日本のサイバーセキュリティを「連携」「学び」「創造」

JNSA PKI & TRUST Days online 2021
「トラスト社会におけるトラスト」

DX社会における電子署名の役割

2021年4月16日

電子署名WGリーダー　宮崎一哉

目次

- DXとトラスト
- 電子署名、eシール、デジタル署名
- 「トラスト」と検証
- 「トラスト」の源泉
- 課題、電子署名WGの関連の活動

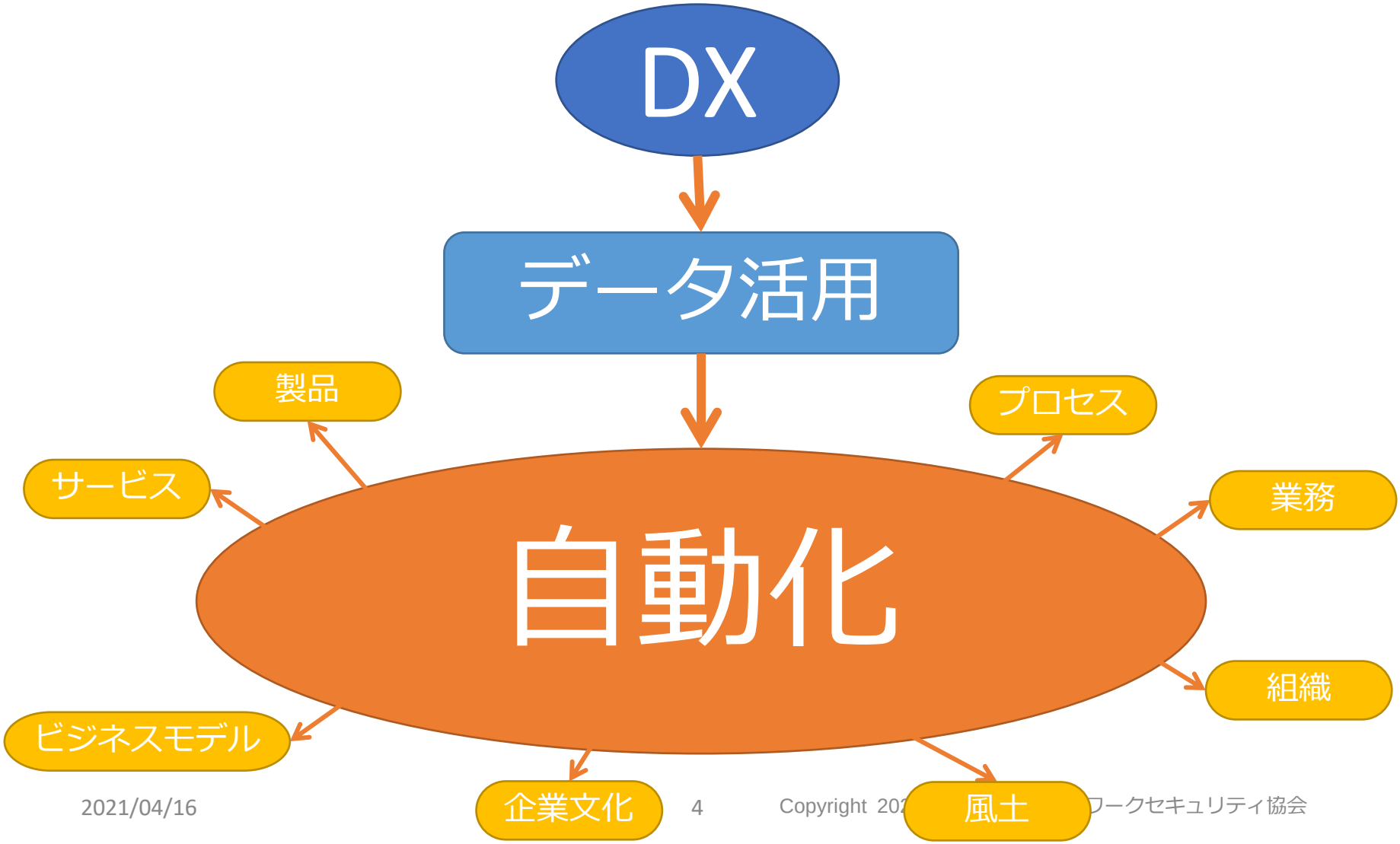
DXとトラスト

DXとは

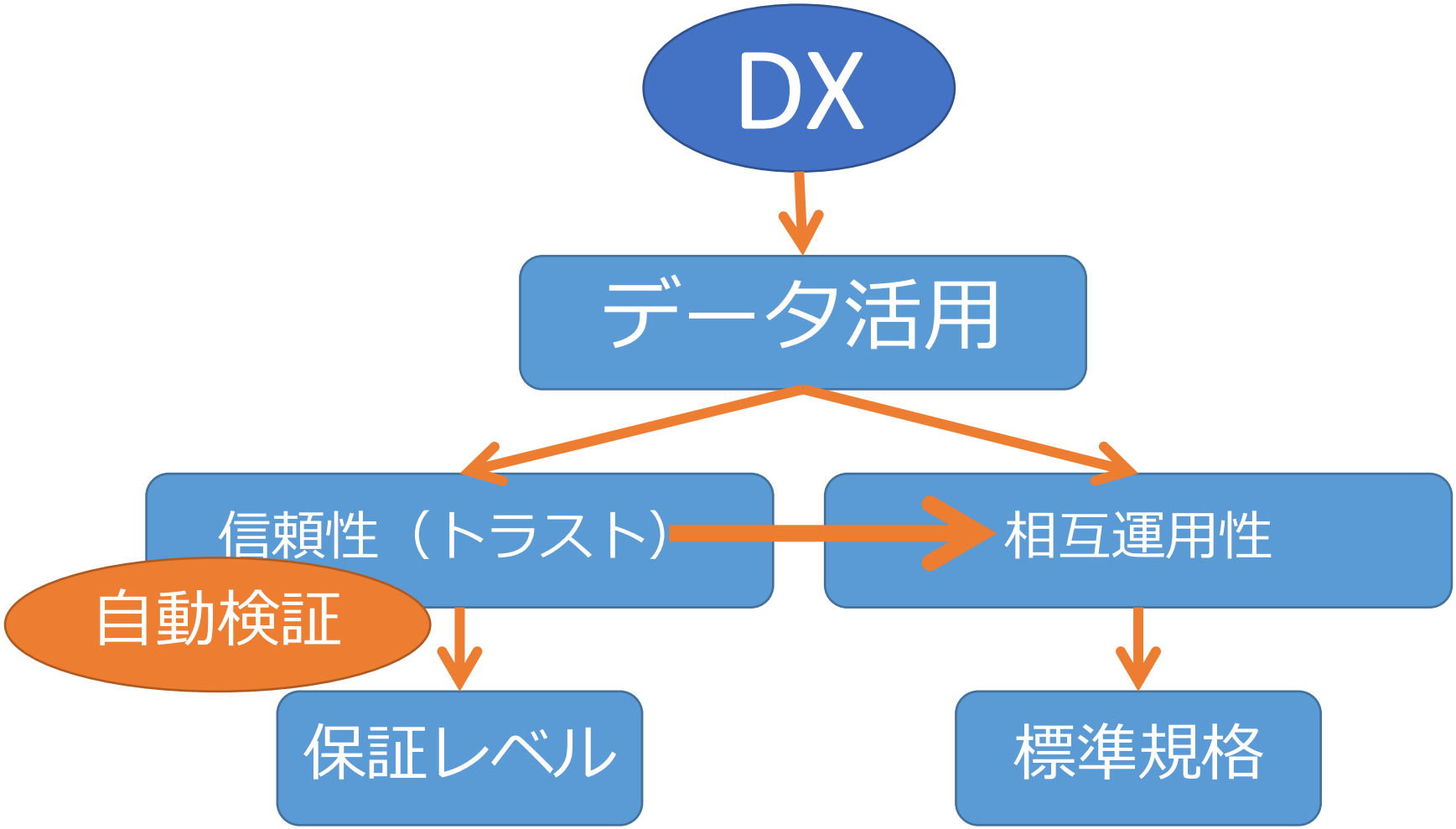
“企業がビジネス環境の激しい変化に対応し、**データ**とデジタル技術**を活用**して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、**競争上の優位性を確立**すること。”

出典：経済産業省「デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン）Ver1.0 (2018/12/12)」
（https://www.meti.go.jp/press/2018/12/20181212004/20181212004-1.pdf）

