

券面の可変情報を起因とする ICチップ内情報の読出しに関する研究

前 東京工業大学 像情報工学研究所特別研究員
角 憲祐

個人番号カードについて



カード画像出典 ; <http://www.soumu.go.jp>

磁気ストライプ

電子証明書の有効期限

サインパネル



QRコード; 格納情報は個人番号 個人番号12桁

ICチップに格納された番号法に基づく事務で利用するための基本AP(一部抜粋)

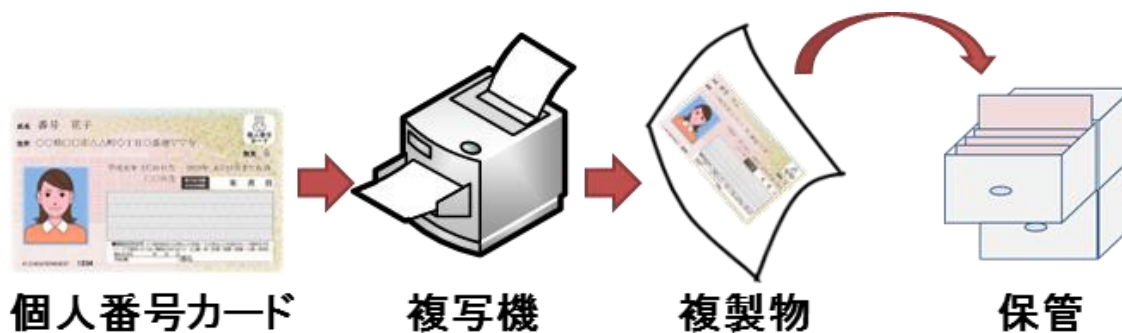
AP	個人番号取得における役割	アクセスコントロール
券面事項確認AP	(記録する情報) ・表面情報: 4情報 + 顔写真の画像 ・裏面情報: 個人番号の画像	券面情報を展開 照合番号A; 表裏 照合番号B; 表のみ
券面事項入力補助AP	(記録・利用する情報) ① 個人番号と4情報とその電子署名データ ② 個人番号とその電子署名データ ③ 4情報とその電子署名データ	テキストデータを展開 ① 暗証番号 ② 照合番号A ③ 照合番号B

これらのAPを使用した本人確認、券面の真正性の確認には作業に人手と労力がかかる

個人番号を使用した証跡作業

身分証明の持参証拠として複製物を保存する場合、

現状



課題 複写作業や保管場所の設置、維持管理などの手間がかかる
複製されたQRコードが第三者に悪用される恐れがある

電子的に
格納された
情報

AP	券面事項確認AP	券面事項入力補助AP
個人番号が 不要な利用者	表面情報: 4情報 + 顔写真の画像	4情報とその電子署名データ
個人番号が 必要な利用者	表面情報: 4情報 + 顔写真の画像 裏面情報: 個人番号の画像	個人番号とその電子署名データ 4情報とその電子署名データ

課題 それぞれの情報抽出にそれぞれ照合番号の入力が必要

旅券のように券面下部を読取らせる仕組みを個人番号カードにも導入した方が望ましい

QRコードの不正利用

ビットコインの盗難(2013年12月)

米)ビットコイン付きクリスマスカードのレポート

司会者がQRコードを数秒カメラに向けたところ...



