経済産業省　御中

令和３年度補正中小企業サイバーセキュリティ対策促進事業

# IoT 機器脆弱性検証事業

## 報告書

三菱総合研究所
デジタル・イノベーション本部

2023 年 3 月 31 日

# 目次

# 図 目次

# 表 目次

# 1. 調査概要

## 1.1 調査背景・目的

家庭内ではインターネットにつながる IoT 家電が登場し、スマートホームのような家電間の連携が進んでいる。こうした中、コロナ禍で 4 割の方が家事の機会が増え、家事が便利になる消費者向けの IoT 機器の販売数は急速に増加している。また、職場環境においても、照明や入退室管理等の効率的な管理のため、IoT 機器の活用が進んでいる。さらに、産業分野でもリモートワークが進み、これまで出社することが必要であった生産ラインのモニタリングにおいても、センサ等の IoT 機器を活用したオンラインモニタリングの仕組みが普及し始めている等、IoT 機器は全体で 20～30 億台／年で増加している。

一方、一般消費者のうち IoT 機器に関する脅威を理解している者は 1 割にも満たず、日本の中小企業が販売する IoT 機器についてはセキュリティ対策が十分であるか不明な部分がある。また、脆弱性の検証サービスの利用は中小企業にとって決して費用が安いものではない、開発に要する日数が増加する等の理由で、現時点で必ずしも必要性が浸透しているとは言えない。

このような状況下で、市場投入後、機器に脆弱性が見つかれば、最低限の対応として緊急のセキュリティアップデートの対応が求められるだけでなく、場合によっては回収等の対応を求められる可能性もあり、中小企業の経営に大きな影響を及ぼす可能性があることから、中小企業の負担軽減も考慮しつつ中小企業が開発・販売する IoT 機器の効果的な検証を行うための手法の整理や中小企業が IoT 機器を開発する段階からセキュリティ面で注意すべき事項等の整理を早急に行う必要がある。

本事業では、開発段階からセキュリティを意識するセキュリティ・バイ・デザインを採り入れた効果的な検証手法を整理し、コスト低減を図った中小企業等の IoT 機器の脆弱性検証を促進するために、中小企業等の IoT 機器の脆弱性等の検証の現状に関する調査し、調査結果を踏まえて IoT 機器を開発・販売する中小企業や検証サービス事業者が活用することを想定したガイド等を作成した。また、IoT 製品の安全性を確保するために、あるセキュリティ要求基準に対するセキュリティ対策の適合性を評価し、その結果を利用者や調達者が分かる形で可視化する制度（以下「適合性評価制度」と言う。）について、検討を行った。

## 1.2 調査実施概要

調査目的を達成するために、以下の項目に関して調査・検討・支援等を行った。

（1） 中小企業等の IoT 機器の脆弱性等の検証の現状に関する調査
（2） IoT 機器を開発・販売する中小企業や検証サービス事業者が活用するガイドライン等の作成
（3） ガイドライン等の作成に関する検討会の実施
（4） IoT 製品に対するセキュリティ適合性評価制度の構築に係る検討

# 2. 中小企業等の IoT 機器の脆弱性等の検証の現状に関する調査

中小企業等が開発・販売する脆弱性攻撃の対象となり得る IoT 機器を募集するとともに、当該機器に対するセキュリティ検証サービスを提供する検証事業者を 10 社程度選定した上で、機器に対する脆弱性検証に関する実証を行った。検証を通じ、IoT 機器の設計、製造工程等におけるセキュリティ対策の現状を把握するとともに、検証サービス事業者による脆弱性検証の実効性について調査を行った。

## 2.1 中小企業等の募集・選定

### 2.1.1 関連企業・関連団体への依頼

実証に協力いただける中小企業等を募集するために、以下の業界団体や関連団体に対して実証に関する説明及び会員企業に対する周知を依頼した。

【業界団体】

- 一般社団法人日本医療機器産業連合会
- 一般社団法人電子情報技術産業協会（JEITA）
- 一般社団法人日本工作機械工業会
- ロボット革命イニシアティブ（RRI）
- Industrial Value Chain Initiative（IVI）
- 一般社団法人日本電機工業会（JEMA）
- 一般社団法人日本電気計測器工業会（JEMIMA）
- 一般社団法人日本電気制御機器工業会（NECA）

【セキュリティ関連団体】

- 特定非営利活動法人日本ネットワークセキュリティ協会（西日本支部）
- セキュア IoT プラットフォーム協議会

【IoT 関連団体】

- 一般社団法人組込みシステム技術協会（JASA）
- IoT 推進コンソーシアム

【中小企業関連団体】

- 日本商工会議所
- 全国中小企業団体中央会
- 中小企業基盤整備機構

### 2.1.2 各種媒体を通じた募集案内

実証を広く周知するために、以下の媒体において実証に関する案内を掲載した。

- ScanNetSecurity
- JapanSecuritySummit Update


出所）ScanNetSecurity, https://scan.netsecurity.ne.jp/article/2022/08/25/48092.html

図 2.1-1 ScanNetSecurity 掲載記事

JAPANSecuritySummit Update

EVENT JSS2022 | Special Edition | Solutions | セミナー/展示会 | 記事一覧 | メールマガジン

ホーム > ブログ > 経済産業省「開発段階におけるIoT機器の脆弱性検証促進事業」のご案内

# 経済産業省「開発段階におけるIoT機器の脆弱性検証促進事業」のご案内

2022.09.20

Tweet | Share | B! Hatena

サイバーセキュリティの課題をテーマ別に紹介中！！

サイバーセキュリティの事故は、毎月のようにニュースに取り上げられ、その数は増加傾向である。
昨今ではDXの進展により増大するIoT機器がターゲットになっているケースも多く見られることから、IoT機器のセキュリティ確保は重要な課題となっている。
出荷されたIoT機器に脆弱性が含まれることにより、セキュリティ事故の発生可能性が高まるだけでなく、その修正対応に工数やコストが発生する恐れがある。さらにはセキュリティ事故が、市場の信頼低下や企業経営に対する悪影響に繋がる恐れがある。
そのため事前に機器のおける機関の脆弱性検査を受け、安全であることを確認した上で出荷することがなによりも重要である。

ところがこういったリスクを認識はするものの、対応方法が分からない、コスト面が心配などの理由で悩んでいる企業は多いのではないだろうか。そこで、経済産業省では、IoT関連企業が開発・製造するIoT機器等に対して、専門家による脆弱性検証を無償で実施する事業を開始した。

この事業におけるIoT機器とは産業・一般消費者等対象を問わず、ネットワークに接続して利用される機器を幅広く対象としており、最終製品に限らず製品を構成する部品等も対象としている。

この事業におけるIoT機器とは産業・一般消費者等対象を問わず、ネットワークに接続して利用される機器を幅広く対象としており、最終製品に限らず製品を構成する部品等も対象としている。

**対象となる「IoT機器等」の例**



本事業では、産業用・一般消費者用問わず、ネットワークに常時接続される機器
及び機器に使用される部品等を対象とします。
IoT機器等のデータを収集・分析したり、制御を行うアプリケーション・ソフトウェアも対象とします。

また、機器だけではなく、IoT機器等のデータを収集・分析し、制御を行うアプリケーションやソフトウェア、機器の設計書やプログラムのソースコード等も検証の対象となる。

当事業の詳細は以下のページより確認を頂きたい。
**「開発段階におけるIoT機器の脆弱性検証促進事業」（経済産業省事業）においてIoT機器の脆弱性検証を希望する中小企業の募集のご案内について**

製品や検証内容次第では、企業規模を問わず参加可能であるので、関心のある企業は、下記より気軽に相談していただきたい。
安心安全なIoT社会の実現のために、ぜひこの機会を積極的に活用してもらいたい。

＜本事業に関するお問合せ先＞

株式会社三菱総合研究所
サイバーセキュリティ戦略グループ
「開発段階におけるIoT機器の脆弱性検証促進事業」事務局
Email：iot-sec@ml.mri.co.jp

出所）JapanSecuritySummit Update, https://japansecuritysummit.org/2022/09/4539/

図 2.1-2 JapanSecuritySummit Update 掲載記事

また、日経 XTech への広告を掲載した。


出所）日経 XTech

図 2.1-3 日経 XTech 広告

### 2.1.3 募集・選定結果

実証に協力いただける中小企業等を 2022 年 4 月 25 日～2022 年 10 月 17 日の期間で募集した。募集は三菱総合研究所の HP にて行い、参考資料として募集用パンフレットも添付した（図 2.1-4）。

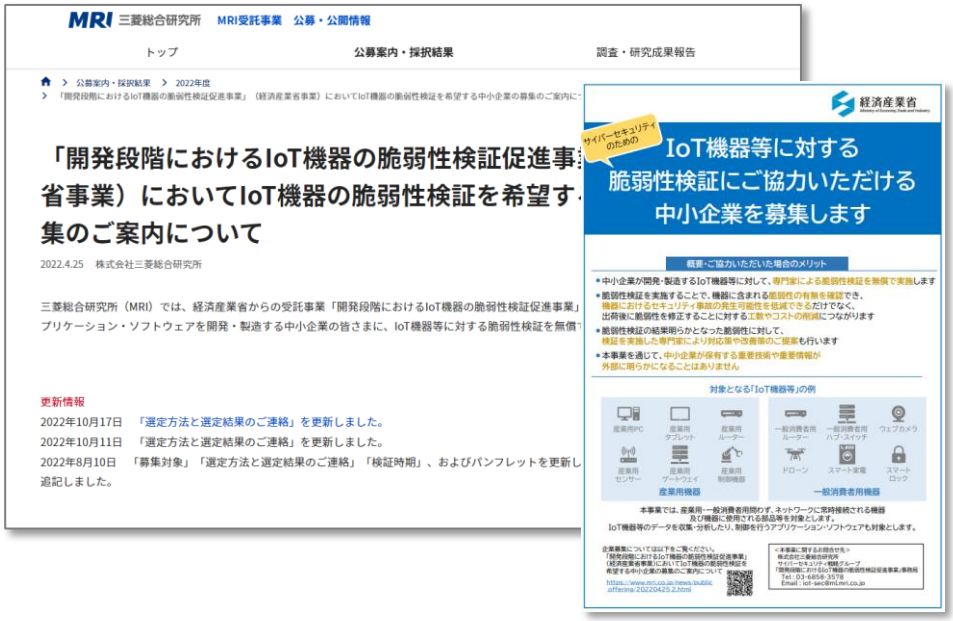



図 2.1-4 募集 HP 及び募集用パンフレット

上記募集期間内で、目標の 150 製品に対して 83 社・180 製品の応募が寄せられた。応募が寄せられた製品のうち、74 社・155 製品を選定し、脆弱性検証の対象とした。

## 2.2 検証事業者の選定

募集・選定した 155 製品に対し、セキュリティ検証サービスを提供する検証事業者による脆弱性検証

を行った。本事業では、以下の検証事業者 11 社を選定した。

- 株式会社 AGEST
- 株式会社 FFRI セキュリティ
- GMO サイバーセキュリティ by イエラエ株式会社
- 株式会社ラック
- 株式会社ベリサーブ
- 株式会社ユビキタス AI
- 株式会社ベルウクリエイティブ
- サイバートラスト株式会社
- 株式会社 SYNCHRO
- 大日本印刷株式会社
- 株式会社神戸デジタル・ラボ

各検証事業者の実績や得意領域等を踏まえて、選定した 155 製品の割当を行った。中小企業等の IoT 機器に対する検証の実施概要

### 2.2.1 検証の全体プロセス

本実証事業における検証の全体プロセスを図 2.2-1 に示す。検証のフェーズは、(1)検証準備フェーズ、(2)検証実施フェーズ、(3)検証結果報告フェーズの 3 つに分類される。

(1)検証準備フェーズでは、応募のあった製品について検証事業者への割当を行い、正式な割当が決定した後、検証事業者から中小企業等に対して秘密保持誓約書を発出した。この秘密保持誓約書では、検証対象とする製品や検出された脆弱性等に関する秘密情報を検証事業者が保持することに関する誓約を明記した。なお、中小企業等が別途用意した秘密保持契約書等に基づく秘密保持の管理を要望した場合には、当該契約書等に基づく対応を行った。秘密保持誓約書の発出以降、検証事業者と中小企業等の間で連絡を行い、検証準備を進めた。検証準備フェーズで、一度打合せを行い、検証実施に向けた意識合わせのほか、機器調達方法の相談を行った。打合せの結果を踏まえ、検証方針を策定した。また、進捗管理のために、各機器の検証に関する WBS の策定を依頼した。

(2)検証実施フェーズでは、策定した検証方針に基づき検証を行った。また、進捗管理に関して、隔週程度で、策定した WBS の提出を求め、進捗等について課題が生じた際には、課題管理表での管理を求めた。なお、各検証事業者で得意とする領域や検証手法、検証の進め方等が異なるところ、本実証では、経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」[1]をベースに検証を進めることのみ取り決め、適用する検証手法や検証の進め方は一律化せずに各検証事業者に一任する形式で進めた。ただし、後述するとおり、検証結果報告書に記載する項目のみ指定した。

(3)検証結果報告書フェーズでは、検証を通じて策定した検証結果報告書に基づく報告会の実施を求めた。最終的には、報告会において挙げられた意見を踏まえて修正した検証結果報告書について、当社への提出を求めた。

[1] https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

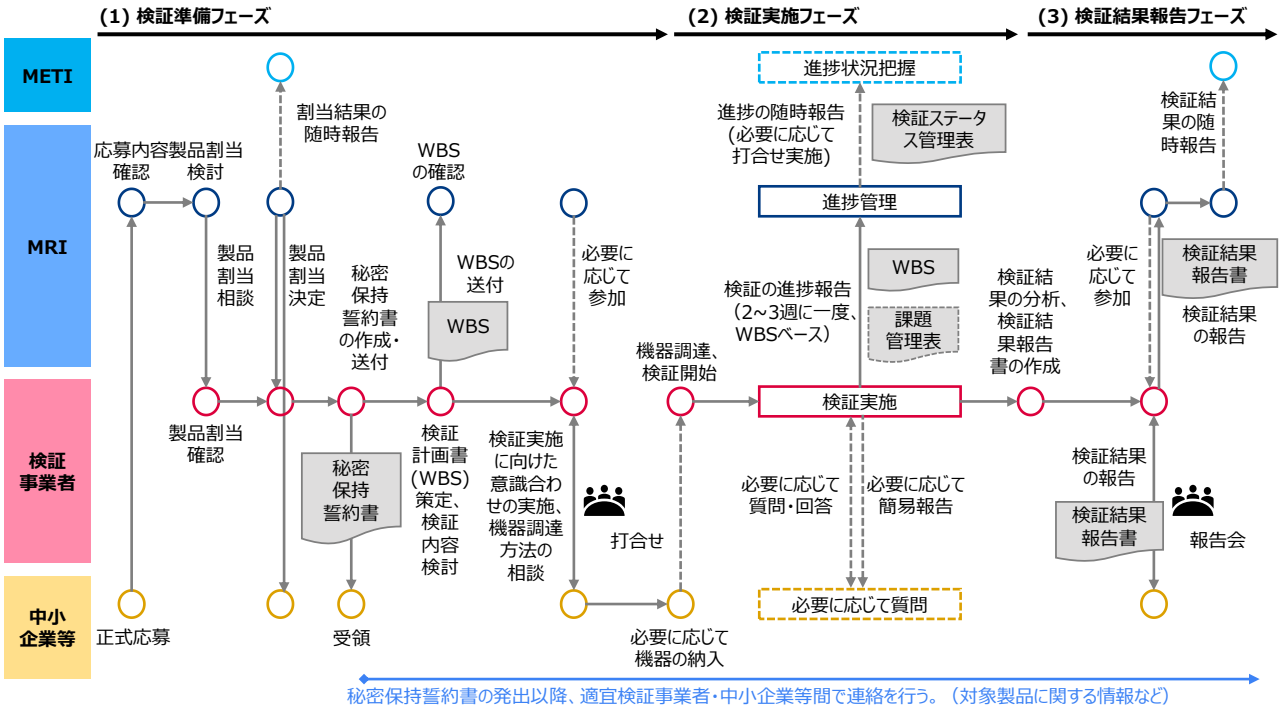



図 2.2-1 実証の検証全体プロセス

## 2.2.2 検証結果報告書の記載項目

本実証事業で作成する検証結果報告書について、経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の記載に則り、以下の項目を含めることを検証事業者に求めた。

表 2.2-1 実証事業で作成した検証結果報告書の記載項目

| 大項目 | 項目 | 記載内容 |
|---|---|---|
| エグゼクティブ・サマリー | エグゼクティブ・サマリー | 検証のエグゼクティブ・サマリーを 1 ページ程度で記載する。これには、検証結果から得られる示唆を含めることが望ましい。 |
| 検証概要 | 検証目的 | 検証の目的について記載する。 |
| | 検証期間 | 検証を実施した期間について記載する。 |
| | 検証対象 | 検証対象機器及び検証範囲について可能な限り記載する。これには、製品名、メーカー、製造年月、シリアルナンバー・機器番号等、及びファームウェアバージョンが含まれる。 |
| | 検証環境 | 検証の環境(ネットワーク構成等)について記載する。 |
| | 検証の手法 | 検証した手法(既知脆弱性の診断等)の項目を記載する。 |
| | 脆弱性の評価基準 | 検出された脆弱性やリスクの深刻度を判断する際の基準(CVSS v3.1 等)を記載する。 |

| 大項目 | 項目 | 記載内容 |
|---|---|---|
| | 使用ツール | 検証に使用したツールの名称及びバージョンを記載する。 |
| 検証結果 | 総合評価 | 検証結果の概要を記載する。これは、検出された代表的な脆弱性の概要と、その脆弱性を悪用することで想定される影響を記載することが望ましい。 |
| | 検証の観点 | 検証を行うに当たって想定した脅威や検証の優先順位を記載する。これは、検証を実施した結果、脆弱性が見つからなかった手順についても記載することが望ましく、どのような観点から検証項目を選定したかという基準があることが望まれる。また、あえて検証を行わなかった項目等があれば、それを除外した理由も含めて記載する。 |
| | 検出脆弱性一覧 | 検出された脆弱性の一覧を記載する。 |
| | 検証結果の詳細 | 検出された脆弱性について、検証の詳細結果を記載する。これには、それぞれの検出事項の評価と概要、その脆弱性や脅威により想定される影響、及び対策事項を含める必要がある。 |
| 推奨事項 | 推奨事項 | 検証結果を踏まえて、検証依頼者に求められる対応事項を記載する。 |
| 特記事項 | 特記事項 | 免責事項や事後対応可能期間等、特記事項があれば記載する。 |

出典）経済産業省、機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き

## 2.3 中小企業等の IoT 機器に対する検証の現状に関する調査結果

### 2.3.1 脆弱性の検出結果

155 製品に対する検証によって複数の脆弱性が検出された。実証を通じて検出された脆弱性のうち、深刻度の高い代表的な脆弱性は表 2.3-1 に示すとおりであり、多くの脆弱性がソフトウェアのバージョンが古いこと等に起因する既知の脆弱性であった。表 2.2-1 に記載のとおり、検出された脆弱性については、検証結果報告書において推奨事項を記載し、当該製品のベンダーに対して対応を推奨した。

表 2.3-1 実証において検出された代表的な脆弱性の概要

| 機器区分 | 検出された代表的な脆弱性の概要 |
|---|---|
| UTM | 古いバージョンの OpenSSH における権限昇格の脆弱性（CVE-2021-41617） |
| UTM | Web 管理画面における OS コマンドインジェクションの脆弱性 |
| UTM | 非暗号化通信によるファームウェアの更新 |
| ゲートウェイ・ルータ | 古いバージョンの Squid における不正アクセスやリモートコード実行の脆弱性（CVE-2019-12519、CVE-2019-12523、CVE-2019-12524、CVE- |

| 機器区分 | 検出された代表的な脆弱性の概要 |
| --- | --- |
| | 2019-12525、CVE-2019-12526、CVE-2020-11945、） |
| ゲートウェイ・ルータ | 古いバージョンの dnsmasq におけるバッファオーバーフローの脆弱性（CVE-2017-14491、CVE-2017-14492、CVE-2017-14493） |
| ゲートウェイ・ルータ | 古いバージョンの lighttpd における SQL インジェクションの脆弱性（CVE-2014-2323） |
| ゲートウェイ・ルータ | バッファオーバーフローの脆弱性 |
| ゲートウェイ・ルータ | 古いバージョンの OS における不正アクセスやリモートコード実行の脆弱性 |
| ゲートウェイ・ルータ | 古いバージョンの Samba におけるリモートコード実行の脆弱性（CVE-2017-7494） |
| ゲートウェイ・ルータ | アップデートサーバ及びアップデートファイルの署名検証不備 |
| ネットワークスイッチ | 古いバージョンの Dropbear における情報の漏洩や改ざんの脆弱性（CVE-2017-9078、CVE-2019-12953、CVE-2020-36254） |
| ネットワークスイッチ | Web 管理画面に対する非暗号化状態での通信 |
| ネットワークスイッチ | Web 管理画面におけるクロスサイトスクリプティングの脆弱性 |
| ネットワークスイッチ | Web 管理画面における画像アップロード機能において任意のファイルをアップロード可能 |
| モバイル端末 | 初期インストールされた Web アプリケーションにおけるディレクトリトラバーサルの脆弱性 |
| モバイル端末 | タッチパネル操作によって機密情報の閲覧が可能 |
| モバイル端末 | 誰もが匿名で利用可能なサーバが稼働 |
| モバイル端末 | 初期インストールされた Web アプリケーションにおいて権限を改ざんした操作が可能 |
| スマートロック | Web アプリケーションにおいて他ユーザの情報変更が可能 |
| スマートロック | Web アプリケーションにおけるクロスサイトスクリプティングの脆弱性 |
| スマートロック | 古いバージョンの systemd におけるリモートコード実行の脆弱性（CVE-2022-2526） |
| スマートロック | Web アプリケーションにおけるユーザのパスワード攻撃の脆弱性 |
| スマートロック | MQTT（Message Queuing Telemetry Transport）通信における認証制御の不備 |
| スマート家電 | Web アプリケーションにおいて他ユーザの情報変更が可能 |
| スマート家電 | adb（android debug bridge）を利用したスマート家電への接続・任意操作可能 |
| スマート家電 | Web アプリケーションにおける OS コマンドインジェクションの脆弱性 |
| スマート家電 | Web アプリケーションにおけるファイルアップロード機能において任意のファイルをアップロード可能 |
| スマート家電 | Web アプリケーションにおけるバッファオーバーフローの脆弱性 |
| ドローン | ドローン本体のネットワーク設定機能における OS コマンドインジェクションの脆弱 |

| 機器区分 | 検出された代表的な脆弱性の概要 |
| --- | --- |
| | 性 |
| ドローン | Web アプリケーションにおけるファイルアップロード機能において任意のコードを実行可能 |
| ドローン | Web アプリケーションにおける OS コマンドインジェクションの脆弱性 |
| ドローン | 公開フォルダ上に機密情報が設置 |
| ネットワークカメラ | Web アプリケーションにおける OS コマンドインジェクションの脆弱性 |
| ネットワークカメラ | Web アプリケーションおける認証制御の不備 |
| ネットワークカメラ | Web アプリケーションにおけるクロスサイトリクエストフォージェリの脆弱性 |
| ネットワークカメラ | 不正な SD カードを挿入することによる任意コード実行の脆弱性 |
| ネットワークカメラ | Web アプリケーションへのログインパスワードを不正取得可能 |
| ネットワークカメラ | アップデート用ファームウェアファイルから重要情報取得可能 |
| センサ・監視装置 | 古いバージョンの dnsmasq におけるバッファオーバーフローの脆弱性（CVE-2017-14491、CVE-2017-14492、CVE-2017-14493） |
| センサ・監視装置 | Web アプリケーションにおける OS コマンドインジェクションの脆弱性 |
| センサ・監視装置 | DLL ファイルにおける既知のディレクトリトラバーサルの脆弱性 |
| センサ・監視装置 | 管理者権限ユーザの作成における認証回避の脆弱性 |
| センサ・監視装置 | Web アプリケーションにおける任意コード実行の脆弱性 |
| センサ・監視装置 | OS におけるアカウント認証情報を推測可能 |
| センサ・監視装置 | 古いバージョンの Grails が使用している外部ライブラリにおける XML 外部エンティティ参照（XXE）の脆弱性 |
| センサ・監視装置 | Web アプリケーションにおけるファイルアップロード機能において任意のファイルをアップロード可能 |
| センサ・監視装置 | 開放されたポートを経由した不正接続 |
| 産業用コントローラ | 古いバージョンの Apache HTTP Server における認証回避やオーバーフローの脆弱性（CVE-2021-26691、CVE-2021-39275、CVE-2021-44790、CVE-2022-22720 、CVE-2022-22721 、CVE-2022-28615 、CVE-2022-31813） |
| 産業用コントローラ | 古いバージョンの Apache httpd における認証回避やバッファエラーの脆弱性（CVE-2017-3167、CVE-2017-7679） |
| 産業用コントローラ | 古いバージョンの OpenSSL におけるオーバーフローや任意コード実行の脆弱性（CVE-2016-2108、CVE-2016-2177、CVE-2016-6303） |
| 産業用コントローラ | 古いバージョンの glibc におけるバッファオーバーフローの脆弱性（CVE-2015-0235） |
| 産業用コントローラ | 古いバージョンの PHP における任意コード実行、OS コマンドインジェクション、オーバーフロー等の脆弱性（CVE-2015-4116、CVE-2015-4599、CVE-2015-4600、CVE-2015-4601、CVE-2015-4602、CVE-2015-4603、CVE-2015-4604 、CVE-2015-4643 、CVE-2015-5589 、CVE-2015- |

| 機器区分 | 検出された代表的な脆弱性の概要 |
| --- | --- |
| | 6834、CVE-2015-6835、CVE-2015-8876、CVE-2016-3141、CVE-2016-4071、CVE-2016-4072、CVE-2016-4073、CVE-2016-4537、CVE-2016-4538、CVE-2016-4539、CVE-2016-4540、CVE-2016-4541、CVE-2016-4542、CVE-2016-4543、CVE-2016-4544、CVE-2016-5114、CVE-2016-5768、CVE-2016-5769、CVE-2016-5770、CVE-2016-5771、CVE-2016-5772、CVE-2016-5773、CVE-2016-6290、CVE-2016-6291、CVE-2016-6294、CVE-2016-6295、CVE-2016-6296、CVE-2016-7126、CVE-2016-7127、CVE-2016-7411、CVE-2016-7413、CVE-2016-7414、CVE-2016-7417、CVE-2016-7480、CVE-2016-7568、CVE-2016-8670 等） |
| CPU ボード | プロセッサチップにおける既知脆弱性（CVE-2021-0146） |
| 産業用ロボット | USB 接続による任意ファイル起動可能な脆弱性 |
| 産業用ロボット | 古いバージョンの dnsmasq におけるバッファオーバーフローの脆弱性（CVE-2017-14491、CVE-2017-14492、CVE-2017-14493） |
| サーバ装置 | OpenSSH における権限窃取の脆弱性（CVE-2016-1908） |
| サーバ装置 | dnsmasq におけるバッファオーバーフローの脆弱性（CVE-2017-14491、CVE-2017-14492、CVE-2017-14493） |
| 複合機 | 認証情報における脆弱なパスワードの設定 |

### 2.3.2 中小企業等に対するアンケート結果

今年度の実証事業に参画した中小企業等に対して、本事業の満足度や改善点、今後の検証サービスの活用意向やセキュリティ対策の現状・課題等に関するアンケートを実施した。その結果、72 社 145 製品について、回答を得ることができた。

本事業の満足度に関する製品ごとの回答結果を図 2.3-1 に示す。どの項目に関しても、「やや満足」「非常に満足」との回答が 85%以上を占めていた。「やや不満」「非常に不満」との主な回答理由について、表 2.3-2 に示す。検証に向けた準備に関しては、連絡・説明の不足や準備・検証時間の不足に関する理由等、検証の実施内容に関しては、検証内容の擦り合わせの不足やコミュニケーションの不足に関する理由、検証結果報告書の記載内容に関しては、記載不足に関する理由等、検証結果報告会の内容に関しては、報告不足に関する理由等、検証期間に関しては、計画の遅れや検証期間の長さに関する理由等が挙げられた。これらの意見は、3 章で後述する IoT 機器を開発・販売する中小企業や検証サービス事業者が活用するガイド等に反映した。

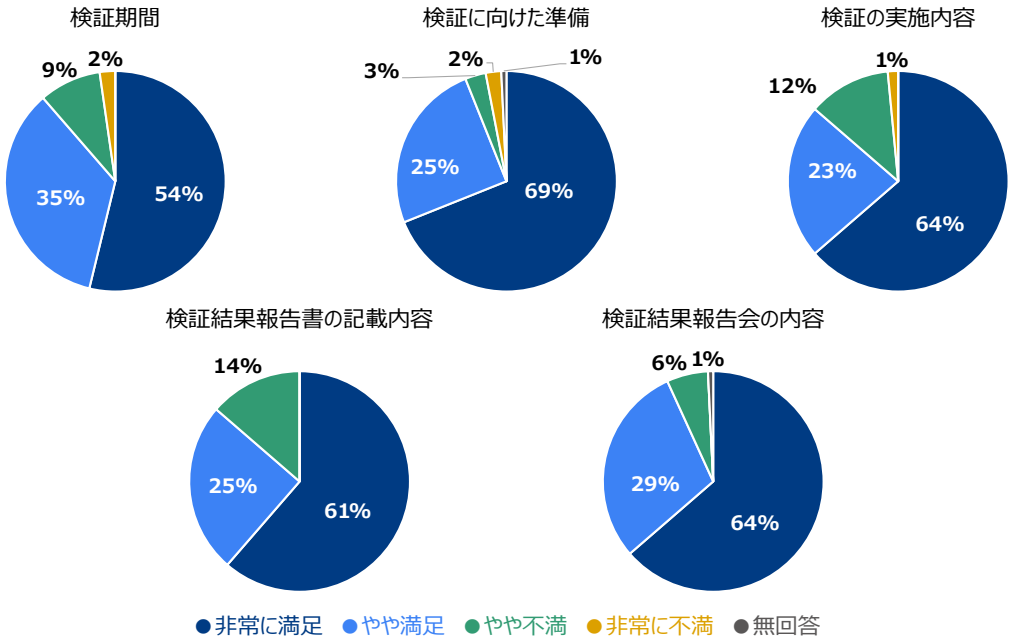



図 2.3-1 製品ごとの本事業の満足度(N=145)

