Secure Innovation

沖縄から日本全国、アジア、そして世界へ

IoTセキュリティ試験/評価サービス

IoTセキュリティ試験/評価

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

以下のようなIoTセキュリティ試験/評価をご相談いただけます。

1.ガイドライン・規約等に沿った評価

IoT機器や業界・組織によって求められるガイドライン・ポリシーのセキュリティ基準要件の項目を可能な範囲で評価いたします。

- 1 EN 18031
- 2 CRAに向けたサイバーセキュリティ支援サービス
- 3 JC-STAR★1
- 4 IEC/JIS T 81001-5-1 脆弱性試験・侵入試験
- その他 EN 303 645

2.OWASP IoT TOP10に基づく試験

OWASPより公開されている「OWASP IoT Top 10 2018」に基づいた項目を試験いたします。すべての項目はもちろん、選定した対応等も柔軟にご相談いただけます。

3. ご希望に沿ったテストの実施

IoT機器に対して適切と思われる試験項目を選定し、セキュリティのテスト手法を駆使し手動でのテストや自動テストツールを組合せて網羅的な試験を実施します。

- 脆弱性テスト
- ファジングテスト
- ペネトレーションテスト

1.ガイドライン・規約等に沿った評価
欧州向けIoTサイバーセキュリティの動向（EU）

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

➢ RE指令

無線機器の指令であり、欧州で当該機器を上市する場合には準拠が必須となります。
2014/53/EU（Radio equipment directive）

・サイバーセキュリティに関連する要求事項を補足する規約としてDR(EU) 2022/30があり、2024年8月1日適用予定でしたが、**2025年8月1日に延期。**

・技術的な要求の仕様を定める整合規格(Harmonized Standards) が**2025年1月30日付で条件付きでOJ（EU官報）に掲載**。

・セキュリティ要件に対応するガイドラインとして、CEN/CENELECより **EN18031**のPublish版が発行。

2024年8月
EN18031発表

2025年8月
DR(EU) 2022/30 適用開始

➢ CRA（欧州サイバーレジリエンス法案）

欧州市場で販売される、デジタル要素を有する様々な製品のセキュリティ対応を義務付け。（EU Cyber Resilience Act）

要求事項

・一部を除くデジタル要素を備えた**全ての製品が対象**。
・SBOM作成や更新プログラム提供など、セキュリティ要件への適合（自己適合宣言/第三者認証）

・重要なデジタル製品のうち、低リスク製品で
EN規格対象の場合、自己宣言。
EN規格対象外の場合、第三者認証。
高リスク製品は 第三者認証。
EUCC認証を利用する場合は、第三者認証のみ可能。
詳細は、後述のCRAの適合性認証方法を参照。
注：EUCCとはIoT製品を対象とする欧州サイバーセキュリティ認証。EN規格とは欧州整合化規格。

・脆弱性の悪用やインシデント発見後、24時間以内にENISAへの報告を義務化。

・**最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内の罰則あり。**

上記の要求事項を守らなければ、欧州市場に上市できない。

1.ガイドライン・規約等に沿った評価
1-1.欧州向けIoTサイバーセキュリティの動向（EU）

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

➢ RE指令　2014/53/EU（Radio equipment directive）

無線機器の安全性要件や電磁両立性、およびセキュリティ要件を規定する
EUの規制です。
EU市場での無線機器の販売と流通に関する要求事項となります。

対象機器例

無線でデータを送信受信する機器。

例えば、無線LANルータ、 IoTデバイスや、Bluetoothデバイス等

適合性評価の方法

Moduld A（自己宣言型）

・自己で機器の適合性を評価
・機器が低リスクの場合に対応

Moduld B（型式検査型）

・認証機関で適合性を評価
・機器が比較的高リスクの場合に対応

製品の特性とリスクレベル等を考慮し、製造者が、適合性評価を決定する。

1.ガイドライン・規約等に沿った評価
1-1. RE指令　サイバーセキュリティ要件 EN 18031

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

➢ **EN 18031**　※機器の機能によって、18031-1～3を行う

EN 18031-1

インターネットに接続された無線機器の共通セキュリティ要件。

制限事項：パスワードを意図的に使わない機器は、NBでの適合性の評価を受ける必要がある。

EN 18031-2

データ保護やプライバシーに関する要件。

制限事項：保護者の権限が意図的に外される機器は、NBでの適合性の評価を受ける必要がある。

EN 18031-3

無線機器におけるセキュリティ技術に関する要件。

制限事項：対象のすべて機器でNBでの適合性の評価を受ける必要がある。

機能

インターネットに接続された無線機器

個人データを処理する機能がある機器

金銭、貨幣価値又は仮想通貨を処理可能な機器

1.ガイドライン・規約等に沿った評価

1-1. EN 18031の工程

Moduld A（自己宣言型）

工程 EN18031-1及び-2	詳細	
必要ドキュメントの準備	Required informationに作成で必要なドキュメントの準備	弊社サービス
Required information 作成	試験に必要なRequired informationを作成	①R/I作成サービス（技術サポート）
Applicability Conceptual 試験 Appropriate Conceptual 試験	**要件・概念の試験確認** 設計やコンセプト観点で機器がどのようなセキュリティ要件を満たすべきかという基本的な概念を確認する試験の実施	②Conceptual 試験サービス
Applicability Functional 試験 Appropriate Functional 試験	**機能試験** セキュリティ設計が正しく適用され、機能的にも、運用でも、Required information通りに機能しているか試験の実施	③ Functional 試験サービス
御社にて自己宣言		

