令 和 ２ 年 ３ 月 ３ ０ 日
総務省サイバーセキュリティ統括官室
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、安全な擬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号ニ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号ニに規定する「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事実を利用者に通知し、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事実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－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」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－２５６、ＳＨＡ－３８４又はＳＨＡ－５１２のうちいずれか一以上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が法、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。