L-002

QR コードを用いた安全な個人情報閲覧システム

A Secure System using Quick Response Code
for Viewing Personal Data

山内 俊明† 関 靖夫†
Tosiaki Yamanouchi Yasuo Seki

1． まえがき

近年，生活を支える各種サービスがインターネットを介しても受けられるようになり，交通の不便な地域の住民・外出が困難な高齢者・仕事が忙しいビジネスマンなど多くの人々がその恩恵を受けている．

当然，サービスを提供する側，特に個人情報を扱う企業,行政機関,医療機関などでは，独自のセキュリティガイドラインを設け,漏洩に対する厳格なセキュリティ対策が実施されている．しかし，「個人情報の保護に関する法律」（個人情報保護法）が 2005 年 4 月に施行されてからは，世間の関心や消費者の意識が急速に高まった．その結果，この法律に違反もしくは関連する不祥事を発生した機関は，法的責任に加えて解約・利用停止などの経済的損失を受け，最悪の場合には業務や機関そのものの存続が危うくなるケースも十分考えられるようになった[1]．このような状況下において，セキュリティ対策に十分な投資が難しい中小企業や非営利機関では，個人情報の活用が危機に瀕しているといってもよいであろう．

そこで，公開鍵暗号と QR コードを組み合わせた個人情報閲覧システムを提案する．本システムは，携帯電話を暗号解読用端末として利用することにより，パソコンや専用端末で個人情報を閲覧している際の後方からの覗き込みやログ等からの情報漏えいを抑止することができる．また，仕様が公開され，かつ無料で利用することができる QR コードと公開鍵暗号の効果的な利用により，比較的安価にシステムを構築することが期待できる．

2．提案システム

本稿では，安価でかつ十分な安全性が期待できる情報閲覧システムを提案する．システム構成は，各ユーザが閲覧対象とする情報が保管されているサーバ及びインターネットで接続されたユーザ端末群である．実際に情報を閲覧する際のデータの流れ，及び本システムの安全性の要となる鍵管理方式の詳細について述べる．

