JT2A 日本トラストテクノロジー協議会
Japan Trust Technology Association

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

JT2Aについて

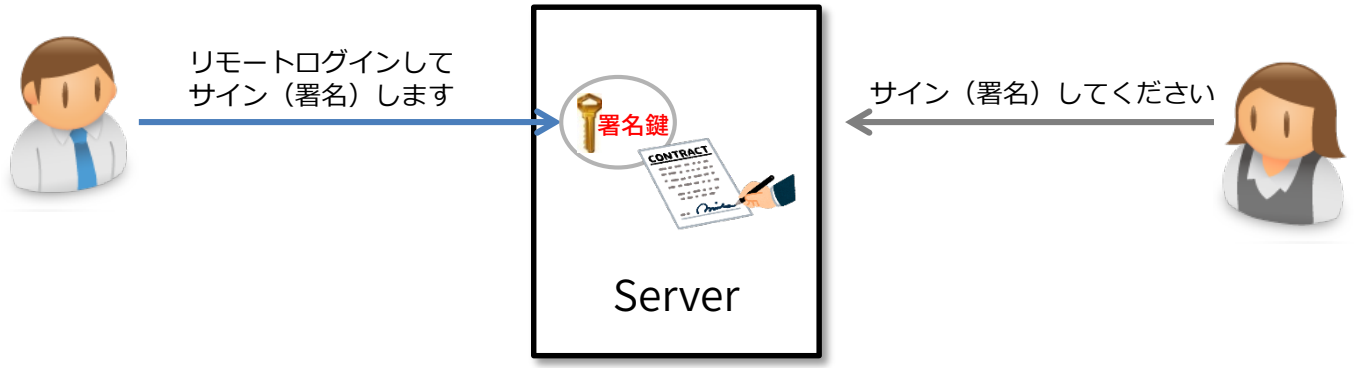
2018年 4月17日

JNSA電子署名WG サブリーダー / JT2A 運営委員長
小川 博久

JT2Aとは

2017年10月に発足、
現在設立準備中の団体

リモート署名を検討する団体（第一段階）

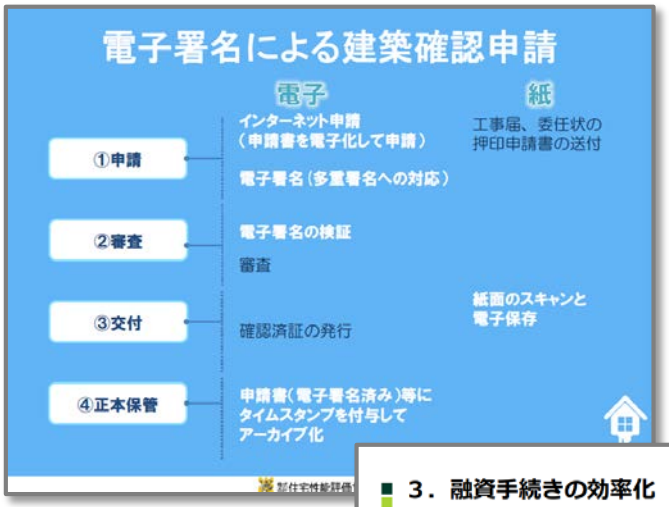


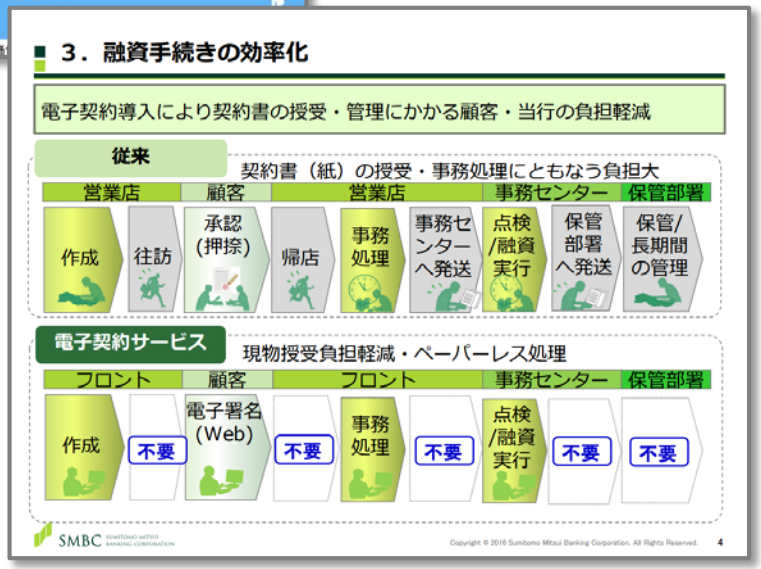
リモート署名の定義※

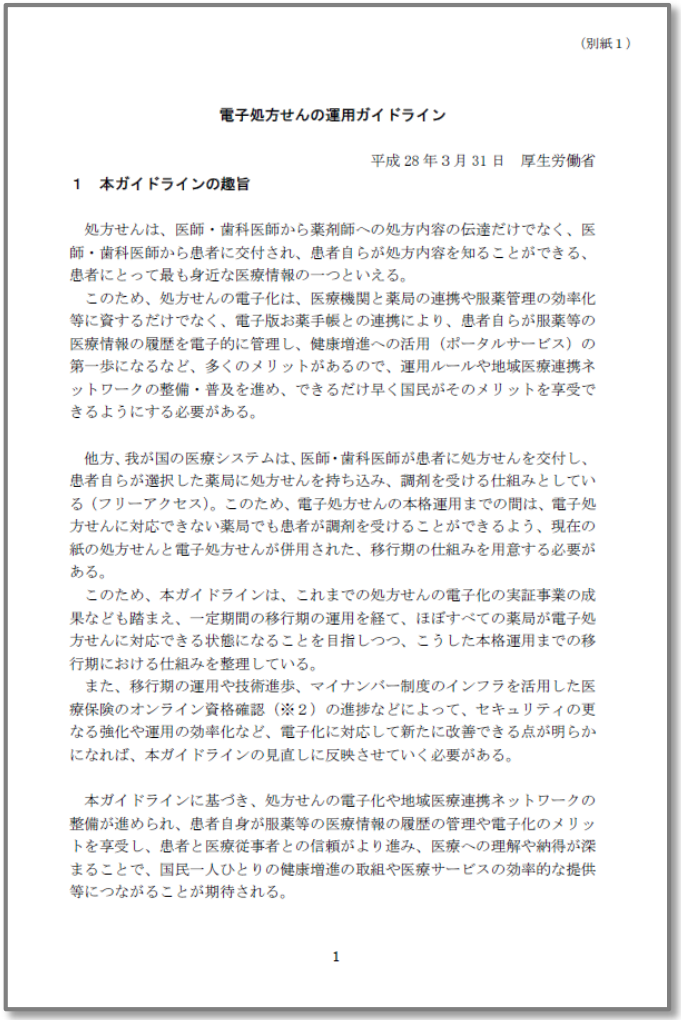
事業者のサーバに利用者（エンドエンティティ）の署名鍵を設置・保管し、利用者がサーバにリモートでログインし、自らの署名鍵で事業者のサーバ上で電子署名を行うこと。

※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

