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

Network Security Forum 2015
電子署名に関わる標準化の最新動向

佐藤雅史

JNSA電子署名WG サブリーダー

セコム株式会社　IS研究所

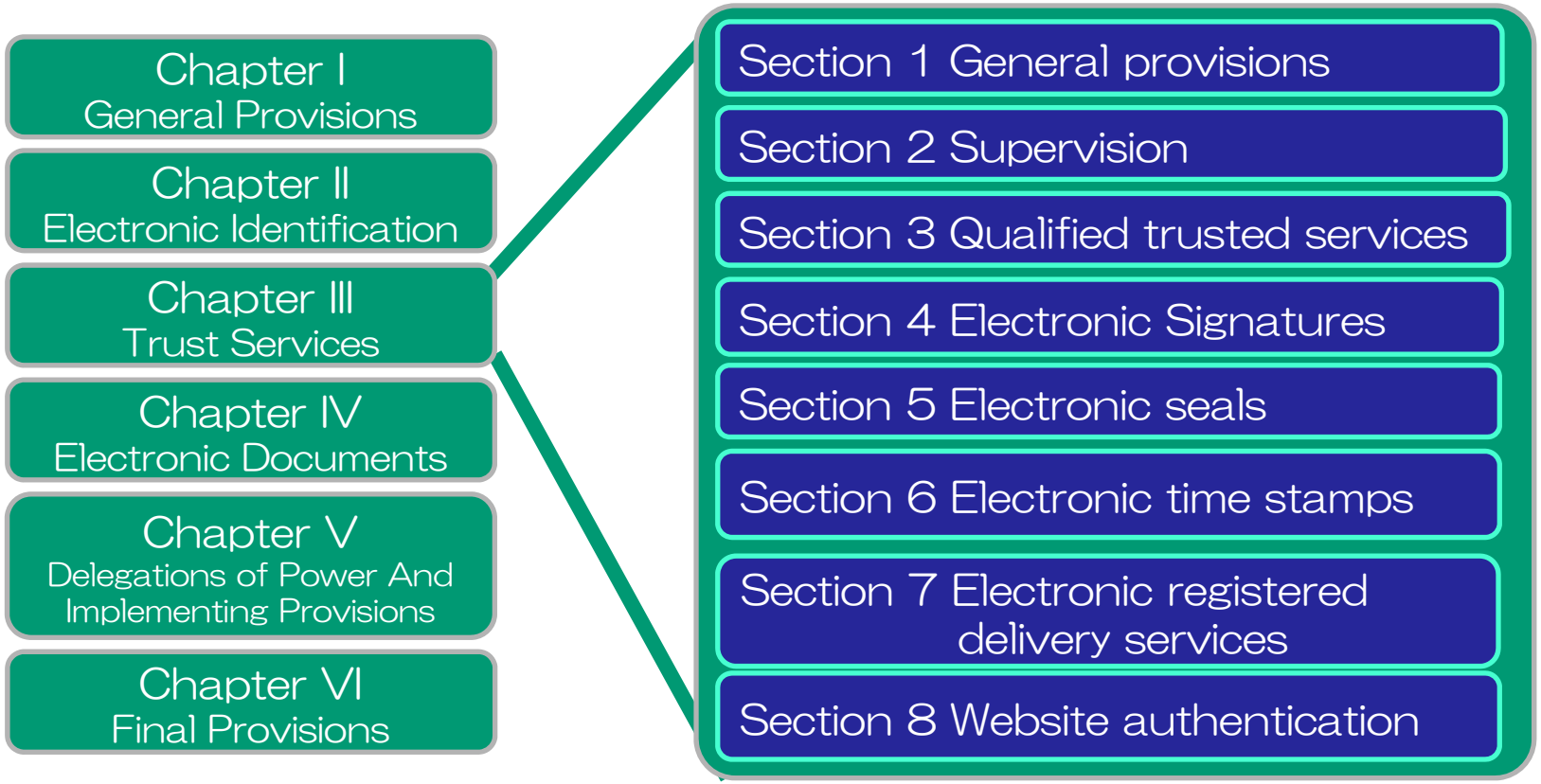
2015 年1月20日

eIDASとは？

- eIDAS: Electronic identification and trust services
- 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。

EU-Regulation eIDASの構成

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014
on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC



EU電子署名指令(Directive)からの変化

- これまでは、EU電子署名指令に基づきEU各国で電子署名法を整備してきたが、eIDAS 規則(Regulation)がそれらに置き換わる。
- 自然人による電子署名だけでなく法人による電子署名(Electronic Seal)が含まれる。
- 電子署名だけでなく、タイムスタンプや電子データ配送サービス、Webサイト認証に関する規則も含まれる。

（参考）日本の電子署名法

第二条　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）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。

- 対象は自然人。
- 認証業務（認証局）に関する言及のみ。

EC指令460(mandate460:2009/12

M/460 STANDARDISATION MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO ELECTRONIC SIGNATURES

- 欧州の電子署名規格の軽量化と再編成
  - 期限切れの規格の更新や廃棄
  - 規格の統合、再構成
  - 理解と利用を促進するための規格の簡素化
- ETSI技術仕様(TS)の生成から欧州規格(EN)やISOへの進化が定義されたライフサイクル
- 4年スパンの行動計画
- TS普及とプレゼンテーションインフラ維持のための恒久的な予算措置

