国立大学法人 東京工業大学

認証局証明書ポリシー（CP）
認証運用規程（CPS）

Ver. 1.0

平成19年3月12日 策定

国立大学法人 東京工業大学

1 はじめに....1
1.1 概要....1
1.2 文書名と識別....1
1.3 PKIの関係者....1
1.3.2 登録局....2
1.3.3 加入者....2
1.3.4 利用者....2
1.3.5 その他の関係者....2
1.4 証明書の用途....2
1.4.1 適切な証明書の用途....2
1.4.2 禁止される証明書の用途....2
1.5 ポリシー管理....2
1.5.1 文書を管理する組織....2
1.5.2 連絡先....3
1.5.3 ポリシー適合性を決定する者....3
1.5.4 承認手続き....3
1.6 定義と略語....3
2 公開とリポジトリの責任....6
2.1 リポジトリ....6
2.2 証明書情報の公開....6
2.3 公開の時期または頻度....6
2.4 リポジトリへのアクセス管理....7
3 識別及び認証....7
3.1 名前決定....7
3.1.1 名前の種類....7
3.1.2 名前が意味を持つことの必要性....7

3.1.3　加入者の匿名性または仮名性 7
3.1.4　種々の名前形式を解釈するための規則 7
3.1.5　名前の一意性 7
3.1.6　認識・認証及び商標の役割 7

3.2　初回の本人性確認 7
3.2.1　私有鍵の所持を証明する方法 7
3.2.2　組織の認証 7
3.2.3　個人の認証 8
3.2.4　検証されない加入者の情報 8
3.2.5　権限の正当性確認 8
3.2.6　相互運用の基準 8

3.3　鍵更新申請時の本人性確認及び認証 8
3.3.1 通常の鍵更新時における本人性確認と認証 8
3.3.2　証明書失効後の鍵更新における本人性確認と認証 8

3.4　失効申請時の本人性確認と認証 8

4　証明書のライフサイクルに対する運用上の要件 8

4.1　証明書申請 8
4.1.1　証明書申請を提出することができる者 8
4.1.2　申請手続及び責任 9

4.2　証明書申請手続き 9
4.2.1　本人性確認と認証の実施 9
4.2.2　証明書申請の承認または却下 9
4.2.3　証明書申請の処理時間 9

4.3　証明書の発行 9
4.3.1　証明書発行時の処理手続 9
4.3.2　加入者への証明書発行通知 9

4.4 証明書の受理確認 9
4.4.1　証明書の受領確認手続 9
4.4.2　認証局による証明書の公開 10
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 10

4.5 鍵ペア及び証明書の用途 10
4.5.1 加入者の私有鍵及び証明書の用途 10
4.5.2 利用者の公開鍵及び証明書の用途 10

4.6 証明書の更新 11
4.6.1 証明書の更新事由 11
4.6.2 証明書の更新を申請することができる者 11
4.6.3 証明書の更新申請の処理 11
4.6.4 加入者に対する新しい証明書発行通知 11
4.6.5 更新された証明書の受領確認の行為 11
4.6.6 認証局による更新された証明書の公開 11
4.6.7 他のエンティティに対する認証局の証明書発行通知通知 11

4.7 鍵更新を伴う証明書の更新 11
4.7.1 更新事由 11
4.7.2 新しい証明書の申請を行なうことができる者 11
4.7.3 更新申請の処理 11
4.7.4 加入者に対する新しい証明書の通知 11
4.7.5 鍵更新された証明書の受領確認手続き 12
4.7.6 認証局による鍵更新済みの証明書の公開 12
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 12

4.8 証明書の変更 12
4.8.1 証明書の変更事由 12
4.8.2 証明書の変更を申請することができる者 12
4.8.3 変更申請の処理 12
4.8.4 加入者に対する新しい証明書発行通知 12
4.8.5 変更された証明書の受領確認の行為 12
4.8.6 認証局による変更された証明書の公開 12
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 12

4.9 証明書の失効と一時停止 12
4.9.1 証明書失効事由 12
4.9.2 証明書失効を申請することができる者 13
4.9.3 失効申請手続 13
4.9.4 失効申請の猶予期間 13
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 13
4.9.6 失効調査の要求 13

4.9.7　証明書失効リストの発行頻度 14
4.9.8　証明書失効リストの発行最大遅延時間 14
4.9.9　オンラインでの失効/ステイタス確認の適用性 14
4.9.10　オンラインでの失効/ステイタス確認を行なうための要件 14
4.9.11　利用可能な失効情報の他の形式 14
4.9.12　鍵の危殆化に対する特別要件 14
4.9.13　証明書の一時停止事由 14
4.9.14　証明書の一時停止を申請することができる者 14
4.9.15　証明書の一時停止申請手続 14
4.9.16　一時停止を継続することができる期間 14

4.10　証明書のステイタス確認サービス 14
4.10.1　運用上の特徴 14
4.10.2　サービスの利用可能性 15
4.10.3　オプショナルな仕様 15

4.11　加入(登録)の終了 15

4.12　キーエスクローと鍵回復 15
4.12.1　キーエスクローと鍵回復ポリシー及び実施 15
4.12.2　セッションキーのカプセル化と鍵回復のポリシー及び実施 15

5　設備上・運営上・運用上の管理 15

5.1　物理的管理 15
5.1.1　立地場所及び構造 15
5.1.2　物理的アクセス 15
5.1.3　電源及び空調 15
5.1.4　水害対策 16
5.1.5　火災防止及び火災保護対策 16
5.1.6　媒体保管 16
5.1.7　廃棄処理 16
5.1.8　オフサイトバックアップ 16

5.2　手続的管理 16
5.2.1　信頼すべき役割 16
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確認と認証 16

5.2.4 職務分割が必要になる役割 16

5.3 人事的管理 17

5.3.1 資格・経験及び身分証明の要件 17
5.3.2 背景調査 17
5.3.3 教育要件 17
5.3.4 再教育の頻度及び要件 17
5.3.5 仕事のローテーションの頻度及び順序 17
5.3.6 認められていない行動に対する制裁 17
5.3.7 独立した契約者の要件 17
5.3.8 要員へ提供される資料 17

5.4 監査ログの手続 18

5.4.1 記録されるイベントの種類 18
5.4.2 監査ログを処理する頻度 18
5.4.3 監査ログを保存する期間 18
5.4.4 監査ログの保護 18
5.4.5 監査ログのバックアップ手続 18
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者への通知 19
5.4.8 脆弱性評価 19

5.5 記録の保管 19

5.5.1 アーカイブの種類 19
5.5.2 アーカイブ保存期間 19
5.5.3 アーカイブの保護 19
5.5.4 アーカイブのバックアップ手続 19
5.5.5 記録にタイムスタンプを付与する要件 19
5.5.6 アーカイブ収集システム 19
5.5.7 アーカイブの検証手続 20

5.6 鍵の切り替え 20

5.7 危殆化及び災害からの復旧 20

5.7.1 事故及び危殆化時の手続 20
5.7.2 ハードウェア，ソフトウェアまたはデータが破損した場合の手続 20
5.7.3 エンティティの私有鍵が危殆化した場合の手続 20
5.7.4 災害後の事業継続性 20

5.8 認証局または登録局の終了 20

6 技術的セキュリティ管理 21

6.1 鍵ペアの生成及びインストール 21
6.1.1 鍵ペアの生成 21
6.1.2 加入者に対する私有鍵の交付 21
6.1.3 認証局への公開鍵の送付 21
6.1.4 利用者へのCA公開鍵の配付 21
6.1.5 鍵のサイズ 21
6.1.6 公開鍵のパラメータ生成及び品質検査 21
6.1.7 鍵の使用目的 21

6.2 私有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 22
6.2.2 複数人による私有鍵の管理 22
6.2.3 私有鍵のエスクロウ 22
6.2.4 私有鍵のバックアップ 22
6.2.5 私有鍵のアーカイブ 22
6.2.6 私有鍵の暗号モジュールへのまたは暗号モジュールからの転送 22
6.2.7 暗号モジュールへの私有鍵の格納 22
6.2.8 私有鍵の活性化方法 22
6.2.9 私有鍵の非活性化方法 22
6.2.10 私有鍵の廃棄方法 22
6.2.11 暗号モジュールの評価 23

6.3 鍵ペア管理に関するその他の面 23
6.3.1 公開鍵のアーカイブ 23
6.3.2 私有鍵と公開鍵証明書の有効期間 23

6.4 活性化用データ 23
6.4.1 活性化データの生成及び設定 23
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 ライフサイクルセキュリティ管理 23
6.6.1 システム開発管理 24
6.6.2 セキュリティ運用管理 24
6.6.3 ライフサイクルのセキュリティ管理 24

