資料８－１

令和２年度タイムスタンプ認定制度に関する調査研究

タイムスタンプの海外動向に関する調査

調査結果報告書

株式会社野村総合研究所
ICTメディア・サービス産業コンサルティング部　上級コンサルタント　山本以誠

2020年11月13日

NRI

Share the Next Values!

目次

1．調査の目的と概要

タイムスタンプ認定制度に関する検討会での議論において、調査すべきとされた海外の動向について調査を実施。結果、国のタイムスタンプ認定制度が存在するのはEUのみであることが判明

- EU、中国、米国を調査対象国・地域として、ウェブ等の公開情報ベースの調査を行い、そのうえで、調査結果の内容確認や内容深堀のために、以下の関係機関へのヒアリング調査を実施した。

  （EU）　TUV－IT社（ドイツの適合性評価機関）

  （中国）北京聯合信任技術サービス有限公司(UTSA)（中国の国家授時センター(NTSC)が、唯一正式に業務提携を行っているタイムスタンプ局(TSA)）及びIP FORWORD（コンサルティング会社、弁護士事務所、弁理士事務所が一体となって、模倣対策・知財保護、中国法務、中国ビジネス・サポートを提供するコンサルティング会社）

  （米国）GMO GlobalSign社（米国のタイムスタンプ局(TSA)）

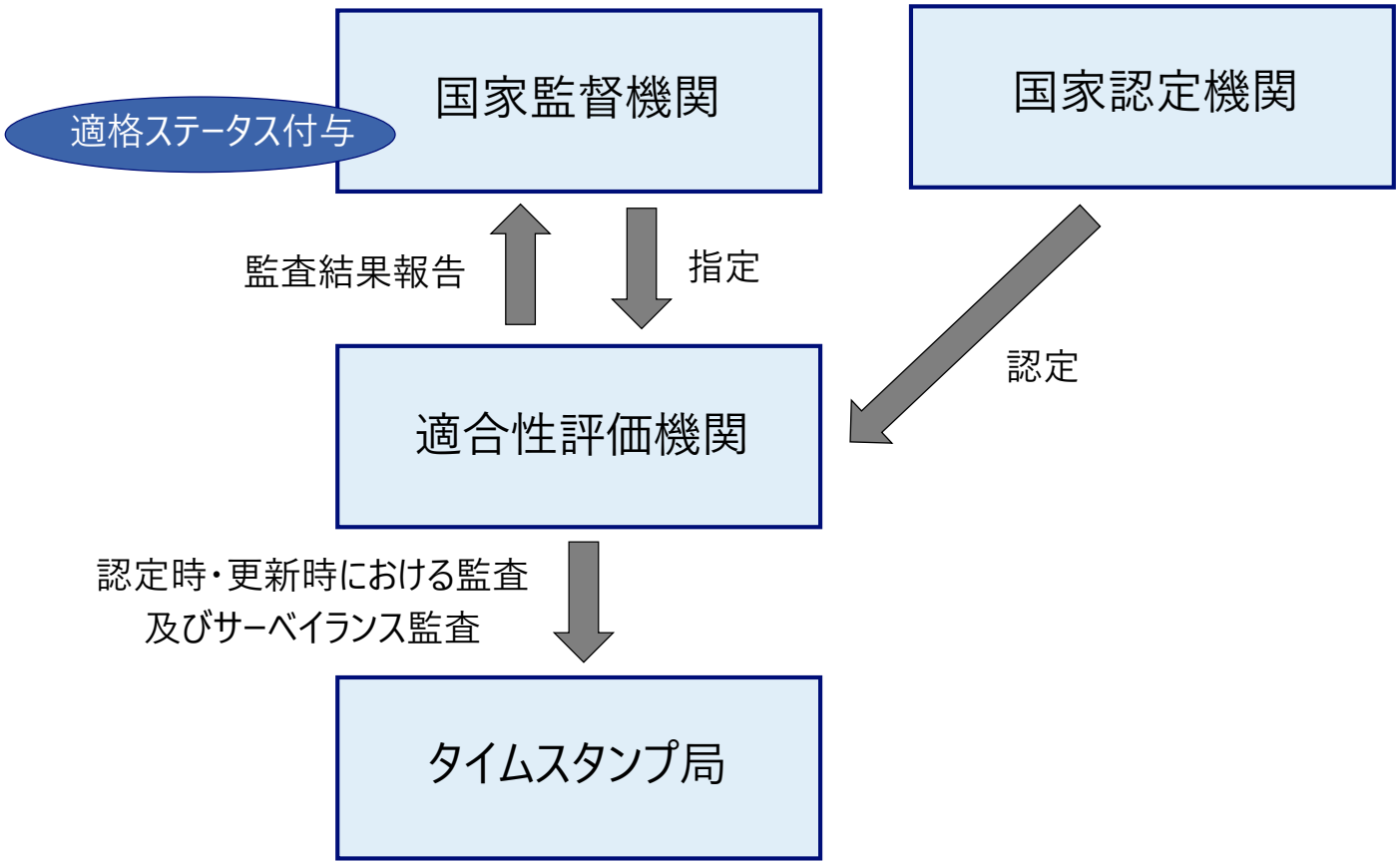
欧中米における調査結果の概要

	EU	中国	米国
国のタイムスタンプ認定制度	存在する	存在しない	存在しない
タイムスタンプ局(TSA)に参照されている主な基準	● ETSI EN 319 401 ● ETSI EN 319 411-1 ● ETSI EN 319 421	● 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」 ・「情報安全技術 公開鍵基礎設備 タイムスタンプ規範 GBT20520-2006」 ● 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）

