

NEWS RELEASE

2026 年 10 月 5 日

株式会社ブロードバンドセキュリティ

IoT 機器の安全性を攻撃者視点で検証、 BB5ec が「IoT セキュリティ診断」を強化

～JC-STAR★1 適合評価支援に対応、実機・ファームウェアから API まで
横断的に検証～

情報漏えい IT 対策などセキュリティに特化したサービスを提供する株式会社ブロードバンドセキュリティ（本社：東京都新宿区、代表取締役社長：森澤 正人、以下 BB5ec）は、IoT 機器を攻撃者視点で検証する「IoT セキュリティ診断」の提供内容を拡充し、セキュリティ要件適合評価及びラベリング制度（JC-STAR）の★1（レベル 1）について、JC-STAR 検証事業者として適合評価の受託、チェックリストの作成、証跡の提供に対応します。

BB5ec の「IoT セキュリティ診断」は、情報セキュリティサービス基準審査登録制度における「機器検証サービス」として登録されています（サービス登録番号：018-0038-50）。これにより BB5ec は、独立行政法人情報処理推進機構（IPA）が定める JC-STAR 検証事業者に該当し、IoT 製品ベンダーからの依頼に基づき、JC-STAR★1 の適合評価を実施することができます。今回、この制度上の立場を活用し、従来の攻撃者視点によるセキュリティ診断と組み合わせて提供します。

【概要】

ネットワークカメラやルーターをはじめとする IoT 機器の普及が進む一方、これらの機器がサイバー攻撃の標的となるだけでなく、利用者が気付かないまま不正アクセスや不正送金などに関わる通信の中継に悪用されるリスクも顕在化しています。

BB5ec の「IoT セキュリティ診断」は、IoT デバイスの実機を使用し、デバイス固有の機能や通信、ファームウェアなどを攻撃者の視点から検証するサービスです。デバイス本体だけでなく、スマートフォンアプリや API も含めて診断することで、IoT 製品・サービス全体に潜むリスクの把握とセキュリティ対策を支援します。

【今回の強化内容】

1. JC-STAR★1 適合評価支援への対応

JC-STAR の★1・★2 は、IoT 製品ベンダー自身による自己適合宣言に基づいて適合ラベルが付与される方式です。一方で、★1 の適合基準・評価手順にもツールを使用した実機テストが含まれており、自社の体制や設備だけでは評価の実施が難しいケースがあります。

BB5ec は、JC-STAR 検証事業者として、IoT 製品ベンダーからの依頼に基づき★1 の適合評価を受託し、申請に用いるチェックリストを作成します。必要な評価項目について BB5ec が一貫して評価し、チェックリスト全体を作成した場合、IoT 製品ベンダーは「JC-STAR 検証事業者による適合評価」として適合ラベルを申請することができます。なお、自己適合宣言および適合ラベルの申請は IoT 製品ベンダーが行い、適合ラベルは IPA が付与します。

2. ハードウェア層・ファームウェアまで踏み込んだ検証

UART/JTAG 等のデバッグインタフェースの開放状況、フラッシュメモリからのファームウェア抽出、ファームウェア内にハードコードされた認証情報・暗号鍵の検出、搭載される OS・ミドルウェア・OSS コンポーネントの既知脆弱性 (CVEⁱ) の確認など、機器の内部構造にまで踏み込んだ検証を実施します。JC-STAR★1 の適合評価に加え、BB5ec が従来から培ってきた IoT セキュリティ診断の知見を活用し、対象機器の特性に応じて攻撃者が取り得る手法を想定した検証を行える点が、本サービスの特長です。

3. 証跡パッケージの納品

自己適合宣言方式では、申請時に IPA へ証跡を提出する必要はありませんが、適合ラベルの有効期間中は、チェックリストを裏付ける文書や実機テストの結果等の証跡を申請者が保管することとされており、IPA によるサーベイランス等の際に証跡の提出を求められることがあります。

BB5ec は、作成したチェックリストに加え、試験ログ、通信キャプチャ、ファームウェアのバージョン・ハッシュ値、対象機器および検証環境の情報、使用ツール、判定根拠などを含む証跡一式をパッケージとして納品します。適合ラベルの有効期間中の証跡保管や、IPA によるサーベイランス等の際の根拠説明に活用いただけます。

