電子署名WG成果報告

デジタル署名検証の意義とガイドライン

2021.09.17

電子署名WG　TFリーダー
政本 廣志

アジェンダ

【0】はじめに
【1】デジタル署名の標準化
【2】署名検証の取り組みと経緯
【3】2020年度の活動の狙い
【4】ガイドラインの概要と要点
【5】今後の活動

【0】はじめに

はじめに

JNSA
- 標準化部会
  - 電子署名WG
    - 標準原案作成TF
    - 署名検証TF
    - 保証レベルTF(立ち上げ中)

2020年度は、

電子署名を取り巻く環境が激動した年

として、歴史に残るかも。
そんな出来事を３つ。

① 脱ハンコ

電子署名法制定以来20年、進まなかったことが、一気に進む(かも)

① 脱ハンコ

- リモートワークを阻むハンコの廃止
  - 単に廃止すれば良いのでしょうか？
- 電子署名の活用
  - 使いにくい？普及していない？
- 様々な電子署名形態の発生

② リモート署名

電子署名の課題の１つを解決する取り組み。

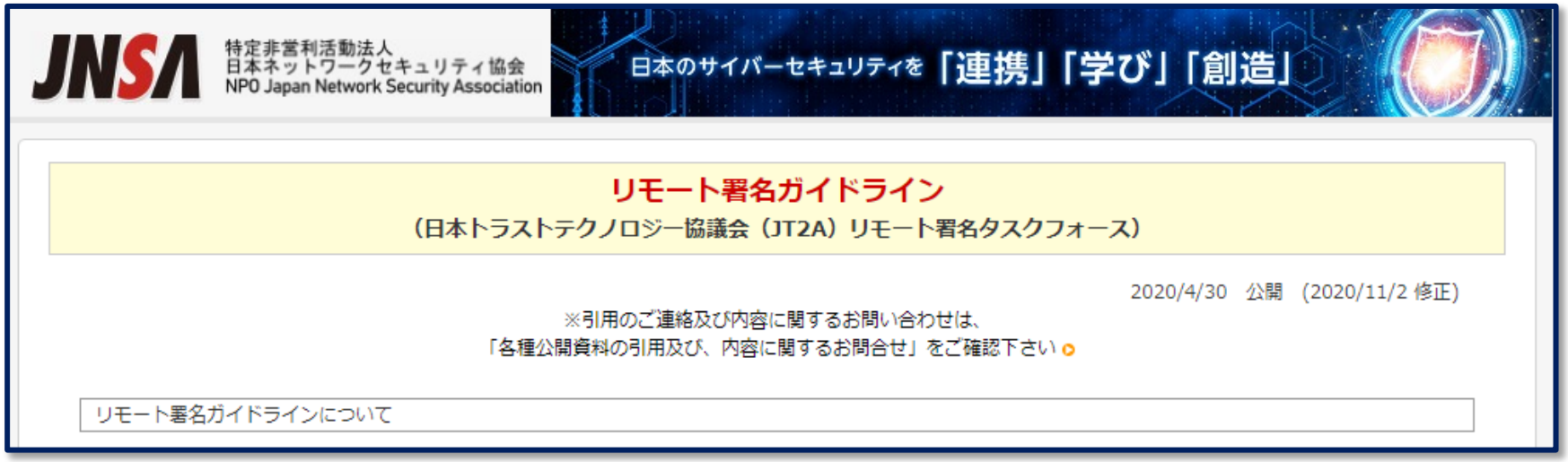
② リモート署名

- リモート署名ガイドラインの発行

2020年4月30日「リモート署名ガイドライン」を公開しました。

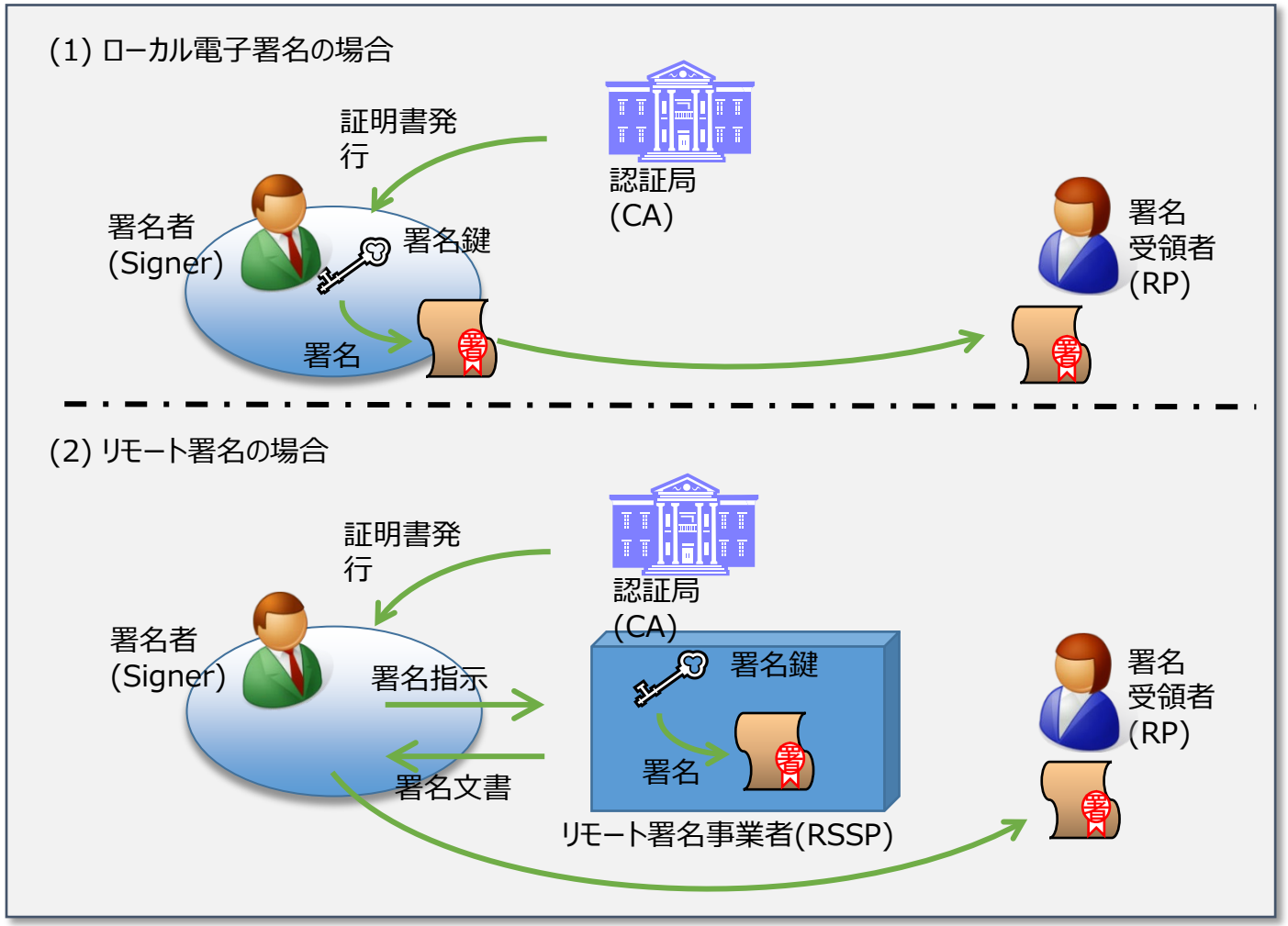
リモート署名TFの成果物「リモート署名ガイドライン」を公開しました。
リモート署名TFでは今後必要に応じて更新していく予定です。

http://www.jt2a.org/



https://www.jnsa.org/result/jt2a/2020/index.html

リモート署名とは (1)



リモート署名ガイドライン（2020.4.30；日本トラストテクノロジー協議会(JT2A)）より

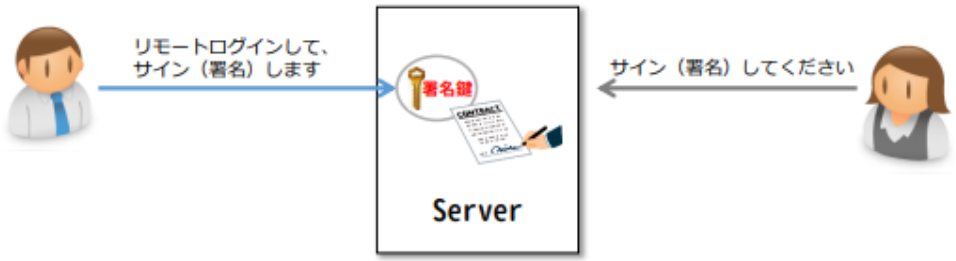
リモート署名とは (2)

1.リモート署名とはなにか？

JNSA

リモート署名の定義※

事業者のサーバに利用者（エンドエンティティ）の署名鍵を設置・保管し、利用者がサーバにリモートでログインし、自らの署名鍵で事業者のサーバ上で電子署名を行うこと。



電子署名及び認証業務に関する法律（平成１２年法律第１０２号）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。

※電子署名法研究会（METI/経済産業省）
http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#denshishomeihou

3

リモート署名の検討状況　2017年1月23日　小川（https://www.jnsa.org/seminar/nsf/2017/data/NSF2017_B1-2_ogawa.pdf）

③ 立会人型署名

新しい電子署名形態の登場!?

③ 立会人型署名

- ３省Q&Aの発表･･･新解釈!

