日・EUのトラストサービスに関する制度比較

2019年2月

一般財団法人日本データ通信協会
トラストサービス推進フォーラム　幹事

セコムトラストシステムズ株式会社

西　山　　晃

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

日・EUのトラストサービスの比較項目（Mapping）

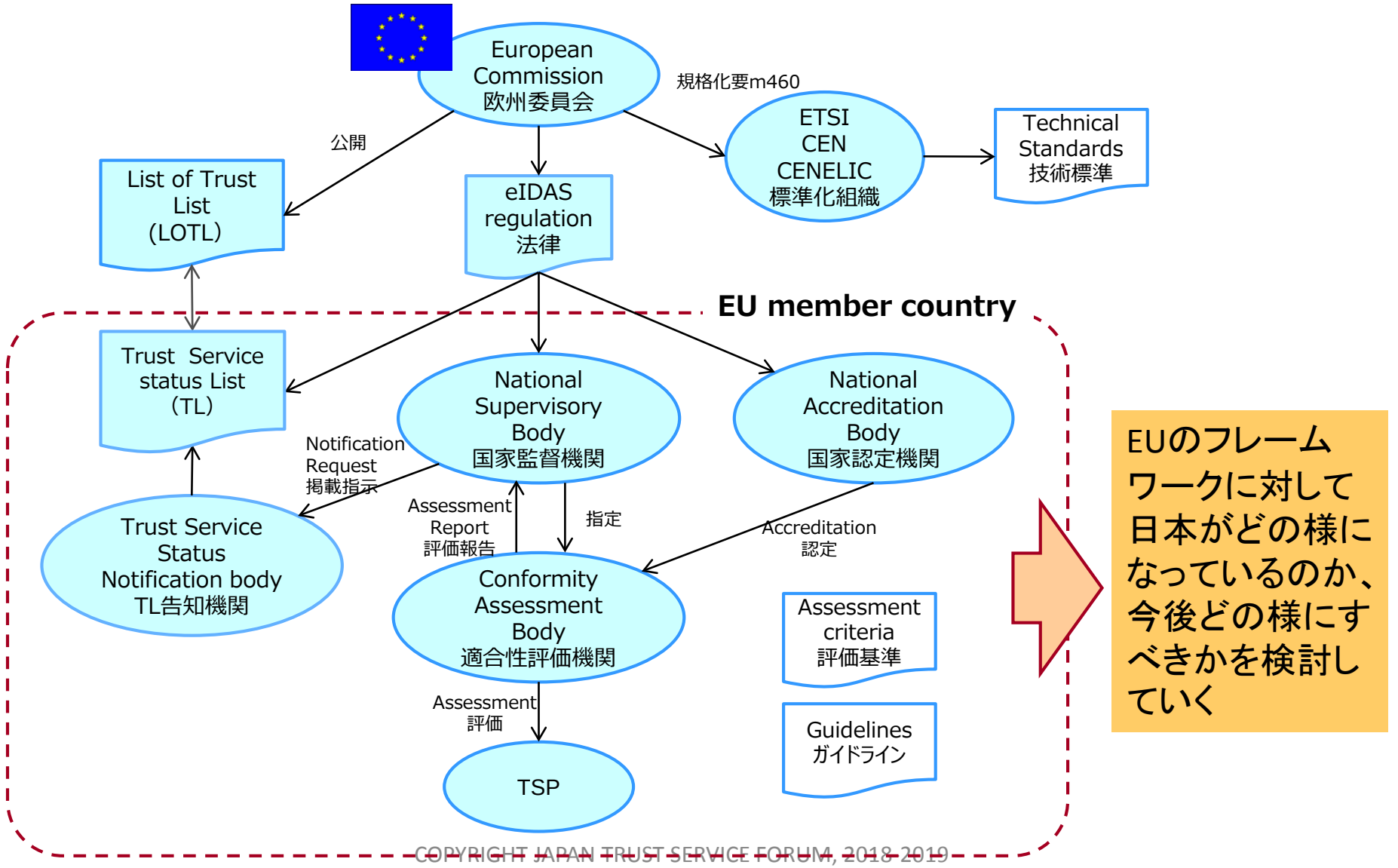
7th EU-Japan ICT Strategies workshop
18 April 2018 -Tokyo

