MobileIO

Specification

1/12/2026

Version1.0

目　　次

1　MOBILEID とは 5
2　個人情報データベース 6
2.1.　構造 7
2.1.1.　データベースの種類 7
2.1.2.　データベースの構造 7
2.2.　自治体管理部個人情報の登録 9
2.2.1.　顔情報の登録 9
2.2.2.　アカウント及び PinCode の登録 10
2.2.3.　チャージ（銀行システムにより更新されるデータ） 11
2.3.　自己管理部個人情報データの登録 11
2.3.1.　SN の登録 12
2.4.　身分証の発行 12
2.5.　個人情報の更新 15
2.6.　個人情報データベースの暗号化 15
2.6.1.　AES（256）（Advanced Encryption Standard）暗号 16
2.6.2.　RSA(1,024)（Rivest–Shamir–Adleman）暗号 16
3　本人確認 18
3.1.　電子 ID カード@オンライン 18
3.2.　電子 ID カード@オフライン 20
3.3.　印刷 ID カード 23
4　投票 25
5　CQR 決済 29
5.1.　オンライン対面決済 33
5.2.　オフライン対面決済 36
5.3.　非対面決済 39
6　オプション機能 40
6.1.　運転免許証 40
6.2.　所有自動車（州資産の追跡） 41
6.3.　所得証明書（納税証明書） 42
6.4.　教育・医療・文化・社会保障等証明書 43

7 メンテナンス・保守 44
7.1. メンテナンス 44
7.2. 保守 45
8 バックアップ 46
9 動作確認スマートフォン 48
10 FAQ 49
10.1. MOBILEID 49
Q1. MobileID とは何ですか？ 49
Q2. MobileID の利点は何ですか？ 49
Q3. ログイン対策はしていますか？ 50
Q4. MobileID はリバースエンジニアリング対策をしていますか？ 50
Q5. 個人情報の更新手順は？ 50
Q6. MobileID の再発行の手順は？ 50
10.2. 個人情報データベース 51
Q7. 自治体管理部個人情報の登録手順を教えてください。 51
Q8. 登録に必要なエビデンス資料は何ですか？ 51
Q9. 個人情報データベースとは何ですか？ 51
Q10. 個人情報データベースにはどのような情報が含まれますか？ 51
Q11. 個人情報 DB のセキュリティ対策はしていますか？ 51
10.3. 本人確認 52
Q12. 電子 ID カードと印刷 ID カードの両方を持つことはできるのでしょうか？ 52
Q13. オンラインでの本人確認手順は？ 52
Q14. オフラインでの本人確認手順は？ 52
Q15. IMEI の偽造 52
Q16. ラミネートプリンターについて教えてください 53
10.4. 投票 53
Q17. 年齢や国籍での制限は簡単にできるのでしょうか？ 53
Q18. 選挙期間中に ID カードを再発行した場合、2 回投票できるのですか？ 53
10.5. CQR 決済 54
Q19. 取引履歴の暗号化方法を教えてください 54
Q20. 支払して、そこで終わってしまいました 54
Q21. オフライン取引の履歴を消してしまいました 55
Q22. オフライン取引の履歴改ざん対策を教えてください 55
Q23. 同一人物（または仲間）の履歴改ざん対策を教えてください 55
Q24. 最初から払う気がない（詐欺）場合の対策を教えてください 55
Q25. 取引履歴の偽造対策を教えてください 56
Q26. 盗んだスマホで取引されたらどうなりますか？ 56
Q27. スマートフォンを無くしてしまいました。チャージ金は戻りますか？ 56
10.6. オプション機能 57
Q28. 本人が登録するオプションって、その情報に信憑性を保証できるのですか？ 57
Q29. 顔認証機能を「監視システム」に応用できますか？ 57
10.7. メンテナンス 57

Q30. MobileID システムのメンテナンスについて教えてください。 57
10.8. バックアップ 57
Q31. バックアップはどのように行われますか？ 57

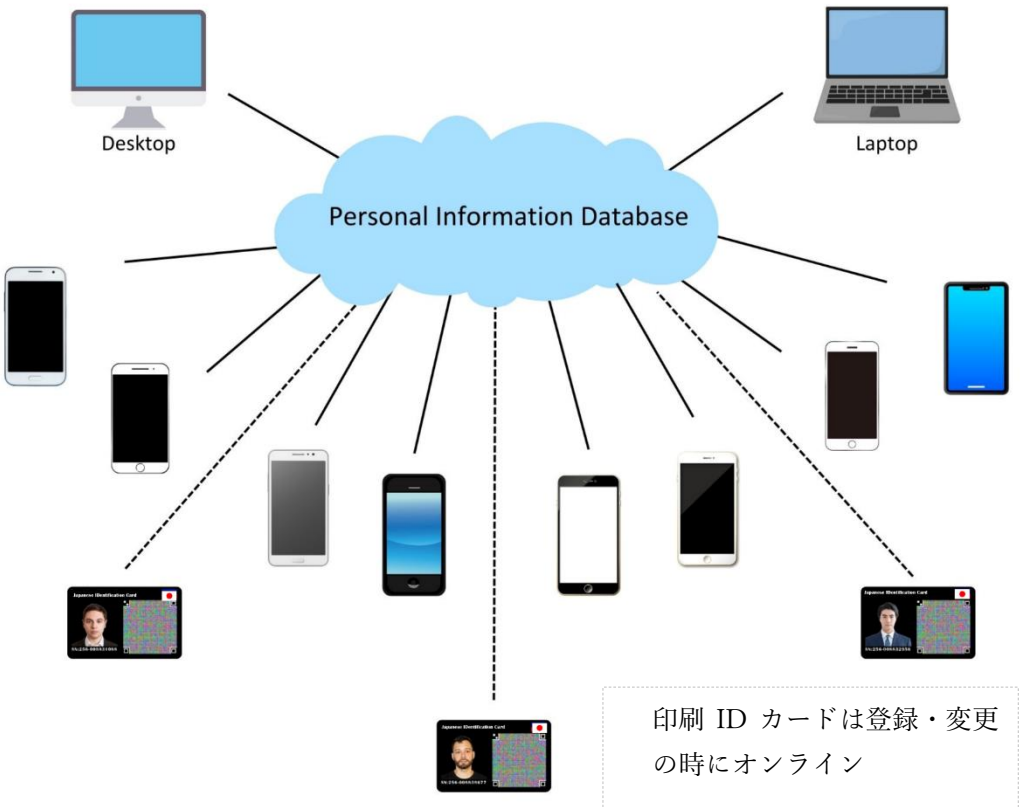
1 MobileID とは

MobileID は、個人情報データベースに安全にアクセスできるスマートフォンアプリで、公式な身分証明書として機能します。このアプリは、印刷 ID カードにも対応しているのでスマホを ID カードリーダーの代わりに使うことができます。特に優れているのは、インターネットに接続していなくても本人確認ができる点です。印刷 ID カードであっても、従来の ID カードリーダーを使わずに、オンラインと同様に本人確認が可能になります。

また、MobileID には投票機能があり、すべての市民がどこからでも簡単に投票できるため、投票率の向上やコスト削減、集計の効率化及び不正の排除にも寄与します。

さらに、オンラインでもオフラインでも利用可能な決済機能を搭載。MobileID は電子 ID カードとしてだけでなく「電子決済カード（※)」としても活用できます。

MobileID を利用することで、従来の身分証明書に比べて偽造や盗難のリスクが減り、デジタル社会での生活がより安全かつ便利になります。そのセキュリティ性と利便性から、今後、普及していくべき社会基盤と考えられます。



MobileID と個人情報データベース

※電子決済機能は銀行システムとのインテグレーション開発が前提となります。

2 個人情報データベース

個人情報データベースにはユニークな個人番号として PID（Personal IDentification）が割り当てられており、これをキーにして下記の個人情報をデータベース化しています。これらの情報を用いて本人が何者であるかを証明することや投票及び電子取引、そして高額商品等の所有証明や資格証明を可能としています。

権限を有する者が登録・更新できる自治体管理部	PID（個人番号）	自治体番号＋シーケンシャル番号	第1AES暗号＋公開暗号化方式で暗号化
	氏名	Abcd xyz	
	生年月日	ddmmyyyy	
	国籍	出生証明書、またはパスポートを参照	
	現住所	自治体データベースとの連携が必須	
	出生地住所	自治体データベースとの連携が必須	
	滞在証明	管理官庁データベースとの連携が必須	
	出入国履歴	管理官庁データベースとの連携が必須	
	顔写真	RDB （写真は複数登録可）	
	顔ベクトル	顔の特徴を数値化したもの。特徴量ベクトル	
	性別	パスポートの参照が望ましい	
	履歴用秘密鍵	登録時に自動生成	
	PinCode	6 桁の数字、ログインパスワード	
	アカウント	７～14 桁の数字、ログインアカウント	
	チャージ	CQR 決済で使える金額	
	死亡日(or 抹消日)	ddmmyyyy　（個人情報は消去されない）	
	PID 発行者と登録日	オペレータ番号 xxxx と ddmmyyyy	
	RDB 暗号鍵	RDB 用 AES 暗号鍵	
	投票状況	現在進行中の選挙情報及び投票情報　RDB	
	公開鍵	RSA 暗号化せずに単に AES 暗号化	
本人が登録・修正できる自己管理部	SN	有効な印刷 ID カードの Seral Number	第2AES暗号化
	スマホ番号	電話番号	
	IMEI International Mobile Equipment Identification	端末識別番号（自動登録） GSM/W-CDMA/iDEN の全てのスマホや一部の衛星電話に付与される識別番号。*#06# と入力すればスマホの画面にも表示できる。	
	運転免許証 No(※)	オプション	
	所有自動車 No(※)	オプション　または州資産の追跡　RDB	
	所得証明書(※)	オプション　または納税証明書　RDB	
	医療・教育等（※）	オプション　教育・医療・社会保障等証明書	
	銀行口座番号(※)	オプション　RDB（複数登録可）	

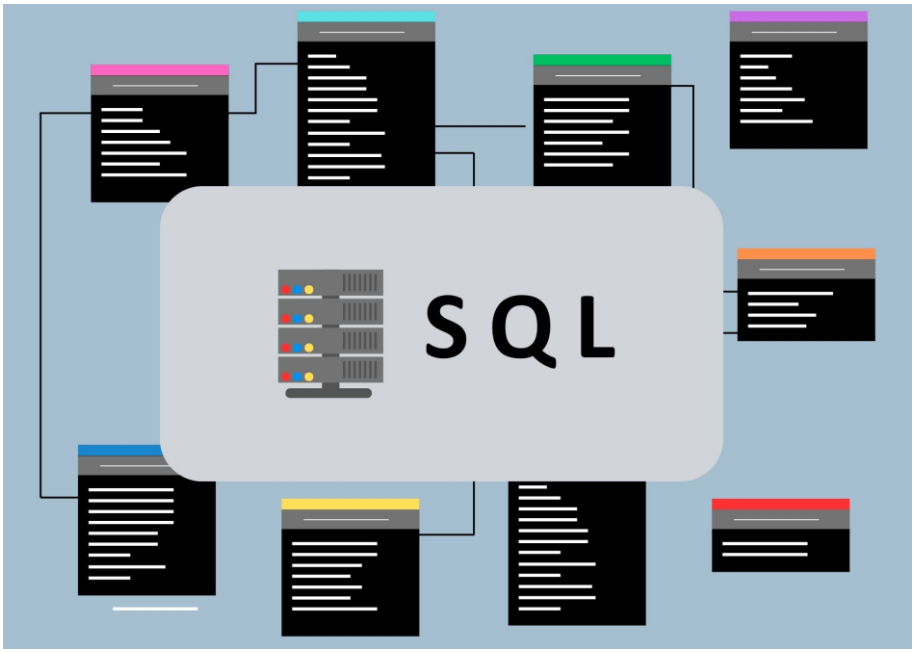
個人情報データベース（システム要件により変更される場合があります）

※情報の登録・変更に用いられたエビデンス資料（画像 or PDF）がサーバーに保管されています。

2.1. 構造

2.1.1. データベースの種類

個人情報データベースはデータをテーブル形式で管理し、SQL（Structured Query Language）を使用してデータの操作や照会を行います。



リレーショナル SQL データベースは、データの整理・管理に優れており、大規模なデータセットを効率的に扱うのに適しています。個人番号のような一意の識別子を使用してデータを管理することで、正確な情報の管理が可能となります。
そうすることで、データの一貫性、整合性、効率的な検索・操作が可能です。例えば、免許証データベース（テーブル）、犯罪歴データベース（テーブル）、州資産データベース（テーブル）などの拡張が容易になります。

