

JC-STAR制度とは何か、運営するIPAセキュリティセンターに聞く セキュリティ対策されたIoT機器が見分けやすく

グリッドコードの要件化により分散型電源の開発にも影響する、IoT製品のセキュリティ要件適合評価及びラベリング制度 (Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements, JC-STAR)。2025年3月から運用された制度だが、その背景や概要について、所管する情報処理推進機構 (IPA) セキュリティセンターの神田雅透フェローに聞いた。

-IPAについて教えてください

神田 経済産業省とデジタル庁が共同で所管している独立行政法人。主に「サイバーセキュリティの確保」「デジタル人材の育成」「デジタル基盤の提供」を担っている。このうちセキュリティセンターではサイバーセキュリティに関する啓発活動や評価・認証制度の運営を行っている。

-JC-STAR制度が必要になった背景は

神田 サイバー攻撃が増加している中、IoT機器向けの制度がなかった。ITに対する攻撃、例えばランサムウェアに感染した場合、業務は立ち行かなくなるものの必ず気づく。しかしIoT機器は想定通りの動作を行いつつ、それと並行して外部から勝手にDDoS攻撃の踏み台などに用いられるため、利用者が異常に気づけないまま使っていることも多い。

-JC-STAR制度の対象は

神田 ベンダー側でセキュリティ対策を行うことが前提となるIoT機器に対するラベリング制度として構築されたのがJC-STARである。対象は、IP通信機能を有し、かつ利用者が後からセキュリティ対策ソフトウェアのインストールなどの対策ができないIoT機

器。そのため、スマートフォンやパソコンは対象外になる。

基本的には機器を対象に適合ラベルを取得する制度だが、蓄電池システムだけは「システム」としても申請できるようにしている。これは納入者とは別のベンダーが後から内部の機器を入れ替えるようなケースがあまり想定されず、また内部ではIP以外の通信を用いることも少なくないため。

JC-STAR制度の適合ラベルにより、利用者は所定のセキュリティ要件に適合した製品を一目で見分けられるようになったほか、ベンダー側から見ても、これまで訴求しにくかった「セキュリティ対策」という価値をアピールしやすくなった。

-制度のレベルについて教えてください

神田 ★1から4までであり、★1で求める考え方としては、マルウェアに感染してポット化しないこと、特に感染した機器からの感染拡大を防止することを主眼に置いている。例えばパスワードの強度を高め、簡単に外部からログインされないようにする。また、IoT機器は売り切りも多い中、適合ラベル有効期限内はアップデートファームウェアなどのサポート提供を求める。



神田氏

このほか、運用中に生成されたデータを適切に削除できる機能も必要としている。

★1は入門中の入門で、IoT機器の種類を問わず共通して、必要最小限の16個の要件を求める。これに対し、★2以降は製品類型ごとの要件になる。また、★2までは民需、一般消費者向けで、★3、4は政府機関や重要インフラなどをはじめ、高度なセキュリティが求められる領域向けとなる。評価の仕方も★2までが自己適合型だが、★3、4は第三者機関で評価する形になる。

-どのようにラベル取得できるのか

神田 申請書類はIPAと経産省が共同で確認している。★1は自己適合宣言なので、16個の要件についてのチェックリストのほか、製品の製造情報なども確認する。ラベル取得までの時間は申請内容により変わる。2026年4月までにラベル取得した約230件では、半数程度が1カ月半以内であった一方、3カ月以上を要したものも少なくない。確認作業が終わり申請が受理されると、手数料振込後、2週間程度でラベルが発行される。



IPA説明資料より