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

第 2.85 版

令和 2 年 12 月 25 日

改版履歴		
版数	日付	内容
1.00	2015.01.01	初版発行
2.00	2015.04.01	クライアント証明書、S/MIME 証明書、コード署名用証明書のサービスを追加 用語の統一
2.10	2016.03.14	OCSP の提供について説明を追記 システム用 S/MIME 証明書プロファイルを追加 証明書の利用者条件の追記 クライアント証明書の用途の追記 誤植の修正
2.20	2016.12.20	認証局「NII Open Domain S/MIME CA」の追加 システム用 S/MIME 証明書プロファイルの変更 誤植の修正
2.30	2017.02.28	コード署名用証明書プロファイルの変更 OCSP の提供について説明を修正 OCSP サーバ証明書プロファイル「NII Open Domain Code Signing CA - G2」を追加
2.40	2017.09.08	CAA レコードに関する記述を追加
2.50	2018.02.26	認証局「NII Open Domain CA - G3」の削除 認証局「NII Open Domain Code Signing CA」の削除 クライアントおよび S/MIME 証明書有効期間の変更 OCSP サーバ証明書プロファイル「NII Open Domain CA - G3」の削除 CRL のプロファイル「NII Open Domain CA - G3」と「NII Open Domain Code Signing CA」の削除
2.60	2018.03.26	認証局「NII Open Domain CA - G5」の追加 認証局「NII Open Domain CA - G6」の追加 定義と略語に ECDSA を追加 相互運用の基準に Security Communication ECCRootCA1 を追加 サーバ証明書プロファイル「NII Open Domain CA - G5」と「NII Open Domain CA - G6」を追加 OCSP サーバ証明書プロファイル「NII Open Domain CA - G5」と「NII Open Domain CA - G6」を追加 サーバ証明書の証明書発行要求（CSR）プロファイル「NII

		Open Domain CA - G5」と「NII Open Domain CA - G6」を追加
2.70	2018.07.09	定義と略語に ECC と Secp384r1 と SHA-384 を追加 本 CA が発行する証明書の情報の修正 名前が意味を持つことの必要性の修正 サーバ証明書プロファイル「NII Open Domain CA - G5」、 サーバ証明書プロファイル「NII Open Domain CA - G6」の修正 クライアント証明書プロファイル「NII Open Domain CA - G4」の修正 S/MIME 証明書プロファイル「NII Open Domain S/MIME CA」の修正 サーバ証明書の証明書発行要求（CSR)プロファイル「NII Open Domain CA - G5」、 サーバ証明書の証明書発行要求（CSR)プロファイル「NII Open Domain CA - G6」の修正 コード署名用証明書の証明書発行要求（CSR）プロファイルの修正 現在有効なプロファイルを追記 誤植の修正
2.80	2019.03.15	鍵の使用目的の修正 サーバ証明書プロファイル「NII Open Domain CA - G6」の修正
2.81	2020.03.30	サーバ証明書プロファイル「NII Open Domain CA - G5」の修正 サーバ証明書プロファイル「NII Open Domain CA - G6」の修正 表 7-1-5-3 S/MIME 証明書の URL を修正 クライアント証明書を個人認証用証明書に記載変更 本 CA のシステムへアクセスする際に用いる証明書名をク

		ライアント証明書からクライアント認証用証明書に記載変更 NII Open Domain の CA 名に含まれるハイフンの表記ゆれ修正 誤植の修正
2.82	2020.06.09	コード署名用証明書のサービスを削除 「Baseline Requirements」の章立てに合わせるための修正
2.83	2020.08.25	サーバ証明書の有効期間を変更
2.84	2020.10.15	CRL の Reason Code を修正
2.85	2020.12.25	各証明書のプロファイルに発行終了日を記載

－目　次－

1. はじめに

1.1 概要

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（以下「本 CP」という）は、大学共同利用機関法人　情報・システム研究機構　国立情報学研究所（以下「NII」という）が運用する国立情報学研究所オープンドメイン認証局 NII Open Domain CA - G4、NII Open Domain CA - G5、NII Open Domain CA - G6 及び NII Open Domain S/MIME CA（以下、「本 CA」という）が発行する証明書の利用目的、適用範囲、利用申請手続を示し、証明書に関するポリシを規定するものである。本 CA は、セコムトラストシステムズ株式会社のプライベート CA サービスを利用し、RA 業務を NII が担う。
運用維持に関する諸手続については、セコム電子認証基盤認証運用規程（以下、「CPS」という）に規定する。
NII Open Domain CA - G4 、NII Open Domain CA - G5 及び NII Open Domain S/MIME CA には、Security Communication RootCA2 より、片方向相互認証証明書が発行されている。NII Open Domain CA - G6 には、Security Communication ECCRootCA1 より、片方向相互認証証明書が発行されている。
本 CA から証明書の発行を受ける者は、証明書の発行を受ける前に自己の利用目的と本 CP、CPS とを照らし合わせて評価し、本 CP 及び CPS を承諾する必要がある。
なお、本 CP の内容が CPS の内容に抵触する場合は、本 CP、CPS の順に優先して適用されるものとする。また、NII と契約関係を持つ組織団体等との間で、別途規程等が存在する場合、本 CP、CPS より規程等の文書が優先される。

本 CA は、CA/Browser Forum が https://www.cabforum.org/で公開する「Baseline Requirements」に準拠している。

本 CP は、本 CA に関する技術面、運用面の発展や改良に伴い、それらを反映するために必要に応じ改訂されるものとする。

本 CP は、IETF 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」に準拠している。

1.1.1 証明書の種類

本 CA が発行する証明書は以下のとおりである。

CA 名称	証明書の種類
NII Open Domain CA - G4	サーバ証明書 sha256WithRSAEncryption (Certificate

	Transparency 非対応) 個人認証用証明書 S/MIME 証明書 OCSP サーバ証明書
NII Open Domain CA - G5	サーバ証明書 sha256WithRSAEncryption OCSP サーバ証明書
NII Open Domain CA - G6	サーバ証明書 ecdsa-with-SHA384 OCSP サーバ証明書
NII Open Domain S/MIME CA	S/MIME 証明書

1.1.2 身元確認レベル

本 CA は、以下の確認を行う。

証明書の種類	確認内容
サーバ証明書	サービス利用機関の実在性 サービス利用機関で取り扱うドメインの実在性 登録担当者の本人性
個人認証用証明書	サービス利用機関の実在性 登録担当者の本人性
S/MIME 証明書	サービス利用機関の実在性 サービス利用機関で取り扱うドメインの実在性 登録担当者の本人性

本 CA は、以下の確認を直接行わずに申請する機関あるいはその登録担当者に委任する。

証明書の種類	確認内容
サーバ証明書	サービス利用機関で取り扱うドメインの本人性 利用管理者及び利用者の実在性、本人性 サーバの実在性
個人認証用証明書	利用管理者及び利用者の実在性、本人性
S/MIME 証明書	サービス利用機関で取り扱うドメインの本人性 利用管理者及び利用者の実在性、本人性

1.2 文書の名前と識別

本 CP の正式名称は、「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」という。

本 CP には、登録された一意のオブジェクト識別子（以下、「OID」という）が割り当てられている。本 CP の OID 及び参照する CPS の OID は以下のとおりである。

CP/CPS	OID
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（CP）	1.3.6.1.4.1.32264.3.2.1.1
セコム電子認証基盤認証運用規程（CPS）	1.2.392.200091.100.401.1

1.3 PKI の関係者

1.3.1 認証局（CA）

CA（Certification Authority：認証局）とは、IA（Issuing Authority：発行局）及び RA（Registration Authority：登録局）によって構成される。IA は、証明書の発行、失効、CRL（Certificate Revocation List：証明書失効リスト）の開示、OCSP（Online Certificate Status Protocol）サーバによる証明書ステータス情報の提供等を行う。

本 CA は CA の運営主体で定める CP、CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部又は全部を外部に委託することができる。

1.3.2 登録局（RA）

RA は、サービス利用機関の実在性、機関で扱うドメインの実在性、登録担当者の本人性確認を行う。

また、証明書の発行、失効申請及び更新申請する登録担当者の本人性確認及び証明書を発行、失効するための登録業務等を行う。

なお、RA が利用管理者及び利用者の実在性及び本人性を確認できる場合は、利用管理者から直接申請を受けることもできる。

1.3.3 利用管理者・利用者

1.3.3.1 利用管理者

利用管理者とは、NII が定める各種規定に合意し、本 CA より発行される証明書を所有し、証明書に記載された公開鍵と対になる秘密鍵を管理する人、組織をさす。
利用管理者は、本 CP 及び CPS の内容を承諾した上で、登録担当者を介して証明書の発行申請を行うものとする。

利用管理者の範囲は次のとおりとする。

- 教員、職員等の学術機関に所属する者であり、本 CA 又は登録担当者が本人性及び実在性を確認できる者
- 学術機関と何らかの契約関係にある等、学術機関に所属する者が当該利用管理者の実在性、本人性を確認できる者

1.3.3.2 利用者

利用者とは、本 CA より発行される証明書を所有し、証明書に記載された公開鍵と対になる秘密鍵を管理する人、組織をさす。
利用者の範囲は次のとおりとする。

- 学術機関に所属する者
- 学術機関が認めた役職、組織（係、班や課などを単位とするもの）
- 学術機関が認めた、業務上証明書が必要な者

1.3.4 検証者

検証者とは、本 CP 及び CPS を信頼し、利用管理者及び利用者の証明書を検証する者又はコンピュータシステムをさす。

1.3.5 その他関係者

1.3.5.1 サービス利用機関

サービス利用機関とは、NII が別に定める機関の要件を満たし、本 CA から事前の確認を受けた組織をさす。

1.3.5.2 登録担当者

登録担当者は、本 CA が発行する証明書の利用管理者からの申請において、利用管理

者及び利用者の本人性、実在性を確認する者をさす。登録担当者は、利用管理者からの依頼にもとづいて申請をすることができる。

1.4 証明書の使用方法

1.4.1 適切な証明書の使用

本 CA が発行する証明書は、次の目的として利用することができる。

証明書の種類	証明書の用途
サーバ証明書	本 CP 及び NII が別に定める手続きにもとづき、実在性が確認された人又は組織に対し、以下の用途として証明書が発行される。 ・サーバ認証 ・通信経路でのデータ暗号化
個人認証用証明書	本 CP 及び NII が別に定める手続きにもとづき実在性が確認された人又は組織に対し、以下の用途として証明書が発行される。 ・クライアント認証 ・Web サイトのアクセス制御 ・データファイルへの電子署名 ・証明書を利用するシステムの動作試験
S/MIME 証明書	本 CP 及び NII が別に定める手続きにもとづき実在性が確認された人又は組織に対し、以下の用途として証明書が発行される。 ・クライアント認証 ・Web サイトのアクセス制御 ・データファイルへの電子署名 ・電子メールへの電子署名及び電子メールの暗号化
OCSP サーバ証明書	本 CP が定める証明書のステータス情報をリアルタイムに提供するため、以下の用途として証明書が発行される。 ・OCSP による失効検証

