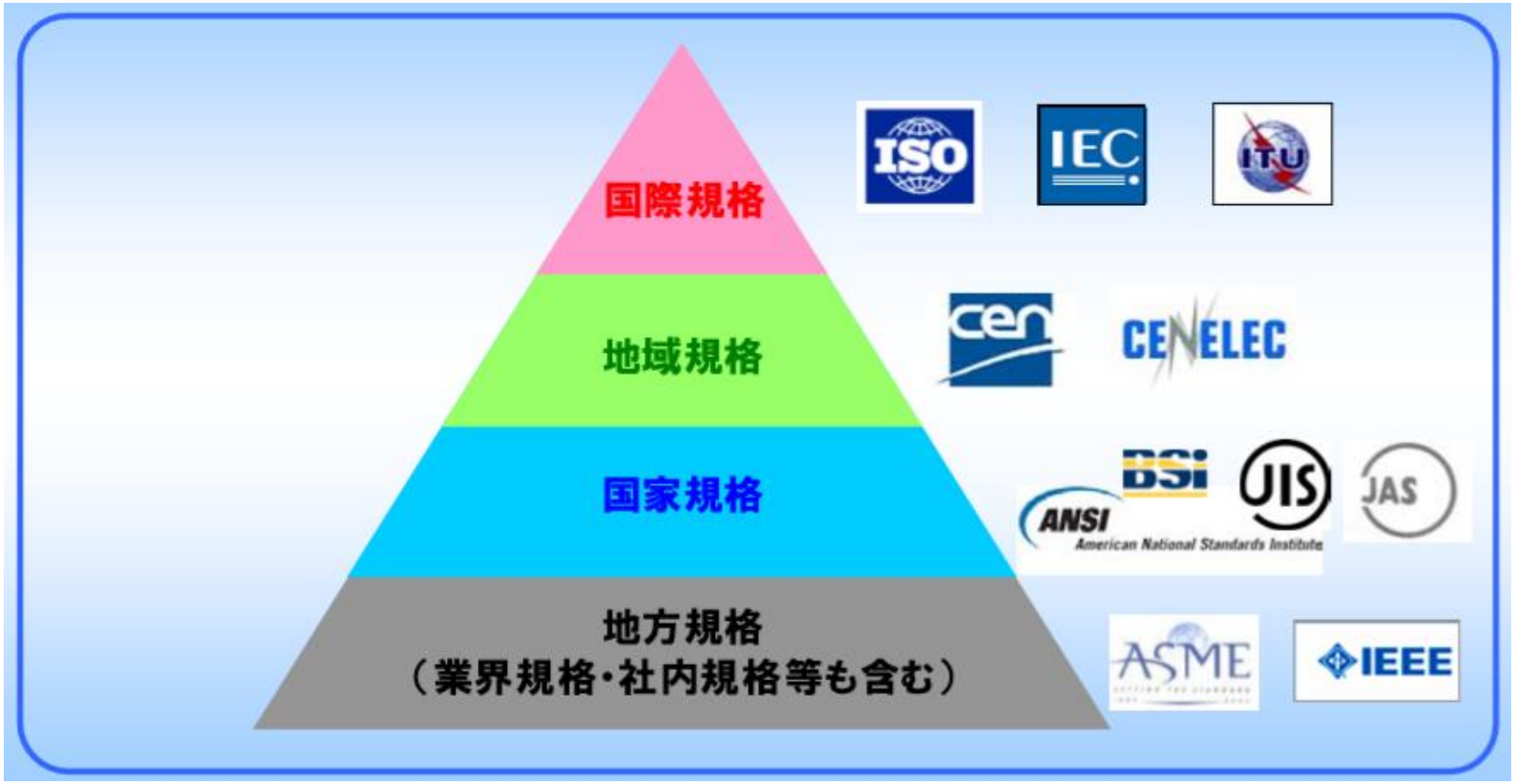
署名検証・知ってるつもり

2019.01.22

JNSA 電子署名WG・署名検証TFリーダー
政本 廣志

さまざまな標準や規格

技術標準、規格



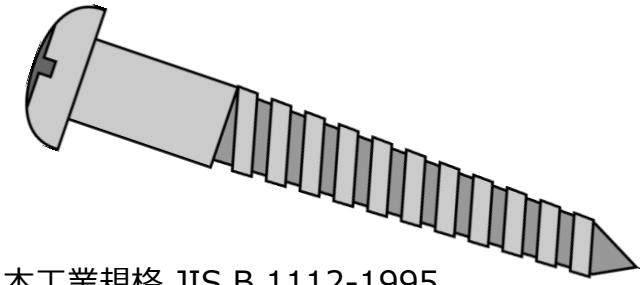
出典：https://www.jsa.or.jp/datas/media/10000/md_774.pdf　制作：山本隆司他

ISOだけで、21991!!(標準と文書　Annual report 2017より)

さまざまな技術標準、規格

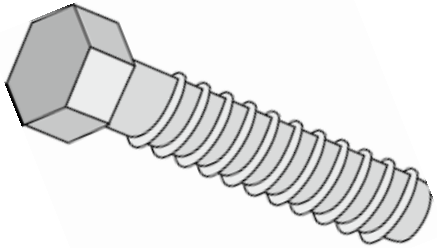
JNSA

- 例えば

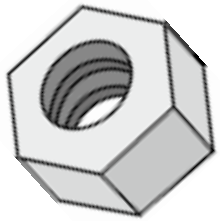


日本工業規格 JIS B 1112-1995
十字穴付き木ねじ Cross-recessed head wood screws

- こちらは対のもの・・・相互運用性



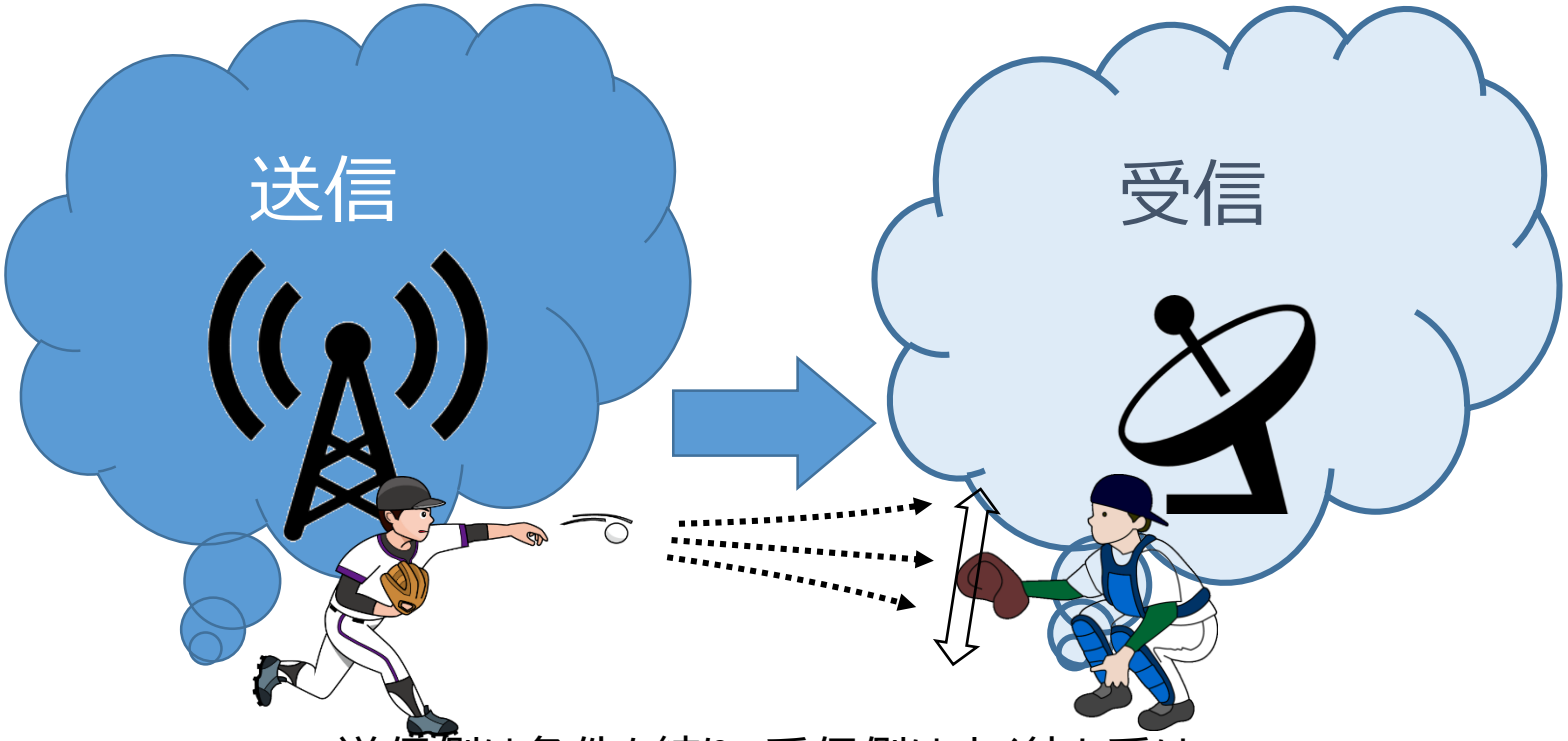
日本工業規格　JIS B 1180：2014
六角ボルト Hexagon head bolts and hexagon head screws



