

H 「ポリシーの検討」

－ 目 次 －

1. 章 電子証明書ポリシー	3
1.1 はじめに	3
1.2 公開とリポジトリの責任	5
1.3 識別と認証.....	5
1.4 証明書のライフサイクルに対する運用上の要件.....	7
1.5 設備上、運営上、運用上の管理	9
1.6 技術的セキュリティ管理	10
1.7 証明書、及びCRLのプロファイル	10
1.8 準拠性監査とその他の評価	10
1.9 他の業務上の問題、及び法的問題.....	10
1.10 定義語	12
1.11 添付資料-1 (証明書プロファイル)	14
1.12 添付資料-2 (CRLプロファイル)	20

1 章 電子証明書ポリシー

1. 章 電子証明書ポリシー

1.1 はじめに

JCAN 共通 CP「JCAN ビジネス CP」は、JCAN 及び JCAN パートナー認証局（以下「JCAN パートナーCA」という）が発行する証明書の利用目的、適用範囲、利用者手続き等、JCAN が取り扱う証明書に関する共通のポリシーを規定するものである。

JCAN パートナーCA の運用に関する諸手続きは、JCAN 共通 CPS に規定する。

1.1.1 概要

本 CP は、JCAN 及び JCAN パートナーCA 及び JCAN パートナーCA から発行されるすべてのエンドエンティティ証明書（以下「EE 証明書」という）に適用される。本 CP の目的は、JCAN の証明書の利用目的、適用範囲、証明書の種類と用途を示し、証明書の発行に付随する要件を示すことである。

1.1.2 JCANが取り扱う証明書タイプ

本 CP で取り扱う証明書タイプは、以下のとおりである。総称して「JCAN 証明書」と呼ぶ。

(1) パートナーCA証明書

JCAN CA により認定されたパートナーCA の CA 証明書である。パートナーCA 証明書は以下の 2 通りで発行される。

- ・ JCAN ルート CA 又は JCAN 中間 CA から発行される
- ・ WebTrust の認定をうけているパブリック認証局から発行される

何れの場合も、パートナーCA 証明書の発行に当たっては、本 CP が定める証明書プロファイルに準拠しなければならない。なお、パートナーCA 証明書の発行に当たっての諸手続きは、パートナーCA 証明書の発行元認証局が個別に CPS に規定する。

(2) JCANビジネス証明書

JCAN は、幾つかのタイプの個人及び組織が使用する EE 証明書を提供する。これらの証明書は、認証サービス、セキュア電子メール、及び組織内、組織間、インターネットでの金額を伴わない取引で利用者を認証することに利用できる。JCAN が取扱う証明書（以下「JCAN 証明書」という）のタイプを下記に示す。

- (a) 企業／団体内個人及びそれに結びつく属性（肩書き等）を証明する証明書
- (b) 企業／団体の組織（部門名、役割）であることを証明する証明書
- (c) 企業／団体の設備であることを証する証明書

1.1.3 文書名と識別

本 CP の正式名称は“JCAN 共通 CP「JCAN ビジネス CP」”である。

1.1.4 PKIの関係者

(1) JCANルート認証局

JCAN ルート認証局（以下「JCAN ルート CA」という）は、本 CP を含め、JCAN が取り扱う証明書の全てのポリシーを起草する責任を負うポリシー管理局である。

(2) パートナー認証局

パートナーCAは、本 CP が定めるポリシーに従い、2.1.2.に記載の証明書（以下「JCAN 証明書」という）を、その利用目的、適用範囲、手続き等に準拠して発行する JCAN が認定する認証局である。

(3) 登録局

パートナーCAは登録局を通じて利用者に連絡をする。登録局は本 CP の下、証明書を申請する利用者の実在性確認と本人性確認の審査を行い、証明書の発行と失効のための登録業務を行う。

(4) 利用者

JCAN 認証サービスの利用者は、認証局から 2.1.2.の (2) に記載の EE 証明書の発行をうける主体である。なお、証明書の発行をうける主体が組織または設備である場合は、利用者は指定された組織内の個人である。

(5) サブジェクト（利用者識別情報）

JCAN 認証サービスの EE 証明書のサブジェクトは、企業／団体に属する、個人、部門、及び設備である。

(6) 証明書申請者

証明書申請者は、サブジェクトの代わりに認証局の利用者規約に同意し、証明書を申請する者である。

証明書申請者は、以下の通りである。

- ・ サブジェクトが個人である場合は、サブジェクト自身である。
- ・ サブジェクトが組織である場合は、組織・法人に属する個人である。
- ・ サブジェクトが設備である場合、設備を管理する組織・法人に属する個人である。

(7) 検証者

検証者は、利用者の証明書を信頼する者、又は利用者の電子署名を信頼する者である。証明書の有効性を検証するために、検証者は必ず認証局失効情報を参照しなければならない。

