Network Security Forum 2017

リモート署名の検討状況

2017年1月23日

JNSA電子署名WG / みずほ情報総研株式会社
小川 博久

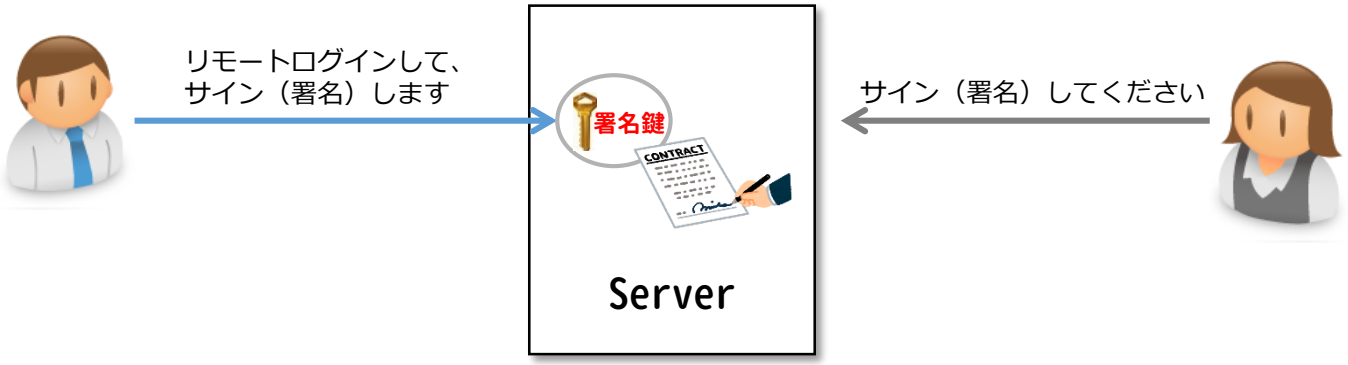
内容

1. リモート署名とは何か？
2. なぜ、リモート署名が重要なのか？
3. 国内の検討は？
4. 海外での検討は？
5. 重要な論点
6. まとめ

1.リモート署名とはなにか？

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。



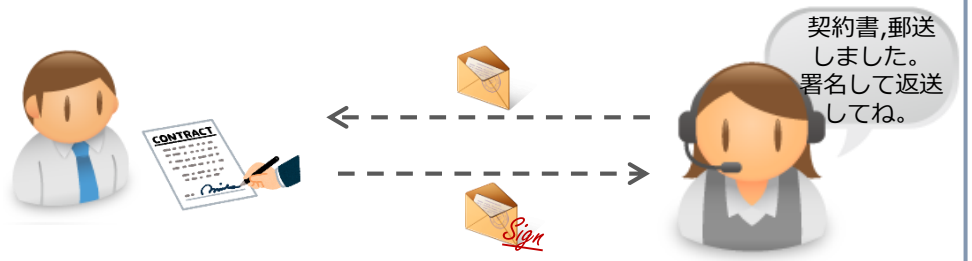
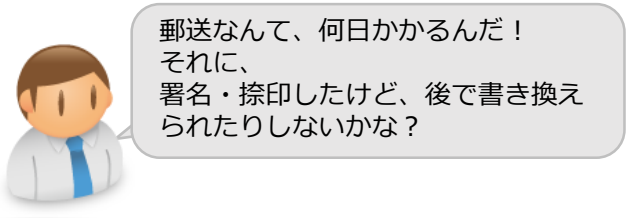
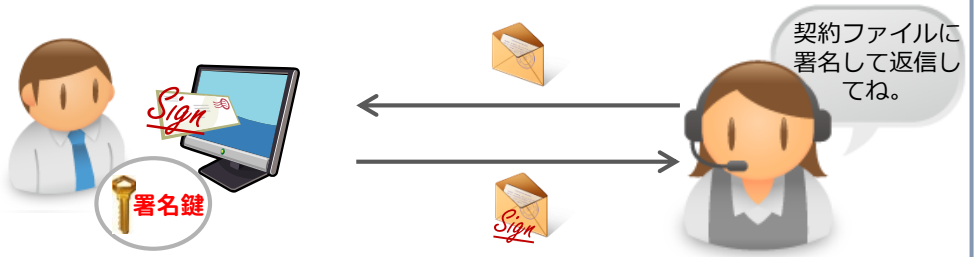
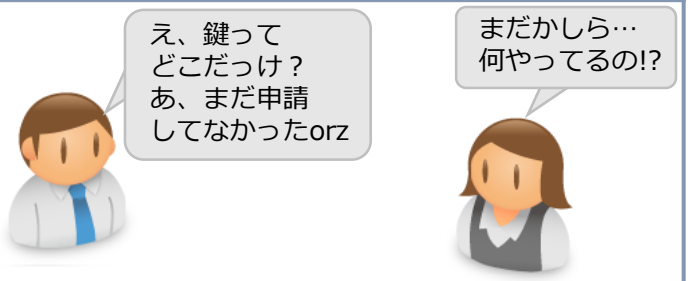
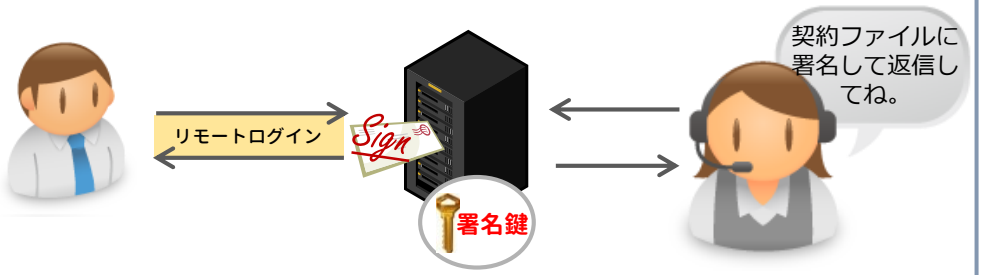
電子署名及び認証業務に関する法律（平成１２年法律第１０２号）第二章　電磁的記録の真正な成立の推定、第三条

