経済産業省　御中

令和3年度サイバー・フィジカル・セキュリティ対策促進事業

先進的手法を用いたセキュリティ検証及び検証サービスビジネスの発展に関する調査

報告書

三菱総合研究所

デジタル・イノベーション本部

2022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

近年、IoT や AI 技術が普及するにつれ、これらを活用して産業構造の変化を先導する取組が世界で進展している。我が国が提唱する「Society 5.0」においては、サイバー空間とフィジカル空間を高度に融合させ、経済発展と社会的課題の解決を両立することを目的としている。一方で、サイバー空間とフィジカル空間が融合することは、サイバー空間での出来事が、フィジカル空間により大きな影響を及ぼすことにつながりうる。実際、これまでサイバー空間に閉じていたサイバー攻撃が、ネットワーク化された機器を通じて現実社会に悪影響を及ぼす事例も発生している。加えて、そのようなサイバー攻撃は、IoT 機器の増加により、今後、より身近な脅威となっていくことが考えられる。こうした状況を踏まえれば、Society 5.0 の実現を促進する観点からは、IoT 機器について十分なセキュリティを確保すること、そのために IoT 機器の脆弱性等について適切な検証を行う基盤を構築することが重要である。

また、そのような基盤の構築は、我が国のイノベーションを支えるサイバーセキュリティビジネスの強化という観点からも重要である。この点については、2018 年に閣議決定したサイバーセキュリティ戦略に基づく、2019 年度の行動計画「サイバーセキュリティ 2019」（令和元年 5 月 23 日、サイバーセキュリティ戦略本部）においても、「我が国における検証等を通じて Society 5.0 を支える信頼の価値を創出するというコンセプト、“Proven in Japan”を旗印として、新たなセキュリティ技術の有効性を検証・評価する仕組みを検討するとともに、IoT 機器等の信頼を高度に検証するハイレベルな検証サービスの実証等を通じ、世界に貢献する高水準・高信頼の検証サービスを拡大するための包括的な検証基盤を構築する等の取組を進めていく」旨がうたわれている。

そこで本調査では、我が国における包括的なサイバーセキュリティ検証基盤の構築に資するために、昨年度に引き続き国内外の IoT 機器等に対する先進的手法を用いた脆弱性等の検証技術等について調査を行い、セキュリティ検証方法の技術動向や、機器ごとに効果的な検証手法等の考え方を整理し、検証サービス事業者等に向けたガイドラインを拡充した。さらに、我が国における検証サービス事業の効果・信頼性を向上させ、検証サービスビジネスを重要な産業として活性化させることを目的に、信頼できる検証主体（検証者・検証サービス事業者等）を確認する仕組み等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） IoT 機器等に対する先進的手法を用いた脆弱性等の検証の現状に関する調査
（2） 検証サービスに係るガイドラインの拡充
（3） 検証サービスビジネスの発展に関する調査・検討

2. IoT 機器等に対する先進的手法を用いた脆弱性等の検証の現状に関する調査

2.1 調査概要

スマート TV、スマートリモコン、自動車 ECU、カーナビゲーションシステム、IoT ゲートウェイ等の脆弱性攻撃の対象となりうる IoT 機器、通信機器、コンピュータ等を計 7 製品程度選定し、それぞれについて民間検証サービス事業者における脆弱性等の検証の取組について調査を行ったうえで、これを比較・整理した。

2.2 脆弱性攻撃の対象となりうる IoT 機器等の選定

まず、脆弱性攻撃の対象となりうる IoT 機器、通信機器、コンピュータ等を選定した。選定に関しては、攻撃者の視点から攻撃の容易性や攻撃が与える影響を検討するために、以下の観点を考慮した。

- 常時アクセス可能なことで攻撃対象となりうるインターネットやモバイルネットワークに常時接続されている機器
- 攻撃によって、機密性・可用性・完全性の観点で利用者に影響が発生する可能性がある機器
- 法人向けの製品に比べてセキュリティレベルが低いことが想定される、個人向けの機器
- 過年度事業において対象としていない機器

これらの観点を勘案し、本調査では、スマートTV、スマートリモコン、カーナビゲーションシステム及び産業用無線ルータ・産業用コントローラの 4 機器区分を選定した。

2.3 民間検証サービス事業者における脆弱性等の検証の取組についての調査

上記の 4 機器に対して、民間検証サービス事業者における脆弱性等の検証の取組について調査を行ったうえで、これらを比較・整理した。検証の取組として、それぞれの機器に対する検証手法及び検証に必要なシステム環境について整理を行い、それらの整理結果に基づき、検証者に求められる知識や能力を分析した。調査・整理は、検証サービス事業者が提供している有償の検証結果報告書に基づき実施した。なお、それぞれの機器について 2 社の検証サービス事業者、一部の機器については 3 社の検証サービス事業者による検証結果報告書を比較して調査した。

2.3.1 スマート TV に対する検証の取組についての調査

スマート TV は、インターネットへの接続機能を備え、多機能・双方向の利用を可能にしたテレビ受像機である。スマート TV のネットワーク構成例を図 2-1 に示す。

以降では、スマート TV に対する代表的な検証手法、検証にシステム環境及び検証に求められるスキル・知識を示す。

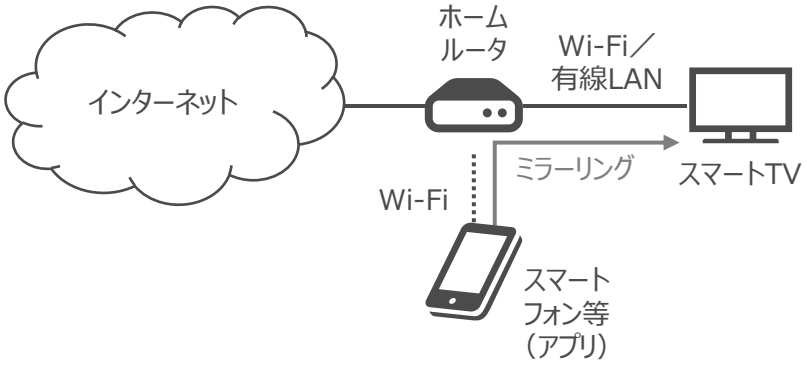


図 2-1 スマート TV のネットワーク構成例

（1） スマート TV に対する検証において用いられる検証基準・検証手法

民間検証サービス事業者が提供している検証結果報告書を比較・整理したところ、スマート TV の一般的な検証手法は主に表 2-1 のとおりであった。三社の検証サービス事業者による検証報告書を調査したが、いずれの事業者においてもまず機器に関する情報収集及び想定脅威の分析を行っていた。加えて、いずれの事業者においても、本体の分解によるハードウェアの調査、ファームウェア解析を実施していた。

表 2-1 スマート TV の一般的な検証手法[1]

検証手法	概要
情報収集	公開情報に基づき機器の仕様を確認するとともに、関連機器に存在する脆弱性の情報を収集する。
想定脅威の分析	情報収集結果に基づき、機器に対して想定される脅威や攻撃手法を検討する。以降の検証では、この脅威につながりうる脆弱性が検出されるかを確認する。
ハードウェア調査	本体を分解し、IC の型番等を確認する。あわせて、フラッシュメモリやデバッグ端子の有無について確認する。
ファームウェア解析	基盤からファームウェアの抽出を試みる。
ネットワークキャプチャ	スマート TV とスマートフォンアプリ間の通信や、スマート TV とクラウドサーバやストレージデバイスとの通信を解析する。

（2） スマート TV に対する検証に必要なシステム環境

調査を行った検証結果報告書では、ハードウェア調査において、前述のとおり分解後に構成物を確認していた。ファームウェア解析においては、フラッシュ ROM からファームウェアを抽出するために ROM プログラマを活用していることが確認された。ファームウェアのバイナリ解析においては、逆アセンブラ・デコンパイラ及びバイナリエディタを活用していることが確認された。そして、ネットワークキャプチャにお

[1] 「情報収集」や「想定脅威の分析」は機器に対する直接的な検証手法ではないが、検証を実施するにあたって重要なプロセスであるため表内に記載している。以降の機器における検証手法の表でも同様である。

いては、パケット解析ツールを活用している旨が記載されていた。

2.3.2 スマートリモコンに対する検証の取組についての調査

スマートリモコンは、家電・照明などを外部のリモコン専用機器やスマホ、AI スピーカーなどからコントロールする機器である。今回調査した検証結果報告書では、特にスマホの専用アプリを用いて宅内の家電・照明など制御可能で、AI スピーカー機能を有していないスマートリモコンを検証していた。スマートリモコンのネットワーク構成例を図 2-2 に示す。以降では、スマートリモコンに対する代表的な検証手法、検証にシステム環境及び検証に求められるスキル・知識を示す。

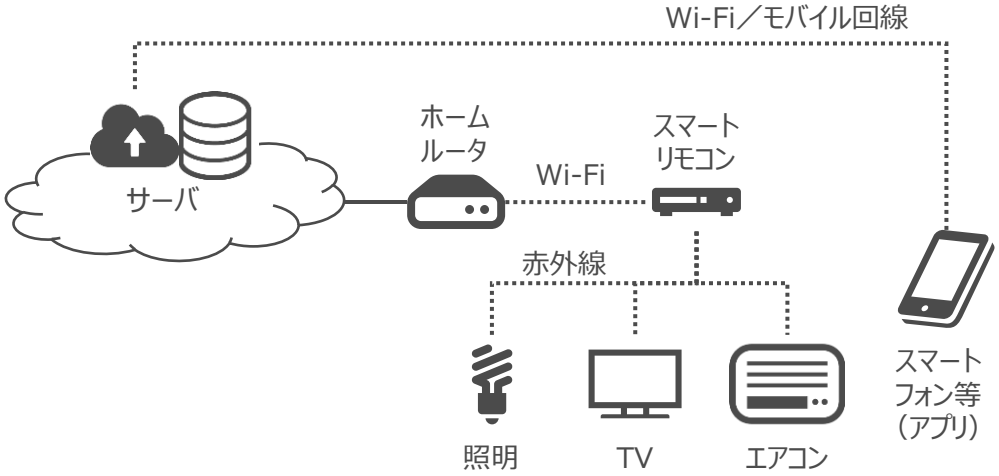


図 2-2 スマートリモコンのネットワーク構成例

（1） スマートリモコンに対する検証において用いられる検証基準・検証手法

民間検証サービス事業者が提供している検証結果報告書を比較・整理したところ、スマートリモコンの一般的な検証手法は主に表 2-2 のとおりであった。三社の検証サービス事業者による検証報告書を調査したが、いずれの事業者においても、まず機器に関する情報収集が行われ、想定脅威の分析を行っていた。また、本体を分解してハードウェア調査を行った後、ファームウェア解析、抽出したファームウェアに対するバイナリ解析が行われていた。また、一部の検証結果報告書では、ネットワークキャプチャに関する検証結果が記載されていた。

表 2-2 スマートリモコンの一般的な検証手法

検証手法	概要
情報収集	公開情報に基づき機器の仕様を確認するとともに、関連機器に存在する脆弱性の情報を収集する。
想定脅威の分析	情報収集結果に基づき、機器に対して想定される脅威や攻撃手法を検討する。以降の検証では、この脅威につながりうる脆弱性が検出されるかを確認する。
ハードウェア調査	本体を分解し、IC の型番等を確認する。あわせて、フラッシュメモリや

検証手法	概要
	デバッグ端子の有無について確認する。
ファームウェア解析	基盤からファームウェアの抽出を試みる。
バイナリ解析	ファームウェアに対してバイナリ解析を行い、実装の不備による脆弱性や既知の脆弱性の存在、攻撃に悪用されうる情報が含まれていないかを確認する。
ネットワークキャプチャ	スマートリモコンと他機器の通信、スマートリモコンとスマートフォンアプリ間の通信や、スマートリモコンとクラウドサーバとの通信を解析する。

（2）スマートリモコンに対する検証に必要なシステム環境

調査を行った検証結果報告書では、ハードウェア調査において、デバッグ端子を特定するためのデジタルオシロスコープを活用していることが確認された。ファームウェア解析においては、フラッシュ ROM からファームウェアを抽出するために ROM プログラマを活用していることが確認された。ファームウェアのバイナリ解析においては、逆アセンブラ・デコンパイラ及びバイナリエディタを活用していることが確認された。そして、ネットワークキャプチャにおいては、パケット解析ツールを活用している旨が記載されていた。

ある検証報告書では、同一機種について二台のスマートリモコンを用意したことが明示されていた。これは一台を分解し、もう一台は通常の目的通り動作させ、検証を行うためである。ハードウェア調査等、物理的破壊を伴う検証の場合、複数台の検証機器を用意することが想定される。

2.3.3 カーナビゲーションシステムに対する検証の取組についての調査

カーナビゲーションシステム（Car Navigation System）は、自動車に搭載される情報機器の一種で、道順を案内することで運転者を支援する機器である。電子的に自動車の走行時に現在位置や目的地への経路案内を行う機器のことであり、USB や Bluetooth 等のインタフェースを有する。カーナビゲーションシステムのネットワーク構成例を図 2-3 に示す。以降では、カーナビゲーションシステムに対する代表的な検証手法、検証にシステム環境及び検証に求められるスキル・知識を示す。

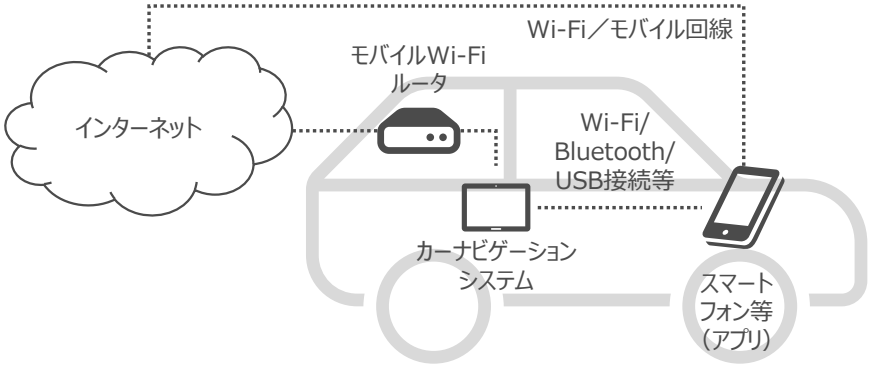


図 2-3 カーナビゲーションシステムのネットワーク構成例

（1） カーナビゲーションシステムに対する検証において用いられる検証基準・検証手法

民間検証サービス事業者が提供している検証結果報告書を比較・整理したところ、カーナビゲーションシステムの一般的な検証手法は主に表 2-3 のとおりであった。三社の検証サービス事業者による検証報告書を調査したが、スマートリモコンの検証手法と大きな差異がないことが確認された。いずれの事業者においても、まず機器に関する情報収集が行われ、想定脅威の分析も行っていた。そのうち二社は、本体を分解してハードウェア調査を行った後、ファームウェア解析、抽出したファームウェアに対するバイナリ解析が行われていた。また、一部の検証結果報告書では、ネットワークキャプチャに関する検証結果が記載されていた。

表 2-3 カーナビゲーションシステムの一般的な検証手法

検証手法	概要
情報収集	公開情報に基づき機器の仕様を確認するとともに、関連機器に存在する脆弱性の情報を収集する。
想定脅威の分析	情報収集結果に基づき、機器に対して想定される脅威や攻撃手法を検討する。以降の検証では、この脅威につながりうる脆弱性が検出されるかを確認する。
ハードウェア調査	本体を分解し、IC の型番等を確認する。あわせて、フラッシュメモリやデバッグ端子の有無について確認する。
ファームウェア解析	基盤からファームウェアの抽出を試みる。
バイナリ解析	ファームウェアに対してバイナリ解析を行い、実装の不備による脆弱性や既知の脆弱性の存在、攻撃に悪用されうる情報が含まれていないかを確認する。
ネットワークキャプチャ	カーナビゲーションシステムとスマートフォンアプリ間の通信を解析する。

（2） カーナビゲーションシステムに対する検証に必要なシステム環境

調査を行った検証結果報告書では、ハードウェア調査において、デバッグ端子を特定するためのデジタルオシロスコープを活用していることが確認された。ファームウェア解析においては、フラッシュ ROM

からファームウェアを抽出するためにROMプログラマを活用していることが確認された。ファームウェアのバイナリ解析においては、逆アセンブラ・デコンパイラ及びバイナリエディタを活用していることが確認された。そして、ネットワークキャプチャにおいては、パケット解析ツールを活用している旨が記載されていた。

2.3.4 産業用無線ルータ・産業用コントローラに対する検証の取組についての調査

産業用無線ルータは、産業用機器を無線LANやインターネットに接続する機器である。産業用コントローラは、産業機器の稼動及び制御する機器である。産業用無線ルータ及び産業用コントローラのネットワーク構成例を図 2-4 に示す。産業用無線ルータは、産業用機器から収集したデータを外部に送信するために無線 LAN やインターネット等の通信やインタフェースが存在している。また、産業用コントローラは、産業機器を制御するために各種の通信やインタフェースが存在している。そのため、通常の産業用機器よりも通信や制御を行う機能を有しているため、これら検証対象の特定や検証手法が適用を考える必要がある。以降では、産業用無線ルータ及び産業用コントローラに対する代表的な検証手法、検証にシステム環境及び検証に求められるスキル・知識を示す。

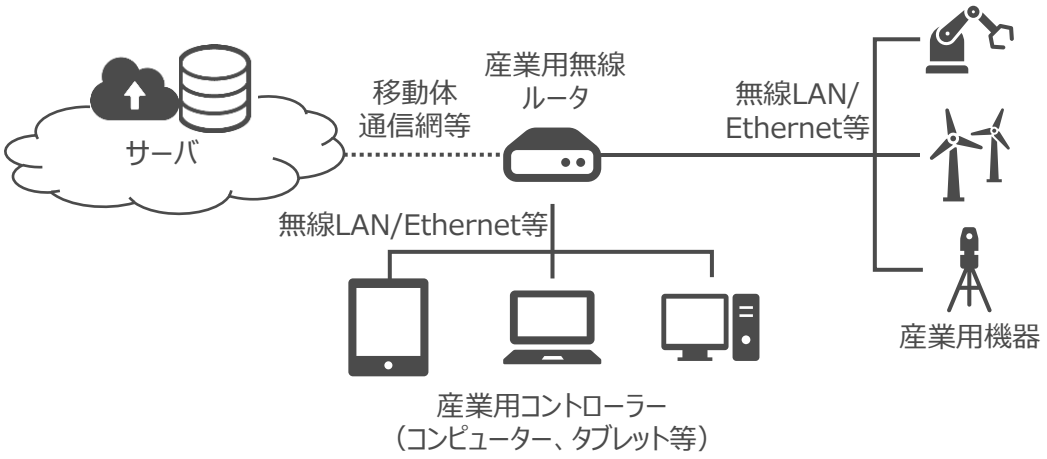


図 2-4 産業用無線ルータ・産業用コントローラのネットワーク構成例

（1） 産業用無線ルータ・産業用コントローラに対する検証において用いられる検証基準・検証手法

民間検証サービス事業者が提供している検証結果報告書を比較・整理したところ、産業用無線ルータ・産業用コントローラの一般的な検証手法は主に表 2-4 のとおりであった。二社の検証サービス事業者による検証報告書を調査したが、スマートリモコンの検証手法と大きな差異がないことが確認された。いずれの事業者においても、まず機器に関する情報収集が行われ、そのうち二社は想定脅威の分析も行っていた。この二社では、本体を分解してハードウェア調査を行った後、ファームウェア解析、抽出したファームウェアに対するバイナリ解析が行われていた。また、一部の検証結果報告書では、ネットワークキャプチャに関する検証結果が記載されていた。

表 2-4 産業用無線ルータ・産業用コントローラの一般的な検証手法

検証手法	概要
情報収集	公開情報に基づき機器の仕様を確認するとともに、関連機器に存在する脆弱性の情報を収集する。
想定脅威の分析	情報収集結果に基づき、機器に対して想定される脅威や攻撃手法を検討する。以降の検証では、この脅威につながりうる脆弱性が検出されるかを確認する。
ハードウェア調査	本体を分解し、IC の型番等を確認する。あわせて、フラッシュメモリやデバッグ端子の有無について確認する。
ファームウェア解析	基盤からファームウェアの抽出を試みる。
バイナリ解析	ファームウェアに対してバイナリ解析を行い、実装の不備による脆弱性や既知の脆弱性の存在、攻撃に悪用されうる情報が含まれていないかを確認する。
ネットワークキャプチャ	産業用無線ルータ・産業用コントローラと外部機器との通信を解析する。
設定用コンソールに対する検証	機器設定用の Web コンソールに対して、検証用コードを実行し、脆弱性の有無を調査する。

（2） 産業用無線ルータ・産業用コントローラに対する検証に必要なシステム環境

調査を行った検証結果報告書では、ハードウェア調査において、前述のとおり分解後に構成物を確認していた。ファームウェア解析においては、フラッシュ ROM からファームウェアを抽出するために ROM プログラマを活用していることが確認された。ファームウェアのバイナリ解析においては、逆アセンブラ・デコンパイラ及びバイナリエディタを活用していることが確認された。そして、ネットワークキャプチャにおいては、パケット解析ツールを活用している旨が記載されていた。

3. 検証サービスに係るガイドラインの拡充

第 2 章の調査結果を踏まえ、令和 2 年度事業で作成したガイドラインの内容の拡充を行った。ガイドラインの拡充においては、IoT 機器等の特徴に応じた脆弱性等の検証に用いるべき先進的手法や、IoT 機器等の種類に特有の脆弱性等の具体的な検証手順等の項目を検討した。具体的には、第 2 章で示した各検証事業者の検証報告書にて把握した検証の手順や検証者に求められる知識・能力等を基に、過年度事業で作成した「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」の付録 5.1「機器固有の検証手法等」において、第 2 章の調査で選定した IoT 機器に関して検証者に求められる知識・能力、具体的な検証手順、検証にあたっての留意点等を追記した。拡充した手引きを本報告書の別紙1に示す。

4. 検証サービスビジネスの発展に関する調査・検討

4.1 調査概要

産業として重要になっていくと考えられる検証サービスビジネスを、更に発展させ利用を促進していくために必要な事項について調査・検討を行った。具体的には、下記の項目について、調査・検討を行った。

- 信頼できる検証事業者を確認する仕組みについて
- 機器のサイバーセキュリティ確保のために求められる取組について
- 検証サービスに係るガイドラインの普及、啓発手法について

4.2 信頼できる検証事業者を確認する仕組みについて

検証等を通じて「Society5.0」を支える信頼の価値を創出するというコンセプト「Proven in Japan」では、IoT 機器等の信頼性を高度に検証する検証基盤を日本に構築する取組みが進められており、このような検証基盤の構築により、IoT 機器等のセキュリティ確保や信頼の繋がりの確保だけではなく、国内における検証事業の活性化にも寄与すると考えられている。検証基盤の構築に向け、検証事業を活性化させるためには、我が国における検証事業の効果・信頼性を向上し、その信頼性を可視化することが求められる。これを踏まえ、有識者検討会を設置し、我が国における IoT 機器等に対する検証事業者の信頼性を可視化する仕組みについて検討を行った。

4.2.1 調査・検討プロセス

調査・検討プロセス概要を図 4-1 に示す。

まず調査方針を整理し、論点を整理した。その後、諸外国の制度で用いられている信頼性要件に関して調査し、検証事業者に求める信頼性要件の素案を検討するとともに、仕組みの活用目的の検討を行った。策定した要件項目案について検証事業者や機器メーカーに対するヒアリングを通じて妥当性を確認し、要件項目を修正した後、第一回有識者検討会において仕組みの活用目的や要件項目の素案について議論した。第一回有識者検討会で得られた意見を踏まえて活用目的や要件項目の再修正を行うとともに、制度化に向けた検討を行った。また、検証事業者や機器メーカーに対するヒアリングを再度実施し、制度運用イメージに関する意見を聴取した。第二回有識者検討会で得られた意見を踏まえ、要件項目案について再度修正するとともに、制度運用に向けたロードマップ等を整理した。この際、制度運用に関連する機関に対してヒアリングを実施し、制度運用に向けた課題等を確認した。

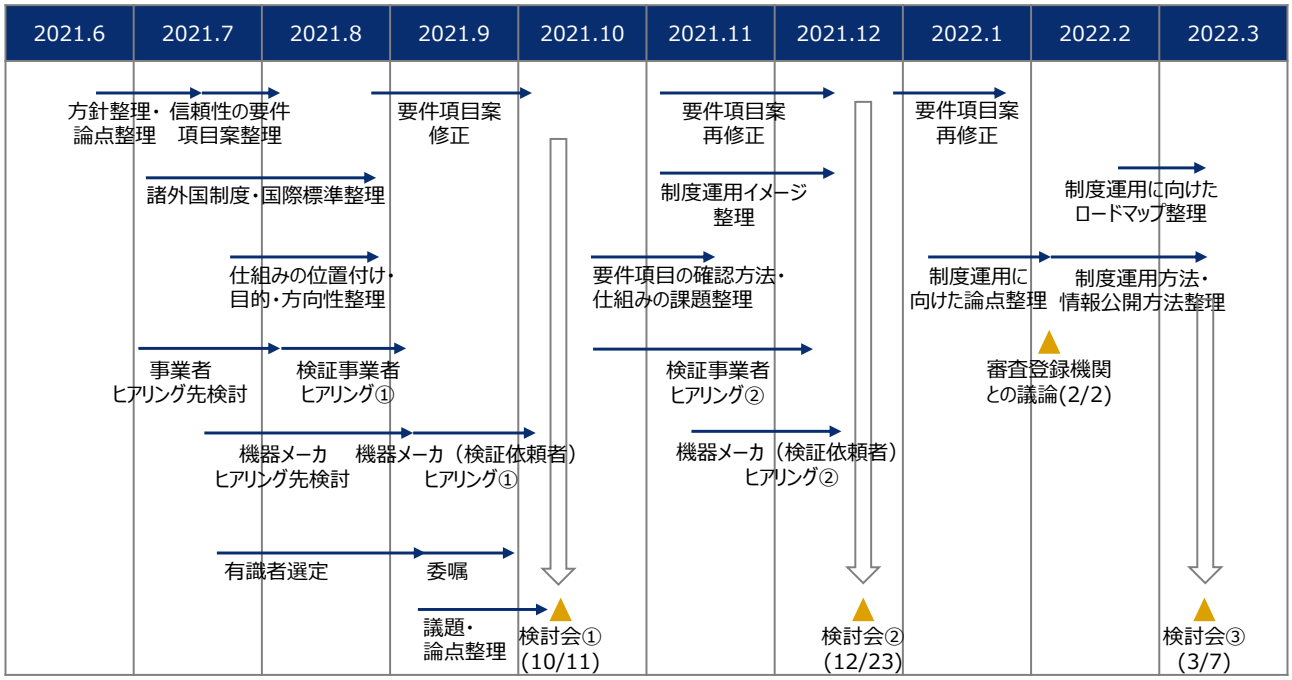


図 4-1 信頼できる検証事業者を確認する仕組みの調査・検討プロセス（概要）

4.2.2 調査・検討における論点

我が国における IoT 機器等に対する検証事業者の信頼性を可視化する仕組みについて、以下の 5 つの論点を軸に調査・検討を行った。

1. 信頼できる検証事業者に求められる要件は何か。また、各要件についてどの程度のレベルが、どの対象に対して求められるか。
2. 構築した仕組みは、どのような目的で、どの依頼者によって活用されるべきか。
3. 検証事業者の信頼性を誰が、どのように確認し、可視化するか。
4. 検証依頼者が、信頼できる検証事業者を選定するために必要な仕組みは何か。
5. 信頼できる検証事業者に対して、どのようなインセンティブが考えられるか。

2 つ目の論点について、当初は 2 つの活用目的を想定した検討を行った。具体的には、活用目的 1 として、IoT 機器等のベンダーが機器に対して検証を実施する際に、適切な品質管理及び情報管理に努めている検証事業者の選定するために活用する目的、活用目的 2 として、重要インフラ事業者、政府機関等が利用する重要機器に対する検証にあたって、高信頼な検証事業者を選定するために活用する目的を検討した。しかしながら、第一回有識者検討会において、これら 2 つの活用目的を一度に議論することが困難であるとの意見が挙げられ、以降は活用目的 1 に対象を絞って調査・検討を行った。

4.2.3 国内外の関連する取組において求められる要件

信頼できる検証事業者に対して求める要件を検討するために、国内外の関連する取組において求められる要件を調査した。具体的には、米国 GSA（General Services Administration：連邦政府の独立機関）、英国 NCSC（National Cyber Security Centre）及び国内の情報セキュリティサービ

ス基準審査登録制度について調査を行った。それぞれの取組の概要を表 4-1 に示す。なお、いずれの制度も、本検討の主な対象である IoT 機器等に対する検証事業者に関連する制度ではないことに留意が必要である。以降では、各取組のスキームや、それぞれの取組において検証事業者等に求められる要件について説明する。

表 4-1 検証事業者に求める信頼性の要件を規定した制度概要

制度名	Highly Adaptive Cybersecurity Services (HACS)	CHECK (IT Health Check Service)	情報セキュリティサービス基準審査登録制度
概要	連邦政府や地方自治体が調達するペネトレーションテストやリスクアセスメントについて、登録されたサービス事業者を紹介する制度	政府機関や重要インフラの IT システムに対してペネトレーションテストサービスを提供する制度	一定の品質基準を満たしていることを客観的に判断し、その結果を公開することで、基準を満たしているサービスを、当該サービスを利用したい事業者が参照できる制度
制度運用主体	米国 GSA	英国 NCSC	経済産業省／IPA
制度の主な目的	政府機関や地方自治体におけるセキュリティサービス調達の簡易化	重要 IT サービスの堅牢性向上	サービス品質の維持・向上への取組評価、情報セキュリティサービス産業の強化
検証実施主体	検証事業者	検証事業者（CHECK Company）／NCSC	情報セキュリティサービス基準適合サービス企業
検証対象	連邦政府、州政府、地方自治体の IT システム	政府機関や重要インフラ（CNI）の IT システム	ユーザー企業、政府機関等の Web アプリ、プラットフォーム、スマートフォンアプリ

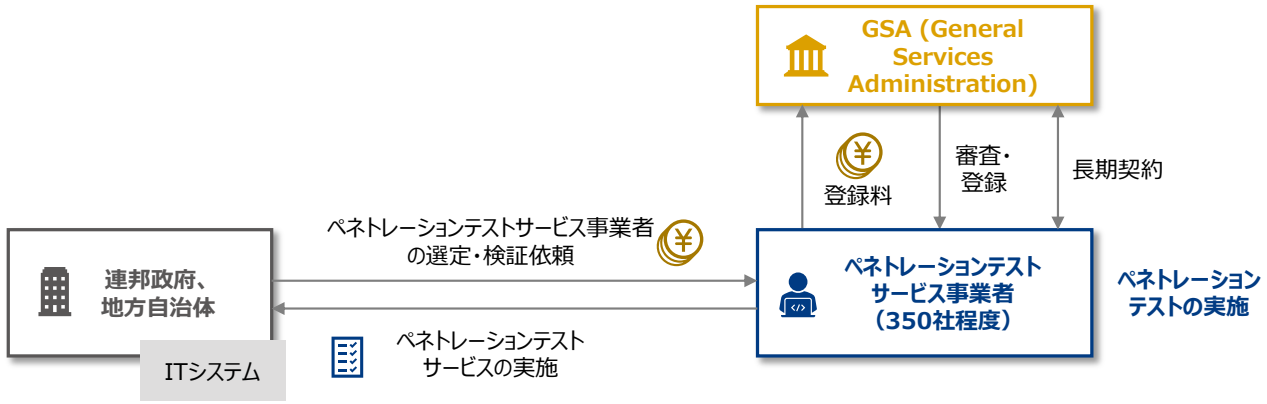
出所）各国制度に関する公開情報に基づき三菱総合研究所作成

（1） 米国 GSA：HACS

米国 GSA は、IT Schedule 70 と呼ばれる、GSA と民間企業との間で政府調達のために長期契約を行うプログラムを展開している。連邦政府や地方自治体が、事前に GSA が登録・契約した民間企業から調達を行うことで、煩雑な手続きを省き、政府調達を迅速にすることが目的であり、HACS は、IT Schedule 70 におけるセキュリティ関連サービスの一つとして位置づけられている。HACS には、ペネトレーションテストサービス、インシデント・レスポンスサービス、サイバーハントサービス[2]、リスク・脆弱性アセスメントサービスの 4 つのサービス分類が存在しており、それぞれのサービスについて、GSA に審査された事業者が登録されている。HACS の制度スキームを図 4-2 に示す。なお、HACS の契約はエバーグリーン契約（Evergreen contracting）を採用しており、契約は 5 年単位で、3 回更新