6.7 ネットワークのセキュリティ管理 24

6.8 タイムスタンプ 24

7 証明書・証明書失効リスト及びOCSPのプロファイル 24

7.1 証明書プロファイル 24
7.1.1 バージョン番号 25
7.1.2 証明書の拡張 26
7.1.3 アルゴリズムオブジェクト識別子 27
7.1.4 名前の形式 27
7.1.5 名前制約 27
7.1.6 証明書ポリシーオブジェクト識別子 27
7.1.7 ポリシー制約拡張の使用 27
7.1.8 ポリシー修飾子の構文及び意味 27
7.1.9 クリティカルな証明書ポリシー拡張に対する解釈の方法 27

7.2 CRLプロファイル 27
7.2.1 バージョン番号 27
7.2.2 証明書失効リスト及び証明書失効リストエントリ拡張 28

7.3 OCSPプロファイル 29
7.3.1 バージョン番号 29
7.3.2 OCSP拡張 29

8 準拠性監査とその他の評価 29

8.1 監査の頻度 29

8.2 監査者の身元・資格 29

8.3 監査者と被監査者の関係 29

8.4 監査で扱われる事項 29

8.5 不備の結果としてとられる処置 29

8.6 監査結果の開示 29

9 他の業務上及び法的事項 29

9.1 料金 29

9.1.1 証明書の発行または更新料 29

9.1.2 証明書へのアクセス料金 30

9.1.3 失効またはステータス情報へのアクセス料金 30

9.1.4 その他のサービスに対する料金 30

9.1.5 払い戻し指針 30

9.2 財務的責任 30

9.2.1 保険の範囲 30

9.2.2 その他の資産 30

9.2.3 エンドエンティティに対する保険または保証 30

9.3 本学に帰属する情報の機密性 30

9.3.1 機密情報の範囲 30

9.3.2 機密情報の範囲外の情報 30

9.3.3 機密情報を保護する責任 31

9.4 個人情報の保護 31

9.4.1 プライバシープラン 31

9.4.2 プライバシーとして扱われる情報 31

9.4.3 プライバシーとはみなされない情報 31

9.4.4 個人情報を保護する責任 31

9.4.5 個人情報の使用に関する個人への通知及び承諾 31

9.4.6 司法手続または行政手続に基づく公開 32

9.4.7 他の情報公開の場合 32

9.5 知的財産権 32

9.6 表明保証 32

9.6.1 認証局の表明保証 32

9.6.2 登録局の表明保証 32

9.6.3 加入者の表明保証 32

9.6.4 利用者の表明保証 32

9.6.5　他の関係者の表明保証 33

9.7　無保証 33

9.8　責任の制限 33

9.9　補償 33

9.10　有効期間と終了 33

9.10.1　有効期間 33

9.10.2　終了 34

9.10.3　終了の効果と効果継続 34

9.11　関係者間の個別通知と連絡 34

9.12　改訂 34

9.12.1　改訂手続き 34

9.12.2　通知方法及び期間 34

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 34

9.13　紛争解決手続 34

9.14　準拠法 35

9.15　適用法の遵守 35

9.16　雑則 35

9.16.1　完全合意条項 35

9.16.2　権利譲渡条項 35

9.16.3　分離条項 35

9.16.4　強制執行条項（弁護士費用及び権利放棄） 35

9.16.5　不可抗力 35

9.17　その他の条項 36

1 はじめに

1．1　概要

国立大学法人東京工業大学認証局証明書ポリシー(Certificate Policy，以下「本CP」という)は，国立大学法人東京工業大学(以下「東京工業大学」という)が認証局(以下「CA」という)として発行する証明書に関するポリシーを規定するものである．また，東京工業大学認証運用規程(Certificate Practice Statement，以下「本CPS」という)は，東京工業大学のCA(以下「本CA」という)のポリシーを実践するための運用規則を定めるものである．東京工業大学においては，単一のCAを運用するためCPとCPSをまとめてCP/CPSとして取り扱う．東京工業大学はCAとして，本CP/CPSに基づき，加入者が利用するICカードに対して電子証明書(以下「証明書」という)を発行する．加入者は，証明書が格納されたICカードを利用することで，東京工業大学の教育・研究・事務処理システムへのアクセス及び電子文書への署名を行ない関連する業務等を行なうことができる．

本CP/CPSは，IETF(The Internet Engineering Task Force)が認証局運用のフレームワークとして提唱するRFC3647「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠する．

1．2　文書名と識別

本CP/CPSの正式名称を「国立大学法人東京工業大学認証局証明書ポリシー/認証運用規程」とする．
本CPに基づき発行される証明書には，次のOIDが割り当てられる．

表1.1 本CPで定めるOID

名称	オブジェクト識別子
東京工業大学認証・認可システム枝番	<東京工業大学組織OID>.1
認証ポリシー枝番	<東京工業大学組織OID>.1.1
認証ポリシー種別枝番	<東京工業大学組織OID>.1.1.1
CPS	<東京工業大学組織OID>.1.1.1.1
CP(X.509電子証明書格納用)	<東京工業大学組織OID>.1.1.1.2
ディレクトリスキーマ枝番	<東京工業大学組織OID>.1.2
ディレクトリスキーマ種別枝番	<東京工業大学組織OID>.1.2.1
属性	<東京工業大学組織OID>.1.2.1.1
オブジェクトクラス	<東京工業大学組織OID>.1.2.1.2

(東京工業大学組織OID=1.2.6.1.4.1.8732)

1．3　PKIの関係者

1．3．1　認証局

本CAは，登録局(RA)と証明書発行局(IA)から構成される．ただし，IAの管理・運用は外部委託とする（以下「IA外部委託業者」という）．IAは，証明書の発行・取消，CRL（Certificate Revocation List：証明書失効リスト）の開示，リポジトリの維持管理等を行なう．また，RAは，証明書の発行・取消を申請する申請者の実在性確認，本人性確認の審査及び証明書を発行・失効するための登録業務等を行なう．

本CAでは，認証局は複数の階層構成をとることができ，本CAの階層構成の頂点の認証局(ルートCA)は，本CP/CPSに準拠する他組織のルートCAと相互認証を行なうことがある．ただしその場合は，必要に応じて本CP/CPSの改訂を行なうことがある．

１．３．２　登録局

上記に含む．

１．３．３　加入者

加入者とは，本CAから証明書の発行を受け，東京工業大学の教育・研究・事務処理システムへのアクセス及び電子文書への署名のために当該証明書を利用する者をいう．ここで，加入者の範囲は次の通りとする．

- 本学構成員（教員，職員，非常勤職員，学生，その他本学が認めた者）
- 本学が認めた他組織の構成員

１．３．４　利用者

利用者とは，電子署名の付されたメッセージ等について，その電子署名が間違いなく加入者によって行なわれているということを検証する者をいう．

１．３．５　その他の関係者

規定しない．

１．４　証明書の用途

１．４．１　適切な証明書の用途

加入者は，本CAが発行する証明書を東京工業大学の教育・研究・事務処理システムへのアクセス及び電子文書への署名のために用いるものとする．

１．４．２　禁止される証明書の用途

本CAが発行する証明書の用途は「1.4.1 適切な証明書の用途」の通りであり，それ以外の利用に関しては本CAはその責を負わない．

１．５　ポリシー管理

１．５．１　文書を管理する組織

本CP/CPSの維持・管理は，国立大学法人東京工業大学情報セキュリティ委員会（以下「情報セキュリティ委員会」という）が行なう．

1．5．2　連絡先

本CP/CPSに関する問い合わせ先を以下のように定める．

東京工業大学 学術情報部 情報基盤課 認証認可システム係
〒152-8550 東京都目黒区大岡山2-12-1
受付時間：平日 9時～17時（休日・祝祭日及び年末年始休暇をのぞく）
電話番号：03-5734-3381
FAX番号：03-5734-3198
e-mailアドレス：query@nap.gsic.titech.ac.jp

1．5．3　ポリシー適合性を決定する者

本CPSの本CPへの適合性を決定する者は，情報セキュリティ委員会とする．

1．5．4　承認手続き

本CP/CPSは，情報セキュリティ委員会によって承認されるものとする．

1．6　定義と略語

（あ～ん）

- アーカイブ（Archive）
  電子証明書の発行・失効に関わる記録や，認証局のシステム運用に関わる記録等を保管すること．
- 暗号モジュール（Security Module）
  私有鍵や証明書等を安全に保管し，鍵ペア生成や署名等の暗号操作を行なうハードウェアまたはソフトウェアのモジュール．
- エンドエンティティ（End Entity）
  証明書の発行対象者の総称．公開鍵ペアを所有している実体（エンティティ）で，公開鍵証明書を利用するもの（個人・組織・デバイス・アプリケーションなど）．なお，認証局はエンドエンティティには含まれない．
- オブジェクト識別子（Object Identifier）
  オブジェクトの識別を行なうためオブジェクトに関連付けられた一意な値．
- 活性化（Activate）
  鍵を署名などの運用に使用することができる状態にすること．逆に，使用できない状態にすることを非活性化という．
- 鍵長（Key Length）
  鍵データのサイズ．