1.ガイドライン・規約等に沿った評価

1-2. CRA（Cyber resilience act）適合性評価

➢ CRA（Cyber resilience act）とは

この規則は、デジタル製品がより少ない脆弱性で市場に投入され、製造業者が製品のライフサイクル全体にわたってセキュリティを考慮することを保証することにより、デジタル要素を備えた安全な製品の開発の境界条件を設定することを目的としています。

対象機器例

デジタル要素を含む製品。

例えば、ルータ、スイッチ、 IoTデバイスや、個人用ウェアラブル製品
商用利用されるソフトウェア

適合性評価の方法

Moduld A（自己宣言型）

・自己で機器の適合性を評価

・機器が低リスクの場合に対応

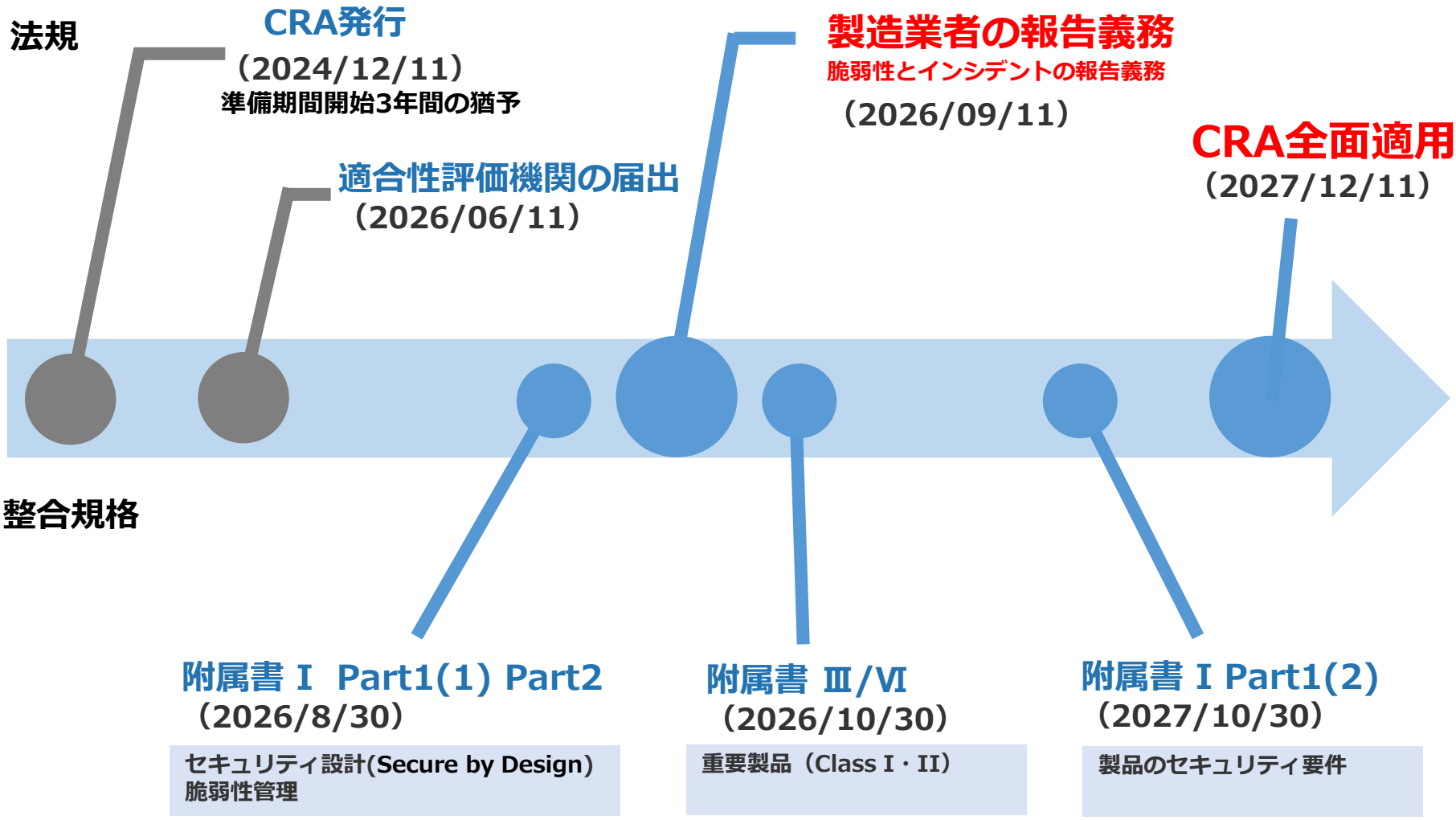
Moduld B（型式検査型）

・認証機関で適合性を評価

・機器が比較的高リスクの場合に対応

製品のカテゴリにおけるリスクレベル等を考慮し、適合性評価が決定される。

1.ガイドライン・規約等に沿った評価
1-2. CRA適用に向けた今後のスケジュール



1.ガイドライン・規約等に沿った評価
1-2. CRAに向けたサイバーセキュリティ支援サービス

CRAへ向けて必要な対策と支援について

■現時点においては、CRAではまだ整合規格がでていないため、ENISAが提供している対応表等により、関連性が高い標準規格を元にサイバーセキュリティ支援サービスをご提供致します。

