TOiNX TA 認証サービス

認証局運用規則

（Ver 1.04）

平成 26 年　4 月

東北インフォメーション・システムズ株式会社

改訂履歴

Version	変更内容	適用日	変更者/作成者	承認者
1.00	初版	2006/02/23	市川正彦	荒川務
1.01	TOiNX 代表者変更に伴う修正	2007/07/06	市川正彦	遠藤友太
1.02	TA 証明書の鍵長に関する記述変更	2008/09/12	五十嵐和成	遠藤友太
1.03	TOiNX 代表者変更に伴う修正	2011/06/17	立川由美子	横田勇一
1.04	営業日変更に伴う修正	2014/04/23	杉山幸博	横田勇一

目 次

1 はじめに

1.1 概要

東北インフォメーション・システムズ株式会社（以下，「TOiNX」という）は，時刻配信サービスを提供している組織の実在性を保証する TOiNX TA 認証サービス（以下，「本サービス」という）を提供する。

本サービスは，TOiNX と本サービスの利用契約を締結した，商業登記された法人の代表者（または代表権を有する者），商業登記された商号を持つ個人事業主，地方自治体などの公共機関の代表者（以下，「申請者」という）が所属する時刻配信サービス事業者に対して電子証明書（以下，「TA 証明書」という）を発行する。

本文書「TOiNX TA 認証サービス認証局運用規則」（以下，「本 CPS」という）は，TOiNX が運営する TOiNX TA 認証局（以下，「本認証局」という）が行う TA 証明書の発行，失効およびその他の認証局業務の運用管理に関する諸手続と認証局，申請者，技術管理担当者および検証者の義務，責任等について規定する。

本 CPS は，IETF（Internet Engineering Task Force）の PKIX（Public Key Infrastructure working group）が提唱する「電子証明書ポリシーと認証実践の枠組み（Certificate Policy and Certification Practices Framework）」（RFC2527）に従い記述されている。

1.2 識別

本認証局に関連するオブジェクト識別子は、次のとおりとする。

表 1-1 TOiNX の OID とオブジェクトの対応表

OID	オブジェクト
1.2.392.200121	Tohoku Information Systems Co.,Inc.
1.2.392.200121.1	TOiNX CA Service
1.2.392.200121.1.5	TOiNX TA CA Service
1.2.392.200121.1.5.1	TOiNX TA CA Service Policy & CPS

1.3 コミュニティと適応可能性

1.3.1 本 CPS の適用範囲

本 CPS は，以下の図 1 に示す本認証局により実施される TA 証明書の発行業務および失効業務に適用される。本認証局より発行される電子証明書には，全て本 CPS が適用される。

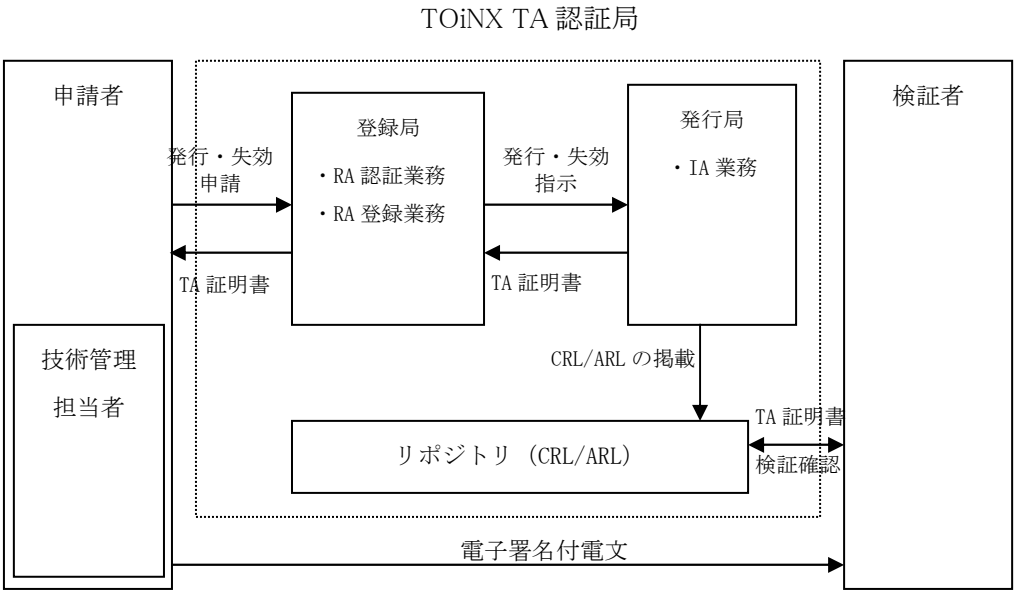

図 1 認証局の構成

1.3.2 認証局

本認証局は，登録局（以下，「RA」という）と発行局(以下，「IA」という)から構成され，TOiNX により運営される。TOiNX は，本認証業務の運営管理主体であり，その業務を統制，管理する本 CPS を策定しこれを公開する。

1.3.3 発行局

本認証局において発行業務は IA によって行われる。IA は，本 CPS に従い TA 証明書の発行処理，失効処理および TA 証明書の失効リスト（以下，「CRL」という）の発行処理を行う。TA 証明書の発行指示および失効指示は RA から安全な通信方法を介して行われる。

1.3.4 登録局

本認証局において登録業務は RA によって行われる。RA は，RA 認証業務と RA 登録業務からなる。RA 認証業務は，申請者から提出される電子証明書発行申請書（以下，「発行申請書」という）の受付や申請者の真偽確認などの書類審査を行い，RA 登録業務に TA 証明書の発行および失効に関する依頼を行う。RA 登録業務は，RA 認証業務からの TA 証明書の発行依頼に従い IA への TA 証明書の発行指示および失効指示を行う。TA 証明書の発行指示および失効指示は RA か

ら安全な通信方法を介して行われる。

1.3.5 申請者

申請者とは，TOiNX と本サービスの利用契約を締結した商業登記された法人の代表者（または代表権を有する者），商業登記された商号を持つ個人事業主，または地方自治体などの組織・団体の代表者である。申請者は，本サービスの発行申請書を提出する際に，証明書を受ける当該サーバが実際に申請者の所属する組織・団体によって（または申請者の所属する組織・団体のために）運用されていることを保証しなければならない。申請者は，本サービスのサービス約款に同意し，本 CPS の申請者の義務に関する条項を遵守しなければならない。

1.3.6 技術管理担当者

技術管理担当者とは，TA 証明書の発行対象となるサーバの管理者であり，申請者から任命，委任または委託をうけた者である。本認証局から発行された TA 証明書は技術管理担当者に配布される。技術管理担当者は，本サービスのサービス約款に同意し，本 CPS の技術管理担当者の義務に関する条項を遵守しなければならない。

1.3.7 検証者

検証者とは，申請者の TA 証明書を信頼し利用する者である。検証者は，本 CPS の検証者の義務に関する条項を遵守し，本 CPS の内容について理解し承諾した上で，TA 証明書を利用しなければならない。

1.3.8 TA 証明書の適用範囲

本サービスにより発行された TA 証明書は，時刻配信業務に使用される。それ以外の用途で使用した場合，本認証局は一切の責任を負わない。

1.4 連絡先の詳細

本サービスに関する問い合わせは，電話，FAX，電子メールにて行うことができる。

問い合わせ先 ： 東北インフォメーション・システムズ株式会社
所在地 ： 〒980-0021 宮城県仙台市青葉区中央二丁目 9-10 セントレ東北
代表者 ： 早坂 栄二
連絡先住所 ： 〒980-0021 宮城県仙台市青葉区中央二丁目 9-10 セントレ東北
連絡担当窓口 ：電子認証センター
営業日 ： 土日祝祭日，年末年始（12 月 29 日から 1 月 3 日まで）を除く日
サポート時間 ： 営業日の午前 9 時から午後 5 時（正午から 1 時までの休憩時間を除く）まで
電話番号 ： 022-799-5566
FAX ： 022-799-5565

Email ： toinx.cert@toinx.co.jp

2 一般的な規定

2.1 義務

2.1.1 認証局の義務

本認証局は，本 CPS で規定する申請者，技術管理担当者および検証者に対し次の義務を負う。

1) 本 CPS に基づき本認証局の運用を行う。
2) 認証局の秘密鍵が危殆化しないように保護する。
3) 本認証局は，本 CPS 1.4（ 連絡先の詳細）に記載された営業日のサポート提供時間に問い合わせを受け付ける。
4) 本認証局は，リポジトリにて本 CPS を開示する。
5) 本認証局は，システム保守による一時停止，緊急時など，やむを得ない場合の停止を除き，CRL を作成し定期的にリポジトリに登録し，TA 証明書の有効期限の間これを公開する。
6) 本認証局は，本認証局の認証業務について定期的に監査を実施し，監査報告に基づいて必要と認められた場合は，認証業務の改善を行う。

