IPA Better Life with IT

情報セキュリティEXPO

外部からの脅威に対し「ファジング」の導入を!
～ さらなる脆弱性発見のためのセキュリティテスト ～

2018年5月9日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
小林 桂

Copyright © 2018 独立行政法人情報処理推進機構

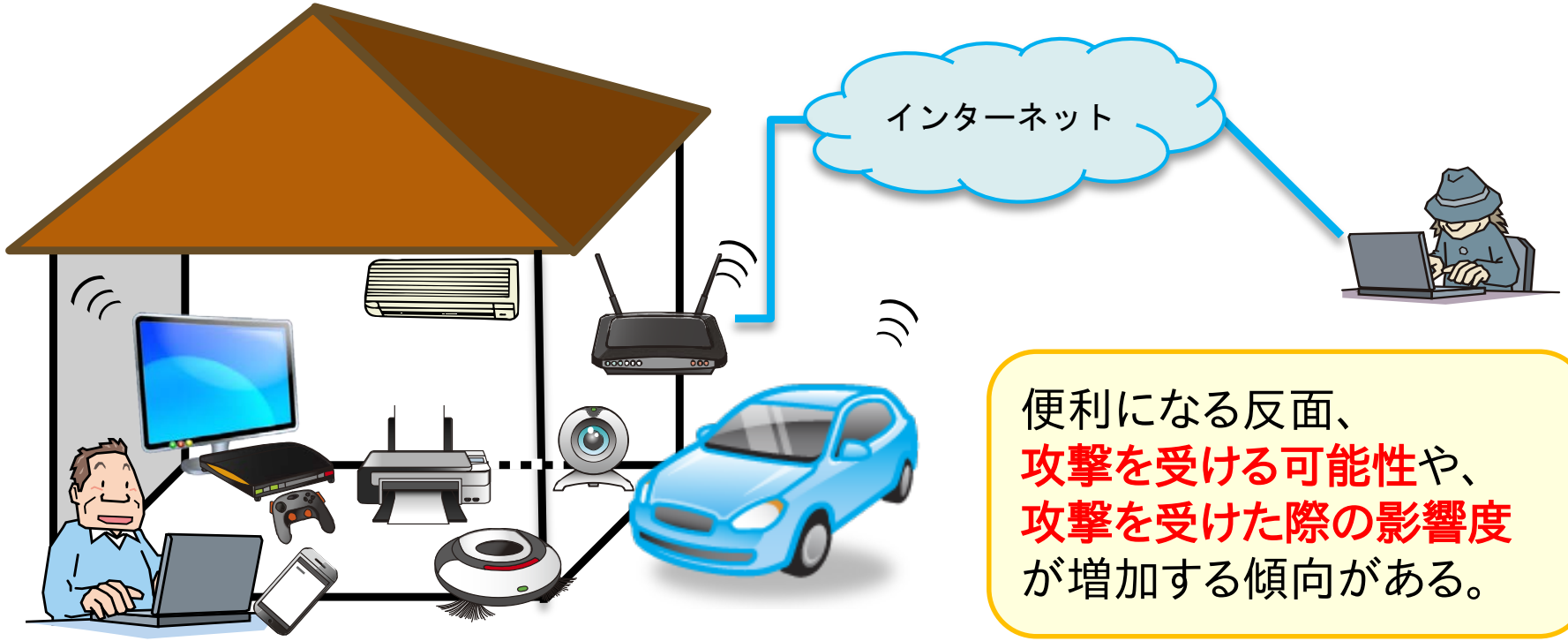
本日の内容

- はじめに
- ファジングとは
- ファジングの活用事例
- まとめ

Copyright © 2018 独立行政法人情報処理推進機構

はじめに
～繋がる多様な機器、便利になる反面で～

- さまざまな製品や機器が通信機能を持ち、相互に情報をやりとりして連携する
  - IoT（Internet of Things）の普及により、様々な”もの”がインターネットにつながる時代



便利になる反面、
攻撃を受ける可能性や、
攻撃を受けた際の影響度
が増加する傾向がある。

Copyright © 2018 独立行政法人情報処理推進機構

はじめに
～出荷後の製品の脆弱性発見事例～

- Webカメラが乗っ取られる！ ネット機器の脆弱性
  - 中国メーカーのWebカメラに認証不備の脆弱性
  - 第三者によって外部から不正アクセスされ、盗み見等をされる可能性
- 米自動車メーカーが開発したコネクテッドカー、脆弱性対策で140万台リコール
  - 米国の大手自動車メーカーが開発したコネクテッドカーに、外部から遠隔操作可能な脆弱性が発見される
  - 対策のため、自社のコネクテッドカー140万台をリコール

