



TRUSTDOCK

デジタル社会の本人確認に関するアドバイザリーボード 第一弾取りまとめ 附属資料

2021年12月14日

株式会社TRUSTDOCK



共創志向の「社会インフラ」を目指して

『デジタルアイデンティティとeKYCの社会インフラを確立する』

これが私たちTRUSTDOCKのミッションです。

TRUSTDOCKは、設立以来、eKYCの専門会社として挑戦を続けています。

自社のみで考え、自社のみの利益を追求する発想では、
この領域で信頼される社会インフラをつくることはできません。

例えば、私たちeKYCサービス事業者は、大切な個人情報数を多く取り扱っています。
しかしながら、法令に基づきeKYCサービス事業者に特化した特別な取扱いを求められることはありません。

私たちは思います。

法令に定めがなくても、eKYCサービス事業者のあるべき姿に率先して取り組んでいきたい。
一足飛びにSFな未来を進めるのではなく、常に半歩先の未来を提供し、
社会インフラづくりを牽引していきたい。

こうした思いを形にできるように、
様々な分野の有識者の皆様のご助言をいただいて視野を広げ、
視座を高め、サービス提供に活かし、社会に発信していく。

私たちが新しい私たちになるために、私たちが新しいデジタル社会をつくるために、
アドバイザリーボードは不可欠な存在です。

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

01 アドバイザリーボードの設置

02 これまでの議論の概要

- 02-01 ユーザー意識調査の結果概要
- 02-02 オンライン本人確認における保証レベルについて
- 02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

- 02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任
- 02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

デジタル社会の本人確認、認証、デジタル ID等に関する課題について、第三者の視点を取り入れながら検討、判断、発信等を行っていくため、有識者の方々に構成されるアドバイザリーボードを設置しました。

基本理念

本人確認・認証・デジタルIDにおいて、

- eKYCサービスを提供する事業者とは、どのようにあるべきか
- 社会にとって、どのようなプロダクトや技術が必要か
- 社会全体として、どのようなルールが求められているか

こうしたテーマについて、eKYCサービス提供側の専門的な知見だけでなく、生活者や社会の視点も交えながら、外部の有識者とともに、検討・判断・発信等を行い、デジタル社会に不可欠なインフラ構築を進めること

検討内容

- eKYCサービス事業者の個人情報の取扱い、セキュリティ対策のあり方
- 本人確認手法の安全性等の整理、簡略な手法 等

アドバイザリーボードは有識者 3名で構成し、当社役職員と議論しながら、専門的知見を提供いただいています。

	所属・氏名	専門領域	主要政府委員歴
座長	 中央大学 石井 夏生利 教授	- プライバシー - 個人情報保護法 - 情報法	- 総務省「プラットフォームサービスに係る利用者情報の取扱いに関するWG」構成員 - 総務省「デジタル時代の地方自治のあり方に関する研究会」構成員 他多数
メンバー	 武蔵大学 庄司 昌彦 教授	- 情報社会学 - 地域情報化 - 電子行政 - 情報通信政策 - オープンデータ・パーソナルデータ活用	- デジタル庁「データ戦略推進ワーキンググループ」構成員 - デジタル庁「マイナンバー制度及び国と地方のデジタル基盤抜本改善ワーキンググループ」構成員 - 総務省「自治体システム等標準化検討会」座長 他多数
	 宮内・水町 IT法律事務所 宮内 宏 弁護士	- 電子契約 - 電子文書保存 - 電子文書の法的有効性確保 - 電子帳簿保存法対応 - IT法務 - 企業法務等	- 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」構成員 - 総務省「プラットフォームサービスに関する研究会」構成員 他多数

アドバイザリーボードをこれまで5回開催し、「信頼されるeKYCサービス事業者」を中心テーマとして、議論や意見交換を行ってまいりました。

	開催日程	主なアジェンダ
第1回	2021年7月27日	● TRUSTDOCKが考える「信頼されるeKYCサービス事業者」とプライバシーポリシーの改訂について ● 「信頼されるeKYCサービス事業者」についての意見交換 等
第2回	2021年9月3日	● 「信頼されるeKYCサービス事業者」についての意見交換 等
第3回	2021年10月5日	● 「総務省の省令改正(案)」についての意見交換 ● 「信頼されるeKYCサービス事業者」についての意見交換 等
第4回	2021年10月27日	● TRUSTDOCKの認証取得について ● コミュニケーション戦略について ● 情報の最小化について 等
第5回	2021年11月29日	● アドバイザリーボード第1弾取りまとめについて 等

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

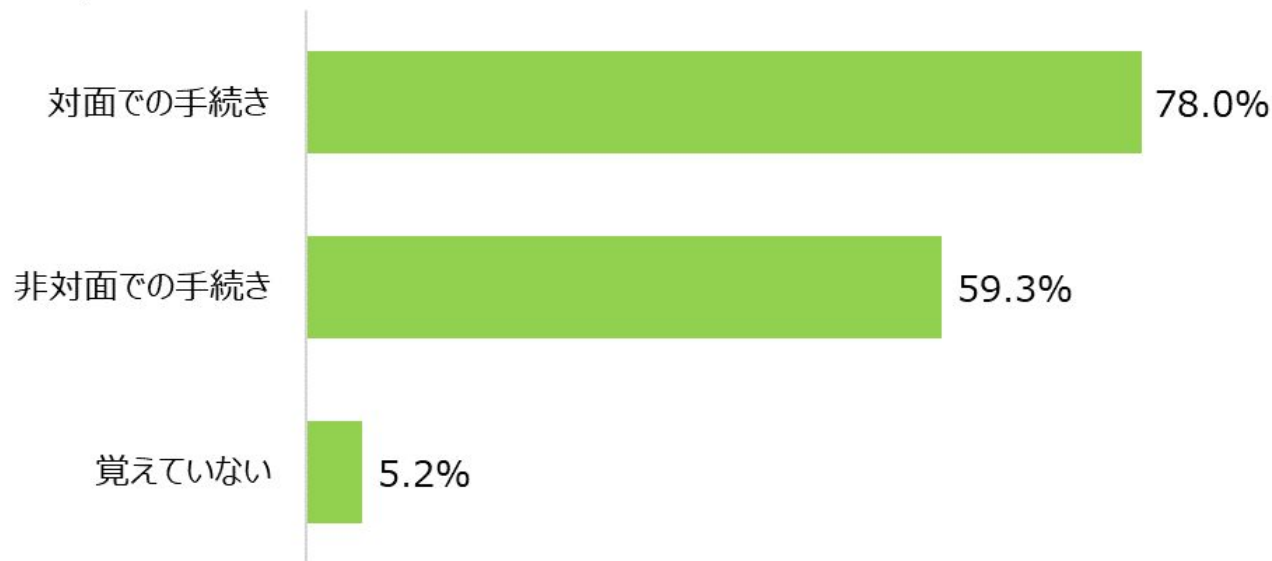
TRUSTDOCKはMMD研究所と共同で、「オンライン本人確認（eKYC）に関する利用動向調査」を実施しました。

調査概要

	予備調査	本調査
目的	eKYC（オンライン本人確認）の利用実態を明らかにすること eKYC（オンライン本人確認）普及の課題を明らかにすること	
期間	2021年7月21日～7月26日	
方法	オンラインによるアンケート調査	
対象者	スマートフォンを所有している 18～69歳の男女 10,000人	左のうち、「オンライン本人確認」 の利用経験者 500人
設問数	10問	15問

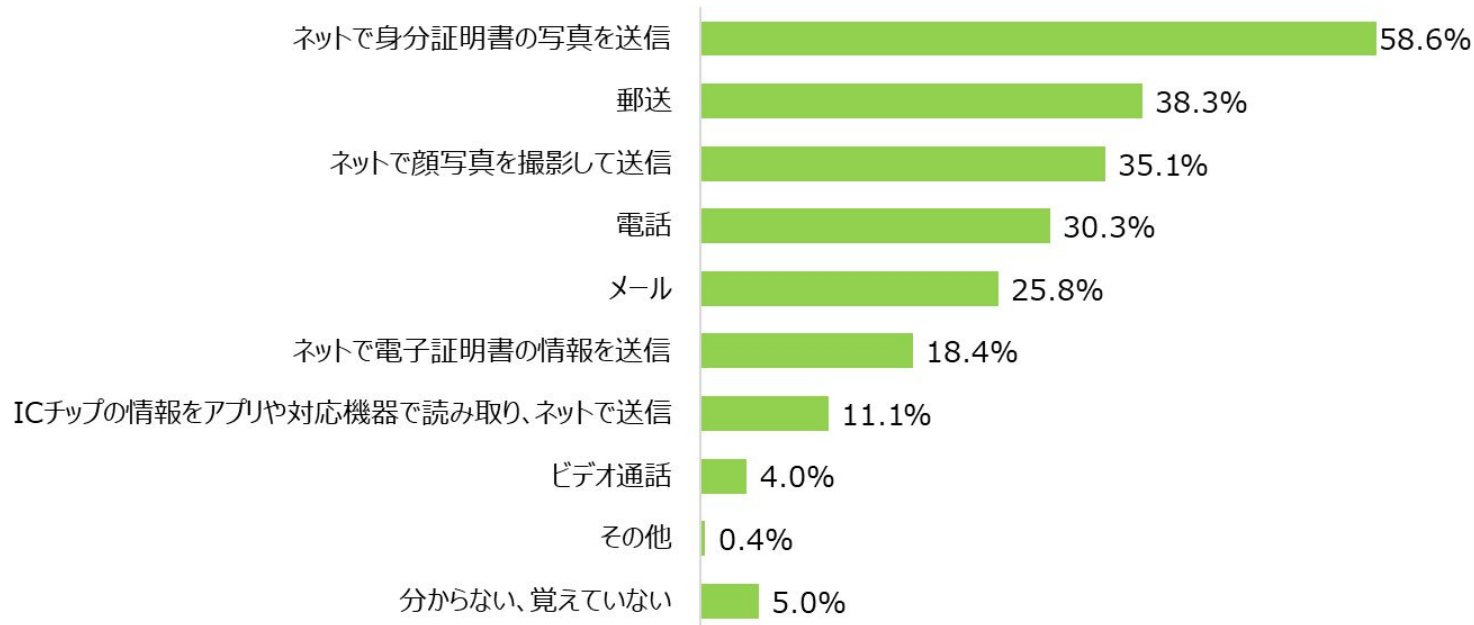
本人確認手続きの手段として、約 6割の対象者が「非対面での手続き」を経験しており、非対面での本人確認が一定程度浸透・認知されています。

● 経験のある本人確認手続きの手段 (n=8,059)



