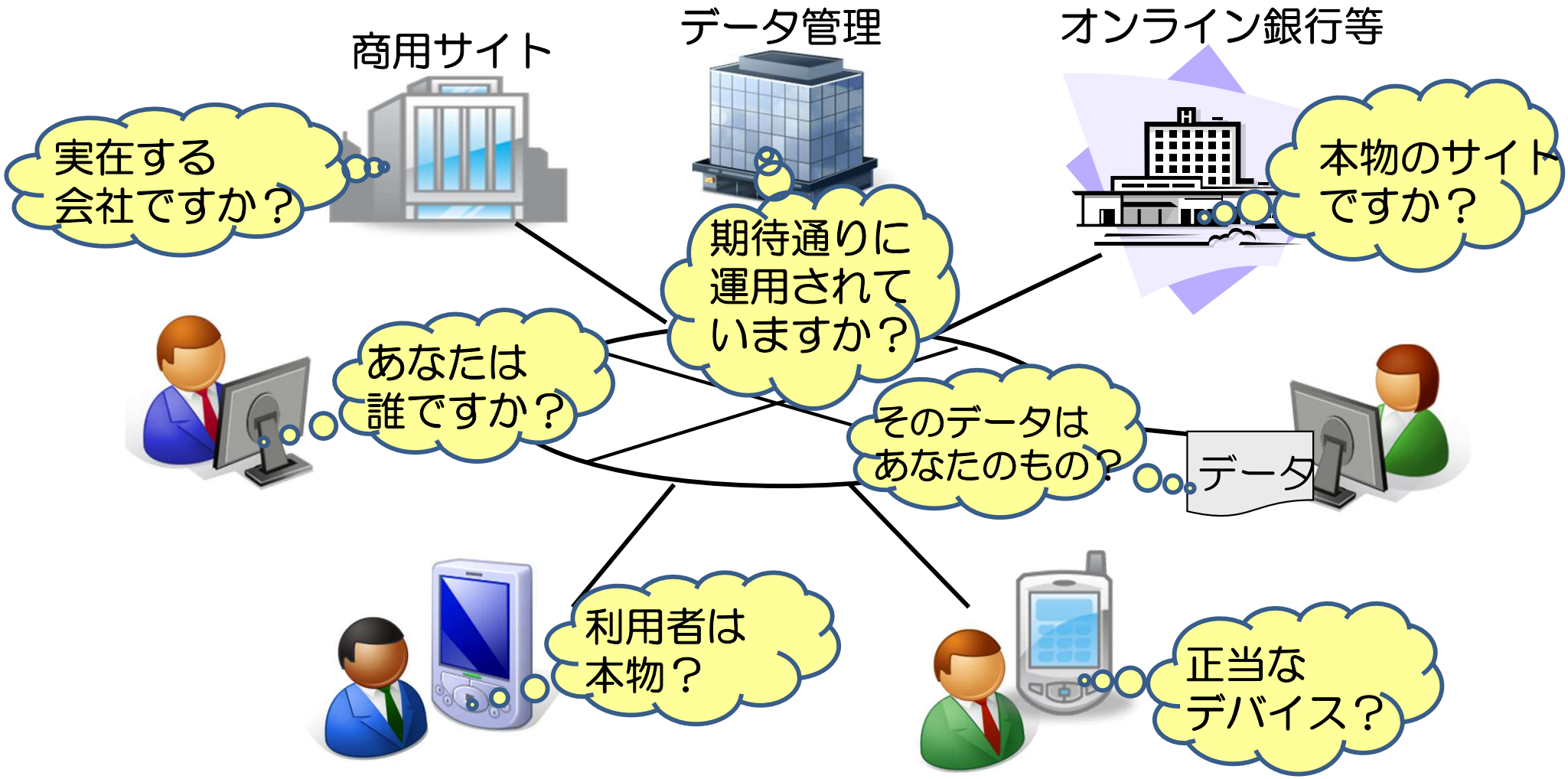
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

