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

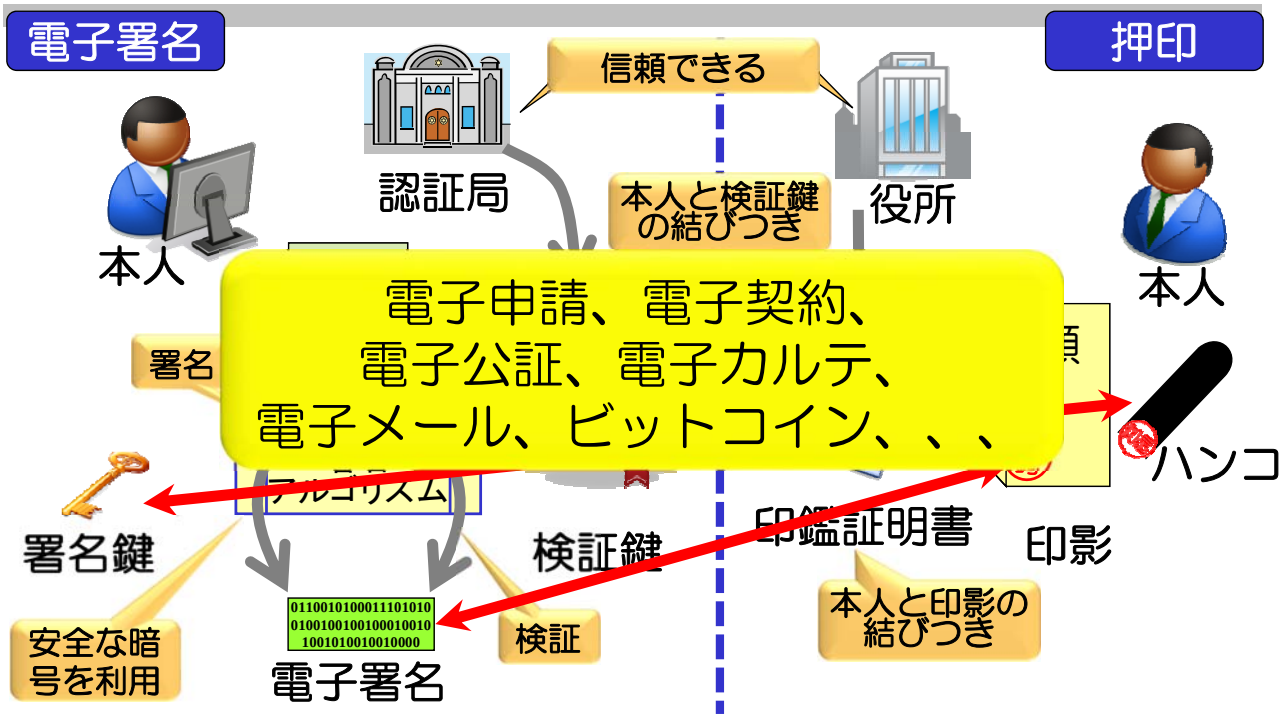
JNSA　2014年度活動報告会

2014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）

2015 年6月9日（火）　秋葉原UDX

電子署名とは

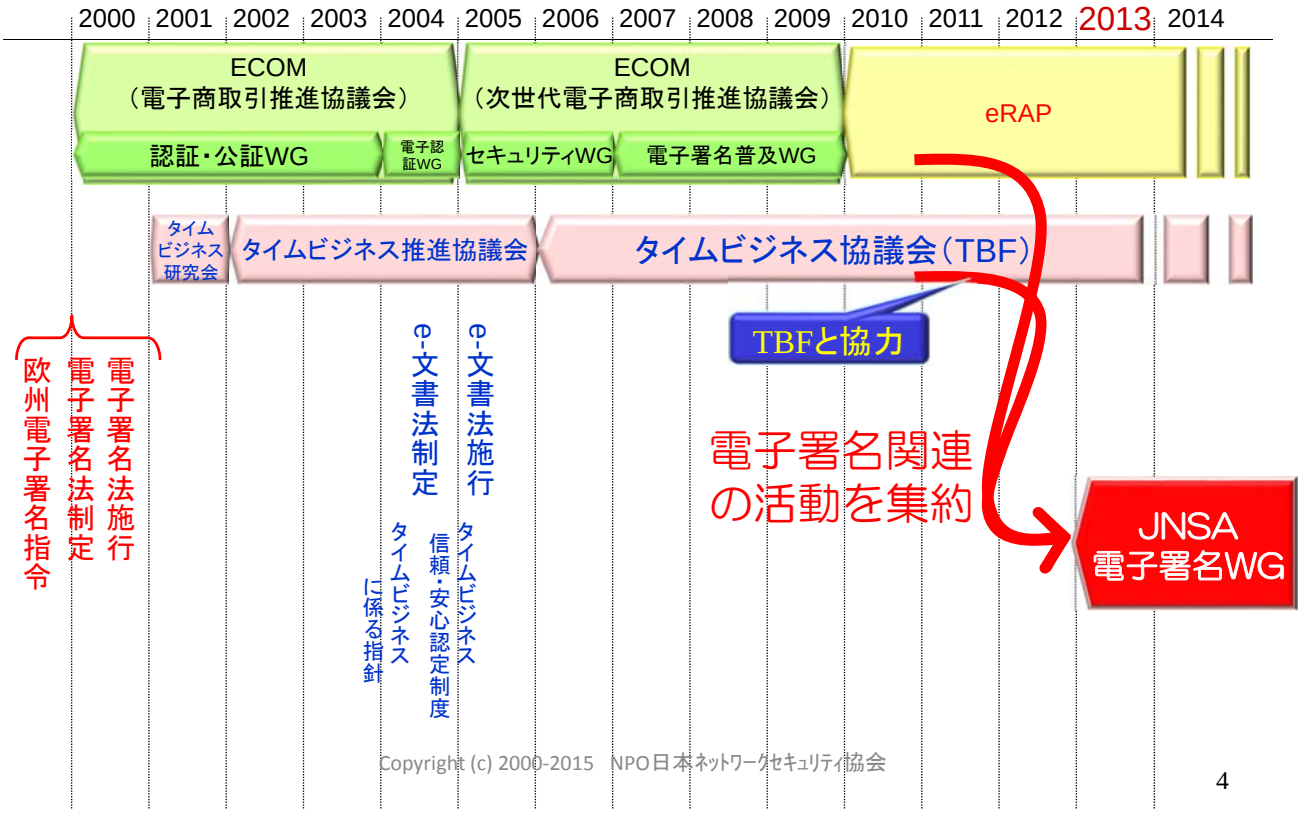


電子署名は、署名者が誰であるかに加え、電子文書が改ざんされていないことも確認できる技術。電子文書に「トラスト」を与える。

報告内容

- 電子署名WG
  - 設立経緯、活動目的、体制、主な活動
- 2014年度活動計画・目標・実績
- 2014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
- 欧州の動向
- 今後の電子署名WG

2013年度：電子署名WG設立



活動目的

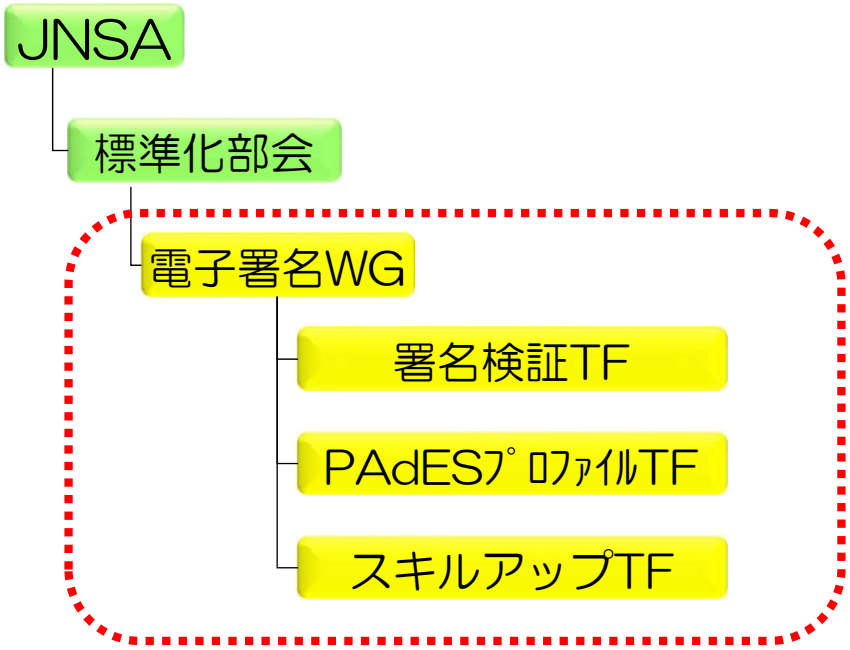
- 電子署名の相互運用性確保のための調査、検討、仕様提案、相互運用性テスト、及び電子署名普及啓発を行う。

⇒ 電子署名の総合拠点

2014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、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回を計画。

体制



主な活動内容

- 電子署名WG
  諸連絡、関連情報交換、企画運営
- 署名検証TF
  署名検証要件の標準化検討
- PAdESプロファイルTF
  経産省国際標準化関連事業対応
- 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

2014年度成果目標

2013年度目論見との関係

① 署名検証要件に関する標準化

- 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（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）

