

○認証業務及びこれに附帯する業務の実施に関する技術的基準（平成十五年十二月三日総務省告示第七百六号）

電子署名に係る地方公共団体の認証業務に関する法律（平成十四年法律第百五十三号）及び電子署名に係る地方公共団体の認証業務に関する法律施行規則（平成十五年総務省令第百二十号）を実施するため、認証業務及びこれに附帯する業務の実施に関する技術的基準を次のように定める。

認証業務及びこれに附帯する業務の実施に関する技術的基準

（用語）

第一条 この技術的基準において使用する用語は、電子署名に係る地方公共団体の認証業務に関する法律（以下「法」という。）及び電子署名に係る地方公共団体の認証業務に関する法律施行規則（以下「規則」という。）において使用する用語の例によるほか、次の定義に従うものとする。

- 一 「受付窓口端末」とは、法第三条第五項の規定による申請書の内容及び利用者署名検証符号の通知、同条第六項の規定による都道府県知事が通知する電子証明書の受信及び同条第七項の規定による電子証明書の電磁的記録媒体（法第三条第四項に規定する電磁的記録媒体をいう。以下第九条まで同じ。）への記録を行うための電子計算機をいう。
- 二 「鍵ペア生成装置」とは、法第三条第四項の規定により申請者が利用者署名字号及び利用者署名検証符号を作成し、電磁的記録媒体に記録するための住所地市町村長の使用に係る電子計算機をいう。

（電子署名に係る基準）

第二条 規則第二条の基準を満たす電子署名の方式は、RSA方式（オブジェクト識別子 一 二 八四〇 一一三五四九 一 一 五）であってモジュラスとなる合成数が千二十四ビットのものとする。

（利用者確認の方法等）

- 第三条 法第三条第三項の規定による利用者確認は、コミュニケーションサーバ（電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成十四年総務省告示第三百三十四号）第1の2に規定するコミュニケーションサーバをいう。以下同じ。）の端末及び受付窓口端末を用いて行うものとする。この場合において、住所地市町村長は、コミュニケーションサーバの端末から受付窓口端末に申請者に係る住民票に記載されている事項のうち住民基本台帳法（昭和四十二年法律第八十一号）第七条第一号から第三号まで及び第七号に掲げる事項（同号に掲げる事項については、住所とする。第十一条において同じ。）を送付するものとする。
- 2 住所地市町村長は、受付窓口端末を操作する職員について、コミュニケーションサーバの端末のアクセス権限を有する職員に限定するものとする。
- 3 受付窓口端末については、ID（操作者を識別するための番号、記号、その他の符号をいう。）及びパスワードによる操作者の認証を行うものとする。

（暗証番号の基準）

第四条 規則第七条第二項の規定により申請者が電磁的記録媒体に設定する暗証番号は他人から容易に推測されるものであってはならない。

（鍵ペア生成装置の基準）

- 第五条 鍵ペア生成装置は、次に掲げる要件を満たすものとする。
- 一 他の電子計算機と電気通信回線により接続されていないこと。
 - 二 内部の情報を読み取られることを防止するための必要な機能を有すること。
 - 三 利用者署名字号及び利用者署名検証符号の作成に当たり、素数の判定その他の措置が適切に行われるものであること。
 - 四 当該鍵ペア生成装置を用いて過去に作成された利用者署名字号又は利用者署名検証符号と同一の利用者署名字号又は利用者署名検証符号が作成されることを防止するための措置が講じられていること。
 - 五 利用者署名字号及び利用者署名検証符号を記録する電磁的記録媒体との間で乱数等を送受信することにより、当該鍵ペア生成装置が正当なものであることを認証するための必要な機能を有すること。
 - 六 作成した利用者署名字号を利用者の電磁的記録媒体に送信する場合において、当該利用者署名字号を暗号化して送信するための必要な機能を有すること。

