事業者名：

業務名：

申請日：

| **No.** | **告示（令和3年総務省告示第146号）** | **実施要項（令和3年4月1日版）** | **説明** | **説明資料** |
| --- | --- | --- | --- | --- |
| 1 | **K3** 第3条（認定）  **K3.1**  １　総務大臣は、次の各号に掲げる要件のいずれにも該当すると認められる時刻認証業務を、認定時刻認証業務（以下「認定業務」という。）として認定することができる。 |  |  |  |
| 2 | **K3.1.1**  一　デジタル署名方式（タイムスタンプを生成する際、信頼できる認証事業者から発行を受けた電子証明書に基づく、当該時刻認証業務に専用の利用者署名符号を用いて時刻情報等にデジタル署名を施すことによってタイムスタンプの信頼性を確保する方式）を用いるものとすること。 | **J4** 第4条（タイムスタンプ）  １　認定時刻認証業務（以下「認定業務」という。）において生成・発行されるタイムスタンプは、IETF（Internet Engineering Task Force、インターネット技術タスクフォース）によるRFC3161及びRFC5816に準拠することとする。 |  |  |
| 3 | **J5** 第5条（電子証明書）  **J5.1**  １　告示第３条第１項の認定を受けた者（以下「認定事業者」という。）は、認定業務でデジタル署名を施すための専用の利用者署名符号（以下「秘密鍵」という。）を用いてタイムスタンプにデジタル署名を付与することとする。 |  |  |
| 4 | **J5.2**  ２　「電子証明書」とは、前項の秘密鍵に対応した公開鍵（以下「公開鍵」という。）を証明する公開鍵証明書をいう。 |  |  |
| 5 | **J5.3**  ３　電子証明書は、以下の要件を満たすこととする。 |  |  |
| 6 | **J5.3.1**  一　発行元である認証事業者の名称が記載されていること。 |  |  |
| 7 | **J5.3.2**  二　秘密鍵の保持主体の名称又は保持主体が行う業務の名称が記載されていること。 |  |  |
| 8 | **J5.3.3**  三　秘密鍵はタイムスタンプ発行に用いるべきものであり、その使用方法が定められていること。 |  |  |
| 9 | **J5.3.4**  四　当該電子証明書の失効情報の公開情報が記載されていること。 |  |  |
| 10 | **J5.3.5**  五　当該電子証明書の有効期間が記載されていること。 |  |  |
| 11 | **J5.3.6**  六　当該電子証明書並びにその発行に係るルート認証局（及び使用している場合は中間認証局）の公開鍵証明書に付されるデジタル署名に用いる署名アルゴリズムには、平成25年3月1日に総務省、経済産業省が公表した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」(注)のうち、「電子政府推奨暗号リスト」に記載された公開鍵暗号技術を用いられていること。  (注) CRYPTREC暗号リストについては、最終更新版を参照することとする。 |  |  |
| 12 | **J5.3.7**  七　当該電子証明書の発行に係るルート認証局の公開鍵証明書の正当性を示す情報が明らかになっていること。 |  |  |
| 13 | **J5.4**  ４　「信頼できる認証事業者」とは、次の各号に掲げる要件を満たす認証事業者をいう。 |  |  |
| 14 | **J5.4.1**  一　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）第４条第１項に基づく特定認証業務の認定を受けていること又は米国公認会計士協会及びカナダ勅許会計士協会によって共同開発された電子商取引認証局監査プログラム（WebTrust for Certification Authorities）に基づく監査を年１回以上の頻度で受けていること。 |  |  |
| 15 | **J5.4.2**  二　自らが発行した電子証明書に対応した秘密鍵を用いたタイムスタンプの生成・発行を認定事業者が継続している間、自らが営む認証業務を終了せず(注)、当該電子証明書に係る失効リストを最新の状態に保ち、またそれを公表しておくこと。  (注)自らが営む認証業務を他の認証事業者に引継ぐ場合は、認証業務終了には当たらないが、引継ぎ先の事業者が本項各号に該当することを認定事業者において確認する必要がある。 |  |  |
| 16 | **J5.4.3**  三　自らが営む認証業務の終了後、当該認証業務で用いた秘密鍵を安全に廃棄し、その旨を認定事業者に文書で通知すること。 |  |  |
| 17 | **K3.1.2**  二　日本標準時通報機関である国立研究開発法人情報通信研究機構が生成する協定世界時（ＵＴＣ（ＮＩＣＴ））を時刻源とし、当該時刻源との時刻差が一秒以内となるよう、時刻の品質を管理及び証明する措置を講じること。 | **J6** 第6条（時刻源）  **J6.1**  １　タイムスタンプに含まれる時刻は、当該時刻を生成するタイムスタンプサーバの時計（以下、「TSA時計」という。）により生成されることとする。 |  |  |