2.1.2. データベースの構造

個人情報データベースは、秘匿性および更新の頻度や重要性、公共性などの観点からロールベースアクセス制御で、管理者だけが登録・更新できる自治体管理部と、本人が登録・修正できる自己管理部の 2 元構造で構成されています。

(1) **自治体管理部個人情報データベース**は AES 暗号化してサーバー上で管理されますが、オフラインでも活用できるようにするために、身分証明

書（ID カード）に複製保存されます。このため、通常の AES 暗号化に加えて公開暗号化方式で暗号化されています（公開鍵は除く）。

(2) **自治体管理部個人情報データベース**は、MobileID アプリケーションで生成、登録、変更が可能ですが、これらの操作は特定のオペレータ番号を有する管理者権限がある人物のみが許可され、顔認証を経て操作可能になります。

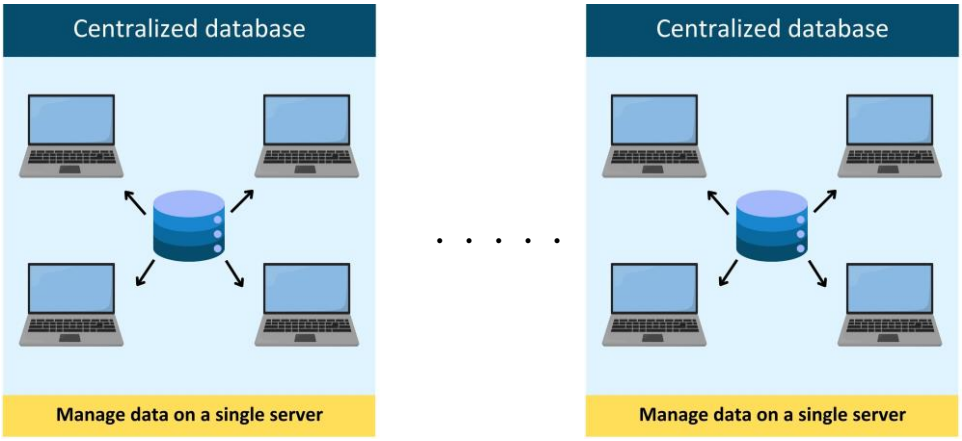
(3) **自己管理部個人情報データベース**は AES 暗号化してサーバー上でのみ運用・管理されるためオンラインでのみ参照することができます。このため、自己管理部の情報を必要とする決済やサービスは、オフラインでは利用できません。

(4) **自己管理部個人情報データベース**は、本人が MobileID アプリケーションにログインし登録・修正することができます。登録・修正を行う際にはエビデンス資料をアップロードする必要があります。入力間違いを防ぐために、エビデンス資料を元に文字識別機能等により自動入力されます。

(5) 国民台帳

個人情報データベースのインデックスとなる PID は 3 桁の自治体番号と 9 桁のシーケンシャル番号で構成された個人番号で、地方自治体が発行します。したがって、個人情報データベースは自治体ごとの集中型データベースが多数存在するデータベースです。これを統合することで、国民全体を対象とするデータベースとなり、国民台帳として運用することが可能になります。

- ひとつの自治体で発行できるPIDの最大値は99,999,999（1億個）です。これを上回る時はその自治体の2つ目の自治体番号を発行します。



個人情報データベースの統合＝国民台帳

2.2. 自治体管理部個人情報の登録

自治体管理部個人情報データベースの情報登録は個人情報登録希望者が来所した際、認定された担当者がMobileIDに管理者ログインし、エビデンス書類を確認しながら来所者の氏名や生年月日現住所などの個人情報を自治体管理部個人情報データベースに登録を行います。なお、エビデンス資料はRDB構成でサーバーに保存されます。

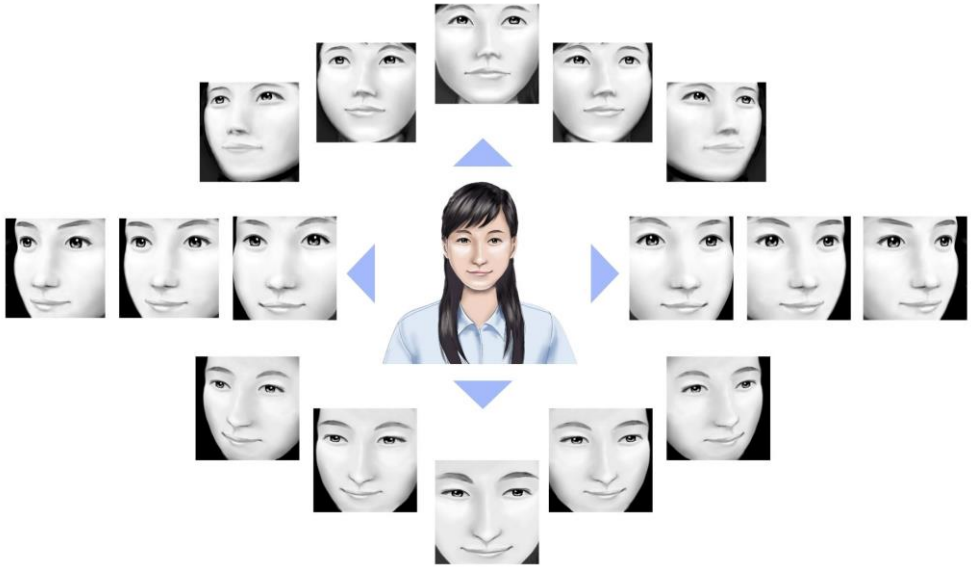
次に2.2.1顔情報の登録、2.2.2アカウント及びPinCodeの登録2.2.3チャージ（銀行システムにより更新されるデータ）、**エラー! 参照元が見つかりません。**等の登録をその場で行います。手順を以下に記します。

上記作業が完了すると、PIDやRDB暗号鍵及び履歴用秘密鍵などの項目が自動生成されて入力担当者には見えない状態で保存されます。

以上で自治体管理部個人情報データベースが完成します。

2.2.1.顔情報の登録

顔情報とは顔写真と顔ベクトルです。来所者の真顔を中心に複数の角度から写真を撮影します。そして、顔写真は個人情報データベース自体には保存せず、RDB(Relational DataBase)構造でサーバーに保存し、顔の特徴を数値化して「顔ベクトル」として登録します。
MobileIDが採用している顔認識技術（FaceNet）は、光の具合、顔の角度、表情の変化など、環境によって認識精度が影響を受けることがあります。この点を踏まえて撮影します。



真顔を中心に複数の角度から写真を撮影

MobileID では顔認証のために顔の特徴を 512 次元のベクトルに変換しています

2.2.2. アカウント及び PinCode の登録

個人情報の登録希望者に、7～14 桁の数字をアカウントとして、そして 6 桁の数字を PinCode として設定してもらいます。アカウント及び PinCode は、MobileID へのログインに使用するパスワードとして機能し、登録希望者自身が管理するものです。このコードは他人に知られないように注意し、万が一忘れた場合は再登録のために来所が必要であることを十分に説明します。

スマートフォンがなく印刷 ID カードの希望者にもアカウント及び PinCode を登録してもらいます。このアカウント及び PinCode は印刷 ID カードでの本人の確認をする際に利用されます。

2.2.3. チャージ（銀行システムにより更新されるデータ）

チャージとは電子決済を行うための電子マネーです。電子マネーは MobileID 間で現金と同等に使うことができます。

電子マネーを利用するには、まず銀行口座を登録し、その口座から MobileID に資金をチャージする必要があります。この際、資金移動を行うためにはスマートフォンを用いた本人確認が必須です。この手続きにより、不正行為を防ぎ、安心して取引を行うことができます

注意

チャージ項目は自治体管理部個人情報データベースにありますが自治体の担当者はアクセスできません。スマートフォンの持ち主だけが銀行システムを経由して増額（銀

行システムからスマートフォンに資金移動）や減額（スマートフォンから銀行システムに資金移動）できます。

2.3. 自己管理部個人情報データの登録

MobileID は初回ログイン時に電話番号の入力を求め、その後、自動的に IMEI を取得し、自治体管理部個人情報データベースに保存します。スマートフォンを変更した場合には、IMEI の更新が必要です。また、電話番号も変更があった場合は更新してください。これらの更新を怠ると、本人確認や取引ができなくなる可能性があります。

自己管理部個人情報データベースへの情報登録は、スマートフォン番号と IMEI を除き任意となっています。ユーザーは、MobileID アプリケーションにログインすることで、いつでも自身で情報を登録・修正できます。

手順

MobileID で、該当する自己管理部個人情報データベースのメニューをタップし、登録・更新を行います。登録・更新には MobileID で撮影したエビデンス資料の画像をアップロードします。

2.3.1.SN の登録

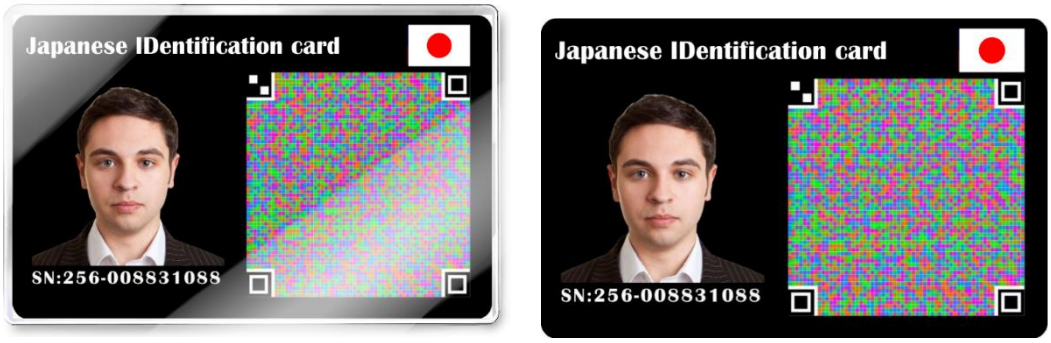
SN（Seral Number）とは印刷 ID カードに付与されるシリアルナンバーで、自己管理部個人情報データベースに書かれた SN の印刷 ID カードが有効であることを示します。スマートフォンを紛失や盗難が発生した際には ID カードを無効化するために SN 値を 0 または他の SN に更新しなければなりません。他人が利用できないように顔認証や Pincode などで守られていますが、盗難届や紛失届が提出されるまでは利用できるので万が一の被害を未然に防ぐためにも届け出る必要があります。スマートフォンを借りて盗難届や紛失届の手続きをすることができます。

一方、印刷 ID カードを複数持っていれば盗難届や紛失届を出さずに再発行の手続きをすることができます。再発行用の印刷 ID カードを選び、そこに記載されている SN を登録することで印刷 ID カードの更新が完了します。わざわざ自治体に出向く必要はありません。

2.4. 身分証の発行

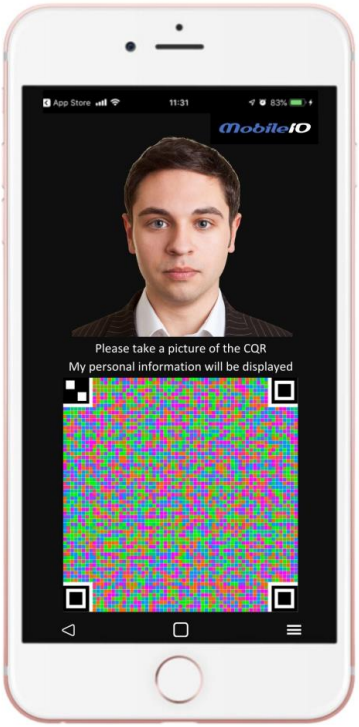
自治体管理部個人情報データベースの登録が完了すると、身分証を発行できるようになります。身分証には MobileID による電子 ID カードと印刷された ID カードの 2 種類があります。スマートフォンを持っている方は電子 ID カードを利用できるようになり、スマートフォンをお持ちでない方には自治体から印刷 ID カードが発行され、受け取ることができます。いずれの ID カードも 8 色のマトリックス型のコード

