Enterprise Premium - G3 認証局

運用管理規程

Ver 2.2

2024 年 01 月 22 日

三菱電機インフォメーションネットワーク株式会社

改定履歴

版数	日付	内容	作成者	承認者
1.0	201609/14	初版作成	合田　悠資	中村 克巳
1.1	2017/04/06	ADFS デバイス証明書に有効期間 1 年を追加 誤記訂正	合田　悠資	中村 克巳
2.0	2018/07/02	運営組織変更に伴う改定	久保田　大稀	中村 克巳
2.1	2020/03/16	「1.5.2 問い合わせ先」を変更	久保田　大稀	中村 克巳
2.2	2024/01/22	「4.9.7 CRL 発行頻度」の記載を追記・修正	合田 悠資	中田 雅宏

－目次－

1　はじめに

1.1　概要

Enterprise Premium - G3 認証局運用管理規程（以下、「CPS」という）は、三菱電機インフォメーションネットワーク株式会社が運営する「Enterprise Premium - G3 認証局」（以下、「本認証局」という）の CPS（Certification Practice Statement)であり、証明書発行（失効も含む）に関して「適用範囲」、「セキュリティ基準」、「審査基準」等の一連の規則を定めるものである。

本認証局が提供する電子証明書発行サービスを「Enterprise Premium 電子証明書発行サービス」（以下、「本サービス」という）と呼ぶ。

本 CPS は、インターネットについて、その仕様等の標準化活動を行なっている組織（IETF：Internet Engineering Task Force）におけるインターネット X.509 PKI 証明書ポリシと認証実施フレームワーク「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」（RFC3647）に従い、加入者証明書の発行、失効及びその他の運用管理等の手続きについて規定した本認証局最高位の規程であり、公開文書である。また、公開鍵インフラストラクチャ（PKI： Public Key Infrastructure。以下「PKI」という。）の構成要素である認証局、加入者及び検証者の義務と責任について規定する。

1.2　文書の名前と識別

本認証局に係るオブジェクト識別子（OID）を表 1-1 に示す。

表 1-1　本認証局に係るオブジェクト識別子

OID	オブジェクト
1.2.392.200127	三菱電機インフォメーションネットワーク株式会社
1.2.392.200127.9	Enterprise Premium 電子証明書発行サービス
1.2.392.200127.9.2	Enterprise Premium - G3 認証局運用管理規程（CPS）

1.3　PKI の関係者

1.3.1　認証局

本認証局は、発行局（IA)と登録局（RA）により構成される。

登録局（RA）は審査登録局（本 CPS では特に断らない限り RA とする）と企業内審査登録局（以下、「企業内 RA」という）により構成される。

1.3.2　審査登録局

審査登録局は、本サービスの契約企業（以降、契約企業という）からの企業内審査登録局設置申込みについて確認を行い、許可した企業内 RA の責任者等の登録を行う。

企業内 RA から受け付けた証明書発行要求又は証明書失効要求について、書類等の確認を行い、所定の証明書発行要求又は証明書失効要求を発行局へ行う。

但し、審査登録局は本 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を外部に委託することができる。

1.3.3　企業内 RA

企業内の加入者から受け付けた証明書発行申請又は失効申請について真偽確認を行い、許可した加入者の証明書発行要求又は証明書失効要求を審査登録局へ行う。

但し、企業内 RA は本 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を外部に委託することができる。

1.3.4　発行局

発行局は審査登録局からの証明書発行要求又は証明書失効要求に基づき証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行う。

但し、本認証局は本 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。

1.3.5　加入者

加入者とは、証明書所有者である。証明書所有者とは、証明書申請を行い認証局により証明書を発行される者をさす。

1.3.6　検証者

検証者とは、加入者の認証又は加入者の電子署名を検証する者をさす。

1.3.7　その他の関係者

規定しない。

1.4　証明書の使用方法

1.4.1　適切な証明書の使用

本 CPS で定める加入者証明書は、証明書の種類に応じてデバイス認証、電子署名、クライアント認証、ネットワーク機器用サーバ認証及び Web サーバ認証の用途で使用できる。証明書の種類とその用途の対応は下記のとおりとする。本 CPS では以降特別に断りがない

限り 7 種類の証明書を総称して「証明書」という。

(1)　「デバイス証明書」: デバイス認証
(2)　「ADFS デバイス証明書」: ADFS 用デバイス認証
(3)　「クライアント証明書 for Sign」: 電子署名
(4)　「クライアント証明書 for Auth」: クライアント認証
(5)　「ネットワーク機器用サーバ証明書」: ネットワーク機器用サーバ認証
(6)　「Web サーバ用証明書」: Web サーバ認証

1.4.2　禁止される証明書の使用

本サービスにより発行される加入者証明書は、本 CPS「1.4.1　適切な証明書の使用」に規定する用途のみに使用するものとする。加入者証明書が用途以外の目的で使用された場合は、本認証局は一切の責任を負わないものとする。

1.5　ポリシ管理

1.5.1　本ポリシを管理する組織

本 CPS の管理組織は、三菱電機インフォメーションネットワーク株式会社とする。

1.5.2　問い合わせ先

本 CPS に関する問い合わせ先を以下のように定める。

【問い合わせ先】
窓口：三菱電機インフォメーションネットワーク株式会社
住所：〒108-0023　東京都港区芝浦 4-6-8　田町ファーストビル
電子メールでの問い合わせ：
ホームページ（https://www.mind.co.jp/）の「お問い合わせ」→「サービス・製品一覧」→「MIND トラストサービス TrustMinder」内の"Enterprise Premium 電子証明書発行サービス（EPPCERT）"から受け付ける。
受付日：月曜日から金曜日（祝祭日、当社休業日を除く）
受付時間：9:00～12:00　13:00～17:00（日本時間）

1.5.3　CPS のポリシ適合性を決定する者

本 CPS「1.5.1 本ポリシを管理する組織」の規定に従うものとする。

1.5.4　CPS 承認手続き

本 CPS は、三菱電機インフォメーションネットワーク株式会社によって承認されるも

のとする。

1.6 定義と略語

（あ～ん）

・ アーカイブ（Archive）
電子証明書の発行・失効に関わる記録や、認証局のシステム運用に関わる記録等を保管すること。

・ 暗号アルゴリズム（Algorithm）
暗号化／復号には、対になる 2 つの鍵を使う公開鍵暗号と、どちらにも同じ鍵を用いる共通鍵暗号（秘密鍵暗号）がある。前者には RSA、ElGamal 暗号、楕円曲線暗号などがあり、後者には米国政府標準の DES や近年新しく DES の後継として決まった AES などがある。

・ 暗号モジュール（Security Module）
私有鍵や証明書等を安全に保管し、鍵ペア生成や署名等の暗号操作を行うハードウェア又はソフトウェアのモジュール。

・エンドエンティティ（EndEntity）
証明書の発行対象者の総称。公開鍵ペアを所有している実体（エンティティ）で、加入者証明書を利用するもの。（個人、組織、デバイス、アプリケーションなど）
なお、認証局はエンドエンティティには含まれない。

・ オブジェクト識別子（Object Identifier）
オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

・ 活性化（Activate）
鍵を署名などの運用に使用することができる状態にすること。逆に、使用できなくすることを非活性化という。

・ 鍵長（Key Length）
鍵データのサイズ。鍵アルゴリズムに依存する。暗号鍵の強度は一般に鍵の長さによって決まる。鍵長は長ければ長いほど解読困難になるが、署名や暗号メッセージを作成する際の時間もかかるようになる。情報の価値を見計らって適切な鍵長を選択する必要がある。

・ 鍵の預託（Key Escrow）
第三者機関に鍵を預託すること。

・ 鍵ペア（Key Pair）
私有鍵とそれに対応する公開鍵の対。

・ 加入者（Subscriber）
証明書所有者である。証明書所有者とは、証明書申請を行い認証局により証明書を発行される者

・ 加入者証明書
認証局から加入者に対して発行された公開鍵証明書のこと。

・ 危殆化（Compromise）
私有鍵等の秘密情報が盗難、紛失、漏洩等によって、その秘密性を失うこと。

・ 公開鍵（Public Key）
私有鍵と対になる鍵で、署名の検証に用いる。公開鍵はたとえ公開されても秘密の私有鍵を類推することが困難である。

・ 公開鍵証明書（Public Key Certificate）
加入者の名義と公開鍵を結合して公開鍵の真正性を証明する証明書で、印鑑登録証明書に相当する。電子証明書あるいは単に証明書ともいう。公開鍵証明書には、公開鍵の加入者情報、公開鍵、認証局の情報、その他証明書の利用規則等が記載され、認証局の署名が付される。

・ 自己署名証明書（Self Signed Certificate）
認証局が自身のために発行する電子証明書。発行者情報と加入者情報が同じである。

・ 失効（Revocation）
有効期限前に、何らかの理由（盗難・紛失など）により電子証明書を無効にすること。基本的には、本人からの申告によるが、緊急時には認証局の判断で失効されることもある。

・ 証明書失効リスト（Certificate Revocation List、Authority Revocation List）

失効した電子証明書のリスト。
エンドエンティティの証明書の失効リストを CRL といい、認証局の証明書の失効リストを ARL という。

・ 証明書配付システム
加入者私有鍵及び加入者証明書をインターネット経由で加入者に配付するためのシステム。加入者の本人確認のため認証機能を有している。

・ 証明書発行要求（Certificate Signing Request）
申請者から認証局に電子証明書発行を求めるための要求。電子証明書を作成するための元となる情報で、その内容には、申請者の固有の ID、公開鍵などの情報が含まれる。

・ 証明書ポリシ（Certificate Policy：CP）
共通のセキュリティ要件を満たし、特定のコミュニティ及び／又はアプリケーションのクラスへの適用性を指定する、名前付けされた規定の集合。

・ 申請者（Applicant）
認証局に電子証明書の発行を申請する主体のこと。

・ 検証者（Relying Party）
文書の署名を加入者証明書の公開鍵で検証する者。

・ 電子署名（Digital Signature）
電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中に改ざんされていないことを証明することができる。公開鍵暗号方式を用いて生成した署名はデジタル署名ともいう。

・ 登録局（Registration Authority：RA）
電子証明書発行の申請者の本人を審査・確認し、主として登録業務を行う機関。登録局は、認証局の機能のうち、一部の業務を行う。認証する加入者の識別と本人性認証に責任を負うが、電子証明書に署名したり、発行したりはしない。

・ 認証局（Certification Authority：CA）
電子証明書を発行する機関。認証局は、公開鍵が間違いなく本人のものであると証

明可能にする第三者機関で、公正、中立な立場にあり信頼できなければならない。

・ 認証局運用管理規程（Certification Practice Statement：CPS）
証明書ポリシに基づいた認証局運用についての規定集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。

・ 登録審査室
認証業務用設備のうち、登録業務用設備のみが設置された室をいう。

・ 認証設備室
認証業務用設備（電子証明書の作成又は管理に用いる電子計算機その他の設備）が設置された室をいう。ただし、登録業務用設備のみが設置される場合を除く。

・ 発行局（Issuer Authority）
電子証明書の作成・発行を主として発行業務を行う機関。発行局は、認証局の機能のうち、一部の業務を行う。

・ ハッシュ関数（Hash Function）
任意の長さのデータから固定長のランダムな値を生成する計算方法。生成した値は「ハッシュ値」と呼ばれる。ハッシュ値は、ハッシュ値から元のデータを逆算できない一方向性と、異なる 2 つのデータから同一のハッシュ値が生成される衝突性が困難であるという性質を持つ。この性質からデータを送受信する際に、送信側の生成したハッシュ値と受信側でデータのハッシュ値を求めて両者を比較し両者が一致すれば、データが通信途中で改ざんされていないことが確認できる。

・ 私有鍵（Private Key）
公開鍵と対になる鍵。公開せず、他人に漏れないように鍵の加入者だけが管理する。私有鍵で署名したものは、それに対応する公開鍵でのみ検証が可能である。

