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

目次

1. はじめに

本ドキュメントでは、NAREGI-CA の Challenge PIN/LicenseID 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。

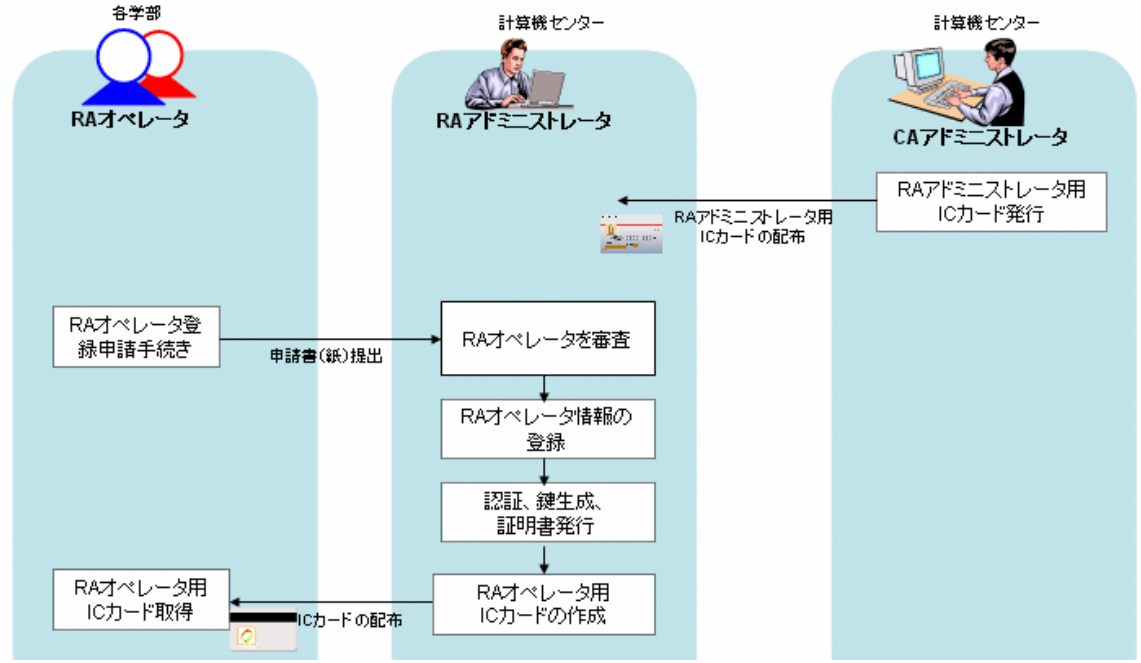


図 1-1 RA オペレータ証明書取得手順(概要)

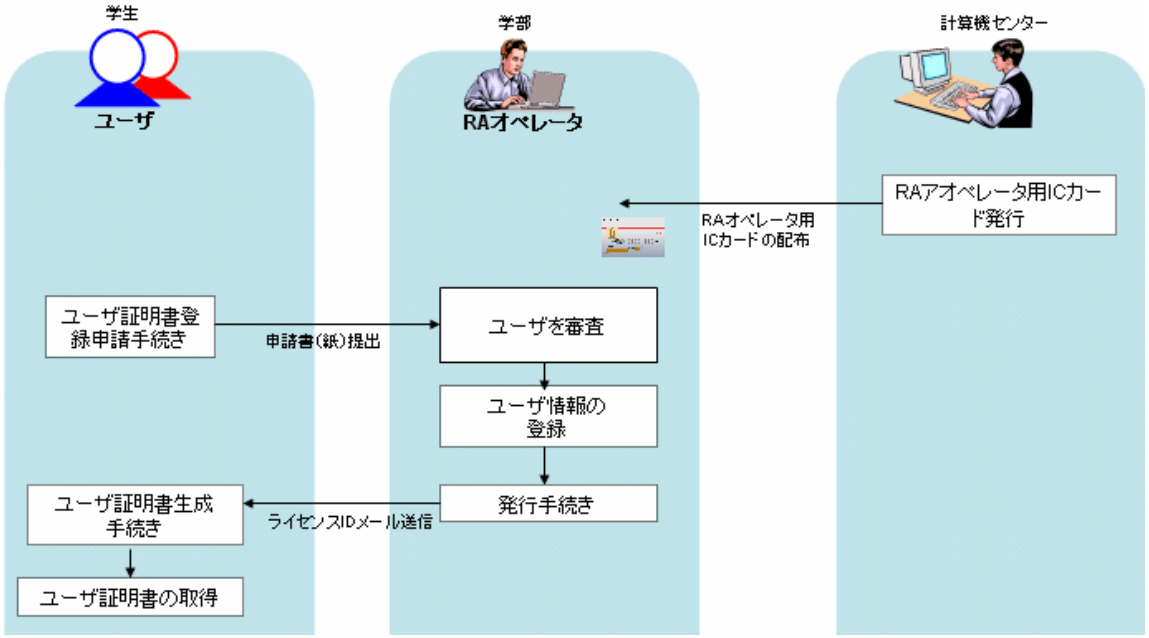


図 1-2 ユーザ証明書取得手順(概要)

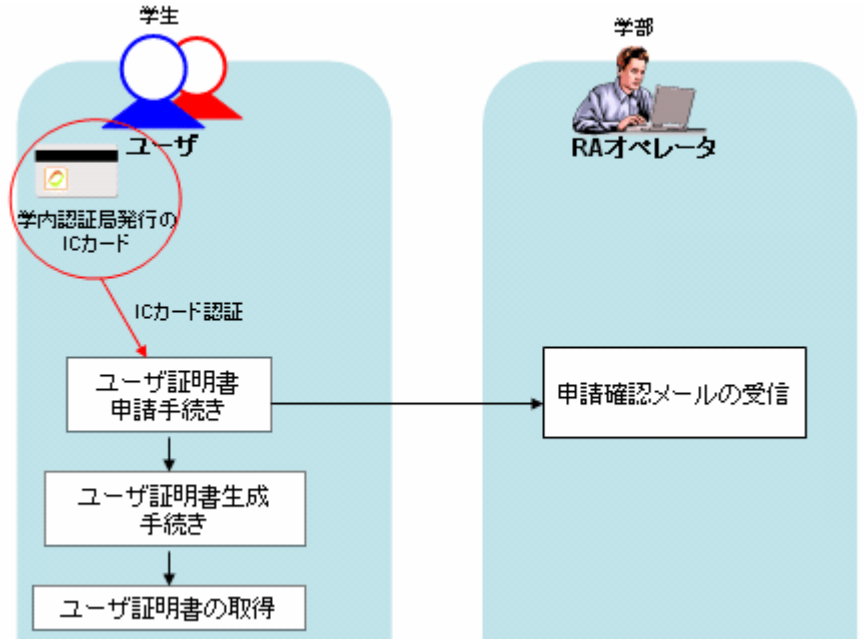


図 1-3 学内認証局から発行された IC カードを利用したユーザ証明書取得手順（概要）

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 [オプション]
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(オフラインのみ):
      -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)
一般オプション:
      -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
oo
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。

それぞれのメニューの内容は以下の通りです。

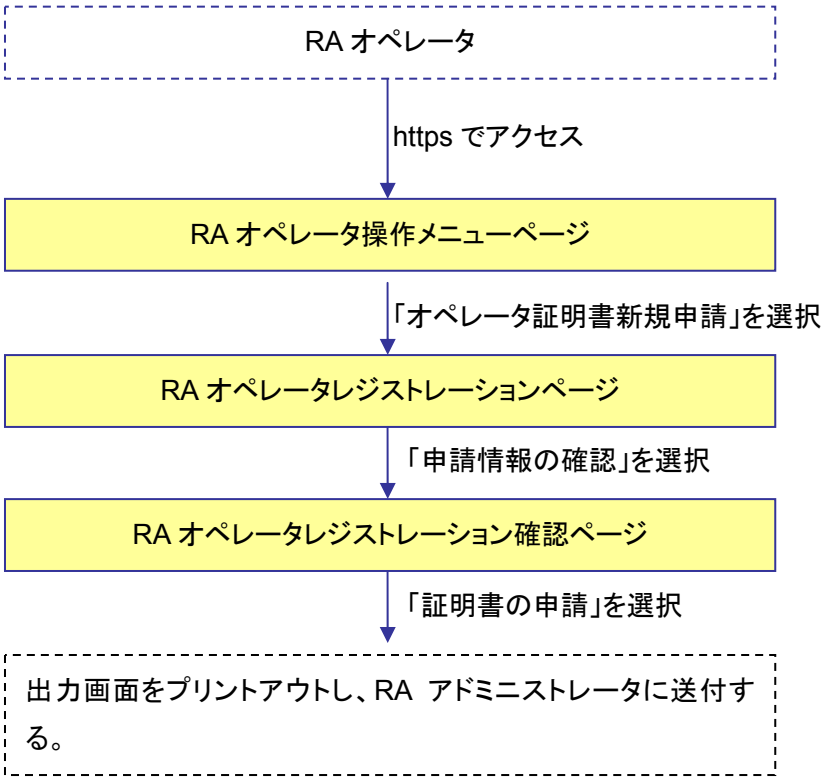
RA アドミニストレータ証明書詳細	RA アドミニストレータ証明書の内容を表示します。
RA アドミニストレータ証明書ダウンロード	RA アドミニストレータ証明書をダウンロードします。秘密鍵はダウンロードできません。
RA CGI 設定表示	RA サーバの CGI 設定を表示します。表示だけであり、修正を行う場合は、RA サーバ上で直接 aica.cnf を編集してください。
CA 証明書詳細	CA 証明書の内容を表示します。
CA 証明書ダウンロード	CA 証明書をダウンロードします。

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 オペレーター一覧	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。

