第6回 タイムスタンプ認定制度に関する検討会

資料６－２

各論点について

2020年9月23日

タイムビジネス認定センター長
伊地知　理

一般財団法人
日本データ通信協会

1. TSAが自ら時刻の信頼性を確保する方式

現状（タイムビジネス信頼・安心認定制度）

- TAA方式による時刻の信頼性の担保
  - 時刻の「精度」について、認定TAAから時刻配信を受けUTC（NICT）に対し±1秒以内で同期していることを規定※1
  - 時刻の「精度の証明」について、認定TAAによる時刻監査を受けることを規定※2
  - 時刻精度を満たしていないタイムスタンプ発行の防止措置を講じることを規定※3
- 時刻のトレーサビリティの担保
  - 認定TAAによる時刻監査記録はじめ、時刻認証業務の運用に関する記録の取得と保管を規定※4
  - 記録は全て期間を決めて保管することを規定※4

※1 **タイムビジネス信頼・安心認定制度　時刻認証業務審査基準（デジタル署名を使用する方式）（1）技術基準 2. 精度**
TSA時計は、認定TAAから時刻配信を受け、UTC (NICT)に対し±1秒以内で同期していること

※2 **（1）技術基準 3. 精度の証明／3. 2　認定を受けたTAAによる時刻監査**
第三者もしくは時刻認証業務とは権限分離された組織が運営し、時刻配信業務についてタイムビジネス信頼・安心認定を受けた機関がTAAとしてTSA時計の時刻監査を行っていることを証明できること

※3 **（1）技術基準　16. タイムスタンプトークンの時刻の品質／16. 2　時刻の品質の管理**
TSAは（1）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トークンの発行を防止するための措置を講じること。当該措置としてタイムスタンプトークンに含まれる時刻を外部の参照時計を用いて監視する場合、異常発生時には異常が明示され、また時刻差が記録されること

※4 **（2）運用基準　7. 時刻認証業務の運用に関する記録の取得と保管**
時刻認証業務の運用に関する重要な事象およびデータを記録すること、また、記録は全て期間を決めて保管すること
7. 3　記録する情報　a）時刻配信局より受けた時刻監査記録(または時刻監査証明書のコピー)／b）タイムスタンプトークン生成に使用する鍵ペアの生成・失効記録ならびに秘密鍵廃棄の記録／c）時刻認証業務にかかわるシステムの動作異常の記録

