面を 表示することができます。この画面を表示するには、SSL クライアント認証が必要であり、RA アド ミニストレータから RA オペレータ用の IC カードを発行してもらい、この IC カードを使用する必要 があります。

NAREGI-CA	dia in	New Street Statistics Viz.		
National Research Grid Initiative				
NAREGI CA - ユーザ管理サイト	操作者名 鍵ID	CN=RAOP0171 61d44653e8ff75cdef71d6c24e1bef534aacd49f		
サイト操作 RAオペレータ操作 ユーザ操作		操作対象グループ: SMIME user 💉		
<ul> <li>► RAオペレータ情報</li> <li>● オペレータ情報詳細 / Challenge PIN 変更</li> <li>● RAオペレータ証明書詳細 / RAオペレータ証明書ダウンロード / RAオペレータ証明書更新 / RAオペレータ証明書失効</li> <li>● CA証明書詳細 / CA証明書ダウンロード / CRLダウンロード</li> </ul>				
▶ ユーザ証明書操作一覧				
◎ユーザ証明書新規申請				
○証明書申請検索/証明書申請一覧/証明書更新申請一覧/証明書失効申請一覧				
◎ ユーザ検索 / ユーザー覧				
(c) 2006 National Research Grid Initiative		NAREGI-CA RA Management.		

#### それぞれのメニューの内容は以下の通りです。

オペレータ情報詳細	RA オペレータ情報を表示します。組織名や電話番号等の登録情報 の表示と更新を行う場合に利用します。
Challenge PIN 変更	RA オペレータの Challenge PIN を変更します。
RA オペレータ証明書 詳細	RA オペレータ証明書の内容を表示します。
RA オペレータ証明書	RA オペレータ証明書をダウンロードします。秘密鍵はダウンロード
ダウンロード	できません。
RA オペレータ証明書 更新	RA オペレータ証明書の更新申請を行います。

RA オペレータ証明書 失効	RA オペレータ証明書の失効申請を行います。
CA 証明書詳細	CA 証明書の内容を表示します。
CA 証明書ダウンロード	CA 証明書をダウンロードします。
CRL ダウンロード	最新の CRL をダウンロードします。
ユーザ証明書新規申請	ユーザ証明書を新規に申請します。 申請ページを新たに開きます。
証明書申請検索	指定の「操作グループ」を対象とする、ユーザ証明書の申請を検索 します。
証明書申請一覧	指定の「操作グループ」を対象とする、ユーザ証明書の申請の一覧 を表示します。
証明書更新申請一覧	指定の「操作グループ」を対象とする、ユーザ証明書の更新申請の 一覧を表示します。
証明書失効申請一覧	指定の「操作グループ」を対象とする、ユーザ証明書の失効申請の 一覧を表示します。
ユーザ検索	指定の「操作グループ」を対象とする、ユーザを検索します。LDAP エントリを検索するため、証明書発行を行っていないユーザの情報 も表示します。
ユーザー覧	指定の「操作グループ」を対象とする、ユーザの一覧を表示します。 LDAP エントリを検索するため、証明書発行を行っていないユーザ の情報も表示します。
トップページ (サイト操作メニュー)	トップページを表示します。
ログアウト (サイト操作メニュー)	ログアウト操作を行い、セッションをクリアします。
操作対象グループ メニュー	RA アドミニストレータにより指定されたグループを操作対象とします。

## 4.2. ユーザ証明書発行



ユーザ 処理の流れ 一証明書の申請—









## 4.2.1. ユーザ ―証明書申請―

- ユーザはユーザ操作メニューサイト(https://サイト名/CA 名\_ra/airegist)にアクセスし、「ユ ーザ証明書新規申請」を選択します。(SSL クライアント認証は不必要です)
  - \* ユーザ名はローマ字のみ対応しています。
  - \* グループ内で同一のユーザ名、Email の場合、申請エラーとなります。

NAREGI-CA Excitization Automaticy for ver Automatica for Autoryphic Library	
National Research Grid Initiative	( Hand
NAREGI CA - ユーザ操作メニュー	
▶ 操作メニュー	
電子証明書に関する操作を行います。 操作メニューをクリックして操作を実行してください。	
新規に電子証明書を申請します。	
◎ ユーザ 証明書 新規申請	
既に証明書を取得している場合、ユーザ証明書の更新と失効の申請が可能です。 また、Challenge PIN の変更も下記メニューにて行ないます。	
◎ ユーザ証明書更新申請 / ユーザ証明書失効申請 / Challenge PIN 変更	
CA証明書の表示とCA証明書のダウンロードを行ないます。 また、最新のCRLのダウンロードを行ないます	
◎ CA証明書詳細 / CA証明書ダウンロード / CRLダウンロード	
(c) 2006 National Research Grid Initiative	NAREGI-CA RA Management

図 4-1 ユーザ操作メニュー画面

2 ユーザ証明書レジストレーションのページが表示されるので、証明書申請ユーザの情報を 入力します(氏名・E-mail・Challenge PIN は必須です)。項目を入力した後、画像認証のた めの文字列を入力し「証明書情報の確認」ボタンをクリックします。

ユーリ油種人力		G.A. 10	
申請先名称	SMIME user	•	
項目名	項目内容		
氏名:	(改生) NEC	(名) HANAKO 0	
Email :	hana_nec@demo.nec.co.jp hana_nec@demo.nec.co.jp		0
Email(確認用):			0
Challenge PIN :	•••••		
Challenge PIN (確認用):		0 •1	
所属:			
・ 画像認証 フォーム入力が正しく行 下記の画像の数字5ケ 文字列: [0737]	われているか確認する タを入力してください。 割 0	ために、画像認証を行か 	よいます。 <b> 578</b> 話にお問い合わせくたさい。

