

日本のサイバーセキュリティを「連携」「学び」「創造」



電子署名ワーキンググループの 活動紹介

2025年7月23日
標準化部会／電子署名WG
(三菱電機株式会社)
宮崎一哉

1. 経緯・位置付け
2. 標準原案作成タスクフォース
3. 署名検証タスクフォース
4. 署名保証レベルタスクフォース
5. その他の活動
6. おわりに

1. 発足の経緯



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

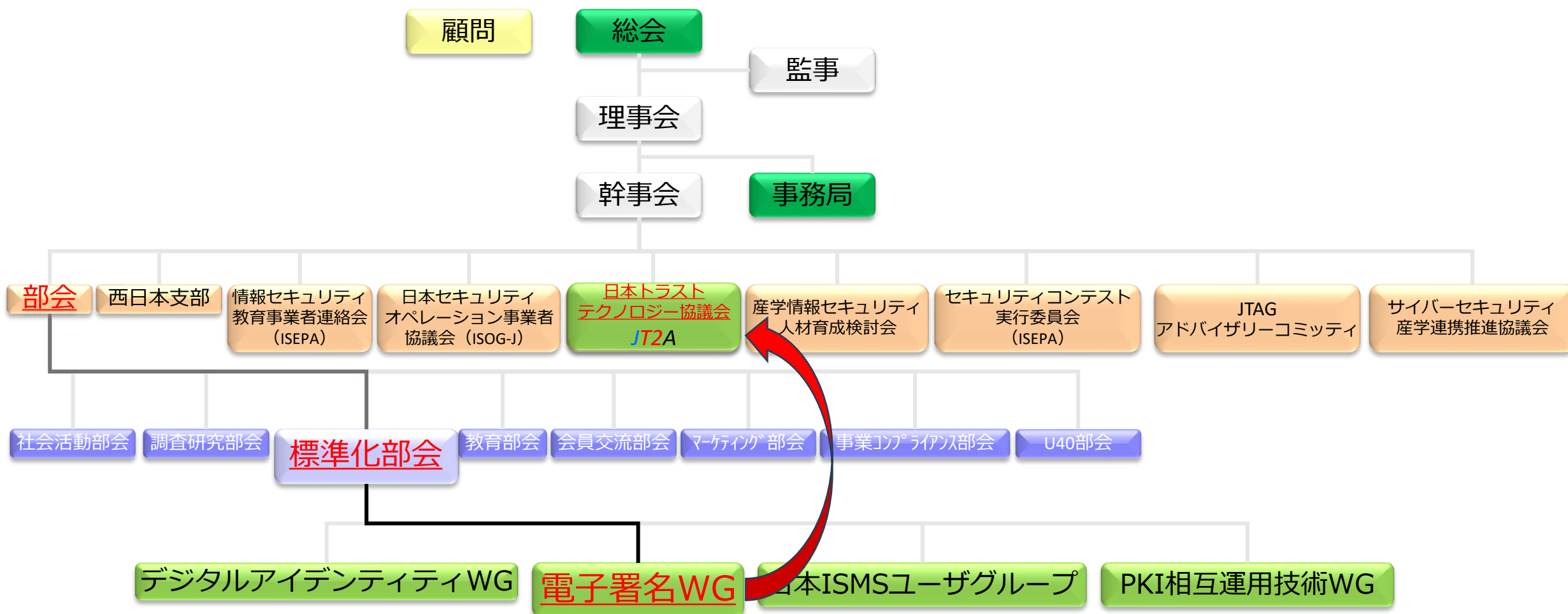
電子署名WG

電子署名法施行
電子署名法制定

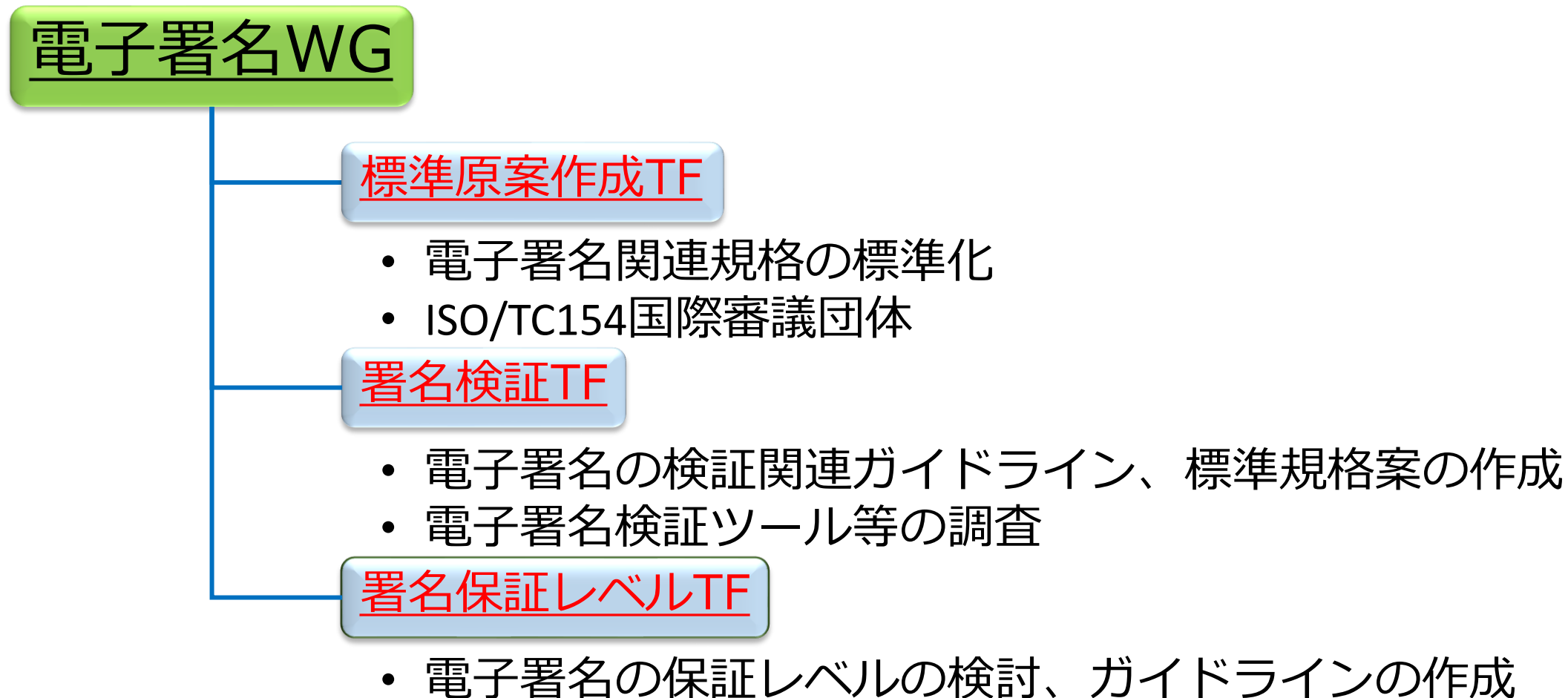
電子署名の相互運用性確保のための調査、検討、仕様作成、標準化、相互運用性テスト、及び電子署名普及啓発を行います。

⇒ **電子署名の総合拠点をめざします。**

1. 電子署名WGの位置づけ



1. 電子署名WGの構成



2. 標準原案作成タスクフォース

- 活動目的と概要

- デジタル署名はデータの真正性を担保し、安全なデジタル社会を築くための重要な技術です。幅広い用途に適用し、活用を広げていくためにはデジタル署名の相互運用性の確保が不可欠です。
- 署名原案作成タスクフォースは、デジタル署名の信頼性や相互運用性を確保することを目的に、ISOやJISなど標準規格の原案作成や標準化活動の促進を行います。これまでもデジタル署名の長期署名プロファイルのISO規格化などを実現しています。

2. 標準原案作成タスクフォース



• 主な活動内容

長期署名プロファイル (ISO 14533シリーズ)

デジタル署名の有効性を長期に担保し、相互運用性を確保するためのプロファイル規格です。デジタル署名のフォーマット形式の違いによりPart 1 (CAAdES), Part2 (XAdES), Part3 (PAdES) が策定されています。

