# 電子記録マネジメント視点からの電子署名

財団法人日本情報処理開発協会
主席研究員　木村　道弘

# 目次

- 電子記録マネジメントの必要性
- 電子記録と電子署名の実際
- クラウド時代の電子記録と電子署名

# 電子記録マネジメントの必要性

- 企業や組織は，スピード・グリーン・効率性・透明性・安全性・持続性・創造性が求められており，これらに応えるには，情報ガバナンスが不可欠
  - 情報ガバナンス：全体最適化をはかるために，情報の扱いに関して明確なポリシー，ルール，体制を決めて，全社的な足並みを揃える取り組み

- 今や，発生文書の大半が電子文書

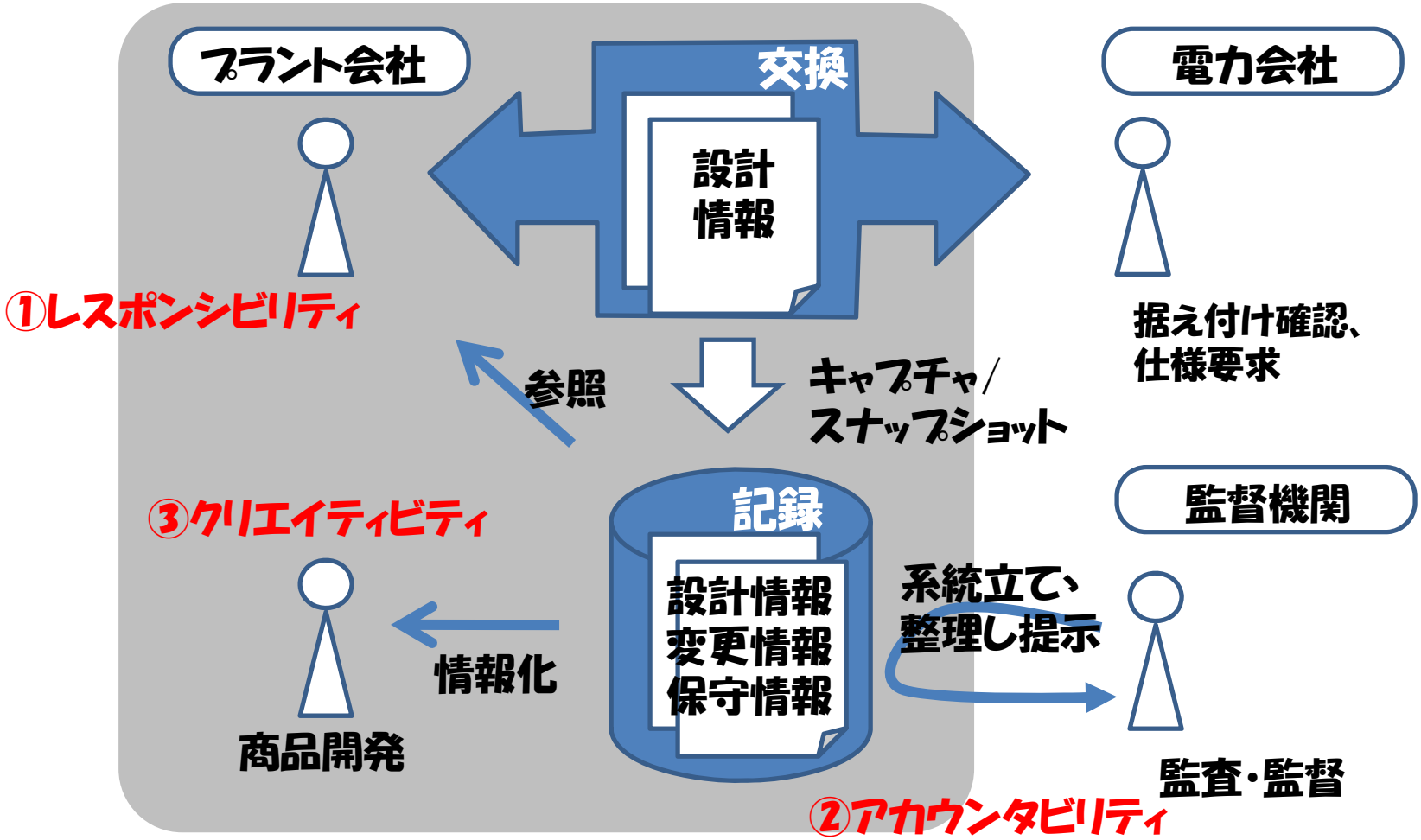
  作成・取得すべき文書を提示すると共に，企業・組織に存在する文書を捕捉・保存・活用した企業活動をコントロールするには

  → 目的に合致した電子記録“マネジメント”が必須
  - 管理：管轄し処理すること，とりしきること （広辞苑）
  - マネジメント：自らしくみを作って目標を達成すること|期待に応えること

1. 記録を生成・取得・参照し記録に裏付けられたスピーディな業務遂行を実現する（レスポンシビリティ）
2. 記録を系統立て、正確に利害関係者に説明したり業務の改善を図る（アカウンタビリティ）
3. 記録を情報化して事業の創出や新商品開発の糧とする（クリエイティビティ）

# 記録の位置付け

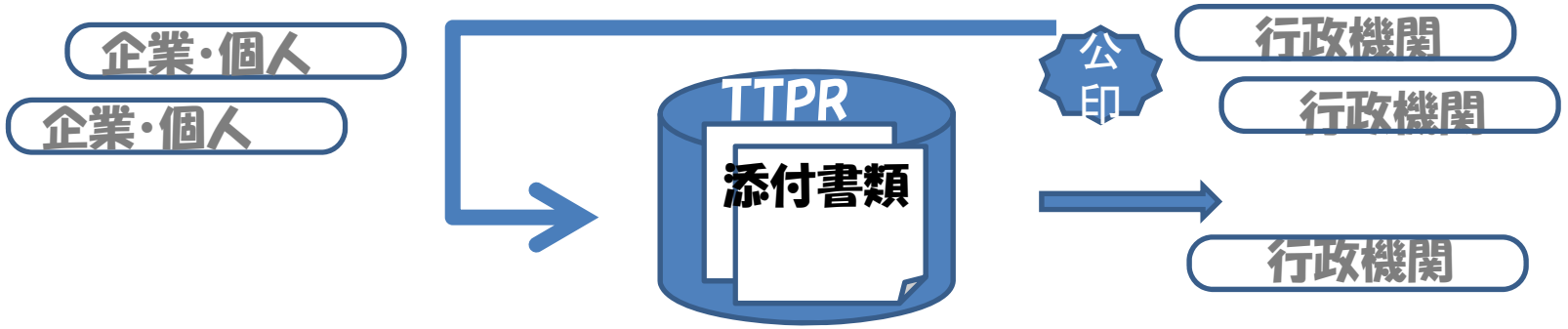
- 情報の交換(Exchange)のなかで生まれる証跡(Evidence)を記録(Record)としてとらえる(Capture)