図 4-2 ユーザ証明書レジストレーション画面

**3** 表示される情報を確認し、入力内容に誤りがなければ「証明書の申請」ボタンをクリックしま す。

I	NAREGI CA - ユーザ証明書レジストレーション			
	証明書の申請が完了しました 必要であれば下記のフォームを印刷して管理者に提出してください。			
	受付け 番号:	REG000257		
	受付け日時:	2006/03/10 15:38:15		
	申請先名称	SMIME user		
	申請者氏名:	NEC HANAKO		

図 4-3 ユーザ証明書レジストレーション確認画面

4 申請が完了すると、RA オペレータから確認メールが送信されます。

タイトル:新規ユーザ証明書の申請 送信者: ra\_ope1@demo.nec.co.jp 宛先: hana\_nec@demo.nec.co.jp 送信日付: Fri, 10 Mar 2006 15:43:52 +0900 新規ユーザ証明書の申請を受け付けました。 受付番号: REGOO0257 ユーザ名称 : NEC HANAKO MAILアドレス: hana\_nec@demo.nec.co.jp 現在、RAオペレータにより審査を行なっています。 審査完了後、メールにて通知を行ないます。

図 4-4 確認メール内容

4.2.2. RA オペレータ —申請許可—

ユーザ管理サイト(https://サイト名/CA 名\_ra/airaop)に RA オペレータでログインし、「証明書申請一覧」を選択します。

NAREGLCA	
Carl file allon Authority Server Foundard by AlCrypta Library	State of the second second second
National Research Grid Initial	tive
NAREGI CA - ユーザ管理サイト	<b>操作者名</b> CN=RAOP0165 鍵ID b59a1590e6ee0b3ed2bf08e1d52e2423e34f897
サイト操作 RAオペレータ操作 ユーザ捕	Mfe 操作対象グループ: SMIME user
○ CA証明書詳細 / CA証明書グウンロード /	で用語をリンロード/RAJベレータ証明語更新/RAJベレータ証明書天効 CRLダウンロード
▶ つ	
<ul> <li>○ ユーザ証明書新規申請</li> <li>○ 正明素申請検4 / 証明素申請→覧 / IFII</li> </ul>	1.* 更新申請一覧 / 証明:# 牛効申請一覧
のユーザ検索/ユーサ い	and an

図 4-5 ユーザ管理サイト画面

2 申請しているユーザの申請番号を選択します。

NAREGI CA -	ユーザギ	管理サイト		操作者名 鍵ID	CN=RAOP0165, b59a1590e6ee0	b3ed2bf08e1d52e24	423e34f8979
サイト操作	RAオペレ	,一夕操作 ユーザ操	ŕŧ		操作	乍対象グループ: SM	AIME user 💌
▶申請一覧							
						最大表示件	⊧数:20 💌
申請番号		氏名	EMAI	L		申請日時	
¥ <u>REG000257</u>	>	NEC HANAKO	hana_ne	ec@demo.nec.	co.jp	2006/03/10 15:3	8:15
X REGUUU253		restinue:	charge	<b>Bésir</b> Mar	nasje	100000000000000000000000000000000000000	18:00
Z <u>REG000229</u>		iligender:	antificia	aliser"		200000000077720	1954
X REG000203		différent:	-	the strict of the second	1450		Eineli
						Page 1	(Return : 4)

図 4-6 申請一覧画面

**3** ユーザの申請内容を確認し「発行を許可する」ボタンをクリックします。申請者に通知する場合は、「申請者に通知する」にチェックを入れます(デフォルト有効)。

NAREGI CA - ユ	ーザ管理サイト	操作者名 鍵ID	CN=RAOP0165. b59a1590e6ee0b3ed2bf08e1d52e2423e34f8975
サイト操作 RA	オペレータ操作 ユーザ操作		
コーザ証明書申	清確認		
ーザ証明書の発行 諸内容を確認し、 た、必要な情報が	i確認を行ないます。 証明書の発行許可もしくは拒認 あれば追加・削除してしてくだ	雪を行なってください。 さい。	
受付け番号:	REG000257		
受付け日時:	2006/03/10 15:38:15		
<ul> <li>✓ 申請者</li> <li>→ → → → → → → → → → → → → → → → → → →</li></ul>	Hこ <b>通知する</b> 5 <u>有効にすると</u> 発行審査の 1時に有効にすると、鍵ペ 頁目です。	結果をメールで申請 アの生成と証明書の	者に通知します。 取得を申請者が行なうことになります。
		<b>巻行を許可する</b>	発行を拒否する

図 4-7 ユーザ証明書申請確認画面

### 4.2.3. ユーザ ―証明書生成―

**1** ユーザは RA オペレータから、発行許可の旨に関する確認メールを受信し、確認メールに記載されている URL に WEB ブラウザでアクセスします。

タイトル: 電子証明書発行申請のお願い 送信者: ra_ope1@demo.nec.co.jp 宛先: hana_nec@demo.nec.co.jp 送信日付: Fri, 10 Mar 2006 16:25:46 +0900
電子証明書を発行します。 下記のサイトにアクセスし、電子証明書の発行手続きを行なってください。
証明書発行: Phttps://
もしくは grid-certreg コマンドにより、以下のコマンドを入力して証明書の 取得を行なってください。
証明書発行: grid-certreq
なお、証明書の更新と失効の申請は以下のサイトより行なえます。

図 4-8 確認メール内容

2 ユーザ認証ページにて Challenge PIN を入力し、「ログイン」ボタンをクリックします。

	J 221	
電子証 Challer	明書の発行操作を行います。 nge PIN を入力してください。	
	Challenge PIN :	
		ログイン

図 4-9 ユーザ認証画面

3 「鍵ペアを生成し電子証明書を発行する」を選択し、「次へ」ボタンをクリックします。



図 4-10 操作選択画面

4 RAオペレータ証明書発行画面にて下記項目を設定し「証明書を発行する」を選択します。

設定項目	備考
CSP	証明書のインストール先。Microsoft~Cryptographic
	Provider を選択すると PC のハードディスクにインストー
	ルします。IC カードにインストールする場合は、対応する
	CSP を選択します。
秘密鍵の長さ	鍵長が長い程安全性が高くなります
秘密鍵のエクスポート	可能に設定すると、Windows の内部ストアから秘密鍵を
	エクスポートすることが可能になります。
秘密鍵の保護レベル	「通常」を選択した場合、Windows で秘密鍵を用いる時に
	パスワードの入力を簡略化できます。
	「強力な保護」を選択した場合、秘密鍵を利用する度にパ
	スフレーズの入力が必要となります。



