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

（平成十三年四月二十七日総務省・法務省・経済産業省告示第二号）

改正：平成十四年十一月二十一日総務省・法務省・経済産業省告示第十三号
改正：平成十五年六月二日総務省・法務省・経済産業省告示第九号
改正：平成二十一年四月二十四日総務省・法務省・経済産業省告示第十一号
最終改正：令和二年三月三十日総務省・法務省・経済産業省告示第二号

（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方式であって、ハッシュ関数としてＳＨＡ－２５６を使用するもの（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一一）、ＳＨＡ－３８４を使用するもの（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一二）又はＳＨＡ－５１２を使用するもの（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一三）のうち、モジュラスとなる合成数が二千四十八ビット以上のもの

二　ＲＳＡ－ＰＳＳ方式（オブジェクト識別子　一　二　八四〇　一一三五四九　一　一　一〇）であって、ハッシュ関数として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）を使用するもののうち、モジュラスとなる合成数が二千四十八ビット以上のもの

三　ＥＣＤＳＡ方式であって、ハッシュ関数としてＳＨＡ－２５６を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四五　四　三　二）、ＳＨＡ－３８４を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四五　四　三　三）又はＳＨＡ－５１２を使用するもの（オブジェクト識別子　一　二　八四〇　一〇〇四五　四

三　四）のうち、楕円曲線の定義体及び位数が二百二十四ビット以上のもの

四　ＤＳＡ方式であって、ハッシュ関数としてＳＨＡ－２５６を使用するもの（オブジェクト識別子　二　一六　八四〇　一　一〇一　三　四　三　二）であり、かつ、モジュラスとなる素数が二千四十八ビット以上のもの

（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をいうものとする。

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。

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－２５６、ＳＨＡ－３８４又はＳＨＡ－５１２のうちいずれか一以上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。

附　則　（平成十四年十一月二十一日総務省・法務省・経済産業省告示第十三号）

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

附　則（平成十五年六月二日総務省・法務省・経済産業省告示第九号）

この告示は、公布の日から施行する。

附　則（平成二十一年四月二十四日総務省・法務省・経済産業省告示第十一号）

この告示は、公布の日から施行する。

附　則（令和二年三月三十日総務省・法務省・経済産業省告示第二号）

この告示は、公布の日から施行する。