LD-002

携帯電話とプロキシサーバを活用した 個人認証・個人情報伝送モデルの提案

Proposal of User Authentication and Personal Information Transfer Model by Utilizing Mobile Phones and a Proxy Server

田中 充† 勅使河原 可海‡

Michiru Tanaka Yoshimi Teshigawara

1． はじめに

現在，個人の利用者がネットワーク上のサービスを受けるために用いる多くの個人認証方式は，依然として固定パスワード方式であることが多い．しかし，1 人当たりのユーザアカウント数は増大し続ける傾向にあり，パスワード忘れの問題も深刻になりつつある．一方，IC カードや USB キーなどのハードウェアトークンを活用した個人認証方式が安全性を高める手段として着目されている．

しかし，これら従来の方式では，導入に手間やコストがかかるものが多い．また，一部の方式では導入が容易でもキーロガーなどによる認証情報の盗聴の問題がある．また，Web 上で個人情報の入力が求められる場合，住所，電話番号，e-mail など同様の情報であるにも関わらず，何度も同じ情報を入力するケースが多々見受けられる．

こうした問題を背景に，筆者らは，これまで携帯電話の２次元コードリーダを活用した個人認証方式 SUAN(Secure User Authentication with Nijigen code)を実証評価し，さらにその拡張型としての個人情報漏洩確率を低減させることが可能な個人情報伝送モデルを考案してきた[1][2][3].

これらの方式は，ブラウザのセッションと関連付けた二次元コードを表示させて，それを携帯電話で読み取り，携帯電話の個体識別 ID と PIN コードおよび読み取った二次元コードのデータなどを組み合わせたハッシュ関数を実行した結果とともに，ユーザ名などの情報を付与させ，それを認証サーバや個人情報管理サービスプロバイダのサーバ上で検証させた上で，Web アプリケーションなどに結果を伝達するものである．

この利点として，(1)個人認証を利用するために，新たなソフトウェアやハードウェアを利用者に要求しないこと，(2)伝達する情報が比較的信頼のおけるキャリアネットワーク経由であるため，スパイウェアなどによる情報漏洩のリスクを低減できること，(3)２次元コードを読み取るだけでよいので簡便な手順で認証がとれること，(4)迂回して情報の伝達ができるため，匿名性が保証できること等を挙げられる．

しかしながら，その方式を採用するアプリケーション側に，対応したプログラムを組み込む必要があるため，既存のシステムでの利用が即座にできないという問題があった．

本稿では，一般利用者が既存の Web アプリケーションなどで提供されるネットワークサービスに対して，個人認証および個人情報伝送を安全に簡便に行うためのシステムのモデルについて提案し，その有効性について考察する．

†岩手県立大学ソフトウェア情報学部, Faculty of Software and Information Science, Iwate Prefectural University

‡創価大学工学部, Faculty of Engineering, Soka University

2．提案する個人情報伝送モデル

2.1 基本コンセプト

我々がこれまで提案してきた携帯電話の２次元コードリーダを活用した認証方式や個人情報伝送モデルをより広範囲に適用させるには， Web アプリケーションの認証として広く用いられている固定パスワード方式を既存のシステムの修正なしに実現することが重要となる．これを実現するために Web プロキシサーバのフィルター拡張機能を活用したモデルを提案する．

SUAN では，Web アプリケーションが認証サーバに対してワンタイムの２次元コードの発行要求を行い，Web ブラウザ上に表示させ，それを携帯電話の２次元コードリーダで読み取って認証をとっていた．

そこで，提案方式では，利用対象の Web サイトにアクセスする際に，２次元コードを発行する HTML や JavaScript を元ページに埋め込んだり，必要に応じてあらかじめ登録された個人情報を埋め込んだりすることが可能な Web プロキシサーバを活用することで対応するというものである．

