資料８－２

タイムスタンプ認定制度に関する検討会
取りまとめ骨子（案）

令 和 ２ 年 １ １ 月 １ ３ 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、**昨年１月に**「プラットフォームサービスに関する研究会」の下に**「トラストサービス検討WG」を立ち上げ、**約１年間検討を進め、**本年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、**本年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**。

タイムスタンプ認定制度に関する検討会

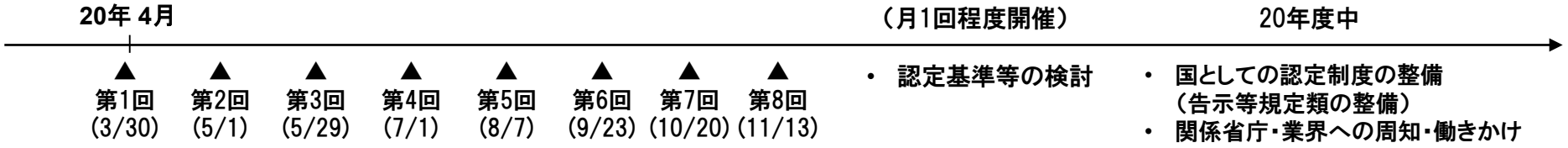
- タイムスタンプについて、国としての認定制度の基準を検討するため、有識者検討会を開催。
- 学識関係者、トラストサービス提供事業者、評価機関、経済団体（利用企業）等で構成。

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　早百合	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 パートナー・公認会計士・公認情報システム監査人
（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

（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」でのタイムビジネスの将来像に関する検討が開始。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）

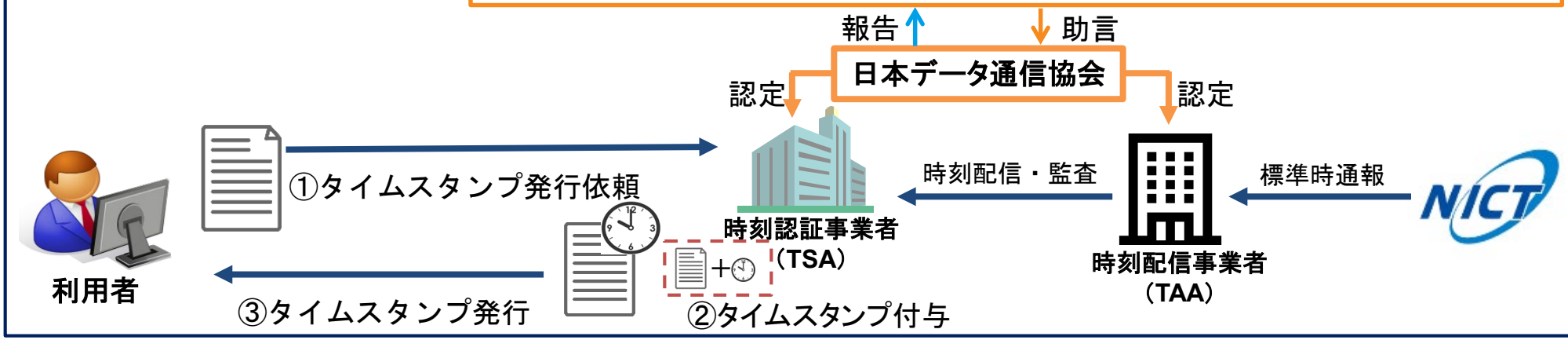
- **タイムビジネス**
  - 「時刻配信業務」及び「時刻認証業務」の総称
- **時刻配信業務**
  - 情報通信ネットワークを利用する上で必要となるサーバ等の電気通信設備に用いられる時刻に高い信頼性を与えるため情報通信ネットワークを通じて時刻情報を配信する業務、更に配信先の時刻精度を計測して報告を行う時刻監査業務。
- **時刻認証業務**
  - 電磁的記録に記録された情報（「電子データ」）について行われる措置であるタイムスタンプの付与及び当該タイムスタンプの有効性を証明する業務。
- **タイムスタンプ**
  - 電子データがある時刻に存在していたこと及びその時刻以降に当該電子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