（利用者署名字号及び利用者署名検証符号を記録する電磁的記録媒体の基準）

- 第六条 利用者署名字号及び利用者署名検証符号を記録する電磁的記録媒体は、次に掲げる要件を満たすものとする。
- 一 電磁的記録媒体が住民基本台帳カードの場合にあっては、公的個人認証サービス利用領域（住民基本台帳カードに関する技術的基準（平成十五年総務省告示第三百九十二号）第1の7に規定する公的個人認証サービス利用領域をいう。）に利用者署名字号及び利用者署名検証符号、電子証明書並びに暗証番号を記録することが可能であること。
 - 二 住民基本台帳カード以外の電磁的記録媒体にあっては、次の要件のすべてを満たすこと。
 - イ 半導体集積回路上に公的個人認証サービスアプリケーション（住民基本台帳カードに関する技術的基準第1の6に規定する公的個人認証サービスアプリケーションをいう。）のための専用の領域を有すること。
 - ロ イに規定する領域に利用者署名字号及び利用者署名検証符号、電子証明書並びに暗証番号を記録することが可能であること。
 - ハ イに規定する領域とそれ以外の領域は、電磁的記録媒体の内部でそれぞれ独立し、イに規定する領域以外の領域に搭載されているアプリケーションに係るシステムが、イに規定する領域に情報を記録し、又は当該領域

- に記録された情報を読み取ることができない仕組みを保持すること。
- 三 受付窓口端末及び鍵ペア生成装置との間で乱数等を送受信することにより、当該鍵ペア生成装置及び受付窓口端末が正当なものであることを確認するための必要な機能を有すること。
 - 四 前条第六号の規定により暗号化されて送信された利用者署名符号を復号するために必要な機能を有すること。
 - 五 利用者署名符号の電磁的記録媒体の外部からの読み取りを防止するために必要な機能を有すること。

(受付窓口端末の基準)

第七条 受付窓口端末は、次に掲げる要件を満たすものとする。

- 一 法第三条第五項の規定による申請書の内容及び利用者署名検証符号の通知の受信、同条第六項の規定による都道府県知事の電子証明書の通知、法第九条第二項において準用する法第三条第五項の規定による申請書の内容の通知の受信及び法第十条第二項において準用する法第三条第五項の規定による届出書の内容の通知の受信等に用いる電子計算機と相互に認証を行うために必要な機能を有すること。
- 二 利用者署名符号及び利用者署名検証符号を記録する電磁的記録媒体との間で乱数等を送受信することにより、当該受付窓口端末が正当なものであることを認証するための必要な機能を有すること。

(発行者署名符号を作成する電子計算機等の基準)

第八条 発行者署名符号を作成するための都道府県知事の使用に係る電子計算機は、次に掲げる要件を満たすものとする。

- 一 外部から内部の情報を読み取られることを防止するための必要な機能を有すること。
 - 二 取扱いに際しては、操作者が正当なアクセス権限を有していることを確認するために必要な機能を有していること。
 - 三 発行者署名符号の入力及び出力に当たって、適切な保護措置が講じられるものであること。
 - 四 バックアップ用の発行者署名符号の複製を行うことが可能であるとともに、複製されたバックアップ用の発行者署名符号を安全に保存することができるものであること。
 - 五 発行者署名符号の作成に当たり、素数の判定その他の措置が適切に行われるものであること。
- 2 発行者署名符号を用いて行う電子署名の方式は、RSA方式（オブジェクト識別子 一 二 八四〇 一一三五四九 一 一 五）であってモジュラスとなる合成数が二千四十八ビットのものとする。
- 3 発行者署名符号の使用期間は、五年とする。

(電子証明書の提供に際しての申請者への説明事項)