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

対になる技術(例１)

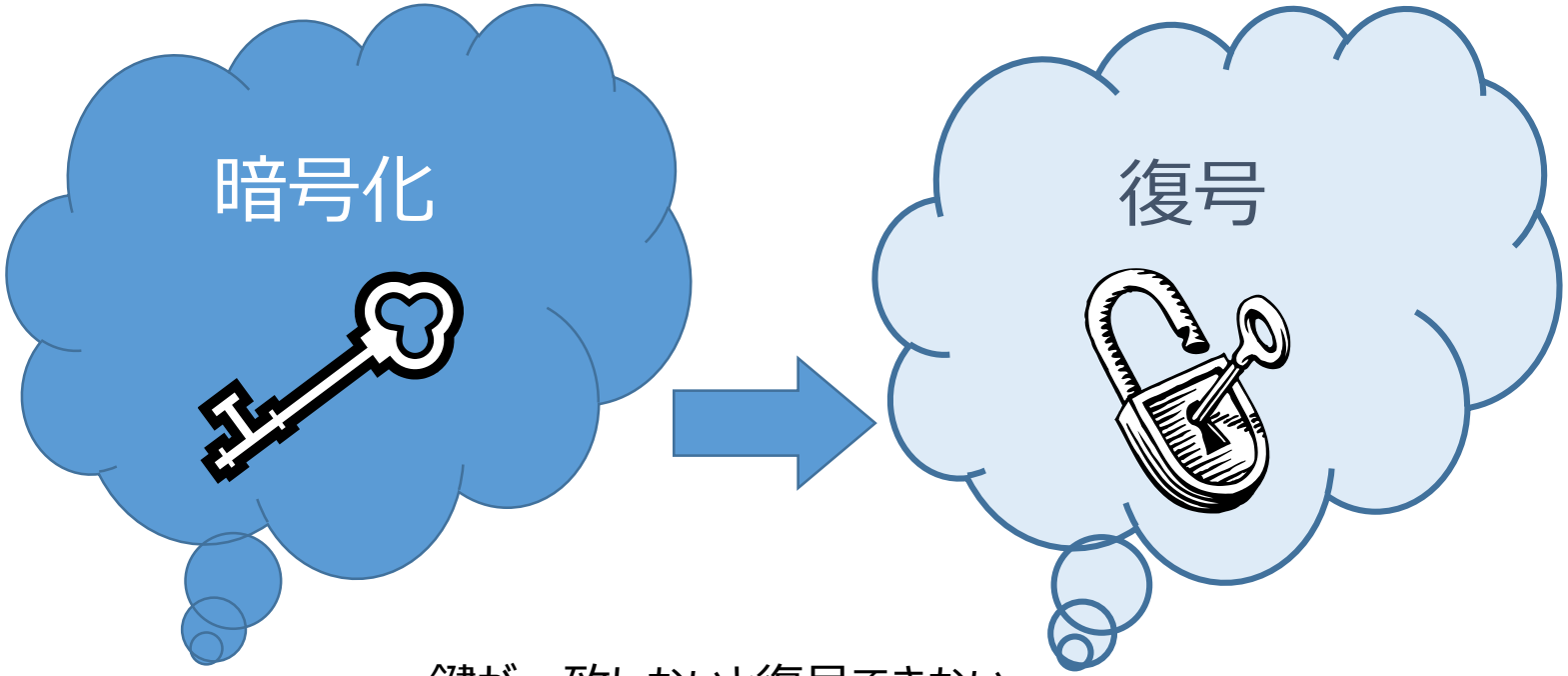
- 通信プロトコルの場合
  - 送信処理と、受信処理



送信側は条件を絞り、受信側は広く待ち受け

対になる技術(例2)

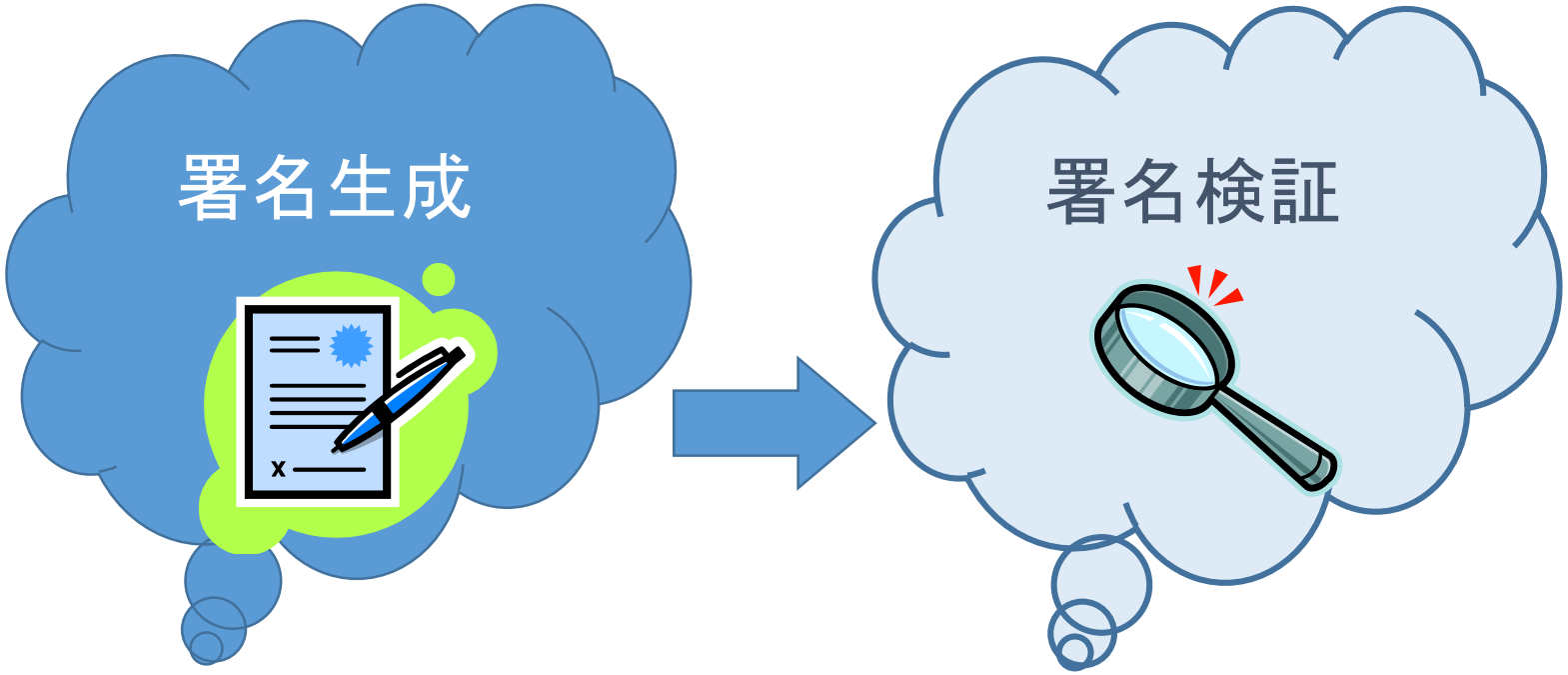
- 暗号文の場合
  - 暗号化と、復号



鍵が一致しないと復号できない
（公開鍵方式では一対の鍵）

対になる技術(例3)