１．電子署名の活用促進について

○ 電子署名法の制定当初は想定されていなかったクラウド型の電子署名が登場し、普及が進みつつある。

○ 押印の代替手段の１つである電子署名の活用を促進するため、クラウド型の電子署名のうち、特にサービス提供事業者が利用者の指示を受けて電子署名を行うサービスについて、所管３省において電子署名法における位置付けの明確化を行った。（総務省、法務省、経産省の連名で７月17日に２条関係、９月４日に３条関係のＱ＆Ａを公表）

電子署名法第３条に関するＱ＆Ａについて（令和２年10月14日） 内閣府 規制改革推進室
https://www.fsa.go.jp/singi/shomen_oin/shiryou/20201014/01.pdf

ちなみに、電子署名法では、

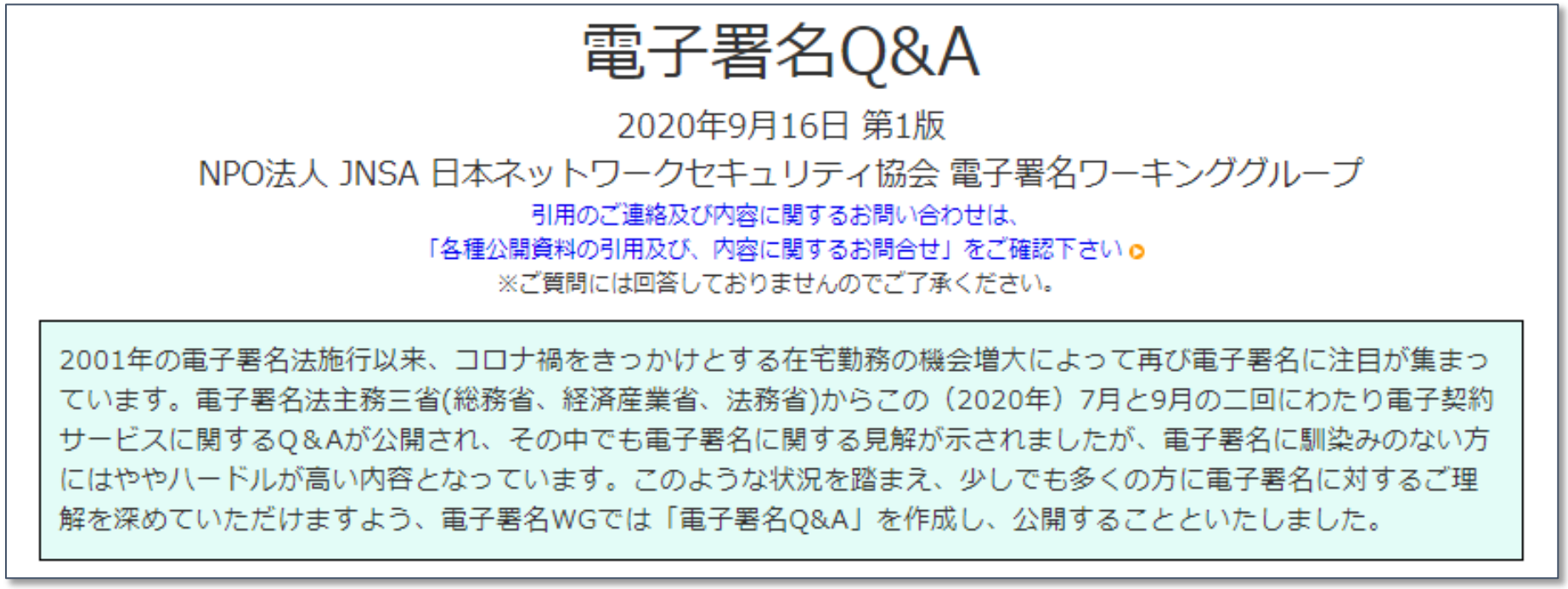
- 電子署名法第2条1項
  - 　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。
  - 一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
  - 二　当該情報について改変が行われていないかどうかを確認することができるものであること。
- 電子署名法第3条
  - 　電磁的記録であって情報を表すために作成されたもの（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。

署名の定義

署名の効果/目的/条件

真正に成立する条件

業界の反応 (1)



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。

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

業界の反応 (2)

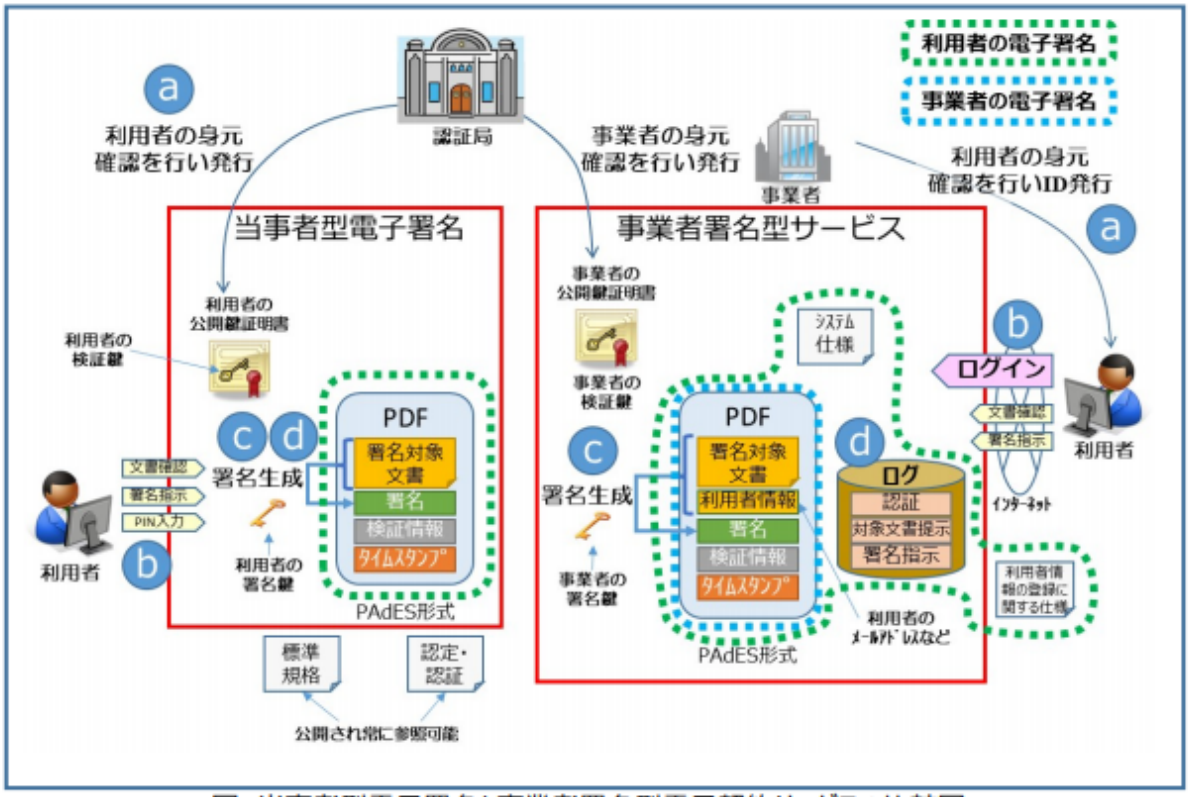


図　当事者型電子署名と事業者署名型電子契約サービスの比較図

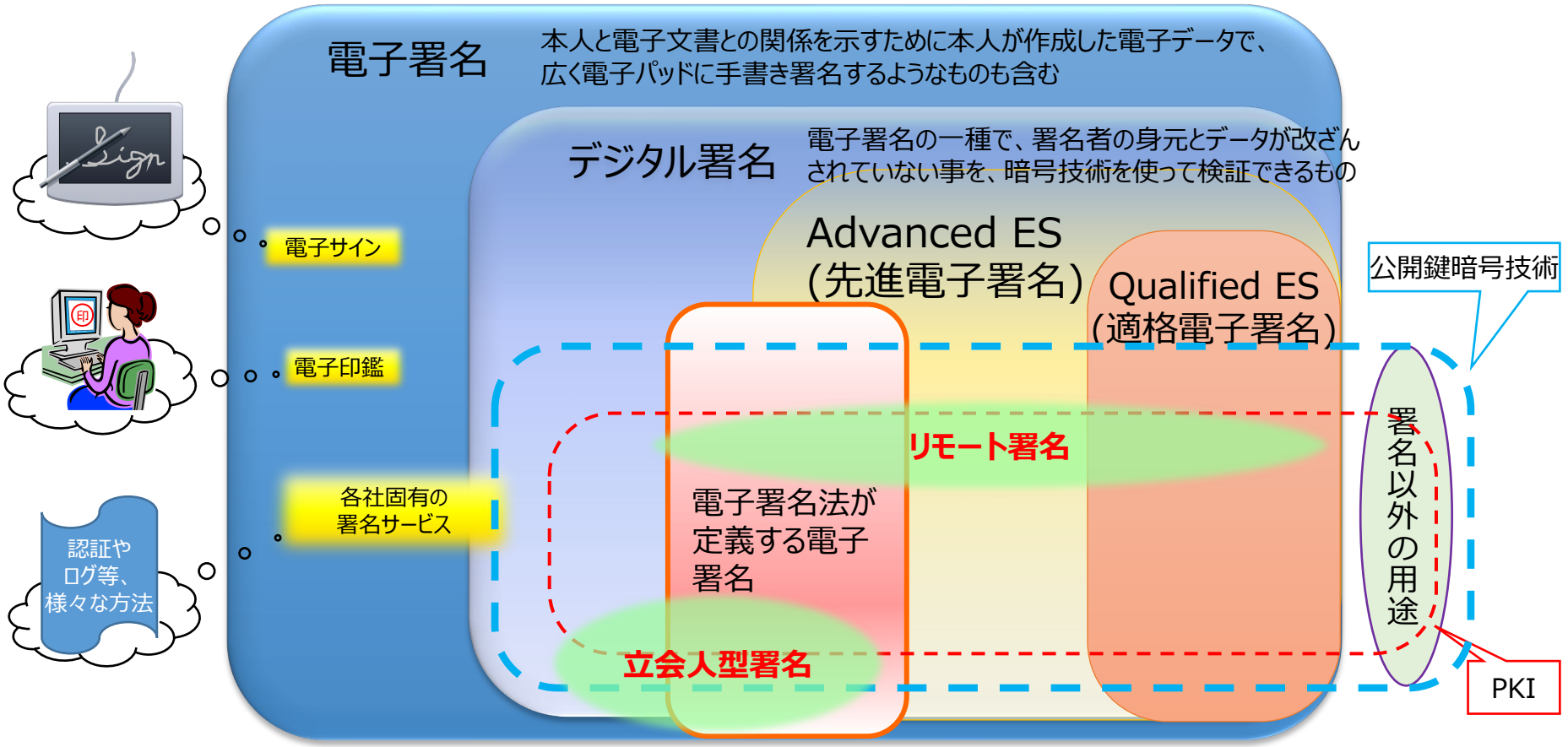
[6] JNSA 2019-2020 年度活動報告会（2020 年 11 月 26 日）標準化部会電子署名 WG リーダー　宮崎一哉氏　発表資料より抜粋、一部加筆