２． EUにおけるタイムスタンプの動向

①認定の対象　：　(ア) 認定の単位

- EUには、eIDAS規則に基づいて、国家監督機関が、同規則に定める適用要件を満たすトラストサービスに対して、「適格(Qualified)」というステータスを付与し、適格トラストサービスとして認定する制度が存在する。
- 国家監督機関は、適格トラストサービスの認定に対して、責任を負う。
- 適格トラストサービスの中には、適格タイムスタンプサービスも含まれる。認定の単位は、サービス(業務)単位である。



①認定の対象　：　(イ) 時刻配信・監査業務事業者(TAA)の扱い

- 時刻のトレーサビリティの起点となる時刻源については、ETSI EN 319 421の7.7.1 Time-stamp issuanceにおいて、UTC(k)であることが規定されている。
- 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については、特定の方法に限定していない。複数の時刻源を用いることについても任意である。

TUV-IT社へのヒアリング結果

- EU各加盟国が、それぞれ時刻標準機間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３つの理由から、世界各国の時刻標準機関(k)であっても可としている。

  ①UTCは世界で合意された唯一の標準時刻である点
  ②ETSI規格は基本的にEUで策定されている規格であるが、EUに限定せずに参照されている環境がある点
  ③EUの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がある点

TUV-IT社へのヒアリング結果

- ドイツのタイムスタンプ局(TSA)の場合、ほとんどのタイムスタンプ局が、時刻源として、タイムスタンプサーバー内のシステムクロックを用いており、時刻精度のチェックやサービスの可用性確保のため、以下の３つの時刻源についても適宜使用している。

  ①GPS satellite systemを介した配信される公式の時報
  ②DCF 77(長波時報信号)を介して配信される公式の時報
  ③NTPサーバーへの接続

注：ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

①認定の対象　：　(イ) 時刻配信・監査業務事業者(TAA)の扱い

- 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源であるUTC(k)との差を± 1 秒以内として、タイムスタンプトークンの発行において、その精度の確認を行うことが、ETSI EN 319 421の7.7.1 Time-stamp issuance、7.7.2 Clock synchronization with UTCにおいて規定されている。なお、ETSIの規格では、時刻精度を確認するための具体的な方法については、特定の方法に限定していない。
- なお、UTC(k)との差について、± 1 秒を上回る結果が検出された場合、タイムスタンプサーバーによるタイムスタンプトークンの発行が停止される。

TUV-IT社へのヒアリング結果

- タイムスタンプサーバー内のシステムクロックについては、その品質によって稀にジャンプやドリフトが発生して、時刻がずれてしまう場合がある。そのため、システムクロックを複数確保して、それらを比較することにより、ジャンプやドリフトが発生していないことを確認する作業を行っている。
- ジャンプやドリフトが発生しないようにすることは、ETSI EN 319 421の7.7.2 Clock synchronization with UTCにおいて規定されている。

注：ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

①認定の対象　：　(イ) 時刻配信・監査業務事業者(TAA)の扱い

- 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が、ETSI EN 319 421の7.12 Collection of evidenceにおいて規定されている。
- また、eIDAS規則の第24条において、適格トラストサービスプロバイダーの業務により発行または受信されるデータに関するすべての関連情報について、適切な期間、記録しアクセス可能にしなければならないことが規定されているが、それが何年間であるかという具体的な年限までは規定されていない。

TUV-IT社へのヒアリング結果

- タイムスタンプサーバー内に保存される時刻同期イベントのログとしては、以下の情報が該当する。

①時刻同期に関するレコード
②時刻同期の喪失に関するレコード
③TSU鍵とTSA公開鍵証明書のライフサイクルに関するレコード
④うるう秒
⑤発行されたタイムスタンプトークンの情報

TUV-IT社へのヒアリング結果

- ドイツの場合、旧電子署名指令が施行されていた頃は、30年間という保存期間が法律で定められていた。但し、実際の運用上は、不定の状態であり、年限を定めずに、保存し続けることが求められていた。
- そのような運用が、現在のeIDAS規則が施行されてからも、ドイツの中では引き継がれているため、不定の状態で、年限を定めずに、保存し続けることが求められている。

注：ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

①認定の対象　：　(ウ) 時刻認証業務の技術方式　(エ)申請できる者の条件

- 時刻認証業務の技術方式については、EUの場合はETSI EN 319 422において、デジタル署名を使用する方式のみの規格が定められている。
- eIDAS規則の第17条において、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定められており、このような状況を踏まえると、申請できる者の条件としては、明示的に要件が定められているわけではないが、実質的に、EU域内に設立されているトラストサービスプロバイダーに限定されていると理解される。

注：ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

②認定の基準　：　(ア) 設備面の基準　(イ)審査プロセス効率化

- タイムスタンプ局(TSA)が用いるHSMが満たすべきセキュリティ要件としては、ETSI EN 319 421の7.6.2 TSU key generation、7.6.3 TSU private key protectionにおいて、FIPS 140-2のレベル 3 以上、またはコモンクライテリア(ISO/IEC 15408)のEAL 4 以上に準拠することが規定されている。
- ISO/IEC 27001など、認証取得の際の第三者機関による監査結果の援用については、完全に否定されるものではないが、実質的な運用を考えると非常に困難であるとされている。

注：ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

③認定の期間　：　(ア) 認定の有効期間

- eIDAS規則の第20条において、適格トラストサービスプロバイダーは２年間(24か月間)に１回以上、自らの費用で適合性評価機関による監査を受けることが規定されていることから、認定の有効期間は２年間となっている。