リモート署名は様々な分野で利用されている JT2A







（別紙１）

電子処方せんの運用ガイドライン

平成 28 年 3 月 31 日　厚生労働省

1　本ガイドラインの趣旨

処方せんは、医師・歯科医師から薬剤師への処方内容の伝達だけでなく、医師・歯科医師から患者に交付され、患者自らが処方内容を知ることができる、患者にとって最も身近な医療情報の一つといえる。

このため、処方せんの電子化は、医療機関と薬局の連携や服薬管理の効率化等に資するだけでなく、電子版お薬手帳との連携により、患者自らが服薬等の医療情報の履歴を電子的に管理し、健康増進への活用（ポータルサービス）の第一歩になるなど、多くのメリットがあるので、運用ルールや地域医療連携ネットワークの整備・普及を進め、できるだけ早く国民がそのメリットを享受できるようにする必要がある。

他方、我が国の医療システムは、医師・歯科医師が患者に処方せんを交付し、患者自らが選択した薬局に処方せんを持ち込み、調剤を受ける仕組みとしている（フリーアクセス）。このため、電子処方せんの本格運用までの間は、電子処方せんに対応できない薬局でも患者が調剤を受けることができるよう、現在の紙の処方せんと電子処方せんが併用された、移行期の仕組みを用意する必要がある。