表 2.3-2 本事業に対する「やや不満」「非常に不満」との主な回答理由

| アンケート項目 | カテゴリ | 主な回答理由 |
|---|---|---|
| 検証に向けた準備 | 連絡・説明の不足 | • 回答が極めて遅く、また回答内容が理解できなかった。<br>• スケジュールが不明であり、事前に検証の範囲がよく理解できなかった。<br>• 事前に議題の連絡がない状態で会議を開催された経験があまりなく、うまく対応できなかったため、せっかくの機会を十分に活用できなかった。 |
| | 準備・検証時間の不足 | • 対象がプロトコルスタックという点では検証は難しかったと思うが、その分検証内容に合わせた準備がもう少し必要だったと思う。<br>• NDA 締結に時間を要し、検証の開始が遅れ、検証に十分な時間がとれなかった。 |
| 検証の実施内容 | 検証内容の擦り合わせの不足 | • 実施内容が若干不明確だった。<br>• 事前の意識合わせが不十分だったため、実施内容の期待値とのギャップが大きかった。<br>• 表面的な解析に留まっており、検証内容は既知のものばかりであった。<br>• 全体的に検証内容が甘いと感じた。<br>• LAN ポートからの評価が主体で、グローバルネットワークの視点からの評価がなかった。<br>• 検証環境においてネットワークに対する制約があったため、 |

| アンケート項目 | カテゴリ | 主な回答理由 |
|---|---|---|
| | | 一部評価することができない項目があった。 |
| | コミュニケーションの不足 | • 検証の状況がどのようなステータスかが分からず、依頼者側からの状況確認が必要だった。<br>• 経過報告がなく、途中で方向修正を依頼することができなかった。<br>• 製品の使い方等についての問い合わせが来ず、組み立てて電源を入れただけの状態で検証をしていた。 |
| 検証結果報告書の記載内容 | 記載不足 | • 検証内容が概要しか書かれていなかったため、検証が意味のあるものだったのか判断しづらかった。<br>• テストの全体像に関する記載がなく、どこまでのテストを実施したのかが分からなかった。<br>• テストに使用したツールの記載はあったが、そのツールでどのようなテストを実施したのかが不明瞭だった。<br>• 結果や改善方法について記載いただいたのはよかったが、詳細な手順が分からなかった。<br>• 問題が無かったテストの結果も報告いただきたかった。<br>• 危険度のレベルと併記して、過去の被害実例や、自社での被害の可能性を記述していただけると、改修に向けての優先度を判断できるため、ありがたい。 |
| | その他 | • 専門用語が多く、理解できない記述が多い。<br>• 脆弱性が1点見つかったことで総合評価が最低ラインとなる書きぶりには違和感がある。<br>• 提示された対策内容が、実施すると製品が動かなくなる方法だった。<br>• 製品に関する規格や顧客利便性とのバランスなどについて配慮が無く、一般論的な報告に期待外れの印象を受けた。<br>• 全機種共通の報告と機器固有の報告とでは、報告書を分けていただきたかった。 |
| 検証結果報告会の内容 | 報告不足 | • テスト手順を含むテスト記録も提供いただきたいと事前に伝えていたが、提供されなかった。<br>• テストの十分性の理解や共有がうまくできなかった。 |
| | その他 | • 懸念事項や、推奨事項の報告に、時間を多く使っていただきたかった。 |
| 検証期間 | 計画の遅れ | • 計画が守られなかった。<br>• 報告書の提出が予定から何度も遅れたため、報告書を見てから報告会までの時間が短くなってしまった。 |
| | 検証期間の長さ | • 内容に対し、検証期間が長かった。 |

| アンケート項目 | カテゴリ | 主な回答理由 |
|---|---|---|
| | | • 開発段階での検証と考えると、時間がかかりすぎている。 |
| | 検証期間の短さ | • 他の検証に至らなかったことを考えると、検証期間としては少々短かったと思う。 |
| | その他 | • 検証が NDA 締結後になってしまったため、製品のリリースタイミングと重なってしまい、一部商用製品で検証を実施することになった。<br>• 商品開発と連動する際、スケジュールに影響が出そうだと感じた。<br>• 検証前のテスト計画や検証期間中の経過報告がなかったため、検証期間が妥当だったか判断できない。 |

本事業を通じて IoT 製品等に対する検証を実施することで、どのような効果・メリットがあったかについての主な回答を表 2.3-3 に示す。最も多かったのは、脆弱性等の確認・対処に関する効果・メリットである。また、今後の製品開発に活かせる知見の習得、セキュリティ意識の向上、説明性の向上に関する効果・メリットについてもあげられた。

表 2.3-3 本事業を通じて IoT 製品等に対する検証を実施することで、どのような効果・メリットがあったかについての主な回答

| カテゴリ | 主な回答 |
|---|---|
| 脆弱性等の確認・対処 | • 脆弱性の発見と対処が可能となった。<br>• 検証できていない手法や観点で脆弱性の検証ができた。<br>• 脆弱性検出ツールでは検出できない脆弱性を検出できた。<br>• 第三者の目から、新しい基準での検証結果を得られた。<br>• これまで具体的なリスクとして想定していなかった点に気づくことができた。<br>• 顧客から指摘される前に、メーカーと脆弱性について共有できた。<br>• 今後取り組むべき内容についても的確に指摘及びアドバイスをいただけ、商品をリリースする前段階で対策漏れや不足部分を把握することができ、商品の脆弱性対策を向上することができた。<br>• リスクに対する処置方法の説明があったため、製品に対するリスクマネジメントが進められる。<br>• 製品内に脆弱性が認められないという想定通りの結果が得られ、その開発手法に問題がないことを検証できた。<br>• 問題が無いという検証結果が得られ、ユーザに安心して提供できるサービスと確信が持てた。<br>• 自社製品のセキュリティ面での品質レベルが一通り把握できた。また、製品開発を委託したパートナー企業のセキュリティに対する設計思想や実力について再確認することができた。 |

| カテゴリ | 主な回答 |
| --- | --- |
| | • 自社の製品のセキュリティ状況を専門家の視点で評価いただけたため、対応すべき点が明確になった。<br>• 課題点が明確になり、今後の改善の方向性が確認できた。<br>• 脆弱性を認識できたことで、今後何らかの対策を行う必要があるかどうかを検討するための情報が得られ、対応に関する工数の削減ができた。<br>• 社内で製品セキュリティ対策を検討するよい機会となった。 |
| 今後の製品開発に活かせる知見の習得 | • 一般的な製品セキュリティのレベルが分かった。<br>• セキュリティ等について考慮すべき項目に関する知識が得られた。<br>• 今後、IoT 製品を開発する上での対策の指標になった。<br>• 検証内容や手順、評価基準等、他の製品開発にも活かせる情報を得ることができた。<br>• どの部分にセキュリティ上の課題があるか分かったため、今後の製品開発において設計からセキュリティを意識することができる。<br>• 今後の社内製品ポリシーを検討する上で、大きな刺激となった。<br>• 今後、新製品の仕様決定の際に要望がなくとも、客先に対して積極的に情報漏洩対策に関して提案していく方針ができた。<br>• 設計部門による設計妥当性検証とは別に、このような第三者検証が有効であることが改めて認識できた。<br>• 診断サービスの流れや内容を経験でき、今後のサービス活用や連携等の検討のベースができた。<br>• 脆弱性検証ツールで何をどのように検証できるかについて理解できたため、次回以降の検証に活かせる。また、さらなる検証の必要性を認識できた。<br>• 外部委託による脆弱性検証を依頼した場合の経験を積むことができ、次回以降の依頼方法や評価観点に関するノウハウを蓄積することができた。<br>• 製品開発に従事するメンバーが、セキュリティ検証の実務経験を積めた。<br>• 検証ツールを紹介いただけたため、今後は自社でテストが行えるようになった。<br>• 社内で検証を実施したときと社外に検証を依頼したときの差異を比較することで、社内での検証の十分性等を見直すことができた。 |
| セキュリティ意識の向上 | • 社内に IoT 製品のリスクを周知できた。<br>• セキュリティについて考えるきっかけとなった。<br>• 脆弱性に関する意識を高める効果があった。<br>• 全社的にセキュリティ検証の必要性の啓蒙ができ、開発者の意識向上につながった。<br>• セキュリティレベルと着手すべき一手目が明確になり、社内的にも脆弱性の対応に力をいれるべきという温度感になった。 |
| 説明性の向上 | • 他社評価を受けることで、社内への説明性が向上する。<br>• セキュリティ対策について対外的に示していく際の説得力ある証跡を得ることができた。 |

| カテゴリ | 主な回答 |
|---|---|
| | • 製品の販売促進の材料を得られた。<br>• 顧客のセキュリティ意識を上げたり、顧客と意思疎通を図ったりするための要素になる。 |

本事業を通じてよかった点についての主な回答を表 2.3-4 に示す。脆弱性等の確認・対処、今後の製品開発に活かせる知見の習得、セキュリティ意識の向上、説明性の向上、費用サポート等に関する意見が挙げられた。

表 2.3-4 本事業を通じてよかった点についての主な回答

| カテゴリ | 主な回答 |
|---|---|
| 脆弱性等の確認・対処 | • 脆弱性を洗い出すことができた。<br>• 社内ガイドラインにはないセキュリティの観点を確認することができた。<br>• 体系的に脆弱性の検証を行っていただいたことで、問題の認識につなげられた。<br>• 指摘事項を製品へフィードバックすることができ、改善につながった。<br>• 対策案について検証事業者と意見交換ができ、対策の方向性を考えることができた。<br>• 社内で製品セキュリティ対策を検討するよい機会と材料が得られた。<br>• 検証製品とその開発を委託した企業の実力を把握できた。<br>• 標準的な基準によって検証が行われたため、定量的な検証結果を得ることができた。<br>• 社内での検証は内部構造を理解した上での内容になりがちであるため、第三者である外部事業者に検証していただくことはよい経験になった。 |
| 今後の製品開発に活かせる知見の習得 | • セキュリティ対策に関する仕様検討、設計、製品の出荷前テスト、バージョンアップの追尾等、製品開発や保守に関し、組織的な運用の取り組みを検討するきっかけとなった。<br>• 開発時におけるセキュリティ対策への参考になった。<br>• 複数の製品について申請を出すことができたため、開発時期や体制の違いによる製品の成熟度の差を評価することができた。<br>• 攻撃者目線での製品の見え方が分かった。<br>• 委託可能な外部検証事業者の存在を知ることができた。<br>• 製品開発時にどのようなセキュリティチェックが必要かについて、勉強になった。今後の新製品開発では、脆弱性診断を実施したい。<br>• 第三者の専門家による検証が必要であることを改めて認識できた。<br>• セキュリティ検証を外部委託する際に、注意すべき点や事前に擦り合わせするべき点等が洗い出せた。<br>• 自社でセキュリティ試験を実施できる知識や技術がないと、外部に委託することは難しいことが分かった。<br>• これまで脆弱性検出ツールのアウトプットを自身で解釈し、手探りで判断を実施し |

| カテゴリ | 主な回答 |
| --- | --- |
| | てきたが、おおむね判断に誤りがないことを確認できた。<br>• 検証すべきポイントがよく理解できた。今後の社内検証にも取り入れたい。<br>• 検証の手法や作業全体の進め方（特に開始時の初期提案、ヒアリング、提案、キックオフの手順）、結果のまとめ方等、検証を実施する側として参考になることが多くあった。 |
| セキュリティ意識の向上 | • 第三者に検証いただくことで、製品の脆弱性対策に対する意識の向上の効果があった。<br>• 開発者が脆弱性について直接報告を受けたことで、開発者自身の意識改革につながった。<br>• セキュリティに関して漠然とした認識でいたが、外部からの攻撃といった実例を挙げて説明いただき、参考になった。<br>• 「組み込み用 OS だから」「LAN 接続限定だから」といった考えでいると、足元を掬われる可能性が高いことが分かった。<br>• 実際の製品・システムで検証を行ったため、紙ベースの教育や座学では得られない実感を得ることができた。<br>• セキュリティ設計の大切さをビジネスとして捉える必要があることについて、考えるトリガーとなった。 |
| 説明性の向上 | • 脆弱性に関する資料を作成することができ、それにより脆弱性に関する引継ぎが可能となった。<br>• IoT 機器の導入に際する方向性や指針の検討に向けた幹部向けの情報共有に結果を活用できた。<br>• 客先からの要件定義に含まれていなくとも、客先に対してセキュリティ対策を提案できるようになった。 |
| 費用サポート | • 組み込み機器のペネトレーション系の検証は一般的に高額であり、どこまで実施すべきかの判断が難しく、ベンチャーにはハードルが高いため、費用面で助かった。<br>• セキュリティ対策の優先度を上げるためには現状の評価が必要である一方、かかるコストによっては評価を躊躇してしまうため、コスト面のサポートをしていただけてよかった。<br>• 中小企業にとって後回しになりがちなセキュリティ検証を気軽にできる機会をいただけてよかった。<br>• 社内ではできなかったセキュリティ検証を無料で受けられてよかった。 |
| その他 | • 経済産業省の推進する事業である点が安心感を与えてくれ、参加の心理的ハードルが下がった。<br>• エントリー時に希望する検証事業者を申請できてよかった。<br>• 検証事業者にある程度ドライブいただけたため、手間が多くかかることなく、検証を実施できた。<br>• 対象製品ごとに選任で担当者がついたため、担当者とのやり取りがスムーズにできた。 |

| カテゴリ | 主な回答 |
|---|---|
| | • ネットワークセキュリティのプロフェッショナルと対話する機会がステップとして組み込まれていてよかった。<br>• セキュリティ専門企業と関係が構築できた。 |

本事業を通じて困った点や改善すべき点についての主な回答を表 2.3-5 に示す。検証に向けた準備、検証の実施内容、検証結果報告、連絡・コミュニケーション、事業設計等についての意見が挙がった。

表 2.3-5 本事業を通じて困った点や改善すべき点についての主な回答

| 項目 | カテゴリ | 主な回答 |
|---|---|---|
| 検証に向けた準備 | 連絡・説明の不足 | • 検証用の装置が 3 セット必要だということは、検証開始前に知りたかった。<br>• テスト実施前に、テスト計画やテスト項目の全体像を共有いただきたい。 |
| | その他 | • 検証実施事業者ごとに提出する資料や機器の必要台数が違ったため、統一化していただきたい。 |
| 検証の実施内容 | 検証内容の擦り合わせの不足 | • 検証内容について、どこまでリソース上可能なのかがよく分からなかった。<br>• 検証内容の説明が漠然としており、検証がどの程度網羅されているものなのかついて判断しづらかった。検証項目のリストを提示いただきたい。<br>• セキュリティに関する知見が不足していたため、検証内容が事実上おまかせの状態となってしまい、結果として自社で想定していたような検証ができなかった。<br>• 検証内容が把握できていない状態で検証が進んだ。内容の理解に対するサポートを検証事業者以外の方に行っていただけるとよい。 |
| | その他 | • 検証の経過報告等が無かった。検証項目の選別にもう少し注力いただきたい。<br>• グルーバルネットワークに接続して使用される観点から評価いただけると、より参考になる。<br>• 今後はクラウドと連携した IoT 製品が主流になってくると思われるため、IoT 製品のみの診断では片手落ちとなる懸念がある。検証の範囲についてご検討いただきたい。<br>• 検証で使用できるネットワーク環境が限られていたため、一部のネットワーク機器に対して主要な機能に関する検証を行うことができなかった。<br>• マシンに搭載された IoT 機器に対応いただくため、検証場所を限定しない検証方法を検討いただきたい。 |

| 項目 | カテゴリ | 主な回答 |
| --- | --- | --- |
| 検証結果報告 | 記載・報告不足 | • 各検証項目／検証目的について、対応する CWE 識別子を事前に明示いただきたい。<br>• 中小企業が目標とすべき検証スコアを参考値として例示いただけると、改善の参考になる。<br>• それぞれの脆弱性をついた代表的なハッキング手口や実害例等を報告書に示していただけると、それぞれの項目に対する危険性が分かりやすくなる。<br>• 今回の検証で追えなかった箇所について、リスクが生じる部分があるか否かの補足説明がもう少し充実していると、より良い検証になると思われる。<br>• 報告会を工場幹部参加のもと実施したが、脆弱性に対する注意喚起に留まり、IoT 機器を導入推進することへ向けての課題の認識にまでは至らなかった。 |
| | その他 | • 商品が過度に脆弱であるような報告書に見えたため、是正コメントを添えて再提出いただいた。 |
| 連絡・コミュニケーション | 連絡体制 | • 複数の方からそれぞれ連絡が来るため、連絡窓口を一本化していただきたかった。<br>• 事前のやり取りから結果までをまとめてアーカイブできるとありがたい。 |
| | コミュニケーション不全 | • 担当者があまりにも専門的な方だと、意思疎通が難しい。<br>• 事業の趣旨を誤解していたように感じている。あまり知識のない人でも理解できるよう、分かりやすく説明をしてほしい。<br>• 検証に別の業者が入るのであれば、事前に通知いただきたい。 |
| | その他 | • 脆弱性検証に不慣れな企業を支援する事業だと認識している。検証を単に実施するだけでなく、企業への教育/アドバイスも行いながら検証を進めていただきたい。 |
| 事業設計 | 検証終了後のフォロー | • 指摘された脆弱性への対策について、社内で対応できる部分と社内だけでは対応できない部分があった。<br>• セキュリティ設計のコンサルや検証メニューの案内といったアフターフォローも行っていただけると、今後の製品開発において、自律的・継続的にセキュリティ設計・検証に取り組めるようになる。<br>• 検証終了後、無料もしくは低価格でのフォローがあれば、さらによかった。<br>• セキュリティ脆弱性検証の結果、どこまでの対策が必要かに関するコンサルまで含めて、補助事業の対象にしていただきたい。<br>• 指摘事項の対策後に、もう一度検証いただける機会を作っていただきたい。 |

| 項目 | カテゴリ | 主な回答 |
|---|---|---|
| | 事業の継続 | • ネットワークの堅牢性は社会インフラの一部であるため、事業の継続を期待する。<br>• 自社でセキュリティ対策ができない零細中小企業が、検証の委託のための予算を確保することは難しいと思われる。中小企業へセキュリティ対策を広めるため、国として予算を確保し、検証の補助を続ける、検証事業者に補助をして委託金額を低くする等、中小企業がコストを抑えて対策できる施策の継続が必要だと感じた。 |
| | その他 | • 基準を満たしていることを第三者として評価いただき、「認証」していただきたい。 |
| その他 | - | • 契約締結は迅速に行っていただきたい。<br>• 検証内容の割に、検証期間が長かった。<br>• ステークホルダーを説得するための材料の用意に苦心したため、脆弱性の潜在的なリスクを詳らかにする重要性を説くための資料等があればよい。<br>• 検証を実施した機器が利用できなくなるため、機器の分解は不要にしていただきたい。 |

IoT 製品等に対する外部事業者の検証サービスの活用意向についての回答を図 2.3-2 に示す。集計は、製品別ではなく、企業別に実施した。同一企業で「今後も活用したい」と「条件付きで活用したい」の両方の回答があった場合は、「製品という条件によって活用意向が変わる」と解釈し、「条件付きで活用したい」に統一を行った。その結果、「今後も活用したい」「条件付きで活用したい」と回答した企業は約 96%という結果になった。

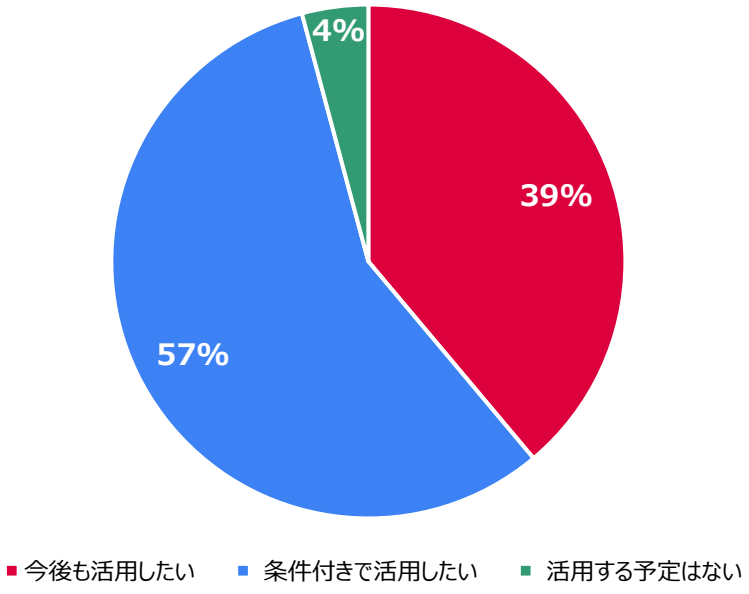



図 2.3-2 IoT 製品等に対する外部事業者による検証サービスの活用意向(N=72)

「今後も活用したい」「条件付きで活用したい」と回答した企業に対して、外部事業者の検証サービスを活用する際、どのような観点を重視して検証サービス事業者を選定するかについて尋ねた結果を図 2.3-3 に示す。「検証にかかる費用」と回答した企業は 69 社中 31 社となっており、費用が重要なファクターになっていることが読み取れる。続いて、「サービス内容」が 22 社、「スキルや知見」が 15 社、「検証実績」が 12 件という結果であった。

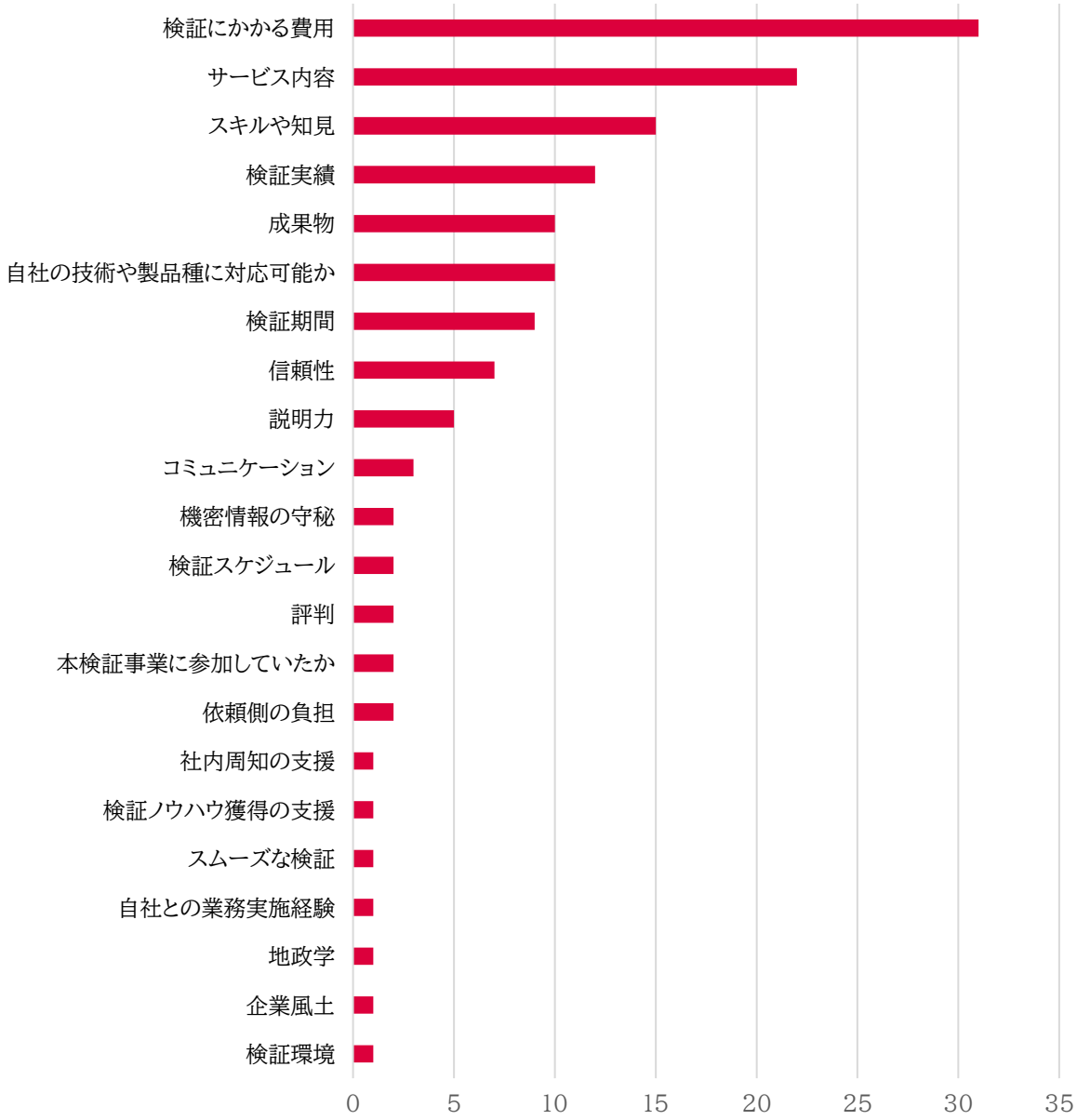



図 2.3-3 外部事業者の検証サービスを活用する際、
どのような観点を重視して検証サービス事業者を選定するか（複数回答）

図 2.3-3 で示された観点以外の活用条件については、以下の意見が挙げられた。

- 自社で実施内容を決められるようになれば、検証を外部に依頼していきたい。現状では、期待した結果を得られるような依頼ができそうもない。
- 検証結果に対する客先のご意見等を踏まえて、今後実施するかを検討することになると思われる。まずは、弊社内での認識・知識の向上が優先だとも考えている。

- 同種製品の他社比較等を行い、脆弱性の危険性が判断できれば、活用したい。

また、「今後も活用したい」「条件付きで活用したい」と回答した理由についての主な回答を表 2.3-6 に示す。「脆弱性や対策の抜け漏れについて確認したいから」「新製品・サービス・機能の確認を行いたいから」「セキュリティ検証の重要性を感じているから」「専門的な知見が必要だから」「付加価値の維持・発展をしていきたいから」「親会社や顧客から求められるから」といった理由が挙げられた。

表 2.3-6「今後も活用したい」「条件付きで活用したい」と回答した理由についての主な回答

| カテゴリ | 主な回答 |
|---|---|
| 脆弱性や対策の抜け漏れの確認 | • 脆弱性を洗い出すことができ、今後のセキュリティ対策において非常に有用であるため。<br>• 様々な機器との通信や IPC 自体の多様化・変更などが考えられるため、セキュリティに関する抜け漏れがないか確認したい。 |
| 新製品・サービス・機能の確認 | • メジャーな機能や製品・サービスの追加があるタイミングで、第三者レビューを受けたい場合に活用したい。<br>• 新たな製品・サービスを提供する際に、ハッキングの手口を知らないと防ぎようがないため。 |
| 重要性の認識 | • 製品の機能実現と同様に、重要な要件だと認識しているため。<br>• 今後、IoT 製品の拡充を予定しており、情報セキュリティの重要性を感じているため。<br>• 今回、セキュリティ検証の重要性を認識し、今後の製品開発でも検証が必要であると認識したため。 |
| 専門的な知見の必要性 | • 自社だけの知見では限界があるため、専門家による診断は必要だと考えている。<br>• セキュリティ基準に関しては日々変化するものであるため、専門の方の目線から意見をいただきたい。<br>• 社内にセキュリティの専門部署が無いため、定期的に自社のスコアを確認したいため。<br>• 専門的なツールを使った解析は現状自社では困難なため。<br>• 外部からの客観的な視点での検証は、有意義な結果が得られる可能性が高いため。 |
| 付加価値の維持・発展 | • 継続的に診断を受けることで、製品の付加価値を維持・発展させていきたいため。 |
| 親会社・顧客対応 | • 今後、ネットワーク関係の部分については、親会社のセキュリティポリシーに準拠するため、そちらで実施する可能性がある。<br>• 先進的な顧客への対応するため、活用する場合がある。<br>• 顧客によっては第三者による評価が必要なケースがあるため、今後も活用してく方針である。 |

加えて、「活用する予定はない」と回答した理由についての主な回答結果は以下のとおりである。

- IoT 機器向けのサービスを提供予定のため、IoT 機器そのものを検証するサービスを活用する予定はないが、検証サービスと弊社サービスの連携は考えたい。
- 今回は、実際の使用方法等をベースにした評価検証になっていなかったため、同様の検証は不要と考える。

本事業で検証対象とした IoT 製品等に対して実施しているセキュリティ対策についての回答結果を図 2.3-4 と表 2.3-7 に示す。出荷後における脆弱性対応のためのアップデート体制の整備については、約 75%実施されていた。また、設計段階における IoT 製品等の守るべき機能や情報の特定、求められるセキュリティ機能の検討、出荷後のリスクに関する情報収集・分析については 50%以上実施されていた。一方、それ以外の対策については実施率が 50%を下回っており、特にセキュリティサポート方針の明確化については、約 14%という結果だった。こうした背景を踏まえ、セキュリティ対策に取り組もうとする企業が最初に検討すべき対策について、3 章で後述する IoT 機器等を開発する中小企業向けのセキュリティ対策に関するガイドに記載している。