【サービス提供の背景】

IoT 機器は、家庭、オフィス、工場、店舗など幅広い環境で利用され、ネットワークに常時接続される機器も増えています。その一方で、IoT 機器を狙った探索や攻撃は継続して観測されており、機器そのものが攻撃の踏み台として悪用されるリスクも高まっています。

こうした中、IoT 製品に求められるセキュリティ対策は、大きな転換期を迎えています。

国内では、IoT 製品に備わるセキュリティ機能を共通の基準で評価・可視化する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が 2025 年に運用を開始しました。2026 年には通信機器やネットワークカメラを対象とした、より高度なセキュリティ要件も整備されるなど、対象や評価内容の拡充が進んでいます。

また、政府機関や重要インフラ事業者、地方公共団体などにおいて、JC-STAR の適合ラベルを取得した IoT 製品を調達時の選定に活用する取り組みも進められています。IoT 製品のセキュリティは、製品提供者による自主的な対策だけでなく、製品を選定・調達する側が確認する要件の一つになりつつあります。

こうした変化を受け、IoT 製品・サービスを提供する企業には、製品が正常に動作することを確認するだけでなく、第三者による不正操作や情報窃取、攻撃の踏み台化などのリスクがないかを、開発・提供段階で検証し、その安全性を説明できることがこれまで以上に重要となっています。

さらに、IoT サービスは、機器本体だけでなく、スマートフォンアプリやクラウドサービス、API など複数のシステムが連携して構成されるケースが一般的です。そのため、個々の機器だけでなく、機器、通信、アプリケーション、APIなどを横断し、サービス全体のセキュリティを検証することが求められます。

BB5ec は、こうした IoT 製品を取り巻くセキュリティ要求の高まりに対応するため、IoT デバイスの実機を用い、攻撃者の視点から不正操作、情報窃取、踏み台化などの可能性を検証する「IoT セキュリティ診断」を提供しています。

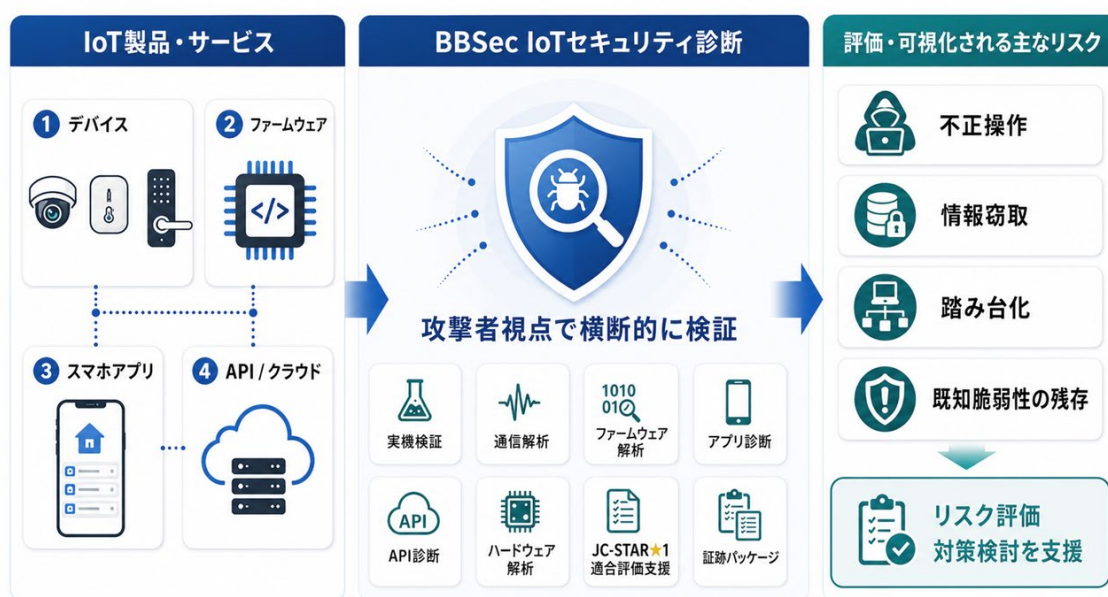
【サービスの概要】

BB5ec の「IoT セキュリティ診断」は、ネットワークにつながる IoT デバイスを、攻撃者と同じ視点から検証するセキュリティ診断サービスです。

IoT デバイスの実機を用いた動的解析に加え、ファームウェア等の静的解析を行い、対象となるデバイス固有の機能や各種プロトコル、インターフェースなどを利用して、主に次のリスクを検証します。