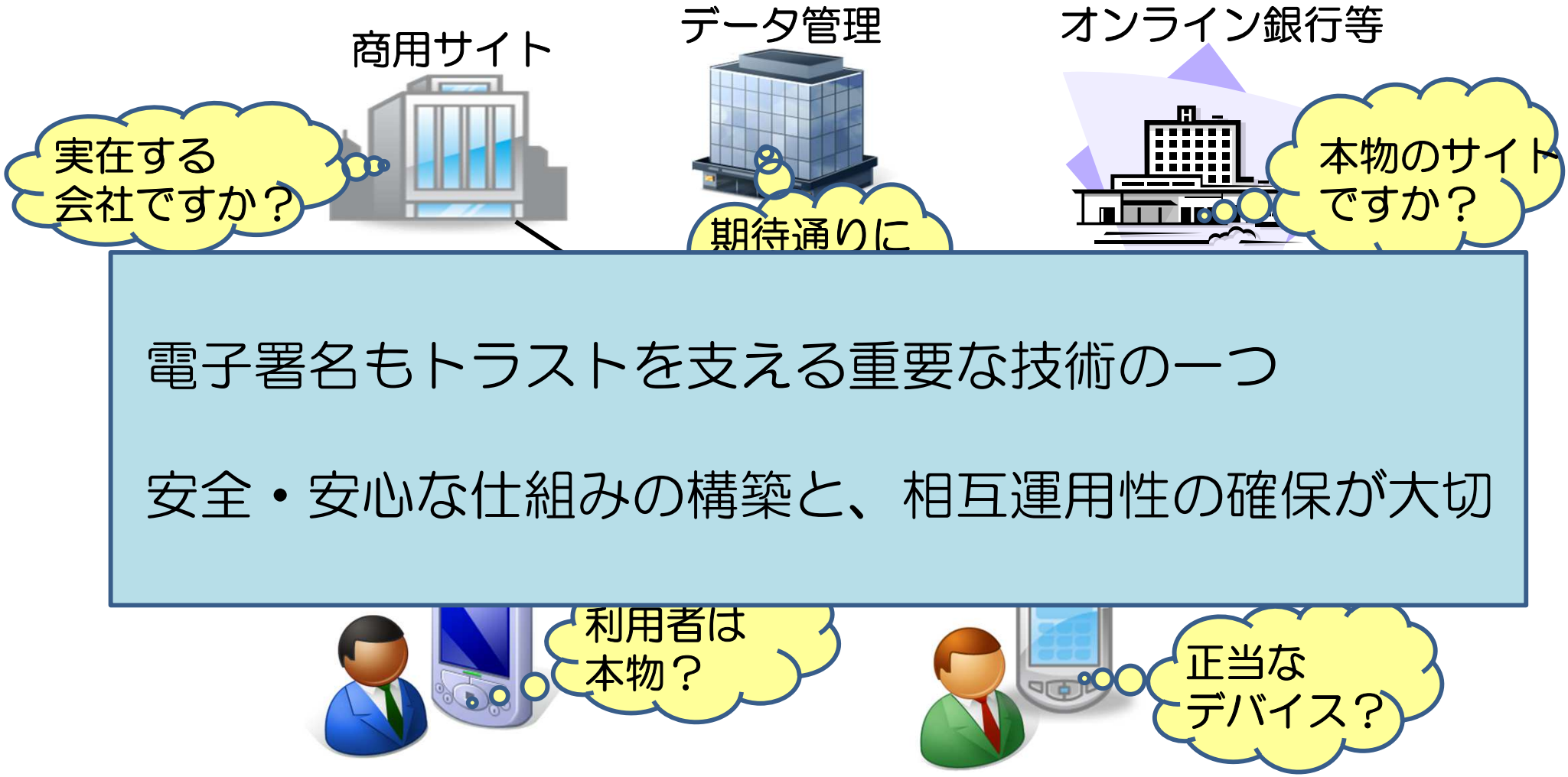
Network Security Forum 2017
PDF長期署名プロファイルの国際標準化を振り返って

2017年1月23日
JNSA電子署名WGサブリーダー
セコム株式会社　IS研究所
佐藤　雅史

安全・安心な情報社会にはセキュリティと共に信頼（トラスト）が必要



安全・安心な情報社会にはセキュリティと共に信頼（トラスト）が必要



本日の発表内容

- PDF電子署名(PAdES)とは？
- PAdES長期署名プロファイル(ISO 14533-3)の策定について
- PAdESに関する標準化の動向
  – と、少々の苦労話？なども入れつつ…

PDF(Portable Document Format)

- みなさんもよく使っているメジャーなデータフォーマット。
- もともとはAdobe社の規格であったが、AIIMに全仕様が譲渡され(2007年)、現在はISO標準となっている。
  - ISO/TC 171
  - ISO 32000-1(PDF1.7相当)が策定済み。
  - 現在ISO 32000-2(PDF2.0)が策定中