第1ステージにおける比較項目（案）

- 枠組み（フレームワーク ）
- 対象とするトラストサービス
  - e-ID
  - 適格 ,または、非適格　電子証明書
  - 適格 ,または、先進　電子署名
  - 適格 ,または、非適格　e-シール
  - 適格 ,または、非適格　タイムスタンプ
  - 適格 ,または、非適格　リモート署名
- 制度（法律、認定制度など）
- 技術基準、運用基準、認定基準
- 主なユースケースで要求されるトラストサービス

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

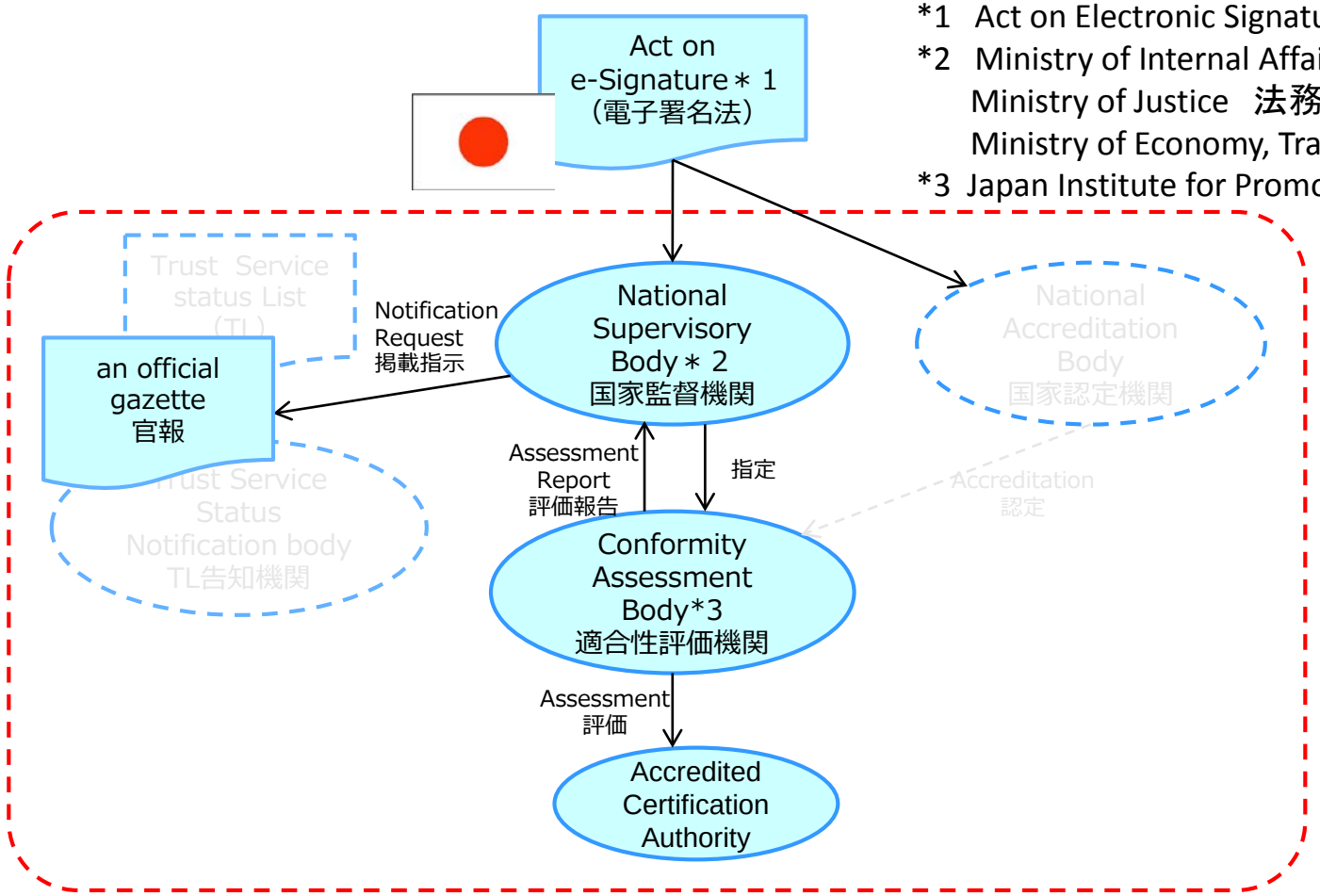
トラストサービスの法的確実性を保証するフレームワーク



EUのフレームワークに対して日本がどの様になっているのか、今後どの様にすべきかを検討していく

