キャンパス PKI CP/CPS ガイドライン

初版(ver1.0)

国立情報学研究所
学術情報ネットワーク運営・連携本部
認証作業部会

2007 年 6 月 6 日

目次

1. はじめに

1.1 目的

大学共同利用機関法人 情報･システム研究機構 国立情報学研究所（以下、「本研究所」という）では、大学間のサービスをセキュアに連携するための全国共同電子認証基盤（以下、「UPKI」という）構築事業を推進している。

UPKI は、これに参加する大学を結ぶﾄﾗｽﾄﾄﾞﾒｲﾝを形成し、相互認証を行う共通の認証基盤である。本キャンパス PKI CP/CPS ガｲﾄﾞﾗｲﾝ（以下、「本ガｲﾄﾞﾗｲﾝ」という）は、各大学に設置が予定されるキャンパス PKI の証明書ﾎﾟﾘｼｰ（Certificate Policy、以下、「CP」という）及び認証局運用規程（Certificate Practice Statement、以下、「CPS」という）に関するガｲﾄﾞﾗｲﾝを示し、相互運用性を確保することを目的としている 。

なお、将来的に GPKI 等他の認証基盤と相互接続を行う場合、証明書の用途を電子署名とする等、認証局ﾎﾟﾘｼｰを見直す必要がある。

1.2 概要

本ガｲﾄﾞﾗｲﾝは、先行してキャンパス PKI を構築した 2 大学（A 大学、B 大学）の CP/CPS を参考とし、相互運用性の確保のための要件をまとめたものである。2 章は、認証局の運用形態（ｱｳﾄｿｰｽ、ｲﾝｿｰｽ）について定義し、3 章は、先行 2 大学の CP/CPS の比較を実施している。4 章では、3 章を比較した結果をガｲﾄﾞﾗｲﾝに反映している。

本ガｲﾄﾞﾗｲﾝは、以下の条件に適用されるよう記述している。

- 発行局（IA サーバ）及び登録局（RA サーバ）の運用を外部に委託する場合
- 発行局（IA サーバ）の運用を外部に委託する場合

2. 認証局の運用形態

認証局を運用する場合、一般的に採用される運用形態を以下に示す。

表 2-1 認証局運用形態

項番	運用形態	運用先				備考
		RA	IA	IC ｶｰﾄﾞ発行	登録用端末	
1	IA サーバ、RA サーバのアウトソース	○	○	△	●	認証局のファシリティやリソースを準備する必要がない。
2	IA サーバのアウトソース	●	○	△	●	RA サーバを運用するための部屋やリソースが必要となる。RA サーバを運用するための部屋は認証局設備と同等のセキュリティレベルが要求される。
3	全てのサーバをインソース	●	●	●	●	高レベルな認証局設備を準備する必要がある。また、認証設備やリポジトリの運用をインソースで実施しなければならない。

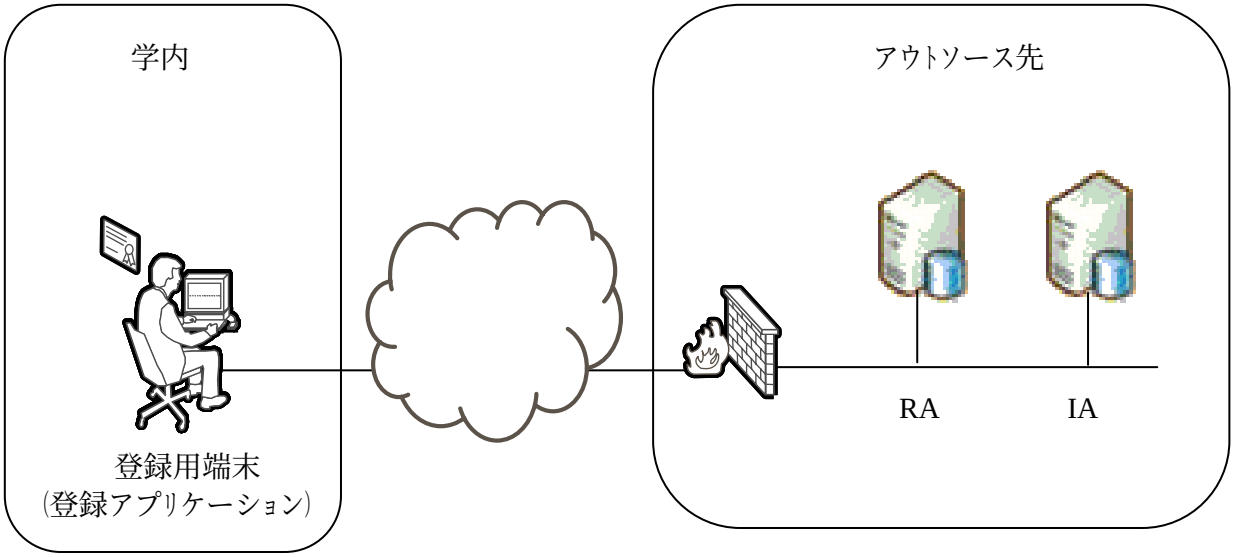
※○:アウトソーシングする。●:インソースする。 △:オプションでアウトソースする。

本ガイドラインでは、1.2 節で述べた通り、太枠で囲った範囲を対象としている。また、キャンパス PKI においては、証明書格納媒体として IC カードを利用することが望ましいため、IC カードを利用することを前提に記述している。

表 2-1 の項番 1、2 の場合、アウトソース先のオプションサービスとして、リポジトリ（LDAP、Web サーバ、OCSP サーバ）をアウトソースするかインソースするかを選択できる場合がある。また、バックアップサービスやシステムの二重化サービス等が存在する。

2.1 IA サーバ、RA サーバのアウトソース

運用形態のイメージは以下の通りである。

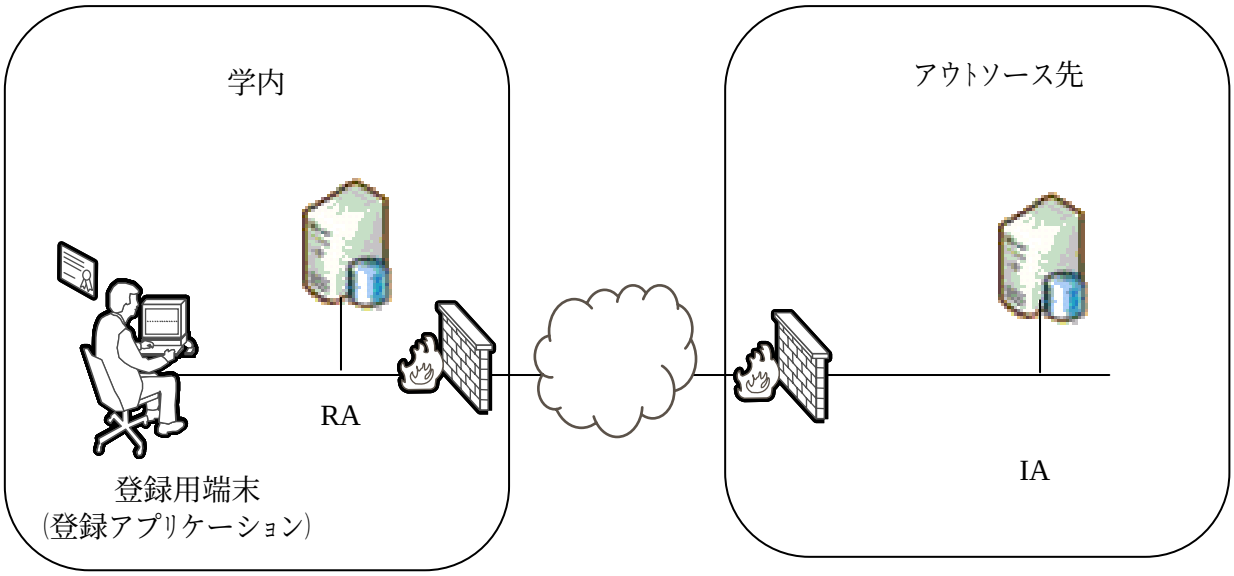


※サーバ数、ネットワーク構成は一例

図2-1 IA サーバ、RA サーバのアウトソースのイメージ

2.2 IA サーバのアウトソース

運用形態のイメージは以下の通りである。

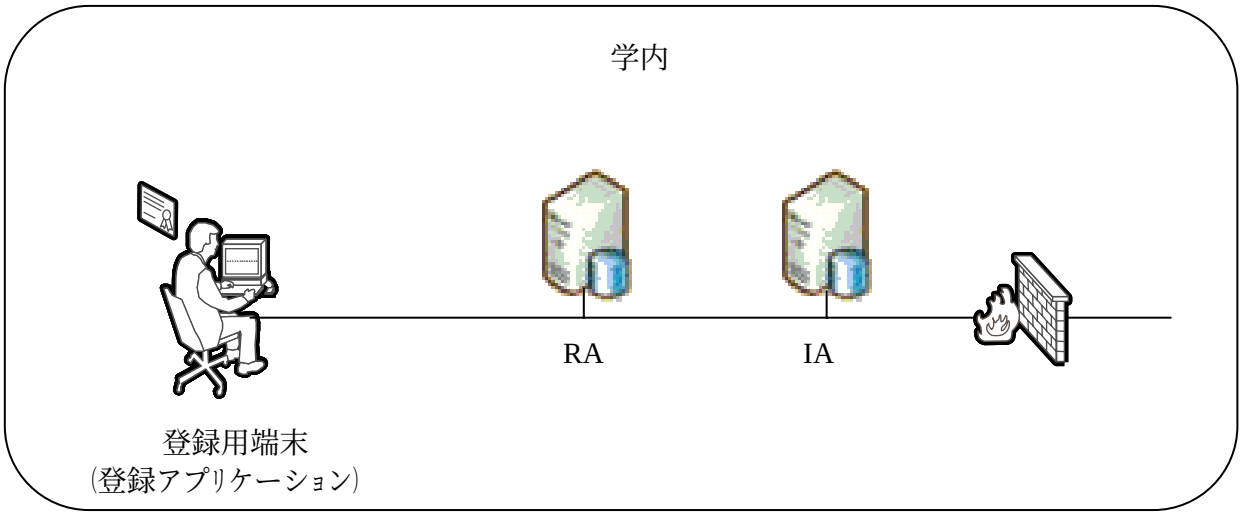


※サーバ数、ネットワーク構成は一例

図2-2 IA サーバのアウトソースのイメージ

2.3 全てのサーバのインソース

運用形態のイメージは以下の通りである。



※サーバ数、ネットワーク構成は一例

図2-3 全てのサーバをインソースした場合のイメージ

3. 先行大学 2 大学 CP/CPS 比較結果

本章では、相互運用性を確立する上で重要なポイントを示し、そのポイント毎に先行大学の CP/CPS の規定内容について比較した結果を記述する。各大学の CP/CPS は大学内に閉じた認証に関するポリシーを規定しているのであって、運用を重ねるにあたり、変更される可能性がある。また、本章で行う比較については、各大学の CP/CPS の優劣を比較しているのではない。

以下に相互運用性を確立する上で重要なポイントを示す。

(1) 認証局階層構造
(2) 発行対象者(以下、「利用者」という)と証明書利用用途
(3) 証明書プロファイル
(4) 利用者の本人確認と審査登録
(5) 利用者の鍵ペア生成と格納媒体
(6) 利用者への配布
(7) 鍵アルゴリズムと証明書有効期間
(8) 失効情報の提供方法と有効期間
(9) 認証局秘密鍵管理
(10) 運営に関する指揮命令系統と内部けん制
(11) アウトソースする業務とその管理
(12) 記録する情報とその管理
(13) 監査

なお、本ガイドラインの付録に先行 2 大学の CP/CPS 比較一覧を示す。付録では CP/CPS の全項目について比較を実施している。

3.1 認証局階層構造

A 大学は、セルフサイン証明書を持つ認証局であり、階層構造を持たない。B 大学は、ルート認証局、中間認証局(発行認証局)からなる階層構造を持つ。

相互認証先と相互認証証明書の取り交わしを行うことによって相互認証する場合、階層構造を持つことによって、認証パス構築等で処理に負担がかかることが予想される。相互認証方式は現段階では未決定であるが、ポリシー上階層構造を持たせる必要性が低ければ、セルフサインの証明書を持つ認証局を前提にした方が良い。

3.2 発行対象者と証明書利用用途

両大学共に発行対象者は人(＝大学の教職員、学生、その他大学が認める者)であるが、B 大学はドメインコントローラ等の機器にも証明書を発行している。本証明書は認証の用途で発行しているため、機器に対する証明書の発行も可能であり、人及び機器への発行手順がそれぞれ確立されていれば、この違いが相互運用性に影響を与えるものではないと考える。

両大学共に以下の項目を共通の証明書の用途として規定している。

- Web ポータルや無線 LAN、VPN、SSO におけるクライアント認証の用途
- スマートカードログオン（Windows、MacOS、Linux）の用途

また、両大学共に S/MIME や電子署名の用途での利用を検討しているが、B 大学は S/MIME 及び電子署名の用途の証明書を発行する認証局を認証ベンダーのパブリック認証サービスを利用し、別途、構築･運用している。

3.3 証明書プロファイル

両大学の証明書プロファイルを以下に示す。証明書に含んでいるフィールドは○、あるいは値で表し、含んでいないものは無記入としている。

<基本フィールド>

フィールド	認証局証明書		利用者用証明書		備考
	A 大学	B 大学	A 大学	B 大学	
Version	CPS 上で規定していない	○	○	○	ver3
serialNumber		○	○	○	
Signature		○	○	○	
Validity		○	○	○	
notBefore		○	○	○	UTCTime
notAfter		○	○	○	UTCTime
Issuer		○	○	○	
Subject		○	○	○	
subjectPublicKeyInfo		○	○	○	
Algorithm		○	○	○	
subjectPublicKey		○	○	○	
Extensions		○	○	○	

<拡張フィールド>

フィールド	認証局証明書		利用者用証明書	
	A 大学	B 大学	A 大学	B 大学
authorityKeyIdentifier	CPS 上で規定していない		○	
subjectKeyIdentifier			○	
keyUsage		・keyCertSign ・cRLSign	・digitalSignature ・keyEncipherment	・digitalSignature ・keyEncipherment
extendedKeyUsage			・clientAuth ・MS-smartCardLogon ・emailProtection	・clientAuth ・codeSigning ・emailProtection
privateKeyUsagePeriod				
certificatePolicies			OID	OID CPS 公開用 URL
policyMapping				
subjectAltName		○ PrintableString	・rfc822mail ・Microsoft 社 UserPrincipalName	Microsoft 社 UserPrincipalName
basicConstraints		TRUE		FALSE
nameConstraints				
policyConstraints				
cRLDistributionPoints		・http ・CRL 用 URL	・http ・ldap ・Entrust CRL DP	・http ・CRL 用 URL
subjectDirectoryAttr				
authorityInfoAccess				・OID ・OCSP 用 URL
netscape-cert-type		・SSL CA ・S/MIME CA		
VeriSignPrivate Extension				OID

両大学共に X.509 バージョン 3 に準拠しており、また、Distinguished Name（以下、「DN」という）は X.500 勧告に従っている。ただし、B 大学は subjectDN 及び SubjectAltName 内において、利用者個人を特定する情報を含んでいないが、A 大学は subjectDN 内の CN において学籍番号を用いていることから、個人を特定する情報を含んでいるという違いがある。

extendedKeyUsage には大学毎に違いがあるが、実際の利用用途としては、クライアント認証及びスマートカードログオンの用途であることから、クライアント認証、スマートカードログオンの用途は必ず規定し、これ以外はオプションとするか規定しないことが望ましいと考える。

B 大学は OCSP を採用していることから、AIA（AuthorityInfoAccess）が規定されている。また、両大学共に採用している認証モジュール及びサービスの都合上、ベンダー固有のエクステンションが存在する。OCSP の採用、不採用及びプライベートエクステンションの有無は各大学の判断に任せることで問題ないと考える。

将来的に相互認証を行う際に、相互認証証明書を取交す場合、OCSP や証明書プロファイルの要件は相互認証先と調整し、要件を満たさなければならない。鍵の用途や DN のポリシーは揃っていることが望ましいものと考える。将来的に相互認証証明書を発行するような運用を行う場合、認証局証明書や利用者証明書、相互認証証明書のフォーマット及びサポートするフィールド、オプションのフィールドについても規定が必要となる。

3.4 利用者の本人確認と審査登録

両大学共に利用者の本人確認は入学時、あるいは採用時に行われ、その時に入手したデータがデータベースに登録されている。

A 大学は入学時、採用時、進学時といったタイミングで利用者に発行申請書及び顔写真を提出させ、大学側で CSV を作成し、発行指示を行っている。B 大学はデータベースのデータを信頼し、入学時、採用時、進学時といったタイミングで、大学側で利用者登録用の CSV を作成し、発行指示を行っている。

両大学共に入学や採用といったタイミングで本人確認が行われていることで、審査は同等のポリシーで実施されていると考えられる。利用者本人に申請書を提出させるか、大学側で判断するかについては、大学側のポリシーで実施することに問題はないと考えるが、利用者には証明書の用途や紛失時の扱いといった運用手順、管理責任について十分な説明、意識付けが必要である。

また、登録業務を実施する際は、内部けん制及び誤発行防止のためのチェック機構としてもデュアルコントロール等を徹底していることが望ましいため、CP/CPS 上で内部けん制について規定し、これに遵守していることが重要である。

