資料3-1

我が国のタイムスタンプサービスについて

2019年2月28日

トラストサービス推進フォーラム　企画運営部会長
セイコーソリューションズ（株）DXソリューション統括部
柴田孝一

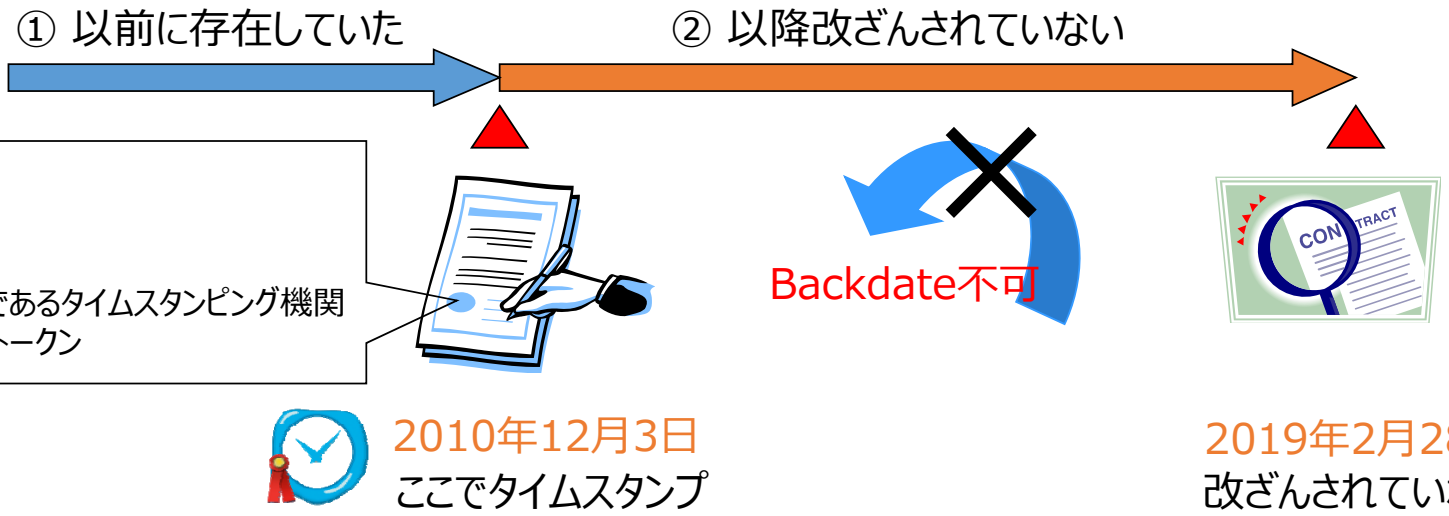
タイムスタンプとは

総務省の指針より

① 電子データがある時刻に存在していたこと

② 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

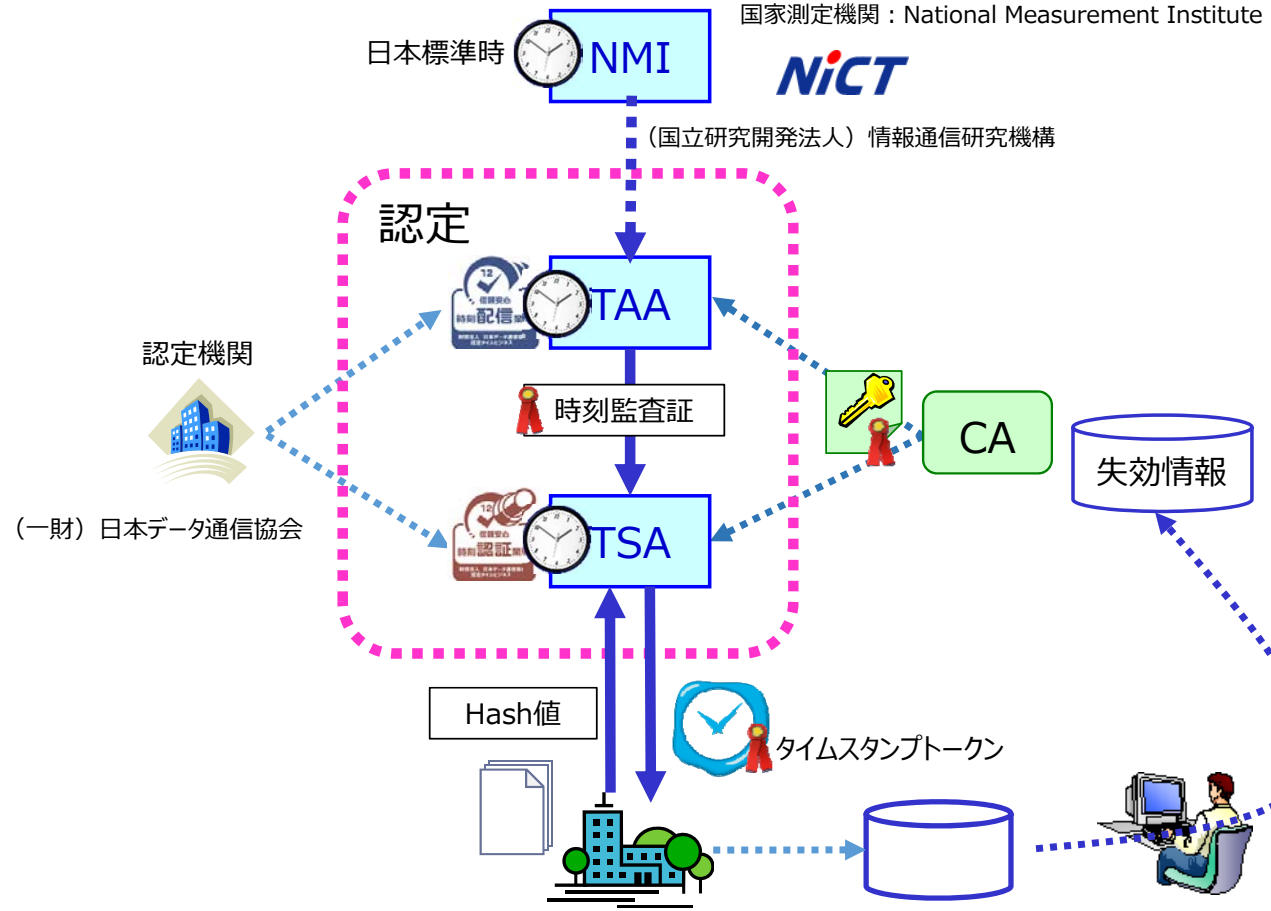