- 電子署名はどうか？
  - 署名生成と、署名検証



検証の標準は、あまり気にしていない？

それぞれの比較

- ありがちなケース

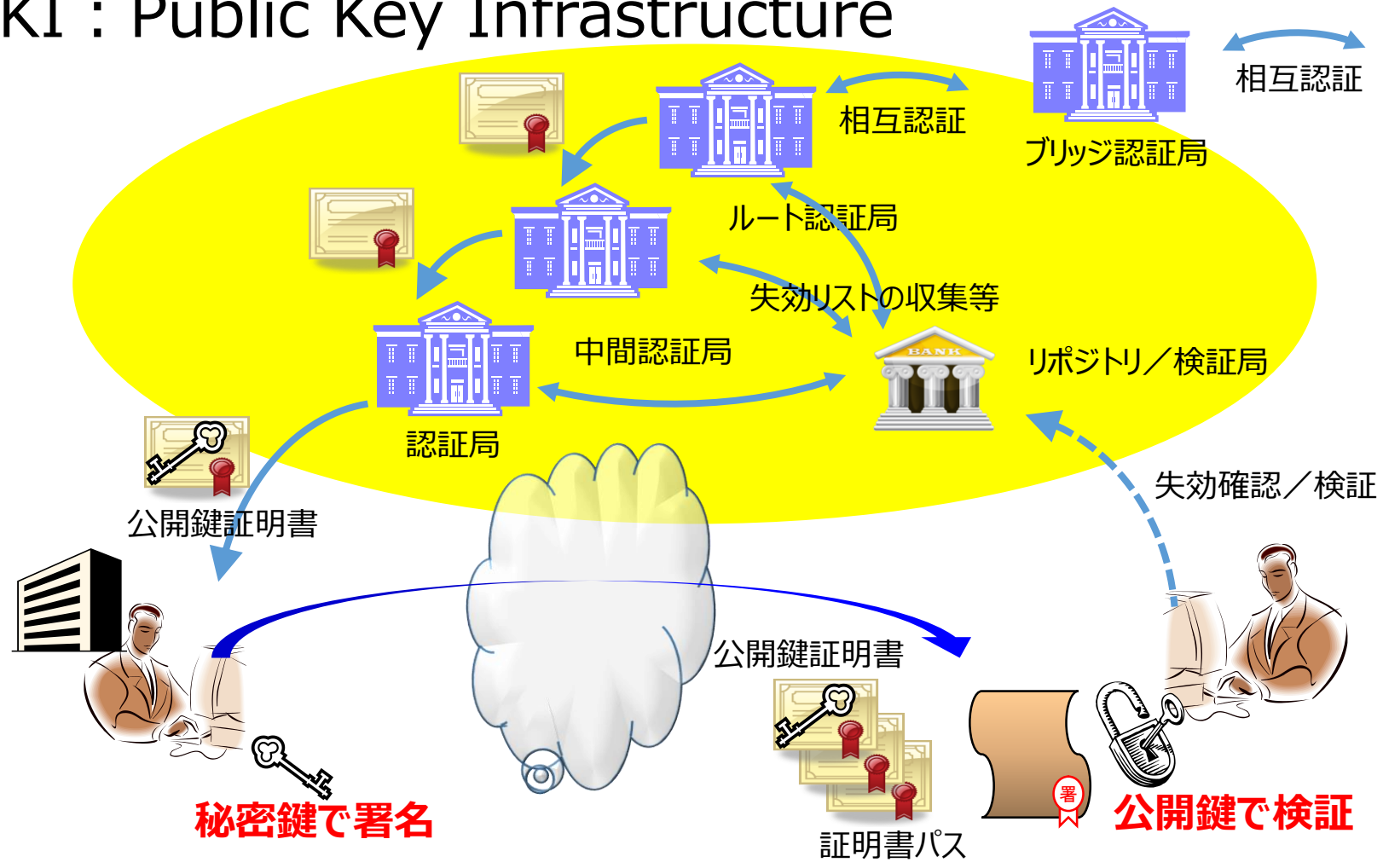
	不成功の場合	後処理
通信の場合	受信できない	再送依頼
暗号化の場合	復号できず、読めない	鍵の再送、再暗号化など
署名・検証の場合	エラーが無ければ気づかない とりあえず本文は読めることが多い	改竄等があった場合、後で困ったことになる