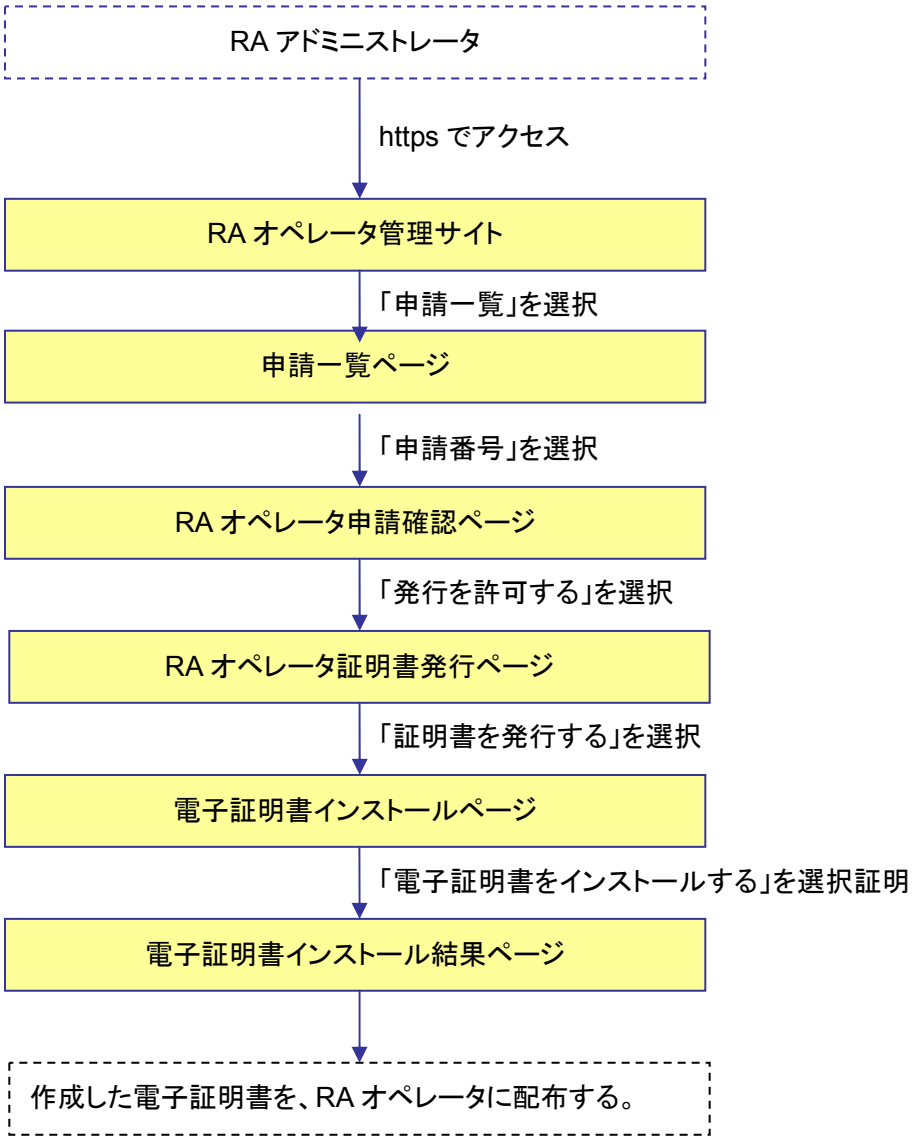
3.2. RA オペレータ証明書発行

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。

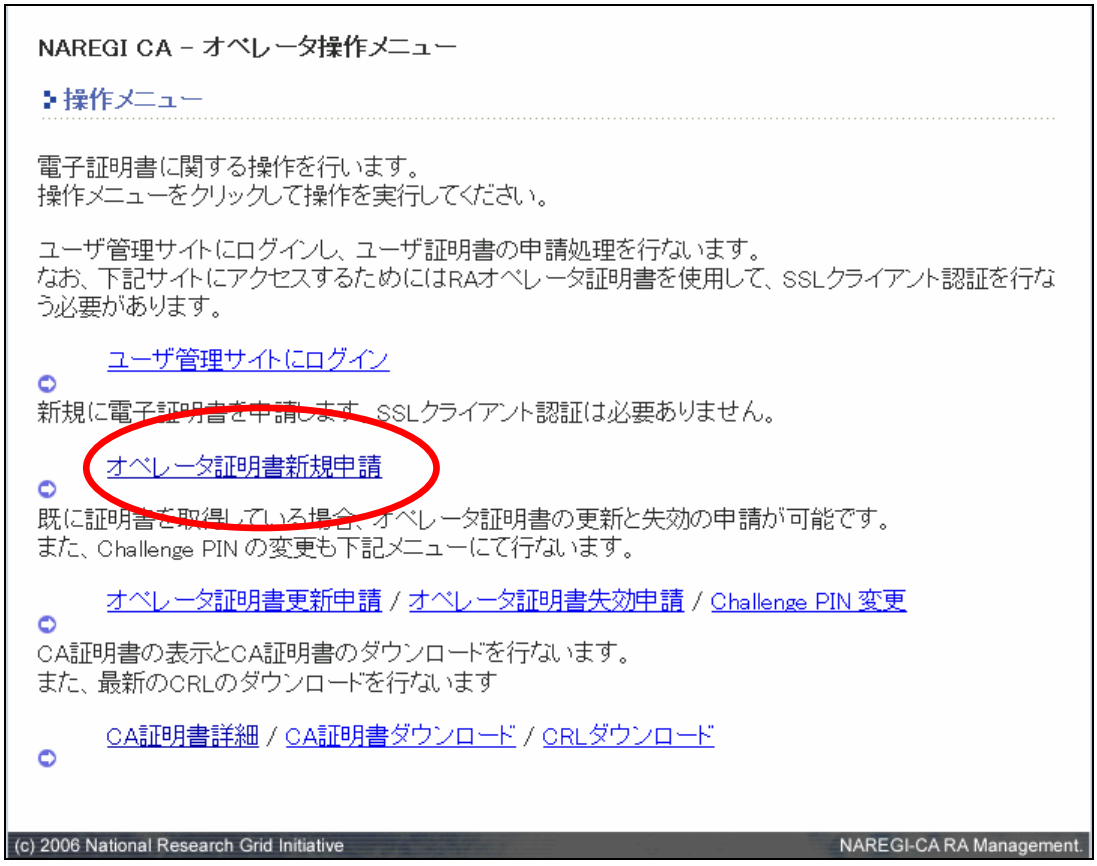


図 3-1 オペレータ操作メニュー画面

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。

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。

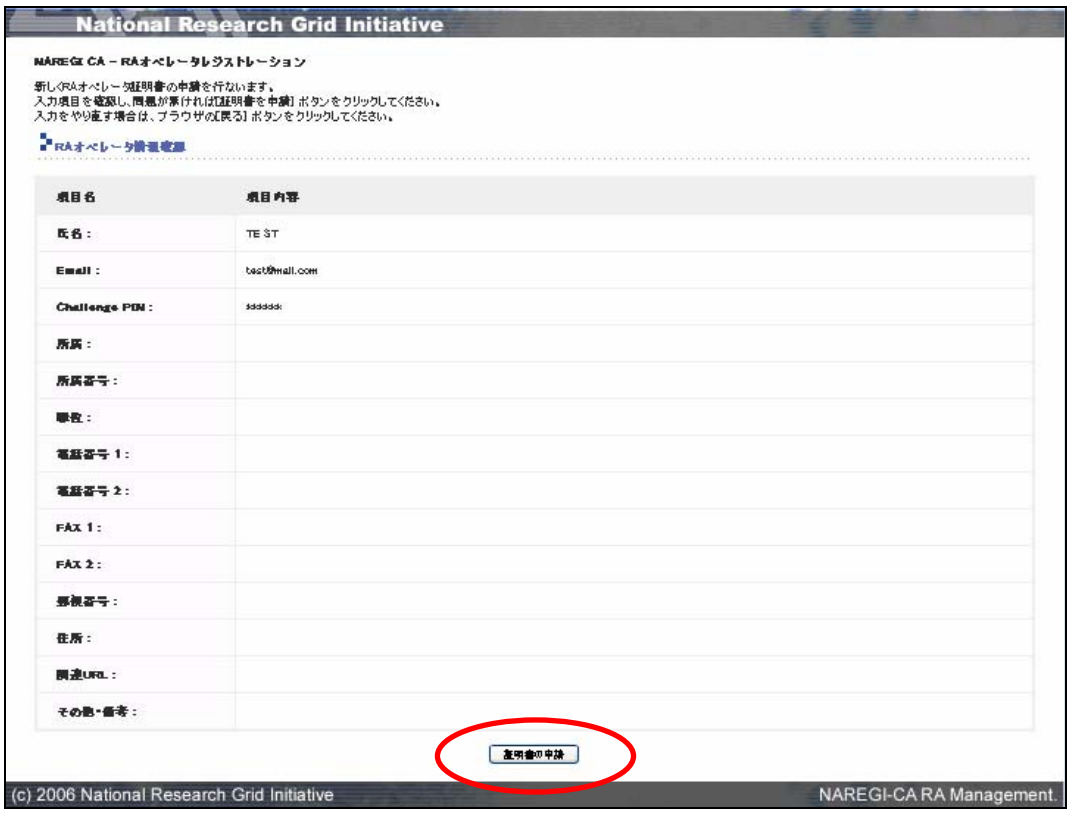


図 3-3 RA レジストレーション確認画面

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。

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。

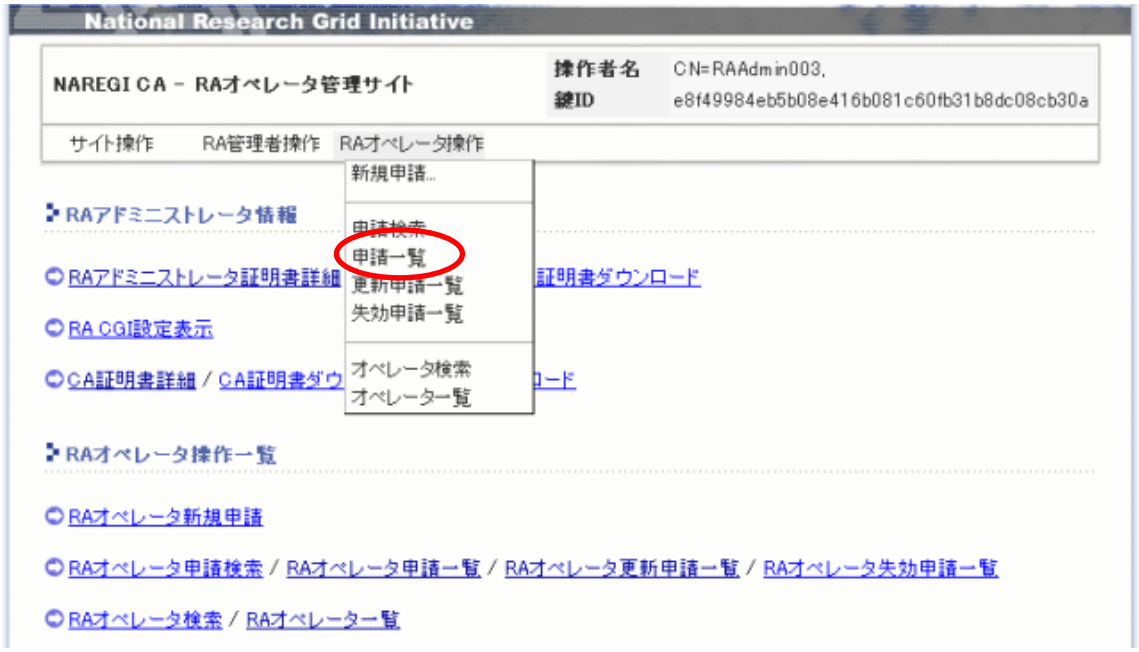


図 3-5 RA オペレータ管理サイト画面

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。

図 3-6 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。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）

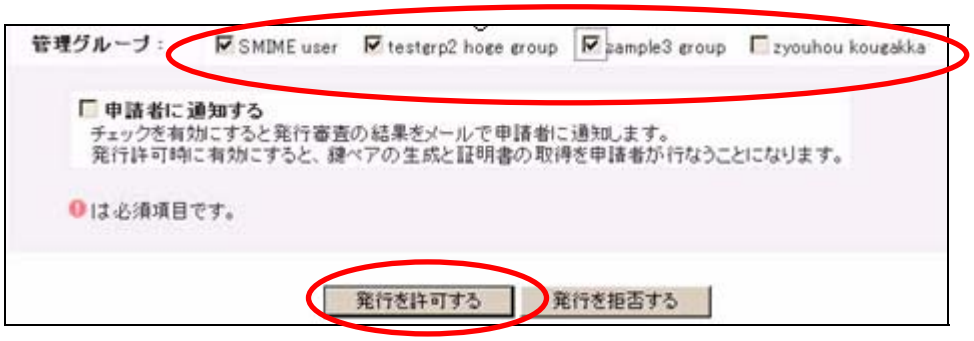


図 3-7 RA オペレータ申請確認画面

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。

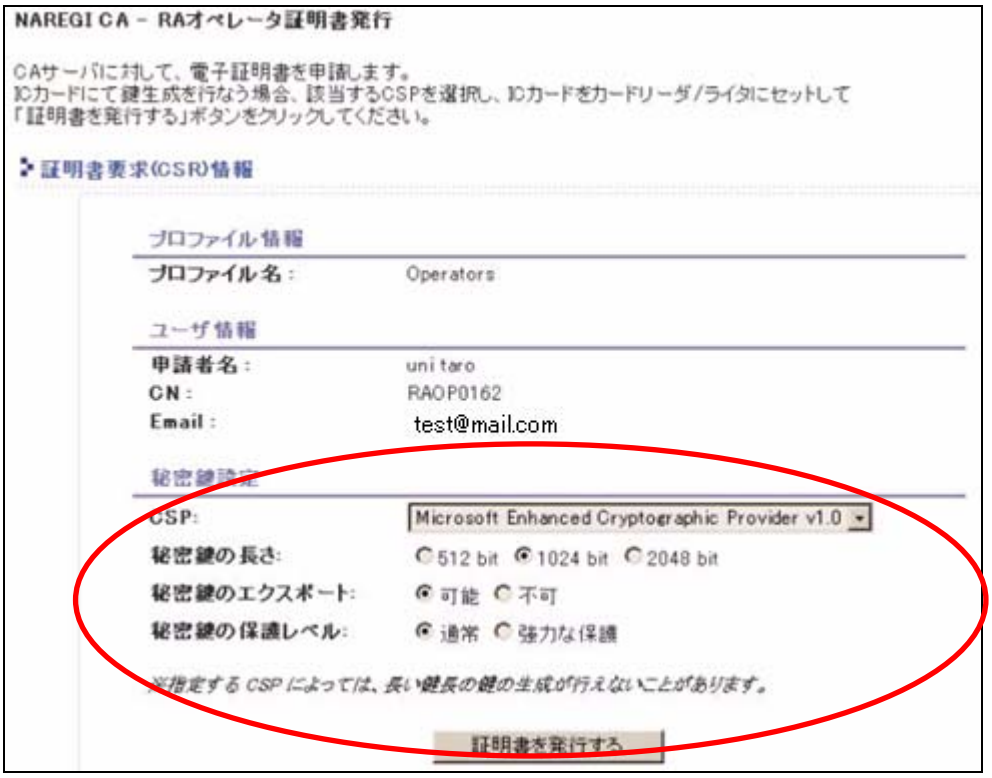


図 3-8 RA オペレータ証明書発行画面

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。

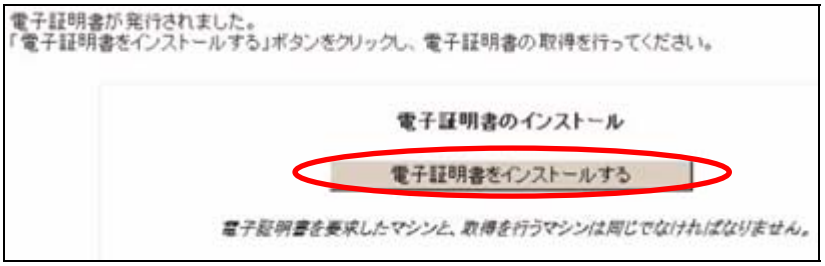


図 3-9 電子証明書インストール画面

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。

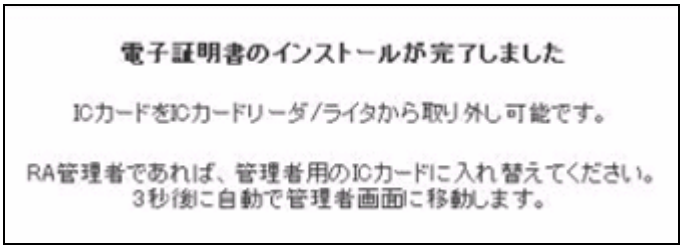
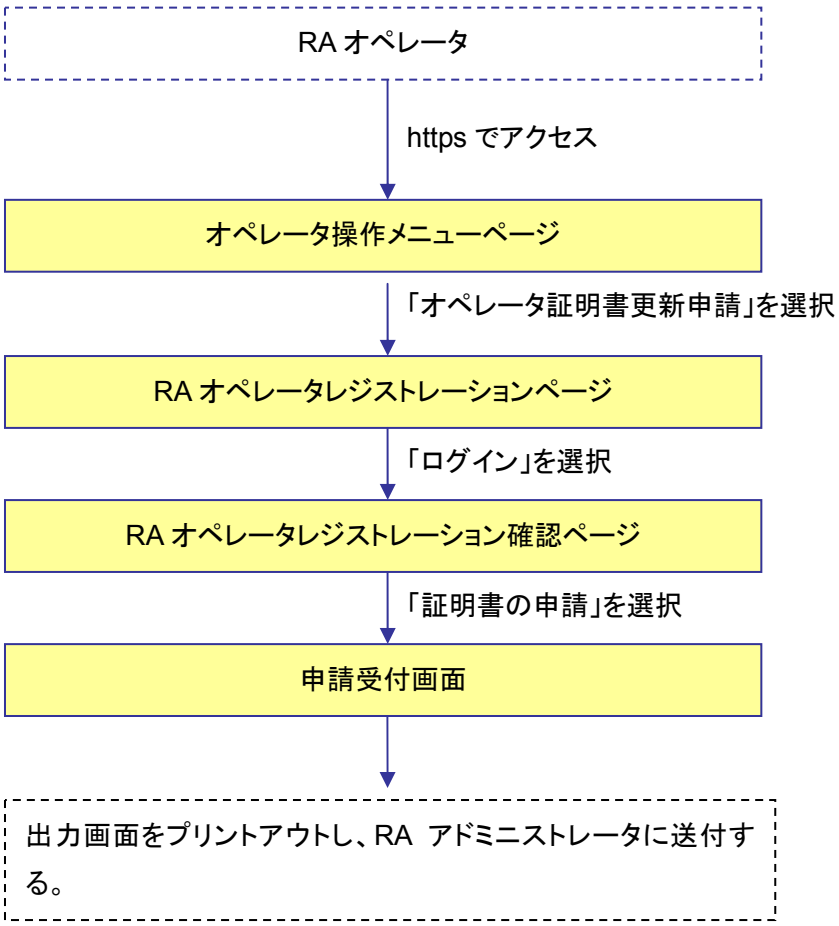


