Digital Architecture Design Center

IPA Better Life with IT

資料2

インキュベーションラボ・プロジェクト

「サービスに応じたデジタル本人確認ガイドラインの検討」

2022年1月25日

独立行政法人情報処理推進機構（IPA）
デジタルアーキテクチャ・デザインセンター（DADC）
インキュベーションラボ
デジタル本人確認プロジェクトチーム

本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

本日のアジェンダ

1. **本インキュベーションラボの背景と目的**
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

採択時の目的

- 目的

日本の産業や生活を、グローバルに通用するデジタル本人確認のガイドラインが普及した、サービス提供者と利用者双方の安全性、利便性が両立した環境にする。このことにより、Society5.0に根差した市場拡大及び国際競争力に資する。

- 目標

サービスに応じたデジタル本人確認のガイドライン及び技術を、世界の動向を踏まえて整備し、広く普及させる。

- デジタル本人確認におけるガイドライン整備の意義

- 身元確認手法の、より精緻な整理
- どのようなサービスであればどのレベルの身元確認手法を選択する必要があるかの整理

このふたつを行うことが重要である。

【活動のスコープ（赤枠内）】

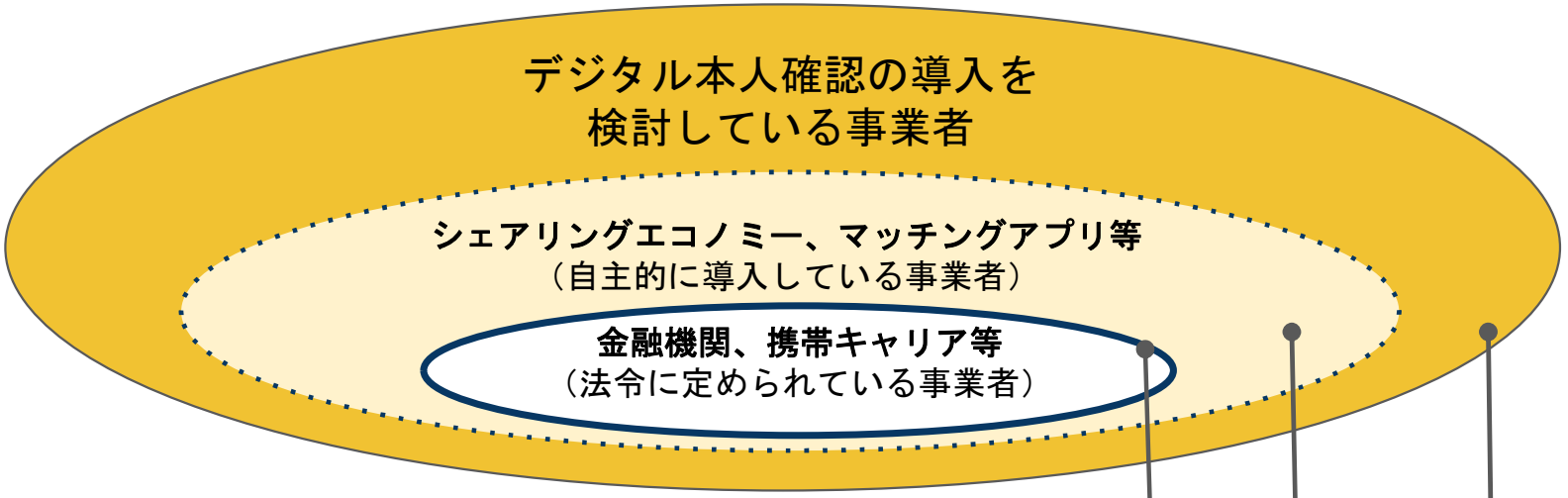
サービスの種類	サービス提供者の種類		利用	ガイドラインの現状
	管理責任	実行責任		
行政サービス、行政手続	行政機関、自治体・省庁及び関連組織	行政機関、自治体・省庁及び関連組織	個人 法人	あり 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」
民間委託、コラボレーション	行政機関、自治体・省庁及び関連組織	企業、個人事業主	個人 法人	なし 但し「行政手続き～」に従うことが適当。管理責任者の基準において、実行責任者が実行するため。
民間サービス	企業、個人事業主	企業、個人事業主	個人 法人	**大部分に存在しない** **身元確認/当人認証の保証レベル判定方法、保証レベルに応じた手法例が必要**

・個人の民間サービス利用をスコープとする。

・既にガイドラインが定められている「行政手続き」は取り扱わない

ガイドラインを策定する趣旨

レベルは違えど、「本人確認手法が分からない」が共通の課題



課題

- 法令に多くの手法が定められているが、安全性や利便性の**違いが分からない。**
- 導入済みの手法が自社のサービスに**最適な手法か分からない。**
- 対面手続に代わる手続として、**どの手法をどのように導入するのか分からない。**

求められる対応

①身元確認手法の保証レベルの整理

↓

②サービスに応じた本人確認手法の提案

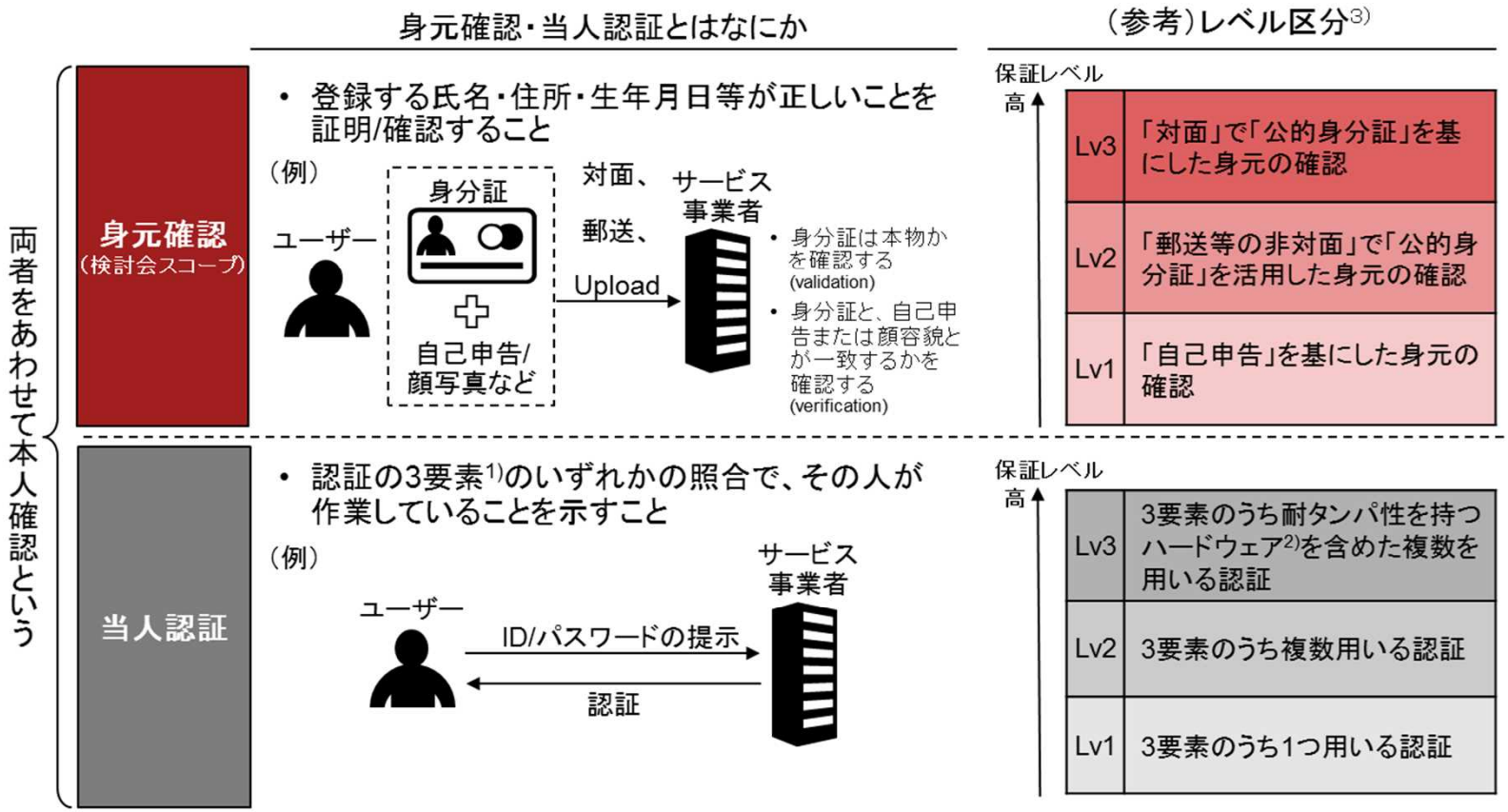
本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. **オンラインの身元確認手法のレベル分けについて**
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