対策	サービス
CRAの規格理解	トレーニング

1.ガイドライン・規約等に沿った評価
1-2. CRAへ向けて必要な対策と支援について

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

CRAへ向けて必要な対策と支援について

サイバーセキュリティ要件	サービス
セキュア開発プロセスの構築	**プロセスの構築支援** **①GAP分析** **②構築支援** 以下内容も含めてのご支援となります。 **- セキュア開発プロセス** - 脆弱性管理プロセス - 報告義務への準拠
リスクアセスメント	**リスクアセスメント** ①トレーニング **②サイバーセキュリティ試験に向けての準備**
製品のサイバーセキュリティ要件の適用及び試験	**サイバーセキュリティ試験** IEC 62443 4-2、EN 18031 の要件を用いた試験を実施
技術文書の作成	**技術文書の作成支援**

1.ガイドライン・規約等に沿った評価
1-2. CRAへ向けて必要な対策と支援について

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

CRAへ向けて必要な対策と支援について

脆弱性管理要件

SBOMの作成

脆弱性管理プロセスの構築

報告義務

報告義務への準拠

・アクティブな脆弱性発生時
・インシデント発生時

サービス

SBOM構築支援

SBOM作成ツール
- ONEKEY
- SBOM.JP

プロセスの構築支援

①GAP分析
②構築支援

以下内容も含めてのご支援となります。
- セキュア開発プロセス
- **脆弱性管理プロセス**
- **報告義務への準拠**

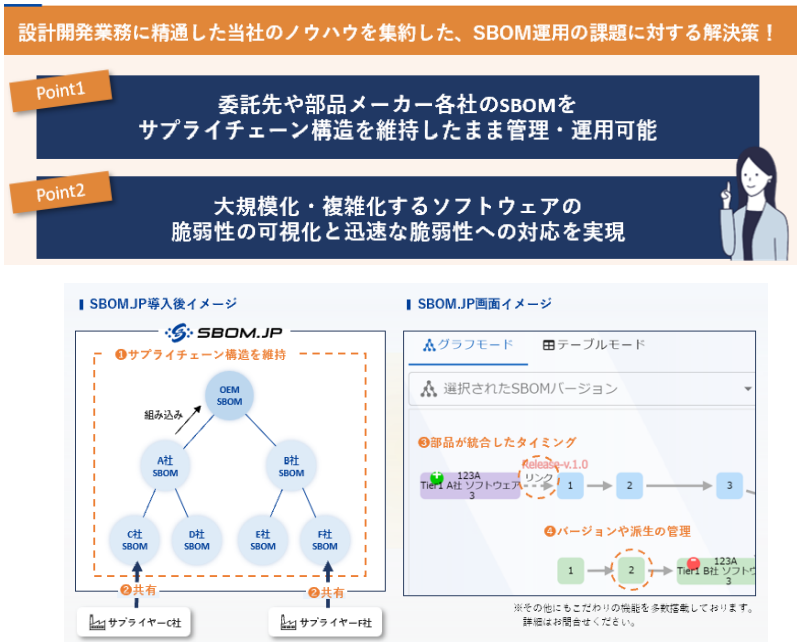
1.ガイドライン・規約等に沿った評価
1-2. CRAへ向けて必要な対策と支援について

CRAの付属書には、SBOMの利活用が明示されていることや
経済省が「重要インフラ保護」の観点からSBOMの活用、デジタル庁の推進計画の中でも
SBOMの利用が言及されています。