図 3-10 電子証明書インストール結果画面

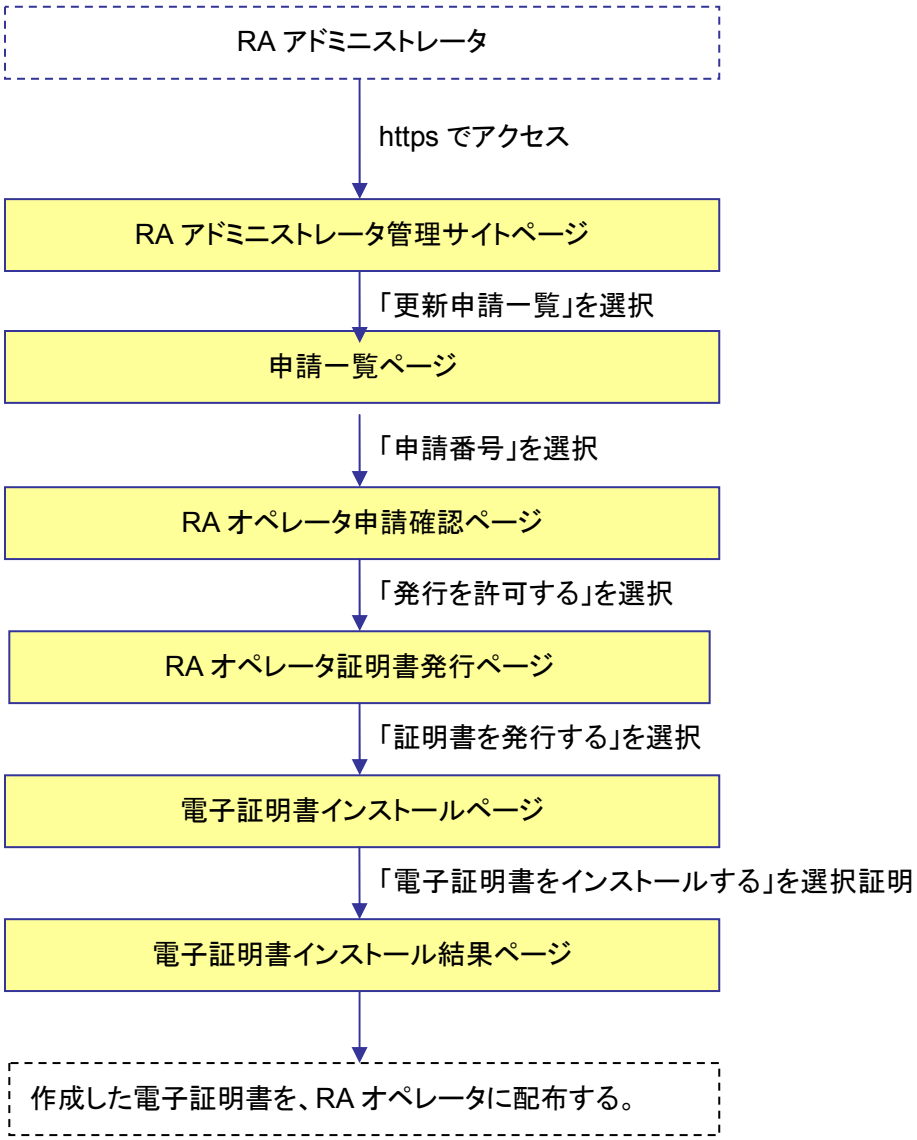
3.3. RA オペレータ更新処理

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

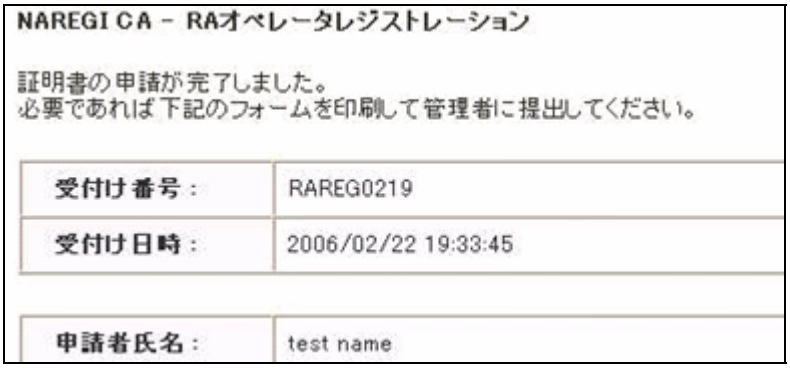
2　ユーザ認証ページで Challenge PIN を入力し、「ログイン」ボタンをクリックします。

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。

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。


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：	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。

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）

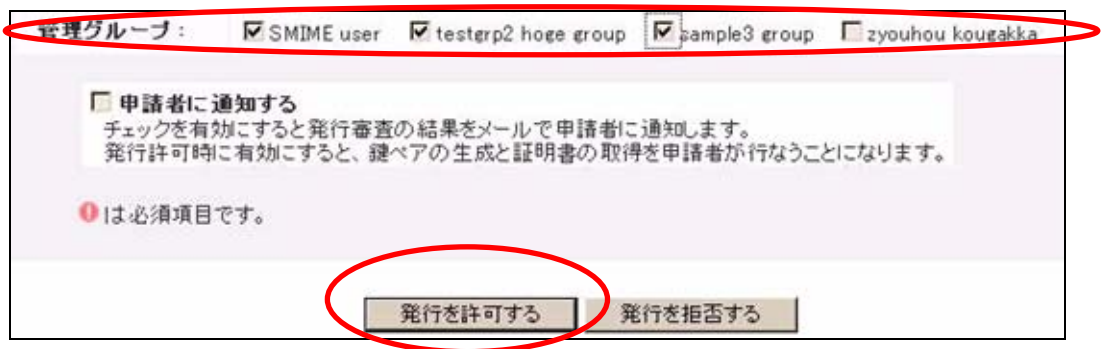


図 3-17 RA オペレータ申請確認画面

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。

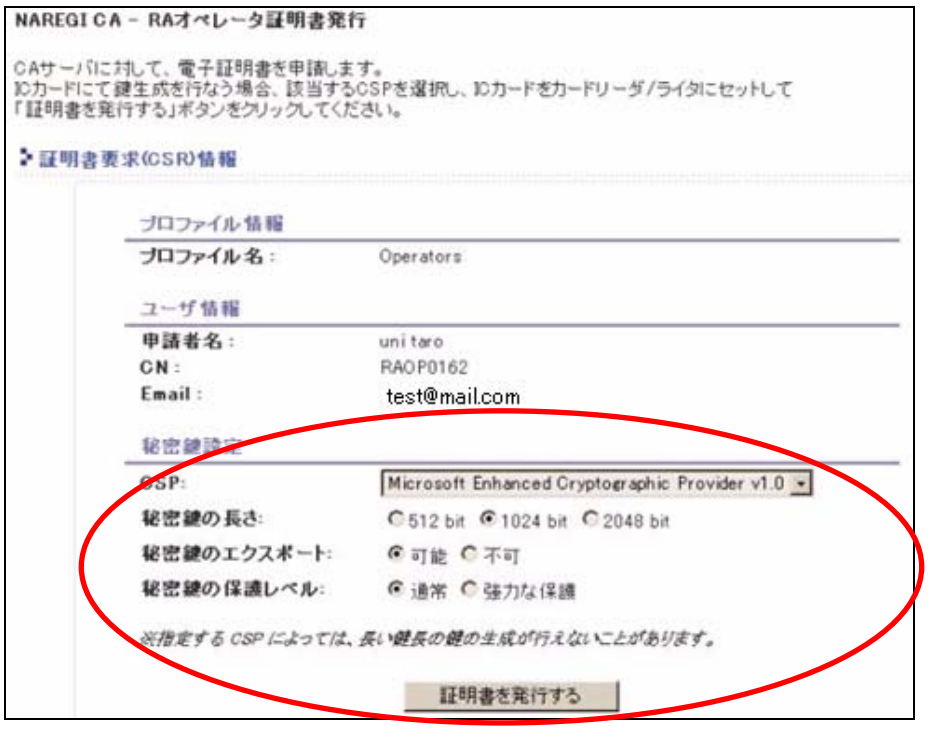


図 3-18 RA オペレータ証明書発行画面

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。

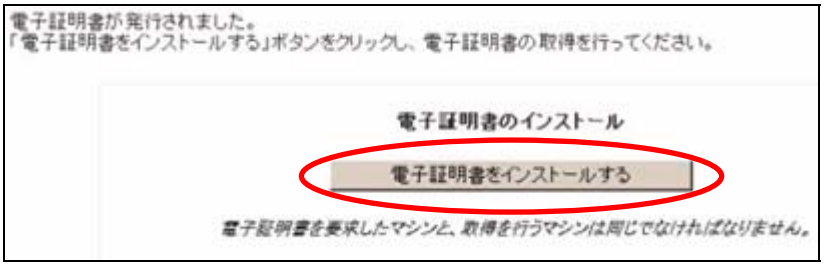


図 3-19 電子証明書インストール画面

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。

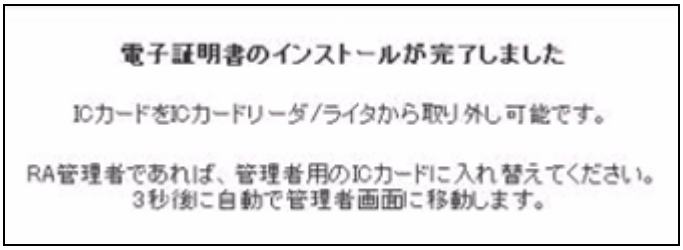
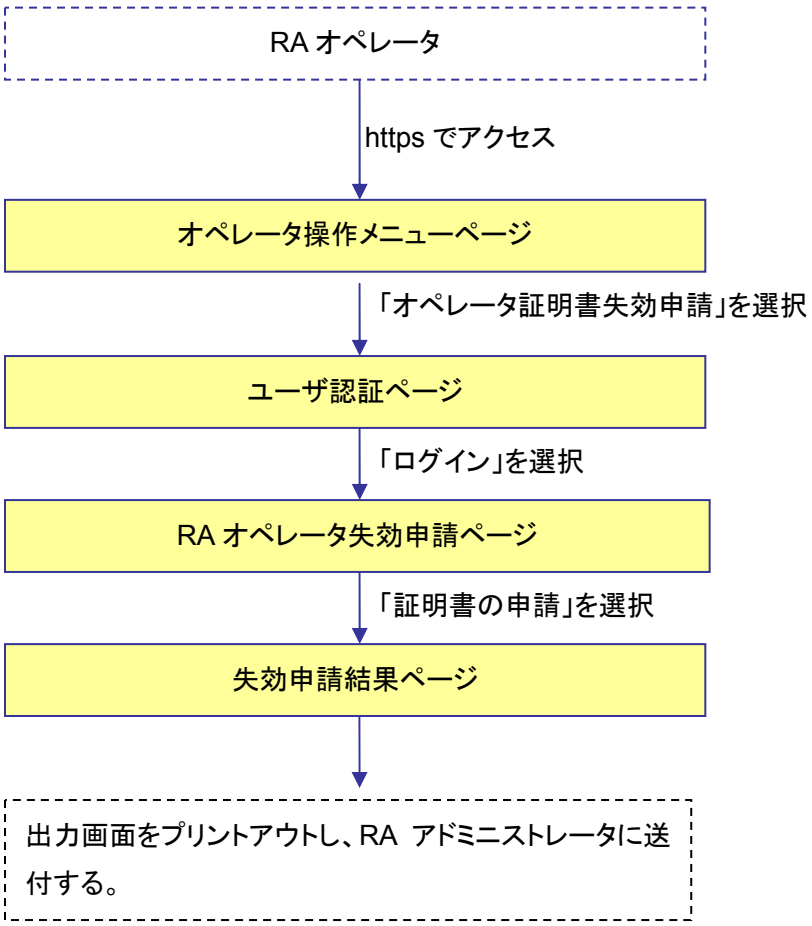