Part1～Part3の原案は本TFに参加するエキスパート達で作成してきました。

2023年から2025年にかけて

Part3(PAdES)の改訂作業を行っています。

NEW

長期署名プロファイル (JIS X 14533シリーズ[予定])

長期署名プロファイルのJIS規格版です。内容はISO 14533シリーズ (Part1～Part3)と同等のものとなっています。これまでJIS X 5092 (CAAdES), JIS X 5093 (XAdES)が策定されていましたが、最新のISO規格の内容と構成に合わせ、新たにJIS 14533シリーズとして生まれ変わる予定です。本TFではJIS原案作成委員会を構成し、原案作成を推進しました。

ISO/TC 154国内審議委員会 事務局運営支援

JNSAではISO/TC 154 (商業、産業、行政におけるプロセス、データ要素、文書)の国内審議委員会の運営を行っています。ISO/TC 154では電子取引に関わる様々な規格の策定を行っており、ISO 14533シリーズもその一つです。本TFでは円滑な標準化活動を促進するため、ISO/TC 154 国内審議委員会の事務局運営を支援しています。

2. 標準原案作成タスクフォース



- これからの活動

- ISO/TC 154では様々な規格が提案されております。デジタル署名の信頼性と相互運用性をより向上させることを目指し、規格策定の議論に積極的に関与していきます。
- 日本からの提案もより推進していきます（標準化の先はISOやJISに限りません）。標準化のあるべき方向性、標準化すべき事項の整理、規格原案の内容など様々な観点の議論があります。
- 皆様からの積極的なご提案やご参加をお待ちしております。

3. 署名検証タスクフォース



• これまでの活動

- 署名検証タスクフォースは、**デジタル署名**の信頼性確保と普及を目的に、**検証方法**や**トラスト要素**を解説する文書を公開しています。**専門家以外**にも理解しやすい形で署名技術と検証指針を示し、電子取引の円滑化を支援しています。

デジタル署名検証ガイドラインv1.1 (2023.12.20改訂)

電子署名は様々な要素から構成されており、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基盤（PKI）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/2021/index.html>

トラストのためのデジタル署名検証解説 (2023.12.22)

電子署名方式について紹介し、標準化の進んでいるデジタル署名について、単なる検証処理だけでは確認できないトラストの要素について解説します。デジタル署名技術の専門家ではない利用者向けの導入から、最新の技術動向まで幅広く記載しています。

<https://www.jnsa.org/result/e-signature/2023/index.html>

3. 署名検証タスクフォース

• これからの活動

- 電子契約の普及により、PDF署名が一般化しつつあります。
それに伴い、PDF署名検証の重要性も一層増しています。
しかし、アプリが示す検証結果はユーザーを混乱させる可能性があります。
特にエラー表記やワーニング表記については不安にさせ、
電子契約利用の障壁となり得ます。
- この課題を解決するため、主要なPDFエディタやビューワを用いて署名と検証の
相互テストを実施し、問題の有無や注意点を明らかにする活動を行います。

検証の重要性 と 利用者の困惑:

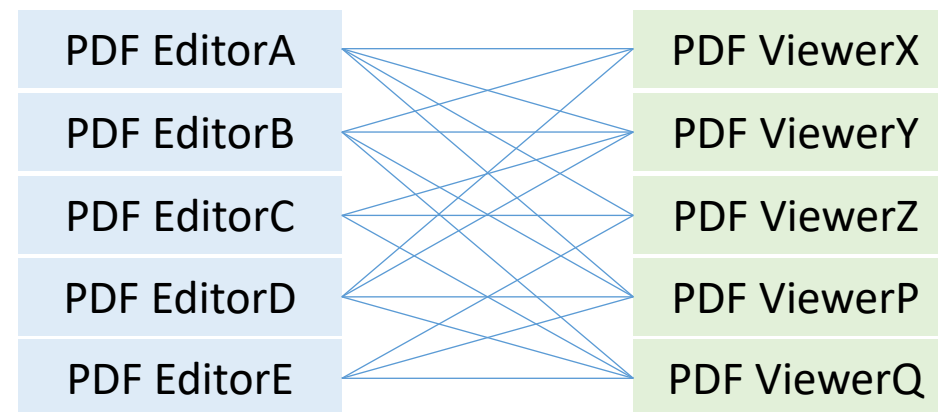
署名の有効性を確認する「署名検証」は不可欠。

しかし、検証が失敗（パスしない） ケースもある。

→ 「署名が無効です」 「文書が変更されています」

これらのメッセージは、何が問題なのか？ どのように
対処すべきなのか？ がわからず、電子契約の利用に対
する不信感や抵抗感に繋がりがねません。

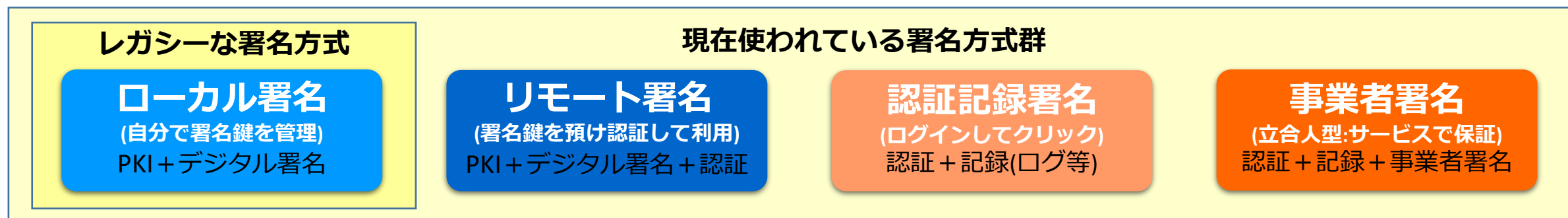
テストのイメージ



4. 署名保証レベルタスクフォース

TFの目的：署名方式に依存しない電子署名の保証レベルを策定する！

背景1：様々な署名方式が使われるようになった（電子署名ってなんだっけ？）

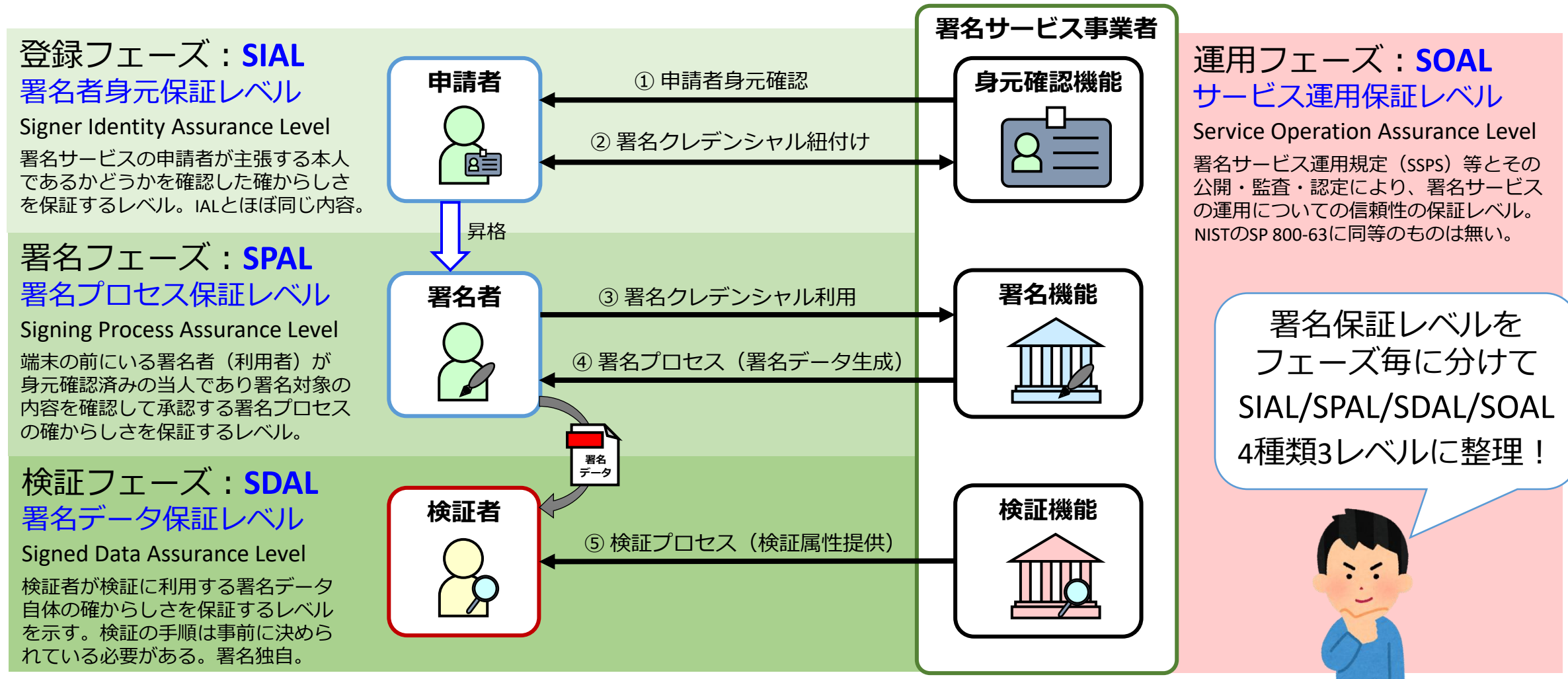


背景2：認証世界のNIST SP 800-63による保証レベルの広がり（保証レベル便利！）

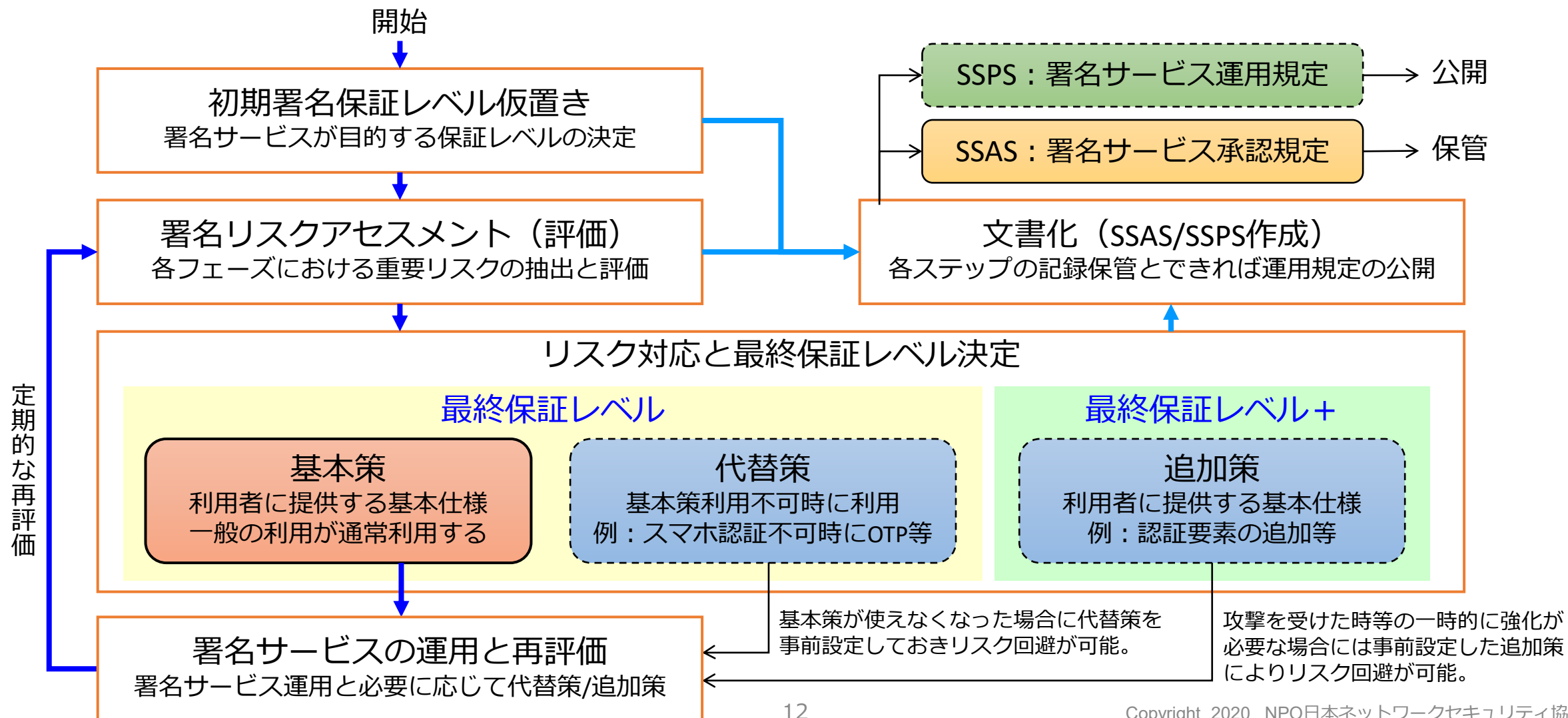


結論：様々な署名方式と電子署名の要素を整理した上で電子署名の技術保証レベルが必要！

4.1 保証レベルTF: 4つの署名保証レベル



4.2 保証レベルTF: 電子署名リスク管理-ESRM



4.3 保証レベルTF: JNSA署名保証ガイドライン



JNSA SAG-1:2025
Draft Version



署名保証ガイドライン (Signature Assurance Guidelines)

第 1.00 版
(Ver 1.00)

2025 年 X 月 X 日
(2025/X/X)

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