TUV-IT社へのヒアリング結果

- タイムスタンプトークンに署名する署名鍵の更新の周期については、ETSIの規定や基準は存在しない。
- TSA公開鍵証明書の有効期間は通常は３年間であり、署名鍵の更新の周期は通常は１～３年間であるが、２年間という認定の有効期間は、これらの期間とは関係性はない。
- トラストリストにはHistoryが含まれており、Historyに基づいて、発行時に遡って、TSA公開鍵証明書が有効であったかどうかを検証できるため、TSA公開鍵証明書の有効期間が３年間でも問題はない。
- サービスの種類に応じて複数の署名鍵を持っており、署名鍵によって更新周期は異なるため、認定の有効期間は、署名鍵の更新周期に縛られるものではない。

TUV-IT社へのヒアリング結果

- 署名鍵の更新については、更新の際に、適合性評価機関等の第三者が立会い、適切に古い署名鍵が廃棄されているかどうかの確認を行うことまでは実施していない。
- 署名鍵の廃棄については、タイムスタンプ局(TSA)が二重管理のもとで行い、署名鍵の適切な廃棄に関するエビデンスを残すことが、ETSI EN 319 421の7.12 Collection of evidenceにおいて規定されている。また、当該エビデンスは、適合性評価機関が監査を行う際に確認している。
- 署名鍵の更新の際に、新たなTSA公開鍵証明書をトラストリストに掲載することが必要になるが、そのような情報の連絡は、トラストリストを所管する機関に対するタイムスタンプ局(TSA)の自己申告が前提となっている。

注：ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

④調査機関の要件、調査・監査の在り方
：　(ア) 調査を委託する機関に求められる要件　　(イ) 調査・監査の内容

- eIDAS規則に基づいて、適格トラストサービスプロバイダーに対する調査・監査を担う適合性評価機関は、国家認定機関により認定されている。
- 適合性評価機関に求められる要件については、ETSI EN 319 403やISO/IEC 17065において規定されている。
- 認定時・更新時における監査において、タイムスタンプ局(TSA)が満たすべき要件については、ETSI EN 319 401、ETSI EN 319 411-1、ETSI EN 319 421において規定されている。
- ETSI EN 319 401においては、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が、また、ETSI EN 319 411-1においては、証明書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一般的な要求事項が規定されている。さらに、ETSI EN 319 421においては、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要求事項が規定されている。

ISO/IEC 17065 Conformity assessment – Requirements for bodies certifying product, processes and services

- ISO/IEC 17065の４ 一般要求事項において、法的及び契約上の事項や公平性のマネジメント、債務及び財務、非差別的条件、機密保持、情報の公開に関わる要件が定められている。
- その他に、ISO/IEC 17065の５ 組織運営機構に関する要求事項や、６ 資源に関する要求事項、７ プロセス要求事項、８ マネジメントシステム要求事項が定められている。

注：ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

④調査機関の要件、調査・監査の在り方　：　(ウ) 監査の在り方

- ETSI EN 319 403で規定される適合性評価機関に求められる要件において、２年間(24か月間)ごとの監査の間(中間年)に、年に１回のサーベイランス監査を実施することが義務付けられている。
- また、ISO/IEC 17065に基づいて認定を受ける適合性評価機関は、２年間(24か月間)の有効期限のある監査結果に対して、それを維持するために、サーベイランス監査プログラムを実施しなければならない。

TUV-IT社へのヒアリング結果

- タイムスタンプ局(TSA)と適合性評価機関との間の監査契約書の中に、認定の有効期間が２年間(24か月間)であることに加えて、２年間(24か月間)ごとの監査の間(中間年)に、サーベイランス監査を受けなければならないことが盛り込まれる 。
- 契約上においても、タイムスタンプ局(TSA)はサーベイランス監査を受けることが求められている。
- なお、サーベイランス監査に係る費用は、タイムスタンプ局(TSA)の自己負担である。