図 4-11 ユーザ情報入力フォーム画面

5 「電子証明書をインストール」ボタンをクリックし、証明書を PC もしくは IC カードにインストー ルします。



図 4-12 電子証明書インストール画面

6 インストールが正常に完了すると、下記の図が表示されます。

電子証明書のインストールが完了しました

ICカードをICカードリーダ/ライタから取り外し可能です。

RA管理者であれば、管理者用のICカードに入れ替えてください。 3秒後に自動で管理者画面に移動します。

図 4-13 電子証明書インストール結果画面

## 4.3. ユーザ証明書更新

ユーザ証明書の更新処理は以下の手順で行います。

ユーザ 処理の流れ





#### ユーザ 処理の流れ-証明書申請-



4.3.1. ユーザ —更新申請—

1 ユーザは証明書更新通知メールを受信します。

送信者: ra_opel@demo.nec.co.jp 宛先: hana_nec@demo.nec.co.jp 送信日付: Fri, 10 Mar 2006 15:43:52 +0900
お使いの電子証明書は、あと 7 日以内に有効期限切れとなります。
証明書の更新を行なう場合は、以下のサイトにアクセスし、更新の申請手続きを 行なってください。
更新申請: https://
証明書の更新を行なわない場合は、手続きを行なう必要はありません。
 NAREGI CA WEB Enroll サービス

図 4-14 証明書更新通知メール

**2** ユーザは証明書更新通知メール記載されている URL に WEB ブラウザでアクセスします。 そしてユーザ認証ページにて Challenge PIN を入力し、「ログイン」ボタンをクリックします。

▶ユーザ型	<b>I</b>	
電子証明書( Challenge PI	D発行操作を行います。 N を入力してください。	
)	Challenge PIN :	
		ログイン

図 4-15 ユーザ認証画面

3 ユーザ証明書レジストレーションのページが表示されるので、ユーザ情報を入力します(氏名・E-mail・Challenge PIN は必須です)。項目を入力した後、画像認証のための文字列を入力し「証明書情報の確認」ボタンを押します。

2ーザ情報入力	112]ホタンをクリックし	てください。		
申請先名称	SMIME user	•		
项目名	项目内容			
天名:	(改生) NEC	(名) HANAKO	0	
ímail :	hana_nec@demo	.nec.co.jp		0
mail(確認用):	hana_nec@demo	.nec.co.jp		0
hallenge PIN :	••••		<b>0</b> +1	
hallenge PIN (確認用):			0 +1	
fi 🖪 :	3			
・ 画像認証 フォーム入力が正しく行れ 下記の画像の数字5ケタネ 文字列: [07378]	のれているか確認 き入力してください ①	するために、画作		

図 4-16 ユーザ証明書レジストレーション画面

- **4** 表示される情報を確認し、入力内容に誤りがなければ「証明書の申請」ボタンをクリックしま す。
- 5 証明書申請完了ページが表示されるので、「印刷する」ボタンを押し、申請書をプリントアウトします。プリントアウトした申請書を RA オペレータに送付します。

١	NAREGI CA - ユーザ≣	証明書レジストレーション
1	証明書の申請が完了しま 必要であれば下記のフォ・	した ームを印刷して管理者に提出してください。
	受付け 番号:	REG000257
	受付け日時:	2006/03/10 15:38:15
	申請先名称	SMIME user
	申請者氏名:	NEC HANAKO

図 4-17 ユーザ証明書レジストレーション確認画面

6 申請手続きが終了すると、RA オペレータからの確認メールを受信します。

タイトル: 新規ユーザ証明書の申請 送信者: ra_opel@demo.nec.co.jp 宛先: hana_nec@demo.nec.co.jp 送信日付: Fri, 10 Mar 2006 16:47:15 +0900
ユーザ証明書の更新申請を受け付けました。
ユーザ名称 : NEC HANAKO MAILアドレス: hana_nec@demo.nec.co.jp
現在、R&オペレータにより審査を行なっています。 審査完了後、メールにて通知を行ないます。
 NAREGI CA WEB Enroll サービス

図 4-18 確認メール

4.3.2. RA オペレータ ―申請許可―

1 ユーザ管理サイト(https://サイト名/CA 名\_ra/airaop)に RA オペレータでログインします。 「証明書更新申請一覧」を選択して更新申請一覧を表示します。