3.5 利用者の鍵ペア生成と格納媒体

両大学共にアウトソース先のサーバ内において利用者の鍵ペアを生成し、鍵ペア及び証明書の格納媒体として IC カードを利用している。IC カードは入館証や身分証明書の役割も果たしている。安全な媒体上で秘密鍵を管理していることは、相互認証先にとっても信頼度が高まるものと考えられ、従って、IC カードを利用者用証明書の格納媒体とすることが望ましいと考えられる。

また、鍵ペアの生成については、認証局設備と同等の設備内で内部けん制の働く環境において行われるべきであり、両大学においてもアウトソース先の安全なファシリティ内で複数人コントロールの下で実施されている。

A 大学はアウトソース先で証明書格納及び券面印刷を実施しているが、B 大学については、現在試行運用ということもあり、IC カードへの証明書格納、券面印刷を学内で実施している。しかし、本格運用を実施する際は認証局設備と同等の設備内で内部けん制の働く環境を持つ委託者にアウトソースする計画であり、利用者鍵ペア生成及び格納に関するポリシーのレベルを合わせることが出来ると考えられる。

3.6 利用者への配付

両大学共に利用者への配付はオリエンテーション時や窓口にて対面で実施されている。券面に印字された顔写真等を元に本人確認される。A 大学については、IC カードの配付と同時に誓約書を利用者に提出させ、学内の情報セキュリティ規則への遵守及び証明書の受領について同意させる方法を用いている。

また、A 大学は IC カードと IC カード PIN を同時に配付しているが、B 大学では IC カードは対面で配付し、IC カード PIN は学内便や郵送等で別送しているという違いがあった。両大学のように代理人を認めず、原則対面（窓口、配送）で配付するような運用であれば、IC カード及び IC カード PIN の配付は同時でも問題ないと考えられる。ただし、遠隔地にいる利用者に発行する場合は IC カード及び IC カード PIN は別送したり、利用者に受領書を返送させたりする等の工夫が必要であると考える。

利用者本人に確実に配付されることは相互認証先を信頼できるか否かにも大きく関わってくるため、先行 2 大学のように対面での配付を義務付けたり、代理人による取得を認めない等、より確実な方法を選択されるように CP/CPS で規定すべきである。

3.7 鍵アルゴリズムと証明書有効期間

A 大学の鍵アルゴリズムと証明書有効期間は以下の通り。

- CA 証明書：10.5 年（SHA-1withRSAEncryption 2048bit）
- 利用者証明書は一般的な卒業、修了までの年数で発行。留年等の場合は、1 年毎の発行（SHA-1withRSAEncryption 1024bit）

B 大学の鍵アルゴリズムと証明書有効期間は以下の通り。

- ルート証明書：25 年 （SHA-1withRSAEncryption 2048bit）
- 発行用 CA 証明書：13 年（SHA-1withRSAEncryption 2048bit）
- 利用者証明書：1 年から 6 年（一般的な卒業、修了までの年数、留年時は 1 年毎の発行）（SHA-1withRSAEncryption 1024bit）
- ドメインコントローラ証明書：6 年（SHA-1withRSAEncryption 1024bit）
- OCSP レスポンダ：13 年（SHA-1withRSAEncryption 2048bit）

証明書の有効期間は相互認証証明書を取交すことになった場合、相互認証証明書の有効期間、更新時期を検討する上でも非常に重要な要素となる。

認証の用途であれば、可能な限り認証局証明書及び相互認証先証明書の有効期間を越えない範囲で相互認証証明書を取交すことが可能となるが、利用者証明書の用途に電子署名を加えた場合、例えば、相互認証証明書の有効期間は認証局証明書の有効期間の 1/2 を越えないよう配慮する等が必要である。

3.8 失効情報の提供方法と有効期間

A 大学の CP/CPS 上は ARL について規定されていないが、実際は両大学共に ARL 及び CRL の提供を行っており、失効情報の提供を Web サーバ＋LDAP、あるいは Web サーバ＋OCSP という複数の方法で行っている。また、失効情報へのアクセスコントロールは特に行われていない。

両大学共に 24 時間以内の発行を行っているが、A 大学の nextUpdate は 96 時間で、B 大学の nextUpdate は 48 時間であることから、障害発生を考慮した運用を行っていることが分る。ただし、相互認証を行う上では nextUpdate のタイミングで取得する情報の新鮮さは同等である必要があると考えられ、今後調整が必要であると考えられる。

学内のクライアント認証用途で利用されるアプリケーションは nextUpdate に設定された日時に失効情報を取得するタイプのものが存在することが想定され、その間に失効した情報が反映されないことを考えると、48 時間程度が望ましいと考える。

また、保守業務及び障害等によってシステムを停止する場合、相互認証先に予め、あるいは適時、連絡する等の取り決めが必要である。

両大学共に証明書の一時停止のサービスは実施しておらず、一時停止を行いたい場合は、アプリケーションの機能（アカウントの停止等）を用いて行っているか、あるいはその方法を検討している状況である。

失効情報(ARL/CRL)のプロファイルは以下の通りである。

<基本フィールド>

フィールド	認証局証明書		利用者用証明書		備考
	A 大学	B 大学	A 大学	B 大学	
Version	CPS 上で規定していない	○	○	○	ver2
Signature		○	○	○	
Issuer		○	○	○	
thisUpdate		○	○	○	UTCTime
nextUpdate		○	○	○	UTCTime
RevokedCertificates		○	○	○	
userCertificate		○	○	○	
revocationDate		○	○	○	UTCTime
crlEntryExtensions			○	○	
crlExtensionts			○	○	

<拡張フィールド>

フィールド	認証局証明書		利用者用証明書		備考
	A 大学	B 大学	A 大学	B 大学	
crlEntryExtensions	CPS 上で規定していない				
reasonCode			○	○	
holdInstructionCode					
invalidityDate					
certificateIssuer					
CrlExtensions					
authorityKeyIdentifier			○		
issuerAltName					
cRLNumber			○	○	
deltaCRLIndicator					
issuingDistributionPoint					

3.9 認証局秘密鍵管理

両大学共にアウトソース先の発行局内で FIPS140-2 レベル3相当の HSM を利用し、秘密鍵を管理している。

3.10 運営に関する指揮命令系統と内部けん制

両大学共に認証局の運営に関する最高意志決定機関を持ち、以下、認証局責任者、アウトソース先の責任者、登録業務（インソース）の責任者とオペレータという組織で成り立っている。

相互認証証明書を取り交わす場合、その意思決定及び相互認証証明書発行に関する指揮命令系統は事前に確立されているべきであり、両大学が組織しているような体制、指揮命令系統は重要なポイントとなる。

また、失効情報の提供が出来ない場合（定期、非定期の保守業務、障害対応）に、相互認証先に通知を行う義務が生じるため、相互認証証明書を取り交わすような場合は、CP/CPS にその点についての規定も必要となる。

3.11 アウトソースする業務とその管理

両大学共に IA サーバは認証ベンダーにアウトソースしている。しかし、B 大学の場合、RA サーバをインソースしている。

RA サーバをアウトソースするかインソースするかは相互認証を行う上で問題にはならないが、RA サーバを運用するファシリティ、リソースについては、認証設備室と同等のレベルが求められるため、インソースする場合は、そのような環境、リソースを準備できる大学に限られるものと考える。

3.12 記録する情報とその管理

3.12.1 監査ログとして記録されるイベント

両大学共に次のイベントに関して記録することを規定している。

- CA 秘密鍵の操作履歴
- 証明書発行、失効の処理履歴
- ARL/CRL 発行の処理履歴
- 認証設備室（IA サーバの設置された部屋）及び登録設備室（RA サーバの設置された部屋）の入退室記録
- 認証局設備（IA サーバ、RA サーバ等、認証業務において重要な役割を果たすサーバ等）へのアクセス記録（不正アクセスを含む）

また、A 大学はこれ以外にも、データベースの操作や権限設定の履歴について記録することを CP/CPS 上で規定している。相互認証する上で、最低限記録しなければならない事項は、両大学共に規定しているイベントであると考える。

3.12.2 アーカイブデータ

両大学共に監査ログに加え、アーカイブデータとして以下を規定している。

- 利用者用証明書
- 証明書利用申請・失効申請のための書類（B 大学では、紛失・再発行に関する申請書類のことを指す）
- 監査の実施結果に関する記録及び監査報告書

上記に加え、A 大学は、これ以外に以下をアーカイブするデータとして規定している。

- CRL
- CP/CPS
- CPS に基づき作成された認証局の業務運用を規定する文書
- 認証業務を他に委託する場合においては、委託契約に関する書類

電子署名の用途ではないため、過去の CRL の保管については優先度を低くすることが可能と考えるが、将来的に電子署名の用途が追加されることを想定した場合は必須になると考えられる。また、将来、相互認証先と相互認証証明書を取り交わすような場合、相互認証証明書もアーカイブ対象であると考えられる。相互認証の方式によって、アーカイブ対象は見直されるべきである。

3.12.3 記録の保管期間と保護

記録されるイベントやアーカイブデータの種類の詳細については、CP/CPS の下位文書で規定する場合もあるため、CP/CPS では、大項目レベルの記述に留める方法もある。

両大学共に記録した情報の重要性に応じて、保管期間及び保護についての規定を行っている。

表 3-1 記録の保管期間

記録対象	A 大学	B 大学
監査ログ	最低 10 年間	認証局設備の監査ログは 2ヶ月間 ただし、証明書のライフサイクルに関するログは 5 年間 登録局設備の監査ログは 6ヶ月
アーカイブログ		作成日から 5 年間
入退室ログ	最低 1 年間	監査ログの規定に準拠する
ネットワークログ	最低 1 年間	監査ログの規定に準拠する

現在は主に認証用途の証明書ということもあり、過去を振り返って有効であったかといった検証を行うことはなく、また、定められた期間内に新しい IC カードが発行されるという現状から、両校のように重要なデータを（作成から）5 年～10 年以内で保管することは十分な保管期間を規定していると考えられる。

ただし、電子署名の用途で利用される場合は証明書の有効期間を超えて署名当時の有効性を検証できなければならない場合があるため、証明書の有効期間を超えて 5 年～10 年といった法的に保管期間が義務付けられている文書に応じて判断することが現実的であると考える。

また、定期的な監査において問題がないと認められるシステムへのアクセス記録、ネットワークシステム上のログ、入退室ログについては監査の記録を残し、廃棄しても問題ないものと考える。

3.13 監査

両校共に認証局の運用が CP/CPS に準拠しているかについて適時監査を行うことを定めている。

相互認証を行う上では、定めたポリシー通りに運用されているかを第三者が監査することは重要であり、その監査結果を相互認証先に報告するような運用が求められるものと想定できるため、監査についての規定は必須であると考える。

4. CP/CPS ガイドライン

本章は、IA サーバや RA サーバをアウトソースする場合（RA サーバモジュールのアウトソースは必須ではない）について、CP/CPS ガイドラインを示す。CP と CPS を分離するか否かは各大学の判断によるが、大学内及び大学間のサービスにおける認証の用途としてポリシーを統一できれば CP/CPS を分離する必要はない。本ガイドラインにおいては、CP/CPS を分離せずに記述するものとする。

本章は、極力 CP/CPS を作成する上で参考となるよう記述することを心がけるが、各大学のポリシーに応じて規定すべき内容及び相互認証を行う上で将来的に調整が必要な内容があることに留意する必要がある。特に、相互認証の方式によって例示が異なる可能性があるため、注意が必要である。

例において、＊(　)の記載があるものは、注意書きを意味する。また、相互認証についての記述は、参考として記載しており、将来的に見直しが必要である。

以降での本章構成は、RFC3647 に基づく。

4.1 はじめに

4.1.1 概要

【解説】
本節では認証局の名前、サービス名、大枠のサービス内容、相互認証を行う等の宣言を行い、認証局の概要について記す。また、相互認証の方式についても簡単に定義しておくことが望ましい。

【記述例】

1　はじめに

○○電子認証局は、○○大学により運営され、○○大学内及び大学間のサービスにおける電子認証のために必要となる電子証明書（以下、「証明書」という）を発行する。

本文書において、「○○ 電子認証局（以下、「本認証局」という）」の権利または義務は国立大学法人たる○○大学 に帰属することを意味する。

本認証局は、大学間のサービスを共有するために相互認証接続を行う。

また、以下の例のように CP/CPS が規定する内容について記述する。

【記述例】

○○電子認証局運用規程（以下、「本 CP/CPS」という）は、本認証局の認証業務に関する運用方針、それに付随する発行業務、登録業務の運用方針、利用者の義務と本認証局との関係、検証者の義務と本認証局との関係、本認証局が発行する証明書の取扱いについて規定する。証明書の取扱いについては、申し込み、登録、発行、再発行、失効、有効期間満了に関する記述が含まれる。

4.1.2 文書名称と定義

【解説】
本節では、CP/CPS の正式名称を定め、そのポリシーのオブジェクト識別子（Object Identifier）（以下、「OID」という）を規定する。

オブジェクト識別子とは、国際的に登録し標準化機関によって承認された特別に形式化された番号であり、一意な英字/数字の識別子で 、ISO 標準に登録された特定のオブジェクトやオブジェクトクラスを示すものである。通常、認証局の証明書ポリシー（CP）に対して、1つの OID が宣言され、その OID を証明書に記載することによって、どの証明書ポリシー（CP）に準拠しているかを宣言する。証明書には、複数の OID（複数の CP）を宣言する場合がある。

【記述例】

1.2 文書名称と定義

本 CP/CPS の正式名称を「○○大学電子認証局運用規程」とする。本認証局が提供するサービスに関連するオブジェクト識別子（OID）は、次の通りである。

- 利用者証明書に記載する certificatePolicies
- 相互認証証明書に記載する certificatePolicies

4.1.3 PKI の関係者

【解説】
本節では、トラストドメインに登場する関係者を規定し（図解することが望ましい）、また、証明書の発行を受ける者（以下、「利用者」という）の窓口となる部署、連絡先、サポート時間等の規定を行う。

【記述例】

1.3 PKI の関係者

（1）認証局意志決定機関
（2）発行局
（3）登録局
（4）登録窓口
（5）リポジトリ（Web サーバ、LDAP サーバ）
（6）利用者（証明書の発行を受ける者）、検証者（本認証局を信頼し、証明書の検証を行う者、機器）
（7）その他の関係者
- 相互認証先
- OCSP

登録窓口情報（申請窓口、受付日時、住所、TEL、FAX、E-Mail）

4.1.4 証明書の用途

【解説】
本節では、認証局が発行する全ての証明書の種類及び用途や禁止されている用途について規定する。

【記述例】

1.4.1 証明書の種類

(1) 自己署名証明書＊(セルフサイン認証局の場合)
(2) 利用者用証明書＊(学生、教職員等)
(3) 機器用証明書＊(機器に対して発行している場合)
(4) 相互認証証明書＊(相互認証の方式により見直しが必要)

1.4.2 正規の証明書用途
○○大学に所属する者のシステム利用者認証(SSL、スマートカードログオンを含む)及び大学間サービスにおける利用者認証の用途とする。

1.4.3 禁止されている証明書用途
本 CP/CPS1.4.2 に規定する以外の用途で使用したことにより発生した損害について、本認証局は一切の責任を負わないものとする。

4.1.5 ポリシー管理

【解説】
本節では、CP/CPS の管理組織、窓口、ポリシーに対する CP/CPS の準拠性調査担当者、CP/CPS の承認手続きについて規定する。相互認証を行う上では少なくとも CP/CPS の管理組織及び承認手続きについて規定する。

【記述例】

1.5.1　文書の管理組織

本 CP/CPS の管理については、本認証局の最高意志決定機関である○○が行う。

1.5.2 窓口
最高意志決定機関の窓口は以下の通りである。＊（存在しない場合は「規定しない」で良い）
組織名：
電話番号：
E-mail：

1.5.3 ポリシーに対する本 CP/CPS の準拠性調査担当者
ポリシーに対する CPS の準拠性調査を行う責任を負う者は○○である。
＊（特に規定しない場合は「規定しない」で良い。）

1.5.4 CP/CPS の承認手続き
本 CP/CPS の承認については、本認証局の最高意志決定機関である○○が

4.1.6 定義と略称

【解説】
本節では、用語及び略語の定義を行う。付録として巻末に記述しても問題はない。本ガイドラインでは付録とする。

4.2 公開とリポジトリの責任

【解説】
本節では、リポジトリにおいて公開する情報、リポジトリのサービス時間、アクセスコントロール等について規定する。相互認証を行う上で将来的に利用するサーバ、更新のタイミングについて調整が入る可能性が高い。

リポジトリは認証局が利用者及び検証者に対して公開、通知するために設置される Web サーバや LDAP サーバ、OCSP レスポンダ等である。失効情報の公開は通常、Web サーバ、LDAP サーバ、OCSP レスポンダのどれか、あるいは組合せで実施される。

【記述例】

2.1 リポジトリ
リポジトリは本認証局における証明書に関する事項を通知するために設置され、○○大学により運営される。リポジトリは原則として 1 日 24 時間、1 年 365 日利用可能とする。但し、定期保守作業等により、一時的にリポジトリを利用できない場合もある 。定期保守等、予め利用できないことが明らかな場合、事前に以下のリポジトリにおいて通知する。
http:// （URLを記述）