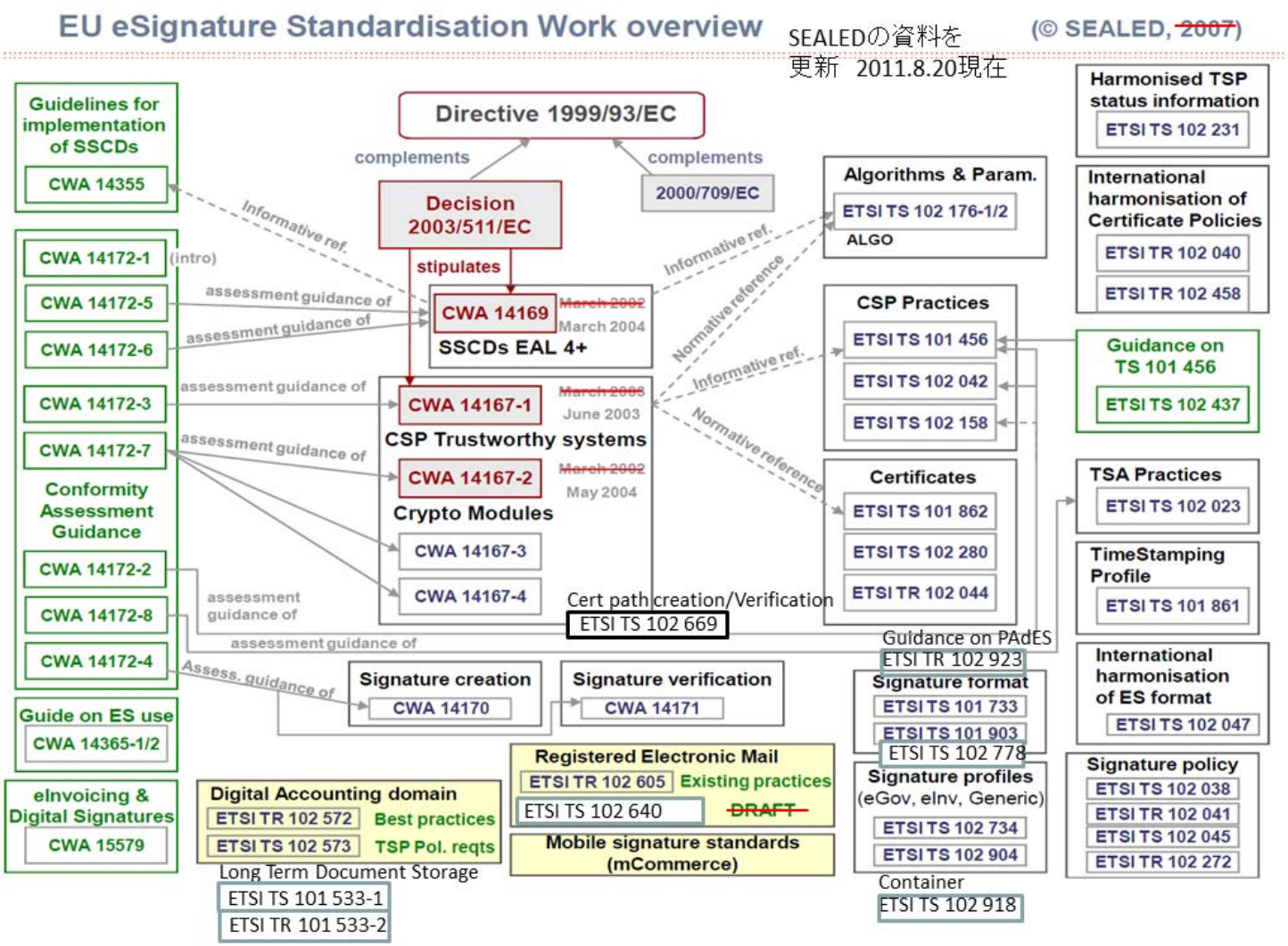
電子署名に関わる欧州の主な標準化団体

CEN：
Comité Européen de Normalisation
(The European Committee for Standardization)

