

JNSA 2015年度活動報告会

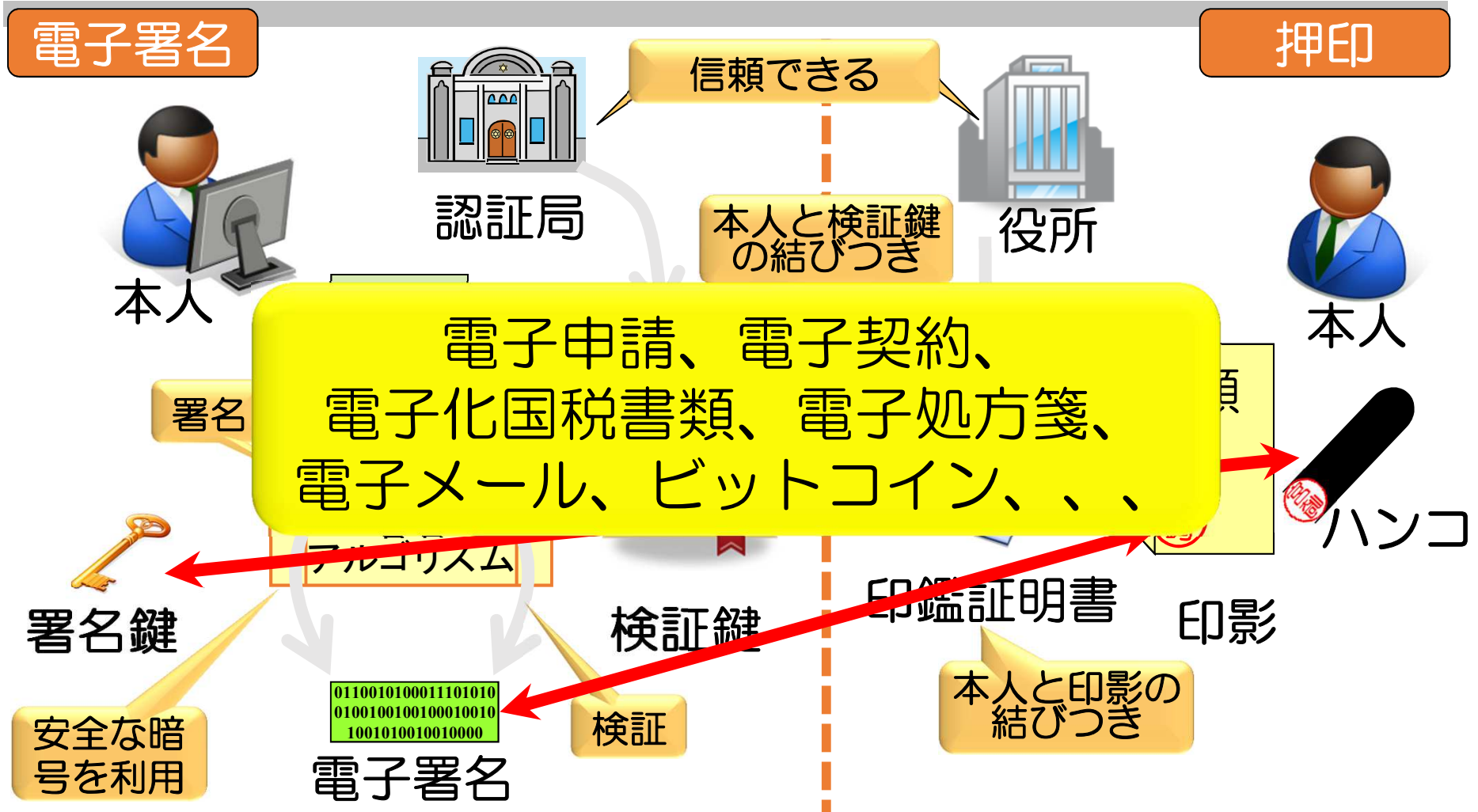
2015年度 電子署名WG成果報告

電子署名WG

宮崎 一哉

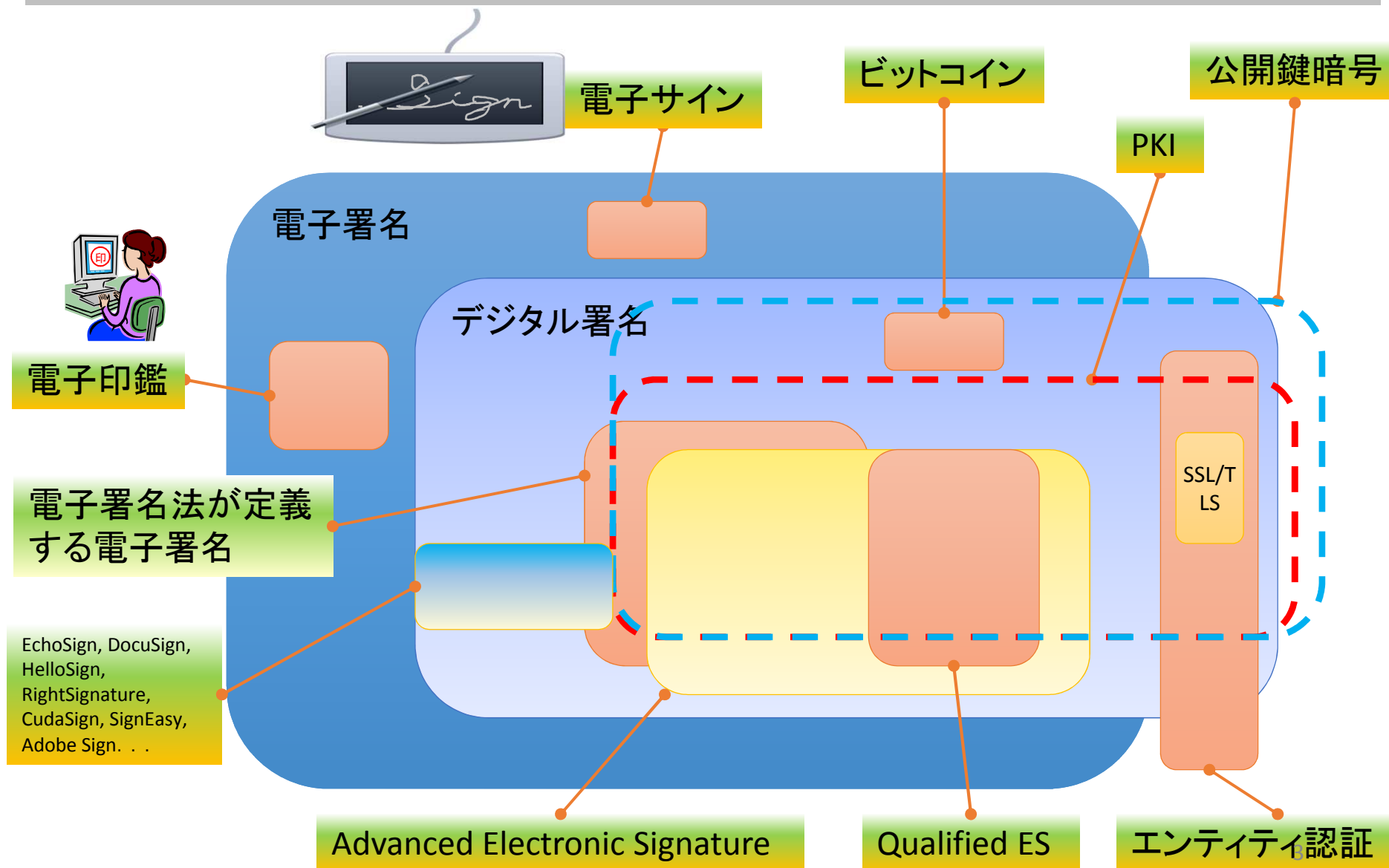
2016年6月17日（金） ベルサール神田

電子署名とは

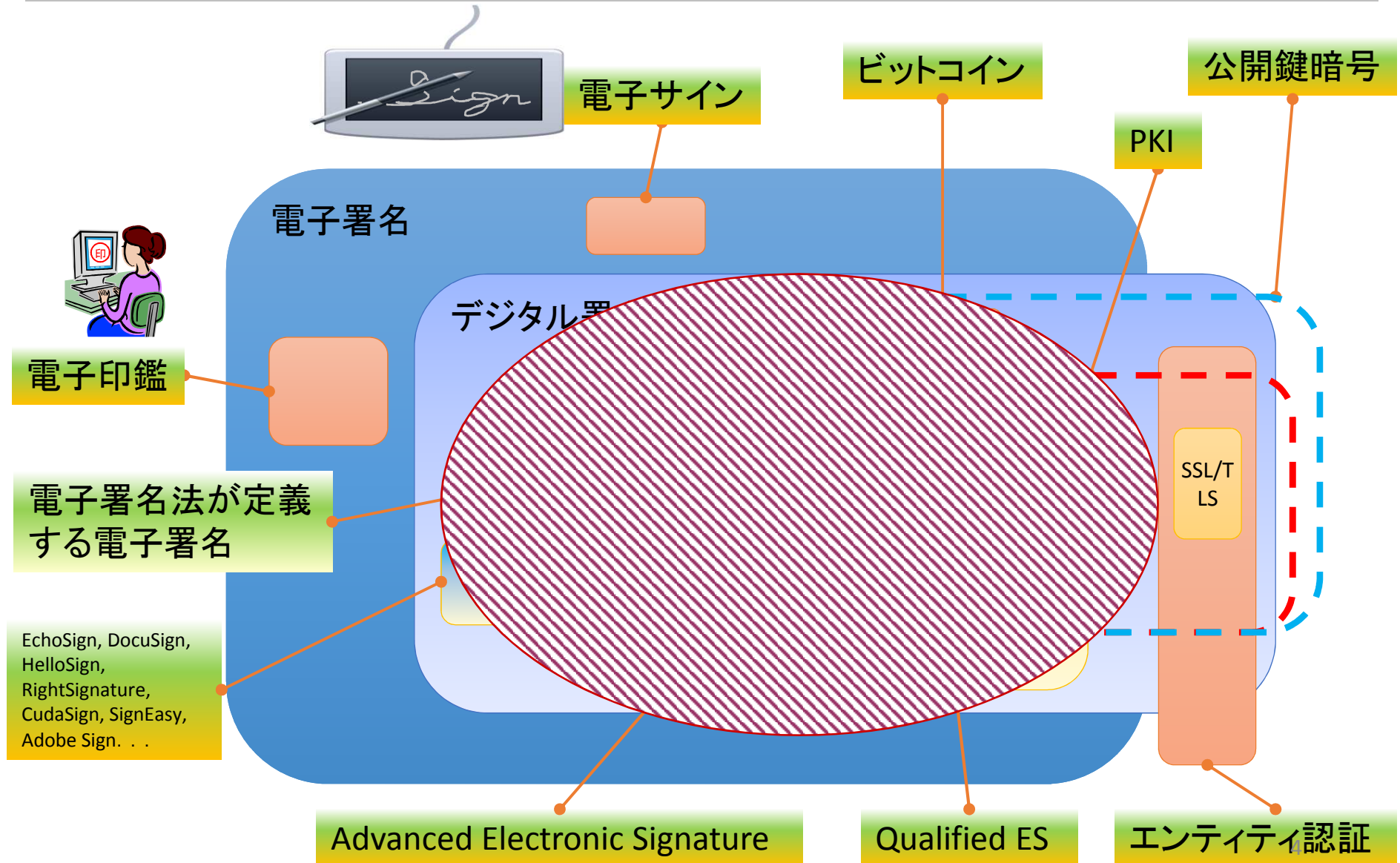