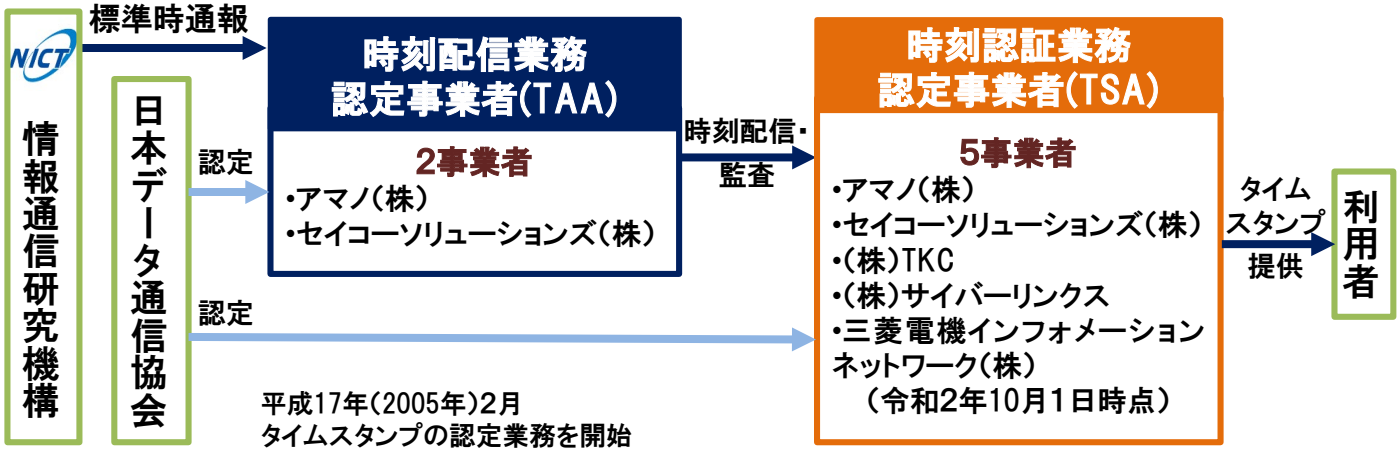
現行のタイムスタンプ制度の仕組みと現状の認定事業者

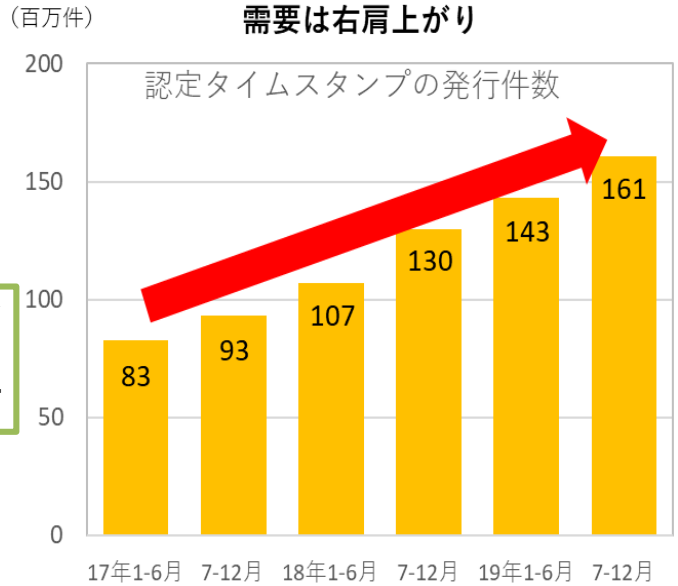
○　一般財団法人日本データ通信協会による民間の認定スキーム（タイムビジネス信頼・安心認定制度）により、タイムスタンプ事業者がサービスを提供

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

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

「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調査機関の要件、調査・監査の在り方

- **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
- **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
- **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

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）を判断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。

議論であがった主な意見

- 電子署名法やEUのeIDAS規則も踏まえ、認定の単位を業務とすることは賛成。
- 利用者が認定された業務を明確に特定できるようにするため、サービス単位で認定することが望ましいのではないか。
- 事業者単位の認定では、事業と直接的な関係を持たない事項も含めて評価する必要が生じるため、ロスが大きいのではないか。
- 業務単位からサービス単位へ変更することによって生じる既存の事業者への新たな事務的な負担や影響は少ないのではないか。

