

時刻認証業務の認定に関する実施要項の一部の改正案新旧対照条文

改正後	改正前
<p>(定義)</p> <p>第2条 (略)</p> <p>一 (略)</p> <p>二 TAA(Time Assessment Authority) <u>時刻配信業務(情報通信ネットワークを利用する上で必要となるサーバ等の電気通信設備に用いられる時刻に高い信頼性を与えるため情報通信ネットワークを通じて時刻情報を配信する業務、更に配信先の時刻精度を計測して報告を行う時刻監査業務)を行う者</u></p> <p>(電子証明書)</p> <p>第5条 (略)</p> <p>2 (略)</p> <p>3 (略)</p> <p>一～五 (略)</p> <p>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、「<u>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)</u>」(令和5年3月30日デジタル庁・総務省・経済産業省策定)(注)のうち、「<u>電子政府推奨暗号リスト</u>」に記載された公開鍵暗号技術を用いられていること。</p> <p>(注) (略)</p> <p>七 (略)</p> <p>4 (略)</p> <p>一～三 (略)</p> <p>(時刻源)</p> <p>第6条 (略)</p> <p>2 (略)</p> <p><u>(注)TAAを除く。</u></p> <p>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、<u>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。</u></p> <p>(時刻の品質管理及び証明)</p> <p>第7条 (略)</p> <p>一～三 (略)</p>	<p>第2条 (同左)</p> <p>一 (同左)</p> <p>二 TAA(Time Assessment Authority) <u>時刻配信業務</u>を行う者</p> <p>(電子証明書)</p> <p>第5条 (同左)</p> <p>2 (同左)</p> <p>3 (同左)</p> <p>一～五 (同左)</p> <p>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、<u>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)」</u>(注)のうち、「<u>電子政府推奨暗号リスト</u>」に記載された公開鍵暗号技術を用いられていること。</p> <p>(注) (同左)</p> <p>七 (同左)</p> <p>4 (同左)</p> <p>一～三 (同左)</p> <p>(時刻源)</p> <p>第6条 (同左)</p> <p>2 (同左)</p> <p><u>(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。</u></p> <p>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、<u>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。</u></p> <p>(時刻の品質管理及び証明)</p> <p>第7条 (同左)</p> <p>一～三 (同左)</p>

<p>(削る)</p> <p><u>四</u> (略)</p> <p>2 (略)</p> <p>3 (略)</p> <p>(タイムスタンプの生成に関わる暗号技術)</p> <p>第9条 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」という。）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。</p> <p>(注) (略)</p>	<p><u>四</u> 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 を用いる場合に限り）</p> <p><u>五</u> (同左)</p> <p>2 (同左)</p> <p>3 (同左)</p> <p>(タイムスタンプの生成に関わる暗号技術)</p> <p>第9条 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」という。）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。</p> <p>(注) (同左)</p>
<p>(秘密鍵の保護装置)</p> <p>第10条 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以上若しくはFIPS 140-3のレベル3以上(注)又はISO/IEC 15408 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。</p> <p><u>(注)運用中のHSMの認証ステータスが「Historical」に移行した場合においては、その要因が秘密鍵の保護等に影響を及ぼさないものであることを確認することが求められる。</u></p>	<p>(秘密鍵の保護装置)</p> <p>第10条 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/IEC 15408 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。</p> <p>(新設)</p>
<p>(認定業務等の特定)</p> <p>第14条 (略)</p> <p>(削る)</p>	<p>(認定業務等の特定)</p> <p>第14条 (同左)</p> <p><u>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。</u></p>
<p>(安全な通信路)</p> <p>第15条 認定業務に係る通信のうち、利用者との通信路等、重要な通信路には安全対策措置を講ずることとする。</p> <p>2 (略)</p> <p>一 暗号鍵は複数人管理(注)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。</p> <p><u>(注)通信の都度、生成・破棄される暗号鍵は、信頼できる鍵生成装置によって自動生成・破棄することができる。</u></p> <p>二～四 (略)</p>	<p>(安全な通信路)</p> <p>第15条 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。</p> <p>2 (同左)</p> <p>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。</p> <p>(新設)</p> <p>二～四 (同左)</p>
<p>(防犯対策)</p> <p>第21条 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又は錠付きラックに設置することにより安全性を確保することとする。</p>	<p>(防犯対策)</p> <p>第21条 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。</p>

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し、これらに設置された設備は原則として外部に持ち出してはならない。

(利用者及び検証者への必要に応じた情報提供)

第25条 (略)