電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

※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

1.リモート署名とはなにか？

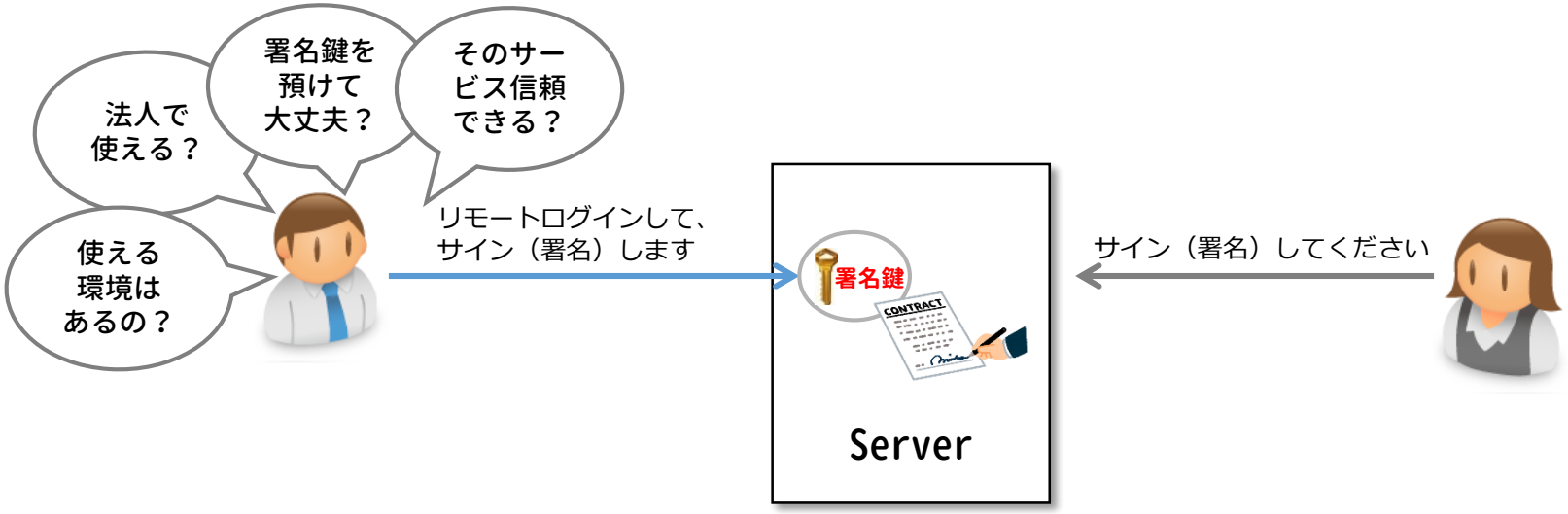
- 紙→電子(ローカル署名)→電子(リモート署名)の簡単な比較イメージ

	処理のイメージ	現実には…
紙の場合		
電子でローカル署名の場合		
電子でリモート署名の場合		

1.リモート署名とはなにか？

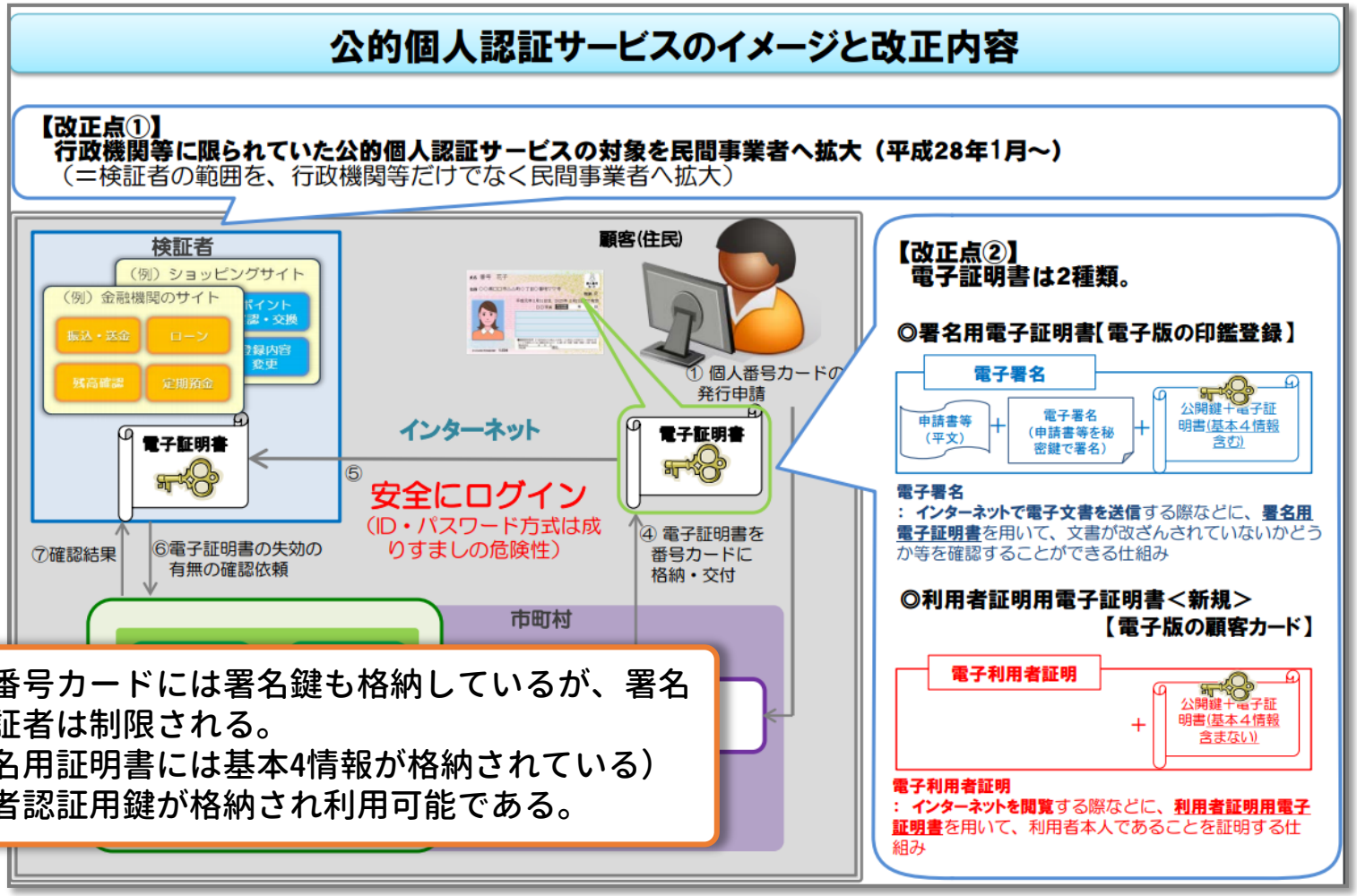
リモート署名の不安

① 契約書に使う署名鍵を預けても大丈夫だろうか？
② そのサービス提供者を信頼してもいいのだろうか？
③ そんなサービスがあっても自分の手元に環境がない？
④ 個人の契約だけで、法人の契約には使えないだろ？



