



2017年度 電子署名WG 成果報告/JT2A紹介

電子署名WG サブリーダー
JT2A運営委員長
小川 博久

活動報告の内容



1. 2017年の活動 → 振り返り
2. 新団体JT2A
3. 2018年の活動 → 抱負

2017年の活動

1. WGの活動目的

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

2. WGの年間活動予定

- ・標準仕様案検討会（年30回程度）
- ・電子署名関連標準化の新規事業獲得に向けた活動
- ・欧州電気通信標準化機構/電子署名基盤技術委員会会議、国際標準化会議（ISO/TC154等）への参加
- ・署名関連実証プロジェクト、勉強会実施、その他普及啓発

※電子署名WGのタスク・フォース

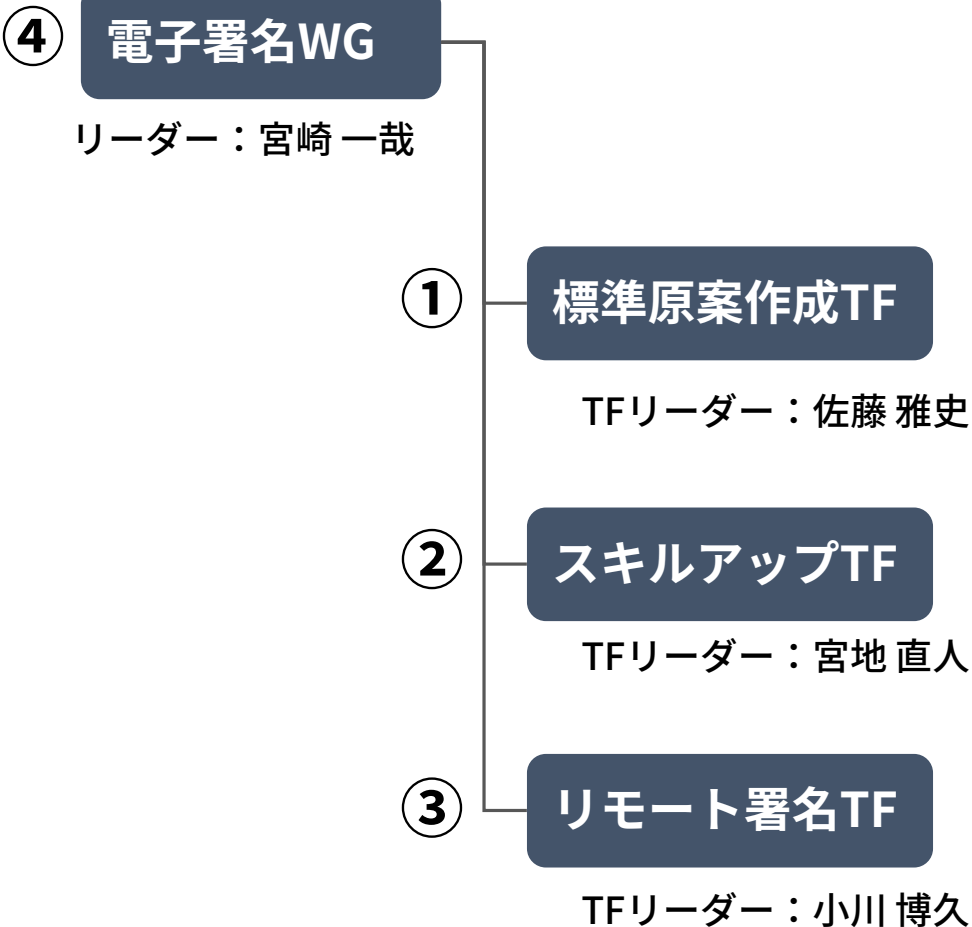
- ・電子署名WG リーダー：宮崎 一哉（三菱電機（株））
- ・標準原案作成TF リーダー：佐藤 雅史（セコム（株）IS研究所）
- ・スキルアップTF リーダー：宮地 直人（（有）ラング・エッジ）
- ・リモート署名TF リーダー：小川 博久（みずほ情報総研（株））