方向性

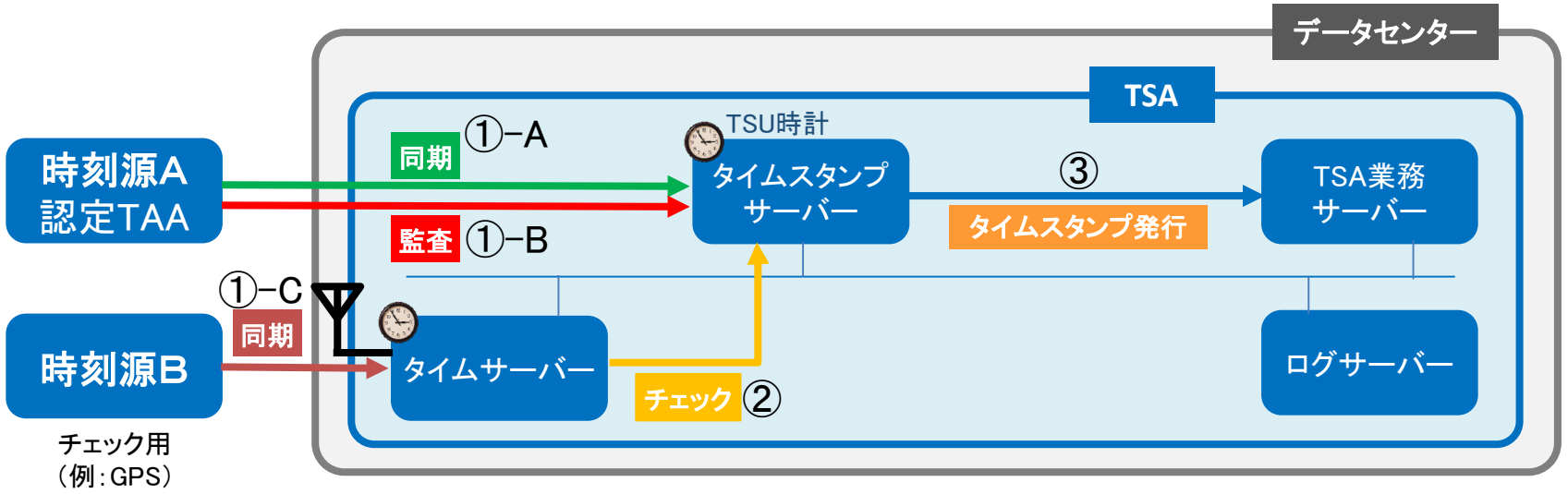
- 認定タイムスタンプ利用者が具体的な認定業務（サービス）を特定できるように、認定の単位は業務**（サービス）単位**とする。

①認定の対象

○時刻配信・監査業務事業者（TAA）の扱い

- 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：タイムサーバーは既定の頻度で時刻源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、タイムスタンプの信頼性を担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量に影響していること等が課題。

論点①

- タイムスタンプの信頼性を担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が自らタイムスタンプの信頼性を確保する方式も認めることが適当か**。

議論であがった主な意見①

- TAA方式以外のものを認めるとしても、トレーサビリティの起点となる時刻源については、少なくともUTC(NICT)を基準とし、それとは別にGPSやGNSSといった時刻源を用いることは妨げないといった方式が適切ではないか。
- TSAが自ら立証する方式を認めるとなった場合でも、方式を追加するだけなので、既存の認定事業者への影響は特段ないのではないか。

方向性①

- タイムスタンプの国としての認定制度の検討に当たっては、**タイムスタンプの信頼性確保に関して、**TAA方式に限定せず、**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**。

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**。
- **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**。

議論であがった主な意見②

- 時刻源はUTC(NICT)であることが適当。
- 時刻源は、チェック用を含めて複数ソース用いることを求めるべき。
- タイムスタンプ発行前の時刻精度の確認方法については、幅広く様々な方式を認めるのが適当ではないか。
- 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機器におけるログを改ざんできない形で保存しておくべき。また、その保存期間は、少なくともタイムスタンプの有効期限以上であることが望ましい。

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。
- **タイムスタンプ発行前に時刻精度の確認を行う**こととし、**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、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