➢ SBOM管理・脆弱性管理支援ツール

ONEKEY

SBOM.JP



運用方法についてもお気軽にご相談ください。

1.ガイドライン・規約等に沿った評価
1-3.国内IoTサイバーセキュリティの動向

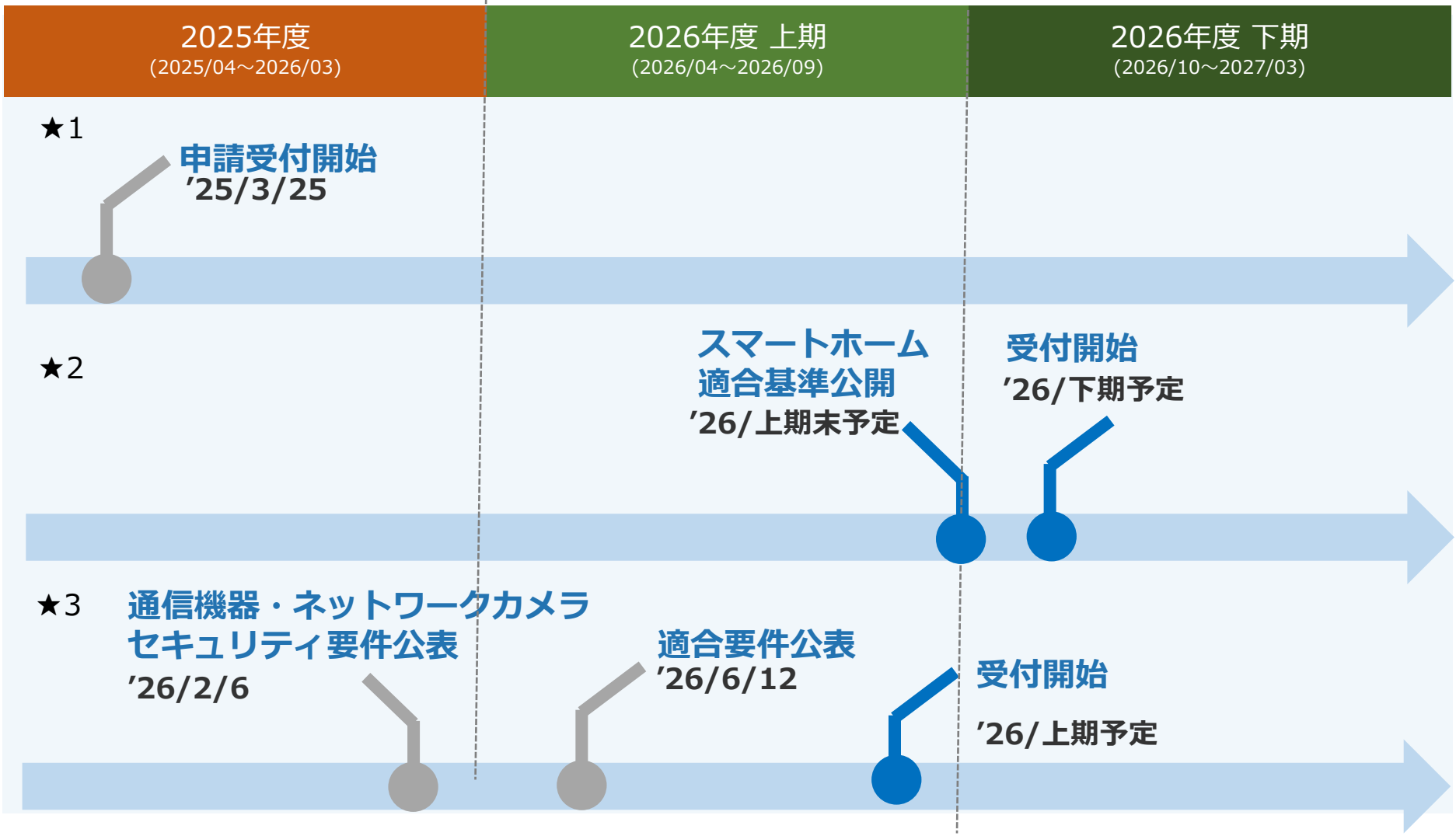
IPAが運営するJC-STAR制度は、2024年8月に経済産業省が公表した制度構築方針に基づき、国内外の規格（例：ETSI EN 303 645やNISTIR 8425）と調和しつつ、独自のセキュリティ基準でIoT製品の適合性を確認・可視化する制度。求められるセキュリティ水準に応じて適合基準・評価手順を定め、適合が認められた製品には二次元バーコード付き適合**ラベル**の付与を行う。

※JC-STAR：Labeling scheme based on Japan Cyber-Security Technical Assessment Requirements

レベル	位置付け
★4	政府機関や重要インフラ事業者、地方公共団体、大企業等の重要なシステムでの利用を想定した製品類型ごとに★1（レベル1）、★2（レベル2）に追加して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
★3	
★2	製品類型ごとの特徴を考慮し、★１（レベル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
★1	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

