第３章　内外の認証機関の運用実態

第１節　国内の認証機関の運用実態例（日本認証サービス㈱）

１　国内の認証機関の設立状況

現在、業務を行なっている認証機関は次のとおりである。日本認証サービス㈱は、主に金融機関を顧客としてサービスを提供しているほか、日立製作所㈱等の多目的スマートカード（社員証、クレジットカード、社内販売、食堂）に電子証明書を付加する発行支援業務を行なっている。

（平成１１年１１月現在）

企業名	日本認証サービス㈱	日本ベリサイン㈱	サイバートラスト㈱	エントラストジャパン㈱
設立	平成9年9月	平成8年2月	平成9年4月	平成10年12月
資本金	4億7000万円	6億400万円	18億5750万円	4億8000万円
従業員数	10名	30名		
株主	㈱日立製作所	VeriSign, Inc.	GTE Cyber Trust	セコム㈱
	富士通㈱	㈱さくら銀行	Solutions inc.	Entrust Technologies
	日本電気㈱	㈱三和銀行	㈱野村総合研究所	Inc.
	㈱あさひ銀行	㈱住友銀行	㈱ビー・ユー・ジー	㈱東京三菱銀行
	㈱さくら銀行	㈱日本長期信用銀行	NTT移動通信網㈱	㈱三和銀行
	㈱三和銀行	住友信託銀行㈱	㈱さくら銀行	㈱富士銀行
	㈱住友銀行	㈱大和證券	㈱三和銀行	㈱住友銀行
	㈱第一勧業銀行	日本生命保険（相）	㈱住友銀行	㈱東海銀行
	㈱東海銀行	㈱住友ｸﾚｼﾞｯﾄｻｰﾋﾞｽ	㈱日本興行銀行	㈱さくら銀行
	㈱東京三菱銀行	日本信販㈱	㈱日本長期信用銀行	野村証券㈱
	㈱大和銀行	日商岩井㈱	三井信託銀行㈱	日本生命保険（相）
	㈱富士銀行	三菱商事㈱	㈱大和證券	住友生命保険（相）
	㈱日本興行銀行	㈱NTTデータ	日興証券㈱	明治生命保険（相）
	㈱大垣共立銀行	㈱NTTPC ｺﾐｭﾆｹｰｼｮﾝｽﾞ	野村証券㈱	オリックス㈱
	㈱千葉銀行	NTTｴﾚｸﾄﾛﾆｸｽ㈱	新日本生命保険（相）	㈱NTTデータ
	㈱横浜銀行	シャープ㈱	第一生命保険（相）	ソニー㈱
	㈱大和證券	新日本製鐵㈱	日本生命保険	住友電気工業㈱
	日興証券㈱	ソニー㈱	オリックスグループ	日本ﾍﾞﾝﾁｬｰｷｬﾋﾟﾀﾙ㈱
	野村証券㈱	ソフトバンク㈱	㈱クレディセゾン	
	住友生命保険（相）	第一生命キャピタル㈱	㈱ジェーシービー	
	第一生命保険（相）	㈱東芝	㈱住友ｸﾚｼﾞｯﾄｻｰﾋﾞｽ	
	日本生命保険（相）	㈱東洋情報システム	日本信販㈱	
	住友海上火災保険㈱	凸版印刷㈱	伊藤忠商事㈱	
	東京海上火災保険㈱	日興キャピタル㈱	住友商事㈱	
	日動火災海上保険㈱	松下電器産業㈱	三井物産㈱	
	三井海上火災保険㈱	日本電気㈱	NTTｿﾌﾄｳｪｱ㈱	
	安田火災海上保険㈱	日本ユニシス㈱	NTTリース㈱	
	ｲｵﾝｸﾚｼﾞｯﾄｻｰﾋﾞｽ㈱	松下電器産業㈱	興銀ｲﾝﾍﾞｽﾄﾒﾝﾄ㈱	

