

5.3.6 認められていない行動に対する制裁

規定しない。

5.3.7 独立した契約者の要件

規定しない。

5.3.8 要員へ提供する資料

規定しない。

5.4 監査ログの取扱い

セキュリティ監査手続きは、JIS X 5080:2002 と同等以上の規格に従うものとする。
例えば、JIS X 5080:2002 の「第 8 章 通信及び運用管理」、「第 9 章 アクセス制御」、
「第 10 章 システムの開発及び保守」、「第 12 章 適合性」等がこれに相当する。

5.4.1 記録するイベントの種類

認証局は、CA システム、リポジトリシステム、認証局に関するネットワークアクセスの監査証跡やイベント・ログを手動或いは自動で取得出来る。

5.4.2 監査ログを処理する頻度

認証局は、監査ログを 3 ヶ月に 1 度以上定期的に検査する。

5.4.3 監査ログを保存する期間

監査ログは、最低 10 年間保存される。

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、オフラインの記録媒体に CPS に定める頻度でバックアップが取られ、それらの媒体はセキュアな保管場所に保管される。

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

記録は、ISO 17799:2005 と同等以上の規格に従って保管されるものとする。

例えば、ISO/IEC17799:2005 の「第 12 章 情報システムの調達、開発及び維持」、「第 15 章 適合性」等がこれに相当する。

5.5.1 アーカイブ記録の種類

認証局 は、以下の情報をアーカイブする。

- ・ 証明書の発行/取消に関する処理履歴
- ・ CRL の発行に関する処理履歴
- ・ 認証局の証明書
- ・ 加入者の証明書
- ・ 証明書申請内容の審議の確認に用いた書類
- ・ 失効の要求に関わる書類

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。

5.5.4 アーカイブのバックアップ手続

規定しない。

5.5.5 記録にタイムスタンプをつける要件

規定しない。

5.5.6 アーカイブ収集システム（内部対外部）

規定しない。

5.5.7 アーカイブ情報を入手し、検証する手続

規定しない。

5.6 鍵の切り替え

認証局は、定期的に CA 私有鍵の更新を行う。CA 私有鍵は、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（HSM）を用いて生成される。

CA 私有鍵の更新と共に自己署名証明書の更新も実施される。この更新においても CA 私有鍵生成の場合と同様に、複数人の立会いのもと執り行われる。

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

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、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、障害発生時には、可能な限り速やかに、加入者、検証者に情報公開用 Web サイト等により通知する。

5.7.3 CA 私有鍵が危殆化した場合の対処

CA 私有鍵が危殆化又はそのおそれが生じた場合は、運用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に基づき、全ての加入者証明書の失効を行い、CRL/ARL 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

認証局が運営を停止する場合には、運営の終了の 90 日前までに加入者に通知し、認証局の鍵と情報の継続的な保管を手配するものとする。

認証局が終了する場合には、当該認証局の記録の安全な保管又は廃棄を確実にするための取り決めを行うこととする。

登録局の運用を停止する場合は、事前に加入者の同意を得たうえで、登録局が有する加入者の情報と運営を他の登録局に移管し、それを加入者に通知する。

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

CA 鍵ペアは、認証設備室内に設置された専用の暗号モジュール (HSM) を用いて、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。

6.1.2 加入者への私有鍵の送付

エンドエンティティの加入者の私有鍵が認証局で生成される場合は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、加入者に引き渡されるものとする。認証局はオリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことの証明ができるものとする。

6.1.3 認証局への公開鍵の送付

エンドエンティティの加入者の公開鍵が加入者により生成される場合は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、認証局に引き渡されるものとする。

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、本ポリシーを公開する機関のサイトで公開するものとする。

6.1.5 鍵のサイズ

鍵の最小サイズは、使用されるアルゴリズムに依存する。CA 証明書の鍵の最小サイズは、RSA アルゴリズムの場合、2048 ビットとする。他のアルゴリズムを使用する CA 証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。