オンラインの本人確認は身元確認と当人認証からなる

身元確認と当人認証の違い



1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「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」（2019年2月CIO連絡会議決定）のレベル区分

本人確認の現状　レベル分表作成についての参考：デジタル本人確認の保証レベルと手法例の根拠

IAL・AALのいずれかのレベルが低ければ、本人確認手法のレベルも下がることから、
サービスリスクに応じてIAL・AALを選択する必要がある

身元確認と当人認証の保証レベル

必要な保証レベル		オンラインによる手法例
IAL	AAL	
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A**
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B**
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	**レベルC**

	AAL 1	AAL 2	AAL 3
IAL 3			**レベルA**
IAL 2		**レベルB**	
IAL 1	**レベルC**		

出所：各府省CIO連絡会議 (2019)「行政手続き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」より作成

本人確認の現状　本人確認手法について

本人確認手法をマトリクスに配置したところ「レベルB」に集中しており、法令内でもばらつきがみられる。

身元確認レベル（IAL） ＼ 当人認証レベル (AAL)	認証なし	レベル1 単要素認証	レベル2 2要素認証	レベル3 2要素認証 (耐タンパを含む)
レベル3 対面確認				・犯収法ワ (犯収法規則6条1項1号) ・公的個人認証
レベル2 郵送・リモート確認		・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (犯収法規則6条1項1号) ・口座連携(犯収令13条1項1号)	・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (施行規則6条1項1号) ・口座連携(犯収施行令13条1項1号) (※1) ・身元確認のAPI連携(銀行API/キャリアAPI) (※1) ・犯収法ヘ (犯収法規則6条1項1号) ・犯収法ヲ (犯収法規則6条1項1号) ・民間APIサービスB (※1)	・犯収法ヘ (犯収法規則6条1項1号) ・犯収法ヲ (犯収法規則6条1項1号) ・身元確認のAPI連携(キャリアAPI) (SIM利用) (※1)
レベル1 自己申告		・身分証に基づかない自己申告での登録	・身分証に基づかない自己申告での登録	

凡例　レベルC　レベルB　レベルA

※1　アカウント作成後は身分証不要

本人確認の現状　オンラインサービスにおける本人確認について

本人確認を実施しているオンラインサービスについてもマトリクスの「レベルB」に集中。
【課題】自社サービスに応じた適切な本人確認手法を選択するためには、**レベルに応じた細分化が必要**

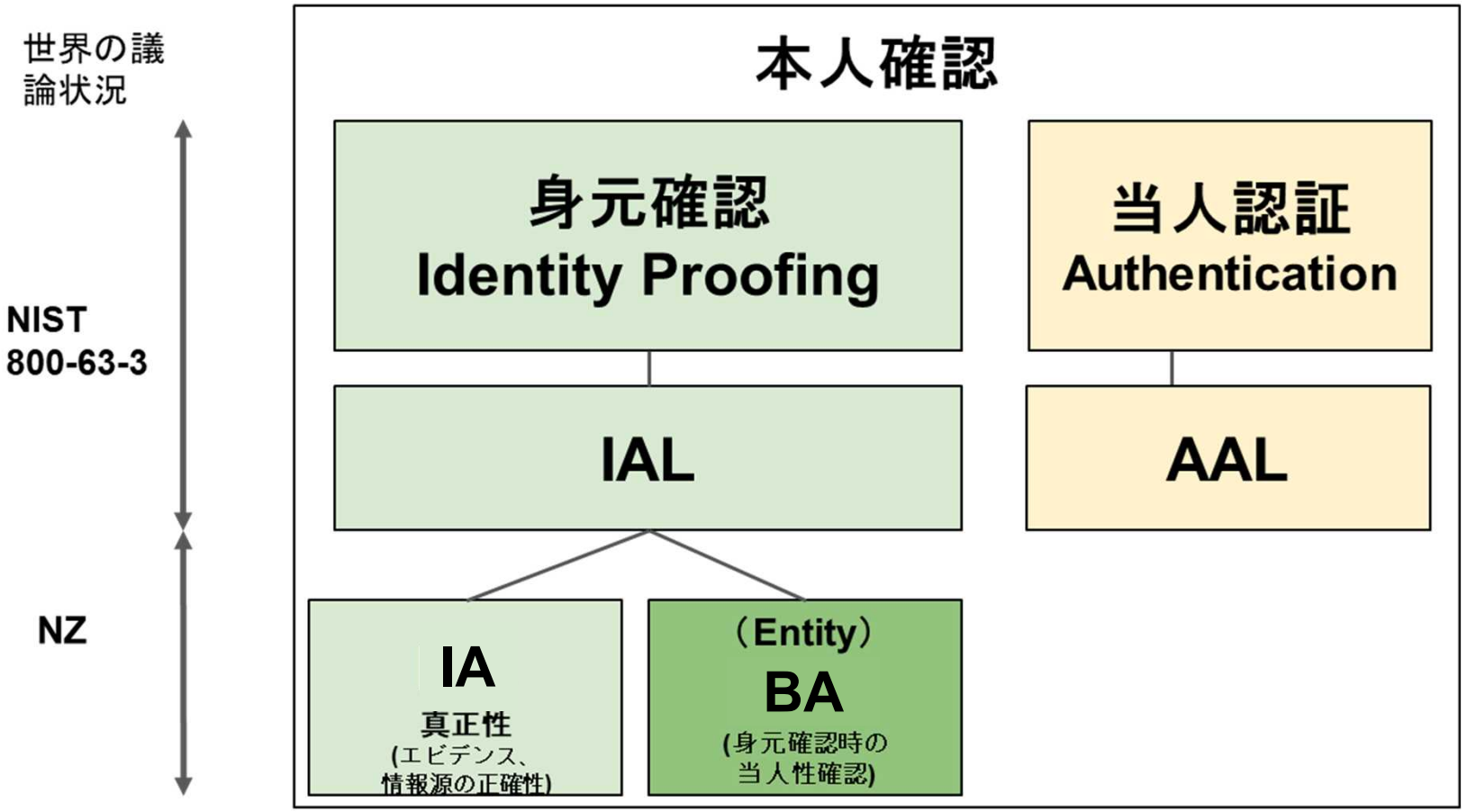
身元確認レベル（IAL） ＼ 当人認証レベル (AAL)	認証なし	レベル1　単要素認証	レベル2　2要素認証	レベル3　2要素認証 (耐タンパを含む)
レベル3 対面確認			・古物商A (※1) ・犯収法の特定事業者 (※1) ・携帯電話事業者 (※1) ・シェアリングエコノミーA社 (※2)	・犯収法の特定事業者 ・携帯電話事業者(※1) ・電子サインA (※1)
レベル2 郵送・リモート確認		・マッチングアプリ ・シェアリングエコノミーB社	・犯収法の特定事業者 (※1) ・携帯電話事業者 (※1) ・古物商B (※1) ・シェアリングエコノミーB社 (※2) ・マッチングアプリ (※3) ・たばこ会員登録 (※3) ・公営ギャンブル (※3) ・eMAFFプライム (オンライン本人確認) (※4) ・gBizプライム (郵送) (※4) ・引越し (※4)	・電子サインA (※1) ・口座開設 (ネット完結) (※2) ・たばこ会員登録 (※3) ・公営ギャンブル (※3)
レベル1 自己申告		・gBiz・eMAFF (エントリー) ・電子サインC (※1)	・電子サインB (※1)	

