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

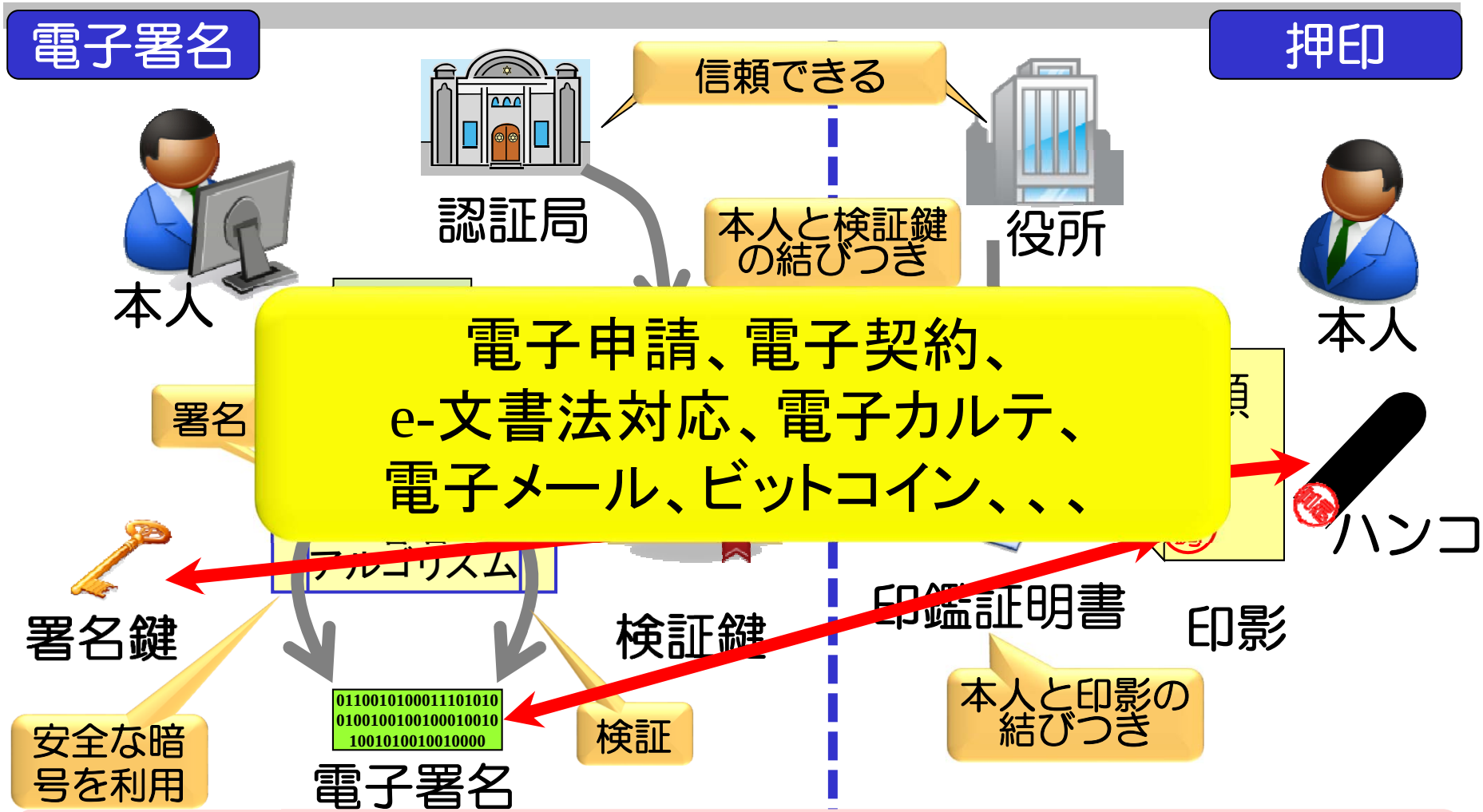
JNSA　2013年度活動報告会

「2013年度 電子署名WG成果報告」

電子署名WG
宮崎　一哉
（三菱電機株式会社）

2014 年　6月　10日（火）　ベルサール神田

電子署名とは

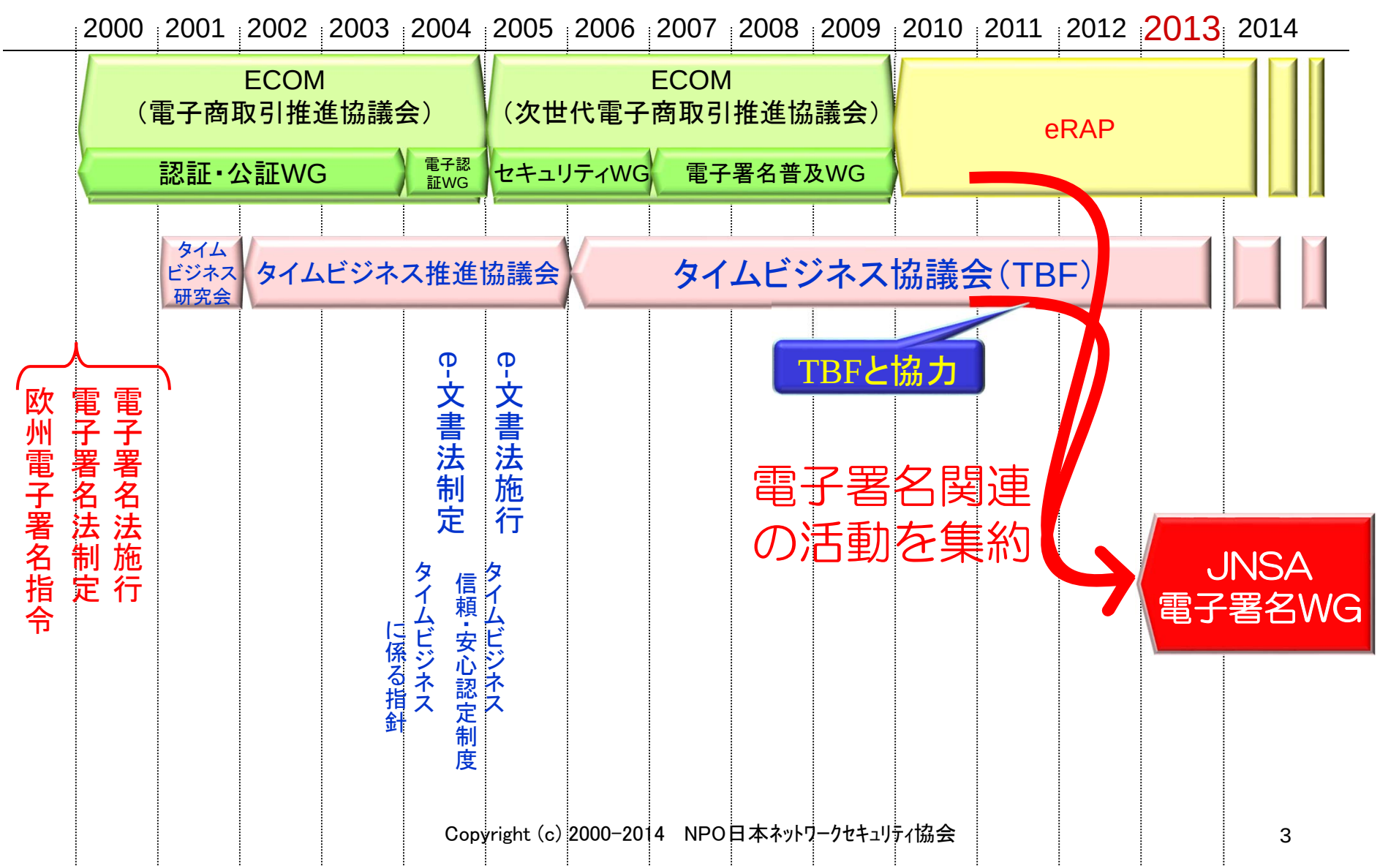


電子署名は、署名者が誰であるかに加え、電子文書が改ざんされていないことも確認できる技術。

報告内容

- 電子署名WG
  - 設立経緯、活動目標、体制
- 2013年度活動計画・成果予定・実績
- 2013年度活動内容
  - 署名検証TF、PAdESプロファイルTF、スキルアップTF
- 2014年度活動計画