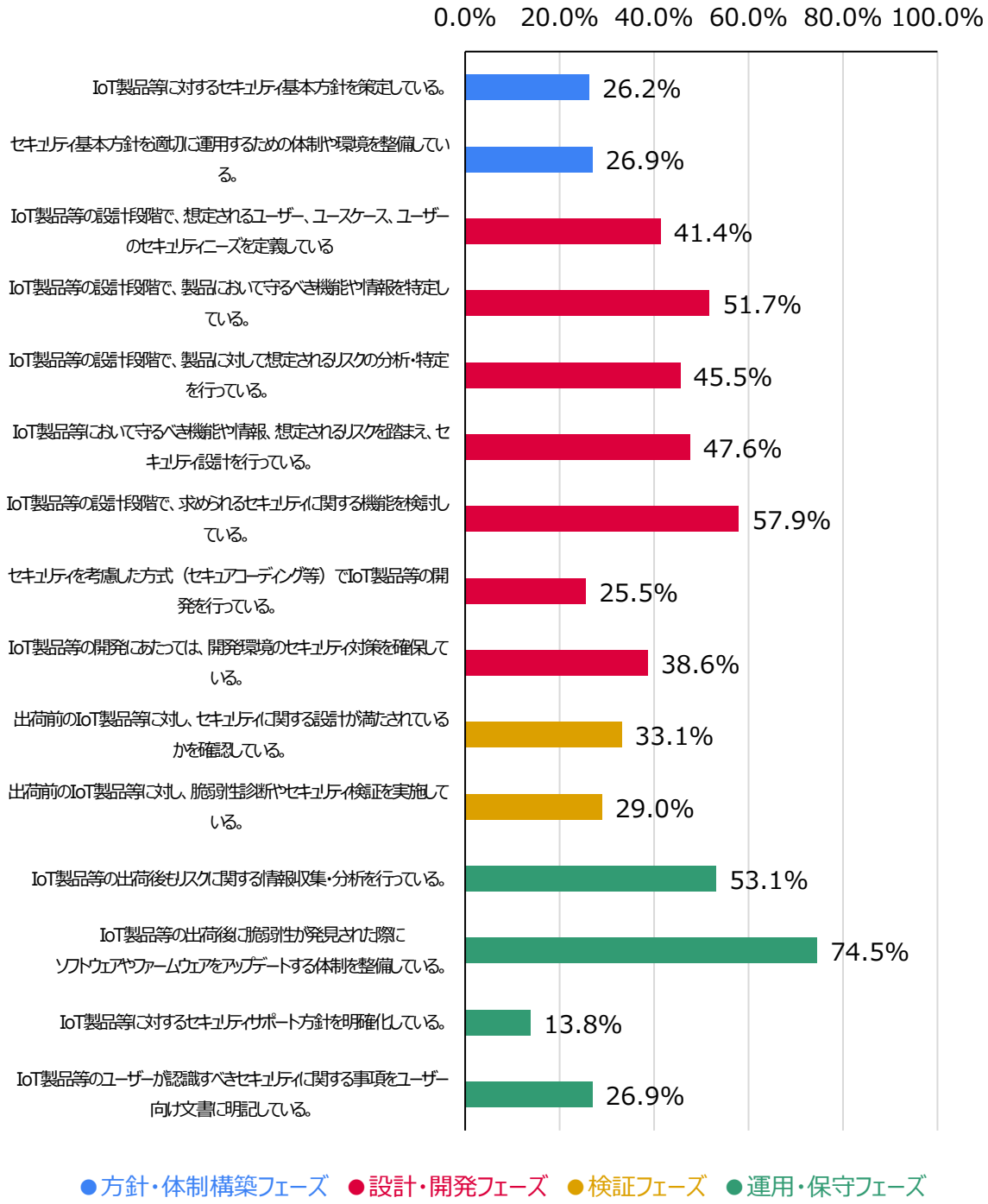



図 2.3-4 本事業で検証対象とした IoT 製品等に対して実施しているセキュリティ対策（N=145）

表 2.3-7 本事業で検証対象とした IoT 製品等に対して実施しているその他のセキュリティ対策

| フェーズ | その他のセキュリティ対策 |
|---|---|
| 方針・体制構築フェーズ | • 開発者を含めた社員へのセキュリティ教育を実施している。<br>• 脆弱性の公開を含め、PSIRT の活動を推進している。<br>• 個人情報の取扱いについて、第三者評価を実施している。 |
| 設計・開発フェーズ | • 使用環境での利便性とセキュリティ対策が両立するよう、物理面も含めて検討している。 |

| フェーズ | その他のセキュリティ対策 |
| --- | --- |
| | • サービス終了後の IoT 製品のデータの取扱いについて、検討・確認を行っている。<br>• プログラム開発前段階で、信頼度の高いフレームワークやライブラリを選定している。<br>• IoT 推進コンソーシアム・総務省・経済産業省による IoT セキュリティガイドラインを参照し、必要と考えられる機能を盛り込んでいる。<br>• セキュリティ対策がしやすい機能を提供している。<br>• ソフトウェア開発の際に、デバッグログやシステムログ等を取得しやすい機能をできるだけ実装し、セキュリティ関連の問題を含め、障害発生時の対応を容易化するための施策を採っている。<br>• データフォーマットを非公開にしている。<br>• データの暗号化を行っている。<br>• バッファオーバーフロー(CWE-119)対策を行っている。<br>• SE や HSM を用いてハードウェアレベルの対策を実施している。<br>• セキュリティを意識したコーディングルールの策定を進めている。<br>• ISO9001 に沿ったプロジェクト開発を行う中で、リスクアセスメントや HW/SW 実装に関するチェックシートの作成、ドキュメントの管理(トレーサビリティ)を実施している。 |
| 検証フェーズ | • 第三者による AWS 脆弱性診断を行っている。 |
| 運用・保守フェーズ | • 出荷前後で発見されたセキュリティリスクについて、ODM 開発元に早急にフィードバックしている。<br>• 出荷前や使用前に、ユーザに対して、生じる可能性のあるリスクの説明を通知できる範囲で行っている。<br>• コンテナベースのリモートメンテナンスサービスを利用している。<br>• IoT 製品が行う通信を監視・記録するサーバを置き、エラーが生じればメールで通知するようにしている。 |

IoT 製品等に対する開発費用のうち、セキュリティ対策にかける費用の割合についての回答結果を図 2.3-5 に示す。半分以上の製品は、セキュリティ対策にかける費用の割合が 10%未満という結果だった。一方、製品によっては 30%以上の費用をかけている製品もあり、具体的にはセキュリティ関連製品やルータ、ネットワークカメラといった製品であった。

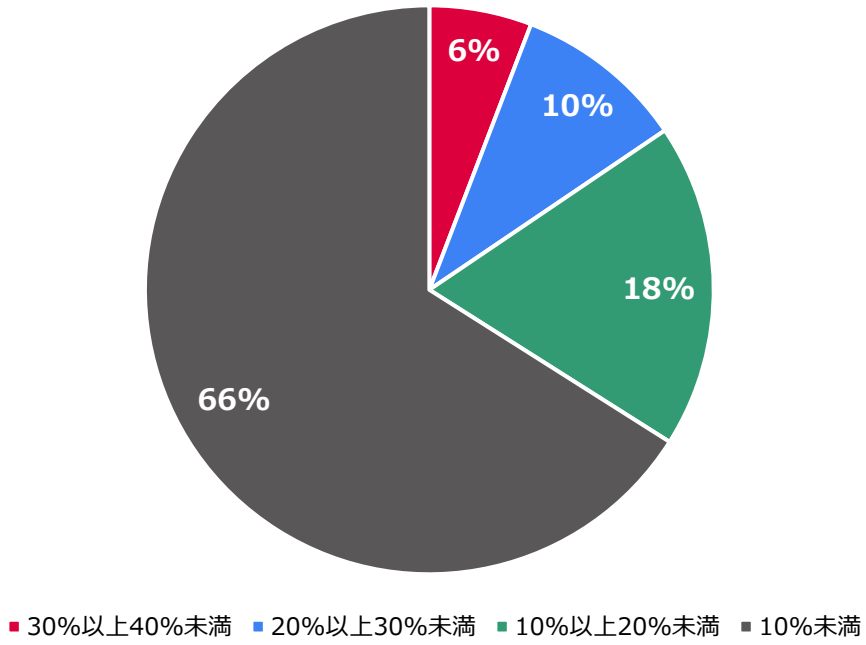



図 2.3-5 IoT 製品等に対する開発費用のうち、セキュリティ対策にかける費用の割合(N=145)

IoT 製品等に対するセキュリティ対策の検討・実装等に当たって、活用しているガイドラインや文書についての回答を表 2.3-8 に示す。IoT 機器等に関する共通的なガイドライン・文書から業界別のガイドライン・文書に至るまで、様々なガイドライン・文書が挙げられた。

表 2.3-8 IoT 製品等に対するセキュリティ対策の検討・実装等に当たって、活用しているガイドラインや文書

| カテゴリ | 活用しているガイドラインや文書 |
|---|---|
| IoT | • IoT セキュリティガイドライン ver 1.0(IoT 推進コンソーシアム・総務省・経済産業省)<br>• つながる世界の品質確保に向けた手引き(IPA)<br>• IoT セキュリティ手引書 Ver2.0(セキュア IoT プラットフォーム協議会)<br>• IoT 機器セキュリティ要件ガイドライン・IoT 機器セキュリティ要件適合基準ガイドライン(重要生活機器連携セキュリティ協議会) |
| 組み込み | • 組込みソフトウェアを用いた機器におけるセキュリティ(改訂版)(IPA)<br>• 組込みシステムのセキュリティへの取組みガイド(2010 年度改訂版)(IPA) |
| 制御システム | • IEC62443-4-1 |
| 脆弱性対策情報 | • JVN iPedia |
| セキュアコーディング | • セキュア・プログラミング講座(IPA)<br>• CERT C コーディングスタンダード(JPCERT/CC) |
| Web サイト | • 安全なウェブサイトの作り方(IPA) |
| クラウド | • クラウドサービスレベルのチェックリスト(経済産業省) |
| IT セキュリティ | • ISO/IEC 15408<br>• サイバーセキュリティ基本法 |

| カテゴリ | 活用しているガイドラインや文書 |
|---|---|
| | • 国民のための情報セキュリティサイト（総務省） |
| 安全側面 | • ISO/IEC Guide 51:2014 |
| 医療 | • 3 省 2 ガイドライン（厚生労働省、経済産業省、総務省）<br>• ISO 14971:2019 |
| 自動車 | • ISO/SAE 21434 |
| 電力 | • 自家用電気工作物に係わるサイバーセキュリティの確保に関するガイドライン（内規）（経済産業省）<br>• 電力制御システムセキュリティガイドライン（JEAG111-2019）（日本電気技術規格委員会） |
| 工場 | • 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver1.0（経済産業省） |
| ネットワークカメラシステム | • ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト第 2 版（IPA） |
| クレジットカード | • PCI DSS<br>• EMV の各種規定 |
| 社内資料等 | • 3G/LTE 機能を有する IoT 機器の適合認定に関する社内資料<br>• 社内のセキュリティ標準規定<br>• セキュリティ部門が作成した社内ガイドライン<br>• 社内で定義しているプロダクトセキュリティガイドライン<br>• IEC 62444-1, 2 に準拠した社内技術文書<br>• 既存製品で適用している業務記録（ISO9001 準拠）に登録されているチェックシート類<br>• グループの上位ドメインが制定しているガイドライン<br>• デバイスメーカー発行のマニュアル・データシート |

IoT 製品等に対するセキュリティ対策の検討・実装等に当たって抱えている課題についての主な回答を表 2.3-9 に示す。セキュリティ意識や知識、経験に関する課題のほか、機器開発の各ライフサイクルフェーズにおける様々な課題が挙げられた。

表 2.3-9 IoT 製品等に対するセキュリティ対策の検討・実装等に当たって抱えている課題についての主な回答

| カテゴリ | 主な回答 |
|---|---|
| セキュリティ意識 | • 求められるセキュリティ対策レベルについての認識を現場に浸透させる必要がある。<br>• 社内で扱う調達品に対するセキュリティの認識が進まなければ、今後開発する IoT 製品へのスムーズな対策実施は難しいと思われる。<br>• セキュリティ意識が高い顧客であれば、セキュリティが機能要件に入るが、そうでない場合、コストが高くなってしまうため、セキュリティ要件は入らない。 |

| カテゴリ | 主な回答 |
| --- | --- |
| | • ローカルネットワーク内の想定で開発を行っていたため、セキュリティを意識していなかった。<br>• インターフェース部分におけるリスクは想定していなかった。 |
| 知識や経験 | • セキュリティ対策を必要とする機器の開発経験が少なく、まず何からスタートすればよいのかが分からない。<br>• セキュリティ管理に関するノウハウが社内になく、自力で完全な要求定義や検証ができない。<br>• ガイドラインを読むだけでは、具体的にどのようにしてセキュリティ対策を行えばよいのか理解できない。<br>• ハードに近い部分に関する知識が薄く、現実問題として対策が行えない。<br>• セキュリティに関する法規についての知識が不足している。 |
| 指針等の策定 | • 顧客によって、セキュリティ対策の要否や要求水準が変わるため、基本方針が策定しづらい。<br>• セキュリティに関する社内基準が明確になっておらず、担当者の力量・意識次第となっている。<br>• 社内共通のセキュリティ対策ガイドラインや脆弱性検証プロセスの取り決め等がない。<br>• セキュリティを含むソフトウェア開発において、全社的なコーディングルールや設計基準が統一されておらず、担当者や開発グループ単位で決めているため、ノウハウが有効に活用されていない。<br>• インターネットに接続した場合のセキュリティ対策に関するチェックシート等の整備が不十分である。<br>• 特に当社主導でセキュリティ対策を施す量産品と、顧客主導でセキュリティ対策を施す個産品で、セキュリティ対応に違いがある中で、全社的な対応をどのように推進していくかが悩ましい。 |
| 体制構築 | • セキュリティ専門の部署や担当者の設置ができていない。<br>• セキュリティ対策に関して属人性があるため、改善したい。<br>• 日々アップデートされるセキュリティ情報を継続的に認識し、選別できるような組織作りができていない。<br>• サポート体制の構築ができていない。<br>• セキュリティインシデントが発生した際の対応体制の整備ができていない。<br>• 品質保証活動においてセキュリティ対策が活動範囲に含まれておらず、専門家も擁していない。<br>• 専門の技術者がおらず、担当者に一任されている。<br>• 社内にセキュリティ設計に関する有識者がおらず、今後どのようにセキュリティ対策を実施すればよいのか、どの程度実施すればよいのかについての方向性が定まらない。<br>• 会社のステージ・規模的に、セキュリティの専門家やスキルフルなレビュワー |

| カテゴリ | 主な回答 |
| --- | --- |
| | を社内で抱えられないため、継続的なセキュリティレベルの維持を行うことができない。<br>• 経営上、社内に専門家を抱えることが難しいため、ニーズに応じて専門家との協働や委託を推進したい。 |
| 対策選定 | • 社内手順に製品開発におけるセキュリティリスクの分析について定められているため実施しているが、形だけとなっており内容が適切とは言えない。<br>• 機能や耐久の品質と比べて、セキュリティの品質は目に見えづらいため、どの程度対策に力をいれるべきか判断しづらい。<br>• セキュリティ対策に明確な基準がなく、顧客からの要望も曖昧であるため、どこまでの対策が必要なのかが判断できない。<br>• 他社の動向が掴めず、どの程度セキュリティ対策に力を注ぐべきかのバランスが取れない。<br>• セキュリティ対策を強化する方法を案出できても、そのために必要なコストや運用上の要求とのバランスで採否を決めざるを得ないことが多くある。<br>• 利用シーンによって、セキュリティ対策の投資対効果が変わってくるため、何らかのガイドラインに自社の基準を合わせていく必要があると考えている。<br>• 開発委託製品に関して、開発時のセキュリティ技術の選択が難しい。<br>• セキュリティ対策が社内基準のみへの対応となっている。 |
| 対策実装 | • 物理的な攻撃に対するセキュリティ対策の実装に課題がある。<br>• セキュリティとソフトウェア開発の両立に課題がある。<br>• セキュリティと使い勝手の両立に課題がある。<br>• ユーザが自由に製品の改造等を行えるようにした上で、セキュリティ対策を行うことに課題を感じている。<br>• セキュリティ対策といった開発のノウハウが開発グループ内でのみ共有されており、他のグループとの連携があまり行われていない。 |
| 検証の実施 | • 検証能力や検証機材が不足している。<br>• 継続的に診断を実施するためのコストの捻出が難しい。<br>• 機器について、定量的・定性的にセキュリティリスク・脆弱性をある程度正確に測るための手段やツールが存在しない。<br>• サードパーティ製の脆弱性テストの導入を検討しているが、費用面が厳しい。 |
| 出荷後の対応 | • 継続的なソフトウェアのアップデートができていない。<br>• 製品のリリース後に発生した脆弱性に対応する際、影響範囲の大きさによって対応コストが肥大化してしまう。また、対策の必要性を判断するために、多くの時間を要しているため、スピーディーに対応することができていない。<br>• 製品内部で使用している OSS モジュールの脆弱性対処において、互換性の観点から単純にモジュールのバージョンを上げる対処をすることができず、 |

| カテゴリ | 主な回答 |
| --- | --- |
| | 出荷時のバージョンのソースに対して対処パッチを適用しているが、製品寿命が長期化しているため、旧バージョンに対する対処パッチを用意することが難しくなっている。<br>• 新製品の販売又はファイアウォールの大規模バージョンアップ時に、セキュリティ強化のためパスワードの禁則内容の変更等の対処をすることがあるが、対処を行うとエンドユーザから従来通りの弱い設定ができなくなったというクレームを受けることが多い。<br>• チップベンダーから提供された SDK そのものに含まれるモジュール自体が古い場合が多く、様々な要因で最新のモジュールにアップデートできない場合が多い。クラウド等と異なり、脆弱性対応のために頻繁にファームウェアアップデートを行うことができない。<br>• IoT バージョンアップ用の保守回線の構築やセキュリティ面でのシステム保守に課題がある。<br>• ユーザとセキュリティに関するコミュニケーションを取るための準備が不十分である。 |
| その他 | • ソフトウェアに関する背景知識を持たない経営上部層に対して、セキュリティ対策の効用を説明することが難しい。<br>• 欧州では ETSI EN 303 645 の義務化の動きがある一方、日本では IoT 機器向けのセキュリティ基準の義務化が進んでいない実情がある中で、セキュリティ対策の必要性やかかるコストについて、ユーザに納得いただくことが困難である。<br>• 自律走行ロボットに関するガイドライン等が存在しないため、クラウドセキュリティガイドラインへの自社の対応状況を回答することが顧客から求められているが、回答が難しい点が多い。<br>• ISO/IEC 27001 等の認証を顧客から求められたとしても、現時点では対応ができない。<br>• 外部に頼る部分を減らして、自己組織内でできる部分を増やしたい。<br>• BtoB の顧客によってセキュリティに関する要件や濃淡が異なることに、課題を感じている。<br>• 製品ライフサイクル全体における製品セキュリティの管理と保証に課題がある。<br>• ODM 製品のため、製品が入荷されるまで完全にブラックボックスとなっている。<br>• ハードウェアに関しては外部委託や調達を行っているため、対策を起案できてもすぐには対処できないケースがある。<br>• 既製品や既製サービスに依存している部分がある。<br>• 個人情報の保護に課題がある。 |

| カテゴリ | 主な回答 |
| --- | --- |
| | • セキュリティ対応を実施することの必要性は理解しているが、いかにコストを下げるかが課題となっている。<br>• セキュリティ対策にかけた費用を製品の売価に反映できない。 |

# 3. IoT 機器を開発・販売する中小企業や検証サービス事業者が活用するガイドライン等の作成

中小企業等が開発・販売する IoT 機器に対する機器検証の実証結果を踏まえ、IoT 機器等を開発する中小企業向けのセキュリティ対策に関するガイドと、中小企業が開発する IoT 機器等に対して検証を実施する検証事業者向けの手引きの 2 つの文書を作成した。作成した 2 つの文書の概要は表 2.3-1 に示すとおりである。

表 2.3-1 本事業で作成した 2 つの文書の概要

| 文書 | 主な対象者 | 目的 | 主な記載内容 | 文書の位置づけ |
|---|---|---|---|---|
| ①IoT 機器等を開発する中小企業向けのセキュリティ対策に関するガイド | IoT 機器等を開発する中小企業 | IoT 機器等を開発する特にセキュリティ対策が進んでいない中小企業に対して、取り組むことを最初に検討すべき事項を示すこと。 | • 対策を怠った場合に想定される影響や、経営層に求められる役割・責任<br>• 機器のライフサイクル全体において、開発する中小企業に求められる対策<br>• 中小企業が対策を選定する上で参考となる情報<br>• 中小企業が自社の状況を踏まえて対策を順次進めるために参考となるような身近な事例 | 既存のガイドには紐付けず、新たなガイドとして公開する。 |
| ②中小企業が開発する IoT 機器等に対して検証を実施する検証事業者向けの手引き | 中小企業が開発する IoT 機器等に対して検証を実施する検証事業者 | 中小企業が開発する IoT 機器等に対して検証を実施する検証事業者に対して、中小企業の特性を踏まえつつ、検証において留意すべき事項を示すこと。 | • 中小企業が開発する機器に対する検証に当たって認識しておくべき中小企業の特性や、それを踏まえて留意すべき事項や実施すべき対応<br>→ 既存の「手引き」本編を拡充<br>• 特定の機器の検証に当たって、検証事業を通じて把握された脆弱性等の状況を踏まえ、検証事業者が留意すべき事項、実施すべき対応、適用すべき検証手法等<br>→ 「機器個別のセキュリティ検証プラクティス集」を新たに策定し、「手引き」の別冊として位置づけ | 既存の「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」を拡充する（本編追記・別冊作成）。 |

## 3.1 中小企業向けガイドの作成

### 3.1.1 作成方針

中小企業向けのガイドの作成に当たって、林立する国内外の既存ガイドラインを中小企業が参照しやすくするために必要な事項とは何か、不足している点はあるか、などの観点も踏まえ、既存ガイドラインの調査を行い、IoT 機器等の開発企業に求められる対策事項や中小企業経営者に求められる対策事項を抽出・整理した。また、中小企業及び検証事業者に対するヒアリング調査を行うことで、中小企業における対策実態を把握するとともに、上記対策項目の実施可否や対策の費用対効果を把握し、ガイドに反映した。加えて、中小企業の IoT 機器等に対する検証の調査の結果を踏まえ、中小企業の IoT 機器等における対策実態や検証フェーズにおいて留意すべき事項を抽出・反映した。さらに、有識者検討会での議論や御意見はガイド全体の記載内容に反映した。

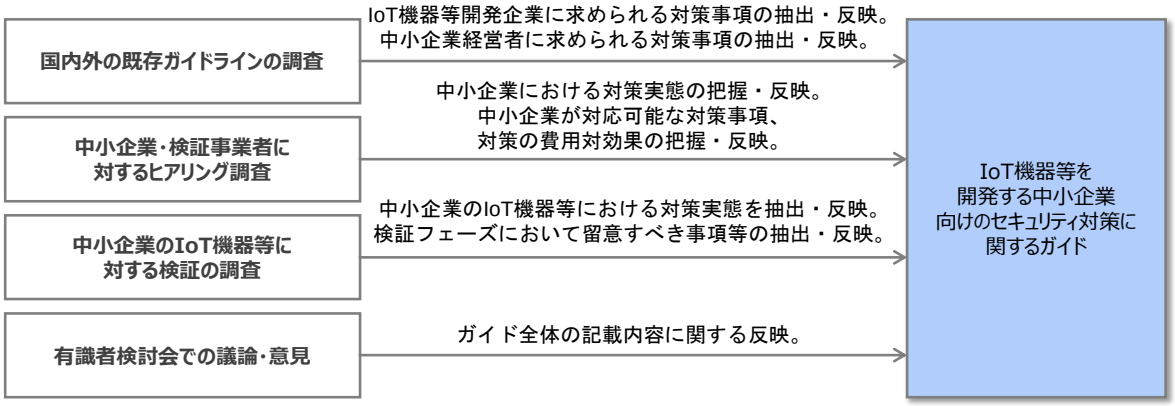



図 3.1-1 中小企業向けガイドの作成方針

### 3.1.2 ヒアリング結果

今年度の実証事業に参画した検証事業者 3 社に対するヒアリングを行い、検証結果を踏まえたガイドに追記すべき事項及びガイド全体に対するコメントについてガイドに反映を行った。ヒアリングの結果を表 3.1-1 に示す。

表 3.1-1 検証事業者に対するヒアリング結果

| カテゴリ | ヒアリング結果 |
|---|---|
| 検証結果を踏まえたガイドに追記すべき事項 | 【Web 管理画面】<br>• Web 管理画面において入力値検証の不備が見受けられた機器が多く存在した。<br>• Web アプリでは、クロスサイトスクリプティング（XSS）やコマンドインジェクションなど、初歩的な脆弱性が多く検出された。IPA の「安全なウェブサイトの作り方」等を参照しつつ、Web アプリに対する対策を支援することがよいのではないか。<br>【開発時のテスト不足】<br>• 開発時のテスト不足が見受けられた機器が多く存在した。パッケージのバージョンを調べ、当該バージョンに既知の脆弱性が存在しないかを NVD を用いて調べる程度は実施すべきである。<br>【機能搭載】 |

| カテゴリ | ヒアリング結果 |
| --- | --- |
| | • 悪用される可能性があるため、不必要な機能はむやみに搭載しない方がよい。<br>• 意図して機能を多く搭載しているケースも存在するが、その場合はアクセス権限を管理者のみにするなどの対策が必要である。<br>【通信セキュリティ】<br>• 通信のセキュリティについて、平文通信しかサポートされていないケースや不要なポートを開放しているケースなど、基本的な対策が実施されていない機器が多く存在した。<br>【アップデート】<br>• 多くの機器においてソフトウェアやファームウェアのアップデート頻度が低いほか、自動更新機能が存在しない機器も存在した。<br>• パッチが適用されていない古い機器は攻撃の起点となる可能性もあるため、セキュリティパッチに関する言及のほか、EOL を明確に定義し、利用者にアナウンスすることの重要性をガイドで記載できるとよい。<br>【注意点の整理】<br>• 機器を活用する際の注意点が整理されていない機器が多かった。<br>【ユースケースの想定】<br>• 機器のユースケースが想定されていない機器が多いと感じた。<br>【組織全体の取組】<br>• 組織全体における機器開発の成熟度向上に向けた取組が必要だと感じた。IPA の「つながる世界の開発指針」のようなドキュメントを一読いただくことから始めていく必要がある。<br>• 検証事業に応募いただいた企業の経営層やセキュリティ担当者の意識は高い一方、開発担当者の意識は必ずしも高いとは言えず、企業内での意識のギャップを感じた。企業全体でのセキュリティ意識醸成に向けた取組も必要である。<br>【リスク認識】<br>• 製品のリスクを認識していない中小企業が多かった。また、大手企業と比較して、製品に対する攻撃可能性の理解が低いと感じた。製品が安全であるという前提を疑うことのアドバイスをガイドに含めてもよいのではないか。<br>【構成管理】<br>• 自社で開発していないコンポーネントがある際に、ブラックボックスであるため把握していないという中小企業もいた。自社製品に含まれるコンポーネントは把握しておくべきであり、中小企業であっても構成管理が実施されることが望ましい。<br>【パスワード設定】<br>• ラズベリーパイのような市販 IoT 機器を活用した製品に対して検証を実施することが比較的多かったが、ラズベリーパイの初期設定に関して、パスワードが |

| カテゴリ | ヒアリング結果 |
| --- | --- |
| | 弱かった。<br>• パスワードの取扱いが甘いものが多かった。例えば、脆弱なパスワードを設定可能なケースがあったほか、初期パスワードを変更しないで機器を利用できるケース、初期パスワードに再変更できるケースも散見された。<br>【デバッグポートへの対策】<br>• 大手企業の場合、デバッグポートへの侵入を防ぐ対策を施すことが多いが、中小企業の製品では、あまりデバッグポートへの対策が施されていなかった。<br>【検証に対する意識】<br>• 検証を通じて、セキュリティ対策を適切に施していることをアピールしたいと意気込んでいた中小企業がいた。大手企業は、設計工程での検証の必要性を理解しているほか、対策上の不安があって検証を依頼することが多い。<br>【検証によって明らかになる事項】<br>• 検証結果を報告したところ、検証で明らかになる内容について驚かれる中小企業も存在した。検証によって明らかとなる事項についても記載されるとよい。<br>【システムテストの有効性】<br>• 未知の脆弱性（想定していなかった挙動による問題）を発見する手法としてシステムテストを活用することの有効性を追記いただきたい。<br>【モバイルアプリのセキュリティ対策】<br>• IoT 製品に付随するモバイルアプリが存在する場合、モバイルアプリのバグ又はモバイルアプリが使用する API の脆弱性によってセキュリティ侵害が発生するケースも多い。今後、特に消費者向け IoT 製品ではモバイルアプリが付属することが主流になると考えられるため、可能な範囲でガイドでも言及できるとよい。 |
| ガイド全体に対するコメント | • 平易な用語を使うとともに、現状の目次案のように、対策が構造化されて記載されるとよい。対策を羅列するだけであると中小企業の多くは理解できないと考えている。また、文字だけで示すのではなく、ビジュアル的にも分かりやすいガイドとなるとよい。<br>• 対策 1～対策 6 のすべてを自らで対策する必要がある、という書きぶりにすると中小企業のやる気を削いでしまう可能性がある。<br>• コストや効果を定量的に示すことは難しいため、簡単に実施できる対策は、その容易性が伝わるような記載がなされるとよい。<br>• IoT 製品が有する機能に対して、どのようなリスクが存在し、そのリスクに対してどのような対策が想定されるかが分かりやすくまとまっているとよい。すべてのリスクを網羅することは難しいため、実証事業で明らかになったリスクを示しつつ、推奨される対策を記載する方針でもよいと思う。 |

また、セキュリティ対策に意欲的な中小企業による実際の対策事例を示すことで、それぞれの企業の状況に応じてどのような対策を実施すればよいかについての参考情報を提供するため、今年度の実証

事業に参画した中小企業 5 社にヒアリングを行い、対策のポイントや対策内容、対策に力を入れたことによるメリットについて記載した「IoT 機器等を開発する中小企業の対策事例集」の章をガイドに追加した。対策事例集に掲載した企業と製品種、そしてそれぞれ対策のポイントを表 3.1-2 に示す。

表 3.1-2 対策事例集の概要

| 掲載企業 | 製品種 | 対策のポイント |
|---|---|---|
| 株式会社 SYNCHRO | アプライアンス製品 | • 社内開発のほか、開発パートナーに製品開発を委託している部分もあり、パートナーやエンドユーザと相談しながらセキュリティ対策を実施している。 |
| GROOVE X 株式会社 | ロボット | • 開発リソースが限られているスタートアップ企業であったが、開発当初からセキュリティに対する高い意識をもって対策を進めていた。<br>• セキュリティコンサルタントとともに脅威分析を実施し、ユーザの個人情報の保護とアップデート対応できない機能を最優先に対策を実施した。 |
| ソナス 株式会社 | 無線モジュール・センサ | • スタートアップで技術の商品化に取り組んでおり、社内体制が整備できている段階ではないが、顧客からセキュリティの確保を求められていることもあり、エンジニアの意識やスキルが高く、連携しながら、積極的にセキュリティ対策を実施している。<br>• 社長に直接報告や相談をしやすい環境であり、セキュリティに関して課題があれば、社内でスピード感を持って対応することが可能である。 |
| A 社 | CPU ボード・ゲートウェイ | • 開発部門のセキュリティ意識や技術力が高く、国内外の規格を元にした独自のセキュリティポリシーに基づき、セキュリティ対策の実施を行っている。<br>• 半完成品を扱っているため、ハードウェアセキュリティは自社の責任とする一方、OSS をベースとしたソフトウェアのソースコードと仕様は全て公開し、ソフトウェアに関する対策責任は顧客として、契約で責任範囲を定めている。<br>• 出荷後も顧客と頻繁にコミュニケーションを取り、顧客のリクエストに応じて、セキュリティに関するアドバイスを実施している。<br>• 最新製品ではソフトウェアアップデートを OTA で毎月実施している。 |
| B 社 | モバイルルータ | • 開発メンバーの議論を基に、利便性やコストとのバランスを踏まえ、社長が製品に実装するセキュリティ対策の選定を行っている。<br>• 第三者による検証を活用し、実施したセキュリティ対策に不 |

| 掲載企業 | 製品種 | 対策のポイント |
|---|---|---|
| | | 備がないかを確認している。 |

### 3.1.3 作成した中小企業向けガイドの概要

ガイドの基本的な考え方は以下のとおりである。

- IoT 製品にセキュリティが実装されていることを確認するために、セキュリティ検証を行うことが有効であるものの、出荷前の検証で問題が発見された場合には、製品リリースが遅くなる、改修に新たなコストがかかる、本来の機能を制限してリリースをせざるを得なくなる等、製品の販売に影響が出ることも考えられるほか、必要な機能が実装できないなどセキュリティ自体の確保に支障が出てしまう可能性もあり、設計や開発段階からセキュリティを考慮した取組(セキュリティ・バイ・デザイン)を始めることがとても重要である。(→機器開発のライフサイクルフェーズを通じて必要な対策を整理)
- IoT のセキュリティに関しては国内外に複数のガイドラインや規格等が提示されており、セキュリティ対策に取り組もうとする企業には、何から始めてよいかが分かりにくい場合がある。(→IoT 機器等のセキュリティ対策を行おうとする企業が第一歩として取り組む対策を提示)
- 特に予算や人員が限定される中小企業等においては、対策全てを網羅的に実施することは難しい場合もあると考えられる。企業の経営方針、成長ステージ、人員の状況や体制、予算、製品の特性、顧客との関係等、自社を取り巻く様々な環境を考慮しつつ、優先順位をつけて、まずできるところから対策を進めることが重要である。(→リソースに限りがありながらも、セキュリティ対策を効果的に進める中小企業の事例集を掲載)