※電子署名WG実験サーバー → <http://eswg.jnsa.org/>

3. 予定成果物

- ・PDF署名(PAdES)プロファイルのISO国際標準化
- ・リモート署名ガイドライン

2017年の体制



①標準原案作成TFの活動

1. 活動内容

- 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
 - 上記の標準化事業終了後の2017年度も国際標準発行を目指して活動を継続

2. 成果物

- ISO 14533-3 PDF署名(PAdES)プロファイルのISO国際標準化
- ISO 32000-2 (PDF 2.0)

①標準原案作成TFの活動



JNSAが推進したISO 14533-3
(PAdES長期署名プロファイル)は2017年9月に発行

The screenshot shows the ISO 14533-3:2017 standard page. The header includes the ISO logo and the text "International Organization for Standardization When the world agrees". The main content area displays the standard title "ISO 14533-3:2017" with a "Preview" button. Below the title, it states: "Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)". A "Buy this standard" box is visible on the right, showing the format "PDF + ePub" selected, the language "English", and the price "CHF 118". A "General information" box on the left provides details: "Current status : Published", "Publication date : 2017-09", "Edition : 1", "Number of pages : 26", "Technical Committee : ISO/TC 154 Processes, data elements and documents in commerce, industry and administration", and "ICS : 35.240.63 IT applications in trade". At the bottom, it mentions "Life cycle" and "A standard is reviewed every 5 years".

JNSAメンバーも議論に加わった
ISO 32000-2 (PDF 2.0)は2017年7月に発行

The screenshot shows the ISO 32000-2:2017 standard page. The header includes the ISO logo and the text "International Organization for Standardization When the world agrees". The main content area displays the standard title "ISO 32000-2:2017" with a "Preview" button. Below the title, it states: "Document management -- Portable document format -- Part 2: PDF 2.0". A "Buy this standard" box is visible on the right, showing the format "PDF" selected, the language "English", and the price "CHF 198". A "General information" box on the left provides details: "Current status : Published", "Publication date : 2017-07", "Edition : 1", "Number of pages : 971", "Technical Committee : ISO/TC 171/SC 2 Document file formats, EDMS systems and authenticity of information". At the bottom, it mentions "Life cycle" and "A standard is reviewed every 5 years".

<https://www.iso.org/standard/63534.html>

<https://www.iso.org/standard/67937.html>

②スキルアップTFの活動

1. 活動内容：公開勉強会開催

- 5月22日開催：第3回 電子署名WG春祭り2017
 - 「シン・五月祭 電子署名は使われているか？」
 - 参加52名、アンケート結果：満足以上95%
- 6月13日開催：独Utimaco社HSMセミナー
- 7月20日開催：Gemaltoの勉強会（JNSA会員のみ）
- 11月1日開催：第4回 電子署名WG秋祭り2017
 - 「君の署名は。 マイナンバーカードですが何か？」
 - 参加63名、アンケート結果：満足以上97%

2. 成果物：ESWGサーバ運用による公開活動

- 電子署名WG試験サーバー <http://eswg.jnsa.org/>
 - 勉強会資料の公開
 - 電子署名/PKIの試験環境 PKI SandBox の運用
 - 電子署名ポータルサイト（開発中・電子署名WG内向けには公開）

②直近の“祭り”の内容



JNSA電子署名WG秋祭り
「君の署名は。」
～マイナンバーカードですが何か？～

日時：2017年11月1日 16:00～19:00
場所：セコムホールA

【基調1】	マイナンバーカードによる認証と署名 濱野 司（オープンソース・ソリューション・テクノロジー（株））
【LT1】	JPKIを活用してみたかったこと 戸谷 樹一郎（（株）システムコンサルタント）
【LT2】	J-LIS公開のAPIを読み解くなど 村尾 進一（セイコーソリューションズ（株））
【休憩】	
【LT3】	組織認証と委任とその法律（1月1日施行予定） 新井 聡（電子認証局会議）
【LT4】	こんなマイナンバーカードが欲しい！ 政本 廣志（NTTアドバンステクノロジー（株））
【基調2】	マイナポータルの今後の展開と利用環境改善の取り組み 楠 正憲 氏（内閣官房 番号制度推進室 番号制度推進管理補佐官）
【成果発表】	ISO 14533-3 PAdES Profileが正式に発行（仮） 佐藤 雅史（セコム（株）IS研究所）
【特別発表】	新団体 JT2Aの紹介 小川 博久（リモート署名TFリーダー）