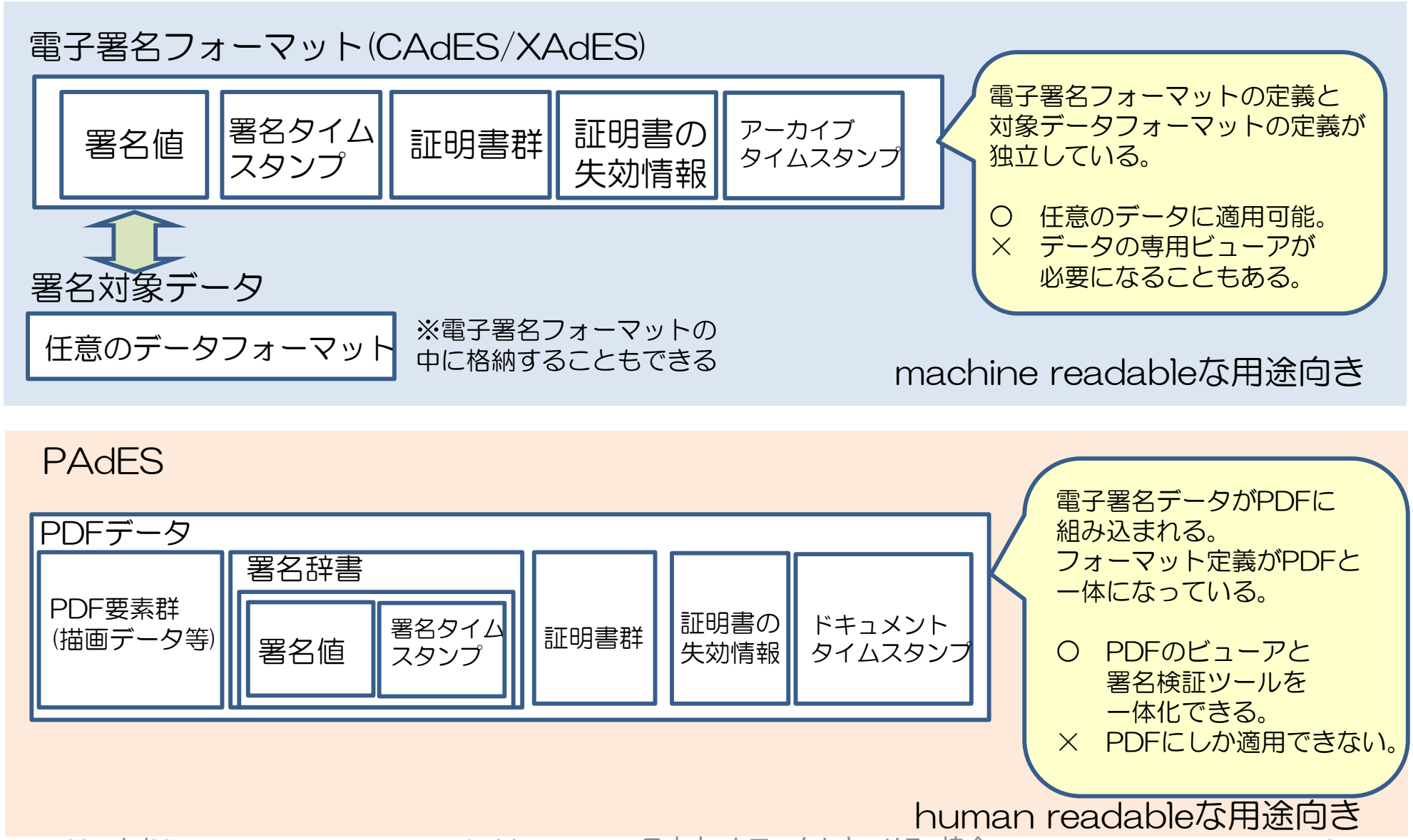
ISO 32000-2 (PDF2.0)

- 2009年～2013年 最初のプロジェクト(廃止)
  2013年～現在 2回目のプロジェクト実施
- FDIS投票中
- ISO 32000-1 (PDF1.7)からの変更点の一部
  - 3D and RichMedia annotations
  - Geospatial features
  - ″Namespaces″ for tagged PDF
    - PDF文書のコンピュータ処理
  - Associated files
    - コンテナとしての利用
  - 256-bit AES encryption
  - ECC-based certificates
  - PAdESサポート
  - etc.

