2D-03

DSQR コードを利用した Web システムにおける相互認証

氏　名　先名　健一†
所　属　合同会社ＱＲテクノロジー‡

１．はじめに

最近、フィッシング攻撃やファーミング攻撃などと呼ばれる手口でユーザを偽サイトへ誘導し、ユーザの個人情報を詐取する不正行為が多発している．その有効な対策として、二経路認証が実用化されている[1]．二経路認証は取引を行っている経路とは別の経路を併用して認証を行う手法である。また別の対策として、Web ブラウザに ID、パスワード(PW)を入力する欄を設けてサーバとクライアント間の相互認証をすることで、不正を防止するプロトコルも提案されている[2]．一方、EC サイトでのクレジット決済に使われる本人確認としては、VISA、MasterCard、及び JCB が推奨している PW による「３Ｄセキュア」という本人認証システムがある．この３Ｄセキュアには、EC サイトの真正性を確認するための機能として「パーソナルメッセージ」があり、これを使い相互認証を実現している．

上記の手法を含め、これまでの相互認証手法においては、ユーザ ID と PW はサーバ側で管理しているため事前にその登録が必要であり、利便性に課題がある．またサーバからの情報漏洩リスクも常に存在する。実際、サーバ攻撃によって PW の大量の流出被害が度々発生している．

本研究で提案する相互認証システムの特徴は、ID と PW をサーバ側で保管・管理する必要がないことにあり、それは、QR コードにコード自身の真正性の判定機能と QR コード所有者の個人認証機能を付加したコード（以下、DSQR コード）を用いることで実現している．また、提案システムは、公開鍵を介してサーバ側の所有する DSQR コードデコーダとユーザ所有の DSQR コードが紐付いていればどのサーバとも自由な相互認証を可能にするなど利便性も高い．提案手法によりフィッシング攻撃に耐性のある利便性の高い相互認証システムの構築が可能となる．

２．DSQR コードについて

DSQR コードは、楕円曲線デジタル署名アルゴリズム（以下、ECDSA）によって生成される署名値を XOR で QR コードに埋め込んだものである．また QR コードの復号アルゴリズムにはリードソロモン(RS)符号による誤り訂正技術が使われており、QR コードリーダで DSQR コードを読み取ったとしても、上記署名値が復号結果として出力されることはない．署名値を出力するには DSQR コード専用のリーダが必要になる．また、DSQR コードと DSQR コードリーダが同じ公開鍵を用いて構成されていないと上記署名値を正しく読めない．

次に DSQR コードの性質を簡単に示す．

・秘密でない情報は QR コードリーダで読める．
・ECDSA によりコード自身の真正性が判定できる．
・コード所有者の PW やパスフレーズを格納し認証する機能がある．PW の解読には楕円曲線離散対数問題（以下、ECDLP）を解く必要がある．
・秘密の言葉シークレットワード（SW)が格納できる．
・各々の認証はオフラインにおいて実行できる．

DSQR コードは相互認証だけでなく対象物の真贋判定などにも利用することができる．

３．DSQR コードを用いた相互認証

今回の相互認証実験で用いた DSQR コードは、7H 型の QR コードをベースに、160bit 鍵長の ECDSA を使い、ユーザの PW(160bit 長まで可)とサーバの真正性確認用の SW を格納している．SW は、ユーザが設定する 18Byte までの日本語や英数字記号から構成され、XOR で DSQR コードに埋め込まれている．なお、ECDSA の署名値 160bit ×２も同様に DSQR コードに埋め込まれている．

前述したように、DSQR コードをスマートフォンの QR コードリーダアプリで読み取ると、秘密でない情報データのみが表示される．SW は２次元的コードにランダムに埋め込まれているため、SW の情報エントロピーは非常に大きく、ブルートフォース攻撃等による解読は困難である．

ここでは、DSQR コードを用いた相互認証について２つの例を示す．ただし、ECDSA の秘密鍵及び DSQR コードリーダは Web サイトの運営組織、或いはカード発行会社等が厳重に保管するものとする．

（１）Web サイトとユーザの相互認証

図１は相互認証システムのイメージ図であり、図２は相互認証の実験に用いた DSQR コードである．実験は、サーブレットトレーラとして

Mutual Authentication in the Web system by using DSQR code
†Ken-ichi Sakina
‡QRTechnology LLC

Tomcat7 を用い、ローカルサーバで行った.