求められる要件

① 付与される時刻が、**信頼できる時刻** であること

② インターネットを介して将来に亘って利用されることから**国際標準**であること

タイムビジネス信頼・安心認定制度



TAA：Time Assessment Authority

タイムアセスメント機関

TSA時計に対して時刻監査を行うことに加え，時刻配信もできる機関。

TSA：Time Stamping Authority

タイムスタンピング機関

タイムスタンピングサービスを提供する信頼できる第三者（ISO/IEC 18014-1:2008の3.17）

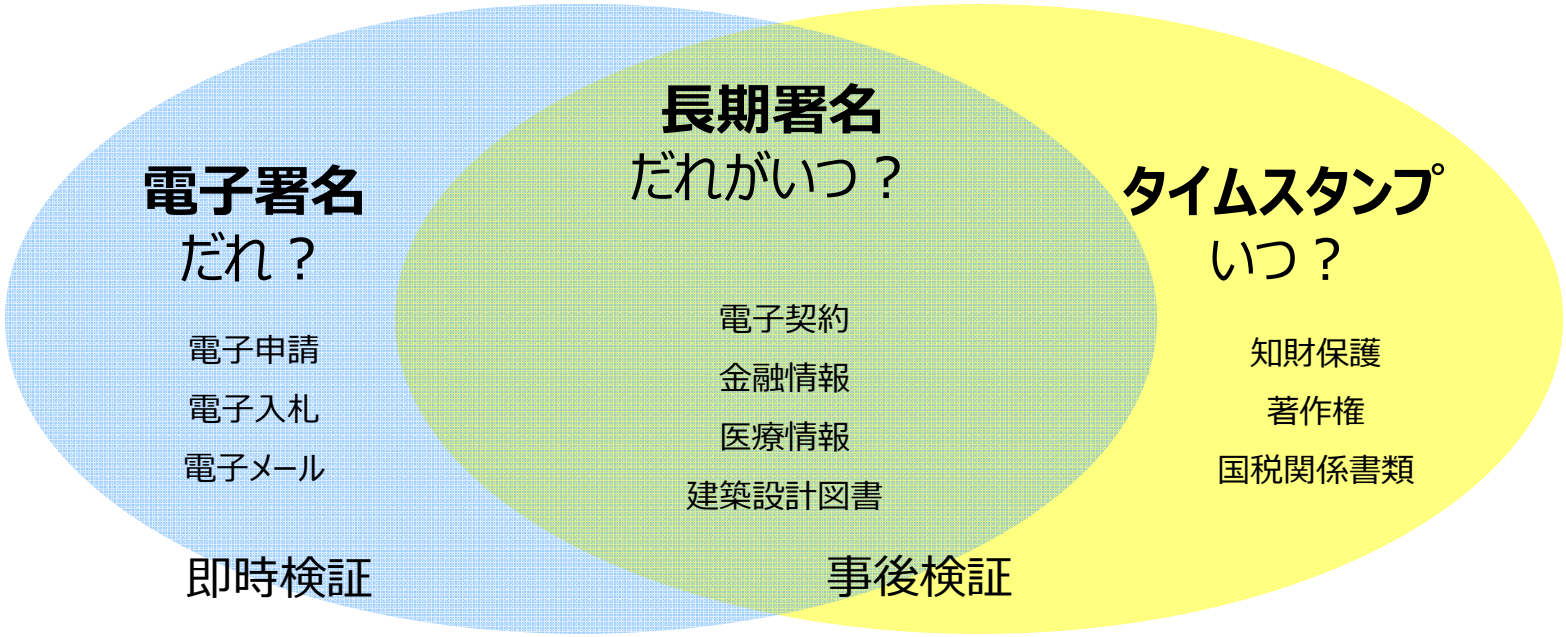
CA：Certification Authority

デジタル証明書発行局

電子証明書を発行と失効の依頼を受けた電子証明書や秘密鍵の危殆化の可能性のある証明書を失効させる機関

Hash値：元になるデータから一定の計算手順により求められた、規則性のない固定長の値であり元データの特定に利用する。

長期署名の概念



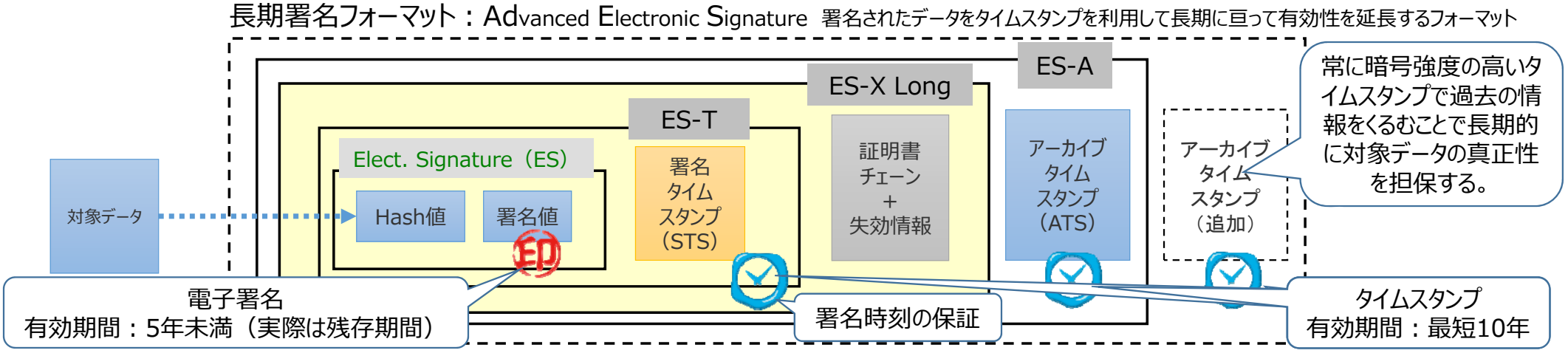
どちらも暗号技術を利用した電子データの**完全性を担保する技術**ではあるが利用目的が異なる

