

リモート署名について

株式会社コスモス・コーポレーション
濱口 総志

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

発表内容の概要

1. リモート署名の必要性
2. リモート署名に関する法律上の課題
3. リモート署名に関する技術上の課題
4. 今後に向けた提言

リモート署名の必要性

電子署名は電子文書の真正な成立を保証するデジタル社会に必要な仕組みであるが、一方で秘密鍵を署名者が管理する必要があり、その安全な運用には利便性が犠牲となるケースが多い。

この課題を解決する方式が、秘密鍵を署名者に代わって事業者が管理するリモート署名である。リモート署名では、署名者はリモート署名サービスに対してユーザ認証(電子的な本人確認)を行うことによって、リモート署名サービスが管理する署名者の秘密鍵を利用し、電子署名を遠隔で生成することができる。

リモート署名は、既に欧米及び我が国でも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している。

欧州でも、適格電子署名*1についてセキュリティ評価を受けたICカード*2の利用を要求していたことから、適格電子署名の普及が進んでいなかったが、eIDAS規則によって適格電子署名をリモート署名で実現することが可能となった。

➡あらゆる電子署名をリモート署名に置き換えることが可能に。

我が国のリモート署名については、主としてB2Bにおける電子契約で利用されているが、認定認証業務の証明書をリモート署名で安全に利用する為の環境は整っていない。また、リモート署名の法的安定性には未だ課題がある。

➡認定認証業務相当の信頼性をリモート署名で保証することに課題がある

*1 適格電子署名: eIDAS規則によって手書き署名と同等の法的効力を持つと定められている電子署名

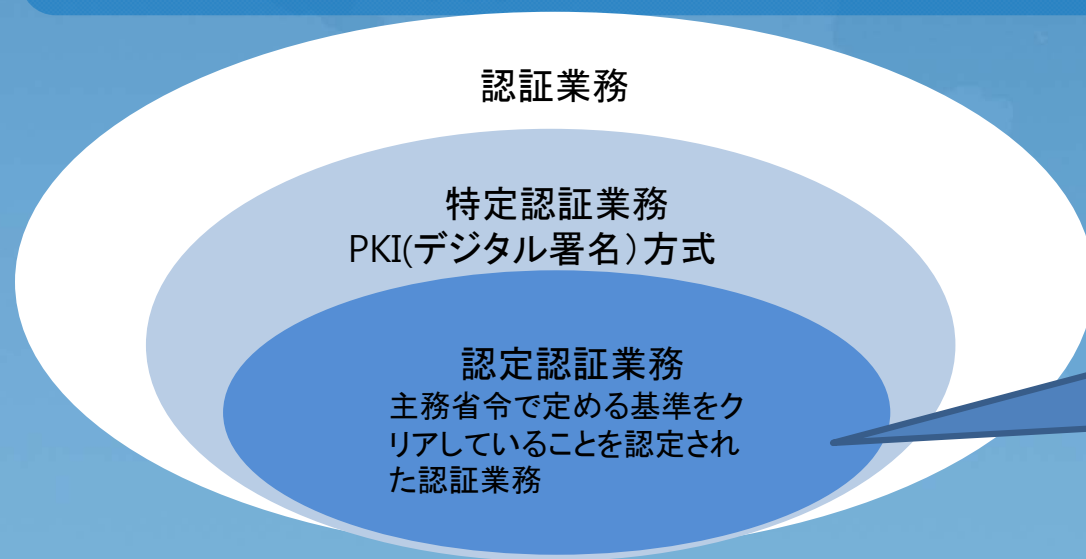
*2 ISO/IEC 15408 (コモンクライテリア) による評価/認証を受けたICカード

リモート署名の必要性

一般の認証業務に基づく電子署名の用途
電子契約、ワークフロー等(主としてtoB)

認定認証業務に基づく電子署名の用途
一般の認証業務に基づく電子署名の用途に加えて、電子入札、電子申請、電子納税、e文書法 (主としてto G)

欧州のリモート署名(適格電子署名)の用途
保険契約、金融契約、電子申請、雇用契約 (to B(特に規制産業)及びto G)



