

キャンパス PKI CP/CPS テンプレート  
インソース編

初版 (Ver.1.0)

平成 20 年 3 月 31 日

目次

<b>1. はじめに</b> .....	<b>1</b>
1.1 概要.....	1
1.2 文書名称と定義.....	1
1.3 PKI の関係者.....	1
1.4 証明書の用途.....	2
1.4.1 証明書の種類.....	2
1.4.2 正規の証明書用途.....	2
1.4.3 禁止されている証明書用途.....	2
1.5 ポリシー管理.....	2
1.5.1 文書の管理組織.....	2
1.5.2 窓口.....	2
1.5.3 ポリシーに対する CPS の準拠性調査担当者.....	2
1.5.4 CP/CPS の承認手続き.....	2
1.6 定義と略称.....	2
<b>2. 公開とリポジトリの責任</b> .....	<b>3</b>
2.1 リポジトリ.....	3
2.2 認証情報の公開.....	3
2.3 公開の時期と周期.....	3
2.4 リポジトリに対するアクセスコントロール.....	3
<b>3. 本人性確認と認証</b> .....	<b>4</b>
3.1 名称.....	4
3.1.1 名称のタイプ.....	4
3.1.2 名称の意味に関する要件.....	4
3.1.3 利用者の匿名・仮名について.....	4
3.1.4 様々な名称形式を解釈するためのルール.....	4
3.1.5 名称の一意性.....	4
3.1.6 商標等の認識、認証及び役割.....	4
3.2 初回の利用者の本人性確認.....	4
3.2.1 秘密鍵の所有を検証する方法.....	4
3.2.2 利用者の確認.....	5
3.2.3 確認しない利用者の情報.....	5
3.2.4 権限確認.....	5
3.2.5 相互運用性基準.....	5
3.2.6 鍵更新時の本人性確認.....	5
3.2.7 失効後の証明書再発行時の本人性確認.....	5
3.3 失効申請時の本人性確認と認証.....	5
<b>4. 証明書のライフサイクル</b> .....	<b>6</b>
4.1 証明書申請.....	6
4.1.1 証明書申請を提出することができる者.....	6
4.1.2 登録手続きと責任.....	6
4.2 証明書申請手続き.....	6

4.2.1	本人性確認と認証機能の実行.....	6
4.2.2	証明書申請の承認または却下.....	6
4.2.3	証明書申請の処理時間.....	6
4.3	証明書発行.....	7
4.3.1	証明書発行時の認証局の行動.....	7
4.3.2	利用者に対する証明書発行通知.....	7
4.4	証明書受領.....	8
4.4.1	証明書受領手続き.....	8
4.4.2	認証局による証明書の公開.....	8
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.....	8
4.5	鍵ペアと証明書の用途.....	8
4.5.1	利用者による秘密鍵及び証明書の使用.....	8
4.5.2	信託者による公開鍵及び証明書の使用.....	8
4.6	鍵更新を伴わない証明書の更新.....	9
4.7	鍵更新を伴う証明書の更新.....	9
4.7.1	更新事由.....	9
4.7.2	新しい利用者証明書の発行申請が出来る者.....	9
4.7.3	証明書の鍵更新申請の処理.....	9
4.7.4	利用者に対する新しい証明書の通知.....	9
4.7.5	鍵更新された証明書の受領確認.....	9
4.7.6	認証局による更新済みの証明書の公開.....	9
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.....	9
4.8	証明書の変更.....	10
4.8.1	証明書変更に関する要件.....	10
4.8.2	証明書の変更を申請できる者.....	10
4.8.3	変更申請の処理.....	10
4.8.4	利用者に対する新しい証明書の通知.....	10
4.8.5	変更された証明書の受領確認の行為.....	10
4.8.6	認証局による変更された証明書の公開.....	10
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.....	10
4.9	証明書の失効と一時停止.....	11
4.9.1	失効事由.....	11
4.9.2	証明書の失効申請が出来る者.....	11
4.9.3	証明書の失効申請手続き.....	11
4.9.4	失効申請の猶予期間.....	12
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.....	12
4.9.6	信託者の失効確認の要求.....	12
4.9.7	証明書失効リストの発行頻度.....	12
4.9.8	証明書失効リストの発行最大遅延時間.....	12
4.9.9	オンラインでの失効ステータス確認の適用性.....	12
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.....	12
4.9.11	利用可能な失効通知の他の形式.....	12
4.9.12	鍵更新の危殆化に対する特別要件.....	12
4.9.13	証明書の一時停止.....	13
4.9.14	相互認証証明書の失効.....	13
4.10	証明書のステータス確認サービス.....	13

