くまもとメディカルネットワーク PKI 認証局運用規程

（CPS: Certification Practice Statement）

Ver. 1.00

2016 年 2 月 25 日

公益社団法熊本県医師会

くまもとメディカルネットワーク PKI 認証局運用規程（CPS）

改定履歴

版数	日付	内容
1.00	2016-2-25	初版制定

― 目次 ―

1. はじめに

1.1 概要

公益社団法人熊本県医師会（以下、「本会」という。）は、くまもとメディカルネットワークの利用施設（以下、「利用施設」という。）に、利用者認証用証明書を IC チップに格納した「くまもとメディカルネットワーク利用者カード」（以下、「利用者カード）という。）を提供する。
利用者カードの発行、失効を含む証明書の運営サービス（以下、「本サービス」という。）は、本会が運営する、くまもとメディカルネットワーク PKI 認証局（以下、「本認証局」という。）が行う。
本認証局運用規程（以下、「本 CPS」という。）は、証明書ポリシ（以下、「CP」という。）を個別に定めず、本 CPS が CP を包含するものとする。
本 CPS は、以下に準拠して構成される。

- IETF/RFC3647　Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- 日本国内に設置される本認証局業務に関連する日本国法

1.2 文書の名前と識別

本ドキュメントの正式名称を以下の通りとする。
公益社団法人熊本県医師会くまもとメディカルネットワーク PKI 認証局運用規程（Certification Practice Statement）（以下、「本 CPS」という。）

1.3 PKI の関係者

本 CPS は、本認証局により実施される証明書発行及び失効業務に適用される。また、本認証局により発行される全ての証明書には本 CPS が適用される。

1.3.1 認証局

本認証局（CA）は、発行局（IA）と登録局（RA）をその構成要素とし、本会により運営される。但し、本 CPS の遵守及び個人情報の厳正な取扱いを条件に、契約を取り交わすことで認証業務の一部又は全部を外部委託することができる。

1.3.2 発行局

発行局は、登録局からの証明書発行、失効等の指示を受け、証明書利用者の鍵ペアの生成及び証明書の発行、失効の業務を行う。また、証明書失効リスト（以下、CRL という。）の生成と公開を行う。
また、本 CPS に従い秘密鍵の管理を行う。
本 CPS の遵守及び個人情報の厳正な取扱いを条件に、契約を取り交わすことで発行局業務の一部又は全部を外部委託することができる。

1.3.3 登録局

登録局は、利用者カードの利用施設からの発行申請を受け、発行局に証明書の発行要求をし、発行された証明書を利用者カードに格納する、あるいは失効要求等の業務を行う。

なお、本 CPS の遵守及び個人情報の厳正な取扱いを条件に、契約を取り交わすことで登録局業務の一部又は全部を外部委託することができる。

1.3.4 利用施設

利用者管理組織ともいう。

利用施設は、利用者カードの管理を行うため、本 CPS 及び関連諸規程に同意の上、利用施設が申込責任者として選任した個人（以下、「本サービス申込責任者」という。）から本会に利用者カードの発行等を申請し、利用施設の利用者に交付する。

利用施設は、利用者カードの利用に際しては、当該利用施設に所属する利用者に本 CPS 及び関連諸規程を遵守させる。

1.3.5 利用者

利用施設に所属する者であり、利用者カードを利用する個人をいう。利用者は、利用者カードの利用停止等の必要が生じた場合、利用施設の指示又は定めに従わなくてはならない。

1.3.6 検証者

信頼当事者ともいう。

利用者カード証明書の検証者とは、加入者組織の指示または定める事項に従い、利用者カード証明書の有効性にについて検証を行い、それらの証明書を信頼するよう設定されたネットワーク機器等を利用又は管理する組織又は個人をいう。

ただし、本証明書を利用するくまもとメディカルネットワークでは、システムのサーバで有効性検証をしており、本 CPS では特に規定しない。

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

（1）本 CPS で定める利用者カードに格納された証明書は、利用施設に所属する個人を認証し、それらと、くまもとメディカルネットワーク機器間におけるユーザ認証を実現する。

（2）本証明書は、くまもとメディカルネットワークの利用にのみ使用され、他の目的に使用してはならない。

（3）利用施設が、くまもとメディカルネットワークに参加しており、かつ参加利用施設がその所属する利用者への証明書発行を許可した利用者のみが使用することができるものとする。

（4）複数の利用施設に所属する利用者の場合、当該複数の施設から証明書の発行申請をすることとし、利用者は当該施設で当該証明書を利用するものとする。

（5）本認証局は、本認証局の判断と管理の下で、動作確認を目的としたテスト用利用者カードの発行・失効を行えるものとする。

1.4.2 禁止される証明書の使用

本 CPS で定める利用者カード証明書は、くまもとメディカルネットワークでの利用に限られ、かつ、本 CPS「1.4.1 適切な証明書の使用」で定める用途でのみ利用するものとする。それ以外の用途で使用された場合、本会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 文書を管理する組織

本 CPS は、本会により管理される。

1.5.2 問い合わせ先

本 CPS に関する問い合わせ先を以下に定める。

くまもとメディカルネットワークサポートセンター

公益社団法人 熊本県医師会（内）

電話：0120-25-3735　　FAX：096-211-9926

（受付）午前 9：00～12：00　午後 1：00～午後 5：00

（土日、祝日、熊本県医師会の休日を除く）

1.5.3 CPS のポリシ適合性を決定する者

規定しない。

1.5.4 CPS 承認手続き

規定しない。

1.6 定義と略語

（あ～ん）

- 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。

- 秘密鍵管理モジュール（Hardware Security Module：HSM）

  秘密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、公開鍵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。

- 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）
  秘密鍵とそれに対応する公開鍵の対
- 業務記録の保管（Archive）
  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。
- 危殆化（Compromise）
  秘密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。
- 検証者（Relying Party）
  信頼当事者ともいう。検証者とは、証明書の有効性を確認する者をいう。
  本システムで利用する利用者カード（証明書）の有効性検証は、システムで自動検証される。
- 公開鍵（Public Key）
  秘密鍵と対になる鍵で、デジタル署名の検証に用いる。
- 公開鍵証明書（Public Key Certificate：PKI）
  利用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、公開鍵の利用者情報、公開鍵、CA 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証明書。発行者名と利用者名が同じである。
- 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 CA の判断で失効されることもある。
- 秘密鍵（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所有者だけが管理する。秘密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。
- 証明書
  電子証明書をいう。本認証用は、認証用証明書を利用者カードに格納して発行する。
- 証明書失効リスト（Certificate Revocation List、Authority Revocation List：CRL）
  失効した証明書のリスト。
  本認証局においては、利用者証明書の失効リストが CRL に記載される。
- 証明書発行要求（Certificate Signing Request）
  登録局から発行局に証明書発行を求めるための要求。証明書を作成するための元となる情報。
- 証明書発行（失効）申請
  利用施設から登録局に、利用施設に所属する利用者用の証明書発行（失効）等の申し込みを行う。
- 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。