2013年度：電子署名WG設立

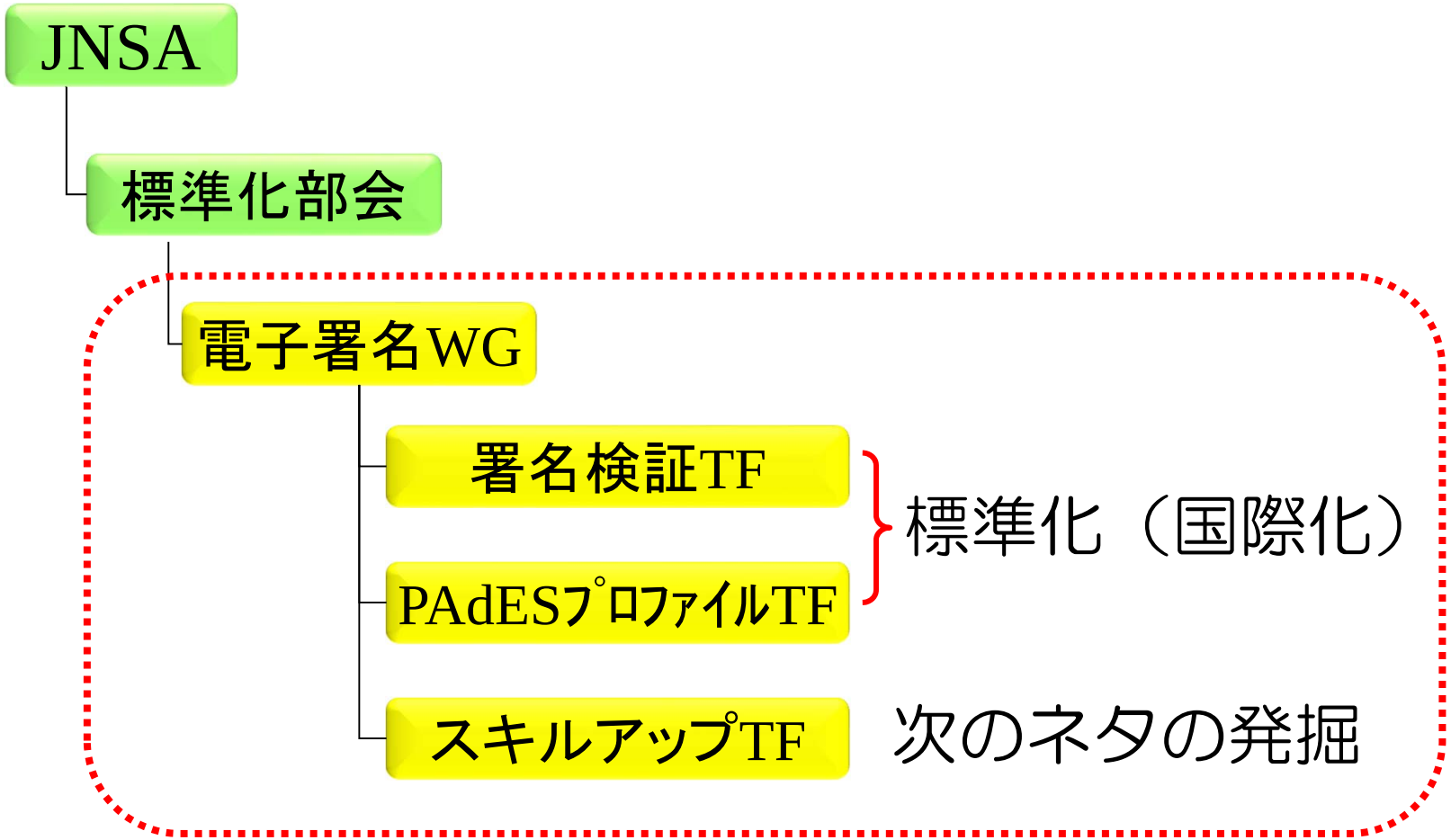


活動目標

- 電子署名（含タイムスタンプ）の相互運用性確保のための調査、検討、仕様提案、相互運用性テスト、及び電子署名普及啓発を行う。

⇒　電子署名の拠点

体制



2013年度活動計画

- テーマ
  - ① 署名検証要件に関する標準作成
  - ② PAdESプロファイルに関する標準作成
  - ③ 署名関連の勉強会、情報交換
- 活動方法
  - テーマ毎にTFを設置し、個別に会合を実施。
  - 欧州電気通信標準化機構/電子署名基盤技術委員会（ETSI/TC ESI）†、 TBF等と連携しつつ、国内で年間10回程度の会合を実施。
  - 合宿1回、懇親会2回を予定。

†JNSAをETSI会員として登録済み

2013年度成果予定（1/2）

① 署名検証要件に関する標準案

- 2012年度作成の初版をベースにETSIに提案し、ETSI標準として成立させる。
- ETSI/TC ESI#38会議（3月12-13日）に初版を、ESI#39会議（6月3-5日）に第2版をインプット済み。

② PAdESプロファイルに関する標準案

- CAdES/XAdESプロファイルに倣い、ETSIと情報交換を行いつつ、まずJIS化に向けたドラフトを作成する。