JNSA電子署名WG春祭り2018
「電子署名の世界（SIGN WORLD）」
～電子署名の技術と法律の棚卸をしよう～

日時：2018年5月23日 16:30～19:30
場所：NTTテクノクロス 品川 セミナールーム

【基調1】	電子政府における本人確認の見直しと法人共通認証基盤の検討 満塩 尚史（経済産業省 CIO補佐官）
【基調2】	個人の電子証明書と法人役職者の電子証明書 ～意外と使える電子委任状法～ 宮内 宏（宮内・水町IT法律事務所）
【特別発表】	サイバーセキュリティトレンド2018 星 敬一（NTTテクノクロス（株））
【休憩】	
【LT1】	電子署名法視点で技術の棚卸をしてみよう 佐藤 雅史（セコム（株）IS研究所）
【LT2】	Re:FreeXAdESから始める長期署名 ～オープンソースでタイムスタンプを使おう編～ 宮地 直人（（有）ラング・エッジ）
【LT3】	クラウド署名とCSC対応について 村尾 進一（セイコーソリューションズ（株））
【LT4】	JT2A 真正性検証TFについて 山中 忠和（三菱電機（株））
【LT5】	X-Roadと電子署名 濱口 総志（（株）コスモス・コーポレーション）

③ リモート署名TFの活動

1. 活動内容

- リモート署名ガイドラインの検討は一旦ペンディング
- JT2Aの設立に関する調整
(あとで説明します)