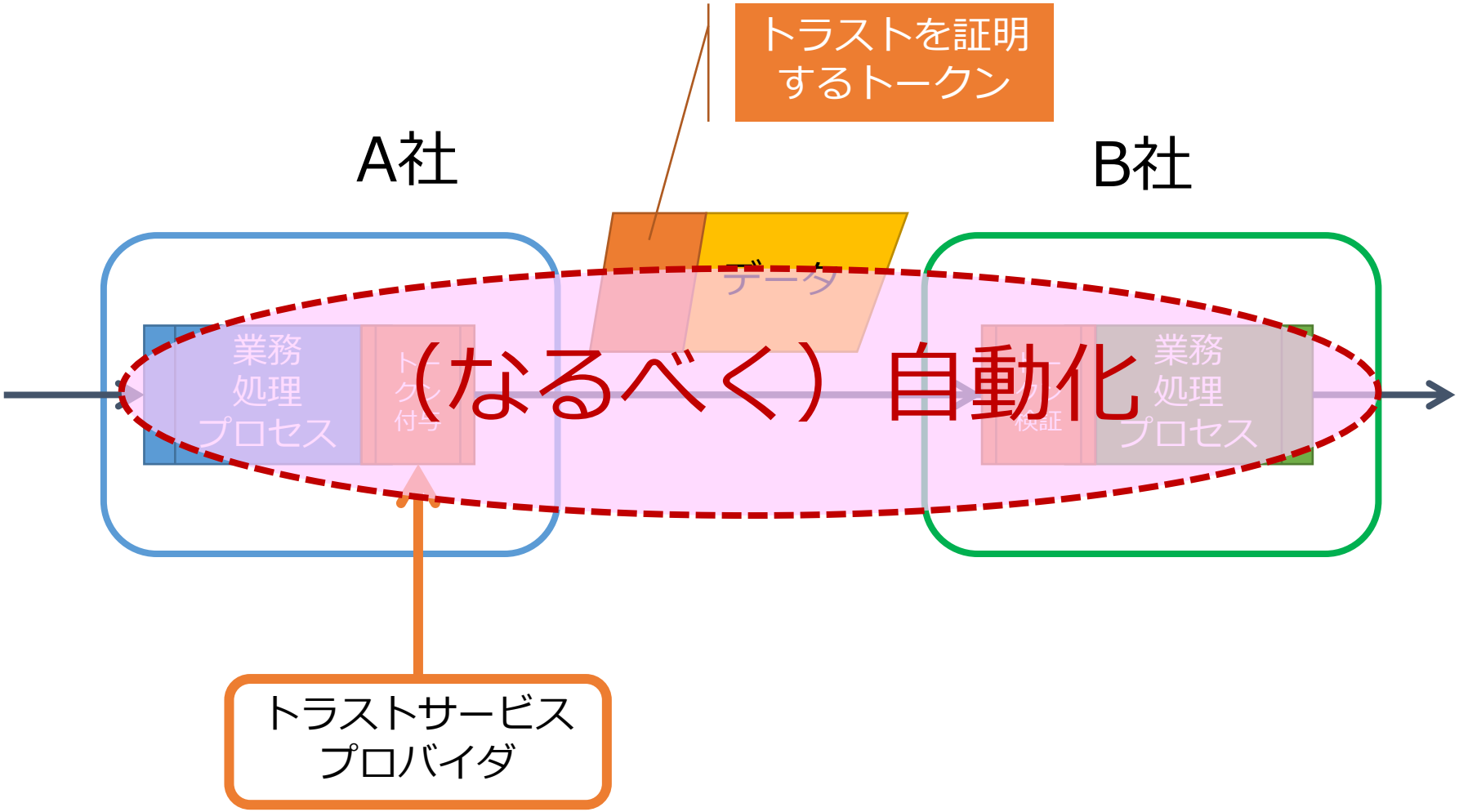
DXで重要なのは自動化



自動化のための保証レベル、標準規格



トラストの付与と検証



データにトラストを与えるサービス

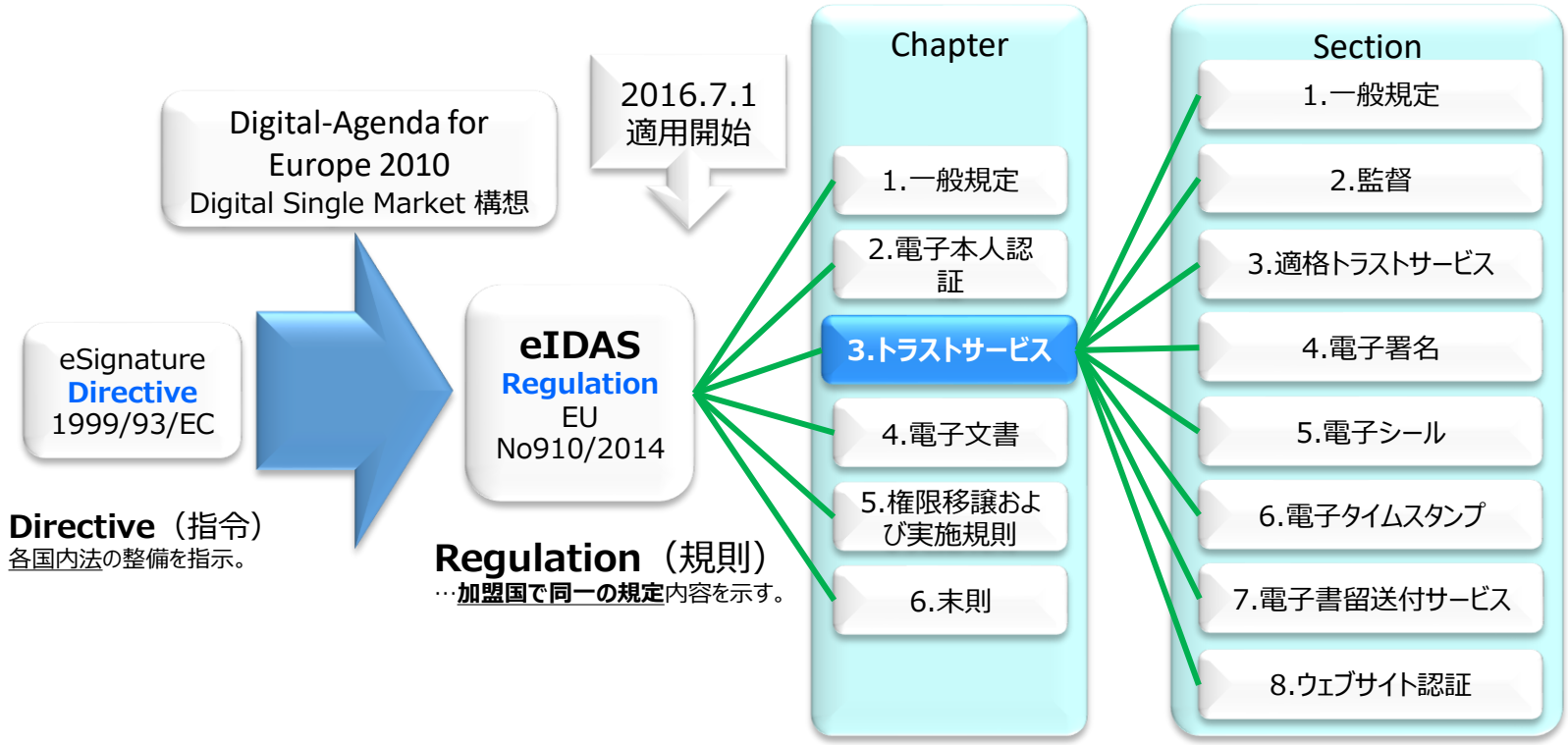
トラストサービス

- EU：eIDAS規則で規定
- 総務省：トラストサービス検討ワーキンググループで定義

eIDAS規則

eIDAS規則とは、ＥＵ加盟国間の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、「電子本人認証手段（eID）」と「トラストサービス（eTS）」について法的枠組みを整備し、旧指令の適用範囲を拡大しその実効性を強化したもの。

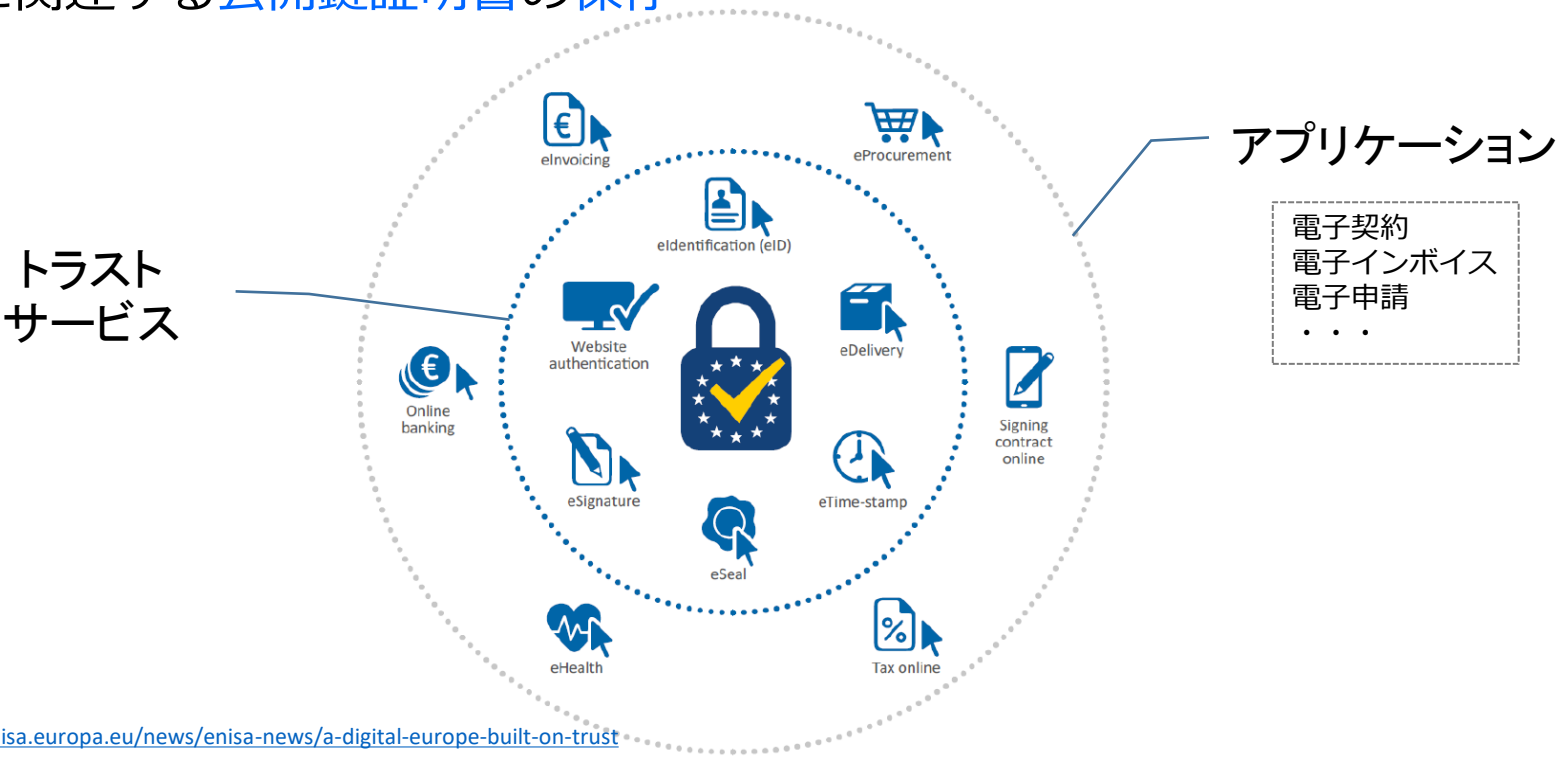
eIDASの構成



eIDASにおけるトラストサービスの定義

1. 電子署名、e-シール、タイムスタンプ、電子登録配布サービス（e
デ
生
2. We
3. 電子
に関連する公開鍵証明書の保存

基本的にすべてPKI（公開鍵基盤）ベース



https://www.enisa.europa.eu/news/enisa-news/a-digital-europe-built-on-trust

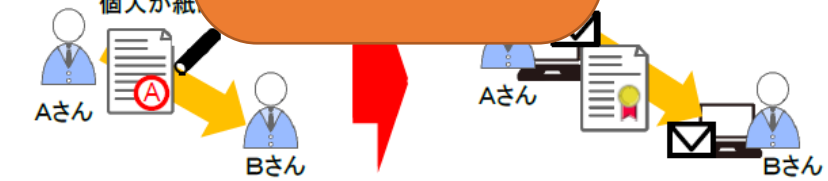
総務省：トラストサービス検討ワーキンググループ

JNSA

・電子署名（電子文書の作成者を示す目的で行われる暗号化等の措置であって、電子署名が付されて以降、当該電子文書が改変されていないことを確認可能とする仕組み）

国の制度(電子署名)　業務を主務大臣が認定

従来　正当性を確認）



電子署名

・eシール（電子文書の発信元の組織を示す目的で行われる暗号化等の措置であり、電子署名が付されて以降、当該文書が改ざんされていないことを確認可能とする仕組みであって、電子文書の発信元が個人ではなく組織であるもの）

