UPKI オープンドメイン証明書自動発行検証プロジェクトサーバ証明書利用に係る申合せ

（平成２１年４月１日
学術情報ネットワーク運営・連携本部決定）

１．（概要）

国立情報学研究所（以下「研究所」という。）　学術情報ネットワーク運営・連携本部認証作業部会（以下「部会」という。）が実施する「UPKI オープンドメイン証明書自動発行検証プロジェクト」（以下「本プロジェクト」という。）では，国立情報学研究所 オープンドメイン認証局 2（以下「オープンドメイン認証局 2」という。）を運用し，本プロジェクト参加機関のサーバに対してサーバ証明書の発行を行うこととする。

この UPKI オープンドメイン証明書自動発行検証プロジェクトサーバ証明書利用についての申合せ（以下「本申合せ」という。）は，オープンドメイン認証局 2 が発行するサーバ証明書を信頼し，検証する者（以下「利用者」という。）が，サーバ証明書を利用するために必要な事項を定める。

２．（サーバ証明書の目的）

利用者は，サーバ証明書を信頼し，検証することによって，サーバ証明書がインストールされているサーバとの通信において，所定の方法による暗号化通信及びサーバの実在性確認に利用することができるものとする。他の用途にサーバ証明書を使用した場合，部会はサーバ証明書の有効性について一切の責任を負わないものとする。

３．（認証局）

オープンドメイン認証局 2 は，部会が運用し，上位の認証局として WebTrust for CA 規準の認定を取得したセコムトラストシステムズ(株)の「Security Communication Root CA1」（以下「ルート認証局」という。）から，下位認証局証明書（以下「CA 証明書」という。）の発行を受けている。

４．（同意事項）

利用者は以下に定める同意事項の内容が適用されることを確認します。ただし，同意事項の内容と本申合せの定めが異なる場合は，本申合せの定めが優先して適用されるものとする。

・同意事項

①「UPKI オープンドメイン証明書自動発行検証プロジェクトサーバ証明書利用についての申合せ」（本申合せ）

②「国立情報学研究所オープンドメイン認証局 2　証明書ポリシ（Certificate Policy）」（以下「CP」という。）

③「セコム電子認証基盤認証運用規程（Certification Practice Statement）」（以下「CPS」

という。）

・上記同意事項を確認できる URL
①本申合せ　：https://repo1.secomtrust.net/sppca/nii/odca2/index.html
②CP　　：https://repo1.secomtrust.net/sppca/nii/odca2/index.html
③CPS　　：https://repo1.secomtrust.net/spcpp/cps/index.html

５．（対応サーバ及び推奨ブラウザ）
オープンドメイン認証局 2 で発行される証明書の対応するサーバを以下に掲載することとする。また，当該サーバと所定の方法による暗号化通信を実現する推奨ブラウザを以下に掲載することとする。
・上記対応サーバ及び推奨ブラウザが確認できる URL
https://upki-portal.nii.ac.jp/docs/odcert

６．（リポジトリの利用）
①利用者は，証明書の検証を行う際に，オンラインによって閲覧できる以下のリポジトリを参照すること。
https://repo1.secomtrust.net/sppca/nii/odca2/index.html
②リポジトリ上には，CA 証明書およびそのハッシュ値，証明書失効リスト（以下「CRL」という。），CP 及び CPS，本申合せを公開し，２４時間３６５日利用可能としています。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。
③オープンドメイン認証局 2 は通常 72 時間ごとに新たな CRL を発行し，リポジトリ上に公開する。また，証明書の失効が行われた場合は，すみやかに新たな CRL を発行し，その都度リポジトリ上に公開するものとする。

７．（証明書検証）
利用者は，サーバ証明書を利用する際に，サーバ証明書の他，サーバ証明書の発行者であるオープンドメイン認証局 2 の CA 証明書の有効性を以下の方法により確認しなければならない。なお，確認の対象となるサーバ証明書と CA 証明書をあわせて本条では単に「証明書」とする。
①利用者は，サーバ証明書がオープンドメイン認証局 2 により電子署名されていること及びサーバ証明書が改ざんされていないことを確認しなければならない。
②利用者は，CA 証明書がルート認証局により電子署名されていること及び CA 証明書が改ざんされていないことを確認しなければならない。
③利用者は，証明書を信頼すべきか否かの判断をするときは，発行者証明書の公開鍵を用いて，当該証明書に行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

確認しなければならない。

④利用者は，証明書を信頼すべきか否かの判断をするときは，当該証明書の利用目的もしくは使用範囲またはその制限を確認しなければならない。

⑤利用者は，証明書を信頼する前に，その証明書が失効されていないことを CRL によって確認しなければならない。

⑥利用者は，証明書を信頼する前に，適切な手段により，その証明書の有効期間を確認しなければならない。

８．（再委託）

部会は，認証局運用の全部または一部を部会の責任で第三者に委託することができるものとする。

この場合，部会は，当該第三者に対し，本申合せに基づき部会が利用者に対して負う義務と同等の義務を遵守させるものとし，当該第三者の認証局運用に関し，利用者に対し責任を負うものとする。

９．（本申合せの変更）

部会は，利用者に事前に通知することなく合理的な範囲で，本申合せの内容を変更できるものとする。本申合せは，変更後速やかにリポジトリ上で公開するとともに，公開を以て新しい申合せを適用するものとする。

１０．（免責）

加入者が本申合せを遵守していたにもかかわらず，本プロジェクトが発行した証明書に起因して発生した損害に対する本プロジェクトの賠償責任について，部会は，証明書を無償で提供していることから，本プロジェクトに関連して発生するいかなる間接損害，特別損害（かかる損害発生の可能性につき部会が現実に予見し，または予見し得た場合を含む），付随的損害または派生的損害に対する責任を負わないものとする。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もしくは派生的損害に対する責任を負わないものとする。ただし，部会に故意または重大な過失がある場合は，法律上認められる範囲の責任を負う場合がある。

１１．（準拠法および管轄裁判所）

オープンドメイン認証局 2，加入者及び利用者の所在地にかかわらず，本申合せ，CP 及び CPS の解釈，有効性及び本プロジェクト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し，仲裁及び裁判地は，東京地方裁判所を第一審の専属的合意管轄裁判所とする。

１２．（協議事項）

本申合せの取り決めについて疑問が生じた場合，または本申合せに取り決めのないことについては，利用者，部会が誠意を持って協議し，これを解決するものとする。

附　則

この申合せは，平成２１年４月１日から実施する。