

■ 開発のねらい

- ・テスト効率による検査コストの削減
- ・検証スキルに依存しないテスト品質と簡単操作
- ・安心安全な製品の提供
- ・セキュリティ人材教育への活用

■ ツールの特長 - 製品の入出力による検査 -

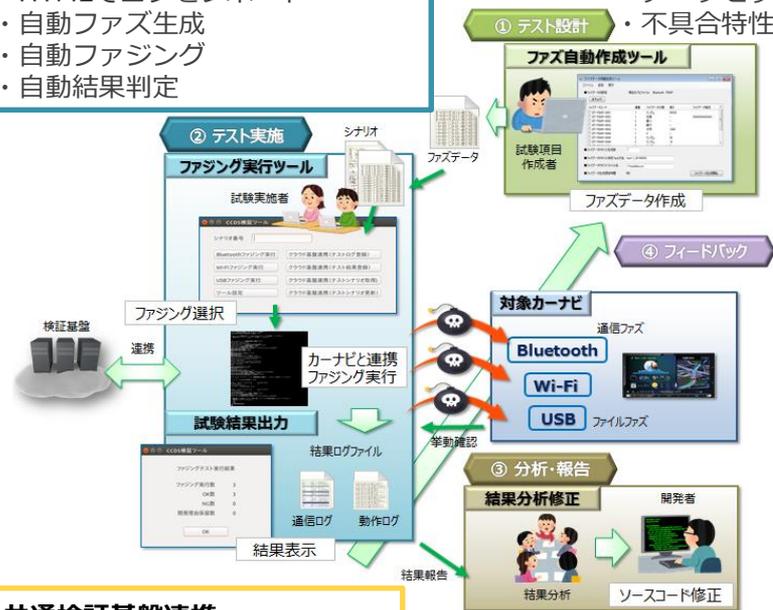
- ・製品のプログラムを開示せずに検査が可能
- ・狙った任意の場所へのファジングが可能
- ・脆弱性につながる不具合の見逃しを削減
- ・シーケンス終了保証によりテストフリーズを回避

ファジングツール

- ・プロトコルファジング Wi-Fi/BT
- ・ファイルファジング USB
- ・HTMLでログをレポート
- ・自動ファズ生成
- ・自動ファジング
- ・自動結果判定

フィードバックツール

- ・機械学習で分析/予測/生成
- ・不具合データの蓄積辞書化
- ・データセットの可視化
- ・不具合特性別に絞込



共通検証基盤連携

- ・API対応
- ・クラウド/オンプレ
- ・シームレス/ノンシームレス

検証プロセス

- ・IoTセキュリティ評価検証ガイドライン
- ・ISO/IEC/IEEE 29119

◆ 脆弱性検査と利用フェーズ

検査名	フェーズ	
	開発	運用
ソースコードセキュリティ検査	○	-
ファジングによる検査	○	-
システムセキュリティ検査	○	○
ウェブアプリケーションセキュリティ検査	○	○
ペネトレーションテスト	-	○

◆ IoT機器特有のI/Fとプロトコルの検査

通信プロトコルファジング		ファイルファジング
Wi-Fi	Bluetooth	USB
アプリケーションレイヤ DLNA HTTP UPnP	Bluetooth Profile PBAP A2DP	アプリケーションレイヤ MSC(MP3,WAV) HID
TCP/UDP	Bluetooth Core Spec	クラスドライバ/API
IP		ホストドライバ
物理層	物理層	ドライバ
		コントローラ