日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA標準化部会主催セミナー
「デジタル社会に不可欠なサイバーセキュリティ標準化動向」
巧妙化、高度化、多様化するサイバー攻撃に備えて

電子署名WGにおける サイバーセキュリティ標準化との関わり

2021年1月15日

電子署名WGリーダー　宮崎一哉

自己紹介

宮崎 一哉

三菱電機株式会社 生産技術本部

【主な所属団体】

JNSA（日本ネットワークセキュリティ協会）電子署名WGリーダ

JT2A（日本トラストテクノロジー協議会）運営委員

ARMA（Association of Records Managers and Administrators）**International** 東京支部　理事

TSF（トラストサービス推進フォーラム）副会長・幹事・トラストサービスの在り方検討WG主査・調査研究WG副主査・タイムスタンプ認証制度検討SWG主査

総務省タイムスタンプ認定制度に関する検討会構成員

【主な著書】

概説　e-文書法（NTT出版）共著

電子文書保存のしくみと実務―e-文書法への実践的対応（中央経済社）共著

電子文書保存のしくみと実務―記録管理の基本と標準化（中央経済社）共著

帳簿保存・スキャナ保存　完全ガイド（税務研究会出版）監修

電子署名WG

2013年4月活動開始

【活動目的】

電子署名関連技術の相互運用性確保のための調査、検討、標準仕様提案、及び電子署名普及啓発。

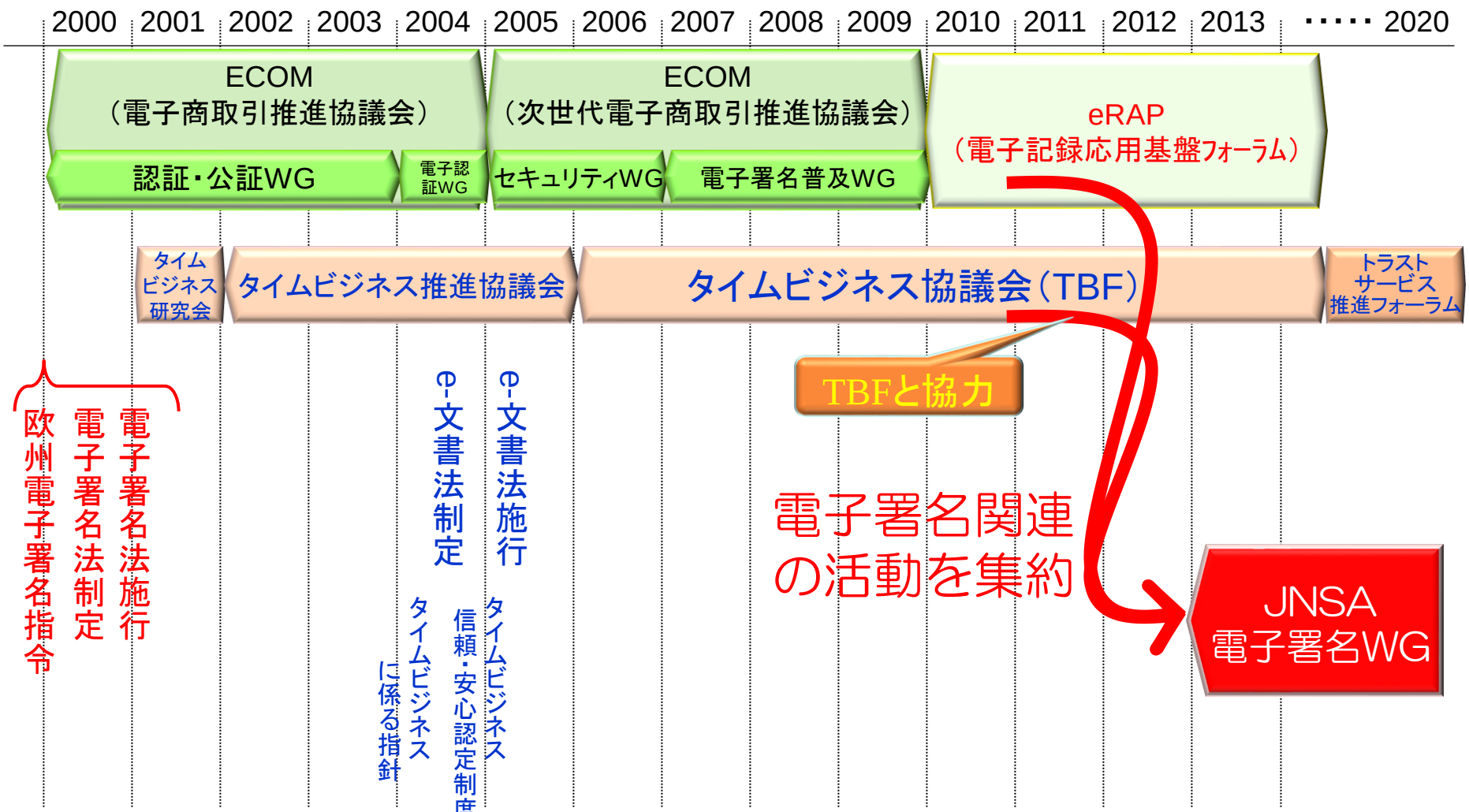
【年間活動予定】

- 標準仕様案等検討会（年30回程度）
- ISO/TC154国内審議委員会の運営支援、ISO/SC34のリエゾン、JAHISへの技術協力、欧州電気通信標準化機構/電子署名基盤技術委員会（ETSI/ESI）会議参加
- PKI Day等講演会の開催支援