1. 活動内容と成果物

●PKI Dayの共催

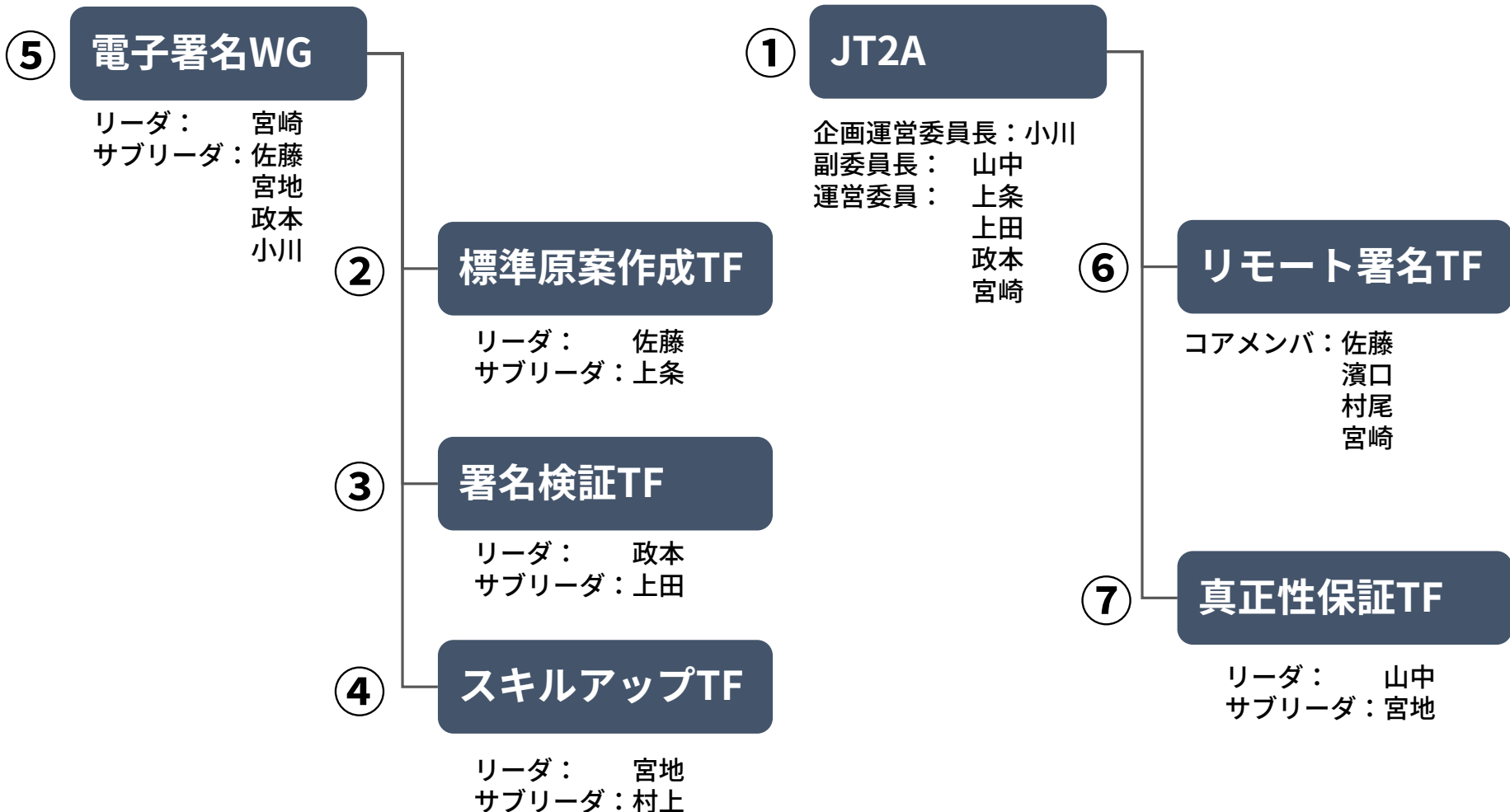
- PKI Day 2017「IoT・ブロックチェーン時代のPKI」（2017年4月19日）
- PKI Day 2018「超スマート社会（Society 5.0）におけるトラストの在り方」（2018年4月17日）

●JAHISへの技術支援

- JAHIS標準「ヘルスケアPKIを利用した医療文書に対する電子署名規格PAdES編Ver.1.0」の作成支援
- JAHIS技術文書「JAHIS電子処方せん実装ガイドVer.1.0」の作成支援

●ISO/IEC JTC1 SC34のリエゾンとしてのOOXMLのOPC改定支援

2018年は新体制でスタート



JNSA史上初の充実感

- 念願の署名検証TFの始動
- アプリケーション分野であるリモート署名TF
- 本人認証と電子署名を整理する真正性保証TF

(日本酒で)乾杯戦士アツターV



① JT2Aの概要

英文	Japan Trust Technology Association (JT2A)
事務局	NPO日本ネットワークセキュリティ協会 (JNSA)
代表者	手塚 悟 慶應義塾大学大学院 政策・メディア研究科特任教授/JNSA顧問
副代表者	松本 泰 セコム（株）IS研究所/JNSA PKI相互運用技術WGリーダー
運営 委員長	小川 博久 JNSA電子署名WGサブリーダー
目的	電子署名や電子証明書など含むトラストテクノロジーに関連する事業者及び利用者が主体となり、産学官及び国内外の関連団体と連携して信頼性を担保するための <u>技術等の検討</u> を行い、より信頼できる電子社会の促進に寄与する。

