日鉄ソリューションズ株式会社
電子証明書発行サービス
証明書ポリシー／認証局運用規程
(Certificate Policy/Certification Practice Statement)

Version 1.04

2022年9月

変更履歴

バージョン	日付	改訂事由
1.00	2019/08/01	初版
1.01	2020/02/01	利用者証明書発行手順修正
1.02	2021/12/15	認証局事務局組織名を修正
1.03	2022/06/01	認証局事務局組織名を修正
1.04	2022/09/27	２．２認証情報の公開 の公開方法を修正

目　　次

１．　はじめに

１．１　目的

この証明書ポリシー／認証局運用規程（以下、「本 CP/CPS」という。）は、日鉄ソリューションズ株式会社（以下、「当社」という。）が定める電子証明書発行サービス（以下、「本サービス」という。）の利用規約（以下、「サービス規約」という。）に基づいて、当社が電子証明書利用者（本 CP/CPS1.4 に定義する。以下、「利用者」という。）へ発行する利用者電子証明書（本 CP/CPS1.5.1（2）に定義する。以下、「利用者証明書」という。）の適切な運用・管理に関する当社のポリシーおよびこのポリシーを運用するための方針、諸手続を定めることを目的とする。

１．２　概要

当社は、本サービスにおいて電子認証局（以下、「本認証局」という。）を設置し、当社の提供する電子契約サービスを利用者が利用するために必要な利用者証明書の発行と管理を行う。

本 CP/CPS は、本認証局が認証業務を行う際の運用に関する規程であり、発行局および登録局を含む本認証局の運用方針、利用者と本認証局との関係、本認証局が利用者に対して発行する利用者証明書の取り扱い等を定めている。利用者証明書の取り扱いには、申請・登録・発行・更新・再発行・失効・有効期間満了に関する記述、および発行方針と利用に関連する要件が含まれる。

当社は、IETF PKIX ワーキンググループが定める RFC3647「Certificate Policy and Certification Practices Framework」のフレームワークに準じて本 CP/CPS を記載する。

本 CP/CPS は、本認証局が発行する電子証明書のプロファイルについても定める。本認証局は、電子証明書毎の証明書ポリシー（以下、「CP」という。）を個別に定めず、本 CP/CPS が CP を包含するものとする。

利用者は、本 CP/CPS の条項に全て同意するものとする。

当社は、ウェブサイト上で変更内容を告知することにより、本 CP/CPS の内容を変更することができるものとする。この場合、告知日以降は、利用者の同意の有無にかかわらず、変更後の規定を適用するものとする。

１．３　文書名称と識別

本CP/CPSの正式名称は、「日鉄ソリューションズ株式会社　電子証明書発行サービス 証明書ポリシー／認証局運用規程（Certificate Policy/Certification Practice Statement）」とする。

本認証局では識別子は設定しない。

１．４　PKI の関係者

本 CP/CPS に記述される PKI の関係者を以下に定める。各関係者は、本 CP/CPS の内容に同意し、本 CP/CPS の定める義務を遵守しなければならない。

本認証局に係わる関係者の位置づけを図　１に示す。

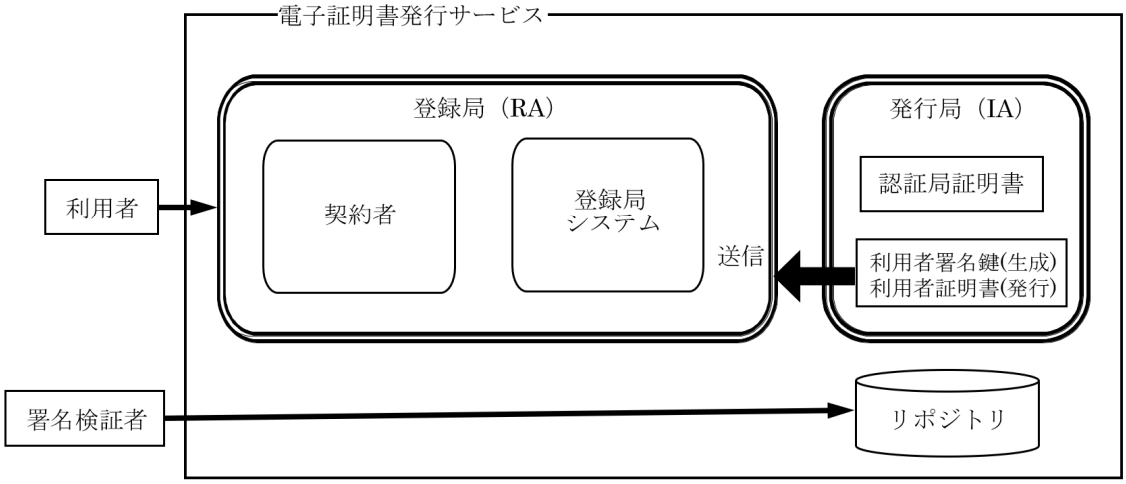

図１．関係者

本認証局に係る関係者とその役割を、表 1 に示す。

表1. 関係者とその役割

関係者	役割
契約者	サービス規約に同意した機関を指し、電子証明書取扱業務を行う。電子証明書取扱業務では、利用者から利用者証明書の発行申請又は、利用者証明書の失効申請を受けた場合、法令に準拠した資格審査、申請内容の真偽確認及び本人確認を行い、利用者証明書発行要求又は、失効要求を、登録局システムを通して発行局に対して行う。 なお、契約者は、利用者証明書の紛失などの緊急時に対し、利用者証明書の失効の要求を、登録局システムを通して発行局に対して行うことができる。
登録局(RA*1)	登録局は、契約者からの利用者証明書発行要求又は失効要求を受取り、承認する。承認後、発行局に、利用者証明書の発行要求又は失効要求を行う。登録局システムは、利用者情報登録、発行要求及び、失効要求を行う登録用 RA 端末と RA 端末から入力されたデータを蓄積する RA サーバから構成される。 *1: Registration Authority

利用者	契約者が、本サービスを利用することを承認した下記の者をいう。 ・個人 ・法人を代表する個人 ・法人を代表する個人から当社の提供するサービスの利用に関する権限を委任された者 ・個人事業主 ・個人事業主から当社の提供するサービスの利用に関する権限を委任された者 登録局は、発行局に対し、利用者証明書の発行要求を行い、利用者は、本認証局から、利用者署名鍵および利用者証明書の利用許諾を受ける。 利用者は本 CP/CPS に同意し、本 CP/CPS の利用者の義務を遵守しなければならない。
署名検証者	利用者証明書を信頼し、利用する者をいう。 署名検証者は、本規程内容について理解し同意した上で、利用者証明書を利用しなければならない。
認証局(CA*2)	本サービスの認証業務を行う。 登録局(契約者を含む)、発行局及びリポジトリ(※)から構成される。 *2: Certification Authority (※)リポジトリとは……CP/CPS 2. に定義する
発行局 (IA*3)	登録局からの利用者証明書の発行指示又は、失効指示に基づき、利用者証明書の発行又は、失効を行う。発行局は以下の事務を取り扱う。 ・証明書失効リスト（以下、「CRL*4」という。）の発行 ・利用者署名鍵、利用者公開鍵のペアの生成、PIN*5) コード等の生成及び電子証明書格納媒体への利用者署名鍵と利用者証明書の格納 ・発行局より発行された電子証明書格納用符号の利用者への発送 ・本認証局の認証局署名鍵の生成から廃棄までの認証局署名鍵のライフサイクル管理及び発行局の運用管理 なお、発行局のコンピュータシステムは、電子証明書を発行するための発行用 RA 端末および HSM を含む IA サーバから構成される。 *3: Issuing Authority *4: Certificate Revocation List *5: Personal Identification Number
電子証明書	ある公開鍵を、記載されたもの(利用者)が保有することを証明する電子的文書をいう。 認証局が電子署名を付与することでその公開鍵の正当性を保証する。 本サービスが発行する電子証明書としては下記のものがある。 ・認証局証明書 ・利用者証明書

１．５　証明書の用途

１．５．１　証明書の種類

本認証局は、以下の電子証明書を発行する。

(1)　認証局証明書

認証局証明書は、本認証局自身の電子証明書であり、本認証局の公開鍵に対して本認証局の署名鍵で電子署名されている。本認証局の署名鍵は、利用者に配付される利用者証明書および CRL への電子署名の用途に使用される。

(2)　利用者証明書

利用者に発行される電子証明書である。

なお、本認証局は、本認証局の判断および管理の下、動作確認を目的としたテスト用の利用者証明書の発行・失効を行うことができるものとする。

１．５．２　証明書の有効期間

本認証局が発行する電子証明書の有効期間は、以下のとおりとする。

① 認証局証明書：15 年 1 ヶ月

② 利用者証明書： 最大 13 ヶ月

当該利用者証明書の自動更新及び自動継続は行わない。

１．５．３　正規の証明書用途

利用者証明書および対応する鍵ペアは、以下の用途で使用できる。

- 当社の提供するサービス業務に適用する電子署名に係わる用途
- その他、当社の提供するサービス業務に係わる用途

１．６　ポリシー管理

１．６．１　ポリシー承認機関

本 CP/CPS に関する意思決定を実施する機関を当社のデジタルテクノロジー&ソリューション事業部アプリケーションサービス部（以下、「認証局事務局」という。）とする。当社の

認証局事務局は、本 CP/CPS、関連する規定を策定し承認する最高意思決定機関として権限を有する。

１．６．２　お問合わせ先

本 CP/CPS 等に関するお問い合わせ先は、契約者が定める連絡先とする。

１．６．３　ポリシーに対する本 CP/CPS の適合性調査担当者

本 CP/CPS の内容に関して、当社の認証局事務局が適合性を決定する。

１．６．４　適合性の承認手続き

本 CP/CPS の承認に関して、当社の所定の手続きにより認証局事務局が実施する。

２．　公開とリポジトリ

２．１　リポジトリ

本認証局は、以下に示す本認証局に関する重要事項等の情報を目的別に当社の指定するウェブサイトにリポジトリとして公開する。リポジトリの公開は、24 時間 365 日利用可能とする。ただし、システムの保守などの理由により、利用者及び署名検証者に予め通知した上で、一時的にリポジトリの公開を停止することができる。

２．２　認証情報の公開

リポジトリで公開される情報及び公開方法を、表 2 に示す。本認証局は、認証局証明書のフィンガープリントなどを公開するサーバについては、通信路の暗号化、及び情報の改ざん検知・防止措置を施している。