PAdES
(PDF Advanced Electronic Signature)

- 元々は欧州ETSIで策定された規格
  - ETSI TS 102 778 (2009年)
  - 上記の策定には米Adobe社や日本のECOM(現在は解散)のメンバーも協力している
    - ECOMのメンバー（の一部）はJNSA電子署名WGに合流
  - この規格に基づいた実証実験も度々行われている
- 従来(PDF1.7以前)のPDF署名とは以下が異なる
  - 署名データと署名者の対応づけの強化
  - 長期署名（署名データの長期有効性担保）への対応

従来の電子署名(CAdES/XAdES)とPAdESの違い



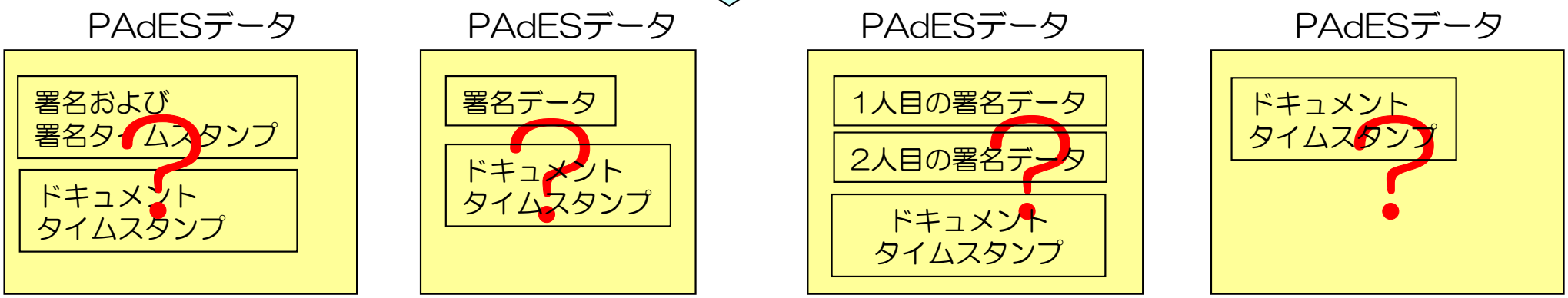
PAdESの相互運用性の問題

PAdES規格では要素の定義が列挙されている。

署名データ | 署名タイムスタンプ属性 | ドキュメントタイムスタンプ | 電子証明書格納エリア | 署名データ付加情報 | ・・・・

組み合わせについての制約は記載されていない

様々な実装が存在しうる



要素の組み合わせや配置を定めるプロファイル規格が必要

PAdESの相互運用性の問題

JNSA

ISO 32000-2(PDF2.0)

要素群の定義

PAdES規格では要素の定義が列挙されている。

署名データ　署名タイムスタンプ属性　ドキュメントタイムスタンプ　電子証明書格納エリア　署名データ付加情報　・・・・

組み合わせについての制約は記載されていない

様々な実装が存在しうる

PAdESデータ　PAdESデータ　PAdESデータ　PAdESデータ

署名および署名タイムスタンプ　ドキュメントタイムスタンプ　署名データ　ドキュメントタイムスタンプ　1人目の署名データ　2人目の署名データ　ドキュメントタイムスタンプ　ドキュメントタイムスタンプ