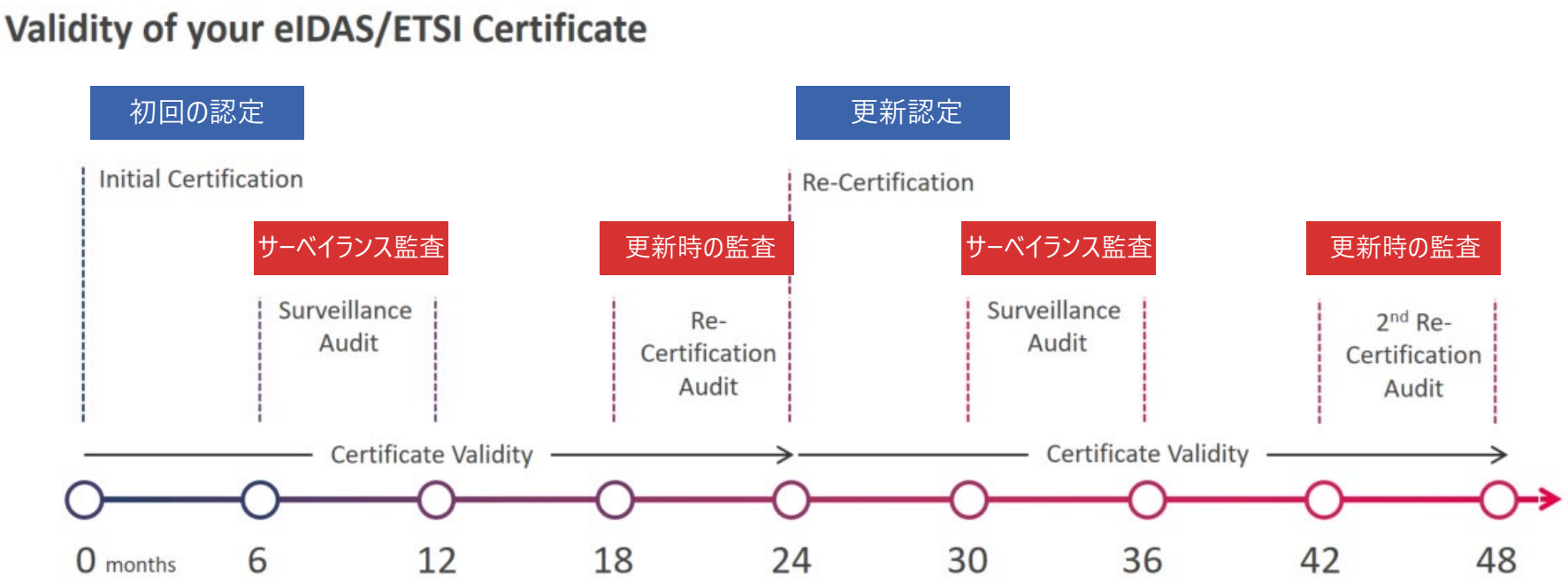
TUV-IT社へのヒアリング結果

- サーベイランス監査は、約１年前に実施した認定時や更新時における監査(フル監査)の状態から、適格性の付与について何らかの影響を及ぼすような変更が発生していないことを確認するものである。
- よって、サーベイランス監査における監査項目は、例えば、システムが適切に更新されているか、新しく配属された要員に対して教育が適切に実施されているか、ドキュメントが最新のものに更新されているか、運用体制に変更が生じていないか等の限定された項目になるため、その結果として、認定時や更新時における監査(フル監査) の監査項目の約50％程度となっている。

注：ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

④調査機関の要件、調査・監査の在り方　：　(ウ) 監査の在り方

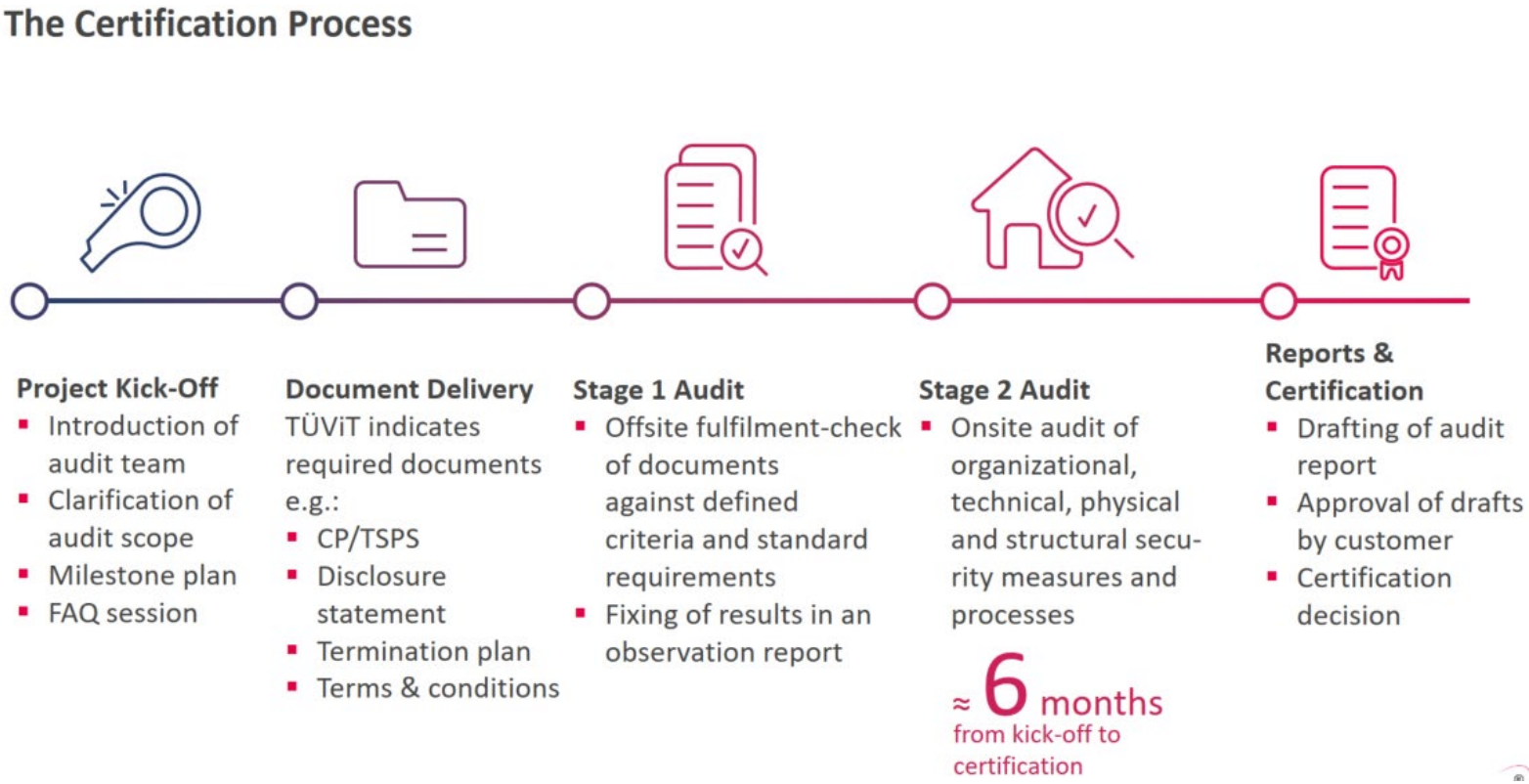
- サーベイランス監査は、認定時や更新時における監査(フル監査) の終了時点から12か月以内のタイミングで実施される。監査のサイクルを以下に示す。