- JSAの「JIS原案作成公募制度」に応募し、JIS原案作成に着手できるようにする。

JSA：一般財団法人日本規格協会

2013年度成果予定（2/2）

③ 署名関連の勉強会

- オープンソースプロジェクト
  FreeXAdES
- Java6以降標準提供された
  XMLSignature クラスを拡張して実装
- 成果物はMITやGPLのライセンスで公開
- ２ヶ月に1回程度の勉強会を開催し少しずつ実装を進める

2013年度活動実績

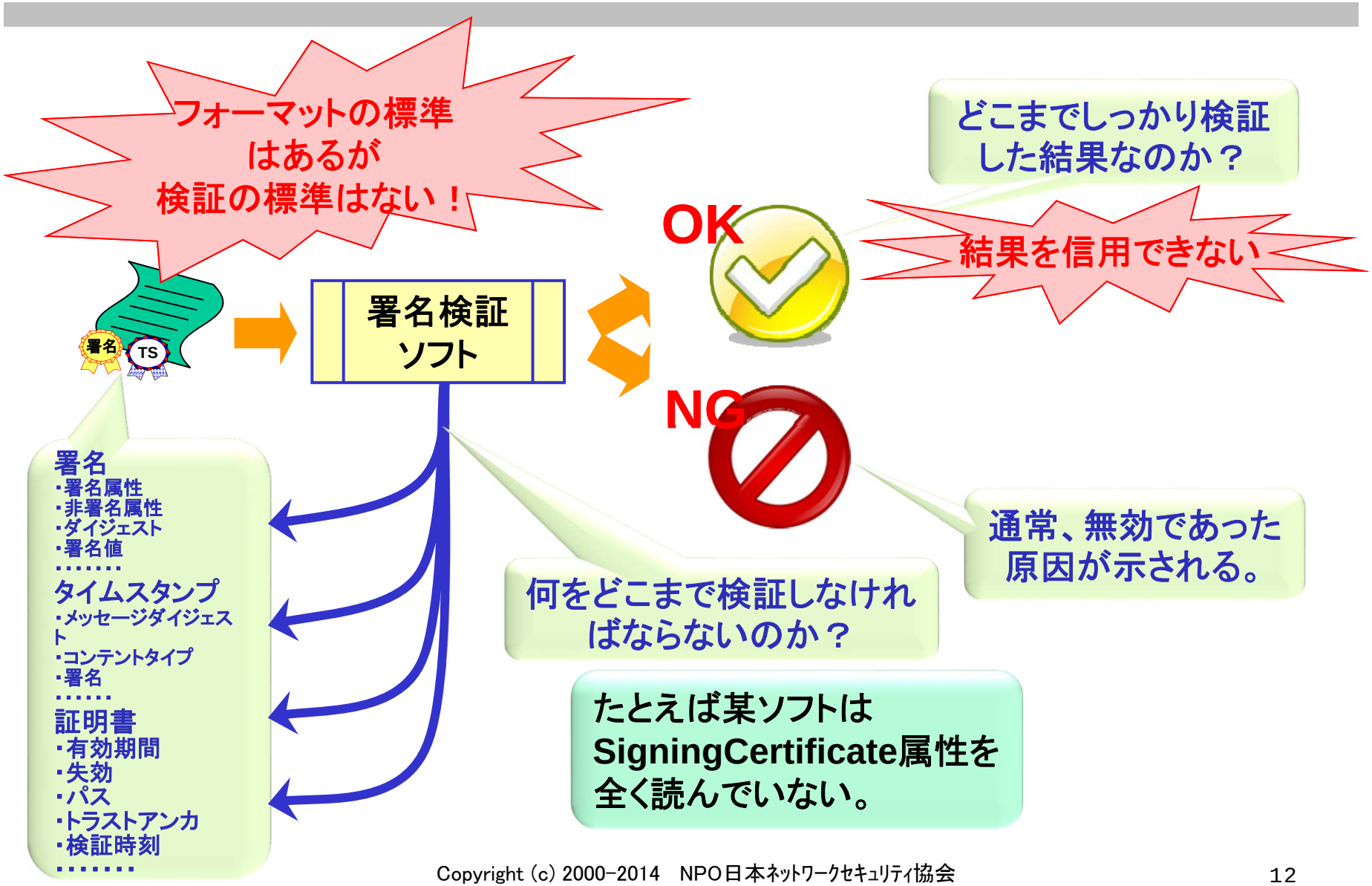
- WG／TF（計38回）
  - 電子署名WG：11回
  - 署名検証TF：9回
  - PAdESプロファイルTF：11回
  - スキルアップTF：7回
- セミナー／講演
  - JNSA 2012年度活動報告会
  - Network Security Forum 2014
  - PKI Day 2014
- ETSI対応
  - 第40回 ETSI/TC ESI会議（@スペイン ビルバオ）
  - 第42回 ETSI/TC ESI会議（@オーストリア ウィーン）
  - ETSI/TC ESI会議議長との会議（@東京）
- その他
  - 合宿（@伊東）
  - ビットコイン勉強会
  - 懇親会：2回

2013年度活動実績

	4	5	6	7	8	9	10	11	12	1	2	3
電子署名WG	△ 説明会	△	△	△	△	△	△	△	△ ★合宿	△	△	△
署名検証TF				△	△	△	△	△	△	△	△	△
PAdES ﾌﾟﾛﾌｧｲﾙTF			△	△	△	△	△	△	△	△	△	△ △
スキルアップTF				△	△	△	△	△		△	△	△
講演会			△ JNSA 2012年度活動報告会							△ NSF2014		△ PKI Day 2014
ETSI会議			#39			#40			#41		#42	△ ESI議長との会議

署名検証TF

署名検証の問題点



署名検証標準規格の意義

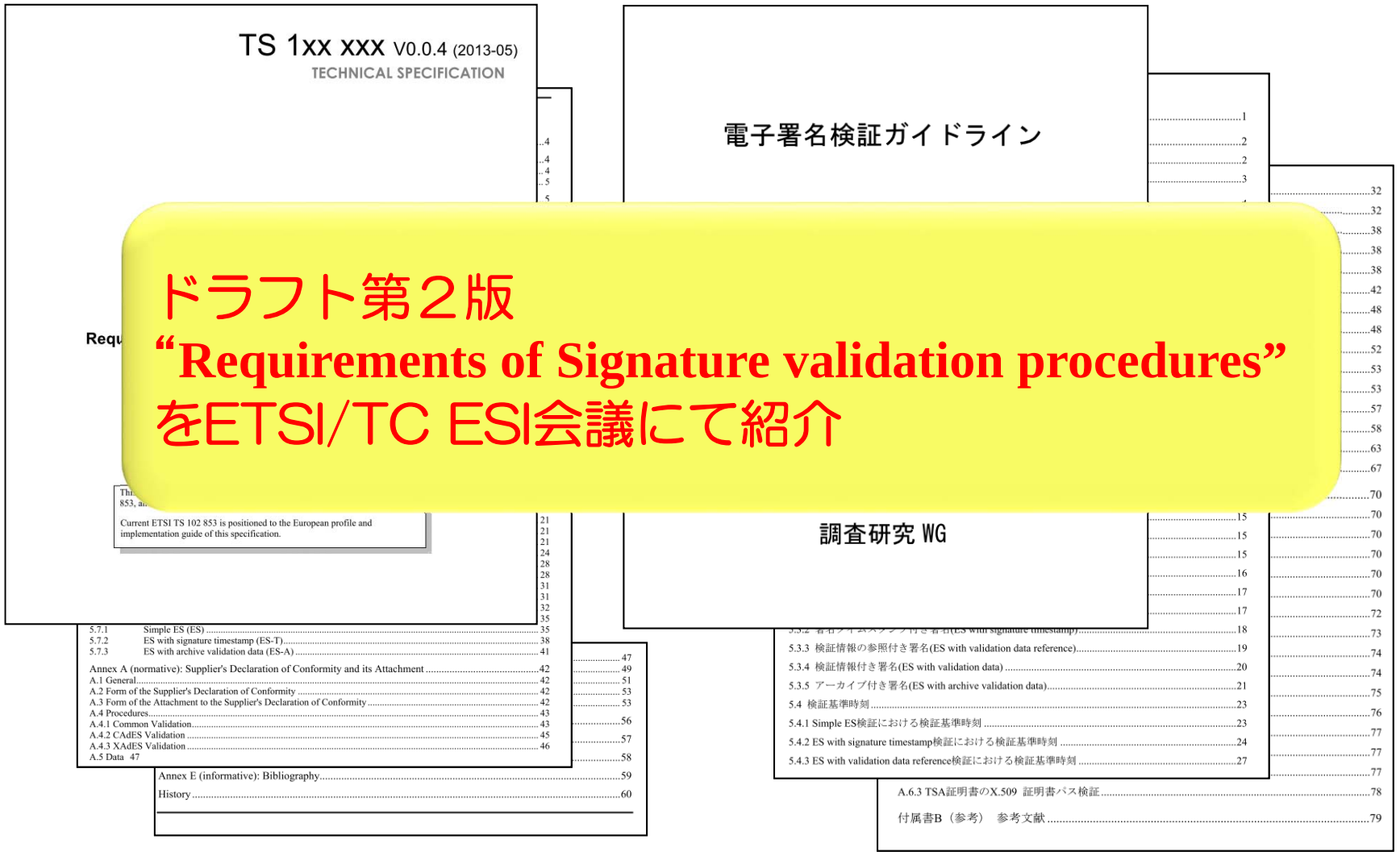
- 署名検証における検証項目等の要件を定義
- 検証結果の出力内容を定義
- 検証ソフトウェアの検証範囲を明示できる枠組み（適合宣言書）を提供

