国立情報学研究所クライアント証明書サービスのための東京大学登録局の運用ポリシーおよび運用規則

Version 1.2

東京大学情報基盤センター

2018 年 12 月 7 日

バージョン	日付	適用
国立情報学研究所クライアント証明書サービスのための東京大学登録局の運用ポリシーおよび運用規則		
1.0	2018/2/9	NII「UPKI　電子証明書発行サービス」クライアント証明書配布開始にともない制定
1.1	2018/7/9	NII の CP/CPS 改訂のうち、ST フィールドを定めることに対応するために記述を追加
1.2	2018/12/7	S/MIME証明書プロファイルに関する記述を追加

1　はじめに

本文書は、「国立情報学研究所オープンドメイン認証局 証明書ポリシ（Certificate Policy）」(OID=1.3.6.1.4.1.32264.3.2.1.1)（以下「元CP」という。）の定めるところに従って実施されるクライアント証明書の発行業務の一部を国立大学法人東京大学（以下「東大」という。）で運用するための運用ポリシーと運用規則を定めるものである。本文書は東大における運用ポリシーのみを記述し、元CP の補足文書として扱われるべきものである。また、本文書にしたがって運用される局は、PKI の用語でいうLRA とは厳密にいって異なる可能性を持つものである。このような事情に鑑み、本文書はたとえばRFC3647　で定めるような標準的なCP/CPS の記述形式をとらず、運用ポリシーとして必要な部分だけに関する記述のみを与えることにする。

クライアント証明書の発行は、国立情報学研究所（以下NII という）の事業「電子証明書発行サービス」として実施されている。東大側での対応部署は、情報基盤センターである。本文書が元CP に抵触する場合は元CP、本文書の順に適用されるものとする。元CP が東京大学情報セキュリティ・ポリシーに抵触されると判断した場合は、東京大学情報セキュリティ・ポリシーを優先する。

1.1　文書の名前と識別

本文書の名称は「国立情報学研究所クライアント証明書発行サービスの運用において東京大学からの申請を処理するための局の運用ポリシーおよび運用規則」とする。本文書の版は 1.2 である。識別子としての OID は取得しない。

1.2　関係者

1.2.1　認証局

元 CP に定める通りとする。

1.2.2 東大登録局 (TRA)

東大登録局（以下 TRA という）は、認証局に対し、証明書の発行、失効申請することを承認した者（以下承認者という）の実在性確認、本人性確認の審査及び証明書を発行、失効するための東大側における承認と代理申請の業務等を行う。TRA の行う「承認」と「代理申請」は、元 CP と適合する。

1.2.3 東大部局登録局 (TLRA)

東大部局登録局（以下 TLRA という）を、東大のそれぞれの部局または部局に相当する組織に対しておくことがある。TLRA は、TRA に対し、証明書の発行、失効申請することを承認した者（以下承認者という）の実在性確認、本人性確認の審査及び証明書を発行、失効するための部局内における承認と申請業務等を行う。TLRA の行う「承認」と「申請」は、元 CP の意味では使わず、TRA に対するものとしてそれぞれ使用する。

1.2.4 東大加入者

東大加入者とは、元CP にいう加入者または加入者になるべくクライアント証明書およびS/MIME証明書の発行を申請しようとする者とする。東大加入者は東大の教職員または学生でなければならない。

1.2.5 UTNET

UTNET とは、東大におけるキャンパスネットワークのことである。本文書では、そのUTNET 基幹部の管理主体としての組織も UTNET ということにする。

1.3 ポリシー管理

本ポリシーを管理する組織および本文書に対する問合せ先は以下のとおりである。

東京都文京区弥生 2-11-16
東京大学情報基盤センター
メールアドレス：PublicServerCertificates@itc.u-tokyo.ac.jp

2 識別および認証

2.1 名前決定

元CP に定めるものであるが、本文書で扱うクライアント証明書およびS/MIME証明書では特に次のものに制限して使用する。

2.1.1 クライアント証明書

- 「都道府県名」（ST）は原則 Tokyo とする。ただし、勤務場所を反映する ST を利用することを認めることがある。
- 「組織名」(O) は The University of Tokyo とする。
- 「組織単位名」(OU) は審査を委譲された TLRA の定める名称とする。最上位階層のOUは、TLRA設置時に届け出るものとし、その下に複数指定することができる。更に、TRA および認証局が認めた場合は、「空白」とすることもできる。
- 「コモンネーム」(CN) は、共通IDの下10桁を設定する。

