文書番号	HPCI-CA03-001-19

HPCI 認証局運用規程

Ver9.1

2024.01.25

HPCI 認証局ポリシー管理委員会

改訂履歴

発行年月日	Ver.	OID	改訂内容
2011.12.28	1.0	1.3.6.1.4.1.32264.2.1.1	新規作成
2012.05.29	1.1	1.3.6.1.4.1.32264.2.1.2	「9．12．1 改訂手続き」にて、「誤字修正等の軽微な変更については、…（中略）…新たな OID を割り振る。」に修正。
2012.06.19	1.2	1.3.6.1.4.1.32264.2.1.3	「4．9．3 失効申請の手続き」「(2) HPCI-ID 管理機関による失効手続き」にて、「HPCI 認証局へ失効申請書又は同等の内容を紙媒体又は電子媒体で送付」に修正。
2012.08.16	1.3	1.3.6.1.4.1.32264.2.1.4	「3．2．3 利用者の確認」ならびに「5．2．1 信頼すべき役割」の「表 5 1」にて、国立情報学研究所が運用するサーバのホスト管理者の識別について追記。 「4．3．1 証明書の発行処理」にて、「通信路はすべて暗号化され」を削除し、手続きについての条件の記載を修正。 「5．4．4 監査ログの保護」にて、「施錠可能な」を削除。 用語「認証ポータル」を「証明書発行システム」に修正。HPCI ID の記載を「HPCI-ID」に修正。
2012.08.28	1.4	1.3.6.1.4.1.32264.2.1.5	「3．2．3 利用者の確認」にて、提示する資料の候補から公文書を削除し、身分証に写真がない場合の記述を追加。
2013.03.01	1.5	1.3.6.1.4.1.32264.2.1.6	「1．1 概要」「1．3．3 証明書利用者」にて、クライアント証明書の発行対象の条件を修正。 「1．4．2 禁止されている証明書用途」「6．2．8 秘密鍵活性化の方法」にて、クライアント証明書の利用対象資源の条件を修正。 「4．9．2 失効申請者」にて、「HPCI アカウント IdP 運用機関」を「HPCI-ID 管理機関」に修正。 「9．6．2 HPCI-ID 管理機関の義務と責任」にて、「証明書利用者の氏名、所属組織の変更」を「証明書利用者の氏名の変更」に修正。
2013.04.01	1.6	1.3.6.1.4.1.32264.2.1.7	「4．3．1 証明書の発行処理 クライアント証明書」にて、「ユーザと HPCI 認証局間の…（中略）…全て暗号化される。」を削除。
2013.08.16	1.7	1.3.6.1.4.1.32264.2.1.8	「5．4．1 記録されるイベントの種類」「5．5．1 アーカイブデータの種類」にて、HPCI-ID 管理機関の記録の定義を変更。 「8．1 準拠性監査の頻度又は条件」にて、HPCI-ID 管理機関が実施する準拠性監査の定義を変更。 「8．3 監査人と被監査人の関係」にて、監査人の定義を変更。 「9．6．1 HPCI 認証局の義務と責任」にて、運用要件の定義を変更。 「9．6．2 HPCI-ID 管理機関の義務と責

			任」にて、HPCI 認証局の運用要件を遵守するための義務の定義を変更。
2014.03.05	1.8	1.3.6.1.4.1.32264.2.1.9	「1．3．2 登録局」にて、利用者情報に連絡先が含まれることを明記。 「1．3．4 証明書検証者」、「1．3．5 その他関係者」を新設。 「1．4．1 証明書の用途」にて、旧版の「証明書の種類」と「証明書の用途」を統合。 「2．2 証明情報の公開」にて、CRL の公開先 URL を変更。 「4．9．3 失効申請の手続き」にて、証明書発行システムから失効申請を実施した場合も、失効申請の手続きとして適当である旨を追記。 「5．1．1 設備の所在と構造」にて、旧版の「地震対策」を統合。 「5．5．2 アーカイブデータの保管期間」にて、アーカイブデータの保存期間の説明を追記。 「5．6 鍵の更新」にて、CA のライフサイクルを説明するよう修正。 「6．2．2 秘密鍵の複数人制御（n out of m）」にて、担当者を変更。 「6．2．4 秘密鍵のバックアップ」にて、秘密鍵の保管について追記。 「6．3．2 証明書の運用上の期間及び鍵ペアの使用期間」にて、旧版の「利用者証明書の有効期限」と「CA 証明書の有効期間」を統合。有効期限を「毎年 4 月 24 日」に修正。 「9．3 業務情報の秘密性」、「9．4 個人情報の保護」にて、URL を修正。 「9．6．2 HPCI-ID 管理機関の義務と責任」にて、認証情報のネットワーク送信について追記。 「9．6．3 利用者の義務と責任」にて、失効申請の1営業日以内に行うよう修正。 RFC3647 に準拠したセクション名に修正。 「1．3 PKI の関係者」に合わせて用語を統一。
2015.11.30	1.9	1.3.6.1.4.1.32264.2.1.10	本規程は、APGridPMA による MICS 準拠に関する承認を受けたため、「9．12．1 改訂手続き」にて、「また、APGridPMA による…（中略）…、再度承認を受ける。」を削除。
2016.06.15	2.0	1.3.6.1.4.1.32264.2.1.11	「1．1 概要」、「1．3．1 認証局」、「1．4．1 証明書の用途」、「1．6 定義と略称」、「2．1 認証局リポジトリ」、「2．2 証明情報の公開」、「4．9．6 検証者に対する失効情報の要件」、「4．9．9 オンラインでの失効/ステータス（OCSP）確認の適用性」、「4．10．1 証明書ステータスサービスの内容」、「6．1．5 アルゴリズムと鍵長」、「6．1．7 鍵利用目的(X.509 v3 KeyUsage Field)」「6．3．2 証明書の運用上の期間

			及び鍵ペアの使用期間」、「7. 証明書、CRLのプロファイル」、「9. 6. 1 HPCI認証局の義務と責任」、図 1-1 HPCI認証局の構成 にて、OCSP レスポンダの情報を記載。 「ステイタス」を「ステータス」に統一
2016.08.16	3.0	1.3.6.1.4.1.32264.2.1.12	「9. 6. 3 利用者の義務と責任」にて、「クライアント証明書は、共有しない」を追記。
2016.11.11	4.0	1.3.6.1.4.1.32264.2.1.13	「1. はじめに」にて、HPCI の説明を追記。 「3. 3. 1 鍵の定期更新時の識別と認証」にて HPCI アカウント更新時の手続きに関して修正 「4. 9. 1 失効事由」「4. 9. 3 失効申請の手続き」にて証明書失効の手続きに関して修正
2017.06.01	5.0	1.3.6.1.4.1.32264.2.1.14	「3. 1. 2 名前の意味に関する要件」にて、クライアント証明書における commonName は、少なくとも姓および名をそれぞれ完全な形で含むよう追記。
2017.09.25	6.0	1.3.6.1.4.1.32264.2.1.15	「6. 3. 2 証明書の運用上の期間及び鍵ペアの使用期間」にて、クライアント証明書の有効期限を「発行してから 395 日後」に変更。
2020.10.02	7.0	1.3.6.1.4.1.32264.2.1.16	[3. 2. 3(1)ユーザの確認」にて、物理的に対面して行う場合に加えて、テレビ会議を通じて遠隔で行う場合を追記。 「5. 5. 1アーカイブデータの種類」にて、HPCI-ID 管理機関において保管する書類として、「テレビ会議を通じてユーザの識別を遠隔で行った場合の申請責任者の顔と写真付き身分証が同時に写った画像」を追記。
2021.06.30	8.0	1.3.6.1.4.1.32264.2.1.17	「1. 3 PKI の関係者」にて、RFC 3647 に準拠するように構成を変更。 「1. 3. 1 認証局」、「1. 6 定義と略称」、「4. 1. 1 証明書申請を提出することができる者」にて、「オンライン証明書発行処理」を「オンライン証明書発行申請」に修正。 「1. 3. 2 登録局」にて、1. 3. 2(4)HPCI連携サービス運営・作業部会」を追加。 「1. 3. 5その他関係者」にて、HPCI PMA の役割のうち「HPCI アカウント IdP 運用機関からの連携申請の承認」を「HPCI アカウント IdP 運用機関の組織認定」に修正。 「1. 5. 2 連絡先」にて、メールで受け付けた問い合わせは、原則として 1 営業日以内の返信を目標とすることを追記。担当部署名は法人名を含めた正式名称に修正。電話番号を修正。 「3. 1. 2 名前の意味に関する要件」にて、クライアント証明書の commonName はアルファベット表記であることを追記、サー

			ビス証明書の commonName に含まれるサービス名に関する説明を追記。 「３．１．２ 名前の意味に関する要件」の「表 3-1 証明書で使用する属性」にて、クライアント証明書の commonName の設定値を「ユーザ名と HPCI-ID」から「ユーザ識別名」、「[ユーザ姓名（ヘボン式ローマ字）HPCI-ID]」から「[ユーザ姓名 HPCI-ID]」に修正、ホスト証明書の commonName の設定値を「ホスト名」から「ホスト識別名」に修正、サービス証明書の commonName の設定値を「サービス名」から「サービス識別名」に修正。 「３．２．３ 利用者の確認 (2)」にて、ホスト管理者及びサービス管理者の識別方法の記載内容見直し。 「３．３．２ 失効後の鍵更新時の識別と認証」「３．４ 失効申請時の識別と認証」にて、Shibboleth 認証でのアクセスも許容することを追記。 「４．１．２ 申請及び責任 (2)」にて、提出する対象から写真付き身分証を削除。 「４．２．３ 証明書申請の処理時間」にて、証明書申請の処理時間の記載を修正。 「４．７．２ 証明書の更新申請を行う者」にて、オンラインでの証明書発行申請について追記。 「４．９．１ 失効事由 (1)」にて、失効事由として所属組織の変更を追加。 「５．１．１ 設備の所在と構造」にて、HPCI 認証局の所在を掲示しない旨の記述を削除。 「５．１．２ 物理的アクセス」「５．２．２ 業務ごとに必要とされる人数」にて、入室とサーバ管理に必要な人数を修正。 「５．２．１ 信頼すべき役割」にて HPCI 認証局の運用体制リストは、年に一回の頻度で更新を行う旨記載。 「５．２．１ 信頼すべき役割」にて HPCI-ID 管理機関の運用体制リストは、年に一回の頻度で確認を行う旨記載。 「５．２．１ 信頼すべき役割」にて、ラック物理鍵の管理者を変更。 「５．５．２ アーカイブデータの保管期間」にて HPCI-ID 管理機関において保管する「証明書利用者からの各種申請書、写真付き身分証のコピーと審査結果等の記録」の保管期間の見直し 「５．７．２ ハードウェア、ソフトウェア又はデータ破壊からの復旧手続き」にて HSM 装置リカバリ訓練について追記。 「６．１．５ アルゴリズムと鍵長」にて RSA 2048bit の鍵強度は、112 ビットセキュリティに相当する旨記載。 「６．２．４ 秘密鍵のバックアップ CA 秘密