・ 鍵ペア(Key Pair)
私有鍵とそれに対応する公開鍵の対.
・ 加入者(Subscriber)
認証局から電子証明書を発行され，電子証明書内に記載された公開鍵に対応する私有鍵を用いて東京工業大学の教育・研究・事務処理システムへのアクセス及び電子文書への署名を行なう者.
・ 加入者証明書
認証局から加入者に対して発行された公開鍵証明書のこと.
・ キーエスクロー
第三者機関に鍵を預託すること.
・ 危殆化(Compromise)
私有鍵等の秘密情報が盗難・紛失. 漏洩等によってその秘密性を失うこと.
・ 公開鍵(Public Key)
私有鍵と対になる鍵で，署名の検証に用いられる.
・ 公開鍵証明書(Public Key Certificate)
加入者の名義と公開鍵を結合して公開鍵の真正性を証明する証明書.
・ 失効(Revocation)
有効期限前に，盗難・紛失などの理由により電子証明書を無効にすること. 基本的には，本人からの申告によるが，緊急時にはCAの判断で失効されることもある.
・ 証明書失効リスト(Certificate Revocation List: CRL, Authority Revocation List: ARL)
失効した電子証明書のリスト. エンドエンティティの証明書の失効リストをCRLといい，CAの証明書の失効リストをARLという.
・ 証明書ポリシー(Certificate Policy: CP)
共通のセキュリティ要件を満たし，特定のコミュニティ及び／またはアプリケーションのクラスへの適用性を指定する名前付けされた規定の集合.
・ 申請者
認証局に電子証明書の発行を申請する主体のこと.
・ 利用者(Relying Party)
文書の署名を公開鍵証明書の公開鍵で検証する者.
・ 電子署名(Electronic Signature)
電子文書の正当性を保証するために付けられる署名情報.
・ 登録局(Registration Authority: RA)
認証局の機能の一部であり，電子証明書発行の申請者の本人を審査・確認し登録業務を行なう機関. 加入者の識別と本人性確認の責任を負うが，証明書の発行は行なわない.
・ 認証局(Certificate Authority: CA)
電子証明書を発行する機関. 認証局は，公開鍵が間違いなく本人のものであると証明可能にする第三者機関で，公正，中立な立場にあり信頼できなければならない.

・ 認証実施規程(Certificate Practice Statement: CPS)
証明書ポリシーに基づいた認証局運用についての規定集であり，認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる.
・ 発行局(Issuer Authority: IA)
認証局の機能の一部であり，電子証明書の作成・発行を主として行なう機関.
・ ハッシュ関数(Hash Function)
任意の長さのデータから固定長のランダムな値(ハッシュ値)を生成する関数.
・ 私有鍵(Private Key)
公開鍵と対になる鍵. 公開せず，他人に漏れないように鍵の所有者だけが管理する.
・ ハードウェアセキュリティモジュール
物理的な安全性が保証されたハードウェアモジュール.
・ プロファイル(Profile)
電子証明書や証明書失効リストに記載する事項及び拡張領域の利用方法を定めたもの.
・ リポジトリ(Repository)
電子証明書及び証明書失効リストを格納し公開するデータベース.
・ ルートCA(Root CA)
階層型の認証構造において，階層の最上位に位置する認証局のこと. 下位に属する認証局の公開鍵証明書の発行・失効を管理する.

(A～Z)
・ ARL(Authority Revocation List)
認証局の証明書の失効リスト，証明書失効リストを参照のこと.
・ CA(Certificate Authority)
認証局を参照のこと.
・ CA証明書
認証局に対して発行された電子証明書.
・ CP(Certificate Policy)
証明書ポリシーを参照のこと.
・ CPS(Certificate Practice Statement)
認証実施規程を参照のこと.
・ CRL(Certificate Revocation List)
エンドエンティティの証明書の失効リスト. 証明書失効リストを参照のこと.
・ DN(Distinguished Name)
X.500規格において定められた識別名. X.500規格で識別子を決定することによって，加入者一意性を保障する.
・ FIPS 140-2(Federal Information Processing Standard)

FIPSとは米国連邦情報処理標準で，FIPS 140-2は暗号モジュールが満たすべきセキュリティ要件を規定したもの．各セキュリティ要件に対して4段階のセキュリティレベル（最低レベル1～最高レベル4)を定めている．

- HSM(Hardware Security Module)
  ハードウェアセキュリティモジュールを参照のこと．
- IA（Issuer Authority）
  発行局を参照のこと．
- OID（Object ID）
  オブジェクト識別子を参照のこと．
- PKI(Public Key Infrastructure)
  公開鍵基盤．公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し，この証明書を用いて署名／署名検証，暗号／復号，認証を可能にする仕組み．
- RA（Registration Authority）
  登録局を参照のこと．
- RSA
  Rivest，Shamir，Adlemanの3名によって開発された公開鍵暗号方式の一つ．
- SHA1（Secure Hash Algorithm 1）
  任意の長さのデータから160bitのハッシュ値を作成するハッシュ関数．
- X.500
  ITU-T/ISOが定めたディレクトリサービスに関する国際基準．
- X.509
  ITU-T/ISOが定めた電子証明書及び証明書失効リストに関する国際標準．X.509v3では電子証明書に拡張領域を設けて，電子証明書の発行者が独自の情報を追加することができる．

2　公開とリポジトリの責任

2．1　リポジトリ

本CAは，リポジトリを年間を通じて毎日24時間利用できるように維持管理を行なう．ただし，利用可能な時間内においてもシステム保守等により利用できない場合がある．

2．2　証明書情報の公開

本CAは，証明書失効リスト（以下「CRL」という）をリポジトリ上に公開し，加入者および利用者がオンラインによって閲覧可能な環境を提供する．

2．3　公開の時期または頻度

本CAは，CRLを発行の都度リポジトリ上に公開する．

2．4　リポジトリへのアクセス管理

本CAは，リポジトリでの公開情報に関して，特段のアクセスコントロールは行なわない．加入者及び利用者は，本CAのCRLを，リポジトリを通じて入手することが可能である．また，リポジトリへのアクセス手段として，一般的なWebインターフェースで可能とする．

3　識別及び認証

3．1　名前決定

3．1．1　名前の種類

本CAが発行する証明書に記載される発行者及び加入者の名前は，X.500シリーズの識別名規定に従って設定する．

3．1．2　名前が意味を持つことの必要性

本CAが発行する加入者の証明書に記載される名前には，東京工業大学において加入者個人を一意に識別可能なID（東京工業大学共通ID）を用いる．

3．1．3　加入者の匿名性または仮名性

規定しない．

3．1．4　種々の名前形式を解釈するための規則

様々な名前の形式を解釈する規則は，X.500シリーズの識別名規定に従う．

3．1．5　名前の一意性

証明書に記載される名前は，本CAが発行する証明書内において加入者ごとに一意とする．

3．1．6　認識・認証及び商標の役割

規定しない．

3．2　初回の本人性確認

3．2．1　私有鍵の所持を証明する方法

私有鍵は本CAで作成し，本CP/CPS「4.3.1 証明書発行時の処理手続き」に定める手続きにより，加入者に配布することによって行なう．

3．2．2　組織の認証

規定しない．

3.2.3　個人の認証

本CAに証明書を申請する個人は「国立大学法人東京工業大学共通認証・認可システムにおける東工大ICカード等の発行・利用に関する取扱い」に従って，申請者自身の実在性・本人性・申請意思を本CAに立証しなくてはならない．

3.2.4　検証されない加入者の情報

認めない．

3.2.5　権限の正当性確認

規定しない．

3.2.6　相互運用の基準

規定しない．

3.3　鍵更新申請時の本人性確認及び認証

3.3.1 通常の鍵更新時における本人性確認と認証

鍵更新時における加入者の本人性確認及び認証は，本CP/CPS「3.2 初回の本人性確認」と同様とする．

3.3.2　証明書失効後の鍵更新における本人性確認と認証

証明書失効後の鍵更新時における加入者の本人性確認及び認証は，本CP/CPS「3.2 初回の本人性確認」と同様とする．

3.4　失効申請時の本人性確認と認証

証明書の失効を申請する場合，加入者本人が「国立大学法人東京工業大学共通認証・認可システムにおける東工大ICカード等の発行・利用に関する取扱い」に従って，本CAに対して失効の申請書を提出する．本CAは，失効の申請書に記載の情報により，申請者本人の名前・失効理由等を確認する．

4　証明書のライフサイクルに対する運用上の要件

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

証明書の発行申請を行なうことができる者は，加入者（本学の構成員及び本学が認めるもの）のみとする．また，加入者は証明書の発行申請を行なう前に，本CP/CPSを承諾するものとする．