2.1.2 発行局の義務

IA は，本 CPS で規定する申請者，技術管理担当者，検証者および RA に対して，次の義務を負う。

1) IA は，本 CPS に基づき運用される。
2) IA は，本 CPS に従い認証局の秘密鍵を生成し，危殆化することの無いように管理する。
3) IA は，RA の指示に従い，TA 証明書発行要求内容を正確に反映した TA 証明書を発行する。
4) IA は，RA の指示に従い TA 証明書の失効を行う。
5) IA は，本 CPS に規定された認証設備を使用する。

2.1.3 登録局の義務

RA は，本 CPS で規定する申請者，技術管理担当者，検証者および IA に対し，次の義務を負う。

1) RA は，本 CPS に基づき運用される。
2) RA は，TA 証明書の発行申請を適正に審査し，IA に対して TA 証明書の発行指示を行う。
3) RA は，TA 証明書の失効申請を適正に審査し，IA に対して TA 証明書の失効指示を行う。

4) RA は，TA 証明書を失効する事由が生じた場合，遅滞なく IA に失効の指示を行う。
5) RA は，申請者から入手した情報を機密情報として取り扱う。

2.1.4 申請者の義務

申請者は，本認証局によって発行された TA 証明書を技術管理担当者に使用させるにあたって，本認証局が提示するサービス約款に同意し，以下の事項について実施する義務を負う。

1) 正確な情報の記載確認

申請者は，TA 証明書の発行申請に際して提出する発行申請書に記載される申請者情報，技術管理担当者情報等を十分に確認し，正確，最新かつ真実の情報を記載しなければならない。

2) 申請者の秘密鍵の危殆化等に伴う失効申請

申請者は，申請者の秘密鍵が危殆化した場合またはその恐れがある場合，直ちに当該 TA 証明書の失効申請を行わなければならない。

3) TA 証明書の記載内容変更および使用中止等に伴う失効申請

申請者は，TA 証明書に記載されている事項に変更が生じた場合または TA 証明書の使用を中止する場合には，直ちに当該 TA 証明書の失効申請を行わなければならない。

4) TA 証明書記載事項の承諾

申請者は，発行申請書および CSR に記載された事項が，TA 証明書に転載される事を承諾しなければならない。

5) TA 証明書使用についての制限

申請者は，技術管理担当者に本 CPS に定める TA 証明書の適用範囲以外で TA 証明書を利用させてはならない。

6) 技術管理担当者への通知文書受け渡しの義務

申請者は，技術管理担当者への通知事項や送付文書を本認証局から受け取った場合，確実に技術管理担当者に渡さなければならない。

7) その他

上記の他，申請者は，サービス約款に定められた義務を負う。

2.1.5 技術管理担当者の義務

本認証局によって発行された TA 証明書を技術管理担当者が使用するにあたって，技術管理担当者は，本認証局が提示するサービス約款に同意し，以下の事項について遵守する義務を負う。

1) 申請者の秘密鍵の防護

技術管理担当者は，申請者の秘密鍵について技術管理担当者の責任において，危殆化しないように十分な注意をもって管理しなければならない。

2) 申請者の秘密鍵の危殆化の通知

技術管理担当者は，申請者の秘密鍵が危殆化した場合またはその恐れがある場合は，申請者を通じて直ちに本認証局に TA 証明書失効の申請を行わなければならない。

3) TA 証明書記載内容変更および使用中止等に伴う通知

技術管理担当者は，TA 証明書に記載されている事項に変更が生じた場合または TA 証明書の使用を中止する場合には，申請者を通じ直ちに TA 証明書の失効申請を行わなければならない。

4) TA 証明書使用についての制限

技術管理担当者は，本 CPS で規定された TA 証明書の適用範囲以外で TA 証明書を使用してはならない。

5) TA 証明書記載事項の承諾

技術管理担当者は，TA 証明書の発行申請の際に本認証局に届け出た技術管理担当者の電子メールアドレスが TA 証明書に記載される事を予め承諾しなければならない。

6) TA 証明書記載事項の確認

技術管理担当者は，発行された TA 証明書の記載内容を TA 証明書の取得時に確認しなければならない。また，TA 証明書の記載内容が誤りであることを認識した場合は，申請者を通じ直ちに TA 証明書の失効申請を行わなければならない。

7) 個人情報の取扱いおよび TA 証明書への記載範囲の承諾

本認証局は，技術管理担当者が TA 証明書の発行申請時に提出した個人情報の取扱いおよび TA 証明書への記載範囲について本 CPS に定める。技術管理担当者は本 CPS に記載された個人情報の取扱いおよび TA 証明書への記載範囲について承諾しなければならない。

8) 申請者への通知文書受取権限の付与

技術管理担当者は，本認証局が技術管理担当者への通知事項または通知文書を申請者に送付または通知することを承諾しなければならない。

9) その他

上記の他，技術管理担当者は，サービス約款に定められた義務を負う。

2.1.6 検証者の義務

本認証局で発行された TA 証明書を信頼するにあたって，検証者は，以下の事項を確認する義務を負う。

1) 利用範囲の確認

検証者は本 CPS に規定された TA 証明書の使用範囲を理解しその範囲内で TA 証明書を利用しなければならない。

2) TA 証明書の真正性の確認

検証者が，本認証局の認証局証明書を信頼し TA 証明書の真正性の検証を行う場合，

検証者は，本認証局の認証局証明書を入手し，その認証局証明書のハッシュ値と別途書面または電子媒体により入手した認証局証明書のハッシュ値を比較検証しなければならない。

また，認証局の秘密鍵による TA 証明書への電子署名が正しく行われており，当該 TA 証明書が本認証局から発行されたものであること，および TA 証明書が改竄されてないことを確認しなければならない。

3) TA 証明書の有効性の確認

検証者は，TA 証明書が有効期間内であるか，失効されていないかを検証しなければならない。

2.1.7 リポジトリの義務

本認証局は，CRL／ARL を常時公開する（認証設備の保守による一時的な停止，または，災害や障害等のやむを得ない場合の停止を除く）。また，本認証局は，本サービスに関する情報を本 CPS 2.7（公開およびリポジトリ）に従い開示する。

2.2 責任

2.2.1 認証局の責任

本認証局は，本 CPS およびサービス約款に従い本サービスを提供する。また，認証局の秘密鍵を適切に運用管理し，TA 証明書の信頼性を確保する。本認証局は申請者に対し以下の責任を負う。

- TA 証明書の発行および失効申請情報の適切な取扱いおよび情報の誤用がないこと
- 本認証局の運用および発行する TA 証明書が本 CPS に準拠していること

（１） 認証局の責任の制限

本認証局の責任は，本 CPS に定める認証局業務を信頼できる認証業務就業者によって行うことに限られ，本 CPS において本認証局が免責される旨を明示している事項や本認証局の責任や義務を明示していない一切の事項について義務および責任を負わない。

（２） 免責事項

以下の事象が発生した場合，本認証局は，全ての参加者（申請者，技術管理担当者，検証者）に対し免責とする。

1) 地震，水害，噴火，津波などの天災に起因する損害
2) 火災，停電などのあらゆる災害に起因する損害
3) 戦争，動乱，騒乱，暴動，労働争議などのあらゆる不可抗力に起因する損害
4) 本認証局が技術的あるいは運用上のやむを得ない理由で緊急にサービスを停止することに起因する損害

5) 申請者，技術管理担当者および検証者における電子署名および電子署名の検証に用いるソフトウェア，ハードウェアの誤動作又は障害に起因する損害
6) 本サービスの一部又は全部の終了に伴う TA 証明書発行の停止ならびに停止するリポジトリサービスに起因する損害
7) TA 証明書の失効処理を遅延なく行ったにもかかわらず，当該失効情報が掲載された CRL/ARL の公開前に TA 証明書が検証者に送付された結果発生する損害
8) 申請者，技術管理担当者および検証者が本 CPS，サービス約款に定められた義務および責任を果たさなかった結果発生した損害
9) 申請者の秘密鍵の危殆化に起因するあらゆる損害
10) 本サービスが使用する署名アルゴリズム（SHA-1withRSA）が将来において解読，危殆化した結果発生しうる損害
11) 郵便事故に起因するあらゆる損害