このため、本ガイドラインは、これまでの処方せんの電子化の実証事業の成果なども踏まえ、一定期間の移行期の運用を経て、ほぼすべての薬局が電子処方せんに対応できる状態になることを目指しつつ、こうした本格運用までの移行期における仕組みを整理している。

また、移行期の運用や技術進歩、マイナンバー制度のインフラを活用した医療保険のオンライン資格確認（※2）の進捗などによって、セキュリティの更なる強化や運用の効率化など、電子化に対応して新たに改善できる点が明らかになれば、本ガイドラインの見直しに反映させていく必要がある。

本ガイドラインに基づき、処方せんの電子化や地域医療連携ネットワークの整備が進められ、患者自身が服薬等の医療情報の履歴の管理や電子化のメリットを享受し、患者と医療従事者との信頼がより進み、医療への理解や納得が深まることで、国民一人ひとりの健康増進の取組や医療サービスの効率的な提供等につながることが期待される。

1

タイムビジネス協議会 電子署名及び認証業務等利用促進セミナー
～電子署名・認証、タイムスタンプの国内外の動向及び国内先進ユーザ事例紹介～
http://www.dekyo.or.jp/tbf/seminar/semi14.html

電子処方せんの運用ガイドライン
平成 28 年 3 月 31 日 厚生労働省
http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000119545_2.pdf

H27・H28経済産業省事業での検討

資料１

平成２７年度サイバーセキュリティ経済基盤構築事業

（電子署名・認証業務利用促進事業（電子署名及び認証業務

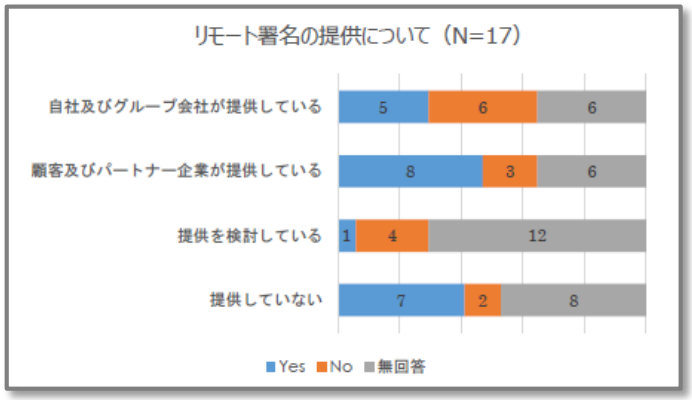
に関する調査研究等））調査報告書

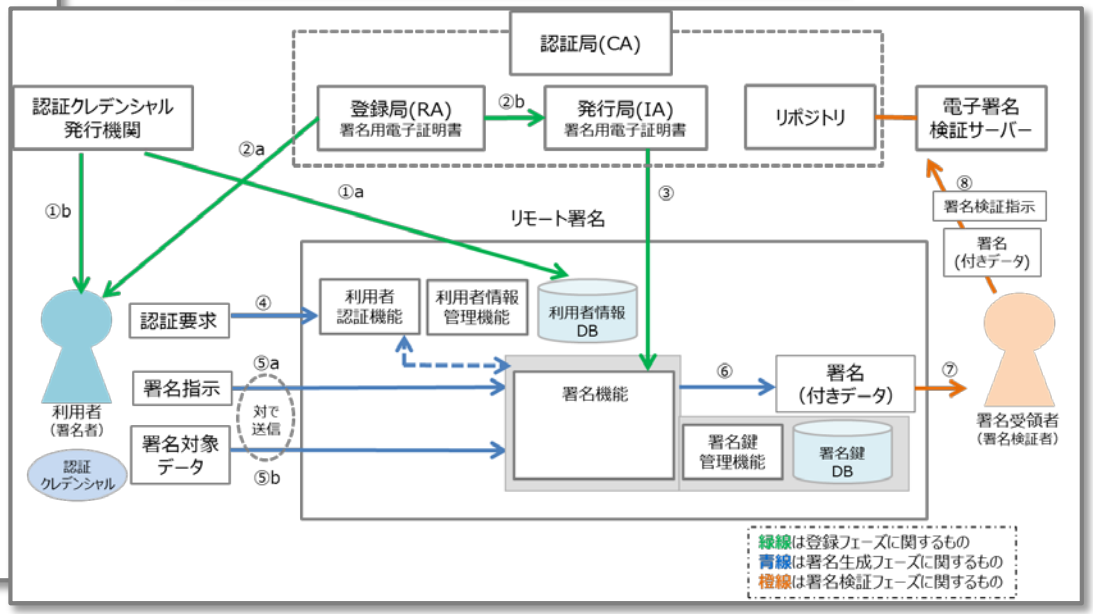
平成２８年３月２５日版

経済産業省

※本資料は、平成２７年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））において、みずほ情報総研株式会社が作成した報告書をもとに作成したものです。