後悔先に立たず

検証の標準が無いと何が困るのか

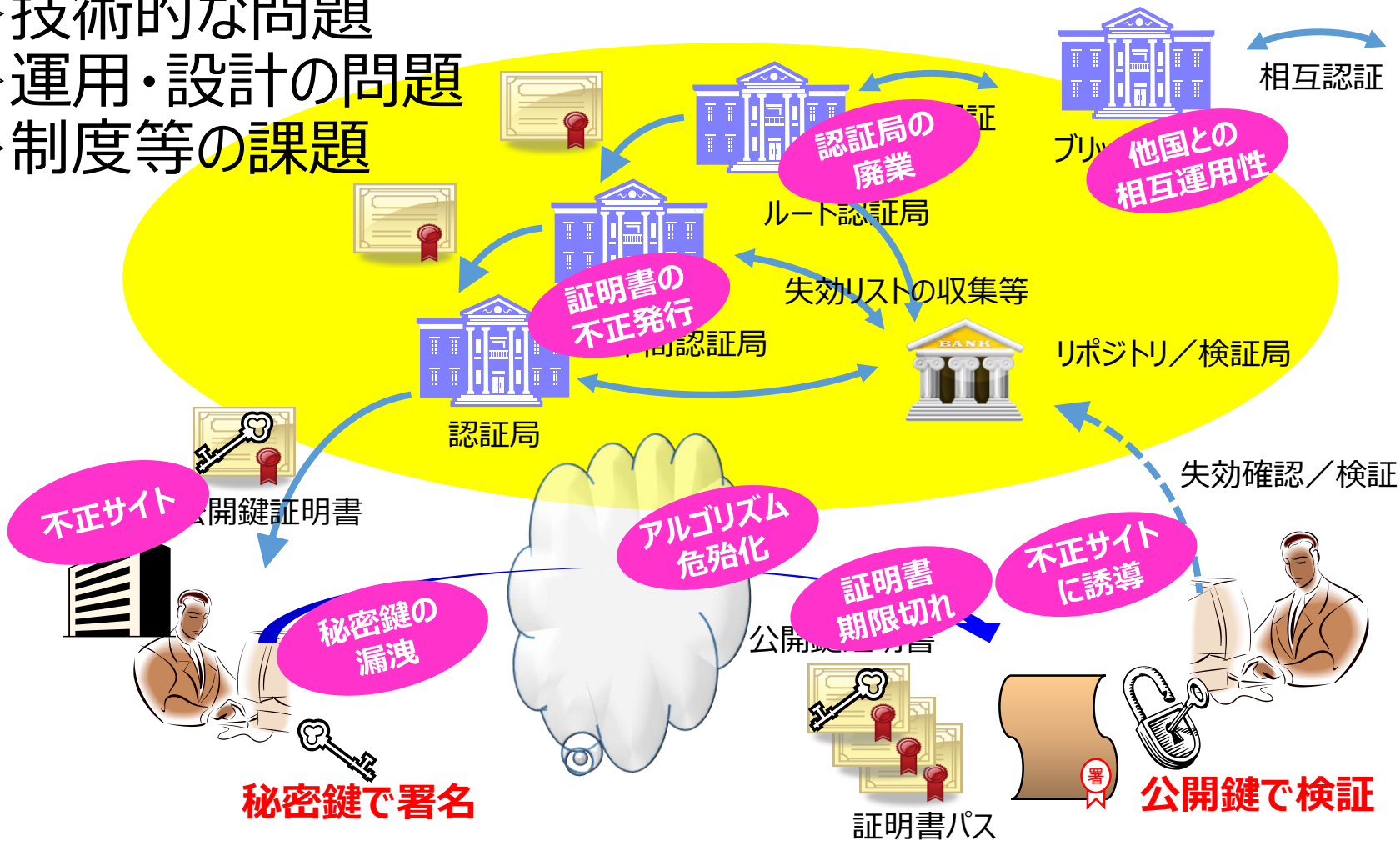
署名・検証のおさらい

PKI：Public Key Infrastructure



『PKIの陥穽』の例

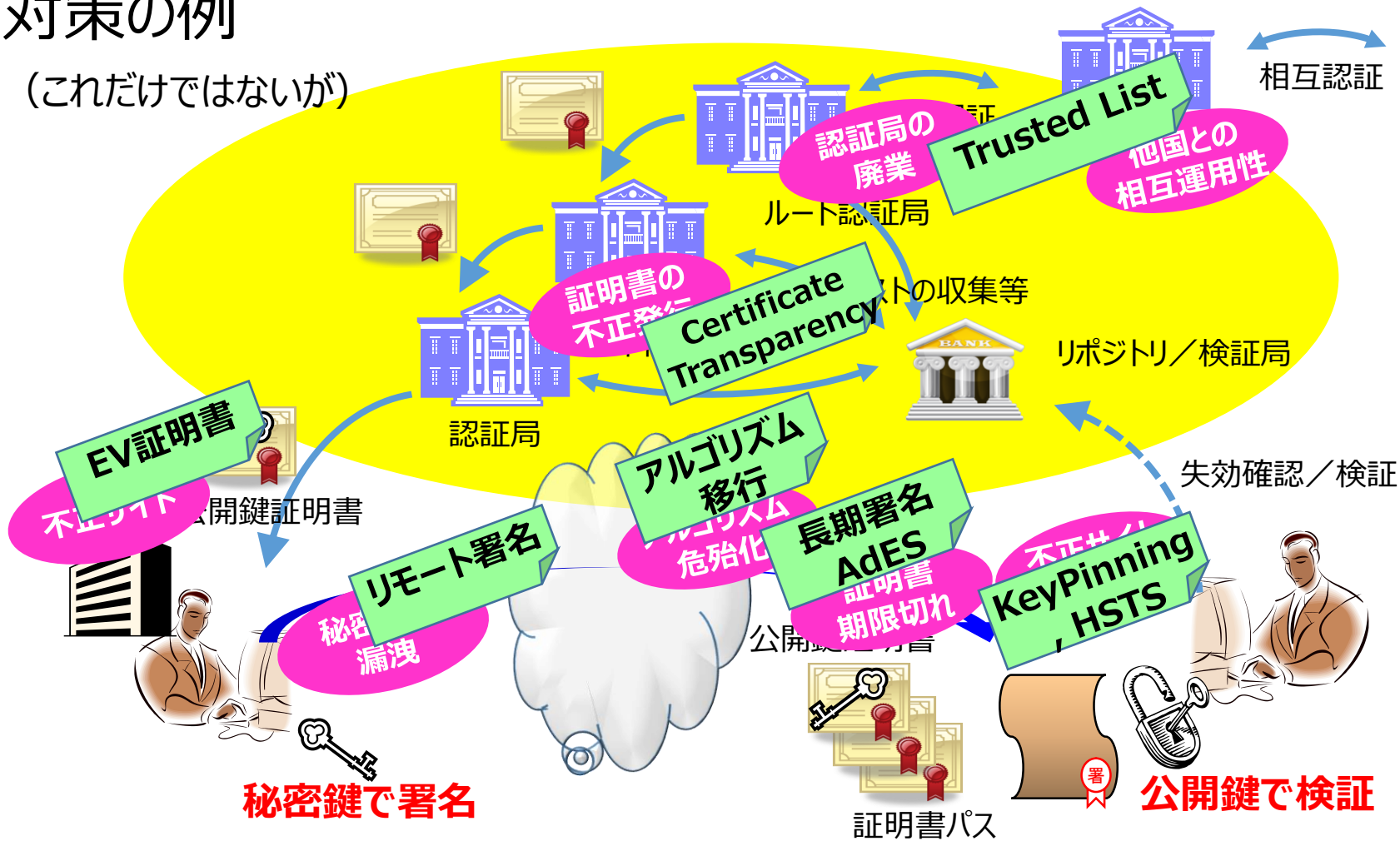
- 技術的な問題
- 運用・設計の問題
- 制度等の課題



『陥穽』への対策

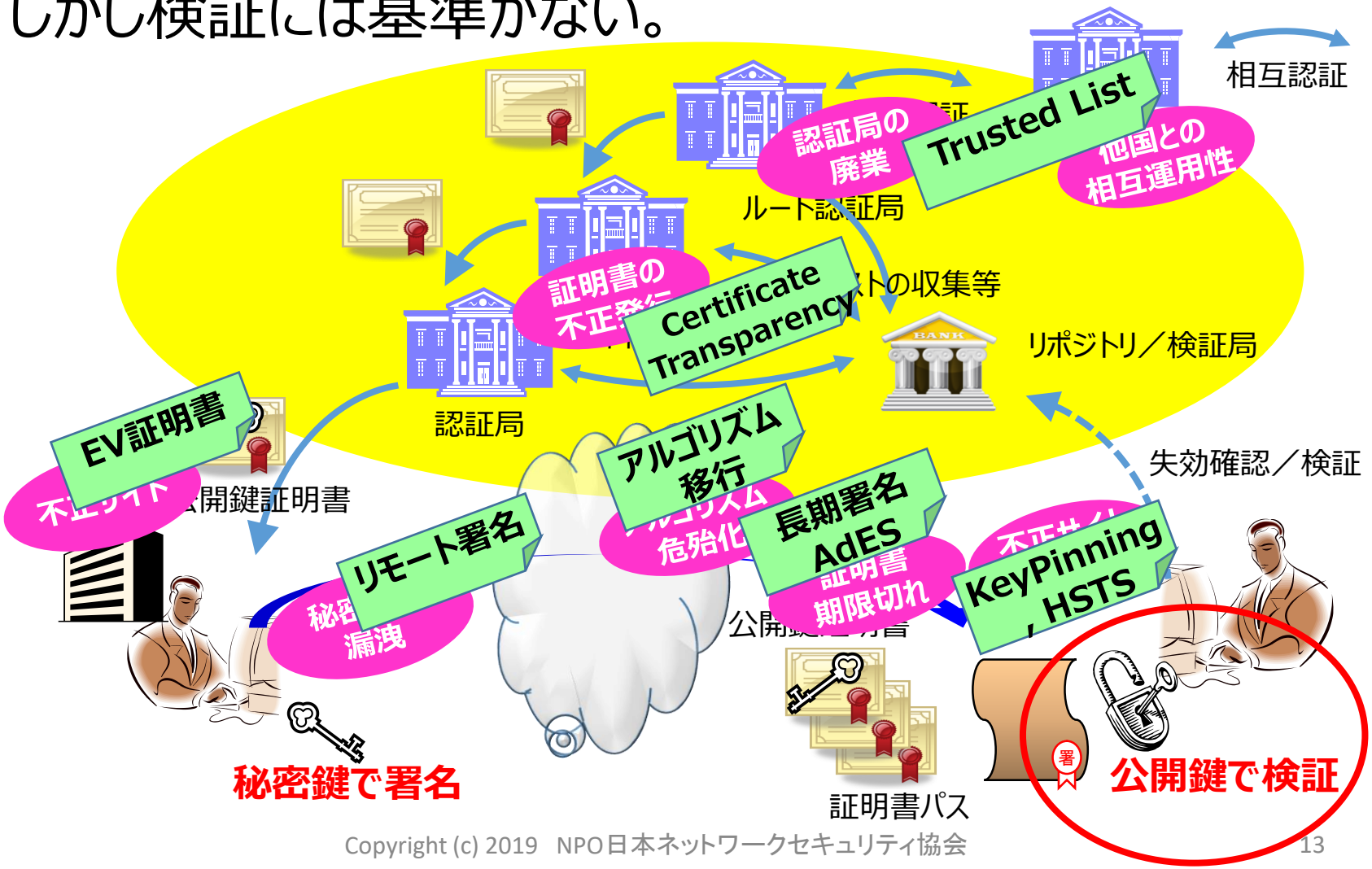
対策の例

（これだけではないが）



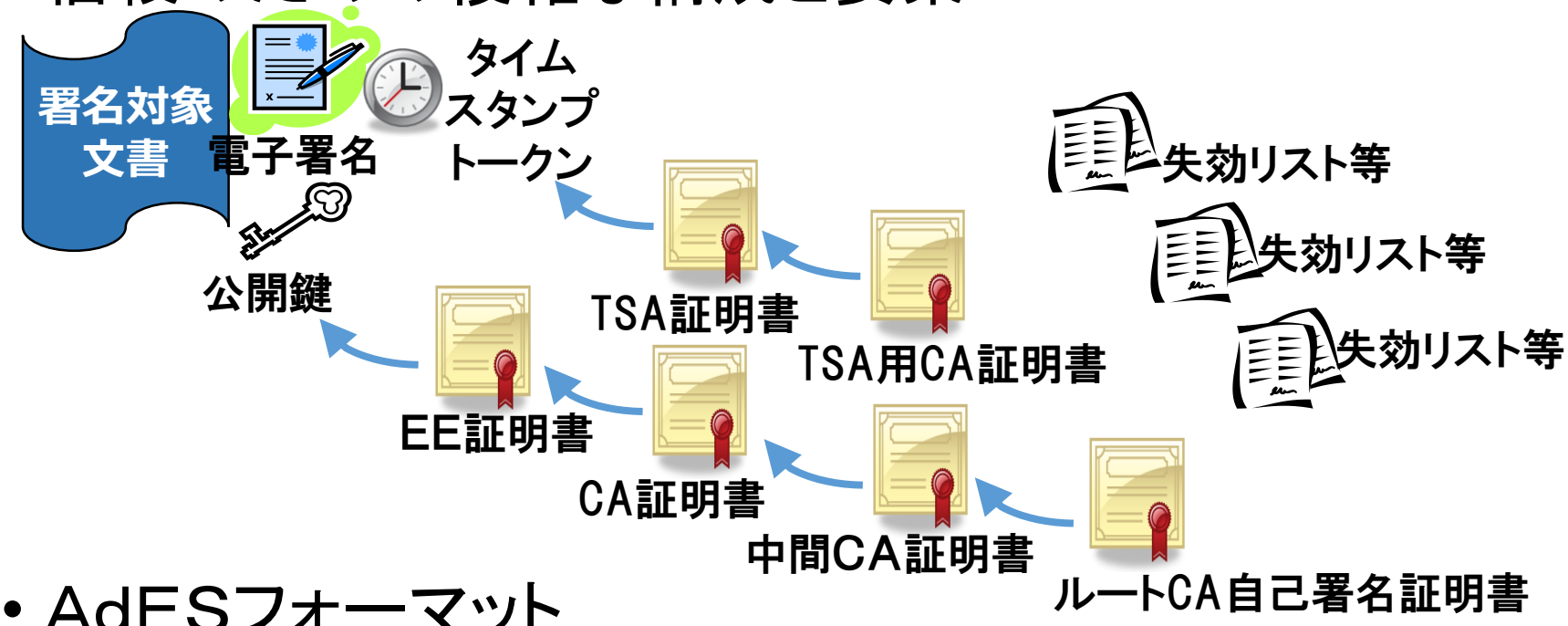
検証は最後の砦

しかし検証には基準がない。

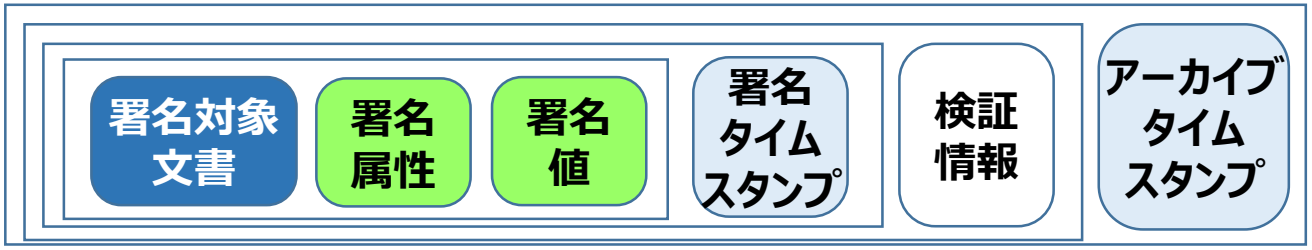


電子署名・検証の特徴

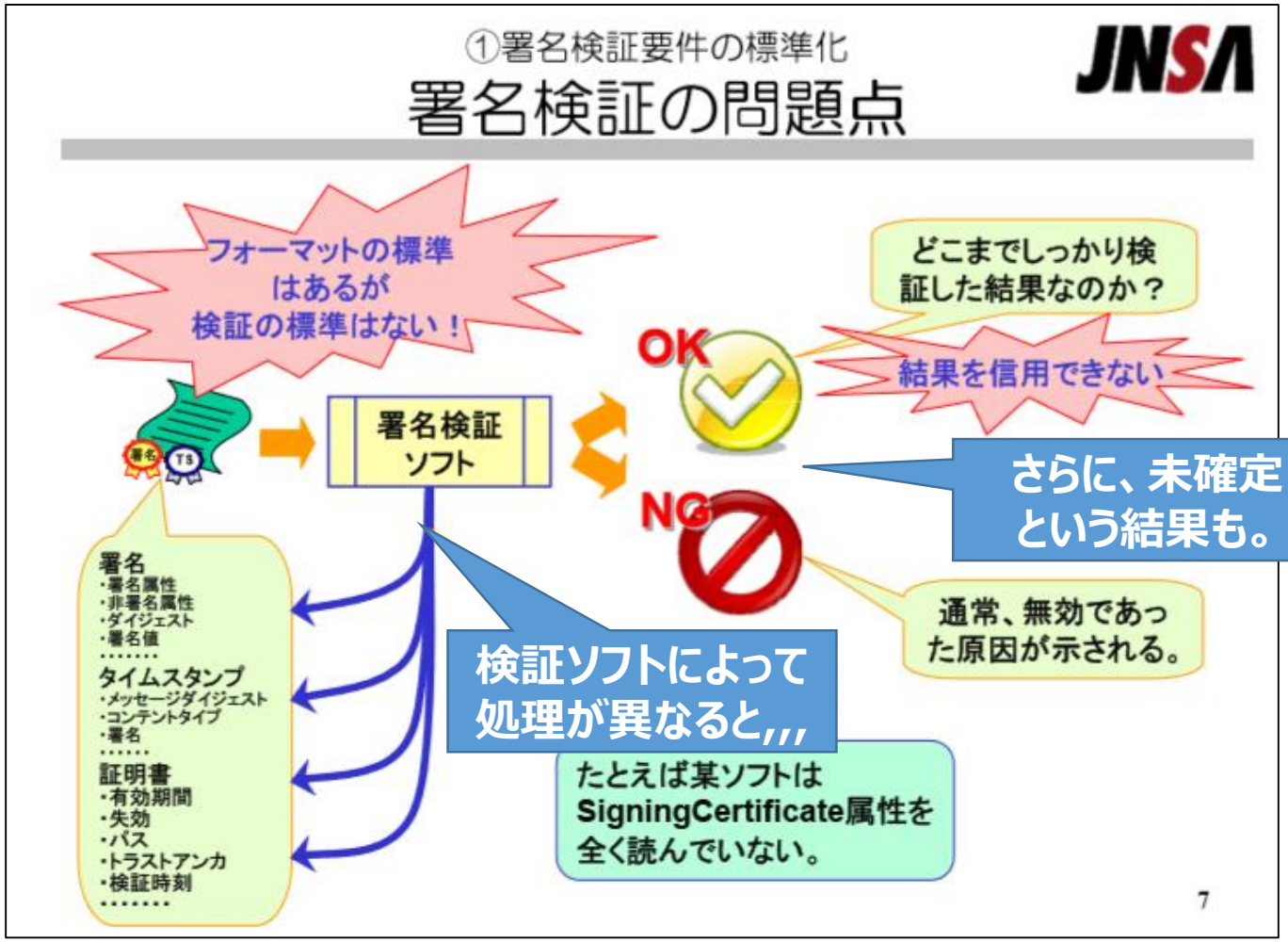
- 信頼のための複雑な構成と要素



- AdESフォーマット



検証標準がないと何が問題か



出典:「PKIday2014 宮崎 一哉」資料に追記