制度無し　従来　正当性を確認）

eシール

・タイムスタンプ（電子データがある時刻に存在し、その時刻以降に当該データが改ざんされていないことを証明する仕組み）

民間の認定スキーム有り　一定の基準を満たす事業者を（一財）日本データ通信協会が認定

従来　性の保証）

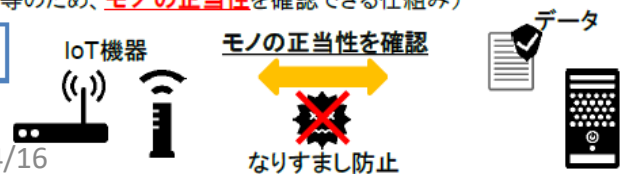
タイムスタンプ

・eデリバリー（送信・受信の正当性や送受信されるデータの完全性の確保を実現する仕組み）　制度無し

eデリバリー

・モノの正当性の認証（IoT時代における各種センサーから送信されるデータのなりすまし防止等のため、モノの正当性を確認できる仕組み）

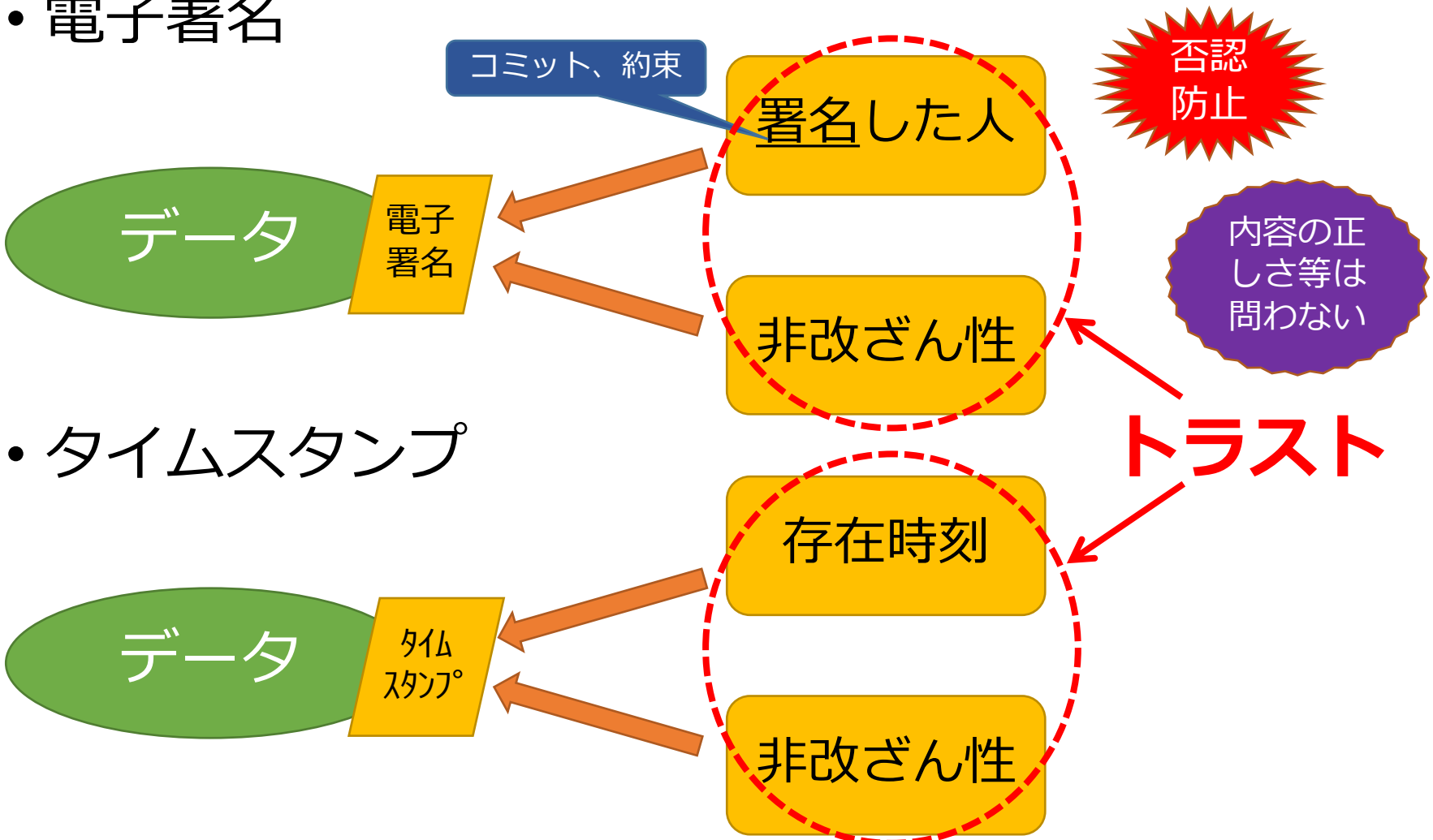
制度無し



データの「トラスト」の例

JNSA

- 電子署名



- タイムスタンプ

電子署名、eシール、デジタル署名

電子署名とｅシール

電子署名

否認防止

- 自然人が主体
- 意思（約束、コミットメント）を証明
- 手書き署名や記名押印に相当

日本では

ｅシール

- 法人が主体
- 発出元（出所）を証明
- 社印や角印に相当

責任の所在を証明

電子署名-eシール相関図

（欧米での）電子署名
Electronic Signature

eシール
Electronic Seal

欧米の電子署名と日本の電子署名

◆欧米の電子署名

- 本人と電子文書との関係（約束やコミットメント）を示すために本人が作成した電子データで、広く電子パッドに手書き署名するようなものも含む。

◆日本の電子署名法＊における電子署名：

- 電子文書が電子署名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。
- 電子文書の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。

＊「電子署名及び認証業務に関する法律」

電子署名-eシール相関図

（欧米での）電子署名

日本の電子署名法での電子署名
（ＥＵでは先進電子署名）

eシール

電子署名とデジタル署名

◆米の場合

- 電子署名：
  本人と電子文書との関係（約束やコミットメント）を示すために本人が作成した電子データで、広く電子パッドに手書き署名するようなものも含む。
- デジタル署名：
  電子署名の一種で、署名者の身元とデータが改ざんされていない事を、暗号技術を使って検証できるもの。

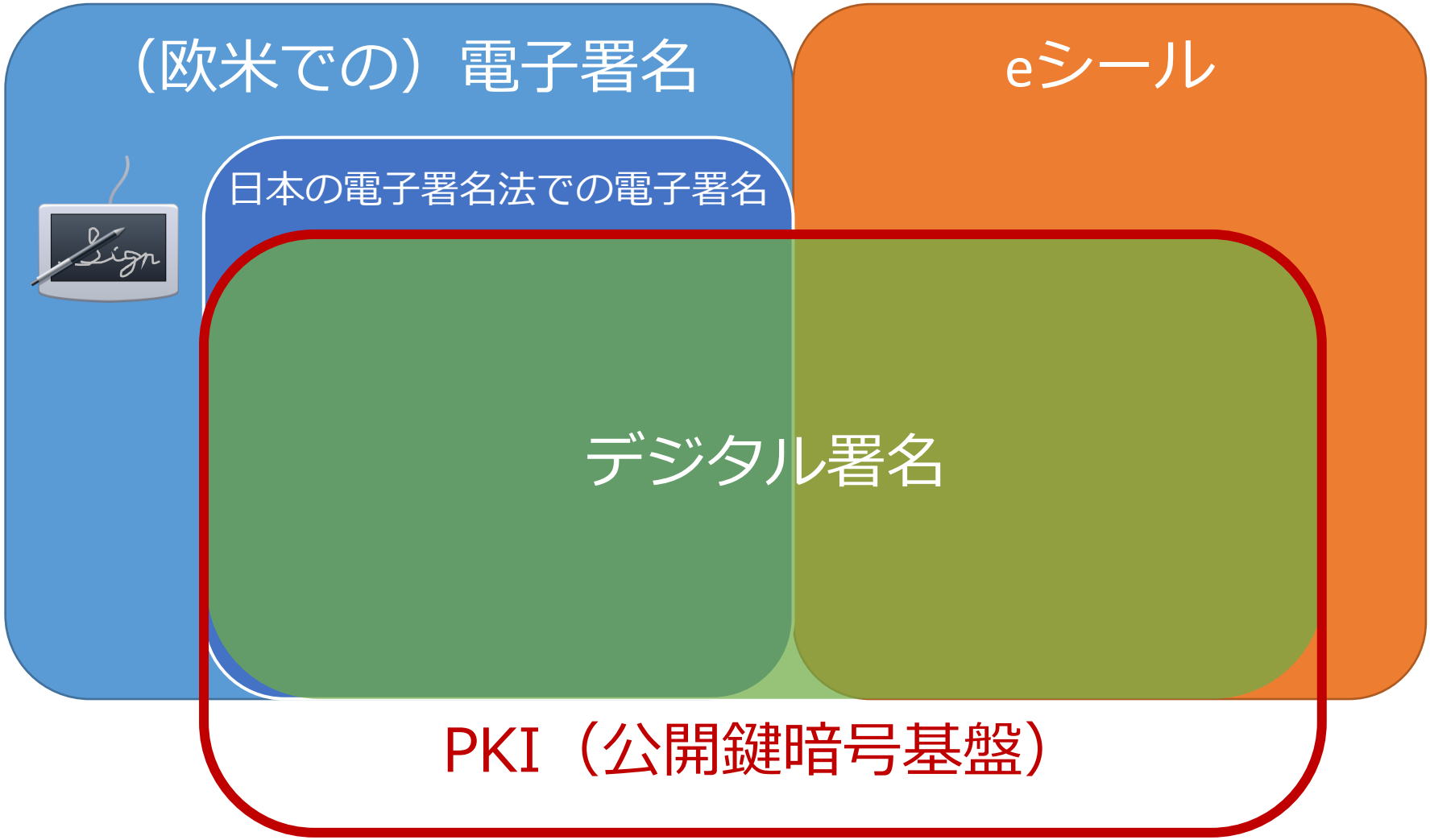
◆日本の電子署名法における電子署名：

- 電子文書が電子署名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。
- 電子文書の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。