課題

- 課題1：長期署名が必要
- 課題2：廃局・廃業の対応策が未整備
- 課題3：法的安定性が無い
- 課題4：国際的な相互承認が必要

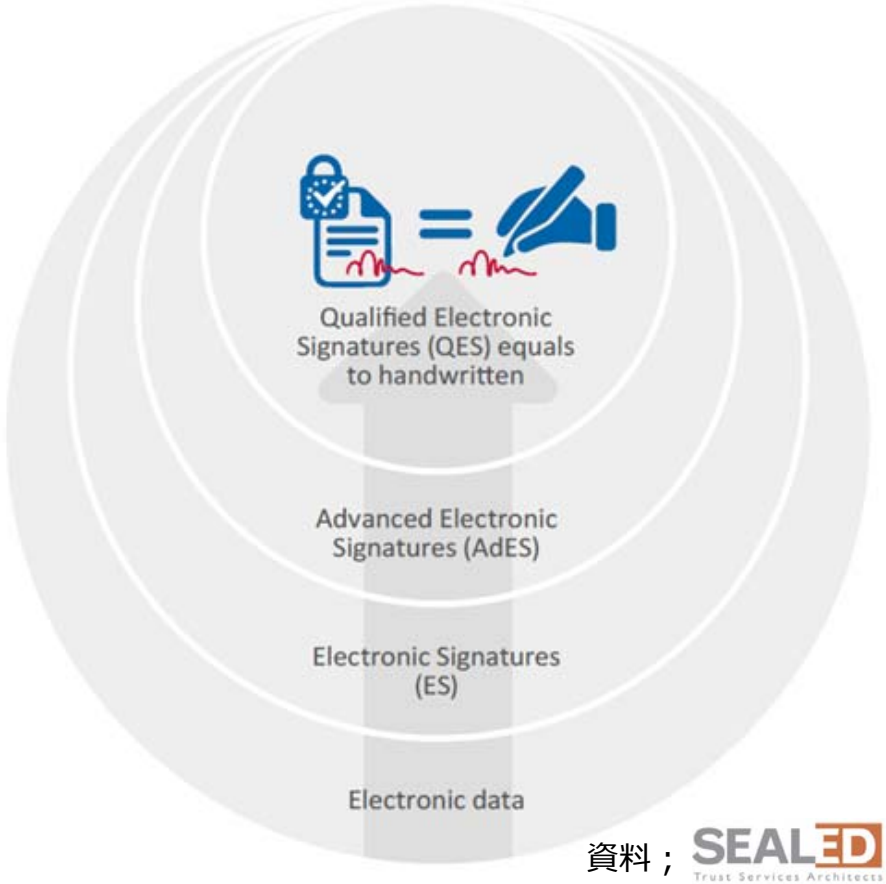
課題1：長期署名が必要

- 具体的な例
  - 電子署名のみでは長期的に真正性を検証できない。
    - 電子契約：住宅ローン、取引基本、売買、貸借、雇用、贈与、請負、委任など
    - 医療情報：法的に保存期間が定められている書類や訴訟対応で保存する書類
    - 建築設計図書：電子署名により電子的に作成できるが長期的な保存義務（15年）がある。
  - 長期署名が法令で規定されていない。
  - 長期署名に用いられているタイムスタンプには法的な安定性がない。