・ プロファイル（Profile）
電子証明書や証明書失効リストに記載する事項及び拡張領域の利用方法を定めたもの。

・ リポジトリ（Repository）
電子証明書及び証明書失効リスト、その他公開文書を公開するシステム。

（A～Z）

- ADFS（Active Directory Federation Service）
  Microsoft Active Directory と ID 情報を連携してシングルサインオン環境を実現するサービス。

- ARL （Authority Revocation List）
  認証局の証明書の失効リスト、証明書失効リストを参照のこと。

- CA（Certification Authority）
  認証局を参照のこと。

- CA 証明書
  自己署名証明書を参照のこと。

- CPS（Certification Practice Statement）
  認証局運用管理規程を参照のこと。

- CRL（Certificate Revocation List）
  エンドエンティティの証明書の失効リスト、証明書失効リストを参照のこと。

- CRL 検証
  証明書失効情報が、認証局が発行する CRL に記載されているかを確認すること。

- CSR（Certificate Signing Request）
  証明書発行要求を参照のこと。

- DN（Distinguished Name）
  X.500 規格において定められた識別名。X.500 規格で識別子を決定することによって、加入者の一意性を保障する。

- FIPS 140-2（Federal Information Processing Standard）
  FIPS とは米国連邦情報処理標準で、FIPS140-2 は暗号モジュールが満たすべきセキュリティ要件を規定したもの。各セキュリティ要件に対して 4 段階のセキュリティレベル（最低レベル 1～最高レベル 4）を定めている。

- IA（Issuer Authority）

発行局を参照のこと。

- OID（Object ID）
  オブジェクト識別子を参照のこと。

- PKI（Public Key Infrastructure）
  公開鍵基盤。公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し、この証明書を用いて署名／署名検証、暗号／復号、認証を可能にする仕組み。

- RA（Registration Authority）
  登録局を参照のこと。

- RSA
  公開鍵暗号方式の一つ。Rivest、Shamir、Adleman の 3 名によって開発され、その名前をとって名付けられた。巨大な整数の素因数分解の困難さを利用したもので、公開鍵暗号の標準として普及している。

- SHA-1（Secure Hash Algorithm 1）
  ハッシュ関数の一つ。任意の長さのデータから 160bit のハッシュ値を作成する。

- SHA-256（Secure Hash Algorithm 256）
  ハッシュ関数の一つ。任意の長さのデータから 256bit のハッシュ値を作成する。

- X.500
  ITU-T/ISO が定めたディレクトリサービスに関する国際基準。

- X.509
  ITU-T/ISO が定めた電子証明書及び証明書失効リストに関する国際標準。X.509v3 では、電子証明書に拡張領域を設けて、電子証明書の発行者が独自の情報を追加することができる。

2　公開及びリポジトリの責任

2.1　リポジトリ

リポジトリは認証局の証明書及び加入者証明書の失効情報を保持し、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、一時的にリポジトリを利用できない場合もある。

2.2　証明書情報の公開

本認証局は、以下の情報を検証者と加入者が入手可能とする。

- 本認証局の CA 証明書
  http://www.eppcert.jp/
- CRL
  http://www.eppcert.jp/g3/rlist/epg3ca.crl

2.3　公開の時期又はその頻度

認証局は、認証局に関する情報が変更された時点で、その情報を公開するものとする。証明書失効についての情報は、本 CPS「4.9　証明書の失効と一時停止」に従うものとする。

2.4　リポジトリへのアクセス管理

リポジトリに公開する情報へのアクセス制御は行なわない。

3　識別及び認証

3.1　名称決定

3.1.1　名称の種類

本認証局が発行する電子証明書の発行者名（Issuer Name）及び加入者名（Subject Name）は、国際電気通信連合（ITU：International Telecommunication Union）で標準化されているディレクトリに関する一連の規格 X.500 識別名（DN：Distinguished Name）の形式に従い設定する。

3.1.2　名称が意味を持つことの必要性

本 CPS により発行する証明書の相対識別名は、検証者によって理解され、使用されるよう意味のあるものとする。

本認証局にて発行される証明書に記載される加入者情報(subject)の識別名(DN)は、証明書申請時に提出される申請書に記載された内容に基づいて、認証局側で設定する。

証明書に設定されている内容の詳細は、デバイス証明書の「subject」については表 3.1、ADFS デバイス証明書の「subject」については表 3.2、クライアント証明書 for Sign の「subject」については表 3.3、クライアント証明書 for Auth の「subject」については表 3.4、ネットワーク機器用サーバ証明書の「subject」については表 3.5、Web サーバ用証明書の「subject」については表 3.6 に示す。

表 3.1　デバイス証明書の加入者情報（subject）

属性	値	説明	備考
c（国名） 「OID：2.5.4.6」 countryName	“c=JP”で固定 （Printable）	日本を示す左記の国名を設定する。（英語）	－
o（組織名） 「OID：2.5.4.10」 organizationalName	例　“o=ABC Corporation-XXXX” （Printable）	加入者の会社名等＋企業内 RA コードを設定する。（英数字）	必須
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=XYZ Department” （Printable）	加入者の部署名等を設定する。（英数字）	オプション
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=FCxxxxxxxxxx”又は “ou=ECxxxxxxxxxx” （Printable）	証明書の固有番号を設定する。（英数字）	必須
cn（一般名） 「OID：2.5.4.3」 commonName	例“cn=xxxxxxxx” （Printable）	加入者のデバイス識別子を設定する。（英数字）	必須

表 3.2　ADFS デバイス証明書の加入者情報（subject）

属性	値	説明	備考
c（国名） 「OID：2.5.4.6」	“c=JP”で固定 （Printable）	日本を示す左記の国名を設定する。	－

countryName		（英語）	
o（組織名） 「OID：2.5.4.10」 organizationalName	例“o=ABC Corporation-XXXX” （Printable）	加入者の会社名等＋企業内 RA コードを設定する。（英数字）	必須
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=XYZ Department” （Printable）	加入者の部署名等を設定する。（英数字）	オプション
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=FCxxxxxxxxxx” 又は “ou=ECxxxxxxxxxx” （Printable）	証明書の固有番号を設定する。（英数字）	必須
cn（一般名） 「OID：2.5.4.3」 commonName	例“cn=xxxxxxxx” （Printable）	加入者のデバイス識別子を設定する。（英数字）	必須

表 3.3　クライアント証明書 for Sign の加入者情報（subject）

属性	値	説明	備考
c（国名） 「OID：2.5.4.6」 countryName	“c=JP”で固定 （Printable）	日本を示す左記の国名を設定する。（英語）	－
o（組織名） 「OID：2.5.4.10」 organizationalName	例“o=ABC Corporation-XXXX” （Printable）	加入者の会社名等＋企業内 RA コードを設定する。（英数字）	必須
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=XYZ Department” （Printable）	加入者の部署名等を設定する。（英数字）	オプション
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=xxxxxxxx” （Printable）	加入者の役職等を設定する。（英数字）	オプション
cn（一般名） 「OID：2.5.4.3」 commonName	例“cn=Taro Mitsubishi” （Printable）	加入者の固有名称、固有番号等を設定する。（英数字）	必須
uid（ユーザ ID） 「OID：0.9.2342.19200300.100.1.1」 userId	例“uid=FCxxxxxxxxxx” 又は “uid=ECxxxxxxxxxx” （Printable）	証明書の固有番号を設定する。（英数字）	必須
serialNumber（シリアル番号） 「OID：2.5.4.5」	例“serialNumber=xxxxxxxx” （Printable）	加入者の固有番号等を設定する。（数字）	オプション

表 3.4　クライアント証明書 for Auth の加入者情報（subject）

属性	値	説明	備考
c（国名） 「OID：2.5.4.6」 countryName	“c=JP”で固定 （Printable）	日本を示す左記の国名を設定する。（英語）	－
o（組織名） 「OID：2.5.4.10」 organizationalName	例“o=ABC Corporation-XXXX” （Printable）	加入者の会社名等＋企業内 RA コードを設定する。（英数字）	必須
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=XYZ Department” （Printable）	加入者の部署名等を設定する。（英数字）	オプション
ou（組織単位名） 「OID：2.5.4.11」 organizationalUnitname	例“ou=xxxxxxxx” （Printable）	加入者の役職等を設定する。（英数字）	オプション
cn（一般名） 「OID：2.5.4.3」 commonName	例“cn=Taro Mitsubishi” （Printable）	加入者の固有名称、固有番号等を設定する。（英数字）	必須
uid（ユーザ ID）	例“uid=FCxxxxxxxxxx” 又は	証明書の固有番号を	必須

「OID : 0.9.2342.19200300.100.1.1」 userId	“uid=ECxxxxxxxxxx” （Printable）	設定する。（英数字）	
serialNumber（シリアル番号） 「OID : 2.5.4.5」	例“serialNumber=xxxxxxxx” （Printable）	加入者の固有番号等を設定する。（数字）	オプション

表 3.5　Web サーバ用証明書の加入者情報（subject）

属性	値	説明	備考
c（国名） 「OID : 2.5.4.6」 countryName	例“c=JP” （Printable）	CSR に指定された countryName を設定する。（英語）	－
st（州名/都道府県名） 「OID : 2.5.4.8」 stateOrProvinceName	例“st=Tokyo” （Printable）	CSR に指定された stateOrProvinceName を設定する。（英語）	
l（地域名） 「OID : 2.5.4.7」 localityName	例“l=Minatoku-Shibaura” （Printable）	CSR に指定された localityName を設定する。（英語）	
street（街路名） 「OID : 2.5.4.9」 streetAdress	例“street=4-16-36” （Printable）	CSR に指定された streetAdress を設定する。（英語）	
o（組織名） 「OID : 2.5.4.10」 organizationalName	例“o=Mitsubishi Electric Information Network Corporation” （Printable）	CSR に指定された organizationName を設定する。（英語）	
ou（組織単位名） 「OID : 2.5.4.11」 organizationalUnitname	例“ou=xxxxx” （Printable）	CSR に指定された organizationUnitName を設定する。（英語）	
cn（一般名） 「OID : 2.5.4.3」 commonName	例“cn=xxxxx” （Printable）	CSR に指定された commonName を設定する。（英語）	

3.1.3　加入者の匿名性又は仮名性

本認証局が発行する加入者証明書には加入者の名称等が記載される場合がある。

3.1.4　種々の名称形式を解釈するための規則

本認証局が発行する加入者証明書に記載される名称は、ITU-T X.500 識別名（DN）の規定及び本 CPS「3.1.2 名称が意味を持つことの必要性」の規定に従うものとする。

3.1.5　名称の一意性

加入者証明書に記載される加入者情報（subject）の識別名（DN）は、本認証局が発行した加入者証明書において一意に割り当てる。

3.1.6　認識、認証及び商標の役割

商標使用の権利は、商標所持者が全ての権利を保有するものとする。本認証局は、必

要に応じて、商標所持者に対し、商標に関する出願などの公的書類の提出を求めることがある。

3.2　初回の本人性確認

3.2.1　私有鍵の所持を証明する方法

本認証局は、本認証局にて加入者鍵ペアを生成し、加入者証明書とともに媒体に格納して企業内 RA に送付、又は加入者鍵ペアと加入者証明書を証明書配付システムに登録し配付するため、加入者私有鍵の所持確認は行なわない。

3.2.2　組織の認証

本認証局に加入者証明書の申請を行う企業は、予め、企業内 RA 審査登録担当者（以下、「RA 担当者」と呼ぶ。）を指名し、当該組織の責任者より、「Enterprise PremiumCA 企業内審査登録局設置申込書」（以下、「企業内 RA 設置申込書」という）を提出することにより、その任命と本認証局への通知を行なう。なお、企業内 RA 設置申込書情報が変更となる場合は速やかには変更申込を本認証局に行ない、本サービスの契約を継続しない場合は廃止申込を本認証局に行うものとする。

（1）　電話による認証を行う場合

第三者データベースに記載されている代表電話番号へ連絡し、企業内 RA 設置申込書に記載された当該組織の責任者及び RA 担当者の在籍を確認し、RA 担当者の部門、住所、電話番号、メールアドレスを確認する。