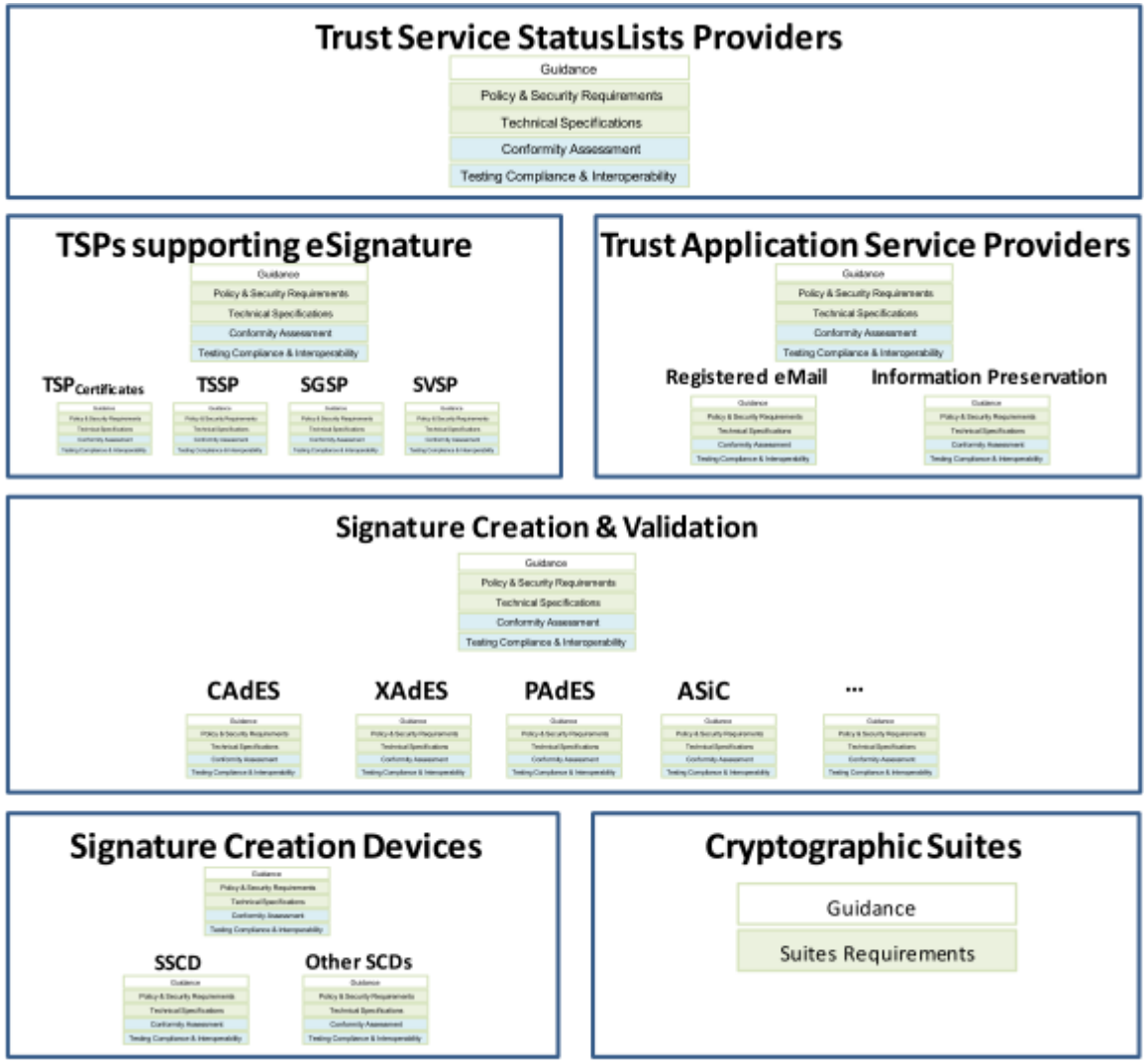
ETSI：
The European Telecommunications Standards Institute