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

日本における認証局の認定フレームワーク

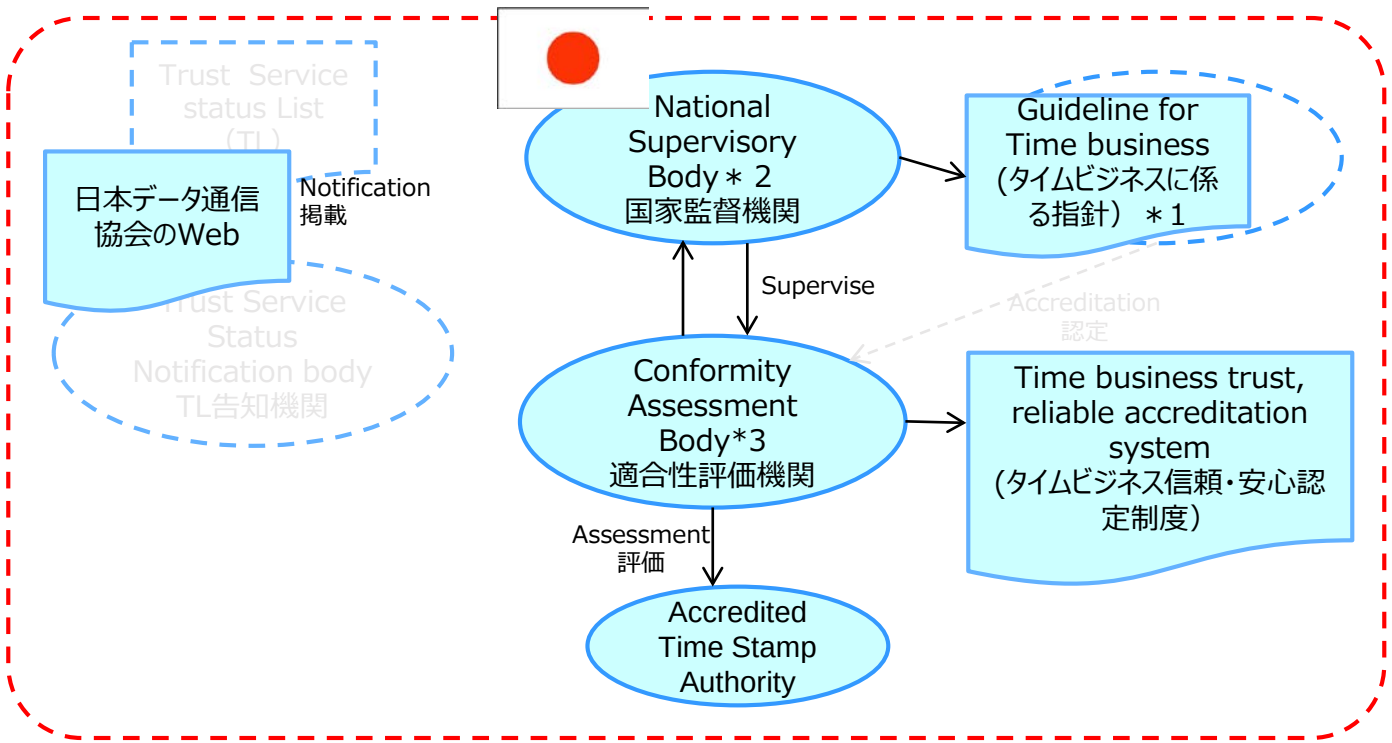


*1　Act on Electronic Signatures and Certification Business　電子署名法
*2　Ministry of Internal Affairs and Communications　総務省
Ministry of Justice　法務省
Ministry of Economy, Trade and Industry　経産省
*3 Japan Institute for Promotion of Digital Economy and Community（JIPDEC）

