別紙 1

■ 脆弱性検出ツール「iFuzzMaker」

▼「iFuzzMaker」とは

「iFuzzMaker」は、「JPEG 画像を読み込む機能」を持つ製品にセキュリティテスト「ファジング」（図 1）を支援するツールです。

製品の「JPEG 画像を読み込む機能」に脆弱性が存在すると、問題を起こすデータ（例えば極端に長い文字列）を持つ JPEG 画像を読み込んだ場合、製品の動作に問題（製品そのものの強制終了、最悪の場合、ウイルスへの感染や外部からの遠隔操作）が生じます。この脆弱性を作り込まないためには、製品出荷前に、このような JPEG 画像（テストデータ）を読み込ませて、製品の動作に問題が生じないかを確認するテストが有効です。「iFuzzMaker」は、このテストデータを生成します。製品開発者は「iFuzzMaker」で生成したテストデータを製品に読み込ませるだけでファジングを実行できます。

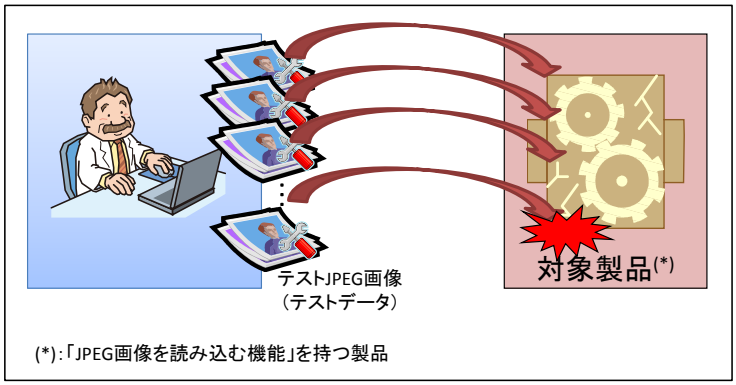

図 1「JPEG 画像を読み込む機能」に対するセキュリティテスト「ファジング」のイメージ

▼「iFuzzMaker」の利用とテストデータの活用までの流れ

- 準備
  - ✓ 「iFuzzMaker」を使ってテスト JPEG 画像を生成するために次の 2 つを準備します。
    - テストデータの基となる「JPEG 画像」
    - どのようなテストデータを生成するかを決める「テストデータ生成ルール」
- 生成
  - ✓ 「iFuzzMaker」を操作して、テストデータを生成します。
- 活用
  - ✓ 生成したテストデータをファジングに活用します。

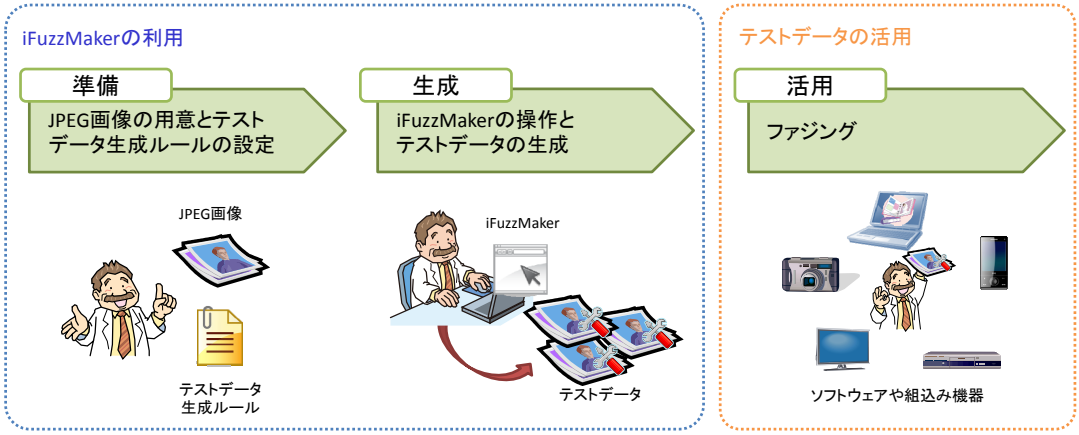

図 2「iFuzzMaker」活用の流れ