何者かがビットコイン(20ドル相当)を盗む

情報出典: <http://gigazine.net/news/>

個人番号カード



課題: 格納情報が不正利用される恐れ

カード画像出典: <http://www.soumu.go.jp>

QRコードの格納情報の一般的なリーダーによる読取不可にする
QRコードを複製させないようにする

⇒ QRコード自体を秘匿化することが必要

ステルス型QRコードの検討

説明時にご覧いただけます。

QRコードのデコード

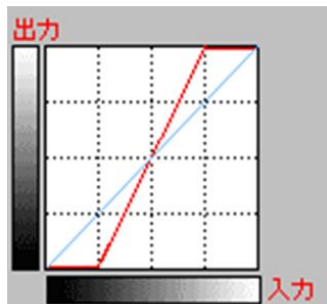
説明時にご覧いただけます。

読取ったQRコードは
デコードできなかった

画像処理を施し、デコードが可能となる条件を検討

QRコードのコントラスト補正処理

コントラスト補正



中心点は同じだが、明るい部分はさらに明るく、暗い部分はより暗く出力される

補正前

補正後



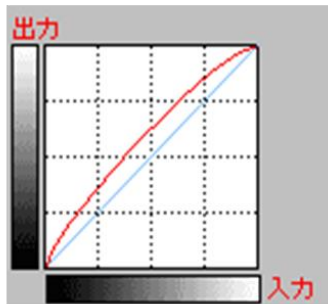
引用 ; <http://www.geocities.co.jp>

説明時にご覧いただけます。

補正後のデコード率は向上したが、迅速かつ確実な読取不可

QRコードのガンマ補正処理

