2024年度JNSA活動報告会　2024.7.19

デジタル社会におけるトラストのための電子署名WGの取り組み紹介

電子署名WG 署名検証TFリーダー　政本廣志
（株式会社サイバー創研）

https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog
Peter Steiner's 1993 cartoon, as published in The New Yorker

On the Internet, nobody knows you're a dog

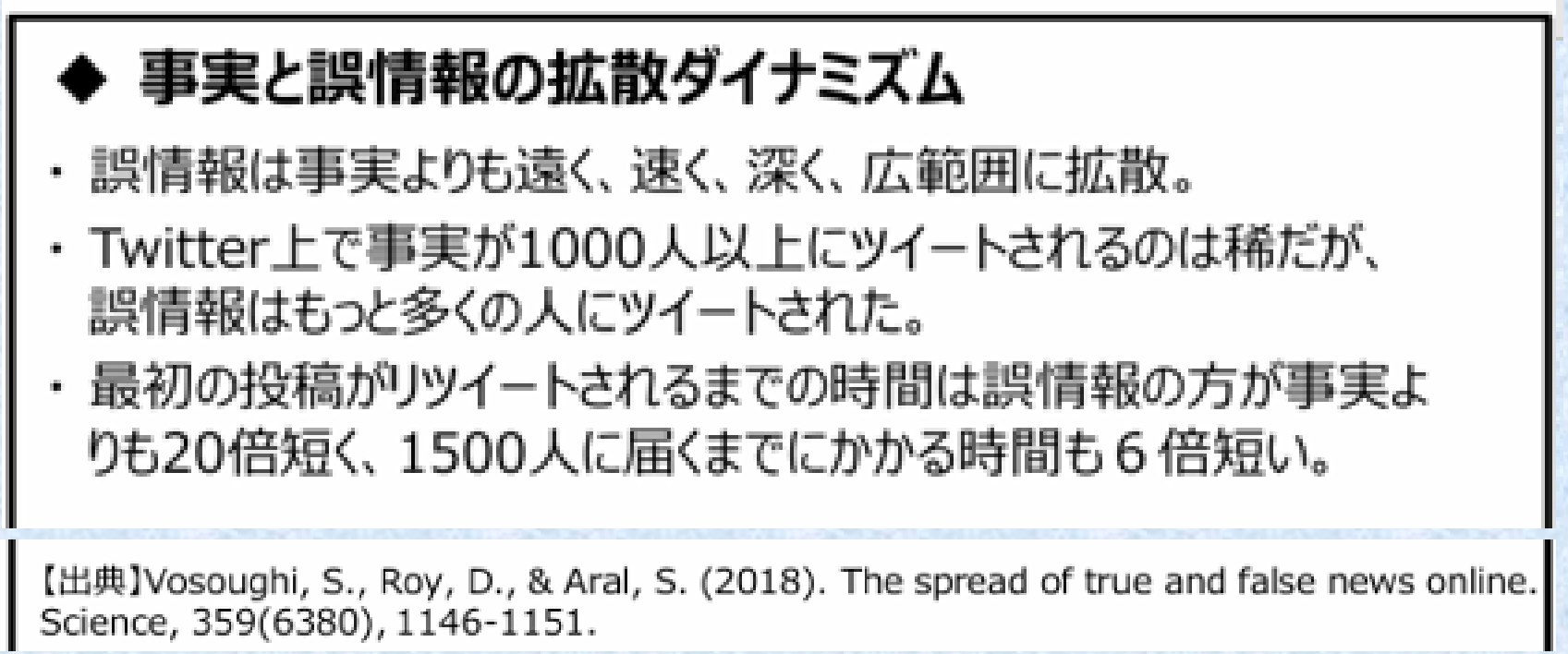
Peter Steiner's 1993 cartoon, as published in The New Yorker