⇒実装者にとって、実装方法がわかる。

⇒調達者・利用者にとって、検証範囲がわかる。

⇒安全・安心な署名検証ソフト

署名検証標準規格の作成状況



ドラフト第２版
“Requirements of Signature validation procedures”
をETSI/TC ESI会議にて紹介

我々の標準案の特徴

- 実装方式に依存しない汎用的な要求仕様
- 作成された実装のチェックが容易なテーブル表記をベースとした記述
  - チェックリスト⇒付録に「適合宣言書」

テーブル表記の例

検証対象

要求レベル

Object	Criteria	Semantics	M/O	Status Indication	Report (example)
Data structure	Validity of the data structure	The signature data structure is contained all the mandatory elements of Table 15.	M	VALID	- Validation result
				INVALID	- Reason of INVALID - Missing elements
	CMS data type	"ContentType" is object identifier of "id-signedData".	M	VALID	- Validation result
				INVALID	- Reason of INVALID
	Signed data type	"eContentType" is object identifier of "TSTInfo".	M	VALID	- Validation result
				INVALID	- Reason of INVALID
TSA certificate	Validity of TSA certificate	It is verified according to the requirements of TSA certificate validation in Clause 5.7.2.	M	Refer to Clause 5.7.2.	
Signature of TSA	Validity of "digestAlgorithms" field	"digestAlgorithms" field in "Content" is verified according to the requirement of the Digest alogorithm validation in Clause 5.5.1.	M	Refer to Clause 5.5.1.	
	Validity of "digestAlgorithm" field	"digestAlgorithm" field in "signerInfo" is verified according to the requirement of the Digest alogorithm validation in Clause 5.5.1.	M	Refer to Clause 5.5.1.	
	Consistency of "MessageDigest" attribute	The following two values in "signerInfo" are matched. 1) The hash value of "eContent" value computed with the algorithm specified in "digestAlgorithm" field 2) The value of "MessageDigest" in "signedAttrs" field	M	VALID	- Validation result
				INVALID	- Reason of INVALID - Each hash value
	Consistency of the hash value for TSA certificate in "SigningCertificate" attribute	The following two values in are matched. 1) The hash value of TSA certificate computed with the algorithm used in "SigningCertificate" attribute 2) The value of "certHash" in "SigningCertificate" attribute	M	VALID	- Validation result
				INVALID	- Reason of INVALID - Each hash value
	Validity of "signatureAlgorithms" field	"signatureAlgorithm" field in "signerInfo" is verified according to the requirement of the Signature alogorithm validation in Clause 5.5.1.	M	Refer to Clause 5.5.1.	
	Validity of the signature value by public key in a TSA certificate	According to the algorithms of "signatureAlgorithm" and "digestAlgorithm" in "signerInfo", the consistency of the signature value in "signerInfo" and the hash value for e verified with public key in TSA	M	VALID	- Validation result
				INVALID	- Reason of INVALID

検証基準

出力内容

ETSIの標準案

- ETSI EN 319 102, “Electronic Signatures and Infrastructures (ESI); **Procedures for Signature Creation and Validation**”
- ETSIの専門家チームにより、ドラフトのレビュー結果に対応中。

仕様ドラフト間の相違

ETSI	JNSA
実装方式依存	汎用仕様
プロ	
出力	
POE （何らかの存在証明）	（時刻ありき）

ESI議長との会議により、
国際標準化に向けて協調していくことに合意。

Timestampに関する記述が足りない

コントロールタイムやフレッシュネスの概念が分かりにくい

PAdESプロファイルTF

PAdESプロファイルの標準化

- PAdES(PDF Advanced Electronic Signature)
  - ベース規格 ETSI TS 102 778 Part1～Part6
  - 現在策定作業中のPDF規格(ISO 32000-2)に取り入れられる予定。
- PAdESの主な特徴と問題点
  - 従来のPKCS#7ベースのPDF署名(PAdES Basic)に加え、CAdESを用いたPAdES Enhancedを定義している。
  - 検証に必要な証明書や失効情報を格納するためにDSSというPDFの要素を定義している。
  - PDFに適用するタイムスタンプ（ドキュメントタイムスタンプ）を定義している。
  - 問題点：DSSや署名、ドキュメントタイムスタンプ等の様々な要素の組み合わせの自由度が高い一方で、様々なパターンに応じた利用方法（生成・検証）が示されておらず、相互運用性の問題が生じる。
- PAdESプロファイルの考え方
  - 長期的に保存可能なPAdESを実現するうえで必要な各要素の利用方法（生成方法）を定める。
  - ベース規格へ反映すべき事項はETSIやISOに提言する。

PAdESプロファイルの位置付け

CAdES
（CMS Advanced Electronic Signature）

バイナリデータ形式（ASN.1）のフォーマット

母体となる規格

- ETSI TS 101 733
- RFC 5126 (IETF)

