eシールと法人KYC

～組織における構成員の身元確認に関連して～

セコム株式会社IS研究所
島岡　政基

お題

- 高いIALを保証するためのエビデンスを電子的に流通させたい

- 現状UPKIでは電子署名ができる証明書が発行できるが、運用が若干心許ない
- 組織が発行する文書に対する署名(いわゆるeシール)について、運用面での基準を少し厳格化すれば、参加機関の間で、エビデンスの保証レベルの高さについて合意がとれるのではないか

以下の2点について情報共有します

- eシールの国内外の動向
- 法人KYCにまつわる議論
  - 組織における構成員の身元保証に関連するトピックとして

eシールの国内外の動向

eシールとは

- 電子文書等が法人により発行されたことを示すもの
  - 請求書・領収書等の電子的な処理において簡便に付与できることへの期待
  - 特にインボイス制度導入による電子インボイスへの活用が期待
- 技術的には電子署名と同じ
  - 署名者が**自然人か法人か**の違い　←証明書発行時の身元確認が大きく異なる

eシールのイメージ

出典：デジタル庁、トラストを確保したDX推進サブワーキンググループ（第2回）
資料2 eシール政策の検討状況と今後の課題・ニーズ）

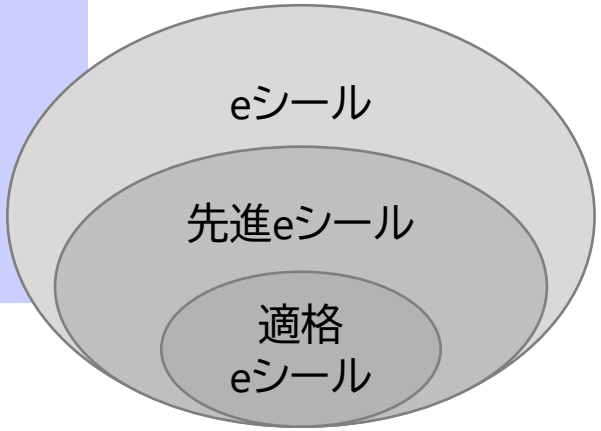
- 欧州eIDASでは、(自然人の)電子署名、タイムスタンプなどと並ぶ
  トラストサービスのひとつとして規定されている

- 国内では、総務省が2021年6月に「eシールに係る指針」を公表

eIDAS規則で定められている3つのeシール

名称	定義	法的効力	用途
適格eシール (Qualified e-Seal)	適格eシール生成装置を利用して生成され、eシールの適格証明書に準ずる先進eシール	適格eシールは、適格eシールがリンクするデータの完全性及びデータの起源の正確性を推定することができる	電子申請、法的に保存義務のあるデータ、規制産業におけるデータの自動処理 (B2B, B2C)及び保護、保険契約／契約の提示、電子インボイス、財務報告書、PSD2、X-Road、官公庁システム
先進eシール (Advanced e-Seal)	第36条*で規定する要件を満たすeシール	下記eシールの法的効力から追加の規定はない。	B2B、B2Cにおけるデータの自動処理、保護、システムログの保存、業務プロセス
eシール (Electronic Seal)	データの期限と完全性を保証する為に電子データに添付又は論理的に関係している電子形式のデータ	eシールは、その法的効力及び法的手続きにおける証拠としての能力を、それが電子形式である、又は適格eシールの要件を満たさないという理由だけで否定されない	-

*第36条：eシール生成者が識別でき、eシールと一意に紐づくこと及び改ざん検知等。



出典：総務省、組織が発行するデータの信頼性を確保する制度に関する検討会（第8回）
資料8－2 より

ETSIにおけるeシールのレベルと証明書ポリシ

eシール用電子証明書を発行する認証局のポリシー及びセキュリティ要件を定めているETSI EN 319 411-1,-2には、**QCP-l-qscd**、**QCP-l**、**NCP+**、**NCP**、**LCP**の5つのポリシーが定められており、5段階の基準となっている。