表２．リポジトリの内容

情報	対象	公開方法
本 CP/CPS	関与する者全員	https://www.marketing.nssol.nipponsteel.com/contracthub/cpcps
CRL	利用者及び署名検証者	http://mpkicrl.managedpki.ne.jp/mpki/NSSOLe-Contract-CA-G1/cdp.crl
認証局証明書のフィンガープリント*10	利用者及び署名検証者	https://www.marketing.nssol.nipponsteel.com/contracthub/fing
サービス規約等本サービスに関わる文書	関与する者全員	https://www.marketing.nssol.nipponsteel.com/contracthub/kiyaku

*10: 認証局証明書の値を SHA-1 で変換した値

２．３　公開の時期と周期

本認証局が公開する情報の公開頻度は、下記のとおりとする。
本 CP/CPS の公開については、下記の周期で更新、公開する。

(1) CRL については、発行した CRL の有効期間を 7 日間とし、CP/CPS4.9.7 による周期

で更新する。

(2) サービス規約は変更の都度、更新しリポジトリで公開する。

(3) 認証局証明書、及び認証局証明書のフィンガープリントは、発行及び更新の都度、リポジトリに登録し、公開する。

２．４　リポジトリに対するアクセスコントロール

本認証局は、リポジトリに対する情報セキュリティ対策以外の目的で特段のアクセスコントロールは行わない。

３．　本人性確認と認証

３．１　名称

３．１．１　名称のタイプ

本認証局で使用する名称は、ITU X.500 シリーズ定義の識別名（DN: DistinguishedName）の形式に従う。

３．１．２　名称の意味に関する要件

本認証局において発行する利用者証明書に記載される証明書所有者情報（subject）の識別名（DN）は、当社の提供するサービスの利用を申請した利用者に対し、契約者がサービス利用審査時に提出される利用者本人の確認資料（利用者から提出された公的証明書、またはそれに準ずる証明書（以下、「公的書類」という。））に基づき、契約者で設定することができる。詳細については、本 CP/CPS11.3 に定める。

３．１．３　利用者の匿名・仮名についての要件

利用者証明書の Common Name（以下、「CN」という。）について、契約者は利用者が提出した公的書類に基づき設定する場合には、匿名や仮名は認めない。

３．１．４　様々な名称形式を解釈するためのルール

本認証局が発行する電子証明書の DN の形式は、X.500 に従う。

３．１．５　名称の一意性

本 CP/CPS3.1.3 に従う。

利用者証明書に記載される利用者情報（subject）の識別名（DN）は、本認証局が発行した利用者証明書において一意に定まる。

３．１．６　商標等の認識、認証および役割

本認証局は、利用者証明書の発行に際し、著作権、営業権、商標権、実用新案権、特許権その他の知的財産権（特許その他の知的財産を受ける権利を含むがこれらに限られない。）については、審査で確認しない。

３．２　初回の利用者の本人性確認

３．２．１　利用者署名鍵の所有を検証する方法

本認証局は、本認証局にて利用者の鍵ペアを生成し、利用者証明書とともに当社が指定した、利用者だけがアクセス可能な領域に送付したことをもって、利用者が利用者署名鍵を所有したものとみなす。

３．２．２　利用者の確認

本認証局は、利用者が契約者に提出した利用者本人の公的書類を契約者が確認することをもって本サービスの利用者を確実に確認するものとする。なお、利用者本人確認の方法の詳細については、契約者で定める審査基準に従うものとする。

３．２．３　権限の正当性確認

本認証局は、登録局による本 CP/CPS3.2.2 に定める確認をもって、当該利用者が利用者証明書の発行をうける権限を有することを確認する。

３．３　利用者署名鍵および利用者証明書更新申請時の本人性確認と認証

３．３．１　利用者証明書定期更新時の本人性確認と認証

本認証局では、利用者証明書の更新は実施しない。

３．３．２　失効後の利用者署名鍵および利用者証明書再発行時の本人性確認と認証

本認証局では、鍵ペアおよび利用者証明書の失効後に失効前の鍵ペアおよび利用者証明書の再発行は実施せず新たな鍵ペアおよび利用者証明書を生成する。

３．４　失効申請時の本人性確認と認証

本認証局では、利用者は、契約者に失効を依頼する。本認証局（契約者）は、利用者本人からの失効依頼であることを確認し、当該証明書を失効させる。利用者証明書を失効後、そのシリアル番号を CRL に掲載する。

４．　証明書のライフサイクル

４．１　利用者証明書申請

４．１．１　利用者証明書の利用申請が認められる者

利用者証明書の利用申請が認められる者は、契約者に対し本人の情報を提示し、本サービスによる証明書発行に同意した者である。

４．１．２　利用者証明書の利用申請方法

契約者において本人情報を審査するものとする。本認証局は、利用者証明書の発行時において利用者が契約者に対し利用者証明書発行に同意することで、利用者証明書の発行申請を行ったものとみなす。

４．２　証明書申請プロセス

４．２．１　本人性確認と認証業務の実行

本 CP/CPS3.2.2 に従う。

４．２．２　利用者証明書申請の承認または拒否

契約者は、本サービスの利用申込みに対する審査において疑義がないことを確認することができた場合は、登録局に対し利用者情報の登録及び利用者証明書の発行を要求する。

契約者は、本サービスの利用申込みに対する審査において疑義が認められた場合は、必要書類の訂正又は再提出を求める。

４．３　利用者証明書の発行

４．３．１　利用者証明書発行時の認証局の行動

登録局システムは、契約者からの発行要求受領後に発行局に対し利用者証明書の発行指示を行う。発行局は、指示送信元である登録局の正当性を確認した上で、利用者の鍵ペアを生成し、対応する利用者証明書を発行する。

４．３．２　認証局から利用者への利用者証明書発行の通知

本認証局による利用者証明書の発行に関する利用者への通知については、契約者から利用者に対してメールもしくはSMSを送信することにより行う。

４．４　利用者証明書受領

４．４．１　利用者証明書受領確認手続き

本認証局は、契約者が利用者証明書の受領確認をするものとする。

４．４．２　認証局による利用者証明書および認証局証明書の公開

本認証局は、利用者証明書を公開しない。

また、本認証局は、認証局証明書のフィンガープリントを、本 CP/CPS2.2 に定めるリポジトリにて公開する。

４．４．３　認証局による他の関係者に対する利用者証明書発行の通知

本認証局は、本 CP/CPS4.3.2 の規定に基づくもの以外への利用者証明書の発行通知を行わない。

４．５　鍵ペアと証明書の利用

４．５．１　利用者による署名鍵と証明書の利用

利用者は、利用者証明書と利用者署名鍵の用途について、本 CP/CPS1.5.3 に従うこととし、規定された用途以外に使用してはならない。

また、第三者に使用させてはならない。

なお、利用者署名鍵の PIN コードを複写してはならない。

４．５．２　署名検証者に対する利用者の公開鍵と利用者証明書の利用

署名検証者は、契約者の指示または定めに従い、本認証局および利用者の電子証明書の有効性について検証を行う。

また、利用者の公開鍵と利用者証明書の用途については、本 CP/CPS1.5.3 に従うこととし、署名検証者は、規定された用途以外に利用者の公開鍵を使用してはならない。

また、署名検証者は、利用者の公開鍵の使用に際して、CRL によりその時点での有効性の検証を必ず行わなければならない。

４．６　鍵更新を伴わない利用者証明書更新

４．６．１　鍵更新を伴わない利用者証明書更新に関する要件

本認証局は、署名鍵更新を伴わない利用者証明書の更新を行わないため、規定せず。

４．６．２　利用者証明書利用申請者

本認証局は、署名鍵更新を伴わない利用者証明書の更新を行わないため、規定せず。

４．６．３　利用者証明書申請プロセス

本認証局は、署名鍵更新を伴わない利用者証明書の更新を行わないため、規定せず。

４．６．４　利用者への新しい利用者証明書発行の通知

本認証局は、署名鍵更新を伴わない利用者証明書の更新を行わないため、規定せず。

４．６．５　利用者証明書受領確認手続き

本認証局は、署名鍵更新を伴わない利用者証明書の更新を行わないため、規定せず。

４．６．６　認証局による新しい認証局証明書の公開

本認証局は、署名鍵更新を伴わない認証局証明書の更新を行わないため、規定せず。

４．６．７　認証局による他の関係者に対する新しい利用者証明書発行の通知

本認証局は、署名鍵更新を伴わない利用者証明書の更新を行わないため、規定せず。

４．７　鍵更新を伴う利用者証明書更新

４．７．１　鍵更新に関する要件

本認証局は、署名鍵更新を伴う利用者証明書の更新に際して、利用者が保持する既存の鍵ペアの継続利用を認めず、新しい鍵ペアを生成し、その公開鍵に対する新しい利用者証明書を発行する。

４．７．２　新しい公開鍵に対する利用者証明書利用申請者

本 CPS4.1.1 を準用する。

４．７．３　鍵更新における利用者証明書申請プロセス

本 CPS4.2 を準用する。

４．７．４　利用者への新しい利用者証明書発行の通知

本 CPS4.3.2 を準用する。

４．７．５　鍵更新された利用者証明書の受領確認手続き

本 CPS4.4.1 を準用する。

４．７．６　鍵更新された利用者証明書の公開

本 CPS4.4.2 を準用する。

４．７．７　鍵更新された利用者証明書の他の関係者に対する発行の通知

本 CPS4.4.3 を準用する。

４．８　利用者証明書の変更

４．８．１　利用者証明書の変更に関する要件

利用者は、利用者証明書の記載内容に変更の必要が生じた場合、契約者の指示または定めに従うものとする。本認証局は、利用者証明書に関する変更要請に応じ、適切な内容の利用者証明書を発行する。

４．８．２　利用者証明書変更の申請者

本 CPS4.1.1 を準用する。

４．８．３　利用者証明書変更の申請プロセス

利用者証明書の変更については、契約者から登録局への変更申請により行われる。

４．８．４　利用者への新しい利用者証明書発行の通知

本 CP/CPS4.3.2 を準用する。

４．８．５　変更された利用者証明書の受領確認手続き

本 CP/CPS4.4.1 を準用する。

４．８．６　変更された利用者証明書の公開

本 CP/CPS4.4.2 を準用する。

４．８．７　変更された利用者証明書の他の関係者に対する発行の通知

本 CP/CPS4.4.3 を準用する。

４．９　利用者証明書の失効と一時停止

４．９．１　失効の要件

本認証局は、下記の事由により当該利用者証明書の失効を行う。

(1)　本認証局側の事情による失効事由

（ア）　利用者署名鍵が危殆化したことを知り得た場合

（イ）　利用者証明書の記載内容に誤りがある場合
（ウ）　本認証局が利用者の利用継続が困難と判断した場合
（エ）　本サービスが終了した場合
（オ）　本認証局の署名鍵が危殆化した場合
（カ）　本認証局が認証業務を廃止する場合
（キ）　サービス規約に定める場合
（ク）　利用者署名鍵及び利用者証明書が利用者に正しく配付されなかった場合
（ケ）　利用者が死亡または失踪した場合
（コ）　その他、本認証局が必要と判断した場合