1. TSAが自ら時刻の信頼性を確保する方式

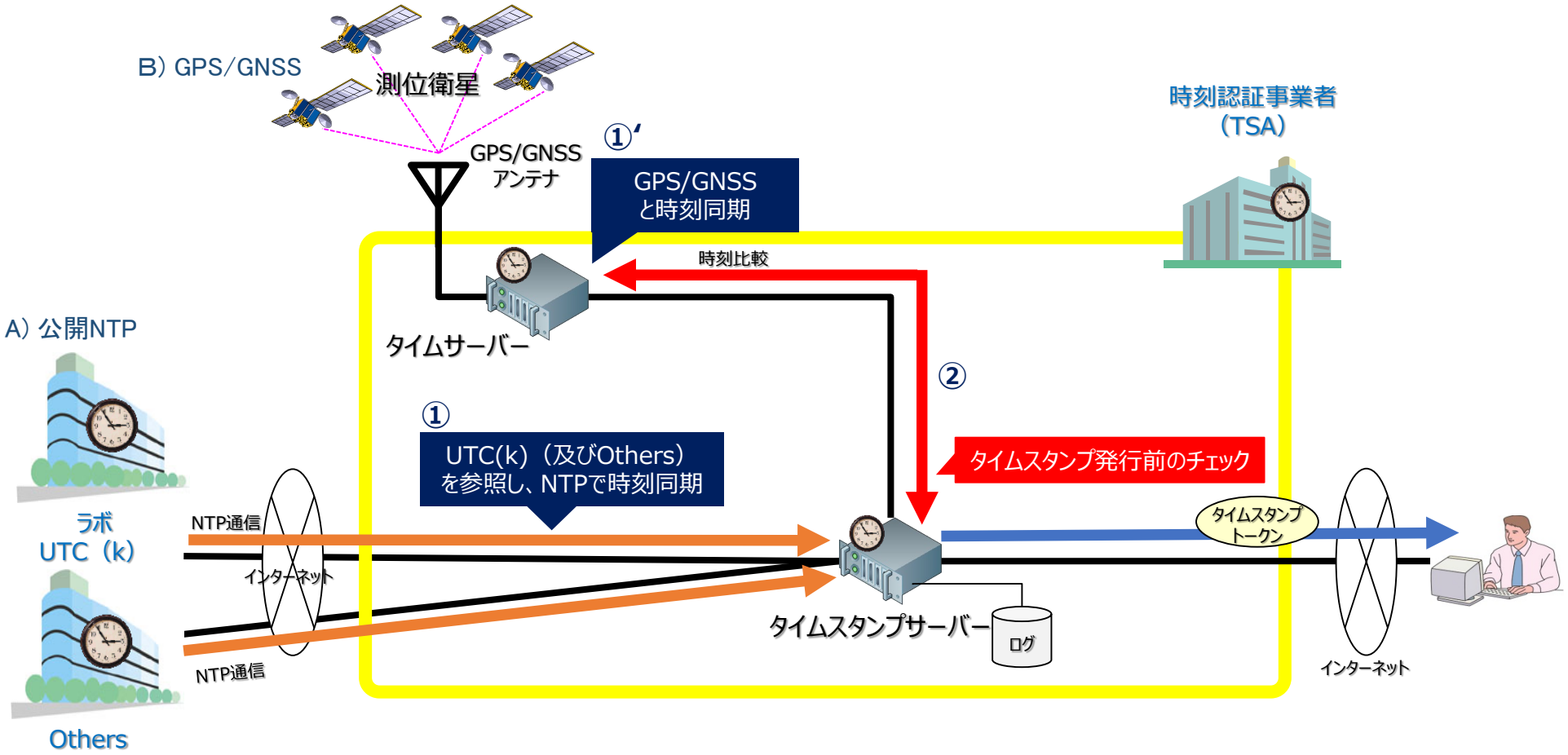
EUに関する調査結果※1

- トレーサビリティの起点となる時刻源について、**UTC(k)**であることを規定
  - EU各国がそれぞれの時刻標準機関を有しているわけではないことを前提として、主に以下の理由から、世界各国の時刻標準機関(k)であっても可としている
    ① UTC自体が世界で合意された標準時刻
    ② ETSI規格は、EU域外でも利用できる
    ③ トラストサービスプロバイダーが、EU域外にデータセンターを保有している場合もある
  - なお、ETSIの規格では時刻の信頼性を確保するための具体的な方法(特定の機器構成、複数の時刻源の使用等)に限定していない
- 発行するタイムスタンプの時刻精度の基準はトレーサビリティの起点となる時刻である**UTC(k)との差を±1秒以内**とし、**発行前にその精度の確認**を行うことを規定
  - なお、精度確認の具体的な方法は限定していない
- 時刻のトレーサビリティを担保するための情報として、**タイムスタンプサーバーの時刻同期イベントのログを保存**することを規定
  - 当該情報の保存期間について、具体的な年限の要件を定めていない
    - 参考)一般的には、TSA公開鍵証明書の有効期間が切れてから10年保存とする事例が多い。

※1㈱野村総合研究所によるTUV-IT社へのヒアリング結果(総務省委託事業)

1. TSAが自ら時刻の信頼性を確保する方式

EUにおけるTSAの時刻の信頼性確保例



- 複数の時刻源を用いることは任意で、UTC(k)にトレーサブルであることが求められる
- タイムスタンプ発行前の時刻精度(±1秒以内)確認用の時刻について、特定の手段や時刻源を指定していない
- トレーサビリティの担保のために、タイムスタンプサーバーでのログの保管を義務づけ(その他の機器は任意)