	㈱オリエントコーポレーション		㈱シャフコ	
	㈱クレディセゾン		新日本ファイナンス㈱	
	㈱ジェーシービー		大日本印刷㈱	
	㈱ディーシーカード		凸版印刷㈱	
	日本信販㈱		日興キャピタル㈱	
	㈱ミリオンカード・サービス		㈱日本総合研究所	
	ユーシーカード㈱		日本ベンチャーキャピタル㈱	
	伊藤忠商事㈱		㈱フィクス	
	住友商事㈱		富士銀キャピタル㈱	
	丸紅㈱			
	三井物産㈱			
	㈱NTTデータ			
	沖電気工業㈱			
	大日本印刷㈱			
	凸版印刷㈱			
主要顧客	松下電器産業㈱ UCカード あさひ銀行 大和銀行 大垣共立銀行 富士銀行 三和銀行 住友銀行 日本信販 ミリオンカード 共同コンピュータサービス 東京相和銀行 オリエントコーポレーション NTTデータ 日立製作所 日本電気㈱	 住友銀行 安田信託銀行 大和證券 NTTデータ センチュリー監査法人 プロミス 富士銀行 AIU保険 アメリカンホーム・ダイレクト JCB 三井海上火災保険 日本電気 日本IBM 日商岩井㈱ 帝国データバンク	住友クレジットサービス JCB DCカード 野村証券 日本興行銀行	

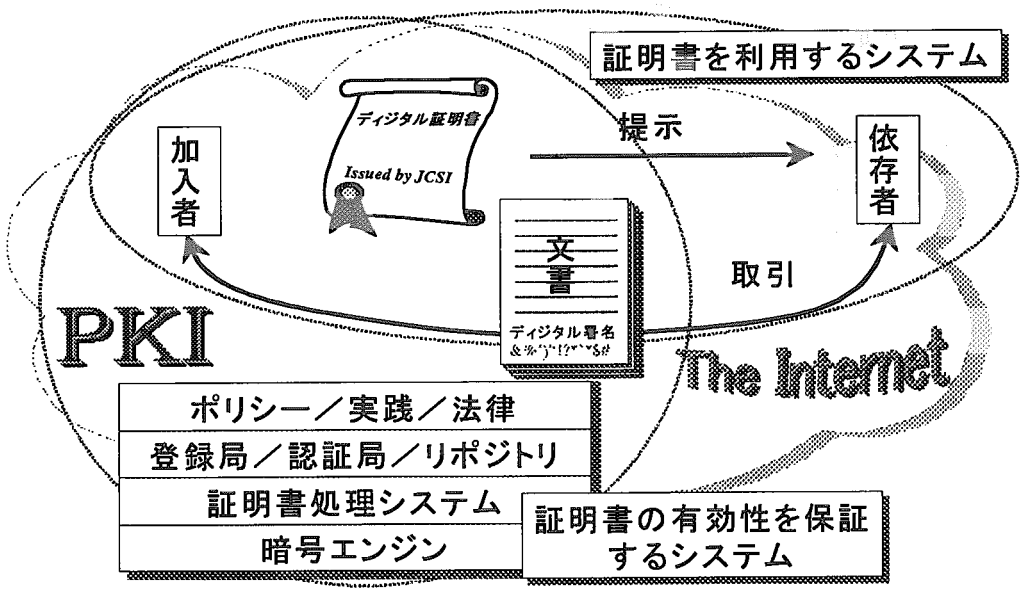
2　日本認証サービス㈱の業務の概要

（1）ＰＫＩが必要となる背景

ネットワーク社会は、電子情報（資産）のみで構成されており、そこはグローバルかつオープンな意思疎通や商取引が可能である。そこには、人為、プログラム、事故、自然災害等により、電子情報（資産）を目減りさせる脅威が存在する。人が電子情報（資産）を目減りさせる場合として、過失で行なわれる他、金銭目的、産業スパイ、愉快犯など故意によって行なわれる場合もある。また、方法としては、盗聴器等を利用した通信傍受のような受動的に電子情報（資産）を目減りさせる場合と、通信文の改竄、システムへの侵入等電子情報（資産）にアクセス、システムを混乱させるような能動的に電子情報（資産）を目減りさせる場合がある。このような脅威の対策としては、セキュリティホールを補強する等システムの脆弱性を最小化させるほか、入手し得る価値に比較して悪用行為に係る費用が膨大になるようにする方法が考えられる。すなわち、ＰＫＩの基礎をなす暗号技術を利用する方法である。