2.2 認証情報の公開
- CP/CPS の公開先
- 利用規約の公開先
- ARL の公開先
- CRL の公開先
- OCSP レスポンダ
- その他

2.3 公開の時期と周期
本認証局は、本 CP/CPS、あるいは利用規約が改訂され承認されたときは、速やかにこれを公開する。
CRL/ARL は「4.9.7 証明書失効リストの発行頻度」で示された発行周期で更新、公開する。＊（本節内で規定しても良い）

2.4 リポジトリに対するアクセスコントロール
参照権限の制限を行わない。情報の更新については、本認証局の権限ある者のみがアクセスできるよう管理される。

4.3 本人性確認と認証

4.3.1 名称

【解説】
本節では、利用者証明書に記載する issuerDN 及び subjectDN について準拠する規格、subjectDN に規定する個人を特定できる情報、利用者の匿名･仮名の許可･不許可等について規定する。相互認証を行う上で、証明書のみで利用者の氏名あるいは学籍番号を把握するニーズがなければ、DN は一意性が保たれればよく、CN（Common Name）に氏名や学籍番号を記載する必要はない。

【記述例】

3.1.1 名称のタイプ
本認証局が発行する利用者用証明書の主体者（Subject）である利用者は、利用者用証明書の中の X.500 識別名（DN）で一意に識別される。X.500 は、ITU-T で 1988 年に規格化されたディレクトリ･サービスの勧告（国際標準）である。

3.1.2 名称の意味に関する要件
利用者用証明書中の DN に含まれる固有名 CN には利用者を一意に識別可能な ID を指定する。
＊（CN に利用者名（ローマ字または、英字表記）を指定しても問題ない。）

3.1.3 利用者の匿名･仮名について
規定しない。
＊（CN に利用者氏名を指定している場合、「利用者の登録原票記載事項証明書における通称名、併記名については許可するが、これ以外の匿名、仮名、旧姓を許可しない。」といった規定をしても構わない。）

3.1.4 様々な名称形式を解釈するためのルール
参照権限の制限を行わない。情報の更新については、本認証局の権限ある者のみがアクセスできるよう管理される。

3.1.5 名称の一意性
本認証局が発行する証明書の DN は、「3.1.2 名称の意味に関する要件」に従い、CN により一意に割り当てる。

3.1.6 商標等の認識、認証及び役割
本認証局は、商標、ドメイン名について、認識、認証を行わない。

4.3.2 初回の利用者の本人性確認

【解説】
本節では、初回の利用者の確認方法、権限確認、相互運用性基準、更新時の本人性確認について規定する。

本人確認時において利用者の秘密鍵の保持を確認する場合があるが、先行大学が実施しているように利用者に鍵ペアの生成、証明書発行リクエスト（PKCS#10、PKCS#7 形式）を実施させず、認証局側で実施する方が利用者に無用な混乱を生じさせないメリットがある。従って、認証局内でセキュアなファシリティ、デュアルコントロールの下で、安全に利用者用鍵ペアを生成する方法を推奨する。

【記述例】

3.2.1 秘密鍵の所有を検証する方法
利用者秘密鍵は本認証局の認証設備室内において生成され、複数人コントロールの下で IC カードに格納、配付されるため、秘密鍵の所有を検証しない。
相互認証証明書を発行する場合、相互認証先 から提出される証明書発行要求（PKCS#10 形式）における相互認証証明書のフィンガープリント等の確認を行うことで、秘密鍵の所有を確認する。＊（相互認証の方式により、見直しが必要）

3.2.2 利用者の確認
利用者は、本学の学生、教職員、その他本学が認める者に限定される。利用者の本人性確認は、入学、進学、採用時等に行われ、本学に所属する利用者本人を特定する情報は本学内のデータベースにより管理される。このデータベースを信頼することにより利用者の確認を行う。

3.2.3 確認しない利用者の情報
規定しない。＊（規定すべきことがあれば、記載する。）

3.2.4 権限確認
本認証局は、代理人が利用者用証明書を申し込み、取得することを認めない。従って、権限の確認は行わない。

3.2.5 相互運用性基準
規定しない。＊（相互認証を行わない現段階での規定）
本認証局は、他の認証局と相互認証する場合、相互認証の実施及び終了については、相互認証先との調整の下、合意した手順に従い適切な判断、処理を行う。＊（相互認証の方式により、見直しが必要）

3.2.6 鍵更新時の本人性確認
利用者の証明書の有効期間満了に際し、鍵更新及び証明書の再発行を行う必要があるかどうかは、学内のデータベースにより確認する。

3.2.7 失効後の証明書再発行時の本人性確認
利用者の証明書の失効後に鍵更新及び証明書の再発行を行う場合は、学内のデータベースとの照合により確認する。

4.3.3 失効申し込み時の本人性確認と認証

【解説】
本節では、利用者が証明書の失効申請を行う場合の利用者の本人性確認と認証について規定する。失効に際しては、IC カードの紛失といった緊急性の高い場合とそうでない場合が存在するため、両方の場合について規定する。

緊急失効の際、電話での受付けを行い、コールバックで本人確認を行うことを規定した場合、予め利用者に連絡するための電話番号（研究室電話番号、携帯電話等）を認証局が知る必要があるため、これを安全に入手、管理しておく必要がある。

【記述例】

3.3 失効申し込み時の本人性確認と認証

利用者本人による失効申し込みの場合、本認証局は利用者用証明書の失効申込者が利用者本人であることの真偽確認を以下のように実施する。

(1) 利用者本人が登録窓口に○○申請書並びに IC カードを提出する。
(2) 登録窓口担当者は、IC カード券面に印刷された顔写真および学内のデータベースと照合し、本人性を確認する。

なお、IC カード紛失等の緊急の場合は、窓口での申請並びに電話連絡による申請を受付ける。この際には、学内データベースとの照合あるいは、利用者にコールバックを行う等、利用者を特定できる方法により本人性の確認を行う。

4.4 証明書のライフサイクル

4.4.1 証明書申し込み

【解説】
本節では、証明書の申込者、申し込み方法、登録手続きと責任について規定する。利用者に申請書を提出させ、認証局が登録を行う場合と、利用者が申請したものとみなし、認証局が登録を行う場合とが想定されるが、いずれも発行すべき利用者本人に対し、確実に証明書の発行を行えるよう規定する必要がある。

将来、相互認証を行う際に、相互認証証明書を発行する場合、相互認証証明書の発行申し込み、手続きに関しても規定する必要がある。

【記述例】

4.1.1 証明書申請を提出することができる者
本認証局の証明書の申請を行える者は、〇〇大学の教職員、学生、本学が認める者とする。
相互認証証明書の発行申請を行うのは認証局責任者であり、認証局責任者は最高意志決定機関である〇〇に対して証明書発行の申し込みを行い、〇〇の承認を得て発行局に発行の指示を行う。＊（相互認証の方式により、見直しが必要）

4.1.2 登録手続きと責任
利用者は本 CP/CPS、利用規約、個人情報保護方針について承認した上で本認証局に対し、〇〇に定める申請書類一式を提出あるいは郵送する。
本認証局に提出された申請書類及びすべての書類は、原則利用申込者に返却せず、本認証局に保管される。
なお、申し込みに係る書類の受領後、これら必要書類の不備確認が完了した時点を受理とする。
＊（認証局が利用者本人に代わって申請を行う場合、「本認証局は、〇〇大学の教職員、学生の採用、入学等を以って、利用者が証明書の申請を行ったものとみなし、登録局により証明書の一括登録、発行局への発行指示を行う。」等と規定する。）

登録局は複数人により審査･登録業務を行い、発行局に対する発行指示を行う。

相互認証の開始時においては、最高意志決定機関である〇〇の承認後、相互認証証明書の発行を行う。
相互認証の開始は、相互認証先と合意した安全な手順により実施する。＊（相互認証の方式により、見直しが必要）

4.4.2 証明書申請手続き

【解説】
本節では、CP/CPS3.2 節と重複していることでもあるが、申請手続きの際の本人性確認について規定する。更に、証明書申請の承認または却下の条件、証明書申請の処理時間について規定する。

【記述例】

4.2.1 本人性確認と認証機能の実行
本認証局は、「3.2.2 利用者の確認」に定められた方法で利用者の本人性確認を行う。

4.2.2 証明書申し込みの承認または却下
登録局は利用者が提出する書類の不備等を確認し、受理する。その後、登録局が「3.2.2 利用者の確認」に規定する本人性の真偽確認を行い、承認を行う。定められた利用申し込み以外の方法による申し込みであった場合や本人性の真偽において疑義が生じた場合等、利用者用証明書の申し込みを却下する。＊（利用者の申請を必要とせず、入学や採用時等のタイミングで認証局が発行する場合は、この手続きは存在しないため、次のように規定する。「登録局は、証明書の発行を必要とする教職員、学生が存在する場合、証明書の発行を承認する。」等）

4.2.3 証明書申請の処理時間
本認証局は、申請を承認した後に、速やかに証明書発行の処理を行う。＊（利用者の申請が不要な場合、次のように規定する。「登録局は、教職員の採用並びに学生の入学等に際し、可能な限り速やかに証明書の発行を行う。」等）

4.4.3 証明書発行

【解説】
本節では、証明書発行時の認証局、登録局の行為及び利用者に対する証明書の発行通知に関して規定する。

利用者の証明書格納媒体として、IC カード、利用者の利用するコンピュータ、PKI に対応した USB トークン等が考えられる。しかし、利用者 PC ではその利用が固定的になる等の問題があり、USB トークンではパーソナライズや大量発行に向かないといった問題が生じる。本ガイドラインでは認証局において利用者の鍵生成を行い、証明書発行後、IC カードへの格納を行うことを推奨している。

従って、本節においては、以下について明確に規定している必要がある。

- 鍵生成に関する記述
- 証明書発行
- IC カード格納
- IC カード PIN の管理
- IC カード及び IC カード PIN の配付

将来、相互認証を行う際に相互認証証明書を発行する場合、相互認証証明書の発行に関しても同様に規定する必要がある。

【記述例】

4.3.1　証明書発行時の本認証局の行動

- 自己署名証明書＊（セルフサインの認証局の場合）

認証局責任者は自己署名証明書の発行について、最高意志決定機関である○○の承認を得る。認証局責任者は承認された自己署名証明書発行を発行局に指示し、発行局では認証設備室内において複数人コントロールの下、本認証局秘密鍵の漏えい、破損、消失等の事象の発生を可能な限り低い確率に抑える機器を用いて鍵ペアを生成し、その後自己署名証明書を発行、管理する。

- 利用者用証明書

本認証局は、利用者の鍵ペア及び利用者用証明書を複数の操作者の操作により、本認証局の認証設備室内で安全に生成し、発行する。生成された鍵及び発行された利用者用証明書は、複数人コントロールの下、IC カードに格納する。本認証局は、利用者に、原則対面で IC カードを配付するが、郵送する場合、配達記録郵便にて配付する。IC カードを活性化する IC カード PIN 通知書は IC カード配付時に利用者へ対面で配付するが、郵送する場合、学内郵便、配達記録郵便等で別送する。

- 相互認証証明書

相互認証証明書の発行の際、相互認証証明書の有効期間は、相互認証証明書に係る本認証局の有効な公開鍵の残存有効期間内であるものとする。相互認証証明書の発行において、認証局責任者は○○の承認を得る。認証局責任者は承認された相互認証証明書発行を発行局に指示し、発行局では証明書発行要求（PKCS#10 形式）を作成する。認証局責任者は、証明書発行要求と証明書発行要求のフィンガープリントを相互認証先 へ送付し、相互認証証明書の発行依頼をオフラインで行う。また、相互認証先 よりオフラインで提供される証明書発行要求（PKCS#10 形式）を証明書発行要求のフィンガープリント等で確認を実施し、相互認証証明書を発行する。本認証局は、発行した相互認証証明書とフィンガープリントをオフラインで相互認証先 へ配付し、相互認証先 が発行する相互認証証明書をフィンガープリント等で確認する。認証局責任者は相互認証証明書をフィンガープリント等で確認を実施し、発行局にリポジトリへ登録するように指示する。発行局は相互認証証明書をリポジトリに登録する。相互認証証明書の発行手順の詳細は、相互認証先 と合意した安全な手順により実施する。＊（相互認証の方式により、見直しが必要）

4.3.2　利用者に対する証明書発行通知

利用者への利用者用証明書発行の通知は、IC カード及び IC カード PIN 通知書を配布することにより行う。

相互認証先への相互認証証明書発行通知は、相互認証証明書をオフラインで相互認証証明書のフィンガープリントと共に送付することにより行う。＊（相互認証の方式により、見直しが必要）

4.4.4 証明書受領

【解説】
本節では、利用者が証明書を受領した際の受領確認手続き、認証局が発行した利用者証明書をリポジトリ等で公開するか否か、利用者以外に証明書の発行の通知を行うかを規定する。受領手続きについては、利用者に証明書（IC カード）の受領書を提出させるか、配付した記録を残す等、何らかの記録を残すことが望ましい。

将来、相互認証を行う際に、相互認証証明書を発行する場合、相互認証証明書の受領手続きに関しても規定する必要がある。

【記述例】

4.4.1 証明書受領手続き
- 利用者証明書

本認証局は、IC カード及び IC カード PIN を配付した際に、利用者本人に対し受領書の提出を求める。＊（あるいは「本認証局は、利用者本人に対し、IC カード及び IC カード PIN を配付した記録を残す。」等）
- 相互認証証明書

オフラインにて相互認証接続先と取り交わすとともに、リポジトリにて公開を行い、受領確認を行う。相互認証証明書の受領確認は相互認証先の規定の手順によって行う。＊（相互認証の方式により、見直しが必要）

4.4.2 本認証局による証明書の公開
利用者用証明書は公開する義務を負わない。
相互認証証明書はリポジトリ上で公開する。＊（相互認証の方式により、見直しが必要）

4.4.3 他のエンティティに対する認証局の証明書発行通知
規定しない。＊（あるいは「本認証局は、第三者に対する証明書の発行通知は行わない。」等）

4.4.5 鍵ペアと証明書の用途

【解説】
本節では、利用者が自身の利用者秘密鍵と証明書の使用を行う際の用途、検証者が利用者の公開鍵と証明書を使用する際の用途について規定する。

【記述例】

4.5.1 利用者による秘密鍵及び証明書の使用
利用者は秘密鍵及び証明書の利用に際し、以下を遵守しなければならない。
(1) 証明書の用途
本 CP/CPS1.4.2 に示した証明書の用途以外に秘密鍵及び利用者用証明書を利用してはならない。
(2) 利用制限
利用者は鍵ペア及び利用者用証明書を、有効期限を越えて利用してはならない。

4.5.2 検証者による公開鍵及び証明書の使用
検証者は電子認証における復号の用途及び本認証局及び利用者の証明書の有効性の検証の用途で、利用者の公開鍵と利用者用証明書を利用する。利用者用証明書の利用に際しては、「9.6.3 検証者の表明保証」及び「9.16.5 不可抗力」に記述された内容について承諾しなければならない。

4.4.6 鍵更新を伴わない証明書の更新

【解説】
鍵更新を伴わない証明書の更新は混乱を伴うことが予想されるため、一般的には実施されることは少ない(リンク証明書の場合実施しているケースがある)。従って、明確な理由がない限り、本節は鍵ペアを更新することを規定する。

【記述例】

全ての証明書の更新は必ず鍵ペアの更新を伴うこととし、その要件については「4.7 鍵更新を伴う証明書更新」に規定する。

4.4.7 鍵更新を伴う証明書の更新

【解説】
本節では、鍵更新及び証明書の更新時の手続きについて規定する。

将来、相互認証を行う際に相互認証証明書を発行する場合、相互認証証明書の更新手続きに関しても規定する必要がある。

新規発行時と更新時で発行手続きが異なる場合は、詳細に規定しなければならない。以下の例は新規発行と更新時の手続きが同じ場合の例である。

【記述例】

4.7.1 更新事由

- 自己署名証明書（セルフサインの認証局の場合）

本認証局は、自己署名証明書の有効期間内に新しい鍵ペアを生成し、証明書を発行する。

- 利用者用証明書

本認証局は、利用者用証明書の有効期限が切れることにより、利用者が保持する既存の鍵ペアの有効期限を延長せず、新しい鍵ペア（新たに生成される鍵ペア）の公開鍵に対する新しい利用者用証明書を発行する。利用者は、「4.1 証明書申し込み」に示す新規の証明書発行申込手続きと同様の手続きを行う。

- 相互認証証明書

相互認証証明書は、本認証局の鍵ペア及び証明書が更新された際に、「4.1 証明書申し込み」に示す新規の証明書発行申込手続きと同様の手続きを行う。＊（相互認証の方式により、見直しが必要）

4.7.2 新しい利用者証明書の発行申請が出来る者

本 CP/CPS4.1.1 と同様とする。

4.7.3 証明書の鍵更新申請の処理

本 CP/CPS4.3.1 と同様とする。

4.7.4 利用者に対する新しい証明書の通知

本 CP/CPS4.3.2 と同様とする。

4.7.5 鍵更新された証明書の受領確認

本 CP/CPS4.4.1 と同様とする。

4.7.6 認証局による更新済みの証明書の公開

本 CP/CPS4.4.2 と同様とする。

4.7.7 他のエンティティに対する認証局の証明書発行通知

本 CP/CPS4.4.3 と同様とする。

4.4.8 証明書の変更

【解説】
基本的には証明書の変更に関して規定するが、IC カードの券面の変更に際しても同様の処理を行う場合は、変更条件として明記する。本人を特定できることが前提であるが、証明書及び IC カードの券面情報の変更は必須事項でなく、希望者のみという運用でも問題ないと考えられる。