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

日本におけるタイムスタンプ局の認定フレームワーク

*1　Guideline for Time business　「タイムビジネスに係る指針」
*2　Ministry of Internal Affairs and Communications　総務省
*3　Japan Data Communications Association（JADAC）　一般財団法人日本データ通信協会



COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

トラストサービスの法的効力に関する日欧比較

トラストサービス	eIDASの法的効力 （適格サービス）	日本における法的効力
電子署名	手書きの署名と同等	電磁的記録の真正な成立の推定
eシール	データの完全性と起源と正確性の推定	未整備 *
タイムスタンプ	時刻の正確性とデータの完全性の推定	
eデリバリー	送受信者の識別、データの完全性、送受信時刻の正確性の推定	

* タイムスタンプの法的効力を規定する法律はないが、国税関係文書、医療文書、建築図面などについては、日本データ通信協会の認定を受けたタイムスタンプを用いることで電子形式での保存が認められている。また、これらの文書に署名が求められている場合は、高度電子署名を適用する必要がある。

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

電子署名に関する日欧比較（１）

	EU	日本
法律	eIDAS規則	電子署名及び認証業務に関する法律
CABの認定機関	加盟国の認定機関	主務大臣
認証機関	監督機関	主務大臣
適合性評価機関（CAB)	加盟国の認定を受けた適合性評価機関	主務大臣の指定を受けた調査機関
適合性評価機関の認定基準	● ISO 17065 製品、プロセス、サービスの認証機関に対する要求事項 ● EN 319 403 v2.2.2 一般的規定ISO/IEC17065に対し、TSP及びそのサービスを認証するCAB特有の追加要件	● 電子署名及び認証業務に関する法律（指定の基準） 第二十条
認証局（TSP)の監査基準	● ETSI EN 319 401 TSPに対するベースラインのポリシ要求事項 ● ETSI EN 319 411-1 証明書を発行するTSPに対するポリシー、及びセキュリティ要求事項Part1：一般要求事項 ● ETSI EN 319 411-2 Part2：適格証明書を発行するTSPへの要求事項 ● TR 119 411-4 v1.1.1 TSPの監査チェックリスト	● 電子署名及び認証業務に関する法律施行規則 ● 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針 ● 特定認証業務の認定に係る調査表

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

電子署名に関する日欧比較（２）

	EU	日本
署名フォーマット	● ETSI EN 319 122　CAdES ● ETSI EN 319 132　XAdES ● ETSI EN 319 142　PAdES ● ETSI EN 319 162　ASiC	なし
署名生成装置	ISO/IEC 15408	なし
証明書プロファイル	● EN 319 412-1 v1.1.1 概説と共通データ構造 ● EN 319 412-2 v2.1.1 自然人に対して発行する証明書 ● EN 319 412-3 v1.1.1 法人に対して発行する証明書 ● EN 319 412-4 v1.1.1 組織に対して発行するWebサイト証明書 ● EN 319 412-5 v2.2.1 適格証明書ステートメント	なし
適合性の検証手段	トラステッドリスト ● TS 119 612	官報

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

タイムスタンプに関する日欧比較

	EU	日本
法律	eIDAS規則	確定日付の法的効力は無い。国税関係書類等の一部文書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。 ● 電子帳簿保存法施行規則
CABの認定機関	加盟国の認定機関	ない
認証機関	監督機関	日本データ通信協会
適合性評価機関（CAB)	加盟国の認定を受けた適合性評価機関	日本データ通信協会
適合性評価機関の認定基準	（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	● 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	● タイムビジネスに係る指針 ● タイムビジネス審査基準 ● JIS X 5094
タイムスタンプフォーマット	●RFC 3161　●ISO/IEC 18014-1　●ISO/IEC 18014-2	
		● JIS X 5063-1
タイムスタンプトークンのプロファイル	●RFC 3161　●ISO/IEC 18014-2	
	● 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	トラステッドリスト	日本データ通信協会のWeb

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

日本の電子署名法

特定認証業務

署名法　第2条1項の電子署名

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
二　当該情報について改変が行われていないかどうかを確認することができるものであること。