一 時刻の品質を証明するために必要な情報

(削る)

二～六 (略)

2 (略)

(認定の申請)

第30条 (略)

一 (略)

(注) いずれも、英語での表記も付すこととする。

二～九 (略)

(認定の公示)

第32条 (略)

2～3 (略)

4 タイムスタンプの検証に必要な情報については、当該有効期限後も総務省ホームページに掲載する。

(認定の更新の申請)

第33条 認定事業者は、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6月前から4月前までに、第30条に規定する申請書及び文書を、総務大臣に提出することとする。

2 第4条から第32条までの規定は、認定の更新に準用する。なお、認定の更新の公示については、総務省のホームページへの掲載によるのみ行う。

(軽微な変更)

第36条 (略)

一～二 (略)

2 認定事業者は、前項第2号の変更があったときは、遅滞なく、次の各号に掲げる事項を記載した文書及び第30条第6号に規定する文書を総務大臣に届け出ることとする。

一 (略)

二 (略)

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。

(利用者及び検証者への必要に応じた情報提供)

第25条 (同左)

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

二～六 (略)

2 (同左)

(認定の申請)

第30条 (同左)

一 (同左)

(注) (法人にあってはその代表者の) 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。

二～九 (同左)

(認定の公示)

第32条 (同左)

2～3 (同左)

(新設)

(認定の更新の申請)

第33条 認定事業者は、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4月前から2月前までに、第30条に規定する申請書及び文書を、総務大臣に提出することとする。

2 第4条から第32条までの実施要項は、認定の更新に準用する。なお、認定の更新の公示については、総務省のホームページへの掲載によるのみ行う。

(軽微な変更)

第36条 (同左)

一～二 (同左)

2 認定事業者は、前項第2号の変更があったときは、遅滞なく、次の各号に掲げる事項を記載した文書を総務大臣に届け出ることとする。

一 (同左)

二 (同左)

(注) いずれも、英語での表記も付すこととする。

三 (略)

(注) いずれも、英語での表記も付すこととする。

四～五 (略)

3～4 (略)

(変更の認定)

第37条 (略)

一～五 (略)

2 第4条から第32条までの規定は、変更の認定に準用する。

(指定の公示)

第65条 (略)

2 (略)

一 指定調査機関の名称、住所、調査等の業務を行う事務所の所在地及び法人番号

二 (略)

3 (略)

(変更の届出)

第66条 指定調査機関は、告示第15条各号、第60条第1項第1号若しくは第2号又は同条第2項第5号ニの内容を変更しようとするときは、変更しようとする日の2週間前までに、次の各号に掲げる事項を記載した届出書を総務大臣に届け出ることとする。

一～四 (略)

2 指定調査機関は、第60条第2項第5号イ又はハの内容に係る変更をしようとするときは、遅滞なく、次の各号に掲げる事項を記載した届出書を総務大臣に届け出ることとする。

一～四 (略)

3 (略)

(指定調査機関に係る変更の公示)

第67条 前条第1項の届出による変更の公示は、官報への掲載で告示することによって行う。

2 (同左)

一～三 (同左)

3 前条第1項の届出による変更に関する、前項各号を含む事項は、総務省ホームページにも掲載する。

(注) (法人にあってはその代表者の) 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。

三 (同左)

(注) (法人にあってはその代表者の) 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。

四～五 (同左)

3～4 (同左)

(変更の認定)

第37条 (同左)

一～五 (略)

2 第4条から第32条までの実施要項は、変更の認定に準用する。

(指定の公示)

第65条 (同左)

2 (同左)

一 指定調査機関の名称及び住所並びに調査等の業務を行う事務所の所在地

二 (同左)

3 (同左)

(変更の届出)

第66条 指定調査機関は、第60条第1項第1号若しくは第2号又は同条第2項第5号イ、ニ若しくはハへの文書の内容を変更しようとするときは、変更しようとする日の2週間前までに、次の各号に掲げる事項を記載した届出書を総務大臣に届け出ることとする。

一～四 (略)

2 指定調査機関は、告示第15条各号の内容に係る変更をしようとするときは、変更しようとする日の2週間前までに、次の各号に掲げる事項を記載した届出書を総務大臣に届け出ることとする。

一～四 (略)

3 (同左)

(指定調査機関に係る変更の公示)

第67条 前条第1項又は第2項の届出による変更の公示は、官報への掲載で告示することによって行う。

2 (同左)

一～三 (同左)

3 前条第1項又は第2項の届出による変更に関する、前項各号を含む事項は、総務省ホームページにも掲載する。