資料4

JPKI（署名用証明書）により本人確認を行った民間の電子証明書の利用検討

2021年3月3日

電子認証局会議　理事
セコムトラストシステムズ株式会社
西山　晃

ー　アジェンダ　ー

1. 日本の認証局の概要
2. JPKIにより本人確認を行った民間電子証明書の利用
3. 【参考法令】電子申請で利用可能な電子証明書の規定例
4. 認証局の信頼性の確認とは？
5. 認証局の信頼性の確認方法（Trust Representation）
6. ブリッジモデルによる相互認証
7. ブリッジモデルによる相互認証の論点
8. リストモデルによる相互認証
9. リストモデルによる相互認証の論点
10. JPKIを活用した今後の民間CAのユースケース
11. まとめ

1. 日本の認証局の概要

➢ 政府ブリッジCAモデルと階層型CAモデル

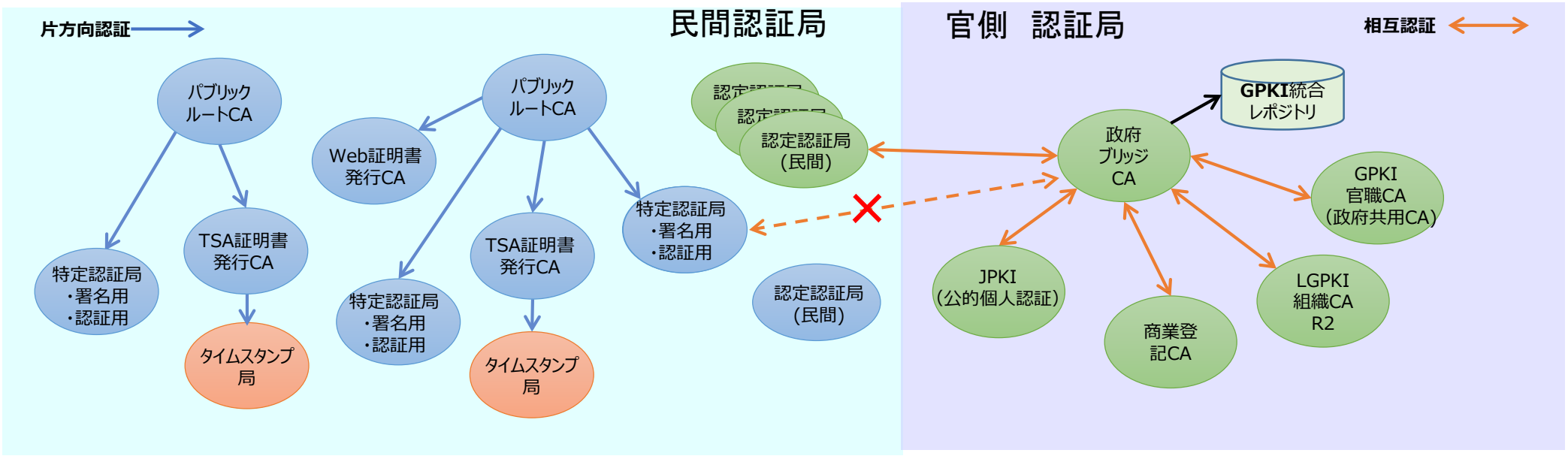
・日本では認証局の信頼モデルとして、電子政府のブリッジモデルと、パブリックルートをトラストアンカーとする階層型モデルがある。
・政府ブリッジCAと相互認証できる民間認証局は電子署名法の認定を受けた認定認証局に限られている。

パブリックルート認証局*をトラストアンカーとする階層型CAモデルなど

・電子署名法に基づく認定認証局は政府ブリッジCAに接続することができる

政府ブリッジCAモデル

・政府ブリッジCAに接続、トラストアンカーとして保証される。



*WebTrust for　CA監査、ESTI監査を受け、「信頼ある第三者認証機関」としてブラウザーに登録された認証局

2. JPKIにより本人確認を行った民間電子証明書の利用

➢ 電子申請で利用可能な電子証明書

・政府電子調達（GEPS）や国税電子申告（eTAX）などの電子申請で利用可能な電子証明は「情報通信技術を活用した行政の推進等に関する法律（デジタル手続法）」および、関連各府省令により定められており、JPKIの署名用証明書、法務省の商業登記認証局、認定認証局の証明書に限られる。(次ページ、【参考法令】参照)