# 記録の流動化と電子署名

- 解決すべき3つの課題
  - 意図的破棄 ― ルールと運用で解決
  - 改竄，偽造
  - 否認

  } 電子署名で解決

# 電子文書を原本とするための要件

| 項目 | | 概要 |
|---|---|---|
| 要件 | 見読性 | 使用に係わる機器に直ちに表示 |
| | 完全性 | 滅失、毀損、改変、消去防止 |
| | 機密性 | 漏洩防止（個人情報など） |
| | 検索性 | 記録の体系的構成 |
| | 真正性（真実性） | 何時，誰が，何を作成したかの特定 |
| | 識別性 | 管理対象の特定（台帳） |
| 努力基準 | ログ | ログ採取・保存 |
| | アクセス | 利用者認証、アクセス制御 |
| | バックアップ | 定期的な保管状況確認 |
| | セキュリティ対策 | ウイルス、不正アクセス対策 |
| | スキャナー取扱 | 作業責任者明確化等 |
| | システム運用管理 | 管理規定明文化 |
| | 点検・監査 | 内部監査 |

共通課題研究会報告書，文書の電磁的保存等に関する検討委員会報告，e文書法，公文書管理法を参考に要件をまとめた

# 電子記録の真正性・証拠性

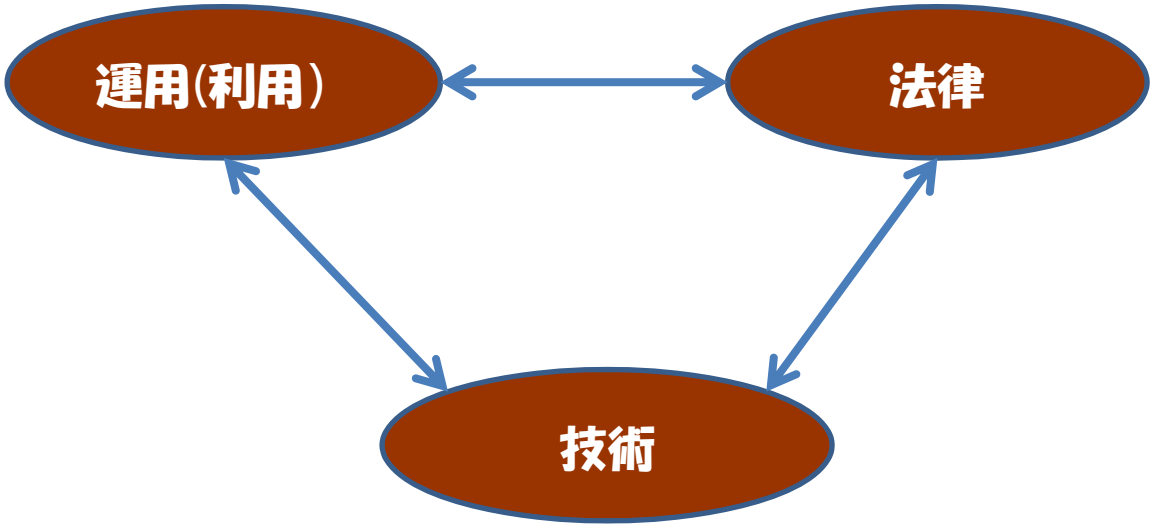
- 電子データの特性
  - 作成者の確定が困難
  - 作成時期の確定が困難
  - 痕跡を残さず改変(改竄)可能