2.2.2 発行局の責任

IA は，本 CPS に従った運用を行い，RA の指示に基づき，TA 証明書の発行，失効を適切に行うことで，本認証局の発行する TA 証明書に係る情報の信頼性を確保する。

2.2.3 登録局の責任

RA は，本 CPS に従い，CSR を基に IA に対して適切な指示を行うことで，本認証局の発行および失効する TA 証明書に係る情報の信頼性を確保する。また，申請者の真偽確認のために提供された申請者の個人情報を適切に保護する。

2.2.4 申請者の責任

申請者は，本 CPS およびサービス約款で示される申請者の義務を遵守しなかったことに起因して発生する本認証局および検証者の損害に対し責任を負うものとする。また，技術管理担当者が本 CPS およびサービス約款で示される技術管理担当者の義務を遵守しなかったことに起因して発生する本認証局および検証者の損害に対し連帯して責任を負うものとする。

2.2.5 技術管理担当者の責任

技術管理担当者は，本 CPS およびサービス約款で示される技術管理担当者の義務を遵守しなかったことに起因して発生する本認証局および検証者の損害に対し責任を負うものとする。

2.2.6 検証者の責任

検証者は，本 CPS で示される検証者の義務を遵守しなかったことに起因して発生する本認証局および申請者の損害に対し責任を負うものとする。

2.3 財務上の保証

TOiNX は，本認証局の運営を維持し，かつその義務を履行するために十分な財政的基盤を有するものとする。

2.3.1 認証局の保証

本認証局が本 CPS 2.2.1（認証局の責任）に定める責任に違反して損害賠償責任を負う場合は，申込みの際に認証局が受領した発行手数料、あるいは契約手続きの際に認証局が受領した契約金額を上限とする。いかなる場合においてもこの賠償額の上限を超える請求には応じない。

2.3.2 申請者による保証

申請者は，本 CPS およびサービス約款で示される申請者の義務を遵守しなかったことに起因して発生する本認証局および検証者の損害に対し賠償しなければならない。また，技術管理担当者が本 CPS およびサービス約款で示される技術管理担当者の義務を遵守しなかったことに起因して発生する本認証局および検証者の損害に対し連帯して賠償しなければならない。

2.3.3 技術管理担当者による保証

技術管理担当者は，本 CPS およびサービス約款で示される技術管理担当者の義務を遵守しなかったことに起因して発生する本認証局および検証者の損害に対し賠償しなければならない。

2.3.4 検証者による保証

検証者は，本 CPS で示される検証者の義務を遵守しなかったことに起因して発生する本認証局および申請者の損害に対し賠償しなければならない。

2.4 人事管理などの規定

2.4.1 認証業務の委託

本認証局は，認証局の秘密鍵の運用管理および本サービスの TA 証明書発行および失効の運用管理など認証局業務の一部を信頼性ある第三者に委託することができる。認証業務の一部を委託した場合，委託先は，本 CPS を遵守して業務を行う。

2.4.2 専門性

本認証局は，本 CPS に従い，認証局としての信頼性を維持するため，専門性をもつ要員によって運用される。

2.4.3 組織体制

本認証局は，本 CPS に従い，認証局としての信頼性を維持するため，必要な組織体制を構築し，

運用する。

2.4.4 人事管理

本認証局は，認証業務就業者の信頼性および適格性並びにその満足な職務執行可能な人事管理に関する実務を確立し，これに従う。

2.5 解釈および執行

2.5.1 準拠法

当事者間の契約または他の準拠法を選択する旨の規定の有無にかかわらず，本 CPS の解釈および有効性等は日本国内法によって判断される。

2.5.2 分離、存続、合併、通知

本サービスが細分化されたり、他サービスを統合したり、または他サービスに統合される場合、本認証局は本サービスを実質的に継続すべく最善を尽くす。
上記に伴い本規定の変更が必要とされる場合には、本 CPS8（仕様管理）の規定に従う。

2.5.3 紛争解決手続き

全ての当事者は，本 CPS または本認証局が発行した TA 証明書に関して生じた紛争についての第 1 審の専属合意管轄裁判所を，仙台地方裁判所とすることで合意するものとする。本 CPS 及びサービス約款に定められていない事項やこれらの文書の解釈に関して疑義が生じた場合、各当事者は、その課題を解決するために誠意をもって協議するものとする。

2.6 料金

本サービスに係わる料金は別途定める。

2.7 公開およびリポジトリ

2.7.1 認証局の情報の公開

本認証局は，認証局の情報について以下に定める方法により提供する。

1) CPS
https://www.toinx.net/ta/cps.pdf
2) サービス約款
https://www.toinx.net/ta/agreement.pdf
3) 認証局証明書
https://www.toinx.net/ta/ca-certificate/toinxcata.cer

4) 認証局証明書のハッシュ値(フィンガープリント)
https://www.toinx.net/ta/ca-fingerprint/fp.pdf
5) CRL/ARL
http://crl.toinx.net/TohokuInformationSystemsCoIncTOiNXTACA/LatestCRL.crl
6) 認証局からのお知らせ
電子メールまたは書面にて通知

2.7.2 公開頻度

- 本 CPS の公開は, 本 CPS 8(仕様管理)に従い開示される。
- CRL/ARL は, 有効期間を 72 時間とし, 24 時間毎にリポジトリへ公開される。
- TA 証明書の失効情報は, 当該 TA 証明書の有効期間が満了するまで CRL に登録される。
- その他の本サービスに関する情報は, TOiNX の判断で適宜公開される。
- 認証局証明書, 認証局証明書のフィンガープリントは, 発行および更新の都度、開示可能とする。

2.7.3 アクセス管理

本認証局は, 公開可能な本サービスに関する情報について改竄防止措置を施したリポジトリを通じて公開する。申請者, 技術管理担当者および検証者は, 公開情報をリポジトリから入手可能である。ただし, 申請者, 技術管理担当者および検証者は, これらに修正を加えてはならない。

2.7.4 リポジトリ

リポジトリは 1 日 24 時間, 1週 7 日間運用される。ただし, システムの保守などにより予め通知し, 一時停止することがある。なお, 緊急時等やむを得ない場合は, 事前に連絡できない場合がある。
リポジトリに公開されている内容の変更は, 認証局責任者の指示のもとで行われる。

2.8 準拠性監査

本認証局は, 本 CPS に従い適正な業務を行っていることを検証するため監査を実施する。監査は, TOiNX 代表者が任命した監査人により実施される。

2.8.1 準拠性監査の頻度

本認証局は, TOiNX 代表者の指示により定期監査を実施する。

2.8.2 監査人の選定

監査人は, TOiNX 代表者によって, 認証局の監査に関する十分な知識を持った者が任命される。

2.8.3 監査人の監査される主体との関係

監査人は，独立性を確保するために認証業務部門には属さない TOiNX の専任監査担当者，または TOiNX 代表者が任命する外部監査人とする。

2.8.4 監査テーマ

本認証局が運営する IA，RA が，本 CPS を遵守して運営されているかを監査する。主な監査項目は次の通りである。

- IA および RA の運用業務
- 電子証明書のライフサイクル管理
- 認証局の秘密鍵の管理
- ソフトウェア，ハードウェアおよびネットワーク
- 物理的環境および設備
- 認証局の運営

監査項目は，TOiNX 代表者と監査人の間で検討し，決定される。

2.8.5 監査指摘事項への措置

本認証局は，監査結果の指摘事項について，セキュリティ対策技術の最新の動向を踏まえた業務の改善および設備，規定等の見直しを含む対策を講じる。重要または緊急を要する監査指摘事項については，認証局責任者の決定に基づき速やかに対応する。

2.8.6 監査結果の公開

本認証局は，監査結果の外部への公開を行わない。ただし，公的機関などから法律に基づく開示要求があった場合，その指示に従いこれを開示する。

2.9 機密情報

本サービスの業務を通じて知りえる本認証局のシステム，ネットワーク，詳細な認証手順などの公開されない情報の機密保持に関して，本認証局の定める規定に則り，その内容が，本認証局の業務に係る就業者の役割に応じて理解され，且つ維持されるようにする。

2.9.1 機密情報の種類

本認証局が保有する情報のうち，リポジトリに公開されている情報を除き，全て機密情報として取扱う。本認証局は，法の定めによる場合を除いて，原則としてこれらの情報を開示しない。また，漏洩，毀損，滅失などから保護し安全に保存するとともに，本サービスを提供するために必要な範囲を超えて使用しない。

2.9.2 個人情報の取扱い

本認証局は，TA 証明書の発行申請時に発行申請者から提供される情報および TA 証明書の失効申請時に失効申請者から提供される情報を個人情報として取扱い，本サービスを提供するための必要な範囲を超えて使用しない。また，その保護について以下に従う。