Color Quick Reference(CQR）※と顔写真及び SN（Serial number、印刷カードのみ）で構成されています



印刷 ID カード（左：ラミネート加工、右：プラスチック）
8 色の 4 次元マトリックスコードが CQR（40mm x 40mm）

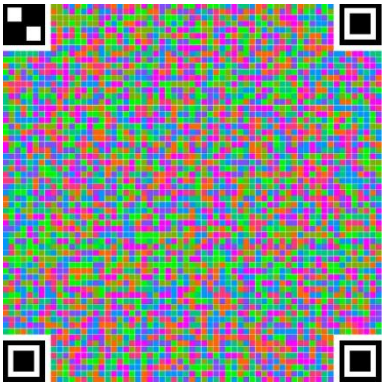
※Color Quick Reference(CQR）は当社が開発した 4 次元マトリックスの情報格納コード。



スマートフォンで ID カードを表示している MobileID 画面
この画面を **電子 ID カードまたは単に ID カード**という
8 色の 4 次元マトリックスコードが CQR

CQR とは

Color Quick Response（CQR）は、当社が開発した 4 次元マトリックス型コードで、高速な読み取りと大容量の情報記憶に特化した情報格納コードです。CQR には暗号化された個人情報データベースの自治体管理部個人情報データベース及びメタデータが書かれています。MobileID はこの情報を用いて個人認証や投票及び電子取引などをオンライン・オフライン問わずに安全にサービスできる仕組みになっています



当社が開発した情報格納コード CQR(Color Quick Response)
詳細は MobileID Technical Notes を参照してください。

複製の防止

CQR コードには隠蔽署名が施されており、これにより印刷 ID カードの複製が困難になります。隠蔽された署名はコピーによって変化するので、CQR がコピーされた場合にはその変化を検知することができるため、複製を見破ることが可能です。さらに、MobileID の顔写真に隠蔽署名を追加することで顔写真の偽造を防ぎ、セキュリティをさらに強化することが可能です。

■CQR に関する特許 No6989859、No7748756、No745799、特願 2023-196632
■CQR の性能や仕組み等は別紙 MobileID Technical Notes を参照してください。

契約時に決定すべき事項　■印刷 ID カードの発行枚数

印刷 ID カードは損傷が大きいと読み取りができなくなります。損傷する度に自治体に行き再発行をするのは運用上望ましくなく、普及の妨げになると言えます。これを回避するために、印刷 ID カードを複数枚発行・運用することが考えられます。印刷 ID カードにはユニークな SN が記載されています。同一人物の印刷 ID カードが複数枚発行されていても、ひとつの SN を有効化し、それを無効化してから次の ID カードを運用できるようにすることで、実質的に 1 枚の ID カードとして運用できます。むしろ複数枚あることで、第三者はどれが有効なのか分からず、セキュリティ

性が高まるとも考えられます。複数枚発行するかどうかは運用者の判断に委ねられるべきです。契約時に複数枚発行の是非や最大発行枚数などを決めて頂きます。

2.5. 個人情報の更新

自治体管理部個人情報データベースの変更が必要な場合には自治体に出向いて手続きを以下の手順で行うことができます

■ 自治体管理部個人情報データベースの全項目の更新

① 自治体に出向き更新したい項目を申し出ます。
② 更新に必要な情報を提出し、ID カードで本人確認を行います。
③ 本人確認が完了すると、情報の更新作業を行います
④ 完了すると、スマートフォンがない方には新しい印刷 ID カードが発行されるので、古い印刷 ID カードを差し出し、新しい ID カードを受け取ってください。なお、電子 ID カードは自動更新されます。

一方、人の顔は時間とともに変化するため、登録後数年経過すると CQR に保存されている顔認証の正確度が低下する可能性があります。顔の変化により、本人であっても他人と誤認されるリスクが高くなります。本人確認の顔認証精度が「一定レベル以下になったかな？」と判断されたら顔情報を更新してください。**オンラインの時**に本人確認をしてから顔情報の更新をする機能が実装されています。認証の精度を維持するために顔情報の定期的な更新を推奨します。

2.6. 個人情報データベースの暗号化

個人情報データベースは下記の通り暗号化してサーバーに保存されています。サーバーから CQR にダウンロードする際も暗号化されたままです。そのため、CQR には暗号化された状態で自治体管理部個人情報データベースだけが保存されます。

(1) 自治体管理部個人情報データベースの暗号化

① 自治体管理部個人情報データベースを AES 暗号化（公開鍵を除く）
② ①を公開暗号化方式の秘密鍵で暗号化（RSA 暗号）
③ ②の公開鍵を AES 暗号化し、個人情報データベースに保存する

(2) 自己管理部個人情報データベースの暗号化

自己管理部個人情報データベースを AES 暗号化

※AES 暗号化鍵はそれぞれ異なります。

2.6.1.AES（256）（Advanced Encryption Standard）暗号

データを強力に暗号化するために使用される対称鍵暗号の一種です。アメリカ国立標準技術研究所（NIST）によって 1997 年に開発され、2001 年に標準化されました。AES は非常に高い安全性とパフォーマンスを備えていると言われています。

暗号化の例

平文　吾輩は猫である

AES(256)暗号　JoRn8z1jwVIPYZfJbmHG+vOTZmLcPTBOmUtGNAOTBDQ=

256 は鍵長。暗号文は鍵長に比例して長くなる。

2.6.2.RSA(1,024)（Rivest–Shamir–Adleman）暗号

RSA（Rivest-Shamir-Adleman）は、広く使用されている公開鍵暗号方式の一つです。1977 年にロン・リベスト、アディ・シャミール、レナード・アデルマンによって提案されました。

主な特徴

- 公開鍵と秘密鍵: RSA は、2 つの異なる鍵を使用します。公開鍵は誰でもアクセスでき、一般的に秘密鍵は所有者だけが持つものです。
- 数学的基盤: RSA は、大きな素数の積を利用した数学的な原理に基づいています。素因数分解が難しいため、高いセキュリティを提供します。
- デジタル署名: RSA はデジタル署名にも使われ、データの真正性と整合性を確認できます。

暗号化の例

平文　吾輩は猫である

RSA(26)暗号　61908299

素数 p=8009、　素数 q=8011、　公開鍵=64160099　秘密鍵=4072513

上記で RSA(26)の 26 は鍵長の意味であり、公開鍵 64160099 は鍵、鍵の大きさは素数 p と q によって決まる。個人情報データベースでは安全性を高めるためにより大きな素数 p と q を用いて、1024bits 相当の鍵長とする。参考までに、1024bits（2^{1024}）は 10 進数で表現すれば 308 桁になる。

下記が 2 の 1024 乗である（本システムでの鍵候補の数)。改ざんするためにはこの数の中から唯一の正しい鍵を見つけなければならい

179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416

662249284743063947412437776789342486548527630221960124609411945308295208500576883815068234246288147391311054082723716335051068458629823994724593847971630483535632962422413721 6

■暗号化の詳細は FAQ10 及び別紙 MobileID Technical Notes を参照

3 本人確認

本人確認とは ID カードを用いて自分の身分を証明する機能です。MobileID の主要機能でありオンライン・オフラインに関わらず利用可能です。

3.1. 電子 ID カード@オンライン

サーバーに保存されている個人情報と電子 ID カードを照合することによって本人確認を行います。「A は Z が何者であるかを知らず Z の確かな個人情報を知りたい」という背景での具体的な手順を以下に示します。

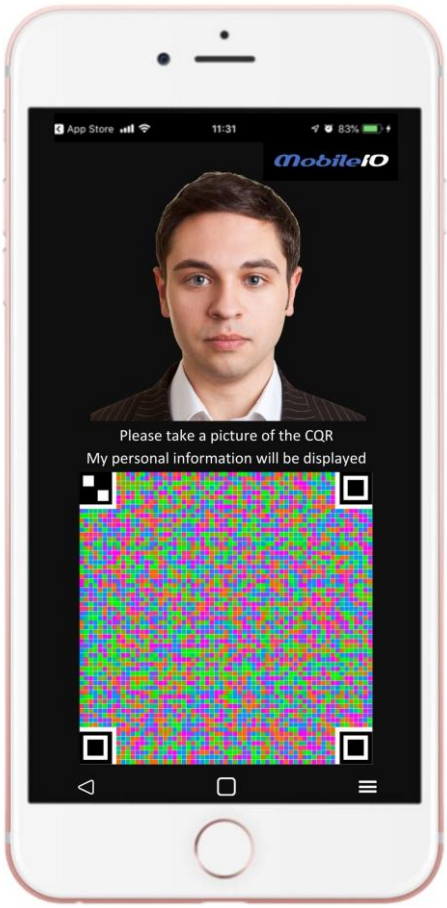
(1) ログイン認証(第 1 段階認証)

- Z が、電子 ID カード（自身の公的個人情報（自治体管理部個人情報データベース）が記載されているスマホの画面）を A に提示するために、MobileID アプリケーションを起動します。
- ログインするためにアカウントと PinCode の入力します。
- 入力されたアカウントと PinCode はサーバーに送信され、自治体管理部個人情報データベースに登録されたアカウント及び PinCode と照合され本人確認が行われます。アカウント及び PinCode は、Z 本人のみが知っている情報です。

MobileID のログイン画面（Z）

(2) 開示情報の設定

- ログイン後、Z が A に個人情報を提示するにあたり、「氏名、生年月日、国籍、現住所、出生地住所、滞在期間、出入国履歴、性別」から、提示したくない項目は非表示に設定できます。この設定は CQR で表示されるため設定内容を目視で読み取ることはできません。
- 表示設定が完了すると、スマートフォンに自身の電子 ID カード（顔写真と CQR コード）が表示されるので、Z はそれを A に提示します。



非確認者（Z）の電子 ID カード

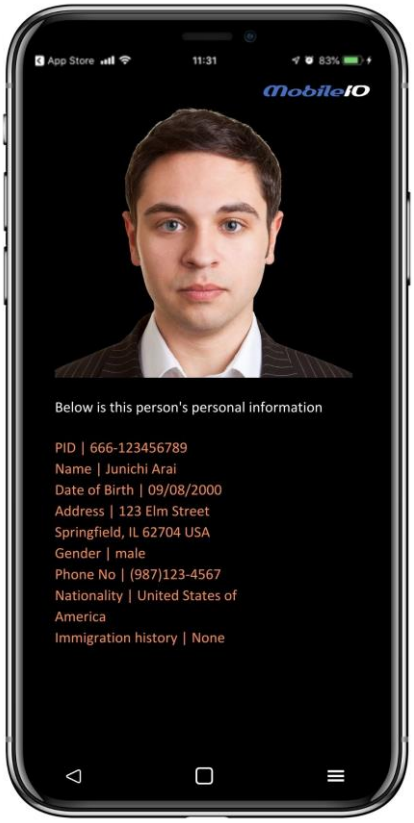
(3) 顔認証（第 2 段階認証）

- A は MobileID アプリケーションを使用して、Z の電子 ID カードを読み取ります。読み込まれた情報はサーバーに送信され、自治体管理部個人情報データベースに登録されている Z の顔情報と照合されます。
- A のスマートフォンからサーバーに送信された情報には、Z の電子 ID カードの CQR コードに Z の PID（個人識別子）が含まれており、この PID をもとに Z の自治体管理部個人情報と照合が行われます

(4) SMS（Short Message Service）（第 3 段階認証）

- 顔認証に合格すれば、Z のスマホに 4 桁の数値の SMS が送られます
- その数値を A のスマホアプリに入力します
- 数値が正しければ、CQR に記録されていた情報を A が読み取れる形式（文字）で A のスマホアプリに開示されます

以上の 3 つの照合ステップを経て Z が何者であるかを A が知ることができ、A の個人情報を見ることができます。



確認者（A）のスマホ画面
表示されているのは相手（Z）の個人情報

3.2. 電子 ID カード@オフライン

オフラインの場合は、スマホに保存された CQR（※）と電子 ID カードの情報を照合することで、本人確認を行います。以下の手順は、「A は Z が誰か分からないが、Z の正確な個人情報を知りたい」という状況に基づいています。具体的な手順は以下の通りです。