つまり、相手は本当は誰だか分からない。

ちなみに、1993年は
・Mosaic公開
・HTMLバージョン1.0公開
・郵政省がインターネットの商用利用許可
（JPNICインターネット歴史年表より）

デジタル社会におけるトラストの問題

相手は誰か分からない/誰が作ったデータか分からない
正しいデータか分からない/元のデータの通りか分からない



デジタル空間における情報流通の健全性確保の在り方に関する検討会（第1回）令和5年11月7日
・参考資料1-1　デジタル空間における情報流通に関する現状と課題 参考資料PDF
https://www.soumu.go.jp/main_content/000910440.pdf

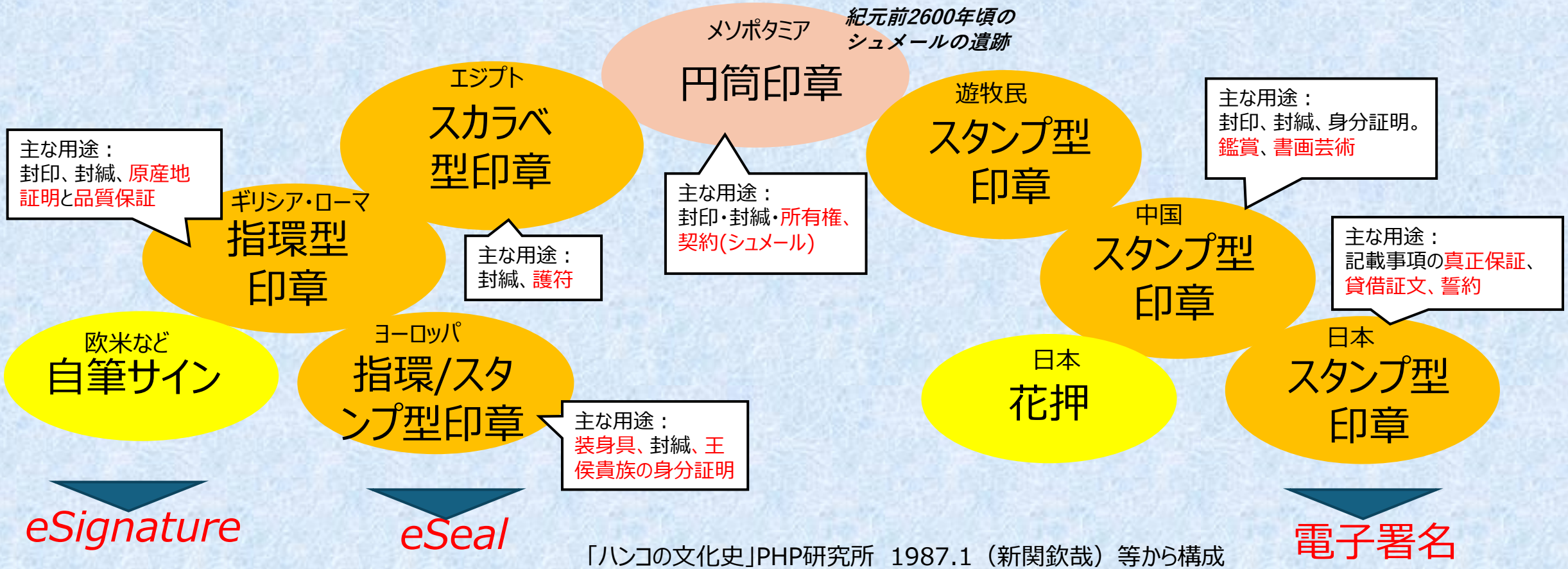
アナログ時代のトラストは、、

誰が作ったものか分からない　→　署名・押印

元の通りかどうか分からない　→　封緘

それなりに担保されてきた。

アナログは4000年以上の歴史



「ハンコの文化史」PHP研究所　1987.1（新関欽哉）等から構成

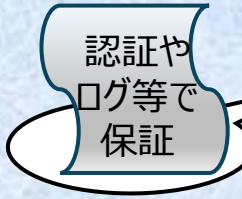
デジタル時代の対策：さまざまな電子署名

電子署名

本人と電子文書との関係を示すために本人が作成した電子データで、
広く電子パッドに手書き署名するようなものも含む

電子サイン

電子印鑑



各社固有の
署名サービス

デジタル署名

電子署名の一種で、署名者の身元とデータが改ざん
されていない事を、暗号技術を使って検証できるもの

事業者型署名

欧州の先進電子署名
(Advanced)