1.1.5 証明書の用途

(1) 用途

JCAN 証明書は、1.2.2 に記載される範囲で、認証サービス、セキュア電子メール、及び組織内、組織間、インターネットでの金額を伴わない取引で利用者を認証することに利用できる。

(2) 適切な証明書の用途

JCAN 証明書は、本 CP に記載の範囲での適切な用途に利用できる。その他の許可されない用途への利用は、認証局が提供する保証の対象から外れる場合がある。

1.1.6 ポリシー管理

JCAN ルート CA は、JCAN の領域内の証明書サービスを管理する最上位のポリシー管理局（トラストアンカーとも呼ばれる）である。JCAN ルート CA が本 CP を管理する。

1.2 公開とリポジトリの責任

1.2.1 リポジトリ

JCAN は、発行する証明書に関する情報をリポジトリに公開する。JCAN は、本 CP を含む、その業務手続、特定のポリシーの内容について、リポジトリに一定の開示を行う。

1.2.2 証明書情報の公開

JCAN は、次の内容をリポジトリに公開し、証明書利用者及び検証者がオンラインで参照できるようにする。

- ・ CRL
- ・ 本 CA 証明書
- ・ 最新の CP、CPS
- ・ 本 CA が発行する証明書に関するその他の情報

1.2.3 公開の時期と頻度

本 CP 及び CPS は更新の都度、公開される。CRL は失効情報に変更がある都度と、CRL の有効期限内で定期的に更新される。

なお、証明書の有効期限を過ぎたものは CRL から削除される。

1.3 識別と認証

JCAN CA 及びパートナーCA は、証明書の発行の前に、認証局への証明書申請者の本人識別と他の属性を審査し、認証する業務手続文書を保持する。

1.3.1 名前決定

JCAN は、利用者を本人識別するために、例えば X.500 の Distinguished Names、RFC 822 の Names、及び X.400 の Names のように、サブジェクトに割り当てられた名前のタイプを含む、特定の命名と本人識別の規則に従う。

パートナーCA 証明書を申請する場合、申請者の名前は、申請者を表す正式な名称でなければならない。

1.3.2 初回の本人確認

(1) 秘密鍵の所有を検証する方法

証明書利用者が鍵ペアを生成する場合、秘密鍵を所有していることの検証は以下の方法で行う。証明書署名要求ファイル（以下「CSR」という）の署名検証を行い、CSRの公開鍵に対応する秘密鍵で署名されていることを確認する。

(2) 組織の認証

JCANは、組織の認証を、標準企業コード（証券コード、TDB企業コード、指定団体発行コード）と、国や地方公共団体が発行する公的書類、国や地方公共団体が管理する信頼できるデータベース（以下「QGIS」という）、JCANが信頼する第三者データベース（以下「QIIS」という）、JCANが独自に保有する組織に関するデータベース、その他JCANのポリシー管理局が同等の信頼性があると判断した方法によって実施する。

(3) パートナーCA証明書申請時の権限確認

JCANは、パートナーCA証明書の申請があった場合、「3.2.2 組織の認証」に記載の方法による組織の認証後、当該申請における申請者と承認者の権限確認を行う。

(4) RA管理者の認証

JCAN CAは、パートナーCAのRA管理者用証明書の発行に際し、「3.2.2 組織の認証」に記載の方法による組織の認証と、当該組織の代表者によるRA管理者の指名の事実を確認する。

(5) パートナーCAから発行するEE証明書の本人確認

エンドエンティティ証明書の発行に際しては、パートナー登録局にて本人確認を行う。本人確認は企業/団体に保有する人事台帳、体制表、資産台帳での確認を行う。

- ・ 台帳、体制表による確認
- ・ EE証明書の申請者の確認

(6) 利用者の登録に必要な情報

(a) 企業／団体内個人及びそれに結びつく属性（肩書き等）を証明する証明書

個人、肩書きの正式名称

(b) 企業／団体の組織（部門名、役割）であることを証明する証明書

部門名、役割名の正式名称

(c) 企業／団体の設備であることを証する証明書

設備の名称、管理番号等、設備を特定する情報

(7) 利用者の登録の記録

認証局は、検証に使用した文書に記載された参照番号と、その有効性に関する制限を含む、利用者の本人識別を検証するために使用した全ての情報を記録する。

認証局は上記に示された記録を証明書の有効期限が切れた後、少なくとも5年間保存する。

1.3.3 鍵の再生成申請時の利用者の本人確認

(1) 通常の鍵更新における本人性確認と認証

鍵更新における証明書利用者の本人確認は、「3.2 初回の本人確認」に準拠する。

1.3.4 失効申請時の本人性確認と認証

証明書の失効要求における本人識別と認証手続として、失効要求をする利用者の署名入り依頼書を要求する。

1.4 証明書のライフサイクルに対する運用上の要件

登録局、利用者、その他 JCAN 領域内の全てのエンティティは、証明書が有効期限切れになるか、失効されるまでの運用期間中、かかる証明書に記載される情報の全ての変更について、登録局を介して当該認証局に報告する継続的な義務を負う。