凡例	レベルC	レベルB	レベルA

※1　法令に基づく
※2　自主的取組
※3　自主的取組 (年齢確認のみ)
※4　行政

＜参考＞ニュージーランドにおけるレベル分け（概要）

身元確認時の「当人性」の確認を含めてIALを整理する動きが見られ始めている。



活動状況　IAL細分化

- IALの細分化に当たり、ニュージーランドのBALの概念を導入
- チーム内で複数回議論を重ね、マトリクス、および手法のマッピングを一旦、完成
- 現在、外部有識者と意見交換し、助言に対しての対応を検討中

  エビデンスに対する支配権、管理権限の観点も必要／リスク（具体的な例示が必要）、UXを考慮した手法の選択する旨の説明が必要 等

手法	DADC IAL (Information Assurance Level)	DADC BAL (Entity Binding Assurance Level)	再考後の DADC IAL (Identity Assurance Level)
公的個人認証による署名用電子証明書＋電子署名付契約書	4	4	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3	4	**3** 調整中
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	3	4	
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	3	4	
認定認証事業者による電子証明書＋電子署名付契約書	3	3	
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）	3	3	
公的身分証のリアルタイム撮影	2	2	**2**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1	2	**1**
身分証確認なし（自己申告＋eメール、SNSログイン等）	0	0	**0**

【参考】ニュージーランドの新しいInformation Assurance

IAレベル	要求事項(レベルごとに差分があるもののみ抜粋)
4	情報の正確性 ・RPは、**権威ある情報源**であるか、または**権威ある情報源と連続的に同期したリンクを持つエビデンス**を選択しなければならない。 エビデンスの質 ・信頼できる通信チャネルを介してシステム的に識別され、アクセスされる証拠に基づいて品質を設定しなければならない。 コントロール ・RP は詐欺対策技術を適用しなければならない。
3	情報の正確性 ・RP は、**少なくとも権威のあるソースのコピーである証拠**を選択しなければならない。 エビデンスの質 ・RPは、手動で特定された証拠に基づいて品質を決定しなければならず、また、 **再現するために独自の知識を必要とする物理的なセキュリティ機能**を含まなければならない。 コントロール **・RPは詐欺対策技術を適用すべきである。**
2	情報の正確性 ・RPは、少なくとも作成時に権威あるソースのコピーを参照した証拠を選択すべきである。 エビデンスの質 ・RP は証拠を「額面通り」に受け取らなければならない。
1	情報の正確性 ・RPはエンティティを証拠として用いるべきである。 エビデンスの質 ・RPはそのエンティティを証拠として受け入れなければならない。

【参考】ニュージーランドの新しいEntity Binding Assurance

BAレベル	要求事項(レベルごとに差分があるもののみ抜粋)
4	エンティティと情報との関係の確立 **・RP は、バイオメトリクス要素を、知識または所有のいずれかのバインディング要素タイプで使用するか、または同等以上の保証レベルの既存の認証機関またはクレデンシャルを使用しなければならない。** 詐欺対策技術 ・RPは不正防止技術を適用しなければならない。 エンティティバインディングの再確認 ・認証イベントに生体認証要素が含まれていない限り、少なくとも5年に1回RPはこの管理を実施しなければならない。
3	エンティティと情報との関係の確立 ・RP は、**最低でも 2 種類の結合要素、**または保証レベルが同等以上の既存の認証機関やクレデンシャルを使用しなければならない。 詐欺対策技術 **・RP は詐欺対策技術を適用すべきである。** エンティティバインディングの再確認 ・認証イベントに生体認証要素が含まれていない限り、少なくとも5年に1回RPはこの管理を実施しなければならない。
2	エンティティと情報との関係の確立 ・RP は、**最低でも 1 種類の結合要素**を使用するか、同等以上の保証レベルの既存の 認証子またはクレデンシャルを使用しなければならない。 エンティティバインディングの再確認 ・少なくとも5年に1回行うべきである。
1	エンティティバインディングの再確認 ・少なくとも5年に1回行うべきである。