署名法　第2条3項の特定認証業務

電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

署名法　第3条　電磁的記録の真正な成立の推定

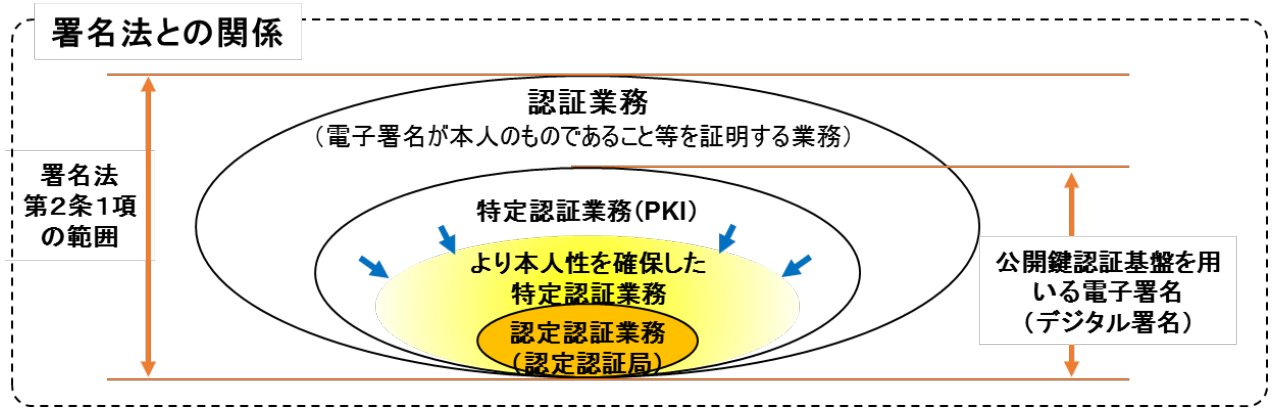
本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

認定認証業務

署名法　第4条　特定認証業務の認定

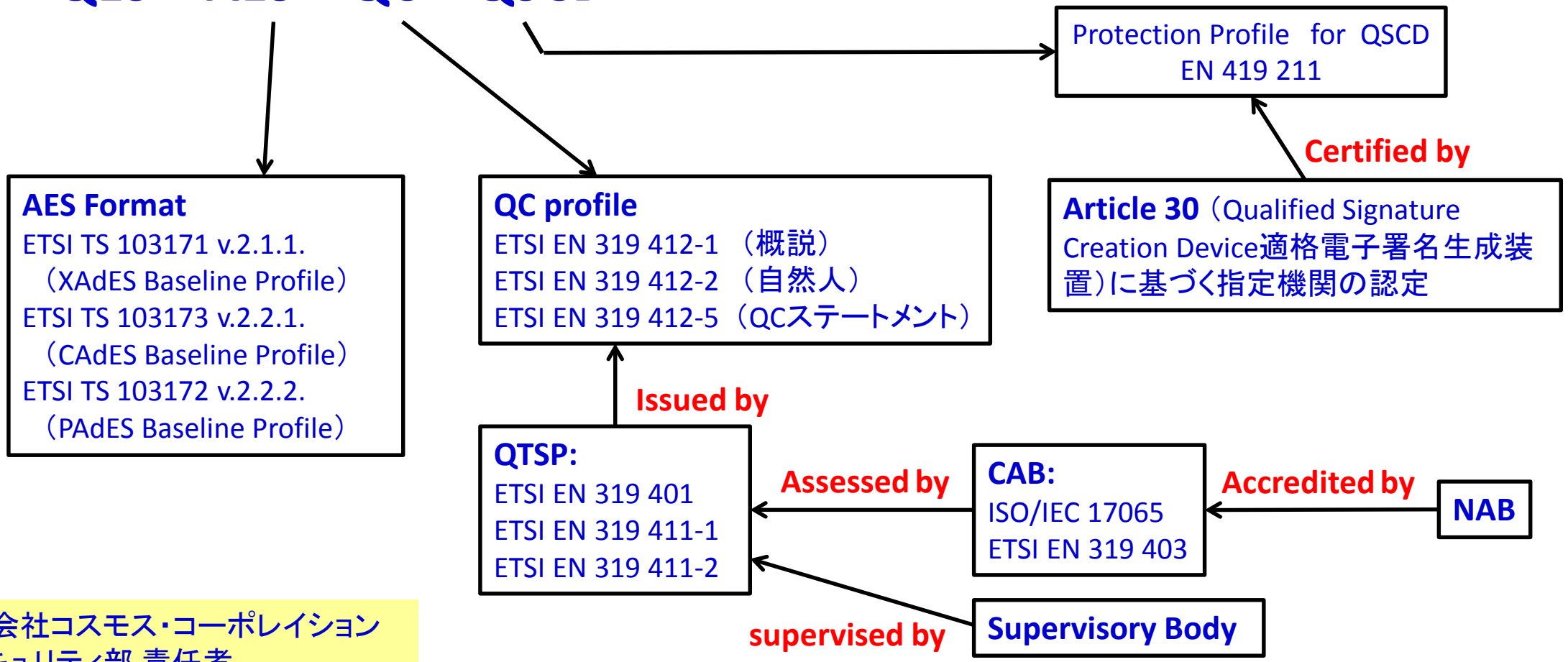
特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