(2)　利用者申し出による失効

４．９．２　失効申請が認められる者

本 CP/CPS4.9.1 に記載の事由に限り、登録局が失効申請者として発行局に対し失効を指示することができる。

４．９．３　失効申請プロセス

利用者証明書の失効申請については、登録局から発行局への失効指示により行われる。

失効申請が承認された場合、発行局は、登録局からの失効指示に基づき、当該利用者証明書を失効させる。

なお、有効な電子証明書を失効した場合は、契約者が利用者へ失効した旨について速やかに連絡を行う。

４．９．４　失効申請までの猶予期間

登録局は、本 CP/CPS4.9.1 に定める事由が発生した場合、速やかに発行局へ失効指示を行うものとする。

４．９．５　失効申請プロセスの時間

登録局は、失効申請を受領後、遅滞なく当該利用者証明書の失効を発行局へ指示を行う。

４．９．６　署名検証者による失効情報確認の要件

署名検証者は、本認証局が発行する CRL により、利用者証明書の失効を確認することができる。

４．９．７　CRL 発行周期

本認証局は、CRL を 24 時間の周期で発行する。

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

本認証局は、発行された CRL は遅くとも 1 時間以内にリポジトリにて公開する。

４．９．９　オンラインでの利用者証明書の有効性確認

CRL を利用者証明書の失効情報確認の手段として提供する。その他オンラインでの失効情報の提供は行わない。

また、有効期間の満了した利用者証明書の失効情報確認についての問い合わせには応じない。

４．９．１０　オンラインでの利用者証明書の失効情報確認要件

本認証局は、CRL 以外でオンラインでの利用者証明書の失効情報を提供しない。

４．９．１１　その他の利用可能な失効情報確認の手段

CRL 以外の失効情報確認の手段を提供しない。

４．９．１２　一時停止の要件

本認証局は、一時停止の機能を持たない。

４．９．１３　一時停止申請者

本認証局は、一時停止の機能を持たないため、規定せず

４．９．１４　一時停止申請の手続き

本認証局は、一時停止の機能を持たないため、規定せず

４．９．１５　一時停止可能な期間

本認証局は、一時停止の機能を持たないため規定せず。

４．１０　利用者証明書ステータス確認サービス

本認証局は、CRL 以外で利用者証明書のステータスを確認できるサービスを提供しない。

４．１０．１　運用上の特徴

本認証局は、CRL 以外で利用者証明書のステータスを確認できるサービスを提供しないため規定せず。

４．１０．２　サービスの可用性

本認証局は、CRL 以外で利用者証明書のステータスを確認できるサービスを提供しないため、規定せず。

４．１０．３　他の要件

本認証局は、CRL 以外で利用者証明書のステータスを確認できるサービスを提供しないため、規定せず

４．１１　認証局への登録の終了

当該利用者証明書が有効期日を迎えた場合、もしくは本 CP/CPS4.9.1 に基づく当該利用者証明書の失効および CRL への反映をもって、本認証局は利用者証明書の利用を終了したとみなす。

４．１２　鍵の第三者預託と鍵回復

４．１２．１　鍵預託とリカバリのポリシーと手順

本認証局は、利用者署名鍵の第三者預託を行わない。

４．１２．２　セッションキーのカプセル化・復旧のポリシーと手順

本認証局は、利用者証明書を電子署名用途のみで使用するためセッションキーのカプセル化を行わない。

５．　設備、管理、運用統制

５．１　物理的な管理

５．１．１　施設の所在と構造

本認証局のシステムに係る施設（以下、「本施設」という。）は、地震、火災および水害、その他の災害による影響を容易に受けない施設に設置する。本施設には、建物構造上、耐震、耐火、水害および不正侵入防止の措置を講じる。

また、本施設は、建築物の外部および建築物内に発行局の所在を明示または暗示する名称を看板もしくは表示板等により一切掲示しない。

５．１．２　物理的アクセス

本施設は、入退館等に際して資格確認を行い、識別証等により入退出を管理する。

(1)　登録局（RA 局）

認証業務を行う各室では、業務の重要度に応じたセキュリティレベルを設定し、相応する入退室管理を行う。

(2)　発行局（IA 局）

入退室時の認証には、各室内において行われる認証業務の重要度に応じ、権限保有者であることを確認できる入退室用カードもしくは生体認証等を用いる。

建物内および各室内は、監視システムおよび監視要員による 24 時間 365 日監視を行う。

５．１．３　電源設備と空調設備

本施設は、機器類の運用のために十分な容量の電源を確保し、また、空調設備により機器類の動作環境および要員の作業環境を適切に維持する。発行局については、瞬断、停電に備えた対策を講じ、商用電源が供給されない事態においては、自家発電機による電源供給に切り換える。また、空調設備は冗長化する。

５．１．４　水害対策

本施設は、水害による影響を容易に受けない場所に設置する。発行局については、建物および各室に漏水検知器を設置し、天井、床には防水対策を講じる。

５．１．５　火災に対する予防措置と対策

本施設は、耐火構造とする。発行局については、本認証局に係るシステムを設置する室は防火区画とし、自動ガス消火設備を備える。

５．１．６　地震に対する予防措置と対策

本施設は、現行の建築基準法に規定する構造上の安全を有する。建物は、新耐震規準に基づいた耐震構造にて設計する。また、本認証局のシステム機器および什器には転倒および落下を防止する対策を講じる。

５．１．７　媒体保管場所

本認証局のシステムのバックアップデータが含まれる媒体、審査業務で使用した書類等については、職務上利用することが許可された者のみが入室またはアクセス（利用）できる環境に保管する。

５．１．８　廃棄物処理

本施設では、機密情報を含む書類はシュレッダーにより裁断、もしくは当社が指定する専門業者による溶解処理の上、廃棄する。電子媒体については、物理的破壊、初期化、消磁等の措置によって記録されたデータを完全に抹消の上、廃棄する。

５．１．９　オフサイトバックアップ

本認証局は、オフサイトバックアップについては公開しない。

５．２　職務統制

５．２．１　信頼される役割および人物

本認証局は、認証局を運営するために必要な人員（以下、「認証局員」という。）およびその役割を以下のとおり定める。

(1)　ポリシー承認局

本認証局におけるポリシーの決定、承認、本 CP/CPS 等の重要ドキュメントの変更、承認等を行う最高意思決定機関であり、当社の認証局事務局が行う。

(2)　認証局責任者

本認証局を統括し、登録局責任者および発行局責任者を管理する。

(3)　登録局責任者

本認証局の登録局に係る業務を統括し、業務オペレータを管理する。

(4)　登録局オペレータ

本認証局の登録局に係る業務を行う。

(5)　発行局責任者

本認証局の発行局に係る業務を統括し、発行局システムアドミニストレータおよび発行局オペレータを管理する。

(6)　発行局システムアドミニストレータ

発行局システムアドミニストレータは、発行局責任者の管理の下、本認証局のシステムの維持・管理を行う。

(7)　発行局オペレータ

本認証局に係るシステムの運用、保守および鍵管理等を行う。

(8)　監査人

本認証局とは独立した組織で監査を行う。

(9)　電子証明書取扱業務管理責任者

契約者の電子証明書取扱業務の責任者とする。

(10)　電子証明書取扱業務オペレータ

電子証明書取扱業務管理責任者の管理の下、契約者の電子証明書取扱業務をする。

５．２．２　役割ごとに必要な人員の数

本認証局は、発行局システムアドミニストレータおよび発行局オペレータについては、2名以上配置する。また、契約者ごとに電子証明書取扱業務管理責任者を1名ずつ配置する。

５．２．３　各役割における本人性確認と認証

本認証局は、各役割に応じ、認証業務を行う各室の入室権限および本認証局のシステムの操作権限を定める。また、発行局に関する各室への入室時またはシステムの操作時においては、入退室カード、生体認証、電子証明書、ID およびパスワード等の単体または組合せにより、本人性および入室・操作権限の確認ならびに認証を行う。

５．２．４　職務の分離が要求される役割

本認証局は、下記の職務については、兼務することを認めない。

(1)　認証局責任者
(2)　登録局責任者
(3)　登録局オペレータ
(4)　発行局責任者
(5)　監査人

５．３　人事面の管理

５．３．１　経歴、資格、経験などに関する要求事項

本認証業務に従事する全ての職員については、職務規程に基づき、審査、教育、配置転換等を行う。但し、業務の一部が外部の委託会社に委託される場合、当該委託業務に従事する職員は、当該委託会社の職務規程に基づき審査、教育、配置転換等を行う。

５．３．２　教育訓練要件

本認証局は、認証局員として従事するすべての職員に対し、その業務に応じた知識・技術情報の提供または教育訓練等を行う。

５．３．３　教育訓練の周期

本認証局は、認証局員に対する年１回以上の再教育および新任担当者の訓練を実施する。また、以下の事態が生じた場合には、教育・訓練を実施する。

① 本 CP/CPS、および関連諸規定が改訂され、認証局責任者、発行局責任者、または登録局責任者が必要と判断した場合。
② 本認証局システムを変更する場合であって、認証局責任者、発行局責任者、または登録局責任者が必要と判断した場合。
③ その他、認証局責任者、発行局責任者、または登録局責任者が必要と判断した場合。

５．３．４　ジョブローテーションの周期と順序

本認証局は、必要に応じて認証局員の配置転換を行う。

５．３．５　許可されていない行動に対する罰則

認証局員が過失、故意に関わらず、本 CP/CPS に記載されるポリシーと手続き、もしくは運用手順書に定める手順等に違反した場合、速やかに原因および影響範囲の調査を行った上で、処罰を課す。

５．３．６　職員に対する契約要件

本認証局は、外部の委託会社に委託された業務に係る職員については、本 CP/CPS 及び委託先の規則に則った義務を遵守させる。

５．３．７　職員が参照できるドキュメント

本認証局は、認証局員が、運用手順書等、業務に係るドキュメントをその役割に応じて参照できる措置を講じる。

５．４　監査ログの手続き

５．４．１　記録されるイベントの種類

本認証局は、本 CP/CPS の準拠性および情報セキュリティ対策の妥当性を評価するために、本認証局における業務および情報セキュリティに関する重要な事象を対象に、アクセスログや操作ログ等、監査ログを収集する。

５．４．２　監査ログを処理する頻度

本認証局は、認証局運用に疑義が生じた際などにおいて、機能不全、脆弱性または悪意の行動を検出する目的で監査ログを確認する。

５．４．３　監査ログの保持期間

本認証局は、発行した電子証明書の有効期間満了後の少なくとも 1 年間は監査ログを保管する。他の記録については、当該ログ発生より 3 年間保持する。

５．４．４　監査ログの保護

本認証局は、許可された者のみが閲覧可能となるよう、監査ログへのアクセスコントロールを施す。保管庫への物理的なアクセスコントロール、電子媒体であればフォルダ等への論理的なアクセスコントロールを施す。