出所）TUV-IT

④調査機関の要件、調査・監査の在り方　：　(ウ) 監査の在り方

- 実際のサーベイランス監査は、ISO/IEC 17065の中で２つのステージがあり、ファーストステージの文書監査(Stage1 Audit)とセカンドステージのオンサイト監査(Stage2 Audit)が要求される。
- 適合性評価機関とTSAの間で監査契約書が締結されると、キックオフミーティングが開催され、ファーストステージの文書監査とセカンドステージのオンサイト監査の実施のおおよそのマイルストーンが設定される。その後、セカンドステージのオンサイト監査において、どのサイトを訪問して、どの要員に対してインタビューを実施して、どのような情報にアクセスして、どのような点について確認するか等といった事項を取りまとめた監査計画が作成される。



出所）TUV-IT

⑤認定業務の公表内容及び公表方法　：　(ア) トラストリストへの記載事項等

- eIDAS規則の第22条に基づいて、各加盟国は、適格トラストサービスプロバイダーに関する情報や提供される適格トラストサービスに関連する情報を含め、トラストリストを作成し、公開している。
- EUは、各加盟国のトラストリスト(eIDAS Trusted Lists)を集約して、一括して閲覧できるようにするためのツールとして、リストオブトラストリスト(EU List of eIDAS Trusted Lists(LOTL))を提供している。
- トラストリストに記載される事項については、Commission Implementing Decision (EU) 015/1505というeIDAS規則の下位規則に規定されている。その中で、ETSI TS 119 612に規定されている要件が参照されている。
- また、トラストリストに記載される情報については、マシンによる読み取りが可能となるように、XML形式で掲載し公開されている。

TUV-IT社へのヒアリング結果

- 基本的な考え方として、トラストリストは、eIDAS規則のフレームワークのトラストアンカーになっている。
- タイムスタンプトークンを受け取った者が、受け取ったタイムスタンプトークンから、このサービスが適格タイムスタンプサービスであるか否かを、過去に遡って検証できるという点が、最も重要な観点であり、そのような観点を重視して、トラストリストは作成されている。

トラストリスト

- トラストリストに記載されている事項としては、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)のほか、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、連絡先、情報公開場所(URL)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、名称、デジタルID、認定状況等)が含まれている 。

注：ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists

⑥その他　：　(ア) 事業体として求められる要件

- 前述したとおり、認定時・更新時における監査において、タイムスタンプ局(TSA)が満たすべき要件については、ETSI EN 319 401、ETSI EN 319 411-1、ETSI EN 319 421において規定されている。その中には、財務の安定性といったタイムスタンプ局(TSA)の事業体としての要件も含まれる。
- トラストサービスプロバイダーに対する要求事項を定めたeIDAS規則の第24条において、損害に対する賠償責任のリスクに関して、国内法に従い、十分な資本を保有し、かつ適切な損害賠償責任保険を付保するか、またはそのいずれかの対応策をとることが規定されている。

TUV-IT社へのヒアリング結果

- ドイツの場合、タイムスタンプ局(TSA)に対して、年度ごとに財務諸表を公開することが義務付けられている。
- 監査法人や公認会計士に、財務諸表を確認してもらい、問題ない旨のステートメントを出してもらう。それをもって、適合性評価機関は、当該タイムスタンプ局(TSA)の財務が安定しているとみなしている。

注：ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

⑥その他　：　(イ) 廃止の場合の取扱い

- ETSI EN 319 421の7.14 TSA termination and termination plansにおいて、タイムスタンプ局(TSA)の終了計画に関する要件が規定されており、その中で、ETSI EN 319 401の7.12 TSP termination and termination plansが参照されている。認定時には、財政の安定性や終了計画をもとに、サービスが継続的に運用されるかどうかを確認している。
- トラストサービスプロバイダーに対する要求事項を定めたeIDAS規則の第24条において、トラストサービスプロバイダーは、監督機関によって監査されたサービスの継続を確保するための終了計画を持つことが規定されている。

TUV-IT社へのヒアリング結果

- 終了計画を適用する際には、以下のステップに則り、対応を行うことが必要となる。

  第１ステップ：タイムスタンプ局(TSA)が廃業する際には、３か月前までに監督機関にその旨を通知しなければならない。
  第２ステップ：利用者に対してサービスが終了することを通知しなければならない。
  第３ステップ：サービスの引継ぎ先を探す必要がある。引継ぎ先が見つからなければ、サービス自体を停止する。
  第４ステップ：サービスを運用してきた中で、保管義務のあるアーカイブのログ等を保管する手配を行う。
  第５ステップ：タイムスタンプトークンの発行を停止し、TSA公開鍵証明書を失効する。

- ドイツの場合、廃業したタイムスタンプ局(TSA)が持っていた、サービス運用中に保管義務のあるアーカイブのログ等は、サービスの引継ぎ先となるタイムスタンプ局(TSA)が見つかれば、当該タイムスタンプ局(TSA)が保管することになるが、サービスの引継ぎ先が見つからなければ、監督機関が保管することになる。

注：ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

⑥その他　：　(ウ) TSA公開鍵証明書を発行する認証事業者の基準

- 認定されたタイムスタンプ局(TSA)においては、正当な理由なしに、適格性が付与されていない公開鍵証明書を、TSA公開鍵証明書に用いることはできない（適格性が付与された公開鍵証明書を、TSA公開鍵証明書に用いることが強く推奨されている）。
- なお、認定されたタイムスタンプ局(TSA)が、適格性が付与されていない公開鍵証明書を、TSA公開鍵証明書に用いる場合には、適合性評価機関に対して、その正当性を主張できるだけの理由付けが必要となる。なかには、その理由が妥当であると認められるケースもあり、その結果として、トラストリストの中には、適格性が付与されていない認証事業者が発行する公開鍵証明書を、TSA公開鍵証明書に用いている認定されたタイムスタンプ局(TSA)が存在する。

