携帯電話向けウェブアプリケーションにおける ユーザ識別認証機能要件に関する分析

小池大生† 武田圭史††金井瑛†† 佐藤直之‡ 市川博基‡‡ 村井純‡‡
慶應義塾大学 総合政策学部† 政策・メディア研究科†† 日本ベリサイン株式会社‡ 環境情報学部‡‡

1 背景

携帯電話からのインターネット上に設置された Web サーバへのアクセスの増化[1]及び各種通信プラットフォームのオープン化に伴い，携帯電話向けコンテンツプロバイダが利用している携帯電話独自のユーザ識別/認証機構に関してセキュリティあるいはユーザのプライバシに関する懸念が声が高まっている．本研究では，主に携帯電話からのアクセスを想定した Web アプリケーションが備えるべき識別認証のあり方についての検討の前提とするべく，携帯電話向け Web サービスに関する様々なステークホルダーからの要件を整理し，その課題等について分析する．

2 現行の識別認証機能について

携帯電話向け Web アプリケーションにおいては HTTP セッションにおけるユーザ識別認証要素として，PC 向けの Web サイトで広く利用されている Cookie が利用されていない．これは携帯電話に搭載されている多くの Web ブラウザに Cookie を送受する機能が実装されていないことによる．

このためユーザを識別する必要のある携帯電話向け Web アプリケーションサイトでは，回線契約または利用機器を一意に特定することのできる固有の識別子を用いてユーザの識別・認証やセッション管理が行なっていることが多い．

An Analysis of User Identification and Authentication requirements in Web Applications for Mobile Phone.
Hiroki KOIKE†, Keiji TAKEDA††, Akira KANAI††, Naoyuki Sato‡ Hiroki ICHIKAWA‡‡ and Jun MURAI‡‡
†Faculty of Policy Management, Keio University
††Graduate School of Media and Governance, Keio University
‡‡Faculty of Environment and Information Studies, Keio University
5322 Endo Fujisawa Kanagawa, 252-8520, Japan
/koiking, keiji, kanai, jun/@sfc. wide. ad. jp
‡VeriSign Japan K.K.
2-8-1 Yaesu Chuo-ku Tokyo 104-0028 Japan
sato@verisign.co.jp

上記目的で使用される識別子は概念上，回線契約毎に割り当てられている「回線契約 ID」と端末毎に割り当てられている「端末 ID」の二種類に分類することができる．

「回線契約 ID」は，利用している回線契約につき割り当てられる識別子であり，原則として変更することが出来ない．（サービスの解約・再契約による変更は可能）回線契約 ID は携帯通信事業者からゲートウェイを通過する際に HTTP プロトコルヘッダ内に付与され，ユーザ側からは通信相手のサイト毎に送信の可否を選択することはできない．この ID は通信事業者においてデフォルトで送信する設定となっているか，送信設定を許可することが強く推奨されており，特に意識しない限り一意の ID を送信する状態で利用されることが多いと考えられる．

「端末 ID」は，携帯端末または SIM カードの製造番号であり，機種変更を行うことで ID も変更される．端末 ID の送信に関しては通信事業者により都度送信可否をユーザに確認するもの，端末 ID を使用しないもの，常に送信するものがある．日本国内の主要３通信事業者で使用する識別子には以下のようなものがある．

通信事業者	回線契約 ID	端末固有 ID
Docomo	i モード ID	FOMA カード製造番号
		FOMA/MOVA 端末製造番号
au	EZ 番号	—
SoftBank	ユーザ ID	製造番号

[表 1]各携帯電話通信事業者で使用可能な識別子の名称

以下ではこうした識別子が現在の形態で使用されるに至った背景として考えられる各ステークホルダー毎の識別認証に対する機能要件について分析する．

a)青少年保護の観点からの要件（コンテンツプロバイダ等）

携帯電話向け Web サイト利用を通じて犯罪などに巻き込まれるなどの問題が社会問題化し，青少年の保護を目的として有害サイトにつき，フィルタリングを行うべきとの意見が高まった．これを受けて，著名なコミュニティサイトでさえもフィルタリングの対象となるおそれもあったため，民間団体による自主的な基準を定め適