◆欧米・日本含めてデジタル署名のより一般的な認識：

- 電子署名とeシールの両者に適用可能な公開鍵暗号（PKI：公開鍵基盤）を使った技術。

電子署名-eシール相関図

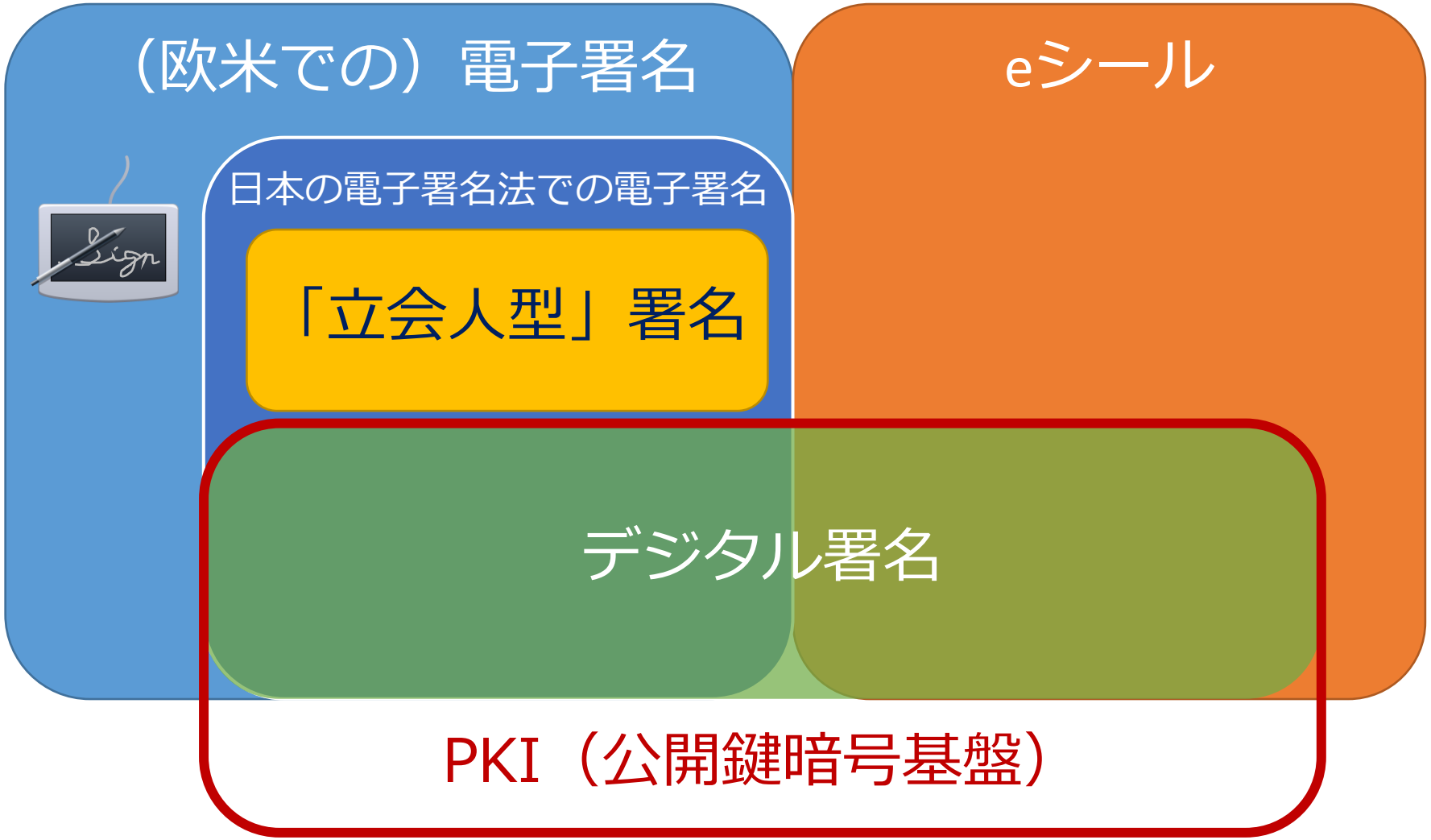


「立会人型」署名の出現

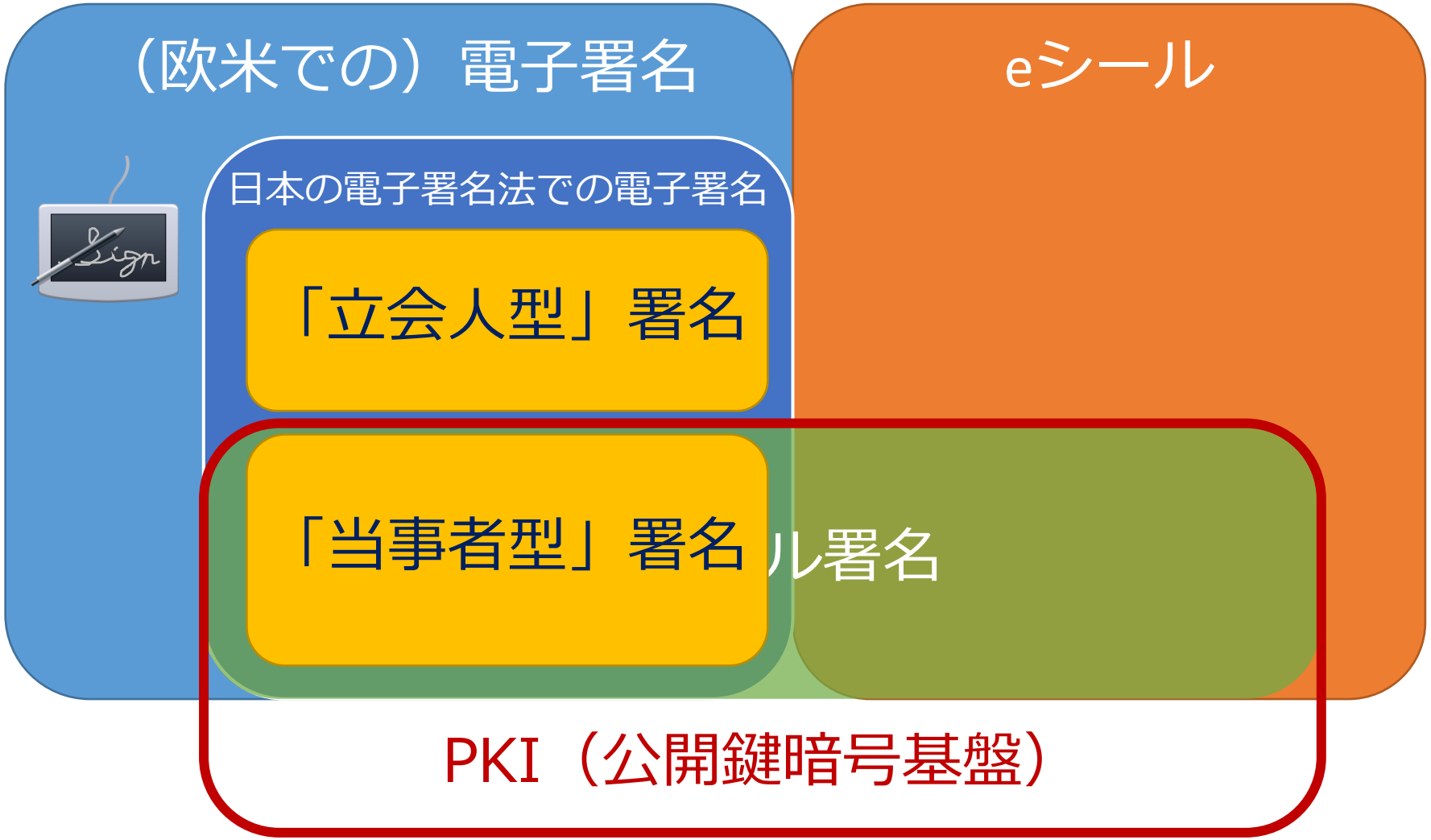
- 第三者である事業者（の提供するサーバー）が、利用者が文書に署名したことの立会人や目撃承認の役割を果たす。
- 立会人型署名、第三者型署名、事業者型署名、クラウド型署名、事業者署名型署名、、、などと呼ばれる。