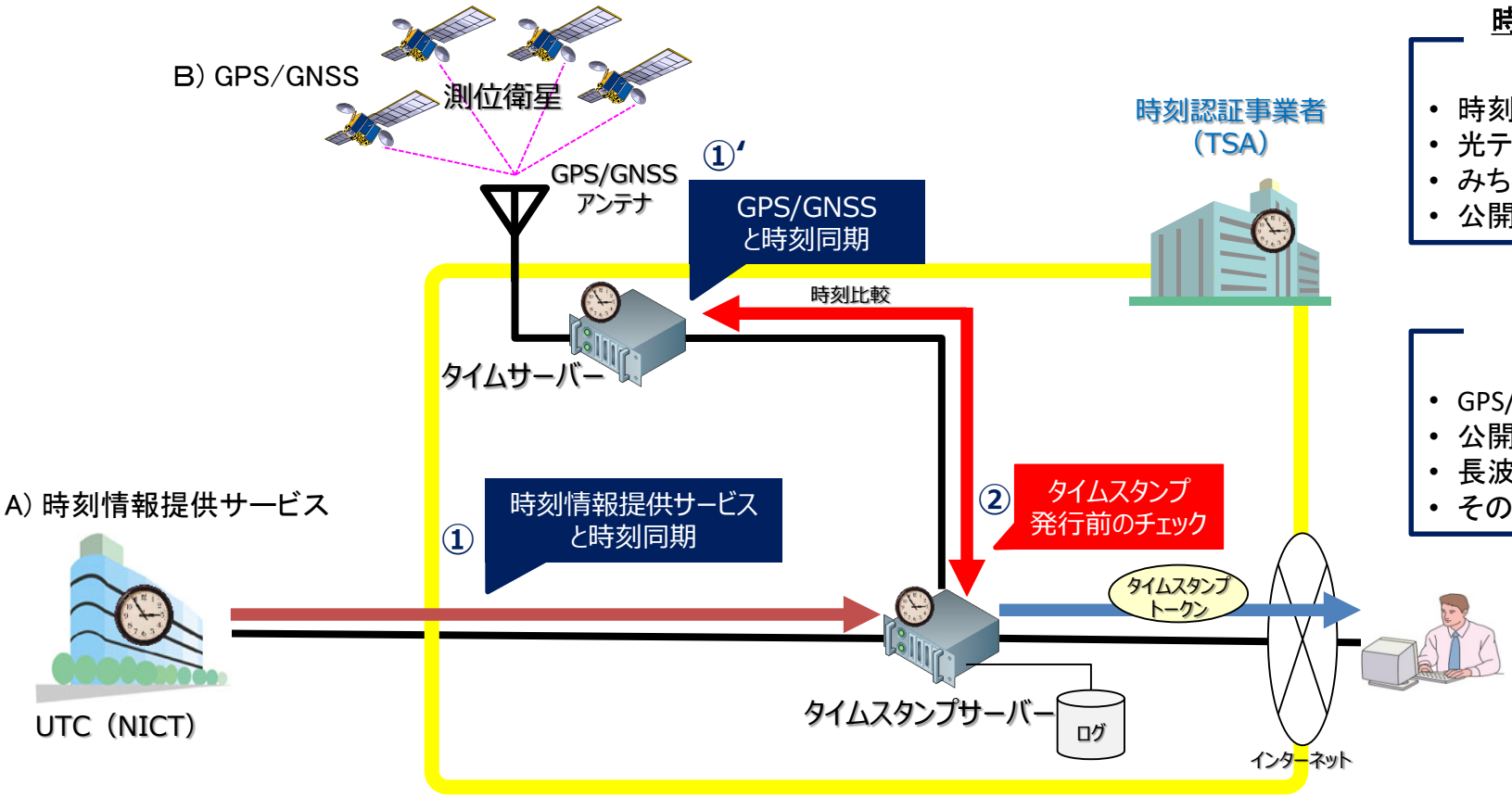
- 発行したタイムスタンプ時刻の時刻源に対するトレーサビリティをTSA自身が立証するために、**適切な機器における適切なログの保管**を行う。

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。
- **タイムスタンプ発行前の時刻精度の確認（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
- みちびき
- 公開NTPサーバー（UTC（NICT））

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

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**

議論であがった主な意見

- まずはデジタル署名方式で制度を開始することに異論はない。

方向性

- 審査の効率性の観点や現行の制度ではデジタル署名方式の事業者しかいないことも踏まえ、まずは**デジタル署名方式**で制度を開始する。

※ 制度創設当初に定める審査基準はデジタル署名方式のみとし、技術動向等を踏まえ、必要に応じて他の方式の検討を行う。

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、認定の申請を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。

議論であがった主な意見

- 海外の事業者からの申請も許容することが適当ではないか。
- 申請や調査にあたってかかるコストについて、事業者負担とするのであれば、海外の事業者からの申請も受け付けることが適当。