			鍵」にて、PIN 番号（パスワード）はオフライン媒体に保管することを追記。 「6．2．9 秘密鍵非活性化の方法」にて、ユーザ秘密鍵の非活性化について追記。 「6．7 ネットワークセキュリティ管理」にて、暗号強度は 112 ビットセキュリティ以上である旨記載。 「7． 証明書、CRL のプロファイル」にて、RFC6818 に準拠していることを追記。 「8．3 監査人と被監査人の関係」にて外部監査実施時、被監査人である HPCI 認証局は、監査人である政府組織や学術機関からの要求に応じ監査ログを提示する旨記載。 「9．3 業務情報の秘密性」「9．4 個人情報の保護」にて、規程を定める主体を修正。 「9．4 個人情報の保護」にて、リンクを修正。 「9．6．1 HPCI 認証局の義務と責任」にて、証明書利用者及び組織の識別と認証に関する業務は HPCI-ID 管理機関に委任する記載に修正。運用要件を規定することを削除し、要件を担保しているか定期的に検証することを記載。 「9．6．3 利用者の義務と責任」に利用者の義務と責任を追加 「9．9 補償」にて、誤字を修正。
2021.10.28	9.0	1.3.6.1.4.1.32264.2.1.18	「1．5．2 連絡先」にて電話番号を削除 「4．6 鍵更新を伴わない証明書更新」にて CA 証明書においては条件付きで CA 証明書の有効期限の延長を可能にする方針に変更 「4．7．1 証明書更新が行われる場合」にて「証明書の有効期限が満了する場合」の参照先として、「6．3．2 証明書の運用上の期間及び鍵ペアの使用期間」を追記 「4．8 証明書の変更」にて「4．6 鍵更新を伴わない証明書更新」で定める条件を満たす場合、CA 証明書の有効期間を延長することができる方針に変更 「5．6 鍵の更新」にて CA 秘密鍵の更新タイミングの明確化 「6．3．2 証明書の運用上の期間及び鍵ペアの使用期間」にて CA 証明書の有効期間の上限を 10 年から 20 年に修正
2024.01.25	9.1	1.3.6.1.4.1.32264.2.1.19	各見出しのフォントを調整 「6．3．1．1 公開鍵のアーカイブ」を「6．3．1 公開鍵のアーカイブ」へ修正

目次

1. はじめに

「HPCI 認証局運用規程」（以下、「本 CP/CPS」という。）は、HPCI 認証局の運用に関する規程である。なお、HPCI とは、革新的ハイパフォーマンス・コンピューティング・インフラ（High Performance Computing Infrastructure）の略であり、日本の分散型スーパーコンピューティング・インフラである。

本 CP/CPS は、IETF (Internet Engineering Task Force)の PKIX (Public-Key Infrastructure Working Group)が提唱する、RFC (Request For Comments) 3647 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠する。

HPCI 認証局の CP（証明書ポリシー）は、本 CP/CPS に包含し規定する。

1．1 概要

本 CP/CPS は、HPCI 認証局が行う証明書の発行、失効及びその他の運用管理等に関する認証業務の諸手続きについて記述している。

HPCI 認証局は、以下の証明書を発行する。証明書の発行対象は、HPCI コンソーシアムが定める利用規程（以下、「利用規程」という。）に定める利用資格を持つ者とする。

- HPCI 並びにそれと連携する計算・ストレージ資源の利用者を認証するためのクライアント証明書
- 計算環境及びストレージ環境を利用するために必要なホスト証明書、サービス証明書
- OCSP レスポンス署名用として OCSP レスポンダ証明書

1．2 文書の名前と定義

HPCI 認証局は、本 CP/CPS の内容及び HPCI 認証局の証明書ポリシーを識別するためのポリシー識別子として以下を利用する。

表 1-1 OID とオブジェクト

OID	オブジェクト
1.3.6.1.4.1.32264.2	HPCI 認証局
1.3.6.1.4.1.32264.2.1.X (注)	HPCI 認証局運用規程
1.3.6.1.4.1.32264.2.2.1	HPCI 認証局証明書ポリシー

（注）X の割り当てルールは、「9．12 改訂」参照。

1．3 PKI の関係者

1．3．1 認証局

(1) CA

RA からの証明書発行要求に対し、証明書を発行する。また、RA で受け付けた失効申請に対し、該当する証明書を失効し、CRL を発行する。

1．3．2 登録局

(1) RA

証明書利用者からのオンライン証明書発行申請を受け付け、CA に証明書発行要求を行う。HPCI-ID 管理機関と連携し、HPCI アカウント IdP 運用機関により、識別及び認証された証明書利用者であることを確認する。また、証明書失効申請を受け付け CA に失効要求を行う。CA から発行された CRL を認証局リポジトリへ登録する。

(2) HPCI 運用事務局

利用者から HPCI システムの利用申請を受け、HPCI-ID を付与する。HPCI-ID とその他利用者の情報（連絡先を含む）を管理する。認証局とは別の外部機関である。

(3) HPCI アカウント IdP 運用機関
利用者受付において利用者からの証明書発行申請を受け付ける。利用者の識別及び認証を行い、許可された利用者に対し HPCI アカウントを発行する。認証局とは別の外部機関である。

(4) HPCI 連携サービス運営・作業部会
ホスト証明書またはサービス証明書を必要とする組織からのホスト管理者あるいはサービス管理者の登録・変更申請を受け付ける。ホスト管理者およびサービス管理者の識別及び認証を行い、許可されたホスト管理者あるいはサービス管理者を『HPCI 認証基盤・管理者リスト』に登録する。認証局とは別の外部機関である。

１．３．３ 証明書利用者

(1) 証明書利用者
HPCI 認証局から発行される証明書の利用者。ユーザ、ホスト管理者、サービス管理者の総称。
ユーザは、クライアント証明書を使って HPCI の資源をシングルサインオンで利用する資格を有する者であり、ユーザの代表者が申請責任者として利用者受付に証明書発行申請を行う。
ホスト管理者、サービス管理者は、HPCI 上の資源を利用するために必要なホスト、サービスの管理者であり、利用者受付にそれぞれの証明書発行申請を行う。

１．３．４ 証明書検証者

(1) 証明書検証者
HPCI 認証局を信頼し、証明書の検証を行う者を指す。

１．３．５ その他関係者

(1) HPCI 認証局ポリシー管理委員会
HPCI 認証局の運営に関する下記に示すような意思決定は、HPCI 認証局ポリシー管理委員会（以下、「HPCI PMA」という。）にて行う。

- 本 CP/CPS の決定及び承認
- CA 秘密鍵危殆化時の対応
- 災害発生等による緊急時の対応
- HPCI アカウント IdP 運用機関の組織認定
- その他、CA の運営に関する重要事項

(2) 認証局リポジトリ
本 CP/CPS、CA 証明書、CRL、OCSP レスポンダ等 HPCI 認証局が関係者に対し公開する情報を登録し、提供する。

(3) 証明書管理システム
RA と連携し、ユーザの鍵ペア生成、クライアント証明書の格納及び管理を行うシステム。

(4) 証明書発行システム
ユーザに対し証明書発行申請のインタフェースを提供する Web システム。

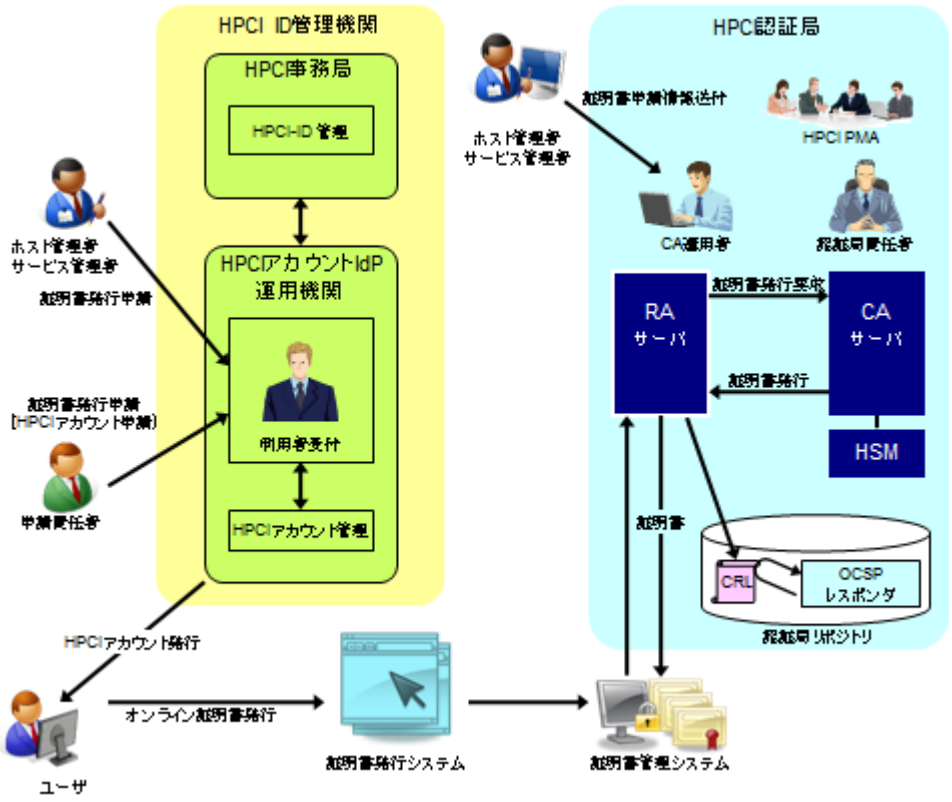

図 1-1 HPCI 認証局の構成

1．4 証明書の用途

1．4．1 証明書の用途

HPCI 認証局は、以下の証明書を発行する。

- クライアント証明書
- ホスト証明書
- サービス証明書
- OCSP レスポンダ証明書

HPCI 認証局において発行する証明書は、それぞれ以下の用途及びアプリケーションでの使用を前提とする。

表 1-2 証明書の種類と用途

種類	用途
クライアント証明書	HPCI 上の資源及びそれと連携する資源利用時のクライアント認証
ホスト証明書	HPCI 上の資源利用時のサーバ認証
サービス証明書	HPCI 上の資源利用時のサービス認証
OCSP レスポンダ証明書（注）	OCSP レスポンス署名用