[2] 脅威インテリジェンスや関連組織でのインシデントの情報等を活用して、対象組織の潜在的な脅威を調査・軽減するサービス。

することが可能である。そのため、最大で 20 年間の契約を結ぶことが可能である。



出所）GSA の IT Schedule 70 及び HACS に関する公開情報に基づき三菱総合研究所作成

図 4-2 米国 HACS 制度のスキーム

HACS のペネトレーションテストサービスでは、GSA は事業者に対して口頭インタビューを実施し、ペネトレーションテストに関する技術的な基礎知識を確認している。具体的に求められる基礎知識を表 4-2 に示す。この表から分かるとおり、特段レベルの高いスキル・知識が求められるわけではない。また、情報管理や品質管理に関する要件は求められていない。口頭インタビューは、事業者に対する質問とシナリオベースでの確認によって構成され、所要時間は 40 分程度とされている。インタビューでは、表 4-2 の要件が確認され、インタビュー回答が要件を満足していると判断された場合には合格となる。

表 4-2 米国 GSA の HACS 制度において求められる要件

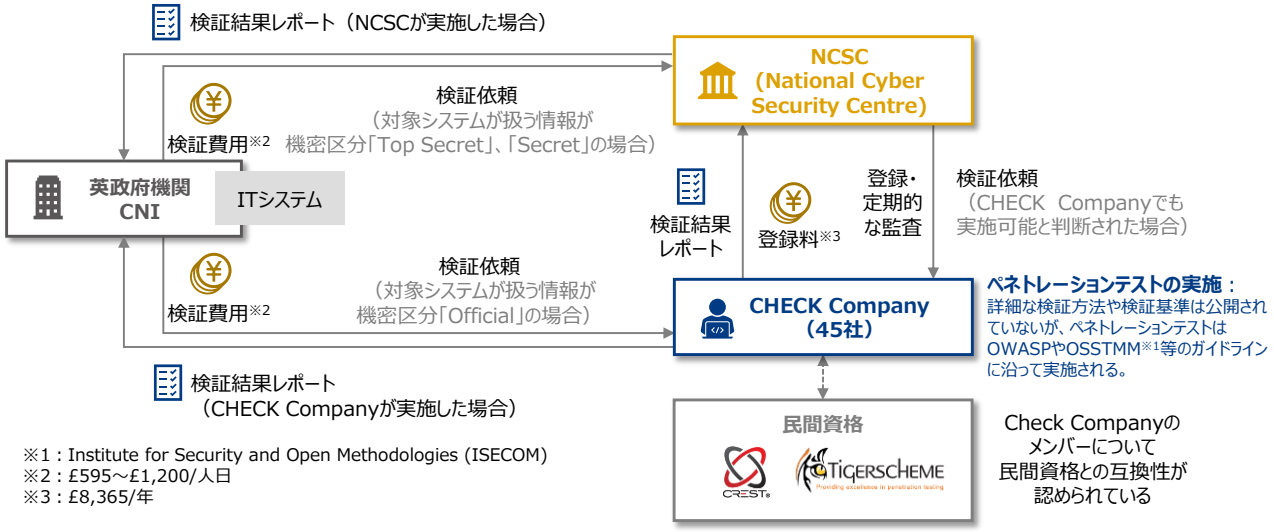
要件分類	要件
責任者・メンバーのスキル・知識	ペネトレーションテストに関する原則、ツール、手法の知識を有していること。（例：Metasploit 等）
	一般的な攻撃手法に関する知識を有していること。（例：フットプリンティング、スキャニング、対象列挙、アクセス権の奪取、権限昇格、アクセス権の保持、ネットワーク・エクスプロイト 等）
	システムの脆弱性やデータの分析に基づき、セキュリティ問題を特定するスキルを有していること。
	あるシナリオに対して、妥当なペネトレーションテスト実施方法を提示できること： • ペネトレーションテストの評価を実施するために、どのようなプロセスと方法を利用するか。 • 脆弱性を発見して列挙するために、どのようなツール、技術、手順を利用するか。 • 特定された脆弱性を悪用するために、どのようなツール、技術、手順を利用するか。 • システムやデータにアクセスした後、新たな攻撃源を確立するために、どのようなツール、技術、手順を利用するか。

要件分類	要件
責任者・メンバーの過去の経験	関連する 3 つのプロジェクト経験を提示できること: • 1 つのプロジェクトあたり、4 ページを超えないこと • プロジェクトにおける作業と結果について詳細に説明すること • プロジェクトにおいて、手法、ツール、手順を説明すること • 法律、規制、基準等への準拠の確からしさを説明すること • 当該プロジェクト経験や資格の確からしさを説明すること
ペネトレーションテスト業務の実施方法	企業のネットワークに対する承認された侵入テストの実施やサポートをすること。
	サイトや企業のコンピュータネットワーク防御に対するポリシー、構成を分析し、規制と企業規則への準拠を評価すること。
	リスクを軽減するための費用対効果の高いセキュリティ管理策の選択を支援すること。

出所)GSA の IT Schedule 70 及び HACS に関する公開情報[3]に基づき三菱総合研究所作成

(2) 英国 NCSC:CHECK

英国 NCSC の CHECK は政府機関や重要インフラの IT システムに対してペネトレーションテストサービスを提供する制度である。一部の機密性の高いシステムを除き、NCSC により審査された CHECK Company と呼ばれる検証事業者によってペネトレーションテストが実施される。英国 CHECK 制度のスキームを図 4-3 に示す。



出所)NCSC の CHECK Service に関する公開情報に基づき三菱総合研究所作成

図 4-3 英国 CHECK 制度のスキーム

CHECK Company として NCSC に登録されるためには、NCSC が定めた要件を満たしているこ

[3] GSA, Factor 5 Oral Technical Evaluation Criteria
https://interact.gsa.gov/sites/default/files/Factor5OralTechnicalEvaluationCriteria.pdf
GSA, Highly Adaptive Cybersecurity Services Webinar
https://interact.gsa.gov/sites/default/files/HACS%20SIN%20Webinar%208.24.16_508.pdf

とを証明する必要がある。CHECK Company として登録されるために求められる要件を表 4-3 に示す。この表から分かるとおり、NCSC が定めた要件には診断技術に関する要件だけでなく、セキュリティクリアランスに関する要件など、「検証事業の信頼性」及び「情報管理に係る信頼性」の両面で厳格な要件が含まれている。

表 4-3 英国 NCSC の CHECK 制度において求められる要件

要件分類	要件
責任者・メンバーのスキル・知識	原則として、CHECK は、特定のシステムの構成技術に対応するために、あらゆる技術的専門知識の分野に対応すること。特に、以下の技術的専門知識を有していること： UNIX、Windows NT、ネットワークプロトコル、ネットワークテストツールの使用、ファイアウォール
	専門知識を獲得していることを示すために、CHECK Company のスタッフのうち少なくとも一名は、NCSC が承認したアサルトコース（実技試験）を含む資格を取得していること。
	すべてのチームメンバーの専門知識を示すために、以下に関する情報を NCSC に提供すること： 学術的な IT 資格、関連する IT 業務経験、IT システム管理の正式なトレーニング、特定のコンピュータ・セキュリティ・トレーニング、実務経験、脆弱性調査経験
責任者・メンバーの過去の経験	すべてのチームメンバーについて、関連する経験、学歴、資格に関する最新の記録を NCSC に提供すること。更新があった場合には、再度 NCSC に提出し、記録を常に最新に維持すること。
責任者・メンバーのセキュリティクリアランス	すべてのチームメンバーは、最低でも SC（Security Check）のセキュリティクリアランス[4]を保持すること。
ペネトレーションテスト業務の準備	CHECK Company は、テスト戦略、テスト計画及びテストで用いるスクリプトを策定し、テストのための適切な準備を確実に行うこと。また、テストの過程で、必要に応じて、戦略、計画及びスクリプトを改良し、さらに発展させること。
	CHECK Company は、顧客との契約締結前に、顧客が使用しているシステムや製品に関する情報を顧客に申告すること。
	CHECK Company は、顧客との契約締結前に、従事するスタッフと顧客との利害関係（例えば、前職での関係 等）を申告すること。
ペネトレーションテスト業務の実施方法	CHECK Company は、外部からの攻撃、内部からの攻撃、他のネットワークノードからの攻撃に関するテストを実施すること。

[4] 「Secret」の情報に頻繁アクセス又は「Top Secret」の情報に稀にアクセスする人員に対するセキュリティクリアランスのレベルで、人員の信用性、完全性、信頼性に係る確認である BPSS（Baseline Personnel Security Standard）と、イギリスにおける犯罪歴チェック、セキュリティチェック、信用調査に基づき付与される。
https://www.gov.uk/government/publications/united-kingdom-security-vetting-clearance-levels/national-security-vetting-clearance-levels#security-check-sc

要件分類	要件
	CHECK Company は、NCSC が助言した脆弱性がある場合には、その脆弱性に関するテストを実施すること。
	CHECK Company は、顧客との契約で定義された脅威、脅威に関連する攻撃モード（ブルートフォース 等）、攻撃モードを構成するパラメータ（弱いパスワードの設定 等）、及び脅威の対象となるシステムコンポーネントについてテストを実施すること。
	CHECK Company は、システムコンポーネントの構成の安全性・信頼性を確認すること。
	CHECK Company は、すべての潜在的脆弱性をテストすることが不可能な場合は、リスクが最大であると考えられるものに優先的にテストを行うこと。
	システムに損害を与える可能性のあるテスト（例：ウイルス感染、悪意のあるコードのリリース、インターネットからダウンロードした未チェックのハッキングスクリプト、許容できないほどの高負荷のネットワーク負荷など）を行わないこと。
	CHECK Company は、顧客との契約において期待されるすべての側面をカバーすること。
	チームリーダーは、ペネトレーションテスト期間中に現場に立ち会うこと。
	CHECK Company は、テスト範囲を最大化するために、パスワードクラッキングツール、ネットワークスキャンツール、サービススキャンツールについては、自動化ツールを用いること。
ペネトレーションテスト結果の報告	CHECK Company は、顧客と合意した取引条件、 CHECK Company の結果及び推奨事項を文書化した報告書を作成し、顧客に提出すること。また、その内容を、1 ヶ月以内に NCSC にも提供すること。
	CHECK Company が利用する特定のツールやサービスに利害関係が発生している場合、同等の能力を有すると想定される代替ツールやサービスの存在を報告書に記載すること。
事業者の品質管理	CHECK の作業で雇用するすべてのスタッフについて、まず NCSC の同意を得ること。
	NCSC による定期的な監査として、CHECK Company の施設、システム、その他の資料に全面的にアクセスすることを許可すること。
	情報保証の国家技術機関である NCSC は、CHECK サービスの運営及び管理に責任を負う。サービスの管理において、NCSC が実施する以下の事項について協力すること： • CHECK Company が、CHECK スキームの最低基準を超えることができるかどうかを毎年評価する。 • CHECK 基準の定義を維持し、推奨されるパブリックドメインの脆弱性情報源の CHECK Company への提供を促進する。

要件分類	要件
	• 定義された CHECK 基準が一貫して達成されていることを確実にするために、CHECK Company の運営を監視する。 • CHECK サービスを管理・推進し、CHECK Company が承認された状態を、そのような企業のリストに掲載して公表する。

出所）NCSC“CHECK service provision guidelines”[5]に基づき三菱総合研究所作成

CHECK Company が対応する必要がある審査や監査等の概要を表 4-4 に示す。この表で示されるとおり、CHECK Company として登録されるためには、NCSC の定めた試験への合格やセキュリティクリアランスの保持に基づき NCSC の同意が必要となるほか、登録後も NCSC の監査を受ける必要がある。

表 4-4 英国 NCSC の CHECK 制度において事業者に求められる対応

要件準拠の確認方法	要員及びチームの審査	民間資格の取得有無	テスト報告書の確認	定期的な監査
実施者	NCSC	CREST、Tiger Scheme、Cyber Scheme 等の民間資格運用者	NCSC	NCSC
実施概要	すべての要員の経験、学歴、資格に関する最新の記録、及びセキュリティクリアランスを保持の保持状況を、NCSC が審査する	筆記試験、多肢選択式試験、6 時間のアサルトコース（実技試験）、そして実技試験から得られた知見を説明するための面接によって構成される試験は 2 日～4 日を要する	CHECK Company が顧客に提示したペネトレーションテスト報告書を、NCSC が確認する	CHECK Company の施設、システム、その他の資料に基づき、NCSC が監査する

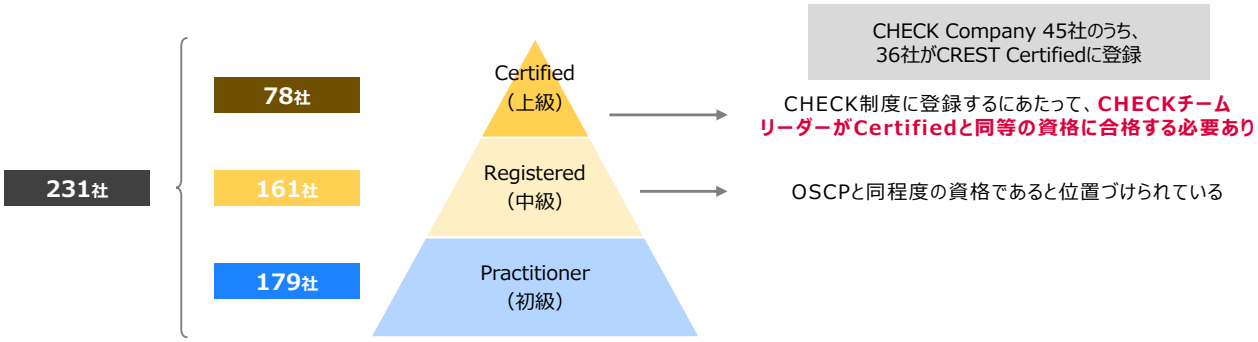
[5] https://www.ncsc.gov.uk/files/CHECK-Service Provision Guidelines.pdf

要件準拠の確認方法	要員及びチームの審査	民間資格の取得有無	テスト報告書の確認	定期的な監査
確認項目	• すべての要員が、CHECK サービスに足る学術的な IT 資格、関連する IT 業務経験、IT システム管理の正式なトレーニング、特定のコンピュータ・セキュリティ・トレーニング、実務経験、脆弱性調査経験等を有しているか • すべての要員が、セキュリティクリアランスを保持しているか	• 技術的な専門知識を有しているか • 法的知識、顧客の要求事項の理解等、管理、倫理、コンプライアンスの側面でのスキル・知識を有しているか • テストの成果を経営者に報告するための文書化やプレゼンスキルを有しているか	• CHECK サービスを実施するにあたって十分な品質を維持しているか	• CHECK サービスを実施するにあたって十分な品質を維持しているか
要件準拠の確認基準	具体的な基準は公開されていない	事前作成レポートに基づく評価、多肢選択式試験、記述試験、実技試験及び面接の 5 つのステージそれぞれにおいて、60%以上を取得すること	具体的な基準は公開されていないが、十分な品質が確保されていない場合、NCSC とのメンバーシップ契約が解除される	具体的な基準は公開されていないが、十分な品質が確保されていない場合、NCSC とのメンバーシップ契約が解除される

出所）NCSC の CHECK Service に関する公開情報[6]に基づき三菱総合研究所作成

[6] NCSC, CHECK service provision guidelines https://www.ncsc.gov.uk/files/CHECK-Service Provision Guidelines.pdf

前述のとおり、CHECK 制度は民間ペネトレーションテスト資格との互換性が認められている。互換性が認められている資格の例として CREST が挙げられる。CREST は、2006 年に英国で設立されたペネトレーションテストに関する業界団体である CREST(The Council of Registered Ethical Security Testers)に基づき実施されている資格制度である。CREST の要員認定資格は 3 段階用意されており、最上級の資格取得によって CHECK 制度の要求事項の一部を満たすことができるため、多くの CHECK Company が CREST の最上級資格を取得している。CREST 制度におけるレベルごとの資格認定者数の比較を図 4-4 に示す。



出所)NCSC の CHECK Service 及び CREST に関する公開情報に基づき三菱総合研究所作成

図 4-4 CREST 要員制度におけるレベル毎の資格認定社数[7]

CREST 認定制度では、技術的な観点だけでなく、情報管理、法律、倫理の観点で審査が行われ、特に最上級の Certified[8]では、高いレベルの要件への遵守が求められる。そのため、登録事業者は限定的である。

CREST 制度では、情報管理や品質管理に関する要件は事業者単位で審査され、技術力や倫理に関する要件はメンバー単位で審査がなされる。審査は事業者とメンバーの単位で行われるものの、認定は事業者単位で行われる。事業者の審査にあたっては、国際標準(ISO/IEC 27000、ISO 9001 等)への準拠証明、品質管理や情報セキュリティに関するプロセス及び手順、苦情対応や利益相反に関するポリシーの提出が必要となるほか、実地監査が行われる可能性もある。また、メンバーの審査にあたって、最上級の Certified の場合、実技試験への合格が必要となる。メンバーの審査では、ペネトレーションテストに関する技術的な知識・スキルだけでなく、プロジェクト管理・リソース管理や法律・コンプライアンス、文書管理や報告書作成に関する知識・スキルも問われる。

CREST 認定事業者は、審査に合格した後、「CREST 苦情対応プロセスへの同意」と「CREST 行動規範への同意」が必要となる。この同意によって、CREST 認定企業において統一的な苦情解決方法が提示されることを保証している。また、メンバーにおける CREST 行動規範への同意によって、それぞれのメンバーが倫理的に行動し、勤務する事業者のポリシー、プロセス、手順を遵守することが求められる。なお、CREST 認定企業は 1 年毎に申請書を再提出する必要があるとともに、3 年毎に新たな審査を受ける必要がある。

Tiger Scheme, Tiger Scheme SST Standards https://www.tigerscheme.org/pdf/sst-standard-v2-5.pdf
Tiger Senior Tester Assessment Notes to Candidates
https://www.tigerscheme.org/pdf/sst-standard-notes-to-candidate-v2-5.pdf

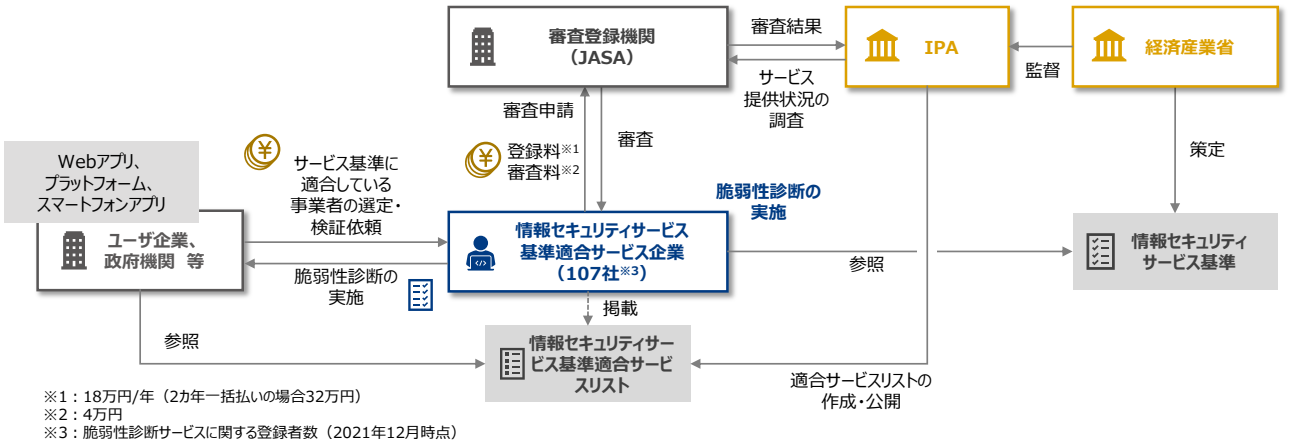
[7] 複数のレベルに登録している事業者も存在するため、登録事業者の総数が各レベルの総和に一致しないことに留意。また登録されている企業は英国企業に限定されない。

[8] 最上級の Certified レベルのみ、“Infrastructure”に関する資格と“Web Application”に関する資格の 2 つが用意されている。

（3）IPA・経済産業省：情報セキュリティサービス基準審査登録制度

「情報セキュリティサービス審査登録制度」は、情報セキュリティサービスについて一定の品質の維持向上が図られていることを第三者が客観的に判断し、その結果を台帳等で公開し、利用者が調達時に参照できるような仕組みである。この制度のスキームを図 4-5 に示す。サービス分野として、「情報セキュリティ監視サービス」、「脆弱性診断サービス」等の 4 つが定義されている。「脆弱性診断サービス」には、「Web アプリケーション脆弱性診断」、「プラットフォーム脆弱性診断」、「スマートフォンアプリケーション脆弱性診断」の 3 つのサービス区分が存在しており、107 社（2021 年 12 月時点）がサービス基準に適合した「情報セキュリティサービス基準適合サービス」として登録されている。IoT 機器等に関するサービス区分は現状存在していない。

求められる要件に関して、2022 年 1 月 31 日に情報セキュリティサービス基準第 2 版が公開[9]された。この基準は 2022 年 4 月 1 日に施行となる。第 2 版の改訂に際して、情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示が新たに追加され、具体的な例示内容について追加が行われた。



出所）情報セキュリティサービス基準及び情報セキュリティサービス基準審査登録チェックリストに基づき三菱総合研究所作成

図 4-5 情報セキュリティサービス基準審査登録制度のスキーム

（4）国内外の関連する取組を踏まえた要件項目の素案

米英日の 3 つの制度で求められる要件やそのレベル、要件に遵守していることの確認方法等について表 4-5 に示す。それぞれの制度で目的や位置づけが異なるため、差異があることは当然であるが、英国 CHECK 制度では責任者・メンバーのスキル・知識や経験、セキュリティクリアランス、検証業務の実施方法、及び品質管理に関する要件を設け、いずれも高いレベルでの遵守を求めていることが分かる。

[9] 経済産業省、情報セキュリティサービス審査登録制度
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html

表 4-5 各国制度における審査対象・審査対象に求める要件及び当該要件の確認方法

制度名	Highly Adaptive Cybersecurity Services (HACS)	CHECK (IT Health Check Service)	情報セキュリティサービス基準審査登録制度
審査の対象	• 組織 • 検証サービスの責任者 • 検証サービスに係るメンバー	• 組織 • 検証サービスの責任者 • 検証サービスに係るメンバー • 検証サービス自体	• 組織 • 検証サービスの責任者 • 検証サービス自体
審査対象に求める要件	• 責任者・メンバーのスキル・知識 • 責任者・メンバーの過去の経験 • 検証業務の実施方法	• 責任者・メンバーのスキル・知識 • 責任者・メンバーの過去の経験 • 検証業務の実施方法 • 事業者の品質管理 • メンバーのセキュリティクリアランス	• 責任者の資格・経験 • サービスの実施方法の明示 • 事業者の品質管理
求める要件レベル	一定のレベル	ハイレベル	一定のレベル
要件に遵守していることの確認方法	• GSA による口頭インタビューの実施	• NCSC による書類審査 • NCSC による検証結果報告書の確認 • NCSC による定期的な監査 • CREST 等の高度な民間資格の取得	• 審査登録機関(JASA)による書類審査 • JASA による定期的なサーベイランス(監査)
登録事業者数	350 社程度	45 社	107 社

3 つの制度で求められる要件に基づき、本調査における信頼できる検証事業者を確認する仕組みで求められる要件の検討を行った。このために、3 つの制度で求められる要件を整理したうえで、それらの要件に対する国内検証事業者の対応状況を確認した。国内外の制度に基づく信頼性要件項目の素案一覧を表 4-6 に示す。なお、国内検証事業者の対応状況は次項で記載する。

表 4-6 国内外の制度に基づく信頼性要件項目の素案

#	対象	分類	要件項目
1	組織	企業概要	IoT 機器等のセキュリティ検証サービスの概要を提出すること。

#	対象	分類	要件項目
2	組織	実績	一定期間における IoT 機器等のセキュリティ検証サービスの実施件数（案件数）を提出すること。
3	組織	実績	過去に実施した IoT 機器等に対する検証結果報告書のコピーを提出すること。（ただし、機器を識別可能な情報や脆弱性に関する情報はマスクすること。）
4	組織	セキュリティ対策	組織が、ISMS と同等のセキュリティ対策を実施していることを証明すること。（ISMS 認証証明書のコピーの提出等）
5	組織	セキュリティ対策	組織における情報セキュリティポリシーのコピーを提出すること。
6	組織	セキュリティ対策	組織における、検証サービスによって検出された脆弱性情報の管理に関するポリシーのコピーを提出すること。
7	組織	セキュリティ対策	組織における、検証サービスに関する機密情報の管理（例：検証対象となる IoT 製品に関する情報 等）に関するポリシーのコピーを提出すること。
8	組織	品質管理	組織が、QMS と同等の品質管理対策を実施していることを証明すること。（QMS 認証証明書のコピーの提出等）
9	組織	品質管理	品質管理担当者のリストを提出すること。
10	組織	品質管理	品質管理マニュアルのコピーを提出すること。
11	組織	品質管理	IoT 機器等のセキュリティ検証サービスに関する再委託先のリストを提出すること。
12	組織	品質管理	IoT 機器等のセキュリティ検証サービスにおける、再委託先の利用に関するポリシー（例：再委託先管理に関する社内マニュアル 等）のコピーを提出すること。
13	組織	品質管理	IoT 機器等のセキュリティ検証サービスに関して、苦情対応に関するポリシー（例：苦情対応に関する社内マニュアル 等）のコピーを提出すること。
14	組織	品質管理	IoT 機器等のセキュリティ検証に関する賠償責任保険（例：情報漏洩賠償責任保険 等）の証書のコピーを提出すること。
15	組織	契約管理	利益相反防止に関するポリシー（例：利益相反防止に関する社内マニュアル 等）のコピーを提出すること。
16	組織	教育体制	IoT 機器等のセキュリティ検証サービスに従事する者に対して、年間 20 時間以上の教育又は研修を実施又は受講させていること。（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT、社内講習や自習を含む。）また、この旨が、社内の規定等に明記されていること。

#	対象	分類	要件項目
17	責任者	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、以下をはじめとするセキュリティ検証技術に関するスキル・知識を有していることを、資格や過去の実績等によって証明すること。・ファームウェア解析・バイナリ解析・ネットワークスキャン・既知脆弱性の診断・ファジング・ネットワークキャプチャ・ハードウェア解析
18	責任者	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、攻撃手法に関する知識を有していることを、資格や過去の実績等によって証明すること。
19	責任者	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、コンピュータ、ソフトウェア、ネットワーク、ハードウェア、OS 等の IT に関する基礎的な知識を有していることを、資格や過去の実績等によって証明すること。
20	責任者	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、脅威分析・リスク評価に関する知識を有していることを、資格や過去の実績等によって証明すること。
21	責任者	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、プロジェクト管理に関する知識を有していることを、資格や過去の実績等によって証明すること。
22	責任者	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、法律・コンプライアンスに関する知識を有していることを、資格や過去の実績等によって証明すること。
23	責任者	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、リソース管理・スコープ管理に関する知識を有していることを、資格や過去の実績等によって証明すること。
24	責任者	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、リスク管理に関する知識を有していることを、資格や過去の実績等によって証明すること。
25	責任者	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスの責任者に関して、文書管理に関する知識・文書作成スキルを有していることを、資格や過去の実績等によって証明すること。
26	責任者	過去の経験	IoT 機器等のセキュリティ検証サービスに責任者に関して、関連する経験、学歴、資格、受賞歴に関する最新の記録を提供すること。また、セキュリティ検証や関連する IoT 機器等の開発等について 5 年以上の経験を有していること。

#	対象	分類	要件項目
27	責任者	資格	IoT 機器等のセキュリティ検証サービスの責任者において、以下に例示する内容相当の資格を有していること。 ・ 情報処理安全確保支援士 ・ CISSP（Certified Information Systems Security Professional） ・ CISA（Certified Information Systems Auditor）
28	責任者	資格	IoT 機器等のセキュリティ検証サービスの責任者において、以下に例示する内容相当の資格を有していること。 ・ CEH（Certified Ethical Hacker） ・ GIAC（Global Information Assurance Certification） ・ GXPN（GIAC Exploit Researcher and Advanced Penetration Tester） ・ OSCP （Offensive Security Certified Professional） ・ OSCE（Offensive Security Certified Expert） ・ OSEE（Offensive Security Exploitation Expert） ・ CompTIA PenTest+
29	責任者	教育実績	IoT 機器等のセキュリティ検証サービスの責任者において、以下に定める教育及び研修等のいずれかを実施又は受講していること。 ・ JNSA, ISOG-J, OWASP 等の専門家コミュニティの講師・リーダーの経験者 ・ SANS Security Courses （504, 542, 560）の研修を終了した者
30	メンバー	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、以下をはじめとするセキュリティ検証技術に関するスキル・知識を有していることを、資格や過去の実績等によって証明すること。 ・ファームウェア解析 ・バイナリ解析 ・ネットワークスキャン ・既知脆弱性の診断 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
31	メンバー	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、攻撃手法に関する知識を有していることを、資格や過去の実績等によって証明すること。

#	対象	分類	要件項目
32	メンバー	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、コンピュータ、ソフトウェア、ネットワーク、ハードウェア、OS 等の IT に関する基礎的な知識を有していることを、資格や過去の実績等によって証明すること。
33	メンバー	技術的スキル・知識	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、脅威分析・リスク評価に関する知識を有していることを、資格や過去の実績等によって証明すること。
34	メンバー	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、法律・コンプライアンスに関する知識を有していることを、資格や過去の実績等によって証明すること。
35	メンバー	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、リスク管理に関する知識を有していることを、資格や過去の実績等によって証明すること。
36	メンバー	非技術的スキル・知識	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、文書管理に関する知識・文書作成スキルを有していることを、資格や過去の実績等によって証明すること。
37	メンバー	過去の経験	IoT 機器等のセキュリティ検証サービスに従事するメンバーに関して、関連する経験、学歴、資格、受賞歴に関する最新の記録を提供すること。また、セキュリティ検証や関連する IoT 機器等の開発等について 3 年以上の経験を有していること。
38	メンバー	資格	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、以下に例示する内容相当の資格を有していること。 ・ 情報処理安全確保支援士 ・ CISSP（Certified Information Systems Security Professional） ・ CISA（Certified Information Systems Auditor）
39	メンバー	資格	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、以下に例示する内容相当の資格を有していること。 ・ CEH（Certified Ethical Hacker） ・ GIAC（Global Information Assurance Certification） ・ GXPN（GIAC Exploit Researcher and Advanced Penetration Tester） ・ OSCP （Offensive Security Certified Professional） ・ OSCE（Offensive Security Certified Expert） ・ OSEE（Offensive Security Exploitation Expert） ・ CompTIA PenTest+