2.2 システム構成

図１に従来方式のシステム構成を，図２に提案方式のシステム構成を示す．

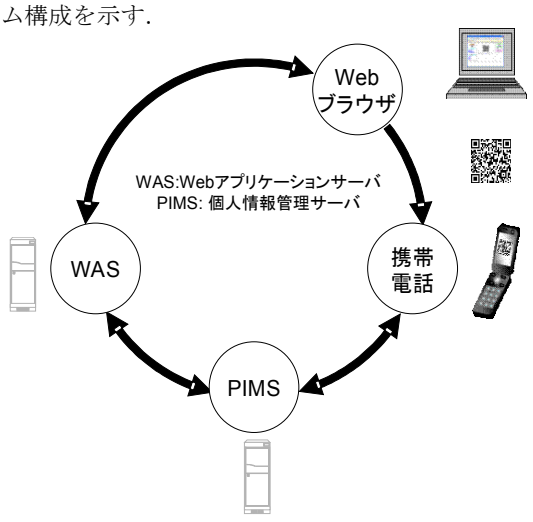

図１ 従来方式である SUAN 等のシステム構成

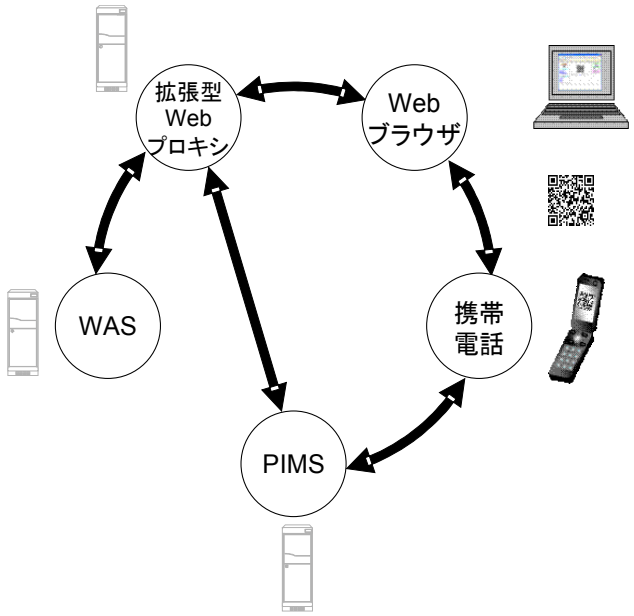

図２　提案モデルのシステム構成

従来方式の特徴としてリング型の情報伝送モデルを挙げることができる．これは個人情報などの重要な情報はWebブラウザから直接的に対象のWebアプリケーションサーバ(以降WAS)に伝送するのではなく，携帯電話のキャリアネットワークを経由して伝送するものである．これを実現するためには，WASに専用のプログラムを組み込む必要があった．

(1) Webブラウザ

利用者がWASにアクセスするためのクライアントソフトウェア．通常，このWebブラウザ経由で個人情報の入力送信されることが多いが，一般利用者などがスパイウェアやフィッシング詐欺による被害を受けるリスクが比較的高い．そのため，提案方式では，重要な個人情報に該当するものはこのWebブラウザを用いて入力しない．このブラウザ上には，携帯電話と関連付けるための２次元コードの表示と，認証後機微情報が除去されたHTMLの表示が行われる．

また，提案方式を採用するにはプロキシサーバの設定のみ必要となる．この設定は，ブラウザの設定経由で行う方法と，直接Webブラウザ上から対象のURLを入力して行う方法の２通り考えられる．前者の場合，一度設定すれば通常通りの操作で認証機能が利用可能である．一方，キオスク端末などブラウザのプロキシ設定を操作できない場合は後者が有効である．

(2) 携帯電話

利用者自身が保持する携帯電話．２次元コードリーダが搭載されており，提案方式は携帯アプリケーションから利用する．携帯アプリケーションでは，トークンの読み取り，認証のためのハッシュ関数の実行，個人情報の入力・保存が行われる．

(3) WAS (Web Application Server)

パスワード型の認証方式を用いるWebアプリケーションサーバ．本稿では，既存のWASのことを想定しており，提案モデルを利用するために新たに内部プログラムの修正を必要としない．

(4) PIMS (Personal Information Management Server)

携帯電話とWebブラウザのセッションの関連付けをするための機能（トークン生成，検証）と暗号化された個人情報を保存する．

(5) 拡張型Webプロキシサーバ(EWPS: Extended Web Proxy Server)

通常のWebプロキシサーバの機能に加えて，２次元コード表示のためのHTMLの埋め込みやWASから受けた機微情報除去機能を持つ．また，フィッシングサイトに関するブラックリストやホワイトリストを保持することによって，フィッシング対策が可能な機能も持つ．