以下の内容について本認証局の認証業務に係わる全ての就業者に，それぞれの役割に応じて理解させるものとする。

1) 個人情報の位置付け

本認証局は，TA 証明書の発行申請および失効申請にあたり申請者から提供された情報のうち個人を特定可能な情報を個人情報として扱う。本認証局は，TA 証明書の発行申請および失効申請時に提出された申請書類の原本の還付を行わない。

2) 利用目的の特定

本認証局は，本サービスを申請者に提供するために必要な個人情報を本サービスの提供の目的にのみ利用する。

3) 利用目的による制限

本認証局は前項の目的以外に個人情報を使用しない。また，第三者から目的外利用を求められた場合，法令に定められた場合を除き，一切これに応じない。

4) 適正な取得

本認証局は，不正な手段により個人情報を取得しない。

5) 個人情報に関する事項の公表

本認証局は，個人情報の使用目的，情報の開示等について本 CPS で規定し，公表する。

6) データ内容の正確性の確保

本認証局は，発行申請や失効申請により申請者から取得する個人情報を用いて，個人情報の正確性の確保を行う。また，個人情報の取得により，TA 証明書の失効が必要な場合は，速やかに TA 証明書を失効する。

7) 安全管理措置および従業者，委託先の監督

本認証局は，申請者から取得した個人情報に対して，情報を取り扱う就業者の監督も含め，その漏洩，滅失，毀損の防止措置をとる。

8) 開示

本認証局は，申請者から権利又は利益を侵害され，又は，侵害される恐れがあるとの申し出があった場合，本 CPS の規定に従い法令に定められた場合を除き，申請者からのみ個人情報の開示申請を受け付ける。

2.9.3 TA 証明書の失効情報の公開

TA 証明書が失効された場合，失効された TA 証明書の CRL を生成し，検証者に対し提供する。CRL に含まれる情報は機密情報ならびに個人情報としない。失効に関するその他の情報は機密

情報として開示されない。

2.9.4 法執行機関への情報開示

本認証局で取扱う情報に対し，法的根拠に基づいて情報を開示するように請求があった場合は，本認証局は法の定めに従い法執行機関へ情報を開示する。

2.9.5 民事手続き上の情報開示

本認証局は，調停，その他の法的，裁判上または行政手続きの過程において，機密保持対象である情報を開示することができる。

2.9.6 情報の主体者の要請による情報開示

TA 証明書に記録されている者から，権利または利益を侵害され，あるいはその恐れがあるとして申し出があった場合，本認証局は，当該申出者（以下，「開示請求者」という）が TA 証明書に記録されている者であることを確認し，開示請求者に対して以下の書類を本認証局にて閲覧開示する。

- TA 証明書に係る発行申請書
- TA 証明書の記載内容

2.9.7 機密とみなされない情報

- CRL／ARL に含まれる情報。
- 本 CPS に含まれる情報。

2.10 知的財産権

別段の合意がなされない限り，以下の情報資料およびデータは，下記に示す当事者に帰属する知的財産として扱われる。

- 発行された全ての電子証明書は，これを発行した本認証局に帰属する財産である。
- 作成された CRL/ARL は，本認証局に帰属する財産である。
- 本 CPS は，本認証局に帰属する財産である。
- 申請者の秘密鍵および公開鍵は，これを保存し又は保護する物理的媒体が誰に帰属するかを問わず，申請者に帰属する財産である。
- 認証局の秘密鍵と公開鍵は，本認証局に帰属する財産である。

3 識別と本人確認

3.1 発行申請

TA 証明書の発行申請方法は，本 CPS に規定される。RA は，申請者の真偽の確認を適切に行わなければならない。なお，申請者が申し込みできる TA 証明書は1CSR に対し 1 枚とする。なお，複数の当該サーバに対して TA 証明書の発行を申請することができる。

3.1.1 名称の型

本認証局が発行する TA 証明書の発行者名（IssuerName），主体者識別名（Subject Name），主体者識別別名（SubjectAltName）は，ITU X.500 識別名（DN:DistinguishedName）の形式に従って設定される。

3.1.2 名称の意味に関する要件

TA 証明書に記載される名称（DN）は，RA が申請者の真偽確認の際に申請者から提出される発行申請書および添付される書類に記載されている内容が含まれる。詳細については，CPS9(別表 1 電子証明書詳細プロファイル)を参照のこと。

3.1.3 名称形式を解釈するための規則

ITU X.500 識別名（DN：DistinguishedName）の規定に従う。

3.1.4 名称の一意性

TA 証明書に記載される名称（DN）は，本認証局が発行した TA 証明書において一意に割り当てられる。

3.1.5 名称に関する紛争の解決手順

TA 証明書に記載される申請者の主体者識別名に係る紛争は本認証局と申請者での解決を原則とする。

3.1.6 商標の認識・認証・役割

本認証局から発行される TA 証明書に記載される申請者の主体者識別名には，商標を含む場合がある。ただし，本認証局は申請者に商標権が帰属することや，商標登録の有無等を確認しない。TA 証明書に記載された主体者識別名が，申請者に帰属しない商標を含むことにより，損害を被る者が発生した場合は，本認証局は一切の責任を負わず，当該申請者が自己の負担と責任の下で解決するものとする。

なお，申請者は，かかる商標を本認証局が TA 証明書に登録することを予め承諾しなければなら

ない。

3.1.7 秘密鍵の所有を証明するための方法

RA 登録業務で使用された CSR は TA 証明書の発行作業完了後，複数人の管理のもとで確実に消去・破棄される。TA 証明書の受取り確認は，技術管理担当者からの特段の申し出がない限り実施しない。

3.1.8 発行申請者の真偽の確認

本認証局は，TA 証明書の発行に先立って申請者の真偽確認を行う。RA 認証業務では，申請者の真偽確認を以下に定める方法により行う。

1) 申請者の存在確認・意思確認

- 必要な発行申請書類が全て提出されていること，および記入漏れが無いことを確認する。
- 申請者の所属する組織・団体が商業登記されている法人または個人事業主の場合，商業登記簿謄本によって存在を確認する。さらに申請者が TA 証明書の発行申請を行う時に提出する印鑑証明書によって，申請者の真偽確認を行う。発行申請書に記載されている氏名が印鑑証明書に記載されている氏名と同一であること，印鑑証明書の形式が公的機関からの発行形式であり公的機関の押印があること，有効期限が発行日から発行申請書の受付日までが 3 カ月以内であることを確認し，かつ，発行申請書に押印された実印の印影と印鑑証明書に証明されている印影が一致することを確認する。
- 申請者の所属する組織・団体が地方自治体などの場合，財務省印刷局発行の職員録により存在確認する。職員録による確認ができない場合は，官報により存在確認する。なお，職員録あるいは官報による確認ができない場合は，別途申請者と協議し確認方法を定める。

上記の審査において全ての確認が正しく検証できた場合，申請者の実在性および申込みの意思が確認できたと判断する。審査過程において，提出書類の不備や記載内容の不備などにより疑義が生じた場合は，本認証局は，技術管理担当者の連絡先に確認が正しく為されなかった理由を通知し，必要書類の再提出などを要請する。

3.2 更新申請

電子証明書の更新申請に対する審査は，発行申請の場合と同様の本 CPS 3.1（発行申請）に定める手続きに基づいて行う。

3.3 失効申請

TA 証明書の失効申請方法は，本 CPS にて規定される。RA は，失効申請者が申請者本人であることの確認を適切に行わなければならない。

3.3.1 失効申請者の真偽の確認

本認証局は，失効申請者が申請者本人であることの真偽の確認を行う。本認証局は，失効申請書を受付け，失効申請書に記載されている内容と失効申請の対象となる当該 TA 証明書の発行申請書に記載されている内容および押印されている印の印影が一致する場合は，本認証局は，申請者本人からの申請であると判断する。

申請者の印鑑証明書が失効申請書に添付されている場合は，失効申請書に押印された申請者の印の印影と印鑑証明書で証明された印の印影が一致することを確認する。

上記の審査において全ての確認が正しく検証できた場合，発行申請を行った申請者からの失効申請であることが確認できたと判断する。提出書類の不備や記載内容の不備などにより疑義が生じた場合は，本認証局は，失効申請者の確認が正しく為されなかった理由を申請者本人に通知し，必要書類の再提出などを要請する。