以下、図１に従って認証実験のプロセスを概説すると、まず、クライアントは Web サイトの認証ページの入力フォームからユーザ所有の DSQR コードを送信する. Web サイトは受信した DSQR コードを専用リーダで読み取り、抽出した SW をクライアントに返す. 受信した SW が正しいとき、Web サイトの真正性が確認される. 次に、クライアントはユーザの ID などの個人情報と PW を送信する. Web サイトは受信した PW と DSQR コードに格納されている PW とが一致するかを判定する. 一致した場合、ユーザは DSQR コード所有者本人であることが確認される. 以上より、Web サイトとユーザとの相互認証が成立する.

ここに提案の相互認証システムは、例えば、Web サイトへのログインに利用することができる. この場合、DSQR コードは、Web サイトを運営する組織において生成し、Web サイト利用者に配布しておく.

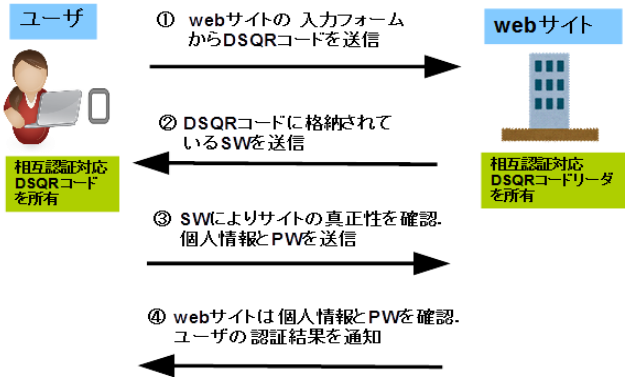

図１　Web サイトにおける相互認証

==========

情報データ：先名健一　0123456******

SW　：私の情報保護

PW　：S0123456789

==========

図２　実験で用いた DSQR コード

（2）EC サイトとユーザとの相互認証

ここで提案する相互認証は、従来のクレジット決済のようにカード番号を入力する代わりに、クライアントは DSQR コードを送信し、EC サイトの真正性を確認してから顧客の PW を送信する.

以下、図３を元に説明すると、顧客は購入する商品を選択した後、クライアントは顧客所有の DSQR コードをオンラインショップに送信する. オンラインショップでは、通常の QR コードリーダを使い DSQR コードからクレジットカードの種類と ID を読み取り、カード発行会社に転送する. カード発行会社は DSQR コードリーダを使い DSQR コードから秘密情報であるカード番号・有効期限を読み取りそれを顧客に送信する. 顧客は、受信したカード番号・有効期限と顧客が所有するクレジットカードのカード番号・有効期限とを照合する. 照合が一致するとき、クライアントは顧客の PW を送信する. カード発行会社は受信した PW と DSQR コードに格納されている PW を照合し、認証結果をオンラインショップに通知する.

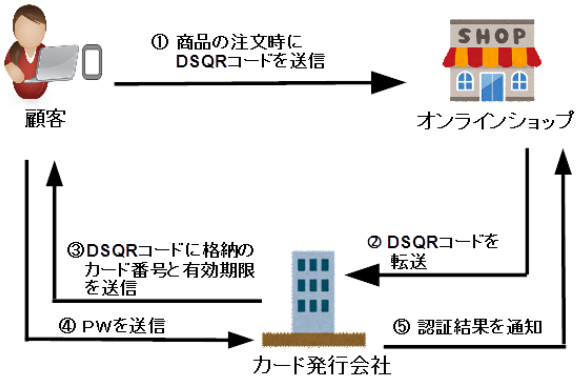

図３　EC サイトにおける相互認証

４．まとめ

本研究は、DSQR コードという全く新しい２次元コードを使う相互認証を提案したもので、以下の特徴をもっている.

① サイトは PW を保管・管理する必要がない.
② 偽サイトを簡単に見破ることができる.
③ 手軽に相互認証システムを構築できる.

このうち、①は従来の個人認証にはない新しい技術で、サイトに個人認証用の情報を事前に登録する必要がないため、サイト運営者の利便性は高く、また、ユーザにも個人情報保護の観点から安心感を与えるものである.

参考文献

[1]藤井治彦ほか：電話網の発信者番号通知を利用した本人認証方式, 情報処理学会論文誌, Vol.54, No.2, pp.992-1001(2013).

[2]https://www.rcis.aist.go.jp/special/MutualAuth/files/papers/MutualAuth-SCIS2008.pdf