資料９－１

タイムスタンプ認定制度に関する検討会
取りまとめ（案）

令 和 ２ 年 １ ２ 月 １ ６ 日

サイバーセキュリティ統括官室

はじめに

- Society5.0においては、実空間とサイバー空間が高度に融合し、**実空間での紙や対面に基づく様々なやりとりを、サイバー空間においても電子的に円滑に実現**することが求められる。

- その実現のためには、データを安全・安心に流通できる基盤が不可欠であり、**データの改ざんや送信元のなりすまし等を防止**する仕組みである**トラストサービスの重要性が高まっている**。

- 我が国におけるトラストサービスの在り方については、**2019年１月に**「プラットフォームサービスに関する研究会※1」の下に**「トラストサービス検討WG※2」を立ち上げ、**約１年間検討を進め、**2020年２月に最終取りまとめ**を実施した。

- トラストサービスの１つであるタイムスタンプについては、総務省が平成16年に策定した「タイムビジネスに係る指針」をもとに日本データ通信協会によって民間の認定制度「タイムビジネス信頼・安心認定制度」が運用されてきたが、**国による信頼性の裏付けがない**ことや**国際的な通用性への懸念**等の声が強く、**国としての認定制度の創設**がトラストWGの最終取りまとめで提言された。

- 当該提言を受け、**2020年３月に「タイムスタンプ認定制度に関する検討会」を設置**し、**タイムスタンプの国による認定制度について、検討**を進めてきた。

- 本取りまとめは、**タイムスタンプに係る国の認定制度の創設に当たり、検討が必要な各論点について、**現行の「タイムビジネス信頼・安心認定制度」における課題等を踏まえながら**方向性等を取りまとめたもの**。

※1　総合通信基盤局長及びサイバーセキュリティ統括官共同開催。プラットフォーム事業者による利用者情報の適切な取扱いの確保の在り方等を検討
※2　サイバーセキュリティ統括官主催の研究会。

タイムスタンプ認定制度に関する検討会

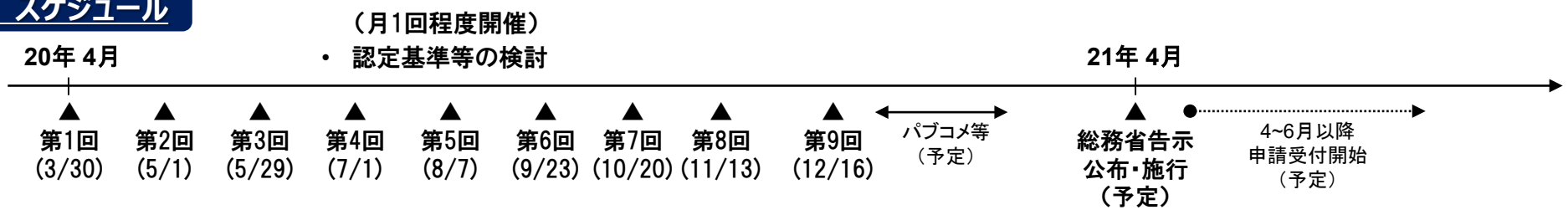
- タイムスタンプについて、国としての認定制度の基準を検討するため、有識者検討会を開催。
- 学識関係者、トラストサービス提供事業者、評価機関、経済団体（利用企業）等で構成。

１．構成員

	伊地知　理	一般財団法人日本データ通信協会 情報通信セキュリティ本部 タイムビジネス認定センター長
	岩間　司	国立研究開発法人情報通信研究機構 電磁波研究所 時空標準研究室 研究マネージャー
	上原　小百合	公益社団法人日本文書情報マネジメント協会 R&Dデータ保存委員会 委員長
	梅本　大祐	ブレークモア法律事務所 弁護士
	小木曽　稔	一般社団法人新経済連盟 政策部 部長
	小田嶋　昭浩	電子認証局会議 事務局
（座長代理）	柿崎　淑郎	東京電機大学 研究推進社会連携センター 准教授
	小松　博明	有限責任あずさ監査法人 東京IT監査部 パートナー
（座長）	東條　吉純	立教大学法学部 教授
	西山　晃	セコムトラストシステムズ株式会社 プロフェッショナルサポート１部 担当部長
	宮崎　一哉	トラストサービス推進フォーラム 副会長
	吉田　理重	富士通株式会社 政策渉外室 シニアマネージャー
	山内　徹	一般財団法人日本情報経済社会推進協会 常務理事
	若目田　光生	一般社団法人日本経済団体連合会 デジタルエコノミー推進委員会 主査 株式会社日本総合研究所 リサーチ・コンサルティング部門 上席主任研究員

（オブザーバー）　内閣府、内閣官房、法務省、財務省、経済産業省

２．スケジュール



タイムスタンプ制度に関する経緯

○ タイムスタンプについては、2002年に総務省「標準時配信・時刻認証サービスの研究開発に関する研究会」にてタイムビジネスの将来像に関する検討を開始。その後、2004年の**総務省の「タイムビジネスに係る指針」**を基に、2005年に**日本データ通信協会が「タイムビジネス信頼・安心認定制度」を開始**し、以降15年間にわたり、当該制度を運営。

○ 2019年1月から開催された**トラストサービス検討WG**※にて、タイムスタンプ等の制度化に関する検討が行われ、**国による認定制度**の創設が2020年２月に提言されたことを受け、今般具体的な審査基準等を検討する検討会を開始。

※プラットフォームサービスに関する研究会の下に設置

総務省タイムビジネスに係る指針（2004年11月5日）

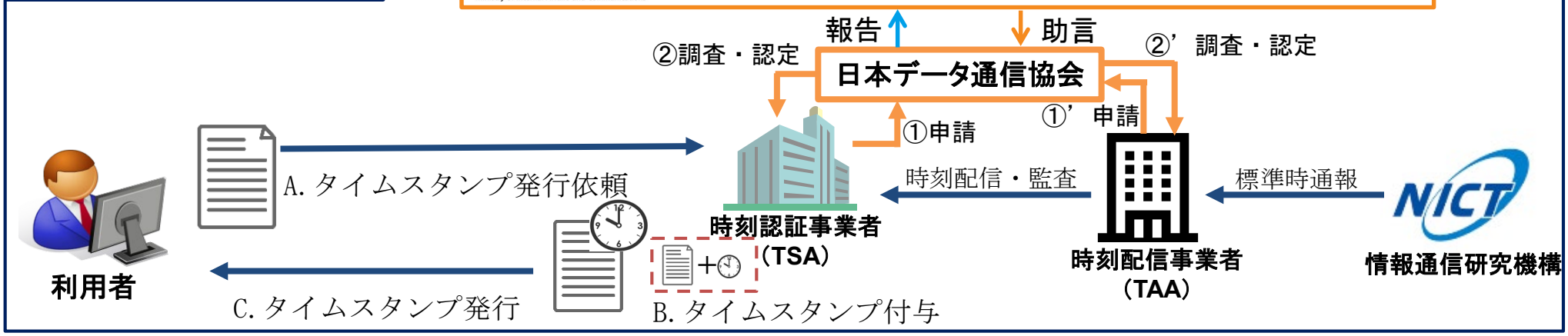
- **タイムビジネス**
  - 「時刻配信業務」及び「時刻認証業務」の総称
- **時刻配信業務**
  - 情報通信ネットワークを利用する上で必要となるサーバ等の電気通信設備に用いられる時刻に高い信頼性を与えるため情報通信ネットワークを通じて時刻情報を配信する業務、更に配信先の時刻精度を計測して報告を行う時刻監査業務。
- **時刻認証業務**
  - 電磁的記録に記録された情報（「電子データ」）について行われる措置であるタイムスタンプの付与及び当該タイムスタンプの有効性を証明する業務。
- **タイムスタンプ**
  - 電子データがある時刻に存在していたこと及びその時刻以降に当該電子データが改ざんされていないことを証明できる機能を有する時刻証明情報。
- 標準時
  - 独立行政法人情報通信研究機構法に基づき、独立行政法人情報通信研究機構が通報する標準時。

