資料5

JC-STARスマートホーム★2に向けた ECHONET Liteの対応について

2025/11/25

JEITA スマートホーム部会 スマートホームセキュリティWG
エコーネットコンソーシアム

目次

① JC-STAR スマートホーム分野★2で想定される脅威とECHONET Liteの課題

② ★2におけるECHONET Liteの対応について

③ 今後のスケジュール（案）

目次

① JC-STAR スマートホーム分野★2で想定される脅威とECHONET Liteの課題

② ★2におけるECHONET Liteの対応について

③ 今後のスケジュール（案）

スマートホーム★2で想定される脅威

■ スマートホームIoT機器での**特有の状況**を踏まえて、考慮する主な脅威を修正

【想定されるスマートホームでのセキュリティ脅威】
- MiraiやMirai亜種による攻撃
- 不正F/Wや脆弱性を突いた遠隔コード実行
- 機器初期設定時の乗っ取り
- 踏み台による他の機器への攻撃

【スマートホーム★2の位置づけの概要】
- スマートホームで想定される脅威に対抗できる
- 低コストで自己評価できる
- スマートホーム分野で必要となる海外制度の基準と整合する

★2で考慮する主な脅威の絞り込み

★1で考慮する主な脅威	スマートホーム★2で考慮する主な脅威	★2での修正の理由
1. ①弱い認証機能、②脆弱性の放置、③未使用インタフェースの有効化により、外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	1. ①弱い認証機能、②脆弱性の放置、③未使用インタフェースの有効化により、ネットワークからの不正アクセスの対象となり、不正F/W配布や遠隔コード実行等の攻撃を受けることで、情報漏えい、情報や制御指示の改ざん、機能異常の発生につながる脅威	RTOSで動作することの多いスマートホームIoT機器では、マルウェア感染よりも不正F/W配布や遠隔コード実行のリスクが高いため。 また、改ざんについては制御指示が対象となることも明記。
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威	2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威	
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威	3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威	
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威	4. ①機器初期設定時の乗っ取り、②ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威	必ずしもIoT技術に詳しくない一般の利用者が設定するスマートホームIoT機器であるため、機器初期設定時の乗っ取りのリスクについても明記。

スマートホーム★2におけるECHONET Liteの課題

- ★２にてECHONET Liteでも用いている「制御指示」、「機器が保存又は通信する、動作情報およびセンサ収集情報」が「**守るべき資産**」として、★１から追加で定義
- アタックサーフェスとして、IP通信を行う部分（クラウド通信、機器間通信を問わず）を、★１から追加で対象とする
- 現行のECHONET Liteでは、スマートホーム分野★2の要件を満たすことができないと判断

IoT製品において守るべき資産	★1で想定する守るべき資産	スマートホーム分野★2で想定する守るべき資産
1. IoT機能 機器やシステムがIoTにつながるための機能	・有線通信機能 ・無線通信機能	・有線通信機能 ・無線通信機能
2. 本来機能 「モノ」本来の機能、セキュリティ対策・セーフティ対策のための機能	・セキュリティ機能	・セキュリティ機能 ・**制御指示**
3. 情報 ユーザの個人情報、収集情報、各機能の設定情報など	・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・機器の意図する使用において、機器が収集し、保存又は通信する、個人情報等の一般的に機密性が高い情報	・通信機能に関する設定情報 ・セキュリティ機能に関する設定情報 ・**機器が保存又は通信する、動作情報およびセンサ収集情報** ・ユーザに関する設定情報 ・機器の初期ネットワーク設定情報 ・機器のファームウェア
4. その他の物理的資産 ユーザの健康・生命やIoT機器が内蔵する物理的資産	-	-