※CQR
CQR には自治体管理部個人情報データと電話番号及び IMEI が書かれている。

(1) ログイン認証（第 1 段階認証）

- Z は自分の電子 ID カード（自身の公的個人情報（自治体管理部個人情報データベース））を A に見せるために、MobileID アプリを起動します。
- ログイン時に、アカウント及び 6 桁の PinCode を入力するよう求められます。
- 入力されたアカウント及び PinCode が CQR と照合され、正しいかどうかが確認されます。アカウント及び PinCode は本人のみが知っている情報です。

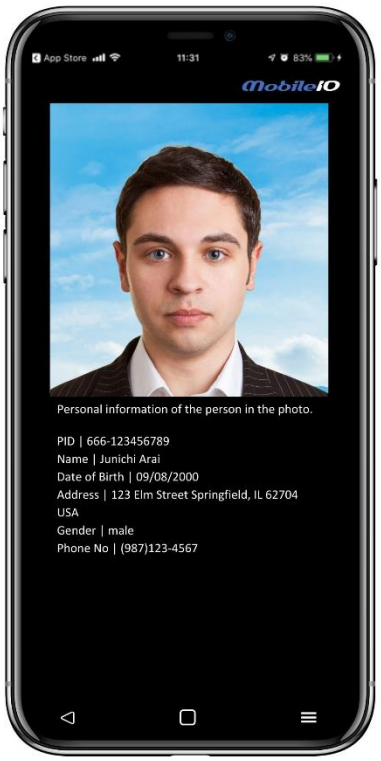
(2) 登録電話確認（第 2 段階認証）と開示情報の設定

- CQR に保存された IMEI と実機の IMEI が一致すれば、次のステップに進みます。
- この先、Z は自らの個人情報を A に伝えることになるため、「氏名、生年月日、国籍、現住所、出生地住所、滞在期間、出入国履歴、性別」の中で伝えたくない項目については表示 OFF にすることができます。表示設定が終了すると、スマホに電子 ID カードが表示されるので、スマホを A にかざします

Z の電子 ID カード

(3) 顔認証（第 3 段階認証）と情報開示

A は MobileID アプリを使い、Z の顔を撮影して、Z の電子 ID カードの CQR コードを読み取ります。顔の照合処理が開始され、認証されれば、Z の個人情報が A のスマホに表示されます。今撮影した Z の顔も表示されます。



A のスマホ画面：
Z の個人情報と
顔写真が表示されています

以上の 3 ステップを経て本人確認が完了します。

3.3. 印刷 ID カード

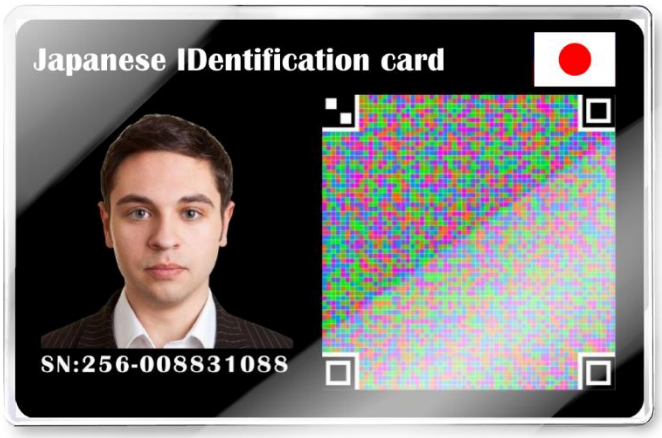
スマートフォンを持っていない方にも対応できるよう、MobileID には ID カードリーダー機能と、印刷 ID カード（ラミネート加工の紙製またはプラスチック製）の生成機能が実装されています。印刷 ID カードには、顔写真、CQR コード、および SN が記載されています。

印刷 ID カードでの本人確認手順

本人かどうかの判定は

① アカウント及び PinCode 認証
② 署名確認
③ 顔認証

の 3 ステップを経て行います。いずれの認証も CQR コード内の個人情報と照合されます。



Z の ID カード

① Z は印刷 ID カードを A に提示する
② A はその ID カードの CQR を MobileID で撮影する
③ **（認証 1）**アカウント及び PinCode の入力が求められるので、Z にアカウント及び PinCode を入力してもらいます
④ **（認証 2）**認証が通過するとログインできるので、署名が正しいか否かが自動判定され、
⑤ **（認証 3）**署名が正しい場合は、顔認証のために Z の顔を撮影して顔認証処理が始まります。顔認証が通れば Z の本人確認が完了します
⑥ 認証できたら、Z の個人情報の表示する項目の ON/OFF を Z が設定します。「氏名、生年月日、国籍、現住所、出生地住所、滞在期間、出入国履歴、性別」の中で伝えたくない項目については表示 OFF にすることができます。設定には PinCode 入力が必要なので Z だけが設定できます。

⑦ 設定が終了すると、Z の個人情報と今撮影した Z の顔写真が A のスマホに表示される。

A のスマホ画面：Z の個人情報と顔写真が表示されています

4 投票

MobileID には ID カードで管理された投票機能が実装されています。選挙をデジタル化することで、選挙プロセスを大幅に改善できます。選挙が行われる際には、立候補者登録アプリ（納品物）によって、立候補者の顔写真、氏名、年齢、投票情報などを入力して立候補者データベースを作成します。作成と同時に投票状況を保存するための空の投票箱データベースが生成されます。

投票は MobileID アプリを使って行うことができ、スマートフォンを持っていない人でも印刷 ID カードで、周囲にスマートフォンがあれば投票が可能です。投票ができるのは「投票日」の投票開始時刻から投票締め切り時刻までとします。

オフライン環境で投票する場合は、本人認証などのプロセスは CQR コード内の個人情報と照合され、投票データは暗号化された状態でスマートフォンに保存されます。オンラインになると投票データがアップロードされますが、オンラインになった時刻が投票締め切り時間を過ぎるとアップロードされず、無効票になります。

※オフラインでの投票の是非及びアップロード締め切り時間を何時にするかは契約者の判断に委ねられます。是非及び締め切り時間は契約時に決定して頂きます。

機能

(1) 立候補者データベースの生成
立候補者データベースとは、候補者名、立候補者番号、顔写真、年齢、経歴、公約や主張及び選挙期間や投票日、投票所番号などのメタデータが格納された SQL データベース。ウエブサイトで閲覧できます。

(2) 投票箱データベースの生成
立候補者の獲得票や投票時間、投票所番号などのメタデータが AES 暗号化された SQL データベース。本データベースは専用のアプリケーション以外は開くことができません。

(3) 投票
MobileID にログイン後、PID を元に 1 回目の投票かどうかを判定します　(2 回以上の投票はできません)

「投票」が有効であると判断されると当該立候補者に無記名投票という形で 1 票加算されます。

集計できる項目
票の保存と同時に投票時刻や投票所番号及び年齢や性別なども保存できます。何を保存するかは運用者の判断に委ねられます。契約時にご指定ください。

(4) 集計

選挙集計アプリ（納品物）を起動する。選挙期間中に本アプリが起動された場合は投票率が表示されます。

選挙集計アプリは、投票締め切り後であれば投票箱データベースにアクセスして、結果（投票結果・投票率・年齢別投票率など）を瞬時に表示します。

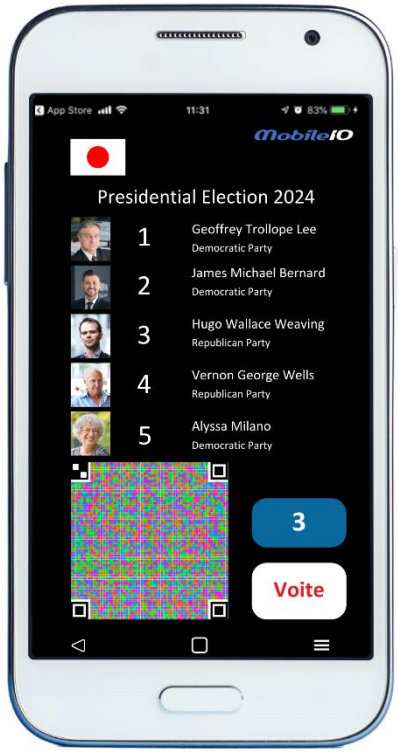
選挙集計アプリの集計結果には MobileID 投票機能を使わずに投票したデータは含まれていません。

投票全体を集計できるようにするためには、「従来の投票所に MobileID 登録システムを設置して投票に来た人達に個人情報を登録してもらい、投票用のスマートフォンを渡して投票してもらう」その後、印刷 ID カードを私という方策がベストと考えられます。

個人情報の登録を拒む場合には「顔写真を撮影してから MobileID で投票してもらう」という方法があります。顔の撮影は重複投票を見破るためです。すなわち、既存顔写真に該当者（投票者）がいるかどうかを調べ、既存に顔写真があれば投票できないようにします（重複投票確認機能は MobileID 製品に含まれています）。いずれにしても MobileID で投票してもらう手立てが必要です。

MobileID カードでの投票

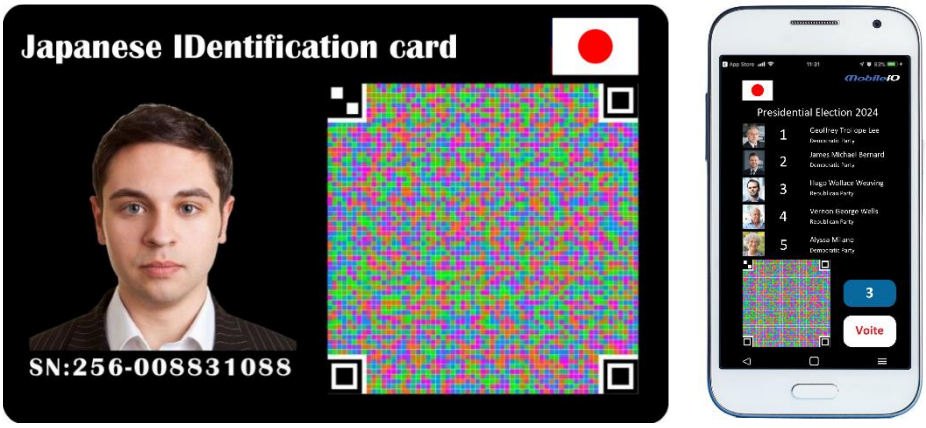
① MobileID にログインする
② 選挙ボタンをタップ （➡未投票か投票済か、あるいは投票権の有無などがチェックされる）
③ 本人確認のために自らの顔を撮影して、顔認証を行う
④ 認証されれば、候補者の中から 1 名を選択
⑤ 投票ボタンをタップ
⑥ 投票情報がサーバーにアップロードされる



印刷 ID カードでの投票

印刷 ID カードの場合には第 3 者のスマートフォンを使用して投票します。

① 印刷 ID カードの所有者が第 3 者のスマートフォンを借りて MobileID にログインする
② 印刷 ID カードによる選挙ボタンをタップ
③ 印刷 ID カードの CQR を撮影する　（➡未投票か投票済か、あるいは投票権の有無などがチェックされる）
④ 本人確認のために印刷 ID カードの所有者の顔を撮影して、顔認証が起動される
⑤ 認証されれば、候補者の中から 1 名を選択
⑥ 投票ボタンをタップ
⑦ 投票情報がサーバーにアップロードされる



印刷 ID カードの場合は第 3 者のスマホを利用して投票します

本システムでの投票のメリット

① 投票前にはスマホ画面には補者一覧が表示されます。立候補に関連する情報をリンク設定することも可能です
② スマートフォンがあれば、どこでも簡単に投票が可能、投票率の向上が見込めます
③ 投票ボタンを押すと同時に本人確認が行われるため、他人がなりすまして投票することはできません。
④ 印刷 ID カードしかない場合でも、他の人のスマートフォンを利用して投票することができます
⑤ 投票できるのは投票日だけ、有資格者か否か、重複投票か否か、本人か否かなどを判定するための人手が不要になります。
⑥ スマートフォンを持っている未投票の人に対して投票の督促メッセージの送信ができます。
⑦ 集計がデジタル化されるため集計に関する違法行為や間違いを排除でき、早く正確である
⑧ 投票管理全般的に人手コストを削減できる