#	対象	分類	要件項目
40	メンバー	教育実績	IoT 機器等のセキュリティ検証サービスに従事するメンバーにおいて、以下に定める教育及び研修等のいずれかを実施又は受講していること。 ・ JNSA, ISOG-J, OWASP 等の専門家コミュニティの講師・リーダーの経験者 ・ SANS Security Courses (504, 542, 560)の研修を終了した者
41	サービス	準備	IoT 機器等のセキュリティ検証サービスの実施前に検証計画・スケジュールを策定し、検証依頼者とその計画・スケジュールに関してすり合わせをすること。また、依頼者とのすり合わせを実施する旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
42	サービス	準備	IoT 機器等のセキュリティ検証サービスの実施前に検証対象範囲(例:ファームウェアに対する検証のみ実施 等)を明確化し、検証依頼者とその対象範囲に関してすり合わせをすること。また、依頼者とのすり合わせを実施する旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
43	サービス	準備	検出された脆弱性情報の取り扱い方法について、検証実施前に依頼者と合意すること。また、依頼者と合意する旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
44	サービス	事業実施方法	依頼者とすり合わせを行った検証計画に基づき、検証を実施すること。また、検証計画に基づき検証を実施する旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
45	サービス	事業実施方法	すべての潜在的な脆弱性を検証することが困難な場合にリスクが高い箇所を優先的に検証する等、優先度に基づく検証を実施すること。また、優先度に基づき検証を実施する旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
46	サービス	事業実施方法	検証を効率的に実施するために、パスワードクラッキングツール、ネットワークスキャンツール、サービススキャンツール等については、自動化ツールを用いること。また、自動化ツールを用いて検証を実施する旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
47	サービス	事業実施方法	検証にあたって活用する代表的な手法(ファームウェア解析、バイナリ解析、ファジング 等)や確認する項目が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。

#	対象	分類	要件項目
48	サービス	事業実施方法	検証にあたって活用したツール名を依頼者に提示すること。独自ツールを活用した場合には、その必要性や代替候補となりうる既存ツールの名称を依頼者に提示すること。また、これらの旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
49	サービス	結果報告	検証結果報告書をとりまとめること。報告書は、当該案件に従事した者以外の者がレビューを行っていること。また、これらの旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
50	サービス	結果報告	検証結果に関する報告会を開催すること。また、報告会を開催する旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。
51	サービス	結果報告	検証結果に基づき、検証対象機器に求められるセキュリティ管理策の提案を行うこと。また、セキュリティ管理策の提案を行う旨が、サービス仕様が明示された HP、契約・約款、その他の資料等に記載されていること。

4.2.4 国内検証事業者に対するヒアリング結果

国内で IoT 機器等に対する検証事業を展開する 4 社に対してヒアリング調査を行った。主に以下の項目に関してヒアリングを行った。なお、(1)の信頼性要件項目の素案に関する対応可否は、ヒアリングシートに基づき確認した。

(1) 要件項目の素案(表 4-6)に対する対応可否
(2) 信頼できる検証事業者が有するべき要件
(3) 信頼できる検証事業者に求められる要件項目の確認方法
(4) 信頼できる検証事業者を確認する仕組みや制度の登録意向

(1) 要件項目の素案に対する対応可否

表 4-6 で示した信頼性要件項目の素案に対し、国内検証事業者の対応可否を確認した。対応可否について、各項目に対して「対応可能」、「条件付きで対応可能」、「対応不可」の 3 段階を位置づけた。確認の結果、すべての事業者が対応可能である要件は「企業概要の提出」と「過去のサービス実施件数の提出」に限定され、その他の要件に関して対応可能と回答した事業者は、一部の事業者に限定された。具体的には、責任者・メンバーのスキル・知識に関する要件へ対応できる事業者が一部の検証事業者に限定されたほか、組織に関する要件及び検証サービス自体に関する要件について、すべての事業者が対応不可、もしくは「条件付きで対応可能」と回答した要件が多く存在した。

責任者・メンバーのスキル・知識に関する要件へ対応が困難な理由として、求める要件のレベルに応じて対応難易度が変化するものの、資格等については、登録のためのコストや準備の観点で対応は困

難であるとの意見が挙げられた。また、組織に関する要件の対応が不可である理由として、ポリシー等が定義されていないこと、もしくは第三者への開示が不可であることの大きく２つの要因が挙げられた。また、検証サービスの品質に関わる要件項目について、検証依頼者との検証計画のすり合わせや検証計画に則った検証実施等、実務上は実施されている項目が多いものの、ホームページ等でその実施を明示することは対応不可であるとの意見が挙げられた。

（2）信頼できる検証事業者が有するべき要件

信頼できる検証事業者が有するべき要件に関するヒアリング結果は以下のとおりである。

- 「信頼性」に関して、「脆弱性を検出できる」という技術力に関する信頼性の観点と、脆弱性情報等の管理に関する情報管理の信頼性の 2 つが重要となる。自社でも、提案の際に情報管理を徹底していることをアピールしている。
- IoT 機器では、これまでの Web アプリケーションに対する検証とは異なり、ハードウェアとソフトウェアの両面を検証することが必要となり、低レイヤーも含めた様々な知識が必要になる。
- 資格を求める対象について、責任者に求める方針は良いだろう。責任者レベルの方が記載の資格を持っていて損はない。
- 資格や研修制度を技術責任者に求めるのであれば問題ないのではないか。すべてのメンバーに求めることは現実的ではない。技術責任者がマネジメントの観点から管理する方針とすれば、ある程度の技術力は担保されると考えている。
- 技術責任者が有する資格に基づき、適切な管理を行うという前提があるのであれば、メンバーに対する指示も適切に行われると考えられるため、資格を求めるのは技術責任者だけでも問題ないと思われる。
- 市場に出ていない製品をお預かりして脆弱性を検証するため、情報管理に関する取り組みが要件として挙げられる。自社は ISMS を取得しており、機器や得られた情報を厳格に管理していることは顧客に第一に説明している。
- 情報管理に関する信頼性に関して、ISMS の取得が一つの基準となりうる。
- 対応のためのコストが与える影響は事業者の規模で大きく異なる。高いレベルを要求した場合、大規模事業者以外は排除される可能性がある。
- 情報管理の要件について、IPA の「組織における内部不正防止ガイドライン」の項目は対応可能。ただし、既存の情報セキュリティサービス審査登録制度では情報管理に関する要件は明に求めていないところ、他のサービス区分との整合も考える必要がある。
- 品質要件について、既存の情報セキュリティサービス審査登録制度と同等であれば、求める要件として特に問題ないと考える。

諸外国制度で求められる信頼性要件を踏まえ、ヒアリング調査実施前の検討仮説として、検証事業者においては「技術要件」、「情報管理要件」、「品質管理要件」の大きく 3 つの要件が求められると考えた。より具体的には、「技術要件」について、IoT 機器等の検証業務の特性上複数のレイヤーにまたぐ広範な知識・スキルが求められるほか、「情報管理要件」については ISMS が一つの基準になりうると想定した。

ヒアリング調査の結果、検討仮説のとおり、信頼できる検証事業者には技術力だけでなく、情報管理に関する要件や品質管理に関する要件も重要であることが確認された。具体的な技術力の観点について、ハードウェアとソフトウェアの両方に対する技術力の必要性、特に低レイヤーも含めた様々な知識の必要性が提起された。技術要件を求める対象に関して、すべてのメンバーに求めることは現実的ではなく、技術責任者に対してのみ求めることが現実的であるとの意見が挙げられた。あわせて、技術責任者に対して技術要件を求めることで、チーム全体の技術力がある程度担保されるとの意見も得られた。

情報管理要件に関して、ISMS が一つの基準となるとの意見が挙げられた一方で、仮に ISMS のレベルを要求した場合、大手企業以外は対応が困難であることも示唆された。また、既存の情報セキュリティサービス審査登録制度では情報管理に関する要件は明に求めていないところ、仮に審査登録制度と同等のレベルを位置づける場合には、他のサービス区分との整合性についても検討する必要があるとの意見がなされた。品質管理の要件について、既存の情報セキュリティサービス審査登録制度と同等であれば、求める要件として特に問題ないとの意見が得られた。

（3）信頼できる検証事業者に求められる要件項目の確認方法

信頼できる検証事業者が有するべき要件に関するヒアリング結果は以下のとおりである。

- 技術的スキルやサービスの品質を測ることを目的として面接や実技試験を行う場合、評価項目を設定することは困難である。面談で何を見るのか、そして実技試験において何をさせるのかは難しいところである。
- 検証主体を評価するという観点で言えば、一度の実技試験だけで評価すると取りこぼしが生じるかもしれない。
- IoT のペネトレーションテストの技量を測る資格はないが、Web アプリやスマートフォンアプリの脆弱性は IoT に関連しているため、そういった研修経験や資格は評価項目として採用できる。
- 技術的な基礎スキル・知識は情報処理安全確保支援士や CEH で確認できる。
- 検証・診断に関する資格を取得する人が増えている。例えば、CompTIA も候補になりうるのではないか。また、OSCP のほかにも Offensive Security の資格は用意されているため、追記できると良い。
- 技術力の示し方として、資格で示す方法も考えられるが、その他の軸として、組織としての実績等をエビデンスとして示すことも考えられる。
- 過去に検証を実施した機器のリストの提示は可能だが、機器区分の粒度は検討が必要。申請用紙において機器区分を例示し、その記載をベースに事業者にて過去に検証を実施した実績のある機器を記入いただく形が良いのではないか。
- 現状、IoT 系の資格が乏しいため、IoT に関する技能や知識を属人的に測ることは難しい。そのため、検証事業者としての実績を公表することで、必須スキル・知識の有無を示せば良いと考えている。
- 過去に検証を実施した機器の区分を提出することは可能だが、どのように更新するかが課題ではないか。
- IoT 機器の過去の検証報告書は守秘義務のもと作られたものであるため、提出は非常にハードルが高い。

- 過去の検証実績を第三者に提示するにあたっては、概要的な検証内容と一般的なサンプルレポートを提出することしかできない。
- サンプルレポートはほとんどの事業者が用意しており、一般的な検証項目や検証手法を確認できるという点で有用ではないか。検証結果報告書の写しに代替しうると考えている。

前述のとおり、検証事業者においては「技術要件」、「情報管理要件」、「品質管理要件」の大きく 3 つの要件が求められると考えられる。ヒアリングでは、このうち技術要件及び品質管理要件の確認方法について、検証事業者より意見を伺った。

技術力の確認方法について、資格制度による確認、実技試験による確認、面接による確認等、様々な確認方法が想定されるが、実技試験や面接の場合、評価の項目を設定することが困難であるほか、一度の実技試験では、評価の取りこぼしが生じる恐れが示唆された。したがって、資格制度による確認が有効であると想定されるが、IoT 機器等に対する検証にあたっては幅広いスキル・知識が求められるところ、複数の資格が対象資格の候補として提示された。具体的には、情報安全確保支援士、CEH、CompTIA、Offensive Security 関連の資格等が候補として意見された。また、技術要件の確認方法として、資格に基づく方法のほか、組織としての実績も重要になるとの意見が挙げられた。具体的には、検証事業者が過去に実施した検証対象機器の区分を確認することが一案として挙げられた。

品質管理に関する要件の確認方法について、ヒアリング調査実施前の検討仮説として、検証事業者による実際の検証レポートに基づく確認が有効ではないかと考えた。しかしながら、すべてのヒアリング対象検証事業者より、実際の検証報告書を提出することは守秘義務の観点で非常に困難であるとの意見が得られた。代替する確認方法として、事業者が用意するサンプル報告書を基に確認する方法が挙げられた。サンプル報告書では、一般的に検証サービスで活用される検証項目や検証手法が記載されるため、品質管理要件の確認という観点では、実際の検証報告書に基づく確認とほぼ同等の効果が得られることが示唆された。

（4）信頼できる検証事業者を確認する仕組みや制度の登録意向

信頼できる検証事業者を確認する仕組みや制度の登録意向に関するヒアリング結果は以下のとおりである。

- 制度が実際に構築された暁には、自社は登録するであろう。
- 制度が仮に運用された場合、登録されていないことがデメリットになりうる。
- 審査登録制度において、書類審査とはいえ、経産省により設置された委員会で審査し、登録されていることは顧客からの信頼に繋がる。
- 認定者リストに掲載されていることで、依頼者からの信頼の獲得につながり、結果として自社の売上につながることがインセンティブになりうる。
- 制度そのものがメーカーに周知されている必要がある。例えば CISSP は、(ISC)²が積極的に広報し、制度そのものの価値を高める活動を継続的に行っているため、CISSP の信頼性が保たれている。
- 認定取得するか否かは、それを取得することで案件に繋がるかどうかで決まる。例えば、官公庁入札要件に必須化される等、取得しなければならない状況ができるとモチベーションとなる。

- 費用については JASA の所管かと考えているが、既に脆弱性診断サービスで登録されている事業者が、新たに機器検証サービスにも登録する際に手数料がかかるとなると事業者の負担につながるため、ご検討いただきたい。

今回ヒアリングを実施した検証事業者においては、検証事業者の信頼性を確認する仕組みや制度に対して一定の登録意向が確認された。仮に仕組みや制度が運用された際に、登録されていないことがデメリットになりうるとの意見が挙げられたほか、登録されることで顧客の信頼につながり、結果として事業者の売上につながりうるとの意見が得られた。検証事業者が登録するか否かは、登録によって売上につながるかどうかが非常に重要であり、制度が活用されるためには、検証を依頼する立場にある機器メーカーに対して制度を適切に周知することの必要性が意見された。

4.2.5 国内機器メーカーに対するヒアリング結果

国内で IoT 機器等を開発しているメーカー7 社に対してヒアリング調査を行った。主に以下の項目に関してヒアリングを行った。

（1） 検証サービスの利用状況及び課題
（2） 信頼できる検証事業者を選定する際の観点
（3） 信頼できる検証事業者を確認する仕組みや制度の活用意向

（1） 検証サービスの利用状況及び課題

検証サービスの利用状況及び課題に関するヒアリング結果は以下のとおりである。

【メーカー内部での検証状況及び外部検証事業者への依頼状況について】
- セキュリティ検証は、開発者自身が実施しているケースが多い。
- 自社検証により最低限のセキュリティ対策は行っているが、それ以上の対策については顧客の要望に応じて行っている。検証については、顧客のニーズに応じて無償オプション、有償オプションを用意している。顧客からの要望があれば有償で認証取得にも対応する。
- 自社製品に対しては、内部でセキュリティ検証を行う部署を立ち上げ、DevSecOps の形で対応を行っている。
- インターネットから侵入できる製品については、外部の検証事業者に対して検証を依頼している。ブラックボックスで実施しており、攻撃者視点で機器に対してアクセスできるかを主に検証する。それ以外の製品についても、自社内で検証を行っている。
- セキュリティ検証は自社内で実施しているが、そのうえでさらに、重要な製品やリスクが高い製品に対して外部の検証サービスを利用している。具体的には、自社ビジネスにおけるメインの製品、新製品や新たなアーキテクチャを使用した製品、海外で展開している製品などに対して、ホワイトハッカーによるペネトレーションテストの依頼を行っている。近年定常的に検証を行い始めたのは、顧客からの要望がきっかけになったと考えている。
- 外部の検証事業者に対して自社製品の検証を依頼するのは以下の場合である。

- 内部のリソースが足りず、手が回らない場合。このケースが最も多い。
- 技術的に難しく、内部では対応ができない場合。
- Amazon の認証（Alexa と IoT 機器を連動させるために必要な認証）のように、特定の検証事業者による検証しか認められていない場合。
- B to B 案件で、発注元から第三者によるセキュリティ検証結果を求められた場合。

- すべての製品に対して検証を行っているわけではなく、脅威分析やリスク評価により検証の必要性が明らかになった製品やサービスに対して、検証を依頼している。静的診断や動的診断、ツールによる自動診断のような検証は社内で行い、ペネトレーションテストといった専門的な知見が必要となる検証を外部の検証事業者に依頼している。外部の検証事業者に検証を依頼する際、基本的には以下のプロセスで検証を実施いただく。
  1. 脅威分析を行う。
  2. アタックサーフェスを洗い出す。
  3. 攻撃手段を提案し、すり合わせを行う。
  4. 本番のテストを実施する。
  5. 報告書を提出する。
  6. 報告会を実施する。
- 現状では、医療機器に対するペネトレーションテストに関するガイドラインは存在していないと思われる。米国の顧客、特に病院施設からは、セキュリティに関する厳しい調達要件を提示されている。そのため、法規制に対する対応より、むしろ顧客要望に対応する目的で外部の検証事業者に検証を依頼している。

今回ヒアリングを実施したメーカーでは、水準に差はあるが、自社内である程度のセキュリティ検証を実施していた。外部の検証サービス事業者への依頼は、顧客から要望があった場合に実施していることが多かった。また、製品の特性に応じて依頼を行っているという意見や専門的な知見が必要な場合に依頼するといった意見も一部の企業から得られた。そのほかには、内部のリソースが足りていない場合や、Amazon の認証のように特定の検証事業者による検証しか認められていない場合に依頼を行うといった意見も得られた。顧客からの要請が検証に対する一番の動機づけになることが示唆された一方で、サイバー攻撃を受けた場合に重大なリスクに繋がる場合など、顧客がその重要性を認識していない場合でも、検証が求められることがあることが分かった。これらの意見を踏まえ、検証のニーズが顕在化していない場合において、どのように検証を促進していくかという観点についても検討を行った。

【外部検証事業者に対する検証の依頼意向について】

- 標準規格やガイドライン、要求仕様等でセキュリティ検証が要件化された場合には対応することになるが、すべての製品に対して外部委託して検証を実施することは、コストの観点で現実的ではない。顧客や取引先からセキュリティ対策に関する強い要望があれば、セキュリティ検証を行う強い動機になると考えている。
- 政府が IoT 機器を販売する際の条件として一定水準の検証を要件として定めるならば、それに沿った検証を行う。
- ユーザーからの強い要望や政府調達で要件化されない限り、外部の検証事業者に検証を依頼

することはない。
- 医療機器に関して、日本の顧客からの要望は現時点では少ないが、今後は米国に追従して徐々に多くなると考えている。

外部検証事業者に対する検証の依頼意向について、顧客からの要請や政府による要件化が行われた場合には外部検証事業者に検証を依頼するという声が多く寄せられた。検証の必要性が高いと思われる分野において、検証の重要性に関する啓発を顧客に対して行うほか、政府による要件化を行うことも外部事業者への検証依頼を促進する観点では重要である。医療機器に関しては、今後顧客からの要望が多くなると推測されるという意見も得られた。

【検証サービスを利用するうえでの課題について】

＜使用環境について＞
- 顧客によって使用環境が異なるため、必ずしも診断・検証が必要であるとは限らない。
- 検証によって、デバイスのセキュリティ対策に関するお墨付きが、リーズナブルなコストで取得できることは良い。しかしながら、IoT 機器の特性上、導入環境によって必要なセキュリティレベルが異なるため、求める対策は一意に決まらないと考えている。

＜製品の特性について＞
- 今後、セキュリティ検証が重要となる製品として、公共分野に納入する製品、専用のオペレーターが操作できない製品、個人情報を取り扱う製品等が挙げられる。この中でも、特に個人情報を取り扱う製品の重要性が高い。
- 外部の検証サービスの要否について、製品分野に起因する差異はあまりない。分野を問わずセキュリティ確保に対するニーズがある。一方、ビジネスとして立ち上げ途中の商品は比較的検証の優先順位が低い。このような領域では、まずビジネスを立ち上げことが優先される。

＜コストについて＞
- 検証に関する課題として、コストの問題も存在する。IoT 機器の場合、各デバイスによって単価や流通量が大きく異なる。流通量が限定的かつ廉価な製品に対して、どの程度のセキュリティ対策を求めるかは悩ましいところである。ベンダーがコストをかけて実施した対策が報われるような仕組みができることが望まれる。検証を実施し、アシュアランスレベルが高いことを証明したとしても、その情報が消費者に周知されなければ意味がない。
- 開発部門からは検証にかかる費用が高いという声が挙がっている。

＜その他＞
- 動的セキュリティ診断を考慮したうえで、長期的なサービスの連携ができるような検証サービスがあれば良い。一般的な検証では、ある時点での静的な状態を見て、その時点でのリスクを示す。一方、将来的に生じるリスクに対しても、絶えずアップデートをして脆弱性対策を行っていく

ことが重要である。そのため、求められるセキュリティ対策の基準も徐々に変わっていくものであると考えている。
- 汎用的な OS であれば、多くの検証事業者で対応ができるであろうが、組込機器に多いリアルタイム OS の場合は、対応できる事業者が多くないと考えている。自社の要望と折り合わないことも多い。
- 様々な検証事業者に依頼してみたいが、どのような条件であれば採用して良いのかが分からず困っている。条件リストを作成しようと考えているが、現状実施できていない。

検証サービスを利用するうえでの課題について、顧客によって使用環境が異なり、それによって必要なセキュリティレベルが異なるため、必ずしも診断・検証が必要であるとは限らないといった意見が得られた。そして、外部の検証サービスの要否について、製品分野に起因する差異はあまりないという声が挙がった一方、個人情報を取り扱う製品といったものは特に検証が求められるという意見や、ビジネスとして立ち上げ途中の商品は比較的検証の優先順位が低いという意見も得られた。導入環境や製品の特徴に応じた外部検証の必要性について整理を行い、外部検証が求められる部分については、その実施を促進していくことが求められる。

検証にかかるコストに関する指摘も行われた。特に、流通量が限定的かつ廉価な製品は、検証を行うための費用を捻出することが難しいという意見である。また、かけたコストが報われるような仕組みが必要だという声も挙げられた。これらの意見を踏まえ、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製品が積極的に導入されるような社会の仕組みについて検討を行った。

そして、将来的に生じるリスクに対しても、絶えずアップデートをして脆弱性対策を行っていくことが重要であるため、動的セキュリティ診断を考慮したうえで、長期的な連携ができるような検証サービスが求められるという意見が得られた。加えて、リアルタイム OS に対応できる事業者が多くないといった声も挙がった。今後、検証依頼者のニーズに対応できる検証事業者を確認する仕組みについても、検討を行っていくことが望まれる。

また、どのような条件で検証事業者を選定すれば良いかが分からないといった声も挙げられた。本事業で検討した仕組みが構築されることで、このような機器メーカーにおいて効率的に検証事業者を選定することができると考えられる。

（2）信頼できる検証事業者を選定する際の観点

信頼できる検証事業者を選定する際の観点に関するヒアリング結果は以下のとおりである。

【実績について】
- 過去に取引があるか、関連製品に対する検証の実績があるかという情報は、信頼できる検証事業者を選定するうえで参考となる。
- 実績は重要である。
- 品質、信頼性、検証処理能力等は、事業者の実績に現れると考えている。検証事業者において、どういった会社のどういった案件を定期的にこなしているかという点が 1 番分かりやすい指標となるのではないか。例えば、日経 225 の企業の製品に対する検証を一定程度こなしている事業

者であれば、信頼性は高いと思われる。他方で、実績のみで判断した場合に、新規参入の検証事業者に対して依頼が難しいという懸念はある。

- どのような分野で検証の実績があるかは、検証事業者の選定を行ううえで 1 つのポイントになると考えている。特に、特定の分野の検証を継続的に行っている検証事業者の方が安心して依頼ができる。
- 依頼を行う際には、信用できる会社であることを示す書類を用意して内部稟議にかける必要がある。実績があり、規模が大きい企業の方が稟議で通しやすい。
- 依頼する製品の分野に対する検証実績も、事業単位で規定している外部の検証事業者の選定要件に含ませることを検討している。

【情報管理体制について】

- ソースコードを用いたセキュリティ検証の場合は、厳密な情報管理を求めることになる。一方、製品自体は最終的に流通するものであるため、製品情報に関する厳密な管理は求めない。競合他社の製品を検証している事業者であっても、情報管理が適切に実施されていることが分かれば忌避することはない。
- 情報管理に関しては社内でも徹底しており、重視するポイントである。
- 情報管理体制は、最も基本的なことであると考えている。ほとんどの検証事業者は問題なく実施できているのではないか。
- 検証事業者に対して依頼する際、事業者の情報管理は重要であると考えている。事業者が ISMS を取得していなくても発注はできるものの、ISMS を取得していない事業者においては、取引や情報の取扱いに関するチェックリストの提出をいただく必要がある。
- 検証事業者の情報管理体制は重視しているものの、情報管理体制を評価するための指標はまだ設けていない。

検証事業者を選定する際の観点について、ヒアリングを実施した企業のほとんどが検証実績を重視していた。特に、依頼する製品の分野について継続的に検証を行っているかという点は、信頼できる検証事業者を選定するうえで重要とのことであった。一方、実績のみで判断すると、検証事業者の新規参入が難しくなるという意見も挙げられたため、その点も踏まえて検討を行った。

次に、情報管理体制を重視しているとの声も多く寄せられた。他方、情報管理体制を評価するための指標が設けられていないとの声も挙がった。これらの点を踏まえ、検証事業者に求める情報管理に関する要件の検討を行った。

【技術力について】

- 検証事業者には、技術力が当然求められる。
- 組織的にレベルを上げて一定品質のサービスを提供している企業でないと、依頼は厳しい。また、検証を実施する人のレベルが非常に重要だと感じている。
- 検証事業者を選定する際、検証の力量を重視している。特に、脅威分析や試験シナリオを作成するか、見つかった脆弱性に対する推奨対策を記載するか、脆弱性の再現性に関する考察を記

載するかといった点を重視している。新規の検証事業者であっても、実力があれば選定していく方針である。

【報告について】
- サンプルレポートを提出いただき、契約前にレポートの内容について口頭で確認を行っている。
- 信頼できる検証事業者を判断するためには、サンプルレポートを強く求めていく方針が良いと考えている。
- レポートの記載内容について、セキュリティの専門家であれば分かるが、開発現場からすると分かりづらいことがある。細かく噛み砕いて説明いただけるとありがたい。
- 検証結果に関する報告会は実施いただきたい。

【アフターフォローについて】
- アフターフォローの観点も肝要である。
- 検証後のフォローアップに関するサービス基準は設けていないが、見つかった脆弱性に開発部門が対応した後、検証事業者に改めて脆弱性のチェックをしていただけるとありがたい。

【認証や資格について】
- イギリスでは政府が実施するテストに合格して認証を取得しなければ検証を実施できない。そういった認証を取得している海外企業であれば信頼できるのではないかという議論を行ったことがあるが、認証要件を確認すると、認証を取得していることが本当に信頼性の証左になるのかについて疑問を感じた。
- CEH、OSCP、SANS といったペネトレーションテストに関する資格も重視しており、検証事業者の選定要件に含まれている。検証に携わる全てのメンバーが資格を有することは厳しいと思われるため、少なくとも1人以上の実績を持つ有資格者が検証に携わっていれば良いと考えている。

信頼できる検証事業者を選定する際の観点について、検証の技術力も重視しているとの意見が得られた。その中で、組織と検証者、両方のレベルが求められるとの声も挙がった。それを明らかにする手法としては、実績以外に、サンプルレポートの質や資格の有無等が考えられる。資格に関しては、CEH、OSCP、SANS といったペネトレーションテストに関する資格を重視し、それらを検証事業者の選定要件に含んでいるメーカーも存在した。検証に携わるすべてのメンバーが資格を有することは厳しいと思われるため、少なくとも1人以上の実績を持つ有資格者が検証に携わっていれば良いと考えているとのことであった。また、実力さえあれば、新規の事業者でも選定する方針との意見も得られた。これらの点を踏まえ、検証事業者に求める要件について検討を行った。また、検証結果の説明の分かりやすさや報告会の実施の有無、アフターフォローの充実度といったカスタマーサポートの観点についても声が挙がった。したがって、検証の実績や技術力の観点だけでなく、カスタマーサポートの観点についても確認ができるような仕組みを検討した。

【その他】

- どのような機器を検証した際にどの程度の納期であったかも分かると良い。
- 依頼してすぐに検証してもらえるかどうかは、重要な点である。
- コストとセキュリティの兼ね合いについて相談できる事業者であれば良い。
- 検証事業者によって見積り金額のブレが大きく、複数の事業者から見積りを頂いた後に事業者の選定をしている。
- オンサイトの検証が対応可能かについて確認したい。
- 脅威分析を第三者の視点で行っていただくことを重視している。
- 近頃の IoT 製品は、デバイス・スマホアプリ・クラウドサービスの 3 つで 1 つの製品という構成になっていることが多い。総合的に全ての領域を検証できる検証事業者が存在するのであれば、依頼がしやすい。
- 外部の検証事業者を選定する際、ペネトレーションテストの質を確認するにあたって以下の点を主に確認した。
  - 検証対象となる製品に関する検証経験がこれまでにあるか。
  - 適切な情報管理体制が構築されているか。
  - ペネトレーションテストの品質を証明するような認証を有しているか。
  - サンプルレポートの質は高いか。
  - 具体的にどのようなテストを行うかが明確になっているか。
  - ツールを使用するのみの検証ではないか。
  - テストの実施人数や実施時間が明確になっているか。
  - テスト後のフォロー内容が充実しているか（例えば、テスト半年後に、見つかった脆弱性の詳細について問い合わせをすることが可能かどうか。）
  - 制約事項や実施を禁止する事項が明確か。
  - テストの実施場所は明確か。
  - 検証中のコミュニケーションプランが明確であるか。
  - 連絡窓口が設置されているか。
  - 検証結果に関する定期的な報告がなされるか。
  - 異なる製品を一度に複数台依頼する際、それらに対応できるキャパシティがあるか。
  - 検証に要する費用はどの程度か。

信頼できる検証事業者を選定する際のその他の観点として、納期はどれくらいか、すぐに対応してもらえるか、コストとセキュリティの兼ね合いについて相談できるか、オンサイト検証に対応しているか、脅威分析を実施できるか、デバイス・スマートフォンアプリ・クラウドサービスについて総合的に検証できるか、認証の有無、どのような検証を行うか明確になっているか、検証中のコミュニケーションプランが明確かといった観点が挙げられた。今回検討を行った仕組みでは、技術要件と品質管理要件に関する検証事業者の最低限の信頼性要件を定めているため、すべての観点を含められているわけではない。他方、検証事業者に対するより高度な要件を規定する際には、考慮することが望まれる。

（3）信頼できる検証事業者を確認する仕組みや制度の活用意向

信頼できる検証事業者を確認する仕組みや制度の活用意向に関するヒアリング結果は以下のとおりである。

【基準について】
- 共通のクライテリアや判断する基準が国から出ていれば、それを活用することで優れた事業者を見つけやすくなるだろう。
- ペネトレーションテストに関する何らかの基準があれば、検証を実施しやすくなると認識している。
- 信頼できるセキュリティ検証サービス事業者の認証制度について、海外で展開している製品やサービスがあるため、認証基準や制度がグローバルで共通化されたものとなれば活用しやすい。

【リストや情報の公開について】
- 信頼できるセキュリティ検証事業者を選定する場合、リストが策定されていた方が問い合わせや見積の段階で検討しやすい。
- 事業者において検証実施が可能な分野に関する情報が分かれば、検証事業者に声をかけやすい。
- 信頼できる検証事業者を選定する際の観点に関する情報が公開されていれば便利だと思われる。

【お墨付きについて】
- 開発現場からは、製品がきちんと検証を受けていることに対するお墨付きが欲しいという声が挙がっている。経産省からそういったお墨付きがもらえるのであれば、検証を受けるモチベーションに繋がるだろう。ただし、お墨付きを得るためにかかる時間やコストが大きいのであれば、取得は難しい。また、このお墨付きが消費者の購買に繋がるかが重要である。現状、消費者は基本的に値段とメイン機能に着目している。認証を取らなければ市場から排除されるくらいの強制力がなければ、手が出しづらい。そうでないと、認証を取得していない中小企業や海外メーカーが市場に参入し、価格競争で負けてしまうということが想定される。
- セキュア開発やインシデントレスポンスを行おうと考えているため、一定程度の基準や国際標準にもとづいて取り組んでいることを顧客にアピールできるような制度があれば良い。登録にかかるコストが大きいと負担になるため、きちんとしたプロセスを踏んでいるといったポイントをおさえている制度であれば良いだろう。