課題1：長期署名が必要

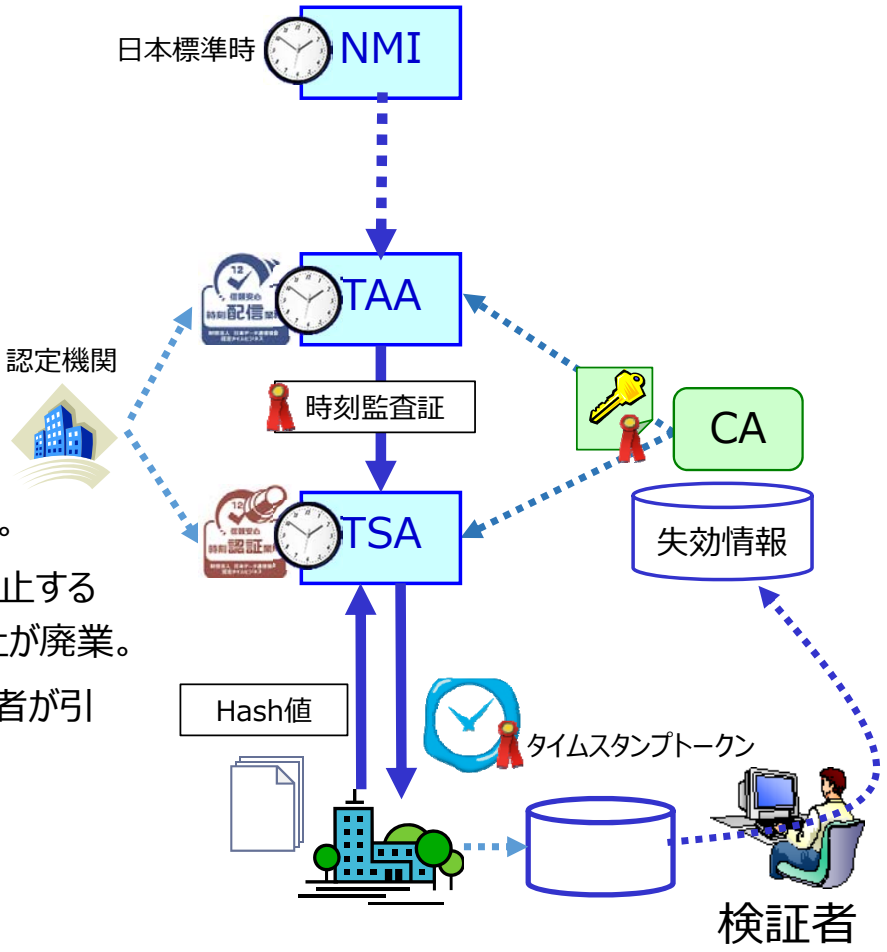
- EUでは、DigitalSingleMarketを推進するため、電子署名指令からAdvanced Electronic Signatureを加え、eIDASとして整備されている。
- 電子署名のみ場合、検証時に、検証者のPCにおける時間との比較で、電子署名の有効期間内であれば、その有効性が確認できるが、有効期間を超えた時点では、有効性が検証ができなくなってしまい、データの正確性を確認できない。
- 電子申請や電子入札においては、電子署名のみで、なりすまし・改ざんのリスクを回避できる。
- 一般的な電子取引では、即時に検証することはなく、後日に対象情報の検証をすることから、電子取引を推進するには、長期に亘って電子記録の真正性を検証できる必要がある。
- AdESであると、署名時の有効性をタイムスタンプによって検証が可能になり、電子署名の有効期限を超えた時点でも、署名の有効性が確認できる。
- タイムスタンプによってねつ造のリスクも回避できる。