- 電子署名法主務三省のQ&Aにより、条件を満たす「立会人型署名」も電子署名法の定義による電子署名に含められることに。

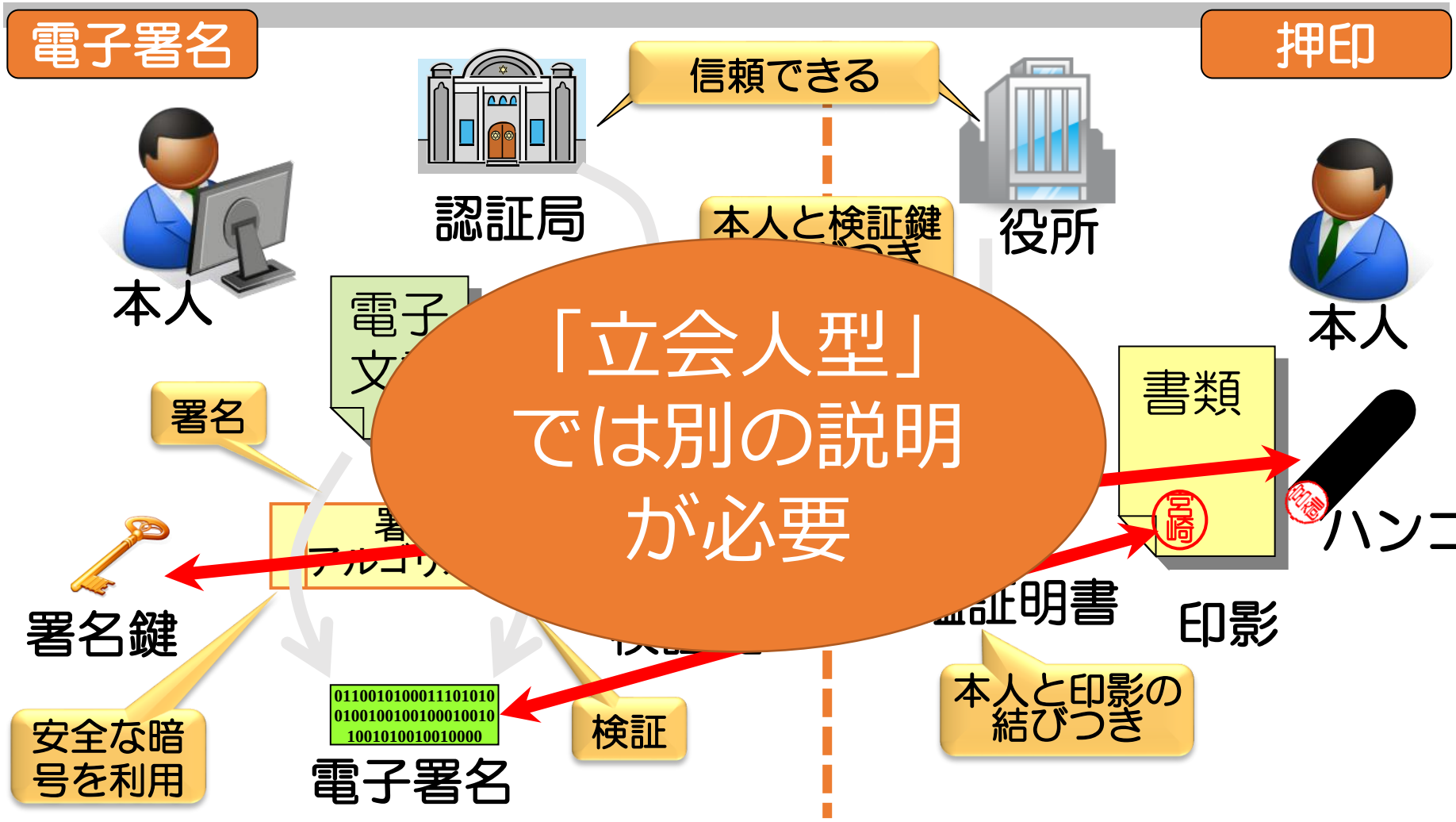
電子署名-eシール相関図



電子署名-eシール相関図



従来の電子署名の説明

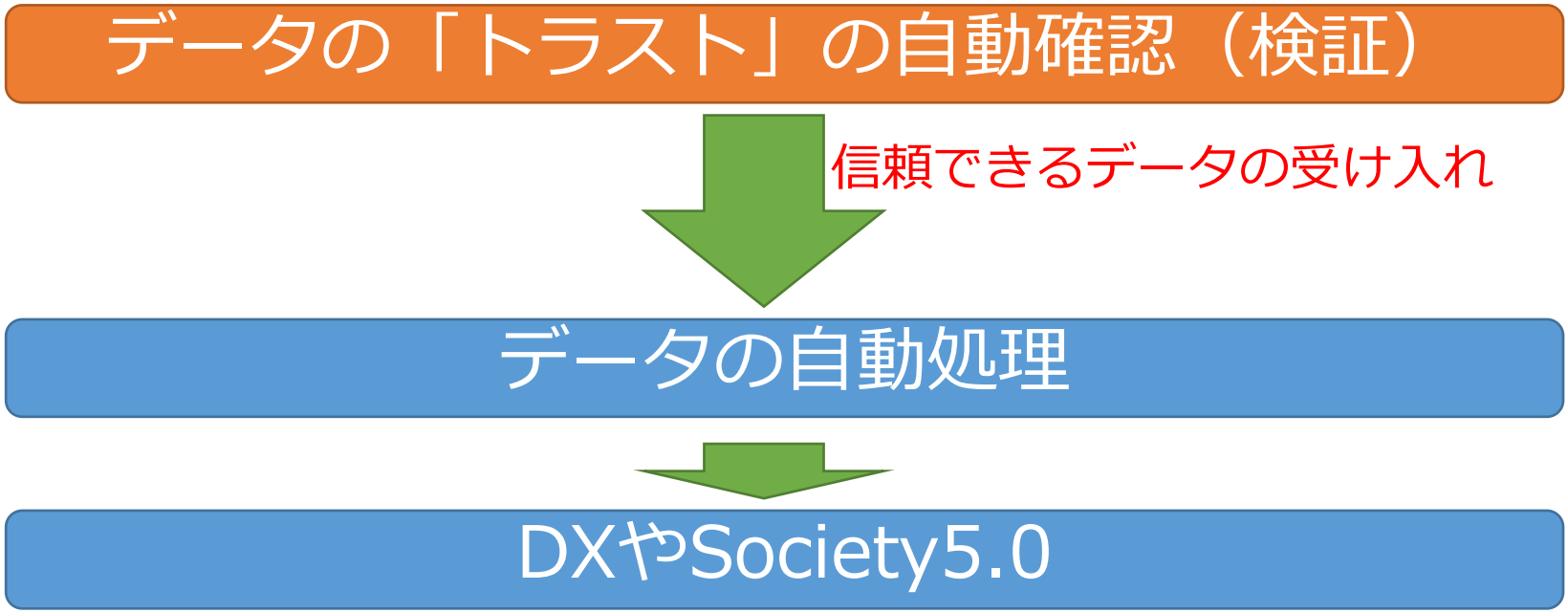


PKI（公開鍵基盤）に基づくデジタル署名を前提

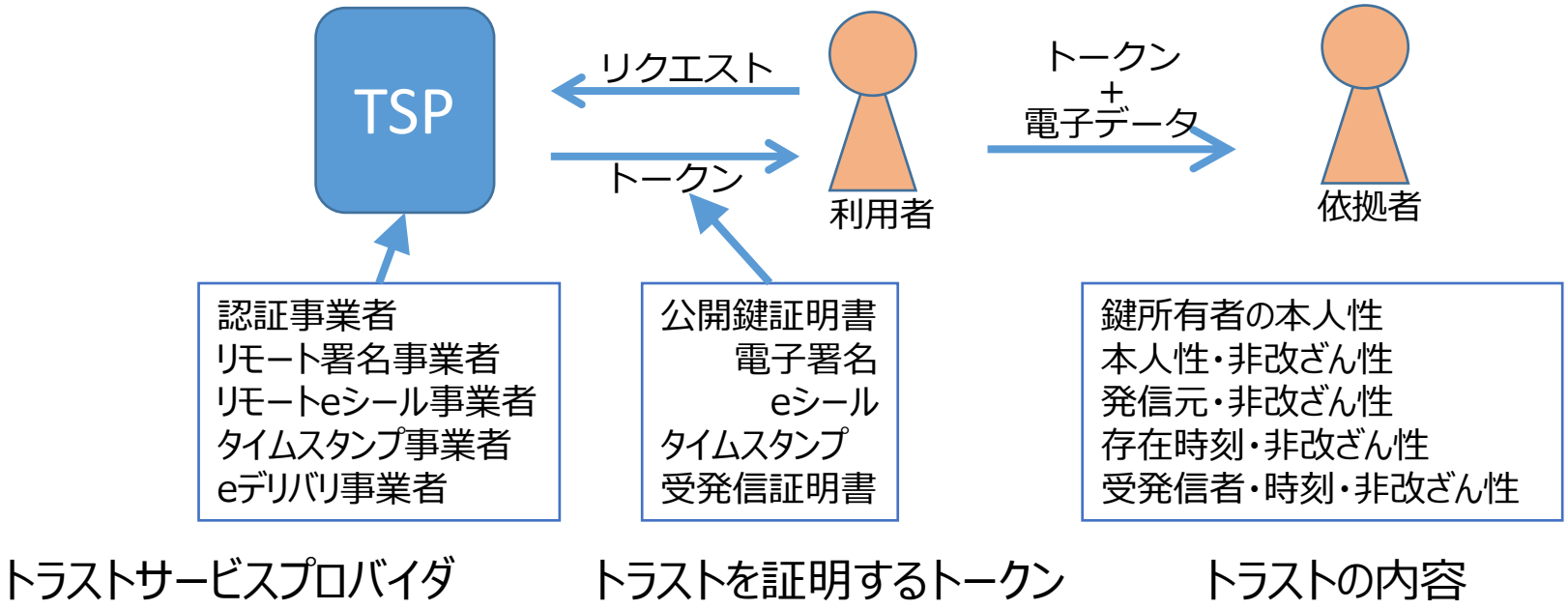
「トラスト」と検証

DX社会と「トラスト」の検証

- DXやSociety5.0でも想定されるデータ中心社会、データ駆動社会において、データの「トラスト」が重要。

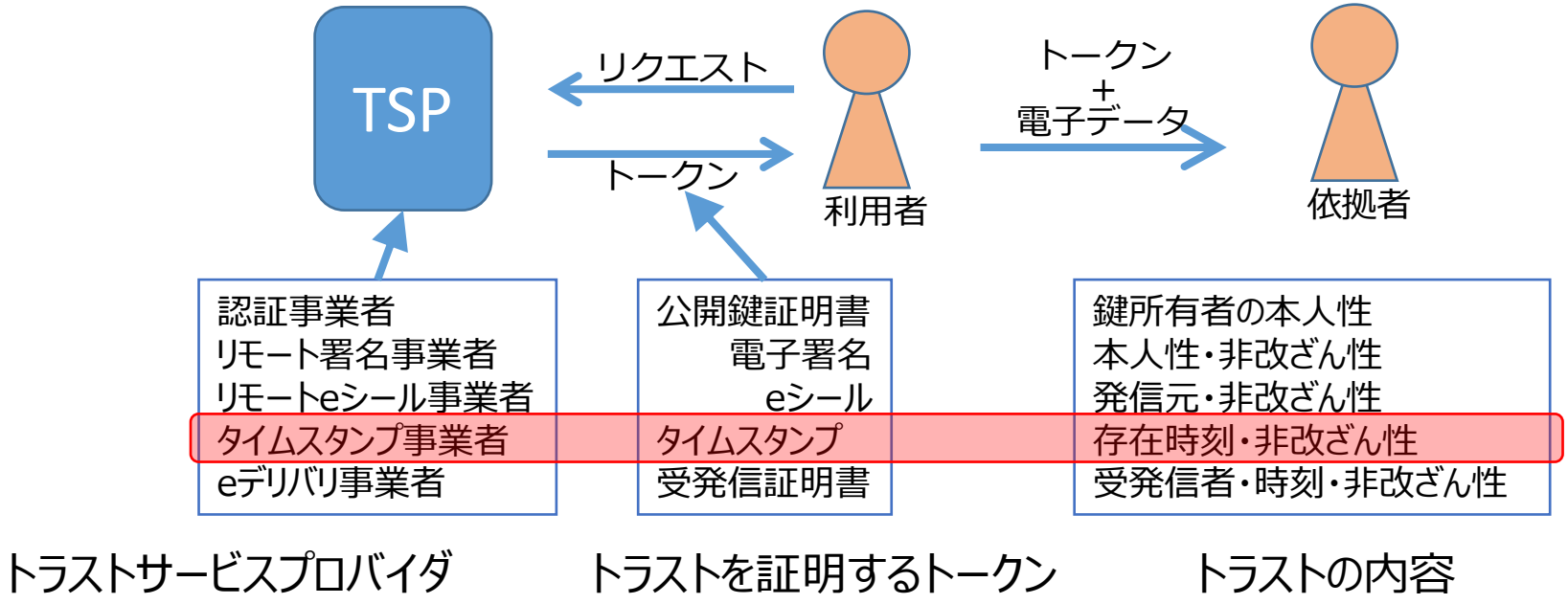


トラストサービスと検証



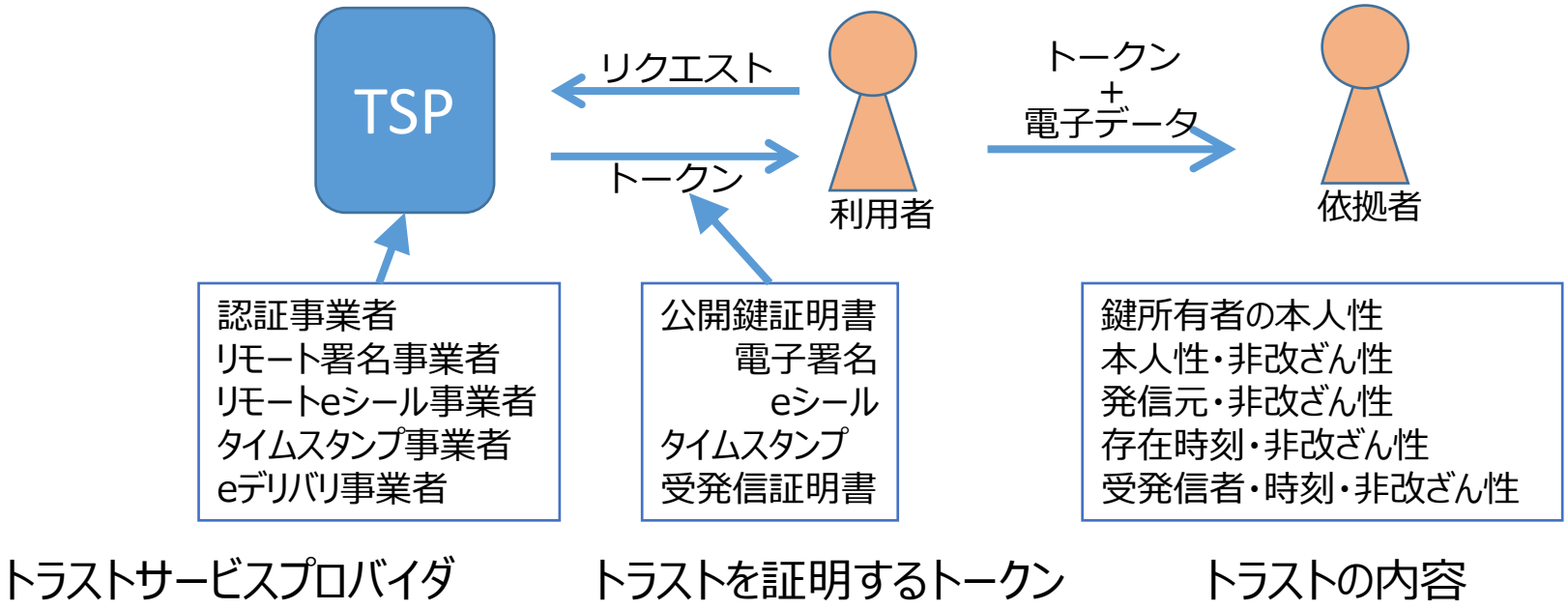
利用者は、電子データの「トラスト」を証明するために、TSP（トラストサービスプロバイダ）にトークンを要求する。

トラストサービスと検証



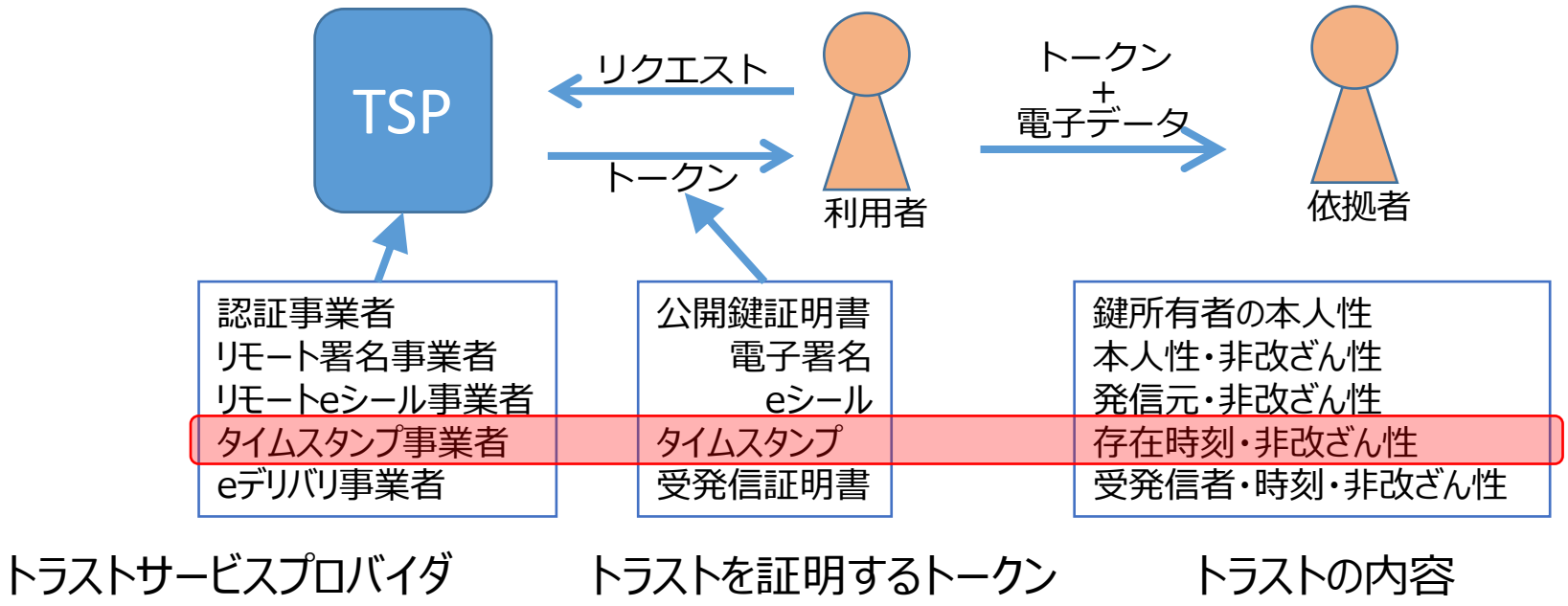
例えば、技術情報の存在時刻を証明するためにそれを記した電子文書に対するタイムスタンプを取得し、依拠者（データに基づき処理を実行する人やマシン）にそのデータの存在時刻・非改ざん性を証明しようとする。

