セコムIS研究所
Intelligent Systems Laboratory

InternetWeek2021
C19 電子契約, 公開鍵基盤(PKI), 証明書, リーガルテックの基盤技術

電子署名の明日に向かって

2021年11月25日

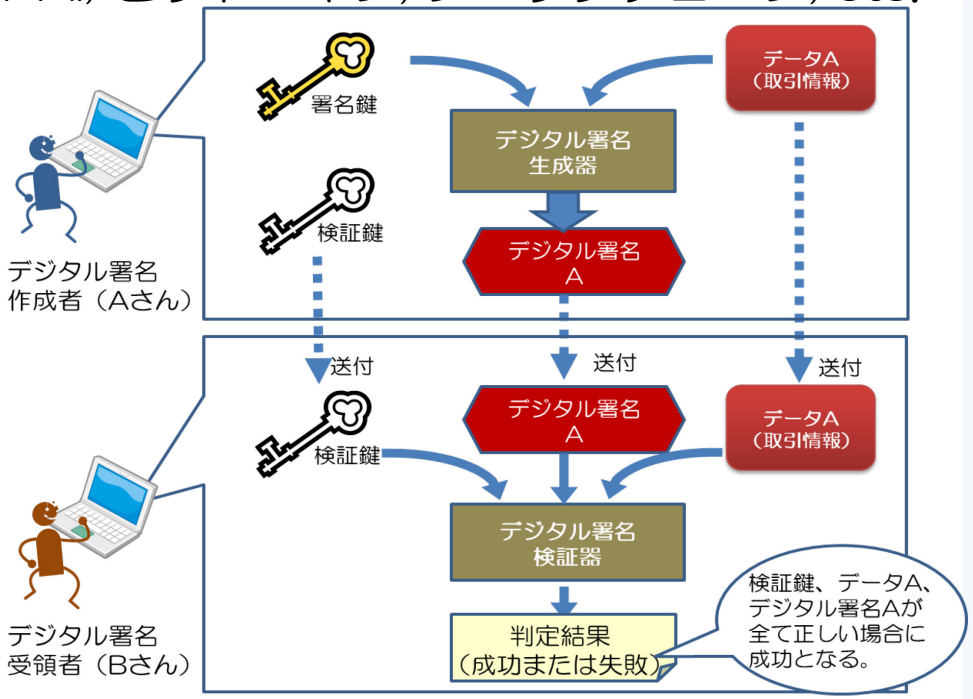
セコム株式会社　IS研究所
コミュニケーションプラットフォームディビジョン
暗号・認証基盤グループ　主任研究員
佐藤雅史

デジタル署名？電子署名？

セコム IS研究所
Intelligent Systems Laboratory

デジタル署名(技術的観点)

- 暗号技術(公開鍵暗号)。
- 署名鍵の所有者が作成したことが証明できる。データ改ざん検知ができる。
- ユーザ/デバイス/サーバ認証(Authentication)や電子署名(右記)などに使える。
- PKI, ビットコイン, ブロックチェーン, etc.



電子署名(法制度等の観点)

- ≒否認防止
- デジタルデータ(スキャン画像含む)の内容に対して、合意や意思を示すもの。
  - 行政文書, 電子申請, 契約書, 取引データ etc.
- 広義の電子署名：電子サイン(手書き署名画像等), 合意に至る過程の記録(ログ), デジタル署名, etc.
- 電子署名として成立しうる要件を規定した電子署名法を定めている国もある。
  - 日本の電子署名法、欧州のeIDAS