エンドエンティティの証明書の鍵の最小サイズは、RSA アルゴリズム又は技術的に同等のアルゴリズムの場合、1024 ビットとする。他のアルゴリズムを使用するエンドエンティティの証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。

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

認証局の鍵は、keyCertSign と cRLSign のビットを使用する。

エンドエンティティの鍵は、nonRepudiation のビットを使用する。

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 と同等以上の規格に準拠するものとする。

エンドエンティティの加入者私有鍵の格納モジュールは、US FIPS 140-2 レベル 1 と同等以上の規格に準拠するものとする。

6.2.2 私有鍵の複数人によるコントロール

CA 私有鍵の生成には、運用管理者と複数名の権限者を必要とする。また、鍵生成後の私有鍵の操作（活性化、非活性化、バックアップ、搬送、破棄等）においても複数名の権限者を必要とする。

6.2.3 私有鍵のエスクロウ

CA 私有鍵は、法律によって必要とされる場合を除き、エスクロウされないものとする。

エンドエンティティの加入者の私有鍵は、法律によって必要とされる場合を除き、エスクロウされないものとする。

6.2.4 私有鍵のバックアップ

CA 私有鍵のバックアップは、安全な方法で行う。例えば、バックアップ作業の権限を有する複数人の立会いのもとで行うようにしたり、バックアップデータとして CA 私有鍵に関する情報を暗号化したり分散させて保管するなどの方法がある。

6.2.5 私有鍵のアーカイブ

認証局は加入者の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

CA 私有鍵は、安全に格納することとする。例えば、認証設備室内にある暗号モジュール内に格納するなどの方法がある。

外部へのバックアップの転送や外部からのリストアの場合は、セキュアチャネルを通して行うものとする。

6.2.7 暗号モジュールへの私有鍵の格納

私有鍵がエンティティの暗号モジュールで生成されない場合は、IETF RFC 2510「証明書管理プロトコル」に従って、又は同様に安全な方法で、モジュールに入力されるものとする。

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 CP「6.2.2 私有鍵の複数人によるコントロール」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 CP「6.2.2 私有鍵の複数人によるコントロール」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 CP「6.2.2 私有鍵の複数人によるコントロール」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 を完全に初期化し、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。

加入者私有鍵破棄手続きは、CPS 又は加入者が入手可能な文書に記述するものとする。

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 と同等以上のものを使用する。

エンドエンティティの加入者の私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 1 と同等以上のものを使用する。

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

公開鍵は、後日の署名の検証を可能にするために、信頼できる方法でアーカイブする必要がある。認証局は、公開鍵が CPS で定める期間アーカイブされることを保証する責任があるものとする。

6.3.2 公開鍵証明書の有効期間と鍵ペアの使用期間

CA 公開鍵証明書の有効期間は 20 年を越えないものとし、その私有鍵の使用は 10 年を越えないものとする。

エンドエンティティの加入者の公開鍵証明書の有効期間は 5 年を越えないものとし、その私有鍵の使用は 2 年を越えないものとする。

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認証局で定められた規定に従い実施されるものとする。

エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、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認証局で定められた規定に従い実施され、加入者に安全に伝えられるものとする。

加入者私有鍵の活性化データを加入者が生成する場合は、活性化データは予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施されるものとする。

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、認証局で定められた規定に従い安全に保護される。

エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、活性化データが加入者に伝えられた後は、認証局においては完全に破棄し保管しないものとする。また、伝えられた活性化データは、認証局で定められた規定に従い、加入者により安全に保護するものとする。

加入者私有鍵の活性化データを加入者が生成する場合は、認証局で定められた規定に従い、加入者により安全に保護するものとする。

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

認証業務用設備に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するための対策を行うこと。

CA システムへのログイン時には、本 CP「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

ISO15408 を参考にセキュリティ基準を設ける等の対応を行い、客観的に評価を行うこと。

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ーを導入すべく、随時 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