JNSA電子署名WGとETSI/TC ESI (Electronic Signature Infrastructure)は
パートナーシップ関係にある。

旧来の欧州電子署名の技術標準体系

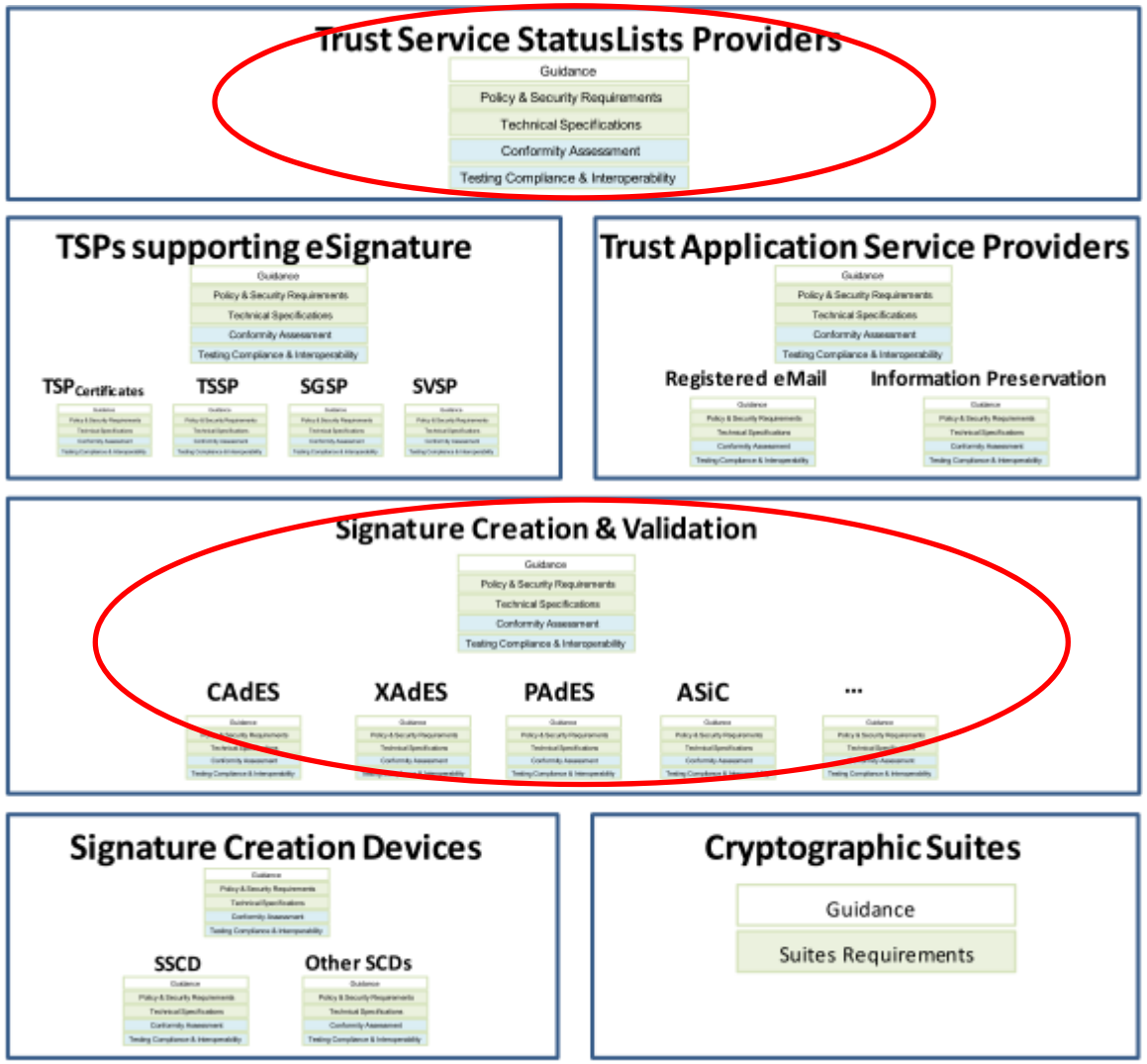


欧州電子署名標準の新体系



ETSI SR 001 604より

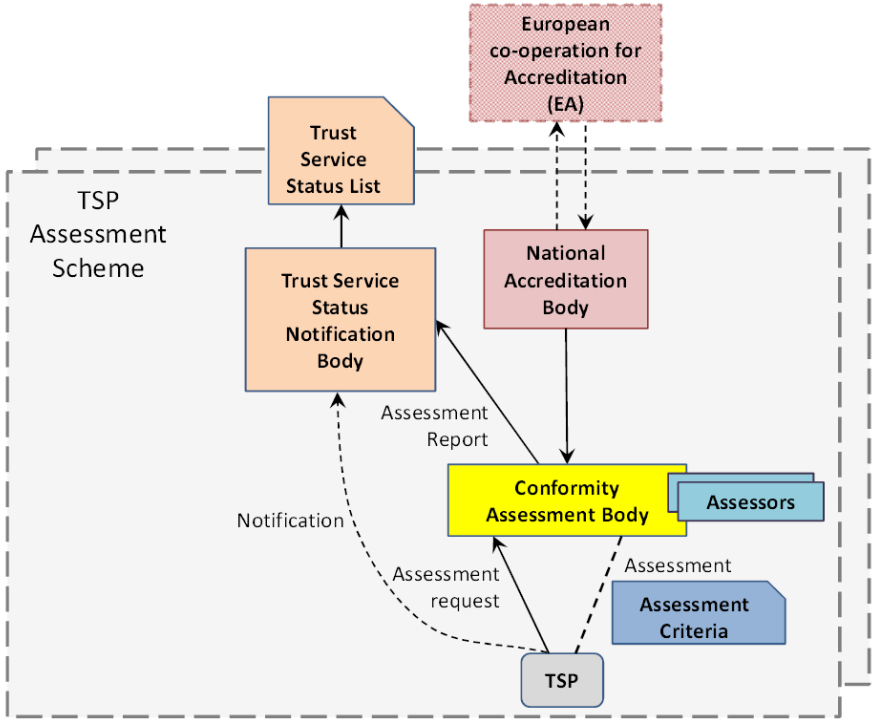
現在の議論の中心（ETSIにて）



ETSI SR 001 604の図に追記

Trusted Service Status List

- EU各国で監査、認定されたサービスのリストを作成し、EU内で統一的な方法で管理する。
- サービスの対象は電子認証局だけでなく、タイムスタンプ局や電子データ配送サービスなども含まれる。
- MicrosoftやAdobeとも協調している。
  - （例）Adobe Readerで対応済み



出典：ETSI TS 119 403

電子署名フォーマット規格

CAdES
(CMS Advanced Electronic Signature)

・バイナリデータ形式のフォーマット。
・任意のデータ形式に署名可能。
・最も歴史が古い。
・現在も改定が進んでいる。

XAdES
(XML Advanced Electronic Signature)

・XML形式のフォーマット。
・任意のデータ形式に署名可能。
・特にXMLデータとの親和性が高い。

PAdES
(PDF Advanced Electronic Signature)

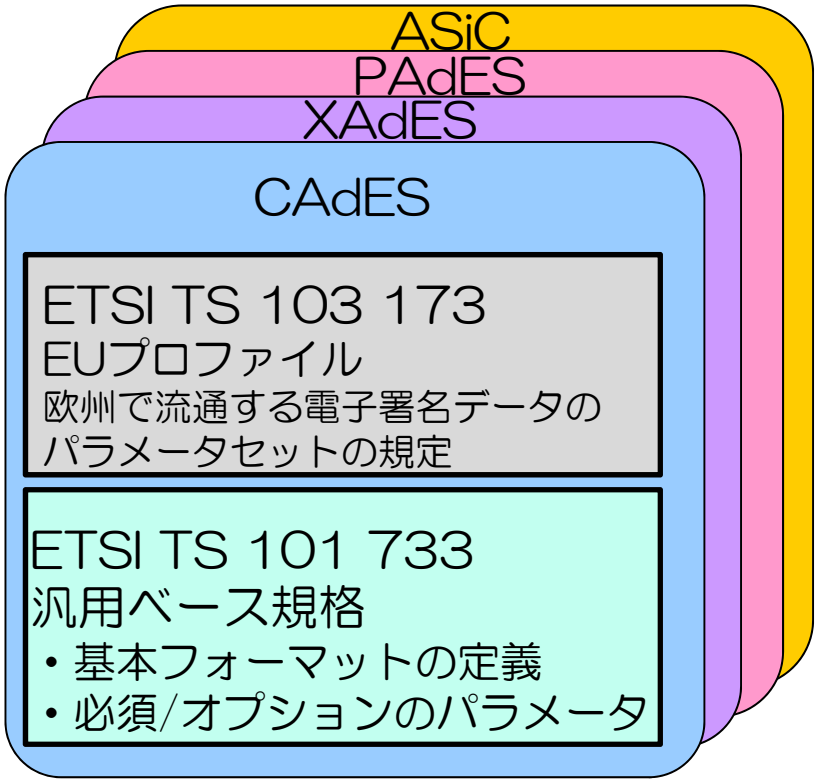
・PDFに特化したフォーマット。
・同仕様がPDF規格に取り込まれる。
（ISO/DIS 32000-2）