⑥その他　：　(ウ) TSA公開鍵証明書を発行する認証事業者の基準

- 認定されたタイムスタンプ局(TSA)において、適格性が付与された公開鍵証明書を、TSA公開鍵証明書に用いることは必須ではない。（Web Trust for CAの監査を受けた認証事業者が発行する公開鍵証明書を、TSA公開鍵証明書に用いることも否定されていない。）
- 但し、認定されたタイムスタンプ局(TSA)が、適格性が付与されていない公開鍵証明書を、TSA公開鍵証明書に用いている場合には、適合性評価機関に対して、その正当性を主張できるだけの理由付けが必要となる。
- 理由が妥当であるということが認められた結果として、トラストリストの中には、適格性が付与されていない認証事業者が発行する公開鍵証明書を、TSA公開鍵証明書に用いている認定されたタイムスタンプ局(TSA)が存在する。

3． 中国におけるタイムスタンプの動向

①タイムスタンプの認定制度

- 中国においては、タイムスタンプの認定制度は存在しない。
- 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(NTSC)が、唯一正式に業務提携を行っているタイムスタンプ局(TSA)が存在する。その業務提携先である北京聯合信任技術サービス有限公司(UTSA)は、元中国国家工業及び情報化部の電子認証業務部門の責任者が代表を務めるなど、国家との結びつきが深い。
- 国家授時センター(NTSC)は、北京聯合信任技術サービス有限公司(UTSA) の株主でもあり、お互いに資本関係がある。よって、UTSAは、中国政府の関連企業として一般に認識されている。

UTSAへのヒアリング結果

- 業務提携における双方の業務分担としては、国家授時センター(NTSC)が国家標準時刻とタイムスタンプサービスシステムの時刻の同期、時刻精度の確認、時刻源の提供・採用を担当し、北京聯合信任技術サービス有限公司(UTSA)がタイムスタンプシステムの構築、技術支援、商用サービスの運営を担当している。

IP FORWORDへのヒアリング結果

- 北京聯合信任技術サービス有限公司(UTSA)が発行するタイムスタンプは、UTSA以外のタイムスタンプ局(TSA)が発行するタイムスタンプよりも法的効力が高いという事実を、中国裁判所が認定したことはない。
- ただし、UTSAが中国政府の関連企業という位置づけであることから、発行されたタイムスタンプに対する信頼度が高く、中国裁判所が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となっている。

②タイムスタンプ局(TSA)に参照されている主な基準

- 北京聯合信任技術サービス有限公司(UTSA)は、主に以下の規準を参照して、タイムスタンプサービス事業を実施している。
  - 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」
    - 「情報安全技術 公開鍵基礎設備 タイムスタンプ規範 GBT20520-2006」
  - 北京聯合信任技術サービス有限公司(UTSA)内部規準
- 北京聯合信任技術サービス有限公司(UTSA)内部規準は、UTSAが、上記の国際規準と中国国家(推奨)規準を基にして作成している内部規則(内部のタイムスタンプ業務操作規則)である。

TSAのウェブサイトの調査

- 北京聯合信任技術サービス有限公司(UTSA) 以外のタイムスタンプ局(TSA)においても、UTSAと同じように、「RFC3161」や「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」、「情報安全技術 公開鍵基礎設備 タイムスタンプ規範 GBT20520-2006」が参照されている。

中国国家(推奨)規準

- GBT36631-2018は、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・義務などを規定するものである。
- GBT20520-2006は、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するものである。

③信頼できる時刻源

- 「情報安全技術 公開鍵基礎設備 タイムスタンプ規範 GBT20520-2006」の9.2.2 信頼できる時刻源において、UTC(NTSC)、または国家授時センター(NTSC) が認可したハードウェア及び方法で取得する時刻を使用することが可能であることが規定されている。
- 「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」の6.4 時刻同期の管理において、時刻源の同期するUTCとして、UTC(NTSC)を使用することが規定されている。
- 北京聯合信任技術サービス有限公司(UTSA)においては、国家授時センター(NTSC) が認可したハードウェア及び方法で取得する時刻が使用されている。当該時刻は、UTC(NTSC)に同期されている。
- 北京聯合信任技術サービス有限公司(UTSA)は、タイムスタンプトークンの発行において、時刻精度の確認は実施していないが、国家授時センター(NTSC) が認可したハードウェア及び方法に対して、NTSCが定期的に時刻精度の確認、監査を実施している。

UTSAへのヒアリング結果

➢ 北京聯合信任技術サービス有限公司(UTSA)は、タイムスタンプサービスに関わるすべてのシステム及び設備(サーバーを含む)を、国家授時センター(NTSC) 内に設置している。これらのシステム及び設備(サーバーを含む)は、UTSAとNTSCが共同で構築したものである。

UTSAへのヒアリング結果

➢ 国家授時センター(NTSC) が認可したハードウェア及び方法で取得する時刻については、UTC(NTSC)との誤差がほとんどなく、北京聯合信任技術サービス有限公司(UTSA) においては、時刻精度に対する懸念は希薄である。万が一の場合に誤差が生じたとしても、±数マイクロ秒程度であると考えられている。