【予定成果物】

・長期署名プロファイルの制改定
・署名検証プロセスに関する標準仕様作成

電子署名WG設立経緯



電子署名WG

2013年4月活動開始

【活動目的】

電子署名関連技術の相互運用性確保のための調査、検討、標準仕様提案、及び電子署名普及啓発。

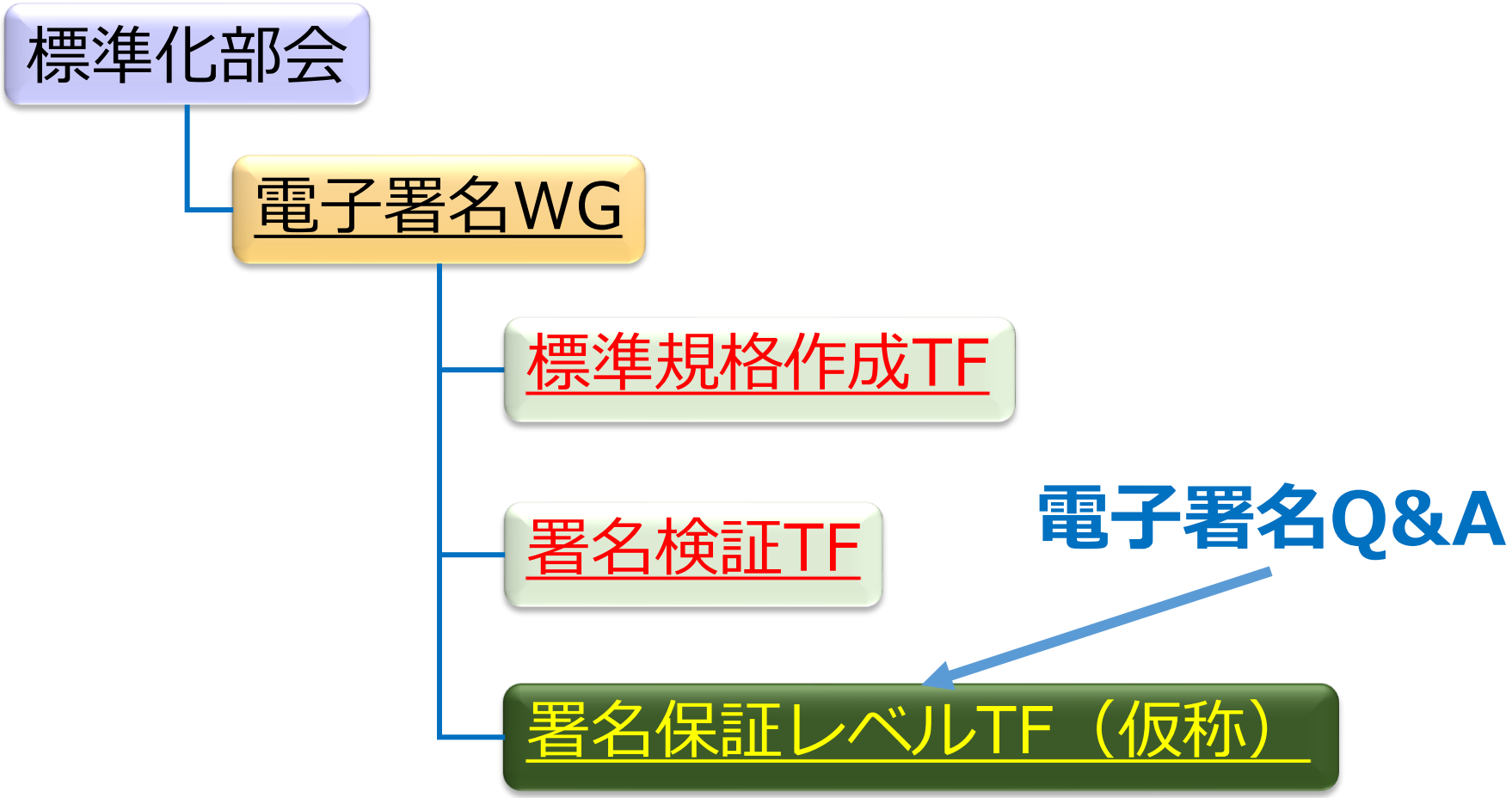
【年間活動予定】

- 標準仕様案等検討会（年30回程度）
- ISO/TC154国内審議委員会の運営支援、ISO/SC34のリエゾン、JAHISへの技術協力、欧州電気通信標準化機構/電子署名基盤技術委員会（ETSI/ESI）会議参加
- PKI Day等講演会の開催支援

【予定成果物】

・長期署名プロファイルの制改定
・署名検証プロセスに関する標準仕様作成

電子署名WG構成



※今後設置予定

標準規格作成TF–現在の活動

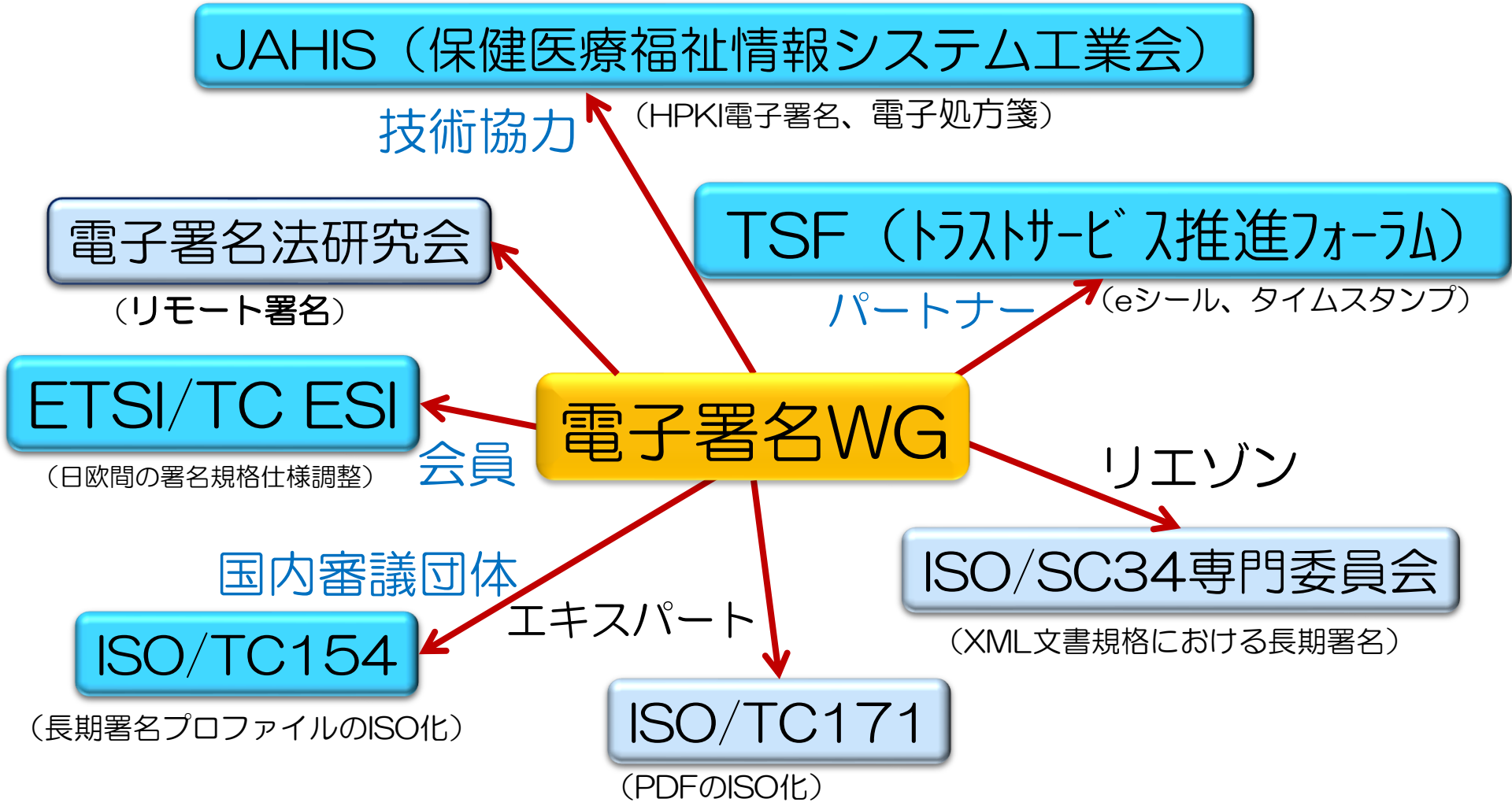
- ISO/TC154国内審議団体をJIPDECより引継ぎ
- XML形式の長期署名プロファイル改定
  ISO 14533-2
  Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 2: profiles for XML Advanced Electronic Signatures (XAdES)
  - 2019/10/10：新規プロジェクト承認
  - 2020/05/02：CD→DIS
  - 2020/11/05：DIS投票