② PAdESプロファイルに関する標準化

- JSA（一般財団法人日本規格協会）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。

⇒ 経産省「平成２６年度戦略的国際標準化加速事業」受託し、TC154にてISO14533 - 3として標準化する。

③ 署名関連の勉強会

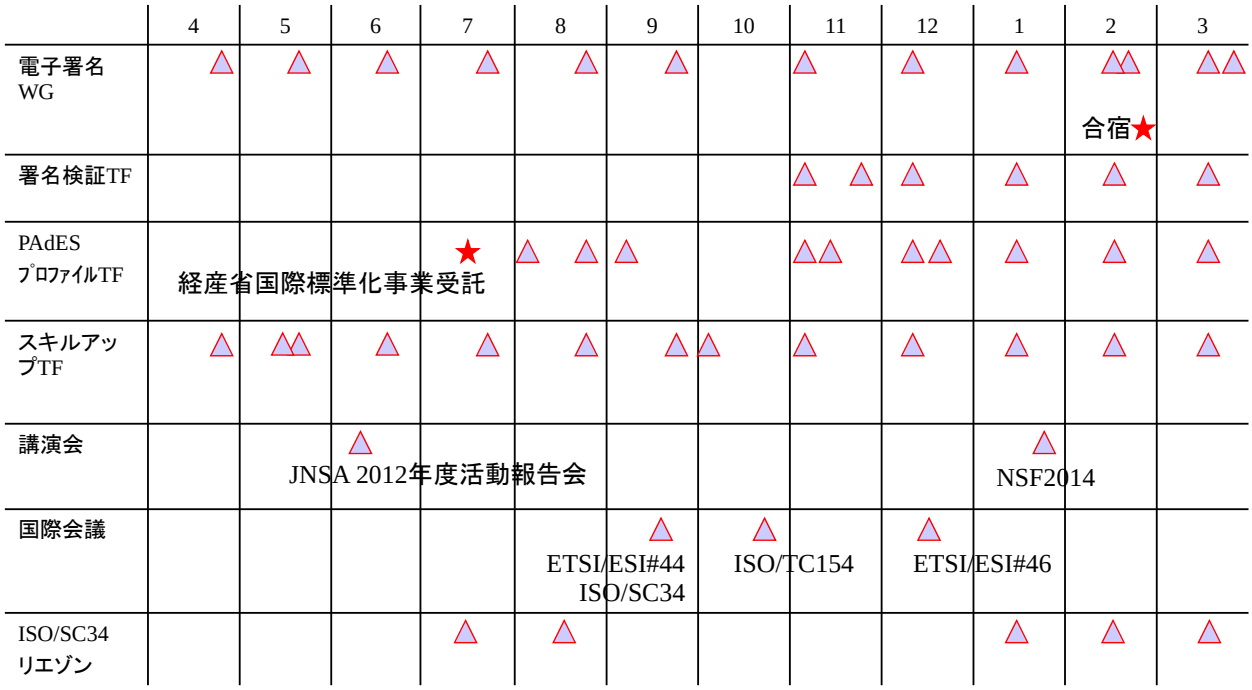
- オープンソースプロジェクト （FreeTSAなど）

⇒ PKI SandBox Project

2014年度活動実績

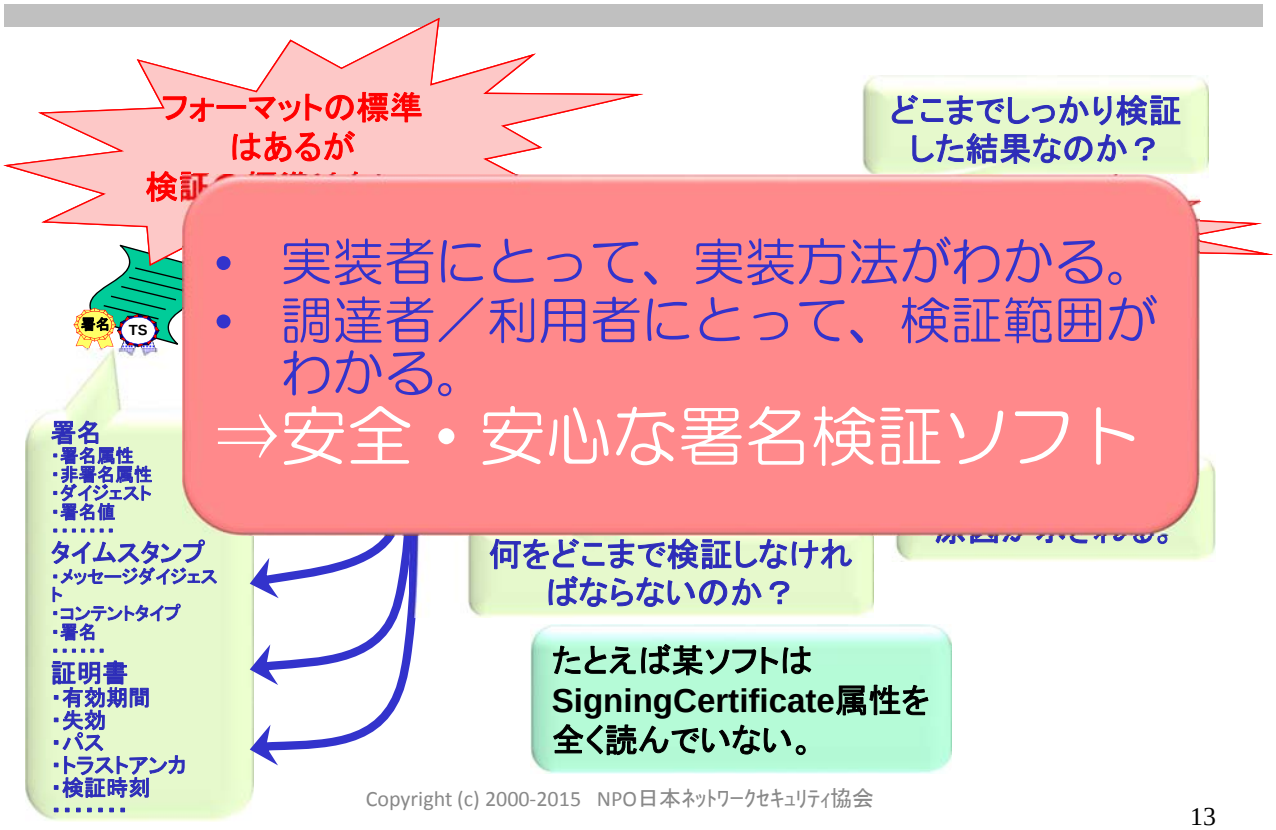
- WG／TF（計43回）
  - 電子署名WG：11回（＋臨時2回）
  - 署名検証TF：6回
  - PAdESプロファイルTF：10回
  - スキルアップTF：11回（＋ハンズオン1回、臨時2回）
- ETSI
  - 第44回 ETSI/TC ESI会議（@スペイン マドリード）
  - 第46回 ETSI/TC ESI会議（@フランス ソフィアアンティポリス）
- ISO
  - ISO/TC154国際会議（@韓国 仁川）
  - ISO/SC34国際会議（@京都）
  - ISO/SC34国内専門委員会：5回
- セミナー／講演
  - JNSA 2013年度活動報告会
  - Network Security Forum 2015
- その他
  - JNSAリレーコラム（第57号～第60号）
  - 合宿（@上総一ノ宮）
  - ビットコイン勉強会
  - 懇親会：2回