4.10.1	運用上の特徴	13
4.10.2	サービスの利用可能性	13
4.10.3	オプションな仕様	13
4.11	利用の終了	13
4.12	キーエスクローとリカバリ	13
<b>5.</b>	<b>設備、管理、運用上の統制</b>	<b>14</b>
5.1	物理的管理	14
5.1.1	立地場所及び構造	14
5.1.2	物理的アクセス	14
5.1.3	電源及び空調	15
5.1.4	水害対策	15
5.1.5	火災防止及び火災保護対策	15
5.1.6	媒体保管場所	15
5.1.7	廃棄処理	15
5.1.8	施設外のバックアップ	15
5.2	手続き的管理	15
5.2.1	信頼すべき役割	15
5.2.2	職務ごとに必要とされる人数	16
5.2.3	個々の役割に対する本人性の確認と認証	16
5.2.4	職務分割が必要となる役割	16
5.3	人事的管理	16
5.3.1	経歴、資格、経験等に関する要求事項	16
5.3.2	教育訓練要件	16
5.3.3	教育訓練の周期	16
5.3.4	ジョブローテーションの周期と順序	16
5.3.5	許可されていない行動に対する罰則	17
5.3.6	職員に対する契約要件	17
5.3.7	職員が参照できるドキュメント	17
5.4	監査ログの手続き	17
5.4.1	記録されるイベントの種類	17
5.4.2	監査ログを処理する頻度	17
5.4.3	監査ログを保持する期間	17
5.4.4	監査ログの保護	17
5.4.5	監査ログのバックアップ手続き	17
5.4.6	監査ログの収集システム	18
5.4.7	イベントを起こしたサブジェクトへの通知	18
5.4.8	脆弱性評価	18
5.5	記録のアーカイブ	18
5.5.1	アーカイブ記録の種類	18
5.5.2	アーカイブ保持期間	18
5.5.3	アーカイブの保護	18
5.5.4	アーカイブのバックアップ手続き	18
5.5.5	記録にタイムスタンプを付ける要件	18
5.5.6	アーカイブ収集システム	18
5.5.7	アーカイブの情報を入手し検証する手続	18
5.6	鍵の切り替え	18

5.7	危殆化及び災害からの復旧.....	19
5.7.1	事故及び危殆化の取り扱い手続き.....	19
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.....	19
5.7.3	災害後の事業継続能力.....	19
5.8	認証局の業務終了.....	19
<b>6.</b>	<b>技術的セキュリティ管理.....</b>	<b>20</b>
6.1	鍵ペアの生成及びインストール.....	20
6.1.1	鍵ペアの生成.....	20
6.1.2	利用者に対する秘密鍵の配付.....	20
6.1.3	認証局への公開鍵の配付.....	20
6.1.4	信頼者に対する認証局公開鍵の配付.....	20
6.1.5	鍵サイズ.....	20
6.1.6	公開鍵パラメータの生成及び品質検査.....	21
6.1.7	鍵用途の目的.....	21
6.2	秘密鍵の保護及び暗号モジュール技術の管理.....	21
6.2.1	暗号モジュールの標準及び管理.....	21
6.2.2	秘密鍵の複数人管理.....	21
6.2.3	秘密鍵のエスクロー.....	21
6.2.4	秘密鍵のバックアップ.....	21
6.2.5	秘密鍵のアーカイブ.....	21
6.2.6	秘密鍵の暗号モジュールへの転送.....	21
6.2.7	暗号モジュールへの秘密鍵の格納.....	22
6.2.8	秘密鍵の活性化方法.....	22
6.2.9	秘密鍵の非活性化方法.....	22
6.2.10	秘密鍵の破棄方法.....	22
6.2.11	暗号モジュールの評価.....	22
6.3	その他の鍵ペア管理.....	22
6.3.1	公開鍵のアーカイブ.....	22
6.3.2	証明書の運用上の期間及び鍵ペアの使用期間.....	22
6.4	活性化データ.....	22
6.4.1	活性化データの生成及び設定.....	22
6.4.2	活性化データの保護.....	23
6.4.3	活性化データの他の考慮点.....	23
6.5	コンピュータのセキュリティ管理.....	23
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.....	23
6.5.2	コンピュータセキュリティ評価.....	23
6.6	ライフサイクルの技術上の管理.....	23
6.6.1	システム開発管理.....	23
6.6.2	セキュリティ運用管理.....	23
6.6.3	ライフサイクルのセキュリティ管理.....	23
6.7	ネットワークセキュリティ管理.....	23
6.8	タイムスタンプ.....	24
<b>7.</b>	<b>証明書、失効リスト、OCSP のプロファイル.....</b>	<b>25</b>
7.1	証明書プロファイル.....	25
7.1.1	バージョン番号.....	25

