

<<システム正常系>>

- ・ 証明書発行管理システムに関するRAA固有の設定情報はRAAconfファイルに記述される。

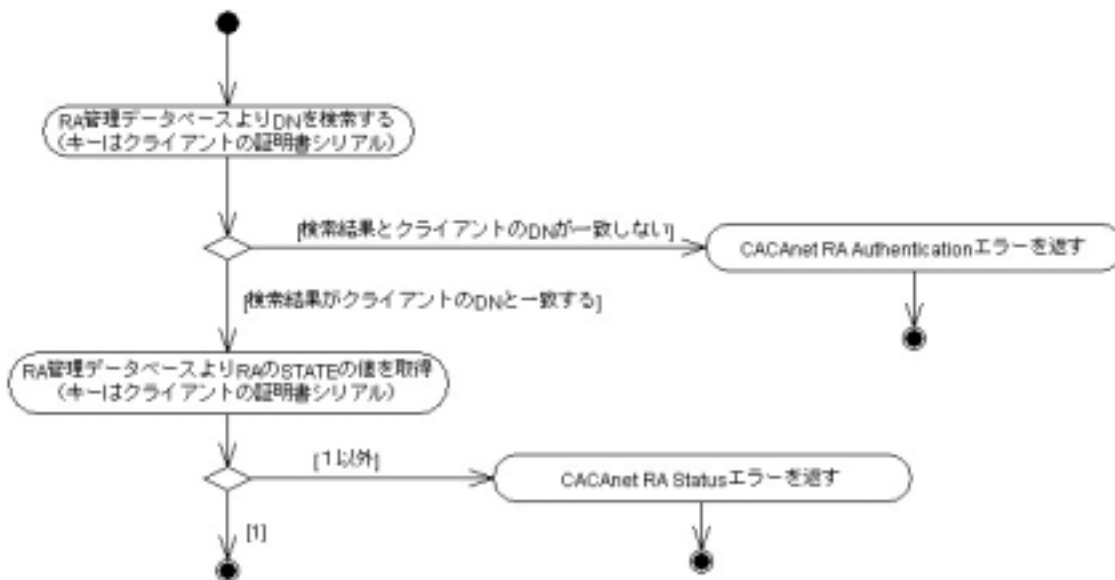
RAA

- ・ RAの管理ページ
- ・

RA

- ・
- ・
- ・
- ・
- ・

- ・ RAの正当性の確認方法
radb.rbの機能を利用し、下図のようなフローで確かめられる。



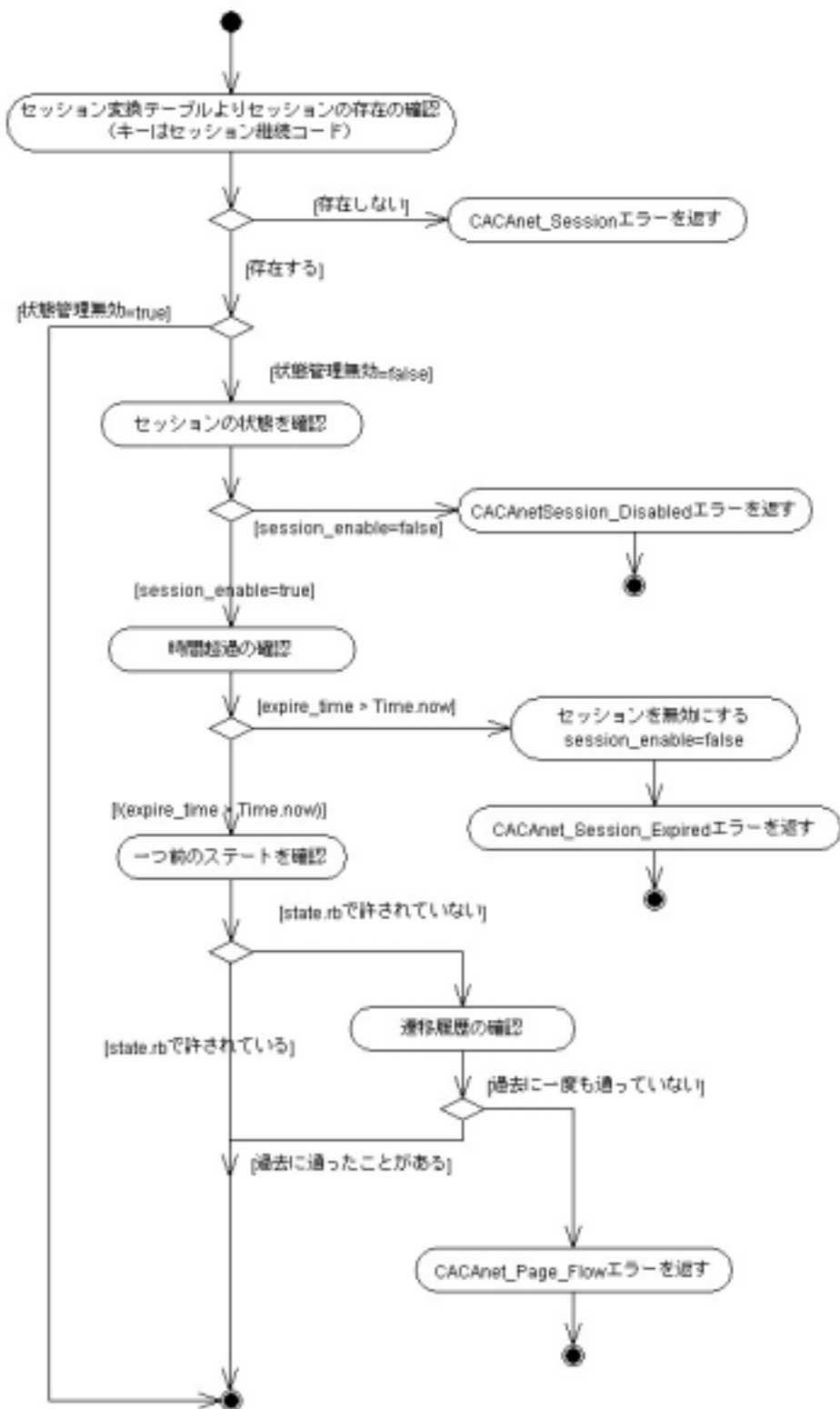
Subject

- ・
- ・
- ・
- ・
- ・

セッション管理

セッションの管理は scdb.rb の機能を利用し、その正当性は下図のようなフローで確か

められる。



* state.rb に記述されている、ステートごとの制限時間、許された遷移状態を下に示す。

状態遷移コード	制限時間	許可遷移状態
S000	10分	"INIT", "S010"
S010	5分	"S000"
S020	7分	"S010"
S100	10分	"S020", "S110"
S110	10分	"S100", "S120"
S120	10分	"S110"
S130	10分	"S120", "S200", "S300", "S400"
S200	10分	"S130", "S200"
S210	7日	"S200"
S300	10分	"S130"
S310	7日	"S300"
S400	10分	"S130"
S410	7日	"S400"
S500	1日	"S210", "S310", "S410"
S510	30日	"S500"
S600	10分	"S510", "S610", "S700"

<<システム異常系>>

- ・ 本システムで返すエラーは全て exsption.rb により定義される。
- ・ システムがエラーを返した場合、エラーごとに指定されている Web ページを表示する。
- ・ 各エラーと対応するエラーページは以下の表のとおりである。(エラーページは全て rhtml)

クラス名	説明	エラーページ
Exception	ruby 例外基底クラス	e999
CACAnet_Error	CACAnet 例外基底クラス	e000
CACAnet_Status_Error	状態異常	e010
CACAnet_Authentication_Error	認証失敗	e020
CACAnet_RA_Authentication_Error	RA 認証失敗	e021
CACAnet_RA_Status_Error	RA 認証失敗	e022
CACAnet_Subject_Authentication_Error	Subject 認証失敗	e023
CACAnet_IO_Error	入出力エラー	e030
CACAnet_Communication_To_CA_Error	CA との通信のエラー	e031
CACAnet_Input_Data_Error	入力データが不正	e040
CACAnet_Mandatory_Data_Error	必須情報が入っていない	e041