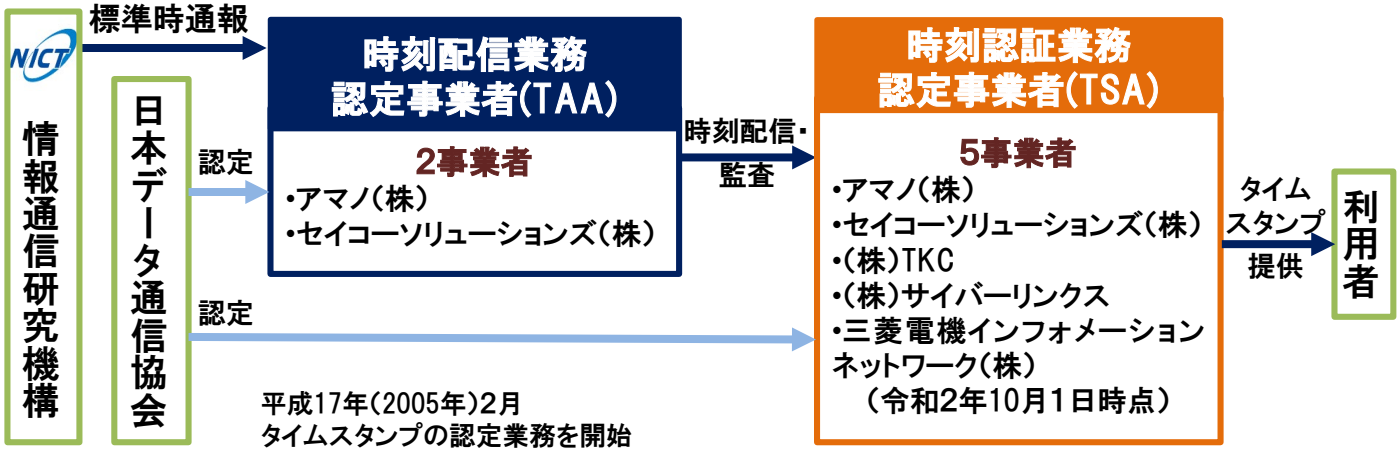
日本データ通信協会の認定制度の仕組みと認定事業者

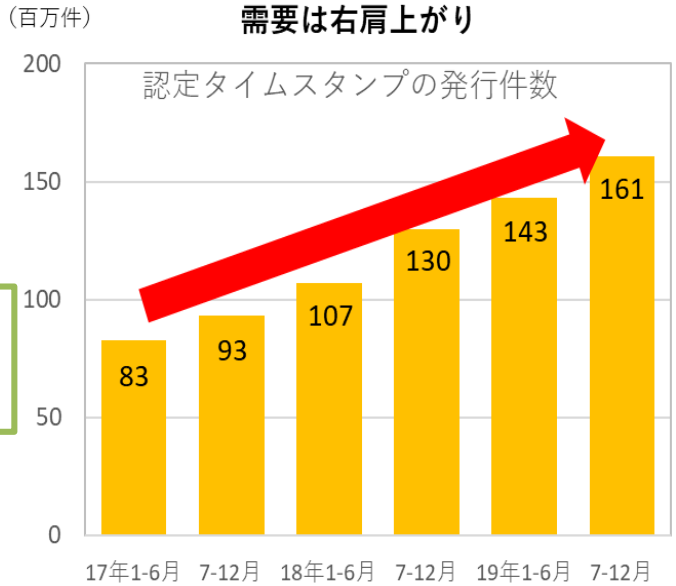
○　一般財団法人日本データ通信協会による民間の認定スキーム（タイムビジネス信頼・安心認定制度）により、タイムスタンプ事業者がサービスを提供

タイムスタンプの仕組み

総務省 Ministry of Internal Affairs and Communications　「タイムビジネスに係る指針」 平成16年11月５日







（注）日本データ通信協会まとめ

本検討会における検討事項

本検討会における主な検討事項

- 時刻認証業務の認定の仕組み
- 時刻認証業務の認定の基準
- その他（他の制度（法令、ガイドライン）への位置づけの整理　等）

現行制度における課題

- トラストサービス検討WGで寄せられた意見
  - ✓ 制度の永続性
  - ✓ 国際的な通用性
  - ✓ 法令等の要件を満たすか不明確等
- 事業者からのヒアリングで寄せられた意見

EU等の国際的な制度との整合性

- eIDAS規則をはじめとする諸外国の制度
- ISO等の国際基準　等

検討に当たっての主な観点

１．既存の制度からのシームレスな移行

- 既存の日本データ通信協会の認定制度における認定事業者への影響
- 現在の日本データ通信協会のタイムスタンプ認定制度を引用している関係省庁の法令等や業界ガイドラインへの影響　等

２．国際的な制度との整合性

- EU等の諸外国の制度との整合性
- ISO等国際標準との整合性　等

３．制度の普及・利用促進

- 調査、監査やサービス提供のコスト面への影響
- サービス利用者の立場から見ても、その信頼性担保の仕組みがわかりやすい制度設計（例：トラストリスト）が必要　等

諸外国におけるタイムスタンプの動向

総論

- EUでは、デジタルシングルマーケットを目的として、その基盤を支えるトラストサービスについて包括的に法制度化されており、トラストサービスの1つであるタイムスタンプについても規定されている。タイムスタンプの適格トラストサービスプロバイダーの数は111（2020年12月時点）。
- 中国には、タイムスタンプの認定制度は存在しないが、中国科学院直下で、国家時刻標準機構である国家授時センターが、唯一正式に業務提携を行っているTSA（北京聯合信任技術サービス有限公司）が存在。中国国内では広くタイムスタンプが使用されており、裁判でも証拠としてタイムスタンプが利用されることが多い。
- 米国には、認定制度が存在せず、民間（AdobeやMicrosoft、Oracle(Java)等のITベンダー）がビジネスの世界をリードする形でタイムスタンプサービスが運用されている。

諸外国における制度及び参照している技術基準

	EU	中国	米国
国のタイムスタンプ認定制度	あり	なし	なし
タイムスタンプ局(TSA)に参照されている主な基準	● RFC3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol) ● ETSI EN 319 401 (General Policy Requirements for Trust Service Providers) ● ETSI EN 319 411-1 (Policy and Security Requirements for Trust Service Providers issuing certificates ; Part 1: General Requirements) ● ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Time-Stamps)	● 国際規準：RFC3161 ● 中国国家(推奨)規準： ・「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 GBT36631-2018※1」 ・「情報安全技術 公開鍵基礎設備 タイムスタンプ規範 GBT20520-2006※2」 ● （北京聯合信任技術サービス有限公司(UTSA)内部規準）	特定の基準について参照することを規定する法律や基準は存在しない。（但し、RFC3161は、業界のデファクトスタンダードとしての位置付け）

※1　GBT36631-2018：タイムスタンプポリシー、タイムスタンプサービス運用規程及び責任・義務などを規定
※2　GBT20520-2006：タイムスタンプシステムユニットの構成、タイムスタンプの管理、タイムスタンプの形式およびタイムスタンプシステムのセキュリティ管理などの要件を規定

「タイムスタンプ認定制度に関する検討会」論点全体像

タイムスタンプについて、国としての認定制度を創設するにあたって、主に検討・議論した論点は以下のとおり。

①認定の対象

- **認定の単位**
  認定は、業務（サービス）単位とする
- **時刻配信・監査業務事業者（TAA）の扱い**
  TSAが自らタイムスタンプの信頼性を確保する方式も認める
- **時刻認証業務の技術方式**
  まずは、デジタル署名方式で制度を開始する
- **申請できる者の条件**
  海外拠点で業務を行おうとする申請者も認める

②認定の基準

- **設備面の基準**
  審査基準として、他の認証制度（コモンクライテリア等）も活用する
- **審査プロセス効率化**
  他の認証制度を活用する

③認定の期間

- **認定の有効期間**
  認定の有効期間は、2年とする

④認定に当たっての調査機関の要件、調査・監査の在り方

- **認定に当たっての調査を実施する機関**
  民間の第三者機関に行わせることができるように規定し、当該機関の基準は、すでに法制度化されている電子署名法を参考にする
- **認定に当たっての監査の在り方**
  現行の制度と同様に内部監査も認め、年に1回実施することを求める
- **認定に当たっての調査・監査の内容**
  調査は、現行の制度の審査観点に「事業体として求められる要件」を追加する
  監査は、調査と同じ審査項目で実施することを規定する

⑤認定業務の公表内容及び公表方法

- **トラストリストへの記載事項等**
  認定された業務及び当該業務を実施する事業者が特定可能な情報を公表する

⑥その他

- **事業体として求められる要件**
  認定・更新時の審査項目として、財務状況等を求める
- **廃止の場合の取扱い**
  事前の届出を終了計画と併せて主務省に提出すること、事前に利用者へ廃止の旨を通知することを求める
- **TSA公開鍵証明書を発行する認証事業者の基準**
  電子署名法における認証事業者、Web Trust認証を受けた認証事業者とする
- **利用の拡大に向けた取組**
- **経過措置**

①認定の対象

○認定の単位

現状・課題

- 現行の制度における認定の単位は事業者。
- 認定業務以外を含む複数のサービスを提供している認定事業者も存在するため、認定タイムスタンプの利用者が具体的な認定業務（サービス）を判別できないことが課題。

論点

- 認定の単位は現行の制度と同様に**事業者単位とすることが適切**か、それとも電子署名法やEUの制度を踏まえて**業務単位とすることが適切**か。

方向性

- 認定の単位は**業務（サービス）単位**とする。

現行の制度において、認定の単位は事業者だが、認定対象となっていないタイムスタンプサービスも並行して提供している事業者もおり、認定されたタイムスタンプサービスであるかを利用者が特定・判断することが困難であるとの課題があった。

他方、電子署名法やEUにおいては、業務（サービス）単位で認定を行っており、電子署名法の主務省のHPやEUのトラストリストを確認することで、認定業務を特定することが可能となっている。

したがって、認定タイムスタンプサービスの利用者及び検証者が具体的な認定業務（サービス）を特定・判断することができるように、認定の単位は業務（サービス）単位とすることが適切だと考えられる。