「主務三省 Q&A（電子署名法第 3 条関係）に関する解説」（TSF & CACより）

https://www.dekyo.or.jp/tsf/wp-content/uploads/2021/02/%E9%9B%BB%E5%AD%90%E7%BD%B2%E5%90%8D%E6%B3%95Q%EF%BC%86A%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E8%A7%A3%E8%AA%AC.pdf

まとめると、

- 様々な電子署名と関連技術の関係（イメージ）



2016年度 活動報告会 宮崎氏資料を基に加工
https://www.jnsa.org/seminar/2017/0612/data/A3-2.pdf

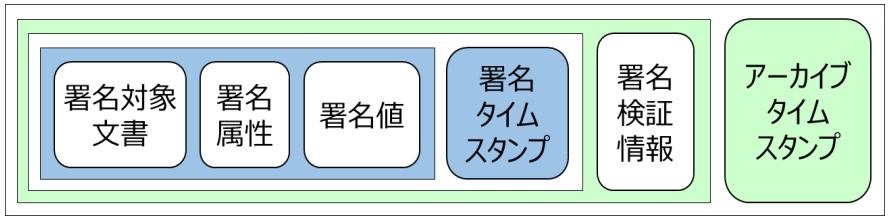
【1】デジタル署名の標準化

標準化のターゲット

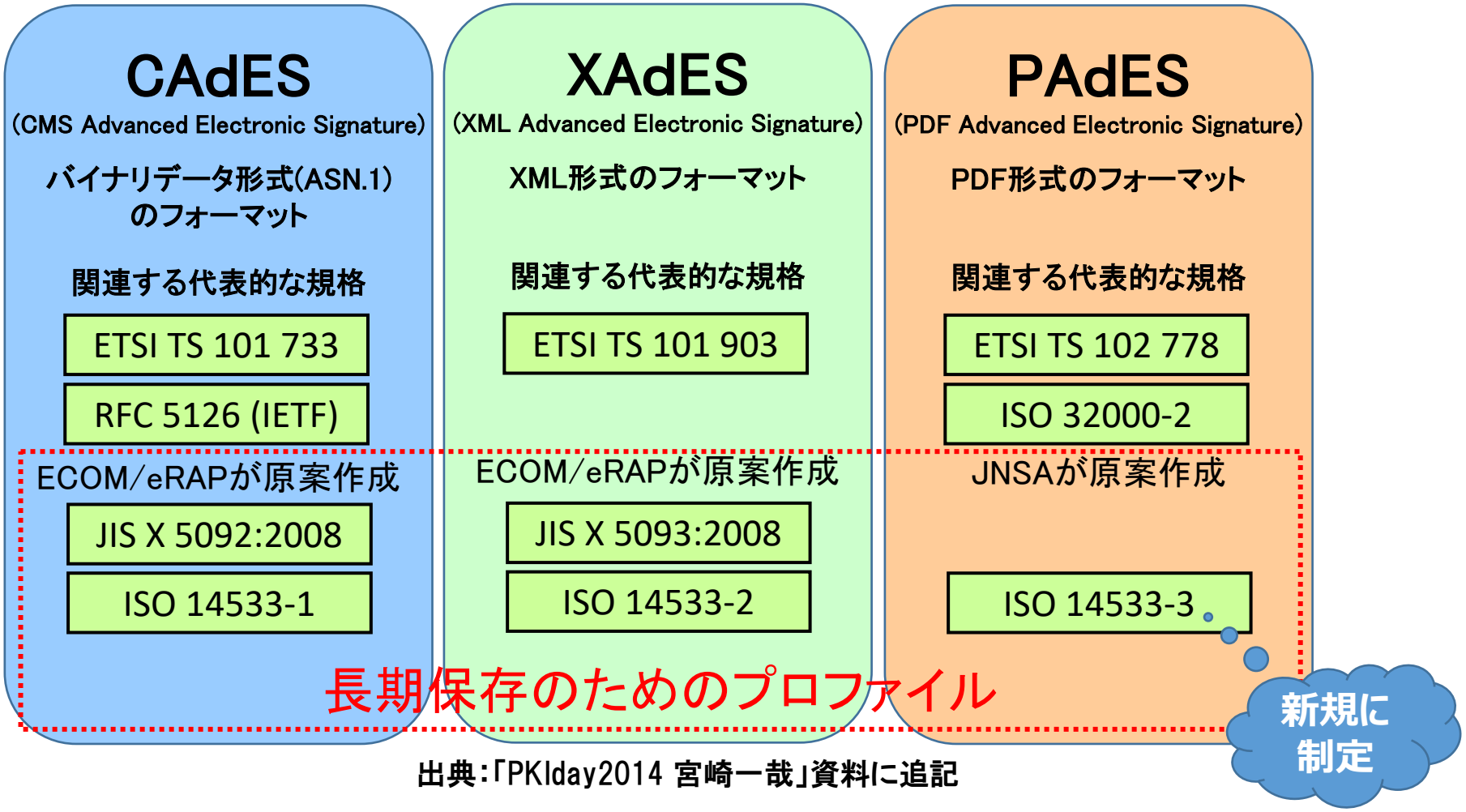
IPSJデジタルプラクティス,Vol.9 No.3,「ディジタル社会のトラストを支える電子署名」
https://www.ipsj.or.jp/dp/contents/publication/35/S0903-S05.html

- 電子署名の本来果たすべき機能は，・・・「署名者が署名対象にコミットしたこと」を証明することである.
- 時間が経つと電子署名の効力が失われるという課題がある．これに対して，長期に電子署名の有効性を保証する技術として長期署名がある.
- (長期署名の)標準化の検討が進みつつあった欧州のETSI（European Telecommunications Standards Institute）と連携しながら長期署名のプロファイル策定と標準化を推進することとした.
- 電子署名が有効性を失っていないことを確認できるようにするため，・・・オプション領域に，署名タイムスタンプ，署名検証情報，アーカイブタイムスタンプを追加する.

長期署名フォーマットのイメージ

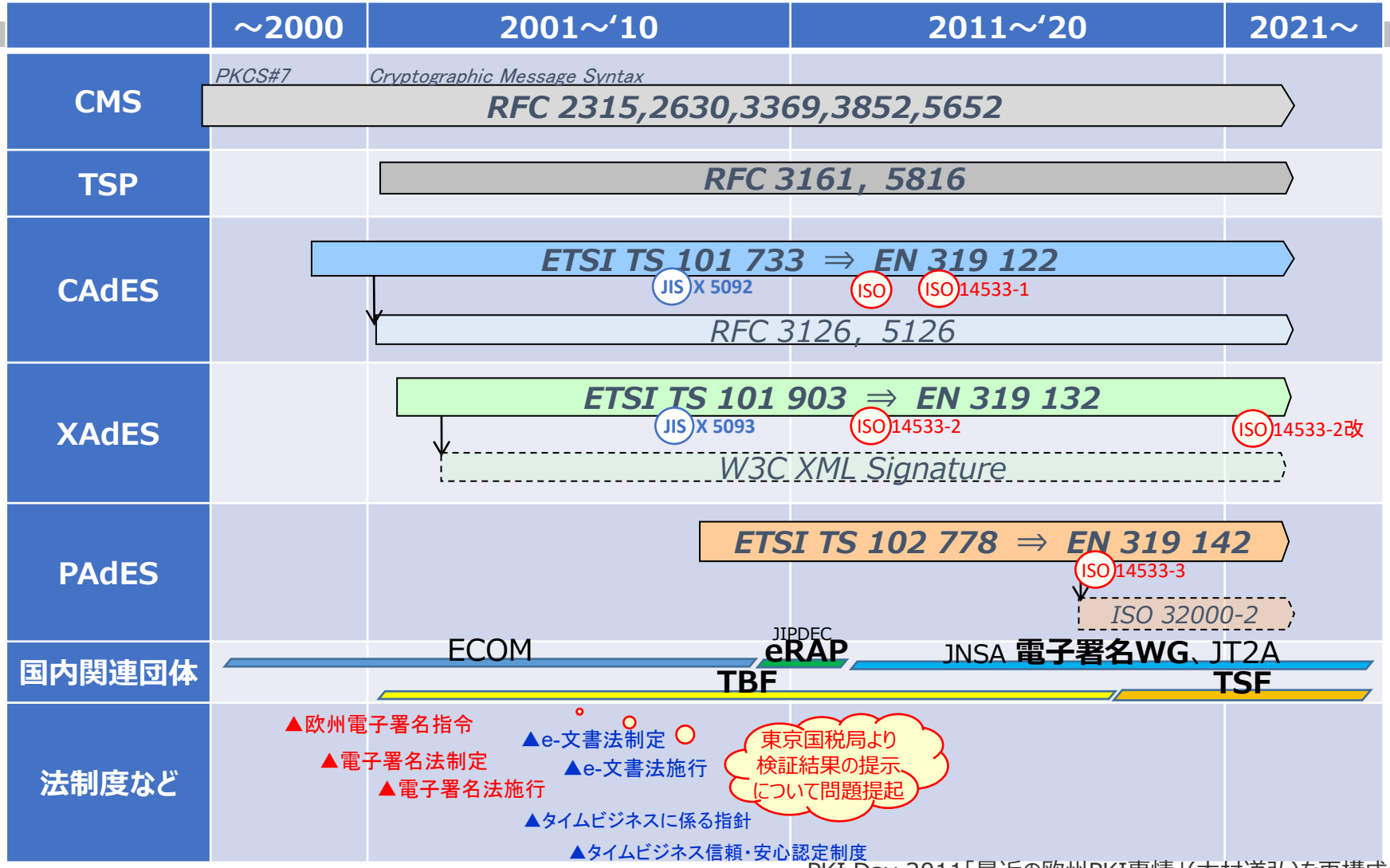


署名プロファイル



出典:「PKIday2014 宮崎一哉」資料に追記

署名標準化の経緯まとめ

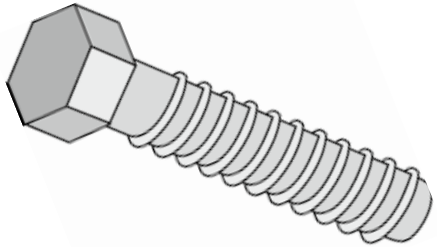


PKI Day 2011「最近の欧州PKI事情」(木村道弘)を再構成
https://www.jnsa.org/seminar/pki-day/2011/data/05_kimura.pdf