① JT2A 直近の検討と今後 JNSA

トラストテクノロジー利用普及

電子署名/電子認証等の
トラストテクノロジーの活用を産官学及
び海外との連携により実現する

超スマート社会の実現

超スマート社会の実現に寄与する
信頼ベースのサービスや技術
の検討と公開を目指す。

国内外の関連団体との連携

リモート署名等ガイドライン策定

- ・実装ガイドライン
- ・運用ガイドライン
- ・サービスポリシー規程

Japan Trust Technology
Association



リモート署名ガイドライン

リモート署名に求められる
安全基準要素をまとめる事で
リモート署名/クラウド署名の
安全な構築と運用に寄与する

②標準原案作成TFの抱負

1. 活動内容

- CAdES長期署名プロファイル（ISO 14533-1 およびJIS X 5092）の改訂
- XAdES長期署名プロファイル（ISO 14533-2 およびJIS X 5093）の改訂
 - ・ フォーマット新バージョンへの対応
 - ・ 新たに発行されたEN(欧州規格)との整合性
- PAdES長期署名プロファイルのJIS化
- 長期署名検証の要件定義、検証結果レポート
 - ・ 署名検証TFと連携して推進
- ヘルスケア分野の署名規格についてJAHIS(保健医療福祉情報システム工業会)と連携

2. メンバ

- ・ リーダー：佐藤雅史（セコム（株）IS研究所）
- ・ サブリーダー：上条桃花（NTTデータ（株））



③署名検証TFの抱負

1. 活動予定

『標準の長期署名をしたけれど、検証してみたら、アレ??』
とならないために、署名検証の標準化を進めよう。

- 欧州の標準化状況の調査
- 国際/国内標準化に向けた活動
- 実用に供するためのガイドラインや認証・評価制度に向けた取り組み

3年ぶりの再開！

2. 予定成果物

- まずは署名検証標準・調査報告書（欧州調査結果、取組み案）

3. メンバ

- リーダー：政本 廣志（NTTアドバンステクノロジー（株））
- サブリーダー：上田 祐輔（アマノビジネスソリューションズ（株））
- メンバ：署名利用者、検証ソフト作成者など、募集中！！



④スキルアップTFの抱負

1. 活動予定

- ・ **第5回 電子署名WG春祭り2018**（5月23日開催済み）
 - ・ 「電子署名の世界 技術と法律の棚卸をしよう」
 - ・ 参加84名（過去最大の参加人数！）
- ・ **第6回 電子署名WG秋祭り2018**
 - ・ 10月または11月に開催予定（JT2Aとの共同開催を検討中）
- ・ 他にも公開/会員限定の勉強会やハンズオンを実施予定。

2. 成果物（予定）： ESWGサーバ運用による公開

- 勉強会資料の公開
- 情報検索サイト電子署名ポータルサイトの外部公開
- PKI SandBox の更新と第2回PKIハンズオンの実施

3. その他：若手技術者の育成を目指す（発表の場提供等）

4. メンバ： リーダー 宮地直人（（有）ラング・エッジ）

サブリーダー 村上耕平（三菱電機インフォメーションシステムズ（株））



⑤電子署名WGの抱負



1. 活動内容

- 講演会（PKI Day等）の共催
- JAHISへの技術支援
- ISO/IEC JTC1 SC34のリエゾン
- トラストサービス推進フォーラムへの参加
- 暗号モジュール試験及び認証制度技術審議委員会への参加

電子署名のことならなんでもござれ！

1. 活動内容

- リモート署名の重要な論点をまとめ
- ガイドラインとして記載すべき全体構成を議論
- 例えば、このような内容
 - EUの法制度・要件等との関連性は？
 - 本当に安全なのか？セキュリティは大丈夫なのか？

2. コアメンバ

- 佐藤雅史（セコム（株）IS研究所）
- 濱口総志（（株）コスモス・コーポレーション）
- 村尾進一（セイコーソリューションズ（株））
- 宮崎 一哉（三菱電機（株））