- JAHIS(一般社団法人保健医療福祉情報システム工業会)技術協力
  『電子処方箋実装ガイド』
  電子処方箋におけるXML署名規格作成支援

担当する主な標準規格

- JIS X 5092（CMS利用電子署名(CAdES)の長期署名プロファイル）
- JIS X 5093（XML署名利用電子署名(XAdES)の長期署名プロファイル）
- JIS X 5094（UTCトレーサビリティ保証のためのTAAの技術要件）
- ISO 14533-1（Long term signature profiles for CMS Advanced Electronic Signatures (CAdESプロファイル)）
- ISO 14533-2（Long term signature profiles for XML Advanced Electronic Signatures (XAdESプロファイル)）
- ISO 14533-3（Long term signature profiles for PDF Advanced Electronic Signatures (PAdESプロファイル)）
- ISO 17090-4（Digital Signatures for healthcare documents）
- ISO 18014-4（Traceability of time sources）

他団体との関係



署名検証TF

- 2013年発行の第1版「電子署名検証ガイドライン」の改定
- 2020年度中に第2版完成予定
  ⇒ その後、全面改定を経て将来的には標準規格化を目指す

日本版・検証ガイドラインの改版のポイントと方針案

① 日本版の構成を維持しつつ、最新化
- ◆誤記修正、未定部分の追記
- ◆用語・参照規約の最新化

② ガイドラインの分かり易さ、使い易さの向上
- ◆内容の分かり易さ、使い勝手向上
- ◆リモート署名など、関連技術記載（付録）

③ レポート等について、欧州版との整合
- ◆ETSI版パート1、2との対応確認

署名検証規格の必要性

署名検証
ソフト

OK

- 実装者にとって、実装方法がわかる。
- 調達者・利用者にとって、検証範囲がわかる。

⇒信頼できる署名検証ソフト

・署名
……
証明書
・有効期間
・失効
・パス
・トラストアンカ
・検証時刻
……

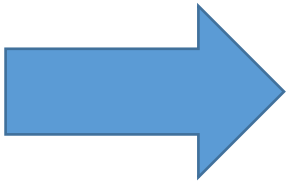
たとえば某ソフトは
SigningCertificate属性を
全くチェックしていない。

何が、無効の原因
だったのか？

結果を信用できない

背景

- EU　eIDASにおけるeシールの規定
- 同じくEUにおけるリモート署名の普及
- いわゆる『立会人型署名』の台頭と三省Q&A
- 電子署名とデジタル署名



電子署名Q&A

電子署名法解釈アドホックグループ：2020/7/1活動開始　9/16公開

【電子署名Q&A】

電子署名Q&A

2020年9月16日 第1版

NPO法人 JNSA 日本ネットワークセキュリティ協会 電子署名ワーキンググループ

引用のご連絡及び内容に関するお問い合わせは、
「各種公開資料の引用及び、内容に関するお問合せ」をご確認下さい
※ご質問には回答しておりませんのでご了承ください。

2001年の電子署名法施行以来、コロナ禍をきっかけとする在宅勤務の機会増大によって再び電子署名に注目が集まっています。電子署名法主務三省(総務省、経済産業省、法務省)からこの（2020年）7月と9月の二回にわたり電子契約サービスに関するQ&Aが公開され、その中でも電子署名に関する見解が示されましたが、電子署名に馴染みのない方にはややハードルが高い内容となっています。このような状況を踏まえ、少しでも多くの方に電子署名に対するご理解を深めていただけますよう、電子署名WGでは「電子署名Q&A」を作成し、公開することといたしました。