わが国には認定認証業務相当の信頼性をリモート署名で保証できる制度がなく、高い信頼性を求める電子申請や、規制産業におけるリモート署名の採用に課題がある

- 
1. リモート署名の必要性
 2. リモート署名に関する法律上の課題
 3. リモート署名に関する技術上の課題
 4. 今後に向けた提言

リモート署名に関する法律上の課題

紙文書の証拠力における二段の推定

[一段目の推定]

最高裁判例 昭和39(オ)71

私文書の作成名義人の印影が当該名義人の印章によつてされたものであるときは、反証のないかぎり、該印影は本人の意思に基づいて顕出されたものと事実上推定するのを相当とするから、民訴法第三二六条により、該文書が真正に成立したものと推定すべきである。

→私文書の作成名義人本人の印影があれば、作成名義人の意思を事実上推定できる。

[二段目の推定]

民事訴訟法第228条第4項

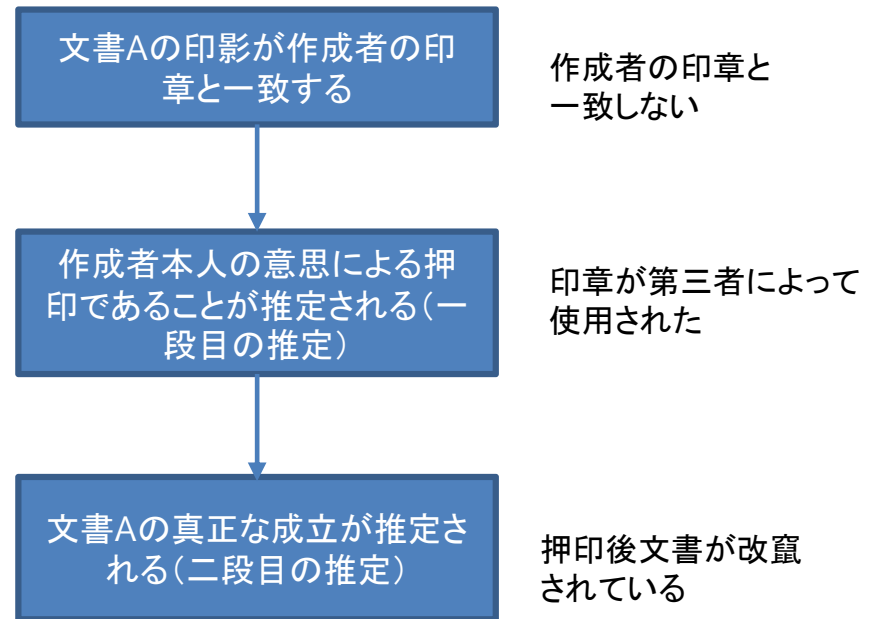
私文書、本人又はその代理人の署名又は押印のあるときは、真正に成立したものと推定する。

→上記一段目の推定により、作成名義人の意思が推定できるので、文書に署名又は押印があることで、真正な成立が推定される。

一段目、二段目共に事実上の推定であり、反証のハードルがそれ程高くない

二段の推定

反証例



Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

リモート署名に関する法律上の課題

[電子署名法における推定項]