・ 登録局（Registration Authority：RA）
証明書発行の申請組織の申請を審査・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。

・ 認証局（Certification Authority：CA）
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な第三者機関で、公正、中立な立場にあり信頼できなければならない。

・ 認証実施規程（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。本認証局は、CP を包含した CPS を運用規程として定めている。

・ 発行局（Issuer Authority：IA）
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。

・ プロファイル（Profile）
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。

・ 利用者
認証局から認証のための証明書を利用施設経由で交付される者。

・ 利用施設
利用者管理組織ともいう。
本認証局へ証明書の発行・失効等の申請を行う組織で、利用（施設）組織に所属する利用者に証明書を交付し、適切な利用を管理する。

・ リポジトリ（Repository）
証明書及び証明書失効リストを格納し公開するデータベース。

・ リンク証明書

（A～Z）

・ CA 証明書
認証局に対して発行された証明書。本認証局における CA 証明書は、自己署名証明書である。

・ CP（Certificate Policy）
証明書ポリシを参照のこと。

・ CPS（Certification Practice Statement）

認証実施規程を参照のこと。

- CRL（Certificate Revocation List）
  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。
- 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、利用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、FIPS140-1/140-2 は暗号化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。
- 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。
- SHA-2（Secure Hash Algorithm-2）
  SHA-2 グループの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。

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、24 時間 365 日運用利用可能なものとし、常に最新に保たれるものとする。但し、システム保守作業等により予め情報公開用 Web サイト等で通知して、一時的に停止することがある。また、緊急時などやむを得ない場合は、事前に通知できない場合もある。
リポジトリは、認証局の証明書と失効情報及び利用者の失効情報を保持する。

リポジトリ及び情報公開用 Web サイトは、以下に示す URL にて公開される。
くまもとメディカルネットワークホームページ
http://kmn.kumamoto.med.or.jp
(くまもとメディカルネットワーク内リポジトリ)
http://pki.kmn.kumamoto.med.or.jp/revoke.crl
(くまもとメディカルネットワーク外リポジトリ)
http://mpkicrl.managedpki.ne.jp/mpki/KumamotoMedicalAssociationCAG1/cdp.crl

2.2 証明書情報の公開

本認証局では、以下の情報をリポジトリもしくは公開用 Web サイトを利用して公開する。

（1）リポジトリで公開される情報
- CA 証明書
- CRL

（2）Web サイト上で公開される情報
- 本 CPS
- 利用規約
- 個人情報保護方針
- 証明書及び CRL のプロファイル、その他、本認証局の運営上、必要なもの

2.3 公開の時期又はその頻度

本 CPS「2.2 証明書情報の公開（1）リポジトリで公開される情報」で定めた情報は、情報の変更が確定してから 24 時間以内に更新されるものとする。また、本 CPS「2.2 証明書情報の公開（2）Web サイト上で公開される情報」で定めた情報は、情報の変更が確定してから速やかに更新されるものとする。

2.4 リポジトリへのアクセス管理

本認証局のリポジトリに公開された情報は、インターネットを通じて提供される。なお、公開情報は利用者及び検証者に対しては読み取り専用として公開する。
公開情報は、インターネットなどの媒体を使い速やかに提供されるものとする。

3. 識別及び認証

3.1 名称決定

3.1.1 名称の種類

利用者名は X.500 の Distinguished Name（以下、DN という。）により識別される。

3.1.2 名称が意味を持つことの必要性

本認証局が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。

3.1.3 利用者の匿名性又は仮名性

規定しない。

3.1.4 種々名称形式を解釈するための規則

本認証局が発行する証明書の DN 等の形式の解釈は、X.500 に準ずる。

3.1.5 名称の一意性

発行局は、発行する証明書に記載される組織名（Organization）により登録局を一意に識別する。登録局は、利用施設が管理する利用者個人の情報を DN 及び SubjectAltName により一意に識別するよう、利用者カードの証明書を発行・管理する。

3.1.6 認識、認証及び商標の役割

本認証局は、登録局の登録及び証明書の発行に際し、著作権、営業秘密、商標権、実用新案権、特許権その他知的財産権については、確認しない。

3.2 初回の本人性確認

3.2.1 秘密鍵の所有を証明する方法

本認証局は、利用施設からの利用者リストの申請に基づき証明書を生成し利用施設に配布を行う。利用施設から利用者に確実に交付されることをもって、利用者が秘密鍵を保有したものとみなす。

3.2.2 利用者の確認

本認証局は、登録局が利用施設から申請される利用者リスト上で、利用者個人を確認することをもって利用者の確認とする。

3.2.3 確認しない利用者の情報

本認証局は、登録局が利用施設から申請された利用者リストについて、その真正性または正確性の確認は行わない。

3.2.4 利用施設の正当性確認

利用施設の実在性、保険医療機関である等の確認はしない。

但し、くまもとメディカルネットワークに利用参加している利用施設であることを確認する。（不参加もしくは参加撤回した利用施設には利用者カードを発行しない、もしくは返却を求める。）

3.2.5 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

本 CPS「3.2 初回の本人性確認」を準用する。

3.3.2 証明書失効後の鍵更新時の本人性確認

本 CPS「3.2 初回の本人性確認」を準用する。

3.4 失効申請時の本人性確認及び認証

本認証局は、登録局が利用施設から失効が必要になる利用者リストを受け取ることをもって、確認とする。

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

くまもとメディカルネットワークを利用する利用施設。

4.1.2 申請手続及び責任

利用施設が登録局に利用者リストを提出することをもって申請とする。利用施設は、申請における利用者リストを正確に記載する義務を負う。

4.2 証明書申請手続

4.2.1 利用者の本人性及び資格確認

本認証局は、利用者の本人性確認及び資格の確認は行わない。

4.2.2 証明書申請の承認又は却下

本認証局は、利用施設からの発行申請の受け取りにおいて、書類不備や確認過程において疑義が生じた場合には、利用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

登録局は、本 CPS「3.2.2　利用者の確認」に 従い発行局に対し証明書の発行指示を行う。発行局は、発行指示送信元である登録局の正当性を確認した上で、自動的に利用者の鍵ペアを生成し、対応する証明書を発行する。