信頼できる検証事業者を確認する仕組みとして、まずは信頼できるか否かを判断するための共通の基準の策定が求められるという指摘があった。その点を踏まえ、策定した基準のもと信頼できる検証事業者か否かについて判断できるような仕組みについて検討を行った。認証基準や制度はグローバルで共通化されているとよいという声も挙がっているため、今後はその点も考慮していく必要がある。また関連して、ペネトレーションテストに関する基準があればよいという意見も得られた。

そして、信頼できるセキュリティ検証事業者のリストが公開されていた方がよいという声が挙がった。

加えて、検証の実施が可能な分野といった信頼できる検証事業者を選定する際の観点に関する情報を公開してほしいという意見も得られた。これらの点を踏まえ、一定の基準をクリアした検証事業者に関する情報を公表することで、信頼できる検証事業者への問い合わせを円滑に行えるようにする仕組みの検討を行った。

また、信頼できる検証事業者を確認する仕組みと直接的に関係しないが、検証を適切に受けている製品に対するお墨付きが欲しいという意見が得られた。インセンティブを設け、検証を受けるモチベーションを確保することは、検証サービスビジネスのエコシステムを円滑に回すことに繋がるほか、信頼できる検証事業者を確認する仕組みの活用にも繋がると思われる。そのため、機器メーカーにおけるセキュリティ対策の取組を適切に評価するとともに、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製品が積極的に導入されるような社会の仕組みについて検討を行った。

4.2.6 有識者検討会における議論結果

有識者による検討会を三回開催し、信頼できる検証事業者を確認する仕組みのあり方、外部検証事業者による検証の訴求方法、機器のサイバーセキュリティ確保のために求められる取組等について議論を行った。各回の議題は表 4-7 に示すとおりである。検討会の有識者は、検証者に求められるスキル・知識に関する知見を有する学識経験者に加え、検証に関する知見を有する業界団体関係者、検証を依頼する立場にある機器メーカー担当者、検証された機器を調達する立場にある地方公共団体担当者によって構成された。

表 4-7 有識者検討会の開催概要

回・実施日	議題
第 1 回 （2021 年 10 月 11 日）	• 本検討会の背景及び検討方向性について • 諸外国における取組及び国内事業者における取組の状況について • 検証主体の信頼性を確認する仕組みについて
第 2 回 （2021 年 12 月 23 日）	• 検証事業者の信頼性を確認する仕組みについて • 外部検証事業者により検証が望まれる機器区分及び検証の訴求方法について
第 3 回 （2022 年 3 月 16 日）	• 信頼できる検証事業者を確認する仕組みについて • 機器のサイバーセキュリティ確保のために求められる取組について

以降では、4.2.2 項で示した 5 つの論点に対する有識者検討会の議論内容を示す。なお、機器のサイバーセキュリティ確保のために求められる取組等に関する議論内容は 4.3.3 項にて別途記載する。

（1） 論点 1 に関する有識者検討会での議論内容

論点 1「信頼できる検証事業者に求められる要件は何か。また、各要件についてどの程度のレベルが、どの対象に対して求められるか。」に関する有識者検討会での主な議論内容は以下のとおりである。

【求められる技術要件について】

- IoT 機器の検証にあたっては、幅広い技術に対する知見があることを示さなければならない。
- 提示されていた資格はセキュリティ系に偏っていたため、GICSP といった制御系の資格やフォレンジック系の資格も含めていただきたい。
- IoT のセキュリティ検査に関する資格がないため、それに近い資格を組み合わせ総合的に判断するしかない。また、研修も SANS が開催している研修程度である。IoT 検証と関係が薄い資格によって検証能力を判断するのは良くないと考えている。IoT を開発する能力と検証する能力は異なる。また、検証対象に関するトレーニングも必要である。

【求められる情報管理要件・品質管理要件について】

- 事業者に対しては、レポーティングや情報管理といった部分についての力量も求められるため、こうした点についても確認できる仕組みが必要ではないか。
- ISMS 取得が信頼性要件の基準案として挙げられていたが、この要件を採用すると大企業向けの制度とならざるを得ない。幅広い検証事業者を対象にすることと矛盾しているのではないか。
- 検証事業者に対する何らかの認定制度は必要だと考えているが、幅広に認定を出しておき、実際の中身は企業の努力に委ねるという形になるのではないか。
- この業界の特徴として人材の流動性が高く、転職の結果、適した人材がいなくなり、診断ができなくなることや品質が落ちる可能性もあるため、品質については確認できる仕組みが必要だろう。

【求められる信頼性要件のレベルについて】

- IoT に関する検証事業は、国内ではまだそれほど成熟していないと思われる。その点を踏まえると、活用目的によっても異なるとは思うが、現段階ではそこまで厳しい基準ではない方が良いと考えられる。
- 信頼できる事業者として太鼓判を押すのであれば、検証実績に関する約 200 項目の確認が必要であろう。一方、そこまでのレベルを求めないのであれば、審査登録制度と同等のレベルを求める方針で良いと思われる。

検証事業者に求められる要件に関して、まず技術要件について、IoT 機器の検証にあたっては幅広い技術に対する要件を確認する必要があるとの意見が挙げられた。他方で、IoT 機器のセキュリティ検証に特化した資格がないため、類似した資格を組み合わせて総合的に判断するしかないとの意見も得られた。したがって、技術要件については、既存の検証に関する資格や研修制度を組み合わせ、その資格や研修制度の取組状況をもって判断することとした。資格や研修制度の検討にあたっては、GICSP 等の制御系の資格や、フォレンジック系の資格など、セキュリティに関する資格以外も含めることとした。

検証事業者に求められる情報管理要件について、当初の仮説では、ISMS 取得が一つの要件指標になると考えていた。一方で、ISMS 取得を要件として位置づけると中小規模の検証事業者の対応が難しく、幅広い検証事業者を対象とした仕組みとしては望ましくないとの意見が挙げられた。この意見を踏まえ、検証事業者に求める情報管理に関する要件については、ISMS のレベルまで求めず、情報管理に関する手続を設けていること、そして、当該手続について監査を実施することで実効性を確保していること

を要件として位置づけた。また、検証事業者においては、文書作成等の管理に関する力量が求められる一方で、人材流動性が高く、事業者としての品質を管理することの重要性が意見された。

これらの要件に関して求められる要件のレベルについて、幅広の検証事業者を対象とした最低限の要件レベルを位置づけつつ、検証の内容は検証事業者の努力に委ねる仕組みが望ましいとの意見が挙げられた。具体的な最低限のレベルとして、既に国内で制度運用がなされている「情報セキュリティサービス基準審査登録制度」と同等のレベルが候補となりうるとの意見が挙げられた。

（2）論点 2 に関する有識者検討会での議論内容

論点 2「構築した仕組みは、どのような目的で、どの依頼者によって活用されるべきか。」に関する有識者検討会での主な議論内容は以下のとおりである。

- 活用目的 1 と 2 は別物だと感じており、ビジネスモデルも異なるため、誰が受益者かについて明らかにならなければ、検証事業者のインセンティブも見えてこないだろう。これら 2 つの活用目的について、一度に検討することが正しいのか疑問に感じている。
- 官公庁調達を対象とした議論であるか、民間も含めて幅広くセキュアな製品の使用を促したいのか、対象を検討する必要がある。
- 法人向けの IoT サービスであれば、製品の利用者から継続的にコストを回収できる。他方、一般消費者向けの場合、売り切り型のサービスとなり、収入は一度しか得られないがコストは継続してかかることになる。検証事業者と機器メーカーがどのようにビジネスを回していけるかについて、課題感を抱いている。

前述のとおり、今回検討する検証事業者可視化の仕組みについて、当初は 2 つの活用目的を想定した検討を行った。活用目的 1 として、IoT 機器等のベンダーが機器に対して検証を実施する際に、適切な品質管理及び情報管理に努めている検証事業者の選定するために活用する目的、活用目的 2 として、重要インフラ事業者、政府機関等が利用する重要機器に対する検証にあたって、高信頼な検証事業者を選定するために活用する目的を検討したが、有識者検討会において、これら 2 つの活用目的を一度に議論することが困難であるとの意見が挙げられた。そのため、今年度の検討においては、活用目的 1 に対象を絞って調査・検討を行った。

（3）論点 3 に関する有識者検討会での議論内容

論点 3「検証事業者の信頼性を誰が、どのように確認し、可視化するか。」に関する有識者検討会での主な議論内容は以下のとおりである。

- 情報セキュリティサービス審査登録制度の運営は日本セキュリティ監査協会（JASA）に全て委託している。
- 登録された検証事業者が適切な検証を行うためのケイパビリティを有しているかについては、制度開始後も見守る必要があると考えている。検証事業者によって得意分野や不得意分野が生じると考えられる。どのような形で検証事業者のケイパビリティを可視化していくかについては、今

後も検討する必要があるだろう。
- 審査費用を抑えるため、審査事業者を支援する仕組みを構築するべきである。審査機関に対して事業再構築助成金を使えれば、審査費用を抑えることができるだろう。

前述のとおり、今回検討する検証事業者の信頼性を確認する仕組みについて、既に国内で制度運用がなされている「情報セキュリティサービス基準審査登録制度」が参考となる。今回検討している IoT 機器等の検証に関する内容を仮にこの制度に含める場合、当該制度の審査登録機関により検証事業者の信頼性を確認する必要がある。有識者検討会でも意見されたとおり、現行の審査登録制度では日本セキュリティ監査協会（JASA）が唯一の審査登録機関である。また、有識者検討会では継続的な検証事業者の可視化方法について今後も検討すべきとの意見が挙げられたほか、審査登録機関を支援する仕組みの必要性についても意見がなされた。

（4）論点 4 に関する有識者検討会での議論内容

論点 4「検証依頼者が、信頼できる検証事業者を選定するために必要な仕組みは何か。」に関する有識者検討会での主な議論内容は以下のとおりである。

- 機器の種類ごとに検証実績や対応可否が明示されれば、検証を依頼する際に役立つと思われる。
- 検証実績についてカテゴライズや区分けがなされていると検証事業者を選定しやすい。
- 検証事業者の得意分野が分かりやすくなるよう、検証実績の内訳を明示するといった工夫が必要。実績件数だと大企業と中小企業で差が生じる可能性があるため、割合での表示が望まれる。
- どのような機器に対して検証を行ったことがあるのかについて、具体的に書ける範囲で提示していただきたい。

機器メーカーに対するヒアリングにおいても意見されたとおり、検証を依頼する機器メーカーの立場では、メーカーが開発する機器に関連する検証実績を検証事業者が持ち合わせているかが事前にわかれば、効率的に検証事業者を選定できる。有識者検討会においても、登録する検証事業者について、検証実績を有する機器のリストが明らかになると良いとの意見が挙げられた。これに加え、各機器の実績について、内訳等の定量値が明記されると良いとの意見が挙げられた。

（5）論点 5 に関する有識者検討会での議論内容

論点 5「信頼できる検証事業者に対して、どのようなインセンティブが考えられるか。」に関する有識者検討会での主な議論内容は以下のとおりである。

- 登録企業が少なければ制度が成り立たなくなるため、本制度においてもブランディングは重要。
- 検証事業者の負担軽減策として、資格や検証実績といった基準に応じて審査登録料の割引を行うのも一手だと思われる。

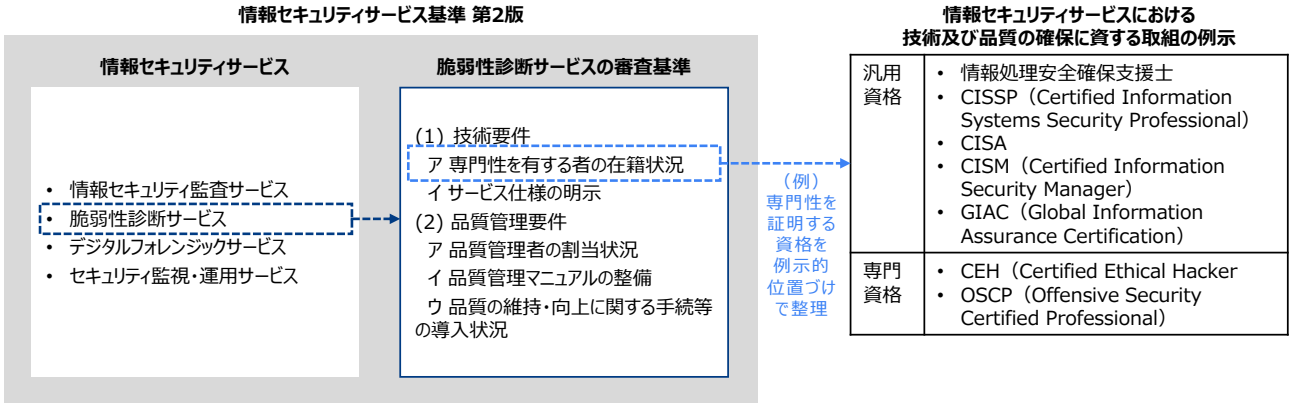
- 検証は属人的な要素が強いため、人材の流動を考慮すると、登録内容のアップデートが簡便にできるかが重要になる。

検証事業者に対するヒアリング結果で明らかになったとおり、検証事業者が登録するか否かは、登録によって売上につながるかどうかが非常に重要である。このためには、有識者検討会で意見されたとおり、制度のブランディングが必要であり、検証事業者と検証依頼者の両方に対してアプローチすることが望まれる。また、登録事業者数を増やすために、審査登録料の割引を行う方針も意見された。後述するとおり、今回検討する仕組みは、既に国内で運用されている情報セキュリティサービス基準審査登録制度に追加する方針とするが、IoT 機器等に対する検証サービスを展開する検証事業者の多くは、既に「脆弱性診断サービス」の審査登録を受けている可能性がある。そのため、既にサービス登録されている事業者は審査登録料を割引するなど、金銭的支援を行うことで登録事業者数を増やすことも想定される。

4.2.7 審査登録機関との議論結果

有識者検討会での意見を踏まえ、本事業で検討する信頼できる検証事業者を確認する仕組みについて、国内で既に制度が開始している情報セキュリティサービス基準審査登録制度に対し、新たに IoT 機器等の検証サービスに関するサービス区分を追加する方針で検討した。前述のとおり、情報セキュリティサービス基準審査登録制度とは、経済産業省の「情報セキュリティサービス基準」[10]に基づき、一定の技術要件及び品質管理要件を満たした情報セキュリティサービスを登録・公開する制度である。経済産業省の「情報セキュリティサービスに関する審査登録機関基準」[11]に適合する審査登録機関によって審査・登録された情報セキュリティサービスが公開されている。ここで、「情報セキュリティサービス基準」とは、情報セキュリティサービス業の普及を促進し、国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的として情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示した基準であり、現行では、「情報セキュリティ監査サービス」、「脆弱性診断サービス」、「デジタルフォレンジックサービス」、「セキュリティ監視・運用サービス」の 4 つのサービスが定義されている。情報セキュリティサービス基準は、第 2 版が 2022 年 1 月 31 日に公表され、2022 年 4 月 1 日より施行となる。この第 2 版では、情報セキュリティサービス基準で明記されている資格等の各審査基準について、その基準を満たしていることを証明できる取組（資格、専門家コミュニティ、参照する基準、結果に関する取扱方法及びその明示方法 等）[12]が例示的位置づけで整理されている。情報セキュリティサービス基準と取組の例示の関係性を図 4-1 に示す。

[10] https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun2.pdf
[11] https://www.meti.go.jp/policy/netsecurity/shinsatouroku/tourokukizyun2.pdf
[12] https://www.meti.go.jp/policy/netsecurity/shinsatouroku/reiji.pdf



出所）経済産業省「情報セキュリティサービス基準第 2 版」及び「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」に基づき三菱総合研究所作成

図 4-6 情報セキュリティサービス基準及び取組の例示の関係性

本事業で対象とする IoT 機器等に対する検証サービスを情報セキュリティサービス基準及び情報セキュリティサービス基準審査登録制度に追加することの実現可能性や、実際の制度運用にあたって想定される課題等について、現行唯一の審査登録機関である日本セキュリティ監査協会（JASA）と議論を行った。主な議論内容は以下のとおりである。

- 技術要件のうち、サービス実施方法の明確化に関する例示は更に具体化する必要がある。例えば、「脆弱性診断サービス」であればツールの例示が記載されているため、そのツールに基づいた審査が実施できる。現状の例示だと審査の拠り所が無い。様々な例示方法が想定されるが、根拠基準や具体的なツールを含める必要がある。また、あくまで例示であるため、申請者が例示したツール以外の情報を記載した場合には、別途同等性を確認する必要がある。
- 情報管理要件を特出しして追加することは望ましくない。現行の「脆弱性診断サービス」においては、品質管理要件のウ（ウ）において情報管理に関する要件を含めているため、同じように品質管理要件に含めるべきである。
- 「検証事業者の過去の実績」を、件数等の定量値を含めて公開することは現実的に不可能。現状、JASA や IPA が公開している情報では、申告ベースかつ注釈をつけたうえで「主たる顧客対象の分野・業種」を記載している。同様のスキームで、「過去に検証を実施した実績のある IoT 機器等」を申告ベースで追加することは可能かもしれない。
- 今回の「機器検証サービス」を「脆弱性診断サービス」の一部に含めないことについては、今後も議論になる可能性がある。「脆弱性診断サービス」に含めることで「IoT」というキーワードが埋没する恐れがあるほか、既存の脆弱性診断サービスとマーケットが異なるため、サービスを分けておいた方が扱いやすいかもしれない。しかしながら、セキュリティ対策の不備を確認するサービスという定義が不明瞭にも感じる。
- それ以外の要件について、現行の審査登録制度の要件と大きく変わるものではないため、特段問題はない。

IoT 機器等に対する検証のサービスである「機器検証サービス」を情報セキュリティサービス基準や情報セキュリティサービス基準審査登録制度に追加する方向性について理解いただくとともに、具体的

な審査要件の対応可否について確認をいただいた。全体的な方向性や要件の位置づけについて異論は無かったものの、一部の要件や対応については修正すべきとの意見が挙げられた。具体的には、サービス実施方法の明確化に関する例示は更に具体化する必要がある点や、検証事業者の過去の実績を実績件数等の定量値を含めて公開することは現実的に不可能であるとの意見が挙げられた。頂いた意見を踏まえ、本事業で考える IoT 機器等に対する検証サービスの仕組みの全体像を修正した。

4.2.8 調査・検討を踏まえた仕組みの案

諸外国の制度で用いられている信頼性要件、検証事業者や検証依頼者に対するヒアリング結果、有識者検討会での議論及び審査登録機関に対するヒアリング結果を踏まえ、IoT 機器等に対して検証を実施する検証事業者の信頼性を確認する仕組みの案について検討を行った。

（1） 仕組みの位置づけ

前述のとおり、今回考える仕組みは、既に国内で運用されている情報セキュリティサービス基準審査登録制度に追加する方針とする。具体的には、今回検討した IoT 機器等に対する検証サービスを「機器検証サービス」として、情報セキュリティサービス基準に新たに追加する方針とした。ここで、現状の情報セキュリティサービス基準では「脆弱性診断サービス」というサービス区分が存在し、今回対象とする機器検証サービスと類似する要件がいくつか存在する。他方、今回議論する IoT 機器等に対する検証では、脆弱性に関する網羅的な確認だけでなく、セキュリティ対策の不備を確認するための深掘的・属人的な検証を実施することもある。また、「機器検証」と「脆弱性診断」とで対象となるマーケットが異なるため、現行の「脆弱性診断サービス」と区分を分けた方が良いとの意見も挙げられた。これらの検討を踏まえ、図 4-7 に示すとおり、脆弱性診断サービスとは別に機器検証サービスの区分を新たに追加する方針とし、機器検証サービスでは「IoT 機器をはじめとするネットワークに常時接続する機器及びその関連サービスを対象に、当該対象におけるセキュリティ対策の不備や脆弱性の有無を確認するサービス」を対象とすることとした。

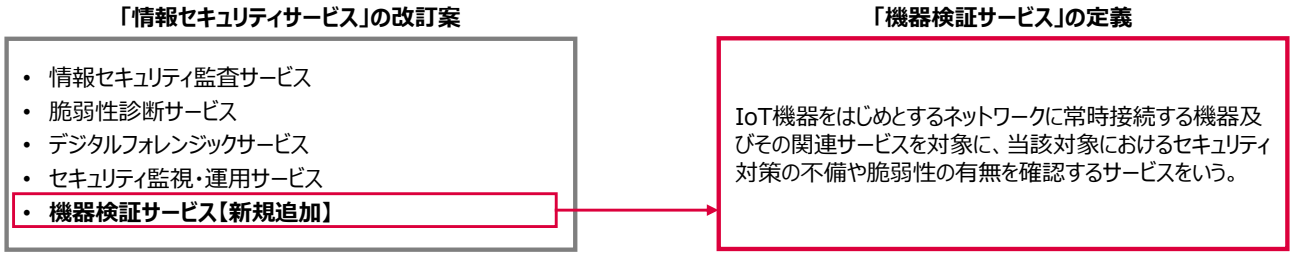


図 4-7 情報セキュリティサービスの改訂案：「機器検証サービス」の追加

機器検証サービスにおいても、現行の審査登録制度と同様のスキームで、検証事業者の審査・登録を行う。仕組みの運用スキームを図 4-8 に示す。なお、機器検証サービスにおける審査登録機関について、現行の審査登録制度の運用状況を鑑み、JASA が担うことを前提とて検討を行ったが、現行の審査登録制度と同様に、今後新たな審査登録機関の追加を妨げるものではないことに留意する必要がある。

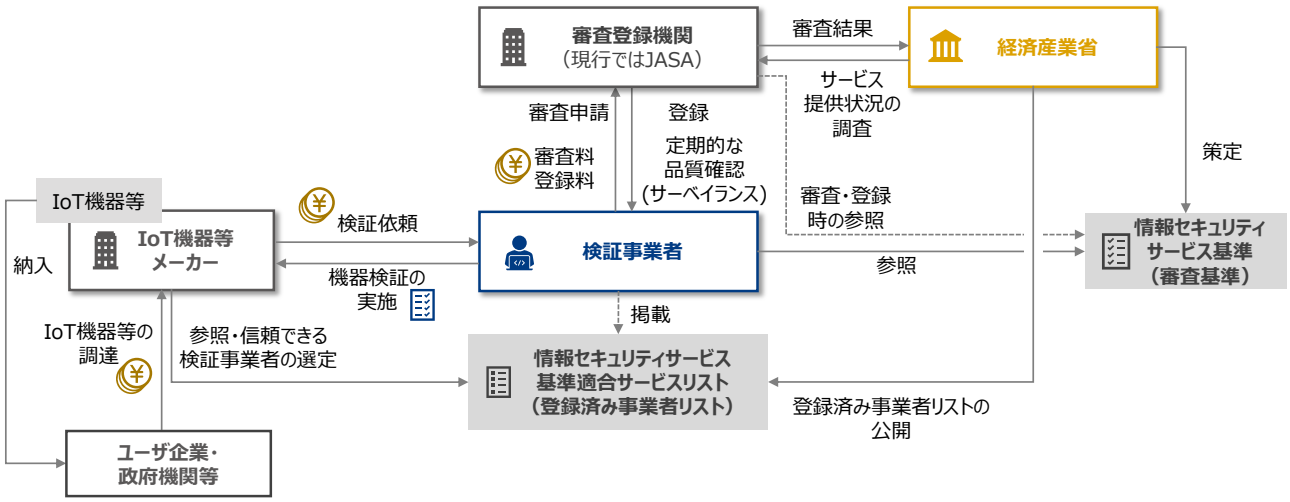


図 4-8 機器検証サービスの運用スキーム

（2）仕組みで求める要件・審査基準

機器検証サービスの登録にあたって検証事業者に求める要件及び審査基準を表 4-8 に示す。これらの要件及び審査基準は、諸外国の制度で用いられている信頼性要件、検証事業者や検証依頼者に対するヒアリング結果、有識者検討会での議論及び審査登録機関に対するヒアリング結果等を踏まえて策定した。表 4-8 に示すとおり、検証事業者に対しては、技術要件と品質管理要件に関する最低限の信頼性要件を求める。品質管理要件の一部として、事業者における情報管理に関する要件を含むことに留意する必要がある。なお、各審査基準について、2022 年 1 月に改訂された情報セキュリティサービス基準の第 2 版に基づき、資格要件や参照する基準等について、具体的な技術及び品質の確保に資する取組の例示を参照する形とした。表 4-8 に示す例示番号は、現行の「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」の連番として定義している。

表 4-8 機器検証サービスの要件項目・審査基準案

要件区分	要件項目	審査基準
(1) 技術要件	ア 専門性を有する者の在籍状況	サービス品質の確保のため、機器検証サービスに従事する要員のうち、次の要件を満たす者を技術責任者として業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。 （ア）例示1－5に定める資格または同等のものを有する者 （イ）例示3－4に定めるサービス品質確保に資する研修または同等のものを修了している者

要件区分	要件項目	審査基準
	イ サービス実施方法の明確化	サービス品質の確保のため、次に掲げる事項を明らかにしていること。 （ア）検証計画を策定することの提示 （イ）検証環境及び検証のスコープを明確化することの提示 （ウ）脅威分析の結果等を踏まえ、機器に存在しうる脅威や脆弱性を確認する旨の提示 あわせて、例示4－4に定める基準または同等のものに従って機器検証サービスが行われていることとともに、例示5－2に定める機器検証の結果の取扱または同等のものを明らかにしていること。
（2）品質管理要件	ア 品質管理者の割当状況	品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。
	イ 品質管理マニュアルの整備	品質維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルや規則等を整備していること。 （ア）サービス利用者（検証依頼者）との仕様調整（例：検証計画、検証対象範囲、実施内容、情報の取り扱い）に関する内容 （イ）サービス実施方法に関する内容 （ウ）サービス利用者からの要求、意見、クレーム等への対応に関する内容
	ウ 品質の維持・向上に関する手続等の導入状況	品質の維持・向上のため、次に掲げる手続等を行っていること。 （ア）機器検証サービスを行った案件について、当該案件に従事した者以外の者が検査実施報告書についてレビューを行っていること。 （イ）機器検証サービスに従事する者に対して例示7－5に定める教育及び研修等または同等のもののいずれかを実施又は受講させていること。 （ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続について機器検証サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

技術要件の「ア 専門性を有する者の在籍状況」のうち、資格に関する例示 1-5 の案を表 4-9 に、研修に関する例示 3-4 の案を表 4-10 に示す。専門性に関する要件については、IoT 機器等の検証において求められる技術的なスキル・知識を整理し、当該スキル・知識を有していることを確認しうる資格及び研修を例示として位置づけた。これらの資格及び研修の例示は有識者検討会で挙げられた意見を踏まえて作成した。

表 4-9 例示 1-5（機器検証サービスに係る資格要件の例示）案

1－5	機器検証サービスの提供に必要な専門性	汎用資	• 情報処理安全確保支援士 • CISSP（Certified Information Systems Security Professional）

	を満たすとみなすことができる右に例示する内容相当の資格	格[13]	• CISM（Certified Information Security Manager）
		専門資格[14]	• エンベデッドシステムスペシャリスト • CompTIA Security+ • CompTIA PenTest+ • CEH（Certified Ethical Hacker） • CHFI(Certified Hacking Forensic Investigator) • GPEN（GIAC Penetration Tester） • GXPN（GIAC Exploit Researcher and Advanced Penetration Tester） • OSCP（Offensive Security Certified Professional） • OSCE（Offensive Security Certified Expert） • OSEE（Offensive Security Exploitation Expert） • GICSP（Global Industrial Cyber Security Professional） • デジタル・フォレンジック資格（CDFP-B、CDFP-P、CDFP-M）

表 4-10 例示 3-4（機器検証サービスに係る研修受講実績の例示）案

3－4	当該研修の修了をもって機器検証サービスの提供に必要な専門性を満たすとみなすことができる右に例示する内容相当の研修	• SANS Security Courses（556, 560, 642, 660, 760）

技術要件の「イ サービス実施方法の明確化」のうち、機器検証サービスに係る参照基準の例示 4-4 の案を表 4-11 に、結果に関する取扱方法及びその明示方法の例示 5-2 の案を表 4-12 に示す。サービス実施方法の明確化に関する要件については、機器検証サービスの品質確保のために求められる取組を位置づけた。これらの取組は、有識者検討会での意見やヒアリング結果を踏まえつつ、昨年度策定した手引きに基づき整理した。また、機器検証サービス品質の確保のための基準について、昨年度策定した手引きに記載されているツールを例示的位置づけで扱うこととした。加えて、機器検証結果に関する取扱やその明示に関する取組を例示として位置づけた。具体的には、検証結果報告書において、脆弱性に関する情報やその影響、検証結果に対する分析・考察結果等を含めることを明記した。これらの取組は、後述するとおり機器検証サービスにおける検証結果報告書サンプルに基づき審査・確認を行うことを想定している。

[13] 情報セキュリティ分野の幅広い知識を有することを証する資格の例示を意味する。
[14] 機器サービスの提供に関する専門的な知識を有することを証する資格の例示を意味する。

表 4-11 例示 4-4(機器検証サービスに係る参照する基準の例示)案

4－4	機器検証サービス品質の確保のため、右に定める基準に従って機器検証サービスが行われていることの例示	• 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」において明記されているツールの一部を使用して検証を行う旨の提示

表 4-12 例示 5-2(機器検証サービスに係る結果に関する取扱方法及びその明示方法の例示)案

5－2	機器検証サービス提供において示す結果に関する取扱方法及びその明示方法	• 検証結果報告書としてとりまとめる。 • 検証結果報告書において、検出された脆弱性に関する情報と、当該脆弱性が悪用された場合に想定される影響、攻撃の再現手順を記載する。 • 検証結果報告書において、検証結果に対する分析や考察等の追加情報を記載する。 • 検証結果に基づき、検証対象機器に求められるセキュリティ管理策の提案を行う。 • 検証結果に関する報告会を開催する。

機器検証サービスに関する品質管理要件について、既存の情報セキュリティサービス基準にて求められている品質管理要件を参考に、品質管理者の割当、サービス実施方法の明確化及び品質の維持・向上に関する手続等に関する要件項目を位置づけた。サービス実施方法の明確化に関する要件の審査にあたっては、サービス実施方法に関する内容やクレーム対応等に関する内容を含んだ品質管理マニュアルや規則等を確認する。また、品質管理要件の「ウ 品質の維持・向上に関する手続等の導入状況」のうち機器検証サービスに係る継続教育については、表 4-13 に示す例示 7-5 を位置づけた。加えて、情報管理に係る要件の一つとして、顧客の情報保護に関する要件を含めた。現行の審査登録制度の運用を踏まえ、情報管理に関する手続を設け、その手続について監査を実施することで実効性を確保していることを求めることとした。

表 4-13 例示 7-5(機器検証サービスに係る継続教育の例示)案

7－5	機器検証サービスの品質確保に資する教育又は研修	• 機器検証サービスに従事する者 ➢ 年間 20 時間以上の教育又は研修(資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT、社内講習や自習を含む。) ➢ 上記、教育、研修における活動を合計で年間 20 時間以上実施していること。

(3) 仕組みにおける事業者の登録・更新プロセス

表 4-8 に示した要件項目の審査にあたって、検証事業者による提出が必要な関連書類のリストを表 4-14 に示す。多くの関連資料は、現状の審査登録制度と大きく変更はないが、機器検証サービスでは

