Japan IT Week 春 参加報告書

検印 3	検印 2	検印 1	期間/報告日	2013/05/08 ～ 2013/05/08	2013/05/09
			実 施 場 所	東京都江東区有明 3-11-1	
				東京ビッグサイト	
			所 属 / 氏 名	システム開発部	小野　敬二

IT 専門展「Japan IT Week 春 2013」に参加してきたので、そこで得た情報について報告いたします。

Ⅰ：ファジングの紹介

1. ファジングとは

ファジングとは、ソフトウェア製品に、問題を引き起こしそうなテストデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検査手法である。ソフトウェア製品の開発ライフサイクルにファジングを導入すると、以下のような利点がある。

(1) バグや脆弱性の低減
(2) テストの自動化・効率化による労力削減

2. ファジングツール

ソフトウェア製品に送り込む「問題を引き起こしそうなデータ」のことを「ファズ」と呼ぶ。ファジングを実施するための専用ツールであるファジングツールには、以下の 3 つの機能があり、これら一連の動作を自動で繰り返し行う。

(1) ファズの生成・加工
(2) ファズの送信・入力
(3) ファジング対象の挙動・死活監視

3. ファジングの特徴

ファジングはソフトウェア製品の内部構造を考慮せず、データの入出力に注目することで外から不具合を見つけるブラックボックス検査である。ソースコードは必要なく、動作するソフトウェア製品があれば実施できる。また大量にファズを生成し対象ソフトウェア製品に送り込む総当たり的な検査手法であるので、手動でファジングを実施することはまれで、ファジングツールにより自動化して行うのが一般的である。一方、ファジングはブラックボックス検査であるので脆弱性の種類や原因となっている場所を特定できない。脆弱性を修正するには、別途ソースコードから問題個所を探し出す必要がある。

4. ファジングツールの紹介

オープンソースソフトウェアのファジングツールを紹介する。

(1) ファジングツール「Peach」
① ファイル、ネットワーク、ウェブアプリケーションに対するファジング
② URL：http://peachfuzzer.com/

Ⅱ：所感

情報処理推進機構(IPA)が提唱するファジング導入の勧めに着眼し、紹介させてもらったが、製品の単体テストでそのまま使えるというよりは、ソフトウェア品質の向上のための補助ツール的な位置付けであると感じた。

今回のような大規模な IT 展に参加するのは初めてであったが、会場の熱気に触れて日本の IT 業界の活力を感じたように思う。

以 上