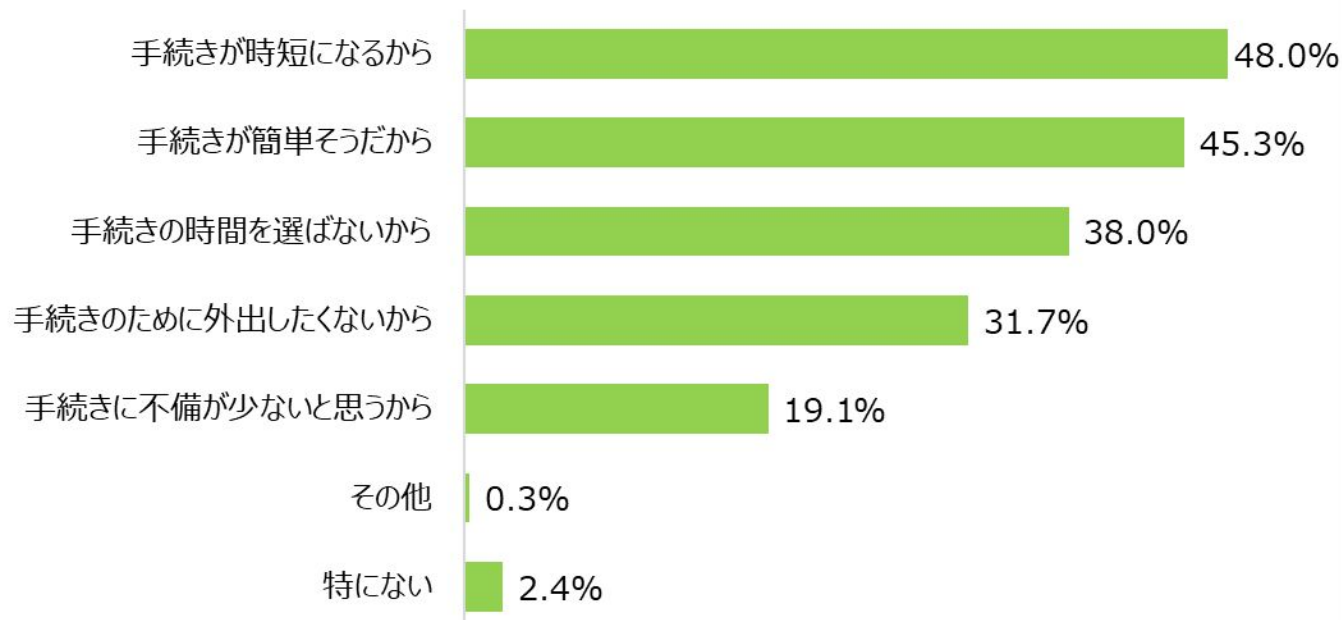
非対面での本人確認手法は、「ネットで身分証明書の写真を送信」が約 6割と最も多く、オンラインでの本人確認が主流となってきています。

● 非対面での本人確認手続き時に利用したことのある手段 (n=4,780)



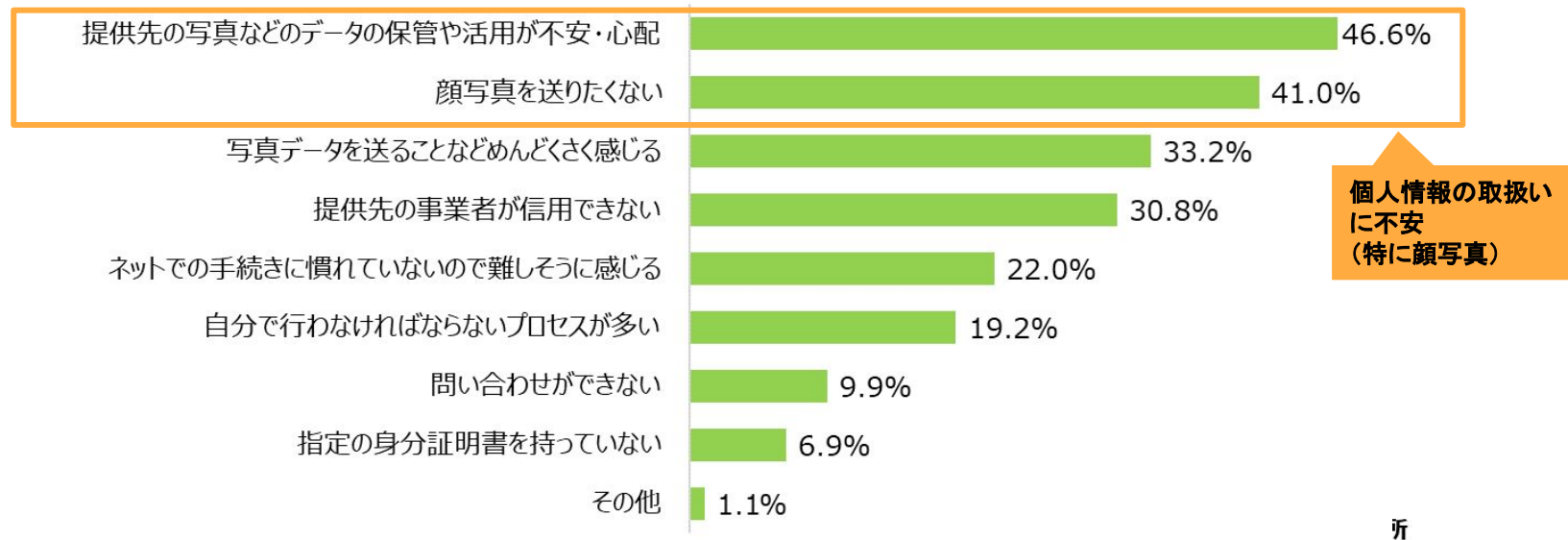
まだeKYCを利用したことがない人がeKYCを利用したいと思う理由は、「時短」「簡単」「時間を選ばない」「外出したくない」と、利便性向上に関する意見が上位を占めました。

● eKYC未利用者のeKYCを利用したいと思う理由 (n=1,016)



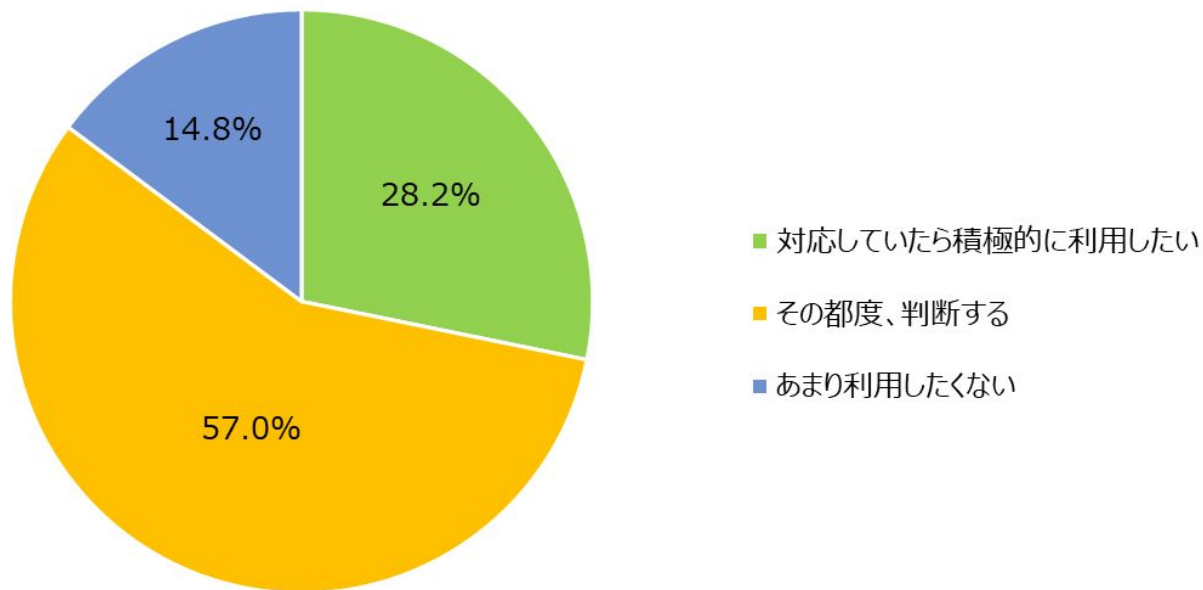
eKYCに対する懸念としては、「写真などのデータの保管や活用が不安・心配」「顔写真を送りたいくない」等、顔写真データを含む個人情報の取扱いに対する不安が多くを占めました。

● eKYC未利用者が持つeKYCに関する懸念や不便なイメージ (n=4,965)



eKYCの継続的な利用意向は「その都度判断する」が約 6割を占めており、eKYCを次回利用するにあたって、eKYCの利便性と懸念を都度判断していると考えられます。

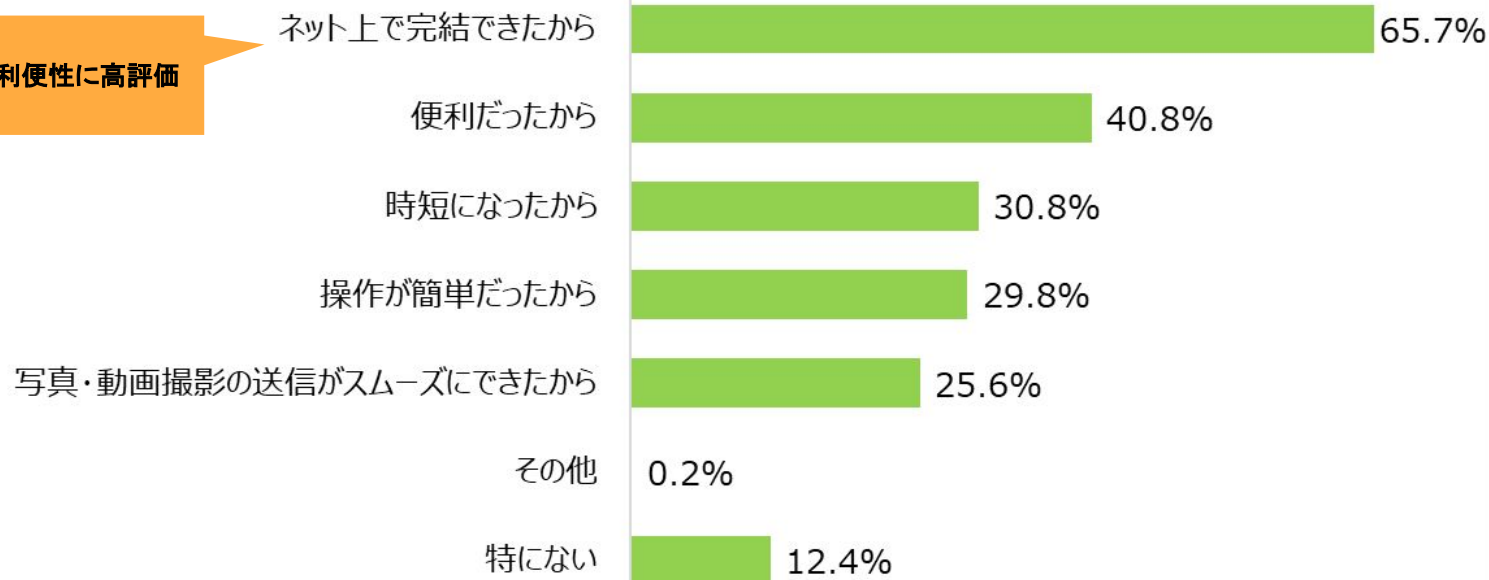
● eKYCを次回以降も利用したいと思うか (n=500)