方向性

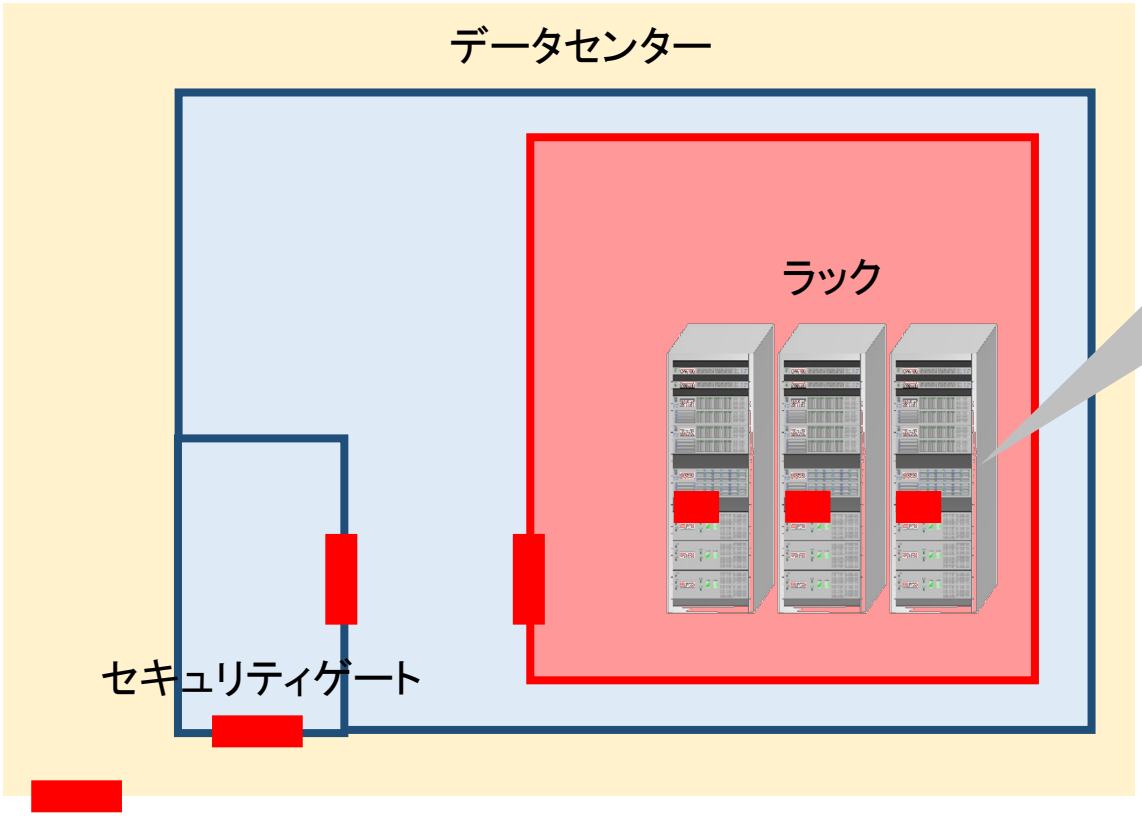
- 国内に限定せず、**外国の事業者の申請も可能なものとする**。

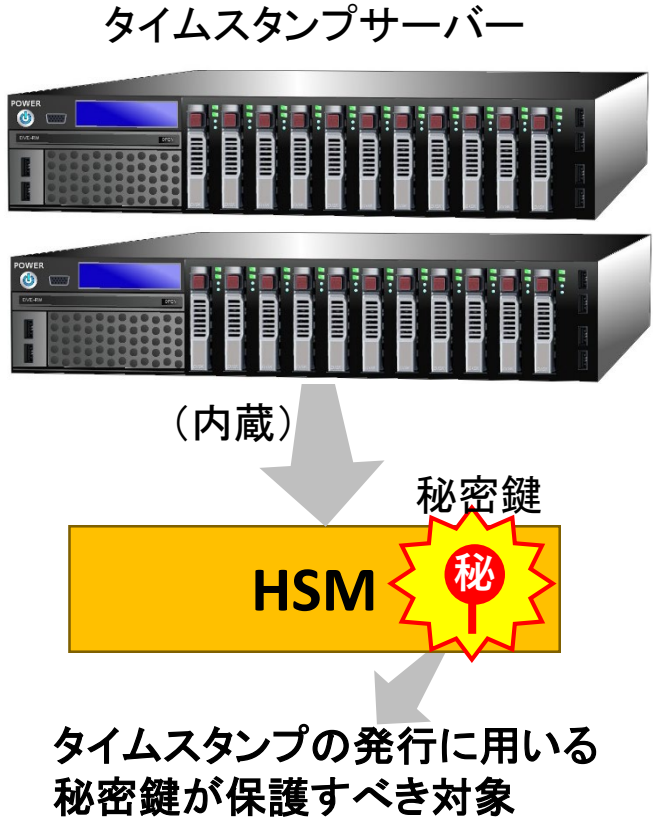
※ 海外の事業者であっても、日本の時刻を使うということを前提にすべきではないか。
海外の事業者であっても、国内の事業者と同様の審査を行うことを前提とする。

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

- タイムスタンプトークン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、継続的な調達の不安や、障害発生時の予備機の確保などの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**。

議論であがった主な意見

- 秘密鍵を保管するHSMはトラストサービスの根幹をなすものであり、ある程度のコストがかかっても、安全性が高い設備を求めるべき。
- HSMの基準としてコモンクライテリアを活用することに異論はないが、その保証レベルを示すEALをどう設定するかが重要。
- コモンクライテリアの保証レベルはEAL4以上であれば、FIPS140-2レベル3と同等以上の安全性があるといえるのではないか。

方向性

- 裾野を広げるために、HSMの基準として、現行のFIPSの基準に加え、タイムスタンプサービスに求められるHSMの要件を満たした**他の認証制度（コモンクライテリア等）も活用する**。