	ECLOA		Tet	
AVAD S	CECI-CA Information Authority Server	350		No. 10 Addition Vice
$\Delta M$			1	and the second sec
Nationa	I Research Grid	d Initiative		
NAREGICA	- ユーザ管理サイト		操作者名	CN=RAOP0165
			鍵ID	b59a1590e6ee0b3ed2bf08e1d52e2423e34f897
サイト操作	RAオペレータ操作	ユーザ操作		操作対象グルーブ: SMIME user 🔊
D <u>オペレータ</u> 個 D <u>RAオペレー</u> タ	報詳細 / Challenge	PIN 変更 ペレータ証明書ダウ		ペレータ証明書更新 / RAオペレータ証明書失効
D <u>オペレータ</u> 情 D <u>RAオペレージ</u> D <u>CAIE明書</u> 詳	報評編 / Challenge 対証明素詳細 / RA才 編 / <u>CA証明素</u> がの)	<u>PIN 変更</u> ペレータ証明書ダウ / <u>ロード</u> / <u>CRLダウン</u>	ンロード / RAZ /ロード	ペレータ証明書更新 / RAオペレータ証明書失効
● <u>オペレータ</u> 備 ● <u>RAオペレー</u> ク ● <u>CA証明書詳</u> ◆ユーザ証明	報詳細 / <u>Challenge</u> 2 <u>証明書詳細</u> / <u>RA才</u> 2 <u>編</u> / <u>CA証明書がつい</u> 書操作一覧	<u>PIN 変更</u> ベレータ証明書ダウ ノ <u>ロード</u> / <u>GRLダウン</u>	ンロード / RAZ /ロード	ペレータ証明書更新 / RAオペレータ証明書失効
● <u>オペレータ</u> 舗 ● <u>RAオペレー</u> 3 ● <u>CAIE明書詳</u> ●ユーザ証明 ●ユーザ証明	報詳鐘 / <u>Challenge</u>  2証明書詳細 / <u>RA才</u>  編 / <u>CA証明書がつい</u> 書操作一覧   開新規申議	<u>PIN 変更</u> ペレータ証明書ダウ <u>パロード</u> / <u>GRLダウン</u>	<u>20-</u> F / BAZ 2 <u>0-F</u>	ペレータ証明書更新 / RAオペレータ証明書失効
● <u>オペレータ</u> 儲 ● <u>BAオペレー</u> 分 ● <u>CA証明</u> 書詳 ● ユーザ 証明 ● <u>ユーザ 証明</u> ● <u>証明</u> 衆申請:	報詳細 / <u>Challence</u>       短明書詳細 / <u>RA才</u>       編 / <u>CA証明書がつい</u>     書   	<u>PIN 変更</u> ペレータ証明書ダウ <u>パロード / GRLダウン</u> & / 証明書更新申		ペレータ証明書更新 / RAオペレータ証明書失効 島失効申請一覧

図 4-19 ユーザ管理サイト画面

2 ユーザ証明書更新申請の一覧が表示されるので、証明書を更新するユーザの「update」を 選択します。



図 4-20 更新申請一覧画面

3 ユーザ証明書の情報が表示されるので、ユーザを審査し「発行許可」ボタンをクリックします。 この時ユーザに許可した旨を通知するために「申請者に通知する」にチェックを入れます(デ フォルト有効)。

NAREGI CA - 2	-ザ管理サイト		律作者名 鍵ID	CN=RAOP0165, b59a1590e6ee0b3ed2bt08e1d52e2423e34f8975
サイト操作 RA	オペレージ幹作	ユーザ操作		
>ユーザ証明書中)	清確認			
ユーザ証明書の発行 申請内容を確認し、日 また、必要な情報があ	確認を行ないます 同者の発行許可 5れば通知・新約	-。 もしくは拒否を行な してしてください。	いてください。	
受付け番号:	REG000257	t.		
受付け日時:	2006/03/10	0 15:38:15		
<ul> <li>申請者に</li> <li>第二〇支車</li> <li< th=""><th>: <b>通知する</b> (<u>か): すみと元</u> 句: 有効にする。 目です。</th><th>⊤審査の結果を と、 纏べアの生⊧</th><th>メールで申請: 成と証明書の)</th><th>暫に通知します。 取得を申請者が行なうことになります。</th></li<></ul>	: <b>通知する</b> ( <u>か): すみと元</u> 句: 有効にする。 目です。	⊤審査の結果を と、 纏べアの生⊧	メールで申請: 成と証明書の)	暫に通知します。 取得を申請者が行なうことになります。
		発行を許	न इठ	発行を拒否する

図 4-21 ユーザ証明書申請確認画面

## 4.3.3. ユーザ ―証明書生成―

**1** RA オペレータから送信されたライセンス ID メールを受信します。

タイトル:電子証明書発行申請のお願い 送信者: ra_ope1@demo.nec.co.jp 宛先: hana_nec@demo.nec.co.jp 送信日付: Fri, 10 Mar 2006 16:25:46 +0900
電子証明書を発行します。 下記のサイトにアクセスし、電子証明書の発行手続きを行なってください。
証明書発行: https://
もしくは grid-certreq コマンドにより、以下のコマンドを入力して証明書の 取得を行なってください。
証明書発行: grid-certreg
なお、証明書の更新と失効の申請は以下のサイトより行なえます。

図 4-22 ライセンス ID メールの受信

**2** ライセンス ID メールに記載されている URL に WEB ブラウザでアクセスします。ユーザ認証 ページにて Challenge PIN を入力し、「ログイン」ボタンをクリックします。

+2-	ザ認証	×
電子証 Challer	明書の発行操作を行います。 nge PIN を入力してください。	
>	Challenge PIN :	
		ログイン

図 4-23 ユーザ認証画面

3 「鍵ペアを生成し電子証明書を発行する」を選択し、「次へ」ボタンをクリックします。



図 4-24 操作選択画面

4 ユーザ情報入力フォームにて、下記項目を設定し「証明書を発行する」を選択します。

設定項目	備考
CSP	証明書のインストール先。Microsoft~Cryptographic
	Provider を選択すると PC のハードディスクにインスト
	ールします。IC カードにインストールする場合は、対
	応する CSP を選択します。
秘密鍵の長さ	鍵長が長い程安全性が高くなります
秘密鍵のエクスポート	可能に設定すると、Windows の内部ストアから秘密
	鍵をエクスポートすることが可能になります。
秘密鍵の保護レベル	「通常」を選択した場合、Windows で秘密鍵を用いる
	時にパスワードの入力を簡略化できます。
	「強力な保護」を選択した場合、秘密鍵を利用する度
	にパスフレーズの入力が必要となります。