第九条 法第三条第七項の規定により住所地市町村長が電子証明書を申請者に提供するときは、次に掲げる事項を申請者に説明しなければならない。

- 一 電子署名は署名又は押印に相当する法的効果が認められ得るものであることから、法第四条の規定により、利用者は、自己に係る利用者署名符号の漏えい、滅失又はき損の防止その他の利用者署名符号の適切な管理を行わなければならないこと。
- 二 法第十条第一項の規定により、利用者は、利用者署名符号が漏えいし、滅失し、若しくはき損したとき、又は当該利用者署名符号を記録した電磁的記録媒体が使用できなくなったときは、住所地市町村長を経由して、速やかに当該利用者に係る電子証明書を発行した都道府県知事にその旨を届け出なければならないこと。
- 三 虚偽の申請をして、不実の電子証明書を発行させた者は、法第六十一条の規定により罰せられること。

(住所地市町村長と都道府県知事との間の情報の送受信)

第十条 法第三条第八項に規定する電気通信回線は、総合行政ネットワークその他の電気通信回線であって総務大臣が適当と認めるものでなければならない。

- 2 法第三条第五項の規定により通知される申請書の内容及び利用者署名検証符号並びに同条第六項の規定により通知される電子証明書を同条第八項の規定により電気通信回線を通じて送信するときは、住所地市町村長又は都道府県知事は、当該申請書の内容及び利用者署名検証符号並びに電子証明書を暗号化しなければならない。

(電子証明書の様式)

第十一条 電子証明書の様式は、ITU-T勧告X. 509 (03/2000)に準拠するものとし、利用者に係る住民票に記載されている事項のうち住民基本台帳法第七条第一号から第三号まで及び第七号に掲げる事項は、電子証明書の拡張領域に記録するものとする。

(相互認証)

第十二条 都道府県知事は、国又は地方公共団体が実施する認証業務（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）第二条第二項に規定する認証業務をいう。第三十一条第一号において同じ。）のうち総務大臣が適当と認めるものと相互認証を行わなければならない。

(認証業務実施設備等)

第十三条 都道府県知事（法第三十四条第一項の規定により認証事務を指定認証機関に行わせることとした場合にあつては指定認証機関。）は、認証業務（指定認証機関にあつては認証事務。）の用に供するため、認証業務実施設備その他総務大臣が必要と認める設備を備えなければならない。

(認証業務実施設備への入出場を管理するために必要な措置)

第十四条 規則第十三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認証業務実施設備室（認証業務実施設備を設置する室をいう。以下同じ。）が次の各号に定める要件を満たすものをいうもの

とする。

- 一 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。
- 二 入室者の数と同数の者の退室を管理すること。
- 三 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。
- 四 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。

（認証業務実施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）

第十五条 規則第十三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 認証業務実施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 認証業務実施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

（正当な権限を有しない者による認証業務実施設備の作動を防止するための措置等）

第十六条 規則第十三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をいうものとする。

- 一 認証業務実施設備を作動させる権限を操作者ごとに設定することができること。
- 二 認証業務実施設備を作動させるに当たっては、操作者及びその権限の確認を行うことができること。
- 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電子計算機の操作については、この限りでない。
- 四 認証業務実施設備の所在を示す掲示がされていないこと。

2 規則第十三条第三号に規定する認証業務実施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、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

（認証業務実施設備等の災害を防止するために必要な措置）

第十七条 規則第十三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 認証業務実施設備 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 認証業務実施設備室 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 認証業務実施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つて、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。

（認証業務実施設備の操作等に関する許諾等）

第十八条 規則第十四条第二号に規定する認証業務実施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符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 認証業務実施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業務実施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の措置）

第十九条 規則第十四条第三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、認証業務実施設備室内で複数の者によって規則第十三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 認証業務実施設備室内で規則第十三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、認証業務実施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 認証業務実施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実施設備の設定の変更は、認証業務実施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。

（発行記録の記録及び保存の方法）

第二十条 法第八条の規定による発行記録の記録及び保存は、専用の電磁的記録媒体（法第三条第一項に規定する電磁的記録に係る記録媒体をいう。以下同じ。）に記録し、保存することによるものとする。