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

検証標準がないと何が問題か

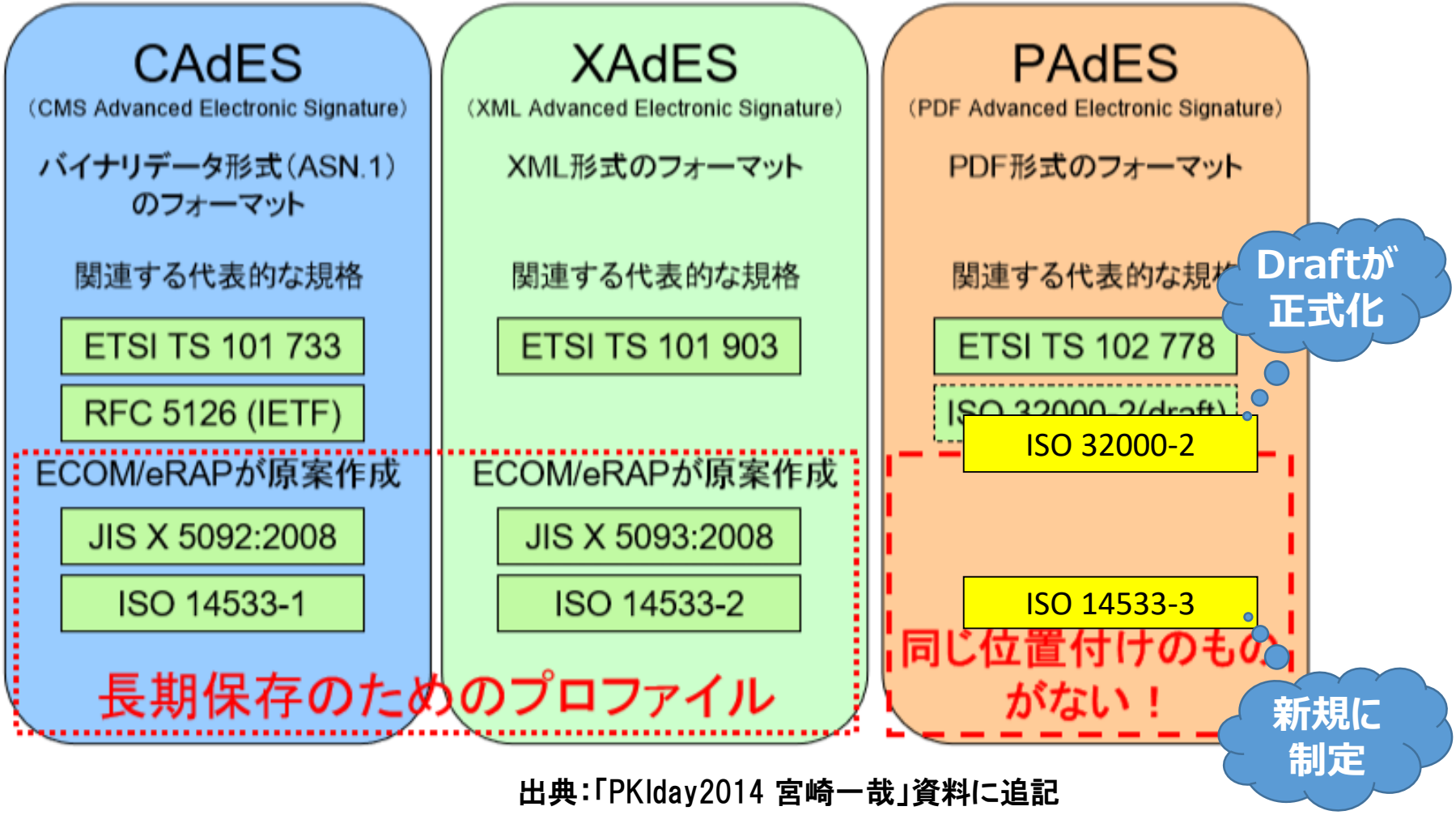
JNSA

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？

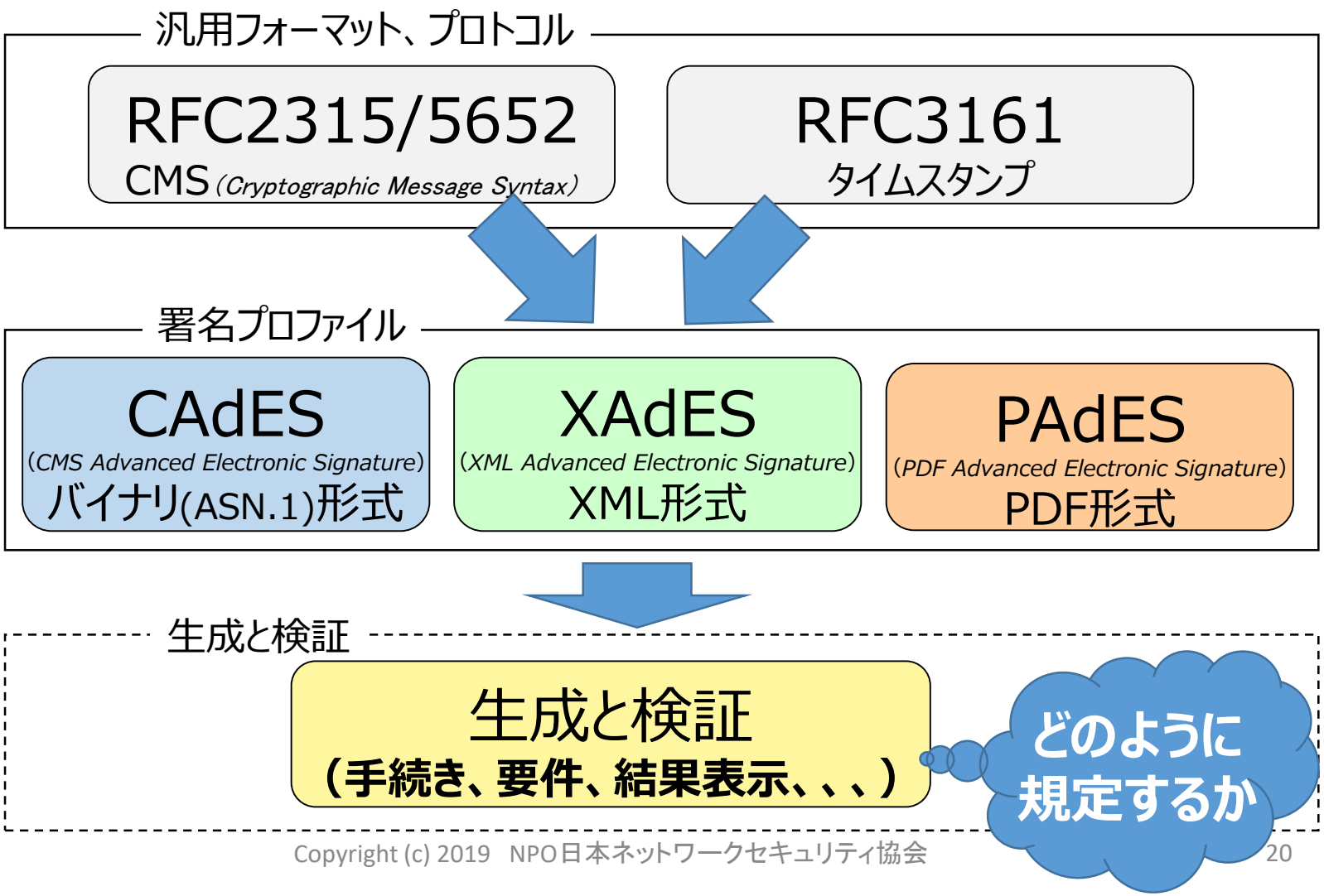
標準化の
経緯と現状
（日欧の状況）

署名プロファイル



出典:「PKIday2014 宮崎一哉」資料に追記

電子署名関連の標準

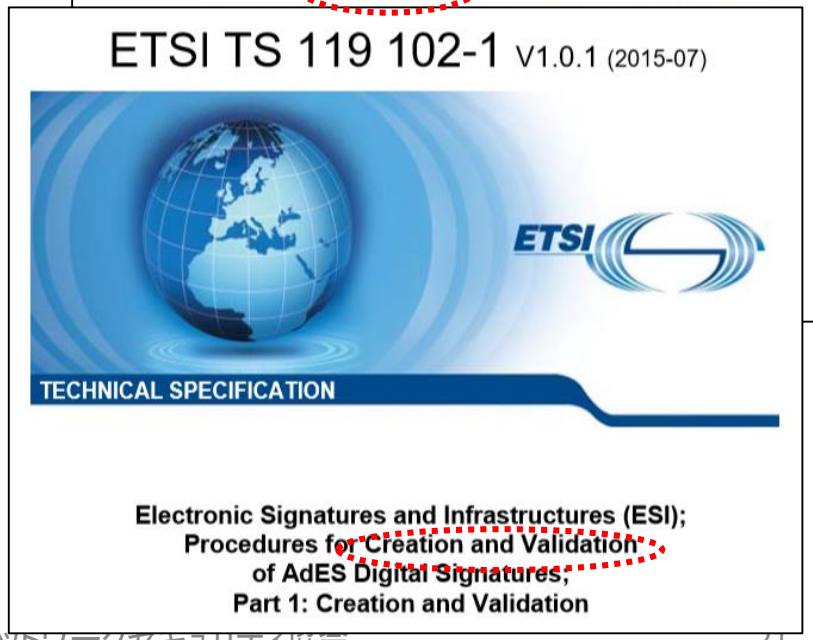


経緯（欧州）

欧州の状況

- 2012年、検証の手順

- 2015年、生成と検証

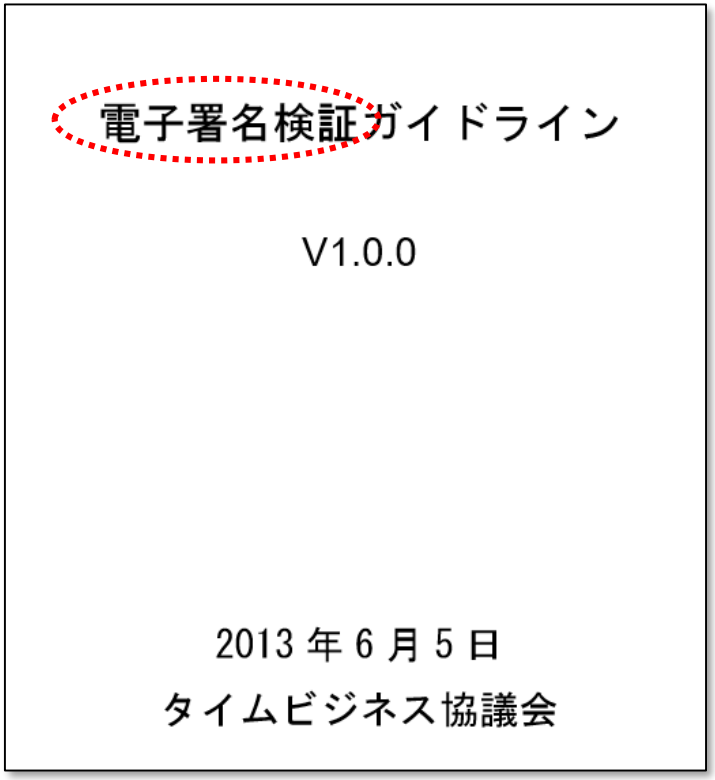


- 2018年、同ver1.2.1(2018-08)

経緯（日本）

日本の状況

- 2010年前後より問題意識
- 2013年、ガイドライン
- 2013～14年、欧州と協議。
  折り合いはつかず、
  標準提案はペンディング。



タイムビジネス協議会（TBF）

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。）

これからの取組み

今の取組み

2018年度より、検証TFを再開

- まずは、ETSI版(TS 119 102)の理解
  - Part１:プロセスの解析・・・フロー化
  - Part２:結果表示の解析（予定）
- 次に、日本版(TBF-2013)との対比予定

調査対象

	版番号	題名	内容
EU版最新TS	ETSI TS 119 102-1 V1.2.1 (2018-08)	"Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"	Procedure
	ETSI TS 119 102-2 V1.1.1 (2018-08)	"Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report"	Report
日本版	電子署名検証ガイドライン V1.0.0 2013/6/5		

署名プロセス(モデル)