目次

① JC-STAR スマートホーム分野★2で想定される脅威とECHONET Liteの課題

② ★2におけるECHONET Liteの対応について

③ 今後のスケジュール（案）

JC-STAR スマートホーム分野★2セキュリティ要件案への対応

- スマートホーム分野★2 セキュリティ要件案（特に通信路保護）をふまえて、過去検討済の仕様をベースに、実運用を想定して改善した「ECHONET Lite Device Authentication(DA)仕様書」を策定中
- DA仕様の★2適合基準の達成可否確認について、スマートホームSWG等にご相談・確認実施

【スマートホーム分野★2 セキュリティ要件案（抜粋）】

特に「制御指示」、「機器が保存又は通信する、動作情報およびセンサ収集情報」に関わるセキュリティ要件案を以下に抜粋

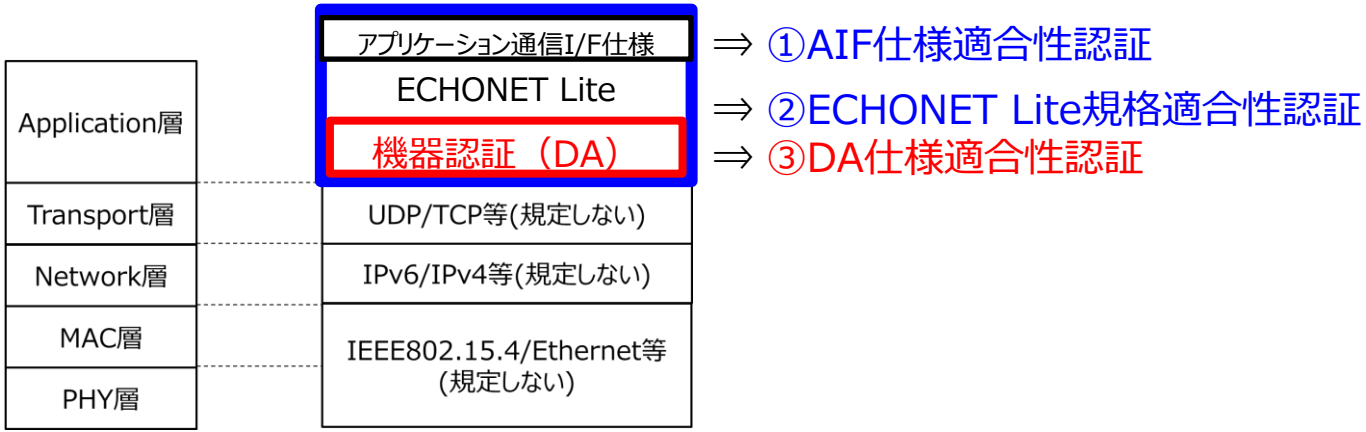
番号	分類	要件内容		適合基準	DA仕様での対応
1-5	技術要件	IoT機器	IoT機器が、制約のある機器ではない場合、ネットワークを介して行われる認証に対する総当たり攻撃等のブルートフォース攻撃が実行できないようにするメカニズムを保有しなければならない。	IPA様にて今後検討（DA仕様が基準を満たすことをスマートホームSWGで確認）	ペアリング（期間制限、電子証明書を用いた相互認証）
5-1	技術要件	IoT機器	IoT機器は、ベストプラクティスの暗号技術を使用してセキュアに通信をしなくてはならない。		暗号通信・メッセージ認証、送信元認証（AES-CCM、ECDSA）
8-2	技術要件	IoT機器	IoT機器と他のIoT機器や必須付随サービスとの間で通信されるIoTデータ(機器の動作情報やセンサ収集情報)の機密性は、技術の特性と使用法に適した暗号技術によって保護されなければならない。		暗号通信（AES-CCM）

Device Authentication(DA)仕様の位置付け

CONFIDENTIAL

- 本仕様は、ECHONET Lite機器間において、機器がお互いを識別し、通信対象を適切に限定して安全に通信を行うための機能を提供

- 相互接続性が高いECHONET Liteプロトコルを使用できることを前提とした、**機器認証（Device Authentication：DA）機能**を備えた通信仕様をECHONET Lite Device Authentication仕様として規定



