TCODE
テララコード研究所

2019.10.26
@名城大学

電子署名付きQRシンボルのご紹介

内容
1. 既存のシンボルとセキュリティ
2. 電子署名付きQRシンボル
3. 想定用途

テララコード研究所
寺浦　信之

0.　自己紹介

1976年　名古屋大学工学部原子核工学科卒業
1979年　名古屋大学大学院工学研究科原子核工学専攻修了
1979年　日本電装（現デンソー）入社　開発研究部パターン認識グループ配属
　・音声認識、音声合成
　・FAコンピュータ
　・RFID
2000年　JAISA　RFID部会　部会長　（～2009）
　（日本自動認識システム協会）
2008年　RFタグ技術課題検討委員会委員長
　・ECOM（電子商取引推進センター）
2009年　テララコード研究所　所長
　・原子力研究開発機構と共同研究
2017年　九州大学システム情報科学府博士課程修了（博士（工学））
2019年　電子署名付きQRシンボルを開発

かんばんシステム

耐放射線RFタグの開発

二次元シンボルの
セキュリティの研究

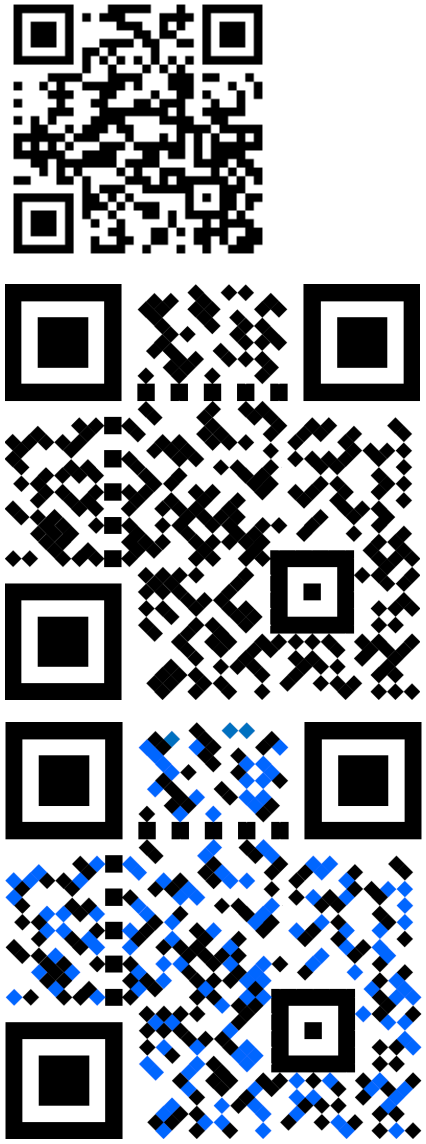
本日のお話の内容

1．既存シンボルのセキュリテイ
・QRコードは誰でもが作成可能
・セキュリティ低い

2．電子署名とは
・通信と同等の安全性を実現

3．電子署名付きQRシンボル
・菱形サブセルの導入
・二重符号化（コピー不可）

4．想定用途
・認証の必要な書類（証明書、有価証券）
・WEB参照
・キャッシュレス決済



1．既存シンボルとセキュリティ

1．1．1　種類

①一次元シンボル

JAN-13	Code-39	NW-7	ITF-14
			
商品コード	工業製品ラベル	宅配便送り状	物流段ボール箱

②二次元シンボル

マルチロー型	
マトリックス型	

特徴：①データ量大きい　②誤り訂正機能具備

1．1．2　開発履歴

一次元シンボル	二次元シンボル
1970年　CODE 2of 5　開発 1971年　JANシンボル開発（IBM） 1972年　NW7開発 1974年　CODE39開発 1984年セブンイレブン（日本） 商品バーコード導入	1982年　ベリコード（マトリックス） 1987年　CODE49（マルチロー） 1987年　データマトリックス（マトリックス） 1989年　PDF417（マルチロー） 1994年　QRコード（マトリックス）

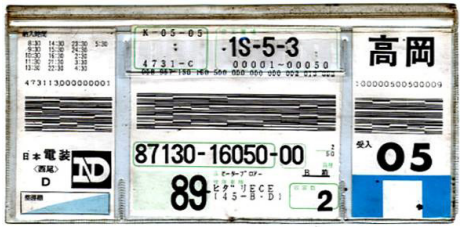
高度化の余地が大きい

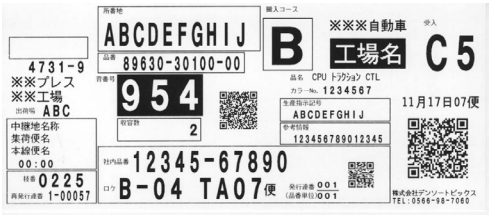
1980年代後半から
1990年代前半の読
取り技術を前提

１．２　セキュリティの必要性

（１）QRコード
- ・開発経緯
  - ・かんばんシステム用
    - ・確実に読める
    - ・セキュリティ不要
  - ・携帯電話対応
    - ・WEB参照
    - ・セキュリティ必要