【記述例】

4.8.1 証明書変更に関する要件
利用者は証明書情報、あるいは IC カードの券面情報の変更を希望する場合、本認証局に失効及び新規発行の申請を行うことが出来る。

4.8.2 証明書の変更を申請できる者
変更を希望する利用者本人とする。

4.8.3 変更申請の処理
利用者は本 CP/CPS4.9 に示す失効申請、並びに本 CP/CPS4.1.2 に示す発行申請を行わなければならない。

4.8.4 利用者に対する新しい証明書の通知
本 CP/CPS4.3.2 と同様とする。

4.8.5 変更された証明書の受領確認の行為
本 CP/CPS4.4.1 と同様とする。

4.8.6 認証局による変更された証明書の公開
本 CP/CPS4.4.2 と同様とする。

4.8.7 他のエンティティに対する認証局の証明書発行通知
本 CP/CPS4.4.3 と同様とする。

4.4.9 証明書の失効と一時停止

【解説】
本節では、証明書は、利用者、認証局のそれぞれの失効事由により失効するため、それぞれについて規定する。想定されていない失効事由が発生した場合、認証局責任者の判断に基づき証明書を失効できるよう規定しておく必要がある。

また、IC カードの紛失等、緊急を要する失効手続きとそうでない場合の手続きについて違いがある場合は、それについても規定する必要がある。

将来、相互認証を行う際に相互認証証明書を発行する場合、相互認証証明書の失効に関しても規定する必要がある。

【記述例】

4.9.1 失効事由
⑴ 利用者用証明書
⒜ 利用者による失効事由
- IC カードを紛失･盗難した場合など、自らが所有する秘密鍵が危殆化もしくは危殆化の恐れがある場合
- IC カードの破損等により IC カードが使用不可能となった場合
- 利用者用証明書の記載内容あるいは IC カードの券面を変更したい場合
- 利用者用証明書の利用を中止する場合

⒝ 本認証局による失効事由
- 利用者が○○大学に所属しなくなった場合
- 本認証局が利用者の不正利用を確認した場合
- 本認証局の秘密鍵が危殆化もしくは危殆化の恐れがある場合
- 本認証局が認証業務を廃止する場合

⑵ 相互認証証明書＊（相互認証の方式により、見直しが必要）
(a) 相互認証先による失効事由
- 相互認証を停止する場合
- 相互認証先認証局の秘密鍵が危殆化もしくは危殆化の恐れがある場合
- 相互認証先が業務を廃止する場合
- 認証ポリシーの変更がある場合
- その他、相互認証先 が必要と判断した場合

(b) 本認証局による失効事由
- 相互認証を停止する場合
- 本認証局の秘密鍵が危殆化もしくは危殆化の恐れがある場合
- 本認証局が業務を廃止する場合
- 相互認証基準違反がある場合
- 認証ポリシーの変更がある場合
- その他、本認証局が必要と判断した場合

【記述例】

4.9.2 証明書の失効申請が出来る者
証明書の失効の申請が出来る者は、失効事由に応じて利用者本人及び認証局責任者、相互認証先＊（相互認証の方式により、見直しが必要）である。

4.9.3 証明書の失効申請手続き
（1）利用者による通常の失効申請手続き
利用者が「4.9.1 失効事由」に定める失効事由により、利用者用証明書を失効しなければならないと判断した場合、○○申請書を本認証局に提出しなければならない。本認証局は、失効申込者の真偽確認の結果、正当であると認められた場合、失効処理を行う。
（2）利用者による緊急の失効申請手続き
IC カードの紛失等、利用者用証明書の緊急な失効が必要な場合、これを電話連絡により本認証局に要求することができる。
本認証局は、可及的速やかに失効申込者の真偽確認を行い、失効が正当であると認められた場合は失効処理を行う。緊急失効時においては、本認証局側からのコールバック等により失効申込者の失効が正当であると認められた場合は、失効処理を行う。
（3）本認証局による失効手続き
本 CP/CPS4.9.1 に示す事由が生じた場合、認証局責任者の判断により、本認証局が利用者用証明書を失効する。

4.9.4 失効申請の猶予期間
利用者あるいは認証局責任者は、本 CP/CPS4.9.1 に示す事由に気付いた時、遅滞なく失効の申請を行わなければならない。

4.9.5 認証局が失効申請を処理しなければならない期間
本認証局は、失効の申請が発生した場合、サポート時間の範囲で速やかに本人性の真偽確認を行い、失効可否を判断する。本認証局は、失効が承認された場合、速やかに失効処理を行う。

4.9.6 検証者の失効確認の要求
検証者は、リポジトリに格納された CRL/ARL により証明書の失効リストを確認しなければならない。

4.9.7 証明書失効リストの発行頻度
本認証局は、CRL の発行を前回の発行から 24 時間ごとに行う。

4.9.8 証明書失効リストの発行最大遅延時間
本認証局は発行した CRL を前回リポジトリに格納してから 24 時間ごとに格納する。

【記述例】

4.9.9　オンラインでの失効ステータス確認の適用性
本認証局は、利用者の証明書の有効性について OCSP レスポンダを利用し、オンラインで失効情報を提供している。＊（OCSP レスポンダを利用していない場合、「本認証局は、CRL/ARL 以外の失効リスト検査手段を提供しない。」等）
また、有効期間の満了した証明書の有効性確認についての問い合わせには応じない。

4.9.10　オンラインでの失効/ステータス確認を行うための要件
検証者は、利用者の証明書ステータスについて、CRL の代わりに、OCSP レスポンダの応答により確認できる。＊（OCSP レスポンダを利用していない場合、「規定しない。」等）

4.9.11　利用可能な失効通知の他の形式
規定しない。＊（規定すべきことがあれば規定する）

4.9.12　鍵更新の危殆化に対する特別要件
規定しない。＊（規定すべきことがあれば規定する）

4.9.13　証明書の一時停止
本認証局は、証明書の一時停止を行わない。

4.9.14　相互認証証明書の失効＊（相互認証の方式により、見直しが必要）
本認証局は相互認証先より書面にて相互認証証明書の失効の申し込みが行われた場合、〇〇の検討及び承認後、相互認証証明書を失効する。失効申し込みは、以下の情報が明記された書面にて行われなければならない。

- 失効対象となる相互認証証明書を一意に識別するための情報
- 失効事由
- 失効日時

失効結果については、ARL に記載し公表することに加えて、要求元に対して通知を行う。
本認証局の理由により、相互認証証明書の失効申し込みを行わなければならない場合も同様に、書面によって失効の申し込みを行う。失効の事由が本認証局の業務の終了を意味している場合、その手続きに則る。

4.4.10 証明書のステータス確認サービス

【解説】
本節では、CRL/ARL 及び OCSP レスポンダによる証明書のステータス確認について規定する。

【記述例】

4.10.1 運用上の特徴
利用者の証明書ステータスは CRL、あるいは OCSP レスポンダにより確認することができる。認証局証明書のステータスは ARL により確認することができる。

4.10.2 サービスの利用可能性
証明書ステータスに関するサービスは 2 章において規定するリポジトリにおいて提供する。

4.10.3 オプショナルな仕様
規定しない。＊（規定すべきことがあれば規定する）

4.4.11 利用の終了

【解説】
本節では、利用者が退職、退学等により証明書の利用を終了する際の手続きについて規定する。

【記述例】

利用者が証明書の利用を終了する場合、「4.9.3 証明書の失効申請手続き」に定めた手続きと同様とする。

4.4.12 キーエスクローとリカバリ

【解説】
本節では、利用者の鍵のエスクロー（預託）、リカバリ（回復）について規定する。キーエスクローとリカバリのサービスは、認証局が利用者の鍵の複製を保管し、利用者、あるいは大学が認めた者に対し、必要な時（鍵データが破損した場合、暗号を復号したい場合等）に複製を提供するサービスである。

しかし、このサービスは利用者用証明書の用途によって向き不向きがある。例えば、電子署名の場合、利用者本人だけが鍵を持ちえることによって、その電子署名が利用者本人によってなされたと見なされる必要があり、このサービスの利用にはむいていないと言える（認証局が複製を保持しているため）。

また、クライアント認証の用途においては、リカバリする理由によっては失効・再発行が望ましいケースがあり、また、リカバリ先の利用者を新規発行時と同様の本人確認と在籍確認をする必要がある。

暗号の用途の場合、過去に暗号化したデータを利用者、あるいは権限のある者が復号化する必要がある場合があり、過去の鍵をリカバリするためにサービスが有効なケースである。しかし、クライアント認証と同様に長期間に渡る鍵の管理や、本人あるいは権限者の確認等は非常に煩雑な運用を強いられる可能性が高い。

キャンパス PKI を暗号の用途で用いていない現状では、このようなサービスを提供する意義は少なく、安全性を一定レベルに維持するためには、運用上も煩雑であるため、提供しないことが望ましい。

【記述例】

本認証局は、キーエスクロー及び鍵のリカバリを行わない。

4.5 設備、管理、運用上の統制

4.5.1 物理的管理

【解説】
本節は、認証局を構成する重要な設備の設置場所について、その立地や構造、様々な設備について規定する。本ガイドラインでは、少なくとも発行局についてのアウトソースが前提条件であるため、発行局の要件はアウトソース先に課されるものとなる。

RA サーバをインソースで運用する場合は、発行局に近いセキュリティレベルの施設を備える必要がある。

オフサイトバックアップについては必須としないが、大規模な障害や災害に備える必要はある。オフサイトバックアップに加え、ローカルでのバックアップや二重化等の要件は各大学において判断する必要がある。

以下の例においては、IA サーバ、RA サーバの運用及び IC カード発行業務をアウトソースする場合を示す。RA サーバをインソースで運用する場合は、RA サーバを設置する部屋についても同様に規定する必要がある。

【記述例】

5.1.1　立地場所及び構造
認証設備を収容する建築物の外部及び建築物内に認証設備の所在を明示または暗示する名称を、看板もしくは表示板等により建物内外に一切掲示しない。
(1) 認証設備室及び IC カード発行室
鍵生成及び証明書の発行処理、失効処理、IC カード作成等のオペレーションを行う場所であり、そのための設備、システムが存在する。認証設備を収容する建築構造物は停電、地震、火災及び水害その他の災害の被害を容易に受けないよう防止策を講じている。発行局認証設備室は隔壁による独立した区画であり、入室権限を有しない者の入室は原則認められないが、やむを得ずこれを認める場合、予め許可を得て、入室権限者との帯同の上、入室させる規定とする。
また、認証設備の操作は、許可された者のみが行うことができる。所在については非公開とする。
(2) 登録端末設置室
申請受付、審査、登録端末を用いた利用者用証明書の発行指示、失効指示等のオペレーションを行う場所であり、そのための設備、端末が存在する。登録局システムの操作は予め登録された操作権限者でなければ行うことができない。

5.1.2　物理的アクセス
認証設備室への入室は予め警備システムにおいて入室権限者を登録する必要がある。入室の度に予め入室権限を付与された複数人の入室権限者が同時に生体認証装置による認証、識別操作を行うことが必要である。認証設備室への入退室の情報は、記録、管理される。入退室に関するログは、定期的にチェックし、認証設備室への入室が許可されている者が警報を発報した場合の警備システムの異常ログについても、定期的にチェックする。入室権限を有しない者が認証設備室に入室する場合は、入室権限を有する複数人の同行が必要である。入室権限を持たない者の入室時は入室目的を確認する。また入室権限を有し同行した 2 名の職員は、同行の記録を残し、これを定期的にチェックする。
認証設備室への入退室については以下の管理が実施されている

- 2 人による生体認証装置の識別、認証操作による入室
- 入室操作に要する時間、試行回数の制限
- 不正な操作による開扉があった場合の通報
- 入室の際、入室者数と同人数の退室を確認
- 遠隔監視カメラによる継続的な監視の実施及びその記録

【記述例】

5.1.3　電源及び空調
認証局の電源設備は運用に十分な電源容量を確保した無停電電源装置である。無停電電源装置とは、瞬断しないように電源そのものに UPS の機能が備わっており、かつ電源が供給されない事態に備えて発電機を用意し、一定時間内に発電機による電源供給に切り替える仕組みを持つ電源のことを指す。
また、空気調和機を用意し、機器類の動作環境及び要因の作業環境を適切に維持する。

5.1.4　水害対策
認証設備室は容易に水害の被害を受けない場所に設置する。また、空気調和機には、防水提と漏水検知器を設置する。

5.1.5　火災防止及び火災保護対策
建物は耐火構造である。認証局の機器は建物の防火区画内に設置する。また、自動火災報知機や消火設備を備える。

5.1.6　媒体保管場所
アーカイブデータ、バックアップデータ等を記録した媒体は施錠のできる書庫もしくは金庫に保管し、媒体の搬入管理を行う。また、媒体の保管場所には、地震、火災、水害対策を講じる。

5.1.7　廃棄処理
秘密鍵、利用者の個人情報等の重要な本認証局の情報が記録された文書及び記憶媒体を廃棄する場合、物理的に完全に破壊するか、廃棄物よりデータを復元することを不可能にする措置を講じる。

5.1.8　施設外のバックアップ
本認証局の運用に必要なデータ、機器等は、遠隔地に保管するか、あるいは調達できる手段を講じる。

4.5.2 手続き的管理

【解説】
本節では、認証局における役割に応じ、必要な最低人数、兼務の可否等を規定する。フォーカスすべきポイントは、内部けん制が出来ているかどうかであり、不正が起こりえる手続きを回避する必要がある。

【記述例】

5.2.1 信頼すべき役割
本認証局は、次の職制を信頼する。
- 最高意志決定機関○○
- 認証局責任者
- 発行局委託先責任者
- 発行局オペレータ
- 登録局責任者
- 登録局オペレータ
- 認証システム管理者
- その他本認証局が認めた者

5.2.2 職務ごとに必要とされる人数
次の職制については少なくとも 2 名の職員が個々の発行及び失効業務に携わるよう規定する。
- 発行局オペレータ
- 登録局オペレータ

5.2.3 個々の役割に対する本人性の確認と認証
認証設備へのアクセスには、IC カードを使用した認証を必要とする。

5.2.4 職務分割が必要となる役割
- 最高意志決定機関○○の代表者と認証局責任者
- 登録局責任者と登録局オペレータ
- 発行局委託先責任者及び発行局オペレータと認証システム管理者

4.5.3 人事的管理

【解説】
本節では、CP/CPS5.2.1 に規定した職制の要員に対する要件及び教育に関する要件を規定する。

【記述例】

5.3.1　経歴、資格、経験等に関する要求事項
本認証局の職員はその職制に応じて本認証局業務についての教育･訓練後、業務に配置する。

5.3.2　教育訓練要件
本認証局は、職員に対して職制に応じ、業務を円滑に遂行するために必要な教育訓練を受けることを課す。

5.3.3　教育訓練の周期
業務を開始する前に必要な教育･訓練を受けるものとし、その後十分な知識、経験をもち、職務を遂行する上で十分な素養を備えている者に対する再教育は省略することが出来るものとする。
本認証局の運用が変更された場合、臨時の教育訓練を行う。

5.3.4　ジョブローテーションの周期と順序
規定しない。＊（「内部けん制を実現できる適切なジョブローテーションを行う。」等、規定すべきことがあれば規定する）

5.3.5　許可されていない行動に対する罰則
過失、故意に関わらず、本 CPS で規定されたポリシー、手続き及び本認証局が定める手順に違反したと認められた場合、認証局責任者が速やかに調査を行い、適切な罰則を適用する。

5.3.6　職員に対する契約要件
発行局運用業務を外部の組織に業務委託する場合、本学 と業務委託先との間で秘密保持契約を締結するものとし、業務委託先の従業員はその契約で締結される秘密保持義務を遵守するものとする。

5.3.7　職員が参照できるドキュメント
本認証局の職員はその役割、権限に応じたドキュメントを参照することができる。

4.5.4 監査ログの手続き

【解説】
本節では、監査対象となる記録の種類、保管期間、記録の保護等について規定する。証明書の発行及び失効といった重要なイベントに関する記録、運用規程や下位文書に関する記録、体制及び契約に関する記録、監査に関する記録は重要な記録であるため、これらの保管期間、バックアップ、保護について規定する必要がある。

なお、OS やネットワーク、入退室の記録については、監査終了後、監査の記録を残した上で破棄しても問題ないと考える。

重要な情報の保管期間については証明書の用途が認証であるため、10 年を越えるような長期間の保管義務は生じないと考える。ただし、将来的に電子署名の用途が付加された場合は、長期間の要件が課される場合が多いと考えられ、証明書の有効期間を越えて何年保管すべきか大学側で判断する必要が生じる。

【記述例】

5.4.1　記録されるイベントの種類
以下に関するログ、文書、データ等を記録する。
- 本認証局が発行する電子証明書のライフサイクル等に関する記録
- 認証設備、登録端末設備等の管理に関する記録
- 認証局運用規程及び手続きに関する規定の管理に関する記録
- 組織体制等の管理に関する記録
- 監査等に関する記録

5.4.2　監査ログを処理する頻度
本認証局は、本 CP/CPS5.4.1 に定める記録を定期的に確認する。

5.4.3　監査ログを保持する期間
本 CP/CPS5.4.1 に規定する重要な記録は少なくとも 5 年以上保管する。ただし、証明書のライフサイクルとは関係のないシステムログ、入退室ログ等の運営記録については、少なくとも次の監査終了まで保管されるものとする。