1.4.2 禁止される証明書の使用

本 CA が本 CP に基づき発行する証明書は、本 CP「1.4.1 適切な証明書の使用」に記載する目的以外で利用してはならない。

1.5 ポリシ管理

1.5.1 本ポリシを管理する組織

本 CP の維持、管理は、NII が行う。

1.5.2 問い合わせ先

本 CP に関する連絡先は、次のとおりである。

名称：大学共同利用機関法人　情報・システム研究機構　国立情報学研究所

住所：〒101-8430　東京都千代田区一ツ橋 2 丁目 1 番 2 号

　　学術基盤推進部 学術基盤課

TEL：03-4212-2218

メールアドレス：certs@nii.ac.jp

1.5.3 CP のポリシ適合性を決定する者

本 CP の内容について、NII が適合性を決定する。

1.5.4 CP 承認手続き

本 CP は、NII の承認によって発効される。

1.6 定義と略語

＜A～Z＞

・ CA（Certification Authority）：認証局

証明書の発行・更新・失効、CA 秘密鍵の生成・保護、利用管理者及び利用者の登録等を行う主体のことをいう。

・ CAA (Certification Authority Authorization)

ドメインを使用する権限において、DNS レコードの中にドメインに対して証明書を発行できる認証局情報を記述し、意図しない認証局からの証明書発行を防ぐ機能のことをいう。本機能は RFC6844 で規定されている。

・ CP/CPS（Certificate Policy：証明書ポリシ/Certification Practices Statement：認証実施規程）

CP ：CA が証明書を発行する際の運用方針を定めた文書。

CPS：CA の信頼性、安全性を対外的に示すために、CA の運用、証明書ポリシ、鍵の生成・管理、責任等に関して定めた文書。証明書ポリシが何を運用方針にするのかを示すのに対して、認証実施規程は運用方針をどのように適用させるのかを示す。

・ CRL（Certificate Revocation List）：証明書失効リスト

証明書の有効期間中に、証明書記載内容の変更、秘密鍵の紛失等の事由により失効された証明書情報が記載されたリストのことをいう。

・ ECC (Elliptic Curve Cryptography)

楕円曲線暗号のこと。楕円曲線上の離散対数問題（EC-DLP）の困難性を安全性の根拠とする暗号のことをいう。

・ ECDSA（Elliptic curve digital signature algorithm）

楕円曲線電子署名アルゴリズムのことをいう。RSA よりも短い鍵長で同等の安全性を持つ。

・ FIPS140-2

米国 NIST（National Institute of Standards and Technology）が策定した暗号モジュールに関するセキュリティ認定基準のこという。最低レベル 1 から最高レベル 4 まで定義されている。

・ FQDN（Fully Qualified Domain Name）

ホスト名からドメイン名までを省略なしに完全に指定した形式。例えば、ホスト名が「www」、ドメイン名が「nii.ac.jp」である場合、FQDN は「www.nii.ac.jp」となる。

・ HSM（Hardware Security Module）

秘密鍵の生成、保管、利用などにおいて、セキュリティを確保する目的で使用する耐タンパー機能を備えた暗号装置のことをいう。

・ IA（Issuing Authority）：発行局

CA の業務のうち、証明書の発行・更新・失効、CA 秘密鍵の生成・保護、リポジトリの維持・管理等を行う主体のことをいう。

・ OCSP（Online Certificate Status Protocol）

証明書のステータス情報をリアルタイムに提供するプロトコルのことをいう。

・ OID（Object Identifier）：オブジェクト識別子

ネットワークの相互接続性やサービス等の一意性を維持管理するための枠組みであり、国際的な登録機関に登録された、世界中のネットワーク間で一意となる数字のことをいう。

・ PKI（Public Key Infrastructure）：公開鍵基盤

電子署名、暗号化、認証といったセキュリティ技術を実現するための、公開鍵暗号方式という暗号技術を用いる基盤のことをいう。

・ RA（Registration Authority）：登録局

CA の業務のうち、申込情報の審査、証明書発行に必要な情報の登録、IA に対する証明書発行要求等を行う主体のことをいう。

・ RFC3647（Request For Comments 3647）

インターネットに関する技術の標準を定める団体である IETF（The Internet Engineering Task Force）が発行する文書であり、CP/CPS のフレームワークを規定した文書のことをいう。

・ RSA

公開鍵暗号方式として普及している最も標準的な暗号技術のひとつである。

・ Secp384r1

ECC で利用する楕円曲線のひとつであり、公開鍵 384 ビットで利用する。

・ SHA-1（Secure Hash Algorithm 1）

電子署名に使われるハッシュ関数（要約関数）のひとつである。生成するハッシュ値のビット長は 160 ビットである。

・ SHA-256（Secure Hash Algorithm 256）

電子署名に使われるハッシュ関数（要約関数）のひとつである。生成するハッシュ値のビット長は 256 ビットであり、SHA-1 よりも高い強度を持つ。

・ SHA-384 (Secure Hash Algorithm 384)

電子署名に使われるハッシュ関数（要約関数）のひとつである。生成するハッシュ値のビット長は、384 ビットであり、SHA-256 よりも高い強度を持つ。

＜あ～ん＞

・ アルゴリズム
計算や問題を解決するための手順、方式。

・ アーカイブ
法的又はその他の事由により、履歴の保存を目的に取得する情報のことをいう。

・ 鍵ペア
公開鍵暗号方式において、秘密鍵と公開鍵から構成される鍵の対のことをいう。

・ 監査ログ
CA システムへのアクセスや不正操作の有無を検査するために記録される CA システムの動作履歴やアクセス履歴等をいう。

・ 公開鍵
公開鍵暗号方式において用いられる鍵ペアの一方をいい、秘密鍵に対応し、通信相手の相手方に公開される鍵のことをいう。

・ サーバの実在性
サーバの管理責任及びドメインの実在性について、NII が別に定めるサーバとしての要件を満たすものであること。

・ サーバの本人性
サーバの鍵ペアのうち秘密鍵が外部へ漏れないよう利用管理者及び利用者が管理していること。

・ サービス利用機関の実在性
サービス利用機関が、NII が別に定めるサービス利用機関としての要件を満たすものであること。

・ タイムスタンプ
電子ファイルの作成日時やシステムが処理を実行した日時等を記録したデータのことをいう。

・ 電子証明書

ある公開鍵を、記載された者が保有することを証明する電子データのことをいう。CA が電子署名を施すことで、その正当性が保証される。

・ 登録担当者の実在性

当該サービス利用機関のサーバの発行・失効・更新にかかる申請を行うものとして、NII が別に定める手続きに従い、機関責任者に任命されたものであること。

・ 登録担当者の本人性

証明書の発行・失効・更新にかかる申請が、間違いなく登録担当者によって行われたものであること。

・ ドメインの実在性

ドメインが、NII が別に定めるドメインとしての要件を満たすものであること。

・ ドメインの本人性

サービス利用機関が取り扱うドメイン名を使用することについて、当該ドメイン登録担当者の合意が得られていること。

・ ハッシュ関数

与えられた原文から固定長のビット列を生成する演算手法をいう。

データの送信側と受信側でハッシュ値を比較することで、通信途中で原文が改ざんされていないかを検出することができる。

・ 秘密鍵

公開鍵暗号方式において用いられる鍵ペアの一方をいい、公開鍵に対応する本人のみが保有する鍵のことをいう。

・ プライベート CA サービス

セコムトラストシステムズが提供する認証サービスの名称のことをいう。

・ リポジトリ

CA 証明書及び CRL 等を格納し公表するデータベースのことをいう。

・ 利用管理者の実在性

NII が別に定める利用管理者及び利用者としての要件を満たすものであること。

・ 利用管理者の本人性

NII が別に定める各種規程に合意していること、及び登録担当者への申請が間違いなく利用管理者自身によるものであること。

2. 公開及びリポジトリの責任

2.1 リポジトリ

本 CA は、リポジトリを 24 時間 365 日利用できるように維持管理を行う。また、証明書ステータス情報を 24 時間 365 日利用できるように OCSP サーバの維持管理を行う。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 認証情報の公開

本 CA は、CA 証明書及びそのハッシュ値、証明書失効リスト（以下「CRL」という）、本 CP 及び CPS をリポジトリ上に公開し、利用管理者、利用者及び検証者がオンラインによって閲覧できるようにする。また、本 CA は、サーバ証明書のステータス情報を OCSP サーバにより利用管理者、利用者及び検証者がオンラインによって参照できるようにする。なお、その他の証明書は OCSP サーバによるステータス情報の提供を行わない。

2.3 公開の時期又はその頻度

本 CA は、通常 24 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、新たな CRL を発行し、発行の都度、リポジトリ上に公開する。

本 CP 及び CPS は、改訂の都度、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

利用管理者、利用者及び検証者は、リポジトリでの公開情報に関して随時、リポジトリを参照することができる。リポジトリへのアクセスは、一般的な Web インターフェースを通じて可能であり、公開する情報に対し、特段のアクセス制御は行わない。

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主体者の名前は、ITU-T X.500 シリーズの識別名の形式に従って設定する。

本 CA が発行する証明書には下記の情報を含むものとする。

(1)サーバ証明書（NII Open Domain CA - G4）

1.「国名」（C）は JP とする。
2.「都道府県」（ST）は使用しない。
3.「場所」（L）は Academe とする。
4.「組織名」（O）とは、利用管理者及び利用者が所属し、サブジェクトに記載されたサーバを管理する主体となる組織とし、原則として事前に RA に登録したサービス利用機関名(英語表記)を用いる。
5.「組織単位名」（OU）は、任意選択の記入欄とする。OU の欄は、組織内のさまざまな部門等（例えば、工学部、理学部、法学部の各学部）を区別するために使用する。
6.「コモンネーム」（CN）は本 CA が発行する 証明書をインストールするサーバにおいて使用するホスト名（FQDN）とする。
7.「主体者別名」（subjectAltName）拡張は本 CA が発行する証明書をインストールするサーバにおいて使用するホスト名及び必要に応じてホスト別名（alias）とする（いずれも FQDN）。

(2)サーバ証明書（NII Open Domain CA - G5）

1.「国名」（C）は JP とする。
2.「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則として RA に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定する。
3.「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則として RA に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定する。
4.「組織名」（O）とは、利用管理者及び利用者が所属し、サブジェクトに記載されたサーバを管理する主体となる組織とし、原則として事前に RA に登録したサービス利用機関名(英語表記)を用いる。

5.「組織単位名」（OU）は、任意選択の記入欄とする。OU の欄は、組織内のさまざまな部門等（例えば、工学部、理学部、法学部の各学部）を区別するために使用する。
6.「コモンネーム」（CN）は本 CA が発行する 証明書をインストールするサーバにおいて使用するホスト名（FQDN）とする。
7.「主体者別名」（subjectAltName）拡張は本 CA が発行する証明書をインストールするサーバにおいて使用するホスト名及び必要に応じてホスト別名（alias）とする（いずれも FQDN）。

(3)サーバ証明書（NII Open Domain CA - G6）

1.「国名」（C）は JP とする。
2.「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則として RA に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定する。
3.「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則として RA に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定する。
4.「組織名」（O）とは、利用管理者及び利用者が所属し、サブジェクトに記載されたサーバを管理する主体となる組織とし、原則として事前に RA に登録したサービス利用機関名(英語表記)を用いる。
5.「組織単位名」（OU）は、任意選択の記入欄とする。OU の欄は、組織内のさまざまな部門等（例えば、工学部、理学部、法学部の各学部）を区別するために使用する。
6.「コモンネーム」（CN）は本 CA が発行する 証明書をインストールするサーバにおいて使用するホスト名（FQDN）とする。
7.「主体者別名」（subjectAltName）拡張は本 CA が発行する証明書をインストールするサーバにおいて使用するホスト名及び必要に応じてホスト別名（alias）とする（いずれも FQDN）。