リモート署名

欧州の
適格電子署名
(Qualified)

ローカルな
デジタル署名

2022 JPNIC勉強会より（「2021 JNSA活動報告会(政本資料)」を再構成）

署名検証TFの2023年度活動と成果

- 2023/12/22
  「**デジタル署名検証ガイドライン**」v1.1を公開
  （2021年公開版の改訂）
  https://www.jnsa.org/result/e-signature/2023/2023-001.pdf

- 2023/12/22
  「**トラストのためのデジタル署名検証解説**」を公開
  https://www.jnsa.org/result/e-signature/2023/2023-002.pdf

基本と応用に
レベル分けを
試みた

デジタル社会のデータのトラスト

・誰が作ったものか（署名者）／元の通りかどうか（非改ざん）

・署名等で担保することは重要だが、検証しなければ意味がない！

表1.2-1　アナログの署名等における検証

	手書きサイン	押印	封緘
署名者の確認	本人のみが書ける前提、筆跡鑑定	本人のみが印章を持つ前提、印鑑の登録制度	本人/当該組織のみが印章を持つ前提、登録制度
非改ざん確認	紙やインクの状態で判断	紙やインクの状態で判断	封筒や封蝋の状態で判断

表2.2-1　各種の電子署名における検証

		認証記録型署名	ローカル署名	リモート署名	事業者型署名
署名者の確認	身元確認	事業者による保証	認証局が発行した電子証明書	認証局が発行した電子証明書	事業者による保証
	当人確認	事業者による利用者認証	(本人のみが署名鍵を持つ前提)	事業者による利用者認証	事業者による利用者認証
非改ざん確認	改ざん検知	事業者による記録を確認	本人のデジタル署名を検証	本人のデジタル署名を検証	事業者のデジタル署名を検証
	長期の保証	事業者の継続	長期署名を検証	長期署名を検証	事業者の継続

署名者の確認

・基本技術と運用（証明書）
PKI(Public Key Infrastructure)

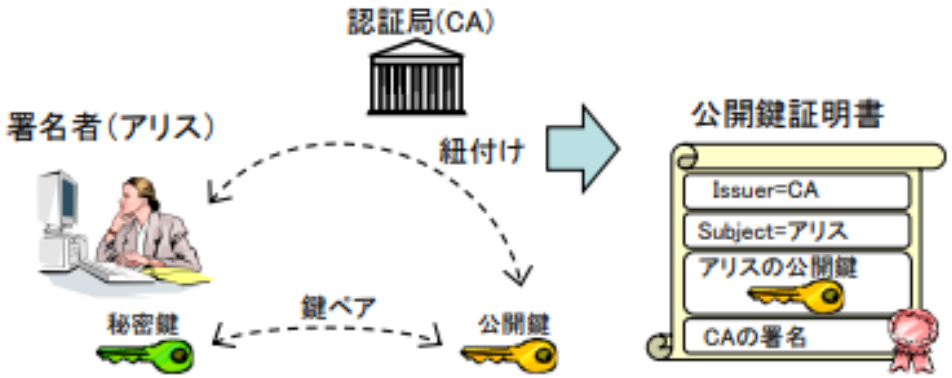


図 3.1.2-1 認証局と公開鍵証明書

[認証パス]