- 電子データの証拠性
  - 裁判での前提は自由心証主義(自由な証拠評価)
    真正性(何時、誰が、何を)を証明できなければ証拠として認められない

→第三者機関が証明
  - 誰が、何を・・・電子署名
  - 何を、何時・・・タイムスタンプ

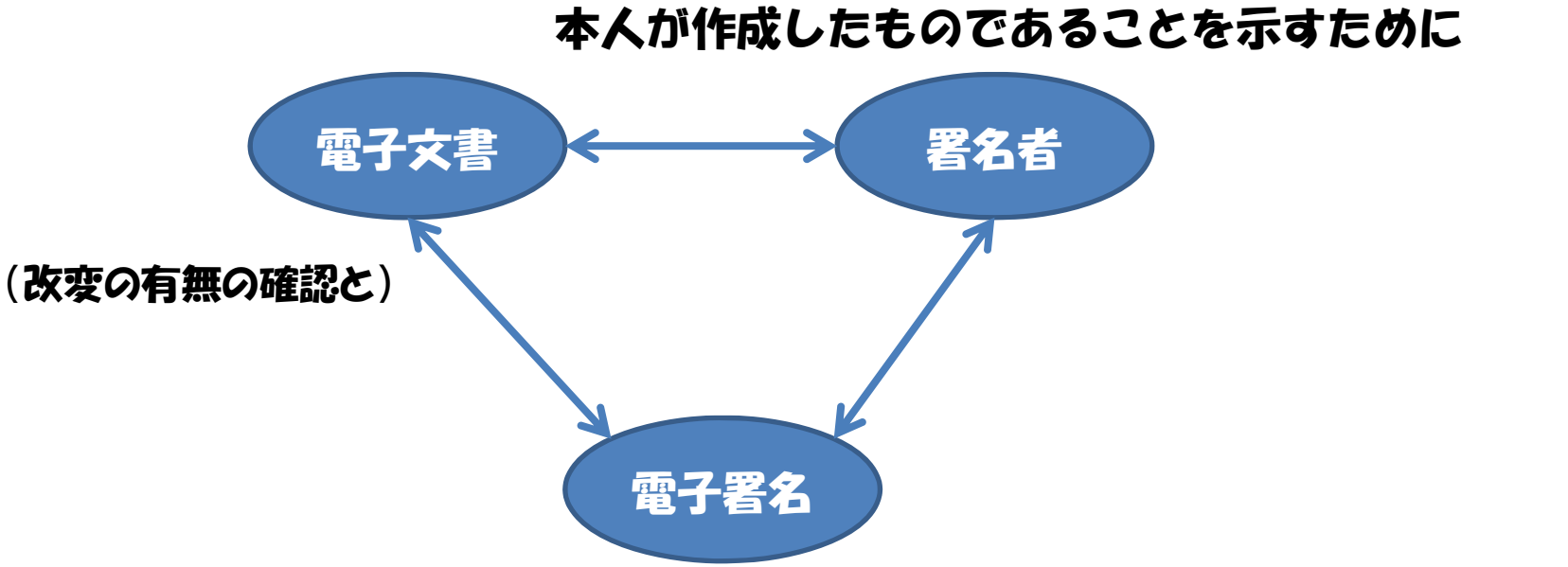
# 電子署名～考慮すべき3つの視点～

- 運用(利用)，技術，法律が相互に関連



# 法的視点

- 電子署名の要件
  →電子文書，電子署名，署名者の関係が維持されること



# 電子署名法

第二条　この法律において「**電子署名**」とは、電磁的記録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。

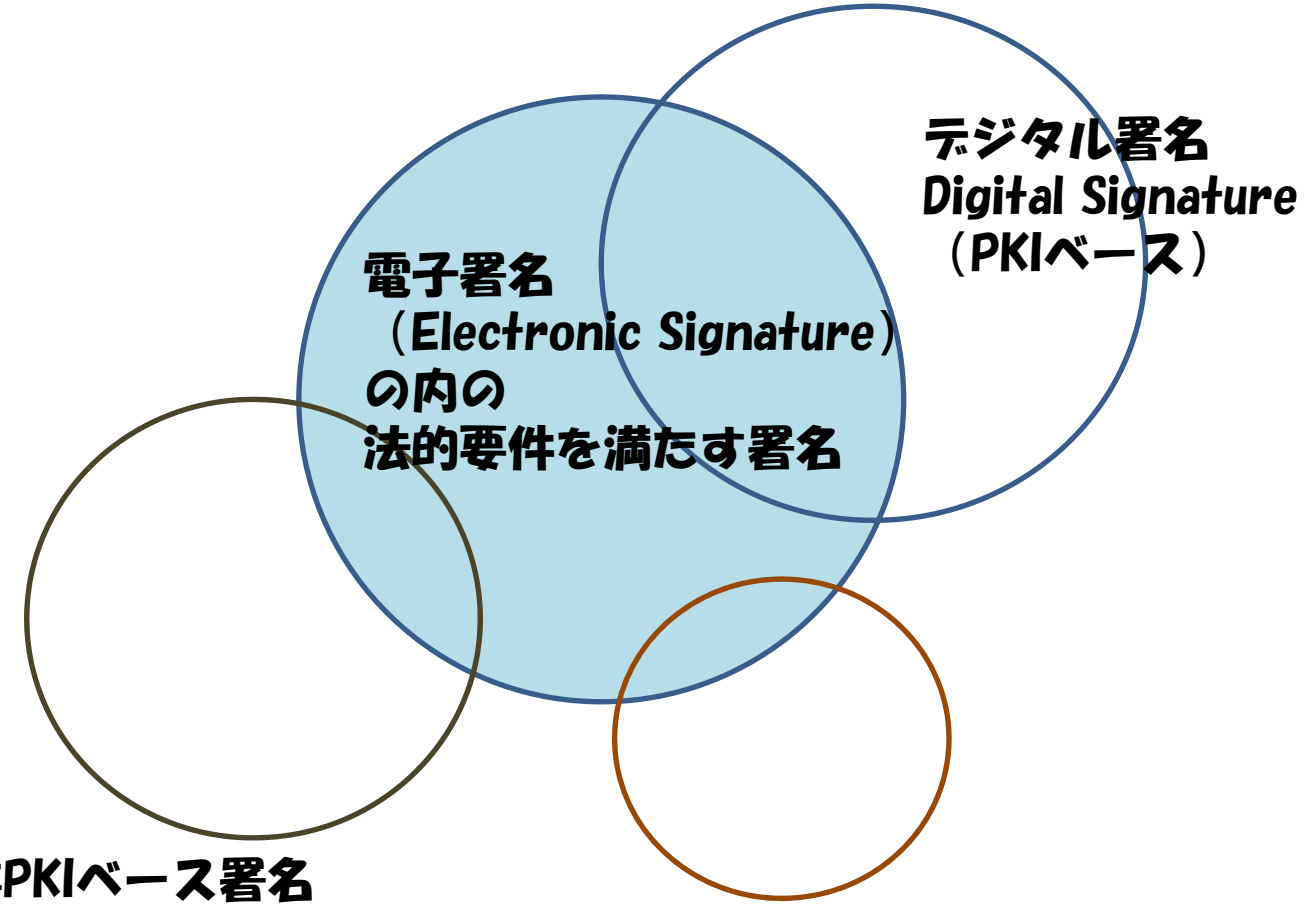
二　当該情報について改変が行われていないかどうかを確認することができるものであること。