| 18 | **J6.2**  ２　TSA時計は、時刻源として時刻情報提供サービス等(注)を用い、時刻精度に影響を及ぼす脅威からの保護等の措置により、UTC（NICT）に対し±1秒以内で同期していることとする。  (注)TAAを用いる場合、日本データ通信協会による「タイムビジネス信頼・安心認定制度」の認定を受けたTAAから時刻配信を受けることとする。 |  |  |
| 19 | **J6.3**  ３　上記の同期はうるう秒が発生した場合も維持することとする。なお、うるう秒を考慮した変更を行う場合には、UTCにおけるうるう秒調整の直前の１分間に行うこととし、当該変更が発生した正確な時刻の記録を維持することとする。 |  |  |
| 20 | **J7** 第7条（時刻の品質管理及び証明）  **J7.1**  １　認定事業者は、時刻の品質を管理及び証明するべく、次の各号に掲げる記録について完全性及び機密性を保ちながら、必要に応じて利用できるように保管することとする。 |  |  |
| 21 | **J7.1.1**  一　TSA時計がUTC（NICT）に同期されるまでに経由する各機器における時計間の時刻差を測定した時刻同期ログ |  |  |
| 22 | **J7.1.2**  二　鍵ペア（秘密鍵及び公開鍵）の生成・失効記録及び秘密鍵廃棄の記録 |  |  |
| 23 | **J7.1.3**  三　認定業務に関わるシステムの動作異常の記録 |  |  |
| 24 | **J7.1.4**  四　TAAより受けた時刻監査記録又は時刻監査証明書の写し（TAAを用いる場合に限る） |  |  |
| 25 | **J7.1.5**  五　その他時刻の品質を管理又は証明するために必要な記録 |  |  |
| 26 | **J7.2**  ２　前項各号の記録は、その保管期間を明記の上、文書化しておくこととする。なお、保管期間は、認定業務において発行するタイムスタンプが有効である間は最低限確保することとする。 |  |  |
| 27 | **J7.3**  ３　認定事業者は、前条第２項で定められた時刻精度を満たしていないタイムスタンプの発行を防止するための措置を講ずることとする。なお、当該措置としてタイムスタンプに含まれる時刻を外部のGPS等を時刻源として用いる参照時計を用いて監視する場合、当該時刻と参照時計の時刻との時刻差等が記録されること及び異常発生時に当該異常が記録されるとともに認定業務に直接従事する者へ通知されることが必要となる。 |  |  |
| 28 | **K3.1.3**  三　認定業務であるかどうかを一意に特定できる情報を含み、自らが改ざんされた際にこれを検知する手段を有するタイムスタンプを、当該タイムスタンプが有効である間十分な安全性を有する暗号技術や装置等を用いて堅実に生成すること。 | **J8** 第8条（認定業務の特定）  **J8.1**  １　タイムスタンプには、対応するオブジェクト識別子（OID）等、認定業務を一意に特定できる情報を含めることとする。 |  |  |
| 29 | **J9** 第9条（タイムスタンプの生成に関わる暗号技術）  **J9.1**  １　タイムスタンプの付与対象となる電子データのハッシュ値（以下「ハッシュ値」と する。）を得るためのハッシュ関数及び告示第３条第１項第１号のデジタル署名に用いる署名アルゴリズムはCRYPTREC暗号リスト(注)のうち、「電子政府推奨暗号リスト」に記載された暗号技術を用いることとする。  (注)CRYPTREC暗号リストについては、最終更新版を参照することとする。 |  |  |
| 30 | **J10** 第10条（秘密鍵の保護装置）  **J10.1**  １　秘密鍵は、ハードウェア・セキュリティ・モジュール（FIPS 140-2のレベル3以上又はISO/IEC15408 EAL4＋以上（EN 419 221-5に対応するもの）の認証を受けた製品とし、以下「HSM」という。）を用いて保護することとする。 |  |  |
| 31 | **J11** 第11条（タイムスタンプの生成処理）  **J11.1**  １　タイムスタンプの生成処理においては、耐タンパ性を有する装置等を用いることとする。 |  |  |
| 32 | **J11.2**  ２　前項の装置等に実装された時刻情報の取得からタイムスタンプの生成に至るまでのプログラム等（以下「プログラム等」という。）が正確に動作することを説明できることとする。 |  |  |
| 33 | **J11.3**  ３　プログラム等には改ざんを防止する仕組みを備え、改ざんを検知した場合にはその結果を記録することとする。 |  |  |
