



電子署名・認証関連 用語・技術標準集 Ver.1.3



財団法人 日本情報処理開発協会

電子署名・認証センター

〒105-0011 東京都港区芝公園3丁目5番8号 機械振興会館内
TEL 03-3432-6597 FAX 03-3432-6201
URL <http://www.jipdec.jp/esac/>

発行：(財)日本情報処理開発協会 電子署名・認証センター
住所：東京都港区芝公園3-5-8 機械振興会館内
電話番号：03-3432-6597



古紙パルプ配合率100%再生紙を使用



地球環境に配慮した大豆油インキを使用

発行年月 2007年3月



電子署名・認証関連 用語・技術標準集とは

本電子署名・認証関連 用語・技術標準集は、電子署名等に関する基本的な用語、技術標準および標準化組織・機関について簡単に説明を加えてまとめたものです。

「1.電子署名関連の用語」では、電子署名に関連する法律等を読む上で整理しておくべき用語について整理するとともに、電子署名に関連する法律等の要件に満たしていると思われるデジタル署名技術の主な用語についてまとめました。

「2.デジタル署名関連の技術標準」では、デジタル署名技術に関連する標準化を進めている組織・機関について、整理しました。

さらに、付録として電子署名に関する法律等(2006年2月現在)と、電子証明書及び認証業務運用規程に関する標準化資料を掲載しました。

本資料が、これから電子署名を利用されようとしている利用者の皆さんにとって、電子署名・認証を理解するための一助になれば幸いです。

CONTENTS

■1. 電子署名関連の用語	電子署名関連の用語	3
1-1.	電子署名に関連する関係法令による用語	3
1-2.	デジタル署名関連の用語	6
■2. デジタル署名関連の技術標準		10
2-1.	IETF (Internet Engineering Task Force)	10
2-2.	ITU (International Telecommunication Union)	13
2-3.	その他デジタル署名関連の標準化機関・組織	14
■付録A. 電子署名に関連する関係法令		16
A-1.	電子署名及び認証業務に関する法律	16
A-2.	電子署名及び認証業務に関する法律施行令	27
A-3.	電子署名及び認証業務に関する法律施行規則	29
A-4.	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	40
A-5.	電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針	47
■付録B. 電子証明書及びCRLのプロファイル		54
B-1.	電子証明書のプロファイル	54
B-2.	CRLのプロファイル	55
■付録C. CPSの構成案		56

電子署名関連の用語

1-1

電子署名に関連する関係法令による用語

電子署名に関連する関係法令で用いられている用語の解釈や定義についてまとめました。

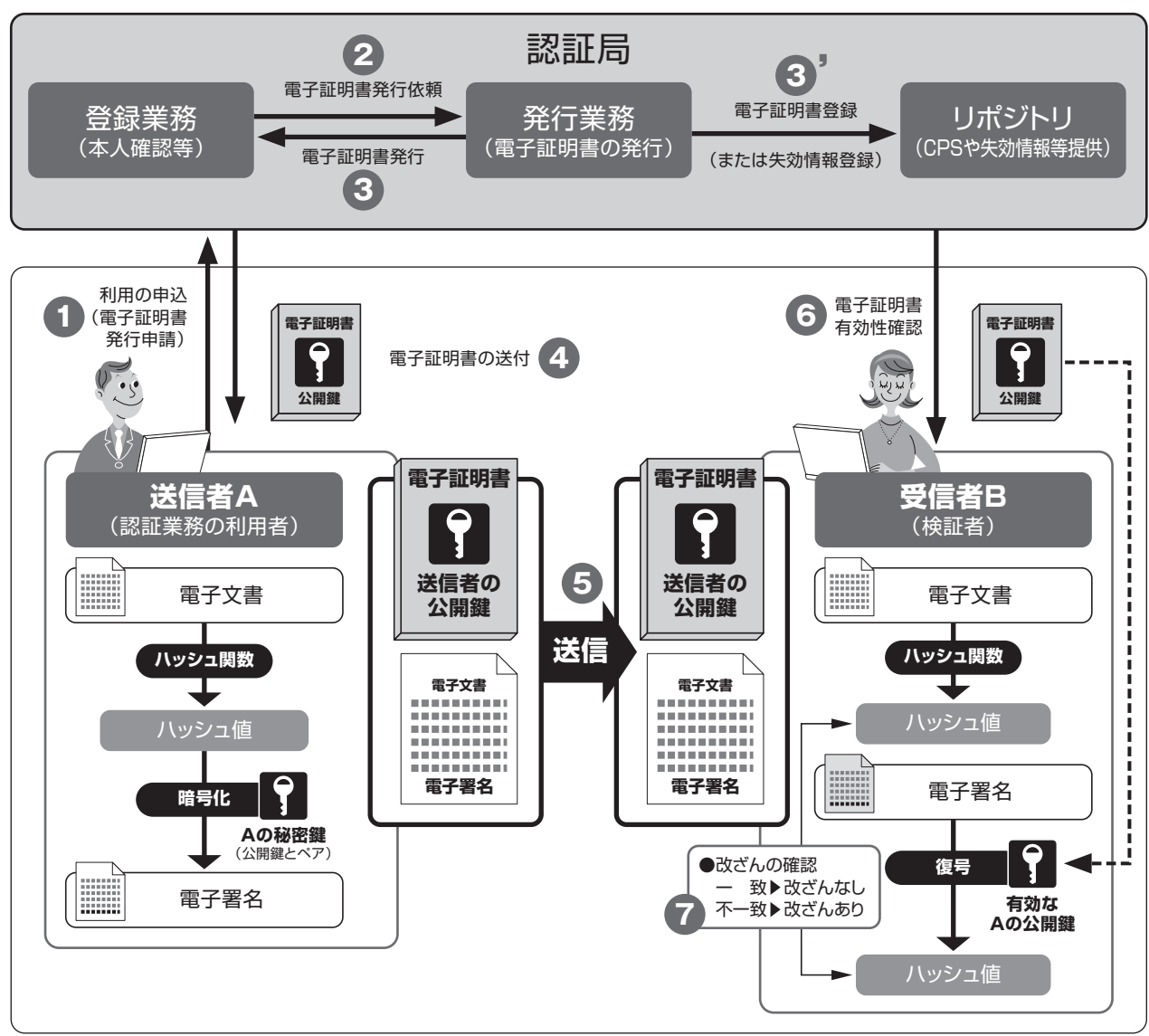
電子署名に関連する関係法令	<ul style="list-style-type: none"> ● 電子署名及び認証業務に関する法律（平成12年法律第102号） ● 電子署名及び認証業務に関する法律施行令（平成13年政令第41号） ● 電子署名及び認証業務に関する法律施行規則（平成13年総務省、法務省、経済産業省令第2号） ● 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針 ● 電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針 <p>参照→付録A. 電子署名に関連する関係法令</p>
電子署名	<p>電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。</p> <p>① 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。</p> <p>② 当該情報について改変が行われていないかどうかを確認することができるものであること。</p> <p>電子署名法は技術中立性を確保するため、特定の技術に限定していないが、現時点では、PKI (Public Key Infrastructure: 公開鍵認証基盤) 技術をベースにしたデジタル署名が電子署名法の基準を満たしているといえる。</p> <p>参照→1-2. 署名 (デジタル署名)、PKI (Public Key Infrastructure: 公開鍵認証基盤)</p>
電磁的記録	<p>電子的方式、磁氣的方式その他の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。</p> <p>一般的には、ディスクやICカードなどに記録されたものをいう。</p>
認証業務	<p>利用者及び署名検証者などの求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる情報（デジタル署名の場合は利用者の公開鍵）が当該利用者に係るものであることを証明する業務をいう。</p>
特定認証業務	<p>電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。</p>
認定認証業務	<p>電子署名法等の認定基準を満たし、認定を受けた特定認証業務をいう。</p>
認証業務用設備	<p>認証業務の用に供する設備のうち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をいう。</p> <p>参照→1-2. 認証局 (CA: Certification Authority)</p>
登録用端末設備	<p>専ら電子証明書の利用者を登録するために用いられる設備をいう。</p>
利用者識別設備	<p>専ら利用者情報及び利用者識別符号を識別するために用いられる設備をいう。</p>

認証設備室	<p>認証業務用設備を設置する室をいう。ただし、認証業務用設備のうち、登録用端末設備のみが設置されている室を除く。</p> <p>認証設備室には、生体認証を用いた入退室管理装置、監視モニター等による監視システム等の安全性を図るセキュリティ要件が必要である。</p>
利用申込者	<p>認証業務の利用の申込みをする者をいう。</p>
利用者	<p>自らが行う電子署名について認証業務を利用する者をいう。</p> <p>自然人に限られ、法人は含まない。</p>
署名検証者	<p>利用者から電子署名が行われた情報の送信を受け、当該利用者が当該電子署名を行ったものであることを確認する者をいう。</p>
電子証明書	<p>「利用者署名検証符号」が当該利用者に係るものであることを証明するために作成する電磁的記録をいう。</p> <p>電子証明書には、利用者の電子証明書や認証局の電子証明書などがあるが、電子署名法において単に電子証明書と表記した場合は、利用者の電子証明書を指す。</p> <p>参照→1-2. 電子証明書 (Certificate)</p>
電子証明書の失効	<p>電子証明書の失効とは、電子証明書の有効期間内であるにも係らず、当該電子証明書の効力を失わせることをいう。</p> <p>電子証明書は、その有効期間内において、利用者から電子証明書の失効の請求があったとき又は電子証明書に記録された事項に事実と異なるものが発見されたときなどに失効される。</p> <p>また、電子証明書の失効に関する情報については、以下の事項が認定基準として定められている。</p> <p>① 遅滞なく当該電子証明書の失効の年月日その他の失効に関する情報を電磁的方法により記録すること。</p> <p>② 電子証明書の有効期間内において、署名検証者からの求めに応じ自動的に送信する方法その他の方法により、署名検証者が失効に関する情報を容易に確認することができるようにすること。</p> <p>参照→1-2. CRL (Certificate Revocation List: 電子証明書失効リスト)</p>
利用者署名符号	<p>利用者が電子署名を行うために用いる符号をいう。</p> <p>参照→1-2. 利用者秘密鍵</p>
利用者署名検証符号	<p>利用者が電子署名を行ったものであることを確認するために用いられる符号をいう。</p> <p>参照→1-2. 利用者公開鍵</p>
発行者署名検証符号	<p>署名検証者が電子証明書の発行者を確認するために用いる符号をいう。</p> <p>参照→1-2. 認証局の公開鍵</p>
発行者署名符号	<p>電子証明書の発行者を確認するための措置であって、発行者が電子証明書の電子署名に用いる符号をいう。</p> <p>参照→1-2. 認証局の秘密鍵</p>
危殆化	<p>(利用者署名符号や発行者署名符号が) 盗難、漏えい等により他人によって使用され得る状態になることをいう。</p>

<p>発行者署名符号の生成、管理に使用する暗号装置</p>	<p>発行者署名符号(認証局の秘密鍵)を安全に生成し保管する装置をいう。 参照→1-2. HSM (Hardware Security Module)</p>
<p>電子署名の方式(電子署名のためのアルゴリズム)</p>	<p>「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」で認められている方式は、次の通りである。</p> <ul style="list-style-type: none"> ●RSA方式(オブジェクト識別子 1 2 840 113549 1 1 5) モジュラスとなる合成数が1024ビット以上のもの ●RSA-PSS方式(オブジェクト識別子 1 2 840 113549 1 1 10) モジュラスとなる合成数が1024ビット以上のもの ●ECDSA方式(オブジェクト識別子 1 2 840 10045 4 1) 楕円曲線の定義体及び位数が160ビット以上のもの ●DSA方式(オブジェクト識別子 1 2 840 10040 4 3) モジュラスとなる素数が1024ビットのもの <p>参照→1-2. オブジェクト識別子 (OID:Object Identification)</p>
<p>発行者署名検証符号に係る電子証明書の値をSHA-1で変換した値</p>	<p>認証局の電子証明書をハッシュ関数であるSHA-1を用いて変換した160ビットのハッシュ値をいう。 参照→1-2. ハッシュ値</p>

1-2 デジタル署名関連の用語

電子署名のうち、PKI (Public Key Infrastructure:公開鍵認証基盤) 技術をベースにしたデジタル署名技術に関連する主な用語についてまとめました。



<p>ARL (Authority Revocation List: 認証局証明書失効リスト)</p>	<p>認証局の電子証明書及び相互認証証明書の有効期間中に、認証局の秘密鍵の危殆化、相互認証基準違反等の事由により失効した認証局の電子証明書及び相互認証証明書のリスト。このリストには、失効した電子証明書を発行した認証局が電子署名を行う。</p>
<p>CP (Certificate Policy: 証明書ポリシー)</p>	<p>認証局が電子証明書を発行する際の運用方針を定めた文書。</p>
<p>CPS (Certification Practices Statement: 認証業務運用規程)</p>	<p>認証局の信頼性、安全性を対外的に示すために、認証局の運用、鍵の生成・管理、責任等に関して定めた文書。CPが何を運用方針にするのかを示すのに対して、CPSは運用方針をどのように適用させるのかを示す。 参照→付録C CPSの構成案</p>

CRL (Certificate Revocation List: 電子証明書失効リスト)	電子証明書の有効期間中に、電子証明書記載内容の変更、秘密鍵の紛失・盗難等の事由により、発行した電子証明書を失効した際に、認証局が公表する電子証明書の失効を示す情報のリスト。電子証明書失効リストには、失効した電子証明書の番号、失効日時、失効事由などが記載されている。このリストには、失効した電子証明書を発行した認証局の署名が付与される。電子証明書の失効情報を通知する手段として、他にOCSPがある。 参照→付録B-2. CRLのプロファイル
CSR (Certificate Signing Request)	電子証明書を発行する際の元となるデータ。CSRには電子証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して電子証明書を発行する。データ形式として、PKCS#10 などがある。
GPKI (Government Public Key Infrastructure: 政府認証基盤)	国民等と行政機関との間でインターネット等を利用してやり取りされる電子文書について、その文書が真にその名義人によって作成され、内容に改変がないことを相互に確認するための仕組み、基盤。具体的には、公開鍵暗号方式による署名を用いた行政機関側の認証システムであり、BCA と各府省CA から構成される。 GPKIに関連する情報は、 http://www.gpki.go.jp/ にて公開されている。
HSM (Hardware Security Module)	暗号鍵等の生成、保管、利用などにおいて、セキュリティを確保する目的で使用するハードウェア。不正アクセスに備えるための機能(耐タンパ機能)を備えている。
IA (Issuing Authority: 発行局)	認証局の業務のうち、電子証明書発行業務及び認証局の秘密鍵の生成、管理を行う機関。
OCSP (Online Certificate Status Protocol)	電子証明書が失効しているかどうかを確認するためのオンラインによる電子証明書検証手順であり、サーバ(OCSPレスポンド)に対して、クライアント(OCSPリクエスト)から電子証明書が失効しているかを問い合わせ、サーバから回答を受け取る。
PKI (Public Key Infrastructure: 公開鍵認証基盤)	公開鍵暗号方式によるデジタル署名を用いた認証システムで、なりすましや否認防止などインターネット通信などにおけるセキュリティ確保のための技術である。
RA (Registration Authority: 登録局)	認証局の業務のうち、登録業務を行う機関。主な業務は、電子証明書発行対象者の本人確認、電子証明書発行に必要な情報の登録、IAに対する電子証明書発行要求等である。
URI (Uniform Resource Identifier)	IETFのRFC2396において、URIとURLが定義されている。 URIは、人間や企業などを含むさまざまなリソース(インターネット上に限定しない)を特定するための表記形式である。
URL (Uniform Resource Locator)	URLはインターネット上のリソースを特定するための表記形式である。 たとえば、 http://www.jipdec.jp/ のように記述される。
X.509 (Information Technology - Open Systems Interconnection - The Directory: Authentication Framework)	ITU-Tの認証フレームワークに関する規格で、電子証明書フォーマットについて定義している。 ISO/IEC 9594-8としても規定されている。 RFC3280ではX.509 (1997 E) が参照されており、電子証明書はX.509ver3の形式、電子証明書失効リストはX.509ver2の形式が用いられている。

オブジェクト識別子 (OID: object identifier)	国際的に一意識別となる値を登録機関(ISO、ITU-T)に登録した識別子。電子証明書で使用する署名アルゴリズム名等は、オブジェクト識別子として登録されているものが使用される。以下のオブジェクト識別子を持つ4つの電子署名アルゴリズムは、電子署名法における特定認証業務に係る電子署名の基準を満たしている。 ● RSA方式(オブジェクト識別子 1 2 840 113549 1 1 5) ● RSA-PSS方式(オブジェクト識別子 1 2 840 113549 1 1 10) ● ECDSA方式(オブジェクト識別子 1 2 840 10045 4 1) ● DSA方式(オブジェクト識別子 1 2 840 10040 4 3)
鍵ペア	公開鍵暗号方式における公開鍵と秘密鍵のペア。 鍵ペアの一方の鍵で暗号化したものは、鍵ペアの他方の鍵でしか復号できない性質を持つため、一方(秘密鍵)を秘密にし、他方(公開鍵)を公開する。
活性化データ	HSM(暗号モジュール)、システム、装置等を動かす(活性化する)のに要求され、防護される必要のあるデータ値で鍵以外のもの。(例: PIN、パスフレーズなど) アクティベーション データ(Activation data)ともいう。
セキュリティ監査	システムやネットワーク等の操作、動作についてセキュリティ面から実施される監査。
自己署名証明書	自認証局の公開鍵に対して、自認証局の秘密鍵で署名した電子証明書。自認証局の公開鍵の正当性を保証するために発行する認証局の電子証明書。
準拠性監査	CP、CPSなどの当該認証業務の運用に関する規定事項に従って業務が実施されたかどうかを評価すること。
署名検証者 (Relying party)	依存者もしくは信頼者等とも表現する場合があります。デジタル署名を受け取り検証する側の人またはサーバ等。
相互認証証明書	2つの異なる認証ドメインの認証局がそれぞれ発行した電子証明書を相互認証するために、相互に発行する電子証明書。GPKIでは、府省CAと民間CA間で直接相互認証証明書を交換せずに、それぞれがBCAと相互認証証明書を交換することによって相互認証を行う。
耐タンパ機能	不正アクセスに対してその侵入の痕跡を残したり、データを消去することにより、データを保護する機能。不正アクセスの証拠を残す不正表示機能、不正アクセスからデータを防護する不正防護機能、不正アクセスに対してデータを消去する対抗動作を行う不正対抗機能等がある。
ディレクトリサーバ	階層構造を持ち、電子証明書や失効情報等を格納するデータベースサーバ。
電子証明書	公開鍵証明書ともいい、ある公開鍵を、記載された者が保有することを証明する電子的文書。認証局が記載内容を確認のうえ、認証局の署名を付与することで、その公開鍵の正当性を保証する。電子証明書には、発行者名、利用者名、電子証明書の有効期間、利用者の公開鍵などが記載されている。 参照→付録B-1. 電子証明書のプロファイル
電子証明書の有効期間	電子証明書発行時に設定する電子証明書が有効である期間。 具体的には電子証明書プロファイルの開始日時と終了日時の間の期間である。