5.4.4　監査ログの保護
各記録は漏えい、滅失またはき損防止のため、適切な措置を講ずる。

5.4.5　監査ログのバックアップ手続き
電子データのバックアップを取得する場合、複数人により安全な環境で行う。紙媒体については原本のみを安全に保管する。

5.4.6　監査ログの収集システム
審査登録業務及び発行業務に関わるサーバにおいて情報の収集がなされる。収集された記録については、「5.4.4 監査ログの保護」で規定された保護がなされる。

5.4.7　イベントを起こしたサブジェクトへの通知
本認証局は、監査ログの収集をそのイベントを発生させた者（人、アプリケーション）に対して通知することなく行う。

5.4.8　脆弱性評価
本認証局は監査等において脆弱性の評価を行う。脆弱性が発見された場合、認証局責任者は速やかにその問題を解決する。

4.5.5 記録のアーカイブ

【解説】
本節では、監査ログとして定義された記録に加え、保管対象となるデータ、文書を規定し、規定したそれぞれについて保管期間及び保護に関する規定を行う。

【記述例】

5.5.1　アーカイブ記録の種類
本認証局は、本 CP/CPS5.4.1 で規定する監査ログに加え、認証局証明書、利用者証明書、相互認証証明書＊（相互認証の方式により、見直しが必要）及び ARL、CRL をアーカイブする。

5.5.2　アーカイブ保持期間
本 CP/CPS5.4.3 と同様とする。

5.5.3　アーカイブの保護
本 CP/CPS5.4.4 と同様とする。

5.5.4　アーカイブのバックアップ手続き
本 CP/CPS5.4.5 と同様とする。

5.5.5　記録にタイムスタンプを付ける要件
本 CP/CPS5.4.1 及び 5.5.1 の記録は、日付あるいは日時が記録される。

5.5.6　アーカイブ収集システム
本 CP/CPS5.4.6 と同様とする。

5.5.7　アーカイブの情報を入手し検証する手続
本 CP/CPS5.4.1 及び 5.5.1 で規定された記録は、可用性と完全性が確保された形で保存される。

4.5.6 鍵の切り替え

【解説】
本節では、認証局の秘密鍵に関する鍵更新について規定する。認証局は鍵更新に際して新たな証明書の発行を行うが、この時リンク証明書を発行し、認証局の世代管理を行う場合がある。リンク証明書は、古い鍵で新しい証明書に電子署名を行い、新しい鍵で古い証明書に電子署名を行った 2 つの証明書からなる。リンク証明書が発行されれば、旧認証局と新認証局が同じ認証局であることを表明することができ、操作についても新しい認証局で古い認証局から発行された証明書を失効する等が出来る。

リンク証明書を発行せずに認証局が鍵更新をした場合は、全く別の認証局と見なされるが、CP/CPS を引き継ぐ等、同じポリシーで運用される認証局であることを表明することは可能である。

一方でリンク証明書が発行されている場合、通常の認証パスにおける有効性検証に加え、リンク証明書の有効性を検証する必要があるため、認証に要する時間がかかるといった問題も存在している。また、リンク証明書を検証しないアプリケーションが多く存在しているといった現状も存在する。現在の状態を鑑みて、現段階ではリンク証明書の発行は行わないことが望ましいと考えるが、将来的には見直す余地があるものと考える。

【記述例】

本認証局は、認証局の秘密鍵に対応する証明書の有効期間が加入者の証明書の最大有効期間よりも短くなる前に、新たな秘密鍵の生成を行う。新たな秘密鍵が生成された後は、新しい秘密鍵を使って、証明書及び ARL、CRL の発行を行う。また、古い秘密鍵では証明書の発行は行わず、ARL、CRL の発行のみを行う。

4.5.7 危殆化及び災害からの復旧

【解説】
本節では、システム的な障害、自然災害、認証局の秘密鍵の危殆化といった障害、災害が発生した際の手続き及び復旧に関する手続きについて規定する。

重要な認証設備及び失効情報を提供するﾘﾎﾟｼﾞﾄﾘ等については、各大学において、ﾊﾞｯｸｱｯﾌﾟ要件、二重化要件を定め、障害復旧のための手続きを規定しておくことを推奨する。

将来、相互認証を行った場合に、大規模な障害、災害が発生した際は、速やかに相互認証先に通知し、また、その対応方針について報告を行う必要があると考えられる。

【記述例】

5.7.1　事故及び危殆化の取り扱い手続き
本認証局は、以下の項目を含む不測の事態、災害が発生した場合、速やかに復旧計画を策定する。
- 鍵が危殆化するような事態
- ハードウェア、ソフトウェア、通信に関連する故障、不具合
- 火災、洪水等の自然災害

5.7.2　コンピュータの資源、ソフトウェア・データが破損した場合
本認証局は、機器、ソフトウェア、データ等の障害の発生に備えるために必要な措置を行う。また、障害が発生した場合には、復旧計画に従い、適切な措置をとる。障害発生時の際は、利用者、信頼者への障害情報の通知を、ﾘﾎﾟｼﾞﾄﾘへの公開により行う。
「CRL/ARL の更新が停滞し CRL/ARL の有効期限がきれるような事態が発生した」場合、速やかに相互認証先 へ通知する。＊（相互認証の方式により、見直しが必要）

5.7.3　災害後の事業継続能力
認証局秘密鍵の危殆化の恐れがない場合、復旧計画に基づいて復旧する。
また、相互認証先に復旧に関する報告を行う。＊（相互認証の方式により、見直しが必要）

4.5.8 認証局の業務終了

【解説】
本節では、認証局が業務を終了する際の手続きについて規定する。

将来、相互認証を行った場合、認証局の業務の終了については事前に相互認証先に通知する必要があると考えられる。

【記述例】

本認証局が認証業務を廃止する場合、廃止日の 3 ヶ月前までにﾘﾎﾟｼﾞﾄﾘ上で告知、あるいは利用者に対し書面による通知を行う。さらに、有効な利用者用証明書の全てと相互認証証明書を廃止日までに失効し、バックアップを含む全ての本認証局秘密鍵を削除する。また、利用者用証明書の信頼者、相互認証先に対して、認証業務の廃止、発行済み証明書の失効処理方法等の通知を行う。＊（相互認証の方式により、見直しが必要）

本認証局は、業務終了時、発行した全ての有効な証明書の有効期間を包含する有効期間を持った CRL/ARL を作成し、CRL/ARL が有効な間、ﾘﾎﾟｼﾞﾄﾘにて公開する。この際、CRL/ARL は日次での更新は行わない。

4.6 技術的セキュリティ管理

4.6.1 鍵ペアの生成及びインストール

【解説】
本節では、利用者及び認証局の鍵生成、秘密鍵及び公開鍵の配付、認証局証明書の配付、鍵サイズや品質検査について規定する。鍵のアルゴリズム、鍵長については、CRYPTREC や IPA が公開している電子政府推奨アルゴリズムに従い、かつ、より一般的なアプリケーションにおいて利用可能なものを選択するものとする。

キャンパス PKI としては、2007 年度以降に構築される認証局証明書は、最も長い有効期間を持つ利用者用証明書（例えば 6 年）に合わせた 10 年未満の有効期間を持つことが合理的であると考える。

将来、証明書の利用用途の範囲が拡大（電子書名の用途等）する場合や相互認証を行うにあたり、鍵の用途は変更（追加）される可能性がある。また、鍵のアルゴリズム及び鍵長については、電子政府推奨アルゴリズム等[1]の最新の情報によって、定期的に見直される必要があり、その際は本節の規定が変更されることが予想される。

【記述例】

6.1.1　鍵ペアの生成
(1)本認証局の鍵ペア生成
アクセスコントロールがなされる認証設備室内において、発行者署名符号の生成は、複数名の操作により、暗号装置の中で行われる。
(2)利用者の鍵ペア生成
利用者の鍵ペアは、登録局の権限ある複数人の審査、承認を経て、アクセスコントロールされる認証設備室内において生成される。生成された鍵ならびに利用者用証明書は複数人の内部牽制のもと、IC カードへ格納後、利用者に配付される。利用者への配付方法は「6.1.2　利用者に対する秘密鍵の配付」に規定する。

6.1.2　利用者に対する秘密鍵の配付
本 CP/CPS4.3.1 に規定する。

[1]現在、NSA では、2010 年には、SHA-1 に代わる新たなハッシュ関数の採用に動き出すこと、RSA1024bit（署名、認証）は、2008 年以降の利用は推奨されず、楕円暗号方式に移行することなどのアクションプランが立てられている。ただし、一般的なアプリケーションへの実装が伴うかどうか定かではないのが現状である。

【記述例】

6.1.3　認証局への公開鍵の配付
利用者の鍵ペアは本認証局の認証設備室内で生成されるため、利用者の公開鍵を本認証局へ配送する必要はない。
相互認証先との相互認証証明書の取り交わしに際し、本認証局は、相互認証先から手交あるいは安全に郵送された証明書発行要求ファイルを受け取る。＊（相互認証の方式により、見直しが必要）

6.1.4　検証者に対する認証局公開鍵の配付
検証者が認証局証明書を必要とする場合、本認証局にその旨を申請しなければならない。本認証局は、認証局証明書を格納媒体に記録した上で手交、もしくは郵送により配付する。

6.1.5　鍵サイズ
(1) 自己署名証明書
本認証局が発行する自己署名証明書に係る鍵は、以下の仕様に適合する鍵を利用する。
- 署名方式：SHA-1withRSAEncryption (OID=1 2 840 113549 1 1 5)
- 合成数：2048 bit

(2) 利用者用証明書
利用者用証明書に係る鍵は、以下の仕様に適合する鍵を利用する。
- 署名方式：SHA-1withRSAEncryption (OID=1 2 840 113549 1 1 5)
- 合成数：1024 bit

【記述例】

6.1.7　公開鍵パラメータの生成及び品質検査
(1) 本認証局の公開鍵パラメータ
公開鍵暗号方式に用いる素数は、安全な素数生成技術に基づき、HSM により生成される。
(2) 利用者の公開鍵パラメータ
公開鍵暗号方式に用いる素数は、安全な素数生成技術に基づき、認証設備室内のサーバに搭載されたソフトウェアにより生成される。＊（IC カード内で鍵ペアを生成する場合は、その旨を記載する。「公開鍵暗号方式に用いる素数は、IC カード内で生成される。」等）

6.1.8　鍵用途の目的
鍵用途の目的
本認証局の鍵の用途は、keyCertSign 、cRLSign とし、以下の目的に使用する。

- 自己署名証明書への電子署名
- 利用者用証明書への電子署名
- 認証用設備の証明書への電子署名＊（発行している場合）
- ARL/CRL への電子署名
- OCSP レスポンダの電子証明書に対する電子署名＊（発行している場合）
- 相互認証証明書への電子署名＊（相互認証の方式により、見直しが必要）

利用者の鍵の用途は digitalSignature 及び keyEncipherment とし、クライアント認証の目的で利用する。

4.6.2 秘密鍵の保護及び暗号モジュール技術の管理

【解説】
本節では、認証局秘密鍵及び利用者の秘密鍵についての保護、エスクロー、バックアップ、活性化･非活性化、破棄について規定する。

【記述例】

6.2.1　暗号モジュールの標準及び管理
本認証局で用いる暗号装置は FIPS140-2 のレベル 3 相当の基準を満たすものが使用する。

6.2.2　秘密鍵の複数人管理
暗号装置の使用については、権限を有する担当者が複数人揃わなければ行うことはできない。

6.2.3　秘密鍵のエスクロー
本認証局秘密鍵のエスクローは行わない。

6.2.4　秘密鍵のバックアップ
暗号装置内の本認証局秘密鍵のバックアップは、認証設備室内において、権限を有する複数の担当者により行われ、安全な環境に保管する。

6.2.5　秘密鍵のアーカイブ
本認証局は、本認証局の秘密鍵のアーカイブを行わない。

6.2.6　秘密鍵の暗号モジュールへの転送
本認証局秘密鍵は認証設備室内に設置された HSM 内で生成されるため、規定しない。

6.2.7　暗号モジュールへの秘密鍵の格納
本認証局秘密鍵は認証設備室内に設置された HSM 内で生成されるため、規定しない。利用者の秘密鍵は、認証設備室内で複数人コントロールの下で、安全に IC カードに格納する。＊（IC カード内で鍵を生成する場合、「利用者秘密鍵は、IC カード内で生成されるため、規定しない。」等）

6.2.8　秘密鍵の活性化方法
本認証局秘密鍵の活性化は、認証設備室内において、権限を有する複数の担当者が行う。
利用者の秘密鍵は IC カードの PIN を入力することにより活性化する。

【記述例】

6.2.9　秘密鍵の非活性化方法
本認証局秘密鍵の非活性化は、認証設備室内において、権限を有する複数の担当者が行う。
利用者の秘密鍵は IC カードを IC カードリーダから抜き取ることにより非活性化する。

6.2.10　秘密鍵の破棄方法
本認証局の秘密鍵を破棄する場合は、権限を有する複数の操作者が秘密鍵に関する全ての情報を完全に抹消する。同時にバックアップデータが格納された記録媒体についても物理的に破壊する。

6.2.11　暗号モジュールの評価
暗号装置は FIPS140-2 レベル 3 相当 の基準を満たし、日本国内において稼動実績のあるモジュールを使用する。

4.6.3 その他の鍵ペア管理

【解説】
本節では、認証局証明書並びに利用者証明書のアーカイブ及び使用期間に関して規定する。

認証局証明書の有効期間は利用者証明書の発行のタイミングと合わせ、合理的な期間が規定される必要がある。ただし、利用する鍵アルゴリズムやハッシュ関数の攻撃に対する耐性に関し、定期的に見直す必要がある。

また、電子署名の用途が追加される場合は、電子署名及び認定認証業務に関する法律によって、認証局証明書は 10 年、利用者証明書は 5 年を越える有効期間は証拠力が低いと見なされることも考えられる。また、認証局証明書は最初の 5 年で証明書の発行を行い、残りの 5 年未満は新たな証明書の発行を行わず、CRL の発行のみを行う運用をすることが想定される。

将来、相互認証を行う上で相互認証証明書の発行を行う場合、相互認証証明書の使用期間については相互認証先と調整の上、決定されるものと考える。よって、その際には、CP/CPS に相互認証証明書の規定を追加しなければならない。

相互認証証明書は認証の用途であれば、相互認証先の証明書有効期間の範囲、かつ認証局証明書の有効期間の範囲で取交すことが可能となるが、利用者証明書の用途に電子署名を加えた場合、例えば、相互認証証明書の有効期間は、認証局証明書の有効期間の 1/2 を越えないよう考慮する等、配慮する必要がある。

【記述例】

6.3.1　公開鍵のアーカイブ
公開鍵の保存については、それを含む証明書を保存することによって行う。
自己署名証明書と利用者用証明書は、本 CP/CPS5.4.3 に規定した期間、アーカイブする。

6.3.2　証明書の運用上の期間及び鍵ペアの使用期間
- 認証局証明書　10.5 年
- 利用者用証明書　利用者に応じ（（1 年～6 年）＋30 日）
- 相互認証証明書　6.5 年＊（相互認証の方式により、見直しが必要）

4.6.4 活性化データ

【解説】
本節では、認証局及び利用者の秘密鍵の活性化情報の作成、設定、保護等に関し規定する。

【記述例】

6.4.1 活性化データの生成及び設定
本認証局秘密鍵の活性化情報、及び利用者秘密鍵の活性化情報は安全に生成、管理する。
利用者秘密鍵の活性化情報は、盗聴、改変、容易に類推されることのないよう厳重に管理する。利用者秘密鍵は認証設備室内で IC カードに格納し、IC カードに活性化情報を設定する。利用者秘密鍵の IC カードへの格納、及び IC カードの活性化情報の生成及び転送、出力については、権限コントロールされた操作者複数名により内部けん制され、取り扱われる。
IC カードの活性化情報は IC カードと共に利用者本人に対面で配付するが、対面でない場合、IC カードとは別に利用者に郵送される。

6.4.2 活性化データの保護
本認証局内で使用される本認証局秘密鍵の活性化情報は安全に保管される。利用者秘密鍵に対する活性化情報（IC カード PIN）は、利用者が責任をもって保護しなければならない。

6.4.3 活性化データの他の考慮点
規定しない。＊（規定すべきことがあれば規定する）

4.6.5 コンピュータのセキュリティ管理

【解説】
本節では、認証設備及び登録設備に用いられるソフトウェアシステムに関する技術的要件や、必要とする認定等の要件を規定する。

【記述例】

6.5.1　コンピュータのセキュリティに関する技術的要件
認証設備として使用される機器については、そのセキュリティレベル、品質、安定性、拡張性について十分に考慮し、導入を決定する。

6.5.2　コンピュータセキュリティ評価
本認証局は、使用される機器におけるセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、重大な脆弱性が発見された場合には速やかに必要な対処を行う。

4.6.6 ライフサイクルの技術上の管理

【解説】
本節では、システム開発におけるライフサイクル、運用管理、セキュリティ管理に関する要件を規定する。

【記述例】

6.6.1　システム開発管理
本認証局で使用するシステムを開発する場合、本認証局は、開発環境について十分に検討し、適切な品質管理の下で開発する。

6.6.2　セキュリティ運用管理
認証設備に使用されるシステムは、十分なセキュリティレベルを確保するために必要な設定が行われる。また、システムのセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対処を行い、これを検証する。

