「ゼロトラストにとってのデジタル署名 vs. 電子署名にとってのデジタル署名」

2023/08/23

電子署名WG　リーダー　宮崎 一哉

電子署名WGの紹介

サブタイトル

目的・活動予定等

１．WGの活動目的

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、電子署名保証レベルの検討、電子署名関連パブコメへの対応、及び電子署名普及啓発を行う。

２．WGの2023年度の活動予定

・標準仕様案等検討会（年20回程度）

・ISO/TC154国内審議委員会の運営支援、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、ISO/SC34及びJAHISのリエゾン

・PKI Day等講演会の開催

・デジタル庁の電子署名に関する議論への参画

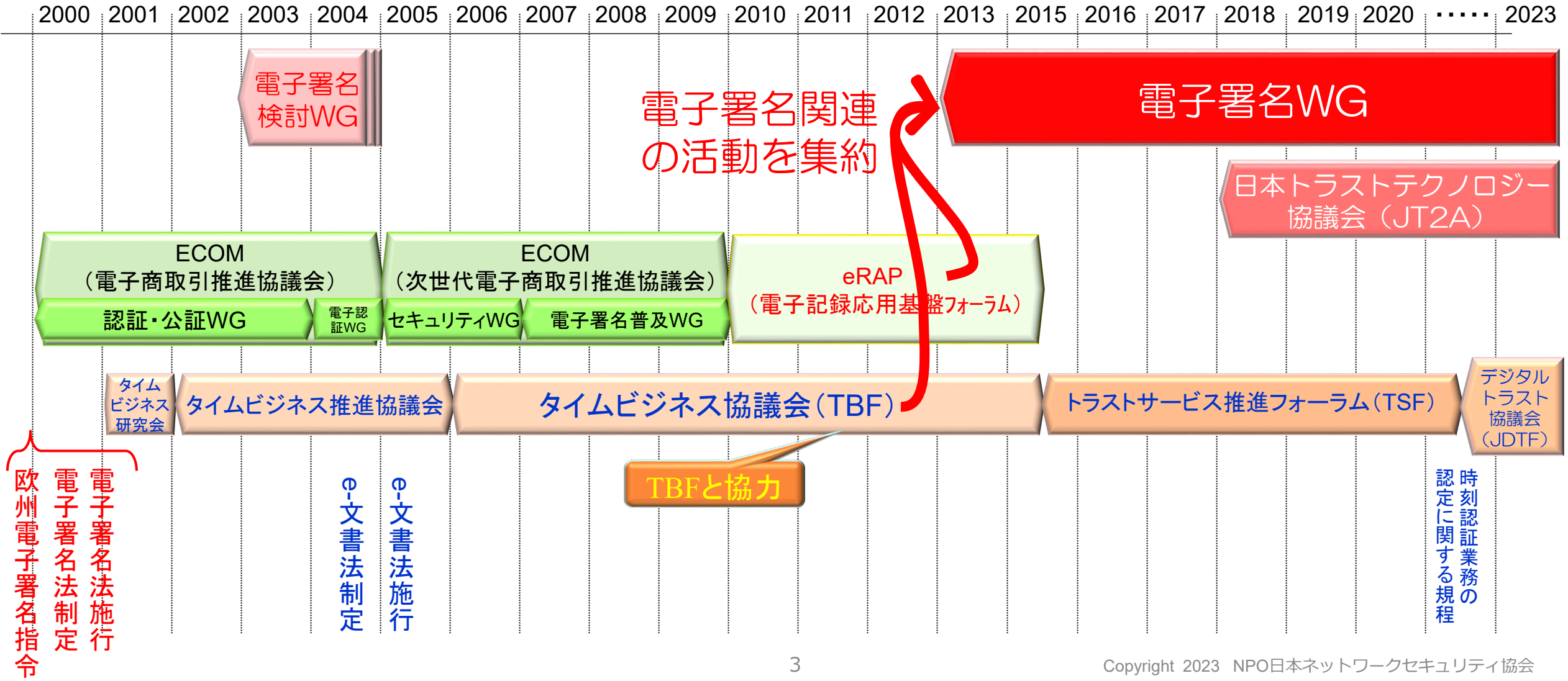
３．2023年度の予定成果物

・長期署名プロファイル標準の制改定

・署名検証プロセス及び署名検証レポートに関する標準仕様案、解説書

・電子署名保証レベルに関する報告書

電子署名WG発足の経緯



電子署名WGの紹介記事

JNSA PRESS　JNSAワーキンググループ紹介

- 『電子署名検討WG』第8号（2003年9月発行）
  https://www.jnsa.org/active/press/vol8/3-1WG.pdf
- 『電子署名WG』第37号（2014年3月発行）
  https://www.jnsa.org/jnsapress/vol37/5_WG.pdf
- 『JNSA標準化部会・電子署名ワーキンググループ』
  第45号（2018年3月発行）
  https://www.jnsa.org/jnsapress/vol45/3_WG-1.pdf
- 『標準化部会・電子署名ワーキンググループ』
  第52号（2023年3月発行）
  https://www.jnsa.org/jnsapress/vol52/3_WG.pdf

電子署名WGの最近の成果

電子署名WG/JT2A　報告書・成果物紹介ページ

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

- 2022/7/5：「電子署名保証レベル要約版」
  （標準化部会 電子署名ワーキンググループ 保証レベルタスクフォース）
- 2021/11/9：「オンライン身元確認(eKYC)金融事例調査報告書」
  （日本トラストテクノロジー協議会（JT2A）　真正性保証タスクフォース）