ECOM/eRAPが原案作成

- JIS X 5092:2008
- ISO 14533-1

XAdES
（XML Advanced Electronic Signature）

XML形式のフォーマット

母体となる規格

- ETSI TS 101 903

ECOM/eRAPが原案作成

- JIS X 5093:2008
- ISO 14533-2

長期保存のためのプロファイル

PAdES
（PDF Advanced Electronic Signature）

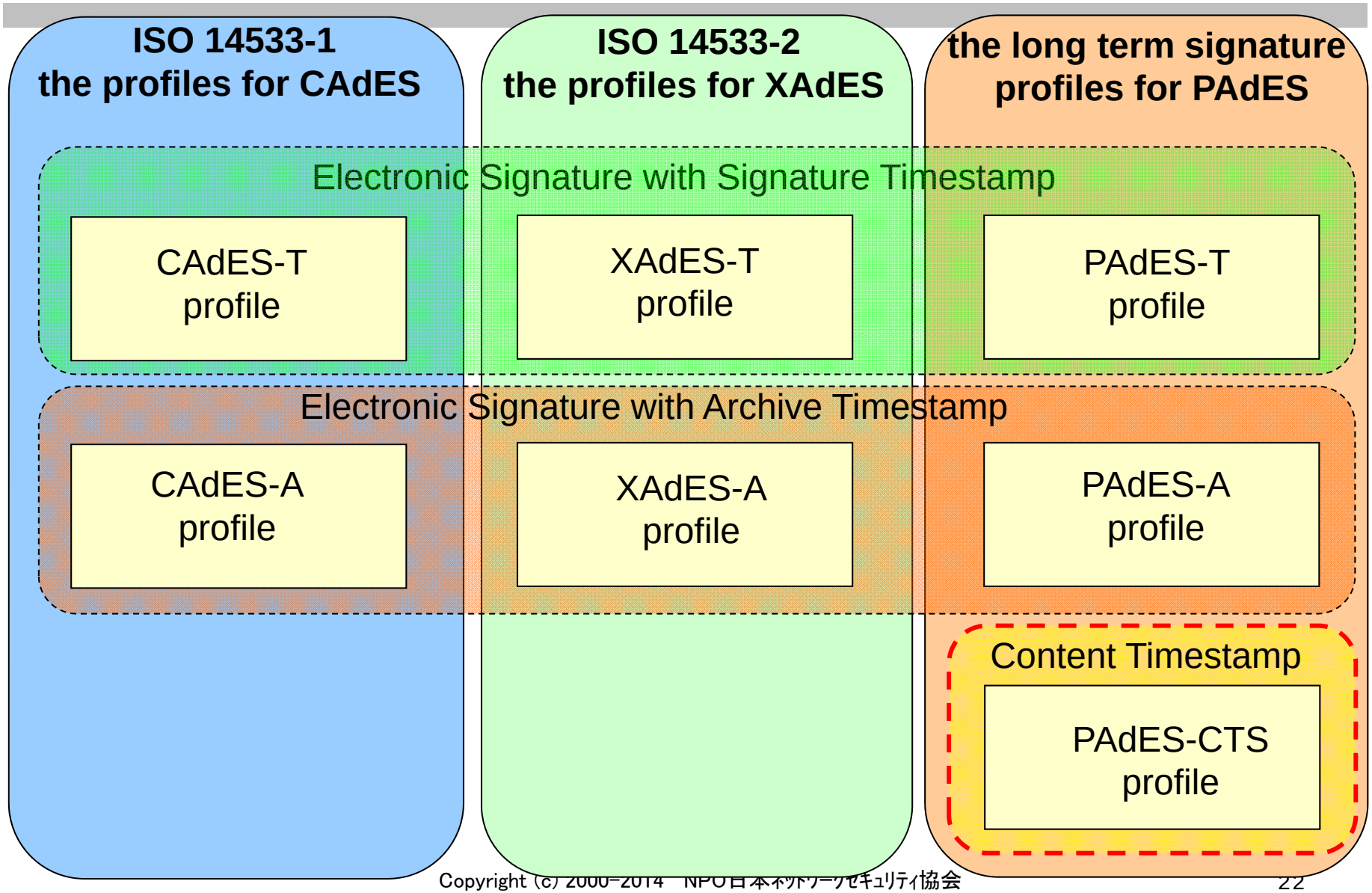
PDF形式のフォーマット

母体となる規格

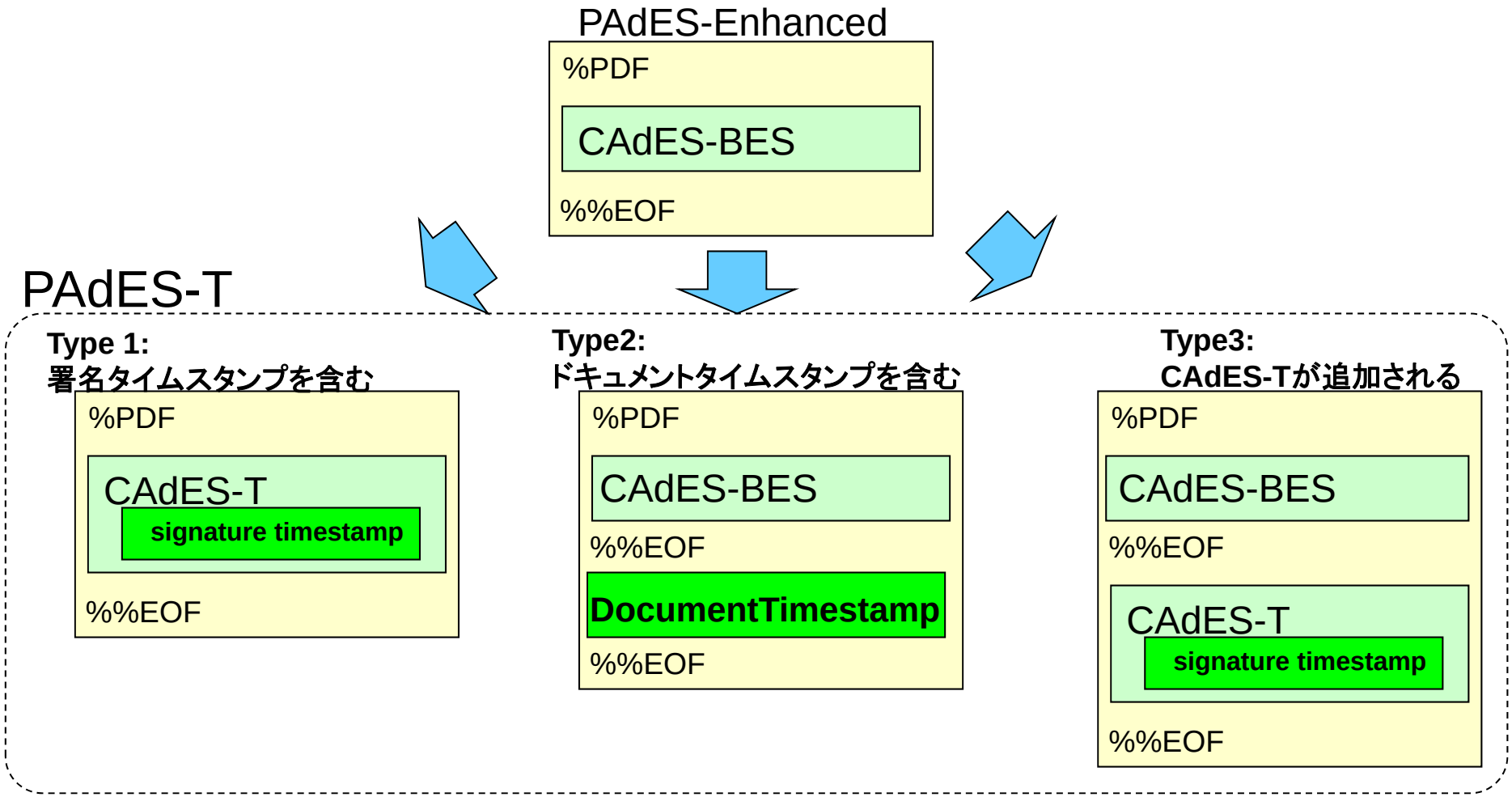
- ETSI TS 102 778
- ISO 32000-2(draft)