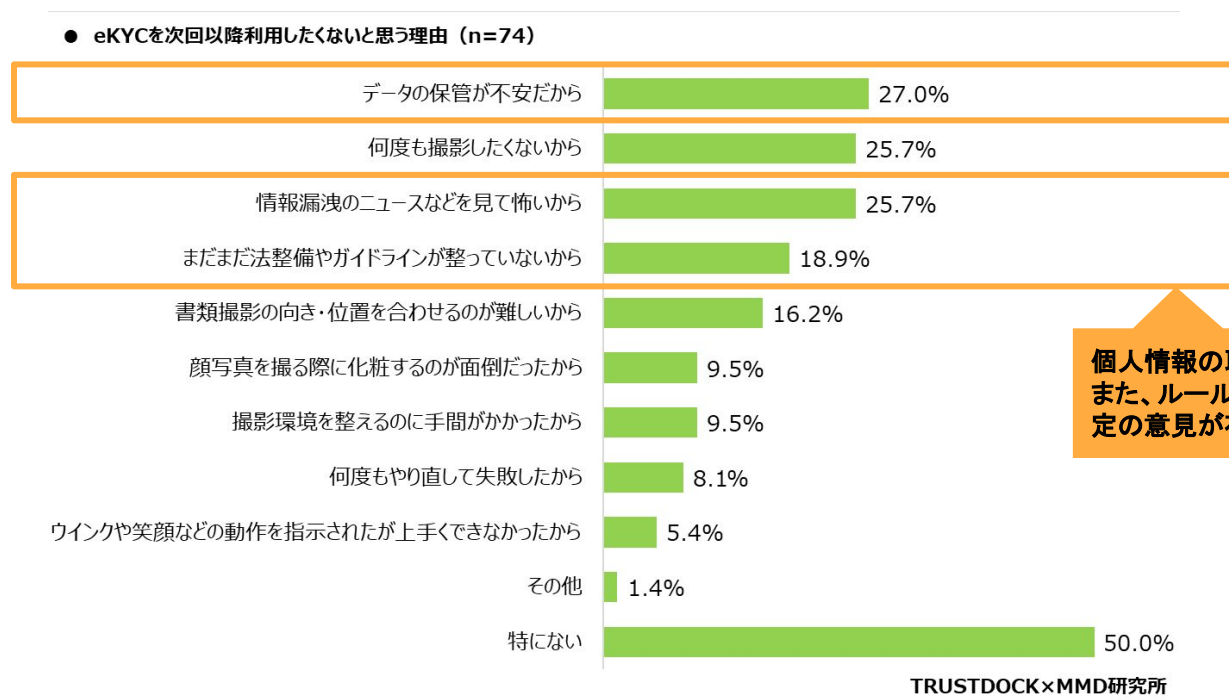
次回以降もeKYCを利用したいと思う理由として、「ネット上で完結」が約 7割を占めたほか、「便利」「時短」など利便性向上に関わる項目が上位を占めています。

● 次回以降もeKYCを利用したいと思う理由 (n=426)

利便性に高評価

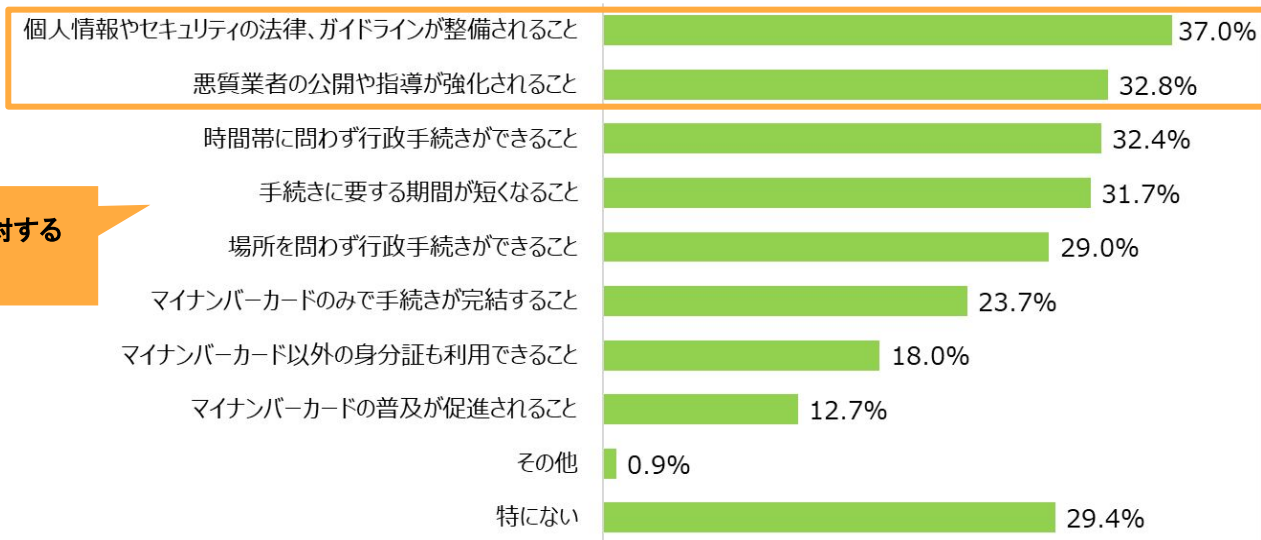


eKYCを利用したくない理由として、「データの保管が不安」「情報漏洩のニュースなどを見て怖い」「法整備やガイドラインが整っていない」等、個人情報の取扱いに不安を感じている方が多い実態があります。



行政手続きのオンライン化に関する要望として、「法律、ガイドラインが整備されること」「悪質業者の公開や指導が強化されること」等、安全性確保に関わる施策等が重視されています。

● 行政手続きのオンライン化が進んだときの行政手続きに関する要望 (n=10,000)



ルール形成や悪質業者の取締が最重要

次いで利便性に対する意見が多い

民民の手続きにおいても同様の回答が想定されるため、ガイドライン等のルール形成が急務である

ユーザーの意識調査からは、eKYCの利便性に魅力を感じているものの、個人情報の取扱いに不安を抱えている実態が明らかになりました。

調査結果まとめ

	利用経験者	利用未経験者
利用したい	● ネット上で完結できる ● 便利 ● 時短になる	● 時短 ● 簡単そう ● 時間を選ばない ● 外出したくない
利用したくない	● データの保管が不安 ● 情報漏洩のニュースなどを見て怖い ● 法整備やガイドラインが整っていない	● データの保管や活用が不安・心配 ● 顔写真を送りたいくない ● 提供先の事業者が信用できない

信頼されるeKYCサービス事業者としては、①個人情報の取扱いの明確化・透明化、②事業者の信頼性確保、③法やガイドラインの整備が重要だと考えます。

信頼されるeKYCサービス事業者になるための視点

ユーザーが感じている不安

- データの保管や活用が不安・心配
- 顔写真を送りたくない
- 提供先の事業者が信用できない
- 情報漏洩のニュースなどを見て怖い
- 法整備やガイドラインが整っていない



個人情報の取扱い



事業者の信頼性



ルールの存在

信頼されるeKYCサービス事業者となるための視点

- 個人情報の取扱いの 明確化・透明化
- 特にユーザーが不安を感じている 顔写真データの取扱いの留意

- 認証取得等による信頼性の確保
- 信頼を維持する 不断の努力

- 法やガイドライン整備への積極関与
- ユーザーの安全性を第一にしつつ、実社会で利用されるルール形成

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

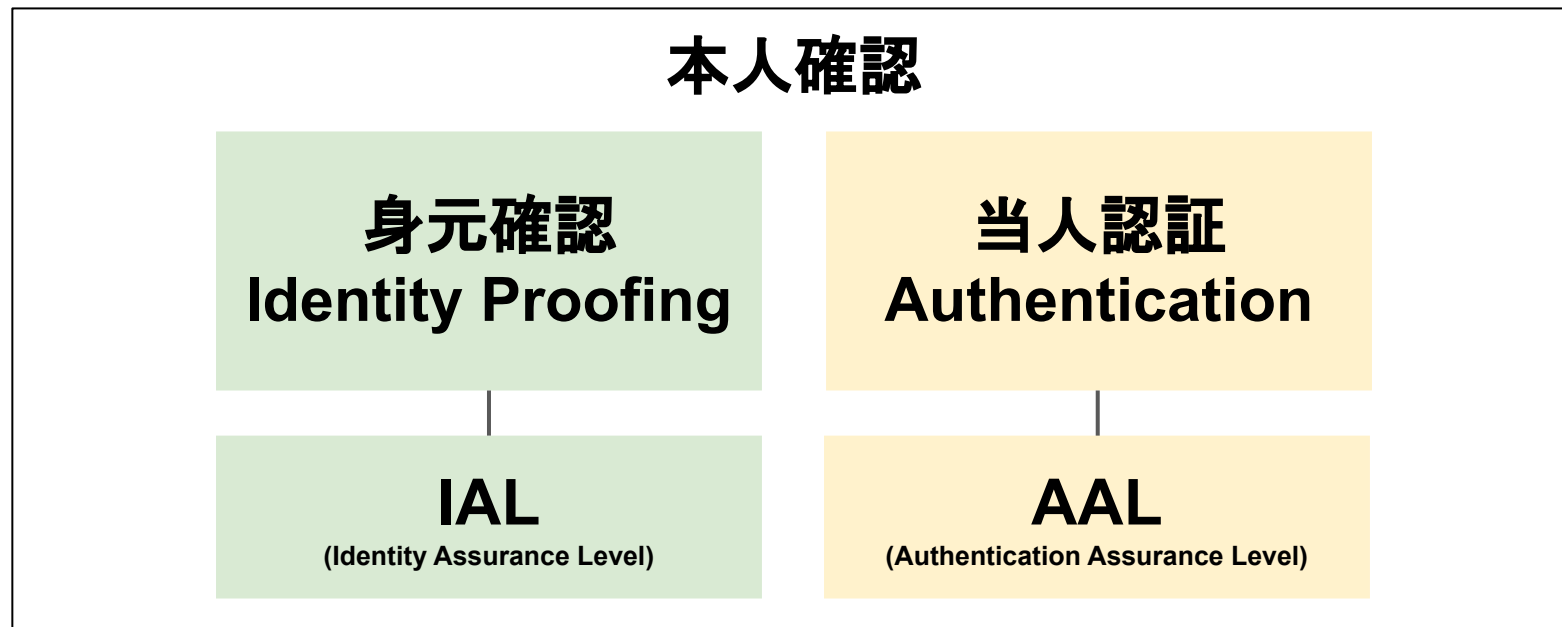
02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