ASiC
(Associated Signature Container)

・関連する複数の電子データを一つにパッケージングするフォーマット。
・CAdES/XAdESを適用した形式がある。

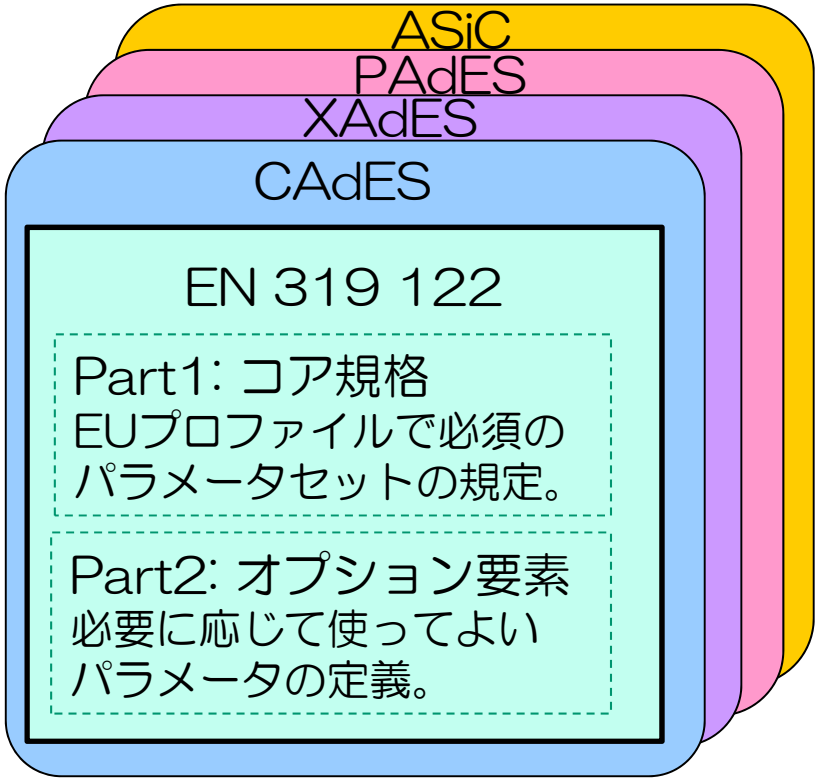
電子署名フォーマット規格の再構築

従来の構成



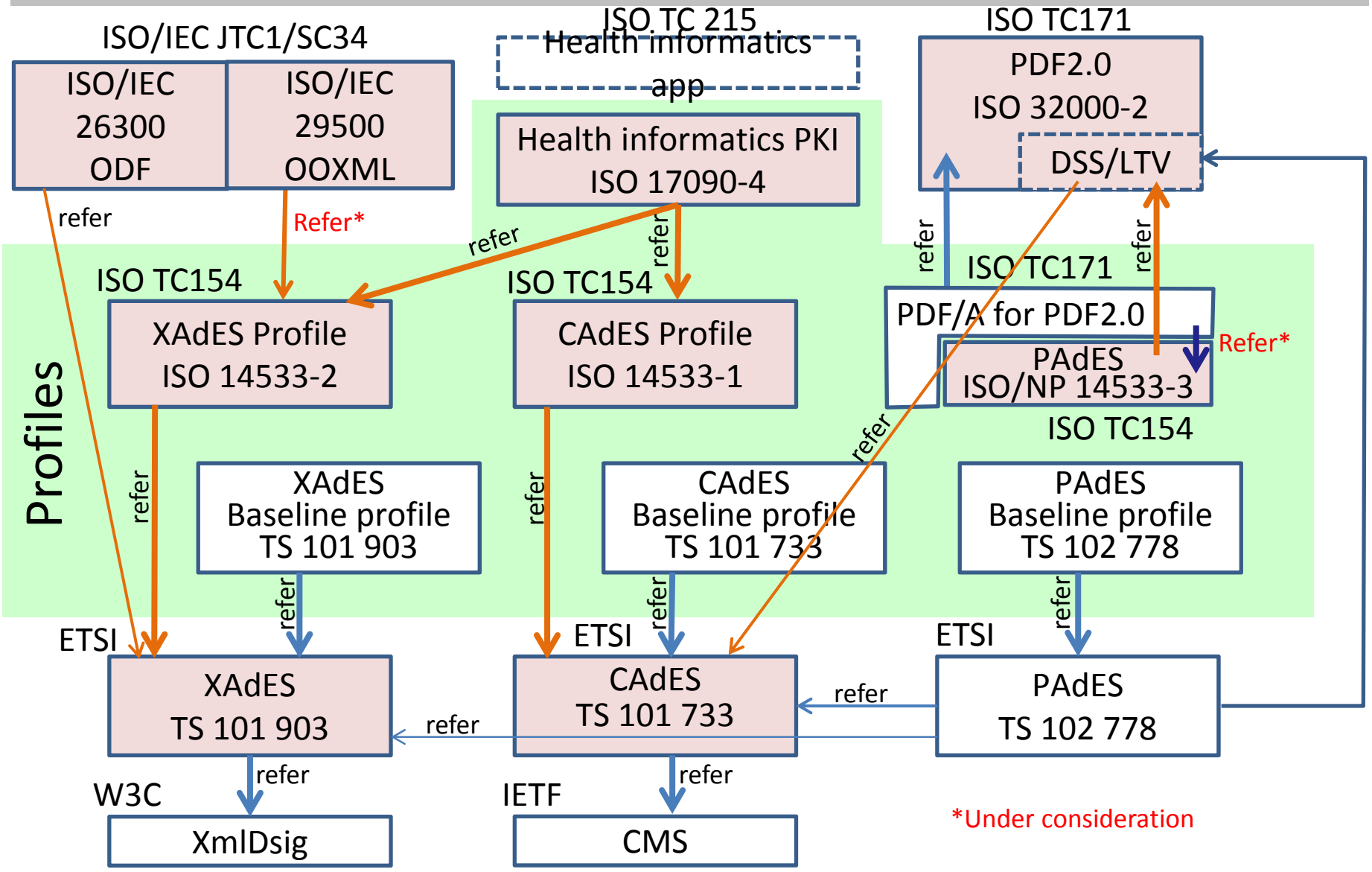
ベース規格とプロファイルが独立しているため、
ベース規格のみ参照することができた。