認証局は、登録局により提出される署名入りの要求に従って、証明書を発行／失効する。

パートナーCA は、その業務を実施するため、第三者の代理人を使用することがある。この場合、パートナーCA は、認証局業務のサービス提供に関する代理人の作為と不作為に対する全責任と説明責任を負う。

1.4.1 証明書申請手順

登録局は証明書申請を受けて、申請者の本人識別を検証する。続いて、登録局は証明書申請を承認又は棄却する。

1.4.2 証明書発行

証明書申請の検証後、登録局は、認証局に証明書発行要求を送信する。登録局からの要請は、有効に作成され、有効な利用者データが含まれ、認証局の仕様に合致していれば、承認される。発行された証明書は、サブジェクトに配送される。

(1) 証明書生成

証明書の発行及び更新に関して、認証局は、全ての当事者に対し、以下に規定される条件に従って、証明書が安全に発行する。

- ・ 認証局は、認証局の領域内において利用者に割り当てられた識別名の唯一性を保証する。
- ・ 登録データの機密性と完全性は、常時、適切な手段によって保証される。
- ・ 登録機関の認証は、その機関に発行される適切な信用証明を通じて保証される。

1.4.3 証明書の受領

発行された証明書は、認証局が発行する証明書の受領を登録局が確認した時点で、利用者により受領されたと見なされる。

1.4.4 鍵ペアと証明書の用途

(1) 利用者による秘密鍵、及び証明書の使用

(a) 利用者の義務

利用者の義務は以下の通り。

- ・ JCAN リポジトリに公開された本 CP の諸条件を承諾すること
- ・ 証明書の信頼性に重大な影響を及ぼす情報の変更は、認証局又は登録局に、速やかに知らせること
- ・ 証明書が有効でなくなった場合は、使用をやめること
- ・ 証明書を、合理的な環境下で使用すること
- ・ 秘密鍵を危殆化、紛失、不正開示、改ざん、その他の不正使用から防護すること
- ・ 秘密鍵を適切に保護すること
- ・ 証明書の完全性に重大な影響を及ぼす事象が発生した場合、当該証明書の失効を要求すること
- ・ 証明書を不正操作から防護すること
- ・ CP 及び利用規約に従って法例を遵守し、許可された用途にのみ、証明書を使用すること
- ・ 利用者は、常に上記に述べた認証局に対する義務を負う。

(b) 電子証明書のライフサイクル運用要件

利用者は、認証局証明書の有効期間中における認証局証明書に記載された情報についての全ての変更、又は証明書の有効性に重大な影響を及ぼす事実を、直接登録局に知らせる継続的な義務を負う。

(c) 自己責任での信頼

JCAN CA リポジトリに掲示される情報を適切に評価し信頼することは、当事者自身の責任である。

(2) 検証者による公開鍵、及び証明書の使用

検証者の義務は以下の通りである。

(a) 検証者の義務

証明書の検証者は、以下を実施する。

- ・ 認証局が公開する証明書ステータス情報を使用して、認証局証明書を検証する。
- ・ かかる検証手続により、証明書に記載された情報が正しく、最新であると検証できたときに限り証明書を信頼する。
- ・ JCAN CA 証明書を、合理的な環境下でのみ信頼する。

(b) JCAN CA リポジトリとウェブサイトの条件

認証局のリポジトリ及びウェブサイトにアクセスする利用者及び検証者は、本 CP の条項、及び認証局が供する他の使用条件を承諾する必要がある。

リポジトリの使用により、以下のことが可能になる。

- ・ 認証局証明書の検索の結果、情報を取得すること
- ・ 証明書に含まれる公開鍵に対応する秘密鍵を使用して生成された電子署名のステータスを検証すること

- ・ 認証局のウェブサイトに公開される情報を取得すること

1.4.5 証明書の更新

JCAN の証明書は、鍵更新を伴わない証明書の更新には対応しない。鍵更新を伴う証明書の更新は、「2.3.3 鍵の再生成申請時の利用者の本人確認」による。

1.4.6 証明書の失効

登録局からの要請を受けて、認証局は、次のような場合に認証局証明書を失効する。

- ・ 証明書サブジェクトの秘密鍵の紛失、盗難、不正開示、その他の危殆化があった場合
- ・ 証明書サブジェクト又はその指名した利用者が、本 CP の下の重大な義務に違反した場合
- ・ 本 CP の義務の履行遂行が、自然災害、コンピュータ又は通信障害、その他制御不能な事象により妨げられ、情報が重大な脅威に晒され危殆化した場合
- ・ 証明書に含まれる、証明書サブジェクトの情報の変更があった場合