攻撃を受けた際により大きな影響が発生する可能性
→ 従来よりも 網羅的なセキュリティテスト が必要に

Copyright © 2018 独立行政法人情報処理推進機構

はじめに
～ファジングを推奨する理由～

- ✓ 従来よりも厳重なセキュリティテストの必要性
- ✓ テストを実施する技術者が足りない
- ✓ テスト工程で、できるだけ不具合を取り除きたい
  - ソフトウェア品質の向上
  - 脆弱性対応、修正対応コストの削減

バグや脆弱性を見つけるセキュリティテストとして導入を推奨するのが「ファジング」

Copyright © 2018 独立行政法人情報処理推進機構

本日の内容

- はじめに
- ファジングとは
- ファジングの活用事例
- まとめ

Copyright © 2018 独立行政法人情報処理推進機構

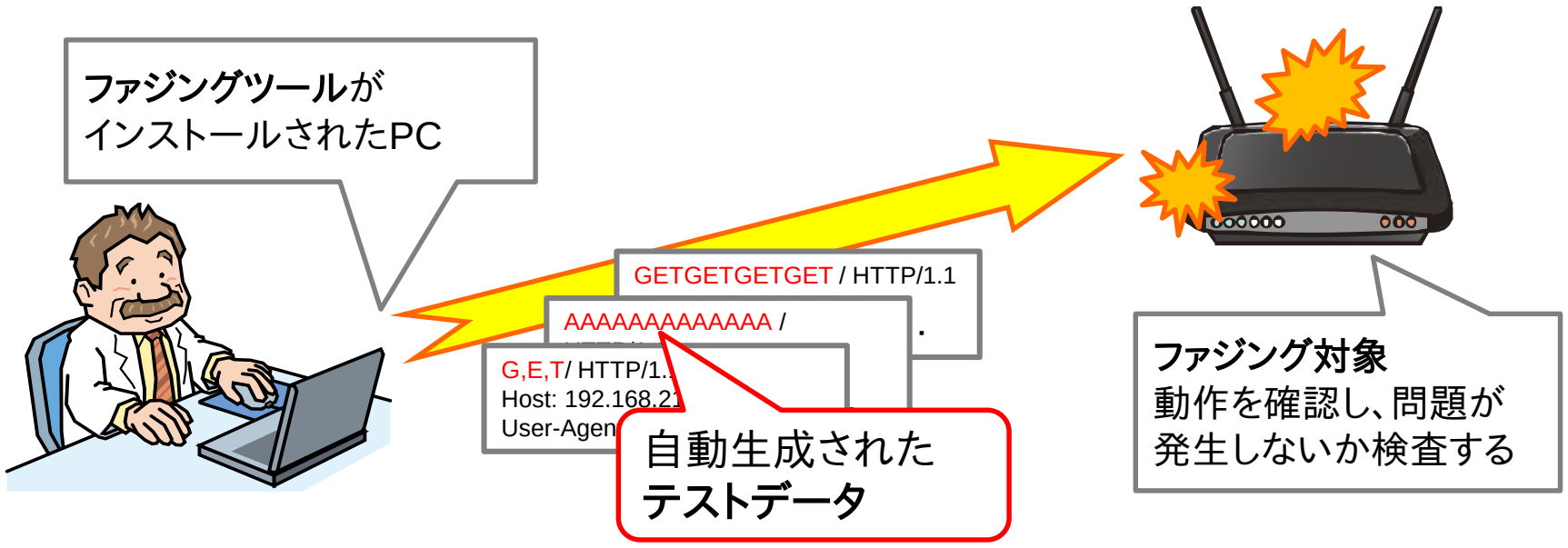
ファジングとは
～どのようなセキュリティテストか～

- ソフトウェア製品等のバグや脆弱性を検出するセキュリティテスト手法の一種
  - 一般的に、細工をした異常データを大量に生成し、テスト対象に処理させることで、これらの処理に起因するバグや脆弱性を検出する。
- 自動的に実行される
  - セキュリティの専門家でなくてもソフトウェアのバグ除去に取り組める。
- ソフトウェアの品質向上を目的としている。

