携帯電話用Webブラウザの安全性向上に関する提案

村田　薫†　　小柳　和子‡
情報セキュリティ大学院大学†‡

1　はじめに

日本国内における携帯電話端末においてWebブラウザを利用したインターネット接続において第2世代端末でも第3世代端末でもほぼ同様のサービスを利用可能ではあるが、携帯電話端末に施されているセキュリティに関する機能は端末毎に異なっている。

近年、携帯電話端末が内包する情報の重要さが指摘され紛失時のリスクに対する機能の研究開発が重視され、以前より一般ユーザー側のセキュリティ対策意識も向上しているといえる。しかし実際には高度なセキュリティ対策が利用可能な携帯電話端末は法人用途が大半であり、一般ユーザー側が利用可能な端末で最新のセキュリティ対策を行いたい場合は携帯電話端末自体の機種変更が必要になるのが現状である。

その為共通したシステムや機能の修正変更が可能なアプリケーション作成へのガイドラインや仕様に関して研究開発が行われているが[1][2]、それが可能となるのは次世代機種以降からであり、現行端末を所持する一般ユーザーへのセキュリティ性の向上にはならないのが現状である。

またサイト運営業者はコンピュータ向けのWebサイトの安全性と比較して携帯電話向けのWebサイトにおける安全対策が不十分な場合があり、キャリアや機種毎に異なる仕様も安全性対策への足枷となっている側面がある。

本論文では、携帯電話用Webブラウザにおけるパスワード等の入力及び操作作業後ログアウト処理を行った場合に関して、入力内容や作業内容がキャッシュされログアウト後でも端末を入手した第3者が調査可能になる危険性が存在している問題に対して、Webサイト運営側において改善可能な対策を行う事により携帯電話用Webブラウザの安全性向上を提案するものである。

Security improvements for a Web browser used with mobile telephones
†Kaoru Murata　‡Kazuko Oyanagi
†‡Institute of Information Security

2　提案手法

2．1　概要

サイト運営者は自身が管理するWebサイトにおけるログイン処理とログアウト処理に関するシステムを改善する事により安全性を高められるシステムを提案する。

ログイン処理におけるユーザー情報確認と共に現在Webサイトへのアクセスに使用した携帯電話端末の機種判別を行い、ログイン中ユーザー情報と共にサイト内で保持しておき、ユーザーがログアウト選択時に機種判別により得られた情報から端末が受信可能なデータを送り込む事によりユーザーが使用する端末のキャッシュデータは上書きされログアウト後に端末側から以前の情報を引き出す事を不可能にし、安全性を高める手法である。

2．2　従来の携帯電話用Webブラウザ

現在日本国内における携帯電話のシステムやアプリケーションは各キャリア、端末、製造メーカーごとに異なるのが現状である。また搭載したソフトウェアの更新手段がなく、セキュリティホールが存在しても改善手段がない端末も存在しており、最新の端末ではシステム更新機能の搭載など改善が行われつつある。更新機能のない端末においては対策手法がなく、ユーザーは端末自体の変更が必要である。現状一般開発者が開発したプログラムによって携帯電話端末システムに関わる命令の実行に関しては厳しい制限があり通常ではコンピュータやPDAのようなセキュリティの改善も行うことはできない。

また使用可能な設定事項に関して端末毎に異なりユーザーが設定し易いとは言い難く、機能を生かし切れていない場合がある。

2．3　システムの詳細

ログイン処理における端末情報の取得に関してユーザーに対して取得確認を行う必要がある。また今回提案するシステムにおいては端末情報は毎回ログアウト処理時に破棄する仕組みだが、ユーザー情報と同様に安全管理を行う必要があ

る。

ログアウト処理におけるユーザーが使用する端末へのデータ転送に関して、事前に得られた端末情報から各端末が受信可能な1ページ当たりの総データ量と Web ブラウザ全体の総キャッシュ量の情報と照らし合わせを行い受信可能なデータの送信を行う。携帯電話端末用 Web ブラウザでは各システムにおいて1ページ当たり受信可能なデータ量が決まっており、それを超える量を送信とようとするとエラー処理が行われる。その為今回の提案では1ページ当たりのデータ量を受信可能量より下回るようなデータを作成した。

3　実験

3．1実験方法

異なる世代や端末で同様のシステムが利用可能である必要があるため、国内各キャリアが公開している携帯電話端末用エミュレータを用意し、仮想環境上で実験を行った。第3世代型と第2世代型それぞれにおいて端末毎に受信可能な1ページ当たりの総データ量を下回るデータ量が書き込まれた HTML テキストデータを用意した。HTML テキストデータの内容はなるべく単調な内容とし、同様の内容が記録されたページに連続して自動的に読み込みを行えるような設定とし、順次データを読み込ませキャッシュ空間が上書きされるようにした。データの読み込み後、過去にキャッシュされたデータへ遡った場合にターゲットとしたページが再表示不可能となる事によりキャッシュデータの上書きが可能であるとする実験を行った。

各携帯電話端末によって受信可能なデータ総量だけでなく通信速度も異なる事からエミュレータ上での実験によって得られたデータから今回の実験により生じる通信コスト、処理の待ち時間など試算も同時に行った。

3．2　実験結果と課題

第2世代端末における実験では、受信可能な1ページ当たりのデータ量が少ない事もあり、通信速度が理論値通りだとすると約 2.3 秒程の待ち時間で読み込みが可能であり、通信コストも1パケット当たり 0.015 円とすると1回の操作において約 12 円の通信コストが発生する試算となった。

第3世代端末においては端末自体がキャッシュ可能なデータ量が非常に多い事から読み込み待ち時間は約 21 秒、1回の操作にかかる通信コストも約 766 円とユーザーにとって利便性が低くなる結果となった。

実験結果により本来キャッシュデータの消去機能がない Web ブラウザを搭載する端末においてキャッシュデータの上書きによる消去が可能である事が確認できた。このことから第2世代端末における安全性向上が実現することができた。第3世代端末における結果では通信コスト自体は定額サービスを利用する事によりコストを軽減できる。また待ち時間に関しては今後の改善点である。実運用においては機種判別による機種判定が誤った場合、対象外のデータを送信する事となりエラーを発生させる要因となる[3]ことから、今後は実運用に向けての改善を行っていく予定である。

4　まとめ

今回 Web サイトにおけるログイン処理とログアウト処理に関するシステムを改善する事によりシステムの更新不可能な Web ブラウザの安全性を高められるシステムを提案と実験を行った。本システムを用いることで、キャッシュに保存されたパスワード等の捜査情報などの消去が可能であると確認できた。今回のシステムでは全ての世代や端末に対応するためにキャッシュデータを直接上書きする手法をとったが、今後は送信するデータの圧縮など効率を高めるなど、通信コストを抑えより利便性のあるシステムの設計を行う予定である。

また次世代携帯電話におけるセキュリティの改善が重要であり、ユーザーが設定しやすい工夫も必要と思われる。

参考文献

[1]モバイル IT フォーラム:"公開資料庫"
http://www.mitf.org/public_j/archives/index.html
[2]Open Mobile Alliance.
http://www.openmobilealliance.org/index.html
[3]Ankit Fadia (著), 小川晃夫 (訳) : モバイルに潜む危機-天才ハッカーが指摘するユビキタスの問題点, トムソンラーニング社(2007)