| 34 | **J11.4**  ４　プログラム等にはタイムスタンプの生成に係る正常なプロセスが動作していること及び不要なプロセスが動作していないことを確認する仕組みを備え、不正な状態を検知した場合にはその結果を記録することとする。 |  |  |
| 35 | **J11.5**  ５　プログラム等の設定に関する操作は複数人管理のもと行うこととする。 |  |  |
| 36 | **J12** 第12条（秘密鍵の管理）  **J12.1**  １　秘密鍵は安全に管理することとする。 |  |  |
| 37 | **J12.2**  ２　秘密鍵は複数人管理のもと、信頼できる鍵生成装置によって生成し、次の各号に掲げる要件を満たした上で HSM内に保管することとする。 |  |  |
| 38 | **J12.2.1**  一　秘密鍵はバックアップを行わないこととする。なお、秘密鍵を保管するHSMに秘密鍵のバックアップ機能がある場合は、当該機能を使用できない設定にしておくこととする。 |  |  |
| 39 | **J12.2.2**  二　複数人の権限を有する者が揃わない限りはHSMの持ち出し等ができないようにすることとする。 |  |  |
| 40 | **J12.3**  ３　秘密鍵を用いてデジタル署名を付与する際には、HSM内部で安全に処理することとし、HSMのタイムスタンプ生成装置等への接続や、HSM内の秘密鍵を利用可能状態にする操作は、複数人管理のもとで行うこととする。 |  |  |
| 41 | **J12.4**  ４　秘密鍵の必要な期間が終了した場合や、秘密鍵が失効又は危殆化した場合等(注)は、その後の不正利用や継続利用が行われないように当該秘密鍵を廃棄することとする。また、電子証明書を発行する認証事業者が認証業務を終了する（失効に係る認証業務を継続する場合を除く）場合、当該認証事業者の認証業務終了までに、当該認証事業者の発行に係る電子証明書に対応する秘密鍵を、複数人管理のもとで、秘密情報を露顕又は残存させることなく安全に廃棄することとする。  (注)秘密鍵を用いていた認定業務が認定の効力を失った場合を含む。 |  |  |
| 42 | **J12.5**  ５　秘密鍵の更新を行い、新たな電子証明書を認定業務で用いる際には、当該電子証明書が第５条第４項の信頼できる認証事業者から発行を受けた、同条第３項の要件を満たすものであることを確認し、更新を反映して認定業務を行う前には、タイムスタンプが第45条第７号のプロファイルに即したものであることを確認することとする。 |  |  |
| 43 | **J12.6**  ６　秘密鍵は、第９条の暗号技術についてのCRYPTREC暗号リスト等の最新の安全性評価を基に、第45条第９号イのとおり、告示第６条に規定する規程（以下「運用規程」という。）でその有効期間及び活性化期間をあらかじめ適切に定めるとともに、定期的に更新する こととする。 |  |  |
| 44 | **J12.7**  ７　秘密鍵を第三者が利用可能となるような事態が生じた場合に備え、対応策を策定しておくこととする。 |  |  |
| 45 | **J13** 第13条（タイムスタンプの有効期間）  **J13.1**  １　第５条第３項第６号及び第９条の内容を満たす暗号技術や前条第６項で定めた秘密鍵の活性化期間を基に、第45条第９号ロのとおり運用規程でタイムスタンプの有効期間を適切に定め、秘密鍵の危殆化や暗号技術の安全性評価の更新等により当該期間が短縮される可能性があることと併せて、認定業務を利用して自らタイムスタンプを付与する者（以下「利用者」という。）に通知することとする。 |  |  |
| 46 | **K3.1.4**  四　当該時刻認証業務に係る電気通信システムに、十分なサイバーセキュリティ対策を講ずること。 | **J14** 第14条（認定業務等の特定）  **J14.1**  １　利用者からタイムスタンプの発行要求を受付ける際には、なりすまし対策を講じたウェブサイト等の認定業務を特定する手段を用いることとする。 |  |  |
| 47 | **J14.2**  ２　TAAを用いる場合、時刻配信を受けるTAAの配信元機器の特定及び認証が可能な手段を用いることとする。 |  |  |
| 48 | **J15** 第15条（安全な通信路）  **J15.1**  １　認定業務に係る通信には、なりすましや改ざんの防止、暗号化等の措置を講ずることとする。 |  |  |
| 49 | **J15.2**  ２　前項の措置を公開鍵暗号技術又は共通鍵暗号技術により実現する場合、CRYPTREC暗号リスト(注)のうち、「電子政府推奨暗号リスト」に記載された暗号技術を用いることとし、暗号鍵を安全に管理するに当たっては次の各号に掲げる要件を満たすこととする。  (注)CRYPTREC暗号リストについては、最終更新版を参照することとする。 |  |  |
| 50 | **J15.2.1**  一　暗号鍵は複数人管理のもと、信頼できる鍵生成装置によって生成することとする。 |  |  |
| 51 | **J15.2.2**  二　通信に用いる秘密鍵又は共通鍵は、十分なサイバーセキュリティが確保できる環境で保管することとする。 |  |  |
| 52 | **J15.2.3**  三　暗号鍵は、用いる暗号技術についての最新の安全性評価を基に、適切な有効期間を定めることとする。 |  |  |
| 53 | **J15.2.4**  四　暗号鍵の有効期間が経過した場合や、暗号鍵が失効又は危殆化した場合等は、その後の不正利用等が行われないように当該暗号鍵を廃棄することとする。 |  |  |
| 54 | **J16** 第16条（外部ネットワークとの接続）  **J16.1**  １　ファイアウォール等の、外部ネットワークからの不正アクセスや攻撃等を検知及び防御するためのシステムを備え、必要に応じてセキュリティ更新を行うこととする。 |  |  |
| 55 | **J17** 第17条（内部ネットワーク（LAN））  **J17.1**  １　認定業務を含む業務又はその機能ごとに、サーバ等の機器を適切に配置し、不要な通信を遮断できるようにすることとする。また、ネットワーク機器は必要に応じてセキュリティ更新がなされることとする。 |  |  |
| 56 | **J18** 第18条（サーバの設定）  **J18.1**  １　認定業務に係る全てのサーバについて、不要なポートの利用停止等の機能設定及びシステムログの記録等の運用管理を適切に行うこととする。なお、当該サーバは十分な 精度で時刻同期が取れていることとする。 |  |  |
| 57 | **J19** 第19条（システムの可用性）  **J19.1**  １　認定業務に係るシステムは、障害に備えて、認定業務を継続するための対策を実施することとする。 |  |  |
| 58 | **K3.1.5**  五　当該時刻認証業務に係る設備を含む建築物に、震災、風水害、落雷、火災その他これらに類する災害の被害を容易に受けないようにするための措置を講ずるとともに、十分な防犯対策を講ずること。 | **J20** 第20条（災害対策）  **J20.1**  １　認定業務に係る設備を含む建築物（以下「建築物」という。）は、その建築主が「建築基準法（昭和25年法律第201号）」第６条第１項の規定による確認済証の交付を受けていることとする。 |  |  |
| 59 | **J20.2**  ２　建築物は、建築基準法第２条第９の２号及び第９の３号に規定する耐火建築物又は準耐火建築物であることとし、自動火災報知機及び消火装置を設えることとする。 |  |  |
| 60 | **J20.3**  ３　建築物には、瞬時停電、電源検査及び災害時に認定業務を継続するに足りる無停電電源装置やバックアップ発電機等を設置することとする。 |  |  |
| 61 | **J20.4**  ４　建築物内では、認定業務に係る設備が認定業務を行うための性能を維持できる温湿度管理を行うこととする。 |  |  |
| 62 | **J20.5**  ５　認定業務に係る設備は、通常想定される規模の地震による転倒や構成部品の脱落などを防止するための構成部品の固定その他の耐震措置を講ずることとする |  |  |
| 63 | **J20.6**  ６　建築物には、第１項から前項までのほか風水害及び落雷の被害を容易に受けないようにするための措置を講ずることとする。 |  |  |
| 64 | **J21** 第21条（防犯対策）  **J21.1**  １　認定業務に係るシステム全体を、権限を有する者のみが開錠可能な別室に設置する、又は錠付きラックで囲うことにより安全性を確保することとする。 |  |  |
| 65 | **J21.2**  ２　認定業務に係るシステム全体が設置された部屋及び当該システムの操作室は、ICカード等により入退室の管理を実施することとする。 |  |  |
| 66 | **K3.1.6**  六　認定業務を利用して自らタイムスタンプを付与する者（以下「利用者」という。）及びタイムスタンプが付与された電子データを有し、かつ当該タイムスタンプの改ざん等に関する検証を行う者（以下「検証者」という。）に対し、電子データ及びそれに付されたタイムスタンプの改ざん等に関する検証を適切に行うに当たり必要な情報を提供すること。 | **J22** 第22条（検証処理の要件）  **J22.1**  １　利用者及びタイムスタンプが付与された電子データを有し、かつ当該タイムスタンプの改ざん等に関する検証を行う者（以下「検証者」という。）が次の各号に掲げる検証を適切に行うに当たり必要な情報を提供することとする。 |  |  |
| 67 | **J22.1.1**  一　検証の対象となるタイムスタンプのデータ形式の崩れや改ざんが判別できること。 |  |  |
| 68 | **J22.1.2**  二　当該タイムスタンプに電子証明書が含まれる場合、タイムスタンプ発行時における当該電子証明書の有効性を検証できること。 |  |  |
| 69 | **J22.1.3**  三　当該タイムスタンプに電子証明書が含まれない場合、安全なリポジトリから当該電子証明書を取得し、検証できること。 |  |  |