④監査の在り方

- 「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」や「情報安全技術 公開鍵基礎設備 タイムスタンプ規範 GBT20520-2006」には、監査を受けることが規定されていないが、国家授時センター(NTSC)が唯一正式に業務提携する北京聯合信任技術サービス有限公司(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。
- 「情報安全技術 公開鍵基礎設備 タイムスタンプ規範 GBT20520-2006」の9.2.5.1 監査データの生成において、内部監査用に、時刻同期等の各種ログを含め、監査記録を作成することが規定されている。
- 業務提携における業務分担において、NTSCが、時刻同期、時刻精度の確認、時刻源の提供・採用を担当していることから、UTSAは、時刻同期等の各種ログを保存していない。

UTSAへのヒアリング結果

- 北京聯合信任技術サービス有限公司(UTSA) が発行するタイムスタンプの有効期間は、少なくとも30年間である。30年間にわたり有効である状態が続くため、利用者は、有効期間を確認するという考え方を持ち合わせていない。

UTSAへのヒアリング結果

- 北京聯合信任技術サービス有限公司(UTSA)が用いるTSA公開鍵証明書の有効期間は、概ね２～５年間である。UTSAは、業務の内容等に応じて、適宜、TSA公開鍵証明書の更新を行っている。
- UTSA自らがTSA公開鍵証明書を発行する認証事業者にもなっている。

【参考】北京聯合信任技術サービス有限公司(UTSA)が発行したタイムスタンプトークンの実物

タイムスタンプトークン

- 証明書ビューアで確認したところ、北京聯合信任技術サービス有限公司(UTSA)が発行したタイムスタンプトークンにおいては、ハッシュアルゴリズムにSHA1 RSA、TSUの署名鍵にRSAの2048bitsが採用されている。それでいて、TSA公開鍵証明書の有効期間は30年間と非常に長くなっている。
- また、ルートCAのTSA公開鍵証明書、中間CAのTSA公開鍵証明書のいずれも、発行機関は共に北京聯合信任技術サービス有限公司(UTSA)であり、有効期間も共に30年間となっているなど、中国特有の特殊な状況が見られる。

４． 米国におけるタイムスタンプの動向

①タイムスタンプの認定制度

- 米国においては、タイムスタンプの認定制度は存在しない。また、タイムスタンプ局(TSA)やタイムスタンプサービスを監督・管理する政府機関や法制度も存在しない。

GMO GlobalSignへのヒアリング結果

- 治験データ等に関する監査証跡にタイムスタンプを利用することを義務付けている、FDA(米国食品医薬品局)のCode of Federal Regulations Title 21のPart11 Electronic Records; Electronic Signaturesの11.10(e) Audit Trailsのような普及を後押しする法制度は存在する。
- 但し、上記においても、タイムスタンプの利用やセキュリティ確保等に関する具体的な方法までは規定されていない。

②タイムスタンプ局(TSA)に参照されている主な基準

- 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が、米国のタイムスタンプ局(TSA)は、アプリケーション側からの処理要求等のもとで、国際標準であるRFC3161に準拠したタイムスタンプサービス事業を実施している。RFC3161は、米国タイムスタンプ業界のデファクトスタンダードとして位置付けられている。
- タイムスタンプサービスは、民間がビジネスの世界をリードする形で運用されている。具体的には、AdobeやMicrosoft、Oracle(Java)等といったITベンダーが、TSA公開鍵証明書を発行する認証局を承認して事前に登録しており、自社の製品・サービスにおいて、登録された認証局からTSA公開鍵証明書の発行を受けたタイムスタンプ局(TSA)が提供するタイムスタンプサービスを使用可能にしている。このような民間主導の取組がドキュメント用のタイムスタンプやコードサイニング用のタイムスタンプ等の普及に繋がっている。

GMO GlobalSignへのヒアリング結果

- ルート証明書の配布をサポートし、Windows クライアントが互いに信頼できるようにしているMicrosoftルート証明書プログラムにおいて、同プログラムで承認された認証局(CA)がコードサイニング証明書を発行する場合には、RFC 3161に準拠したタイムスタンプ局(TSA)が提供するタイムスタンプサービスを使用する必要があることが規定されている。
- このような要件を踏まえ、GMO GlobalSignを含めて、米国でコードサイニング証明書を発行する認証局(CA)は、自前でタイムスタンプ局(TSA)を運用し、タイムスタンプサービスを提供しているケースが多い。