1

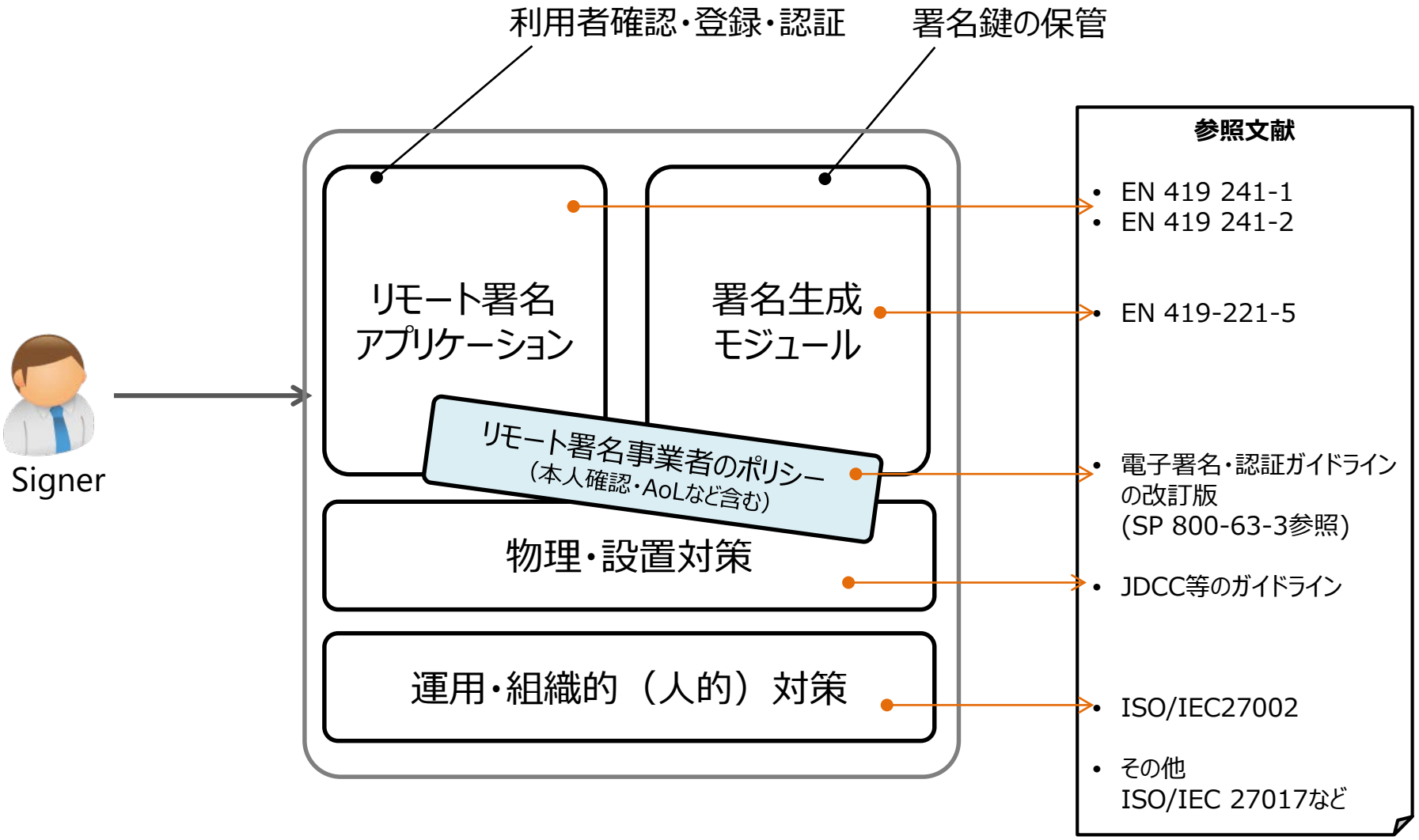




電子署名法研究会（平成27年度第4回） - 配布資料 資料1　調査報告書（平成28年3月25日版）
http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/pdf/h27_004_01_00.pdf

