『デジタルトラストの最新動向と展望』

電子署名とトラスト

2025年10月23日

標準化部会／電子署名WGリーダー
宮崎 一哉

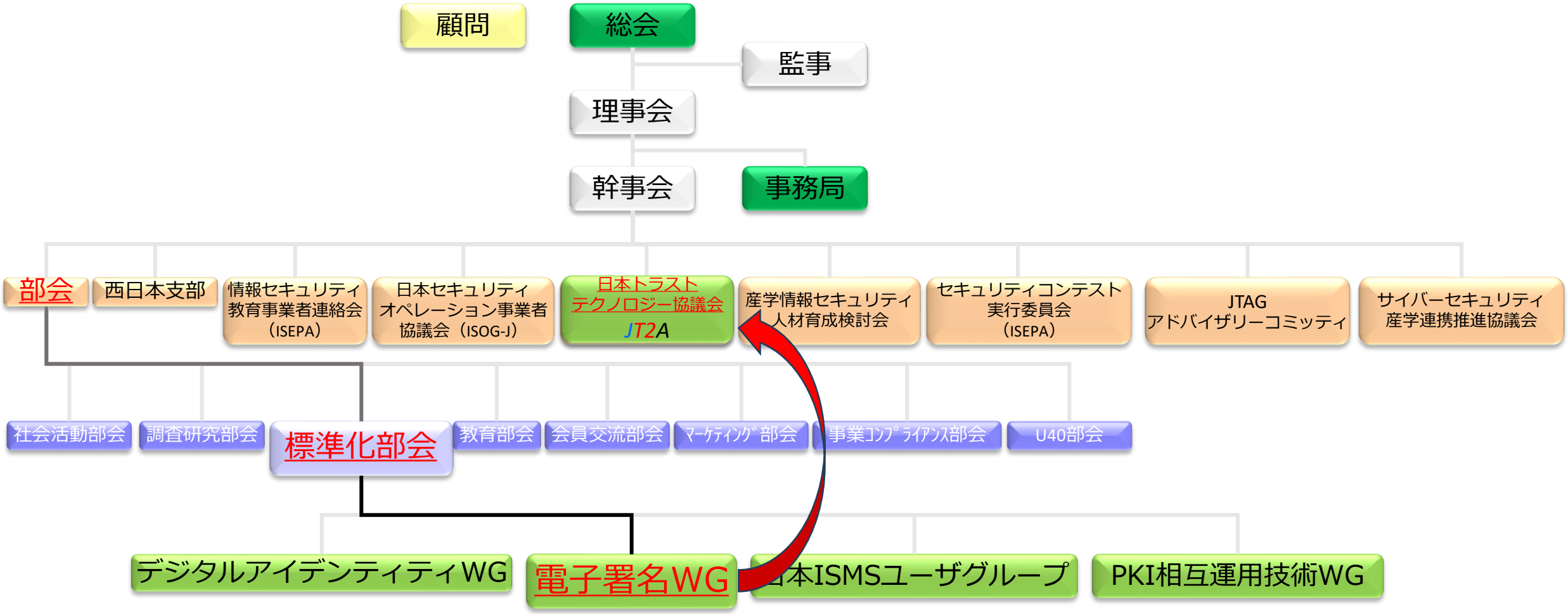
Copyright 2020 NPO日本ネットワークセキュリティ協会

報告内容

1. 電子署名WGの位置付け・設立経緯・構成など
2. 改めて電子署名とは
3. （日本での）電子署名の定義
4. 否認防止
5. 否認防止とメッセージ認証
6. 電子署名の実現技術としてのデジタル署名
7. デジタル署名における「トラスト」の源泉
8. eシールとは
9. トラストサービスの最重要部品としてのデジタル署名
10. トラストサービスが「トラスト」を生み出すメカニズム
11. 電子署名と属性
12. eシール用証明書が企業等の属性証明の枠組みを与える
13. まとめ

Copyright 2020 NPO日本ネットワークセキュリティ協会

1. 電子署名WGの位置づけ



Copyright 2020 NPO日本ネットワークセキュリティ協会

1. 設立経緯

2000　　2013

	2001	2002	2003	2004	2005	2006	2007	2007	2008	2009	2010	2011	2012		2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026