再構築案（進行中）



EUプロファイルをもとにコア規格を作成。
これまでEUプロファイルと無縁だった所
（特に日本）も影響を受ける。

国際標準（ISO）とETSI規格の関係



国際標準（ISO）の動向

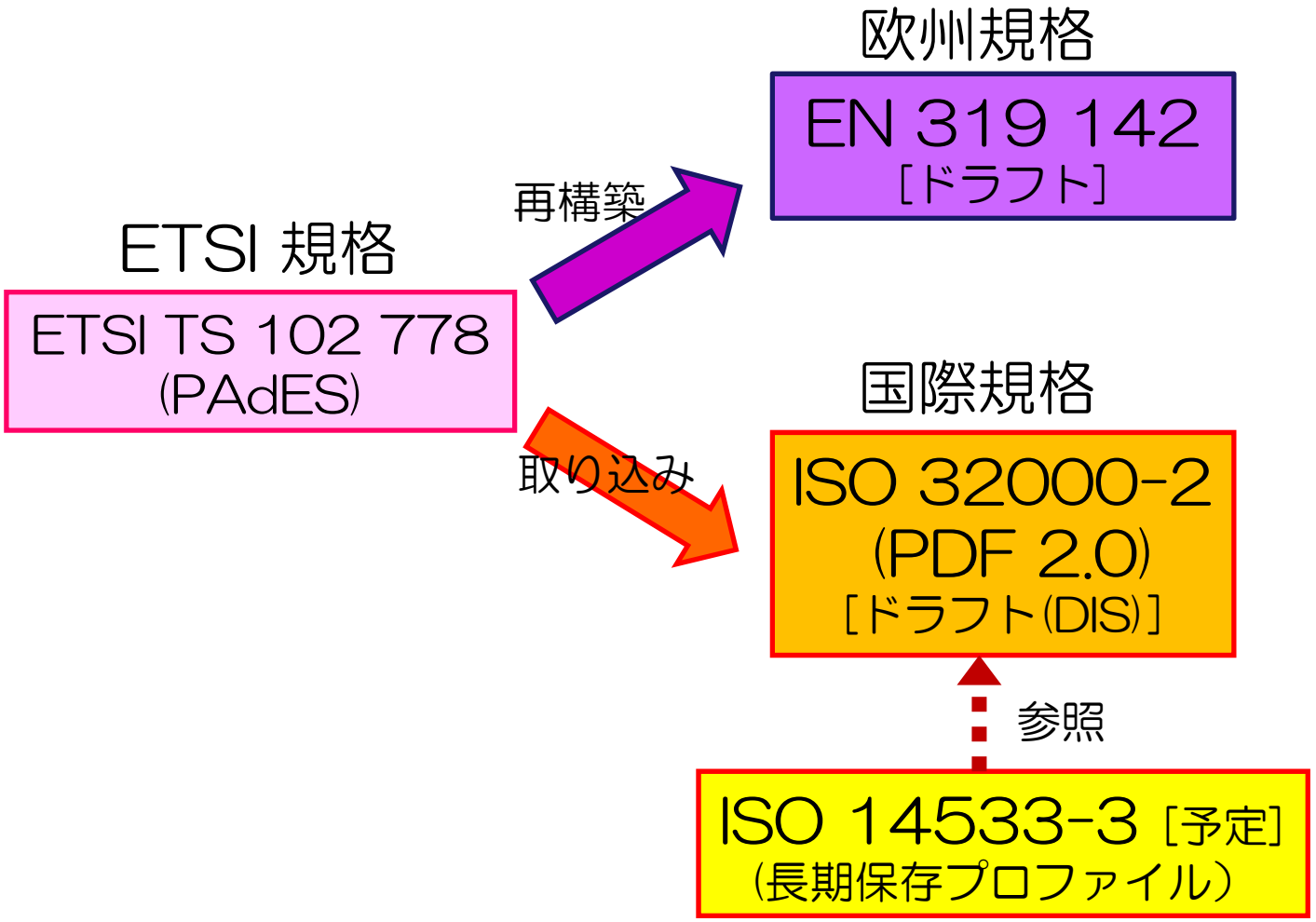
- CAdES関連
  - ISO14533-1:2014
    - CAdES長期保存プロファイル(2012年)の改定版
    - 2014年11月13日発行
    - 新アーカイブタイムスタンプ(v3)仕様対応
    - JNSA電子署名WGが改定作業に参画
- XAdES関連
  - XML文書フォーマット(ODF, OOXML)へのXAdES対応の議論。
    SC34の国内委員会のリエゾンとしてJNSA電子署名WGが参加。
- PAdES関連
  - PDF 2.0 (ISO/DIS 32000-2)のPAdES対応。
    - JNSA電子署名WGがTC171国内委員会を通じてコメント。
  - ISO/NP 14533-3(PAdES長期保存プロファイル)の提案。
    - JNSA電子署名WGが規格原案を作成。