「本人確認」は、その人が実在することを確認する「身元確認」と、その人が登録された本人であることを確認する「当人認証」に分けることができます。

「本人確認」「身元確認」「当人認証」の概念整理



「身元確認」と「当人認証」のそれぞれに強度が設定されており、その掛け合わせで本人確認の強度が決定されます。

「身元確認」「当人認証」の強度

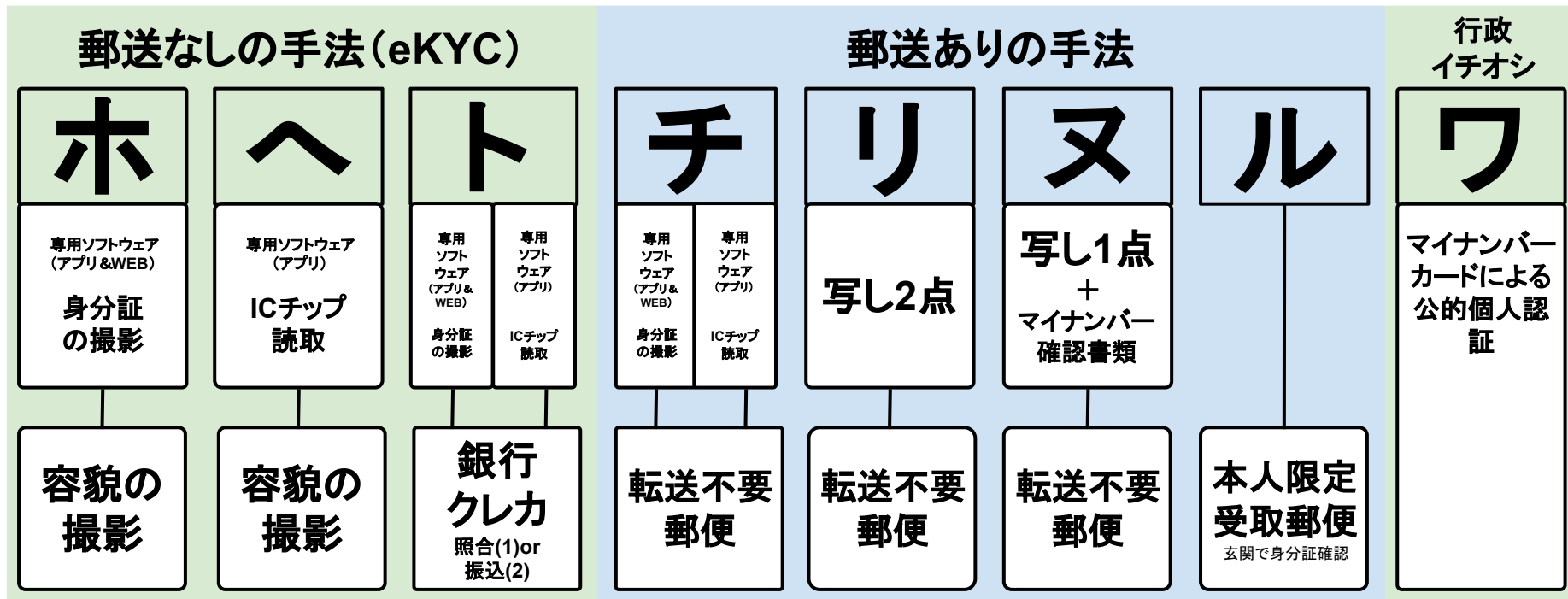
身元確認 (IAL)	当人認証 (AAL)	オンラインによる手法例	
レベル3 対面での 身元確認	レベル3 耐タンパ性が確 保された ハード ウェアトークン	レベルA	- マイナンバーカード(公的個人認証署名用電子証明書)による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード(公的個人認証利用者証明用電子証明書)の耐タンパ性ハードウェアトークンによる当人認証を実施。 - 申請データに対するマイナンバーカード(公的個人認証署名用電子証明書)による電子署名を付与。
レベル2 遠隔又は対面 での身元確認	レベル2 複数の 認証要素	レベルB	マイナンバーカード(公的個人認証署名用電子証明書)等による身元確認でアカウント作成し、アカウント作成後はマイナンバーカード(公的個人認証利用者証明用電子証明書)若しくはこれによることができない場合、その他の多要素認証による当人認証を実施。
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	身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後単要素認証で当人認証を実施。
該当しない	該当しない	レベルD	身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後もアカウントを入力する(当人認証を行わない。)

出所:NIST (2017) “NIST Special Publication 800-63-3 Digital Identity Guidelines”

各府省情報化統括責任者(CIO)連絡会議決定(2019)「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」より作成

犯罪収益移転防止法では、オンラインによる身元確認の手法が複数整理されています。

犯罪収益移転防止法におけるオンラインの身元確認手法



出所: 犯罪収益移転防止法施行規則第1項1号から作成

行政機関向けガイドラインでは複数手法が同じ IALレベルに位置づけられていますが、実際には手法によって強度に差があると考えられます。

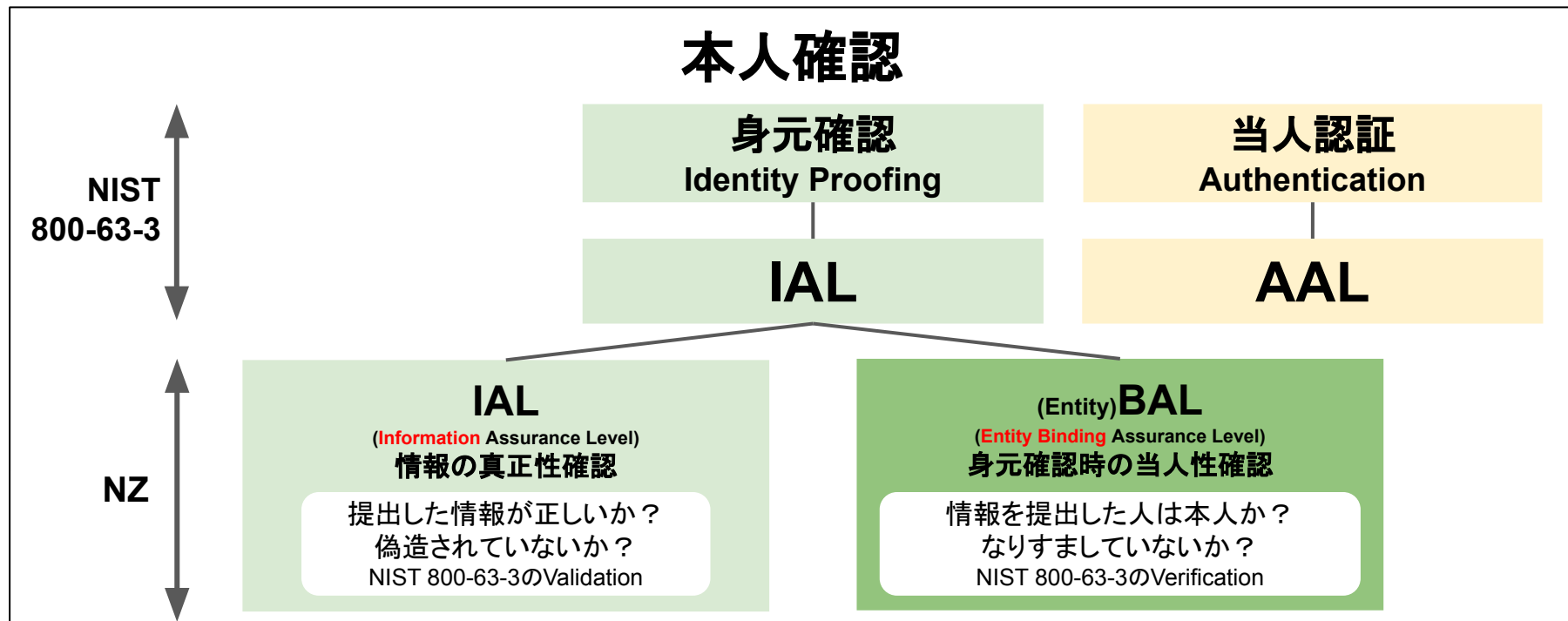
犯罪収益移転防止法における身元確認手法の IALの整理

自主基準	eKYC(身分証撮影+セルフイー)	ICチップ+セルフイー	認定認証事業者電子証明書	公的個人認証
				
身分証の撮影（表・裏）	身分証の撮影（表・裏・厚み）	身分証ICチップ読取	認定認証事業者による電子証明書 +特定取引等に関する情報に署名	マイナンバーカードの署名用電子証明書 +特定取引等に関する情報に署名
				
	容貌の撮影	容貌の撮影	電子証明書のPIN入力	マイナンバーカード 署名用電子証明書のPIN入力

犯収法施行規則 6 条 1 項 1 号	該当なし	ホ	ヘ	ヲ	ワ
強み	利用者が多い		不正・偽造が困難(安全性が高い)		
課題	不正等が多い	一定程度の不正あり	利用者数が少ない		
行政手続きガイド ラインのIAL	2	2	2	2	3

ニュージーランドでは、身元確認レベルの IALをさらに分解し、情報の真正性と身元確認時の当人性を確認する概念が提唱されています。

ニュージーランドにおける IAL分解の考え方



出所: Digital.GOV.T.NZ "Identification Management Standards" より作成

(参考) NZの新しいInformation Assurance Level(仮訳)

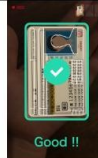
IALレベル	要求事項(レベルごとに差分があるもののみ抜粋)
1	- 情報の正確性: RPはエンティティを証拠として用いるべき。 - エビデンスの質: RPはそのエンティティを証拠として受け入れなければならない。
2	- 情報の正確性: RPは、少なくとも作成時に権威あるソースのコピーを参照した証拠を選択すべき。 - エビデンスの質: RP は証拠を「額面通り」に受け取らなければならない。
3	- 情報の正確性: RP は、少なくとも権威のあるソースのコピーである証拠を選択しなければならない。 - エビデンスの質: RPは、手動で特定された証拠に基づいて品質を決定しなければならず、また、再現す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。
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系統的に識別され、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。

(参考) NZの新しいEntity Binding Assurance Level(仮訳)

BAレベル	要求事項(レベルごとに差分がある部分を抜粋)
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。
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。
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。
4	- エンティティと情報との関係の確立: RP は、コントロール AA6.04、AA6.05、AA7.01 に準拠した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。

既存の身元確認手法に対してBAL等の概念を適用することにより、IALのレベルの細分化を検討することができると考えています。

既存のIALに対してBALを適用したイメージ (例示)

	自主基準	eKYC(身分証撮影+セルフイー)	ICチップ+セルフイー	認定認証事業者電子証明書	公的個人認証
Information Assurance 情報の真正性確認					
	身分証の撮影 (表・裏)	身分証の撮影 (表・裏・厚み)	身分証ICチップ読取	認定認証事業者による電子証明書 +特定取引等に関する情報に署名	マイナンバーカードの署名用電子証明書 +特定取引等に関する情報に署名
Entity Binding Assurance 身元確認時の当人性確認					
		容貌の撮影	容貌の撮影	電子証明書のPIN入力	マイナンバーカード 署名用電子証明書のPIN入力
行政手続きガイド ラインのIAL	2	2	2	2	3
Information Assurance Level	コピースキャンNGのため 2といえない可能性あり	2 (or 3)	3	3	4
Entity BAL	-	3	3 (or 4)	3	3