目次

51項目

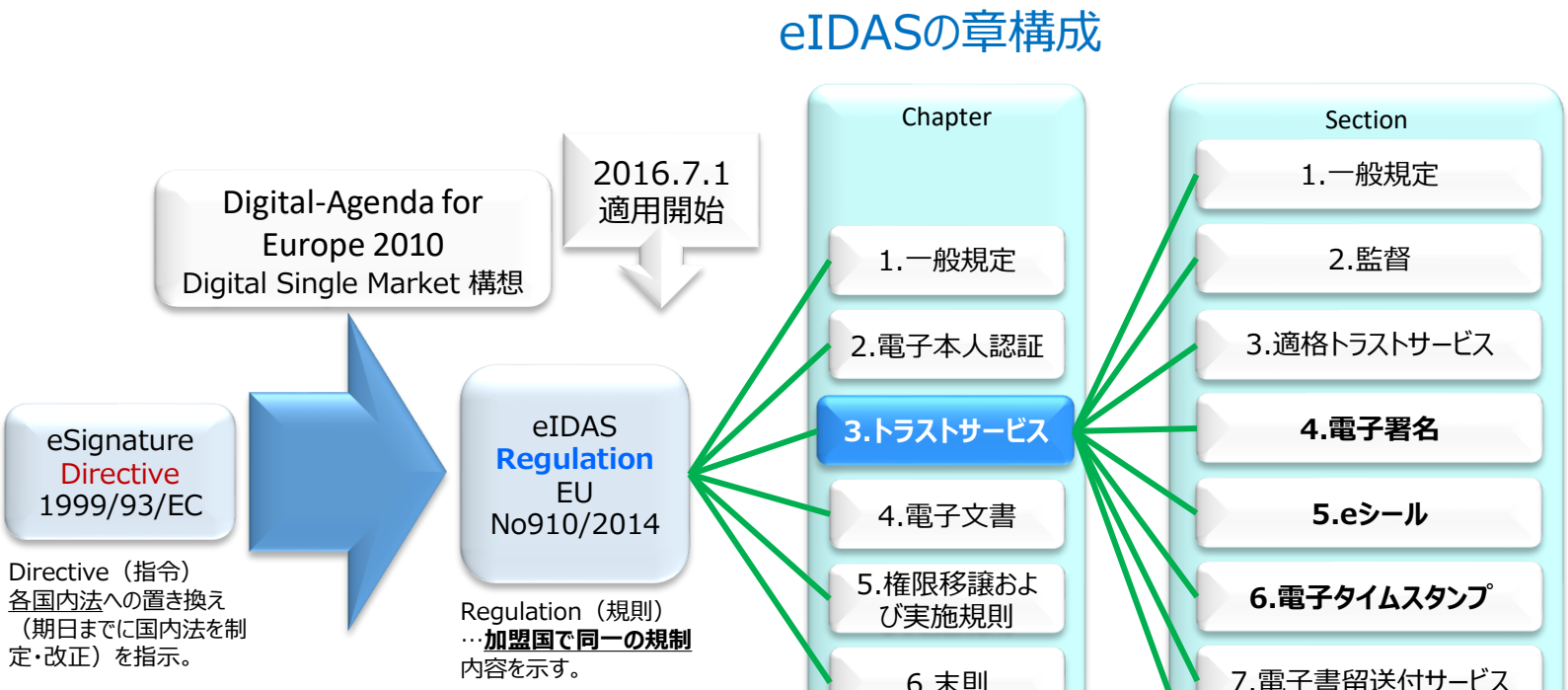
https://www.jnsa.org/result/e-signature/e-signature-qa/index.html

電子署名とeシール

EUのeIDASで定義

- 電子署名（electronic signature）：
  主体者（生成者）：自然人
  主体者本人の意思と非改ざんを証明
  紙文書における手書き署名や記名押印に相当
- eシール（electronic seal）：
  主体者（生成者）：法人（組織、装置）
  発出元と非改ざんを証明
  紙文書における印章で押された紋章に相当
  （日本の会社印のようなもの）
  ⇒日本の電子署名法ではeシールは想定外
  ⇒日本でも制度化に向けて検討開始
  総務省：組織が発行するデータの信頼性を確保する制度に関する検討会

eIDAS



eIDAS規則とは、EUにおいて、電子取引を安全にし、デジタル単一市場に備える目的から、「電子認証手段（eID）」と「トラストサービス」について法的枠組みを整備し、旧電子署名指令の適用範囲を拡大しその実効性を強化したもの。