CACAnet_Session_Error	セッション継続不能	e054
CACAnet_Page_Flow_Error	ページ(状態)の遷移の異常	e051
CACAnet_Session_Expired	セッション情報の期限切れ	e052
CACAnet_Session_Disabled	セッション情報が無効	e053
CACAnet_CA_Communication_Error	CA との通信のエラー	なし

<<RAAconf の仕様>>

概要

- ・ 証明書発行管理システムに関する共通変数を保存するファイルである

基本仕様

- ・ ファイル名は「RAA のディレクトリ名」.rb とする
- ・ 以下に示す変数を保存する

変数名	説明
\$raserver_debug['セッション管理無効']	セッション管理を無効にする (boolean)
RAA_NAME	RAA 名
CACAnet_RAA_DN	RAA の DN
CACAnet_RAA_DN2	代替 RAA の DN
CACAnet_Top_Page	CACAnet Top Page URL
CACAnet_RAServer	RA server のホスト名
CACAnet_HOME	ホームディレクトリ
CACAnet_LIB	lib のパス
CACAnet_WORDS	秘密情報生成単語辞書
CACAnet_HTDOCS	htdocs のパス
CACAnet_HTDOCS_RAA	RAA ディレクトリ
CACAnet_USER_CERTS	個人証明書ディレクトリ
CACAnet_URL	個人証明書 URL
CACAnet_DB	DB 用ディレクトリのパス
CACAnet_SCDB	セッション管理 DB
CACAnet_SCTB	セッション変換テーブル
CACAnet_LOCK_FILE	SCDB 排他制御用 lock file
CACAnet_RADB	RA 管理 DB
CACAnet_P12	
CACAnet_P12_URL	P12 ファイル URL
CACAnet_Error_Pages	エラーページのディレクトリ

OPENSSL	openssl のパス
OPENSSL_CONF	openssl 設定ファイルパス
OPENSSL_CONF_PERSON	openssl 設定ファイルパス (person.conf)
OPENSSL_CONF_SERVER	openssl 設定ファイルパス(server.conf)
OPENSSL_CONF_CA	openssl 設定ファイルパス(ca.conf)
SENDMAIL	sendmail のパス
TEMPDIR	TEMP ファイル保存ディレクトリ
CA_MAIL_CERT	CA 公開鍵のパス
CA_MAIL_KEY	CA 秘密鍵のパス
CA_PASS	CA 秘密鍵のパスワードのパス
REQUIRED_INFO_LIST	必須入力情報のリスト
SUBJECT_INFO_LIST	Subject に個人情報属性のリスト
CERT_COUNTRY	証明書に記載される C
CERT_ORGANIZATION	証明書に記載される O0
CERT_ORGANIZATION_UNIT	証明書に記載される O1
CERT_4_ORGANIZATION_UNIT	証明書に記載される OU2

<<scdb.rb の仕様>>

概要

- ・ scdb.rb は複数の Web ページに亘って変数の内容を保持できるセッション機能を有し、システム上でセキュリティーを管理する本システム専用の Ruby ライブラリである。

機能

- ・ セッションの正当性を確認する
- ・ セッション管理データベースにセッション情報を格納する
- ・ セッション管理データベースからデータの取得
- ・ セッション管理データベースからレコードの削除
- ・ 新しいセッション ID、レコードの生成
- ・ セッション変換テーブルにデータを格納する
- ・ セッション継続コードとセッション ID の整合性を保つ
- ・ セッション継続コードの生成
- ・ セッション継続コードを<input>タグに埋め込んだ HTML の作成
- ・ ランダムな文字列の生成

<radb.rb の仕様>>

概要

- ・ RA の情報を管理する Ruby ライブラリ。

機能

- ・ RA 管理データベースへのレコードの追加、削除
- ・ RA 管理データベースへのデータの追加
- ・ RA 管理データベースからデータの取得
- ・ RA の正当性の検査