※電話による確認が出来ない場合、「（2）書類による認証を行う場合」の確認が必要となります。

（2）　書類による認証を行う場合

企業内 RA 設置申込書と一緒に当該組織の印鑑証明書の提出が必要となる。企業内 RA 設置申込書に記載された組織名、押印された印を当該組織の印鑑証明書で確認する。また、企業内 RA 設置申込書に記載された電話番号へ連絡し、RA 担当者の部門、住所、電話番号、メールアドレスを確認する。

（3）　対面による認証を行う場合

対面及び名刺にて企業内 RA 設置申込書に記載された当該組織の責任者及び RA 担当者の在籍を確認し、RA 担当者の部門、住所、電話番号、メールアドレスを確認する。なお、対面による認証は弊社と事前に取引がある又は弊社が認めた場合のみ認めるものとする。

証明書発行要求がメールを利用した電子申請で行われる場合には、RA 担当者のメールアドレスにより、RA 担当者の本人確認を行ない、弊社指定のデータ交換サービスを利用した電子申請で行われる場合には、RA 担当者のデータ交換サービスの認証によっ

て本人確認を行う。

3.2.3 個人の認証

本認証局に加入者証明書を申請しようとする個人が加入者本人であることの真偽の確認は、RA 担当者が、以下に定める方法を参考に策定した企業内登録審査基準によって行う。

本認証局は、企業内 RA からの証明書発行要求データに基づき証明書を発行する。加入者の真偽確認は、一切行わない。

企業内 RA が実施する真偽確認の例を以下に示す。

＜加入者の真偽確認（例）＞

(1) 証明書申請書に記入されている加入者情報の真正性を確認する。加入者情報には、氏名・所属部署名・社員番号・現住所等がある。

(2) 加入者が法人代表者（企業関連会社等）である場合は、証明書申請書に記入されている加入者の氏名が、事前届出の会社法人などの代表者名と一致すること。加入者が法人代表者から契約等に関する権限を委任された者である場合は、証明書申請書に記入されている加入者が会社法人などに所属することを証明する書類（以下、「企業による申請者の在職を証明する書類」という。）に記載されている当該法人名が、事前届出の法人名と一致し、かつ証明書申請書に記入されている加入者の氏名が、「企業による申請者の在職を証明する書類」に記載されている在職者名と一致すること。

＜証明書申請を行った者に対する疑義（例）＞

(1) 上記「加入者の真偽確認」の検査において、証明書申請に係る書類の不備や記載内容に疑義を検出した場合、企業内 RA は証明書申請を行った者に対し、修正あるいは再提出を求める。

3.2.4 確認しない加入者の情報

規定しない。

3.2.5 機関の正当性確認

本 CPS「3.2.2 組織の認証」で規定された書類の確認を実施することにより、正当性確認を行う。

3.2.6 相互運用の基準

規定しない。

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

初回の証明書発行と同様の手順とする。

なお、企業内 RA との取り決めに則り、加入者証明書の有効期限切れが近づいた時期に、本認証局からその旨を通知する場合がある。

3.3.2 証明書失効後の鍵更新の本人性確認及び認証

初回の証明書発行と同様の手順とする。

3.4 失効申請時の本人性確認及び認証

失効申請を行う者が加入者の場合は、その真偽の確認を RA 担当者が、企業内審査基準に定める方法によって行う。

本認証局は、企業内 RA からの証明書失効要求データに基づき当該証明書を失効する。本認証局への証明書失効要求は、企業内 RA からのみ受け付け、加入者からの失効申請は受け付けない。但し、オンラインでのみ加入者からの失効申請を受け付ける場合がある。

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

証明書の申請者は証明書の利用を希望する個人又は企業（又は団体。総称として企業と呼ぶ）とする。証明書の利用を希望する個人又は企業は、本 CPS に、同意しなければならない。

4.1.2　申請手続及び責任

証明書の申請については、企業内 RA から下記のいずれかの方法によるものとする。

- 本認証局の窓口へ RA 担当者のメールアドレスを利用した電子申請
- 本認証局の窓口へ弊社指定のデータ交換サービスを利用した電子申請

上記以外の方法による証明書の申請は受け付けない。

また、本サービスは加入者から本認証局の窓口への証明書申請は受け付けない。

4.2　証明書申請手続き

4.2.1　本人性及び資格確認

加入者の本人性及び資格確認は、企業内 RA にて策定した企業内審査基準によって RA 担当者が行う。

本認証局は、加入者の真偽確認は、一切行わない。

4.2.2　証明書申請の承認又は却下

RA 担当者は、企業内 RA にて策定した企業内審査基準によって書類不備や本人性の確認等の審査過程において疑義が生じた場合には、証明書申請を不受理とする。

4.2.3　証明書申請手続き期間

規定しない。

4.3　証明書発行

4.3.1　証明書発行時の認証局の機能

1. 本認証局は、企業内 RA にて審査して認めた証明書発行要求データの情報を認証局システム（以下、「CA システム」という）に対し登録する。
2. 発行局は、認証設備室にて加入者鍵ペア、加入者証明書を生成し、生成した加

入者の私有鍵と加入者証明書を証明書格納媒体に格納、又は証明書配付システムに登録する。このとき生成された加入者の私有鍵は証明書格納媒体に格納、又は証明書配付システムに登録後速やかに、認証業務用設備から完全に削除される。

3. 発行局は発行した証明書格納媒体を所定の封筒に封緘し、RA 担当者宛に郵送する。証明書配付システムに登録した場合、又はメールによる配送の場合は郵送を行わない。

4.3.2 証明書発行後の通知

本認証局は、発行された証明書格納媒体を RA 担当者宛に郵送、又はメールすること、及び証明書配付システムに加入者の私有鍵と加入者証明書のペアを登録することにより、証明書を発行したことを通知したものとみなす。

4.4 証明書の受理

4.4.1 証明書の受理

本認証局は、証明書格納媒体を RA 担当者宛に郵送、又はメールした場合は、RA 担当者が受領したことをもって受理したものとみなし、証明書配付システムに登録した場合は、加入者により証明書がダウンロードされたことをもって受理したものとみなす。

ただし、企業内 RA との取り決めに則り、本認証局で受理確認を行う場合もある。

4.4.2 認証局による証明書の公開

本認証局は、加入者証明書の公開は行わない。

4.4.3 他のエンティティに対する認証局による証明書発行通知

本認証局は、他エンティティに対する証明書発行通知は行わない。

4.5 鍵ペアと証明書の利用目的

4.5.1 加入者の私有鍵と証明書の利用目的

加入者は、私有鍵を本 CPS「1.4.1 適切な証明書の使用」に規定する用途のみに使用できる。また、本認証局は、加入者証明書が用途以外の目的で使用された場合には、一切の責任を負わない。

4.5.2 検証者の公開鍵と証明書の利用目的

検証者は、加入者の認証又は加入者の電子署名を検証する用途で公開鍵と証明書を

利用する。

4.6　証明書更新

本 CPS に則り認証局から発行される証明書の更新は行わない。

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

本認証局が発行する加入者私有鍵は、自動的に更新されない。

加入者証明書の有効期間が切れると同時に、鍵も無効となる。但し、加入者証明書及び鍵の更新が必要な場合は、初回の証明書発行手順と同様に CA システムを使用して加入者証明書を発行することが出来る。

4.7.2　鍵更新申請者

本 CPS「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 CPS「4.2.1 本人性及び資格確認」に定める本人性確認並びに資格確認を行う。

4.7.4　加入者への新証明書発行通知

認証局は、本 CPS「4.3.2 証明書発行後の通知」に定める発行通知を行う。

4.7.5　鍵更新された証明書の受理

本 CPS「4.4.1 証明書の受理」に定める受理確認を行う。

4.7.6　認証局による鍵更新証明書の公開

本認証局は、加入者証明書の公開は行わない。

4.7.7　他のエンティティへの証明書発行通知

本認証局は、他エンティティに対する証明書発行通知は行わない。

4.8　証明書変更

本 CPS に則り認証局から発行される加入者証明書は、証明書変更を行わない。

4.9　証明書の失効と一時停止

4.9.1　証明書失効の要件

認証局は、次の場合に証明書を失効するものとする。

＜加入者による失効申請の場合＞

次の各項に該当する場合、加入者は所属する企業内 RA 経由で失効申請を行わなくてはならない。但し、オンラインでのみ加入者からの失効申請を受け付ける場合がある。

- 証明書格納媒体を紛失した場合
- 証明書格納媒体を破損した場合
- 証明書格納媒体の盗難を知った場合
- 証明書格納媒体の不正使用を知った場合
- 加入者私有鍵の不正な複製を知った場合
- 加入者私有鍵を削除した場合
- 加入者私有鍵の不正使用を知った場合
- 証明書格納媒体又は加入者私有鍵の PIN を紛失した場合
- 証明書格納媒体又は加入者私有鍵の PIN の漏洩を知った場合
- 証明書格納媒体又は加入者私有鍵の PIN の不正使用を知った場合
- 証明書格納媒体の PIN の入力ミスで証明書格納媒体が利用できなくなった場合
- 加入者私有鍵が危殆化又は、危殆化の恐れがある場合
- 加入者証明書の利用を停止する場合
- その他、加入者が加入者証明書を失効させる必要があると判断した場合

本認証局は、企業内 RA からの証明書失効要求を受けた場合は、理由の如何に関わらず証明書の失効を行う。

＜認証局による失効の場合＞

次の各項に該当する場合、加入者証明書を失効させる。

- 加入者が、本 CPS、又はその他の契約、規制、あるいは有効な証明書に適用される法に基づく義務を満たさなかった場合
- 加入者私有鍵の危殆化が認識されたか、その疑いがある場合
- 本 CPS に従って加入者証明書が適切に発行されなかったと認証局が判断した場合
- 加入者の特定ができない場合で、緊急に失効する必要があると認証局が判断した場

合

- 認証局の私有鍵が危殆化又は、危殆化の恐れがある場合
- 認証局のオペレーションミスにより証明書の記載事項に誤りがあった、もしくは証明書格納媒体の不具合により証明書が使用できない場合
- その他の事由により証明書の記載事項に誤りがあった場合
- 認証局が認証業務を廃止する場合

4.9.2 失効申請者

RA 担当者とする。但し、オンラインでのみ加入者とする場合がある。

4.9.3 失効申請の処理手順

失効申請手続きは、下記のとおりとする。

＜失効申請者からの失効申請の場合＞

1. 失効申請の受付け

本認証局は企業内 RA から下記のいずれかの方法による証明書失効要求を受け付ける。

- 本認証局の窓口へ RA 担当者のメールアドレスを利用した電子申請
- 本認証局の窓口へ弊社指定のデータ交換サービスを利用した電子申請

上記以外の方法による証明書失効要求は受け付けない。

但し、オンラインでのみ加入者からの失効申請を受け付ける場合がある。

2. 失効処理

本認証局は、上記「1. 失効申請の受付け」で受付けた証明書失効要求データの情報に基づき、発行局にて速やかに当該証明書を失効させる。また、当該証明書の失効を実施した後、CRL を発行する。

＜認証局による失効の場合＞

本認証局は「4.9.1 証明書失効の要件」の中の認証局からの失効の場合は、速やかに当該証明書を特定し、失効の事由の真偽の確認を実施する。また、失効事由が真実であった場合は速やかに証明書を失効させる。

証明書の失効を実施した場合は、CRL を発行する。

4.9.4 失効における猶予期間

「4.9.1 証明書失効の要件」に規定されている事由が発生した場合には、速やかに失効申請を行うものとする。

4.9.5　認証局による失効申請の処理期間

規定しない。

4.9.6　検証者の失効情報確認の要件

検証者は、被認証者又は署名者の公開鍵を使う時に有効な CRL を使用して失効の有無をチェックし、証明書状態の確認を行うものとする。

4.9.7　CRL 発行頻度

本認証局は、CRL の発行頻度を決定し、決定した頻度に従い CRL の更新を行う。本 CPS「4.9.7 CRL 発行頻度」で規定する頻度で CRL の更新が行えない場合は、加入者、検証者にリポジトリにより通知する。