	首報	
グループ 名:	SMIME user	
ユーザ情	報	
ユーザ	NEO UANAKO	
名:	NEC HANAKO	
Email :	hana_nec@demo.nec.co.jp	
秘密鍵部	(定)	
CSP:	Microsoft Enhanced Cryptographic Provider v1.0	~
秘密鍵の 長さ:	0512 bit ⊙1024 bit 02048 bit	
秘密鍵の		
秘密鍵の エクスポー		
秘密線の エクスポート:		
秘密鍵の エクスポート: 秘密鍵の (2速しく)	<ul> <li>● 通常 ○ 強力な保護</li> </ul>	
秘密鍵の エクスポー ト: 秘密鍵の 保護レベル	● 通常 ○ 強力な保護	

図 4-25 ユーザ情報入力フォーム画面

**5**「電子証明書をインストール」をクリックし、PC もしくは IC カードに証明書をインストールします。



図 4-26 電子証明書インストール画面

6 インストールが正常に完了すると、以下のような画面が表示されます。



図 4-27 電子証明書インストール結果画面

## 4.4. ユーザ証明書失効

ユーザ証明書の失効処理について以下に示します。

ユーザ 失効処理の流れ





# 4.4.1. ユーザ ―失効申請―

 ユーザ操作メニューページ(https://サイト名/CA 名\_ra/airegist)にて、「ユーザ証明書失効 申請」を選択します。

NAREGI-CA	
National Research Grid Initiative	1 2
NAREGI CA - ユーザ操作メニュー	
▶ 操作メニュー	
電子証明書に関する操作を行います。 操作メニューをクリックして操作を実行してください。	
新規に電子証明書を申請します。	
◎ユーザ証明書新規申請	
期に証明書を取得している場合、ユーザ証明書の更新と失効の申請が可能です。 また、Challenge PIN の変更も下記メニューにて行ないます。	
◎ ユーザ証明書更新申請(ユーザ証明書失効申述(challenge PIN 変更	
CA証明書の表示とCA証明書のダウンロードを行ないます。 また、最新のCRLのダウンロードを行ないます	
◎CA証明書詳細/CA証明書ダウンロード/CRLダウンロード	
	_
c) 2006 National Research Grid Initiative	NAREGI-CA RA Management.

図 4-28 ユーザ操作メニュー画面

2 Challenge PIN を入力して「ログイン」ボタンをクリックします。

>ユーザ	21	in olimitan i mittiitio.	1660 ( 100 ( 100 ( 166 ( 10) 166 ( 10
電子証明 Challenge	書の発行操作を行います。 PIN を入力してください。		
	Challenge PIN :		
		ログイン	

図 4-29 ユーザ認証画面

**3** ユーザ証明書失効申請ページにて失効理由を選択し、「失効の申請」ボタンをクリックします。

NAREGI CA - ユーサ	「証明書失効申請
>ユーザ証明書情報 !! ユーザ証明書を失う	i 効します!!
ユーザ 証明書を失効す 失効を行なう場合 [失す	ると、「該当するユーザによる操作が行なえなくなります。 かの申請】ボタンをクリックしてください。
項目名	项目内容
シリアル番号:	1976
サブジェクト:	C=JP, O=my organization, OU=myorg2, CN=NEC HANAKO /Email=hana_nec@demo.nec.co.jp
開始日時:	2006/03/10 17:07:46
終了日時:	2006/03/17 17:07:46
失効理由の設定	
⊙ 特定しない	◎ 縺の破損
○ 証明書更新	○ 一時停止
	失効の申請

図 4-30 ユーザ証明書失効申請画面

**4** 失効申請結果が表示されるので、表示されたページをプリントアウトし、RA オペレータに送付します。

REGI CA - ユーザ証明書失効申請					
した。 ォームさ印刷して管理者に提出してください。					
2006/03/10 17:12:13					
1976					
C=JP, O=my organization, OU=myorg2, CN= NEC HANAKO /Email=hana_nec@demo.nec.co.j					
2006/03/10 17:07:46					
2006/03/17 17:07:46					
特定しない					

図 4-31 失効確認結果画面

4.4.2. RA オペレータ —失効許可—

**1** ユーザ管理サイト(https://サイト名/CA 名\_ra/airaop)にログインし、「証明書失効一覧」を選択します。

NAREGI-CA	· ····	A AND A AND A AND A
National Research Grid Initiative		
NAREGI CA - ユーザ管理サイト	操作者名 鍵ID	CN=RAOP0165 b59a1590e6ee0b3ed2bf08e1d52e2423e34f8979
サイト操作 RAオペレータ操作 ユーザ操作		操作対象グルージ: SMIME user 💌
<ul> <li>○ RAJベレータ証明書詳細 / RAJベレータ証明書がつ</li> <li>○ CA証明書詳細 / CA証明書がつンロード / CRLダウ</li> </ul>	22 <u>0-</u> E / BAZ	ペレータ証明書更新 / RAオペレータ証明書天効
© <u>CA証明書詳細/CA証明書ダウンロード</u> / <u>CRLダウ</u>	20-1	
> ユーザ 証明書操作一覧		
○ ユーザ証明書新規申請		$\frown$
○ <u>証明書申請検索/証明書申請一覧/証明書更新</u> 明	目请一覧/ 証明:	<u>最失効申請一覧</u>
◎ユーザ検索/ユーザー覧		

図 4-32 ユーザ管理サイト画面

2 失効申請一覧が表示されるので、失効申請者の脇にある「revoke」を選択します。

NAREGI CA - ユーザ管理サイ	ſŀ	操作者名 鍵ID	CN=I b59a	RAOP016 1590e6e	5. e0b3ed	264084	e1d52e2423e	34(8)	979
サイト操作 RAオペレータ操作	乍 ユーザ操作			ħ	象作时刻	をグル	-J: SMIME	user	~
▶ユーザー覧								0.0	
						最	大表示件数	20	~
🗌 ユーザ名称	EMAIL		A 4	状態	**	88 *2	操作		
E S NEC HANAKO	hana_nec@dem	io.nec.co.jp		WAIT_RE	VOKE		[revoke] [delete][.rev	1	
							Page 1 (R	eturn	:1)
[自動承認ON][自動承認OFF] • ###9800項目に対して、一個優性を行われる									