2.なぜ、リモート署名が重要なのか？

- 公的個人認証サービスと個人番号カードの民間利用の拡大で利用できる環境が整う。



- 個人番号カードには署名鍵も格納しているが、署名の検証者は制限される。
- （署名用証明書には基本4情報が格納されている）
- 利用者認証用鍵が格納され利用可能である。

番号制度、個人番号カード及び公的個人認証サービスの概要
http://www.soumu.go.jp/main_content/000378708.pdf

2.なぜ、リモート署名が重要なのか？

- 企業（属性）の鍵としての利用も検討されている。

1. 電子委任状の実現方式の類型

HITACHI
Inspire the Next

- 電子委任状の実現方式を4類型に整理。
- 第3回属性認証検討SWG(1月28日開催)において議論された、電子委任状の種別との対応関係についても整理。

No	実現方式	概要	電子委任状種別※1
①	電子証明書方式	利用者の属性情報を民間認証局の発行する電子証明書に格納する方式	Ⅰ
②	属性情報証明書方式（代表者署名）	利用者の属性情報を属性情報証明書(PDF、XML等の電子的ファイル)に格納する方式。属性情報証明書には、委任者(法人代表者)の電子署名を付与。	Ⅱ
③	属性情報証明書方式（取扱事業者署名）	利用者の属性情報を属性情報証明書(PDF、XML等の電子的ファイル)に格納する方式。属性情報証明書には、電子委任状取扱事業者の電子署名を付与※2。	Ⅲ
④	属性情報DB方式	利用者の属性情報を電子委任状取扱事業者の管理するDBに格納し、これをサービス事業者(電子委任状の受信者)が閲覧する方式。	―

③と④は、電子委任状の受信者から見た場合の属性情報の信頼の対象が一義的には電子委任状取扱事業者となる点では同じと考えられる。

次頁以降に、①～③の実現方式のイメージ、メリット、課題を整理
（課題については、電子委任状取扱事業者の認定要件として特に重要となると考えられる点を抽出）

※1：第3回属性認証検討SWG 資料3-3「電子委任状取扱業務の実務イメージについて(電子認証局会議)」における電子委任状の種別
http://www.soumu.go.jp/main_content/000398182.pdf
※2：現行の電子署名法指針では、民間認証局の発行者署名符号を電子委任状への電子署名に用いることはできない。

電子委任とは、権限者・権利者から、電子的に代理人の委任をすること。

例えば、企業代表者の委任を受け総務部門長が代理で電子署名を行うなど。

「国の調達手続及び電子私書箱における属性認証の実現に向けた調査」の結果 ～電子委任状の実現方式について～
http://www.soumu.go.jp/main_content/000414103.pdf

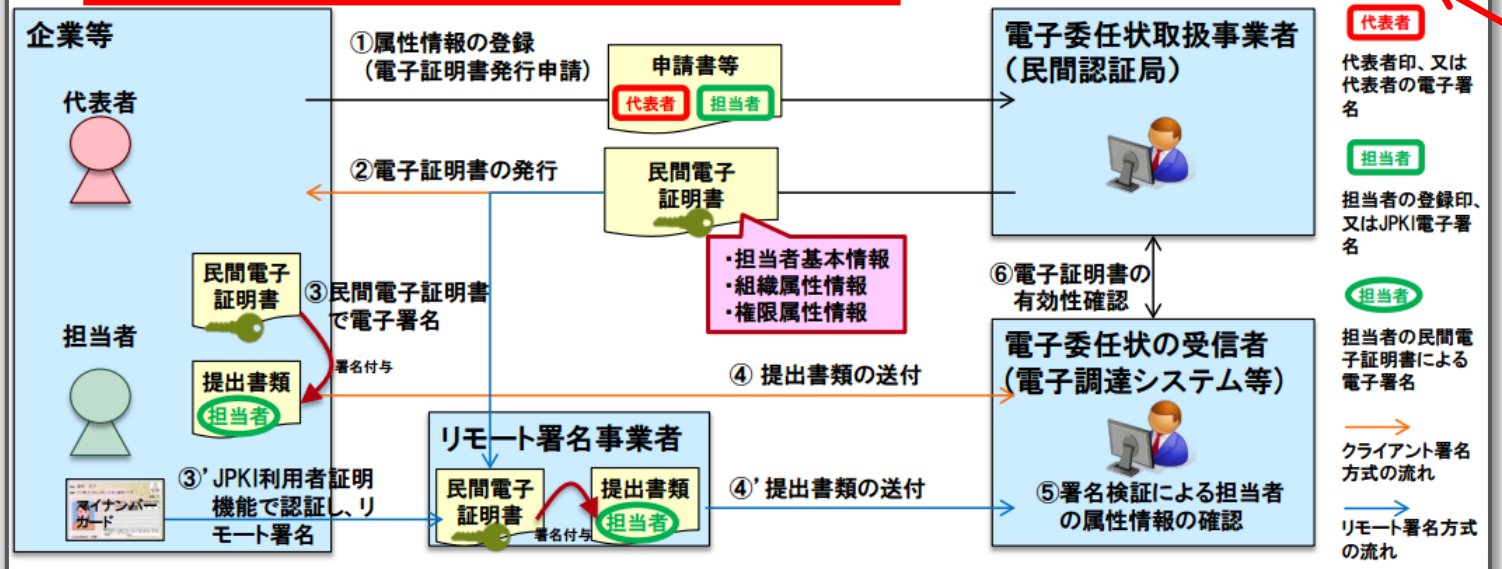
2.なぜ、リモート署名が重要なのか？

- 企業（属性）の鍵としての利用も検討されている。

2-①. 電子証明書方式

HITACHI
Inspire the Next

- 企業等は、電子委任状取扱事業者に対して、紙媒体又は電子媒体で属性情報を登録。
- 企業等は、民間電子証明書を用いて、提出書類に属性情報付きの電子署名を付与。
- 電子署名の実施方法としては、クライアント署名とリモート署名（サーバ署名）があり得るが、権限情報の変更頻度を考えると、リモート署名と親和性が高い※。