ニュージーランド/IALの要件を参考にしたDADC/IALの考え方

NZレベル	1	2	3			4			DADC IAL (Information Assurance Level)
	IA3.03	IA3.03	IA3.03	IA4.02	IA4.03	IA3.03	IA4.02	IA4.03	
	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、使用できないような登録状態（一時停止、取り消し等）の証拠があるかを確認すること	依拠当事者が、可能な限り不正行為対策技術を適用すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、使用できないような登録状態（一時停止、取り消し等）の証拠があるかを確認すること	依拠当事者が、可能な限り不正行為対策技術を適用すること	
	依拠当事者はエンティティーを証拠として使用すべきです。	[SHOULD]権威ある情報源のコピーを参照した証拠	[SHOULD]権威ある情報源のコピーである証拠	[SHOULD]証拠発行者又は同等のサービス・プロバイダーに登録状態を確認	[SHOULD]不正行為対策技術を適用	[MUST]権威ある情報源である証拠、又は権威ある情報源と継続的に同期したリンクを持つ証拠	[MUST]証拠発行者又は同等のサービス・プロバイダーに登録状態を確認	[MUST]不正行為対策技術を適用	
チーム内で検討した補足条件 / 手法					以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する			以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する	
公的個人認証による署名用電子証明書＋電子署名付契約書						〇	〇	〇	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影			〇	×	〇	×	×	〇	**3**
認定認証事業者による電子証明書＋電子署名付契約書			〇	×	〇	×	×	〇	**3**
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）			〇	〇	〇	×	〇	〇	**3**
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影			〇	×	〇	×	×	〇	**3**
公的身分証のリアルタイム撮影		〇	〇	×	×	×	×	×	**2**
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）			×	〇	〇	×	〇	〇	**3**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	〇	×	×	×	×	×	×	×	**1**
身分証確認なし（自己申告＋eメール、SNSログイン等）		×	×	×	×	×	×	×	**0**

ニュージーランド/BALの要件を参考にしたDADC/BALの考え方

NZレベル	1	2	3		4		DADC BAL (Entity Binding Assurance Level)
		BA3.02	BA3.02	BA3.06	BA3.02	BA3.06	
	なし	依拠当事者が、以下の紐づけ要素タイプを用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、以下の紐づけ要素タイプを用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、可能な場合に詐欺対策技術を適用すること	依拠当事者が、以下の紐づけ要素タイプを用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、可能な場合に詐欺対策技術を適用すること	
		[MUST]最低でも 1 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[MUST]最低でも 1 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[SHOULD]不正行為対策技術を適用	[MUST]最低でも 1 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[SHOULD]不正行為対策技術を適用	
チーム内で検討した補足条件 / 手法				以下のいずれかを満たせば○ 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する	対面で証明書を渡してる事が保証でき、それが確実に確認出来る場合（ICチップ読取り）に○。	以下のいずれかを満たせば○ 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する	
公的個人認証による署名用電子証明書＋電子署名付契約書	—				○	○	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	—				○	○	**4**
認定認証事業者による電子証明書 ＋電子署名付契約書	—		○	○	×	×	**3**
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	—				○	○	**4**
顔写真のある公的身分証の撮影（表・裏・厚み） ＋容貌の撮影	—				○	○	**4**
公的身分証のリアルタイム撮影	—	○	×	×	×	×	**2**
法律に基づく身元確認のAPI連携 （銀行API、携帯キャリアAPI等）	—		○	○	×	○	**3**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	—	○	×	×	×	×	**2**
身分証確認なし（自己申告＋eメール、SNSログイン等）	—	×	×	×	×	×	**0**

DADCが提案する民民手続におけるIAL

手法	DADC IAL (Information Assurance Level)	DADC BAL (Entity Binding Assurance Level)	再考後の DADC IAL (Identity Assurance Level)
公的個人認証による署名用電子証明書＋電子署名付契約書	4	4	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3	4	
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	3	4	**3**
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	3	4	調整中
認定認証事業者による電子証明書＋電子署名付契約書	3	3	
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）	3	3	
公的身分証のリアルタイム撮影	2	2	**2**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1	2	**1**
身分証確認なし（自己申告＋eメール、SNSログイン等）	0	0	**0**

今回の整理における IAL間の外形的な違い

・現況確認の有無

・確認対象の有無
・偽造等不正対策の有無

・保有確認の有無

・身分証の有無

新たな手法の検討の必要性

手法	再考後の DADC IAL (Identity Assurance Level)
公的個人認証による署名用電子証明書＋電子署名付契約書	4
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3
顔写真のある公的身分証のICチップ読み取り／顔写真のある公的身分証の撮影撮（表・裏・厚み）＋法律に基づく身元確認済のAPI連携（銀行など）	
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	
認定認証事業者による電子証明書＋電子署名付契約書	
法律に基づく身元確認のAPI連携（銀行API、携帯キャリアAPI等）	
公的身分証のリアルタイム撮影	2
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1
身分証確認なし（自己申告＋eメール、SNSログイン等）	0

既存手法の要件を足し引きすることで、
◈新たな手法の確立
◈新たな手法のIALの明確化
が容易となる

IALが明確な手法の選択肢が広がり、**各事業者が、サービス内容やユーザの特性などを踏まえて、適切な手法を選択しやすくなる**

本日のアジェンダ

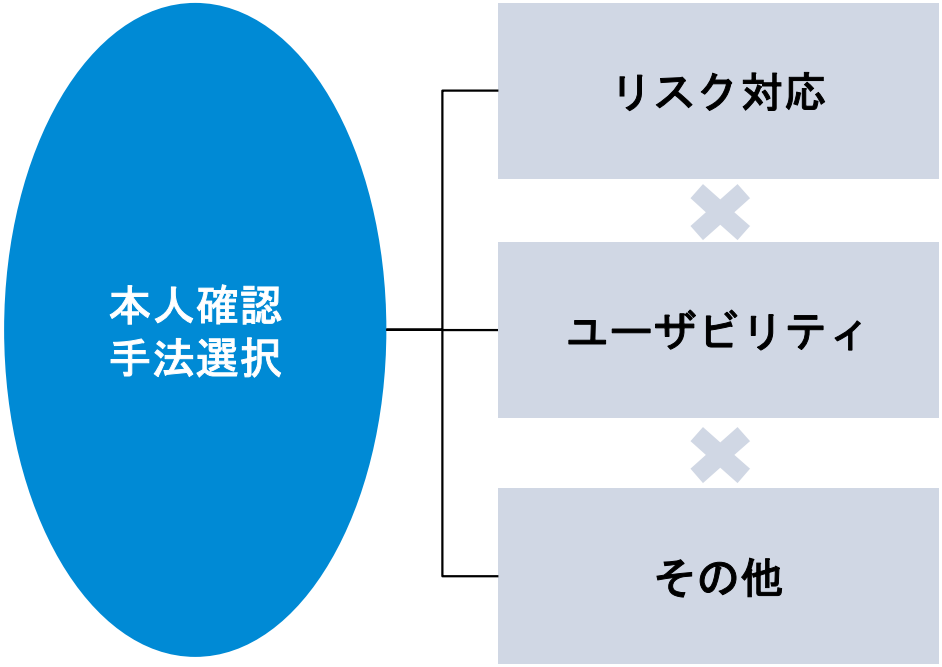
1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. **リスクに応じた本人確認手法選択の考え方について**
4. ガイドラインの策定に向けた進め方について

参考

事業者は、どのように本人確認手法を選択しているか

ラボチームの行ったヒアリングによると、
各事業者は、①リスク対応と②ユーザビリティを重視した上で、コストや事業者の信頼度も踏まえ、
本人確認手法を選択している

本人確認手法の選択軸



ヒアリングでの事業者からの主なコメント

- オンラインで完結できる手法を選択した
- 依頼者が起こすトラブルを回避したい
- 偽造身分証を防ぎたい

- セキュリティを強化するとユーザーのハードルが上がるが、サービスが使われないと意味がない。本人確認を強固に行うことで、利用者のハードルがどれだけ上がるかのバランスで手法を決めた