| 70 | **J22.1.4**  四　有効性を確認した公開鍵を用いて当該タイムスタンプに付与されたデジタル署名の有効性を検証できること。 |  |  |
| 71 | **J22.1.5**  五　当該タイムスタンプが有効である場合、当該タイムスタンプから当該タイムスタンプの付与対象となる電子データの改ざんが判別できること。 |  |  |
| 72 | **K3.1.7**  七　当該時刻認証業務を継続的に安定して遂行するに足りる経理的基礎及び技術的能力その他の能力を有すること。 | **J23** 第23条（経理的基礎）  **J23.1**  １　経理的基礎について、財政の状況（過事業年度に係るものを含む財産目録、貸借対照表、損益計算書、事業計画書等）は次の各号に掲げる要件を満たすこととする。 |  |  |
| 73 | **J23.1.1**  一　継続的な債務超過がないなど、認定業務の継続的かつ安定した遂行が担保できること。 |  |  |
| 74 | **J23.1.2**  二　賠償責任保険に加入しているなど、損害賠償請求をされた場合に対応できる能力があること。 |  |  |
| 75 | **J23.2**  ２　前項第１号に係る情報については、認定事業者において公表することとする。 |  |  |
| 76 | **J24** 第24条（技術的能力）  **J24.1**  １　技術的能力については、時刻やサイバーセキュリティに関する専門性の優れた要員を配置し、認定業務を継続的に安定して遂行するための教育訓練を行うこととする。 |  |  |
| 77 | **K3.1.9**  九　利用者及び検証者に、必要に応じて当該時刻認証業務に関連する情報を提供すること。 | **J25** 第25条（利用者及び検証者への必要に応じた情報提供）  **J25.1**  １　運用規程の公表に加え、利用者及び検証者に、必要に応じて次の各号に掲げる情報を提供することとする。 |  |  |
| 78 | **J25.1.1**  一　時刻の品質を証明するために必要な情報(注)  (注)TAAを用いる場合、時刻監査証、監査記録 |  |  |
| 79 | **J25.1.2**  二　電子証明書の有効期間 |  |  |
| 80 | **J25.1.3**  三　電子証明書の失効情報の公開場所 |  |  |
| 81 | **J25.1.4**  四　検証のための情報  イ　電子証明書並びにその発行に係るルート認証局（及び使用している場合は中間認証局）の公開鍵証明書  ロ　検証手順、ツール等の検証方法 |  |  |
| 82 | **J25.1.5**  五　利用者の個人情報についての開示請求手続き等の情報 |  |  |
| 83 | **J25.1.6**  六　その他各号に掲げる運用規程の記載事項以外の注意事項 |  |  |
| 84 | イ　タイムスタンプの付与対象となる電子データの保存期間内にタイムスタンプの有効期間が満了する場合は、当該有効期間内にタイムスタンプの再付与等の措置が必要となること。 |  |  |
| 85 | ロ　本認定は有効期間を超過したタイムスタンプの信頼性を裏付けるものではないこと。 |  |  |
| 86 | ハ　認定業務に用いる暗号アルゴリズムの安全性評価や危殆化等によりタイムスタンプの有効期間が短縮される可能性があること。 |  |  |
| 87 | **J25.2**  ２　前項の提供情報の内容に変更があったときは、速やかに利用者へ連絡することとする。 |  |  |
| 88 | **K3.1.10**  十　その他確実かつ安定的にタイムスタンプを発行するために必要な措置を講ずること。 | **J26** 第26条（組織・人事管理）  **J26.1**  １　次の各号に掲げる要件を満たし、適切な組織構成並びに認定業務の開発・運用の維持、信頼性及び可用性の確保に必要な能力・体制を確保することとする。 |  |  |
| 89 | **J26.1.1**  一　事故を未然に防ぐための内部牽制が働く組織構造、業務手順を有すること。 |  |  |
| 90 | **J26.1.2**  二　認定業務に直接従事しない者からの業務監査等のチェック機能が働くこと。 |  |  |
| 91 | **J26.1.3**  三　事故発生時に、その発生源を特定し適切に対応するための手順を定めておくこと。 |  |  |
| 92 | **J26.1.4**  四　災害、セキュリティ事故等の発生が利用者に大きな影響を与える可能性があることを認識し、利用者へのこれらの影響を最小限に抑えた事業継続計画を策定した上で平時から事業継続に留意すること。 |  |  |
| 93 | **J27** 第27条（認定業務の運用に関する記録の取得と保管）  **J27.1**  １　本実施要項の他の条項に定めのあるものに加え、認定業務の運用に関する重要な記録について完全性と機密性を保ちながら、必要に応じて利用できるように保管することとする。 |  |  |