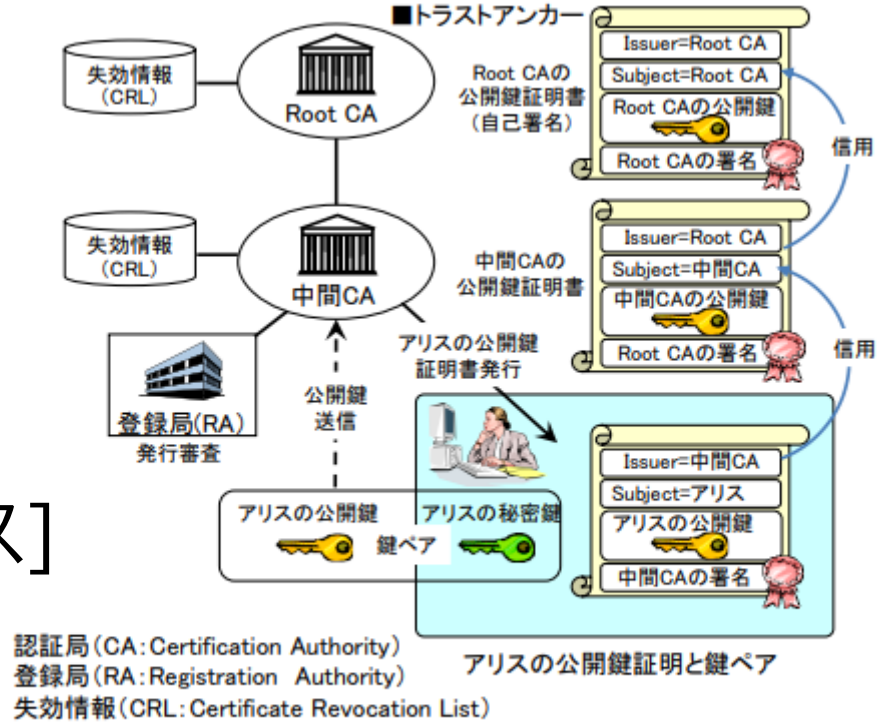


図 3.1.2-2 認証局の階層構造と公開鍵証明書

[失効情報]

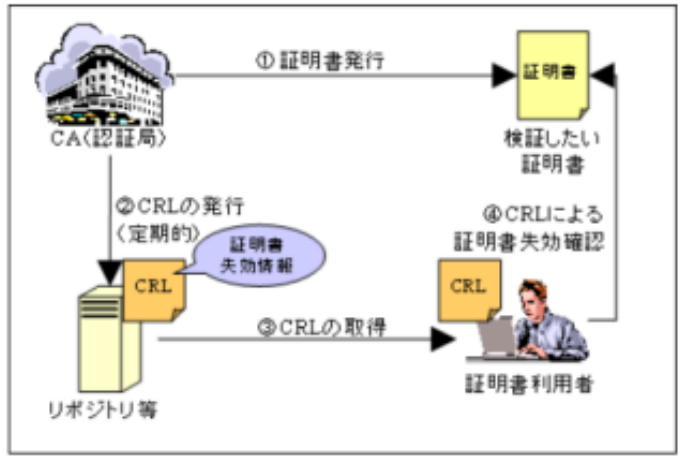


図 3.1.2-3 証明書の失効(出典:「PKI 関連技術情報」[5])

データ非改ざんの確認

・技術的な原理（公開鍵暗号）

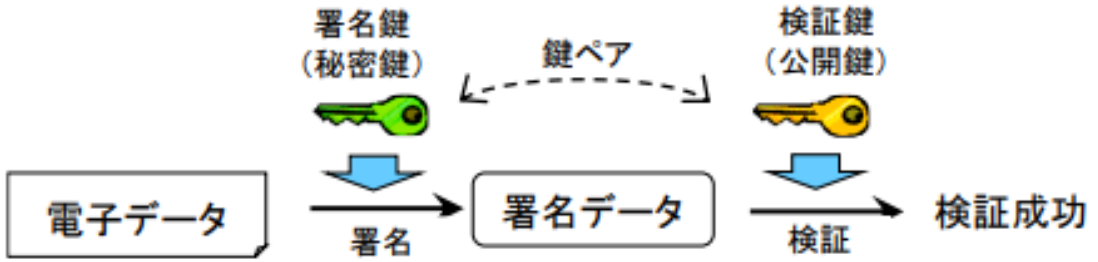


図 3.1.1-1 公開鍵暗号技術による署名・検証

[検証の原理]