図 3-20 電子証明書インストール結果画面

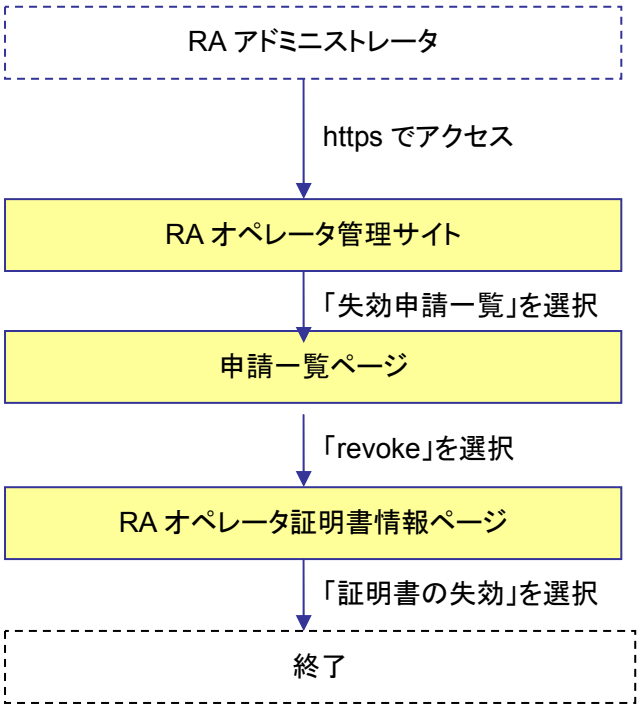
3.4. RA オペレータ失効処理

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。

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。

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。

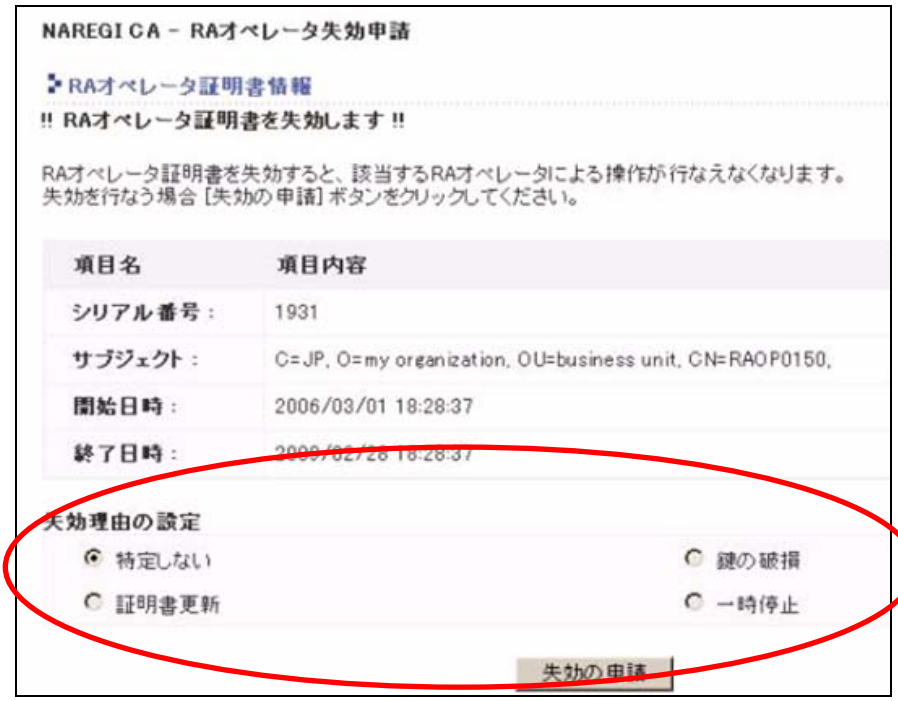


図 3-23 RA オペレータ失効申請画面

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。

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。

図 3-25 RA オペレータ管理サイト画面

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。

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。

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。

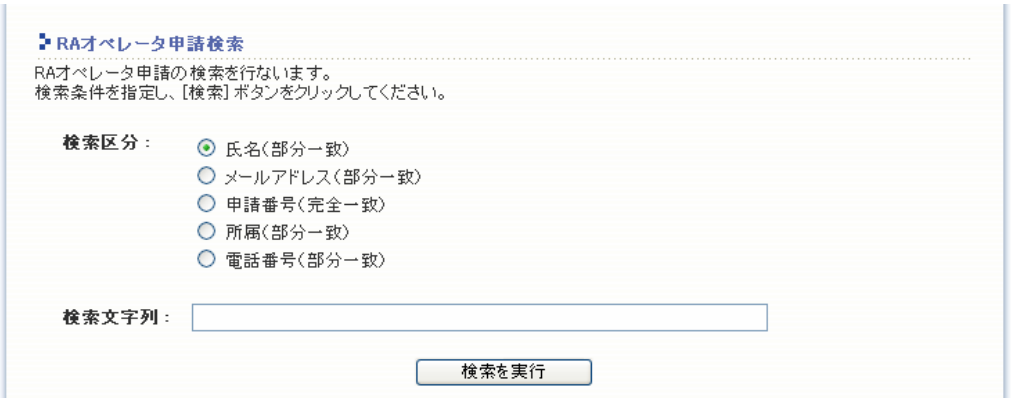


図 3-28 RA オペレータ申請検索画面

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。

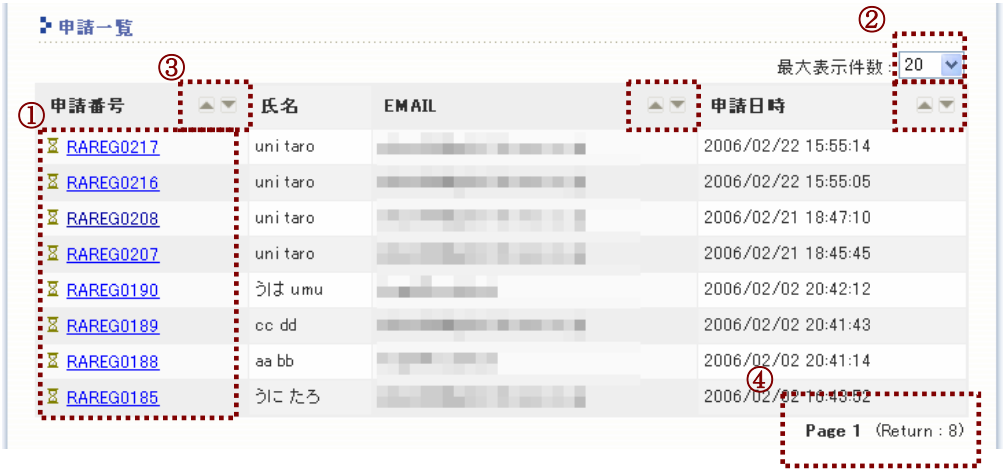


図 3-29 RA オペレータ申請リスト画面

① 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。

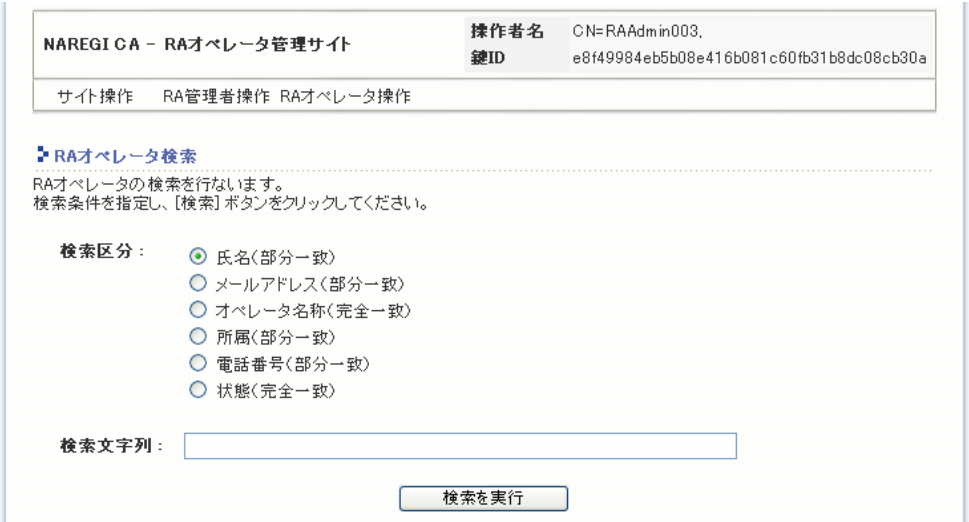


図 3-30 RA オペレータ検索画面

検索項目はそれぞれ以下の通りです。

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@
オペレータ名称	オペレータ名称(属性型 CN)の完全一致の値を指定します。 例. RAOP0011
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
状態	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。 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。

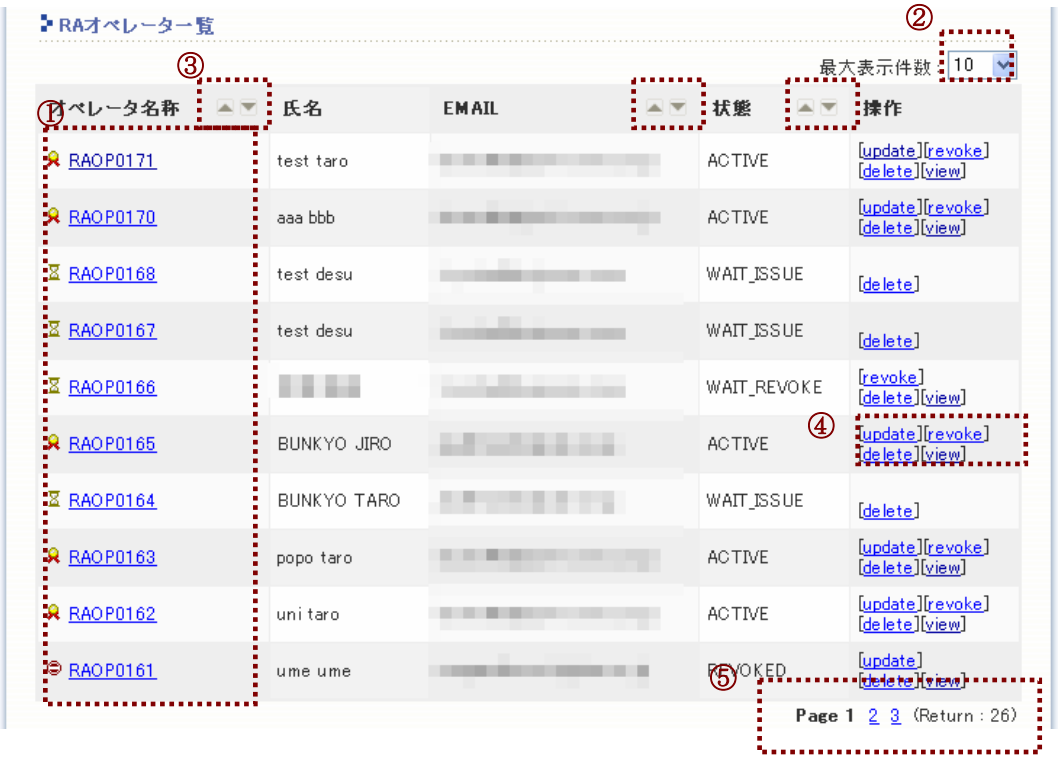


図 3-31 RA オペレータリスト画面

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。

update	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。
revoke	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。
delete	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。

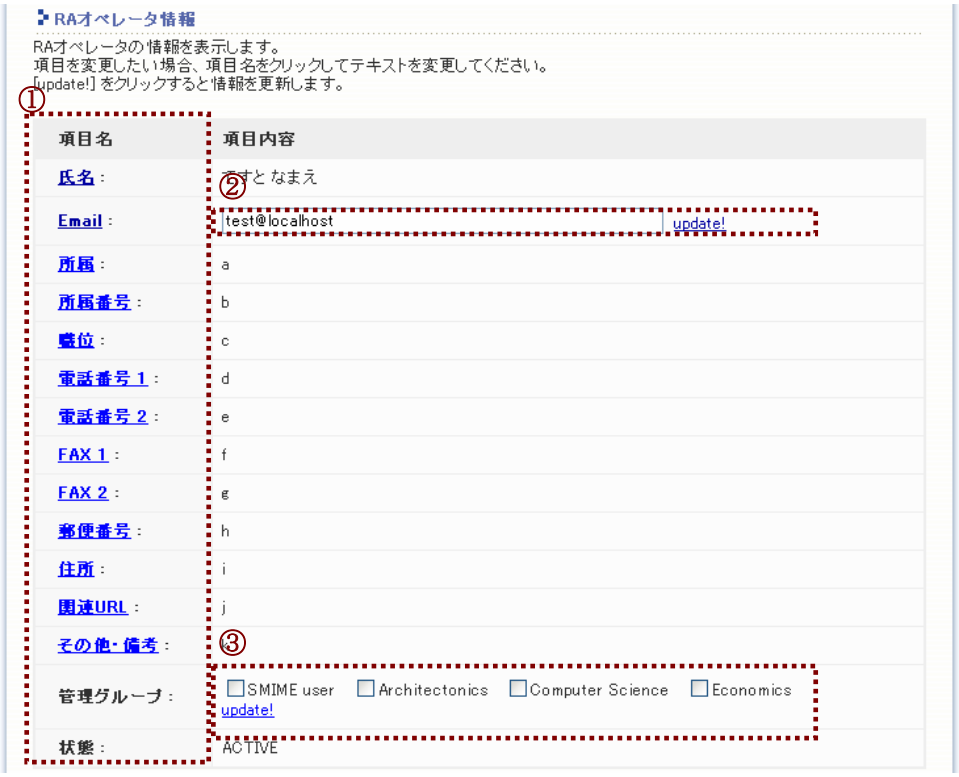


図 3-32 RA オペレータ情報画面

① 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。

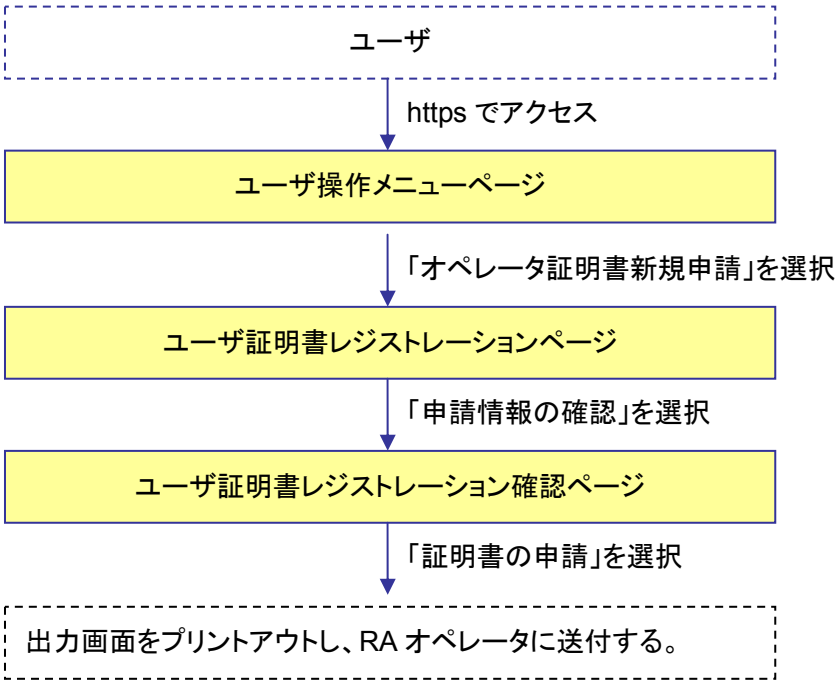
それぞれのメニューの内容は以下の通りです。

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 オペレータ証明書ダウンロード	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。