目次

① JC-STAR スマートホーム分野★2で想定される脅威とECHONET Liteの課題

② ★2におけるECHONET Liteの対応について

③ 今後のスケジュール（案）

今後のスケジュール（案）

- 「ECHONET Lite DA仕様書 2ndDraft」のエコーネットコンソーシアム会員レビュー完了。コメント対応検討完了し、3rd Draftとして、会員レビュー実施中。およびスマートホームSWGへの仕様照会を予定
- 「DA仕様適合性 認証試験仕様書 第1版Draft」を並行して会員レビューを実施中
  今後、「認証試験ツール」について開発着手予定
- IPA様でのJC-STARスマートホーム★2運用開始（来年夏～秋の開始見込み）に合わせて「DA認証制度」構築について検討着手。
  併せて、関係各所へのヒアリングを通じて、DA仕様で用いる電子証明書・認証局の運用検討中。

IPA様によるJC-STAR制度のスマートホーム★2の検討スケジュールと足並みをそろえて、仕様書・ツール類などの公開、規格適合性認証制度の運用を開始予定

参考資料

背景：IoT製品に対するセキュリティ適合性評価制度について

✓ 2024年度より、経済産業省にて、IoT製品に対するセキュリティ適合性評価制度☆１の運用が開始予定。
✓ ☆2以上の特定分野として、スマートホーム／工場システム等が挙げられ、JEITAにスマートホーム基準等の検討要請があったもの。

【目的】

以下を目的とする 任意の制度（今後見直される可能性あり）。

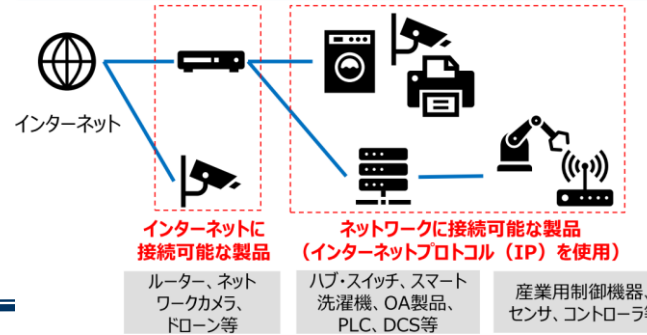
① 政府機関・企業等のIoT製品調達ニーズへの対応
共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度が必要

② 特定分野で使用されるIoT機器の最低限のセキュリティ確保
国民が安心してネットワークを使用したサービスを利用できるよう、**特にリスクの高いサービス分野（スマートホーム／工場システム等）**において使用されるIoT機器の最低限のセキュリティ基準を整備

【対象製品】

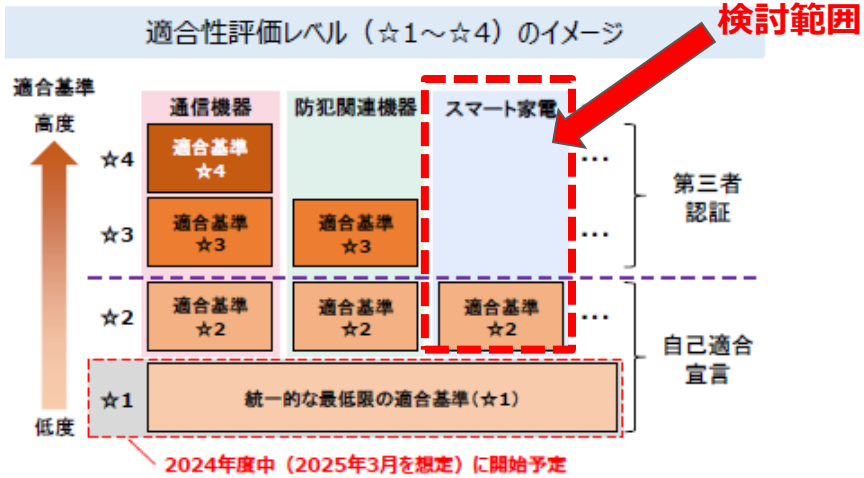
間接的又は直接的にインターネットに接続する機器が対象。

対象製品の概要



（経済産業省 サイバーセキュリティ研究会WG3 IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会公開資料より作成）