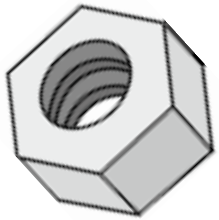
【2】署名検証の取り組みと経緯

対になる技術

- 例えば、



日本工業規格　JIS B 1180：2014
六角ボルト Hexagon head bolts and hexagon head screws



日本工業規格　JIS B 1181：2014
六角ナット　Hexagon nuts and hexagon thin nuts

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

他にも、相互運用性の必要な技術がある

- 通信における送信と受信
- 暗号における暗号化と復号
- 署名における署名と検証 ・・・ 署名すればOK、ではない

対になる技術(続き)

- 問題になるケース

	不成功の場合	後処理
通信の場合	受信できない	再送依頼
暗号化の場合	復号できず、読めない	鍵の再送、再暗号化など
署名・検証の場合	エラーが無ければ気づかない とりあえず本文は読めることが多い	改竄等があった場合、後で困ったことになる

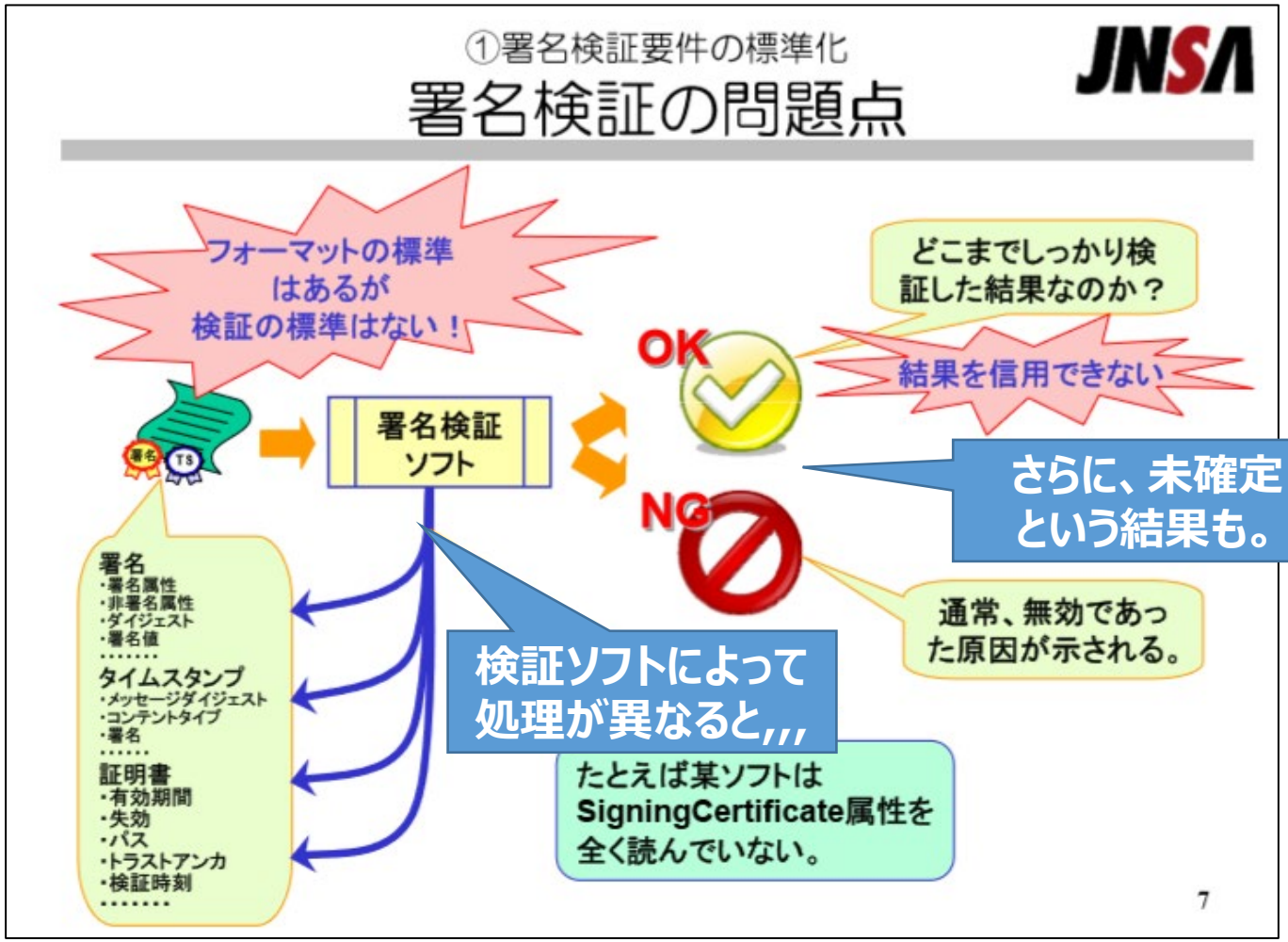
後悔先に立たず

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

検証の標準が無いと何が困るのか

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

検証標準がないと何が問題か(1)



https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

出典:「PKIday2014 宮崎 一哉」資料に追記

参考：検証プロセスの状態表示

- VALID (有効)、またはPASSED
  - 技術的に有効である場合
- INVALID (無効)、またはFAILED
  - VALIDとなる要求事項のいずれかが失敗となる場合
- INDETERMINATE (未確定)
  - 入手可能な情報ではVALIDかINVALIDか判断できない場合（その後の追加情報でVALID/INVALIDに変わる場合もある）
  - 検証プロセスの途中経過でINDETERMINATEとなり、次のステップでVALID/INVALIDに変わる場合や、最終的な出力としてINDETERMINATEのままで終わる場合もある

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

検証標準がないと何が問題か(2)

結果の一貫性が保証されない

- 利用者にとって：
  何を信用すればよいのか？
- 開発者にとって：
  どこまで実装すればよいのか？
- 調達者にとって：
  どれを選定すればよいのか？

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

検証標準がないと何が問題か(3)

さらに、

様々な署名方式の登場

- 署名者は用途に応じて署名方式を選択：
  何を基準に選択すればよいのか？
- 検証者は署名方式に応じた検証を実施：
  検証結果はどこまで信頼できるのか？

標準化の
経緯と現状
（日欧の状況）

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

経緯の振り返り

日本の状況

- 2000頃～　（ECOMにて）
  - 長期署名の規格化、プラグテスト
  - 電子文書長期保存ハンドブック(2006年度成果)
- 2008～2012頃　（TBFにて）
  - 長期署名検証ツール認証制度検討報告書(2008年度成果)
  - 電子署名検証ガイドライン(2012年度成果)
- 2013-14年頃　（JNSAにて）
  - 署名検証標準の検討
    - ⇒ 欧州版との関係により、中断
- 2018年度　（JNSAのTF再開）
  - ETSI　TS 119 102-1 の解読、フロー作成

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

欧州の状況

2012年：署名検証処理の標準

2015年：生成と検証処理の標準

【3】2020年度活動の狙い

日欧の比較

	表題	書き方	メリット	デメリット
ETSI (欧)	生成と検証	判定のProcessを記述	処理が同じなら結果が一意に決まる※1	(本来なら)処理の工夫の余地が少ない※2
TBF (日)	検証	各要素の判定条件を表記述	条件が分かりやすい（適合宣言書で実装範囲の宣言が可能）	実装にあたり、処理の組み立てをよく考える必要がある