7.1.2	証明書拡張領域 .....	25
7.1.3	アルゴリズムオブジェクト識別子 .....	25
7.1.4	名前の形態 .....	25
7.1.5	名前制約 .....	25
7.1.6	証明書ポリシーオブジェクト識別子 .....	25
7.1.7	ポリシー制約拡張の使用 .....	25
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 .....	25
7.1.9	重要な証明書ポリシー拡張についての処理方法 .....	25
7.2	CRL、ARL プロファイル .....	26
7.2.1	バージョン番号 .....	26
7.2.2	CRL、CRL エントリ拡張 .....	26
7.3	OCSP プロファイル .....	26
<b>8.</b>	<b>準拠性監査とその他の評価 .....</b>	<b>27</b>
8.1	監査の頻度 .....	27
8.2	監査人の要件 .....	27
8.3	監査人と非監査者との要件 .....	27
8.4	監査で扱われる事項 .....	27
8.5	監査における指摘事項への対応 .....	27
8.6	監査結果の開示 .....	27
<b>9.</b>	<b>他の業務上の問題及び法的問題 .....</b>	<b>28</b>
9.1	料金 .....	28
9.2	金銭上の責任 .....	28
9.2.1	保険の適用範囲 .....	28
9.2.2	その他の資産 .....	28
9.2.3	利用者を保護する保険、保証 .....	28
9.3	業務情報の機密性 .....	28
9.3.1	秘密情報の範囲 .....	28
9.3.2	秘密情報の範囲外の情報 .....	28
9.3.3	秘密情報を保護する責任 .....	28
9.4	個人情報の保護 .....	28
9.4.1	プライバシープラン .....	28
9.4.2	プライバシーとして扱われる情報 .....	29
9.4.3	プライバシーと見なされない情報 .....	29
9.4.4	個人情報を保護する責任 .....	29
9.4.5	個人情報の使用に関する個人への通知及び承諾 .....	29
9.4.6	司法手続きまたは行政手続きに基づく公開 .....	29
9.4.7	他の情報公開の場合 .....	29
9.5	知的財産権 .....	29
9.6	表明保証 .....	29
9.6.1	認証局の表明保証 .....	29
9.6.2	利用者の表明保証 .....	29
9.6.3	信賴者の表明保証 .....	30
9.6.4	他の関係者の表明保証 .....	30
9.7	無保証 .....	30
9.8	責任の制限 .....	31