1. CRL の有効期間を 2 ヶ月とし、日次で更新する。
2. 加入者証明書の失効を行った場合は、CRL を更新する。
3. 認証局私有鍵が危殆化し、又はその恐れがある場合は、直ちに発行した全ての証明書を失効させ、CRL を発行する。

4.9.8　CRL/ARL が公開されない最大期間

規定しない。

4.9.9　オンラインでの失効／ステータス情報の入手方法

規定しない。

4.9.10　オンラインでの失効確認要件

規定しない。

4.9.11　その他利用可能な失効情報確認手段

使用しない。

4.9.12　鍵の危殆化に関する特別な要件

認証局は、認証局私有鍵の危殆化の際には関連組織に直ちに通知するものとする。

4.9.13　証明書一時停止の要件

一時停止は行わない。

4.9.14　一時停止申請者

一時停止は行わない。

4.9.15　一時停止申請の処理手順

一時停止は行わない。

4.9.16　一時停止期間の制限

一時停止は行わない。

4.10　証明書ステータスの確認サービス

4.10.1　運用上の特徴

規定しない。

4.10.2　サービスの利用可能性

規定しない。

4.10.3　オプショナルな仕様

規定しない。

4.11　加入の終了

加入者が、証明書の利用を終了する場合、本 CPS「4.9 証明書の失効と一時停止」に規定する失効手続きを行うものとする。

4.12　私有鍵預託と鍵回復

規定しない。

4.12.1　預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

規定しない。

5　建物・関連設備、運用のセキュリティ管理

5.1　建物及び物理的管理

5.1.1　施設の位置と建物構造

本認証業務のための設備を維持・運用するための場所である認証設備室については、下記のセキュリティを確保する。

1. 認証設備室は、外部からの侵入が容易にできないようセキュリティが確保された建物の内部に、物理的な仕切りに囲まれた区画（「サイト」ともいう。）の施設とし、物理的な階層構造の中に設置する。
2. 認証設備室については、独自のセキュリティ基準を設けることにより、認証業務用設備が物理的に安全な環境において運用する。
3. 認証設備室及び認証設備室が設置された建物等には、その施設に認証業務用設備があることを示す掲示及びパンフレット等への記載を一切行わない。

5.1.2　物理的アクセス

認証設備室への入退室においては、下記のセキュリティを確保する。

1. 認証設備室への入室においては、入室を許可されない者の不正侵入を防止するため、入室を許可された運営要員の生体をあらかじめ生体認証装置に登録し、生体が登録された運営要員の生体認証が行なわれることにより、入室を可能とするとともに、生体認証装置により入室の記録が行われる。
2. 認証設備室への入室においては、入室操作の時間と入室操作の試行回数をチェックすることにより、許可されない者が室内に不正侵入できないようにする。また、そのチェックにより検知した異常については、24 時間監視を行っている監視室へ警告する。
3. 認証設備室の入室及び退室並びに認証設備室内での作業については、監視カメラにより、運営要員の活動を記録する。
4. 認証業務用設備の補修工事等に際し、入室権限を有する運営要員以外の者が認証設備室へ入室しなければならない場合は、認証業務責任者の事前の許可を得て、入室権限を有する作業監督者が同行し監督することにより、認証設備室への入室ができるものとする。

5.1.3　電源及び空調設備

認証業務用設備については、商用電源が断たれた場合に CA システムの異常停止又はサービスの中断を防止するために、設置された無停電源装置（UPS：Uninterruptible Power

Supply）及び自家発電装置からの給電を行う。また、認証設備室は、空調システムにより温度及び湿度の制御を行う。

5.1.4 水害及び地震対策

認証設備室は、建物の 2 階以上に設置され、洪水・津波等の水害から守り、漏水対策も施す。また、耐震対策を講じた建物に設置するとともに、認証設備室に設置される機器については、地震による移動及び転倒等を防止する措置を講じる。

5.1.5 防火設備

認証設備室は、建築基準法に適合した耐火建物の中に設置する。また、認証設備室は、建築基準法に適合した防火区画に設置し、自動火災報知器及び消火設備を設置する。

5.1.6 記録媒体

アーカイブデータ、バックアップデータを含む媒体は、施錠された安全な保管場所で管理する。

5.1.7 廃棄物の処理

機密扱いとする情報を含む書類・記録媒体の廃棄については、情報の漏洩がないよう、下記の方法で行う。

1. 紙等に記録された情報
   - 文書等については、シュレッダー等により、記載された内容を確認できないよう処理する。
2. 補助記録媒体等に記録されたデータ
   - 磁気テープ等については、無効データの上書き等を行なった上で完全消去する等により、記録されたデータを確認できないよう処理する。また、補助記録媒体の物理的な破壊により、記録されたデータを復元できないよう処理する。
3. コンピュータ機器等に記録されたデータ
   - コンピュータディスク、暗号化装置等については、完全な初期化を行うことにより、記録されたデータを確認できないよう処理する。また、本認証局の CA 私有鍵のバックアップが格納された記録媒体については、物理的な破壊により、記録されたデータを復元できないよう処理する。

5.1.8 施設外のバックアップ

規定しない。

5.2 手続的管理

5.2.1 信頼すべき役割

本認証業務に携わる運営要員とその業務は、表 5-1 に示す。

表 5-1 本認証局の運営要員の役割

運営要員の区分	業　　務
電子認証局代表者	① 認証局運営方針の決定および運営方針変更の決定 ② 認証局運営の監査指示 ③ CA 私有鍵の危殆化、災害などにおける対応に関する決定 など
電子認証局責任者	① 認証局運用規程（CPS）の策定、開示および変更管理 ② 認証局運用に係る要員の任命、解任および人事管理 ③ 鍵の危殆化や災害などの緊急時における対応の統括 など
監査者	① 監査体制（監査規程、監査基準、監査手順など）の整備 ② 監査計画の立案、監査の実施、監査報告 ③ 監査指摘事項に関する対応の確認 など
審査登録業務責任者	① 企業内 RA からの証明書発行要求及び証明書失効要求に係る書類等の確認結果の検認 ② 発行局への証明書発行要求および証明書失効要求 ③ 企業内 RA からの書類等の確認結果など三菱電機インフォメーションネットワーク内審査登録業務に関わる書類（アーカイブ）の保管 など
受付担当者	① 証明書発行要求申請および証明書失効要求に係る書類の受付けおよび確認 ② 加入者証明書の有効期限管理 など
認証業務責任者	① CA 私有鍵の生成および自己署名証明書の作成 ② CA 私有鍵のバックアップおよびバックアップからのリストア ③ 証明書の発行指示および失効指示 ④ 認証設備室の維持管理および認証設備室のセキュリティ監査イベント（アーカイブ）の採取および検査 ⑤ CA システムにおける鍵危殆化や災害発生など緊急時の対応 など
IA 操作員	① 証明書申請が許可された、企業内加入者情報の CA システムへの登録 ② CA 私有鍵のアクティベーションおよび非アクティベーション ③ CA システムの起動および停止 ④ 証明書の発行処理および失効処理、CRL の生成

運営要員の区分	業　　務
	⑤ CA システムのセキュリティ監査イベント（アーカイブ）の採取および検査 ⑥ CA システムの認証機能（セキュリティなどを含む）変更に関する設定変更 ⑦ 企業内の RA 担当者への加入者証明書の発行、および発送 など
システム保守員	① リポジトリの更新 ② CA システム、リポジトリのバックアップ ③ リポジトリのセキュリティ監査イベント（アーカイブ）の採取および検査 ④ CA システム、リポジトリの稼動状況監視 ⑤ CA システム、リポジトリのハードウェア保守点検、ソフトウェア機能強化 など

5.2.2　職務ごとに必要とされる人数

本認証業務に携わる運営要員の最低限必要な人数は、各運営要員 1 人とする。

5.2.3　個々の役割に対する本人性確認と認証

CA システムへのアクセスには、運用関係者に発行された電子証明書を使用した本人しか持ち得ない私有鍵を用いた強固な認証を行う。

5.2.4　職務分轄が必要になる役割

CA 私有鍵について、本 CPS「表 5-1 本認証局の運営要員の役割」に示す運営要員が実施する重要操作においては、適切な複数人による管理を採用する。

5.3　要員管理

信頼される役割を担う者は、認証局の業務に関して、操作や管理の責務を負う。認証局の運営においては、これら役割の信頼性、適合性及び合理的な職務執行能力を保証する人事管理がなされ、そのセキュリティを確立するものとする。

5.3.1　資格、経験及び身分証明の要件

認証局の業務運営に関して信頼される役割を担う者は、認証局運営組織の採用基準に基づき採用された職員とする。CA システムを直接操作する担当者は、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解しているものを配置する。

本認証局の業務の一部を外部委託する場合、又は本認証局の一部を外部のサービスを利用して実現する場合の、外部委託先の要員に関する要件は本書では規定しない。

5.3.2　研修要件

信頼される役割を担う者は、その業務を行うための適切な教育を定期的に受け、以降必要に応じて再教育を受けなければならない。

5.3.3　再研修の頻度及び要件

規定しない。

5.3.4　職務のローテーションの頻度及び要件

規定しない。

5.3.5　認められていない行動に対する制裁

認証業務に携わる者が､定められた権限を逸脱し認められていない行動を行った場合、その行為が故意か過失かに関わらず、定められた罰則が適用されるものとする。

5.3.6　独立した契約者の要件

規定しない。

5.3.7　要員へ提供する資料

認証業務に携わる者は、次の文書にアクセスすることができる。ただし、その文書については、認証業務に携わる者の役割に応じてアクセスできる者を定めるとともに、定められた者のみがアクセスできるよう制限された場所に保管されるものとする。

1. 本 CPS を含む認証局の運用に関する規程
2. 事務取扱要領などの手順書
3. 認証設備に関する仕様書および操作マニュアル
4. CA システムに関する仕様書および操作マニュアル

5.4　監査ログの取扱い

5.4.1　記録するイベントの種類

本認証局は、CA システム、リポジトリ及び認証設備室内のネットワーク機器に関する記録である監査イベントを監査ログとして記録する。監査ログには、下記のものが含まれる。また、イベントを起こした者への通知は行わない。

1. CA システムの起動・停止等の稼動ログ及び機能変更等の操作ログ
2. CA システムにおける加入者の登録、加入者証明書の発行要求及び失効要求並びに

加入者証明書の生成処理及び失効処理に関するログ

3. リポジトリにおける掲載情報の変更記録
4. ファイアウォール等の認証設備室内のネットワークログ
5. 認証設備室の入退室管理装置の動作ログ及び監視カメラの映像記録

5.4.2 監査ログを処理する頻度

認証局は、監査ログを必要に応じて適宜検査する。

5.4.3 監査ログを保存する期間

監査ログ（認証設備室の監視カメラの映像記録を除く）は、1 年間保存する。

5.4.4 監査ログの保護

認証局は、認可された人員のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを採用し、権限を持たない者の閲覧や、改ざん、不正な削除から保護する。

5.4.5 監査ログのバックアップ手続

監査ログは、月 1 回の頻度でバックアップする。

5.4.6 監査ログの収集システム（内部対外部）

規定しない。

5.4.7 イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8 脆弱性評価

規定しない。

5.5 記録の保管

5.5.1 アーカイブ記録の種類

本認証局は、認証業務に関わる以下の書類及び情報をアーカイブする。

- 本認証局から発行する証明書の発行/失効に関する処理履歴
- CRL の発行に関する処理履歴
- CA 証明書

- 加入者証明書
- 証明書発行要求に関わる書類
- 証明書失効要求に関わる書類
- CA 証明書の発行、更新及び失効に関わる書類

5.5.2 アーカイブを保存する期間

アーカイブする情報は、記録が作成されてから最低 10 年間は保存する。

5.5.3 アーカイブの保護

アーカイブ情報の収められた媒体は物理的セキュリティによって保護され、許可された者しかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護する。また、自然災害、火災及び盗難などから保護された場所に保存する。