電子署名は、署名者が誰であるかに加え、電子文書が改ざんされていないことも確認できる技術。電子文書に「トラスト」を与える。

電子署名の周辺技術



電子署名WGの対象領域



要するにポイントは

否認防止

約束

コミットメント

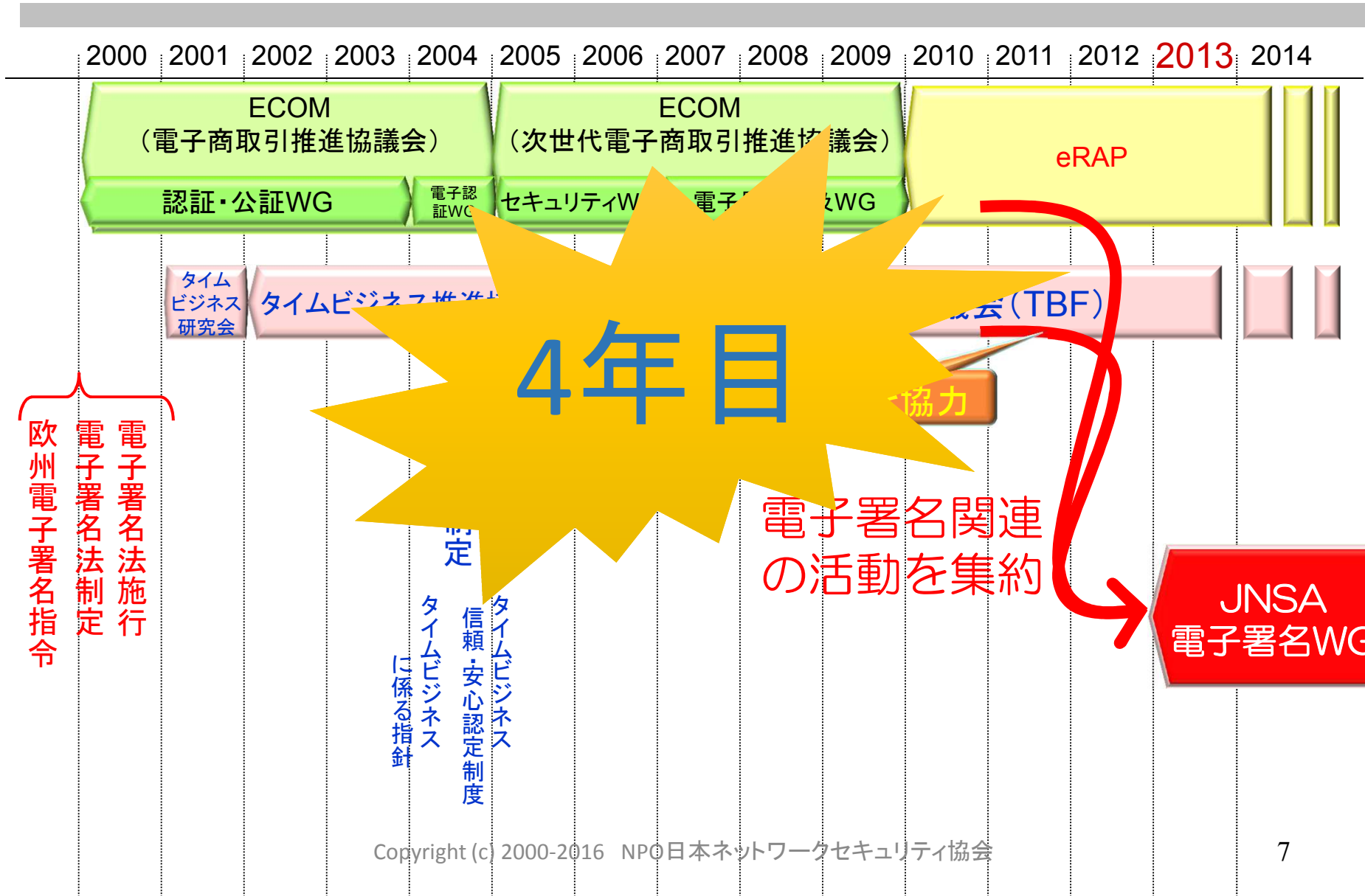
トラスト

報告内容



- 電子署名WG