- 2 都道府県知事は、発行記録を記録及び保存した電磁的記録媒体の滅失又はき損の防止その他の電磁的記録媒体の適切な管理を行わなければならない。

（失効申請等情報の記録及び保存の方法）

第二十一条 法第十一条の規定による失効申請等情報の記録及び保存は、専用の電磁的記録媒体に記録し、保存することによるものとする。

- 2 都道府県知事は、失効申請等情報を記録及び保存した電磁的記録媒体の滅失又はき損の防止その他の電磁的記録媒体の適切な管理を行わなければならない。

（異動等失効情報の記録及び保存の方法）

第二十二条 法第十二条の規定による異動等失効情報の記録及び保存は、専用の電磁的記録媒体に記録し、保存することによるものとする。

- 2 都道府県知事は、異動等失効情報を記録及び保存した電磁的記録媒体の滅失又はき損の防止その他の電磁的記録媒体の適切な管理を行わなければならない。

（記録誤り等に係る情報の記録及び保存の方法）

第二十三条 法第十三条の規定による記録誤り等に係る情報の記録及び保存は、専用の電磁的記録媒体に記録し、保存することによるものとする。

- 2 都道府県知事は、記録誤り等に係る情報を記録及び保存した電磁的記録媒体の滅失又はき損の防止その他の電磁的記録媒体の適切な管理を行わなければならない。

（発行者署名符号の漏えい等に係る情報の記録の方法）

第二十四条 法第十四条の規定による発行者署名符号の漏えい等に係る情報の記録及び保存は、専用の電磁的記録媒体に記録し、保存することによるものとする。

- 2 都道府県知事は、発行者署名符号の漏えい等に係る情報を記録及び保存した電磁的記録媒体の滅失又はき損の防止その他の電磁的記録媒体の適切な管理を行わなければならない。

（失効情報ファイルの記録及び保存の方法）

第二十五条 法第十六条の規定による失効情報ファイルの記録及び保存は、専用の電磁的記録媒体に記録し、保存することによるものとする。

- 2 都道府県知事は、失効情報ファイルを記録及び保存した電磁的記録媒体の滅失又はき損の防止その他の電磁的記録媒体の適切な管理を行わなければならない。

（認証設備室への入退場を管理するために必要な措置）

第二十六条 規則第二十五条第一号に規定する入退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をいうものとする。

- 一 認証設備室（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（電子署名及び認証業務に関する法律施行規則（平成十三年総務省・法務省・経済産業省令第二号）第四条第一号に規定する電子証明書をいう。以下第三十三条まで同じ。）の利用者（電子署名及び認証業務に関する法律第二条第二項に規定する利用者をいう。以下第三十三条まで同じ。）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（電子署名及び認証業務に関する法律施行規則第六条第三号の二に規定する利用者識別符号をいう。以下同じ。）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。
- ニ 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。
- 二 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)

第二十七条 規則第二十五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装置
- 三 利用者署名検証符号（電子署名及び認証業務に関する法律施行規則第四条第一号に規定する利用者署名検証符号をいう。次条において同じ。）、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)

第二十八条 規則第二十五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をいうものとする。

- 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が確認できること。
 - 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 規則第二十五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)

第二十九条 規則第二十五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つて、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)

第三十条 規則第二十六条第一号に規定する利用申込者（電子署名及び認証業務に関する法律施行規則第五条第一項に規定する利用申込者をいう。）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 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ことから、利用者署名符号（電子署名及び認証業務に関する法律施行規則第六条第三号に規定する利用者署名符号をいう。以下同じ。）の漏えい、滅失又はき損の防止その他の利用者署名符号の適切な管理を行わなければならないこと。
- 二 利用者署名符号が漏えいし、滅失し、若しくはき損したとき、又はそのおそれがある場合、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。
- 三 認定申請者が行う特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、認定申請者が指定したものを使用する必要があること。