？　？　？

ISO 14533-3 プロジェクト

PAdESデータを保存可能にするために必要な要素と組み合わせを定め、実装間の相互運用性を確保する。

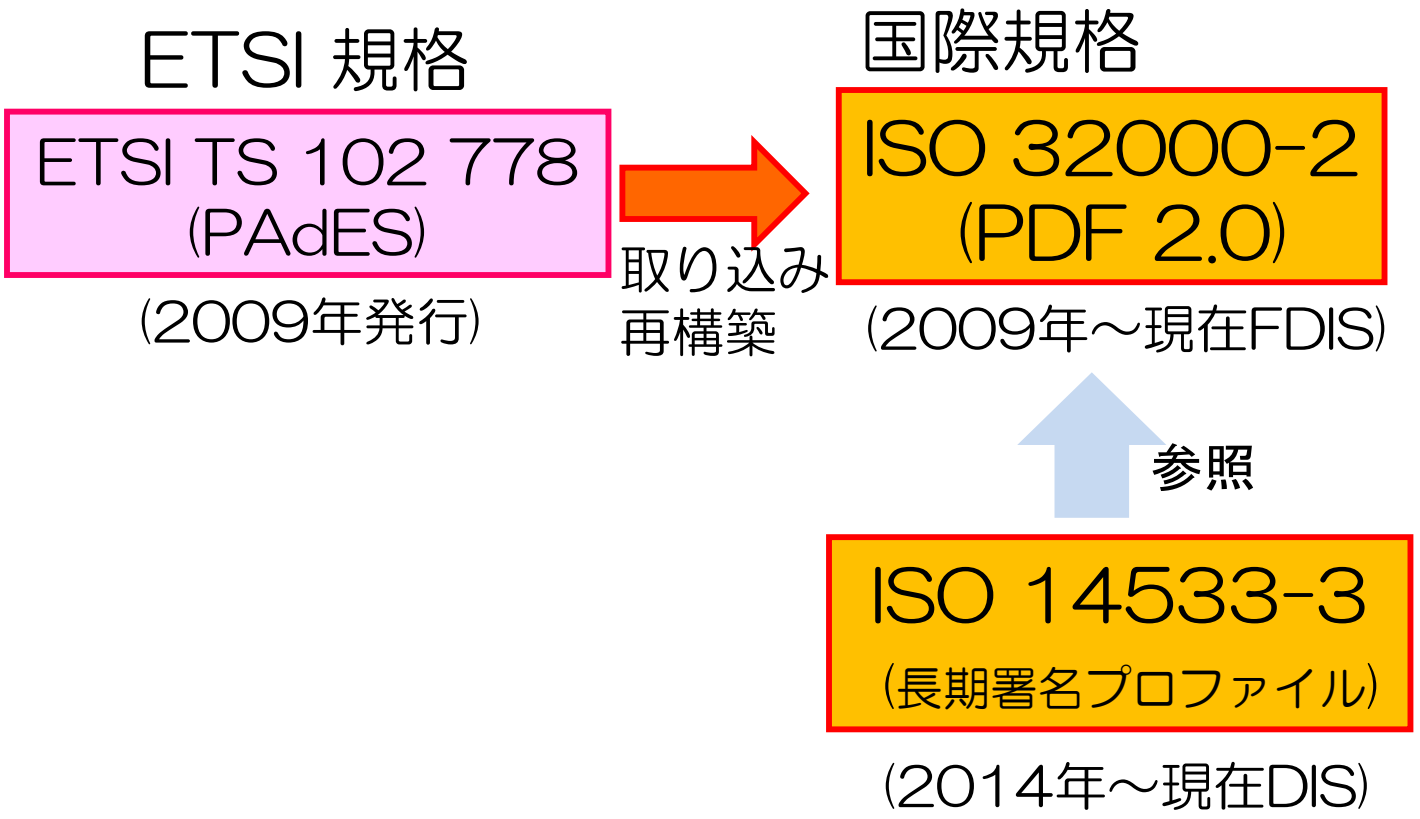
要素の組み合わせや配置を定めるプロファイル規格が必要

ISO 14533-3プロジェクト
（PDF長期署名プロファイルに関する国際標準化）

- ３ヵ年計画の事業（経済産業省）
  - 平成２６年度社会ニーズ（安全・安心）・国際幹事等輩出分野に係る国際標準化活動
  - 平成２７年度社会ニーズ（安全・安心）・国際幹事等輩出分野に係る国際標準化活動
  - 平成２８年度戦略的国際標準化加速事業（政府戦略分野に係る国際標準開発活動）
- JNSAが事務局を担当しプロジェクトを推進。
  - ベンダーと利用者の双方の専門家が集う電子署名プロファイル国際標準化委員会の設置。
  - JNSA電子署名WGの専門家チームで規格原案を作成。

PAdESに関する標準化の動向
(と、ISO 14533-3策定での議論)