1.4.7 証明書のステータス確認サービス

認証局は、CRL、及び適当なウェブインタフェースを含む、証明書ステータス確認サービスを提供する。

1.4.8 利用の終了

利用者の加入は、証明書の失効、有効期限切れ、又はサービスが終了したとき、終了する。

1.5 設備上、運営上、運用上の管理

“規定しない”

1.5.1 物理的管理

“規定しない”

1.5.2 手続的管理

“規定しない”

1.5.3 人事的管理

“規定しない”

1.5.4 監査ログの手続

“規定しない”

1.5.5 記録のアーカイブ

“規定しない”

1.5.6 危殆化、及び災害からの復旧

“規定しない”

1.5.7 認証局又は登録局の終了

“規定しない”

1.6 技術的セキュリティ管理

“規定しない”

1.6.1 鍵ペアの生成、及びインストール

“規定しない”

1.6.2 鍵ペアの再生成と再インストール

“規定しない”

1.6.3 秘密鍵の保護、及び暗号モジュール技術の管理

“規定しない”

1.6.4 その他の鍵ペア管理

“規定しない”

1.6.5 活性化データ

“規定しない”

1.6.6 コンピュータのセキュリティ管理

“規定しない”

1.6.7 ライフサイクルの技術上の管理

“規定しない”

1.6.8 ネットワークセキュリティ管理

“規定しない”

1.7 証明書、及びCRLのプロファイル

このセクションは、証明書フォーマット、CRL を規定する。

1.7.1 証明書プロファイル

添付資料-1 を参照。

(EE 証明書プロファイル、subCA 証明書プロファイル、RootCA 証明書プロファイル)

1.7.2 CRLプロファイル

添付資料-2 を参照。(CRL プロファイル)

1.8 準拠性監査とその他の評価

“規定しない”

1.8.1 監査の頻度あるいは条件

“規定しない”

1.9 他の業務上の問題、及び法的問題

“規定しない”

1.9.1 料金

“規定しない”

1.9.2 財務的責任

“規定しない”

1.9.3 業務情報の機密性

“規定しない”

1.9.4 個人情報のプライバシー保護

“規定しない”

1.9.5 知的財産権

本 CP 及び CPS を含み JCAN が発行するすべての刊行物の知的財産権について、JCAN はその権利を留保する。

1.9.6 表明保証

“規定しない”

1.9.7 無保証

“規定しない”

1.9.8 責任の制限

“規定しない”

1.9.9 補償

“規定しない”

1.9.10 期間と終了

“規定しない”

1.9.11 関係者間の個別通知と連絡

“規定しない”

1.9.12 改訂

本 CP の変更は、適切に付与する番号を通じて表示する。

JCAN CA のポリシー管理局が、付与するバージョン番号を決定する。

1.9.13 紛争解決手続

“規定しない”

1.9.14 準拠法

“規定しない”

1.9.15 適用法の遵守

“規定しない”

1.9.16 雑則

“規定しない”

1.10 定義語

CA (Certification Authority) : 認証局

証明書の発行・更新・失効、CA 鍵の生成及び証明書利用者のをを行う主体をいう。

CP (Certificate Policy) : 証明書ポリシー

CA が発行する証明書の種類、適用範囲、発行対象、用途等、証明書に関する規程文書をいう。

CPS (Certification Practice Statement) : 認証業務運用規程

CA を運用するうえでの運用手続きやセキュリティ基準を明示した規定文書をいう。

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

証明書の有効期間内にも拘わらず失効された証明書情報を記載したリストをいう。

CSR(Certificate Signing Request) : 証明書署名要求

申請者から認証局へ、証明書を要求する際に送られる機械可読の申込書式をいう。

QGIS(Qualified Government. Information Source) : 行政機関の信頼情報源

EV ガイドラインで認められている「信頼できる行政機関の情報源」をいう。オンラインで公開され、定期的に更新される、行政機関が運営するデータベースで、データの報告が法律で義務付けられ、虚偽の報告には刑事罰または民事罰が科せられるものをいう。