2.3　処理手順

SUAN等のこれまでの情報伝達モデルを，新たに提案するモデル上に適用させるには，次の工夫が必要となる．

- WASは内部プログラムの修正変更ができたいため，それ以外の構成要素上で携帯電話とブラウザを関連付けするためのワンタイムトークン（２次元コード）を出力すること．
- WASに送信されるHTTPリクエストに，固定パスワードや個人情報に関するリクエストパラメータを挿入すること．

EWPSを活用して，上記を実現するための手順を次に示す．

(1) Webブラウザのセッションと携帯電話の関連付け

STEP1：Webブラウザから WASへのアクセス要求とトークンの表示(図３)

STEP1-1 WebブラウザからEWPSを経由して WASへのアクセスを要求する．EWPSとWASはクッキー情報を用いWebブラウザのセッションIDを保持する．

STEP1-2 WASからEWPSに対して要求されたHTMLのレスポンスを行う．

STEP1-3 EWPSは，PIMSに対してトークンの発行要求を行う．

STEP1-4 PIMSは，指定されたセッションIDとWASの識別子などを元にワンタイムのトークンを生成し，DBに格納する．

STEP1-5 PIMSからEWPSへ生成したトークンを送信する．

STEP1-6 取得したトークンを元に２次元コードの発行のためのHTMLを生成し，WASから得られたHTMLレスポンスに埋め込む．

STEP1-7 トークン出力用HTMLタグを埋め込んだHTMLをWebブラウザに返却する．

STEP1-8 Webブラウザ上に得られたHTMLを出力する．

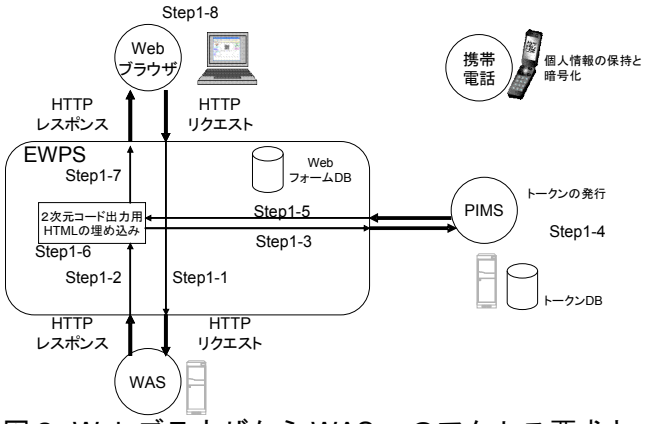

図３ Web ブラウザから WAS へのアクセス要求とトークンの表示

STEP2：携帯電話のトークンの読み取りとトークンの検証・PIMS における Web ブラウザと携帯電話の関連付け(図４)

STEP2-1 Web ブラウザ上に表示されたトークンを携帯電話で読み取る．

STEP2-2 携帯電話上で，トークン，携帯電話の個体識別 ID，PIN コードとハッシュ関数を実行する．

STEP2-3 携帯電話から PIMS に関数実行前後のトークンを送信する．

STEP2-4 PIMS 上で，携帯電話から得られたトークンと同一のトークンを PIMS 上のトークン DB から探索する．対象のトークンが存在した場合，トークンの有効期限範囲内か検証する．対象のトークンが PIMS 上のトークン DB 上に存在しない，あるいは存在してもトークンの有効期限範囲外であった場合，携帯電話と Web ブラウザの関連付けが失敗した際の処理を行う．

STEP2-5 検証成功の場合，Web ブラウザと携帯電話を関連付けるために，Web ブラウザのセッション識別子と WAS 識別子および携帯電話のセッション識別子と関連付けしたレコードをトークン DB に記録する．