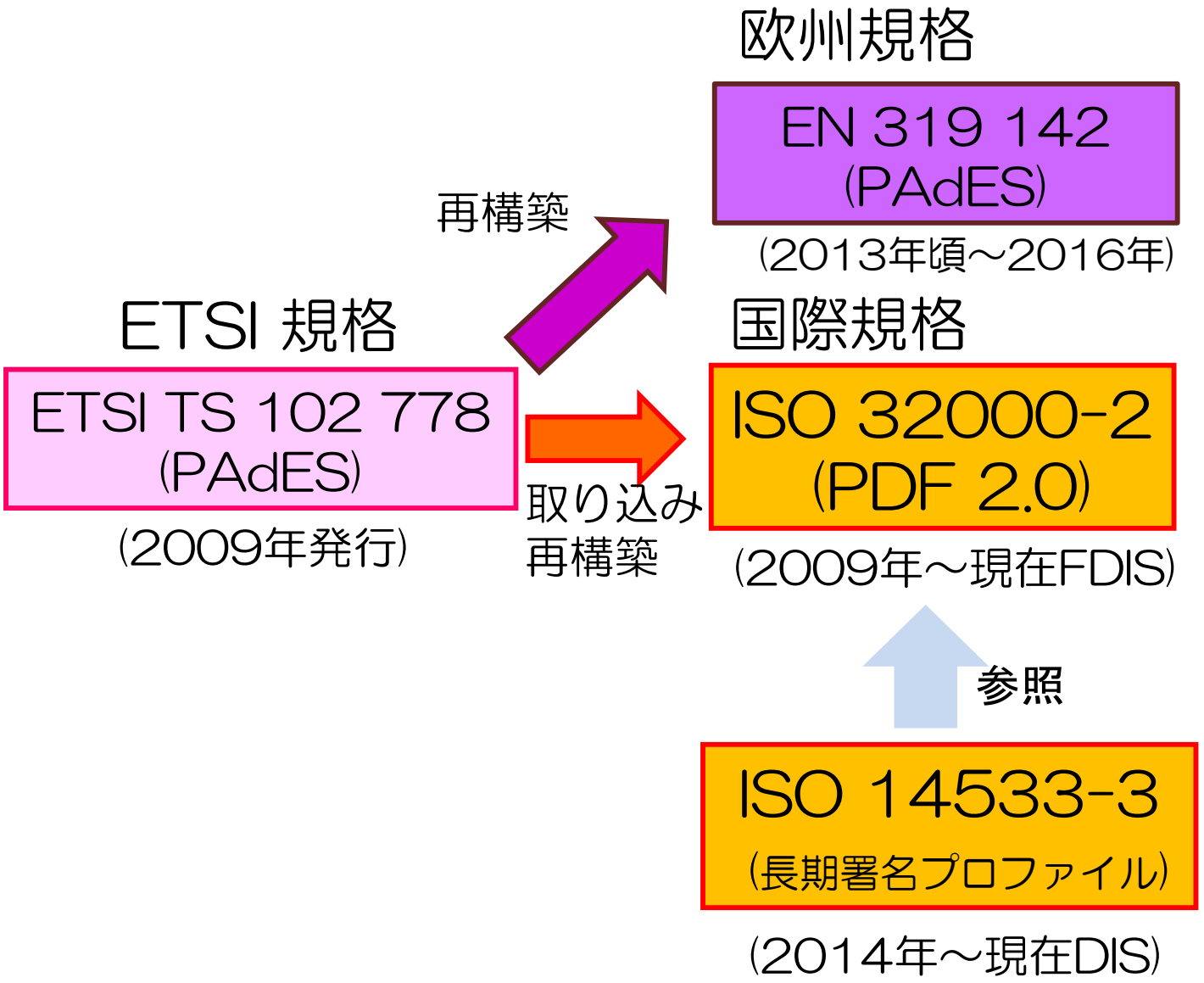
ISO 14533-3に関する関係



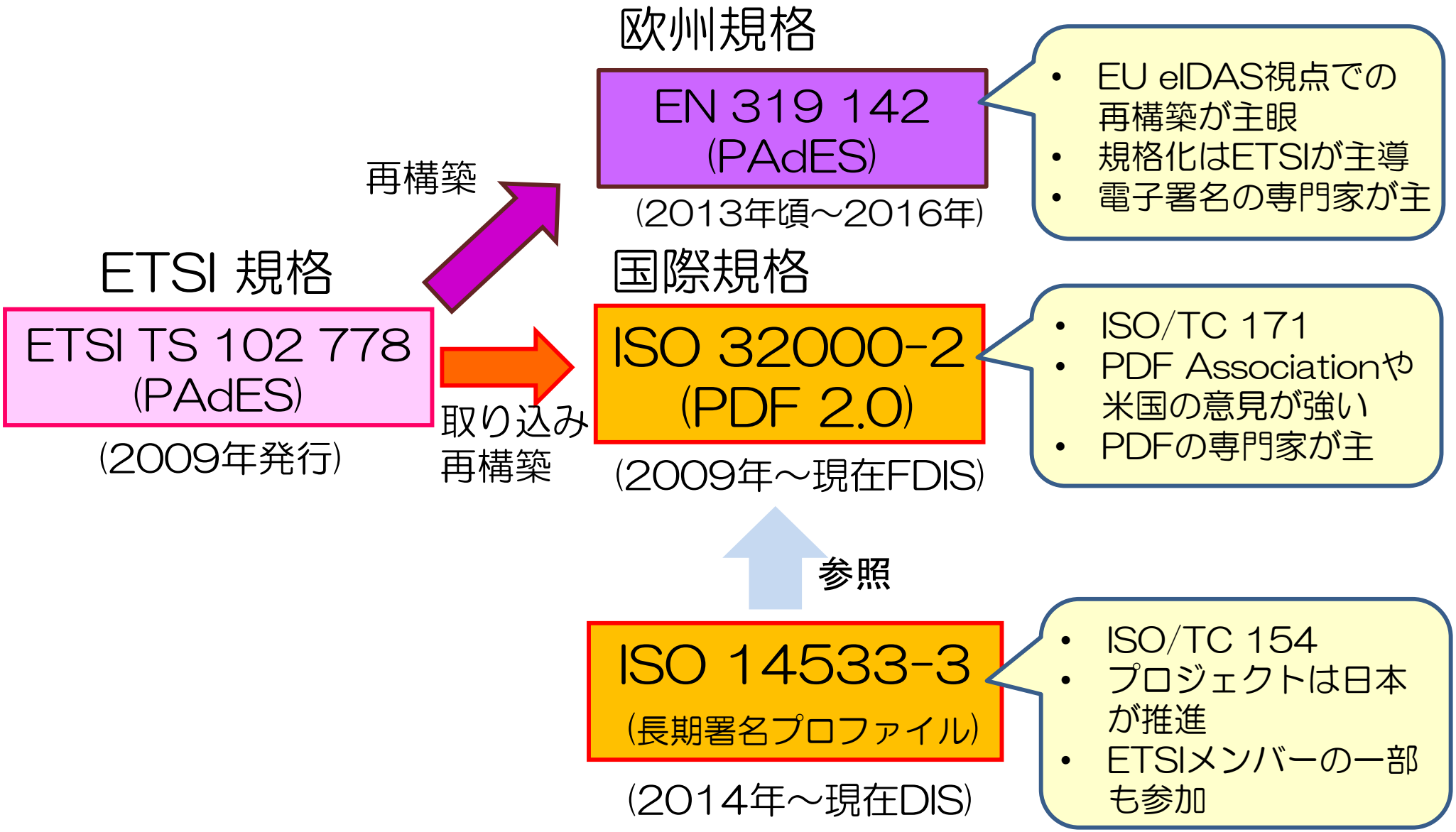
EU eIDAS Regularation

- eIDAS: Electronic identification and trust services
- 2014年に成立。
- EUで定めた電子認証や電子署名を含めたトラストサービスに関する規則。
- 電子認証やトラストサービスを普及させることで、国境を越えた電子取引を安全かつシームレスに実現させることが目的。
- eIDASに関連する指令の中で、標準規格の再整理と国際標準化への展開も示されている。

PAdESに関して2つの流れができた



PAdESに関して2つの流れができた