QIIS(Qualified Independent Information Source) : 第三者機関の信頼情報源

EV ガイドラインで認められている「信頼できる独立した第三機関の情報源」をいう。オンラインで公開され、定期的に更新される民間機関が運営するデータベースをいう。

X.400

ITU-TS の勧告の一つで電子メールについての標準を定めたもの。

X.500

ITU-T が定めた、ネットワーク上での分散ディレクトリサービスに関する規格。X.509 は公開鍵認証の標準形式を規定している。

アーカイブ

複数のファイルを一つのファイルにまとめたファイルをいう。

サブジェクト（利用者識別情報）

利用者を識別するための情報をいう。

タイムスタンプ

ファイルなどの電子データにおいて、その作成や更新などが行われた日時を示す情報。PKIの仕組みによって正確な日時、存在証明、非改ざん証明を行える。

パートナーCA：パートナー認証局

JCAN ルートによる認証を受け、JCAN エンドエンティティ証明書を発行するサービスを行う認証局をいう。

証明書プロファイル

汎用的な x.509 証明書に対して、証明書の使用方法が明記されていることをいう。

リポジトリ

証明書及び他の関連情報を列挙する、オンラインで利用できるデータベース及び/又はディレクトリをいう。

ルートCA：ルート認証局

電子証明書の認証局の種類の一つで、上位の認証局による認証を受けず、自分の正当性を自ら証明する認証局をいう。

中間CA：中間認証局

上位の認証局による認証を受けることにより自らの正当性を認証する認証局をいう。

登録局

CAの業務のうち、利用者(申請者)の本人識別と登録業務を行い、発行した証明書を利用者に安全に配布する責任を負う主体をいう。

1.11 添付資料-1 (証明書プロファイル)

EE証明書プロファイル (1/2)

■証明書プロファイル(Basic Certificate Fields)

項目 Certificate Fields	設定	データタイプ	説明	JCANチェック欄			
				形式	内容		
Version		INTEGER	v3 のため「2」			必須	
SerialNumber		INTEGER	CAが割り当てる一意な番号			必須	
Signature		AlgorithmIdentifier	SHA-256withRSAEncryption (1.2.840.113549.1.1.11)			必須	
Validity		Validity	証明書の有効期間(1年、他任意)要検討			必須	
	NotBefore	UTCTime	YymmddhhmmssZ(年月日時間分秒Z) ※発行判断を行った時から6か月以内の任意の日時			必須	
	NotAfter	UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須	
Issuer		Name	電子証明書を発行した機関(CA)の名前、X.500 識別名(DN)で記述 CA 証明書に含まれる subject と同じDNを記述			CA証明書に依存?	
	CountryName	PrintableString	JP			必須?	
	StateName	PrintableString	Tokyo			オプション?	
	LocalityName	PrintableString	Minato-Ku			オプション?	
	OrganizationName		オブジェクト識別子(OID)	2.5.4.10			
			PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code(0147506022) or ISO/IEC8824_OID(1.2.392.200063)			必須?
	OrganizationUnitName		オブジェクト識別子(OID)	2.5.4.11			
		PrintableString	Head Quarter			必須?	
CommonName		オブジェクト識別子(OID)	2.5.4.3			必須?	
		PrintableString	JIPDEC Head Quarter CA1				
Subject		Name	電子証明書の所有者の名前 ユーザの名前やサーバ名などを記述				
	CountryName	PrintableString	JP			必須	
	StateName	PrintableString	【OP: Option】 Tokyo			オプション	
	LocalityName	PrintableString	【OP】 Minato-Ku			オプション	
	OrganizationName		オブジェクト識別子(OID)	2.5.4.10			
			PrintableString	ID_1.2.392.200063_JIPDEC			必須
	OrganizationUnitName		オブジェクト識別子(OID)	2.5.4.11			
			PrintableString	+81-3-3436-7500.www.jipdec.or.jp ※64文字以内に制限			必須
CommonName		オブジェクト識別子(OID)	2.5.4.3			必須	
		PrintableString	BN_shunin_shizaibu				
SerialNumber		INTEGER	10.1023.20100137 ※管理番号			必須	
SubjectPublicKeyInfo			証明書所有者(主体者)の公開鍵に関する情報				
	Algorithm	AlgorithmIdentifier	1.2.840.113549.1.1.1(rsaEncryption)			必須	
	SubjectPublicKey	BIT STRING	2048bitの公開鍵			必須	

■証明書プロフィール(Standard Certificate Extensions)