4 運用上の要件

4.1 TA 証明書発行申請

4.1.1 発行申請手続き

申請者は，発行申請書に明記されている本 CPS およびサービス約款を承諾した旨を記載した文面を確認して発行申請書上に署名，押印する。この署名，押印により，本認証局は申請者が本 CPS およびサービス約款に記載された事項を承諾しこれに遵守することに同意したと判断する。また，本 CPS およびサービス約款には，技術管理担当者に対する約款事項も記載されている。申請者は，本 CPS およびサービス約款内の技術管理担当者に対する約款事項の内容を理解，承諾の同意を得る必要がある。本認証局は，申請者の発行申請書上の署名，押印をもって，申請者が技術管理担当者に本 CPS およびサービス約款上に記述された各事項を承諾しこれを遵守することに同意させたと判断する。

申請者は取得した本 CPS およびサービス約款の内容を十分理解し同意しなければならない。同意できない場合，申請手続きを中止しなければならない。

申請者は，本 CPS 4.1.2（発行申請書類）に記載された書類を本認証局に提出する。本認証局は，郵送等によって申請者からの申請を受け付ける。

4.1.2 発行申請書類

申請者は，TA 証明書の発行申請にあたり，次の発行申請書類を本認証局に郵送等により提出しなければならない。

1) 発行申請書

申請者により押印された発行申請書の提出が必須である。なお，印鑑は申請者の印鑑証明書に係る印鑑である必要がある。

発行申請書の記載項目には以下のものを含む。

- サーバのコモン・ネームの英字表記
- 申請者の会社・団体名の英字表記
  - 申請者が商業登記されている法人または個人事業主の場合，登記されている商号
  - 申請者が地方自治体などの場合，その名称（県名など）
- 申請者の会社・団体の部門名称の英字表記
- 申請者の都道府県，市区町村の英字表記
  - 申請者が商業登記されている法人または個人事業主の場合，登記されている法人の本社住所
  - 申請者が地方自治体などの場合，その所在地住所（県庁の住所など）

- 技術管理担当者の氏名, 所属部署, 役職名, 会社名, 都道府県, 市区町村, 会社住所, 郵便番号, 電子メールアドレス, 電話, FAX
- 事務手続担当者の氏名, 所属部署, 役職名, 会社名, 都道府県, 市区町村, 会社住所, 郵便番号, 電子メールアドレス, 電話, FAX
- 申請者の所属する会社名, 役職名, 会社代表者名, 印鑑証明書で証明される会社代表者の実印
- 本 CPS およびサービス約款への同意, 承諾を示す記述

2) 申請者の印鑑証明書

申請者の真偽確認のために, 発行申請書に押印した印鑑に係る申請者が所属する法人の印鑑証明書の提出が必須である。印鑑証明書の有効期限は発行日から申請書類の受付日までが 3 カ月以内であること。

3) 商業登記簿謄本

申請者の実在性確認のために, 商業登記簿謄本の提出が必須である。商業登記簿謄本の有効期限は発行日から申請書類の受付日までが 3 カ月以内であること。

4) CSR

TA 証明書発行手続きのために, 当該サーバにて生成した CSR の提出が必須である。なお, CSR は原則として, フロッピーディスクに格納して提出するものとする。

4.1.3 発行申請の審査

RA 認証業務は, 本 CPS 3.1.8(発行申請者の真偽の確認)に従って発行申請者の真偽の確認を行う。審査に不備がない場合, RA 認証業務は, 申請者の発行申請の登録作業を RA 登録業務に依頼する。

4.1.4 発行申請の登録

RA 登録業務は, RA 認証業務からの発行依頼に従い, 権限のある操作者によって申請者から受理した CSR を登録する。RA 登録業務は, 登録した CSR と RA 認証業務から提供された TA 証明書記載情報を用いて専用の RA 登録業務用設備内で証明書発行リクエストを生成し, IA に証明書発行指示と共に送信する。送信される証明書発行リクエストは, RA 登録業務用設備により電子署名され且つ暗号化されている。

4.2 TA 証明書の発行

IA 認証業務用設備は, 権限のある操作者の操作により RA 登録業務用設備から送信された証明書発行リクエストの電子署名を解読し, 正当な RA 登録業務用設備からの証明書発行リクエストであることを確認する。RA 登録業務用設備の電子署名が正しく確認できた場合, IA 認証業務用設備は, TA 証明書を生成し, 電子メールにて技術管理担当者に送信する。

4.3 TA 証明書の受取

技術管理担当者は、電子メールにて TA 証明書を受領した後、TA 証明書の記載内容の確認などを行わなければならない。

本認証局は、当該 TA 証明書の発行後、技術管理担当者からの TA 証明書を受領できない旨の報告を受け、本認証局がその事実を確認できた場合、当該 TA 証明書の失効処理を行うことができる。

4.4 TA 証明書の更新申請

本 CPS 4.1(TA 証明書発行申請)と同様とする。

4.5 TA 証明書の失効申請

4.5.1 申請者による失効申請

申請者は，以下の項目に該当する場合には，直ちに本認証局に対して TA 証明書の失効申請を行わなければならない。

- 申請者から TA 証明書の失効申請の依頼を受けた場合
- 申請者の秘密鍵について危殆化もしくはその恐れが生じた場合
- 申請者の秘密鍵が破損し使用不能となった場合
- TA 証明書の利用を中止した場合
- TA 証明書の記載事項が事実と異なる場合
- TA 証明書の記載事項が変更された場合
- その他，技術管理担当者が TA 証明書を失効させる必要があると判断した場合

4.5.2 認証局による失効申請

本認証局は，申請者からの失効請求の他に，有効期限内にある TA 証明書について，以下の理由により TA 証明書の有効性が損なわれたと判断した場合には，TA 証明書を遅滞なく失効する。本認証局は，失効処理が完了した後，申請者に失効完了通知を行う。

- 本認証局を廃止する場合
- 認証局の秘密鍵が危殆化もしくはその恐れがある場合
- TA 証明書記載事項が事実と異なる場合
- 申請者の秘密鍵が危殆化もしくはその恐れがある場合
- ネットワーク上の不具合または電子メール不達により技術管理担当者が正しく TA 証明書を受領できなかった場合
- その他，本認証局の認証局責任者が必要と判断した場合

4.5.3 失効申請書類

申請者は，TA 証明書の失効にあたり，失効申請書を本認証局に提出しなければならない。

1） 失効申請書

失効申請書には以下の項目が含まれる。

- 失効理由
- コモン・ネーム（当該失効対象の TA 証明書の発行申請時に申請した情報）
- シリアル番号（TA 証明書のシリアル番号）
- 技術管理担当者の氏名，所属部署，役職名，会社名，都道府県，市区町村，会社住所，郵便番号，電子メールアドレス，電話，FAX
- 事務手続担当者の氏名，所属部署，役職名，会社名，都道府県，市区町村，会社住所，郵便番号，電子メールアドレス，電話，FAX
- 申請者の所属する会社名，役職名，会社代表者名，印鑑証明書で証明される会社代表者の実印（当該失効対象の TA 証明書の発行申請時に押印された印）

2） 申請者の印鑑証明書

申請者の印が変更され，当該失効対象の TA 証明書の発行申請書に押印した印鑑による押印が不可能である場合，新たに押印した印に係る印鑑証明書を提出しなければならない。

3） 商業登記簿謄本

申請者の住所が変更された場合，失効申請書に記載した新たな住所を証明する商業登記簿謄本を提出しなければならない。

4.5.4 失効申請の審査

RA 認証業務は，申請者からの失効申請書を受領し，本 CPS 3.3.1(失効申請者の真偽の確認)に従い複数人により失効申請者の真偽の確認および失効申請書の記述内容の確認を行う。真偽の確認の結果が真であり且つ失効申請書の記述が適切である場合に失効を承認し，RA 登録業務に失効依頼を行う。

4.5.5 失効申請の登録

RA 登録業務は，RA 認証業務の依頼に従い，複数人の管理の下，RA 登録業務用設備内で証明書失効リクエストを生成し，IA に証明書失効指示と共に送信する。送信される証明書失効リクエストは，RA 登録業務用設備により電子署名され且つ暗号化されている。

4.5.6 TA 証明書の失効

IA は，RA 登録業務用設備から送信された証明書失効リクエストの電子署名を検証し，正当な RA 登録業務用設備からの証明書失効リクエストであることを確認する。RA 登録業務用設備の電子署名が正しく確認できた場合，IA は，TA 証明書を失効する。