電子署名とeシール

EUのeIDASで定義

- 電子署名（electronic signature）：
  主体者（生成者）：自然人

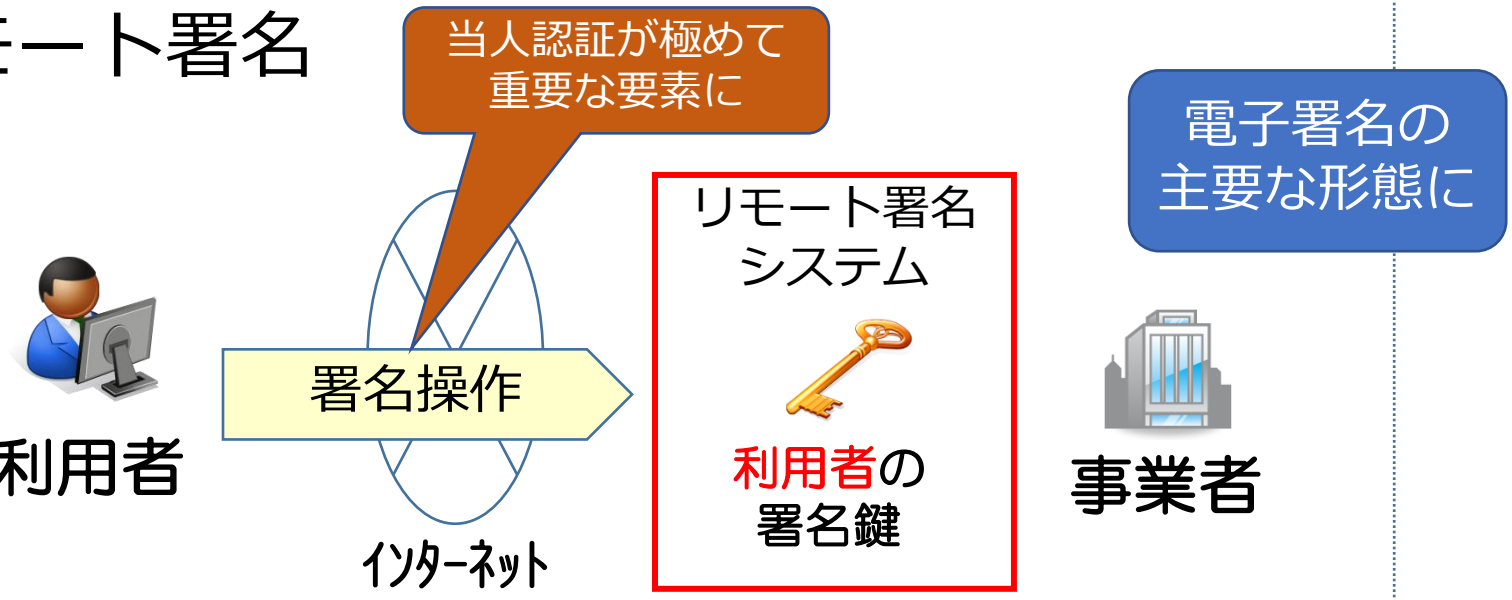
認証：その場で本人性を確認
電子署名：係争時等に責任の内容と追及先を確認

  主体者（生成者）：法人（組織、装置）
  発出元と非改ざんを証明
  紙文書における印章で押された紋章に相当
  （日本の会社印のようなもの）

⇒日本の電子署名法ではeシールは想定外
⇒日本でも制度化に向けて検討開始
  総務省：組織が発行するデータの信頼性を確保する制度に関する検討会

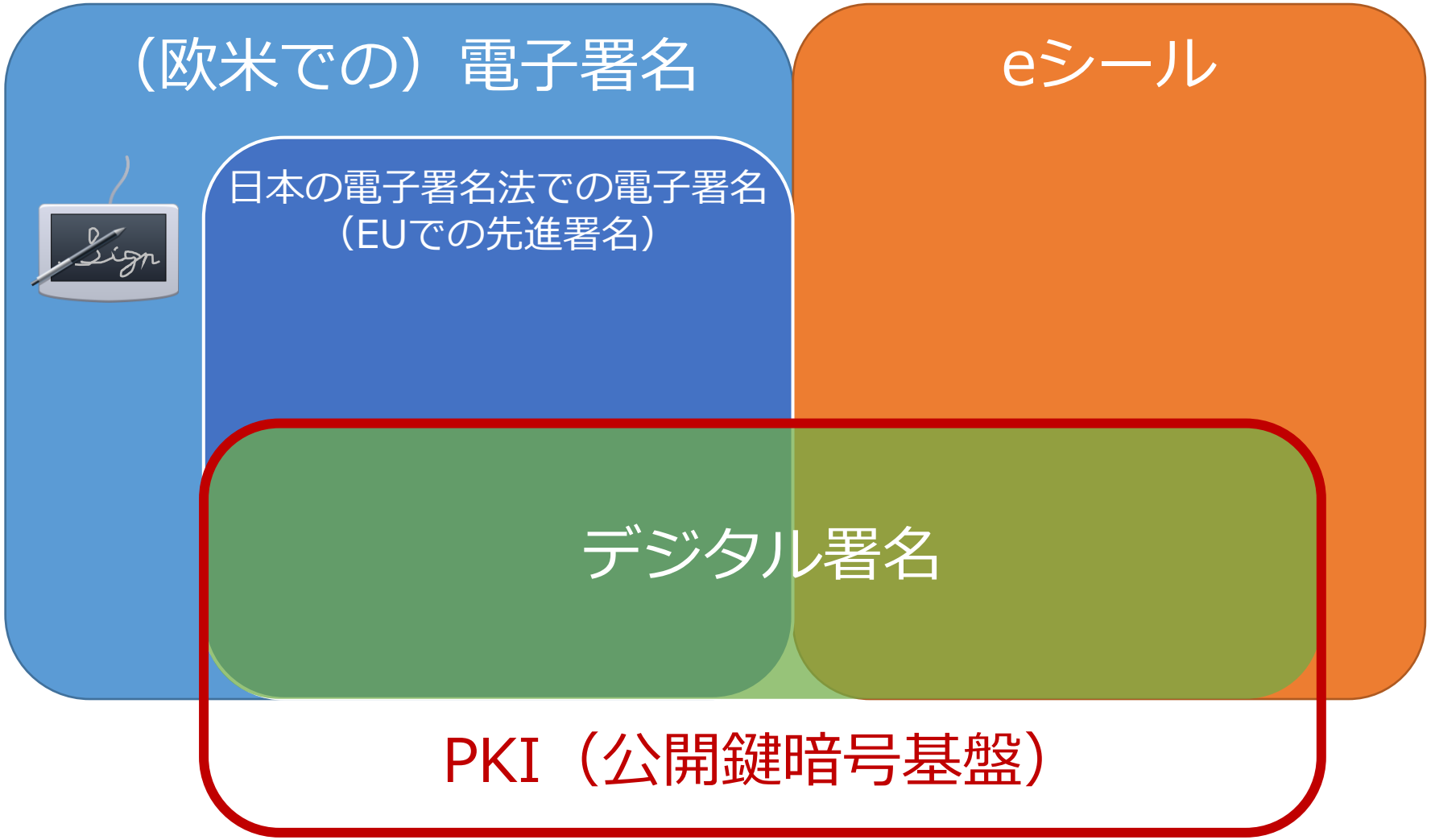
新たな電子署名①-リモート署名

- リモート署名

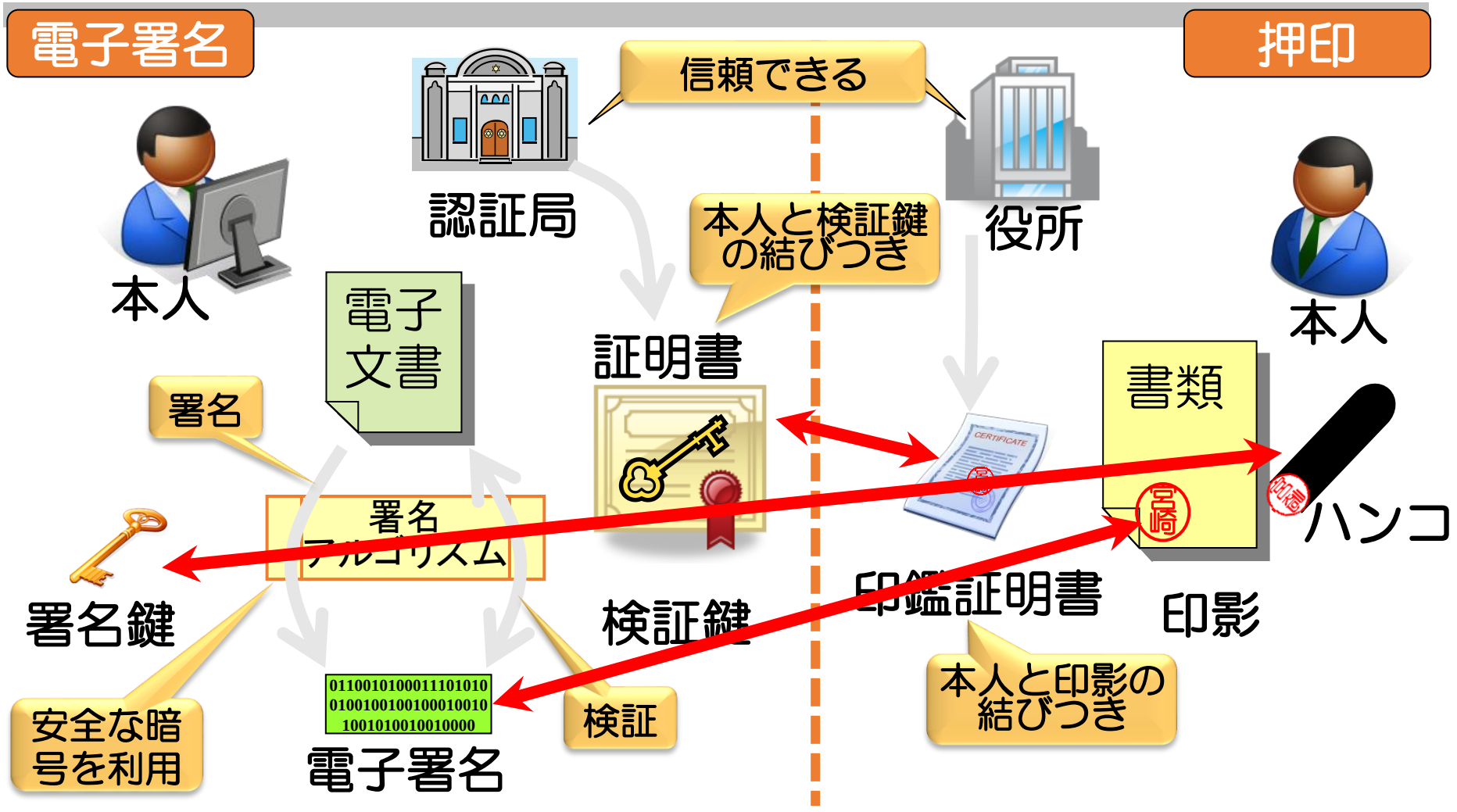


- 従来のローカル署名

電子署名-eシール-デジタル署名の関係