6.6.3　ライフサイクルのセキュリティ管理
開発においては、設計･開発･試験のフェーズごとに品質とセキュリティレベルについての評価が行われる。

4.6.7 ネットワークセキュリティ管理

【解説】
本節では、ネットワークセキュリティに関する要件を規定する。

【記述例】

本認証局では、ネットワークセキュリティに関して以下の措置を講じている。

- 外部ネットワークから 認証設備室の設備に対する不正なアクセスを防止するため、ファイアーウォールを導入している。また、認証設備室の設備に対する不正侵入を検知するためのシステムを導入している。
- 認証設備間の通信においては、交換される情報の重要性に応じて、設備等の認証、盗聴防止、改ざん防止措置を講ずる。

4.6.8 タイムスタンプ

【解説】
本節では、日時の記録に関する要件を規定する。

【記述例】

発行する証明書及び監査用記録に対して正確な日付･時刻を記録するため、本認証局は認証設備に対し、タイムサーバによる時刻同期を行う。

4.7 証明書、失効リスト、OCSP のプロファイル

【解説】
本節では、認証局証明書、利用者用証明書、ARL 及び CRL、OCSP（利用する場合）のプロファイルを規定する。本節で規定せず、付録や別紙として記載することも可能である。

相互認証証明書を発行する場合は、相互認証証明書のプロファイルについての規定も必要である。相互認証の方式によって各種プロファイルの設定は変更が必要になる可能性がある。

【記述例】

7.1.1　バージョン番号
本認証局は、X.509 バージョン 3 に準拠した自己署名証明書、相互認証証明書、利用者用証明書を発行する。＊（相互認証の方式により、見直しが必要）

7.1.2　証明書拡張領域
本認証局は、X.509 で定義された拡張領域を利用する。利用する拡張領域については別紙に示す。

7.1.3　アルゴリズムオブジェクト識別子
本認証局が発行する自己署名証明書、相互認証証明書、利用者用証明書、CRL/ARL における電子署名アルゴリズムは SHA-1WithRSAEncryption (OID=1 2 840113549 1 1 5)である。各証明書に記載される主体者の公開鍵のアルゴリズムは、RSA(OID=12 840 113549 1 1 1)である。＊（相互認証の方式により、見直しが必要）

7.1.4　名前の形態
本認証局が発行する自己署名証明書、相互認証証明書、利用者用証明書は、X.500 勧告における識別名（DN：Distinguished Name）の規定に従い決定する。＊（相互認証の方式により、見直しが必要）

7.1.5　名前制約
本認証局では NameConstraints を設定しない。

7.1.6　証明書ポリシーオブジェクト識別子
本認証局では、相互認証証明書及び利用者用証明書の certificatePolicies に certPolicyID として定義する。詳細は別紙に示す。

7.1.7　ポリシー制約拡張の使用
別紙　証明書プロファイルに示す。

7.1.8　ポリシー認定子のシンタックスとセマンティックス
別紙　証明書プロファイルに示す。

7.1.9　重要な証明書ポリシー拡張についての処理方法
別紙　証明書プロファイルに示す。

4.7.1 CRL、ARL プロファイル

【解説】
本節では、ARL/CRL のプロファイルに関する要件を規定する。

【記述例】

7.2.1 バージョン番号
本認証局は、X.509 バージョン 2 に準拠した ARL/CRL を発行する。詳細は別紙 ARL/CRL プロファイル参照。

7.2.2 CRL、CRL エントリ拡張
別紙 ARL/CRL プロファイルに示す。

4.7.2 OCSP プロファイル

【解説】
本節では、OCSP のプロファイルに関する要件を規定する。OCSP レスポンダを利用しない認証局は規定する必要はない。

【記述例】

本認証局が用いる OCSP は、RFC2560 に準拠している。OCSP レスポンダに対し、リクエストを行う場合は、reqCert の項目として別紙 OCSP プロファイルに示すフィールドを含める。
OCSP レスポンダは、OCSP リクエストの処理が成功した場合、responseStatus に successful(0)のステータスを返し、処理が失敗した場合、その理由に応じて successful(0)以外のステータスを返す。
OCSP レスポンダは、BasicOCSPReaponse は、別紙 OCSP プロファイルに示すフィールドを含む。

4.8 準拠性監査とその他の評価

【解説】
本節では、認証局が CP/CPS に準拠し運用がなされていることを確認、是正するために行う準拠性監査について規定する。具体的には、監査の頻度、監査人の要件、監査の範囲、是正処置等について規定する。

将来、相互認証を行う場合、相互認証先に監査の報告を行う義務が発生する可能性がある。

【記述例】

8.1　監査の頻度
本認証局は、本認証局責任者が必要と認めた場合には都度、準拠性監査を実施する。＊（相互認証先との相互認証の要件においては、変更の可能性がある。）

8.2　監査人の要件
監査人には必要な知識と経験を有し、本業務に一切関わりのない者が任命される。

8.3　監査人と非監査者との要件
公正な準拠性監査を遂行するために、監査人は本認証局とは独立していなければならない。

8.4　監査で扱われる事項
準拠性監査は、本認証局の本 CPS 及び事務取扱要領に対する準拠性を監査する。具体的な監査対象は、関連する全施設、設備、本認証局の鍵管理、利用者用証明書及び相互認証証明書に係る業務を含む全業務、要員の教育状況である。

8.5　監査における指摘事項への対応
監査人から指摘を受けた本認証局責任者は、監査人からの指摘事項に対して暫定処置も含め、速やかにその指摘事項に対する対応策を決定し、〇〇の承認を受ける。
本認証局責任者は、監査報告書での指摘事項及びセキュリティ対策技術の最新動向等を踏まえ、設備、規程等の見直しの実施を含む具体的対応措置を講じその結果の評価を行う。
指摘事項が相互認証証明書に関する指摘である場合、上記に加えて、指摘事項、影響範囲、対策防止策（案）について相互認証先 に報告し、承認を受ける。＊（相互認証の方式により、見直しが必要）

8.6　監査結果の開示
監査結果は、〇〇及び〇〇が認めた対象にのみ開示される。＊（相互認証する際、相互認証先に開示する可能性が考えられる。）

4.9 他の業務上の問題及び法的問題

【解説】
本節は、料金や個人情報の保護、ﾄﾗｽﾄﾄﾞﾒｲﾝ内の関係者毎の保証内容、補償、改訂手続き、紛争時の解決手段、準拠法等について規定する。

【記述例】

9.1　料金
別途、規定する。

9.2　金銭上の責任
9.2.1　保険の適用範囲
規定しない。＊（規定すべきことがあれば規定する）

9.2.2　その他の資産
規定しない。＊（規定すべきことがあれば規定する）

9.2.3　利用者を保護する保険、保証
規定しない。

9.3　業務情報の機密性
9.3.1　秘密情報の範囲
本認証局が入手した情報は、証明書、失効情報、本 CP/CPS として明示的に公表するものを除き、機密保持対象として扱う。本認証局は、正当な理由に基づき、法執行機関からの要請がある場合は、法の定めに従い法執行機関へ情報を開示することがある。

9.3.2　秘密情報の範囲外の情報
証明書及び失効情報に含まれる情報は機密保持対象外とする。また、本認証局の出所以外から既知となった情報は、機密保持対象外とする。

9.3.3　秘密情報を保護する責任
本認証局は、正当な理由に基づき、法執行機関からの要請がある場合は、法の定めに従い法執行機関へ情報を開示することがある。

9.4　個人情報の保護
9.4.1　プライバシープラン
○○大学が別途定めるプライバシープランに関する規程に従う。

【記述例】

9.4.2 プライバシーとして扱われる情報
本認証局は、本 CP/CPS9.3.2 に含まれない、利用者個人を特定可能な情報を個人情報として取り扱う。

9.4.3 プライバシーと見なされない情報
利用者証明書及び失効情報、その他リポジトリで公開される情報は個人情報として取り扱わない。

9.4.4 個人情報を保護する責任
○○大学が別途定めるプライバシープランに関する規程に従う。

9.4.5 個人情報の使用に関する個人への通知及び承諾
利用者及び信頼者は、本認証局のサービスを利用するにあたり、本 CP/CPS の内容を理解し、同意しなければならない。

9.4.6 司法手続きまたは行政手続きに基づく公開
○○大学が別途定めるプライバシープランに関する規程に従う。

9.4.7 他の情報公開の場合
規定しない。＊(規定すべきことがあれば規定する)

9.5 知的財産権
以下の情報及びデータは、本認証局の知的財産である。
- 発行された全ての証明書
- 本 CPS
- 本認証局の秘密鍵及び公開鍵

9.6 表明保証
9.6.1 認証局の表明保証
(1) 本 CP/CPS に則って運用を行う
(2) 本認証局秘密鍵を適切に管理し、発行した証明書及び CRL/ARL の信頼の確保を行う
(3)「3.2.2 利用者の確認」に従い利用者の本人性確認を行う
(4) 電子証明書利用申込書に則り、正しい証明書を発行する。
(5)「4.9.3 証明書の失効申請手続き」に従って利用者用証明書の失効処理を行う

【記述例】

9.6.2 利用者の表明保証
利用者は以下の事項を保証することに対し、義務及び責任を負う。
(1) 証明書の適切な使用
「1.4.2 正規の証明書用途」で規定された証明書用途を遵守する。
(2) 利用者秘密鍵（IC カード）、IC カード PIN の管理
利用者は秘密鍵（IC カード）及び IC カード PIN について、充分な注意をもって厳重に保管し、紛失、改変、第三者による使用・複製等が行われない様、厳重に管理しなければならない。
(3) 手続きの遵守
利用者は、本 CP/CPS で定めた利用者用証明書の失効、発行申し込み等の手続きを遵守し、虚偽の申請を行ってはならない。
(4) 利用者用証明書の速やかな失効申し込みの届出
利用者は、利用者秘密鍵が危殆化している、もしくは危殆化している恐れがある場合、または IC カードの利用を中止する場合、IC カードの券面の情報や証明書の情報に誤りがある場合、あるいは変更の希望がある場合は、本認証局に速やかに失効の申請を行わなければならない。
(5) 本 CP/CPS の内容を理解し、本 CP/CPS で利用者に定めた規定に同意しなければならない。

9.6.3 信頼者の表明保証
(1) CPS への同意
信頼者は、利用者用証明書の利用目的や使用範囲、制限を理解し、証明書を信頼すべきか否かの判断を行うために、本認証局のリポジトリにある CP/CPS を理解し、同意しなければならない。
(2) 証明書の適切な使用
利用者の公開鍵と利用者用証明書は、本 CP/CPS4.5.2 に規定する用途でのみ使用する。
(3) 証明書の有効性の確認
信頼者は、利用者用証明書の有効性について、以下を確認しなければならない。
本認証局が発行した利用者用証明書を信頼すべきかどうかを判断するために、次の内容を確認する。
- 利用者用証明書が本認証局から発行され、有効であること
- 証明書が改ざんされていないこと

9.6.4 他の関係者の表明保証
規定しない。＊（規定すべきことがあれば規定する）

【記述例】

9.7　無保証
本認証局は、本 CP/CPS に記載してある事項を遵守し、記載事項に適合するよう本認証局の運用を行うが、これにも関わらず発生した損害について、本認証局は一切の責任を負わないものとする。
本認証局は、利用者及び信頼者が本 CP/CPS に記載されている事項について必要な情報を提供し、その内容を遵守することを勧奨するが、本認証局は、他の関係者に対し、利用者及び信頼者が「9.6.2 利用者の表明保証」及び「9.6.3 信頼者の表明保証」に記述されている事項を遵守することは保証しない。

9.8　責任の制限
利用者が「9.6.2 利用者の表明保証」に違反したことに起因して生じた損害及び信頼者が「9.6.3 信頼者の表明保証」に違反したことに起因して生じた損害に関し、本認証局は、関係者に対し一切の責任を負わないものとする。

9.9　補償
利用者、信頼者の行為に起因して第三者に損害が生じた場合、本認証局は免責されるものとし、利用者または信頼者は損害賠償の責めを負わなくてはならないものとする。本認証局が第三者に損害賠償をした場合、利用者または信頼者は本認証局に対してその賠償額及び本認証局において発生する訴訟に係る費用等の損害を補償しなくてはならないものとする。

9.10　有効期間と終了
9.10.1 有効期間
本 CPS は、文書の作成後、ポリシー承認局が承認することにより有効となる。「9.10.2 終了」で記述する本 CPS の終了以前に本 CPS が無効となることはない。

9.10.2 終了
本 CP/CPS は、「9.10.3 終了の影響と存続条項」に掲げる存続条項を除き、本認証局が業務を終了した時点で無効となる。

9.10.3 終了の影響と存続条項
本認証局が業務を終了した後も、9.4、9.5、9.6.2、9.7、9.8、9.9、9.10.3、9.13 ないし 9.16 の各項の規定については効力をもつものとする。

9.11　関係者間の個別通知と連絡
本認証局は、利用者に対する必要な通知をリポジトリでの告知、書面による通知により行う。
相互認証先に関する通知は、相互認証先と調整した方法により通知を行う。
＊（相互認証の方式により、見直しが必要）

【記述例】

9.12　改訂
9.12.1 改訂手続き
本 CP/CPS の改訂については、認証局責任者が起案し、○○が承認する。

9.12.2 通知方法及び期間
変更版の本認証局の CP/CPS をﾘﾎﾟｼﾞﾄﾘ上において公開することをもって通知する。公開後 14 日を経過しても利用者から異議申し立てがなかった場合は当該期間満了日に、または、変更版の CP/CPS を公開した後、利用者が利用者用証明書を利用した場合は当該利用日に、利用者は変更事項を承認したものとする。

9.12.3 オブジェｸﾄ識別子が変更されなければならない場合
本認証局の CP/CPS が大幅に変更された場合等、本学の判断によりﾘ本認証局のﾎﾟﾘｼｰ識別子を変更することができるものとする。

9.13　紛争解決手段
本認証局の利用に関して生じた全ての訴訟の際、全ての当事者は、○○地方裁判所を第一審の専属管轄裁判所とする。

9.14　準拠法
本認証局と関係者の間で係争が生じた場合に適用される法令は、日本国内法を準拠法とする。

9.15　適用法の遵守
規定しない。＊（規定すべきことがあれば規定する）

9.16　雑則
9.16.1 完全合意条項
本 CPS の規定は口頭で追加、変更、削除、または終了させることはできない。

9.16.2 権利譲渡条項
本 CP/CPS、及びその他の契約、合意により規定された権利義務は、○○大学と事前の合意なく第三者に譲渡、相続することは出来ない。

【記述例】

9.16.3 分離条項
本 CP/CPS 中のある規定が、何らかの理由により、無効または執行不可能であるとされた場合においても、残余の規定は有効であり、当事者の意思に最も合理的に合致するよう解釈される。
責任の制限、保証、その他の義務の免責、若しくは制限、または損害の排除について規定する本 CP/CPS の各条項は他の規定と分離され、また、その条項に従って執行可能であることにつき当事者は合意するものとする。

9.16.4 強制執行条項
規定しない。＊（規定すべきことがあれば規定する）

9.16.5 不可抗力
(1)本認証局は、利用者が利用者用証明書を取得、利用することによりコンピュータシステム等のハードウェア・ソフトウェアに何らかの影響、障害が発生しても、その責を一切負わない。
(2)本認証局は、利用者や所属組織の代表者からの失効申し込みに伴う本認証局内での失効処理が、正当な事由により遅延した場合、これにより発生した損害については、一切損害賠償責任を負わない。
(3)本認証局は、本認証局を廃止することにより発生した損害については、一切損害賠償責任を負わない。
(4)本認証局は次に掲げる事象または状況によって利用者、その他第三者（信頼者を含むがこれに限らない）に損害が生じた場合でも、一切の責任を負わないものとする。

- 天災：火災、雷、噴火、洪水、地震、嵐、台風、津波等
- 人災：戦争、革命、暴動、内乱、労働争議等
- 裁判所、政府、行政、省庁等による作為、不作為、または命令等
- 電源の供給停止、回線の停止等、本認証局以外のシステムの停止
- 技術上若しくは運用上緊急に本認証局に係わるシステムを停止する必要があると本認証局が判断した場合
- 本認証局が、本 CP/CPS に基づく義務を適切に履行したにも関わらず、不完全履行または履行遅滞を生じさせ、または、かかる結果に至ることとなった事象若しくは状況
- その他本認証局の責に帰すべからざる事由

9.17　その他の条項
規定しない。＊（規定すべきことがあれば規定する）

4.10 証明書、ARL/CRL プロファイル例

4.10.1 証明書プロファイル例

<基本フィールド>

フィールド	認証局証明書	利用者用証明書	備考
version	○	○	ver3
serialNumber	○	○	
signature	○	○	
validity	○	○	
notBefore	○	○	
notAfter	○	○	
Issuer	○	○	
subject	○	○	
subjectPublicKeyInfo	○	○	
algorithm	○	○	
subjectPublicKey	○	○	