主な想定読者は、IoT 機器等を開発する中小企業の経営者、IoT 機器等を開発する中小企業のセキュリティ担当者・開発担当者・品質管理者であるが、これからセキュリティ対策に取り組もうしているIoT 機器等を開発する皆様にご活用いただけるガイドとした。

本ガイドで示した対策の全体像を図 3.1-2 に示す。本ガイドでは、機器開発のライフサイクルフェーズを「方針・体制構築」「設計・開発」「検証」「運用・保守」の 4 つに大別している。「各フェーズで求められる対策」の章に、各ライフサイクルフェーズにおいて、セキュリティ対策に取り組もうとする企業が最初に検討すべき対策を示し、「設計・開発フェーズで検討すべき主な技術的対策」の章に、特に設計・開発の段階において、セキュリティ対策に取り組もうとする企業が最初に検討すべき主な技術的対策について、IoT 機器等の特徴別に示している。また、「IoT 機器等を開発する中小企業の対策事例集」の章に、中小企業による実際の対策事例を示しており、それぞれの企業の状況に応じてどのような対策を実施すればよいかについての参考情報を提供している。


図 3.1-2 本ガイドで示した対策の全体像

## 3.2 検証事業者向け手引きの拡充

### 3.2.1 拡充方針

本事業で作成した 2 つ目の文書である検証事業者向けの手引きについて、今年度実証での検証結果を踏まえ、既存の「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」を拡充した。拡充の方針は図 3.2-1 に示すとおりであり、既存の手引き本編を拡充することに加え、新たな文書である「機器個別のセキュリティ検証プラクティス集」を策定し、手引きの新たな別冊に位置づけた。前者の手引き本編の拡充について、実証結果や検証事業者に対するヒアリングを踏まえ、検証依頼者が中小企業である場合に検証事業者が留意すべき事項を拡充した。後者の「機器個別のセキュリティ検証プラクティス集」について、155 製品に対する検証結果報告書や脆弱性の検出結果を踏まえ、代表的な IoT 機器において適用し得る検証手法、検出された脆弱性の概要、想定される推奨事項、検証に当たって留意すべき事項をプラクティス集としてまとめた。

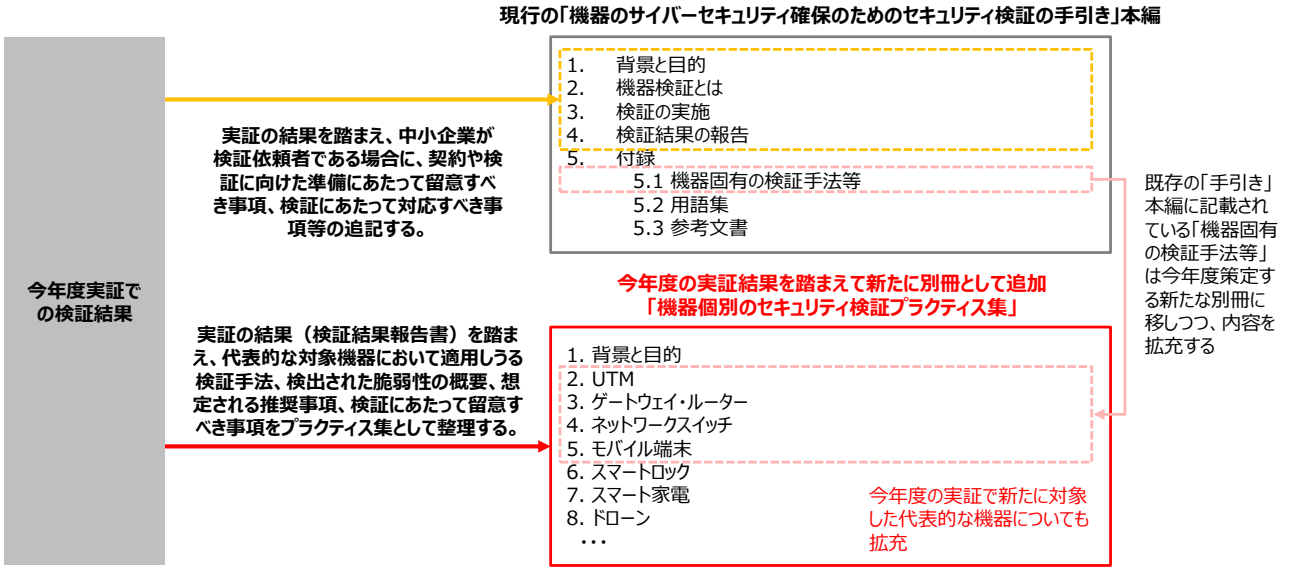



図 3.2-1 検証事業者向け手引きの拡充方針

## 3.2.2 ヒアリング結果

手引き本編の拡充について、検証依頼者が中小企業である場合に検証事業者が留意すべき事項に関して、検証事業者に対するヒアリングを行った。ヒアリングでは主に以下の項目について確認した。

- 検証準備フェーズにおいて検証事業者が留意すべき事項
- 検証実施フェーズにおいて検証事業者が留意すべき事項
- 検証結果報告フェーズにおいて検証事業者が留意すべき事項

主なヒアリング結果は以下に示すとおりであり、検証依頼者が中小企業である場合、検証事業者が検証方針の決定や手続きをリードする必要があるほか、検出された脆弱性に対して想定される影響や対策の必要性・方向性についても検討し、提案する必要性が明らかとなった。

【検証準備フェーズにおいて検証事業者が留意すべき事項】

- 秘密保持管理に向けた手続きなど、検証に向けて必要な手続きを検証事業者から提示する必要がある。
- 依頼内容が定まっていないケースも多い。中小企業の要望を引き出しつつ、機器の特性を踏まえ、どのような検証が求められるかを検証事業者で検討し、提示する必要がある。
- 破壊的な検証に対する認識が大手企業と異なるため、破壊的な検証を実施する場合、原状復帰が難しい可能性があることを事前に合意する必要がある。
- 検証が 100％のセキュリティを保証するものではないことを説明する必要がある。

【検証実施フェーズにおいて検証事業者が留意すべき事項】

- 中小企業の場合、事前に内部で検証を行っているケースは稀であるため、まず自動化ツールを用いた診断を実施し、脆弱性が含まれる箇所のあたりをつけた上で詳細な検証を実施することが必要である。

- 深刻な脆弱性が検出された場合の速報がスルーされるケースもあり、検出された脆弱性は、想定される影響も含めて中小企業に連絡する必要がある。

【検証結果報告フェーズにおいて検証事業者が留意すべき事項】
- 脆弱性の報告だけでなく、対策の必要性や方向性についても、検証事業者が検討し、提案する必要がある。

### 3.2.3 既存の検証事業者向け手引きに関するアンケート調査結果

今年度の実証事業に参画した検証事業者に対して、現状の「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の活用状況・認知度に関するアンケートを実施した。アンケートで得られた回答を表 3.2-1 に示す。

検証事業者における手引きの活用状況について、度合いの差はあるものの、多くの検証事業者において活用されていることが分かった。活用内容について、検証に当たっての参考資料としての活用、検証依頼者との意識合わせに当たっての活用、検証報告書作成時の活用、検証作業の標準化に当たっての活用、社内の人員確保のための説明資料としての活用等が挙げられた。一方で、機器メーカー等の検証依頼者における「手引き」の認知度は極めて低いことが分かった。検証依頼者に対する普及策の案として、業界団体と連携したプロモーションや説明会の開催、産業ごとの基準やセキュリティガイドラインにおける引用、既存制度における活用、アンケート形式での認知度確認・普及等が意見された。

表 3.2-1 現状の手引きの活用状況・認知度に関するアンケート結果

| 項目 | 手引きの活用状況・認知度に関する検証事業者の回答 |
|---|---|
| 検証事業者における「手引き」の活用状況 | • 機器の脆弱性診断にて、検証時の参考資料としている。<br>• ICT 機器や IoT 機器を検証する際、5.1 節 機器固有の検証手法等を参考にすることがある。<br>• 検証依頼者との検証の意識合わせのために活用している。<br>• 検証内容を提案する際の根拠資料の一つとして使用している。<br>• 検証結果報告書は「手引き」に記載の項目を参考に作成している。<br>• 検証担当者の作業標準化に活用している。<br>• 「別冊 3 検証人材の育成に向けた手引き」について、社内にて人材確保と必要体制の説明に活用している。<br>• 今後、自社サービスにおける検証項目として導入できるものがあるか検討する資料として活用したい。 |
| 機器メーカー等の検証依頼者における「手引き」の認知度 | • 検証依頼者における認知度は恐らく低い。外部に委託されているメーカーや初めて検証を実施するメーカーは、「手引き」に記載されているような内容はほとんど理解されていないのが現状である。<br>• 「手引き」を認識している検証依頼者はほとんどいない。 |

| 項目 | 手引きの活用状況・認知度に関する検証事業者の回答 |
|---|---|
| | • 依頼者との相談に当たって、「手引き」自体及びその利用について話題となることはほとんどない。 |
| 機器メーカー等の検証依頼者に対する効果的な「手引き」の普及策 | • 業界団体セミナーでの普及活動が有効。<br>• 業界団体と連携したプロモーション。<br>• 各業界へ「手引き説明会」を開催し、トップダウン的に「手引き」活用の指導を行うことが効果的と考えられる。<br>• セミナー、勉強会等での訴求、業界団体からの告知。<br>• 各業界の規格における引用。(例:車載の ISO 21434、医療の IMDRF ガイダンス 等)<br>• 情報セキュリティサービス審査登録制度等における「手引き」の活用や、制度化済みの他のセキュリティガイドラインにおける手引きの引用が重要。<br>• 本アンケートのように、アンケート形式で認知度を確認しつつ、手引きの普及や活用のテコ入れは有効だと感じる。 |

### 3.2.4 拡充した検証事業者向け手引きの概要

まず、手引き本編の拡充結果概要について記載する。前述のとおり、検証事業者に対するヒアリング結果や実証での検証結果を踏まえ、検証依頼者が中小企業である場合に検証事業者が特に留意すべき事項を既存の手引き本編に反映した。具体的な拡充内容は表 3.2-2 に示すとおりである。

表 3.2-2 手引き本編に対する拡充内容

| 章 | 節 | 拡充内容(検証依頼者が中小企業である場合に、検証事業者が特に留意すべき事項) |
|---|---|---|
| 3. 検証の実施 | 3.1 検証手順<br>3.2 検証に向けた準備<br>3.3 検証結果の策定 | • 検証が 100%のセキュリティを保証するものではないことを中小企業に説明する必要がある。<br>• 具体的な依頼内容や検証の要望が決まっていない場合があるため、中小企業の要望を引き出しつつ、どのような検証が求められるかを検証事業者で検討し、提示する必要がある。<br>• 秘密保持管理に向けた手続きなど、検証に向けて必要な手続きを検証事業者から提示する必要がある。<br>• 破壊的検証を行う場合の留意事項や免責事項を適切に中小企業に伝える必要がある。<br>• 中小企業が理解できるよう、可能な限り平易な用語を用いて検証内容を説明する必要がある。<br>• 事前に中小企業内部で検証を行っているケースは稀であるため、まず自動化ツールを用いた診断を実施し、脆弱性が含まれる箇所 |

| 章 | 節 | 拡充内容（検証依頼者が中小企業である場合に、検証事業者が特に留意すべき事項） |
|---|---|---|
| | | のあたりをつけた上で詳細な検証を実施することが効率的である。<br>• 深刻な脆弱性が検出された場合の速報が中小企業にスルーされないよう、適切な連絡体制を構築する必要がある。併せて、どのような連絡を中小企業と取る必要があるかを事前に伝えておくことが望まれる。<br>• 検出された脆弱性は、想定される影響も含めて中小企業に連絡する必要がある。 |
| 4. 検証結果の報告 | 4.1 検証結果の分析<br>4.2 検証結果の報告 | • 脆弱性の報告だけでなく、対策の必要性や方向性についても、検証事業者が検討し、提案する必要がある。<br>• 報告書及び報告会の説明について、中小企業が理解できるよう、可能な限り平易な用語を用いて説明する必要がある。 |

次に、新たな手引き別冊である「機器個別のセキュリティ検証プラクティス集」の概要について記載する。本プラクティス集では、155 製品に対する検証結果報告書や脆弱性の検出結果を踏まえ、多数の検証結果報告書が存在する機器類型について、実証で検出された深刻度の高い脆弱性の情報を基に、当該脆弱性の検出に至った検証プロセス、脆弱性を悪用された場合に想定される影響、脆弱性に対する推奨事項を整理した。具体的な対象機器類型及び記載内容は図 3.2-に示すとおりである。

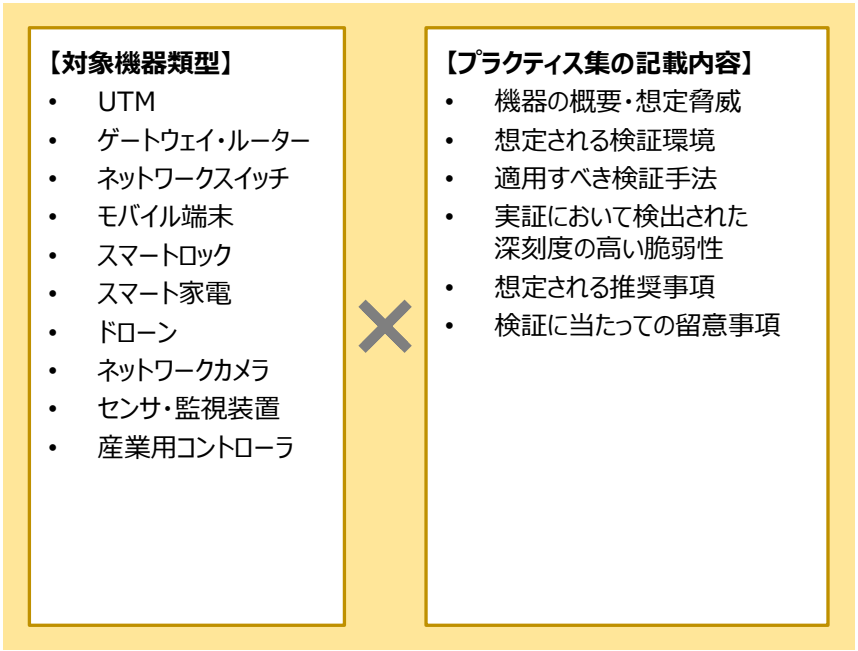



図 3.2-2 「機器個別のセキュリティ検証プラクティス集」の対象機器類型・記載内容

プラクティス集の目次構成は表 3.2-3 に示すとおりであり、2 章以降の機器類型に関する章の節構

成は共通である。「X.3 適用すべき検証手法」[2]では、実証において適用された検証手法をベースに、各機器の検証に当たって適用すべき検証手法や検証に当たって確認すべき範囲を整理しているほか、「X.4 実証において検出された深刻度の高い脆弱性」では、実証で検出された深刻度の高い脆弱性を記載しつつ、当該脆弱性が悪用された場合に想定される影響と脆弱性検出に至った検証プロセスを整理している。そして、「X.5 想定される推奨事項」では、当該脆弱性に対して推奨される対策事項を整理している。

表 3.2-3 「機器個別のセキュリティ検証プラクティス集」の目次構成

| 章 | 節 | 主な記載内容 |
|---|---|---|
| 1. 背景と目的 | 1.1 背景<br>1.2 本別冊の目的<br>1.3 本別冊の対象者・活用方法<br>1.4 本別冊の構成 | • 本別冊(プラクティス集)策定に当たっての背景や目的を記載。<br>• 本別冊で対象とする機器や活用方法を明記する。活用方法については、検証事業者だけでなく、IoT機器を開発する中小企業等において、社内で検証を実施する際の手引きとして活用可能であることを明記。 |
| 2. UTM<br>3. ゲートウェイ・ルータ<br>4. ネットワークスイッチ<br>5. モバイル端末<br>6. スマートロック<br>7. スマート家電<br>8. ドローン<br>9. ネットワークカメラ<br>10. センサ・監視装置<br>11. 産業用コントローラ | X.1 機器の概要・想定脅威 | • 当該機器の概要及び想定されるユースケースを記載。<br>• 当該機器で考慮すべきセキュリティ脅威を記載。 |
| | X.2 想定される検証環境 | • 当該機器の検証に当たって、構築すべき検証環境を記載。 |
| | X.3 適用すべき検証手法 | • 当該機器の検証に当たって、適用すべき検証手法や検証に当たって確認すべき範囲を記載。 |
| | X.4 実証において検出された深刻度の高い脆弱性 | • 今年度の実証を通じて検出された脆弱性のうち、深刻度が高い脆弱性について、その概要や悪用された場合の影響について記載。 |
| | X.5 想定される推奨事項 | • 検出された脆弱性に対して、どのような対策が推奨されるかを記載。 |
| | X.6 検証に当たっての留意事項 | • 当該機器の検証に当たって、検証事業者が留意すべき事項を記載。 |

## 3.3 今後求められる取組

中小企業や関連団体へのヒアリングを通じて、中小企業向けガイドの普及策の具体化を行った結果を表 3.3-1 に示す。今後、この表で示した取り組みを実施し、中小企業向けガイドの普及を推進していくことが求められる。

[2] X は章番号を意味する。

表 3.3-1 中小企業向けガイドの普及策

| 目的 | 連携先 | 普及策 | 具体的な手法、対象 |
|---|---|---|---|
| ガイドの認知向上 | 商工会議所 | セミナー等を通じた経営者向け案内<br>HP、メールマガジンを通じた開発者向け案内 | 可能な限り、IoT 機器の開発企業に案内が届くような媒体を選定する。 |
| | 商工会連合会 | | |
| | 全国中小企業団体中央会 | 各都道府県の中小企業団体の企業担当者による経営者/開発者向け案内 | |
| | 中小機構 | 地域本部の企業支援担当者による経営者/開発者向け案内 | |
| | 業界団体 | 各業界団体の周知媒体、関連会合による開発者向け案内 | 工場セキュリティガイドラインの普及対象等、機器製造社が多く参画する団体を選定する。 |
| | 自治体 | 各自治体の周知媒体、関連会合による中小企業(製造業・IoT 関連事業)経営者/開発者向け案内 | 普及が効果的と考えられる自治体を選定する。 |
| | IPA | 「中小企業の情報セキュリティ対策ガイドライン」での参照<br>メールマガジン、SNS を通じたセキュリティ担当者向け案内 | － |
| | 情報通信関連学会 | HP、メールマガジンを通じた研究者・開発者向け案内 | 例)電子情報通信学会、情報システム学会等 |
| | 各種ニュースサイト | ニュース記事による開発者・セキュリティ担当者向け案内 | 例)日経系(日経ものづくり)、ITmedia 等 |
| ガイドの活用 | SC3 | 各団体・企業が実施している IoT・セキュリティ関連の取組に合わせてセミナー・研修会を実施 | ものづくりが盛んな地域、活動が活発であることが HP 等から確認できる、普及が効果的と考えられる地域・団体を選定する。 |
| | 地域 SECUNITY | 各地域が実施している IoT・セキュリティ関連セミナー・研修会での紹介・活用、セミナー・研修会の実施 | |
| | 地方版 IoT 推進ラボ | | |
| | 業界団体 | 各業界団体が実施している IoT・セキュリティ関連の取組に合わせてセミナー・研修会を実施 | |
| | 自治体 | 各自治体が実施している IoT・セキュリティ関連セミナー・研修会での紹介・活用、セミナー・研修会の実施 | |
| | 展示会 | メーカー主体の活用事例の紹介・座談 | 例)Japan IT Week、 |

| 目的 | 連携先 | 普及策 | 具体的な手法、対象 |
|---|---|---|---|
| | | 会 | スマート系 EXPO 等 |
| | JNSA | HP、メールマガジンを通じた検証事業者・ベンダー向け案内 | － |
| 費用負担軽減 | ものづくり補助金（中企庁/中小機構） | セキュリティ検証を通じて把握された脆弱性に対応するためにものづくり補助金を活用 | ものづくり補助金が脆弱性対処にも活用可能な旨を HP 等に明記する。 |

3.2.3 で示した既存の検証事業者向け手引きに関するアンケート結果を見ると、検証事業者における手引き」認知度は高く、多くの検証事業者で一部活用されている状況である。他方、効果的な検証サービスを提供するため、検証依頼者である機器メーカーに対する普及も必要となる。アンケートで「検証事業者に回答いただいた機器メーカー等の検証依頼者に対する効果的な手引きの普及策」として挙げられた業界団体と連携したプロモーションや説明会の開催、産業ごとの基準やセキュリティガイドラインにおける引用、既存制度における活用、アンケート形式での認知度確認・普及といった施策を行っていくことが求められる。

# 4. ガイドライン等の作成に関する検討会の実施

IoT 機器等を開発する中小企業向けのセキュリティ対策に関するガイドと、中小企業が開発する IoT 機器等に対して検証を実施する検証事業者向けの手引きの 2 つの文書を作成に当たって、有識者による検討会を開催した。

## 4.1 開催概要

有識者検討会は年度内に三回開催し、ガイドや手引きの作成等について議論を行った。各回の議事は表 4.1-1 に示すとおりである。

表 4.1-1 ガイド等の作成に関する有識者検討会の開催概要

| 回・実施日 | 議事 |
|---|---|
| 第 1 回<br>（2022 年 6 月 16 日） | 1. 開会<br>2. 本検討会の背景及び検討内容について<br>3. IoT 機器を開発・販売する中小企業や検証事業者が活用するガイドライン等について<br>4. 討議<br>5. 閉会 |
| 第 2 回<br>（2022 年 11 月 25 日） | 1. 開会<br>2. 構成員からのプレゼンテーション<br>3. IoT 機器を開発・販売する中小企業や検証事業者が活用するガイドライン等について<br>4. 討議<br>5. 閉会 |
| 第 3 回<br>（2023 年 3 月 2 日） | 1. 開会<br>2. IoT 機器を開発・販売する中小企業や検証事業者が活用するガイド等について<br>3. 討議<br>4. 閉会 |

## 4.2 主な議論内容

### （1） 第 1 回有識者検討会

第 1 回の有識者検討会で挙げられた主な意見は表 4.2-1 に示すとおりである。中小企業向けガイドの経営者向けページや各フェーズで求められる対策、中小企業が開発・販売する IoT 機器のセキュリティ対策の向上に関していただいたご意見をもとに、中小企業向けガイドの修正・追記を行った。

表 4.2-1 ガイド等の作成に関する第 1 回有識者検討会で挙げられた主な意見

| カテゴリ | 主な意見 |
|---|---|
| 中小企業向けガイドの経営者向けページについて | • 経営者の方に読んでいただくには、伝えたい内容を資料 1 枚で端的にまとめる必要がある。<br>• セキュリティ対策の実施判断ができる人材がいなければ対策費用が増えてしまうため、経営層に対して人材の育成や配置、活用の必要性を訴えてはどうか。 |
| 中小企業向けガイドの各フェーズで求められる対策について | • 「方針・体制構築フェーズで求められる対策」では ISO/IEC 27001 の記載項目が多く、中小企業にはハードルが高いと思われる。<br>• 他社の動向を把握できるような形でガイドラインを作成すれば、中小企業により活用いただけるようになると思われる。<br>• 使用目的や場面に合わせた要求性能を定義した上で分類ができれば、より活用しやすいガイドラインになる。<br>• ガイドラインの項目を全て実施することは中小企業には難しいため、その対策を削るとどのようなリスクが生じるのか、その対策を行うと何を守れるのかが明記されていると、経営判断が行いやすくなる。<br>• 廃棄や転売されたときにユーザの情報が第三者にわたることのないよう、適切に情報を削除する機能を設けることについてガイドラインに明記するとよい。<br>• 製品のエンドオブライフについて検討する必要がある。一社だけでエンドオブライフの取組を行うと、その企業だけが損をしてしまう可能性がある。<br>• セキュリティ対策について安心して相談できる組織や企業を増やしていくことが中小企業の支援となるため、外部の相談先について記載いただきたい。 |
| 中小企業が開発・販売する IoT 機器のセキュリティ対策の向上について | • 努力してセキュリティ対策を実施しているメーカーの製品が選ばれるようになるよう検討を進めていただきたい。<br>• 業界の中に、他社との連携や情報共有を行えるようなコミュニティがあれば、セキュリティ対策を実行しやすくなると思われる。<br>• 本ガイドラインに沿って開発した製品を仕入れていただくためにはどうすればよいか検討する必要がある。例えば、本ガイドラインに沿って開発した製品を企業が調達する際に活用できるチェック項目を設けるといった施策をラベリング制度が導入されるまでに実施することが考えられる。<br>• 中小企業だからセキュリティ対策は緩くてもよいということは考えられない。セキュリティ性能についてユーザに伝え、それにより製品を選んで購入していただくというスキームが必要である。 |

### （2）第 2 回有識者検討会

第 2 回の有識者検討会で挙げられた主な意見は表 4.2-2 に示すとおりである。中小企業向けガイドの位置づけや経営者向けページ、各フェーズで求められる対策や中小企業の対策事例に関していただいたご意見をもとに、中小企業向けガイドの修正・追記を行った。

表 4.2-2 ガイド等の作成に関する第 2 回有識者検討会で挙げられた主な意見

| カテゴリ | 主な意見 |
|---|---|
| 中小企業向けガイドの位置づけについて | • 本書は、「ガイド」というよりも「入門書」に相当すると感じた。「入門書」の位置づけであることをうまくアピールできるとよい。<br>• 対象を中小企業だけに絞るとガイドの主張が見えにくいと感じた。 |
| 中小企業向けガイドの経営者向けページについて | • 経営者が最低限知っておくべき内容として当たり前の内容は記載しつつ、今回のガイド独自の内容を追記すべきである。<br>• 開発者自身に自分事になってもらうことの必要性が記載されているとよい。 |
| 中小企業向けガイドの各フェーズで求められる対策について | • BtoB の場合、納入先から仕様について要求される場合があり、中小企業側で対応できる領域が限定的となる場合がある。中小企業向けガイドでも、BtoB と BtoC とで考え方の違いが存在することを記載できるとよい。<br>• 機器の製造を外部に委託したりモジュールを買い入れたりするケースもあるため、その管理の部分で考慮すべき事項について追記することが望ましい。<br>• 買入品の扱いについて、納入時に脆弱性が発見された際に、開発側とベンダー側のどちらの責任で、どのような対応を実施する必要があるかという点を契約項目に含めるべきである。<br>• IoT 機器が含む OSS をリスト化して脆弱性情報を監視することは求めるべきではないか。<br>• 利用しているライブラリやモジュールの情報は適切に管理すべきである。<br>• 脆弱性情報に関する外部とのコミュニケーションについて複数のケースが想定されるため、追記することが望まれる。 |
| 中小企業の対策事例について | • 同業他社の対策事例やケーススタディが含まれていると参考になると思われる。<br>• 各社がローンチ時点でフォーカスしていたポイントやどの程度の対策を行っていたかについてガイドに記載されているとよい。 |

### （3）第 3 回有識者検討会

第 3 回の有識者検討会で挙げられた主な意見は表 4.2-3 に示すとおりである。中小企業向けガイドのサブタイトルや各フェーズで求められる対策、対策事例集に関していただいたご意見をもとに、中小企業向けガイドの修正・追記を行った。また、中小企業向けガイドの普及に関するご意見をもとに、普及策の見直しを行った。加えて、ガイド・手引きの更新や検出された脆弱性の評価、脆弱性検証等の普及や適合性評価についてもご意見をいただいた。

表 4.2-3 ガイド等の作成に関する第 3 回有識者検討会で挙げられた主な意見

| カテゴリ | 主な意見 |
|---|---|
| 中小企業向けガイドのサブタイトルについて | • 自分ごとに感じていただくようなサブタイトルを検討いただけるとよい。 |

| カテゴリ | 主な意見 |
| --- | --- |
| 中小企業向けガイドの各フェーズで求められる対策について | • 自社の製品で脆弱性が検出された際のトリアージの観点を明記した方がよいのではないか。<br>• 脆弱性が存在した場合に製品リスクに与える影響を適切に記載する必要がある。<br>• 自分ごととしてセキュリティに取り組むことで、自社でセキュリティに関する判断ができるようになる、ということはどこかに言及してもよいと感じた。<br>• チームや組織としてセキュリティ対策に関する風土を高める必要がある。今回のガイドにおいて経営者向けの内容があることはよいと思うが、開発者に対しても、自分ごととして捉えていただけるような記載があるとよい。<br>• 製品の用途や利用環境によって、物理的に及ぼす影響の度合いが異なる。用途ごとに対策を記載することは難しいか。<br>• 脆弱性への対応については、設計段階から製品の標準利用期間を考慮する必要がある。部品としての IoT 機器を想定したとき、利用期間を想定してハードウェアのスペックを見積もる必要がある。もし見積もりができない場合、その他の方法で対応する必要があり、これらを設計段階で検討することの必要性が示されるとよい。特定の期間でサポートが切れる場合、その事実をメーカーが適切に宣言する必要がある。<br>• Log4j の脆弱性にも関係するが、依存関係のあるコンポーネントの管理も重要となる。このような脆弱性は一般的なスキャンでは検出されない。ガイドの中でも、依存関係のあるコンポーネントの管理に関して言及があるとよい。<br>• 中小企業が SBOM に対応するのはまだ難しいと考えられるが、ソフトウェア管理手法として SBOM が注目を集めていることは言及があってもよいと思う。<br>• 中小企業の IoT デバイスについて、サプライチェーンの中でどういう位置づけにあるのかを書いてほしいという意見が挙がっている。ただし、使う用途によってセキュリティレベルも異なるので、一律に書くことは難しい。 |
| 中小企業向けガイドの対策事例集について | • 検討会資料に記載されている検証手法の金額は公になるものではないとのことだが、この方針には同意する。価格だけが独り歩きして、業界標準として扱われることは避けるべきである。一方で、中小企業が検証を依頼するに当たって、検証にかかる費用の相場観は記載できるとよい。<br>• モデル機器ごとの相場が記載されているとよいかもしれない。 |
| 中小企業向けガイドの普及について | • 普及の観点で、脆弱性やセキュリティに関するニュースに紐づく形で今回のガイドを展開できるような手段があれば、普及促進に進むのではないか。<br>• セキュリティ対策や脆弱性診断に活用できる補助金を中小企業に訴求し、その取組と合わせてガイドの普及を行う方針がよい。 |
| ガイドや手引きの更新について | • 数年後にはセキュリティの状況が大きく異なるため、今回作成する文書について更新のスキームを検討いただきたい。 |

| カテゴリ | 主な意見 |
| --- | --- |
| 検出された脆弱性の評価について | • 実証で検出された脆弱性の評価に関して、CVSS に基づき IoT 機器のリスクを評価することは厳しいのではないか。CVSS スコアの扱い方については、今後検討する必要がある。また、脆弱性件数のみが独り歩きすることは避けるべきである。<br>• 脆弱性の有無だけではなく、攻撃における脆弱性の悪用可能性が重要となる。<br>• ソフトウェア・バージョンのみでの評価では誤検出が発生する可能性がある。また、攻撃者の視点では、脆弱性の影響を受けるコンポーネントが含まれている場合、機能を利用していない場合でも悪用できる可能性があることに留意が必要である。<br>• 脆弱性の評価に関して、CVSS では基本評価基準だけでなく環境評価基準の考え方もある。将来的には環境評価基準も考慮する必要がある。 |
| 脆弱性検証等の普及について | • IoT 機器に対する脆弱性検証は、継続的に実施することが必要である。そのためには、中小企業の動機付けと、コストに厳しい中小企業が検証と対策に取り組める（制度も含めた）環境作りが必要であり、今回のような取組を継続し、普及していくことが重要である。今回の検証を受けて対策をされた機器があれば、再検証することも有効である。また、製品の検証だけでなく、設計段階からの取り組みも必要だという観点も重要であるため、「ものづくり補助金」の活用に関して、中小企業にご案内するなど普及を促進していくことが必要だと思われる。<br>• ガイドの普及に関して、METI の入札でガイドへの言及があることが最も効果があると思われる。 |
| 適合性評価について | • 重要インフラであればラベルが付与された製品のみ導入できるなど、利用環境とセキュリティレベルとのバランスを考えていく必要がある。また、脆弱性の有無だけではなく、脆弱性に対する過去の対応といった来歴も評価できるとよいのではないか。 |