9.9	補償.....	31
9.10	有効期間と終了.....	31
9.10.1	有効期間.....	31
9.10.2	終了.....	31
9.10.3	終了の影響と存続条項.....	31
9.11	関係者間の個別通知と連絡.....	31
9.12	改訂.....	31
9.12.1	改訂手続き.....	31
9.12.2	通知方法及び期間.....	31
9.12.3	オブジェクト識別子の変更されなければならない場合.....	32
9.13	紛争解決手段.....	32
9.14	準拠法.....	32
9.15	適用法の遵守.....	32
9.16	雑則.....	32
9.16.1	完全合意条項.....	32
9.16.2	権利譲渡条項.....	32
9.16.3	分離条項.....	32
9.16.4	強制執行条項.....	32
9.16.5	不可抗力.....	32
9.17	その他の条項.....	33
<b>別紙 1</b>	<b>証明書、ARL/CRL プロファイル例.....</b>	<b>34</b>
<b>別紙 2</b>	<b>用語集.....</b>	<b>37</b>
<b>別紙 3</b>	<b>本テンプレートについて.....</b>	<b>52</b>

---

## 1. はじめに

### 1.1 概要

大学電子認証局は、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、「大学電子認証局(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先との相互認証接続を行う。

大学電子認証局認証及び運用規定(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、信頼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、申請、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。

なお、本 CP/CPS の構成は、IETF PKIX による RFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework」に基づく。

### 1.2 文書名称と定義

本 CP/CPS の正式名称を「大学電子認証局ポリシー及び運用規程」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 (OID を記載)
- 相互認証証明書に記載する certificatePolicies (OID を記載)

### 1.3 PKI の関係者

- (1) 最高意思決定機関
- (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)、信頼者(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

## 1.4 証明書用途

### 1.4.1 証明書の種類

- (1) 自己署名証明書
- (2) 利用者証明書
- (3) 機器用証明書
- (4) 相互認証証明書

### 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/CPS 「1.4.2 正規の証明書用途」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。

## 1.5 ポリシー管理

### 1.5.1 文書の管理組織

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

### 1.5.2 窓口

規定しない。

### 1.5.3 ポリシーに対する 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。

### 1.5.4 CP/CPS の承認手続き

本 CP/CPS の承認については、本認証局の最高意思決定機関である  が行う。

## 1.6 定義と略称

別紙 2 に規定する。

---

## 2. 公開とリポジトリの責任

### 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нда
- 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 は本 CP/CPS「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。

### 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。

---

## 3. 本人性確認と認証

### 3.1 名称

#### 3.1.1 名称のタイプ

本認証局が発行する利用者証明書の主体者 (Subject) である利用者は、利用者証明書の中の 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。

#### 3.1.3 利用者の匿名・仮名について

規定しない。

#### 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、本 CP/CPS 「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。

### 3.2 初回の利用者の本人性確認

#### 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。

### 3.2.2 利用者の確認

利用者は、大学の学生、教職員に限定される。利用者の本人性確認は、入学、進学、採用時等に行われ、大学に所属する利用者本人を特定する情報は大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。

### 3.2.4 権限確認

本認証局は、代理人が利用者証明書を申請し、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。

本認証局は、相互認証先との相互認証接続を行う。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。

### 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。

## 3.3 失効申請時の本人性確認と認証

利用者本人による失効申請の場合、本認証局は利用者証明書の失効申請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及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け付ける。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、利用者进行を特定できる方法により本人性の確認を行う。

---

## 4. 証明書のライフサイクル

### 4.1 証明書申請

#### 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、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思決定機関である に対して証明書発行の申請を行い、 の承認を得て発行局に発行の指示を行う。

#### 4.1.2 登録手続きと責任

本認証局は、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。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、最高意思決定機関である の承認後、相互認証証明書の発行を行う。

### 4.2 証明書申請手続き

#### 4.2.1 本人性確認と認証機能の実行

本認証局は、本 CP/CPS「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 証明書申請の承認または却下

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。

#### 4.2.3 証明書申請の処理時間

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。

## 4.3 証明書発行

### 4.3.1 証明書発行時の認証局の行動

#### (1) 自己署名証明書

認証局責任者は自己署名証明書の発行について、最高意思決定機関である 〃 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。

#### (2) 利用者証明書

本認証局は、利用者の鍵ペア及び利用者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。

#### (3) 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。

### 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。

## 4.4 証明書受領

### 4.4.1 証明書受領手続き

#### (1) 利用者証明書

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。

#### (2) 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。

### 4.4.2 認証局による証明書の公開

利用者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。

### 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

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。

## 4.5 鍵ペアと証明書の用途

### 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/CPS 「1.4.2 正規の証明書用途」に示した証明書の用途以外に秘密鍵及び利用者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証明書を有効期限を越えて利用してはならない。