参考：セキュリティ要件適合評価及びラベリング制度：
https://www.ipa.go.jp/security/jc-star/index.html

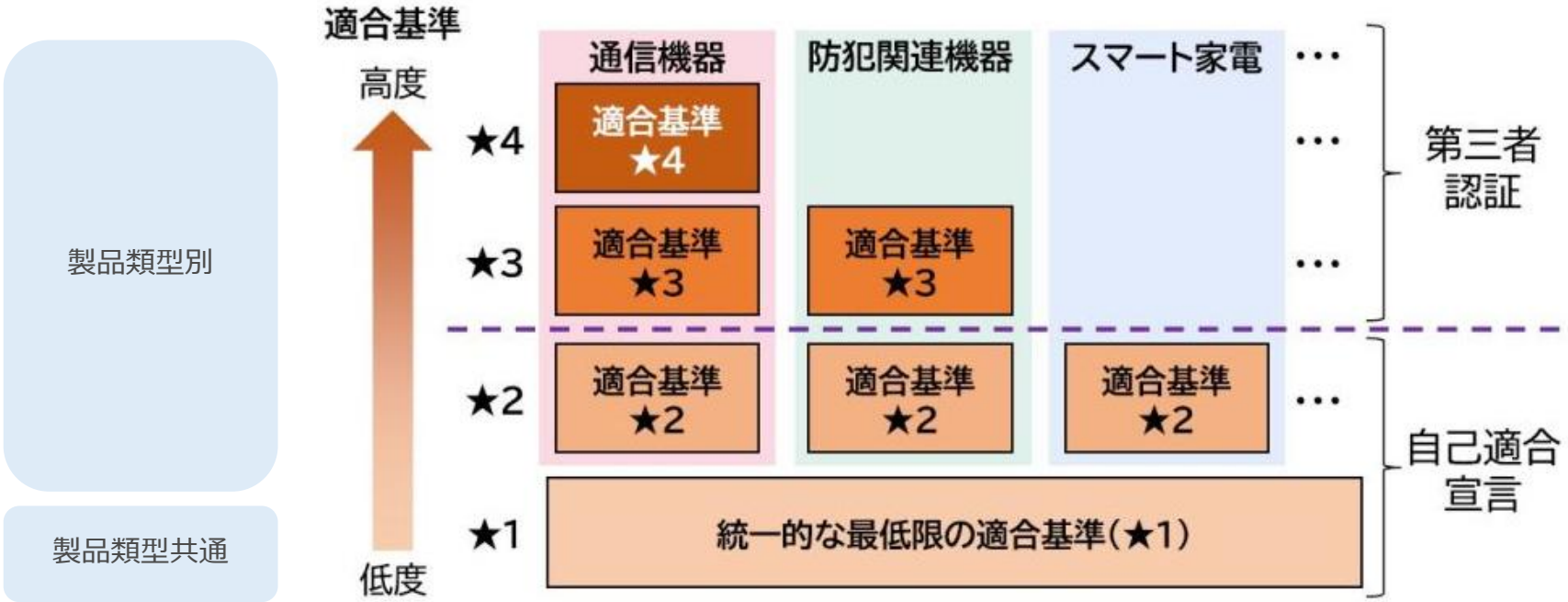
1.ガイドライン・規約等に沿った評価
1-3.国内IoTサイバーセキュリティの動向
JC-STAR スケジュール



1.ガイドライン・規約等に沿った評価
1-3.国内IoTサイバーセキュリティの動向

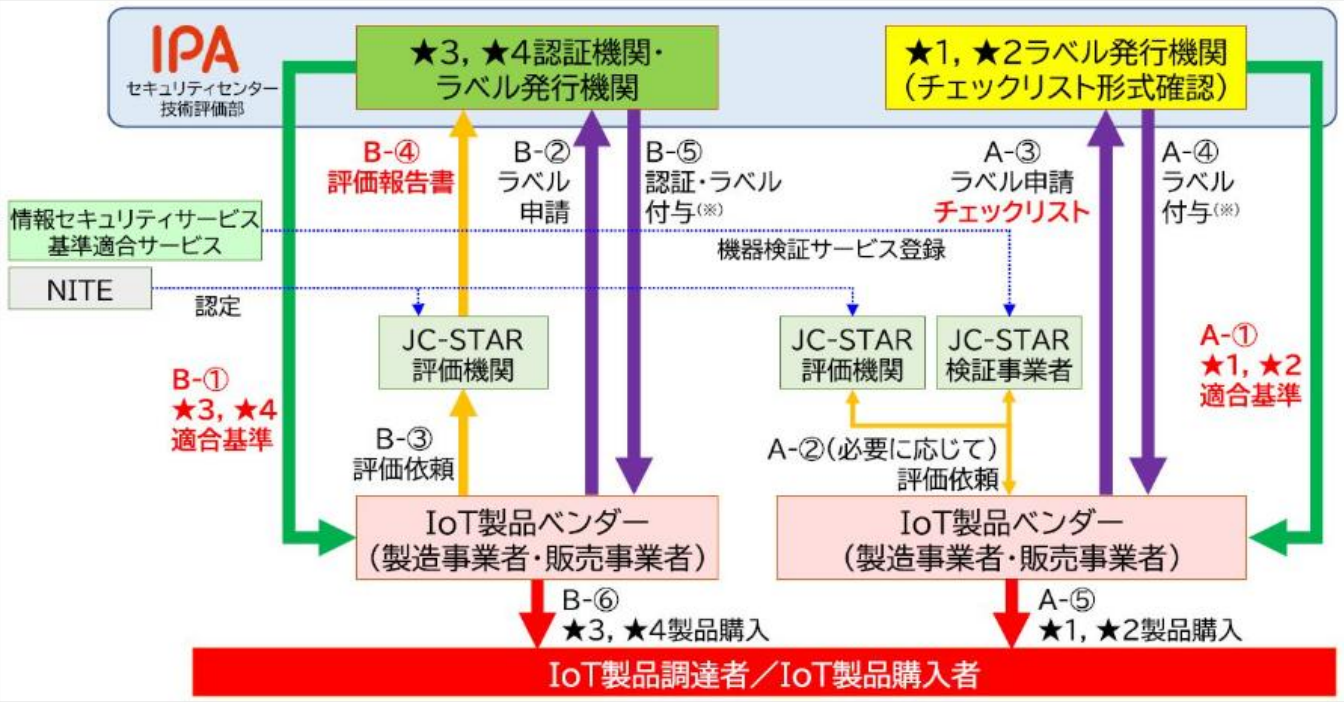
適合基準　評価手順

求められるセキュリティ水準に応じたセキュリティ技術要件として、
最低限の脅威に対応するための製品共通の適合基準・評価手順（★１）と、
製品類型ごとの特徴に応じた適合基準・評価手順（★２～★４）が設定されている。