2.1.2 S/MIME証明書

- 「都道府県名」（ST）は原則 Tokyo とする。ただし、勤務場所を反映する ST を利用することを認めることがある。
- 「組織名」(O) は The University of Tokyo とする。
- 「組織単位名」(OU) は審査を委譲された TLRA の定める名称とする。最上位階層のOUは、TLRA設置時に届け出るものとし、その下に複数指定することができる。更に、TRA および認証局が認めた場合は、「空白」とすることもできる。また、同姓同名の構成員がいる場合は係名英字を含めて識別可能とする。
- 「コモンネーム」(CN) は、利用者氏名英字、もしくは組織内の部門名英字とする。

  利用者氏名英字の例） TODAI Taro もしくは Taro Todai
  部門名英字の例） Accounting Section、General Affairs Sectionなど

- S/MIME証明書プロファイルでは主体者別名（subjectAltName）として RFC822Name に使用するメールアドレスを記載する。
- 前項で使用するメールアドレスは、TLRA が届け出たドメイン名で終わるものに限る。ただし、ドメイン名が u-tokyo.ac.jp で終わる全学メールアドレスを使うこともできる。

2.2 初回の識別と認証

TLRA を部局または部局に相当する組織で組織する場合、実在する UTNET 部局担当者で組織されていることを、情報基盤センターで管理するUTNET の名簿で、各TLRA の権限の範囲を含めて確認する。

具体的な確認事項は運用規則で定める。

3 TRAで行う審査と承認

TRA は、以下について審査を行い、すべてを満たした場合申請を承認し、代理申請を行う。

1. 申請者の本人確認と申請する部局及びその下の組織に対する権限確認の審査
2. NIIに申請済みのドメインであることの審査
3. S/MIME証明書の場合は、申請メールアドレスが本人へ到達可能であることの証明

4 審査の TLRAへの委譲

TRA はTLRA に上記審査を委譲する。TRA は、以下の審査を行い、申請を承認し、代理申請を行う。

1. TLRA の申請が、当該部局及びその下の組織に属し、部局の権限の及ぶ範囲内であることの審査

5 運用の統制

5.1 手続的管理

TRA は、情報基盤センターで以下のように組織する。

- TRA 責任者は NII に届け出る機関責任者と同一とする。
- TRA 担当者は NII に届け出る登録担当者と同一とする。

TRA 責任者と TRA 担当者を合わせた異なりの数は 2 名以上とする。

TLRA は、各部局または部局に相当する組織で以下のように組織し、TRA の認証を受けるものとする。

- TLRA 責任者はUTNET 部局担当者とする。ただし、その所属部局の長から指名されたものに代えることができる。

5.2 記録管理

すべての記録は帳票として保存する。保存期間は運用規則に定める。

5.3 TRA の終了

TRA は、任意の時点でその業務を終了することができる。業務を終了する場合、東大加入者および NII に公表し、運用規則に定める処理を行う。TRA の業務が終了した時点でTLRA の業務も終了する。終了した場合の記録の保管については運用規則に定める。

5.4 内部検査

TRA は、TLRA の運用が適正に行われているかの検査を定期的、不定期的に行う。

5.5 課金

証明書発行に関係する課金については別に定める。

5.6 ビジネス・法的問題

TRA は、元CP に定める以外の事柄については定めない。クライアント証明書の発行に当たり、いかなる事項においても、法令および東大の規則に別に定める場合をのぞき、TRA、TLRA、東大加入者はいずれも懲戒の対象にはならない。

TRA および TLRA の運用規則

1 はじめに

TRA は TRA の運用が、元CP に適合するように努力を払う。

2 TRA の審査

TRA はクライアント電子証明書発行に当たっての審査は以下のように行う。

東大加入者の本人確認 東大加入者が東大の教職員であることを、東大総長の発行する職員証によって目視で確認することで審査する。

3 TLRA の開設にあたっての審査

TRA は、部局、または部局に相当すると認めた組織が TLRA を開設し、TRA が行う審査と承認の委譲を申請するに当たって、認証を行う。認証は以下のように行う。

部局がそこに属する東大加入者を統制できる体制にあることの審査 UTNET 部局担当者のUTNET への届出書類、または担当者を部局長が指名したことを証明する文書を確認することで審査する。

TLRA が、上の認証を受けた場合、TRA はその結果をTLRA に通知し、関係する審査と承認を委譲する。

4 TLRA の運用変更

TLRA は、TRA に運用の変更を申し出ることができる。TRA は、申し出にもとづき速やかに審査を行う。

5 内部検査

内部検査は、TLRA の直近の運用が、申し出通り行われているかどうかにつき、TLRA からの証拠文書と、場合によっては面接により検査する。検査は最低年一回実施する。

6 記録

すべての審査および承認は帳票による記録を行う。TLRA の開設、運用変更にあたっての審査および内部検査の記録は、TRA の運用期間終了日に 90 日を加えた期日まで保存する。サーバ証明書の申請に関する記録は取得サーバ証明書の有効期限に 90 日を加えた期日まで保存する。

以上