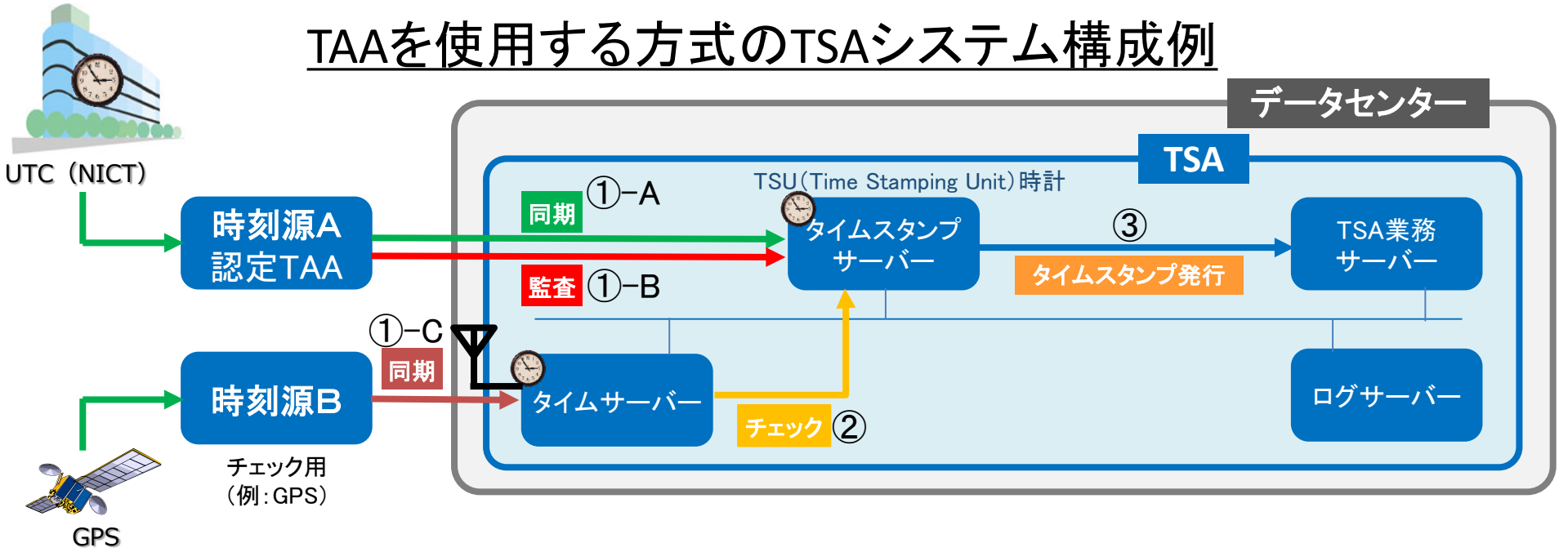
なお、現行の制度からの変更に伴う既存の認定事業者への負担は運用規定類等の整理に留まり、影響は軽微と考えられる。

①認定の対象

○時刻配信・監査業務事業者（TAA）の扱い

- TSA（Time Stamping Authority）とは、ユーザーのリクエストに応じてタイムスタンプを発行する事業者。
- TAA（Time Assessment Authority）とは、TSAに対して時刻の配信・監査を実施する事業者。
- TAAがTSAに配信する時刻は、UTC(NICT)に同期した時刻であり、TSAの時計が当該時刻と規定の精度以内で同期しているかを監査する。

TAAを使用する方式のTSAシステム構成例



①-A：TAAは定期的にTSU時計の時刻を時刻源Aに同期。

①-B：定期的に認定TAAがTSU時計を監査。
（誤差が閾値を越えている場合、TSAに通知。タイムスタンプ発行機能を停止することも可能。）

①-C：タイムサーバーは規定の頻度で時刻源Bに同期。

②：タイムスタンプサーバーは、適宜、タイムサーバーを参照し、TSU時計と比較。

③：②で正常の場合、リクエストを受けてタイムスタンプを発行。なお、比較結果に異常があればタイムスタンプ発行を停止。

①認定の対象

○時刻配信・監査業務事業者（TAA）の扱い

現状・課題

- 現行の制度では、時刻の信頼性を確保するための方式について、TAA方式に限定。
- 例えば、TAAが停止した場合、当該TAAから時刻の配信を受けているTSAのタイムスタンプサービスがすべて停止してしまうことや、TSAがTAAを利用するコストが利用者のタイムスタンプ利用料に影響していること等が課題。

論点①

- 時刻の信頼性を確保するための方式について、現行の制度と同様に**TAA方式に限定することが適切か**、もしくは、TAA方式に依らず**TSAが自ら時刻の信頼性を確保する方式も認めることが適当か**。

方向性①

- 時刻の信頼性確保に関して、TAA方式に限定せず、**TSAが自ら時刻の信頼性を確保する方式も認める**。

現行の制度ではTAA方式に限定しているが、時刻の配信がTAA依存になってしまう、また、TSAのTAA利用コストが利用者のタイムスタンプ利用料に影響する等の課題があった。

他方、EU（や中国※）ではTSAが自ら時刻の信頼性を確保する方式が主流となっており、その方式についても特定の方法に限定していない。

現行の制度の課題やEU（や中国）の実態も鑑みて、時刻の信頼性確保の方式はTAA方式に限定することなく、TSAの自らの責任で、時刻の信頼性を確保する方式も認めることが適当だと考えられる。

なお、TSAが自ら時刻の信頼性を確保する方式を認めることになっても、TAA方式に加えて、新たな方式を追加するだけであることから、既存の認定事業者への影響は特段ないものと考えられる。

※ 中国に認定制度は存在しないが、裁判等でタイムスタンプが証拠として取り扱われる事例が散見される。

①認定の対象

○時刻配信・監査業務事業者（TAA）の扱い～TSAが自ら時刻の信頼性を確保する方式～

論点②

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、日本標準時通報機関である「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。
- 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。

方向性②

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、日本標準時通報機関である「NICT」のUTC（NICT）とする。
- 時刻精度の確認を行うこととし、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の差（時刻精度）の基準は、当該時刻源±１秒以内とする。

② 時刻のトレーサビリティの担保
- 適切な機器における適切なログの保管を行う。

トレーサビリティの起点となる時刻源は、タイムスタンプにおいて最も重要な要素である。その重要性に鑑みて、我が国の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（NICT）が提供する時刻（UTC(NICT)）を用いることを求めることが適切だと考えられる（現行の制度もUTC(NICT)）。

また、タイムスタンプの時刻について、当該時刻源と大幅な誤差が生じてしまえば、時刻の信頼性が損なわれてしまうため、その差は一定の範囲内に収まっている必要がある。この点については、現行の制度及び諸外国でも±１秒以内という基準が規定されていることを踏まえ、現行の制度からのシームレスな移行及び国際的な整合性の観点から、同様に±１秒以内とすることが適当だと考えられる。なお、時刻精度の確認方法は、EU等諸外国の事例も踏まえ、特定の方法に限定せず、幅広い方法を認めることが適当だと考えられる。

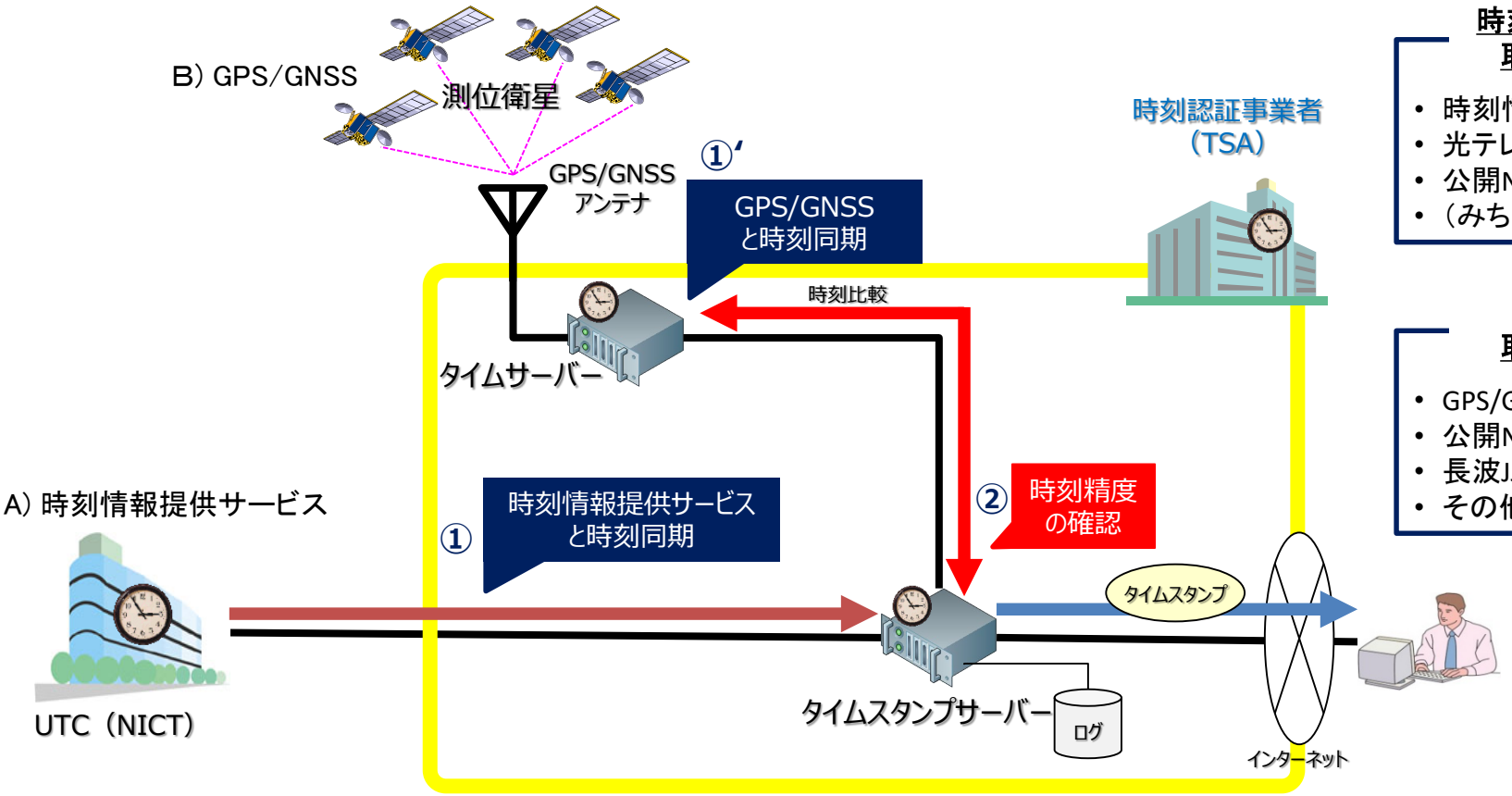
時刻のトレーサビリティについては、TAA方式を使用することによって担保していた現行の制度とは異なり、TSAが自らトレーサビリティを担保する必要がある。この点については、時刻の配信を受ける各タイムサーバー等の適切な機器において、時刻のトレーサビリティを証明するために必要な情報等のログを保管することが必要だと考えられる。