- 2021/10/26：「電子署名保証レベル作業提案」
  （標準化部会 電子署名ワーキンググループ 保証レベルタスクフォース）
- 2021/10/4：「XAdES長期署名プロファイル国際規格の改定」
  （標準化部会電子署名ワーキンググループ標準原案作成タスクフォース）
- 2021/4/15：「デジタル署名検証ガイドライン」（標準化部会電子署名ワーキンググループ）
- 2020/11/6：「リモート署名ガイドライン」修正版
  （日本トラストテクノロジー協議会（JT2A）リモート署名タスクフォース）
- 2020/9/29：「電子署名ワーキンググループ執筆「電子署名Q&A」」
  （標準化部会電子署名ワーキンググループ）
- 2020/4/30：「リモート署名ガイドライン」
  （日本トラストテクノロジー協議会（JT2A）リモート署名タスクフォース）

電子署名とデジタル署名

サブタイトル

電子署名の目的

- 自然人本人の意思の表明　↔　法人からの発出証明　＝　eシール
  - 「自然人以外」に拡大の傾向も
- 電子取引等で広範囲で利用
- 電子署名法（電子署名及び認証業務に関する法律）

（定義）
第二条　この法律において「電子署名」とは、電磁的記録（略）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。
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。

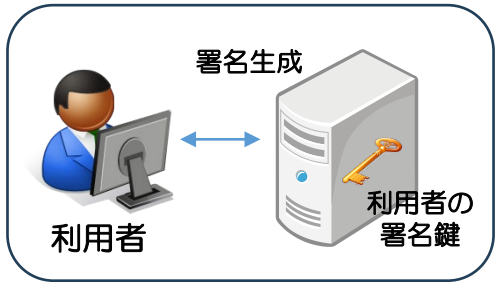
第二章　電磁的記録の真正な成立の推定
第三条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

民事訴訟法第228条第4項
私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。

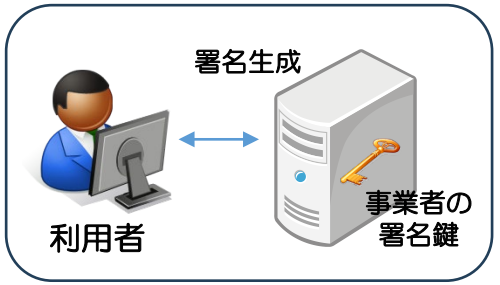
電子署名の方式とデジタル署名

- 「電子署名保証レベル要約版」（電子署名WG/保証レベルTF）より
  https://www.jnsa.org/result/e-signature/2022/index.html
  - ローカル署名　⇒　本人のデジタル署名を付与（署名鍵をローカル管理）
  - リモート署名　⇒　本人のデジタル署名を付与（署名鍵をリモート管理）
  - 事業者型署名　⇒　事業者のデジタル署名を付与
  - 認証記録型署名（新）⇒　デジタル署名を利用しない