Copyright © 2018 独立行政法人情報処理推進機構

ファジングとは
～どのようなセキュリティテストか～

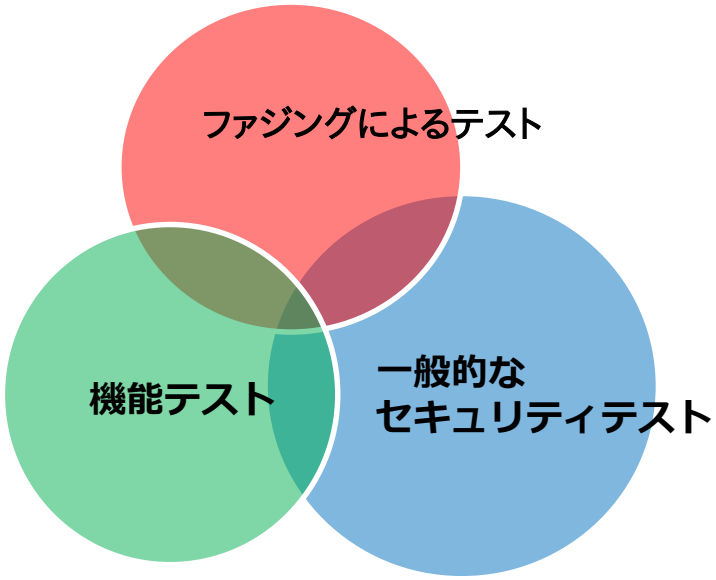
- ソフトウェアのバグや脆弱性を探すブラックボックステストの一種
- 異常データを自動生成し、検査対象に入力する
- 製品の応答や動作を監視して、異常データによって問題が発生しないかを検査する



Copyright © 2018 独立行政法人情報処理推進機構

ファジングとは
～どのようなセキュリティテストか～

- ファジングでは、一般的な機能テストやセキュリティテストでは発見が難しいバグや脆弱性などを検出できる可能性がある



機能テスト:【主にバグを探す】
仕様に基づく動作をすることをテストする。

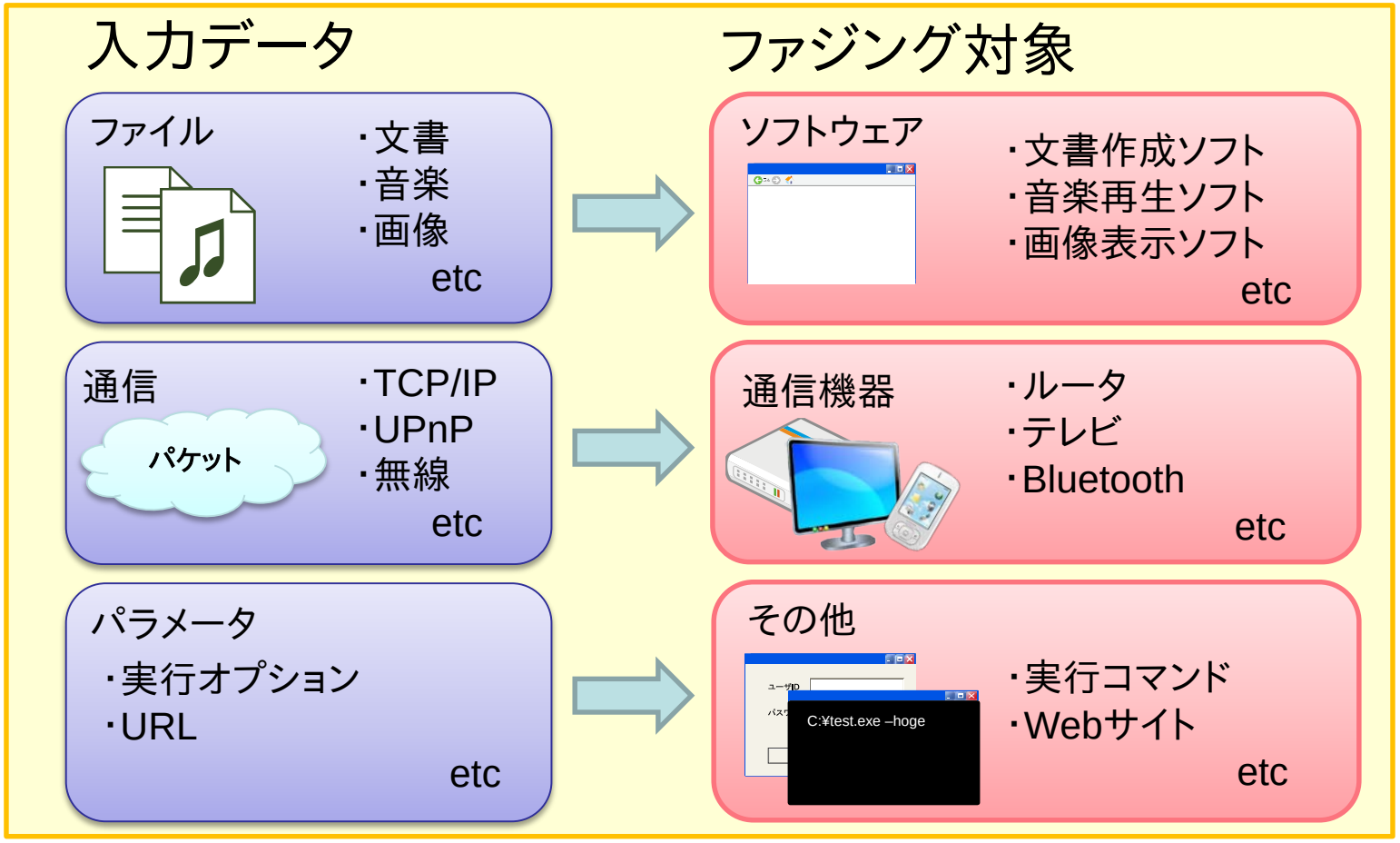
一般的なセキュリティテスト:【主に脆弱性を探す】
（ペネトレーションテスト、ソースコード診断など）
一般的な攻撃手法に対する耐性をテストする。