| 94 | **J27.2**  ２　前項の記録は、その保管期間を明記の上、文書化しておくこととする。なお、保管期間は、認定業務において発行するタイムスタンプが有効である間は最低限確保することとする。 |  |  |
| 95 | **J28** 第28条（システムのトラブル、破壊からの復旧）  **J28.1**  １　認定業務で用いる時計システムの時刻精度が45条第１項第２号のとおり運用規程で保証する範囲から外れた場合は、システムトラブルとみなし、システムの緊急停止及び復旧作業を速やかに行うこととする。 |  |  |
| 96 | **J28.2**  ２　ハードウェア、ソフトウェア又はデータが破壊された場合は、バックアップ用のハード ウェア、ソフトウェア又はデータにより速やかに復旧作業を行うこととする。 |  |  |
| 97 | **J29** 第29条（提供する業務の明確化）  **J29.1**  １　次の各号に掲げる内容を含む認定業務について、文書で明確に定めることとする。 |  |  |
| 98 | **J29.1.1**  一　利用者のリクエストに応じてタイムスタンプを生成・発行すること。 |  |  |
| 99 | **J29.1.2**  二　認定業務で用いる全ての時計の時刻を十分な精度に維持すること。 |  |  |
| 100 | **J29.1.3**  三　認定業務で用いる暗号鍵を安全に生成し、管理すること。 |  |  |
| 101 | **J29.1.4**  四　認定業務で用いる秘密鍵又は暗号アルゴリズムの危殆化が発覚した場合は、速やかに使用を中止するとともに利用者に連絡すること。 |  |  |
| 102 | **J29.1.5**  五　前号の場合において、速やかに失効請求を行う義務を明示すること。 |  |  |
| 103 | **J29.1.6**  六　認定業務を廃止する時や用いる電子証明書の記載事項に変更がある場合、当該電子証明書を発行する認証事業者が定める方法により当該認証事業者に通知すること。 |  |  |
| 104 | **J29.1.7**  七　利用者及び検証者に第22条各号に定める情報を提供すること。 |  |  |
| 105 | **K3.５**  ５　認定を受けた者（以下「認定事業者」という。）は、認定業務について、認定業務であることが分かりやすい表示を行わなければならない。 |  |  |  |
| 106 | **K3.６**  ６　認定事業者は、自らが営む認定業務以外の時刻認証業務について、認定業務である旨の表示又は認定業務であると誤解を招くおそれのある紛らわしい表示を行ってはならない。 |  |  |  |
| 207 | **K5**第5条（変更の認定等）  １　認定事業者は、認定業務の変更（軽微な変更を除く。）をしようとするときは、あらかじめ、総務大臣の認定を受けなければならない。  ２　第三条第一項から第四項までの規定は、前項の変更の認定に準用する。  ３　認定事業者は、認定業務を休止又は廃止しようとするときは、あらかじめその旨を、タイムスタンプの改ざん等に関する検証を適切に行うに当たり必要な情報の継続的な提供その他の利用者及び検証者を保護するために十分な内容を含む終了計画又は再開計画と併せて総務大臣に届け出なければならない。  ４　総務大臣は、前項の規定による届出があったときは、その旨を速やかに公示する。  ５　第一項及び第三項の場合において、認定事業者は、利用者及び検証者へ速やかに通知又は連絡するよう努めなければならない。 | **J41** 第41条 （休廃止時等の利用者等への通知又は連絡）  **J41.1**  １　認定事業者は、次の各号に掲げる場合には、速やかにその旨を利用者及び検証者へ通知又は連絡するよう努めることとする。  一 認定業務の変更の認定を受けた場合。  二 総務大臣に対し、第36条第１項第２号の変更を届け出た場合。  三 総務大臣に対し、認定業務の休止を届け出た場合。  四 総務大臣に対し、認定業務の再開を届け出た場合。  五 総務大臣に対し、認定業務の廃止を届け出た場合。 |  |  |
| 108 | **J41.2**  ２ 前項の利用者及び検証者への通知又は連絡は、電話や電子メール、ホームページ等の日常的に利用でき、かつ広く周知を図ることができる方法により行うものとする。 |  |  |
| 109 | **J42** 第42条（休止時の利用者等への通知事項等）  **J42.1**  １　認定事業者は、休止時において利用者及び検証者の利益を保護するために必要な事項として、次の各号に掲げる事項について通知又は連絡するよう努めることとする。  一 休止しようとする認定業務の内容  二 休止しようとする年月日  三 休止しようとする期間  四 休止の理由  五 休止しようとする認定業務に関する利用者及び検証者からの苦情又は相談に応ずる営業所又は事務所の連絡先  六 休止しようとする認定業務に係る役務の代替となる役務（当該認定業務に係る役務と当該代替となる役務との比較検討が可能となる情報を含む。）  七 休止しようとする認定業務に係る役務に関する利用者及び検証者の被害の発生又は拡大の防止に資する情報 |  |  |