さらなるレベル
分けが可能か？

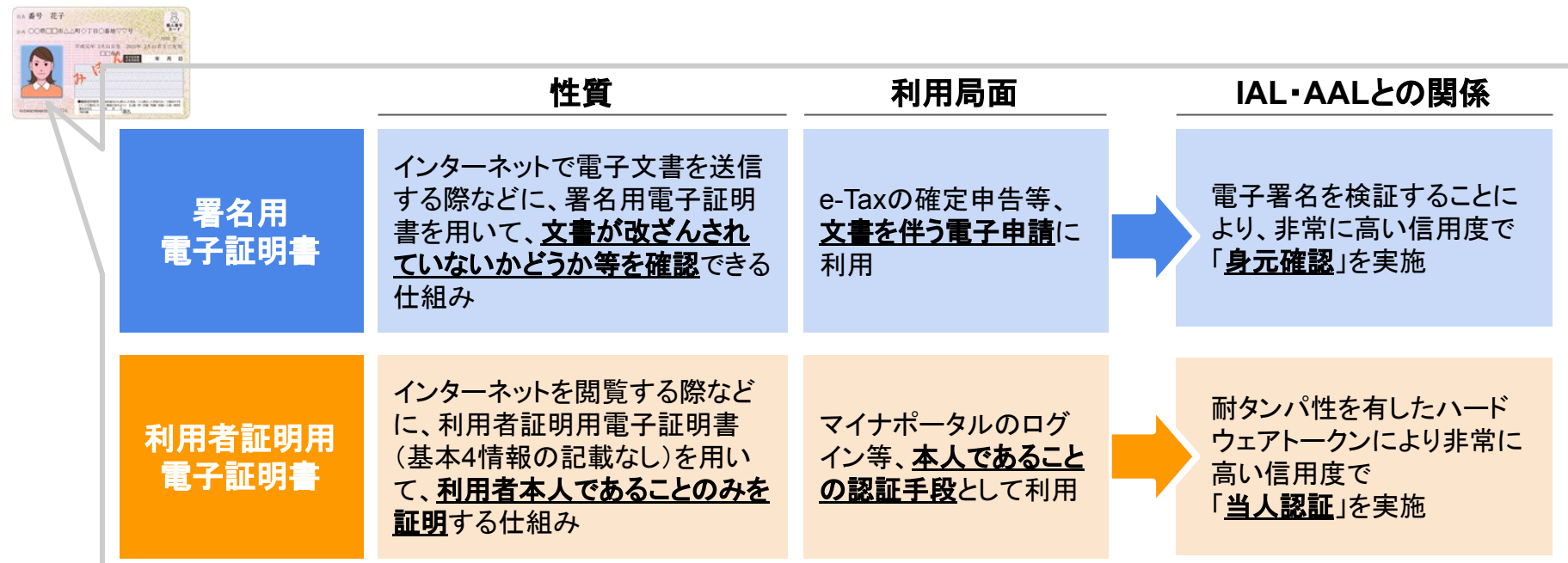
注釈:ここでのレベル分けはあくまでイメージであり、本ボードの共通認識として合意を得たものではない

出所:各府省情報化統括責任者(CIO)連絡会議決定(2019)「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」、

Digital.GOV.TZ "Identification Management Standards"等より作成

マイナンバーカードに格納される公的個人認証は、最も安全性が高い本人確認手法であり、カードの普及とともに利用局面の拡大が期待されます。

公的個人認証の概要



出所：総務省「公的個人認証サービスによる電子証明書」(https://www.soumu.go.jp/kojinbango_card/kojinninshou-01.html),
(2021年11月12日取得),

各府省情報化統括責任者(CIO)連絡会議決定(2019)「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」より作成

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

アドバイザリーボードでは、eKYCサービス事業者として留意すべき点として、「透明性」と「説明責任」についての論点が示されました。

これまでのアドバイザリーボードにおける主な指摘事項等①



- (ISMS等の)認証は取得した方が望ましい。
 - 情報銀行の認定対象事業者でも、Pマークは必須という事例がある。
 - (PマークとISMS)両方とらなければいけないということではないが、事業の性格上、ISMS認証は取得したほうが良い。
- 社内のPDCAサイクルが回ることが保証できている等、形式だけではなく中身が伴っていることが重要。



透明性



- ユーザーの立場に立つと、プライバシーポリシーがシンプルで分かりやすいことは良い。
- プライバシーポリシーの中身を改善することも重要だが、同時に個人データを預けている人と企業との信頼関係の構築が重要である。そのためには、プライバシーポリシー(ルール)の改訂と同時に、ユーザーとのコミュニケーション戦略が必要ではないか。
- 積極的なコミュニケーション戦略により、企業とユーザー間の信頼感が醸成される。



説明
責任

委託業務における情報の取扱いについて、活発な議論が行われたほか、「取得データの最新性」、「データ取得の最小化」が課題とされました。

これまでのアドバイザリーボードにおける主な指摘事項等②

“

- 受託業務として取得している個人情報を受託の範囲内で扱うのは当然であり、委託元の指示に従って情報を取扱う必要がある。
- 第三者提供についてユーザーからの同意を得たとしても、使用目的が委託契約の範囲外であると、委託契約違反になる可能性があり、第三者提供を行ってはいけない。
- 利用目的に適合するためにも、委託契約に基づき取得した情報と、直接取得した情報は別々に管理する必要がある。

目的の
限定

“

- 取得した情報のうち、途中で変わりうる情報(住所や名字等)の取扱いが課題
- 仮にデジタル身分証で住所を更新した際、他の連携しているデータも自動的に更新されとなればユーザビリティが高い

正確性

“

- 基本4情報のうち「性別」は、「性別そのものが機微情報」という点と「本人確認にとって必須ではない」という2つの方向性から取得が不要という議論に結びつき得る
- オンラインでの当人認証時には性別情報は取得しないが、対面での本人確認時には性別も本人確認の手がかりになり、問題が発生し得るという難しさがある

最小化

当社としては、まずは①説明責任への積極対応、②社会情勢変化の情報収集・対応の 2点について、重点的に取組みたいと考えています。

今後TRUSTDOCKが取組む必要がある主要論点整理

対応済みの論点

(デジタル身分証を除く)

取得情報の整理

利用目的等
の明確化

データ保存期間
の明確化

保存期間を過ぎた
データの削除

個人情報の
第三者提供

データの
安全管理措置

開示等請求
への対応

プライバシーポリシーの
改訂によりさらなる明確
化に取り組む

個人情報の取得時だけ
でなく、取得後の透明性
・アカウントビリティも積
極的に推進

社会の変化を見据え、
eKYCを取り巻く新たな
課題にも積極的に取組
む



検討が必要 な主要論点

対応方針

認証取得

- プライバシーマークを取得済
- ISMS認証の取得手続中
- 個人情報保護やセキュリティマネジメントのPDCAサイクルを繰り返し、実効性を確保

コミュニケー
ション戦略

- 個人情報の取扱いについて、ユーザーに対してわかりやすく整理・発信

取得する
個人情報の
最小化

- 利用するサービスに必要な最小限の情報のみ提供できる環境を整備
- ユーザーニーズの多様化にも配慮し、基本4情報の新しい取扱いを提案

保存情報の
更新

- データ連携等を活用し、最新の情報が更新されるプロダクト等を検討

(参考)GDPRの基本原則

原則	概要
適法性、公正性、 透明性	本人(データ主体)によって、適法かつ公正であり、どのような処理がなされているかわかる
目的の限定	明確に限定された正当な目的のために収集され、処理はその範囲内に限定される
データの最小化	利用目的に対して、関連性があり、必要十分な範囲に限定される
正確性	正確性と、必要な場合の最新性が維持される
記録保存の制限	目的のために必要な期間だけ、本人の識別が許容される
完全性および機密性	外部的及び内部的な驚異から、技術面および組織面で適切に保護され、適切な安全性が確保される
アカウントビリティ	管理者は、上記を遵守する責任を負い、遵守することの説明責任を負う

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

03-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

03-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

消費者調査の結果から、ユーザーは個人情報の取扱いについて不安を抱えており、eKYC業者として適切な情報発信の必要性が示唆されました。

信頼されるeKYCサービス事業者になるための視点【再掲】

ユーザーが感じている不安

- データの保管や活用が不安・心配
- 顔写真を送りたくない
- 提供先の事業者が信用できない
- 情報漏洩のニュースなどを見て怖い
- 法整備やガイドラインが整っていない



信頼されるeKYCサービス事業者となるための視点

個人情報の 取扱い

- 個人情報の取扱いの **明確化・透明化**
- 特にユーザーが不安を感じている **顔写真データ**の取扱いの留意

事業者の 信頼性

- **認証取得**等による信頼性の確保
- 信頼を維持する **不断の努力**

ルールの 存在

- **法やガイドライン整備への積極関与**
- ユーザーの安全性を第一にしつつ、実社会で利用されるルール形成

Meta社がFacebookの顔認識システムを停止する等、近年、生体情報の取扱いに対する不安の高まりに対して、規制の動きが拡大しています。

顔認識技術に係る事例

Facebookにおける 顔認識用テンプレートの削除

- Metaは、Facebookにおける顔認識システムを数週間のうちに停止し、これまでに集めた10億人以上のユーザーの顔認識用テンプレートを削除すると発表。
- 停止の理由として、顔認識技術に対する懸念と規制の不透明性を挙げている。
- 顔スキャンデータを識別可能なデータに変換する顔認証技術をめぐっては、プライバシーや人権に関する懸念も高まっていた
- そのほか、この種の技術の問題点として、有色人種を対象とした場合の認識率が低いことも指摘

その他近年の主な動向

- 米IBM、アマゾン、マイクロソフト
 - 2020年、警察への顔認識技術の提供を停止
- EU
 - 2021年4月、公共の場で顔認証システムを使った警察捜査を原則禁止する規制案を公表

AIを使った顔認識技術規制の動きが拡大

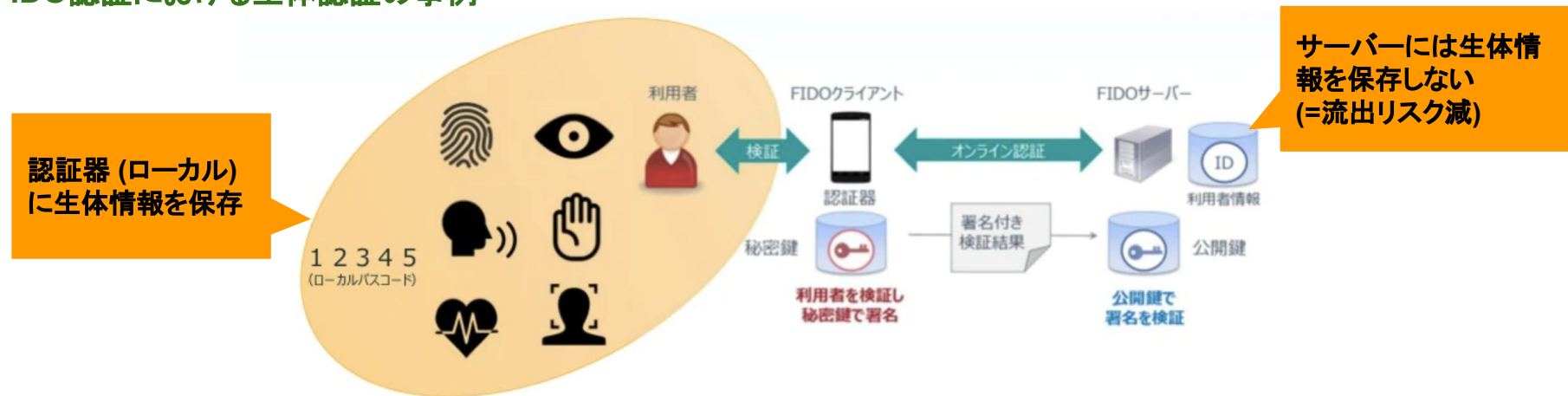
出所: Meta “An Update On Our Use of Face Recognition” (<https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>), (2021年11月9日取得)

CNET Japan「Facebook、顔認識システムを停止へ-ユーザー10億人分の画像を削除(2021年11月4日付)」(<https://japan.cnet.com/article/35178945/>), (2021年11月9日取得)

朝日新聞「フェイスブック、投稿の顔認識を停止へ10億人分の顔データは削除(2021年11月3日付)」(<https://digital.asahi.com/articles/ASPC351F2PC3UHBI013.html>) (2021年11月12日取得)