ECOM

電子商取引推進協議会→次世代電子商取引推進協議会

認証・公証WG→・・・→電子署名普及WG

eRAP

JNSA

電子署名WG

電子署名法制定　電子署名法施行

電子署名の相互運用性確保のための調査、検討、仕様作成、標準化、相互運用性テスト、及び電子署名普及啓発を行います。

⇒ 電子署名の総合拠点をめざします。

Copyright 2020 NPO日本ネットワークセキュリティ協会

1. 電子署名WGの構成

JNSA

電子署名WG

9/22付で長期署名プロファイルJIS発行
JIS X 14533-1～3

標準原案作成TF

- 電子署名関連規格の標準化
- ISO/TC154国際審議団体

署名検証TF

- 電子署名検証ガイドライン、標準規格案の作成
- 電子署名検証ツール等の調査

署名保証レベルTF

- 電子署名の保証レベルの検討、ガイドラインの作成

Copyright 2020 NPO日本ネットワークセキュリティ協会

1. 電子署名ＷＧの成果紹介

- 電子署名WGの成果物紹介ページ
  https://www.jnsa.org/result/e-signature/index.html
  - 「電子署名Q&A」など電子署名WGの成果を公開しています。
- 電子署名WGの紹介資料
  - JNSA Press 第52号 https://www.jnsa.org/jnsapress/vol52/3_WG.pdf
  - 〃　第45号 https://www.jnsa.org/jnsapress/vol45/3_WG-1.pdf
  - 〃　第37号 https://www.jnsa.org/jnsapress/vol37/5_WG.pdf
  - 情報処理学会デジタルプラクティス　Vol.9 No.3 (July 2018)
    「ディジタル社会のトラストを支える電子署名」
    https://www.ipsj.or.jp/dp/contents/publication/35/S0903-S05.html

Copyright 2020 NPO日本ネットワークセキュリティ協会

2. 改めて電子署名とは

- 認証とは違う

- 認証

  ユーザーやデバイスが正当なアクセス権を持っているかどうかを確認するプロセス（識別→認証→認可）

- 電子署名

  紙の文書における押印や手書き署名に相当するもの

  電子文書における本人性の証明と非改ざん性を保証するもの＋α

Copyright 2020 NPO日本ネットワークセキュリティ協会

3.（日本での）電子署名の定義

- 日本における電子署名＝電子署名法での定義

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（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）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。

本人性の証明

非改ざん性の保証

＋α

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。

Copyright 2020 NPO日本ネットワークセキュリティ協会

4. 否認防止

- 真正な成立の推定

作成者の意思：その文書が作成者本人の意思に基づいて作成されたものであること。
証拠としての信頼性：文書が偽造や改ざんされたものではなく、本物であること。
　　⇒反証がない限り真実とみなされる（推定）

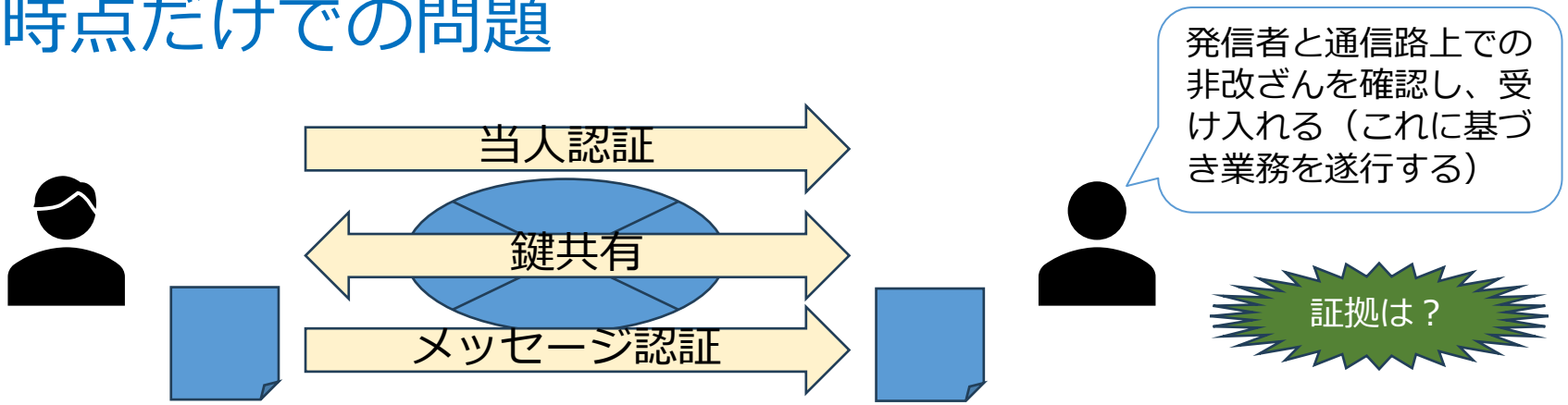
≒否認防止
『自分が意思に基づいて作成したそのものではない』と本人が否定できない（認めないことができない）