(JNSA Electronic Signature Working Group)

概要

1. はじめに
 - 1.1. スコープ
 - 1.2. 構成
 2. 署名モデル
 - 2.1. 概要
 - 2.2. 電子署名の定義
 - 2.3. 署名方式の整理
 - 2.3.1. ローカル署名方式
 - 2.3.2. リモート署名方式
 - 2.3.3. 認証記録署名方式
 - 2.3.4. 事業者署名方式
 - 2.4. 電子署名の保証レベル
 - 2.4.1. 署名者身元 (Signer Identity) 保証: SIAL
 - 2.4.2. 署名プロセス (Signing Process) 保証: SPAL
 - 2.4.3. 署名データ (Signed Data) 保証: SDAL
 - 2.4.4. サービス運用 (Service Operation) 保証: SOAL
 3. 電子署名のリスク管理 (ESRM)
 - 3.1. 概要
 - 3.2. ステップ 0: 保証レベルの仮置き
 - 3.3. ステップ 1: リスクアセスメント実施
 - 3.4. ステップ 2: リスク対応と最終保証レベルの決定
 - 3.5. ステップ 3: 文書化 (SSAS/SSPS作成)
 - 3.6. ステップ 4: 署名サービス運用と再評価
- 付属書A. 署名保証レベル適合宣言書 (規定)
付属書B. 承認目的署名と発行元保証署名 (参考)
付属書C. 電子委任 (参考)
付属書D. トラスト設計 (参考)

2025年(今年)公開予定！
現在仕上げ作業中です！
乞うご期待！！



5. その他の活動

- JAHIS（一般社団法人保健医療福祉情報システム工業会）