トラストサービスと検証



依拠者は、**TSPを信用できる場合**、トークンを**検証**することにより、「トラスト」を受け入れるか否かを判断する。

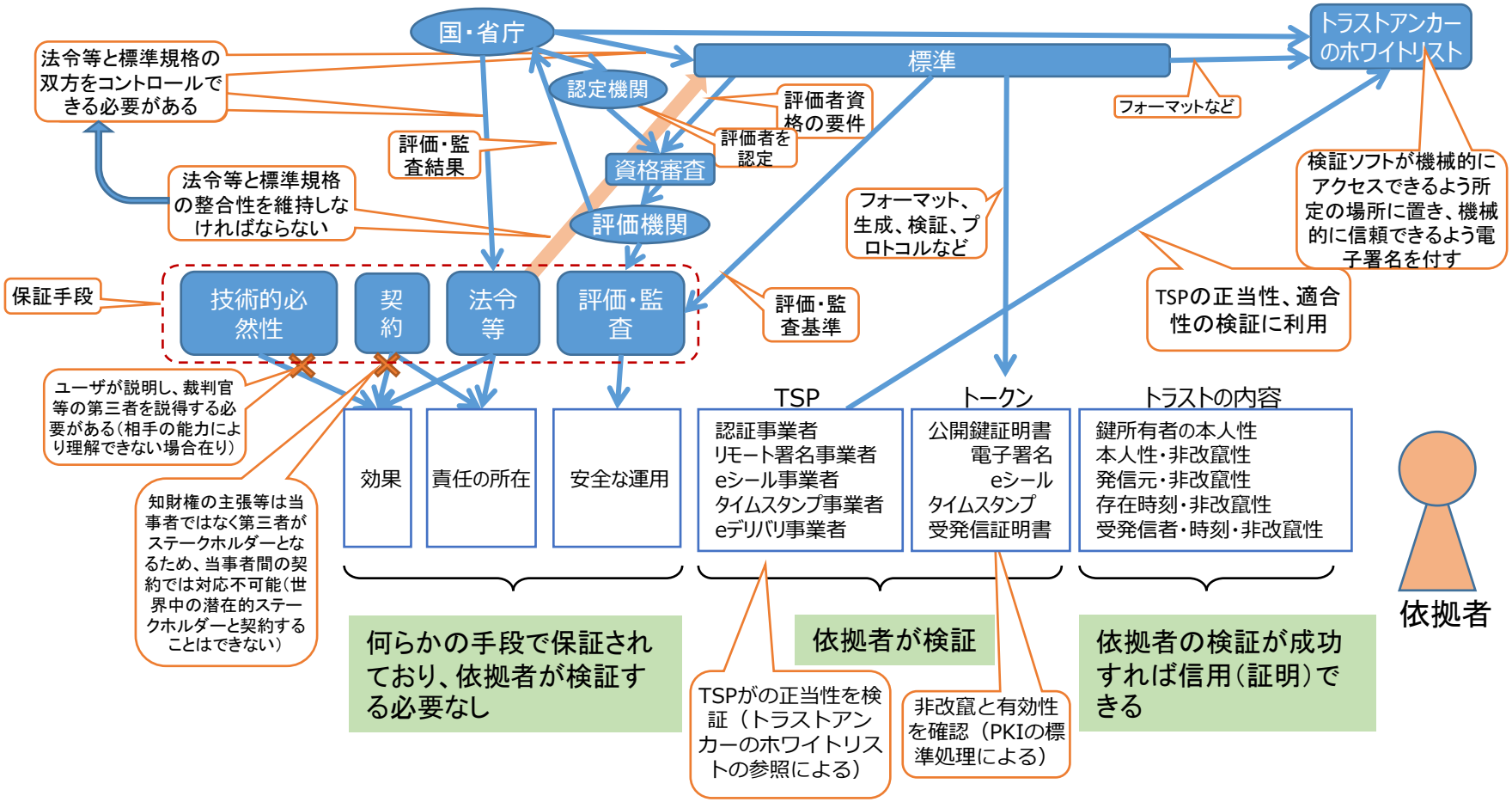
トラストサービスと検証



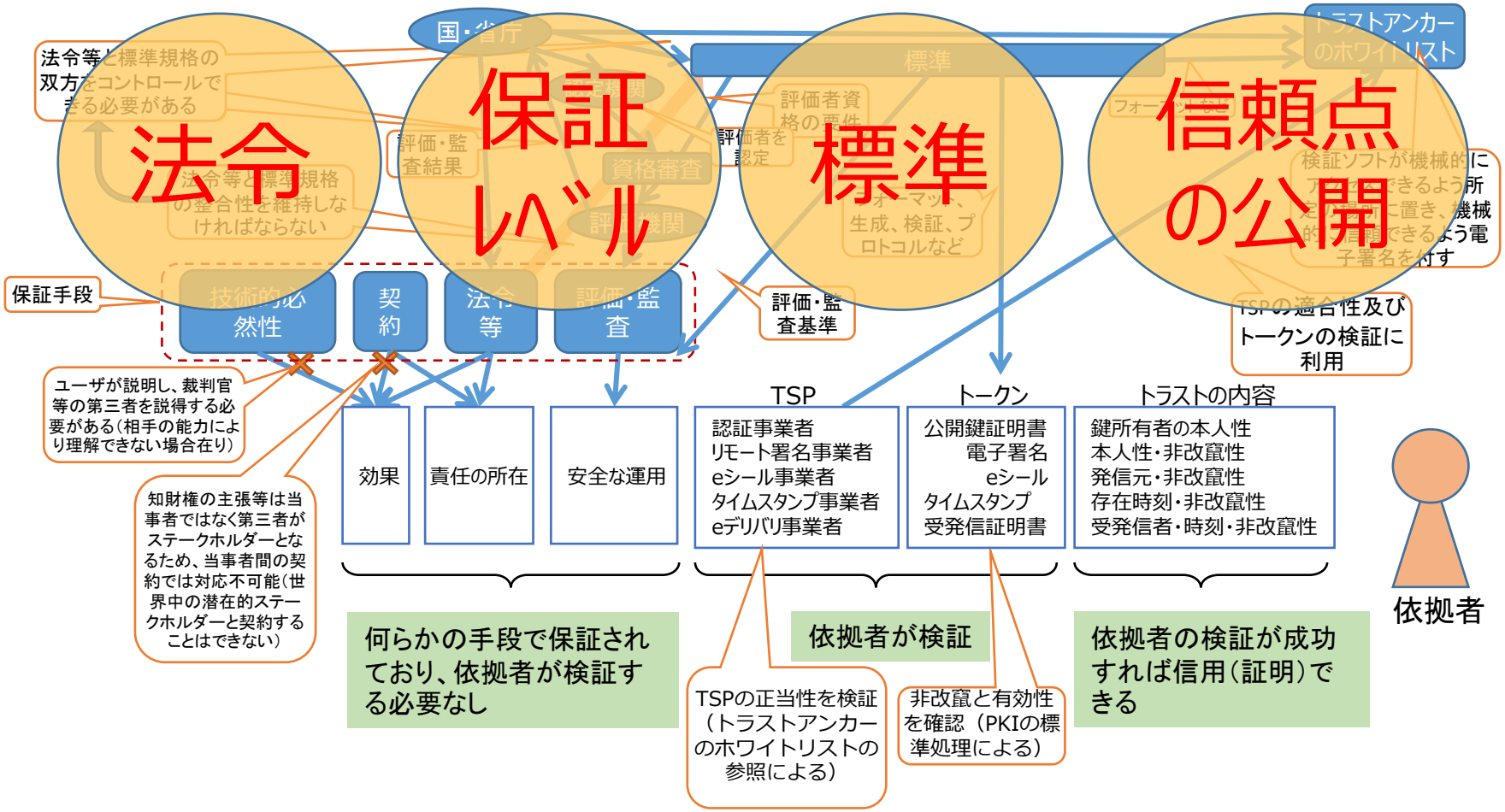
例えば、依拠者はタイムスタンプを検証し、検証結果が「有効」であれば、そのデータがタイムスタンプに記載された時刻に存在し、それ以降、改ざんされていないと判断し、自己の業務でデータを利用する。