4.5.7 失効申請者への通知

本認証局は，TA 証明書の失効処理が完了した後，申請者に失効完了の旨を通知する。

4.5.8 一時停止

本認証局では，TA 証明書の一時停止を行わない。

4.5.9 失効リスト（CRL）

本認証局は，CRLを定期的に更新し，TA 証明書に記載された場所に公開する。CRLの有効期間は 72 時間とし発行のタイミングは 24 時間毎に行う。

4.5.10 秘密鍵の危殆化に関する特別要件

本認証局は，認証局自身の秘密鍵が危殆化または危殆化の恐れがある場合は，本サービスを停止し，遅滞なく全ての TA 証明書を失効し CRL/ARL の登録を行う。

4.6 セキュリティ監査手続き

TOiNX は、本認証局を安全に運営していくための一つの手段として、認証局責任者が必要と判断した場合にセキュリティ監査を実施する。

4.6.1 記録されるイベント

本認証局における監査証跡には、以下のものが含まれる。

- 電子証明書の作成および失効の記録
- 電子証明書の作成および失効に係る認証業務用設備の操作履歴
- 認証設備室への入退室記録
- 認証業務用設備への不正アクセスの記録
- 認証業務用設備の動作に関する記録

4.6.2 監査の頻度

監査証跡は、本認証局のシステムを安全に運営するために適切と考えられる頻度で、セキュリティ上の問題が発生していないか調査する。

4.6.3 監査ログの保存期間

監査証跡の保存期間は、別途定めた規程において定義される。

4.7 記録のアーカイブ

本認証局は、全ての申請書類およびサービスの運営に必要とされる記録類を TA 証明書の有効期間の間保存する。保存にあたっては漏洩、改ざん、毀損、滅失の防止措置をとり、認証業務関係

書類については原本を直射日光があたらない鍵付の保管庫に保存し、間仕切りで独立し、施錠された認証業務室において保存する。各書類が保存される室には、災害、火災対策などの措置が講じられ、保存内容の完全性および機密性が損なわれることがないような措置がとられている。

4.7.1 アーカイブデータの保護

アーカイブに使用するメディアは、認証業務室又は認証設備室内に漏洩、改ざん、毀損、滅失などが行われないように安全に保存管理される。また、温度、湿度、磁気などの環境における要素を考慮した上で保護される。

4.7.2 アーカイブデータのバックアップ

バックアップが必要なアーカイブデータについては、別途定めたバックアップ手順に従いバックアップを行う。

4.7.3 アーカイブ情報の保存

本認証局は、アーカイブされた情報が保存期間を通じて読解可能な状態で保存する。

4.8 秘密鍵の更新

申請者の秘密鍵は、自動的に更新されることなく、対応する TA 証明書の有効期限が切れると同時に申請者の秘密鍵も無効となる。利用者は TA 証明書および申請者の秘密鍵の更新が必要な場合は、TA 証明書の発行申請と同様の方法で再度申請を行わなければならない。本認証局は、発行申請書の審査および承認のプロセスを経て申請者から提示された CSR を基に新たな TA 証明書を発行する。

認証局証明書の秘密鍵の更新は、20年毎に新たな鍵ペアを生成する。

4.9 危殆化と災害の復旧

認証局の秘密鍵の危殆化、災害等による障害の発生など不測の事態が生じた時又は生じる恐れのある時には、本認証局は、対策措置を迅速に講じるとともに次のとおり対応する。

1) 認証局の秘密鍵の危殆化又は危殆化の恐れがあることが判明した場合

- 本認証局の発行業務を直ちに停止する。
- 本認証局は、TA 証明書の検証を一時的に不可能とする対策を行なう。
- 本認証局は、直ちに認証局の秘密鍵を用いて発行した全ての有効な TA 証明書を失効し、全利用者に適切な方法で通知するとともに、CRL/ARL を更新しリポジトリを通じて検証者に公開する。
- 認証局の秘密鍵を完全に破棄する。
- 本認証局は、すみやかに危殆化の原因および被害状況を調査し、対応策および再発防止策を講じる。

- サービスを継続することが可能な場合は、可及的すみやかに本 CPS に従い新たな認証局の秘密鍵を生成し TA 証明書の発行申請を受付け可能とする。

2) 天災事変等の被災、認証業務用設備の故障等により運用を停止した場合
   - 本認証局は、災害等による障害発生により、72 時間を超えて CRL/ARL の更新が見込めない場合、TA 証明書の検証を一時的に不可能とする対策を行なう。
   - 本認証局は、被害の事実を全利用者、検証者に適切な方法で通知する。
   - 本認証局は、災害等による障害発生の原因および被害状況を調査し、対応策および再発防止策を講じる。
3) 本認証局は、鍵の危殆化もしくは被災の際の復旧手順について別途定め、計画に従って教育訓練を行う。

4.10 認証業務の終了

本認証局は、災害等による不測の事態の発生により業務の不履行に至った場合等に認証業務を終了する。

1) 発行済み電子証明書の失効処理方法

   認証業務の廃止日迄に、本認証局によって発行された全ての有効な TA 証明書を失効し、失効情報を登録した CRL/ARL を更新しリポジトリを通じて検証者に公開する。

2) 利用者への連絡方法、連絡時期等

   全ての利用者に対し業務終了の 60 日前から適切な方法で業務終了の案内を通知する。

3) 廃止後の失効情報の公開

   本認証局は、電子証明書の失効完了に伴い、失効した全ての電子証明書に記載されている有効期間満了日まで有効な CRL/ARL を発行し、有効期間が切れるまでリポジトリに公開する。

4) 認証局の秘密鍵の処理

   本認証局は、認証局の秘密鍵およびバックアップされた秘密鍵の全てを完全に初期化する。

5 物理的, 手続き的, 要員的なセキュリティ統制

5.1 物理的セキュリティ統制

認証業務のための設備は, 通常想定される災害に対しては十分耐え得る建築構造物内に設置され, 以下のとおり, そのセキュリティ対策が講じられる。

5.1.1 認証業務室のセキュリティ

認証業務関係書類および記録を保存管理し日常その業務運営を行う室(認証業務室)は、これを独立した区画とし、無人の際には入退室口の施錠を行う。その鍵の管理および授受については予め任命された管理者により管理される。

入室権限を有しない者の入室は原則として認められないが、やむを得ずこれを認める場合には、予め管理責任者の許可を得、入室権限者同行のうえこの者を入室させることができる。

5.1.2 認証設備室のセキュリティ

認証業務用設備を収容する建築構造物(建物および部屋)に関しては、耐震耐火設計、自動火災報知器と消火装置の設置、防火区画内設置、隔壁による区画、水害防止等の措置が予め十分講じられている等、地震、火災、水害等想定される災害にも耐えうる設備とする。また、停電に備えた UPS および自家発電機の設置、配置された設備に応じた空調機器の設置等、サービスの継続に必要な適切な措置が講じられている。認証設備室への入退室等については、厳重に管理される。

5.2 手続き的セキュリティ統制

各役割に従事する者の任命, 物理的な部屋毎の入室権限の設定, 認証業務用設備へのシステム毎のアクセス権限の設定は予め定められた手続に従い, 特定の権限者がこれを行う。

5.3 要員的セキュリティ統制

認証業務に従事する者は入社前・入社後の経歴や経験等を踏まえ, 従事するのに適格であるかどうかの確認を行った上で, 任命・配置を行う。

個人情報の取扱いと保護, 認証局の秘密鍵の危殆化および災害等による障害発生など不測の事態に対する対応策の教育訓練も含め, 本認証局は, 認証業務従事者の信頼性, 適格性および業務遂行能力の維持に努める。

6 技術的セキュリティ統制

6.1 鍵ペアの生成とインストール

認証局の秘密鍵に関しては，信頼性あるシステムを用いて生成し，その漏洩，改変，毀損等，あるいは無断使用の防止措置を十分に講じて保護する。

6.1.1 鍵ペアの生成

1) 認証局鍵ペア生成

認証局の鍵ペアは，本認証局構築時に認証設備室内に設置された暗号装置内で，複数人の管理の下，一人の操作だけではできない方法により生成される。

2) 申請者鍵ペア生成

申請者の鍵ペアは，CSR 作成時に技術管理担当者が管理するサーバ内で生成される。

6.1.2 認証局への公開鍵の配送

申請者の公開鍵は，CSR により申請者から本認証局へ提出される。

6.1.3 申請者への認証局証明書の配送

認証局証明書は、リポジトリからダウンロードすることにより入手することができる。

6.1.4 鍵長

本認証局で生成される各電子証明書で証明される公開鍵の鍵長は以下の通りである。

表 6-1 公開鍵の鍵長

電子証明書種別	鍵長
認証局証明書	2,048bit
TA 証明書	1,024bit または 2,048bit

6.1.5 鍵の使用目的

認証局の秘密鍵は，以下の目的以外に使用されない。

- TA 証明書への電子署名
- CRL への電子署名

6.2 秘密鍵の保護

6.2.1 秘密鍵の管理

認証局の秘密鍵は，その使用にあたり暗号装置の状態変更を行い活性化される必要がある。こ

の活性化にあたっては，その権限をもつ複数人の要員が活性化データにより活性化できるように運用する。秘密鍵の生成および活性化については，複数人の管理の下，認証設備室内において定められた手順により行われる。