3. 予定成果物

- リモート署名ガイドライン

JT2A
リモート署名TF



平成27年度 調査報告書のまとめから抜粋

- リモート署名は、すでに欧州や米国において広く利用されているサービスであり、電子証明書及び電子署名の利用を拡大するものである。
- また、我が国においても2016年からマイナンバーカードの利活用が進み、2017年にはマイナポータルにおいて官民が連携し、各種の申請や手続きが電子化されることで国民にとっても電子証明書及び電子署名がより身近に利用できる環境が整う。
- さらに、昨今の電子契約については、利便性が高く、安全なサービスが求められるため、本事業で検討したリモート署名は、この電子契約の促進に資するものであり、より安全な社会経済の更なる発展に向けて大きく貢献する。

平成28年度 第一回電子署名法研究会の議事要旨から抜粋

- クラウド時代の電子署名のあり方が重要であると考えている。仮にリモート署名が実現できないとすると、クラウドサービス上では自然人の意思の推定効を担保する仕組みが出来ないことになってしまう。

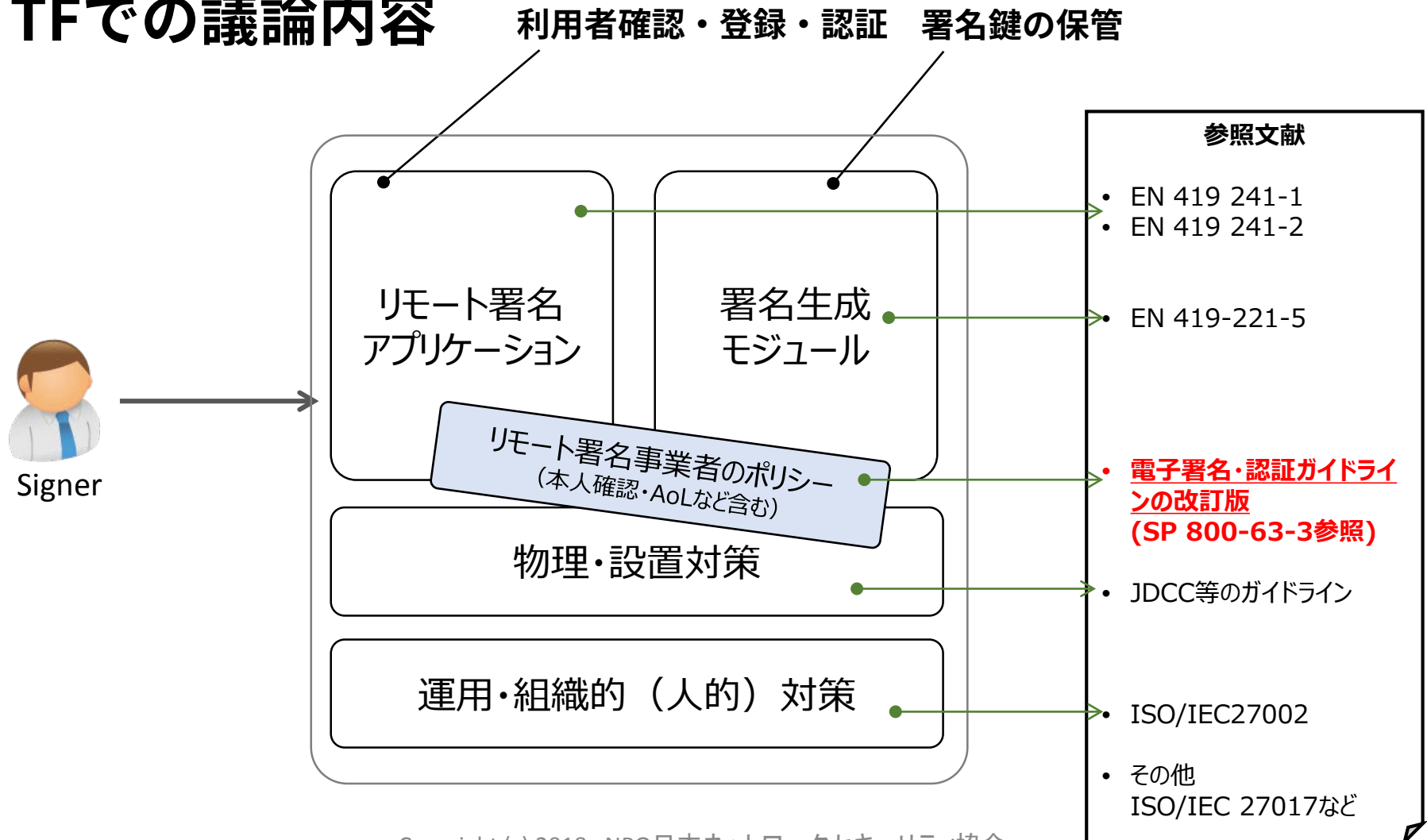
電子署名法研究会（METI/経済産業省）

http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#denshishomeihou

電子署名法研究会（平成28年度第1回） - 議事要旨（METI/経済産業省）

http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/h28_01_giji.html

TFでの議論内容



1. 活動予定

- 真正性保証の指針策定

- 暗号技術に限定せず、真正性の確保に必要な要件等を検討

- 電子署名・認証ガイドライン改定支援

- デジタル・ガバメント技術検討会議の技術TFへ参画。
ガイドラインの改定作業を支援し、本人確認等に関する実装ガイドを策定

2. メンバ

リーダー：山中忠和（三菱電機（株））

サブリーダー：宮地直人（（有）ラング・エッジ）

3. 予定成果物

- 真正性保証ガイドライン
- 本人確認等に関する実装ガイド



資料2

本人確認の検討状況



2018年3月1日

内閣官房 情報通信技術(IT)総合戦略室

第32回新戦略推進専門調査会電子行政分科会
 第14回規制制度改革ワーキングチーム
 第16回各府省情報化専任審議官等連絡会議
 合同会議