ファジングテスト:【バグも脆弱性も探す】
様々な入力データに対し、異常が発生しないことをテストする。

Copyright © 2018 独立行政法人情報処理推進機構

ファジングとは
～多種多様なデータと製品～

- 入力形式が定められていれば、あらゆる製品をテスト可能



Copyright © 2018 独立行政法人情報処理推進機構

本日の内容

- はじめに
- ファジングとは
- ファジングの活用事例
- まとめ

Copyright © 2018 独立行政法人情報処理推進機構

ファジングの活用事例
～ 企業のファジング活用 ～

- 米マイクロソフト社の活用事例
  - 米マイクロソフトは、ファジングを自社の開発ライフサイクル（SDL：Secure Development Lifecycle）に組み込み、自社製品テストを行っている。

https://www.microsoft.com/downloads/ja-jp/details.aspx?familyid=9181a79a-761e-1487a-e2e2-8da72fb9eade

  - 米マイクロソフトではファジングによる自動テストを行い、Office 製品のバグを 1,800 件発見

Copyright © 2018 独立行政法人情報処理推進機構

ファジングの活用事例
～ サービス化と進化するファジング ～

- グーグルのファズテストツール「OSS-Fuzz」、数カ月で1000件以上のバグ発見
  - 47のプロジェクトで1000件以上のバグが発見され、そのうち、264件は潜在的なセキュリティ脆弱性

- 米マイクロソフト、AI利用のクラウドベース脆弱性発見ツール「Security Risk Detection」発表

  https://japan.zdnet.com/article/35104705/
  - 通常の入力データを与えるとAIが自動的に多数のテストを実行
  - バグや脆弱性などが発見されると、リアルタイムで報告される
  - 機械学習とニューラルネットワークを用い、ファジングを改良する研究も行われている。

Copyright © 2018 独立行政法人情報処理推進機構

本日の内容

- はじめに
- ファジングとは
- ファジングの活用事例
- まとめ

Copyright © 2018 独立行政法人情報処理推進機構

まとめ
～ファジング活用のご提案～

- ファジングを活用すると、従来のテストから網羅性を高めて、**製品の品質確保に効果がある**
  - 大手ソフトウェア企業を中心に活用実績がある
  - IPAでも脆弱性検出に効果があることを実証済み
  - ファジングの実施量については、検討が必要

安全な製品を提供していくために
ファジングの導入をご検討ください

Copyright © 2018 独立行政法人情報処理推進機構

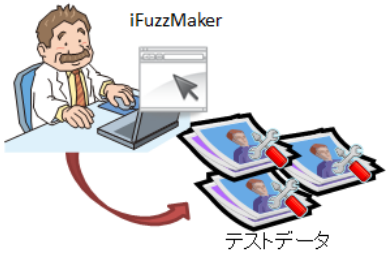
まとめ
～もっとファジングを知りたい方は～

- IPAの「ファジング」関連資料をご活用ください
  - 「ファジング活用の手引き」
  - 「ファジング実践資料（実践編・UPnP編・テストデータ編）」
  - 「スマートテレビの脆弱性検出のレポート」
  - 「製品の品質を確保する『セキュリティテスト』に関するレポート」

- 組み込み製品の脆弱性対策映像コンテンツ
  組込み製品の脆弱性が及ぼす影響 ～製品開発企業はどうすれば～
  - 組込み製品の脆弱性対策に ～知ってみよう ファジング～

- JPEG テスト支援ツール「iFuzzMaker」

IPA　ファジング　**検索**



Copyright © 2018 独立行政法人情報処理推進機構