機器検証サービスにおける検証結果報告書サンプルを求め、「イ サービス実施方法の明確化」について審査を行うことを想定する。

表 4-14 各要件項目の審査にあたって提出が必要な関連資料案

要件区分	要件項目	各要件項目の審査にあたって提出が必要な関連資料案
(1) 技術要件	ア 専門性を有する者の在籍状況	• 有資格者リスト(通し番号、氏名、保有資格名称、資格登録番号、有効期限、初登録年、証書の写し) • 研修修了者リスト(通し番号、氏名、研修機関名、研修名、研修終了年月日、証書の写し)
	イ サービス実施方法の明確化	• サービス内容が明示された資料の写し(HP の写し、サービス仕様が確認できる契約・約款等の写し等) • 機器検証サービスにおける検証結果報告書サンプル
(2) 品質管理要件	ア 品質管理者の割当状況	• 品質管理者のリスト(通し番号、氏名、所属部署名、役職名、連絡先電話番号、連絡先メールアドレス)
	イ 品質管理マニュアルの整備	• サービス品質の管理のためのマニュアルや規則等の表紙及び目次 • 審査基準項目の記述箇所が確認できるもの(該当部分のコピー等)
	ウ 品質の維持・向上に関する手続等の導入状況	• 機器検証サービスに従事するものの教育・研修等の実施又は受講状況リスト(通し番号、氏名、教育・研修等の名称、実施機関名、種別、受講等の時間又は CPE ポイント、開始時期、終了時期)

なお、各要件項目の審査の際に活用する情報ではないものの、審査申請や登録の際に以下の情報の提示を検証事業者に求めることを想定する。

- 申請企業の情報・連絡先
- 機器検証サービスに関する URL、又はホームページの写し
- 審査機関に対する誓約書
- IPA に対する誓約書
- サービス概要
- 主たる顧客対象の分野・業種
- 過去に機器検証サービスにて検証を実施した実績のある機器

前述のとおり、検証依頼者である機器メーカーのヒアリングでは、機器メーカーがリストを踏まえて検証事業者を選定する際、自社製品に関する分野の実績があるかを重視するとの意見が挙げられた。そのため、検証依頼者である機器メーカーが自社の製品の検証に適した検証事業者を選定できるよう、今回の機器検証サービスでは、情報セキュリティサービス基準適合サービスリストにおいて登録された各検証事業者が過去に機器検証サービスにて検証を実施した実績のある機器について記載することを想定する。機器検証サービスにおける情報セキュリティサービス基準適合サービスリストのイメージは図 4-9 のとおりであり、過去に機器検証サービスにて検証を実施した実績のある機器も併記することを想定する。なお、過去の検証実績は事業者の申告内容に基づき、審査登録機関や IPA がリストで明記す

る形式とするため、前述のとおり、実績情報は審査対象ではない情報として事業者より提示いただくことを想定する。

サービス名称	サービス毎のURL	事業者名称	事業者所在地	サービス概要	主たる顧客対象の分野・業種	過去に機器検証サービスにて検証を実施した実績のある機器	対象とする地域	登録年月日	有効期限	審査登録機関名
IoTセキュリティ診断	https://www.example.com	株式会社XXセキュリティ	東京都千代田区Y-Y-Y	IoTセキュリティ診断では、IoTの機器のセキュリティ対策の妥当性や脆弱性有無を確認することで、製品販売前の対策の計画や製品のロードマップ活	機械・電機・精密機器、自動車・輸送機器、医薬品・医療関連・化粧品	スマートロック、ドローン、Webカメラ、ルーター、ハブ・スイッチ、医療機器、カーナビゲーション	日本全国	2021/10/19	2023/1018	●●

機器メーカーが自社の製品の検証に適した検証事業者を選定できるよう、
登録された検証事業者の主たる顧客対象の分野・業種や、
過去に機器検証サービスにて検証を実施した実績のある機器を明記

出所）IPA「情報セキュリティサービス基準適合サービスリスト」に基づき三菱総合研究所作成

図 4-9 機器検証サービスにおける情報セキュリティサービス基準適合サービスリストのイメージ

機器検証サービスの新規登録プロセス及び更新プロセスを、それぞれ表 4-15 及び表 4-16 に示す。機器検証サービスの新規登録及び更新のプロセスの全体像は現行の情報セキュリティサービス審査登録制度と同様のプロセスを想定している。更新プロセスの Step 1 において、前述した「過去に機器検証サービスにて検証を実施した実績のある機器」について更新がある場合、併せて申請を行うことを想定する。

表 4-15 機器検証サービスの新規登録プロセス

フェーズ	ステップ	実施主体	実施概要
新規登録	Step 1 事業者登録	事業者を新規登録する検証事業者	• 「事業者登録申請書」に記名・押印し、「誓約書」等を添えたうえで、事業者としての登録申請を行う。
	Step 2 サービスの登録	サービスを新規登録する検証事業者	• Web システムへのログインログイン後、サービス基準への適合を示す情報を入力する。 • 適合を示す資料等をアップロードする。
	Step 3 審査料の支払	サービスを新規登録する検証事業者	• 申請受領通知書兼契約締結確認書及び請求書を踏まえ、審査料を支払う。 （現状）審査料（消費税を除く：サービス単位） 4 万円
	Step 4 審査	情報セキュリティサービス基準審査登録委員会	• 事業者の申請書類を踏まえ、情報セキュリティサービス基準に適合しているかを審査する。
	Step 5 登録料の支払	サービスを新規登録する検証事業者	• 審査終了後、審査料の請求書を踏まえ、登録料を支払う。 （現状）総額（2 か年分） 36 万円（毎年 18 万円） （現状）2 か年分を一括払いした場合 32 万円
	Step 6 台帳の公開	審査登録機関	• 委員会で認定された情報セキュリティサービスを台帳登録し、ホームページで公開する。

フェーズ	ステップ	実施主体	実施概要
		IPA	• 委員会で認定された情報セキュリティサービスを情報セキュリティサービス基準適合サービスリストに登録し、ホームページで公開する。

表 4-16 機器検証サービスの更新プロセス

フェーズ	ステップ	実施主体	実施概要
更新	Step 1 更新審査の申請	登録されたサービスを更新する検証事業者	• 「登録更新審査申請書」に更新（変更）事項等を記載し、提出する。 （実績等に更新があれば併せて申請を行う。）
	Step 2 審査料の支払	登録されたサービスを更新する検証事業者	• 申請受領通知書兼契約締結確認書及び請求書を踏まえ、審査料を支払う。 （現状）審査料（消費税を除く：サービス単位） 4 万円
	Step 3 審査	情報セキュリティサービス基準審査登録委員会	• 事業者の申請書類を踏まえ、情報セキュリティサービス基準に適合しているかを審査する。
	Step 4 登録料の支払	登録されたサービスを更新する検証事業者	• 審査終了後、審査料の請求書を踏まえ、登録料を支払う。 （現状）総額（2 か年分） 36 万円（毎年 18 万円） （現状）2 か年分を一括払いした場合 32 万円
	Step 5 台帳の更新	審査登録機関	• 委員会で認定された情報セキュリティサービスの台帳を更新し、ホームページで公開する。
		IPA	• 委員会で認定された情報セキュリティサービスについて、情報セキュリティサービス基準適合サービスリストを更新し、ホームページで公開する。

（4） 仕組みの運用・利用促進に向けた今後のステップ及び課題

これまでに記載した仕組みの要件項目や審査基準等に基づき、今後、情報セキュリティサービス基準に新たに機器検証サービスを追加するとともに、情報セキュリティサービス審査登録制度に基づき、検証事業者の登録及び情報セキュリティサービス基準適合サービスリストの公開を通じて、機器メーカーが検証を実施する際に、技術要件及び品質要件に係る最低限の信頼性を有した検証事業者を確認できる仕組みを構築することが望まれる。具体的な今後のステップとして、図 4-10 に示すとおり、2022 年度中に情報セキュリティサービス基準への追加及び登録いただける検証事業者を募集し、2023 年度から制度運用がなされることが望まれる。このために、2022 年度中に情報セキュリティサービス基準

に関する検討会[15]を開催し、機器検証サービスの追加について検討するとともに、パブコメの実施が必要となる。並行して、登録いただける検証事業者への声掛けを実施することが想定される。なお、機器検証サービスの登録事業者数に関する KPI について、国内の機器検証サービス事業者の実態や、業態が類似するデジタルフォレンジックサービスの登録実績[16]を踏まえ、2023 年度には 10 社程度、2025 年度には 20 社程度の登録を目指すことが望まれる。

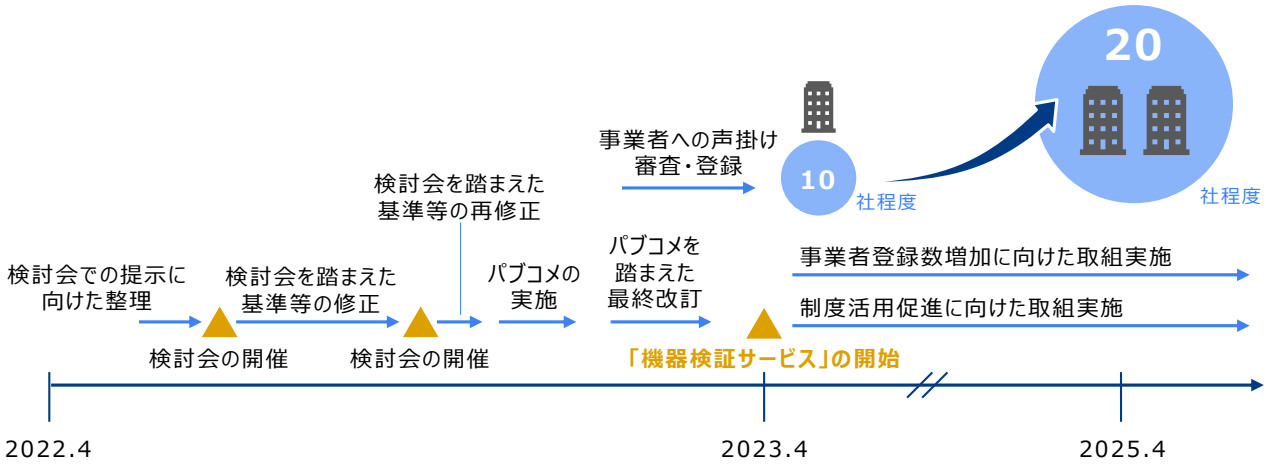


図 4-10 仕組みの運用・利用促進に向けた今後のステップ

今後、機器検証サービスに係る情報セキュリティサービス審査登録制度を実運用するにあたって、制度の活用促進に関する課題と、制度を活用した適切な機器検証の推進に関する課題の大きく 2 つの課題が存在すると考えられる。これら 2 つの課題分類における具体的な論点、そして解決方向性の案を表 4-17 に示す。

表 4-17 機器検証サービスの実運用に関する課題・具体的な論点・想定される解決方向性

課題分類	具体的な論点	想定される解決方向性
制度の活用促進	• 制度の活用を促進するためには一定以上の検証事業者の登録が不可欠であるところ、登録検証事業者をいかに増やすか。 • 制度を活用し検証事業者の選定及び検証依頼を実施する機器メーカーをいかに増やすか。	• 産業分野個別のセキュリティガイドラインにおける検証や「機器検証サービス」の活用に関する訴求 • 中小企業に対する検証の必要性や「機器検証サービス」の活用に関する訴求 • 機器のアシュアランスレベルの観点に基づく検証の必要性の訴求

[15] 「情報セキュリティサービス普及促進に関する検討会」のこと。情報セキュリティサービスを普及させるための方策及び基準の見直し等に関する検討を行うことを目的として設置されている。
[16] デジタルフォレンジックサービスの登録者数について、制度開始後一年以内に 16 社を超える登録、制度開始後三年後には 28 社を超える登録がなされている。

制度を活用した適切な機器検証の推進	• 制度では、検証事業者を選定した後の検証契約の内容については担保していないところ、検証事業者と検証依頼者間の適切な契約をいかに担保するか。 • 制度では、具体的な検証の進め方については担保していないところ、検証依頼者が検証の効果を最大限享受できるよう、検証にあたって検証事業者及び検証依頼者において望まれる対応をいかに周知するか。 • 制度では検証事業者に対して最低限の基準のみを求めているところ、アドバンスドな検証に対応できる検証事業者をいかに可視化するか。	• 検証ビジネス契約に関する「モデル取引・契約書」の新規策定 • 機器に対する検証、分析、解析等が実施できる検証ラボの構築 • 検証事業者及び検証依頼者に求められる対応を記載した「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」の普及促進 • 実際の製品に対する検証試験を含む、機器検証に関する資格制度の新設

前者の課題に関連して、制度の活用を促進するためには、需要サイドである機器メーカーに対して、検証の必要性を訴求するとともに、検証実施に際して情報セキュリティサービス審査登録制度の「機器検証サービス」が活用できることを訴求することが不可欠である。機器によって求められるアシュアランスレベルが異なるところ、機器全般に対してこれらの訴求策を講じるのではなく、検証の必要性が高い個別の産業分野に絞った形での訴求策を講じることが効果的である。例えば、医療分野では、厚生労働省の策定する「医療機器のサイバーセキュリティの確保及び徹底に係る手引書」[17]において医療機器に対するセキュリティ試験（検証）を実施することの必要性が明記されているほか、具体的な試験の実施にあたって、現行の脆弱性診断サービスに登録されている事業者が利用可能であると記載されている。機器検証サービスに関する制度の活用を促進するにあたっても、特定産業分野におけるセキュリティガイドラインにおいて、機器検証サービスの活用に関する言及をするよう、関係各所と連携することが効果的であると考えられる。具体的な特定産業分野として、有識者検討会では、上記の医療機器のほか、自動車分野などの規制産業において、外部検証事業者の活用を促進すべきとの意見が挙げられた。

また、情報セキュリティサービス審査登録制度では、検証事業者と検証依頼者間の具体的な契約内容については担保していないところ、双方が不利益を被らないために適切な契約の方向性を示すことが望まれる。関連する取組として、IPA が公表する「情報システム・モデル取引・契約書　第二版」では、①モデル契約プロセス、②モデル契約書（企画・開発、保守・運用の各フェーズの基本契約書）、③モデルドキュメントの 3 つの文書に基づき、情報システムの企画・運用や開発・保守に係る契約書の作成プロセスを明確化するとともに、そのプロセスを前提とする契約書の条項を整理している。本モデル取引・契約書は、情報システムの開発や運用・保守を対象としているため、脆弱性診断や機器検証に関する契約内容は含まれていない。今後、検証事業者と検証依頼者間の適切な契約を担保するために、脆弱性診断や機器検証を対象とした同様の文書を作成することが望まれる。

加えて、検証人材の育成についても検討する必要がある。後の第 4.3.3 項で示すとおり、有識者検

[17] https://www.mhlw.go.jp/hourei/doc/tsuchi/T211228I0070.pdf

討会において、人材育成を行ううえでは知識・環境・経験を醸成する仕組みが必要であり、特に環境に関しては、IoT 機器に対して、検証、分析、解析等を行える検証センターの構築を求める意見が多数挙げられた。このような検証センターは検証事業者側の検証人材の育成だけでなく、機器メーカーにおけるセキュリティ人材育成にも資すると考えられるところ、コミュニティ全体でのセキュリティレベル向上に寄与すると考えられる。

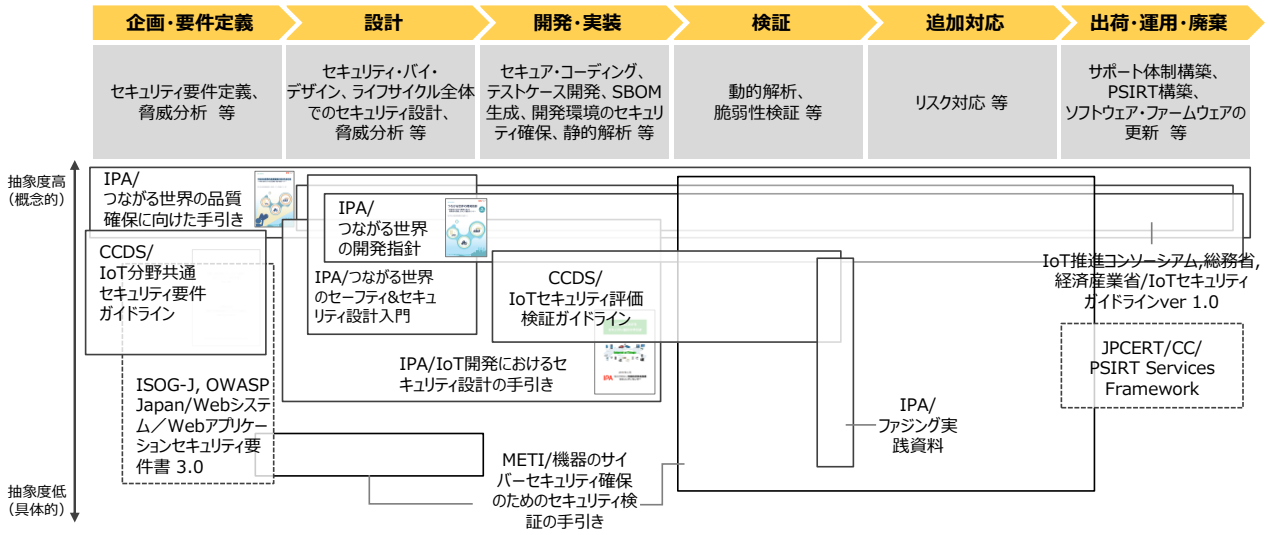
4.3 機器のサイバーセキュリティ確保のために求められる取組について

前節では、IoT 機器等に対する検証事業者の信頼性を可視化する仕組みについて、情報セキュリティサービス基準に新たに「機器検証サービス」として追加すること、また追加を踏まえ、情報セキュリティサービス基準審査登録制度により、信頼できる検証事業者を審査・登録し、検証依頼者が信頼できる検証事業者を確認できる仕組みについて示した。また、この制度化に向けた今後のプロセスや検討課題に関して整理を行った。

IoT 機器等に対する検証により、機器における脆弱性の有無や脅威に対する対策の妥当性を確認できるが、機器検証は機器におけるセキュリティ対策状況を確認する一つの手法に過ぎず、機器のセキュリティ確保のためには、その他の取組も推進することが必要不可欠である。有識者検討会においても、IoT 機器等のセキュリティ確保や信頼の繋がりの確保のためには、機器検証だけでなく、その他のセキュリティ対策の取組についても考慮すべきとの意見が挙げられた。これらを踏まえ、大局的な視点から、機器検証に限らず機器のサイバーセキュリティ確保のために求められる取組について調査・検討を行った。このために、国内機器メーカーにおけるセキュリティ対策状況や機器メーカーが抱えている課題について調査するとともに、国内外における機器のセキュリティ確保・向上に係る代表的な取組について調査し、国内で取り組むべき施策の方向性について検討した。

4.3.1 国内機器メーカーにおけるセキュリティ対策の状況

機器のセキュリティ対策においては、企画・設計段階から開発・実装・検証、そして出荷後といったライフサイクル全体での対策が必要となる。機器のライフサイクル各段階で求められるセキュリティに関する取組の概要と既存のガイドラインとのマッピングを行った図を図 4-11 に示す。企画・要件定義の段階では、セキュリティに関する要件定義を行うほか、脅威分析を検討する必要がある。また、機器の設計段階では、セキュリティ・バイ・デザインの思想に代表されるように、ライフサイクル全体でのセキュリティ設計を検討する必要がある。開発・実装段階では、セキュアコーディングやテストケース開発、SBOM（Software Bill of Material）の生成、静的解析等の取組を推進することが望まれるほか、検証段階では、動的解析や脆弱性検証等の機器検証を実施することが望まれる。検証により抽出されたリスクに対して追加対応を行った後、出荷を行う必要がある。出荷・運用・廃棄の段階では、機器のサポート体制を構築・運用するほか、機器のセキュリティに関する PSIRT の構築・運用、ソフトウェアやファームウェアの更新対応を行うことが望まれる。



出所）各種ガイドラインに基づき三菱総合研究所作成

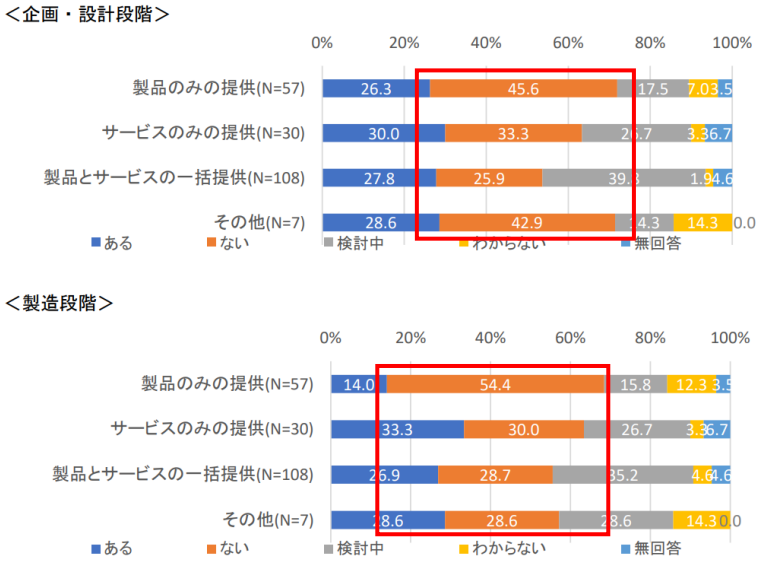
図 4-11 機器ライフサイクルにおいて求められる対策と既存ガイドラインのマッピング[18]

以降では、IPA 調査結果[19]に基づき、国内の IoT 機器等のメーカーにおけるセキュリティ対策の状況及び当該メーカーが抱えているセキュリティ対策上の課題について概説する。

まず、企画・要件定義段階から開発・実装段階におけるセキュリティ対策に関する取組状況について、図 4-12 に示すとおり、企画・設計段階におけるセキュリティ方針・基準（具体的なセキュリティ対策手順や技術詳細）が「ある」と回答した機器メーカーは全体の 27.3%であり、「ない」と回答したメーカーは全体の 33.2%であった。また、製造段階におけるセキュリティ方針・基準が「ある」と回答した機器メーカーは全体の 23.9%であり、「ない」と回答したメーカーは 36.1%であった。したがって、いずれの段階についても、セキュリティ方針・基準を策定しているメーカーは限定的である。また、図 4-13 に示すとおり、開発段階において重要となるセキュアプログラミング技術の適用やコーディング規約の利用等の脆弱性対策を行っているメーカーは 4 割程度と少ない状況であった。

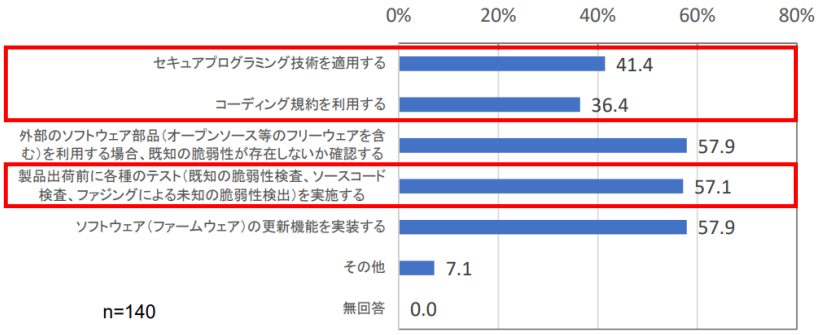
[18] 特定機器分野ではなく、IoT 機器等全般を対象としたガイドラインのみを一部抜粋。点線は IoT 機器等を対象としたガイドラインではないことに留意。

[19] IPA「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」より。2017 年 11 月～12 月に実施した有効回答数 205 件のアンケート調査結果に基づく。



出所）IPA「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

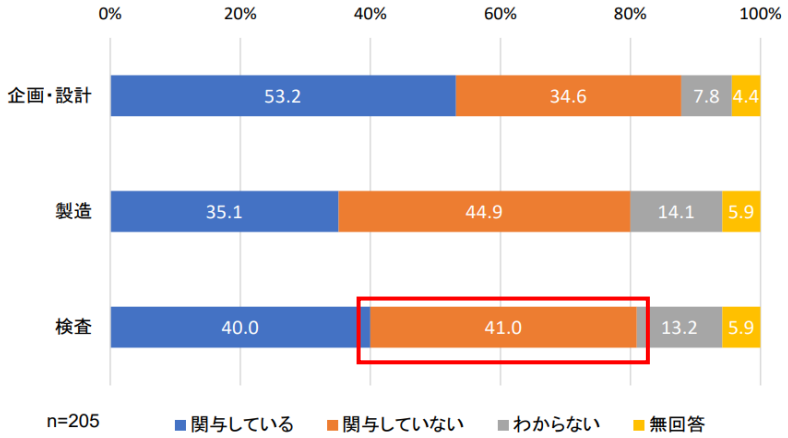
図 4-12 機器メーカーにおける企画・設計段階、製造段階でのセキュリティ方針・基準の有無



出所）IPA「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

図 4-13 機器メーカーにおける脆弱性対策の実施状況

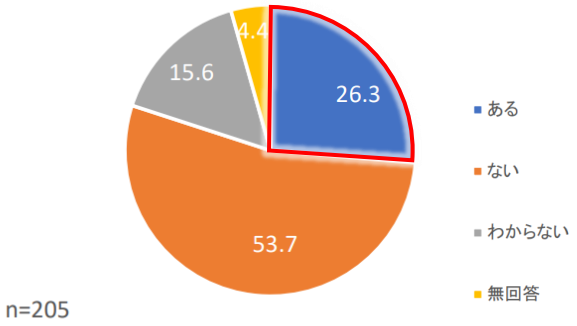
検証段階におけるセキュリティ対策に関する取組状況について、上部図 4-13 で示されるとおり、製品出荷前に各種検証（既知の脆弱性検査、ファジング等）を実施しているメーカーは 60%未満であった。また、図 4-14 に示すとおり、検証段階においてセキュリティ担当部門の関与が「ある」と回答したメーカーは 40.0%であり、「ない」と回答したメーカーは 41.0%であった。したがって、セキュリティ担当部門が関与せずに、機器出荷前の検証が実施されているケースも存在することが分かる。



出所）IPA「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

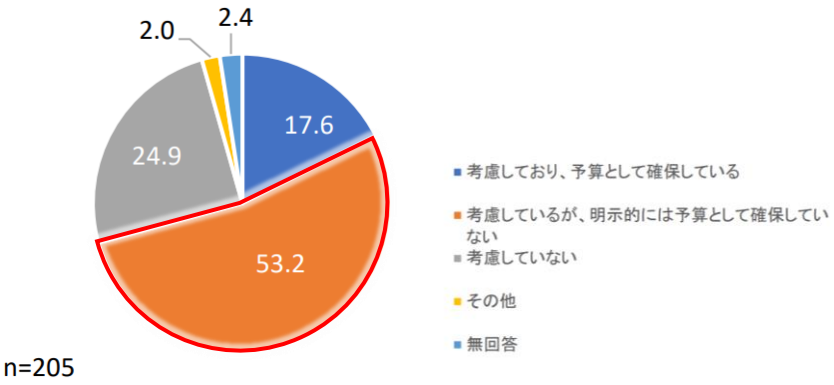
図 4-14 機器メーカーにおけるセキュリティ担当部門の関与状況

最後に、出荷・運用・廃棄段階でのセキュリティ対策に関する取組状況について、図 4-15 に示すとおり、26.3%のメーカーにおいて、製品販売後に脆弱性が発見された経験を有する結果が得られた。製品販売後に顧客に提供する脆弱性対策としては、パッチの作成・リリースが 83.3%と最も多いが、製品販売後のサポート時のセキュリティ対策費について、図 4-16 に示すとおり、「考慮しているが、明示的に予算としては確保していない」という回答が 53.2%と最も多く、製品販売後の対応について予算として確保しているメーカーは 17.6%にとどまった。



出所）IPA「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

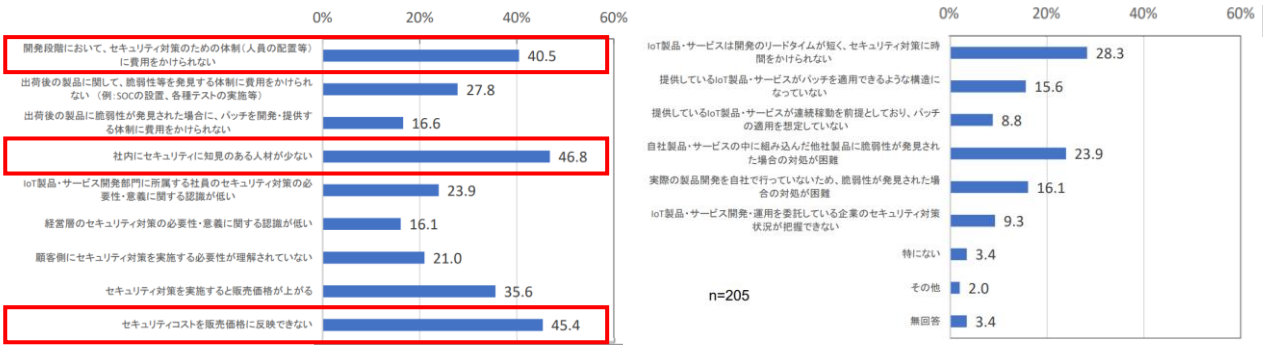
図 4-15 機器メーカーにおける製品販売後に脆弱性が発見された経験の有無



出所）IPA「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

図 4-16 機器メーカーにおけるサポート時のセキュリティ対策費用の有無

機器メーカーにおけるセキュリティ対策の課題を図 4-17 に示す。「社内にセキュリティに知見のある人材が少ない」が 46.8%と最も多く、次点で「セキュリティコストを販売価格に反映できない」が 45.4%、そして「開発段階において、セキュリティ対策のための体制（人員の配置等）に費用をかけられない」が 40.5%と続いた。したがって、半数程度の機器メーカーが、セキュリティ対策に要するコスト負担や、セキュリティ対策にあたっての人材不足の側面で課題を抱えていることが分かる。前者の課題に関して、セキュリティ対策に要するコスト負担は製品の販売価格に反映されるところ、機器メーカーにおける機器開発へのセキュリティ対策の取組を適切に評価するとともに、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製品が積極的に導入されるような社会の仕組みを構築することが望まれる。また、後者の課題に関して、機器メーカーにおけるセキュリティ対策の人材不足を解決する人材支援策を講じることが望まれる。



出所）IPA「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」

図 4-17 機器メーカーにおけるセキュリティ対策の課題

次項では、これらの課題解決に関連する国内外の取組として、機器のセキュリティ確保・向上に係る国内外政府機関の代表的な取組及び機器のセキュリティ対策のためのセキュリティ人材確保に関する海外政府機関による代表的な取組について説明する。

4.3.2 機器のサイバーセキュリティ確保に係る既存の取組

（1） 国内政府機関における機器のセキュリティ確保・向上に係る代表的な取組

機器のセキュリティ確保・向上に係る取組として、図 4-11 に示したとおり機器ライフサイクルの各段階におけるセキュリティ対策を支援するガイドラインが複数公表されているほか、国内政府機関により様々な取組が推進されている。国内政府機関による機器のセキュリティ確保・向上に係る代表的な取組を表 4-18 に示す。国内政府機関においても様々なガイドラインやフレームワークが公表されているほか、総務省の省令改正により、電気通信業者のネットワークに直接接続する機器については、最低限のセキュリティ対策が義務化されている。

表 4-18 機器のセキュリティ確保・向上に係る国内政府機関による代表的な取組

主体	取組名称	概要	目的	時期
経済産業省	「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の策定	フィジカル空間とサイバー空間のつながりの信頼性の確保の考え方を整理。	サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされるリスクに備えること。	2020 年 11 月 15 日
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」の策定	検証事業者及び検証依頼者が実施すべき事項やコミュニケーションにおいて留意すべき事項を整理。	セキュリティ検証における、検証サービス事業者が実施すべき事項を示すこと。	2021 年 4 月 19 日
IPA	「つながる世界の開発指針 第２版」の策定	IoT 製品があらゆるモノとつながることを想定し、IoT 製品の開発者が開発時に考慮すべきリスクや対策を指針として明確化。	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ることで、つながる世界のリスクに備えること。	2017 年 6 月 30 日
IPA	「脆弱性対処に向けた製品開発者向けガイド」の策定	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。	製品開発者が実施している脆弱性対処を積極的に開示しアピールすること。	2020 年 8 月 27 日
総務省	端末設備等規則（省令）（第34条の10）の改正	電気通信業者のネットワークに直接接続する IoT 機器に対するアクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の義務化。	電気通信業者のネットワークに直接接続する機能を持つ IoT 機器に対して、最低限のサイバーセキュリティ対策を求めること。	2020 年 4 月 1 日 施行