 - 設立経緯、活動目的、体制、主な活動
- 2015年度活動計画・実績
- 2015年度活動内容
- 標準化と欧州の動向
- 今後の電子署名WG

2013年度：電子署名WG設立



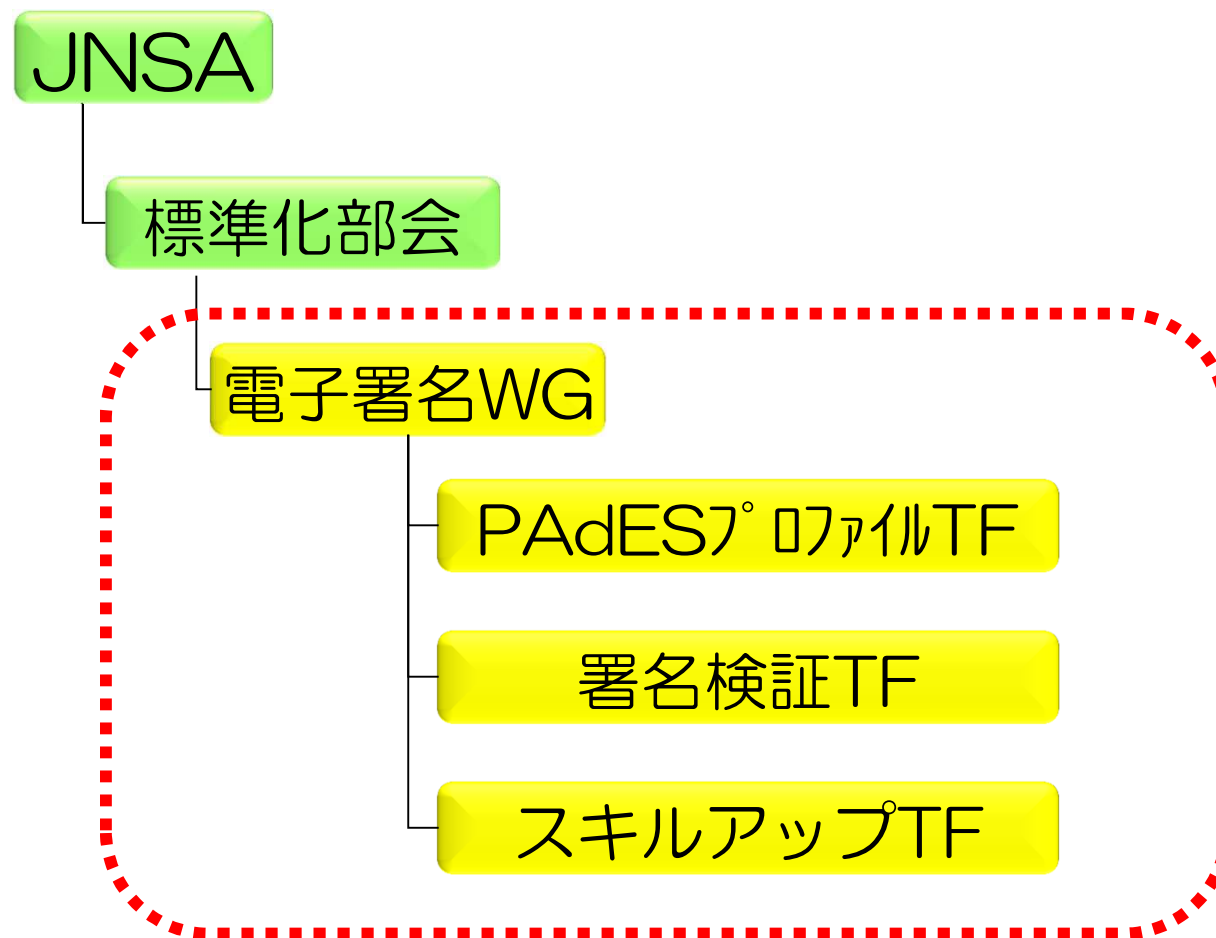
- 電子署名の相互運用性確保のための調査、検討、仕様作成、標準化、相互運用性テスト、及び電子署名普及啓発を行う。