https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/densi/dai32/gijisidai.html

IT総合戦略本部電子行政分科会での検討状況

■ 議論を深めるため、ワークショップで議論を実施

➢ これまでの経緯、技術的バックグラウンド等を解説後、6人程度のグループで議論を実施し、グループ毎の取りまとめを実施。

9月24日(神戸)

デジタル時代の押
 印を考えよう
 ワークショップ

参加者： 内閣官房 他1府省
 地方公共団体
 市民

・押印の課題の明確化
 ・本人確認手法の検討



10月10日(東京)

本人確認等の在り
 方に関する
 ワークショップ

参加者： 内閣官房 他4府省
 経済団体
 セキュリティ団体
 弁護士

・押印の課題の明確化
 ・本人確認手法の検討



12月13日(東京)

本人確認等の在り
 方に関する
 ワークショップ2

参加者： 内閣官房 他2府省
 経済団体
 セキュリティ団体
 弁護士

・押印見直しガイドラインの
 案の検討
 ・技術的課題の検討



政府CIOポータル

・本文へ 文字サイズの変更: 標準 拡大

Language: 日本語 検索

IT総合戦略室について お知らせ 政策 法令 刊行物 その他

政府CIOポータルホーム > お知らせ > 「デジタル・ガバメント技術検討会議」を設置しました。

電子行政

「デジタル・ガバメント技術検討会議」を設置しました。

2018.5.18

デジタル社会に対応した電子行政を実現するため、デジタル・ガバメント推進方針（平成29年5月30日 IT本部・官民データ活用推進戦略会議決定）が決定しました。この方針を推進するに当たって、政府職員だけでは解決が困難な技術的、専門的な課題等について検討するため、政府CIO補佐官から構成される「デジタル・ガバメント技術検討会議」を各府省情報化統括責任者（CIO）連絡会議の下に設置しました。

また、個別内容について集中的に検討するため、「デジタル・ガバメント技術検討会議タスクフォース（以下、「TF」という。）」として「ガイドTF」、「データTF」、「技術TF」及び「人材TF」を設置しました。

今後は各TFにおいて、データ標準や技術標準等、デジタル・ガバメントの推進に係る技術的かつ横断的な内容について具体的な検討を行い、その結論をCIO連絡会議に提案していくこと等を通じて、行政サービスの向上や行政の効率的な運営等の成果につなげていくこととしています。