2014年度活動実績



署名検証TF

署名検証の問題点



- 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

仕様ドラフト間の相違

ETSI	JNSA
実装方	
プロセ	ーブ
出力メ	未定義
POE （何らか	

ETSIはETSI仕様に固執、変更の意思なし。
電子署名WGとしては、仕様の位置づけを変更（長期署名プロファイルの検証要件）し、ISO化に向けた検討を続ける。

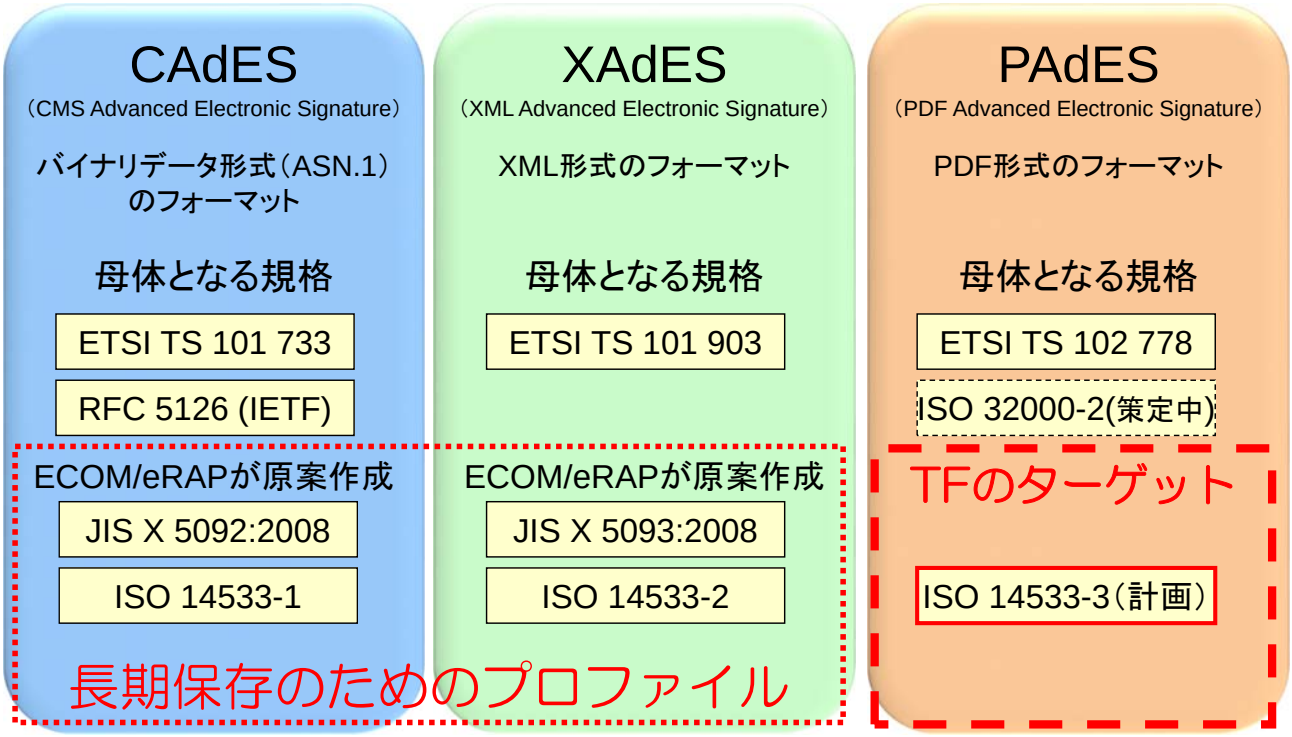
Timestampに関する記述が足りない
コントロールタイムやフレッシュネスの概念が分かりにくい