4.3.2 証明書発行後の通知

本認証局は,登録局から利用施設に利用者カードを送付することにより、証明書を発行したことを通知する。

4.4 証明書の受理

4.4.1 証明書の受理

本認証局は、利用者カードを受領した利用施設から受領書を確認することにより、利用者が受領したことを確認する。

4.4.2 認証局による証明書の公開

本認証局は、利用者証明書の公開を行わない。

4.4.3 他の関係者に対する証明書発行通知

規定しない。

4.5 鍵ペアと証明書の利用目的

4.5.1 利用者の秘密鍵と証明書の利用目的

利用者は、本 CPS「1.4.1　適切な証明書の使用」に規定する利用目的にのみ証明書を利用しなければならない。

4.5.2 検証者の公開鍵と証明書の利用目的

規定しない。

4.6 証明書更新

本認証局が発行する全ての証明書の更新は鍵ペアの更新を伴うものとし、鍵ペアの更新を伴わない証明書発行は行わない。鍵ペアの更新を伴う証明書更新の要件については、本 CPS「4.7 証明書の鍵更新（鍵更新を伴う証明書更新）」に規定する。

4.6.1 証明書更新の要件

規定しない。

4.6.2 証明書の更新申請者

規定しない。

4.6.3 証明書更新の処理手順

規定しない。

4.6.4 利用者への新証明書発行通知

規定しない。

4.6.5 更新された証明書の受理

規定しない。

4.6.6 証明書による更新証明書の公開

規定しない。

4.6.7 他エンティティへの証明書発行通知

規定しない。

4.7 証明書の鍵更新（鍵更新を伴う証明書更新）

証明書更新（再発行等を含む）は、鍵ペアの更新を伴うものとする。

4.7.1 証明書鍵更新の要件

本認証局は、登録局が利用施設から更新の利用者リストを受け取った利用者に対し、鍵ペアの更新を伴う証明書の更新発行を行う。

4.7.2 鍵更新申請者

本 CPS「4.1.1　証明書の申請者」を準用する。

4.7.3 鍵更新申請の処理手順

本 CPS「4.2　証明書申請手続」を準用する。

4.7.4 利用者への新証明書発行通知

本 CPS「4.3 証明書発行後の通知」を準用する。

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」を準用する。

4.7.6 認証局による鍵更新証明書の公開

本認証局は、利用者証明書の公開を行わない。

4.7.7 他の関係者への証明書発行通知

本 CPS「4.4.3　他の関係者に対する証明書発行通知」を準用する。

4.8 証明書変更

本認証局は、証明書の記載事項に変更が生じた場合、利用者証明書のみの変更は行わず、当該証明書を失効させ、新規に鍵ペアの生成及び証明書発行を行うものとする。

4.8.1 証明書変更の要件

規定しない。

4.8.2 証明書変更申請者

規定しない。

4.8.3 変更申請の処理手順

規定しない。

4.8.4 利用者への新証明書発行通知

規定しない。

4.8.5 変更された証明書の受理

規定しない。

4.8.6 認証局による変更証明書の公開

規定しない。

4.8.7 他の関係者に対する変更された証明書の発行通知

規定しない。

4.9 証明書の失効と一時停止

4.9.1 証明書失効の要件

本認証局は、以下に示す場合に当該証明書を失効するものとする。

(1) 登録局による失効事由

登録局は、以下に示す証明書の失効事由が発生した場合、当該証明書を失効する権限を有するものとする。

- 利用施設もしくは利用者が本 CPS 及び利用規約に基づく義務に違反した場合
- 利用者秘密鍵が危殆化若しくはその恐れがあると認めた場合

- 利用者秘密鍵又は当該証明書が不正利用された場合、若しくはその危険性があると認めた場合
- 当該証明書の記載情報に事実と相違があり、又はその情報が変更されたことを登録局が確認した場合
- 利用施設の解散もしくはくまもとメディカルネットワークの利用中止を確認した場合
- 登録局の責めに帰すべき事由により当該証明書の誤発行等を行った場合
- 必要なサービス料金の支払いが得られない場合
- その他、登録局が必要と判断した場合

(2) 利用施設による失効事由

利用施設は、以下の場合には、直ちにその旨を登録局に申請し、当該証明書の失効申請を行わなければならない。

- 利用者カードの紛失または盗難があった場合
- パスワードの漏洩等で、利用者カードの不正使用の危険が予見される場合
- 当該証明書の記載事項が事実と異なる場合
- 当該証明書の記載事項に変更が生じた場合
- 利用施設が、事実と異なる申請をした場合
- 利用者秘密鍵が危殆化又は、危殆化の恐れがあると根拠のある確認をした場合
- 当該証明書の利用を中止する場合
- 利用施設の解散、もしくは、くまもとメディカルネットワークの利用中止をする場合

(3) 利用者による失効事由

登録局は、利用者からの失効申請を認めず、利用施設からの失効申請を認める。

利用者は、利用者カードの紛失、盗難等、パスワードの漏洩等で、利用者カードの不正使用の恐れがある場合、直ちに利用施設の窓口に申し出を行い、証明書の失効を依頼するものとする。

4.9.2 失効申請者

「4.9.1　証明書失効の要件」に準ずる。

4.9.3 失効申請の手続き

利用施設、登録局、発行局は、本 CPS「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、速やかに失効申請もしくは失効の処理を行わなければならない。

4.9.4 認証局による失効申請の処理期間

発行局は、登録局から失効の指示を受けた後、遅滞なく当該証明書の失効を行う。

4.9.5 検証者の失効の確認

規定しない。

4.9.6 CRL 発行周期

本認証局は、CRL を 24 時間周期で発行する。

本認証局 CRL の有効期間は、168 時間である。

4.9.7 CRL が公開されない最大期間

CRL は発行後 24 時間以内に公開される。

4.9.8 オンラインでの失効／ステータス情報の入手方法

本認証局は、CRL をもって失効情報を提供する。その他の方法での失効情報の提供は行わない。

4.9.9 オンラインでの失効確認要件

規定しない。

4.9.10 その他利用可能な失効情報確認手段

規定しない。

4.9.11 鍵の危殆化に関する特別な要件

本 CPS「5.7 危殆化及び災害からの復旧」の要件に従う。

4.9.12 証明書一時停止の要件

証明書の一時停止は行なわず、証明書の失効を行う。

4.9.13 一時停止申請者

証明書の一時停止は行なわず、証明書の失効を行う。

4.9.14 一時停止申請の処理手順

証明書の一時停止は行なわず、証明書の失効を行う。

4.9.15 一時停止期間の制限

証明書の一時停止は行なわず、証明書の失効を行う。

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 利用（登録）の終了

発行された証明書の有効期限をもって利用（登録）の終了とする。
証明書が有効である期間においては、本 CPS「4.9.1　証明書失効の要件」に基づく証明書の失効をもって利用（登録）の終了とする。