eシールのレベル		ポリシー	定義
適格eシール		**QCP-l-qscd** (Qualified Certification Policy -Legal person-QSCD)	この要件に従って発行された証明書は、欧州規則(EU)No 910/2014 [i.1]の第3条(27)で規定されているような適格eシールをサポートすることを目的としている QSCD:Qualified Seal Creation Device(適格eシール生成装置) ※ISO/IEC 15408(Common Criteria)とProtection Profile(EN 419 211シリーズ)に適合した認証製品を使用
先進eシール	適格証明書に基づく先進eシール	**QCP-l** (Qualified Certification Policy-Legal person)	この要件に従って発行された証明書は、欧州規則(EU)No 910/2014 [i.1]の第36条及び37条で規定されている適格証明書に基づく先進eシールをサポートすることを目的としている
	先進eシール(秘密鍵をセキュア暗号装置で管理)	**NCP+** (Extended Normalized Certification Policy)	セキュア暗号装置が必要であると考えられる場合に使用され、NCPと同じクオリティを持つ、拡張標準証明書ポリシー
	先進eシール(秘密鍵の保護環境の指定なし)	**NCP** (Normalized Certification Policy)	すべての取引形態で使用される証明書を発行するTSPの一般的なベストプラクティスを満たす、標準証明書ポリシー
		LCP (Lightweight Certification Policy)	すべての取引の形式(デジタル署名、Web認証またはeシール)で使用される証明書のための、NCPのすべての要件(物理的存在など)を遵守する追加的な負担をリスクアセスメントが正当としない場合に使用するNCPより負担の少ないサービス品質を提供する、簡易証明書ポリシー

出典:総務省、組織が発行するデータの信頼性を確保する制度に関する検討会(第8回)
資料8－2 より

eシールに係る指針の策定

➢ 意見募集（意見募集期間：R3.5.1～6.4）の結果を踏まえ、我が国のeシールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準等について整理した**「eシールに係る指針」を令和３年６月25日に公表。**

eシールに係る指針の概要

- 我が国におけるeシールの定義は、「電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み」とする。
- 発行元証明の信頼性を担保するための措置の水準に応じて、eシールのレベル分けを行う。
  - レベル1：上記eシールの定義に合致するもの
  - レベル2：一定の技術基準を満たすもの
  - レベル3：レベル2に加えて、十分な水準を充たしたトラストアンカー※1によって信頼性が担保されたもの（組織等の実在性の確認の方法や設備のセキュリティ要件等について、十分な水準を満たし、第三者のお墨付きがあるもの）
- eシール用電子証明書の発行対象となる組織等は、法人、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等とする。