1.ガイドライン・規約等に沿った評価
1-3.国内IoTサイバーセキュリティの動向

JC-STAR制度のスキーム



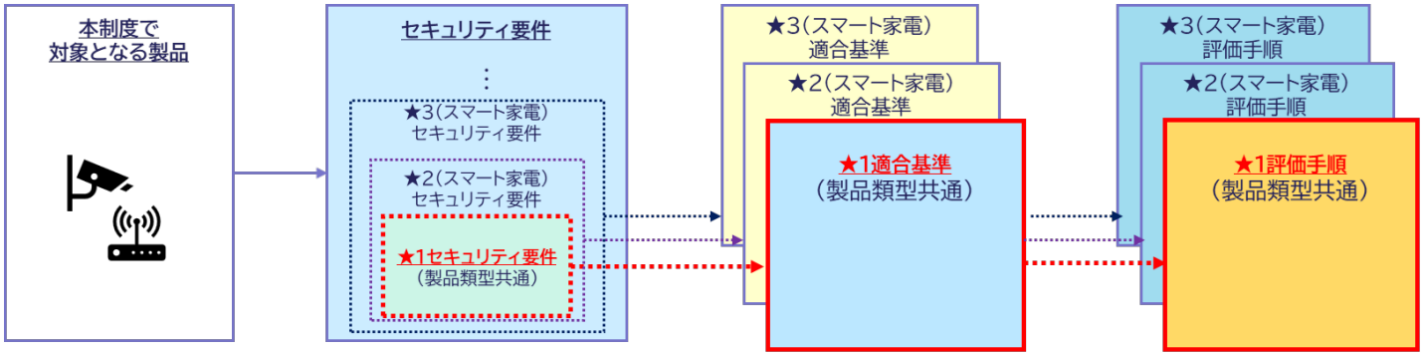
（※4）IPA は、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

JC-STAR検証事業者
経済産業省が定めた「情報セキュリティサービス基準」に基づく審査登録制度により、「機器検証サービス」に登録された事業者

JC-STAR評価機関
製品評価技術基盤機構（NITE）の製品評価技術基盤機構認定制度（ASNITE）に、ISO/IEC17025に基づくJC-STAR評価機関認定制度を設け、★3（レベル3）以上の評価を行える事業者を認定する予定。

1.ガイドライン・規約等に沿った評価
1-3. JC-STAR★１(レベル１)について

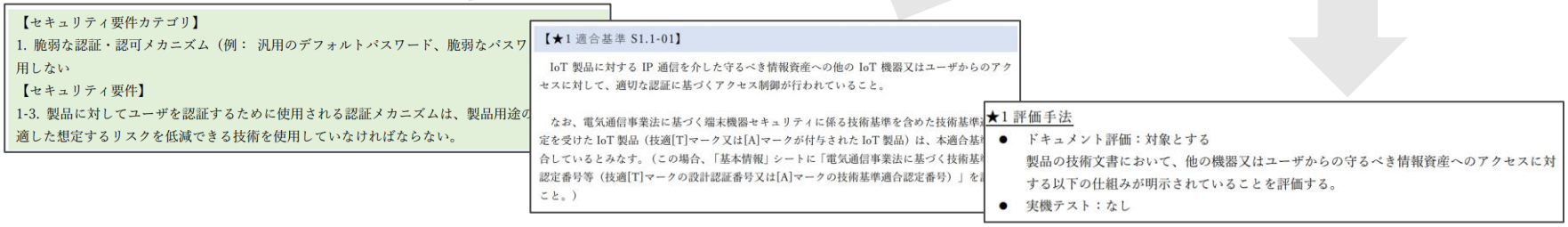
★1 適合基準類は、「セキュリティ要件」「適合基準」「評価手順」より構成される。



★1 に想定される脅威や保護すべき情報資産等を考慮し、その脅威に対抗するために IoT 製品の★1 のセキュリティ機能として具備すべきセキュリティ要件

★1 セキュリティ要件に準拠するために IoT 製品が適合すべき基準

★1 適合基準に適合しているかを評価・判断するための評価手法及び評価ガイドによって構成される手順書



★１の評価方法

評価項目：16項目
評価手法：「ドキュメント評価：12項目」「実機テスト：6項目」のいずれか、もしくは両方で実施
評価結果：「適合（Y）」「非適合（N）」「対象外（NA）」のいずれかで判断

★1（レベル1）適合基準・評価ガイド
https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html

1.ガイドライン・規約等に沿った評価
1-3. JC-STAR★１　セキュリティ要件適合評価サービス

JC-STAR★１評価メニュー

項目	内容
JC-STAR★1 要件理解	レベル1の適合基準および評価ガイドラインに基づき、求められるサイバーセキュリティ要件について、2～3時間で分かりやすく解説します。
フル試験	レベル１の適合基準と評価ガイドラインに基づき、対象機器のドキュメント評価・実機テストを実施し、チェックリスト及び証跡(エビデンス)を作成いたします。
実機テスト試験	レベル１の適合基準と評価ガイドラインに基づき、対象機器の実機テストのみ実施いたします。 実機テストの項目のみ、チェックリスト及び証跡(エビデンス)を作成いたします。
オプション	報告会