4.12 秘密鍵預託と鍵回復

利用者の秘密鍵は、法律によって必要とされる場合を除き、預託されないものとする。また、秘密鍵の回復も行わない。

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の手順

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

本認証局のシステムに係る施設（以下、「本施設」という。）は、地震、火災及び水害、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、水害及び不正侵入防止の措置を講じる。

また、本施設の内の発行局は、建築物の外部及び建築物内に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

本認証局に係る施設は、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

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。

（2）発行局

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。建物内及び各室内は、監視システム及び監視要員による 24 時間 365 日監視を行う。

5.1.3 電源設備及び空調

本認証局（登録局・発行局）に係る施設は、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及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、空調設備は二重化する。

5.1.4 水害及び地震対策

（1）水害対策

本認証局（登録局・発行局）に係る施設は、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、建物及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。

（2）地震対策

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及び什器には転倒及び落下を防止する対策を講じる。

5.1.5 防火設備

本認証局（登録局・発行局）に係る施設は、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 記録媒体の保管場所

本認証局（登録局・発行局）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できる室内に保管する。

5.1.7 廃棄物の処理

本認証局施設（登録局・発行局）では、機密情報を含む書類はシュレッダーにより裁断の上、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。

5.1.8 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。）及びその役割を以下のとおり定める。

（1） 認証局責任者

本認証局を統括し、登録局責任者及び発行局責任者を管理する。

（2） 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。

（3） 登録局オペレータ

本認証局の登録局に係る業務を行う。

証明書に関する窓口として、利用者・信頼者からの問い合わせにも対応する。

（4） 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及び発行局オペレータを管理する。

（5） 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。

（6） 発行局オペレータ

本認証局に係るシステムの運用、保守及び鍵管理等を行う。

（7） 業務監査担当者

本認証局とは独立した組織で監査を行う。

5.2.2 職務ごとに必要とされる要員数

発行局は、発行局システムアドミニストレータ及び発行局オペレータについては、2 名以上配置する。

登録局は、各役割に対して１名以上を配置する。但し、セキュリティ上問題が無いと判断された場合には、職務分離を必要としない場合に限り１名が複数の役割を兼務することがある。

5.2.3 個々の役割に対す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及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、証明書、ID 及びパスワード等の単体または組合せにより、本人性及び入室・操作権限の確認ならびに認証を行う。

5.2.4 職務分離が必要となる役割

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） 業務監査担当者

5.3 要員管理

5.3.1 資格、経験及び身分証明の要件

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 経歴の調査手続

規定しない。

5.3.3 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。

5.3.4 教育訓練の頻度及び要件

本認証局は、認証局員に対する再教育及び訓練を適宜実施する。

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 CPS、及び関連諸規程が改訂され、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。

5.3.5 職務のローテーションの頻度及び要件

本認証局は、必要に応じて認証局員の配置転換を行う。

5.3.6 認めら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 CPS に記載されるポリシと手続き、もしくは運用手順書に定める手順等に違反した場合、速やかに原因及び影響範囲の調査を行った上で、処罰を課す。

5.3.7 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、就業規則に則った義務を遵守させる。

5.3.8 要員へ提供する文書

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 監査ログの取扱い

5.4.1 記録するイベントの種類

本認証局は、本 CPS の準拠性及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及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 監査ログを保存する期間

本認証局は、発行した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、発行した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。

5.4.5 監査ログのバックアップ手続

本認証局は、監査ログに関する電子データのバックアップは、発行局規定によるものとする。紙媒体については、原本のみを保管する。

5.4.6 監査ログの収集システム（内部対外部）

発行局のシステムは、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 イベントを引き起こした当事者への通知

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

規定しない。

5.5 業務記録の保管

5.5.1 業務記録の種類

本認証局は、本 CPS「5.4.1　記録するイベントの種類」で規定された監査ログのほか、以下の情報を保管する。

（1） CA 証明書
（2） 証明書発行・失効に係る情報
（3） 利用者証明書
（4） 内部監査報告書
（5） 本 CPS 及び関連諸規程

5.5.2 業務記録を保存する期間

本認証局の登録局は、本 CPS「5.5.1　記録するイベント種類」に規定される記録の内、登録局業務に関わるものを証明書の発行日から４年間保管する。

発行局は、本 CPS「5.5.1　記録するイベント種類」に規定される記録の内、発行局業務に関わるものを証明書の発行日から発行局が規定する期間まで保管する。

5.5.3 業務記録の保護

本 CPS「5.4.4　監査ログの保護」を準用する。

5.5.4 業務記録のバックアップ手続

本 CPS「5.4.5　監査ログのバックアップ手続き」を準用する。

5.5.5 業務記録の日付要件

本認証局は、本 CPS「5.5.1　業務記録の種類」に関し、帳票類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立証性に欠ける場合は、時刻も記録する。本認証局及び利用者の証明書については、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、発行する証明書及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（内部対外部）

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 業務記録を入手し、検証する手続

本認証局は、本 CPS「5.5.1　業務記録の種類」に関し、記録の取得及び閲覧は、業務監査担当者及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 認証局秘密鍵の更新

本認証局は、定期的に認証局秘密鍵の更新を行う。認証局秘密鍵は、暗号化モジュール（HSM）を用いて生成される。

認証局秘密鍵の更新と共に CA 証明書の更新も実施される。

CA 証明書の更新実行後、本認証局は新しい CA 証明書、CRL を速やかにリポジトリにて公開する。

5.7 危殆化及び災害からの復旧

5.7.1 災害及び認証局秘密鍵危殆化からの復旧手続き

本会は、本認証局の責による場合を除き、認証局秘密鍵の危殆化もしくは災害による本認証局サービスの停止を不可抗力事項として取り扱い、本認証局の復旧を行うと共に本サービスの再開に努めるが、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、秘密鍵の危殆化もしくは災害が発生した場合、利用施設に当該事実を連絡すると共にリポジトリにおいても公開する。

利用施設は、これら連絡を受けた場合は、速やかに当該事実を当該利用施設の利用者に通知するものとする。

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、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。