1. TSAが自ら時刻の信頼性を確保する方式

中国に関する調査結果※1

- タイムスタンプに関する認定制度はないが、TSAは主に以下の基準を参照
  - 国際規準：RFC3161
  - 中国国家（推奨）規準
    - GBT36631-2018「情報安全技術 タイムスタンプ策略及びタイムスタンプ業務操作規則」
    - GBT20520-2006「情報安全技術 公開鍵基礎設備 タイムスタンプ規範」

> 中国国家（推奨）規準では、**時刻源としてUTC(NTSC)を用いること**を基準として示している
>
> なお、時刻取得の手段（NTSC認可のハードウェア、NTPサーバ、GNSS（北斗）、長波 等）は限定していない
> また、内部監査用に、時刻同期等の各種ログの記録について基準を示している

  - TSA各社の内部規則（非公開）

- また、中国国家時刻標準機構である国家授時センター（NTSC）が唯一正式に業務提携するTSAとして联合信任技术服务有限公司（UTSA）※2が存在
  - 時刻はUTC(NTSC)に同期
  - NTSC認可のハードウェア及び方法で取得する時刻を使用
  - タイムスタンプ発行前の時刻精度確認は実施していないが、NTSC認可のハードウェアに対するNTSCによる定期的な時刻精度の確認、監査を実施

※1 ㈱野村総合研究所によるヒアリング結果（総務省委託事業）
※2 UTSAは中国政府の関連企業であることから、発行されたタイムスタンプに対する信頼度も高く、中国裁判所は証拠として採用しているタイムスタンプのほとんどがUTSAが発行するタイムスタンプである

1. TSAが自ら時刻の信頼性を確保する方式

論点について

① 時刻の信頼性の担保

- トレーサビリティの起点となる時刻源は、日本標準時決定機関である「NICT」のUTC（NICT）とすべきか、各国の時刻標準機関 “k”によるUTC（k）でも可とするか
- 発行されるタイムスタンプの時刻とトレーサビリティの起点となる時刻源の時刻差（時刻精度）の基準はどうあるべきか。
- タイムスタンプ発行前の時刻精度の確認（時刻が一定の基準内に収まっているかどうか）を要件として求めることが適切か。

② 時刻のトレーサビリティの担保

- TSAが自らトレーサビリティを立証するために、適切な機器のログを保管させることで十分か。
- 十分である場合、適切な「機器」、「ログ」とは何か。

1. TSAが自ら時刻の信頼性を確保する方式

方向性に関する見解

① 時刻の信頼性の担保

- トレーサビリティの起点となる時刻源について
  - NICTが日本標準時を管理していることを踏まえ、**「NICT」のUTC（NICT）に対してトレーサブルであることを求める**ことが適切ではないか。
  - 参考）NICTが提供している時刻提供手段：
    - 時刻情報提供サービス、光テレホンJJY、長波JJY、みちびき、公開NTPサーバー　等
- 発行するタイムスタンプの時刻精度について
  - 国際標準やEUの規定も踏まえ、**トレーサビリティの起点となる時刻源±1秒以内**とすることが適当ではないか。
- タイムスタンプ発行前の時刻精度の確認について
  - 現行の制度及びEUの規定も踏まえ、基準から外れたタイムスタンプの発行を防止するために、**タイムスタンプ発行前に時刻精度の確認を行う**ことが適切ではないか。

② 時刻のトレーサビリティの担保

- ログ等の保管について
  - 発行したタイムスタンプ時刻の時刻源とのトレーサビリティをTSA自身が立証するために、**適切な機器における適切なログの保管**を規定することが望ましいのではないか。
  - なお、適切な“機器”や“ログ”については、具体的な審査基準検討の場において、具体的な議論が必要