JIS X 5080:2002「第 10 章 システムの開発及び保守」と同等以上の規格に従うものとする。

6.6.2 セキュリティ運用管理

JIS X 5080:2002「第 10 章 システムの開発及び保守」、「第 11 章 事業継続管理」と同等以上の規格に従うものとする。

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

JIS X 5080:2002 と同等以上の規格に従うものとする。

例えば、JIS X 5080:2002 の「第 8 章 通信及び運用管理 8.5 ネットワークの管理」、「第 9 章 アクセス制御 9.4 ネットワークのアクセス制御」等がこれに相当する。

6.8 タイムスタンプ

認証設備は、アプリケーション等において正確な日付・時刻を使用することとする。例えば、NTP サービスや GPS、電波時計等による時刻同期が挙げられる。

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 CP の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。

本ポリシーに従い発行される電子証明書のプロファイルは、基本領域のプロファイルを表 7.1.1 に示し、拡張領域のプロファイルを表 7.1.2 の通りとする。

なお、Issuer の DN は CPS 及びその他開示文書に記述されることとする。

7.1.1 バージョン番号

本ポリシーの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 (保健医療福祉分野の属性を含む)

本ポリシーに従い発行される電子証明書の拡張領域のプロファイルは以下の表 7.1.2 の通りとする。

subjectDirectoryAttributes 拡張で用いる保健医療福祉分野の属性 (hcRole) については 7.1.10 で定める。

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通りとする。

sha1WithRSAEncryption (1.2.840.113549.1.1.5)
sha256WithRSAEncryption (1.2.840.113549.1.1.11)
sha384WithRSAEncryption (1.2.840.113549.1.1.12)
sha512WithRSAEncryption (1.2.840.113549.1.1.13)

基本領域のsubjectPublicKeyInfoアルゴリズムは以下の通りとする。

RSASignature (1.2.840.113549.1.1.1)

7.1.4 名称の形式

Issuer と Subject の名前の形式は表 7.1.1 に示される。

7.1.5 名称制約

用いない。

7.1.6 CP オブジェクト識別子

別途規定する。

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

CPS を参照する URL を含めることができる。

7.1.9 証明書ポリシ拡張フィールドの扱い

本 CP の OID を格納する。

表 7.1.1 証明書のプロフィール (基本領域)

項目	設定	説明
Version	◎	Ver3 とする。
SerialNumber	◎	同一認証局が発行する証明書内でユニークな値とする。
Signature	◎	
Validity	◎	
NotBefore	◎	
NotAfter	◎	
Issuer	◎	英数字のみ使用する。(CountryName は Printable、それ以外は UTF-8 で記述する)
CountryName	◎	c=JP (固定) とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシーを示す文字列を記載する。 (「HPKI-01-*forNonRepudiation」とする。なお、文字列中の"01"は、本 CP の版数である"第 1.0 版"を示す。また、"*"は CA を唯一に識別できる文字列とする。)
Subject	◎	英数字のみ使用する。(CountryName は Printable、それ以外は UTF-8 で記述する)
CountryName	◎	c=JP (固定) とする。
LocalityName	△	
OrganizationName	○	加入者が医療機関等の管理者の場合は必須。 その場合は医療福祉機関名をローマ字あるいは英語名で OrganizationName に記載し、
OrganizationUnitName	○	OrganizatioUnitName に " Director" の文字列を格納する。
CommonName	◎	加入者の氏名をローマ字で記載する。
GivenName	×	
SurName	×	
e-Mail	×	
SerialNumber	△	医籍登録番号などを記載することができる。
SubjectPublicKeyInfo	◎	
Algorithm	◎	RSASignature とする。
SubjectPublicKey	◎	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	◎	拡張領域 (Extensions) 参照