（注）HPCI 認証基盤が運用するサーバのみを対象とする。

1．4．2 禁止されている証明書用途

本 CP/CPS「1．4．1 証明書の用途」に規定する以外の用途は、禁止とする。

1．5 ポリシー管理

1．5．1 管理組織

本 CP/CPS の維持管理は、HPCI PMA が行う。

1．5．2 連絡先

本 CP/CPS に関する問合せ先

担当部署	:大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 学術基盤推進部 学術基盤課
住所	:〒101-8430 東京都千代田区一ツ橋 2-1-2
メールアドレス	:hpci-ca-support@nii.ac.jp

本メールアドレスで受け付けた問い合わせについては、原則として1営業日以内に返信することを目標とする。

1．5．3 適合性の責任

規定しない。

1．5．4 CPS 承認手続き

本 CP/CPS の制定及び変更は、HPCI PMA の承認又は認証局責任者の決定をもって有効なものとする。 また、HPCI PMA が必要と判断した場合は、The Asia Pacific Grid Policy Management Authority（APGridPMA）の Member Integrated X.509 PKI Credential Services（MICS）に関する適合審査を受け、承認を得る。

1．6 定義と略称

・CA（Certification Authority）
　認証局。鍵ペア（秘密鍵と公開鍵）の所有者に対し、公開鍵証明書の発行、失効を行う。

・CP（Certificate Policy）
　証明書ポリシー。一般的なセキュリティ要件を伴った特定のコミュニティやアプリケーションに対する証明書の適用方針。

・CPS（Certification Practices Statement）
　認証局運用規程。CP で規定された方針を認証局の運用に適用するための実施手順、約款及び外部との信頼関係等を詳細に規定した文書。

・CRL（Certificate Revocation List）
　有効期限前に失効した証明書の識別リスト。CA によるデジタル署名が付与される。

・FIPS（Federal Information Processing Standard）
　米国連邦情報処理標準。FIPS140-2 は暗号モジュール評価の基準。

・HPCI（High Performance Computing Infrastructure）
　革新的ハイパフォーマンス・コンピューティング・インフラの略。本 CP/CPS では、HPCI と連携する計算・ストレージ資源や HPCI 環境として整備されるシステムを HPCI システムという。

・HPCI-ID

HPCIを利用するユーザ毎に発行されるユニークなID。所属組織が変わってもHPCI-IDは変わらない。

・HPCI アカウント
HPCI 環境にシングルサインオンするためのアカウント。ユーザは、HPCI アカウントを使用し証明書発行システム経由でオンライン証明書発行申請を行う。

・OCSP (Online Certificate Status Protocol)
証明書の失効状態を取得するための通信プロトコル。

・OID (Object Identifier)
情報を相互に区別するために、情報の意味とは無関係に割り当てられた識別子。一意に特定するためにツリー構造で管理される。

・PKCS (Public Key Cryptography Standards)
米国 RSA 研究所が提唱する、暗号アルゴリズムなどの暗号演算の周辺におけるアプリケーションのポータビリティや相互接続性を目的とした業界標準群。
PKCS#12:個人秘密情報に関する標準

・PKI (Public Key Infrastructure)
公開鍵の正当性を保証する公開鍵証明書を利用するための基盤。本人認証(本人確認)をインターネット上でより厳密(確実)に行うための基盤。

・RA (Registration Authority)
登録局。PKI システムへの利用者の登録を行う。公開鍵証明書の発行、失効申請を審査する。

・RSA (Rivest-Shamir-Adleman)
現在最も一般的な公開鍵暗号方式。十分に大きな 2 つの素数を掛け合わせた数の素因数分解が難しいことを暗号技術の基礎としている。

・所定休日
教職員の労働時間、休日及び休暇等に関する規程第 8 条第 1 項の各号に定める日。

2. 公開と認証局リポジトリの責任

2．1 認証局リポジトリ

認証局リポジトリは、次の義務及び責任を負う。

- 本 CP/CPS「2．2 証明情報の公開」で規定される情報を公開し、証明書利用者及び証明書検証者による関連情報及び CRL の検索を可能とする。
- 定期保守等による一時的な停止を除き、24 時間 365 日の安定的な運用を目標とする。
- 定期保守等により予め認証局リポジトリを停止させることが分かっている場合は、事前通知を行う。なお、緊急時等やむを得ない場合は、事前通知せずに停止することがある。
- 保管する CRL に関して要求された時点での最新の CRL であることを保証しない。
- OCSP レスポンダが提供する証明書失効情報に関して要求された時点での最新の情報であることを保証しない。
- 認証局リポジトリに登録された情報の保護を行う。

2．2 証明情報の公開

以下の情報を HPCI 認証局が運営する認証局リポジトリ上で公開する。

表 2-1 HPCI 認証局の公開情報

文書名	公開先（URL）
CA 証明書のフィンガープリント、その他 HPCI 認証局に関する情報	https://www.hpci.nii.ac.jp/ca/
HPCI 認証局 CA 証明書	https://www.hpci.nii.ac.jp/ca/hpcica.cer
CRL	http://www.hpci.nii.ac.jp/ca/hpcica_crl.der
OCSP レスポンダ	http://ocsp.hpci.nii.ac.jp
CP/CPS	https://www.hpci.nii.ac.jp/ca/hpcicacps.pdf

なお、HPCI システムの各種申請手続き及び利用規程等については、HPCI コンソーシアムの公開情報に従う。

2．3 公開の時期又は頻度

情報の公開頻度は、次のとおりとする。

- CA 証明書及び CA 証明書のフィンガープリントは、CA 証明書発行の都度、認証局リポジトリにて公開される。
- CRL は、CRL 発行（証明書失効）の都度及び本 CP/CPS「4．9．7 CRL 発行周期」に規定する定期的な更新処理により認証局リポジトリにて公開される。
- 本 CP/CPS 及びその他 HPCI 認証局に関する情報は、更新の都度、認証局リポジトリにて公開される。

2．4 認証局リポジトリに対するアクセス管理

本 CP/CPS「2．2 証明情報の公開」に規定する公開情報は、参照の制限を行わない。
情報の更新については、HPCI 認証局の権限のある者のみが行えるようアクセス制限を行う。

3. 識別及び認証

3．1 名前

3．1．1 名前の種類

HPCI 認証局が発行する証明書の識別名は、X.500 識別名(DN：Distinguished Name)の形式に従い指定する。

3．1．2 名前の意味に関する要件

HPCI 認証局が発行する証明書において、名前として使用される属性を表 3-1 に示す。

表 3-1 証明書で使用する属性

使用する属性	内容	設定値
commonName	ユーザ識別名 （クライアント証明書）	[ユーザ姓名 HPCI-ID]
	ホスト識別名 （ホスト証明書）	[FQDN]
	サービス識別名 （サービス証明書）	[サービス名/FQDN]
organizationalUnitName	組織単位名	HPCI（固定）
organizationName	組織名	NII （固定）
countryName	国名	JP （固定）

クライアント証明書における commonName はアルファベット表記で、少なくとも姓および名をそれぞれ完全な形で含むものとする。クライアント証明書の commonName は、証明書発行システムが、HPCI アカウント IdP 運用機関から SAML アサーションにて受信する属性をもとに、HPCI 運用事務局へ問い合わせて HPCI-ID と英字氏名を取得し、設定する。
サービス証明書の commonName は、ミドルウェアの動作要件でサービス名が必要なもの以外は FQDN のみとする。

3．1．3 利用者の匿名、仮名についての要件

規定しない。

3．1．4 種々の名前形式を解釈するためのルール

使用する識別名は、表 3-1 で定める規則に従う。

3．1．5 名前の一意性

クライアント証明書は、ユーザに対し一意に付与される HPCI-ID を識別名に含む。また、RA において、重複している識別名が存在しないか確認を行うことにより、名前の一意性を保証する。

3．1．6 商標の認識、認証及び役割

規定しない。

3．2 初期登録時の識別

クライアント証明書、ホスト証明書及びサービス証明書を新規に発行する際の確認方法について規定する。

３．２．１ 秘密鍵の所有を検証する方法

(1) クライアント証明書
クライアント証明書の秘密鍵は、証明書管理システム内において作成するため、ユーザは秘密鍵を保持しない。

(2) ホスト証明書、サービス証明書
HPCI 認証局は、証明書発行要求（CSR）の署名の検証を行い、含まれている公開鍵に対応する秘密鍵で署名されていることにより秘密鍵の所有を確認する。

３．２．２ 組織の確認

証明書利用者の所属組織の実在性確認は、HPCI 運用事務局が HPCI システムの利用申請手続において実施する。

３．２．３ 利用者の確認

(1) ユーザの確認

ユーザの識別は、HPCI-ID 管理機関の利用者受付が申請者責任者と物理的に対面して、もしくはテレビ会議を通じて遠隔で行う。

- 物理的に対面して行う場合
  申請責任者は、申請するユーザのリストと写真付き身分証のコピーを利用者受付へ対面にて提示する。
  利用者受付は、申請責任者の写真付き身分証に問題がないことを対面にて確認した上で、提示されたユーザのリストに記載の氏名と写真付き身分証のコピーに記載の氏名が一致しているかを確認する。またユーザの HPCI-ID に登録の所属組織と写真付き身分証明書のコピーに記載の発行元が一致しているかを確認する。確認を行った申請責任者の写真付き身分証はコピーを取り保管する。

- テレビ会議を通じて遠隔で行う場合
  利用者受付と申請責任者は別途定める『テレビ会議システムのライブビューによる遠隔での本人確認の実施手順』に従う。
  利用者受付は、テレビ会議を通じてユーザの識別を遠隔で行った際の申請責任者の顔と写真付き身分証が同時に写った画像を保管するものとする。

いずれの方法の場合も、申請責任者以外のユーザの写真付き身分証に問題がないことは、申請責任者が確認済みであることを前提とする。ユーザの身分証に写真が掲載されていない場合は、申請責任者については利用者受付が、申請責任者以外のユーザについては申請責任者が、それぞれユーザの写真付き公文書等を確認することにより、当該身分証を写真付き身分証と同等に扱う。

(2) ホスト管理者、サービス管理者の確認

ホスト管理者およびサービス管理者の識別は HPCI 連携サービス運営・作業部会が行う。ホスト証明書またはサービス証明書を必要とする組織は、申請元の組織内で身分を認められた者をホスト管理者あるいはサービス管理者として登録することを HPCI 連携サービス運営・作業部会に申請する。HPCI 連携サービス運営・作業部会は申請を確認した上で、ホスト管理者あるいはサービス管理者として登録することを承認し、ホスト管理者あるいはサービス管理者を『HPCI 認証基盤・管理者リスト』に掲載する。
HPCI 認証局は、ホスト証明書またはサービス証明書の発行申請方法に応じて申請者の認証を行う。