※1 インターネットなどで行われる、電子的な認証の手続きのために置かれる基点のこと。本指針においては、信頼性の起点となる認証局を想定。

レベル3のeシールの基準となる要件（抜粋）

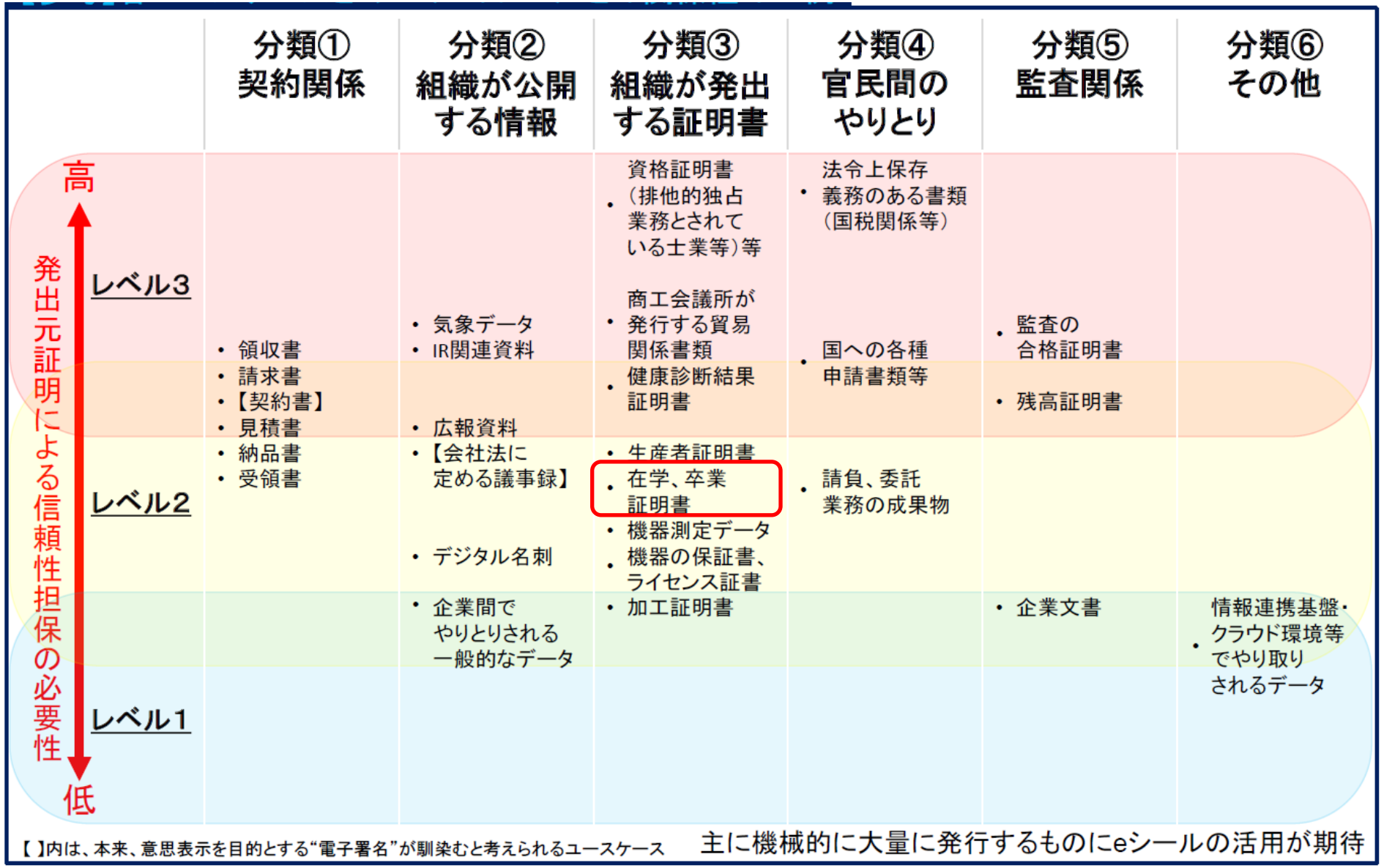
- ○ eシール用電子証明書の発行の際には、当該組織等の代表者の意思による申請に基づき、当該組織等の実在性を公的な情報（登記情報等）に裏付けられたエビデンスで確認すること。
- ○ eシール用電子証明書のフォーマットは、国際標準としても規定されているITU-T X.509を用いること。
- ○ 認証局の秘密鍵は、一定の厳しい要件を満たしたHSM※2によって厳格に管理されること。
- ○ 利用者の秘密鍵は、利用者自身で管理することとするが、認証局から利用者に対する説明事項として、秘密鍵の管理に係る事項（秘密鍵の管理は厳格に行うこと）を規定すること。

※2 Hardware Security Module の略。耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。