4．1．2　申請手続及び責任

証明書の利用を希望する者は，本CAに対して正確な情報を提出しなければならない． また，証明書の利用を希望する者は，以下のいずれかの手続きによって証明書の利用申請を行なう．

1．本人が利用申請書を持参する場合
　本人が登録局に本CP/CPS「3.2.3 個人の認証」及び「国立大学法人東京工業大学共通認証・認可ICカード等の発行・利用取扱い」の定める書類を持参することにより利用申請を行なう．
2．本人が利用申請書を郵送する場合
　本人が登録局に本CP/CPS「3.2.3 個人の認証」及び「国立大学法人東京工業大学共通認証・認可ICカード等の発行・利用取扱い」の定める書類を郵送する（学内便を含む）ことにより利用申請を行なう．

4．2　証明書申請手続き

4．2．1　本人性確認と認証の実施

本人性及び資格の確認については，原則申請者の持参あるいは郵送（学内便を含む）による申請とし，申請者本人から提出された各種の書類に関して，人事情報・教務情報もしくはその他の東京工業大学構成員名簿と照合し記載事項が一致していることの確認や印影が一致していることの確認を行なう．

4．2．2　証明書申請の承認または却下

本CAは，審査の結果，承認を行なった申請について証明書の発行登録を行なう．不備がある申請については申請を却下し，申請を行なった者に対し申請の再提出を依頼する．

4．2．3　証明書申請の処理時間

本CAは，承認を行なった申請に対して適時証明書の発行登録を行なう．

4．3　証明書の発行

4．3．1　証明書発行時の処理手続

本CAは「国立大学法人東京工業大学共通認証・認可システムにおける東工大ICカード等の発行・利用に関する取扱い」に従い，発行申請を受け付けた後に，証明書を発行し当該加入者のICカードに格納する．

4．3．2　加入者への証明書発行通知

本CAは，証明書を発行したことを加入者に電話・電子メールなどにより通知する．

4．4 証明書の受理確認

4．4．1　証明書の受領確認手続

本CAは「国立大学法人東京工業大学共通認証・認可システムにおける東工大ICカード等の発行・利用

に関する取扱い」に従い，証明書を格納したICカードを申請者に手渡しする際に，受領した旨を確認しなければならない．なお，本CAは，証明書を交付してから一定の期間内に受領が確認できない場合，証明書を失効させる．

4．4．2　認証局による証明書の公開

本CAは，加入者の証明書の公開は行なわない．

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 CA は，第三者に対する証明書の発行通知は行なわない．

4．5　鍵ペア及び証明書の用途

4．5．1　加入者の私有鍵及び証明書の用途

加入者の私有鍵及び証明書は，東京工業大学の教育・研究・事務処理システムへのアクセス及び電子文書への署名に用いるものとする．また，私有鍵及び証明書をその他の用途に使用する場合は，本CAはその責を負わない．加入者は，本CAが発行する秘密鍵および証明書を利用するにあたって，以下の義務を負うものとする．

- 秘密鍵を紛失から防止し，第三者に対する開示または危殆化を防止すること．
- 証明書に格納されたデータや情報を修正し，変更しまたは改変しないこと．
- 秘密鍵の危殆化またはそのおそれが生じた場合，直ちに本CAに失効の申込を行なうこと．
- 証明書に記載されているデータまたは情報に変更がある場合，本CAに対し，直ちに変更に関する申請を行なうこと．
- 証明書に対応する秘密鍵を利用する前に，証明書の記載内容に誤りがないということを確認すること．
- 証明書を利用する場合における電子署名方式は，ハッシュアルゴリズムとしてSHA-1を用いたRSA方式であって，鍵長は1024ビットとすること．

4．5．2　利用者の公開鍵及び証明書の用途

利用者は，証明書を信頼し利用するにあたって，次の義務を負うものとする．

- 利用者の責任において，証明書を信頼することを決定する前に，加入者を適切に評価し，合理的な判断を行なうこと．
- 証明書の利用目的が，自己の利用目的に合致していることを承諾していること．
- CA公開鍵を用いて証明書に行なわれた電子署名を検証することにより，当該証明書の発行者を確認すること．
- 東京工業大学のWEBサーバで公開されるフィンガープリントを確認し，本CA証明書であることを確認すること．
- 証明書の有効期限が満了していないことを確認すること．

- 証明書が失効または一時停止されていないことをCRLによって確認すること.
- 本CP/CPSに定める諸規則を遵守すること.

4.6 証明書の更新

4.6.1 証明書の更新事由

規程しない.

4.6.2 証明書の更新を申請することができる者

規定しない.

4.6.3 証明書の更新申請の処理

規定しない.

4.6.4 加入者に対する新しい証明書発行通知

規定しない.

4.6.5 更新された証明書の受領確認の行為

規定しない.

4.6.6 認証局による更新された証明書の公開

規定しない.

4.6.7 他のエンティティに対する認証局の証明書発行通知通知

規定しない.

4.7 鍵更新を伴う証明書の更新

4.7.1 更新事由

証明書の更新は, 証明書の有効期限において行なう.

4.7.2 新しい証明書の申請を行なうことができる者

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 更新申請の処理

本CP/CPS「4.3.1 証明書発行時の処理手続」と同様とする.

4.7.4 加入者に対する新しい証明書の通知

本CP/CPS「4.3.2 加入者への証明書発行通知」と同様とする.

4.7.5 鍵更新された証明書の受領確認手続き

本CP/CPS「4.4.1 証明書の受領確認手続」と同様とする.

4.7.6 認証局による鍵更新済みの証明書の公開

本CAは, 加入者の証明書の公開は行なわない.

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CAは, 第三者に対する証明書の発行通知は行なわない.

4.8 証明書の変更

4.8.1 証明書の変更事由

証明書の変更は, 証明書の記載内容に変更が発生した場合にのみ行なう.

4.8.2 証明書の変更を申請することができる者

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.

4.8.3 変更申請の処理

本CP/CPS「4.3.1 証明書発行時の処理手続」と同様とする.

4.8.4 加入者に対する新しい証明書発行通知

本CP/CPS「4.3.2 加入者への証明書発行通知」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 証明書の受領確認手続」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CAは, 利用者証明書の公開は行なわない.

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CAは, 第三者に対する証明書の発行通知は行なわない.

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

加入者は, 次の事由が発生した場合, 本CAに対し速やかに証明書の失効申請を行なわなければなら

ない.

- 証明書記載情報に変更があった場合
- 私有鍵の盗難・紛失・漏洩・不正利用等により私有鍵が危殆化したまたは危殆化のおそれがある場合
- 証明書の内容，利用目的が正しくない場合
- 証明書の利用を中止する場合（卒業・修了・退学・退職・転出等を含む）

また本CAは，次の事由が発生した場合に，本CAの判断により加入者の証明書を失効させる.

- 加入者が本CP/CPS，関連する契約または法律に基づく義務を履行していない場合
- 加入者が東京工業大学の学則あるいは就業規則に違反し東京工業大学の籍を失った場合
- 東京工業大学が本CAを終了する場合
- 本CAの私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合
- 本CAが失効を必要とすると判断するその他の状況が認められた場合

4．9．2　証明書失効を申請することができる者

証明書の失効申請を行なうことができる者は，当該加入者とする．また，本CP/CPS「4.9.1 証明書失効事由」に該当すると本CAが判断した場合，本CAが当該加入者に代わって失効申請者となることができるものとする.

4．9．3　失効申請手続

失効時の処理手順は，次の通りとする.

- 加入者は，本CP/CPS「3.4 失効申請時の本人性確認と認証」及び「国立大学法人東京工業大学共通認証・認可システムにおける東工大ICカード等の発行・利用に関する取扱い」に従って，本CAに必要書類を提出することとする.
- 本CAは，所定の手続によって受け付けた情報が有効な失効の申請であることを確認し，証明書の失効処理を行なう.

4．9．4　失効申請の猶予期間

失効の申請は，失効すべき事象が発生してから速やかに行な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CAは，有効な失効の申請を受け付けてから速やかにに証明書の失効処理を行ない，CRLへ当該証明書情報を反映させる.

4．9．6　失効調査の要求

本CAが発行する証明書には，CRLの格納先であるURLが記載され，CRLへのアクセスは，一般的なWebインターフェースで可能とする．なお，CRLには，有効期限の切れた証明書情報は含まない.