①認定の対象

○時刻配信・監査業務事業者（TAA）の扱い～TSAが自ら時刻の信頼性を確保する方式～

- トレーサビリティの起点となる時刻源は、日本標準時通報機関である「NICT」の**UTC（NICT）**とする。
- **時刻精度の確認（トレーサビリティの起点となる時刻源±1秒以内）**は必須とするが、その確認方法については特定の方法に限定しない。
- TSAは時刻のトレーサビリティを担保するために、タイムスタンプサーバー等の**適切な機器における適切なログの保管**を行う。

TSAが自ら時刻の信頼性を確保する方式の構成例



時刻源A（UTC（NICT））の取り得る選択肢の例

- 時刻情報提供サービス
- 光テレホンJJY
- 公開NTPサーバー（UTC（NICT））
- （みちびき）

時刻源Bの取り得る選択肢の例

- GPS/GNSS
- 公開NTPサーバー
- 長波JJY
- その他（時刻源Aの選択肢を含む）

①認定の対象

○時刻認証業務の技術方式

現状・課題

- 現行の制度においては、時刻認証業務の技術方式について、デジタル署名方式・リンキング方式・アーカイビング方式の3方式を規定。
- 現行の制度において、現在、認定を受けている事業者は全てデジタル署名方式を採用。

論点

- タイムスタンプの技術方式について、以下の**どの方式を認定の対象とすることが適切か**。
  - **デジタル署名方式**
  - **アーカイビング方式**
  - **リンキング方式**

方向性

- 当面は**デジタル署名方式**とする。

現行の制度においては、デジタル署名方式、リンキング方式、アーカイビング方式の3つの方式が規定されているが、現在認定を受けている事業者はすべてデジタル署名方式を採用している。また、EUにおいては、デジタル署名方式のみ規格が定められており、米国や中国においてもデジタル署名方式が主流となっている。

このような実態や今後の国による認定制度の技術方式の基準のメンテナンスに係るコスト、調査の効率性等も鑑みて、まずは幅広く使われているデジタル署名方式で国による認定制度を開始することが適当だと考えられる。

なお、今後の技術動向等を踏まえ、必要に応じて他の方式についても検討を行い、適宜基準に新たな技術方式を追加していくことが必要。

①認定の対象

○申請できる者の条件

現状・課題

- 現行の制度においては、認定の申請ができる者を日本国内に拠点を有する者に限定。
- 現状、海外の事業者による申請の実績はない。

論点

- 申請できる者については、現行の制度と同様に日本国内に拠点を有する者に限定することが適切か、それとも海外に拠点を有する者についても含めることが適切か。
- 海外に拠点を有する者を申請者に含めるにあたり、考慮すべき事項はあるか。

方向性

- 国内に限定せず、**外国の事業者も申請可能とする**。

現行の制度では、認定の申請を行うことができる者を国内に限定している。他方、電子署名法の認定においては、海外の事業者が日本市場へ参入する際の障壁とならないよう、海外の事業者であっても認定を受けることができるように規定（認定基準や義務は国内の事業者と同一のものを課す）されている。

これを踏まえ、タイムスタンプの国による認定制度についても、国内の事業者のみに限定することなく、海外の事業者であっても申請可能とし、基準を満たしていれば当該事業者の業務を認定することが適当だと考えられる。

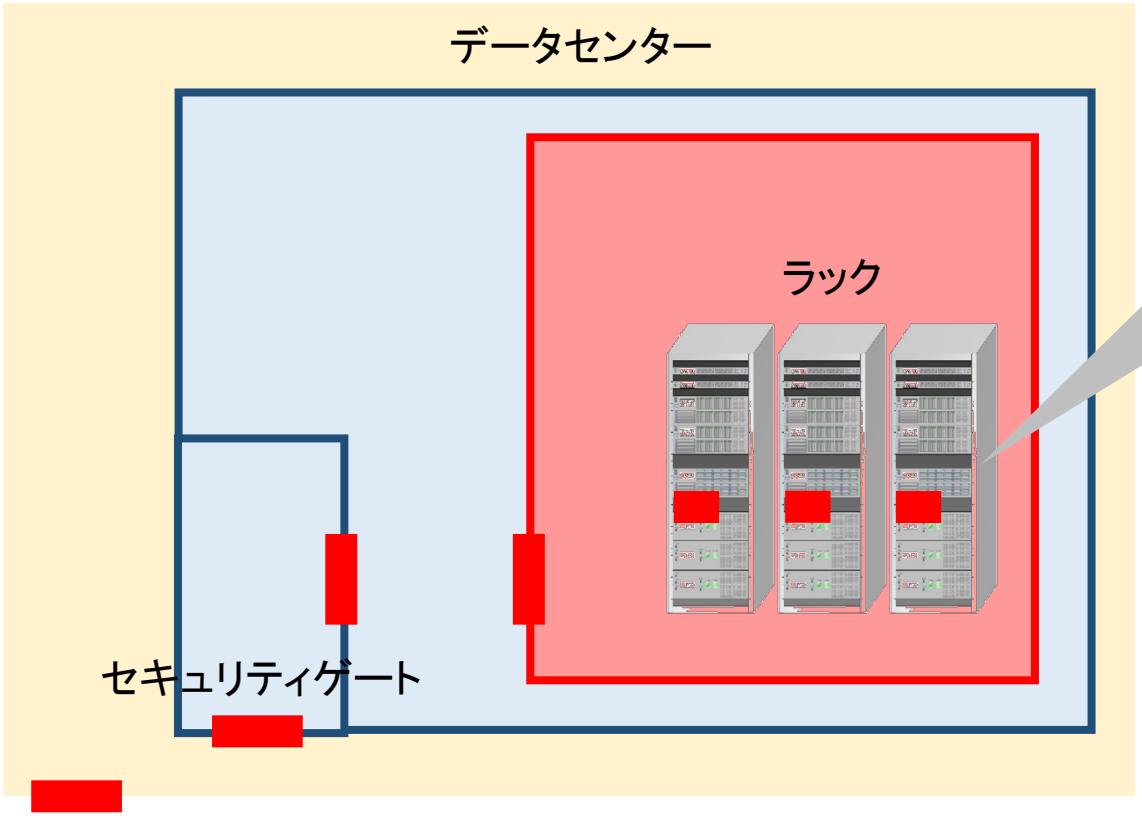
なお、海外の事業者であっても、時刻源はUTC(NICT)とすることをはじめ、国内の事業者と同様の審査基準、義務を課すことを前提とする。

（参考）EUにおいては、申請できる者の条件をEU域内に限定する規定は存在しないが、監督機関の役割として、指定加盟国の領域に設立された適格トラストサービスプロバイダーを監督することが求められていることから、実質的にはEU域内に限定されているのが実態となっている。

②認定の基準

○設備面の基準

- HSM（Hardware Security Module）とは、耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。
- 一般に、鍵の生成やデジタル署名の生成等の機能も備えている。



秘密鍵が漏えいすると

- 秘密鍵を取得した者が、不正なタイムスタンプを発行できる
- 失効処理が行われ発行済みタイムスタンプの正しい検証ができなくなる

②認定の基準

○設備面の基準

現状・課題

- タイムスタンプの生成に用いる秘密鍵を格納するHSMについて、FIPS140-2のレベル3認証相当以上の製品に限定。
- 当該基準を満たしたHSMは世界的にも限定的であり、継続的な調達に対する不安や、当該HSMの障害発生時の予備機の確保など、TSAのコスト負担等が課題。

論点

- 現行の基準を満たすHSMは調達先が限定的であることを踏まえ、**HSMの基準として他の認証も活用し、調達先の裾野を広げることは適切か**。
- 他の認証の活用が適切である場合、**FIPS以外に活用しうる認証制度としてどのようなものが考えられるか**。

方向性

- HSMの基準として、現行のFIPSの基準に加え、時刻認証業務に求められるHSMの要件を満たした**他の認証制度（ISO/IEC 15408（コモンクライテリア）のEAL4以上 等）も活用する**。

秘密鍵を保護するHSMは、時刻認証業務において極めて重要な設備であり、現行の制度の「FIPS140-2のレベル3認証相当以上」という基準は、秘密鍵の漏えいを防ぐために必要最低限のレベルである。したがって、当該基準を満たしたHSMの調達に課題（高コスト、継続的な調達の不安等）があったとしても、当該基準を緩める余地はないと考えられる。

他方、EUにおいては、FIPS140-2のレベル3認証に加えて、ISO/ICE 15408（コモンクライテリア）のEAL4以上も活用しており、より調達の裾野が広くなっている。

このような実態に鑑みて、国による認定制度においても、他の認証制度（ISO/ICE 15408（コモンクライテリア）のEAL4以上 等）を活用可能とし、安全性を担保しつつ調達の裾野を広げることが適当だと考えられる。

②認定の基準

○審査プロセスの効率化

現状・課題

- 現行の制度では、他の仕組みや認証制度を審査に活用する仕組みは特段ない。

論点

- 同じトラストサービスの枠組みである**電子署名法の認定時の提出書類や調査結果、ISMS**（Information Security Management System）**等の他の認証を活用し、審査プロセスの効率化を図ることは適当か**。
- 電子署名法の認定時の提出資料や調査結果、ISMS等の他の認証を活用することが適切である場合、考慮すべき事項としてどのようなことがあげられるか。