eシールのレベルはeIDASの規定する3種類に相当すると考えるのが妥当
- レベル1：eシール
- レベル2: 先進eシール
- レベル3: 適格eシール

出典：デジタル庁、トラストを確保したDX推進サブワーキンググループ（第2回）資料2 eシール政策の検討状況と今後の課題・ニーズ）に一部加筆

【参考】各ユースケースとeシールのレベルとの関係性の一例



出典：組織が発行するデータの信頼性を確保する制度に関する検討会取りまとめ（案）及びeシールに係る指針（案）に対する意見募集の結果 別紙3 p.10に一部加筆

法人KYCにまつわる議論

法人KYC(本人確認)とは？

認証プロバイダーにおける組織の身元確認における抽象化

- 組織の存在確認
  - 組織の属性情報自体の確認：法人番号、商号、本店の住所が法人番号公表サイト、印鑑証明書上での確認
  - 組織の属性情報の信頼性の確認：印鑑証明書の真偽
- 個人の存在確認
  - 個人の属性情報自体の確認：個人名、生年月日が印鑑証明書上での確認
  - 個人の属性情報の信頼性の確認：印鑑証明書の真偽
- 個人の組織所属者の確認
  - 個人が組織に所属していることの確認：法人代表者の印鑑証明書であることで、法人代表者の確認
- 組織所属者（個人）の申請事実の確認
  - 組織所属者が申請していることの確認：申請書の押印と印鑑証明書の印影の確認

実務上は法人代表者以外のケースが少なくない

出典：OpenID BizDay #14 - OpenID Connectと身元確認/KYCのトレンド
「法人認証基盤GビズIDと今後の法人KYCJに一部加筆

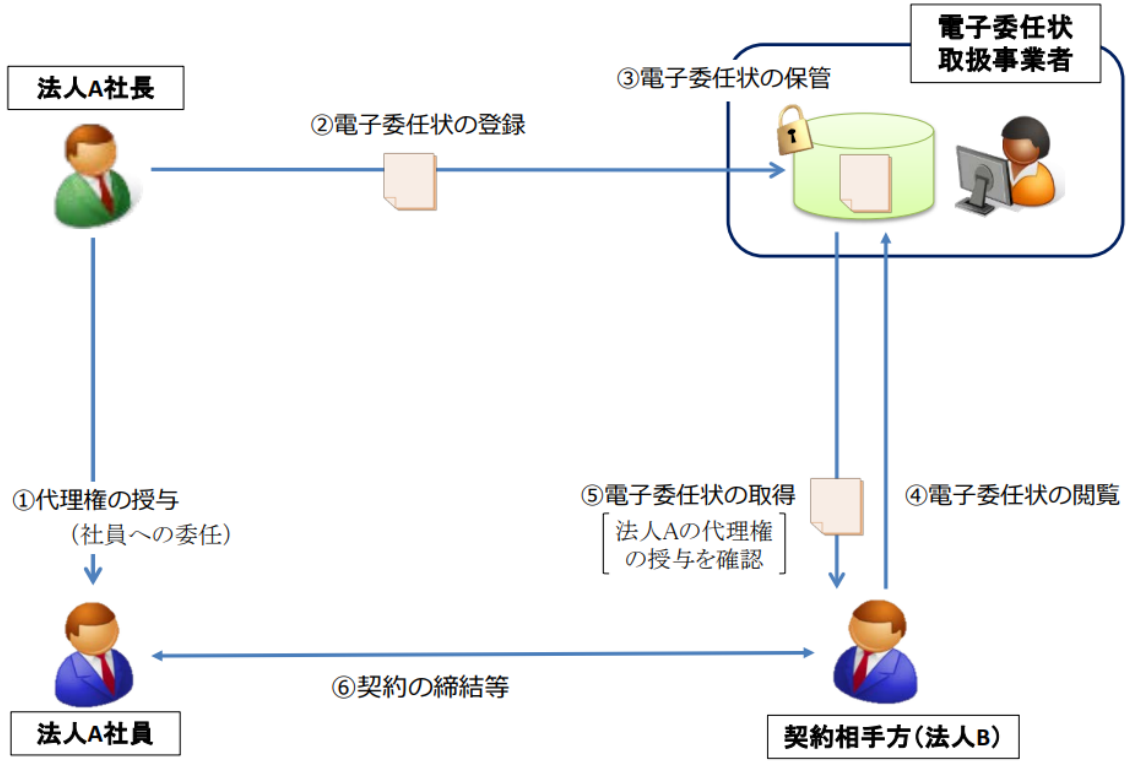
法人と担当者の関係の確認の例

- 法人代表者の場合は、登記情報により法人と代表者の関係を確認できる
- その他の担当者の場合は、その者が当該業務の任にあることを、その法人に確認する
  - 委任状
  - 電話による確認　など