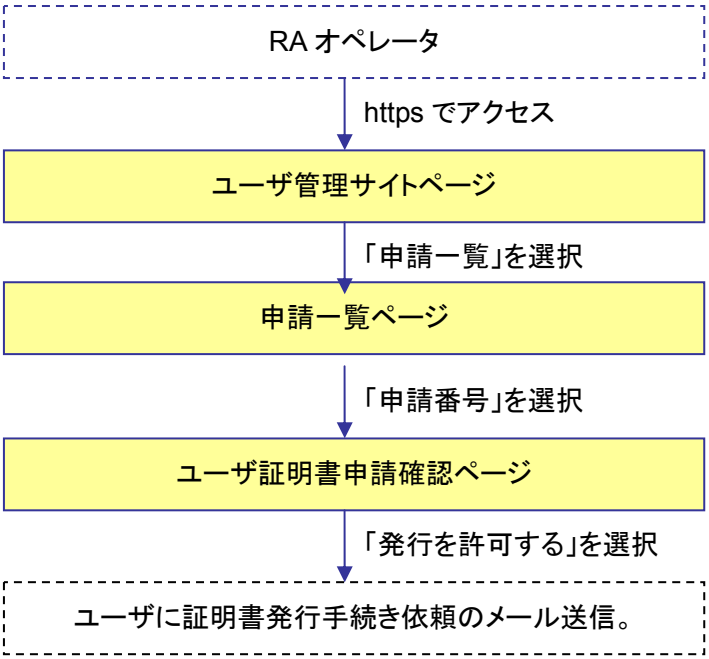
RA オペレータ証明書失効	RA オペレータ証明書の失効申請を行います。
CA 証明書詳細	CA 証明書の内容を表示します。
CA 証明書ダウンロード	CA 証明書をダウンロードします。
CRL ダウンロード	最新の CRL をダウンロードします。
ユーザ証明書新規申請	ユーザ証明書を新規に申請します。 申請ページを新たに開きます。
証明書申請検索	指定の「操作グループ」を対象とする、ユーザ証明書の申請を検索します。
証明書申請一覧	指定の「操作グループ」を対象とする、ユーザ証明書の申請の一覧を表示します。
証明書更新申請一覧	指定の「操作グループ」を対象とする、ユーザ証明書の更新申請の一覧を表示します。
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

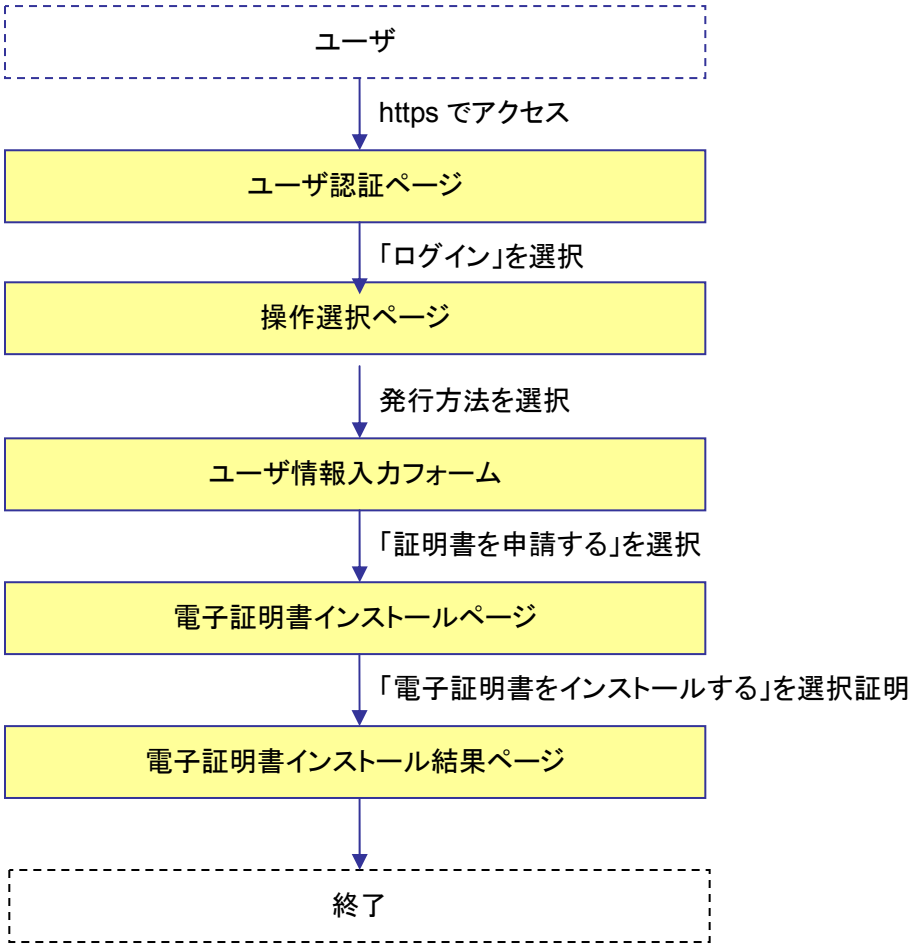
ユーザ　処理の流れ　―証明書の申請―



RA オペレータ　処理の流れ



ユーザ　処理の流れ　ー証明書の取得ー



4.2.1. ユーザ —証明書申請—

1 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。

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。

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。


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：　REG000257

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。

--
NAREGI CA WEB Enroll サービス

図 4-4 確認メール内容

4.2.2. 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、「証明書申請一覧」を選択します。

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。

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）。

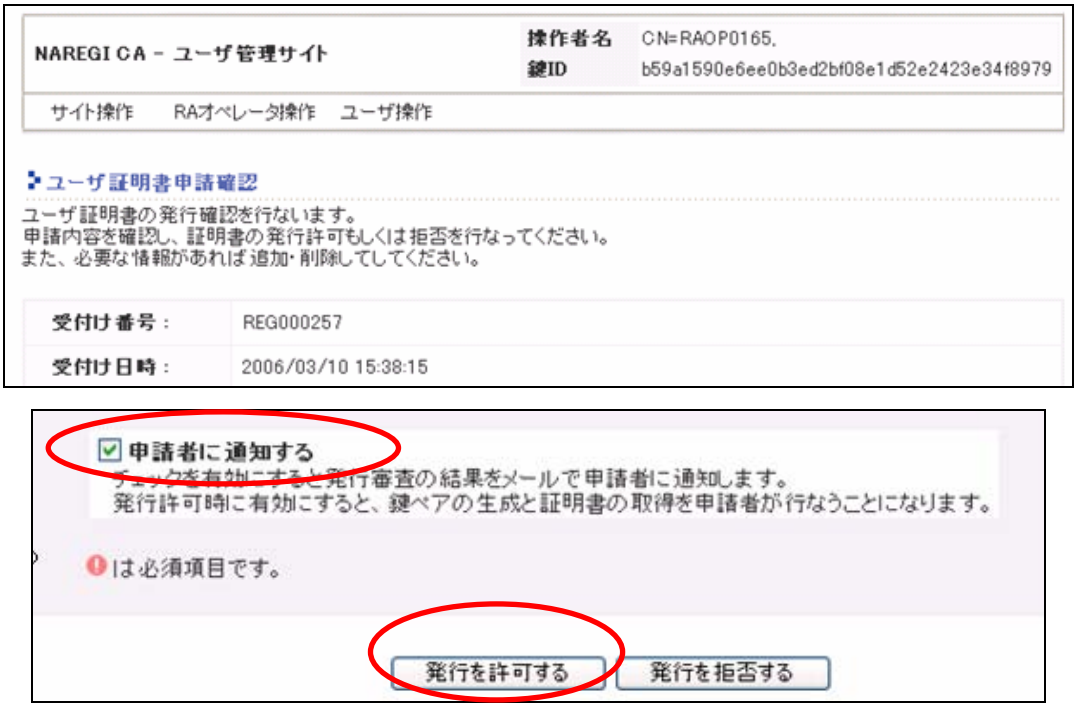
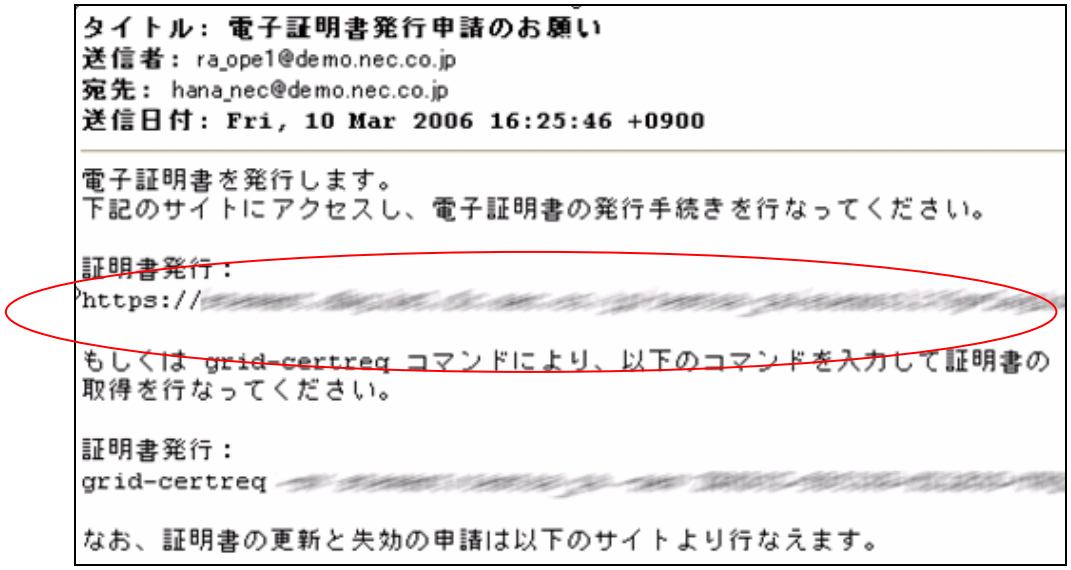


図 4-7 ユーザ証明書申請確認画面

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：
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-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。