ISO/IEC JTC 1/SC 34における XAdESの議論

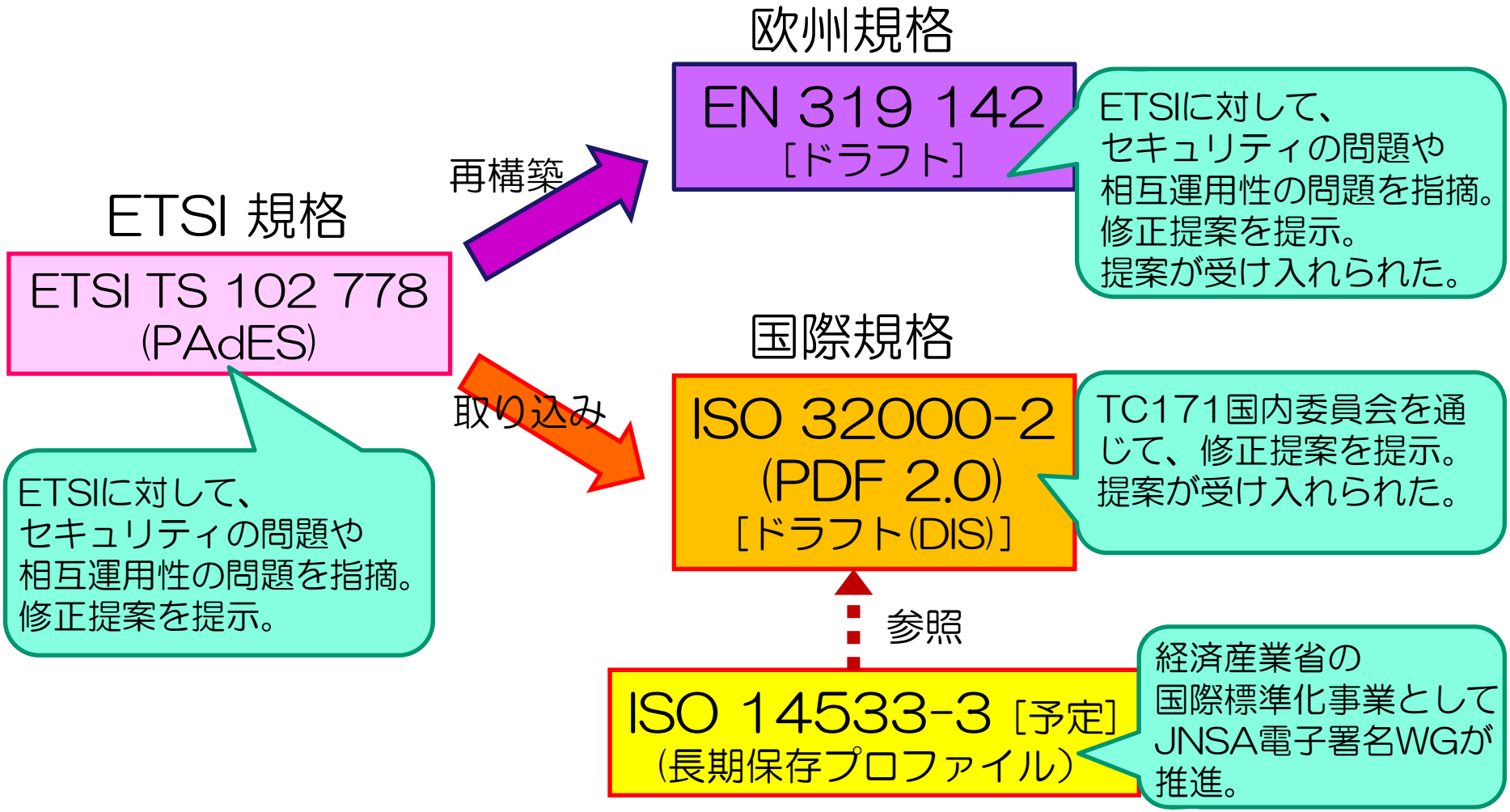
JNSA電子署名WGが国内委員会にリエゾンとして参加。

SC34	フォーマット	ISO/IEC	XAdES対応	現在の状況
WG4	OOXML (MS-Office)	ISO/IEC 29500	議論中	SC34国際会議(京都)にて、Microsoftと規格上の問題と実装の問題について議論。
WG6	ODF (OpenOffice) (LibreOffice)	ISO/IEC 26300	対応済み	国内委員会を通じてコメントし、ODF 1.2 仕様で、XAdESがサポートされるようになった。
JWG7	EPUB (Digital Publishing)	IEO/IEC TS 30135	未定	新たにIDPF(International Digital Publishing Forum)のWGが設立。2015年5月の北京会議で最初のミーティングが行われる。