関連トピックの紹介
- 電子委任状制度
- 法人共通認証基盤(gBizID)
- OpenID for Identity Assurance

電子委任状制度

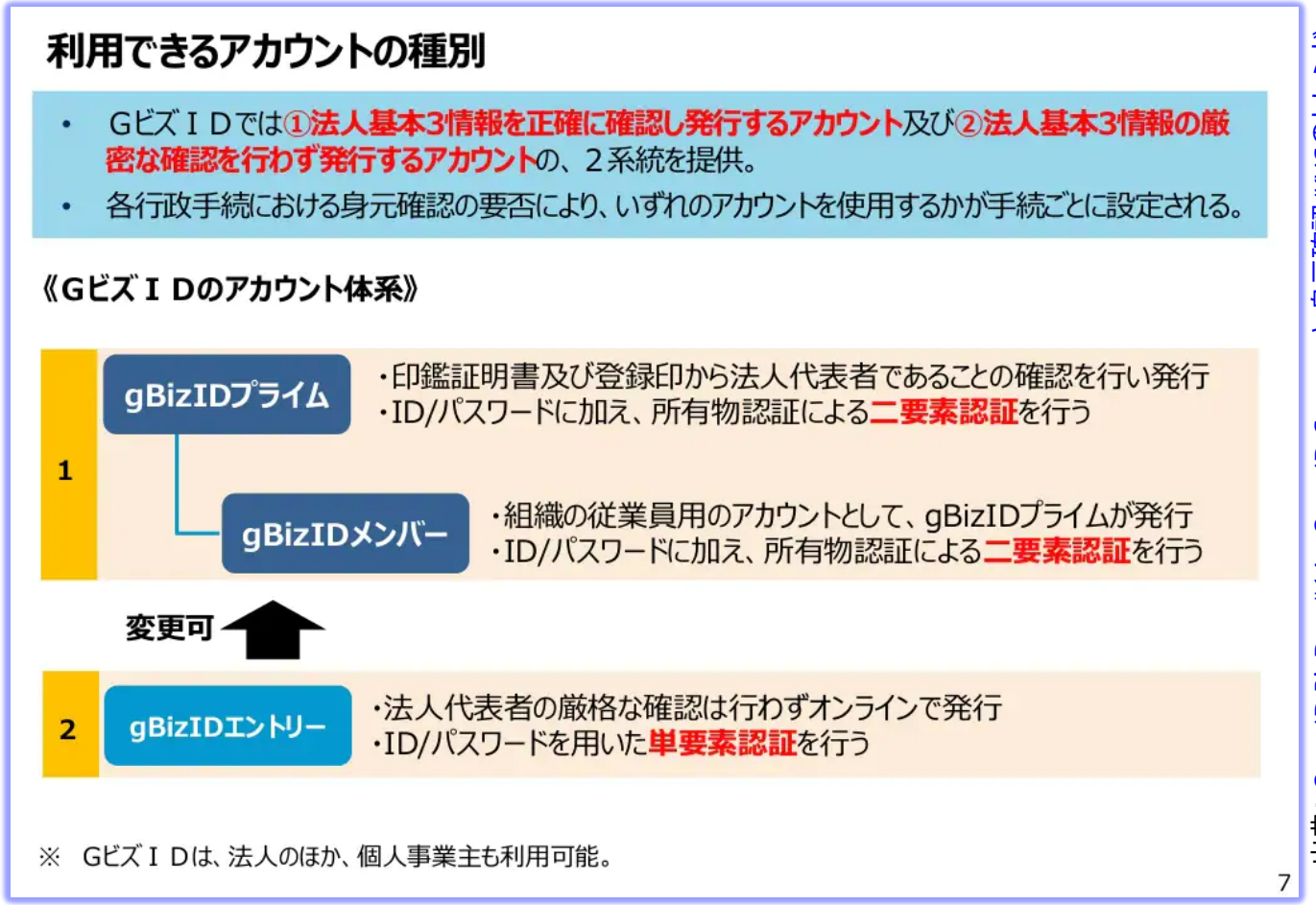
- 電子委任状
  - 法人の代表者等が社員等に代理兼を与えた旨を表示するもの
- 電子委任状の普及の促進に関する法律（電子委任状法）
  - 電子委任状の記録方式や、電子委任状取扱業務及び同認定制度を規定している
  - 2021年5月から政府電子調達において利用可能