電子署名法第二章第三条

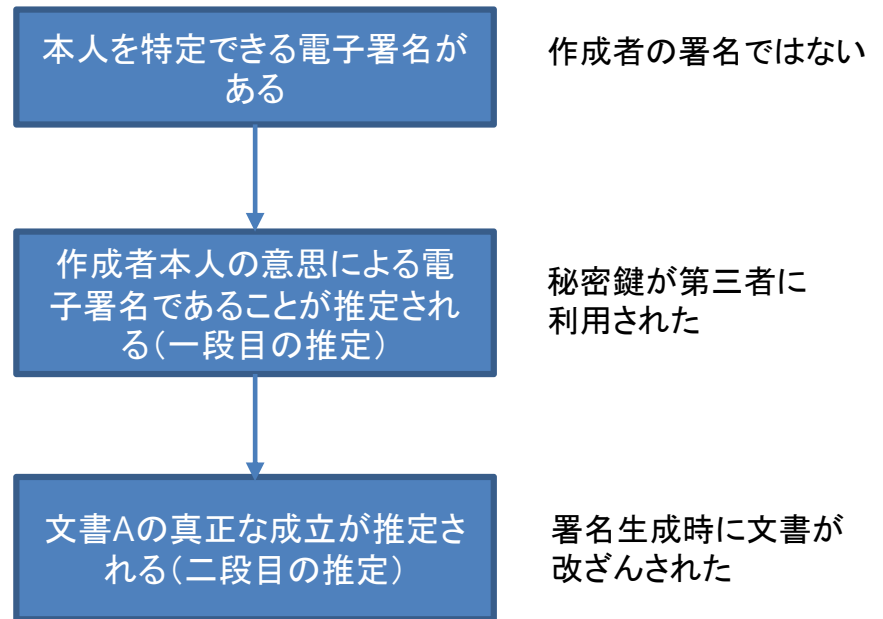
電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

→電子文書の場合、符号及び物件の適正な管理することで、本人だけが行える方式の電子署名が行われていれば、電子文書の真正な成立が推定される。

[課題] リモート署名では利用者の秘密鍵を第三者が管理するが、その場合であっても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。）と言えるか。