5.5.4 アーカイブのバックアップ手続

アーカイブは、月 1 回の頻度でバックアップを実施する。

5.5.5 記録にタイムスタンプをつける要件

本 CPS「5.5.1 アーカイブ記録の種類」で規定する情報の記録時間は、処理を行った日付を記録する。

5.5.6 アーカイブ収集システム（内部対外部）

アーカイブの収集機能は、本認証局の CA システム及びリポジトリの機能とし、業務及びセキュリティに関する重要な事象をアーカイブとして収集する。

5.5.7 アーカイブ情報を入手し、検証する手続

本 CPS「5.5.1 アーカイブ記録の種類」で規定する情報については、本 CPS「5.5.3 アーカイブの保護」で規定する方法により、可用性と完全性が確保された形で安全に保管される。

5.6 鍵の切り替え

鍵が自動的に更新されることはない。証明書の有効期限が切れると同時に、鍵も無効となる。加入者は、証明書および鍵の更新が必要な場合は、再度、企業内 RA に証明書申請を行わなければならない。

5.7　危殆化及び災害からの復旧

5.7.1　災害及び CA 私有鍵危殆化からの復旧手続き

認証局は、想定される以下の脅威に対する復旧手順を規定し、関係する認証局運営要員全員に適切な教育・訓練を実施する。

- CA 私有鍵の危殆化
- 火災、地震、事故等の自然災害
- システム（ハードウェア、ネットワーク等）の故障

5.7.2　コンピュータのハードウェア、ソフトウェア、データが破損した場合の対処

ハードウェア、ソフトウェア、データが破壊又は損傷した場合、バックアップ用のハードウェア（保守)、ソフトウェア、バックアップデータを用いて、速やかに復旧作業を行い、合理的期間内に認証局業務を再開する。また、障害発生時の際には、可能な限り速やかに、加入者、検証者にリポジトリにより通知する。

5.7.3　CA 私有鍵が危殆化した場合の対処

CA 私有鍵が危殆化又その恐れが生じた場合は、認証局責任者の判断により、速やかに認証業務を停止するとともに、認証局で規定された手続きに基づき、全ての加入者証明書の失効を行い、CRL を開示し、CA 私有鍵を廃棄する。更に、原因の追求と再発防止策を講じる。

5.7.4　災害等発生後の事業継続性

災害などにより、認証施設及び設備が被災し、通常の業務継続が困難な場合には、認証局で規定された手続きに基づき、加入者及び検証者に情報を公開する。

5.8　認証局又は登録局の終了

1. 本サービスの廃止日までに有効期間の残っている全ての加入者証明書を失効し、その失効リストはリポジトリに 3 ヶ月公開する。
2. 本サービスを廃止する場合、廃止日の 90 日前までに企業内 RA に通知するとともに、リポジトリに廃止理由を公開する。

6　技術的なセキュリティ管理

6.1　鍵ペアの生成と実装

6.1.1　鍵ペアの生成

本認証局の鍵ペアは、認証設備室内で、複数人の立会いのもと、権限を持った者による操作により生成される。

加入者の鍵ペアは、厳重な管理のもと認証設備室で生成され、証明書格納媒体に格納、又は証明書配付システムに登録する。証明書格納媒体に格納後、又は証明書配付システムに登録後加入者の鍵ペアは、本認証局内の設備より削除する。

6.1.2　加入者への私有鍵の送付

加入者の私有鍵は認証局で生成されるため、郵便、メール又は証明書配付システムによって、加入者に引き渡されるものとする。

6.1.3　認証局への公開鍵の送付

加入者の公開鍵は本認証局で生成するため、加入者から本認証局へ配送されない。

6.1.4　検証者への CA 公開鍵の配付

CA 公開鍵は、検証者によるダウンロードを可能とするために、本認証局のリポジトリにて公開するものとする。

6.1.5　鍵のサイズ

本認証局で生成する鍵のサイズは、下記のとおりとする。

1. 本認証局の鍵のサイズは、RSA アルゴリズムの 2048 ビット
2. 加入者証明書の鍵のサイズは、RSA アルゴリズムの 2048 ビット。

6.1.6　公開鍵のパラメータ生成及び品質検査

公開鍵パラメータは、信頼できる暗号モジュールによって生成される。公開鍵パラメータの品質検査も暗号モジュールにより行うものとする。

6.1.7　鍵の利用目的

加入者証明書の鍵の利用目的は証明書の種類に応じてデバイス認証、電子署名、クライアント認証、ネットワーク機器用サーバ認証及び Web サーバ認証とする。証明書の種類とその鍵の利用目的の対応は下記のとおりとする。

（1）　「デバイス証明書」、「ADFS デバイス証明書」の keyUsage は、digitalSignature

及び keyEncipherment のビットを使用し、extendKeyUsage には clientAuth、smartCardLogon を使用するを使用する

(2) 「クライアント証明書 for Sign」の keyUsage は、digitalSignature 、nonRepudiation、keyEncipherment 及び dataEncipherment のビットを使用する

(3) 「クライアント証明書 for Auth」の keyUsage は、digitalSignature 及び keyEncipherment のビットを使用する

(4) 「ネットワーク機器用サーバ証明書」の keyUsage は digitalSignature 、nonRepudiation、keyEncipherment 及び dataEncipherment のビットを使用し、extendKeyUsage には serverAuth、clientAuth を使用する

(5) 「Web サーバ用証明書」の keyUsage は、digitalSignature 、keyEncipherment 及び dataEncipherment のビットを使用し、extendKeyUsage には serverAuth、clientAuth を使用する

6.2 私有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

CA 私有鍵の格納モジュールは、US FIPS 140-2 レベル 3 相当の暗号化装置によって生成、保存等の管理を行う。

6.2.2 私有鍵の複数人による管理

本認証局の CA 私有鍵の生成及び管理は、本認証局の鍵の管理を担う複数人の運営要員よって行われる。

6.2.3 私有鍵のエスクロー

本認証局は、CA 私有鍵及び加入者私有鍵のエスクローを行わない。

6.2.4 私有鍵のバックアップ

本認証局の CA 私有鍵は、本認証局の鍵の管理を担う複数人の運営要員よって行われ、かつ、そのうちの 1 名だけではできない方法によって認証設備室内でバックアップされ、複数に分割されたバックアップ用の鍵として保管する。バックアップ用の鍵の個々については、一つずつ権限を有する者以外が触れることができないアクセス制御などの措置がされ、耐火等の防災措置がとられた異なる場所に施錠して保管する。

6.2.5 私有鍵のアーカイブ

認証局は CA 私有鍵をアーカイブしない。

6.2.6　暗号モジュールへの私有鍵の格納と取り出し

本認証局の CA 私有鍵をバックアップ用の鍵からリストア（復元）する場合は、本認証局の鍵の管理を担う複数の運営要員によって認証設備室にて行う。

6.2.7　暗号モジュールへの私有鍵の格納

CA 私有鍵は、FIPS 140-2 レベル 3 相当の暗号化装置によって生成し、暗号化して暗号化装置内に保存する。

6.2.8　私有鍵の活性化方法

CA 私有鍵の活性化の方法は、認証局室内において本 CPS「6.2.2 私有鍵の複数人による管理」と同じく、複数名の権限を有する者を必要とする。

6.2.9　私有鍵の非活性化方法

CA 私有鍵の非活性化の方法は、認証局室内において本 CPS「6.2.2 私有鍵の複数人による管理」と同じく、複数名の権限を有する者を必要とする。

6.2.10　私有鍵の廃棄方法

CA 私有鍵を破棄しなければならない状況の場合、認証局室内で本 CPS「6.2.2　私有鍵の複数人による管理」と同じく、複数名の権限を有する者によって、私有鍵の格納された HSM を完全に初期化、又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続きによって破棄する。

6.2.11　暗号モジュールの評価

CA 私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 3 相当のものを使用する。

6.3　鍵ペア管理に関するその他の面

6.3.1　公開鍵のアーカイブ

本 CPS「5.5.2　アーカイブを保存する期間」及び「5.5.3　アーカイブの保護」で規定するとおり行う。

6.3.2　加入者証明書の有効期間と鍵ペアの使用期間

私有鍵と公開鍵の有効期間については、表 6-1 に示す。

表 6-1 鍵の有効期間

加入者	私有鍵有効期間	公開鍵有効期間

デバイス証明書	60 日,3 年,5 年	60 日,3 年,5 年
ADFS デバイス証明書	60 日,1 年,5 年	60 日, 1 年,5 年
クライアント証明書 for Sign	60 日,1 年,2 年,3 年,5 年	60 日,1 年,2 年,3 年,5 年
クライアント証明書 for Auth	60 日,1 年,2 年,3 年,5 年	60 日,1 年,2 年,3 年,5 年
ネットワーク機器用サーバ 証明書	60 日,1 年,2 年,3 年,5 年	60 日,1 年,2 年,3 年,5 年
Web サーバ用証明書	60 日,1 年,2 年,3 年,5 年	60 日,1 年,2 年,3 年,5 年

本認証局は証明書発行要求に指定された発行日の 0 時 0 分 0 秒を有効期間の開始日時に設定する。有効期間 60 日の場合は有効期間終了日時を開始日時から起算して 60 日後の 23 時 59 分 59 秒とする。有効期間 60 日以外は有効期間終了日時を開始日時から起算して各有効期間後の同月末日の 23 時 59 分 59 秒とする。

6.4 活性化用データ

6.4.1 活性化データの生成とインストール

認証局において用いられる CA 私有鍵の活性化データは一意で予測不能なものとし、その生成とインストールは定められた規則に従い実施する。

加入者私有鍵の活性化データ（PIN）は認証局側で生成し、本認証局が加入者私有鍵又は証明書格納媒体に設定する。

本認証局は加入者私有鍵の活性化データ（PIN）を郵送、E-mail などで加入者に通知する。

6.4.2 活性化データの保護

認証局において用いられる CA 私有鍵の活性化データは、権限者の責任で厳重に管理、保護される。

6.4.3 活性化データのその他の要件

規定しない。

6.5 コンピュータのセキュリティ管理

6.5.1 特定のコンピュータのセキュリティに関する技術的要件

認証業務用設備は、ファイアウォールを介して外部ネットワークと接続し、不正アク

セスを検知・防止する。本認証業務で用いる暗号化装置は、FIPS140-2 レベル 3 相当の暗号化装置を用いる。

CA システムへのログイン時には、本 CPS「5.2.3　個々の役割に対する本人性確認と認証」で定めるユーザの認証を必須とする。

6.5.2　コンピュータセキュリティ評価

本認証局で使用する製品については、セキュリティに関する情報等を定期的に収集し、最新のセキュリティ技術の最新動向を踏まえて、使用する製品が設けたセキュリティに関する基準を満たすよう維持管理する。

6.6　ライフサイクルの技術的管理

認証局 のハードウェア及びソフトウェアは、適切なサイクルで最新のセキュリティテクノロジを導入すべく、随時本 CPS の見直し及びセキュリティチェックを行う。

6.6.1　システム開発管理

本認証局のシステムは、適切な品質管理が行われた信頼できる組織で開発されたものを使用する。

本認証局のシステムについては、電磁的記録で保存される記録の内容が表示できるように、当該システムの機器、OS 及びアプリケーションを維持する。

本認証局のシステムに係る機器、OS 及びアプリケーションを更新する場合は、更新前に試験等を行い、互換性を確保する。

6.6.2　セキュリティ運用管理

本認証局のシステムについては、別に定めるセキュリティに関する規程（以下「セキュリティ規程」という。）の定めに従い、適切な運用を行う。

6.6.3　ライフサイクルのセキュリティ管理

規定しない。

6.7　ネットワークのセキュリティ管理

本認証局のネットワークについては、セキュリティ規程の定めに従い、適切な運用を行う。また、定期的な評価を実施し、ネットワーク運用がセキュリティ規程を満たすよう、下記の措置を行い、維持する。