※ 我が国で選択するタイムスタンプに用いるHSMについてのコモンクライテリアの要件は要検討。

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。

議論であがった主な意見

- 既に電子署名法で提出しているエビデンスは、省略の余地があるのではないか。
- ただし、申請する側、受け取る側の双方において、運用面や体制面での工夫が必要。
- 電子署名とタイムスタンプの認証機関が異なる場合は、双方のノウハウを共有する必要がある。
- 他の認証と新しいタイムスタンプの国の認定制度の有効期間がバラバラだった場合、あまり効率化につながらない可能性があることは配慮すべき。
- トラストサービスプロバイダー全体に共通するクライテリアは、将来的には検討すべき。

方向性

- 審査プロセス効率化の観点から、**他の認証**（ISMS等）や**既存の制度**（電子署名法等）**も活用する**。

③認定の期間

○認定の有効期間

現状・課題

- 現行の制度において、認定の有効期間は2年。
- 年に1回以上の部署外からの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

議論であがった主な意見

- EUとの整合性を考えると、認定の有効期間は2年が適切ではないか。
- 日本では鍵更新が毎年行われることを踏まえると、適切に鍵更新、鍵廃棄が実施されたかどうかを確認するための監査のやり方等について工夫が必要。
- 鍵更新や鍵廃棄に関して監査等で十分にチェックされるのであれば、認定の有効期間は2年で問題ないのではないか。
- なお、適切に鍵更新が行われていたかどうかを確認する手段として、タイムスタンプトークンのサンプリングチェックが考えられるのではないか。

方向性

- **認定の有効期間は2年**とする。

※ 年に1回実施する監査において、認定の適切性の確認を行うこととする。

④調査機関の要件、調査・監査のあり方

○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、**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**。

議論であがった主な意見

- 第三者機関が調査を行えるように規定する場合、EUのEN 319 403やISO/IEC17065等に準拠できるような形で規定すべき。
- その上で、タイムスタンプ特有の差分を考慮して、各標準等でカバーしきれない部分の基準を定義していくことが重要。
- 電子署名法の指定のような方式をとるとしても、EUの制度といった国際的な制度との整合性は重要。

方向性

- 行政事務の簡素化や民間能力の活用の観点から、**民間の第三者機関に調査を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。

※ 今後トラストサービスの包括的な制度検討を行う場合には、必要に応じて国際標準であるISO/IEC17065やEUの標準であるEN 319 403を活用した要件を参考にすることは有用。

④調査機関の要件、調査・監査のあり方

○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**。

議論であがった主な意見

- 制度運用過程における調査・監査の内容の見直し（改正等）については、アドホックな対応ではなく、定期的なメンテナンスを検討すべき。
- 事業体として求められる要件について詳細に検討する際には、事業の継続性を担保するための要件としてある程度総合的に見て、柔軟に判断できるような基準であることが望ましい。
- EUはサーベイランス監査の他に内部監査も年に1回実施しており、その点が日本の認定制度とは差があるということは、将来的なEUとの交渉等に向けて留意しておくべき。

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、内部監査も可とすることも踏まえて、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。

④調査機関の要件、調査・監査のあり方

○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。

議論であがった主な意見

- 内部監査の客観性、信頼性をいかに担保するかという点には配慮が必要。
- 必要に応じて、外部の監査を使うといったチェックの仕組みは有用ではないか。

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。

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**。

議論であがった主な意見

- 誰が何のためにタイムスタンプを検証するのかという観点で、トラストリストに掲載する項目を検討することが重要。
- 公開すべき内容としては、法人番号、業務の名称・業務を行う者の名称（英文併記）、TSA公開鍵証明書のハッシュ値、公開鍵証明書、認証局の証明書等があげられるのではないか。
- EUのトラストリストのような仕組みで、履歴情報を用いて長期にわたって検証できるような環境が望ましい。
- ヒューマンリーダブルな形式がサービス選択を行う際の手がかりとなる一方で、マシンリーダブルな形式は既に発行されているタイムスタンプの自動的な検証のために必要。

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、国による認定タイムスタンプに限る）

※ タイムスタンプの自動的な検証の観点から、**マシンリーダブルな形式でも公表することが有用**。他方、**マシンリーダブルな形式での公開は、**トラストサービス横断的な要素も考えられることから、具体的なデータ形式や構造等を含め、**将来的には別途検討が必要**。

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**。

議論であがった主な意見

- 既存の制度を踏まえると、国の認定制度として整備するにあたっては、経済的基礎を求めることは適当ではないか。

方向性

- 事業体として求められる要件として、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として規定**する。

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、運用規定にて、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。

議論であがった主な意見

- 認定業務を公表することを考えると、廃止の届出は事後ではなく事前に求めるのが適当ではないか。
- 利用者の予見性の観点から、認定時に事業者に対して終了計画を策定させることが適切ではないか。
- 認定の段階で策定した終了計画が実際に廃止する際の事業者の過度な負担となり、また、認定時の手厚い終了計画を信用して契約した利用者に過剰な信頼を与える恐れがあるということにも考慮が必要。
- 利用者への事前通知については、“事前”の具体的な基準を何かしら定める必要があるのではないか。
- 継続性を保証するという点では、保険の活用についても検討の余地があるのではないか。