署名法との関係



EUの適格電子署名（QES）

- **QES = AES + QC + QSCD**



株式会社コスモス・コーポレイション
ITセキュリティ部 責任者
濱口 総志　氏　資料より

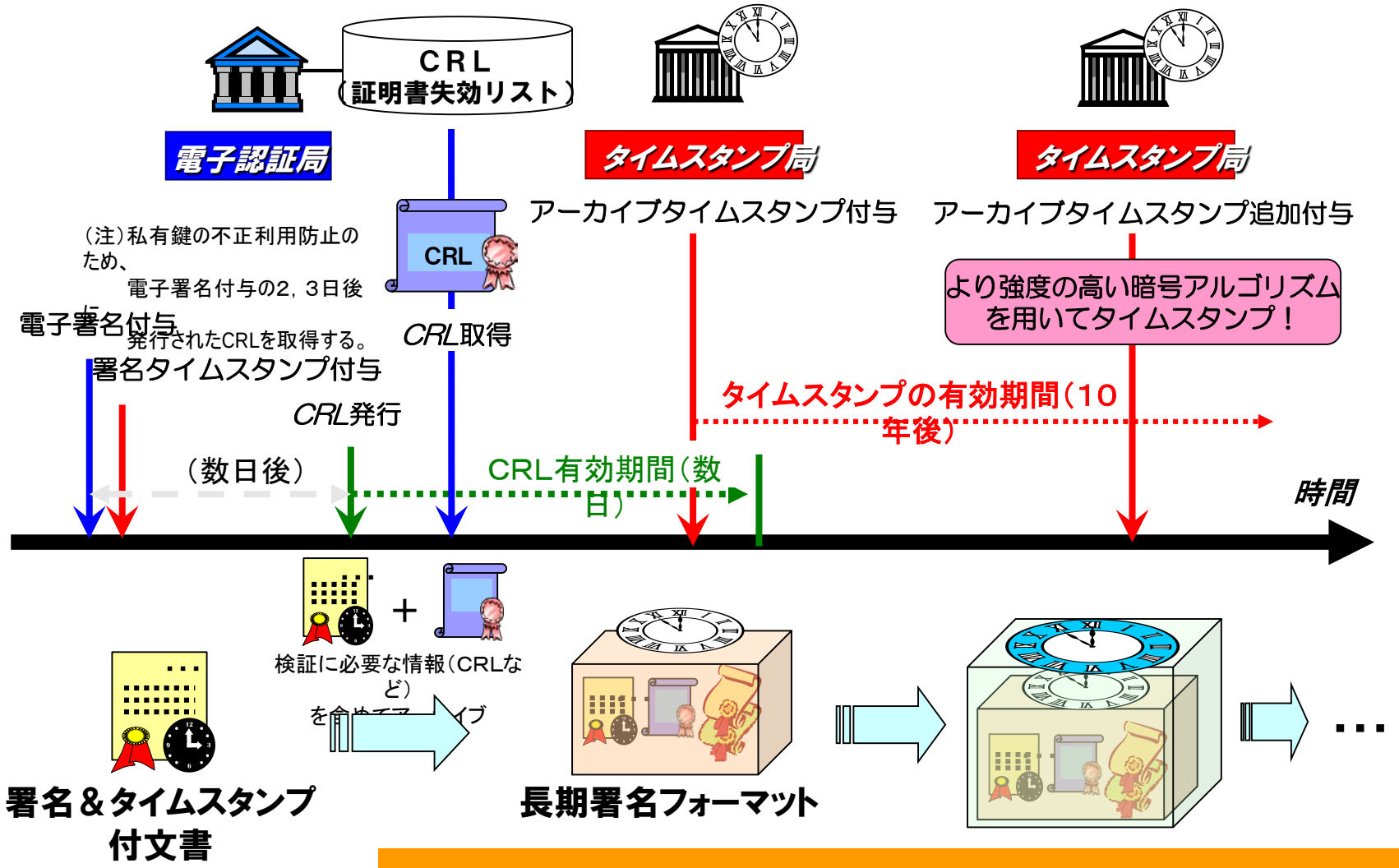
COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