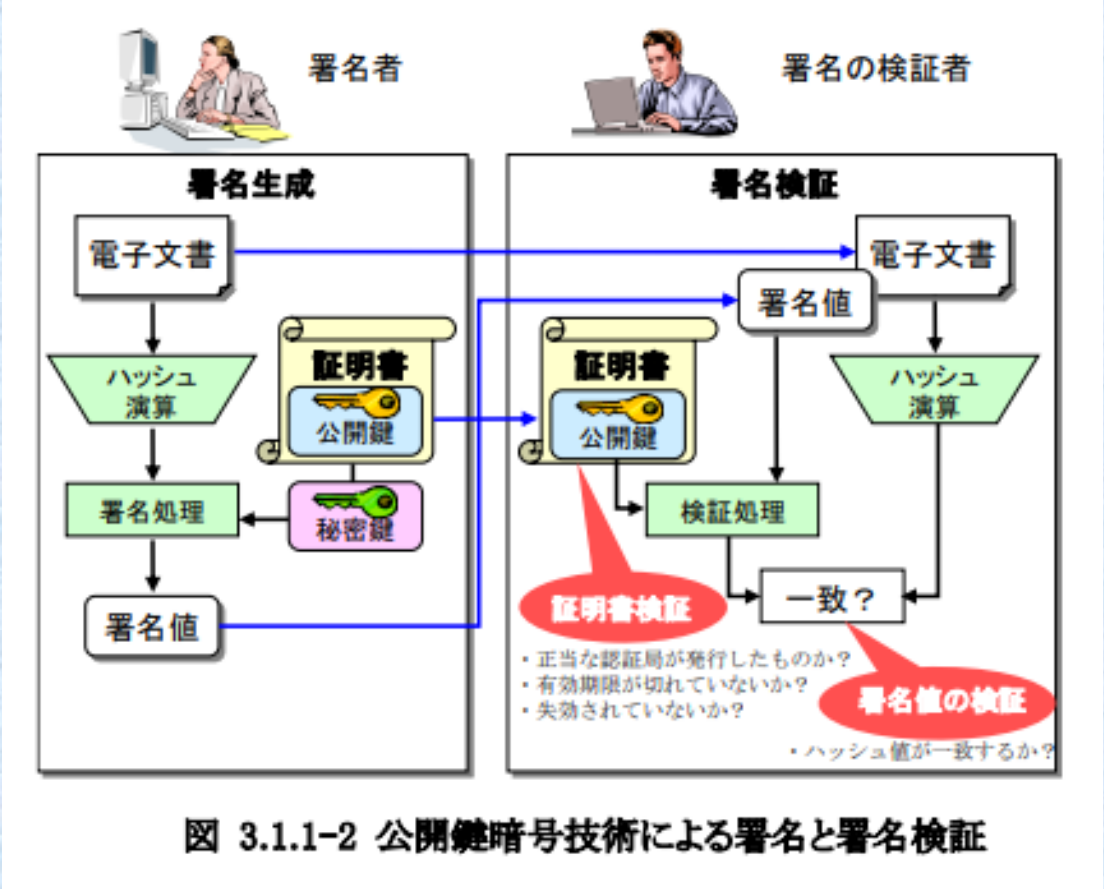


図 3.1.1-2 公開鍵暗号技術による署名と署名検証

トラストの確認

基本原理に加えて以下も注意が必要。

[署名者の確認]
- トラストアンカー
- 身元確認と当人確認
- 失効情報の信頼性

[非改竄の確認]
- アルゴリズムと鍵長
- 鍵保管の安全性

[その他]
- 時刻情報
- 署名制約

さらなる詳細は附録参照

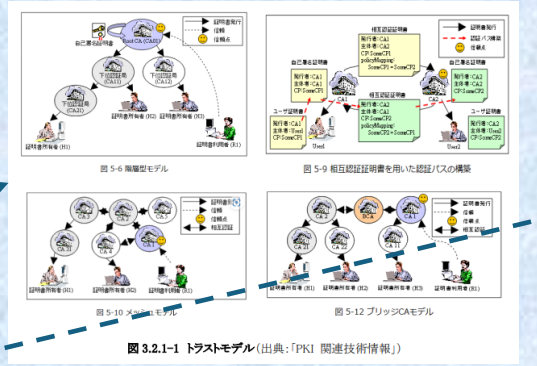


図 3.2.1-1 トラストモデル（出典：「PKI 関連技術情報」）

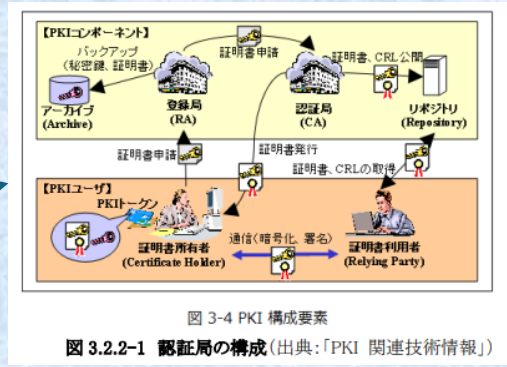