➢ 電子申請での利用可能な認証局はGPKIのブリッジ認証局との相互運用が前提

1. GPKIでは認証局の信頼性を確認するためブリッジモデルを採用しており、電子申請で利用する電子証明書は、認証局の信頼性を確認する必要からGPKIのブリッジ認証局との相互認証を行った認証局から発行したものが必要。
2. 特定認証局は、現状ではGPKIのブリッジ認証局との相互認証の対象外であり、電子申請での利用はできない。

➢ 認定認証局、特定認証局での証明書発行

認定認証局での利用 ➡ 公的個人認証法の4号届出事業者＊1

・認定認証業務での本人確認に公的個人認証証明書（電子署名用）を利用
→公的個人認証証明書はリモートでの本人確認が可能で、**Authoritative Source(権威ある情報源)**として機能

特定認証局での利用 ➡ 公的個人認証法の5号認定事業者＊2

・特定認証業務での本人確認に公的個人認証証明書（電子署名用）を利用
・5号認定の基準には、上記以外に設備基準、運用基準あり（施行令第8条、施行規則第25条、第26条）
→認定認証業務と同等の基準が示されている(参考資料1、ご参照)
技術（暗号強度）、運用（2マンルール）、設備（HSM）などの基準あり

＊1，＊2：電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律
（署名検証者等に係る届出等）
第十七条 .・・・省略・・・
四 電子署名及び認証業務に関する法律第八条に規定する認定認証事業者
五 電子署名及び認証業務に関する法律第二条第三項に規定する特定認証業務を行う者であって政令で定める基準に適合するものとして総務大臣が認定する者

3.【参考法令】電子申請で利用可能な電子証明書の規定例

■情報通信技術を活用した行政の推進等に関する法律（デジタル手続き法）

（電子情報処理組織による申請等）

第六条　申請等のうち当該申請等に関する他の法令の規定において書面等により行うことその他のその方法が規定されているものについては、当該法令の規定にかかわらず、主務省令で定めるところにより、主務省令で定める電子情報処理組織（行政機関等の使用に係る電子計算機（入出力装置を含む。以下同じ。）とその手続等の相手方の使用に係る電子計算機とを電気通信回線で接続した電子情報処理組織をいう。次章を除き、以下同じ。）を使用する方法により行うことができる。

4　申請等のうち当該申請等に関する他の法令の規定において署名等をすることが規定されているものを第一項の電子情報処理組織を使用する方法により行う場合には、当該署名等については、当該法令の規定にかかわらず、電子情報処理組織を使用した個人番号カード（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号）第二条第七項に規定する個人番号カードをいう。第十一条において同じ。）の利用その他の氏名又は名称を明らかにする措置であって主務省令で定めるものをもって代えることができる。

■総務省関係法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則

（定義）

第二条　この省令において使用する用語は、特段の定めがある場合を除くほか、情報通信技術活用法において使用する用語の例による。

2　この省令において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　電子署名　電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成十四年法律第百五十三号）第二条第一項又は電子署名及び認証業務に関する法律（平成十二年法律第百二号）第二条第一項に規定する電子署名をいう。

二　電子証明書　次に掲げるもの（行政機関等が情報通信技術活用法第六条第一項に規定する行政機関等の使用に係る電子計算機から認証できるものに限る。）をいう。

イ　電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律第三条第一項に規定する署名用電子証明書

ロ　電子署名及び認証業務に関する法律第八条に規定する認定認証事業者が作成した電子証明書（電子署名及び認証業務に関する法律施行規則（平成十三年総務省・法務省・経済産業省令第二号）第四条第一号に規定する電子証明書をいう。）

ハ　商業登記法（昭和三十八年法律第百二十五号）第十二条の二第一項及び第三項の規定に基づき登記官が作成した電子証明書

（電子情報処理組織による申請等）

第四条　　情報通信技術活用法第六条第一項の規定により電子情報処理組織を使用する方法により申請等を行う者は、行政機関等の定めるところにより、当該行政機関等の指定する電子計算機に備えられたファイルに記録すべき事項又は当該申請等を書面等により行うときに記載すべきこととされている事項を、申請等をする者の使用に係る電子計算機から入力して、申請等を行わなければならない。

2　前項の規定により申請等を行う者は、入力する事項についての情報に電子署名を行い、当該電子署名を行った者を確認するために必要な事項を証する電子証明書と併せてこれを送信しなければならない。...(略)・・・