５．４．５　監査ログのバックアップ手続き

本認証局は、監査ログに関する電子データを日次でバックアップし取得する。紙媒体については、原本のみを保管する。

５．４．６　監査ログ収集システム

本認証局は、実装された機能により監査ログを自動的に収集する。

５．４．７　当事者に対する通知

本認証局は、イベントを発生させた当事者に通知することなく、監査ログを収集、検査する。

５．４．８　脆弱性評価

本認証局は、本認証局に係るシステムに対し、外部の専門機関による定期的な脆弱性評価を行う。また、その評価結果を文書化し保管する。

５．５　業務記録の保存

５．５．１　保存対象となる業務記録

本認証局は、本 CP/CPS5.4.1 で規定された監査ログのほか、以下の情報を保管する。

(1)　認証局証明書
(2)　利用者証明書発行・失効に係る情報
(3)　内部監査報告書
(4)　本 CP/CPS および関連諸規定

５．５．２　業務記録の保持期間

本認証局は、本 CP/CPS5.5.1 に規定される記録について、関連する電子証明書の有効期間を超えて少なくとも 1 年間保管する。ただし、法令やその利用目的などによって、別途適切な保管期間を設定する必要がある場合は、その期間保管するものとする。

５．５．３　業務記録の保護

本 CP/CPS5.4.4 を準用する。

５．５．４　業務記録のバックアップ手続き

本 CP/CPS5.4.5 を準用する。

５．５．５　業務記録の日付要件

本認証局は、本 CP/CPS5.5.1 に関し、帳票類については起票日もしくは処理した日付を記録する。また、日付のみでは記録としての証明力に欠ける場合は、時刻も記録する。本認証局および利用者の電子証明書については、発行された日時を記録する。また、本認証局のシステムには、発行する電子証明書および監査ログに対して正確な日付・時刻を記録するために必要な措置を講じる。

５．５．６　業務記録収集システム

本認証局は、電子データについては本認証局に係るシステムの機能により収集する。その他、紙媒体については、認証局員が収集する。

５．５．７　業務記録の取得と検証手続き

本認証局は、本 CP/CPS5.5.1 に関し、記録の取得および閲覧は、監査人および認証局責任者が認めた者に限定する。また、記録の可読性に関わる検証は、必要に応じ、実施する。

５．６　認証局の鍵更新

本認証局は、14 年ごとに、認証局の鍵ペアを更新する。

５．７　危殆化および災害からの復旧

５．７．１　認証局署名鍵の危殆化および災害からの復旧手続き

本認証局は、発行局の責による場合を除き、本認証局の署名鍵の危殆化によるサービスの停止を不可抗力事項として扱い、同サービス再開に要する時間について保証しない。

本認証局は、以下の措置を実施するとともに、利用者・署名検証者への周知を図る。

(1)　危殆化した署名鍵を用いた認証業務の停止
(2)　全ての電子証明書の失効
(3)　危殆化の原因調査
(4)　本認証局の新しい鍵ペアの生成と対応する電子証明書の発行
(5)　本認証業務の再開の妥当性評価
(6)　本認証業務の再開
(7)　新たな鍵ペアの生成および電子証明書の発行

本認証局が被災した場合には、本 CP/CPS5.7.4 に基づき、復旧に努める。

５．７．２　ハードウェア、ソフトウェア、データの障害時の手続き

本認証局は、ハードウェア、ソフトウェア、データが破壊された場合には、バックアップ用のハードウェア、ソフトウェア、データにより、遅滞なく復旧作業を行う。

５．７．３　利用者署名鍵危殆化時の手続き

利用者は、自身の署名鍵の危殆化または危殆化が疑われる事態が生じた場合、本CP/CPS4.9に記載されたとおり、当該事態の発生を契約者に連絡し、契約者の指示または定めに従うものとする。

５．７．４　認証局署名鍵の危殆化および災害後の事業継続性

本認証局は、災害による認証局の停止を不可抗力事項として取扱い、サービスの再開に要する時間について保証しない。

本認証局は、災害によりサービスが停止した場合、当社のウェブサイトにおいて、その旨公開する。

本認証局を管理する当社は、以上に掲げる措置を実施するとともに、被災状況の調査を行い、調査結果に基づき、復旧方針を定めるものとし、発行局、登録局は当該復旧方針に従い復旧作業を実施する。

５．８　認証局の業務終了

本認証局は、業務を終了する場合、契約者に事前に通知するほか、当社のウェブサイトにおいても、その旨公開する。

本認証局が保有する電子証明書発行・失効申請に関わる情報については、すべての利用者証明書の有効期間が終了してから７年間保存する。

認証局の業務を終了する場合は、利用者及び署名検証者への混乱の最小化に努める。

(1)　発行済み利用者証明書の失効処理

本認証局の終了日までに発行された全ての利用者証明書を失効し、失効情報を CRL より発行する。失効情報は、発行した CRL を、リポジトリを通じて署名検証者に公開する。

(2)　利用者への連絡方法等

業務を終了する場合、60 日前に次の関係者にリポジトリでの公開を含め周知する。

- 全ての利用者
- 署名検証者
- その他、本認証局と関係している組織等

(3)　終了後の失効情報の公開

利用者証明書の有効期間が終了するまで公開する。

(4)　認証局署名鍵の処理

本認証局は認証局署名鍵及びバックアップされた署名鍵の全てを完全に初期化する。

６．　技術面のセキュリティ管理

６．１　鍵ペア生成と導入

６．１．１　鍵ペアの生成

本認証局の鍵ペアは、認証局責任者の管理の下、認証局の運用担当者により FIPS 140-2 レベル 4 の署名鍵管理モジュール（以下、「HSM」という。）を用いて生成する。

利用者の鍵ペアについては、本認証局が定める暗号ライブラリにより生成する。

６．１．２　利用者への利用者署名鍵の配送

本認証局は、利用者からの申請に基づいて当該利用者証明書に関わる利用者署名鍵を生成し、その機密性および完全性を確保する措置を講じた上で、利用者だけがアクセス可能な領域へ配付する。

６．１．３　本認証局への公開鍵の配送

本認証局は、利用者からの公開鍵の配送を受け付けない。

６．１．４　署名検証者への認証局公開鍵の配送

本認証局は、署名検証者に対する本認証局の公開鍵の配送を行わない。本認証局の公開鍵が含まれる認証局証明書は、本認証局のリポジトリにて公開する。

６．１．５　鍵長

本認証局が発行する認証局証明書に係る鍵は、下記の仕様に適合する鍵を利用する。

署名方式　：　SHA256withRSA

合成数　：　2048 bit

利用者証明書に係る鍵は、下記の仕様に適合する鍵を利用する。

署名方式　：　SHA256withRSA

合成数　：　2048 bit

６．１．６　公開鍵パラメータ生成および検査

本認証局は、公開鍵を生成する手段および検査手法を公開しない。

６．１．７　鍵用途（X.509 v3 key usage フィールド）

本認証局の鍵は、以下の目的にのみ使用される。

①　利用者証明書に対する電子署名

②　認証局証明書に対する電子署名

③　CRL に対する電子署名

本認証局が発行する電子証明書に記載する鍵用途（X.509 v3 key usage フィールド）は、本 CP/CPS1.5.3 に定める。

６．２　署名鍵保護と署名鍵管理モジュール技術の管理

６．２．１　署名鍵管理モジュールの標準と管理

本認証局の鍵ペアは、FIPS 140-2 レベル 4 の署名鍵管理モジュール（HSM）にて保護する。上記のモジュールは、権限が与えられた複数人の発行局オペレータが管理する。

６．２．２　署名鍵の複数人管理（n out of m）

本認証局の署名鍵の管理は、権限が与えられた複数人の発行局システムアドミニストレータが行う。

６．２．３　署名鍵の預託

本認証局は、本認証局および利用者の署名鍵の預託を行わない。

６．２．４　署名鍵のバックアップ

本認証局の署名鍵のバックアップは、権限が与えられた複数人の発行局オペレータが行う。HSM からバックアップした本認証局の署名鍵は、暗号化して複数に分割し、施錠可能な保管庫にて定められた手順により安全に保管する。

なお、利用者署名鍵のバックアップは行わない。

６．２．５　署名鍵のアーカイブ

本認証局は、本認証局の署名鍵のアーカイブを行わない。

なお、利用者署名鍵は、利用者に配布された後、適切な方法により完全に消去される。

６．２．６　署名鍵管理モジュールからの署名鍵の転送

本認証局は、HSM の故障など署名鍵の復元が必要な場合、発行局責任者の管理・指示の下、権限が与えられた発行局システムアドミニストレータおよび発行局オペレータが、バックアップからの署名鍵の復元を行う。このとき、バックアップデータを本施設外へ移送しない。

６．２．７　署名鍵管理モジュール内での署名鍵保存

本認証局の署名鍵は、HSM 内で生成する。署名鍵管理モジュール内で署名鍵は暗号化し保存する。

６．２．８　署名鍵の活性化

本認証局の署名鍵は、本認証局起動手順に従い、発行局管理者の管理の下、権限が与えられた複数人の発行局システムアドミニストレータが活性化を行う。また、活性化作業の内容を記録する。

６．２．９　署名鍵の非活性化

本認証局の署名鍵は、本認証局停止手順に従い、発行局管理者の管理の下、権限が与えられた複数人の発行局システムアドミニストレータが非活性化を行う。また、非活性化作業の内容を記録する。

６．２．１０　署名鍵破壊の方法

本認証局の署名鍵は、認証局責任者の指示を受け、発行局管理者の管理の下、別途規定された手順に基づき、権限が与えられた複数の発行局システムアドミニストレータが完全に破壊する。同時に、バックアップされたデータについても、同様の手順に基づき完全に破壊する。また、破壊作業の内容を記録する。

６．２．１１　署名鍵管理モジュールの評価

本認証局は、本 CP/CPS6.2.1 に定める標準を満たした HSM を使用する。

６．３　鍵ペア管理に関するその他の項目

６．３．１　公開鍵の保存

公開鍵の保存については、それを含む電子証明書を保存することによって行う。

６．３．２　証明書と鍵ペアの使用期間

電子証明書および鍵ペアの有効期間を次に示す。

(1)　認証局証明書　　：　15 年 1 ヶ月
(2)　利用者証明書　　：　最大 13 ヶ月
(3)　認証局証明書鍵ペア　：　15 年 1 ヶ月
(4)　利用者証明書鍵ペア　：　最大 13 ヶ月