# 5. IoT 製品に対するセキュリティ適合性評価制度の構築に係る検討

IoT 製品の安全性を確保するとともに、メーカーのセキュリティ対策の取組を適切に評価し、多少高価であっても適切なセキュリティ対策を講じている IoT 製品が積極的に購入されるような社会の仕組みを構築するため、IoT 製品のセキュリティに関する適合性評価制度の構築に向けた検討を行った。

## 5.1 検討背景

### 5.1.1 IoT 製品に対するセキュリティ脅威の現状

近年、インターネットに接続される IoT 製品の数は急速に増加している。総務省の令和 4 年度情報通信白書[3]によれば、世界の IoT 製品数について、2021 年には 292 億台程度であるが、2023 年には 323 億台、2023 年には 358 億台、2024 年には 400 億台程度と、今後も増加の一途を辿ることが予想されている。

IoT 製品数の急激な増加に伴い、IoT 製品の脆弱性を狙ったサイバー脅威も増加傾向にある。Kaspersky の調査[4]によれば、2021 年上半期だけで、2020 年の 2 倍以上の IoT 製品に対するサイバー攻撃が発生した。また、IBM Security X-Force の調査[5]によれば、2019 年第 3 四半期から 2020 年第 4 四半期にかけて、IoT 製品を対象としたマルウェアの活動が 3,000%増加した。同調査によれば、2020 年から 2021 年にかけて脆弱性全体の増加率は 0.4%の増加に留まった一方で、IoT 製品関連の脆弱性の件数は 16%も増加した。加えて、Checkpoint の研究者[6]は、IoT 製品に対するサイバー攻撃は日々増加するだけでなく、洗練かつ広範で破壊的になりつつあることを指摘している。

IoT 製品に対するセキュリティ脅威の高まりを受け、日本を含む各国は IoT 製品の安全性確保に向けた取組に力を入れている。

### 5.1.2 諸外国政府における IoT 製品の安全性確保に向けた取組

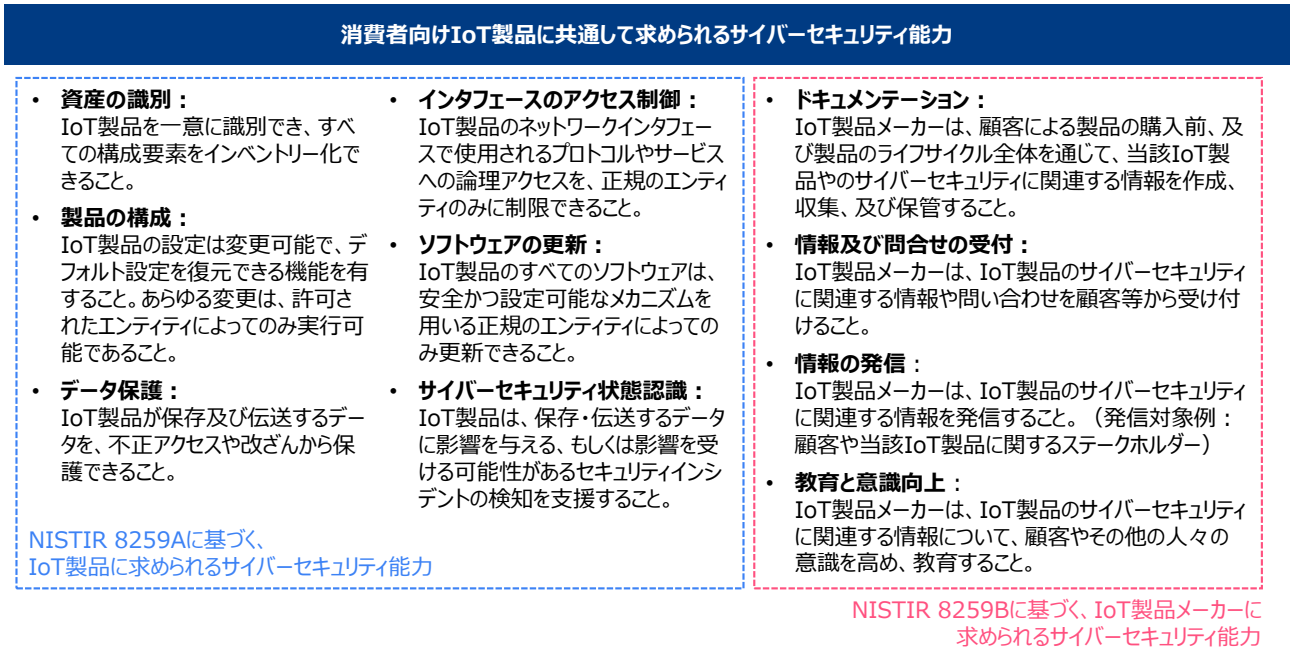
#### （1） 米国における取組

米国政府における IoT 製品の安全性確保に向けた近年の代表的な取組として、2020 年に成立した「IoT Cybersecurity Improvement Act of 2020」[7]が挙げられる。この法律では、NIST に対し

---

[3] 総務省、令和 4 年度情報通信白書
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nb000000.html
[4] Threatpost, IoT Attacks Skyrocket, Doubling in 6 Months
https://threatpost.com/iot-attacks-doubling/169224/
[5] IBM Security X-Force, X-Force 脅威インテリジェンス・インデックス 2022
https://www.ibm.com/security/jp-ja/data-breach/threat-intelligence/,
https://www.ibm.com/downloads/cas/QA59ZP3P
[6] Checkpoint, Protecting IoT Devices from Within – Why IoT Devices Need A Different Security Approach? https://blog.checkpoint.com/2022/07/25/protecting-iot-devices-from-within-why-iot-devices-need-a-different-security-approach/
[7] IoT Cybersecurity Improvement Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/1668

て、政府機関が所有・管理する情報システムに接続された IoT 製品を適切に使用・管理するための標準やガイドラインの作成が指示された。また、本法律の制定を受け、2021 年 11 月、NIST より、連邦政府が IoT 製品を調達する際のガイドラインである NIST SP 800-213 及び NIST SP 800-213A が公表された。これらのガイドラインでは、具体的なセキュリティ対策内容について、NISTIR 8259 シリーズが引用されている。NISTIR 8259 シリーズに関連して、2022 年 9 月には、消費者向け IoT 製品に共通して求められるサイバーセキュリティ能力を示した NISTIR 8425 を公開した。具体的なサイバーセキュリティ能力について、図 5.1-1 に示すとおり、NISTIR 8259 の基準に基づき、IoT 製品自体及び IoT 製品メーカーに求められる 10 個のサイバーセキュリティ能力によって構成される。

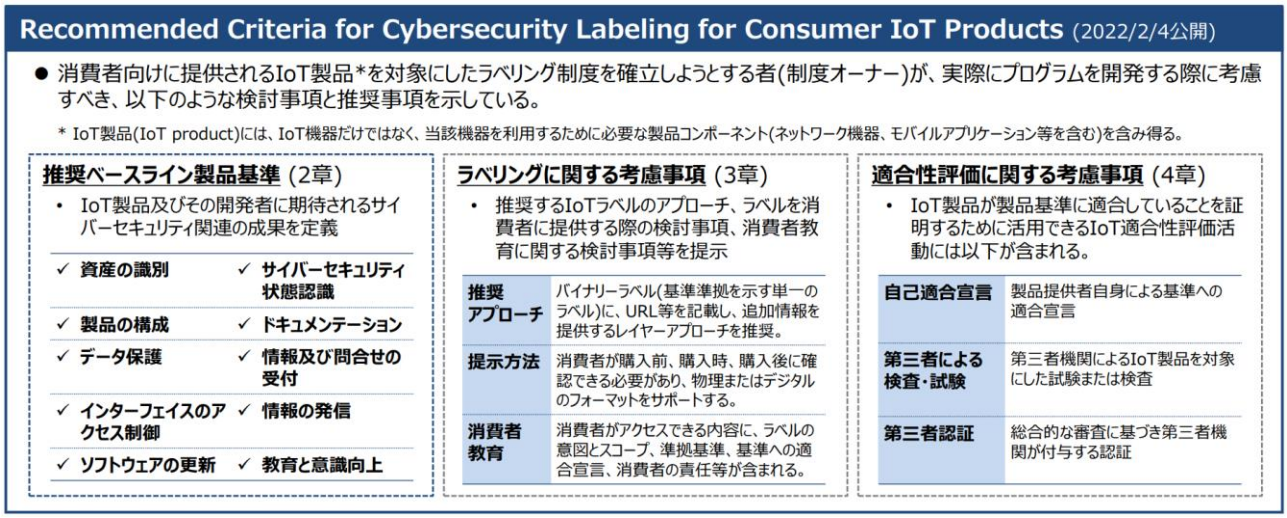



出典）NIST、NISTIR 8425 Profile of the IoT Core Baseline for Consumer IoT Products に基づき三菱総合研究所作成

図 5.1-1 NISTIR 8425 における消費者向け IoT 製品に共通して求められるサイバーセキュリティ能力

また、2021 年に署名されたサイバーセキュリティを強化する大統領令（Executive Order on Improving the Nation's Cybersecurity）[8]に基づく動向も挙げられる。この大統領令では、NIST に対して、消費者向け IoT 製品に対するセキュリティラベリング制度の検討を指示した。2022 年 2 月、NIST は消費者向け IoT 製品に対するラベリング制度に関する考慮事項を示した文書を発表し、ラベリングのためのベースライン基準として、NISTIR 8259 に基づく基準を推奨した（図 5.1-2）。ただし、具体的な制度オーナー、評価方法、ラベルの種類等は定められておらず、今後の検討事項に位置づけられている。

[8] White House, Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/




出典）経済産業省、第 6 回『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース 資料 3[9]

図 5.1-2 2022 年 2 月に NIST が発表した IoT 製品のラベリング制度に関する考慮事項の文書概要

大統領令に関連して、2022 年 10 月、ホワイトハウスは、消費者向け IoT 製品のラベリング制度の構築に向け、企業、団体及び政府機関のステークホルダー間で議論を実施した。ラベル付与の方法について、米国政府の基準に基づき、審査・承認された機関によってテストする方針を示しつつ、まずルータ及びホームカメラ[10]から着手して、2023 年春の制度展開を目指すと発表した。

そのほか、州の取組として、カリフォルニア州（SB-327：Information privacy: connected devices）やオレゴン州（HB-2395：Oregon Cybersecurity Bill）では IoT 製品に対するセキュリティ対策が州法に基づき義務化されている。それぞれの州法では、インターネットに接続するコネクテッドデバイスに対するセキュリティ強化を目的としており、それぞれの州で IoT 製品を販売するメーカーに対し、パスワードの管理等を含む合理的なセキュリティ機能を具備することを求めている。対象となる IoT 製品について、インターネットに直接的・間接的に接続される機器が対象となるが、他の法令やガイダンスに基づくセキュリティ要件の対象となっている製品（産業用 IoT 製品、PC、サーバ、モバイル端末等の IT 製品等）は対象外である。

## （2）英国における取組

英国政府における IoT 製品の安全性確保に向けた近年の代表的な取組として、2018 年に DCMS（デジタル・文化・メディア・スポーツ省）が発表した消費者向け IoT 製品のセキュリティに関する 13 の行動規範である「Code of Practice for Consumer IoT Security」[11]が挙げられる。この行動規範では、消費者向け IoT 製品の設計段階で安全性が確保されること、また、利用者がデジタルの世界を安心して楽しめるようにガイドラインを設けることで、IoT 製品の開発、製造、販売に携わる利害関係者を支

9 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/006.html

10 この 2 機器の選定理由として、最も一般的かつリスクが高い機器であることを挙げている。

11 DCMS, Code of Practice for Consumer IoT Security https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

援することを目的としている。対象製品について、インターネットやホームネットワーク（両方又はその一方）と関連サービスに接続する消費者向け IoT 製品を対象としている。英国 DCMS は本行動規範を EU 全体に普及させるべく、技術仕様の国際標準化を ETSI に提案した。ETSI はこの提案に基づき、EU 加盟各国のステークホルダーによる討議を実施し、2019 年 2 月に TS（技術仕様）である ETSI TS 103 645 を公表、2019 年 11 月には、EN 303 645 として欧州規格化された。なお、ETSI EN 303 645 はフィンランド、ドイツ、シンガポールのラベリング制度のベースとなっているほか、後述する PSTI 法のベースにもなっている。

また、消費者向け IoT 製品に対してセキュリティ対策の義務化を求める「Product Security and Telecommunications Infrastructure Act（PSTI 法）」[12]が 2022 年 12 月に成立した。この法律の文面には明確なセキュリティ要件や経過措置の期間などは明記されておらず、具体化については担当国務大臣に委ねられている。法案検討段階では、具体的な対策として、デフォルトパスワードの禁止、脆弱性開示ポリシーの開示、セキュリティアップデートを受ける期間に関する情報の開示の 3 点が含まれており、これらの対策実施に関して、第三者評価による適合性評価が必要となる見込みである。なお、法律には、これらの対策に遵守しない企業に対する罰金に関する条項も含まれており、最高 1,000 万ポンド又は当該企業の全世界売上高の 4%以内の罰金が科せられる内容となっている。また、対象となる企業について、IoT 製品のメーカーだけでなく、輸入業者や販売業者も含まれる。

### （3）EU における取組

EU 全体の IoT 製品の安全性確保に向けた近年の代表的な取組として、2019 年に規則（EU）2019/881「Cybersecurity Act」[13]が施行され、IoT 製品を含む製品の認証スキームである EUCC（Common Criteria based European Candidate Cybersecurity Certification Scheme）が検討されている。EUCC はサイバーセキュリティ法に基づく任意の認証制度で、その枠組みも同法に定められており、既存の CC（Common Criteria）のスキームの後継として機能させることを目的としている。2021 年 5 月には、EUCC のスキーム候補に関する報告書（Ver 1.1.1）を公表し、ISO/IEC 15408 と ISO/IEC 18045 に基づいて、ICT 製品のサイバーセキュリティの認証を検討していることを発表した。

また、2022 年 1 月、欧州委員会は、Radio Equipment Directive（RED：欧州無線機器指令）のサイバーセキュリティ関連条項の施行に関する委任規則（EU） 2022/30[14] を発行し、EU 市場に投入される無線機器に対してセキュリティの強化を求めた。具体的な規則は 2024 年 8 月 1 日より義務化となる予定であり、対象機器について、直接・間接問わずインターネットに接続される無線機器が対象となる。求められる対策として、許容できないサービスの低下を引き起こさないこと、個人データ及びプライバシーを保護するための手段を組み込んでいること、不正行為から保護するための一定の機能をサポートすることの 3 点が求められているが、具体的な規格要件は 2023 年 10 月までに準備される予定である。

---

[12] Product Security and Telecommunications Infrastructure Act 2022 https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

[13] Regulation (EU) 2019/881: Cybersecurity Act https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG

[14] Commission Delegated Regulation (EU) 2022/30 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.007.01.0006.01.ENG

加えて、2022 年 9 月、欧州委員会は、EU 市場に投入されるデジタル製品のセキュリティ対応を義務づける「EU サイバーレジリエンス法（CRA：Cyber Resilience Act）」[15]の草案を発表した。サイバーレジリエンス法と他の EU 法令との関係性は図 5.1-3 に示すとおりである。サイバーレジリエンス法は、2022 年 5 月に欧州議会・欧州理事会が改訂に合意し、2023 年 1 月に発効された NIS2 指令（Network and Information Security 2 Directive）を補間する目的で策定された。サイバーレジリエンス法は、前述した RED の対策要件を包含する位置づけであるため、サイバーレジリエンス法が施行された後、RED のセキュリティ関連要件は廃止となる。また、サイバーレジリエンス法と EUCC との関係について、EUCC に基づく適合性証明書をサイバーレジリエンス法で求められる適合性証明に用いることが可能である。対象について、ICT サービスやプロセスも対象としている EUCC の方が対象範囲は広いものの、製品自体の定義に大きな差異はない。

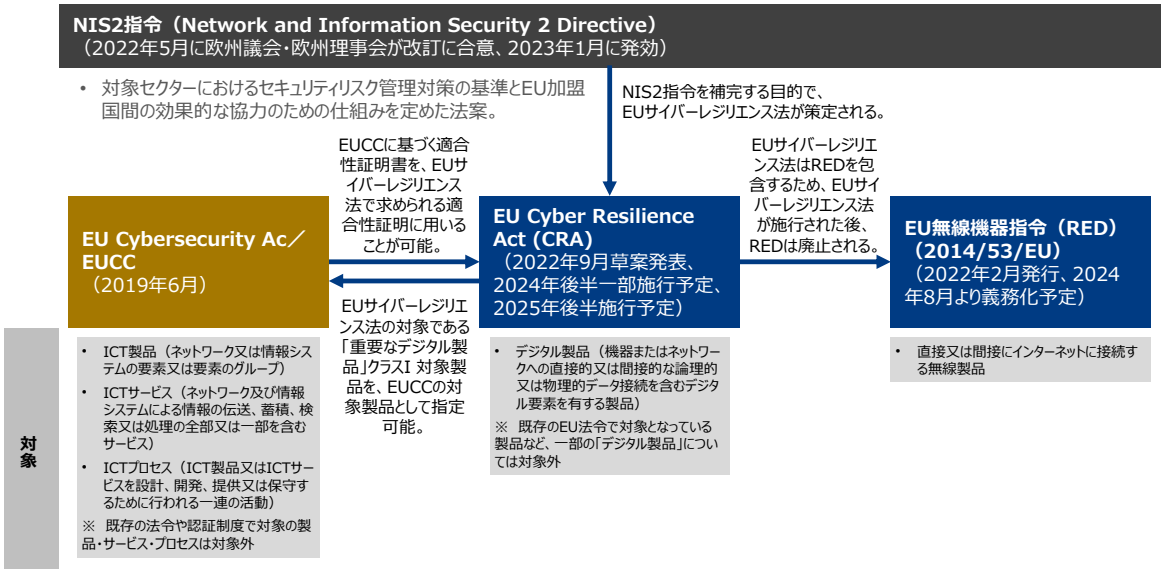



図 5.1-3 サイバーレジリエンス法と他の EU 法令との関係性

サイバーレジリエンス法の対象となる製品について、ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆる「デジタル製品」が対象となる。ただし、既存の規則で対象となる製品は対象外であり、医療機器・体外診療用医療機器、自動車、航空機関連のデジタル製品、SaaS 等のソフトウェアサービス、国家安全保障又は軍事目的にのみ開発されたデジタル製品及び機密情報を処理するために特別に設計された製品は対象外である。対象となる「デジタル製品」のうち、重要な「デジタル製品」のうちリスクが低い製品をクラスⅠ、リスクが高い製品をクラスⅡとして詳細に定義（図 5.1-4 参照）しており、クラスに応じて、選択できる適合性証明の方法が異なる。適合性証明のスキームとして、EU 適合宣言（CE マーク）のスキームを採用している。

これらの対象製品に求められる対策として、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、生産することのほか、悪用可能な既知の脆弱性がない状態とすること、製品の SBOM（ソフトウェア部品表）を作成すること等、多岐にわたる対策が求められる。英国の PSTI 法と同様に罰則が規定されており、要件に違反した場合には、罰金として 1,500 万ユーロ又は全世界売上高

[15] European Commission, Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

の 2.5%のいずれか高い方が科される可能性がある。本法案では、法制化された後の経過措置として、24 ヶ月の猶予期間が設定されているが、製造業者における脆弱性とインシデントの報告に関しては、12 ヶ月のみの猶予期間が設定されている。

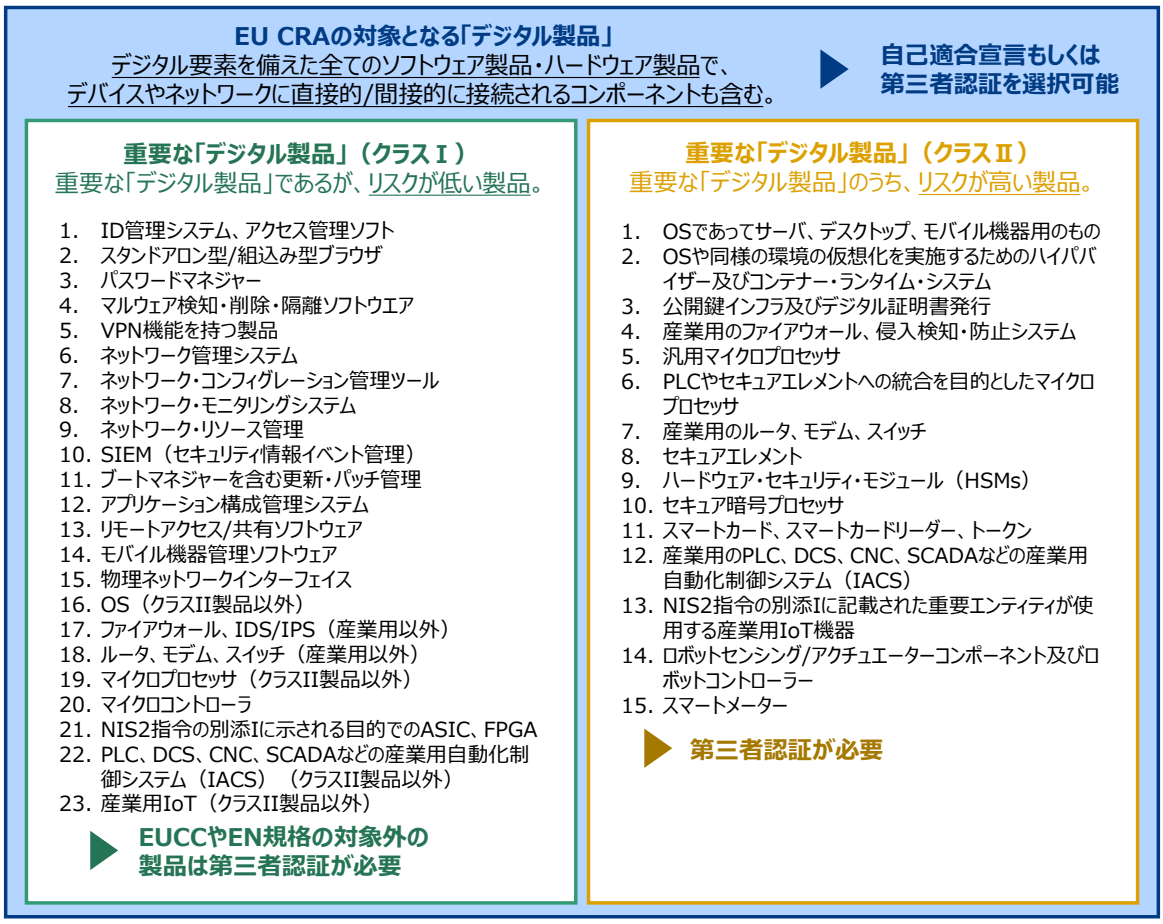



図 5.1-4 サイバーレジリエンス法の対象製品のうちクラスⅠ・クラスⅡに該当する製品

## （4）その他主要国における取組

その他諸外国政府における IoT 製品の安全性確保に向けた近年の代表的な取組として、ドイツ、シンガポール、フィンランドでは、消費者向け IoT 製品に対するセキュリティラベリング制度が既に開始しているほか、オーストラリアでも同様のラベリング制度の構築に向けた検討がなされている。

ドイツの BSI（連邦情報セキュリティ庁）の任意のラベリング制度（IT-Sicherheitskennzeichen）[16]は 2021 年 12 月から開始している。対象製品について、現状ではブロードバンドルータ、電子メールサービス、スマートテレビ、スマートスピーカー等の一部の消費者向け IoT 製品のみを対象としている。ただし、今後対象製品を拡大する方針を示している。ラベル付与のためには、ETSI EN 303 645 の要件に加え、BSI 及び ETSI が作成した各製品分野のセキュリティ要件を満たしていることを自己確認

[16] BSI, IT-Sicherheitskennzeichen https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html

し、確認結果を BSI に承認されることが必要となる。2023 年 2 月時点で 37 製品・サービスがラベルを取得している。

シンガポールの CSA（サイバーセキュリティ庁）が運用するラベリング制度（Cybersecurity Labelling Scheme: CLS）[17]は、すべての消費者向け IoT 製品を対象とした任意のラベリング制度であり、2020 年 10 月から制度が開始している。付与されるラベルは 4 段階に分かれ、レベル 1・2 は開発者の自己適合宣言で取得可能、レベル 3・4 では第三者機関による検証が必要となる。ラベル付与のためには ETSI EN 303 645 の要件に加え、レベル 3 では、第三者機関によるバイナリ解析、レベル 4 では機器に対するペネトレーションテストにクリアする必要がある。2023 年 2 月時点で 233 製品がラベルを取得している。なお、本制度はドイツのラベリング制度やフィンランドのラベリング制度との相互運用を実施している。また、本制度の要件は ISO/IEC 27404 として、国際標準化に向けた提案がなされている。

フィンランドの TRAFICOM（運輸通信庁）が運用するラベリング制度（Finnish Cybersecurity Label）[18]は、すべての消費者向け IoT 製品を対象とした任意のラベリング制度であり、2020 年 1 月から制度が開始している。ラベル付与のためには、ETSI EN 303 645 をベースに作成された情報セキュリティ要件を満たしていることを、認定を受けたセキュリティ機関によって評価されることが必要となる。2023 年 2 月時点で 25 製品がラベルを取得している。

オーストラリアでも内務省を中心に、インターネットやホームネットワークに接続される前提で開発されたあらゆる消費者向け IoT 製品を対象としたセキュリティラベリング制度の検討が進められている[19]。ラベル付与のための基準として、ETSI EN 303 645 を採用する方針が示されている。

### （5）各国の取組比較

前述のとおり、米国やオーストラリアで IoT 製品のセキュリティラベリング制度構築に向けた検討がなされているほか、ドイツ、シンガポール、フィンランドでは既に制度が構築され、運用されている。これらのラベリング制度のオーナー、ラベル取得にかかる費用、基準、取得製品数を比較すると、以下のとおり整理される。

[17] CSA, Cybersecurity Labelling Scheme https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls

[18] TRAFICOM, Finnish Cybersecurity Label https://tietoturvamerkki.fi/en/cybersecurity-label

[19] Department of Home Affairs, Strengthening Australia' s cyber security regulations and incentives https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives

表 5.1-1 各国ラベリング制度の概要[20]

| 国 | 制度名 | 制度分類 | 制度オーナー | 認証取得・ラベル取得に要する費用 | 基準 | 製品数※1 |
|---|---|---|---|---|---|---|
| 米国、英国、日本など※2 | Common Criteria | 認証 | 各国セキュリティ関係機関 | EAL2で1,000万～2,000万円、EAL3で1,600万～2,700万円、EAL4で4,000万～1億円程度。 | ISO/IEC 15408 | 1,652 |
| 米国、日本など | Component Security Assurance (CSA) | 認証 | ISASecure | 約1,000万円 | IEC 62443-4-1, IEC 62443-4-2 | 60 |
| | Cybersecurity Labeling for Consumer IoT Product | ラベリング | 未定 | - | NISTIR 8425に基づく基準の予定 | – |
| 相互運用を実施 | IT-Sicherheitskennzeichen (IT Security Label) | ラベリング | BSI | 約1万円～50万円 | ETSI EN 303 645やBSIの技術ガイドラインに基づく基準 | 37 |
| | Labelling for Smart Devices | ラベリング | 未定 | - | ETSI EN 303 645の予定 | – |
| | Cybersecurity Labelling Scheme (CLS) | ラベリング | CSA | 約5,000円～35万円＋検証費用 | ETSI EN 303 645やIMDAガイドラインに基づく基準 | 233 |
| | Finnish Cybersecurity Label | ラベリング | TRAFICOM | 約10万円＋検証費用 | ETSI EN 303 645に基づく基準 | 25 |

※1: 2023年2月時点。
※2: CCRAにより、認証国17カ国でCC認証を受けた製品は、CCRC加盟国において、CC認証製品として相互に承認される。

出典）各国関連制度に関する公開情報に基づき三菱総合研究所作成

この表から分かるとおり、既存のセキュリティ認証制度である CC（Common Criteria）や CSA（Component Security Assurance）と比較して、ラベル取得に要する費用が安いことが分かる。また、用いられている基準について、多くは ETSI EN 303 645 をベースとしているが、米国の制度のみ NISTIR 8425 に基づく基準となっている。

ラベル取得製品数の比較について、シンガポールの制度の取得実績が 233 製品と多い。この要因として、審査費用が安いことがまず挙げられる。シンガポールの CLS の制度の審査費用について、レベル 1 で$53、レベル 2 で$418、レベル 3 で$1,080、レベル 4 で$3,810 であり[21]、他の制度と比較して廉価あることが挙げられる。また、制度の黎明期においてラベル取得製品を増加させる目的で、制度開始後 1 年間の 2021 年 10 月まで申請料を免除する取組も実施しており、この要因もあり製品数が増加したと考えられる。

