

リモート署名の制度化に向けた論点について

令和元年11月8日
事務局

現状とこれまでの議論

- 電子契約サービス等において、リモート署名の利用が進んでいるところ。
- リモート署名は利便性を向上させる一方で、どのような要件を満たせば、本人による電子署名といえるのか、制度的な整理が明確ではない。
- 本人による電子署名といえるためには、リモート環境へのアクセス方法等について、本人だけが行うことができるといえるだけの技術的要件を明確化する必要がある。
- この点については、平成27年度及び平成28年度電子署名法研究会においても検討が行われ、そこでの議論を踏まえ、現在、日本トラストテクノロジー協議会(JT2A)により、EUにおけるリモート署名関連の標準を参照しながら、リモート署名の技術的要件に関するガイドラインの策定に向けた作業が行われているところである。

検討中のガイドラインに盛り込まれる予定の内容

(令和元年8月8日トラストサービスWGにおけるJT2A発表資料より抜粋)

- 署名鍵の生成及び保管はHSM(Hardware Security Module。耐タンパ性を有する頑強なモジュール。)に限定。
- 署名鍵の活性化には複数要素認証を必須化。

- このような状況を踏まえ、本WG中間取りまとめ(令和元年8月9日)において、リモート署名に関する取組の方向性を以下のとおり提言した。

トラストサービスWG中間取りまとめ(抜粋)

第4章 個別論点と取組の方向性 4.1 リモート署名について (4) 取組の方向性

クラウド等を介するリモート署名におけるアクセス方法の技術基準については、経済産業省の電子署名法研究会(平成27年12月～平成29年3月)での検討を踏まえ、トラストサービスに係る技術関連のガイドライン策定などを行っているJT2Aにおいて議論をしているところであり、当該議論も注視しつつ、並行してリモート署名の電子署名法上の扱いについて、主務省において整理することが必要である。

その上で、リモート署名について、特定認証業務と認定認証業務に係る基準の具体化を進めることが必要である。

ローカル署名とリモート署名の違い

ローカル署名

(1) CAが鍵ペアを生成

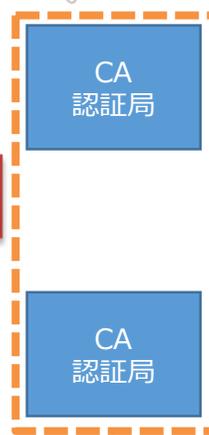


利用者

署名鍵



例: 本人限定
受取郵便



(2) 利用者が鍵ペアを生成



利用者

利用者識別符号

公開鍵



リモート署名

(1) CAが鍵ペアを生成



利用者

契約

署名鍵

本人のみ
利用可

クラウドに記録

(2) RSが鍵ペアを生成

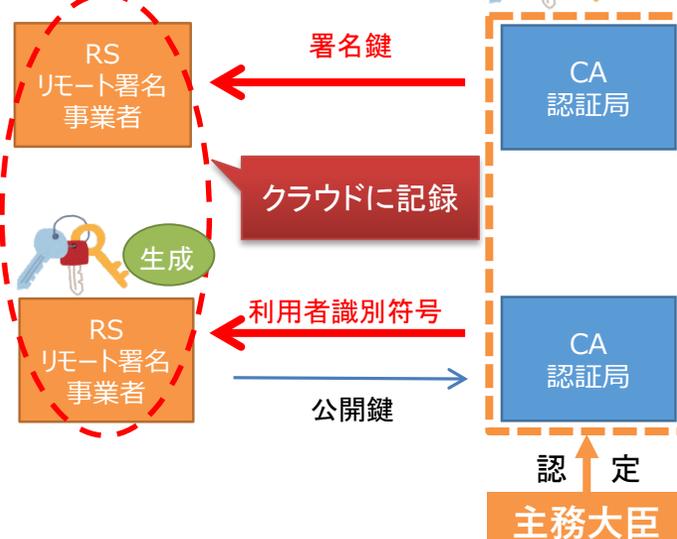


利用者

契約

利用者識別符号

公開鍵



署名鍵や利用者識別符号を「安全かつ確実に利用者
に渡すことができる方法」により交付

リモート署名においては、署名鍵や利用者識別符号を利用者が委託す
る事業者のサーバに記録することにより行われる。

論点

現行の電子署名法及び認証業務の認定制度を前提に、リモート署名を電子署名法制度上どのように位置づけることができるか。その前提として、今後、関係者によるどのような取組が必要か。

取組の方向性に関する検討

- JT2Aにおいては、特に以下の事項に留意しながら、ガイドラインの策定・公表に向けた検討作業を継続することが適切ではないか。
 - 利用者やリモート署名サービスを提供する事業者にとってもわかりやすいものとなるよう、ガイドラインが前提とするリモート署名の仕組みやガイドラインの対象範囲、専門用語についての解説を充実させること
 - 事業者がガイドラインに適合するかどうかの評価を外部から行いやすくなるよう、具体的な要求事項を単なる規格や標準のような形よりも詳細かつわかりやすく提示すること
- 信頼の置けるリモート署名サービスの普及に向け、ガイドラインに適合する事業者を利用者が容易に判別可能となるような、事業者のガイドラインへの適合性評価を第三者が行う民間の自主的な仕組みを設けることが有用ではないか。
- 利用者が本人による電子署名として利用可能な信頼できるサービスを利用できるようにし、利用者によるリモート署名の円滑な利用を図るため、JT2Aのガイドラインの策定・公表や自主的な適合性評価の仕組みの整備を受け、リモート署名の電子署名法制度上の位置づけについて、主務省において以下の取組を進めながら検討することが適切ではないか。
 - JT2Aにより策定されるリモート署名に関する技術基準の内容の精査
 - 当該技術基準及び適合性評価の仕組みの運用状況のモニタリング
 - 当該技術基準及び適合性評価の仕組みやそれらの運用状況を踏まえ、リモート署名の電子署名法上の電子署名への該当性、同法第3条の規定による真正成立の推定効の適用の可否及び認証業務の認定基準との関係の整理に関する検討