- コストとのバランスを見ながら（身分証の偽造を検知するという）目的を達成できる手法を選択した
- 当社の求める目的に過不足ない適切な手法を提示してくれた(eKYCサービス事業者の信頼度)

本インキュベーションラボにおける検討事項

本インキュベーションラボでは、「リスクに応じた本人確認手法を選択できる」という目的を踏まえ、
まずはリスクに関して、事業者が捉えているリスクレベル等について調査・整理した

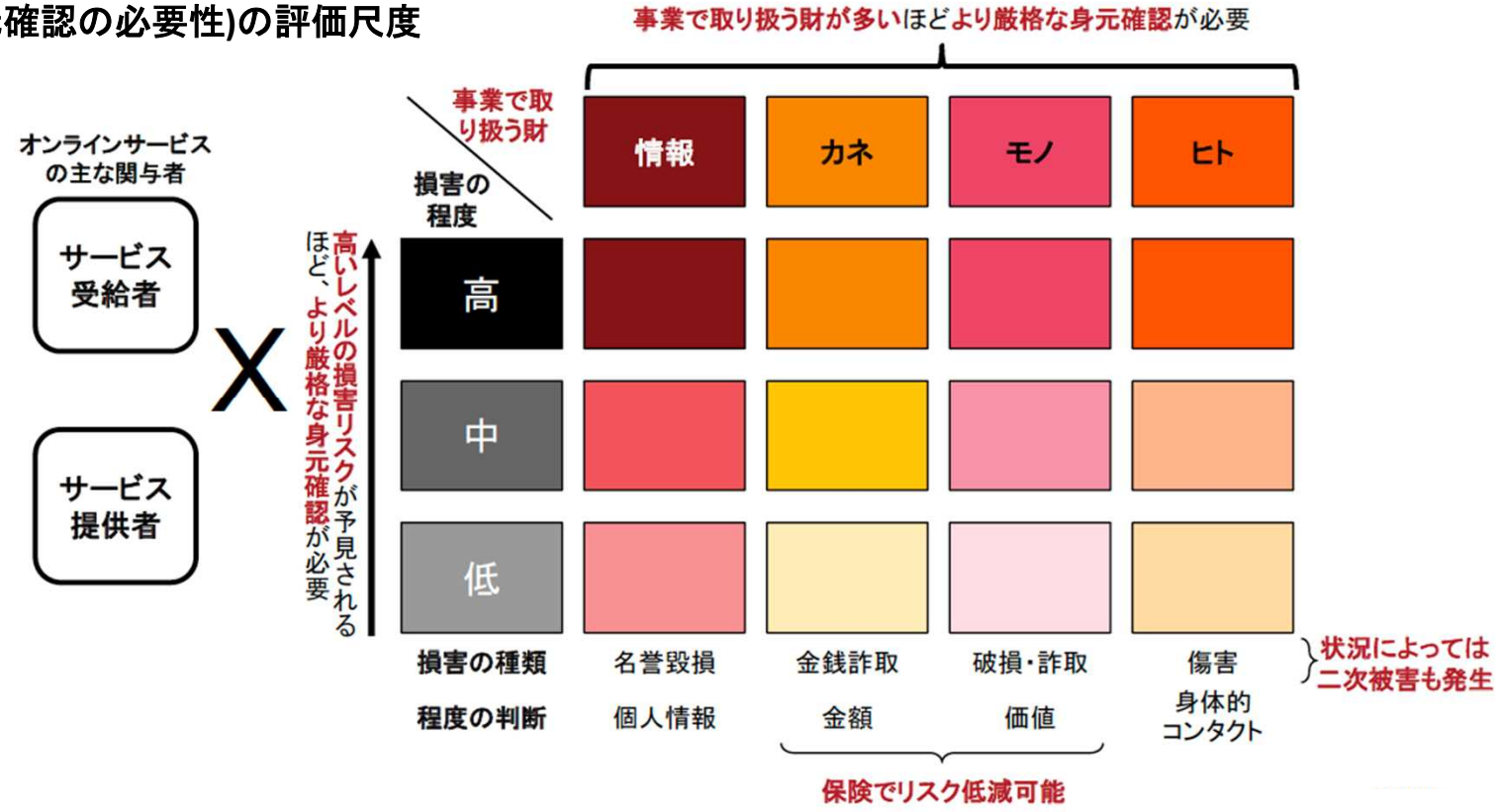
検討事項の整理

本人確認手法の選択軸	論点	検討の方向性
リスク対応	● 事業者がどのようなリスクを抱えて、本人確認で対応しているか ● 本人確認で対応できている点、できていない点 等	**本インキュベーションラボで検討を開始**
ユーザビリティ	● ユーザーにとっての負荷をどう整理するか ● 既存の手法をユーザビリティの視点でどう整理するか	手法のレベル整理を行った後、議論すべき論点
その他	● コストについては、各eKYC事業者の競争領域で、ガイドライン等では対象外 ● eKYC事業者の信頼度については、認証制度等も考えられるが、本ラボのスコープ外と思料	コストは、各事業者判断。事業者の認証等は将来的な課題

前回研究会におけるリスクの整理

経済産業省「オンラインサービスにおける身元確認に関する研究会」では、リスク評価の際には、事業で扱う財とその内容や関与者、保険/補償の有無、二次被害の可能性、等を踏まえた被害程度を見積る必要性が指摘された