(4)個人認証用証明書

1.「国名」（C）は JP とする。
2.「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則として RA に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定する。
3.「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則として RA に事前に届出したとおりの所在地の市区町村名をローマ字表記で

指定する。

4.「組織名」（O）とは，利用管理者及び利用者が所属する組織とし，原則として事前に RA に登録したサービス利用機関名(英語表記)を用いる。

5.「組織単位名」（OU）は、任意選択の記入欄とする。OU の欄は、組織内のさまざまな部門（例えば、工学部、理学部、法学部の各学部）及び学籍番号等により利用管理者及び利用者を区別するために使用する。

6.「コモンネーム」（CN）は、利用者氏名、利用者の識別子（文字列や数字)、利用者に含まれる組織名、利用者に含まれる役職名、組織内のさまざまな部門名を用いる。

⑸S/MIME 証明書

1.「国名」（C）は JP とする。

2.「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名とし、原則として RA に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定する。

3.「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、原則として RA に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定する。

4.「組織名」（O）とは，利用管理者及び利用者が所属する組織とし，原則として事前に RA に登録したサービス利用機関名(英語表記)を用いる。

5.「組織単位名」（OU）は、任意選択の記入欄とする。OU の欄は、組織内のさまざまな部門（例えば、工学部、理学部、法学部の各学部）及び学籍番号等により利用管理者及び利用者を区別するために使用する。

6.「コモンネーム」（CN）は、利用者氏名、利用者の識別子（文字列や数字)、利用者に含まれる組織名、利用者に含まれる役職名、組織内のさまざまな部門名を用いる。

7.「主体者別名」（subjectAltName）は、利用者の電子メールアドレスを用いる。

3.1.2 名前が意味を持つことの必要性

本 CA が発行するサーバ証明書、個人認証用証明書、S/MIME 証明書の国名(C)、都道府県名(ST)及び場所名(L)は、利用管理者及び利用者が所属する学術機関の所在地を示すために用いられる。

本 CA が発行する証明書の組織名及び組織単位名は、検証者が利用管理者及び利用者が所属する組織のものであることを確認するために参照される。

本 CA が発行するサーバ証明書のコモンネーム及び主体者別名は、検証者がアクセスするサーバの FQDN と一致していることを確認するために参照される。

本 CA が発行する個人認証用証明書及び S/MIME 証明書のコモンネームは、検証者が利用者氏名、利用者の識別子（文字列や数字)、利用者に含まれる組織名、利用者に含まれる役職名、組織内のさまざまな部門名と一致していることを確認するために参照される。

3.1.3 名前の匿名性又は仮名性

本 CA が発行する証明書の名前は、匿名や仮名の登録は行わないものとする。また、名前に関する要件は、本 CP「3.1.1 名前の種類」及び「3.1.2 名前が意味を持つことの必要性」のとおりとする。

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、ITU-T 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 が発行する全証明書内において一意性を備えたものとする。

3.1.6 認識、認証及び商標の役割

本 CA は、証明書申請に記載される名称について知的財産権を有しているかどうかの検証を行わない。利用管理者は、第三者の登録商標や関連する名称を、本 CA に申請してはならない。本 CA は、登録商標等を理由に利用管理者と第三者間で紛争が起こった場合、仲裁や紛争解決は行わない。また、本 CA は紛争を理由に利用管理者からの証明書申請の拒絶や発行された証明書を失効させる権利を有する。

3.2 初回の識別と認証

3.2.1 秘密鍵の所持を証明する方法

利用管理者及び利用者が公開鍵と対になる秘密鍵を所有していることの証明は、利用管理者及び利用者が公開鍵に自己署名を行い、本 CA が受け取った公開鍵の署名を検証することで、公開鍵と対になる秘密鍵を所持しているという確認方法をとる。

3.2.2 組織の認証

3.2.2.1 サービス利用機関における確認実施手順の規定

サービス利用機関は、事前の作業として以下のことを行うものとする。

(1) 登録担当者の任命

サービス利用機関は、NII が別に定める手続きにもとづき、予め登録担当者を任命し、RA に届け出ておくものとする。

登録担当者の実在性確認は、サービス利用機関によって行われるものとする。

(2) サービス利用機関で取り扱うドメインの本人性確認

サービス利用機関は、当該ドメインのサーバに対してサーバ証明書を発行することや、利用管理者及び利用者に対してメールアドレスを登録する S/MIME 証明書を発行することについて、ドメイン登録担当者の合意を得ておくものとする。

(3) 確認実施手順の規定

サービス利用機関は、利用管理者及び利用者からの申請を登録担当者がとりまとめるにあたって、以下の手続きについて予め規定し、NII が別に定める手続きにもとづき、RA に届け出ておくものとする。

・利用管理者及び利用者の実在性、本人性確認

・サーバの実在性(サーバの管理責任及びドメインの実在性)確認

3.2.2.2 RA が事前に行う確認作業

RA は、事前の作業として以下のことを行う。

(1) サービス利用機関の実在性

RA は、NII が別に定める手続きにもとづき、サービス利用機関の実在性の確認を行う。

(2) サービス利用機関で取り扱うドメインの実在性

RA は、NII が別に定める手続きにもとづき、ドメインの実在性の確認を行う。

(3) 確認実施手順の審査

RA は、サービス利用機関が届け出た確認実施手順について、NII が別に定める手続きにもとづき、審査を行う。

審査の結果、不備がなければ確認実施手順の届出を承認する。

不備があれば届出を却下し、必要に応じて、届出を行ったサービス利用機関に対し届出の再提出を依頼する。なお、提出された届出書類は返却しない。

3.2.3 個人の認証

RA は、事前の作業として以下のことを行う。

(1) 登録担当者の本人性確認

RA は、NII が別に定める手続きにもとづき、登録担当者の本人性の確認を行う。

(2) 登録担当者用証明書の発行

RA は、本人性確認を行った登録担当者に対して、NII が以下に定める CA から登録担当者用証明書を発行する。

認証局名：国立情報学研究所　運用支援認証局

証明書ポリシ OID：　1.3.6.1.4.1.32264.3.2.2.1

RA は、証明書の発行申請の都度行う確認として以下のことを行う。

(1) 登録担当者の本人性確認

登録担当者の本人性は、NII が予め発行した登録担当者用証明書による認証を経て申請が行われることによって、確認を行う。

登録担当者は、証明書の発行申請の都度行う確認として以下のことを行う。

(1) 利用管理者及び利用者の実在性、本人性確認

登録担当者は、サービス利用機関が別に定める手続きにもとづき、利用管理者及び利用者の実在性及び本人性の確認を行う。

3.2.4 検証対象としない利用管理者及び利用者情報

RA は、ドメインの本人性、登録担当者の実在性、利用管理者及び利用者の実在性、本人性及びサーバの実在性、本人性の確認を行わない。

ドメインの本人性は、サービス利用機関によって事前に確認が行われるものとし、ドメインに対する証明書発行の合意を確認するものとする。

登録担当者の実在性は、NII が予め発行する登録担当者用証明書によって、確認されているものとみなす。

利用管理者及び利用者の実在性、本人性及びサーバの実在性は、サービス利用機関が別に定める確認実施手順にもとづき、登録担当者によって確認が行われるものとする。

サーバの本人性は、利用管理者自身によって確認が行われるものとし、登録担当者は利用管理者からの申請を受け付けるにあたって、サーバの本人性が確認されていることを、利用管理者に確認するものとする。

3.2.5 権限確認

RA は、登録担当者用証明書を認証することによって、証明書に関する申請を行うものが登録担当者の権限を有していることの確認を行う。

3.2.6 相互運用の基準

本 CA は、Security Communication RootCA2 及び Security Communication ECCRootCA1 より、片方向相互認証証明書を発行されている。

3.2.7 ドメインの認証

本 CA は、利用者がドメイン名の利用権を有しているか確認するため、次の方法でドメインの認証を行う。

1. ローカル部は'admin'、 'administrator'、 'webmaster'、 'hostmaster'、または'postmaster'とし、「@」以下は認証ドメイン名として作成した電子メールアドレスにランダム値を送信して、ランダムな値が含まれた確認応答を受け取ることによって、要求された FQDN の制御を実証する。
2. WHOIS レジストリサービスに登録されたドメイン管理者の電子メールアドレスにランダム値を送信し、ランダムな値が含まれた確認応答を受け取ることによって、要求された FQDN の制御を実証する。
3. その他　Baseline Requirements に準拠した合理的な方法で確認する。

3.3 鍵更新申請時の本人性確認及び認証

3.3.1 通常の鍵更新時の本人性確認及び認証

鍵更新時における本人性確認及び認証は、本 CP「3.2 初回の識別と認証」と同様とする。

3.3.2 証明書失効後の鍵更新の本人性確認及び認証

証明書失効後の鍵更新時における本人性確認及び認証は、本 CP「3.2 初回の識別と認証」と同様とする。

3.4 失効申請時の本人性確認及び認証

RA は、証明書の失効申請の都度行う確認として以下のことを行う。

(1) 登録担当者の本人性

登録担当者の本人性は、NII が予め発行した登録担当者用証明書による認証を経て申

請が行われることによって、確認を行う。
RA は、登録担当者の実在性、利用管理者及び利用者の本人性及びサーバの本人性の確認を行わない。
登録担当者の実在性は、NII が予め発行する登録担当者用証明書によって、確認されているものとみなす。
利用管理者及び利用者の本人性は、サービス利用機関が別に定める確認実施手順にもとづき、登録担当者によって確認が行われるものとする。
サーバの本人性は、利用管理者自身によって行われるものとし、登録担当者は利用管理者からの申請を受け付けるにあたって、サーバの本人性が確認されていることを、利用管理者に確認するものとする。
利用管理者の実在性及びサーバの実在性は確認を行わない。

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 証明書の申請者

証明書の発行申請を行うことができる者は、本 CP「1.3.5.2 登録担当者」で定義する登録担当者とする。ただし、実在性及び本人性を RA で確認できる場合に限り、本 CP「1.3.3 利用管理者・利用者」で定義する利用管理者も含む。

4.1.2 申請手続及び責任

証明書の発行申請を行う者は、本 CP 及び CPS の内容を承諾した上で、NII が別に定める手続きに基づき、本 CA に対して正確な情報を提出するものとする。

証明書の発行申請を行う者は、本 CP「3.2.4 検証対象としない利用管理者及び利用者情報」の真正性について、責任を負うものとする。

4.2 証明書申請手続き

4.2.1 本人性及び資格確認

本 CA は、本 CP「3.2 初回の識別と認証」に記載の情報をもって、申請情報の審査を行う。

4.2.2 証明書申請の承認又は却下

本 CA は、NII が別に定める手続きに基づき、証明書の発行申請に関する情報について審査を行う。

審査の結果、不備がなければ、申請を承認する。

不備がある申請については申請を却下する。不備の内容に応じて、申請を行った者は、申請の再提出を行うことができる。なお、提出された申請書類は返却しない。

4.2.3 証明書申請手続き期間

本 CA は、承認を行った申請について、適時証明書の発行登録を行う。

4.2.4 CAA レコードの確認

本 CA は、申請情報の審査時に CAA レコードを確認する。本 CA を DNS の CAA レコードに記載する場合、 Issuer Domain Name は “certs.nii.ac.jp" とする。