FIDO認証モデルでは、生体情報の保存を認証器 (=ローカル)で完結しており、生体情報が流出するリスクを減らしています。

FIDO認証における生体認証の事例



- 生体認証の欠点は、サーバから情報が流出したときに顔や指紋を変えることができない こと
- FIDOという認証技術では、端末(認証器)での検証とサーバでの認証を分けている
- 生体情報を認証器内に留めておくことで、生体情報がサーバから流出しないようにしている

出所:FIDOアライアンス(2020)「パスワードのいらない世界へ FIDOアライアンスとFIDO認証の最新状況」

(<https://www.slideshare.net/FIDOAlliance/2020-0218-fidofido>), セキュリティマネジメントカンファレンス2020 冬 大阪. (2021年11月11日取得)

認証・認可プロトコルである CIBA を利用する場合も生体認証は端末内に閉じた実装が可能となっておりサーバーからの生体情報流出を防いでいます。

CIBA のサポートによる決済・送金フローの事例



- OpenID Connectで本人情報を提供する場合に、認証・認可・同意のために生体認証を求める場合がある
- 生体認証がついたデバイス(消費デバイス)がデータを提供するデバイス(消費デバイス)と分かれている場合が多く、消費デバイスと認証デバイスを分けるCIBAという仕様が作られている
- CIBA利用の場合も、生体認証は端末内に閉じた実装が可能になっている

出所: AUTHLETE (2019)「認可サービスAUTHLETE、オープンAPIの適用シーンを広げる新仕様CIBA」に対応~ スマートフォンを活用したオンライン・オフライン融合型決済・本人確認・送金プロセスのスピーディーな構築が可能に~ (<https://prtimes.jp/a/?f=d24448-20190213-6653.pdf>), (2021年11月11日取得)

TRUSTDOCK eKYCサービスとしては、これまでも適正に個人情報を取り扱っており、プライバシーポリシーで情報の取扱い等について公表しています。

TRUSTDOCKのプライバシーポリシー

TRUSTDOCKのプライバシーポリシーの構成

個人情報保護方針

個人情報の取り扱いについて

1. 個人情報の利用目的
 - 1.1. ご本人から直接書面により取得する場合の利用目的
 - 1.2. ご本人から直接書面以外により取得する場合の利用目的
2. 個人情報の開示等請求について
 - 2.1. 受付手続
 - 2.2. 手数料
3. 個人情報保護方針、開示等、苦情・相談の受付窓口
 - 3.1. お問い合わせ先
 - 3.2. 認定個人情報保護団体について

TRUSTDOCK社の認識

必要事項は網羅済
み

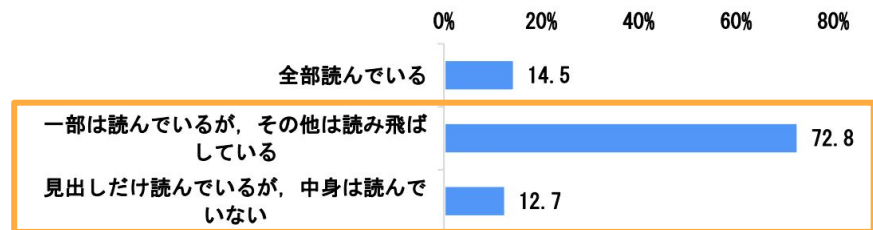
より分かりやすい
記載・表現が必要

文書以外での
情報伝達方法も検討

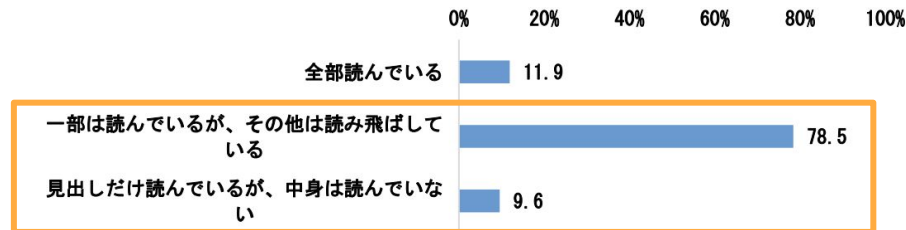
一方で、プライバシーポリシーを読むユーザーは少ないと想定され、ユーザーに個人情報の取扱いについて正しく理解いただく不断努力が必要と考えています。

利用規約等に対する消費者の認知・理解・同意

検索サービスの利用規約を
どの程度読んでいるか(回答数: 448)

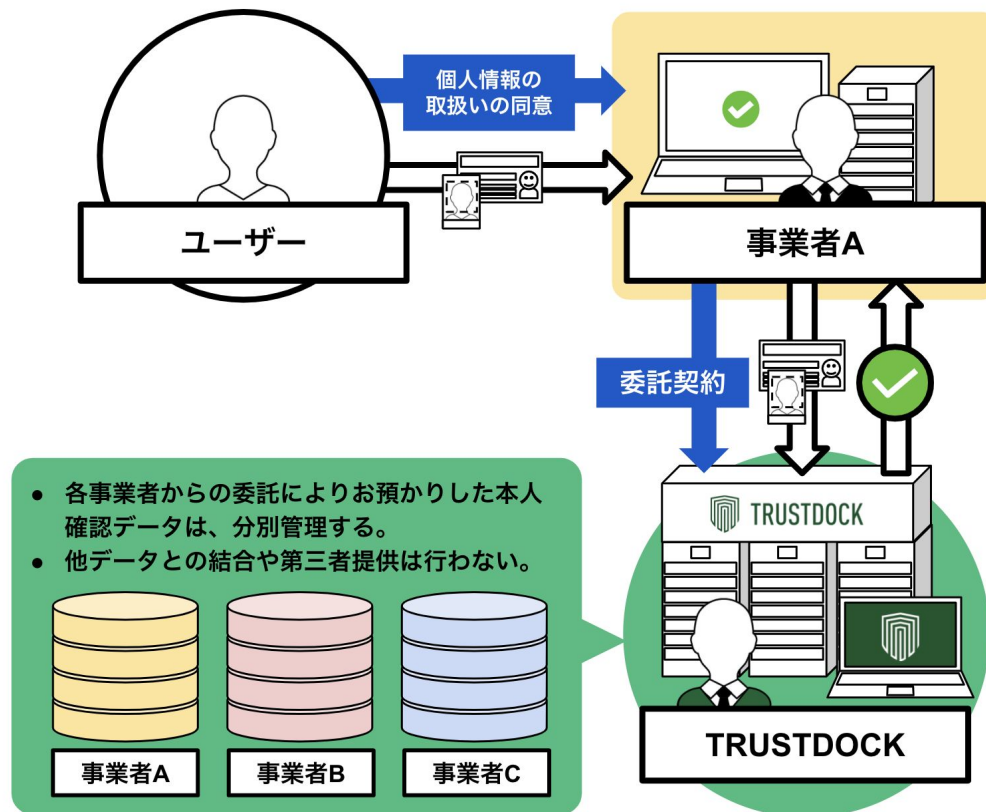


SNS 等の利用規約を
どの程度読んでいるか(回答数: 929)



同意を取得していたとしても、そもそもプライバシーポリシー等が読まれていない可能性

TRUSTDOCK eKYCサービスは委託契約で、利用企業様からユーザーの個人情報の提供を受け、本人確認業務後にも情報を適切に保持・廃棄しております。



GDPR

個人情報を取扱う際の説明責任が基本原則
正当化根拠が示されていない個人情報の取扱いは違法

- ①本人の同意 ②契約等の履行のための必要性 ③法的義務
④生命に関する利益 ⑤公共の利益・公的権限の遂行 ⑥適法な利益

のいずれかの適法化根拠が必要



✗ 本人の同意をとればよい

(第三者提供についての説明が十分でないケースなどが生じている)

同意は、
十分な説明を受けた本人が、自由な意思に基づいて、明確に示したもの
でなければならない。

TRUSTDOCKは、プライバシーマークを取得し、現在は ISMS認証の取得準備を進めており、eKYCサービス事業者としての信頼性確保に努めています。

TRUSTDOCKの認証取得状況

ロゴ

プライバシー
マーク



認証の概要

- 「JIS Q 15001個人情報保護マネジメントシステム—要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して、事業活動に関してプライバシーマークの使用を認める制度

TRUSTDOCKの取得状況

- 2018年取得済み
- 2020年更新済み

ISMS認証



- 国際的に整合性のとれた情報セキュリティマネジメントシステムに対する第三者適合性評価制度
- わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的とする

- 通常のISMS(JIS Q 27001)認証に加えて、クラウドサービス固有の管理策(ISO/IEC 27017)の取得手続き中
- 2022年初の取得を目指している

TRUSTDOCKは、大切な個人情報を取り扱う事業者として、「ユーザー視点を欠かさないこと」「透明性を確保すること」に一番の力点を置き、こだわり続けます。

TRUSTDOCKのアカウントビリティへのこだわり

規定等の整備

必要な事項を網羅しつつ、明確かつ分かりやすい記載・表現を追求

文書以外のチャネルでの伝達を検討

同意取得を目的化せず、ユーザーが自らの情報や同意をコントロールできる環境整備

事業者としての 信頼性確保

認証の取得

PDCAサイクルや改善事項について積極的に公表



「不透明な情報の取扱いは行わない」
これが安心や信頼を得る唯一の方策です
そのための環境整備も重要なミッションと位置づけ
TRUSTDOCKはeKYCやデジタルアイデンティティの未来を拓くために
今後も山を登っていきます

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

総務省の調査では、パーソナルデータの提供に対する不安はアジア地域で高く、特に日本では「とても不安に感じる」割合が高いことが示されました。

パーソナルデータの提供全体に対する不安感



出所: 総務省「平成29年版情報通信白書」(<https://www.soumu.go.jp/johotsusintokei/whitepaper/h29.html>)より
(原資料) 総務省「安心・安全なデータ流通・利活用に関する調査研究」(平成29年)

デジタル庁が開発するコロナワクチン接種証明書アプリでも、個人情報に関する意見が複数あり、情報提示レベルを選択できる仕様になりました。

情報の最小化に関する事例 — コロナワクチンの接種証明書(電子交付)の仕様

主な意見 (個人情報に関するもの抜粋)

(カジュアルなユースケースに関しては)生年月日や氏名を知られたくないなど、利用者が表示する情報をコントロールできるようにすべき

セキュリティ上「プライバシー情報を含まず、接種したことのみを証明するコード」と「プライバシー情報を含むコード」の2つに分け、ユーザーが任意に選択できるようにすべき

接種済みかどうかだけの表示を基本としてもらいたい

二次元コードにどんな情報が含まれているか不明



デジタル庁の対応方針

利用者が自分で情報提示レベルを選択できるように、アプリの画面上、以下3つのレベルに分けて情報を表示できるように変更

1. 接種済みであることのみを確認できるレベル
2. 二次元コードのみを確認できるレベル
3. 二次元コード+(コードに含まれる)情報が表示できるレベル

出所: デジタル庁ウェブページ「「コロナワクチンの接種証明書(電子交付)の仕様に関するご意見」の取りまとめ結果を公表しました」

(<https://www.digital.go.jp/posts/LbGO0j4g>)より作成

また、近年では、EU一般データ保護規則 (GDPR)を皮切りに「データの最小化」が世界的な潮流になりつつあります。

世界の個人情報保護法令の事例

GDPR (EU)



- adequate, relevant and **limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation')

適切で、関連性があり、処理される目的に関連して**必要なものに限定される**こと(「データの最小化」)

California Consumer Privacy Act (CA州)



- be **reasonably necessary and proportionate** to achieve the purposes for which the personal information was collected or processed...