### 4.5.2 信頼者による公開鍵及び証明書の使用

信頼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証明書を利用する。利用者証明書の利用に際しては、本 CP/CPS 「9.6.3 信頼者の表明保証」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。

## 4.6 鍵更新を伴わない証明書の更新

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本 CP/CPS 「4.7 鍵更新を伴う証明書更新」に規定する。

## 4.7 鍵更新を伴う証明書の更新

### 4.7.1 更新事由

#### (1) 利用者証明書

本認証局は、利用者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証明書を発行する。利用者は、本 CP/CPS 「4.1 証明書申請」に示す新規の証明書発行申請手続きと同様の手続きを行う。

#### (2) 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、本 CP/CPS 「4.1 証明書申請」に示す新規の証明書発行申請手続きと同様の手続きを行う。

### 4.7.2 新しい利用者証明書の発行申請が出来る者

本 CP/CPS 「4.1.1 証明書申請を提出することができる者」と同様とする。

### 4.7.3 証明書の鍵更新申請の処理

本 CP/CPS 「4.3.1 証明書発行時の本認証局の行動」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/CPS 「4.3.2 利用者に対する証明書発行通知」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/CPS 「4.4.1 証明書受領手続き」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/CPS 「4.4.2 本認証局による証明書の公開」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/CPS 「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」と同様とする。



## 4.8 証明書の変更

### 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/CPS「4.9 証明書の失効と一時停止」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/CPS「4.3.2 利用者に対する証明書発行通知」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/CPS「4.4.1 証明書受領」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/CPS「4.4.2 認証局による証明書の公開」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/CPS「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」と同様とする。

## 4.9 証明書の失効と一時停止

### 4.9.1 失効事由

#### (1) 利用者証明書

##### (a) 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
- 利用者証明書の利用を中止する場合

##### (b) 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

#### (2) 相互認証証明書

##### (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

### 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

利用者が本 CP/CPS「4.9.1 失効事由」に定める失効事由により、利用者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、失効申請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請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請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/CPS「4.9.1 失効事由」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/CPS「4.9.1 失効事由」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 信頼者の失効確認の要求

信頼者は、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、48 時間有効な CRL/ARL を 24 時間ごとに発行する。

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/ARL を速やかにリポジトリに格納する。

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。

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

信頼者は、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出来る。

4.9.11 利用可能な失効通知の他の形式

規定しない。

4.9.12 鍵更新の危殆化に対する特別要件

規定しない。

#### 4.9.13 証明書の一時的停止

本認証局は、証明書の一時的停止を行わない。

#### 4.9.14 相互認証証明書の失効

規定しない。

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請が行われた場合、の検討及び承認後、相互認証証明書を失効する。失効申請は、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請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請を行う。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。

### 4.10 証明書のステータス確認サービス

#### 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 レスポンド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、本 CP/CPS 「2 公開とリポジトリの責任」において規定するリポジトリにおいて提供する。

#### 4.10.3 オプションな仕様

規定しない。

### 4.11 利用の終了

利用者が証明書の利用を終了する場合、本 CP/CPS 「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。

### 4.12 キーエスクローとリカバリ

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。

## 5. 設備、管理、運用上の統制

### 5.1 物理的管理

#### 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ま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) 登録用端末設置室

申請受付、審査、登録用端末を用いた利用者証明書の発行指示、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認証設備室の管理責任者が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入室権限者が IC カードによる認証、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、定期的にチェックする。

認証設備を設置するラックは、認証設備専用であり、物理鍵により施錠管理される。物理鍵は開錠権限者と異なる職員により管理する。ラックの開錠は開錠権限を有する複数人の立会いの下で行い、また開施錠及の記録を残し、これを定期的にチェックする。