本システムでの投票のデメリット

MobileID 投票機能を使わずに投票したデータは別の集計が必要になり、データベースが 2 元化してしまうので、管理が大変になりコスト削減効果が減少します。

5 CQR 決済

MobileID を利用した決済機能とは、MobileID の CQR を使った決済なので言わば CQR コード決済と言えます。MobileID では CQR コードによって、オンライン・オフラインを問わず決済が利用できるように開発しました。オフラインで得た電子マネーをオンライン確認することなく使うことができます。

MobileID では、複数の銀行口座を登録することが可能ですが、指定した口座から MobileID にチャージすることで購入決済を行うことができます。また、MobileID にチャージした金額を銀行口座に振り込むことも可能です。

例えば、既存の店舗が CQR 決済を使いたい時は、MobileID をスマートフォンにインストールするだけで店舗がオフライン地域にあっても CQR コード決済ができるようになります。取引には銀行登録さえも不要ですが、チャージ金を現金化するためには銀行登録が必要になります。以下の例では Z（売主）が既存店舗に該当します、利用利用方法について参考にしてください。

以上のように、MobileID は便利で柔軟な利用手段を提供しているので様々な活用方法が考えられます。

注意

CQR コード決済機能を使うためには銀行側システムの API が公開されていて当社がインテグレーション開発できる環境が必要です。

CQR コードの記載内容

CQR コード決済の CQR に書かれている取引情報は下記の通りです。

A の PID	Z の PID	商品名	価格	数量	CQR 件名	Time Stamp	取引番号	日時	公開鍵

基本的な CQR コード決済の CQR に書かれている情報（RSA 暗号）

改ざんや偽造防止のための暗号化と履歴及び署名

取引情報の改ざんや偽造対策として 2 重の暗号化と隠蔽署名をしています。具体的には改ざんを防ぐために、決済内容（図の青色部分）は AES 暗号化し、それを秘密鍵で暗号化し、解読のための公開鍵（図の緑色部分）を付加して CQR に格納しています。RSA 暗号なので公開鍵を使って青色部分を解読することはできますが、暗号化できないために改ざんして保存することはできません。解読ができるとい

っても、それは AES 暗号化されているので、さらに解読しなければ平文を得ることはできません。

一方、RAS 暗号の性質を利用して撮影した CQR を保存すれば、**自分では修正できない履歴**として扱うことができるということになります。

また、CQR の偽造防止のために CQR を作成したスマートフォンを特定できるように AES 暗号化された署名を CQR コードに隠蔽署名します。

以上により CQR コード決済は高度なセキュリティを保証しています。

CQR コードの項目の詳細

① **A の PID：**A の Personal ID
② **Z の PID：**Z の Personal ID
③ **商品名：**商品名（取引前に売主が決める）
④ **価格：**価格（取引前に売主が決める）
⑤ **数量：**数量（取引前に売主が決める）
⑥ **CQR 件名:** CQR の発行目的（意味）を示し、購入意思や支払、領収書、キャンセルなどの役割が MobileID によって自動的に明記されます。
⑦ **TimeStamp：**CQR 決済コードには有効時間があります（通常、CQR の発行時刻から 60 秒)。TimeStamp は有効時間の最後の時刻です。最終時刻を過ぎると、その CQR は無効になり、取引が中断します（タイムオーバー)。**従って、規定時間内に CQR を撮影して取引を進める必要があります。**撮影ができない又はしない場合は、タイムオーバーで取引が中断されたらキャンセル手続きが必要になります。
オンラインの時に取引が中断した場合は自動的にキャンセル処理されます。
オフラインの時に取引が中断したら、タイムオーバーになった方（CQR を撮影すべき人、通常は売主）が「キャンセル CQR」を発行し、それを相手方（撮影されるべき CQR を発行した人）が撮影するという流れです。
キャンセル CQR の発行はタイムオーバー前でも発行可能です。
⑧ **取引番号：**（重複処理の防止）1 度読み込んだ CQR を再び読み込んだ場合に無効にするためのユニークな番号
⑨ **日時：**CQR 発行日時
⑩ **A の公開鍵**：暗号化された文字列（青色部分）の公開鍵。暗号化した人（この場合は A）だけが発行できる。また、発行後に秘密鍵を消去してセキュリティレベルを向上させています。

決済の準備（購入者）

(1) CQR コード決済で商品を買うには、まず口座からスマホにチャージ（資金移動）しておく必要があります。

(2) チャージ金額を超える決済はできないのでそれを考慮してチャージしてください。チャージ額が不足していると、オンラインの場合ならその場で追加チャージして取引を続けることが可能ですが、オフラインの場合はチャージ不足によって決済が中断されます。

(3) チャージの手順

① MobileID アプリ下部の［ウォレット］をタップ
② MobileID 残高表示部の［内訳・送金］をタップ
③ MobileID マネー欄にある［送金］をタップ
④ 登録済み口座が複数ある場合、希望の口座を選択
⑤ 送金したい金額と日時を入力し、［送金］をタップ
⑥ 手続きが完了すると即時処理か振り込み予定日が表示される

画面は⑤の画面

CQR 決済は

① 売主（Z）が、商品説明や価格及び売主の PID が書かれた CQR を表示
② 買主（A）が、CQR を撮影し、購入意思を示す CQR をスマホに表示
③ 売主（Z）が、それを撮影して決済を実行、領収書を意味する CQR が表示される
④ 買主（A）が、その領収書 CQR を撮影・保存

という手順で行われます。

CQR 決済で利用される CQR に記載される情報

A の PID	Z の PID	商品名	価格	数量	CQR 件名	Time Stamp	取引番号	日時	A の公開鍵

基本的な決済内容：CQR には公開暗号化方式で格納される。

(1) **暗号化と履歴**：決済内容（図の青色部分）は AES 暗号化し、さらに秘密鍵で RSA 暗号化し、公開鍵（図の緑色部分）を付加して CQR に格納しています。RSA 暗号なので CQR を撮影した側では公開鍵を使って CQR の内容を読み取ることはできますが、改ざんして保存する（暗号化）ことはできません。この性質を利用して、**撮影した CQR を履歴として保存すれば、自分では修正でいない取引履歴 CQR として扱うことができる**ということになります。

(2) **署名**: 署名値は IMEI で、CQR コードに署名されます。この結果、改ざんや偽造をするには AES 及び RAS そして署名の解析が必要になります。

履歴項目の詳細

① **A の PID**：A の Personal ID
② **Z の PID**：Z の Personal ID
③ **商品名**：商品名（売主が決める）
④ **価格**：価格（売主が決める）
⑤ **数量**：数量（売主が決める）
⑥ **CQR 件名**: CQR に含まれる文字列の発行目的（意味）を示し、購入意思や支払、領収書、キャンセルなどの役割が明記されます。
⑦ **TimeStamp**：これは CQR が有効な最終時刻を示します。最終時刻（通常、CQR の発行時刻から 60 秒後）を過ぎると、その CQR(取引)は無効になります（タイムオーバー)。従って、規定時間内にスキャンして取引を進める必要があります。**支払いを受け取る撮影（支払 CQR の撮影。撮影は代金をもらう行為）**ができない又はしない場合は、取引が中断されキャンセル手続きが必要になります。
オフライン取引の時のキャンセル手続きは、CQR の撮影タイムオーバーまたは止めたくなった方（通常は売主）が「キャンセル CQR」を発行し、それを相手方（タイムオーバーになった CQR を発行した人、通常は買主）がスキャンするという流れです。キャンセル CQR はタイムオーバー前でも発行可能です。
⑧ **取引番号**： 1 度処理 CQR を再び読み込んだ場合に無効にするためのユニークな番号
⑨ **日時**：CQR 発行日時
⑩ **A or Z の公開鍵**：暗号化された文字列（青色部分）を解読するための公開鍵。秘密鍵で暗号化した人（A or Z）が発行できる。また、取引終了後に秘密鍵を消去してセキュリティレベルを向上させています。秘密鍵はメンテナンス等に合わせて定期的に更新することが望ましい。

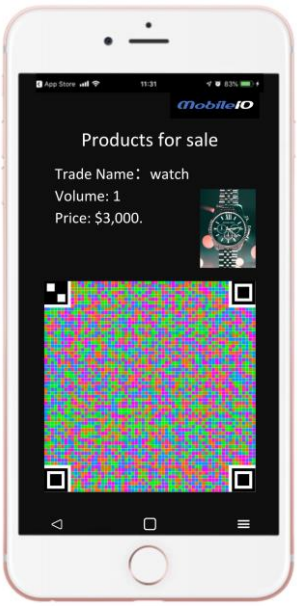
以下に各決済手順を説明します。

5.1. オンライン対面決済

オンライン環境下では、サーバーに保存されている自治体管理部個人情報データベースのチャージと照合を行い、決済を進めます。**A が購入者、Z が販売者**として決済を行います。すべての操作は MobileID を使用します。
なお、決済前に A 及び Z はそれぞれ個人認証を経てログインしているものとします。

(1) 決済の開始

- **CQR の提示**: Z は、商品の価格情報や自分の PID が書かれた CQR を A に提示し、A がスマホで読み取れるようにします。
- **購入意思の表示**: A が Z の CQR をスキャンし、取引内容に問題が無ければ支払いを示す取引 CQR を提示します(2)
  チャージ不足時の対応: A のサーバー上のチャージが不足している場合、A に確認を取った上で銀行からチャージできる場合は取引を継続できます。

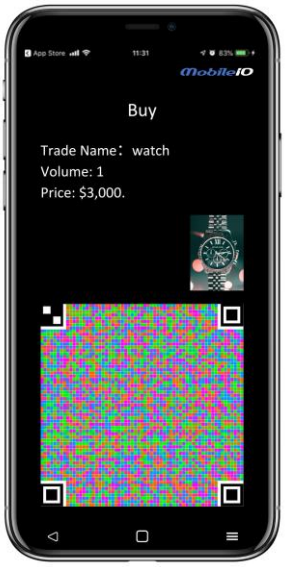


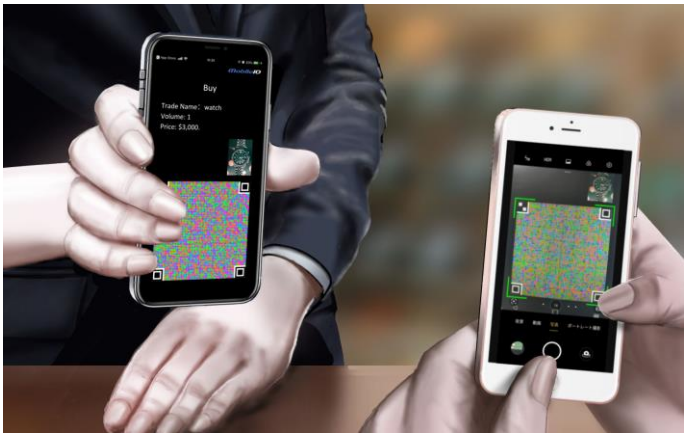
A の PID	Z の PID	商品名	価格	数量	件名 商品	Time Stamp	取引番号	日時	Z の 公開鍵

右：Z のスマホ（商品説明 CQR）
左：A が Z のスマホを撮影している様子

(2) A が支払いを意味する購入 CQR を表示

- **Z が A の購入 CQR をスキャンすることで決済が成立します。**この時、Z のサーバー上のチャージが増加し、同時に A のサーバー上のチャージが減少します。