4.3 証明書発行

4.3.1 証明書発行時の本 CA の機能

本 CA は、発行申請を受け付けた後に、証明書の発行登録作業を行う。発行登録作業によって、証明書を発行し、利用管理者及び利用者に証明書を配付する。

なお、証明書発行については、本 CP 公開前にテストを目的とした証明書の発行作業を行う。

4.3.2 証明書発行後の通知

本 CA は、利用管理者及び利用者に対し証明書を渡すことで、通知したものとする。

また、登録担当者に対し、証明書の発行が完了したことを通知する。

4.4 証明書受領

4.4.1 証明書受領確認

本 CA から利用管理者及び利用者へ証明書を配付されたことをもって、証明書が受領されたものとする。

4.4.2 本 CA による証明書の公開

本 CA は、利用管理者及び利用者の証明書の公開は行わない。

4.4.3 他の関係者への通知

本 CA は、登録担当者を除く第三者に対する証明書の発行通知は行わない。

4.5 鍵ペアと証明書の用途

4.5.1 利用者の秘密鍵と証明書の使用

本 CP「1.4.1 適切な証明書の使用」と同様とする。利用者は、「1.4.1 適切な証明書の使用」に記載された用途のみに当該証明書及び対応する秘密鍵を利用するものとし、その他の用途に利用してはならない。

4.5.2 検証者の公開鍵と証明書の使用

検証者は、公開鍵及び証明書を使用し、本 CA が発行した証明書の信頼性を検証することができる。本 CA が発行した証明書を検証し信頼する前に、本 CP 及び CPS の内容について理解し、承諾しなければならない。

4.6 証明書更新（鍵更新を伴わない証明書更新）

本 CA は鍵更新を伴わない証明書の更新を認めない。

4.6.1 証明書の更新事由

規定しない。

4.6.2 証明書の更新申請を行うことができる者

規定しない。

4.6.3 証明書の更新申請の処理手続

規定しない。

4.6.4 証明書利用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手続

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

規定しない。

4.7 証明書の鍵更新（鍵更新を伴う証明書更新）

4.7.1 証明書鍵更新の要件

証明書の更新は、証明書の有効期間が満了する場合や、危殆化等の理由で秘密鍵が利用できなくなった場合などに、新たに生成された鍵ペアを使って行うことができる。失効した証明書又は有効期限が切れた証明書は鍵ペアの更新を伴わずに更新することはできない。

4.7.2 鍵更新申請者

本 CP「4.1.1 証明書の申請者」と同様とする。

4.7.3 鍵更新申請の処理手順

本 CP「4.1.2 申請手続及び責任」、「4.2 証明書申請手続き」及び「4.3.1 証明書発行時の本 CA の機能」と同様とする。

なお、申請を行う者の本人性確認及び資格確認については、本 CA が、本 CP「3.3 鍵更新申請時の本人性確認及び認証」に記載の情報をもって、申請を行う者の審査を行う。

4.7.4 証明書更新後の通知

本 CP「4.3.2 証明書発行後の通知」と同様とする。

4.7.5 証明書受領確認

本 CP「4.4.1 証明書受領確認」と同様とする。

4.7.6 本 CA による証明書の公開

本 CP「4.4.2 本 CA による証明書の公開」と同様とする。

4.7.7 他の関係者への通知

本 CP「4.4.3 他の関係者への通知」と同様とする。

4.8 証明書の変更

4.8.1 証明書変更の要件

証明書の変更は、有効期限内の失効していない証明書の記載内容に変更が発生した場合に、新たに生成された鍵ペアを使って行うことができる。

4.8.2 証明書の変更申請者

本 CP「4.1.1 証明書の申請者」と同様とする。

4.8.3 証明書変更の処理手順

本 CP「4.1.2 申請手続及び責任」、「4.2 証明書申請手続き」及び「4.3.1 証明書発行時の本 CA の機能」と同様とする。

なお、申請を行う者の本人性確認及び資格確認については、本 CA が、本 CP「3.3 鍵更新申請時の本人性確認及び認証」に記載の情報をもって、申請を行う者の審査を行う。

4.8.4 証明書変更後の通知

本 CP「4.3.2 証明書発行後の通知」と同様とする。

4.8.5 変更された証明書の受理

本 CP「4.4.1 証明書受領確認」と同様とする。

4.8.6 本 CA による変更証明書の公開

本 CP「4.4.2 本 CA による証明書の公開」と同様とする。

4.8.7 他の関係者への通知

本 CP「4.4.3 他の関係者への通知」と同様とする。

4.9 証明書の失効と一時停止

4.9.1 証明書失効事由

本 CA は次の事由が発生した場合、登録担当者からの申請に基づき証明書の失効を行う。

- 証明書記載情報に変更があった場合
- 秘密鍵の盗難、紛失、漏洩、不正利用等により秘密鍵が危殆化した又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

また、本 CA は、次の事由が発生した場合に、本 CA の判断により証明書を失効する。

- 利用管理者、利用者及び登録担当者が本 CP、CPS、関連する規程又は法律に基づく義務を履行していない場合
- 本 CA を終了する場合
- 本 CA の秘密鍵が危殆化した又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 失効申請者

証明書の失効の申請を行うことができる者は、登録担当者とする。なお、本 CP「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 が失効申請者となり得る。

4.9.3 失効申請の手続き

本 CP「4.1.2 申請手続及び責任」、「4.2 証明書申請手続き」及び「4.3.1 証明書発行時の本 CA の機能」と同様とする。

なお、申請を行う者の本人性確認及び資格確認については、本 CA が、本 CP「3.4 失

効申請時の本人性確認及び認証」に記載の情報をもって、申請を行う者の審査を行う。

4.9.4 失効における猶予期間

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わなければならない。

4.9.5 本 CA による失効申請の処理期間

本 CA は、有効な失効の申請を受け付けてから速やかに証明書の失効処理を行い、CRL へ当該証明書情報を反映する。

4.9.6 検証者の失効情報確認の要件

本 CA が発行する証明書には、CRL の格納先である URL を記載する。また、サーバ証明書については CRL の他に OCSP サーバの URL を記載する。なお、その他の証明書には OCSP サーバの URL は記載しない。

CRL 及び OCSP サーバは、一般的な Web インターフェースを用いてアクセスすることができる。なお、CRL には、有効期限の切れた証明書情報は含まれない。

検証者は、利用管理者及び利用者の証明書について、有効性を確認しなければならない。証明書の有効性は、リポジトリに掲載している CRL 又は OCSP サーバにより確認する。

4.9.7 CRL の発行周期

CRL は、失効処理の有無にかかわらず、24 時間ごとに更新を行う。証明書の失効処理が行われた場合は、その時点で CRL の更新を行う。

CRL の有効期間は 96 時間とする。

4.9.8 CRL がリポジトリに格納されるまでの最大遅延時間

本 CA が発行した CRL は、即時にリポジトリに反映させる。

4.9.9 OCSP の提供

NII Open Domain CA - G4、NII Open Domain CA - G5、NII Open Domain CA - G6 では、OCSP サーバを通じてサーバ証明書ステータス情報の提供を行う。

その他 CA については OCSP サーバを提供しない。

4.9.10 OCSP 確認要件

本 CA より発行される証明書について、検証者は有効性の確認を行わなければならない。リポジトリに掲載している CRL により、サーバ証明書の失効登録の有無を確認しない場合には、OCSP サーバにより提供されるサーバ証明書ステータス情報の確認を

行わなければならない。

4.9.11 その他の利用可能な失効情報検査手段

本 CA は、RFC4366 に従い、ステープリングを利用して OCSP レスポンスを配布できる。この場合、本 CA は利用者が TLS 処理に証明書の OCSP レスポンスを含めることを確実なものにする。本 CA は、利用者に対してこの要件を実施する場合は、NII が別に定める各種規程にて定める。

4.9.12 鍵の危殆化の特別な要件

本 CP「4.9.1 証明書失効事由」に記載する。

4.9.13 証明書の一時停止

本 CA は、証明書の一時停止は行わない。

4.9.14 証明書の一時停止の申請者

該当しない。

4.9.15 一時停止申請の手続き

該当しない。

4.9.16 証明書の一時停止の限度

該当しない。

4.10 証明書ステータスサービス

4.10.1 証明書ステータスサービスの内容

検証者は OCSP サーバを通じてサーバ証明書のステータス情報を確認することができる。

4.10.2 サービスの利用時間

本 CA は、24 時間 365 日、証明書ステータス情報を確認できるよう OCSP サーバを管理する。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。

4.10.3 その他特徴

規定しない。

4.11 利用の終了

利用管理者及び利用者は本サービスの利用を終了する場合、登録担当者を介して証明書の失効申請を行わなければならない。

4.12 秘密鍵寄託と鍵回復

本 CA は、利用管理者及び利用者が所有する秘密鍵の寄託は行わない。

4.12.1 寄託と鍵回復ポリシ及び実施

規定しない。

4.12.2 セッションキーのカプセル化と鍵回復のポリシ及び実施

該当しない。

5. 設備、運営、運用統制

5.1 建物及び物理的管理

5.1.1 施設の所在と建物構造

本項については、CPS に規定する。

5.1.2 物理的アクセス

本項については、CPS に規定する。

5.1.3 電源及び空調設備

本項については、CPS に規定する。

5.1.4 水害

本項については、CPS に規定する。

5.1.5 火災防止及び保護対策

本項については、CPS に規定する。

5.1.6 媒体保管場所

本項については、CPS に規定する。

5.1.7 廃棄物の処理

本項については、CPS に規定する。

5.1.8 オフサイトバックアップ

本項については、CPS に規定する。

5.2 手続き的管理

5.2.1 信頼される役割

本項については、CPS に規定される役割以外に下記の役割を定める。

(1)　RA 責任者

RA 責任者は、RA 管理者を任命することができる。

(2)　RA 管理者

RA 管理者は、事前の作業として、以下のことを行うことができる。

・サービス利用機関の実在性の確認
・サービス利用機関で取り扱うドメインの実在性の確認
・確認実施手順の審査
・登録担当者の本人性の確認

(3)　証明書自動発行支援システム

証明書自動発行支援システムは、申請の都度の作業として、以下のことを行うことができる。

・登録担当者の本人性の確認
・証明書の申請に関する情報の審査
・証明書の発行・更新・失効操作

(4)　登録担当者

登録担当者は、申請の都度の作業として、以下のことを行うことができる。

・証明書の発行申請
・証明書の更新申請
・証明書の失効申請

5.2.2 職務ごとに必要とされる人数

本項については、CPS に規定される以外に下記のとおりとする。

(1)　RA 責任者

RA 責任者は、1 名とする。

(2)　RA 管理者

RA 管理者は、複数名とする。

(3)　証明書自動発行支援システム

証明書自動発行支援システムは、1 系統とする。

5.2.3 個々の役割に対する識別と認証

本 CA は、本 CA のシステムへのアクセスに関し、クライアント認証によって、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。

クライアント認証に用いるクライアント認証用証明書は、NII が別に定める CA から発

行する。

5.2.4 職務の分割を必要とする役割

本項については、CPS に規定する。

また、RA 管理者の任命は RA 責任者のみを可能とする。

RA 責任者と RA 管理者は職務を兼務することを可能とする。

5.3 要員管理

5.3.1 資格、経験及び身分証明の要件

本項については、CPS に準ずる。

5.3.2 経歴の調査手続

本項については、CPS に準ずる。

5.3.3 研修要件

本項については、CPS に準ずる。

5.3.4 再研修の頻度及び要件

本項については、CPS に準ずる。

5.3.5 職務のローテーションの頻度及び要件

本項については、CPS に準ずる。

5.3.6 認められていない行動に対する制裁

本項については、CPS に準ずる。

5.3.7 独立した契約者の要件

本項については、CPS に準ずる。

5.3.8 要員へ提供する資料

本項については、CPS に準ずる。

5.4 監査ログ記録手順

5.4.1 記録される事項

本項については、CPS に準ずる。

5.4.2 監査ログを処理する頻度

本項については、CPS に準ずる。

5.4.3 監査ログを保存する期間

本項については、CPS に準ずる。

5.4.4 監査ログの保護

本項については、CPS に準ずる。

5.4.5 監査ログのバックアップ手続

本項については、CPS に準ずる。

5.4.6 監査ログの収集システム（内部又は外部）

本項については、CPS に準ずる。

5.4.7 イベントを起こしたサブジェクトへの通知

本項については、CPS に準ずる。

5.4.8 脆弱性評価

本項については、CPS に準ずる。

5.5 記録のアーカイブ化

5.5.1 アーカイブ記録の種類

本項については、CPS に準ずる。

5.5.2 アーカイブを保存する期間

本項については、CPS に準ずる。

5.5.3 アーカイブの保護

本項については、CPS に準ずる。

5.5.4 アーカイブのバックアップ手続

本項については、CPS に準ずる。

5.5.5 記録にタイムスタンプをつける要件

本項については、CPS に準ずる。

5.5.6 アーカイブ収集システム（内部又は外部）

本項については、CPS に準ずる。

5.5.7 アーカイブ情報を入手し検証する手続き

本項については、CPS に準ずる。

5.6 鍵の切り替え

本 CA の秘密鍵は、秘密鍵に対応する証明書の有効期間が本 CA から発行する証明書の最大有効期間よりも短くなる前に新たな秘密鍵の生成及び証明書の発行を行う。新しい秘密鍵が生成された後は、新しい秘密鍵を使って証明書及び CRL の発行を行う。

5.7 危殆化及び災害復旧

本 CA は、本 CA の秘密鍵が危殆化した場合又は事故・災害等により本 CA の運用の停止を伴う事象が発生した場合は、速やかに業務復旧に向けた対応を行うとともに、サービス利用機関、登録担当者、利用管理者、利用者及びその他関係者に対し、必要情報を連絡する。

5.7.1 事故及び危殆化の取り扱い手続き

本 CA は、事故および危殆化が発生した場合に速やかに本 CA に関連するシステムおよび関連する業務を復旧できるよう、以下を含む事故および危殆化に対する対応手続を策定する。

- CA 秘密鍵の危殆化
- 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 コンピュータの資源、ソフトウェア、データが破損した場合の対処

本 CA は、本 CA に関連するシステムのハードウェア、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 に関連するシステムの復旧作業を行う。

5.7.3 CA 秘密鍵が危殆化した場合の対処

本 CA は、本 CA の秘密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、および災害等により本 CA に関連するシステムの運用が中断、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 災害等発生後の事業継続性

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 に関連するシステムの代替機の確保、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、可能な限りすみやかに認証基盤システムを復旧するための対策を行う。

5.8 CA 又は RA の廃業

本 CA 又は RA を終了する場合、終了する 30 日前にサービス利用機関、登録担当者、利用管理者、利用者及びその他関係者に対して終了の事実を通知又は公表し、所定の終了手続を行う。ただし、緊急等やむをえない場合、この期間を短縮できるものとする。

6. 技術面のセキュリティ管理

6.1 鍵ペアの生成と導入

6.1.1 鍵ペアの生成

本 CA では、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。
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う。
利用管理者及び利用者の鍵ペアは、利用管理者及び利用者自身で生成するか、又は本 CA の施設内において生成する。

6.1.2 利用管理者及び利用者に対する秘密鍵の送付

利用管理者及び利用者の秘密鍵は、利用管理者及び利用者自身が生成する。本 CA が利用管理者及び利用者秘密鍵を生成する場合は、秘密鍵を使用するための PIN と秘密鍵を安全な方法で利用管理者及び利用者へ送付する。

6.1.3 本 CA への公開鍵の送付

本 CA への利用管理者及び利用者公開鍵の送付は、オンライン若しくはオフラインによる安全な方法によって行われる。

6.1.4 CA 公開鍵の配付

本 CA のリポジトリにアクセスすることにより、CA 公開鍵を入手することができる。

6.1.5 鍵長

本 CA の鍵ペアは、RSA 方式鍵長 2048 ビット又は ECC 方式鍵長 384 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われる。
利用管理者及び利用者の公開鍵のパラメータの生成及び品質検査については規定しない。

6.1.7 鍵の使用目的

本 CA の証明書の KeyUsage には keyCertSign,cRLSign のビットを設定する。
本 CA が発行する利用管理者及び利用者の証明書の KeyUsage には、digitalSignature, keyEncipherment を設定可能とする。ただし、Subject Public Key Info が secp384r1

である利用管理者及び利用者の証明書の KeyUsage は、digitalSignature を設定可能とする。

6.2 秘密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

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵については規定しない。

6.2.2 複数人による秘密鍵の管理

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵の活性化、非活性化、バックアップ等の操作は、利用管理者及び利用者の管理の下で安全に行わなければならない。

6.2.3 秘密鍵の寄託

本項は CPS に準ずる。

また、本 CA は、利用管理者及び利用者の秘密鍵の寄託は行わない。

6.2.4 秘密鍵のバックアップ

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵のバックアップは、利用管理者及び利用者の管理の下で安全に保管しなければならない。

6.2.5 秘密鍵のアーカイブ

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵のアーカイブは行わない。

6.2.6 暗号モジュールへの秘密鍵の格納と取り出し

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵については規定しない。

6.2.7 暗号モジュール内での秘密鍵保存

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵については規定しない。

6.2.8 秘密鍵の活性化方法

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵については規定しない。

6.2.9 秘密鍵の非活性化方法

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵については規定しない。

6.2.10 秘密鍵の廃棄方法

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵については規定しない。

6.2.11 暗号モジュールの評価

本項は CPS に準ずる。

また、利用管理者及び利用者の秘密鍵については規定しない。

6.3 鍵ペア管理に関するその他の項目

6.3.1 公開鍵のアーカイブ

本項については、CPS に規定する。

6.3.2 証明書と鍵ペアの使用期間

本 CA の秘密鍵及び公開鍵の有効期間は 10 年以内とする。

利用管理者及び利用者の秘密鍵及び公開鍵の有効期間は 2020 年 8 月 25 日 14 時 30 分以前に発行された、サーバ証明書 25 ヶ月以内、2020 年 8 月 25 日 14 時 30 分以降に発行されたサーバ証明書 13 ヶ月以内、個人認証用証明書 52 ヶ月以内、S/MIME 証明書 52 ヶ月以内とする。

6.4 秘密鍵の活性化情報

6.4.1 活性化データの生成および設定

本項については、CPS に規定する。

6.4.2 活性化データの保護

本項については、CPS に規定する。

6.4.3 活性化データの他の考慮点

本項については、CPS に規定する。

6.5 コンピュータセキュリティ管理

6.5.1 コンピュータセキュリティに関する技術的要件

本項については、CPS に規定する。

6.5.2 コンピュータセキュリティ評価

本項については、CPS に規定する。

6.6 技術面におけるライフサイクル管理

6.6.1 システム開発管理

本項については、CPS に規定する。

6.6.2 セキュリティマネジメント管理

本項については、CPS に規定する。

6.6.3 ライフサイクルセキュリティ管理

本項については、CPS に規定する。

6.7 ネットワークセキュリティ管理

本項については、CPS に規定する。

6.8 タイムスタンプ

本項については、CPS に規定する。

7. 証明書、CRL 及び OCSP のプロファイル

7.1 証明書のプロファイル

本項に示すプロファイルのデータフォーマットについては、IETF RFC 5280 に準拠するものとし、そのプロファイルは以下の通りである。

(1) サーバ証明書プロファイル（NII Open Domain CA - G4）

表 7-1-1-1 サーバ証明書（NII Open Domain CA - G4）

2018 年 3 月 26 日 14 時（日本時間）までに発行されたサーバ証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G4	-
Validity	NotBefore	例) 2018/01/01 12:00:00 GMT	-
	NotAfter	例) 2020/02/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Locality	L=Academe（固定値）	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=upki-portal.nii.ac.jp	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical

KeyUsage	digitalSignature, keyEncipherment	y
ExtendedKeyUsage	serverAuth,clientAuth （その他必要に応じて設定）	n
CertificatePolicies	[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
CRL Distribution Points	URL=http://repo1.secomtrust.net/spca/nii/ odca3/fullcrlg4.crl	n
SubjectAltName	dNSName：サーバ FQDN （必要に応じて複数設定可）	n
Authority Information Access	URL=http://niig4.ocsp.secomtrust.net	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

(2)サーバ証明書プロファイル（NII Open Domain CA - G5）

表 7-1-2-1 サーバ証明書（NII Open Domain CA - G5）

2018 年 7 月 9 日 11 時（日本時間）までに発行されたサーバ証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G5	-
Validity	NotBefore	例) 2018/01/01 12:00:00 GMT	-
	NotAfter	例) 2020/02/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	StateOrProvince	ST=証明書毎に任意に指定	-
	Locality	L=証明書毎に任意に指定	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=upki-portal.nii.ac.jp	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		serverAuth,clientAuth （その他必要に応じて設定）	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1	n

	[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/sppca/nii/odca3/ [2]Certificate Policy: Policy Identifier =2.23.140.1.2.2	
CRL Distribution Points	URL=http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg5.crl	n
SubjectAltName	dNSName：サーバ FQDN （必要に応じて複数設定可）	n
Authority Information Access	URL=http://niig5.ocsp.secomtrust.net	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n
Certificate Transparency 用拡張	SignedCertificateTimestampList の値	n

表 7-1-2-2 サーバ証明書（NII Open Domain CA - G5）

2018 年 7 月 9 日 18 時（日本時間）～2020 年 4 月 13 日 13 時（日本時間）までに発行されたサーバ証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G5	-
Validity	NotBefore	例) 2018/01/01 12:00:00 GMT	-
	NotAfter	例) 2020/02/01 12:00:00 GMT	-

Subject	Country	C=JP（固定値）	-
	StateOrProvince	ST="都道府県" ＊ サービス利用機関毎に指定 例)ST=Tokyo	-
	Locality	L="市区町村" ＊ サービス利用機関毎に指定 例)L=Chiyoda-ku	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=upki-portal.nii.ac.jp	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		serverAuth,clientAuth （その他必要に応じて設定）	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/sppca/nii/odca3/ [2]Certificate Policy: Policy Identifier =2.23.140.1.2.2	n
CRL Distribution Points		URL=http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg5.crl	n