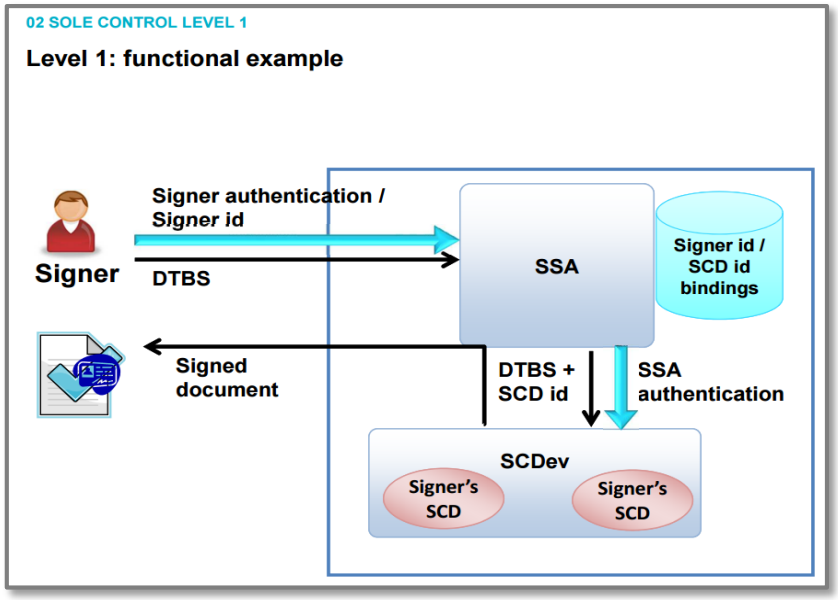
ガイドラインの作成に向けて検討中

TFでの議論内容



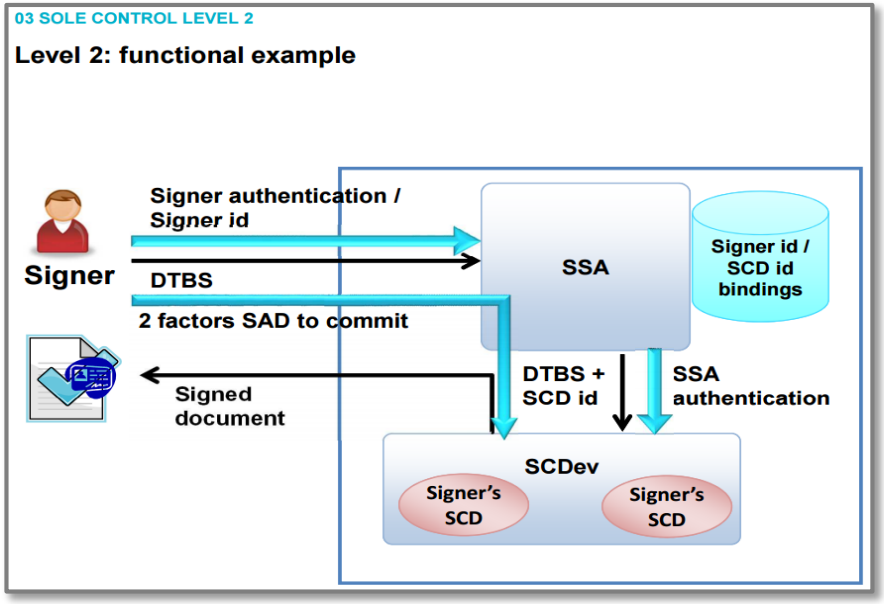
欧州の例（アプリケーションを信頼するか）

- 欧州では、署名鍵が利用者本人のコントロール下にあることをSole Controlとして規定し、2つのレベルを定めている。
- Level1(右)はアプリケーションを信頼するモデル、Level2(左)はアプリケーションを信頼しないモデルとも言える。



Sole Control Level 1の機能構成例1

署名者(Signer)は、署名アプリケーション(SSA)に対して、自らの識別子である署名者ID(Signer id)と署名対象データ(DTBS)を送るとともに、認証要求を行う。



Sole Control Level 2の機能構成例2

機能構成例1との違いは、2要素認証を行っている点。
（2要素認証は、Sole Control Level 2の要求事項）

SSA：Server Signing Application、署名者：Signer、DTBS：Data to be Signed、
SAD：Signer‘s Activation Data、SCDev：Signature Creation Device