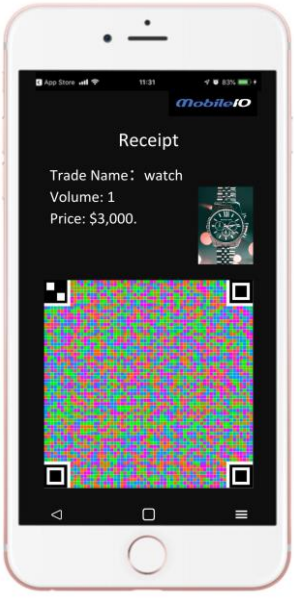




A の PID	Z の PID	商品名	価格	数量	件名支払	Time Stamp	取引番号	日時	A の公開鍵

左：A のスマホ（支払い CQR）
右：Z が A のスマホを撮影している様子

(3) **取引完了と領収書の表示:** 決済が成完了すると、Z のスマホには、入金を示す取引 CQR（領収書）が表示されます。Z は A にかざして撮影してもらいます。タイムオーバーはありませんが、速やかに撮影してください。撮影後に、システムから A のスマホに完了を示すメッセージが送れてきます。



右：Z のスマホ（領収 CQR）
左：Z のスマホを A が撮影している様子

A の PID	Z の PID	商品名	価格	数量	件名領収	Time Stamp	取引番号	日時	Z の公開鍵

(4) 取引完了

以上で決済が終了し、物品の受け渡しが行われます。オンライン環境下では、決済に伴いサーバー上のチャージ及びスアホのチャージが自動的に更新されます。

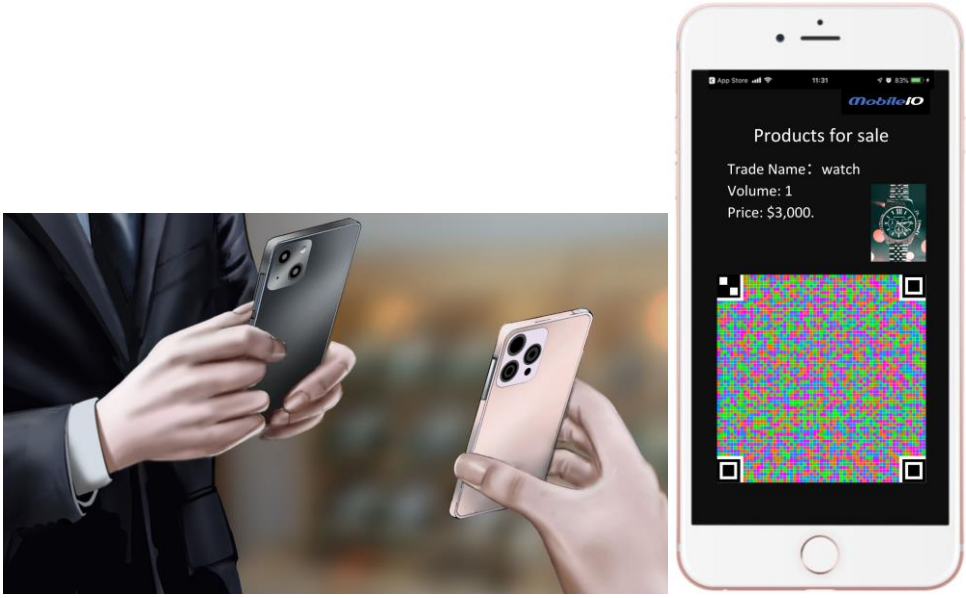
5.2. オフライン対面決済

オフライン対面決済は、スマホに保存されている CQR のチャージと照合することで進行します。

以下に、A が購入者、Z が販売者として、オフラインでの決済フローを説明します。すべての操作は MobileID を使用します。

(1) 決済の開始

- **本人確認(省略可)**： A と Z は互いに本人確認を行い、盗まれたスマホが使用されていないことを確認します。
- **商品 CQR の提示**: Z は、商品の価格や自身の PID が記載された販売条 CQR を A に提示し、A がスマホで読み取れるようにします。



A が Z のスマホを撮影している様子

A の PID	Z の PID	商品名	価格	数量	件名 商品	Time Stamp	取引番号	日時	Z の公開鍵

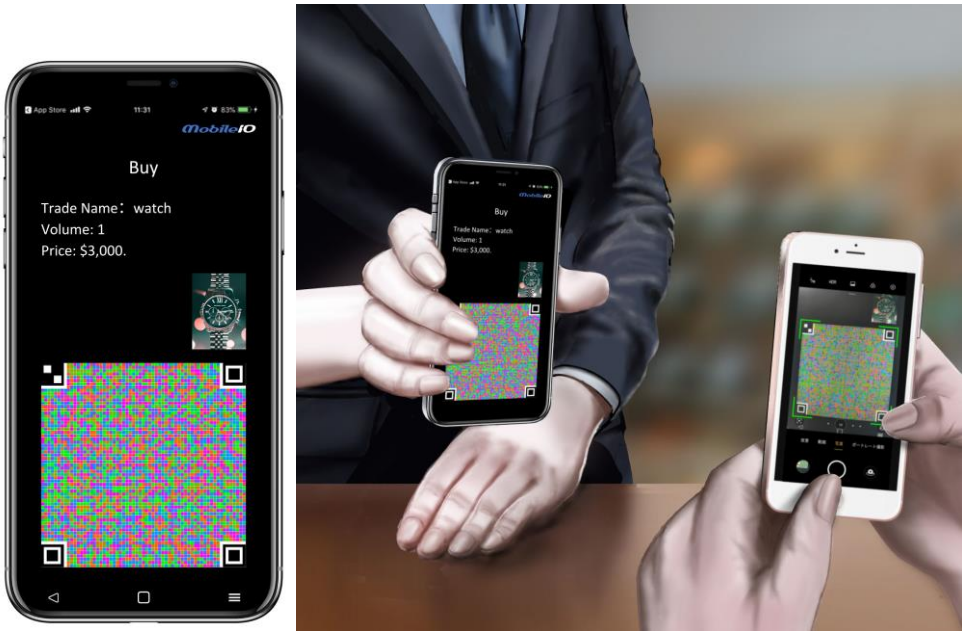
Z の商品 CQR の記載内容

(2) A の支払と履歴の保存

- **購入意思の表示**: A が Z の CQR をスキャンし、価格や数量などを確認の上、支払いを示す CQR を表示します。CQR を表示すると同時に、A のチャージから代金分の料金が減額され、支払いが完了します。

なお、撮影した CQR は商品の販売条件が記載されており、A のスマホに保存されます。

- **チャージ不足時の対応**: CQR のチャージが不足している場合、取引はチャージ減額前に中断されます



左：A のスマホ（購入意思、支払いと同等）
右：Z が A スマホを撮影している風景

A の PID	Z の PID	商品名	価格	数量	件名 支払	Time Stamp	取引番号	日時	A の 公開鍵

支払 CQR の記載内容（CQR 件名＝支払）

注意

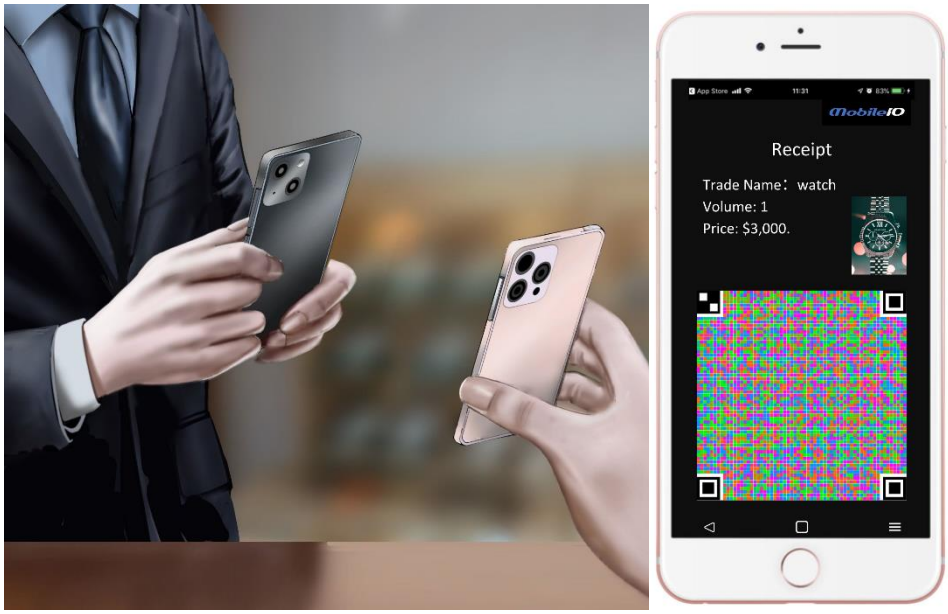
A が支払いをしただけで、この段階では、Z にはまだ資金が移動していません。Z が A の CQR を撮影することで資金が移動します。A のスマートフォンを撮影せず、Z がここで取引を中止したい場合、あるいはタイムオーバーになってしまった時は資金移動してないので、Z が**キャンセル CQR** を表示してキャンセル処理することが必要です。キャンセル CQR を A が撮影することによって、A が支払い済の代金がチャージに戻ります。

(3) Z の売上と入金

- **取引の完了: Z が A のスマホに表示された支払 CQR をスキャンすると、決済が成立します。**このスキャンによって入金され、Z のスマホのチャージに代金分が加算されます。領収を意味する CQR が表示される。
- **領収書の表示**: Z のスマホに領収を意味する領収 CQR が表示される。

- A が Z のスマホの領収書 CQR をスキャンして終了です。スキャンしなくても取引は成立していますが、Z に「支払いを受け取っていない」と言われないよう、スキャンを推奨します。スキャンされた領収書 CQR は A のスマホに保存されます。

- タイムオーバーはありませんが、再表示はできないので消す前に撮影してください



左：A が Z の領収書 CQR を撮影している様子　右：Z のスマホ

A の PID	Z の PID	商品名	価格	数量	件名	Time Stamp	取引番号	日時	Z の公開鍵

領収書 CQR の記載内容（CQR 件名＝領収書）

(4) 決済の終了と物品の受け渡し

- 決済が完了しました。物品の受け渡しを行なってください。

5.3. 非対面決済

非対面決済とは、ネットショップでの買い物やネットワークを通じて行われる CQR 決済のことを指します。通常はクレジットカードが使われますが、CQR を利用することで、顔認証による本人確認が追加されるため、より安全性が高まります。CQR コード決済はせずに本人確認のためだけに CQR コードを利用することも可能です。CQR コードをどのように採用するかは契約者に委ねられます。詳細は契約時に決定して頂きます。

以下が MobileID の CQR を使った非対面決済のディフォルト機能です。

(1) **販売者：商品の情報入力**

ネットショップ販売を展開中または開始するとします。この時、ネットショップでの購入方法として CQR を選択できるようにしたいと考えた場合、商品名や価格及び PID などが記載された取引用の CQR を準備して表示すればいいのですが、そのための CQR を MobileID で作成します。なお、ネットショップ販売会社が非対面決済を利用するには代表者または担当者が個人情報データベースに登録する必要があります。

(2) **購入者：支払い方法から CQR 決済を選択**

① 購入者は CQR コード決済で支払いたいので、MobileID アプリを起動し、アカウント及び PinCode を入力してログインします。

② ネットショップで、購入者が買いたい商品の CQR をスマホで撮影します

③ MobileID アプリが、撮影した CQR から支払い金額や商品名などを確認し、確認画面をスマホに表示します。

(3) **顔認証と決済完了**

確認画面で購入 OK の場合、顔認証を行い、通過すれば支払いが実行されます。具体的な支払い実行とは、購入者のチャージから支払い先である Z の PID の個人情報データベースの銀行口座に代金が移動することを言います。代金移動はネットワークによって販社及び購入者に伝わり、購入者のスマホには完了通知として表示されます。

(4) 販売者は入金を確認したら商品を発送します。

(5) 商品を受け取って取引完了となります。

注意

インテグレーションはディフォルト以外に様々な方法があります。契約時に詳細を詰めてからの開発になります。

---

6 オプション機能

オプション機能とは MobileID のディフォルト機能に含まれず、料金が追加になる機能です。オプション機能は自己管理部個人情報データベースに格納される情報になるため、オンラインでは利用できず、オフラインでのサービスになります。

以下は一例です、ご希望に添える仕様を提案いたしますので、その機能は「なぜ欲しいのか、何を期待しているのか」をお教えください。ご要望に応えらえる提案をさせていただきます。