図 3-4 PKI 構成要素

図 3.2.2-1 認証局の構成（出典：「PKI 関連技術情報」）

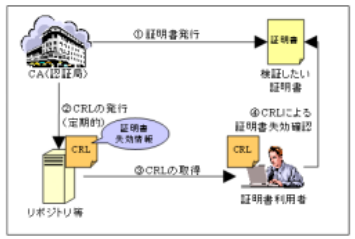


図 4-1 CRL モデル概要

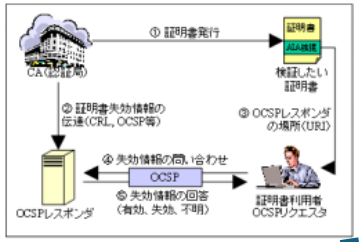


図 4-9 OCSP 概要

図 3.2.3-1 失効情報の確認方法（出典：「PKI 関連技術情報」）

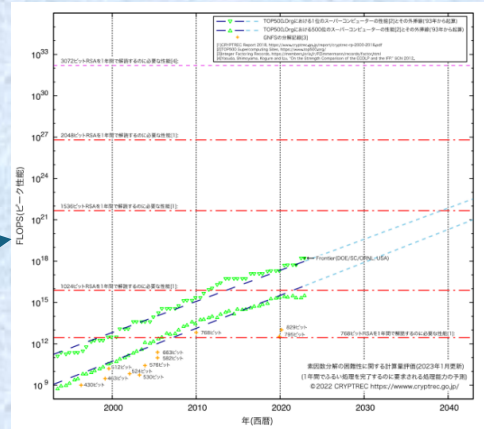
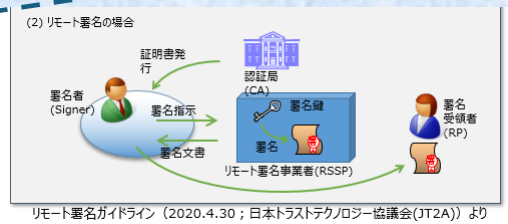
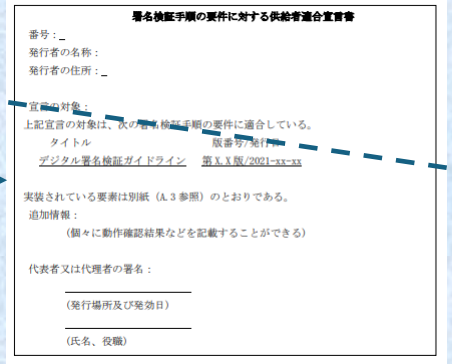