（２）セキュリティのニーズ
- ・秘密データの受渡し
- ・偽造防止
- ・フィッシング防止
- ・キャッシュレス決済





①誰でも作れる
- ・WEB利用

②誰でも読める
- ・スマホ

セキュリティ性のあるQRシンボルが必要

1960年代のかんばん

①バーコード導入前のかんばん

・物と情報の一体化
・作業者が見てわかる

ビニール
袋入り

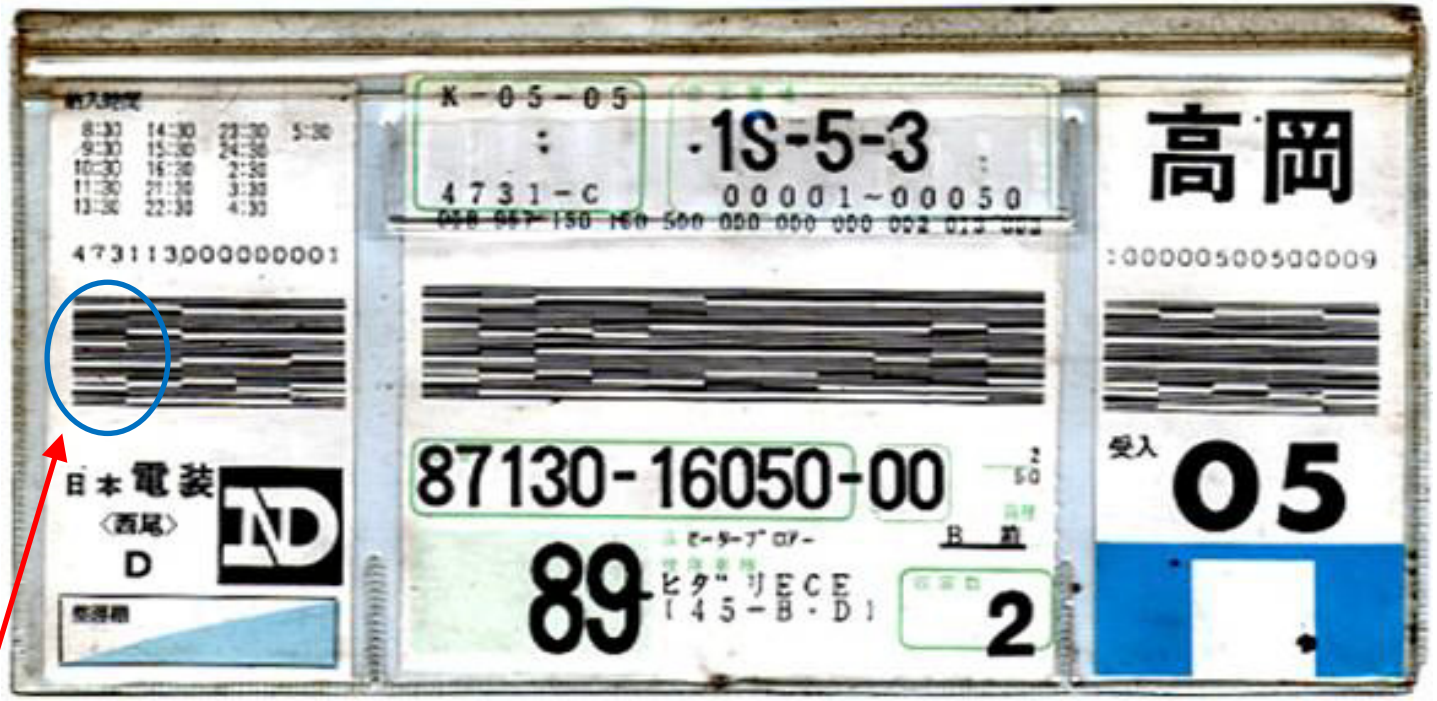
世界で最初の二次元コード

1970年台に開発

②バーコード導入後の（リサイクル）かんばん

データを記憶するデータキャリア

・物と情報の一体化
・作業者が見てわかる
・データの自動入力
・再利用



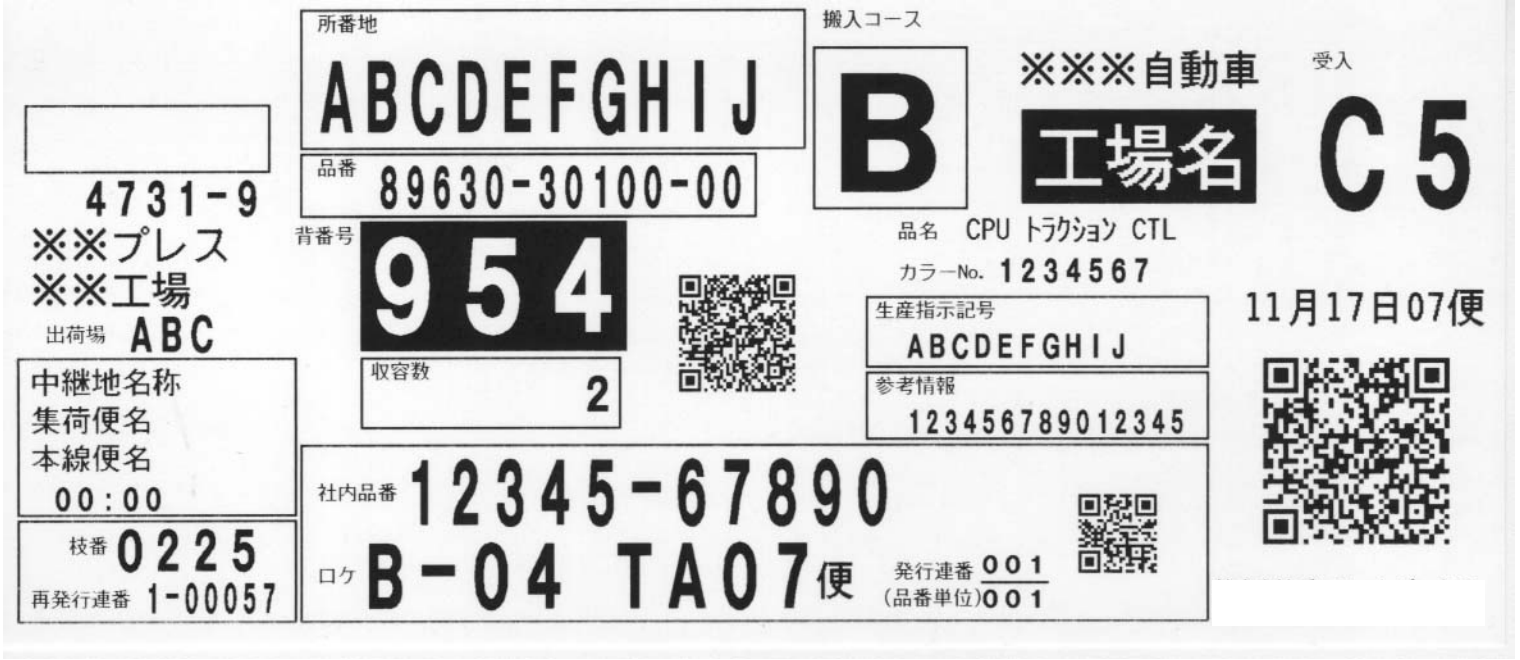
ビニール
袋入り

3桁（1桁チェックビット） X 21 ＝ 63文字

特長
・ローラーで自動スキャン
・バーコードを平行に10回以上読取