#### 図 4-33 失効申請一覧画面

**3** 失効するユーザの証明書情報を確認し、失効理由を選択して「証明書の失効」ボタンをクリックします。

ユーザ証明書信頼 リユーザ証明書を失い ユーザ証明書を失効す 失効を行なう場合[証明 【失効をキャンセルする]	i 幼します! ると、咳当するユーザによる操作が行なえなくなります。 月書の失効] ボタンをクリックしてください。 ) ボタンをクリックすると WAIT_REVOKE から ACTIVE 状態に復帰します。
項目名	項目內容
シリアル番号:	1976
サブジェクト:	C=JP, O=my organization, OU=myorg2, CN= NEC HANAKO /Email=hana_nec@demo.nec.co.jp
開始日時:	2006/03/10 17:07:46
終了日時:	2006/03/17 17:07:46
【証明書詳細を表示】	
失効理由の設定	
<ul><li>特定しない</li></ul>	○ 縺の破損
○ 証明書更新	○ 一時停止
	11日月書の失効 失効をキャンセルする

図 4-34 ユーザ証明書失効画面

4 失効確認メールがユーザに送信されます。

RA運用者によりユーザ証明書が失効されました。
なお、失効処理について疑問等ありましたら、RA運用者にお問い合わせください。
 NAREGI CA WEB Enroll サービス

図 4-35 失効確認メール

## 4.5. 証明書申請検索

RA オペレータの操作画面から「証明書申請検索」を選択することで、ユーザの申請を検索することができます。検索結果はリストで表示され、証明書申請一覧と同じように証明書の発行審 査画面へリンク移動が可能です。

▶ ユーザ証明書申請検索				
ユーザ証明書申請 検索条件を指定し	約 検索を行ないます。 、[検索]ボタンをクリックしてください。			
検索区分:	<ul> <li>氏名(部分一致)</li> </ul>			
	○ メールアドレス(部分一致)			
	○ 申請番号(完全一致)			
	○ 所属(部分一致)			
	○ 電話番号(部分一致)			
検索文字列:				
	検索を実行			

図 4-36 RA オペレータ申請検索画面

検索項目はそれぞれ以下の通りです。

氏名	氏名(属性型 CN)の一部を指定します。 例. suzuki
メールアドレス	メールアドレス(属性型 mail)の一部を指定します。 例. suzuki@
申請番号	申請番号(属性型 CN)の完全一致の値を指定します。 例. REG000011
所属	所属(属性型 OU)の一部を指定します。 例. science
電話番号	電話番号(属性型 telephoneNumber)の一部を指定します。 例. 090 1234

### 4.6. 証明書申請リスト表示

「証明書申請検索」もしくは「証明書申請一覧」にて、現在ユーザ証明書申請中の申請リストを 表示することができます。これらの表示項目について解説します。

2	申請一覧					2		
	(3)	)				最大表示件数:	20 💌	
ത	申請番号		氏名	EMAIL		申請日時		
U	8 <u>REGUUU253</u>		maho taro	and the second second	· · · · · · · · · · · · · · · · · · ·	2006/03/02 18:28:20	:	1
	8 <u>REG000229</u>	- 1	hoge taro			2006/02/17 17:20:54		
	8 <u>REG000203</u>		bbb ccc	1. State 1. State		2006/02/10 19:45:46	•••••	1
						Page 1 (R	eturn : 3)	
						· · · · · · · · · · · · · · · · · · ·		- 6



- 申請番号のリンクを表します。このリンクをクリックすることで、ユーザ証明書申請の審 査画面に移行します。
- ② 最大表示件数を示すリストボックスです。10, 20, 50, 100 件を選択することができます。
- ③ ソートを行うためのアイコンです。「申請番号」「EMAIL」「申請日時」について昇順、降 順でソートが可能です。
- ④ 現在の表示ページとLDAPのリターン項目数を表します。最大表示件数を超えるリターン項目数がある場合、別ページへのリンクが表示されます。なお、最大リターン項目数は 1000 件となります。

## 4.7. ユーザ検索

RA オペレータの操作画面から「ユーザ検索」を選択することで、ユーザを検索することができます。検索結果はリストで表示され、ユーザー覧と同じように証明書の更新や失効処理等が行えます。

NAREGI CA -	ユーザ管理サイト	操作者名 鍵ID	CN=RAOP0171, 61d44653e8ff75cdef71d6c24e1bef534aacd49
サイト操作	RAオペレータ操作 ユーザ 操作		操作対象グループ: SMIME user 💊
コーザ検索			
ユーザの検索を行 検索条件を指定し	ないます。 、[検索] ボタンをクリックしてください。		
検索区分:	⊙ 氏名(部分一致)		
	○ メールアドレス(部分一致)		
	○ 所属(部分一致)		
	○ 電話番号(部分一致)		
	○ 状態(完全一致)		
検索文字列:			
検索文字列 :		検索を実行	]

図 4-38 ユーザ検索画面

検索項目はそれぞれ以下の通りです。

氏名	氏名(属性型 CN)の一部を指定します。
	例. suzuki
メールアドレス	メールアドレス(属性型 mail)の一部を指定します。
	例. suzuki@
正居	所属(属性型 OU)の一部を指定します。
	例. science
電託来旦	電話番号(属性型 telephoneNumber)の一部を指定します。
电前面方	例. 090 1234
	状態値(属性型 st)の完全一致の値を指定します。
	指定できる値は以下の通り。
	ACTIVE 現在有効な証明書を保持しています。
状態	REVOKED 証明書が無効なユーザです。
	WAIT_ISSUE 発行許可後、ユーザによる証明書発行待ちです。
	WAIT_REVOKE 失効申請中です。
	WAIT_UPDATE 更新申請中です。
### 4.8. ユーザリスト表示