<<コード仕様>>

- ・ 状態遷移コード

証明書発行の作業状態に割り当てられたコード。コード毎にWebページが1ページずつ存在する。コード表は下に示すとおりである。

コード名	作業内容	クライアント
S000	Subject の連絡先の入力	RA
S010	Subject の連絡先の入力（確認画面）	RA
S020	Subject の連絡先の登録、メール送信	RA
S100	秘密情報の入力	Subject
S110	個人情報の入力	Subject
S120	個人情報の入力（確認画面）	Subject
S130	個人情報の登録、鍵生成方法の選択	Subject
S200	[PKCS#12] パスワードの入力	Subject
S210	[PKCS#12] メールの送信	Subject
S300	[IE] 登録する DN 情報の確認	Subject
S310	[IE] リクエストファイルの生成、メール送信	Subject
S400	[NS] 登録する DN 情報の確認	Subject
S410	[NS] リクエストファイルの生成、メール送信	Subject
S500	Subject の登録情報の確認	RA
S510	[承認] リクエストファイルへの署名	RA
S550	[非承認] 承認できない理由を入力	RA
S560	[非承認] メールの送信	RA
S600	証明書の取得	Subject

- ・ セッションID

証明書発行の手続きが開始されると生成され、ひとつの手続きは1つのセッションIDを持つ。scdb.rb の関数 gen_rand を利用して生成される。

- ・ セッション継続コード

Webページにアクセスするたびに生成されるセッションを継続するためのコード。scdb.rb の関数 gen_rand を利用して生成される。

- ・手続き中、次のWebページに移動する際、直接セッションIDを渡すのではなくセッション継続コードを渡しセッションを継続する。ただし、クライアントが変わる場面（ex.RA Subject など）ではセッション継続コードは使用されず、セッションIDを利用してセッションを継続する。

<<データベース仕様>>

- ・ファイルの保存場所は RAAconf により指定される。

- ・セッション管理データベース

セッションIDをキーとする。

以下の表で示すデータと RAAconf 内の SUBJECT_INFO_LIST で定義されたデータを格納している。

変数名	型	説明
session_id	ストリング	セッションID
session_enable	Boolean	レコードの有効性
Auth_info	ストリング	秘密情報の MD5 ハッシュ値
state_code	ストリング	現在の状態遷移コード
state_vector	配列	状態遷移コードの履歴
create_time	Time	レコード作成時刻
Last_update_time	Time	前回状態変更時刻
expire_time	Time	セッションを無効にする時刻
subject_mail_n	ストリング	Subject の電子メールアドレス（連絡用）
subject_name_j	ストリング	Subject の名前（漢字氏名）
subject_mail	ストリング	Subject の電子メールアドレス（証明書用）
subject_name	ストリング	Subject のローマ字氏名（DN 生成用）
keygen_method	ストリング	鍵生成の方法(nn,ie,p12)
ra_mail	ストリング	RA のメールアドレス
ra_name_j	ストリング	RA の名前（漢字氏名）
ra_dn	ストリング	RA の DN
ra_serial_no	ストリング	RA のシリアル番号
p12_password	ストリング	p12 用パスワードの一時記憶
Form_data	ハッシュ	Form(CGI)データの保存
temp_data	ハッシュ	一時データ
session_x_code	ストリング	セッション継続のための秘密コード

- ・セッション変換テーブル

セッション継続コードをキーとし、1レコードはセッションID、生成時間、状態遷移コ

ードの順で格納された配列で構成される。

- RA 管理データベース

RA の証明書の DN とシリアルナンバーをキーとし、以下のデータを格納する。

変数名	型	説明
serial	ストリング	証明書のシリアル番号
dn	ストリング	RA の証明書の DN
state	実数	RA の状態 1:正常,0:異常
racert	ストリング	RA の証明書の实体 (PEM)
raname	ストリング	RA のローマ字名
ra_org_unit_name	ストリング	RA の組織部署名
raname_j	ストリング	RA の日本語名
ramail	ストリング	RA のメールアドレス
raasn	ストリング	RAA の証明書のシリアル番号
create_time	Time	レコードの登録日時
last_update_time	Time	最終更新日時