「トラスト」の源泉

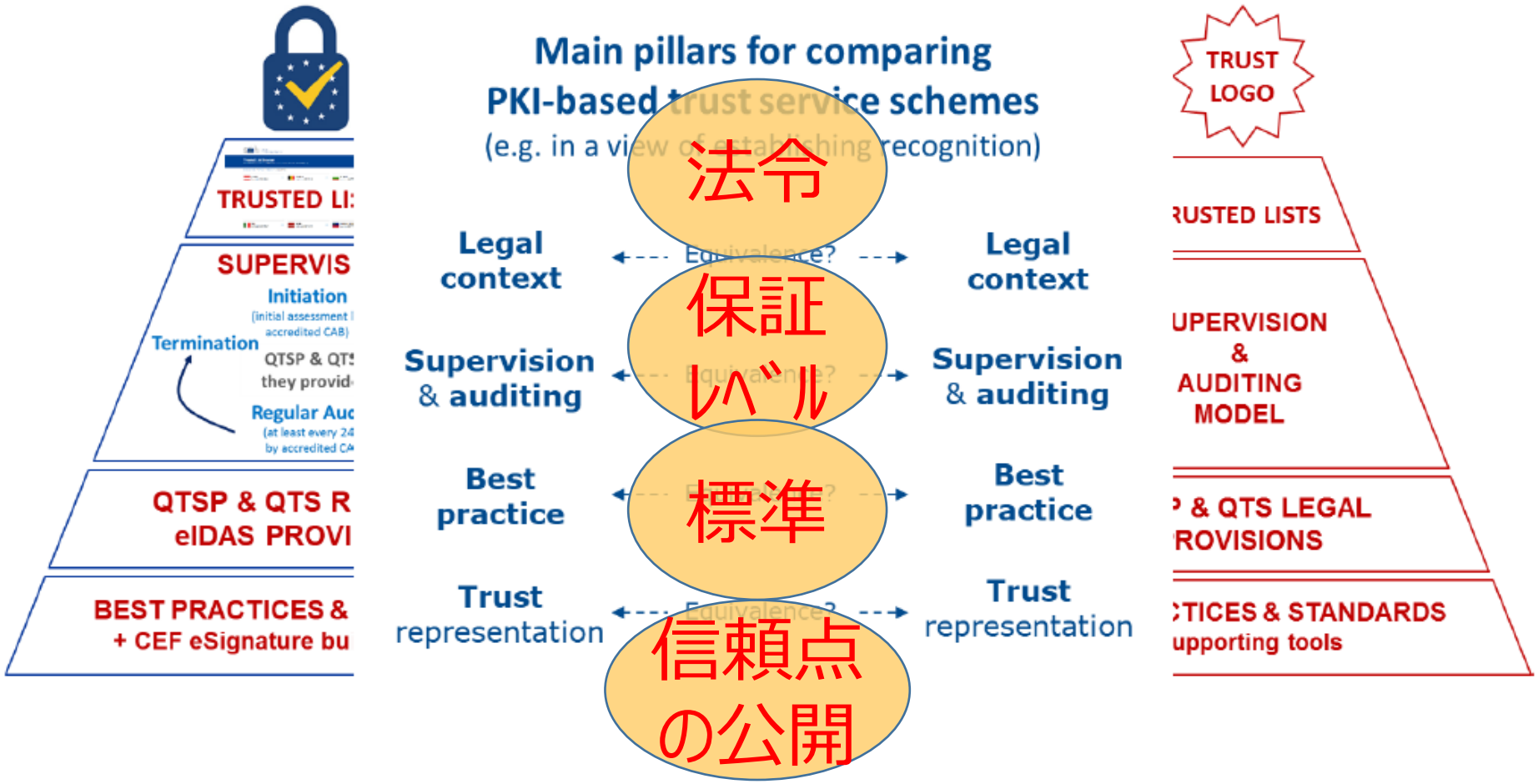
「トラスト」の源泉



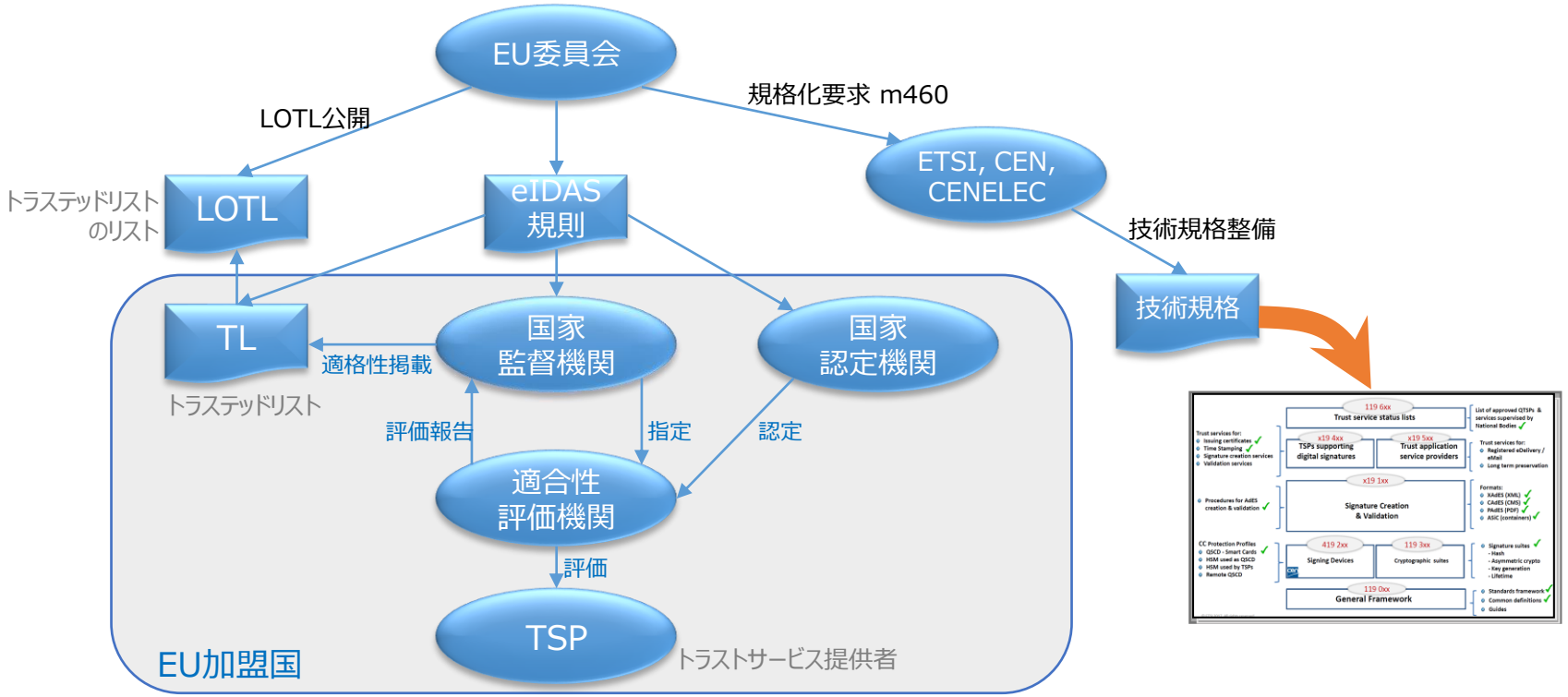
「トラスト」の源泉



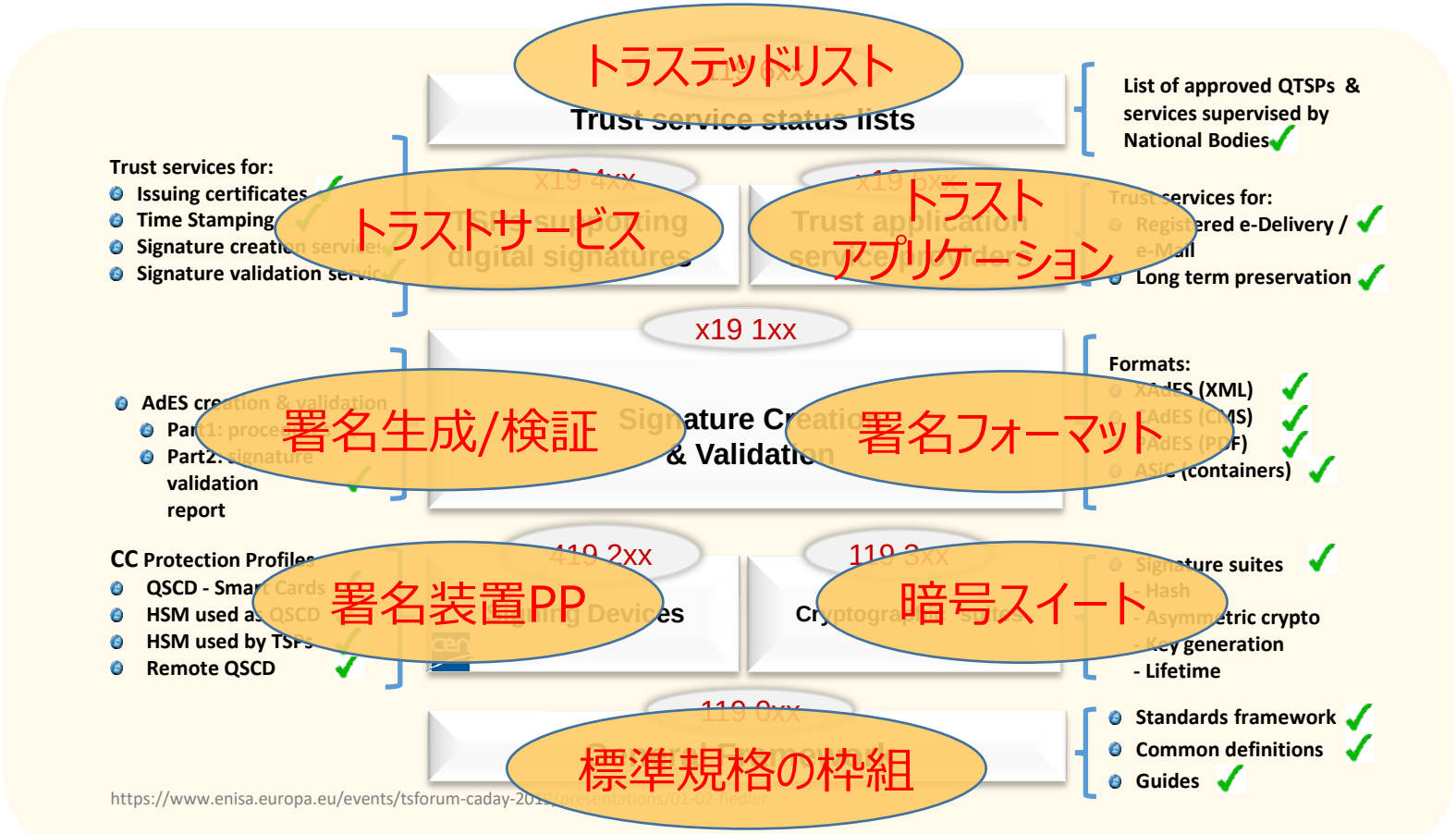
EUによる相互承認の観点



EUにおけるトラストサービスの枠組み



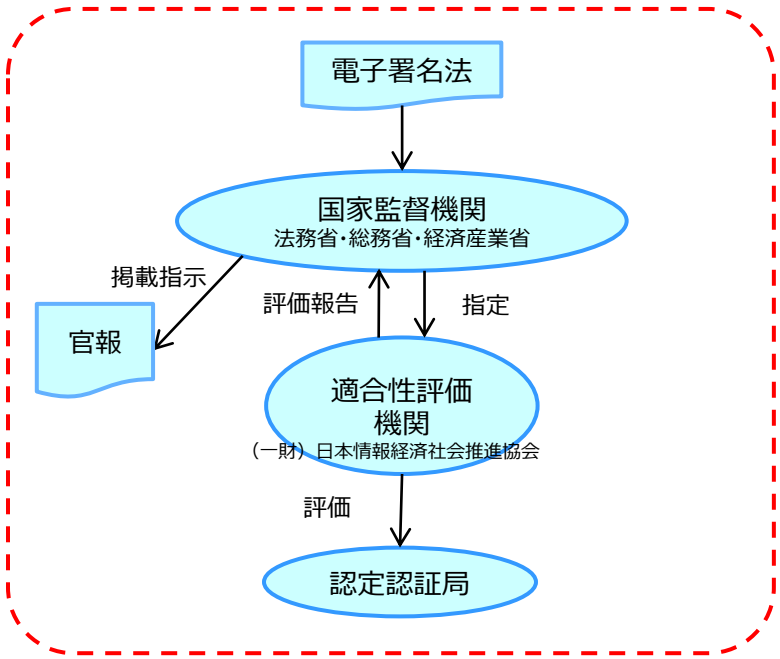
EUにおける関連の標準ドキュメントの整備



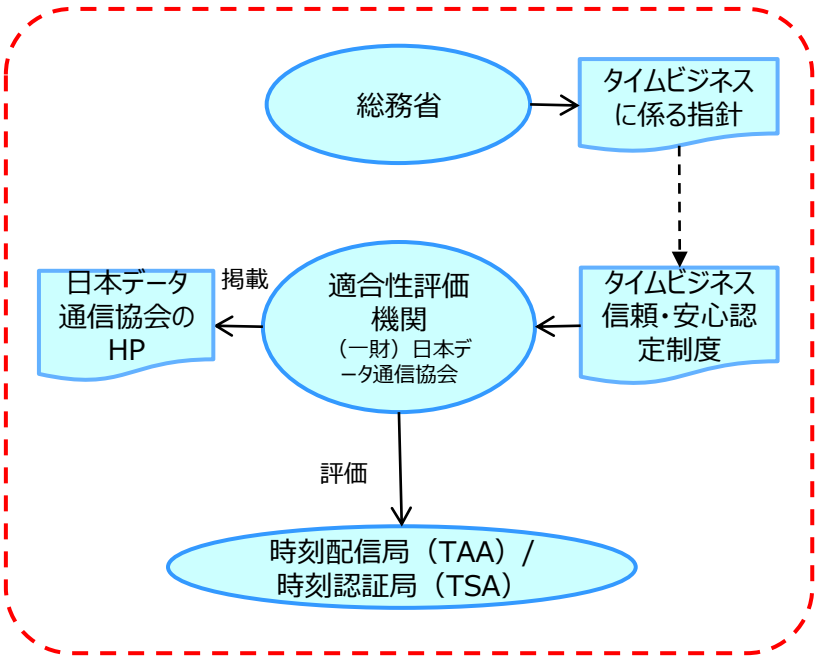
日本のトラストサービスの枠組

2021/3/31まで

電子署名



タイムスタンプ



タイムスタンプの国による認定制度

- 2020年3月より、**「タイムスタンプ認定制度に関する検討会**（座長：立教大学法学部教授　東條吉純）」を開催し、国際動向も踏まえつつ、**国としての認定の仕組みを検討**。
- 2020年12月、「タイムスタンプ認定制度に関する検討会取りまとめ（案）」と、本案を踏まえた**告示として「時刻認証業務の認定に関する規程（案）」を公表**し、意見募集を実施。**2021年４月１日に公布・施行（指定調査機関の関係のみ）**。