「ユーザ検索」もしくは「ユーザー覧」にて、現在のユーザリストを表示することができます。こ れらの表示項目について解説します。

サイト操作 RAオ	ペレータ操作 ユーザ操作	操作	F対象グループ:	SMIME user
▶ユーザー覧				2
	-			最大表示件数 10 🔽
□ ユーザ名称	③ ▲ ▼ EMAIL	▲ ▼ 状態	自 ▲▼ 動 承 認	操作
	KO	ACTIV	/E 🕜 🗆	[ <u>update][revoke]</u> [ <u>delete][view]</u>
	100000000	WAIT	ISSUE 🗌	(4) [delete]
🔲 🔒 <u>RAOP taro</u>		ACTIN	Æ	[ <u>update][revoke]</u> [ <u>delete][view]</u>
🗌 homu taro		(null)		[delete]
🔲 <u>koko neko</u>		(null)	V	[ <u>delete]</u>
🔲 <u>kuni jiro</u>		(null)	0	[delete]
🔲 <u>kuniyasu</u>		(null)	0	[delete]
🔲 🎗 <u>sato jiro</u>		ACTIN	/E	[ <u>update][revoke]</u> [ <u>delete][view</u> ]
t0012346		(null)		[delete]
☐ <u>test</u>	(null)	(null)		(b) (refete)
	記 OFF1			rage i Z (Return:16)
* チェック80%項目にす	扎 で、 一括操作を行ないます。			

図 4-39 ユーザリスト画面

- ユーザ名称のリンクを表します。このリンクをクリックすることで、ユーザ情報の表示と 修正画面に移行します。
- ② 最大表示件数を示すリストボックスです。10, 20, 50, 100 件を選択することができます。
- ③ ソートを行うためのアイコンです。「ユーザ名称」「EMAIL」「状態」について昇順、降順 でソートが可能です。
- ④ ユーザに対する操作メニューです。操作内容は次の通りです。

	証明書の更新を行うメーユーです。ユーサからの申請かなくても、
update	証明書の更新が可能です。
	状態が ACTIVE、REVOKED の場合に表示されます。
	証明書の失効を行うメニューです。ユーザからの申請がなくても、
revoke	証明書の失効が可能です。
	状態が ACTIVE の場合に表示されます。

delete	ユーザ情報の削除を行います。LDAP からエントリの削除を行うため、この操作を行うと、該当するユーザへの一切の操作が行えなくなります。
	全ての状態で表示されます。
view	ユーザ証明書の詳細情報を表示します。
	状態が ACTIVE、REVOKED の場合に表示されます。

- ⑤ 現在の表示ページとLDAPのリターン項目数を表します。最大表示件数を超えるリターン項目数がある場合、別ページへのリンクが表示されます。なお、最大リターン項目数は1000件となります。
- ⑥ 自動承認用のチェックボックスです。自動承認を ON にしたい場合、複数のユーザを指定して[自動承認 ON]をクリックすることで、「自動承認」項目のチェックアイコンが表示され、該当するユーザに対して自動承認を許可できます。同様に、[自動承認 OFF]をクリックすると自動承認を無効にできます。また、一番上の項目名("ユーザ名称")の横に表示されているチェックボックスにより、一括チェックが可能です。
- ⑦ 自動承認の許可/無効を表すアイコンです。アイコンを直接クリックすることで、自動承認の ON/OFF が行えます。

### 4.8.1. ユーザ情報表示・変更

ユーザリストのユーザ名称をクリックすると、ユーザ情報の表示と修正画面を表示することが できます。これらの表示項目について解説します。

- IJ	■ユーザ情報 ニーザの情報を表示します 項目を変更したい場合、可	す。 頁目名をクリックしてテキストを変更してください。 体和な事業は ナナ	
Č	Dare:1.520.623.95		
	項目名	項目内容	
	<u>氏名</u> :	RACP taro	
	<u>Email</u> :	raoptaro@localhost	
	<u>所属</u> :	а	
	<u>所属番号</u> :	b	
	<u>職位</u> :	c	
	<u>電話番号1</u> :	d	
	<b>重話番号 2</b> :	e	
	<u>FAX 1</u> :	f	
	<u>FAX 2</u> :	g	
	<u> 郵便番号</u> :	1110001	
	住所:	東京都	
	<u>関連URL</u> :	http://hoge.com/	
	<u>その他・備考</u> :	なし。	
	状態:	ACTIVE	

図 4-40 RA オペレータ情報画面

- ユーザ情報の項目名です。修正したい項目をクリックすると、項目内容が編集可能になります。
- ② ユーザ情報の項目内容です。編集可能な状態で「update!」をクリックすると該当する LDAP エントリの属性値を更新します。

## 5. 自動承認発行(IC カード連携)

自動承認発行とは、予め LDAP のユーザエントリに証明書発行許可のフラグを追加し、このユ ーザエントリに該当するユーザ(例えば、他の認証局から既に証明書を取得しているユーザ)が、 SSL クライアント認証を行ってきた場合に、RA オペレータによる承認処理を行わずに、その場で 証明書発行許可を行うものです。

この手順で証明書を発行する場合、以下のようなフローになります。

#### ユーザ 処理の流れ 一証明書の申請一



# 5.1. 事前準備

**1** RA オペレータはユーザ管理サイト(https://サイト名/CA 名\_ra/airaop)にアクセスし、「ユー ザー覧」を選択します。

National Research Grid Initiative	ET	1
NAREGI CA - ユーザ管理サイト	操作者名 鍵ID	CN=RAOP0171 61d44653e8ff75cdef71d6c24e1bef534aacd49f
サイト操作 RAオペレータ操作 ユーザ操作		操作対象グループ: SMIME user 🛛 👻
▶RAオペレータ情報		
◎ <u>オペレータ情報詳細</u> / <u>Challenge PIN 変更</u>		
◎ RAオペレータ証明書詳細 / RAオペレータ証明書ダ	<u>ウンロード</u> / <u>RAオ/</u>	ペレータ証明書更新 / <u>RAオペレータ証明書失効</u>
◎ <u>CA証明書詳細</u> / <u>CA証明書ダウンロード</u> / <u>CRLダウ</u>	<u>א-םעל</u>	
▶ユーザ証明書操作一覧		
◎ ユーザ証明書新規申請		
○ 証明書申請検索 / 証明書申請一覧 / 証明書更新	申請一覧/証明書	<u>≵失効申請一覧</u>

