

# ユビキタス性の有る Web アプリケーション認証情報管理システムの提案

研究系卒研 制作系卒研

068105 手塚悠太

(指導教員 速水 治夫 教授)

## 1. はじめに

現在, Web アプリケーションにおける個人認証方式は, ユーザ ID とパスワードの組み合わせによるものが一般的である. しかし, パスワードが短ければ総当たり攻撃で, 長くても意味があると辞書攻撃で敗れられてしまう. 安全性を高めるには, パスワードにランダムな英数記号を用いるしか無いが, 英数記号からランダムに生成したパスワードを覚えることは難しい<sup>1)</sup>. つまり, この方式は本人拒否又は他人許可の二極化しやすいという側面を持っている.

本研究では, ユビキタス性を備え, ランダムパスワードを使用した際の管理・入力負担軽減を図る, 認証情報管理システムを提案する.

## 2. システム概要

本システムでは, ユビキタス性確保のため, Web アプリケーションの形態を採り, 携帯電話を用いて認証を行う. その後, ユーザはサーバへアクセスし, 対象 Web アプリケーションの認証情報の登録・編集・利用が可能となる.

### 2.1 ユーザ登録

本システムのユーザ登録時には, 携帯電話と操作中の PC を結びつけるため, セッションを含んだ QR コードを携帯電話で読み取らせる. その後, 携帯電話からユーザ登録操作を行う. その際, 携帯電話端末製造番号及び SIM カード固有情報 (以下個体識別情報)<sup>2)</sup> を登録する. 本システムへの認証は, この個体識別情報を用いてユーザの識別を行う.

### 2.2 本システムへの認証

本システムへの認証には, 携帯電話を用いた認証システムを採用した. ユーザが本システムへの認証を要求すると, サーバはセッションを確立してログインページを送る. その後, ユーザは携帯電話で iAppli をお起動する. iAppli はモバイルパスワードを生成し, サーバにサーバパスワードを要求, その二つのパスワードを画面に表示する. ユーザはこれの二つのパスワードを見て, ブラウザから入力し, 承認されれば本システムへの認証が完了する.

### 2.3 対象 Web アプリケーションへの認証

ユーザから対象 Web アプリケーションへのログイン要求があると, サーバは対象のログインのログインペ

ージを取得し, 携帯電話から受け取った共通鍵で復号した認証情報を埋め込む. それをクライアントへ送ることで, ユーザはログインボタンをクリックするだけで対象 Web アプリケーションへの認証が完了する.

対象 Web アプリケーションへの認証の流れ図を図 1 に示す.

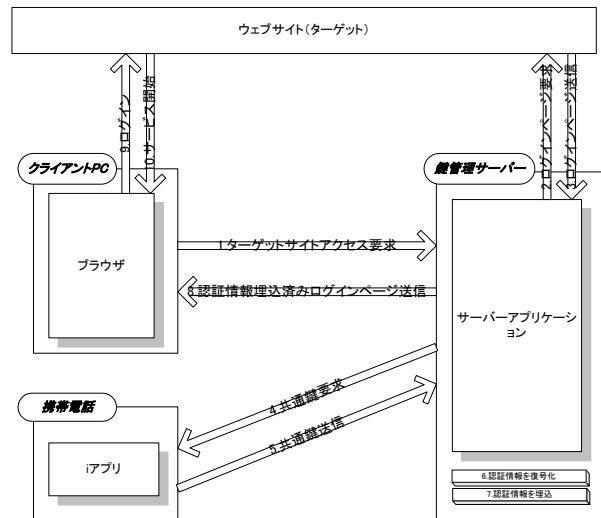


図1 対象 Web アプリケーションへの認証

## 3. 結果

本システムの操作性と機能を評価した. 本システムへの認証に用いられている技術は, モバイルウェブで広く使われている方式であるが, これを PC からの認証の際に応用することで, 携帯電話所持による本人認証を実現することができた. また, ランダムパスワードを用いた場合の入力負担を軽減することができた.

## 4. おわりに

本論文では, 現状の認証情報の管理を, 携帯電話を用いてネットワーク上で一元管理する事で, ユビキタス性とセキュリティを向上させた.

今後は非対応 Web アプリケーションへの対応, 非対応携帯電話端末への対応などを行ってきたい.

## 参考文献

- 1) インターネットユーザーの ID に関する意識についてのアンケート調査

<http://www.nri.co.jp/news/2009/090611.html>

- 2) 契約者固有 ID, Wikipedia

<http://ja.wikipedia.org/wiki/%E5%A5%91%E7%B4%84%E8%80%85%E5%9B%BA%E6%9C%89ID>