5.7.3 認証局秘密鍵が危殆化した場合の対処

認証局秘密鍵が危殆化又は危殆化の恐れが生じた場合、認証局責任者の判断により、速やかに利用施設に連絡し、認証業務を停止するとともに、本認証局で規定された手続きに基づき、全ての証明書の失効を行い、CRL を開示し、認証局秘密鍵を廃棄する。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

本会は、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、利用施設に被災状況、復旧方針等を連絡すると共に、復旧作業を実施する。

5.8 認証局又は登録局の終了

本会は、本認証局のサービスを終了する場合、利用施設に廃止日の 60 日前までに通知を行い、認証業務の終了日までに、当該認証業務によって発行された全ての証明書を失効し、リポジトリに CRL を公開し、業務終了手続きを行う。

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、認証局責任者の指示の下、発行局責任者の管理の下、複数の発行局システムアドミニストレータにより生成される。鍵ペア生成の際には、FIPS140-1 レベル 4 の規格を満たす秘密鍵暗号化モジュール（以下、「HSM」という。）が用いられる。

6.1.2 利用者秘密鍵の配布

本認証局は、利用施設の申請に基づき秘密鍵を生成して、機密性、安全性を確保する措置を講じた上で、利用施設を通じて利用者に交付する。

6.1.3 認証局への利用者公開鍵の送付

配布しない。

6.1.4 検証者への認証局公開鍵の配布

本認証局は、認証局公開鍵をシステムのサーバに格納する。

6.1.5 鍵のサイズ

本認証局が発行する証明書に係る鍵は、下記の仕様に適合する鍵を利用する。

署名方式　：　SHA2withRSA

合成数　　：　2048 bit

6.1.6 公開鍵のパラメータ生成及び品質検査

規定しない。

6.2 秘密鍵の保護及び秘密鍵管理モジュール技術の管理

6.2.1 秘密鍵管理モジュールの標準と管理

本認証局の鍵ペアは、FIPS 140-1 レベル 4 の秘密鍵管理モジュール（HSM）にて保護する。上記のモジュールは、発行局オペレータが管理する。

6.2.2 複数人による秘密鍵の管理

本認証局の秘密鍵の管理は、常時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 秘密鍵のエスクロウ

本認証局は、本認証局の及び利用者の秘密鍵の預託を行わない。

6.2.4 秘密鍵のバックアップ

本認証局の秘密鍵のバックアップは、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秘密鍵は、暗号化して複数に分割し、施錠可能な保管庫にて安全に保管する。

6.2.5 秘密鍵のアーカイブ

本認証局は、本認証局の秘密鍵のアーカイブを行わない。

6.2.6 秘密鍵管理モジュールへの秘密鍵の格納と取り出し

本認証局は、HSM の故障など秘密鍵の復元が必要な場合、発行局責任者の管理・指示の下、発行局オペレータが、バックアップからの秘密鍵の復元を行う。このとき、バックアップデータを発行局施設外へ移送しない。

6.2.7 秘密鍵管理モジュール内での秘密鍵の保存

本認証局の秘密鍵は、HSM 内で生成する。秘密鍵管理モジュール内で秘密鍵は暗号化し保存する。

6.2.8 秘密鍵の活性化方法

本認証局の秘密鍵は、本認証局起動手順に従い、発行局管理者の管理の下、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 秘密鍵の非活性化方法

本認証局の秘密鍵は、本認証局停止手順に従い、発行局管理者の管理の下、複数人の発行局技術担当者が非活性化を行う。また、非活性化作業の内容を記録する。

6.2.10 秘密鍵の破壊方法

本認証局の秘密鍵は、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、複数の発行局システムアドミニストレータが破壊する。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破壊する。また、破壊作業の内容を記録する。

6.2.11 秘密鍵管理モジュールの評価

本認証局は、本 CPS「6.2.1 暗号モジュールの標準と管理」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面

6.3.1 公開鍵の保存

公開鍵の保存は、それを含む証明書を保存することによって行う。

6.4 活性化データ

6.4.1 活性化データの生成とインストール

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 活性化データの保護

本認証局内で使用される活性化情報は、本 CPS５．１　に基づき適切な入退室管理がなされた室内において、施錠可能な保管庫に保管する。

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

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 ライフサイクルの技術的管理

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、信頼できる組織及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、登録局については登録局オペレータの判断により、作業を実施する。

6.6.2 セキュリティ運用管理

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 ライフサイクルのセキュリティ管理

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 ネットワークのセキュリティ管理

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、発行する証明書及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. 証明書及び CRL のプロファイル

7.1 証明書のプロファイル

7.1.1 バージョン番号

別表　証明書プロファイルに規定する。

7.1.2 証明書の拡張領域

別表　証明書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

別表　証明書プロファイルに規定する。

7.1.4 名前の形式

別表　証明書プロファイルに規定する。

7.1.5 名前の制約

別表　証明書プロファイルに規定する。

7.1.6 証明書ポリシオブジェクト識別子

別表　証明書プロファイルに規定する。

7.1.7 ポリシ制約拡張の使用

別表　証明書プロファイルに規定する。

7.1.8 ポリシ修飾子の構文及び意味

別表　証明書プロファイルに規定する。

7.1.9 証明書ポリシ拡張についての処理

別表　証明書プロファイルに規定する。

7.2 CRL のプロファイル

7.2.1 バージョン番号

別表　証明書プロファイルに規定する。

7.2.2 CRL と CRL エントリ拡張

別表　証明書プロファイルに規定する。

7.3 OCSP のプロファイル

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 監査頻度と要件

本認証局は、認証業務に疑義が生じた場合、発行局及び登録局の全部または一部について、本 CPS「8.2　監査人の要件」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、必要な知識と経験を有する者が行う。

8.3 監査者と被監査者の関係

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 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、発行局責任者及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 監査結果の通知

本認証局は、監査結果を利用施設、利用者及び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. その他の事業上と法務上の事項

9.1 料金

本認証局に関わるサービス等の料金に関わる事項は、本 CPS では定めない。

9.1.1 証明書の発行又は更新料

規定しない。

9.1.2 証明書へのアクセス料金

規定しない。

9.1.3 失効又はステータス情報へのアクセス料金

規定しない。

9.1.4 その他のサービスに対する料金

規定しない。

9.1.5 払い戻し指針

規定しない。

9.2 財務上の責任

9.2.1 保険の適用範囲

規定しない。

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

規定しない。

9.3 情報の機密保護

9.3.1 機密情報の範囲

本会は、本認証局の発行局、登録局が取り扱う情報のうち、以下の情報を機密情報の範囲とする。

① 利用施設が登録局に提出する発行申請等の情報
② 本 CPS「9.4.2 個人情報として扱われる情報」に定める情報
③ 本認証局のセキュリティに関する情報

9.3.2 機密情報の範囲外の情報

本会は、本認証局の発行局、登録局が取り扱う利用施設から提供された情報のうち、以下の情報は機密情報の範囲外とする。

① 本 CPS「2.2 証明書情報の公開」において公開するものとしている情報
② 発行された証明書及び利用者カードの券面記載情報
③ 本認証局の過失によらず公知となった情報
④ 本認証局以外から機密保持の制限なしに開示され公知となった情報
⑤ 利用施設から事前に開示又は事前に第三者への提供の承諾を得た情報