２　この法律において「**認証業務**」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

３　この法律において「**特定認証業務**」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

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。

# 技術的視点

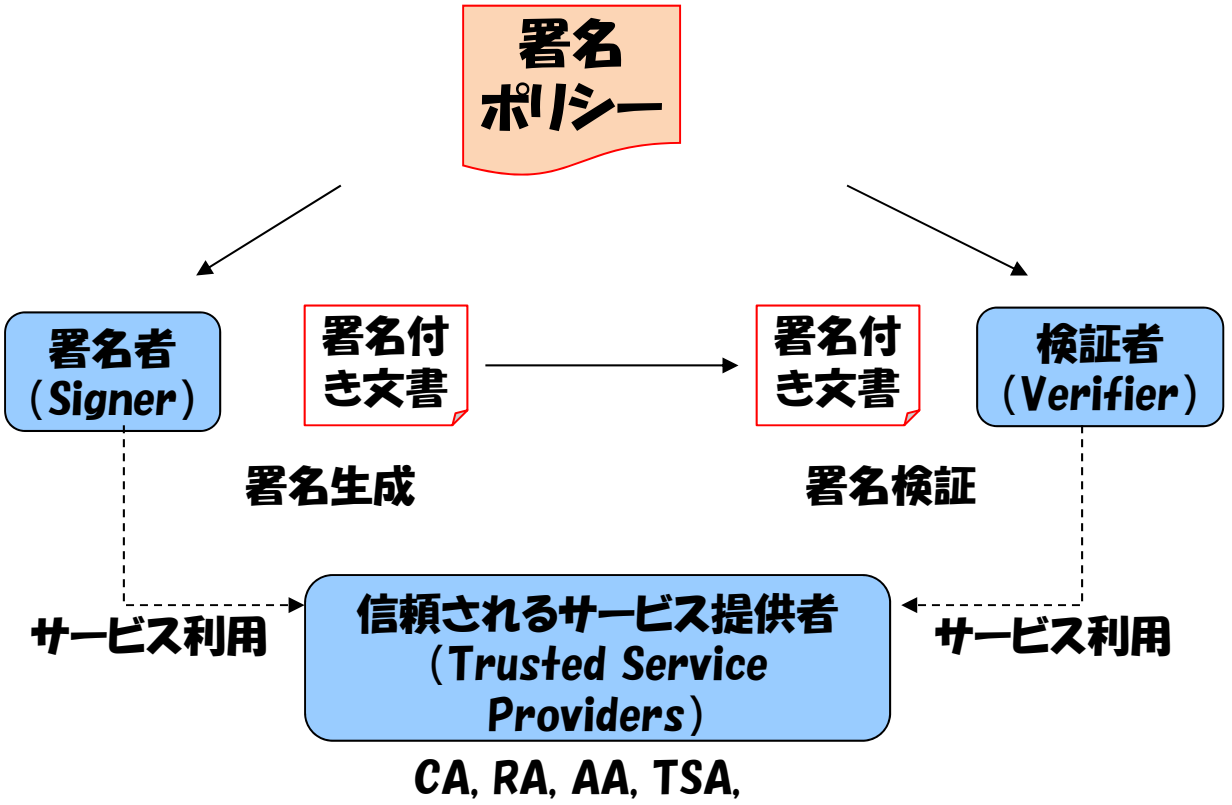



PKI：公開鍵基盤

# 運用的視点～署名ポリシー～

署名者と検証者との間の署名に関する事前の約束事

- 署名の方式
  - 署名範囲
  - 署名属性
- 署名の意味
  - 作成
  - 承認
  - 受取確認
- 信頼点



# 参考）電子署名のいろいろ

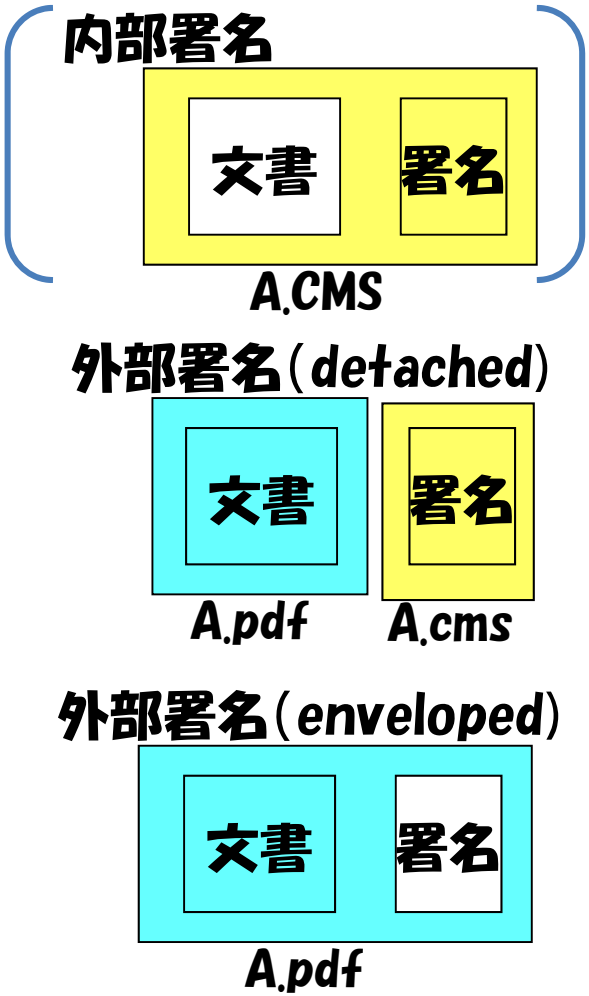
対象文書
- 一般文書、契約書
- 電子メール本文および添付ファイル
- Webダウンロードファイル