- お知らせ
- 会見
- パブリックコメント等
- 報道発表
- 行事案内
- 関連イベント

・技術TF（2018年4月時点）

主査	満塩尚史政府CIO補佐官
副主査	西村毅政府CIO補佐官
メンバー	細川努政府CIO補佐官 楠正憲政府CIO補佐官 高橋邦明会計検査院CIO補佐官 山中忠和日本トラストテクノロジー協議会 真正性検証タスクフォースリーダー
主な検討内容	政府情報システムに係る標準的な技術の 取扱いに関する検討

「デジタル・ガバメント技術検討会議」を設置しました。
<https://cio.go.jp/node/2361>

資料 1-2

デジタル社会における行政手続の本人性の確認
及び真正性の確保等の手法に関するガイドラインについて



2018年5月29日

内閣官房 情報通信技術(IT)総合戦略

「デジタル社会における行政手続の本人性の確認及び真正性の確保等の手法に関するガイドライン」の概要について

本ガイドラインは下記2点で構成され、各府省はそれぞれを活用し、デジタル・ガバメント中長期計画を策定

1. デジタル社会における行政手続の本人性の確認及び真正性の確保等の手法に関する**ガイドライン**
2. デジタル社会における行政手続の本人性の確認及び真正性の確保等の手法に関する**テクニカルガイドブック(仮)**

1. デジタル社会における行政手続の本人性の確認及び真正性の確保等の手法に関するガイドライン（以下、「ガイドライン」と略す）

- 1-1 「ガイドライン」の概要
- 1-2 確認レベル分けと手法一覧

2. デジタル社会における行政手続の本人性の確認及び真正性の確保等の手法に関するテクニカルガイドブック(仮)（以下、「テクニカルガイドブック(仮)」と略す）

- 2-1 テクニカルガイドブック(仮)の概要
- 2-2 テクニカルガイドブック(仮)の記載予定事項

内閣府 規制改革推進会議 第8回行政手続部会 議事次第
<http://www8.cao.go.jp/kisei-kaikaku/suishin/meeting/bukai/20180529/agenda.html>

2-2. テクニカルガイドブック(仮)の記載予定事項

- 各定義の具体的な説明
 - 認証情報、ID・パスワード等方式、複数要素認証
- 具体的な実施方法
 - 電子署名方式の実施方法
 - ID・パスワード等方式(氏名等確認あり)、ID・パスワード等方式(氏名等確認なし)の実施方法
 - ・ 氏名等を確認する方法
 - ・ 認証情報や複数要素認証の確認方法
 - 真正性の確保の実施方法
 - ・ 電子署名方式、受信側による電子署名、タイムスタンプ、本人確認等に資するデジタル記録の保全とその突合等
- 留意事項
 - 電子署名方式を構築する際の留意事項
 - ID・パスワード等方式を構築する際の留意事項
 - ID・パスワード等方式の連携基盤を構築する際の留意事項
- 参考情報
 - 確認レベルの検討のためのリスク分析手法(グローバルスタンダード)

JT2Aの参加について



セキュリティ・ベンダー
セキュリティ・関連会社/組織
トラストテクノロジーを商売に
利用している企業や組織等

正会員

セキュリティ・ユーザ
ユーザ企業・非セキュリティSler他
トラストテクノロジーを利用して
ビジネスを展開する企業等

情報会員(仮)

JT2A

JNSA 正会員の資格が必要
(JNSA年会費24万円)
すぐに参加可能です！

入会時にJT2A参加希望とご連絡を！

<https://www.jnsa.org/aboutus/07.html>

JNSA 情報会員の資格が必要
2018年JNSA規約の変更により新設予
定の情報会員（仮）になることで
JT2Aへの参加が可能になります！
※ 当面オブザーバー参加は可能！
(年間参加費は年間10万円未満を予定)

参加希望に関してはJNSA電子署名WGメンバーまでご相談ください

コア技術と応用を充実・加速させる