<拡張フィールド>

フィールド	認証局証明書	利用者用証明書	備考
authorityKeyIdentifier		○	FALSE
subjectKeyIdentifier		○	FALSE
keyUsage	・keyCertSign ・cRLSign	・digitalSignature ・keyEncipherment	TRUE
extendedKeyUsage		・clientAuth ・MS-smartCardLogon	TRUE
privateKeyUsagePeriod			FALSE
certificatePolicies		○ CPS 公開用 URL	TRUE
policyMapping			FALSE
subjectAltName		・Microsoft 社 UserPrincipalName	FALSE
issuerAltName	○	○	FALSE
basicConstraints	○		TRUE
nameConstraints			TRUE
policyConstraints			TRUE
cRLDistributionPoints		http ldap	FALSE
subjectDirectoryAttr			FALSE
authorityInfoAccess		OCSP URI	FALSE
netscape-cert-type			FALSE
VeriSignPrivateExtension			FALSE

4.10.2 ARL/CRL プロファイル例

<基本フィールド>

フィールド	ARL	CRL	備考
Version	○	○	ver2
Signature	○	○	
Issuer	○	○	
thisUpdate	○	○	
nextUpdate	○	○	
RevokedCertificates	○	○	
userCertificate	○	○	
revocationDate	○	○	
crlEntryExtensions			
crlExtensionts			

<拡張フィールド>

	ARL	CRL	備考
crlEntryExtensions			
reasonCode		○	
holdInstructionCode			
invalidityDate			
certificateIssuer			
CrlExtensions			
authorityKeyIdentifier		○	FALSE
issuerAltName			
cRLNumber		○	FALSE
deltaCRLIndicator			
issuingDistribution Point		○	TRUE

用語集

RFC2828[2]に基づき、本ガイドライン中で用いた用語の定義を行う（引用したものは※とする）。RFC2828 に定義がないものは、本ガイドライン独自で定義している。

あ行

- **アクセスコントロール（Access Control）　※**

権限のないアクセスに対するシステムリソースの保護。システム資源を使用するプロセスは、セキュリティポリシーによってコントロールされ、権限を持った主体（ユーザ、プログラム、プロセス、または他のシステム）によってのみセキュリティポリシーに基づいて許可される。

「資源に対する権限のない使用を防止すること。権限のない方法による資源の使用を防止することも含む。」

- **アルゴリズム（Algorithm）　※**

問題を解決するためのステップごとの命令または計算手順の有限個のセットで、特にコンピュータに実装されるもの。

- **一時停止（Suspension）**

証明書を一時的に無効な状態にすること。

か行

- **下位認証局（Subordinate CA）　※**

公開鍵証明書が、別の（上位）CA によって発行されている CA。

- **鍵ペア（Key Pair）　※**

公開鍵暗号技術に使われる数学的に関連する一式の鍵（公開鍵と私有鍵）であり、私有鍵を公開鍵の知識から引き出すことが計算量的に非現実的なやり方で生成される。

[2] http://www.ipa.go.jp/security/rfc/RFC2828-03AJA.html#access%20control

鍵ペアの所有者は、データの暗号化、デジタル署名の正確性検証、保護されたチェックサムの計算もしくは鍵共有アルゴリズムにおける鍵の生成にその鍵を使えるように、他のシステム主体に公開鍵を開示する。それに対応するプライベート鍵は、データの復号、デジタル署名の生成、保護されたチェックサムの正確性検証もしくは鍵共有アルゴリズムにおける鍵の生成のためにそれを使う所有者によって秘密に保たれる。

- 鍵長 (Key Length)

鍵ペアのデータ長のこと。一般に鍵が長ければ長いほど解読がされにくいとされる。

- 鍵の預託 (Key Escrow) ※

特定の環境下において、暗号技術的な鍵が復元でき、使えるように、その鍵もしくはその部分についての知識を、ひとつ、あるいは、複数の「寄託エージェント (escrow agent)」と呼ばれる第三者のカストディに蓄積するための鍵回復テクニック。鍵寄託は、典型的には、知識分割テクニックとして実施される。例えば、Escrowed Encryption Standard は、デバイス固有の分割鍵の 2 つのコンポーネントを分離された寄託エージェントに委託する。そのエージェントは、そのコンポーネントを、その特定のデバイスによって暗号化された遠隔通信の電子的な監視を行うことが法的に認可された者にのみ提供する。このコンポーネントは、デバイス固有の鍵を再構築するために使われ、これは、通信を復号するために必要とされるセッション鍵を取得するために使われる。

- 活性化情報 (Activation Data)

鍵以外のデータ値で、暗号化モジュール等に格納されている秘密鍵にアクセスするためのもの。具体的には、PIN コード、パスフレーズ等を指す。

- 危殆化 (Compromise) ※

セキュリティ侵害のひとつ。ここで、システム資源が、不正 (無権限) アクセスに対して露出されるか、あるいは、潜在的に露出される。

本ガイドラインでは、秘密鍵や関連秘密情報等が盗難や漏洩、第三者による解読等によって、秘密性を失ったか、あるいはその可能性があること。

- 公開鍵 (Public Key) ※

公開鍵暗号技術について使われる暗号技術的な鍵のペアのうち、公衆に開示可能なコンポーネントの方。

「(公開鍵暗号システムにおいて) ユーザの鍵ペアのうち、公知の鍵。」

さ行

- 自己署名証明書 (self-signed certificate) ※

その公開鍵が証明書内にあり、そのプライベート鍵が証明書に署名するのに使われる公開鍵証明書が、署名者の同一の鍵ペアのコンポーネントであるもの。

自己署名 X.509 公開鍵証明書において、発行者の DN は、サブジェクトの DN と等しい。

- 失効 (Revoke、certificate revocation) ※

CA によって発行され、有効であったデジタル証明書が無効になったことを CA が宣言したときに発生するイベント。通常、失効日と共に宣言される。

X.509 では、証明書を記載した CRL を発行することにより、潜在的な証明書ユーザに失効が通知される。失効と CRL のリストは、証明書の期限が切れる前にのみ必要である。

- 失効リスト (Certificate Revocation List = CRL) ※

予定された有効期限を迎える前に、発行者によって失効されたデジタル証明書を列挙するデータ構造体。

「有効とみなされなくなった証明書のセットを示す、証明書の発行者による署名付きのリスト。CRL に掲載された後で証明書の有効期限が切れると、次回の CRL にはその証明書は掲載されない。CRL は、失効された公開鍵証明書または属性証明書を識別するために使用され、認証局またはユーザに発行された証明書の失効を表す。また、CRL という用語は、CRL、ARL、ACRL 等を含むさまざまな種類の失効リストに適用される一般的な用語としても用いられる。」

- 信頼者 (Relying Party) ※

デジタル証明書によって提供された情報の正当性 (他の主体の公開鍵の値など) に依存するシステム主体。

「確信をもって、他の主体の公開鍵を知る必要がある主体。」

システム主体は、人間、組織、あるいは人間またはシステムによって制御されているデバイスまたはプロセスである。

た行

- 登録局 (Registration Authority = RA) ※

(CA からは分離された) オプションとしての PKI 主体であり、これは、デジタル証明書にも、CRL にも署名しないが、証明書や CRL を発行し、他の証明書管理機能を行うために CA によって必要とされる情報 (特に、サブジェクトの身元) の部分または全体の記録もしくは正確性検証について責任を負う。

しばしば、CA は、その CA が証明書に署名しているすべてのエンドユーザのために、すべての証明書管理機能を行う可能性がある。また、大規模な、あるいは、地理的に分散したコミュニティにおけるように、CA の 2 番目の役割の重責を降ろして、それらをアシスタントに代理させる一方で、CA は、主要な機能（証明書や CRL に署名すること）を維持することが必要不可欠、もしくは、渇望される可能性もある。CA によって RA に代理されるタスクは、個人の認証、名前の割り当て、トークン配布、失効報告、鍵生成およびアーカイブ化を含む可能性がある。RA は、CA からは分離された、副次的な機能を割り当てられたオプションとしての PKI コンポーネントである。RA に割り当てられた義務は、場合に応じて様々であるが、下記の事項を含む可能性がある。

サブジェクトの身元を検証すること。すなわち、個人認証機能を行うこと。

サブジェクトに名前を割り当てること。

「サブジェクトが 証明書について要求された属性をもつ資格があること」を検証すること。

「サブジェクトが 証明書について要求された公開鍵に対応するプライベート鍵を所持すること」を検証すること。

鍵ペア生成、トークンの配布および失効報告の取り扱いのような登録以外の機能を行うこと。（このような役割は、CA と RA の両方から分離された PKI 要素に割り当てられる可能性がある。）

PKIX における用法： オプションとしての PKI コンポーネントであり、CA とは別のもの。RA が行う機能は、場合に応じて様々であるが、身元認証および名前の割り当て、鍵生成、および、鍵ペア、トークン配布および失効報告のアーカイブ化を含む可能性がある。

- 電子証明書（Public-key Certificate） ※

システム主体の身元を公開鍵の値に結合し、追加的なデータ項目にも結合する可能性があるデジタル証明書。公開鍵の所有を証明するデジタル的に署名されたデータ構造体。

公開鍵証明書上のデジタル署名は、偽装不能である。それゆえ、その証明書は、ディレクトリに収めることによって、（ディレクトリが証明書のデータインテグリティを保護する必要なく）公開できる。

「ユーザの公開鍵は、何らかの他の情報とともに、それを発行した認証機関のプライベート鍵で署名することによって偽装不能なものとして与えられる。」

- 電子署名（Digital Signature）

データのあらゆる受信者が、その署名をデータの発信元およびインテグリティを検証するために使えるようなやり方で、暗号アルゴリズムによって算出され、データオブジェクトに追加される値。

「データユニットの受信者がデータユニットの源泉とインテグリティを証明できるようにし、（例：受信者による）偽装から防護する、データユニットに追加されたデータ、もしくは、データユニットの暗号技術的な変換。」

典型的にはそのデータオブジェクトは、ハッシュ関数に対する最初の入力であり、次に、そのハッシュ結果は、署名者のプライベート鍵を使って、暗号技術的に変換される。最終結果としての値は、そのデータオブジェクトのデジタル署名と呼ばれる。その署名の値は、保護されたチェックサムである。なぜなら、暗号技術的ハッシュの属性は、「データオブジェクトが変更された場合、そのデジタル署名は、もはや一致しないこと」を確保するからである。デジタル署名は、偽造不能である。なぜなら、想定される署名者のプライベート鍵を知らずして、署名を正しく作成することや、変更することについて、確信を持つことはできないからである。

デジタル署名スキームには、ハッシュ結果を変形するために、公開鍵暗号アルゴリズムを使うものがある。それゆえ、アリスがボブに送るためにメッセージに署名する必要があるとき、彼女は、そのハッシュ結果を暗号化するために彼女のプライベート鍵を使うことができる。ボブは、メッセージとデジタル署名の両方を受け取る。ボブは、アリスの公開鍵をその署名を復号するために使うことができ、次に、平文の結果を彼が自信でメッセージをハッシュ化して求めたハッシュ結果と比較する。値が等しい場合、ボブは、そのメッセージを受け入れる。なぜなら、それはアリスからのものであり、変更されずに到着したと確信を持てるからである。その値が等しくない場合、ボブは、そのメッセージを棄却する。なぜなら、そのメッセージも、その署名も経路において変えられているからである。

他のデジタル署名スキームは、そのハッシュ結果をデータ暗号化するためには直接使うことができないアルゴリズムで変換する。このようなスキームは、そのハッシュから署名値を作成し、その署名値を検証するやり方を提供するが、署名値からハッシュ結果を復元するやり方は提供しない。国によっては、このようなスキームは、輸出可能性を高め、利用における他の法的制約を避ける可能性がある。

な行

- 認証局（Certification Authority = CA） ※

デジタル証明書（特に X.509 証明書）を発行し、証明書内のデータ項目間の結びつきを保証する主体。

「1 人以上のユーザに信用され、証明書を作成および割り当てる機関。認証局がユーザの鍵を作成することもある。」

証明書ユーザは、証明書によって提供された情報の正当性に依存する。このため、CA は、証明書ユーザが信頼する第三者でなければならず、通常、政府、企業、またはその他の組織によって認められた権限をともなう公的な地位を持つ。CA は、証明書のライフサイクルを管理する責任を持ち、証明書の種類および適用する CPS に応じて、その証明書に対応する鍵ペアのライフサイクルを管理する責任を持つことがある。

- 認証局運用規程（CPS：Certification Practice Statement） ※

「認証局が証明書の発行のために採用する運用規定」

CPS は公開されたセキュリティポリシーで、特定の CA から発行された証明書が特定のアプリケーションで十分に信頼できるかどうかを証明書ユーザが判断するときに役立つ。CPS は、
(a) CA によるシステムの詳細と証明書管理業務で採用している既定の定義、
(b) CA と証明書を発行された主体との間の契約の一部、
(c) CA に適用される法令または規制、
(d) 複数のドキュメントを含むこれらの種類の組み合わせ　　である。

通常、CPS は証明書ポリシーよりも詳細で手続き的な目的を持つ。CPS が特定の CA または CA コミュニティに適用されるのに対し、証明書ポリシーは CA 間また CA コミュニティ間に適用される。1 つの CPS を持つ CA が複数の証明書ポリシーをサポートすることがある。これは、異なる適用目的として、または異なるユーザコミュニティによって使用される。それぞれ異なる CPS を持つ複数の CA が、同じ証明書ポリシーをサポートすることがある。

は行

- ハッシュ関数　※

（通常、可変長であり、非常に大きい可能性があるメッセージもしくはファイルのような）データオブジェクトに基づいて値を計算するアルゴリズム。これによって、データオブジェクトを より小さなデータオブジェクト（「ハッシュ結果 (hash result)」通常は固定長）に対応づける。

「広範囲（非常に広範囲である可能性がある）ドメインからの値を、より狭い範囲に対応づける（数学的）関数。「良い」ハッシュ関数は、その関数をドメイン中の（大きな）値に適用した結果が、全域にわたって一様な分散（かつ、乱雑に見えるもの）となるものである。」

セキュリティアプリケーションに必要とされる種類のハッシュ関数は、「暗号技術的ハッシュ関数 (cryptographic hash function)」と呼ばれる。このためのアルゴリズムについて、（ブルートフォースよりも効果的な攻撃は無いので）下記の条件は計算量的に現実的でない。

(a) データオブジェクトが事前に定めたハッシュ結果になる（「一方向」性）。あるいは、

(b) 2 つのデータオブジェクトが同一のハッシュ結果になる（「衝突困難」性）。

(c)暗号技術的ハッシュは、ハッシュ関数の定義に記述されている意味において「良い」といえる。入力データオブジェクトに対するいかなる変更も、高い確率で、異なるハッシュ結果をもたらすので、暗号技術的ハッシュ（cryptographic hash）の結果がデータオブジェクトについての良いチェックサムを作り出すようになる。

- 秘密鍵（Private Key）　※

公開鍵暗号技術について使われる暗号技術的鍵のペアの秘密コンポーネント。

「（公開鍵暗号システムにおいて）ユーザの鍵ペアのうち、そのユーザのみが知っている鍵。」

- **秘密鍵管理モジュール (Hardware Security Module)**

暗号鍵の生成､保管､利用等において、セキュリティを確保する目的で主に認証局で使用されるハードウェアのこと。

- **プロファイル (Profile)**

証明書、失効リスト (CRL) 等の設定情報のこと。

- **本人性確認 (Identification & Authentication)　※**

システム主体によって／システム主体について、主張された身元を検証するプロセス。
認証過程は、2 つのステップから成る。
1. 識別ステップ:
識別子をセキュリティシステムに渡す。
(認証された同一性はアクセス制御サービスなどの他のセキュリティサービスのベースとなるので、識別子は慎重に割り当てなければならない。)
2. 検証ステップ:
主体と識別子間のバインディングを確証する認証情報を提供または生成する。

ま行

ら行

- **リポジトリ (Repository)　※**

デジタル証明書や、(CRL、CPS および証明書ポリシーを含む) 関連情報を蓄積し、証明書ユーザに配布するためのシステム。

「証明書や証明書に関する他の情報を蓄積･取得するための信用に値するシステム。」

証明書は、リポジトリ中に置くことによって、必要とする可能性がある者宛に発行される。このリポジトリは、通常、公衆がアクセス可能なオンラインサーバである。例えば、Federal PKI において、期待されるリポジトリは、LDAP を使うディレクトリであるが、DAP を使う X.500 ディレクトリ、もしくは、HTTP サーバ、もしくは、匿名によるログインを許容する FTP サーバである可能性もある。

- **利用者 (Certificate User)**

大学により利用者用証明書の使用を認められたその大学に所属する個人。

- **ルート認証局 (Root Certification Authority)　※**

エンド主体によって直接、信用されている CA であり、root CA の公開鍵の値の入手は、回線外の手順によることを含む。

階層型 PKI (Hierarchical PKI) における用法:

認証階層 (certification hierarchy) において、最高レベルの (最も信頼される) CA。 すなわち、すべての証明書ユーザが信用の基礎とする公開鍵をもつ機関。

階層型 PKI において、root は、2 番目に高位なレベルである CA のひとつもしくは複数宛に公開鍵証明書を発行する。これらの各 CA は、3 番目に高位なレベルの CA 等宛により多くの証明書を発行できる。階層型 PKI の運用を開始するために、ルートの初期公開鍵は、すべての証明書ユーザ宛に PKI の認証関係に依存しないやり方でセキュアに配布される。ルートの公開鍵は、単純に数値として配布される可能性があるが、典型的には、root がサブジェクトである自己署名証明書中において配布される。ルートの証明書は、認証階層 (certification hierarchy) において高位の者がいないので自己署名される。それゆえ、ルートの証明書は、すべての認証パスにおいて最初の証明書となる。