その場その時点だけでの問題ではなく、それ以降の継続（永続）的な問題

Copyright 2020 NPO日本ネットワークセキュリティ協会

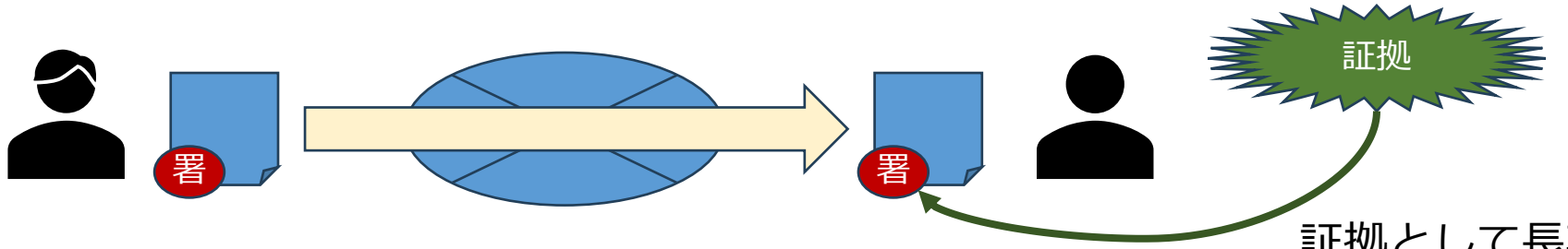
5. 否認防止とメッセージ認証

- その場その時点だけでの問題



- それ以降の継続（永続）的な問題

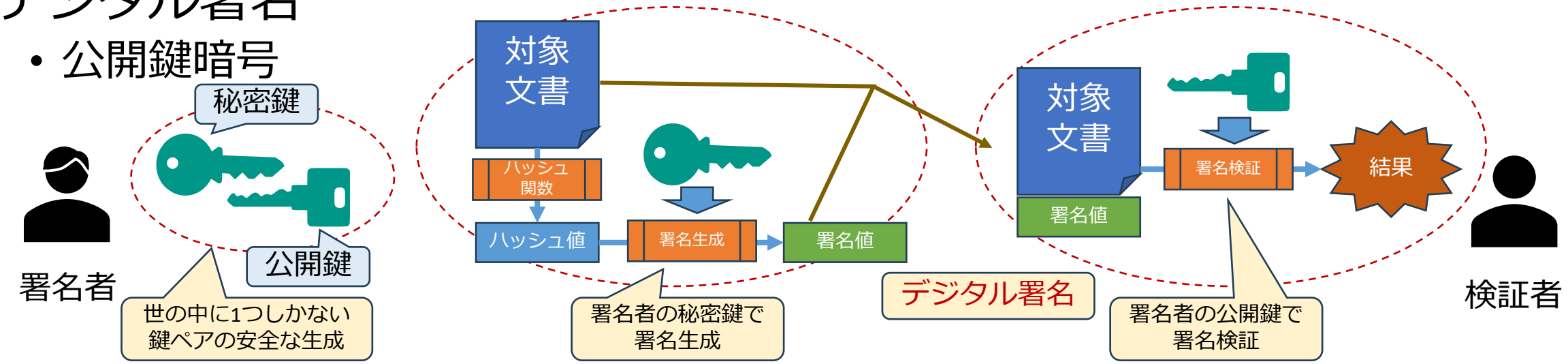
あの時のあの業務は正当だったのか？



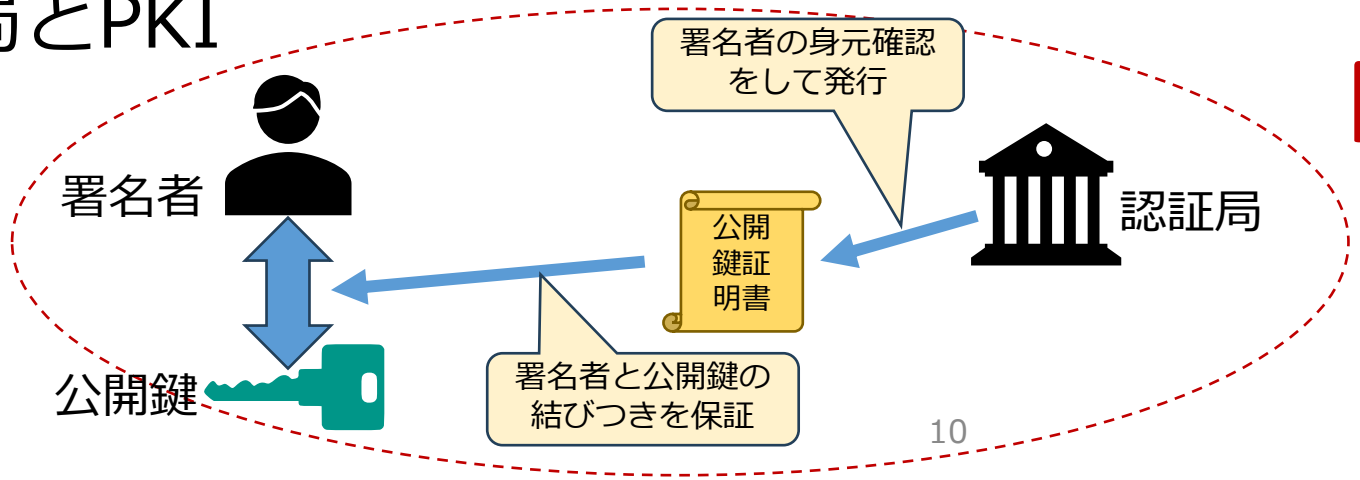
Copyright 2020 NPO日本ネットワークセキュリティ協会

6. 電子署名の実現技術としてのデジタル署名

- デジタル署名
  - 公開鍵暗号



- 認証局とPKI

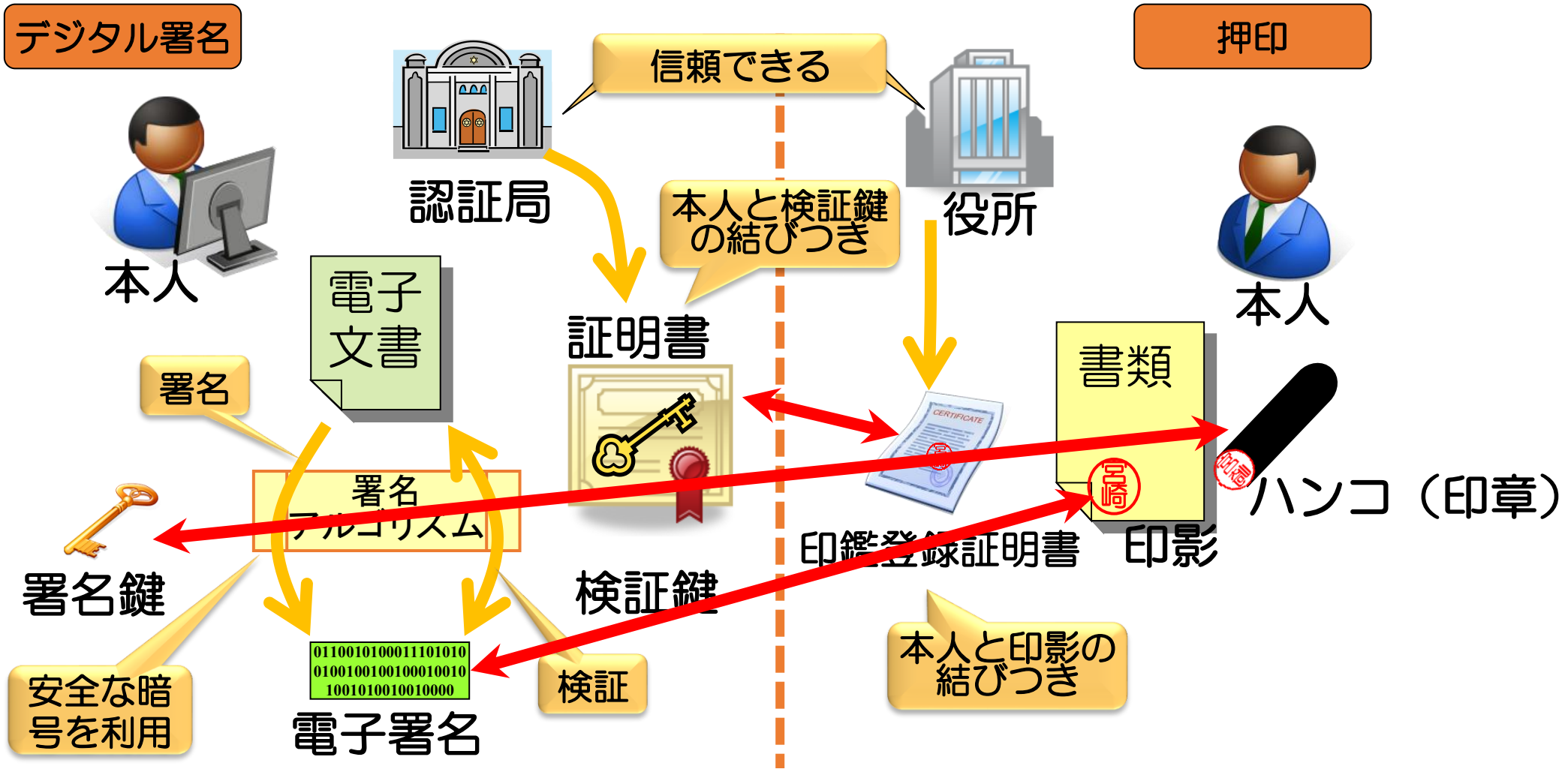


PKI

認証局の発行する証明書に基づき、公開鍵暗号により安全なITを形成する基盤（適用は署名だけではない）

Copyright 2020 NPO日本ネットワークセキュリティ協会

7. デジタル署名における「トラスト」の源泉



Copyright 2020 NPO日本ネットワークセキュリティ協会

8. eシールとは

- ｅシールに係る指針（第２版）（令和６年４月　総務省）

  ｅシールは、企業等が発行する電子データの発行元を証明し、また、電子データに改ざんがないことを証明できるようにするために用いられる。

- eシールに係る認証業務の認定に関する規程を定める件
  （令和7年総務省告示第113号）

  「ｅシール」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録された情報（以下「電子データ」という。）に付与された又は論理的に関連付けられた電子データであって、次の要件のいずれにも該当するものをいう。
  一 当該情報の出所又は起源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確認することができるものであること。