■経済産業省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則

第四条

3　申請等を行う者は、次の各号のいずれかの方法により申請等を行わなければならない。

一　第一項の規定により入力する事項についての情報に電子署名を行い、当該電子署名に係る電子証明書であって次のいずれかに該当するものと併せてこれを送信する方法

イ　商業登記法（昭和三十八年法律第百二十五号）第十二条の二第一項及び第三項（これらの規定を他の法令の規定において準用する場合を含む。）の規定に基づき登記官が作成した電子証明書

ロ　電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成十四年法律第百五十三号）第三条第一項に規定する署名用電子証明書

ハ　イ及びロに掲げるもののほか、経済産業大臣が告示で定める電子証明書

〇電子情報処理組織による申請等に関する告示（平成十五年二月三日　経済産業省告示第二十号）

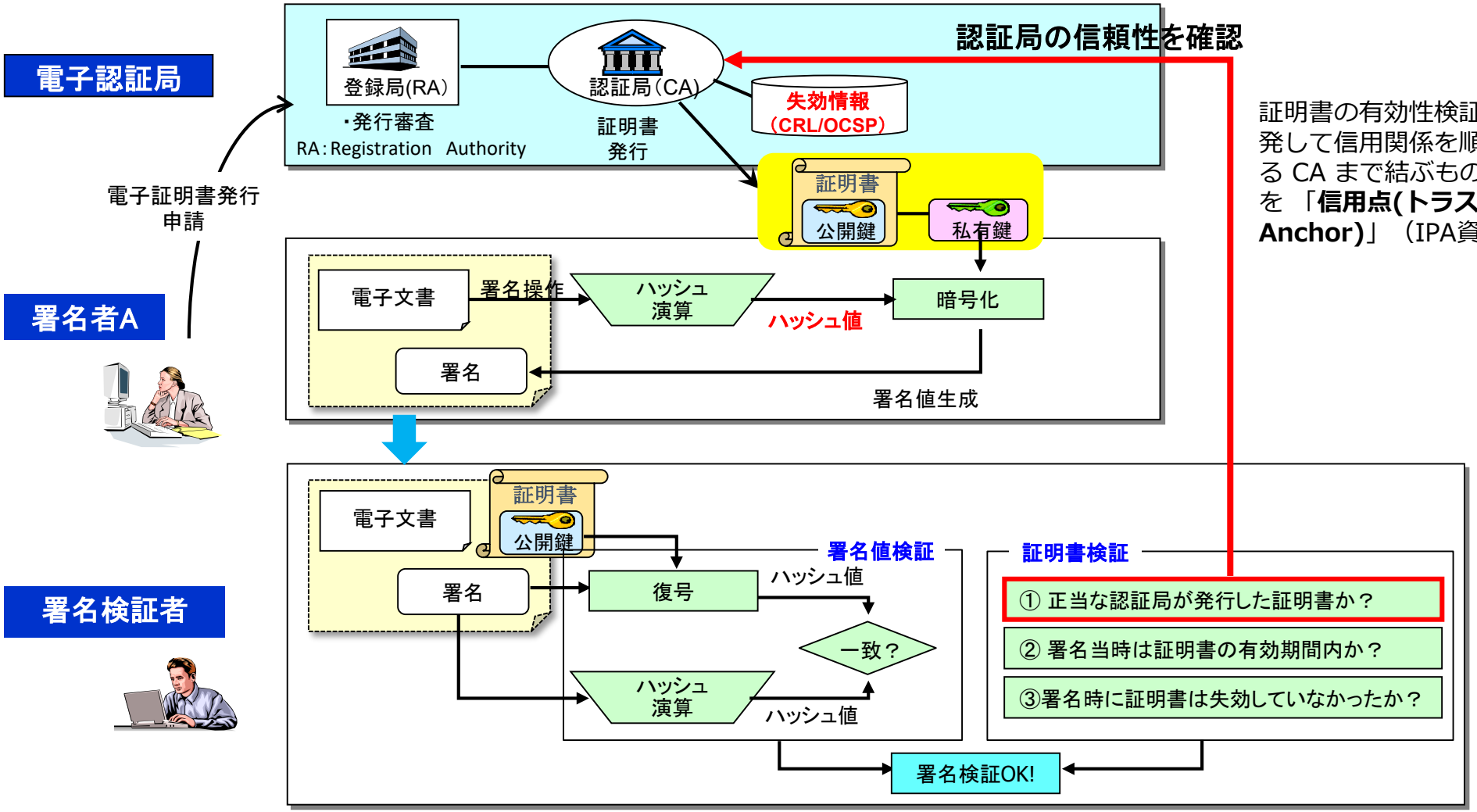
政府ブリッジ認証局と相互認証を行っている認証局で政府認証基盤を構成する認証局以外のものが作成した電子証明書