STEP2-6 Web ブラウザと携帯電話を関連付けした結果を EWPS に通知する．

STEP2-6' Web ブラウザと携帯電話を関連付けした結果を携帯電話に通知する．

STEP2-7 必要に応じて携帯電話からユーザ名とパスワードなどを EWPS の公開鍵を用いて暗号化し，PIMS に送信保存しておく．

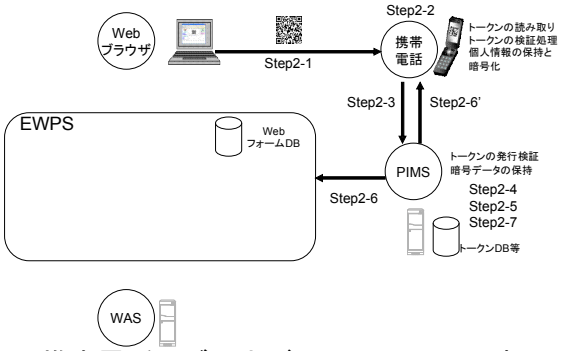

図４ 携帯電話とブラウザセッションの関連付け

(2) 個人認証方式

(1)の Web ブラウザのセッションと携帯電話が関連付けられた後に次のようなステップで個人認証を実現する．

STEP3: パスワード認証処理(図５)

STEP3-1 ユーザが Web ブラウザを用いて，WAS が提供する Web サイトの認証ページへ移動し，ユーザ名とパスワードを空の状態にしたままフォームの送信ボタンをクリックし，EWPS にアクセス要求を出す．

STEP3-2 EWPS は，対象の Web サイトが既に登録された Web サイトと判別できる場合，携帯電話から送信されたユーザ名とパスワード情報を復号した上で，その Web サイトで用いられるリクエストパラメータに対して，情報を付与する． なお，この手順はあらかじめ STEP2 で行ってもよい．

STEP3-3 EWPS から WAS に対して認証情報が付与された HTTP リクエストを送信する．

STEP3-4 WAS から HTTP レスポンスを EWPS に返す．

STEP3-5 HTTP レスポンスを解析し重要な個人情報がないか探索し，もし存在すれば削除する．その一方で，そこで削除された情報を携帯電話の方に送信して，大体表示させてもよい．

STEP3-6 EWPS から Web ブラウザに機微情報を削除した内容の HTTP レスポンスを返す．

(3) 個人情報の伝送方式

基本的にはパスワード認証処理と同様な方式で行う．パスワード認証方式の多くの場合，リクエストパラメータは，ユーザ名とパスワードのみであるので，予測は容易であるのに対して，ユーザ登録のための Web フォーム上に入力される情報は，パラメータ数に決まりがないことが多いため，携帯電話上で登録される個人情報（住所，電話番号，クレジットカード番号）とリクエストパラメータをマッチングするスキーマ変換情報が必要となる．携帯電話上に登録されていない情報も含まれることが考えられるが，この場合，ユーザは，フォームに何らかの情報を入力することで対応する．この情報は基本的に手動で登録される．

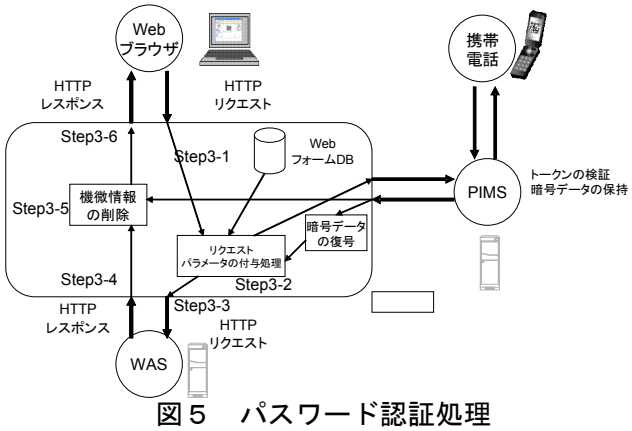

図５　パスワード認証処理

3. 考察

(1) セキュリティ

個人所有の PC は，企業で用いる PC と比較して，管理が手薄になる傾向にあるため，スパイウェアの感染率が比較的高く，そのために個人情報漏洩のリスクが比較的高いものと考えられる．その一方で，企業での利用の場合，同じ空間を他の社員と共有する場合も多く，肩越しに入力している内容を盗み見するショルダーハッキングによる個人情報漏洩の被害も考えられる．

提案方式では，PC 上でユーザ ID，パスワードを入力することなしに，従来のパスワード認証を実現することが可能であり，家庭内で利用する個人所有の PC 及び企業内で利用する PC の双方のセキュリティ環境の改善が期待できる．

携帯電話のセキュリティについては，携帯電話の種類に依存する部分が多いが，一般的に電話帳などの個人情報を記録することが想定されているため，標準の状態で PC と比較して個人情報を保護するための対策がとられているのが一般的である．