GMO GlobalSignへのヒアリング結果

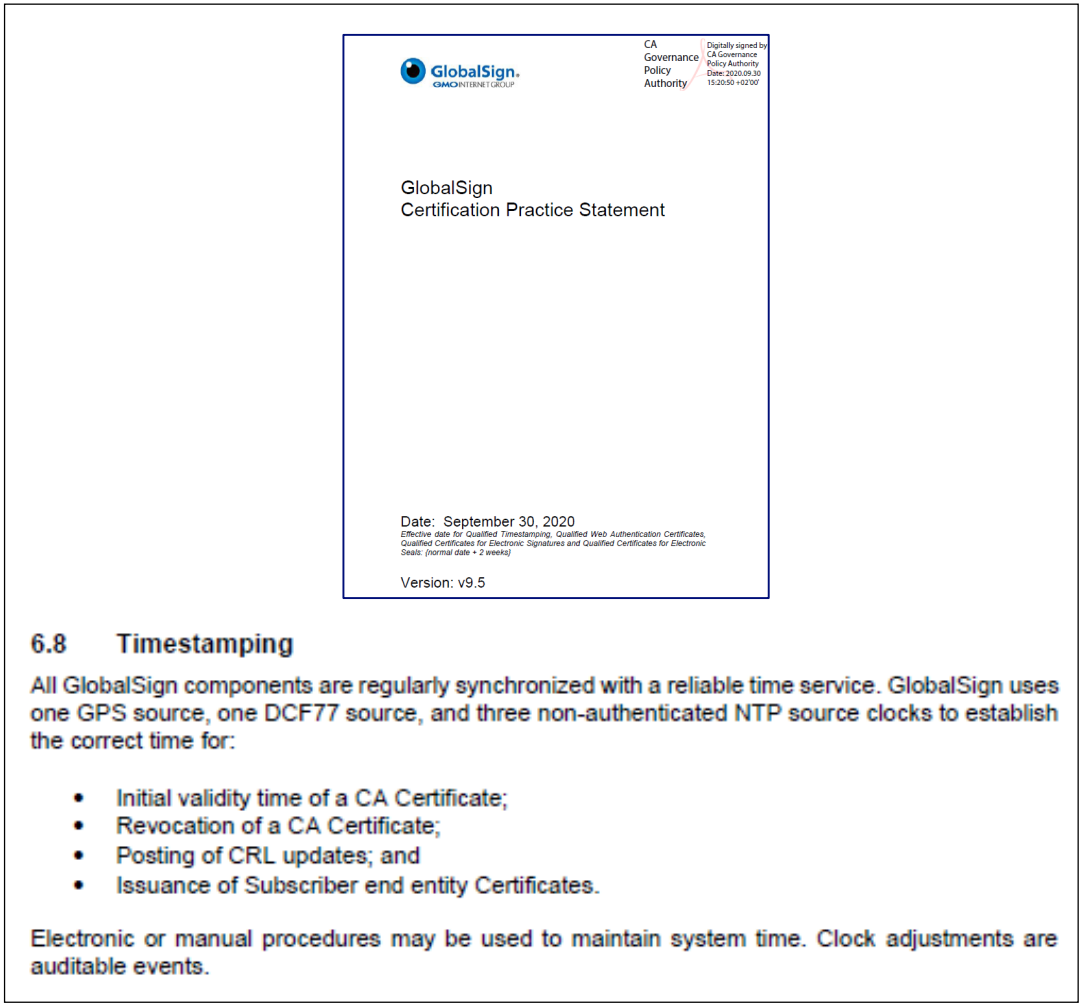
- RFC3161以外では、技術方式・性能について規定されているNIST SP800-102 Recommendation for Digital Signature Timelinessや、タイムスタンプサービスの運用について規定されているISO/IEC 18014 Information technology-Security techniques-Time-stamping services(Part1:FRAMEWORK、Part2:Mechanisms producing independent tokens、Part3: Mechanisms producing linked tokens、part4: Traceability of time sources) が、タイムスタンプ局(TSA) において参照されているケースが多い。

③信頼できる時刻源

- タイムスタンプ局(TSA)がタイムスタンプの発行に用いる信頼できる時刻源について規定する法律や基準は存在しない。

GMO GlobalSignへのヒアリング結果

- GlobalSignにおいては、①GPS satellite systemを介した配信される公式の時報、②DCF 77(長波時報信号)を介して配信される公式の時報、③認証されていないNTPサーバーへの接続で時刻を合わせられるシステムクロック(３つのシステムクロックを使用)により、正確な時刻を得ている。



GlobalSign
GMO INTERNET GROUP

CA Governance Policy Authority

Digitally signed by CA Governance Policy Authority
Date: 2020.09.30 15:20:50 +02'00'

GlobalSign
Certification Practice Statement

Date: September 30, 2020
Effective date for Qualified Timestamping, Qualified Web Authentication Certificates, Qualified Certificates for Electronic Signatures and Qualified Certificates for Electronic Seals: (normal date + 2 weeks)

Version: v9.5

6.8 Timestamping

All GlobalSign components are regularly synchronized with a reliable time service. GlobalSign uses one GPS source, one DCF77 source, and three non-authenticated NTP source clocks to establish the correct time for:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

④監査の在り方

- 監査を受けることを規定する法律や基準は存在しない。

GMO GlobalSignへのヒアリング結果

- Adobeが、Adobe AcrobatやAdobe Acrobat Readerにおいて承認・登録された認証局(CA)を、Adobe Approved Trust List(AATL)として取りまとめ、公表している。
- また、Adobeは、eIDAS規則に基づき、EU加盟国で承認されたトラストサービスプロバイダー(TSP)の認証局証明書情報が記載されたEU Trusted Lists(EUTL)を自社製品で利用可能とする機能も提供している。
- 認証局(CA)やトラストサービスプロバイダーが、このようなトラストリストに掲載されるためには、Adobeが定めるTechnical Requirementsの該当要件を満たすことが求められる。その際、Web Trustの監査またはETSIの監査を受けていることが、必須の要件となっている。
- Technical Requirements(2017年6月28日公表)の要件は、①General Requirements、②Requirements for End-entity certificates、③Requirements for Issuing CA certificates、④Requirements for Upper level CA or Root CA certificatesの 4 つのパートから構成されている。
- Microsoft においては、自社製品・サービスへの認証局ルート証明書搭載要件を、Microsoftルート証明書プログラムとして規定し、当該プログラムに基づき承認・登録された認証局とそのルート証明書を、Included CA Certificate Listとして取りまとめ、公表している。その際、Web Trustの監査またはETSIの監査を受けていることが、必須の要件となっている。
- このようなAdobe が公表するAdobe Approved Trust List(AATL)や、Microsoft が公表するIncluded CA Certificate Listは、タイムスタンプ局(TSA)が発行するタイムスタンプの信頼性・安全性を、ユーザが確認するための有用な拠り所となっている。


Share the Next Values!