方向性

- **既存の制度**（電子署名法等）や**他の認証**（ISMS等）**も活用可能な制度設計とする**。

EUでは、トラストサービスが包括的に法制度化されており、トラストサービスの横断的な調査内容は省略可能となっている。
我が国においても、同じトラストサービスの枠組みである電子署名（電子署名法）の認定認証業務の用に供する設備等（データセンター等）で、時刻認証業務と共通するものがある場合は、審査プロセスの効率化の観点から、調査省略の余地があると考えられる。また、ISMS等のその他の認証制度を活用することでも調査省略の余地があると考えられる。
したがって、タイムスタンプの国による制度の検討に当たっては、電子署名法や他の認証制度を活用可能なように制度設計を行っていくことが有用だと考えられる。
ただし、実際に他の制度の活用を検討する際には、認定時刻認証業務の適正な運用状態が損なわれることがないよう、活用する制度の有効期間等を十分考慮した制度設計が必要。

③認定の期間

○認定の有効期間

現状・課題

- 現行の制度の認定の有効期間は2年。
- 年に1回以上の自主監査（内部監査（部署外）又は外部の機関による監査）を義務付けているところ、有効期間が2年であっても、これまでタイムスタンプの信頼性に係る問題は発生していない。

論点

- **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**。

※ 毎年実施している鍵更新との関係については、配慮が必要

方向性

- **認定の有効期間は2年**とする。

現行の制度の認定の有効期間は2年であり、年に1回以上の部署外からの監査（認定及び更新時と同じ内容）を行うことで、運営状態を確認し、適正な運用状態を維持している。EUにおいても、認定の有効期間は2年であり、認定の有効期間中に適合性評価機関によるサーベイランス監査を1回と年に1回の内部監査によって適切な認定の状態を維持している。

したがって、認定の有効期間が複数年であったとしても、毎年の監査等で認定の適格性を確認することで、適切な認定の状態を維持することは可能であり、また、認定期間中に生じた軽微な変更にも対応することが可能だと考えられる。

なお、有効期間が2年よりも長いものとしてISMS認証（3年）が挙げられる。ISMS認証は、年に1回の維持審査（認定時の審査の3分の1程度の内容）を実施している。ISMS認証は企業における総合的な情報セキュリティの確保を目的とした制度であるが、今回検討している時刻認証業務は、他の事業者に提供する業務（サービス）に関する認定制度であることから、自社で完結するISMS認証の3年の有効期間よりも短くすることが適切だと考えられる。

これらの実態及び現行の制度からのシームレスな移行、国際的な制度との整合性の観点から、年に1回の監査等によって認定の適正な運用状態を確認することを前提として、認定の有効期間は2年とすることが適当だと考えられる。

（参考）
毎年実施している鍵更新（及び鍵廃棄）については、毎年の監査でそれらが適切に行われているかどうかを確認することとする。

④認定に当たっての調査機関の要件、調査・監査のあり方

○認定に当たっての調査を実施する機関

現状・課題

- 現行の制度においては、認定主体と調査主体がともに日本データ通信協会。
- 制度運用規定はあるが、調査機関に関する要件は定められていない。

論点

- 国の認定制度においては、行政事務の簡素化や民間能力の活用の観点から、**第三者機関に調査を行わせることができるようにすることが適当か**。
- **第三者機関の要件については、電子署名法の規定を踏まえて検討することが適当か**。

方向性

- **認定に係る調査は、民間の第三者機関に行わせることができるように規定**する。
- 調査を委託する機関の要件は、**電子署名法の指定調査機関の指定の基準をもとに規定**する。

国による認定制度において、認定主体及び調査主体は基本的には国（総務大臣）が実施することが想定される。他方、電子署名法は、認定主体と調査主体がともに主務大臣であるが、調査については行政事務の簡素化や民間能力の活用の観点から民間の第三者に行わせることができるように規定している。

タイムスタンプにおいても、認定の適格性を判断するための調査を実施するには専門的知識・経験が不可欠であり、また当該調査を行政機関が行うにはかなりの事務負担となることが想定される。

したがって、タイムスタンプも電子署名法と同様に、行政事務の簡素化や民間能力の活用の観点から、民間の第三者に調査を行わせることができるように規定することが適切だと考えられる。また、第三者機関の要件については、同じトラストサービスの枠組みとして既に法制度化されている電子署名法の規定を参考に検討することが適切だと考えられる。

なお、今後トラストサービスの包括的な制度検討を行う際には、調査主体の要件として、必要に応じて国際標準であるISO/IEC 17065やEUの標準であるEN 319 403等を参考にすることは有用である。

（参考）
EUにおいては、認定主体にあっては、各加盟国が指定する監督機関が行い、調査主体にあっては、各加盟国が指定する認定機関が認定している適合性評価機関が実施している。

④認定に当たっての調査機関の要件、調査・監査のあり方

○認定に当たっての監査のあり方

現状・課題

- 日本データ通信協会の認定制度では、TSAに対して、年に1回、新規及び更新認定と同じ調査内容の自主監査を実施することを規定。（内部監査（部署外）又は外部の機関による監査も可）
- 現行の制度においては、年に1回の自主監査の仕組みで、これまで認定の適否に係る問題やタイムスタンプの信頼性に係る問題は生じていない。

論点

- 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

- 現行の制度と同様、**内部監査も認める**が、必要に応じて外部監査も活用する。
- 監査は、**年に1回実施**することを規定する。

現行の制度において、TSAは毎年部署外による内部監査又は外部の機関による監査を受けることを規定しており、当該監査によって、2年の認定の有効期間中の認定業務の適正な運用状態を確認していることから、当該監査は必要不可欠である。

国による認定制度においても、認定の有効期間は2年（P19「③認定の期間」参照）であることから、当然毎年の監査は必須であると考えられる。他方、監査の客観性の観点から内部監査の可否が問われるところ、内部監査を実施する場合は認定業務とは無関係な部署による実施を求めることに加え、当該監査の結果の妥当性について、調査主体である主務大臣または指定調査機関が確認することで、客観性は担保可能であると考えられることから、現行の制度と同様に内部監査も認めることが適当だと考えられる。

④認定に当たっての調査機関の要件、調査・監査のあり方

○認定に当たっての調査・監査の内容

現状・課題

- 現行の制度では、「技術面」、「運用面」、「ファシリティ面」、「システムの安全性」、「情報開示にかかる事項」の5つの観点で調査を実施。
- 認定制度の運用が始まってからこれまで、必要に応じて審査基準（調査内容）の改訂を実施。
- 現行の制度では、監査にて審査基準の全項目を実施することを規定。（監査の頻度は年に1回以上、内部監査可）

論点

- これまで検討会で示された方向性や議論等を踏まえ、調査の観点については、現行の制度における5つの観点に加え、**「事業体の要件」を追加することで十分か**。
- **監査の内容について、**現行の制度では**全項目を確認しているが、**EUの実態も踏まえて内容を**省略する余地はあるか**。
- 監査の内容（新規・更新認定における全項目の確認）を**省略する余地がある場合、どのような観点で省略する項目を検討することが適切か**。

方向性

- 調査の観点については、現行の制度における5つの観点に加え、**「事業体の要件」を追加**する。
- 監査は、現行の制度と同様に新規・更新認定における**調査の項目をすべて実施**する。

調査については、利用者視点での信頼性向上の観点から、現行の制度で確認していた5つの観点に加えて、事業体として求められる要件（P25 ⑥その他 「事業体として求められる要件」参照）も確認することが適切だと考えられる。

また、監査は、2年間の認定の有効期間中の適正な運用状態を維持するために必須であり、内部監査も認めるとしていることも踏まえて、現行の制度と同様に調査で実施する全項目を対象とすることが適切だと考えられる。

他方、EUでは、新規及び更新認定時に調査（フル監査）を1回、認定期間中に適合性評価機関による監査（サーベイランス監査）を1回と内部監査を2回（年に1回）の計4回実施しており、今後国際相互運用を検討していく際には、我が国とEUとの差異を考慮して検討することが必要。

なお、調査及び監査に当たっては、前提としてその調査基準（項目）が適切であることが求められるため、調査基準（項目）を定期的にメンテナンスする仕組みも重要であるが、その仕組みについては別途検討が必要。

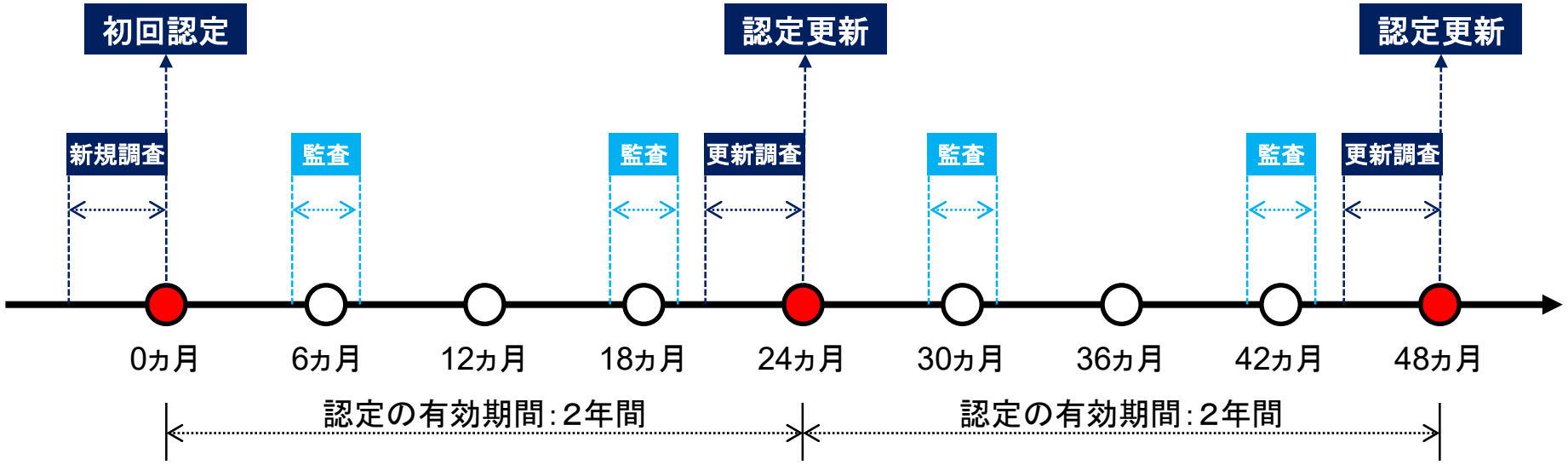
④認定に当たっての調査機関の要件、調査・監査のあり方

国による認定制度の調査及び監査の方向性

- 認定に係る**新規調査及び更新調査は、総務大臣（調査機関を指定する場合は、指定調査機関）が実施**する。
- 調査の内容は、**「事業体の要件」、「技術面」、「運用面」、「ファシリティ面」、「システムの安全性」、「情報開示に係る事項」**の観点から実施する。
- 認定事業者は、**当該認定業務について、年に1回監査**を受けることとする。
- **監査は、内部**（タイムスタンプの認定業務を行う者を除く）**、または第三者**によって実施されることとする。
- **監査の内容は、調査**で実施する内容**と同じ項目**とする。