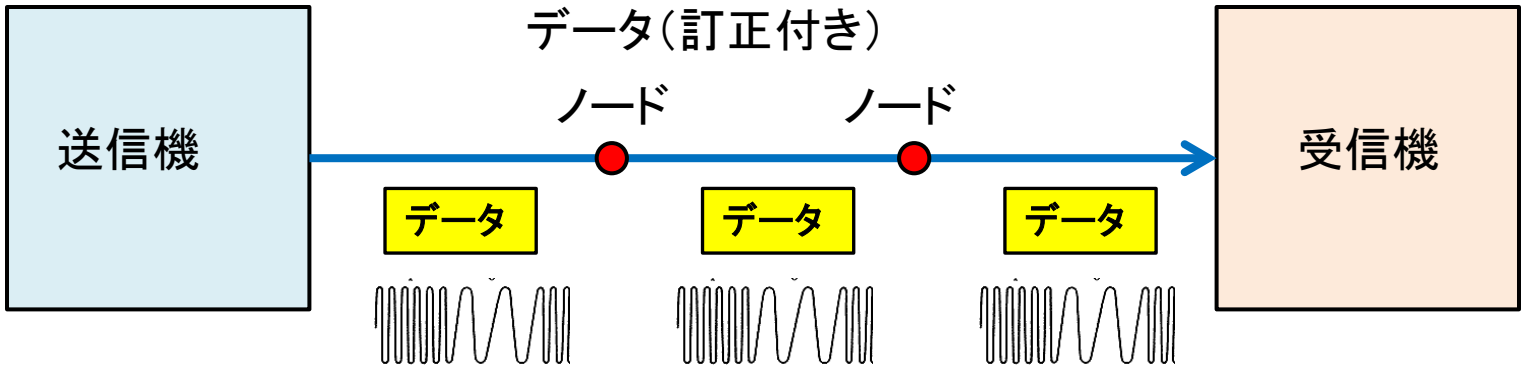
2000年代のかんばん

③ QRコードかんばん



1．3　電子署名の実装

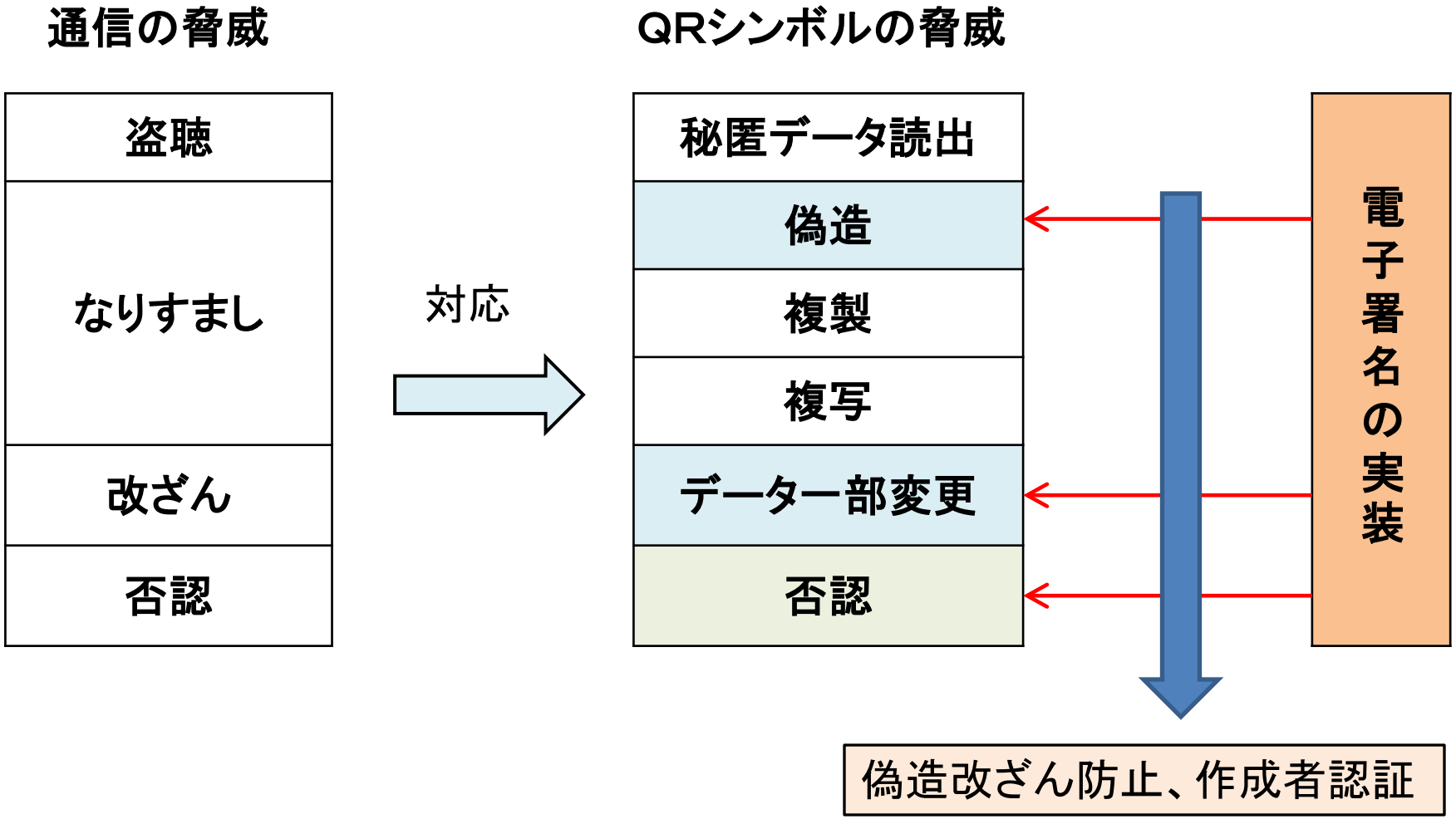
①通信路による送受信



②二次元シンボルによる送受信

二次元シンボルは通信路 ⇒ **電子署名の実装を検討**

1．4　電子署名の効果


通信の脅威
盗聴
なりすまし
改ざん
否認
対応
QRシンボルの脅威
秘匿データ読出
偽造
複製
複写
データー部変更
否認
電子署名の実装
偽造改ざん防止、作成者認証

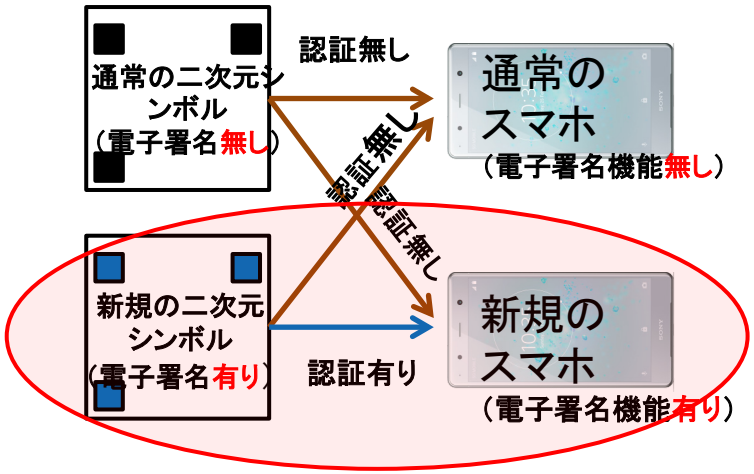
3.　電子署名付きQRシンボル

2.　**電子署名付きQRシンボル**
- 2．1　電子署名収容の条件
- 2．2　記憶領域の拡大
- 2．3　ダイアモンドシンボル
- 2．4　特徴
- 2．5　認証システム構成