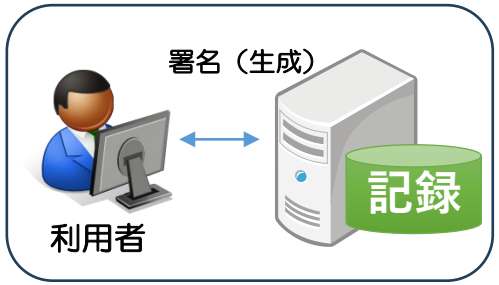
ローカル署名



リモート署名



事業者型署名



認証記録型署名

電子署名の目的とデジタル署名の検証

- 自然人本人の意思の表明
- 承諾、約束などの何らかのコミットメントを受信時及び事後に証明
- 事後の否認を防止する

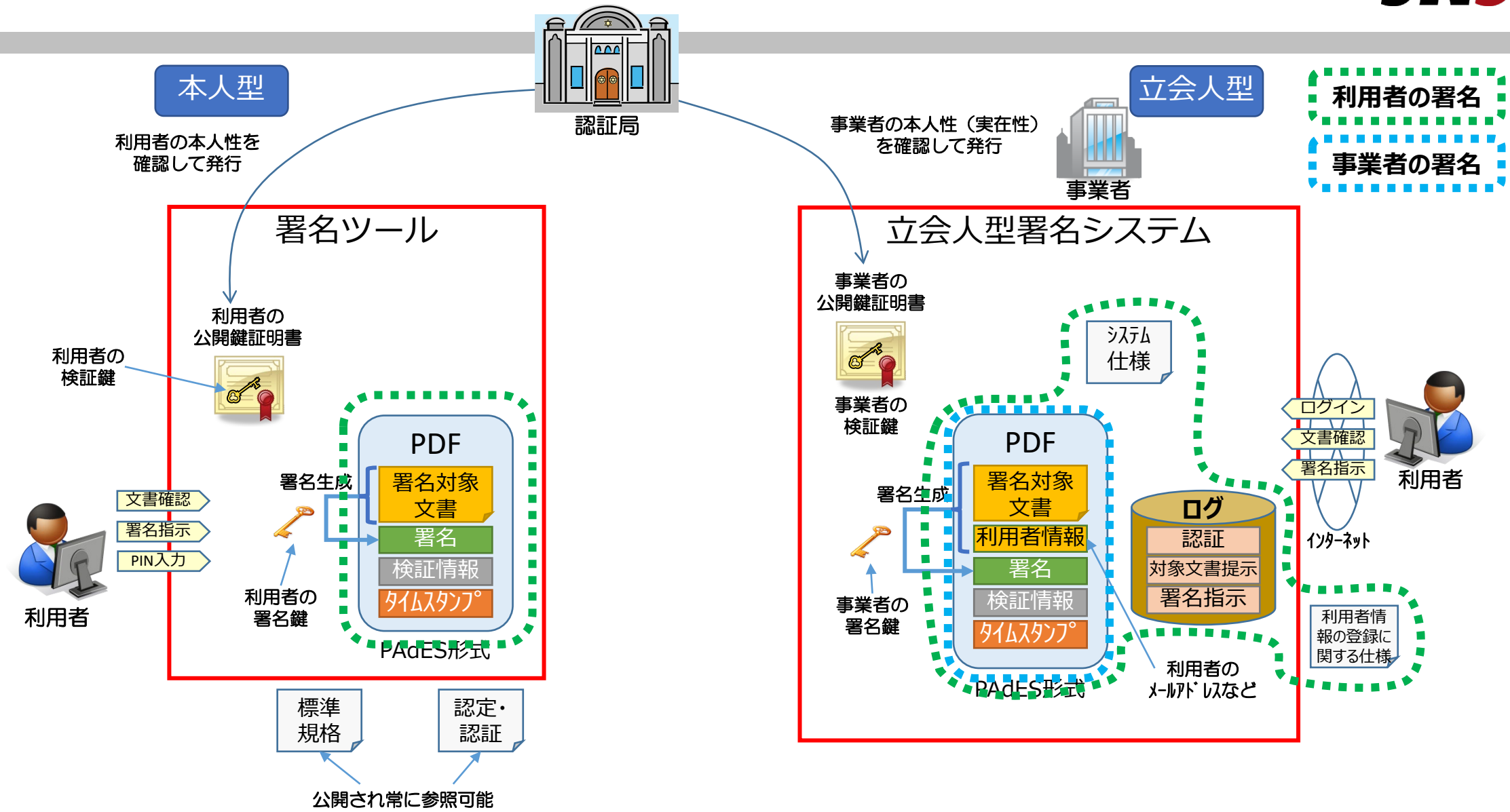
責任追及先

証拠としての効果

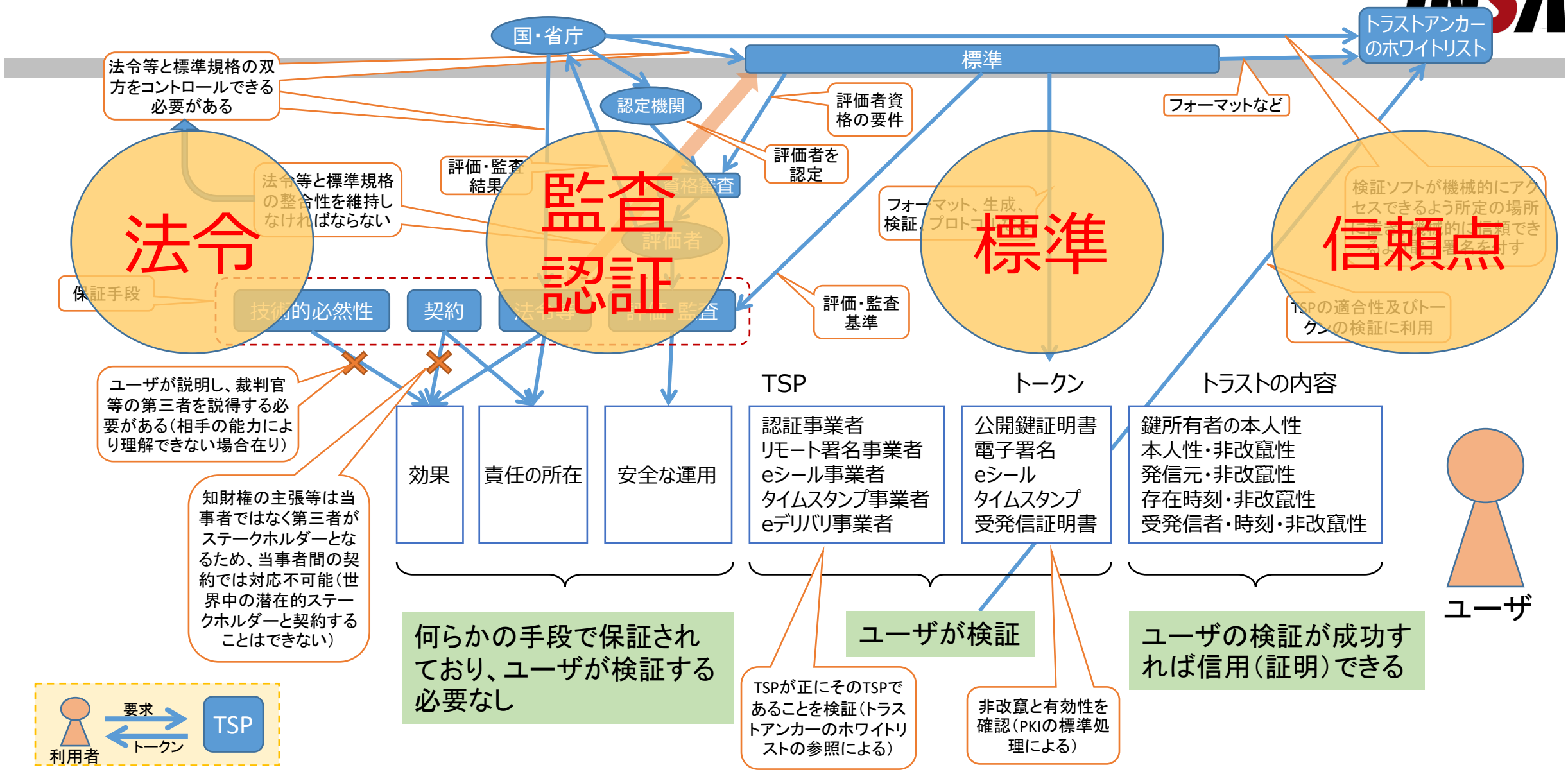
デジタル署名の検証

「デジタル署名検証ガイドライン」
https://www.jnsa.org/result/e-signature/2021/index.html

利用者本人の署名と事業者型署名の検証



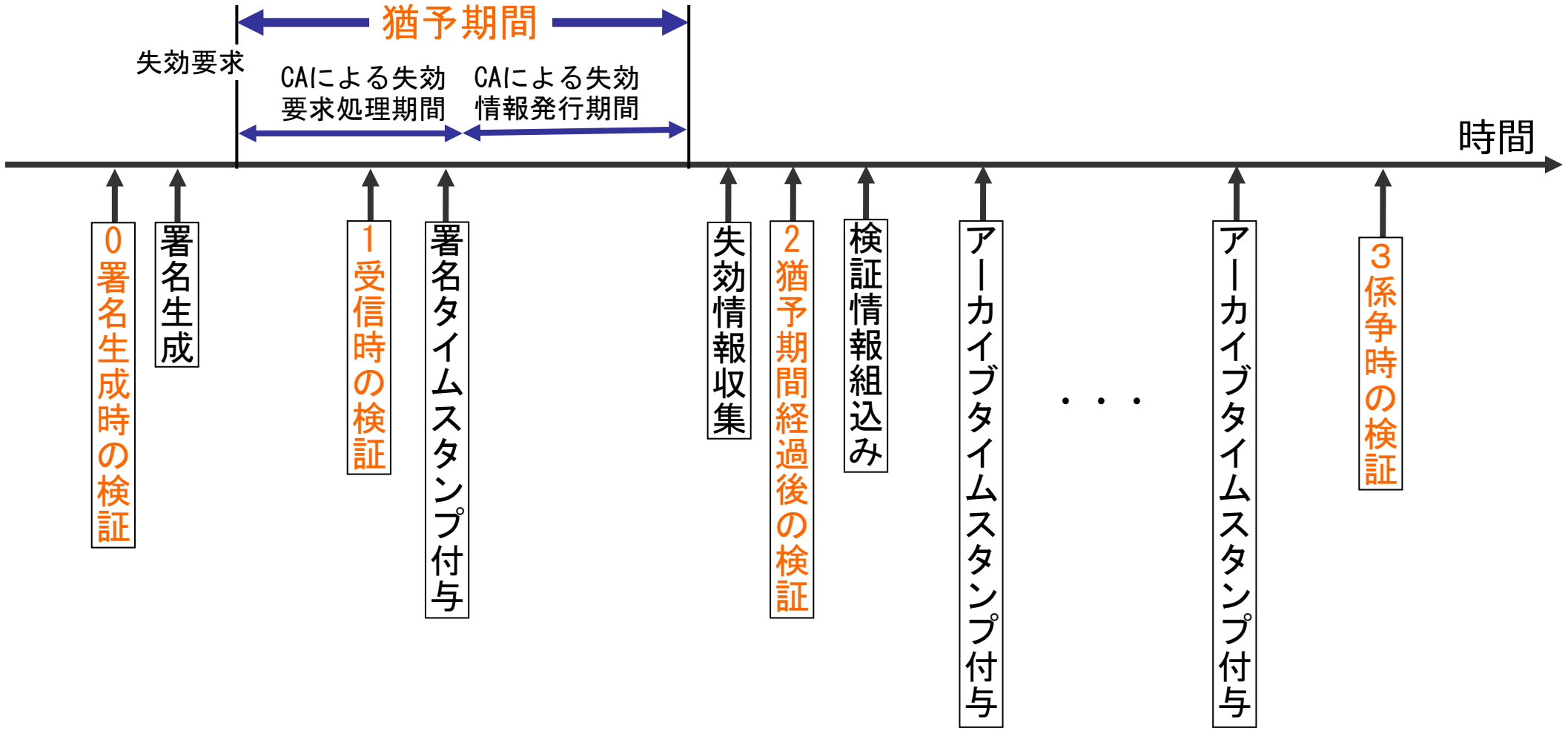
トラストサービスが「トラスト」を生み出す原理



デジタル署名の3度の検証

0. デジタル署名生成時
   - 公開鍵証明書の有効性（有効期間、失効状況）確認
1. デジタル署名受信時