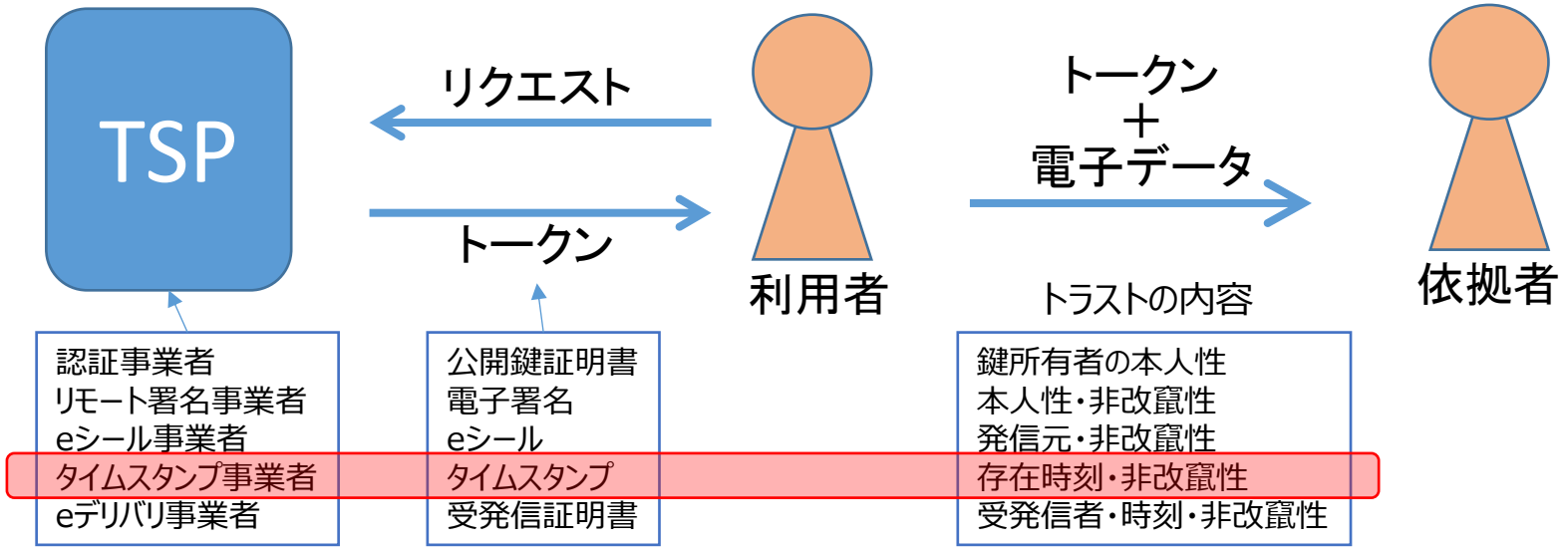
  企業等の本人性証明

  非改ざん性の保証

- 電子署名法の第三条に相当するものはない。
  　　が、否認はできない！
- 仕組みは電子署名と同様、PKIに基づくデジタル署名を利用。

Copyright 2020 NPO日本ネットワークセキュリティ協会

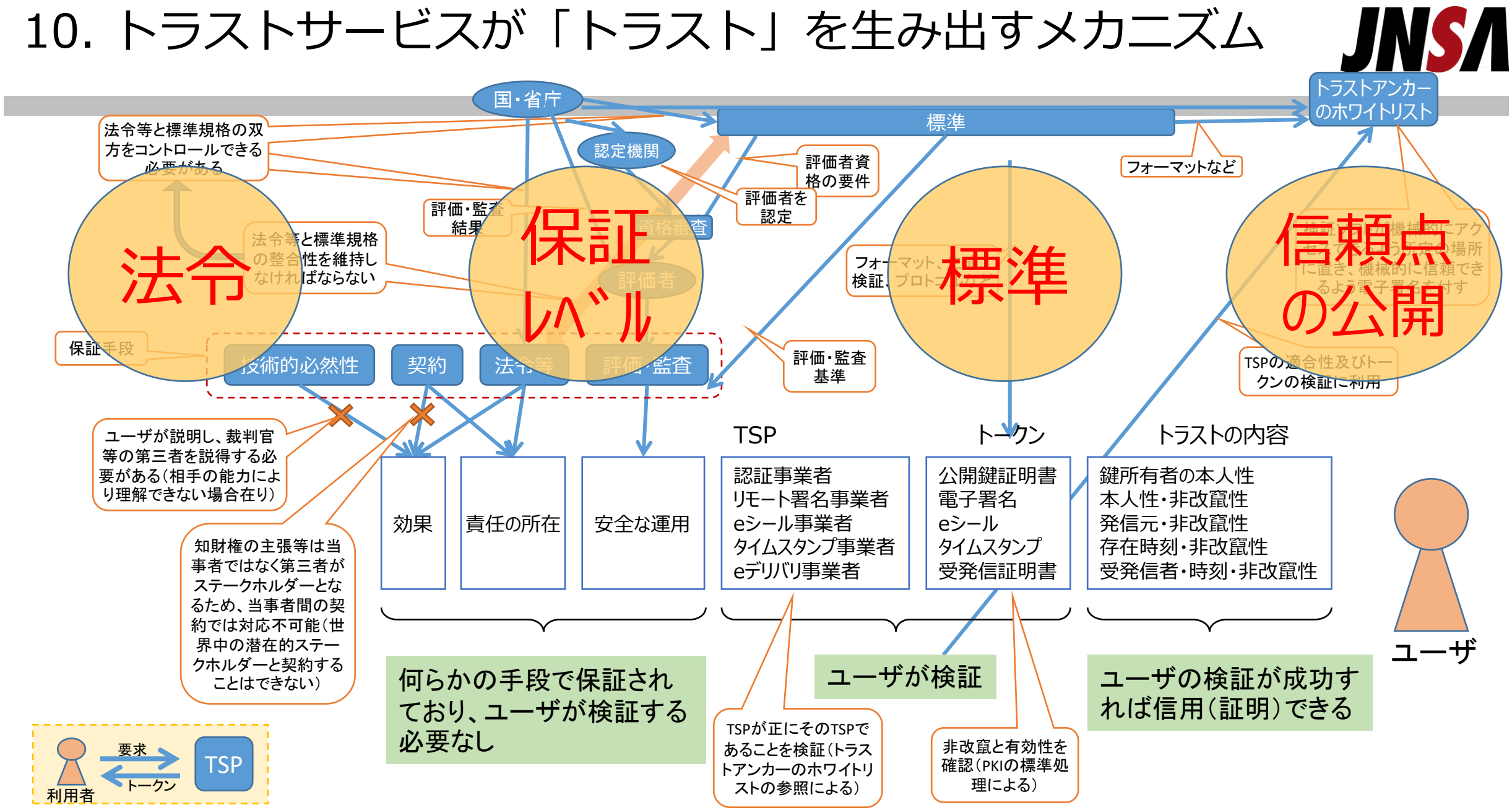
9. トラストサービスの最重要部品としてのデジタル署名



- 利用者は、電子データに関するある種の「トラストの内容」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。
  例）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、依拠者にその情報の存在時刻を証明する。
- TSPはサービス内容により、トラストの内容を表すトークンにeシール（デジタル署名）を付与して利用者に提供する。
- 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、「トラストの内容」を受け入れる。
- TSPの信頼性は認定・認証や保証レベルで確認できる。
- 検証手段は標準化、公開され、自動化や万人による評価が可能である。