方向性

- 認定を受けた業務の適切なタイミングでの公表を考慮し、TSAから主務省への**廃止の届出は終了計画と併せて事前に求めることを規定する**。
- 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を通知することを規定する**。

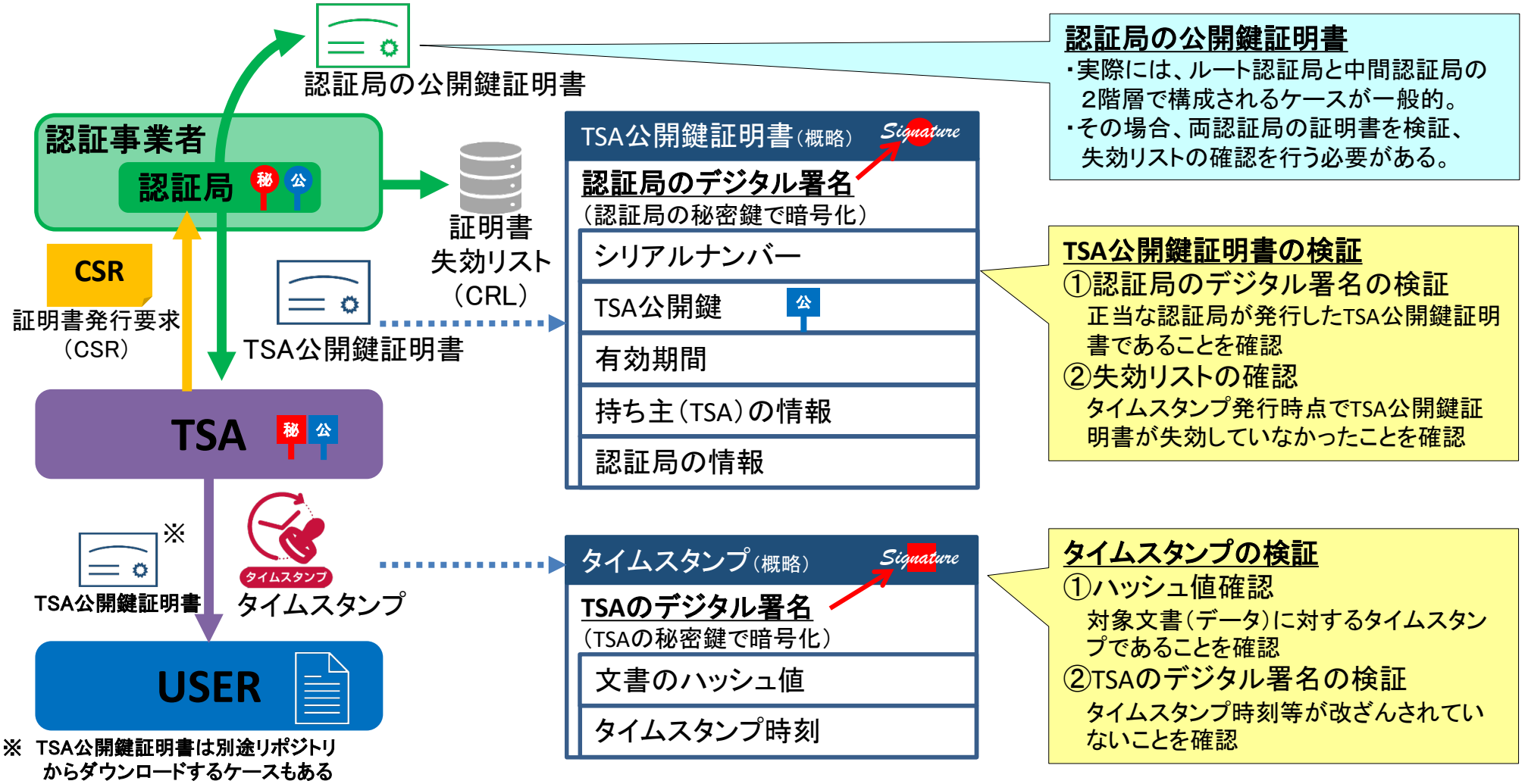
※ なお、**終了計画として規定すべき項目**については別途検討が必要。
（例：利用者への事前通知に必要な期間、タイムスタンプの継続的な検証に係る項目、鍵の安全な廃棄及びその過程の記録・報告に関する事項 等）

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
タイムスタンプ発行時点で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認証に限定）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。

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、Web Trust認証を受け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Web Trust認証以外に、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。