| 110 | **J43** 第43条（再開時の利用者等への通知事項等）  **J43.1**  １　認定事業者は、再開時において利用者及び検証者の利益を保護するために必要な事項として、再開計画を通知又は連絡するよう努めることとする。 |  |  |
| 111 | **J44** 第44条（廃止時の利用者等への通知事項等）  **J44.1**  １　認定事業者は、廃止時において利用者及び検証者の利益を保護するために必要な事項として、次の各号に掲げる事項について通知又は連絡するよう努めることとする。  一 廃止しようとする認定業務の内容  二 廃止しようとする年月日  三 廃止の理由  四 廃止しようとする認定業務に関する利用者及び検証者からの苦情又は相談に応ずる営業所又は事務所の連絡先  五 廃止しようとする時刻認証業務に係る役務の代替となる役務（当該認定業務に係る役務と当該代替となる役務との比較検討が可能となる情報を含む。）  六 廃止しようとする認定業務に係る役務に関する利用者及び検証者の被害の発生又は拡大の防止に資する情報 |  |  |
| 112 | **K6** 第6条（運用規程）  **K6.1**  １　認定事業者は、自らが営む認定業務について、第三条第一項第一号から第七号まで、第九号及び第十号を満たす内容及び運用並びに免責事項に関する規程を定め、公表しなければならない。これを変更しようとするときも、同様とする。 | **J45** 第45条（運用規程）  **J45.1**  １　運用規程には、次の各号に掲げる内容を含むこととする。なお、運用規程に認定業務以外の時刻認証業務に関する内容は含めないこととする。 |  |  |
| 113 | **J45.1.1**  一　事業者情報  イ　氏名又は名称(注)及び住所  (注)氏名又は名称については、英語での表記も付すこととする。  ロ　電話番号、電子メールアドレス等の問い合わせ窓口情報 |  |  |
| 114 | **J45.1.2**  二　UTC（NICT）との最大時刻差等の、タイムスタンプの時刻に関し保証する時刻精度 |  |  |
| 115 | **J45.1.3**  三　時刻の品質を証明するために必要な情報の開示方法 |  |  |
| 116 | **J45.1.4**  四　認定業務の内容と認定事業者の責務 |  |  |
| 117 | **J45.1.5**  五　認定事業者が負う賠償責任の範囲と免責事項 |  |  |
| 118 | **J45.1.6**  六　認定業務の安全性や信頼性を判断できる技術情報 |  |  |
| 119 | **J45.1.7**  七　タイムスタンプのプロファイル |  |  |
| 120 | **J45.1.8**  八　認定業務で用いる暗号アルゴリズムに関する情報  イ　ハッシュ値を得るためのハッシュ関数及び告示第３条第１項第１号のデジタル署名に用いる署名アルゴリズム  ロ　認定業務で用いる暗号アルゴリズムが危殆化した場合の対応策  ハ　認定業務で用いる暗号アルゴリズムの危殆化がタイムスタンプの有効期間内に予測される場合の対応策 |  |  |
| 121 | **J45.1.9**  九　タイムスタンプの有効期間  イ　秘密鍵の有効期間及び活性化期間  ロ　タイムスタンプの有効期間 |  |  |
| 122 | **J45.1.10**  十　検証のための情報  イ　電子証明書並びにその発行に係るルート認証局（及び使用している場合は中間認証局）の公開鍵証明書の入手方法  ロ　検証手順、検証ツール等の検証方法に関する情報 |  |  |
| 123 | **J45.1.11**  十一　認定業務の提供時間帯 |  |  |
| 124 | **J45.1.12**  十二　認定業務の利用に関する情報  イ　認定事業者が定める認定業務の利用規約  ロ　認定業務の利用に関わる注意事項 |  |  |
| 125 | **J45.1.13**  十三　運用体制、マシン室のレイアウト、監査情報、設備・システムのセキュリティ等の機密情報（以下「機密情報」という。）及び認定業務の運用に際して知り得た利用者をはじめとする者の個人情報（以下「個人情報」という。）に関する取扱い  イ　個人情報の取得及び利用に関わる要件  ロ　機密情報及び個人情報の管理に関わる要件  ハ　機密情報及び個人情報の保存期間に関わる要件  ニ　機密情報及び個人情報の廃棄に関わる要件  ホ　機密情報及び個人情報の開示に関わる要件 |  |  |
| 126 | **J45.1.14**  十四　認定業務の廃止又は一時停止時に認定事業者がとる対応と利用者への通知 |  |  |
| 127 | **J45.1.15**  十五　認定業務に用いる暗号鍵の管理、更新時期、危殆化時の対応 |  |  |
| 128 | **J45.1.16**  十六　システムトラブル、システム破壊、災害発生時に認定事業者がとる対応と利用者へ の通知方針 |  |  |