主体	取組名称	概要	目的	時期
総務省／NICT	NOTICE	IoT 機器へのアクセスによる、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を行う取組。	対策に不備がある IoT 機器を調査し、利用者自身で適切なセキュリティ対策を講じること。	2019 年 2 月 1 日開始
NISC ／デジタル庁	IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ	政府機関等の重要な IT 製品・サービス等の調達時にサプライチェーン・リスクの懸念有無を確認し、懸念が払拭できない場合には、代替品への差替や低減策の実施等を助言する取組。	政府の重要業務の調達におけるサイバーセキュリティ上の深刻な悪影響を軽減し、政府機関等におけるサイバーセキュリティ対策を一層向上させること。	2018 年 12 月 10 日

以降で各取組の概要について説明するが、前項で述べた機器メーカーが抱える課題に直接的に資する、機器メーカーにおける機器開発へのセキュリティ対策の取組を評価する施策や適切なセキュリティ対策が施された製品の導入支援に関する施策、人材的側面を支援する施策等は講じられていない状況である。

1）「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の策定

2020 年 11 月 5 日、経済産業省は IoT や AI によって実現される「Society5.0」、「Connected Industries」におけるフィジカル空間とサイバー空間のつながりの信頼性の確保の考え方を整理した「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」を策定した[20]。このフレームワークは、IoT 機器・システムの性質や利用環境によって課題が一様ではないことに着目し、IoT 機器・システムをリスクに応じてカテゴライズしたうえで、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示することを目的としている。

フレームワークでは、様々な人命/身体、プライバシー/名誉、資産、生活環境、経済活動への影響、風評等の影響を受ける様々な事象を、「発生したインシデントの影響の回復困難性の度合い」と「発生したインシデントの経済的影響の度合い（金銭的価値への換算）」の 2 つの基準に抽象化して整理するとともに、この 2 つの基準（軸）に基づいて、フィジカル・サイバー間をつなぐ IoT 機器・システムを、当該機器・システムに潜むリスクに基づいてマッピングしている。

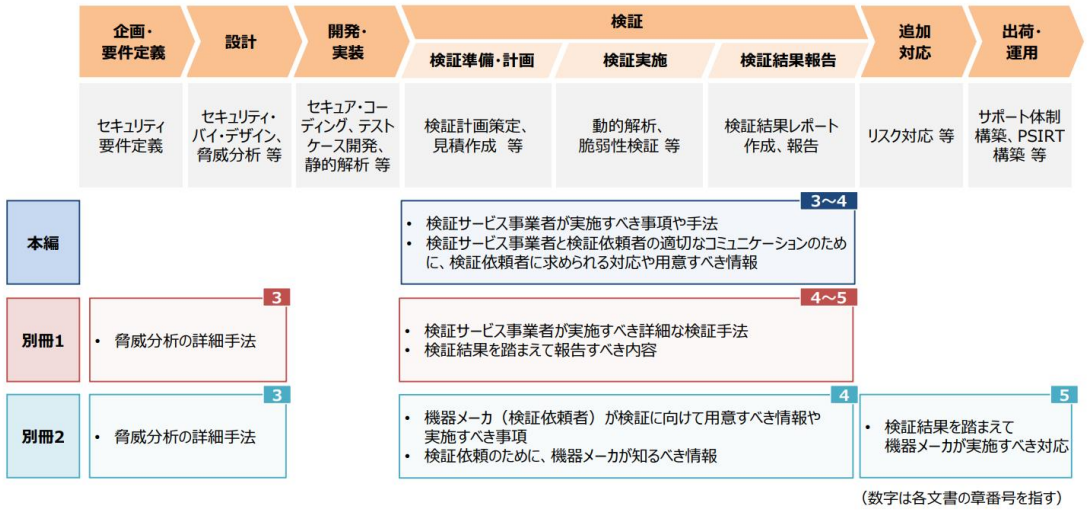
2022 年 3 月に開催された『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースでは、IoT-SSF をより活用しやすいものにすることを目的として、IoT-SSF の実践に向けたユースケース集の案が示されており、具体的なユースケースとして、家庭

[20] https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html

用ガス給湯器の遠隔操作、ドローンを活用した個人による写真撮影、物流倉庫内の AGV による自動ピッキング等が示されている[21]。それぞれのユースケースにおいて、リスクアセスメントに向けた事前準備として必要な情報や事項、IoT-SSF の 2 つの軸をベースとしたリスクアセスメント実施方法、そして、アセスメントの結果を踏まえたリスク対応の方向性が示されている。

2）「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」の策定

2021 年 4 月 19 日、経済産業省は IoT 機器等に対するセキュリティ検証サービスの高度化を目的とし、検証サービス事業者及び検証依頼者が実施すべき事項や、二者間のコミュニケーションにおいて留意すべき事項等について整理した「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」を公開した[22]。この手引きは本編及び 3 つの別冊により構成され、本編及び別冊 1・別冊 2 は図 4-18 に示すとおり、機器開発プロセスにおける「検証」のフェーズに焦点を当て、検証において検証サービス事業者が実施すべき事項及び機器メーカーが検証依頼のために準備すべき事項等を整理している。加えて、別冊 1 及び別冊 2 では、機器に対する脅威分析手法についても示している。



出所）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」

図 4-18 機器開発プロセスにおける手引き本編及び別冊 1・別冊 2 のスコープ

3）「つながる世界の開発指針 第 2 版」の策定

2017 年 6 月 30 日、IPA は安心安全な IoT の実現に向け、IoT システムに関する開発者が最低限考慮すべき事項をまとめた「つながる世界の開発指針」の第 2 版を公開した[23]。本開発指針では、個別具体的な遵守基準ではなく、業界横断的な安全安心の取組の方向性を示している。17 の指針により構成され、機器の開発段階だけでなく、ライフサイクル全体で留意すべき指針が整理されている。

- 指針 1 安全安心の基本方針を策定する

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

22 https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

23 https://www.ipa.go.jp/sec/publish/tn16-002.html

- 指針 2 安全安心のための体制・人材を見直す
- 指針 3 内部不正やミスに備える
- 指針 4 守るべきものを特定する
- 指針 5 つながることによるリスクを想定する
- 指針 6 つながりで波及するリスクを想定する
- 指針 7 物理的なリスクを認識する
- 指針 8 個々でも全体でも守れる設計をする
- 指針 9 つながる相手に迷惑をかけない設計をする
- 指針 10 安全安心を実現する設計の整合性をとる
- 指針 11 不特定の相手とつなげられても安全安心を確保できる設計をする
- 指針 12 安全安心を実現する設計の検証・評価を行う
- 指針 13 自身がどのような状態かを把握し、記録する機能を設ける
- 指針 14 時間が経っても安全安心を維持する機能を設ける
- 指針 15 出荷後も IoT リスクを把握し、情報発信する
- 指針 16 出荷後の関係事業者に守ってもらいたいことを伝える
- 指針 17 つながることによるリスクを一般利用者に知ってもらう

4）「脆弱性対処に向けた製品開発者向けガイド」の策定

2020 年 8 月 27 日、IPA は、IoT 機器等の製品開発者がセキュリティ対策として実施すべき項目を把握できるようすること、実施する対処を徐々にレベルアップできるようすること、一般消費者に自組織の取組み状況をアピールするために実施すべきことを把握できるようにすることを目的とし、「脆弱性対処に向けた製品開発者向けガイド」を公開した[24]。本ガイドは国内外の主要なガイド等から抽出した標準的に実施が求められる対処集の位置づけであり、チェックリストを活用することで、自組織の脆弱性対処の状況が把握可能である。また、レベル分けした対処方法により、自組織の状況に応じた対処から実施可能であるほか、一般消費者にアピールするために、対処の実施状況の開示方法についても掲載されている。本ガイドでは、に示すとおり、製品開発者が実施すべき項目を「方針・組織」、「設計・開発」、「出荷後の対応」の 3 つのフェーズに分け記載している。

表 4-19 「脆弱性対処に向けた製品開発者向けガイド」における製品開発者が実施すべき脆弱性対処項目

カテゴリ	No	項目
I.方針・組織	1	製品セキュリティポリシーの策定
	2	セキュリティサポート方針の明示
	3	製品セキュリティを維持するための体制と管理
II. 設計・開発	4	セキュリティを確保するための設計
	5	アップデートを考慮した設計
	6	既知の脆弱性解消
	7	セキュアコーディング

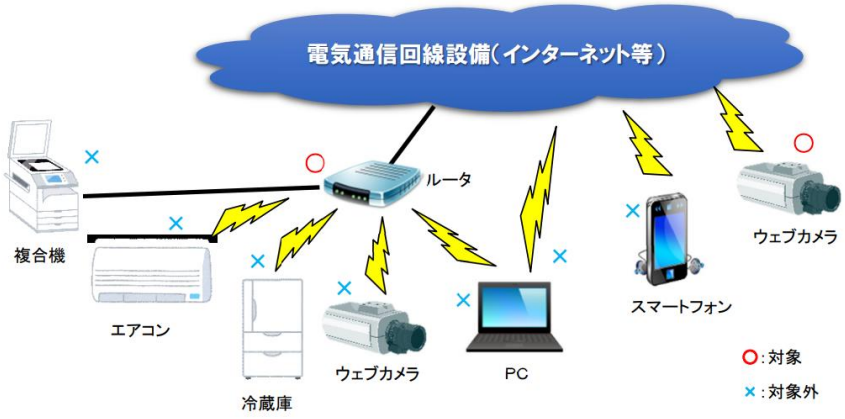
[24] https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

カテゴリ	No	項目
	8	開発環境のセキュリティ確保
	9	開発時の脆弱性検査
III. 出荷後の対応	10	製品と構成要素の脆弱性監視
	11	脆弱性報告の受付・対策情報の公表
	12	一般消費者の製品利用時における実施事項の明示

出所）IPA「脆弱性対処に向けた製品開発者向けガイド」

5）端末設備等規則（省令）（第 34 条の 10）の改正

2019 年 3 月 1 日、総務省は「端末設備等規則及び電気通信主任技術者規則の一部を改正する省令（平成 31 年総務省令第 12 号）」を公布した。そして、2020 年 4 月 1 日、端末設備等規則の一部改正が施行され、電気通信業者のネットワークに直接接続する 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が義務化された。対象となる設備のイメージは図 4-19 に示すとおりであり、例えば、ルータ、ウェブカメラ等は該当するが、IP を使用しない機器、専用線のみにつながる機器等は対象外である。



出所）総務省「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第2版）」[25]

図 4-19 端末設備等規則（第 34 条の 10）に係る技術基準適合認定等の対象機器の範囲のイメージ

6）NOTICE（National Operation Towards IoT Clean Environment）

2019 年 2 月 20 日より、総務省及び NICT は、インターネットサービスプロバイダー（ISP）と連携し、IoT 機器へのアクセスによる、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を行う取組である NOTICE を開始している。この取組では、NICT がインターネット上の IoT 機器に容易に推測されるパスワードの入力等を行うことで、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報を ISP に通知する。ISP は、NICT から受け取った情報を元に当該機器の利用者を特定し、電子メールや郵送などにより注意喚起を行う。2020 年 8 月時点で 62 社の ISP と連携し、当該 ISP の約 1.1 億の IP アドレスに対して調査を実施した。調査の結果、

[25] https://www.soumu.go.jp/main_content/000744264.pdf

ログインが可能であり、注意喚起対象として ISP に通知された IoT 機器の件数は 2020 年 8 月分で 309 件であった[26]。

7）IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ

2018 年 12 月 10 日、NISC を中心とした日本政府は、「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」を発出、2021 年 9 月 1 日には一部改正がなされた[27]。この申合せは、政府機関等の重要な IT 製品・サービス等の調達時にサプライチェーン・リスクの懸念有無を NISC やデジタル庁が確認し、懸念が払拭できない場合には、代替品への差替や低減策の実施等を助言することを申し合わせたものである。当初は政府行政機関のみが対象であったが、改正により独立行政法人やサイバーセキュリティ基本法に定める指定法人も対象に加えられた。対象となる情報システム・機器・役務等について、通信回線装置、サーバ装置、端末、複合機等の一般的な ICT 機器のほか、特定用途機器、ソフトウェア、周辺機器、外部電磁的記憶媒体も含まれる。また、通信サービスやクラウドサービスの提供等の役務も対象となる。NISC の報告によれば、令和 2 年度の申合せ運用実績として、助言数は 3,515 件であり、そのうち 190 件（5%）を「懸念あり」として助言したと発表している[28]。

（2）諸外国政府機関における機器のセキュリティ確保・向上を支援する代表的な取組

海外政府機関による機器のセキュリティ確保・向上に係る代表的な取組を表 4-20 に示す。米国 NIST をはじめとして、諸外国においても機器ライフサイクルの各段階におけるセキュリティ対策を支援するガイドラインが複数公表されているほか、近年では、機器メーカーにおけるセキュリティ対策の取組を評価するとともに、適切なセキュリティ対策が施された製品の導入を促進するために、製品に対するセキュリティラベリング制度が検討されている。既にシンガポールやフィンランドで制度が開始しているほか、米国においても、大統領令によってラベリング制度のパイロットプログラム実施が指示されている。

表 4-20 機器のセキュリティ確保・向上に係る海外政府機関による代表的な取組

主体	取組名称	概要	目的	時期
米国 NIST	“NISTIR 8259” の策定	IoT 機器のメーカーに推奨されるサイバーセキュリティに関連する活動を整理したガイドライン。	IoT 機器メーカーが開発する製品の安全性を向上させるための推奨事項を示すこと。	2020 年 5 月 29 日

[26] https://www.soumu.go.jp/main content/000706574.pdf
[27] https://www.nisc.go.jp/active/general/pdf/choutatsu moushiawase0901.pdf
[28] https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai18/pdf/18shiryou0201.pdf
なお、助言件数は、個々の機器に対する助言件数ではなく、助言にあたって対象政府機関等から提示される機器リストの数を計上したものであることに留意。

主体	取組名称	概要	目的	時期
米国 NIST	Cybersecurity Labeling for Consumer IoT Products	2021 年 5 月の米国大統領令によってパイロット版の開始が指示された、IoT 製品の安全性を確認するためのラベリング制度。これまで、NIST により、ラベリング制度構築に向けた推奨事項の検討等がなされている。	一般消費者が IoT 製品の安全性を判断できるよう、セキュアな製品に対してラベルを付与すること。	2022 年 2 月 4 日に推奨事項に関する文書が公開
カリフォルニア州	SB-327 Information privacy: connected devices	IoT 機器のメーカーに対して、機器や保存された情報を不正アクセス、破壊、使用、変更及び開示から保護する相応なセキュリティ機能を搭載することを求めた法律。	IoT 機器に対するセキュリティ強化を行うこと。	2020 年 1 月 1 日 施行
英国 DCMS[29]	“Code of Practice for Consumer IoT Security”の策定	消費者向け IoT 機器及び関連サービスのセキュリティ確保のために機器メーカーが実施すべき 13 項目を行動規範としてまとめたもの。本規範に基づき EN 303 645 が策定。	消費者向け IoT 製品の開発、製造、販売に携わる利害関係者を支援すること。	2018 年 10 月 14 日
英国 DCMS	“Product Security and Telecommunications Infrastructure” 法案の提出	インターネットに接続する IoT 機器に対して、機器導入時のデフォルトパスワードの禁止等を義務化する法案。遵守しない企業に対する罰金に関する条項も含まれている。	インターネットに接続される IoT 製品に対して、脆弱性の悪用によるサイバー攻撃を防ぐための最低限の対策を求めること。	2021 年 11 月 24 日 庶民院に提出

[29] Department for Digital, Culture, Media and Sport の略で、英国デジタル・文化・メディア・スポーツ省のこと。

主体	取組名称	概要	目的	時期
独国 BSI[30]	IT Security Label	セキュリティ要件を満足している IT 製品やサービスに対してラベリングを行う制度。	IT 製品やサービスのセキュリティ特性を簡単に認識できるようにすることで、消費者の情報ニーズの高まりに対応し、市場での製品アピールの機会を提供すること。	2021 年 12 月開始
シンガポール CSA[31]	Cybersecurity Labelling Scheme (CLS)	セキュリティ要件を満足している消費者向け IoT 製品(ネットワーク接続する製品)に対してラベリングを行う制度。	消費者がより安全な IoT 製品を購入・利用できるようにすること。	2020 年 10 月開始
フィンランド TRAFICOM[32]	Finnish Cybersecurity Label	セキュリティ要件を満足している消費者向け IoT 製品(ネットワーク接続する製品)に対してラベリングを行う制度。	製品に対する脅威に対応し、安全な環境で消費者が製品を利用できるようにすること。	2019 年 11 月開始

以降では、各取組の概要について説明する。ただし、国内で取り組むべき施策の方向性検討に資する、IoT 製品へのラベリング制度に係る米国、ドイツ、シンガポールの取組については、詳細に説明する。

1) 米国:“NISTIR 8259”の策定

2020 年 5 月、米国 NIST は IoT 機器のメーカー向けサイバーセキュリティ対策指針をまとめた文書 NISTIR 8259 : Foundational Cybersecurity Activities for IoT Device Manufacturers を公表した[33]。この文書は、IoT 機器を管理する組織向けの推奨事項をまとめた NISTIR 8228 に対し、製品の販売前及び販売後に影響する活動として、IoT 機器の製造者に推奨される 6 つのサイバーセキュリティに関連する活動を整理した。具体的な 6 つの活動は以下のとおりである。

【販売前に影響する活動】

- 活動 1:想定顧客の特定、想定ユースケースの定義
- 活動 2:顧客が有するサイバーセキュリティのニーズ及び目的の調査
- 活動 3:顧客のニーズ及び目的への対処方法の決定

[30] Bundesamt für Sicherheit in der Informationstechnik の略で、ドイツ連邦政府情報セキュリティ庁のこと。
[31] Cyber Security Agency of Singapore の略で、シンガポールサイバーセキュリティ庁のこと。
[32] Finnish Transport and Communications Agency の略で、フィンランド運輸通信庁のこと。
[33] https://csrc.nist.gov/publications/detail/nistir/8259/final

- 活動 4：顧客のニーズ及び目的の適切なサポートに向けた計画（ハードウェア、ソフトウェアの適切なプロビジョニング、ビジネスリソースの考慮）

【販売後に影響する活動】

- 活動 5：顧客とのコミュニケーション手段の定義
- 活動 6：顧客に伝える内容と伝達方法の決定（製造業者の設計・開発時のリスク関連の仮説、サポートと寿命、デバイス構成・機能、ソフトウェアの更新、デバイスの廃止オプション、技術的及び非技術的手段）

活動 3 におけるベースラインとなる 6 つのコアサイバーセキュリティ機能については、関連文書の NISTIR 8259A において以下のとおり定義されている[34]。

1. 資産の識別：
   IoT 機器を論理的・物理的に一意に識別できること。
2. 製品の構成：
   IoT 機器のソフトウェアの構成変更を、正規のエンティティのみが行うことができること。
3. データ保護：
   IoT 機器が保存・伝送するデータを不正アクセス及び改ざんから保護することができること。
4. インタフェースのアクセス制御：
   IoT 機器のインタフェースへの論理アクセス、及びインタフェースで利用されるプロトコルとサービスを正規のエンティティのみに制限できること。
5. ソフトウェアの更新：
   IoT 機器のソフトウェアは、安全かつ設定可能なメカニズムを用いる正規のエンティティにみによってのみ更新できること。
6. サイバーセキュリティ状態認識：
   IoT 機器は自身のセキュリティに関する状態を報告し、その情報に対するアクセスを正規のエンティティのみに制限すること。

また、関連文書の NISTIR 8259B では、非技術的なコアサポート機能として、4 つの機能が定義されている。

1. ドキュメンテーション：
   メーカーやメーカーの支援団体は、顧客による製品の購入前、及び製品のライフサイクル全体を通じて、当該 IoT 製品やその製品コンポーネントのサイバーセキュリティに関連する情報を作成、収集、及び保管する機能を有すること。
2. 情報及び問合せの受付：
   メーカーやメーカーの支援団体は、IoT 製品及びその製品コンポーネントのサイバーセキュリティに関連する情報や問い合わせを顧客等から受け付ける機能を有すること。
3. 情報の発信：
   メーカーやメーカーの支援団体は、IoT 製品及びその製品コンポーネントのサイバーセキュリティに関連する情報を発信する機能を有すること。（発信対象の例：顧客や当該 IoT 製品に関する

[34] https://csrc.nist.gov/publications/detail/nistir/8259a/final

ステークホルダー）

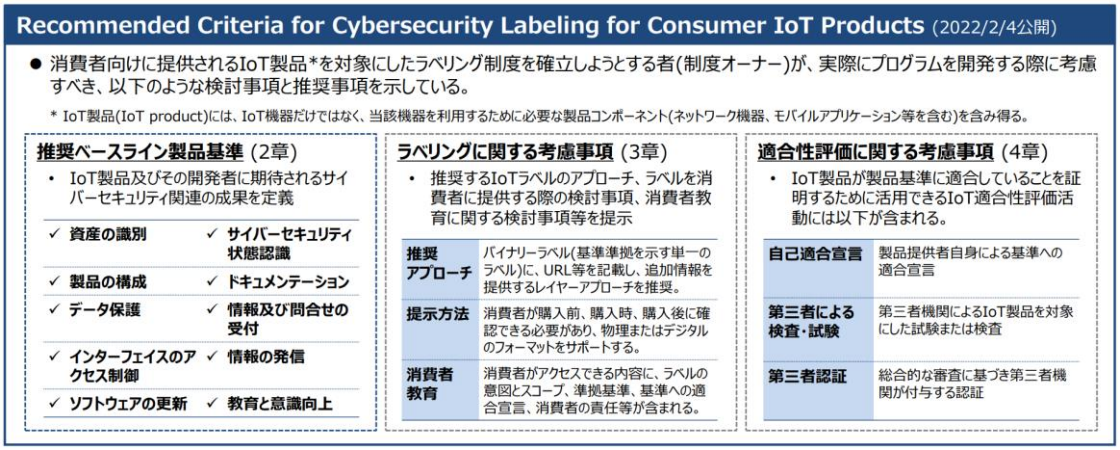
4. 教育と意識向上：

メーカーやメーカーの支援団体が、IoT 製品とその製品コンポーネントのサイバーセキュリティに関連する情報や考慮事項、機能などについて、顧客やその他の人々の認識を高め、教育する機能を有すること。

2）米国：Cybersecurity Labeling for Consumer IoT Products

2021 年 5 月 12 日、“Presidential Executive Order on Improving the Nation’s Cybersecurity（14028）”によって、NIST に対し、消費者向け IoT 機器に関するラベリングプログラムを開始するよう指示が出された[35]。大統領令における IoT 製品のサイバーセキュリティラベリング規定は、製品間の比較を可能にし、IoT サイバーセキュリティへの配慮について消費者に啓蒙することで、消費者が IoT を購入する際の意思決定を支援することを目的としている。

これを受け、2022 年 2 月 4 日、NIST は“Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things（IoT）Products”を公開した[36]。この文書の概要を図 4-20 に示す。文書では、消費者向け IoT 製品のラベル基準、ラベルデザインや消費者教育、適合性評価に関する考慮事項が推奨されている。以降では、本文書の詳細について記載する。



出所）経済産業省『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タスクフォースの検討の方向性[37]

図 4-20 NIST “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”の概要

対象となる消費者向けの IoT 機器・IoT 製品に関して、NIST は IoT 機器を「少なくとも 1 つのトランスデューサ（センサー又はアクチュエータ）及び少なくとも 1 つのネットワークインタフェースを備えたコンピューティング機器」と説明している。また、IoT 製品とは、「IoT 機器単体及び IoT 機器を使用するた

[35] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[36] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

[37] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/pdf/006_03_00.pdf

めに必要な追加の製品コンポーネント」と定義している。文書では、特に以下の 3 種類の IoT 製品を考えることが有益であると述べられている。

- ネットワーキング／ゲートウェイ・ハードウェア（例：IoT 機器が使用されるシステム内のハブ）
- 付属アプリケーションソフトウェア（例：IoT 機器と通信するためのモバイルアプリ）
- バックエンドサービス（例：IoT 機器からのデータを格納や処理することができるクラウドサービス）

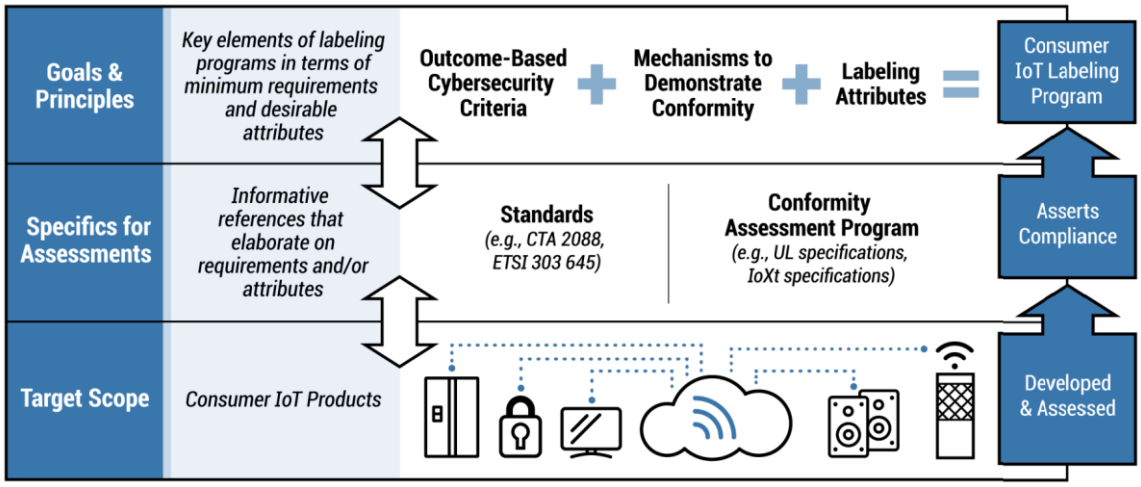
これらの製品コンポーネントは、IoT 機器やそれが作成し使用するデータにアクセスできるため、攻撃を受けた場合、IoT 機器や顧客などに影響を与える可能性がある。

消費者向け IoT 製品のラベリングプログラムの一環として IoT 製品及び IoT 製品開発者に期待されるサイバーセキュリティの成果を定義するために、NIST は、NISTIR 8259 に基づく以下のベースライン基準を推奨している。

1. 資産の識別：
   IoT 機器を論理的・物理的に一意に識別できること。
2. 製品の構成：
   IoT 機器のソフトウェアの構成変更を、正規のエンティティのみが行うことができること。
3. データ保護：
   IoT 機器が保存・伝送するデータを不正アクセス及び改ざんから保護することができること。
4. インタフェースのアクセス制御：
   IoT 機器のインタフェースへの論理アクセス、及びインタフェースで利用されるプロトコルとサービスを正規のエンティティのみに制限できること。
5. ソフトウェアの更新：
   IoT 機器のソフトウェアは、安全かつ設定可能なメカニズムを用いる正規のエンティティにみによってのみ更新できること。
6. サイバーセキュリティ状態認識：
   IoT 機器は自身のセキュリティに関する状態を報告し、その情報に対するアクセスを正規のエンティティのみに制限すること。
7. ドキュメンテーション：
   メーカーやメーカーの支援団体は、顧客による製品の購入前、及び製品のライフサイクル全体を通じて、当該 IoT 製品やその製品コンポーネントのサイバーセキュリティに関連する情報を作成、収集、及び保管する機能を有すること。
8. 情報及び問合せの受付：
   メーカーやメーカーの支援団体は、IoT 製品及びその製品コンポーネントのサイバーセキュリティに関連する情報や問い合わせを顧客等から受け付ける機能を有すること。
9. 情報の発信：
   メーカーやメーカーの支援団体は、IoT 製品及びその製品コンポーネントのサイバーセキュリティに関連する情報を発信する機能を有すること。（発信対象の例：顧客や当該 IoT 製品に関するステークホルダー）
10. 教育と意識向上：
    メーカーやメーカーの支援団体が、IoT 製品とその製品コンポーネントのサイバーセキュリティに

関連する情報や考慮事項、機能などについて、顧客やその他の人々の認識を高め、教育する機能を有すること。

文書で示されている推奨事項や考慮事項に従った消費者向け IoT 製品ラベリングプログラムの実施には、制度オーナーが必要であると言及されている。制度オーナーとは、ラベリングスキームを管理・関しする主体である。そして、基準の調整、適合性評価要件の定義、ラベルと関連情報の開発、関連する消費者への働きかけと教育の実施に責任を負う。制度オーナーは、公共機関又は民間組織が担うことができるとしている。また、既存のリソースを利用することで、文書で推奨している基準の実施を可能にし、これらのリソースの継続的な開発と拡張を促進することができると言及されている。図 4-21 では、制度オーナーが既存のリソースを利用する方法が示されている。制度オーナーは、UL Specifications や IoXt Specifications 等の既存の適合性評価プログラムを利用し、それらのプログラムオーナーと協力して、消費者向け IoT ラベリング制度の全体又は一部の構築に役立てることができる。また、ANSI/CTA 2088 や ETSI EN 303 645 等の既存基準を活用することもでき、これにより、国際的な消費者向け IoT ラベリングプログラムとの整合性確保など、さらなる利点を得られる可能性がある。なお、既存の基準やプログラムをラベリングプログラムの一部として使用するかどうかは、制度オーナーの裁量に委ねられる。



出所）NIST “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products” (2022)[38]

図 4-21 消費者向け IoT ラベリングの制度オーナーが既存のリソースを利用する方法を示した図

IoT 製品に対して個別に利用できる適合性評価プログラムが存在する可能性があるため、これらのプログラムで使用されている既存のスキームとの調和と分断について考慮することは重要であると述べられている。ただし、技術基準や適合性評価、ラベリング要件は、他のプログラムの一部または全部と完全に一致させることができない可能性があり、制度オーナーは、調和の度合いを検討する際に、調和による利点と分断による課題を考慮する必要があると述べられている。

文書では、与えるラベルに関して、製品が基準を満たしていることを示す単一ラベル（バイナリラベル）

[38] 脚注 36 参照。

とし、関心のある消費者がオンラインで詳細な情報にアクセスできるよう、URL 又は QR コードをラベルに記載することを推奨している。またラベルは、購入前と購入時に購入場所において、そして購入後にも消費者が利用できるようにする必要があり、物理的な形式とデジタル形式の両方を適切にサポートする柔軟性を持つことを推奨している。

加えて、文書ではラベルの認知度を確立・向上させ、ラベリングスキームの透明性を消費者に提供し、IoT 製品の関係者間でラベルについて確認するための共通言語を確保するため、単一ラベルに関する適切な消費者教育キャンペーンを開発することが推奨されている。消費者教育は複雑な事業であるため、複数の IoT 製品セキュリティ関係者（制度オーナー、小売業者、メーカー、業界団体、非営利のセキュリティ団体、学術研究機関、政府等）が責任を共有する必要があるとも言及されている。