4. 認証局の信頼性の確認とは？

➢ 認証局の信頼性確認(トラストアンカーの確認)

・電子署名済みの文書の受領者は電子署名の検証を行うことにより当該電子文書の真正性を確認しますが、その際、電子証明書を発行した**認証局の信頼性を確認**することが必要となる。

・4号届出、5号認定を受けた認証事業者であることを署名検証者はどのように確認可能とするか？



証明書の有効性検証は、検証したい証明書から出発して信用関係を順にたどり、自分が信用している CA まで結ぶものです。信用の基点となる CA を「**信用点(トラストアンカー： Trust Anchor)**」（IPA資料より引用、加筆）

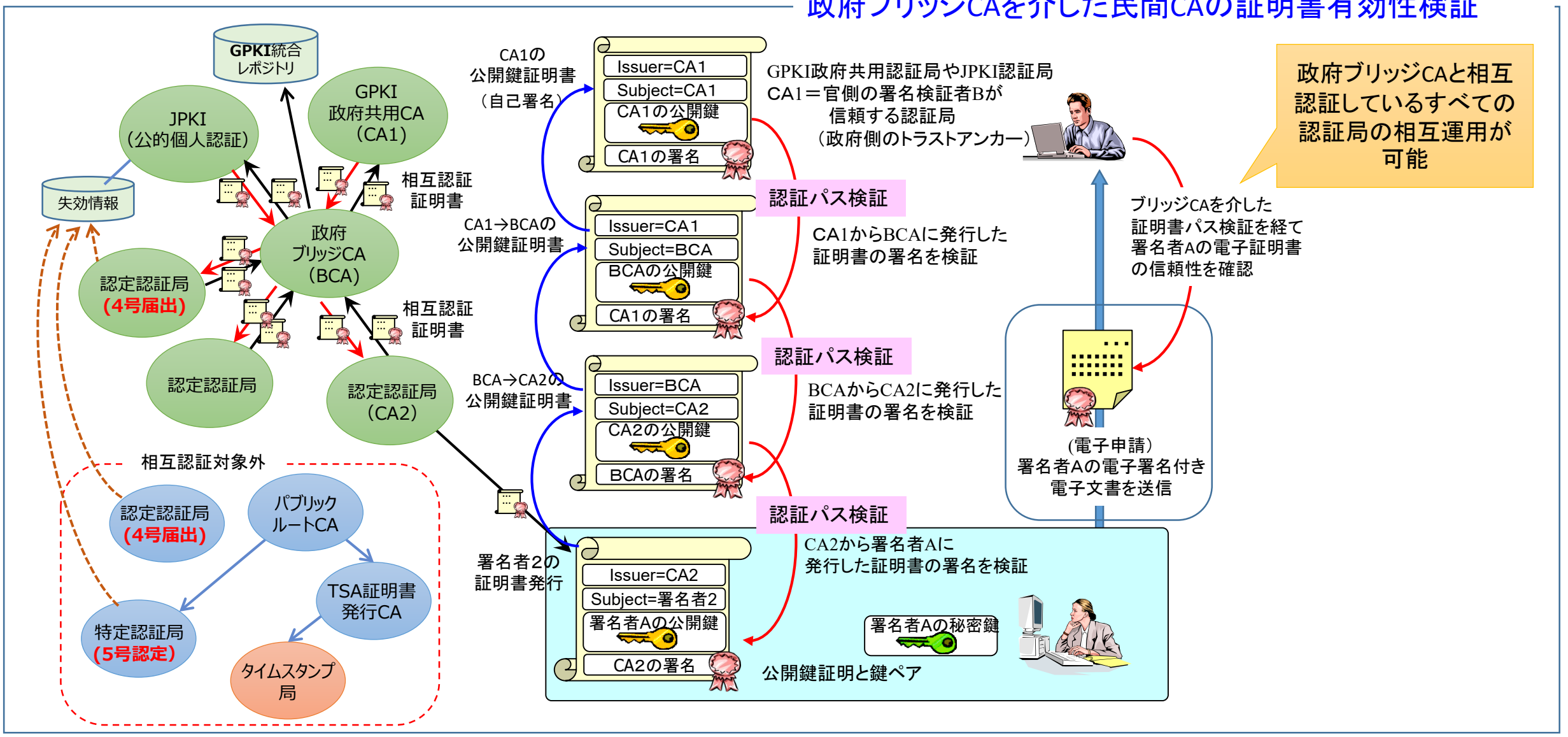
5. 認証局の信頼性の確認方法（Trust Representation）

➢ 信頼された認証局(トラストアンカー)の開示方法

方　式		対象となる認証局等	一意に特定	可読性		廃業TSPの検証	日本での制度運用	課題
				人	機械			
ブリッジ型	ブリッジCAと相互認証	GPKI、認定認証局（署名法認定）	○	×	○	×	○	官側の検証は問題ないが、検証に必要な情報が民間開放されていない。
リスト型	官報にCA認証局のハッシュ値を公開	認定認証局（署名法認定）	○	×	×	×	○	実際の確認が困難
	ホームページでサービス名を公開	認定認証局（署名法認定） タイムスタンプ（デ協認定）	×	○	×	×	○	実際の検証時に本物の証明書か不明
	ブラウザーにルート証明書を登録 (Common CA Data Base:CCADB)	Webサーバー証明書を発行するパブリック認証局（WebTrust監査、ETSI監査）	○	○	○	×	○	民間団体（CAブラウザーフォーラム）による運用であり制度安定性が課題
	アドビ製品に登録（AATL)	ドキュメント署名用のパブリック認証局（WebTrust監査、ETSI監査）	○	△	○	×	○	民間企業による自社製品での運用。PDF署名に限定
	リストで公開（EU　Trusted List)	EUのトラストサービス事業者（CABの適合性監査）	○	○	○	○	×	認証局だけでなくタイムスタンプ局等も取り扱い可能。EU域内で相互運用されているが国際的な相互運用はトライアル中