認証設備の操作は、権限を有する複数人の立会いの下で可能とする。

権限を有しない者が認証設備にアクセスする場合は、権限を有する複数人の同行が必要である。権限を持たない者の認証設備へのアクセス時は、その目的を確認した上で、権限を有する複数人の同行の下で行い、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。

認証設備への物理的アクセスについては以下の管理が実施されている。

- 専用ラックの物理鍵による施錠管理
- 認証設備室への IC カード等の認証操作による入退室管理、及び入退室情報の記録

- 認証設備室への入室権限の事前付与
- 認証設備室の入退室に用いる IC カードの貸与記録の管理 (IC カードの使用者の適切な識別)
- 認証設備室内の監視カメラによる継続的な監視の実施及びその記録
- ラックの開錠記録
- ラックの鍵の施錠された場所での保管管理と、複数人の鍵の管理者による貸出承認及びその記録
- ラックの鍵の管理者と開錠権限者 (認証設備の操作権限者) の権限分離

### 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、防水堤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

建物は容易に火災が発生しない構造である。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。

## 5.2 手続き的管理

### 5.2.1 信頼すべき役割

本認証局は、次の職制を信頼する。

- 最高意思決定機関

- 認証局責任者
- 発行局責任者
- 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、職員証明書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

- 最高意思決定機関 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
- 発行局責任者及び発行局オペレータと認証システム管理者

### 5.3 人事的管理

#### 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、業務に配置される。

#### 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。

### 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 CP/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

本認証局の職員は、大学が別途定める職務規定及びセキュリティポリシーに関する規定に従うものとする。

また、認証局業務の一部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。

## 5.4 監査ログの手続き

### 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、登録用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/CPS「5.4.1 記録されるイベントの種類」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/CPS「5.4.1 記録されるイベントの種類」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、本 CP/CPS「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。

### 5.5 記録のアーカイブ

#### 5.5.1 アーカイブ記録の種類

本認証局は、本 CP/CPS「5.4.1 記録されるイベントの種類」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/CPS「5.4.3 監査ログを保持する期間」と同様とする。

#### 5.5.3 アーカイブの保護

本 CP/CPS「5.4.4 監査ログの保護」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/CPS「5.4.5 監査ログのバックアップ手続き」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/CPS「5.4.1 記録されるイベントの種類」及び「5.5.1 アーカイブ記録の種類」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/CPS「5.4.6 監査ログの収集システム」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/CPS「5.4.1 記録されるイベントの種類」及び「5.5.1 アーカイブ記録の種類」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。

### 5.6 鍵の切り替え

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。

## 5.7 危殆化及び災害からの復旧

### 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し、最高意思決定機関である 〃〃〃 の承認を得る。

- 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、リポジ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。

### 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。

## 5.8 認証局の業務終了

本認証局が認証業務を廃止する場合、廃止日の3ヶ月前までにリポジトリ上で告知、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。

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、リポジトリにて公開する。この際、CRL/ARLは日次での更新は行わない。

---

## 6. 技術的セキュリティ管理

### 6.1 鍵ペアの生成及びインストール

#### 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、耐タンパ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本 CP/CPS 「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/CPS 「4.3.1 証明書発行時の認証局の行動」に規定する。

#### 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。

#### 6.1.4 信頼者に対する認証局公開鍵の配付

信頼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) 利用者証明書

利用者証明書に係る鍵は、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

### 6.1.6 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耐タンパ装置により生成される。

#### (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。

### 6.1.7 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 レスポンド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

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。

## 6.2 秘密鍵の保護及び暗号モジュール技術の管理

### 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 2 相当の基準を満たすものを使用する。

### 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耐タンパ装置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耐タンパ装置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。

### 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。

### 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 カードリーダー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 2 相当の基準を満たし、日本国内において稼働実績のあるものを使用する。

## 6.3 その他の鍵ペア管理

### 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証明書は、本 CP/CPS「5.4.3 監査ログを保持する期間」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 6.5 年
- 利用者証明書 利用者に応じ((1 年 ~ 6 年) + 30 日)
- 相互認証証明書 6.5 年