(A)オンライン申請
証明書発行システムを利用して発行申請する場合、申請者の認証は、HPCI アカウントに

よって行われるものとする。加えて、システムは、ホスト管理者またはサービス管理者であることを示す属性によってサービス利用を認可する。

(B)メール申請

メールによる発行申請の場合、HPCI 認証局は受信したメールの申請者情報を『HPCI 認証基盤・管理者リスト』と照合して一致することを確認した後、申請内容に不備がなければ『HPCI 認証基盤・管理者リスト』に登録の「ホスト証明書管理者電話番号」宛てに架電してホスト管理者およびサービス管理者の認証を行う。

3．2．4 審査対象としない利用者情報

氏名、所属のみを利用し、その他の情報については審査に利用しない。

3．2．5 権限の正当性確認

HPCI-ID 管理機関は、HPCI 運用事務局の管理する情報により、ユーザが利用資格を有しているかを確認する。

3．2．6 相互運用性基準

規定しない。

3．3 鍵更新申請時の識別と認証

クライアント証明書、ホスト証明書及びサービス証明書を更新もしくは再発行する際の確認方法について規定する。

3．3．1 鍵の定期更新時の識別と認証

HPCI 認証局は、証明書利用者が HPCI-ID 管理機関より証明書更新を許可されていることを、有効な HPCI アカウントを保持していることをもって確認する。
なお、HPCI アカウント更新時の識別と認証は、HPCI-ID 管理機関において以下を確認した場合に限り、利用者受付での対面による本人確認を省略可能とする。

- 前回の本人確認を行った証明書申請から 5 年以内であること
- 証明書利用者の所属組織、証明書記載事項(subject)に変更が無いこと
- HPCI アカウントが継続されること

HPCI-ID 管理機関において上記に該当しないことを確認した場合は、本 CP/CPS「3．2．2 組織の確認」及び「3．2．3 利用者の確認」において定める手続きに従う。

3．3．2 失効後の鍵更新時の識別と認証

失効後の再発行時の識別と認証は、本 CP/CPS「3．2．2 組織の確認」及び「3．2．3 利用者の確認」において定める手続きに従う。
なお、HPCI アカウントで証明書発行システムにログインし、証明書再発行申請に必要な情報の入力を行った場合は、上記の手続きに代えるものとする。

3．4 失効申請時の識別と認証

証明書の失効申請時における識別と認証は、本 CP/CPS「3．2．2 組織の確認」及び「3．2．3 利用者の確認」において定める手続きに基づいて行う。
証明書の失効申請は、申請責任者が書面で行うが、緊急を要する場合は、利用者本人からの対面又はメールによる失効申請も受け付ける。対面の場合は、本人を示す写真付き身分証により本人を確認する。メールの場合は、HPCI 運用事務局に登録済みのメールアドレスからの申請であることを確認する。
また、その他の者であっても、クライアント証明書、ホスト証明書及びサービス証明書に対応する秘

密鍵が漏洩、又は利用している暗号アルゴリズムが危殆化したことが説明され、その妥当性が確認できた場合は、失効申請を受け付ける。
なお、HPCI アカウントで証明書発行システムにログインし、証明書失効申請に必要な情報の入力を行った場合は、上記の手続きに代えるものとする。

4. 証明書のライフサイクルに対する運用上の要件

クライアント証明書、ホスト証明書及びサービス証明書の運用要件について、以下に定める。

4．1 証明書申請

クライアント証明書の申請は、HPCI システム利用の為の HPCI アカウント発行申請に含まれる。
HPCI アカウント発行申請により、証明書の発行申請も行われたものとする。
ホスト証明書、サービス証明書の申請は、HPCI 認証局が定める発行申請書により申請を行うものとする。

4．1．1 証明書申請を提出することができる者

HPCI-ID 管理機関への証明書発行申請は、申請責任者、ホスト管理者及びサービス管理者が行う。
HPCI 認証局に対するオンライン証明書発行申請は、ユーザ、ホスト管理者及びサービス管理者が行うものとする。

4．1．2 申請及び責任

(1) クライアント証明書
ユーザは、写真付き身分証のコピーを申請責任者へ提出する。申請責任者は、提出された写真付き身分証の正当性を確認し、HPCI-ID 管理機関の利用者受付へ提出する。申請責任者は、HPCI-ID 管理機関に対し、正確な情報を提示しなければならない。

(2) ホスト証明書、サービス証明書
ホスト管理者及びサービス管理者は、ホスト名及びサービス名等を HPCI-ID 管理機関の利用者受付へ提出する。ホスト管理者及びサービス管理者は、HPCI-ID 管理機関に対し、正確な情報を提示しなければならない。

4．2 証明書申請の手続き

4．2．1 識別及び認証の実施

HPCI 運用事務局及び HPCI アカウント IdP 運用機関は、本 CP/CPS「3．2．2 組織の確認」及び「3．2．3 利用者の確認」による審査を行う。
HPCI 認証局は、証明書利用者が HPCI-ID 管理機関における審査を受け、証明書発行を許可されていることを確認する。

4．2．2 申請の承認及び却下

HPCI-ID 管理機関は、申請責任者、ホスト管理者及びサービス管理者の申請内容に問題がないと判断した場合、申請を受理する。
HPCI 認証局は、HPCI-ID 管理機関における審査内容に問題がないと判断した場合、証明書利用者からのオンライン証明書発行処理を受理する。

4．2．3 証明書申請の処理時間

(1) クライアント証明書
HPCI 証明書発行システムは、申請を受理したと同時にクライアント証明書の発行申請に対応する。

(2) ホスト証明書、サービス証明書
HPCI 認証局は、申請を受理した日の翌日から起算して 5 日以内（当該期間内に所定休日があるときは、その日数を加算した期間）に、ホスト証明書及びサービス証明書の発行申請に対応する。

４．３ 証明書発行

４．３．１ 証明書の発行処理

(1)　クライアント証明書
ユーザは、HPCI アカウントを使用し、証明書発行システムから証明書申請情報の入力を行う。証明書発行システムからユーザの認証情報が証明書管理システムへ送られ、証明書管理システム内で該当するユーザの鍵ペアを生成する。証明書管理システムから RA サーバへ証明書発行申請を送付する。RA サーバは、CA サーバへ証明書発行要求を行い、CA サーバにおいてクライアント証明書が生成される。
HPCI 認証局から発行されたクライアント証明書は、証明書管理システムに格納される。

(2)　ホスト証明書、サービス証明書
ホスト管理者及びサービス管理者は、それぞれのサーバ上で鍵ペアを生成し、HPCI 認証局へ証明書発行要求（CSR）を送付する。HPCI 認証局は、CSR 受領後、本 CP/CPS「３．２．１ 秘密鍵の所有を検証する方法」に従い検証を行い、ホスト証明書及びサービス証明書を発行する。
HPCI 認証局から発行されたホスト証明書及びサービス証明書は、ホスト管理者及びサービス管理者へオンラインにて送付される。

４．３．２ 利用者への通知

(1)　クライアント証明書
クライアント証明書発行後、HPCI-ID 管理機関において管理しているユーザのメールアドレスを利用し、証明書管理システムからユーザへ発行通知を行う。

(2)　ホスト証明書、サービス証明書
HPCI 認証局からのホスト証明書及びサービス証明書の送付をもって、ホスト管理者及びサービス管理者への通知とする。

４．４ 証明書受領

４．４．１ 証明書受領確認

(1)　クライアント証明書
ユーザが証明書管理システムからクライアント証明書をダウンロードすることにより、受領とする。ダウンロードしない場合は、クライアント証明書が証明書管理システム内へ格納された時点でユーザが受領したとみなす。

(2)　ホスト証明書、サービス証明書
ホスト証明書及びサービス証明書入手後、ホスト管理者及びサービス管理者が端末に表示される証明書内容を確認することにより受領とする。

４．４．２ 認証局による証明書の公開

クライアント証明書、ホスト証明書及びサービス証明書は、公開しない。

４．４．３ 他の関係者への発行通知

規定しない。

４．５ 鍵ペアと証明書の用途

４．５．１ 利用者の秘密鍵と証明書の使用

本 CP/CPS「１．４．１ 証明書の用途」に規定する用途において使用する。

４．５．２ 検証者による利用者の公開鍵と証明書の利用

本 CP/CPS「1．４．１ 証明書の用途」に規定する用途において使用する。

４．６ 鍵更新を伴わない証明書更新

HPCI 認証局では、CA 証明書については下記の全ての条件を満たす場合にのみ、鍵更新を伴わない証明書更新を許容する。

- CA 証明書が失効していないこと
- 「6．３．２ 証明書の運用上の期間及び鍵ペアの使用期間」で定める CA 証明書の最長有効期間を超えないこと
- 「５．６ 鍵の更新」で定める新たな CA 秘密鍵の生成のタイミングが到来していないこと

CA 証明書以外の証明書の更新は必ず鍵ペアの更新を伴うこととし、鍵更新を伴わない証明書更新は行わない。

４．７ 鍵更新を伴う証明書更新

４．７．１ 証明書更新が行われる場合

以下の場合に証明書更新を行う。

- 証明書の有効期限が満了する場合（「6．３．２ 証明書の運用上の期間及び鍵ペアの使用期間」参照）
- 利用者秘密鍵の危殆化や証明書記載事項変更等による証明書失効後に再発行を行う場合

４．７．２ 証明書の更新申請を行う者

申請責任者、ホスト管理者及びサービス管理者は、HPCI-ID 管理機関に対し証明書の更新申請を行う。
HPCI 認証局に対するオンライン証明書発行申請は、ユーザ、ホスト管理者及びサービス管理者が行うものとする。

４．７．３ 証明書更新申請の処理

⑴ 証明書の有効期間が満了する場合

クライアント証明書、ホスト証明書及びサービス証明書の更新処理は、本 CP/CPS「４．１ 証明書申請～４．４ 証明書受領」と同様の手順で行う。ただし、「４．２．１ 識別及び認証の実施」については、「３．３．１ 鍵の定期更新時の識別と認証」に従う。
更新申請は、有効期限切れの１ヶ月前から可能とする。