SubjectAltName	dNSName：サーバ FQDN （必要に応じて複数設定可）	n
Authority Information Access	URL=http://niig5.ocsp.secomtrust.net	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n
Certificate Transparency 用拡張	SignedCertificateTimestampList の値	n

表 7-1-2-3 サーバ証明書（NII Open Domain CA - G5）

2020 年 4 月 13 日 13 時（日本時間）～2020 年 12 月 25 日 0 時（日本時間）までに発行されたサーバ証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G5	-
Validity	NotBefore	例) 2020/08/25 12:00:00 GMT	-
	NotAfter	例) 2021/09/25 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	StateOrProvince	ST="都道府県" ＊ サービス利用機関毎に指定 例)ST=Tokyo	-
	Locality	L="市区町村" ＊ サービス利用機関毎に指定 例)L=Chiyoda-ku	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of	-

		Informatics	
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=upki-portal.nii.ac.jp	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		serverAuth,clientAuth （その他必要に応じて設定）	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/sppca/nii/odca3/ [2]Certificate Policy: Policy Identifier =2.23.140.1.2.2	n
CRL Distribution Points		URL=http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg5.crl	n
SubjectAltName		dNSName：サーバ FQDN （必要に応じて複数設定可）	n
Authority Information Access		CA Issuers - URL: http://repo1.secomtrust.net/sppca/nii/odca3/nii-odca3sha2ct******.cer OCSP - URL=http://niig5.ocsp.secomtrust.net ※CA Issuers の cer ファイル名の******部分には、年月が入る。もし、	n

	同月に 2 回以上発行する場合は、アルファベット順に英字を付加する。 （例：nii-odca3sha2ct202003.cer（1 回目）、nii-odca3sha2ct202003a.cer（2 回目））	
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n
Certificate Transparency 用拡張	SignedCertificateTimestampList の値	n

(3)サーバ証明書プロファイル（NII Open Domain CA - G6）

表 7-1-3-1 サーバ証明書（NII Open Domain CA - G6）

2020 年 12 月 25 日 0 時（日本時間）までに発行されたサーバ証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G6	-
Validity	NotBefore	例) 2020/08/25 12:00:00 GMT	-
	NotAfter	例) 2021/09/25 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	StateOrProvince	ST="都道府県" ＊ サービス利用機関毎に指定 例)ST=Tokyo	-
	Locality	L="市区町村" ＊ サービス利用機関毎に指定 例)L=Chiyoda-ku	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=upki-portal.nii.ac.jp	-
Subject Public Key Info		主体者の公開鍵 384 ビット ＊ ただし secp384r1 に限定とする	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y

ExtendedKeyUsage	serverAuth,clientAuth （その他必要に応じて設定）	n
CertificatePolicies	[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/sppca/nii/odca3/ [2]Certificate Policy: Policy Identifier =2.23.140.1.2.2	n
CRL Distribution Points	URL=http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg6.crl	n
SubjectAltName	dNSName：サーバ FQDN （必要に応じて複数設定可）	n
Authority Information Access	CA Issuers - URL: http://repo1.secomtrust.net/sppca/nii/odca3/nii-odca3ecdsa******.cer OCSP - URL: http://niig6.ocsp.secomtrust.net ※CA Issuers の cer ファイル名の******部分には、年月が入る。もし、同月に 2 回以上発行する場合は、アルファベット順に英字を付加する。 （例：nii-odca3ecdsa202003.cer（1 回目）、nii-odca3ecdsa202003a.cer（2 回目））	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

Certificate Transparency 用拡張	SignedCertificateTimestampList の値	n

(4) 個人認証用証明書プロファイル

表 7-1-4-1 個人認証用証明書

2018 年 7 月 9 日 11 時（日本時間）までに発行された個人認証用証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G4	-
Validity	NotBefore	例) 2015/04/01 12:00:00 GMT	-
	NotAfter	例) 2019/08/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Locality	L=Academe（固定値）	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="利用管理者及び利用者氏名又は識別子" ＊証明書毎に任意に指定 例) cn=Ichiro Suzuki	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		clientAuth	n

CertificatePolicies	[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
CRL Distribution Points	URL=http://repo1.secomtrust.net/spca/nii/odca3/fullcrlg4.crl	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

表 7-1-4-2 個人認証用証明書

2018 年 7 月 9 日 18 時（日本時間）～2020 年 12 月 25 日 0 時（日本時間）までに発行された個人認証用証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G4	-
Validity	NotBefore	例) 2018/04/01 12:00:00 GMT	-
	NotAfter	例) 2022/08/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	StateOrProvince	ST="都道府県" ＊ サービス利用機関毎に指定 例)ST=Tokyo	-
	Locality	L="市区町村"	-

		＊ サービス利用機関毎に指定 例)L=Chiyoda-ku	
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="利用管理者及び利用者氏名又は識別子" ＊証明書毎に任意に指定 例) cn=Ichiro Suzuki	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		clientAuth	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
CRL Distribution Points		URL=http://repo1.secomtrust.net/spca/nii/odca3/fullcrlg4.crl	n
Authority Key Identifier		発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier		主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

(5) S/MIME 証明書プロファイル

表 7-1-5-1 S/MIME 証明書

2016 年 12 月 26 日 11 時（日本時間）までに発行された S/MIME 証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O=National Institute of Informatics	-
	Common Name	CN=NII Open Domain CA - G4	-
Validity	NotBefore	例) 2015/04/01 12:00:00 GMT	-
	NotAfter	例) 2017/05/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Locality	L=Academe（固定値）	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="利用管理者及び利用者氏名又は識別子" ＊証明書毎に任意に指定 例) cn=Ichiro Suzuki	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		clientAuth, EmailProtection	n

CertificatePolicies	[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
Subject Alt Name	rfc822Name="メールアドレス" ＊証明書毎に任意に指定 例）rfc822Name=certs@nii.ac.jp	n
CRL Distribution Points	URL=http://repo1.secomtrust.net/spca/nii/odca3/fullcrlg4.crl	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

表 7-1-5-2 S/MIME 証明書

2016 年 12 月 26 日 15 時（日本時間）～2018 年 7 月 9 日 11 時（日本時間）までに発行された S/MIME 証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O=National Institute of Informatics	-
	Common Name	CN=NII Open Domain S/MIME CA	-
Validity	NotBefore	例) 2015/04/01 12:00:00 GMT	-
	NotAfter	例) 2019/08/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-

	Locality	L=Academe（固定値）	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="利用管理者及び利用者氏名又は識別子" ＊証明書毎に任意に指定 例) cn=Ichiro Suzuki	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		clientAuth, EmailProtection	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
Subject Alt Name		rfc822Name="メールアドレス" ＊証明書毎に任意に指定 例）rfc822Name=certs@nii.ac.jp	n
CRL Distribution Points		URL=http://repo1.secomtrust.net/spcpa/nii/odca3/fullcrlsm.crl	n
Authority Key Identifier		発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier		主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

表 7-1-5-3 S/MIME 証明書

2018 年 7 月 9 日 18 時（日本時間）～2020 年 12 月 25 日 0 時（日本時間）までに発行された S/MIME 証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O=National Institute of Informatics	-
	Common Name	CN=NII Open Domain S/MIME CA	-
Validity	NotBefore	例) 2018/04/01 12:00:00 GMT	-
	NotAfter	例) 2022/08/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	StateOrProvince	ST="都道府県" ＊ サービス利用機関毎に指定 例)ST=Tokyo	-
	Locality	L="市区町村" ＊ サービス利用機関毎に指定 例)L=Chiyoda-ku	-
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例)O= National Institute of Informatics	-
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例)OU=Cyber Science Infrastructure Development Department	-
	Common Name	CN="利用管理者及び利用者氏名又は識別子" ＊証明書毎に任意に指定 例) cn=Ichiro Suzuki	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y

ExtendedKeyUsage	clientAuth, EmailProtection	n
CertificatePolicies	[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
Subject Alt Name	rfc822Name="メールアドレス" ＊証明書毎に任意に指定 例）rfc822Name=certs@nii.ac.jp	n
CRL Distribution Points	URL=http://repo1.secomtrust.net/spca/nii/odca3/fullcrlsmime.crl	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

(6) OCSP サーバ証明書プロファイル

表 7-1-6-1 OCSP サーバ証明書プロファイル（NII Open Domain CA - G4）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G4	-
Validity	NotBefore	例) 2018/01/01 00:00:00 GMT	-
	NotAfter	例) 2019/01/01 00:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Locality	L=Academe（固定値）	-
	Organization	O= National Institute of Informatics	-
	Common Name	OCSP サーバ名（必須）	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		Null	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

表 7-1-6-2 OCSP サーバ証明書プロファイル（NII Open Domain CA - G5）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G5	-
Validity	NotBefore	例) 2018/01/01 00:00:00 GMT	-
	NotAfter	例) 2019/01/01 00:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Organization	O= National Institute of Informatics	-
	Common Name	OCSP サーバ名（必須）	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		Null	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/sppca/nii/odca3/	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

表 7-1-6-3 OCSP サーバ証明書プロファイル（NII Open Domain CA - G6）

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G6	-
Validity	NotBefore	例) 2018/01/01 00:00:00 GMT	-
	NotAfter	例) 2019/01/01 00:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Organization	O= National Institute of Informatics	-
	Common Name	OCSP サーバ名（必須）	-
Subject Public Key Info		主体者の公開鍵 384 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature	y
ExtendedKeyUsage		OCSPSigning	n
OCSP No Check		Null	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/sppca/nii/odca3/	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n
Subject Key Identifier		主体者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

(7) システム用 S/MIME 証明書プロファイル

表 7-1-7-1 システム用 S/MIME 証明書

2016 年 12 月 26 日 11 時（日本時間）までに発行されたシステム用 S/MIME 証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain CA - G4	-
Validity	NotBefore	例) 2018/04/01 12:00:00 GMT	-
	NotAfter	例) 2020/05/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Organization	O=SECOM Trust Systems Co.,Ltd	-
	Organizational Unit	OU=UPKI Digital Certificate Issuance Service	-
	Common Name	CN=CA Support Center	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		EmailProtection	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
Subject Alt Name		rfc822Name= ca-support@ml.secom-sts.co.jp	n

CRL Distribution Points	URL=http://repo1.secomtrust.net/spca/nii/odca3/fullcrlg4.crl	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

表 7-1-7-2 システム用 S/MIME 証明書

2016 年 12 月 26 日 15 時（日本時間）～2018 年 7 月 9 日 11 時（日本時間）までに発行されたシステム用 S/MIME 証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O=National Institute of Informatics	-
	Common Name	CN=NII Open Domain S/MIME CA	-
Validity	NotBefore	例) 2018/04/01 12:00:00 GMT	-
	NotAfter	例) 2022/08/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	Organization	O=SECOM Trust Systems Co.,Ltd	-
	Organizational Unit	OU=UPKI Digital Certificate Issuance Service	-
	Common Name	CN=CA Support Center	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		clientAuth, EmailProtection	n