認証局 (CA:Certification Authority)	電子証明書の発行・更新・失効、認証局の秘密鍵の生成・保護及び利用者の登録を行う機関。一般に認証局は、利用者の審査・登録を行う登録局(RA)、電子証明書の発行・管理を行う発行局(IA)、電子証明書の失効情報などを公開するリポジトリなどにより構成される。
認証局の公開鍵	署名検証者が利用者の電子証明書等に付されている認証局の署名を確認する際に用いる鍵。
認証局の秘密鍵	認証局が利用者の電子証明書等を発行する際に、利用者の電子証明書等の署名に用いる鍵。
ハッシュ値	文字や数字などのデータ(入力値)を一定の長さのデータ(出力値)に変換するための手順(関数)のことをハッシュ関数といい、ハッシュ関数を用いて出力された値を「ハッシュ値」と呼ぶ。ハッシュ関数は、異なる2つの入力値から同じ出力値を算出することが困難な特徴をもち、また、出力値から入力値を逆算することも困難である。ハッシュ値は、ハッシュ関数の特徴で一意に決まることからフィンガープリント(指紋)ともいわれている。
ブリッジ認証局 (BCA:Bridge CA)	複数の認証局と相互認証証明書を交換し、相互接続を可能とする認証局のこと。相互認証の中継地点として設けることで、各認証局はBCAと相互認証することにより、同様にBCAに繋がる別のCAで発行された電子証明書の検証ができ、相互運用が可能となる。
プロファイル	電子証明書及びCRL/ARLに含まれるデータの内容を定義したもの。 参照→付録B-1. 電子証明書のプロファイル
リポジトリ (Repositories)	電子証明書及びCRL/ARL等を格納し公表するデータベース。ディレクトリサーバが使用されることが多い。
利用者(Subscriber)	加入者とも表現する場合があります、デジタル署名を生成し送付する側の人またはサーバ等。
利用者公開鍵	RSA、DSAなどの公開鍵暗号技術で使用される鍵ペアの一方で通信相手等に公開される鍵。
利用者秘密鍵	RSA、DSAなどの公開鍵暗号技術で使用される鍵ペアの一方で利用者本人のみが保有し、他人に秘密にする鍵。 秘密鍵で署名されたものは、当該秘密鍵に対応した公開鍵でしか署名検証できない。
リンク証明書	認証局の鍵更新時に、同時に存在することとなる新しい認証局の鍵ペアと古い認証局の鍵ペアの関係を保証するために発行される電子証明書。

〈参考文献〉

- 政府認証基盤 (GPKI) 電子政府の認証基盤に関する情報を案内するホームページ <http://www.gpki.go.jp/>
- The Internet Engineering Task Force (IETF) のホームページ <http://ietf.org/>
- 電子商取引推進協議会 (ECOM) 「認証局運用ガイドライン」 http://www2.ecom.jp/report/pdf/H09/h9_cert2.pdf

2

デジタル署名関連の技術標準

2-1

IETF (Internet Engineering Task Force)

IETF PKIX
(Public-Key Infrastructure
(X.509))

インターネットにおけるプロトコルの技術の標準化を検討しているインターネットの技術的活動部会IETF (Internet Engineering Task Force) のセキュリティ分野の1つのワーキンググループ。電子証明書及びCRL/ARLのプロファイルやPKIに関連するプロトコルを検討している。IETFで合意された仕様はRFC (Request For Comments) として公開される。
<http://www.ietf.org/html.charters/pkix-charter.html>

RFC2560

(X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP)

オンラインによる電子証明書有効検証を行うプロトコルを規定したドキュメント。
<http://www.ietf.org/rfc/rfc2560.txt>

RFC 3279

(Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)

電子証明書や電子証明書失効リストに用いる署名方式などの暗号アルゴリズムとそのオブジェクト識別子に関するRFCである。本RFCの補足として、2005年6月にRFC4055等が勧告されている。署名アルゴリズムのオブジェクト識別子は電子証明書プロファイルのsignatureフィールドのalgorithmに記載される。

md2WithRSAEncryption

OID={ iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 2 }

md5WithRSAEncryption

OID={ iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 4 }

sha-1WithRSAEncryption

OID={ iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 5 }

sha224WithRSAEncryption

OID={ iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 14 }

sha256WithRSAEncryption

OID={ iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 11 }

sha384WithRSAEncryption

OID={ iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 12 }

sha512WithRSAEncryption

OID={ iso (1) member-body (2) us (840) rsadsi (113549) pkcs (1) pkcs-1 (1) 13 }

id-dsa-with-sha1

OID={ iso (1) member-body (2) us (840) x9-57 (10040) x9cm (4) 3 }

ecdsa-with-SHA1

OID={ iso (1) member-body (2) us (840) ansi-X9-62 (10045) Signsture (4) 1 }

原文<http://www.ietf.org/rfc/rfc3279.txt> <http://www.ietf.org/rfc/rfc4055.txt>

IETF PKIX (Public-Key Infrastructure (X.509))	RFC3126 (Electronic Signature Formats for long term electronic signatures) デジタル署名の付与、デジタル署名に対するタイムスタンプの付与、電子証明書と失効情報の保持を行うことができるように、長期間の正当性を維持できる形式を定めている長期署名フォーマット仕様を規定したドキュメント。 原文 http://www.ietf.org/rfc/rfc3126.txt
	RFC3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) PKIの基本的な枠組み、電子証明書と電子証明書失効リストのプロファイルに関するRFCで、RFC2459の更新版である。本RFCの補足として、2006年8月にRFC4630が勧告されている。 原文 http://www.ietf.org/rfc/rfc3280.txt http://www.ietf.org/rfc/rfc4630.txt 参照→付録B 電子証明書及びCRLのプロファイル
	RFC3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) CPとCPSのフレームワークを規定したドキュメント。 本RFCは、RFC2527の更新版であり、2003年11月にInformational RFCとなった。 原文 http://www.ietf.org/rfc/rfc3647.txt 参照→付録C CPSの構成案
	RFC4210 (Internet X.509 Public Key Infrastructure Certificate Management Protocols) 電子証明書の作成、管理に係る全ての局面に関するプロトコルを規定したドキュメントで、RFC2510の更新版である。 原文 http://www.ietf.org/rfc/rfc4210.txt
	RFC4211 (Internet X.509 Certificate Request Message Format) 電子証明書要求メッセージフォーマットを規定したドキュメントで、RFC2511の更新版である。 原文 http://www.ietf.org/rfc/rfc4211.txt
	その他に、署名されたドキュメントや電子証明書の検証サーバとアクセスプロトコルを規定したRFC3029 (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols)、タイムスタンプに関連したRFC3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)) やRFC 3628 (Policy Requirements for Time-Stamping Authorities) などのRFCがある。

**PKIXと関連がある
ワーキンググループ**
PKI Profile for IPsecPKI4IPSEC WG

X.509証明書のIPsecでの利用に関する検討ワーキンググループである。
<http://www.icsalabs.com/pki4ipsec/>

S/MIME WG

インターネットの電子メール(MIME)のセキュリティを確保するために、デジタル署名や暗号などの拡張の標準化を検討しているワーキンググループである。
<http://tools.ietf.org/wg/smime/>

TLS WG

インターネットにおける認証プロトコルであるNetscape Communications社が開発したSSLの標準化を検討しているワーキンググループである。
<http://tools.ietf.org/wg/tls/>

その他に、**Long-Term Archive and Notary Services**などを検討しているワーキンググループなどがある。

2-2

ITU (International Telecommunication Union)

**ITU-T
(International
Telecommunication
Union-
Telecommunication
Standardization
Sector)**

ITUは国際連合 (UN) の専門機関であり3つの標準化部門がある。
その一つであるITU-Tでは、電気通信の改善、合理的利用を目的とした国際電気通信連合の電気通信標準化部門である。
<http://www.itu.int/ITU-T/>

X.500シリーズ

広範囲なサービスを提供することを目的にITUが開発したOSI (Open Systems Interconnection) のディレクトリに関する勧告 (Recommendation)。

X.509
(Information Technology-Open Systems Interconnection-The Directory: Authentication Framework)

ITU-Tの認証フレームワークに関する規格で、電子証明書フォーマットについて定義している。
ISO/IEC 9594-8としても規定されている。
RFC3280ではX.509 (1997 E) が参照されており、電子証明書はX.509ver3の形式、電子証明書失効リストはX.509ver2の形式が用いられている。

X.520
(Information Technology-Open Systems Interconnection-The Directory: Selected Attribute Types)

ITU-Tの属性定義に関する規格である。
RFC3280ではX.520 (1993) が参照されている。電子証明書の発行者や利用者の属性は、本規格に準拠している。

2-3

その他デジタル署名関連の標準化機関・組織

**NIST
(米国標準技術研究所:
National Institute
of Standards and
Technology)**

NISTが策定したFIPS (米国連邦情報処理標準:Federal Information Processing Standard) のうち、デジタル署名に関連する主な標準は次の通りである。
<http://www.itl.nist.gov/fipspubs/>

FIPS 140-2
(Security Requirements for Cryptographic Modules)

コンピュータと通信システムの暗号モジュールに関するセキュリティ要件を定義している。
セキュリティ要件レベルには、最高レベル4からレベル1までである。

FIPS 180-1 Secure Hash Standard (SHS)

デジタル署名に用いるハッシュ関数の仕様について定義している。

FIPS 180-2 Digital Signature Standard (DSS)

デジタル署名に用いる署名アルゴリズムの仕様について定義している。
2000年にFIPS 186-1の更新版としてFIPS 186-2が公開された。

**PKCS
(Public-Key
Cryptography
Standards)**

米国RSA Data Security 社による公開鍵暗号方式に関する技術標準がPKCS (Public-Key Cryptography Standards) であり、デジタル署名に関連する主な標準は次の通りである。
<http://www.rsa.com/rsalabs/>

PKCS#1 Cryptographic Cryptography Standard

RSA暗号方式を定義した仕様であり、現在はVersion 2.1である。
<http://www.rsa.com/rsalabs/node.asp?id=2125>

PKCS#7 Cryptographic Message Syntax Standard

デジタル署名や暗号を含むメッセージに関する一般的な構文を定義した仕様であり、現在はVersion 1.6を検討中である。
<http://www.rsa.com/rsalabs/node.asp?id=2129>

PKCS#10 Certification Request Syntax Standard

電子証明書発行要求形式を定義した仕様であり、現在はVersion 1.7である。
<http://www.rsa.com/rsalabs/node.asp?id=2132>

PKCS#11 Cryptographic Token Interface Standard

ICカードなどの暗号デバイスのインタフェースを定義した仕様であり、現在はVersion2.20である。
<http://www.rsa.com/rsalabs/node.asp?id=2133>

PKCS#12 Personal Information Exchange Syntax Standard

秘密鍵と電子証明書を安全に交換するための方法を定義した仕様であり、現在はVersion 1.0である。
<http://www.rsa.com/rsalabs/node.asp?id=2138>

その他にPKCS #8 (Private-Key Information Syntax Standard) などがある。

CRYPTREC (CRYPTography Research & Evaluation Committees)	<p>日本における暗号技術の評価プロジェクトである。</p> <p>電子署名法における電子署名の安全性はCRYPTRECの評価結果が参考にされている。CRYPTREC活動の成果として、「電子政府推奨暗号リスト」が総務省および経済産業省から公表されている。</p> <p>平成15年2月に決定された「電子政府推奨暗号リスト」には公開鍵暗号・署名としてDSA、ECDSA、RSASSA-PKCS1-v1_5、RSA-PSSがあり、ハッシュ関数としてRIPEMD-160、SHA-1、SHA-256、SHA-384、SHA-512がある。</p> <p>また電子署名法に関する暗号についての技術的提案を行っている。</p> <p>http://www.cryptrec.jp/</p>
ISO/IEC JTC1/SC27	<p>ISO(国際標準化機構:International Organization for Standardization)とIEC(国際電気標準会議:International Electrotechnical Commission)の共同委員会(Joint Technical Committee 1)の1つであり、情報セキュリティ技術全般の国際標準を検討している。</p> <p>SC27(IT Security Techniques)には3つのWGがあり、WG2ではITセキュリティ技術とメカニズム関数として、鍵管理やデジタル署名等の標準化に取り組んでいる。WG1では情報セキュリティ要求条件と統合技術、WG3ではセキュリティ評価基準の標準化を進めている。</p> <p>http://www.iso.ch/iso/en/ISOOnline.openpage</p>
ANSI (米国規格協会: American National Standards Institute)	<p>ANSIでは、米国における工業製品やサービスの規格の統一標準化を検討している機関であり、ANSI X9.30やANSI X9.62などでデジタル署名に関する標準を定めている。</p> <p>http://www.x9.org/</p>
ETSI (欧州電気通信標準化協会: European Telecommunications Standards Institute)	<p>ETSIは欧州における情報通信関係の標準を検討している機関であり、電子署名に関連する文書を公開している。</p> <ul style="list-style-type: none"> ● ETSI ES 201 733 Electronic Signature Formats (長期署名フォーマット仕様) ● ETSI TS 101 903 XML Advanced Electronic Signature (XML版長期署名フォーマット) <p>http://www.etsi.org/</p>
次世代電子商取引 推進協議会 (ECOM)	<p>「長期署名フォーマットの相互運用性試験プロジェクト」として、RFC 3126やXAdESなどの標準に基づく長期署名フォーマットを日本国内で普及定着させるべく、データ構造や処理手順の必要条件をまとめた「長期署名フォーマットのプロファイル」を策定や、長期署名に関するJIS原案の検討等を行っている。</p> <p>http://www.ecom.jp/</p>

その他の電子署名に関連する機関・組織としては下記がある。

- **CEN (European Committee for Standardization)**
<http://www.cenorm.be/>
- **EESSI (欧州電子署名標準化イニシアティブ:European Electronic Signature Standardization Initiative)**
<http://www.cenorm.be/iss/>
- **IEEE (米国電気電子学会:Institute of Electrical and Electronics Engineers)**
<http://grouper.ieee.org/groups/1363/index.html>
- **W3C (The World Wide Web Consortium)**
<http://www.w3.org>

電子署名及び認証業務に関する法律

(平成十二年五月三十一日法律第百二号)

第一章 総則

(目的)

第一条 この法律は、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とする。

(定義)

第二条 この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

- 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
- 二 当該情報について改変が行われていないかどうかを確認することができるものであること。

2 この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

3 この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

第二章 電磁的記録の真正な成立の推定

第三条 電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

第三章 特定認証業務の認定等

第一節 特定認証業務の認定

(認定)

第四条 特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

2 前項の認定を受けようとする者は、主務省令で定めるところにより、次の事項を記載した申請書その他主務省令で定める書類を主務大臣に提出しなければならない。

- 一 氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
- 二 申請に係る業務の用に供する設備の概要
- 三 申請に係る業務の実施の方法

3 主務大臣は、第一項の認定をしたときは、その旨を公示しなければならない。

(欠格条項)

第五条 次の各号のいずれかに該当する者は、前条第一項の認定を受けることができない。

- 一 禁錮以上の刑（これに相当する外国の法令による刑を含む。）に処せられ、又はこの法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者
- 二 第十四条第一項又は第十六条第一項の規定により認定を取り消され、その取消しの日から二年を経過しない者
- 三 法人であって、その業務を行う役員のうち前二号のいずれかに該当する者があるもの

(認定の基準)

第六条 主務大臣は、第四条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。

- 一 申請に係る業務の用に供する設備が主務省令で定める基準に適合するものであること。
- 二 申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること。
- 三 前号に掲げるもののほか、申請に係る業務が主務省令で定める基準に適合する方法により行われるものであること。

2 主務大臣は、第四条第一項の認定のための審査に当たっては、主務省令で定めるところにより、申請に係る業務の実施に係る体制について実地の調査を行うものとする。

(認定の更新)

第七条 第四条第一項の認定は、一年を下らない政令で定める期間ごとにその更新を受けなければ、その期間の経過によって、その効力を失う。

2 第四条第二項及び前二条の規定は、前項の認定の更新に準用する。

(承継)

第八条 第四条第一項の認定を受けた者（以下「認定認証事業者」という。）がその認定に係る業務を行う事業の全部を譲渡し、又は認定認証事業者について相続、合併若しくは分割（その認定に係る業務を行う事業の全部を承継させるものに限る。）があったときは、その事業の全部を譲り受けた者又は相続人（相続人が二人以上ある場合において、その全員の同意により事業を承継すべき相続人を選定したときは、その者。以下この条において同じ。）、合併後存続する法人若しくは合併により設立した法人若しくは分割によりその事業の全部を継承した法人は、その認定認証事業者の地位を承継する。ただし、その事業の全部を譲り受けた者又は相続人、合併後存続する法人若しくは合併により設立した法人若しくは分割によりその事業の全部を承継した法人が第五条各号のいずれかに該当するときは、この限りでない。

(変更の認定等)

第九条 認定認証事業者は、第四条第二項第二号又は第三号の事項を変更しようとするときは、主務大臣の認定を受けなければならない。ただし、主務省令で定める軽微な変更については、この限りでない。