6. ブリッジモデルによる相互認証

- 政府ブリッジCAを介したルート認証局の相互認証(米国連邦政府PKI（FPKI)と同じブリッジモデルを採用）

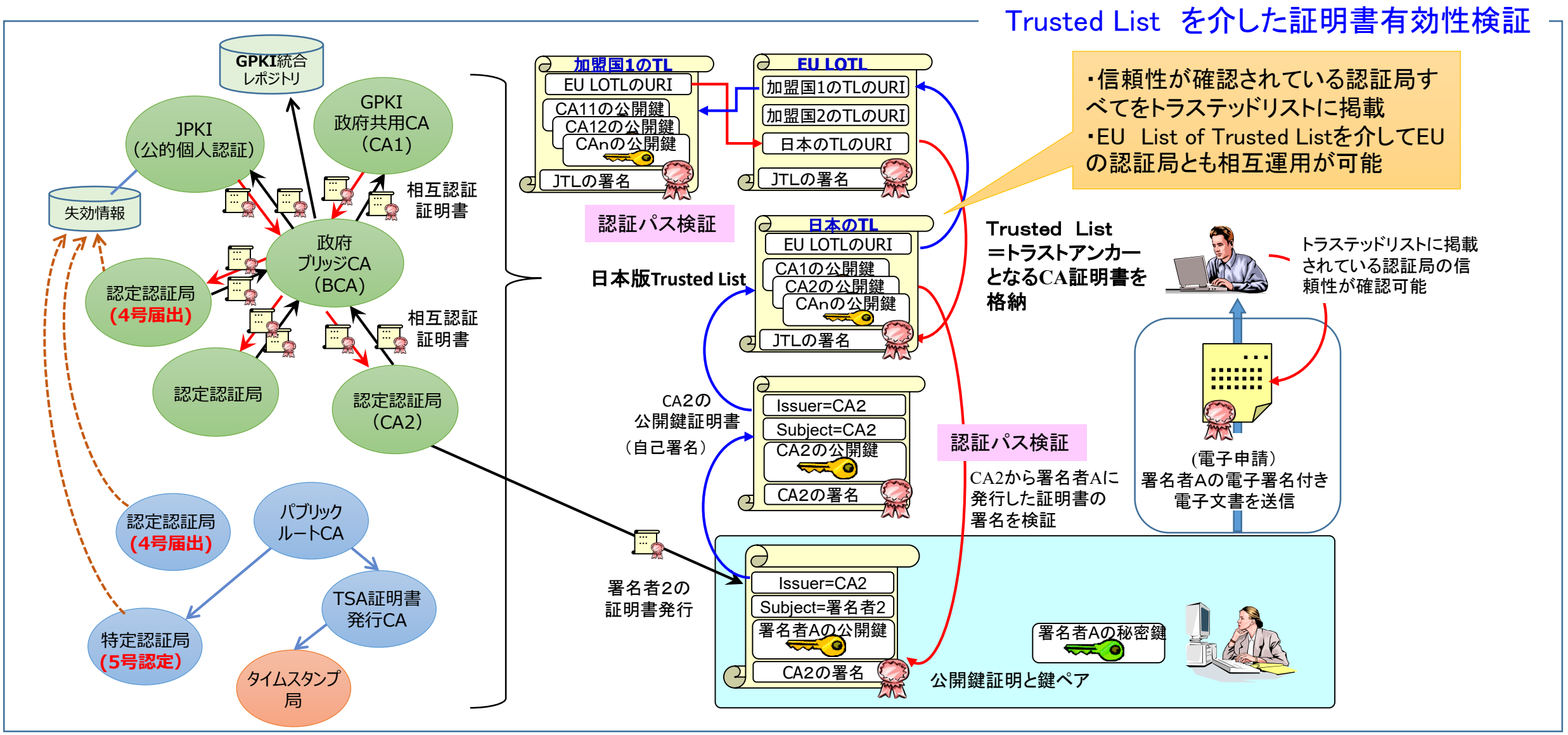


7. ブリッジモデルによる相互認の論点

- 政府ブリッジCAを介したルート認証局の相互認証
  - メリット
    - BCAと相互認証をしているすべての認証局間で相互運用が可能。
  - 現時点の課題
    - 相互認証証明書や検証情報が格納されている「GPKI統合レポジトリ」や署名検証システムの利用は官側に閉じられているため民間での利用に制限がある
    - BCAと相互接続できる民間認証局は認定認証局に限られ、5号認定を受けた特定認証局は対象外
    - タイムスタンプは政府ブリッジCAとの相互認証対象として想定しておらず、政府ブリッジCAを介した信頼性の確認ができない
    - 海外の認証局との相互運用が現時点では難しい
  - 対応策
    - 「GPKI統合レポジトリ」等署名検証システムの民間開放
    - 5号認定を受けた特定認証局のBCAとの相互接続
    - タイムスタンプ局に証明書を発行している民間認証局のBCAとの相互接続
    - 海外のCAと相互接続を行うブリッジ認証局の検討（米国FPKI等との相互接続）