電子文書における推定

反証例

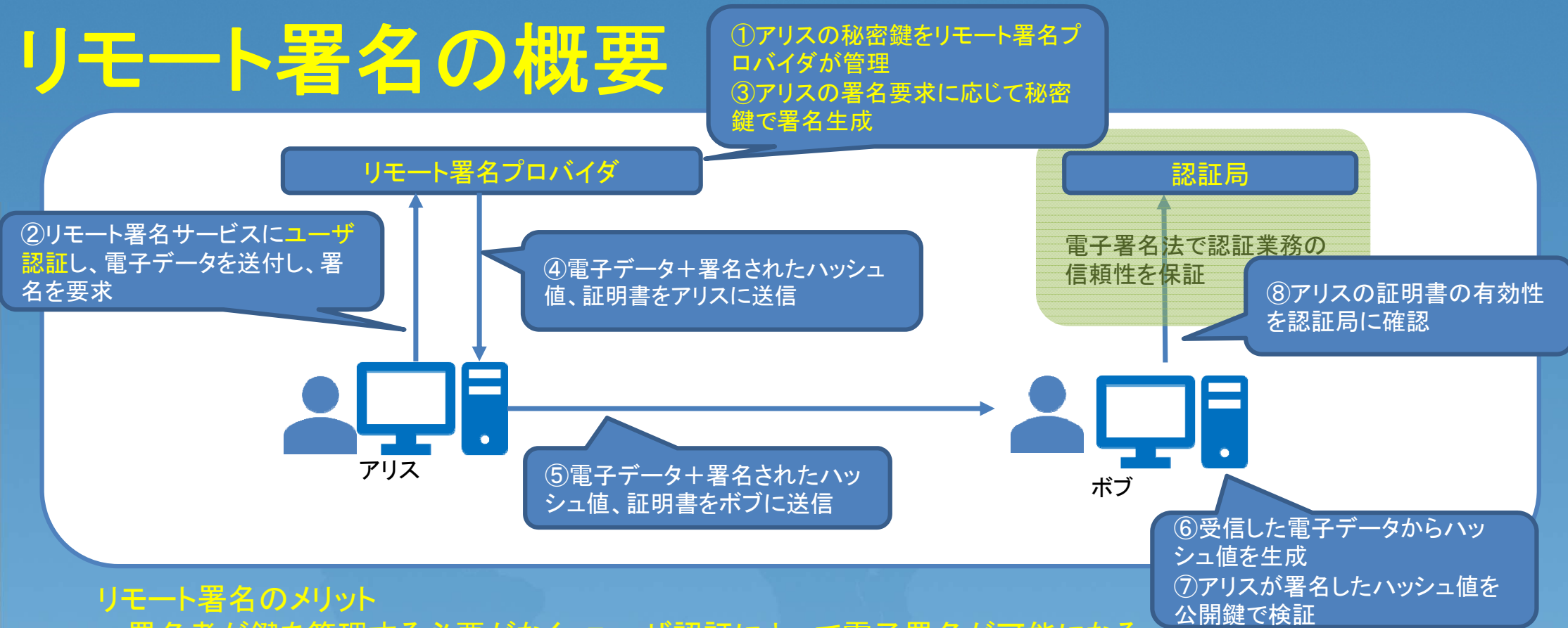


Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

- 
- A faint world map is visible in the background of the slide, rendered in a light blue color that matches the overall theme.
1. リモート署名の必要性
 2. リモート署名に関する法律上の課題
 3. リモート署名に関する技術上の課題
 - a. ユーザ認証と記録管理
 - b. 鍵管理と事業者の信頼性
 4. 今後に向けた提言

リモート署名の概要



リモート署名のメリット

- 署名者が鍵を管理する必要がなく、ユーザ認証によって電子署名が可能になる。
(電子署名の利便性が認証と同等になる)
- 秘密鍵をリモート署名プロバイダによって安全に管理してもらうことで、OS上での管理と比較し、より安全な運用が可能になると考えられる

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

技術上の課題 ユーザ認証と記録管理

秘密鍵を署名者自身が管理するローカル署名と比較して、リモート署名が同程度の信頼性が確保されているという為には、少なくとも以下の2点を保証する必要があると考えられる。

1. リモート署名事業者が管理する秘密鍵を署名者が利用する際に署名者が特定され、署名者の意思が推定できること
2. 署名者の秘密鍵が、当該署名者の意図した使用以外に用いられないこと

1、について、ローカル環境では、署名者が秘密鍵を管理する為、署名者の秘密鍵によって電子署名が生成された場合、署名者による電子署名であることが類推できるが、リモート署名の場合には①第三者の管理する署名者の秘密鍵を利用したユーザが確かに署名者であること、及び、②署名者が署名意思をもって秘密鍵を利用したことをリモート署名事業者が保証する必要がある。

このため、リモート署名サービスにおいて、秘密鍵の利用時に確かなユーザ認証と署名要求の記録が必要となると考えられるが、国内において信頼できるユーザ認証の技術的基準が存在しない為、どのユーザ認証の方式を採用すればよいか、どこまで記録を管理すればよいか不明確である。

[課題]秘密鍵利用時のユーザ認証及び記録管理の技術基準が存在しない

ユーザ認証技術の例:ID+パスワード、OTP、生体認証、PKI

記録管理(保管期間、記録対象データ、記録方法等)

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

技術上の課題 ユーザ認証と記録管理

ユーザ認証の基準例

- ・認証手段発行の為の本人確認には以下の何れかの本人確認資料を用いること。(免許証、パスポート、マイナンバーカード等)
- ・多要素認証を用いること
- ・中間者攻撃、リプレイ攻撃等の既知の攻撃手段に耐性のある認証プロトコルを用いること
- ・認証手段は署名者に安全に送付されること
- ・認証手段を活性化データを用いて個人化する場合、活性化データは安全に用意され、認証手段の送付とは別の手段で送付されること等

記録管理の基準例

- ・少なくとも以下のイベントの記録対象とすること
 - ・本人確認
 - ・システム環境に重大な影響を及ぼすイベント、及び鍵管理(鍵生成、使用及び破棄)に係るイベント
 - ・署名処理、
 - ・ユーザ認証 等
- ・保存期間は署名者の証明書の有効期限後、少なくとも10年間とする
- ・記録の不正な変更を防ぐために完全性を保証する機能を用いること等

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

技術上の課題 鍵管理と事業者の信頼性

1. リモート署名事業者が管理する秘密鍵を署名者が利用する際に署名者が特定され、署名者の意思が推定できること
2. 署名者の秘密鍵が、当該署名者の意図した使用以外に用いられないこと

リモート署名事業者は、署名者が秘密鍵を署名意思を以て利用したに加えて、①当該秘密鍵が署名者以外によって利用されないこと、また、②署名者の意図した使用以外に用いられないこと保証する必要があると考えられる。

