資料２

基本的な議論の視点

（参考）

「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」

（平成22年８月31日 各府省情報化統括責任者（ＣＩＯ）連絡会議決定）

■ 各保証レベルに求められる具体的な対応基準を、4つの評価軸ごとに規定。
■ 対策基準の適用の考え方（※1※2）など、基準実現のための配慮事項についても規定。

＜主な対策基準＞

保証レベル	登録	発行・管理	トークン	認証プロセス	署名等プロセス
レベル4	**（窓口）** •写真付き身分証明1種の提示 •申請情報の台帳照合 •重複登録ではないことの確認	• 手渡し、本人限定受取郵便、によるトークン発行	• レベル3の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること	• レベル3と同等の基準	• 電子政府推奨暗号リストに記載の署名方式 • 電子署名用の証明書の用途は電子署名限定
レベル3	**（窓口）** •写真付き身分証明1種（or他2種）の提示 •申請情報の台帳（又は公的証明書）照合 **（郵送 or オンライン）** •申請書に対する電子署名 •申請情報の台帳（又は公的証明書）照合	• レベル4の方法に加え、書留郵便、書留郵便＋ダウンロード、電子署名＋ダウンロード、によるトークン発行	• レベル2の基準に加え、複数の認証要素を利用すること	• レベル2と同等の基準に加え、フィッシングの脅威に対する耐性	• 電子政府推奨暗号リストに記載の署名方式
レベル2	**（窓口）** •写真付き身分証明1種（or他2種）の提示 **（郵送 or オンライン）** •申請情報に他機関の登録情報（クレジットカード番号等）を含めて申告	• レベル3の方法に加え、分割配付（一方を郵送）、メール通知後のダウンロード、によるトークン発行	• 認証情報の推測確率が16384分の1未満であること	• レベル1と同等の基準に加え、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性	
レベル1	**（窓口 or 郵送 or オンライン）** •身元確認は不要 •メールアドレスの到達確認	• レベル2の発行方法に加え、電子メールによる送付、ダウンロード、によるトークン発行	• 認証情報の推測確率が1024分の1未満であること	• オンライン上の推測、リプレイ攻撃の脅威に対する耐性	

※1　上位基準の採用：認証方式の強度とコスト及び利便性は一般的にトレードオフの関係にあり、コストや利便性等の多様な観点による総合的な判断が必要となる。
※2　代替基準の採用：ガイドラインの対策基準は絶対的なものではなく、同等の代替基準であれば他の対応策による代替が許容される。

本人認証の基本的な分類

			認証技術
基本認証	知識	本人しか知らない情報（知識情報）を持っていることを利用。本人のみが知っていてかつ記憶できる情報と、本人のみが知っている情報ではあるが記憶できない情報があり、記憶できない情報は、本人の所持物（ICカード、PCなど）に格納して管理	・**ワンタイムパスワード**（アクセス毎に生成する使い捨てのパスワードを利用） ・**チャレンジレスポンス**（アクセス毎に異なる方式でパスワードを暗号化して行う認証）**など**
			・**公開鍵による認証** ・**対称鍵**（特定の者同士が復号して得られる鍵）**による認証** ・**3交信プロトコル**（関数・計算規則を確認する３度の交信で、本人しか知り得ない情報を知っていることを確認して行う認証）**など**
			属性認証の原理、仕組みなど
	所持	本人しか持ち得ない情報（所持情報）が焼き付けられた物理的媒体（内蔵する情報の書換えが不可能な物理的媒体）を認証	**クレジットカード、銀行カードなど**
	上記以外	本人の体や器官が持つ固有情報（生体情報）の個人差を利用	**指紋、網膜、虹彩、手の平・指静脈、顔型、DNAの各認証技術**
応用認証	複合認証	基本機能の欠点を補いセキュリティを強化するため、基本機能を組み合わせることを利用	**二要素認証、三要素認証**
	匿名認証	本人であることを知られずに認証することを利用	・**グループ署名**（署名者個人は分からないがあるグループに所属することを証明） ・**ブラインド署名**（署名者と署名されたデータの内容を第三者の署名により暗号化）**など**
	統合認証	一度認証すれば、ほかのサイトの認証にも利用できることを利用	・**リバティ・アライアンス**（他者サービス向けＩＤを相互に認証するための枠組み） ・**OPEN-ID**（個人が自身のＨＰ上で管理し、サービス事業者に公開して用いるＩＤ）**など**

※「ネット社会と本人認証　－原理から応用まで－」（平成22年、板倉征男・外川政夫共著、電子情報通信学会編）をもとに編集

認証技術毎の主たる特徴

方式	具体例	主たる特徴	
		利点	留意点
記憶 （知識）	暗証番号、パスワード、質問応答　等	・利用・変更が容易 ・広く普及している　等	・忘却の可能性 ・推測による攻撃が可能 ・虚偽メールによる詐取、資料盗取や会話盗聴による不正入手　等
所持物	ICカード、身分証明書、磁気カード、USB、携帯電話、パスポート　等	・暗号技術が併用可能 ・操作が容易である ・偽造対策技術が存在　等	・暗号方式の強度に依存 ・紛失・盗難の可能性 ・スキミングへの警戒 ・製造・設置コストが必要　等
上記以外	筆跡、音声、顔、 指紋、虹彩、静脈、 行動パターン　　等	・忘却・盗難がない ・偽造困難なものが多い　等	・無効化が困難 ・偽造の可能性 ・心理的抵抗感　等

※「バイオメトリクス・セキュリティ評価に関する研究会　平成18年度　研究会中間報告書」（独立行政法人　情報処理推進機構セキュリティセンター）をもとに編集

電子署名の推定効について①

紙文書と印鑑（民事訴訟法の推定効（私文書の場合））

第1段目の推定
（最判昭39.5.12民集18-4-597）

第2段目の推定
（民事訴訟法第228条4項）

本人の印章による印影 → 本人又はその代理人の署名又は押印 → 真正な成立

本人の印章の印影と私文書の印影とが一致していること

印鑑登録証明書による「本人の印章の印影」の立証

電子文書（電子署名法の推定効）

・カード所持（正しい証明書を持っていることの証明）
・PIN入力（本人しか知り得ない情報を知っていることの証明）

推定
（電子署名法第3条）

本人の公開鍵による認証 → 本人による電子署名 → 真正な成立

本人の公開鍵で電子署名を復号し、電子文書のハッシュ値と一致していること（公開鍵暗号方式の場合）

電子証明書による本人の公開鍵の立証

電子署名の推定効について②

判例（最判昭和39.5.12民集18-4-597）

【判決要旨】

民事訴訟法第326条（現第228条第4項）に「本人又ハ其ノ代理人ノ署名又ハ捺印アルトキ」というのは、該署名または捺印が、本人またはその代理人の意思に基づいて、真正に成立したときの謂であるが、文書中の印影が本人または代理人の印章によって顕出された事実が確定された場合には、反証がない限り、当該印影は本人または代理人の意思に基づいて成立したものと推定するのが相当であり、右推定がなされる結果、当該文書は、民事訴訟法第326条にいう「本人又ハ其ノ代理人ノ署名又ハ捺印アルトキ」の要件を充たし、その全体が真正に成立したものと推定されることとなるのである。

民事訴訟法（平成8年法律第109号）

（文書の成立）

第228条 （略）

2・3 （略）

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

5 （略）

電子署名及び認証業務に関する法律（平成12年法律第102号）

第3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。

認証の用途と対応する認証手段の関係性（イメージ）

○　各種手続における認証（本人確認）では、その用途に応じて必要とされる情報やその精度が異なる。対応可能な最適な認証手段を採用することが必要ではないか。
○　上位の認証手段を用いる場合、必要とされる情報は入手できるが、利用者側の利便性を損なう（情報の精度と利用者利便性のトレードオフの関係になる）のではないか。

	＜行政サービス＞	＜民間サービス＞	現行対応可能な認証手段	
類型① 誰でも利用可能な手続 ⇒特段の情報不要	・公共交通サービス	・民間交通サービス ・飲食の提供　等	対面 非対面	・特に必要なし
類型② 条件を満たせば幅広い者に利用させる手続 ⇒資格や属性の情報が必要	・市民マラソン ・図書館利用 ・学割・シニア割 ・宿泊施設利用提供	・会員制サービス利用 ・酒・煙草・ギャンブル ・航空券販売　等	対面 非対面	・会員証等提示 （会員証、学生証、社員証（所属等）orマイナンバーカード（年齢、住所地）） ・利用者証明用電子証明書 ・ＩＤ／パスワード
類型③ サービス内容・場所が個人によって異なる手続 ⇒正確な本人情報が必要	・各種証明書請求 ・給付金申請 ・ライフライン契約	・会員制サービス登録 等	対面 非対面	・申請等書面+身分証提示・添付（マイナンバーカードor住民票の写し等） ・署名用電子証明書（４情報）（２回目以降：利用者証明用電子証明書）
類型④ 財産権等重要な権利義務を確定させる手続 ⇒・正確な本人情報 ・権利義務の確定に向けた本人意思の確認 が必要	・確定申告 ・不動産移転登記 ・法人設立登記	・携帯電話契約 ・不動産売買契約 ・住宅ローン契約　等	対面 非対面	・申請等書面+実印+印鑑証明書 ・署名用電子証明書（４情報＋真正性の推定効）

＜各手続の信用の基点となる認証手段を形成する手続＞

住民 ― 対面確認 ＝信用の基点（トラストアンカー） ― 確認者

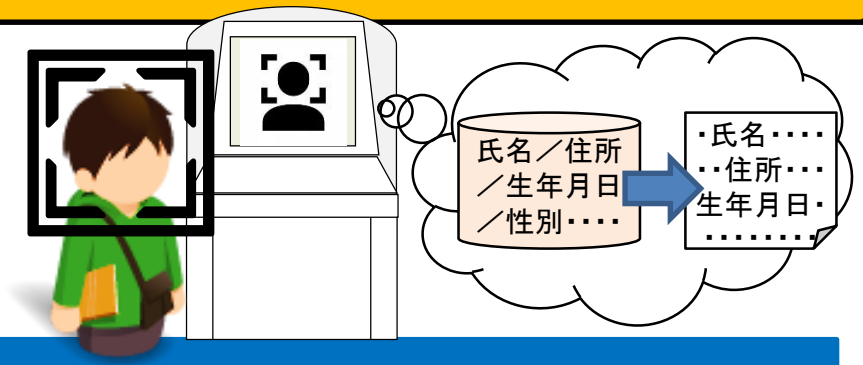
対面での厳格な本人確認
・マイナンバーカードの交付
・電子証明書の発行

個人認証とＡＩの活用による行政のイノベーション（イメージ）

受付
（手続内容の確認）

本人確認／申請事項記入

申請・届出完了
／書類交付

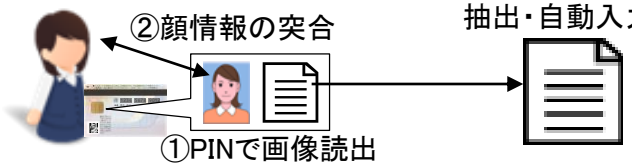


AIとの対話
（文字・音声）

本人情報の自動入力

AIとの対話
（文字・音声）

パターン1

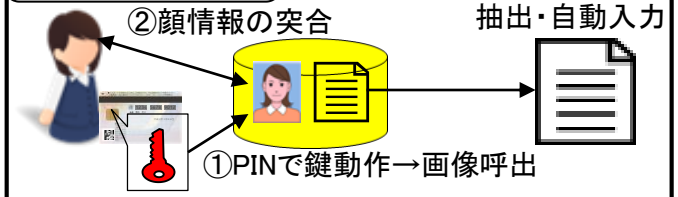


媒体：あり、認証：顔＋知識

＜認証を求める本人意思＝ PIN入力＞

①カード等内の画像を読み取り
②手続者の顔との突合・確認
③②の認証が成立すれば、カード内の記録事項などを活用して本人情報データを自動入力

パターン2

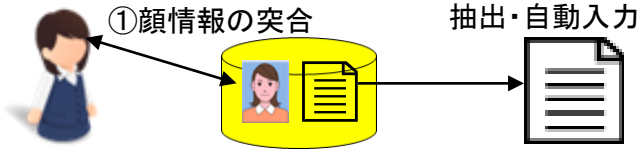


媒体：あり、認証：顔＋知識

＜認証を求める本人意思＝ PIN入力＞

①カード等内の鍵を用いてバックヤードの顔情報にアクセス
②手続者の顔との突合・確認
③②認証が成立すれば、バックヤードに登録されている本人情報データを自動入力

パターン3



媒体：なし、認証：顔

＜認証を求める本人意思⇒代替必要？＞

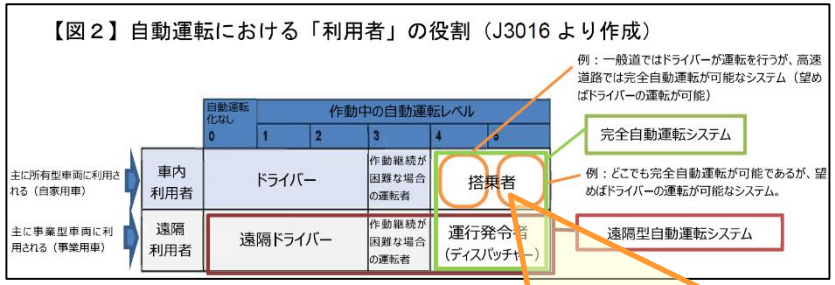
（例：AIの口頭確認ボタン押下）
①手続者自身の顔情報とバックヤードの顔情報と突合・確認
②①の認証が成立すれば、バックヤードに登録されている本人情報データを自動入力

今後の議論に向けて②：自動走行車の操作権利／操作資格の確認（イメージ）

自動運転技術等の検討

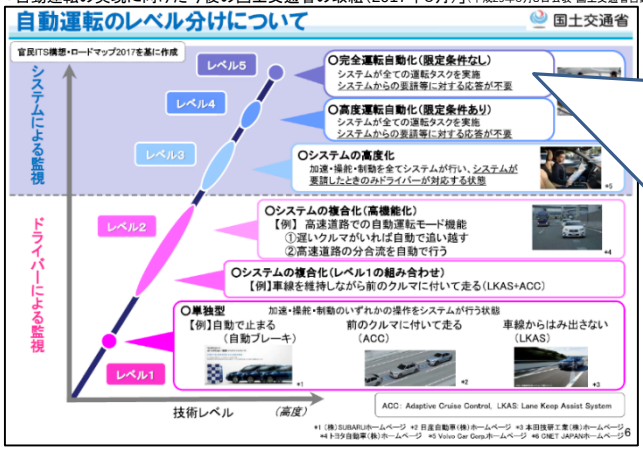
＜出典＞
「官民ITS構想・ロードマップ2017
～多様な高度自動運転システムの社会実装に向けて～」
（平成29年5月30日高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定）

【図２】自動運転における「利用者」の役割（J3016 より作成）



レベル4・5では「ドライバー」は「搭乗者」へと性格が変異

＜出典＞
「自動運転の実現に向けた今後の国土交通省の取組（2017年6月）」（平成29年6月8日公表 国土交通省自動運転戦略本部）



レベル5	・システムがすべての運転タスクを実施（限定領域内ではない） ・作動継続が困難な場合、利用者が応答することは期待されない
レベル4	・システムがすべての運転タスクを実施（限定領域内※） ・作動継続が困難な場合、利用者が応答することは期待されない

※限定領域
当該運転自動化システムが機能すべく設計されている特有の条件。
（運転モード、地理、道路、環境、交通状況、速度、高（低）速道路等

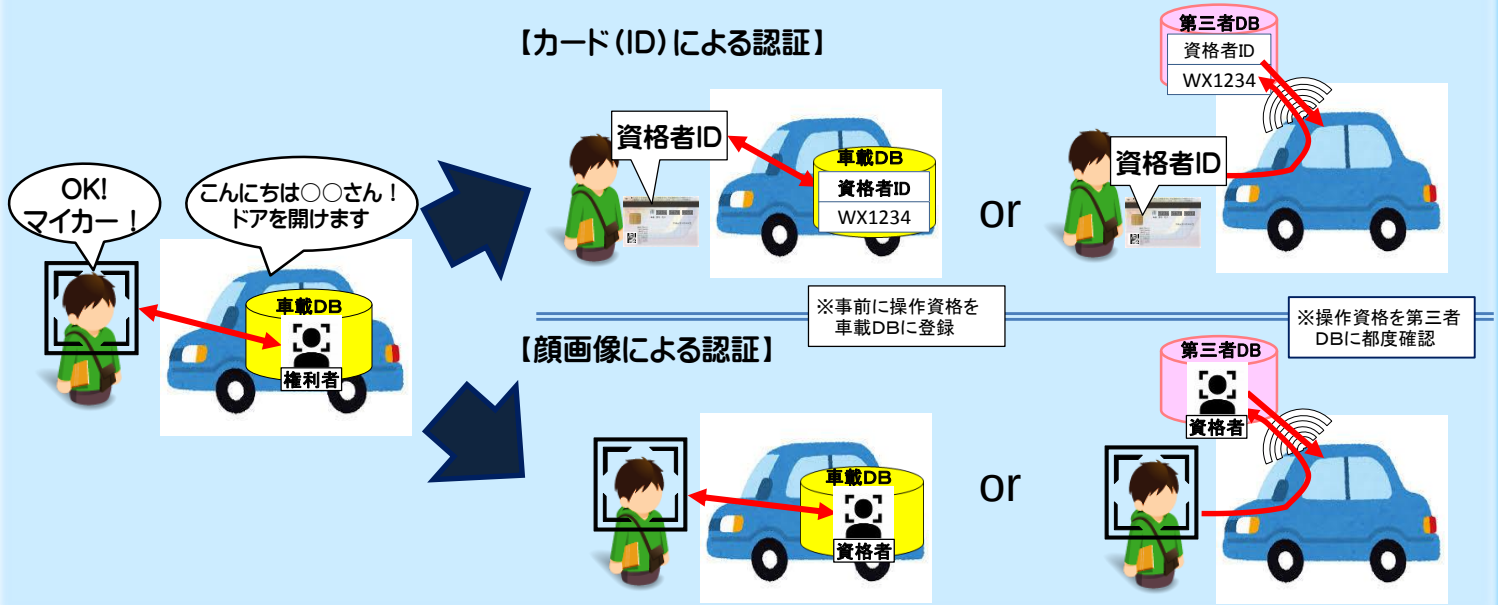
操作権利／操作資格の確認

・操作権利＝個別の自動走行車を操作する権利（例：所有権等）
・操作資格＝自動走行車を操作する技能があることについての第三者機関による証明

＜ステージⅠ 操作権利及び操作資格の双方の確認が必要な場合（レベル4まで）＞

⇒ 限定領域外では一定の操作を求められるため、操作『資格』の確認も必要

①操作権利の確認 → ②操作資格の確認



＜ステージⅡ：操作権利の確認のみ必要な場合（レベル5）＞

⇒ 限定領域がない（操作機会がない）ため、操作『権利』のみ