出典：総務省、制度検討サブワーキンググループ（第2回）
資料2-1より

法人共通認証基盤(gBizID)

- 様々な行政サービスで利用可能な法人認証基盤。
- gBizIDに法人アカウント登録することでそのIDを用いて様々な行政サービスにログインすることができる。



出典：OpenID BizDay #14 - OpenID Connectと身元確認/KYCのトレンド
「法人認証基盤GビズIDと今後の法人KYC」より

保証レベル（NIST SP 800-63-3との関係）

✓ NIST SP 800-63-3（アメリカ国立標準技術研究所（NIST）が定める電子的認証に関するガイドライン）の各ユーザモデルの保証レベルと、GビズＩＤとの関係については、以下のとおり整理。

	gBizIDエントリー	gBizIDプライム	gBizIDメンバー	※未対応※
IAL 身元情報検証時の保証レベル (Identity Assurance Level)	1	2		3
	本人確認不要、自己申告での登録でよい	サービス内容により識別に用いられる属性をリモート又は対面で確認する必要あり		識別に用いられる属性を対面で確認する必要有
AAL 認証プロセスの保証レベル (Authenticator Assurance Level)	1	2		3
	単要素認証でOK	２要素認証が必要（2要素目の認証手段はソフトウェアベースのものでOK）		２要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたものが必要

⇒ 電子署名方式の利用の検討

出典：OpenID BizDay #14 - OpenID Connectと身元確認/KYCのトレンド「法人認証基盤GビズIDと今後の法人KYC」より

本人確認ガイドラインとGビズＩＤとの対応

- 平成31年２月、ＣＩＯ連絡会議において、「**行政手続におけるオンラインによる本人確認の手法に関するガイドライン**」が策定された
- GビズＩＤとしては、当該**ガイドラインとも整合を取りつつ整理**

《本人確認の手法例の対応表（法人等に係る行政手続）》

	必要な保証レベル	
	身元確認	当人認証
レベルA	（レベル３） 対面での身元確認	（レベル３） 耐タンパ性が確保されたハードウェアトークン
レベルB	（レベル２） 遠隔又は対面での身元確認	（レベル２） 複数の認証要素
レベルC	（レベル１） 身元確認のない自己表明	（レベル１） 単一又は複数の認証要素