⇒ **電子署名の総合拠点**

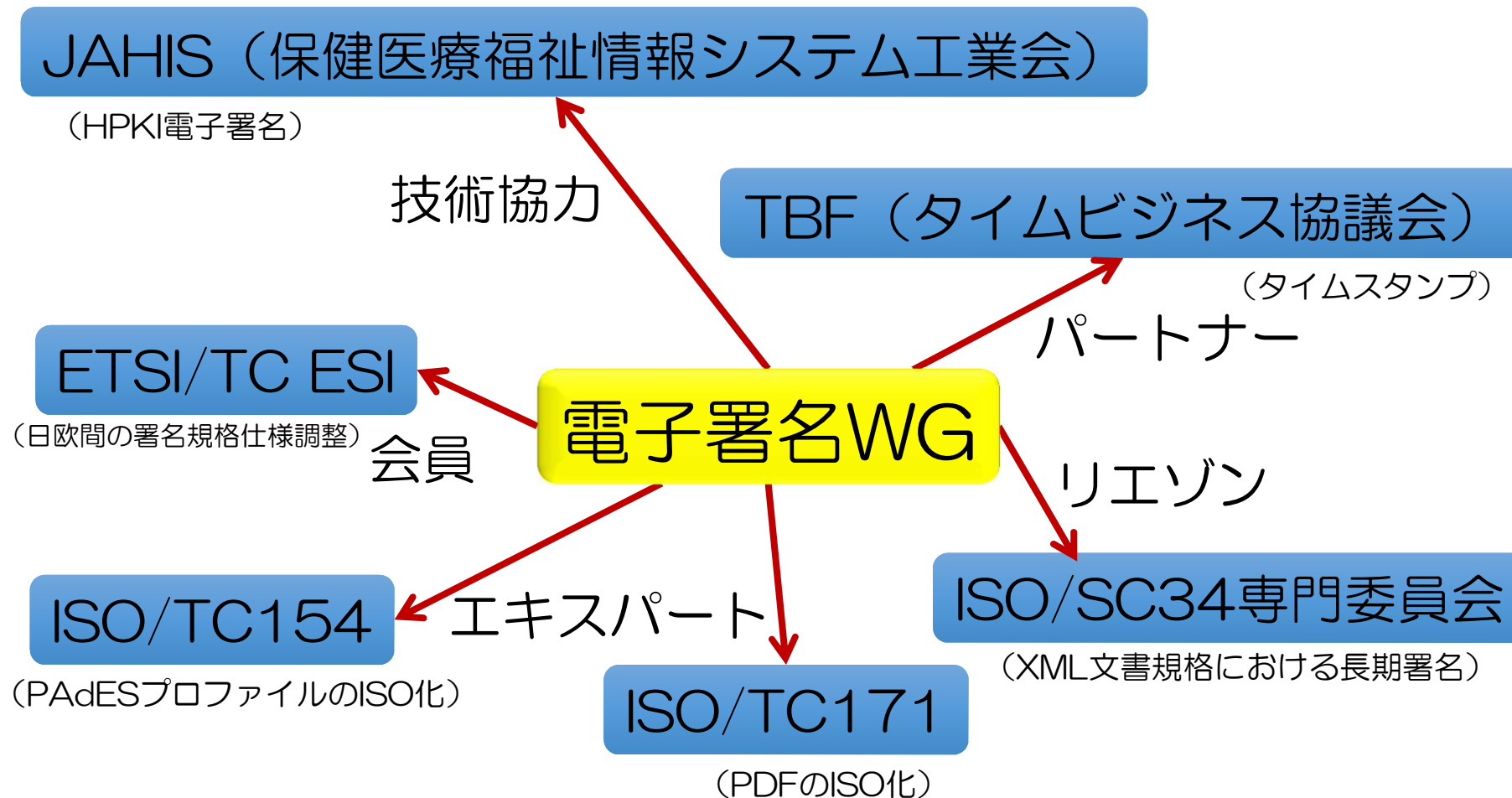
2015年度活動



- テーマ
 - ① PAdESプロファイルに関する標準作成
⇒経産省国際標準化事業
PDF長期署名プロファイルに関する国際標準化
 - ② 署名検証要件に関する標準作成
 - ③ 署名関連の勉強会/情報交換、新規課題発掘
- 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。



他団体との関係



主な活動内容



- **電子署名WG**
諸連絡、関連情報交換、企画運営
- **PAdESプロファイルTF**
経産省**国際標準化**関連事業対応
- **署名検証TF**
署名検証要件の**標準化**検討
- **スキルアップTF**
勉強会、PKI SandBox Project、**普及啓発**、**次期課題発掘**
- **ETSI/TC ESI**
準会員（日欧間の署名規格仕様調整）
- **ISO/TC154**
エキスパート（PAdESプロファイルのISO化）
- **ISO/SC34専門委員会**
リエゾン（XML文書規格における長期署名）
- **講演会**
成果報告会、NSF、PKI Day

2015年度活動実績



- WG/TF (計45回)
 - 電子署名WG：12回 (+臨時3回)
 - 署名検証TF：8回
 - PAdESプロファイルTF：7回 (+電子署名プロファイル国際標準化委員会2回)
 - スキルアップTF：11回 (+臨時2回)
- ETSI
 - 第50回 ETSI/TC ESI会議 (@ドイツ ベルリン)
 - 第55回 ETSI/TC ESI会議 (@スペイン バルセロナ)
- ISO
 - ISO/TC154国際会議 (オンライン)
 - ISO/TC171国際会議 (@スイス バーゼル)
 - ISO/SC34国内専門委員会：7回
- セミナー/講演
 - JNSA 2014年度活動報告会
 - PKIDay 2015
- その他
 - 合宿 (@横浜 あざみ野)
 - 懇親会：2回