２．１　電子署名収容の条件

①互換性

・既存の機器やスマホソフトでデータが読み取れる。

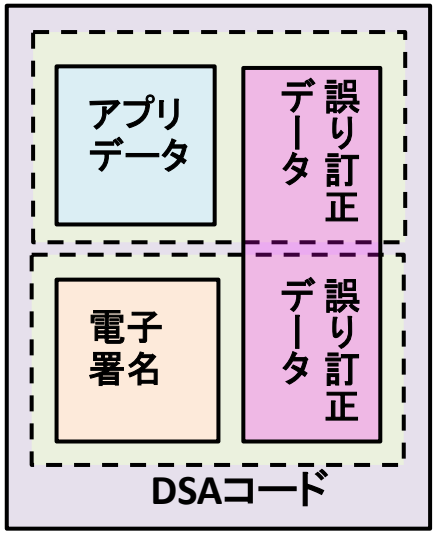


②読取り性

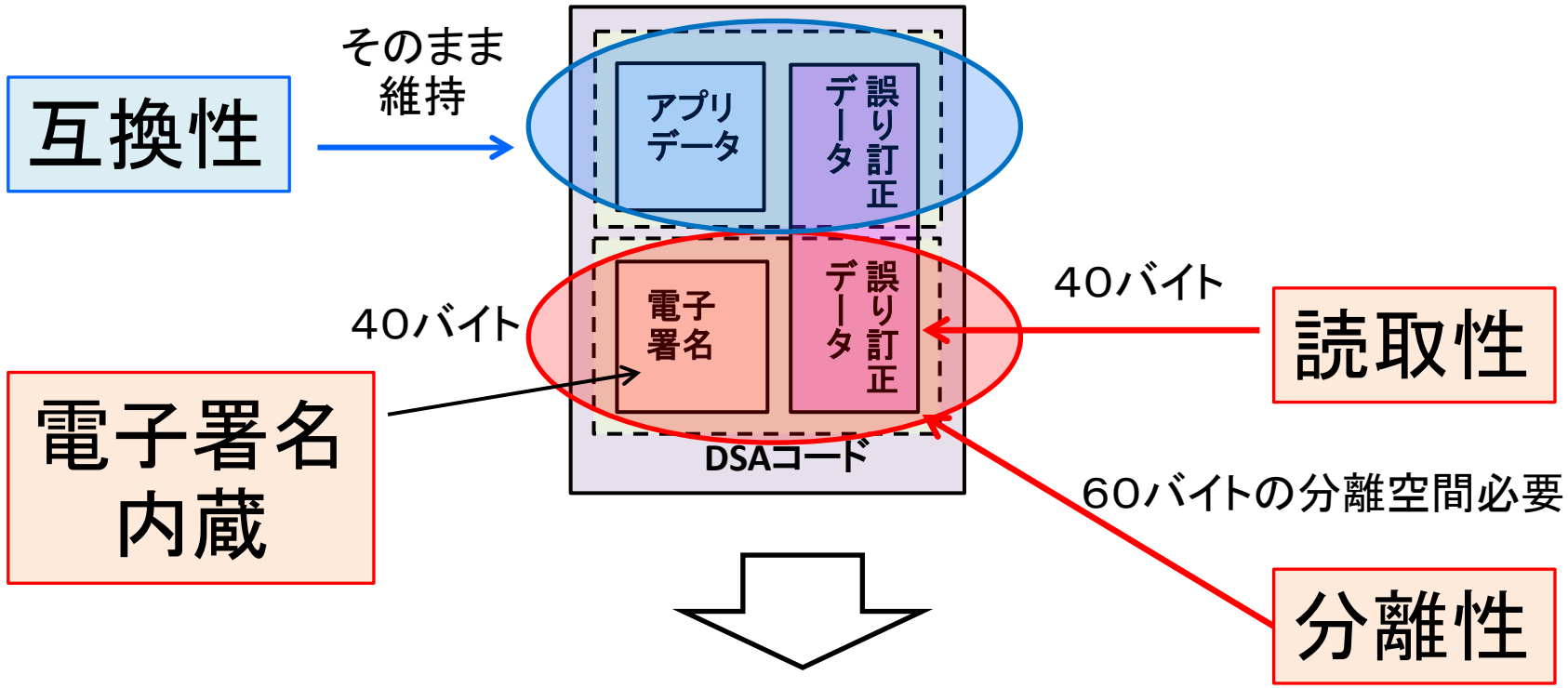
・既存のQRシンボルでも誤り訂正機能具備
・少し読取り誤りあっても、読取り可能
・電子署名にも誤り訂正具備し、読取り性確保