2.1 情報閲覧時のデータの流れ

信頼性の高いユーザ認証を経て，ユーザ端末からのデータ送信要求が正当なものであると判断された場合のデータの流れは，次の通りである（図１）．

(1)当該データに対して，当該ユーザ向けの公開鍵としてサーバに登録してある鍵を用いて暗号化を行う．

(2)暗号化されたデータを QR コード化し，当該ユーザ端末にネットワークを介して送信する．

(3)ユーザ端末側で受信した QR コードは，端末画面上に表示される．

(4)当該ユーザは，所有の携帯電話を用いて，撮影及び QR コードの復号を行う．

(5)QR コード化されていたデータに対し，当該携帯電話のみが知りうる秘密鍵を用いて公開鍵暗号の解読を行い，サーバに要求していた情報を無事取得する事ができる．

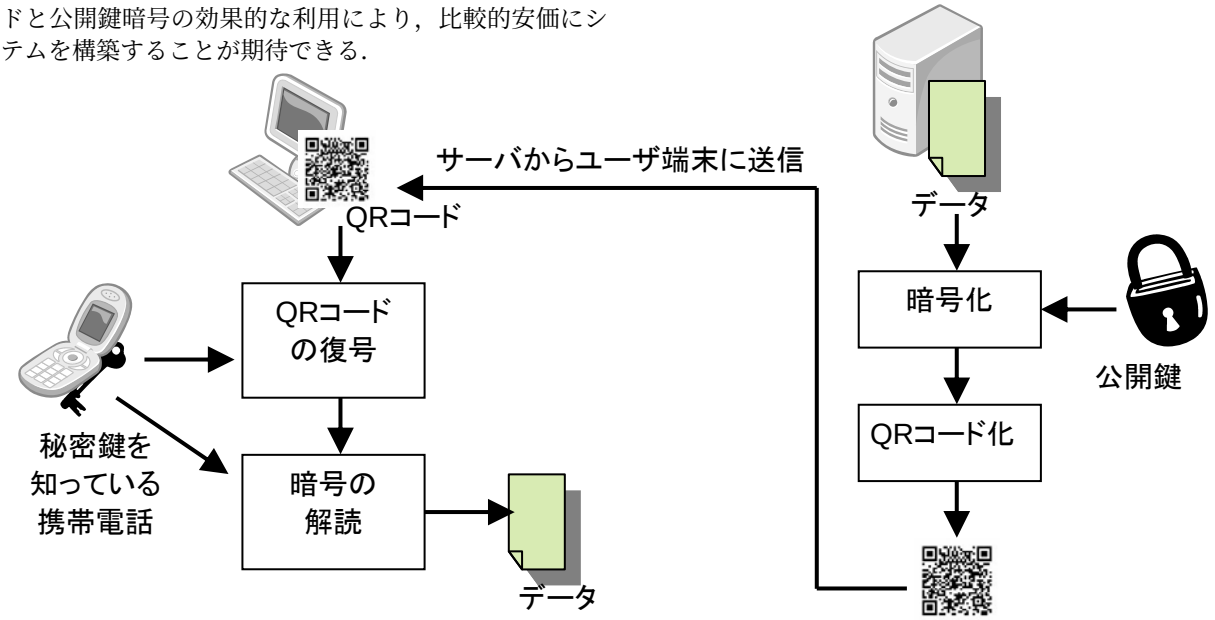


図1 情報閲覧時のデータの流れ

† 神奈川工科大学, Kanagawa Institute of Technology

2.2　鍵管理方式

公開鍵暗号は，暗号化する際の鍵（公開鍵）と解読する時に必要となる鍵（秘密鍵）が異なるため，一般には共通鍵方式よりも安全性が高い．しかし，公開鍵の受け渡しの際に発生する問題として，成りすましがある．これは，正当な情報の受け手とは異なる者が作成した公開鍵を，正当な受け手の鍵として送り手に誤認させることである．このような問題を解決するために一般に利用される方策として，PKI(Public Key Infrastructure)がある．認証局が電子署名をすることにより，公開鍵と所有者の正当性を証明する手法であるが，手続きの手間や費用の面に問題がある[2],

そこで，安価な鍵管理方式として，ワンタイムパスワードのように情報閲覧時に毎回異なる鍵ペアの生成・公開鍵の登録を行うことを提案する．具体的には，次のようになる．

(1)携帯電話上に作成したアプリケーション（以後，携帯アプリ）により，サーバとの間で信頼性の高いユーザ認証（ワンタイムパスワードなど）を行う．

(2)認証に成功したら，携帯アプリ内で新規に公開鍵暗号のペア鍵を生成し，公開鍵をサーバに送り，通信路を閉じる．

(3)直ちに，端末からサーバに対してユーザ認証を行った後，必要な情報を QR コードとして取得する．携帯アプリで QR コードの復号・暗号の解読が行われる時に，(2)で作成された最新の秘密鍵が利用される．

3．適用例

提案方式の有効性を確認するために，実際に個人情報のサンプルを用いて暗号化した QR コードを作成した．サンプルとして用いたデータは，表１に示すように大学等の教育機関内で発生する個人情報である．提案手法により暗号化された QR コードと暗号化せずにそのまま QR コード化したものを図２に示す．また，これらの QR コードを携帯電話で認識した結果を図３に示す．提案方式で暗号化された QR コードは，携帯電話で認識すると暗号化されたバイナリデータとして復号されることが確認できる．当該バイナリデータについては，秘密鍵を用いて解読できることを確認した．

4．むすび

本稿では，安価に実現できる安全な個人情報閲覧システムを提案した．提案方式は，携帯電話を暗号解読端末として利用することにより，閲覧時の後方からの覗き込みや端末ログからの情報漏洩を抑止することができる．採用した公開鍵暗号の問題点である公開鍵の管理方式は，アクセスごとに携帯電話から新しい公開鍵を送ることにした．これにより，携帯電話の機種変更などにも柔軟に対応できると考えられる．

参考文献

[1] 岡村久道,"個人情報保護法の知識",日本経済新聞社,2005

[2] 坂本千鶴,G. De Marco,多々内允晴,"携帯電話網を用いた公開鍵交換システム",FIT2007(第 6 回情報科学技術フォーラム), Sep.,2007,pp.45-48

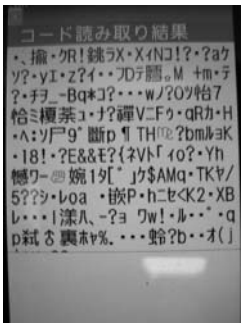
表１　使用した個人情報のサンプル

学籍番号 0800999 山田太郎さんのレポート提出状況は以下の通りです(2008 年 6 月 30 日現在)。
第 1 回 採点済み
第 2 回 採点済み
第 3 回 未提出
第 4 回 再提出
第 5 回 採点済み
第 6 回 採点済み
第 7 回 採点済み
第 8 回 呼び出し
第 9 回
第 10 回

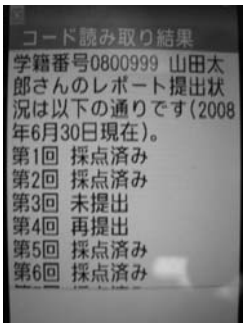
(a)　提案手法により暗号化された QR コード

(b)　暗号化しない場合の QR コード

図２　サンプルデータに対する QR コードの例



(a) 図 2(a)の認識結果



(b) 図 2(b)の認識結果

図３　携帯電話による QR コードの認識結果