9.3.3 機密情報を保護する責任

本会は、本 CPS「9.3.1 機密情報の範囲」で規定された認証局が保有する機密情報を保護する責任を負う。

但し、本認証局が保持する情報を、法の定めによる場合及び利用施設による事前の承諾を得た場合に開示することがある。その場合、当該情報を知り得た者は契約あるいは法的に当該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、当該情報が漏洩した場合、その責は漏洩した者が負う。

9.4 個人情報のプライバシー保護

9.4.1 プライバシーポリシ

本会は、本認証局の発行局及び登録局が保有する情報のうち、本 CPS「9.4.2 個人情報として扱われる情報」に 該当する情報について、本会の「個人情報保護方針」を適用する。

9.4.2 個人情報として扱われる情報

本会は、本認証局の登録局、発行局が保有する次の情報を保護すべき個人情報として取り扱う。

本認証局が、利用施設から発行申請等で提供された個人の情報であって、当該情報に含まれる氏名、生年月日その他から特定の個人を識別できるものを個人情報として取り扱う。

9.4.3 個人情報とはみなされない情報

本 CPS「9.4.2 個人情報として扱われる情報」以外は、個人情報とみなされない。

9.4.4 個人情報を保護する責任

本会は、本 CPS「9.4.2 個人情報として扱われる情報」で規定された個人情報を保護する責任を負う。

9.4.5 個人情報の使用に関する個人への通知及び同意

本会は、本認証局の登録局、発行局が保有する個人情報を、本認証局業務、くまもとメディカルネットワークの運営に関わる業務で利用するものとする。

それ以外の目的で個人情報を利用する場合は、利用施設から利用者本人に、予め同意を得るものとする。ただし、下記の場合はこの限りではない。

- 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利を害するおそれがある場合
- 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

- 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- 本会の公益目的のため、個人を特定できない状態に加工あるいは統計データ化して使用するとき。

9.4.6 司法手続又は行政手続に基づく公開

司法機関、行政機関その他の公的機関の決定、命令、勧告等があった場合、本会は個人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

証明書の発行申請等に、利用施設を通じて個人情報を提供した利用者本人から、当該利用施設を通じて当該本人に関する情報の開示を求められた場合は、別途定める手続きに従って、当該利用者カード（証明書）の有効期間内に限り、情報を開示する。この場合、開示作業にかかる費用については、情報開示を求める者の負担とする。

9.5 知的財産権

本会と、本認証局に関して利用施設との間で特段の合意がなされない限り、本認証局が提供するサービスに関わる情報資料及びデータは、次に示す当事者の権利に属するものとする。

- 利用者カード媒体：本会に帰属する財産とする。
- 証明書及び CRL 情報：本会または本会の委託先に帰属する財産とする。
- 本 CPS 及び関連諸規程：本会または本会の委託先に帰属する財産とする。

9.6 認証局及び利用者の義務

9.6.1 発行局の義務

発行局を運営する組織は、以下の義務を負う。

（1）本 CPS に従った認証局秘密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証明書の発行及び失効を行うこと
（3）CRL の発行及び公開を行うこと
（4）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 CPS に従ったシステムの監視及び運用を行うこと

9.6.2 登録局の義務

登録局を運営する組織は、以下の義務を負う。

（1） 本 CPS 及び各種関連諸規程を遵守すること
（2） 発行局へ証明書の発行、失効等情報を正確に指示すること
（3） 証明書の生成と利用者カード作成を、安全に行うこと
（4） 利用者カード（証明書）を利用施設に正しく配布すること
（5） 業務記録を、証明書の有効期間満了まで安全に保管すること

9.6.3 利用施設の義務

利用施設は、以下の義務を負う。

（1） 本 CPS 及び各種関連諸規程を遵守すること
（2） 本 CPS「9.6.4　利用者の義務」に示す事項を、利用者が履行するよう管理すること。
（3） 登録局に発行・失効等の申請を行う場合、登録局に提示する各書面の内容について、虚偽なく正確に記述すること
（4） 登録局から届けられる利用者カード（証明書）を、確実に利用者に交付すること
（5） 利用者が利用者秘密鍵を保護し、紛失、暴露、改ざん、または盗用されることを防止するために妥当な措置をとること
（6） 利用者が、利用者カード（証明書）の記載内容について、受領時に申請内容との相違がないかを確認するための妥当な措置をとること。また、その後も記載内容に現状との乖離が発生した場合には、速やかに変更・失効等の手続きを行うこと
（7） 利用者が、利用者カードの紛失等が発生した場合、速やかに届け出する措置をとること
（8） 利用者が、利用者カードのパスワードを秘匿するよう適切な措置をとること
（9） 利用施設の名称変更、申請責任者の変更、連絡先の変更、くまもとメディカルネットワークの利用中止が発生した場合、速やかに登録情報変更の届け出すること

9.6.4 利用者の義務

利用施設は、本認証局サービスを利用する当該利用施設に所属する利用者に、以下の義務を履行するよう管理する義務を負います。

（1） 本 CPS 及び各種関連諸規程を遵守すること
（2） 利用施設に提示する各書面の内容について、虚偽なく正確に記述すること
（3） 利用者は、利用者カードの秘密鍵を保護し、紛失、暴露、改ざん、盗用されることを防止すること
（4） 利用者が、利用者カード（証明書）の記載内容について、受領時に申請内容との相違がないかを確認すること。また、その後も記載内容に現状との乖離が発生した場合には、速やかに利用施設に届出すること
（5） 利用者カードの紛失等が発生した場合、速やかに届出すること
（6） 利用は、利用者カードのパスワードを秘匿すること
（7） くまもとメディカルネットワークの利用目的にのみ利用者カードを使用すること

9.6.5 検証者の義務

規定しない。

本認証局の検証者は、利用システムのサーバに該当する。

9.6.6 他の関係者の義務

規定しない。

9.7 無保証

本会は、本認証局サービスに関し、本 CPS「9.6.1　発行局の義務」及び「9.6.2　登録局の義務」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利用施設、利用者、若しくはその他の第三者において損害が生じた場合、一切の責任を負わない。