   - 受信時に受入れ可能か否かを検証、必要に応じ、署名タイムスタンプを付与
2. 猶予期間経過後
   - 失効状況を正しく把握するために検証、検証情報（認証パス上の公開鍵証明書、CRLやOCSPレスポンス等）を収集し、署名データに組込む
3. 係争時
   - 裁判等で提出した証拠の有効性を確認

デジタル署名の3度の検証（説明図）



信頼点（トラストアンカー）の重要性

- 認定認証業務（公的認定制度）　法的バックグラウンド
- AATLやWebTrust認証などの実績のある民間の認証制度
  ⇒パブリック認証局　広範囲での利用を期待
- ブリッジ認証局、相互認証　やや暗黙の信頼となりやすい
- EUのトラステッドリスト　最新状況の反映にタイムラグ
- HPKI　特定分野としての検証が要求される
- プライベート認証局　特定の閉鎖的コミュニティー内での利用

ゼロトラストとデジタル署名

サブタイトル

ゼロトラストの目的

- リソースに対するアクセスコントロール＋α
  - より広範の信頼性に対する要求

- そのために、、、
  - 信頼しない：境界やネットワークを信頼しない、暗黙の信頼はしない
    ＝
  - 常に検証する：リソースへのアクセス時（アクセス前）に検証する
    ⇒　常に最新の状況をもとに検証する必要がある

ゼロトラストにおけるデジタル署名

- ゼロトラストにおけるデジタル署名は、
  - デバイス、ユーザー、アプリケーション等の認証の手段
    ⇒　認証　　⇔　　署名
    - ランダム値への署名
  - 環境の正当性や完全性の確認の手段
    ⇒　署名的
    - 環境に関する特定のデータに署名

ゼロトラストにおける検証

- ネットワークフローはすべて処理前に検証されなければならない
  ⇒事前の検証
  　　リアルタイムの検証　⇔　事後の検証（電子署名）
  　　手遅れにならないように　　猶予あり

- 変化する環境に追随した検証
  ⇒CDM、PA、PEP、、、
  ⇒リモートアテステーション（松本さんが詳細を）

ゼロトラストにおける信頼点

- パブリック認証局ではなく、プライベート認証局を利用すべき。
- 「パブリック」は暗黙の信頼と同じようなもの？
  ⇒信頼点の変化を制御できない。
  そもそも変更にタイムラグ
  固定的なポリシーも問題か

- プラットフォームやデバイス等に埋め込まれた信頼点
  ⇒暗黙的に信頼してしまっているかも
  ⇒比較的固定的

評価基準を満足したCAの証明書のリスト

ゼロトラストにとってのデジタル署名
vs.
電子署名にとってのデジタル署名

サブタイトル

比較とまとめ

	目的	手段	検証	信頼点
電子署名	事後の否認防止	署名	事後の検証 長期検証可能性確保 multi-times verify	パブリックCAが使いやすい
ゼロトラスト	事前のアクセス可否判断	認証 署名（非改竄性・正当性確認）	事前の検証 always verify リモートアテステーション	プライベートCAが適している

- まとめ
  - 電子署名とゼロトラストは目的が大きく異なるため、同じデジタル署名技術でも使い方や要件は当然のことながら大きく異なる。
  - 電子署名は、『トラストサービスが「トラスト」を生み出す原理』で述べたとおり、背景がオープンで「公的」と言う意味で安心。
  - ゼロトラストは上記のような背景はないが、技術的に信頼できる、閉じている、ちゃんとしたベンダーが提供している、と言う意味で安心？。
  - 標準化の重要性への認識も。

ご清聴ありがとうございました。