申請者の秘密鍵は，CSR 作成時に技術管理担当者が管理するサーバ内で生成されるため，技術管理担当者の責任において安全に管理される。

6.2.2 秘密鍵の寄託

本認証局は，認証局の秘密鍵の寄託を行わない。

6.2.3 秘密鍵のバックアップ

認証局の秘密鍵は，鍵が格納されている暗号装置と同型の暗号装置間のクローニング（複製）機能によりバックアップを行う。バックアップは，複数人の管理の下，認証設備室内において定められた手順により行われる。バックアップ用の暗号装置は，定められた手順に従って認証設備室内の安全な場所に保存される。

6.2.4 秘密鍵の暗号装置への格納

認証局の秘密鍵は暗号装置内で生成保存されるため，暗号装置の外から格納されることはない。

6.2.5 秘密鍵を非活性化する方法

認証局の秘密鍵を非活性化する方法は，認証設備室内において，複数人の要員が認証アプリケーションを停止し，暗号装置に格納された認証局の秘密鍵を非活性化にする。

申請者の秘密鍵を非活性化にする方法は，技術管理担当者の責任において削除することにより行われる。

6.2.6 秘密鍵の破棄

認証局の秘密鍵の廃棄は，定められた手順に従い，専用の機器を用いて，複数人の管理の下，鍵を完全に復元できない方法により行われる。また，バックアップされた秘密鍵も一連の作業指示において遅延なく完全に破棄される。

申請者の秘密鍵の破棄は，技術管理担当者の責任において削除することにより行われる。

6.3 ネットワークセキュリティ

RA 登録業務用設備は，外部からの不正なアクセスを防止するためのファイヤーウォールを備えており，IA 認証業務用設備は，外部からの不正なアクセスを防止するためのファイヤーウォールおよび不正なアクセス等を検知するシステムを備えている。

RA，IA 間で行われる通信に関しては，送信をした設備の誤認，通信内容の盗聴および改変を

防止するセキュリティ機能を持ったアプリケーションが使用される。通信設備についても安全に関して適切な管理を行っている。

6.4 暗号装置セキュリティ

本認証局は，FIPS（連邦情報処理標準）140-1 Level3 の認定を受けた暗号装置を使用する。また，その安全性に対する脅威についての情報を常に収集し，問題があればそれに対する対策を行う。

7 電子証明書と CRL/ARL のプロファイル

本認証局が発行する電子証明書と CRL/ARL の形式，属性の仕様は，以下の標準仕様に従い定義している。

1) ITU-T Recommendation X.509 (1997)
2) RFC3280：Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (RFC3280)

7.1 電子証明書と CRL/ARL のプロファイル詳細

電子証明書と CRL/ARL の各フィールドの設定内容は RA または IA で設定する。設定内容は本 CPS 9(別表1 電子証明書詳細プロファイル)および本 CPS 10(別表2 CRL／ARL 詳細プロファイル)に記述する。

7.1.1 バージョン番号

電子証明書と失効リストのバージョンは，次のとおりとする。

表 7-1 バージョン番号

電子証明書	バージョン番号
TA 証明書	X.509 バージョン 3
認証局証明書	X.509 バージョン 3

失効リスト	バージョン番号
CRL/ARL	X.509 バージョン 2

7.1.2 電子証明書拡張領域(CertificateExtensions)

電子証明書および CRL/ARL の拡張領域では各フィールドにクリティカル指定(Criticality)を行う。拡張領域の各フィールドのエンコーディング順序はIAが設定する。詳細は，本CPS 9(別表1 電子証明書詳細プロファイル)および本 CPS 10(別表2 CRL／ARL 詳細プロファイル)に記述する。

7.1.2.1 鍵種別(KeyUsage)

電子証明書の鍵種別は，次のとおりとする。

表 7-2 鍵種別(KeyUsage)

電子証明書	値	説明
TA 証明書	DigitalSignature NonRepudiation KeyEncipherment	電子署名 否認防止 鍵暗号化
認証局証明書	KeyCertSign CRLSign	TA 証明書中の CA の署名検証 CRL 中の CA の署名検証

7.1.2.2 証明書ポリシー(CertificatePolicies)

本 CPS1.2(識別)で定めるオブジェクト識別子(OID)と本 CPS を公開した URL を指定する。詳細は本 CPS 9(別表1 電子証明書詳細プロファイル)に記述する。

表7－3

電子証明書	種別	値
TA 証明書	PolicyIdentifier PolicyQualifiers	1.2.392.200121.1.5.1 https://www.toinx.net/ta/cps.pdf
認証局証明書	設定しない	－

7.1.2.3 基本制約(BasicConstraints)

認証局証明書の場合, cA=TRUE を設定する。クリティカル指定は, TRUE とする。TA 証明書については、設定しない。詳細は, 本 CPS 9(別表1 電子証明書詳細プロファイル)に記述する。

7.1.2.4 認証局鍵識別子(AuthorityKeyIdentifier)

表 7-4 の通り設定する。詳細は, 本 CPS 9(別表1 電子証明書詳細プロファイル)に記述する。

表 7-4 認証局鍵識別子(AuthorityKeyIdentifier)

電子証明書	値の説明
TA 証明書	認証局公開鍵の SHA-1 ハッシュ値
認証局証明書	認証局公開鍵の SHA-1 ハッシュ値

失効リスト	値の説明
CRL	認証局公開鍵の SHA-1 ハッシュ値
ARL	認証局公開鍵の SHA-1 ハッシュ値

7.1.2.5 主体者鍵識別子(SubjectKeyIdentifier)

表 7-5 の通り設定する。詳細は, 本 CPS 9(別表1 電子証明書詳細プロファイル)に記述する。

表 7-5 主体者鍵識別子(SubjectKeyIdentifier)

電子証明書	値の説明
TA 証明書	申請者公開鍵の SHA-1 ハッシュ値
認証局証明書	認証局公開鍵の SHA-1 ハッシュ値

7.1.2.6 CRL 配布点(CRLDistributionPoints)

CRL／ARL の公開場所は, 設定する。詳細は, 本 CPS 9(別表1 電子証明書詳細プロファイル)に記述する。

7.1.3 署名アルゴリズム

電子証明書と CRL/ARL の署名アルゴリズムは sha1WithRSAEncryption(オブジェクト識別子: 1 2 840 113549 1 1 5)方式を用い, TA 証明書、認証局証明書及び CRL／ARL は、2048bit

の RSA 鍵で署名される。また，各々の電子証明書に含まれる公開鍵は RSA 方式（オブジェクト識別子: 1 2 840 113549 1 1 1）である。ただし，署名に用いている秘密鍵や署名方式が危うくなった場合には，アルゴリズムや鍵長を変更する。

7.1.4 名称形式（NameForms）

本認証局が発行する全ての電子証明書および CRL/ARL の識別名称は，ITU X.500 識別名（DN：DistinguishedName）の規定に従い指定する。本認証局が発行する電子証明書の発行者識別名（IssuerName），主体者識別名（SubjectName）の記述は英語またはローマ字を使用する。

7.1.5 名称制限（NameConstraints）

設定しない。

7.1.6 ポリシー制限の使用方法（PolicyConstraints）

設定しない。

7.1.7 有効期間

電子証明書と失効リストの有効期間は，次のとおりとする。

表 7-6 有効期間

電子証明書	有効期間または 有効期限	更新の時期
TA 証明書	2221 日間 （6 年 1 ヶ月）	有効期間満了の 30 日前から有効期間が満了するまでに更新
認証局証明書	2026/2/12 23:59:59 まで(UTCTime)	

失効リスト	有効期間または 有効期限	発行頻度
CRL/ARL	72 時間	24 時間毎

7.1.8 失効に関する情報

TA 証明書の失効情報は CRL に記載される。認証局証明書の失効情報は ARL に記載される。CRL/ARL には，失効した電子証明書のシリアル番号，失効日時および失効理由（RFC3280 で定義されている失効の理由コード）が記載される。また，拡張部に AuthorityKeyIdentifier，CRLNumber が記載される。詳細は，本 CPS 10（別表2 CRL／ARL 詳細プロファイル）に記述する。