## 6.4 活性化データ

### 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。

### 6.5 コンピュータのセキュリティ管理

#### 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。

### 6.6 ライフサイクルの技術上の管理

#### 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。

### 6.7 ネットワークセキュリティ管理

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。

## 6.8 タイムスタンプ

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。

---

## 7. 証明書、失効リスト、OCSP のプロファイル

### 7.1 証明書プロファイル

#### 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、利用者証明書を発行する。

#### 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 1 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。

#### 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。

#### 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 1 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 1 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 1 に示す。



## 7.2 CRL、ARL プロファイル

### 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 1 に示す。

### 7.2.2 CRL、CRL エントリ拡張

別紙 1 に示す。

## 7.3 OCSP プロファイル

本認証局が用いる OCSP レスポンドは、RFC2560 に準拠している。OCSP レスポンドに対し、リクエストを行う場合は、reqCert の項目として別紙 1 に示すフィールドを含める。

OCSP レスポンドは、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 レスポンドは、BasicOCSPResponse には、別紙 1 に示すフィールドを含む。

---

## 8. 準拠性監査とその他の評価

### 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。

### 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 CP/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、相互認証証明書及び利用者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、 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。

### 8.6 監査結果の開示

監査結果は、相互認証先及び が認めた対象にのみ開示される。

---

## 9. 他の業務上の問題及び法的問題

### 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。

#### 9.2.2 その他の資産

規定しない。

#### 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。

#### 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/CPS「9.3.2 秘密情報の範囲外の情報」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。

### 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 CP/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

本認証局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) 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) 本 CP/CPS「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) 電子証明書利用申請書に則り、正しい証明書を発行する
- (5) 本 CP/CPS「4.9.3 証明書の失効申請手続き」に従って利用者証明書の失効処理を行う

#### 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

本 CP/CPS「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、十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 で定めた利用者証明書の失効、発行申請等の手続きを遵守し、虚偽の申請を行ってはならない。

(4) 利用者証明書の速やかな失効申請の届出

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

信頼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) CP/CPS への同意

信頼者は、利用者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本 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証明書は、本 CP/CPS 「4.5.2 信頼者による公開鍵及び証明書の使用」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。

## 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本 CP/CPS 「9.6.2 利用者の表明保証」及び本 CP/CPS 「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

利用者が本 CP/CPS「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本 CP/CPS「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 CP/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。本 CP/CPS「9.10.2 終了」で記述する本 CP/CPS の終了以前に本 CP/CPS が無効となることはない。

### 9.10.2 終了

本 CP/CPS は、本 CP/CPS「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、本 CP/CPS の 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。

## 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 をリポジ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の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、本学の判断により本認証局のポ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。

## 9.16 雑則

### 9.16.1 完全合意条項

本 CP/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。

### 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。

### 9.16.5 不可抗力

- (1) 本認証局は、利用者が利用者証明書を取得、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請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。



## 別紙 1 証明書、ARL/CRL プロファイル例

(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	利用者証明書	備考
authorityKeyIdentifier			FALSE
subjectKeyIdentifier			FALSE
keyUsage	<ul style="list-style-type: none"> <li>・keyCertSign</li> <li>・cRLSign</li> </ul>	<ul style="list-style-type: none"> <li>・digitalSignature</li> <li>・keyEncipherment</li> </ul>	TRUE
extendedKeyUsage		<ul style="list-style-type: none"> <li>・clientAuth</li> <li>・MS-smartCardLogon</li> </ul>	TRUE
privateKeyUsagePeriod			FALSE
certificatePolicies		CPS 公開用 URL	TRUE
policyMapping			FALSE
subjectAltName		<ul style="list-style-type: none"> <li>・Microsoft 社</li> <li>UserPrincipalName</li> </ul>	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

(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			
crlExtensions			

<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

(3) OCSP プロファイル例

OCSP リクエスト中の reqCert

領域名	型	値	備考
reqCert			
hashAlgorithm	AlgorithmIdentifier	-	
issuerNameHash	OCTET STRING	-	
issuerKeyHash	OCTET STRING	-	
serialNumber	INTEGER	-	

