White Paper

ウェブアプリケーション統合テストにおける留意点の検討と評価専用ブラウザの開発

２００９年 11 月 30 日

セキュリティフライデー株式会社
中岡　義雄

azbil

1　はじめに

現在、企業内の管理システムや生産システムはもちろん、装置や携帯電話に至るまで、そのユーザインターフェースとして、ウェブインターフェースが多く使用されている。ウェブアプリケーションの使用が拡大するにつれ、ウェブブラウザにはユーザ指向の新しい技術、機能が次々と搭載される一方、ウェブアプリケーションのセキュリティ面の強化やより高い品質が求められるようになってきている。

弊社では、ウェブアプリケーションをより安心、快適に使えるよう、ネットワークセキュリティの側面から研究を行ってきたが、ウェブアプリケーション開発においては、評価指針が十分には確立されておらず、セキュリティ強化の前段階として、ウェブアプリケーションの評価テストの課題解決が必要であると捉えた。

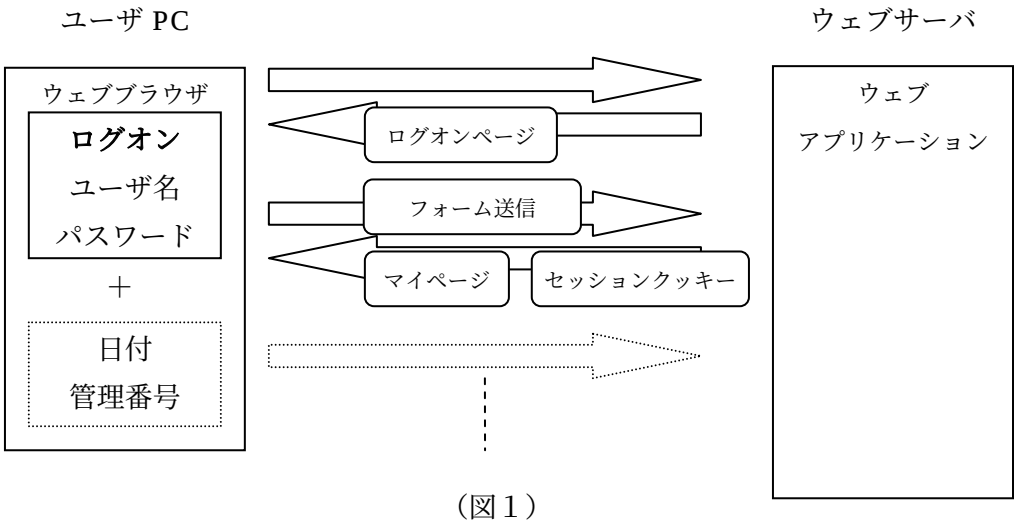
今回、統合（結合）テスト、システムテスト、受入検査での検証（Verification）を目的としたテスト設計における基本的な留意点をアプリケーションの特性から検討し、テスト実施を支援する評価テスト専用ブラウザの開発を行ったので報告する。

2　ウェブアプリケーションの仕組

ウェブアプリケーションのテスト設計を検討するにあたり、その基本的なシステムとアクセス手順の例を図１に表わす。

図１では、ユーザはアクセス先のウェブサーバにアクセスすると、サーバ側からはログオン画面のデータが送信され、ブラウザ上に表示される。入力ボックスから、ユーザ名とパスワードを入力しウェブサーバに送信する。この時、ブラウザからは、入力ボックスに入れた値以外にも、日付や管理番号等、サーバ側で必要な Hidden データ（ユーザには知らされないデータ）等が付加され送信される（フォーム送信）次に、ウェブサーバ側でユーザ認証がされ、次のページ（マイページ）データに加えセッションクッキーが送信され、ユーザは次のページでの操作を行う。マイページからさらに別のページへの遷移時には、サーバから受け取ったセッションクッキーが使われる。サーバ側では、ユーザの持つセッションクッキーを元に別ページへのアクセス許可を与える。以降の遷移も同様に行われる。

セッション管理のためのパラメータは、クッキーやクッキー以外の他のデータ、あるいは他のデータとの組合せ等により行われるが、開発環境によっては、アプリ開発者は具体的な管理方法を意識せず、開発環境で用意されたライブラリー（フレームワーク）を利用し行われている場合もある。