CertificatePolicies	[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
Subject Alt Name	rfc822Name= ca-support@ml.secom-sts.co.jp	n
CRL Distribution Points	URL=http://repo1.secomtrust.net/spcpca/nii/odca3/fullcrlsmime.crl	n
Authority Key Identifier	発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier	主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

表 7-1-7-3 システム用 S/MIME 証明書

2018 年 7 月 9 日 18 時（日本時間）～2020 年 12 月 25 日 0 時（日本時間）までに発行されたシステム用 S/MIME 証明書に適用

基本領域		設定内容	critical
Version		Version 3	-
Serial Number		例) 0123456789	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O=National Institute of Informatics	-
	Common Name	CN=NII Open Domain S/MIME CA	-
Validity	NotBefore	例) 2018/04/01 12:00:00 GMT	-
	NotAfter	例) 2022/08/01 12:00:00 GMT	-
Subject	Country	C=JP（固定値）	-
	StateOrProvince	ST=Tokyo	-

	Locality	L=Shibuya	-
	Organization	O=SECOM Trust Systems Co.,Ltd	-
	Organizational Unit	OU=UPKI Digital Certificate Issuance Service	-
	Common Name	CN=CA Support Center	-
Subject Public Key Info		主体者の公開鍵 2048 ビット	-
拡張領域		設定内容	critical
KeyUsage		digitalSignature, keyEncipherment	y
ExtendedKeyUsage		clientAuth, EmailProtection	n
CertificatePolicies		[1]Certificate Policy: Policy Identifier =1.3.6.1.4.1.32264.3.2.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repo1.secomtrust.net/spcpp/cps/index.html	n
Subject Alt Name		rfc822Name= ca-support@ml.secom-sts.co.jp	n
CRL Distribution Points		URL=http://repo1.secomtrust.net/spcpca/nii/odca3/fullcrlsmime.crl	n
Authority Key Identifier		発行者の公開鍵識別子 （発行者公開鍵の 160bit SHA-1 ハッシュ値）	n
Subject Key Identifier		主体者の公開鍵識別子 （主体者公開鍵の 160bit SHA-1 ハッシュ値）	n

(8)サーバ証明書の証明書発行要求 NII Open Domain CA - G4 (CSR)

表 7-1-8-1 サーバ証明書 NII Open Domain CA - G4 用 CSR のプロファイル

基本領域	設定内容	補
Version	Version 1(0)	-

Subject	Country	C=JP（固定値）	1
	Locality	L=Academe（固定値）	1
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例) O= National Institute of Informatics	1
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例) OU=Cyber Science Infrastructure Development Department	1
	commonName	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=www.nii.ac.jp	1
SubjectPublicKeyInfo		主体者の公開鍵　2048 ビット	2
attributes		原則 Null 値とする （ただし、例外を認める）	3
SignatureAlgorithm		以下のいずれかとする sha1WithRSAEncryption sha256WithRSAEncryption sha384WithRSAEncryption sha512WithRSAEncryption md5WithRSAEncryption	

1. 上記指定以外の属性を利用する必要がある場合には事前相談すること。少なくとも ST（State Or Province name）属性は使用しないこと。また、例えば利用管理者メールアドレスなど本サービスの確認項目対象外の情報を含めないこと。
2. RSA2048 ビットとする。
3. 任意の属性を含めても構わないが、必ずしも証明書に反映されるわけではない。また、含めた属性によっては受理不能とし、当該属性を除いて証明書発行要求の再生成を RA から求める場合がある。少なくとも SubjectAltName.rfc822Name 属性は使用しないこと。

(9) サーバ証明書の証明書発行要求 NII Open Domain CA - G5 (CSR)

表 7-1-9-1 サーバ証明書 NII Open Domain CA - G5 用 CSR のプロファイル

基本領域		設定内容	補
Version		Version 1(0)	-
Subject	Country	C=JP（固定値）	1
	StateOrProvince	ST="都道府県" ＊ サービス利用機関ごとに RA に事前に届出したとおりの所在地を指定 例)ST=Tokyo	1
	Locality	L="市区町村" ＊ サービス利用機関ごとに RA に事前に届出したとおりの所在地を指定 例)L=Chiyoda-ku	1
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例) O= National Institute of Informatics	1
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例) OU=Cyber Science Infrastructure Development Department	1
	commonName	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=www.nii.ac.jp	1
SubjectPublicKeyInfo		主体者の公開鍵　2048 ビット	2
attributes		原則 Null 値とする （ただし、例外を認める）	3
SignatureAlgorithm		以下のいずれかとする sha1WithRSAEncryption sha256WithRSAEncryption sha384WithRSAEncryption sha512WithRSAEncryption md5WithRSAEncryption	

1. 上記指定以外の属性を利用する必要がある場合には事前相談すること。また、例えば利用管理者メールアドレスなど本サービスの確認項目対象外の情報を含めないこと。 2. RSA2048 ビットとする。 3. 任意の属性を含めても構わないが、必ずしも証明書に反映されるわけではない。また、含めた属性によっては受理不能とし、当該属性を除いて証明書発行要求の再生成を RA から求める場合がある。少なくとも SubjectAltName.rfc822Name 属性は使用しないこと。

(10)サーバ証明書の証明書発行要求 NII Open Domain CA - G6 (CSR)

表 7-1-10-1 サーバ証明書 NII Open Domain CA - G6 用 CSR のプロファイル

基本領域		設定内容	補
Version		Version 1(0)	-
Subject	Country	C=JP（固定値）	1
	StateOrProvince	ST="都道府県" ＊ サービス利用機関ごとに RA に事前に届出したとおりの所在地を指定 例)ST=Tokyo	1
	Locality	L="市区町村" ＊ サービス利用機関ごとに RA に事前に届出したとおりの所在地を指定 例)L=Chiyoda-ku	1
	Organization	O="主体者組織名" ＊ サービス利用機関毎に任意に指定 例) O= National Institute of Informatics	1
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例) OU=Cyber Science Infrastructure Development Department	1
	commonName	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=www.nii.ac.jp	1
SubjectPublicKeyInfo		主体者の公開鍵　384 ビット	2

attributes	原則 Null 値とする （ただし、例外を認める）	3
SignatureAlgorithm	以下のいずれかとする ecdsa-with-SHA256 ecdsa-with-SHA384	-

1. 上記指定以外の属性を利用する必要がある場合には事前相談すること。また、例えば利用管理者メールアドレスなど本サービスの確認項目対象外の情報を含めないこと。
2. ECC384 ビット とする。（ただし secp384r1 に限定とする）
3. 任意の属性を含めても構わないが、必ずしも証明書に反映されるわけではない。また、含めた属性によっては受理不能とし、当該属性を除いて証明書発行要求の再生成を RA から求める場合がある。少なくとも SubjectAltName.rfc822Name 属性は使用しないこと。

7.1.1 バージョン番号

本 CA は、バージョン 3 を適用する。

7.1.2 証明書拡張

本 CA が発行する証明書は、証明書拡張フィールドを使用する。

7.1.3 アルゴリズムオブジェクト識別子

本サービスにおいて用いられるアルゴリズム OID は、次のとおりである。

アルゴリズム	オブジェクト識別子
RSA Encryption	1.2.840.113549.1.1.1
sha256WithRSAEncryption	1.2.840.113549.1.1.11
ecdsa-with-sha384	1.2.840.10045.4.3.3

7.1.4 名前形式

本 CA および利用者は、X.500 識別名に従って定義された DN によって一意に識別される。

7.1.5 名前制約

サーバ証明書（NII Open Domain CA - G5、NII Open Domain CA - G6）に設定する。

7.1.6 CP オブジェクト識別子

本 CA が発行する証明書の OID は、本「1.2 文書の名前と識別」の OID のとおりであ

る。

7.1.7 ポリシ制約拡張の利用

設定しない。

7.1.8 ポリシ修飾子の文法および意味

ポリシ修飾子については、本 CP および CPS を公表する Web ページの URI を格納している。

7.1.9 バージョン番号

設定しない。

7.2 CRL のプロファイル

本項に示すプロファイルのデータフォーマットについては、IETF RFC 5280 に準拠するものとし、そのプロファイルは以下の通りである。

(1)CRL のプロファイル（NII Open Domain CA - G4）

表 7-2-1-1 証明書失効リスト（CRL）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN=NII Open Domain CA - G4	-
This Update		例) 2018/01/01 00:00:00 GMT	-
Next Update		例) 2018/01/05 00:00:00 GMT ＊ 実更新間隔 24 時間、有効期間 96 時間	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2018/03/01 12:00:00 GMT	-
	Reason Code	当該エントリの指定は任意とする。指定する場合、CRLReason は以下のものから選択するものとする: Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) Cessation of operation(運用停止)	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

(2)CRL のプロファイル（NII Open Domain CA - G5）

表 7-2-2-1 証明書失効リスト（CRL）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-
	Common Name	CN=NII Open Domain CA - G5	-
This Update		例) 2018/01/01 00:00:00 GMT	-
Next Update		例) 2018/01/05 00:00:00 GMT ＊ 実更新間隔 24 時間、有効期間 96 時間	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2018/03/01 12:00:00 GMT	-
	Reason Code	当該エントリの指定は任意とする。指定する場合、CRLReason は以下のものから選択するものとする: Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) Cessation of operation(運用停止)	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

(3)CRL のプロファイル（NII Open Domain CA - G6）

表 7-2-3-1 証明書失効リスト（CRL）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= National Institute of Informatics	-

	Common Name	CN=NII Open Domain CA - G6	-
This Update		例) 2018/01/01 00:00:00 GMT	-
Next Update		例) 2018/01/05 00:00:00 GMT ＊ 実更新間隔 24 時間、有効期間 96 時間	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2018/03/01 12:00:00 GMT	-
	Reason Code	当該エントリの指定は任意とする。指定する場合、CRLReason は以下のものから選択するものとする: Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) Cessation of operation(運用停止)	-
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

(4)CRL のプロファイル（NII Open Domain S/MIME CA）

表 7-2-4-1 証明書失効リスト（CRL）

基本領域		設定内容	critical
Version		Version 2	-
Signature Algorithm		sha256WithRSAEncryption	-
Issuer	Country	C=JP	-
	Locality	L=Academe	
	Organization	O= National Institute of Informatics	-
	Common Name	CN= NII Open Domain S/MIME CA	-
This Update		例) 2018/04/01 00:00:00 GMT	-
Next Update		例) 2018/04/05 00:00:00 GMT ＊ 実更新間隔 24 時間、有効期間 96 時間	-
Revoked Certificates	Serial Number	例) 0123456789	-
	Revocation Date	例) 2018/04/01 12:00:00 GMT	-
	Reason Code	当該エントリの指定は任意とする。指定する場合、CRLReason は以下のも	-

		のから選択するものとする: Key Compromise(鍵危殆化) Affiliation Changed(内容変更) superseded(証明書更新による破棄) Cessation of operation(運用停止)	
拡張領域		設定内容	critical
CRL Number		CRL 番号	n
Authority Key Identifier		発行者公開鍵の SHA-1 ハッシュ値（160 ビット）	n