ガンマ補正



中心域を中心に明るさを変化させる。
完全な黒及び白には変化がない。

補正前

補正後



引用 ; <http://www.geocities.co.jp>

説明時にご覧いただけます。

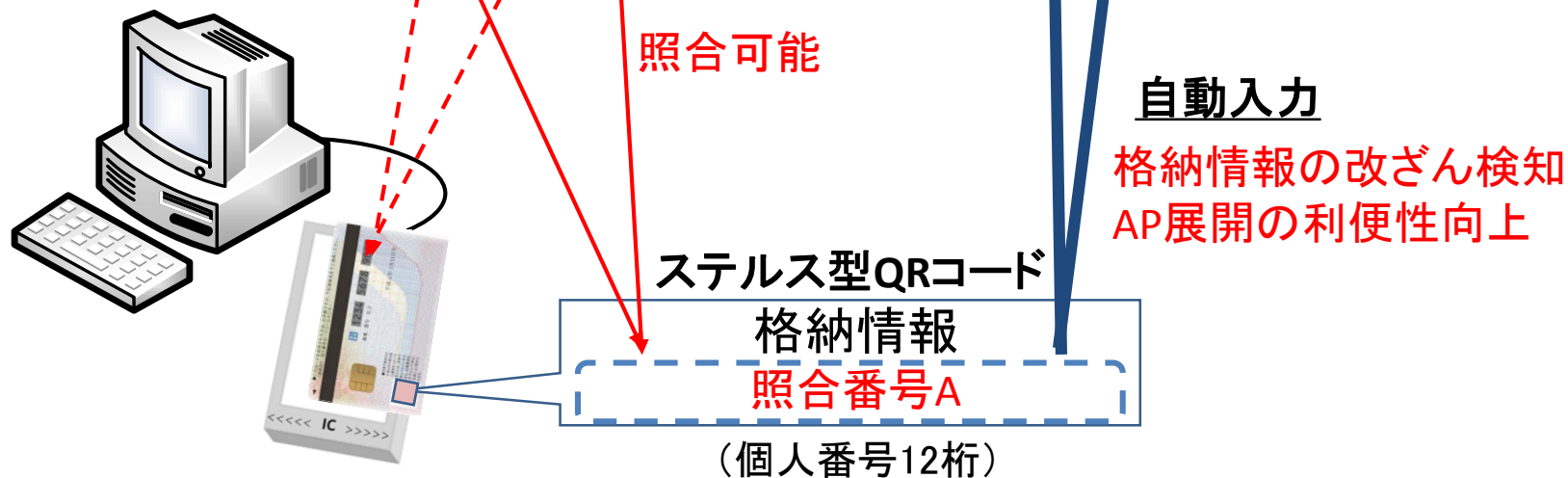
補正後のデコード率が向上、迅速かつ確実な読み取りが可能

複写機で他媒体に複写できず、QRコードは複写媒体で使用不可能に

光学的読み取り媒体のリスクの1つである「複製」を防止

照合番号の自動入力（照合番号A）

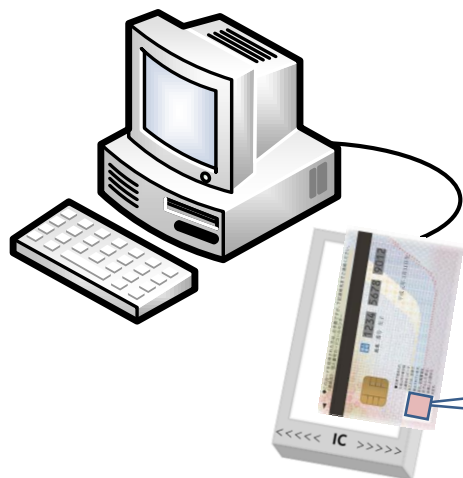
AP	個人番号取得における役割	アクセスコントロール
券面事項確認AP	（記録する情報） ・表面情報：4情報＋顔写真の画像 ・裏面情報：個人番号の画像	表裏の券面情報を展開 照合番号A（個人番号12桁）
券面事項 入力補助AP	（記録・利用する情報） ・個人番号並びにその電子署名データ	テキストデータを展開 照合番号A（個人番号12桁）



ステルス型SQRCに格納した照合番号（個人番号）をアクセス鍵としたAP内格納情報の展開
 ⇒ QRコードに格納された個人番号の改ざん検知とAP展開の利便性向上による
 が期待できる