ここで質問

リモート署名ガイドライン作成には、
鍵をクラウドに保管する等、いろいろと考えることがあります。
どれだけ意見がわかれるか？ここで質問します。

質問

- 認証局から融資契約で利用する署名鍵を購入して、その鍵を電子契約サービス事業者に預けました。
- 後日、もっと安価な電子契約サービス事業者を見つけたので、サービス移行します。
- あなたは、預けた鍵を移動させますか？

回答

1. 新たに利用する電子契約サービス事業者に鍵を移動させる。
2. 安全ではないので移動させず、新たに鍵を購入する。
3. 1・2以外（そんなの知るかを含む）。

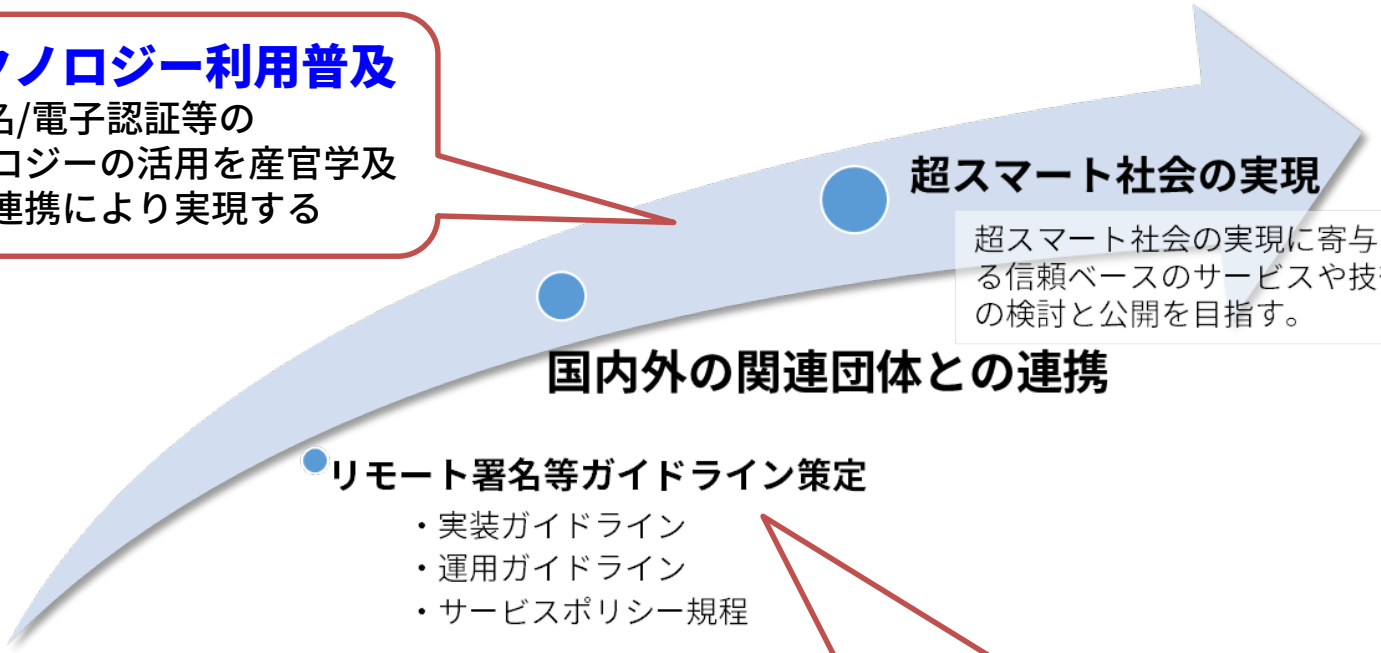
日本トラストテクノロジー協議会

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
副代表者	松本 泰 セコム株式会社 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/リモート署名TF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技術等の検討を行い、より信頼できる電子社会の促進に寄与する。

日本トラストテクノロジー協議会

JT2A

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



Japan Trust Technology Association

JT2A
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

トラストの在り方について

- 何を証明・信頼したいのか？
- 誰に対して証明・信頼させたいか？

- 誰が確認（監査）しているのか？
- 確認（監査）は何を担保するか？

- 社会実装できるのか？
- 連携は？（産学官・国際連携）