電子署名規格作成WGへの技術協力
 - JAHIS標準
『JAHISヘルスケアPKIを利用した医療文書に対する電子署名規格Ver.3.0』 など
 - ISO17090-4
“Health informatics — Public key infrastructure
Part 4: Digital signatures for healthcare documents”
- ISO/SC34（文書の記述と処理の言語/ Document Description and Processing Languages）への技術協力
 - OOXML、ODF等への電子署名規格の作成支援等
- ETSI/TC ESI（欧州電気通信標準化機構／電子署名基盤技術委員会）メンバー
 - 電子署名規格標準化に向けての仕様調整等

6. おわりに

- 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>

6. おわりに

- 20年以上にわたり電子署名に関わってきましたが、未だ課題は尽きません。
- いわゆる立会人型署名などの新たな電子署名方式も普及し始めていますが、どのように評価したり適否の判断をしたりすればよいのかは定着していません。
- また、CAdES、XAdES、PAdESに加え、JAdES、CB-AdESなどの新たな署名形式の検討も始まり、PQCが電子署名に与える影響も気になるところです。
- 今後、電子署名保証要件の整備をはじめ、新たな技術の出現に適応できるガイドラインや標準規格の作成に向けて活動を継続していきます。
- 皆さま、少しでもご興味ありましたら仲間に加わってみませんか？



ご清聴ありがとうございました