

Armadillo が IoT 製品に対するセキュリティ適合性評価制度の★1 に適合予定 ～Armadillo を採用した IoT 製品開発に向け、セキュリティの検証・支援サービスも提供～

株式会社アットマークテクノ（本社：札幌市、代表取締役社長：實吉 智裕）は、主力製品である Arm+Linux の組み込みプラットフォーム「Armadillo（アルマジロ）」を、独立行政法人情報処理推進機構（IPA）が運用開始予定の IoT 製品に対する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）^{※1}」の基準★1 に適合させます。これにより、Armadillo を採用して機器を開発する IoT ベンダーは、セキュリティ水準の高い IoT 製品を容易に開発・製造することが可能となります。また、Armadillo を採用する IoT ベンダー向けに、開発した IoT 製品に対する★1 への適合の検証・支援サービスも提供予定です。

■背景

近年、IoT 製品の脆弱性を狙ったサイバー脅威が高まっています。JC-STAR は、一定のセキュリティ要件を満たした IoT 製品にラベルを付与する制度であり、IoT 製品の調達・購入・利用時に製品のセキュリティ機能を評価・可視化することを目的としています。JC-STAR は通信機能を持つ幅広い IoT 製品を対象としており、セキュリティ水準に応じて★1 から★4 までの基準が設けられています。★1 は 2025 年 3 月から運用開始予定で、適合するには IoT 製品に対して 13 項目と、IoT ベンダーに対して 3 項目の計 16 項目の要件を満たす必要があります。IoT ベンダーには高いセキュリティの知見が求められ、開発費の上昇と開発期間の長期化が予想されます。

■Armadillo は JC-STAR★1 のセキュリティ基準に適合予定

Armadillo は Arm プロセッサ・Linux OS 搭載の CPU ボードと IoT ゲートウェイからなる製品シリーズです。累計 80 万台を超える出荷実績があり、さまざまな IoT ベンダーが Armadillo を IoT 製品のプラットフォームとして採用しています。Armadillo シリーズに搭載されている IoT 製品向け Linux OS「Armadillo Base OS（以下、ABOS）」は、従来から高いセキュリティ機能を有していますが、今回 JC-STAR ★1 の IoT 製品に対する 13 項目の基準に適合するためのアップデートが予定されており、★1 基準を満たす IoT 製品を容易に開発することが可能となります。加えて、今後の★2 以上の基準や、米国の U.S. Cyber Trust Mark、EU のサイバーレジリエンス法などの国際的な IoT セキュリティ制度に対応するため、引き続きアップデートを行う方針です。

IoT製品に対する適合基準	
カテゴリ	適合基準の概要
識別・認証、アクセス制御	(1) 適切な認証に基づくアクセス制御 (2) 容易に推測可能なデフォルトパスワードの禁止 (3) パスワード等の認証値の変更機能 (4) ネットワーク経由のユーザ認証に対する総当たり攻撃からの保護
脆弱性対策、ソフトウェア更新	(6) ソフトウェアコンポーネントのアップデート機能 (7) 容易かつ分かりやすいアップデート手順 (8) アップデート前のソフトウェアの完全性の確認機能 (10) ユーザーが型式番号を認識可能とする記載・機能
インターフェイスへの論理アクセス	(13) 不要かつリスクの高いインターフェースの無効化(物理的・論理的な通信ポート等)
データ保護	(11) 製品に保存される守るべき情報の保護(保存データの暗号化、匿名化等)
データ保護	(12) ネットワーク経由で伝送される守るべき情報の保護(通信の暗号化、保護された通信環境の利用等)
データ保護	(15) 製品内に保存される守るべき情報の削除機能
レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の認証情報やソフトウェア設定の維持(初期状態に戻らないこと)



■Armadillo シリーズの充実したセキュリティ機能

Armadillo シリーズに搭載されている ABOS は、コンテナアーキテクチャを採用し、OS 環境とアプリケーション（コンテナ）環境が明確に分離されていることが特長です。OS とコンテナはそれぞれ独立してアップデートが可能な構造のため、ABOS が標準搭載しているソフトウェアアップデート機能で脆弱性への対処が容易です。

さらに、コンテナごとにファイルやデバイス等のリソースへのアクセス権限を明示する仕組みなので、仮にアプリケーションに脆弱性があったとしても権限以上の不正な動きをしにくい特長があります。

また、IoTベンダーがソフトウェアの脆弱性を管理するためのSBOM^{※2} (Software Bill of Materials) に関する機能を拡充させています。ABOSのSBOMを提供していることに加え、アプリケーションの開発環境ではコンテナのSBOMを生成するツールが用意され、2024年11月にはSBOMからの脆弱性診断機能も提供予定です。また、ツールで生成されたSBOMを、デバイス運用管理クラウドサービス「Armadillo Twin」に登録することで、新たに脆弱性が発見された際にアラートで通知する機能を2024年度中にリリース予定です。脆弱性に対処したソフトウェアはArmadillo TwinからOTA (Over the Air) でアップデートすることも可能で、セキュリティ水準の高いIoT製品の開発・運用管理を実現できます。

■Armadilloを採用したIoT製品に対してラベル付与の申請手続きをサポート

ArmadilloはIoT製品のプラットフォームとして、半完成品の状態でも各種のセキュリティ要件を満たし、★1に適合する予定です。IoTベンダーは、独自のアプリケーション部分と拡張開発したハードウェア部分を検証することで、完成品のIoT製品として★1に適合することができます。また、IoTベンダーがセキュリティに関する十分な知見を持ち合わせていない場合でも、パートナー企業と連携して★1への適合を検証・支援するサービスを提供予定です。



[※1] 独立行政法人 情報処理推進機構: セキュリティ要件適合評価及びラベリング制度 (JC-STAR)

<https://www.ipa.go.jp/security/jc-star/index.html>

[※2] SBOM (Software Bill of Materials): ソフトウェアがどのような構成要素から成り立っているかを示すリストのことで「ソフトウェア部品表」とも呼ばれます。これにより、ソフトウェアのトレーサビリティが確保され、脆弱性残留リスクの低減や脆弱性対応期間の短縮に繋がります。

株式会社アットマークテクノおよび「Armadillo」について

株式会社アットマークテクノは、組み込みプラットフォームのリーディングカンパニーとして、独自ブランド「Armadillo (アルマジロ)」を展開しています。「Armadillo」は2001年に初代機を開発して以来、20年以上にわたり累計80万台を超える省電力CPUボードとIoTゲートウェイ、その関連技術を提供し、データロガーや通信機器、産業機器の操作盤や情報端末など、IoT機器プラットフォームとしてご採用いただいています。

・株式会社アットマークテクノの詳細情報 <https://www.atmark-techno.com>

本件に関するお問い合わせ

報道関係のお問い合わせ：

株式会社アットマークテクノ 営業部 マーケティンググループ (担当：中村)

TEL: 011-299-1501 E-mail: info@atmark-techno.com

購入に関するお問い合わせ：

株式会社アットマークテクノ 営業部

TEL: 03-5904-8031 E-mail: sales@atmark-techno.com

* 「Armadillo」は株式会社アットマークテクノの登録商標です。その他本リリースに記載の会社名および商品名は、各社・各団体の商標または登録商標です。TM、®マークは記載していない場合があります。