4．9．7　証明書失効リストの発行頻度

CRLは，失効処理の有無に関わらず，24時間ごとに更新を行なう．証明書の失効処理が行なわれた場合には，その時点でCRLの更新を行なう．

4．9．8　証明書失効リストの発行最大遅延時間

本CAは，発行したCRLを即時にリポジトリに反映させる．

4．9．9　オンラインでの失効/ステイタス確認の適用性

規定しない．

4．9．10　オンラインでの失効/ステイタス確認を行なうための要件

規定しない．

4．9．11　利用可能な失効情報の他の形式

本CAは，CRL以外による失効情報の公開は行なわない．

4．9．12　鍵の危殆化に対する特別要件

規程しない．

4．9．13　証明書の一時停止事由

一時停止は行なわない．

4．9．14　証明書の一時停止を申請することができる者

一時停止は行なわない．

4．9．15　証明書の一時停止申請手続

一時停止は行なわない．

4．9．16　一時停止を継続することができる期間

一時停止は行なわない．

4．10　証明書のステイタス確認サービス

4．10．1　運用上の特徴

規定しない．

4. 10. 2　サービスの利用可能性

規定しない.

4. 10. 3　オプショナルな仕様

規定しない.

4. 11　加入(登録)の終了

加入者の卒業・退学・退職・転出など本CP/CPS「4.9.1 証明書失効事由」で規定する理由により証明書の利用を終了する場合，本CP/CPS「4.9.3 失効申請手続」に定める通り失効申請を行なわなければならない. 本CAは，有効な申請を受け付けた後に速やかに証明書の失効を行なう. 加入者による失効申請が行なわれない場合，本CAは速やかに当該加入者の証明書を失効させなければならない.

4. 12　キーエスクローと鍵回復

本CAは，加入者の秘密鍵のエスクローは行なわない.

4. 12. 1　キーエスクローと鍵回復ポリシー及び実施

本CAは，加入者の秘密鍵のエスクローは行なわない.

4. 12. 2　セッションキーのカプセル化と鍵回復のポリシー及び実施

本CAは，加入者の秘密鍵のエスクローは行なわない.

5　設備上・運営上・運用上の管理

5. 1　物理的管理

5. 1. 1　立地場所及び構造

本CAは，水害・地震・火災・その他の災害の被害を容易に受けない場所に設置されており，かつ建物の構造上もこれら災害防止のための対策を講じている.

5. 1. 2　物理的アクセス

本CAは，物理的なアクセス制御及び電子的なアクセス制御を組み合わせた適切なセキュリティコントロールを実装し，本CAシステムへのアクセスを監視する. また，RA操作端末は施錠可能な区域に設置されている.

5. 1. 3　電源及び空調

本CAは，瞬断及び長時間の停電時においても本CAの運用を可能とするために，UPS・無停電電源装置・自家発電装置等による電源対策を施している. また，本CAは，空気調和機により最適な温度，湿

度を一定に保つことが可能な環境下に設置する.

5.1.4　水害対策

本CAは，水害対策として本CAを建物の2階以上に設置する. また，防水対策として本CAを設置する室には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

本CAを設置する室は，防火壁によって区画された防火区画とし，火災報知機及び消火設備を設置する.

5.1.6　媒体保管

本CAは，アーカイブデータ・バックアップデータを含む認証業務を行なう上で必要な情報を，適切な入退管理が行なわれた室内の保管庫に保存し，毀損・滅失防止のための措置を施す.

5.1.7　廃棄処理

本CAは，機密情報を含む書類・電子媒体の廃棄を，情報の初期化・裁断等により行なう.

5.1.8　オフサイトバックアップ

本CAの運用のために必要なデータ・機器等は，遠隔地に保管するかまたは調達できる手段を講ずる.

5.2　手続的管理

5.2.1　信頼すべき役割

本CAの運用を行なうために，責任者・システム操作者・受付審査者. 監査実施者の権限は分離する.

5.2.2　職務ごとに必要とされる人数

本CAは，サービス提供に支障を来たさないよう，責任者を除く本CP/CPS「5.2.1 信頼すべき役割」に記載する役割に関し，複数名の要員を配置する.

5.2.3　個々の役割に対する本人性確認と認証

本CAへのアクセスに関し，物理的または論理的な方法によってアクセス権限者の識別と認証，及び認可された権限の操作であることを確認する.

5.2.4　職務分割が必要になる役割

本CP/CPS「5.2.1 信頼すべき役割」に記載する役割は，原則として異なる要員がその役割を担う.

5．3　人事的管理

信頼される役割を担う者は，認証局の業務に関して，操作や管理の責務を負う．認証局の運営においては，これら役割の信頼性，適合性及び合理的な職務執行能力を保証する人事管理がなされ，そのセキュリティを確立するものとする．

5．3．1 資格・経験及び身分証明の要件

本CP/CPS「5.2.1 信頼すべき役割」に記載する役割を担う者は，本CAの採用基準に基づき採用された従業員とする．本CAを直接操作する担当者には，専門のトレーニングを受け，PKIの概要とシステムの操作方法等を理解しているものを配置する．

5．3．2　背景調査

本CP/CPS「5.2.1 信頼すべき役割」に記載する役割を担う者の信頼性と適性を任命時及び定期的に評価する．

5．3．3　教育要件

要員が役割に就く前に本CAの運用に必要な教育を実施し，必要に応じ，役割に応じた教育・訓練を実施する．また， 業務手順に変更がある場合はその変更に関わる教育・訓練を実施する．

5．3．4　再教育の頻度及び要件

本CP/CPS「5.2.1 信頼すべき役割」に記載する役割を担う者に対して，必要に応じ再トレーニングを行なう．

5．3．5　仕事のローテーションの頻度及び順序

不正防止の観点から，必要に応じて要員のジョブローテーションを行なう．

5．3．6　認められていない行動に対する制裁

規定しない．

5．3．7　独立した契約者の要件

本CAの運用のすべてあるいは一部を外部組織に委託する場合，業務委託先との契約によって，業務委託先のもとで運用業務が適切に行なわれていることを確認する．

5．3．8　要員へ提供される資料

東京工業大学は，関連する業務上必要な文書のみの閲覧を要員に対して許可する．

5．4　監査ログの手続

5．4．1　記録されるイベントの種類

本CAは，次の内容を監査ログとして記録する．

【認証局システムに係るログ】

- 認証局の私有鍵の操作
- 認証局システムの起動・停止
- データベースの操作
- 権限設定の履歴
- 証明書の発行・失効の処理履歴
- CRLの発行の処理履歴

【入退室・ネットワークに係るログ】

- 本CAを設置する室への入退室に関する記録
- 本CAへの不正アクセスに関する記録

ただし，監査ログは，以下の項目を含む．

- 日付
- 時刻
- イベントを発生させた主体

5．4．2　監査ログを処理する頻度

本CAは，監査ログを定期的に確認する．

5．4．3　監査ログを保存する期間

本CAは，認証局システムに係る監査ログを，アーカイブとして最低10年保存する．入退室・ネットワークに係るログについては最低1年間保存する．

5．4．4　監査ログの保護

本CAは，認可された者のみが監査ログにアクセスすることができるよう適切なアクセスコントロールを採用し，許可されていない者が閲覧できないようにする．

5．4．5　監査ログのバックアップ手続

監査ログはオフラインの記録媒体にバックアップとして取得し，それらの媒体を物理的に安全な場所に保管する．

5．4．6　監査ログの収集システム

監査ログの収集システムは，本CAの機能に含まれる．

5．4．7　イベントを起こした者への通知

本CAは，監査ログの収集を，事象を発生させた人，システムまたはアプリケーションに対して通知することなく行なう．

5．4．8　脆弱性評価

本CAは，監査ログの検査結果をもとに，運用面及びシステム動作面におけるセキュリティ上のぜい弱性を評価するとともに，必要に応じて最新の実装可能なセキュリティ・テクノロジの導入等，セキュリティ対策の見直しを行なう．

5．5　記録の保管

5．5．1　アーカイブの種類

本CAは，本CP/CPS「5.4.1 記録されるイベントの種類」の認証局システムに係るログに加えて，次の情報をアーカイブとして，RAにおいて保存期間を定めて保存するものとする．

- 発行した証明書及びCRL
- 証明書利用申請・失効申請のための書類等
- 本CP/CPS
- 本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
- 監査の実施結果に関する記録及び監査報告書

5．5．2　アーカイブ保存期間

アーカイブする情報は，記録が作成されてから最低10年間は保存する．

5．5．3　アーカイブの保護

アーカイブ情報の収められた媒体は物理的セキュリティによって保護され，許可されたものしかアクセスできないよう制限された施設に保管する．

5．5．4　アーカイブのバックアップ手続

証明書発行・取消またはCRLの発行等，本CAに関する重要なデータに変更がある場合は，適時，アーカイブのバックアップを取得する．

5．5．5　記録にタイムスタンプを付与する要件

本CAは，NTP(Network Time Protocol)を使用して本CAの時刻同期を行ない，本CA内で記録される重要な情報に対しタイムスタンプを付与する．

5．5．6　アーカイブ収集システム

アーカイブの収集システムは，本CAの機能に含まれる.

5.5.7　アーカイブの検証手続

アーカイブは，物理的に安全なな保管庫からアクセス権限者が入手し，定期的に媒体の保管状況の確認を行なう. また必要に応じ，アーカイブの完全性及び機密性の維持を目的として，新しい媒体への複製を行なう.