６．４　署名鍵の活性化情報

６．４．１　活性化情報の作成と設定

本認証局内で使用される活性化情報は、容易に推測されないように配慮して生成し、設定する。

６．４．２　活性化情報の保護

本認証局内で使用される活性化情報は、本 CP/CPS5.1 に規定した施設内において、施錠可能な保管庫に保管する。

６．５　コンピュータセキュリティ管理

６．５．１　特定のコンピュータセキュリティに関する技術的要件

本認証局に係るシステムは、アクセス制御機能、操作者である発行局オペレータの識別と認証機能、システムのバックアップ・リカバリ機能等を備える。

６．５．２　コンピュータセキュリティの評価

本認証局に係るシステムは、事前に導入評価を実施し、認証業務開始後もセキュリティ上の脆弱性についての情報収集、評価を継続的に行い、重大な脆弱性が発見された場合には、速やかに必要な対処を行う。

６．６　技術面におけるライフサイクルの管理

６．６．１　システム開発管理

本認証局の構築・修正・変更は、認証局責任者の管理の下、信頼できる組織および環境にて作業を実施する。修正・変更に際しては、テスト環境において検証を行い、認証局責任者の承認を得た上で導入する。ただし、軽微な修正・変更の場合、発行局については発行局責任者の承認の下、発行局システムアドミニストレーター―または発行局オペレータが作業を実施する。同様に登録局については登録局責任者の承認の下、登録局オペレータが作業を実施する。

６．６．２　セキュリティマネジメント管理

本認証局に係るシステムでは、十分なセキュリティレベルを確保するために必要な設定を行う。また、システムのセキュリティ上の脆弱性についての情報収集、評価を継続的に行ない、重大な脆弱性が発見された場合には、速やかに必要な対処を行う。

６．６．３　ライフサイクルセキュリティの管理

本認証局のシステムの開発、運用、変更、廃棄の各工程において責任者を定め、作業計画または手順を策定・評価し、必要に応じ試験を行う。また、各作業の内容を記録する。

６．７　ネットワークセキュリティ管理

本認証局のシステムとインターネット等の外部システムとは、ファイアウォール等を介して接続し、また侵入検知システムによる監視を行う。

６．８　日時の記録

本認証局に係るシステムには、発行する電子証明書および監査ログ等に対して正確な日付・時刻を記録するために必要な措置を講じる。

７．　証明書、CRL、OCSP の各プロファイル

本認証局が発行する電子証明書と CRL の型式、属性の仕様は、以下の標準仕様に従い定義している。

1) ITU-T Recommendation X.509(1997)

2) RFC3280:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. April 2002(RFC3280)

７．１　証明書プロファイル

７．１．１　バージョン番号

本 CP/CPS11.に定める証明書プロファイルにおいて規定する。

７．１．２　証明書拡張領域

本 CP/CPS11.に定める証明書プロファイルにおいて規定する。

７．１．３　アルゴリズムオブジェクト識別子

本 CP/CPS11.に定める証明書プロファイルにおいて規定する。

７．１．４　名前の形式

本 CP/CPS11.に定める証明書プロファイルにおいて規定する。

７．１．５　名称制約

本認証局では、日本語およびローマ字を使用する。

７．１．６　証明書ポリシーオブジェクト識別子

本認証局では、規定しない。

７．１．７　ポリシー制約拡張の使用

本認証局では、規定しない。

７．１．８　ポリシー修飾子の構文と意味

本 CP/CPS11.に定める証明書プロファイルにおいて規定する。

７．１．９　重要な証明書ポリシー拡張についての処理方法

本認証局では、規定しない。

７．２　CRL プロファイル

７．２．１　バージョン番号

本 CP/CPS11.2 に定める CRL プロファイルにおいて規定する。

７．２．２　CRL、CRL エントリ拡張

本 CP/CPS11.2 に定める CRL プロファイルにおいて規定する。

７．３　OCSP プロファイル

７．３．１　バージョン番号

本認証局では、OCSP プロファイルを使用しない。

７．３．２　OCSP 拡張

本認証局では、OCSP プロファイルを使用しない。

８．　準拠性監査とその他の評価

８．１　監査の頻度と要件

本認証局は、認証業務に疑義が生じた場合、発行局および登録局の全部または一部について、本 CP/CPS8.2 に定める監査人による監査を実施することができる。

８．２　監査人の要件

本認証局の監査は、当社の認証局事務局が指名する必要な知識と経験を有する者が行う。

８．３　監査人と被監査者の関係

公正な監査を遂行するために、監査人は本認証局から独立していることとする。

８．４　監査の範囲

本認証局の認証業務が、本 CP/CPS に準拠して実施されていることの監査を範囲とする。

８．５　監査における指摘事項への対応

監査により発見された指摘事項は、認証局責任者、発行局責任者および登録局責任者へ報告される。監査人、認証局責任者、発行局責任者、または登録局責任者により是正措置が必要と判断された場合、発行局責任者または登録局責任者の管理の下、是正措置を実施する。

８．６　監査結果の開示

本認証局は、監査結果を利用者および署名検証者へ開示しない。

本認証局は、本認証局が必要と認めた対象にのみ監査結果を開示する。

９．　他のビジネス的・法的問題

９．１　機密情報の管理

９．１．１　機密情報の範囲

本認証局は、発行局、登録局が保有する情報のうち、以下の情報（以下、「機密情報」という。）を機密として取り扱い、本 CP/CPS9.1.3 に掲げる場合を除き、第三者に開示しないこととする。

① 契約者からの依頼情報
② 本 CP/CPS9.2.2 に定める情報
③ 本認証局の情報セキュリティに関する情報

９．１．２　署名情報の範囲外の情報

本認証局は、発行局、登録局が保有する情報のうち、以下の情報については機密情報の範囲外とする。

① 本 CP/CPS2.2 において公開するものとして定める情報
② 本認証局の過失によらず公知となった情報
③ 本認証局以外のものから機密保持の制限なしに開示された情報
④ 第三者への提供の承諾を得た情報

９．１．３　第三者への開示

本 CP/CPS9.1.1 に関わらず、本認証局は、弁護士、公認会計士もしくは税理士等の専門家、業務の全部もしくは一部を委託する特定の第三者、裁判所、行政当局、弁護士その他の法令・規則等に基づき開示を求める権限を有する者から機密情報の開示を求められた場合は、当該機密情報を開示することができる。

９．１．４　機密情報の保護責任

本認証局は、機密情報の漏えいを防止する対策を実施する。また、本認証局の運営の用に供する以外には機密情報を使用しない。なお、個人情報の取り扱いは、本 CP/CPS9.2 に定める。

９．２　個人情報の保護

９．２．１　プライバシーポリシー

本認証局は、発行局および登録局が保有する情報のうち、本 CP/CPS9.2.2 に該当する情報については、本 CP/CPS に定める事項以外の事項に関しては個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号)、及び当社に適用される、行政機関が定める個人情報の保護に関するガイドラインに基づいて取り扱う。

また、当社は、本認証局の業務のうち自社が担当する業務については、ウェブサイトで公開するプライバシーポリシーを遵守する。委託先が担当する業務については、当社は、委託先がプライバシーポリシーを定め、遵守していることを確認する。

９．２．２　個人情報として扱われる情報

本認証局は、契約者から登録局へ電子証明書の発行または失効の指示等に含まれる、氏名、生年月日、その他の記述等により特定の個人を識別することができるものを個人情報として扱う。

９．２．３　個人情報とみなされない情報

本認証局は、本 CP/CPS9.2.2 に定める情報以外は、個人情報としてみなさない。

９．２．４　個人情報を保護する責任

本認証局が保有する個人情報の保護責任は、本 CP/CPS9.2.1 に定めるとおりとする。

９．２．５　個人情報の使用に関する個人への通知および承認

本認証局は、利用者証明書の利用申請もしくは失効申請をもって、本認証業務上必要とする個人情報の使用の承認を利用者から得たものとする。

９．２．６　司法手続または行政手続に基づく公開

本認証局で取扱う個人情報に関して、裁判上、行政上その他の法的手続きの過程において情報の開示要求があった場合、本認証局は、当該個人情報を開示することができるものとする。

９．２．７　他の情報公開の場合

本認証局は、業務の一部を外部の委託会社に委託する場合、秘密情報を委託会社に対して開示することがある。この場合、本認証局は、委託会社による情報の漏洩を防ぐため、委託会社との間で秘密保持に関する契約を締結し、守秘を義務づける。

９．３　知的財産権

本 CP/CPS の著作権は、当社に帰属する。

９．４　表明および保証

９．４．１　発行局の表明および保証

当社は、本認証局を構成する発行局として発行局の義務の遂行にあたり、以下の義務を負うことを表明し保証する。

(1)　本 CP/CPS に従った認証局署名鍵の安全な管理を行うこと
(2)　登録局からの指示に基づき正確に電子証明書の発行および失効を行うこと
(3)　CRL の発行および公開を行うこと
(4)　電子証明書に記載される情報と、申請にあった情報とが一致していること
(5)　本 CP/CPS に従ったシステムの監視および運用を行うこと

９．４．２　登録局の表明および保証

契約者は、本認証局を構成する登録局として登録局の業務の遂行にあたり、以下の義務を負うことを表明し保証する。

(1)　本 CP/CPS、サービス規約および関連諸規定を遵守すること
(2)　発行局への利用者証明書発行および失効の正確な指示を行うこと
(3)　利用者証明書の発行を利用者に正しく通知し、または発行された利用者証明書を正しく配付すること
(4)　本項に規定された登録局の義務、債務の不履行により発生した事態に対し、合理的な範囲で対処すること

９．４．３　利用者の表明および保証

利用者は、以下の義務を負うことを表明し保証する。

(1)　本 CP/CPS および関連諸規定を遵守すること

(2)　本 CP/CPS1.5 で規定された利用者証明書の用途を遵守すること

(3)　利用申請にあたり申請者が本認証局に提供する情報が正確であること

(4)　本認証局より送られる PIN について、紛失、改変、第三者による使用・複製等が行われない様、十分な注意をもって厳重に管理すること

(5)　本 CP/CPS4.8.1 に示す内容に変更があるとき、本 CP/CPS4.8.3 に従い、遅滞なく登録局に対して変更に関する申請を行うこと

(6)　有効期間が満了した利用者証明書および失効された利用者証明書を使用しないこと

９．４．４　署名検証者の表明および保証

署名検証者は、以下の義務を負うことを表明し保証する。

(1)　本 CP/CPS1.5 で規定された電子証明書用途を遵守すること。

(2)　電子証明書の有効性の確認等により、利用者証明書を信頼するか否かを判断すること。

(3)　本認証局が発行した電子証明書の有効期間と記載事項の確認を行うこと

(4)　CRL による失効登録の有無の確認を行うこと

(5)　本項に規定された義務の不履行により発生した事態に対し責任を負うこと

９．５　無保証

本認証局は、本 CP/CPS9.4.1、9.4.2 に定める保証に関連して直接かつ現実に発生する通常の損害以外の損害については、本 CP/CPS に基づく債務不履行に関していかなる責任も負わない。