ISO 14533-3策定での調整事項①

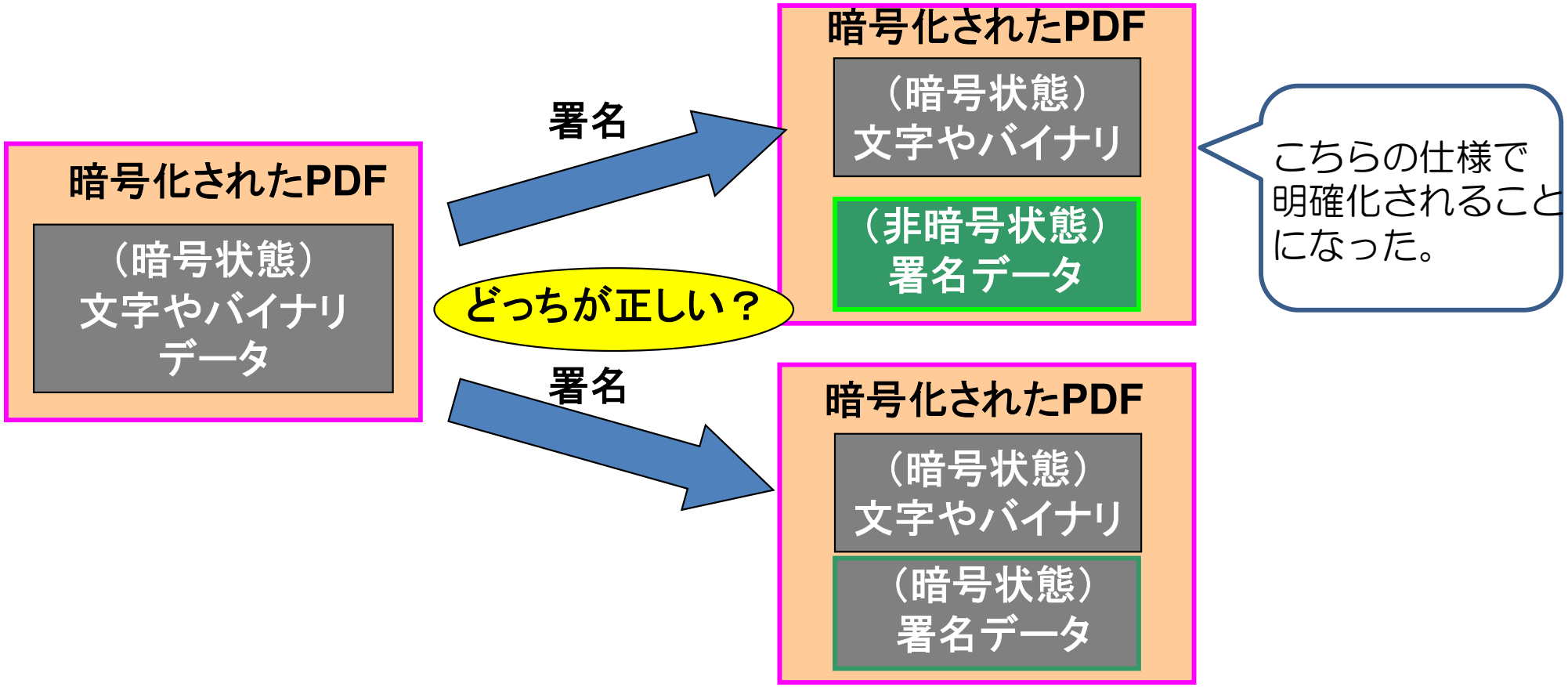
- EUからのリクエスト
  - EUはISO 14533-3と欧州規格のバッティングを懸念。
  - ETSI/TC ESI議長が来日し、JNSAとの非公式会議。その後、欧州規格との整合化を含め、JNSAとETSIの協力関係に関する合意に至る。
  - それでも一部にISO 14533-3に反対する声もあった。
    - 最終的には、説得を続けた結果、反対の声は無くなった。
- 欧州規格との整合化
  - 欧州向けプロファイル（eIDASに関連）との整合化を行う過程で日欧の意見の食い違い。
    - 欧州視点のため、欧州以外には必要のない要素まで必須と主張される。
    - 検証の要件（その要素がなくてもエラーとしない）で回避することとした。

