保健医療福祉分野 PKI 認証局　証明書ポリシ

平成 18 年 3 月

厚生労働省

改定履歴

版数	日付	内容	
初版	平成 17 年 4 月	初版発行	
1.1 版	平成 18 年 3 月	1.1 概要	セキュリティマネジメントに関する参照文書を JIS X 5080:2002 とした。
		3.2.3 個人の認証 ＜郵送の場合＞ 2 個人の本人性	本人性の確認が可能であるとして認証局が定める書類のうち一点について、当該書類のコピーの適当な空欄に実印を捺印して郵送することとした。
		3.2.3 個人の認証 ＜郵送の場合＞ 4 国家資格及び医療機関等の管理者権限	国家資格証明書等のコピーの郵送にあたり、当該証明書等のコピーの適当な空欄に実印を捺印し、印鑑登録証明書を添えて郵送することとしているが、本取扱を当該証明書等に本人の顔写真が貼付されていない場合に限定する旨の記述を削除した。
		4.2.1 本人性及び資格確認 ＜本人からの申請の場合＞ 2 国家資格を有する者への証明書発行 (2) 郵送の場合	国家資格免許証等のコピーの郵送にあたり、当該免許証等のコピーの適当な空欄に実印を捺印し、印鑑登録証明書を添えて郵送することとしているが、本取扱を当該免許証等に本人の顔写真が貼付されていない場合に限定する旨の記述を削除した。
		5.4.3 監査ログを保存する期間	最低 10 年間とした。
		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 年を超えないものとし、その私有鍵の使用は 10 年を越えないものとした。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した。
		7.1.3 アルゴリズムオブジェクト識別子	基本領域の Signature アルゴリズムに以下を追加した。 sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13)
		9.3.1 秘密情報の範囲	「認証局が秘密保持対象として扱う情報を開示することができる場合」に関する記述の一部を削除した。

－目次－

1 はじめに

1.1 概要

証明書ポリシ（Certificate Policy、以下 CP という）は、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。また、保健医療福祉分野 PKI は、保健医療福祉分野において情報を連携して利用するための公開鍵基盤である。

本ポリシは、保健医療福祉サービス提供者及び保健医療福祉サービス利用者への署名用公開鍵証明書を発行する「保健医療福祉分野 PKI 認証局」の証明書ポリシである。

保健医療福祉分野 PKI 認証局が発行した証明書は、個人とその公開鍵及び資格属性等が一意に関連づけられることを証明するものである。認証局が証明書を発行するにあたって、その審査過程、登録、発行及び失効方法は、CP 及び認証局により開示される文書によって規定される。

加入者及び検証者は、保健医療福祉分野 PKI 認証局によって発行された証明書を利用する時は、CP 及び認証局により開示される文書の内容を、その利用方法に照らして評価する必要がある。

本 CP に準拠する個々の「保健医療福祉分野 PKI 認証局」は、本 CP を基準にして、個々の環境に適合した認証実施規程（Certificate Practice Statement、以下 CPS という）を作成するものとする。なお、CPS が本 CP に抵触する場合は CP が優先する。

本 CP は、電子署名及び認証業務に関する法律（以下、電子署名法という）に規定された「特定認証業務の認定」を受けた認証局のみを対象としているわけではなく、認定を受けない認証局も対象としている。従って、特定認証業務の認定を受ける場合は、本 CP に従い CPS に「特定認証業務の認定」を受けるに足る詳細を規定する必要がある。

なお、本 CP は以下の文書に依存して構成される。

- IETF/RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework
- ISO/TS 17090-1:2002 Health informatics - Public key infrastructure Part 1 : Framework and overview
- ISO/TS 17090-2:2002 Health informatics - Public key infrastructure Part 2 : Certificate profile
- ISO/TS 17090-3:2002 Health informatics - Public key infrastructure Part 3 : Policy management of certification authority

また、本 CP は以下の文章を参照する。なお本 CP ではセキュリティマネジメントに関する部分は JIS X.5080:2002 を参照しているが、セキュリティマネジメント全体を考える場合は ISO 17799 :2005 も参照することが望ましい。

- ISO 17799:2005 Information technology - Code of practice for information security management
- IETF/RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
- IETF/RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP
- IETF/RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
- US FIPS140-2(Federal Information Processing Standard) : Security Requirements for Cryptographic Modules (http://csrc.nist.gov/cryptval/)
- JIS X 5080:2002 : 情報技術－情報セキュリティマネジメントの実践のための規範 (ISO/IEC17799:2000)
- 電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日　法律第 102 号）
- 電子署名及び認証業務に関する法律施行規則（平成 13 年 3 月 27 日　総務省・法務省・経済産業省令第 2 号）
- 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年 4 月 27 日　総務省・法務省・経済産業省告示第 2 号）

1.2　文書の名前と識別

本ポリシの名称を「保健医療福祉分野 PKI 認証局　証明書ポリシ」とする。本ポリシにて発行する証明書及び関連サービスに、厚生労働省より「保健医療福祉分野の公開鍵関連分野」のオブジェクト識別子（OID）を「1.2.392.100495.1」と割り当てる。その基本体系を示す。

OID の基本体系

{ iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) ca(5) A B C V }

A：証明書ポリシ　cp（1）

B：認証局の証明書種類　signature(1),　authentication(2)

C：セキュリティ保証レベル（n）　n=0, 1, 2, 3, 4　(0 はテスト用、3 は HPKI の業務用)

V：証明書ポリシのメジャーバージョン番号　v(1)

また、本 CP で定める OID を表 1.2 に示す。

表 1.2　本 CP で定める OID

名称	オブジェクト識別子
HPKI 署名用証明書ポリシ	1.2.392.100495.1.5.1.1.3.1
HPKI 認証用証明書ポリシ（予約）	1.2.392.100495.1.5.1.2.3.1
HPKI 署名テスト用証明書ポリシ	1.2.392.100495.1.5.1.1.0.1
HPKI 認証テスト用証明書ポリシ（予約）	1.2.392.100495.1.5.1.2.0.1

1.3　PKI の関係者

1.3.1　認証局

認証局（CA）は、証明書発行局（IA)と登録局（RA）により構成される。保健医療福祉分野 PKI では、認証局は複数の階層構成をとることができる。また、保健医療福祉分野 PKI の階層構成の頂点の認証局（Root CA）は、本 CP に準拠する他の保健医療福祉分野 PKI の Root CA と相互認証を行うことがある。

発行局は証明書の作成、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、認証局は認証局の運営主体で定める 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。

1.3.2　登録局

登録局は、適切な申請者の本人確認、登録の業務を行い、発行局への証明書発行要求を行う。なお、証明書登録の業務は、発行、失効を含む。

但し、登録局は認証局の運営主体で定める 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　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、証明書発行申請を行い認証局により証明書を発行される個人をさす。証明書所有者の範囲は次のとおりとする。

- 保健医療福祉分野サービスの提供者及び利用者
- 上記の提供者の内、以下の者がその有する資格において、あるいは管理者として署名を行う場合は、「その資格を有していること」あるいは「管理者であること」を証明書に記載しなくてはならない。
- 保健医療福祉分野に関わる国家資格を有する者
- 医療機関等の管理者

1.3.4 検証者

検証者とは、加入者の署名を検証する者をさす。

1.3.5 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 CP で定める加入者証明書は、次に定める利用目的にのみ使用できる。

(1) 医療従事者等の保健医療福祉分野サービス提供者の署名検証用

(2) 患者等の保健医療福祉分野サービス利用者の署名検証用

1.4.2 禁止される証明書の使用

本 CP で定める加入者証明書は、署名検証以外には用いないものとする。

1.5 ポリシ管理

1.5.1 本ポリシを管理する組織

本 CP の管理組織は、「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」(以下、「HPKI 認証局専門家会議」という) とする。

1.5.2 問い合わせ先

本 CP 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：厚生労働省　医政局　研究開発振興課　医療機器・情報室

受付時間：10 時～17 時

電話番号：03-3595-2430

FAX 番号：03-3503-0595

e-mail アドレス：hpki-cp@mhlw.go.jp

1.5.3 CPS のポリシ適合性を決定する者

CPS の本 CP への適合性を決定する者は、HPKI 認証局専門家会議とする。

1.5.4 CPS 承認手続き

本 CP は、HPKI 認証局専門家会議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、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。

・ 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