ラベリング制度は任意の制度であるが、上述のとおり、法規制による対策義務が存在する国や地域も存在する。これらの概要は以下のとおり整理される。

表 5.1-2 各国法規制の概要[22]

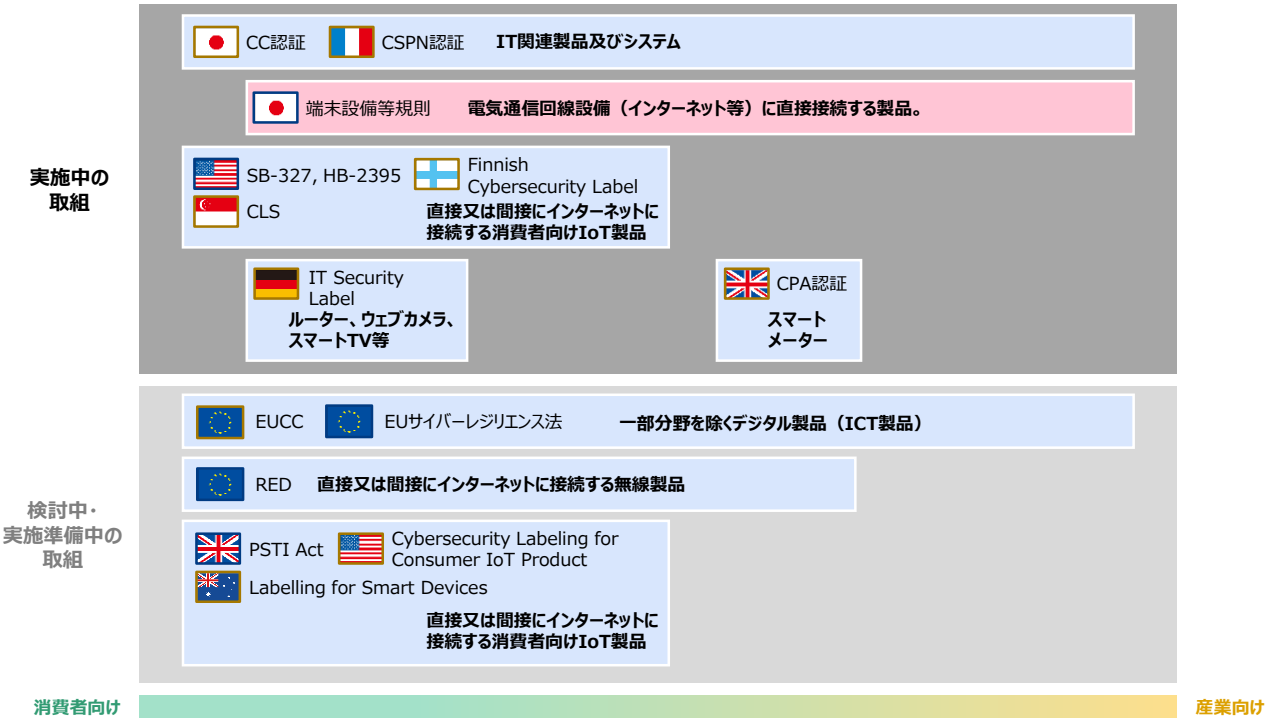
| 国 | 法規制名称 | 所管組織 | 対象製品 |
|---|---|---|---|
| | 端末設備等規則（省令）（第34条の10） | 総務省 | 電気通信事業者のネットワーク（インターネット等）に直接接続する製品。ホームネットワークのみに繋がるスマートホーム機器やPC、モバイル端末等は対象外。 |
| | SB-327 Information privacy: connected devices（カリフォルニア州） | カリフォルニア州 | 直接又は間接にインターネットに接続することができ、かつ、IPアドレス又はBluetoothアドレスを割当てられた製品。ただし、他法令やガイダンスに基づくセキュリティ要件の対象となっている製品（産業用IoT製品、PC、サーバー、モバイル端末等のIT製品等）は対象外。 |
| | HB-2395 (2019) Oregon Cybersecurity Bill（オレゴン州） | オレゴン州 | 直接又は間接にインターネットに接続することができ、個人又は家庭での目的で使用され、他の機器に短距離無線接続する目的でIPアドレス又は接続機器を識別するその他のアドレスが割当てられている製品。ただし、他の法令やガイダンスに基づくセキュリティ要件の対象となっている製品（産業用IoT製品、PC、サーバー、モバイル端末等のIT製品等）は対象外。 |
| | EUサイバーレジリエンス法【2025年後半より施行予定】 | 欧州委員会 | ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品。ただし、既存の規則で対象となる製品は対象外。 |
| | EU無線機器指令（RED）【2024年8月より義務化】 | 欧州委員会 | 直接又は間接にインターネットに接続する無線製品。 |
| | Product Security and Telecommunications Infrastructure (PSTI) Act | DCMS | インターネット接続可能な製品、及びIPを利用しインターネット接続可能な製品に接続できる製品。 |

[20] 灰色塗りは、現在検討中の制度を意味する。
[21] すべてシンガポールドル。また、レベル 3・4 では、第三者機関（CCTL）に対する検証費用も別途必要となる。
[22] 灰色塗りは、現在検討中の制度を意味する。

出典）各国関連制度に関する公開情報に基づき三菱総合研究所作成

対象製品について、国内の端末設備等規則では、インターネット等に直接接続する製品のみが対象となっているが、多くの国・地域の法規制では、接続方式に限らず、インターネットに接続される製品が対象となっている。ただし、既存規制で対象となる製品などは対象外となっている。

各国任意制度・法規制で求められる製品範囲のポジショニングマップイメージを整理すると、以下のように示される。




出所）各国関連制度に関する公開情報に基づき三菱総合研究所作成

図 5.1-5 国内外の任意対策・対策義務に関する取組のポジショニングマップイメージ[23]

## 5.1.3 日本政府における IoT 製品の安全性確保に向けた取組

我が国においても IoT 製品の安全性確保に向けた取組を推進してきた。代表的な取組として、表 5.1-3 に示すとおり、IoT 製品メーカーのセキュリティ対策を支援するガイドラインが経済産業省、IPA、総務省等から複数発表されている。

[23] 各枠は、各取組の対象製品範囲のイメージを示す。青塗枠は直接的・間接的にインターネットに接続する製品を対象としている取組、赤塗枠は直接的のみインターネットに接続する製品を対象としている取組を意味する。

表 5.1-3 IoT 製品メーカーのセキュリティ対策を支援するガイドライン

| # | 文書タイトル | 発行時期 | 発行者 | 文書概要 |
|---|---|---|---|---|
| 1 | サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF） | 2019 年 4 月 | 経済産業省 | 新たなサプライチェーン構造において求められるセキュリティ対策の全体像を整理し、セキュリティ対策例をまとめた文書 |
| 2 | IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF） | 2020 年 11 月 | 経済産業省 | IoT 機器・システムをリスクに応じてカテゴライズし、各カテゴリに対するセキュリティ・セーフティ要求の検討の考え方を示した文書 |
| 3 | 機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き | 2021 年 4 月 | 経済産業省 | 機器のセキュリティ検証において検証サービス事業者や検証依頼者が実施すべき事項等について整理した文書 |
| 4 | 電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドライン | 2021 年 4 月 | 経済産業省 | 家電製品などがインターネット環境で使われることで想定されるリスクに対し、安全確保の在り方を示した文書 |
| 5 | IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集 | 2022 年 4 月 | 経済産業省 | 一連の IoT-SSF の適用の流れを、複数のユースケースを用いて例示した文書 |
| 6 | IoT セキュリティガイドライン ver 1.0 | 2016 年 7 月 | IoT 推進コンソーシアム、総務省、経済産業省 | リスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめた文書 |
| 7 | つながる世界のセーフティ&セキュリティ設計入門 | 2015 年 10 月 | IPA | IoT 製品のセーフティ設計・セキュリティ設計の手法の用い方について解説した文書 |
| 8 | つながる世界の開発指針 | 2016 年 3 月 | IPA | IoT 製品の開発時に考慮すべき安全安心に関わる事項を指針としてとりまとめた文書 |
| 9 | IoT 開発におけるセキュリティ設計の手引き | 2016 年 5 月 | IPA | IoT 製品のセキュリティ設計を担当する開発者に向けた手引きとして、参考となる情報をまとめた文書 |

| # | 文書タイトル | 発行時期 | 発行者 | 文書概要 |
|---|---|---|---|---|
| 10 | つながる世界の品質確保に向けた手引き | 2018 年 6 月 | IPA | IoT 製品やシステムの品質をライフサイクルにわたり確保・維持するために注意が必要となるポイントをまとめた文書 |
| 11 | 脆弱性対処に向けた製品開発者向けガイド | 2020 年 8 月 | IPA | 製品開発者において実施すべき脆弱性対処と、その開示方法を掲載した文書 |
| 12 | IoT 機器等を開発する中小企業向け製品セキュリティ対策ガイド（仮称） | 作成中 | 経済産業省（予定） | 中小の IoT 機器メーカーが現実的に対応可能な範囲で実施が求められる対策を示した文書（予定） |

ガイドラインに関する取組に加え、総務省は、端末設備等規則（省令）（第 34 条の 10）を 2020 年 4 月に一部改正し、電気通信業者のネットワークに直接接続する同規則の施行後に販売された IoT 機器においてアクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装を原則義務化した。対象となる設備について、例えば、ルータやインターネットに直接接続するウェブカメラ等は該当するが、電気通信回線設備（インターネット等）に直接接続して使用されない機器、PC・スマートフォン、専用線のみにつながる機器等は対象外である。また、総務省及び NICT は、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起の取組である NOTICE（National Operation Towards IoT Clean Environment）を 2019 年 2 月から開始している。

そのほか、IoT 製品を対象に含むセキュリティに関する認証制度として、IPA による CC（Common Criteria）に基づく IT セキュリティ評価及び認証制度（JISEC）が存在する。JISEC は、IT 関連製品のセキュリティ機能の適切性・確実性を CC（ISO/IEC 15408）に基づき適合性評価機関が評価し、その評価結果を認証機関が認証する制度であり、IT 関連製品の認証取得のためには、認定機関によって認定された適合性評価機関（試験機関）によって検証・評価が実施される必要がある。認証機関は、評価結果を確認した後、その製品に対する認証書を発行する。なお、認証は国際的承認アレンジメント加盟国（CCRA 加盟国）でも通用する。また、産業用 IoT 製品に対する認証制度としては、IEC 62443-4-2 に基づく CSA（Component Security Assurance）認証制度が存在する。CSA 認証では、ソフトウェア開発プロセスのセキュリティ評価、機能的セキュリティ評価、脆弱性テストの 3 つの観点から評価される。対象機器について、ソフトウェアアプリケーション、組込み機器、ホストデバイス、ネットワークデバイス等を含む産業用コンポーネント機器が対象となる。認証機関として、国内では技術研究組合制御システムセキュリティセンター CSSC 認証ラボラトリーが存在する。加えて、政府機関が主導する認証制度ではないが、重要生活機器連携セキュリティ協議会（CCDS）が運用する「CCDS サーティフィケーションプログラム」も存在する。これは、一定のセキュリティ確保のための要件を満たした IoT 製品に対する認証サービスであり、2019 年 10 月より開始している。認証は 3 段階のレベルに分かれ、レベル 1 は IoT 製品として共通する一般的要件、レベル 2 以上は製品分野別に設定された要件への遵守が必要となる。対象製品について、インターネットにつながる IoT 製品全般が現状の対象であるが、今後 IoT 機器を利用したサービスも範囲に含むことが検討されている。認証は、CCDS が独自で策定した「IoT 機器セキュリティ要件ガイドライン」の要件に基づき行われる。

### 5.1.4 IoT 製品の安全性確保に向けた現状の課題

IoT 製品の安全性確保に向けては、我が国においても取組を進めてきたところであるが、現状の取組ではカバーできていない課題が存在すると考えられる。具体的には、IoT 製品ベンダーにおける課題、IoT 製品利用者・調達者における課題及び国民全体の課題が存在すると考えられる。

- IoT 製品ベンダーにおける課題
  - IoT 製品に対するセキュリティ対策状況が適切に評価されず、製品価値の向上につながらないおそれがある。
  - 既存制度の認証取得による明確なインセンティブが存在せず、認証を取得してもコスト増のみで、製品売上につながらないおそれがある。
  - 諸外国の制度と協調的な制度が構築されない場合、諸外国の制度の適合性評価を受ける際に別途の負担が必要となる。
- IoT 製品利用者・調達者における課題:
  - 現状ではセキュリティ対策状況が可視化されていないため、適切な対策が施された IoT 製品を選ぶことができないおそれがある。
  - 適切な対策が施された IoT 製品を利用できない場合、当該 IoT 製品がサイバー攻撃を受け、利用者に対して悪影響を及ぼすおそれがある。
- 国民全体の課題
  - マルウェア攻撃により IoT 製品がボット化して他のシステムに悪影響を及ぼすリスク、不正アクセスにより利用者のプライバシー侵害に関するリスク、サイバー攻撃により人体への物理的影響を及ぼすリスク等、IoT 製品を狙ったサイバー脅威が高まっている。
  - 諸外国は IoT 製品に対するセキュリティ対策の取組を進めているところ、十分な取組を実施しない場合、我が国の IoT 製品が集中的に狙われ、国内のシステムや国民の生活に悪影響を及ぼすおそれがある。

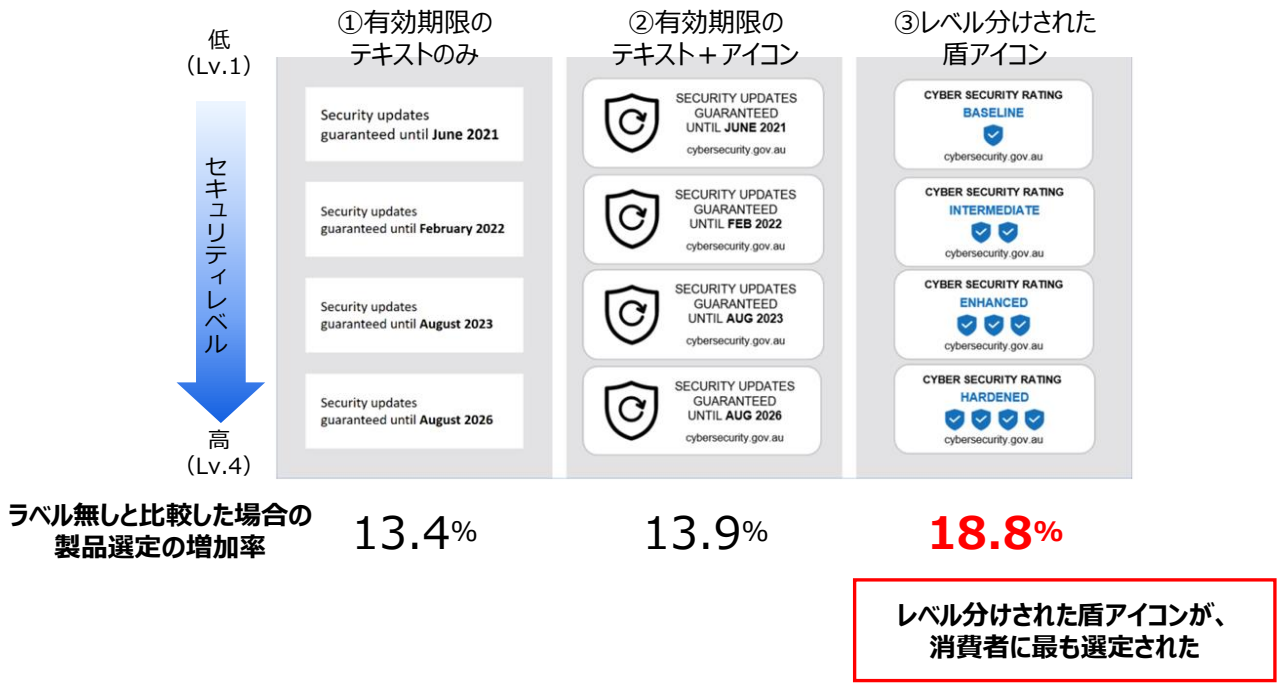
これらの課題を踏まえ、諸外国の取組も踏まえつつ、IoT 製品の安全性を確保するためには、あるセキュリティ要求基準に対するセキュリティ対策の適合性を評価し、その結果を利用者や調達者が分かる形で可視化する制度(適合性評価制度)が求められる。したがって、制度構築に向け、有識者検討会を組成しつつ、構築すべき適合性評価制度について検討を行った。

### 5.1.5 IoT 製品に対する適合性評価が与える影響に関する調査結果

IoT 製品に対するラベリング等、適合性評価が与える影響に関しては、これまでも科学的に様々な研究がなされている。例えば、2021 年に BETA(豪州政府行動経済学チーム)がオーストラリア国民 6,000 人を対象に実施した調査[24]では、オンラインショッピングにおける IoT 製品のセキュリティラベルの有効性が示された。具体的には、3 種類のセキュリティラベル(有効期限のテキスト、有効期限のテキスト+アイコン、レベル分けされた盾アイコン)を対象に、種類ごと効果の差異、セキュリティレベルごとの

[24] BETA、Helping consumers choose cyber secure smart devices(March 2022)
https://behaviouraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf

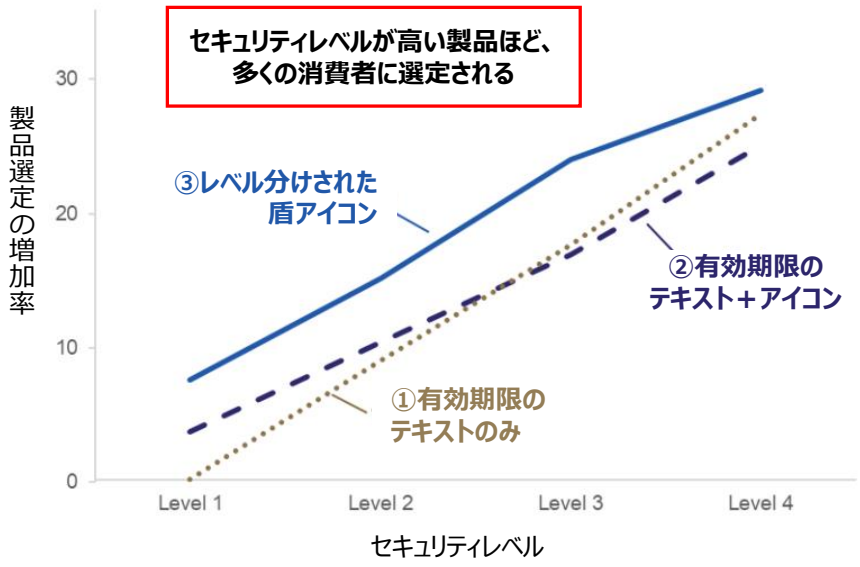
効果の差異、ラベル付与による WTP（支払意思額）への影響等が分析され、調査の結果、ラベルが付与された IoT 製品は、付与されていない製品よりも、製品選定率が 13～19%増加した。また、種類別の比較結果について、図 5.1-6 に示すとおり、3 種類のラベルの中で最も高い選定率となったのは人目につきやすい盾アイコンのラベルであった。




出典）豪州 BETA の調査に基づき三菱総合研究所作成

図 5.1-6 豪州 BETA の調査で使用した 3 種類のセキュリティラベル及び製品選定増加率

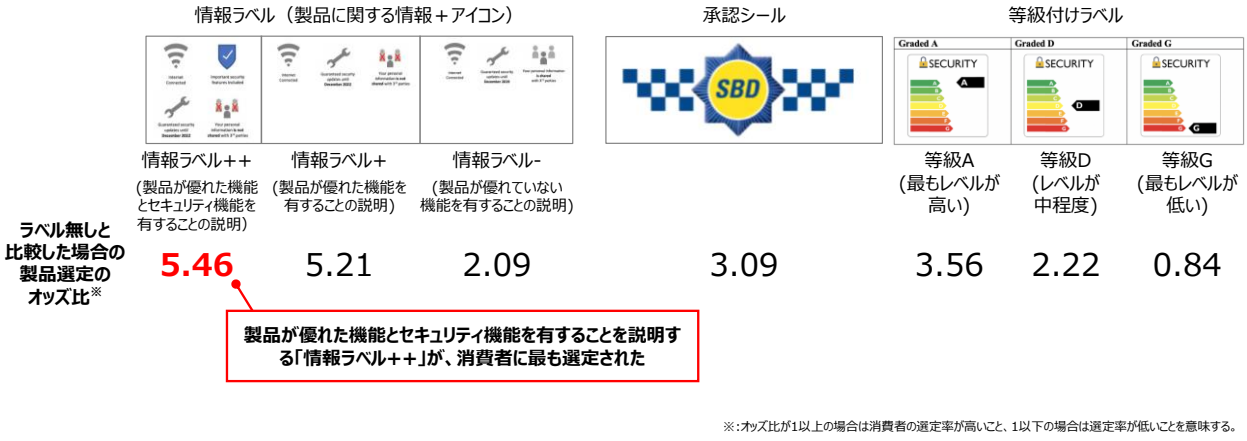
セキュリティレベルごと比較結果について、セキュリティレベルが高いことを示すラベルの方が高い確率で選定された。また、ラベルが付与されていることで消費者による製品に対する WTP（支払意思額）が増加することが確認され、ラベルが付与されている製品に多くの金額を支払う傾向にあることが明らかとなった。なお、セキュリティラベルの意味を理解できていない消費者も確認されたため、ラベルに関する解釈や使用方法に関する説明資料を準備することが有効であることが示唆された。




出典）豪州 BETA の調査に基づき三菱総合研究所作成

図 5.1-7 豪州 BETA の調査による各セキュリティレベルにおける製品選択の増加率（%）

異なる調査として、2019 年に英国 University College London（UCL）の研究者らが英国の成人約 3,000 人を対象に実施した調査結果[25]が挙げられる。この調査では、セキュリティラベルが IoT 製品の購買意思にどのような影響を与えるかが分析された。具体的には、3 種類のセキュリティラベル（情報ラベル、承認シール、等級付けラベル）を対象に、種類ごと効果の差異、ラベル付与による WTP（支払意思額）への影響、ラベル付与による消費者購買行動への定性的影響等が分析され、結果として、一部のラベルを除き、ラベルが付与された IoT 製品は、付与されていない製品よりも製品選定率が増加した。種類別の比較結果について、3 種類のラベルの中で最も高い選定率となったのは最上位の情報ラベルであった。



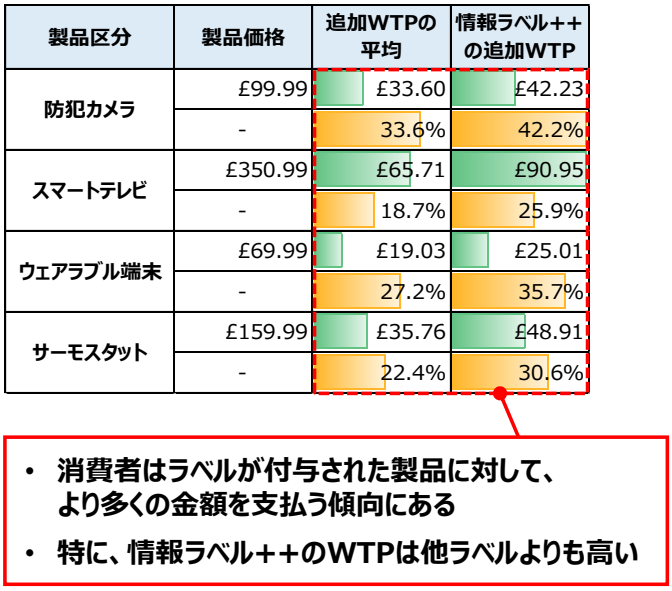

出典）UCL の調査に基づき三菱総合研究所作成

図 5.1-8 UCL の調査で使用した 3 種類のセキュリティラベル及び製品選定増加率

等級 G ラベルを除き、ラベルが付与されていることで、製品に対する WTP（支払意思額）が増加する

[25] UCL、The impact of IoT security labelling on consumer product choice and willingness to pay https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800

ことが確認された。特に、最上位の情報ラベルが付与された製品に対する WTP が最も高かった。図 5.1-9 に示すとおり、製品区分別で比較すると、多くの消費者がセキュリティ対策を懸念する防犯カメラにおける WTP の増加率が最も高かった。ラベルが付与されていることで、消費者における製品購入時の意思決定が容易となり、また、製品の比較が容易となった。この傾向は、特に情報ラベルと等級付けラベルにおいて顕著であった。また、ラベルの影響力を高めるためにデザインや配置箇所を検討する必要があるほか、ラベルが示す情報に関するマニュアルの必要性も示唆された。




出典）UCL の調査に基づき三菱総合研究所作成

図 5.1-9 UCL の調査におけるラベルが付与された製品に対する追加 WTP（支払意思額）

関連する調査研究として、2021 年にパロアルトネットワーク株式会社がグローバルの IoT ユーザ企業 1,900 社を対象に実施した調査[26]が挙げられる。この調査は、北米、EMEA（ヨーロッパ、中東、アフリカ）、JAPAC（日本、アジア太平洋地域）の 19 の国と地域における、従業員 1,000 人以上の企業に所属する IT 部門の意思決定者 1,900 人に対して行われた。調査で明らかとなった結果として、「IoT 製品の増加に対して、国や業界の規制が追いついていない」と回答した企業は 7 割（日本：72%、グローバル：72%）を超えた。この現状に対する具体的な方策に関して、グローバルの企業では、グローバルでの IoT セキュリティ基準の策定を求める企業が多く存在した一方で、国内企業では、IoT 製品のプライバシー・セキュリティに対する取組に関する情報を含むセキュリティラベルをメーカーに義務づけることを求める企業が最も多い結果となった。これより、特に国内企業において、ラベリング制度に関する一定のニーズがあることが確認できる。

## 5.2 ヒアリング調査

適合性評価制度の構築に向け、関係者に対するヒアリング調査を行った。ヒアリングは主に 2 つのフェーズに分けて実施した。ヒアリング調査①では、国内で構築すべき適合性評価制度のあるべき姿に

[26] パロアルトネットワーク株式会社、日本を含むグローバルにおける IoT セキュリティ実態調査を公開：7 割以上が IoT 機器の増加に法・業界規制が追いついていないと回答 https://www.paloaltonetworks.jp/company/press/2021/palo-alto-networks-releases-global-iot-security-survey

ついて意見を伺った。ヒアリング調査②では、初回の検討会を踏まえて構築した制度の方向性のうち、特に、対象製品範囲、評価基準及び評価スキームに関する仮説について、意見を伺った。以降では、それぞれのフェーズのヒアリング結果概要を示す。

### 5.2.1 ヒアリング調査①:適合性評価制度のあるべき姿に関するヒアリング

#### (1) ヒアリング項目

ヒアリング調査①では、学識者、IoT 製品ベンダー、IoT 製品調達者、業界団体、認証機関等にヒアリングを行い、適合性評価制度のあるべき姿に関して意見を伺った。具体的には、我が国における IoT 製品に対するセキュリティ適合性評価制度のあるべき姿として、以下の 4 点を考慮した制度を構築することを、本制度構築に当たって目指すべき仮説として提示した。

(1) すべての IoT 製品メーカーが適合性評価を受けることができる制度とすること。

(2) 製品メーカーの過渡な負担とならないよう、効果に見合った程度の費用・期間によって適合性評価を受けることができる制度とすること。

(3) 適切なセキュリティ対策を講じている製品が選定されるために、評価の結果が第三者に対して可視化される制度とすること。

(4) 評価を受けた製品が国内市場だけでなく、グローバル市場に対してアピールできる制度とすること。

ヒアリングでは、このあるべき姿の仮説をベースに、以下の項目について意見を聴取した。

- IoT 製品に対する国内のセキュリティ適合性評価制度のあるべき姿(仮説)について
- 既存のセキュリティ適合性評価制度・プログラムの課題について
- セキュリティ適合性評価制度の構築に向けた既存スキームの活用について
- セキュリティ適合性評価制度の対象となる IoT 製品の類型について

#### (2) ヒアリング結果概要

ヒアリング結果の概要を以下に示す。

まず、IoT 製品に対する国内のセキュリティ適合性評価制度のあるべき姿(仮説)について、以下のような意見が主に挙げられた。国内のセキュリティ適合性評価制度のあるべき姿の(1)～(4)の項目や実現性については、特段異議は唱えられなかったが、あるべき姿の項目のうち、「(2) 効果に見合った程度の費用・期間によって評価を受けることができること」と「(4) 諸外国制度との相互運用可能であること」を重視する意見が挙げられた。ただし、諸外国との相互運用可能性について検討を行うと議論が前に進まなくなる可能性があるとの意見もあった。

- 民生品を対象とする場合は、ラベリング制度でなければビジネスとして回らないと思われる。ラベリング制度の場合、簡易的な審査となるため、ラベルの有効期間を 3 年ほどに設定する必要がある。

- 項目(2)が肝要だと感じている。コストを負担してでも認証を取得する必要性があるかどうかが現場としては重要となる。認証を取得していない海外製品との競争に負けるという事態は避ける必要がある。
- 海外にも流通させる製品であれば海外の制度との相互運用ができるとよいだろう。
- 海外の制度との相互認証ができるのであれば、メリットになると思われる。
- IoT 製品の認証において、メーカーが大きなコストを払うことは、日本では現実的ではない。そのため、簡易的な適合性評価制度を設けるべきだと考えている。簡単なお墨付きを与える制度を設けることはよいことだと考えている。
- 相互運用可能性を実現させようとすると、認証の取得にかかるコストが上がってしまう。諸外国との相互運用可能性について検討を行うと、議論が前に進まなくなるのではないかという懸念がある。まずはシンプルな制度を設計し、国内で十分に普及した後に、グローバル展開を視野に入れた方がよい。
- 認証取得にかかる費用に関するバランスをどのように取るか、(2)の項目の検討が重要である。
- 諸外国でも認証をアピールできるとよい。海外市場に参入するために取得しなければならない認証が存在する。日本の制度と相互運用できるのであれば、申請の手間が省けてよい。
- (1)～(4)の項目は非常に重要である。制度は作って終わりではなく、活用されなければ意味がない。活用されるためにはインセンティブが必要であり、(5)に追加するかは議論が必要だが、制度が活用されるための仕組みやインセンティブ設計も重要な論点である。
- 海外の法規制がきっかけとなり認証制度が普及することがよくある。(4)の諸外国制度との相互運用性は非常に重要で、これができていないと活用されない制度となる。日本独自のガラパゴス的な制度は絶対に避けるべきである。
- ETSI EN 303 645 は、欧州だけでなく世界中で活用されており、IEC の国際相互運用スキームである CB スキーム化を目指す動きもある。 EN 303 645 を前提とした検討が妥当である。

次に、既存のセキュリティ適合性評価制度・プログラムの課題について、以下のような意見が主に挙げられた。具体的には、既存のセキュリティ適合性評価制度・プログラムについて、評価を受けることのインセンティブが不明瞭であるため、活用状況が限定的との意見が挙げられた。