⑵ 証明書失効後に再発行を行う場合

失効後の再発行申請は、本 CP/CPS「４．１ 証明書申請～４．４ 証明書受領」と同様の手順で行う。

４．７．４ 利用者に対する証明書更新の通知

本 CP/CPS「４．３．２ 利用者への通知」に従う。

４．７．５ 更新された証明書の受領確認

本 CP/CPS「４．４．１ 証明書受領確認」に従う。

４．７．６ 認証局による更新された証明書の公開

本 CP/CPS「４．４．２ 認証局による証明書の公開」に従う。

４．７．７ 他の関係者への証明書発行通知

本 CP/CPS「４．４．３ 他の関係者への発行通知」に従う。

４．８ 証明書の変更

HPCI 認証局では、「４．６ 鍵更新を伴わない証明書更新」で定める条件を満たす場合、CA 証明書の有効期間を延長することができる。

４．９ 証明書の失効と一時保留

４．９．１ 失効事由

HPCI 認証局は、以下の事由が発生した場合、証明書の失効を行う。

(1) 証明書利用者による失効事由
- 証明書記載内容（氏名等）、所属組織の変更
- 証明書利用者の秘密鍵危殆化もしくは危殆化の疑いがある場合

(2) HPCI-ID 管理機関による失効事由
- 証明書利用者の実在性が確認できなくなった場合
- 利用資格喪失

(3) HPCI 認証局による失効事由
- 証明書利用者が本 CP/CPS もしくは利用規程に定める事項に違反した場合
- 証明書管理システム内で管理する利用者の秘密鍵の危殆化もしくは危殆化の疑いがある場合
- HPCI 認証局において証明書の誤発行が判明した場合
- HPCI 認証局が失効を必要と判断するその他の状況が認められた場合（ただしこの場合、HPCI PMA から承認を得ることとする）
- HPCI 認証局の CA 秘密鍵の危殆化もしくは危殆化の疑いがある場合
- HPCI 認証局の認証業務を終了する場合

４．９．２ 失効申請者

(1) 証明書利用者による失効事由が発生した場合
申請責任者、ホスト管理者及びサービス管理者が HPCI-ID 管理機関の利用者受付に対し、失効申請を行う。緊急の場合は、HPCI 認証局の判断によりユーザからも失効申請を受け付ける。

(2) HPCI-ID 管理機関による失効事由が発生した場合
HPCI 運用事務局が HPCI 認証局に対し、失効申請を行う。

(3) HPCI 認証局による失効事由が発生した場合
認証局責任者又は HPCI PMA の判断により、失効を行う。

４．９．３ 失効申請の手続き

(1) 証明書利用者による失効
- クライアント証明書

ユーザは、失効事由が発生した場合、できる限り速やかに、失効申請書に必要な事項を記入後、申請責任者へ提出する。申請責任者は、ユーザの本人性及び失効事由の妥当性を確認し、利用者受付へ失効申請書を提出する。緊急を要する場合は、ユーザ本人が、利用者受付へ失効申請

書を対面又はメールで提出する。
　利用者受付は、申請責任者又はユーザに対し、本 CP/CPS「3．4 失効申請時の識別と認証」による審査を行う。
　利用者受付は、HPCI 認証局に対し失効申請書を送付し、該当証明書の失効を依頼する。
なお、HPCI アカウントで証明書発行システムにログインし、証明書失効申請に必要な情報の入力を行った場合は、上記の手続きに代えるものとする。

・　ホスト証明書、サービス証明書

　ホスト管理者及びサービス管理者は、失効事由が発生した場合、できる限り速やかに、失効申請書に必要な事項を記入後、利用者受付へ提出する。
　利用者受付は、ホスト管理者及びサービス管理者に対し、本 CP/CPS「3．4 失効申請時の識別と認証」による審査を行う。
　利用者受付は、HPCI 認証局に対し失効申請書を送付し、該当証明書の失効を依頼する。

(2)　HPCI-ID 管理機関による失効手続き
本 CP/CPS「4．9．1 失効事由」に示す事由が生じた場合、HPCI 運用事務局は、HPCI 認証局へ失効申請書又は同等の内容を紙媒体又は電子媒体で送付し、該当証明書の失効を依頼する。

(3)　HPCI 認証局による失効手続き
本 CP/CPS「4．9．1 失効事由」に示す事由が生じた場合、認証局責任者又は HPCI PMA の判断により、該当証明書を失効する。

HPCI 認証局は、失効処理完了後、証明書利用者に対して、失効完了を通知する。ただし、失効完了の通知は、必要に応じて HPCI-ID 管理機関に対しても行う。

4．9．4 失効要求までの猶予期間

証明書利用者、HPCI-ID 管理機関及び HPCI 認証局は、失効事由が発生した場合、できる限り速やかに HPCI 認証局に対し、失効要求を行なわなければならない。

4．9．5 認証局が失効処理を行うまでの時間

HPCI 認証局は、失効要求が発生した場合、速やかに失効可否を判断する。HPCI 認証局は、失効が承認された場合、所定休日を除き 1 日以内に速やかに失効処理を行う。

4．9．6 検証者に対する失効情報の要件

証明書検証者は、認証局リポジトリに公開された最新の CRL を取得、又は OCSP レスポンダに照会することにより、証明書の有効性を確認する。

4．9．7 CRL 発行周期

HPCI 認証局は、失効処理の都度及び定期的に CRL を発行する。
CRL の有効期間は 30 日とし、遅くとも期限が切れる 7 日前までに新たな CRL を発行するものとする。
なお、通常時運用においては、24 時間毎に CRL を発行する。

4．9．8 CRL 公開の最大遅延時間

CA からの CRL 発行後、認証局リポジトリにおいて公開するまでの最大遅延は、12 時間とする。

4．9．9 オンラインでの失効/ステータス（OCSP）確認の適用性

HPCI 認証局は、OCSP による証明書有効性情報の提供を行う。また、有効期間の満了した証明書の有効性確認についての問合せには応じない。

４．９．１０ オンラインでの失効/ステータス（OCSP）確認を行うための要件

規定しない。

４．９．１１ その他の利用可能な失効通知手段

規定しない。

４．９．１２ 鍵更新の危殆化の特別な要件

規定しない。

４．９．１３ 証明書の一時保留

HPCI 認証局は、証明書の一時保留を行わない。

４．９．１４ 証明書の一時保留の申請者

規定しない。

４．９．１５ 一時保留申請の手続き

規定しない。

４．９．１６ 証明書の一時保留期間

規定しない。

４．１０ 証明書ステータスサービス

４．１０．１ 証明書ステータスサービスの内容

HPCI 認証局は、CRL 及び OCSP レスポンダを認証局リポジトリ上で公開することにより、証明書の失効情報を提供する。

４．１０．２ サービスの利用時間

本 CP/CPS「２．３ 公開の時期又は頻度」に従う。

４．１０．３ その他の特徴

規定しない。

４．１１ サービスからの脱退

証明書利用者が証明書の利用を終了する場合、本 CP/CPS「４．９．３ 失効申請の手続き」に従う。

４．１２ キーエスクロー（鍵預託）とリカバリ

HPCI 認証局は、鍵預託を行わない。

5. 設備上、運営上、運用上の管理

5．1 物理的セキュリティ管理

5．1．1 設備の所在と構造

HPCI 認証局の施設は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための安全対策を考慮する。 また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。
CA 等機器は、専用のラック内に設置し、専用ラックには転倒防止措置を講じる。

5．1．2 物理的アクセス

HPCI 認証局を設置するマシン室への入室は、予め認証システムにおいて、入室権限者を登録する必要がある。入室の度に、入室権限者が認証装置による認証、識別操作を行うことが必要である。
マシン室への入退室の情報は、記録、管理される。入退室に関するログは、定期的にチェックする。
入室権限を有しない者がマシン室に入室する場合は、入室権限を有する者の同行が必要である。
入室権限を持たない者の入室時は、入室目的を確認する。また、入室権限を有し同行した職員は、同行の記録を残し、これを定期的にチェックする。
マシン室からの退室の際には、入室者数と同人数の退室を確認する。
CA 等機器は、マシン室内に専用の鍵付きラックを設置し、ラック内に収容する。

5．1．3 電源設備と空調設備

CA 等機器には、分電盤から専用電源ケーブルを敷設し十分な容量の電源を確保する。
マシン室内には、空調設備を設置し、CA 等機器の動作環境及び要員の作業環境を適切に維持する。

5．1．4 水害対策

マシン室は、容易に水害の被害を受けない場所に設置し、漏水警報装置を設置する。

5．1．5 火災予防及び防火対策

HPCI 認証局の施設を設置する建物は、耐火構造であり、自動火災報知機や消火設備を備える。

5．1．6 媒体保管

媒体は、適切な入退室管理が行われている室内の施錠可能な保管庫に保管する。

5．1．7 廃棄処理

秘密鍵、証明書利用者の個人情報等の重要な HPCI 認証局の情報が記録された文書及び記憶媒体を廃棄する場合は、物理的に完全に破壊するか、廃棄物よりデータを復元することを不可能にする措置を講じる。

5．1．8 オフサイトバックアップ

HPCI 認証局は、オフサイトバックアップを行わない。

５．２ 手続き的管理

５．２．１ 信頼すべき役割

HPCI 認証局の運用体制と役割を以下に示す。

表 5-1 HPCI 認証局の運用体制と役割

担当者／担当機関	主な役割
認証局責任者	・認証業務統括 ・CA 秘密鍵管理 ・国立情報学研究所が運用する認証基盤に関わるシステムの構成サーバのホスト管理者の本人確認、FQDN との関連性確認
CA 運用者	・CA 秘密鍵の活性化/非活性化 ・認証局システム（CA サーバ/RA サーバ/リポジトリ）の操作・保守管理
ログ管理者	・バックアップ媒体、ログ/アーカイブ媒体の管理 ・耐火金庫、キャビネットの物理鍵管理 ・システムログ、帳票の検査（セキュリティ監査） ・CA 等機器専用ラックの物理鍵管理
認証局ヘルプデスク	・HPCI ヘルプデスクからの証明書利用に関する問い合わせ窓口

※HPCI 認証局の運用体制リストは、年に一回の頻度で更新を行う。

HPCI-ID 管理機関の運用体制と役割を以下に示す。

表 5-2 HPCI-ID 管理機関の運用体制と役割

担当者／担当機関	主な役割
HPCI アカウント IdP 運用機関 利用者受付	・申請責任者の本人確認、ユーザの写真付き身分証の確認 ・ホスト管理者、サービス管理者の本人確認、FQDN との関連性確認 ・ユーザの利用資格確認 ・証明書利用者から提出された申請書類、審査結果等記録の保管
HPCI 運用事務局	・証明書利用者の所属組織の実在性確認、確認結果の保管 ・利用資格喪失時の HPCI 認証局への失効申請