文書構造
- TIFF文書 （バイナリオブジェクト）
- pdf文書
- XML文書（Office文書）

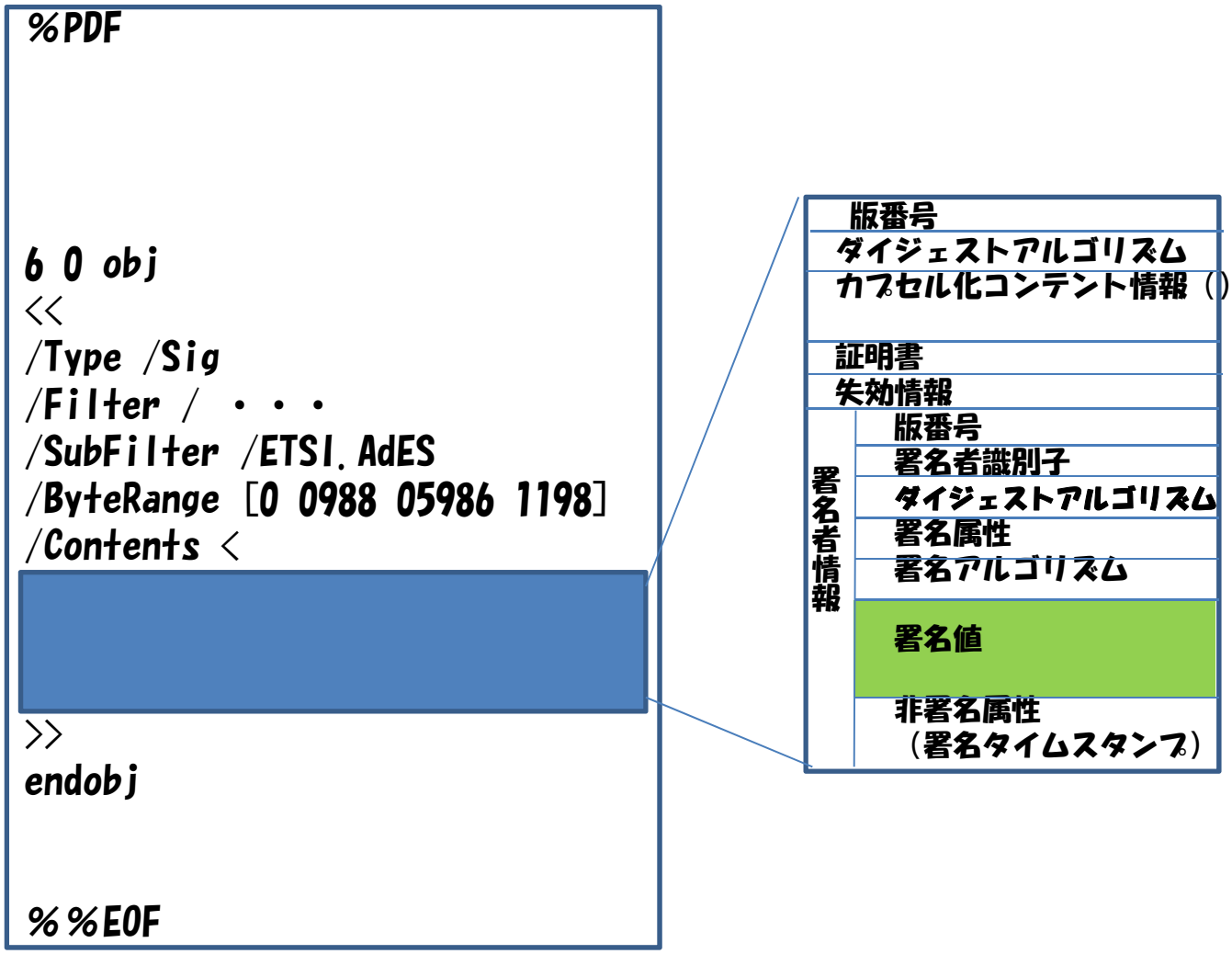
} Envelopedが可能

署名方式
- パラレル署名
- カウンタ署名（順序に意味がある）≠副署

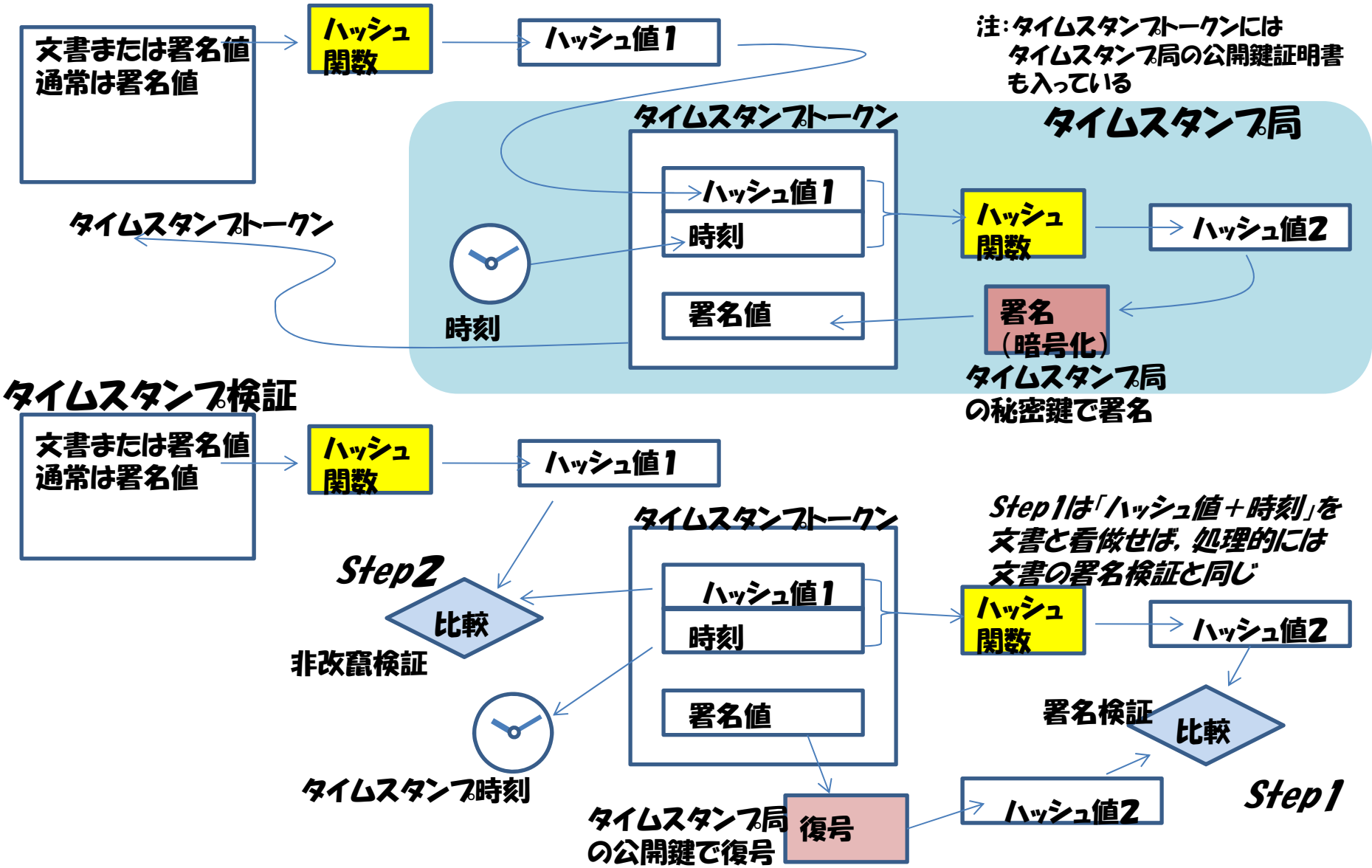
署名形式
- 内部署名（Enveloping）
- 外部署名（Detached、Enveloped）