照合番号の自動入力（照合番号B）

AP	個人番号取得における役割	アクセスコントロール
券面事項確認AP	（記録する情報） ・表面情報：4情報＋顔写真の画像	表裏の券面情報を展開 照合番号B
券面事項 入力補助AP	（記録・利用する情報） ・4情報並びにその電子署名データ	テストデータを展開 照合番号B



照合可能

ステルス型QRコード

格納情報
照合番号B

（生年月日＋有効期限西暦部分＋セキュリティコード）

自動入力

格納情報の改ざん検知
AP展開の利便性向上

照合番号Aと照合番号BをQRコードに格納すれば、2種類の自動入力が可能となる

⇒ 個人番号を取り扱えない者が個人番号を取り出すことが可能となってしまうため
二つの異なる格納情報を分けて展開する方法が必要

ステルス型QRコードの読取制限機能追加

SQRC® (セキュリティ機能搭載QRコード)

(概要) QRコードの情報の一部を非公開にすることができる機能を追加したコード



(特徴)

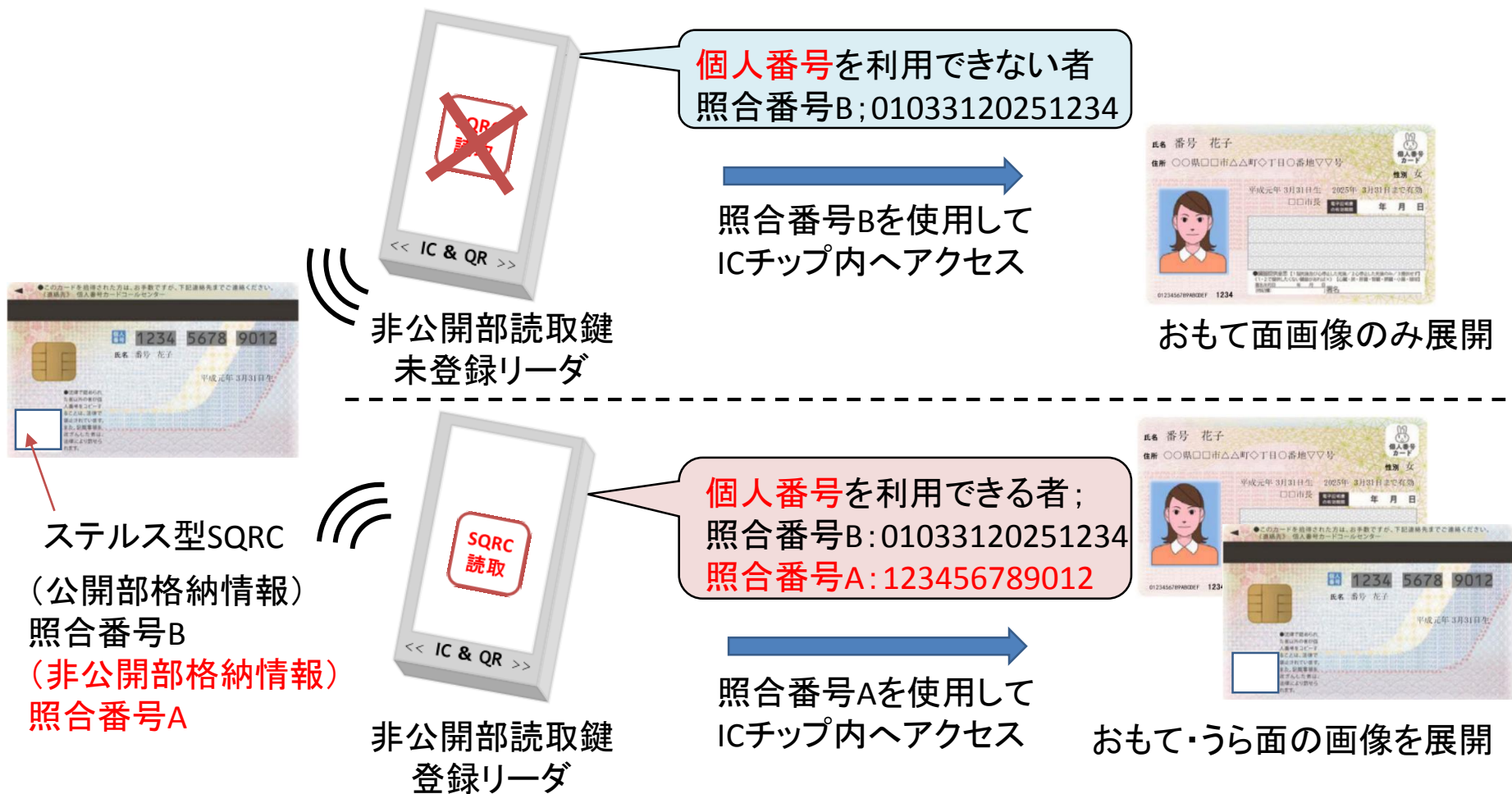
- ・特別なデータの暗号化や、復号ソフトが不要
- ・見た目はQRコードと同じ(見分けがつかない)
- ・偽造不可能(非公開部を含めた再生成が不可)