- CCDS サーティフィケーションプログラムの取得製品が少ない理由としては、認知度が高くないためであると考えている。公的な制度となれば、早く普及していくと思われる。現時点では、認証を取得するためのインセンティブが少ないと思われる。
- EDSA 認証制度が普及していない理由としては、IEC 62443 のハードルが高いためだと思われる。企業は限られており、認証を取得して活用するインセンティブが見出せなかったのだと思われる。
- 国の事業を通じて IEC 62443-2-1 に基づく CSMS 認証の普及を図ったが、認証取得は 5 件程度であった。JQA も 2 件認証を行ったが、すでに認証は失効しており、いまは JQA も CSMS 認証サービスを終了した。CSMS 認証が普及しない理由をヒアリングしたところ、認証取得で売上に直結せず、メリットが不明確であることが挙げられた。

次に、セキュリティ適合性評価制度の構築に向けた既存スキームの活用について、以下のような意見が主に挙げられた。具体的には、今回構築するセキュリティ適合性評価制度について、既存の制度や取組をうまく活用することが望まれるとの意見が複数挙げられた。

- CCDS サーティフィケーションプログラムと共存できる制度を検討するべきである。国として枠組みを作った上で、一領域を CCDS に外部委託するというスキームがよいのではないか。NITE のような機関を認定機関として設定し、その認定機関によって CCDS を認証機関として認定いただくスキームがよいと思われる。
- 適合性評価制度のあるべき姿は意識しつつ、CCDS サーティフィケーションプログラムの仕組みをうまく活用した方が早く制度を構築することができると考えている。
- 制度構築に当たって、既存の制度や仕組みは活用するべきである。現状の資料では、CC や CCDS サーティフィケーションプログラムなどサイバーセキュリティ関連の認証が中心に整理されているが、消費者向け IoT 製品を対象とするのであれば、製品安全に関する取組にセキュリティの適合性評価制度をアドオンする方針も一案ではないか。製品安全に関する適合性評価の取組として、S マークの取組が挙げられる。電気用品安全法に関連する制度であるものの、法律事項ではないため、比較的フレキシブルにマークの基準を変更することができる。

最後に、セキュリティ適合性評価制度の対象となる IoT 製品の類型について、以下のような意見が主に挙げられた。特に、本事業で検討するセキュリティ適合性評価制度について、まず対象となる IoT 製品を明確化すべきとの意見が多数寄せられた。対象とする IoT 製品の観点について、製品の顧客（消費者向け、産業向け、政府向け）に関する観点や、セキュリティリスクに基づく観点が意見されたほか、対象とする IoT 製品について、制度開始当初では優先度の高い製品のみを対象とし、徐々に対象範囲を広げていく方針も意見された。また、幅広い IoT 製品を対象とする場合には、単一のラベルではなく複数段階のラベルを用意する必要性が意見された。

- IoT 製品と一口に言っても幅広い。製品の値段や顧客層、使用目的等によって、求められる制度の形も変わってくる。特に顧客層（消費者向け・産業向け・政府向け）が重要であると感じている。
- どのような IoT 製品を対象とするかについては、早めに定めた方がよい。セキュリティレベルを複数想定し、家庭用から医療に使えるものまでカバーできるようにすればよいと思われる。ラベルも一様とするよりは、数段階に分けた方がよい。
- IoT 製品と一口に言っても幅広い。対象製品を定めるべきだという議論が生じると思われる。対象製品によって、制度の形も変わってくると思われる。
- IoT 製品全域をカバーする制度を構築することは難しいと思われる。海外の事例でも、まずは重要な機器を定め、そこにフォーカスを当てるところから制度を始めていると認識している。このように、IoT 製品の中でも優先順位を定めるのは一案だと思われる。消費者向けの製品でも、ブロードバンドルータのように境界に位置するようなセキュリティリスクが高い製品は、一定のセキュリティ性能を有する必要がある。

### 5.2.2 ヒアリング調査②：適合性評価制度の方向性に関するヒアリング

#### （1） ヒアリング項目

ヒアリング調査②では、初回の検討会を踏まえて構築した制度の方向性のうち、特に、対象製品範囲、評価基準及び評価スキームに関する仮説について、IoT 製品ベンダー及び業界団体より意見を伺った。具体的には、以下に示す仮説について、ヒアリングを行った。

【1：製品範囲】

1. 適合性評価制度で対象とする製品の範囲について、「直接的又は間接的にインターネットに接続する製品」とする考え方について、この対象範囲に懸念はあるか。
2. 高いセキュリティレベルが求められる一方でその多くが法規制対象外である産業用ルータや産業用制御機器を、本適合性評価制度の対象製品範囲に含めるべきか。
3. 諸外国制度では対象外である PC、スマートフォン等の汎用 IT 製品について、本制度でも対象範囲外とすることに懸念はあるか。

【2：評価基準】

1. 適合性評価制度で採用する基準について、本制度と諸外国制度とのハーモナイゼーションのために、国際的な標準（ETSI EN 303 645、NISTIR 8425 等）を基軸とした基準とすることに懸念はあるか。
2. 適合性評価制度で採用する基準について、ETSI EN 303 645 や NISTIR 8425 のそれぞれを採用した場合に、どの程度のコスト増などの影響につながるか。

【3：適合性評価スキーム】

1. 既に認知・普及されている既存任意認証スキームにサイバーセキュリティ要件を追加する方針で検討を進めることに懸念はあるか。
2. 既存の S マーク認証制度に基づくセキュリティ適合性評価制度とすることに懸念はあるか。

#### （2） ヒアリング結果概要

ヒアリング項目として設定した各仮説について複数の IoT 製品ベンダー・業界団体に意見を伺ったところ、賛否両論の意見が挙げられた。まず、質問事項 1-1 に対する主な意見は表 5.2-1 に示すとおりであった。対象製品範囲を「直接的又は間接的にインターネットに接続する製品」とすることについて、おおむね賛成とする意見もあった一方で、より丁寧に議論すべき点として、製品ごとのリスクの優先度を踏まえるべき、対象製品を具体化すべきといった意見もあった。

表 5.2-1 ヒアリング調査②：質問事項 1-1 に関する意見概要

| 意見区分 | ヒアリング結果概要 |
|---|---|
| おおむね賛成 | 《「直接的又は間接的にインターネットに接続する製品」を範囲とすることにおおむね賛成の意見》 |

| 意見区分 | ヒアリング結果概要 |
| --- | --- |
| | ・ 間接接続する IoT 製品であってもアタックサーフェスは存在するため、提案の対象製品範囲でよい。<br>・ 任意制度であるため、今回の制度の対象範囲を広く「直接的又は間接的にインターネットに接続する IoT 製品」とすることに、特に懸念はない。<br>・ インターネットからの直接アクセス、間接的なアクセスに依存したセキュリティ対策ではないため、懸念はない。<br>・ 端末設備等規則のようにインターネットに直接接続する製品だけを対象にするのは、実効性の観点で疑問があるため、「直接的又は間接的にインターネットに接続する IoT 製品」を対象とすることはよい。<br>・ 今回の認証制度の考え方が「最低限のセキュリティレベル」を求めるということであれば、提案の対象製品範囲でよい。一部の機器を除くとなると、その機器の定義が必要となるため、範囲としては「直接的又は間接的にインターネットに接続する IoT 製品」でよいのではないか。 |
| より丁寧に議論すべき点 | 《製品ごとのリスクの優先度を踏まえた議論をすべきとの意見》<br>・ リスクが高いのは直接接続している機器であり、優先度としては、直接的にインターネットに接続する IoT 製品で十分ではないか。<br>・ 直接的間接的にネット接続する製品も無条件で一律に対象範囲内とすることには懸念がある。<br>・ まずは直接的にインターネットに接続する製品を適切に保護することが重要で、間接的につながる機器についてはレベルを分ける等の仕組みが必要ではないか。<br>・ 《対象製品を具体化すべきとの意見》<br>・ 対象製品範囲を広く定義すると、ベンダーとしては迷う可能性がある。具体的に明記した方がベンダーとしては対応しやすい。 |
| その他 | ・ 任意の認証制度であれば懸念はないが、製品カテゴリごとに異なる要求基準/認証スキームの検討が必要ではないか。<br>・ 自動車や医療機器など、独自規格が進んでいる製品は対象から除外してもよいのではないか。<br>・ 間接的な IoT 製品も範囲に含めるべきだが、「間接的にインターネットに接続する」という表現を明確化すべきである。 |

次に、質問事項 1-2 に対する主な意見は表 5.2-2 に示すとおりであった。具体的には、任意制度であること、国際調和の観点、ベンダーの選択肢を広げる観点で、産業用製品を対象範囲に含めることに肯定的であるとの意見があった一方で、高いセキュリティレベルを求める既存認証制度（CC 認証、CSA 認証等）の対策を追求すべきという意見もあった。

表 5.2-2 ヒアリング調査②：質問事項 1-2 に関する意見概要

| 意見区分 | ヒアリング結果概要 |
|---|---|
| おおむね賛成 | 《任意制度であることを前提に、あえて対象外とする必要がないとの意見》<br>・ あえて除外する必要は無いが、別途業界で議論し、それぞれの業界の中で何が必要なのか、ということを判断していくことが必要となる。<br>・ 産業用 IoT 機器であっても、消費者向け IoT 機器のセキュリティ水準以上と言って販売してもよいので、あえて対象外とする必要もない。<br>・ 除外するか否かの議論をすると、線引きが難しく、どの機器を含めるか否かの議論が紛糾すると思う。<br>・ 境界線が不明確となる可能性があるため、抜け漏れを無くすために、今回の任意認証制度としてカバーしておく方針はよいと考えている。<br>《国際ハーモナイゼーションの観点で、産業用製品を含めることに賛成の意見》<br>・ 国際整合を図る前提で対象範囲に含めるべきである。<br>《ベンダーの選択肢の一つとして、産業用製品を含めることに賛成の意見》<br>・ 産業用 IoT も対象に含め、CC 認証や EDSA 認証への橋渡し的な役割の制度とするのがよいのではないか。PLC や SCADA においてどれだけ対策が進んでいるか未知数であるため、橋渡し的な制度があると、業界としてセキュリティレベルは高まっていくのではないか。<br>・ 今回の制度を土台としつつ、追加で産業用ルータや制御機器に対する対策を求めた方がよいのではないか。ベースラインを定めつつ、各産業分野にて追加で求める対策を検討する方針がよいと思う。<br>・ 産業用ルータや産業用制御機器は高いセキュリティレベルが求められるが、メーカーが取り組む選択肢の一つとして、今回の適合性評価制度の範囲に含めてもよいのではないか。 |
| より丁寧に議論すべき点 | 《高いセキュリティレベルの対策を追求すべきとの意見》<br>・ 高いセキュリティレベルが求められることを踏まえると、今回の制度の対象とはせず、既存の認証制度の訴求を促すべき。<br>・ 社会インフラのセキュリティ対策に注目が集まっており、産業制御系の機器に対しても適切なセキュリティ対策を求める必要があるため、別の取組で対策を推進する方針もあり得る。 |
| その他の意見 | 《認証を実施するか否かは市場原理に基づき判断されるとの意見》<br>・ 産業用ルータや産業制御機器については、既に CC 認証や EDSA 認証のような任意認証制度が存在し、市場原理に基づいてベンダーが取捨選択している。 |

次に、質問事項 1-3 に対する主な意見は表 5.2-3 に示すとおりであった。汎用 IT 製品の扱いについて、販売後の利用者の設定でセキュリティレベルが変わることや、国際調和の観点で、汎用 IT 製品を対象範囲外とすることに賛成といった意見があった一方で、より詳細にリスクの優先度を踏まえるべき、という意見もあった。

表 5.2-3 ヒアリング調査②：質問事項 1-3 に関する意見概要

| 意見区分 | ヒアリング結果概要 |
|---|---|
| おおむね賛成 | 《汎用 IT 製品では、販売後の利用者の設定でセキュリティレベルが変わるため、範囲外とすることに賛成の意見》<br>・ 技術的に対象範囲外にせざるを得ないのではないか。PC やスマートフォン等の汎用 IT 製品では、購入後に利用者でアプリケーションをインストールでき、セキュリティ対策レベルも変わる。そのため、セキュリティをメーカーで担保することは難しい。<br>・ 汎用 IT 製品の場合、販売後にセキュリティの対策状況が変わる可能性があるため、対象範囲外とすることに懸念は無い。ただし、もし範囲外とする場合には丁寧な説明が必要となる。<br>・ 多くの IoT 製品はなるべく無駄な機能を削っているため、汎用 IT 製品とは位置づけが異なる。そのため、現状では範囲外とすることに賛成である。<br>《国際ハーモナイゼーションの観点で、汎用 IT 製品を対象範囲外とすることに賛成の意見》<br>・ 国際的な相互運用性の確保を優先すべきと考える。<br>・ 諸外国制度での議論と同様に、容易にセキュリティ対策できるため対象外がよい。あえて日本で追加する必要はない。<br>・ 国際的な整合性と一致させている点において矛盾はなく、懸念はない。<br>・ 汎用 IT 製品については、後からセキュリティソフトウェアを導入することで対策ができる。諸外国の動向も踏まえると、あえて今回の制度に含める必要はない。 |
| より丁寧に議論すべき点 | 《製品ごとのリスクの優先度を踏まえた議論をすべきとの意見》<br>・ 汎用 IT 製品・IoT 製品ともに、論理的に見れば違いは無いため、範囲に含めるべきと考えている。<br>・ 工場設備のセキュリティ対策を考えたとき、PC 及びそのソフトウェアで設備のメンテナンスを管理しているため、対策を求めることは重要となる。 |
| その他の意見 | ・ 最初から PC・スマートフォンを対象に含めると制度設計に時間がかかり、制度構築がつまずくのではないか。 |

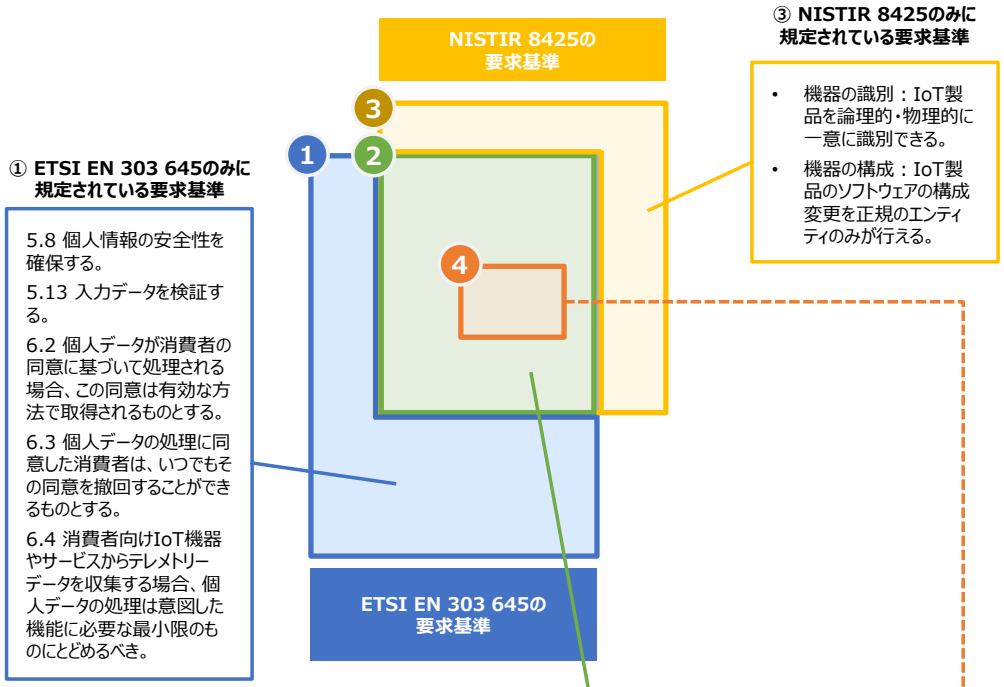
つづいて、適合性評価基準に関する質問事項のうち、質問事項 2-1 に対する主な意見は表 5.2-4 に示すとおりであり、本適合性評価制度で用いる基準を国際的な標準を基軸とした基準とすることについて、ほとんどが賛成の意見であった。ただし、基準の日本語版の作成に関する要望や、必要に応じて日本独自の基準を追加検討することの必要性が意見されたほか、より丁寧に議論すべき点として、特定の分野における新たな国際基準策定の必要性について意見が挙げられた。

表 5.2-4 ヒアリング調査②：質問事項 2-1 に関する意見概要

| 意見区分 | ヒアリング結果概要 |
|---|---|
| おおむね賛成 | 《国際ハーモナイゼーションの観点で、国際的な標準を基軸とした基準とすることに賛成の意見》 |

| 意見区分 | ヒアリング結果概要 |
| --- | --- |
| | ・ 採用する基準について、日本独自の基準を採用することは得策ではなく、グローバルで活用されている国際的な基準を用いるべきである。<br>・ 海外との相互運用性は考慮すべきであり、基本的には国際的な標準に則った形がよい。<br>・ ETSI EN 303 645 や NISTIR 8425 を基軸とする方針に異論はない。<br>・ 諸外国制度とのハーモナイゼーションのために、国際的に広く使われている基準を用いるのがよい。特に、グローバル企業にとって重要となる。<br>・ 目的から考えると国際的な標準をベースとすることが現実的である。できるだけダブルスタンダードとなることは避けたい。<br>・ 国際的な標準を基軸とした基準とすることに賛成である。しかし、ETSI EN 303 645 や NISTIR 8425 は英語版のみ公開されているため、JIS 化する等、正式な日本語版の基準を作成いただきたい。<br>・ 国際的な標準を基軸とすることに賛同するが、国際的にコンセンサスを得た単一の基準は無いため、何を「国際標準」と見なして活用するか、国際的な動向に加えて認証制度の趣旨も踏まえた上で判断することが必要である。<br>・ 日本独自の基準や項目の導入は認証制度の利用を妨げることにもつながるため避けることが望ましい。<br>・ 似て非なるものを日本独自で求められることは、コスト・心理的に厳しく、グローバルの制度で採用している基準を元に設計することが望まれる。<br>・ 一部だけを抽出した基準とするのであれば、ETSI や NIST との対応づけを整理しつつ、独自の基準とした方がよい。<br>・ ETSI EN 303 645 は基本的事項が記載されたものと認識しており、ここから削るという議論でもよいし、削る項目が決められなかったら ETSI EN 303 645 と同じでもよい。<br>・ 基本的な項目は同盟国の基準と整合を図りつつも、必要に応じて、日本独自の経済安全戦略に合わせた基準を策定すべきである。<br>《特定分野について、新たに国際基準を策定すべきとの意見》<br>・ 欧州基準、米国基準はいずれも受け入れられない。自動車分野で WP29 国際基準策定のように、家電機器・住設機器分野でも「国際基準」の策定が求められる。経済産業省においては、各国政府機関とも連携の上で、策定に向けて主導的な取り組みをお願いしたい。 |
| その他の意見 | ・ どの規格であっても、国内で評価できる体制が必要である。 |

次に、質問事項 2-2 について、図 5.2-1 に示す ETSI EN 303 645 及び NISTIR 8425 の要求基準の関係性イメージを示しつつ、適合性評価制度で採用する基準について、ETSI EN 303 645 や NISTIR 8425 のそれぞれを採用した場合に、どの程度のコスト増などの影響につながるかを確認した。




② ETSI EN 303 645とNISTIR 8425の両方に規定されている要求基準

| ETSI EN 303 645ベース | NISTIR 8425ベース | 総務省：端末設備等規則ベース |
|---|---|---|
| 4.1 報告書を作成すること。 | ドキュメンテーション | – |
| 5.1 共通の初期パスワードを設定しない。 | インターフェイスへの論理アクセス | 第三十四条の十 一（アクセス制御機能）<br>第三十四条の十 二（初期設定のパスワードの変更を促す等の機能） |
| 5.2 脆弱性報告の管理手段を導入する。 | 情報及び問合せの受付、教育及び意識向上 | – |
| 5.3 ソフトウェアを定期的に更新する。 | ソフトウェアの更新、情報発信 | 第三十四条の十 三（ソフトウェアの更新機能） |
| 5.4 機密性の高いセキュリティパラメータを安全に保存する。 | データ保護、インターフェイスへの論理アクセス | – |
| 5.5 安全に通信する。 | データ保護 | – |
| 5.6 攻撃対象となる領域を最小限に抑える。 | インターフェイスへの論理アクセス | – |
| 5.7 ソフトウェアの整合性を確保する。 | サイバーセキュリティの状態認識 | – |
| 5.9 機能停止時のシステムの復旧性を確保する。 | インターフェイスへの論理アクセス、ソフトウェアの更新 | 第三十四条の十 四（電力供給が停止した場合でも、出荷状態に戻ることなく、アクセス制御機能に係る設定や更新されたソフトウェアの維持） |
| 5.10 システムのテレメトリデータを検証する。 | サイバーセキュリティの状態認識 | – |
| 5.11 ユーザーがユーザーデータを容易に削除できるようにする。 | データ保護、教育及び意識向上 | – |
| 5.12 デバイスを容易に設置してメンテナンスできるようにする。 | 教育及び意識向上 | – |
| 6.1 製造者は、消費者に対し、機器やサービスごとに、どのような個人データが、誰によって、どのような目的で処理されているかについての明確かつ透明性のある情報を提供するものとする。これは、広告主を含む関与しうる第三者にも適用される。 | 教育及び意識向上 | – |
| 6.5 消費者向けIoT機器やサービスから遠隔測定データを収集する場合、消費者はどのような遠隔測定データが収集され、それが誰によって、どのような目的で使用されているかについての情報を提供されるものとする。 | 教育及び意識向上 | – |

図 5.2-1 ETSI EN 303 645 及び NISTIR 8425 の要求基準の関係性イメージ[27]

[27] 下表は ETSI EN 303 645 を軸とした項目レベルでの対応関係のマッピングであり、詳細な対策要求項目を比較するとより多くの差異が存在することに留意。ETSI/NIST の対応関係のマッピングは、NISTIR 8259A 及び NISTIR 8259B の記載に基づき作成。また、総務省の端末設備等規則は義務要件であり、必要最低限の規程となっていることに留意。

質問事項 2-2 に対する主な意見は表 5.2-5 に示すとおりであり、採用する基準によって、ベンダーのコスト増などの影響が変わるとの意見が挙げられたほか、メーカーに与える影響、適合性評価に要するコスト、国際動向等を踏まえた基準の検討の必要性が示唆された。

表 5.2-5 ヒアリング調査②：質問事項 2-2 に関する意見概要

| ヒアリング結果概要 |
| --- |
| 《ETSI EN 303 645 で求められる基準のみを採用した場合（①＋②の範囲）の影響に関する意見》<br>・ ETSI EN 303 645 は基礎的な事項とプライバシーが考慮されている。プライバシーをどこまで見るかはあるが、ETSI EN 303 645 を元に考えることになるのではないか。<br>・ ETSI EN 303 645 の基準をすべて採用することは過剰である。<br>・ 産業用機器では個人データの取扱いがないことが多いため、冗長だと考えられる。<br>・ ETSI EN 303 645 は少しハードルが高く、大手企業のような体力がある企業に限られるのではないか。<br>・ 欧州は強制法規となる一方で、NISTIR は任意基準なので、強制法規の ETSI EN 303 645 が優先されるのではないか。<br>・ ETSI EN 303 645 を採用している各国制度においても一部の要求基準を抽出していると思う。日本においても、必要な要件を取捨選択するのがよいのではないか。<br>《NISTIR 8425 で求められる基準のみを採用した場合（②＋③の範囲）の影響に関する意見》<br>・ NISTIR 8425 の基準をすべて採用することは過剰である。<br>・ ETSI EN 303 645 よりも対応しやすいと考えられるが、中小企業等のリソースが限られる事業者にとって「非技術的サポート機能」の対応が困難となる可能性がある。<br>・ グローバルで共通的に求められる基準であれば、国内の適合性評価制度に対応するためのコスト増にはならない。NISTIR 8425 の場合、米国では任意制度なので、日本企業としては取得のインセンティブが低い。<br>・ NISTIR 8425 は比較的対応しやすいが、組織的対策も含まれているので、リソースが限られている中小企業のような会社は対応が難しいかもしれない。<br>《ETSI EN 303 645 と NISTIR 8425 の両方で求められる基準を採用した場合（②の範囲）の影響に関する意見》<br>・ メーカーにとって、そこまで負担にはならないと思う。<br>・ レベル分け次第ではあるが、まずは NIST と ESTI の両方で求められる基準を考えるのがよいのではないか。<br>《ETSI EN 303 645 と NISTIR 8425 のいずれかのみを採用した場合（①＋②又は②＋③の範囲）の影響に関する意見》<br>・ ETSI EN 303 645 と NISTIR 8425 をベースとするのであれば、どちらかの規格に適合していれば、「適合」と見なすと影響は小さくなる可能性がある。 |

| ヒアリング結果概要 |
| --- |
| ・　製品によって国内向け、欧州向け、米国向け、グローバル展開など様々であり、基準・規定が多いと手間暇がかかるので、ETSI 基準、NISTIR 基準の少なくとも一方を求める、とすることが実用的である。<br>《ETSI EN 303 645 と NISTIR 8425 のいずれかで求められる基準すべてを採用した場合（①＋②＋③の範囲）の影響に関する意見》<br>・　ETSI と NIST のいずれかで求められている基準に全て対応するとなると正直かなり厳しい。対策コストが倍増することとなる。<br>・　最も高コストになると考えられ、事業者が対応できずに普及が進まなくなる可能性がある。<br>・　対応コストがかかり、競争力が低下する。<br>《その他の意見》<br>・　ETSI EN 303 645、NISTIR 8425 のどちらもコスト増につながる。<br>・　現状達成している基準より低い基準であっても、対応コストはかかることとなる。<br>・　大手メーカーにおいては、ETSI や NIST の基準を採用することの影響は限定的ではないか。他方で、国内向けのみに製品販売している中小企業等の場合、追加の対応が必要なケースが多く、大きな影響を及ぼすのではないか。 |

つづいて、適合性評価スキームに関する質問事項のうち、質問事項 3-1 に対する主な意見は表 5.2-6 に示すとおりであり、効率的に制度を普及・促進する観点で、既存任意認証スキームにサイバーセキュリティ要件を追加する方針に賛成の意見が挙げられた一方で、より丁寧に議論すべき点として、制度間の整合化が図れないことへの懸念、市場の混乱、将来の発展可能性等の観点で、独自認証制度を新たに構築すべきとの意見が挙げられた。関連して、第三者認証のみを許容する場合、評価にコストがかかり、IoT 製品ベンダーの負担が増加することから、自己適合宣言による評価を求める意見が挙げられた。

表 5.2-6 ヒアリング調査②：質問事項 3-1 に関する意見概要

| 意見区分 | ヒアリング結果概要 |
| --- | --- |
| おおむね賛成 | 《効率的に制度を普及・促進する観点で、既存任意認証スキームにサイバーセキュリティ要件を追加する方針に賛成の意見》<br>・　新しいスキームを作るよりは既存のスキームを活用できた方が効率的と考える。<br>・　既存の認証スキームを利用している企業は既存制度を活用した方が負担は少ない。<br>・　認証申請の手間が省けるためよいと考える。<br>・　既存の任意認証スキームを用いることで、既に認証取得している企業としては受け入れやすく、新たに制度を構築して広報するよりよいと思う。<br>・　社内に訴求する際は、既存の仕組みにセキュリティ要件が追加された方が動きやすい。新たな制度を構築し、それをメーカーに訴求することは大変な作業となるため、既存の仕組みに入れ込んだ方が導入のハードルは低い。 |
| より丁寧に議 | 《様々な既存任意認証スキームにセキュリティ要件を追加した場合、制度間の整合化が図 |

| 意見区分 | ヒアリング結果概要 |
|---|---|
| 論すべき点 | れない可能性があるため、既存任意認証スキームにサイバーセキュリティ要件を追加すべきではないとの意見》<br>・ 様々な既存の評価制度にセキュリティ要件が含まれる場合、それぞれの評価制度のセキュリティ要件が重複、あるいは相反することも考えられるため、現状では既存制度に絡めた評価制度とすることには反対する。<br>《市場の混乱を防ぐために、独自認証制度を新たに構築すべきとの意見》<br>・ セキュリティの任意認証制度としては、新たな制度（例: S マーク セキュリティ版など）の導入が市場混乱も少ないと考えられる。<br>《既存任意認証スキームの制約を受けるため、将来の発展可能性のために、独自認証制度を新たに構築すべきとの意見》<br>・ 既存の任意認証スキームを活用することで広く活用される可能性はあるが、当該スキームの制約条件を受けることとなる。活用拡大は、制度の普及など運用面でカバーする話であるが、制約条件はどうしようもない可能性がある。そのため、将来的なことを考えると、独自の認証制度を作った方がよいのではないか。 |
| 自己適合宣言に関する意見 | 《自己適合宣言を許容する認証スキームとすべきとの意見》<br>・ 多くの IoT 製品メーカーは自社でセキュリティ対策の確認を実施しているため、追加コストを避けるために、自己適合宣言を許容することが望まれる。<br>・ コスト面からは自己宣言型が望ましい。レベルを分け、自己宣言と第三者認証が分かれるという考えがある。 |
| その他の意見 | ・ いずれの任意認証スキームを活用する場合でも各国との相互認証が必要となる。<br>・ セキュリティ要件が足されることによって、現行普及している制度の普及率が減る可能性も高いため、慎重な議論が必要である。<br>・ 消費者において任意の制度であることが理解されるかどうかが疑問である。制度の品格を高めないとメーカーとしても動きづらく、制度が活用されない懸念がある。 |

最後に、質問事項 3-2 に対する主な意見は表 5.2-7 に示すとおりであった。現状の S マーク認証制度を利用することに賛成の意見は限定的であり、S マークを活用した制度とする場合、市場の混乱を可能な限り低減するために、「S マークセキュリティ」等のセキュリティに関する個別の S マーク認証制度を新たに構築することが望ましいとの意見が挙げられた。