用語集

QES: Qualified Electronic Signature, 適格電子署名
AES: Advanced Electronic Signature, 先進電子署名
QC: Qualified Certificate, 適格証明書
QSCD: Qualified Signature Creation Device, 適格電子署名生成装置(e.g. ICカード等)
QTSP: Qualified Trust Service Provider （i.e. 認証局）
CAB: Conformity Assessment Body, 適合性調査機関
NAB: National Accreditation Body, 認定機関

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

AES（長期署名）生成フロー



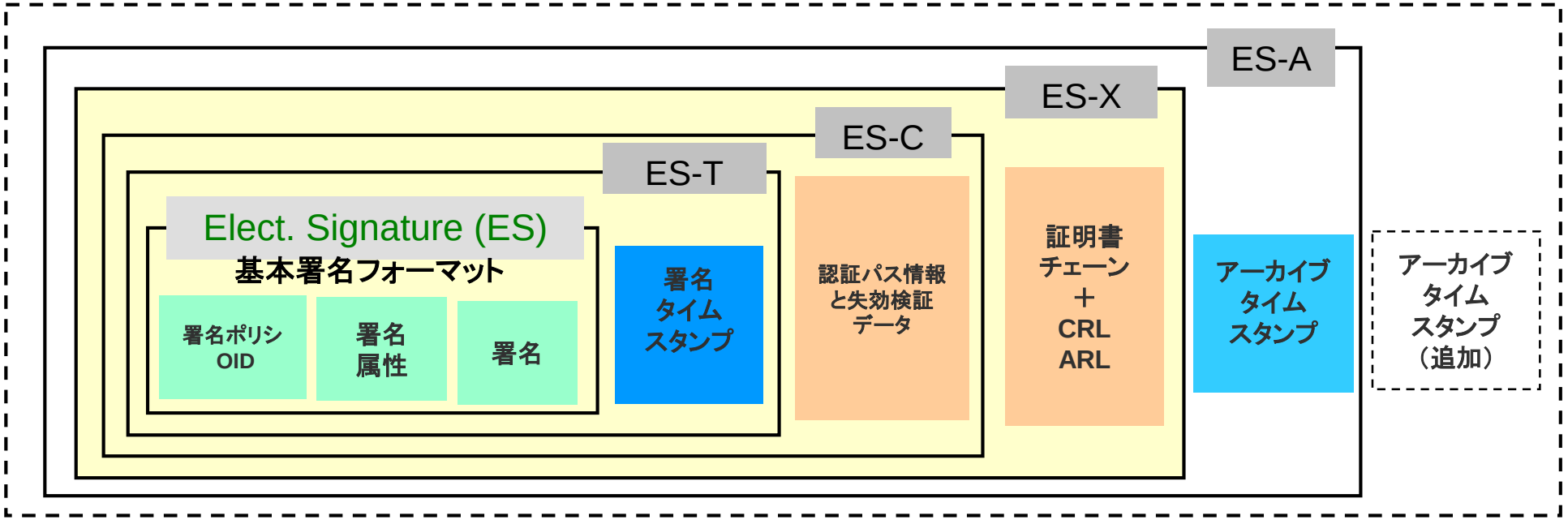
外殻のタイムスタンプが破られない限り、内部の真正性は保たれる

AESフォーマットイメージ(ES-A)

