国立情報学研究所電子証明書発行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 2.0

東京大学情報基盤センター

2016 年 3 月 23 日

バージョン	日付	適用
国立情報学研究所オープンドメイン認証局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		
1.00	2007/03/30	「サーバ証明書発行・導入の啓発・評価プロジェクト」参加準備のために制定
1.01	2007/05/11	「サーバ証明書発行・導入の啓発・評価プロジェクト」正式参加にともない改版
2.0	2009/06/26	「UPKI オープンドメイン証明書自動発行検証プロジェクト」参加にともない改版
国立情報学研究所電子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	2015/1/26	NII「UPKI 電子証明書発行サービス」参加にともない NII の事業名と東大側の実施主体の変更を上記文書に反映させて制定
2.0	2016/3/23	TLRA の適用範囲を部局等に拡大し、さらに u-tokyo.ac.jp 以外のドメインに対する電子証明書発行に対応するため、さらに課金に対応するために改版

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 とよぶ）の定めるところに従って実施されるサーバ証明書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。

サーバ証明書の発行は、国立情報学研究所（以下 NII という）の事業「UPKI 電子証明書発行サービス」として実施されている。東京大学側での対応部署は、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 UPKI 電子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 1.0 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東京大学ドメイン名運用規則によって認められたドメインを運用管理し、かつ元 CP の条件が満たされると TRA および認証局が判断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サーバ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、本文書で扱うものとして特に次のものに制限して使用する。

- 「組織名」(O) は The University of Tokyo とする。

- 「組織単位名」(OU) は原則として、東大加入者が属し、かつ元 CP の条件を満たす部局の名称とする。ただし、東京大学ドメイン名運用規則によって認められたドメインを運用管理し、かつ元 CP の条件が満たされると TRA および認証局が判断する組織の名称とすることもできる（以下、これらの組織と部局を総称して「部局等」と呼ぶ）。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、u-tokyo.ac.jp の下にある FQDN とする。ただし、TLRA はそれ以外のドメイン下にある FQDN をあらかじめ届け出ることにより使用することができる。

2.2 初回の識別と認証

TLRA を部局で組織する場合、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。

部局ではない組織に対して TLRA を設置する場合は、その組織が部局の管理下のもとで安定して運用されていることを確認する。

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サーバに対する権限確認の審査
2. サーバの属するドメインの統制が取れていることの審査

4 審査の TLRA への一部委譲

TRA は TLRA に上記審査の一部を委譲することがある。委譲する項目については、TLRA ごとに定める。この場合、TRA は、以下の審査を行い、申請を承認し、代理申請を行う。

1. 委譲をしない部分についての審査
2. TLRA の申請が、当該部局に属し、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。サーバ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 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。

東大加入者の権限確認 東大加入者が当該ドメインにサーバを設置でき、かつその運用に責任をもつことを、本人の自署または押印のある申請書によって審査する。申請書は FQDN を含むものとする。審査にあたって、必要に応じて面接を行い、その記録を保存する。

ドメインの統制の確認 ドメイン内の名前付けがその部署の意思を正しく反映できる体制であることを、DNS の管理体制についての文書または面接により審査する。承認は TRA 責任者が行う。承認の結果は帳票として保存する。

3　TLRA の開設にあたっての審査

TRA は、部局等が TLRA を開設し、TRA が行う審査と承認の全部または一部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。

部局等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 の審査体制の構築に関する審査 TLRA が本人確認にあたって TRA と同等の質の審査体制を構築しているかを、関連する文書の提出により審査する。

部局が東大加入者の属するドメインを統制できる体制にあることの審査 UTNET 部局担当者の属するドメインが部局に割り当てられたものであることを UTNET の発行した文書により確認する。ドメインが UTNET 外のものである場合、部局がその意思で当該ドメインを管理運用していることを証明する文書により確認する。さらに、自ドメインおよび支配下におくサブドメインについて、名前付けがその部署の意思を正しく反映できる体制にあるかどうかを審査できることを、IP アドレスの管理体制および DNS の管理体制についての文書により確認する。

TLRA が、上の認証を全部または一部で受けた場合、TRA はその結果を TLRA に「制限なし委譲」または「制限つき委譲」として通知し、関係する審査と承認を委譲する。制限つき委譲の通知の場合は、委譲する範囲を明確に指定する。

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