- ・公開部と非公開部の2領域から構成される
(非公開部格納情報は**非公開部読取鍵をもつリーダ装置でのみ読出し可能**)



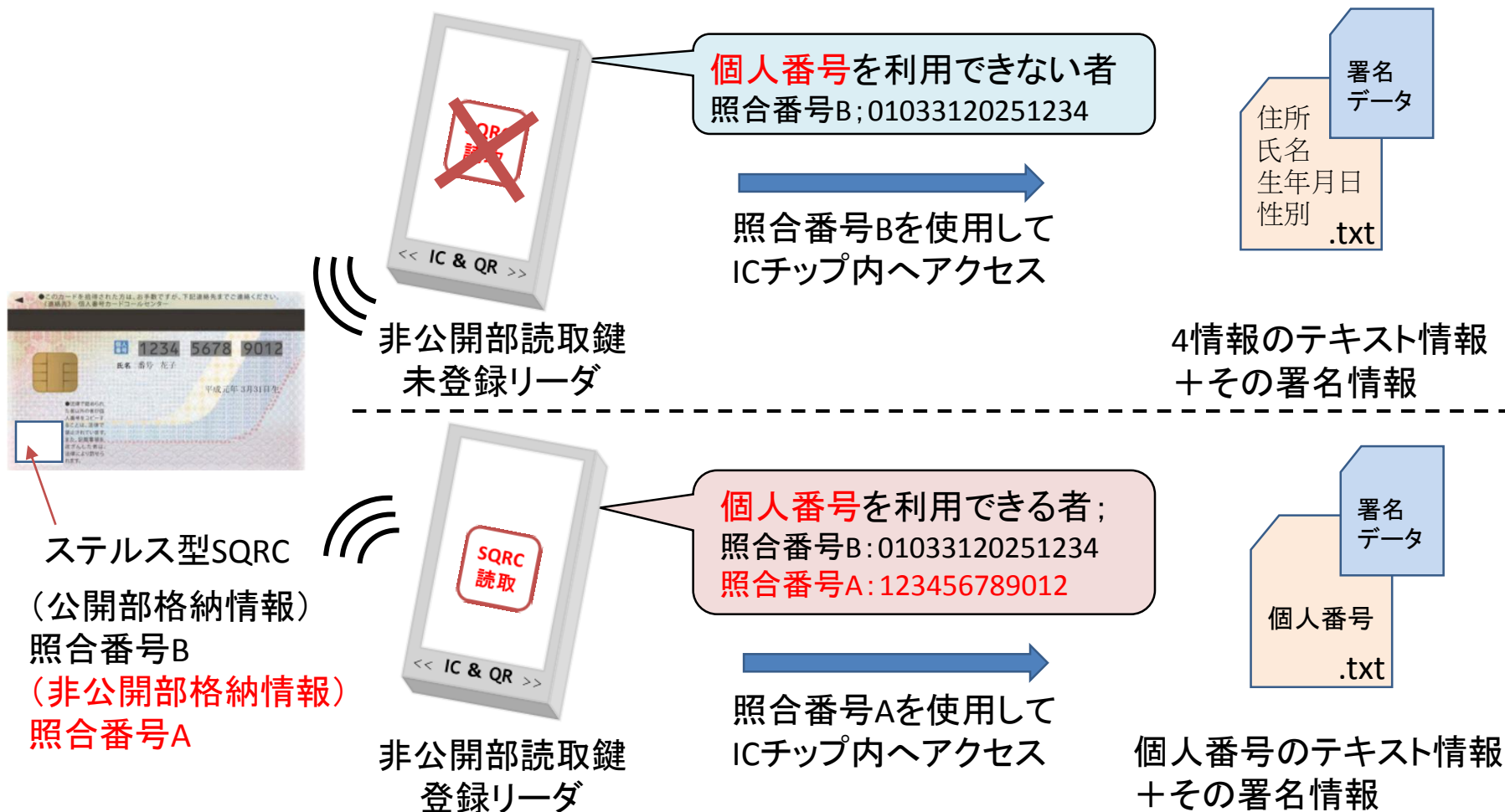
QRコードの「複製、偽造、改ざん」防止だけでなく格納情報の読み分けが可能

券面事項確認AP情報の展開



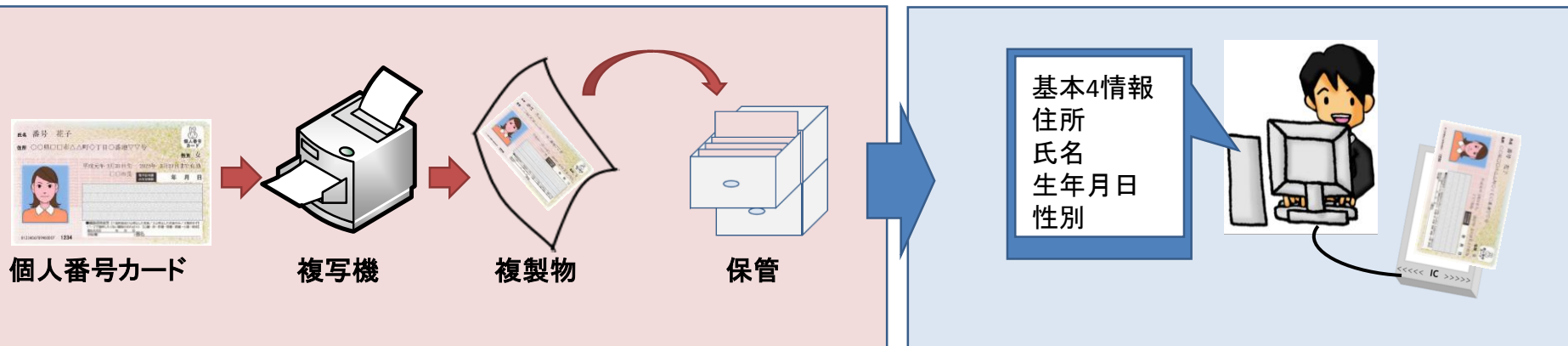
2つの照合番号を1つのステルス型SQRCリーダで読み分け、各々に必要な情報を展開