PAdESプロファイルTF

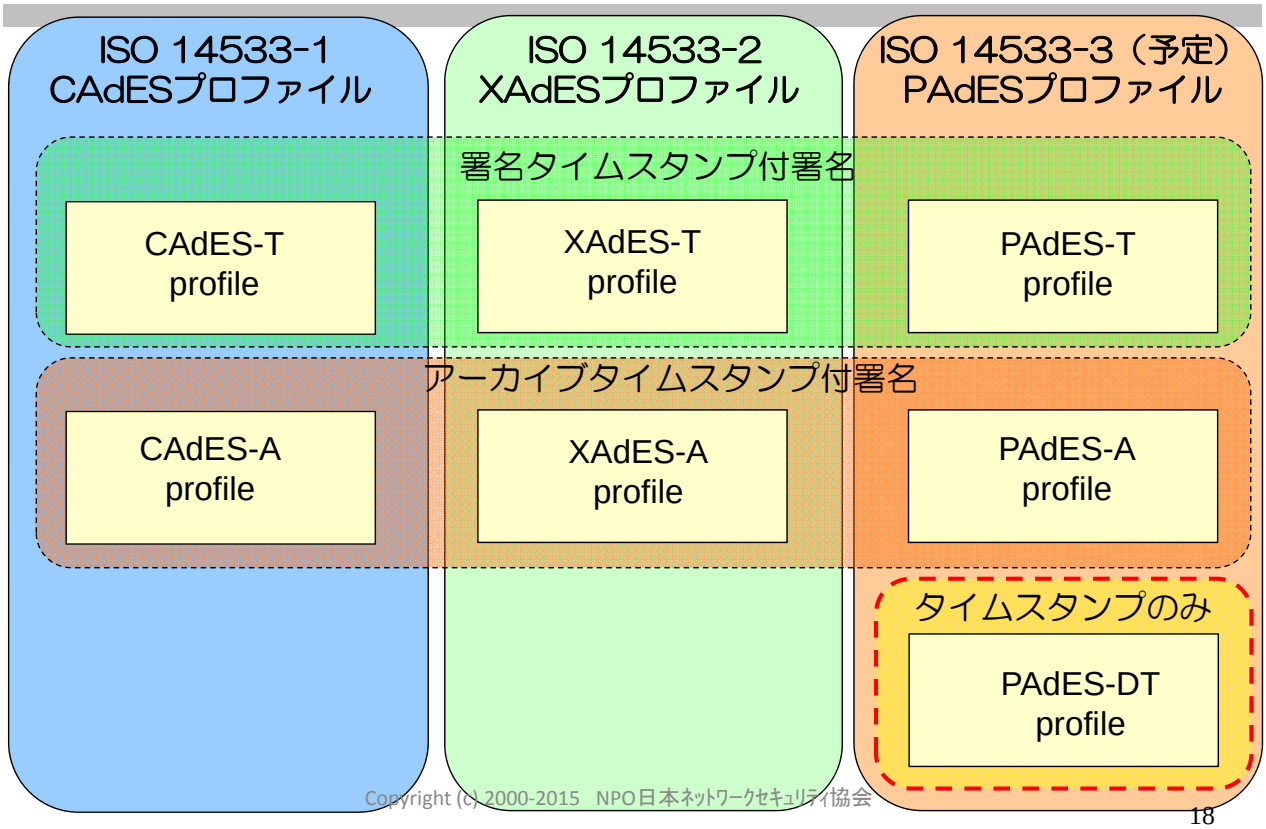
PAdESプロファイルとは

- 電子署名プロファイル規格：
  電子署名の相互運用性を確保し、長期に保存可能にするために必要な要件（パラメータの取捨選択など）を定めたもの。
- PAdESプロファイル規格：
  ETSIでベース規格が策定され、ISOで策定中のPDF規格（ISO 32000-2）に取り入れられるPDF電子署名のプロファイル。

PAdESプロファイルの位置付け



長期署名保存のためのプロファイルの構造



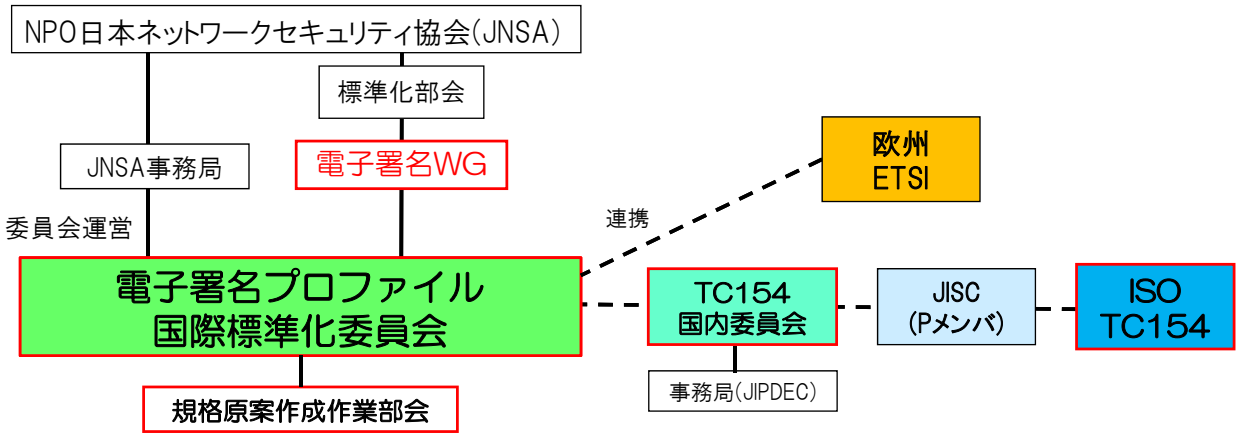
日本から提案する意義

- 電子署名プロファイルのISO規格は日本がコントロールしている。
  - ISO 14533 Part1/Part2の提案と原案作成は日本が行った。
  - 電子署名の長期保存に関する運用実績は日本が先行している。
- タイムスタンプ単独での運用（ETSIは無関心）についても日本が主導したい。
  - 知的財産の保護などでタイムスタンプ単独での運用が有用。