6.1. 運転免許証

身分証明として「私は免許証を持っていますよ」という自己防衛的なニーズの 1 例として運転免許証があります。

「所有資産」➡「運転免許証」ボタンをタップし、相手の CQR を MobileID で撮影すると、サーバーにある情報の確認を行い、免許証を持っている場合にはエビデンス資料と CQR が表示されます。また、自分自身の免許証を表示することもできます。

6.2. 所有自動車（州資産の追跡）

指定資産の所有登録を義務付けることができます。(※)。
本機能は所有を第 3 者に示す証明書です。し州資産を追及する側と所持す側で共通する資産証明が必要になります。それは資産の登録データベースとの連携を意味します。資産証明」メニューから「所有自動車」を選択し、相手の CQR を MobileID で撮影すると、サーバー上の情報を確認します。自動車を所有している場合、署名付ナンバープレートと共にエビデンス資料および CQR が表示され、複数台の所有がある場合はその台数分が表示されます。

※　州管理の資産についても同等機能を作成することができます。
※１　エビデンス資料は車検証または同等書類とします。
※２　法人所有車や借用中の車、その他正当な理由で非所有者となっている場合は、自動車データベースに運転を承認された人として登録する対応が必要です。

6.3. 所得証明書（納税証明書）

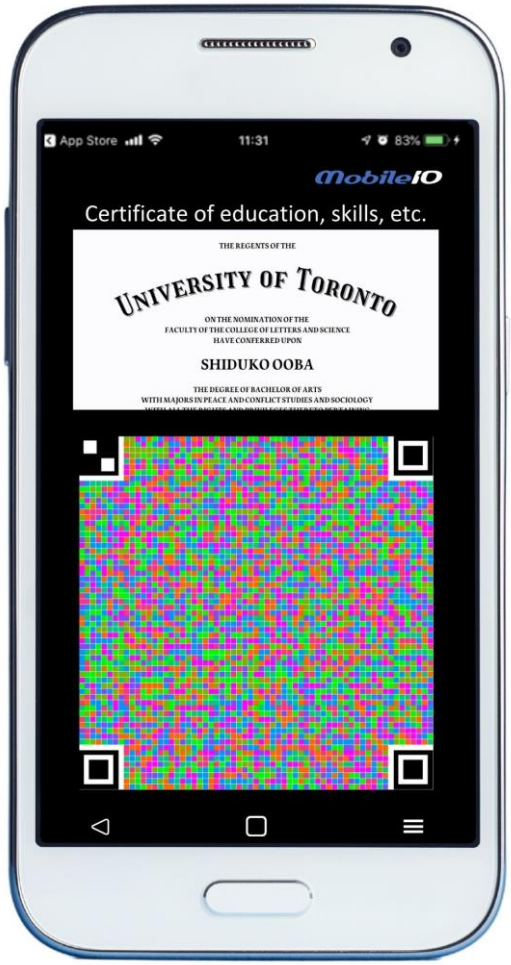
MobileID は所有している所得証明を登録することができます。「資産証明」➡「所得証明」メニューをタップし、相手の CQR を MobileID で撮影すると、サーバーにある情報の確認を行い、所得証明のエビデンス資料と CQR が表示されます。下記は源泉徴収書の例である。
なお、所得証明の登録は任意です。

※エビデンス資料は納税証明書または同等書類とします。

6.4. 教育・医療・文化・社会保障等証明書

MobileID は教育・医療・文化・社会保障等の社会的な再建を目指して雇用促進のための情報を登録することができます。雇用主が求める職歴履歴情報DBを構築して雇用促進を図ります。

※登録にはエビデンス資料が必要です。



7 メンテナンス・保守

7.1. メンテナンス

MobileID のメンテナンスは、システムの安定性とセキュリティを維持するために定期的に行われます。メンテナンス中は、一時的にサービスが利用できなくなる場合があります。
トラブル時のメンテナンスは基本的にネットワーク対応（リモートログインにて即時対応)。「リモートでは解決できない」と当社が判断した場合は現地出向対応とします。
費用は、設置後 1 年間は無償保証、2 年目からは有料保証

(1) **データベースのバックアップと保護**
データベースの定期バックアップを行い、万が一のデータ損失や不具合に備えます。また、暗号化などの手段でデータ保護の強化も行います。

(2) **システムの更新とパッチ適用**
OS や ID カード管理ソフトウェアの最新パッチやアップデートを適用し、システムを最新の状態に保つことでセキュリティの強化と不具合の修正を行います。

(3) **データ整合性のチェック**
データの正確さや整合性を確認し、不要なデータのクリーニングや重複の削除を行います。エラーや不正なデータがあれば修正します。

(4) **ハードウェアの点検と清掃**
カードリーダーや印刷機などのハードウェアの点検、清掃、消耗品（インク、カードストックなど）の補充を行い、正常に動作するか確認します。

(5) **セキュリティチェック**
認証方法やアクセス制御の見直し、セキュリティポリシーの適用を行い、不正アクセスの防止やシステムの安全性向上を図ります。

(6) **パフォーマンスの最適化**
データベースの最適化やメモリ管理を行い、システムの動作が遅くならないようにパフォーマンスの向上に努めます。

(7) **障害対応の準備とテスト**
予期せぬ障害が発生した際に迅速に対応できるよう、緊急対応手順の確認やテストを行います。

7.2. 保守

システム運用及び開発の移管　当社ではシステムの運営や拡張開発は運用者に委ねられるべきと考えています。導入後１年を最大として移管することを前提としています。移管サポート期間は最大１年

Web カメラ及びテンキーなどの設備サポート

物品交換にて対応

- お客様に起因する損傷は有償交換。
- 当社に起因する障害の場合は無償交換。但し、設置作業費は有償。

8 バックアップ

システムのバックアップとは、データやシステムの状態を定期的にコピーして保存することです。これにより、データの損失や障害が発生した場合に、元の状態に復元できるようにします。バックアップは、ハードディスクの故障や誤操作、サイバー攻撃などからシステムを保護するための重要な手段です。MobileID のデータは定期的にバックアップが取られ、万が一のデータ損失に備えます。バックアップデータは暗号化され、安全な場所に保管されます

(1) 完全バックアップ

- 定期的にシステム全体のデータをすべてバックアップします。例えば、毎週日曜日の夜間に完全バックアップを実行し、ID カードデータや設定情報、システムログなどすべてのデータが保存されます。
- **利点**：すべてのデータをまとめて保存するため、障害時に元の状態に完全に戻せます。
- **欠点**：データ容量が大きくなりやすく、バックアップに時間がかかる。

(2) 差分バックアップ

- 前回の完全バックアップ以降に変更があったデータのみを保存します。例えば、毎週日曜日の完全バックアップ後、平日は差分バックアップを行うことで、バックアップ時間を短縮できます。
- **利点**：バックアップ時間が短縮され、ストレージの節約が可能。
- **欠点**：復元には完全バックアップと差分バックアップが両方必要になる。

(3) 増分バックアップ

- 前回のバックアップ以降に変更があったデータのみを保存します。例えば、毎日夜間に増分バックアップを行い、迅速かつ効率的に更新データを保存します。
- **利点**：バックアップデータ量が最小限に抑えられ、ストレージの節約が大きい。
- **欠点**：復元に複数の増分バックアップが必要で、完全バックアップよりも復元が複雑になる。

(4) リアルタイムバックアップ

- 変更が発生したデータをリアルタイムで自動的にバックアップする仕組みです。ID カードシステムの場合、例えば、毎回カードが発行されたり更新されるたびに即座にバックアップが取られ、データの損失リスクを最小限に抑えます。

- **利点**：データ更新が即座にバックアップされるため、データ損失がほとんど発生しない。
- **欠点**：リアルタイムの監視とストレージ容量が必要になり、運用コストが高くなる場合がある。

(5) オフサイトバックアップ

- バックアップデータを別の場所（クラウドや別拠点のサーバーなど）に保存します。災害やシステム障害に備えて、地理的に分離した場所にデータを保管します。
- **利点**：自然災害や大規模なシステム障害の際にもデータを確保できる。
- **欠点**：通信やアクセスに時間がかかる場合がある。

(6) スナップショットバックアップ

- 現時点のシステム状態をスナップショットとして保存します。例えば、ID カードシステムの主要な設定やデータベースの状態を保存することで、システムが正常な状態に戻せます。
- **利点**：復元が迅速で、システムを以前の状態に即座に戻せる。
- **欠点**：容量を消費しやすく、変更が多い場合にはバックアップが膨大になる。

バックアップ戦略は、システム規模や重要性、利用頻度に応じて最適な方法を組み合わせて実施します。

9 動作確認スマートフォン

MoibleID の最新版での動作確認です。最新版は、Android 版は Google Play から、iOS 版は App Store からダウンロードしてください

Android のサポートは発売後 4 年間の機器まで、iPhone のサポートは発売後 5 年までです。本システムのサポート機器も同等させて頂きます。それ以前のスマートフォンも動作すると思われますが、サポートは対象になりません。

動作確認機器(2024/11/05)

OS	機種	詳細
Android	OPPO A1030P	Android12
	ALLDOCUBE	Android14
	Redmi Pad SE 8.7	Android14
iOS	iPhone12min	
	iPhone8	
	iPhone6	

10 FAQ

10.1. MobileID

Q1. MobileID とは何ですか？

「MobileID」はスマートフォンのアプリで、公的な身分証明書として機能します。オフラインの状態でも本人確認ができるため、投票や電子決済にも使えるようになっています。

Q2. MobileID の利点は何ですか？

MobileID はいわば CQR を使った電子証明書のひとつです。利点には、以下のようなものがあります。

なりすましの防止

電子証明書には公開鍵と所有者の身元情報が含まれており、MobileID がこれを保証しています。このため、証明書を持つ人やシステムが正当であることを証明でき、なりすましを防止できます。

データの改ざん防止

MobileID アプリケーションが扱う個人情報データベースは暗号化されたデータベースです。サーバー、通信、CQR いずれの状態においても盗聴や改ざんはできません。これにより、データの信頼性を保証しています。

セキュアな情報格納

電子証明書は CQR に格納されていますが、CQR への隠蔽署名によってデータの信頼性が確保しています。これにより、第三者による偽造や改ざんから保護され、安全な情報交換が可能です。

アクセス制御の強化

特定のユーザーやシステムにだけアクセスを許可するための手段としても活用できます。電子証明書を利用した認証により、システムやネットワークへのアクセスを適切に制御できます。

業務効率の向上

CQR 電子証明書を使った投票や電子取引がオンライン・オフライン問わず迅速に完了でき、物理的な書類のやり取りや作業を減らせます。

以上の利点から、MobileID はオンラインやオフラインでの安全な取引や情報保護のために幅広く使用できます。MobileID の導入により、従来の身分証明書のリスクを減らし、選挙や取引において安全かつ便利なデジタル社会を実現します。

Q3. ログイン対策はしていますか？

ログインには、本人しか知らない 7〜14 桁のアカウントと 6 桁の Pin コードが必要です。利用者ごとに異なるアカウントと Pin コードで不正ログインを防止します。アカウントや Pin コードは利用者本人だけが知っています。

ただし、7〜14 桁の数字や 6 桁の数字は総当たり攻撃で推測されるリスクがあるため、セキュリティ対策が施されています。アカウントまたは Pin コードを 5 回連続で間違えると、そのコードは無効になり、デバイスがロックされます。ロックされたデバイスで MobileID を再度使用するには、発行場所に行き、リセットとアカウント及び Pin コードの更新を行う必要があります。

Q4. MobileID はリバースエンジニアリング対策をしていますか？

はい、MobileID はリバースエンジニアリング（※）対策を強化しています。秘密鍵の隠蔽や顔認証アルゴリズム及び AES 暗号化アルゴリズムなどターゲットとなるところには細心の注意をしています。

※詳細は別紙「MobileID Technical Notes　Q9」を参照してください

Q5. 個人情報の更新手順は？

MobileID アプリにログインすることで、自己管理部の情報を更新できますが、エビデンス資料が必要になります。なお、自治体管理部の情報は発行所に行かないと更新できません。

Q6. MobileID の再発行の手順は？

MobileID はスマホアプリケーションです。発行や再発行ではなくダウンロードすることにより更新されます。何度でもダウンロード、インストールができますが、アカウント及びログイン PinCode が分からないとログインできません。

