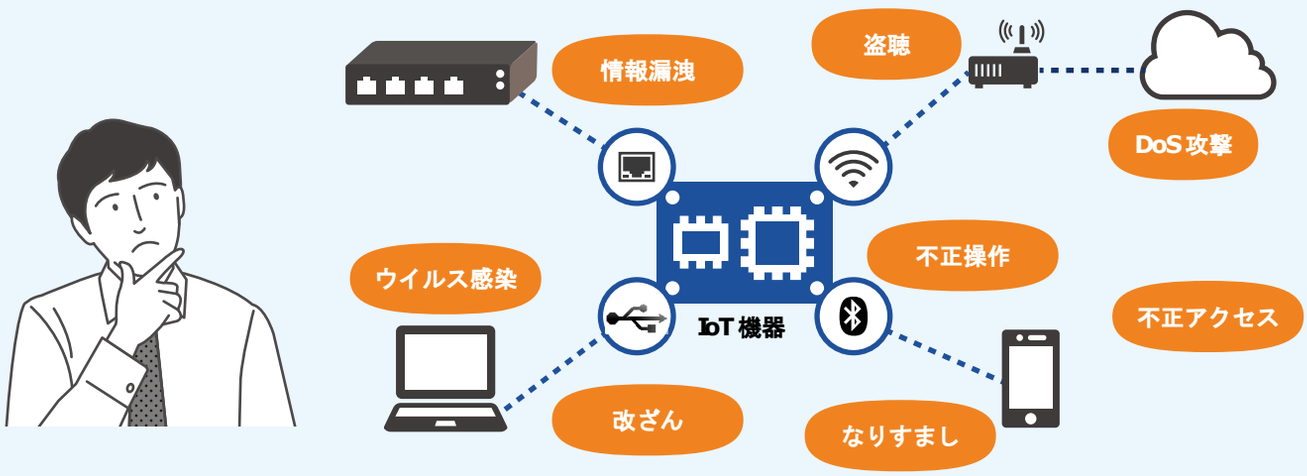
IoT脆弱性診断サービス

IoT機器、ブラックボックスのままで大丈夫ですか?

高度・複雑化するサイバー攻撃



根本対策！！

IoT機器の開発フェーズにおいて、セキュリティ強化をサポートするサービスです。
開発者にとって、攻撃者への対策を事前に設計へ入れ込むことは、非常に困難です。
一般的な第三者検証だけでなく、実際に開発を行っているセキュリティの専門家が設 計・開発に介入することで、リリース後の手戻りを抑えるとともに、リスクを見える化します。

セキュリティ・バイ・デザイン
企画・設計からセキュリティ観点を含めた製品計画が重要!

企画 設計 開発 運用 破棄

サイエンスパーク株式会社
セキュリティ検証サービス

3つの特徴

企画・設計段階のプロトタイプから診断

IoT機器の企画・設計から出荷検査まで、ご要望のフェーズにおいて脆弱性診断を行います。
一般的なソフトウェアと異なり、出荷後に問題発覚しますと、回収による修正のリスクがあり得ます。企画・設計段階から備えることでリスクを最小化します。

出荷後のご要望にも合わせた多様な診断プラン

既に出荷されたIoT機器に対しても潜在的な脆弱性を診断し、次版の設計に反映できる情報をご提供します。ハードウェアやデバイスドライバ開発の専門会社である、サイエンスパーク㈱では適切なタイミング・手段での診断をご提案します。

診断後のアフターサービス

診断結果の報告だけでなく、マイコンやハードウェア構成の問題を検出した場合は、チップや基板の実装方法・想定される攻撃への対策をご提案します。また、弊社で修正作業をお請けすることもいたします。

／ サービス内容 ／

IoT機器の各レイヤに対して攻撃者の視点でセキュリティリスクを診断します。

ハードウェア

採用予定のCPU・メモリ・セキュリティチップに対して、事前に問題点が無いかを調査し、実装時の注意点などを的確にアドバイスします。

ファームウェア

ファームウェアの設計時に、採用予定のOS・OSS・ベンダ提供SWの脆弱性を事前に診断します。ソースコードが無く、バイナリでの提供のみでも診断できます。

機器仕様による問題点の検出

例えばBluetoothの弱い認証方式など、脆弱性とは判断されないが攻撃の入り口になり得る、仕様上の問題点を事前に診断します。

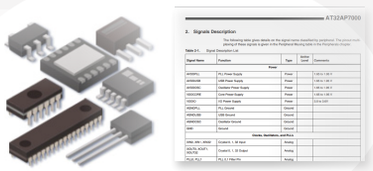
アップデート方式の診断

USBメモリやOTAなどのアップデート機能は、ファームウェア改ざんの起点となる代表的な機能であり、改ざんへの耐性の診断を行います。

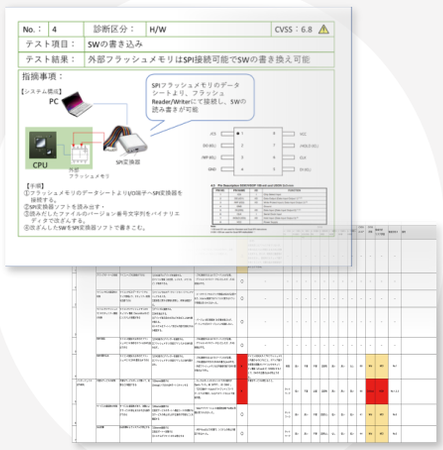
IoT機器の診断イメージ

ファームウェアの診断

ハードウェア



チップ仕様の診断



診断報告書

／ サービスフロー ／

事前準備		診断の実施		診断後		
診断対象の選定	**キックオフ**	**診断実施**	**診断速報**	**報告書提出**	**報告会**	**再診断**
対象システムの診断対象スコープを、事前の打ち合わせやドキュメント精査にて決めます。	選定結果をもとに、キックオフを実施し、診断期間や事前準備の打ち合わせを行います。	お客様とのお打ち合わせで同意した、各種診断を実施します。	診断作業中に危険度の高い脆弱性が発見された場合は、速報として報告します。	診断結果をまとめた報告書を作成します。	報告書の内容を基に、発見された脆弱性や具体的対策方法を説明します。	検出された脆弱性の改修確認を実施します。

すべてのフローをIoT機器の開発者様向けに強化します

お問い合わせ・ご相談はこちら

サイエンスパーク株式会社

〒252-0029 神奈川県座間市入谷西3-24-9
TEL: 046-255-2544　FAX: 046-255-0319
https://sciencepark.co.jp　sales@sciencepark.co.jp

IoT脆弱性診断サービスに関するWebサイトはこちら

SP2201-E2