９．６　責任制限

９．６．１　利用者の義務違反

本認証局は、利用者が本 CP/CPS9.4.3 に違反したことに起因して生じた損害について、関係者に対し一切の責任を負わない。

利用者が本 CP/CPS9.4.3 に述べる責任・義務に違反していることが明らかな場合、本認証局は利用者への事前の通知を行うことなく、利用者に対して発行した利用者証明書を失効させることができるものとし、これに対し利用者は一切の請求、異議申し立てを行うことができない。

９．６．２　署名検証者の義務違反

本認証局は、署名検証者が本 CP/CPS9.4.4 に違反したことに起因して生じた損害について、関係者に対し一切の責任を負わない。

９．６．３　不可抗力等

(1)　電子証明書や CRL の取得、利用等により利用者もしくは署名検証者等のコンピュータシステム等に合理的な管理を超える状況により何らかの影響、障害が生じても、その責任を一切負わない。

(2)　利用者からの失効申請に伴う本認証局内での失効処理が、正当な事由により遅延した場合、これにより発生した損害については、損害賠償責任を一切負わない。

(3)　本認証局の廃止に伴う事前通知を実施し、廃止以降に発生した損害については、損害賠償責任を一切負わない。

(4)　次に掲げる事象または状況によって利用者、その他第三者（署名検証者を含むがこれに限らない）に損害が生じた場合でも、その責任を一切負わない。

（ア）　天災：火災、雷、噴火、洪水、地震、嵐、台風、津波等

（イ）　人災：戦争、革命、暴動、内乱、労働争議等

（ウ）　裁判所、政府、行政、省庁等による作為、不作為、命令等

（エ）　電源の供給停止、回線の停止等、本認証局以外のシステムの停止

（オ）　技術上もしくは運用上緊急に本認証局に係るシステムを停止する必要があると本認証局が判断した場合

（カ）　本認証局が、本 CP/CPS に基づく義務を適切に履行したにも関わらず、不完全履行もしくは履行遅滞を生じさせ、かかる結果に至ることとなった事象または状況

（キ）　当社が責任を負わない事由としてサービス規約に記載されている事由その他本認証局の責に帰すべからざる事由

９．７　補償

利用者、署名検証者の行為に起因して、第三者に損害が生じた場合、本認証局は免責されるものとし、利用者または署名検証者が、損害賠償の責めを負う。

９．８　文書の有効期間と終了

９．８．１　文書の有効期間

本 CP/CPS は、当社が本 CP/CPS をウェブサイト上に掲載した日より有効となる。本 CP/CPS9.8.2 で記載する本 CP/CPS の終了以前に本 CP/CPS が無効となることはない。

９．８．２　終了

本 CP/CPS は、本 CP/CPS9.8.3 に掲げる存続条項を除き、本認証局が業務を終了した時点で無効となる。

９．８．３　終了の影響と存続条項

本 CP/CPS9.2、9.3、9.4、9.5、9.6、9.7、9.8.2、9.8.3、9.11、9.12、9.13 の規定については本 CP/CPS の終了後も、存続するものとする。

９．９　個々の関係者間に対する通知と連絡

本認証局から利用者に対し個別の通知が必要となった場合、適切な手段をもって行う。

９．１０　改訂

９．１０．１　改訂手続き

当社の認証局事務局は、適宜、本 CP/CPS の改訂を行うことができる。認証局員の評価、または弁護士等外部の専門家または有識者の評価を得た後、認証局事務局が改訂の承認を行う。

９．１０．２　通知方法と期間

本 CP/CPS の内容に変更があった場合は、リポジトリにて適宜通知する。

９．１０．３　オブジェクト識別子の変更理由

本認証局では、オブジェクト識別子は証明書フォーマットで固定されるため規定しない。

９．１１　紛争解決手続き

本 CP/CPS に基づく認証業務から生じる紛争については、東京地方裁判所を第一審の専属管轄裁判所とする。

９．１２　準拠法

本 CP/CPS に基づく認証業務から生じる紛争については、日本国の法令を適用する。

９．１３　準拠法の遵守について

関係者は、本 CP/CPS9.12 の準拠法を遵守する。

９．１４　その他の条項

９．１４．１　完全合意

本 CP/CPS における合意事項は、特段の定めをしている場合を除き、本 CP/CPS が改訂または終了されない限り、他のすべての合意事項より優先される。

９．１４．２　譲渡

本認証局は、本認証局に関わる業務について、第三者への事業譲渡を行わない。

９．１４．３　分離可能性

本 CP/CPS 中のある規定が、何らかの理由により、無効または執行不可能であるとされた場合においても、残余の規定は有効であり、当事者の意思に最も合理的に合致するよう解釈する。

責任制限、保証、免責、または損害の排除等について規定する本 CP/CPS の各条項は、他の規定とは分離し、また、その条項に従って執行可能であることにつき当事者は合意するものとする。

９．１４．４　執行（弁護士費用と権利の放棄）

利用者は、本サービスに関する紛争のために負担した弁護士費用について、当社に請求することはできないものとする。また、利用者の本サービスにかかる契約違反に対する当社の請求権放棄は、本サービス以外の契約への違反に対する請求権の放棄とはならないものとする。

９．１４．５　改廃

附則に準ずる。

附則

本 CP/CPS は、2019 年 8 月 19 日から施行する。

１０．　用語集

あ行

- アーカイブ（Archive）
  証明書の発行履歴、失効履歴等を必要に応じて閲覧可能な状態にて長期間保管すること。

- アクセス制御（Access Control）
  ユーザの権限に応じた制御を行う方法。データへのアクセスについて、閲覧が許可されている人に限りアクセスできるように物理的、電子的な手法で制御すること。

- アルゴリズム（Algorithm）
  ここにおいては、暗号化アルゴリズムをさす。暗号化アルゴリズムは、情報に対して一連の変換を施して情報を第三者に理解困難な形式にするための数学的に表現した規則の集まりを指す。

- 暗号モジュール（Cryptographic Module）
  暗号鍵等の生成、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されるソフトウェア、ハードウェアあるいはそれらを組み合わせた装置。

か行

- 鍵ペア（Key Pair）
  公開鍵暗号方式における公開鍵およびそれに対応する署名鍵。２つの鍵は、一方の鍵から他方の鍵を導き出せない性質を持つ。

- 鍵長（Key Length）
  鍵の長さをビット数で表したもの。暗号の強度を決定する要素の１つ。一般に鍵長が長いほど解読がされにくいとされる。

- 鍵の預託（Key Escrow）
  署名鍵または公開鍵を第三者機関に登録保管すること。

- 活性化（Activation）
  システムや装置等を使用可能な状態にすること。

- 活性化情報（Activation Data）
  システムや装置等を活性化するために必要となるデータ。具体的には、PIN コードやパスフレーズ等を指す。

- 危殆化（Compromise）
  署名鍵や関連署名情報等の署名性が、盗難や漏洩、第三者による解読等によって失われた、もしくは失われた可能性のある事態の発生をいう。認証局の署名鍵が危殆化した場合、当該認証局から発行された全ての証明書の信頼性が失われる。

- 公開鍵（Public Key）
  公開鍵暗号方式における鍵ペアのうちの一つで、通信相手等の他人に知らせて利用してもらうための鍵。電子署名の検証に用いる場合、署名検証鍵とも呼称される。

- 公開鍵暗号方式（Public Key Cryptographic Algorithm）
  関連した２つの鍵（公開鍵と署名鍵）を使用する非対称暗号方式(asymmetric cryptographic algorithm)の１つであり、一方の鍵（公開鍵）で暗号化したデータは、他方の鍵（署名鍵）でのみ復号できるようになっている。

さ行

- 自己署名証明書（Self-signed Certificate）
  認証局が、自己を証明するために発行する証明書。証明書に記載される証明書発行主体（Issuer）と被発行者（Subscriber）とが同一になっている。本 CP/CPS では認証局証明書と記載している。

- 失効（Revocation）
  証明書の有効期間内に、署名鍵が危殆化もしくはその可能性が発生した場合、証明書の記載内容に変更が生じた場合等に、対象の証明書を無効にすること。

- 証明書（Certificate）
  認証対象者の識別情報と公開鍵とが対応していることを証明する電子文書。認証対象者の識別情報、その公開鍵、鍵の利用目的・範囲、発行認証局名などが含む一連の情報に、認証局の電子署名を付加したもの。

- 証明書失効リスト（Certificate Revocation List = CRL）
  失効した証明書のリスト。失効リストには、証明書を発行した認証局による電子署名

が付される。

- 証明書ポリシー（Certificate Policy = CP）
  認証局が証明書を発行する際の運用方針を定めた文書。

- 署名鍵（Private Key）
  公開鍵暗号方式における鍵ペアのうちの一つで、他人には知られないようにしておく鍵。電子署名の作成に用いられるため、署名鍵とも呼称される。

- 署名鍵管理モジュール（Hardware Security Module = HSM）
  暗号モジュールのうちハードウェアにより署名鍵を安全に管理する装置。主に認証局で使用され、耐タンパ性をもち安全な署名鍵管理機能を備えた暗号モジュールのこと。「暗号モジュール」参照。

た行

- 登録局（Registration Authority = RA）
  証明書の発行や失効のプロセスにおいて、本人性確認や認証局システムへのデータ登録等の一部機能を認証局の承認を受けて行う組織。登録局は、証明書および失効リストの生成は行わない。

- 電子署名（Electronic Signature）
  間違いなく本人であることを証明する電子的なデータで、広義ではアナログ署名を電子データにしたものも含まれるが、ここでは、デジタル署名(digital signature)の意味で用いる。具体的には、署名対象データのハッシュ値に対して、署名鍵で暗号化したもの。電子署名の検証は､電子署名を公開鍵で復号した値と元のデータのハッシュ値とを照合することで可能となる。

な行

- 認証局（Certification Authority = CA）
  証明書の発行、失効、失効リストの開示等のサービスを行う信頼された組織。

- 認証局運用規程（Certification Practice Statement = CPS）
  認証局の信頼性、安全性を対外的に示すために、認証局の運用規則、鍵の生成・管理、遵守事項等を文書化したもの。利用者・署名検証者等の認証局の外部者に開示されるもの。

は行

- 発行局（Issuing Authority = IA）
  登録局において審査・承認され、送信される証明書の発行指示に対し、電子署名を行い、電子証明書を発行する機関。

- ハッシュ関数（Hash Function）
  データを数学的な操作によって一定の長さに縮小させる関数であり、異なる２つの入力値から同じ出力値を算出することが困難な関数。出力値から入力値を逆算することは不可能。