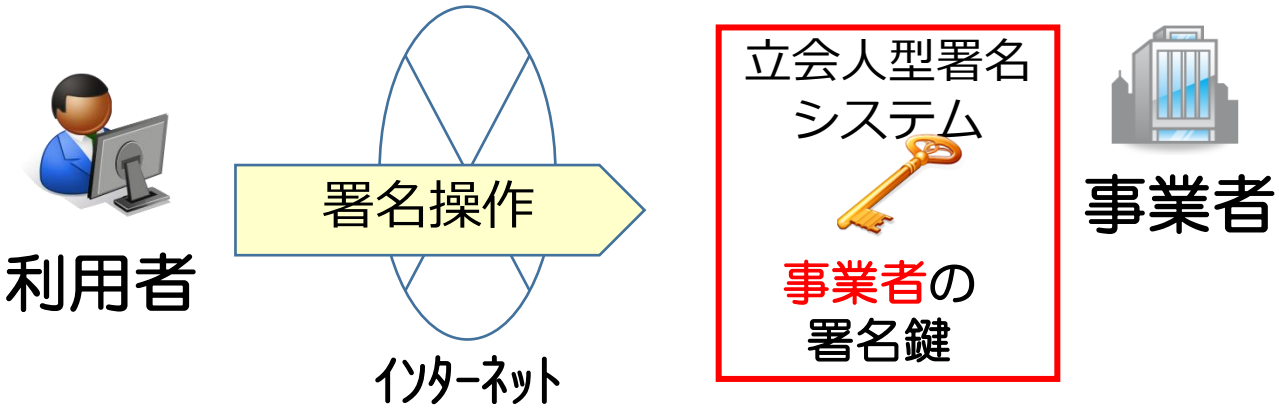
電子署名とは−従来の説明



PKI（公開鍵暗号基盤）に基づくデジタル署名を前提

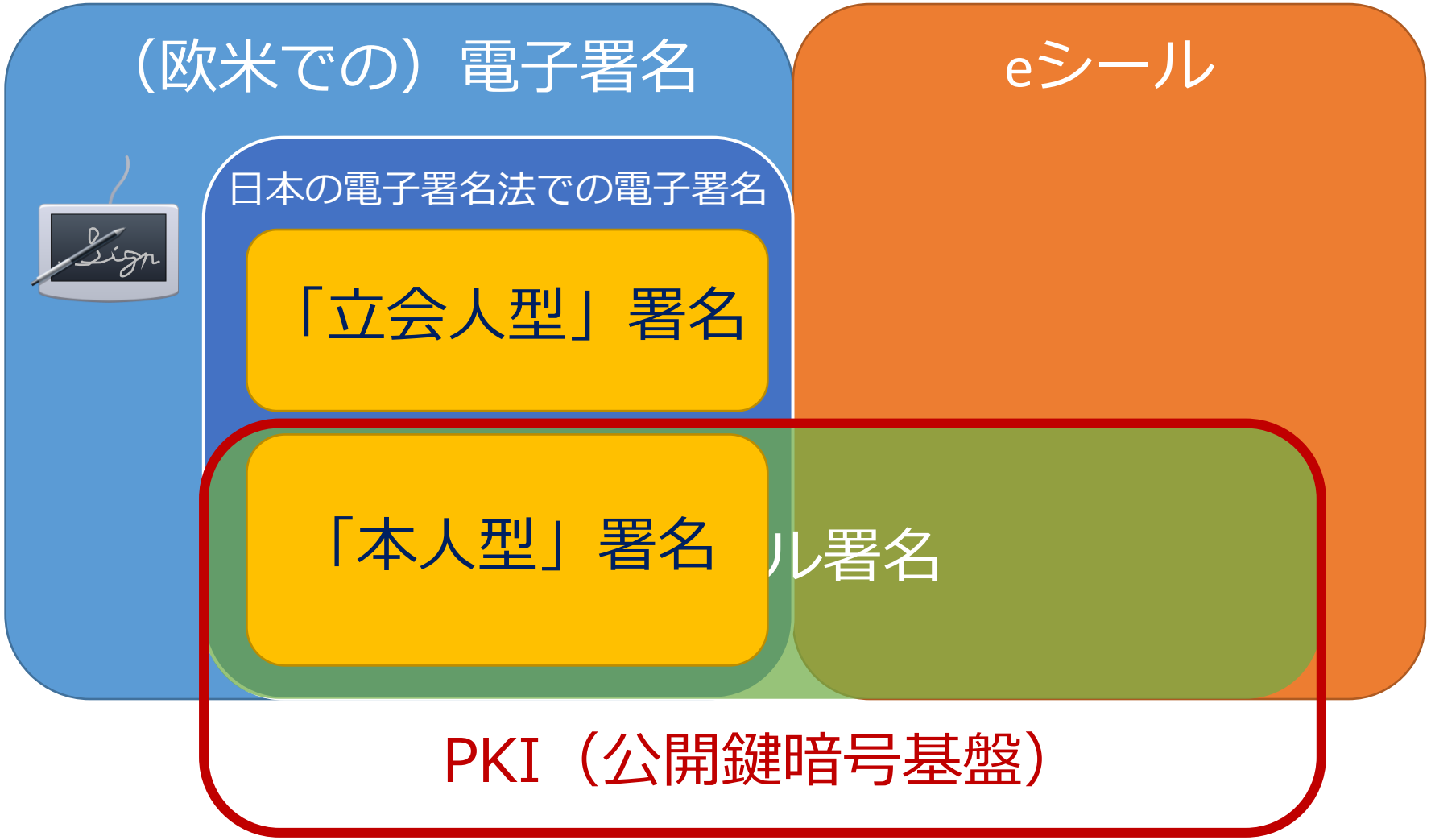
新たな電子署名②-立会人型署名

- 事業者署名型電子署名、第三者型署名、クラウド型電子署名などとも呼ばれる
- 利用者が署名操作を行ったことを事業者が証明



- 電子署名法主務三省（総務省・法務省・経済産業省）の2つのQ&A
  - 利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するＱ＆Ａ（2020年7月17日）
  - 利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するＱ＆Ａ（電子署名法第３条関係）（2020年9月4日）

電子署名-eシール相関図



三省Q&Aにおける「立会人型署名」の解釈

- 法第2条関連のQ&A：電子署名と見なされる要件

  『技術的・機能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されていると認められる場合』

- 法第3条関連のQ&A：電子文書の真正な成立の推定を得られる（署名者の意思を反映していると仮定できる）要件

  『①利用者とサービス提供事業者の間で行われるプロセス及び②①における利用者の行為を受けてサービス提供事業者内部で行われるプロセスのいずれにおいても十分な水準の固有性が満たされている必要がある』

十分な水準の固有性

①利用者とサービス提供事業者の間で行われるプロセス

⇒利用者がセキュアな認証を経なければ措置ができないこと

②①における利用者の行為を受けて事業者内部で行われるプロセス

⇒事業者が暗号化等を行う措置において、十分な暗号強度と利用者ごとの個別性を担保すること

特に②については、事業者の内部の処理において、電子文書が利用者の作成に係るものであること（個別性）を示すための措置として十分な水準の固有性が満たされていることが求められる、ということで、