1.　認証業務用設備を構成するネットワーク及びリポジトリを構成するネットワーク

に対する不正アクセスを防止するためのファイアウォールによる制御及び監視。また、リポジトリを構成するネットワークに対する不正アクセスを検知するための不正侵入検知システムによる監視

2. 証業務用設備を構成するネットワーク上の通信データの漏洩及び盗聴防止のための暗号化

6.8 タイムスタンプ

本認証局は、正確な時刻源を取得し、NTP（Network Time Protocol）を使用し認証業務用設備の時刻同期を行う。

7　証明書及び失効リスト及び OCSP のプロファイル

7.1　証明書のプロファイル

本認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成され、また証明書は X.500 識別名（Distinguished Name、以下 DN という）により一意に識別されるものとする。

本 CPS に従い発行される CA 証明書のプロファイルは、基本領域のプロファイルを別紙 1.表 A-1 に示し、拡張領域のプロファイルを別紙 1.表 A-2 に示すとおりとする。また、加入者証明書のプロファイルは、それぞれ下記のとおりとする。

（1）　デバイス証明書：基本領域のプロファイルを別紙 1.表 A-3 に示し、拡張領域のプロファイルを別紙 1.表 A-4 に示すとおりとする

（2）　ADFS デバイス証明書：基本領域のプロファイルを別紙 1.表 A-5 に示し、拡張領域のプロファイルを別紙 1.表 A-6 に示すとおりとする

（3）　クライアント証明書 for Sign：基本領域のプロファイルを別紙 1.表 A-7 に示し、拡張領域のプロファイルを別紙 1.表 A-8 に示すとおりとする

（4）　クライアント証明書 for Auth：基本領域のプロファイルを別紙 1.表 A-9 に示し、拡張領域のプロファイルを別紙 1.表 A-10 に示すとおりとする

（5）　ネットワーク機器用サーバ証明書：基本領域のプロファイルを別紙 1.表 A-11 に示し、拡張領域のプロファイルを別紙 1.表 A-12 に示すとおりとする

（6）　Web サーバ用証明書：基本領域のプロファイルを別紙 1.表 A-13 に示し、拡張領域のプロファイルを別紙 1.表 A-14 に示すとおりとする

7.1.1　バージョン番号

本認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成されることとする。

7.1.2　証明書の拡張

本認証局が発行する CA 証明書の拡張領域のプロファイル及び加入者証明書の拡張領域のプロファイルは本 CPS「7.1　証明書のプロファイル」に規定する。

7.1.3　アルゴリズムオブジェクト識別子

基本領域の Signature アルゴリズムは以下のとおりとする。

sha256WithRSAEncryption (1.2.840.113549.1.1.11)

基本領域のsubjectPublicKeyInfoアルゴリズムは以下のとおりとする。

rsaEncryption (1.2.840.113549.1.1.1)

7.1.4　名称の形式

Issure と Subject の名前の形式は別紙 1.表 A-1 に示される。

7.1.5　名称制約

本認証局では、名前制約の設定を行わない。

7.1.6　CP オブジェクト識別子

使用しない。

7.1.7　ポリシ制約拡張

使用しない。

7.1.8　ポリシ修飾子の構文及び意味

規定しない。

7.1.9　証明書ポリシ拡張フィールドの扱い

規定しない。

7.2　証明書失効リストのプロファイル

7.2.1　バージョン番号

認証局が発行する CRL/ARL は、X.509CRL フォーマット形式のバージョン 2 に従うものとする。

7.2.2　CRL と CRL エントリ拡張領域

CRLエントリの基本領域のプロファイル及び拡張領域のプロファイルは別紙2.表B-1のとおりとする。

7.3　OCSP プロファイル

7.3.1　バージョン番号

規定しない。

7.3.2　OCSP 拡張領域

規定しない。

8　準拠性監査とその他の評価

8.1　監査頻度

自己監査は、1 年に一度の定期監査として実施する。

セキュリティに関する重要な変更などについては、都度、自己監査を実施する。

8.2　監査者の身元・資格

監査人は、本認証局運営部門の要員以外から、電子認認証局代表者の指示に基づいて、選定される。

8.3　監査者と被監査者の関係

監査人は、被監査部門である認証局運用部門外から選定する。

8.4　監査テーマ

1. 本認証局、は、自己監査を実施するために監査規程と手順を定め、監査計画として監査目的、監査組織、スケジュール、監査対象、作業要領を明確にする。
2. 監査では、本認証業務が本 CPS などの基準・手順に則って実施されていること、ならびに不正行為などの脅威に対する措置が有効に機能していることを検証する。

8.5　監査指摘事項への対応

本認証局は、監査結果である監査報告書で指摘された事項に関して、速やかに改善の措置を行う。

8.6　監査結果の通知

監査結果は、監査報告書にて監査人から電子認証局代表者へ行われる。電子認証局代表者は、監査結果を、その監査結果に係る証明書の有効期間満了後 10 年間保存する。

9　その他の業務上及び法務上の事項

9.1　料金

本サービスに係る料金は、別途規定する。

1. 加入者は、加入者証明書の発行手数料として、別途定める金額を所定の方法で指定する期日までに本認証局に支払うものとする。
2. 指定する期日までに支払いがない場合、本認証局は加入者への事前通知なしに、発行済の加入者証明書を失効させることができるものとする。

9.2　財務上の責任

9.2.1　保険の適用範囲

1. 本認証局は、本 CPS「9.6.1 認証局の表明保証」に規定する責任及び義務に違反したことにより、加入者及び検証者に損害を与えた場合には、その損害の賠償責任を負うものとする。ただし、本認証局の責に帰すことができない事由から生じた損害及び逸失利益については、賠償責任を負わないものとする。

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に対する保険又は保証

エンドエンティティに対する保証は、下記のとおりとする。

1. 加入者は、加入者が本 CPS で定める範囲以外の用途に加入者証明書を使用した結果生じたトラブルについては、一切の責任を負うものとする。当該トラブルにより、本認証局及び検証者に損害を与えた場合には、本認証局及び検証者に対し、加入者の責任において損害賠償を行うものとする。
2. 加入者は、加入者が本 CPS で定める失効申請を怠った結果生じたトラブルについては、一切の責任を負うものとする。当該トラブルにより本認証局及び検証者に損害を与えた場合には、本認証局及び検証者に対し、加入者の責任において損害賠償を行うものとする。

9.3　企業情報の秘密保護

9.3.1　秘密情報の範囲

本認証局が保有する情報のうち、加入者証明書、CRL、本 CPS 等の公開文書を除いた情報が、秘密情報の対象として扱われる。

9.3.2　秘密情報の範囲外の情報

本認証局は、以下の情報を秘密情報として扱わない。

- 加入者証明書、又は CRL に含まれる情報
- 本 CPS 及びその他本認証局の公開文書
- リポジトリで公開される情報
- 本認証局以外の出所から、秘密保持の制限無しに公知となった情報

9.3.3　秘密情報を保護する責任

本認証局は「9.3.1　秘密情報の範囲」で規定された秘密情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。

ただし、本認証局が保持する秘密情報を、法の定めによる場合及び加入者による事前の承諾を得た場合に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。にもかかわらず、そのような情報が漏洩した場合、その責は漏洩した者が負う。

9.4　個人情報の保護

9.4.1　プライバシープラン

本認証局において提供するサービスの円滑な運営に必要な範囲で、本認証局の加入者の情報を収集する場合がある。収集した情報は利用目的の範囲内で適切に取り扱う。本認証局では、加入者の情報を本認証局が提供する認証業務のサービスを円滑に運営するために、加入者の組織確認、及び加入者証明書の送付先として利用する。

また、本認証局では、収集した情報について、法令に基づく開示請求があった場合、その他特別な理由のある場合を除き、利用目的以外の目的のために自ら利用、又は第三者に提供しない。更に、本認証局は、収集した情報の漏えい、滅失又はき損の防止その他収集した情報の適切な管理のために必要な措置を講じる。

9.4.2　プライバシーとして保護される情報

認証局は、次の情報を保護すべき個人情報として取り扱う。

- 登録局が本人確認や各種審査の目的で収集した情報の中で、証明書に含まれない情報。

  例えば、身分証明書、自宅住所、連絡先の詳細など、他の情報と容易に照合することができ、それにより特定の個人を識別することが可能な情報を指す。
- CRL に含まれない加入者の証明書失効又は停止の理由に関する情報。

・ その他、認証局が業務遂行上知り得た加入者の個人情報。

9.4.3 プライバシーとはみなされない情報

次の情報は、秘密情報として扱わない。

・ 加入者証明書
・ CRL に記載された情報

9.4.4 個人情報を保護する責任

認証局は「9.4.2 プライバシーとして保護される情報」で規定された情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。

9.4.5 個人情報の使用に関する個人への通知及び同意

認証局は、証明書発行業務及びその他の認証業務の利用目的に限り個人情報を利用する。それ以外の目的で個人情報を利用する場合は、法令で除外されている場合を除き、あらかじめ本人の同意を得るものとする。

9.4.6 司法手続又は行政手続に基づく公開

司法機関、行政機関又はその委託を受けたものの決定、命令、勧告等があった場合は、認証局は情報を開示することができる。

9.4.7 その他の情報開示条件

個人情報を提供した本人又はその代理人から当該本人に関する情報の開示を求められた場合、認証局で別途定める手続きに従って情報を開示する。この場合、複製にかかる実費、通信費用等については、情報開示を求める者の負担とする。

9.5 知的財産権

下記の情報及びデータについての著作権その他知的財産権等の全ての権利は、本認証局に帰属するものとする。

・ 本認証局より発行された加入者証明書
・ 本認証局より公開された CRL
・ 本 CPS

9.6　表明保証

9.6.1　認証局の表明保証

本認証局は、下記の責任及び義務を負う。

1. 提供するサービスと運用のすべてが、本 CPS の要件に従い行う。
2. 加入者証明書の発行時に、申請情報が正当な企業内 RA からであることの確認を確実に行う。
3. 公開鍵を含む加入者証明書を企業内 RA（オンラインの場合のみ加入者）に確実に届ける。
4. 本認証局で定める失効ポリシに従って失効事由が生じた場合は、加入者証明書を確実に失効する。
5. CRL などの重要事項を認証局の定める方法により、速やかに入手できるようにする。
6. 認証局の定める方法で、本 CPS に基づく企業内 RA の権利と義務を各企業内 RA に通知する。
7. CA 私有鍵の危殆化のおそれ、サービスの取り消し、及び紛争解決をするための手続きを企業内 RA に通知する。
8. 本 CPS「5　建物及び関連施設、運用のセキュリティ」及び「6　技術的セキュリティ管理」に従い本認証局を運営し、CA 私有鍵の危殆化を生じさせない。
9. CA 私有鍵が、加入者証明書及び証明書失効リストに署名するためだけに使用されることを保証する。
10. 企業内 RA から提出された加入者証明書発行等に関わる各種の書類の滅失、改ざんを防止し、本認証局が定める期間保管する。
11. 加入者が使用する電子署名アルゴリズムとして、法令で定めるアルゴリズムのうち、公開鍵暗号方式については、鍵長 2,048 ビットの RSA 方式を、ハッシュ関数については、SHA-256 方式を指定し、電子署名アルゴリズムは、本認証局が指定するものを使用する。

9.6.2　企業内 RA の表明保証

企業内 RA は、下記の責任及び義務を負う。

1. 企業内 RA の業務と運用のすべてが、本 CPS の要件及び企業内 RA で策定した企業内審査基準に従い行う。
2. 加入者からの証明書申請及び失効申請に際して、加入者の申請内容の真偽の確認を確実に行う。

3. 認証局への証明書発行要求及び証明書失効要求に際して、正確な加入者の申請内容を認証局に提出する。
4. 公開鍵を含む加入者証明書を加入者に確実に届ける。
5. 企業内 RA の定める方法で、本 CPS に基づく加入者の権利と義務を各加入者に通知する。
6. 加入者から提出された加入者証明書申請等に関わる各種の書類の滅失、改ざんを防止し、企業内 RA が定める期間保管する。
7. リポジトリを随時閲覧し、本サービスに関する情報を適宜取得する。