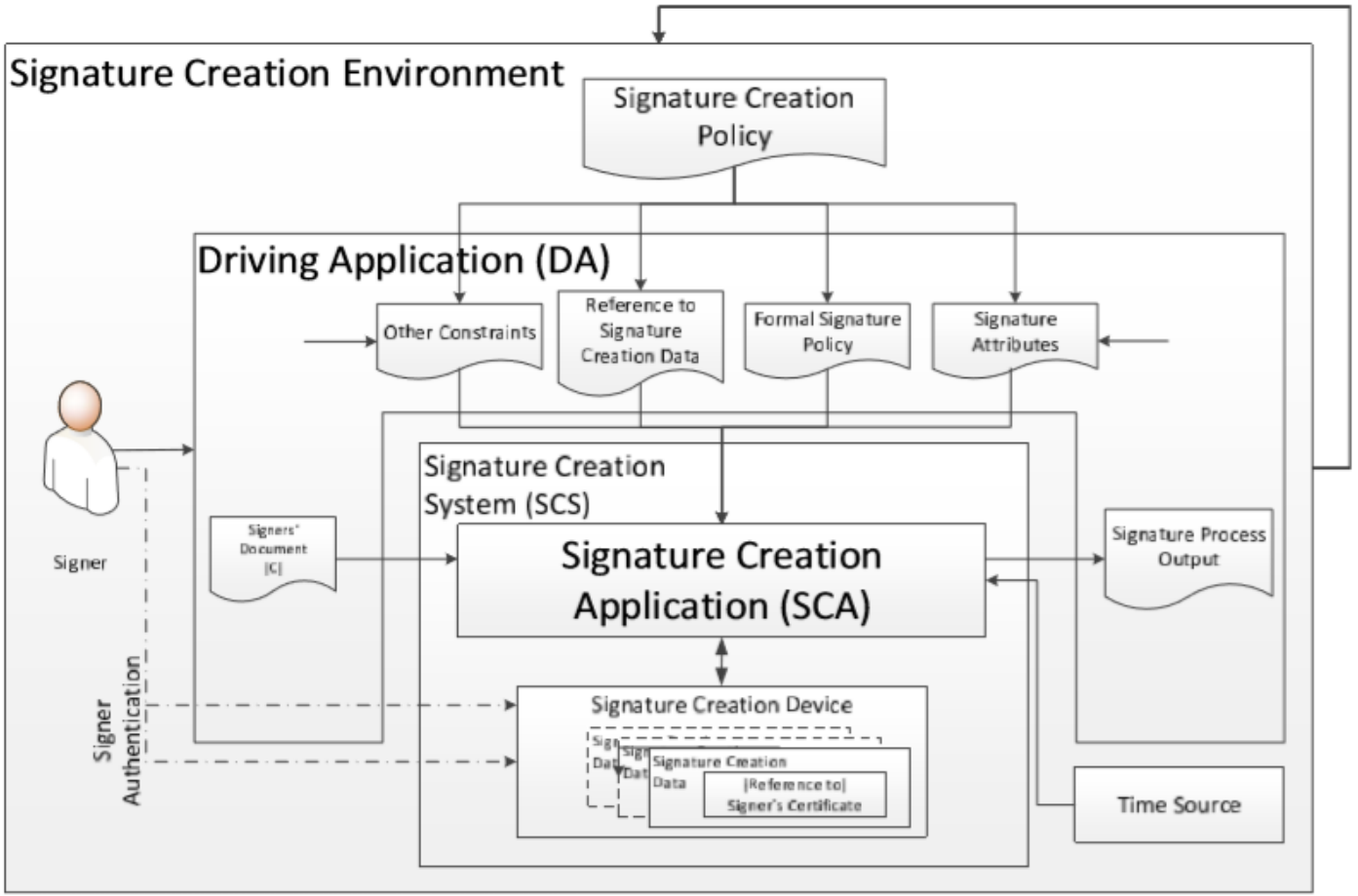


Figure 1: Functional Model of Signature Creation

出典:ETSI TS 119 102-1 V1.2.1 (2018-08)より

検証プロセス(モデル)