2015年度活動実績



	4	5	6	7	8	9	10	11	12	1	2	3
電子署名 WG	▲	▲	▲	▲▲▲	▲	▲	▲	▲	▲	▲	▲▲	▲
								合宿★				
署名検証TF	▲	▲	▲	▲	▲	▲	▲			▲		
PAdES プロフィールTF	▲	▲	▲	▲	▲	▲	▲	▲				
		電子署名プロフィール国際標準化委員会★					電子署名プロフィール国際標準化委員会★					
スキルアッ プTF	▲	▲	▲▲	▲	▲▲	▲	▲	▲	▲	▲	▲	
講演会	▲		▲									
	PKIDay2015		JNSA 2014年度活動報告会									
国際会議		▲					▲	▲				▲
	ETSI/ESI#50					ISO/TC154	ISO/TC171			ETSI/ESI#55		
ISO/SC34 リエゾン		▲		▲	▲		▲		▲		▲	▲

① PAdESプロファイルに関する標準化

- 経済産業省「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」を受託。2014年度から3カ年計画の2年目
- ISO/TC154にてISO14533-3として標準化を推進し、ステージ30.20（CD投票開始）へ。
- ISO/TC 171 SC2 PDF専門家会議にPAdESプロファイルをインプット。

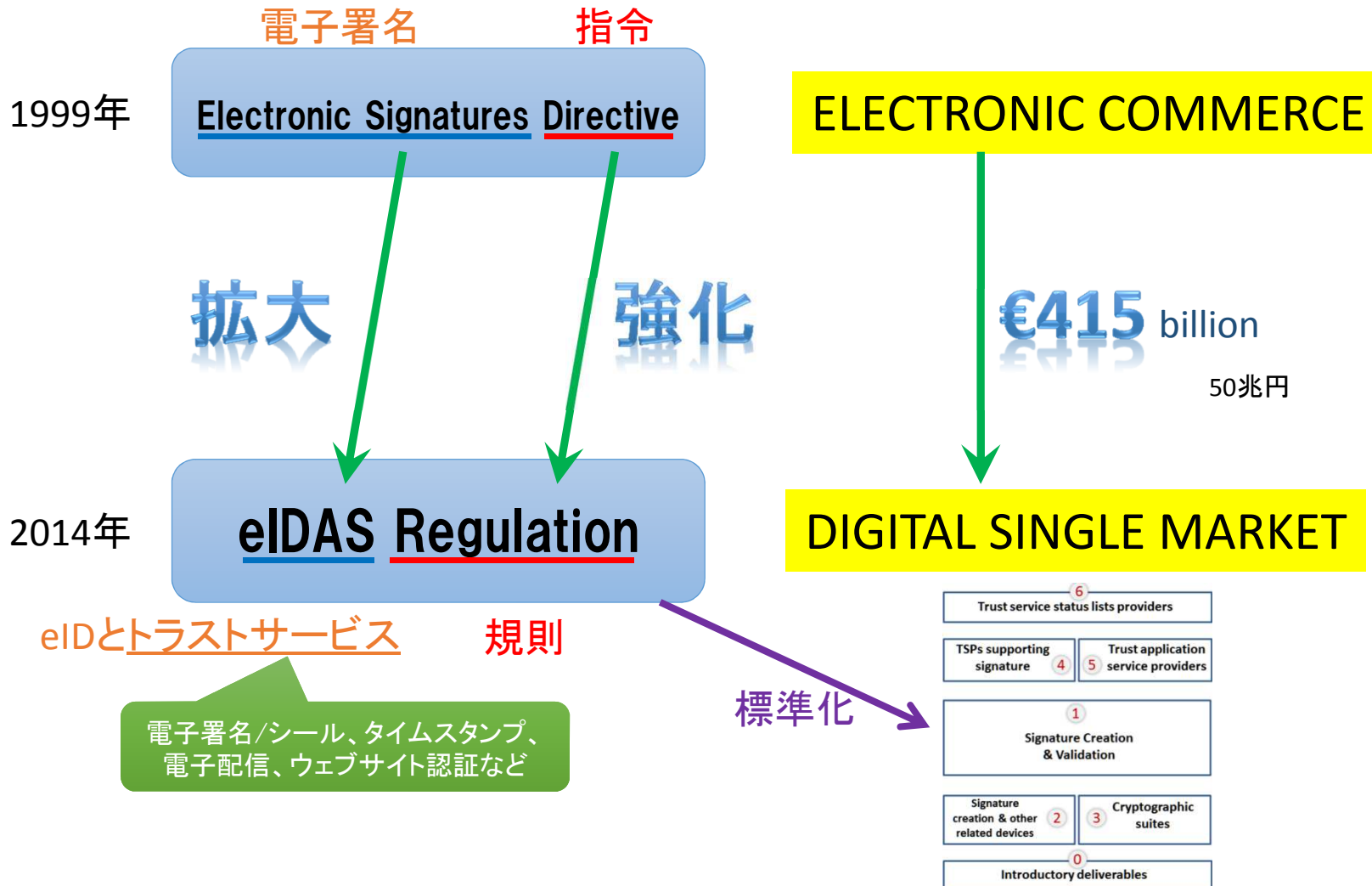
② 署名検証要件に関する標準化

- 長期署名プロファイル対応の検証規格としてISO化を目指すという方針のもと、PAdESプロファイル対応の仕様案を作成。

③ 署名関連の勉強会

- HSM、CT、エストニアICカード、などなど多数の勉強会
- （2016年度ではあるが）5月23日に電子署名WG五月祭を実施。参加者多数、盛況。

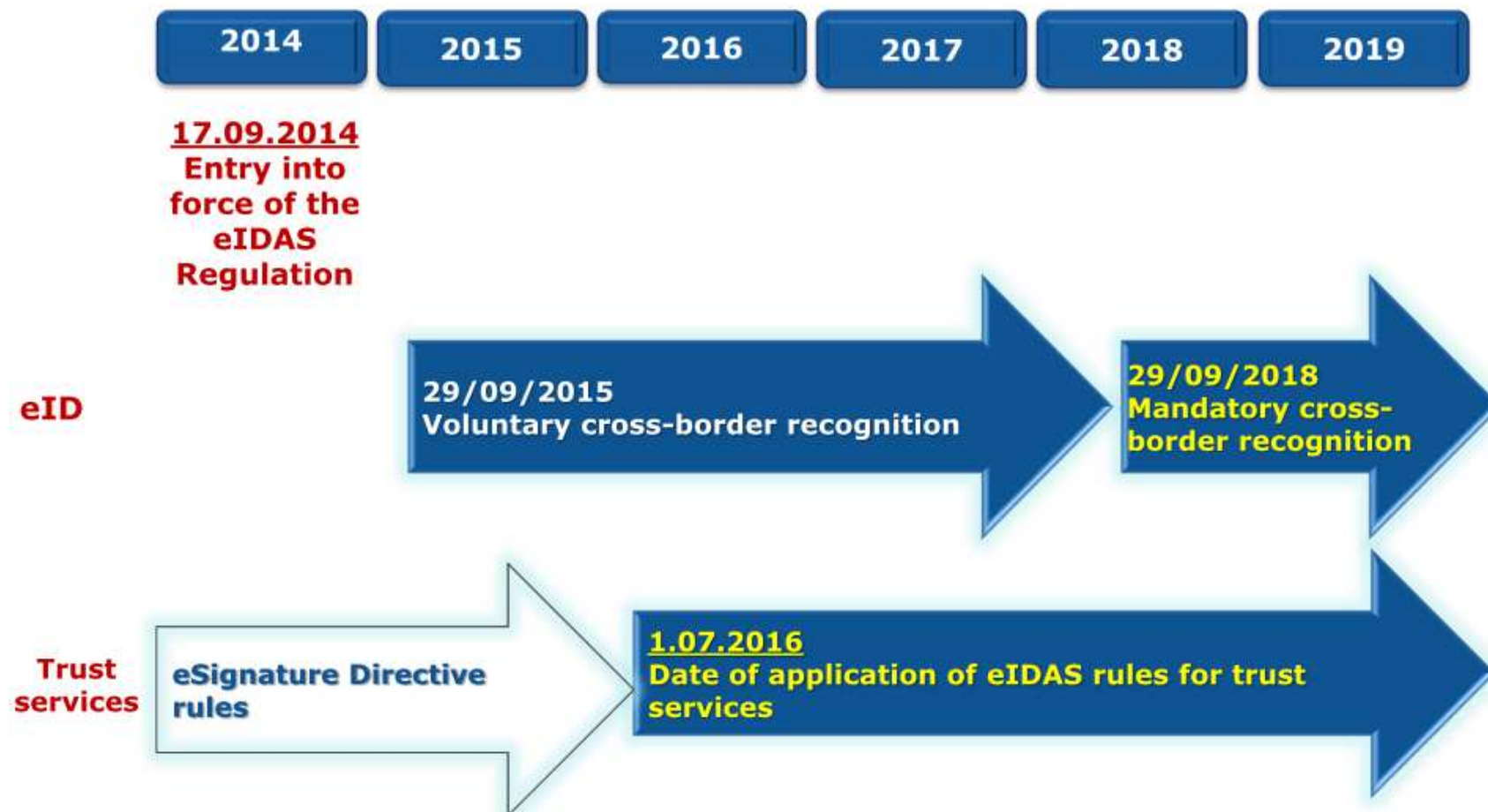
標準化と欧州の動向



eIDASのタイムライン

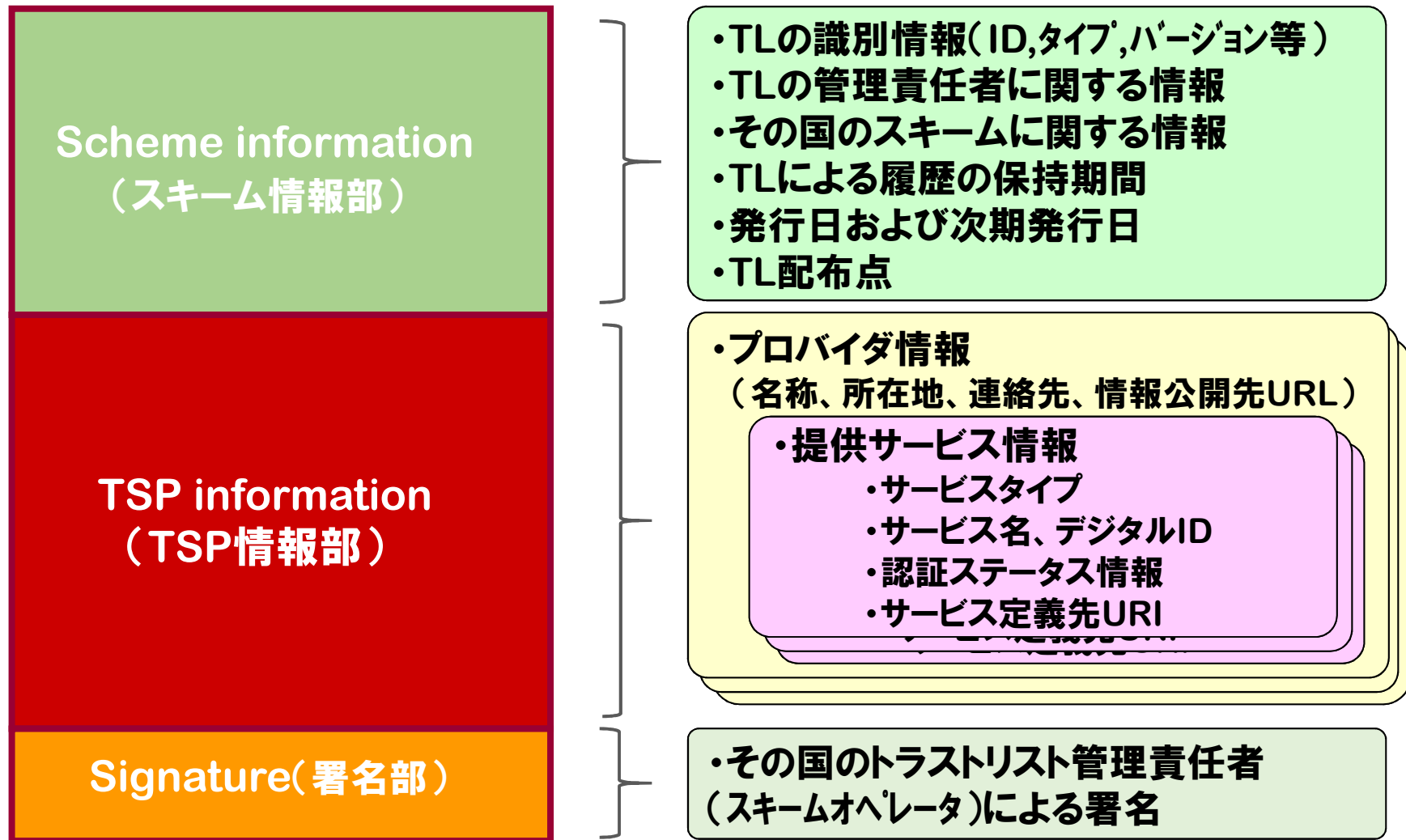


Timeline



出典: TSP Compliance Info-Day (2015.12.15)

