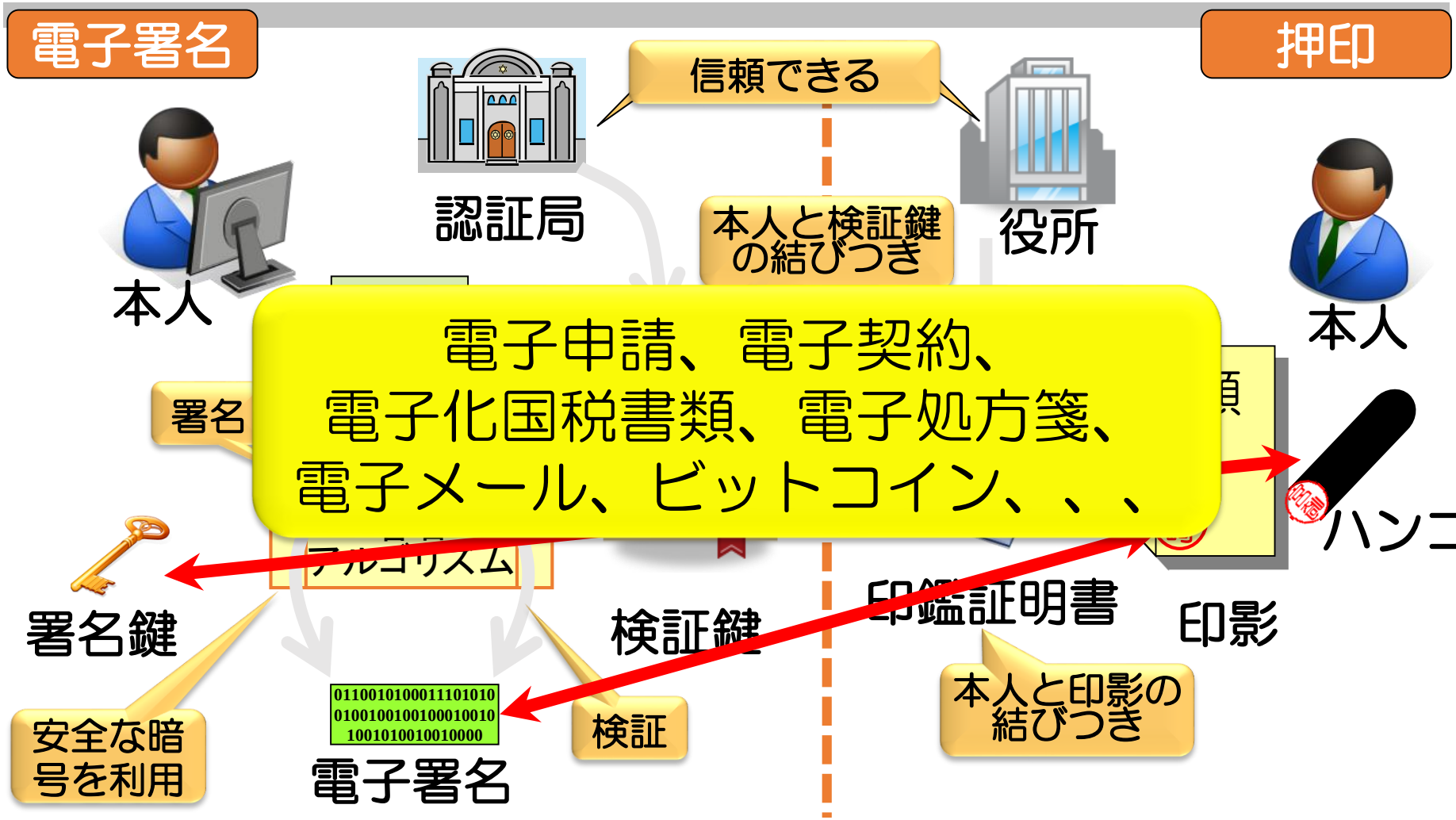
JNSA　2016年度活動報告会

2016年度 電子署名WG成果報告

電子署名WGリーダー
宮崎　一哉

2017年6月12日（月）　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。

電子署名WGの対象領域

電子サイン

ビットコイン

公開鍵暗号

PKI

電子署名

電子印鑑

デジタル署

SSL/TLS

電子署名法が定義する電子署名

EchoSign, DocuSign, HelloSign, RightSignature, CudaSign, SignEasy, Adobe Sign. . .