表 5.2-7 ヒアリング調査②：質問事項 3-2 に関する意見概要

| 意見区分 | ヒアリング結果概要 |
|---|---|
| おおむね賛成 | ・ 現状の S マーク認証制度を利用することでよい。 |
| セキュリティに関する新たな S マーク | 《既存の S マーク認証制度ではなく、「S マークセキュリティ」等、セキュリティに関する個別の S マークの構築に関する意見》 |

| 意見区分 | ヒアリング結果概要 |
| --- | --- |
| 認証制度に関する意見 | ・ セキュリティの任意認証制度としては、新たな制度（例: S マーク セキュリティ版など）の導入が市場混乱も少ないと考えられる。<br>・ 既に S マークを取得している製品が多数ある中で、新たにセキュリティ要件が追加されることで、対応できない製品もあるだろう。例えば、既存の S マークは活かしつつ、セキュリティに関する S マークを別スキームとして作るなど、既存の S マーク認証を取得している製品にとって不利益にならない設計が必要となる。<br>・ S マークを活用するとしても、現行の S マークにアドオンするのではなく、S マークのセキュリティ版のような、新たな S マークを構築すべきである。 |
| S マークを活用した制度とする場合に留意すべき事項に関する意見 | 《セキュリティ要件を追加した場合の、既存の S マーク認証済み製品の関係性に関する意見》<br>・ 仮に S マークに追加する場合、認証時期や製品によって求められる対策が違うということは避けるべきである。<br>・ S マークにセキュリティ要件を追加する場合、既存の S マークとセキュリティに関するマークを分けるかどうかは検討が必要である。<br>・ 仮に S マークにセキュリティ要件を追加する場合、過去に S マーク認証を受けた製品をどのように扱うか、整理した上で制度設計をお願いしたい。<br>《セキュリティ要件を追加した場合の、工場検査の要否に関する意見》<br>・ セキュリティの観点では、S マーク認証制度における生産ラインの確認は不要ではないか。 |
| より丁寧に議論すべき点 | 《S マーク認証制度は製品安全を目的とした制度で、セキュリティに関する制度ではないため、S マーク認証制度に含めるべきではないとの意見》<br>・ S マークは、電気製品から遠いイメージの製品が参加しないことを懸念するため、どちらかと言えば反対である。<br>・ 既存の S マークの基準と今回のサイバーセキュリティの基準は方向性が異なる。新たにセキュリティが入ると混乱する可能性があるので、新たに別の認証制度でセキュリティを扱う方が、かえって受け入れやすいのではないか。<br>・ S マーク認証制度は電安法をベースとしているが、製品安全とセキュリティはリスク分析の考え方が異なるため、懸念がある。<br>・ S マーク認証は主にハードウェアの適合であるが、本制度の案件は主にソフトウェアで構成するもの。よって、現 S マーク認証とセキュリティ認証はそぐわない。<br>・ 現状の S マークは製品安全に関する適合性評価であり、メーカーや消費者が混乱する可能性があるため、どちらかと言えば反対である。<br>・ 既存の認証スキーム加えるのは悪くないアイデアだと思うが、S マークは適していないと思う。電安法では直流電源機器は対象外であるため、ルータ等は対象外である。そのため、〇PSE を補足する S マークの認証取得実績も無く、このような機器ベンダーにとっては新たな認証制度と同じ形となる。<br>《S マークの認証機関が限定的であるため、認証に要する期間が長期になることを防ぐため |

| 意見区分 | ヒアリング結果概要 |
|---|---|
| | に、S マーク認証制度に含めるべきではないとの意見》<br>・ S マーク認証は 4 機関(JET、JQA、UL Japan、TUV Rheinland Japan)で実施であるが、本制度の案件は大量で、認証待ち状態が想定される。 |
| その他の意見 | ・ IEC 62443 のように、開発体制と製品とを分けて考えることが妥当ではないか。<br>・ CCDS サーティフィケーションプログラムを活用することも一つの方法論だと思う。 |

## 5.3 有識者検討会の実施

適合性評価制度構築に向けた検討を行うために、令和 4 年 11 月より「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」を開催し、現状の課題、適合性評価制度構築の目的、構築すべき適合性評価制度等について議論を行った。

### 5.3.1 有識者検討会の構成員

本有識者検討会の構成員は以下に示すとおりである。

| | |
|---|---|
| (副座長)猪俣 敦夫 | 大阪大学 情報セキュリティ本部 教授 |
| 稲垣 隆一 | 稲垣隆一法律事務所 弁護士 |
| 岩﨑 章彦 | 一般社団法人電子情報技術産業協会 セキュリティ専任部長 |
| (座長)高倉 弘喜 | 国立情報学研究所 アーキテクチャ科学研究系 教授 |
| 高橋 範 | 株式会社ソラコム 事業開発ディレクター |
| 中尾 康二 | 国立研究開発法人情報通信研究機構<br>サイバーセキュリティ研究所 主管研究員 |
| 中野 学 | パナソニックホールディングス株式会社 技術部門 テクノロジー本部<br>製品セキュリティセンター 製品セキュリティグローバル戦略部 部長 |
| 花見 英樹 | 株式会社日立製作所 インダストリアルデジタルビジネスユニット CTO |
| 広瀬 良太 | ヤマハ株式会社 音響事業本部 基盤技術開発部 部長 |
| 松浦 芳樹 | GROOVE X 株式会社 Software チーム エリアプロダクトオーナー |
| 唯根 妙子 | 消費生活アドバイザー |

(オブザーバー)
内閣官房内閣サイバーセキュリティセンター
総務省 サイバーセキュリティ統括官室
経済産業省 情報産業課、製品安全課、産業機械課、国際電気標準課、通商機構部
独立行政法人情報処理推進機構(IPA)
独立行政法人製品評価技術基盤機構(NITE)
国立研究開発法人新エネルギー・産業技術総合開発機構(NEDO)
公益社団法人日本通信販売協会(JADMA)

一般社団法人重要生活機器連携セキュリティ協議会（CCDS）
一般社団法人情報通信ネットワーク産業協会（CIAJ）
一般財団法人電気安全環境研究所（JET）
一般社団法人日本電機工業会（JEMA）
一般財団法人日本品質保証機構（JQA）
一般社団法人ビジネス機械・情報システム産業協会（JBMIA）
技術研究組合制御システムセキュリティセンター（CSSC）
電気製品認証協議会（SCEA）

### 5.3.2 開催概要

有識者検討会は年度内に三回開催し、適合性評価制度構築に向けた議論を行った。各回の議事は表 5.3-1 に示すとおりである。構成員からのプレゼンテーションについて、第 1 回有識者検討会では、情報通信研究機構 中尾委員、パナソニック中野委員、CCDS 荻野氏、JQA 大塚氏の 4 名からプレゼンテーションを実施いただいた。第 2 回有識者検討会では、IPA 神田氏、SCEA 平井氏の 2 名からプレゼンテーションを実施いただいた。なお、第 3 回有識者検討会では、本検討会の中間とりまとめ案についても議論を行った。

表 5.3-1 適合性評価制度に関する有識者検討会の開催概要

| 回・実施日 | 議事 |
|---|---|
| 第 1 回<br>（2022 年 11 月 1 日） | 1. 開会<br>2. 構成員からのプレゼンテーション<br>3. IoT 製品に対するセキュリティ適合性評価制度の構築について<br>4. 自由討議<br>5. 閉会 |
| 第 2 回<br>（2023 年 2 月 6 日） | 1. 開会<br>2. 前回の御議論の振り返り<br>3. 構成員からのプレゼンテーション<br>4. IoT 製品に対するセキュリティ適合性評価制度の構築について<br>5. 自由討議<br>6. 閉会 |
| 第 3 回<br>（2023 年 3 月 17 日） | 1. 開会<br>2. IoT 製品に対するセキュリティ適合性評価制度の構築について<br>3. 自由討議<br>4. 閉会 |

### 5.3.3 主な議論内容

#### （1） 第 1 回有識者検討会

第 1 回の有識者検討会で挙げられた主な意見は表 5.3-2 に示すとおりである。制度の位置づけについて、本制度を法的に義務化すれば制度が活用される一方で、義務化には責任も伴うため、慎重に検討すべきとの意見が挙げられた。また、対象製品に関して、消費者向け IoT 製品からスタートして課題を整理することが重要との意見のほか、消費者向け製品も産業向け製品のどちらも制度の対象とするべきとの意見も挙げられた。適合性評価基準に関して、IoT 製品メーカーに与える影響やメリットを鑑みた検討の必要性が提示された。採用する適合性評価スキームについて、簡易的な方法で評価を行うことが望ましいとの意見が挙げられた。前述のとおり、第 1 回有識者検討会で挙げられた意見を踏まえ、IoT 製品ベンダー及び業界団体に対してヒアリング調査（ヒアリング調査②）を実施した。

表 5.3-2 適合性評価制度に関する第 1 回有識者検討会で挙げられた主な意見

| カテゴリ | 主な意見 |
|---|---|
| 制度の位置づけ（義務／任意）について | • 法的に義務化すれば、制度が活用されるようになると思われる一方で、義務化には責任も伴うため、慎重に検討した方がよい。<br>• 義務的な法制度としなければ、制度は広がらない。強制力がない限り、メーカーは重い腰を上げられないのが現状である。 |
| 制度の対象製品について | • 消費者向け製品も産業向け製品のどちらも制度の対象とするべきだと考えているが、レベルは分けるべきであり、消費者向け製品であっても最低限のセキュリティ対策は求められるべき。<br>• ラベリング制度を設けるのであれば、有効なのは消費者向け IoT 製品である。<br>• 消費者向け IoT 製品からスタートし、様々な課題を整理していくことが重要である。<br>• 同じ IoT 機器であっても、消費者向けとして使われる場合と重要インフラ向けに使われる場合があるため、対象とする機器の検討が必要である。 |
| 制度で用いる適合性評価基準について | • 適合性評価制度に取り組んだメーカーや輸入業者が泣きを見るような事態にならないよう、レベルは適切に設定する必要がある。<br>• どのような基準を定めるのかについては、メーカーのメリットを鑑みつつ検討を行っていくべきである。 |
| 制度で用いる適合性評価スキームについて | • 簡易的かつ適切な方法で評価を行っていく必要がある。<br>• IoT 機器の脆弱性や脅威分析に関する取組と連動するようなスキームがあればより良い。 |
| その他 | • 制度な目的として、誰の利益を想定するかを明らかにした方がよい。<br>• 制度のスコープをきちんと定め、誰が、どのように本制度を活かしていくのかを議論していくべきである。<br>• IoT 製品の適合性評価制度は、ベンダーに負担をかけないような形で実現していくべきである。<br>• 制度の知名度を上げる努力をしない限り、メーカーの説明コストは変わらないため、本制度の普及活動を消費者向けに行う必要がある。<br>• IT 導入補助金との連携や政府の調達要件になる等、取り組んだ企業にメリットがあるような制度になればよい。 |

### （2）第 2 回有識者検討会

第 2 回の有識者検討会で挙げられた主な意見は表 5.3-3 に示すとおりである。政府の関与や検討体制のあり方について、基準検討のための体制構築の必要性に関する意見が挙げられた。対象製品に関して、「間接的又は直接的にインターネットに接続する製品」でよいとする意見が多く、適合性評価基準に関しても、国際的な基準を基軸とする方針でよいとする意見が多く挙げられた。採用する適合性評価スキームについて、コストや IoT 製品の特性を踏まえたスキーム構築の必要性について意見が挙げられた。その他、制度の目的の明確化、プロモーションやインセンティブ設計の重要性、事案への対応等に関する意見が挙げられた。

表 5.3-3 適合性評価制度に関する第 2 回有識者検討会で挙げられた主な意見

| カテゴリ | 主なご指摘事項 |
|---|---|
| 政府の関与や検討体制のあり方について | • 基準の作り方を検討すべきである。小規模な検討グループを作り、関連基準の重複等を調査し、本制度で採用する部分を整理するとよいのではないか。<br>• セキュリティの確保された社会を構築するという、社会に対する貢献も重要であるため、視点に入れていただきたい。 |
| 制度の対象製品について | • 「間接的又は直接的にインターネットに接続する製品」として、技適の対象より広げる方向性はよい。<br>• 製品によって使われる環境が異なり、リスクも変わる点について議論する必要がある。<br>• 「間接的又は直接的にインターネットに接続する製品」という表現は、技術的な観点では曖昧なので、より範囲が明確になるように議論したい。<br>• 特に産業系の機器ではシステムとしてセキュリティを守る観点で作られたガイドラインに沿って対応している現状を踏まえて議論を進めていきたい。<br>• 製品単位で評価する方針でよいのか、構成部品やプログラムまで評価すべきかについて検討した方がよい。 |
| 制度で用いる適合性評価基準について | • ETSI EN 303 645 はセキュリティ要件として過度に厳密ではないため、基準として適している。<br>• 欧州や米国による国際標準を軸とすることは賛成だが、それらの基準の要素をどれだけ取り入れたかについては明確にしながら検討を進めていただきたい。<br>• 任意制度を前提とするのであれば、評価基準を細分化せず、一つの基準で広い範囲をカバーできた方がメーカーとしてはありがたい。<br>• 国際競争力を考え、国際標準に合わせる点と、日本が優位性を取れる点も含めて、検討していく必要がある。 |
| 制度で用いる適合性評価スキームについて | • 評価や認証にかかる費用及び期間を算出する必要がある。認証要件や評価品質を均一化するための方法論によっても、取得期間やコストは変わる。 |

| カテゴリ | | 主なご指摘事項 |
|---|---|---|
| | | • IoT 製品は製品寿命が長くないため、サーベイランスの視点から更新制度を設けるかについては検討が必要である。<br>• S マークの知名度を活用するメリットは理解するが、既存のマークと新しいマークは違う意味を持つことをはっきりさせた方がよい。 |
| その他 | 制度の目的 | • 誰に対してどのようなメリットを与えるために本制度を立ち上げるか、前提条件を関係者で共有する必要がある。<br>• 認証を取ることでどのようなメリットがあるかについて、投資対効果として考え、市場原理を考慮して制度設計を行う必要がある。 |
| | プロモーション | • 多少高価でもセキュリティを講じる IoT 製品が積極的に購入されるような社会の仕組みの構築や制度のプロモーションに向けた具体的な検討をお願いしたい。 |
| | インセンティブ | • 調達要件として市場を守るといった取組を行えれば、足並みを揃えて本制度を普及させることができるのではないか。<br>• セキュリティを自ら守る必要があるとメーカーに認識いただかなければ、本制度は普及しないのではないか。<br>• メーカーや販売側に対して適切なインセンティブを設けることと、購入する側が安心できる製品を適切に選択できることの両立が、重要だと認識している。<br>• 海外メーカーが日本での販売に躊躇しないようにしていただきたい。国際的に商品展開をするベンダーの競争力を削がないようにすることが重要である。 |
| | 事案への対応 | • 消費者のセキュリティに関する利益を守る人はたくさんおり、損害が生じた場合に補填を行う保険制度も社会的な仕組みとして確立している。<br>• 事故により消費者から訴えられた場合、ステークホルダーが複数存在する可能性があるため、広く考慮や目配りが必要である。 |

### （3）第 3 回有識者検討会

第 3 回の有識者検討会で挙げられた主な意見は表 5.3-4 に示すとおりである。中間とりまとめ（案）の記載内容について、制度が果たすべき役割や目標、消費者における状況についての言及を求める意見が挙げられた。政府の関与や検討体制のあり方について、検討委員会の体制に関する意見が複数挙げられたほか、産業競争力強化や国際競争力強化の見据えた政府の関与のあり方についても意見が挙げられた。IoT 製品ベンダーの能動的な制度活用を促す仕掛けについて、認証機関に対する支援の必要性について意見がなされた。適合性評価済製品におけるセキュリティ事案への対応について、評価済製品における責任分界に関して意見が挙げられたほか、サーベイランスの必要性に関する意見が挙げられた。適合性評価のスキーム（方式）について、検討会では、以下の 2 つの方式の可能性を提示した。

- 方式 1：広範な IoT 製品が活用可能な統一的なスキーム（既存スキームの活用も考慮）を用意し、レベル 1（IoT 製品において最低限求められる対策レベル）については、統一的なスキームで適合

性評価・マーク等の付与を行う。より高いレベル(2,3・・・)に関する適合性評価を行う場合のみ、既存スキームにて適合性評価・マーク等の付与を行う。

- 方式 2:レベル 1 の基準を各スキームに落とし込み、それぞれのスキームにおいて適合性評価・マーク等の付与を行う。

各方式の是非について様々な意見が挙げられたが、制度の構築のスピード感や海外のスキーム等を踏まえ、方式 1・2 のハイブリッド方式を望む意見が複数挙げられた。

表 5.3-4 適合性評価制度に関する第 3 回有識者検討会で挙げられた主な意見

| カテゴリ | 主なご指摘事項 |
|---|---|
| 中間とりまとめ(案)の記載内容について | • 産業競争力の強化・支え、デバイス・アプリケーション・制御の関係で支えられる国民生活の安心・安全の実現、そしてそれを通じた世界への貢献といった、本制度の仕組みや議論が果たすべき役割や目標について、一言触れられているとよい。<br>• 産業経済や社会の活力向上に資するという積極的な位置づけで規制についても検討を行う必要があると思われる。<br>• セキュリティに関する知識やスキルを持っていない消費者が少なくないことについても言及いただきたい。 |
| 政府の関与や検討体制のあり方について | • 本検討会で議論を行った点について見識を持つ学者や有識者を交え、IoT 製品を供給する実業界に力点をおいた実務的な委員会を構築いただきたい。<br>• 専門的な知見を有した人を集めた部会に分けて議論を行うのも一つの方法と考える。<br>• 従来とは異なる、国際的に今後必ず必要となるような、IoT 時代における責任分担のあり方、すなわち誰かの責任を追及することなく被害が公平に分担される社会の構築に資する制度の提言について、日本がリードできるとよい。<br>• 米国と EU の Trade and Technology Council で IoT セキュリティに関するワーキンググループを立ち上げ、同じ土俵で議論したいという話がある。日本もその土俵の中で同じような議論をした方がよいと思う反面、日本の特徴を出していく必要がある。<br>• 医療系の JIS T において、ライフタイムを考えて製品を作ることが産業規格化し始めているため、このような動向を注視しながら検討を行う必要がある。<br>• NITE はセーフティ領域を管轄する組織である。セキュリティ領域に関する経済産業省の関係組織で言えば、IPA が最も馴染みある。<br>• すぐに着手するという意味で、JISEC の仕組みを適用すればよいのではないかと考える。<br>• 認定機関と認証機関の役割分担について、ISO の様々な規格との関係で決まったものはあるが、それに必ずしも囚われる必要はないと思われる。政府の関与のあり方も含めて、検討いただきたい。 |
| IoT 製品ベンダーの能動的な制度 | • IoT 機器に対して広く対応していく認証機関を後押ししなければ、うまく制度が回らないと考えている。 |

| カテゴリ | 主なご指摘事項 |
| --- | --- |
| 活用を促す仕掛けについて | • 本制度をプロモーションする上で、2025 年の大阪万博が期待できると考えている。 |
| 適合性評価済製品におけるセキュリティ事案への対応について | • IoT 機器のライフタイムを考えると、サーベイランスまで要求する必要はなく、一回きりの認証でも十分と考える。厳密さばかりを意識しない形を検討いただけると、より良い制度設計ができると思われる。<br>• 製造物責任に関する明確化や深掘りの議論が今後なされてもよいのではないか。サポート期間・期限に関しても、責任に伴って議論する必要がある。任意制度からでよいと考えるが、対策を講じていたことを示すことにつながる制度になればよい。<br>• 保険も含めてリスクをどう考えるかご意見を伺う中で、購入者や利用者に対して本制度を通じて、技術的な担保とは別の安心を提供するためにはどうすべきか議論することが大きな論点になると感じた。 |
| 適合性評価のスキーム(方式)について | • 産業界の必要性やニーズに従って、進められるものを進めていくという点では、方式 2 が適していると考えている。<br>• 早く制度が構築できるよう順番に取組み、最終的には方式 1 と方式 2 のハイブリッドになることがベストだと考えている。<br>• 最低限のレベルを統一的なスキームでカバーする方式 1 の方が望ましいと考える。日々新しい攻撃手法が出てくるため、それに応じてセキュリティ要件も早いペースで更新していく必要がある。その意味では、統一的に管理されている方が、実効的なセキュリティ評価スキームになると考える。<br>• 米国では、方式 1 と方式 2 の間をとった方式 1.5 のようなスキームを採用しており、統一的なクライテリアが方式 2 の下に存在するような形である。本制度でも、そのような方式 1.5 を採用するのがよいと思われる。<br>• 業界や機種によって大きな違いがないのであれば、方式 1 の方がよいと考える。統一的な基準で全体として取り組むべきことを決めた方がよいと思われる。<br>• 一般的な規格体系として、IEEE でもよくあるように、全体を統括するマザー規格があり、各業界・各分野の規格はそれにぶら下がるという形はある。どのようにエンドースするかが検討できれば、制度としてまとまるのではないか。<br>• 方式に関わらず、消費者が理解しやすいような制度・スキームを構築いただきたい。<br>• 万が一レベル 1 が機能しなくなった場合、レベル 2 とレベル 3 でカバーできるのか否かについては整理すべきである。 |
| その他 | • 欧州でサイバーレジリエンス法の議論が行われているが、同じような課題が生じると思われる。彼らがどのように整合を取ろうとしているか、経済産業省に調べていただき、共有いただけるとありがたい。 |

## 5.4 構築すべき適合性評価制度の概要

有識者検討会での議論を踏まえ、構築すべき適合性評価制度の位置づけ、制度の対象とする製品範囲、制度で用いる適合性評価基準、制度で活用する適合性評価スキームの概要について記載する。また、各項目について、制度の構築に向けて今後議論が必要な事項を以降に示す。

### 5.4.1 制度の位置づけ

有識者検討会での議論を踏まえると、適合性評価制度はまずは任意制度として運用することが適当である。なお、任意制度として運用を開始しつつも、制度の浸透・活用の程度、国内 IoT 製品ベンダーによる対応状況、IoT 製品に対する脅威の状況、諸外国の取組との整合性や国際的な動向等によっては、任意制度で措置されていた製品類型に対し、法令に基づく義務化に向けた検討を新たに行うことも必要になり得ると考えられる。なお、適切なルール設計は産業活動や社会の活力向上にもつながるものであるため、こうした点も義務化に向けた検討を新たに行う場合に踏まえるべき重要な観点である。

### 5.4.2 制度の対象とする製品範囲

有識者検討会での議論を踏まえると、適合性評価制度の対象製品範囲は「直接的[28]又は間接的[29]にインターネットに接続する製品」とすることが適当である。その上で、いかなる製品を対象にするかについては、各製品が有するリスクや、事業への影響、普及効果、既存制度等を考慮し、精緻に検討を行っていく必要がある。

### 5.4.3 制度で用いる適合性評価基準

有識者検討会での議論を踏まえると、適合性評価制度で用いる適合性評価基準については、国際的な標準を参照の上、国際的な標準と整合的な形で構築していくことが適当である。その上で、具体的な適合性評価基準の策定に当たっては、どのような体制で検討を行っていくか、いくつかのリスクレベルが想定されるところどの程度の基準を策定するべきか、いかなる製品類型に対しどのような考え方で基準を適用していくか、等の考え方について、国内外の関連する動向を踏まえつつ、詳細に検討を行っていく必要がある。

### 5.4.4 制度で活用する適合性評価スキーム

---

[28] 「直接的にインターネットに接続する製品」とは、総務省「端末設備等規則（省令）」第三十四条の十の対象となる製品を指し、インターネットプロトコル（IP）の一部を構成する通信プロトコルを使用してインターネットに直接接続してデータの送受信を行う製品を指すことを想定する（ルーター、ネットワークカメラ等）。

[29] 「間接的にインターネットに接続する製品」とは、以下のいずれかに該当する製品を指すことを想定する。ただし、製品を他製品に接続するためにのみ使用される電線又はケーブルから成る製品は除外することを想定する。

1） インターネットプロトコル（IP）の一部を構成する通信プロトコルを使用して「直接的にインターネットに接続する製品」に接続し、データの送受信が可能である製品

2） 2 つ以上の製品が併せて利用されることを想定しており、少なくとも 1 つの製品（「上流製品」という。）が「直接的にインターネットに接続する製品」に接続可能であり、それ以外の製品（「下流製品」という。）が上流製品に接続してデータの送受信を行う場合の下流製品

適合性評価制度の運用に当たっては、既存の評価スキームを活用した制度とすることが適当である。具体的に、どの製品類型に対して、どの既存スキームを活用するかについては、各製品が有するリスクや、事業への影響、普及効果、既存制度等を考慮し、精緻に検討を行っていく必要がある。検討に当たっては、諸外国の制度との連携や、現行制度との整合性、運用能力等について、既存の評価スキームを所掌している機関と丁寧に検討を進めていくことが重要と考えられる。

## 5.5 今後議論すべき事項

適合性評価制度の構築に向け、前節で記載した事項以外にも今後議論すべき事項が存在する。本節では、有識者検討会の意見・議論を踏まえ、制度構築に向けて今後議論すべき事項を記載する。

### 5.5.1 政府の関与や検討体制のあり方

#### （1） 認証機関との連携

複数の既存スキームを活用する場合、適合性評価を行う認証機関が複数となり得ることや、認証取得数の増加に向けては認証機関の適格性が重要となることから、各主体の適格性について、政府のガバナンスが効く構造を構築することが重要となる。

#### （2） 評価基準等を検討する委員会の構築

具体的な適合性評価基準の策定に当たっては、IoT 製品の性質やリスク、海外制度等について専門的な知見が必要となるため、各分野の専門家を招聘し、評価基準等を検討する委員会を設置することが適当と考えられることから、あるべき具体的な体制や方針について、詳細に検討を行っていく必要がある。

#### （3） 政府基本方針の策定

認証機関の適格性を向上させる観点や、基準等を検討する委員会のガバナンスの観点、複数になり得る認証機関の方向性を束ねる観点、企業の社会貢献の観点等から、政府は基本方針のような形で大きな方向性を示していく必要がある。

### 5.5.2 IoT 製品ベンダーの能動的な制度活用を促す仕掛け

#### （1） 各種調達要件との連携、消費者に対する需要喚起策

ベンダーの能動的な制度活用を促す仕掛けとして、各種調達要件[30]との連携や消費者に対する需要

[30] 例えば、政府調達におけるセキュリティの取組として、経済産業省はデジタル複合機、ファイアウォール等の製品類型ごとに考慮すべきセキュリティ上の脅威とそれに対抗するためのセキュリティ要件をまとめた「IT 製品の調達におけるセキュリティ要件リスト」を公開している。IPA では、当該リストの活用方法をまとめた「IT 製品の調達におけるセキュリティ要件リスト活用ガイドブック」を公開している。内閣官房内閣サイバーセキュリティセンター（NISC）では、「IT 調達に係る国等の物品等又は役務の調

喚起策が想定される。今後、各種調達要件と連携について、その効果や、いかなる調達要件とどのように連携すべきか等について、その根拠付けとともに検討する必要がある。

また、消費者に対する需要喚起策についても、適合性評価制度がどう安全・安心につながるのか、適合性の評価がなされていない製品とはどのような差があるのか、等の観点も踏まえ、その効果、他の取組との連携可能性、具体的な喚起方法等について、検討する必要がある。

### （2） 諸外国の適合性評価制度との国際連携

諸外国では IoT 製品の適合性評価制度の検討が進んでおり、この認証取得のために日本企業の負担が増えることが想定されるところ、適合性評価制度と諸外国の制度の連携を図ることで、負担幅を抑えることが重要と考えられる。今後、諸外国制度の動向を踏まえつつ、どの諸外国制度と、どのような国際相互承認方式で連携し、基準について具体的にどのように整合的に連携するか等について、検討する必要がある。

### （3） IoT 製品ベンダーや認証機関等に対する支援策

適合性評価を行うには認証機関やベンダー、消費者等の関係者に様々なコストが発生すると考えられる。まずは、どのような製品類型に対し、いかなる基準を適用することで、関係者にどの程度のコストが発生するかについて実証等を通じて検証する必要がある。その上で、制度普及を後押しする観点から、関係者において発生するコストを抑制するため支援策[31]について、必要に応じて検討する必要がある。

## 5.5.3 適合性評価済製品におけるセキュリティ事案への対応

### （1） 法的な論点整理

適合性評価を受けた製品に脆弱性が見つかり、セキュリティ事案につながるおそれがあることから、適合性評価を受けることでどのような責任分界につながるか、事案発生時にどのような関係者がどのような責任を負う必要があるか、どのような備えをしておくべきか、等について検討する必要がある。利用者の立場から見ても、認証を取得した製品を選んだという説明責任が果たせることは重要であると考えられる。

### （2） リスクに対応するための資源の確保策

事案発生時の法的な責任分担の整理に加え、例えば保険制度のような、事案発生時に対処を適切に

---

達方針及び調達手続に関する申合せ」において、政府機関等が IT 製品を調達する際に、NISC に対してサプライチェーン・リスクの観点から講ずべき措置について助言を求めることを関係省庁間で申合せしている。デジタル庁では、デジタル臨時行政調査会が、規制所管省庁が規制の見直しに当たってどのような技術が活用可能であるかを把握できるよう、アナログ規制の類型と、その見直しに活用可能な技術の対応関係を整理、可視化したテクノロジーマップ等を整備していく予定。

[31] シンガポールが実施しているセキュリティラベリング制度である Cybersecurity Labelling Scheme では、制度開始後 1 年間、適合性評価にかかる申請料を無償とすることで制度活用促進を図った。この結果、2023 年 2 月時点で 230 製品以上にラベルが付与されている。

行い、被害救済や原因是正につながる資源の確保策についても、どのような策が効果的か等について、必要に応じて検討する必要がある。

### （3） 評価済製品のサーベイランス、取り消し

一度適合性評価を行った後の製品が、市中に流通した際に、不適合の状態でないかを監視（サーベイランス）し、不適合であった場合には取消措置を行える制度[32]を整えることは、粗悪な製品の流通を防止することに有効であると考えられる。一方で、特にサーベイランスについて、IoT 製品のライフサイクルによっては、必ずしもそぐわない場合もあると想定される。したがって、現行制度の状況や、どのような製品類型を対象とするか、どのような者が運用するか、どのような仕組みとするか、適合性評価結果の有効期限についてどう考えるか、どの程度コストが発生するか、等の想定される基本的な事項について、必要性も含めて検討をする必要がある。

[32] 例えば、シンガポールのラベリング制度では、ラベル取得済み製品に対する無作為のサーベイランスが実施され、基準に適合していないと判断される場合にはラベルの取り消しがなされる。ドイツのラベリング制度においても、ランダムサンプリングに基づき基準に適合しているかが確認され、申請内容に反していることが明らかになった場合には、製品ベンダーに対して監査が行われる可能性がある。

令和３年度補正中小企業サイバーセキュリティ対策促進事業

IoT 機器脆弱性検証事業

報告書

2023 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL (03)6858-3578

（様式２）

# 二次利用未承諾リスト

令和３年度補正中小企業サイバーセキュリティ対策促進事業（ＩｏＴ機器脆弱性検証事業）報告書

令和３年度補正中小企業サイバーセキュリティ対策促進事業（ＩｏＴ機器脆弱性検証事業）

株式会社三菱総合研究所

| 頁 | 図表番号 | タイトル |
|---|---|---|
| 3 | 図2.1-1 | ScanNetSecurity掲載記事 |
| 4 | 図2.1-2 | JapanSecuritySummit Update掲載記事 |
| 5 | 図2.1-3 | 日経XTech広告 |
| 63 | 図5.1-6 | 豪州BETAの調査で使用した3種類のセキュリティラベル及び製品選定増加率 |
| 64 | 図5.1-7 | 豪州BETAの調査による各セキュリティレベルにおける製品選択の増加率（%） |
| 64 | 図5.1-8 | UCLの調査で使用した3種類のセキュリティラベル及び製品選定増加率 |