7.2.1 バージョン番号

本 CA は、CRL バージョン 2 を適用する。

7.2.2 CRL 拡張

本 CA が発行する CRL 拡張フィールドを使用する。

7.3 OCSP のプロファイル

本 CA は、RFC2560、5019 又は 6960 に準拠する OCSP サーバを提供する。

7.3.1 バージョン番号

本 CA は、OCSP バージョン 1 を適用する。

7.3.2 OCSP 拡張

本 CP「7.1 証明書のプロファイル」に記載する。

8. 準拠性監査とその他の評価

8.1 監査頻度

本 CA は、本 CA の運用が本 CP に準拠して行われているかについて、1 年以内に 1 度以上、監査を行う。

8.2 監査者の身元・資格

準拠性監査は、監査に必要な知識を有し、CA 運用業務に関与しない第三者が行うものとする。

8.3 監査者と被監査者の関係

監査人は、監査に関する事項を除き、被監査部門の業務から独立した立場にあるものとする。監査の実施にあたり、被監査部門は監査に協力するものとする。

8.4 監査テーマ

監査は、本 CA の運用に関して、本 CP に対する準拠性を中心とする。

8.5 監査指摘事項への対応

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う。

8.6 監査結果の通知

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、本 CA 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、及び NII が承認した場合を除き、監査結果を外部へ開示することはない。

9. 他のビジネス的・法的問題

9.1 料金

9.1.1 証明書の発行または更新にかかる料金

NII が別に定める各種規程にて定める。

9.1.2 証明書のアクセス料金

NII が別に定める各種規程にて定める。

9.1.3 失効またはステータス情報のアクセス料金

NII が別に定める各種規程にて定める。

9.1.4 他サービスの料金

NII が別に定める各種規程にて定める。

9.1.5 返金ポリシ

NII が別に定める各種規程にて定める。

9.2 財務上の責任

9.2.1 保険の補償

本 CA は、本 CA の運用維持にあたり、十分な財務的基盤を維持するものとする。

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の保険または保証範囲

規定しない。

9.3 機密情報の保持

9.3.1 秘密情報の範囲

NII が保持する個人及び組織の情報は、証明書、CRL、本 CP 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。NII は、法の定めによる場合及び証明書利用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、NII 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。また、研究所の合併、再編成に関連してアドバイスする弁護士、会計士、金融機関及びその他の専門家に対しても、NII 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 秘密情報範囲外の情報

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。

- NII 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
- NII 以外の出所から、機密保持の制限無しに NII に知られた、あるいは知られるようになった情報
- NII によって独自に開発された情報
- 開示に関して利用管理者及び利用者によって承認されている情報

9.3.3 秘密情報を保護する責任

NII は、法の定めによる場合、利用管理者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 個人情報のプライバシー保護

9.4.1 個人情報保護方針

NII は、当研究所の CA サービスから収集した個人情報を、申請内容の確認、必要書類等の送付、権限付与対象者の確認など CA の運用に必要な範囲で利用する。NII の個人情報保護方針については、NII のホームページ（http://www.rois.ac.jp/pdf/kojinkitei.pdf）において公表する。

9.4.2 個人情報として扱われる情報

NII の個人情報保護方針に規定する。

9.4.3 個人情報とみなされない情報

NII の個人情報保護方針に規定する。

9.4.4 個人情報を保護する責任

NII の個人情報保護方針に規定する。

9.4.5 個人情報の使用に関する通知と同意

NII の個人情報保護方針に規定する。

9.4.6 司法または行政手続に沿った情報開示

NII の個人情報保護方針に規定する。

9.4.7 その他の情報開示条件

NII の個人情報保護方針に規定する。

9.5 知的財産権

本 CP、本 CA から発行する証明書は著作権を含み、NII の権利に属するものとする。

9.6 表明保証

9.6.1 本 CA の義務と責任

(1) 本 CA の運営

本 CA は、CPS に基づき本 CA の運営を行う。

(2) 本 CA 業務の委託

業務の一部又は全部を外部に委託する場合、本 CA は、委託者に本 CA の運営主体が定める本 CP、CPS の遵守及び個人情報の厳正な取り扱いを遵守させなければならない。

(3) 証明書の発行及び失効

本 CA は、RA からの適切な証明書発行指示、失効指示に基づき証明書発行及び失効を行う。

(4) 本 CA 秘密鍵の保護

本 CA の秘密鍵を適切に管理し、発行した証明書及び証明書失効情報の信頼の確保を行う。

(5) リポジトリの公開

リポジトリにて本 CA に関する情報を公開する。

(6) 秘密情報の取り扱い

本 CA は、本 CP 及び CPS に基づき、秘密情報を適切に取り扱う。

(7) 監査

本 CA が実施する認証業務について定期的に監査を行う。

9.6.2 RA の義務と責任

(1) RA の運営

RA は、本 CP に基づき運営を行う。

(2) 登録担当者からの申請確認

RA は、登録担当者からの申請であることを本 CP の本人性及び実在性の確認方法に基づき、申請を行う者の確認を実施する。

(3) 証明書の発行及び失効指示

RA は、本項「(2) 登録担当者からの申請確認」による申請を確認した後、IA に証明書発行及び失効の指示を行う。

9.6.3 機関、登録担当者、利用管理者及び利用者の義務と責任

9.6.3.1 機関の義務と責任

(1) 登録担当者の実在性の確認

NII が別に定める手続きにもとづき、登録担当者の実在性を保証し、登録担当者の存在確認の義務を負う。

(2) ドメインの本人性確認

NII が別に定める手続きにもとづき、機関で取り扱うドメインについて、当該機関の所有するドメインであり、また証明書の発行を受けることについて機関の許諾を得ていることの義務を負う。

9.6.3.2 登録担当者の義務と責任

(1) 利用管理者及び利用者の本人性・実在性の確認

本 CA が発行する証明書について、登録担当者は利用管理者及び利用者の本人性・実在性を保証し、利用管理者及び利用者の存在確認の義務を負う。

(2) 証明書の失効承認

本 CA が発行する証明書において登録担当者は、利用管理者から失効申請に承認を求められた場合、失効事由が適切であることを確認の上、承認する。

(3) サーバの実在性の確認

本 CA が発行するサーバ証明書について、登録担当者はサーバがサービス利用機関の所有又は管理下にあり、利用管理者及び利用者がサーバの管理者であることを保証し、サーバの実在確認の義務を負う。

9.6.3.3 利用管理者及び利用者の義務と責任

(1) サーバの本人性の確認

利用管理者及び利用者は、サーバの鍵ペアのうち秘密鍵がサーバ外部へ漏れ

ないよう管理する義務を負う。

(2) 証明書の適切な使用

利用管理者及び利用者は、本 CP「1.4 証明書の使用方法」で規定された証明書用途を遵守する。

(3) 証明書記載事項の管理

利用管理者及び利用者は発行された証明書の記載事項を受領時に確認し、記載事項に誤りがあった場合には、直ちに登録担当者を介して本 CA に連絡する。

(4) 秘密鍵の危殆化についての届出

利用管理者及び利用者は、秘密鍵が危殆化している、又はその疑いがある場合は、直ちに登録担当者を介して本 CA に証明書の失効申請を行う。

(5) 証明書の利用停止の届出

利用管理者及び利用者は、証明書の利用を停止する場合、直ちに登録担当者を介して本 CA に証明書の失効申請を行う。

(6) 秘密鍵の破棄

利用管理者及び利用者は、失効時において、又は秘密鍵の危殆化若しくはその疑いがある場合、直ちに証明書の利用を停止し秘密鍵を完全に破棄する。

(7) 本 CA による失効

利用管理者及び利用者は、本 CA の判断により、証明書が失効されることがあることを承諾する。

(8) 証明書記載事項の変更

利用管理者及び利用者は、証明書記載事項に変更があった場合は、登録担当者を介して、失効申請と、必要に応じて証明書の再発行の手続きを行う。

9.6.4 検証者の義務と責任

(1) CP 及び CPS への同意

検証者は、本 CA が発行する証明書の検証において本 CP 及び CPS へ同意しなければならない。

(2) 証明書の有効性確認

検証者は、本 CA が発行する証明書の有効性を確認しなければならない。

9.6.5 他の関係者の表明保証

規定しない。

9.7 限定保証

本 CA は、本 CP「9.6.1 本 CA の義務と責任」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、付随的損害又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、データの紛失又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「9.6.1 本 CA の義務と責任」の内容に関し、次の場合、本 CA は責任を負わないものとする。

・本 CA に起因しない不法行為、不正使用又は過失等により発生する一切の損害
・利用管理者、利用者及び検証者が自己の義務の履行を怠ったために生じた損害
・利用管理者及び利用者のシステムに起因して発生した一切の損害
・本 CA、利用管理者及び利用者のハードウェア、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
・利用管理者及び利用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われ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、利用管理者及び利用者には、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する。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 文書の有効期間と終了

9.10.1 文書の有効期間

本 CP は、NII の承認により有効となる。本 CP「9.10.2 終了」に規定する終了以前に本 CP が無効となることはない。

9.10.2 終了

本 CP は、本 CA の終了と同時に無効となる。

9.10.3 終了の影響と存続条項

サービス利用機関と本 CA との間で利用契約等を終了する場合、又は、本 CA 自体を終了する場合であっても、その性質上存続されるべき条項は終了の事由を問わず利用管理者、利用者、検証者及び本 CA に適用されるものとする。

9.11 関係者間の個々の通知と連絡

本 CA は、利用管理者、利用者及び検証者に対する必要な通知をホームページ上（https://certs.nii.ac.jp）、電子メール又は書面等によって行う。

9.12 改訂

9.12.1 改訂手続き

本 CP は、本 CA の判断によって適宜改訂され、NII の承認によって発効するものとする。

9.12.2 通知方法と期間

本 CP を変更した場合、速やかに変更した本 CP を公表することにより、利用管理者、利用者及び検証者に対しての告知とする。利用管理者、利用者及び検証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 は利用管理者、利用者及び検証者に同意されたものとみなす。

9.12.3 OID の変更

NII が必要であると判断した場合に、OID を変更する。

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、利用管理者、利用者及び検証者の所在地にかかわらず、本 CP 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 適用される法律の遵守

本 CA は、国内における各種輸出規制を遵守し、暗号ハードウェアおよびソフトウェアを取扱うものとする。

9.16 雑則

規定しない。

9.16.1 完全合意条項

本 CA は、本サービスの提供にあたり、証明書利用者または検証者の義務等を本 CP、サービス利用規定、および CPS によって包括的に定め、これ以外の口頭であると書面であるとを問わず、いかなる合意も効力を有しないものとする。

9.16.2 権利譲渡条項

本 CA は、本サービスを第三者に譲渡する場合、本 CP、サービス利用規定、および CPS において記載された責務およびその他の義務の譲渡を可能とする。

9.16.3 分離条項

本 CP、サービス利用規定、および CPS の一部の条項が無効であったとしても、当該文書に記述された他の条項は有効であるものとする。

9.16.4 強制執行条項

本サービスに関して紛争が発生した場合の第一審専属管轄裁判所は東京地方裁判所とする。

9.16.5 不可抗力

本 CA は、天変地異、地震、噴火、火災、津波、水災、落雷、動乱、テロリズム、その他の不可抗力により生じた一切の損害について、その予見可能性の有無を問わず一切責任を負わないものとし、本 CA の提供を不可能にするに至ったときは、本 CA はその状況の止むまでの間、本 CA を停止することができる。

9.17 その他の条項

規定しない。