Advanced Electronic Signature

Qualified ES

エンティティ認証

要するにポイントは

否認防止

約束

コミットメント

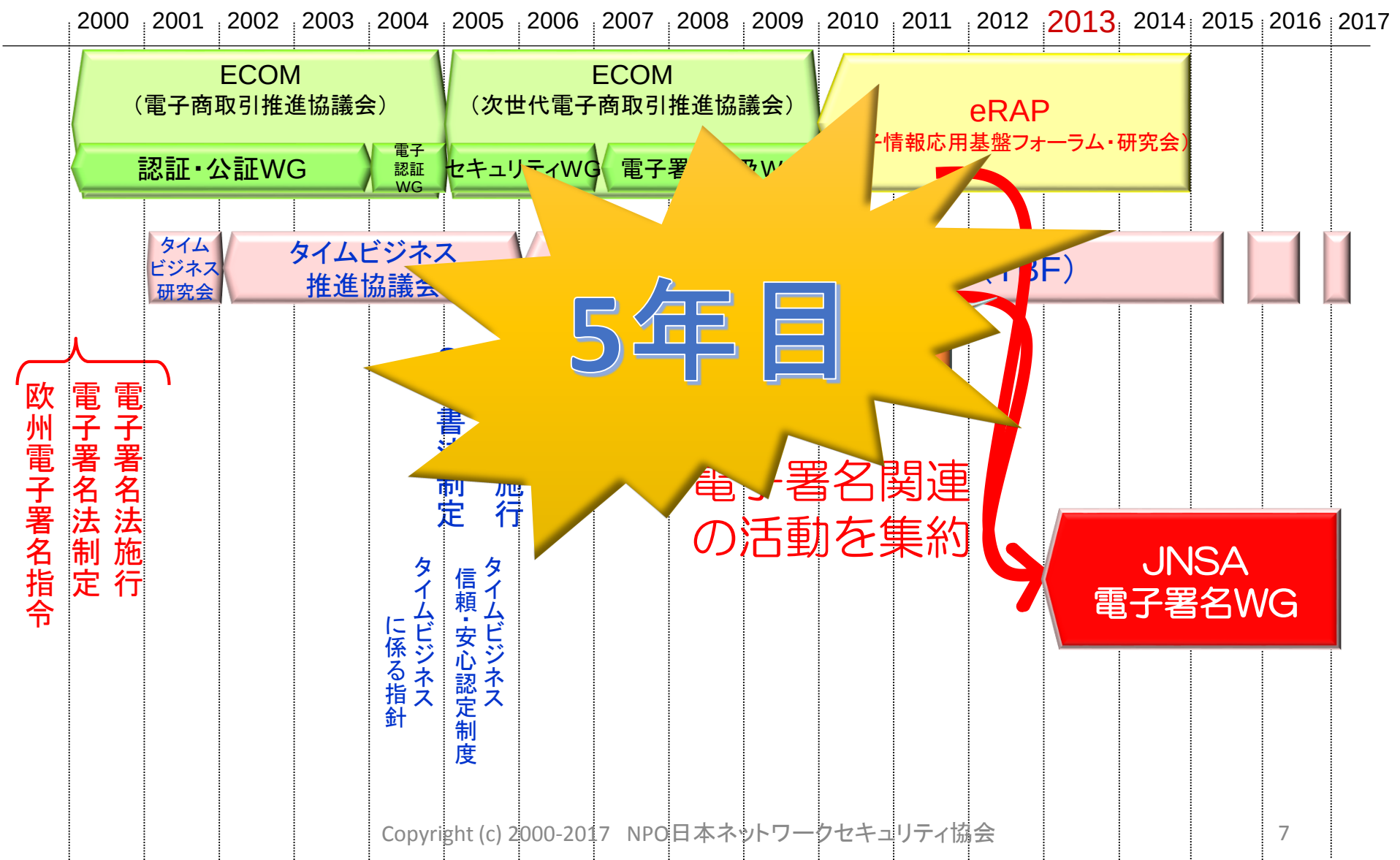
トラスト

報告内容

- 電子署名WGについて
  - 設立経緯、活動目的、体制
- 2016年度活動実績
- 2016年度成果紹介
  - PAdESプロファイルの標準化
  - リモート署名の検討
  - スキルアップTF
- 今後の電子署名WG