- 第三者による「不正操作」が可能ではないか
- 機器や通信から「情報の窃取」が可能ではないか
- サイバー攻撃の「踏み台」として悪用される可能性がないか
- 使用されている OS やミドルウェアに既知の脆弱性が存在しないか

デバイス本体だけでなく、デバイスを制御するスマートフォンアプリ、デバイスとサーバー間の通信を担う API までを対象とし、IoT 製品・サービスを構成する各要素に潜むセキュリティリスクを可視化します。対象機器の特性や利用シーンに合わせて診断項目を選定し、機器固有のリスクを考慮した検証を実施します。



発見した脆弱性については、CVSSⁱⁱ、CWEⁱⁱⁱなど、国際的に広く利用されている脆弱性の評価・分類体系等を踏まえ、標準的な指標で整理したうえで、BBSec 独自の基準でランク付けします。ただし、スコアの高さがそのまま対処の優先度になるとは限りません。BBSec は、誤検知・過検知を精査したうえで、実際に攻撃が成立するか、成立した場合に何が起きるかという観点から、対象機器の利用環境や保持する情報を踏まえてリスクを評価し、どこから直すべきかを示します。

BBSec はこれまで、IoT 機器に対する検証を通じて、スマートロックの不正開錠、スマート

タグの位置情報の改ざん、防犯用 IoT センサーの機能無効化、無線 LAN アクセスポイントにおける任意コマンド実行などを実証してきました。また、スマート TV を起点としてバックヤードシステムへ到達できた事例もあり、IoT 機器のリスクが機器単体にとどまらないことを確認しています。

BB5ec は今後も、IoT 機器をはじめとするデジタル製品・サービスについて、実際の攻撃を想定したセキュリティ診断を提供し、お客様の安全な製品・サービスの開発、提供及び利用を支援してまいります。

【BB5ec について】

BB5ec は、2000 年創業のトータルセキュリティ・サービスプロバイダーです。現状の可視化や診断から事故発生時の対応、24 時間/365 日体制での運用まで、フルラインアップのサービスを提供しています。高い技術力と豊富な経験、幅広い情報収集力を生かし、「サプライチェーンを狙った攻撃」「社会インフラを狙った攻撃」「AI 時代のセキュリティ」を解決すべき社会課題ととらえ、より多くのお客様を悪意ある攻撃者から守ることで、「便利で安全なネットワーク社会を創造する」というビジョンを実現します。

【本リリースに関するお問い合わせ】

株式会社ブロードバンドセキュリティ 経営企画部

TEL：03-5338-7430 E-mail：press@bbsec.co.jp

【本サービスに関するお問い合わせ】

株式会社ブロードバンドセキュリティ 営業本部

TEL：03-5338-7425 E-mail：sales@bbsec.co.jp

i CVE (Common Vulnerabilities and Exposures)

公開された個々の脆弱性を一意に識別するための共通識別子。脆弱性ごとに「CVE-年-番号」の形式で付与され、製品やサービスの既知脆弱性を確認する際に広く利用されます。

ii CVSS (Common Vulnerability Scoring System)

脆弱性の技術的な深刻度を共通の基準で評価するための国際的なスコアリング方式。攻撃の容易さや影響範囲などを基に、原則として 0.0～10.0 の数値で示します。

iii CWE (Common Weakness Enumeration)

ソフトウェアやハードウェアにおける、脆弱性の原因となり得る弱点を体系的に分類した共通リスト。入力値検証の不備など、脆弱性の種類や根本原因を整理する際に利用されます。