# 参考)電子署名フォーマットの実際(PDFの例)



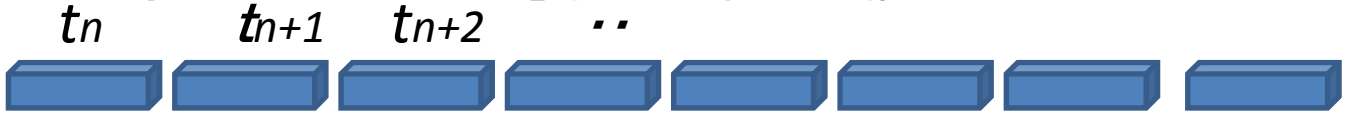
# 参考）タイムスタンプ（RFC3161方式）



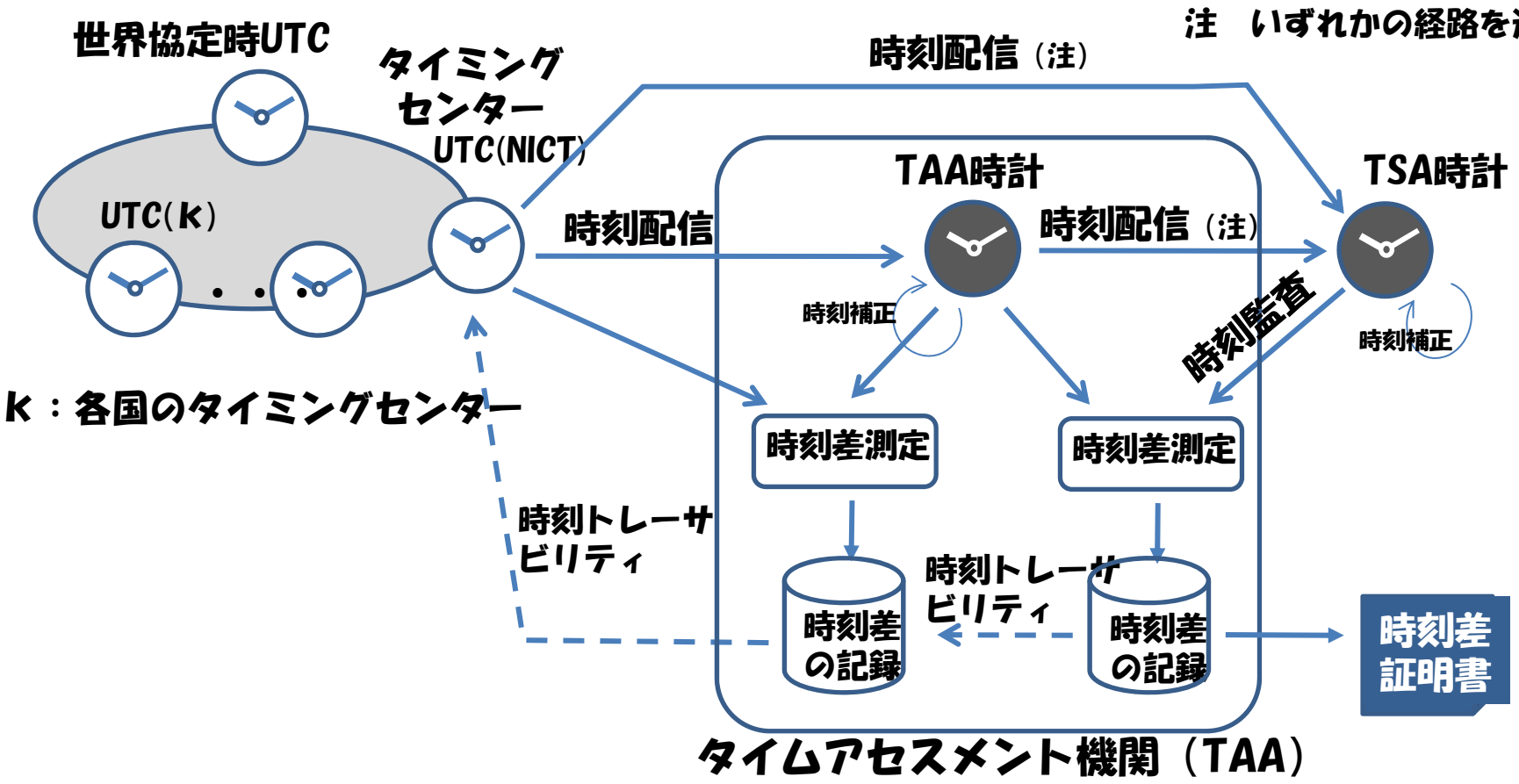
# 参考）各種タイムスタンプ方式

<table>
<tr><th></th><th colspan="2">信頼点はタイムスタンプ局<br>（検証は利用者）</th><th colspan="2">信頼点は新聞広告<br>（hash値を掲載）</th></tr>
<tr><th></th><th colspan="2"></th><th>検証は利用者<br>（照合データ開示）</th><th>検証はタイムスタンプ局（照合データ非開示）</th></tr>
<tr><td>文書毎にタイムスタンピング<br>（フロー向き）</td><td colspan="2">RFC3161方式</td><td>ー</td><td>アーカイビング方式</td></tr>
<tr><td>複数文書をまとめてタイムスタンピング<br>（ストック向き）</td><td>LTANS方式<br>（Marcle Tree※）</td><td colspan="2">3161併用方式</td><td>ー</td></tr>
</table>

※時刻に対応したスロットに記録のHASH値が格納される



# 参考）時刻の供給とトレーサビリティの体系

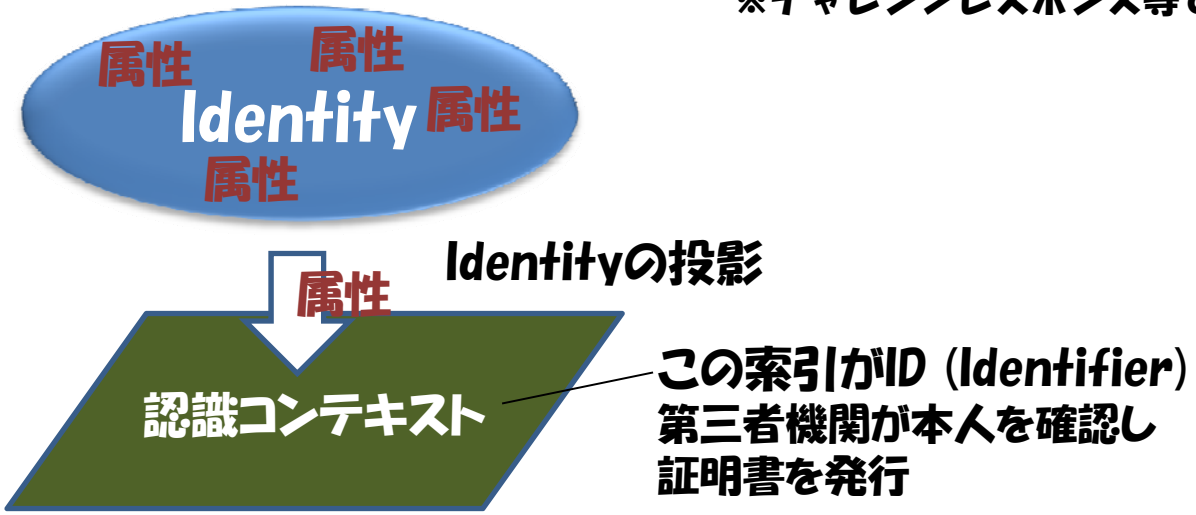



※独立行政法人情報通信研究機構法第十四条三項によりNICTが標準時を通報

# 証明書・・何を証明？

| | 実社会 | 電子社会 |
|---|---|---|
| 署名 | 印影 | 電子署名（署名値） |
| | 印鑑 | 秘密の鍵 |
| | 印鑑登録証明書<br>（印鑑の所有者が本人であることを証明） | 電子証明書<br>（秘密の鍵の所有者が本人であることを証明） |
| 認証 | 身分証明書 | 電子証明書 |
| | 証明書の所持，生体特徴（顔） | 秘密の鍵の所持※ |