8. リストモデルによる相互認証（将来構想）

- トラステッドリストを介した認証局の相互認証



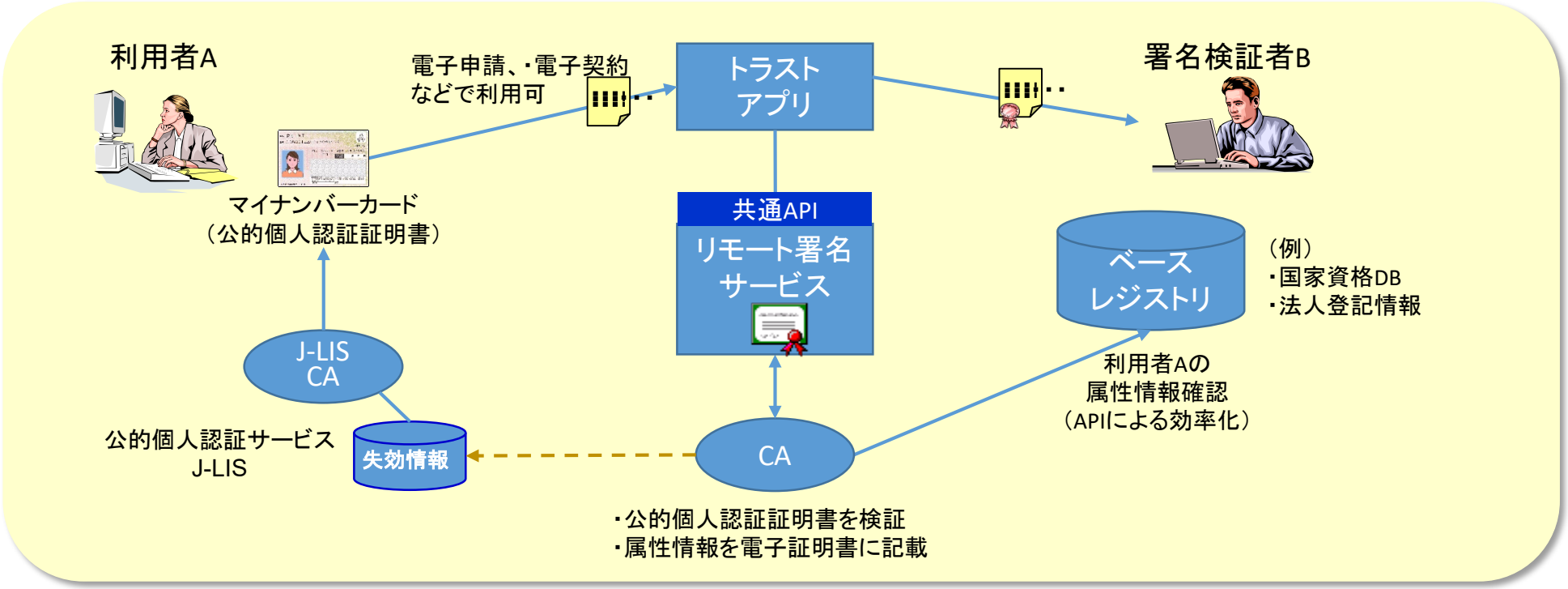
9. リストモデルによる相互認証の論点

- トラステッドリストを介した認証局の相互運用
  - メリット
    - 政府BCAと相互接続していない認証局（5号認定）やタイムスタンプ局等トラストサービス全般に取り扱い可能。
    - EU標準と協調することにより認証局の国際的な相互運用が可能。
  - 課題
    - 日本ではトラステッドリストに対応する制度が無い
  - 対応策
    - トラステッドリストに掲載するトラストサービスの包括的な認証制度の検討

10. JPKIを活用した今後の民間CAのユースケース

➢ オンラインによるワンストップでの電子署名の利用

マイナンバーカードによりオンラインで本人確認、法人登記情報などのベースレジストリを確認し法人代表者などの属性付き証明書をリモート署名サービス内に発行して、クラウド上でワンストップで電子署名が利用可能



(注) 認定認証局の証明書をリモート署名サービスで利用する場合について、H28年度の経産省、電子署名法研究会で検討されている。署名鍵を認証局、または、利用者が作成する場合における基準について規定している電子署名法施行規則第6条第3号及び第3号の2との関係では、一定の要件を満たすものであれば、リモート署名はいずれも認定認証業務の基準を満たすものとされている。
従って、今後、具体的な認定基準を作成する必要があると考えられる。

電子署名法研究会（平成28年度第4回）-資料2-1　事業報告書（2017 年3 月）
https://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/h28_04_haifu.html

11. まとめ

- 公的個人認証証明書で本人確認を行う民間認証局は、認定認証局(4号届出)と特定認証局(5号認定)がある。電子申請での利用は政府ブリッジ認証局と相互認証を行う必要があり現状では認定認証局(4号認定)に限られる

- 5号認定を受けた特定認証局であっても、その認定基準には電子署名法と同等な技術、設備、運用要件が示されており電子申請での利用の可否を検討すべきではないか

- 5号認定を受けた特定認証局も含む相互認証の方法を検討すべきかではないか

- 公的個人認証証明書で本人確認を行う民間の電子証明書の利用は、オンラインでの本人確認が可能なため、今後は、リモート署名サービスやベースレジストリーと連携した属性情報の付加により、電子申請や電子契約など様々な官民のアプリでワンストップでクラウド上での電子署名の利用が容易となると考えられる。

- 今後、認定認証局(4号認定)と特定認証局(5号認定)は対面と同等な本人確認や技術、設備、運用要件が示されており、EUの適格電子証明書と技術的同等性が確保されていると考えられるため、国際相互運用も視野にいれた相互認証の方法を検討すべきかではないか