リモート署名に関係する内容

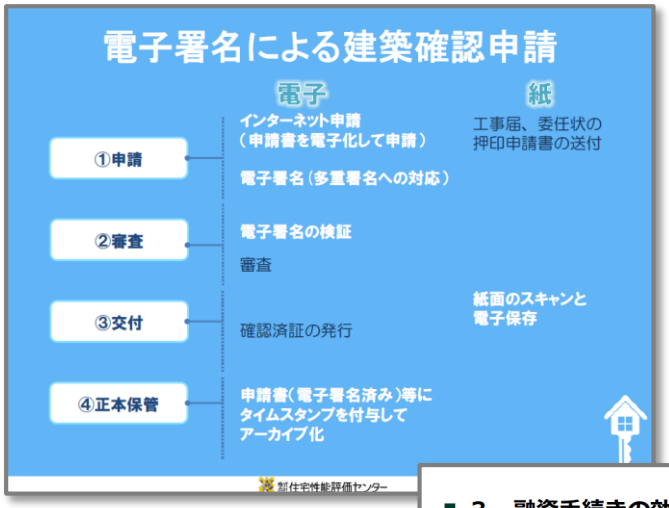
※ICカード方式と比較して、権限情報の変更の都度、電子証明書を書き換える手間が削減される。
また、担当者は、自己のマイナンバーカード1枚のみ管理すればよく、民間電子証明書の保持が不要。

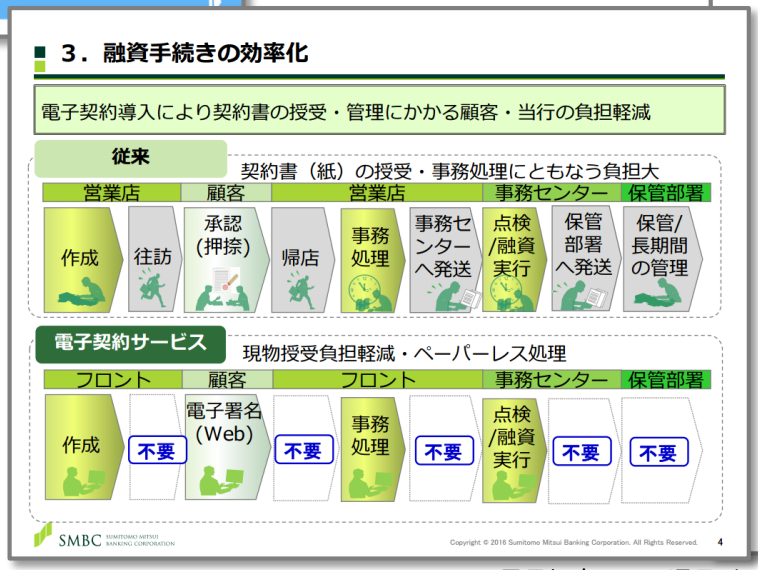
主なメリット	・既存の認証業務の延長線上で実現可能
主な課題	・電子証明書への属性情報(特に権限情報)の記載方法 ・リモート署名の場合の実施要件 ・法人代表者性の確認方法

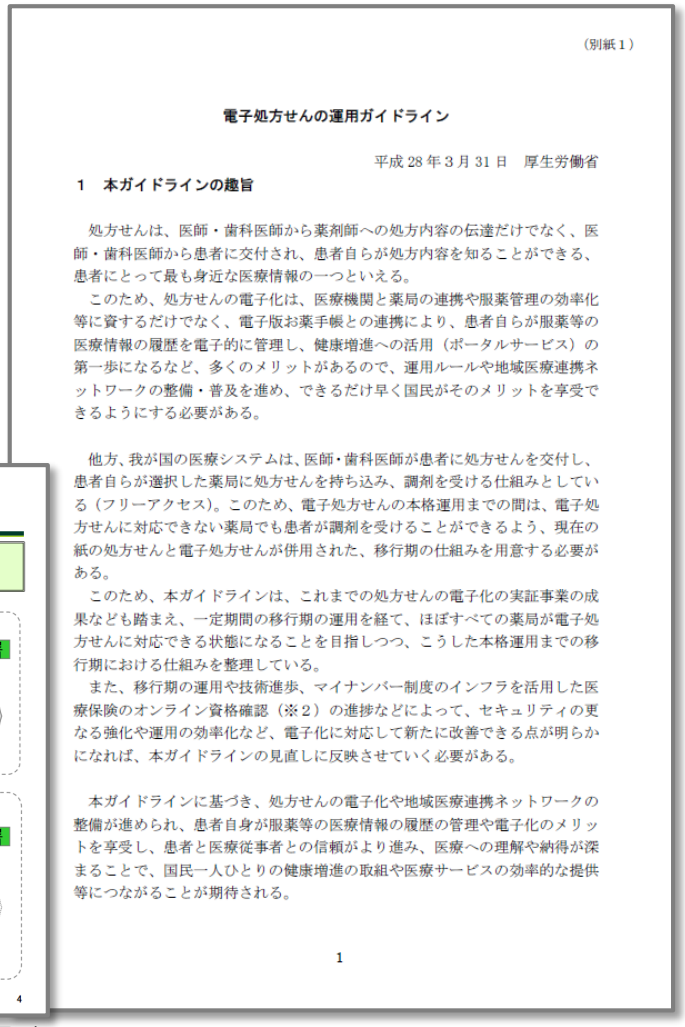
「国の調達手続及び電子私書箱における属性認証の実現に向けた調査」の結果 ～電子委任状の実現方式について～
http://www.soumu.go.jp/main_content/000414103.pdf

2.なぜ、リモート署名が重要なのか？

- すでに、様々な分野で利用されはじめている。







（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

2.なぜ、リモート署名が重要なのか？

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

3. 国内の検討は？

- 経済産業省の電子署名法研究会で、
  昨年度からリモート署名に関する本格的な検討を開始。

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

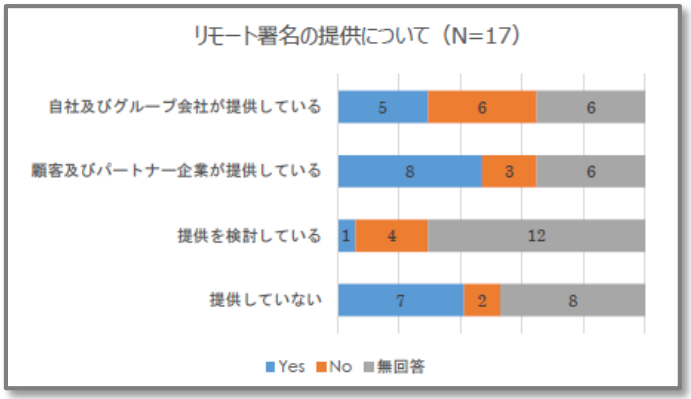
に関する調査研究等））調査報告書

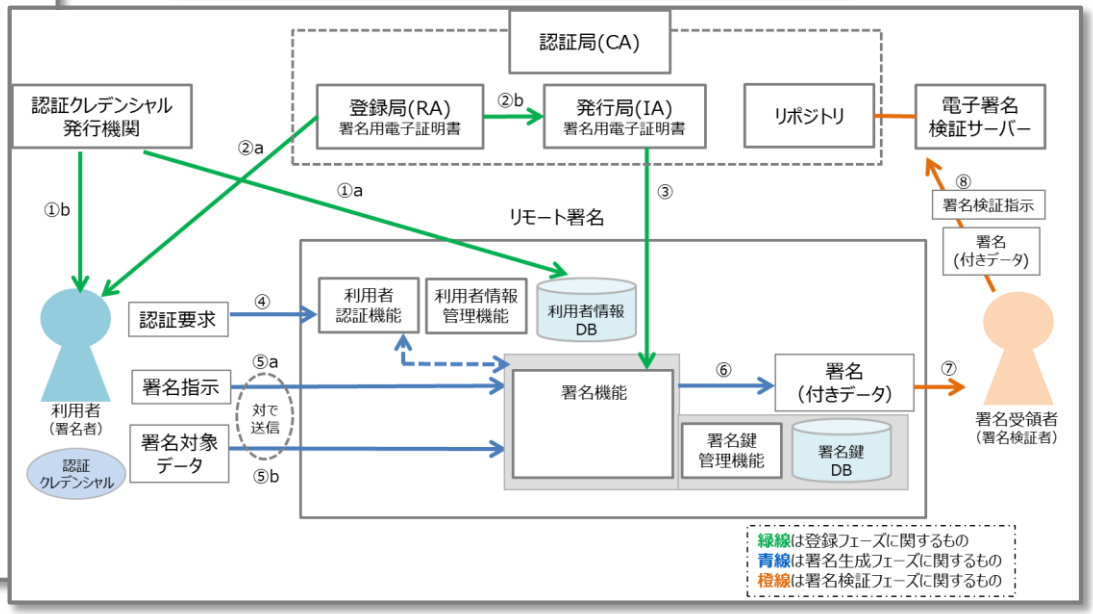
平成２８年３月２５日版

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

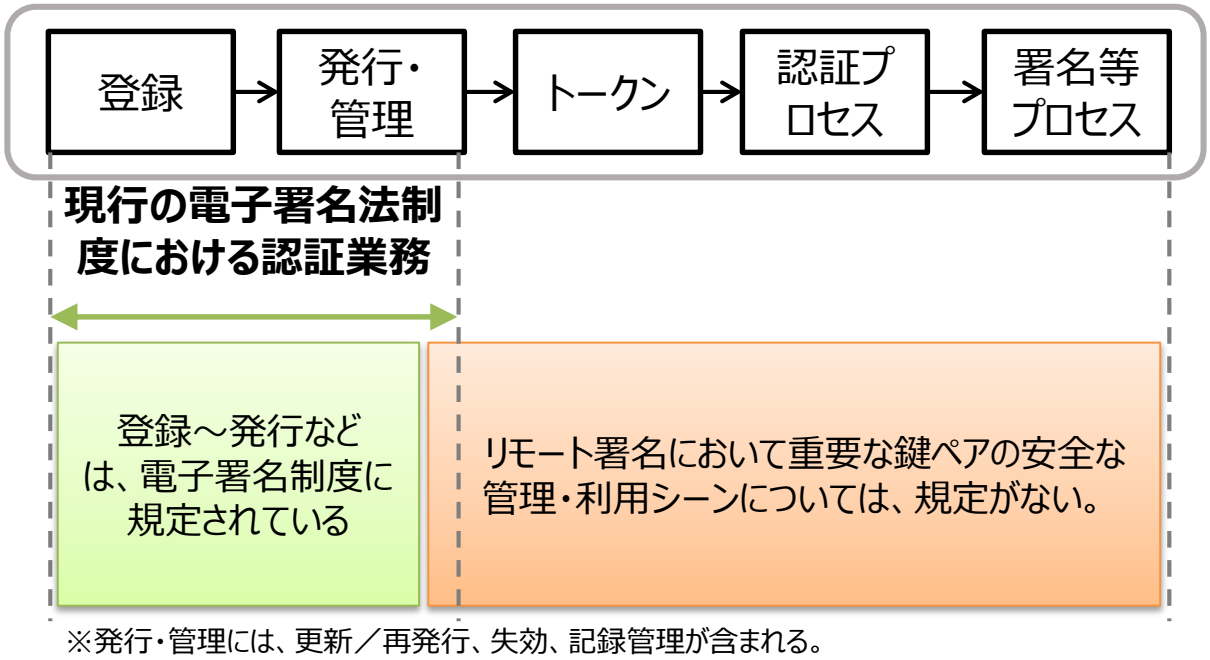
3. 国内の検討は？

- 経済産業省の電子署名法研究会の主な検討項目

検討項目	詳細
Ⅰ．プレイヤ・役割	1.リモート署名のプレイヤ・役割の整理
Ⅱ．リモート署名・提供者	2.リモート署名提供者の要件・保証レベル
	3.署名の利用用途に応じたレベルの検討
	4.リモート署名の構成・設置環境の検討
Ⅲ．リモート署名を行う際に必要な機能	5.署名機能要件
	6.署名検証機能の有無
	7.署名鍵のバックアップ機能の有無
	8.署名生成ログ機能の有無
	9.署名付きデータの送信機能の有無
Ⅳ．登録フェーズ	10.利用者登録方法
	11.利用者の署名鍵の設置
	12.利用者の署名鍵の保護対策
Ⅴ．署名フェーズ	13.署名指示の要件
	14.利用者認証方法
	15.利用者情報と署名鍵情報の保護対策
Ⅵ．その他	16.利用者環境での分散署名処理
	17.利用者による署名対象データの確認
	18.長期署名の適用
	19.電子署名法との関連

3. 国内の検討は？

- リモート署名の利用者登録から署名生成までのプロセスで電子署名法に関係している部分は、ごく僅かである。



リモート署名のプロセスは、電子署名・認証ガイドラインを参考に検討。
※電子署名・認証ガイドライン：各府省情報化統括責任者（CIO）連絡会議決定，オンライン手続におけるリスク評価及び電子署名・認証ガイドライン

3.国内の検討は？

- 主な検討項目の他に、昨年度の電子署名法研究会の議事要旨では、5つの課題があった。

	項目	内容
モデルの違い	(1) 海外モデルとの比較	• 市場優先型の市場モデル（北米）、規制優先型の規制モデル（欧米）がある。 • 日本は電子署名法があるため規制モデル、その規制を適切に改定していかないとイノベーションを阻害する場合もある。
法制度の違い	(2) 電子署名の実施環境が未規定	• 署名鍵の利用環境を定めていない。 • 署名鍵の保管状態を定めていない。
	(3) 認証用途の電子証明書が発行不可	• 認証用証明書を署名用証明書と同じルート鍵から発行できない。
	(4) 官民の法律の違い	• 署名に関する法律は、官民両方ある。 • 認証に関する法律は、官だけある。
フレームワークの違い	(5) 証明書発行対象による認証枠組みの相違	• 日本は、証明書の用途（自然人、法人、Webサイト等）によって認証の枠組みが異なる。

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

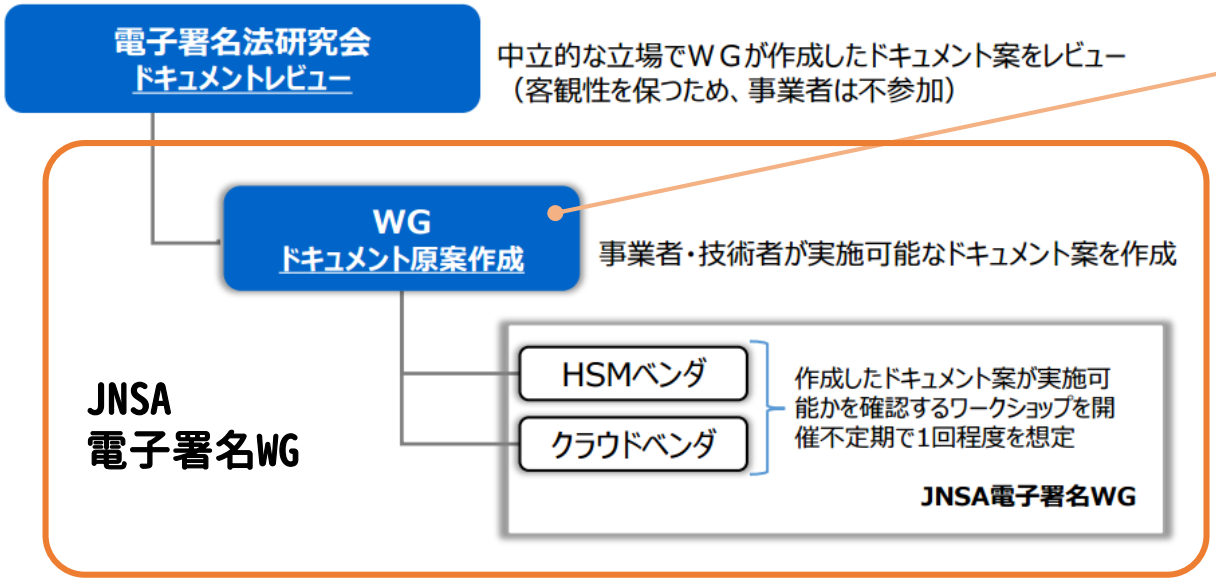
3.国内の検討は？

- 今年度のスコープと検討体制

■スコープ

昨年度における本研究会の報告書において示した、電子署名制度においてリモート署名を実施するための基準に係る大枠について具体化し、それらを明文化したドキュメント（成果物）を作成する。

■検討体制



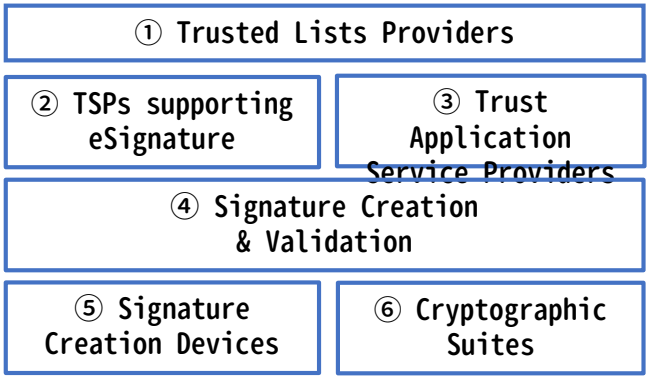
エディタWGの企業・団体

（JNSA電子署名WGの特命TFに設置）

①アドビシステムズ株式会社、②株式会社エヌ・ティ・ティネオメイト、③GMOグローバルサイン株式会社／GMOクラウド株式会社、④株式会社帝国データバンク、⑤一般財団法人日本情報経済社会推進協会、⑥セコム株式会社IS研究所、⑦セイコーソリューションズ株式会社、⑧ジャパンネット株式会社、⑨セコムトラストシステムズ株式会社、⑩株式会社コスモス・コーポレイション、⑪ジェムアルト株式会社、⑫エヌ・ティ・ティ・アドバンステクノロジ株式会社、⑬株式会社シマンテック、⑭三菱電機株式会社、⑮有限会社ラングエッジ、⑯日本電子認証株式会社、⑰タレスジャパン株式会社

４.海外の検討は？

- 欧州では、安全なリモート署名についてPPや評価制度も含めて古くから検討されている。
  eIDAS / eSignature Standards Framework



①～⑤のフレームワークを定義して、多くの規定を検討。
これは、2015年のデータなので、現時点ではさらに詳細化されている。
目が痛くなるほどある…

① TS 119 612 v1.2.1 Trusted Lists
② EN 319 403 / TS 119 403 TSP Conformity Assessment
EN 319 401 / TS 119 401 General Policy Requirements for TSPs
EN 319 411 / TS 119 411 Policy Requirements for TSPs issuing Certificates
EN 319 412 / TS 119 412 : Certificate Profiles
EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
EN 319 422 Time-stamping protocol and electronic timestamp profiles
③ TS 102 640 Registered e-Mail
E_Delivery
Long term preservation
④TS 119 102-1 / EN 319 102-1: Procedures for Creation and Validation of AdES Digital Signatures. Part 1: Creation and Validation.
TS 119 122 / EN 319 122: CAdES digital signatures.
TS 119 132 / EN 319 132: XAdES digital signatures.
TS 119 142 / EN 319 142: PAdES digital signatures.
TS 119 162 / EN 319 162: Associated Signatures Containers.
TS 119 172 / EN 319 172-1: Signature policies
⑤ EN 419 211-1 to -5: Protection profiles for secure signature creation device
EN 419 221-1 to -5: Protection profiles for TSP Cryptographic modules
TS 419 241 - Security Requirements for Trustworthy Systems Supporting Server Signing
EN 419 241-2 & 3 Protection profiles for Server Signing
EN 419 231 - Protection profile for trustworthy systems supporting time stamping
EN 419 261 Security requirements for trustworthy systems managing certificates and time-stamps
⑥ ETSI TS 119 312: Cryptographic Suites

Overview CEN/ETSI eSignature Standardization including standards for TSP Compliance
https://www.tuvit.de/cps/rde/xbcr/SID-AE27C844-D865FD46/tuevit_en/ca-day-2015-nick-pope.pdf

４.海外の検討は？

	サービスタイプ	説明
1	CA/PKC	証明書発行サービス（適格証明書以外）
2	CA/QC	適格証明書の発行サービス
3	TSA	タイムスタンプトークンを生成、署名するタイムスタンプサービス
4	TSA/QTST	適格証明書を使用して署名するタイムスタンプサービス
5	TSA/TSS-QC	証明書の期限切れとともに失効するタイムスタンプサービス
6	TSA/TSS-dESQCandQES	証明書の期限切れ時に有効性を確認して延長できるタイムスタンプサービス
7	Certstatus/OCSP	OCSP により証明書の有効性状態を応答するサービス
8	Certstatus/OCSP/QC	適格証明書の有効性を応答する OCSP サービス
9	Certstatus/CRL	CRL により証明書の有効性情報を提供するサービス
10	Certstatus/CRL/QC	CRL により適格証明書の有効性情報を提供するサービス
11	RA	身元を確認し、証明書発行サービスに渡す情報を登録するサービス
12	RA/nothavingPKIid	非 PKI の登録サービス
13	ACA	属性証明書発行サービス
14	SignaturePolicyAuthority	証明書発行や署名ポリシーを管理するサービス
15	NationalRootCA-QC	国の適格証明書のルート CA
16	Archiv	アーカイブサービス
17	REM	登録型電子メールサービス
18	EDS	電子配信サービス
19	EDS/Q	適格電子配信サービス
20	PSES	電子署名の保存サービス
21	PSES/Q	適格電子署名の保存サービス
22	IdV	アイデンティティ検証サービス
23	Kescrow	キーエスクロー(鍵預託)サービス
24	PPwd	PIN またはパスワードベースの ID クレデンシャル発行サービス
25	TLIssuer	信頼リストを発行するサービス
26	Unspecified	未規定の信頼サービス

欧州のTSL対象サービス
（ETSI TS 119 612 v1.1.1
）

トラストサービスも
目が痛くなるほどある…

５.重要な論点

電子署名及び認証業務に関する法律（平成１２年法律第１０２号）第二章
電磁的記録の真正な成立の推定、第三条

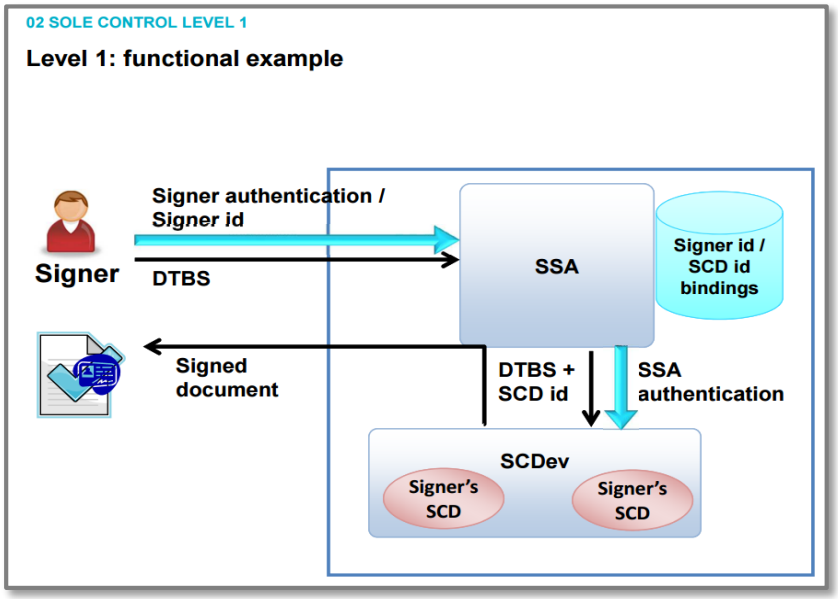
電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