③分離性

・通常のデータ記憶領域とは異なる領域に電子署名記憶する。
・同じ領域に記憶すると、アプリソフトで意識する必要。アプリ互換性がなくなる。



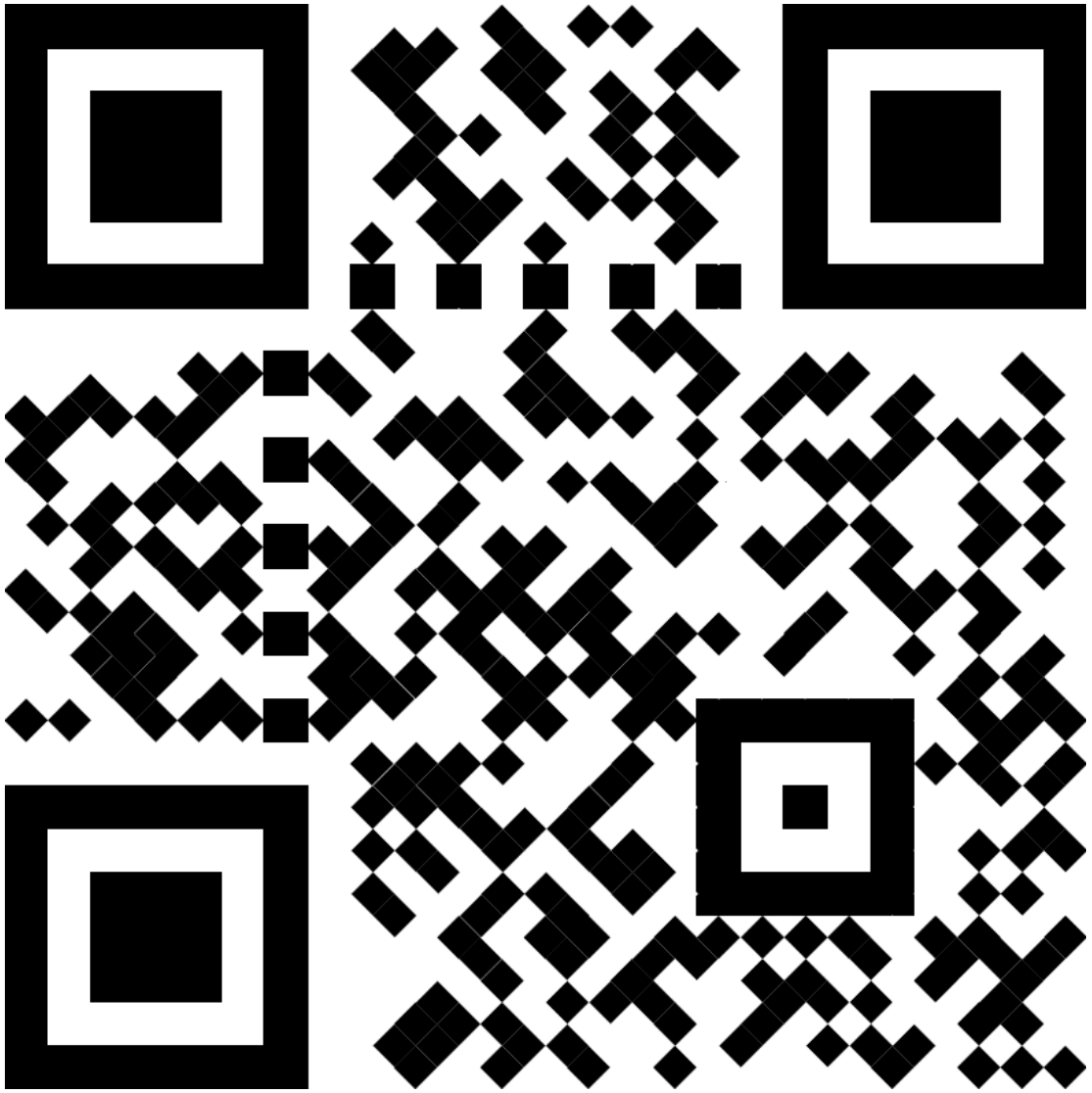
2．2　互換性を維持した別空間での記憶領域の拡大



課題
①互換性維持しつつ、分離された空間を創出
②記憶容量の拡大（60バイト以上）
　・記憶密度の増大

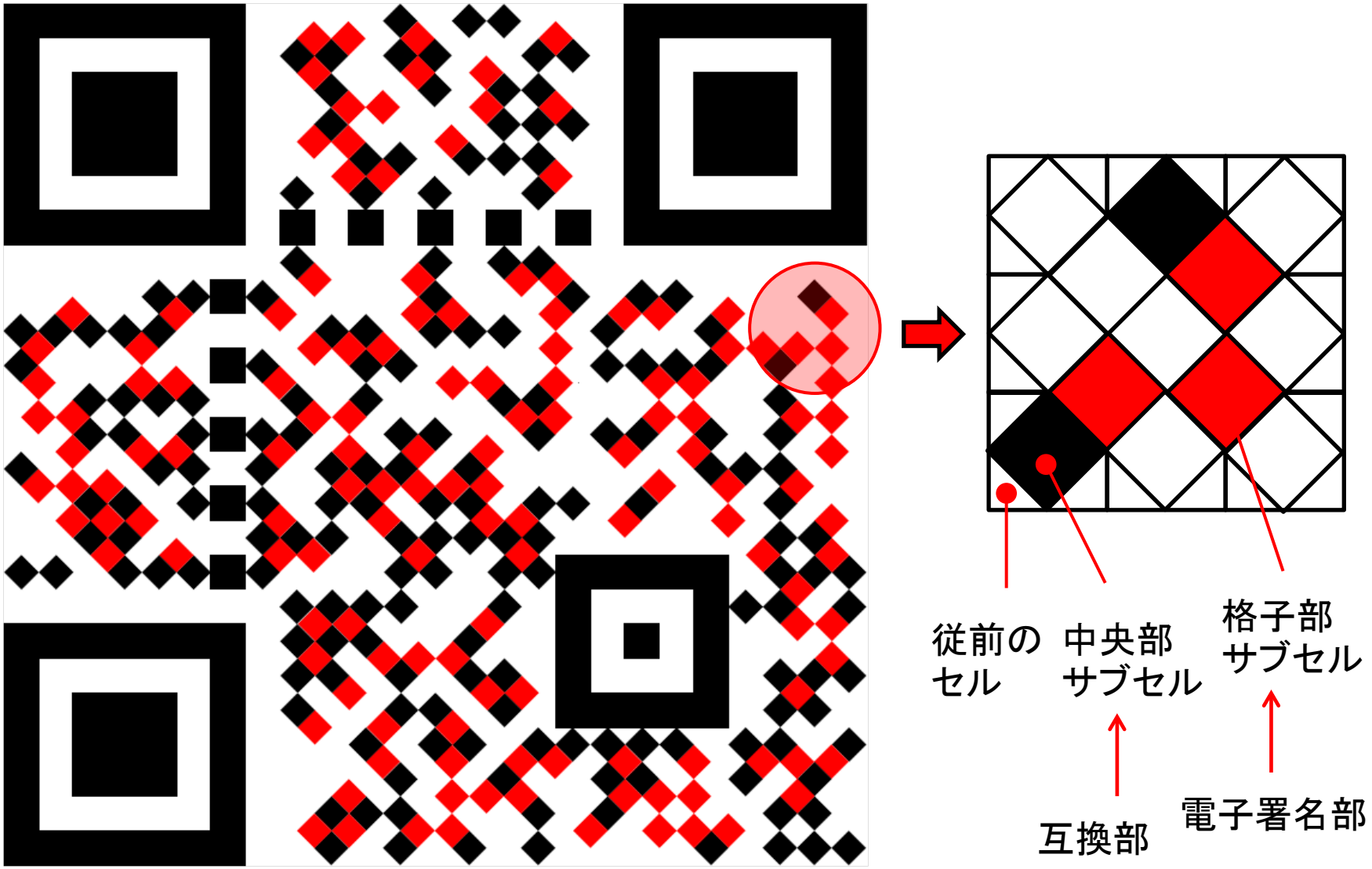
２．３　ダイアモンド　シンボル（QRシンボル２．０）

・標準表示



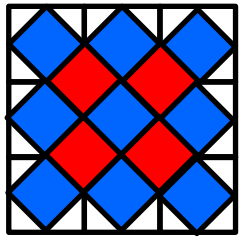
2．3　ダイアモンド　シンボル（QRシンボル2．0）

・中央部と格子部を黒と赤で区別



２．４　特徴

１．菱形サブセル
- ・中央部と格子部の２領域化
- ・セルの不感領域にサブセル挿入



２．電子署名内蔵
- ・ECDSA（楕円曲線）方式
- ・十分な安全性

３．互換性
- ・既存機器で既存部読取可