※チャレンジレスポンス等で確認

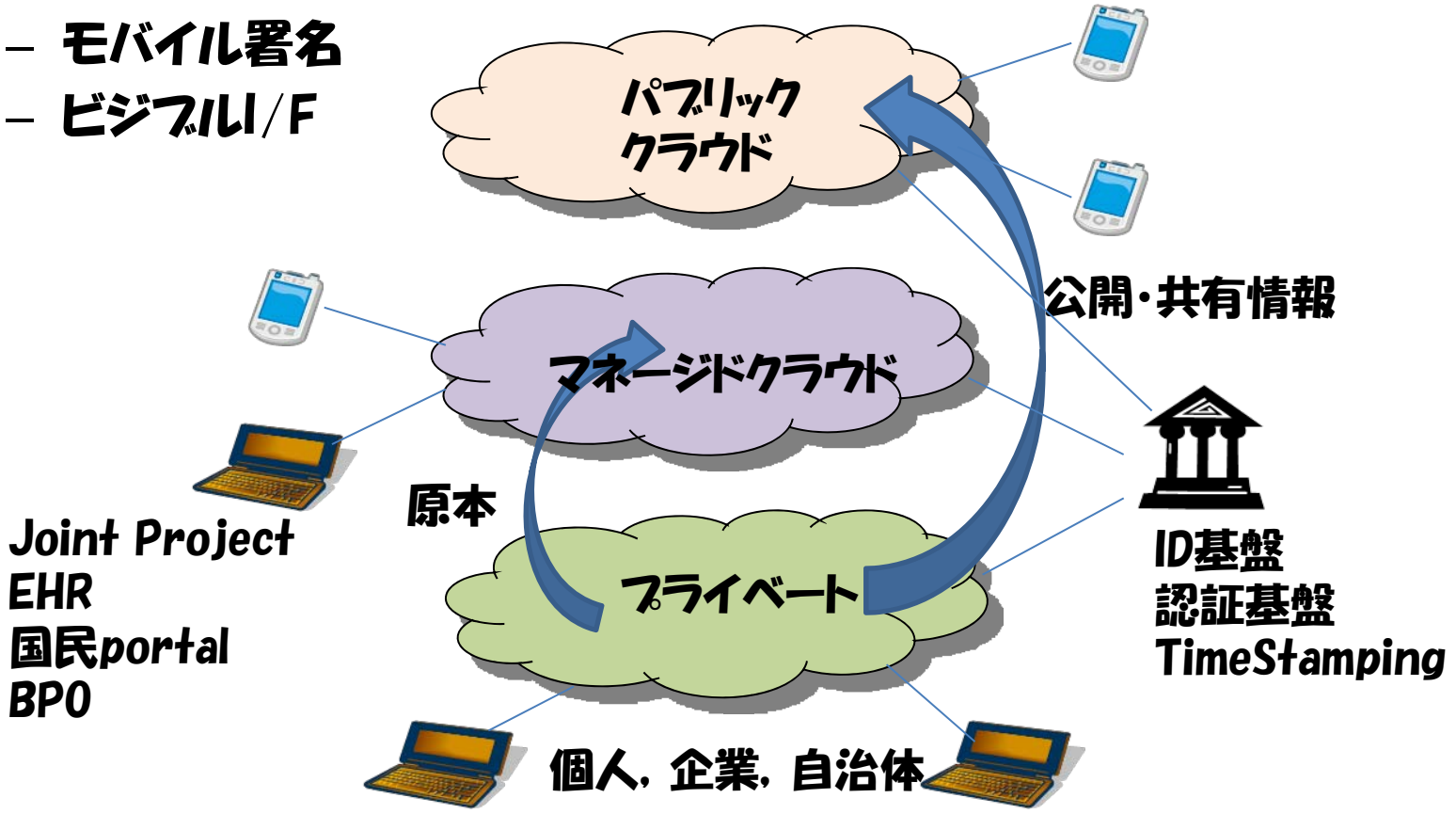


# 長期保存の阻害要因と解決策

<table>
<tr><td>長期保存の阻害要因</td><td>記録媒体劣化</td><td>署名危殆化</td><td>ファイル非互換</td><td>災害など</td></tr>
<tr><td>対処方針</td><td colspan="3">問題が発生する前に適切な措置を行い、問題の発生に至らないようにする(=リスクの先だし)</td><td rowspan="3">従来対策を踏襲</td></tr>
<tr><td>課題</td><td>記録媒体の劣化検知</td><td>再検証に必要な情報の保存</td><td>特定ベンダ依存からの独立</td></tr>
<tr><td rowspan="2">解決策</td><td>・高品質記録媒体の選択<br>・定期検査と媒体移行<br>ISO/IEC 10995<br>JIS Z 6017</td><td>・長期保存フォーマット導入<br>・長期運用タイムスタンプ局選定<br>JIS X 5092<br>(ISO/DIS14533-1)<br>JIS X 5093<br>(ISO/DIS14533-2)<br>ETSI TS 102 778-1～6</td><td>・長期保存ファイル形式導入<br>・既存システムの移行<br>ISO 32000-1<br>ISO 19005-1<br>ISO/IEC 26300<br>ISO/IEC 29500</td></tr>
<tr><td colspan="3">文書管理プロセス構築<br>ISO 15489-1 (JIS X 0902-1)</td></tr>
</table>