消費者がオンラインでアクセスできるようにする必要がある最低限の情報として、以下の項目が挙げられている。

- 意図と範囲：潜在的な誤解への対処を含め、ラベルが意味すること及び意味しないこと（例：ラベルのセキュリティ基準を満たすことでリスクは低減するが完全に排除できるわけではないこと、ラベル付き製品はラベルなし製品よりも安全であるとは必ずしも限らないこと等）、並びにラベルは製品推奨を意味するものではないこと。
- 基準：基準にはどのようなサイバーセキュリティ特性が含まれ、なぜ、どのようにそれらが選択されたのか。製品の一般的な使用目的に関し、消費者と他者の両方のセキュリティリスクに対して、基準がどのように対処するか。
- 平易な言葉で書かれた専門用語の用語集。
- 適合性評価に関する一般的な情報：サイバーセキュリティの特性がどのように評価されるか。
- 適合性宣言：ラベルが最後に付与された日を含む、製品の基準への適合に関する具体的な宣言。
- 範囲：ラベルの対象となる製品の種類と、ラベル付き製品を消費者が簡単に識別する方法。
- 適用範囲の変更：新たなサイバーセキュリティの脅威や脆弱性の出現に伴う製品ラベリングへの影響。
- 製品寿命が近い IoT 製品へのセキュリティ配慮及び製品がネットワークに接続されなくなった場合の機能への影響。
- 消費者への期待：消費者がソフトウェアの安全性を確保するために負う責任と、消費者の行動がソフトウェアのサイバーセキュリティにどのような影響を及ぼす可能性があるか。
- ラベリングプログラムの連絡先及び消費者が製品ラベルに関してベンダーに苦情を申し立てる方法に関する情報。

ラベルをデザインする際には、ラベルデザインのユーザビリティと消費者教育資料のユーザビリティを、厳密な消費者テストを通じて評価する必要があると言及されている。またラベリング制度開始後は、多様な消費者サンプルを用いた定期的なテストが不可欠であり、そのテストにはラベルアプローチの継続的な適切性と有用性、消費者の購入意思決定への影響、時間の経過によるブランド認知度の向上を評価するための市場調査も含められることが述べられている。

適合性評価活動の構造や管理について、文書は制度オーナーが決定するよう述べている。消費者向け IoT 機器が技術要件に適合していることを実証するために活用できる IoT 適合性評価活動について、以下の 3 つが例示されている。

- 自己適合宣言（自己証明）
  適合宣言は、消費者向け IoT 機器を提供する組織が行う。これは、定義された一連の基準に対する自己証明である。
- 第三者による検査・試験
  定義された基準に基づき、第三者機関による消費者向け IoT 機器の試験・検査を行う。
- 第三者認証
  IoT 製品が定義された基準を満たしているという総合的な審査を行う。

NIST は、2022 年 5 月 12 日までに、消費者向け IoT 製品のサイバーセキュリティラベリングに関する概要報告書を発行する予定である。この報告書では、これまでに寄せられたコメントに加え、パイロット版や関連する問題についての一般からの追加的なコメントも考慮される予定である。

3）カリフォルニア州：SB-327 Information privacy: connected devices

2018 年 9 月 28 日、米国カリフォルニア州において IoT 機器（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た法律“SB-327 Information privacy: connected devices”が成立し、2020 年 1 月 1 日より施行となった[39,40]。本法律はカリフォルニア州民法第 3 編第 4 部に追加され、当該機器の製造者に対して、合理的なセキュリティ機能を装備させることを求めている。また、機器がローカルエリアネットワークの外部に認証手段を備えている場合、製造者に対し、各機器の固有のパスワードを割り当てるか、デフォルトのパスワードのままでは接続して使用することができないようにすることを求めた。

規制対象は当該機器の製造者であり、カリフォルニア州で販売する製造者はすべて規制対象である。なお、OEM 製造も規制の対象に含まれる。適用対象機器として、インターネットに接続される機器は対象となるが、「その機能性が、その執行権限に従って連邦政府機関により公布された連邦法、規則またはガイダンスに基づくセキュリティ要件の対象となる接続機器には、適用されない」ことが明記されている。このような機器の例として、例えば、産業用 IoT 機器、コネクテッドカーのような大型 IoT 機器のほか、医療機器は適用対象外となる。

4）英国：“Code of Practice for Consumer IoT Security”の策定

2018 年 10 月 14 日、英国 DCMS は消費者向け 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”を公開した[41]。本行動規範は、消費者向け IoT 製品の設計段階で安全性が確保されるよう、またユーザー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、こうした製品の開発、製造、販売に携わる利害関係者を支援することを目的としており、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

[39] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[40] 湯淺 墾道、IoT セキュリティ法制をめぐって https://digitalforensic.jp/wp-content/uploads/2019/03/law-15-4.pdf
[41] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

消費者向け IoT 製品が対象となる。本行動規範は日本語版も公開されている[42]。具体的な 13 の行動規範は以下のとおりである。

1. 初期パスワードを設定しない
2. 脆弱性に関する情報の公開方針を導入する
3. ソフトウェアを定期的に更新する
4. 認証情報とセキュリティ上重要なデータを安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの整合性を確認する
8. 個人データの保護を徹底する
9. 機能停止時のシステムの復旧性を確保する
10. システムの遠隔データを監視する
11. 消費者が個人データを容易に削除できるように配慮する
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配慮する
13. 入力データを検証する

なお、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[43]。

5) 英国:"Product Security and Telecommunications Infrastructure"法案の提出

2021 年 11 月 24 日、英国庶民院に"Product Security and Telecommunications Infrastructure"法案が提出された[44]。この法案はインターネットに接続するスマートフォン、スマート TV、スマートスピーカー等の機器に対して、セキュリティ対策を義務化する内容が含まれており、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 点を求めている。法案には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。対象となる企業について、機器のメーカーだけでなく、輸入業者や販売業者も含まれる。なお、法案が可決された後、完全に施行される前に少なくとも 12 ヶ月の準備期間を設ける予定であることが示されている。

---

42 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973920/054718_DCMS_IoT_Code_of_Practice_JAPANESE_V2.pdf

43 https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
なお、EN とは EU 加盟国の統一規格のことで、EU 加盟各国は、EN 規格を自国の国家規格として採用することが義務付けられている。

44 https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets

6）独国：IT Security Label

2021 年 12 月よりドイツの BSI は、IT Security Label 制度を開始した[45]。本制度は IT 製品やサービスを対象としたラベルであり、製品やサービスのセキュリティ特性を簡単に認識できるようにすることで、消費者の情報ニーズの高まりに対応し、市場での製品アピールの機会を提供することを目的としている。2022 年 2 月時点で、4 つのサービスに対してラベルの付与が行われている[46]。

2022 年 2 月時点では、ブロードバンドルータ及び電子メールサービスに対してラベル申請が可能となっている。前者はブロードバンドルータ対する技術ガイドラインである BSI TR-03148[47]に基づく申請、後者は電子メールサービスの技術ガイドラインである BSI TR-03108[48]に基づく申請が必要となる。将来的には、別のカテゴリの製品についてもラベル申請が可能となる予定である。

ラベルの申請の際、メーカーは製品やサービスが各製品カテゴリの要件を満たしていることを確認し、そのことを宣言する必要がある[49]。BSI は、メーカーからの申請書とメーカーによる宣言の完全性と妥当性を審査する。ラベル付与が認められた場合は、BSI から一定期間（製品カテゴリによって変わりうるが通常は 2 年間）、IT セキュリティラベルを使用する権利が与えられる。また、製品やメーカー宣言の情報が掲載された製品情報 Web ページが作成され、消費者に対してアピールすることができるようになる。この Web ページにはラベルに記されている QR コードから飛ぶことができる（図 4-22 参照）。申請書類の提出からラベルの付与までは、通常 6 週間かかる。ラベル付与後も、要件が満たされているかが BSI により確認される。もし申請内容に反していることが明らかになった場合、BSI は当該メーカーに対して監査を行うことがある。

出所）BSI ホームページ IT-Sicherheitskennzeichen

図 4-22 IT Security Label のイメージ図

[45] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211208_IT-SiK_Antragsverfahren-startet.html
[46] https://www.bsi.bund.de/SiteGlobals/Forms/IT-Sicherheitskennzeichen/IT-Sicherheitskennzeichen_Formular.html?nn=935184
[47] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03148/tr03148_node.html
[48] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03108/tr-03108.html
[49] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/fuer-Hersteller/IT-SiK-fuer-hersteller_node.html

7）シンガポール：Cybersecurity Labelling Scheme（CLS）

2020 年 10 月より、シンガポール CSA はサイバーセキュリティ要件を満足している消費者向け IoT 製品に対するラベリング制度である Cybersecurity Labelling Scheme（CLS）を開始した[50]。この制度では、消費者がより優れたサイバーセキュリティ対策を施された製品を特定し十分な情報を得たうえで意思決定することができるようになること、そしてメーカーが競合他社に差をつけ、より安全な製品を開発する動機付けに繋げることを目的としている[51]。2022 年 2 月時点でラベルの取得は任意であるが、消費者向け IoT 機器の必須要件となる時期について CSA が検討を行っている[52]。

ラベルは 4 段階に分かれ、レベル 1･2 はメーカーの自己宣言で取得できるが、レベル 3･4 では Singapore Common Criteria Scheme（SCCS）に基づき、CSA によって承認された検証ラボである Common Criteria Test Laboratory（CCTL）による検証が必要となる[53]。レベルが上がるにつれて、満たすべき ETSI EN 303 645 の規定の数が増えるほか、他の要件も追加されていく（図 4-23 参照）。

出所）CSA Cybersecurity Labelling Scheme（CLS）に関する公開情報に基づき三菱総合研究所作成

図 4-23 CLS において求められるサイバーセキュリティレベルの概要

レベル 1 では、ETSI EN 303 645 の 67 ある規定のうち 13 の規定（表 4-21 参照。）を満たす必要がある。レベル 1 では、デフォルトのパスワードのような一般的な弱点に基づく攻撃を防ぐために、「よくある間違い」を排除し、セキュリティアップデートの可用性を確保するとともに、脆弱性の報告を管理する手段を実装することが求められる。

表 4-21 CLS のレベル 1 において満たすべき ETSI EN 303 645 の 13 の規定

Provision	説明
5.1-1	パスワードが使用され、工場出荷時のデフォルト以外の状態にある場合、パスワードは機器ごとに一意であるか、ユーザーが定義すること。

[50] https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/updates
[51] https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls
[52] https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/faqs
[53] https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/for-manufacturers

Provision	説明
5.1-2	機器ごとに固有のプリインストールされたパスワードを使用する場合、機器のクラスやタイプに対して自動攻撃のリスクを低減するメカニズムでパスワードを生成すること。
5.1-3	ユーザーを認証するために機器に対して使用される認証メカニズムは、技術の特性やリスク、使用法に適したベストプラクティスの暗号技術を使用すること。
5.1-4	ユーザーが機器に対して認証を行うことができる場合、ユーザーまたは管理者に対して、使用される認証値を変更するための簡単なメカニズムを提供すること。
5.1-5	機器に制約がない場合、認証メカニズムへのネットワークインタフェースを介したブルートフォース攻撃を実行不可能とするメカニズムが利用できること。
5.2-1	脆弱性開示ポリシーを公開すること。このポリシーには少なくとも、問題を報告するための連絡先、受領の初期確認のタイムラインに関する情報、報告された問題の解決までの状況更新のタイムラインに関する情報を含める必要がある。
5.3-2	機器に制約がない場合、アップデートを安全にインストールするための更新メカニズムがあること。
5.3-3	アップデートの仕組みが実装されている場合、そのアップデートはユーザーが簡単に適用できるものであること。
5.3-7	アップデートの仕組みが実装されている場合、安全なアップデートメカニズムを促進するため、ベストプラクティスの暗号技術を使用すること。
5.3-8	アップデートの仕組みが実装されている場合、セキュリティのアップデートがタイムリーに行われること。
5.3-10	アップデートの仕組みが実装されていて、そのアップデートがネットワークインタフェースを介して配信される場合、機器は信頼関係のもと各アップデートの信頼性と完全性を検証すること。
5.3-13	ユーザーにとって明確で透明性の高いアクセス可能な方法で、定められたサポート期間を公表すること。
5.3-16	モデル名称は、機器へのラベリングもしくは物理インタフェースを介して明確に認識できるようにすること。

レベル 2 では、レベル 1 の要件に追加して、ETSI EN 303 645 の規定のうち、新たに 8 の規定（表 4-22 参照。）を満たす必要がある。また、シンガポール情報通信メディア開発庁（IMDA）が策定した IoT Cyber Security Guide[54]のライフサイクルセキュリティに関する 9 つの考慮事項（表 4-23 参照。）を満たす必要がある。

表 4-22 CLS のレベル 2 において追加で満たすべき ETSI EN 303 645 の 8 の規定

Provision	説明
5.5-8	機器に関連する重要なセキュリティパラメータの安全な管理プロセスに従うこと。

[54] https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf

Provision	説明
5.8-2	機器と関連サービス間で通信される機密性の高い個人データを、技術の特性や使用方法に適した暗号化によって保護すること。
5.8-3	機器のすべての外部センシング機能は、ユーザーにとって明確で透明性の高いアクセス可能な方法で文書化すること。
5.11-1	ユーザーがユーザーデータを機器から簡単に消去できるような機能を提供すること。
6.1	機器やサービスごとに、どのような個人データを処理するのか、そしてそれを誰がどのような目的でどのように使用するのかについて、明確で透明性の高い情報を消費者に提供すること。これは、広告主を含む関与する可能性のある第三者にも適用される。
6.2	消費者の同意にもとづいて個人データが処理される場合、この同意は妥当な方法で得ること。
6.3	個人データの処理に同意した消費者が、いつでもその同意を撤回することができること。
6.5	テレメトリデータが機器やサービスから収集される場合、どのようなテレメトリデータが収集されるのか、そしてそれを誰がどのような目的でどのように使用するのかについて、消費者に情報を提供すること。

表 4-23 ライフサイクルセキュリティに関する 9 つの考慮事項

ID	説明
CK-LP-01	機器に対する脅威を特定、分析、軽減するために脅威モデリングを実施していること。
CK-LP-02	安全なエンジニアリングアプローチを使用して機器を設計・開発すること。
CK-LP-03	未解決である既知の脆弱性がなく、安全なサプライチェーンからのコンポーネントで機器を実装・保守していること。
CK-LP-04	セキュリティ情報（利用規約、機能、ガイドライン、指示、通知等）を分かりやすい用語でタイムリーに提供、伝達、更新していること。
CK-LP-05	リリース前に機器が強化されていることを確認すること。
CK-LP-06	バージョン、適用されたパッチ、アップデートを含むコンポーネントのインベントリを維持していること。
CK-LP-07	ペネトレーションテストや脆弱性評価を定期的かつ各メジャーリリースの前に実施していること。
CK-LP-08	脆弱性を適切に開示・管理すること。
CK-LP-09	ID や証明書、機密がライフサイクル全体（作成、供給、更新、廃止等）で保護されていることを確認すること。

レベル 3 では、レベル 2 までの要件に追加して、ETSI EN 303 645 の規定のうち新たに 3 の規定（表 4-24 参照。）を満たす必要がある。またファームウェアと付属するモバイルアプリケーションは、CCTL が実施する自動バイナリ解析ツールによるソフトウェアバイナリ解析を受け、一般的なソフトウェ

アエラーや既知の脆弱性、マルウェアがないかを確認する必要がある。

表 4-24 CLS のレベル 3 において追加で満たすべき ETSI EN 303 645 の 3 の規定

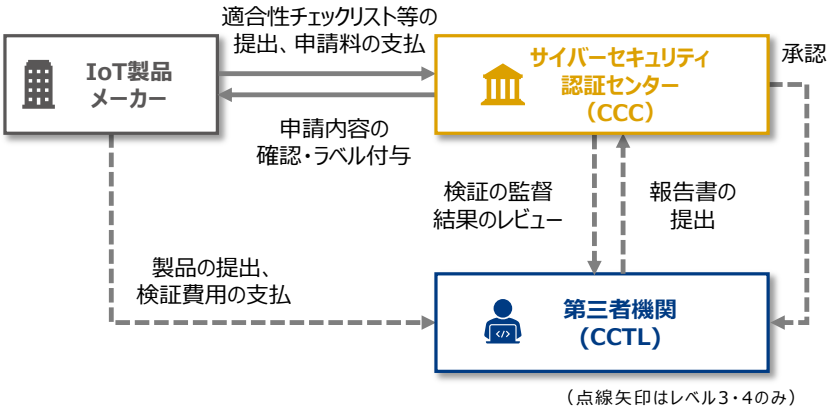
Provision	説明
5.4-1	機器ソフトウェアのソースコードにハードコードされた重要なセキュリティパラメータを使用しないこと。
5.4-4	ソフトウェアアップデートの完全性と信頼性のチェック及び機器ソフトウェアの関連サービスとの通信の保護に使用される重要なセキュリティパラメータは、機器ごとに一意であり、機器のクラスに対する自動攻撃のリスクを軽減するメカニズムで生成すること。
5.13-1	機器ソフトウェアにより、ユーザーインタフェースを介して入力されたデータ、アプリケーションプログラミングインタフェース（API）を介して転送されたデータ、サービスと機器のネットワーク間で転送されたデータが検証されること。

レベル 4 では、レベル 3 までの要件に追加して、ETSI EN 303 645 の規定のうち新たに 8 の規定を満たす必要がある。また、一般的なサイバーセキュリティ攻撃に対する基本的なレベルの耐性を提供するため、CCTL によるペネトレーションテストを受ける必要がある。このペネトレーションテストには、定められた最低限のテスト仕様に沿ったものと自由形式のものの 2 種類あり、その両方を受ける必要がある。

表 4-25 CLS のレベル 4 において追加で満たすべき ETSI EN 303 645 の 8 の規定

Provision	説明
5.4-1	永続ストレージ内の機密性の高いセキュリティパラメータは、機器によって安全に保存されること。
5.4-2	機器ごとに一意でハードコードされた ID がセキュリティ目的のために機器で使用される場合、物理的手段や電気的手段、ソフトウェア的な手段による改ざんに耐えられるように実装すること。
5.5-1	安全に通信するために、ベストプラクティスの暗号技術を使用すること。
5.5-5	ネットワークインタフェースを介してセキュリティに関連した設定変更を可能にする機器の機能は、認証後にのみアクセスできるようにすること。ただし、機器が依存するネットワークサービスプロトコルで、機器の動作に必要な設定をメーカーが保証できない場合は、例外とする。
5.5-7	リモートアクセス可能なネットワークインタフェースを介して通信される重要なセキュリティパラメータの機密性を保護すること。
5.6-1	未使用のネットワークや論理インタフェースはすべて無効にすること。
5.6-2	初期化された状態において、認証されていない場合、機器のネットワークインタフェースによるセキュリティ関連情報の開示は最小限にすること。
5.6-4	デバッグインタフェースが物理的にアクセス可能な場合、ソフトウェアで無効にすること。

ラベリングの審査にあたって、製品メーカーは適合性チェックリストとそれを裏付ける証拠を提出する必要があるが、レベル 2 以上では、それらに関してサイバーセキュリティ認証センター（CCC）による審査を受けなければならない。また申請受付やラベルの発行も CCC が行う。申請を行ってからラベルを取得するまでに、レベル 1・2 では最大 5 営業日、レベル 3・4 では 3 週間程度かかる。ラベルの有効期間は 3 年であり、審査費用はレベル 1 で$53、レベル 2 で$418、レベル 3 で$1,080、レベル 4 で$3,810 である（すべてシンガポールドル）。ただし、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。CSA は、市販されているラベル付き製品に対して無作為にサーベイランスを実施し、ラベル要件に適合されていないと判断される場合にはラベルが取り消されるとしている。なお、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、CSA は制度開始後 1 年間の 2021 年 10 月まで申請料を免除した。



出所）CSA Cybersecurity Labelling Scheme（CLS）に関する公開情報に基づき三菱総合研究所作成

図 4-24 CLS 制度のスキーム図

なお、SCCS で規定されている CCTL の一般要件は以下のとおりである[55]。

- コモンクライテリア（CC）に準拠した IT セキュリティ分野の試験所として、シンガポール認定評議会（SAC）や国際認定機関フォーラム（IAF）及び国際試験所認定協力機構（ILAC）の会員である他の認定機関により、ISO/IEC 17025 に従って認定されているか、認定中（ローカルラボの場合のみ適用）であること。
- （可能であれば ISO/IEC 27001 に準拠した）適切なセキュリティポリシーを有し、IT 製品の評価に関連する保護された情報を取り扱うためのセキュリティ要件を満たすことができること。情報セキュリティ管理の実施に関するガイダンスについて、ISO/IEC 27002 を参照することができること。
- 顧客のニーズを満たすような方法で評価活動を行うこと。
- 以下に対応できることを CSA に対して証明すること。
  - CC のパート 3 で定義された AVA_VAN.5 及び ALC_FLR.2 で補強された、評価保証レ

[55] https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/csa-common-criteria/publications

ベル 4 までの IT セキュリティ評価が実施できること。
  - CC 及び共通評価方法論（CEM）を正しく一貫して適用すること。
  - SCCS のポリシーと手順に従って運用すること。
- SCCS に基づく評価技術報告書を発行する前に、ISO/IEC 17025 の認定を受けること。

CCTL の設立を容易にするため、他の Common Criteria Recognition Arrangement（CCRA）スキームで承認された既存の CCTL は、シンガポール国外で運営される場合、いくつかの条件を満たせば、SCCS に基づくリモート CCTL としての承認を CSA に申請することができる。また、シンガポールの法律のもとで法的責任を負うことができるシンガポールの登録事業体であることが推奨されているほか、公平性や品質システム、スタッフ、環境条件、メソッド、セキュリティポリシー等に関する要件も存在する。

8）フィンランド：Finnish Cybersecurity Label

2019 年 11 月よりフィンランドの TRAFICOM は、セキュリティ要件を満足している消費者向け IoT 製品（ネットワーク接続する製品）に対してラベリングを行う制度である Finnish Cybersecurity Label を開始した[56]。本制度では、消費者がスマートデバイスやサービスを購入する際に安全に選択できること、そして IoT 機器等の開発メーカーが設計の責任を伝えられることを目的としている。2018 年末からパイロットプログラムを開始したほか、消費者に対するニーズ調査も実施した。ニーズ調査の結果、消費者の 3 人に 2 人が、購入する IoT 製品について、セキュリティ対策に関する情報が把握できることが非常に重要であると明らかになったとしている[57]。

本ラベルは、TRAFICOM の NCSC-FI（National Cyber Security Centre Finland）が設定した情報セキュリティ要件を満たす消費者向けスマートデバイスに付与され、スマート TV、スマート端末、家庭用ルータ等も含まれる。ラベル付与にあたっては、独立したセキュリティ企業による製品のセキュリティ機能の検証が必要となる。この検査では、NCSC-FI が定めたセキュリティ要件について確認され、これには具体的に以下の項目が含まれ、それぞれの項目は ETSI EN 303 645 の要件をベースとしている[58]。

- パスワード管理（ETSI EN 303 645, 5.1-1）
- 安全かつ最新のコンポーネントの使用（ETSI EN 303 645, 5.3-2, 5.3-3, 5.3-8, 5.3-11, 5.2-1, 5.2-3）
- プライバシー保護（ETSI EN 303 645, 6.1）
- データの安全な転送と保存（ETSI EN 303 645, 5.4-1, 5.5-1, 5.5-8）
- ネットワークサービスやエコシステムのインタフェースのセキュリティ（ETSI EN 303 645, 5.5-5, 5.6-1, 5.6-7, 5.13-1）
- 安全な初期設定（ETSI EN 303 645, 5.12-1）

[56] https://tietoturvamerkki.fi/en/
[57] TRAFICOM, Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label
[58] https://tietoturvamerkki.fi/en/requirements

検証結果はTRAFICOMにより確認され、承認された製品に対してラベルが付与される。ラベル取得後もTRAFICOMによる審査を毎年受ける必要がある。セキュリティ製品の検証機関として認定されるためには、フィンランドのLaki tietoturvallisuuden arviointilaitoksista（Act on Information Security Inspection Bodies）の法律[59]に基づきTRAFICOMによる認定を受ける必要がある。

ラベル取得企業は、毎年製品に関する変更情報を TRAFICOM に提出する必要があるほか、変更内容が重大と判断された場合には、新たに外部企業の検証を受ける必要がある。ラベル取得に要する費用は外部セキュリティ企業の検証費用によって変わるが、最低限、ラベル使用料 350EUR と年一回の審査費用 350EUR を支払う必要がある。検証に要する期間は 5～20 営業日であるとしている。

本ラベルを付与された製品は 2022 年 2 月時点で 10 製品である[60]。なお、本ラベリング制度とシンガポール CSA のラベリング制度は相互運用がなされており、フィンランドの制度でラベルが付与された製品はシンガポール CSA の制度でレベル 3 を満たしていると認められる。同様に、シンガポール CSA のラベリング制度でレベル 3 以上を取得している製品は、フィンランドのラベル制度を満たしていると認定される。

（3）諸外国政府機関における機器のセキュリティ対策のためのセキュリティ人材確保に関する取組

海外政府機関における機器のセキュリティ対策のためのセキュリティ人材確保に関する取組の概要を表 4-26 に示す。米国 NIST をはじめとして、諸外国では、セキュリティ人材に求められるスキルや人材の不足状況の可視化に関する取組が中心に進められているが、機器メーカーに対する直接的な人材支援策は講じられていない。

表 4-26 機器のセキュリティ対策のためのセキュリティ人材確保に関する海外政府機関による代表的な取組

主体	取組名称	概要	目的	時期
米国 NIST	“NICE Framework”の策定	サイバーセキュリティ業務に関する 52 種類の役割と、各役割に求められるタスクや知識・技能・能力の関係を明確化。	経営層のニーズに合致する人材の育成・強化を推進するとともに、サイバー安全国家を支援する能力を有した人材プールを備えること	2017 年 8 月
米国 NIST, CompTIA 等	Cyberseek プロジェクト	米国の各地域におけるセキュリティ人材の求人状況等の情報を、NICE Framework や民間団体が提供する資格と紐づけて視覚的に提供。	セキュリティ人材が求人を把握しやすくすること。また、求められるスキルやスキルについて把握しやすくすること。	2017 年 8 月運用開始

[59] https://www.finlex.fi/fi/laki/smur/2011/20111405
[60] https://tietoturvamerkki.fi/en/products/

主体	取組名称	概要	目的	時期
米国 DHS/ CISA	NICCS Education and Training Catalog	産学官における様々なサイバーセキュリティ教育プログラム・訓練プログラムのカタログを提供する。	米国政府や産業界、教育者、学生等が適切なセキュリティ教育プログラム・訓練プログラムを確認できるようにすること。	2015 年 11 月運用開始
米国 DHS/ CISA	Cybersecurity Talent Management System	DHS が求めるセキュリティ人材のポジション、各ポジションに求められる能力や資格を明確化した人材管理システム。	DHS においてサイバーセキュリティ専門家をより効果的に募集、採用、維持すること。	2021 年 11 月運用開始
英国 DCMS	“Cyber security skills in the UK labour market”の策定	英国サイバーセキュリティ市場で求められる求人の性質や、求められるスキル、人材の不足状況をまとめた文書。2018 年、2020 年、2021 年と定期的に整理されている。	サイバーセキュリティスキルに関するギャップ、人材の不足状況とその影響、人材が多く募集されている地域、セキュリティ人材に求められるスキル等を明確化すること。	2021 年 3 月
シンガポール CSA/IM DA	CSAT（Cyber Security Associates and Technologists）プログラム	パートナー企業と協力し、サイバーセキュリティの専門家によるセキュリティ人材のスキル育成を図る教育プログラム。	ICT 分野や工学分野など、セキュリティに隣接する分野の人材に対して、サイバーセキュリティに関する知識・スキルの醸成を図ること。	2016 年

以降では、各取組の概要について説明する。

1） 米国：“NICE Framework”の策定

2017 年 8 月、米国 NIST はセキュリティ業務の役割や専門分野、必要される知識・能力に関する共通言語や分類法を提供したフレームワークである NICE（National Initiative for Cybersecurity Education）を NIST SP 800-181 として発表した。2020 年 11 月には、Rev. 1 が公開され、用語の定義が改定されたほか、コンピテンシーが新たに追加された[61]。

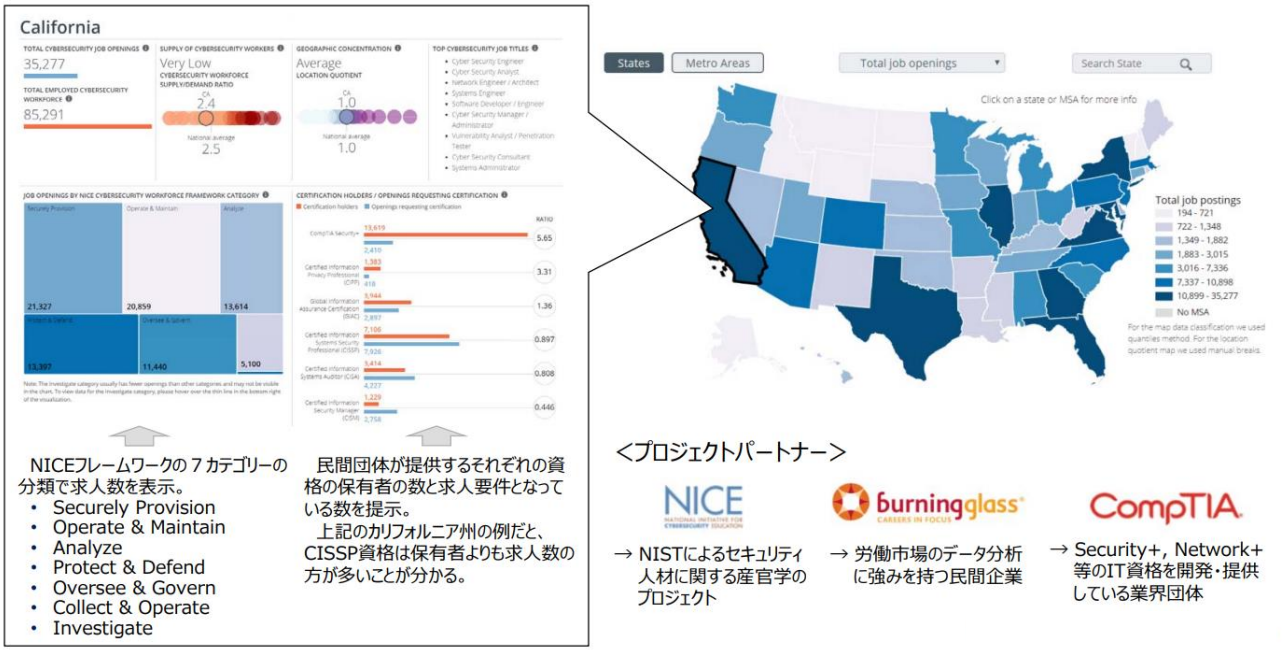
NICE フレームワークは、7 種類のカテゴリ（Category）、33 種類の専門分野（Specialty Area）、

[61] https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

52 種類の役割(Work Role)から構成され、各役割には達成される作業(Task)及び役割を果たすために必要な知識(Knowledge)、技能(Skill)、能力(Ability)が紐付けられている。作業の総数は1,007 項目、知識の総数は 630 項目、技能の総数は 374 項目、能力の総数は 176 項目であり、セキュリティ業務に関する役割や必要とされる知識・能力が詳細かつ網羅的に整理されている。

2）米国:Cyberseek プロジェクト

米国の Cyberseek は、NICE フレームワークに基づき米国各州の求人情報等を可視化したウェブサイトであり、NICE フレームワークを開発した NIST のほか、CompTIA 及び労働市場のデータ分析等を行う民間企業である burning glass により運用されている[62]。Cyberseek の概要を図 4-25 に示す。Cyberseek では、NICE フレームワークの 7 つのカテゴリの分類に基づき、各州における求人数が表示されるほか、各職種の平均報酬、需要の多い職種、民間団体が提供する資格の保有者数、主要スキル等が確認できる。



出所)経済産業省「第 3 回産業サイバーセキュリティ研究会 ワーキンググループ 2(経営・人材・国際) 事務局説明資料」[63]