調査・監査のサイクルイメージ

※ 監査のタイミングは、必ずしも認定を受けてから6ヵ月後、18か月後ではなく、１年に1回の任意のタイミング



⑤認定業務の公表内容及び公表方法

○トラストリストへの記載事項等

現状・課題

- 日本データ通信協会の認定制度では、①氏名又は名称及び法人にあっては、その代表者、②認定に係る業務の種類、③住所、④認定日及びその更新日並びにその有効期間を協会のウェブページに公開。
- 利用者が、認定を受けたタイムスタンプか否か識別することが困難であることが主な課題。

論点

- **認定を受けたタイムスタンプかどうかをユーザー側で識別することができるための情報として、どのようなものが考え得るか**。
- **それ以外に公開すべき情報として、どのようなものが考え得るか**。
- **以上の情報を**トラストリスト（仮）として、**総務省HPへ公開することで十分か**。

方向性

- **当該業務を特定可能な情報**（業務の名称、TSA公開鍵証明書及びその公開鍵のハッシュ値等）及び**当該業務を実施する者を特定可能な情報**（法人番号、業務を行う者の名称（英文併記）等を公開する。（履歴情報については、国により認定されたタイムスタンプに関する情報に限る）

現行の制度においては、認定に係る情報（サービス提供事業者等）を日本データ通信協会のHPに掲載していたが、利用者が当該情報を確認し、認定を受けたタイムスタンプかどうかを判別することが困難だったことに鑑みて、国による制度では、認定を受けた業務によって発行されたタイムスタンプかどうかを特定可能な情報も公開することが適切だと考えられる。

他方、EUにおいては、認定に係る情報をトラストリストとして、過去の履歴情報も含め、機械可読な形式で公開している。

過去の履歴情報については、タイムスタンプの長期的な検証の観点からも必要不可欠であるため、掲載することが適切だと考えられる。（ただし、国により認定されたタイムスタンプに関する情報に限る。）

機械可読な形式については、タイムスタンプの自動検証の観点から有用である一方、トラストサービス横断的な要素もあるため、具体的なデータ形式や構造等を含めた詳細な検討が別途必要である。

また、掲載場所は、認定主体が総務大臣であることや、信頼性向上の観点から総務省HPが適当だと考えられる。なお、今後トラストサービスの包括的な制度検討を行う際には、トラストリストの掲載の在り方についても検討が必要。

⑥その他

○事業体として求められる要件

現状・課題

- 日本データ通信協会の認定制度では、TSAに対しては欠格条項を規定し、TAAに対しては欠格条項に加えて経営情報開示の基準を規定。

論点

- 業務（サービス）を維持及び適格に遂行可能かどうかの基準として、**財務状況等の要件を求める必要があるか**。
- 財務状況等を要件として求める場合、**審査項目として規定することが適切か、欠格条項として規定することが適切か**。

方向性

- 事業体に求められる要件は、当該時刻認証業務を継続的に安定して遂行する能力として、現状規定している技術的能力に加えて、**財務状況等も審査項目に規定**するとともに、当該事業者は当該項目を含め、運用規定に定めて開示する。

現行の制度では、TSAの事業体の要件として欠格条項が定められており、認定の申請を実施する者の財務状況等は特段確認していない。

他方、タイムスタンプはその性質（有効期間が10年以上）上、長期的な検証が必要であることに加え、国による制度が創設されることによる一層の信頼性の向上が期待されることから、事業体の要件を欠格条項として規定するだけではなく、認定を受ける者が長期的に当該認定業務を継続可能かどうかの指標として、財務状況等も含め、「事業体として求められる要件」を審査項目として設けることが適切だと考えられる。

⑥その他

○廃止の場合の取扱い

現状・課題

- 現行の認定制度では、運用規定で、TSAが業務を廃止した際の事後的な届出の提出を規定。また、審査基準に利用者に対する事前通知を規定。
- 現行の制度において、TSA業務廃止の実績はあるが、実際の廃止時及び廃止後に特段の問題（特に発行済みのタイムスタンプの信頼性等）は生じていない。

論点

- 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

- TSAから主務省への**廃止の届出は終了計画と合わせて事前に提出することを規定する**。
- TSAの認定業務廃止に際し、**利用者に余裕をもって廃止の旨及びその終了計画**（タイムスタンプの継続的な検証に係る項目、鍵の安全な廃棄及びその過程の記録・報告に関する事項 等）**を通知することを規定する**。

現行の制度においては、認定を受けたTSAの業務廃止に際して、事後的な届出の提出を規定している。事後的な届出では、認定タイムスタンプの信頼の起点となる情報（認定に係る情報等）の更新も廃止後になり、制度の信頼性に直接影響を及ぼすことが懸念される。したがって、国による認定制度においては、トラストリスト（仮）の適切なタイミングでの更新を考慮し、総務大臣への廃止の届出は事前とすることが適切だと考えられる。

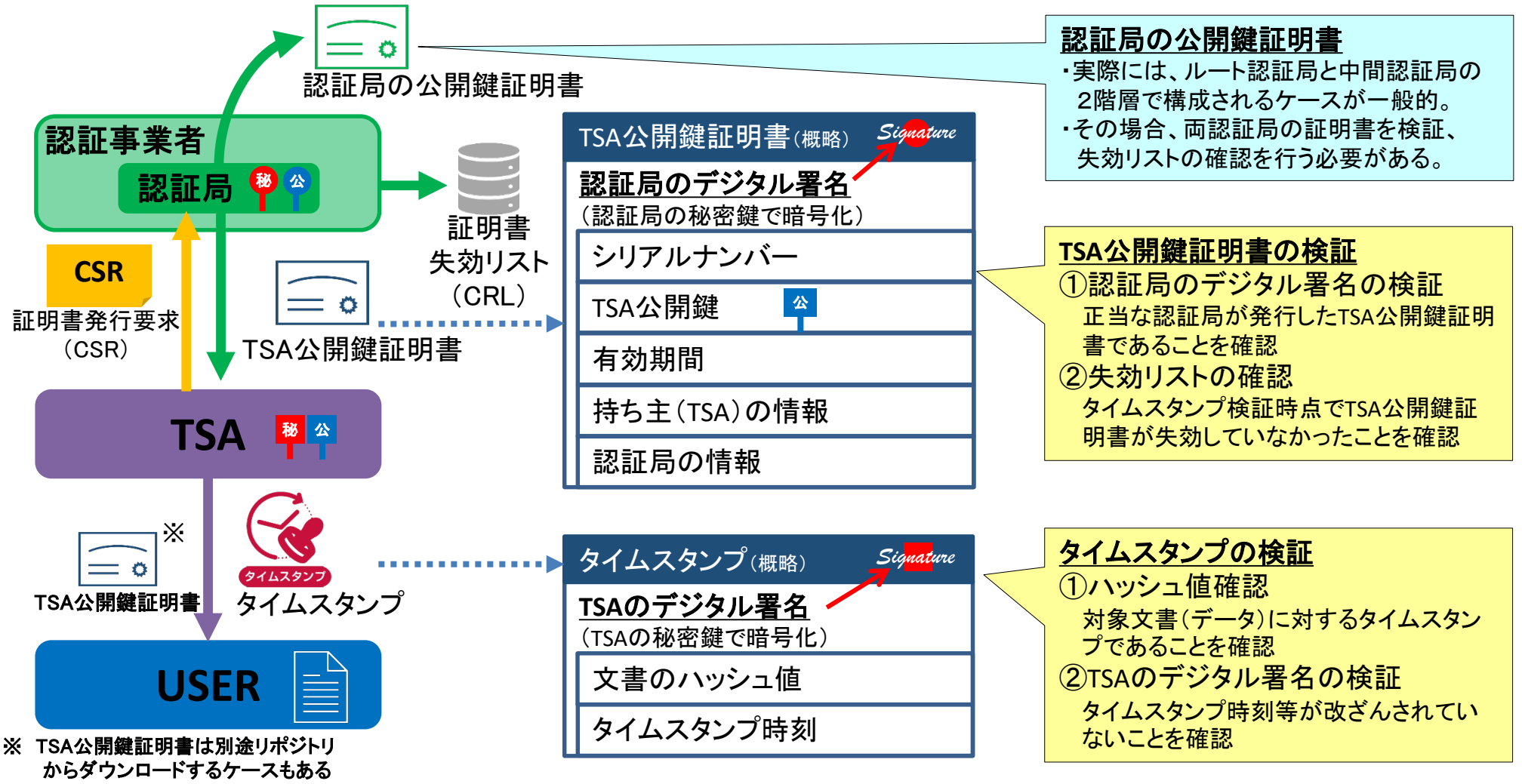
また、利用者の予見性の観点から、認定業務の突然の廃止によって利用者が不測の不利益を被ることがないよう、認定事業者は事前に廃止の旨と終了計画について利用者に通知することが適切だと考えられる。なお、認定時に予め終了計画を策定する場合は、その手厚い終了計画によって、認定事業者に過度な負担がかかる恐れがあること、また、その終了計画を信頼した利用者に過剰な信頼を与える恐れがあることに鑑みて、認定時に終了計画を求めることは規定せず、事前の廃止の届出とあわせて総務大臣に提出することを求めることが適当だと考えられる。