5.6　鍵の切り替え

本CAの私有鍵は，私有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私有鍵の生成及び証明書の発行を行なう. 新しい私有鍵が生成された後は，新しい私有鍵を使って証明書及びCRLの発行を行なう. また，古い私有鍵はでは証明書の発行は行なわずCRLの発行のみを行なう.

5.7　危殆化及び災害からの復旧

5.7.1　事故及び危殆化時の手続

本CAは，事故及び危殆化が発生した場合に速やかに本CA及び関連する業務を復旧できるよう，以下を含む事故及び危殆化に対する対応手続を策定する.

- CA私有鍵の危殆化
- ハードウェア・ソフトウェア・データ等の破損・故障
- 火災・地震等の災害

5.7.2　ハードウェア，ソフトウェアまたはデータが破損した場合の手続

本CAのハードウェア・ソフトウェアまたはデータが破損した場合，バックアップ用として保管しているハードウェア・ソフトウェアまたはデータを使用して，速やかに本CAの復旧作業を行なう.

5.7.3　エンティティの私有鍵が危殆化した場合の手続

本CAの私有鍵が危殆化したまたは危殆化のおそれがあると判断した場合，及び，災害等により本CAの運用が中断・停止につながるような状況が発生した場合には，予め定められた計画・手順に従い，安全に運用を再開させる.

5.7.4　災害後の事業継続性

本CAは，不測の事態が発生した場合に速やかに復旧作業を実施できるよう，予め本CAの代替機の確保，復旧に備えたバックアップデータの確保，復旧手続の策定等，可能な限り速やかに本CAを復旧するための対策を行なう.

5.8　認証局または登録局の終了

本CAは，本CAを終了する場合，終了する少なくとも90日前までに加入者に対して終了の事実を通知または公表し，所定の終了手続を行なう．ただし，緊急またはやむをえない場合，この期間を短縮できるものとする．

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

本CAは，FIPS140-2レベル3準拠のハードウェアセキュリティモジュール(Hardware Security Module, 以下「HSM」という)上でCAの鍵ペアを生成する．CA鍵ペアの生成作業は，複数名の権限者による操作によって行なう．また，加入者の鍵ペアはIA内部で生成しICカードに格納する．

6．1．2　加入者に対する私有鍵の交付

ICカードが加入者本人に手渡しされる．

6．1．3　認証局への公開鍵の送付

IA内部で鍵ペアの生成及び証明書の発行を行なうので認証局への公開j鍵の送付は行なわない．

6．1．4　利用者へのCA公開鍵の配付

CA公開鍵は，利用者によるダウンロードを可能とするために，本CP/CPSを公開する機関のサイトで公開するものとする．このサイトの通信はSSLにより暗号化し保護される．

6．1．5　鍵のサイズ

加入者の鍵ペアの電子署名方式は，ハッシュアルゴリズムとしてSHA-1を用いたRSA方式であり，鍵長は1024ビットとする．　また，CAの鍵ペアの電子署名方式は，ハッシュアルゴリズムとしてSHA-1を用いたRSA方式であり鍵長は2048ビットとする．

6．1．6　公開鍵のパラメータ生成及び品質検査

本CAの公開鍵のパラメータの生成，及びパラメータの強度の検証は，鍵ペア生成に使用される暗号装置に実装された機能を用いて行なわれる．

6．1．7　鍵の使用目的

本CAのCA証明書のKeyUsageには，keyCertSign,, cRLSignのビットを設定する．また，加入者証明書のkeyUsageには，DigitalSignature, KeyEnciphermentのビットを設定する．

6．2　私有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CAの私有鍵の生成・保管・署名操作は，FIPS140-2レベル3準拠のHSMを用いて行なう．また，加入者の私有鍵の生成・保管・署名操作はICカードを用いて行なう．

6.2.2　複数人による私有鍵の管理

本CAの私有鍵の活性化・非活性化・バックアップ等の操作は，安全な環境において複数人の権限者によって行なう．

6.2.3　私有鍵のエスクロウ

本CAでは，CAの私有鍵のエスクローは行なわない．

6.2.4　私有鍵のバックアップ

本CAの私有鍵のバックアップは，CAサーバの設置された室において複数名の権限者によって行なわれ，暗号化された状態でセキュアな室に保管される．加入者の私有鍵のバックアップは行なわない．

6.2.5　私有鍵のアーカイブ

本CA上では，CA及び加入者の私有鍵のアーカイブは行なわない．

6.2.6　私有鍵の暗号モジュールへのまたは暗号モジュールからの転送

本CAの私有鍵のHSMへの転送またはHSMからの転送は，CAサーバの設置された室において私有鍵を暗号化した状態で行なう．一方，加入者の私有鍵の暗号化モジュールへの転送または暗号化モジュールからの転送は行なうことはできない．

6.2.7　暗号モジュールへの私有鍵の格納

本CAの私有鍵は，暗号化された状態でHSM内に格納する．また，加入者の私有鍵は保護された状態でICカードに格納されている．

6.2.8　私有鍵の活性化方法

本CAの私有鍵の活性化は，CAサーバの設置された室において複数名の権限者によって行なう．また，加入者の私有鍵の活性化はPINの入力によって行なう．

6.2.9　私有鍵の非活性化方法

本CAの私有鍵の非活性化は，CAサーバの設置された室において複数名の権限者によって行なう．

6.2.10　私有鍵の廃棄方法

本CAの私有鍵の廃棄は，複数名の権限者によって完全に初期化または物理的に破壊することによっ

て行なう. バックアップについても同様の手続によって行なう.

6. 2. 11　暗号モジュールの評価

本CAで使用するHSMの品質基準については, 本CP/CPS「6.2.1 暗号モジュールの標準及び管理」の通りである.

6. 3　鍵ペア管理に関するその他の面

6. 3. 1　公開鍵のアーカイブ

本CA上における公開鍵のアーカイブは, 本CP/CPS「5.5.1 アーカイブの種類」に含まれる.

6. 3. 2　私有鍵と公開鍵証明書の有効期間

本CAの私有鍵の有効期間は10年以内とする.

6. 4　活性化用データ

6. 4. 1　活性化データの生成及び設定

本CAの私有鍵を操作するために必要な活性化データは, 複数名の権限者によって生成され, 電子媒体に格納する.

6. 4. 2　活性化データの保護

本CAの私有鍵の活性化に必要なデータが格納された電子媒体は, セキュアな室において保管管理を行なう.

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　コンピュータセキュリティに関する技術的要件

本CAに導入するハードウェア・ソフトウェアに対して, その品質・安定性・安定性等について十分に検討を行ない導入を決定する.

6. 5. 2　コンピュータセキュリティ評価

本CAにおいて使用する全てのソフトウェア・ハードウェアに対して, 事前にシステムテストを行ない本CAの信頼性確保に努める. また, 本CAのセキュリティ上の脆弱性についての情報収集・評価を継続的に行ない, 脆弱性が発見された場合には速やかに必要な対処を行なう.

6. 6　ライフサイクルセキュリティ管理

6.6.1　システム開発管理

本CAの構築およびメンテナンスは，安全な環境下で行なう．本CAの変更を行なう場合は，十分に安全性の評価・確認を行なう．また，本CAに対して適切なサイクルで最新のセキュリティ技術を導入するためにセキュリティチェックを行なうことにより，セキュリティを確保する．

6.6.2　セキュリティ運用管理

情報資産管理・要員管理・権限管理等の運用管理の実施，不正侵入対策・ウイルス対策等のセキュリティ対策ソフトウェアの適時更新等を行なうことにより，セキュリティを確保する．

6.6.3　ライフサイクルのセキュリティ管理

本CAのシステム開発・業務運用が適切に行なわれていることを適時評価し，必要に応じ改善を行なう．

6.7　ネットワークのセキュリティ管理

本CAに対するネットワークからのアクセスは，ファイアウォール・IDS等によって保護する．

6.8　タイムスタンプ

タイムスタンプに関する要件は，本CP/CPS「5.5.5 記録にタイムスタンプを付与する要件」と同様とする．

7　証明書・証明書失効リスト及び OCSP のプロファイル

7.1　証明書プロファイル

本CAが発行する証明書は，X509 Version 3 フォーマット証明書形式により作成される．証明書の基本領域のプロファイルを表7.1.1に示す．

表7.1.1 証明書のプロファイル(基本領域)

フィールド(基本領域)		内容	critical
Version (X.509 証明書バージョン)		Version 3 (2)	−
Serial Number MS-Mincho (シリアル番号)		10 桁整数 (発行時に自動採番)	−
Signature Algorithm (署名アルゴリズム)		sha1withRSAEncryption (1.2.840.113549.1.1.5)	−
Issuer (発行者)	Country	Issuer の DN	−
	Organization (組織)		
	OrganizationUnit (部門名)		
	Common Name		
Validity (有効期限)	NotBefore (有効性開始日時)	証明書発行日時(発行時に自動付与)	−
	NotAfter (有効性修了日時)	基準日を起点から有効年数の 15 日後の23:59 (有効年数はユーザ種別によって違う)	
Subject (主体者)	Country (国)	JP	−
	Organization (組織)	Tokyo Institute of Technology	
	OrganizationalUnit (部門名)	People	
	Common Name	東工大共通ID(9 桁の数字 + ″ハイフン″ + 1桁の数字もしくは X (例: 000000001-X)	
Subject PublicKey Info (主体者公開鍵情報)		rsaEncryption (1.2.840.113549.1.1.1) 主体者の RSA 公開鍵 (1024bit)	−

7.1.1 バージョン番号

本CAが発行する証明書は, X.509 Version 3 フォーマット証明書形式により作成する.