※HPCI-ID 管理機関の運用体制リストは、年に一回の頻度で確認を行う。

5．2．2 業務ごとに必要とされる人数

本 CP/CPS「5．2．1 信頼すべき役割」で定められた役割に対し、以下の業務については、権限分離と相互牽制の観点から、必要数以上の要員を配置する。

表 5-3 認証局運用業務における必要要員数

業務	要員（必要数）
認証業務統括	認証局責任者（1 名）
CA 秘密鍵操作と管理	認証局責任者（1 名）、CA 運用者（1 名）
CA 秘密鍵の活性化/非活性化	CA 運用者（2 名）
CA サーバ、RA サーバの管理	CA 運用者（1 名）
認証局システムの保守管理	CA 運用者（1 名）
金庫等の物理鍵管理	ログ管理者（1 名）
監査ログ/アーカイブ媒体の管理	ログ管理者（1 名）
認証局ヘルプデスク	認証局ヘルプデスク（1名）

5．2．3 各役割における識別と認証

CA 運用者がシステム操作を行う際、システムは、操作員が正当な権限者であることの識別・認証を行う。

5．2．4 職務分離が必要な役割

認証局責任者、CA 運用者、ログ管理者間の兼務は不可とする。

5．3 人事的管理

5．3．1 資格、経験及び経歴に関する要件

HPCI 認証局の運用要員に関する契約要件、罰則、適性審査、配置転換等は、別途定められている人事規程に従う。

5．3．2 経歴の調査手続き

規定しない。

5．3．3 トレーニング要件

HPCI 認証局の運用を行うために必要な知識、技術及び機器等操作を習得する教育訓練を行う。

また、実施された教育訓練の履歴は保管する。

5．3．4 再トレーニング期間と要件

配置転換、業務手続の変更等に応じて、認証局責任者の判断で教育訓練を実施する。

5．3．5 役割交代の期間と順序

規定しない。

5．3．6 許可されていない行動に対する罰則

過失、故意に関わらず、本 CP/CPS において規定されたポリシー、手続き及び HPCI 認証局が定める手順に違反したと認められた場合、適切な罰則を適用する。

5．3．7 請負業者等に対する契約要件

規定しない。

5．3．8 要員へ提供される文書

HPCI 認証局の運用に必要となる本 CP/CPS に基づく運用手順書、関連する操作マニュアル等を要員の役割に応じて提供する。

5．4 監査ログ手続き

HPCI 認証局は、安全な環境を維持していくことを目的として、CA、RA 及び運用手続きにおいて発生した事象を監査ログとして記録する。

5．4．1 記録されるイベントの種類

HPCI 認証局は、以下の情報を記録する。各記録には、イベントの種類、イベント発生日時及びイベント発生元情報(システム名、運用要員名等)を含むものとする。

・CA ログ
　CA サーバへのアクセスログ
　証明書の発行/失効及び CRL の発行ログ
　エラーログ

・RA ログ
　RA サーバへのアクセスログ
　証明書の発行/失効ログ
　エラーログ

・OS のログイン/ログアウト/リブートログ
・ハードウェアセキュリティモジュール（以下、「HSM」という。）ログ
・マシン室入退出記録
・マシン室作業記録
・鍵貸し出し管理簿
・教育訓練の履歴
・HPCI-ID 管理機関の業務評価記録（チェックリスト）

5．4．2 監査ログの監査頻度

ログ管理者は、認証局責任者の指示に基づき監査ログの検証を行う。

５．４．３ 監査ログの保管期間

監査ログは、3 年間保管する。 ただし、CA ログ、HSM ログに関しては 10 年間保管する。

５．４．４ 監査ログの保護

CA、RA 及び HSM のログには、OS 機能によるアクセス制御を施す。
適切な入退室管理が行われている室内の保管庫に格納し、不正な閲覧や改ざんを防止する。

５．４．５ 監査ログのバックアップ手続き

CA 運用者は、CA 等に記録された各種ログを定期的に取得し、安全な環境で保管する。

５．４．６ 監査ログ収集システム

規定しない。

５．４．７ 記録事象の通知

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 アーカイブデータの種類

以下の情報をアーカイブデータとして保管する。書類については、変更履歴を含む各版を保管する。

（HPCI 認証局において保管）
- HPCI 認証局が発行した全ての証明書及び CRL
- 証明書利用者への通知書類
- CA 鍵に関する作業記録
- 本 CP/CPS「５．４．１ 記録されるイベントの種類」に規定する監査ログ
- 運用体制表
- 利用者へ提供する説明書類
- 本 CP/CPS、プロファイル設計書及び運用手順書
- その他、HPCI PMA の決定に係る重要書類

（HPCI-ID 管理機関において保管）
- 証明書利用者からの各種申請書、写真付き身分証のコピーと審査結果等の記録、テレビ会議を通じてユーザの識別を遠隔で行った場合の申請責任者の顔と写真付き身分証が同時に写った画像
- 業務評価記録（チェックリスト）

５．５．２ アーカイブデータの保管期間

監査ログに関しては、本 CP/CPS「５．４．３ 監査ログの保管期間」に従う。
HPCI-ID 管理機関において保管する「証明書利用者からの各種申請書、写真付き身分証のコピーと審査結果等の記録」は、下記のいずれかの条件を満たすまで保管する。
(a) HPCI アカウントが廃止され、かつ一番遅く始まった課題の開始日から 1 年が経過した場合。
(b) 前回の対面による本人確認から 5 年が経過したことに伴って、あらためて、対面による本人確認を実施する場合。
(c) 本人確認が完了してから、6 年が経過した場合。

その他アーカイブデータに関しては、3 年間保管する。

5．5．3 アーカイブデータの保護

本 CP/CPS「5．4．4 監査ログの保護」に従う。

5．5．4 アーカイブデータのバックアップ手続き

本 CP/CPS「5．4．5 監査ログのバックアップ手続き」に従う。

5．5．5 アーカイブデータに対するタイムスタンプ要件

電子データで保管するアーカイブデータについては、タイムスタンプを付与する。

5．5．6 アーカイブデータ収集システム

規定しない。

5．5．7 アーカイブデータの検証手続き

規定しない。

5．6 鍵の更新

CA 証明書の残り有効期間が利用者の証明書の有効期間の2倍よりも短くなる前に、新たな CA 秘密鍵の生成を行う。新たな CA 秘密鍵が生成された後は、新しい CA 秘密鍵を使って、証明書及び CRL の発行を行う。また、古い CA 秘密鍵では証明書の発行は行わず、CRL の発行のみを行う。

5．7 鍵の危殆化及び災害からの復旧

5．7．1 CA 秘密鍵危殆化時の復旧手続き

HPCI PMA の決定に基づき、以下の手続きを行う。

- HSM の盗難や管理鍵の紛失等により CA 秘密鍵が危殆化した場合は、関係者へ周知した上で、業務停止を行う。
- CA 秘密鍵が危殆化したと判断した場合は、その鍵を利用し HPCI 認証局の信頼性を検証するシステムが動作することがないように所定の手続きに従い、CA 証明書を含めた全ての証明書の失効を行う。
- HPCI 認証局の安全性が確認された時点で、新たな HPCI 認証局の鍵ペアを再生成し、再構築を行う。

5．7．2 ハードウェア、ソフトウェア又はデータ破壊からの復旧手続き

ハードウェア、ソフトウェア又はデータが損傷又は破壊された場合は、バックアップ用のハードウェア、ソフトウェア又はデータにより、できるだけ速やかに復旧作業を行う。特に HSM 装置に対しては、損傷又は破壊された場合を想定し、HSM のバックアップからのリカバリ手順確認を年一回実施する。

5．7．3 利用者秘密鍵の危殆化時の手続き

証明書利用者は、秘密鍵の危殆化又はその疑いがある場合、HPCI 認証局に対し、できる限り速やかに失効申請を行なわなければならない。また、HPCI 認証局内の利用者秘密鍵が危殆化又はその疑いがある場合、HPCI 認証局責任者は速やかに失効申請を行わなければならない。

5．7．4 災害後の事業継続性

CA 秘密鍵の危殆化及び危殆化の疑いがない場合、本 CP/CPS「5．7．2 ハードウェア、ソフトウェア又はデータ破壊からの復旧手続き」に従い復旧する。

５．８ 認証局の業務終了

HPCI 認証局における認証業務の終了及びそれに伴うバックアップデータ等の保管については、事前に認証局責任者により関連者に告知し、所定の業務終了手続きを行う。

6. 技術的セキュリティ管理

6．1 鍵ペア生成とインストール

6．1．1 鍵ペア生成

(1) CA 鍵
CA の鍵ペアは、認証局責任者と CA 運用者により、HSM で生成される。

(2) 利用者鍵
ユーザの鍵ペアは、ユーザからのオンライン証明書発行処理時に証明書管理システム内で生成される。
ホスト及びサービスの鍵ペアは、各ホスト及びサービス上でホスト管理者及びサービス管理者により生成される。

6．1．2 秘密鍵の配付

(1) ユーザ秘密鍵
- クライアント証明書を証明書管理システム内にのみ保管する場合
  ユーザ秘密鍵は、証明書管理システム内のみに保管され、ユーザには配付されない。

- クライアント証明書をユーザがダウンロードする場合
  ユーザ秘密鍵は、ユーザにより証明書管理システムから PKCS#12 形式にてダウンロードされる。

(2) ホスト及びサービスの秘密鍵
各ホスト及びサービス上で秘密鍵を生成するため、秘密鍵の配付は行わない。

6．1．3 CA への利用者公開鍵の送付

ユーザの公開鍵は、証明書管理システム内で生成し、RA サーバへ送付される。RA サーバから証明書発行要求として CA サーバへ送付される。
ホスト及びサービスの公開鍵は、ホスト管理者及びサービス管理者が生成し、証明書発行要求（CSR）として HPCI 認証局へ送付する。

6．1．4 検証者への CA 公開鍵の配布

CA 証明書は、認証局リポジトリに公開し配布する。

6．1．5 アルゴリズムと鍵長

生成される鍵のアルゴリズム及び鍵長は、以下の通りである。

表 6-1 使用する鍵長

種類		鍵アルゴリズムと鍵長
CA 鍵		RSA 2048bit
利用者鍵	クライアント証明書	RSA 2048bit
	ホスト証明書	RSA 2048bit
	サービス証明書	RSA 2048bit
	OCSP レスポンダ証明書	RSA 2048bit

※RSA 2048bit の鍵強度は、112 ビットセキュリティに相当する

6．1．6 公開鍵パラメータ生成及び検査

規定しない。

６．１．７ 鍵利用目的(X.509 v3 KeyUsage Field)