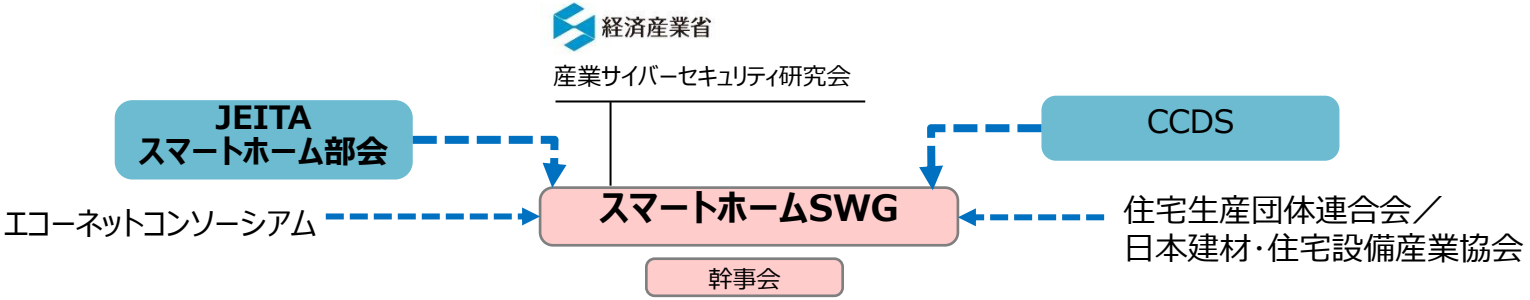
【レベル】



レベル	位置付け	適合基準	評価方式
☆3以上	**政府機関等や重要インフラ事業者、大企業の重要なシステムでの利用を想定**したIoT製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを**独立した第三者が評価して示す**もの	製品類型別	第三者認証
☆2	**IoT製品類型ごとの特徴を考慮**し、☆1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの		自己適合宣言
☆1	IoT製品として共通して求められる**最低限のセキュリティ要件**を定め、それを満たすことを**IoT製品ベンダーが自ら宣言**するもの	製品類型共通	

IoT製品に対するセキュリティ適合性評価制度　特定分野　スマートホーム　検討体制

- ✓ 前述の検討を行うためには、幅広い関係者を巻き込んだ議論が必要である。
- ✓ そこで、現状、JEITAスマートホーム部会が権能を担っている経済産業省内の「産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化）スマートホームサブワーキンググループ」のスキームを拡大し、検討を進めて行く。



オブザーバ：IPA／経済産業省／その他関連組織

主査：JEITA/CCDSから選出、共同主査形式
委員：JEITA/CCDSの両会員企業から、IoT製品メーカ、ユーザを中心に委員を招聘する。
主な活動内容：
- **評価基準検討**
  - ースマートホームの定義
  - ースマートホームで実施すべきセキュリティ対策の検討
  - ースマートホーム関連の各IoT製品類型におけるIoTセキュリティラベル☆１の活用及び☆２以上の整備要否の検討
  - ー☆２以上の整備のIoTセキュリティ適合性評価制度（IPA+経産省）への依頼
- **普及促進検討**
  - ースマートホームの普及・セキュリティ対策状況の現状確認、セキュリティを考慮した普及促進策の検討
  - ーIoT製品の販売・購入の促進施策の検討、IoT製品類型の活用に関する製品ベンダー、調達関係者との合意