- ハッシュ値（Hash Value）
  ある値に対するハッシュ関数の出力値。「ハッシュ関数」参照。

- フィンガープリント（Finger Print）
  自己署名証明書などの証明書が改ざんされていないことを証明するためのデータ（ハッシュ値）のことをいう。その証明書が唯一無二であることを証明できることから、拇印と呼ばれている。SHA-1（ハッシュ関数）により算出したフィンガープリントは、40 桁の 16 進数であり、「0」～「9」及び「A」～「F」の文字の組合せで示される。ただし、フィンガープリントを表示するソフトウェアの種類又はバージョンにより、大文字又は小文字の相違、「:」又は「 」（スペース）の付加等表示方法が異なることがある。

- 複数人管理（Dual Control）
  署名情報へのアクセス､システム運用・操作等における不正行為を防止する為に、複数の人間に管理機能を分散させ、全員がそれぞれの管理機能を遂行してはじめて所定の機能が働くようにする作業方式または管理方式。

- プロファイル（Profile）
  証明書（自己署名証明書、利用者用証明書）、失効リスト（CRL）等の設定情報のこと。

- ポリシー承認局(Policy Authority = PA)
  本認証局のポリシーの決定や CPS（本 CP/CPS）の承認等を行う、本認証局における最高意思決定機関。当社のセキュリティ委員会をいう。

- 本人性確認（Identification and Authentication）
  個人や機器等の認証対象に関する情報が、本人（本体）のものであることを審査する行為。

ま行

ら行

- リポジトリ（Repository）
  証明書や失効リスト、CPS 等を保管し、証明書利用者等に対してこれらの開示等のサービスを提供するシステム。

- 利用者（Subscriber）
  本認証局への申請主体である個人もしくは機器等であり、実際に証明書を利用する者を指す。

- ログ（Log）
  コンピュータの利用状況や通信の記録。操作やデータの送受信等が行われた日時と、操作者、操作内容、通信内容等が記録される。

Ａ－Ｇ

- CA（Certification Authority）
  「認証局」参照。

- CN（Common Name）
  ITU-T（国際電気通信連合－Ｔ）が策定した X.500 勧告において定められた、識別名（Distinguished Name）の中のひとつの属性。通常、一般的な名称（対象が人であれば人名）を表す。

- CP（Certificate Policy）
  「証明書ポリシー」参照。

- CPS（Certification Practices Statement）
  「認証局運用規程」参照。

- CRL（Certificate Revocation List）
  「証明書失効リスト」参照。

- DN（Distinguished Name）
  ITU-T（国際電気通信連合－Ｔ）が策定したX.500 勧告において定められた識別名。CO（Organization Name = 組織名）、OU（Organization Unit Name = 組織部局名）、CN（Common Name = 一般名）等の属性で構成される。

- FIPS 140-2（Federal Information Processing Standard 140-2）
  FIPS は商務省連邦情報処理規格を指し、FIPS 140 は暗号モジュール用セキュリティ要件を規定している。2019 年 7 月現在の規格の最新版は 2001 年 5 月発行の FIPS 140-2 である。暗号モジュールは、セキュリティレベルという段階基準があり、どの要件に適合するかにより、最低レベル 1 から最高レベル 4 のいずれかに当てはめられる。

Ｈ－Ｎ

- HSM（Hardware Security Module）
  「署名鍵管理モジュール」参照。

- IETF（Internet Engineering Task Force）
  インターネットで利用される技術を標準化する組織。インターネットの標準化を統括する IAB の下部機関。ここで策定された技術仕様は RFC として公表される。

- ISO(International Organization for Standardization)
  国際標準化機構。電気分野を除くあらゆる分野において、国際的に通用する規格・標準類の制定を目的としている。

- ITU（International Telecommunication Union）
  国際連合(UN)の専門機関の１つである国際電気通信連合。電気通信の改善、合理的利用を目的としている。

- ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)
  国際電気通信連合の電気通信標準化部門。

O－U

- OCSP（Online Certificate Status Protocol）
  証明書のステータス(失効・一時停止していないかどうか)をオンラインで問い合わせるプロトコル。OCSP クライアントと OCSP レスポンダ（サーバ）との間の通信方法について取り決めている。OCSP クライアントは、OCSP レスポンダに対して、対象となる証明書のシリアル番号を、電子署名付きで送信する。
  OCSP レスポンダは、問い合わせのあった証明書の状態を電子署名付きで返答する。

- OID（Object Identification：オブジェクト識別子）
  世界で一意となる値を登録機関（ISO、ITU）に登録した識別子。暗号アルゴリズムや証明書内に格納する名前（subject）のタイプ（Country 名等の属性）等は、オブジェクト識別子として登録されているものが使用される。

- PIN（Personal Identification Number）
  個人識別番号のこと。本認証局においては、利用者の署名鍵を活性化するための PIN がこれに該当する。

- PKI（Public Key Infrastructure）
  公開鍵暗号方式を用いて情報システム、コミュニケーションシステムのセキュリティを確保するための一連の技術及びサービス。

- RA（Registration Authority）
  「登録局」参照。

- RFC3647（Request For Comments 3647）
  RFC とは、インターネットに関する標準文書の総称。その１つである RFC3647 は、CP もしくは CPS を作成するためのフレームワーク及びガイドラインを提供している。

- RSA
  Rivest、Shamir、Adelman の 3 人が開発した公開鍵暗号方式の一つ。

- SHA-1（Secure Hash Algorithm -1）
  電子署名等に使われるハッシュ関数のひとつ。原文から 160 ビットのハッシュ値を発生し、通信経路の両端で比較することで、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。不可逆な一方向関数を含むため、ハッシュ値から原文を再現することはできず、また同じハッシュ値を生成する別のメッセージを作成することは極めて困難である。

- SHA256（Secure Hash Algorithm 256）
  SHA-1 の後継となるハッシュ関数 SHA-2 のバリエーションの 1 つ。原文から 256 ビットのハッシュ値を生成する。

Ｖ－Ｚ

- X.500
  X.500 シリーズは、ITU-T で 1988 年に規格化されたディレクトリ・サービスの勧告（国際標準）であり 1997 年に新しい仕様が加えられている。この仕様には、ディレクトリの概念やその階層構造、サービスやオブジェクトの定義などが含まれる。

- X.509
  ITU-T が定めた、証明書に関する規格。バージョンが 1，2，3 とある。本認証局が発行する証明書はバージョン 3 を用いており、CRL はバージョン 2 を用いている。

- X.509v3
  証明書に関する ITU-T 規格のバージョン 3。既にエクステンション（拡張領域）を含むか、含むことが可能な証明書のこと。電子署名、否認防止等の鍵利用目的が設定される。

- X.509v3 key usage
  証明書エクステンションの一つで、鍵が利用される目的を設定する項目のこと。電子署名、否認防止等の鍵利用目的がある。

１１．　証明書プロファイル

１１．１　認証局証明書

(1) 証明書基本領域(Basic)

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier	電子証明書への署名に使用された署名アルゴリズムの識別子	
Algorithm	署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫	 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	署名アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**値**
CountryName	電子証明書発行者の国名	
Type	国名のオブジェクト ID 型：OID 値：2 5 4 6	 2.5.4.6
Value	国名の値 型：PrintableString 値：JP	 JP
OrganizationName	電子証明書発行者の組織名	
Type	組織名のオブジェクト ID 型：OID 値：2 5 4 10	 2.5.4.10

Value	組織名の値	
	型：PrintableString	
	値：<<名称>>	NS Solutions Corporation
OrganizationalUnitName	電子証明書所有者の部署名	
Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString	
	値：<<部署名称>>	IT infrastructure Solutions Bureau
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<認証局名称>>	NSSOL e-Contract-CA-G1
Validity		**値**
Validity	電子証明書の有効期間	15 年 1 ヶ月
notBefore	開始日時	
	型：UTCTime	＊有効開始日時
	値：yymmddhhmmssZ	190409152932Z
notAfter	終了日時	
	型：UTCTime	＊有効終了日時
	値：yymmddhhmmssZ	340509152932Z
Subject		**値**
CountryName	電子証明書発行者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	電子証明書発行者の組織名	
Type	組織名のオブジェクト ID	

	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString	
	値：<<名称>>	NS Solutions Corporation
OrganizationalUnitName	電子証明書所有者の部署名	
Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString	
	値：<<部署名称>>	IT infrastructure Solutions Bureau
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<認証局名称>>	NSSOL e-Contract-CA-G1
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子認証書発行者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	RSA Encryption
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	2048Bit

(2) 証明書標準拡張領域(extensions)

basicConstraints (extnId ::== 2 5 29 19, critical ::== TRUE)		**値**
BasicConstraints	基本的制限	

cA	CA かどうかを示すフラグ 型：Boolean 値：True（CA である）	 TRUE
subjectKeyIdentifier (extnId ::= 2 5 29 14，critical ::= FALSE)		**値**
SubjectKeyIdentifier keyIdentifier	電子証明書発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値:発行者の subjectPublicKey の Hash 値	 66:92:bf:b0:6a:9c:63:e4:20:18:37:3a:1f:e5:5d:64:48:6f:fc:52
keyUsage　(extnId ::= 2 5 29 15，critical ::= TRUE)		**値**
KeyUsage	鍵の使用目的 型：BitString 値：11000110 (digitalSignature,NonRepudiation, CertificateSigning,CRLSigning)	 11000110

１１．２　証明書失効リスト

(1) CRL 標準領域(Basic)

Version		**値**
Version	フォーマットのバージョン番号 型：INTEGER 値：1	 1 (Ver.2)
Signature		**値**
AlgorithmIdentifier	証明書失効リストへの署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数）	
Algorithm	署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫	 1.2.840.113549.1.1.11(SHA256withRSA)
Parameters	署名アルゴリズムの引数 型：NULL 値：	 NULL
Issuer		**値**
CountryName	証明書失効リスト発行者の国名	
Type	国名のオブジェクト ID 型：OID 値：2 5 4 6	 2.5.4.6
Value	国名の値 型：PrintableString 値：JP	 JP
OrganizationName	証明書失効リスト発行者の組織名	
Type	組織名のオブジェクト ID 型：OID 値：2 5 4 10	 2.5.4.10
Value	組織名の値 型：PrintableString 値：<<名称>>	 NS Solutions Corporation
OrganizationalUnitName	電子証明書所有者の部署名	
Type	部署名のオブジェクト ID 型：OID	

	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString	
	値：<<部署名称>>	IT infrastructure Solutions Bureau
CommonName	証明書失効リスト発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<発行局名称>>	NSSOL e-Contract-CA-G1
thisUpdate		**値**
thisUpdate	有効開始日	
	型：UTCTime	＊有効開始日時
	値：yymmddhhmmss	例 yymmddhhmmss
nextUpdate		**値**
nextUpdate	次回更新予定日時	有効開始日から 7 日間後
	型：UTCTime	＊更新予定日時
	値：yymmddhhmmss	例 yymmddhhmmss