| 129 | **J45.1.17**  十七　準拠法令 |  |  |
| 130 | **J45.1.18**  十八　その他告示第３条第１項第１号から第７号まで、第９号及び第10号を満たすことが確認できる情報 |  |  |
| 131 | **J45.2**  ２　前項の記載事項の内容に変更があるときは、変更を反映した運用規程を速やかに公表することとする。 |  |  |
| 132 | **K7** 第7条（個人情報等の取扱い）  **K7.1**  １　認定事業者は、認定業務の運用に際して知り得た個人情報をはじめとする重要な情報について、適正な取扱いの確保のための措置をとらなければならない。 | **J46** 第46条（個人情報等の取扱い）  **J46.1**  １　機密情報及び個人情報については、施錠を行い物理的に隔離された設備において保管するなど、適正な保護のための措置を講ずることとする。 |  |  |
| 133 | **J46.2**  ２　機密情報については、認定業務に直接従事する者を特定した上で、漏えいした際の認定業務への影響度を十分考慮した取扱い方法を定め、それに従った運用を行うこととする。 |  |  |
| 134 | **J46.3**  ３　個人情報については、目的外利用や漏えいがないように取扱い方法を定め、それに従った運用を行うこととする。 |  |  |
| 135 | **K8** 第8条（実施状況の報告等）  **K8.1**  １　認定事業者は、認定業務の運用の適正性について、毎年、自ら（認定業務に直接従事する者を除く。）監査を行い、又は第三者による監査を受け、当該監査の結果を総務大臣に報告しなければならない。  **K8.２**  ２　総務大臣は、認定制度の適正な運営のために必要があると認めるときは、認定事業者に対し、実地の調査等を行うことができる。  **K8.3**  ３　総務大臣は、前項の調査等の結果に基づき、認定制度の適正な運営のために必要があると認めるときは、認定事業者に対し、改善その他必要な措置を講ずるよう指導することができる。  **K8.4**  ４　総務大臣は、前項の規定による指導を行ったときは、その旨を遅滞なく公表する。 | **J47** 第47条（監査）  **J47.1**  １　認定事業者は、認定業務が本実施要項に沿って適切に運営されていることを確認する監査を計画し、実施することとする。 |  |  |
| 136 | **J47.2**  ２　認定事業者は、保管すべき監査情報と保管期間を定めるとともに、保管に当たってはアクセス権限を明確にし、完全性及び機密性を保つための措置を講ずることとする。 |  |  |
| 137 | **J47.3**  ３　監査は、最低年１回実施することとする。 |  |  |
| 138 | **J47.4**  ４　認定事業者は、監査実施後に、総務大臣に対して監査結果を速やかに報告するものとし、監査の結果として改善その他必要な措置が指摘された場合には、次に掲げる事項につい て速やかに対処することとする。 |  |  |
| 139 | **J47.4.1**  一　必要な措置が講じられるまでの運用の停止や利用者及び検証者への通知又は連絡等 |  |  |
| 140 | **J47.4.2**  二　必要な措置の実施 |  |  |
| 141 | **K11**第11条（報告の義務）  １　認定事業者は、認定業務の確実性又は安定性を損なうおそれがある事態が発生又は発覚した場合は、速やかに総務大臣へその旨を通知するとともに、必要な対処を行い、その経過を報告しなければならない。  ２　前項の場合において、認定事業者は、速やかに利用者及び検証者への通知又は連絡に努めなければならない。  ３　総務大臣は、第一項の場合において、必要に応じ、速やかに次条第一項の指定調査機関に情報を共有する。 | **J55** 第55条 （通知等を要する緊急事態）  １　「認定業務の確実性又は安定性を損なうおそれがある事態」とは、次の各号に掲げるものとする。  一 認定業務で用いる秘密鍵又は暗号アルゴリズムの危殆化が発覚する事態  二 認定業務で用いる暗号アルゴリズムの危殆化が有効期間内に予測される事態  三 認定業務に係る設備・システムの重大な故障、自然災害又はセキュリティ事故等の発生により当該認定業務の運営に大きな影響を与える可能性がある事態  四 その他タイムスタンプを発行する当該認定業務の全部又は一部の提供を停止又は品質を低下させる事態 |  |  |
| **J56** 第56条 （緊急時の利用者等への通知又は連絡）  １　認定業務の確実性又は安定性を損なうおそれがある事態が発生又は発覚した場合の利用者及び検証者への通知又は連絡は、電話や電子メール、ホームページ等の日常的に利用でき、かつ広く周知を図ることができる方法により行うものとする。  ２ 通知又は連絡の内容については、事態への対処状況又はその方針についても含むこととする。 |  |  |