8 仕様管理

本認証局は，新技術の動向を踏まえ，業務の改善に努めるとともに，必要ある場合には本 CPS を改訂する。

8.1 CPS の仕様変更手続き

本認証局は，本 CPS の仕様に変更が発生した場合，申請者および検証者に事前の承諾なしに随時，本 CPS を修正することができる。本認証局は，本 CPS の修正版の修正部分または修正後の全文を書面または電子媒体で開示することにより申請者および検証者へ提供可能とする。

9 別表1 電子証明書詳細プロファイル

TA 証明書プロファイル

【 基本部 】

項目	型	値
Version (X.509のバージョン)	INTEGER	2
SerialNumber (発行番号)	INTEGER	ユニークな数
Signature.AlgorithmIdentifier (証明書に付された署名アルゴリズムの識別)		
Algorithm (署名アルゴリズム)	オブジェクト識別子(OID)	1 2 840 113549 1 1 5 (sha1withRSAEncryption を示します)
Parameters (パラメータ)	ヌル(NULL)	
Issuer (発行者)		
organizationalUnitName (認証業務名)	オブジェクト識別子(OID)	2 5 4 3
	PrintableString	"TOiNX TA CA"
OrganizationName (組織名)	オブジェクト識別子(OID)	2 5 4 10
	PrintableString	"Tohoku Information Systems Co.,Inc."
Country (国名)	オブジェクト識別子(OID)	2 5 4 6
	PrintableString	"JP"
Validity (有効期間)		
NotBefore(開始日)	UTCTime	YymmddhhmmssZ(年月日時間分秒 Z)
NotAfter(終了日)	UTCTime	YymmddhhmmssZ(年月日時間分秒 Z)
Subject (申請者)		
Specified By CSR		

【 拡張部 】

項目	Critical	型	値
AuthorityKeyIdentifier (認証局鍵識別子)	FALSE	オブジェクト識別子(OID)	2 5 29 35
KeyIdentifier		OCTET STRING	認証局公開鍵 SHA-1 ハッシュ値
SubjectKeyIdentifier (主体者鍵識別子)	FALSE	オブジェクト識別子(OID)	2 5 29 14
KeyIdentifier		OCTET STRING	申請者公開鍵の SHA-1 ハッシュ値
Key Usage (鍵の用途)	TRUE	オブジェクト識別子(OID)	2 5 29 15
DigitalSignature		BIT STRING	1
NonRepudiation		BIT STRING	1
KeyEncipherment		BIT STRING	1
SubjectAltName (サブジェクトの別名)	FALSE	オブジェクト識別子(OID)	2 5 29 17
Rfc822Name		IA5String	申請者のEmail address

certificatePolicies （証明書ポリシ）	FALSE	オブジェクト識別子(OID)	2 5 29 32
policyIdentifier			
certPolicyId		オブジェクト識別子(OID)	1.2.392.200121.1.5.1
policyQualifiers			
policyQualifierID		オブジェクト識別子(OID)	1 3 6 1 5 5 7 2 1(CPS の配布点)
qualifier		IA5String	https://www.toinx.net/ta/cps.pdf
CRLDistributionPoints (CRLのリポジトリ登録先)	FALSE	オブジェクト識別子(OID)	2 5 29 31
URI		URL	http://crl.toinx.net/TohokuInformationSystemsCoIncTOiNXTACA/LatestCRL.crl

認証局証明書プロファイル

【 基本部 】

項目	型	値
Version (X.509のバージョン)	INTEGER	2
SerialNumber （発行番号）	INTEGER	ユニークな数
Signature.AlgorithmIdentifier（証明書に付された署名アルゴリズムの識別）		
Algorithm (署名アルゴリズム)	オブジェクト識別子(OID)	1 2 840 113549 1 1 5 (sha1withRSAEncryption を示します)
Parameters（パラメータ）	ヌル(NULL)	
Issuer（発行者）		
CommonName (認証業務名)	オブジェクト識別子(OID)	2 5 4 3
	PrintableString	“TOiNX TA CA”
OrganizationName (組織名)	オブジェクト識別子(OID)	2 5 4 10
	PrintableString	“Tohoku Information Systems Co.,Inc.”
Country （国名）	オブジェクト識別子(OID)	2 5 4 6
	PrintableString	“JP”
Validity（有効期間）		
NotBefore(開始日)	UTCTime	YymmddhhmmssZ(年月日時間分秒 Z)
NotAfter(終了日)	UTCTime	YymmddhhmmssZ(年月日時間分秒 Z)
Subject（申請者）		
CommonName (認証局名)	オブジェクト識別子(OID)	2 5 4 3
	PrintableString	“TOiNX TA CA”
OrganizationName (組織名)	オブジェクト識別子(OID)	2 5 4 10
	PrintableString	“Tohoku Information Systems Co.,Inc.”
Country （国名）	オブジェクト識別子(OID)	2 5 4 6
	PrintableString	“JP”
SubjectPublicKeyInfo(サブジェクトの公開鍵)		
Algorithm (公開鍵の暗号方式)	オブジェクト識別子(OID)	1 2 840 113549 1 1 1 （rsaEncryption を示します）
SubjectPublicKey (認証局公開鍵)	ビット数(BIT STRING)	2048it の公開鍵

【 拡張部 】

項目	Critical	型	値
AuthorityKeyIdentifier （認証局鍵識別子）	FALSE	オブジェクト識別子(OID)	2 5 29 35
KeyIdentifier		OCTET STRING	認証局公開鍵 SHA-1 ハッシュ値
SubjectKeyIdentifier （主体者鍵識別子）	FALSE	オブジェクト識別子(OID)	2 5 29 14
KeyIdentifier		OCTET STRING	認証局公開鍵の SHA-1 ハッシュ値

Key Usage (鍵の用途)		TRUE	オブジェクト識別子(OID)	2 5 29 15
	KeyCertSign		BIT STRING	1
	cRLSign		BIT STRING	1
BasicConstraints (基本制約)		TRUE	オブジェクト識別子(OID)	2 5 29 19
	CA		BOOLEAN	TRUE(CA であることを示します)
	pathLen		INTEGER	0
CRLDistributionPoints (CRLのリポジトリ登録先)		FALSE	オブジェクト識別子(OID)	2 5 29 31
	URI		URL	http://crl.toinx.net/TohokuInformationSystemsCoIncTOiNXTACA/LatestCRL.crl

10 別表2 CRL／ARL 詳細プロファイル

CRL／ARL プロファイル

X.509 バージョン 2 の CRL を利用する。

【 基本部 】

項目	型	値
Version (バージョン番号)	INTEGER	1(V2)
Signature (署名アルゴリズム)	オブジェクト識別子(OID)	1 2 840 113549 1 1 5 (sha1withRSAEncryption を示します)
Parameters	ヌル(NULL)	NULL
Issuer (発行者)		
CommonName (認証業務名)	オブジェクト識別子(OID)	2 5 4 3
	PrintableString	"TOiNX TA CA"
OrganizationName (組織名)	オブジェクト識別子(OID)	2 5 4 10
	PrintableString	"Tohoku Information Systems Co.,Inc."
Country (国名)	オブジェクト識別子(OID)	2 5 4 6
	PrintableString	"JP"
ThisUpdate (今回更新日時)	UTCTime	YymmddhhmmssZ(年月日時間分秒 Z)
NextUpdate (次回更新日時)	UTCTime	YymmddhhmmssZ(年月日時間分秒 Z)
RevokedCertificates (失効した TA 証明書のリスト)		
UserCertificate (失効されるTA証明書)	INTEGER	失効される TA 証明書のシリアル番号
RevocationDate (失効の日時)	UTCTime	YymmddhhmmssZ(年月日時間分秒 Z)
CrlEntry Extentions(失効された TA 証明書ごとの拡張領域)		

ReasonCode (理由コード)	FALSE	オブジェクト識別子(OID)	2 5 29 21
		BIT STRING	理由コードの値

【 拡張部 】

項目	Critical	型	値
AuthorityKeyIdentifier (認証局鍵識別子)	FALSE	オブジェクト識別子(OID)	2 5 29 35
KeyIdentifier		OCTET STRING	認証局公開鍵 SHA-1 ハッシュ値
CRLNumber	FALSE	オブジェクト識別子(OID)	2 5 29 20
			CRL 番号
IssuingDistributionPoint	TRUE	オブジェクト識別子(OID)	2 5 29 28
DistributionPoint			
Fullname		オブジェクト識別子(OID)	2 23 42 2 0

			URI		IA5String	http://crl.toinx.net/TohokuInformationSystemsCoIncTOiNXTACA/LatestCRL.crl