項目	設定 criticality	データタイプ	説明	JCANチェック欄		
				形式	内容	
authority Key Identifier	FALSE	オブジェクト識別子 (OID) OCTET STRING	2.5.29.35 RFC5280 4.2.1.2 に基づくSHA-1ハッシュ値			必須
subjectKeyIdentifier	FALSE	オブジェクト識別子 (OID) OCTET STRING	2.5.29.14 RFC5280 4.2.1.2 に基づくSHA-1ハッシュ値			必須
KeyUsage	TRUE	オブジェクト識別子 (OID)	2.5.29.15			必須
DigitalSignature		BIT STRING	1			必須
NonRepudiation		BIT STRING	1			必須
KeyEncipherment		BIT STRING	1			必須
DataEncipherment		BIT STRING	1			必須
KeyAgreement						
KeyCertSign						
CRLSign						設定しない
EncipherOnly						
extendedKeyUsage	FALSE	オブジェクト識別子 (OID)	2.5.29.37			必須
clientAuth		オブジェクト識別子 (OID)	1.3.6.1.5.5.7.3.2			必須
emailProtection		オブジェクト識別子 (OID)	1.3.6.1.5.5.7.3.4			必須
msSmartcardLogin		オブジェクト識別子 (OID)	1.3.6.1.4.1.311.20.2.2			オプション
msEncryptionFileSystem		オブジェクト識別子 (OID)	1.3.6.1.4.1.311.10.3.4			オプション
certificatePolicies	FALSE	オブジェクト識別子 (OID)	2.5.29.32			必須
policyIdentifier						
certPolicyId		オブジェクト識別子 (OID)	1.2.392.200121.1.1.1			必須
policyQualifiers						
policyQualifierID		オブジェクト識別子 (OID)	1.3.6.1.5.5.7.2.1(id-qt-cps)			必須
qualifier		IA5String	https://www.iiddec.or.jp/ra/repository/			必須
policyQualifierID		オブジェクト識別子 (OID)	1.3.6.1.5.5.7.2.2(id-qt-unotice)			必須
qualifier		UTF8String	JCAN Business CP			必須
subjectAltName	FALSE	オブジェクト識別子 (OID)	2.5.29.17			必須
DirectoryName						
countryName		PrintableString	JP			オプション
organizationName		UTF8String	一般財団法人日本情報経済社会推進協会			オプション
organizationalUnitName		UTF8String	資材部、主任			オプション
commonName		UTF8String	日本太郎			オプション
rfc822Name		IA5String	nihon-taro@jpdec.or.jp			必須
OtherName						
UPN(プリンシパル名)		オブジェクト識別子 (OID)	1.3.6.1.4.1.311.20.23			オプション
UPN(プリンシパル名)		UTF8String	ActiveDirectoryのプリンシパル名			オプション
issuerAltName	FALSE	オブジェクト識別子 (OID)	2.5.29.18			必須
DirectoryName						
countryName		PrintableString	JP			必須
organizationName		UTF8String	一般財団法人日本情報経済社会推進協会			オプション
organizationalUnitName		UTF8String	本部			オプション
subjectDirectoryAttributes	FALSE					
attrType						将来使う?
attrValues						
cRLDistributionPoints	FALSE	オブジェクト識別子 (OID)	2.5.29.31			必須
distributionPoint						
FullName		オブジェクト識別子 (OID)	2.23.42.2.0			必須
uniformResourceIdentifier		IA5String	http://*****			必須
authorityInfoAccess	FALSE	オブジェクト識別子 (OID)	1.3.6.1.5.5.7.1.1			必須
AccessMethod		オブジェクト識別子 (OID)	1.3.6.1.5.5.7.48.2			必須
AccessLocation UniformResourceIdentifier		IA5STRING	"http://*****"			必須
netscape-cert-type	FALSE	オブジェクト識別子 (OID) BIT STRING	2.16.840.1.113730.1.1 SSL client, S/MIME			SUNIに確認中 当面入れておく

■証明書プロファイル(Basic Certificate Fields)

項目 Certificate Fields	設定	データタイプ	説明	JCANチェック欄			
				形式	内容		
Version		INTEGER	v3 のため「2」			必須	
SerialNumber		INTEGER	CAが割り当てる一意な番号			必須	
Signature		AlgorithmIdentifier	SHA-256withRSAEncryption (1.2.840.113549.1.1.11)			必須	
Validity		Validity	証明書の有効期間(10年?) CA階層を考慮			必須	
	NotBefore	UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須	
	NotAfter	UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須	
Issuer		Name	電子証明書を発行した機関(CA) の名前、X.500 識別名(DN) で記述			必須	
	CountryName	PrintableString	JP			必須	
	StateName	PrintableString	【OP: Option】 Tokyo			オプション	
	LocalityName	PrintableString	【OP】 Minato-Ku			オプション	
	OrganizationName	オブジェクト識別子 (OID)	2.5.4.10				
		PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code(0147506022) or ISO/IEC8824_OID(1.2.392.200063)				必須
	OrganizationUnitName	オブジェクト識別子 (OID)	2.5.4.11				
PrintableString		JCAN Root CA1				必須	
CommonName	オブジェクト識別子 (OID)	2.5.4.3					
	PrintableString	JCAN Root Certificate Authority				必須	
Subject		Name	電子証明書の所有者の名前			必須	
	CountryName	PrintableString	JP			必須	
	StateName	PrintableString	【OP: Option】			オプション	
	LocalityName	PrintableString	【OP】			オプション	
	OrganizationName	オブジェクト識別子 (OID)	2.5.4.10				
		PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code(0147506022) or ISO/IEC8824_OID(1.2.392.200063)				必須
	OrganizationUnitName	オブジェクト識別子 (OID)	2.5.4.11				
		PrintableString	Head Quarter				必須
	CommonName	オブジェクト識別子 (OID)	2.5.4.3				
		PrintableString	JIPDEC Head Quarter CA1				必須
e-Mail							
SerialNumber							
SubjectPublicKeyInfo		SubjectPublicKeyInfo	証明書所有者(主体者)の公開鍵に関する情報			必須	
	Algorithm	AlgorithmIdentifier	1.2.840.113549.1.1.1 (rsaEncryption)			必須	
	SubjectPublicKey	BIT STRING	2048bitの公開鍵				