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。

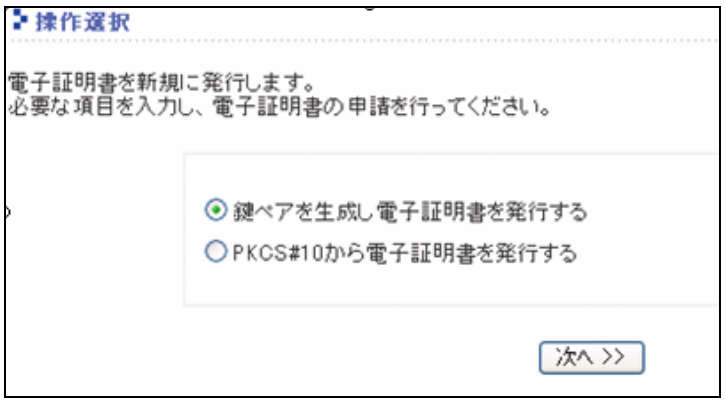


図 4-10 操作選択画面

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。

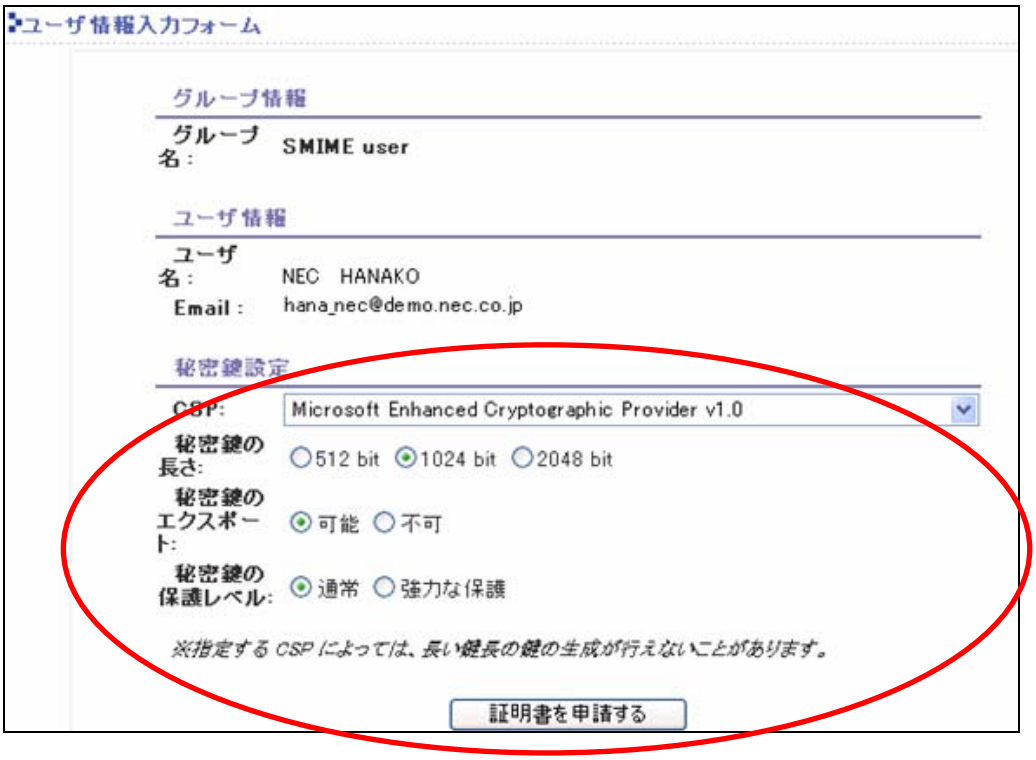


図 4-11 ユーザ情報入力フォーム画面

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。

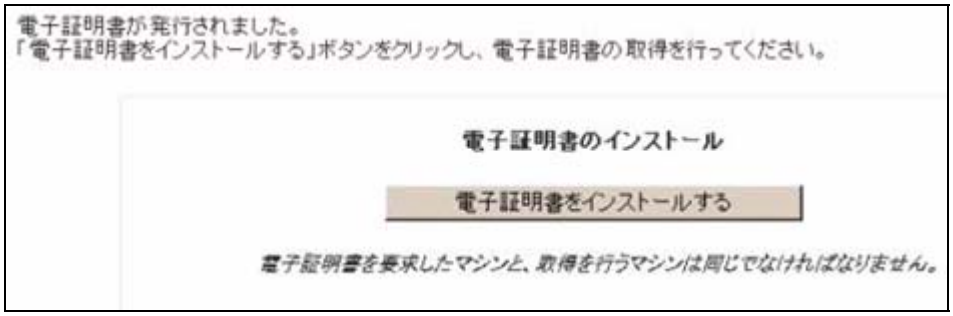


図 4-12 電子証明書インストール画面

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。

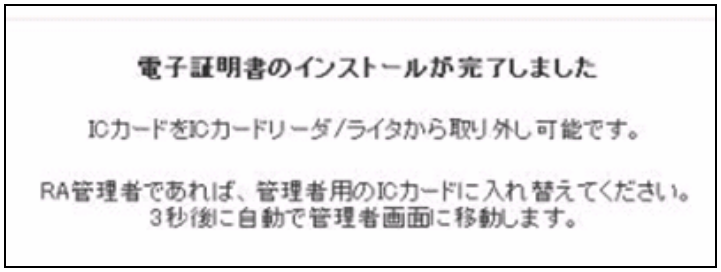
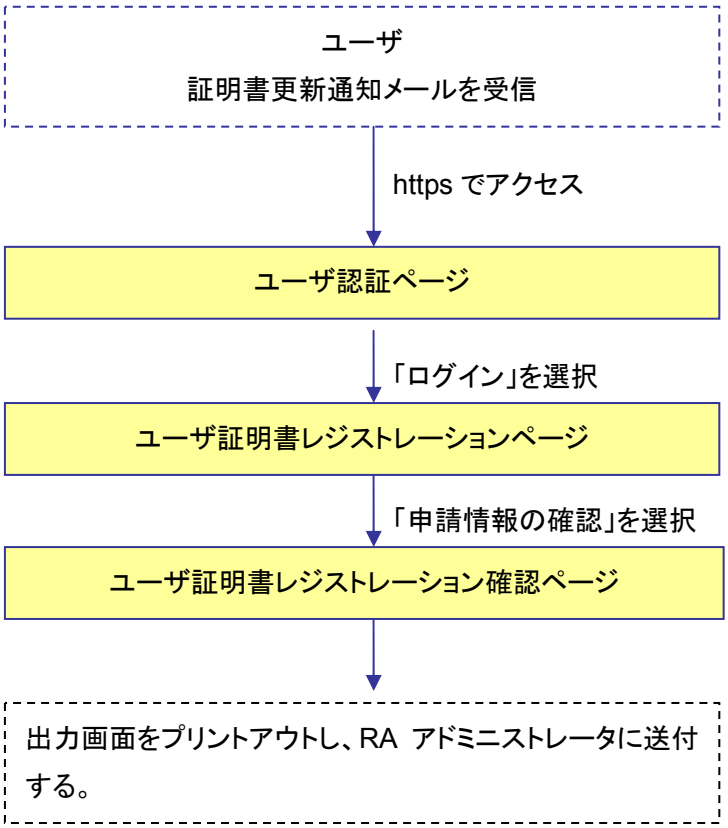


図 4-13 電子証明書インストール結果画面

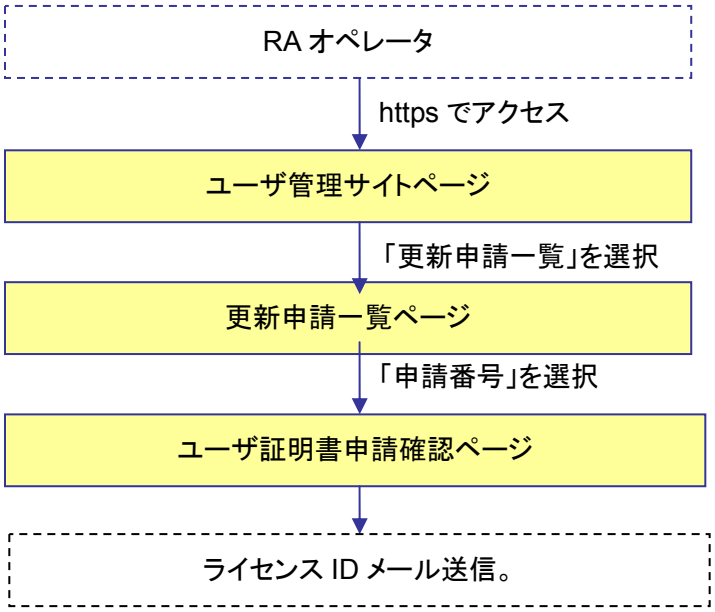
4.3. ユーザ証明書更新

ユーザ証明書の更新処理は以下の手順で行います。

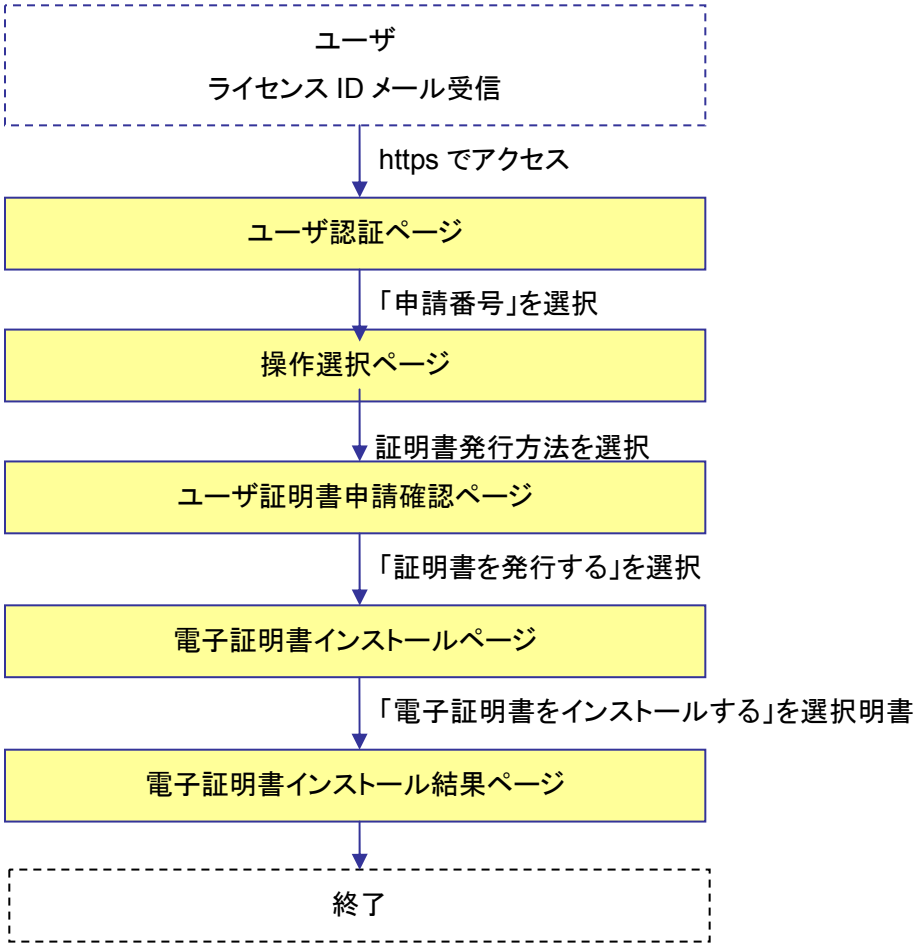
ユーザ　処理の流れ



RA オペレータ　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。

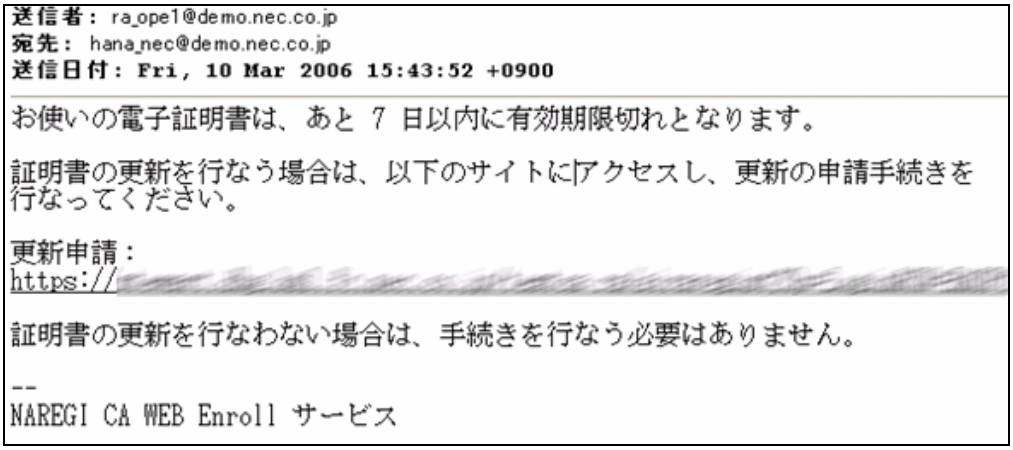


図 4-14 証明書更新通知メール

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。

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。

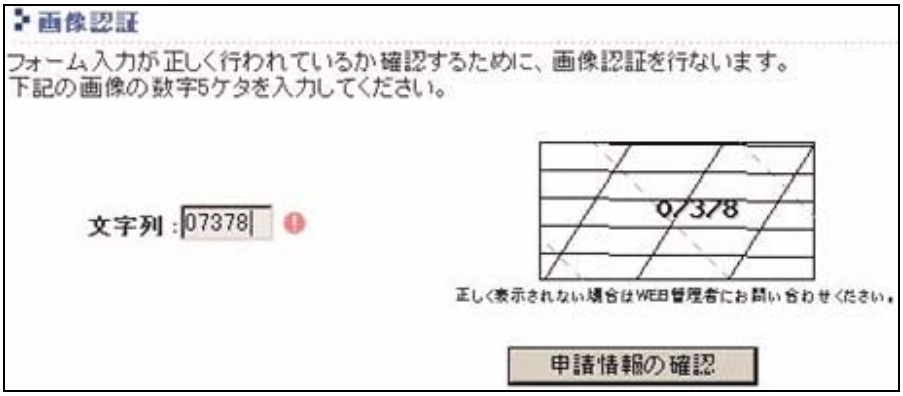


図 4-16 ユーザ証明書レジストレーション画面

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。

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 4-17 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_ope1@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、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。

--
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。

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。

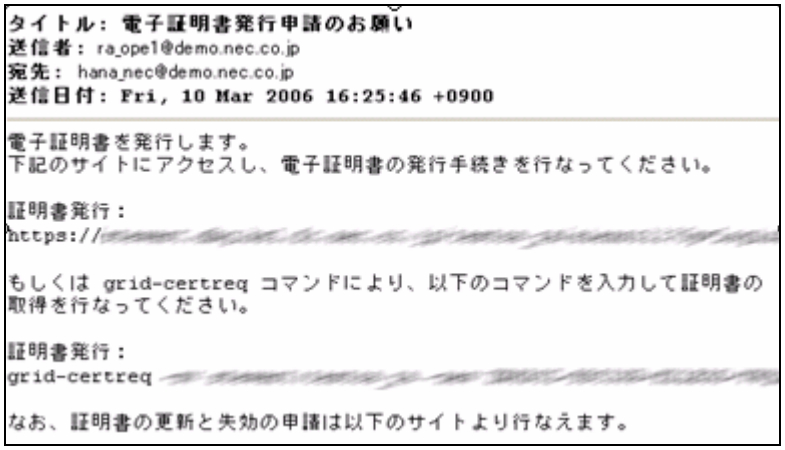
図 4-20 更新申請一覧画面

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）。

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-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 4-22 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。