2 前項の変更の認定を受けようとする者は、主務省令で定めるところにより、変更に係る事項を記載した申請書その他主務省令で定める書類を主務大臣に提出しなければならない。

3 第四条第三項及び第六条の規定は、第一項の変更の認定に準用する。

4 認定認証事業者は、第四条第二項第一号の事項に変更があったときは、遅滞なく、その旨を主務大臣に届け出なければならない。

(廃止の届出)

第十条 認定認証事業者は、その認定に係る業務を廃止しようとするときは、主務省令で定めるところにより、あらかじめ、その旨を主務大臣に届け出なければならない。

2 主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

(業務に関する帳簿書類)

第十一条 認定認証事業者は、主務省令で定めるところにより、その認定に係る業務に関する帳簿書類を作成し、これを保存しなければならない。

(利用者の真偽の確認に関する情報の適正な使用)

第十二条 認定認証事業者は、その認定に係る業務の利用者の真偽の確認に際して知り得た情報を認定に係る業務の用に供する目的以外に使用してはならない。

(表示)

第十三条 認定認証事業者は、認定に係る業務の用に供する電子証明書等（利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明するために作成する電磁的記録その他の認証業務の用に供するものとして主務省令で定めるものをいう。次項において同じ。）に、主務省令で定めるところにより、当該業務が認定を受けている旨の表示を付することができる。

2 何人も、前項に規定する場合を除くほか、電子証明書等に、同項の表示又はこれと紛らわしい表示を付してはならない。

(認定の取消し)

第十四条 主務大臣は、認定認証事業者が次の各号のいずれかに該当するときは、その認定を取り消すことができる。

- 一 第五条第一号又は第三号のいずれかに該当するに至ったとき。
- 二 第六条第一項各号のいずれかに適合しなくなったとき。
- 三 第九条第一項、第十一条、第十二条又は前条第二項の規定に違反したとき。
- 四 不正の手段により第四条第一項の認定又は第九条第一項の変更の認定を受けたとき。

2 主務大臣は、前項の規定により認定を取り消したときは、その旨を公示しなければならない。

第二節 外国における特定認証業務の認定

(認定)

第十五条 外国にある事務所により特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

2 第四条第二項及び第三項並びに第五条から第七条までの規定は前項の認定に、第八条から第十三条までの規定は同項の認定を受けた者（以下「認定外国認証事業者」という。）に準用する。この場合において、同条第二項中「何人も」とあるのは、「認定外国認証事業者は」と読み替えるものとする。

3 主務大臣は、第一項の認定若しくはその更新又は前項において準用する第九条第一項の変更の認定を受けようとする者が外国の法令に基づく認証業務に関する制度で第四条第一項の認定の制度に類するものに基づいて当該外国にある事務所により認証業務を行う者である場合であって、我が国が当該外国と締結した条約その他の国際約束を誠実に履行するために必要があると認めるときは、それらの者に対して、前項において準用する第六条第二項（前項において準用する第七条第二項及び第九条第三項において準用する場合を含む。）の規定による調査に代えて、主務省令で定める事項を記載した書類の提出をさせることができる。

4 前項の場合において、これらの者から当該書類の提出があったときは、主務大臣は当該書類を考慮して第一項の認定若しくはその更新又は第二項において準用する第九条第一項の変更の認定のための審査を行わなければならない。

(認定の取消し)

第十六条 主務大臣は、認定外国認証事業者が次の各号のいずれかに該当するときは、その認定を取り消すことができる。

- 一 前条第二項において準用する第五条第一号又は第三号のいずれかに該当するに至ったとき。
- 二 前条第二項において準用する第六条第一項各号のいずれかに適合しなくなったとき。
- 三 前条第二項において準用する第九条第一項若しくは第四項、第十一条、第十二条又は第十三条第二項の規定に違反したとき。
- 四 不正の手段により前条第一項の認定又は同条第二項において準用する第九条第一項の変更の認定を受けたとき。

五 主務大臣が第三十五条第三項において準用する同条第一項の規定により認定外国認証事業者に対し報告をさせようとした場合において、その報告がされず、又は虚偽の報告がされたとき。

六 主務大臣が第三十五条第三項において準用する同条第一項の規定によりその職員に認定外国認証事業者の営業所、事務所その他の事業場において検査をさせようとした場合において、その検査を拒まれ、妨げられ、若しくは忌避され、又は同項の規定による質問に対して答弁がされず、若しくは虚偽の答弁がされたとき。

2 主務大臣は、前項の規定により認定を取り消したときは、その旨を公示しなければならない。

第四章 指定調査機関等

第一節 指定調査機関

(指定調査機関による調査)

第十七条 主務大臣は、その指定する者（以下「指定調査機関」という。）に第六条第二項（第七条第二項（第十五条第二項において準用する場合を含む。）、第九条第三項（第十五条第二項において準用する場合を含む。）及び第十五条第二項において準用する場合を含む。）の規定による調査（次節を除き、以下「調査」という。）の全部又は一部を行わせることができる。

2 主務大臣は、前項の規定により指定調査機関に調査の全部又は一部を行わせるときは、当該調査の全部又は一部を行わないものとする。この場合において、主務大臣は、指定調査機関が第四項の規定により通知する調査の結果を考慮して第四条第一項の認定若しくはその更新、第九条第一項（第十五条第二項において準用する場合を含む。）の変更の認定又は第十五条第一項の認定若しくはその更新のための審査を行わなければならない。

3 主務大臣が第一項の規定により指定調査機関に調査の全部又は一部を行わせることとしたときは、第四条第一項の認定若しくはその更新、第九条第一項（第十五条第二項において準用する場合を含む。）の変更の認定又は第十五条第一項の認定若しくはその更新を受けようとする者は、指定調査機関が行う調査については、第四条第二項（第七条第二項（第十五条第二項において準用する場合を含む。）及び第十五条第二項において準用する場合を含む。）及び第九条第二項（第十五条第二項において準用する場合を含む。）の規定にかかわらず、主務省令で定めるところにより、指定調査機関に申請しなければならない。

4 指定調査機関は、前項の申請に係る調査を行ったときは、遅滞なく、当該調査の結果を主務省令で定めるところにより、主務大臣に通知しなければならない。

(指定)

第十八条 前条第一項の規定による指定（以下「指定」という。）は、主務省令で定めるところにより、調査を行おうとする者（外国にある事務所により行おうとする者を除く。）の申請により行う。

(欠格条項)

第十九条 次の各号のいずれかに該当する者は、指定を受けることができない。

- 一 禁錮以上の刑に処せられ、又はこの法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者
- 二 第二十九条第一項の規定により指定を取り消され、又は第三十二条第一項の規定により承認を取り消され、その取消しの日から二年を経過しない者
- 三 法人であって、その業務を行う役員のうち前二号のいずれかに該当する者があるもの

(指定の基準)

第二十条 主務大臣は、指定の申請が次の各号のいずれにも適合していると認めるときでなければ、その指定をしてはならない。

- 一 調査の業務を適確かつ円滑に実施するに足りる経理的基礎及び技術的能力を有すること。
- 二 法人にあっては、その役員又は法人の種類に応じて主務省令で定める構成員の構成が調査の公正な実施に支障を及ぼすおそれがないものであること。
- 三 調査の業務以外の業務を行っている場合には、その業務を行うことによって調査が不公正になるおそれがないものであること。
- 四 その指定をすることによって申請に係る調査の適確かつ円滑な実施を阻害することとならないこと。

(指定の公示等)

第二十一条 主務大臣は、指定をしたときは、指定調査機関の名称及び住所並びに調査の業務を行う事務所の所在地を公示しなければならない。

- 2 指定調査機関は、その名称若しくは住所又は調査の業務を行う事務所の所在地を変更しようとするときは、変更しようとする日の二週間前までに、その旨を主務大臣に届け出なければならない。
- 3 主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

(指定の更新)

第二十二条 指定は、五年以上十年以内において政令で定める期間ごとにその更新を受けなければ、その期間の経過によって、その効力を失う。

- 2 第十八条から第二十条までの規定は、前項の指定の更新に準用する。

(秘密保持義務等)

第二十三条 指定調査機関の役員（法人でない指定調査機関にあっては、当該指定を受けた者。次項並びに第四十三条及び第四十五条において同じ。）若しくは職員又はこれらの職にあった者は、調査の業務に関して知り得た秘密を漏らしてはならない。

- 2 調査の業務に従事する指定調査機関の役員又は職員は、刑法（明治四十年法律第四十五号）その他の罰則の適用については、法令により公務に従事する職員とみなす。

(調査の義務)

第二十四条 指定調査機関は、調査を行うべきことを求められたときは、正当な理由がある場合を除き、遅滞なく、調査を行わなければならない。

(調査業務規程)

第二十五条 指定調査機関は、調査の業務に関する規程（以下「調査業務規程」という。）を定め、主務大臣の認可を受けなければならない。これを変更しようとするときも、同様とする。

- 2 調査業務規程で定めるべき事項は、主務省令で定める。

- 3 主務大臣は、第一項の認可をした調査業務規程が調査の公正な実施上不適当となったと認めるときは、その調査業務規程を変更すべきことを命ずることができる。

(帳簿の記載)

第二十六条 指定調査機関は、主務省令で定めるところにより、帳簿を備え、調査の業務に関し主務省令で定める事項を記載し、これを保存しなければならない。

(適合命令)

第二十七条 主務大臣は、指定調査機関が第二十条第一号から第三号までに適合しなくなったと認めるときは、その指定調査機関に対し、これらの規定に適合するため必要な措置を講ずべきことを命ずることができる。

(業務の休廃止)

第二十八条 指定調査機関は、主務大臣の許可を受けなければ、調査の業務の全部又は一部を休止し、又は廃止してはならない。

- 2 主務大臣は、前項の許可をしたときは、その旨を公示しなければならない。

(指定の取消し等)

第二十九条 主務大臣は、指定調査機関が次の各号のいずれかに該当するときは、その指定を取り消し、又は期間を定めて調査の業務の全部若しくは一部の停止を命ずることができる。

- 一 この節の規定に違反したとき。
- 二 第十九条第一号又は第三号に該当するに至ったとき。
- 三 第二十五条第一項の認可を受けた調査業務規程によらないで調査の業務を行ったとき。
- 四 第二十五条第三項又は第二十七条の規定による命令に違反したとき。
- 五 不正の手段により指定を受けたとき。

- 2 主務大臣は、前項の規定により指定を取り消し、又は調査の業務の全部若しくは一部の停止を命じたときは、その旨を公示しなければならない。

(主務大臣による調査の業務の実施)

第三十条 主務大臣は、指定調査機関が第二十八条第一項の規定により調査の業務の全部若しくは一部を休止した場合、前条第一項の規定により指定調査機関に対し調査の業務の全部若しくは一部の停止を命じた場合又は指定調査機関が天災その他の事由により調査の業務の全部若しくは一部を実施することが困難となった場合において、必要があると認めるときは、第十七条第二項の規定にかかわらず、調査の業務の全部又は一部を自ら行うものとする。

- 2 主務大臣は、前項の規定により調査の業務を行うこととし、又は同項の規定により行っている調査の業務を行わないこととするときは、あらかじめ、その旨を公示しなければならない。

- 3 主務大臣が、第一項の規定により調査の業務を行うこととし、第二十八条第一項の規定により調査の業務の廃止を許可し、又は前条第一項の規定により指定を取り消した場合における調査の業務の引継ぎその他の必要な事項は、主務省令で定める。

第二節 承認調査機関

(承認調査機関の承認等)

第三十一条 主務大臣は、第十五条第二項において準用する第六条第二項（第十五条第二項において準用する第七条第二項及び第九条第三項において準用する場合を含む。）の規定による調査（以下この節において「調査」という。）の全部又は一部を行おうとする者（外国にある事務所により行おうとする者に限る。）から申請があったときは、主務省令で定めるところにより、これを承認することができる。

2 主務大臣が前項の承認をしたときは、第十五条第一項の認定若しくはその更新又は同条第二項において準用する第九条第一項の変更の認定を受けようとする者は、前項の承認を受けた者（以下「承認調査機関」という。）が行う調査については、第十五条第二項において準用する第四条第二項（第十五条第二項において準用する第七条第二項において準用する場合を含む。）、第十五条第二項において準用する第九条第二項及び第十七条第三項の規定にかかわらず、主務省令で定めるところにより、承認調査機関に申請をすることができる。この場合において、主務大臣は、承認調査機関が次項の規定により通知する調査の結果を考慮して第十五条第一項の認定若しくはその更新又は同条第二項において準用する第九条第一項の変更の認定のための審査を行わなければならない。

3 承認調査機関は、前項の申請に係る調査を行ったときは、遅滞なく、当該調査の結果を主務省令で定めるところにより、主務大臣に通知しなければならない。

4 承認調査機関は、調査の業務の全部又は一部を休止し、又は廃止したときは、遅滞なく、その旨を主務大臣に届け出なければならない。

5 主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

6 第十九条から第二十二條までの規定は第一項の承認に、第二十四条から第二十七條までの規定は承認調査機関に準用する。この場合において、第二十五条第三項及び第二十七條中「命ずる」とあるのは、「請求する」と読み替えるものとする。

(承認の取消し)

第三十二条 主務大臣は、承認調査機関が次の各号のいずれかに該当するときは、その承認を取り消すことができる。

- 一 前条第三項若しくは第四項の規定又は同条第六項において準用する第二十一条第二項、第二十四条、第二十五条第一項若しくは第二十六条の規定に違反したとき。
- 二 前条第六項において準用する第十九条第一号又は第三号に該当するに至ったとき。
- 三 前条第六項において準用する第二十五条第一項の認可を受けた調査業務規程によらないで調査の業務を行ったとき。
- 四 前条第六項において準用する第二十五条第三項又は第二十七條の規定による請求に応じなかったとき。
- 五 不正の手段により前条第一項の承認を受けたとき。

六 主務大臣が、承認調査機関が前各号のいずれかに該当すると認めて、期間を定めて調査の業務の全部又は一部の停止の請求をした場合において、その請求に応じなかったとき。

七 主務大臣が第三十五条第三項において準用する同条第二項の規定により承認調査機関に対し報告をさせようとした場合において、その報告がされず、又は虚偽の報告がされたとき。

八 主務大臣が第三十五条第三項において準用する同条第二項の規定によりその職員に承認調査機関の事務所において検査をさせようとした場合において、その検査が拒まれ、妨げられ、若しくは忌避され、又は同項の規定による質問に対して答弁がされず、若しくは虚偽の答弁がされたとき。

2 主務大臣は、前項の規定により承認を取り消したときは、その旨を公示しなければならない。

第五章 雑則

(特定認証業務に関する援助等)

第三十三条 主務大臣は、特定認証業務に関する認定の制度の円滑な実施を図るため、電子署名及び認証業務に係る技術の評価に関する調査及び研究を行うとともに、特定認証業務を行う者及びその利用者に対し必要な情報の提供、助言その他の援助を行うよう努めなければならない。

(国の措置)

第三十四条 国は、教育活動、広報活動等を通じて電子署名及び認証業務に関する国民の理解を深めるよう努めなければならない。

(報告徴収及び立入検査)

第三十五条 主務大臣は、この法律の施行に必要な限度において、認定認証事業者に対し、その認定に係る業務に関し報告をさせ、又はその職員に、認定認証事業者の営業所、事務所その他の事業場に立ち入り、その認定に係る業務の状況若しくは設備、帳簿書類その他の物件を検査させ、若しくは関係者に質問させることができる。

2 主務大臣は、この法律の施行に必要な限度において、指定調査機関に対し、その業務に関し報告をさせ、又はその職員に、指定調査機関の事務所に立ち入り、業務の状況若しくは帳簿、書類その他の物件を検査させ、若しくは関係者に質問させることができる。

3 第一項の規定は認定外国認証事業者に、前項の規定は承認調査機関に、それぞれ準用する。

4 第一項及び第二項（それぞれ前項において準用する場合を含む。）の規定により立入検査をする職員は、その身分を示す証明書を携帯し、関係者に提示しなければならない。

5 第一項及び第二項（それぞれ第三項において準用する場合を含む。）の規定による立入検査の権限は、犯罪捜査のために認められたものと解釈してはならない。

(手数料)

第三十六条 次の各号に掲げる者は、実費を勘案して政令で定める額の手数料を国に納めなければならない。

- 一 第四条第一項の認定を受けようとする者（主務大臣が第十七条第一項の規定により指定調査機関に調査の全部を行わせることとしたときを除く。）
- 二 第七条第一項（第十五条第二項において準用する場合を含む。）の認定の更新を受けようとする者

三 第九条第一項（第十五条第二項において準用する場合を含む。）の変更の認定を受けようとする者

四 第十五条第一項の認定を受けようとする者（主務大臣が第十七条第一項の規定により指定調査機関に調査の全部を行わせることとしたときを除く。）

2 指定調査機関が行う調査を受けようとする者は、政令で定めるところにより指定調査機関が主務大臣の認可を受けて定める額の手数料を当該指定調査機関に納めなければならない。

（主務大臣と国家公安委員会との関係）

第三十七条 国家公安委員会は、認定認証事業者又は認定外国認証事業者の認定に係る業務に関し、その利用者についての証明に係る重大な被害が生ずることを防止するため必要があると認めるときは、主務大臣に対し、必要な措置をとるべきことを要請することができる。

（審査請求）

第三十八条 この法律の規定による指定調査機関の処分又は不作為について不服がある者は、主務大臣に対し、行政不服審査法（昭和三十七年法律第百六十号）による審査請求をすることができる。

（経過措置）

第三十九条 この法律の規定に基づき政令又は主務省令を制定し、又は改廃する場合においては、それぞれ、政令又は主務省令で、その制定又は改廃に伴い合理的に必要と判断される範囲内において、所要の経過措置（罰則に関する経過措置を含む。）を定めることができる。

（主務大臣等）

第四十条 この法律における主務大臣は、総務大臣、法務大臣及び経済産業大臣とする。ただし、第三十三条においては、総務大臣及び経済産業大臣とする。

2 この法律における主務省令は、総務大臣、法務大臣及び経済産業大臣が共同で発する命令とする。

第六章 罰 則

第四十一条 認定認証事業者又は認定外国認証事業者に対し、その認定に係る認証業務に関し、虚偽の申込みをして、利用者について不実の証明をさせた者は、三年以下の懲役又は二百万円以下の罰金に処する。

2 前項の未遂罪は、罰する。

3 前二項の罪は、刑法第二条の例に従う。

第四十二条 次の各号のいずれかに該当する者は、一年以下の懲役又は百万円以下の罰金に処する。

一 第十三条第二項の規定に違反した者

二 第二十三条第一項の規定に違反してその職務に関して知り得た秘密を漏らした者

第四十三条 第二十九条第一項の規定による業務の停止の命令に違反したときは、その違反行為をした指定調査機関の役員又は職員は、一年以下の懲役又は百万円以下の罰金に処する。

第四十四条 次の各号のいずれかに該当する者は、三十万円以下の罰金に処する。

一 第九条第一項の規定に違反して第四条第二項第二号又は第三号の事項を変更した者

二 第十一条の規定による帳簿書類の作成若しくは保存をせず、又は虚偽の帳簿書類の作成をした者

三 第三十五条第一項の規定による報告をせず、若しくは虚偽の報告をし、又は同項の規定による検査を拒み、妨げ、若しくは忌避し、若しくは同項の規定による質問に対して答弁をせず、若しくは虚偽の答弁をした者

第四十五条 次の各号のいずれかに該当するときは、その違反行為をした指定調査機関の役員又は職員は、三十万円以下の罰金に処する。

一 第二十六条の規定による帳簿の記載をせず、虚偽の記載をし、又は帳簿を保存しなかったとき。

二 第二十八条第一項の規定に違反して調査の業務の全部を廃止したとき。

三 第三十五条第二項の規定による報告をせず、若しくは虚偽の報告をし、又は同項の規定による検査を拒み、妨げ、若しくは忌避し、若しくは同項の規定による質問に対して答弁をせず、若しくは虚偽の答弁をしたとき。

第四十六条 法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、第四十二条第一号又は第四十四条の違反行為をしたときは、行為者を罰するほか、その法人又は人に対して各本条の罰金刑を科する。

第四十七条 第九条第四項又は第十条第一項の規定による届出をせず、又は虚偽の届出をした者は、十万円以下の過料に処する。

附 則

（施行期日）

第一条 この法律は、平成十三年四月一日から施行する。ただし、次条の規定は平成十三年三月一日から、附則第四条の規定は商法等の一部を改正する法律の施行に伴う関係法律の整備に関する法律（平成十二年法律第九十一号）の施行の日から施行する。

（準備行為）

第二条 第十七条第一項の規定による指定及びこれに関し必要な手続その他の行為は、この法律の施行前においても、第十八条から第二十条まで、第二十一条第一項並びに第二十五条第一項及び第二項の規定の例により行うことができる。

（検討）

第三条 政府は、この法律の施行後五年を経過した場合において、この法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずるものとする。

（商法等の一部を改正する法律の施行に伴う関係法律の整備に関する法律の一部改正）

第四条 商法等の一部を改正する法律の施行に伴う関係法律の整備に関する法律の一部を次のように改正する。第百五十条の次に次の一条を加える。（電子署名及び認証業務に関する法律の一部改正）第百五十条の二電子署名及び認証業務に関する法律（平成十二年法律第百二号）の一部を次のように改正する。第八条中「若しくは合併が」を「合併若しくは分割（その認定に係る業務を行う事業の全部を承継させるものに限る。）が」に、「若しくは合併後」を「合併後」に改め、「設立した法人」の下に「若しくは分割によりその事業の全部を承継した法人」を加える。

A-2

電子署名及び認証業務に関する法律施行令

政令第四十一号

(平成十三年二月二十八日)

電子署名及び認証業務に関する法律施行令

内閣は、電子署名及び認証業務に関する法律（平成十二年法律第百二号）第七条第一項（同法第十五条第二項において準用する場合を含む。）、第二十二條第一項（同法第三十一条第六項において準用する場合を含む。）並びに第三十六条第一項及び第二項の規定に基づき、この政令を制定する。

(特定認証業務に係る認定の有効期間)

第一条 電子署名及び認証業務に関する法律（以下「法」という。）第七条第一項（法第十五条第二項において準用する場合を含む。）の政令で定める期間は、一年とする。

(指定調査機関の指定等の有効期間)

第二条 法第二十二條第一項（法第三十一条第六項において準用する場合を含む。）の政令で定める期間は、五年とする。

(認定等の申請に係る手数料の額)

第三条 法第三十六条第一項各号に掲げる者が同項の規定により国に納めなければならない手数料の額は、次の各号に掲げる場合に応じ、それぞれ当該各号に定める額とする。

- 一 主務大臣が法第十七条第一項の指定調査機関に同項の規定による調査の全部を行わせる場合 イ又はロに掲げる者の区分に応じ、それぞれイ又はロに定める額
 - イ 法第七条第一項（法第十五条第二項において準用する場合を含む。）の認定の更新を受けようとする者 一万三百円
 - ロ 法第九条第一項（法第十五条第二項において準用する場合を含む。）の変更の認定を受けようとする者 五千六百円
- 二 主務大臣が法第十七条第一項の指定調査機関に同項の規定による調査の全部を行わせない場合 別に政令で定める額

2 行政手続等における情報通信の技術の利用に関する法律（平成十四年法律第百五十一号）第三条第一項の規定により同項に規定する電子情報処理組織を使用して認定又はその更新の申請を行なう場合における前項の規定の適用については、同項第一号中「一万三百円」とあるのは「九千九百円」と、「五千六百円」とあるのは「五千二百円」とする。

(指定調査機関が行う調査に係る手数料の額の認可)

第四条 法第三十六条第二項の規定による認可を受けようとする指定調査機関は、認可を受けようとする手数料の額及び調査の業務の実施に要する費用の額に関し主務省令で定める事項を記載した申請書を主務大臣に提出しなければならない。手数料の額の変更の認可を受けようとするときも、同様とする。

2 主務大臣は、次の各号のいずれにも適合すると認めるときでなければ、前項の認可をしてはならない。

- 一 手数料の額が当該調査の業務の適正な実施に要する費用の額を超えないこと。
- 二 特定の者に対して不当な差別的取扱いをするものでないこと。

附 則

この政令は、平成十三年四月一日から施行する。

附 則（平成十六年一月三十日政令第一一号）

この政令は、平成十六年三月二十九日から施行する。

A-3

電子署名及び認証業務に関する法律施行規則

総務省

○法務省令第二号

経済産業省

電子署名及び認証業務に関する法律（平成十二年法律第百二号）の規定に基づき、及び同法を実施するため、電子署名及び認証業務に関する法律施行規則を次のように定める。

平成十三年三月二十七日

総務大臣 片山虎之助
法務大臣 高村 正彦
経済産業大臣 平沼 赳夫

電子署名及び認証業務に関する法律施行規則

（用語）

第一条 この規則において使用する用語は、電子署名及び認証業務に関する法律（以下「法」という。）において使用する用語の例による。

（特定認証業務）

第二条 法第二条第三項の主務省令で定める基準は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。

- 一 ほぼ同じ大きさの二つの素数の積である千二十四ビット以上の整数の素因数分解
- 二 大きさ千二十四ビット以上の有限体の乗法群における離散対数の計算
- 三 楕円曲線上の点がなす大きさ百六十ビット以上の群における離散対数の計算
- 四 前三号に掲げるものに相当する困難性を有するものとして主務大臣が認めるもの

（認定の申請）

第三条 法第四条第二項の申請書は、様式第一によるものとする。

2 法第四条第二項の主務省令で定める書類は、次のとおりとする。

- 一 定款若しくは寄附行為及び登記事項証明書又はこれらに準ずるもの
- 二 申請者が法第五条各号の規定に該当しないことを説明した書類
- 三 法第六条第一項各号の認定の基準に適合していることを説明した書類

（業務の用に供する設備の基準）

第四条 法第六条第一項第一号の主務省令で定める基準は、次のとおりとする。

- 一 申請に係る業務の用に供する設備のうち電子証明書（利用者が電子署名を行ったものであることを確認するために用いられる事項（以下「利用者署名検証符号」という。）が当該利用者に係るものであることを証明するために作成する電磁的記録をいう。以下同じ。）の作成又は管理に用いる電子計算機その他の設備（以下「認証業務用設備」という。）は、入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置されていること。
- 二 認証業務用設備は、電気通信回線を通じた不正なアクセス等を防止するために必要な措置が講じられていること。
- 三 認証業務用設備は、正当な権限を有しない者によって作動させられることを防止するための措置が講じられ、かつ、当該認証業務用設備の動作を記録する機能を有していること。
- 四 認証業務用設備のうち電子証明書の発行者（認証業務の名称により識別されるものである場合においては、その業務を含む。以下同じ。）を確認するための措置であって第二条の基準に適合するものを行うために発行者が用いる符号（以下「発行者署名符号」という。）を作成し又は管理する電子計算機は、当該発行者署名符号の漏えいを防止するために必要な機能を有する専用の電子計算機であること。
- 五 認証業務用設備及び第一号の措置を講じるために必要な装置は、停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて必要な措置が講じられていること。

（利用者の真偽の確認の方法）

第五条 法第六条第一項第二号の主務省令で定める方法は、次の各号に掲げる方法とする。

- 一 認証業務の利用の申込みをする者（以下「利用申込者」という。）に対し、住民票の写し、戸籍の謄本若しくは抄本（現住所の記載がある証明書の提示又は提出を求める場合に限る。）、外国人登録法（昭和二十七年法律第百二十五号）第四条の三に規定する登録原票記載事項証明書又はこれらに準ずるものの提出を求め、かつ、次に掲げる方法のうちいずれか一以上のものにより、当該利用申込者の真偽の確認を行う方法。ただし、認証業務の利用の申込み又はハに規定する申込みの事実の有無を照会する文書の受取りを代理人が行うことを認めた認証業務を実施する場合においては、当該代理人に対し、その権限を証する利用申込者本人の署名及び押印（押印した印鑑に係る印鑑登録証明書が添付されている場合に限る。）がある委任状（利用申込者本人が国外に居住する場合においては、これに準ずるもの）の提出を求め、かつ、次に掲げる方法のうちいずれか一以上のものにより、当該代理人の真偽の確認を行うものとする。
- イ 出入国管理及び難民認定法（昭和二十六年政令第三百十九号）第二条第五号に規定する旅券、別表に掲げる官公庁が発行した免許証、許可証若しくは資格証明書等、外国人登録法第五条に規定する外国人登録証明書、住民基本台帳法（昭和四十二年法律第八十一号）第三十条の四十四第一項に規定する住民基本台帳カード（住民基本台帳法施行規則（平成十一年自治省令第三十五号）別記様式第二の様式によるものに限る。）又は官公庁（独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。）、地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第十五号の規定の適用を受けるものをいう。）を含む。）がその職員に対して発行した身分を証明するに足りる文書で当該職員の写真をはり付けたものうちいずれか一以上の提示を求める方法

□ 利用の申込書に押印した印鑑に係る印鑑登録証明書（利用申込者が国外に居住する場合においては、これに準ずるもの）の提出を求める方法

ハ その取扱いにおいて名あて人本人若しくは差出人の指定した名あて人に代わって受け取ることができる者（以下「名あて人等」という。）に限り交付する郵便（次に掲げるいずれかの書類の提示を求める方法により名あて人等であることの確認を行うことにより交付するものに限る。）又はこれに準ずるものにより、申込みの事実の有無を照会する文書を送付し、これに対する返信を受領する方法

(1) イに掲げる書類のいずれか一以上

(2) 健康保険、国民健康保険、船員保険等の被保険者証、共済組合員証、国民年金手帳、国民年金、厚生年金保険若しくは船員保険に係る年金証書又は共済年金、恩給等の書類のいずれか二以上

(3) (2) に掲げる書類のいずれか一以上及び学生証、会社の身分証明書又は公の機関が発行した資格証明書（イに掲げるものを除く。）であって写真をはり付けたもののいずれか一以上

ニ イ、ロ又はハに掲げるものと同等なものとして主務大臣が認めるもの

二 利用申込者が現に有している電子署名に係る地方公共団体の認証業務に関する法律（平成十四年法律第五十三号）第三条第一項に規定する電子証明書に係る電子署名により当該利用申込者の真偽の確認を行う方法

2 現に電子証明書を有している利用者が当該電子証明書の発行者に対して新たな電子証明書の利用の申込みをする場合において、当該申込みに係る電子証明書の有効期間が前項に規定する方法により当該利用者の真偽の確認を行って発行された電子証明書の発行日から起算して五年を超えない日までに満了するものであるときは、同項の規定にかかわらず、当該発行者は、当該利用者が現に有している電子証明書に係る電子署名により当該利用者の真偽を確認することができる。

（その他の業務の方法）

第六条 法第六条第一項第三号の主務省令で定める基準は、次のとおりとする。

一 利用申込者に対し、書類の交付その他の適切な方法により、電子署名の実施の方法及び認証業務の利用に関する重要な事項について説明を行うこと。

二 利用申込者の申込みに係る意思を確認するため、利用申込者に対し、その署名又は押印（押印した印鑑に係る印鑑登録証明書が添付されている場合に限る。）のある利用の申込書その他の書面の提出又は利用の申込みに係る情報（認定を受けた認証業務（以下「認定認証業務」という。）又はこれに準ずるものに係る電子証明書により確認される電子署名が行われたものに限る。）の送信を求めること。

三 利用者が電子署名を行うために用いる符号（以下「利用者署名符号」という。）を認証事業者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者署名符号及びその複製を直ちに消去すること。

三の二 利用者署名符号を利用者が作成する場合において、当該利用者署名符号に対応する利用者署名検証符号を認証事業者が電気通信回線を通じて受信する方法によるときは、あらかじめ、利用者識別符号（認証事業者において、一回に限り利用者の識別に用いる符号であって、容易に推測されないように作成されたものをいう。）を安全かつ確実に当該利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者の識別に用いるまでの間、当該利用者以外の者が知り得ないようにすること。

四 電子証明書の有効期間は、五年を超えないものであること。

五 電子証明書には、次の事項が記録されていること。

イ 当該電子証明書の発行者の名称及び発行番号

ロ 当該電子証明書の発行日及び有効期間の満了日

ハ 当該電子証明書の利用者の氏名

ニ 当該電子証明書に係る利用者署名検証符号及び当該利用者署名検証符号に係るアルゴリズムの識別子

六 電子証明書には、その発行者を確認するための措置であって第二条の基準に適合するものが講じられていること。

七 認証業務に関し、利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置を講じていること。

八 電子証明書に利用者の役職名その他の利用者の属性（利用者の氏名、住所及び生年月日を除く。）を記録する場合においては、利用者その他の者が当該属性についての証明を認定認証業務に係るものであると誤認することを防止するための適切な措置を講じていること。

九 署名検証者（利用者から電子署名が行われた情報の送信を受け、当該利用者が当該電子署名を行ったものであることを確認する者をいう。以下同じ。）が電子証明書の発行者を確認するために用いる符号（以下「発行者署名検証符号」という。）その他必要な情報を容易に入手することができるようにすること。

十 電子証明書の有効期間内において、利用者から電子証明書の失効の請求があったとき又は電子証明書に記録された事項に事実と異なるものが発見されたときは、遅滞なく当該電子証明書の失効の年月日その他の失効に関する情報を電磁的方法（電子的方法、磁気的方法その他の人の知覚によっては認識することができない方法をいう。以下同じ。）により記録すること。

十一 電子証明書の有効期間内において、署名検証者からの求めに応じ自動的に送信する方法その他の方法により、署名検証者が前号の失効に関する情報を容易に確認することができるようにすること。

十二 第十号の規定により電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該電子証明書の利用者にその旨を通知すること。

十三 認証事業者の連絡先、業務の提供条件その他の認証業務の実施に関する規程を適切に定め、当該規程を電磁的方法により記録し、利用者その他の者からの求めに応じ自動的に送信する方法その他の方法により、利用者その他の者が当該規程を容易に閲覧することができるようにすること。

十四 電子証明書に利用者として記録されている者から、権利又は利益を侵害され、又は侵害されるおそれがあるとの申出があった場合においては、その求めに応じ、遅滞なく当該電子証明書に係る利用者に関する第十二条第一項第一号ロ及びハに掲げる書類を当該申出を行った者に開示すること。

十五 次の事項を明確かつ適切に定め、かつ、当該事項に基づいて業務を適切に実施すること。

イ 業務の手順

□ 業務に従事する者の責任及び権限並びに指揮命令系統

ハ 業務の一部を他に委託する場合においては、委託を行う業務の範囲及び内容並びに受託者による当該業務の実施の状況を管理する方法その他の当該業務の適切な実施を確保するための方法

ニ 業務の監査に関する事項

ホ 業務に係る技術に関し十分な知識及び経験を有する者の配置

ヘ 利用者の真偽の確認に際して知り得た情報の目的外使用の禁止及び第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置

ト 危機管理に関する事項

十六 認証業務用設備により行われる業務の重要度に応じて、当該認証業務用設備が設置された室への立入り及びその操作に関する許諾並びに当該許諾に係る識別符号の管理が適切に行われていること。

十七 複数の者による発行者署名符号の作成及び管理その他当該発行者署名符号の漏えいを防止するために必要な措置が講じられていること。

(調査の方法)

第七条 法第六条第二項の調査は、職員二人以上によって行うものとする。

(認定の更新の申請)

第八条 認定認証事業者は、法第七条第一項の認定の更新を受けようとするときは、現に受けている認定の有効期間が満了する日の三十日前までに、様式第一により作成した更新申請書に第三条第二項各号に掲げる書類を添付して、主務大臣に提出しなければならない。ただし、既に主務大臣に提出されているその書類の内容に変更がないときは、当該書類の添付を省略することができる。

2 第四条から前条までの規定は、法第七条第一項の認定の更新に準用する。

(軽微な変更)

第九条 法第九条第一項ただし書の主務省令で定める軽微な変更は、同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設とする。

(変更の認定等)

第十条 法第九条第二項の申請書は、様式第二によるものとする。

2 法第九条第二項の主務省令で定める書類は、第三条第二項各号に掲げる書類（認定若しくはその更新又は変更の認定の申請書に添えて提出されたものにつきその内容に変更がある部分に限る。）とする。

3 第四条から第七条までの規定は、法第九条第一項の変更の認定に準用する。

4 認定認証事業者は、法第九条第四項に規定する届出をするときは、様式第三による届出書に変更の事実を証する書類を添えて主務大臣に提出しなければならない。

(廃止の届出)

第十一条 認定認証事業者は、法第十条第一項に規定する届出をするときは、様式第四による届出書を主務大臣に提出しなければならない。

(帳簿書類)

第十二条 法第十一条の主務省令で定める業務に関する帳簿書類は、次のとおりとする。

一 認証業務の利用の申込みに関する帳簿書類で次に掲げるもの

イ 第六条第一号の説明に関する記録

ロ 利用の申込書

ハ 利用者の真偽の確認のために認証事業者に提出された書類及び提示された証明書等の写し

ニ 利用の申込みに対する諾否を決定した者の氏名

ホ 利用の申込みに対する承諾をしなかった場合においては、その理由を記載した書類

ヘ 電子証明書及びその作成に関する記録

ト 発行者署名検証符号

チ 発行者署名符号の作成及び管理に関する記録

リ 認証事業者が利用者署名符号を作成したときは、当該利用者署名符号の作成及び廃棄に関する記録並びに利用者からの受領書

二 電子証明書の失効に関する帳簿書類で次に掲げるもの

イ 電子証明書の失効の請求書その他の失効に関する判断に関する記録

ロ 電子証明書の失効を決定した者の氏名

ハ 電子証明書の失効の請求に対して拒否をした場合においては、その理由を記載した書類

ニ 第六条第十号の失効に関する情報及びその作成に関する記録

三 認証事業者の組織管理に関する帳簿書類で次に掲げるもの

イ 第六条第十三号の規程及びその変更に関する記録

ロ 第六条第十五号イの事項及びその変更に関する記録

ハ 第六条第十五号ロの事項及びその変更に関する記録

ニ 認証業務の一部を他に委託する場合においては、委託契約に関する書類

ホ 第六条第十五号ニの監査の実施結果に関する記録

四 設備及び安全対策措置に関する帳簿書類で次に掲げるもの

- イ 第四条第一号の措置に関する記録（映像によるものを除く。）
- ロ 第四条第二号の措置に関する記録（不正なアクセス等があったときのものに限る。）
- ハ 第四条第三号の認証業務用設備の動作に関する記録
- ニ 第六条第十六号の許諾に関する記録
- ホ 認証業務用設備及び第四条各号の基準に適合するために必要な設備の維持管理に関する記録
- ヘ 事故に関する記録
- ト 帳簿書類の利用及び廃棄に関する記録

2 前項第一号から第三号までに掲げる帳簿書類は、当該帳簿書類に係る電子証明書の有効期間の満了日から十年間保存しなければならない。

3 第一項第四号に掲げる帳簿書類は、作成した日から認定の更新の日まで保存しなければならない。

4 第一項各号に掲げる帳簿書類（利用者又はその代理人の署名又は押印がない書類に限る。）は、電磁的方法による記録に係る記録媒体により保存することができる。

5 第一項各号に掲げる帳簿書類（前項に規定する書類を除く。）は、その原本を保存しなければならない。

（表示）

第十三条 法第十三条第一項の主務省令で定めるものは、次のとおりとする。

- 一 電子証明書
- 二 認証業務に関する利用者との契約に係る書類
- 三 第六条第十号の電子証明書の失効に関する情報及び同条第十三号の規程その他の認証業務に関する情報を提供するために作成する電磁的記録
- 四 認証業務に関する広告及び宣伝用物品
- 五 利用者が電子署名を行うために必要な物件その他の利用者に交付する物件
- 六 利用者の真偽の確認を行う認証事業者の営業所、事務所その他の事業場

2 法第十三条第一項の規定による表示は、様式第五により行うものとする。

（準用）

第十四条 第三条から第八条までの規定は法第十五条第一項の認定に、第九条から前条までの規定は認定外国認証事業者について準用する。

（公示）

第十五条 法第四条第三項（法第九条第三項（法第十五条第二項において準用する場合を含む。）及び法第十五条第二項において準用する場合を含む。）、法第十条第二項（法第十五条第二項において準用する場合を含む。）、法第十四条第二項及び法第十六条第二項の公示は、官報で告示することによって行う。

（身分証明書）

第十六条 法第三十五条第四項の証明書は、様式第六によるものとする。

（申請等の方法）

第十七条 法又はこの省令の規定による主務大臣に対する申請書等の提出は、総務大臣、法務大臣又は経済産業大臣のいずれかに、正本一通及び副本二通を提出することにより行うことができる。

2 法又はこの省令の規定により主務大臣に提出する書類のうち主務大臣が別に告示するものは、主務大臣が別に告示する電磁的方法による記録に係る記録媒体により提出することができる。

附 則

この省令は、平成十三年四月一日から施行する。

附 則（平成十五年三月二十四日総務省、法務省、経済産業省令第一号）
この省令は、平成十五年四月一日から施行する。

附 則（平成十五年四月十日総務省、法務省、経済産業省令第二号）
この省令は、平成十五年六月一日から施行する。

附 則（平成十五年六月二日総務省、法務省、経済産業省令第四号）
この省令は、公布の日から施行する。

附 則（平成十五年八月二十八日総務省、法務省、経済産業省令第五号）
この省令は、公布の日から施行する。

附 則（平成十六年四月九日 総務省、法務省、経済産業省令第一号）
この省令は、公布の日から施行する。

附 則（平成十七年二月二十八日 総務省、法務省、経済産業省令第一号）
この省令は、平成十七年三月七日から施行する。

別 表（第五条第一項関係）

運転免許証
 船員手帳
 海技免状
 小型船舶操縦免許証
 猟銃・空気銃所持許可証
 戦傷病者手帳
 宅地建物取引主任者証
 電気工事士免状
 無線従事者免許証
 認定電気工事従事者認定証
 特殊電気工事資格者認定証
 耐空検査員の証
 航空従事者技能証明書
 運航管理者技能検定合格証明書
 動力車操縦者運転免許証
 教習資格認定証
 検定合格証

■様式第1（第3条第1項及び第8条第1項関係）

様式第1（第3条第1項及び第8条第1項関係）

認定（更新）申請書

年 月 日

主務大臣 殿

申請者の住所
申請者の氏名又は名称及び法人 印
にあってはその代表者の氏名

電子署名及び認証業務に関する法律第4条第1項（第7条第1項、第15条第1項、第15条第2項において準用する同法第7条第1項）の認定（更新）を受けたいので、下記のとおり申請します。

記

1 申請に係る認証業務の名称
2 業務の用に供する設備の概要
3 業務の実施の方法

備考 1 不要の文字は、消除すること。
2 用紙の大きさは、日本工業規格A4とすること。
3 登録免許税を納めなければならない場合にあっては当該登録免許税の領収証書をこの申請書の裏面にはり付け、手数料を納めなければならない場合にあっては当該手数料の額に相当する収入印紙をこの申請書の左上に消印せずにはり付けること。
4 氏名を記載し、押印することに代えて、署名することができる。

■様式第2（第10条第1項関係）

様式第2（第10条第1項関係）

変更認定申請書

年 月 日

主務大臣 殿

申請者の住所
申請者の氏名又は名称及び法人 印
にあってはその代表者の氏名

電子署名及び認証業務に関する法律第9条第1項（第15条第2項において準用する同法第9条第1項）の変更の認定を受けたいので、下記のとおり申請します。

記

1 申請に係る認証業務の名称
2 変更の内容
3 変更の理由

備考 1 不要の文字は、消除すること。
2 用紙の大きさは、日本工業規格A4とすること。
3 手数料の額に相当する収入印紙をこの申請書の左上に消印せずにはり付けること。
4 氏名を記載し、押印することに代えて、署名することができる。

■様式第3（第10条第4項関係）

様式第3（第10条第4項関係）

変更届出書

年 月 日

主務大臣 殿

届出者の住所
届出者の氏名又は名称及び法人 印
にあってはその代表者の氏名

電子署名及び認証業務に関する法律第9条第4項（第15条第2項において準用する同法第9条第4項）の規定により、下記のとおり届け出ます。

記

1 届出に係る認証業務の名称
2 変更前の氏名等
3 変更後の氏名等
4 変更の理由大

備考 1 不要の文字は、消除すること。
2 用紙の大きさは、日本工業規格A4とすること。
3 氏名を記載し、押印することに代えて、署名することができる。

■様式第4（第11条関係）

様式第4（第11条関係）

廃止届出書

年 月 日

主務大臣 殿

届出者の住所
届出者の氏名又は名称及び法人 印
にあってはその代表者の氏名

認定に係る業務を廃止するので、電子署名及び認証業務に関する法律第10条第1項（第15条第2項において準用する同法第10条第1項）の規定により、下記のとおり届け出ます。

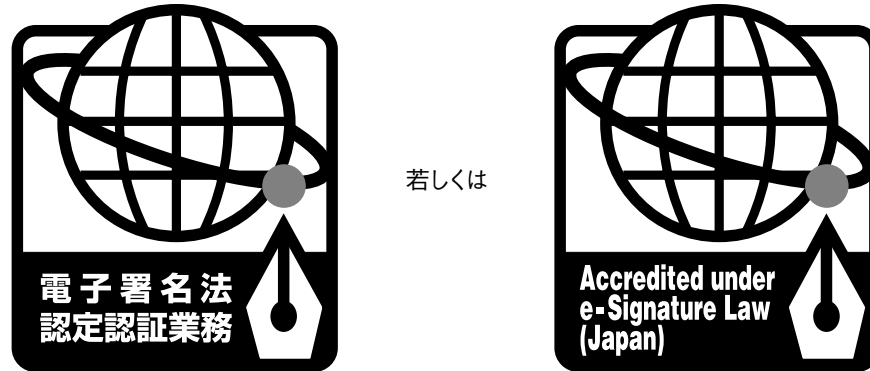
記

1 届出に係る認証業務の名称
2 廃止しようとする年月日
3 廃止の理由

備考 1 不要の文字は、消除すること。
2 用紙の大きさは、日本工業規格A4とすること。
3 氏名を記載し、押印することに代えて、署名することができる。

■様式第5（第13条第2項関係）

「電子署名法認定認証業務」若しくは「Accredited under e-Signature Law (Japan)」又は



- 注1 認定に係らない業務を認定に係る業務と誤認されるおそれがないように表示を付すること。
2 色彩は、適宜とする。

■様式第6（第16条関係）
（表）

番 号	
電子署名及び認証業務に関する法律第35条第4項の規定による	
立 入 検 査 証	
職 名 及 び 氏 名	
年 月 日交付	
発 行 者	印

備考 用紙の大きさは、日本工業規格B8とすること。

（裏）

電子署名及び認証業務に関する法律抜粋

第35条 主務大臣は、この法律の施行に必要な限度において、認定認証事業者に対し、その認定に係る業務に関し報告をさせ、又はその職員に、認定認証事業者の営業所、事務所その他の事業場に立ち入り、その認定に係る業務の状況若しくは設備、帳簿書類その他の物件を検査させ、若しくは関係者に質問させることができる。

2 主務大臣は、この法律の施行に必要な限度において、指定調査機関に対し、その業務に関し報告をさせ、又はその職員に、指定調査機関の事務所に立ち入り、業務の状況若しくは帳簿、書類その他の物件を検査させ、若しくは関係者に質問させることができる。

3 第1項の規定は認定外国認証事業者に、前項の規定は承認調査機関に、それぞれ準用する。

4 第1項及び第2項（それぞれ前項において準用する場合を含む。）の規定により立入検査をする職員は、その身分を示す証明書を携帯し、関係者に提示しなければならない。

5 第1項及び第2項（それぞれ第3項において準用する場合を含む。）の規定による立入検査の権限は、犯罪捜査のために認められたものと解釈してはならない。

第44条 次の各号のいずれかに該当する者は、30万円以下の罰金に処する。

三 第35条第1項の規定による報告をせず、若しくは虚偽の報告をし、又は同項の規定による検査を拒み、妨げ、若しくは忌避し、若しくは同項の規定による質問に対して答弁をせず、若しくは虚偽の答弁をした者

第45条 次の各号のいずれかに該当するときは、その違反行為をした指定調査機関の役員又は職員は、30万円以下の罰金に処する。

三 第35条第2項の規定による報告をせず、若しくは虚偽の報告をし、又は同項の規定による検査を拒み、妨げ、若しくは忌避し、若しくは同項の規定による質問に対して答弁をせず、若しくは虚偽の答弁をしたとき。

備考 用紙の大きさは、日本工業規格B8とすること。

A-4

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

総務省

法務省告示第二号

経済産業省

電子署名及び認証業務に関する法律（平成十二年法律第百二号）及び電子署名及び認証業務に関する法律施行規則（平成十三年 法務省令第二号）を実施するため、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を次のように定めたので、告示する。

平成十三年四月二十七日

総務大臣 片山虎之助
法務大臣 高村 正彦
経済産業大臣 平沼 赳夫

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

（目的）

第一条 この指針は、電子署名及び認証業務に関する法律（以下「法」という。）第二条第三項及び法第六条第一項各号（法第七条第二項（法第十五条第二項において準用する場合を含む。）、法第九条第三項（法第十五条第二項において準用する場合を含む。）及び法第十五条第二項において準用する場合を含む。）並びに電子署名及び認証業務に関する法律施行規則（以下「規則」という。）第二条及び規則第四条から第六条までに規定する認定の基準の細目を定めることにより、法の施行の円滑化を図ることを目的とする。

（用語）

第二条 この指針において使用する用語は、法及び規則において使用する用語の例による。

（特定認証業務に係る電子署名の基準）

第三条 規則第二条の基準を満たす電子署名の方式は、次の各号のいずれかとする。

- 一 RSA方式（オブジェクト識別子1 2 840 113549 1 1 5）又はRSA—PSS方式（1 2 840 113549 1 1 10）であって、モジュラスとなる合成数が1024ビット以上のもの
- 二 ECDSA方式（オブジェクト識別子1 2 840 10045 4 1）であって、楕円曲線の定義体及び位数が160ビット以上のもの
- 三 DSA方式（オブジェクト識別子1 2 840 40040 4 3）であって、モジュラスとなる素数が1024ビットのもの

(認証設備室への入出場を管理するために必要な措置)

第四条 規則第四条第一号に規定する入出場を管理するために業務の重要度に応じて必要な措置とは、次の各号に掲げる区分に応じ、それぞれ当該各号に定める要件を満たすものとする。

- 一 認証設備室（規則第四条第一号に規定する認証業務用設備が設置された室をいう。ただし、認証業務用設備のうち、登録用端末設備（専ら電子証明書の利用者を登録するために用いられる設備をいう。以下同じ。）又は利用者識別設備（専ら利用者情報（利用者に係る情報をいう。以下同じ。）及び利用者識別符号を識別するために用いられる設備をいう。以下同じ。）が設置されている場合においては、当該登録用端末設備又は利用者識別設備以外の認証業務用設備が設置されていない室を除く。以下同じ。） 次に掲げる要件を満たすこと。
 - イ 入室する二以上の者の身体的特徴の識別（あらかじめ登録された指紋、虹彩その他の個人の身体的特徴の照合を行うことをいう。）によって入室が可能となること。
 - ロ 入室者の数と同数の者の退室を管理すること。
 - ハ 入室のための装置の操作に不正常な時間を要した場合においては、警報が発せられること。
- 二 入室者及び退室者並びに在室者を自動的かつ継続的に監視し、及び記録するための遠隔監視装置及び映像記録装置が設置されていること。
- ニ 登録用端末設備又は利用者識別設備が設置された室であって、認証設備室に該当しないもの 関係者以外が容易に登録用端末設備又は利用者識別設備に触れることができないようにするための施錠等の措置が講じられていること。

(認証業務用設備への不正なアクセス等を防止するために必要な措置)

第五条 規則第四条第二号に規定する電気通信回線を通じた不正なアクセス等を防止するために必要な措置とは、次の各号に掲げるものをいうものとする。

- 一 認証業務用設備が電気通信回線に接続している場合においては、認証業務用設備（登録用端末設備を除く。）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ファイアウォール及び不正なアクセス等を検知するシステムを備えること。
- 二 認証業務用設備が二以上の部分から構成される場合においては、一の部分から他の部分への通信に関し、送信をした設備の誤認並びに通信内容の盗聴及び改変を防止する措置
- 三 利用者署名検証符号、利用者情報及び利用者識別符号を電気通信回線を通じて受信するために用いられる電子計算機が設置されている場合においては、当該電子計算機から認証業務用設備への通信に関し、送信をした当該電子計算機の誤認並びに通信内容の盗聴及び改変を防止する措置

(正当な権限を有しない者による認証業務用設備の作動を防止するための措置等)

第六条 規則第四条第三号に規定する正当な権限を有しない者によって作動させられることを防止するための措置とは、次の各号に掲げる要件を満たすものとする。

- 一 認証業務用設備を操作者によって作動させる場合においては、各操作者に対する権限の設定並びに当該操作者及びその権限の確認ができること。
- 二 認証業務用設備を利用者情報及び利用者識別符号の識別によって自動的に作動させる場合においては、各利用者に対する利用者識別符号の設定、利用者署名検証符号、利用者情報及び当該利用者識別符号を電気通信回線を通じて受信するために用いられる電子計算機（施錠等の措置が講じられた

室に設置されたものに限る。)の設置、当該電子計算機から電気通信回線を通じて送信された当該利用者情報及び当該利用者識別符号を識別する機能の設定並びに当該利用者情報及び利用者識別符号の確認ができること。

- 三 電気通信回線経由の遠隔操作が不可能であるように設定されていること。ただし、電子証明書の発行及び失効の要求その他の電子証明書の管理に必要な登録用端末設備の操作については、この限りでない。
- 四 認証業務用設備の所在を示す掲示がされていないこと。

2 規則第四条第三号に規定する認証業務用設備の動作を記録する機能とは、次の各号に掲げるものをいうものとする。

- 一 各動作の要求者名（操作者によって作動させる場合に限る。）、内容、発生日時、結果等を履歴として記録する機能
- 二 特定の操作者による操作の履歴のみを表示することができる機能（操作者によって作動させる場合に限る。)

(認証業務用設備等の災害の被害を防止するために必要な措置)

第七条 規則第四条第五号に規定する停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて必要な措置とは、次の各号に掲げる区分に応じて、当該各号に定める要件を満たすものをいうものとする。

- 一 認証業務用設備 通常想定される規模の地震による転倒及び構成部品の脱落等を防止するための構成部品の固定その他の耐震措置が講じられていること。
- 二 認証設備室 次に掲げる要件を満たすこと。
 - イ 水害の防止のための措置が講じられていること。
 - ロ 隔壁により区画されていること。
 - ハ 自動火災報知器及び消火装置が設置されていること。
 - ニ 防火区画内に設置されていること。
 - ホ 室内において使用される電源設備について停電に対する措置が講じられていること。
- 三 認証設備室を設置する建築物 次に掲げる要件を満たすこと。

- イ 建築されている土地の地盤が地震被害のおそれの少ないものであること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。
- ロ 地震に対する安全性に係る建築基準法（昭和二十五年法律第二百一号）又はこれに基づく命令若しくは条例の規定に適合する建築物であること。
- ハ 建築基準法に規定する耐火建築物又は準耐火建築物であること。

(利用申込者に対する説明事項)

第八条 規則第六条第一号に規定する利用申込者に対して説明を行うべき事項とは、次の各号に掲げる事項を内容として含むものとする。

- 一 認定認証業務においては、虚偽の利用の申込みをして、利用者について不実の証明をさせた者は、法第四十一条の規定により罰せられること。
- 二 電子署名は自署や押印に相当する法的効果が認められ得るものであるため、利用者署名符号については、十分な注意をもって管理する必要があること。
- 三 利用者署名符号が危殆化（盗難、漏えい等により他人によって使用され得る状態になることをいう。以下同じ。）し、又は危殆化したおそれがある場合、電子証明書に記録されている事項に変更が生じた場合又は電子証明書の利用を中止する場合においては、遅滞なく電子証明書の失効の請求を行わなければならないこと。
- 四 認定認証業務に係る電子証明書を使用する場合における電子署名のためのアルゴリズムは、認証事業者が指定したものを使用する必要があること。

(利用申込書等の記載事項等)

第九条 規則第六条第二号の利用申込書その他の書面又は利用の申込みに係る情報は、次の各号に掲げる事項の記載又は記録を含むことを要するものとする。

- 一 利用申込者の氏名、住所、生年月日
- 二 利用の申込みをする電子証明書の用途
- 三 利用申込者の氏名のローマ字表記
- 四 利用申込者の自筆署名又は利用者の真偽の確認の方法として印鑑登録証明書を用いる場合においては、当該証明書に係る印鑑による押印（利用の申込みに係る情報の送信の場合を除く。）
- 五 代理人が申込みをする場合においては、前各号に掲げる事項に加え、代理人の氏名及び自筆署名又は印鑑登録証明書に係る印鑑による押印（代理人の真偽の確認の方法として印鑑登録証明書を用いる場合に限る。）並びに代理人による申込みの理由

(認定認証業務と他の業務との誤認を防止するための措置)

第十条 規則第六条第七号に規定する利用者その他の者が認定認証業務と他の業務を誤認することを防止するための適切な措置には、次の各号に掲げる措置が含まれるものとする。

- 一 発行者署名符号を認定認証業務以外の業務のために使用しないこと。ただし、次に掲げる場合を除く。
 - イ 他の認定認証業務その他認定認証業務と同程度以上の基準に従って国又は地方公共団体等が実施する認証業務との相互認証の実施のための使用
 - ロ 当該認証業務の維持管理のために必要な場合における使用
- 二 発行者署名検証符号に係る電子証明書の値を SHA-1 で変換した値によって認定認証業務を特定すること。

(署名検証者への情報提供)

第十一条 規則第六条第九号に規定する必要な情報は、次の各号に掲げる事項を含むことを要するものとする。

- 一 署名検証者は、電子証明書を信頼すべきか否かの判断をするときは、発行者署名検証符号を確実に入手し、当該電子証明書に行われた発行者による電子署名を検証することにより、当該電子証明書の発行者を確認すべきであること。
- 二 署名検証者は、電子証明書を信頼すべきか否かの判断をするときは、当該電子証明書の利用目的若しくは使用範囲又はその制限（利用者にあらかじめ通知されている利用条件を含む。）を確認すべきであること。
- 三 署名検証者は、適切な手段により、電子証明書について失効に関する情報が記録されていないことを確認すべきであること。

(認証業務の実施に関する規程)

第十二条 規則第六条第十三号に規定する認証業務の実施に関する規程は、次の各号に掲げる事項に関する規定を含むことを要するものとする。

- 一 認証事業者の名称及び連絡先（住所、電話番号、ファクシミリ番号及びメールアドレス）
- 二 証明の目的、対象又は利用範囲について制限を設ける場合においては、その制限に関する事項
- 三 認定事業者が負担する保証又は責任の範囲について制限を設ける場合においては、その制限に関する事項
- 四 利用申込みの方法及び利用者の真偽の確認の方法に関する事項
- 五 電子証明書の失効の請求に関する事項
- 六 電子証明書の失効に関する情報の確認の方法及び確認することができる期間に関する事項
- 七 認証業務に係るセキュリティに関する事項（利用者に係る個人情報の取扱いに関する事項を含む。）
- 八 認証業務の利用に係る料金に関する事項
- 九 帳簿書類の保存に関する事項
- 十 業務の廃止に関する事項
- 十一 認証事業者との間で係争が生じた場合に適用される法令及び解決のための手続に関する事項
- 十二 当該規程の改訂に関する事項及び利用者その他の者に対する通知方法に関する事項

2 前項第十号に掲げる事項には、認定に係る業務を廃止する日（認定の更新を受けない場合においては、認定期間の満了の日。以下同じ。）の六十日前までにその旨を利用者に通知すること（法第十四条第一項の規定により認定を取り消された場合等、やむを得ない場合はこの限りでない。）及び認定に係る業務を廃止する日までに利用者に対して発行した電子証明書について失効の手続を行うことが含まれるものとする。

(認証業務用設備の操作等に関する許諾等)

第十三条 規則第六条第十六号に規定する認証業務用設備が設置された室への立入り及びその操作に関する許諾並びに当該許諾に関する識別記号の管理が適切に行われていることとは、次の各号に掲げる要件を満たすことを要するものとする。

- 一 認証設備室への立入りは、複数の者により行われること。
- 二 設備の保守その他の業務の運営上必要な事情により、やむを得ず、立入りに係る権限を有しない者を認証設備室へ立ち入らせることが必要である場合においては、立入りに係る権限を有する複数の者が同行すること。
- 三 システム管理者に係る識別符号については、特に厳重な管理が行われていること。

(発行者署名符号の漏えいを防止するために必要な措置)

第十四条 規則第六条第十七号に規定する発行者署名符号の漏えいを防止するために必要な措置とは、次の各号に掲げる要件を満たすものをいうものとする。

- 一 発行者署名符号の生成及び管理は、認証設備室内で複数の者によって規則第四条第四号に規定する専用の電子計算機を用いて行われること。
- 二 バックアップ用の発行者署名符号の複製は、次に掲げるいずれかの方法により行われること。
 - イ 認証設備室内で規則第四条第四号に規定する専用の電子計算機を用いて行われ、かつ、複製されたバックアップ用の発行者署名符号は、認証設備室と同等の安全性を有する場所に保存されること。
 - ロ 認証設備室内で発行者署名符号に関する情報を分割し、複数の者が異なる安全な場所に分散して保管する方法（発行者署名符号を再生する場合には、複数の者が集合することを要するものに限る。）により行われること。
- 三 発行者署名符号の使用を可能とし、又は不可能とするための認証業務用設備の設定の変更は、認証設備室内で複数の者により行われること。
- 四 発行者署名符号の使用を終了する場合には、複数の者により物理的な破壊又は完全な初期化等の方法により完全に廃棄し、かつ、複製された発行者署名符号についても同時に廃棄すること。

附 則

この指針は、平成十三年四月一日から適用する。

総務省

附 則（平成十四年十一月二十一日 法務省告示第十三号）

経済産業省

- 1 この告示は、公布の日から施行する。
- 2 この告示の施行の際現に電子署名及び認証業務に関する法律（平成十二年法律第百二号。以下この項において「法」という。）第四条第一項の認定を受けている者については、次の各号に掲げる規定の適用に関しては、この告示の施行の日から当該各号に定める期間はなお従前の例による。
 - 一 改正後の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（次号において「新指針」という。）第三条第一号 一年間

二 新指針第十条第二号 法第七条第一項の認定の更新を受けるまでの期間

総務省

附 則（平成十五年六月二日法務省告示第九号）

経済産業省

この告示は、公布の日から施行する。

A-5

電子署名及び認証業務に関する法律に基づく
指定調査機関の調査に関する方針

平成15年6月2日
総務省情報通信政策局
法務省民事局
経済産業省商務情報政策局

電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針

第1 趣旨等

1. 趣旨

本方針は、電子署名及び認証業務に関する法律に基づく指定調査機関の調査方針を明確化することにより、特定認証業務の認定制度の円滑な運営に資するためのものである。

2. 用語

本方針中、「法」とあるのは、「電子署名及び認証業務に関する法律（平成12年法律第102号）」を、「規則」とあるのは、「電子署名及び認証業務に関する法律施行規則（平成13年総務・法務・経済産業省令第2号）」を、「指針」とあるのは、「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」をいう。

第2 認証業務の用に供する設備関係

1. 総論

法第6条第1項第1号、規則第4条及び指針第4条から第7条までに規定する認証業務の用に供する設備の基準に適合するとは、審査の時点における技術水準等にかんがみ、基準を満たす設備が設置されているのみならず、特定認証業務を適正、円滑かつ安全に行うことができる水準であり、かつ、その実現のため合目的に措置されているものであることをいう。

2. 暗号装置関係

(1) 規則第4条第4号に規定する「専用の電子計算機」（以下「暗号装置」という。）とは、発行者署名符号の漏洩、破損、消失等の事象の発生を可能な限り低い確率に抑えるための以下の機能を備えたものをいう。

ア 暗号化されていない状態の暗号符号や認証データ等、保護されていない形式の重要なデータに係る暗号装置への入出力が行われるインタフェースが存在する場合は、そのインタフェースは他のデータの入出力を行うインタフェースとは物理的に独立したものであること。

イ 暗号装置は、以下の機能を有するものであるとともに、暗号装置の操作者ごとに機能ごとの権限の有無が特定されているものであること。

(ア) 操作者機能：暗号化、署名等、通常の暗号化機能を実施するための機能

(イ) 管理者機能：暗号装置自体の初期化、署名符号などの重要パラメータの投入等、暗号装置を管理するための機能
ウ 発行者署名符号等のデータの盗難を回避するため、暗号装置は、以下のいずれかの物理的なセキュリティ対策が講じられていること。

(ア) 暗号装置がICチップ単体からなる場合、ICチップが強固で除去困難な材質の不透明なコーティングで覆われていること。

(イ) 暗号装置にカバーが施されている場合、物理的な侵入行為に対し、暗号装置の機能の停止、内部データの無効化等の耐タンパ対策が講じられていること。

(ウ) 暗号装置の筐体に排気用スリットもしくは空孔が存在する場合、それらは十分小さく、かつ、検出されずに筐体の中をプローブされることを防止する対策が講じられていること。

エ 暗号装置に係る発行者署名符号の管理に関し、以下の措置が講じられていること。

(ア) 暗号装置内で発行者署名符号の生成を行う場合、安全な擬似乱数生成アルゴリズムを用いるものであること。

(イ) 暗号装置への発行者署名符号の入出力を行う場合には、以下のいずれかの方式であること。

① 発行者署名符号は暗号化された上で入出力されること。

② 発行者署名符号を2つ以上の構成要素に分割して入出力を行う場合は、暗号装置に対して直接行うこととし、発行者署名符号の各構成要素に対する操作者の認証が行われること。また、発行者署名符号の各構成要素は、暗号装置内で分割、結合されること。

(ウ) 発行者署名符号を暗号化されていない状態で暗号装置内に保管する場合は、外部からアクセスできない仕組みとすること。

(エ) 発行者署名符号を廃棄する際には、発行者署名符号その他のセキュリティパラメータを無効化する機能を有すること。

(2) 上記(1)にかかわらず、暗号装置を設置する電子計算機のオペレーティングシステム等が以下の機能・要件を満たし、認証業務用設備及び認証設備室全体のセキュリティ対策を講ずることにより同等の安全性が確保できる場合には、これに代えることができる。

ア 暗号装置を駆動するためのソフトウェア類は、実行可能コードのみの形でインストールされていること。

イ 暗号ソフトウェア、署名符号その他の重要なセキュリティパラメータ、制御情報、状態情報等は、入出力を監査するための機能を備えるオペレーティングシステムの管理下にあること。

ウ 署名符号、認証データその他の重要なセキュリティパラメータ等を不正なアクセス等から保護するための機能を有するオペレーティングシステムが用いられていること。

エ 上記(1)アの物理的に独立したインタフェースに関する事項を満たさない場合、重要なデータの入出力は暗号装置を設置する計算機のオペレーティングシステム等により他のデータと混じることのないよう安全な方法で実施されること。

オ 上記(1)イのうち、操作者ごとの権限の特定ができない場合、暗号装置を設置する電子計算機のオペレーティングシステム等により操作者の特定が行えること。

カ 暗号装置の耐タンパ対策が以下のいずれかの場合、非作動中の装置の安全な場所への保管、電子計算機の物理的な攻撃に対する監視機器等でのモニタ及び論理的な攻撃に対する電子計算機のオペレーティングシステム等で保護されていること。

(ア) ICチップが、不正なアクセス等が試みられたことを検知可能な不透明のコーティングで覆われていること。

(イ) 暗号装置が不透明な筐体でカバー等が施されており、不正なアクセス等が試みられたことを検知可能な不透明のコーティングで覆われていること。

キ 上記(1)エ(イ)に関し、暗号装置を設置する電子計算機のオペレーティングシステム等により、上記(1)エ(イ)①及び②の方式以外では、入出力できないよう措置されること。

第3 認証業務の利用者の真偽の確認方法関係

1. 総論

認定認証事業者は、規則第5条に規定する利用者の真偽の確認の方法のうち、自己の業務において採用する方法及びその方法において使用する利用者の真偽の確認のための資料の種類をあらかじめ特定することができるものとする。

2. 利用者の真偽の確認の手続

- (1) 利用者の真偽を確認するにあたっては、利用者の真偽を確認するための資料が記載内容、形式、有効期限等において真正であることを確認するものとする。
- (2) 代理人による利用申込みの場合において提出を求める委任状とは、利用者が代理人に対し委任する利用申込みの内容が明確に記されているものをいう。
- (3) 利用者の真偽の確認と利用者からの利用者署名検証符号の受領とを同時に行わない場合においては、利用者署名検証符号の提出者と真偽の確認を行った利用者が一致することを、利用者識別符号（真偽の確認をした利用者以外には知り得ない情報）を当該利用者に渡す方法などにより確認を行うものとする。
- (4) 電子証明書の更新時における利用者の真偽の確認を規則第5条第2項の規定により行う場合においては、利用の申込みに係る情報に講じられた利用者の電子署名を検証し、当該電子署名に係る電子証明書について失効に関する情報が記録されていないことを確認するものとする。
- (5) 利用者の真偽の確認を行うにあたって疑義が生じた場合においては、あらかじめ文書等をもって定められた手続に従って、利用者の真偽の確認の手続を行うものとする。

第4 認証業務の実施の方法（利用者の真偽の確認方法を除く。）関係

1. 総論

法第6条第1項第3号、規則第6条及び指針第8条から第14条までに規定する認証業務の実施の方法に関する基準に適合するとは、審査の時点における技術水準等にかんがみ、特定認証業務を適正、円滑かつ安全に行うことができる水準で基準の要件を満たしていることをいい、基準を満たす方法により業務を実施すべきことが認証業務の手順等を定めた文書等において明確に定められており、かつ、その内容がすべての就業者に役割に応じて理解され、実施され、かつ、維持されていることをいう。

2. 認定認証事業者による利用者署名符号及び利用者識別符号の生成等

- (1) 規則第6条第3号に規定する「利用者署名符号を認証事業者が作成する場合」においては、次の措置を含むものとする。
 - ア 利用者署名符号の生成は、認証設備室内又は同等の安全性が確保できる環境において複数人で行われること。
 - イ 当該利用者署名符号の転送や出力等の取扱いは、生成時と同等の安全性が確保された環境で行われること。
 - ウ 当該利用者署名符号を利用者に交付又は送付したときは、利用者から受領書又はこれに準ずるものを受領すること。
- (2) 規則第6条第3号の2に規定する「利用者署名符号を利用者が作成する場合において、当該利用者署名符号に対応する利用者署名検証符号を認証事業者が電気通信回線を通じて受信する方法によるとき」においては、次の措置を含むものとする。
 - ア 当該利用者の識別に用いる利用者識別符号は、安全な疑似乱数生成アルゴリズムを用いて生成するものとし、認証設備室又は同等の安全性が確保できる環境において、複数人で行われること。

- イ 利用者へ電子証明書を発行する際には、利用者識別符号の受領の確認が行われていること。
- ウ 利用者識別符号は、認証設備室又は同等の安全性が確保できる環境に暗号化等の措置を講じて保管すること。
- エ 利用者が利用者識別符号を送信する際には、当該符号を受信する電子計算機の誤認並びに通信内容の盗聴及び改変を防止する措置が行われていること。
- オ 利用者の識別に用いた利用者識別符号がそれ以降の識別処理に用いられないような措置を直ちに講ずること。

3. 利用者署名符号の保有の確認

規則第6条第5号二に規定する電子証明書に記録する利用者署名検証符号は、利用者署名符号によって行われた電子署名を当該利用者署名検証符号を用いて検証する等の方法により、利用者が当該利用者署名検証符号に対応する利用者署名符号を保有していることを確認するものとする。

4. 利用者に係る属性等の証明

電子証明書に記録された利用者の役職等についての証明が法による認定の対象外である旨を記録した情報の参照先を当該電子証明書に記載することは、規則第6条第8号に規定する「利用者の役職名その他の利用者の属性（利用者の氏名、住所及び生年月日を除く。）についての証明を認定認証業務に係るものであると誤認することを防止するための適切な措置」に該当するものとする。

5. 発行者署名検証符号等の情報の提供の方法

電子証明書に発行者署名検証符号その他必要な情報の参照先を記録することは、規則第6条第9号に規定する「発行者署名検証符号その他必要な情報を容易に入手することができるようにするための措置」に該当するものとする。

6. 電子証明書の失効に関する手続

- (1) 認証事業者は、電子証明書の失効の手続を行ったときは、遅滞なく規則第6条第11号の措置を講ずるものとする。
- (2) 規則第6条第11号に規定する「失効に関する情報を容易に確認することができる」とは、失効の記録がされた電子証明書を記録した電子証明書失効リストの開示、オンラインによる電子証明書状態確認プロトコルによる電子証明書の状態（失効に関する記録等が記録されているか否か）についての情報の提供その他これらと同等の機能を有するような措置を講ずることをいう。

7. 利用者の真偽の確認のために用いられた書類等の開示

規則第6条第14号の規定により利用者の真偽の確認のために用いられた書類等を開示する場合においては、開示の請求をした者が請求に係る書類に基づいて発行された電子証明書の名義人であることを確認するものとする。

8. 業務の手順等に係る規程関係

- (1) 規則第6条第15号二に規定する「業務の監査に関する事項」とは、認証業務が、規則第6条第13号に規定する規程及び規則第6条第15号イに規定する業務の手順等に基づき、適正に運営されていることを確認するための監査に係る基準をいい、当該監査の結果及びセキュリティ対策技術の最新の動向を踏まえ、設備及び規程等の見直しが適切に行われることとされているものをいう。
- (2) 規則第6条第15号へに規定する「利用者の真偽の確認に際して知り得た情報の目的外使用の禁止のために必要な措置」とは、以下のものをいう。
 - ア 個人情報の取扱い及び保護に関する規定が明確に定められていること。

- イ 当該情報の取扱いの方法、電子証明書への記載範囲について利用者の承認を受けること。

(3) 規則第6条第15号トに規定する「危機管理に関する事項」とは、発行者署名符号の危殆化又は災害等による障害の発生に対する対応策及び回復手順であって、以下の事項を含むものをいう。

- ア 発行者署名符号が危殆化し、又は危殆化したおそれがある場合には、直ちに発行したすべての電子証明書について失効の手続を行うこと。
- イ 発行者署名符号の危殆化又は災害等による障害の発生の実事を利用者に通知し、かつ、署名検証者に開示すること及びその方法
- ウ 発行者署名符号が危殆化し、又は危殆化したおそれがある場合及び災害又は認証業務用設備の故障等により署名検証者に対する電子証明書の失効に係る情報の提供が規則第6条第13号に規定する認証業務の実施に関する規程に定める時間を超えて停止し、かつ、署名検証者に対しその停止の実事の開示が行われなかった場合においては、直ちに、当該障害の内容、発生日時、措置状況等確認されている事項を主務大臣に通報すること。

9. 認定認証業務を特定するための措置

指針第10条第2号に規定する「発行者署名検証符号に係る電子証明書の値をSHA-1で変換した値によって認定認証業務を特定すること」とは、認定認証業務で用いられる発行者署名符号に対応する発行者署名検証符号を記録した電子証明書の値についてハッシュ関数SHA-1で変換することにより得られる値を用いて、利用者その他の者が認定認証業務を特定できるような措置をいい、かつ、改ざん防止措置が施されて公開されることが含まれるものとする。

第5 認証業務の実施に関する規程関係

- (1) 規則第6条第13号に規定する「認証業務の実施に関する規程」には、指針第12条に掲げる事項のほか、電子証明書の様式、その記録に係る基準、記録に用いる言語並びに記録する事項に係る項目及びその内容を規定するものとする。
- (2) 指針第12条第1項第5号に規定する「電子証明書の失効の請求に関する事項」には、電子証明書の失効事由（認証事業者の行為に起因するものを含む。）、失効の請求の方式、失効の請求書又は請求情報に記載又は記録すべき事項、請求者の真偽の確認の方法、失効に関する情報の記録の手続、失効に関する業務の処理のサイクル等が含まれるものとする。
- (3) 指針第12条第1項第6号に規定する「電子証明書の失効に関する情報の確認の方法及び確認することができる期間に関する事項」には、公開される失効に係る情報の内容、公開の方法及びその更新の周期、失効に係る電子証明書の利用者への通知の方法、有効期間の経過後に署名検証者から電子証明書の失効に関する情報について照会を受けた場合の対応方法等が含まれるものとする。
- (4) 指針第12条第1項第7号に規定する「認証業務に係るセキュリティに関する事項（利用者に係る個人情報の取扱いに関する事項を含む。）」には、当該認証業務が採用しているセキュリティ基準、技術標準等に関する事項が含まれるものとする。

第6 帳簿等の保存関係

1. 総論

- (1) 規則第12条第1項各号に掲げる帳簿書類中、利用の申込書又は電子証明書の失効の請求書その他の利用者等から提出される書類又は送信される情報については、その受領の日付及び受領をした者の識別に関する情報が関連づけられて記録されていることとする。
- (2) 規則第12条第1項各号中、電子証明書の作成に関する記録その他の認証業務の実施に関する記録については、その実施の日付並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報が関連づけられて記録されていることとする。

2. 認証業務の利用の申込みに関する帳簿書類

(1) 規則第12条第1項第1号チに規定する「発行者署名符号の作成及び管理に関する記録」とは、上記1.(2)の実施の日付並びに当該業務を実施した者及び当該業務について責任を有する者の識別に関する情報のほか、主務大臣又は法第17条第1項の指定を受けた者が認定の更新時において、発行者署名符号の作成及び管理法、規則及び指針に従って行われていることを調査するために必要となる記録であって、以下に関するものをいう。

- ア 発行者署名符号の使用範囲の規定
- イ 発行者署名符号の生成、保存
- ウ 発行者署名符号の使用を可能とし、又は不能とする認証業務用設備の設定の変更
- エ 発行者署名符号のバックアップ
- オ 発行者署名符号の復元
- カ 発行者署名符号の廃棄

(2) 規則第12条第1項第1号リに規定する「利用者からの受領書」とは、利用の申込書等で確認できる自筆署名又は押印、あるいは電子署名が付されたものをいう。

3. 電子証明書の失効に関する帳簿書類

規則第12条第1項第2号イに規定する「失効に関する判断に関する記録」とは、電子証明書の失効の請求者の真偽の確認に使用した資料を含むものをいう。

4. 認証事業者の組織管理に関する帳簿書類関係

- (1) 規則第12条第1項第3号ハの記録とは、認証業務に従事する要員に関する組織図又は体制図を含むものをいう。
- (2) 規則第12条第1項第3号ホに関する記録とは、監査実施記録（不定期に実施される監査を含む）、監査報告書（定期的に実施される監査に関するもの）及び監査結果に基づく是正処置報告書をいう。

5. 設備及び安全対策措置に関する帳簿書類関係

- (1) 規則第12条第1項第4号イの記録とは、入退室の日時及び場所、入退室者の識別に関する情報並びに入退室に係る装置の操作の記録及び警報に関する記録を含むものをいう。
- (2) 規則第12条第1項第4号ロの記録とは、ファイアウォール及び侵入検知システムの履歴のうち、異常な状態を示す記録（異常発生の日時、送信元電子計算機のIPアドレス、宛先電子計算機のIPアドレス、使用した通信プロトコル等）を含むものをいう。
- (3) 規則第12条第1項第4号ハの記録とは、認証業務用設備の動作に関する記録のうち、通常の業務に係る操作以外の操作に関する記録及び障害に関するものをいう。
- (4) 規則第12条第1項第4号ニの記録とは、許諾の態様ごとに作成された許諾に係る規定に基づく権限管理の実施の記録を含むものをいう。
- (5) 規則第12条第1項第4号ホの記録とは、設備の保守に関する記録及びシステムの変更に関する履歴を含むものをいう。

- (6) 規則第12条第1項第4号への記録とは、認証設備室への不正な侵入、認証設備の停止若しくは不正な操作及び認証設備室の入退室管理装置の停止若しくは不正な操作に関する記録（ファイアウォール及び侵入検知システムの履歴のうち、異常な状態を示す記録を除く。）、それらの障害に関する報告書及びその復旧に関する報告書を含むものをいう。

6. 電磁的方法による記録

規則第12条第4項に規定する「電磁的方法による記録に係る記録媒体」による保存とは、以下のいずれかの要件を満たす方法による保存をいう。

- ア 当該記録媒体の内容を表示することができるように、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを維持・保存しておくこと。特に、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを更新する場合は、当該記録媒体との互換性を確保すること等により、表示不能を生じさせないこと。
- イ 当該記録媒体の利用が困難になることが予想される等の場合には、別種の記録媒体に複写したものを保存することを妨げない。ただし、その際、保存内容の完全性及び機密性を損なわないための十分な配慮がなされていること。

RFC3280に記載してある、電子証明書プロファイルの主な項目について記述する。

利用者が電子証明書を利用する際には、電子証明書の記載内容を事前に確認する必要がありますが、特に重要な項目としては、subject（利用者名）、subjectAltName（利用者別名）、validity（有効期間）、issuer（発行者名）などがある。詳細は、RFC3280を参照して下さい。

利用者証明書の項目例

英文項目名	日本語項目名（仮訳）	項目説明
基本領域		
version	電子証明書形式のバージョン	X.509の電子証明書形式バージョン 例 2(X.509ver3を表す)
serialNumber	発行番号	電子証明書をユニークに識別する番号
signature	署名アルゴリズム	電子証明書に署名する際に利用する署名アルゴリズムのOID 例 1.2.840.113549.1.1.5 (sha1WithRSA)
issuer	発行者名	発行者を識別する情報 C(国名:countryName) 例 JP(日本) O(組織:organizationName) OU(組織の部門:organizationalUnitName) CN(発行者の名称commonName)など
validity notBefore Time notAfter Time	有効期間	電子証明書の有効期間 (有効となる開始時間と有効でなくなる終了時間)
subject	利用者名	利用者を識別する情報 C(国名:countryName) 例 JP(日本) ST(都道府県名:stateOrProvinceName) L(市町村以下の住所localityName) CN(利用者の氏名commonName) など
subjectPublicKeyInfo algorithm subjectPublicKey	利用者の公開鍵情報	公開鍵のアルゴリズム名と公開鍵 例 1.2.840.113549.1.1.1 (RSAEncryption)、 公開鍵のビット列
拡張領域		
authorityKeyIdentifier	認証局鍵識別子	認証局の電子証明書の確認に用いる識別子 例 認証局の公開鍵の(SHA-1などの)ハッシュ値
subjectKeyIdentifier	利用者鍵識別子	利用者の電子証明書の確認に用いる識別子 例 利用者の公開鍵の(SHA-1などの)ハッシュ値
keyUsage	鍵の用途	秘密鍵の用途 例 デジタル署名(digitalSignature)、否認防止(nonRepudiation)
certificatePolicies	証明書ポリシー	証明書ポリシーのOIDやその公開場所
subjectAltName	利用者別名	subject(利用者名)の代替名称 subjectでローマ字表記し、subjectAltNameで日本語表記する例がある。
issuerAltname	発行者別名	issuer(発行者)の代替名称 issuerでローマ字表記し、issuerAltnameで日本語表記する例がある。
CRLDistributionPoints	CRL配布点	CRL(電子証明書失効リスト)があるディレクトリへのエントリ名

B-2

電子証明書のプロファイル

RFC3280に記載してある、CRLプロファイルの主な項目について記述する。

詳細はRFC3280を参照して下さい。

英文項目名	日本語項目名(仮訳)	項目説明
基本領域		
version	電子証明書形式のバージョン	X.509の電子証明書形式のバージョン 例 1(X.509ver2を表す)
signature	署名アルゴリズム	CRLに署名する際に利用する署名アルゴリズムのOID 例 1.2.840.113549.1.1.5(sha1WithRSA)
issuer	CRLの発行者	CRL発行者を識別する情報 C(国名:countryName) 例 JP(日本) O(組織:organizationName) OU(組織の部門:organizationalUnitName) CN(発行者の名称commonName) など
thisUpdate	CRLの発行日時	CRLの発行日時
nextUpdate	CRLの次回発行予定日時	CRLの次回発行予定日時
revokedCertificates userCertificate revocationDate reasonCode	失効証明書の情報 電子証明書の発行番号 失効日時 失効理由	失効された電子証明書の情報(該当電子証明書の発行番号・失効日時・失効理由)が失効された電子証明書の数繰り返される。
拡張領域		
authorityKeyIdentifier	CRLの発行者鍵識別子	CRLに署名した認証局の確認に用いる識別子
CRLNumber	CRLの発行番号	CRLを識別する番号
issuingDistribution	CRLの配布点	CRL(電子証明書失効リスト)があるディレクトリへのエントリ名

その他CRLの拡張領域の項目としては、issuerAltnameとdeltaCRLIndicatorがある。



CPSの構成案

RFC2527には、CP/CPS等の目次案として、次のような項目を記述している。

利用者は、CP/CPSの記載内容を事前に確認する必要がありますが、特に重要な項目としては、以下の項目などがある。

- 1.4 Contact Details(連絡先)、2.1 Obligations(義務)、2.2 Liability(責任)、
- 2.5 Fees(料金)、2.6 Publication and Repository(公表とリポジトリ)、
- 3.1 Initial Registration(初期登録)、3.2 Routine Rekey(電子証明書の更新)、
- 3.4 Revocation Request(電子証明書の失効請求)、4.1 Certificate Application(電子証明書の適用)、
- 4.2 Certificate Issuance(電子証明書の発行)、4.3 Certificate Acceptance(電子証明書の受け入れ)、
- 4.4 Certificate Suspension and Revocation(電子証明書の一時的停止と失効)、
- 7.1 Certificate Profile(電子証明書プロファイル)、7.2 CRL Profile(CRLプロファイル)

詳細はRFC2527を参照して下さい。

英文目次	日本語目次(仮訳)
1. INTRODUCTION	概説
1.1 Overview	概要
1.2 Identification	識別
1.3 Community and Applicability	コミュニティと適用範囲
1.4 Contact Details	連絡先
2. GENERAL PROVISIONS	一般規定
2.1 Obligations	義務
2.2 Liability	責任
2.3 Financial responsibility	財務的な責任
2.4 Interpretation and Enforcement	解釈と執行
2.5 Fees	料金
2.6 Publication and Repository	公開とリポジトリ
2.7 Compliance audit	準拠性監査
2.8 Confidentiality	機密保持
2.9 Intellectual Property Rights	知的財産権
3. IDENTIFICATION AND AUTHENTICATION	識別と認証
3.1 Initial Registration	初期登録
3.2 Routine Rekey	電子証明書の更新
3.3 Rekey after Revocation	電子証明書失効後の再発行
3.4 Revocation Request	電子証明書の失効請求
4. OPERATIONAL REQUIREMENTS	運用要件
4.1 Certificate Application	電子証明書の申請
4.2 Certificate Issuance	電子証明書の発行
4.3 Certificate Acceptance	電子証明書の受領確認
4.4 Certificate Suspension and Revocation	電子証明書の一時的停止と失効
4.5 Security Audit Procedures	セキュリティ監査手続き
4.6 Records Archival	記録(アーカイブ)
4.7 Key changeover	鍵更新
4.8 Compromise and Disaster Recovery	危殆化と災害の対応
4.9 CA Termination	認証局の終了

英文目次	日本語目次 (仮訳)
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	物理的、手続き的及び要員に関するセキュリティ管理
5.1 Physical Controls	物理的セキュリティ管理
5.2 Procedural Controls	手続き的管理
5.3 Personnel Controls	要員管理
6. TECHNICAL SECURITY CONTROLS	技術的なセキュリティ管理
6.1 Key Pair Generation and Installation	鍵ペアの生成とインストール
6.2 Private Key Protection	秘密鍵の保護管理
6.3 Other Aspects of Key Pair Management	鍵ペア管理におけるその他の考慮点
6.4 Activation Data	活性化データ
6.5 Computer Security Controls	コンピュータセキュリティ管理
6.6 Life Cycle Technical Controls	ライフサイクル管理
6.7 Network Security Controls	ネットワークセキュリティ管理
6.8 Cryptographic Module Engineering Controls	暗号モジュールの技術的管理
7. CERTIFICATE AND CRL PROFILES	電子証明書とCRLのプロファイル
7.1 Certificate Profile	電子証明書プロファイル
7.2 CRL Profile	CRL プロファイル
8. SPECIFICATION ADMINISTRATION	仕様管理
8.1 Specification change procedures	仕様変更手続き
8.2 Publication and notification policies	公開及び通知方針
8.3 CPS approval procedures	CPS承認手続き

RFC2527の更新版であるRFC3647のCP/CPS等の目次案は、以下のようになっている。

英文目次	日本語目次 (仮訳)
1. INTRODUCTION	概説
1.1 Overview	概要
1.2 Document name and identification	ドキュメント体系(名称等)
1.3 PKI participants	PKIコミュニティの関係者
1.3.1 Certification authorities	発行局
1.3.2 Registration authorities	登録局
1.3.3 Subscribers	利用者
1.3.4 Relying parties	署名検証者
1.3.5 Other participants	その他の関係者
1.4 Certificate usage	電子証明書の用途
1.4.1 Appropriate certificate uses	電子証明書用途の範囲
1.4.2 Prohibited certificate uses	禁止される電子証明書の用途
1.5 Policy administration	認証ポリシー
1.5.1 Organization administering the document	認証ポリシー管理者
1.5.2 Contact person	連絡担当者
1.5.3 Person determining CPS suitability for the policy	CPS管理者
1.5.4 CPS approval procedures	CPS承認手続
1.6 Definitions and acronyms	用語の定義