スマートホームSWG 趣意書

■SWGの目的・役割

・IoT機器の急増に加え、IoT機器を狙った攻撃も多く、**IoT機器の脆弱性を狙ったサイバー脅威が高まってきている**。
・諸外国でもIoT製品のセキュリティ対策に関する制度検討が進んでおり、我が国のIoT製品がグローバルマーケットから弾き出されないよう、諸外国の取組も踏まえて、**共通的な物差しで製品のセキュリティ機能を評価・可視化**し、**調達者が求めるセキュリティ水準のIoT製品を容易に選定**できるようにした、IoTセキュリティ適合性評価制度が開始されることになった。
・JEITAスマートホーム部会スマートホームサイバーセキュリティWGが兼ねている、経産省産業サイバーセキュリティ研究会WG1のスマートホームSWGのスキームにおいて、IoTセキュリティ適合性評価制度の開始を踏まえ、スマートホーム分野における**☆１のラベルの活用**及び**スマートホーム関連機器の☆２以上のラベル・認証の必要性**に関して検討し、**消費者向けのIoTセキュリティラベルの普及に合わせて、スマートホーム自体の普及施策**を検討を行う。

■SWG構成メンバ（想定）

・JEITA (スマートホーム部会 会員企業／団体)
・スマートホーム関連団体（CCDS／住宅生産団体連合会／日本建材・住宅設備産業協会／エコーネットコンソーシアム 等）
・関連省庁（デジタル庁、経済産業省等）、IoTセキュリティ適合性評価制度（IPA、経済産業省）
・消費者団体、スマートホーム関連機器の販売・流通事業社（大手家電量販店、大手ネットモール等）
※ 必要に応じて、JEITA関連委員会、スマートホーム関連企業等に本SWGへオブザーバとして参加を要請する。

■SWG開催について

・原則、隔月1回程度の開催を予定。別途幹事メンバーによる幹事会を組織する。

IoT製品に対するセキュリティ適合性評価制度　特定分野　スマートホーム　検討項目

✓ IoTセキュリティ適合性評価制度の開始も踏まえ、スマートホーム分野における☆１のラベル（2025年3月頃～）の活用及びスマートホーム関連機器の☆２以上のラベル・認証の必要性に関して検討を行う。

【主な検討事項】 ※既に整理・検討されたものがあれば、それをベースに検討

①スマートホームの定義（複数のモデルも可）
- スマートホームのネットワーク構成、通信方式、利用が想定される機器（IoT製品を含む）等の特定[Step2]
- スマートホームにおけるセキュリティ脅威の検討[Step2]

②スマートホームで実施すべきセキュリティ対策の検討（モデル別やレベル別も視野に）
- スマートホーム全体のセキュリティガイドラインの整備（更新）、認証・ラベリング制度の要否の検討[Step5]
- スマートホーム関連の各IoT製品類型に求めるセキュリティ要件の検討（IoT製品類型別）[Step2]

③スマートホーム関連の各IoT製品類型におけるIoTセキュリティラベル☆１の活用及び☆２以上の整備要否の検討
- 第三者認証を求める☆３以上のニーズの有無[Step2]
- ラベルを活用するIoT製品の販売・購入ルートの特定[Step2]
- ☆１を活用するIoT製品の製品ベンダーへのラベル取得の促進
- ☆１を活用するIoT製品の販売・購入の促進施策の検討（ハウスメーカー、流通事業者等へのアプローチ等）　※施策の実施は別途
- ☆２以上を整備するIoT製品類型の活用に関する製品ベンダー、調達関係者（ハウスメーカー、流通事業者等）との合意[Step3]

④☆２以上の整備のIoTセキュリティ適合性評価制度（IPA+経産省）への依頼
- 基準検討WGの立ち上げ・検討への協力（詳細な基準の議論は制度側のWGで実施、委員等を出す想定）[Step4]

⑤スマートホームの普及・セキュリティ対策状況の現状確認、セキュリティを考慮した普及促進策の検討 ※他WGとの連携も含む

JEITA 一般社団法人 電子情報技術産業協会 Japan Electronics and Information Technology Industries Association