- ・アプリソフトはそのまま使用可

４．二重符号化

⇨

①電子署名データ実装
- ・格子部サブセルに収容
- ・分離性を確保

②誤り訂正データ実装
- ・読取り性を確保

③データ密度向上
- ・未利用領域を活用

⇨

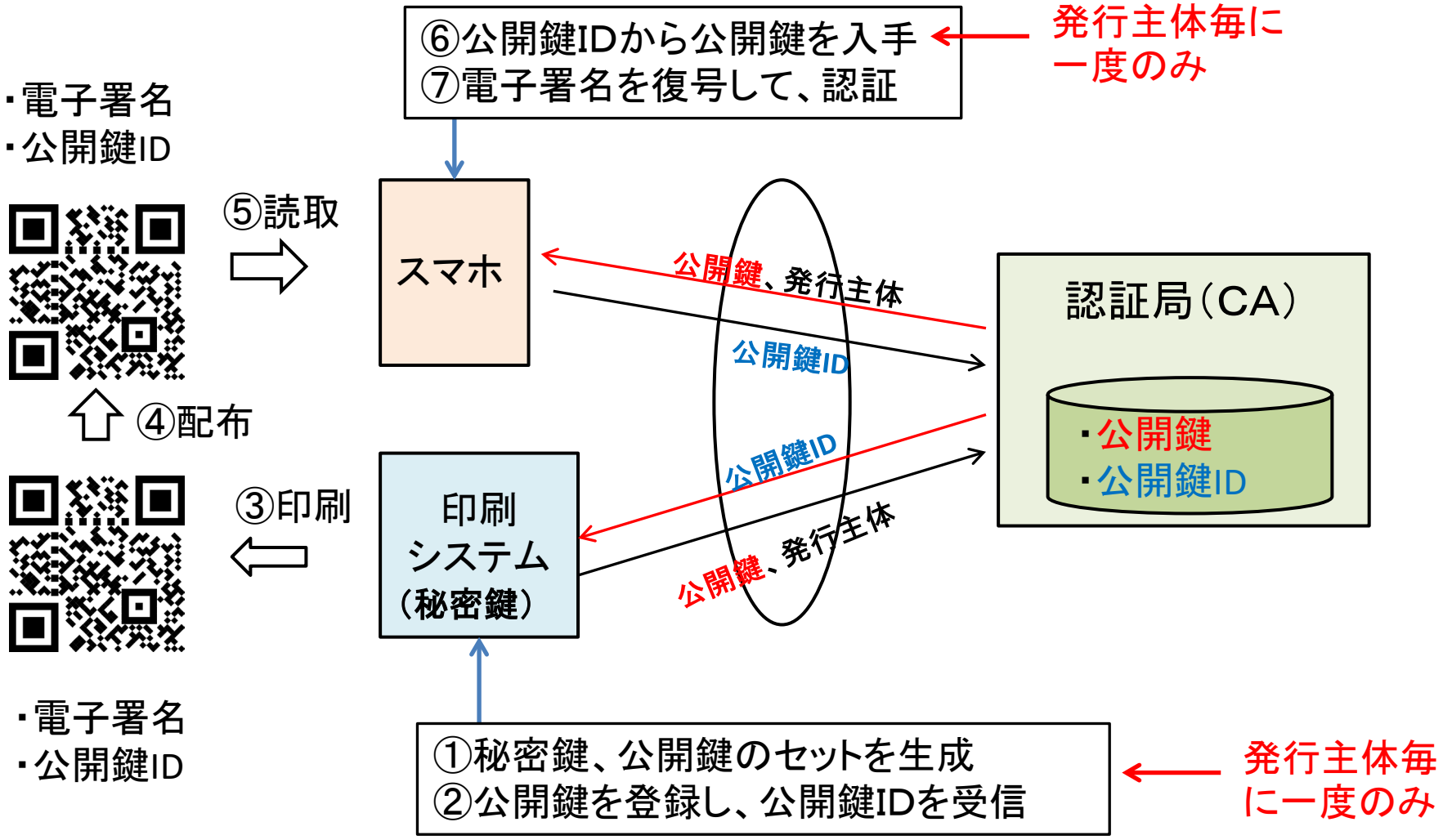
①発行者認証
②偽造防止、改ざん防止

⇨

①既存のQRコードと共存
②既存の機器、ソフトと共存

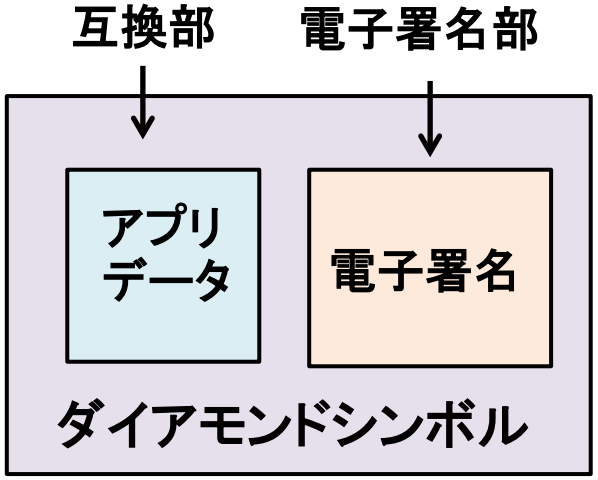
①コピー不可

２．５　認証システム構成


⑥公開鍵IDから公開鍵を入手
⑦電子署名を復号して、認証
発行主体毎に
一度のみ
・電子署名
・公開鍵ID
⑤読取
スマホ
公開鍵、発行主体
公開鍵ID
認証局（CA）
・公開鍵
・公開鍵ID
④配布
公開鍵ID
③印刷
印刷
システム
（秘密鍵）
公開鍵、発行主体
・電子署名
・公開鍵ID
①秘密鍵、公開鍵のセットを生成
②公開鍵を登録し、公開鍵IDを受信
発行主体毎
に一度のみ