GビズＩＤとの対応関係

（レベルＡ相当）
レベルＡに該当する機能はなし

（レベルＢ相当）gBizIDプライム
※身元認証：印鑑証明書等から代表者を確認
※当人認証：２要素認証

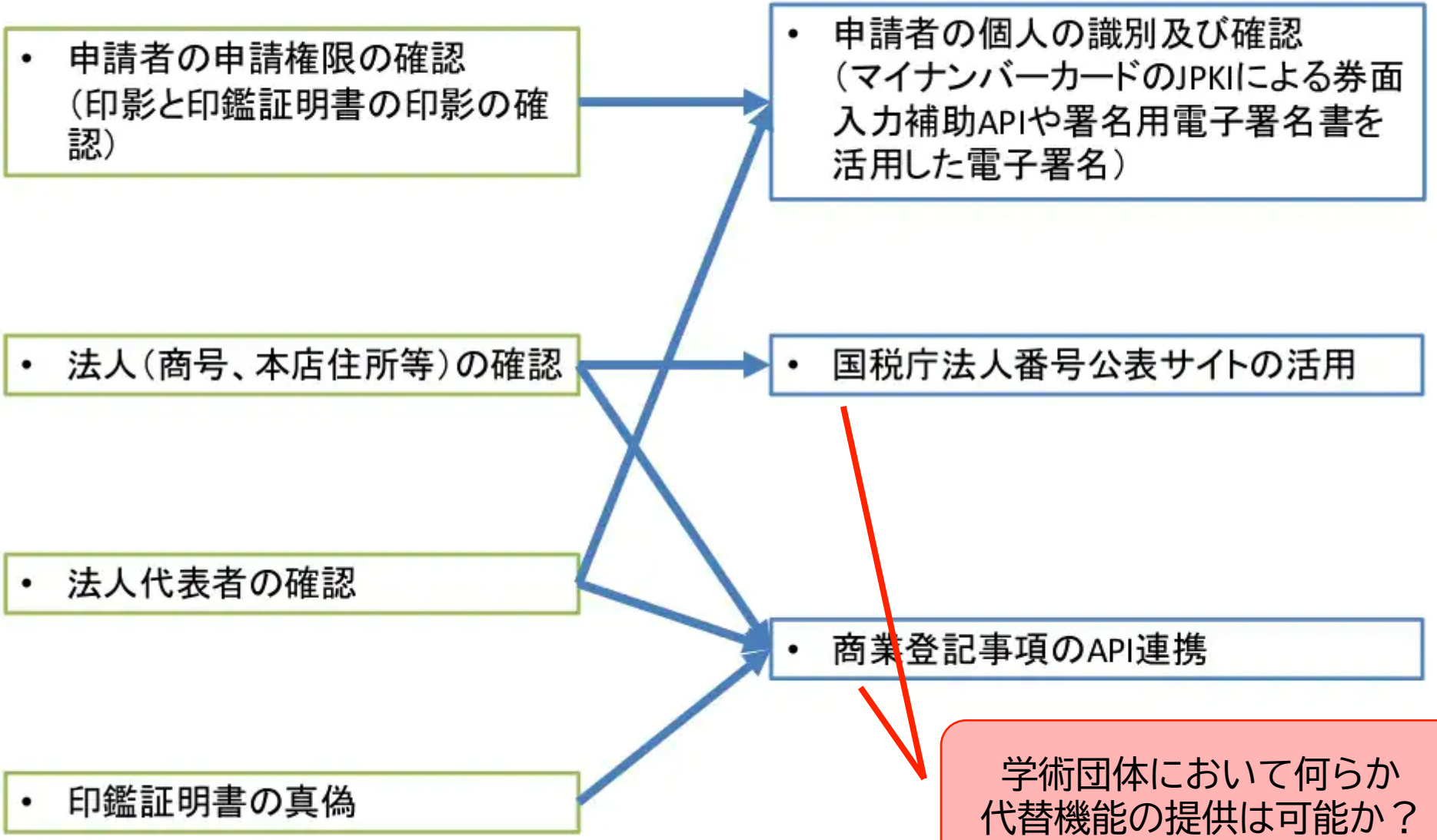
（レベルＣ相当）gBizIDエントリー
※身元確認：存在確認のみ
※当人認証：単要素認証

《GビズＩＤを用いて申請できる手続の具体例（社会保険手続）》

ガイドラインにおいて、社会保険手続のうち「保険の適用日・喪失日を申請内容に含む手続」や「保険料又は給付額算定の根拠となる報酬等を申請内容に含む手続」等については、ログイン履歴の管理機能や未登録端末からのログイン検出機能等を有するGビズＩＤが提供するID・パスワード（多要素認証）により実施可能と考えられる、として例示されている。

出典：OpenID BizDay #14 - OpenID Connectと身元確認/KYCのトレンド
「法人認証基盤GビズIDと今後の法人KYC」より

gBizIDにおける身元確認の自動化の方向性（現状の私案）



出典：OpenID BizDay #14 - OpenID Connectと身元確認/KYCのトレンド「法人認証基盤GビズIDと今後の法人KYC」に一部加筆

OpenID Connect Authority claims extension

- 法人(や、その他の自然人)の代理として行使できる自然人が持つ権限に関する情報を送受可能にする拡張(ドラフト)
  - 例えば、ある会社の担当者がもつ決裁権限の範囲等
- 法人識別情報のための**Claim**や権限を表現するための**Authority Claim**の定義等

- **eKYC&IDA WG**でドラフト作業中
- 経産省が注目している