英文目次	日本語目次 (仮訳)
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	公開とリポジトリ
2.1 Repositories	リポジトリ
2.2 Publication of certification information	公開情報
2.3 Time or frequency of publication	公開の方法(公開期間や更新タイミング)
2.4 Access controls on repositories	リポジトリの参照方法
3. IDENTIFICATION AND AUTHENTICATION	識別と認証
3.1 Naming	識別名
3.1.1 Types of names	識別名タイプ
3.1.2 Need for names to be meaningful	識別名の意味付け
3.1.3 Anonymity or pseudonymity of subscribers	匿名や仮名の利用
3.1.4 Rules for interpreting various name forms	識別名の解釈規則
3.1.5 Uniqueness of names	識別名の一意性
3.1.6 Recognition, authentication, and role of trademarks	商標等について
3.2 Initial identity validation	新規登録時の利用者本人確認
3.2.1 Method to prove possession of private key	秘密鍵の所有確認方法
3.2.2 Authentication of organization identity	利用者の所属組織の確認方法
3.2.3 Authentication of individual identity	利用者本人の確認方法
3.2.4 Non-verified subscriber information	確認できない利用者情報
3.2.5 Validation of authority	利用者の資格や権利に関する確認機関
3.2.6 Criteria for interoperation	相互運用に関する要件
3.3 Identification and authentication for re-key requests	鍵更新時の利用者本人確認
3.3.1 Identification and authentication for routine re-key	有効期間満了に伴う鍵更新時の利用者本人の確認
3.3.2 Identification and authentication for re-key after revocation	失効後の鍵更新に対する本人確認と認証
3.4 Identification and authentication for revocation request	失効請求時の利用者本人の確認
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	電子証明書のライフサイクル運用要件
4.1 Certificate Application	電子証明書申請
4.1.1 Who can submit a certificate application	利用申込者
4.1.2 Enrollment process and responsibilities	利用申込者の役割と責任
4.2 Certificate application processing	電子証明書申請審査(登録業務)
4.2.1 Performing identification and authentication functions	利用者本人の確認業務
4.2.2 Approval or rejection of certificate applications	電子証明書申請の諾否
4.2.3 Time to process certificate applications	電子証明書申請審査にかかる時間
4.3 Certificate issuance	電子証明書発行業務
4.3.1 CA actions during certificate issuance	電子証明書発行業務時の手続きや確認事項
4.3.2 Notification to subscriber by the CA of issuance of certificate	電子証明書発行に関する利用者への通知
4.4 Certificate acceptance	電子証明書の受領確認
4.4.1 Conduct constituting certificate acceptance	電子証明書の受領確認方法
4.4.2 Publication of the certificate by the CA	発行局による認証局の電子証明書の公開
4.4.3 Notification of certificate issuance by the CA to other entities	発行局から登録局などへの電子証明書発行通知
4.5 Key pair and certificate usage	利用者および署名検証者における鍵ペアと電子証明書の用途
4.5.1 Subscriber private key and certificate usage	利用者における秘密鍵と電子証明書の用途
4.5.2 Relying party public key and certificate usage	署名検証者における公開鍵と電子証明書の用途

英文目次	日本語目次 (仮訳)
4.6 Certificate renewal	鍵の更新を伴わない電子証明書の更新
4.6.1 Circumstance for certificate renewal	電子証明書更新の要件
4.6.2 Who may request renewal	電子証明書更新申込者
4.6.3 Processing certificate renewal requests	電子証明書更新業務
4.6.4 Notification of new certificate issuance to subscriber	電子証明書更新に関する利用者への通知
4.6.5 Conduct constituting acceptance of a renewal certificate	更新された電子証明書の受領確認方法
4.6.6 Publication of the renewal certificate by the CA	発行局による更新された認証局電子証明書の公開
4.6.7 Notification of certificate issuance by the CA to other entities	発行局から登録局などへの電子証明書更新通知
4.7 Certificate re-key	鍵の更新を伴う電子証明書の再発行
4.7.1 Circumstance for certificate re-key	電子証明書再発行の要件
4.7.2 Who may request certification of a new public key	電子証明書再発行申込者
4.7.3 Processing certificate re-keying requests	電子証明書再発行業務
4.7.4 Notification of new certificate issuance to subscriber	電子証明書再発行に関する利用者への通知
4.7.5 Conduct constituting acceptance of a re-keyed certificate	再発行された電子証明書の受領確認方法
4.7.6 Publication of the re-keyed certificate by the CA	発行局による再発行電子証明書の公開
4.7.7 Notification of certificate issuance by the CA to other entities	発行局から登録局などへの電子証明書再発行通知
4.8 Certificate modification	電子証明書記載情報の変更による証明書変更
4.8.1 Circumstance for certificate modification	電子証明書変更の要件
4.8.2 Who may request certificate modification	電子証明書変更申込者
4.8.3 Processing certificate modification requests	電子証明書変更業務
4.8.4 Notification of new certificate issuance to subscriber	電子証明書変更に関する利用者への通知
4.8.5 Conduct constituting acceptance of modified certificate	変更された電子証明書の受領確認方法
4.8.6 Publication of the modified certificate by the CA	発行局による変更された電子証明書の公開
4.8.7 Notification of certificate issuance by the CA to other entities	発行局から登録局などへの電子証明書変更再発行通知
4.9 Certificate revocation and suspension	電子証明書の失効と一時停止
4.9.1 Circumstances for revocation	電子証明書失効の要件
4.9.2 Who can request revocation	電子証明書失効請求者
4.9.3 Procedure for revocation request	失効請求手続
4.9.4 Revocation request grace period	失効請求の猶予期間
4.9.5 Time within which CA must process the revocation request	失効処理に要する時間
4.9.6 Revocation checking requirement for relying parties	署名検証者による失効情報確認
4.9.7 CRL issuance frequency (if applicable)	電子証明書失効リスト(CRL)発行頻度(CRL発行時)
4.9.8 Maximum latency for CRLs (if applicable)	電子証明書失効リスト(CRL)発行の最大遅延時間(CRL発行時)
4.9.9 On-line revocation/status checking availability	オンライン証明書有効性確認サービスの提供について
4.9.10 On-line revocation checking requirements	オンライン証明書有効性確認サービス利用の要件
4.9.11 Other forms of revocation advertisements available	その他の電子証明書有効性確認方法
4.9.12 Special requirements re key compromise	鍵の危殆時の特別要件
4.9.13 Circumstances for suspension	電子証明書一時停止の要件
4.9.14 Who can request suspension	電子証明書一時停止請求者
4.9.15 Procedure for suspension request	電子証明書の一時停止請求手続
4.9.16 Limits on suspension period	一時停止可能期間
4.10 Certificate status services	オンライン証明書有効性確認サービス
4.10.1 Operational characteristics	オンライン証明書有効性確認サービスの運用方法

英文目次	日本語目次 (仮訳)
4.10.2 Service availability	オンライン証明書有効性確認サービスの利用
4.10.3 Optional features	追加サービスの提供について
4.11 End of subscription	利用者からの利用終了申請について
4.12 Key escrow and recovery	キーエスクロー(鍵供託)と鍵復元
4.12.1 Key escrow and recovery policy and practices	キーエスクローと鍵復元に関する方針と実施手順
4.12.2 Session key encapsulation and recovery policy and practices	セッション鍵のカプセル化と鍵復元に関する方針と実施手順
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	設備・要員・運用等の管理
5.1 Physical controls	物理的管理
5.1.1 Site location and construction	設置場所と建築構造
5.1.2 Physical access	物理的アクセス
5.1.3 Power and air conditioning	電源と空調
5.1.4 Water exposures	水害防止対策
5.1.5 Fire prevention and protection	防火対策
5.1.6 Media storage	媒体等の災害対策
5.1.7 Waste disposal	廃棄処理
5.1.8 Off-site backup	オフサイトバックアップ
5.2 Procedural controls	手続的管理
5.2.1 Trusted roles	各要員の役割
5.2.2 Number of persons required per task	各要員の必要人員
5.2.3 Identification and authentication for each role	各要員の本人確認と認証
5.2.4 Roles requiring separation of duties	要員の権限分割
5.3 Personnel controls	要員管理
5.3.1 Qualifications, experience, and clearance requirements	要員の資格・経歴・身分証明
5.3.2 Background check procedures	経歴の確認方法
5.3.3 Training requirements	教育訓練
5.3.4 Retraining frequency and requirements	再教育訓練の実施頻度と要件
5.3.5 Job rotation frequency and sequence	要員ローテーションの頻度と方法
5.3.6 Sanctions for unauthorized actions	要員の罰則規定
5.3.7 Independent contractor requirements	委託契約の要件
5.3.8 Documentation supplied to personnel	要員へ配布資料
5.4 Audit logging procedures	監査ログ
5.4.1 Types of events recorded	記録するイベント
5.4.2 Frequency of processing log	監査ログの確認頻度
5.4.3 Retention period for audit log	監査ログ保存期間
5.4.4 Protection of audit log	監査ログの保存方法
5.4.5 Audit log backup procedures	監査ログのバックアップ手続
5.4.6 Audit collection system (internal vs. external)	監査ログシステムの設置場所(内部と外部)
5.4.7 Notification to event-causing subject	イベント実施者への通知
5.4.8 Vulnerability assessments	脆弱性評価
5.5 Records archival	帳簿書類(情報)
5.5.1 Types of records archived	保存する帳簿書類(情報)
5.5.2 Retention period for archive	帳簿書類(情報)の保存期間
5.5.3 Protection of archive	帳簿書類(情報)の保存方法

英文目次	日本語目次 (仮訳)
5.5.4 Archive backup procedures	帳簿書類(情報)のバックアップ
5.5.5 Requirements for time-stamping of records	帳簿書類(情報)に対するタイムスタンプ
5.5.6 Archive collection system (internal or external)	帳簿書類(情報)システムの設置場所(内部又は外部)
5.5.7 Procedures to obtain and verify archive information	帳簿書類(情報)の確認方法
5.6 Key changeover	認証局の鍵更新
5.7 Compromise and disaster recovery	危険化や災害時の対応
5.7.1 Incident and compromise handling procedures	危険化時の対応手順
5.7.2 Computing resources, software, and/or data are corrupted	コンピュータリソース・ソフトウェア・データ等の重大障害時の対応手順
5.7.3 Entity private key compromise procedures	利用者の秘密鍵の危険化時の対応手順
5.7.4 Business continuity capabilities after a disaster	災害時の認証業務の継続について
5.8 CA or RA termination	認証業務の廃止について
6. TECHNICAL SECURITY CONTROLS	技術的なセキュリティ管理
6.1 Key pair generation and installation	鍵ペアの生成及びインストール
6.1.1 Key pair generation	利用者の鍵ペアの生成方法
6.1.2 Private key delivery to subscriber	利用者の秘密鍵の安全な配付方法
6.1.3 Public key delivery to certificate issuer	利用者の公開鍵の認証局への配付方法
6.1.4 CA public key delivery to relying parties	認証局の公開鍵の検証者への配付方法
6.1.5 Key sizes	鍵サイズ
6.1.6 Public key parameters generation and quality checking	公開鍵暗号方式のパラメータ等の鍵ペアの信頼性確保
6.1.7 Key usage purposes (as per X.509 v3 key usage field)	鍵の用途の目的(電子証明書記載の鍵用途)
6.2 Private Key Protection and Cryptographic Module Engineering Controls	秘密鍵の信頼性と暗号モジュール
6.2.1 Cryptographic module standards and controls	暗号モジュールの技術要件
6.2.2 Private key (n out of m) multi-person control	秘密鍵の秘密分散管理
6.2.3 Private key escrow	秘密鍵のキーエスクロー(鍵供託)
6.2.4 Private key backup	秘密鍵のバックアップ
6.2.5 Private key archival	秘密鍵の保管
6.2.6 Private key transfer into or from a cryptographic module	暗号モジュールにおける秘密鍵の入出力
6.2.7 Private key storage on cryptographic module	暗号モジュールにおける秘密鍵の管理
6.2.8 Method of activating private key	秘密鍵の活性化
6.2.9 Method of deactivating private key	秘密鍵の非活性化
6.2.10 Method of destroying private key	秘密鍵の廃棄
6.2.11 Cryptographic Module Rating	暗号モジュールの評価
6.3 Other aspects of key pair management	その他鍵ペアに関する管理
6.3.1 Public key archival	公開鍵の保存
6.3.2 Certificate operational periods and key pair usage periods	電子証明書の実運用期間と鍵ペアの使用期間
6.4 Activation data	活性化データ
6.4.1 Activation data generation and installation	活性化データの生成と設定
6.4.2 Activation data protection	活性化データの保護
6.4.3 Other aspects of activation data	その他活性化データに関する考慮点
6.5 Computer security controls	認証設備のセキュリティ管理
6.5.1 Specific computer security technical requirements	認証設備に関する特別なセキュリティ要件
6.5.2 Computer security rating	認証設備のセキュリティ評価
6.6 Life cycle technical controls	システムのライフサイクル管理

英文目次	日本語目次 (仮訳)
6.6.1 System development controls	システム開発管理
6.6.2 Security management controls	セキュリティ運用管理
6.6.3 Life cycle security controls	ライフサイクルのセキュリティ管理
6.7 Network security controls	ネットワークセキュリティ管理
6.8 Time-stamping	タイムスタンプ
7. CERTIFICATE, CRL, AND OCSP PROFILES	電子証明書、CRLとOCSPのプロファイル
7.1 Certificate profile	電子証明書のプロファイル
7.1.1 Version number(s)	電子証明書のバージョン番号
7.1.2 Certificate extensions	電子証明書の拡張
7.1.3 Algorithm object identifiers	アルゴリズムオブジェクト識別子
7.1.4 Name forms	識別名の形式
7.1.5 Name constraints	識別名の制約
7.1.6 Certificate policy object identifier	CPオブジェクト識別子
7.1.7 Usage of Policy Constraints extension	認証ポリシー制約拡張の使用
7.1.8 Policy qualifiers syntax and semantics	認証ポリシー修飾子の構文及び意味
7.1.9 Processing semantics for the critical Certificate Policies extension	クリティカルな認証ポリシー拡張
7.2 CRL profile	CRLプロファイル
7.2.1 Version number(s)	バージョン番号
7.2.2 CRL and CRL entry extensions	CRLとCRL entry拡張
7.3 OCSP profile	OCSPプロファイル
7.3.1 Version number(s)	バージョン番号
7.3.2 OCSP extensions	OCSP拡張
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	準拠性監査とその他監査基準
8.1 Frequency or circumstances of assessment	監査の頻度と実施要件
8.2 Identity/qualifications of assessor	監査人の資格
8.3 Assessor's relationship to assessed entity	監査人と認証機関
8.4 Topics covered by assessment	監査事項
8.5 Actions taken as a result of deficiency	監査結果の対応
8.6 Communication of results	監査結果の公開
9. OTHER BUSINESS AND LEGAL MATTERS	他のビジネス及び法的要件
9.1 Fees	料金
9.1.1 Certificate issuance or renewal fees	電子証明書の発行及び更新料金
9.1.2 Certificate access fees	電子証明書のアクセス料金
9.1.3 Revocation or status information access fees	電子証明書の失効情報参照料金
9.1.4 Fees for other services	その他認証サービスに関連する料金
9.1.5 Refund policy	払戻し方針
9.2 Financial responsibility	財務的責任
9.2.1 Insurance coverage	保険範囲
9.2.2 Other assets	その他の資産について
9.2.3 Insurance or warranty coverage for end-entities	利用者等への保証
9.3 Confidentiality of business information	ビジネス上の秘密情報の管理について
9.3.1 Scope of confidential information	秘密情報の対象事項
9.3.2 Information not within the scope of confidential information	秘密情報の対象外事項

英文目次	日本語目次 (仮訳)
9.3.3 Responsibility to protect confidential information	秘密情報の管理責任
9.4 Privacy of personal information	個人情報保護
9.4.1 Privacy plan	個人情報保護の方針
9.4.2 Information treated as private	個人情報保護の対象情報
9.4.3 Information not deemed private	個人情報保護の対象外情報
9.4.4 Responsibility to protect private information	個人情報の管理責任
9.4.5 Notice and consent to use private information	個人情報の利用に関する説明
9.4.6 Disclosure pursuant to judicial or administrative process	法的手続による個人情報の公開
9.4.7 Other information disclosure circumstances	その他個人情報公開の要件
9.5 Intellectual property rights	知的財産権
9.6 Representations and warranties	責任と義務
9.6.1 CA representations and warranties	発行局の責任と義務
9.6.2 RA representations and warranties	登録局の責任と義務
9.6.3 Subscriber representations and warranties	利用者の責任と義務
9.6.4 Relying party representations and warranties	検証者の責任と義務
9.6.5 Representations and warranties of other participants	その他コミュニティ関係者の責任と義務
9.7 Disclaimers of warranties	保証外事項
9.8 Limitations of liability	責任の制限
9.9 Indemnities	補償
9.10 Term and termination	本規程の効力
9.10.1 Term	本規程の効力有効期間
9.10.2 Termination	本規程の無効
9.10.3 Effect of termination and survival	本規程の効力継続について
9.11 Individual notices and communications with participants	コミュニティにおける通知と連絡
9.12 Amendments	改訂
9.12.1 Procedure for amendment	改訂手続
9.12.2 Notification mechanism and period	改訂通知方法と通知時期
9.12.3 Circumstances under which OID must be changed	CPオブジェクト識別子の変更の要件
9.13 Dispute resolution provisions	紛争解決手続
9.14 Governing law	準拠法
9.15 Compliance with applicable law	適用法の遵守
9.16 Miscellaneous provisions	雑則
9.16.1 Entire agreement	完全合意条項
9.16.2 Assignment	権利譲渡条項
9.16.3 Severability	分離条項
9.16.4 Enforcement (attorneys' fees and waiver of rights)	強制執行条項 (弁護士費用及び権利放棄)
9.16.5 Force Majeure	不可抗力
9.17 Other provisions	その他事項