9.6.3 加入者の表明保証

加入者は、下記の責任及び義務を負う。

1. 加入者証明書の利用に際して、本 CPS に同意し遵守するとともに、本 CPS「1.4.1 適切な証明書の使用」に規定する用途のみに利用する。
2. 加入者証明書の申請に際して、正確な申込み内容を証明書申請書等に記載し、企業内 RA に提出する。
3. 本サービスによって発行された加入者証明書に対応する私有鍵と証明書格納媒体の PIN を、十分に注意して管理し、秘匿し続ける。
4. 証明書格納媒体の PIN を紛失等した場合には、加入者証明書の失効申請手続を行った後、加入者証明書の証明書申請手続を行わなければならない。
5. 証明書格納媒体受領時に加入者証明書の記載事項及び有効性等を確認し、記載事項に誤りがあった場合には、直ちに、企業内 RA 経由で本認証局へ報告する。
6. 加入者が加入者証明書の利用を中止する場合は、直ちに、企業内 RA 経由で本認証局に加入者証明書の失効申請を行う。
7. 本 CPS「4.9.1 証明書の失効事由」に該当する事由が生じた場合は、直ちに、企業内 RA 経由で本認証局に加入者証明書の失効申請を行う。
8. 本認証局は、加入者が使用する電子署名アルゴリズムとして、法令で定めるアルゴリズムのうち、公開鍵暗号方式については、鍵長 2,048 ビットの RSA 方式を、ハッシュ関数については、SHA-256 方式を指定する。加入者は、本認証局が指定する電子署名アルゴリズムを使用する。
9. リポジトリを随時閲覧し、本サービスに関する情報を適宜取得する。

9.6.4 検証者の表明保証

検証者は、下記の責任及び義務を負う。

1. 加入者証明書の検証に際して、本 CPS に同意し遵守するとともに、本 CPS「1.4.1

適切な証明書の使用」に規定する範囲のみに利用する。

2. 加入者証明書の利用にあたり、加入者証明書の検証を行なわなければならない。即ち、本認証局の CA 証明書により加入者証明書を署名検証することにより、当該加入者証明書が本認証局の CA 私有鍵により電子署名されていることを検証する。本認証局の CA 証明書のフィンガープリント（CA 証明書の値を SHA-1 又は SHA-256 でハッシュ変換した値）と、リポジトリに公開しているフィンガープリントとを比較検証することにより、当該 CA 証明書が本認証局の発行したものであることを確認する。
3. 加入者証明書を利用するにあたり、その加入者証明書が有効期間内であること及び失効されていないかどうかを本認証局がリポジトリで公開する CRL で確認する。
4. 加入者証明書を利用するにあたり、本認証局がリポジトリで公開する本サービスに関する情報を確認する。

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

本認証局は、本 CPS「9.6.1　認証局の表明保証」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、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。

また、本 CPS「9.16.5　不可抗力」で規定される不可抗力によるサービス停止によって加入者、若しくはその他の第三者において損害が生じた場合、或いは「9.17 その他の条項」の規程により本契約を解除した場合に加入者、或いは企業内 RA に損害が生じても、本認証局は一切の責任を負わない。

9.8 責任制限

本 CPS に規定された責任を果たさなかったことに起因して、本認証局が本サービスの加入者に対して損害を与えた場合、証明書発行手数料を上限として、損害を賠償する。ただし、本認証局側の責に帰さない事由から発生した損害、逸失利益、間接損害、又は予見の有無を問わず特別損害については、いかなる場合でも一切の責任を負わない。

また、加入者は認証局が発行する加入者証明書を申請した時点で、検証者は信頼した時点で、認証局及び関連する組織等に対する損害賠償責任が発生する。

9.9　補償

本認証局は、加入者及び検証者において加入者証明書の利用又は私有鍵の管理その他加入者が注意すべき事項の運用が不適切であったために生じた損害に対して、責任を負わない。

9.10　本ポリシの有効期間と終了

9.10.1　有効期間

本 CPS は、作成された後、本認証局が承認することによって有効となり、また、本 CPS「9.10.2　終了」に規定する本 CPS の終了まで有効とする。

9.10.2　終了

本 CPS は、「9.10.3 終了の影響と存続条項」で規定する存続条項を除き、本認証局が無効と宣言した時点、又は本認証局が本認証業務を終了した時点で無効となる。

9.10.3　終了の影響と存続条項

本認証局が終了した場合であっても、本 CPS「9.3　企業情報の秘密保護」、「9.4　個人情報の保護」、「9.5　知的財産権」、「9.8　責任制限」、「9.9　補償」、「9.10.3　終了の影響と存続条項」、「9.13　紛争解決手続」、「9.14　準拠法」及び「9.15　適用法の遵守」の各規定については、なお、効力を有する。

9.11　関係者間の個々の通知と連絡

関係者間の個別通知と報告は、下記のとおりとする。

1. 本認証局は、本認証局から加入者及び検証者への通知方法として、電子メール、郵便及びホームページへの掲示等、本認証局が適当と判断した方法により行う。
2. 電子メールによる通知においては、当該電子メールを本認証局が送信し、送信できたことが確認できた時に通知したものとみなす。
3. 郵便による通知においては、当該郵便の消印日をもって通知したものとみなす。
4. ホームページへの掲示による通知においては、当該ホームページの掲示を本認証局が行い、閲覧できることが確認できた時に通知したものとみなす。

9.12　改訂

9.12.1　改訂手続き

本認証局は、本 CPS 及び別に定める諸規程の仕様を変更することができる。また、本認証局は、加入者及び検証者に事前の了解を得ることなく、本 CPS に定めた仕様の変更をすることができる。仕様変更の内容は、本認証局での審議を経て、電子認証局代表者が変更を承認する。

9.12.2　通知方法と期間

本認証局は、本 CPS に定めた仕様の変更に関する公開と通知を、下記のとおり行い、変更した本 CPS を公開後 15 日以内に、加入者が自己の加入者証明書の失効申請を行わない場合には、変更に同意したものとみなす。

- 仕様が変更された本 CPS については、変更後、速やかに、リポジトリにて公開することにより、加入者及び検証者へ通知されたものとする。
- 仕様が変更された本 CPS については、仕様が変更された抜粋ではなく、全てを公開する。
- 本 CPS の変更については、バージョン番号及び改訂日により識別する。
- 仕様が変更された本 CPS については、リポジトリによる加入者及び検証者への通知をもって、直ちに、有効とする。
- 加入者及び検証者は、本認証局のリポジトリを定期的に参照し、本 CPS の変更について同意するものとする。

9.12.3　オブジェクト識別子（OID）の変更理由

規定しない。

9.13　紛争解決手続

加入者又は検証者と本認証局又は三菱電機インフォメーションネットワーク株式会社との間に、訴訟又は法的行為が起こった場合は、東京地方裁判所を専属管轄裁判所とする。

9.14　準拠法

本 CPS は、日本国内法及び規則に基づき解釈されるものとする。

9.15　適用法の遵守

規定しない。

9.16 雑則

9.16.1 完全合意条項

本 CPS は、本 CPS で定められた事項に対して関係者間における完全合意を構成するものであり、本サービスについて本 CPS より早い時期及び同時期に定めれれた書面、口頭による意思表示、合意及び表明事項のすべてに優先する。

9.16.2 権利譲渡条項

規定しない。

9.16.3 分離条項

本 CPS のひとつ又は複数の条項が司法の判断により、無効であると解釈された場合であっても、その他の条項の有効性には影響を与えない。無効と判断された条項は、法令の範囲内で当事者の合理的な意思を反映した規定に読み替える。

9.16.4 強制執行条項（弁護士費用及び権利放棄）

規定しない。

9.16.5 不可抗力

本認証局は、以下に例示されるような通常人の標準的な注意義務を尽くしても、予防・回避できない事象を不可抗力とする。不可抗力によって損害が発生した場合、本 CPS「9.7 無保証」の規定により認証局は免責される。

- 加入者又は検証者が、加入者証明書を利用する際に発生したコンピュータシステム等のハードウェア又はソフトウェアへの障害
- 火災、雷、噴火、洪水、地震、嵐、台風、天変地異、自然災害、放射能汚染、有害物質による汚染、又は、その他の自然現象
- 暴動、市民暴動、悪意的損害、破壊行為、内乱、戦争（宣戦布告されているか否かを問わない）又は革命
- 裁判所、政府又は地方機関による作為又は不作為
- ストライキ、工場閉鎖、労働争議
- 電気通信事業者が電気通信サービスを中断又は停止した場合
- 認証局の責によらない事由で、本 CPS に基づく義務の遂行上必要とする必須の機器、物品、供給物若しくはサービス（電力、ネットワークその他の設備を含む

がそれに限らない）が利用不能となった場合

9.17　その他の条項

本認証局は、以下に定める事由が発生したときには、加入者、或いは契約企業へ通知または催告をすることなく、加入者、或いは契約企業との契約を解除できるものとする。

(1) 加入者が暴力団、暴力団員、暴力団関係者、その他反社会的勢力に準ずる者（以下、暴力団等という）である場合

(2) 加入者、或いは契約企業の代表者、責任者、又は実質的に経営権を有する者が暴力団等である場合、又は、暴力団等への資金提供を行う等、密接な交際のある場合

(3) 加入者、或いは契約企業が自ら又は第三者を利用して、他方当事者に対して、自身が暴力団等である旨を伝え、又は、関係者が暴力団である旨を伝えた場合

(4) 加入者、或いは契約企業が自ら又は第三者を利用して、他方当事者に対して、詐術、暴力的行為又は脅迫的言辞を用いた場合

(5) 加入者、或いは契約企業が自ら又は第三者を利用して、他方当事者の名誉や信用等を毀損し、又は、毀損するおそれのある行為をした場合

(6) 加入者、或いは契約企業が自ら又は第三者を利用して、他方当事者の業務を妨害した場合、又は、妨害するおそれのある行為をした場合

別紙 1. 証明書プロファイル

記号の意味：

○：使用

×：未使用

凡例

(1) (sha256WithRSAEncryption)及び(rsaEncryption)はそれぞれ、OID に対応づけられた暗号アルゴリズムを示している。

(2) (id-kp 1)及び(id-kp 2)は、それぞれ OID に対応づけられた利用目的を示している。

(3) （Printable）は、設定された文字列が、printable　string の文字コードでエンコードされていることを示す。

(4) （IA5） は、設定された文字列が、IA5　string の文字コードでエンコードされていることを示す。

(5) （UTF-8）は、設定された文字列が、UTF-8　string の文字コードでエンコードされていることを示す。

表 A-1 自己署名証明書プロファイル(基本部)

領域名	規定内容と設定値
基本部	
version	2(v3)
serialNumber	1（例）
signature	sha256WithRSAEncryption
validity	○
notBefore	有効期間は 30 年に設定（UTCTime で設定する）
notAfter	
issuer	c=JP（Printable）， o=Enterprise Premium Service（Printable）， cn=Enterprise Premium CA - G3（Printable）
subject	c=JP（Printable）， o=Enterprise Premium Service（Printable）， cn=Enterprise Premium CA - G3（Printable）
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値(2048bit)
issuerUniqueID	×
subjectUniqueID	×

表 A-2 自己署名証明書プロファイル(拡張部)

領域名	クリティカルフラグ	規定内容と設定値
標準拡張領域		
subjectKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
keyCertSign		1　（電子証明書の署名検証）
cRLSign		1　（証明書失効リストの署名検証）
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies		×
policyMappings		×
issuerAltName		×
subjectAltName		×
basicConstraints	TRUE	○
cA		True
pathLenConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints		×
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×
なし		×

表 A-3 デバイス証明書プロファイル(基本部)