9.8 責任制限

本会は、本認証局サービスに関し、利用施設に所属する利用者において本 CPS 及び関連諸規程が遵守されないために生じた損害に対して、責任を負わない。

9.9 補償

本 CPS 及び関連諸規程に規定された責任を果たさなかったことに起因して、本会が利用施設もしくは利用者に損害を与えた場合、証明書発行サービス料を上限として、損害を賠償する。ただし、本会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、利用施設は証明書を申請した時点で、本会及び関連する組織等に対する損害賠償責任が発生する。

9.10 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、認証局代表者が承認することにより有効になる。また、「9.10.2 終了」で記述する本 CPS の終了まで有効であるものとする。

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、認証局責任者が無効と宣言した時点で、無効になる。

9.10.3 終了の影響と存続条項

終了した場合であっても、「9.3 企業情報の秘密保護」、「9.4 個人情報のプライバシー保護」、「9.5 知的財産権」に関する義務は存続するものとする。

9.11 関係者間の個々の通知と連絡

本認証局は、利用者が利用者証明書を利用するにあたって必要な情報を CRL もしくは情報公開用 Web サイトにおいて公表する。利用者は、定期的に CRL もしくは情報公開用 Web サイトを閲覧してこれらの情報を取得するものとする。

本認証局から利用施設及び利用者への通知方法は、電子メール、ホームページへの掲載、郵送による書面通知など認証局が適当と判断した方法により行うものとする。また、本認証局から利用者の届け出た住所、FAX 番号又は電子メールアドレスに宛てて利用者への通知を発した場合には、当該通知が延着又は不着となった場合であっても、通常到達すべき時に到達したものとみなす。

9.12 改訂

9.12.1 改訂手続き

本 CPS 及び関連諸規程の改訂は、各利用施設に通知し、改訂内容に合意した時点で改訂される。ただし、本認証局から変更内容を通知した後、15 日以内に利用解除の申し出がなかった場合は、利用施設は変更内容に合意したものとみなす。

9.12.2 通知方法と期間

本 CPS が改訂された場合、CRL もしくは情報公開用 Web サイト等を通じて、全ての利用施設と当該施設の利用者が速やかに入手可能な措置をとる。

公開の期間については、以下のように定める。

- 重要な変更は、通知後、15 日（告知期間）を経て効力を発行する。

9.12.3 オブジェクト識別子（OID）の変更理由

重要な変更の場合には、本 CPS のバージョン番号を更新する。

9.13 紛争解決手続

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

9.14 準拠法

本 CPS は、日本国内法を準拠法とする。

9.15 適用法の遵守

本 CPS の運用にあたっては、日本国内法及び公的通知等がある場合はそれを優先する。

9.16 雑則

9.16.1 完全合意条項

本 CPS は、当事者間の完全合意を構成し、本認証業務について記述された書面又は口頭による過去の一切の意思表示、合意事項に取って代わるものである

9.16.2 権利譲渡条項

関係者は、本 CPS に定める権利義務を第三者に譲渡又は担保に供することができない。

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

以下に例示されるような善良なる管理及び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。

- 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
- ストライキ、工場閉鎖、事業所閉鎖、労働争議
- 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

本認証局又は登録局が別の組織と合併若しくは別の組織に移管、譲渡する場合、新しい組織は本 CPS 及び関連諸規程の方針に同意し責任を持ち続けるものとする。

以上

別表　証明書プロファイル

エンドエンティティ認証用証明書プロファイル
CA 証明書プロファイル
CRL プロファイル

エンドエンティティ認証用証明書プロファイル

標準領域

Version		値
Version	電子証明書フォーマットのバージョン 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（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	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 or UTF8String 値：<< お客様会社名称 >>	＊文字値により変更される ＊発行局会社名称（英字）
OrganizationalUnitName	電子証明書発行者の部署名	＊必要な場合のみ
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 or UTF8String 値：<< お客様部署名称 >>	＊文字値により変更される ＊発行局部署名称（英字）
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 or UTF8String 値：<< お客様発行局名称 >>	＊文字値により変更される ＊発行局名称（英字）
Validity		値
Validity	電子証明書の有効期間	電子証明書の有効期間 3年
notBefore	開始日時 型：UTCTime or GeneralizedTime 値：年（2桁 or 4桁）月日時分秒 Z	＋猶予期間（1ヵ月） ＊有効開始日時 例 0602010000000Z
notAfter	終了日時 型：UTCTime or GeneralizedTime 値：年（2桁 or 4桁）月日時分秒 Z	＊有効終了日時 例 0803010000000Z

Subject		値
CountryName	電子証明所有者の国名	
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 *固定
OrganizationName	電子証明書所有者の組織名	
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 or UTF8String	*文字値により変更される
	値: << お客様指定会社名称 >>	*利用者の会社名称（英字）
OrganizationalUnitName	電子証明書所有者の部署名	*必要な場合のみ（最大3つまで）
Type	組織名のオブジェクトID	
	型: OID	
	値: 2 5 4 11	2.5.4.11
Value	組織名の値	
	型: PrintableString or UTF8String	*文字値により変更される
	値: << お客様指定部署称 >>	*利用者の部署名（英字）
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	*文字値により変更される
	値: << 証明書所有者の固有名称 >>	*利用者の氏名（ローマ字）

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（公開鍵と 暗号アルゴリズムの識別子（公開鍵と ハッシュ関数）	
	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
Algorithm	型: OID	
	値: 1 2 840 113549 1 1 1	1. 2. 840. 113549. 1.1. 1
	署名アルゴリズムの引数	
	型: NULL	
	値:	NULL
subjectPublicKe	公開鍵値	
	型:BIT STRING	
	値:公開鍵値	*鍵長は、2048Bit

拡張領域

authorityKeyIdentifier(extnId:==2 5 29 35, critical :== FALSE)		値
AuthorityKeyIdentifier 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 値：認証局のsbjectPublicKeyの Hash 値	＊電子証明書発行者の証明書のsbjectPublicKeyの Hash 値
subjectKeyIdentifier(extnId:==2 5 29 14, critical :== FALSE)		値
SubjectKeyIdentifier keyIdentifier	電子証明書所有者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRINGS 値：所有者のsubjectPublicKeyの Hash 値	＊電子証明書所有の証明書のsbjectPublicKeyの Hash 値
KeyUsage(extnId:==2 5 29 15, critical :== FALSE)		値
KeyUsage	鍵の使用目的 型：BIT STRINGS 値：100000000 （DigitalSignature）	＊電子証明書所有の証明書のsbjectPublicKeyの Hash 値 100000000
cRLDistributionPoints(extnId:==2 5 29 31, critical :== FALSE)		値
cRLDistributionPoints DistributionPoints fullName	CRL 配付ポイント CRL 配付ポイント CRLを配付するURI 型：OCTET STRINGS 値：http URI（ldap URI）	＊http（オプションによりLDAP）