■証明書プロファイル(Standard Certificate Extensions)

項目	設定 criticality	データタイプ	説明	JCANチェック欄			
				形式	内容		
authority Key Identifier	FALSE	オブジェクト識別子 (OID)	2.5.29.35			必須	
		OCTET STRING	RFC5280 4.2.1.2に基づくSHA-1ハッシュ値				
subjectKeyIdentifier	FALSE	オブジェクト識別子 (OID)	2.5.29.14			必須	
		OCTET STRING	RFC5280 4.2.1.2に基づくSHA-1ハッシュ値				
KeyUsage	TRUE	オブジェクト識別子 (OID)	2.5.29.15			必須	
		DigitalSignature					
		NonRepudation					
		KeyEncipherment					
		DataEncipherment					
		KeyAgreement					
		KeyCertSign	BIT STRING	1			必須
		CRLSign	BIT STRING	1			必須
		EncipherOnly					
extendedKeyUsage							
certificatePolicies	FALSE	オブジェクト識別子 (OID)	2.5.29.32			必須	
		policyIdentifier					
		certPolicyId	オブジェクト識別子 (OID)	ポリシーのOID			
		policyQualifiers					
		policyQualifierID	オブジェクト識別子 (OID)	1.3.6.1.5.5.7.2.1(id-gt-cps)			
		qualifier	IA5String	URL			
		policyQualifierID					
qualifier							
policyMapping						使用しない	
Basic Constraints	TRUE	オブジェクト識別子 (OID)	2.5.29.19			必須	
		CA	BOOLEAN	CA:TRUE PathLenConstraint:0			
subjectAltName		Directory Name				使用しない	
		countryName					
		organizationName					
		organizationalUnitName					
		commonName					
		e-Mail					
issuerAltName		Directory Name				使用しない	
		countryName					
		organizationName					
		organizationalUnitName					
subjectDirectoryAttributes	FALSE	attrType				使用しない	
		attrValues					
cRLDistributionPoints	FALSE	オブジェクト識別子 (OID)	2.5.29.31			必須	
		distributionPoint					
		Full Name	オブジェクト識別子 (OID)	2.23.42.0			
		uniformResourceIdentifier	IA5String	URL			
subjectInfoAccess	FALSE					使用しない	
authorityInfoAccess	FALSE	オブジェクト識別子 (OID)	1.3.6.1.5.5.7.1.1			必須	
		AccessMethod	オブジェクト識別子 (OID)	1.3.6.1.5.5.48.2			
		AccessLocation	IA5String	URL			
netscape-cert-type	FALSE	オブジェクト識別子 (OID)	2.16.840.1.113730.1.1			必須	
				SSL CA 、 S/MIME CA			

RootCA証明書 (1/2)

■証明書プロファイル(Basic Certificate Fields)

項目 Certificate Fields	設定	データタイプ	説明	JCANチェック欄		
				形式	内容	
Version		INTEGER	v3 のため「2」			必須
SerialNumber		INTEGER	CAが割り当てる一意な番号			必須
Signature		AlgorithmIdentifier	SHA-256withRSAEncryption (1.2.840.113549.1.1.11)			必須
Validity		Validity	証明書の有効期間(30年) ~2030年まで			必須
	NotBefore	UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須
	NotAfter	UTCTime	YymmddhhmmssZ(年月日時間分秒Z)			必須
Issuer		Name	電子証明書を発行した機関(CA) の名前、X.500 識別名 (DN) で記述			必須
	CountryName	PrintableString	JP			必須
	StateName	PrintableString	Tokyo			オプション
	LocalityName	PrintableString	Minato-Ku			オプション
	OrganizationName	オブジェクト識別子 (OID)	2.5.4.10			
		PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code (0147506022) or ISO/IEC8824_OID (1.2.392.200063)			必須
	OrganizationUnitName	オブジェクト識別子 (OID)	2.5.4.11			
		PrintableString	JCAN Root CA1			必須
	CommonName	オブジェクト識別子 (OID)	2.5.4.3			
		PrintableString	JCAN Root Certificate Authority			必須
Subject		Name	電子証明書の所有者の名前			必須
	CountryName	PrintableString	JP			必須
	StateName	PrintableString	Tokyo			オプション
	LocalityName	PrintableString	Minato-Ku			オプション
	OrganizationName	オブジェクト識別子 (OID)	2.5.4.10			
		PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code (0147506022) or ISO/IEC8824_OID (1.2.392.200063)			必須
	OrganizationUnitName	オブジェクト識別子 (OID)	2 5 4 11			
		PrintableString	JCAN Root CA1			必須
	CommonName	オブジェクト識別子 (OID)	2 5 4 3			
		PrintableString	JCAN Root Certificate Authority			必須
	e-Mail					
	SerialNumber					
SubjectPublicKeyInfo		SubjectPublicKeyInfo	証明書所有者(主体者)の公開鍵に関する情報			必須
	Algorithm	AlgorithmIdentifier	1.2.840.113549.1.1.1 (rsaEncryption)			必須
	SubjectPublicKey	BIT STRING	2048bitの公開鍵			