AESフォーマットにより、電子署名の検証を証明書の有効期限を越えて継続する事が可能となり、長期に渡り、署名文書の有効性を確認可能とします。

【ポイント】
・署名タイムスタンプにより署名時刻の証拠性を確保
・失効情報や証明書を署名データ内に格納し、証明書検証の継続性を確保
・アーカイブタイムスタンプの暗号アルゴリズムにより、署名データや失効情報等を保護。
（署名アルゴリズムの脆弱化による署名偽造を防ぐ）

RFC 3126（Electronic Signature Formats for long term electronic signatures）



ES-T: Electronic Signature with Time stamp

ES-C: Electronic Signature with Complete validation data

ES-X: Electronic Signature eXtended

ES-A: Electronic Signature Archive

適合性評価機関の要求事項

	EU	日本
適合性評価機関の認定基準	● ISO 17065 製品、プロセス、サービスの認証機関に対する要求事項 ● EN 319 403 v2.2.2 一般的規定ISO/IEC17065に対し、TSP及びそのサービスを認証するCAB特有の追加要件	● 電子署名及び認証業務に関する法律 （指定の基準） 第二十条

これを例にして少し詳しく見てみると

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

日本の適合性評価機関の要求事項

日 電子署名及び認証業務に関する法律 （指定の基準） 第二十条)	EU ETSI EN 319 403 V2.2.2 ISO/IEC 17065 （JIS Q 17065）
一　調査の業務を適確かつ円滑に実施するに足りる経理的基礎及び技術的能力を有すること。	4.3 Liability and financing 6 Resource requirements
二　法人にあっては、その役員又は法人の種類に応じて主務省令で定める構成員の構成が調査の公正な実施に支障を及ぼすおそれがないものであること。	5 Structural requirements
三　調査の業務以外の業務を行っている場合には、その業務を行うことによって調査が不公正になるおそれがないものであること。	4.2 Management of impartiality Annex A (informative): Auditors' code of conduct
四　その指定をすることによって申請に係る調査の適確かつ円滑な実施を阻害することとならないこと。	なし

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

EUの適合性評価機関の要求事項

ETSI EN 319 403ではISO/IEC 17065がベースとなっており、CABの要件を詳細に定義できている

1	Scope
2	References
2.1	Normative references
2.2	Informative references
3	Definitions and abbreviations
3.1	Definitions
3.2	Abbreviations
4	General requirements
4.1	Legal and contractual matters
4.2	Management of impartiality
4.3	Liability and financing
4.4	Non-discriminatory conditions
4.5	Confidentiality
4.6	Publicly available information
5	Structural requirements
5.1	Organizational structure and top management
5.2	Mechanism for safeguarding impartiality
6	Resource requirements
6.1	Conformity Assessment Body personnel
6.2	Resources for evaluation
7	Process requirements
7.1	General requirements
7.2	Application
7.3	Application Review
7.4	Audit
7.5	Review
7.6	Certification decision
7.7	Certification documentation
7.8	Directory of certified products
7.9	Surveillance
7.10	Changes affecting certification
7.11	Termination, reduction, suspension or withdrawal of certification
7.12	Records
7.13	Complaints and appeals
8	Management system requirements
8.1	Options
8.2	General management system documentation
8.3	Control of documents
8.4	Control of records
8.5	Management review
8.6	Internal audits
8.7	Corrective actions
8.8	Preventive actions
Annex A (informative):	Auditors' code of conduct
Annex B (informative):	Bibliography
History	

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

日・EU　トラストサービスの制度比較：まとめ

EUの特色

- タイムスタンプの法的位置づけが明確
- 適合性評価機関の要件を示す標準規定を用意

  →日本は要件項目が少ないが、JIS Q 17065　をベースにCABの特色を追記すれば補完可能
- 標準規定に基づく適合性評価機関の認定スキームが確立されている
- ポリシー要件や証明書プロファイルが標準規格として用意され、法律がそれを参照する構造となっており、複数のトラストサービスの法的位置づけが建てつけやすい
- TSPをトラステッドリストに公開するスキームが確立され信頼できるTSPが明確でシステムで自動確認可能

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019

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

COPYRIGHT JAPAN TRUST SERVICE FORUM, 2018-2019