BasicOCSPResponse の tbsResponseData

領域名	型	値	備考
version	INTEGER		v1 を表す
responderID			
byName			
countryName	OID	2 5 4 6	
	PrintableString	JP	
organizationName	OID	2 5 4 10	
	PrintableString	University	
commonName	OID	2 5 4 3	
	PrintableString	University PrivateCA OCSP Responder	
producedAt	GeneralizedTime	yyymmddhhmmssZ	署名時刻
responses			
certID			
hashAlgorithm	AlgorithmIdentifier		
issuerNameHash	OCTET STRING		
issuerKeyHash	OCTET STRING		
serialNumber	INTEGER		
certStatus		Good[0],revoked[1],unknown[2] から選択	
thisUpdate	GeneralizedTime	yyymmddhhmmssZ	失効情報の 確認時刻

---

## 別紙 2 用語集

RFC2828<sup>1</sup>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。

---

<sup>1</sup> <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、パズフレーズ等を指す。

- 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ものみ必要である。

- 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、渴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、鍵生成及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、トークンの配布及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、身元認証及び名前の割り当て、鍵生成、及び、鍵ペア、トークン配布及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及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、署名を正しく作成したり、変更したりすることについて、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、証明書を作成及び割り当てる機関。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、証明書の種類及び適用する 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)。

(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である。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認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 及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。

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、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 (多義の可能性もある) 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)

コンピュータ及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)、及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

FIPS140-2 で定義している 4 段階のセキュリティレベルを以下に示す。

- レベル 1: FIPS で定義している最低限のセキュリティレベルで、情報を保護するための専用の機構を必要としないレベル。IC カードや PC 上のソフトウェアなど。
- レベル 2: 暗号モジュールに、不正アクセスした場合に侵入を検知できる仕組みを備えたレベル。
- レベル 3: 暗号モジュール内の情報を不正に取り出そうとした場合に、情報を消滅させる機構を備えたレベル。
- レベル 4: 最も高いセキュリティレベルで、いかなる方法をもってしても暗号モジュール内に侵入できない機構を備えたレベル。

- FQDN (Fully Qualified Domain Name)

ドメイン名に、サブドメイン名及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

- IC カード (IC Card, Smart Card)

コンピュータの CPU、メモリ及び入出力インタフェー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である。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 及び 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、鍵管理及びトークン管理機能を行う認証局(及び、オプションとして登録局及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、及び手順であり、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(及び、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及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)

X.509 形式に基づいた公開鍵インフラ。

- 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)及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ン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 及び 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、 $m^{**}e \pmod n = c$  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、 $c^{**}d \pmod n = m$  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  $c^{**}d \pmod n = m$  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、 $m^{**}d \pmod n = s$  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、 $s^{**}e \pmod n = m$  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、これらのいずれもが、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及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及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、アプリケーション及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 及び関連する標準 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。

- X.509 v3 key usage

証明書エクステンションの一つで、鍵が利用される目的を設定する項目のこと。デジタル署名、否認防止等の鍵利用目的がある。

以上

---

## 別紙 3 本テンプレートについて

本テンプレートは、UPKIに参加する大学のキャンパス PKI 認証局の CP/CPS のテンプレートを「キャンパス PKI CP/CPS ガイドライン インソース編」に基づいて作成したものです。

本テンプレートの内容は、必要に応じて変更することがあります。本テンプレートをご利用頂く方へその都度ご連絡はいたしかねますので、ご利用の際には本テンプレートの最新の内容をご参考にしてください。

本テンプレート、及びこれらの二次的著作物については、大学共同利用機関法人 情報・システム研究機構 国立情報学研究所に無断で複製、送信、放送、配付、貸与、翻訳、変造、翻案することは、著作権侵害となり、法的に罰せられるほか、損害賠償を請求されることがあります。

本テンプレートを通じて提供される情報、文章等について、時間の経過による変化や UPKI 相互認証方式等によって、変更や追加、削除が必要な場合があります。従って、本テンプレートの完全性、正確性、安全性等いかなる保証も行いません。

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所は、本テンプレートの内容に関し、いかなる保証も行わず、これに起因して利用者やユーザの方に発生したトラブルや損害等について、一切責任を負いません。