券面事項入力補助AP情報の展開



券面事項入力補助APでも利用可能

身分証明等の持参証拠作業の電子化



証跡情報の収集を電子化することで、**ペーパーレス化、不正に個人番号を複写する行為の防止**に繋がる

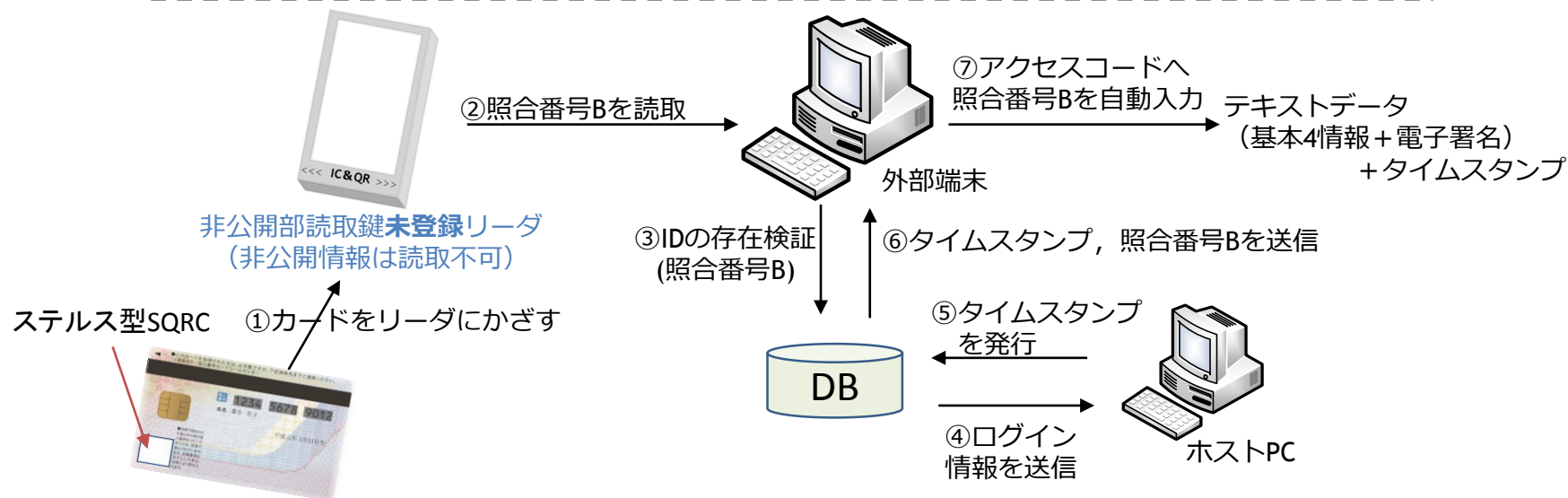
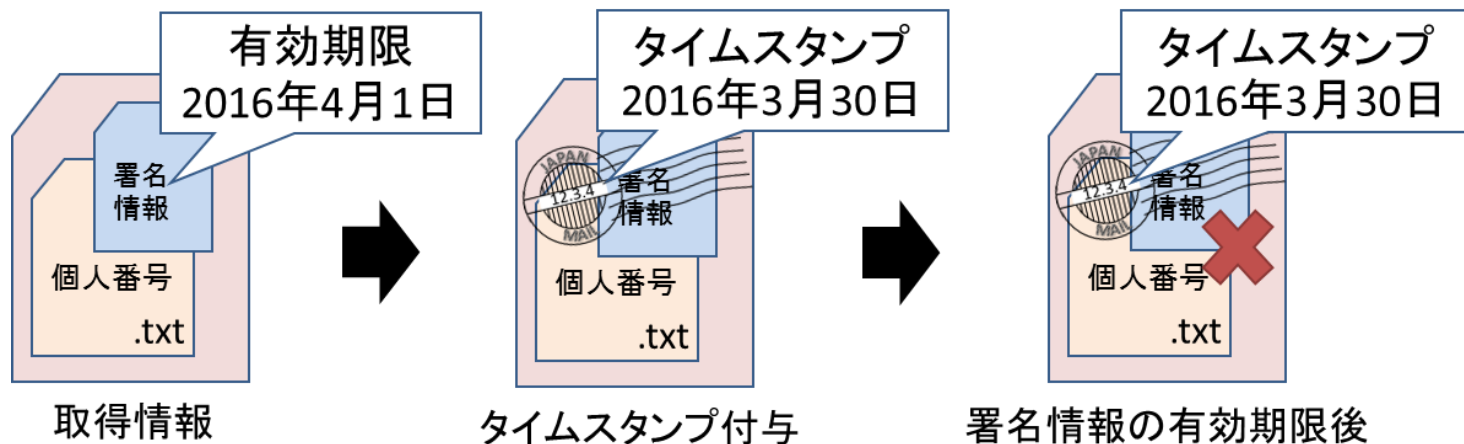