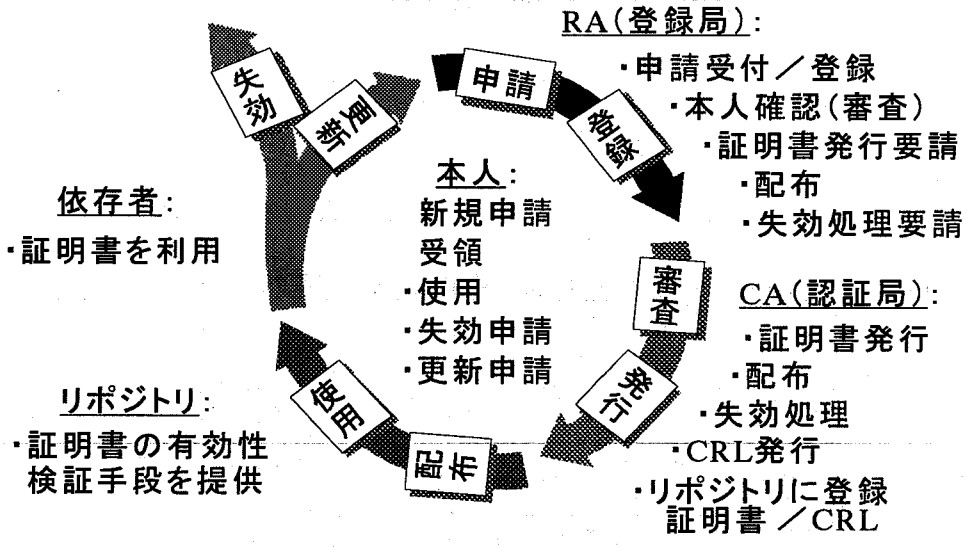
（2）ＰＫＩ（Public Key Infrastructure）

ＰＫＩ（Public Key Infrastructure）とは、公開鍵暗号方式に技術的な根拠を置いて、デジタル署名を信頼して使用できるようにするための仕組みである。ＰＫＩは、証明書の有効性を保証するシステムであり、この外側に証明書を利用するシステム、いわゆる電子商取引がある。証明書を利用するシステムでは、認証機関から認証され、デジタル署名を作成し提示する「加入者」と、提示されたデジタル署名を信頼する「依存者」が存在し、取引を行うことができる。証明書の有効性を保証するシステムとしては、ポリシー／実践／法律、登録局／認証局／リポジトリ、証明書処理システム、暗号エンジンが存在する。登録局／認証局／リポジトリは、ポリシー／実践／法律に従い、暗号エンジンを利用して証明書処理システムの運営を行う。



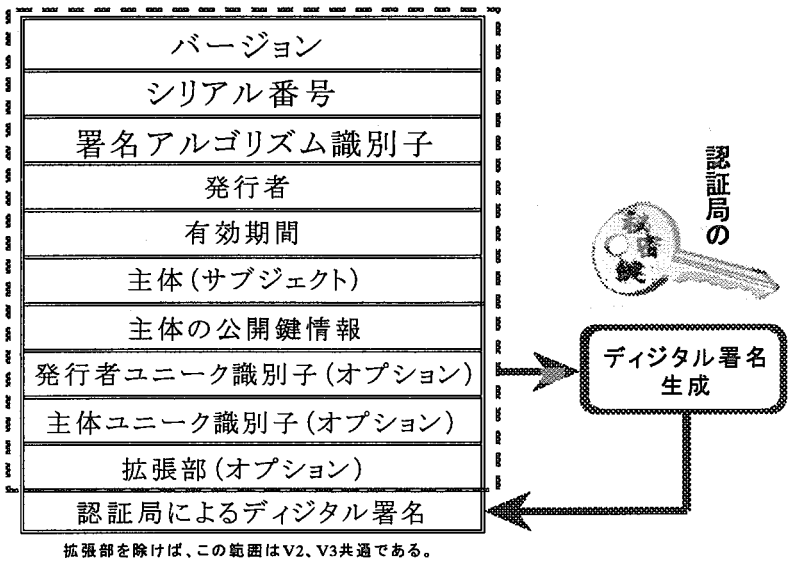
（３）証明書のライフサイクルと主体の役割

証明書のライフサイクルとしては、申請、登録、審査、発行、配布、使用、更新（または失効）という一連の流れがある。まず、「本人」は「ＲＡ」に対し新規申請を行う。「ＲＡ」は「本人」からの申請受付、登録、本人確認（審査）を行い、「ＣＡ」に対し、証明書発行要請を行います。「ＣＡ」は「ＲＡ」の要請に基づき、「本人」に証明書を発行し、「本人」はこれを利用する。また、「本人」が証明書の失効（更新）を希望する場合は、「ＲＡ」に失効（更新）申請を行い、「ＲＡ」の審査を経た後、「ＣＡ」は「ＲＡ」からの失効（更新）処理申請に基づき、失効処理（更新した証明書の発行）を行う。「ＣＡ」は、提示を受けた証明書が真正（または失効）であるかどうかについて、「依存者」からの照会に応じることができるよう、「リポジトリ」に証明書及びＣＲＬ（Certification Revocation List）に関する情報を登録する。「本人」から証明書の提示を受けた「依存者」は、「リポジトリ」で相手の証明書の真正性を確認することによって、取引等を安全に行うことができる。