1.ガイドライン・規約等に沿った評価
1-4.医療機器向けセキュリティ試験サービス

医療機器のセキュリティ

➢ IEC ／ JIS　81001-5-1

EC 81001-5-1／JIS T 81001-5-1は、
ヘルスソフトウェアのサイバーセキュリティを確保するため、開発・保守を含む製品ライフサイクルにおいて実施すべきセキュリティに関する要求事項およびアクティビティを定めた規格です。

本規格では、ソフトウェア開発プロセスの一つとしてソフトウェアシステム試験が規定されており、セキュリティ要求事項試験、脅威軽減試験、脆弱性試験および侵入試験が位置づけられています。

当社では、攻撃者の視点に立った第三者による専門的なセキュリティ評価を実施し、システム等に潜在する脆弱性やセキュリティ上の弱点を確認します。

脆弱性試験および侵入試験を通じて、
規格対応に必要な評価結果・エビデンスを整理するとともに、
潜在的なセキュリティリスクを明確化し、必要な対策の検討を支援します。

1.ガイドライン・規約等に沿った評価
1-4.医療機器向けセキュリティ試験サービス

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

医療機器のセキュリティ

➢ IEC ／ JIS T 81001-5-1

IEC 81001-5-1／JIS T 81001-5-1は、
医療機器およびヘルスソフトウェアのサイバーセキュリティを確保するため、開発・保守を含む製品ライフサイクルにおいて実施すべきセキュリティに関する要求事項およびアクティビティを定めた規格です。

本規格では、ソフトウェア開発プロセスの一つとしてソフトウェアシステム試験が規定されており、セキュリティ要求事項試験、脅威軽減試験、脆弱性試験および侵入試験が位置づけられています。

当社では、IEC 81001-5-1／JIS T 81001-5-1で規定されるソフトウェアシステム試験のうち、専門的なセキュリティ知識・技術が求められる「**脆弱性試験**」および「**侵入試験**」を提供しています。

これらの試験を通じて、潜在的なセキュリティリスクを明確化するとともに、規格対応に必要な評価結果・エビデンスを提供し、必要な対策の検討を支援します。

1.ガイドライン・規約等に沿った評価

1-4.医療機器向けセキュリティ試験サービス

5.7.3 脆弱性試験

項目	内容	主な試験
a) 想定外入力を用いた悪用ケース試験	すべての外部インタフェース／プロトコルに対し、想定外入力を用いた悪用ケース試験を実施（手動／自動）。必要に応じて、ファジングやネットワーク負荷試験（段階実施・停止条件定義）等を含める。	・境界値・不正値試験 ・負荷試験 等
b) 攻撃対象領域試験	進入路・退出路を特定し、全ての外部I/Fとデータ入出力経路（ログ／エクスポート、外部送信等）について、弱いアクセスコントロールでないこと、不要な開放ポートがないこと、サービスが意図した権限で実行されていることを確認する試験。	・アタックサーフェス調査 ・ポートスキャン ・アクセス制御確認 等
c) 既知の脆弱性	ツールを用いて、ハード及びインターフェイス等から既知の脆弱性（CVE等）のスキャンを実施する。	・ネットワーク脆弱性スキャン 等
d) ソフトウェアコンポジション解析	全てのバイナリ実行ファイル（サードパーティ提供の組込みファーム含む）に対し、SCA（ソフトウェアコンポジション解析）で既知の脆弱性・脆弱ライブラリ・ルール違反・危険なビルド設定・SBOMとの差分を検出する。	・ファームウェア及び、バイナリ実行ファイル解析（SCA） ・SBOM照合 等
e) 動的セキュリティ試験	ファジング等の動的試験（ツール使用）で静的解析では見えない実行時欠陥（ランタイムハンドルの解放失敗，メモリーリーク及び認証なしでの共有メモリー へのアクセスによるサービス妨害状況等）を検出する。	・ファジング試験 等
a) 想定外入力を用いた悪用ケース試験	すべての外部インタフェース／プロトコルに対し、想定外入力を用いた悪用ケース試験を実施（手動／自動）。必要に応じて、ファジングやネットワーク負荷試験（段階実施・停止条件定義）等を含める。	・境界値・不正値試験 ・負荷試験 等

1.ガイドライン・規約等に沿った評価

1-4.医療機器向けセキュリティ試験サービス

5.7.4 侵入試験（ペネトレーション試験）

項目	内容	
侵入試験	攻撃者視点で脆弱性を発見・悪用し、機密性／完全性／可用性の侵害に至る弱みを特定する侵入試験（手動＋ツール、複数脆弱性の連鎖も含む）を実施する。	1. 範囲定義（目的・対象・成功条件） 2. 攻撃シナリオ設計 （スキャン結果等も参考） 3. 疑似攻撃の実施 （手動＋ツール：侵入試行／ 認証回避／権限昇格・横展開／ 連鎖攻撃） 4. 結果・対策報告