CA、ユーザ、ホスト及びサービスの公開鍵用途として、X.509 v3 の拡張領域を使用し、以下の内容を設定する。

表 6-2 鍵利用目的

対象	鍵利用目的
CA 証明書	keyCertSign, cRLSign
クライアント証明書	digitalSignature, keyEncipherment
ホスト証明書	digitalSignature, keyEncipherment
サービス証明書	digitalSignature, keyEncipherment
OCSP レスポンダ証明書	digitalSignature, keyEncipherment

６．２ 秘密鍵の保護及び暗号モジュール技術の管理

CA 秘密鍵とユーザ秘密鍵について規定する。ホスト及びサービスの秘密鍵については、ホスト管理者及びサービス管理者が管理する。

６．２．１ 暗号モジュールの標準及び管理

(1) CA 秘密鍵
FIPS140-2 レベル 3 相当の HSM により保護する。

(2) ユーザ秘密鍵
- クライアント証明書を証明書管理システム内にのみ保管する場合
  証明書管理システム内において暗号化し保管する。証明書管理システムは、マシン室内において、権限のある管理者又はサーバのみがアクセス可能とする。

- クライアント証明書をユーザがダウンロードする場合
  ユーザは、証明書管理システムから PKCS#12 形式でダウンロードする。ダウンロードした証明書及び鍵は、ユーザが責任をもって保護するものとする。

６．２．２ 秘密鍵の複数人制御(n out of m)

CA 秘密鍵を使用する操作は、認証局責任者と CA 運用者が実施する。

６．２．３ 秘密鍵の預託

HPCI 認証局は、秘密鍵の預託を行わない。

６．２．４ 秘密鍵のバックアップ

(1) CA 秘密鍵
認証局責任者と CA 運用者で実施する。バックアップした CA 秘密鍵は、HSM トークンに保存し耐火金庫に保管する。また、運用に必要な秘密鍵の HSM 物理キーおよび PIN 番号(パスワード)は、同じ鍵で管理できる場所に保管しない。なお、PIN 番号(パスワード)はオフライン媒体に保管すること。

(2) ユーザ秘密鍵
- クライアント証明書を証明書管理システム内にのみ保管する場合
  証明書管理システムの管理者がシステムのバックアップとして実施する。バックアップ媒体は、適切な入退室管理が行われている室内の施錠可能な保管庫に保管する。

- クライアント証明書をユーザがダウンロードする場合
  ユーザがダウンロードした証明書は、ユーザの責任の下バックアップを行い、バックアップ

媒体は安全な場所に保管する。

６．２．５ 秘密鍵のアーカイブ

秘密鍵のアーカイブは行わない。

６．２．６ 秘密鍵の暗号モジュールへの転送

(1) CA 秘密鍵
HPCI 認証局のマシン室内に設置された HSM 内で生成し、転送は行わない。

(2) ユーザ秘密鍵
- クライアント証明書を証明書管理システム内にのみ保管する場合
  証明書管理システムにおいて秘密鍵を生成、管理するため、転送は行わない。

- クライアント証明書をユーザがダウンロードする場合
  ユーザは、PKCS#12 形式でダウンロードする。

６．２．７ 暗号モジュールへの秘密鍵格納

(1) CA 秘密鍵
HSM の暗号モジュールへの登録は、鍵生成時とバックアップ媒体からのリカバリ時に行う。どちらも認証局責任者と CA 運用者で実施し、その際、少なくとも 15 文字のパスワード入力を必要とする。

(2) ユーザ秘密鍵
- クライアント証明書を証明書管理システム内にのみ保管する場合
  証明書管理システム上の暗号モジュールへの登録は、ユーザからのオンライン証明書発行処理に伴う鍵生成時に行う。鍵生成時、ユーザは 12 桁以上のパスワードを伴う認証を必要とする。

- クライアント証明書をユーザがダウンロードする場合
  証明書をダウンロード後、ユーザ端末内の暗号モジュールへ登録される。

６．２．８ 秘密鍵活性化の方法

(1) CA 秘密鍵
2 名の CA 運用者により HSM 内において活性化される。

(2) ユーザ秘密鍵
- クライアント証明書を証明書管理システム内にのみ保管する場合
  資源利用の認証時に、証明書管理システム内において、活性化される。秘密鍵の活性化は、12 桁以上のパスワードを伴う認証を必要とする。

- クライアント証明書をユーザがダウンロードする場合
  資源利用の認証時に、ユーザ端末内において活性化される。秘密鍵の活性化は、12 桁以上のパスワードを伴う認証を必要とする。

６．２．９ 秘密鍵非活性化の方法

(1) CA 秘密鍵
2 名の CA 運用者により HSM 内において非活性化される。

(2) ユーザ秘密鍵
資源利用の認証時以外は、12 桁以上のパスワードを付与するなどして非活性化すること。

６．２．１０ 秘密鍵破棄の方法

(1) CA 秘密鍵

HSM 内の CA 秘密鍵の破棄は、認証局責任者と CA 運用者が HSM を初期化することによって行う。なお、初期化不能かつ HSM を室外に持ち出す場合は、物理的に HSM を破壊する。

また、破棄する CA 秘密鍵のバックアップ媒体を室外へ持ち出す場合も、物理的に媒体を破壊する。

(2) ユーザ秘密鍵

・ クライアント証明書を証明書管理システム内にのみ保管する場合
証明書管理システム内及びバックアップ媒体内のユーザ秘密鍵の破棄は、証明書管理システムの管理者が再利用不可となるよう定められた手順に従い行う。

・ クライアント証明書をユーザがダウンロードする場合
ユーザがダウンロードした証明書、作成したバックアップ媒体については、ユーザが責任を持って破棄するものとする。

６．２．１１ 暗号モジュールの評価

CA 秘密鍵を格納する HSM は、FIPS140-2 レベル 3 相当の基準を満たす。

６．３ 鍵ペア管理に関する他の局面

６．３．１ 公開鍵のアーカイブ

公開鍵は、アーカイブデータに含まれて保管される。保管期間等については、本 CP/CPS「５．５．２ アーカイブデータの保管期間」に従う。

６．３．２ 証明書の運用上の期間及び鍵ペアの使用期間

HPCI 認証局から発行する証明書の有効期限は、以下の通りである。

表 6-3 証明書の有効期限

種類	有効期限
クライアント証明書	発行してから 395 日後
ホスト証明書	毎年 4 月 24 日
サービス証明書	毎年 4 月 24 日
OCSP レスポンダ証明書	毎年 4 月 24 日

CA 証明書の有効期間は、20 年を超えないものとする。

６．４ 秘密鍵の活性化データ

６．４．１ 活性化データの生成及び設定

(1) CA 秘密鍵

CA 秘密鍵の活性化は、パスワード及び HSM 物理鍵により行う。パスワードは、少なくとも 15 文字以上とし、CA 運用者が決定し、HSM へ入力する。

(2) ユーザ秘密鍵

ユーザ秘密鍵の活性化データは、オンライン証明書発行処理時にユーザから入力される 12 桁以上のパスワードであり、ユーザからの秘密鍵へのアクセス用パスワードとして設定される。

６．４．２ 活性化データの保護

(1) CA 秘密鍵
定められた規則により、CA 運用者が利用、変更等を行う。HSM 物理鍵は、認証局責任者が施錠可能な保管庫において保管する。

(2) ユーザ秘密鍵
ユーザが入力した活性化データは、ユーザが責任をもって保護するものとする。

６．４．３ 活性化データに関する他の局面

規定しない。

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技術要件

CA サーバは、HPCI 認証局として必要な機能のみを備えた専用機とし、本 CP/CPS において規定する業務に限定し使用する。

６．５．２ コンピュータセキュリティの評価

規定しない。

６．６ ライフサイクルセキュリティ管理

６．６．１ システム開発管理

規定しない。

６．６．２ セキュリティ管理

規定しない。

６．６．３ ライフサイクルセキュリティ管理

規定しない。

６．７ ネットワークセキュリティ管理

HPCI 認証局は、ファイアウォールにより外部ネットワークからの不正アクセスを防止する。
CA と RA サーバ間、RA と証明書管理システム間は、特定の通信ポート以外は接続を制限し、不正侵入を防止するセキュリティ対策を行う。また、CA と RA サーバ間、RA と証明書管理システム間の通信路は、全て暗号化（暗号強度は 112 ビットセキュリティ以上）される。

６．８ タイムスタンプ

HPCI 認証局は、発行する証明書及びログ等の記録に対して、正確な日付及び時刻を記録するため、タイムサーバによる時刻同期を行う。

７． 証明書、CRL のプロファイル

証明書及び CRL プロファイルは、RFC5280 と RFC6818 に準拠し、別途定める証明書/CRL プロファイル設計書に従う。なお、OCSP の関連属性は RFC6960 に準拠する。

8. 準拠性監査とその他の評価

8．1 準拠性監査の頻度又は条件

HPCI 認証局は、本 CP/CPS に準拠した運用がなされているかについて、1 年毎に内部監査を実施する。
HPCI-ID 管理機関は、HPCI 認証局から提示される評価チェックリストに従い、1 年毎に内部評価を実施し、結果を HPCI 認証局へ報告する。

8．2 監査人の識別と資格

監査は、監査業務及び認証業務に精通した者が行う。

8．3 監査人と被監査人の関係

HPCI認証局の内部監査は、HPCI認証局の要員が実施する。HPCI-ID 管理機関の内部評価は、HPCI-ID 管理機関の要員が実施する。

外部監査は、適切な管轄権をもつ政府組織や学術機関が実施できる。
外部監査実施時、被監査人である HPCI 認証局は、監査人である政府組織や学術機関からの要求に応じ監査ログを提示する。
他の信頼できる認証局や証明書検証者が外部評価を依頼した場合、依頼した当事者は評価に必要な経費を支払わなければならない。ただし、HPCI 認証局と HPCI-ID 管理機関の運用担当者とインフラの費用は除く。

8．4 監査で扱われる事項

HPCI 認証局の認証業務が、本 CP/CPS 及び運用手順書等に準拠して実施されているかを中心に監査を行う。

8．5 監査指摘事項への対応

HPCI PMA は、速やかに指摘事項への是正措置を検討し、対応方針を決定する。決定後、指摘事項への対応計画を監査人に提出し、HPCI 認証局が措置を完了するまで状況を確認する。