「ＣＡ」が発行する証明書は、Ｘ.５０９標準に準拠しており、この中には本人と本人の公開鍵情報が入っているので、この証明書を検証することによって公開鍵が本人のものであることを確認することができる。また、「ＣＡ」が発行するＣＲＬ（Certification Revocation List）には、失効受付日、失効理由（加入者の秘密鍵の危殆化（漏洩、盗難、紛失又は解読等））等の情報が入っている。

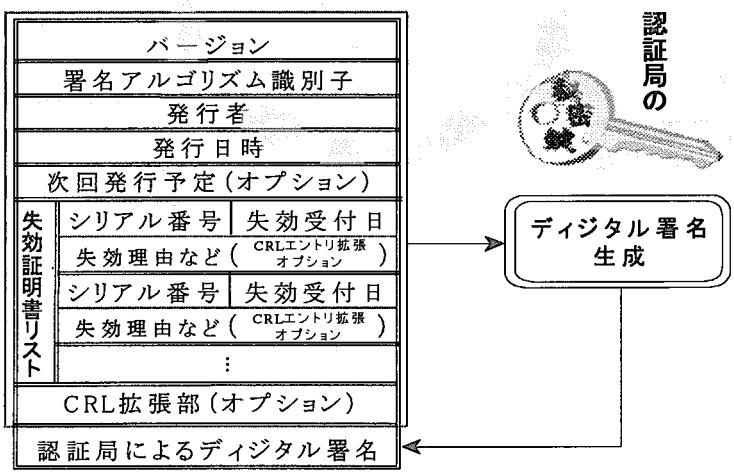
X.509基本証明書項目



拡張部を除けば、この範囲はV2、V3共通である。

CRL : Certification Revocation List

満了していない失効した証明書のシリアル番号のリスト

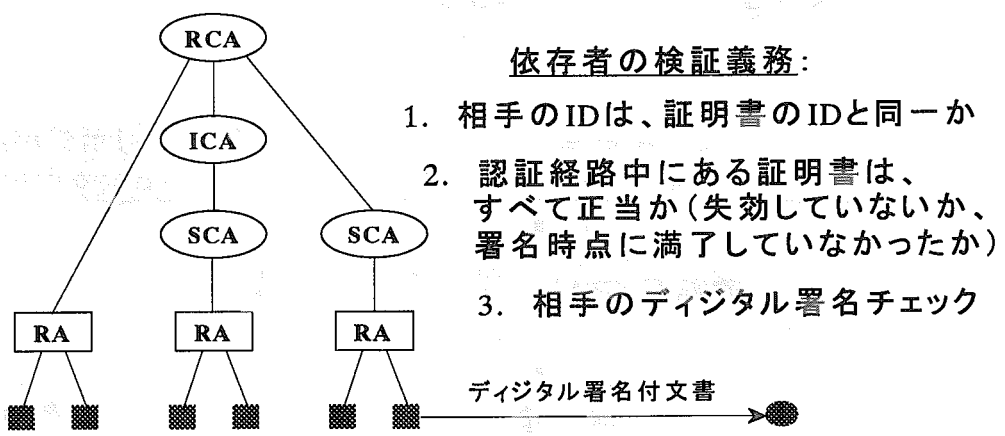


V1形式では、拡張部がない。

（4）ＣＡ／ＲＡ階層モデルと依存者の義務

日本認証サービス㈱が採用しているＣＡ／ＲＡ階層モデルでは、「ＲＡ」が存在することを必須としており、加入者の本人確認に責任を持ちます。「ＳＣＡ」は、「ＲＡ」の協力を得て、認証業務を行うが、その「ＳＣＡ」の正当性を証明する上位のＣＡが存在しており、最も上位にあるものが「ＲＣＡ」である。「ＲＣＡ」は自己の正当性を自ら証明しなければなりません。

送付されたデジタル署名付文書を「依存者」が安心して利用するためには、「相手のＩＤは、証明書のＩＤと同一か」、「認証経路中にある証明書は、すべて正当か（失効していないか、署名時点に満了していなかったか）」及び「相手のデジタル署名チェック」を検証する必要がある。



RCA : Root Certification Authority
ICA : Intermediate Certification Authority
■ : 加入者（Subscriber）

SCA : Subordinate Certification Authority
RA : Registration Authority
● : 依存者（Relying Party）