Copyright 2020 NPO日本ネットワークセキュリティ協会

10. トラストサービスが「トラスト」を生み出すメカニズム



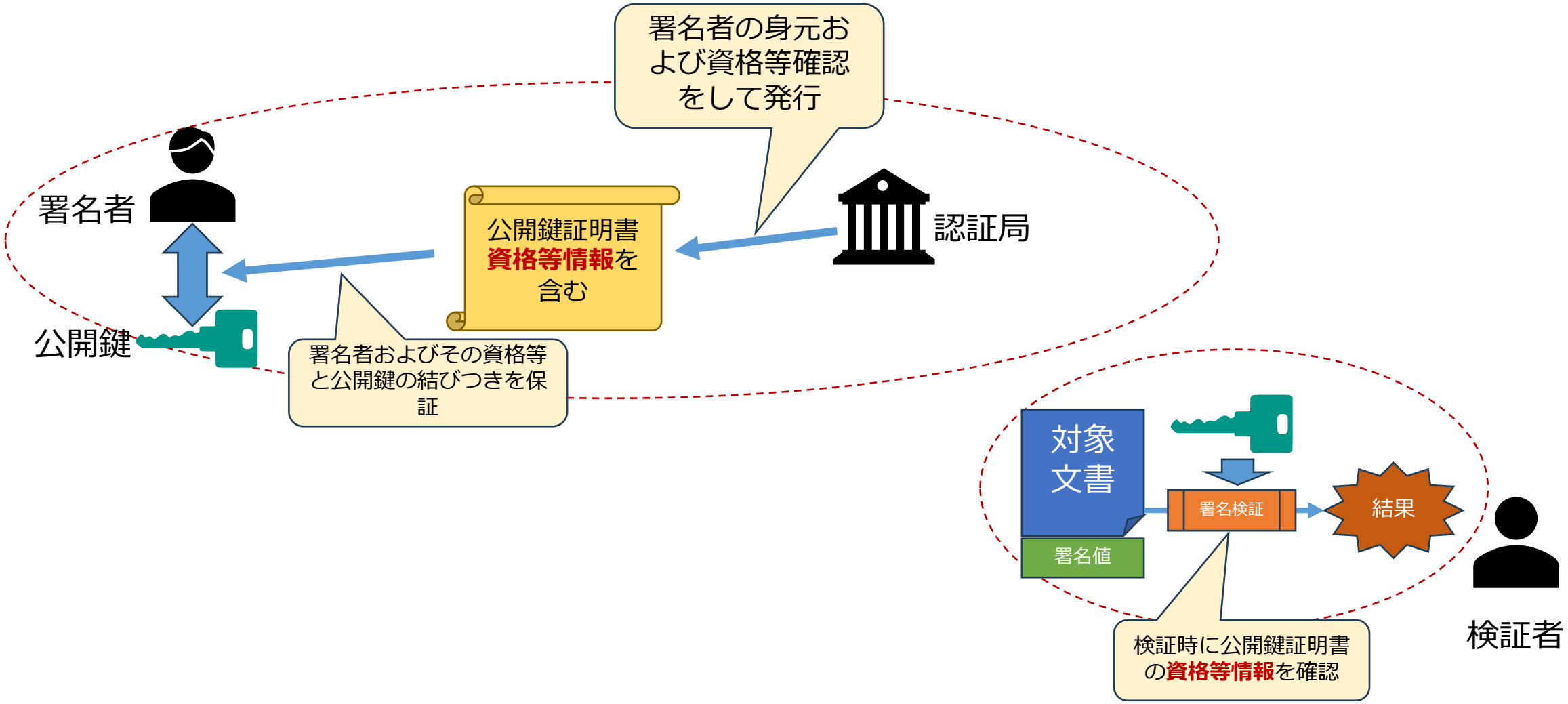
11. 電子署名と属性－公開鍵証明書に属性を記載

- 認定認証業務と属性
  - 電子署名法で規定される範囲は本人性まで（資格は範囲外）
- 士業資格の証明書
  - 認定認証業務より発行される公開鍵証明書に士業資格や登録番号などを格納し、署名者の資格を保証（認証局のポリシーで登録時に身元の証明書のほか、資格の証明書を要求。資格を管理する組織からの資格失効情報を得ての失効処理も実施。）
- HPKI
  - 公開鍵証明書に、国際標準規格*で規定されるhcRoleに医師国家資格等に関する情報を格納し、署名者の資格を保証

    *“ISO 17090-2:2015 Health informatics — Public key infrastructure — Part 2: Certificate profile”
- 電子委任状
  - 受任者であり署名者の公開鍵証明書に、代理権限や役職等を格納（令和５年５月10日デジタル庁告示第７号「電子委任状の普及を促進するための基本的な指針」の電子証明書方式）

Copyright 2020 NPO日本ネットワークセキュリティ協会

11. 電子署名と属性－公開鍵証明書に属性を記載



Copyright 2020 NPO日本ネットワークセキュリティ協会

11. 電子署名と属性－「属性証明書」を利用

- Attribute Certificate（属性証明書）
  - 属性認証局が署名者の公開鍵証明書と属性を関連付けた属性証明書を発行。

    -X.509：Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (2019/10/14)

    -RFC5755：An Internet Attribute Certificate Profile for Authorization (2010/01)

- EAA：Electronic Attestation of Attributes（電子属性証明）
  - 属性プロバイダが、属性と本人の公開鍵証明書を関連付けた属性証明書を発行。

    -eIDAS 2.0：REGULATION (EU) 2024/1183：amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (2024/4/11)

    -ETSI TS 119 472-1 V0.0.11 (2025-10): Profiles for Electronic Attestation of Attributes; Part 1: General requirements