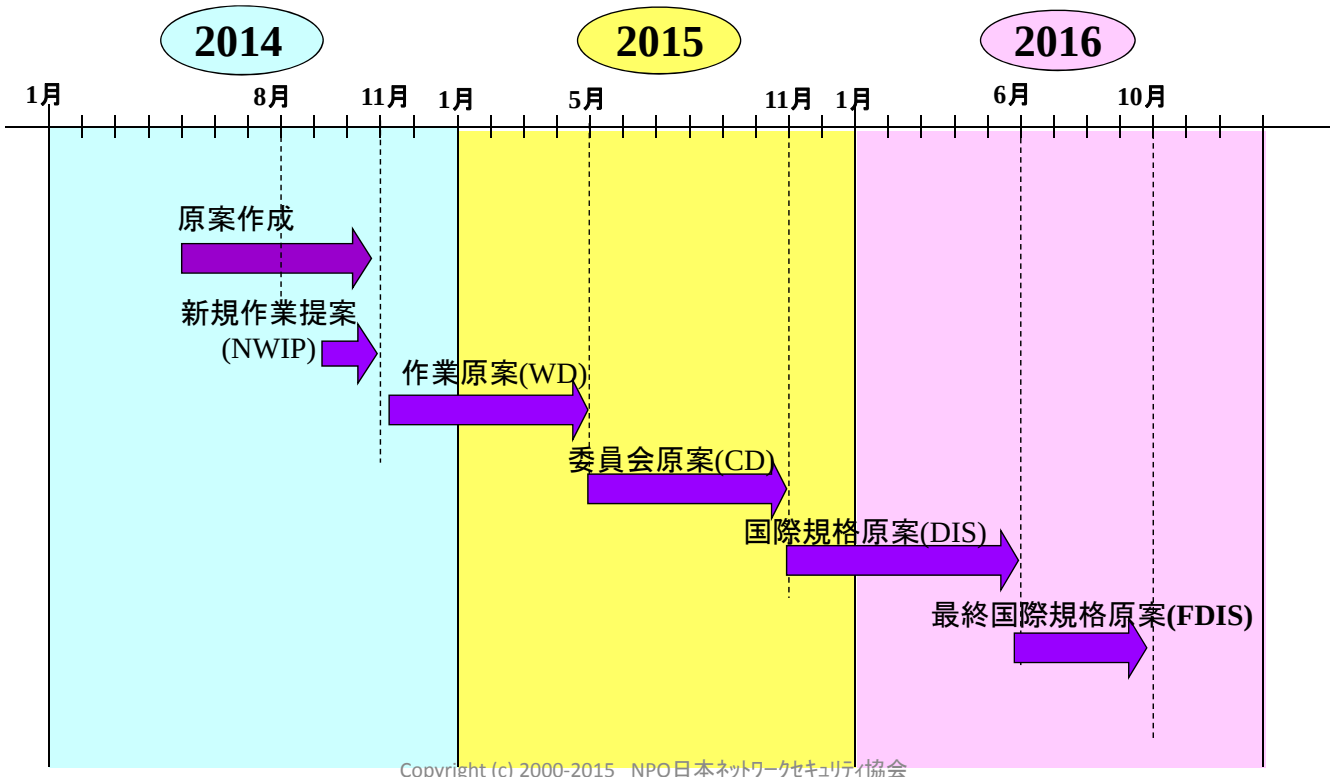
経産省国際標準化事業を受託

- 2014年度より３ヵ年にわたる経産省事業「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（テーマ名：ＰＤＦ長期署名プロファイルに関する国際標準化）」を受託。