※1：ただし、複雑な処理仕様、多様なバリエーションを厳密に標準規約で記述することは難しく、個別の実装に任される部分は残る。

※2：例えば、業界ごとの制約に基づく効率的な実装など。

（しかし、5.1.4.1では「本文書は、制約が検査されるべき時をいつも正確に規定するとは限らない。なぜならこれは実装に依存するからである。」と、書かれていたりする。）

https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_1.pdf

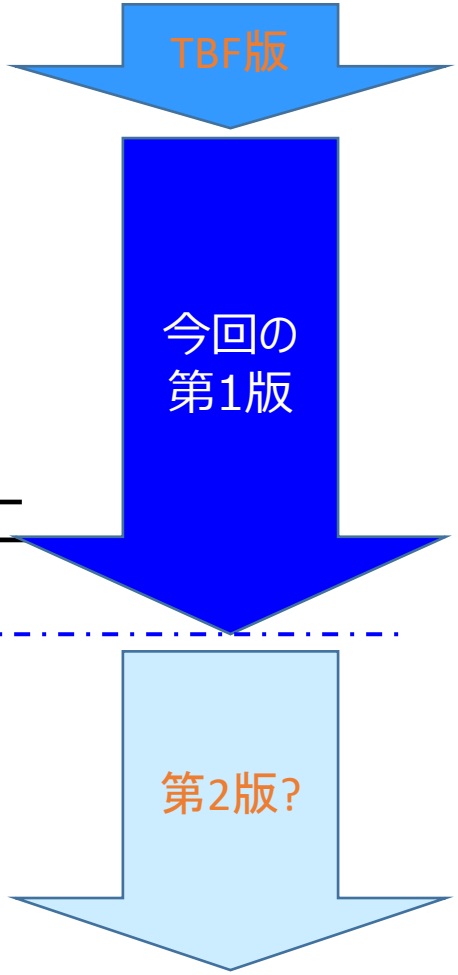
日本版・署名検証ガイドライン

日本版ガイドライン(2012)の改訂方針

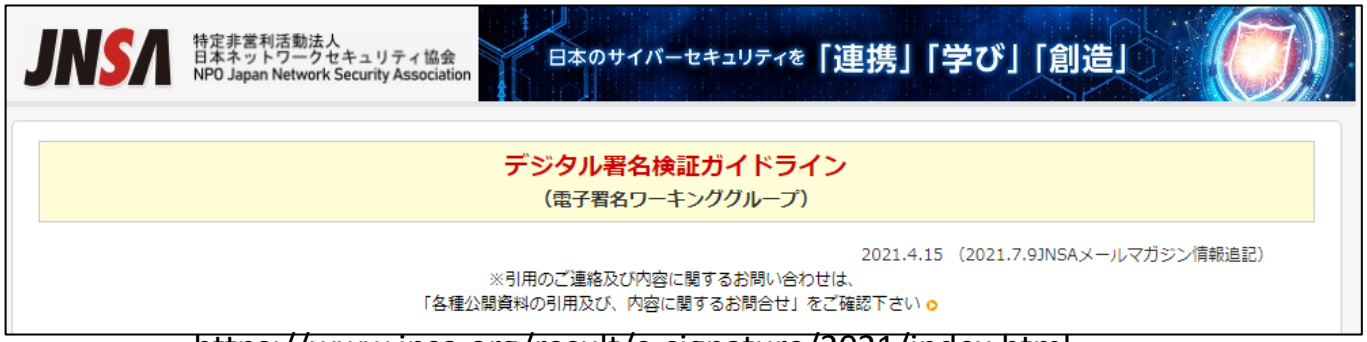
① 日本版の構成を維持しつつ、最新化
- ◆誤記修正、未完部分(PAdES等)の完成
- ◆用語・参照規約の最新化

② ガイドラインの分かり易さ、使い易さの向上
- ◆内容説明追加、コラム補足
- ◆適合宣言書の利用法など解説

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



【4】ガイドラインの概要と要点



https://www.jnsa.org/result/e-signature/2021/index.html

全体構成

デジタル署名検証ガイドライン　第1.0版

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

1章 はじめに

2章 参照文献

3章 用語定義と略語

4章 デジタル署名

5章 デジタル署名の検証

概念モデル、検証プロセス、データ構造、検証基準時刻、署名の検証要件、タイムスタンプの検証要件、証明書の検証要件

付属書A 供給者適合宣言書

付属書B PAdES関連情報

付属書C 暗号アルゴリズム

その前に、AdESについて

- コラム１・・・AdESという呼称の経緯（3.1 用語）

1999年：EU電子署名指令（Directive 1999/93/EC）で“Advanced Electronic Signature”が定義された。日本では「先進電子署名」あるいは「高度電子署名」と訳される。

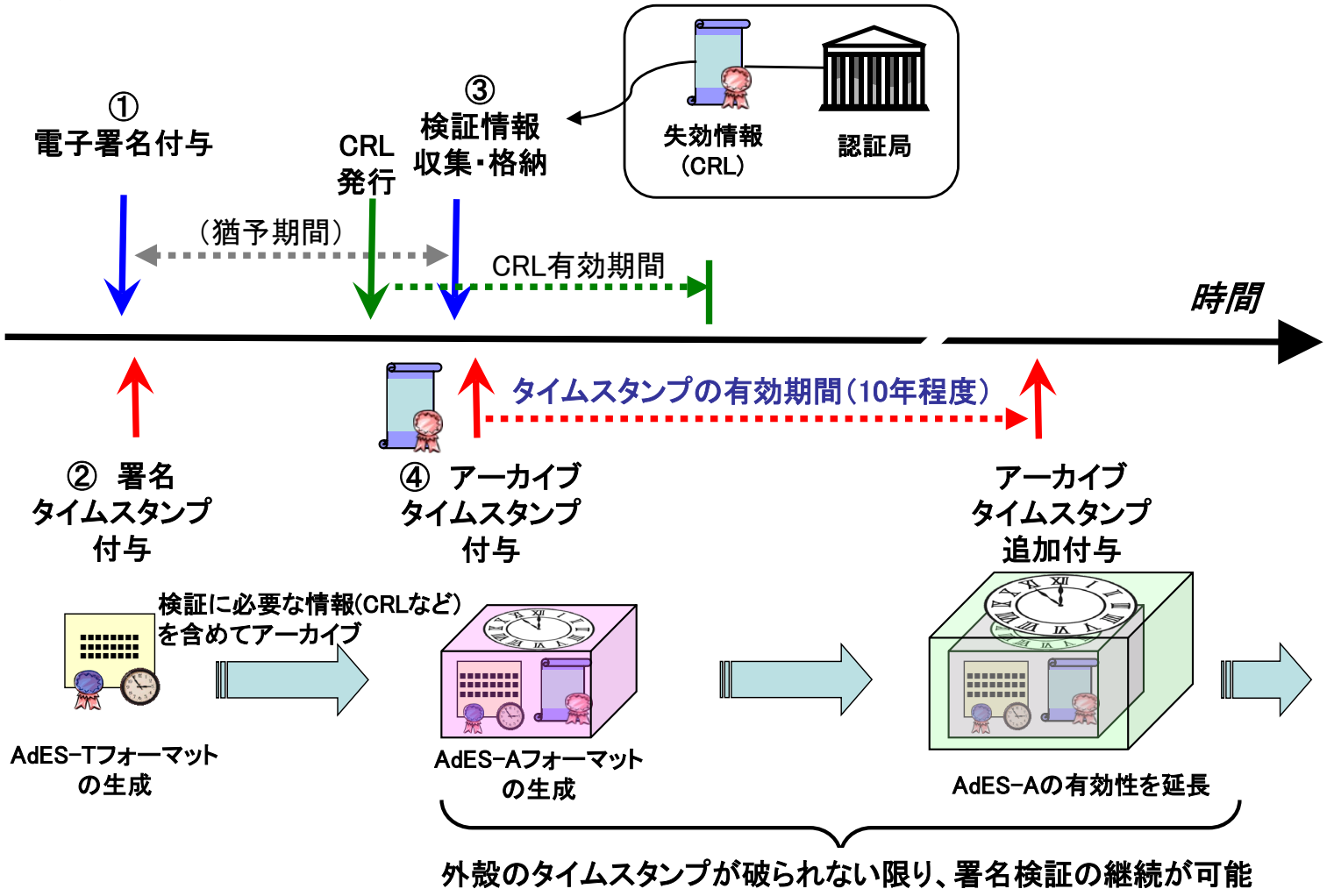
2002年：“ETSI TS 101 903 V1.1.1 (2002-02); XML Advanced Electronic Signatures (XAdES)”で略称が用いられ、その後、CMSの電子署名規格でもCMS Advanced Electronic Signatures (CAdES)が用いられるようになった。

2014年：EUのeIDAS規則（eIDAS Regulation）でも、“Advanced Electronic Signature”に対して電子署名指令とほぼ同等の定義が与えられている（略称“AdES”は用いられていない）。

その後、ETSIでは、“AdES”を略称ではなく固有名詞として扱い、CMS、XML、PDFそれぞれに対する署名として“CAdES Digital Signature”、“XAdES Digital Signature”、“PAdES Digital Signature”を、又その総称として“AdES Digital Signature”を用いるようになった。