事業リスク(身元確認の必要性)の評価尺度

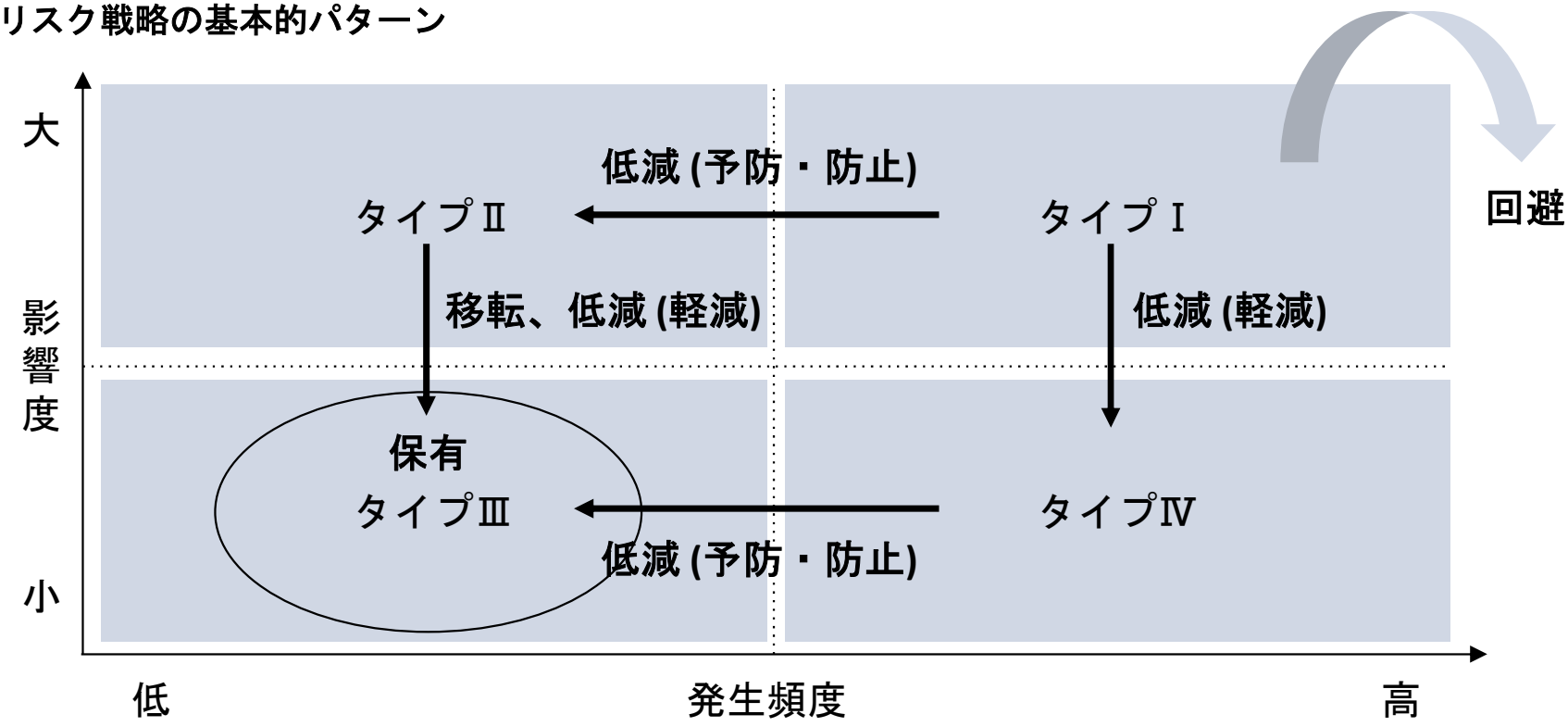


出所：経済産業省 (2020)「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より

ヒアリングにおける示唆・事業リスクに関する整理

一般的にリスクマネジメントでは、各リスクを影響度と発生頻度のリスクマップ上にプロットし、各社が優先順位をつけて適切なリスク戦略を選択している。「リスクに応じた本人確認手法の選択」をガイドライン化するためには、リスク評価・リスク戦略等の手法を参考に「リスクの標準化」が課題となる

リスク戦略の基本的パターン



リスク戦略の例

- 移転:
  損害保険
- 低減(予防・防止):
  本人確認
- 低減(軽減):
  サービスごとに立案
- 回避:
  事業撤退

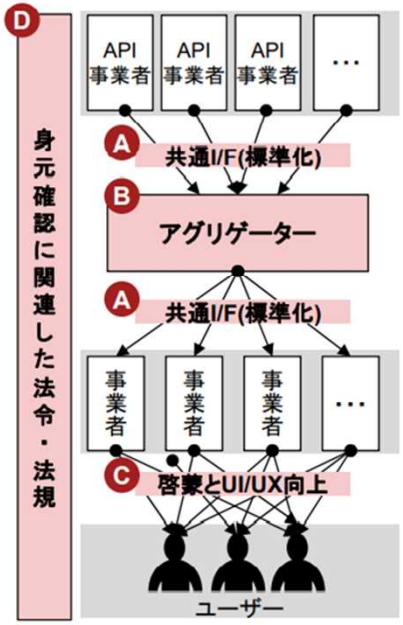
出所：経済産業省 (2005)「先進企業から学ぶ事業リスクマネジメント実践テキストー 企業価値の向上を目指して ー」より

ヒアリングにおける示唆・ユーザビリティについて

本人確認を実施することによるUXの悪化を懸念する意見も得られた。
リスク対策と、ユーザビリティ確保の両立を実現する必要がある。

（参考）「オンラインサービスにおける身元確認に関する研究会」で提示されたアグリゲーターを設置する案

ステークホルダーと論点



論点詳細

A どの標準化動向に、どこまで合わせていくか
- 国際標準、先行プレイヤー等のどの基準にあわせていくか
- 合わせる場合はどこまで合わせていくか

B アグリゲーターの必要性と、どこまで任せるか
- 官、民どちらが行うか、民で行う場合の競争環境をどう考えるか
- APIを取りまとめるだけなのか、ユーザー情報のアグリゲートまで行うのか
- e-KYC事業者等の認定の仕組みが必要ではないか
- 産業毎・アグリゲーター毎の相互接続性を担保できるようにすべきではないか
- データ連携技術で、実装としての共通I/F化が必要ではないか

C UI/UXを向上し、どう利便性向上を図るか
- 国際標準、先行プレイヤー等のどの基準にあわせていくか
- 事業者間の協調及び、ユーザーへの普及をどうやって推進するか

D 身元確認に関連した法令・法規は、それぞれどのように整合しているか

(参考)
標準化・アグリゲーター設置のメリット

- 対象
  - オンラインサービス等の身元確認を活用する事業者
  - 身元確認API事業者
- 効果
  - 開発、接続、カバレッジ、オペレーション等が全て効率化される
    - API・データの仕様を詳細レベルで揃え、共通I/Fで事業者へ提供
    - 複数の身元確認API提供者を束ねて、ユーザーカバレッジが向上
    - 身元確認API業者と事業者との契約・請求業務が一本化される

(参考)
中長期的な検討事項

- マイナンバーカードとの連携、保険証や資格情報[1)]との連携、在留外国人のデジタルアイデンティティの活用、更には海外での活用等の観点も考慮をしておくことが必要か