RootCA証明書 (2/2)

■証明書プロファイル(Standard Certificate Extensions)

項目	設定 <small>criticality</small>	データタイプ	説明	JCANチェック欄				
				形式	内容			
subjectKeyIdentifier	FALSE	オブジェクト識別子 (OID)	2.5.29.14			必須		
		OCTET STRING	RFC5280 4.2.1.2に基づくSHA-1ハッシュ値					
KeyUsage	TRUE	オブジェクト識別子 (OID)	2.5.29.15			必須		
		DigitalSignature						
		NonRepudation						
		KeyEncipherment						
		DataEncipherment						
		KeyAgreement						
		KeyCertSign	BIT STRING	1				必須
		CRLSign	BIT STRING	1				
EncipherOnly								
Basic Constraints	TRUE	オブジェクト識別子 (OID)	2.5.29.19			必須		
		CA	BOOLEAN	CA:TRUE PathLenConstraint:NULL				

1.12 添付資料-2 (CRLプロファイル)

■CRLプロファイル

項目	設定	データタイプ	説明及び記載情報例	
Version		INTEGER	1 v2	必須
Signature			署名アルゴリズム	
algorithm		OID	1.2.840.113549.1.1.11 sha256RSA	必須
Issuer				
CountryName		PrintableString	JP	必須
StateName		PrintableString	【Option】 Tokyo	オプション
LocalityName		PrintableString	【Option】 Minato-Ku	オプション
OrganizationName		PrintableString	JIPDEC+ID_ISOの体系と連携した企業コード等 ISO/IEC6523_Code (0147506022) or ISO/IEC8824_OID (1.2.392.200063)	必須
OrganizationUnitName		PrintableString	Head Quarter	必須
CommonName		PrintableString	JIPDEC Head Quarter CA1	必須
ThisUpdate		UTCTime	YymmddhhmmssZ 今回の更新日時 例) 2010年1月20日 09:00:00	必須
NextUpdate		UTCTime	YymmddhhmmssZ 次の更新日時 例) 2010年1月27日 09:00:00	必須
Revoked Certificates				
userCertificate		INTEGER	失効される証明書	必須
revocationDate		UTCTime	失効される証明書のシリアルナンバー 失効日時	必須
crlEntry Extensions			失効される証明書毎の拡張領域	
reasonCode			理由コード(コードの説明はIPA:PKI関連技術解説より引用)	
unspecified			0 未指定	
keyCompromise			1 鍵漏洩(鍵危殆化)	
cACompromise			2 CA弱体化(CA危殆化)	オプション
affiliationChanged	FALSE		3 所属変更	(ただし 0、6、8 は使用しない)
superseded			4 破棄	
cessationOfOperation			5 運用停止	
certificateHold			6 証明書保留	
removeFromCRL			8 CRLからの削除	
holdInstructionCode			保留指示コード	
id-holdinstruction-none	FALSE		1 何もしない	使用しない
id-holdinstruction-callissuer			2 発行者に連絡する	
id-holdinstruction-reject			3 証明書を受け付けない	
invalidityDate	FALSE		推定無効日 GeneralizedTime	使用しない
certificateIssuer	TRUE		証明書発行者 間接CRL使用時に設定	使用しない
crlExtensions				
AuthorityKeyIdentifier	FALSE	OCTET String	SHA1ハッシュ値	必須
issuerAltName	FALSE		CRL発行者の別名	使用しない
cRLNumber	FALSE	INTEGER	CRLの通し番号(シーケンシャル)	必須
deltaCrlIndicator	TRUE		デルタCRL使用時に設定	使用しない
issuingDistributionPoint	TRUE		間接CRL使用時に設定	
distributionPoint			配布点	
onlyContainsUserCerts			EE証明書のみ	使用しない
onlyContainsCACerts			CA証明書のみ	
onlySomeReasons			特定の失効理由	
indirectCRL			間接CRL	
freshestCRL	FALSE		デルタCRL使用時に設定	使用しない