同じ位置付けの規格がない！

長期署名保存のためのプロファイルの構造

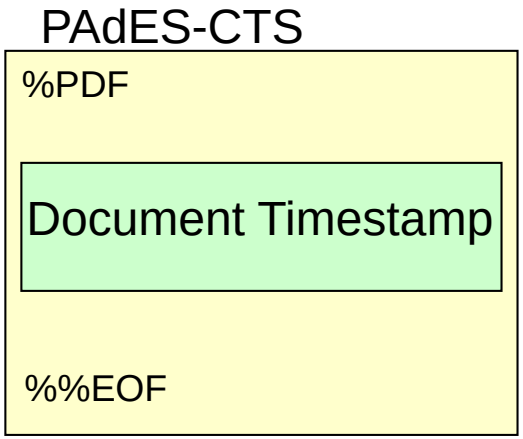


PAdES-Tプロファイル



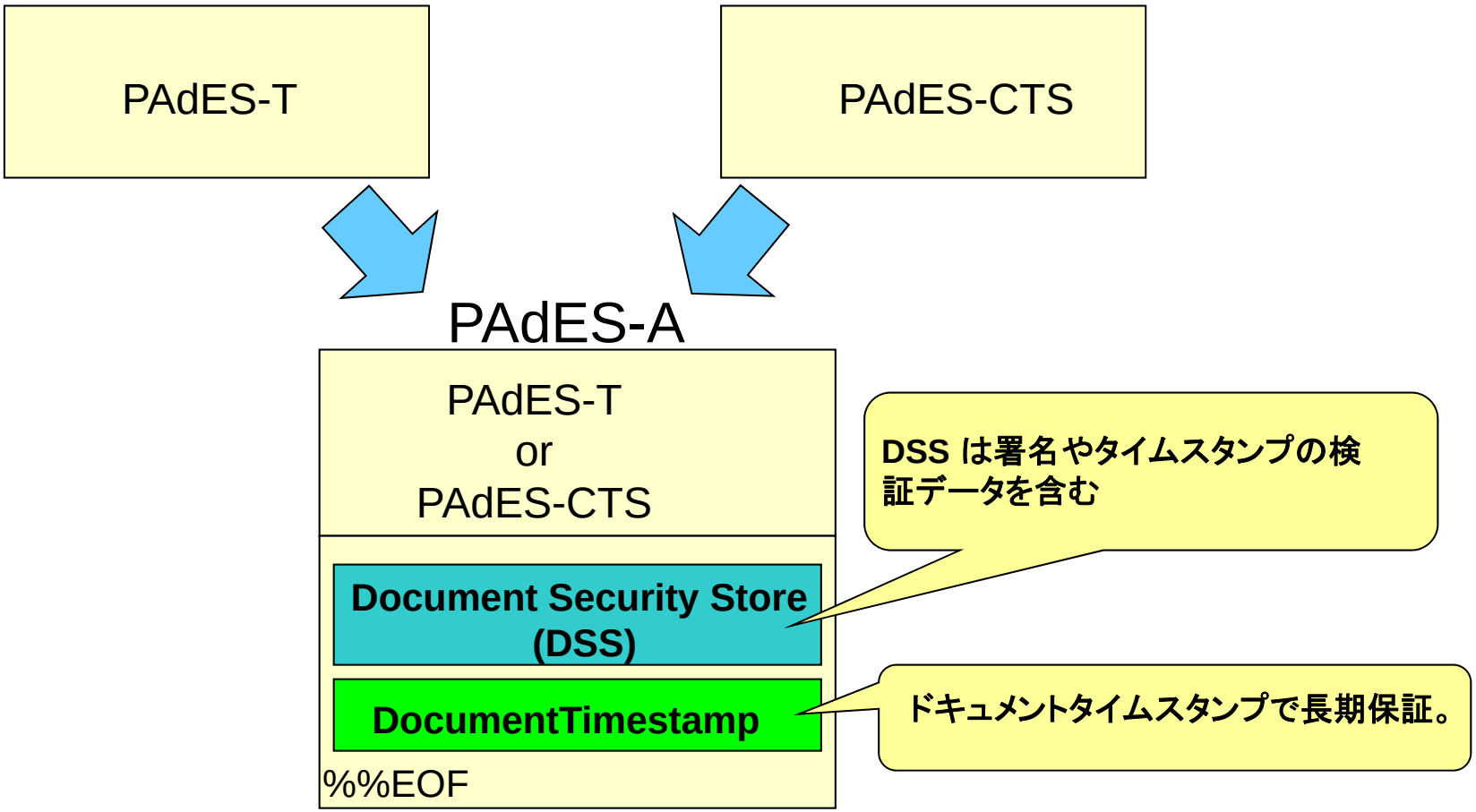
PAdES-CTSプロファイル

署名を含まず、タイムスタンプのみ含む。

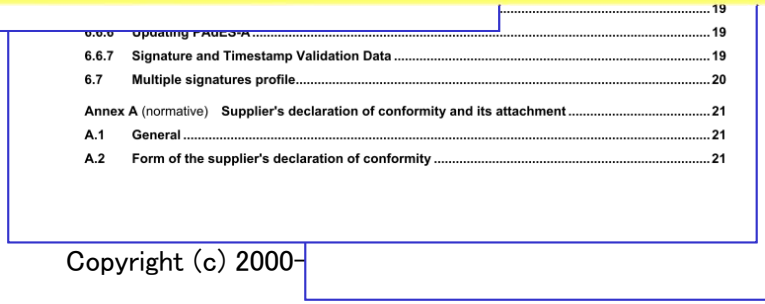


PAdES-Aプロファイル

PAdES-T と PAdES-CTSの両者の有効性を延長するプロファイル。



- ドラフト第１版
“Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)”
をETSI/TC ESI会議にて紹介。
- ISOに提案することに合意。
- PAdESのベース規格へもコメント
⇒ほぼ受け容れられた。