また，プロキシサーバを用いているため，ブラックリストやホワイトリストによるフィッシングや DNS キャッシュポイズニングによるファーミングなどへの対策も実現しやすい．さらに，重要な個人情報を削除することが可能なため安全性が高い方式と考えられる．

(2) ユーザビリティ

導入の手間に関しては，利用者に強いるのはプロキシサーバの設定の変更と携帯アプリケーションのインストールと個人情報入力の初期設定である．

既存の Web アプリケーションに対応させるためには，Web フォームのスキーマ変換情報を作成することが必要となるが，単純な個人認証を行うものである場合，ユーザ名とパスワードの２つのリクエストパラメータの情報があればよいので，即座に作成することができる．これは SUAN などのシステムで WAS の内部プログラムを作成しなければならない手間と比較して格段と労力が削減されたものと考えることができる．

また，提案手法を用いれば固定パスワードは一度，登録しておくだけでよく，パスワード忘れの問題を大きく改善できる．

さらに，一度携帯電話上に氏名，住所，電話番号などの個人情報を入力することで，Web 上の類似した個人情報入力の手間を大幅に削減することができる．

(3) 実現可能性

プロキシサーバ経由の SSL/TLS の場合，一般的に通常プロキシ上で盗み見は行わないように設定されるが，例えば DeleGate[4]には MITM モードがあり，これを活用することで提案方式は SSL/TLS を用いたとしても実現させることは可能である．

ただし，JavaScript を用いて送信する認証情報が動的に変わるタイプの場合，同様の処理を EWPS 上で実行するように拡張しなければならないため，対応が困難になることも予想される．

4. 関連研究

類似した方式に Ravi らの方式がある[5]．この方式では，携帯電話からプロキシを活用して個人情報を伝送するモデルを提案しているが，プロキシサーバと携帯電話間の関連付けの手法が固定的であり，さらにブラウザ上のセッションとの関連付けの手法についても，なりすましの面で深く検討されていない．一方，本提案方式では，ブラウザ上から携帯電話への通信に一方向アナログ通信を用いており，さらにブラウザと携帯電話の認証を多対多で実現することができる．また，複数の利用者が EWPS や PIMS を共有して利用できる．

その他，Web のフォームに個人情報を入力する方式として ID Manager がある[6]．これは利用者端末上にソフトウェアのインストールを必要とするものであり適用範囲がせまく，さらに利用者端末上に個人情報を保存しているが，暗号化しているものの，開示される可能性は否定できない．提案方式では，利用者端末上には一切，個人情報の入力を必要としないため，より安全な方式であると考えられる．

5. まとめ

本稿では，個人情報漏洩のリスクの低減とユーザビリティの向上が可能な個人情報伝送モデルに対して，クライアント側，サーバ側に対して変更を加えることなく，広く既存の Web アプリケーション上で適用可能な方式について述べ，その実現可能性と有効性についての考察を行った．

今後は，提案方式のシステムを開発し，実証評価を行う予定である．

謝辞

本研究のソフトウェア開発は，独立行政法人情報処理推進機構から 2007 年度第 I 期未踏ソフトウェア創造事業として支援を受けています．

参考文献

[1] 田中充，勅使河原可海：携帯電話の 2 次元コードリーダを活用したユーザ認証方式とその個人入力機構，電子情報通信学会（CSS2005），pp.691–696, 2005.10

[2]田中充，勅使河原可海：携帯電話を活用したリング型情報伝送モデルによる Web アプリケーションの個人情報保護方式，電子情報通信学会論文誌 D，Vol.J90-D, No.2, pp.373-383, 2007.2

[3] Michiru Tanaka and Yoshimi Teshigawara, "A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones", Springer Lecture Notes in Computer Science, Vol.4298, pp.225-236, 2007.3

[4] Yutaka Sato: DeleGate, http://www.delegate.org

[5] Ravi Chandra Jammalamadaka, Timothy van der Horst, Sharad Mehrotra, Kent Seamons, and NaliniVenkatasuramanian: “Delegate: A Proxy Based Architecture for Secure Website Access from an Untrusted Machine”, 22nd Annual Computer Security Applications Conference (ACSAC), 2006.12

[6] WoodenSoldier Software: ID Manager, http://www.woodensoldier.info/soft/idm.htm