10.2. 個人情報データベース

Q7. 自治体管理部個人情報の登録手順を教えてください。

認定された担当者が MobileID アプリを使用し、エビデンス資料を確認しながら個人情報を入力し、顔情報を登録します。

Q8. 登録に必要なエビデンス資料は何ですか？

身分証明書や戸籍謄本住民票などその他の証明書類が必要です。

Q9. 個人情報データベースとは何ですか？

個人情報データベースは個人毎に個人情報をテーブル形式でデータベース化したものです。個人情報の公共性や重要度などの観点から 2 つの階層に分かれています。個人情報データベースは、PID をキーとして個人の情報を保持するデータベースで、本人確認や対面取引を可能にします。
新しい個人情報（例えば犯罪歴とか高額品所有物）を追加することは容易なリレーショナルデータベースになっています。

Q10.個人情報データベースにはどのような情報が含まれますか？

氏名、生年月日、顔写真、PinCode など、多岐にわたる個人情報が含まれます。

Q11.個人情報 DB のセキュリティ対策はしていますか？

はい、しています
自治体管理部個人情報データベースは AES 暗号化と秘密鍵で暗号化（RSA 暗号）し、自己管理部個人情報データベースは AES 暗号化で保護しています。
また、個人情報データベースを CQR コードに書く時は隠蔽署名をしてします。

偽装や改ざんをしようとすれば、暗号解析が必要になり、鍵を総当たりで探すのは事実上不可能なので、プログラムのリバースエンジニアリング手法によって解析するのが現実的な方法である。本システムではリバースエンジニアリング対策をしているが、その中での顔認証や隠蔽署名の解析は困難を極め、事実上偽装や改ざんはできないレベルである。
実際に解析しなければならないアルゴリズムは下記の 4 か所

① AES 暗号化アルゴリズム x 2 種類以上
② 顔認証アルゴリズム
③ RSA 暗号化アルゴリズム

④　隠蔽署名アルゴリズム

MobileID アプリケーションの場合は少なくとも 5 つの解析が必要になります。

暗号化については別紙「MobileID Technical Notes Faq10」にも記載されています

10.3.　本人確認

Q12.電子 ID カードと印刷 ID カードの両方を持つことはできるのでしょうか？

できます。しかし、有効な ID はひとつですのでどちらかが使えません。また、無効化した SN は復帰できないことを考えると印刷 ID カードを持つメリットが殆ど見当たりません。従って、電子 ID カードと印刷 ID カードの両方を持つことは推奨できません。

Q13.オンラインでの本人確認手順は？

MobileID へログインするには、アカウントと PinCode 入力、次にスマホが登録されているものか SMS で、そして顔認証を経て本人確認ができます。この手順によって本人であることを保証しています。

Q14.オフラインでの本人確認手順は？

手続きはオンライン環境での手順と同じですが、２つ違いがあります。一つ目は、認証の確認が CQR@現に使っているスマートフォンと照合されることです。2 つ目は SMS による携帯電話確認の有無ですが、それに代わって IMEI 確認をしています。

Q15.IMEI の偽造

オフラインでは IMEI@CQR と IMEI@現に使っているスマートフォンが照合される。スマートフォンの製造番号（IMEI）を偽造することはできないので、別のスマホではログインすることができません。

スマホが盗まれたら・・・

スマホを盗んで、何らかの方法でアカウント及び Pincode を得てそのスマホになりすましログインでき、IMEI 照合も通過できるのですが、しかし、顔認証で不正を見破ることができます。

Q16.ラミネートプリンターについて教えてください

GRASYS という機器を想定しています（https://grasys.jp/）

10.4. 投票

Q17.年齢や国籍での制限は簡単にできるのでしょうか？

個人情報データベースに記載されている情報に対して、投票資格を設定することができます。例えば、年齢は生年月日が ddmmyyyy 以降、国籍は japan などで制限するこができます。
逆に言えば、投票資格を規制したい項目を予め自治体管理部個人情報データベースの項目として設計しておけばよいことになります。

Q18.選挙期間中に ID カードを再発行した場合、2 回投票できるのですか？

当然できません。サーバーには SN の発行履歴や PID が保存されていますので投票済かどうかを判定できます。

10.5. CQR 決済

Q19.取引履歴の暗号化方法を教えてください

A の取引だとすれば取引履歴の内容は下記の通りです。

A の PID	Z の PID	商品名	価格	数量	CQR 件名	Time Stamp	発行番号	日時	A or Z の公開鍵

水色の部分は AES 暗号化され、さらに A が発行する秘密鍵で RSA 公開暗号化方式によって暗号化がされています。緑色の部分は A の公開暗号化方式の公開鍵です。また、この取引履歴を CQR として表示する時は偽造防止のために隠蔽署名がされています。

Q20.支払して、そこで終わってしまいました

「支払のために取引 CQR」を提示したいのですが、相手の方がそれをスキャンニングせずに取引が中断、終了してしまいました」というご質問ですね
この事態になるのはオフライン取引です。このままだと支払いが宙に浮いている状態になります。必ず、購入者がキャンセル CQR を発行し、売主がそれをスキャンしてキャンセル処理してください。支払った料金は元に戻るので、引き続き取引を継続することができます。

本システムでの決済記録は全て AES 暗号化され、さらに公開暗号化方式により改ざん防止が施されています。ハイブリッド化によって決済記録の改ざん防止を強力化しています。
さらに隠蔽署名による偽造防止によってセキュリティを強化しています。

（1）決済記録の形式

- MobileID アプリケーションでは、決済記録は AES 暗号化してから、秘密鍵で暗号化し、その対になる公開鍵を計算して付加します。
- MobileID アプリケーションでは、隠蔽署名は CQR の偽造を防ぐためのものです。IMEI と CQR コードに隠蔽した署名（Steganography）を照合し、一致すれば A または B のスマートフォンで発行したものとし、一致しなければ偽造と判断します。

A の PID	Z の PID	商品名	価格	数量	CQR 件名	Time Stamp	発行番号	日時	A の公開鍵

(2) 改ざん防止　決済記録は取引相手が生成、それをスキャンニングして保存

- 取引者は互いに 1 回、取引履歴 CQR で表示し、相手にスキャンニングしてもらいます。
- MobileID アプリケーションでは、スキャンニングしたら取引履歴として保存されます
- MobileID アプリケーションでは、取引履歴は相手の個人秘密鍵で暗号化されています。つまり、改ざんするには相手の個人秘密鍵が必要になります。それを知ることはできないので、**「スマホに保存された決済記録を自分は改ざんすることができない」**仕組みになっています。

Q21.オフライン取引の履歴を消してしまいました

支払履歴や領収書などの履歴は、削除されても問題ありません（※）。取引が開始されると、価格や商品説明が記載された CQR が売り手によって提示されます。この CQR は保護されており、自動的に保存されています。万が一、この CQR を含めてすべての履歴が削除されてしまうと、取引そのものが存在しないにもかかわらず、売買や金銭のやり取りがあったように見えるリスクが生じます。このような場合、必要に応じて双方に確認を取り、適切な処理を行います。

※履歴は保護され、自動的に保存されているため、誤りやうっかりで削除されることはありませんが、悪意のある者であれば削除が可能です。

Q22.オフライン取引の履歴改ざん対策を教えてください

履歴は取引相手の秘密鍵で暗号化されているため、決済後に悪意を持って改ざんしようとしても、A も B も互いの秘密鍵を知らないため、履歴を復号化できません。そのため、改ざんは不可能です。

Q23.同一人物（または仲間）の履歴改ざん対策を教えてください

履歴は取引相手の秘密鍵で暗号化されていますが、この秘密鍵は仲間であっても簡単に入手できるものではありません。秘密鍵を入手するためには、リバースエンジニアリングによる解析が必要です。さらに、乱数を使った一時的な秘密鍵が用いられているため、たとえリバースエンジニアリングに成功しても、現在の取引履歴に対応する秘密鍵を見つけることはできません。

Q24.最初から払う気がない（詐欺）場合の対策を教えてください

例えば、A が通常通り決済を行い、B から商品を受け取ったとします。この後、A がオンラインに接続しなかったり、取引履歴を削除したり、スマホを廃棄するなどして換金を停止させる行為を行った場合、A の支払いが「宙に浮いた」状態に

なります。しかし、換金には「オンライン後 24 時間以内（24 時間は 1 例、運用者に委ねられる）」という制約があるため、A がなぜオンラインにならないのかを確認し、不正が発覚すれば、その宙に浮いた支払額を B に移動することが可能です。

このケースは後処理に時間がかかる場合もありますが、実質的な被害は発生しません。そのため、この仕組みによりこのような詐欺行為の発生は減少するでしょう。

Q25.取引履歴の偽造対策を教えてください

チャージ以上の取引ができない仕組みが対策のひとつです。
2 つ目は暗号化。偽造は下記のような流れになりますが、暗号化によって偽装は途方もなく時間が掛かるので事実上偽造できないと判断しています。

(1) 偽の取引履歴を作成
(2) 偽取引履歴を AES 暗号化する（鍵は真取引履歴の暗号化に使われている鍵、解析して見つけねばならない）
(3) 偽の秘密鍵で偽取引履歴を公開暗号化
(4) Steganography で CQR に隠蔽署名

Q26.盗んだスマホで取引されたらどうなりますか？

盗んだスマホではアカウントや PinCode を知らないのでログインできませんが、（水原一平事件のように）知り合いから盗んだとか何等かの方法でログインできたとしても、顔認証で本人確認ができずそこで取引がストップし、被害を未然に防げます。

Q27.スマートフォンを無くしてしまいました。チャージ金は戻りますか？

もどりません。
チャージはいわば現金で、スマートフォンが財布になります。現実の世界で、財布を落としたら善良な人が届けない限り現金はもどりません。本質問はそれと同じです、チャージは戻りません。しかし、本人確認ができないので悪用されることはありません。スマートフォンが見つかればチャージが戻る可能性が高いです、戻ることを祈るしかありません。

チャージは現金を持ち歩くのと同様です。あまり大きな金額をチャージせずに利用すること、大きな買い物をする時はオンラインでチャージしつつ取引することを推奨します。こうすることで、チャージ額を低くしておけば、現金を持つよりも安全にご利用できます。

10.6. オプション機能

Q28.本人が登録するオプションって、その情報に信憑性を保証できるのですか？

はい、情報源であるエビデンス資料の真偽を確認してからの登録になります。確認事項や方法については契約時に決定することになります。

Q29.顔認証機能を「監視システム」に応用できますか？

顔の認識を通じて、特定の人物を監視カメラで識別することができます。スマートフォンをカメラとして監視位置に設置すれば、インターネットを経由してどこでも確認できます。ご希望や関心があればご相談ください。

10.7. メンテナンス

Q30.MobileID システムのメンテナンスについて教えてください。

システムのメンテナンスとは、ソフトウェアやハードウェアの正常な動作を維持し、問題が発生しないようにするための作業です。これにはバグ修正、パフォーマンスの最適化、セキュリティアップデート、機能の改善などが含まれます。具体的には、ソフトウェアのアップデートやパッチの適用、データのバックアップ、システムの監視などが行われます。
定期的なセキュリティチェックやシステムのアップデートが行われます。

10.8. バックアップ

Q31.バックアップはどのように行われますか？

システムのバックアップとは、システム内のデータや構成情報などの重要な情報を複製し、安全な場所に保管するプロセスです。バックアップは、予期しないデータの損失やシステム障害、自然災害、サイバー攻撃などのリスクに備え、システムを迅速に復旧できるようにするために行われます。

システムバックアップの主な目的

データの保護

データが削除、上書き、または破損しても、バックアップから復元できるため、データの保護に役立ちます。

迅速な復旧

システム障害やサーバーダウンが発生した際に、バックアップからシステムを復旧することでダウンタイムを短縮し、業務の継続を支援します。

法的・規制要件の準拠

一部の業界では、重要なデータの一定期間の保存や復元可能性を法的に求められる場合があります。バックアップを定期的に行うことで、こうした規制要件を満たせます。

サイバー攻撃対策

ランサムウェアなどの攻撃を受けてデータが暗号化や削除されても、バックアップがあればシステムを再構築し、影響を最小限に抑えることができます。