例えば…　（これですべでではありませんが）

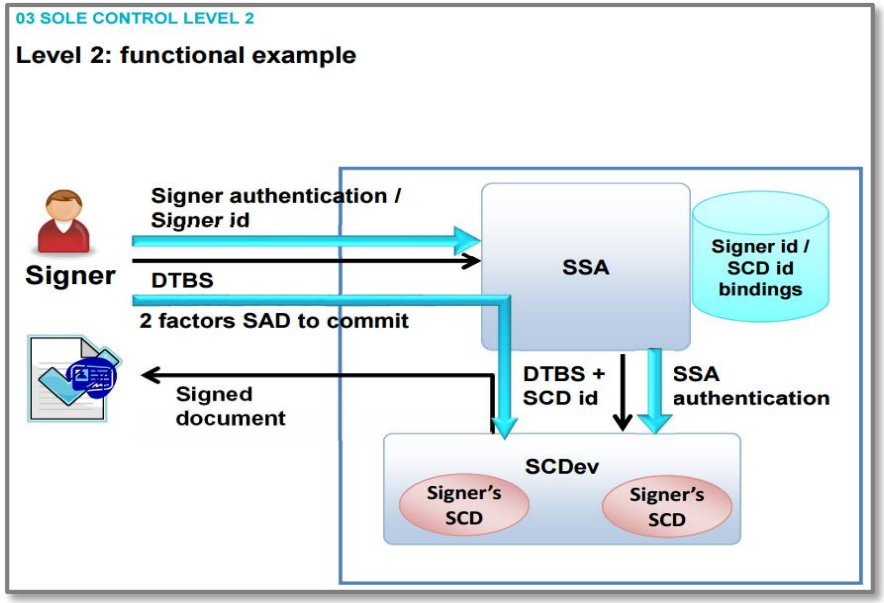
- 利用者（署名者）登録における本人性を確認する
  - 利用者本人でない登録や登録情報の詐称などを防止
- 利用者（署名者）が意図した署名対象データに対して署名
  - 利用者が署名対象データを確認しの確認
  - 利用者による署名結果の確認（検証）
- 署名者しか署名できない
  - 署名鍵が利用者本人のコントロール下にあること（管理者でも勝手に使えないこと）

5.重要な論点（欧州の例）

- 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。



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

まとめ

① 契約書に使う署名鍵を預けても大丈夫だろうか？

➔経済産業省／JNSA電子署名WGの今回説明した検討において、利用者登録の本人確認から署名、検証などの各プロセスに求められる要件を明確化。

② そのサービス提供者を信頼してもいいのだろうか？

➔経済産業省／JNSA電子署名WGの今回説明した検討において、リモート署名サービスに関連する各プレイヤの役割や要件を明確化。

③ そんなサービスがあっても自分の手元に環境がない？

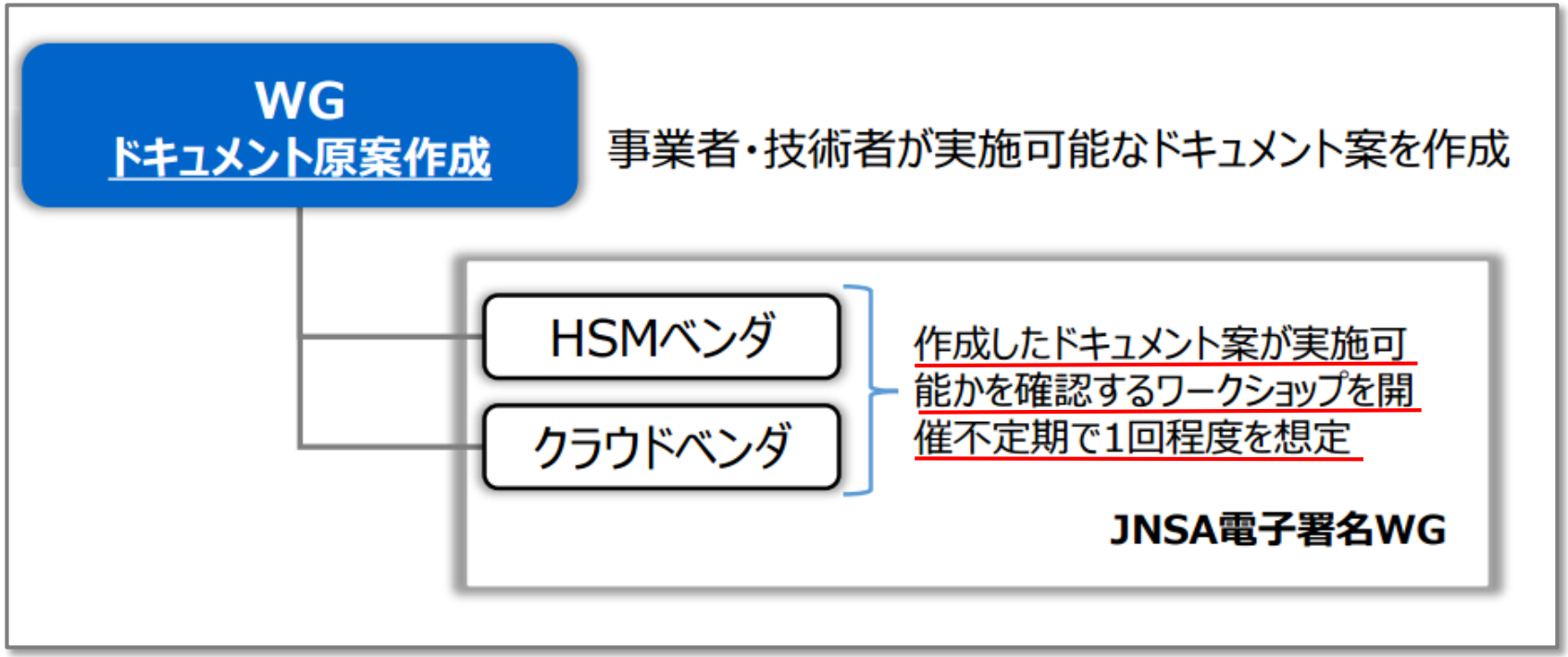
➔公的個人認証サービス等の利用で使える環境が広がる。

④ 個人の契約だけで、法人の契約には使えないだろ？

➔電子委任などにより利用も可能。

最後に重要なこと

- 今年度中に開催するワークショップにご興味のある方は…



①JNSAメールマガジンに登録
http://www.jnsa.org/aboutus/ml.html

②Facebookの「日本ネットワークセキュリティ協会 電子署名ワーキンググループ」をチェック
https://www.facebook.com/eswg.jnsa.org/