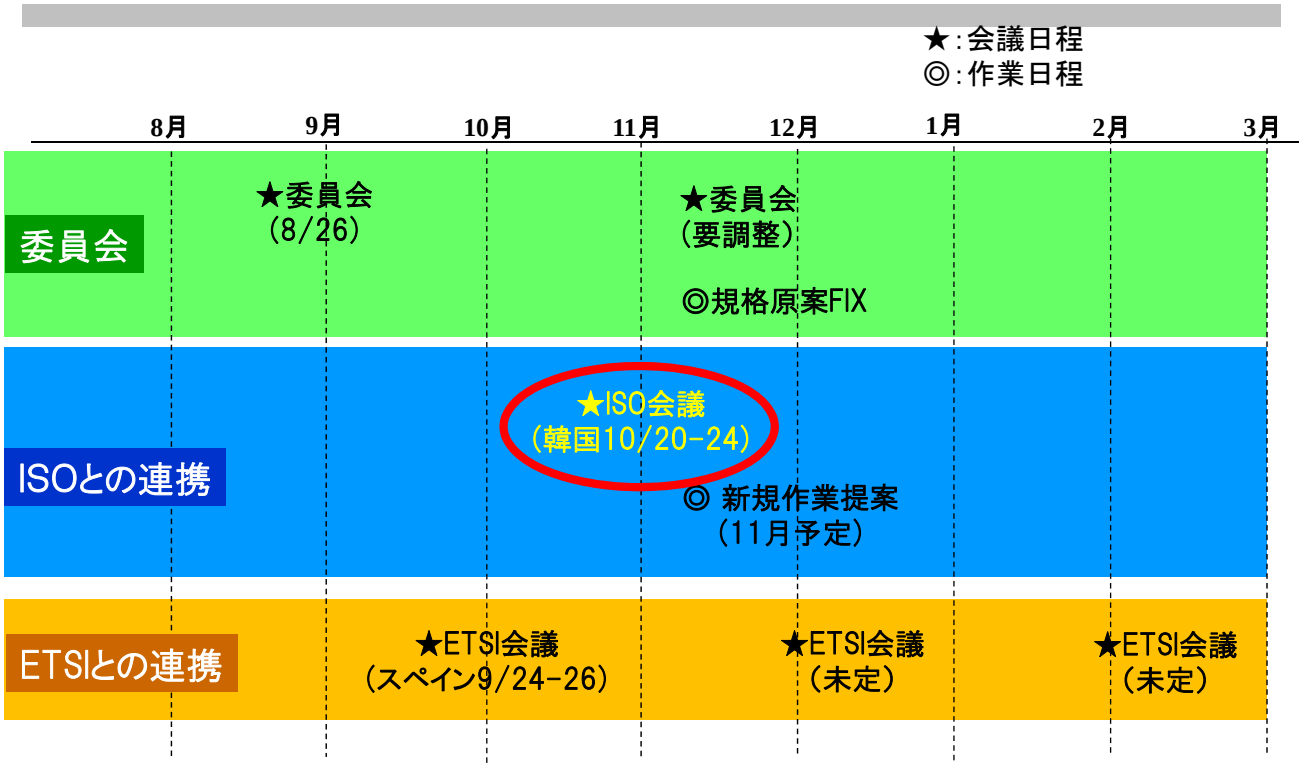
委員会の体制



全体スケジュール（３ヵ年）



２０１４年度スケジュール



ISO/TC 154国際会議

- ISO TC154国際会議
  - 日程：10月20日(月)～24日(金)
  - 場所：韓国（仁川）
- 日本からの発表
  - ISO 14533-3 (PAdESプロファイル)の新規提案
    - 電子署名の課題と長期署名プロファイルの必要性
    - PAdES規格の背景と課題、PAdESプロファイルの必要性／内容
- ETSI/ESIのPeter Rybar氏(スロバキア)が電話会議参加

プレナリー会議での議決

- ISO 14533-3(PAdESプロファイル)はWG6 (Trusted eCommunications)を新設し、
- NWI[illegible]ト)のダブ[illegible]
  ※ W[illegible]スキップされるので策定が早まると期待できる。
- 日本の他、スロバキア、ドイツ、韓国、中国等が参加。

順調に推移。経産省事業を継続し、ISO対応作業を実施。

スキルアップTF

スキルアップTF 2014年度実績

6月26日 :欧州クラウド署名Comfact社プレゼン
9月29日 :IT製品の調達におけるセキュリティ要件リストに関する認定制度の勉強会 ※1
9月30日 :SMS認証製品プレゼン ガプスモバイル社
OpenSSL/LibreSSL勉強会（※ PKI相互運用WGとの共催）
10月2日 :ドイツ署名ビジネス状況の紹介 OpenLimit社 ※1
11月5日 / 12月9日: 電子署名ハンズオン試行（前編/後編）
12月18日:USENIX LISA14 報告会（※ PKI相互運用WGとの共催）
1月15日 :Office Open XML勉強会
2月15日 :PDF/A勉強会
3月14日 :一般向け 電子署名ハンズオン実施（※ AITCとの共催）
3月19日 :トラストリスト解説

※1 JIPDECあんしんかんカフェとの共催

電子署名ハンズオン 概要

主催:JNSA勉強会 / AITCオープンラボ
日時:2015年3月14日(土) 13:30～18:30
参加:[illegible]可）
目的:
一般[illegible]基本
を分[illegible]署名
利用の普及啓蒙活動として利用者の拡大を目指す。

アンケート回答者27名中、
26名の「満足」が得られた。

参加者:

事前申込数	35名	
参加者数	35名	(当日不参加:3名、当日参加:3名)
懇親会	19名	

スキルアップTF 2015年度の活動

- 勉強会・ハンズオン
  - 2014年度に続き会員向け勉強会を定期開催
  - 他WGや団体との共催も積極的に増やす
  - 一般向けの勉強会やハンズオンも開催したい
- 電子署名WGサーバ運用（PKI SandBox Project）
  - 電子署名ハンズオンの資料を公開中（自習可能）
  - 成果を PKI SandBox Project として拡充して行く
  - 協賛ベンダーのソフトウェアの組み込みを予定
  - オープンソースのライブラリ開発と公開（可能なら）