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表す。

表 7.1.2 証明書のプロフィール（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
subjectKeyIdentifier	◎		FALSE
KeyUsage	◎		TRUE
DigitalSignature	×		-
NonRepudiation	◎		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		-
DeciphermentOnly	×		-
extendedKeyUsage	×		FALSE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	◎		TRUE
policyMapping	×		FALSE
subjectAltName	△		FALSE
issuerAltName	△		FALSE
subjectDirectoryAttributes	◎	医療従事者等の資格（hcRole）を記載。	FALSE
AttrType	○	加入者が国家資格保有者及び医療機関等の管理者の場合は必須。その他(患者等)の場合は省略可。	-
AttrValues	○	HCActor の codeDataFreeText に資格名テーブル表 7.1.3 の英表記を UTF8String で設定。subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定する。	-
basicConstraints	×		TRUE
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	◎	DirectoryName あるいは URI で、CRL の配布点を指定する。	FALSE
subjectInfoAccess	×		FALSE
authorityInfoAccess	△		FALSE

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表す。

7.1.10 保健医療福祉分野の属性 (hcRole)

(1) サブジェクトディレクトリ属性拡張での hcRole 属性の使用

本ポリシーでは、ISO TS 17090 で規定した hcRole 属性を下記に示すようにプロファイルして用いることにする。

subjectDirectoryAttributes の attrType には hcRole を表す OID {id-hcpki-at-healthcareactor} を設定する。

attrValue は HCActorData で、HCActor の codedData では codeValueData は用いず、codeDataFreeText を用いる。

本ポリシーでは coding scheme reference の OID として ISO coding scheme reference を用いず、本 CP の元で定めた表 7.1.3 の資格名を参照する local coding scheme reference の OID は、{ iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) hcRole(6) national-coding-scheme-reference(1) version(1) }を用いる。資格名は、表 7.1.3 に示すように英語表記を用い UTF8string で設定する。

subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定することができる。

本拡張は、加入者が国家資格保有者及び医療機関等の管理者の場合は必須、その他(患者等)の場合は省略可とする。

表 7.1.3 HPKI 資格名テーブル (codeDataFreeText の定義)

資格名 (国家資格)	説明
'Medical Doctor'	医師
'Dentist'	歯科医師
'Pharmacist'	薬剤師
'Medical Technologist'	臨床検査技師
'Radiological Technologist'	診療放射線技師
'General Nurse'	看護師
'Public Health Nurse'	保健師
'Midwife'	助産師
'Physical Therapist'	理学療法士
'Occupational Therapist'	作業療法士
'Orthoptist'	視能訓練士
'Speech Therapist'	言語聴覚士
'Dental Technician'	歯科技工士

'National Registered Dietitian'	管理栄養士
'Certified Social Worker'	社会福祉士
'Certified Care Worker'	介護福祉士
'Emergency Medical Technician'	救急救命士
'Psychiatric Social Worker'	精神保健福祉士
'Clinical Engineer'	臨床工学技師
'Masseur'	あん摩マッサージ指圧師/はり師/きゅう師
'Dental Hygienist'	歯科衛生士
'Prosthetics & Orthotic'	義肢装具士
'Artificial Limb Fitter'	柔道整復師
'Clinical Laboratory Technician'	衛生検査技師
'Care Manager'	介護支援専門員
資格名（医療機関の管理責任者）	説明
'Director of Hospital'	病院長
'Director of Clinic'	診療所院長
'Director of Pharmacy'	管理薬剤師
'Director'	その他の保健医療福祉機関の管理責任者

注) 資格名のワード間の空白は一個の Space (x20)とする。

患者に対して署名付の文書を交付することが多い病院長、診療所院長、管理薬剤師を hcRole だけで識別できるように定めている。

なお、上記 Director 4 属性を使用する場合は Subject フィールドの OrganizationName 及び OrganizationUnitName は必須で、OrganizationName に保健医療福祉機関名を英語又はローマ字で格納し、OrganizationUnitName に"Director"の文字列を格納する。