(特定認証業務と他の業務との誤認を防止するための措置)

第三十一条 規則第二十六条第七号に規定する利用者その他の者が認定申請者が行う特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（電子署名及び認証業務に関する法律施行規則第四条第四号に規定する発行者署名符号をいう。第三十五条において同じ。）を当該特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 認定認証業務（電子署名及び認証業務に関する法律施行規則第六条第二号に規定する認定認証業務をいう。）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 当該特定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（電子署名及び認証業務に関する法律施行規則第六条第九号に規定する発行者署名検証符号をいう。次条において同じ。）に係る電子証明書値をSHA-1（オブジェクト識別子 一 三 一四 三二 二六）、SHA-256（オブジェクト識別子 二 一六 八四〇 一 一〇一 三 四 二 一）、SHA-384（オブジェクト識別子 二 一六 八四〇 一 一〇一 三 四 二 二）又はSHA-512（オブジェクト識別子 二 一六 八四〇 一 一〇一 三 四 二 三）のうちいずれか一以上で変換した値によって当該特定認証業務を特定すること。

(署名検証者への情報提供)

第三十二条 規則第二十六条第八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（電子署名及び認証業務に関する法律施行規則第六条第九号に規定する署名検証者をいう。以下この条において同じ。）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認定申請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である認定申請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。

(特定認証業務の実施に関する規程)

第三十三条 規則第二十六条第十二号に規定する認定申請者が行う特定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 認定申請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 認定申請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 当該特定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 当該特定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 認定申請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、認定申請者が行う特定認証業務を廃止する日の六十日前までにその旨を利用者に通知すること（法第十七条第三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。）及び認定に係る特定認証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)

第三十四条 規則第二十六条第十五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符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)

第三十五条 規則第二十六条第十六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二十五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二十五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。

（保存期間に係る失効情報の提供の方法）

- 第三十六条 令第十三条第一号の規定により電気通信回線を通じて失効情報を提供する方法は、署名検証者等からの問い合わせに対して失効情報の集合物を提供する方法又は即時に応答する方法によるものとする。
- 2 令第十三条第一号の規定により電気通信回線を通じて失効情報を提供する場合において、都道府県知事は、失効情報の提供を行うための都道府県知事の使用に係る電子計算機について適切なアクセス制御を行わなければならない。

（団体署名検証者が行う署名確認者への回答の方法）

- 第三十六条の二 令第十五条の規定による回答は、署名確認者からの問い合わせに対して即時に応答する方法によるものとする。
- 2 令第十五条の規定による回答を行う場合において、団体署名検証者は、回答を行うための団体署名検証者の使用に係る電子計算機について適切なアクセス制御を行わなければならない。

（指定認証機関への異動等失効情報の通知の方法）

- 第三十七条 法第三十五条第二項の規定による指定認証機関への異動等失効情報の通知に係る電気通信回線には専用回線を使用し、かつ、当該異動等失効情報を暗号化しなければならない。
- 2 委任都道府県知事（住民基本台帳法第三十条の十第三項に規定する委任都道府県知事を除く。）の使用に係る電子計算機と指定認証機関の使用に係る電子計算機は相互に認証を行わなければならない。

（運用規程）

- 第三十八条 法第五十七条に規定する運用規程は、次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 都道府県における連絡先（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、対象又は利用範囲の制限に関する事項
 - 三 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
 - 四 電子証明書の失効の請求に関する事項
 - 五 失効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
 - 六 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。）
 - 七 認証業務の利用に係る料金に関する事項
 - 八 帳簿書類の保存に関する事項
 - 九 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

附 則

この技術的基準は、法の施行の日から適用する。

附 則 （平成十八年十月三十一日総務省告示第五百六十九号）

この告示は、電子署名に係る地方公共団体の認証業務に関する法律の一部を改正する法律（平成十八年法律第四十四号）の施行の日（平成十八年十一月一日）から施行する。