7．1．2　証明書の拡張

本CAが発行する証明書の拡張領域のプロファイルは以下の表7.1. 2の通りとする.

表7.1.2 証明書のプロファイル(拡張領域)

フィールド(拡張領域)	内容	critical
Key Usage (鍵用途)	DigitalSignature (署名) KeyEncipherment (鍵の暗号化)	y
Authority Key Identifier (発行者鍵識別子)	発行者公開鍵の 160bit SHA-1 ハッシュ値	n
Subject Key Identifier (主体者鍵識別子)	主体者公開鍵の 160bit SHA-1 ハッシュ値	n
SubjectAltName (主体者別名)	rfc822mail : 電子メールアドレス: otherName : Microsoft UPN (例: UPN=user1@name.com, UPN のOIDは 1.3.6.1.4.1.311.20.2.3)	n
CertificatePolicies (証明書ポリシー)	Policy Identitfiler = 1.3.6.1.4.1.8732.1.1.1.2	n
ExtendedKeyUsage (拡張鍵使用法)	1.3.6.1.5.5.7.3.2(TLS クライアント認証)、 1.3.6.1.4.1.311.20.2.2 (Microsoft スマートカードログオン)、1.3.6.1.5.5.7.3.4 (電子メール保護)	n
cRLDistributionPoint (証明書配布点)	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.nap.gsic.titech.ac.jp/crl/fullcrl.crl URL=ldap://ldap.nap.gsic.titech.ac.jp/cn=Tokyo Tech Campus-wide CA, o=Tokyo Institute of Technology, c=jp?CertificateRevocationList (URIエンコード。スペースは%20 など) [2] Entrust CRL DP(cn=CRL1,cn=Tokyo Tech Campus-wide CA,o=Tokyo Instutute of Technology,c=jp) ※CA 鍵が更新されると URL 部分が変更される.	n

7．1．3　アルゴリズムオブジェクト識別子

基本領域のSignatureアルゴリズム及びsubjectPublicKeyInfoアルゴリズムは表7.1.3に示される.

表7.1.3 アルゴリズムOID

アルゴリズム	オブジェクト識別子
sha1WithRSAEncryption	1.2.840.113549.1.1.5
RSAEncryption	1.2.840.113549.1.1.1

7．1．4　名前の形式

Issurer と Subject の名前の形式は表 7.1.1 に示される.

7．1．5　名前制約

用いない.

7．1．6　証明書ポリシーオブジェクト識別子

証明書ポリシーオブジェクト識別子を「1.2.6.1.4.1.87321.1.1.2」とする.

7．1．7　ポリシー制約拡張の使用

使用しない.

7．1．8　ポリシー修飾子の構文及び意味

CPSを参照するURLを含めることができる.

7．1．9　クリティカルな証明書ポリシー拡張に対する解釈の方法

本CPのOIDを格納する.

7．2　CRLプロファイル

7．2．1　バージョン番号

本CAが発行するCRLは，X.509 Version 3 フォーマットCRL形式に従うものとする．基本領域のプロファイルは表7.2.1に示す.

表7.2.1 証明書失効リストのプロファイル(基本領域)

フィールド(基本領域)		内容	critical
Version (X.509CRL バージョン)		Version 2	–
Signature Algorithm (署名アルゴリズム)		SHA-1 with RSAEncryption	–
Issuer (発行者)	Country (国)	JP	–
	Organization(組織)	Tokyo Institute of Technology	
	Organizational Unit (組織単位)	Tokyo Tech Campus-wide CA	
This Update (更新日時)		例) 2005/09/01 00:00:00 GMT	–
Next Update (次回更新予定日時)		例) 2005/09/05 00:00:00 GMT ＊ CRL 記載更新間隔 96 時間、実更新間隔 24 時間	
Revoked Certificates (失効証明書)	Serial Number (証明書シリアル番号)	例) 1234567890	–
	Revocation Date (失効日時)	例) 2005/09/01 12:00:00 GMT	
	Reason Code (失効理由)	例) superseded(破棄)	

7.2.2 証明書失効リスト及び証明書失効リストエントリ拡張

CRL拡張領域のプロファイルは表7.2.2の通りとする.

表7.2.2 証明書失効リストのプロファイル(拡張領域)

フィールド(拡張領域)	内容	critical
CRL Number (CRL 番号)	例) 1 (CRL の発行順序を示す整数値)	n
Authority Key Identifier (発行者鍵識別子)	発行者の公開鍵識別子 (公開鍵の SHA-1 ハッシュ値)	n

7.3　OCSPプロファイル

7.3.1　バージョン番号

規定しない.

7.3.2　OCSP拡張

規定しない.

8　準拠性監査とその他の評価

8.1　監査の頻度

本CAは，本CAの運用が本CP/CPSに準拠して行なわれているかについて，適時，監査を行なう.

8.2　監査者の身元・資格

準拠性監査は，十分な監査経験を有する監査人が行なうものとする.

8.3　監査者と被監査者の関係

本CAは，監査者を本CAの認証業務に携わる要員以外から選定し，被監査者に対しての特別な利害関係を持たないものによって行なわれる.

8.4　監査で扱われる事項

監査対象は，本CAの運用が本CP/CPSに準拠して行なわれているかを中心とする.

8.5　不備の結果としてとられる処置

本CAは，監査報告書で指摘された事項に関し，速やかに必要な是正措置を行なう.

8.6　監査結果の開示

監査結果は，監査人から本CAに対して報告される. 本CAは，法律に基づく開示要求があった場合及びIA外部委託業者との契約に基づき関係組織からの開示要求があった場合以外，監査結果を外部へ開示することはない.

9　他の業務上及び法的事項

9.1　料金

各種の料金については，本CP/CPSでは規定しない.

9.1.1　証明書の発行または更新料

規定しない.

9.1.2　証明書へのアクセス料金
規定しない.

9.1.3　失効またはステータス情報へのアクセス料金
規定しない.

9.1.4　その他のサービスに対する料金
規定しない.

9.1.5　払い戻し指針
規定しない.

9.2　財務的責任
規定しない.

9.2.1　保険の範囲
規定しない.

9.2.2　その他の資産
規定しない.

9.2.3　エンドエンティティに対する保険または保証
規定しない.

9.3　本学に帰属する情報の機密性
9.3.1　機密情報の範囲
本CAのサービスで入手した情報は，証明書・CRL・本CP/CPSとして明示的に公表されたものを除き，機密保持対象として扱われる．本CAは，法の定めによる場合及び利用者による事前の承諾を得た場合を除いてこれらの情報を外部に開示しない．かかる法的手続・司法手続・行政手続あるいは法律で要求されるその他の手続に関連してアドバイスする法律顧問及び財務顧問に対し，本CAは機密保持対象として扱われる情報を開示することができる.

9.3.2　機密情報の範囲外の情報
証明書及びCRLに含まれている情報は機密保持対象外として扱う．その他，次の状況におかれた情

報は機密保持対象外とする.

- 本CAの過失によらず知られた，あるいは知られるようになった情報
- 本CA以外の出所から，機密保持の制限無しに本CAに知られた，あるいは知られるようになった情報
- 本CAによって独自に開発された情報
- 開示に関して利用者によって承認されている情報

9．3．3　機密情報を保護する責任

本CAは，法の定めによる場合及び利用者による事前の承諾を得た場合に機密情報を開示することがある．その際，その情報を知り得た者は，契約あるいは法的な制約によりその情報を第三者に開示することはできない．

9．4　個人情報の保護

9．4．1　プライバシープラン

本CAにおける個人情報の取り扱いについては「国立大学法人東京工業大学個人情報保護規程」並びに「国立大学法人東京工業大学個人情報管理規程」を適用するものとする．

9．4．2　プライバシーとして扱われる情報

認証局は，次の情報を保護すべき個人情報として取り扱う．

- 登録局が本人確認や各種審査の目的で収集した情報の中で，証明書に含まれない情報．例えば，身分証明書，自宅住所，連絡先の詳細など，他の情報と容易に照合することができ，それにより特定の個人を識別することが可能な情報を指す．
- CRLに含まれない加入者の証明書失効または停止の理由に関する情報．
- その他，認証局が業務遂行上知り得た加入者の個人情報．

9．4．3　プライバシーとはみなされない情報

次の情報は，個人情報として扱わない．

- 公開鍵証明書
- CRLに記載された情報

9．4．4　個人情報を保護する責任

本CAは「9.4.2 プライバシーとして扱われる情報」で規定された情報を保護するため，内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う．

9．4．5　個人情報の使用に関する個人への通知及び承諾

本CA，証明書発行業務及びその他の認証業務の利用目的に限り個人情報を利用する．それ以外の

目的で個人情報を利用する場合は，法令で除外されている場合を除き，あらかじめ本人の同意を得るものとする.