(2) CRL 標準拡張領域(extensions)

authorityKeyIdentifier (extnId ::== 2 5 29 35，critical ::== FALSE)		**値**
AuthorityKeyIdentifier	証明書失効リスト発行者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	
	値:認証局の subjectPublicKey の Hash 値	66:92:bf:b0:6a:9c:63:e4:20:18:37:3a:1f:e5:5d:64:48:6f:fc:52
cRLNumber (extnId ::== 2 5 29 20，critical ::== FALSE)		**値**
cRLNumber	CRL の番号	
	型：INTEGER	
	値：ユニークな整数	＊CRL の番号

(3) CRL エントリ領域

revokedCertificates		**値**
CertificateSerialNumber	証明書失効リストのシリアル番号	

	型：INTEGER 値：ユニークな整数	＊シリアル番号
revocationDate	失効日時 型：UTCTime 値：yymmddhhmmss	

(4) CRL エントリ拡張領域

invalidityDate (extnId ::== 2 5 29 24, critical ::== FALSE)		**値**
invalidityDate	無効化日時 型：GeneralizedTime 値：yyyymmddhhmmssz	
cRLReason (extnId ::== 2 5 29 21, critical ::== FALSE)		**値**
cRLReason	失効理由コード	(1) keyCompromise (2) cACompromise (3) affiliationChanged (4) superseded (5) cessationOfOperation *unspecified は、cRLReason として出力しない。

１１．３　利用者証明書

１１．３．１　（利用者証明書：個人）

(1) 証明書基本領域(Basic)

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier Algorithm Parameters	電子証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫ 署名アルゴリズムの引数 型：NULL 値：NULL	 1.2.840.113549.1.1.11(SHA256withRSA) NULL NULL
Issuer		**値**
CountryName Type Value OrganizationName Type	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 電子証明書発行者の組織名 組織名のオブジェクト ID	 2.5.4.6 JP

	型：OID	
	値：2 5 4 10	2.5.4.10
Value	組織名の値	
	型：PrintableString	
	値：<<会社名称>>	NS Solutions Corporation
OrganizationalUnitName	電子証明書所有者の部署名	
Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString	
	値：<<部署名称>>	IT infrastructure Solutions Bureau
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<発行局名称>>	NSSOL e-Contract-CA-G1
Validity		**値**
Validity	電子証明書の有効期間	
notBefore	開始日時	有効期間：最大 13 ヵ月
	型：UTCTime	＊有効開始日時
	値：yymmddhhmmssZ	yymmddhhmmss
notAfter	終了日時	
	型：UTCTime	＊有効終了日時
	値：yymmddhhmmssZ	yymmddhhmmss
Subject		**値**
CountryName	電子証明書所有者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	電子証明書所有者の住所	

Type	住所のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10
Value	住所の値	
	型：PrintableString or UTF8String	
	値：<<住所>>	住所
OrganizationalUnitName	JIPDEC 指定 OID	
Type	JIPDEC 指定のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	JIPDEC 指定 OID の値	
	型：PrintableString	
	値：<<JIPDEC 指定 OID>>	JIPDEC 指定 OID
OrganizationalUnitName	電子証明書所有者の備考	
Type	備考のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	備考の値	
	型：PrintableString or UTF8String	
	値：<<備考>>	備考
OrganizationalUnitName	電子証明書所有者のメールアドレスまたは携帯電話番号	
Type	メールアドレスまたは携帯電話番号のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	メールアドレスまたは携帯電話番号の値	
	型：PrintableString or UTF8String	
	値：<<メールアドレスまたは携帯電話番号>>	メールアドレスまたは携帯電話番号
OrganizationalUnitName	電子証明書所有者の生年月日	
Type	生年月日のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	生年月日の値	
	型：PrintableString or UTF8String	

	値：<<生年月日>>	生年月日
CommonName	電子証明書所有者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString or UTF8String	
	値：証明書 ID-<<利用者の氏名>>	証明書 ID-利用者の氏名
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子証明書所有者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL
	値：NULL	NULL
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	2048Bit

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (extnId ::= 2 5 29 35，critical ::= FALSE)		**値**
AuthorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	
	値：認証局の subjectPublicKey の Hash 値	*電子証明書発行者の証明書の subjectPublicKey の Hash 値
subjectKeyIdentifier (extnId ::= 2 5 29 14，critical ::= FALSE)		**値**
SubjectKeyIdentifier	電子証明書所有者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	
	値：所有者の subjectPublicKey の Hash 値	*利用者証明書の subjectPublicKey の Hash 値

keyUsage　(extnId ::== 2 5 29 15，critical ::== FALSE)		値
KeyUsage	鍵の使用目的 型：BitString 値：111000000 (digitalSignature, nonRepudiation ,keyEncipherment)	111000000
cRLDistributionPoints (extnId ::== 2 5 29 31，critical ::== FALSE)		**値**
cRLDistributionPoints DistributionPoint fullName	CRL 配付ポイント CRL 配付ポイント CRL を配付する URI 型：IA5 String 値：http URI	*CRL が配布される URI http://mpkicrl.managedpki.ne.jp/mpki/NSSOLe-Contract-CA-G1/cdp.crl

１１．３．２　（利用者証明書：法人）

(1) 証明書基本領域(Basic)

Version		**値**
Version	電子証明書フォーマットのバージョン番号 型：INTEGER 値：2	 2 (Ver.3)
serialNumber		**値**
CertificateSerialNumber	電子証明書のシリアル番号 型：INTEGER 値：ユニークな整数	 ＊シリアル番号
Signature		**値**
AlgorithmIdentifier Algorithm Parameters	電子証明書への署名に使用された署名アルゴリズムの識別子 （公開鍵暗号とハッシュ関数） 署名アルゴリズムのオブジェクト ID 型：OID 値：≪署名アルゴリズム≫ 署名アルゴリズムの引数 型：NULL 値：NULL	 1.2.840.113549.1.1.11(SHA256withRSA) NULL NULL
Issuer		**値**
CountryName Type Value OrganizationName Type Value	電子証明書発行者の国名 国名のオブジェクト ID 型：OID 値：2 5 4 6 国名の値 型：PrintableString 値：JP 電子証明書発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10 組織名の値	 2.5.4.6 JP 2.5.4.10

	型：PrintableString	
	値：<<会社名称>>	NS Solutions Corporation
OrganizationalUnitName	電子証明書所有者の部署名	
Type	部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	部署名の値	
	型：PrintableString	
	値：<<部署名称>>	IT infrastructure Solutions Bureau
CommonName	電子証明書発行者の固有名称	
Type	固有名称のオブジェクト ID	
	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString	
	値：<<発行局名称>>	NSSOL e-Contract-CA-G1
Validity		**値**
Validity	電子証明書の有効期間	
notBefore	開始日時	有効期間：最大 13 ヵ月
	型：UTCTime	＊有効開始日時
	値：yymmddhhmmssZ	yymmddhhmmss
notAfter	終了日時	
	型：UTCTime	＊有効終了日時
	値：yymmddhhmmssZ	yymmddhhmmss
Subject		**値**
CountryName	電子証明書所有者の国名	
Type	国名のオブジェクト ID	
	型：OID	
	値：2 5 4 6	2.5.4.6
Value	国名の値	
	型：PrintableString	
	値：JP	JP
OrganizationName	電子証明書所有者の取引会社名	
Type	取引会社名のオブジェクト ID	
	型：OID	
	値：2 5 4 10	2.5.4.10

Value	取引会社名の値	
	型：PrintableString or UTF8String	
	値：<<取引会社名>>	取引会社名
OrganizationalUnitName	JIPDEC 指定 OID	
Type	JIPDEC 指定のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	JIPDEC 指定 OID の値	
	型：PrintableString	
	値：<<JIPDEC 指定 OID>>	JIPDEC 指定 OID
OrganizationalUnitName	電子証明書所有者の備考	
Type	備考のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	備考の値	
	型：PrintableString or UTF8String	
	値：<<備考>>	備考
OrganizationalUnitName	電子証明書所有者のメールアドレスまたは固定電話番号	
Type	メールアドレスまたは固定電話番号のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	メールアドレスまたは固定電話番号の値	
	型：PrintableString or UTF8String	
	値：<<メールアドレスまたは固定電話番号>>	メールアドレスまたは固定電話番号
OrganizationalUnitName	電子証明書所有者の役職・部署名	
Type	役職・部署名のオブジェクト ID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	役職・部署名の値	
	型：PrintableString or UTF8String	
	値：<<役職>>-<<部署名>>	役職-部署名
CommonName	電子証明書所有者の固有名称	
Type	固有名称のオブジェクト ID	

	型：OID	
	値：2 5 4 3	2.5.4.3
Value	固有名称の値	
	型：PrintableString or UTF8String	
	値：証明書 ID-<<利用者の氏名>>	証明書 ID-利用者の氏名
subjectPublicKeyInfo		**値**
SubjectPublicKeyInfo	電子証明書所有者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵暗号とハッシュ関数）	
Algorithm	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
	型：OID	
	値：1 2 840 113549 1 1 1	1.2.840.113549.1.1.1
parameters	署名アルゴリズムの引数	
	型：NULL	NULL
	値：NULL	NULL
subjectPublicKey	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	2048Bit

(2) 証明書標準拡張領域(extensions)

authorityKeyIdentifier (extnId ::== 2 5 29 35，critical ::== FALSE)		**値**
AuthorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	
	値：認証局の subjectPublicKey の Hash 値	*電子証明書発行者の証明書の subjectPublicKey の Hash 値
subjectKeyIdentifier (extnId ::== 2 5 29 14，critical ::== FALSE)		**値**
SubjectKeyIdentifier	電子証明書所有者の公開鍵に関する情報	
keyIdentifier	公開鍵の識別子	
	型：OCTET STRING	
	値：所有者の subjectPublicKey の Hash 値	*利用者証明書の subjectPublicKey の Hash 値
keyUsage　(extnId ::== 2 5 29 15，critical ::== FALSE)		**値**
KeyUsage	鍵の使用目的	
	型：BitString	

	値：111000000 (digitalSignature, nonRepudiation ,keyEncipherment)	111000000
cRLDistributionPoints (extnId :== 2 5 29 31，critical :== FALSE)		**値**
cRLDistributionPoints DistributionPoint fullName	CRL 配付ポイント CRL 配付ポイント CRL を配付する URI 型：IA5 String 値：http URI	 *CRL が配布される URI http://mpkicrl.managedpki.ne.jp/mpki/NSSOLe-Contract-CA-G1/cdp.crl