切な管理が行われているサイトを健全なサイトを認定することによってフィルタリングを受けないようにする取り組みが行われた．民間団体より健全サイトとして認定されるためには，ユーザによるサイトへの投稿においては「携帯端末を特定する個体識別番号等」を取得することが必要と規定されている[2]．

b)通信プラットフォームのオープン化に関する要件（監督省庁）

携帯電話をはじめとする各種通信サービス産業の競争力強化を目的として，携帯電話サービス分野においては，従来の通信事業者主導による垂直統合型ビジネスモデルからインフラ，機器，サービス，及びコンテンツ等の各構成要素を分離させた水平分業型ビジネスモデルへの転換が望ましいとされており，特に従来の公式サイトと非公式サイトの区別なく識別認証及び課金機能が利用できるべきとの見解が示されている[3]．

c)アクセスの利便性に関する要件（ユーザ）

携帯電話からの Web アクセスにおいては，ユーザ名，パスワードの入力などが煩雑であり各種サービスにログインするにあたってはなるべく簡便な方法を用いるのが望ましいと考えられる．コンテンツプロバイダからはこのようなユーザ要件を満たす方法として，従来より回線契約 ID または端末 ID を使用した「簡単ログイン」の機能が提供されてきた．

3 携帯電話向け Web アプリケーションの識別認証機能に関する課題

現行の携帯電話向け Web アプリケーションが使用する固有識別情報を用いた識別認証機能については，今後解決することが望ましいと考えられる数点の課題が考えられる．以下にその代表的なものを示す．

3.1 利用者による識別情報のコントロール

回線契約 ID や端末 ID は携帯電話利用者を一意に特定することが可能であり複数の事業者間で情報を共有・交換することによって容易にネットワーク上での利用者の振る舞いを追跡することが可能となる．各 ID を変更するもしくは訪問サイト毎に切り替えることによってこれらを防止することが可能となるが，現行のシステムでは ID の変更は契約の解約，再契約など煩雑な作業が必要であり変更を行うための障壁が高い．

また，利用者は各 ID の送信を行わない設定とすることもできるが，多くのコンテンツプロバイダがこれらの送信をユーザに求める形となっておりユーザの識別が必要な Web アプリケーションではいずれかの ID の送信を許可せざるを得ないケースが多い．

3.2 回線契約 ID の送信に関するユーザへの告知

各通信事業者において回線契約 ID がデフォルト状態で送信する設定となっているか，初回設定時に送信設定とすることを強く推奨されており，多くのユーザはユニークな識別子を送信することによって発生するプライバシ上の懸念事項等そのリスクに関して十分に理解しない状態で使用している．ユーザ保護の観点からはユーザが各 ID 送信のリスクを十分に理解した上で利用を選択するオプトインの方式をとることが望ましいと考えられるが，この場合コンテンツプロバイダによる個体識別番号等取得要件とのコンフリクトが発生する．

3.3 なりすましや CSRF による攻撃の可能性

端末 ID のみを使用した識別認証やセッション管理においてはヘッダ情報の偽装によるなりすましが可能となる．対策として通信事業者が使用するアドレス範囲により適否を判別する方法が行われるが，任意のプログラムが実行可能なスマートフォンなどの普及によってこの方式も一定の効果しかないと考えられる．また，ユーザにリンク情報等をクリックさせ意図せぬ操作を強要する CSRF(Cross Site Request Forgery) 攻撃を防止するためには Web アプリケーション側で適切なセッション管理が必要である．

3.4 SSL による通信の制限

回線契約 ID を使用する場合，通信事業者のゲートウェイでヘッダ情報に回線契約 ID を付加するため携帯端末と接続先の Web サーバが直接 SSL(Secure Socket Layer)で通信できない仕様となっている．通信事業者によって全く SSL が使用できない場合や，通信事業者が提供するゲートウェイによる中継を受けなければならない場合がある．

4 まとめ

現行の携帯電話向け Web アプリケーションにおけるユーザ識別認証機能に関しては各ステークホルダーからの機能要件が相互に関係しておりそれによりユーザのプライバシ侵害に関するリスクやセキュリティ侵害に関するリスクが高まっているといえる．本分析結果に基づき今後各ステークホルダーの要件を最大限に満たすような最適な識別認証機構の実現に向けた研究を継続したいと考えている．

参考文献

[1]総務省，平成 19 年度通信利用動向調査，2008.
[2]EMA モバイルコンテンツ審査・運用 監視機構，コミュニティサイト運用管理体制認定基準，2008.
[3]総務省，「通信プラットフォーム研究会」報告書案，2008.