

# IoT 機器の脆弱性検査ツール

SecDevice は、ネット接続製品向けに設計された自動化セキュリティ評価ツールです。脆弱性テスト、ファジングテスト、Web セキュリティテストなどの機能を備えています。また、特許取得済みの AI 学習テクノロジーを使用して、脆弱性検出の時間と精度を優れています。IEC 62443、OWASP TOP 10、CVE / SANS TOP 25 などの情報セキュリティ標準に対応しています。10、CVE / SANS TOP 25 などの情報セキュリティ標準に対応しています。



## 製品特徴

### IoT 製品のセキュリティ：

ネット接続製品のセキュリティテスト用に設計されています。イーサネットまたはワイヤレスネットワークを介してテスト対象デバイスに接続され、テスト対象デバイスのセキュリティを自動的に分析及びテストします。また、自動化導通テストもサポートします。手動介入の手間を削減します。

### 多様な脆弱性テスト方法：

ファジング、ネットワーク脆弱性スキャン、Web 脆弱性スキャン、DoS などのテスト方法を使用して、オペレーティングシステム、ネットワークアプリケーション、ネットワークプロトコル、Web やワイヤレスなどに既知と未知の脆弱性を検出できます。

### TCF インテリジェント検出テクノロジー：

AI テクノロジーを使用してネットワークパケットを学習し、テスト係りがさまざまなカスタマイズしたネットワークプロトコルの弱点を検出するのを支援し、検出の範囲と完全性を改善します。

### 完備なテスト記録：

検出プロセス中に攻撃パケットとテスト方法を記録し、弱点発生の明確な原因と関連するサポート情報を提供して、製品のセキュリティ脆弱性を迅速に再現するのに役立ちます。

簡単	統合	高いカバレッジ
3つのステップでスキャン開始	ネット接続デバイスに必要なセキュリティテスト項目が含む	120 個以上の安全テスト項目と特許取得済みのテスト方法



<b>ステップ 1</b> テスト項目を選択	・ポートの自動識別 ・脆弱性テスト ・Web セキュリティテスト ・ファジングテスト ・無線ネットワークテスト ・脆弱性の利用	・システムの弱点 ・ネットワークの弱点 ・プロトコルの弱点 ・ウェブの弱点 ・ワイヤレスの弱点
<b>ステップ 2</b> テスト対象を選択		
<b>ステップ 3</b> テスト開始		

## メリット

- ・ **人材とツールのコストを削減：**  
セキュリティ担当者のトレーニング時間を節約し、複数のツールセットを購入する負担を軽減します。
- ・ **専門家への依存を軽減：**  
簡シンプルな運用設計により、テスト係りは簡単に利用でき、詳細なテスト記録を通じて、開発チームの問題解決を効果的に役に立ちます。
- ・ **製品のセキュリティテストの整合性を向上：**  
特許取得済みの AI 学習テクノロジーは、カスタマイズされたプロトコルのセキュリティテストをサポートし、従来のテスト方法の欠点を補うことができます。



## 製品技術規格

SecDevice は、既知と未知の脆弱性検出技術を使用して、テスト対象のデバイスの下記の項目に対しての脆弱性検出を実行：

インターネットセキュリティ	IPv4 または IPv6 アドレッシング技術に基づいて、セキュリティテストパケットがネットワークを介してターゲットに送信され、テストスコープは対象デバイスのオペレーティングシステムとアプリケーションを含めています。
ウェブセキュリティ	Web アドレス (URL) で定義されたテストターゲットに基づいて、ほとんどの接続デバイスが提供する操作インターフェイスが、Web サイトアプリケーションのセキュリティについてテストされます。
ワイヤレスセキュリティ	サービスセット識別子 (SSID) に基づいてテストターゲットを定義し、デバイスによって提供されるワイヤレス接続サービスにセキュリティ上の弱点があるかどうかを分析します。

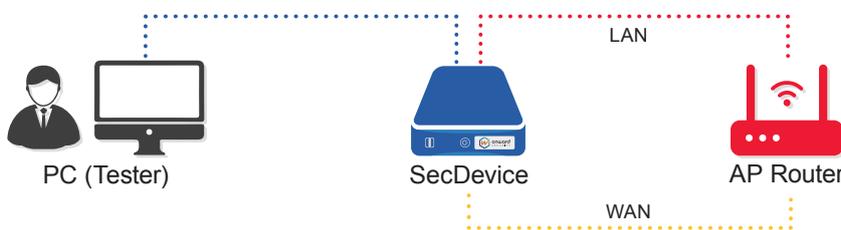
## 適用するプロトコル

<b>Core Network(8)</b>	ETHERNET, IPv4, IPv6, TCP*, UDP*, ARP, ICMPv4, ICMPv6	<b>File System(3)</b>	CIFS, SMB, NFS
<b>IIoT(14)</b>	BACnet, CoAP, DNP3, EtherNet/IP, FINS, S7comm, Goose**, MMS**, Sampled Value**, Modbus, OPC UA, CIP, IEC104, MQTT	<b>Healthcare(2)</b>	DICOM, HL7
<b>Network Management(28)</b>	CWMP, DHCPv4, DHCPv6, DNS, LDAPv3, NTP, OSCP, PPTP, SIP, SNMPv1, SNMPv2, SNMPv3, SNMPTrap, SSHv2, TFTP, Telnet, TLS1.2, UPnP, IPsec, RADIUS, IKEv2, IPMI, NFSv4, VLAN, FTP, BGP, BFD, NetBIOS	<b>Web Application(2)</b>	HTTP, WEB Fuzz***
		<b>VoIP/ IMS(3)</b>	RTP, RTCP, RTSP
		<b>Wireless(4)</b>	802.11 WLAN Client, 802.11 WLAN Client AP, 802.11 WPA Client, 802.11 WPA Client AP

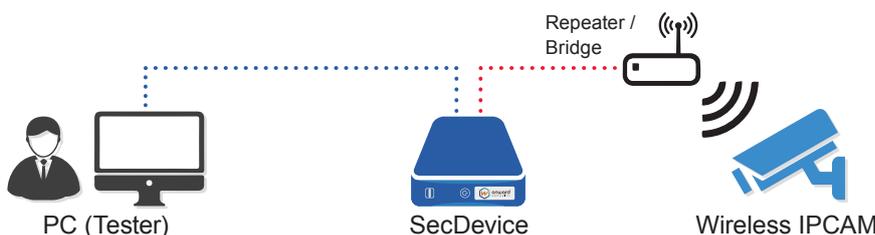
## 製品使用シナリオ



単一の接続インターフェイスを備えたネット接続製品  
例：産業用制御設備または医療設備



2つの接続インターフェイスを備えたネット接続製品  
例：ネットコム設備



ワイヤレスのネット接続製品  
例：監視装置