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。

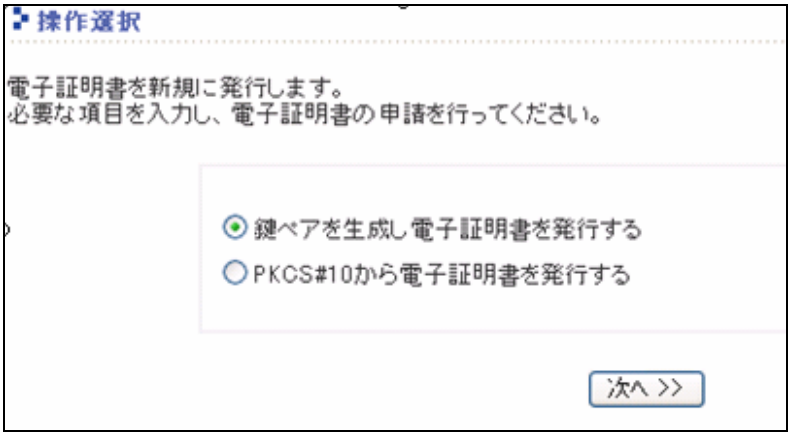


図 4-24 操作選択画面

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。

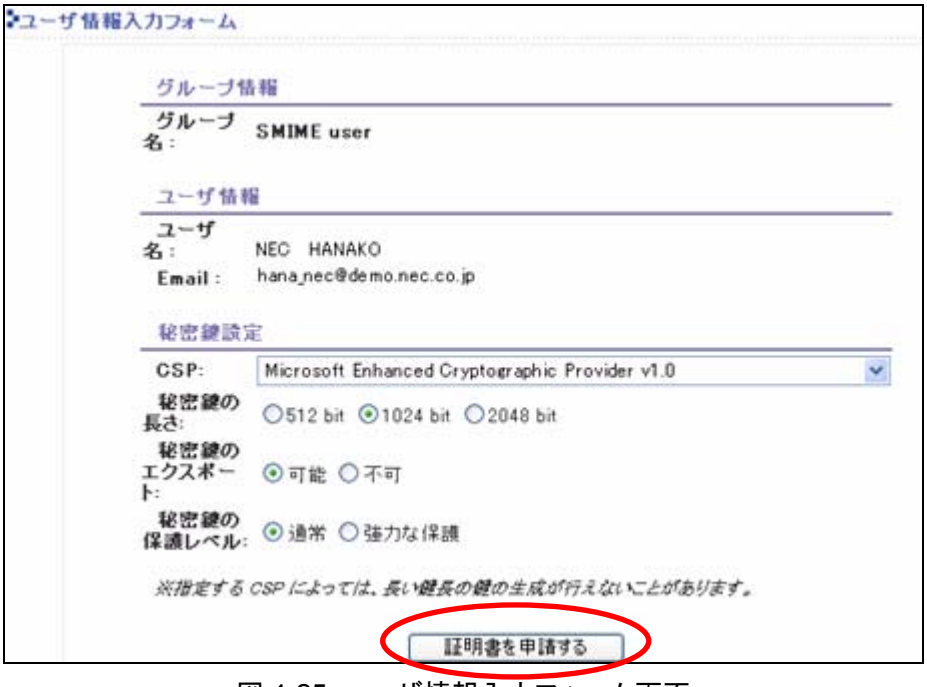


図 4-25 ユーザ情報入力フォーム画面

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。

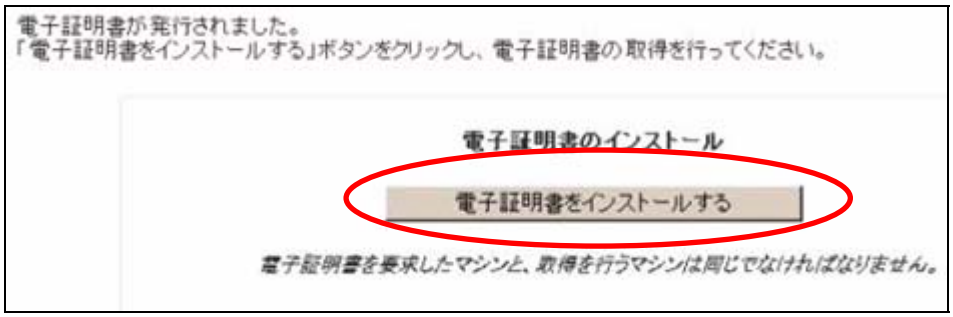


図 4-26 電子証明書インストール画面

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。

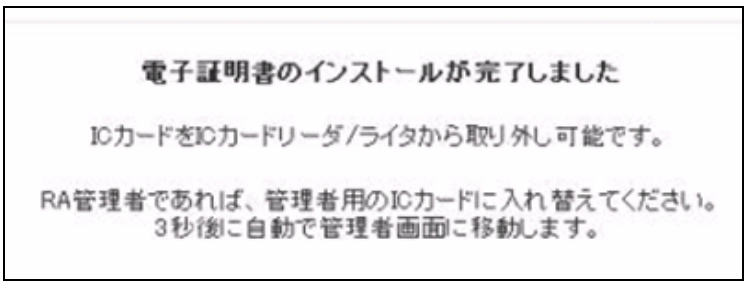
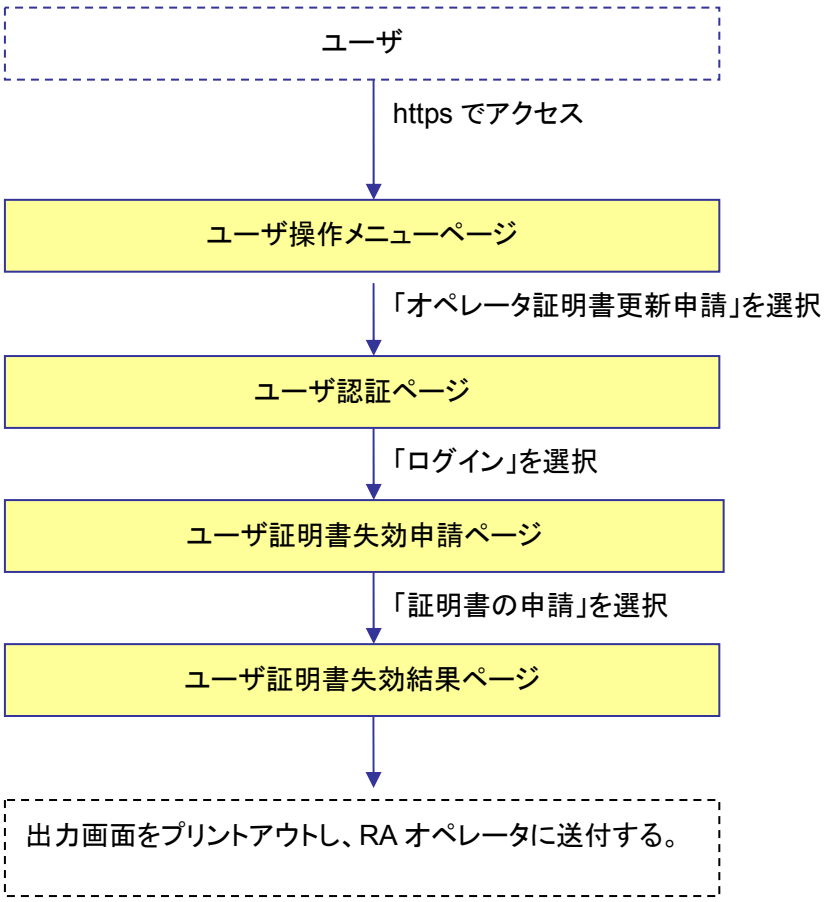


図 4-27 電子証明書インストール結果画面

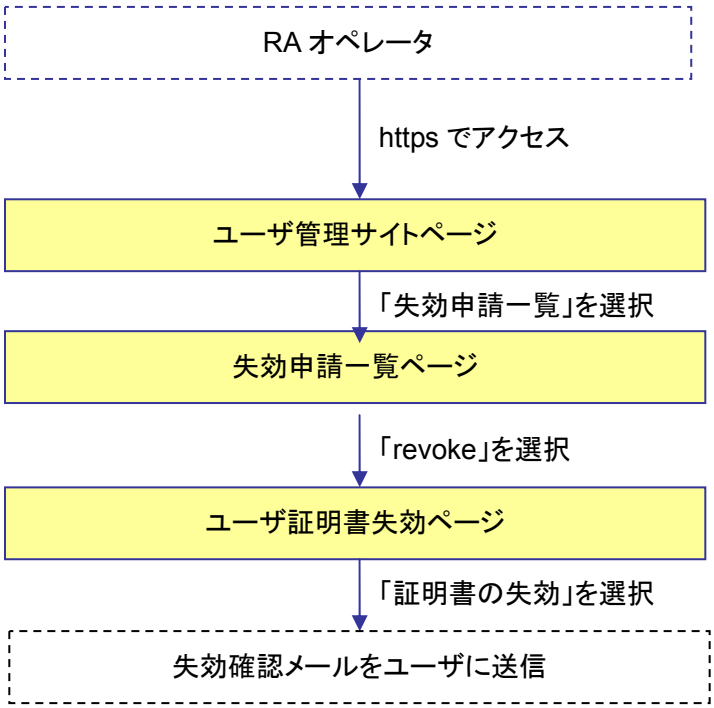
4.4. ユーザ証明書失効

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



RA オペレータ　処理の流れ



4.4.1. ユーザ ―失効申請―

1 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。

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。

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。

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。

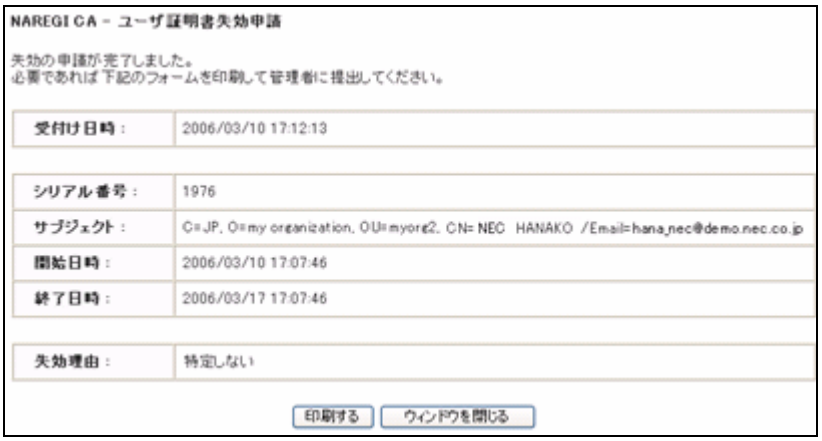


図 4-31 失効確認結果画面

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。

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。

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。

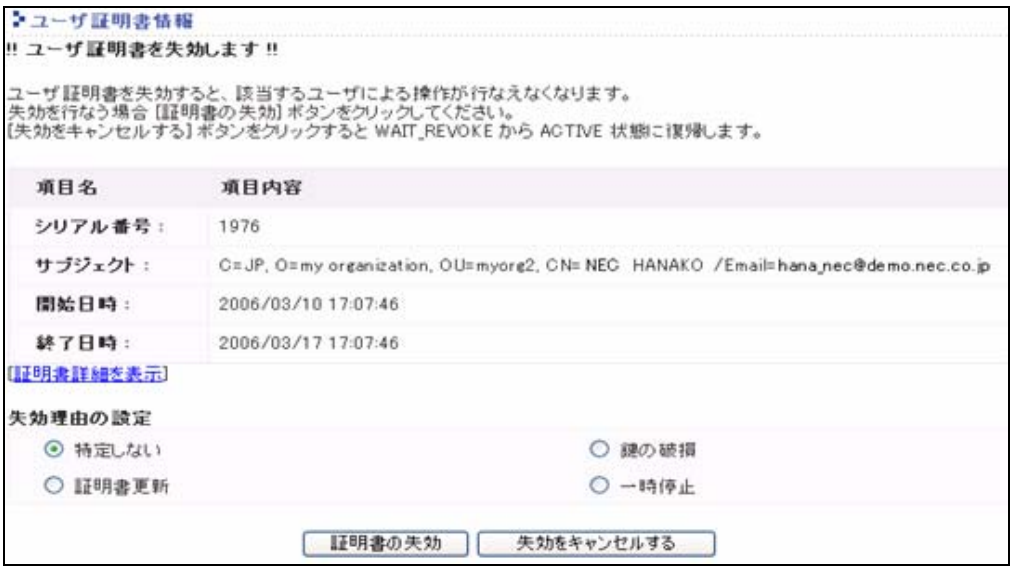


図 4-34 ユーザ証明書失効画面

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。

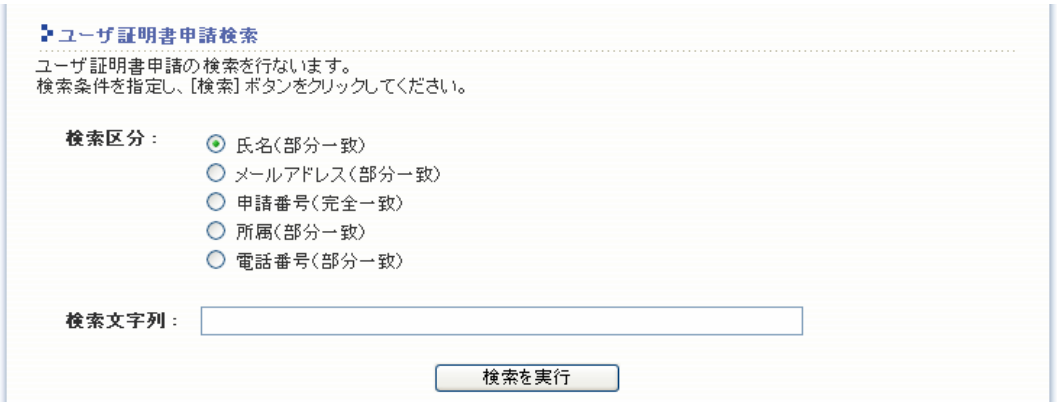


図 4-36 RA オペレータ申請検索画面

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。

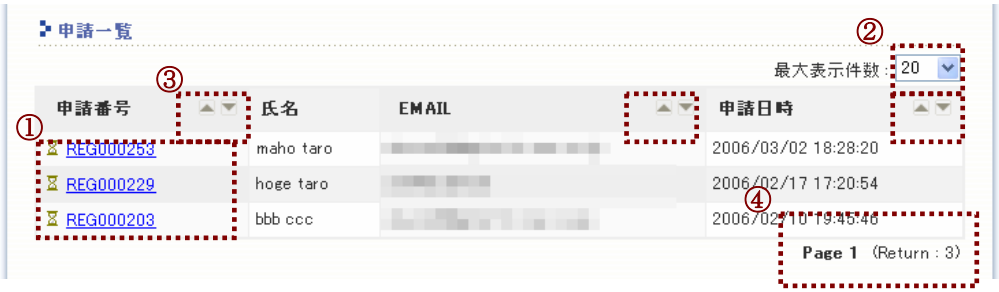


図 4-37 ユーザ証明書申請リスト画面

① 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。

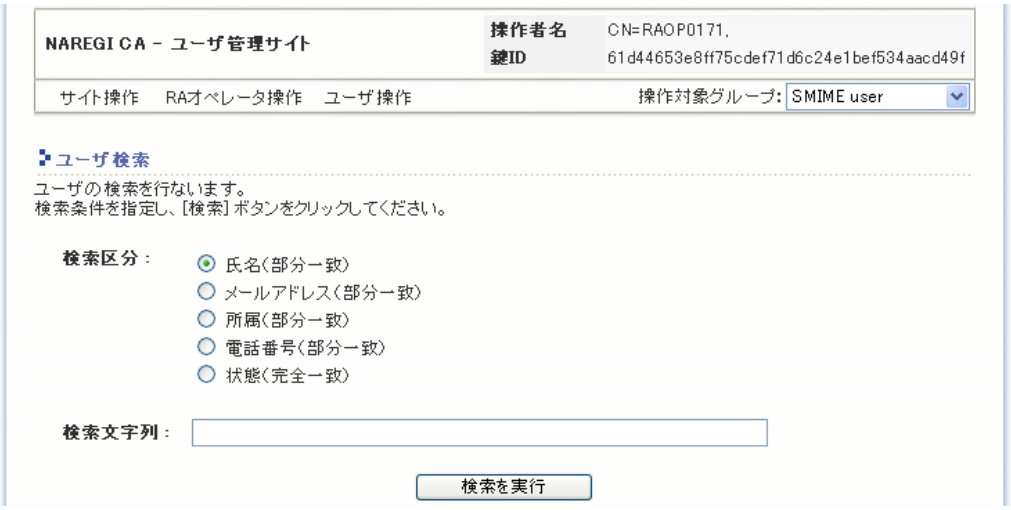


図 4-38 ユーザ検索画面

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@
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
状態	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。 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。