図 5-1 ユーザ管理サイト画面

**2** ユーザー覧が表示されるので、リスト項目のチェックボックスにチェックを入れ、「自動承認 ON」を選択します。

> J	ーザー覧					
					最大調	表示件数: 20 🔽
	ユーザ名称		EMAIL	状態▲▼	自動承認	操作
			hana_nec@demo.nec.co.jp	ACTIVE		[update][revoke] [delete][view]
	承認の1月動な	NOFF 操作を行ない	] ます.			
(c) 2006 I	National Research G	id Initiativ	e		NAR	EGI-CA RA Management.

### 図 5-2 ユーザー覧画面

### 5.2. ユーザ証明書取得処理

- **1** ICカードに入っている証明書を利用して、ユーザ証明書レジストレーションページ(https://サ イト名/CA 名\_ra/airegist)にログインします(SSL クライアント認証が必要です)。
- 2 ユーザ証明書レジストレーションのページが表示されるので、新規にチャレンジ PIN を入力 し「証明書情報の確認」ボタンをクリックします(古い PIN は上書きされます)。

NAREGI-CA Gertification Authority Server Powered by AlCrypto Library	Mary and the Mary
National Research Grid Initiative	1 4 4 2 Martin
NAREGI CA - ユーザ証明書レジストレーシ	(ヨン
SSLクライアント認証により、新しく証明書発行 項目を確認し、問題が無ければ「証明書を申請	が可能であることを確認しました。 1] ボタンをクリックしてください。
なお、初めての証明書発行の場合は Challeng 2回目以降の場合、以前指定した Challenge P	e PIN を指定してください。 IN が使用されます。
■ユーザ情報確認	
項目名	項目内容
氏名 :	NEC HANAKO
Email :	hanako_nec@demo.nec.co.jp
Challenge PIN :	0
Challenge PIN (確認用):	
所属:	

	その他・備考:	
		証明書の申請
(c)	2006 National Research Grid Initiative	NAREGI-CA RA Management.

図 5-3 ユーザ証明書レジストレーション画面

**3** 申請画面が表示されるので、引き続き証明書の発行処理を行う場合は記述されている URL にアクセスします。

NAREGI-CA Certification Authority Server Certification Authority Server
National Research Grid Initiative
NAREGI CA - ユーザ証明書レジストレーション
・申請確認完了
証明書申請が完了しました。 証明書発行処理の手順が記載されたメールを送信済みです。
引き続き証明書の発行処理を行なう場合は、以下のリンクをクリックして Challenge PIN の入力と証明書発行処理を行なってください。
https://domainshiphysicalinewareade/testca_ra/aienroll?Op=Login&ENLoginName=ZNDVP0- 5L7X0G=X0540X=VCMHYR
もしくはUNIX上で証明書発行コマンドを使用する場合。以下のコマンドを実行してくたさい。
☉grid-certreq -sv stewart:testca_ra -new ZNDVP0-5L7X0G-X0540X-VCMHYR -g non -ch
ウィンドウを閉じる
(c) 2006 National Research Grid Initiative NAREGI-CA RA Management

図 5-4 ユーザ証明書申請完了画面

**4** ユーザ認証ページにて、Challenge PIN を入力し「ログイン」ボタンをクリックします。

NARE Gertitos Paratorio National R	EGI-CA Hom Authority Server by AlCrypto Library esearch Grid Initiativ	e	- is splitte	din en
NAREGI CA -	ユーザ証明書発行			
▶ユーザ認証				
電子証明書の発 Challenge PINを	行操作を行います。 こ入力してください。			
Ch	allenge PIN :	•••••		
		ログイン		
	図 5	5-5 ユーザ認証画面	ū	

5 「鍵ペアを生成し電子証明書を発行する」を選択し、「次へ」ボタンをクリックします。



図 5-6 操作選択画面

**6** ユーザ情報入力フォームにて下記項目を設定し「証明書を発行する」ボタンをクリックしま

<b>7</b> o	
設定項目	備考
CSP	証明書のインストール先。Microsoft~Cryptographic
	Provider を選択すると PC のハードディスクにインストール
	します。IC カードにインストールする場合は、対応する
	CSP を選択します。
秘密鍵の長さ	鍵長が長い程安全性が高くなります
秘密鍵のエクスポート	可能に設定すると、Windowsの内部ストアから秘密鍵をエ
	クスポートすることが可能になります。
秘密鍵の保護レベル	「通常」を選択した場合、Windows で秘密鍵を用いる時に
	パスワードの入力を簡略化できます。
	「強力な保護」を選択した場合、秘密鍵を利用する度にパ
	スフレーズの入力が必要となります。

グルーナ 名:	SMIME user
ユーザ情報	12 12
ユーザ 名:	NEC HANAKO
Email :	hana_nec@demo.nec.co.jp
秘密建設	11
CSP:	Microsoft Enhanced Cryptographic Provider v1.0
秘密鍵の 長さ:	○512 bit ④1024 bit ○2048 bit
秘密鍵の エクスボー ト:	●可能 ○不可
秘密鍵の	<ul> <li>● 通常</li> <li>○ 強力な保護</li> </ul>

図 5-7 ユーザ情報入力フォーム画面

**7** 「電子証明書をインストール」ボタンをクリックし、PC もしくは IC カードに証明書をインストー ルします。



図 5-8 電子証明書インストール画面

8 インストールが正常に完了すると、下記の画面が表示されます。



### 図 5-9 電子証明書インストール結果画面