電子署名WGについて

2013年度：電子署名WG設立

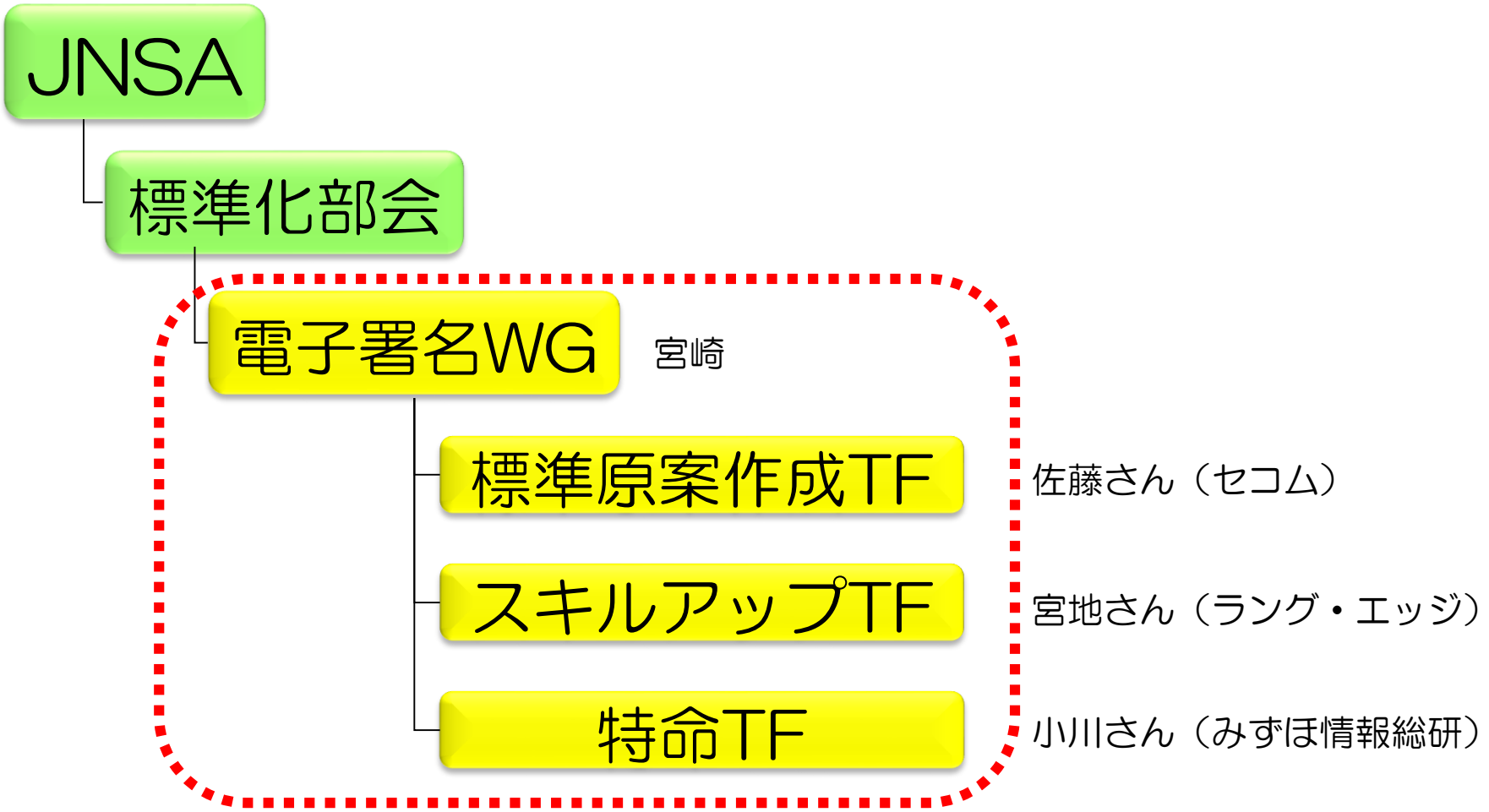


活動目的

- 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

体制

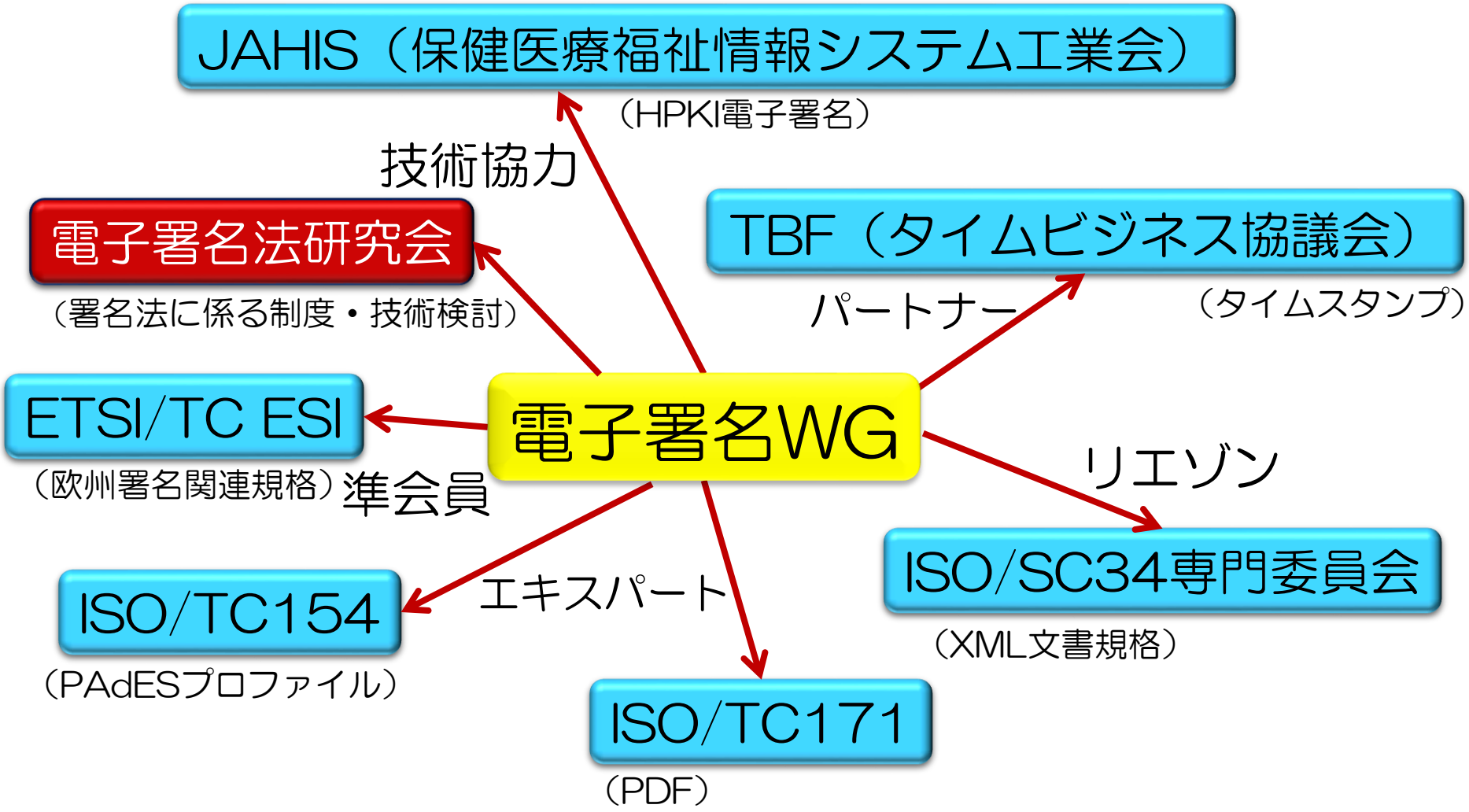


2016年度活動実績

2016年度活動方針

- テーマ
  ① PAdESプロファイルの標準作成
  ② リモート署名の検討
  ③ スキルアップTF
  ④ 電子署名に係る他団体の支援
- 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