2. 認定の有効期間

タイムスタンプ発行に用いる鍵の更新と認定の期間の関係

- 現状（タイムビジネス信頼・安心認定制度）
  - 鍵更新は、複数人管理のもとで行い、作業記録を残すことを義務付けており、2年に1回の更新審査及び1年に1回の監査で確認

✓ TSA事業者は、タイムスタンプ発行に用いる秘密鍵の使用期間を1年程度に規定
  - 毎年、鍵ペアを生成し、それに伴い認証局から新たな公開鍵証明書の発行を受けている

✓ タイムスタンプ発行に用いる秘密鍵は、機器（タイムスタンプサーバー）毎、タイムスタンプサービス毎に異なるため、TSA事業者は同時に複数の秘密鍵を使用

✓ なお、鍵更新のタイミングは、機器毎やサービス提供開始時期によって様々

認定の有効期間（2年間）内に、複数回の鍵更新が行われる場合があり、更新審査の際に審査員立ち会いのもと、鍵更新を行うような運用は困難

- EU
  - 鍵更新（鍵の廃棄）は、TSAが二重管理のもと行い、鍵の適切な廃棄に関するエビデンスを残すことを規定（当該エビデンスをサーベイランス監査の際に確認）

✓TSA公開鍵証明書の有効期間は通常3年であり、鍵更新は1～3年で実施

✓サービス毎に鍵は異なり、鍵更新の時期も様々

✓新たなTSA公開鍵証明書をトラストリストに掲載する場合（鍵更新の際）には、事業者が自己申告
  - なお、認定の有効期間と鍵更新のタイミングの関連性はない

2. 認定の有効期間

論点について

- 認定の有効期間は、監査を含めた現行の制度を踏まえ、2年で十分か。
- 現行の制度及びEUの実態を鑑みて、認定の有効期間とTSA公開鍵証明書の鍵更新は切り離して考えることが適当か。

方向性に関する見解

- 以下を鑑みて、認定の**有効期間は2年**とすることが適切ではないか。
  - 既存のTSA事業者への影響（現行の制度も2年）
  - EU（2年）等の諸外国の制度との整合性
  - 認定の有効期間と鍵更新のサイクルの関連性
    - 現行の制度及びEUにおいても関連性はない

3. 監査の在り方

現状（タイムビジネス信頼・安心認定制度）

- 定期的に部署外からの適切な業務監査を受け、その結果を認定機関へ開示することを規定
  - 監査内容：本審査基準に沿って適切に実施されていることを確認する業務監査
  - 監査の頻度：最低年1回実施すること
- 監査を行う主体の要件として、**部署外からの業務監査等のチェックが働く組織（内部監査でも可）**であることを規定

EU

- ETSIの適合性評価機関に対する要件において、24か月毎のフル監査の間に、**年に1回のサーベイランス監査実施を推奨**すると規定※1
  （実際は、フル監査の内容はサーベイランス監査の内容を包含するため、24か月毎のフル監査の間には1回のサーベイランス監査が行われている）

中国

- 参考）中国国家（推奨）規準に**監査に関する基準はない**が、NTSCが唯一正式に業務提携するUTSAは、毎年第三四半期に中国科学院の年度監査を受ける必要がある

※1 **ETSI EN 319 403 Requirements for conformity assessment bodies assessing Trust Service Providers**
7.9 Surveillance
The requirements from ISO/IEC 17065 [1], clause 7.9 shall apply. In addition, the following TSP-specific requirements and guidance apply.
The Conformity Assessment Body shall define a programme of periodic surveillance and re-assessment that includes on-site audits to verify that TSPs and trust services they provide continue to comply with the requirements. It is recommended that at least one surveillance audit per year is performed in between full (re-)assessment audits.