電子署名としてデジタル署名を使うには？
様々な論点がある。例えば、
- 署名者の本人性
- 否認防止措置

など

デジタル署名を電子署名(否認防止)として使うには？

セコムIS研究所 Intelligent Systems Laboratory

色々な論点の中から、電子署名議論の雰囲気をつかむ一例として。

同じデジタル署名技術は認証用途にも電子署名用途にも応用できるが…

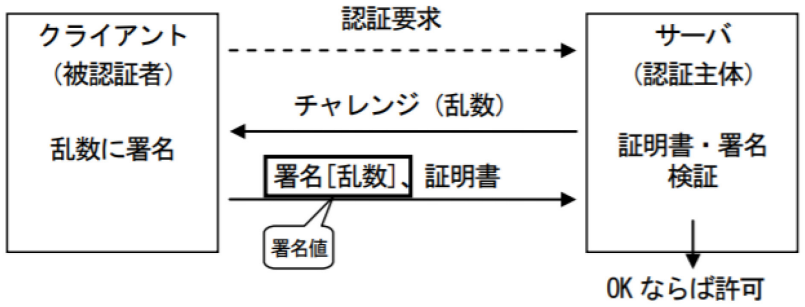


図 9.1.1　単純なチャレンジ&レスポンス方式による認証手順

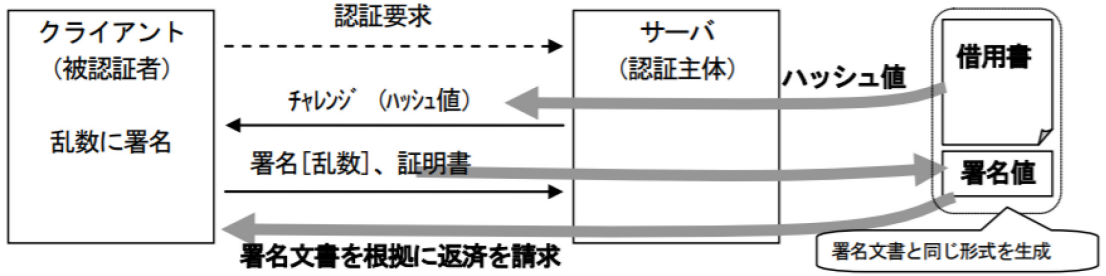


図 9.1.2　意図せぬ電子署名の生成

上図は「JAHIS HPKI電子認証ガイドラインV1.1」より引用

以下を区別する。
- 認証プロトコルで用いるデジタル署名
  ※機械的にソフトウェアが処理する
- 電子署名として用いるデジタル署名
  ※署名者本人が署名行為を認知したうえで実行される

でもデジタル署名の技術自体(アルゴリズム)は一緒。
そこで、署名鍵に関して
- 認証用の署名鍵と電子署名用の署名鍵を別のものにする。
- 鍵使用目的を限定する(X.509証明の記載で可能)。
- 署名鍵を使うときのパスワード(PIN)を別にする。