⑥その他

○TSA公開鍵証明書を発行する認証事業者の基準

- TSA公開鍵証明書とは、TSAの正当性を担保する電子証明書。
- 正当な認証局が、TSAの実在確認、証明書発行要求の発出元確認を行い発行。

（不当な認証局の場合、認定TSAの名を騙る「なりすまし」の証明書発行要求に応じてしまうおそれや、認証局の鍵管理が不十分で不正利用されてしまうおそれ等がある。）



認証局の公開鍵証明書
・実際には、ルート認証局と中間認証局の2階層で構成されるケースが一般的。
・その場合、両認証局の証明書を検証、失効リストの確認を行う必要がある。

TSA公開鍵証明書の検証
①認証局のデジタル署名の検証
正当な認証局が発行したTSA公開鍵証明書であることを確認
②失効リストの確認
タイムスタンプ検証時点でTSA公開鍵証明書が失効していなかったことを確認

タイムスタンプの検証
①ハッシュ値確認
対象文書（データ）に対するタイムスタンプであることを確認
②TSAのデジタル署名の検証
タイムスタンプ時刻等が改ざんされていないことを確認

⑥その他

○TSA公開鍵証明書を発行する認証事業者の基準

現状・課題

- 電子署名法の認定認証事業者と同等の認証事業者、または、信頼のある監査機関の監査（実態としてWebTrust※に限定）を受けた認証事業者であることを審査基準に規定。
- TSAの選定すべきTSA公開鍵証明書を発行する認証事業者の基準が不明確であり、TSAが認証事業者を選定・判断することが困難。

※ AICPA(米国公認会計士協会)とCICA（カナダ勅許会計士協会）によって共同開発されたサーバー証明書を発行する認証局の信頼性を保証するための監査プログラム

論点

- TSAが認証事業者を選定・判断できるよう、**認証事業者の基準を明確にすることが適切か**。
- 明確にすることが適切である場合、その基準は電子署名法の認定認証事業者、または、WebTrustの認証を取得した認証事業者であることを求めることが適切か。
- 電子署名法の認定やWebTrust以外に、他の認証制度や認定制度の活用の余地がある場合、どのような制度の活用が考え得るか。

方向性

- TSA公開鍵証明書を発行する認証事業者は、**電子署名法の認定認証事業者またはWebTrustの認証を取得した事業者**であることを基準として規定する。

現行制度では、TSAが利用すべき認証事業者の基準が不明確で選定・判断が困難だったことを踏まえて、TSAが認証事業者を選定・判断できるよう、認証事業者の基準は明確に定めることが適切だと考えられる。

その基準については、現行の制度の実態として電子署名法の認定認証事業者もしくはWebTrustの認証を取得した事業者であったことにも鑑みて、現行の制度からのシームレスな移行の観点から、電子署名法の認定認証事業者もしくはWebTrustの認証を取得した事業者であることが適当だと考えられる。なお、今後の技術動向等を踏まえ、必要に応じて電子署名法の認定制度及びWebTrustの認証以外の制度の活用についても検討を行い、適宜TSA公開鍵証明書を発行する認証事業者の基準を見直していくことが必要。

（参考）
EUでは、原則（should） TSA公開鍵証明書は、適格認証事業者によって発行される適格証明書であることを求めているが、他の認証を取得している認証事業者が発行する証明書を排除しているという実態はない。

⑥その他

○利用拡大に向けた取組

- 現行制度のタイムスタンプは以下に示すとおり、法令では電子帳簿保存法に位置付けられているほか、医療、知財、建築分野等のガイドラインでも広く求められている。
- 国による認定制度が創設され、制度としての信頼性がより一層向上することで、**利用者がタイムスタンプを導入しやすくなる**ことや、各省・業界において**法令・ガイドラインに位置づけやすくなる**ことが想定され、タイムスタンプの適用領域の更なる拡大が期待される。
- Society5.0の実現に向けて、データの信頼性（トラスト）の一要素である存在証明を担うタイムスタンプについて、**国民に対する広報活動を行う**とともに、**法令・ガイドラインの所管省庁等にタイムスタンプの位置付けについて働きかけ**ていくことが重要。

法令・ガイドライン等における認定タイムスタンプの位置付け

【法令】　電子帳簿保存法施行規則（国税庁）

【ガイドライン等】

（医療分野）
- 医療情報システムの安全管理に関するガイドライン　第5版（厚生労働省）

（知財分野）
- 先使用権制度の円滑な活用に向けて 第2版（特許庁）

（建築分野）
- 建築確認手続き等における電子申請の取扱いについて（技術的助言）（国土交通省　国住指第394号）
- 建築設計業務における設計図書の電磁的記録による作成と長期保存のガイドライン（日本文書情報マネジメント協会）
- 建築工事における書面・図面の電子化/保存ガイドライン（日本建設業連合会）

（環境分野）
- 計量証明書の電子交付等の運用基準（ガイドライン）例示（日本環境測定分析協会）

（消防分野）
- 消防同意等の電子化に向けたシステム導入対応マニュアル（消防庁　消防予第269号）

（契約関係）
- 電子契約活用ガイドライン（日本文書情報マネジメント協会）

（その他）
- JNLA試験証明書の電磁的方法による発行について（製品評価技術基盤機構 認定センター（IAJapan））

（参考）その他法令・ガイドライン等におけるタイムスタンプの位置付け

（学問分野）
- 指導要録等の電子化に関する参考資料（文部科学省）

（セキュリティ分野）
- ASP・SaaSにおける情報セキュリティ対策ガイドライン（総務省）

（手続関係）
- オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者(CIO)連絡会議決定）

（環境分野）
- 事業者向け公害防止ガイドライン（環境省・経済産業省）

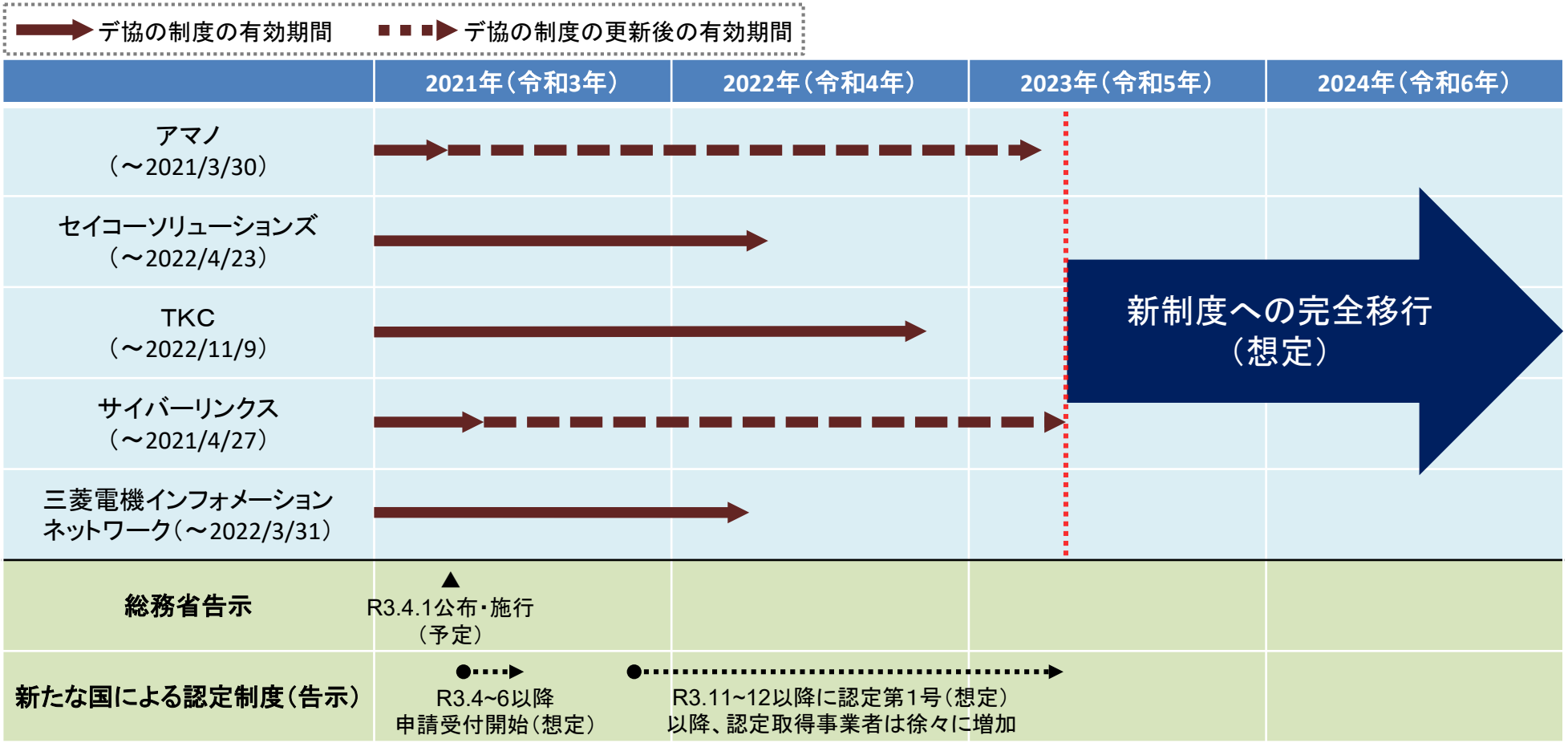
（監査関係）
- 電子的媒体又は経路による確認に関する監査上の留意点（日本公認会計士協会）