3. 監査の在り方

論点について

- 当該監査について、「現行の制度からのシームレスな移行」や「制度の普及・利用促進」の観点から現行の制度同様に内部監査も可能とすることが適切か、あるいは、EU等の「国際的な制度との整合性」の観点から、調査機関による監査を求めることが適切か。
  - 内部監査も可能とする場合：
    - 現行の制度と同様、年に1回規定することが適当か。
  - 調査機関による監査を求める場合：
    - 調査機関による監査を求める場合、調査機関に求める要件は何か。
    - 認定の有効期間内に少なくとも１回の監査を求めることで十分か。

方向性に関する見解

- 現行制度で問題点もなく、「現行の制度からのシームレスな移行」の観点も踏まえ、**内部監査も認める**ことが適切ではないか
- また、**監査の頻度**についても、適切な認定の状態を維持するために、現行の制度と同様に**年に1回と規定**することが適切ではないか
  - 参考）仮に、EUと同様に調査機関による監査を求める場合は、事業者の対応工数及び費用の負担が生じ、ひいては、利用者のコストにはねることが懸念点としてあげられる

4. 廃止の場合の取扱い

現状（タイムビジネス信頼・安心認定制度）

- 業務の廃止に関する規定等
  - TSAに対する規定
    - TSAの業務廃止に関連する規定
      - 時刻認証業務の廃止に関し、運用規約※1に、事後的な届出を規定
      - 審査基準※2に、利用者への事前通知を規定
    - 認証局の業務廃止に関連する規定
      - 認証業務廃止に関し、審査基準※3に、TSAが認証局との間で合意しておくべき事項を規定
- 課題
  - 現時点では業務廃止時及び廃止後に問題は発生していない

※1 **タイムビジネス信頼・安心認定制度　運用規約　第22条（業務廃止の届出）**
認定事業者は、その認定に係る業務を廃止したときは、遅滞なく協会に届け出なければならない。
2 前項の規定による届出は、協会が定める様式による届出書に、認定証及び業務廃止の経過措置に関する説明書類を添えて行わなければならない。

※2 **時刻認証業務審査基準　（2）運用基準　5. 業務の一時停止・終了／5. 1 事前通知**
サービスの一時停止・終了時は、事前にそのスケジュールと手続きを決め、その内容を事前に公知、もしくは利用者へ通知すること

※3 **時刻認証業務審査基準（1）技術基準 14. TSA公開鍵証明書を発行する認証事業者／14. 2 TSA公開鍵証明書を発行する認証局との合意事項等**
時刻認証事業者は、TSA公開鍵証明書を発行する認証局と、その発行に先立ち、認証局の認証業務廃止に係る以下の事項について合意しておくこと。
① 認証局は、時刻認証事業者が発行済みTSA公開鍵証明書に対応した秘密鍵を用いたタイムスタンプ発行を継続している間、認証業務を終了せず、当該公開鍵証明書に係る失効リストを最新の状態に保ち、またそれを公の状態に保つこと
② 認証局は、認証業務の終了後、秘密鍵を安全に廃棄し、その旨を書面にて時刻認証事業者に通知すること
③ 認証局が認証業務を他の認証局に引き継ぐ場合は、認証局の認証業務廃止には当たらないものとし、引継ぎに先立ち、引継ぎ先の認証局と①、②と同様の合意を得ること

4. 廃止の場合の取扱い

電子署名法

- 認定認証事業者は、その認定に係る業務を廃止しようとするときは、あらかじめ、その旨を主務大臣に届け出なければならないことを規定※1
  - 認定に係る業務が行われていないにもかかわらず、認定を受けている状態が生じないようにする主旨

※1 **電子署名及び認証業務に関する法律　第3章（特定認証業務の認定等）**
第1節（特定認証業務の認定）
第10条（廃止の届出） 認定認証事業者は、その認定に係る業務を廃止しようとするときは、主務省令で定めるところにより、あらかじめ、その旨を主務大臣に届け出なければならない。
2 主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

4. 廃止の場合の取扱い

電気通信事業法

- 電気通信業務の全部または一部を廃止しようとするときは、あらかじめ利用者の利益を保護するために必要な事項を周知させなければならないことを規定※1
  - サービス提供が何の前触れもなく、突然打ち切られた場合には、利用者が不測の不利益を被ることとなるおそれがあるため、事前周知を求めているもの。
  - 参考）利用者への利益に及ぼす影響が大きいものは、あらかじめ総務大臣への届出を規定