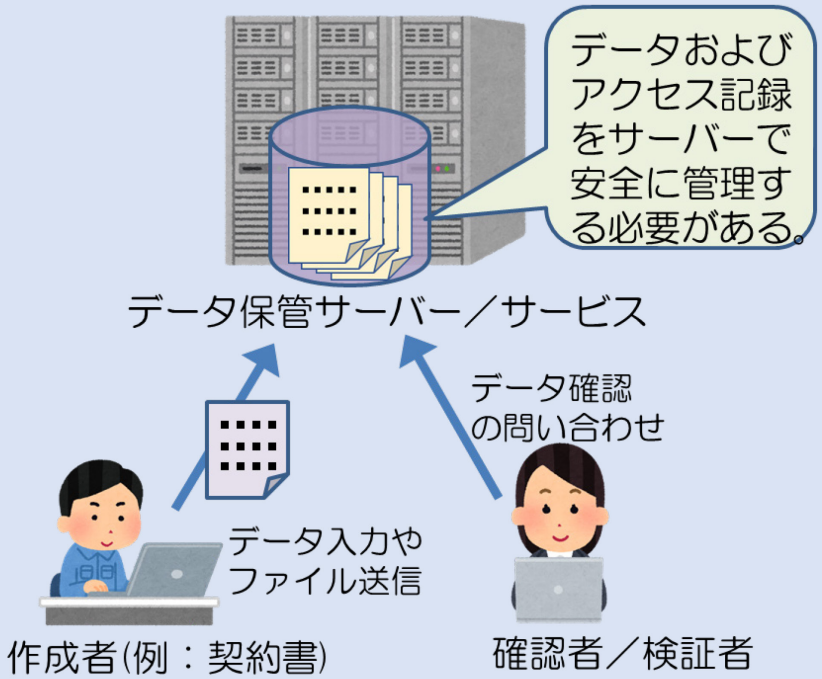
などという事(運用ポリシー)を実施することで署名用途であることを明確化する。

例：公的個人認証での認証用証明書/署名用証明書

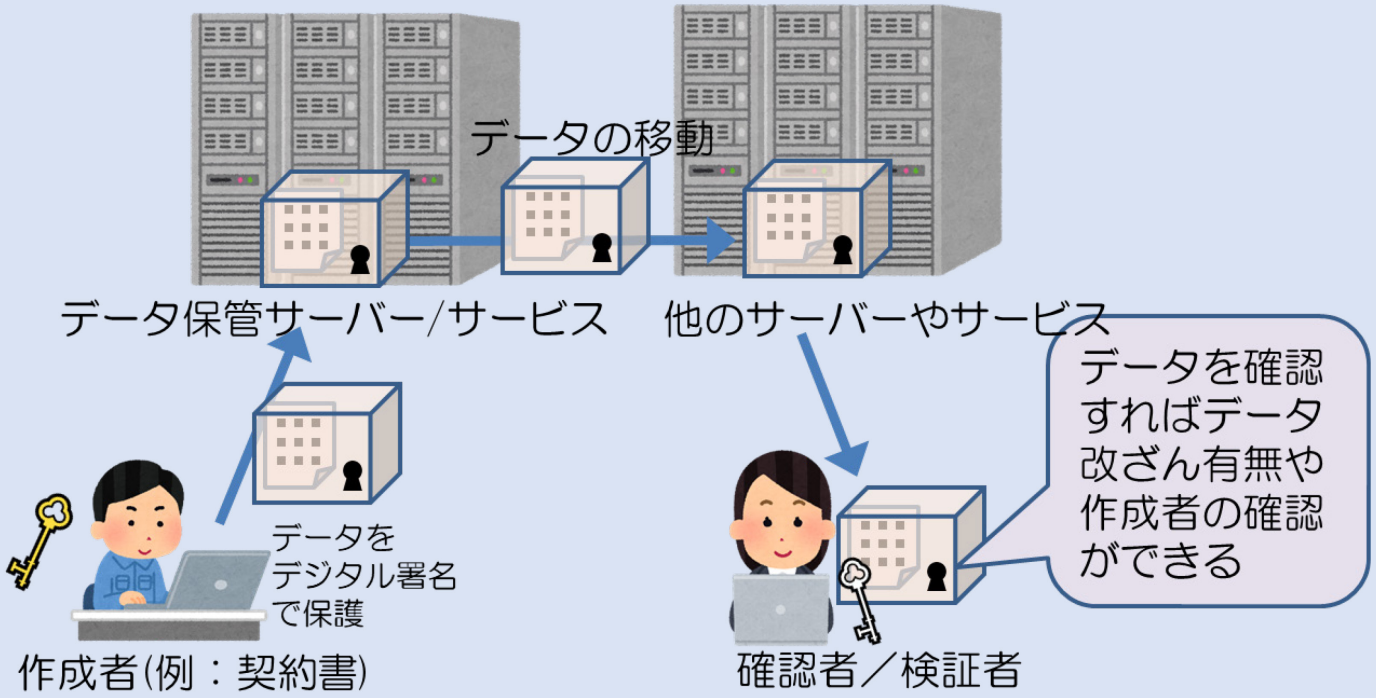
なぜデジタル署名を使おうとするの？

署名者本人に対して発行された証明書＋デジタル署名付きデータにより、そのデータ自身で本人の電子署名(意思)であることを確認できるようにする。

サーバー保管/記録のケース



デジタル署名のケース



(第三者)検証可能性、相互運用性、移行可能性でメリットがある

セコムIS研究所
Intelligent Systems Laboratory

けれども…
デジタル署名に突き付けられた現実？【過去を振り返る】

期待された(デジタル署名的)世界はいずこに？？？

- 対象が従来の紙文書の電子版の域を出ず、人による目視確認等で行われるケースも(電子署名≒押印のイメージの呪い?)
- デジタル署名付きデータも企業や組織内で運用されるだけ？
- 電子契約システム/サービスの相互運用は？
- デジタル署名(電子署名)の検証可能性がそこまで大きな争点とならなかった？

電子署名(デジタル署名)議論の再来 【現在～将来】

セコムIS研究所 Intelligent Systems Laboratory

- 新型コロナ以降の脱ハンコ議論
  - 電子署名法解釈に関わる議論の再燃
  - 「電子署名用途のデジタル署名≒ハンコ」の発想から脱却できるか？
- 分散型アーキテクチャ/データ連携の議論
  - ブロックチェーン, スマートコントラクト, 分散型ID(Verifiable Credentials), etc.
  - 検証可能性(Verifiable)や透明性がポイント。電子署名界隈の議論の再来？
  - 特に分散型アーキテクチャではデジタル署名が重要。対象が自然人とは限らない可能性も。認証や否認防止の区別が難しい場合も。
  - これまで閉じていた電子契約サービスも連携の時代に？！
- eSeal(組織など非自然人によるデジタル署名)
  - 組織等による否認防止, 発出元証明。(≠認証用途)
  - 非自然人のサービス, システム, デバイス等に適用する場合には自然人による電子署名とは異なる考え方が必要にある可能性も 。

電子署名法施行から現在に至るまで周辺の環境も変わりつつある。
電子署名がより身近になる可能性。
議論の巻き戻し(本質的で変わらない部分)もある。
環境の変化にも視線を向けるのも大事。

電子署名(デジタル署名)議論の再来 【現在～将来】

セコムIS研究所
Intelligent Systems Laboratory

電子署名議論再考のヒント

◆ 電子署名保証レベル（宮地さん）
- 電子署名の本人性とは？
- 電子署名の検証可能性とは？
- 技術視点におけるデジタル署名の位置づけとは？

◆ 法制度から見た電子署名技術（宮内先生）
- 電子署名(法/技術)は何を救ってくれるのか？
- 電子署名におけるデジタル署名の意義とは？
- 将来的な電子署名議論の展望は？

電子
電子
議論
環境の変化にも視線を向けるのも大事。