PAdESに関する標準化動向



JNSA電子署名WGによるPAdESへの関与



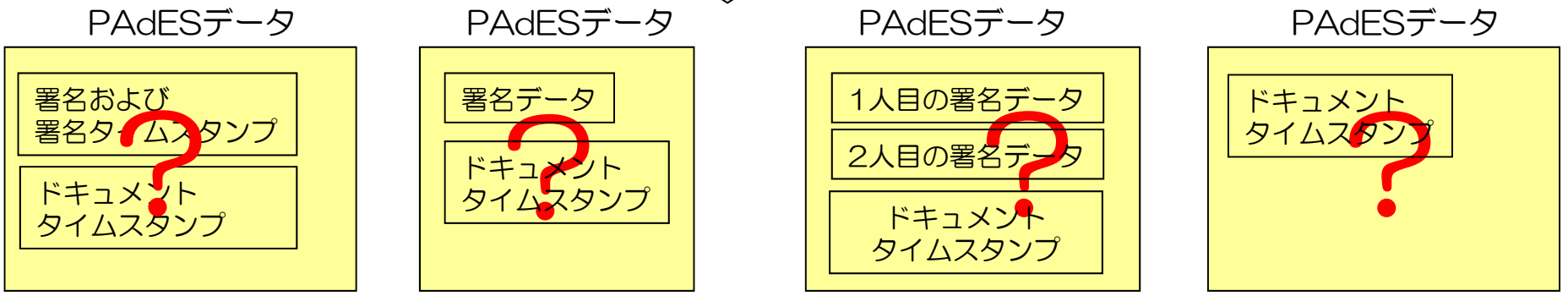
PAdES長期保存プロファイル国際標準化

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
検証のルールも明確でない

様々な実装が存在しうる



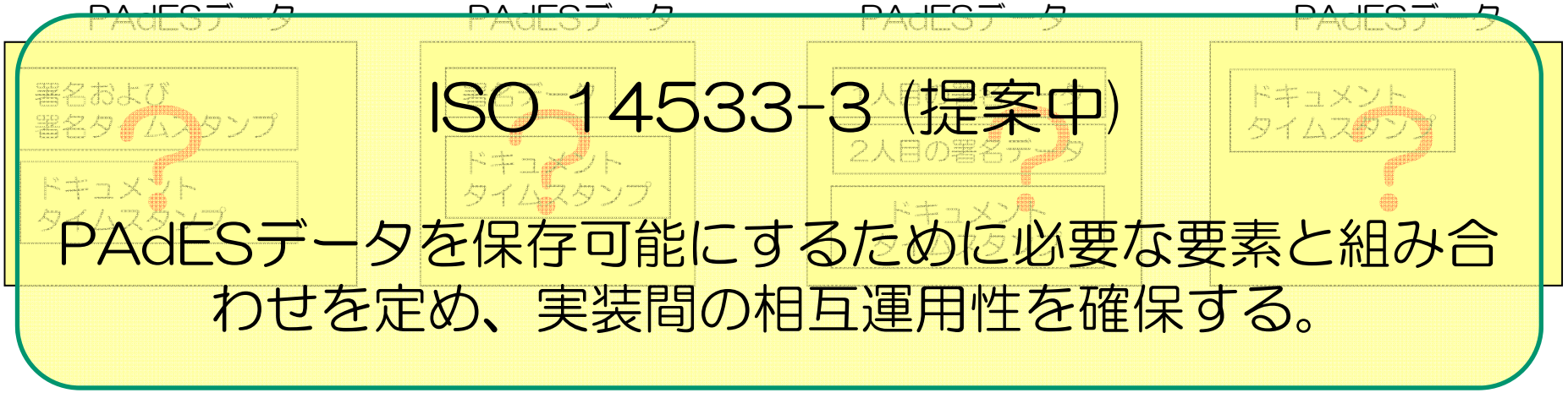
PAdES長期保存プロファイル国際標準化

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
検証のルールも明確でない

様々な実装が存在しうる



ISO 14533-3 (提案中)

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。

ISO 14533-3(提案中)の現在の状況

- 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」の事業として、JNSAが推進。
- JNSA電子署名WGの専門家チームで規格原案を作成。
- 2014年10月のTC154国際会議（韓国・仁川）にてプレゼンテーションを実施。
  - 今後ISO化に向けた作業を進めていくことが承認された。

おわりに

- 欧州では国境を越えて安全な電子取引を推進するためeIDAS規則が定められ、電子署名を含めた標準技術の再構築も行われている。
  - 欧州だけの問題ではなく、国際標準にも影響がある。
- 日本（JNSA電子署名WG）も電子署名の国際標準に対して数々の貢献をしている。
  - 欧州（ETSI）からも期待されており、これまでの貢献についても評価されている。
- 電子上の安全かつトラストな環境づくりが今後も重要である。電子署名は中核の要素と考えられる。
  - トラストサービス全体の視点を持つことが重要。今後の課題でもある。

ご清聴ありがとうございました。