（図１）

3　ウェブアプリケーションの特長

テスト設計で着目する必要のある、ウェブアプリケーションの主な特長は以下である。

3.1　マルチユーザインターフェース

ウェブアプリケーションは、不特定多数のユーザがホームページを同時に利用するインターネットで生まれ、企業内システム等、複数のユーザが同時にひとつのシステムを使用する用途に多く利用されている。

従来のクライアントサーバシステムとは異なり、あらかじめ、ユーザ側にアプリケーションは用意されておらず、ユーザにより異なるアクセスページや状態に応じ、サーバ側からブラウザへページデータが送信され表示されるマルチユーザインターフェースが大きな特長のひとつである。

マルチユーザインターフェースにより主に下記の管理が必要となる。

① アクセス管理

ユーザ毎、ページ毎、操作毎、状態毎等それぞれの状況に応じた、アクセスの許可、不許可の管理

② セッション管理

プロトコル上、ひとつひとつのページへのアクセスは独立し、関連付けされていないため、複数のページにまたがって行われるアクセスが同一ユーザのものか、特定ページへの遷移の前に必要なページの通過（アクセス）が完了しているか等、ブラウザとサーバ間ではセッション追跡パラメータを送受信し、追跡、管理が行われている。

③ パフォーマンス管理

ユーザ側に専用アプリが必要でないことから、ユーザの増減が容易に行えるが、あらかじめ、同時にシステムを利用するユーザ数を想定し、ユーザ数に見合ったパフォーマンスを確保する必要がある。

3.2　ブラウザとの連携

ウェブアプリケーションでは、ユーザインターフェースにブラウザを利用することが必須となり、ブラウザの機能、特性等への対応が必要となる。

① 各種ブラウザへの対応

現在、最も使用されているブラウザは Internet Explorer だが、それ以外にも Firefox、Opera、Safari 等様々なブラウザが使用され、更に、それぞれのバージョンや設定、また、OS の種類等、ユーザの使用環境にあわせ、推奨ブラウザ、動作可能ブラウザとそれらの設定を規定する必要がある。

② ハングアップへの対応

ブラウザが、ハングアップすることを前提にウェブアプリケーション側で対応する必要があり、用途によりユーザ毎のセッション状態をサーバ側かブラウザ側で保持して置くことが必要になる。

③ その他特有の操作への対応

ブラウザの「戻る」ボタン操作による遷移前のセッション状態への対応や、アクセス途中で PC がスリープ状態になり、長時間経過後、以前のセッション状態でアクセスが再開される等、ブラウザやウェブアプリケーション特有の操作への配慮が必要になる。

ウェブアプリケーションでは、複数ユーザのアクセス状態の様々な情報を過去分も含め、サーバ側やブラウザ側で保持、送信、管理していることが大きな特長といえる。

4　統合（結合）テスト、システムテスト、受入検査の基本テスト設計

統合テスト、システムテスト、受入検査では、検証（Verification　正しく製品が作られているか）と妥当性評価（Validation　正しい製品を作っているか）が実施される。

ウェブアプリケーションでは、前述の仕組や特長から考えると、他のアプリケーションに比べ、送信データに、古いデータや他ユーザのデータが混入する、データが化ける、データの一部、即ちパラメータ自体が送信されない等々、様々な送信データに関連するリスクが非常に高くなる。

検証（Verification）において、アプリケーションの特性から基本的に重要となるテストは、ブラウザからの入力値テストとユーザがブラウザからデータを入力した後、実際にウェブサーバに送信されるデータ（送信フォーム）の書換テスト、更にパフォーマンステストになるが、データの書換テストについては以下となる。

4.1　ブラウザ上の入力値テスト

ブラウザ上の入力ボックスに有効値、無効値、境界値を入れ、期待される出力を確認する。

現在、多くのウェブインターフェースでは、入力ボックスに無効値を入力した

場合、期待される出力は、ブラウザ上にスクリプト処理によるメッセージが表示され、ウェブサーバへの送信は行われない。

4.2　ブラウザからの送信データ（送信フォーム）書換テスト

ユーザがブラウザ上で入力したデータとブラウザ側で付加された Hidden データ、スクリプト処理等により加工されたデータを含めた送信データ（送信フォーム）を有効値、無効値、境界値に書換送信し、期待される出力を確認する。無効値としては、送信データの一部（パラメータ）を削除することも必要となる。