出所：経済産業省 (2020)「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より

本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. **ガイドラインの策定に向けた進め方について**

参考

ガイドライン策定に向けた進め方

サービスに応じた本人確認手法の提案に向けて

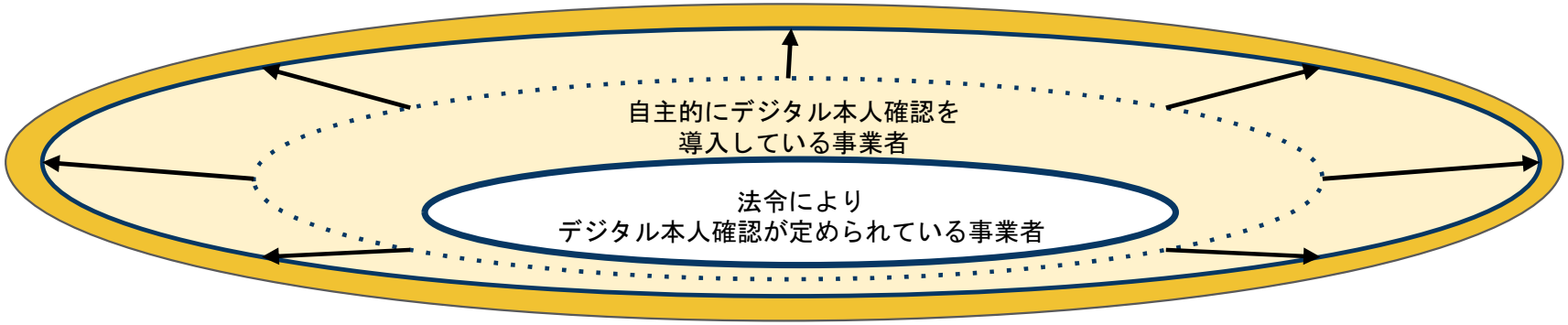
検討内容	① 身元確認手法 の保証レベルの整理	② リスク対応 ユーザビリティの検討
進捗	ニュージランドの基準参考に DADC　IAL案を策定	ヒアリングを実施し、 リスクについて検討開始
今後の 予定	専門家の意見を交え IAL案を確定	幅広い事業者から意見を収集 し、考え方を整理

ガイドラインの策定

ガイドライン策定後の社会

ガイドラインの策定

「分からない」課題が解決し、デジタル本人確認の普及が促進



ガイドライン策定後は下記のニーズが高まることが想定される

ガイドラインのアーキテクチャに基づき、
技術革新に対応した新たな手法

ガイドラインに沿って、的確な手法を
提案する「信頼できるID Provider」

本日のアジェンダ

1. 本インキュベーションラボの背景と目的
2. オンラインの身元確認手法のレベル分けについて
3. リスクに応じた本人確認手法選択の考え方について
4. ガイドラインの策定に向けた進め方について

参考

海外動向調査

- 海外動向についてネットを中心に調査
- スウェーデン、シンガポール、イギリス、ドイツ、エストニア、インドの６ヵ国
- 各国「サービス概要」、「利用状況」、「普及または失敗した背景」、「留意すべき日本との違い」についてまとめました。
- 本人確認も含まれますが、主にデジタルIDを中心とした各国の全体的な取り組み状況についてとなります。

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
1	スウェーデン ・人口：約1,022万人（2018年11月，スウェーデン統計庁） ・面積：約45万平方キロメートル（日本の約1.2倍）	民間主体	Bank ID ・口座開設時に付与 ・IDはパーソナルナンバーと紐づく	2003年に開始。 運営主体は、銀行７行のコンソーシアム。 国の関わり：2004年、電子政府のオンライン申告や申請手続きに使用するデジタルIDに選定される。パーソナルナンバーに紐付けられており、オンラインで各種申請や手続きを行う際の本人認証手段として、Bank IDが利用されている。 2009年、国税庁がBankID利用者の優遇税制を設け利用拡大。BankIDによる電子署名には、法的拘束力がある。	・登録者数：820万人（2019年）人口普及率80%以上。 ・対応可能なサービス：公共サービス：確定申告、各種行政手続、病院関連の手続き等 ・民間サービス：銀行取引、決済サービス、電子商取引、ポイントサービス等 ・BankIDの電子署名は、eIDASのルールを遵守する電子署名法に基づく法的効力のある署名	**普及のきっかけは、2010年にモバイルBank IDが導入され利便性が高まったこと。2012年にはモバイルP2P決済サービス「スウィッシュ(Swish)」の認証手段にBank IDが使われたことで、一気に利用が広がる。**	・パーソナルナンバー（日本のマイナンバーに相当）開始年：1947年 ・ナンバーから生年月日と出生地が一目瞭然。元々ナンバーを使う機会が多く、国民の抵抗感が低い ・高い透明性と国への信頼：公的機関における個人情報の取り扱いの適正性については、独立機関が監督。希望者に対しては公的機関の保有する自己に関する情報を毎年提供し、官庁間や官から民への情報提供ルールが法令で規定されているなど、透明性の高い仕組みが構築されている。 ・国民の プライバシー意識：センシティブな情報の対象範囲が狭い。収入や納税額もオープン。

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
2	シンガポール ・人口：約569万人（うちシンガポール人・永住者は404万人）（2020年） ・面積：約720平方キロメートル（東京23区と同程度）	政府主体	National Digital Identity（NDI） SingPass	・国が主導してNDI（国家デジタル認証）と呼ぶ官民共通のデジタルIDスキームの開発・普及を推進している。 ・NDIは、識別子となる個人登録番号（NRIC番号）と既存の公的認証システム「SingPass」、個人情報の登録・利用の一元化サービス「MyInfo」を基盤とし、市民が単一のデジタルIDで官民のサービスを利用できる共通認証プラットフォームの構築を目指すプロジェクトである。	SingPass/My Infoという既存のサービスは、70の政府機関が提供する160のデジタルサービスの認証基盤として活用されている。今後は民間企業も個人認証のためにNDIプラットフォームを利用できるようになる予定である。 ・SingPassに実装されたクラウドベースの顔認証は、生体認証スキャンによって得られたユーザーの顔データを政府に保管されたデータベースと照合することで、本人確認を行う。政府機関だけでなく、銀行・保険などの民間企業に対しても開放しており、インターネットバンクの新規利用申し込みに必要な本人確認手続きにも利用されている。	**2018年にスマートフォンの生体認証を利用するSingPass Mobileが始まり、2019年には公的身分証明書（NRICカード）を見せなくても本人確認と必要な個人情報を提供可能とするSG Verifyが導入された。** 企業は、独自のインフラやシステムを構築しなくても、政府が提供するNDIの共通APIや各種ツールを使って認証基盤を導入することが可能となり、コスト削減や安全性の強化に繋がる。	・シンガポールのスマートネイション構想は、わが国が推進するソサエティ5.0と類似する点が多く、先行事例として位置づけることができる。

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
3	イギリス ・人口：6,680万人（2019年） ・面積：24.3万平方キロメートル（日本の約3分の2）	政府主体	GOV.UK Verify	2016年に公共サービスの共通認証プラットフォーム「GOV.UK Verify（Verify）」が導入された。オンラインで公共サービスを利用するにあたり、政府の認定を受けた複数のIDプロバイダーのなかから、利用者自身が使用する認証サービスを選択する仕組み	Verifyは当初の計画通りには普及が進んでいない。	普及が進んでいない理由として、**ユーザーエクスペリエンスが不十分であることや、関係する省庁が必ずしも協力的ではないこと、民間サービスプロバイダーの求める要件を満たすものではないことなどが指摘されている。**政府は、2019年に省庁横断的にデジタルIDを推進する組織を設置し、Verifyに代わる新たなデジタルIDの在り方を検討している。	**・識別子となる統一的な国民番号がないことが課題として指摘されている**
4	ドイツ ・人口：約8,319万人（2020年9月、独連邦統計庁）	民間主体	Verimi	業界横断型の連合で消費者データのプライバシーを優先し、FacebookとGoogleの二大覇権に対抗することを目指している。 従来のプラットフォーマーと異なり、参加企業が集めたデータをどう使うかをユーザーの選択に委ねている。ユーザーが同意しない限りデータは広告や外部企業に使われることはない。	自動車メーカーのダイムラー（Daimler）や保険大手のアリアンツ（Allianz）、ドイツ銀行（Deutsche Bank）も参加している。ドイツの航空会社ルフトハンザ（Lufthansa）や通信会社のドイツテレコム（Deutsche Telekom）、ITセキュリティ会社のブンデスドルクレイ		