個人情報収集または処理された目的を達成するために、**合理的に必要なかつ妥当**であり...

注釈: 各条文の日本語約は仮訳

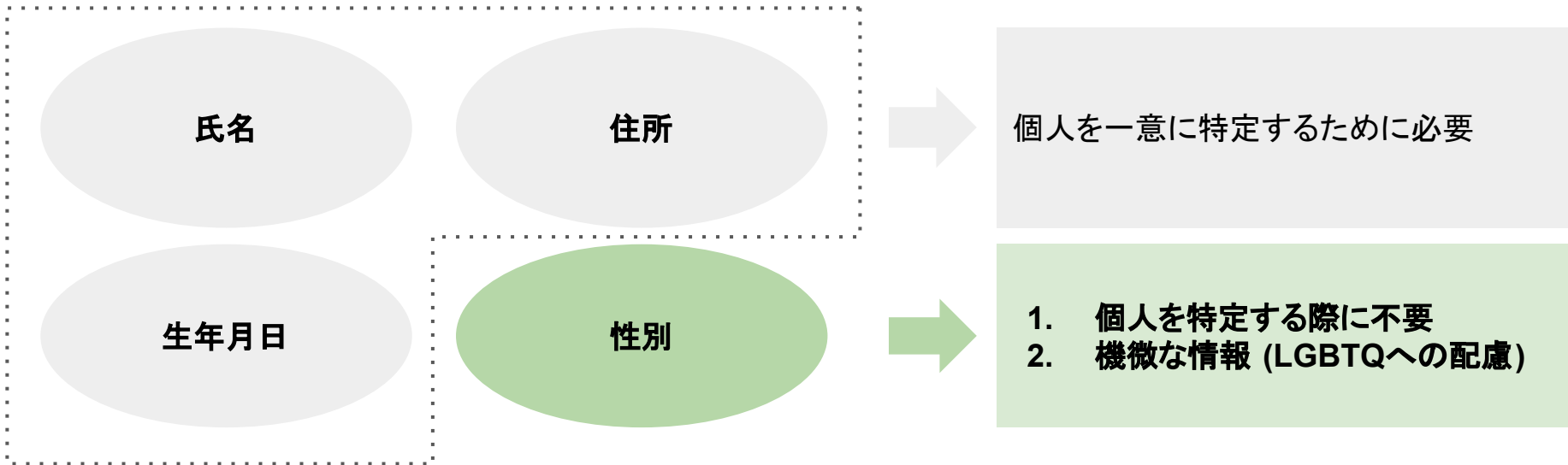
出所: intersoft consulting “General Data Protection Regulation”(<https://gdpr-info.eu/>), (2021年11月9日取得)

Ballotpedia “California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)”

([https://ballotpedia.org/California_Proposition_24_Consumer_Personal_Information_Law_and_Agency_Initiative_\(2020\)](https://ballotpedia.org/California_Proposition_24_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020))), (2021年11月9日取得)

ところで、個人情報の基本4情報として位置づけられている「性別」は、本人確認には必ずしも必要ではなく、機微な情報という側面もあります。

基本4情報と本人確認



脚注:LGBTQとは、LGBTQとは、Lesbian(レズビアン、女性同性愛者)、Gay(ゲイ、男性同性愛者)、Bisexual(バイセクシュアル、両性愛者)、Transgender(トランスジェンダー、性自認が出生時に割り当てられた性別とは異なる人)QueerやQuestioning(クエアやクエスチョニング)の頭文字をとった言葉で、性的マイノリティ(性的少数者)を表す総称のひとつ。

出所:東京レインボープライド2021ウェブページ(<https://tokyorainbowpride.com/>)より(2021年11月8日取得)

例えば、犯罪収益移転防止法や古物営業法等における本人確認では、「性別」の確認は求められていません。

犯罪収益移転防止法・古物営業法の条文(抜粋)

犯罪収益移転防止法

(取引時確認等)

第四条 特定事業者は、顧客等との間で、別表の上欄に掲げる特定事業者の区分に応じそれぞれ同表の中欄に定める業務のうち同表の下欄に定める取引を行うに際しては、主務省令で定める方法により、当該顧客等について、次の各号に掲げる事項の確認を行わなければならない。

- 一 本人特定事項(自然人にあつては 氏名、住居(本邦内に住居を有しない外国人で政令で定めるものにあつては、主務省令で定める事項)及び 生年月日をいい、法人にあつては名称及び本店又は主たる事務所の所在地をいう。以下同じ。)

古物営業法

(確認等及び申告)

第十五条 古物商は、古物を買受け、若しくは交換し、又は売却若しくは交換の委託を受けようとするときは、相手方の真偽を確認するため、次の各号のいずれかに掲げる措置をとらなければならない。

- 一 相手方の 住所、氏名、職業及び年齢を確認すること。
- 二 相手方からその 住所、氏名、職業及び年齢が記載された文書(その者の署名のあるものに限る。)の交付を受けること。
- 三 相手方からその 住所、氏名、職業及び年齢の電磁的方法による記録であつて、これらの情報についてその者による電子署名が行われているものの提供を受けること。
- 四 前三号に掲げるもののほか、これらに準ずる措置として国家公安委員会規則で定めるもの

※その他携帯電話不正利用防止法においても、氏名、住居及び生年月日のみの確認が求められている

そこで、取得情報の最小化の視点から「性別」に着目し、行政手続きにおいて性別が求められているケースや、性別情報の取得見直しの事例について、簡易調査を実施しました。

簡易調査の概要

	法令条文調査	事例調査
目的	手続きや申請に「性別」を求めている条文数や内容等の実態を整理する	国、自治体のそれぞれにおいて、行政手続き等で「性別」の取扱いを見直している事例を整理する
方法	e-Gov法令検索において「性別」で全文検索を行い、目視で内容を確認する	インターネットによるデスクトップリサーチ

データの最小化の視点から、法令における「性別」取扱いの現状や動向を概観する

183の法令で、記載事項や申請等で「性別」が求められています。個々の条文では「性別」を求めるもの・求めないものが混在していました。

本文に「性別」の記載がある法令等

条文により、性別を求めるものと求めないものが混在している
(=情報最小化の可能性が示唆)

分類(カッコ内の数値は法令数)	法令名の例	条文の抜粋例
条文に「性別」を含む法令等 (260)	法律 (16)	精神保健及び精神障害者福祉に関する法律 第二十二条2 前項の申請をするには、次の事項を記載した申請書を最寄りの保健所長を経て都道府県知事に提出しなければならない。 一 申請者の住所、氏名及び生年月日 二 本人の現在場所、居住地、氏名、 性別 及び生年月日 申請者:不要、本人:要
	政令 (22)	保健師助産師看護師法施行令 第二条 保健師籍、助産師籍又は看護師籍には、次に掲げる事項を登録する。 二 本籍地都道府県名(日本の国籍を有しない者については、その国籍)、氏名及び生年月日 三 保健師籍又は看護師籍にあつては、 性別 助産師:不要、保健師・看護師:要
	省令 (145)	出入国管理及び難民認定法施行規則 第五十二条2 一 船舶にあつては次に掲げる事項 ロ 乗員の氏名、国籍・地域、生年月日、乗員手帳又は旅券の番号及び職名 ハ 乗客の氏名、国籍・地域、生年月日、旅券の番号、出発地及び最終目的地 二 航空機にあつては次に掲げる事項 ロ 乗員の氏名、国籍・地域、生年月日、 性別 及び乗員手帳又は旅券の番号 ハ 乗客の氏名、国籍・地域、生年月日、 性別 、旅券の番号、出発地及び最終目的地 船舶:不要、航空機:要
	その他 (77)	日本国憲法 第十四条 すべて国民は、法の下に平等であつて、人種、信条、 性別 、社会的身分又は門地により、政治的、経済的又は社会的関係において、差別されない。

出所:e-Gov法令検索(2021年10月19日時点)

厚生労働省は、2021年4月に新たな履歴書の様式例を作成し、性別欄を任意記載欄にするとともに、未記載とすることも可能としました。

履歴書様式例見直しの概要

見直しの背景

- 厚生労働省では、公正な採用選考を確保する観点から、JIS規格の履歴書様式例の使用を推奨。
- 見直しの大きな契機として、2020年7月に、LGBT当事者を支援する団体から、厚生労働省、日本規格協会等に対して履歴書様式の検討(性別欄の削除等)を求める要請。
- 当該要請も契機に、JIS規格の履歴書の様式例全体が削除。
- このため、公正な採用選考を進める上で参考となる様式を厚労省において定めることとした。

見直しの内容

- 性別欄を「男・女」の選択ではなく任意記載欄に変更。なお、未記載とすることも可能。
- 「配偶者」「扶養家族数」「配偶者の扶養義務」「通勤時間」の各欄を様式内に設けない(削除)。

様式例の位置付け

- 公正な採用選考を確保するため、履歴書の様式例を示すもの。
- 法的拘束力はない。そのため、当該様式の使用は個別の企業が判断可能。
 - 公正採用選考の周知・啓発は法律に基づくものではなく、企業の理解を得て行っているもの。
 - 別の様式の応募用紙を使用する際には、就職差別につながる項目を含めないよう留意が必要。
- 様式例の作成後は活用状況等を把握し、適宜活用状況について公表。

(参考)履歴書の様式例

○厚生労働省が作成した履歴書様式例（厚生労働省様式例）

[illegible]

出所：厚生労働省労働政策審議会安定分科会2021年4月16日）資料、厚生労働省ウェブページより

LGBT法連合会は、性的指向や性自認等による差別や偏見による困難を整理した「困難リスト」を公表。本人確認時の困難事例も存在しています。

本人確認分野におけるLGBTの困難事例(抜粋)

“

公的な書類も不用意に記載された性別欄と外見の性別が異なるため、本人確認ができないという理由で必要な行政サービスや民間サービスが受けられなかった。

“

性別を削除した住民票の写しを市町村役場で希望したが、法令上、そうした扱いは自治体の権限ではできず、戸籍上と外見で性別が違うことが暴露された。

“

マイナンバー(個人番号)カードの表面に性別が記載されているため、本人確認等に支障をきたしたり、外見との違いから差別を受ける不安がある。

“

役所窓口、試験会場、警察、郵便物受取などで本人確認が必要な場合に、身分証明書の性別(戸籍性)と見た目の性別が一致しないことからトラブルがおきた。

複数の自治体において、性別欄の削除が実行済み又は検討されています。

本人確認分野におけるLGBTの困難事例(抜粋)