トラストリスト



トラストリストの全体構成



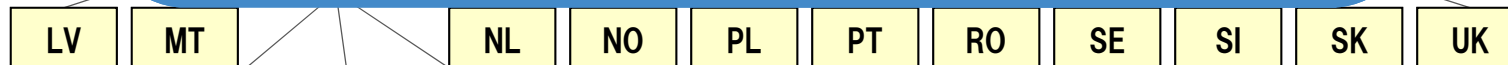
●リストオブトラストリスト(LOTL)

- ・各国のトラストリストへのポインタおよび識別情報(トラストリストへの署名証明書)が記載されたトラストリストの上位リスト

公的機関が最終的なトラストアンカ
とならずに、誰が信用するのか？

ドイツ連邦ネットワーク庁
Jurgen Schwemmer氏

各国TL



TSPs



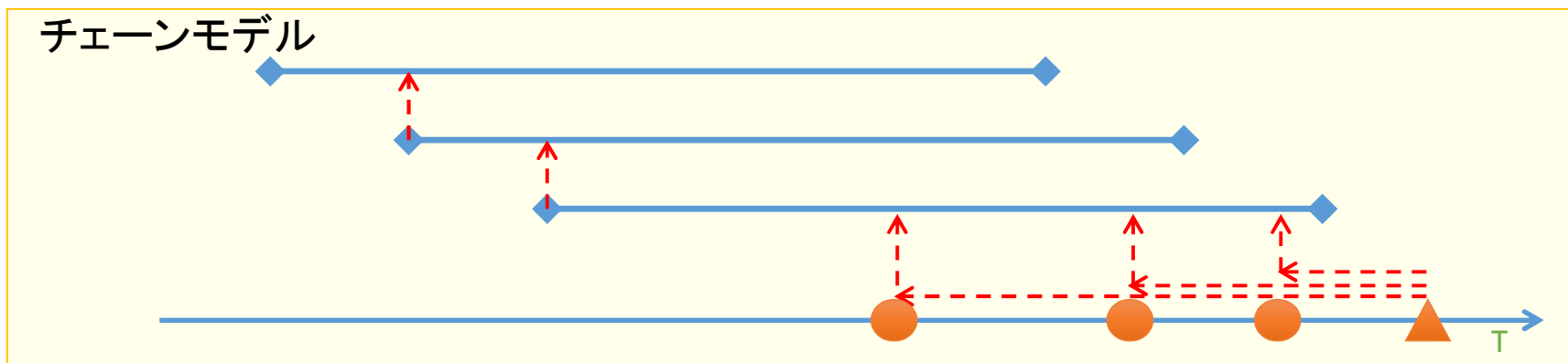
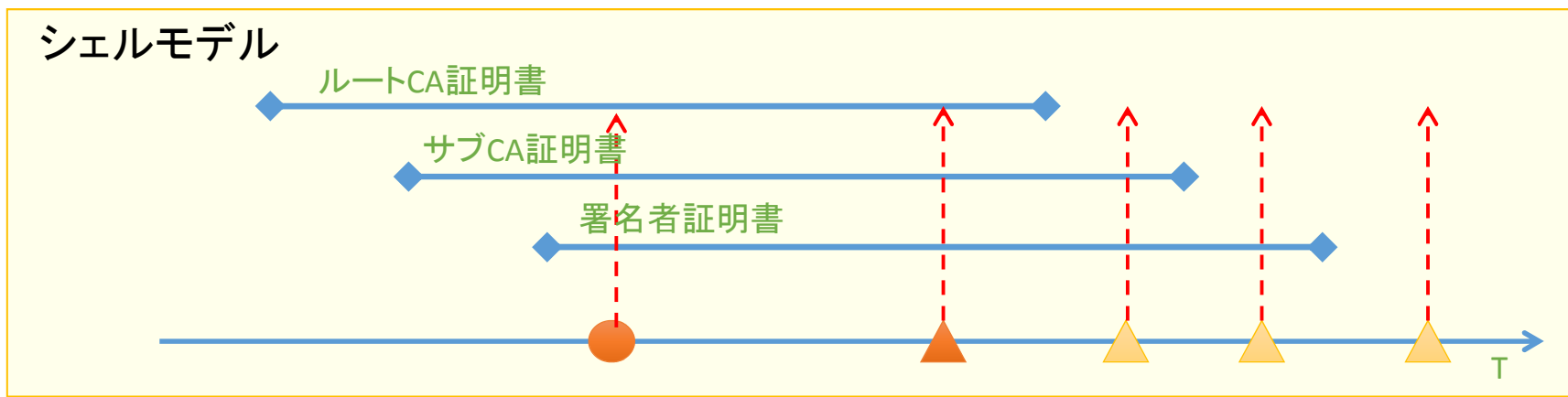
ハッシュ値