図 4-39 ユーザリスト画面

① 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。

update	証明書の更新を行うメニューです。ユーザからの申請がなくても、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。
revoke	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、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。

図 4-40　RA オペレータ情報画面

① 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。

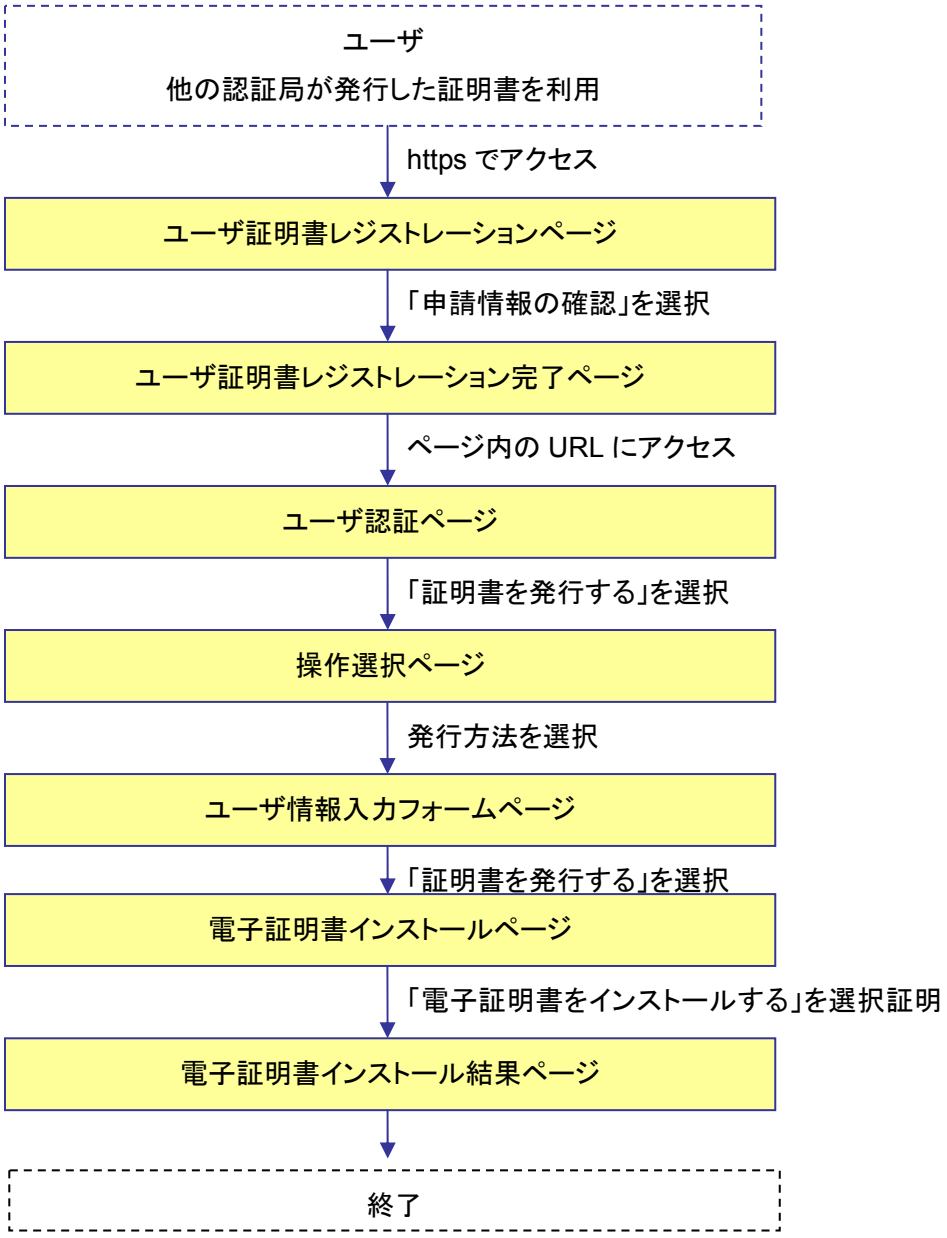
② ユーザ情報の項目内容です。編集可能な状態で「update!」をクリックすると該当するLDAP エントリの属性値を更新します。

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　―証明書の申請―



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。

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。

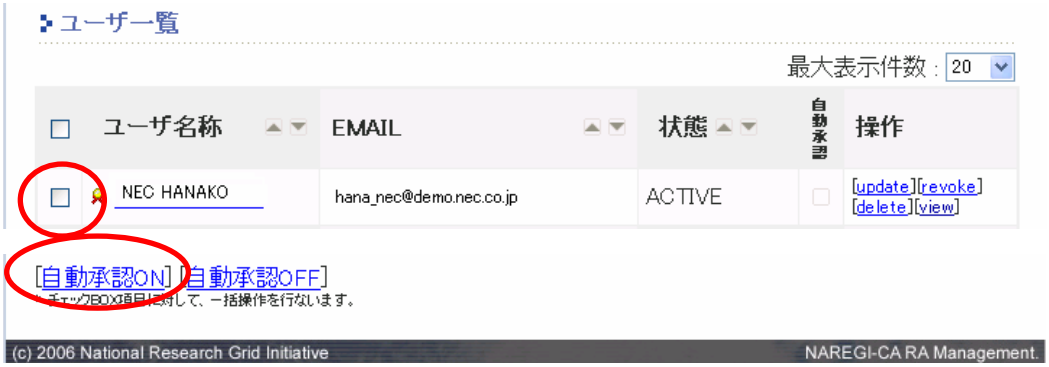


図 5-2 ユーザー覧画面

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）。

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。

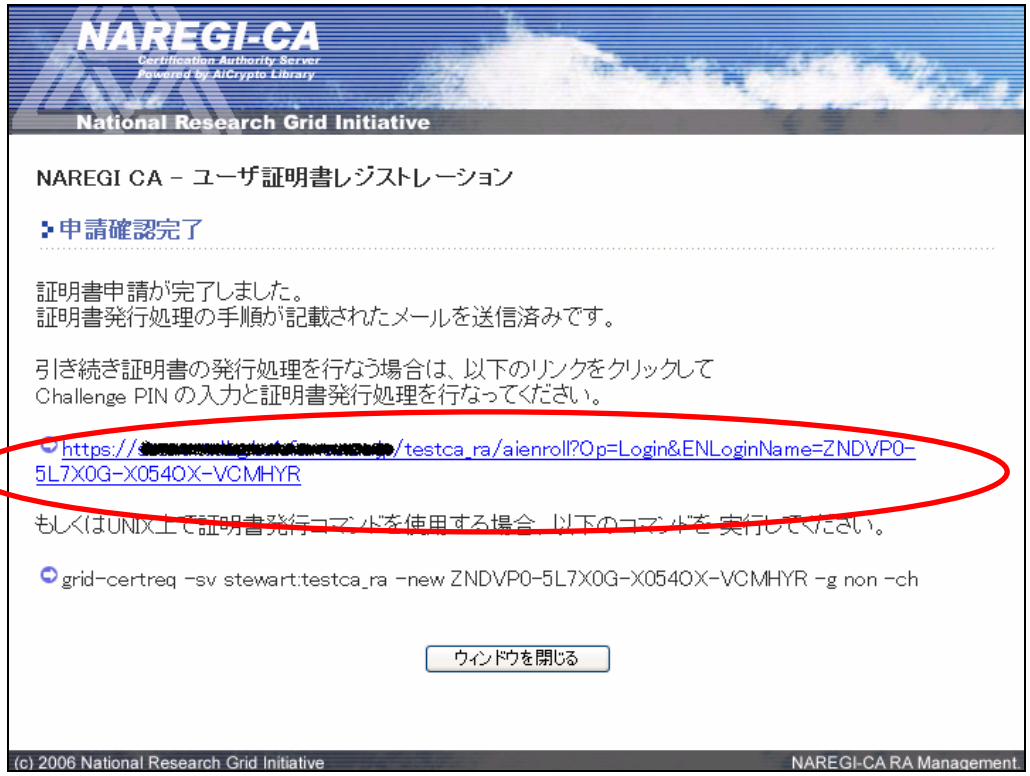


図 5-4 ユーザ証明書申請完了画面

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。

図 5-5 ユーザ認証画面

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。

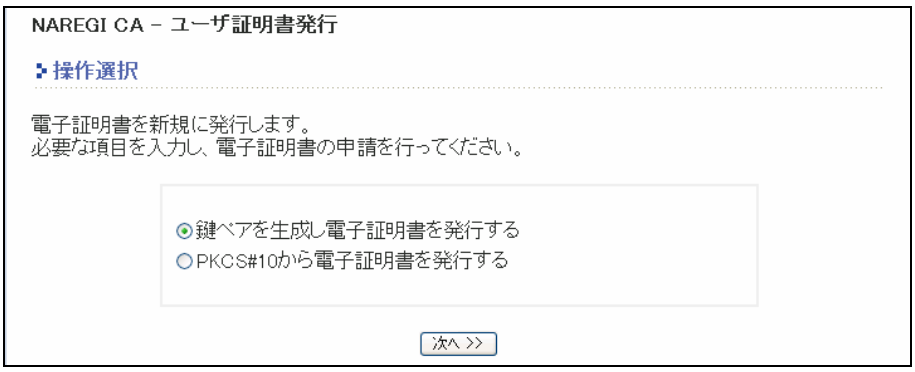


図 5-6 操作選択画面

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。

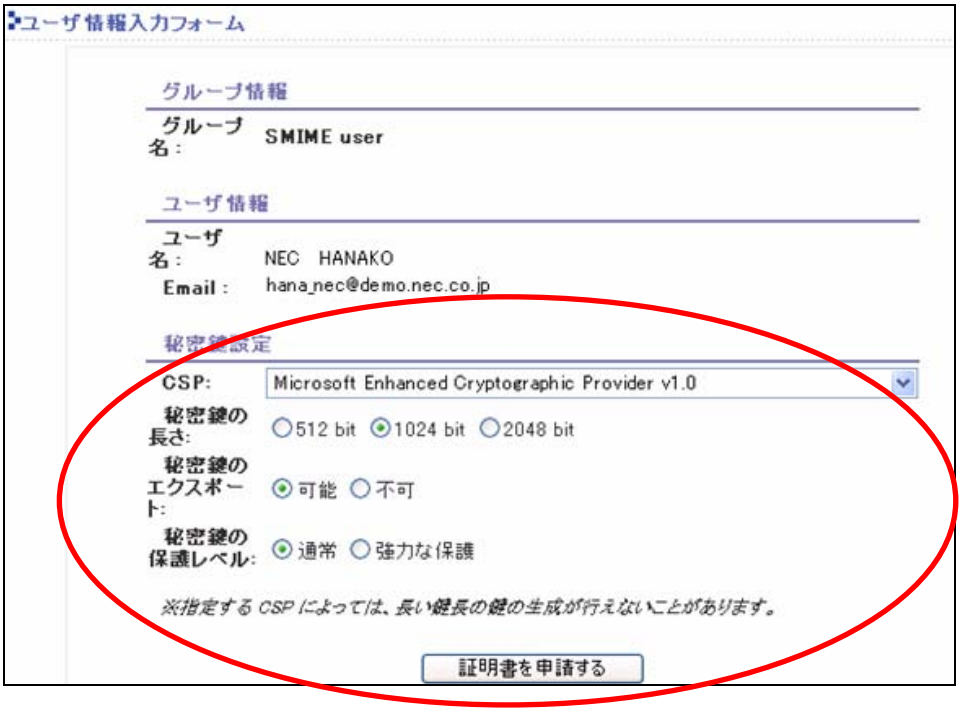


図 5-7 ユーザ情報入力フォーム画面

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。

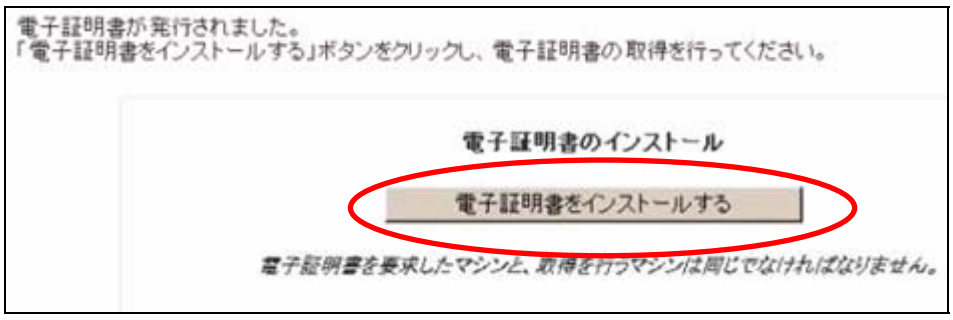


図 5-8 電子証明書インストール画面

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。

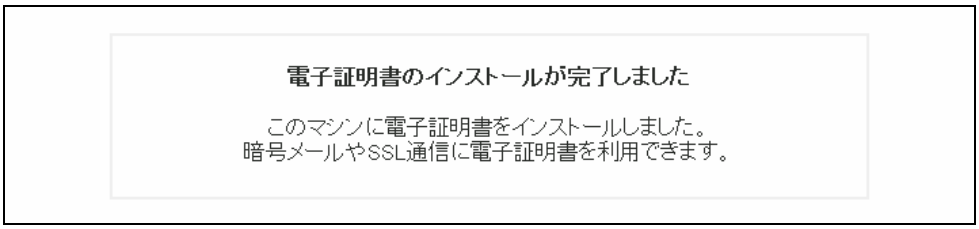


図 5-9 電子証明書インストール結果画面