5　ウェブアプリケーション評価テスト専用ブラウザ「ウエブテイスター」の開発

5.1　開発の背景

通常、開発エンジニアが行う単体テストは、開発環境で送信データ（送信フォーム）の書換を含むデバッグが可能な場合が多いが、テストエンジニアが実施する統合テスト、システムテスト、受入検査においては、十分なテスト環境を用意することが困難な場合があり、ブラウザ上での入力値テストのみで、送信データまでのテストは省略されるケースも見られる。

また、仕様書の元々の用途や完成度のばらつきを配慮すると、ウェブアプリケーションのテストでは有効なテスト設計を仕様書のみから行うことは困難で、テストエンジニアの経験に大きく依存する。テストの設計から実施、報告まで、できるだけ経験に左右されず、誰でも簡単に有効なテストを実施できることが求められている。

5.2　ウエブテイスターとは

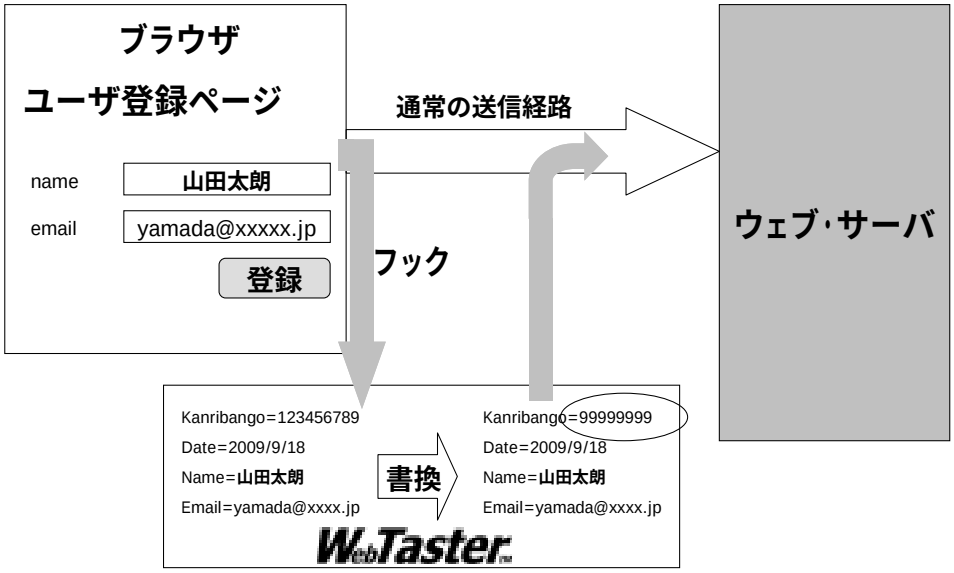
ウエブテイスターは、弊社のセキュリティ技術を応用し、統合テストの設計から実施、報告までを支援する専用ブラウザとして開発した。特長と主な機能は以下のとおりである。

①　特長

- 完成したアプリケーションに対し、ハッカー視点のブラックボックステストが可能
- 専用の評価環境無しに、インターネットエクスプローラベースの標準ブラウザ環境で評価テストを実現
- 各ページ毎の入力ボックス項目と実際に送信されるデータのリストアップからテストの実施、結果報告までを支援
- ブラウジング中のＳＳＬ暗号化された送信データも簡単に書換テストが可能
- 付属のＳＱＬインジェクション基本テストパターンを利用し、セキュリティテストにも応用可能

② 主な機能

- 評価シート作成支援
  - 入力項目を含む送信されるデータ（フォーム）やクッキーの保存機能（CSV 形式）により、実際の完成ページをブラウジングしながらテストケース（評価項目）の元データを生成。
- テスト実施支援
  - 送信されるデータ（フォーム）やクッキーデータの書換機能（図２）
  - 繰返し利用するテストパターンの登録機能（SQL インジェクションの基本テストパターンも提供）



（図２）

- 結果報告支援
  - 実施テストログ機能
  - レスポンスの HTML、クッキー保存機能

6 おわりに

幅広い用途に急拡大するウェブアプリケーションを安心、快適に使用していくために、問題解決の第一弾として、評価テスト専用ブラウザ「ウエブテイスター」を開発したが、今後は、セキュリティ問題の解決や、評価テストの効率化を視野に入れた機能追加、周辺製品等の開発を行っていきたいと考えている。

また、本報告では、ウエブテイスターの技術や詳細仕様、実際の使用例にまで触れることができなかったが、次の機会では、ウエブテイスターを中心に報告したいと考えている。

2009 年 11 月　発行

セキュリティフライデー株式会社
URL http://www.securityfriday.com/jp/