②-1署名対象文書と利用者（利用者情報）とをセキュアに関連付けるために

i)事業者が両者を結合して十分な強度を持った暗号技術を用いて署名する

②-2システム処理が正に当該利用者によって操作されたことを担保するために

ii)正しく適切なログが記録でき、それが改ざんや削除ができない仕様となっている

iii)管理者等が利用者に成り代わって操作できない仕様となっている

等が要件となる。

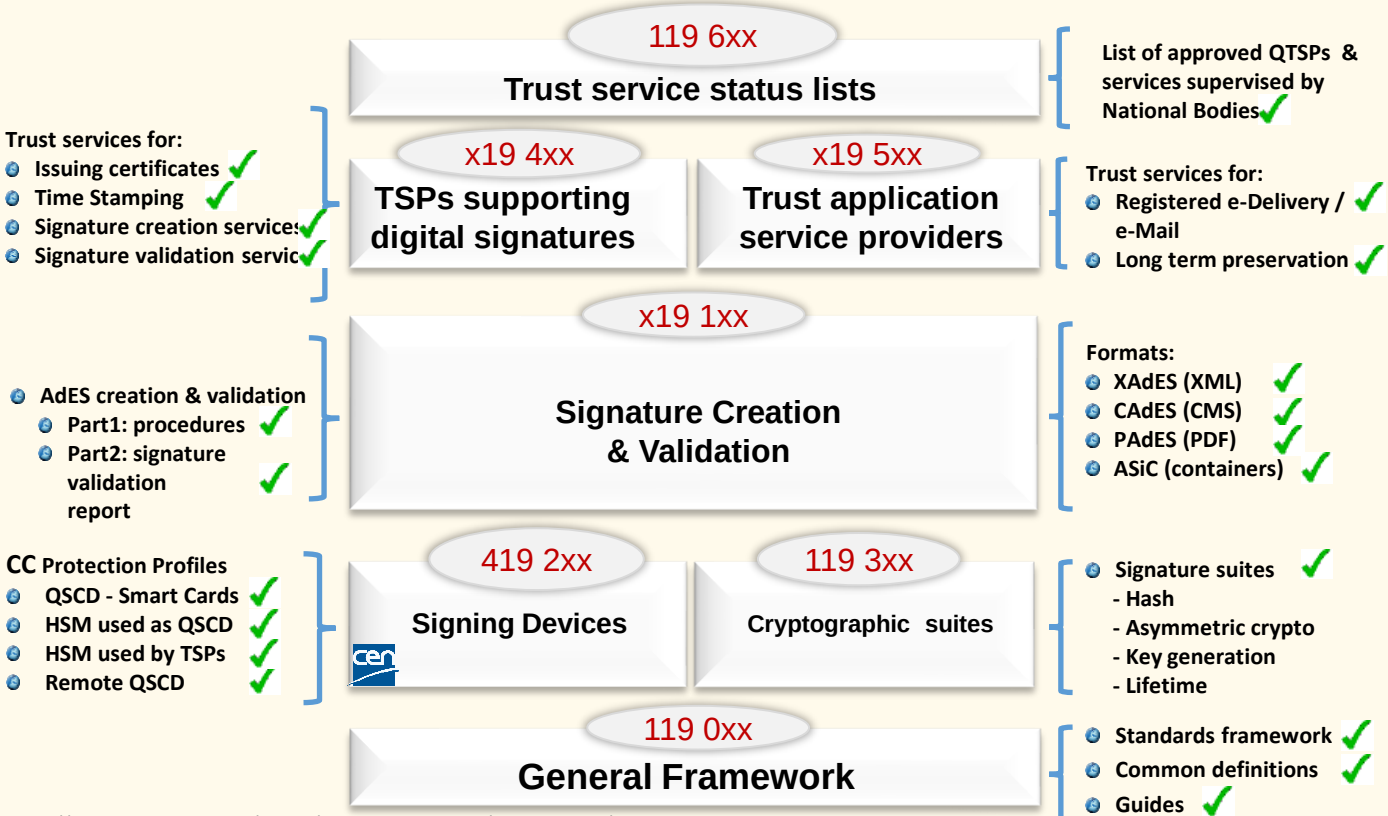
実装できているのか？　どの程度の水準なのか？

電子署名方式の比較

	本人型署名	立会人型署名
標準化	**技術・運用・ﾎﾟﾘｼｰ等が国際標準化されている。**	**なし。**事業者が付与する署名ﾌｫｰﾏｯﾄに標準規格が利用されている場合あり。
ポータビリティ	当事者の署名付き文書全体が検証可能な標準準拠ﾃﾞｰﾀとして自由に交換可能。	当事者の署名である根拠を含めた検証可能なﾃﾞｰﾀ全体を抽出し交換することは困難。特定ﾍﾞﾝﾀﾞｰにﾛｯｸされる。
永続性	関連事業者（認証局やﾀｲﾑｽﾀﾝﾌﾟ局）が廃業後も継続して保存や検証が可能。	事業者廃業後の証拠性（証明力）維持は困難。
国際通用性	標準化が十分進んでおり、各国で法制度も整備されており、日EUでの国際相互承認のための活動も始まっている。	Adobe Sign、DocuSign等、日米欧で実績あり。国際的に有効性が認められる可能性がある。
法的裏付け	あり。電子署名と見なされる要件、真性な成立の推定の要件が明確。	Q&Aの要件を満たせば電子署名法への適合性が認められるが、具体要件は未定義。
認定・認証制度	**特定認証業務の認定制度あり。**	**なし。**
検証可能性（まさにその本人がそのﾃﾞｰﾀに署名したことの検証）	標準処理で利用者や第三者による検証が可能。	利用者や第三者による検証が困難。 事業者に依拠。
署名対象と本人性の関係付け（結合力）	暗号的に不可分。	ｱｸｾｽﾛｸﾞで関係付け。

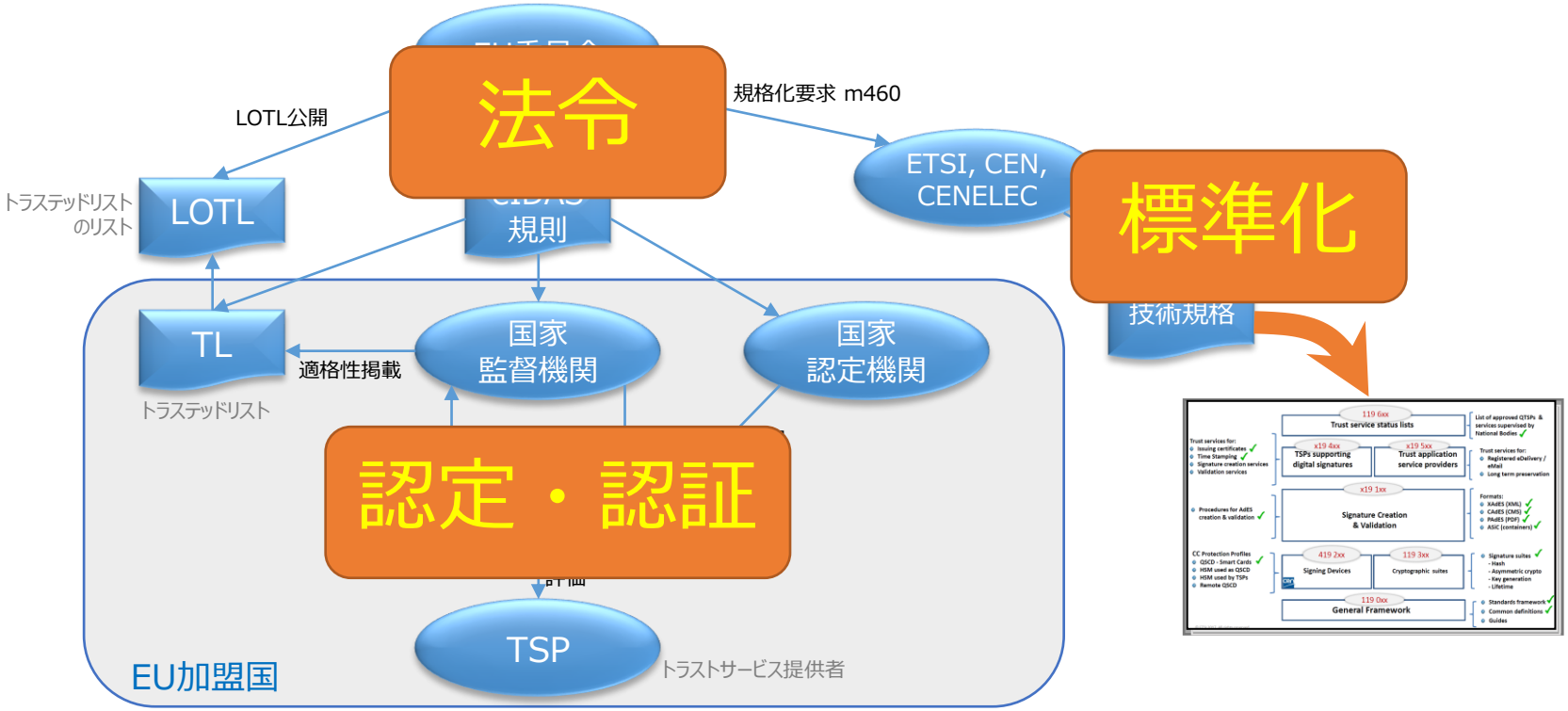
電子署名関連標準（EUを例に）

本人型電子署名は標準規格が体系的に用意される。



電子署名を支える体制（EUを例に）

本人型電子署名は法制度の体制が整備されている。



結論：三省Q&Aより

『電子契約サービスにおける利用者の身元確認の有無、水準及び方法やなりすまし等の防御レベルは様々であることから、各サービスの利用に当たっては、当該各サービスを利用して締結する契約等の重要性の程度や金額といった性質や、利用者間で必要とする身元確認レベルに応じて、適切なサービスを慎重に選択することが適当と考えられる。』

電子署名WG：今後の活動

- 電子署名に関するQ&Aのメンテナンス

- 電子署名保証レベルの検討を開始予定
  - 本人性保証レベル、真正性保証レベル、運用保証レベル、、、（まだ素案の段階です）

⇒各種方式やサービスを客観的に評価できるように。

署名保証レベルTF（仮称）

- 興味がおありの方はJNSAまで。

ご清聴ありがとうございました。