其の為には、以下が必要となる。

- a. 署名者の秘密鍵の保護
- b. リモート署名事業者の信頼性保証

[課題] リモート署名の為の鍵管理とリモート署名事業者の信頼性に関する基準がない

a.については、署名者の秘密鍵の運用に関する技術基準が必要になる。

例えば：秘密鍵を格納するHSMの基準、秘密鍵の活性化方法に関する基準（活性化の為の情報を署名者のみが管理すること望ましい）、HSMの運用基準等がある。

b.については、リモート署名事業者の運用基準が必要になる。

例えば：署名対象文書の完全性保護の為の基準、中立性の基準、サービス運用時のセキュリティ基準等

* HSM（ハードウェアセキュリティモジュール、鍵を安全に管理／運用する為のハードウェア）

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

技術上の課題 鍵管理と事業者の信頼性

鍵管理の基準例

- ・署名者の鍵生成及び鍵の使用はHSM内で行われること
 - ・署名鍵のバックアップは必要最小限とすること
 - ・バックアップは暗号化され、機密性及び完全性についてHSM内と同等の保護を保証すること
 - ・セキュリティ評価を受けたHSMを用いること
 - ・署名者のみが署名鍵を活性化できる機能を用いること
- 等

事業者の信頼性の基準例

- ・署名対象文書の完全性を保護すること
 - ・サービス運用方針文書を作成し、公開すること
 - ・リモート署名サービス運営に係る役割と権限を適切に定めること
 - ・リモート署名サービス運営に係る要員は、業務に必要な知識を所持していること
 - ・リモート署名サービス事業者は財政的に安定していること
 - ・リモート署名サービス運営に係る要員の公平性に係るリスク評価を行うこと
- 等

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

技術上の課題整理

リモート署名がローカル署名と同水準の信頼性を得る為に必要と思われる条件	条件を充足する為にリモート署名事業者に必要なこと	必要な技術基準
リモート署名事業者が管理する秘密鍵を利用する際に署名者が特定され、署名者の意思が推定できること	第三者の管理する署名者の秘密鍵を利用したユーザが確かに署名者であることを保証	ユーザ認証 (署名者を特定できる認証方式等)
	署名者が署名意思もって秘密鍵を利用したことを保証	記録管理 (保管期間、記録対象データ、記録方法等)
署名者の秘密鍵が、当該署名者の意図した使用以外に用いられないこと	当該秘密鍵が署名者以外によって利用されないことを保証	鍵管理 鍵のライフサイクル管理(生成、活性化、削除、バックアップ等)
	署名者の意図した使用以外に用いられないことを保証	信頼性 (署名対象文書の完全性保護の為に基準、サービス運用時のセキュリティ基準、中立性の基準等)

[課題]技術上の課題が解消されていることを保証する為の制度がない

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

JNSA及びJT2Aでの検討

- 2016年 リモート署名検討開始
 リモート署名に係るプレイヤの整理、ローカル署名との差異分析
 リモート署名のライフサイクル及び処理フェーズの整理(登録、署名、署名検証、利用停止)
 各フェーズにおけるプレイヤの役割整理
 リモート署名のモデル整理
 リモート署名の構成を検討
- 2017年 リモート署名ガイドラインの全体構成を議論
 11月 JT2A設立準備会発足
- 2018年 6月 JT2A設立
 リモート署名の活用に関する調査・検討
 リモート署名の活用に関し、アーキテクチャや法的論点を含め調査・検討を実施
- 2019年 5月 ガイドライン(案)の完成を目的とした編集会議開催予定
 6月～ 関係省庁と意見交換

- 
1. リモート署名の必要性
 2. リモート署名に関する法律上の課題
 3. リモート署名に関する技術上の課題
 4. 今後に向けた提言

今後に向けた提言

①技術基準の整備(ユーザ認証、記録管理、鍵管理及び信頼性等の基準)

リモート署名サービスについてローカル署名と同等の信頼性を得る、或いは、「本人による署名」と見なす為の技術要件を整備することで、リモート署名サービスにおいて事業者が達成すべきセキュリティ水準を明確化すべきである