JNSA

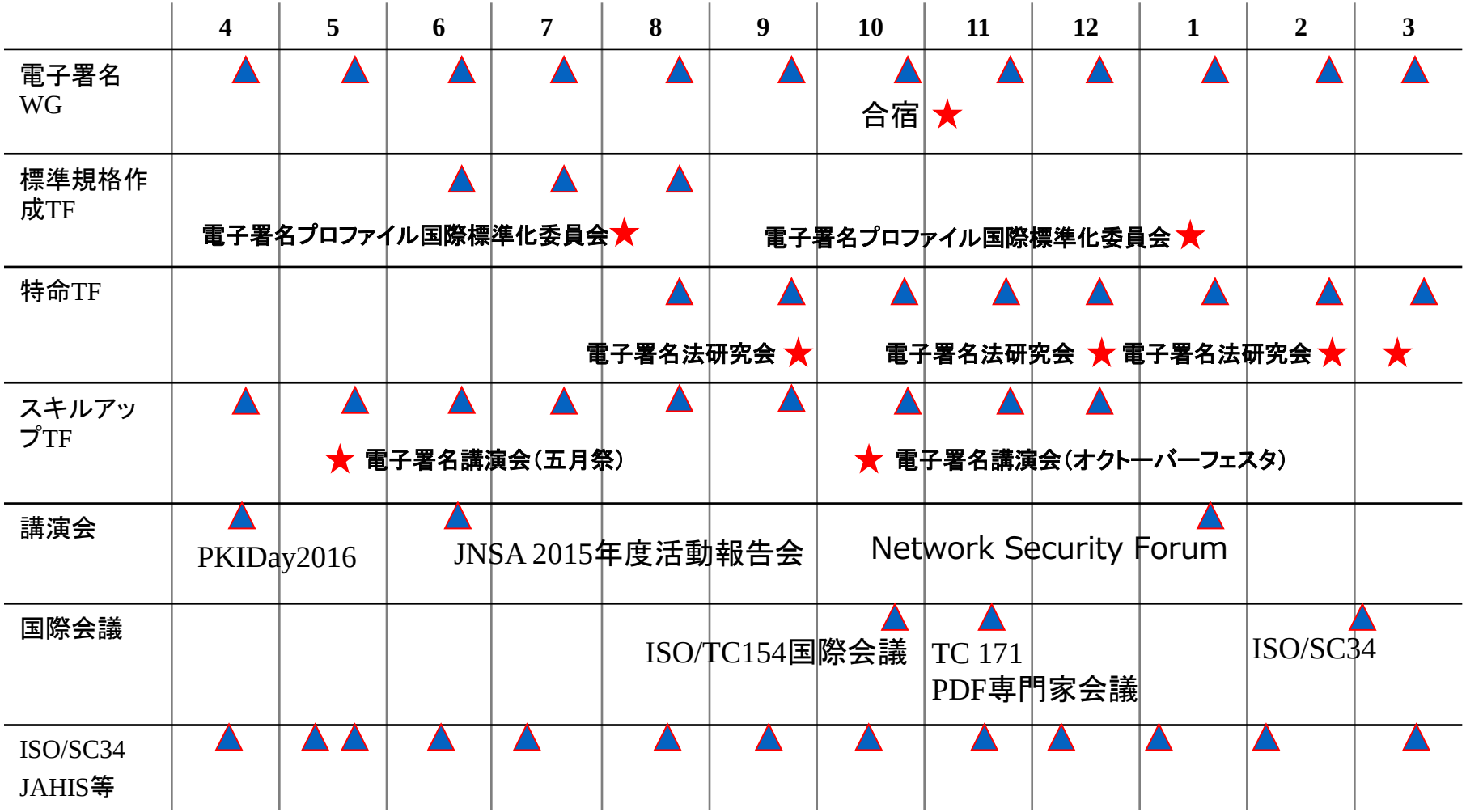
- 電子署名WG
  諸連絡、関連情報交換、企画運営
- 標準原案作成TF
  経産省国際標準化関連事業対応
- 特命TF
  電子署名研究会対応リモート署名の検討
- スキルアップTF
  勉強会、PKI SandBox Project、電子署名WG主催講演会
- ETSI/TC ESI
  日欧間の署名規格仕様調整
- ISO/TC154
  PAdESプロファイルのISO化
- ISO/SC34専門委員会
  XML文書規格における長期署名
- 講演会
  活動報告会、NSF、PKI Day

JAHIS
電子処方箋の署名仕様

2016年度活動実績

- WG／TF（計37回）
  - 電子署名WG：12回（＋臨時1回）
  - 標準原案作成TF：3回（＋電子署名プロファイル国際標準化委員会2回）
  - 特命TF：8回
  - スキルアップTF：9回（＋電子署名WG主催講演会2回）
- ISO
  - ISO/TC154国際会議（@ドイツ ベルリン）
  - ISO/TC171国際会議（@オーストラリア シドニー）
  - ISO/SC34国際会議（@アメリカ シアトル）
  - ISO/SC34国内専門委員会：5回
- 講演会
  - PKI Day 2016「マイナンバー時代のPKI」PKI相互運用技術WGと共催
  - JNSA 2015年度活動報告会
  - 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、リモート署名の検討状況）
  - PKI Day 2017[4/19]「IoT・ブロックチェーン時代のPKI」
- その他
  - JAHIS：HPKI電子署名規格作成WG12回、電子処方せん実装ガイド策定TF3回
  - 経産省：電子署名法研究会：4回
  - 合宿（@茨城 下妻）、懇親会

2016年度活動実績



2016年度成果紹介

① PAdESプロファイル標準化
② リモート署名検討
③ スキルアップTF

① PAdESプロファイル標準化
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。

① PAdESプロファイル標準化
ISO 14533-3

Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)

PAdES-Tプロファイル　(EUプロファイル T-level相当)

署名タイムスタンプ付きのPDF署名
（署名の存在証明が可能に）

PAdES-Aプロファイル　(EUプロファイル LTA-level相当)

アーカイブタイムスタンプ付きのPDF署名
（署名の長期有効性担保が可能に）

PAdES-DT/DTAプロファイル

タイムスタンプのみの適用が可能に

News 1 プロジェクトは順調に進行。めでたく国際規格(IS)として発行準備中！

News 2 PDF/A-next 規格(ISO/CD 19005-4)で採用される予定！

② リモート署名検討
2016年度成果

経済産業省事業において
リモート署名のモデルや機能の詳細を検討

1. 具体的な利用モデルの検討

   事業者、
   と整理

2.

   ation）、
   on

   Module）の具体的な機能構成を詳細化

3. 利用者登録～署名に至る各フェーズのリスク分析

   利用者本人確認から利用者登録、クレデンシャル発行・署名鍵生成と配布、利用者認証と署名に関するシーケンスの作成とリスク分析

報告書公開

② リモート署名検討
2017年度計画

1. リモート署名ガイドラインの作成

- サービスや利用シーンに応じた本人確認の度合い、Identity Proofing、リモート署名事業者のポリシー等、さらに詳細化が必要。
- リモート署名に関係する事業者、利用団体などマルチステークホルダによるガイドラインの検討。

2.リモート署名コンソーシアムの設立準備

- リモート署名の普及には、国内のガイドライン作成だけではなく、関連団体（国内外含む）との連携が必要。
- 上記ガイドライン作成メンバで、Remote Signature Consortium（仮称）を絶賛準備中。

ETSI/eIDASでの検討が知りたい方は！JNSA

日欧インターネットトラストシンポジウム https://itc.jipdec.or.jp/event/20170704.html
日時：２０１７年７月４日（火）９：３０～１７：００（受付開始９：００～）
場所：慶應義塾大学　三田キャンパス
主催：ETSI、慶應義塾大学、JIPDEC

時間	講演内容および講師（※敬称略）
9:30～9:35	主催者挨拶　慶應義塾大学　政策・メディア研究科　特任教授　　手塚　悟
9:35～10:00	仮）eIDAS Defined Trust Services and Context Setting for Policy and Technology Alignment Thales e-Security，Principal Consultant　　Nick Pope
10:00～10:25	仮）日本の動向について（マイナンバーカード、リモート署名、属性証明書）　慶應義塾大学　政策・メディア研究科　特任教授　　手塚　悟
10:25～10:50	仮）ETSI Standards for Signatures, Formats and Trust List SEALED，Managing Director　　Sylvie Lacroix
10:50～11:15	仮）ETSI Certification Policies for eIDAS Trust Services and Electronic Delivery Services Nimbus Technologieberatung GmbH, Managing Director　　Arno Fiedler
11:15～11:40	仮）Audits based on ETSI CP for "qualified TSP" and global recognition TÜV Informationstechnik GmbH　　Clemens Wanko
11:40～12:05	インターネットトラストの実現に向けて　　一般財団法人日本情報経済社会推進協会　常務理事　　山内　徹
12:05～13:05	お昼休憩
13:05～13:30	仮）Cloud signing / remote signing Introduction　　Thales e-Security，Principal Consultant　　Nick Pope
13:30～13:55	仮）Cloud signature consortium　　Cloud signature consortium　　<未定>
13:55～14:20	仮）CEN Standards on remote signing DOCAPOST，Chief Technical Officer of Digital Trust Services　CEN TC224 chairman　　Franck Leroy
14:20～14:50	休憩（ブース見学）
14:50～15:15	調整中　株式会社コスモス・コーポレイション　　濱口　総志
15:15～15:40	仮）日本のリモート署名の検討　特定非営利活動法人日本ネットワークセキュリティ協会　　小川　博久
15:40～16:05	調整中　タイムビジネス協議会　　柴田　孝一
16:05～16:25	質疑応答
16:25～16:30	主催者閉会の挨拶　一般財団法人日本情報経済社会推進協会　常務理事　　山内

③ スキルアップTF

JNSA

人材育成/普及啓発/情報公開/技術公開

- ESWGサーバー **http://eswg.jnsa.org/**

電子署名WG祭り開催
年2回開催の公開勉強会（資料公開）

メンバー向け勉強会
不定期勉強会（資料非公開）

開発成果の公開
お試し環境 PKI SandBox
電子署名ポータルサイト 等

③ スキルアップTF
2016年度成果

1. 年2回の公開勉強会「電子署名WG祭」

第1回：5月23日開催：もう紙の時代じゃない！

参加 57名、アンケート結果：満足以上が86%

第2回：10月26日開催：ライトニングトーク祭り！

基調講演：電子署名入り文書の流通インフラとしての Acrobat Reader

参加 38名、アンケート結果：満足以上が96%

公開資料：**http://eswg.jnsa.org/matsuri/**

2. メンバー向け勉強会（資料はメンバーのみ公開）

エストニアIDカードのPKIマニアック解析 完全版

eIDAS規則とリモート署名の現状について

FreeXAdES第2回タイムスタンプ編

制御システムセキュリティの脅威と対策の動向

③ スキルアップTF
2017年度計画

1. 定期公開勉強会開催（年2回開催）

電子署名WG春祭り：「シン・五月祭」

5月22日開催済み（57名参加、盛況でした）

電子署名WG秋祭り：10月頃に開催予定

2. メンバー向け勉強会（不定期開催）

6月13日（明日）午後に独HSMベンダー勉強会開催！
https://maturi-eswg-jnsa.connpass.com/event/58918/

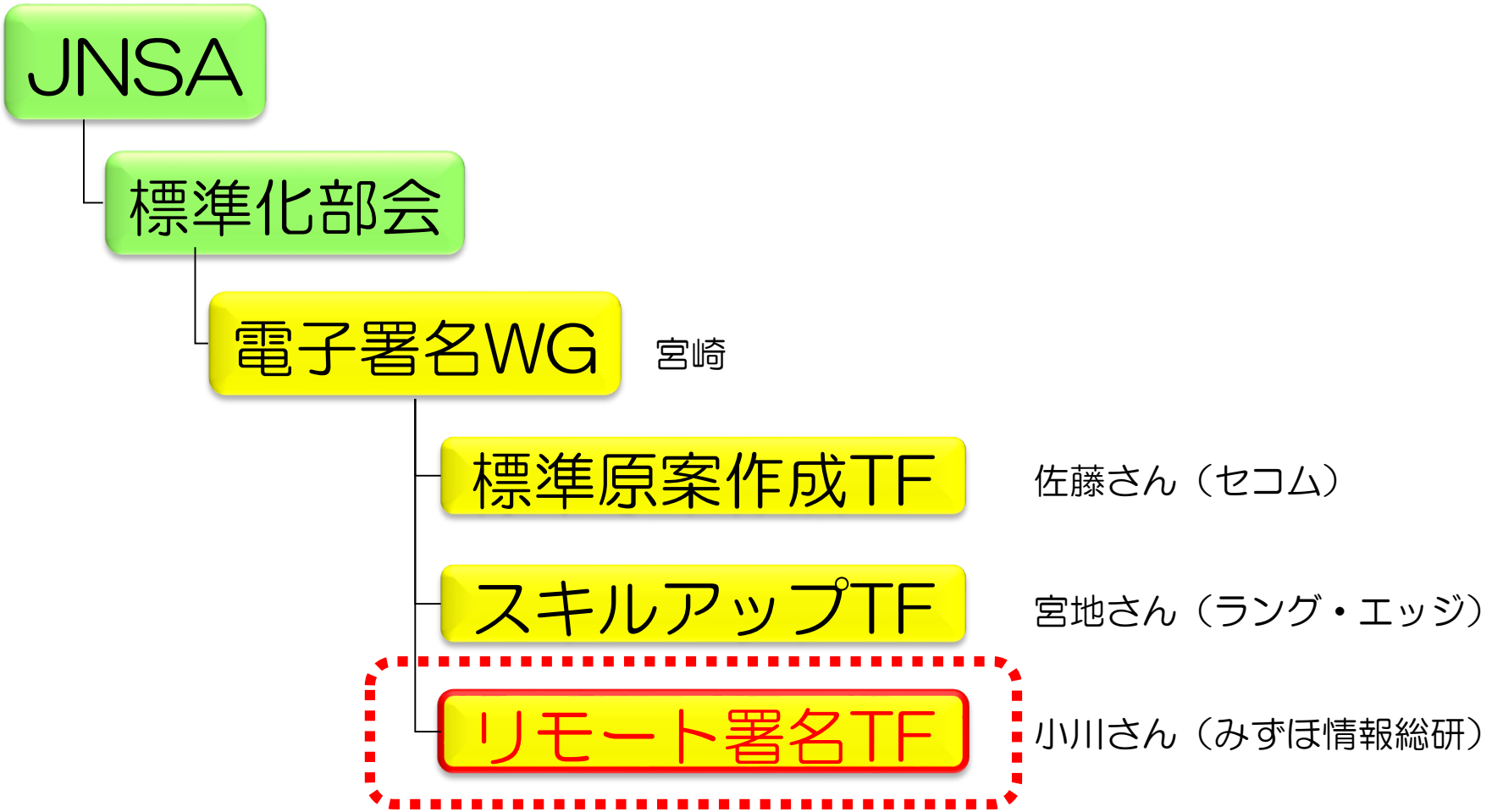
その他色々企画中！WGお試し参加もありです！

3. 電子署名ポータルを今年度中に公開予定

電子署名の利活用情報用ポータルサイトを現在開発中！

今後の電子署名WG

2017年度の体制



今後の課題

- リモート署名ガイドラインの作成
  - JIPDEC、CAC、TBFとの連携で作成・発行
- 標準化
  - EU等における標準化動向を踏まえた既存標準規格（ISO14533-1，2、JIS X5092，5093）の見直し
  - PAdESプロファイルのJIS化
  - 電子署名検証規格への再チャレンジ
- 一段高い視点から、電子的な『トラスト』、『コミット』、『証拠』の在り方やそれを実現するための基盤技術を検討
  ⇒リモート署名コンソーシアム（仮称）の延長線上？

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。

ご清聴ありがとうございました。