※認定関係の施行は2021年7月目処を予定

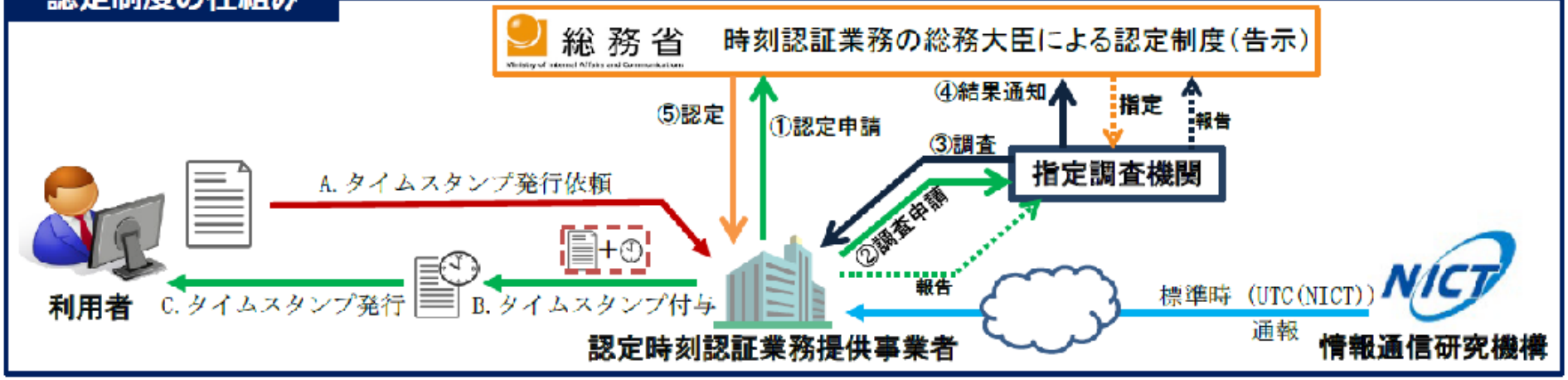
タイムスタンプの国による認定制度（総務省告示）の概要

- **電子データがある時点に存在していたこと及び当該電子データがその時点から改ざんされていないこと**を証明する情報である**「タイムスタンプ」を、電子データに係る情報に付与する役務**を提供する業務を**「時刻認証業務」**とする。
- 時刻認証業務の中で、**確実かつ安定的にタイムスタンプを発行するための要件を満たす**ものを、**「認定時刻認証業務」**とする。

認定要件のポイント（抜粋）

- ○ **デジタル署名方式**を用いること。
- ○ **時刻源は**国立研究開発法人情報通信研究機構の**UTC（NICT）**とすること。
- ○ 発行する(した)タイムスタンプと当該時刻源との**時刻差が１秒以内となるよう、時刻の品質を管理及び証明**する措置を講じること。
- ○ タイムスタンプは**十分な安全性を有する暗号技術や装置**等を用いて生成・管理すること。

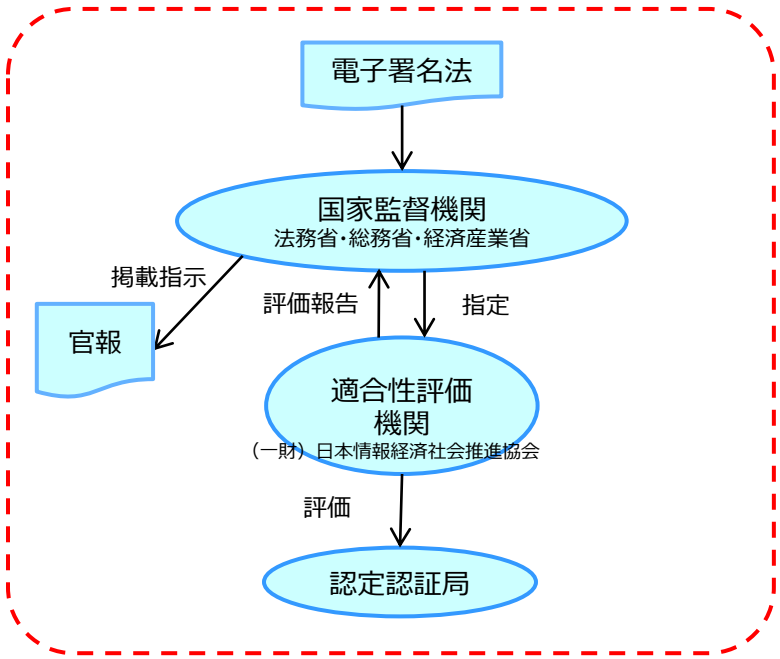
認定制度の仕組み



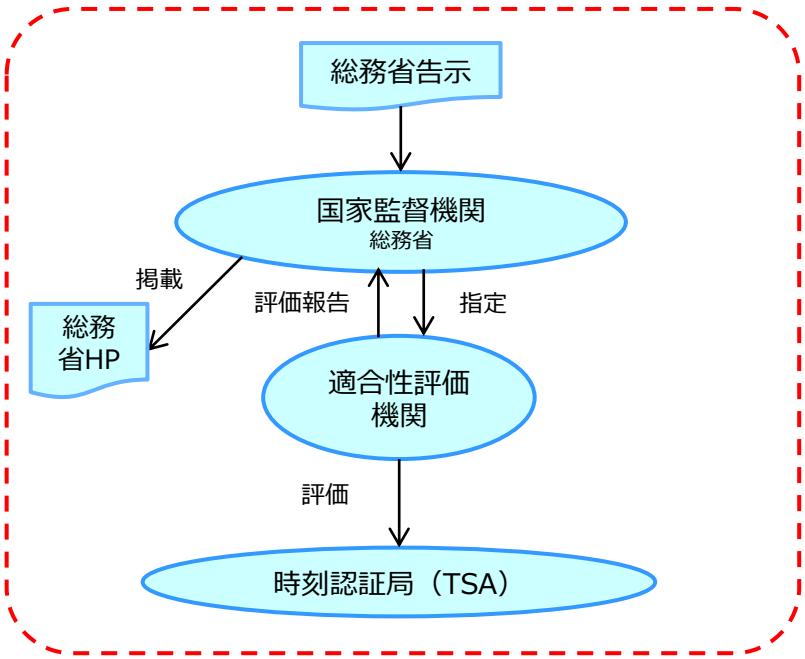
日本のトラストサービスの枠組

2021/4/1以降

電子署名



タイムスタンプ



署名検証標準規格の必要性

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

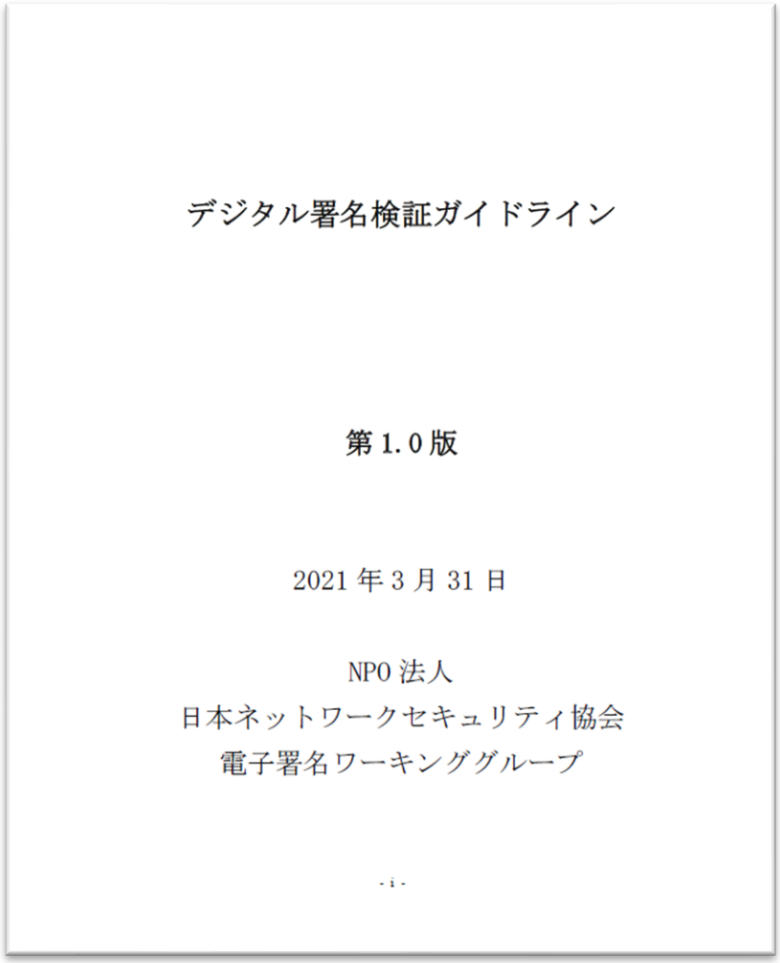
・署名
……
証明書
・有効期間
・失効
・パス
・トラストアンカ
・検証時刻
……

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

デジタル署名検証ガイドライン JNSA



デジタル署名検証ガイドライン

第 1.0 版

2021 年 3 月 31 日

NPO 法人
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

- i -

概要・目的

　デジタル化とネットワーク化の進展に伴い、デジタルデータの保証と取り扱う人やサービスの信頼性が、これまで以上に必要とされるようになっている。中でもデータの作成責任とその真正性は、アナログ時代においては「署名」や「押印」によって担保されてきた。デジタル時代においては、それに相当する技術として「電子署名」がある。

　署名は文書等にそれが付与され、受領者が署名を確認することで文書等の真偽や価値の判断材料となる。しかし、可視データであるアナログの「署名」や「押印」と違い、「電子署名」は機械処理としての「署名検証」が必要であり、検証ツール（ソフトウェア）に依存することになる。さらに、電子署名は様々な要素から構成されており、その判定は注意を要する。その判定基準が検証ツールによって異なると、同じデータに対する判定が異なる結果となり、デジタル化の阻害要因となりかねない。それを防ぐため、本書では、電子署名のうち公開鍵暗号技術に基づくデジタル署名について検証のガイドラインを示すものである。

https://www.jnsa.org/result/e-signature/data/e-signature-guideline_v1.0_20210331.pdf

課題、電子署名WGの関連活動

課題

- デジタル・ガバメント閣僚会議「データ戦略タスクフォース　第一次とりまとめ（2020/12/21）

トラストに関するワーキングチームやデジ庁に期待！

①基盤であるトラストアンカー機能を構築、
②様々なトラストに関わるサービスを包括的に整備、
③あわせて価値観を共有する国々との連携を図ることとする。

- 「トラストの枠組」維持の仕組みの構築が課題
  - 標準規格や適合性評価基準の維持
  - 法制度との整合性の維持
  - 国際通用性の維持

電子署名WGの関連活動

- 電子署名に関するQ&A
  https://www.jnsa.org/result/e-signature/e-signature-qa/index.html

- デジタル署名検証ガイドライン
  https://www.jnsa.org/result/e-signature/data/e-signature-guideline_v1.0_20210331.pdf

- 電子署名レベルの検討を来年度開始予定
  - 本人保証レベル、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捉えられるように。

- 興味がおありの方はJNSAまでご連絡ください。

ご清聴ありがとうございました。