取得情報

真正性が担保できない

署名情報には有効期限があり、長期間の保存や確認には利用不可

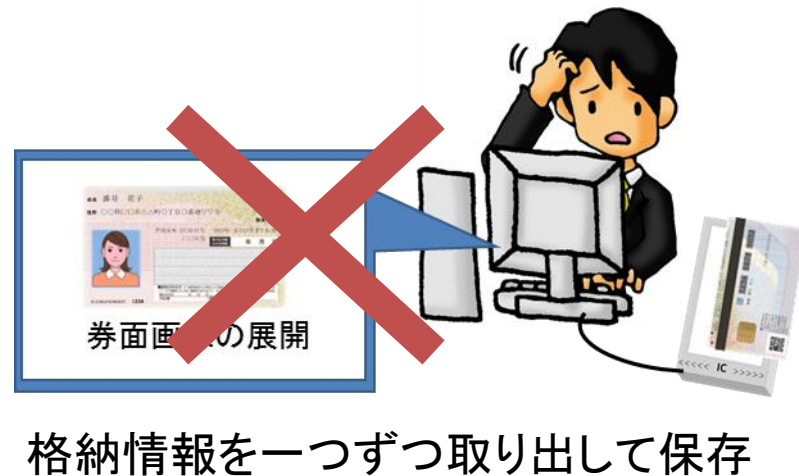
券面事項入力補助AP情報の展開



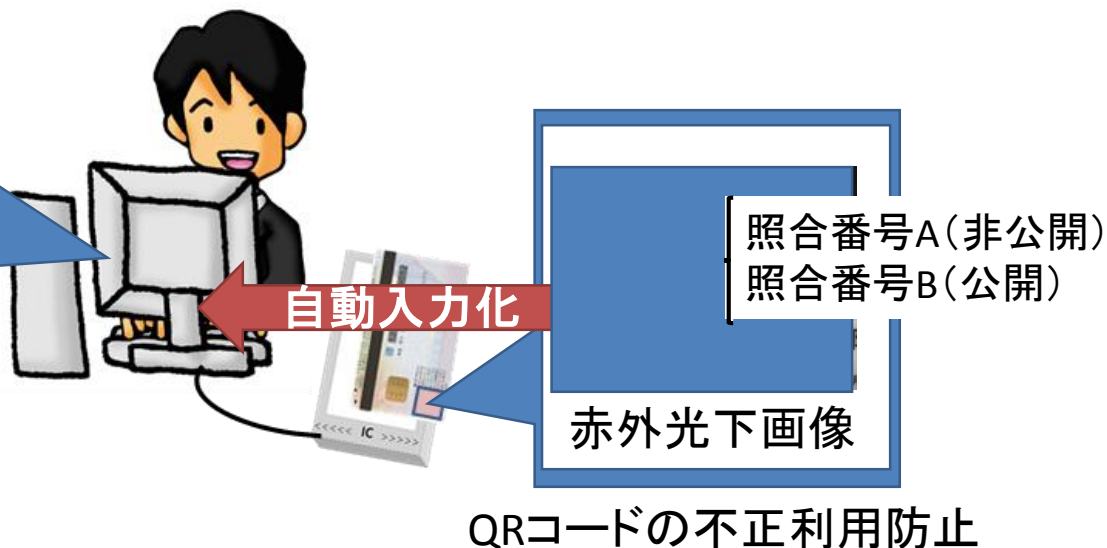
タイムスタンプがあることで署名情報を利用した時点では有効であったことが担保できる

まとめ

証跡作業(現行)



証跡作業(提案)



対応するリーダにかざすだけで、証跡に必要な情報取得が可能に