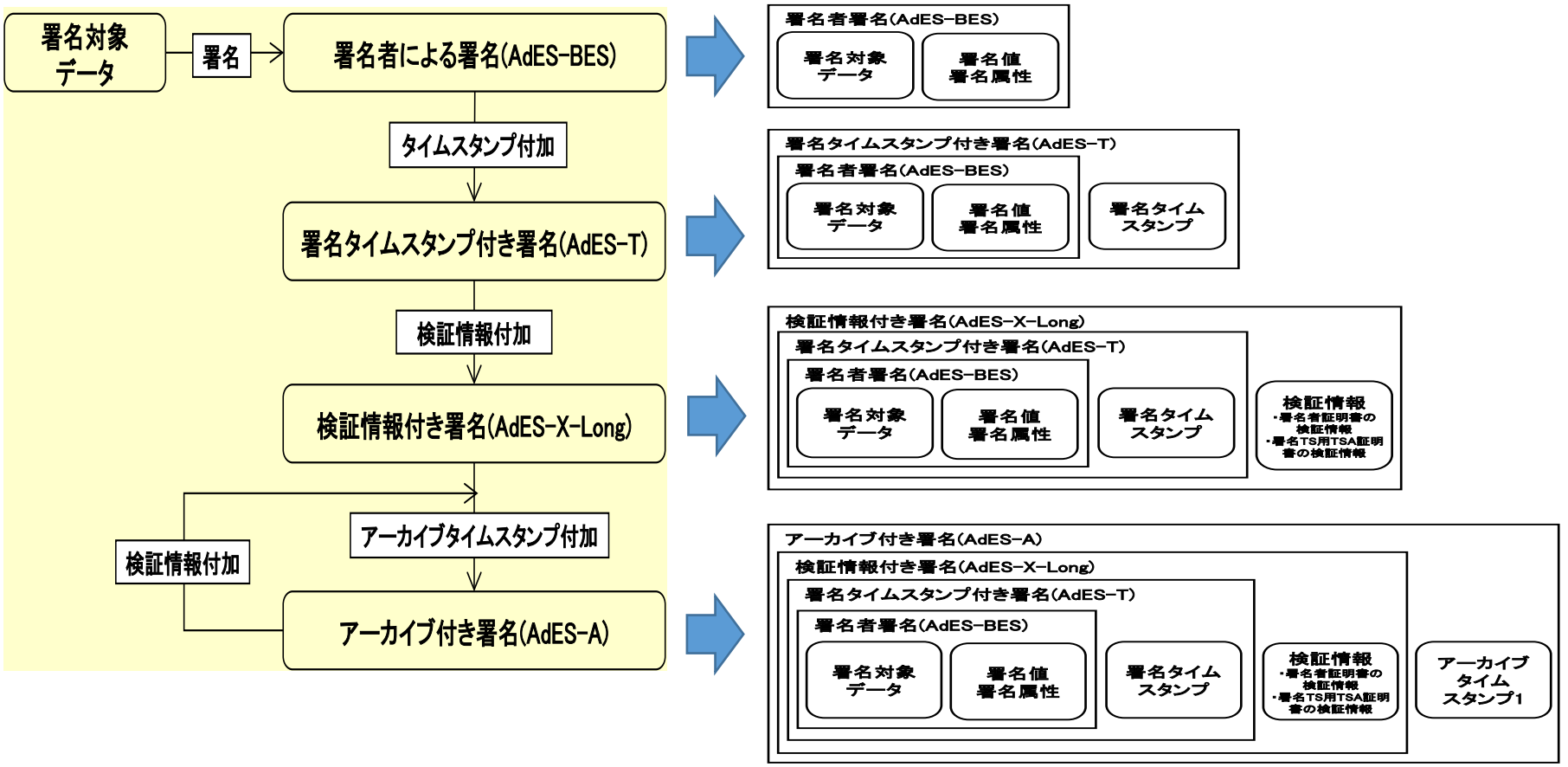
長期署名による署名延長

- 長期署名フォーマットによる署名延長・・・4.2.2



AdESのフォーマット

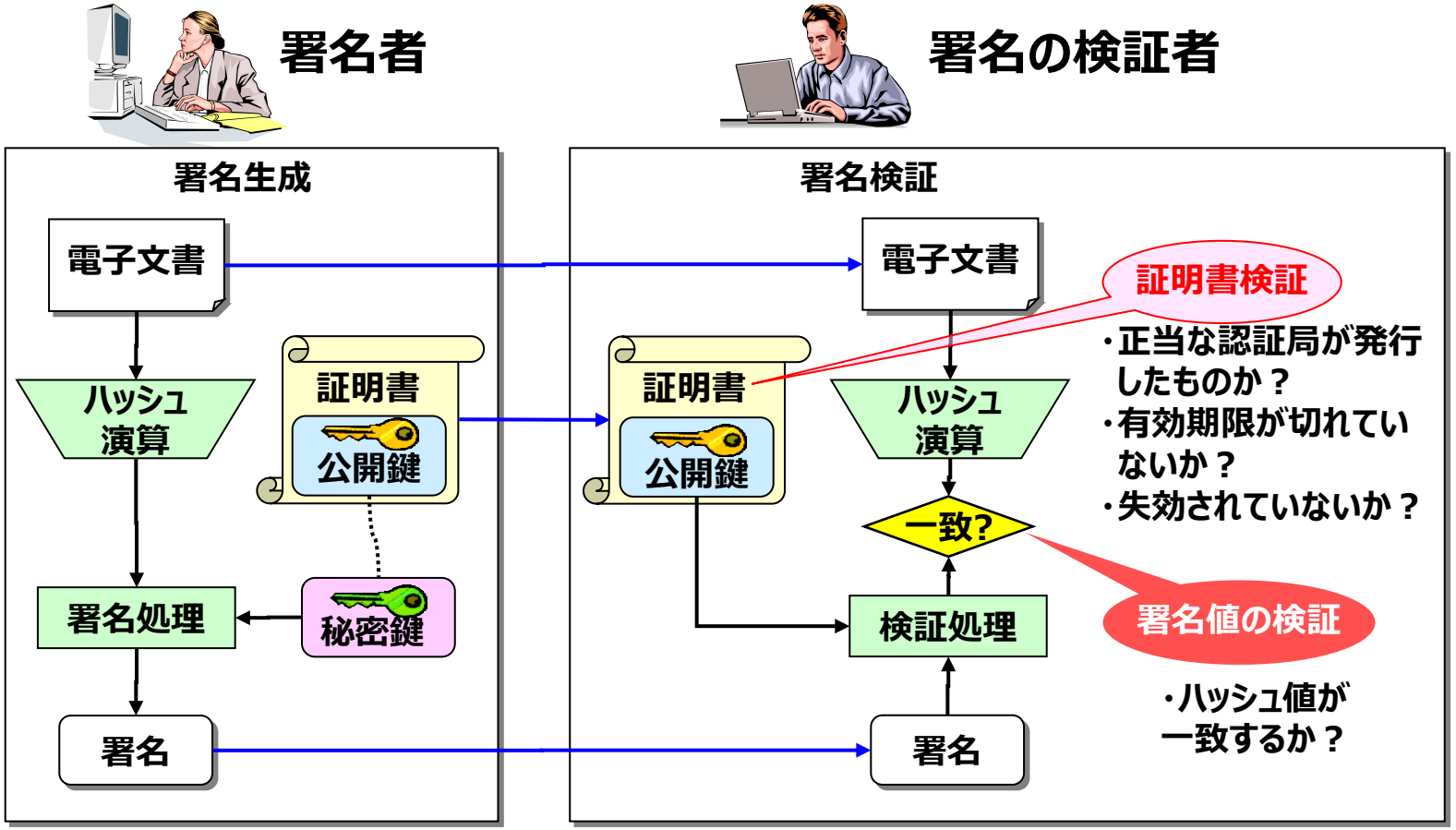
- ライフサイクルとフォーマット（4.2.3）



署名検証とは

署名と検証

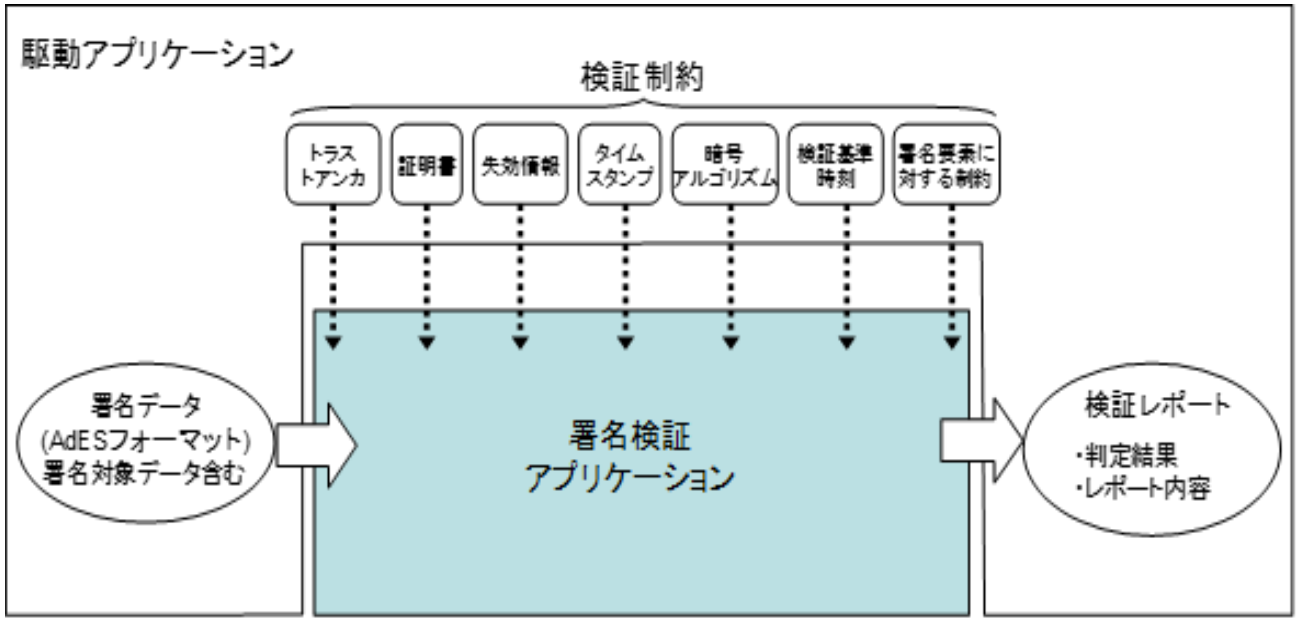
- 署名と検証の一般的な説明（4.1.3 基本メカニズム）



⇒ しかし、実際にはこれだけではない。

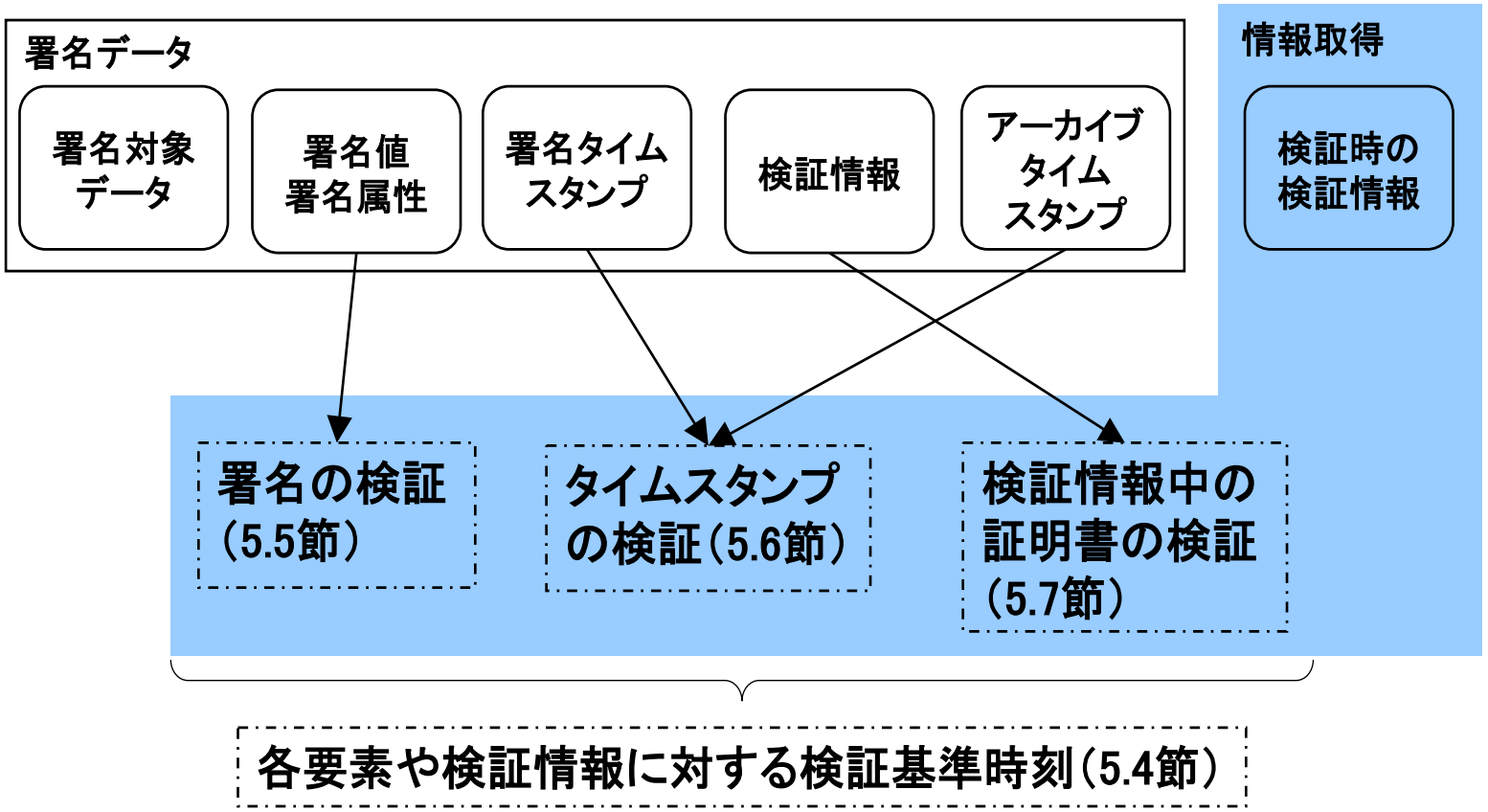
署名検証のモデル

- 署名検証に必要となる情報には、署名対象データと署名値以外に、関連する証明書や失効情報、・・・などの様々な情報が必要となる。これらを、検証制約（Validation constraints）と呼び、以下のようなものが挙げられる。（ 4.2.2）
  - 認証局のトラストアンカー／パスに含まれる全ての証明書,利用用途などの制約／失効情報／タイムスタンプ／検証基準時刻／有効と認められる暗号アルゴリズムの制約／署名データを構成する要素に対する制約



検証プロセス

- 署名検証プロセス（5.2.1）



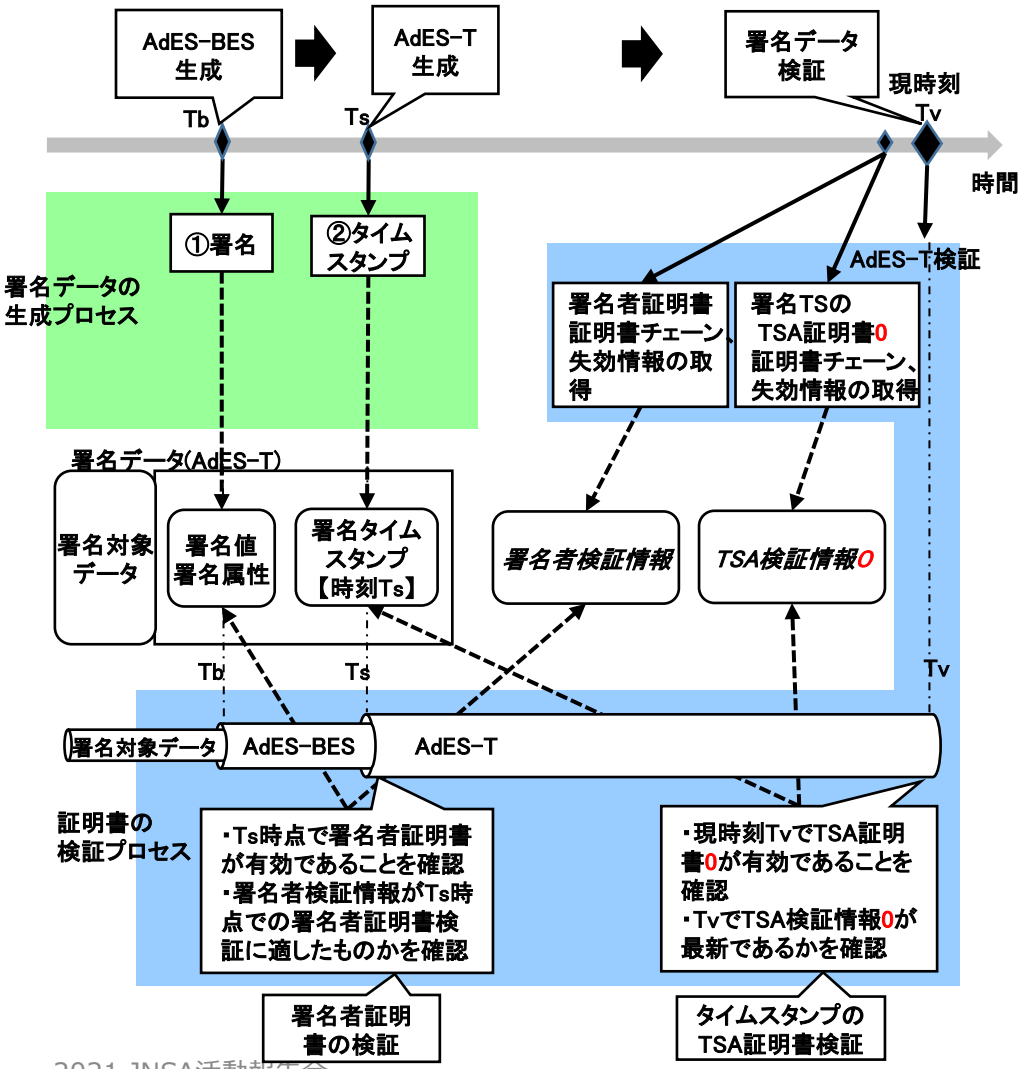
検証の時刻

検証基準時刻