PKI SandBox Project

http://eswg.jnsa.org/sandbox/

電子署名・タイムスタンプの技術を普及促進する為に誰でも自由に使えるPKIの遊び場を作るプロジェクトです！現在は以下を公開！

FreeTSA Project

試験用に使えるRFC 3161タイムスタンプサービス
※ ハンズオン資料を見て実際に試せます。

試験用の証明書発行やTSA証明書用の試験認証局
※ハンズオン資料を見て実際に署名を試せます。

SandBox CA

ESig-PKI HandsOn

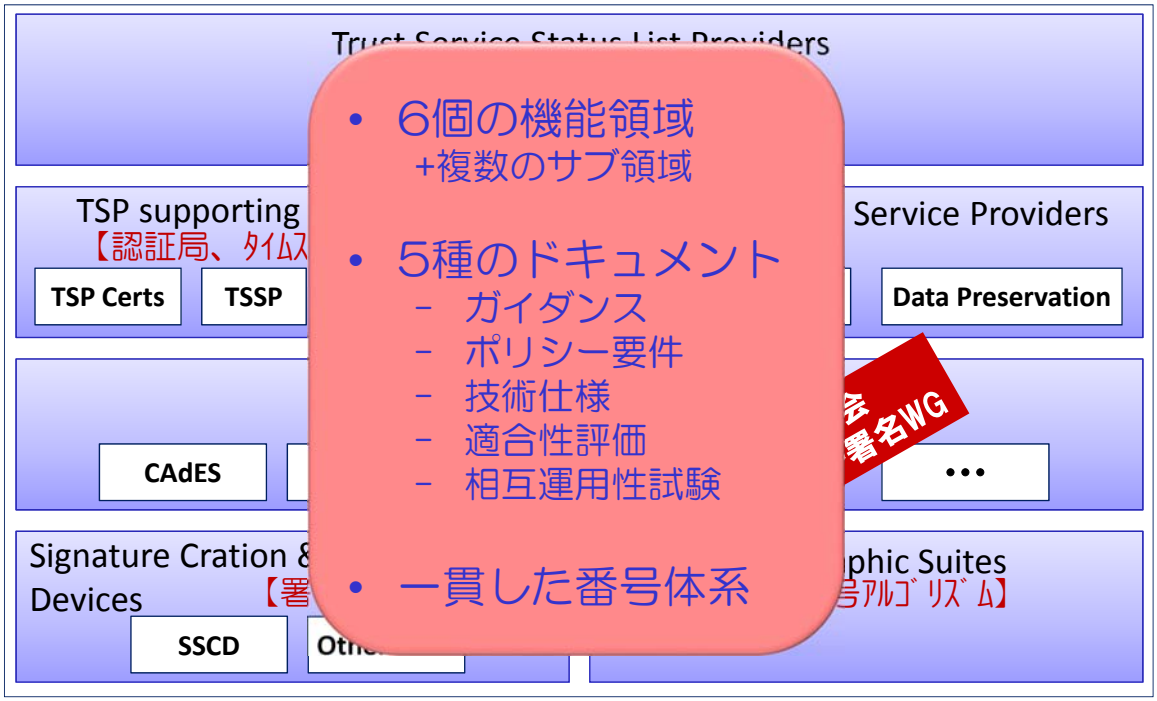
PKI SandBox の環境を使った勉強会と資料の公開
※ 100ページ以上の技術情報とハンズオンとして
署名・タイムスタンプ・長期署名を試すことが可能。

欧州の動向
-eIDAS規則の制定とトラストリスト-

eIDAS規則

- eIDAS（Electronic identification and trust services）規則
- EU電子署名指令（Directive 1999/93/EC）に替わる、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（Regulation(EU) No 910/2014）。
- 電子認証やトラストサービスを普及し、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。
- トラストサービスとは「電子取引の安心と信頼を強化する電子サービスの総称」。

新フレームワークでの技術標準整備



ETSI , CEN, ETSI SR 001 604「Rationalised Framework for Electronic Signature Standardisation」より

トラストリスト

- 国毎にトラストリスト（TSL：Trust-service Status List）を発行
  ⇒CA、TSA等のトラストサービスの信頼性を各国間でレベル合わせ
- 米マイクロソフト、アドビとも協調

日本版トラストリストは？

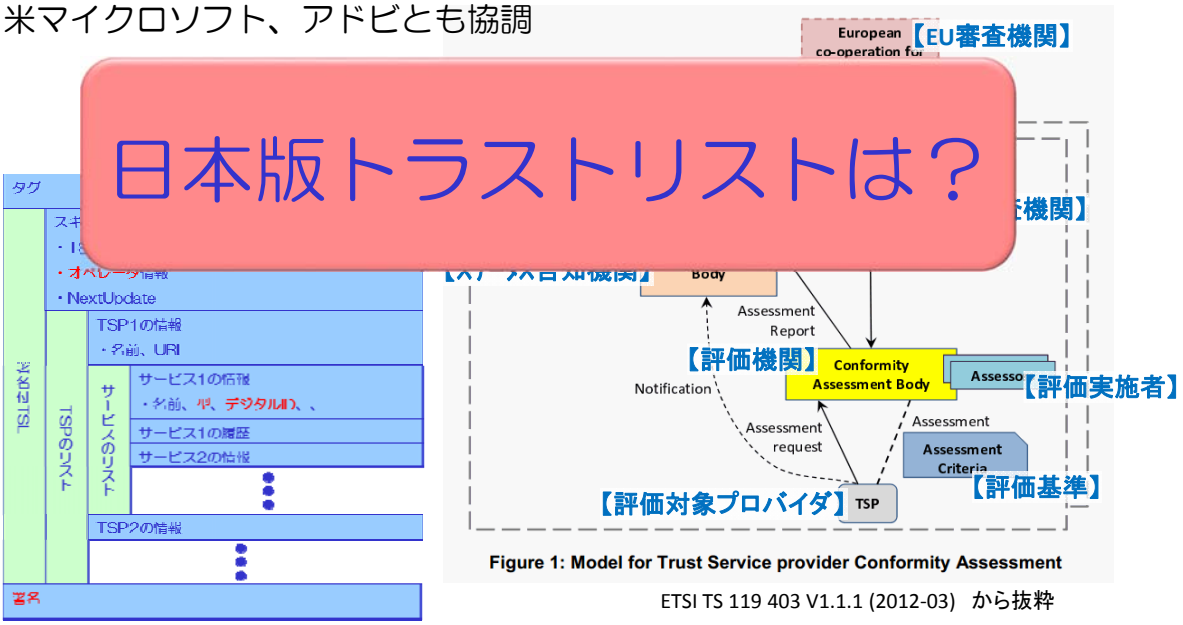


Figure 1: Model for Trust Service provider Conformity Assessment

ETSI TS 119 403 V1.1.1 (2012-03)　から抜粋

今後の電子署名WG

［これまで］
電子署名の専門家集団として課題に取組んできた。
［今後］
上記に加え、新たな市場の創造/先導を目指したい。
［そのために］

- 電子署名の定義を見直すことも。
  ⇒トラストセキュリティ、電子エビデンスなど
- 市場分析も可能な範囲で行い、市場目線の活動も。
- サーバ/クライアントからクラウド/モバイル(IoT含)の時代への適応も視野に。

皆さん、一緒に検討しませんか？

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。（現在の登録者数：約40名）

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。
※MLに登録するメールアドレスをお知らせください。