署名のハッシュ値

証明書

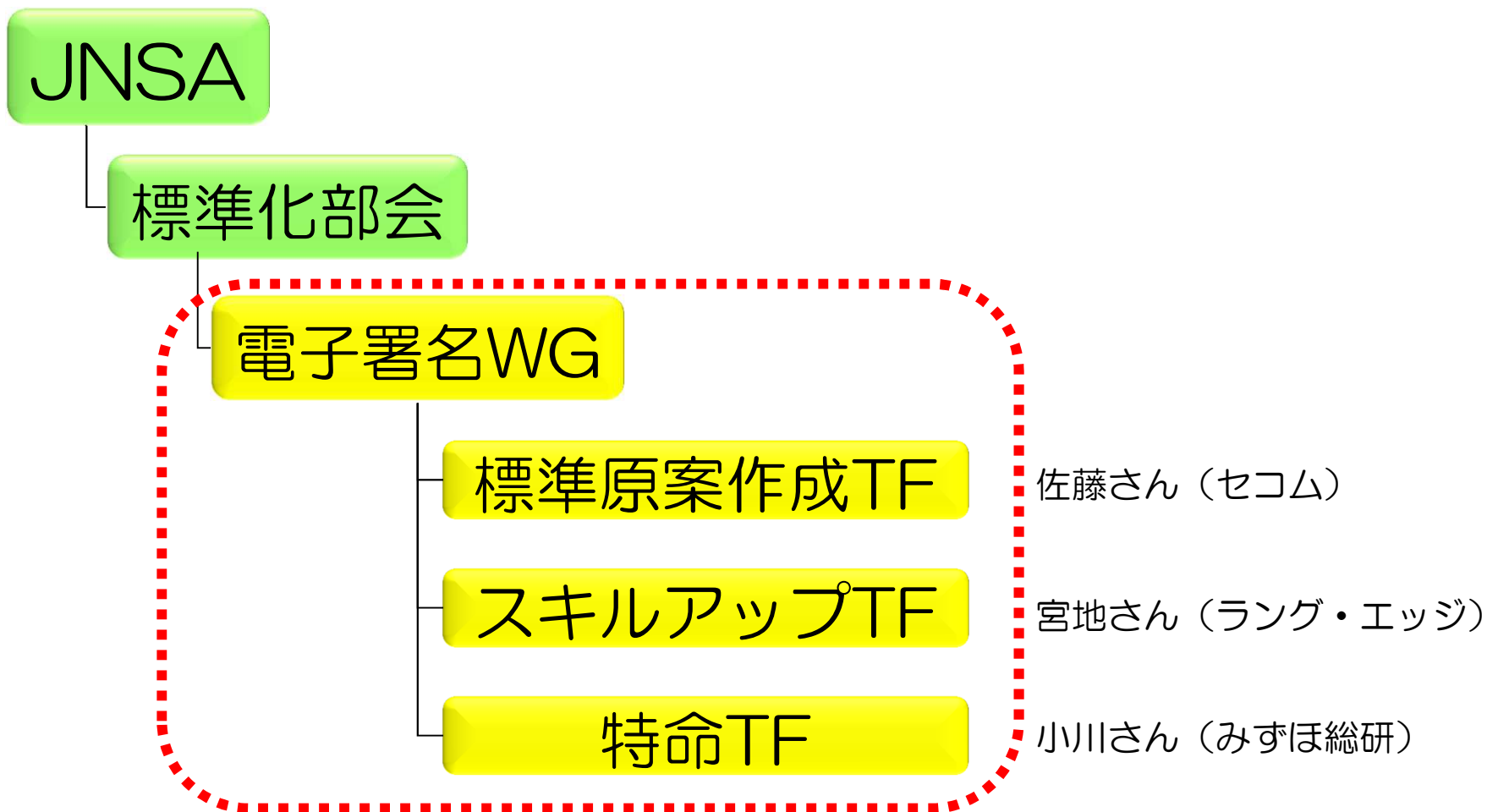
- 欧州のServer Signingへの取組は本気⇒ Qレベル（『適格』）
- DocuSignがOpenTrustのPKI部門を買収 ⇒ PKIサーバ署名？
イタリア、ポーランド、エジプト等
- 独のQCCの署名検証はチェーンモデル、
その他はシェルモデル ⇒ eIDASでは？

署名の検証モデル



今後の電子署名WG

新体制



今後の課題



- 標準化は着実に
 - PAdESプロファイル、署名検証
- 国内外の最新動向を視野に
 - トラストリスト、リモート署名・サーバ署名・モバイル署名、署名検証モデルなどeIDAS関連
 - 米国のオンライン署名、IoTにおける署名、ブロックチェーン
- 一段高い視点から
 - 電子的な『トラスト』、『コミット』、『証拠』の在り方
 - 普及啓発⇒『教育・育成』

人材育成/普及啓蒙/情報公開/技術公開
公開サーバー <http://eswg.jnsa.org/>

- 電子署名を扱える技術者の育成と拡大
新メンバー/若手にレベルアップのチャンスを!
入門者・初心者歓迎です! 是非新規ご参加を!
- 電子署名を利用する為の情報を公開
技術者が実際に動かして試せる環境を整備!
3年間の活動成果をポータルとして公開予定!

スキルアップTF 技術者の育成

1. 公開勉強会開催 (電子署名WG祭イベント)

誰でも参加可能で半年毎に定期開催を予定

若手/新メンバー中心に発表 (勉強になります!)

第1回の電子署名WG五月祭は5月23日に開催!

56名の参加を頂き盛況のうちに終了しました!

資料公開中 <http://eswg.jnsa.org/matsuri/>

次回は秋(10月か11月頃)に祭開催を予定!

2. 内部勉強会開催 (毎月可能なら開催中)

電子署名WGメンバーのみ参加可能な勉強会

今月開催 「eIDAS規則とリモート署名の現状について」

1. 電子署名ポータル (今年度中に公開を予定)

3年間の電子署名WG活動成果をまとめる

ドキュメント類は既に蓄積済み (メンバーサイト内)

2. PKI SandBox ProjeT (PKIの遊び場提供)

サイト公開中 <http://eswg.jnsa.org/sandbox/>

ハンズオン資料も公開しているので自習も可能

オープンソース化活動 (PKI SandBox で公開)

✓ FreeTSA : 誰でも使える試験用タイムスタンプを公開

✓ FreeXAdES : Java用フリーな**XAdES**実装を開発中

公開 <https://github.com/miyachi/FreeXAdES>

注 : まだ開発中の為に現在XAdES-BESまでの生成です。

電子署名WG会員募集



電子署名WGに登録を希望する方は下記にご連絡
ください。

NPO 日本ネットワークセキュリティ協会
事務局宛

<E-Mail>office@jnsa.org

※件名を「電子署名WG登録希望」としてください。

※参加を希望するTFとMLに登録するメールアドレスを
お知らせください。

電子署名WG会員募集



電子署名WG
ください

NPO 日本
ネットワーク
セキュリティ
<E-Mail>

参加のメリット

人脈形成
先行者利益
スキルアップ

するTFとMLに登録する
お知らせください。



ご清聴ありがとうございました。