- ログ (Log)

コンピュータの利用状況や、通信の記録を取ること。また、その記録。操作やデータの送受信が行われた日時と、行われた操作の内容や送受信されたデータの中身等が記録される。

A－G

- ARL (Authority Revocation List) ※

CA 宛に発行されたが、予定されていた失効日以前に発行者によって無効化されたデジタル証明書を列挙するデータ構造。

「証明書発行者によって、もはや有効ではないとみなされる機関に対して発行された公開鍵証明書のリストを含む失効リスト。」

- CA (Certification Authority) ※

＝認証局

- CN (Common Name) ※

(以下の文字列を示す。
(a) ディレクトリオブジェクト ("commonName" 属性) の X.500 DN の一部である可能性があり、
(b) 何らかの制限付きスコープ内でオブジェクトが一般的に知られるために使用されている名前 (多義の可能性がある) で、
それが対応する国または文化での命名規則に従う。

- CRL (Certificate Revocation List) ※

＝失効リスト

- DN (Distinguished Name) ※

X.500 DIT (Directory Information Tree) において、オブジェクトを一意に表現する識別子。

DN は、DIT のベースから命名されたオブジェクトに至るパスを識別する一式の属性値である。X.509 公開鍵証明書もしくは CRL は、その発行者を識別する DN を含み、X.509 属性証明書は、そのサブジェクトを識別する DN もしくは他の形態の名前を含む。

- FIPS 140-1 (Federal Information Processing Standard) ※

コンピュータ および通信システム中の秘密区分とされていない情報を防護するために使われる暗号技術的モジュールが適合すべきセキュリティ要件についての米国政府標準。

この標準は、広範な潜在的アプリケーションや環境を扱うために、4 つの段階的なレベル ("Level 1"から to "Level 4"まで) の要件を規定する。この要件は、基本設計と文書化、モジュールインターフェイス、 認可割れた役割とサービス、物理的セキュリティ、ソフトウェア・セキュリティ、オペレーティングシステムセキュリティ、鍵管理 、暗号アルゴリズム、電磁的インタフェースと電磁的互換性 (EMI/EMC)、および自己検査に対応する。NIST とカナダの CSE (Communication Security Establishment) は、共同でモジュールを認定する。

- FIPS 140-2 (Federal Information Processing Standard)

セキュリティレベル 4 段階の位置付けは FIPS 140-1 とほぼ変わらない。FIPS 140-2 ではセキュリティ要件の 2 項目について見直しが行われている。セキュリティ要件 11 項目の内、ソフトウェア・セキュリティと暗号アルゴリズムがなくなり、代わりに以下が加えられた。

・設計保障
・コンフィグレーション管理, 配布と運用, 開発, ガイダンス文書, 機能テストの規定。
・その他の攻撃の軽減
・現時点でセキュリティ要件が明確になっていない攻撃の軽減。

- FQDN (Fully Qualified Domain Name)

ドメイン名に、サブドメイン名およびホスト名を付加したものをいう。ドメイン・ネーム・システムにおいて 1 個の IP アドレスと対応関係をもつ。

H－N

- HSM (Hardware Security Module)

＝秘密鍵管理モジュール

- IA (Issuing Authority)

＝認証局

- IC カード (IC Card、Smart Card) ※

コンピュータの CPU、メモリおよび入出力インターフェイスの機能を行う ひとつ、もしくは複数の集積回路のチップを含むクレジットカードの大きさのデバイス。

しばしば、この用語は、若干厳密に、銀行や商人によって発行されたプラスチックのクレジットカードの類の形態と外観に適合するカードの意味で使われる。また、この用語は、広く、クレジットカードよりも大きなカード (特に、PC カードのように、より厚いカード) を含むように使われることもある。

「スマートトークン」は、スマートカードの規定に準拠するデバイスである。ただし、このトークンが、犬の首札やドアの鍵の形態のような何らかの他の形態にパッケージ化されて、標準的なクレジットカードの形態をもたない場合を除く。

- IETF (Internet Engineering Task Force) ※

インターネット技術の開発に貢献する人々によって自己組織化されたグループ。これ自体は ISOC の一部ではないが、インターネット標準を開発することに携わっている主たる主体である。(IETF は) WG (ワーキンググループ) から成り、これらは、(セキュリティエリアのように) エリアとしてまとめられており、各々は、ひとり、もしくは、複数名のエリアディレクター (Area Director) によって調整されている。IAB および IESG への指名は、ボランティアとして常連の IETF 会合参加者 の中から無作為に選択された委員会によって行われる。

- LDAP (Lightweight Directory Access Protocol) ※

X.500 ディレクトリ (もしくは、他のディレクトリ サーバ) の基本的用途を DAP (Directory Access Protocol) 全部の資源要件を招くこと無く (訳注：軽便に) サポートするクライアント／サーバ プロトコル。

シンプルな管理と、シンプルな読み書きの双方向的ディレクトリサービスを提供するブラウザアプリケーションのために設計された。クライアントのディレクトリ サーバに対する認証として、シンプル認証とストロング認証の両方をサポートする。

O－U

- OCSP (Online Certificate Status Protocol) ※

クライアントによって、サーバからデジタル証明書に関する有効性の状態と他の情報を入手するために使われるインターネットプロトコルのひとつ。

（高額の商取引を扱うアプリケーションのような）アプリケーションにおいて、CRL によるより適時な証明書失効状態の入手、あるいは、他の状態情報の入手が不可欠である可能性がある。OCSP は、定期的な CRL に照らしてチェックすることの代わり、もしくは、追加的なものとして、デジタル証明書の現在の状態を判定するために使われる可能性がある。OCSP クライアントは、OCSP サーバ宛に状態リクエストを発行し、サーバがレスポンスを提供するまで当該証明書の受領を保留する。

- PIN（Personal Identification Number）

個人識別番号。

- OID（Object Identifier） ※

一連の整数（ASN.1 標準で規定されているように整形・割り当てされる）で書かれた、あるものについての公式な地球規模で固有な名称であり、概要仕様中のものをプロトコルにおけるセキュリティサービスの交渉時に参照するために使われる。

「オブジェクトと関連づけられた（すべての他のこのような値から区別可能な）値。」

OID によって命名されたオブジェクトは、オブジェクト識別子の木の葉である。（これは、X.500 ディレクリ情報の木と似ているが別のものである。）各 arc（すなわち、各木の枝）には、非負の整数のラベルが付けられる。OID は、木のルート（根）から 名前がついたオブジェクトに至るパス上の一連の整数である。

OID の木は、ルート直下に 3 つの arc をもつ。

{0} ITU-T 用

{1} ISO 用

{2} 両者の共同利用

下記 ITU-T には、4 つの arc があり、ここで、{0 0} は、ITU-T 勧告（recommendation）用である。下記 {0 0} には、26 の arc があり、一連の勧告のための arc は、A から Z までのアルファベットで始まり、これらのもとに各勧告のための arc がある。それゆえ、ITU-T 勧告 X.509 についての OID は、{0 0 24 509} である。下記 ISO には、4 つの arc があり、ここで、{1 0 } は、 ISO 標準用であり、これらのもとの arcs は、各 ISO 標準用である。それゆえ、ISO/IEC 9594-8（the ISO number for X.509）用の OID は、{1 0 9594 8} である。

次のものは、追加的例示である。

ANSI は、branch {joint-iso-ccitt(2) country(16) US(840) organization(1)} 下に組織体名を登録する。NIST CSOR は、branch {joint-iso-ccitt(2) country(16) us(840) gov(101) csor(3) pki(4)} 下に PKI オブジェクトを記録する。米国国防総省は、INFOSEC オブジェクトを branch {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1)} の下に登録する。PKIX プライベート拡張のための OID は、{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 1 1} というように、当該 PKIX 名前空間についての arc の下の arc の中に定義される。

- PKI (Public Key Infrastructure) ※

公開鍵暗号技術のアプリケーションについてのユーザのコミュニティのために、何らかの証明書管理、アーカイブ管理、鍵管理およびトークン管理機能を行う認証局（および、オプションとして登録局および他の支援的なサーバやエージェント）のシステム。

PKIX における用法：

一式のハードウェア、ソフトウェア、人間、ポリシー、および手順であり、公開鍵暗号技術に基づくデジタル証明書を作成・管理・蓄積・配布・失効するために必要とされる。

PKI の核となる機能は、次のとおり。

(a) ユーザを登録し、その公開鍵証明書を発行する。

(b) 要求されたとき、証明書を失効する。

(c)後日、証明書の十分性を検証する。

必要とされるデータをアーカイブする。データの守秘性のための鍵ペアは、CA もしくは RA によって生成（および、おそらく寄託）される可能性があるが、PKI クライアントに自身のデジタル署名鍵ペアを生成することを要求することは、暗号技術的システムのシステムインテグリティを維持管理するのに有用である。なぜなら、このようにすれば、当該クライアントのみが、常に自身が使うプライベート鍵を所持するからである。また、PKI のコンポーネントが運用する際に準拠するセキュリティポリシーである CPS を承認し、調整するために、機関が設立される可能性がある。

数多くの他のサーバやエージェントがコア PKI をサポートし、PKI クライアントがそれらからサービスを得る可能性がある。このようなサービスの全体像は、まだ完全には理解されておらず、進化しつつあるが、サポートする役割は、アーカイブエージェント、認定された配布エージェント、確認（confirmation）エージェント、デジタル公証人、ディレクトリ、鍵寄託エージェント、鍵生成エージェント、発行者やサブジェクトが PKI において一意の識別子をもつことを確保する命名エージェント、リポジトリ、チケット交付エージェントおよび タイムスタンプエージェントを含む可能性がある。

- PKIX (Public Key Infrastructure X.509)

IETF において、X.509 形式にもとづいた PKI 技術の標準化を行っているワーキング グループ。

- RA (Registration Authority)

＝登録局

- RFC(Request for comment) ※

インターネット標準文書と、IESG (Internet Engineering Steering Group) 、IAB (Internet Architecture Board) およびインターネットコミュニティ全般の他の発行物についての公式なチャネルである一連のアーカイブするシリーズの文書のひとつ。

この用語は、"Internet Standard" の同義語ではない。

- RSA ※

1977 年に Ron Rivest、Adi Shamir および Leonard Adleman によって発明された公開鍵暗号技術についてのアルゴリズム。

RSA は、2 つの大きな素数から得られる整数の剰余演算を使う。RSA 解読の困難性は、ほぼ同じ大きさの 2 つの大きな素数から得られる整数の素因数分解の困難性と等価であると信じられている。

RSA 鍵ペアを作成するために、2 つの大きな素数 p と q を無作為に選択し、剰余演算 n = pq を計算する。n 未満であり、かつ、(p-1)(q-1) の素数である公開する指数 e を無作為に選択する。ed-1 が (p-1)(q-1) を割り切れるように公開しない他の d を選択する。この公開鍵は、数 (n,e) の組であり、そのプライベート鍵は、組 (n,d) である。

プライベート鍵 (n,d) をその公開鍵 (n,e) から算出することは、困難であると想定されている。しかし、n が p と q に素因数分解可能である場合、そのプライベート有鍵 d は、容易に算出できる。それゆえ、RSA のセキュリティは、「2 つの大きな素数から成る数を素因数分解することは、計算量的に困難である」という想定に依存する。(当然ながら、p と q は、プライベート鍵の一部として扱われるか、あるいは、n を算出した後、破壊される。)

ボブ宛に送られるメッセージ m を暗号化するために、アリスは、m**e (mod n) = c を計算するためにボブの公開鍵 (n,e) を使う。彼女は、c をボブ宛に送る。ボブは、c**d (mod n) = m を計算する。ボブのみが d を知っているので、ボブのみが m を戻すために c**d (mod n) = m を計算できる。

ボブ宛に送るメッセージ m のデータ発信元認証を提供するために、アリスは、m**d (mod n) = s を計算する。ここで、(d,n) は、アリスのプライベート鍵である。彼女は、m と s を ボブ宛に送る。アリスだけが送ることができたメッセージを復元するために、ボブは、s**e (mod n) = m を計算する。ここで (e,n) は、アリス の公開鍵である。

データ発信元認証に加えてデータインテグリティを確保することは、追加的な計算ステップを要求し、ここで、アリスとボブは、暗号技術的ハッシュ関数 h を (デジタル署名について説明したように) 使う。アリスは、ハッシュ値 h(m) = v を計算し、次に v を彼女のプライベート鍵で s を得るために暗号化する。彼女は、m と s を送る。ボブは、m' と s' を受信し、これらのいすれもが、アリスが送信した m と s から変更されている可能性がある。これをテストするのに、彼は、v' を得るために s' を アリスの公開鍵で復号する。彼は、次に、h(m') = v" を計算する。v' が v" と等しい場合、ボブ は、m' はアリスが送った m と同一のものであると確信できる。

- SHA-1 (Secure Hash Algorithm 1) ※

SHA-1（Secure Hash Algorithm）という、2**64 ビット未満の長さのいかなる入力について、160 ビットの出力（ハッシュ結果）を作り出す暗号技術的ハッシュ関数を規定する米国政府標準。

- SHA-256

FIPS 180-2 SECURE HASH STANDARD として SHA-1 と共に、規定されたハッシュ関数群の中の 256 ビットのハッシュ値を出力するＭＤ型ハッシュ関数である。

- SSL（Secure Socket Layer） ※

（もともと Netscape Communications 社によって開発された）インターネットプロトコル。これは、クライアント（しばしば、Web ブラウザ）とサーバの間のトラフィックにデータ守秘性サービスおよびデータ インテグリティサービスを提供し、オプションとしてクライアントとサーバ間におけるピア主体認証を提供できるようにするためのコネクション指向の「エンド to エンド」暗号化を使う 。

SSL は、HTTP の下、かつ、信頼できる TCP（トランスポートプロトコル）の上の層である。SSL は、 カプセル化するアプリケーションとは独立しており、いかなる上位層プロトコルも、SSL 上に透過的にのせることができる。しかし、多くのインターネットアプリケーションは、IPsec によってより良く提供される可能性がある。

SSL は、2 つの層をもつ。

(a) SSL の下位側の層である SSL レコード プロトコルは、トランスポートプロトコルの上に位置し、上位層のプロトコルをカプセル化する。このようなカプセル化されたプロトコルのひとつが SSL ハンドシェイク プロトコルである。

(b) SSL の上位側の層は、サーバ認証用に（サーバの身元をクライアントに対して検証する）公開鍵暗号技術を提供し、オプションとしてのクライアント認証用に（クライアントの身元をサーバに対して検証する）公開鍵暗号技術を提供し、さらに、そのアプリケーションプロトコルがデータを転送／受信する前に、それらが（データ の守秘性保護のために使う）共通鍵暗号化アルゴリズムおよび秘密のセッション鍵を交渉できるようにする。鍵付ハッシュは、カプセル化されたデータにデータインテグリティサービスを提供する。

- S/MIME ※

Secure/Multipurpose Internet Mail Extensions。インターネットメールメッセージについて、暗号化とデジタル署名を提供するインターネットプロトコルのひとつ。

- TLS(Transport Layer Security) ※

TLS バージョン 1.0 は、SSL バージョン 3.0 に基づいた、同様のインターネットプロトコルである。

TLS プロトコルは、誤称である。それは、これは、トランスポート層（OSI 第 4 層）上で動作するからである。

V－X

- X.500　※

ITU-T 勧告。これは、X.500 ディレクトリを規定する ITU-T/ISO 共同の複数パート標準（X.500 - X.525）の一部であり、OSI 主体、プロセス、アプリケーションおよびサービスに分散型のディレクトリ機能を提供するシステムの概念的な収集である。（ISO における同等のものは、IS 9594-1 および関連する標準 IS 9594-x である。）

X.500 ディレクトリは、木（ディレクトリ情報の木）として構築されており、情報は、ディレクトリ項目に保管される。各エントリは、オブジェクトについての情報の収集であり、各オブジェクトは、DN をもつ。ディレクトリのエントリは、各々種別と、ひとつもしくは複数の値をもつ属性から成る。例えば、PKI が証明書を配布するためにディレクトリを使う場合、エンドユーザの X.509 公開鍵証明書は、通常、ディレクトリ項目中の「証明書の対象である DN をもつ "userCertificate" 種類」の属性値として保管される。

- X.509　※

ITU-T 勧告。データ発信元認証サービスとピア主体認証サービスを提供しサポートするフレームワークを規定する。X.509 公開鍵証明書、X.509 属性証明書、X.509 CRL についてのフォーマットを含む。（ISO における同等物は、IS 9498-4。）

X.509 は、2 つのレベルの認証を記述している。パスワードに基づく「シンプル認証」と、公開鍵証明書に基づく「ストロング認証」。

- X.509 v3　※

X.509 v1 か v2 か v3 によって規定されたフォーマットのひとつで表現された公開鍵証明書。（X.509 公開鍵証明書 についての v1 と v2 の指定は、X.509 CRL についての v1 と v2 の指定と、X.509 属性証明書についての v1 の指定によって、支離滅裂なものとされた。）

X.509 公開鍵証明書は、一連のデータ要素を含み、そのシーケンスに基づいて計算されるデジタル署名をもつ。この署名に加えて、3 つのバージョンすべてが、下記の 1 から 7 までの要素を含む。v2 と v3 証明書のみが、8 と 9 も含む可能性があり、v3 のみが 10 を含む可能性がある。

以上