9．4．6　司法手続または行政手続に基づく公開

司法機関・行政機関またはその委託を受けたものの決定・命令・勧告等があった場合は，認証局は情報を開示することができる.

9．4．7　他の情報公開の場合

個人情報を提供した本人またはその代理人から当該本人に関する情報の開示を求められた場合「国立大学法人東京工業大学個人情報保護規程」で定める手続きに従って情報を開示する.

9．5　知的財産権

本CAと加入者との間で別段の合意がなされない限り，本CP/CPSは著作権を含み，本CAの権利に属するものとする.

9．6　表明保証

9．6．1　認証局の表明保証

本CAは，認証業務を遂行するにあたり次の義務を負う.

- CA私有鍵のセキュアな生成・管理
- RAからの申請に基づいた証明書の正確な発行・失効管理
- IAのシステム稼動の監視・運用
- CRLの発行・公表
- リポジトリの維持管理

9．6．2　登録局の表明保証

本CAは，RAの業務を遂行するにあたり次の義務を負う.

- 登録端末のセキュアな環境への設置・運用
- 証明書発行・失効申請におけるIAへの正確な情報伝達
- 証明書失効申請におけるIAへの運用時間中の速やかな情報伝達

9．6．3　加入者の表明保証

加入者は，本CP/CPSに定める諸事項を遵守しなければならない．また，加入者は，本CP/CPSに遵守しない場合，すべての責任を有するものとする.

9．6．4　利用者の表明保証

利用者は，本CP/CPSに定める諸事項を遵守しなければならない．また，利用者は，本CP/CPSに遵守

しない場合，すべての責任を有するものとする.

9.6.5　他の関係者の表明保証

規定しない.

9.7　無保証

本CAは，本CP/CPS「9.6.1 認証局の表明保証」に規定する保証に関連して発生するいかなる間接損害，特別損害，付随的損害または派生的損害に対する責任を負わず，また，いかなる逸失利益，データの紛失またはその他の間接的若しくは派生的損害に対する責任を負わない.

9.8　責任の制限

本CP/CPS「9.6.1 認証局の表明保証」の内容に関し，次の場合，本CAは責任を負わない.

- 本CAに起因しない不法行為，不正使用または過失等により発生する一切の損害
- 加入者が自己の義務の履行を怠ったために生じた損害
- 加入者のシステムに起因して発生した一切の損害
- 本CA，加入者のハードウェア，ソフトウェアの瑕疵，不具合あるいはその他の動作自体によって生じた損害
- 加入者が契約に基づく契約料金を支払っていない間に生じた損害
- 本CAの責に帰することのできない事由で証明書及びCRLに公開された情報に起因する損害
- 本CAの責に帰することのできない事由で正常な通信が行なわれていない状態で生じた一切の損害
- 証明書の使用に関して発生する取引上の債務等，一切の損害
- 現時点の予想を超えた，ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- 天変地異，地震，噴火，火災，津波，水災，落雷，戦争，動乱，テロリズムその他の不可抗力に起因する，本CAの業務停止に起因する一切の損害

9.9　補償

本CAが発行する証明書を申請・受領・信頼した時点で，加入者には，本CA及び関連する組織等に対する損害賠償責任及び保護責任が発生するものとします．当該責任の対象となる事象には，損失，損害，訴訟，あらゆる種類の費用負担の原因となるようなミス，怠慢な行為，各種行為，履行遅滞，不履行等の各種責任が含まれる.

9.10　有効期間と終了

9.10.1　有効期間

本CP/CPSは，作成された後，情報セキュリティ委員会により審査・承認されることにより有効になる.

また「9.10.2 終了」で記述する本CP/CPSの終了まで有効であるものとする.

9.10.2 終了

本CP/CPSは「9.10.3 終了の影響と存続条項」で規定する存続条項を除き，情報セキュリティ委員会が無効と宣言した時点または情報セキュリティ専門委員会が機能を果たさなくなった場合，無効になる.

9.10.3 終了の効果と効果継続

加入者と本CAとの間で利用契約等を終了する場合，あるいは本CA自体を終了する場合であっても，本CP/CPS「9.3 本学に帰属する情報の機密性」，「9.4 個人情報の保護」，「9.5 知的財産権」に関する責務は存続するものとする. また，情報セキュリティ委員会において部分的な存続を定めた場合は，当該存続部分は有効なものとする.

9.11 関係者間の個別通知と連絡

本CAは，加入者に対する必要な通知をホームページ上・電子メール・書面等により行なう.

9.12 改訂

9.12.1 改訂手続き

情報セキュリティ委員会が本CP/CPSの改訂を行なう場合は，改訂に先立ち，本CP/CPSに関連する全てのCAに通知を行ない意見を求める. 本CP/CPSが変更された時は，情報セキュリティ委員会によって承認する.

9.12.2 通知方法及び期間

本CP/CPSを変更した場合，速やかに変更した本CP/CPSを公表することにより，加入者に対しての告知する. 加入者は告知日から一週間の間，異議を申し立てることができ，異議申し立てがない場合，変更された本CP/CPSは加入者に同意されたものとみなす.

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CP/CPSの変更があった場合には，本CP/CPSのバージョン番号を更新する. また，次の場合には，OIDを変更する.

- 証明書またはCRLのプロファイルが変更されたとき
- セキュリティ上重要な変更がされたとき
- 本人性の確認方法の厳密さに重要な影響を及ぼす変更がされたとき

9.13 紛争解決手続

証明書の利用に関し，本CAに対して訴訟，仲裁を含む解決手段に訴えようとする場合，本CAに対して事前にその旨を通知するものとする. なお，仲裁及び裁判地は東京都区内における紛争処理機関を

専属的管轄とする.

9.14　準拠法

本CAは加入者の所在地にかかわらず，本CP/CPSの解釈，有効性及び証明書の利用にかかわる紛争については，日本国の法律が適用されるものとする.

9.15　適用法の遵守

本CPの運用にあたっては，日本国内法及び公的通知等がある場合はそれを優先する.

9.16　雑則

9.16.1　完全合意条項

本CP/CPSは，本CP/CPSに定められたサービスに対して当事者間の完全合意を構成し，認証業務について記述された書面または口頭による過去の一切の意思表示・合意・表明事項に取って代わるものである.

9.16.2　権利譲渡条項

関係者は，本CP/CPSに定める権利義務を担保に供することができない．また，次の場合を除き，第三者に譲渡することができない.

- 認証局が登録局に本CP/CPSに定める業務の委託を行なうとき
- 本CP/CPSに則った認証局の移管若しくは譲渡を行なうとき

9.16.3　分離条項

本CP/CPSのひとつまたは複数の条項が司法の判断により，無効であると解釈された場合であっても，その他の条項の有効性には影響を与えない．無効と判断された条項は，法令の範囲内で当事者の合理的な意思を反映した規定に読み替える.

9.16.4　強制執行条項（弁護士費用及び権利放棄）

規定しない.

9.16.5　不可抗力

以下のような通常人の標準的な注意義務を尽くしても，予防・回避できない事象を不可抗力とする．不可抗力によって損害が発生した場合，本CP/CPS「9.7 無保証」の規定により認証局は免責される.

- 火災，雷，噴火，洪水，地震，嵐，台風，天変地異，自然災害，放射能汚染，有害物質による汚染またはその他の自然現象
- 暴動，市民暴動，悪意的損害，破壊行為，内乱，戦争（宣戦布告されているか否かを問わない）または革命

- 裁判所，政府または地方機関による作為または不作為
- ストライキ，労働争議
- 本CAの責によらない事由で，本CP/CPSに基づく義務の遂行上必要とする必須の機器，物品，供給物若しくはサービス（電力，ネットワークその他の設備を含むがそれに限らない）が利用不能となった場合

9.17 その他の条項

本CP/CPSを採用したCAまたはRAが別の組織と合併若しくは別の組織に移管・譲渡する場合，新しい組織は本CP/CPSの方針に同意し責任を持ちつづけるものとする.