8．6 監査結果の開示

監査結果は、HPCI PMA 及び HPCI 認証局の運用要員に周知される。その他への監査結果の開示については、HPCI PMA にて可否を検討する。

９． 他の業務上の問題及び法的問題

９．１ 料金

HPCI コンソーシアムにおいて定める利用規程に従う。

９．２ 財務的責任

規定しない。

９．３ 業務情報の秘密性

HPCI 認証局は、秘密情報の保護及び取り扱いについて、情報・システム研究機構が定める以下の規程に従う。

情報・システム研究機構情報セキュリティポリシー
http://www.rois.ac.jp/pdf/security_policy.pdf

９．３．１ 秘密情報

本 CP/CPS「２．２ 証明情報の公開」で明示的に示される情報を除き、関連する全ての情報を秘密扱いとする。秘密情報については、第三者に開示及び漏洩しないと共に、必要な範囲を越えて使用しない。秘密扱いとする情報は、当該情報を含む書類及び記憶媒体の管理責任者を定め、安全に保管する。

９．３．２ 秘密情報対象外の情報

本 CP/CPS「２．２ 証明情報の公開」で示される情報は、秘密扱いとしない。
利用者の証明書が失効される場合、CRL に失効理由が含まれ公開される。この CRL に含まれる失効日、失効理由は秘密情報と見なさない。失効に関するその他の詳細情報は、公開しない。

９．４ 個人情報の保護

HPCI 認証局は、HPCI-ID 管理機関へ利用者から提示される個人情報を、証明書を発行及び失効するために必要な範囲を超えて使用しない。
利用者からの要求があった場合は、対面にて本人であることを確認し、以下の情報を開示する。

- HPCI-ID 管理機関及び HPCI 認証局への発行申請書類
- 証明書記載事項
- 証明書状態

その他、個人情報の取り扱いに関しては、情報・システム研究機構が定める以下の規程に従う。

- 情報・システム研究機構個人情報保護規程
  http://www.rois.ac.jp/pdf/kojinkitei.pdf

- 情報・システム研究機構 情報公開
  http://www.rois.ac.jp/open/

９．５ 知的財産権

HPCI 認証局は、発行した証明書に対し、如何なる IPR も主張しない。

９．６ 表明保証

９．６．１ HPCI 認証局の義務と責任

HPCI 認証局は、以下の義務と責任を有する。

- 本 CP/CPS に基づき証明書の発行、失効を行う。
- CA 証明書の情報及び CRL、OCSP レスポンダについて、システム保守などの理由による一時停止、緊急時やむを得ない場合の停止を除き、発行後、認証局リポジトリに登録し、公開する。
- 証明書発行に際して、適用した CP/CPS を特定する。
- 本 CP/CPS に基づく適切な認証業務を行い、発行した証明書及び CRL について、その発行した時点での信憑性に関する責任を持つ。HPCI 認証局は、これらの情報には署名を付与しているが、第三者による改ざん、(攻撃法の発見などによる)署名アルゴリズムの陳腐化があった場合、その信憑性は保証できない。
- HPCI 認証局の秘密鍵について、盗難、紛失等による危殆化がないよう、本 CP/CPS に基づき適切な認証業務を行う。
- HPCI-ID 管理機関からの連携申請を承認する。
- 証明書利用者及び組織の識別と認証に関する業務を HPCI-ID 管理機関に委任する。委任するにあたり下記の本人確認手続きの要件をすべて保証する組織を HPCI-ID 管理機関として選定する。
  (1) 写真付き身分証に基づいて行われること
  (2) 物理的に対面して、もしくはテレビ会議を通じて実施されること
- HPCI-ID 管理機関が、上の要件を満たしているかどうかを定期的に検証する。
- HPCI-ID 管理機関及び証明書管理システムとの全ての通信は暗号化し、安全かつ確実な送受信を実施する。

9.6.2 HPCI-ID 管理機関の義務と責任

HPCI-ID 管理機関は、以下の義務と責任を有する。

- 本 CP/CPS に基づき、証明書利用者からの証明書の発行、更新及び失効申請に際して、受付業務、証明書利用者及び組織の識別と認証を確実に行う。
- 証明書利用者の氏名の変更、利用資格の喪失等を速やかに検知可能とし、検知した場合は、HPCI 認証局に対し、証明書失効申請を行う。
- HPCI 認証局に対して、証明書発行システムと連携し、安全にユーザの証明書記載情報(HPCI-ID、英字氏名)の送付を行う。
- ユーザに対して、証明書の発行完了を証明書管理システムと連携して通知する。
- 各申請手続において入手した証明書利用者の情報を本 CP/CPS に定められた期間、安全に保管する。
- HPCI 認証局の運用要件を遵守するため、内部評価を定期的に実施し、結果を HPCI PMA へ報告する。
- 任意のシステムに対する HPCI-ID 管理機関での認証情報は、必ず暗号化されたネットワークで送信しなければならない。

9.6.3 利用者の義務と責任

証明書利用者は、以下の義務と責任を有する。

- HPCI-ID 管理機関及び HPCI 認証局に対する証明書発行又は失効申請を行う際、正確な情報を提示する。
- 証明書の取得は、HPCI 認証局から提供される手順書に従い実施する。
- 証明書は、本 CP/CPS で定める範囲外の利用用途に使用しない。また、有効期間を超えて使用しない。
- クライアント証明書は、共有しない。
- 秘密鍵の活性化パスワードは、利用者自身の責任において安全に管理する。
- 証明書及び秘密鍵について、盗難、紛失等による秘密鍵の危殆化がないよう管理する責任を負う。
- 秘密鍵の盗難や紛失(秘密鍵の危殆化又は危殆化のおそれが生じた場合)、証明書の利用停止等が発生した場合は、原則として1営業日以内に失効申請を行う。
- ホスト管理者及びサービス管理者は、ホスト証明書、サービス証明書について一つのネットワークエンティティに関連付ける。

・ HPCI 認証局により署名されたクライアント証明書、ホスト証明書、サービス証明書を利用者が使用する場合は、利用者は本 CP/CPS を遵守しなければならない。

９．６．４ 検証者の義務と責任

証明書検証者は、以下の義務と責任を有する。

・ 証明書検証者は、HPCI 認証局の認証局リポジトリにある CP/CPS を理解し同意する。
・ 証明書は、本 CP/CPS「４．５．２ 検証者による利用者の公開鍵と証明書の利用」に規定する用途以外に使用してはいけない。
・ 証明書検証者は、証明書の有効性について、検証対象の証明書が HPCI 認証局から発行され有効であること及び証明書が改ざんされていないことを確認する。

９．７ 無保証

HPCI 認証局は、本 CP/CPS に記載してある事項を遵守し、記載事項に適合するよう HPCI 認証局の運用を行うが、これにも関わらず発生した損害について、HPCI 認証局は一切の責任を負わないものとする。
HPCI 認証局は、証明書利用者及び証明書検証者が本 CP/CPS に記載されている事項について必要な情報を提供し、その内容を遵守することを勧奨するが、HPCI 認証局は、他の関係者に対し、証明書利用者及び証明書検証者が「９．６．３ 利用者の義務と責任」及び「９．６．４ 検証者の義務と責任」に記述されている事項を遵守することは保証しない。

９．８ 責任の制限（義務違反）

証明書利用者が「９．６．３ 利用者の義務と責任」に違反したことに起因して生じた損害及び証明書検証者が「９．６．４ 検証者の義務と責任」に違反したことに起因して生じた損害に関し、HPCI 認証局は、関係者に対し一切の責任を負わないものとする。

９．９ 補償

証明書利用者は、「９．６．３ 利用者の義務と責任」に従わず第三者に対し損害を与えた場合、補償を行う必要がある。証明書検証者は、「９．６．４ 検証者の義務と責任」に従わず第三者に対し損害を与えた場合、補償を行う必要がある。なお、紛争発生時には、紛争の当事者間において個別に紛争解決を行うものとする。

９．１０ 文書の有効期限と終了

本 CP/CPS は、HPCI 認証局が業務を終了した時点で無効となる。

９．１１ 関係者間の個別通知と連絡

規定しない。

９．１２ 改訂

９．１２．１ 改訂手続き

HPCI 認証局は、本 CP/CPS を必要に応じて変更する。変更内容については、HPCI PMA で決定し承認する。
変更した CP/CPS は、メジャーバージョン番号を更新し、新たな OID を割り振る。
なお、誤字修正等の軽微な変更については、HPCI PMA の承認は不要とし、認証局責任者の決定に基づき、変更を行う。その際、マイナーバージョン番号を更新し、新たな OID を割り振る。

９．１２．２ 通知方法と期間

本 CP/CPS を変更した場合は、速やかに認証局リポジトリにて公開する。これをもって証明書利用者及び証明書検証者への通知とする。

9．12．3 OID の変更

本 CP/CPS「9．12．1 改訂手続き」に従う。

9．13 紛争解決手続き

規定しない。

9．14 準拠法

HPCI 認証局と関係者の間で係争が生じた場合に適用される法令は、日本国内法を準拠法とする。

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

関係者の権利義務に直接影響する、本 CP/CPS 及びその他の契約、合意の規定は、本 CP/CPS が別段の定めをしている場合を除き、書面によらず口頭で修正、放棄、追加、変更、削除又は終了させることはできないものとする。

9．16．2 権利譲渡条項

本 CP/CPS 及びその他の契約、合意により規定された権利義務は、HPCI 認証局と事前の合意なく第三者に譲渡、相続することはできない。

9．16．3 分離条項

本 CP/CPS 及びその他の契約、合意の一部分の規定が、いかなる程度でも無効又は執行不可能であるとされた場合であっても、本 CP/CPS 及びその他の契約、合意のその他の規定の有効性には影響を及ぼさず、HPCI 認証局が本来意図する内容に最も合理的に合致するよう解釈されるものとする。

9．16．4 強制執行条項（弁護士費用及び権利放棄）

HPCI 認証局は、本 CP/CPS 及びその他の契約、合意により規定された権利義務が満たされていないと判断した場合又は本 CP/CPS 及び契約書に定められていない事項やこれらの文書の解釈に関して疑義が生じた場合、本 CP/CPS 及びその他の契約、合意を一方的に終了させることができるものとする。

また、証明書利用者及び証明書検証者における紛争解決のための HPCI 認証局側の弁護士費用は、証明書利用者及び証明書検証者に請求することができるものとする。

9．16．5 不可抗力条項

以下の事象が発生した場合、HPCI 認証局及び全ての関係者は、証明書利用者及び証明書検証者に対し責任を負わない。

(1) 地震、水害、噴火などのあらゆる天災に起因する損害
(2) 火災、停電などのあらゆる災害に起因する損害
(3) 戦争、動乱及びその他のあらゆる不可抗力に起因する損害

9．17 その他の条項

規定しない。