図 3.2.4-1 素因数分解の困難性に関する計算量評価（2023 年 1 月更新）
「暗号技術検討会 2022 年度報告書」より



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



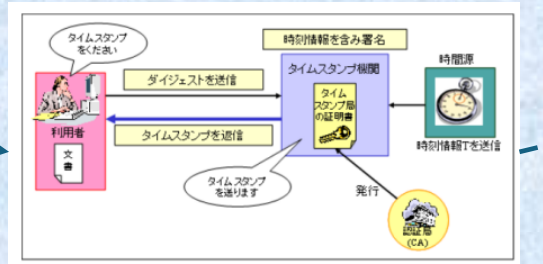


図 3.2.6-1 タイムスタンプの仕組み（出典：「PKI 関連技術情報」）

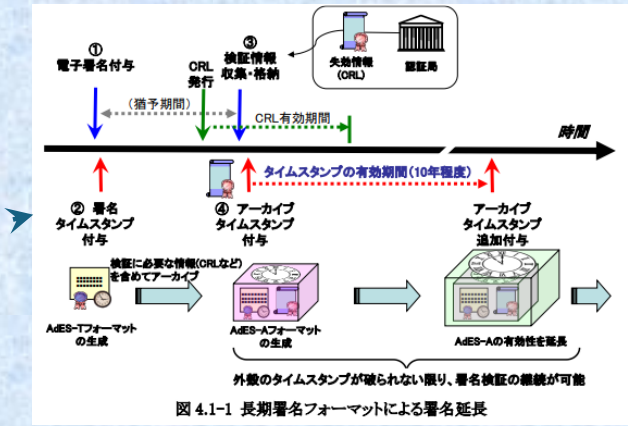


図 4.1-1 長期署名フォーマットによる署名延長

まとめ

データのトラスト要素		デジタル署名の原理	基本の処理（3.1節）	トラストの確認（3.2節）	さらなる情報、トピック（附録）
署名者の確認	身元確認	公開鍵証明書とPKI	証明書検証 ・パス検証 ・失効検証	トラストモデルとトラストアンカー 身元保証 失効情報の確認	トラストフレームワークと国際相互運用(A.4) 証明書検証の留意点(A.6) 有効性モデル(A.2) 猶予期間(A.8)
	当人確認	(ローカル署名は本人所持が前提)	リモートでは認証/認可	（鍵管理）	リモート署名(A.5)
非改ざん確認	改ざん検知	公開鍵暗号技術による検証	デジタル署名検証	アルゴリズム/鍵長 鍵管理方法	（検証ガイドライン付属書C）
	長期の保証	タイムスタンプによる保護	長期署名検証（4章）	時刻情報の確認	タイムスタンプのトラスト(A.7)
その他				検証制約の確認	データ形式の留意点(A.3)

今後、検証サービスと検証レポート(A.1)が重要になると想定される。

電子署名WGの構成と活動内容

JNSA 標準化部会

電子署名WG

ISO/TC154国内審議委員会の運営支援、ETSI/ESI会議参加、ISO/SC34及びJAHISのリエゾン、電子署名関連パブコメへの対応等

- **標準原案作成TF**

  長期署名プロファイル標準の制改定（ISO、JIS）

- **署名検証TF**

  署名検証プロファイル・ガイドラインの検討、普及

- 署名保証レベルTF(予定)

  電子署名の保証レベルに関するガイドライン検討

JT2A（日本トラストテクノロジー協議会）

信頼性を担保するための技術等の検討（「リモート署名ガイドライン」、「民間電子サービスにおける真正性保証の解説書」等を公開）