放送法

- 業務を廃止するときは、その旨を総務大臣に届け出なければならないことを規定※2
  - 電波の効率的利用の観点から、無線局と同様に廃止の届出をなすことを義務付けているもの

※1 **電気通信事業法　第26条の4（電気通信業務の休止及び廃止の周知）**
電気通信事業者は、電気通信業務の全部又は一部を休止し、又は廃止しようとするときは、総務省令で定めるところにより、あらかじめ、当該休止し、又は廃止しようとする電気通信業務に係る利用者に対し、**利用者の利益を保護するために必要な事項**として総務省令で定める事項を周知させなければならない。ただし、利用者の利益に及ぼす影響が比較的少ないものとして総務省令で定める電気通信役務に係る電気通信業務の休止又は廃止については、この限りでない。

2　前項本文の場合において、電気通信事業者は、利用者の利益に及ぼす影響が大きいものとして総務省令で定める電気通信役務に係る電気通信業務の休止又は廃止については、総務省令で定めるところにより、あらかじめ、同項の総務省令で定める事項を総務大臣に届け出なければならない。

※2 **放送法　第100条（業務の廃止）**
認定基幹放送事業者は、その業務を廃止するときは、その旨を総務大臣に届け出なければならない。

4. 廃止の場合の取扱い

EU

- eIDAS規則に、監督機関によって検証された終了計画を持つことを規定※1
  - ETSIが、トラストサービスプロバイダの終了および終了計画について要件を規定※2
    - 実際には、サービス廃止の3か月前までに監督機関に報告
    - 利用者に対して、サービス廃止の旨を通知
    - 参考）サービス運用中の保管義務のあるアーカイブのログ等を保管
  - ENISA※3が、認定トラストサービスの終了に関するガイドラインを公開している

※1 **eIDAS規則 第24条 トラストサービスプロバイダに対する要求事項**
2.適格トラストサービスを提供する適格トラストサービスプロバイダは以下を実施すること
(a)～(h)：略
(i) 第17条(4)の(i)のもと、監督機関によって検証された規定に従ったサービスの継続を保証するための最新の終了計画を持つ
(j), (k)：略

※2 **ETSI EN 319 401 トラストサービスプロバイダーの一般的なポリシー要件**
TSPのサービスの停止の結果として、加入者と依拠当事者に対する潜在的な混乱が最小限に抑えられ、特に、トラストサービスの正当性を検証するために必要な情報の継続的なメンテナンスが提供されるものとします。

※3 ENISA（European UNION Agency for Cybersecurity）：欧州ネットワーク・情報セキュリティ機関
「Guidelines on Termination of Qualified Trust Services」
WP2017 O-2-2-3 Guidelines on Termination of Trust Services Provision.pdf

4. 廃止の場合の取扱い

論点について

- TSAの業務廃止の際の届出については、事前とすることが適切か、廃止後に遅滞なく届出を求めることで十分か。
- TSA業務廃止による利用者への影響を考慮し、利用者へあらかじめ廃止の旨を周知することが必要か。
- その他の手続として、例えば総務省HPで公表といった国民への周知等、規定すべきことはあるか。

方向性に関する見解

- 以下を鑑みて、**廃止後に遅滞なく届出を求める**ことで十分ではないか。
  - 現行の制度においても、「廃止後に遅滞なく届出」としており、廃止時及び廃止後に特段の問題が発生していない
  - 廃止後の秘密鍵の廃棄等が重要
- 現行の制度及びEUの規定を踏まえ、利用者への影響を考慮して、**利用者へあらかじめ廃止の旨を周知**することを規定することが適切ではないか。
- 廃止があった際は、総務省HP等に公開予定のトラストリスト（仮）を速やかに更新することが適切ではないか。

END

各論点について

タイムビジネス認定センター