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
5	エストニア ・人口：約133万人（2021年）日本の約9分の1 ・面積：4.5万平方キロメートル（日本の約9分の1）	政府主体	・Mobile-ID（SIMカード） ・Smart-ID（アプリ）	・Mobile-IDは身分証明書法で本人確認手段として定められているモバイル端末を利用するSIMカード ・Smart-IDはモバイル端末で利用するアプリ 「世界で最も先進的なデジタル社会」と名付けられたエストニアは、政府サービスの99%がオンラインである	・2002年エストニア政府はエストニア版マイナンバーカード「e-IDカード」を国民に配布し、従来は役所に訪問しなければ不可能だった本人確認をオンライン上で可能にした。現在エストニアでは99%の行政申請がオンラインで可能であり、連携したサービスも2,700を超える。 ・結婚、離婚、不動産の手続き以外は全部オンラインでできる。	e-IDカードにも不便な部分は指摘されてきた。e-IDカードで認証を行うためには、カードリーダーを持ち歩き、物理的なカードで認証させなくてはならず、導入当初は利用者からの不満も多かった。**そこで誕生したのが「デジタルIDアプリ」だ。初回登録時にe-IDカードを認証し、アプリと紐付けることで公的身分証による本人性を担保する。それによって、毎回カードリーダーでe-IDカードを読み取る不便さがなくなり、利便性が向上した。現在は国民の35%が「デジタルIDアプリ」を利用している。**	“国の規模”が小さい

海外動向調査

#	国名	区分	サービス名	サービス概要 （取り組みの概要）	利用状況 （結果や現状）	普及または失敗した背景	留意すべき日本との違い （文化、風習、国民性…）
6	インド	政府主体	国民IDシステム「Aadhaar（以下アドハー）」	NECの技術が基盤となっているアドハーは、インドの固有識別番号庁（UIDAI）によって登録が進められている生体認証IDシステムで、国民の名前や住所、生体情報を収集して管理する。システムに登録された国民1人ひとりに12桁の数字からなるIDを発行し、役所などの公共機関や銀行はこの固有のIDを使って社会保障の受け取りや銀行口座開設の本人確認をスムーズに行うことができる。	・2009年から導入された国民IDシステム「Aadhaar」。既に12.3億人以上が登録し、公共福祉サービスが効率的に支払われるようになり、不正行為も激減した。 ・指紋、顔、および虹彩認証を組み合わせた、超高精度なマルチモーダル生体認証。 **・インドのデジタルID普及割合は銀行口座保有者の割合と比例して増加しており、口座を保有できることが1つのデジタルID普及のドライバーになったと考えられる。**2008年時点では人口の4%程度しかIDを持っていなかったが、2018年には10億人以上がIDを保有するようになった。	「デジタル化」されたIDシステムによって、国民が、公共サービスや福祉支援、金融サービスを公平に享受できるようになっている。またインドの成長の足かせとも言われ、長年にわたって深刻な問題となっていた汚職や不正が減ったことで、政府はこれまでに124億ドル（約1.37兆円）の不正支出をなくすことに成功している。 iSPIRT(非営利団体)によれば、企業がユーザーデータから利益を得ていることが問題なのではなく、ユーザーが自分のデータから恩恵を得られないことが問題であるとしている。このため、銀行口座とデジタルIDの紐づけやデータ接続を個人に管理できる環境を提供することで、ユーザーが自分のデータを適切に生かして企業からメリットを得やすくしている。	・10億人をこえる市民に対していかに効率的に行政サービスを提供するかという観点からデジタルテクノロジーの導入を進めた。 ・整備が必要なのは、市民が行政に対して提供したデータを、どの機関に、そこまで共有するかを確認する機能や、行政側からの通知を一元的に受ける機能の提供。個人情報の保護とワンスオンリーを同時に実現するには、事故データの共有先を管理できる機能が欠かせない。

海外動向調査まとめ

- スウェーデンやシンガポール、エストニアの例から、デジタルIDがスマートフォンに搭載され物理的なカードを使わずに本人確認が行えることでユーザーの利便性が高まり、一気に普及していくケースがみられた。

- デジタルIDや本人確認サービスの一極集中について、スウェーデンでは、①単一IDプロバイダーへの過度の依存はリスク、②イノベーションや品質、価格面での競争が不在、③移民や銀行口座のない個人などが排除、などの問題点が指摘されている。また、シンガポールでも中央集権型のシステムであるためトラブルが発生すると機能不全となる事態や、民間企業の採用が想定通りに進むか、といった課題がある。

- イギリスでは、2000年代に入ってテロ対策や犯罪予防等の観点から、厳格に本人確認できる手段として国民IDカードの導入が議論され、IDカード法が成立したものの、費用対効果やプライバシー侵害等が問題視され、政権交代とともに同法は廃止された。この代替策として、2016年に公共サービスの共通認証プラットフォーム「GOV.UK Verify（Verify）」が導入された。政府の認定を受けた複数のIDプロバイダーのなかから、利用者自身が使用する認証サービスを選択する仕組みであるが、Verifyは当初の計画通りには普及が進んでいない。その理由として、ユーザーエクスペリエンスが不十分であることや、関係する省庁が必ずしも協力的ではないこと、民間サービスプロバイダーの求める要件を満たすものではないことなどが指摘されている。政府は、2019年に省庁横断的にデジタルIDを推進する組織を設置し、Verifyに代わる新たなデジタルIDの在り方を検討している。もっとも、識別子となる統一的な国民番号がないことが課題として指摘されている。

- シンガポールのCODEX等、階層化されたアーキテクチャーを前提にデータ層・サービス層を分離した立体的な階層構造で構築、民間にも広く開放している。

海外動向調査 主な参考ソース

- 「行政をハックしよう」吉田 泰己(著)　ぎょうせい
- 日本総研「デジタル時代の社会基盤「デジタルID」」
  https://www.jri.co.jp/MediaLibrary/file/report/jrireview/pdf/11717.pdf
- エストニアの電子証明書等について（総務省）
  https://www.soumu.go.jp/main_content/000731090.pdf
- ドイツのパブリッシャー、共通ログインで「異業種」連携：FacebookとGoogleの2強に対抗
  https://digiday.jp/publishers/german-publishers-joining-forces-duopoly/
- インド13億人の「生体認証」国民IDに、知られざる日本企業の貢献
  https://wisdom.nec.com/ja/collaboration/2019051701/index.html
- GAIN DIGITAL TRUST
  https://gainforum.org/GAINWhitePaper.pdf