3. 想定用途

①発行者の認証
②有価証券、医薬品の偽造防止
③安全なWEB参照
④キャッシュレス決済



3. 想定用途

①発行者の認証

対象	具体例
公的書類	証明書、認証シール、住民票、紙幣
一般書類	契約書（保険）、領収書
郵便物	はがき（年金、銀行、配当）

②有価証券、医薬品の偽造防止

対象	具体例
有価証券	商品券、チケット、乗車券、紙幣
医薬品	包装箱、PTP、錠剤、アンプルシール

③安全なWEB参照

・フィッシング防止

④スマホ決済への適用

①発行者の認証

はがき（年金、銀行、配当）

料金後納郵便

親　展

ＸＸＸ－ＸＸＸＸ
ＸＸＸＸＸＸＸＸＸＸ
ＸＸＸＸＸＸＸＸＸＸ
ＸＸＸＸＸＸＸＸＸＸ
ＸＸＸＸＸＸＸＸＸＸ

ＸＸＸＸＸＸＸＸＸＸＸＸ 様

9999-9999999-9999-999

大切なお知らせ

国民年金保険料のお知らせ

差出人
日本年金機構
Japan Pension Service
〒168-8505
東京都杉並区高井戸西三丁目5番24号

お問い合わせ先（宛先不明の場合の返送先）
ＸＸＸＸＸＸＸＸＸＸＸＸ
ＸＸＸＸＸＸＸＸＸＸＸＸ
〒 999-9999
ＸＸＸＸＸＸＸＸＸＸＸＸＸ
ＸＸＸＸＸＸＸＸＸＸＸＸＸ
ＸＸＸＸＸＸＸＸＸＸＸＸＸ
TEL XXXXXXXXXXXXX
ご案内は内側にあります。
裏面（①）からゆっくりていねいに開いてご覧ください。

②

国民年金未納保険料
納付勧奨通知書（催告状）

お客様の国民年金保険料には、右記の納付状況のとおり未納があります。

未納があると、年金を受け取るときに影響があります。**金融機関**または**コンビニエンスストア**で納めてください。

- 納付書がお手元にない場合は再発行します。年金事務所までご連絡ください。
- 経済的に保険料を納めることが難しい場合は、**国民年金保険料の免除申請**を行うことができます。詳しくは裏面をご覧ください。

このお知らせは、平成30年1月12日現在のデータに基づき、平成29年11月以前に国民年金保険料の未納がある方にお送りしています。

すでに保険料を納めた方や免除申請中の方にも、行き違いでこの通知書が届く場合がありますのでご了承ください。

・免除申請中の方への審査結果は、この通知書とは別に届きます。

お客様の基礎年金番号は 9999-999999 です。

平成●●年●●月より国民年金保険料の納付や免除申請手続きの電話・戸別訪問・文書によるご案内は、業務を委託する下記の事業者から行います。

「○○○○○○○」
お問い合わせ先　○○○○-○○-○○○○
営業時間　○○：○○～○○：○○

納付状況

年度	未納月数	未納金額
ＸＸ Z9	Z9カ月	¥¥,¥¥¥,¥¥9円
	4 5 6 7 8 9 10 11 12 1 2 3	
	ＸＸＸ ＸＸＸ ＸＸＸ ＸＸＸ	
年度	未納月数	未納金額
ＸＸ Z9	Z9カ月	¥¥,¥¥¥,¥¥9円
	4 5 6 7 8 9 10 11 12 1 2 3	
	ＸＸＸ ＸＸＸ ＸＸＸ ＸＸＸ	
年度	未納月数	未納金額
ＸＸ Z9	Z9カ月	¥¥,¥¥¥,¥¥9円
	4 5 6 7 8 9 10 11 12 1 2 3	
	ＸＸＸ ＸＸＸ ＸＸＸ ＸＸＸ	
合計	未納月数	未納金額
	Z9カ月	¥¥,¥¥¥,¥¥9円

・納付期限が到来していない月は、空白としています。

納付状況の記号説明

＊	未納		
A,B,H,¥	納付済	サ	学生納付特例
L,R,Y,Z	全額免除	セ	納付猶予
ア,チ,ヒ	半額,3/4,1/4免除（未納）	＋	第３号納付
イ,ツ,フ	半額,3/4,1/4免除（納付済）	－	納付期限２年経過(注)
／	厚生年金保険・共済組合に加入していた期間または２０歳前の期間		

(注) 納付状況に関わらず「－」と表記しています。

年金加入状況

お客様の現在までの年金加入月数は、次のとおりです。

・共済組合に加入していた月数は含んでいません。
・ご不明な点は、年金事務所にお問い合わせください。

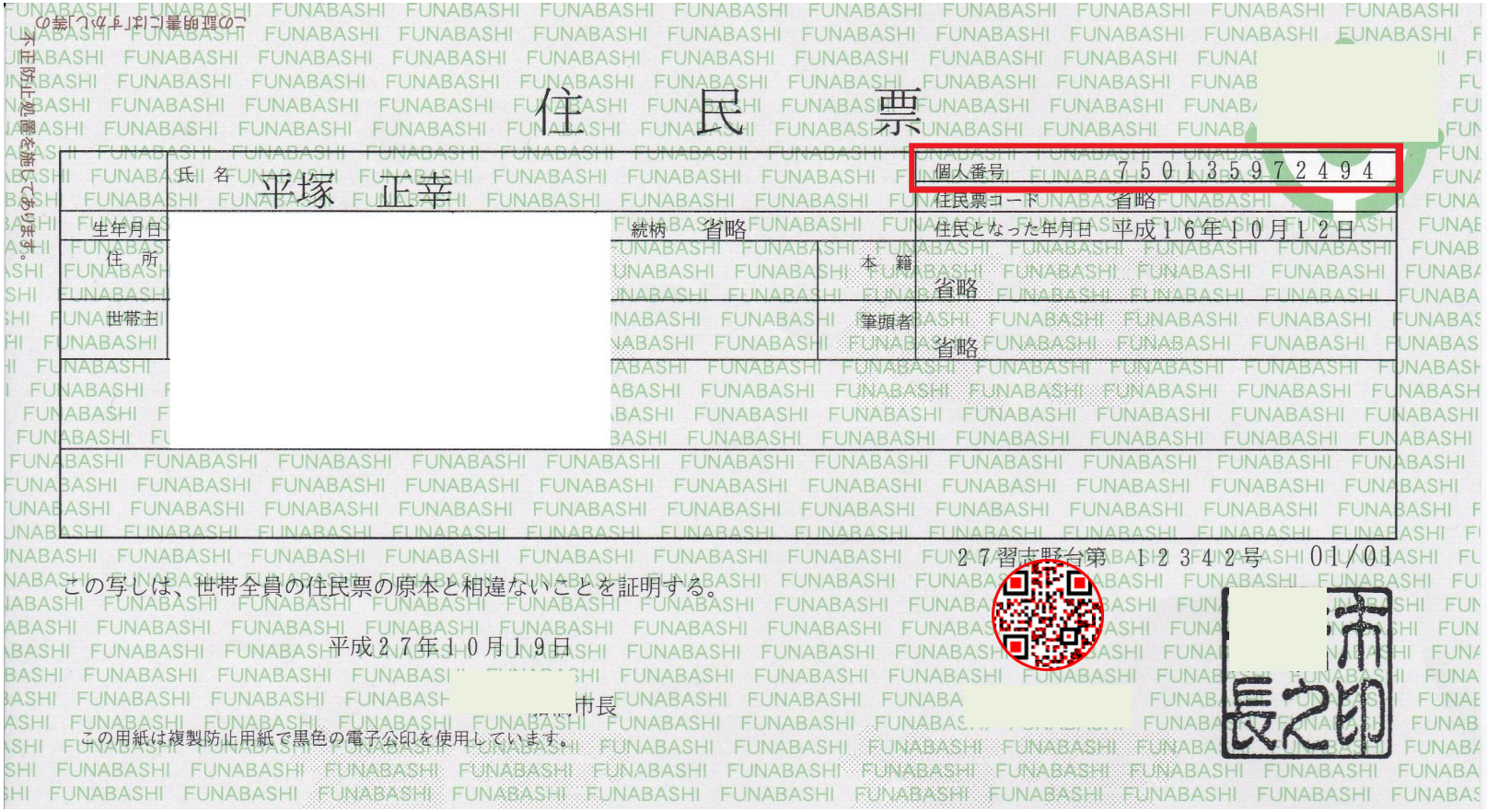
国民年金						
全額納付月数	法定免除・全額免除月数	4分の1納付月数	半額納付月数	4分の3納付月数	学生納付特例月数	納付猶予月数
ZZ9カ月	ZZ9カ月	ZZ9カ月	ZZ9カ月	ZZ9カ月	ZZ9カ月	ZZ9カ月

