通信機器脆弱性試験システム

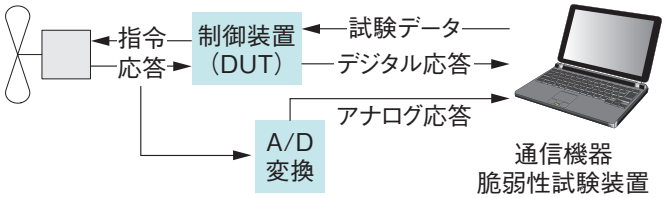
情報技術グループ

インターネットなどのネットワークに接続される機器の脆弱性は、セキュリティ上の問題となります。脆弱性の網羅的な試験は非常に難しいため、開発時に入念な試験を行っていても、脆弱性が残ったまま出荷されてしまう製品も多くあります。「通信機器脆弱性試験システム」は、豊富なテストパターンの通信データを機器に入力することで、機械的に脆弱性を発見する試験（ファジング）を行うことができます。

ファジングによる脆弱性の発見

本装置を用いた試験システムの構成は、右図のようになります。試験対象機器（DUT）を実際の使用時と同様に動作させ、本装置と通信が行えるようにします。DUTが外部装置の制御を行う場合は、それを監視することもできます。

ファジングでは、まず正常なデータを送って、機器が正しく応答することを確認します。次に、異常なデータ（例えば、極端に長いデータ、仕様を逸脱したデータ、ランダムなデータ等）を一つ送信し、正しく応答があるかどうかを確認します。正しい応答が得られれば、次のデータを送信することを繰り返して試験を進めます。試験で送信されるデータ（テストパターン）は、よく使われるものがあらかじめ数千～数百万通り組み込まれています。また、自分で定めることもできます。



「通信機器脆弱性試験システム」の構成例

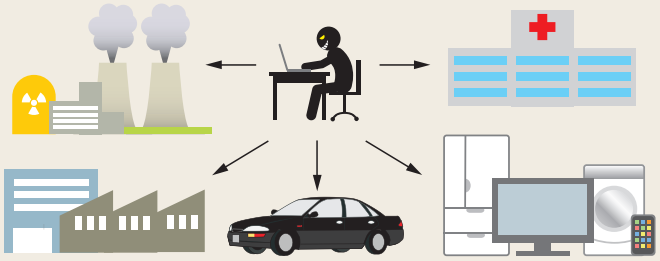
装置外観

試験対象機器の事例

以下のようなさまざまな通信機器の試験を行うことができます。

- スマートフォン、タブレット等の情報機器
- ネットワーク家電、カーナビ等の組み込み機器
- 生産設備や重要インフラで用いられるコントローラ（IEC 62443、EDSA認証※の通信ロバストネス試験（CRT）と同様の試験を実施可）

※EDSA認証は、制御機器のセキュリティに関する認証制度です。



IoT（Internet of Things）等の発展により、さまざまなものがネットワークに接続され、攻撃される恐れがあります

仕　様	
モデル	Synopsys社製Defensics
対応規格	（有線）10Base-T/100Base-TX/1000Base-T
	（無線）Bluetooth
対応プロトコル等	Ethernet、IPv4、TCPv4、ICMPv4、ARP
	MODBUS
	HTTP、TLS
	Bluetoothプロファイル：A2DP、AVRCP、HDP、HFP、L2CAP、BNEP、RFCOMM、OBEX、SDP

機器利用料金※（税込）	中小企業	一　般
通信機器脆弱性試験システム	1,623円	3,219円
通信機器脆弱性試験システム（無線通信）	692円	1,357円

※1件1時間あたりの料金

お問い合わせ　情報技術グループ＜本部＞ TEL 03-5530-2540