⑥その他

○経過措置

検討の観点

- 現行の認定を取得している既存の5事業者が新しい国の認定制度の認定を取得する場合、いつまでに新しい国の認定制度に移行するか。
- 既存の5事業者の移行スケジュール等も踏まえた上で、法令上の経過措置はどうあるべきか。



タイムスタンプの国による認定制度の全体像

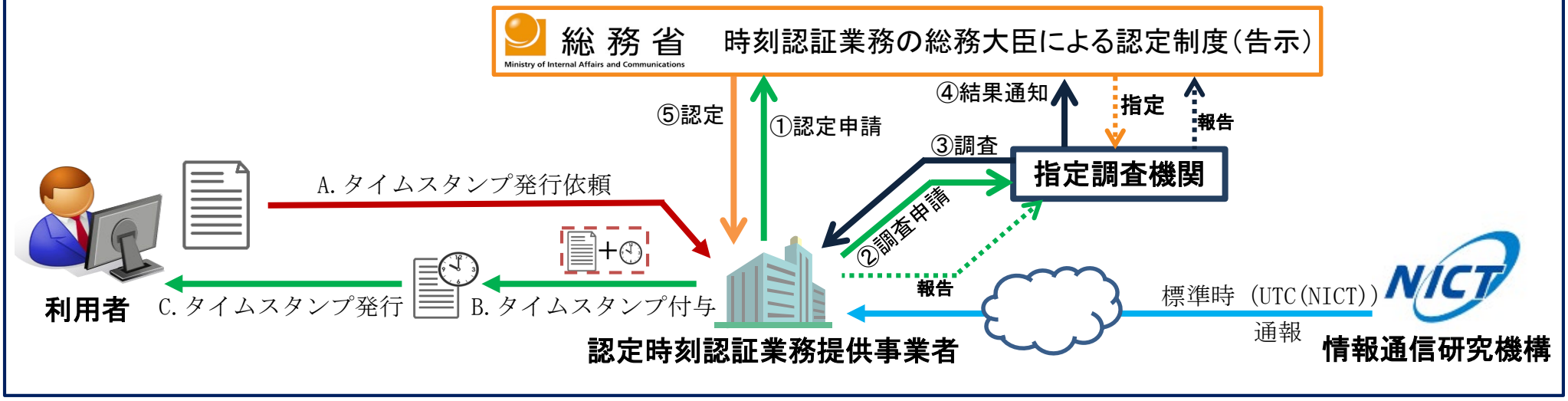
タイムスタンプの国による認定制度（告示）の概要

- **電子データがある時点に存在していたこと**及び**当該電子データがその時点から改ざんされていないこと**を証明する情報である「タイムスタンプ」を、電子データに係る情報に付与する役務を提供する業務を**「時刻認証業務」**とする。
- 時刻認証業務の中で、**確実かつ安定的にタイムスタンプを発行するための要件を満たすもの**を、**「認定時刻認証業務」**とする。

認定要件のポイント（抜粋）

- ○ デジタル署名方式を用いること。
- ○ 時刻源は国立研究開発法人情報通信研究機構のUTC（NICT）とすること。
- ○ 発行する（した）タイムスタンプと当該時刻源との時刻差が1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。
- ○ タイムスタンプは十分な安全性を有する暗号技術や装置等を用いて生成・管理すること。

認定制度の仕組み



現行の日本データ通信協会の認定制度と国による新たな認定制度の比較

□ 変更なし　■ 変更あり

	各論点	日本データ通信協会の制度	国による新たな認定制度
■	認定の単位	事業者単位	業務（サービス）単位
■	タイムスタンプの信頼性確保の方式 （時刻配信・監査業務事業者（TAA）の扱い）	TAA方式に限定	TAA方式以外も認める ※トレーサビリティの起点となる時刻源はUTC（NICT）
■	時刻認証業務の技術方式	デジタル署名方式、アーカイビング方式、リンキング方式	デジタル署名方式
■	申請できる者の条件	日本国内に拠点を有する者	国内に限定しない （外国の事業者の申請も認める）
■	設備面の基準	FIPS140-2 レベル3認証相当以上	FIPS140-2 レベル3認証相当以上に限定せず、コモンクライテリア等の認証制度も活用する
■	審査プロセスの効率化	―	ISMS等の認証や電子署名法の制度（申請時の提出書類、調査結果等）を活用し、効率化を図る
□	認定の有効期間	2年	
■	調査を実施する機関	認定主体：日本データ通信協会 調査主体：日本データ通信協会	認定主体：総務省 調査主体：総務省（第三者機関に委託可）
■	調査の内容	技術面、運用面、ファシリティ面、システムの安全性、情報開示	事業体の要件、技術面、運用面、ファシリティ面、システムの安全性、情報開示
□	監査の内容	調査で実施する全項目を対象	
□	監査のあり方	年に1回自主監査（部署外による内部監査も可）	
■	トラストリストへの記載事項等	• 氏名又は名称、法人はその代表者 • 認定に係る業務の種類 • 住所 • 認定日及び更新日並びに有効期間 を日本データ通信協会のHPに公開	• 認定業務を特定可能な情報（業務の名称、TSA公開鍵証明書 等） • 認定業務を実施する者が特定可能な情報（法人番号 等） 等について、国による認定タイムスタンプの履歴情報含め、総務省HPに公開 ※機械可読形式での公表は今後の検討課題
■	事業体として求められる要件	―	財務状況等を審査項目で規定
■	廃止の場合の取扱い	• 日本データ通信協会への事後的な届出 • 利用者に対する事前通知	• 総務省への事前の届出 • 利用者に対する通知（終了計画を含む） ※終了計画は、届出とあわせて提出
■	TSA公開鍵証明書を発行する認証事業者の基準	• 電子署名法の認定認証事業者と同等の認証局 • 信頼ある監査機関の監査に適合した認証局（WebTrust認証）	• 電子署名法の認定認証事業者 • WebTrust認証に適合した認証局

国による新たな認定制度とEUの制度の比較

□ 違いなし　■ 違いあり

	各論点	国による新たな認定制度	EUの制度
□	認定の単位	業務（サービス）単位	
■	タイムスタンプの信頼性確保の方式 （時刻配信・監査業務事業者（TAA）の扱い）	・TSA自ら時刻の信頼性及びトレーサビリティを担保する方式 ・TAA方式 ※トレーサビリティの起点となる時刻源はUTC（NICT）	・TSA自ら時刻の信頼性及びトレーサビリティを担保する方式 ※トレーサビリティの起点となる時刻源はUTC（k）
□	時刻認証業務の技術方式	デジタル署名方式	
■	申請できる者の条件	国内に限定しない（外国の事業者の申請も認める）	EU域内に限定
■	設備面の基準	FIPS140-2 レベル3認証相当以上に限定せず、コモンクライテリア等の認証制度も活用する	• FIPS140-2 レベル3認証以上 • コモンクライテリア認証EAL4以上
■	審査プロセスの効率化	ISMS等の認証や電子署名法の制度（申請時の書類、調査結果等）を活用し、効率化を図る	他のトラストサービスの審査と重複する部分は省略可
□	認定の有効期間	2年	
■	調査を実施する機関	認定主体：総務省 調査主体：総務省（第三者機関に委託可）	認定主体：EU加盟国が指定した機関（監督機関） 調査主体：適合性評価機関
■	調査の内容	事業体の要件、技術面、運用面、ファシリティ面、システムの安全性、情報開示	トラストサービスプロバイダーに対する一般的なポリシー要求事項、タイムスタンプを発行するトラストサービスプロバイダーに対するポリシー及びセキュリティに関わる要求事項等
■	監査の内容	調査で実施する全項目を対象	フル監査の50%程度の項目
■	監査のあり方	年に1回自主監査 （部署外による内部監査も可）	認定の有効期間内に1回のサーベイランス監査 （規定はないが、年に1回の内部監査も実施）
■	トラストリストへの記載事項等	• 認定業務を特定可能な情報（業務の名称、TSA公開鍵証明書 等） • 認定業務を実施する者が特定可能な情報（法人番号 等） 等について、国による認定タイムスタンプの履歴情報含め、総務省HPに公開 ※機械可読形式での公表は今後の検討課題	• トラストリスト自体に関する事項（公開場所(URL)、管理責任者、発行日 等） • トラストサービスプロバイダーに関する事項（事業者名称、所在地 等） • トラストサービスに関する事項（トラストサービスの種類、デジタルID 等） 等をトラストリストとして過去の履歴情報を含め機械可読形式で公表
■	事業体として求められる要件	財務状況等を審査項目で規定	財政基盤等について規定
■	廃止の場合の取扱い	• 総務省への事前の届出 • 利用者に対する通知（終了計画を含む） ※終了計画は、届出とあわせて提出	• 監督機関への事前通知 • 利用者への事前通知（終了計画を含む） • 終了計画に則った処理（ログ保管、証明書の失効等） ※終了計画は、認定時に策定
■	TSA公開鍵証明書を発行する認証事業者の基準	• 電子署名法の認定認証事業者 • WebTrust認証に適合した認証局	• 適格（Qualified）認証事業者