②技術基準への適合性を保証する制度(監査／認定制度)

①の技術基準への適合性を保証する制度が法令によって定められ、リモート署名が署名者の意思に基づいて行われたことを容易に証明可能な環境を整備すべきである

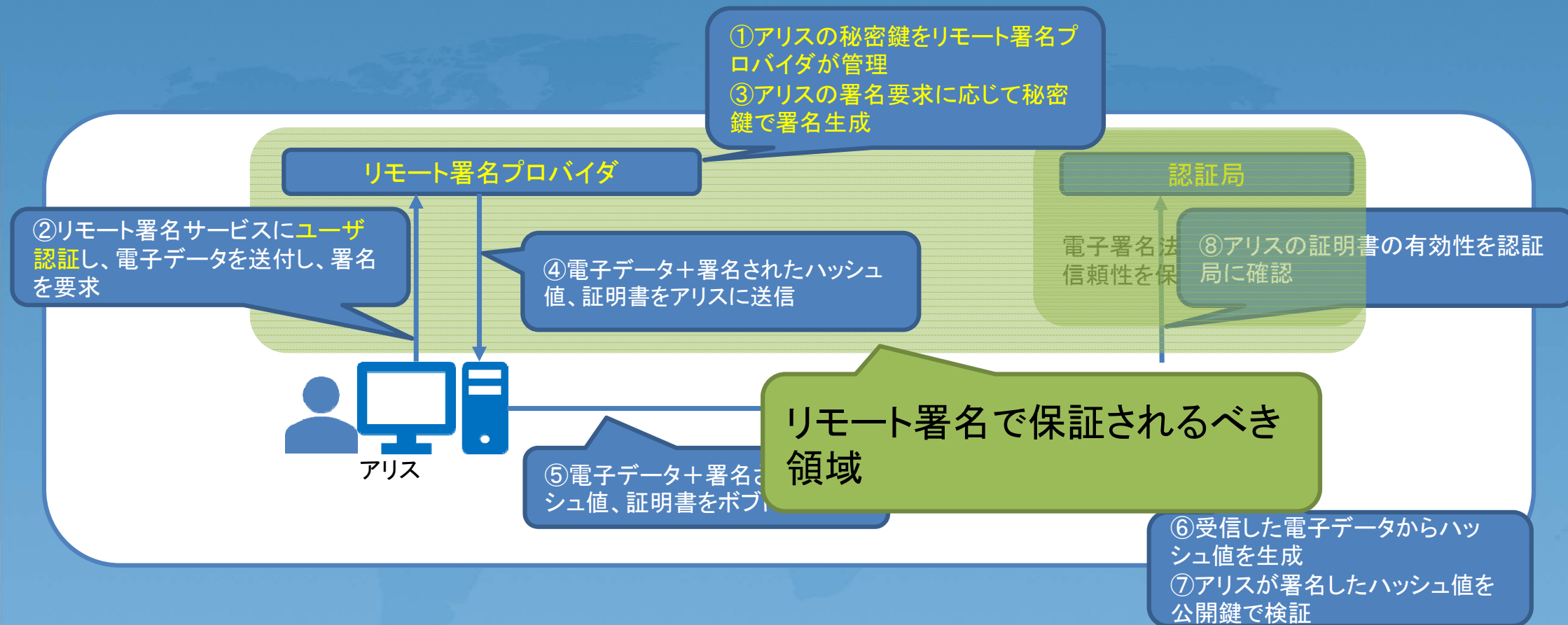


JT2Aで作成中のリモート署名ガイドラインをベースに技術基準を整備し、法令等により電子署名法における認証業務の認定制度と同等の監査／認定制度をリモート署名に対しても整備すべきである

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

今後に向けた提言



Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

ご清聴ありがとうございました

株式会社コスモス・コーポレーション

ITセキュリティ部

濱口 総志

Tel: 0598-30-5911

E-Mail: s.hamaguchi@cosmos-corp.com

URL: www.safetyweb.co.jp/

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING