法制審議会民法（遺言関係）部会
ご説明資料

2024年7月30日
MUFG相続研究所
三菱UFJ信託銀行株式会社　フロンティア事業開発部

日本電気株式会社

目次

1.遺言制度の現状とデジタル技術の整理

1-1. はじめに

本資料作成にあたっての基本的な考え方

（1） 現行の自筆証書遺言と同程度の信頼性が確保される遺言を簡便に作成

（2） 高齢者等を中心として、全文等の自書によって遺言を作成することに相当の負担感

（3） 世代を問わず遺言しようとする者が利用しやすいものとすべき要請（利便性・簡便性の要請）と、遺言制度において求められる真意性・真正性等の担保とのバランス

※以上は、民法（遺言関係）部会資料1より抜粋

（4） 現行の自筆証書遺言の要件のうち「全文等の自書」を外し、秘密証書遺言同様にワープロでの作成を可能とした場合に想定される「真意性・真正性の担保」の観点からの課題について、どのようなデジタル技術の活用が考えられるか

（5） デジタル技術の活用に際しては、現行の自筆証書遺言と比較して、遺言しようとする者にとって、極力、過重な負担（証人の立会い、公的機関での手続き等を要する等）がない方法を想定

Q1 Q2 Q3 Q4

1-2-1. 現行制度との比較 （1）現行制度

- **第三者（遺言書保管官、公証人等）の介在により真意性や真正性等の担保を補完**
- **保管制度により、改ざん・紛失・隠匿を防止（検認不要）**

【表1−1】 現行制度（真意性等、利用者負担、事後検証等）

現行制度	真意性	真正性	熟慮性	利用者負担				保管場所の設置	遺言書のみを用いて本人が作成したかを検証すること
				作成場所の限定	外出（出頭）の必要	第三者の介在	事後に文字化する必要		
自筆証書遺言	全文自書（財産目録を除く）で担保			無	無	無	無	無	可
自筆証書遺言書保管制度利用	上記に加え 本人が法務局に出向き遺言書保管官に提出、保管時に本人確認、形式チェックを行う			無	有	有	無	有	可
秘密証書遺言	本人より遺言書の入った封紙を公証人に提出 公証人、証人により担保			無／有	有	有	無	無	遺言書の作成方法による

【表1−2】 現行制度（改ざん等リスク、利用者負担、無効等リスク、保管コスト）

現行制度	改ざん・紛失・隠匿リスク	利用者負担				無効・執行手続不可リスク		公的機関の保管コスト
		作成場所の限定	自書	検認手続の必要	費用	無効（要件不備）	執行手続不可	
自筆証書遺言	有	無	有	有	無	有	有	無
自筆証書遺言書保管制度利用	無	無	有	無	有	無	有	有
秘密証書遺言	有	無／有	無（自筆も可）	有	有	有	有	無

MUFG

Q1 Q2 Q3 Q4

1-2-2. 現行制度との比較 （2）－1（デジタル技術単体、複合①）

【表2】デジタル技術単体（ 真意性等、利用者負担、事後検証等）

	真意性	真正性	熟慮性	利用者負担				保管場所の設置	遺言書のみを用いて本人が作成したかを検証すること
				作成場所の限定	外出（出頭）の必要	第三者の介在	事後に文字化する必要		
デジタルタッチペン（指等による入力を除く。以下同じ。）	全文を自らペンで入力する（財産目録を除く）ことで担保			無	無	無	無	無	可
ワープロ活用	全て検証不可			無	無	無	無	無	不可
録音・録画	音声・映像（電磁的記録）により確認（ディープフェイクリスク有）			無	無	無	有	無	可

【表3－1】複合①（単体技術＋電子署名（マイナンバー）＋生体認証(顔貌)）（ 真意性等、利用者負担、事後検証等）

	真意性	真正性	熟慮性	利用者負担				保管場所の設置	遺言書のみを用いて本人が作成したかを検証すること
				作成場所の限定	外出（出頭）の必要	第三者の介在	事後に文字化する必要		
デジタルタッチペン	全文を自らペンで入力すること（財産目録を除く）に加え電子署名等で補完する			無	無	無	無	無	可
ワープロ活用	検証不可	検証可	検証不可	無	無	無	無	無	一部につき可
録音・録画	音声・映像（電磁的記録）による確認に加え電子署名等で補完する			無	無	無	有	無	可

MUFG

Q1 Q2 Q3 Q4

1-2-3. 現行制度との比較 （2）－2（複合①、②）

【表3−2】複合①（改ざん等リスク、利用者負担、無効等リスク）

	改ざん・紛失・隠匿リスク	利用者負担			無効・執行手続不可リスク	
		作成場所の限定	自書	検認手続の必要	無効（要件不備）	執行手続不可
デジタルタッチペン	有	無	有	有	有	有
ワープロ活用	有	無	無	有	有	有
録音・録画	有	無	無	有	有	有

【表4】複合②（複合①＋公的機関等が保管※）

※（前提）保管時の要件不備チェックなし、相続発生時の相続人等への通知あり

	改ざん・紛失・隠匿リスク	利用者負担			無効・執行手続不可リスク	
		作成場所の限定	自書	検認手続の必要	無効（要件不備）	執行手続不可
デジタルタッチペン	無	無	有	無とし得る	有	有
ワープロ活用	無	無	無	無とし得る	有	有
録音・録画	無	無	無	無とし得る	有	有

MUFG

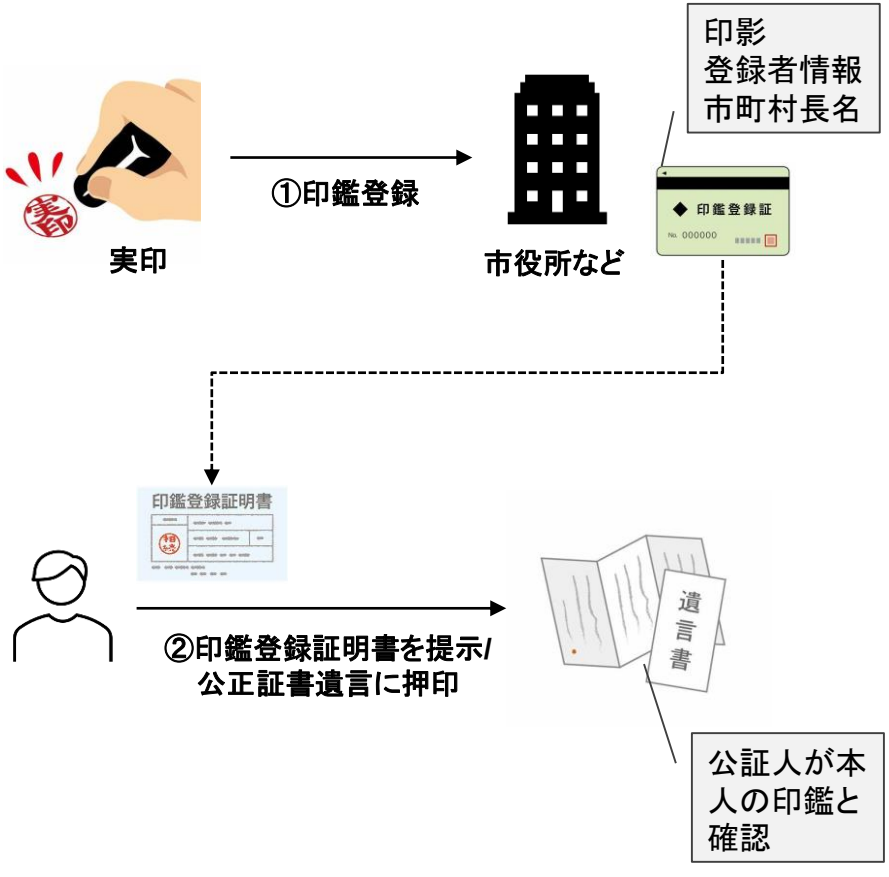
2.デジタル技術のご説明

Q1 Q2 Q3 Q4

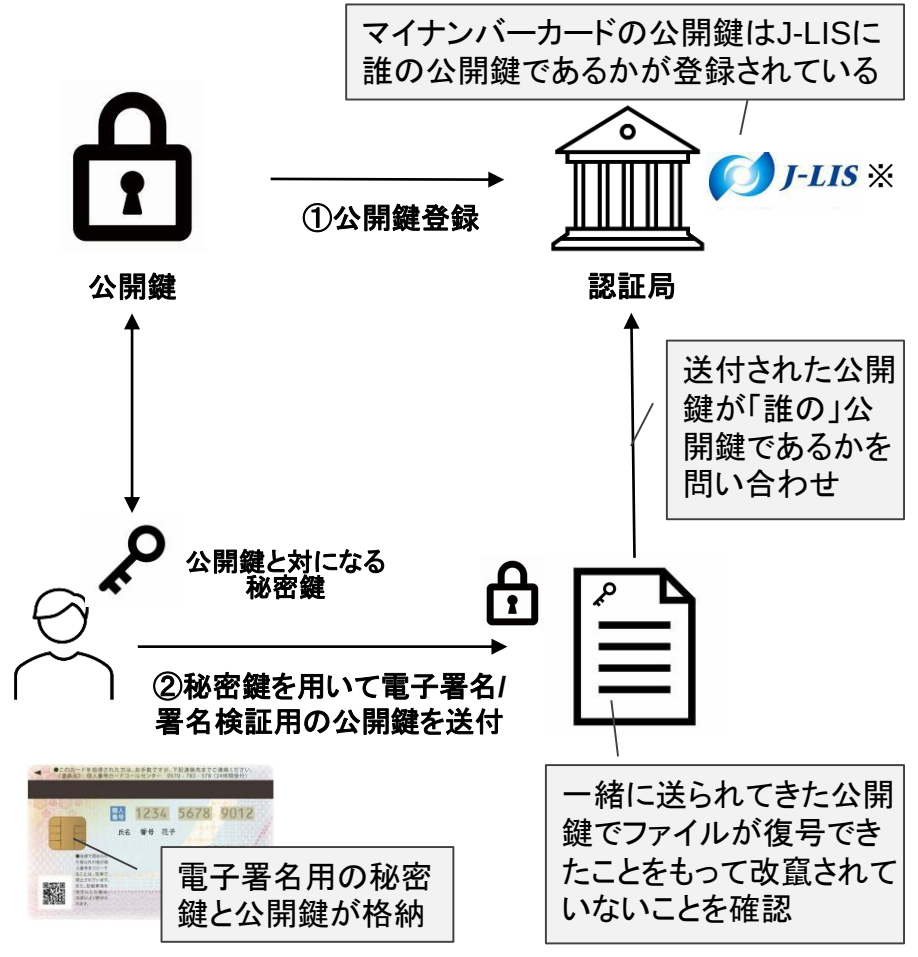
2-1-1. 電子署名について

- **電子署名とは、紙に押印する代わりに、コンピュータやスマートフォンを使って行うデジタルなサイン**
- **電子署名は、サインした人が本当にその人であることを確認し、書類が改ざんされていないことを保証している**

捺印の世界



電子署名の世界



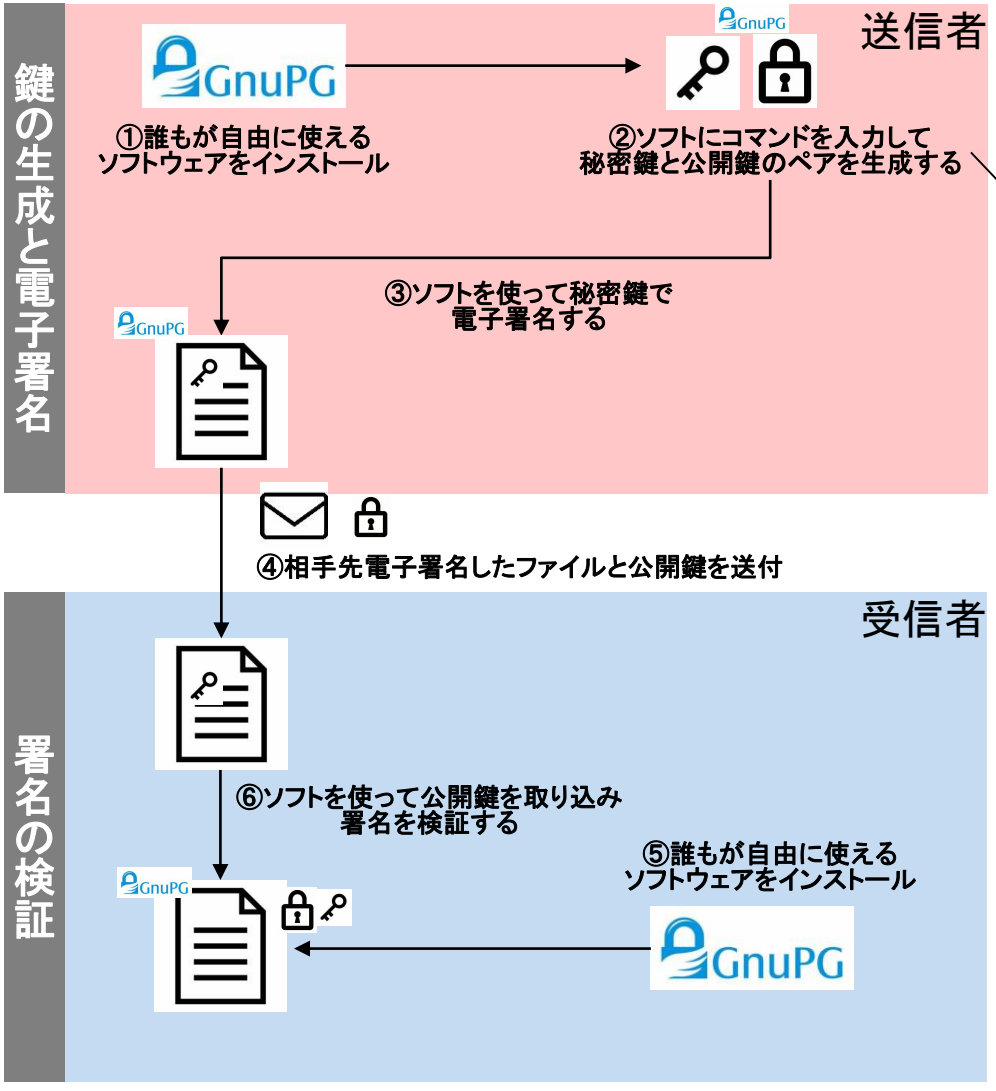
※地方公共団体情報システム機構、公的個人認証法に基づく公的個人認証サービス（JPKI）を提供

MUFG

Q1 Q2 Q3 Q4

2-1-2. 電子署名について | 使い方① すべて手動で対応

- 電子署名には鍵の準備、署名および検証プロセスの実施が必要となるが、専用のシステムを構築せず手動でこれらを行おうとすると一定のリテラシーが求められる
- また署名する秘密鍵の所有者についての身元確認が行われないため、第3者から見て署名者が本人かはわからない



鍵の生成の画面イメージ

```
[ec2-user@ip-172-31-33-30 ~]$ gpg --gen-key
gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

ご希望の鍵の種類を選択してください:
   (1) RSA と RSA (デフォルト)
   (2) DSA と Elgamal
   (3) DSA (署名のみ)
   (4) RSA (署名のみ)
あなたの選択は? 1
RSA 鍵は 1024 から 4096 ビットの長さで可能です。
鍵長は? (2048) 4096
要求された鍵長は4096ビット
鍵の有効期限を指定してください。
         0 = 鍵は無期限
      <n>  = 鍵は n 日間で期限切れ
      <n>w = 鍵は n 週間で期限切れ
      <n>m = 鍵は n か月間で期限切れ
      <n>y = 鍵は n 年間で期限切れ
鍵の有効期間は? (0)2y
鍵は2022年05月29日 03時48分32秒 UTCで期限切れとなります
これで正しいですか? (y/N) y

GnuPGはあなたの鍵を識別するためにユーザIDを構成する必要があります。

本名: r_saiki
電子メール・アドレス: r_saiki@example.com
コメント:
次のユーザIDを選択しました:
    "r_saiki <r_saiki@example.com>"

名前(N)、コメント(C)、電子メール(E)の変更、またはOK(O)か終了(Q)? o
秘密鍵を保護するためにパスフレーズがいります。
```

一部抜粋

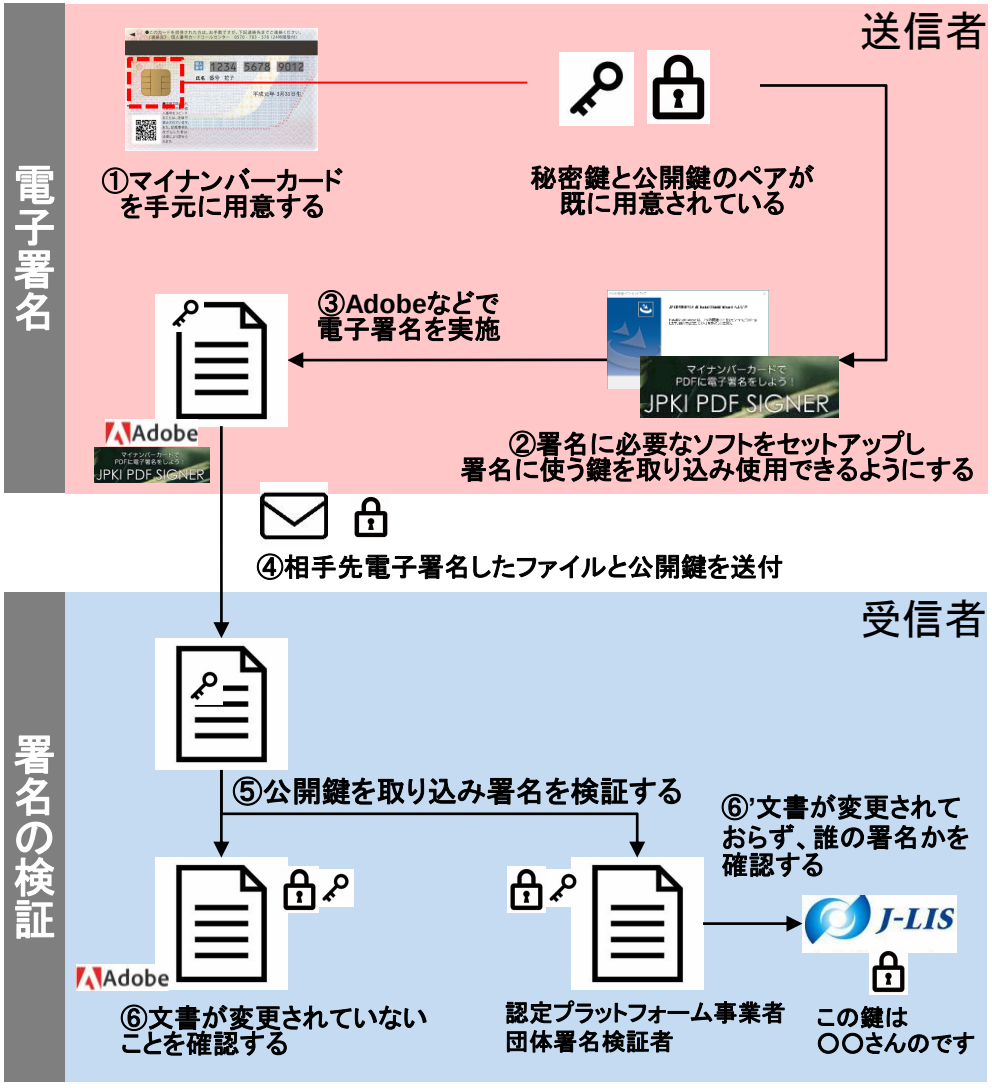
https://qiita.com/r_saiki/items/fb0bbbaa861e93f65ce9

MUFG

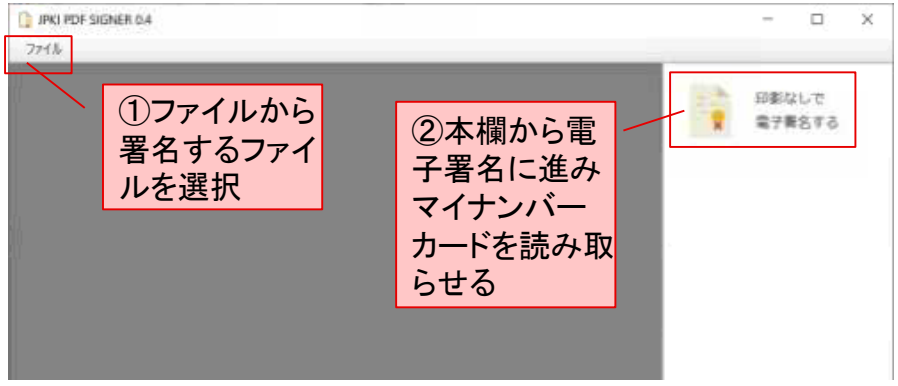
Q1 Q2 Q3 Q4

2-1-3. 電子署名について | 使い方② マイナンバーカードの活用

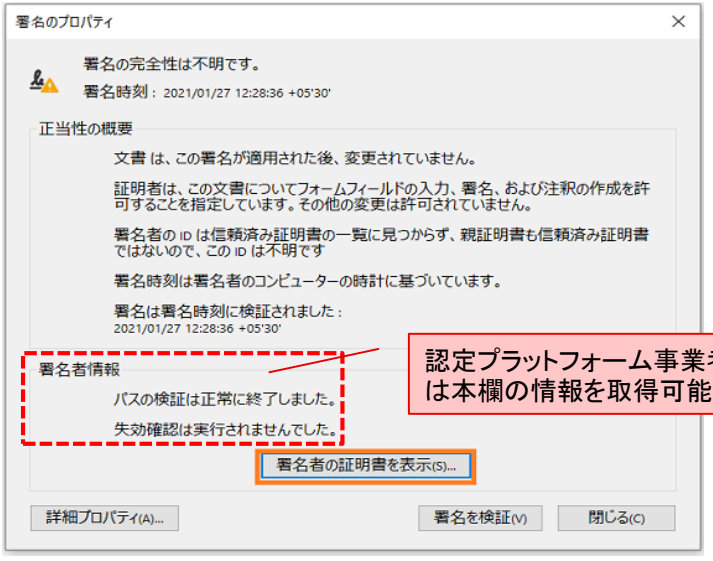
- マイナンバーカードのICチップの中には、電子署名用の秘密鍵と公開鍵が格納されており、これを活用することで、鍵の生成をする必要がなくなる
- また署名する秘密鍵の所有者についての身元の確認がなされているため、第3者から見て署名者が本人か確認できる



署名画面イメージ



署名検証イメージ



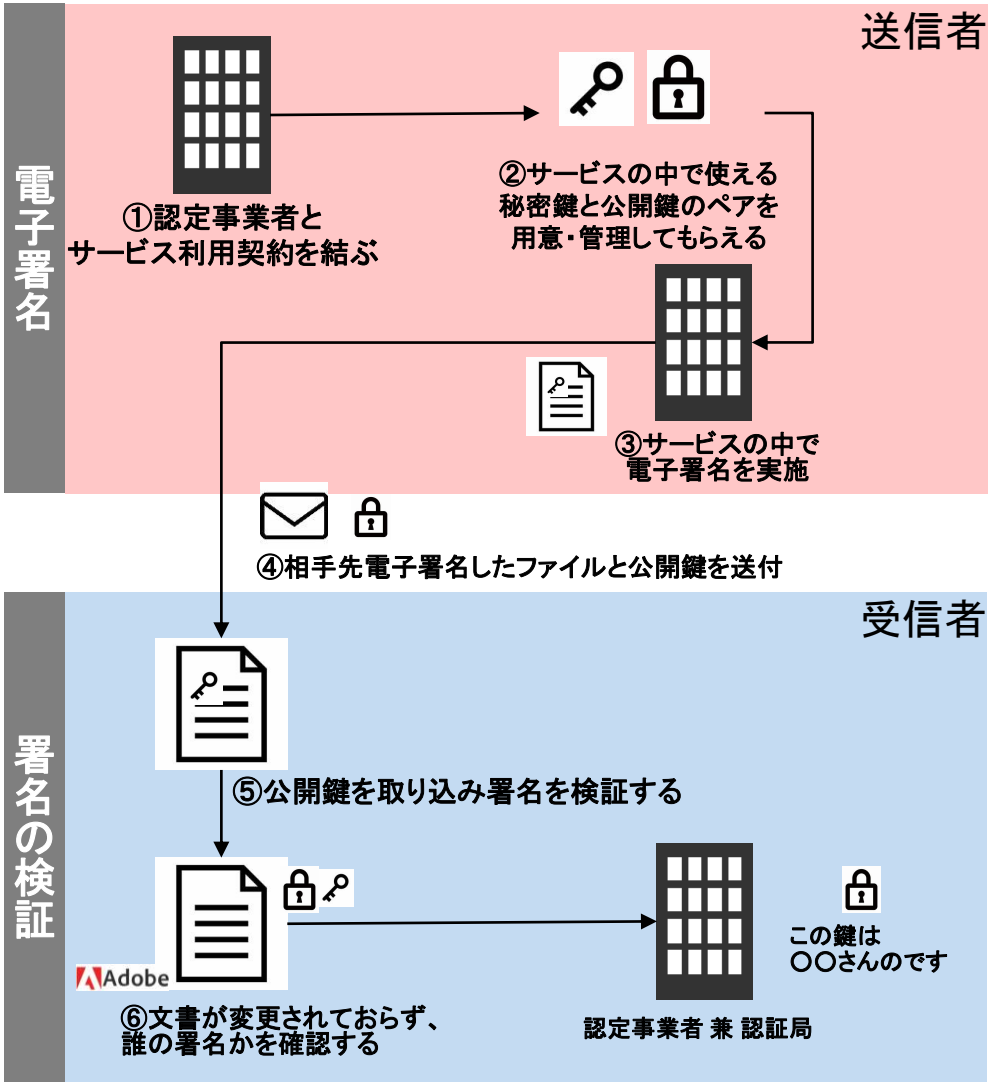
https://helpx.adobe.com/jp/acrobat/using/validating-digital-signatures.html

MUFG

Q1 Q2 Q3 Q4

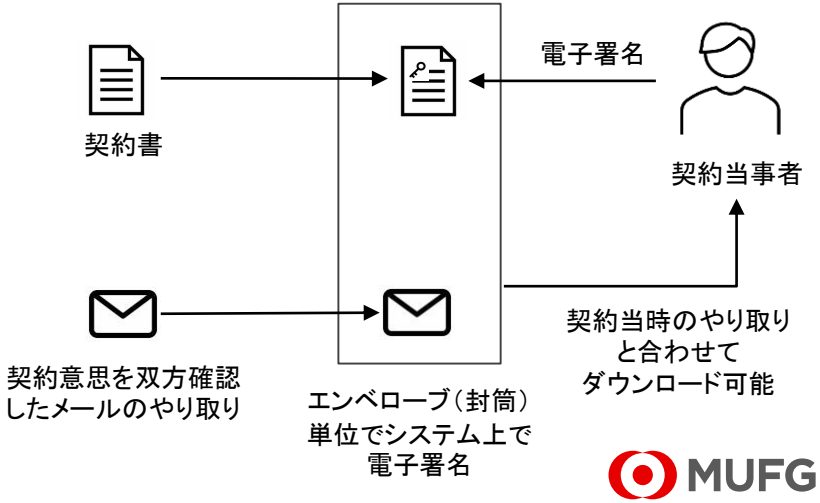
2-1-4. 電子署名について | 使い方③ 民間の電子署名事業者の活用

- 電子署名法で定められる特定認証業務（電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するもの）の認定事業者のサービスを活用する方法も考えられる



署名画面イメージ（署名プロセスが自動化されている）

DocuSign（一般認証）の操作画面、画面の案内に従って操作すると署名できる

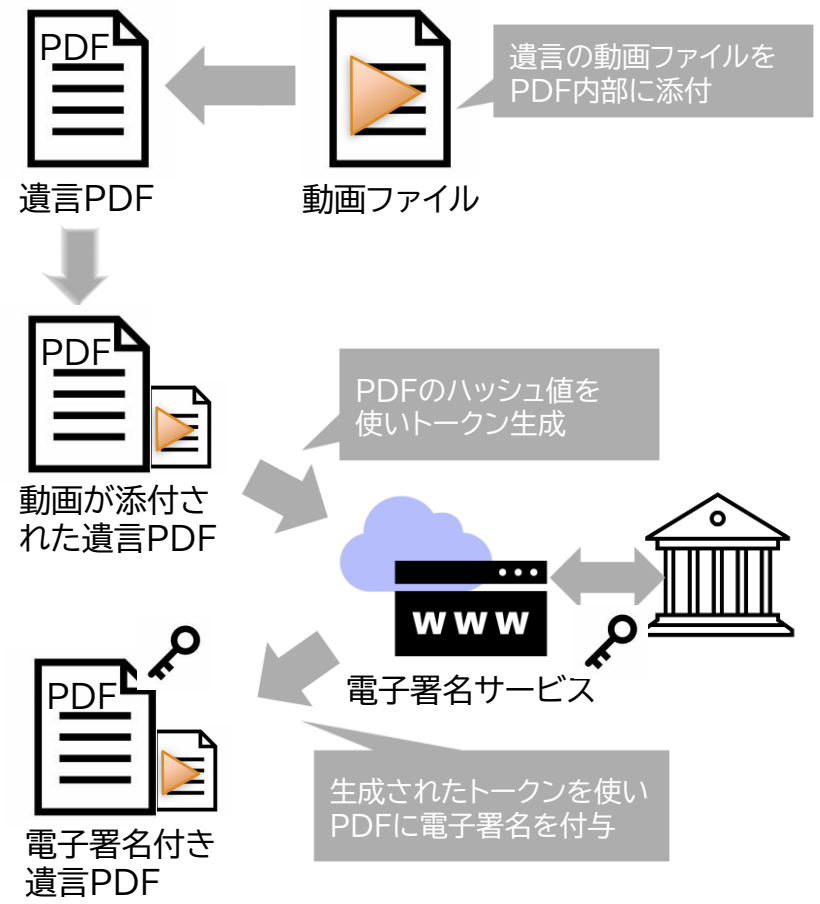


2-1-5. 電子署名について | 複数ファイル・複数人の電子署名

複数ファイルへの電子署名

- PDFに動画ファイルを埋め込んで署名実施可能
- 複数のファイルを1つの封筒に入れて署名する技術・サービスも存在

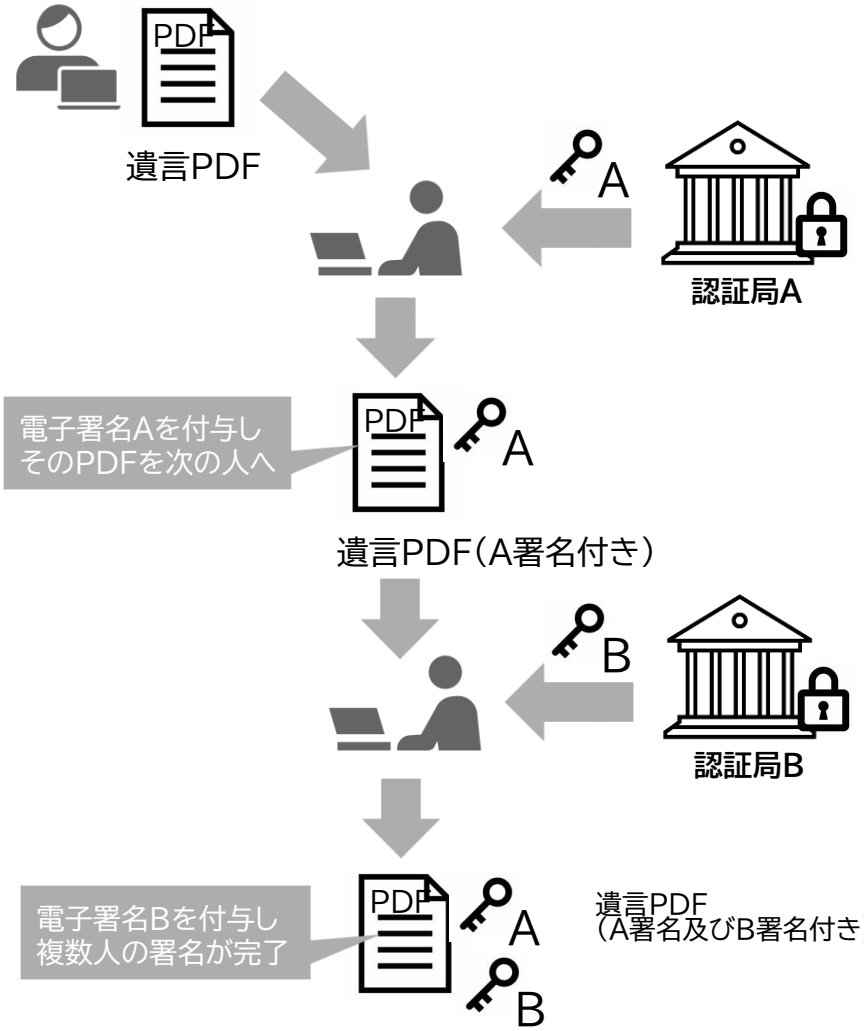
【動画を埋め込んだPDFへの電子署名のイメージ】



複数人での電子署名

◆1つのファイルに対して複数人で電子署名することも可能

【1つのファイルに複数人で電子署名のイメージ】

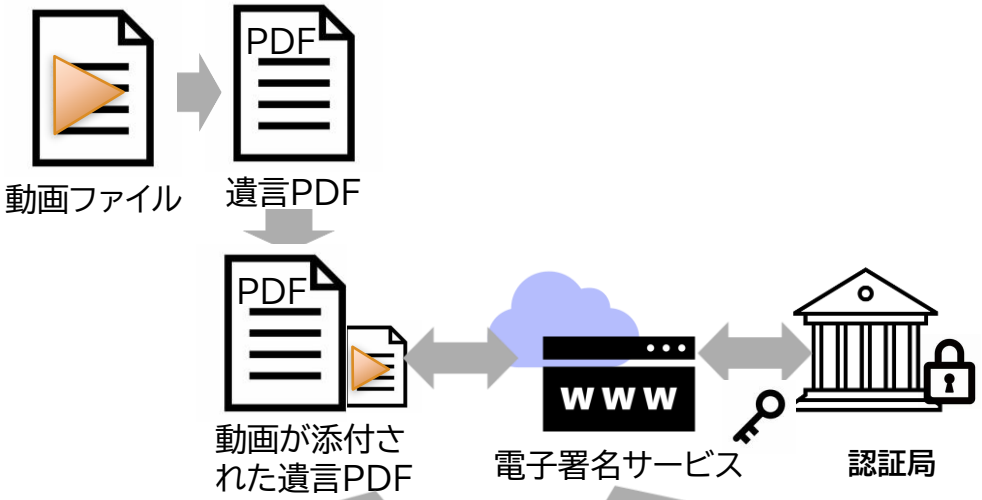


2-1-6. 電子署名について | ファイルサイズの影響

- 動画利用の場合、動画時間によってはファイルサイズがテキスト文書の1000倍以上になり、遺言作成の体験や、保管の運用費用への影響が大きいため、これを標準とするのは難しいと推察される。

電子署名+保管レスポンスへの影響

- 電子署名のためのハッシュ化の時間は必ずしもクリティカルではないが、オンライン保管の場合、登録時の通信時間は影響、全体では5分～かかる。



■ご参考
約1GBの動画ファイルを添付したPDFを電子署名、
ハッシュ値取得の時間を計測したところ15秒程度
※検証サーバースペック(仮想環境)
CPU:Xeon 2.20GHz(2コア)　メモリ:8GB

モバイル回線でアップロードする時間: 285秒程度
※DoCoMo回線+iOSでの上り性能中央値 28Mbpsの場合
https://www.docomo.ne.jp/area/effective_speed/

保管コスト（クラウド利用料）

- iPhone撮影の10分の動画を年間19200件ずつ50年保管するクラウド利用料は年間約1430万円～
- テキストのみ(800文字程度のワープロ文書)のPDFの場合、1件500KB程度となるため、年間1-2万円程度となり他の運用費が支配的になる。

■ご参考
【動画サイズの仮定】
1080p HD /30fps (iPhoneのデフォルト設定、標準画質)で 60MB/分。
遺言1件あたり10分と仮定。
1ファイルのサイズ: 60MB/分 x 10分 = 0.6GB

【遺言保管件数の仮定】
https://www.moj.go.jp/MINJI/common_igonsyo/pdf/number.pdf
月平均約1600件、年間: 1600 x 12=19200件

【1年で増加するストレージ容量】
0.6GB x 19200 = 11520GB (15TB)

【クラウド保管コスト試算】
日本政府がガバメントクラウドとして利用しているAWSの日本国内サイト(東京リージョン)でオンデマンドアクセス(いつでも参照できる)可能な最も安価なアーカイブ用のS3低頻度アクセス
※メタデータ管理と参照時の転送コストはここでは含めていない(登録に対して参照は少ないため)。
https://aws.amazon.com/jp/s3/pricing/

S3低頻度アクセスストレージ単価(東京リージョン): 1月あたり
0.0138USD/GB

年間費用: 0.0138USD/GB x 11520GB x 12ヶ月 x 150円/USD = 28.6万円、50年保管すると、年間費用: 28.6 x 50 = 1430万円

ご参考. 電子署名について | ファイルサイズの影響

保管コスト(すぐ見れなくてもいい場合)

- iPhoneで撮影した10分の動画を年間19200件ずつ50年保管するコストは、年間約200万円～

【動画サイズの仮定】
1080p HD /30fps (iPhoneのデフォルト設定、標準画質)で60MB/分。
※本人確認+本人発話確認だけであれば、低画質(720p)でもOKと推察。その場合40MB/分で2/3。
遺言1件あたり20分と仮定。
1ファイルのサイズ: 60MB/分 x 10分 = 0.6GB

【遺言保管件数の仮定】
https://www.moj.go.jp/MINJI/common_igonsyo/pdf/number.pdf
月平均約1600件、年間: 1600 x 12=19200件

【1年で増加するストレージ容量】
0.6GB x 19200 = 11520GB (11.5TB)

【クラウド保管コスト試算】
AWS東京リージョンで最も安価なアーカイブ用のS3 Glacier Deep Archive (1年に1-2回アクセスされ、12 時間以内に復元できる長期のデータアーカイブ)を利用すると想定。
※オンデマンドでは取り出せない。リクエストしてから参照可能になるまで最大12時間必要。
※メタデータ管理と参照時の転送コストはここでは含めていない(登録に対して参照は少ないため)。
https://aws.amazon.com/jp/s3/pricing/

S3 Glacier Deep Archiveストレージ単価(東京リージョン): 1月あたり 0.002USD/GB

年間費用: 0.002USD/GB x 11520GB x 12ヶ月 x 150円/USD = 4.14万円
50年保管すると、年間費用: 4.14 x 50 = 207万円

Q1 Q2 Q3 Q4

2-2-1. 生体認証について

- ✓ 生体認証では、「どのような手順」で「誰」が取得した情報と突合させるかが重要であり、突合させる情報（突合元情報）に信頼の大元（トラストアンカー）がなければ、いかに精密な生体認証であっても、本人認証方法としては、不十分
- ✓ 例えば、一般にスマートフォンのロックで使用される指紋認証は、端末への指紋の登録自体を本人がやるため、他人から見て「その登録されている指紋が本人のものか」はわからない

	顔貌		指紋		音声		虹彩（高精度）		静脈	
一般的な国民認知度	○	画面ロック解除、イベント入場等	○	画面ロック解除等	×	声紋認証のサービスは一般的でない	×	精度の高い虹彩認証は一部の施設でのみ導入	△	銀行ATMなど
情報の取得難易度	○	スマートフォン等一般的な機材で可	○	スマートフォン等一般的な機材で可	○	スマートフォン等一般的な機材で可	×	専門機材の利用要	×	専門機材の利用要
なりすましリスク	△	ディープフェイクの対策要	△	3Dプリンターなどで再現可	△	生成AIでの合成音声	○	なりすましリスクは低い	○	なりすましリスクは低い
突合元情報の確からしさ	○	国が本人確認の上で取得（マイナンバーカード）	×	警察等が特定条件で本人確認と合わせて取得	×	本人確認と合わせて取得していない	×	本人確認と合わせて取得していない	△	銀行が本人確認の上で取得
サービス提供者	○	様々な事業者がサービス提供	○	様々な事業者がサービス提供	△	専門事業者がサービス提供	△	専門事業者がサービス提供	△	専門事業者がサービス提供

詳細次頁へ

MUFG

2-2-2. 生体認証について | 信頼の大元(トラストアンカー)について

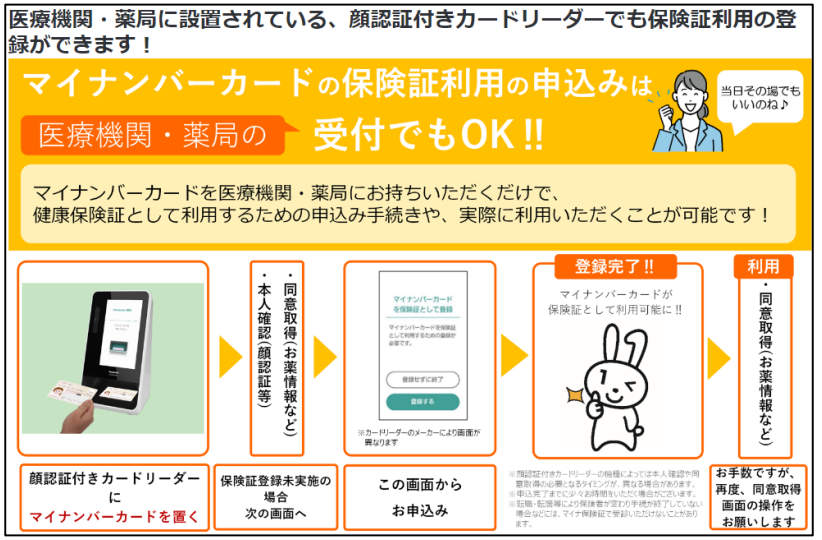
- マイナンバーカード内の券面APには券面の顔写真データが格納されています。
- 顔写真データはマイナンバーカードの交付時に地方公共団体が厳密な本人確認を実施しているため、確実に本人の情報であることが公的に保証されています。
- マイナンバーカード読み取り装置でカードから取得した顔画像とカメラによる本人撮影した顔画像を顔認証システムで比較照合することにより本人確認を行うことが出来ます。(この方法により事前の顔画像データの登録が不要となります)

マイナンバーカードのICチップ

マイナンバーカードのICチップは高度なセキュリティ技術で守られており、
外部から内部の画像の差し替えなど改竄などができません

マイナ保険証の例

マイナ保険証は、保険者本人の来院を確認するために、
格納されている顔写真データと来院者本人の顔認証の実施を始めています



2-2-3. 生体認証について | 顔貌認証の精度について

- 【カメラで撮影した画像】と【マイナンバーカード内の顔画像】を1:1で比較する為、【カメラで撮影した画像】と【データベースに登録した複数人の顔画像】を1:Nで照合を行う場合よりも認証精度は高くなります。
- NEC社内でのウォークスルー顔認証ゲート試験(※1)で算出したエラー率(※2)は、下記のとおり1:1照合では0%(※3)

※1 カメラに向かって静止している本人確認用途よりも厳しい条件
※2 間違って本人を拒否する率(FRR: False Reject Rate)
※3 2020年時点、約1万件の画像数でのデータであり、数が増えればエラーが発生する可能性があります。

1:1照合

おおよその他人受入率(FAR)	本人棄却率(FRR) 通常顔	本人棄却率(FRR) マスク顔
0.01% (1/10,000)	0.00%	0.03%
0.001% (1/100,000)	0.00%	0.06%
0.0001% (1/1,000,000)	0.00%	0.12%
0.00001% (1/10,000,000)	0.00%	0.34%
0.000001% (1/100,000,000)	0.00%	0.62%

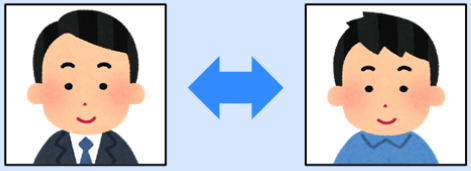
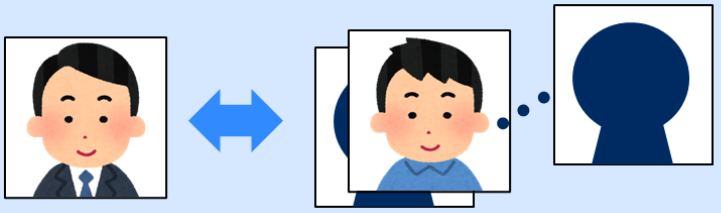
1:N照合

おおよその誤受入識別率(FPIR)	誤拒否識別率(FNIR) 通常顔 N=1万	通常顔 N=10万	マスク顔 N=1万	マスク顔 N=10万
0.1% (1/1,000)	0.00%	0.05%	1.43%	3.41%
0.01% (1/10,000)	-	-	-	-
0.001% (1/100,000)	-	-	-	-

※"-"欄は評価未実施
※所定の条件下における結果であり、
いかなる条件下でも本精度を保証するものではありません

ご参考．生体認証について｜顔認証における「1対1照合」「1対N照合」とは

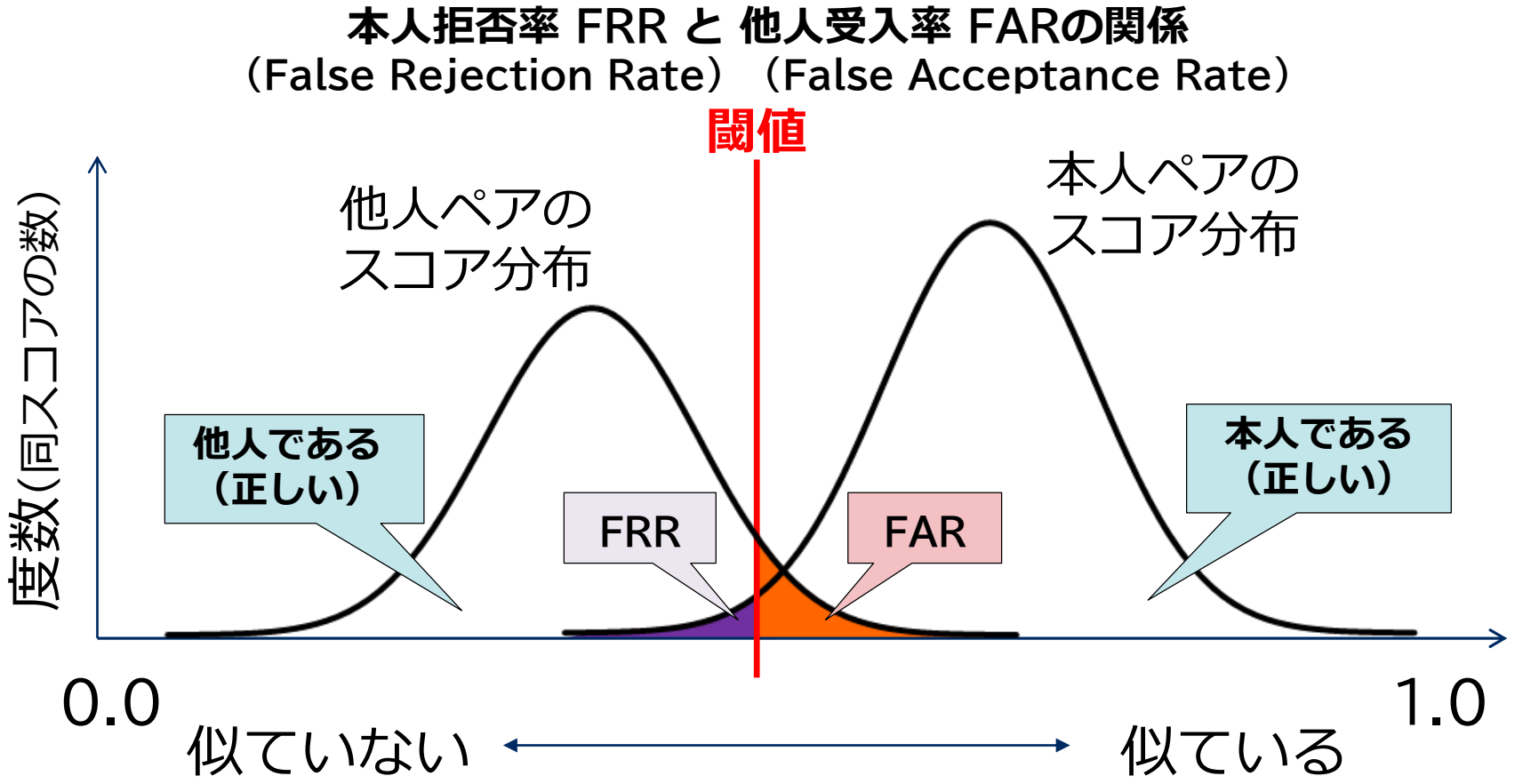
- マイナンバーカードのように本人顔画像と比較する対象がある場合は、「1対1照合」を用いる。
- 1対1照合では、他人を間違って本人と判断してしまう「他人受入率」と、本人を間違って本人でないと判断してしまう「本人拒否率」が顔認証の精度を決める。

方式	**1対1照合**	**1対N照合**
用途	パスポート、社員証等 ID写真に対する**本人確認**	人物検索 **登録画像データベースからの検索**
手法	2枚の顔画像が同一人物か否かを判定 	登録画像データベースから本人の顔画像を検索 
評価尺度	**他人受入率 FAR vs 本人拒否率 FRR**	**x位(1～5位など)照合率 誤受入識別率 FPIR vs 誤拒否識別率 FNIR**

用途に応じた照合方法を用いる

ご参考. 生体認証について | 1対1照合の評価尺度(本人拒否率と他人受入率の関係)

- 業務の要件によって本人と判断する閾値を決める。
- 閾値を高くすると、他人受入率(FAR)は減るが、本人拒否率(FRR)は増える。
- 閾値を低くすると、他人受入率(FAR) は増えるが、本人拒否率(FRR)は減る。
  →閾値により エラー率FRR・FARはトレードオフとなる。



2-2-4. 生体認証について | 顔の経年劣化に伴う認証精度への影響

Q1 Q2 Q3 Q4

- NEC社が米国政府機関で受けた試験では、Mugshot（静止画）との認証では、12年前の写真との認証でのエラー率が0.19%（当人を当人と認証できないエラー、1:N認証の場合）
- マイナンバーカード自体の有効期限が10年であることを考えると、実運用上問題ないと考えられる

Identification Performance

※2024年4月時点

The table below shows False Negative Identification Rates (FNIR) for the case where a threshold is set to limit to the False Positive Identification Rate (FPIR) to 0.003. FNIR is the proportion of mated searches failing to return the mate above threshold. FPIR is the proportion of non-mated searches producing one or more candidates above threshold. The threshold is set for each algorithm and each column separately. The use of thresholding supports use of face recognition in making mostly automated decisions e.g. for access into facility. The first row in the header shows the type of image enrolled in the gallery; the second row shows the search image type; the third row shows the number of persons in the gallery. The images are described in the section 2 of the report. In all cases, each person is enrolled with one image only.

The values in blue correspond to a change in the FRTE API on 2022-02-14 that allows the algorithm to detect and produce templates from multiple faces in one image, which occurs in approximately 3% of border images and 7% of kiosk images. The handling and accuracy consequences of this are detailed on this slide.

Show 25 entries　　Search:

Algorithm	Gallery	Mugshot	Mugshot	Mugshot	Mugshot	Visa	Visa	Border	Mugshot
	Probe	Mugshot	Mugshot	Webcam	Profile 90°	Border	Kiosk	Border ΔT ≥ 10 YRS	Mugshot ΔT ≥ 12 YRS
	Date	N = 12000000	N = 1600000	N = 1600000	N = 1600000	N = 1600000	N = 1600000	N = 1600000	N = 3000000
cloudwalk mt 002	2023-02-24	0.0020[7]	0.0018[11]	0.0113[9]	0.0589[1]	0.0016[1]	0.0477[2]	0.0157[2]	0.0030[2]
nec 009	2023-12-21	0.0012[1]	0.0011[3]	0.0068[2]	0.0640[2]	0.0016[2]	0.0459[1]	0.0062[1]	0.0019[1]
megvii 004	2023-10-18	0.0015[4]	0.0012[7]	0.0081[5]	0.0703[3]	0.0019[3]	0.0564[4]	0.0167[3]	0.0053[4]
sensetime 009	2023-01-04	0.0013[3]	0.0010[1]	0.0065[1]	0.0823[5]	0.0021[4]	0.0741[18]	0.0227[4]	-
paravision 014	2023-06-08	0.0021[8]	0.0012[6]	0.0096[7]	0.4377[42]	0.0026[5]	0.0520[3]	0.0583[13]	0.0090[8]
idemia 010	2023-01-11	0.0012[2]	0.0010[2]	0.0075[3]	0.0931[7]	0.0028[6]	0.0581[7]	0.0366[5]	0.0034[3]

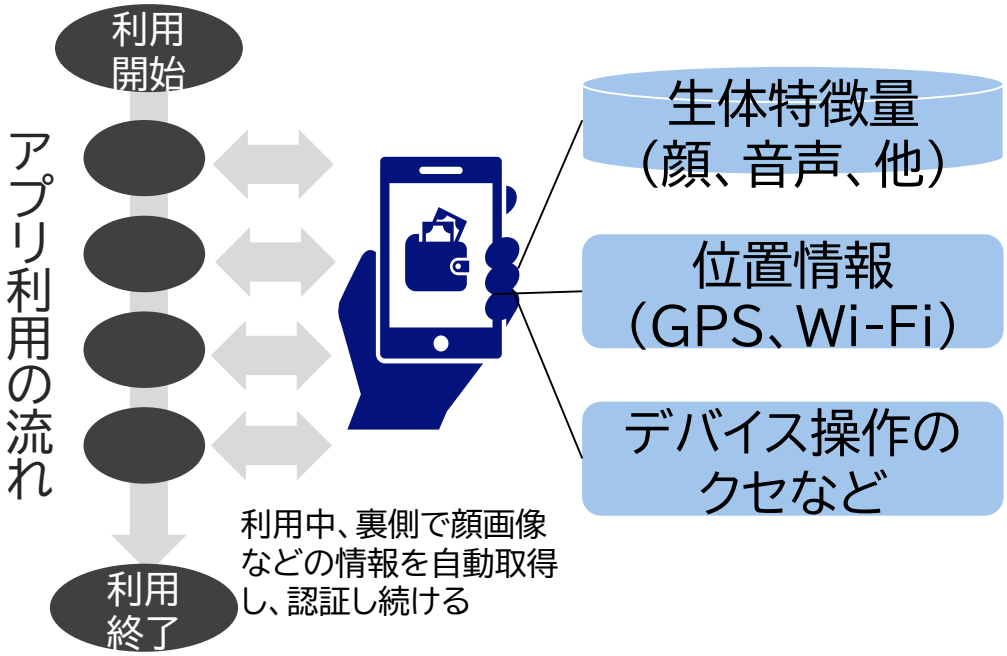
https://pages.nist.gov/frvt/html/frvt1N.html

2-2-5. 生体認証について | バックグラウンド認証について

- 複数の生体認証や、振る舞い認証を組み合わせることで、利用者が能動的に「ログイン操作」を行わなくとも、常時画面の裏側で顔などを自動撮影し、認証し続ける技術。
- 遺言作成途中での家族の別人への入れ替わりを防げるといった効果があるが、現状、まだ一部の企業のみが提供している先端的な技術であり、一般に広く普及しているものではない。

仕組み（生体情報の保管場所）

- 明示的なログイン操作は不要であり、生体認証とふるまい認証を組み合わせてアプリ利用の画面の裏側で、常時認証し続ける仕組み
- 生体情報は端末保存のため、運営側が個人情報となる生体情報を管理しなくて良い



家族のなりすましリスク

- バックグラウンド認証そのものには身元確認を行うためのトラストアンカー（信頼のもととなる根拠）が存在していない
- 例えばそもそも初回登録時に、家族の別人が、本人と偽って登録できた場合、その本人がなりすますことは可能（iPhoneのFaceID、TouchIDと同様）
  →アプリ操作途中での家族の入れ替わりなどは防げるが、あくまでも当人認証の技術であり、大元の身元確認は別に行う必要がある。

Q1 Q2 Q3 Q4

2-3-1. ブロックチェーンの仕組み

◆ ハッシュチェーンと呼ばれるデータ構造を持つデータを複数のノード（サーバー）で管理することで仕組みとしてデータの改ざんを非常に困難にしている。運営者のモデルによりいくつかの形態が存在する。

ブロックチェーンとは

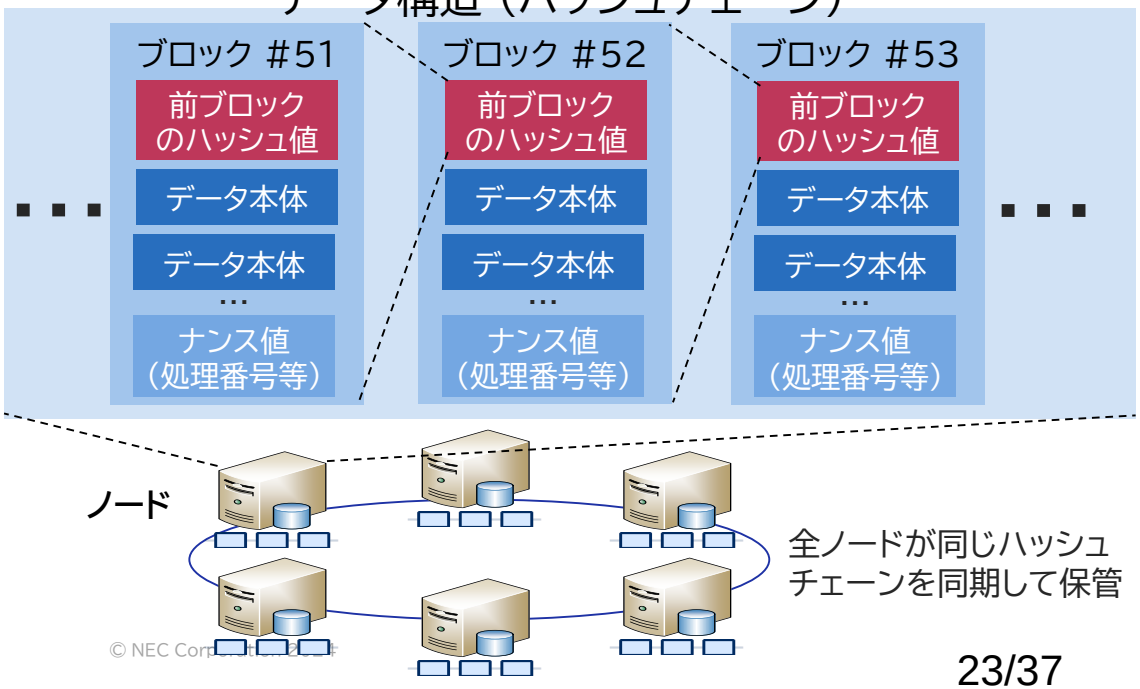
◆ 複数のデータをまとめたブロック単位でデータを管理し、ブロックを追加していくハッシュチェーンのデータ構造を持つ。

◆ ブロックのハッシュを次のブロックに含めており、一部のデータを改ざんするためには、後続データ全体の改ざんが必要になる。

◆ ハッシュとは暗号学的処理で元のデータから計算された短い文字列であり、元のデータが1箇所でも変わると全く異なる文字列になる。

◆ 更にハッシュチェーンを複数の管理者で管理することで、各ノードを同時に攻撃することが必要となり、改ざんが非常に困難になる。

データ構造（ハッシュチェーン）



ブロックチェーンの種類

◆ ブロックチェーンは、誰がノードを運営しているか、誰が書き込みを申請したり承認できるかで様々な運営形態が存在する。

【パブリックチェーン】
- 不特定多数が誰でもノード参加者となれ、誰でも書き込めるチェーン
- 代表例: Bitcoin、Ethereum
- 個人含め誰でもノード参加者となれるため、Bitcoinの場合で全世界約1.5万台、Ethereumで数千台のノードが存在
- 一般に、書き込み申請時にトランザクション利用料が時価で発生（高額申請者が優先される一種のオークション、現在のEthereumの場合、数百円～数千円）

【コンソーシアムチェーン】
- 複数の組織がコンソーシアムを組んでブロックチェーンノードを運営
- 代表例: 貿易情報連携プラットフォーム
- 一般に、書き込める人が限定される
- ノードを運営するコンソーシアム各社で、ノードの運用費用が発生する。利用料は、設計次第

Q1 Q2 Q3 Q4

2-3-2. ブロックチェーンの仕組み | 改ざん耐性と遺言への活用イメージ

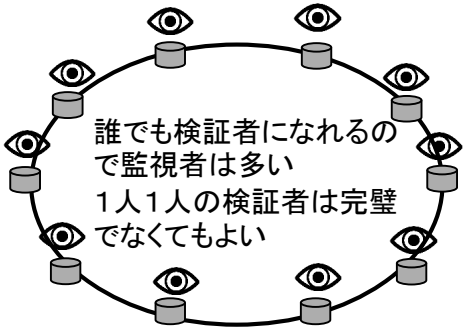
✓ **ブロックチェーンの改ざん耐性とは「衆人環視」による透明性が軸、忘れられる権利の関係から個人情報を記録することは推奨されない**
✓ **W3C（※1）では、関連技術に関する文書（※2）で個人情報の置き場所を示すリンクを記載するなど間接的に取り扱う方法を推奨している**

※1 World Wide Web Consortium　※2 DID Core勧告案

改ざん耐性の考え方

パブリック

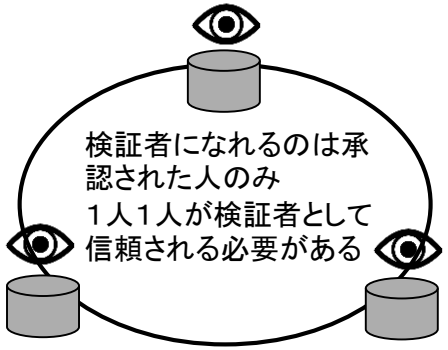
- 「みんなが見ているところ（パブリックな場所）で悪さできない」
- みんなが見てはいけないものには適さない
- パブリックブロックチェーンに一度載せた情報は消せない



チェックする人が多いほど検証の時間がかかる
検証する人に支払うお礼（ガス代）も増える

コンソーシアム

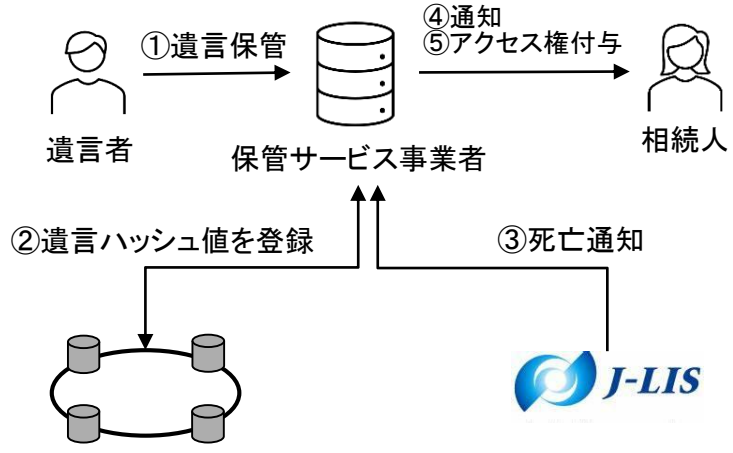
- 「信頼できる人たちで監視し合う」という考え方
- 信頼できる人たちにしか見せる必要がない
- 中央管理者が存在するので情報の削除や修正も可能



チェックする人が少ないので1人1人の責任が重い（不正アクセス被害の被害が大きい）
検証する人に支払うお礼（ガス代）も調整可能

ブロックチェーンの活用イメージ

✓ スマートコントラクトのイメージは自動販売機
✓ 例えば「改変防止措置を講じるとともに、相続開始前は遺言者のみが、相続開始後は関係相続人等が遺言に係る電磁的記録にアクセスする」を実現しようとすると以下のような形になる



ブロックチェーン上で「相続人の死亡をきっかけに、相続人に自動で何らかのアクセス権を付与しようとする機能を実現」しようとすると、ブロックチェーン上に
・個人を特定する識別子とそれに紐づく遺言ファイルを特定する情報
・遺言ファイルの保管先を特定する情報
・通知人の連絡先情報（ウォレットアドレスなど）
を保持する必要があると考えられる

Q1 Q2 Q3 Q4

2-4. 遺言への活用を想定したデジタル技術の整理

【検討の方向性】 PCやスマートフォンを利用し自筆でなくても、デジタル技術を活用することで、真正性・真意性等を担保する新制度の創設
【遺言者の想定】 一般的なPCやスマートフォンの操作方法・使い方に慣れている人

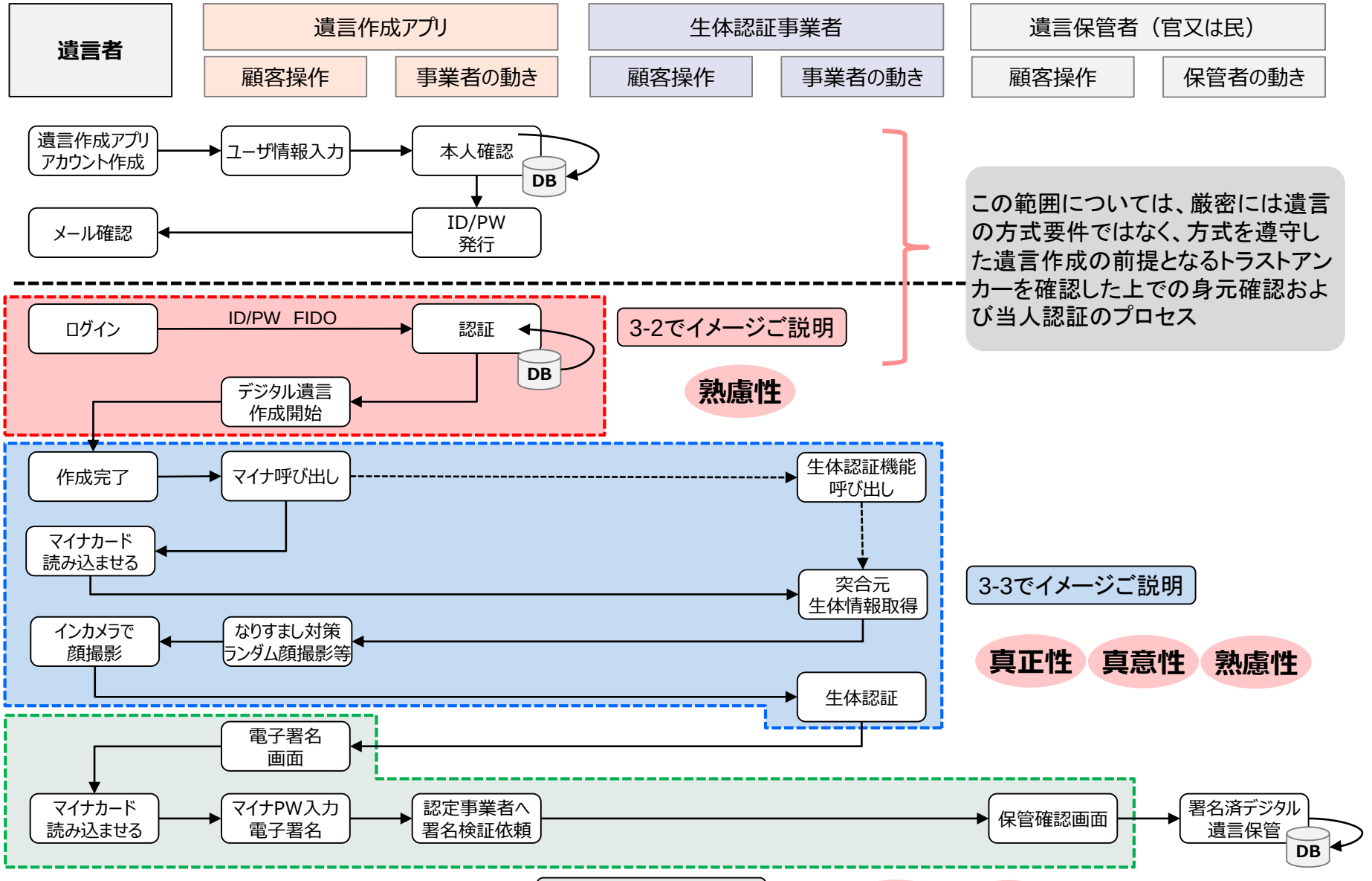
活用主目的／技術		想定される活用内容	期待効果／課題(リスク)	遺言者の利便性・手続き、機材等の一般性	運営者（官民）の負担・コスト
真意性・真正性	電子署名	・遺言として作成された電磁的記録に対し公開鍵暗号方式の電子署名を付与 (改竄検知ができるようになる)	・偽造/変造対策に有効 ・電子署名用のPWと署名鍵が流出している場合なりすましリスクあり	・作成時負担は大きくない ・マイナンバーカードを用いた電子署名は、オンライン確定申告でも実績あり	・公開鍵登録時に認証局に登録手数料が発生(マイナンバーカード活用時は鍵の登録等は無料だが、署名検証時に認定事業者への手数料が発生)
	録音/録画	・本人による遺言内容口述を録音/録画 ・代筆された遺言を本人が承認する場面を録音/録画	・偽造/変造対策に一定の効果有 ・ディープフェイクによる偽造リスクも存在	・作成時負担は大きくない ・PC/スマフォ等の普及に伴い一般性は高い（録音機能がない高齢者向け機種も存在）	・データ量次第で保管負担大 ・文字化及びその検証負担 ・相続手続時、遺言内容の確認に一定時間要
真正性	生体認証(顔貌)	・遺言の作成時、または代筆された遺言を承認する際、端末の操作者が本人であることを担保	・偽造対策に一定の効果有 ・ディープフェイクによるなりすましリスク有	・作成サービスのID/PW保管の負担を低減(FIDO/パスキー) ・スマフォの画面ロック解除やマイナンバー保険証での受診時の当人認証で一般的に利用	・生体認証サービスとのシステム連携コストが発生
	ランダム挙動撮影	・生体認証(顔貌)の際に、上下左右を向くような変則的な動作を要求	・ディープフェイクを含む偽造対策に一定の効果有	・作成時の負担は大きくない ・金融機関の口座開設手続時の身元確認で一般的に利用	・生体認証サービスの中にランダム挙動撮影要素を盛り込む
	ブロックチェーン	・PC/スマフォ等を通じて、遺言ファイルのハッシュ値をブロックチェーン上に保管	・（公的機関の保管がない場合でも）一定の変造防止可 ・個人情報を直接扱うことは推奨されていない	–	・国/事業者がブロックチェーンに情報を書き込む際に発生するガス代（随時変動）を負担
利便性	AI	・PC/スマフォで遺言作成する際の案文作成や端末操作をサポート	–	・AIを活用したサービス/アプリの普及率に依存(Chat GPT等により普及されつつある)	・遺言者の手続きの負担低減やITリテラシーを補う効果が期待される

MUFG

3.民間事業者を活用する場合の
デジタル遺言実装案

Q1 Q2 Q3 Q4

3-1. 手続き全体の流れ（作成～保管）



3-2. 遺言作成時の操作イメージ

Q1 Q2 Q3 Q4

真正性 真意性 熟慮性

①本人がアプリの利用登録を実施・ログイン

②アプリの指示に従って遺言作成に必要な情報を入力

（各事業者の工夫の領域。以下は三菱UFJ信託銀行が考えた一例）

AI等を活用し
遺言能力等を
裏側で診断　等

チャット形式での情報入力等により、熟慮性を一定程度確保するような設問設計や、遺言者の認知能力や遺言能力のスコアリングといった工夫も考えられる

③遺言文案を自動生成、ノウハウをもった組織がチェック

士業・信託銀行等の一定の実務ノウハウ・技術に基づきチェックすることで、手続きに使えないデジタル遺言の濫立を牽制する

有効性診断

〇〇信託銀行に対し、お客様が作成された遺言文案が、相続手続きに使える可能性を診断します。

キャンセル　依頼する

④チェック結果を本人に還元、電子署名フローへ

診断結果

お客様が作成された遺言は、残念ながら手続きに使える可能性が低いです。
遺言執行者のフルネームが登録されていません。（可変文言）

作成画面に戻る　専門家に相談する

診断結果

お客様が作成された遺言は手続きに使える可能性が高いです。

このまま電子署名の手続きに進みますか？

キャンセル　手続きに進む

MUFG

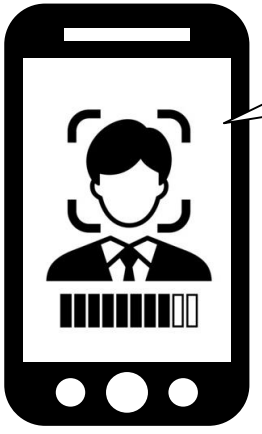
3-3. 生体認証の操作イメージ

Q1 Q2 Q3 Q4

真正性 真意性 熟慮性

①マイナンバーカードの持ち主が操作していることを確認

②ディープフェイク対策でランダム挙動の顔撮影



上を向いてください
斜め左下を向いてください

※リアルタイムに要求内容のディープフェイク映像を流すのは困難

③認証結果を表示

※本人による操作を担保するため、
一定時間でタイムアウトする設定

④意思確認・電子署名の説明

※本人による操作を担保するため、
生体認証完了から一定時間でタイムアウトする設定

MUFG

3-4. 電子署名の操作イメージ

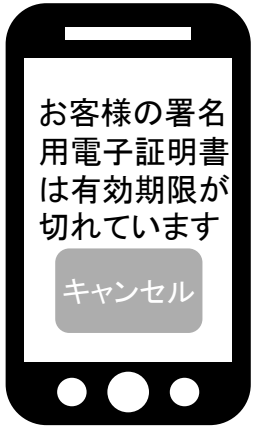
Q1 Q2 Q3 Q4

真正性 真意性 熟慮性

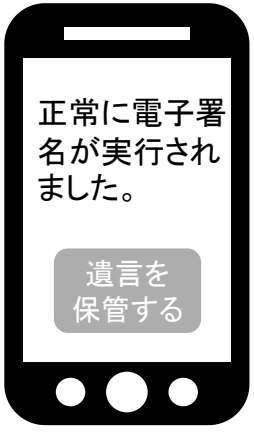
①マイナンバーカードの署名鍵を読み取り

②署名用電子証明書のパスワードの入力

③電子署名の結果を表示

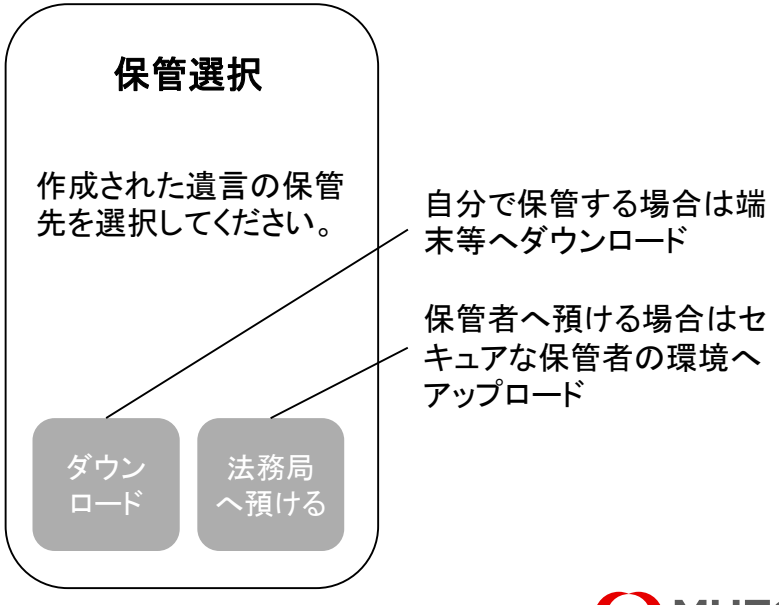


有効期限切れ等で完了しなかったとき



正常に完了したとき

④保管先についての確認



MUFG

用語集

用語	意味
J-LIS	地方公共団体情報システム機構。住民基本台帳ネットワークを運営。
電子署名における 秘密鍵・公開鍵	秘密鍵で電子署名を行い、公開鍵で電子署名が真正なものであるかを検証する。
ハッシュ値	データを固定長の値に変換する関数の出力。 データの指紋のようなもの。
ブロックチェーンにおける トークン	デジタル資産や権利を表す、ブロックチェーン上の単位。
ストレージ	データを保存するための装置やシステム。ハードディスクやSSDなど。
AWS東京リージョン	Amazon Web Servicesの日本にあるデータセンター群。
オンデマンドアクセス	必要なときに即座にデータやサービスにアクセスできる方式。
アーカイブ	長期間保存するためのデータや記録の集積。バックアップなど。
S3体頻度	Amazon Web Servicesのアクセス頻度が低いデータ向けのストレージサービス
アクセスストレージ	頻繁にアクセスされるデータを保存するためのデータの読み書き速度が速いストレージ。
生体認証における1:N照合	生体情報が登録されているデータベースから、照合対象が誰であるかを確認する。