厚生年金保険加入月数計	船員保険加入月数計	合計
ZZ9カ月	ZZ9カ月	ZZ9カ月

署名対象：タイトルと基礎年金番号と発行日
署名　　：日本年金機構

公的書類

①発行者の認証



住　民　票

氏　名　平塚　正幸

個人番号　７５０１３５９７２４９４

住民票コード　省略

生年月日

住　所

続柄　省略

住民となった年月日　平成１６年１０月１２日

本　籍　省略

世帯主

筆頭者　省略

２７習志野台第　１２３４２号　０１／０１

この写しは、世帯全員の住民票の原本と相違ないことを証明する。

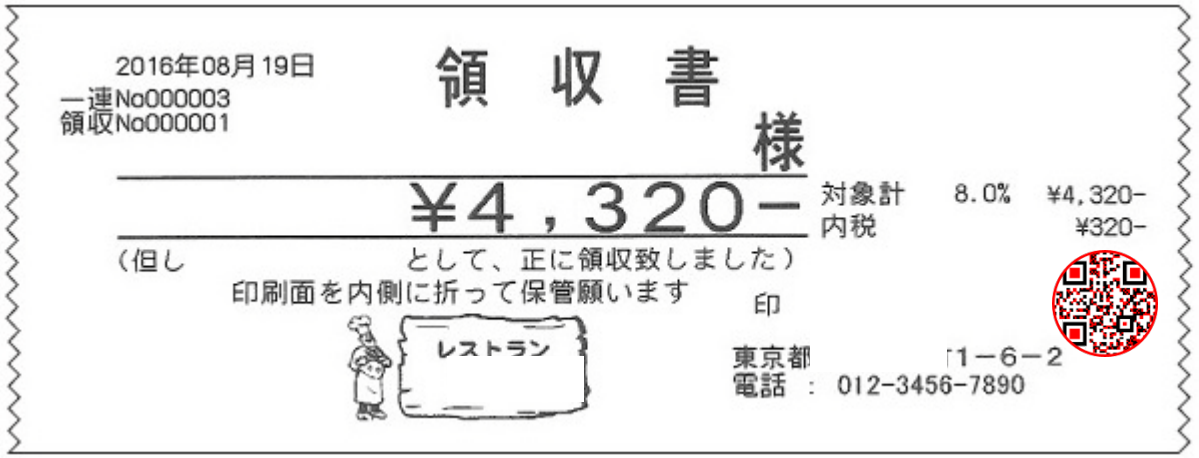
平成２７年１０月１９日

市長

この用紙は複製防止用紙で黒色の電子公印を使用しています。

署名対象：タイトルと個人番号と発行日
署名　　：発行市役所

①発行者の認証



署名対象：宛先、金額と発行日、シリアル番号
署名　　：発行会社

②有価証券の偽造防止

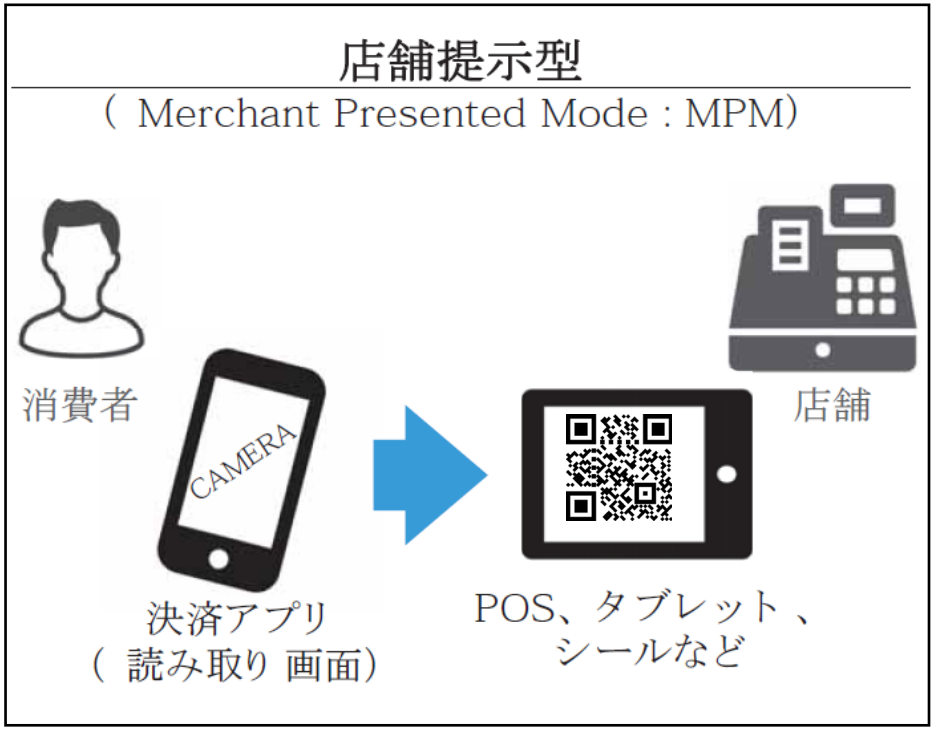
・紙幣の例

・専用機（自販機）（赤外線）で読取り、認証
・コピー検出

署名対象：金額とシリアル番号
署名　　：発行銀行

スマホで読取り、認証

④スマホ決済への適用



・アプリケーションは変更不要
・電子署名の認証はOS部が実施

TCODE
テララコード研究所

ご清聴ありがとうございました。

寺浦　信之
Nobu@TCodes.jp