CA証明書

標準領域

Version		値
Version	電子証明書フォーマットのバージョン 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（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	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 or UTF8String 値：<< お客様会社名称 >>	＊文字値により変更される ＊発行局会社名称（英字）
OrganizationalUnitName	電子証明書発行者の部署名	＊必要な場合のみ
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 or UTF8String 値：<< お客様部署名称 >>	＊文字値により変更される ＊発行局部署名称（英字）
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 or UTF8String 値：<< お客様発行局名称 >>	＊文字値により変更される ＊発行局名称（英字）
Validity		値
Validity	電子証明書の有効期間	電子証明書の有効期間 3年 ＋猶予期間（1ヵ月）
notBefore	開始日時 型：UTCTime or GeneralizedTime 値：年（2桁 or 4桁）月日時分秒 Z	＊有効開始日時 例 060201000000Z
notAfter	終了日時 型：UTCTime or GeneralizedTime 値：年（2桁 or 4桁）月日時分秒 Z	＊有効終了日時 例 0803010000000Z

Subject		値
CountryName	電子証明所有者の国名	
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 *固定
OrganizationName	電子証明書所有者の組織名	
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 or UTF8String	*文字値により変更される
	値：<< お客様指定会社名称 >>	*利用者の会社名称（英字）
OrganizationalUnitName	電子証明書所有者の部署名	*必要な場合のみ（最大3つまで）
Type	組織名のオブジェクトID	
	型：OID	
	値：2 5 4 11	2.5.4.11
Value	組織名の値	
	型：PrintableString or UTF8String	*文字値により変更される
	値：<< お客様指定部署称 >>	*利用者の部署名（英字）
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	*文字値により変更される
	値：<< 証明書発行局名称 >>	*認証局名称（英字）

SubjectPublicKeyInfo		値
SubjectPublicKeyInfo	電子証明 書発行者の公開鍵情報	
AlgorithmIdentifier	暗号アルゴリズムの識別子（公開鍵と 暗号アルゴリズムの識別子（公開鍵と ハッシュ関数）	
	暗号アルゴリズムのオブジェクト ID(RSA PUBLIC KEY)	
Algorithm	型：OID	
	値：1 2 840 113549 1 1 1	1. 2. 840. 113549. 1.1. 1
	署名アルゴリズムの引数	
	型：NULL	
	値：	NULL
subjectPublicKe	公開鍵値	
	型：BIT STRING	
	値：公開鍵値	*2048Bit長の公開鍵

拡張領域

BasicConstraints(extnId:==2 5 29 19, critical :== TRUE)		値
BasicConstraints cA	基本的制限 CAかどうかを示すフラグ 型：Boolean 値：True(CAである。)	 TRUE
authorityKeyIdentifier(extnId:==2 5 29 35, critical :== FALSE)		値
AuthorityKeyIdentifier 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：Root認証局のsbjectPublicKeyの Hash 値	(該当なし。) ＊RootCA証明書の sbjectPublicKeyの Hash 値
subjectKeyIdentifier(extnId:==2 5 29 14, critical :== FALSE)		値
SubjectKeyIdentifier keyIdentifier	電子証明書所有者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRINGS 値：発行者のsubjectPublicKeyの Hash 値	
KeyUsage(extnId:==2 5 29 15, critical :== TRUE)		値
KeyUsage	鍵の使用目的 型：BIT STRINGS 値：11000110 DigitalSignature,NonRepdiation,CertificateSigning,CRLSigning))	 11000110
cRLDistributionPoints(extnId:==2 5 29 31, critical :== FALSE)		値
cRLDistributionPoints DistributionPoints fullName	CRL 配付ポイント CRL 配付ポイント CRLを配付するURI 型：OCTET STRINGS 値：http URI (ldap URI)	(該当なし。) ＊http（オプションによりLDAP）

CRLプロファイル

標準領域

Version		値
Version	フォーマットのバージョン 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 type	証明書発行リスト発行者の国名 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 Type	証明書失効リスト発行者の組織名 組織名のオブジェクト ID 型：OID 値：2 5 4 10	2.5.4.10
Value	組織名の値 型：PrintableString or UTF8String 値：<< お客様会社名称 >>	＊文字値により変更される ＊発行局会社名称（英字）
OrganizationalUnitName Type	証明書失効リスト発行者の部署名 部署名のオブジェクトID 型：OID 値：2 5 4 11	＊必要な場合のみ 2.5.4.11
Value	部署名の値 型：PrintableString or UTF8String 値：<< お客様部署名称 >>	＊文字値により変更される ＊発行局部署名称（英字）
CommonName Type	証明書失効リスト発行者の固有名称 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：<< お客様発行局名称 >>	＊文字値により変更される ＊発行局名称（英字）
thisUpdate		値
thisUpdate	有効開始日 型：UTCTime or GeneralizedTime 値：年（2桁 or 4桁）月日時分秒 Z	＊有効開始日時 例　021225000000Z
nextUpdate		値
nextUpdate	次回更新予定日時 型：UTCTime or GeneralizedTime 値：年（2桁 or 4桁）月日時分秒 Z	有効開始日から1週間後 ＊更新開始日時 例　030101000000Z

拡張領域

authorityKeyIdentifier(extnId:==2 5 29 35, critical :== FALSE)		値
AuthorityKeyIdentifier keyIdentifier	証明書失効リスト発行者の公開鍵に関する情報 公開鍵の識別子 型：OCTET STRING 値：認証局のsbjectPublicKeyの Hash 値	(該当なし。) ＊認証局の sbjectPublicKeyの Hash 値
cRLNumber(extnId:==2 5 29 35, critical :== FALSE)		値
cRLNumbe	CRLの番号 型：INTEGER 値：ユニークな整数	＊CRLの番号

エントリ領域

revokedCertificates		値
CertificateSirialNumber	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	失効日次 型：UTCTime or GeneralizedTime	

エントリ拡張領域

invalidityDate(extnId:==2 5 29 24, critical :== FALSE)		値
invalidityDate	無効化日時 型： UTCTime or GeneralizedTime	
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)cessionOfOperation ＊unspecifiedは、cRLReasonとして出力しない。