議論であがった主な意見

- 認定の単位が業務ということに鑑みて、事業者単位ではなく業務単位で基準を定めることが理想的だが、国の認定制度の運用開始が来年度ということを考慮すると、事業者単位の基準というのは妥当。
- 他の認証制度として、ETSIの監査も候補として考えられるが、監査分野においては、WebTrust認証は国内でも認知されているものの、ETSIの監査はまだあまり知られていないのも実態。

方向性

- 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**。
- その基準は、現行制度からのシームレスな移行を考慮し、**電子署名法の認定認証事業者やWebTrustに適合した事業者であることを求める**。

⑥その他

○利用拡大に向けた取組

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））

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）

（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）

（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）

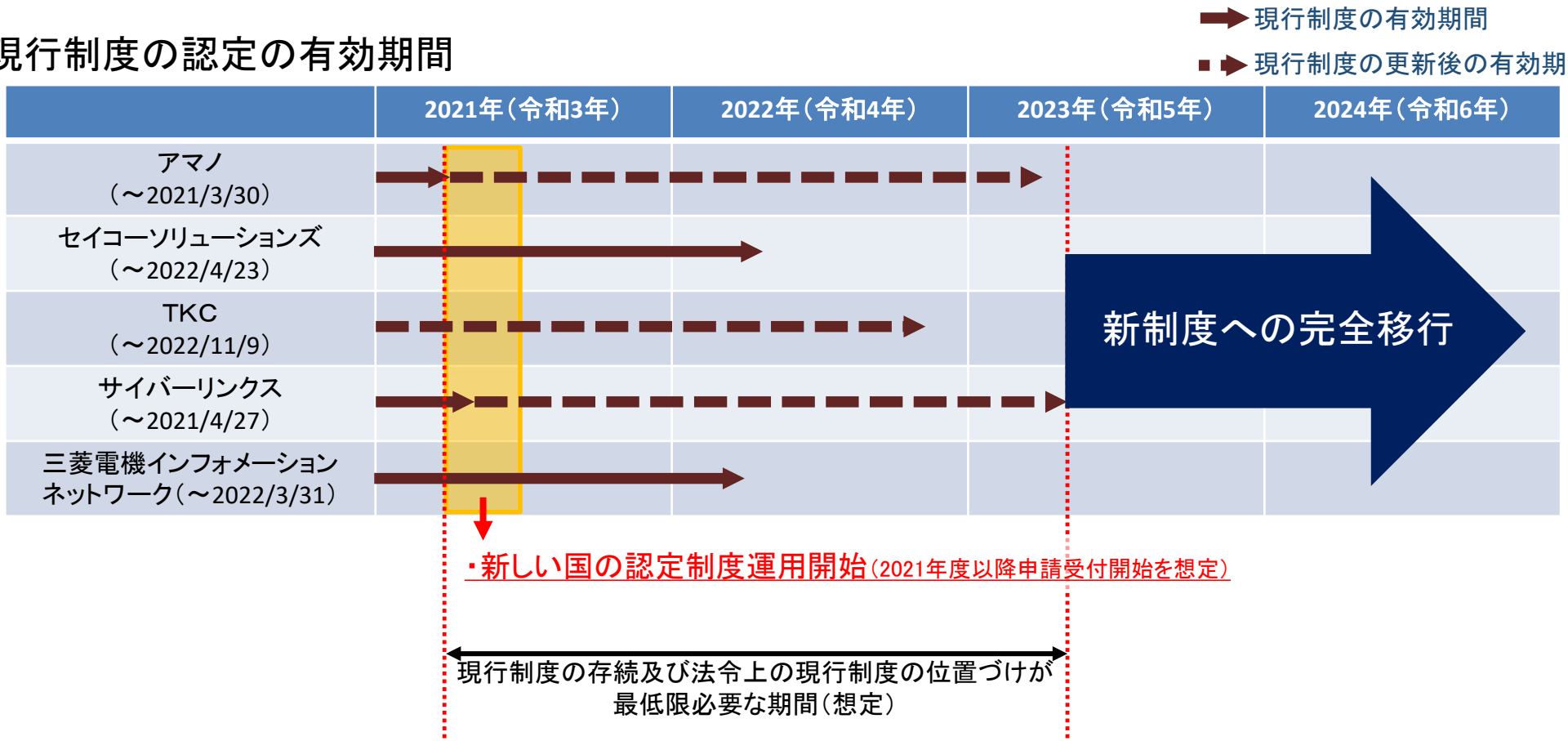
⑥その他

○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。

現行制度の認定の有効期間



現行の制度と新しい国の認定制度の比較

□ 変更なし　■ 変更あり

	各論点	日本データ通信協会の制度	新しい国の認定制度
■	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、廃止決定後に速やかに策定
■	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

新しい国の認定制度とEUの制度の比較

□ 違いなし　■ 違いあり

	各論点	新しい国の認定制度	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