ISO 14533-3策定での調整事項②

- 欧州規格(EN 319 142)とISO 32000-2の仕様の差異（＆意見の食い違い）
  - 共にETSI TS 102 778から派生しているが、並行的に異なるメンバーが作成しているので、その再構築過程で仕様が変わっている。
  - 矛盾をなくすため、日本(JNSA)からも積極的にETSI, ISOのメンバー双方にコメント。
- ISO 32000-2の進捗の遅れ
  - ISO 32000-2の進捗が思ったよりも時間がかかり、ISO 14533-3の方が先に出来てしまう可能性もでてきてしまった。
  - 日本(JNSA)もISO 32000-2が円滑に進めるように会議に加わった。
- ベース仕様の問題点
  - ISO 14533-3の議論の過程で、ベースの仕様自体に問題があることを発見し、ETSI/ISO双方にコミットした。

問題の一例
（暗号化PDFに対する署名適用）

PDFの暗号化は内容を秘匿するだけでなく、PDFの操作の制限（印刷禁止やコピー禁止など）にも使われている。
PDF操作制限と署名を両立したい利用場面は結構多い。
しかし、暗号化されたPDFに対する署名方法は規格では明確に記述されていない。



今後の展開

- ようやくPDF2.0 (ISO 32000-2)が見えてきた
  - 2017年中には発行されるはず（と期待）
- ISO 14533-3もIS化に向けて邁進中
  - PDF2.0と同時期くらいに発行される？（と期待）
  - ISO14533-3から直接欧州規格は参照していないものの整合性のとれた仕様となっている
- 次はPDF/A-4の策定
  - ISO 14533-3のプロファイルが使われる可能性あり

PDFの各種規格

標準PDF (ISO 32000)
コア要素の規定

ISO 14533-3は
ISO 32000-2に対する
プロファイル規格。

PDF/X (ISO 15930)
グラフィック交換

PDF/VT (ISO 16612-2)
バリアブル印刷

PDF/A (ISO 19005)
長期保存

PDF/E (ISO 24517)
エンジニアリング・製造ワークフロー

PDF/UA (ISO 14289)
ユニバーサルアクセス

PDF/H (AIIM)
ヘルスケア

PDF/Aは見読性などを長期間担保するための規格（従来は電子署名はNG）。
PDF/Aの次バージョン(4)に改訂作業中であり、電子署名の要件定義として
ISO 14533-3を提案し受け入れられた。
このまま進めば、PDF/Aでも電子署名が使えるようになります！

おわりに

標準化は労が多いですが…

- 業界がうまく回るためには相互運用性の確保は大切。使えるようにするための標準化が必要。
- 他所で勝手にルールが作られるのではなく、自分たちの意見が反映できることの意義は大きい。
- 作業の過程で潜在していた様々な問題が見つかることも。（議論を見ていても勉強になります）
- こうした活動を積み上げていくことで海外のメンバーとも信頼を築けていけると嬉しい（何かの時に話ができる関係を作れると嬉しい）

今後も様々な観点で標準化などを考えていきますので、皆様のご参加をお待ちしております！

ご清聴ありがとうございました。