# クラウド時代の電子記録

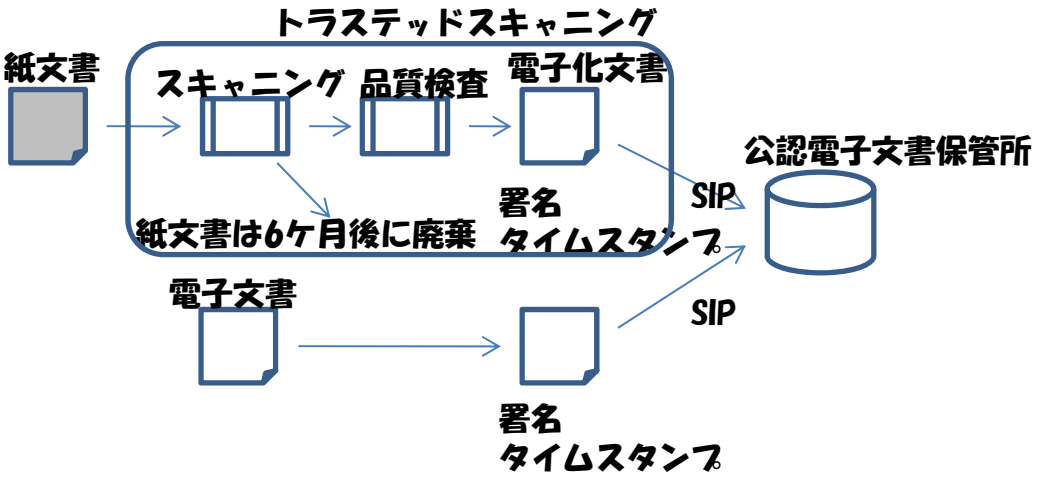
- 安心安全なマネージドクラウドサービス
- クラウド上に保存された電子記録の流動化（活用）
- 電子署名とタイムスタンプによる証拠性担保
  - モバイル署名
  - ビジブルI/F



# 韓国の公認電子文書保管所

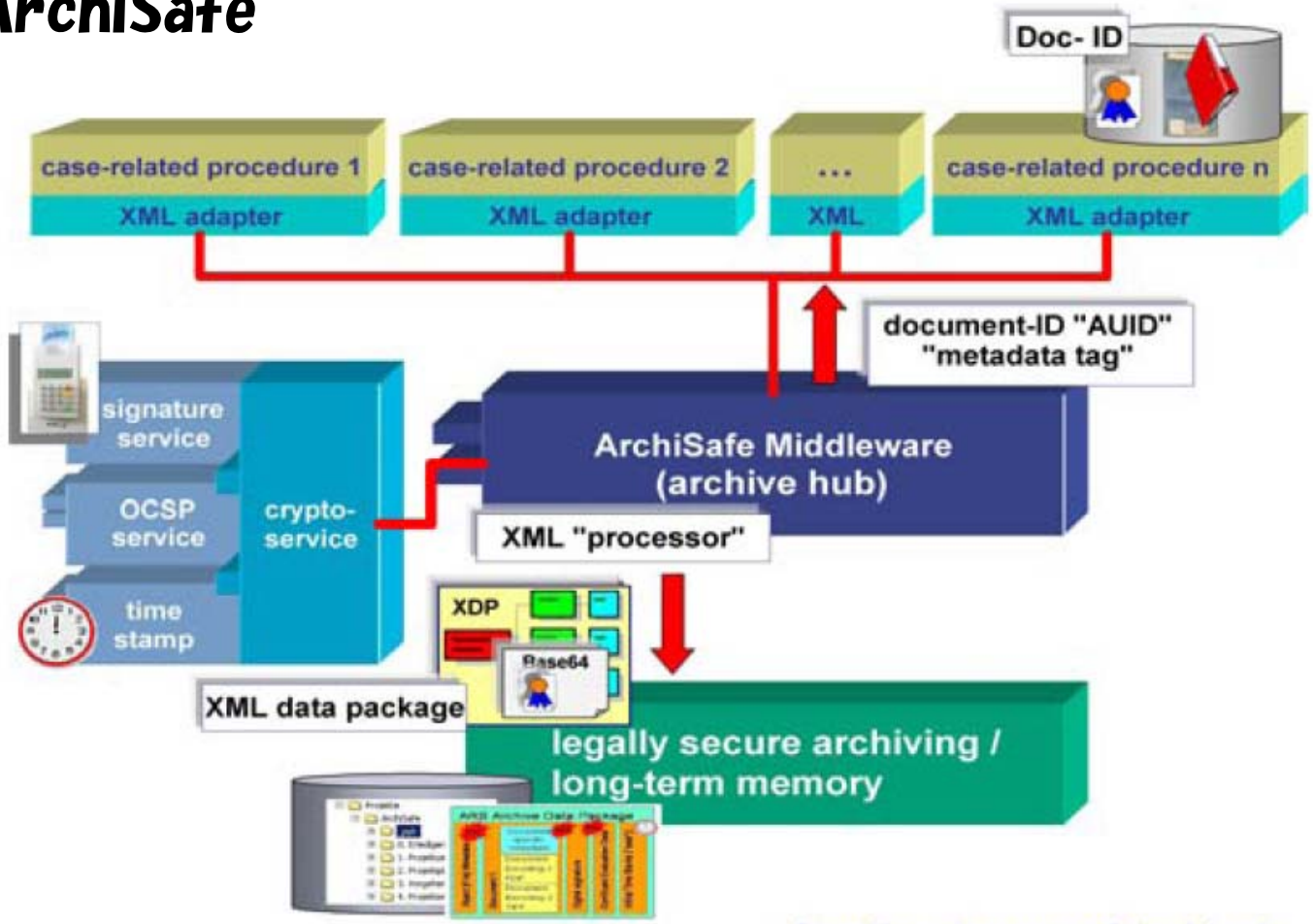
法律に裏付けされた（電子取引基本法第2条8項）信頼のおける第三者機関（提供サービス）

- 保管サービス：デジタルコンテンツ（電子文書）を安全に保管
- 閲覧サービス：保管文書の検索、閲覧
- 発行サービス：保管文書の出力版（原本にかわる）発行
- 流通サービス：保管文書を電子的に第三者（機関、企業）に配送
- スキャンサービス：スキャニング作業による紙文書の電子化
- SIサービス：利用者企業の内部システムと保管所の連携



# 案件管理とパッケージ構造

## 事例：ArchiSafe



# 電子署名に関する最近の海外動向

- TSL extension
  - TSL: Trusted Service Lists, ETSI TS 102 231
- Associate Signature
- Signature Policy
- Visible Interface

# ご清聴ありがとうございました