APPENDIX

APPENDIX. 電子署名にかかる認定事業者等について

特定認証業務を行う者

株式会社日本電子公証機構
（株式会社日本電子公証機構認証サービスｉＰＲＯＶＥ）

セコムトラストシステムズ株式会社
（セコムパスポートforＧ－ＩＤ）

株式会社トインクス
（ＴＯｉＮＸ電子入札対応認証サービス）

株式会社帝国データバンク
（ＴＤＢ電子認証サービスＴｙｐｅＡ）

NTTビジネスソリューションズ株式会社
（e-Probatio PS2 サービス）

三菱電機インフォメーションネットワーク株式会社
（DIACERT サービス）

日本電子認証株式会社
（AOSign サービス G2）

三菱電機インフォメーションネットワーク株式会社
（DIACERT-PLUS サービス）

NTTビジネスソリューションズ株式会社
（e-Probatio PSA サービス）

my FinTech株式会社
（my電子証明書）

マイナンバーカードの電子署名検証者

署名検証者(第17条第1項)、利用者証明検証者(第36条第1項)

- 情報通信技術を活用した行政の推進等に関する法律第三条第二号に規定する行政機関等
- 裁判所
- 行政機関等に対する申請、届出その他の手続に随伴して必要となる事項につき、電磁的方式により提供を受け、行政機関等に対し自らこれを提供し、又はその照会に応じて回答する業務を行う者として行政庁が法律の規定に基づき指定し、登録し、認定し、又は承認した者
- 電子署名及び認証業務に関する法律第8条に規定する認定認証事業者
- 電子署名及び認証業務に関する法律第2条第3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主務大臣が認定する者
- 上記以外の者であって、署名利用者から通知された電子署名が行われた情報について当該署名利用者が当該電子署名を行ったこと又は利用者証明利用者が行った電子利用者証明について当該利用者証明利用者が当該電子利用者証明を行ったことの確認を政令で定める基準に適合して行うことができるものとして主務大臣が認定するもの

認定プラットフォーム事業者

ICTまちづくり共通プラットフォーム推進機構
（株）NTTデータ
GMOグローバルサイン（株）
日本電気（株）
（株）サイバーリンクス
日本医師会
（株）日立製作所
（株）システムコンサルタント
サイバートラスト（株）
TOPPANエッジ（株）
（株）野村総合研究所
（株）シフトセブンコンサルティング
TIS（株）
（株）ダブルスタンダード
（株）フライトソリューションズ
ポケットサイン（株）
弁護士ドットコム（株）
（株）ミラボ
エヌ・ティ・ティ・コミュニケーションズ（株）
（株）ACSiON

団体検証者（17条5項）

全国社会保険労務士会連合会
日本行政書士会連合会
日本司法書士会連合会
日本税理士会連合会
日本土地家屋調査士会連合会
日本弁理士会

法務省

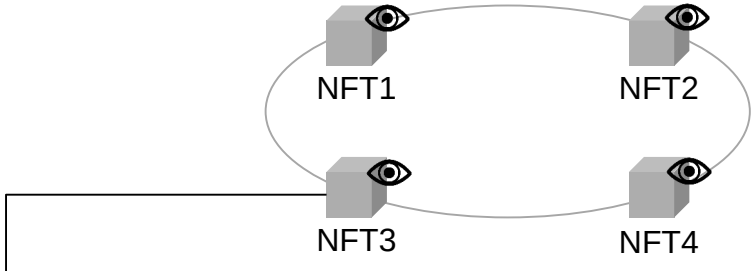
MUFG

APPENDIX. リビールについて

- ✓ **ブロックチェーンゲームで、特定のアクションをキックにNFTの中身を書き換えるリビールという技術がある**
- ✓ **リビールを用いたブロックチェーン上でデジタル遺言のアクセス権管理については公開されるメタデータにどこまでの情報を記載するか、スマートコントラクトに外部からの編集権を記載するかといった論点がある**

リビールの説明

- ✓ 予め決められたスマートコントラクトに基づいて、書き込まれた関数に従ってメタデータの中身を書き換えることが可能
- ✓ ガチャガチャをイメージ（あらかじめ出る順番が定められた筐体に対し、お金を入れてハンドルを回すという動作をきっかけに景品が取り出せ、中身を見ることができる）



トークンID	所有者アドレス	メタデータ
1	0x12345abc	{“ステータス”:”未開封”, ”image”:”https://example.com/hidden.png}

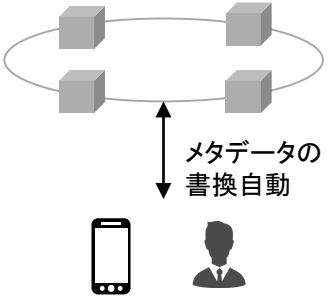
開封動作
（開封動作をきっかけとしたスマートコントラクトの処理により中身が変更）

トークンID	所有者アドレス	メタデータ
1	0x12345abc	{“ステータス”:”開封済”, ”image”:”https://example.com/itemA.png}

リビールの実装方法

スマコン完結型

利用イメージ



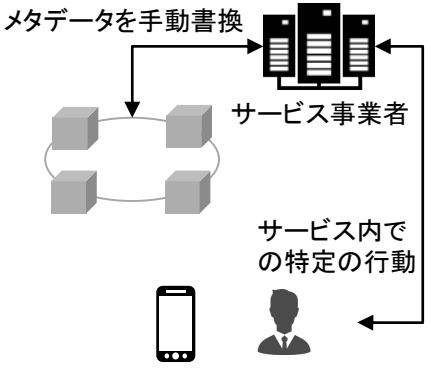
1人でガチャガチャを回して景品を取得

遺言への応用

保存した情報の管理に課題が残ると思われる

1. リビール後のメタデータが公開されるため
2. メタデータを暗号化したとしてもブロックチェーンから削除できないため、暗号化技術のライフサイクルとともに破られる可能性がある

外部操作併用型



屋台で当たったくじを人に景品に変えてもらう

ブロックチェーンである必要性に課題が残ると思われる

1. サービス事業者のDBの役割にしかなっていないのでブロックチェーンである必要性が薄い
2. ブロックチェーンに載せられる情報がステータスぐらいにしかならない

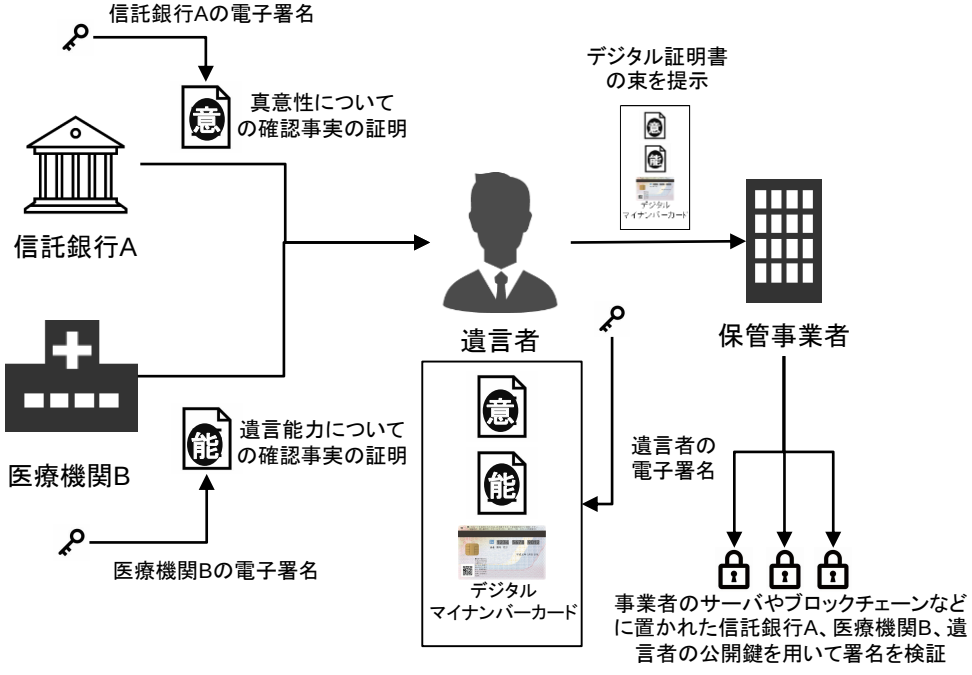
MUFG

APPENDIX. デジタル証明書（Verifiable Credentials）の活用

✓ **遺言者の属性を相手方に証明するデジタル技術としてVerifiable Credentialsの活用も考えられる**
✓ **デジタル化されたマイナンバーカードとセットにすることで相手方に身元情報と付帯する属性情報を通知することが可能**

Verifiable Credentialsの説明

✓ 現実の遺言者を知る信頼性のある組織が、遺言者に対して電子署名されたデジタル証明書を発行
✓ デジタル証明書を受け取った遺言者は、他のデジタル証明書（例えばデジタル化されたマイナンバーカード）と合わせ、証明書を束にしたものに自分の電子署名を付与して相手方に提示することができる）



民間側での活用/検討

✓ 業界横断で共通規格のデジタル証明書発行に向けて協議中

3メガや地銀、銀行共通のデジタル証明書
本人確認、事務負担を軽減　来年にも
2024/6/21付 | 日本経済新聞　朝刊

保存　共有　その他

3メガバンクや大手地銀が、口座開設などの本人確認で利用できる「デジタル証明書」をつくる。データを改ざんしにくいブロックチェーン（分散型台帳）を活用し、氏名や住所、生年月日などの個人情報をデジタル化する。複数の金融機関で利用できるデジタル証明書の仕組みを共通にして、店頭の事務などの効率を高める。

三菱UFJ信託銀行がつくるデジタル証明書の協議会に、三菱UFJフィナンシャル・グループ（FG）、三井住…

https://www.nikkei.com/nkd/industry/article/?DisplayType=2&n_m_code=121&ng=DGKKZO81542760Q4A620C2EE9000

✓ 顔写真情報と合わせて社員証をデジタル化

顔認証と自己主権型 ID管理を組み合わせた「デジタル社員証」の展開がスタート

NECが、顔認証技術と自己主権型 ID 技術を組み合わせたデジタル社員証を新たに開発し、社員への展開を開始しました。デジタル社員証は従来のカード型の社員証を置き換えるもので、スマートフォン アプリとして利用します。本社で勤務する社員への導入からスタートした本取り組みは、今後、グループ会社を含めたNEC国内グループ全社員に拡大し、さまざまなシーンで活用していく予定です。

https://news.mynavi.jp/techplus/kikaku/azure_case_td-274/

ディスクレーマー

本資料に記載している見解等は本資料作成時における見解であり、経済環境の変化、技術進歩、法制・税制等の変更によって予告なしに内容が変更されることがあります。
また、記載されている推計計算の結果等につきましては、前提条件の設定方法によりその結果等が異なる場合がありますので、充分ご留意ください。

本資料は、当社が公に入手可能な情報に基づき作成したものですが、その内容の正確性・完全性を保証するものではありません。

本資料に記載の情報等は内容が要約されていたり、一部分のみをお伝えしている場合もあります。

本資料に記載の内容を利用したことにより生じた損害については、当社は一切責任を負いません。

本資料は、現時点での各種想定条件を設定の上、デジタル遺言の実現に向けた検討のために一例として作成したものです。

本資料に記載の条件は、実際に実現可能であることを保証するものではありません。

本資料に関するお問い合わせ先
三菱UFJ信託銀行株式会社

MUFG相続研究所
三菱UFJ信託銀行株式会社　フロンティア事業開発部

日本電気株式会社