2.OWASP IoT TOP10に基づく試験

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

「OWASP IoT Top 10」とは

OWASPが2014年に発足したOWASP Internet of Thingsプロジェクトの成果物の一つとして公表したもので、IoTにおいて脆弱性を生じやすい10のポイントが整理され、注意点が示されています。現在は2018年公開の「OWASP IoT Top 10 2018」を参照。

OWASP IoT Top10 – 2018　試験項目

No.	カテゴリ	試験項目
1	強度の弱いパスワード、推測可能なパスワード、またはパスワードのハードコード	パスワードの強度の確認、等
2	安全でないネットワークサービス	ポートスキャン、実行中のサービスの検出、等
3	安全でないエコシステムインターフェース	ファームウェアの搾取、等
4	安全でない更新メカニズム	改ざんされたファームウェアによる更新、等
5	安全でない、または古いコンポーネントの使用	ライブラリ、フレームワークの既知の脆弱性調査、等
6	不十分なプライバシー保護	平文による内部ストレージへの重要情報保存、等
7	安全でないデータの転送と保存	通信パケットキャプチャ、暗号化強度の確認、等
8	デバイス管理の欠如	—
9	安全でないデフォルト設定	安全でないデフォルト設定の確認
10	物理的なハードニングの欠如	物理インターフェースの各試験項目

OWASP IoT TOP10に基づいた項目を試験を実施します。
ご要望に応じて最適な試験項目を調整し、ご提供することも可能です。

3.ご希望に沿ったテストの実施

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

IoT機器に対して適切と思われる試験項目を選定し、セキュリティのテスト手法を駆使し手動でのテストや自動テストツールを組合せて網羅的な試験を実施します。

IoTセキュリティ試験/評価のテスト手法例（一部を掲載）

脆弱性テスト	既知の脆弱性がないかテストし検証します。
ファジングテスト	予測していないデータを与え、例外の動作を検証します。
ペネトレーションテスト	開発者が想定しない脆弱性が存在しないか、 また実際に既知の技術を駆使し侵入が行えないかを検証します。

IoTセキュリテ試験/評価サービス提供の流れ

ヒアリング

現状の状況や環境を把握するのに必要な情報を、ヒアリングシートのご入力、またはお打ち合わせ等で確認し、適切な対応方法や試験範囲を検討し御見積りいたします。

試験/評価 実施

ヒアリングした内容をもとに、試験対象に対して脆弱性の調査を実施いたします。試験/評価の実施にあたり、進捗を報告しながら対応させていただきます。

レポート提出

検出した脆弱性の分析結果の報告と影響範囲は対策方法についてご説明させていただき、優先度順位付けや解決策の提案をします。

IoTセキュリティ試験/評価　実施機器事例

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

主な試験/評価実績 (2026年5月時点)

EN18031 試験/評価実施機器事例	RFID機能搭載プリンター
	計測機器
	音源モジュール機器　　等
CRA認証取得に向けた実機試験機器事例	ネットワーク機能搭載プリンター
	精密加工機
	コントローラー等
JC-STAR	蓄電池システム
	発電システムコントローラー
	ゲートウェイ　　等
医療機器・その他	医療系検査機器
	医療系測定装置
	ロボット掃除機　　等

サービスの強み

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

①JAB「適合性評価機関（ISO/IEC 17025）」認定取得

当社は、JAB（公益財団法人日本適合性認定協会）より、ISO/IEC 17025に基づく試験所として、適合性評価機関の認定を取得しています。

ISO/IEC 17025は、試験所が正確で信頼性のある試験結果を提供するための技術的能力と、公平な運営体制を備えていることを示す国際規格です。当社は認定範囲であるEN 18031-1に基づくサイバーセキュリティ試験において、第三者性・信頼性の高い試験サービスを提供します。

JAB
Testing LAB
RTL05410

②経産省「情報セキュリティサービス基準」登録事業

経産省では、「情報セキュリティサービス基準」に適合するサービスとして「機器検証サービス」に登録されています。

経済産業省は「情報セキュリティサービス基準」を策定しております。この「情報セキュリティサービス基準」は、一定の技術要件及び品質管理要件を満たし、品質の維持・向上に努めているサービスであることを示すものです。

019-0022-40

③セキュリティ診断で培った知見の活用

当社はこれまで、情報セキュリティ診断のサービスを提供しており、またIoT機器に対しても、セキュリティガイドラインの知見やセキュリティ評価・試験の実績を積み上げてまいりました。これらの知見や実績をもとに、IoTセキュリティガイドラインの準拠をご検討のお客様をサポートさせていただきます。

④認証機関との包括的なリレーション

当社は認証機関とパートナー提携を結んでおります。
当社の技術試験・テストによるご提供はもちろん、ご検討の規約やガイドラインによっては、認証部分を含めてご相談いただけます。

お問い合わせ

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

資料請求やお見積依頼など、お気軽にお問い合わせください。
担当からすぐにご連絡いたします。

お問い合わせフォーム

https://www.secure-iv.co.jp/contact

pr@secure-iv.com

098-943-2718

受付時間 9:00～18:00（土日祝祭日を除く）