領域名	規定内容と設定値
基本部	
version	2(v3)
serialNumber	1001（例）
signature	Sha256WithRSAEncryption
validity	○
notBefore	有効期間は 60 日,3 年,5 年に設定（UTCTime で設定する）
notAfter	
issuer	c=JP（Printable）, o=Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
subject	c=JP（Printable）, o= ABC Corporation(会社名等英語（オプション）,Printable）, ou= XYZ Department(部署名等英語（オプション）,Printable), ou =FCxxxxxxxxx（証明書固有番号英語（必須）,Printable） cn= xxxxxxxx (デバイス識別子英語（必須）,Printable）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値(2048bit)
issuerUniqueID	×
subjectUniqueID	×

表 A-4 デバイス証明書プロファイル(拡張部)

領域名	クリティカルフラグ	規定内容と設定値
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP（Printable）, o= Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		証明書公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		1　（電子署名）
keyEncipherment		1　（鍵の暗号化が可能）
extendedKeyUsage	FALSE	○
keyPurposeId		○
clientAuth		1.3.6.1.5.5.7.3.2
smartCardLogon		1.3.6.1.4.1.311.20.2.2
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		1.2.392.200127.9.2
policyQualifiers		1.3.6.1.5.5.7.2.1（id-qt-cps）
qualifier		http://www.eppcert.jp/(IA5)
policyMappings		×
issuerAltName		×
subjectAltName	FALSE	○
rfc822Name		(例)taro@dd.co.jp(IA5)
otherName		×
userPrincipalName		×
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		○
uniformResourceIdentifier		http://www.eppcert.jp/g3/rlist/epg3ca.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×
なし		×

表 A-5 ADFS デバイス証明書プロファイル(基本部)

領域名	規定内容と設定値
基本部	
version	2(v3)
serialNumber	1001（例）
signature	Sha256WithRSAEncryption
validity	○
notBefore	有効期間は 60 日,1 年,5 年に設定（UTCTime で設定する）
notAfter	
issuer	c=JP（Printable）, o=Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
subject	c=JP（Printable）, o= ABC Corporation(会社名等英語（オプション）,UTF-8）, ou= XYZ Department(部署名等英語（オプション）,UTF-8), ou =FCxxxxxxxxx（証明書固有番号英語（必須）,UTF-8） cn= xxxxxxxx (デバイス識別子英語（必須）,UTF-8）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値(2048bit)
issuerUniqueID	×
subjectUniqueID	×

表 A-6 ADFS デバイス証明書プロファイル(拡張部)

領域名	クリティカルフラグ	規定内容と設定値
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP（Printable）, o= Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		証明書公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		1　（電子署名）
keyEncipherment		1　（鍵の暗号化が可能）
extendedKeyUsage	FALSE	○
keyPurposeId		○
clientAuth		1.3.6.1.5.5.7.3.2
smartCardLogon		1.3.6.1.4.1.311.20.2.2
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		1.2.392.200127.9.2
policyQualifiers		1.3.6.1.5.5.7.2.1（id-qt-cps）
qualifier		http://www.eppcert.jp/(IA5)
policyMappings		×
issuerAltName		×
subjectAltName	FALSE	○
rfc822Name		×
otherName		○
userPrincipalName		(例)taro@dd.co.jp(UTF8String)
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		○
uniformResourceIdentifier		http://www.eppcert.jp/g3/rlist/epg3ca.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×
なし		×

表 A-7　クライアント証明書 for Sign プロファイル(基本部)

領域名	規定内容と設定値
基本部	
version	2(v3)
serialNumber	1001（例）
signature	Sha256WithRSAEncryption
validity	○
notBefore	有効期間は 60 日,1 年,2 年,3 年,5 年のいずれかに設定（UTCTime で設定する）
notAfter	
issuer	c=JP（Printable）, o=Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
subject	c=JP（Printable）, o= ABC Corporation(会社名等英語（オプション）,Printable ）, ou= XYZ Department(部署名等英語（オプション）,Printable), ou =xxxxxxxx（役職等英語（オプション）,Printable）, cn=Taro Mitsubishi（固有名称,固有番号等英語（必須）,Printable）, uid=FCxxxxxxxxxx(証明書固有番号（必須）,Printable）, serialNumber= xxxxxxxx （固有番号等数字（オプション）,Printable）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値(2048bit)
issuerUniqueID	×
subjectUniqueID	×

表 A-8 クライアント証明書 for Sign プロファイル(拡張部)

領域名	クリティカルフラグ	規定内容と設定値
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP（Printable）, o= Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		証明書公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		1 （電子署名）
nonRepudiation		1 （否認防止用の署名検証）
keyEncipherment		1 （鍵の暗号化が可能）
dataEncipherment		1 （データを直接暗号化可能）
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		1.2.392.200127.9.2
policyQualifiers		1.3.6.1.5.5.7.2.1（id-qt-cps）
qualifier		http://www.eppcert.jp/(IA5)
policyMappings		×
issuerAltName		×
subjectAltName	FALSE	○
rfc822Name		(例)taro@dd.co.jp(IA5)
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		○
uniformResou rceIdentifier		http://www.eppcert.jp/g3/rlist/epg3ca.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×
なし		×

表 A-9 クライアント証明書 for Auth プロファイル(基本部)

領域名	規定内容と設定値
基本部	
version	2(v3)
serialNumber	1001（例）
signature	sha256WithRSAEncryption
validity	○
notBefore	有効期間は 60 日,1 年,2 年,3 年,5 年のいずれかに設定（UTCTime で設定する）
notAfter	
issuer	c=JP（Printable）, o=Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
subject	c=JP（Printable）, o= ABC Corporation(会社名等英語（オプション）,Printable）, ou= XYZ Department(部署名等英語（オプション）,Printable), ou =xxxxxxxx（役職等英語（オプション）,Printable）, cn=Taro Mitsubishi（固有名称,固有番号英語（必須）,Printable）, uid=FCxxxxxxxxxx(証明書固有番号（必須）,Printable）, serialNumber= xxxxxxxx （固有番号等数字（オプション）,Printable）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値(2048bit)
issuerUniqueID	×
subjectUniqueID	×

表 A-10 クライアント証明書 for Auth プロファイル(拡張部)

領域名	クリティカルフラグ	規定内容と設定値
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP（Printable）, o= Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		証明書公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		1 （電子署名）
keyEncipherment		1 （鍵の暗号化が可能）
extendedKeyUsage		×
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		1.2.392.200127.9.2
policyQualifiers		1.3.6.1.5.5.7.2.1（id-qt-cps）
qualifier		http://www.eppcert.jp/(IA5)
policyMappings		×
issuerAltName		×
subjectAltName	FALSE	○
rfc822Name		(例)taro@dd.co.jp(IA5)
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		○
uniformResou rceIdentifier		http://www.eppcert.jp/g3/rlist/epg3ca.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×
なし		×

表 A-11 ネットワーク機器用サーバ証明書プロファイル(基本部)

領域名	規定内容と設定値
基本部	
version	2(v3)
serialNumber	1001（例）
signature	sha256WithRSAEncryption
validity	○
notBefore	有効期間は 60 日,1 年,2 年,3 年,5 年に設定(UTCTime で設定する)
notAfter	
issuer	c=JP（Printable）, o=Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
subject	c=JP（Printable）, o= ABC Corporation(会社名等英語（オプション）,Printable）, ou= XYZ Department(部署名等英語（オプション）,Printable), ou =xxxxxxxx（役職等英語（オプション）,Printable） cn= xxxxxxxx（FQDN 等英語（必須）,Printable） uid=FCxxxxxxxxxx(証明書固有番号（必須）,Printable）, serialNumber= xxxxxxxx （固有番号等数字（オプション）,Printable）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値(2048bit)
issuerUniqueID	×
subjectUniqueID	×

表 A-12 ネットワーク機器用サーバ証明書プロファイル(拡張部)

領域名	クリティカルフラグ	規定内容と設定値
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		
directoryName		c=JP（Printable）, o= Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		証明書公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		1 （電子署名）
nonRepudiation		1 （否認防止用の署名検証）
keyEncipherment		1 （鍵の暗号化が可能）
dataEncipherment		1 （データを直接暗号化可能）
extendedKeyUsage	FALSE	○
dNSName		{id-kp 1} (SSL サーバ認証)
dNSName		{id-kp 2} (クライアント認証)
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		1.2.392.200127.9.2
policyQualifiers		×
qualifier		×
policyMappings		×
issuerAltName		×
subjectAltName	FALSE	×
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		○
uniformResou rceIdentifier		http://www.eppcert.jp/g3/rlist/epg3ca.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×
なし		×

－

表 A-13　Web サーバ用証明書プロファイル(基本部)

領域名	規定内容と設定値
基本部	
version	2(v3)
serialNumber	1001（例）
signature	sha256WithRSAEncryption
validity	○
notBefore	有効期間は 60 日,1 年,2 年,3 年,5 年のいずれかに設定（UTCTime で設定する）
notAfter	
issuer	c=JP(Printable), o=Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
subject	c= CSR に指定した countryName （通常、JP、Printable), st=CSR に指定した stateOrProvinceName （通常、都道府県名、Printable), l= CSR に指定した localityName （通常、市町村名以下の住所、Printable), street=CSR に指定（可能な場合）した streetAdress （通常、住所の localityName 以下の番地等、Printable), o=CSR に指定した organizationName （通常、会社名、Printable), ou=CSR に指定した organizationUnitName （通常、所属名、Printable), cn= CSR に指定した commonName （通常サーバのホスト名(FQDN)、Printable）
subjectPublicKeyInfo	○
algorithm	rsaEncryption
subjectPublicKey	RSA 公開鍵値(2048bit)
issuerUniqueID	×
subjectUniqueID	×

表 A-14　Web サーバ用証明書プロファイル(拡張部)

領域名	クリティカルフラグ	規定内容と設定値
標準拡張領域		
authorityKeyIdentifier	FALSE	○
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		○
directoryName		c=JP（Printable）, o= Enterprise Premium Service（Printable）, cn=Enterprise Premium CA - G3（Printable）
authorityCertSerial		CA 証明書の serialNumber
subjectKeyIdentifier	FALSE	○
keyIdentifier		証明書公開鍵の SHA-1 ハッシュ値
keyUsage	TRUE	○
digitalSignature		1　（電子署名）
keyEncipherment		1　（鍵の暗号化が可能）
dataEncipherment		1　（データを直接暗号化可能）
extendedKeyUsage	FALSE	○
serverAuth		{id-kp 1}　(SSL サーバ認証)
clientAuth		{id-kp 2}　(クライアント認証)
privateKeyUsagePeriod		×
certificatePolicies	FALSE	○
policyIdentifier		○
certPolicyId		1.2.392.200127.9.2
policyQualifiers		×
policyMappings		×
issuerAltName		×
subjectAltName		×
basicConstraints		×
nameConstraints		×
policyConstraints		×
cRLDistributionPoints	FALSE	○
distributionPoint		○
fullName		○
uniformResou rceIdentifier		http://www.eppcert.jp/g3/rlist/epg3ca.crl
subjectDirectoryAttr		×
authorityInfoAccess		×
独自拡張領域		×
なし		

別紙 2. CRL プロファイル

表 B-1 に、CRL プロファイルを示す。

表 B-1 CRL プロファイル

領域名	クリティカルフラグ	規定内容と設定値（〇：設定する、×：設定しない）
CRL 基本部		
version		1（v2）
signature		sha256WithRSAEncryption
issuer		c=JP（Printable）， o=Enterprise Premium Service（Printable）， cn=Enterprise Premium CA - G3（Printable）
thisUpdate		CRL 発行日時（UTCTime で設定する）
nextUpdate		CRL 発行日時 2 ヶ月（UTCTime で設定する）
revokedCertificates		〇
userCertificate		加入者証明書の serialNumber
revocationDate		失効日時（UTCTime で設定する）
crlEntryExtentions		〇
reasonCode	FALSE	RFC2459 で定義される理由コード
CRL 拡張領域		
authorityKeyIdentifier	FALSE	〇
keyIdentifier		CA 公開鍵の SHA-1 ハッシュ値
authorityCertIssuer		〇
directoryName		c=JP（Printable）， o=Enterprise Premium Service（Printable）， cn=Enterprise Premium CA - G3（Printable）
authorityCertSerial		CA 証明書の serialNumber
cRLNumber	FALSE	本 CRL のシリアル番号