福井県 越前市	2021	「性別欄記載あり」の239件中、 71件が独自に削除可能 と整理(2020年4月1日現在)
長野県 松本市	2020	計195、 性別記載欄削除可能40(20.5%) 、検討 38(19.5%)、不可能117(60.0%)
静岡県 伊東市	2020	111件のうち 53件の申請書等の性別欄の削除 し、 11件の申請書等の性別欄については自由記載
愛知県 蒲郡市	2021	申請書等327件のうち、 252件を廃止 。法令等に押印及び性別記載が義務付けられているものについては、 国の動向を確認しながら随時見直し
滋賀県	2017	県以外の機関が様式を定めているものを除き、性別欄のある申請書等は255。その内の 76.9%にあたる 196の申請書等は性別欄を廃止、または、自由記述方式にする等、記載方法について工夫
大阪府 富田林市	2020	市の行政文書総数2,202。性別記載欄があった文書の数446。 うち性別記載欄を削除・修正した文書の数(予定含む)142
熊本県	2018	性別記載欄のある様式の総数は534件。 そのうち204件(38%)について、順次見直し
宮崎県 宮崎市	2018	577文書中 175文書から性別欄を削除 (2019年7月1日現在)

出所:各自治体ウェブサイトより

宮崎市では、性別欄のある申請書・通知書のうち市で対応可能なものについて削除等を検討し、削除できない場合には対応方針等を整理しています

宮崎県宮崎市の取組事例

性別欄のある申請書・通知書等の総数 565

①宮崎市が性別欄を削除できる余地があるか。

- ・法律・政令等や県の条例等で様式が定められていない。
- ・国や県等への報告に性別記載の必要がない。等

NO

対象外

302/565
(53.5%)

YES

263/565
(46.5%)

②業務上、性別情報が必要な理由があるか。

- ・統計上、収集する必要がある。
- ・男女共同参画の観点から収集する必要がある。
- ・医療上、性別の情報を収集する必要がある。
- ・施策の実施に当たり、性別を把握する必要がある。等

YES

性別欄が必要な場合でも、自由記入式にしたり、「戸籍上の性別をご記入ください」や「自認している性別をご記入ください」と記述するなど、配慮を検討する。

NO

198/263
(75.3%)65/263
(24.7%)

③要綱等に基づいており、各所属のみの判断で削除できるものであるか。

- ・条例や規則等の改正の必要がない。
- ・様式が電算システム化されておらず算化の必要がない。等

NO

①規則改正が必要 (22/48)
文化・市民活動課で取りまとめた規則改正を行う。

②システム改修が必要 (17/48)
法改正などの他理由によるシステム改修時に、合わせて実施する。

③関連機関との協議が必要 (7/48)
定期的な会合等において協議し削除する。

※削除済み 印鑑登録関連(7/48)
※規則改正が必要かつシステム改修が必要 (5/48)

YES

150/198
(75.8%)48/198
(24.2%)

性別欄削除

フローチャートで性別欄の削除の可否を検討している

対応場面や望まれる対応方針等を整理した事例集を作成

場面（２） 性別欄や性別表示に関する事例

戸籍上の性別と自身の思う性別が異なる性的少数者の中には、「性別欄にどちらの性別を書けばいいのかわからない」「通知書等に自認している性別と違う性別が記載されており違和感がある」など、生きづらさを感じる方もいます。

②-1 申請書受理の際、担当者欄に性別欄（男・女）が設けられており、本人より「」の部分に○をしてよいかと申し出があった。

アンケート記入者の対応

申し出に対し、全く問題ない旨を伝え、他の申請書と同様の手続きを行った。

②-2 医療検査・問診、当事者の相談業務等での性別欄（男・女）記入の際、どちらにも付けられないとの申し出があった。

アンケート記入者の対応

業務上必要であることを説明し、戸籍上の性別を口頭で確認した。多数職員が関わる場合は、個々に紙面の性別と間違いないことを申し送りし、本人に何度も性別を確認しないように配慮した。

望まれる対応

- ・本市では、平成30年8月に「宮崎市における性別欄削除の基本方針」を定め、申請書・通知書等の不必要な性別欄の削除に取り組んでいます。まずは、基本方針に沿って性別欄を削除できないか確認しましょう。
- （事例②-1の性別欄については、再度削除する方向で検討してみよう。）
- ・下記のような業務上必要な性別欄であっても、「男・女」の選択式から、自由記述式にするなど配慮を検討しましょう。

【性別欄が必要な例】

- 統計上、収集する必要がある。
- 医療上、性別の情報を収集する必要がある。
- 施策の実施に当たり、性別を把握する必要がある。 など

全ての対応に共通するポイント

複数の職員で対応する場合や担当者が変わる場合に、当事者の性的指向や性自認等について、関係職員への周知や申し送りを行う際には、職員間の情報共有は必要最小限としましょう。

なお、地方公務員には守秘義務が課されています。当事者の性的指向や性自認等は職務上知り得た個人情報として、他に漏らしてはなりません。

出所：宮崎市「宮崎市における性別欄削除の基本方針」「性的少数者に配慮した様々な行政場面での対応事例集」より

今回の「性別」の取扱いに関する調査はあくまで簡易調査のため、より正確な理解のためには、条文の精査や海外事例の調査等も必要です。

本簡易調査の到達点と今後の課題

本簡易調査の到達点

法令 条文 調査	- 性別の記載がある<u>条文数を明確化</u>し、特に<u>省令レベルでの規定が多い</u>実態が明らかになった - 条文ごとに性別の申告等の要否が異なっており、<u>必要な手続き等に絞って性別情報を取得している可能性</u>が示唆
事例 調査	- 国においても、LGBTQへの配慮等の観点から性別欄の見直し<u>事例が存在</u> - 多くの自治体で性別欄の<u>見直しが実行</u> - 押印の見直しと合わせて性別欄の見直しも行われている可能性も示唆



今後の課題

国	<u>法令の趣旨に照らして、申告等での性別の要否を検討</u>する必要があると思料
自治体	<u>性別欄を削除できない場合の対応方針</u>の策定が必要と思料 (※宮崎市の事例が参考になると思料)
TRUST DOCK	<u>海外における性別の取扱い等の先進事例</u>の収集・分析 - 各ビジネスの特性に応じた<u>性別情報の要否の精査</u>

TRUSTDOCKは、国際的な視点でニーズや社会の変化をいち早く捉え、先進的な eKYCサービスにより、社会インフラづくりを牽引していきます。

社会



世界的な情勢・ニーズ

国内外の法令等

企業活動を通じて
社会にフィードバック

社会動向を
自社活動に反映

TRUSTDOCK



先進的なeKYCサービス

プライバシーポリシー等の
社内規定

主要論点



- ユーザーニーズの多様化に即した 新たな本人確認スキームを提案する
- 既存の手法の保証レベルを再構成し、ユーザーの利便性の高い新たな手法を構築する
- データ連携等により、ユーザーに過度の負担をかけずに情報が更新される仕組みを提案する

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

2022年のアドバイザリーボードでは、新たに、デジタル身分証についての議論をスタートします。

2022年のアドバイザリーボードにおける主な活動 (案)



- デジタル身分証
- サービスに応じた本人確認のあり方検討
等を中心テーマに議論を深め、2022年夏頃を目途に取りまとめる予定



- 官公庁や大学等と連携したイベントの開催
- アドバイザリーボードでの議論内容について解説する、事業者向けウェビナーの開催
等を企画し、広く社会にも情報発信を行う予定



- 社会情勢を的確に捉えつつ、「個人情報・生体情報等の取扱い」や「データ利活用と個人情報のあり方」等についても、引き続き議論を展開

01 アドバイザリーボードの設置

02 これまでの議論の概要

02-01 ユーザー意識調査の結果概要

02-02 オンライン本人確認における保証レベルについて

02-03 eKYCサービス事業者における個人情報の取扱いに係る論点整理

03 eKYCサービス事業者としての個人情報の取扱い等に係る当社の方針

02-01 個人情報の取得時・取得後それぞれの透明性及び説明責任

02-02 社会の変化を見据え、eKYCを取り巻く新たな課題にも積極的に取組む

04 今後のアドバイザリーボードにおける展望

05 参考資料 株式会社TRUSTDOCKのご紹介

社名	株式会社TRUSTDOCK (英文表記: TRUSTDOCK Inc.) 
本店所在地	〒102-0093 東京都千代田区平河町 2-5-3 Nagatacho GRID
東京オフィス	〒141-0032 東京都品川区大崎 3-5-2 エステージ大崎ビル 6F
設立年月日	2017年11月1日(カーブアウト: 2018年4月1日)
代表者	代表取締役: 千葉 孝浩
役員	取締役: 肥後 彰秀 取締役: 菊池 梓
事業	デジタルアイデンティティ(KYC/本人確認) 事業
連絡先	inquiry@trustdock.io
URL	https://biz.trustdock.io/
認証	Pマーク : 17003414(01)号
主要提携先	アディッシュ株式会社 / アディッシュプラス株式会社 / 株式会社ネクスウェイ / ソースネクスト株式会社
主要株主	経営陣 / GLOBIS CAPITAL PARTNERS / STRIVE / 500 Startups Japan / Innovation Growth Ventures / Sony Innovation Fund / ガイアックス / 三菱UFJキャピタル / みずほキャピタル / SMBCベンチャーキャピタル    

経済産業省の育成支援プログラム「 [J-Startup](#) 」選定企業


所属団体

[FISC 金融情報システムセンター](#)
[Fintech協会](#) (理事)

[日本ブロックチェーン協会](#) (アドバイザー)

[OpenIDファウンデーション・ジャパン](#) (KYCワーキンググループ)

[FIDOアライアンス](#) (Identity Verification & Binding Working Group)

[NPO日本ネットワークセキュリティ協会](#)
[シェアリングエコノミー協会](#)

沿革

2016年春:

(株)ガイアックスのR&D事業部にて、ブロックチェーン技術を用いたデジタルIDの研究開発を開始。ブロックチェーンによるDプロダクトの実用性を検証。

2017年夏:

フィンテック市場の拡大にあわせAPI経由で本人確認を行うプロダクト「TRUSTDOCK eKYCサービス事業者」を提供開始。その後KYC/本人確認に関連する様々なAPIを開発。APIネットワーク構築のため、各社とのAPI連携の提携を開始。

2018年春:

世界中で課題になっているデジタルアイデンティティ問題に取り組み、広くデジタル上の個人認証基盤になるべく、(株)ガイアックスより独立。

外部からの資金調達も実施しKYC/本人確認の専門機関として始動。



本資料は、TRUSTDOCKが信頼できると判断した情報をもとにTRUSTDOCKが細心の注意を払って作成・表示したのですがTRUSTDOCKは本資料の内容および当該情報の正確性、完全性、的確性、信頼性等についていかなる保証をするものではありません。本資料の内容につきましては、利用者の判断に基づきご利用をお願いします。本資料の利用によって何らかの損害（直接損害・間接損害とを問いません）が発生した場合でもTRUSTDOCKは一切の責任を負いません。

本資料に記載された内容は、本資料作成時点におけるものであり、予告なく変更される場合があります。ただしTRUSTDOCKは本資料を更新する義務を負うものではありません。

本資料の内容に関する一切の権利は、当社又は当社にライセンスを行った権利者に帰属するものです。本資料のいかなる部分についてもTRUSTDOCKから事前に同意を得ることなく、複製、翻訳、変造等を行い、あるいは転載、送信、放送、配布等により第三者に伝達することを禁じます。

TRUSTDOCKは、本資料が電子的に配布された場合に、利用者がコンピュータウイルスなど有害なプログラム等による損害を受けないことについて保証をするものではありません。また、TRUSTDOCKは、本資料が電子的に配布されることで生じる本資料の内容の誤り、欠落等に対する一切の責任を負いません。

お問い合わせ

<https://biz.trustdock.io/contact/>



受付時間：24h