資料；SEALED Trust Services Architects

課題2：廃局・廃業対応の規定が無い

- 具体的な例
  - TAA：
    - 利用者/依拠者が過去の時刻の正確性を確認できなくなる。
    - 時刻配信の停止に伴ってTSAのサービスが停止する。
  - TSA：
    - タイムスタンプに依拠しているサービスが一時停止する。
  - CA：タイムビジネス信頼・安心認定制度にはCAに関する規定はない
    - 利用者/依拠者が発行済タイムスタンプの有効性の確認ができなくなる。
    - 実例：A社が発行済タイムスタンプの有効期限を残して新規発行を停止することでTSA廃局、その後、TSAの公開鍵証明書発行事業者であるB社が廃業。
    - 対応：業界としての課題との認識から、失効情報公開運用を別事業者が引き継ぐことで解決した。
  - タイムビジネス信頼・安心認定制度の運用機関：
    - 認定機関が無くなる。
    - 認定タイムスタンプが発行できなくなる。



課題3：法的安定性が無い

- 具体的な例
  - 特許庁の先使用権ガイドラインで例示がされているが、判例がないことと、海外での訴訟時に対抗できないのではないかとの不安から採用を見送る場合がある。
  - 民間事業による認定制度なので、法務部門等で使用を躊躇する企業がある。
  - 法定保存文書の電子保存は、e文書法により広く認められているが、省令やガイドラインの規定が無い場合は、以下のような事業者独自の方法で行われる。
    - 電子化による効率化は進めるが、**保存義務のある文書は印刷して書面で保存**
    - **特定のシステムに依存**することで保存

課題4：国際的な相互承認が必要

	日本	EU	USA
法律	タイムスタンプそのものの法的根拠は無い 電子帳簿保存法施行規則では、国税関係書類は日本データ通信協会認定のタイムスタンプを付与することで電子保存が認められている。	eIDAS規則	ない
CABの認定機関	ない	加盟国の認定機関	ない
認証機関	日本データ通信協会	監督機関	ない
適合性評価機関（CAB）	日本データ通信協会	加盟国の認定を受けた適合性評価機関	ない
適合性評価機関の認定基準	ない	（電子署名と同じ） ISO 17065　EN 319 403 v2.2.2	ない
タイムスタンプ局の監査基準	タイムビジネスに係る指針 タイムビジネス信頼・安心認定制度審査基準	ETSI EN 319 401（電子署名と同じ） EN 319 412-1 v1.1.1 タイムスタンプ事業者へのポリシー、及びセキュリティ要求事項	ANSI X9.95-2016 Trusted Timestamp Management and Security (初版は2005年)
タイムスタンプフォーマット、タイムスタンプトークンのプロファイル	RFC 3161　ISO/IEC 18014		
		ETSI EN 319 422 タイムスタンププロトコルとプロファイル	
適合性の検証手段	データ通信協会のWeb	トラステッドリスト	ない
秘密鍵の暗号期間を超えた署名検証のためのタイムスタンプ	CAdES：JIS-X5092、ISO14533-1 XAdES：JIS-X5093、ISO14533-2 PAdES：ISO14533-3	CAdES：ISO14533-1 XAdES：ISO14533-2 PAdES：ISO14533-3	NIST SP 800-57r4 (2016) Recommendation for Key Management（FIPS 171, 1992 -> SP 800-57, 2005)
署名時刻の保証としてのタイムスタンプ			NIST SP 800-102 (2009) Recommendation for Digital Signature Timeliness
時刻のトレーサビリティ 時刻配信局の監査基準	タイムビジネスに係る指針 タイムビジネス信頼・安心認定制度審査基準 JISX5094、ISO18014-4		

国家機関（NIST）による規定

まとめ

- Society5.0が実現すると、ヒトのみならずIoTから送出される膨大なデジタルデータの流通で、新たなニーズが増えます。

- これらのニーズに対応するには、これまでの紙中心の世界とは異なる発想での大胆な改革が必要となります。

- Society5.0の実現に向けた、大胆な改革を求めます。

デジタルだからできる
情報の
完全性・真正性・責任追跡性
の担保