- 本来の署名検証の目的は署名時点における電子署名の有効性を確認すること・・・、検証基準時刻は“署名を付与した時点”とすることが理想・・・、検証基準時刻はタイムスタンプを併用するなどによる客観的な署名の時刻・・・、できない場合は、署名検証を実施する現在時刻となる。（5.1.1）
- 計算対象に含む有効なタイムスタンプトークンのうち、最も古いものの示す時刻であり、該当するタイムスタンプがない場合、検証処理を実行する時刻となり、検証処理に外部から与える必要がある。（5.2.7）
- 検証の考え方を整理すると、以下となる。
  - 署名、コンテントタイムスタンプ
    - 署名タイムスタンプがなければ現在時刻で検証
    - 署名タイムスタンプがあればその時刻で検証
  - 署名タイムスタンプ
    - アーカイブタイムスタンプがなければ現在時刻で検証
    - アーカイブタイムスタンプがあれば最も古いアーカイブタイムスタンプの時刻で検証
  - アーカイブタイムスタンプ群
    - 自分より新しいアーカイブタイムスタンプがなければ、現在時刻でそのアーカイブタイムスタンプを検証
    - 自分より新しいアーカイブタイムスタンプがあれば、その直後のアーカイブタイムスタンプの時刻で検証
- 具体的には・・・（5.4 検証基準時刻と検証の観点）

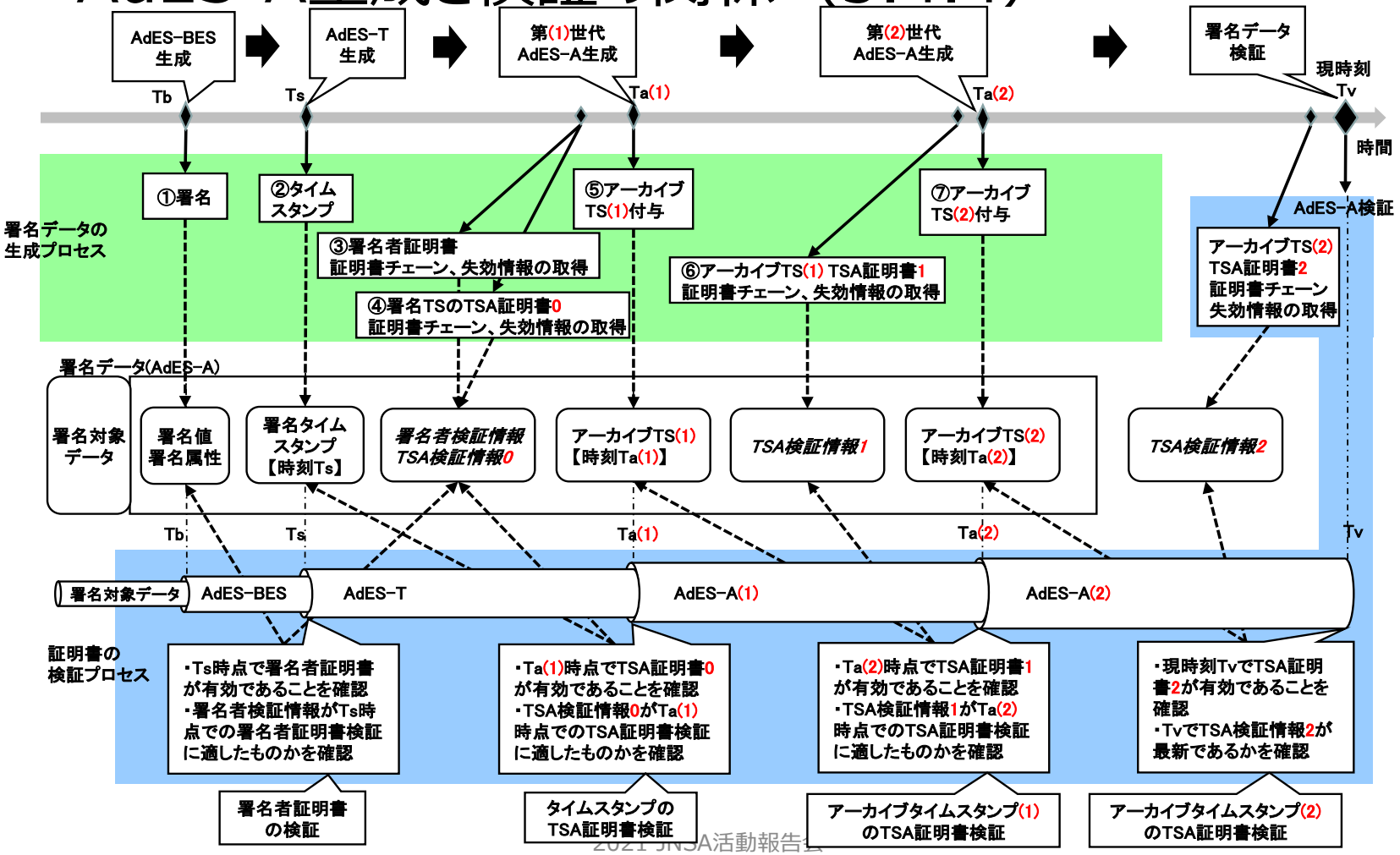
検証と基準時刻(例1)