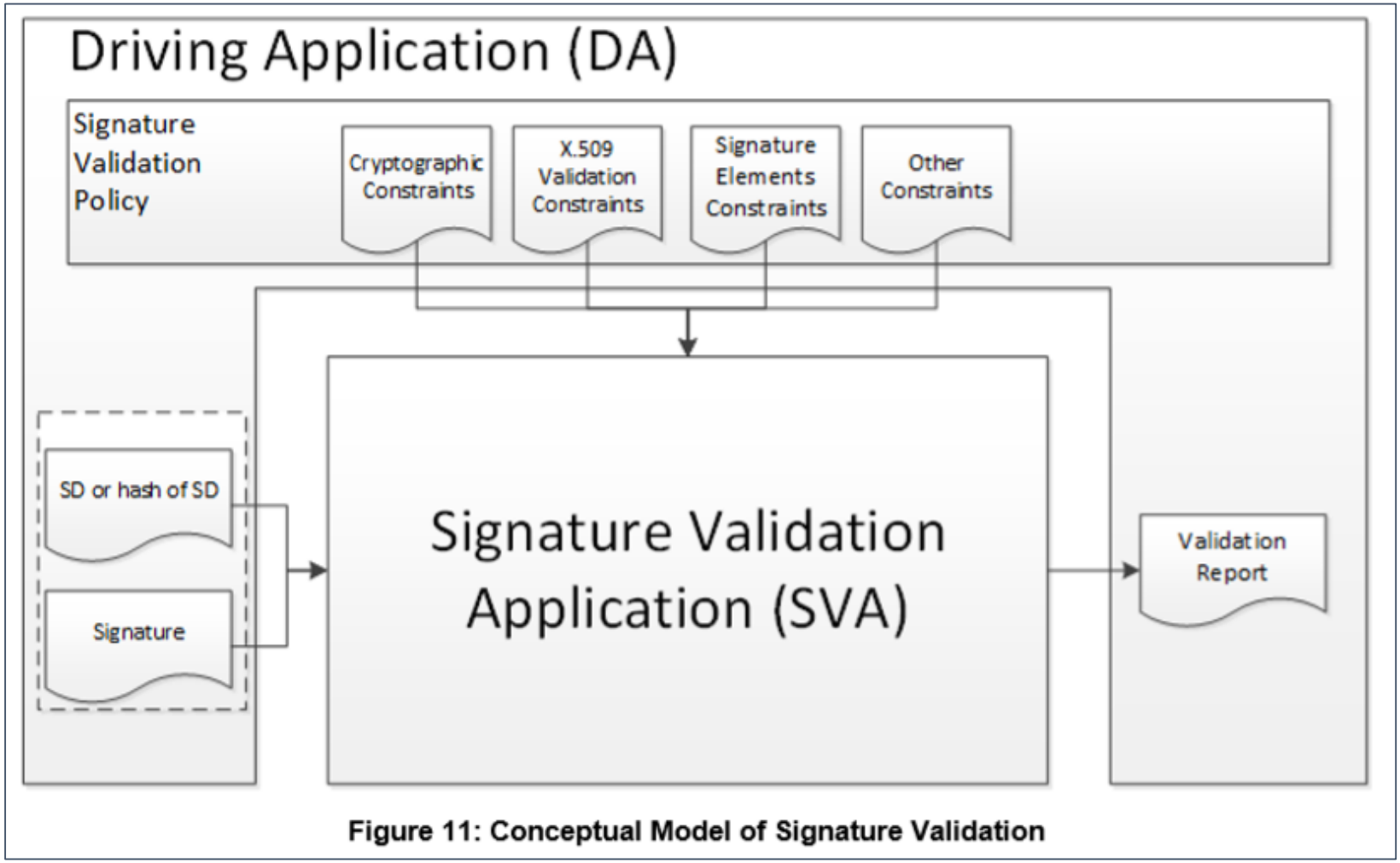


Figure 11: Conceptual Model of Signature Validation

出典:ETSI TS 119 102-1 V1.2.1 (2018-08)より

署名のライフサイクル

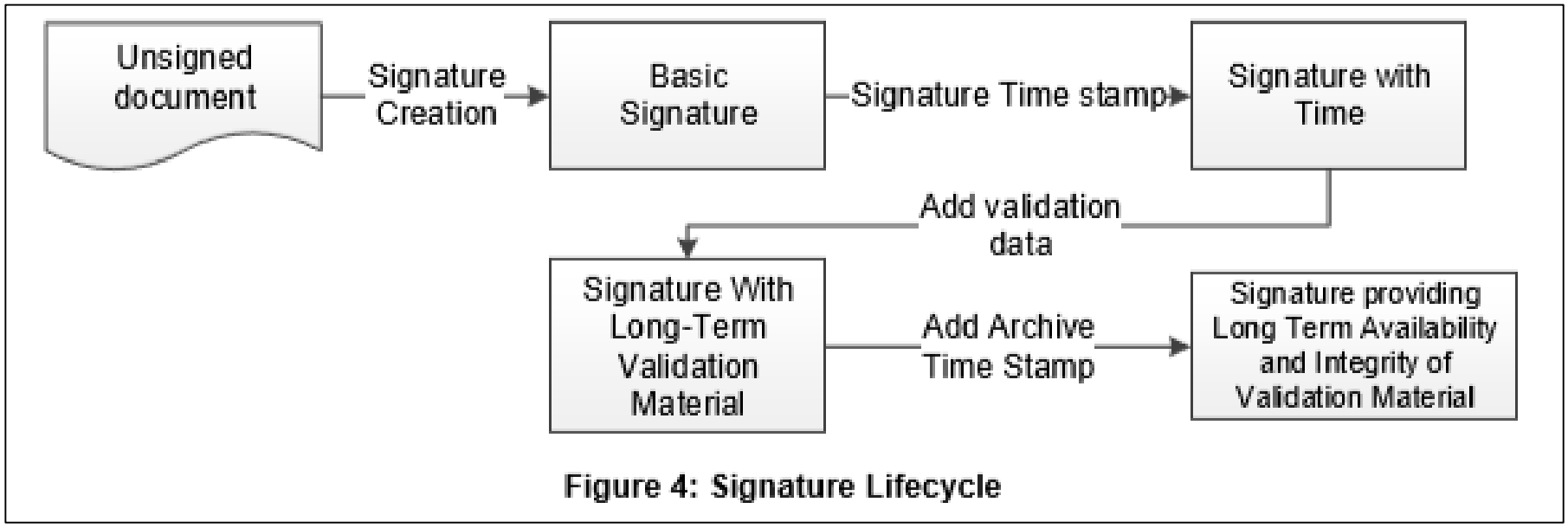
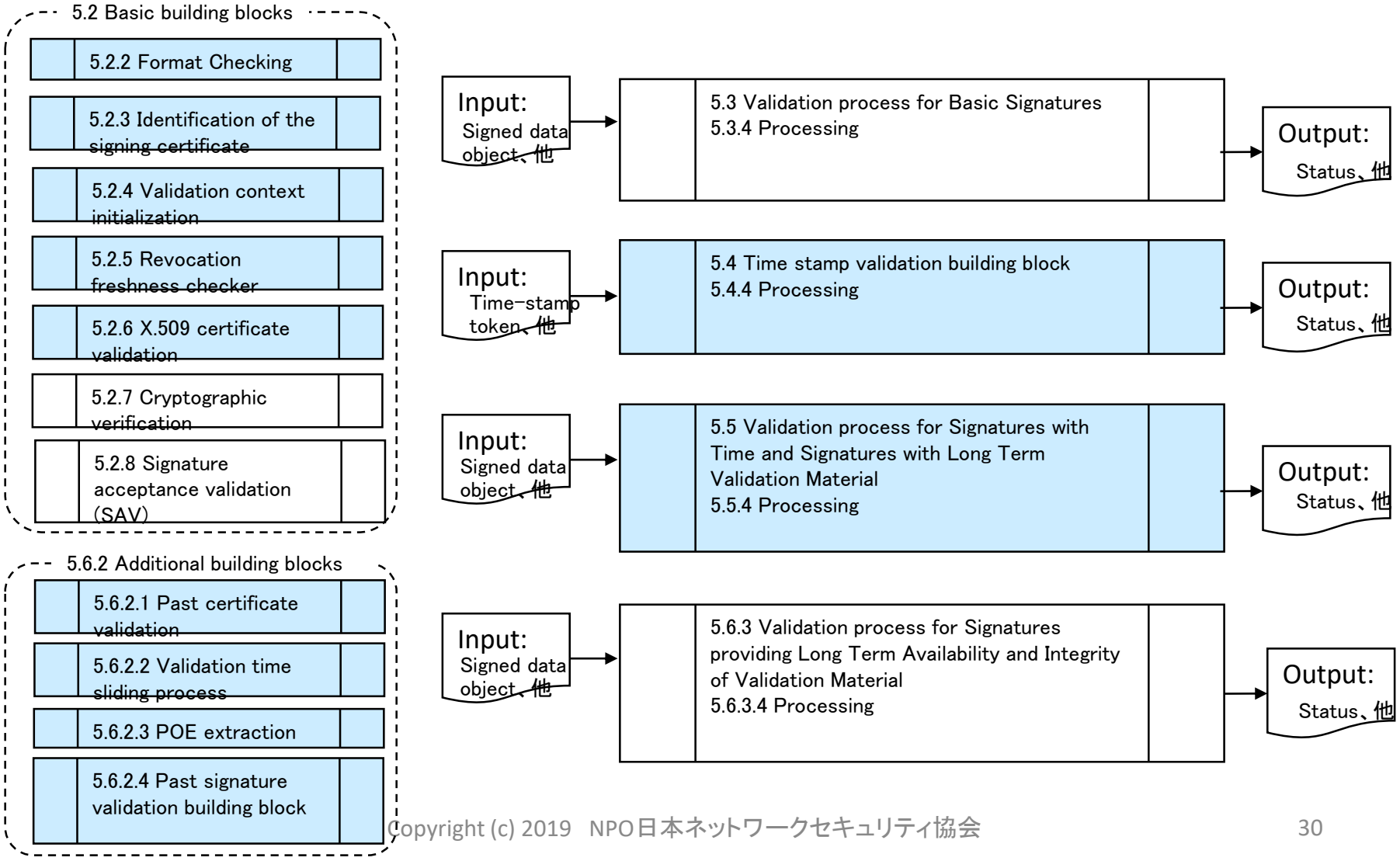


Figure 4: Signature Lifecycle

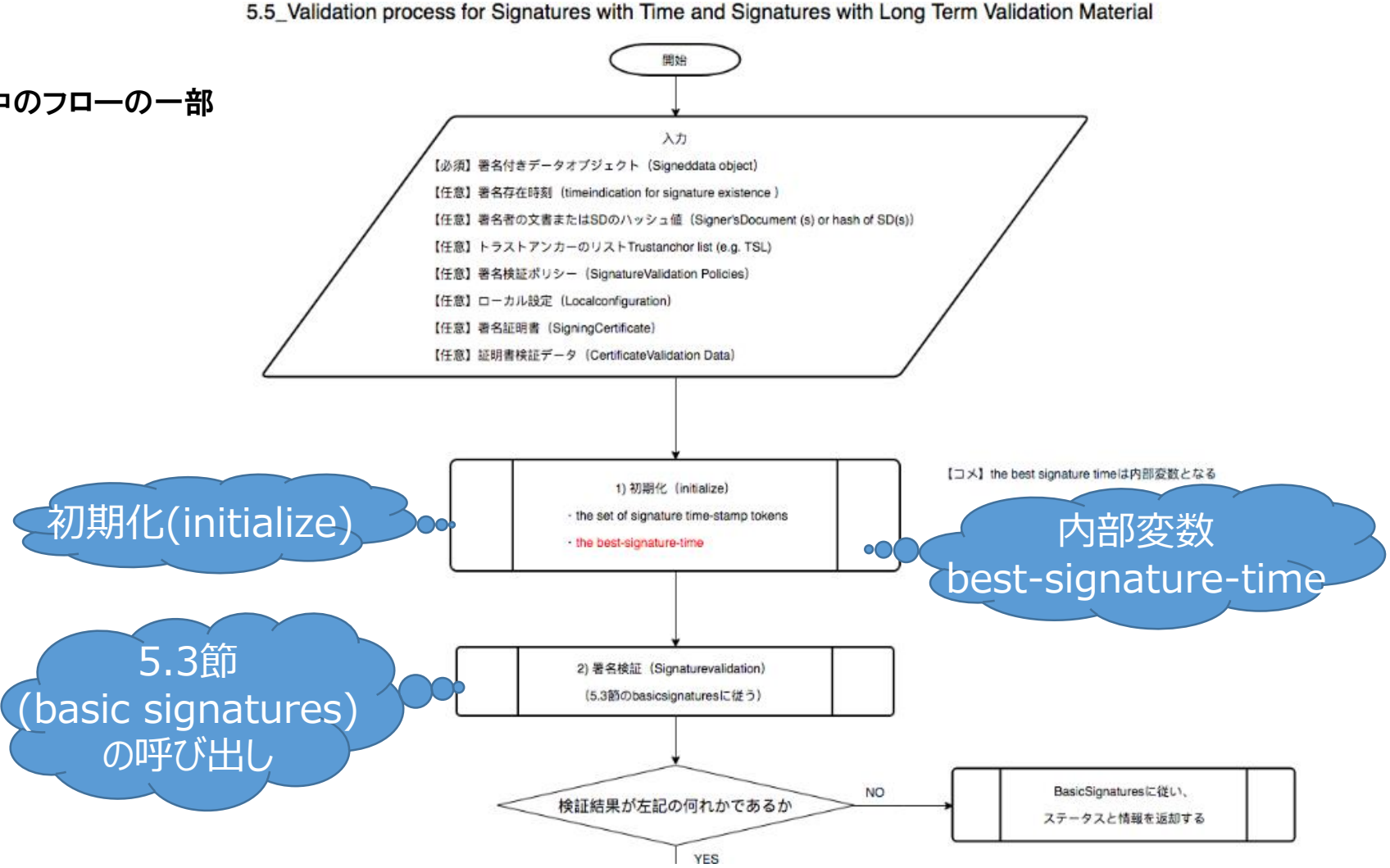
出典:ETSI TS 119 102-1 V1.2.1 (2018-08)より

検証プロセス（全体）



検証プロセスの詳細フロー

作成中のフローの一部



欧州版で気になること

- VALIDとなる要件の明確化
  - VALIDが最後まで分からないこともある。
- 必須要件とオプション要件の区別
  - 例えば、検証プロセスの一部を検証制約で無視してよいものか？
- ポリシーや制約(Constraints)が頻出
  - 整理は不要か？
- 記述されている検証プロセスの妥当性
  - PoE抽出プロセス、Control-timeの判定など
  - タイムスタンプ検証の記述が薄い、など

今後の取組み(案)

① 署名検証規格の現状調査報告書の作成
- EU版の分析、日本版との対比

② 日本版ガイドライン作成
- TBF版の更新・見直し
- 供給者適合宣言書を含む

③ 署名検証の標準化の検討
- EU対応
- 国際標準、国内標準

④ 認証、評価の仕組みの検討
- 製品実装調査
- 基準作り、プラグテスト

電子署名WG
検証TFに
参加者募集中！

ご清聴ありがとうございました

予告

続いて、真正性について、、、