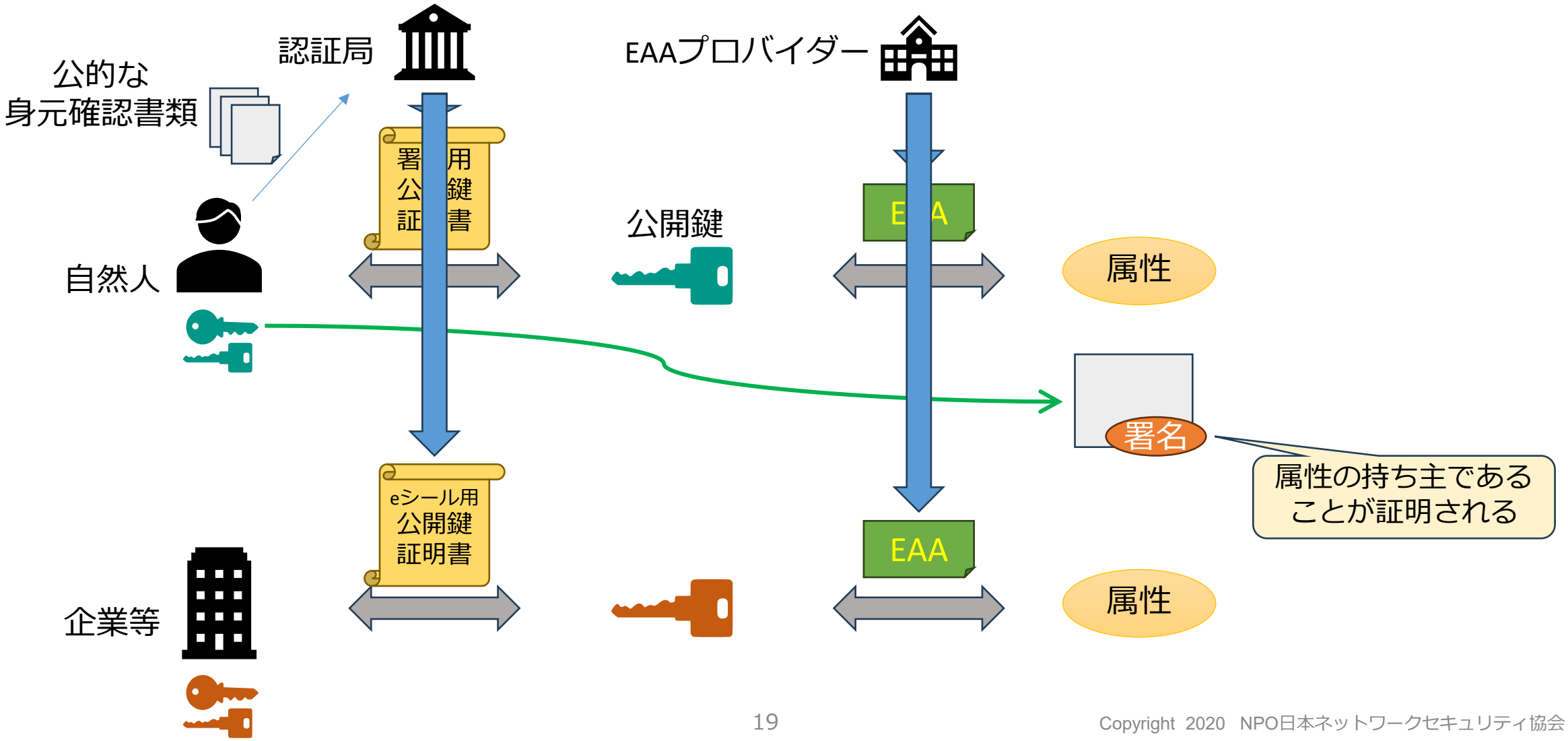
    - ETSI TS 119 472-2 V0.0.5 (2025-10): Profiles for Electronic Attestation of Attributes; Part 2: Profiles for EAA/PID Presentations to Relying Party

Copyright 2020 NPO日本ネットワークセキュリティ協会

11. VCの利用例（ACもよく似ている）

Copyright 2020 NPO日本ネットワークセキュリティ協会

12. eシール用証明書⇒企業等の属性証明の枠組み



Copyright 2020 NPO日本ネットワークセキュリティ協会

13. まとめ

- 電子署名の本質は否認防止（eシールも同様）
- デジタル署名およびPKIは電子署名実現のメカニズム
  ⇒トラストサービス実現のメカニズム＝トラストメカニズム
- AC、EAAは（署名者）本人と属性の関連付けのメカニズム
  ⇒hcRoleも電子委任状もEAAで実現可能
- eシール（用証明書）により企業等の属性を証明する枠組みを実現

- 現状ではPKIにより属性の取扱いも無理なく可能だが、PQC移行後の姿がどのようになるのかを描くことが急務！

Copyright 2020 NPO日本ネットワークセキュリティ協会

ご清聴ありがとうございました

Copyright 2020 NPO日本ネットワークセキュリティ協会