- AdES-T生成と検証の関係（5.4.2）



検証と基準時刻(例2)

- AdES-A生成と検証の関係（5.4.4）



検証の要件

検証要件の要求レベル

- 必須とオプション（5.1.4）
- 多岐にわたる検証項目を下記に分類し、規定。
  - 必須 [M（Mandatory）]
    セキュリティを担保するために必ず実行しなければならない。必要なフィールドが署名データに存在しない場合にはINVALIDと判定する。
  - 存在時必須 [E（Mandatory if Exists）]
    該当するフィールドが存在する場合は、必ず実行しなければならない。
  - オプション [O（Optional）]
    検証を実行するか否かはアプリケーションの要件に依存する。

また、本書の規定を基にして、さらに用途を限定したプロファイルを策定する場合、[O]を[E] 又は[M]に、[E]を[M]に再定義することは可能とする。しかし、[M]もしくは[E] を検証しない実装は供給者の適合宣言書に記して、その制約を明確にする必要がある。

具体的な検証要件（5.5～5.7）

- 検証要件の表の例

検証対象

要求レベル

検証対象	検証内容	判定基準	M/E/O	判定結果（状態）	レポート例
署名構造	PAdES-DT必須要素	表5.5.4-5のDocTimeStamp署名辞書の必須要素が含まれること	M	VALID	判定結果
				INVALID	含まれていない必須要素
オプション要素	PAdES-DTオプション要素	DocTimeStamp署名辞書にName, M, Location, Reason, ContactInfoエントリー要素が含まれないこと	O	VALID	・判定結果 ・オプション情報
				WARNING	・不正内容 ・不正項目の情報
DocTimeStamp署名辞書	タイムスタンプトークン検証	DocTimeStamp署名辞書のContentsエントリーに含まれるタイムスタンプトークンデータが正しく検証できること	M	5.6.1 を参照	
	ByteRange範囲のハッシュ値との比較	タイムスタンプトークンのハッシュ値（MessageImprint）とByteRange範囲から計算したハッシュ値が一致すること	M	VALID	判定結果
				INVALID	不正内容
検証情報	検証情報の過不足	DocTimeStamp署名辞書に含まれるTSA証明書の検証に必要となる証明書と失効情報（CRL/OCSP）が取得できること	M	VALID	判定結果
				INVALID	不正内容

検証基準

出力内容

供給者適合宣言書（付属書A）

署名検証手順の要件に対する供給者適合宣言書

番号:
発行者の名称:
発行者の住所:＿＿＿

宣言の対象:
上記宣言の対象は、次の署名検証手順の要件に適合している。

タイトル	版番号/発行日
デジタル署名検証ガイドライン	第X.X版/2021-xx-xx

実装されている要素は別紙（A.3参照）のとおりである。
追加情報:
（個々に動作確認結果などを記載することができる）

代表者又は代理者の署名:

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
（発行場所及び発効日）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
（氏名、役職）

【5】今後の活動

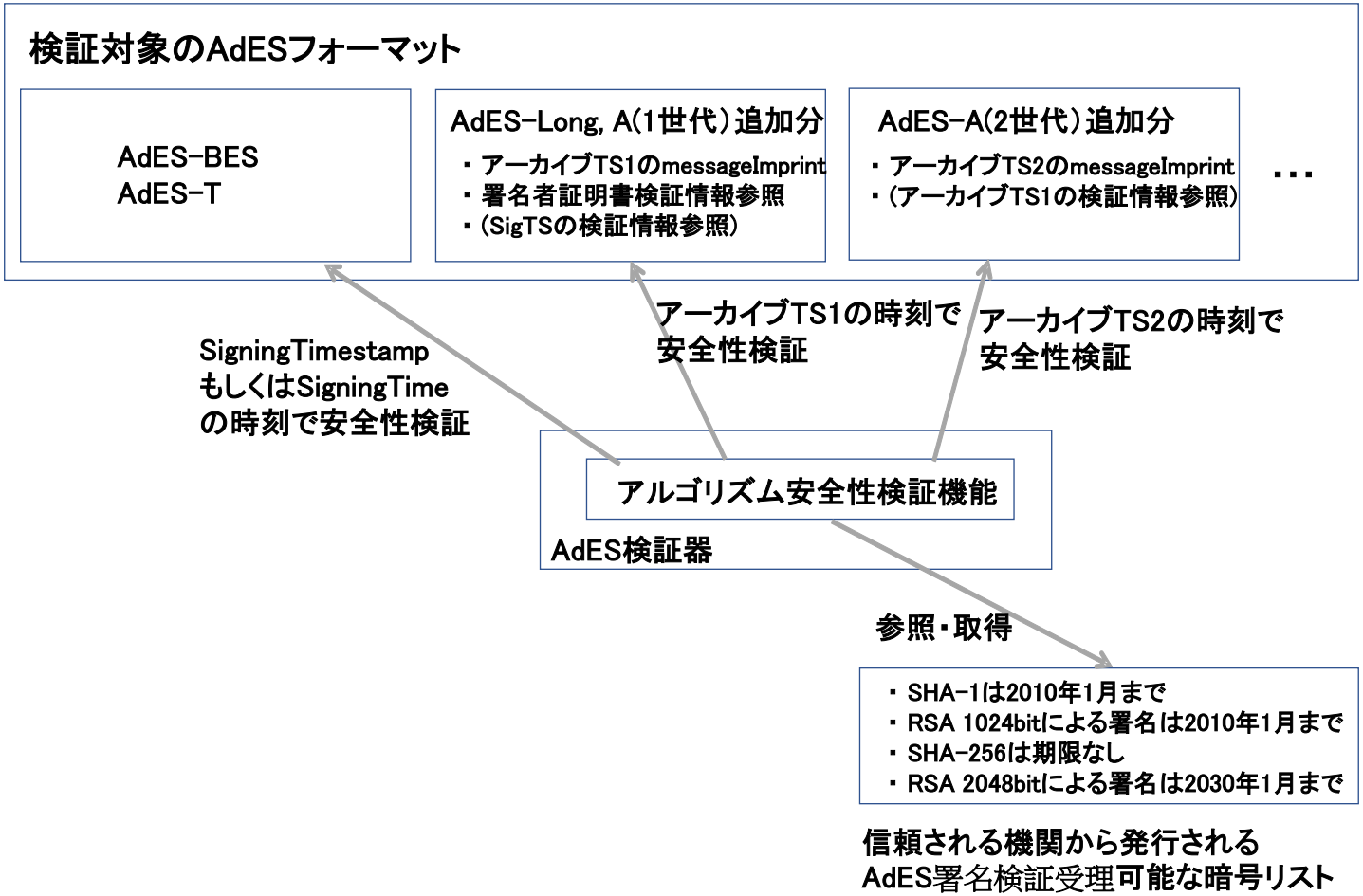
GLの積み残し、今後の課題

- ETSI版との整合
  - ETSI　TS 119 102-2(Signature Validation Report)対応
- 記述の改善・補足
  - 分かり易さ、読みやすさ等
- 適合宣言書の使い方検証
  - 実例への適用
- その他
  - トラストアンカーとしてのTSL(Trust-service Status List)対応
  - ASiC(Associated Signature Container)、JAdES(JSON ～)、リモート署名、eシール、、、
  - 信頼できる暗号リスト

  等々

暗号アルゴリズムの検証課題

- 暗号リスト利用の理想イメージ・・・付C、5.2.5



署名検証TFの今後の取り組み(予定)

１．検証標準化活動
- ETSI　TS 119 102-2（Signature Validation Report）対応
- 標準化(ISO、JIS)の方向性検討

２．検証ガイド普及活動
- ガイドラインの改善（読みやすさ、使いやすさ等）
- 適合宣言書の活用検討
- ガイドライン解説書（新技術への対応など）

３．コンフォーマンス検討活動
- 検証標準器または標準検証サービスの検討
- テストケース、テストデータ検討
- 検証ツールによる差の事例調査

ご清聴ありがとうございました

(ガイドライン執筆メンバーの皆様に感謝!)

電子署名WG
検証TFに
参加者募集中！