スキルアップTF

勉強会

第1回：7月：長期署名入門
講師＞電子署名WGオールスター 宮崎氏、佐藤氏、石本氏、西山氏、宮地

第2回：8月：クラウド署名とHSM
講師＞タレス・ジャパン 住田氏、セーフネット/JIPDEC客員研究員 亀田氏、他

第3回：9月： jsrsasign / jsjws 勉強会
講師＞富士ゼロックス 漆嶌氏
補足＞JavaScriptによるRSA/PKIモジュールとJSON署名

第4回：10月： PDF電子署名仕様入門
講師＞ラング・エッジ 宮地

第5回：11月：クラウド時代のデータセキュリティ
講師＞ガードタイム 柳原氏
補足＞ガードタイム社による非PKI署名他

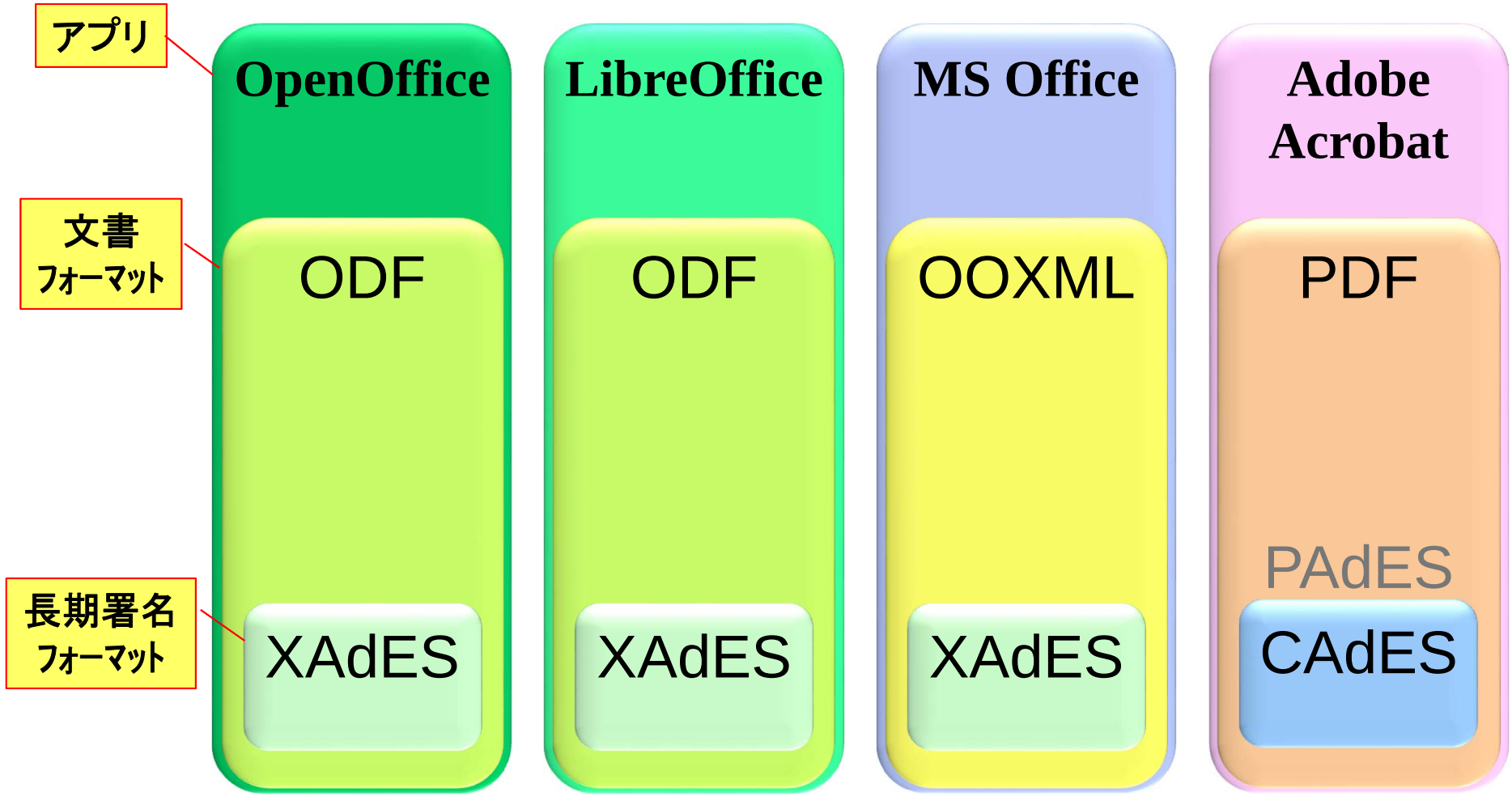
第6回：1月：電子署名WG合宿ダイジェスト

第7回：2月：オープンデータにおける署名・タイムスタンプの活用
講師＞ラング・エッジ 宮地

2014年度の活動計画

- 標準化の完遂
  - 署名検証規格
    - ETSI標準案およびコメントの精査と標準化の方向性の見直し⇒プロファイル対応の検証規格としてISO化
  - PAdESプロファイル規格
    - TC154にてISO15433‐3として標準化
      経産省「平成２６年度戦略的国際標準化加速事業」受託
- 文書形式への長期署名の組込み
  - ISO/IEC JTC 1/SC34とのリエゾン関係確立
    （文書の記述と処理の言語に関する標準化）
  - OOXML、ODF⇒各種オフィス製品

長期署名と文書形式



クラウド署名実証実験の構成案