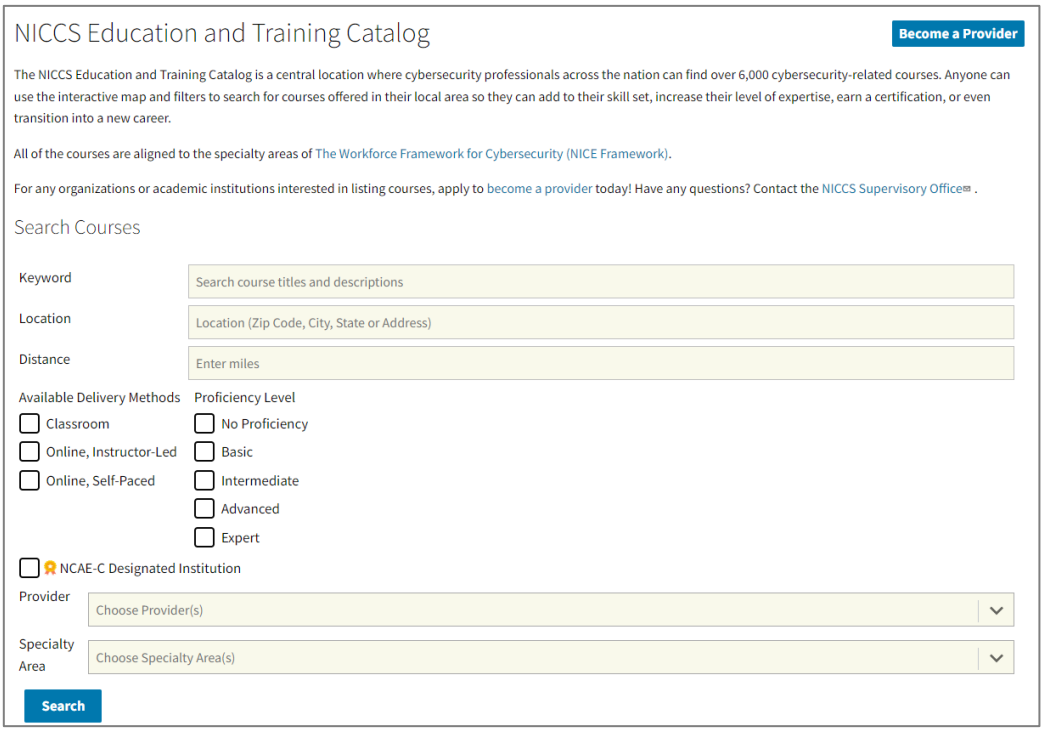
図 4-25 Cyberseek プロジェクトの概要

3）米国:NICCS Education and Training Catalog

米国 DHS/CISA は 2015 年 11 月より、産学官における様々なサイバーセキュリティ教育プログラム・訓練プログラムのカタログである NICCS Education and Training Catalog を運用している[64]。図 4-26 に示すとおり、このカタログを用いることで、米国全土での 6,000 件以上のサイバーセキュリティ関連教育プログラムを確認することができる。教育プログラムが提供されている場所を選択し、インタラクティブな地図を用いて教育プログラムの検索ができるほか、特定の専門領域に限定した検索

62 https://www.cyberseek.org/
63 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/003_03_00.pdf
64 https://niccs.cisa.gov/training/search

も可能である。なお、すべての教育プログラムが、NICE フレームワークの専門分野に紐付いているとしている。



出所）DHS/CISA, NICCS Education and Training Catalog[65]

図 4-26 NICCS Education and Training Catalog の検索画面

4）米国：Cybersecurity Talent Management System

2021 年 11 月より、DHS は、DHS が求めるセキュリティ人材のポジション、各ポジションに求められる能力や資格を明確化した人材管理システムである Cybersecurity Talent Management System（CTMS）の運用を開始した[66]。本システムは、実証を通じて明確化されたサイバーセキュリティ能力によって応募者をスクリーニングするとともに、従業員の競争力維持や採用にかかる時間を短縮することで、DHS におけるサイバーセキュリティ専門家をより効果的に募集、採用、維持することが可能であるとしている。求める技術力（Technical Capability）ごとに、ジョブディスクリプションや基礎技術が明確に定義されており、例えば、「脆弱性評価」の技術力については、以下のジョブディスクリプションが定義されている。

- ネットワーク、システムのソフトウェア及びハードウェアに対する脅威や脆弱性の評価を行い、適切な緩和策を開発・推奨する。
- システム又はその要素の技術的、機能的及び性能的特性を検証する。また、ポリシー、ベンチマーク、業界のベストプラクティスに従って、仕様や要件への準拠を評価するためのテストを開発し実施する。
- プログラムオフィスや様々なステークホルダーと調整し、連携する。

---

65 脚注 64 と同様。
66 https://dhscs.usajobs.gov/Home

また、求めるキャリアレベルも明確化され、それぞれのキャリアレベルにおける潜在的給与も公開されている[67]。

- エントリートラック（Entry Track）：
  サイバーセキュリティに関する新しいキャリアをスタートさせる専門家向けのトラック。潜在的年俸は$61,200～$91,080。
- 発達トラック（Developmental Track）：
  サイバーセキュリティの専門家で、ある程度の経験があるが、まだ技術的な専門知識を身につけていない方向けのトラック。潜在的年俸は$74,000～$110,000。
- テクニカルトラック（Technical Track）：
  成熟した技術的専門知識又は極めて稀なスキルを適用し、様々な役割に特化できる経験豊富なサイバーセキュリティの専門家に関するトラック。潜在的年俸は$94,400～$216,260。
- リーダーシップトラック（Leadership Track）：
  小規模なプロジェクトチームからプログラムや組織全体までの組織管理のために、成熟した技術的専門知識を適用可能な、経験豊富なサイバーセキュリティの専門家に関するトラック。潜在的年俸は$110,500～$211,300。
- エグゼクティブトラック（Executive Track）：
  大規模かつ複雑なサイバーセキュリティ組織やミッション機能全体を監督できる経験豊富なサイバーセキュリティリーダーに関するトラック。潜在的年俸は$157,300～$246,400。

5）英国：“Cyber security skills in the UK labour market”の策定

英国 DCMS は、英国サイバーセキュリティ市場で求められる求人の性質や、求められるスキル、人材の不足状況をまとめた文書の 2021 年版である“Cyber security skills in the UK labour market 2021”を 2021 年 3 月に公開した[68]。本文書はサイバーセキュリティスキルに関するギャップ、人材の不足状況とその影響、人材が多く募集されている地域、セキュリティ人材に求められるスキル等を明確化することを目的としており、2018 年、2020 年、2021 年と定期的に整理されている。

調査の結果、多くの英国企業においてサイバーセキュリティ管理に関する技術スキル、インシデント対応スキル、セキュリティガバナンススキルを有する人材が不足していることが明らかとなった。また、企業に対するインタビューにより、経営層と IT 部門の両方において、サイバーセキュリティのスキルが十分に理解されず、過小評価されていることが明らかとなった。文書では、サイバーセキュリティのリーダーに対し、組織内に行動変革を与えることができるスキルやサイバーセキュリティについてビジネスリスクの観点から議論できるスキルが求められることを示唆している。また、特に小規模な企業では、体系的なトレーニングプログラムの実施、実習生やその他の新入社員の受け入れ、既存のネットワーク以外を活用した採用が困難であるという構造的な障壁も抽出された。他方で、サイバーセキュリティの市場は活発かつ動的な労働市場であり、新型コロナウイルス感染症拡大の影響もあり、求人数の減少から回復しつつあることを示唆している。

[67] https://dhscs.usajobs.gov/Benefits
[68] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021

6）シンガポール：CSAT（Cyber Security Associates and Technologists）プログラム

シンガポールの CSA/IMDA は、パートナー企業と協力し、サイバーセキュリティの専門家によるセキュリティ人材のスキル育成を図る教育プログラムである CSAT（Cyber Security Associates and Technologists）プログラムを 2016 年から開始している[69]。このプログラムは、ICT 分野や工学分野など、セキュリティに隣接する分野の人材に対して、サイバーセキュリティに関する知識・スキルの醸成を図ることを目的とし、Associates Track と Technologists Track という 2 つのトラックにより構成される。前者は、3 年未満の実務経験のみ有する初級の ICT エンジニア向けに提供される 12 ヶ月間のプログラム、後者は 3 年以上の実務経験を有する ICT エンジニア向けに提供される 6 ヶ月間のプログラムである。

（4）IoT 機器等に対する民間認証機関による認証サービス

機器メーカーにおけるセキュリティ対策の取組を評価する観点では、民間認証機関による IoT 機器等に対する認証サービスを活用することも想定される。国内で既に展開されている IoT 機器等に対する主な認証サービスを表 4-27 に示す。

表 4-27 IoT 機器等に対する民間認証機関による認証サービス

認証名	概要	運営主体	認証対象
CCDS サーティフィケーションプログラム	一定のセキュリティ確保のための要件を満たした IoT 機器に対する認証サービス。認証は 3 段階のレベルに分かれ、レベル 1 は IoT 機器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。	重要生活機器連携セキュリティ協議会（CCDS）	IoT 機器全般
UL IoT セキュリティレーティングサービス	IoT 機器を対象としたセキュリティ評価サービスであり、製品を 5 段階（ブロンズ、シルバー、ゴールド、プラチナ、ダイアモンド）で評価・ラベリングする。評価は NIST や ETSI 等のガイドラインや標準に基づき行われ、認証後も継続的に評価が実施される。	UL（国内では UL Japan）	IoT 機器全般

[69] https://www.csa.gov.sg/Programmes/CSAT

認証名	概要	運営主体	認証対象
Kitemark for Internet of Things devices	IoT 機器向けのセキュリティ認証サービス。住環境用、商業用、政府やインフラ向けの高リスク環境用の IoT 機器を特に対象としている。認証には、ペネトレーションテストの実施が要件に含まれるほか、定期的なモニタリング・評価の継続が必要となる。	BSI（国内では認定ラボが創設されている）	住環境用、商業用、政府やインフラ向けの高リスク環境用の IoT 機器
Cybersecurity Certification	消費者向け IoT 機器を対象とした認証サービスで、求められる 5 段階のセキュリティレベルに基づき、評価が実施される。認証基準は 3 段階に分かれており、対象とする機器や用途に応じて適用される基準が異なる。	BUREAU VERITAS	消費者向け IoT 機器

以降では、各取組の概要について説明する。

1）CCDS：CCDS サーティフィケーションプログラム

CCDS は、一定のセキュリティ確保のための要件を満たした IoT 機器に対する認証サービスである CCDS サーティフィケーションプログラムを 2019 年 10 月より開始している[70]。認証は 3 段階のレベルに分かれ、レベル 1 は IoT 機器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。対象設備について、インターネットにつながる IoT 機器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 2021 年版：CCDS-GR01-2021Ver. 2.0」の要件に基づく[71]。本要件ガイドラインは ETSI EN 303 645、NISTIR 8259A、総務省「IoT 機器のセキュリティ基準に係る技術基準適合認定関連要件」、カリフォルニア州法「SB-327 Information privacy: connected devices」等を参考に策定されており、レベル 1 の要件は「IoT 機器の機能要件」、「IoT 機器特有のインタフェースにおける基準」、「管理者画面における具体的な対策基準」、「IoT 機器の運用における要件」の 4 分類・12 要件が設定されている。認証取得にあたっては、各要件に対するセキュリティ検証を実施する必要があるとともに、当該検証結果に関するヒアリングが実施される。

認証に要する費用について、申請手数料、登録管理料、CCDS サーティフィケーション証明書発行費用の 3 種類の費用を要する。まず、申請手数料について、CCDS の一般会員・非会員は 5 万円/件、幹事会員・正会員は 3 万円/件である。次に、登録管理料について、後述する IoT サイバー保険の付帯有無や製品の単体売価によって金額が変わるが、最低 40 万円（幹事会員・正会員の場合最低 20 万円）

[70] https://www.ccds.or.jp/certification/index.html
[71] https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021_v2.0_jpn.pdf

となる。そして、CCDS サーティフィケーション証明書発行費用は 1 万円である。現状、認証を取得した製品のうち、公開されている製品数は 7 製品である[72]。

本認証サービスの特徴として、IoT 機器に関する保険が付帯される点が挙げられる。三井住友海上火災保険株式会社、損害保険ジャパン株式会社、東京海上日動火災保険株式会社と連携し、認証が付与された製品に対して賠償損害や費用損害に対する保険が付与される。

2）UL：IoT セキュリティレーティングサービス

UL は、IoT 機器を対象としたセキュリティ検証プログラムである IoT セキュリティレーティングサービスを 2020 年 7 月より国内で開始している[73]。UL は本認証を取得することのメリットとして、消費者に対する安全性の提示、製品におけるセキュリティの確認、競合製品との差別化、規制等の市場トレンドへの対応の 4 点を挙げている。認証は、図 4-27 に示すとおり 5 段階のレベルに分かれ、下位レベルより順に Bronze、Silver、Gold、Platinum、Diamond と命名されている。各レベルに対応したラベルが用意されており、認証取得した製品は HP 等でラベルを掲載することが可能である。

出所）UL[74]

図 4-27 UL：IoT セキュリティレーティングサービスにおける 5 つのラベル

認証は、UL が独自で策定した「UL MCV 1376」の要件基準に基づく。本要件は、英国 DCMS “Code of Practice for Consumer IoT Security”、NISTIR 8259、ETSI EN 303 645 等の国際的なガイドライン・標準のほか、カリフォルニア州などの規制要件に対応しているとしており、Bronze（レベル 1）を取得すればカリフォルニア州法の要求基準に適合、Gold（レベル 3）を取得すれば ETSI EN 303 645 と同等のセキュリティレベルを確認できるとしている。具体的な要件は「ソフトウェア更新情報」、「データと暗号化」、「論理セキュリティ」、「システムマネジメント」、「顧客識別データ」、「プロトコル・セキュリティ」、「プロセス・ドキュメンテーション」の 7 つのカテゴリに基づき設定され、このカテゴリのうち、Bronze（レベル 1）の場合は 11 の要件、Silver（レベル 2）の場合は 19 の要件、Gold（レベル 3）の場合は 27 の要件、Platinum（レベル 4）の場合は 37 の要件、そして Diamond（レベル 5）の場合は 44 の要件に対応する必要がある。認証取得にあたって、まず UL からの質問票の回答に基づき初期評価及び取得すべきレベルを決定した後、UL に対象製品を送付し、UL によるセキュリティ評価

72 https://www.ccds.or.jp/certification/certification_devices-sevices.html
73 https://japan.ul.com/wp-content/uploads/sites/27/2020/07/10_inforsheet_IoTSecurity_Rating.pdf
74 脚注 73 と同様。

を受ける必要がある。その評価結果に基づき認証レベルが確定する。

認証に要する費用は公開されていない。UL の評価には 1～3 週間の期間を要する。なお、取得したラベルは 1 年間利用できるが、半年毎のサーベイランスに対応する必要がある。現状、グローバルでの認証を取得した製品として 6 製品が公開されている[75]が、国内製品の取得実績は無い。

3）BSI：Kitemark for Internet of Things devices

BSI は、IoT 機器のセキュリティ機能が試験されていることを証明する制度として、Kitemark for Internet of Things devices の認証・ラベリングサービスを 2018 年 5 月から提供している[76]。本サービスでは、住環境用、商業用、政府やインフラ向けの高リスク環境用の IoT 機器を特に対象としている。認証には、ペネトレーションテストの実施が要件に含まれるほか、定期的なモニタリング・評価の継続が必要となる。BSI は、本サービスを活用することで、製品ブランドの確立、プレミアム価格の設定、顧客基盤の拡大、顧客満足度の向上、競合他社との差別化に寄与するとしている。これまで説明した認証サービスとは異なり、レベル分けのされていない単一の認証・ラベリングの制度となっている。

認証要件の詳細は公表されていないが、ETSI EN 303 645 の基準に基づいた要件が設定されている。加えて、製品メーカーにおいて ISO 9001 などに基づく品質マネジメントシステムが構築されていることを明示する必要がある。認証取得にあたっては、BSI により製品に対する検証（ペネトレーションテスト）が実施されるほか、認証取得後も定期的なモニタリング・評価に対応する必要がある。

認証に要する費用は公開されておらず、具体的な認証プロセスも公開されていない。また、認証を取得した製品のリストは公開されていないが、複数の製品ベンダーのウェブサイトに当該ラベルを取得した内容が掲載[77,78,79]されており、複数の認証取得実績があることが確認できる。

4）BUREAU VERITAS：Cybersecurity Certification

BUREAU VERITAS では、消費者向け IoT 機器を対象としたセキュリティ認証サービスである Cybersecurity Certification を提供している[80]。本認証サービスは、比較可能なサイバーセキュリティのレベルを消費者に提供するとともに、セキュリティに関する規制やガイドラインに対応することを目的に開発された。認証基準は 3 つのレベルに分かれており、それぞれ、BV IoT Class 1、BV IoT Class 2、BV IoT Class 3 として定義されている。各レベルで対象となる製品やセキュリティレベルは以下のとおり明確に定義されている。

- Class 1：セキュリティを重視しない環境で動作する IoT 製品。対象がハッキングされた場合の影響が限定的、ローカルネットワークにのみ接続、そしてプライベートなデータは限定的又は皆無

---

[75] https://verify.ul.com/search?&dir=&q=IoT+security+Rating
[76] https://www.bsigroup.com/globalassets/localfiles/en-gb/internet-of-things/bsi_solutions.pdf
[77] Squire, The First Organisation To Achieve BSI Internet Of Things Kitemark For A Bike Lock https://www.squirelocks.co.uk/squire-is-the-first-organisation-to-achieve-bsi-internet-of-things-kitemark-for-a-bike-lock/
[78] Ring, Ring Devices Recognized with BSI Kitemark https://en-uk.ring.com/blogs/alwayshome/ring-devices-recognized-with-bsi-kitemark
[79] Xiaomi, Mesh System AX3000（2-Pack） https://www.mi.com/global/product/xiaomi-mesh-system-ax3000/
[80] https://www.cps.bureauveritas.com/needs/cybersecurity-certification-bureau-veritas-iot-cybersecurity-evaluation

の IoT 製品。例えば、スマート照明、ネットワーク接続型洗濯機、ウェアラブル端末、スマートスピーカー、環境計測センサー等。

- Class 2：最低限のセキュリティ対策が必要な IoT 製品で、サービスの停止や多額の金銭的な影響を受ける場合、深刻な影響を受ける可能性がある製品。対象がハッキングされた場合、個人情報や機密情報に深刻な影響を及ぼす可能性があり、インターネットへの間接的な接続がある製品。（無線 LAN ホームボックスへの接続など。）例えば、ネットワーク接続型の玩具、スマートホームアシスタンス、Web カメラ、ネットワーク接続型冷蔵庫等。
- Class 3：高いレベルでのセキュリティ保証が必要な IoT 製品で、ハッキングされた場合に深刻な経済的影響がある製品。インターネットに直接接続し、情報の不正な流出が重大な悪影響を及ぼすことが想定される製品。さらに、当該製品へのアクセスが中断された場合、サービス又はユーザーに重大な悪影響を及ぼすことが予想される製品。例えば、煙探知器などの安全関連製品、スマートロック、スマートメーター、ドローン等。

Class 1 では CTIA の Internet of Things (IoT) Cybersecurity Certification と同等のレベル、Class 2 では OWASP Top 10 に対抗可能なレベル、Class 3 では ETSI EN 303 645 と同等のレベルの要件が求められる。認証取得にあたっては、BUREAU VERITAS による脆弱性検証を受ける必要があるほか、Class 2 以降では、設計文書を使用したグレーボックステストが実施される。なお、認証取得後も定期的なモニタリング・評価に対応する必要がある。

認証に要する費用は公開されていない。評価に要する期間について、Class 1 では 5 日間、Class 2 では 10 日間、Class 3 では 15 日間を要するとしている。なお、認証を取得した製品のリストは公開されておらず、調査の範囲では、本認証を取得した製品の情報は公開されていない。

4.3.3 有識者検討会における議論結果

機器のサイバーセキュリティ確保のために求められる取組について有識者検討会で議論を行った。有識者検討会では、まず、第 4.3.1 項で示した機器メーカーにおけるセキュリティ対策の状況を示しつつ、機器メーカーにおける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製品が積極的に導入されるような仕組み構築の必要性を示した。そのうえで、この仕組みの一候補として、諸外国の取組を参考に、我が国における IoT 製品等に対するセキュリティラベリング制度の必要性を提示した。製品のラベリング制度に関して、有識者検討会では以下の意見が挙げられた。

【製品に対するセキュリティラベリング制度の基準について】

- ラベリング制度そのものについては賛成である。
- 個人情報を扱わない製品で家庭用のものは自己点検、業務用のものは詳細な自己点検を求め、医療や金融といった高度な信頼性が必要な分野は外部検証を必須とすれば良いのではないか。さらに、防衛分野に関しては高度な外部検証を必須とすれば良いだろう。これくらいのレベル感であれば、メーカーの費用負担としても適切だと考えられる。
- ラベリングや認証を行うのであれば、何に準拠すべきかについて示す必要がある。
- 消費者向け IoT のベースラインとなるセキュリティ要件が規定されている ETSI EN 303 645

には、網羅的にセキュリティ評価をするための基準が記載されていて使いやすい。国際的な基準をどのように捉えていくのかについては整理していく必要がある。

【ラベリング制度の構築に向け検討すべき論点について】

- ある時点で適切に検証されたものだということを明確にしておく必要があると考えている。ラベリングを行うのであれば、検証事業者が検証を適切に行っているかについて確認する仕組みについても検討する必要があると考えている。昨年度策定した手引きに基づく対応が適切に行われているのかについてチェックすることも大切だろう。
- ラベル取得後にセキュリティ課題が発覚することは避けられない。そのような事態に対応できる仕組みを備えておくことは重要であるが、実際に対応を行っているかはメーカー次第でもある。こういった課題の解決策についても検討する必要がある。
- ファームウェアの扱いについては、適切に規定していく必要がある。

【ラベリング制度の活用促進に向けた論点について】

- ラベル取得に対する補助があれば、機器メーカーにとってはありがたいと思われる。また、検証の取り組みを拡大していくという観点から、認証を受けた製品が選ばれ、売上向上やビジネスチャンス拡大に繋がるといったようなインセンティブが求められると考えている。例えば、政府や地方公共団体における機器の調達要件にする、補助金の対象機器とするといった施策が考えられる。

まず、国内でラベリング制度を構築する方針について、有識者より賛成の意見が多数挙げられた。制度を構築するうえでは基準を明確にすべきとの意見が挙げられ、具体的な基準として、シンガポールやフィンランドの制度でも活用されている ETSI EN 303 645 が参考になるとの意見があった。また、既に諸外国でラベリング制度が開始しているところ、国際協調も踏まえて検討できると良いとの意見がなされた。加えて、製品のユースケースを踏まえて 4 段階のラベルを設定する方針が意見された。具体的には、個人情報を扱わない家庭用 IoT 製品、一般業務用 IoT 製品、医療・金融等で活用される高度な信頼性が必要な IoT 製品、そして防衛分野の IoT 製品である。有識者検討会では、個人情報を扱わない家庭用 IoT 製品は自己評価でラベル付与可能、一般業務用 IoT 製品は詳細な自己評価でラベル付与可能、医療・金融等で活用される高度な信頼性が必要な IoT 製品は外部検証を踏まえてラベル付与、そして防衛分野の IoT 製品は高度な外部検証を踏まえてラベル付与の方向性が提示された。今後、ラベリング制度を構築するとしたとき、対象となる製品分野、各製品分野で求められるセキュリティレベル、そのレベルを確認するための基準を明確化する必要がある。

ラベリング制度の構築に向けて検討すべき論点について、制度では、ある時点で適切に検証された製品であることを明確化する必要があるため、外部検証によりラベルが付与された製品については、適切な検証がなされているかを確認する仕組みが必要であるとの意見がなされた。シンガポールのラベリング制度では、外部検証が必要なレベル 3・レベル 4 のラベル付与において、CSA が外部検証事業者の検証結果報告書をレビューする仕組みとなっている。この仕組みのように、ラベルを付与する主体が外部検証事業者の結果を適切に評価できる仕組みが必要となる。また、ある時点での製品のセキュリティ対策に関してラベルが付与されるが、ラベル付与後にセキュリティ課題が発覚した際の対応についても

検討する必要がある。例えば、シンガポールのラベリング制度では、レベル 2 以上のラベルを取得する際、販売後の脆弱性対応を含めた製品のライフサイクルにおけるセキュリティ対策要件に準拠する必要がある。ラベル取得後に製品にセキュリティ課題が検出されることは十分想定されるところ、自己宣言であっても機器メーカーの販売後の対応も確認できる要件を含めることが望まれる。この課題に関連して、ファームウェアの扱いに関しても適切に検討すべきとの意見が有識者検討会にて挙げられた。

仮にラベリング制度が構築された際、その制度の活用促進が不可欠となる。制度の活用促進に向けた取組に関して、検討会では、ラベル取得に対する補助のほか、ラベル取得によるインセンティブを明確にすべきとの意見が得られた。具体的なインセンティブとして、ラベル取得により政府や地方公共団体の調達要件の対象となるという案のほか、補助金の対象に含める案も意見された。

有識者検討会では、機器メーカーが抱える人材不足の課題を解決しうるセキュリティ人材支援施策の方向性について意見を頂戴した。機器メーカーにおけるセキュリティ人材育成に関して有識者検討会で挙げられた意見は以下のとおりである。

【IoT 機器のセキュリティに関するラボやコミュニティに関して】

- 人材が不足している中で、信頼できる仲間と脆弱性情報といった機微な情報の交換ができるコミュニティ形成を推進していく必要がある。機器に対する検証、分析、解析等ができる環境も含めた場づくりが求められる。
- 人材育成を行ううえでは、知識（座学や動画で学べる教材）、環境（アクセスすれば誰でも自由に攻撃ができるラボや、アップデート系やハードコーディング回避などの基本的な実装方法を経験できる場）、経験（攻撃手法と対策方法）が必要である。知識の形成を促進するほか、攻撃手法やベストプラクティスのような基本的な事項を学べる環境で経験をつけていただくことが重要である。
- IPA の ICSCoE の中核人材育成プログラムのような若い世代の人材育成を高等教育でも実施していく必要があると感じた。IoT の分野に関する専門教育はまだ存在しない。テストラボの共有やコミュニティの場の形成を中心に推進していくのは一案だと思われる。
- IoT の検証センターは 7，8 年前から沖縄県で既に運用されているが、こういった検証センターは国内に複数個所あっても良いと考えている。
- 拠点の構築にあたっては、地方公共団体の予算だけで賄うことは困難であり、経済産業省も含めて、そのような拠点づくりについて検討することが望まれる。

【IoT 機器のセキュリティに関するスキルの可視化に関して】

- スキルを表すことは重要だと考えている。JNSA の SecBoK では、脆弱性診断士に求められるスキルが可視化されている。IoT 機器の検証については未対応であるが、今後連携できれば良いと考えている。
- 情報処理安全確保支援士のカリキュラムに制御系の要素をもう少し含めると良いのではないか。

IoT 機器のセキュリティに関する人材育成を行ううえで、知識・環境・経験の 3 つが重要であるとの意見が挙げられた。有識者検討会では、特に環境を重視する意見が多く得られた。特に、検討会では、機器に対する検証、分析、解析等が実施できる検証ラボを望む意見が多数挙げられた。国内では、CCDS が主導して構築された「沖縄県 IoT 推進ラボ」が沖縄県にて運用されているが、国内に複数設けることが望まれ、このような拠点が設立されることで、コミュニティの醸成にも寄与するとの意見が挙げられた。

有識者検討会では、IoT 機器のセキュリティに関するスキルの可視化の必要性も意見された。JNSA の SecBoK において、IoT 機器の検証やセキュリティに関するスキルを含める方向性が意見されたほか、情報処理安全確保支援士のカリキュラムに制御系セキュリティに関する要素を含める方向性も意見された。

4.3.4 機器のサイバーセキュリティ確保のために求められる取組の案

国内機器メーカーにおけるセキュリティ対策状況や機器メーカーが抱えている課題を解決しうる取組の案について、国内外における機器のセキュリティ確保・向上に係る代表的な取組や有識者検討会での議論を踏まえて検討を行った。

（1） IoT 製品に対するセキュリティラベリング制度の構築

セキュリティ対策に要するコスト負担は製品の販売価格に反映されるところ、機器のサイバーセキュリティ確保のために求められる取組として、機器メーカーにおけるセキュリティ対策の取組を適切に評価するとともに、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製品が積極的に導入されるような社会の仕組みを構築することが望まれる。このような仕組みの一候補として、我が国においても IoT 製品に対するラベリング制度を構築することが望まれる。有識者検討会での意見を踏まえ、ラベリング制度の検討にあたっては、以下に示すような論点について議論・検討する必要がある。

表 4-28 ラベリング制度構築に向けた論点

カテゴリ	論点
ラベリング制度の対象	• どのような IoT 製品をラベル付与の対象とするか。
ラベル付与の方法	• ラベルは、シンガポールの事例のように段階的なラベルとするか、フィンランドの事例のように単一のラベルとするか。 • どのような基準に基づいてラベルを付与可能とするか。 • どのような方法に基づいてラベル付与の評価を行うか。（自己宣言を可能とするか、第三者による評価を必要とするか 等）

カテゴリ	論点
ラベリング制度の運用方法	• ラベル制度の運営主体は誰が担うか。 • ラベル取得による追加のインセンティブを付加するか。（例：政府調達の対象となる、補助金の対象となる 等） • ラベルの審査費用はどの程度に設定するか。 • ラベル付与にあたってどのようなマークを用意することが必要か。 • ラベル付与にあたって第三者の検証を必要とする場合、検証機関をどのように認定するか。 • ラベルの期限は設定するか。設定する場合、どの程度の期限とするか。 • ラベル付与した製品において、付与後にセキュリティの懸念が検出された場合にどのように扱うか。
その他	• 海外のラベリング制度と、どのように相互運用すべきか。 • ラベリング制度が構築された後、いかに制度のプロモーションや活用訴求を行うか。

まず、ラベリング制度の対象製品について明確化する必要がある。有識者検討会においては、家庭用の製品のほか、業務用 IoT 製品、医療や金融系などの高度な信頼性が求められる製品、そして防衛分野の製品も対象となり、それぞれ求められるレベルが異なるとの意見が挙げられた。検討会においては具体的な産業分野が意見されたが、すでにラベリング制度が開始しているシンガポールやフィンランドの制度では、家庭用ルータやスマート家電等の消費者向け IoT 製品のみが対象となっている。ラベリング制度を検討するうえでは、対象となる製品や産業分野によって求められる基準が異なるため、まず対象製品分野を明確化する必要がある。高信頼性が求められる製品を対象とする場合、次項で示すセキュリティ・アシュアランスの観点も重要となる。

ラベルの対象分野を明確化した後、具体的なラベリング方法の検討が必要である。この検討においては、具体的なラベルの種類、ラベル付与の基準、当該基準に満足していることの確認方法を明確化する必要がある。まず、ラベルの種類について、シンガポールの制度のような段階的なラベルか、フィンランドの制度のような単一のラベルかの大きく分けて二択が存在する。段階的なラベルを設定した場合、複数の基準を設定することが可能となり、幅広い製品を対象とすることができる反面で、それぞれのレベルに対して基準や確認方法を決定する必要があるため管理コストが増加するという懸念も想定される。それぞれ一長一短であるため、どちらのラベル方式とするかは先述したラベルの対象範囲も踏まえて検討する必要がある。なお、前述のとおり米国 NIST は単一のラベルを推奨しており、この理由として、特定のベースライン基準に基づく適合性評価をもってラベルを付与すべきであるからとしている。

ラベル付与の基準について、有識者検討会でも意見されたとおり、国際的な基準を採用することが望まれる。既存のシンガポールやフィンランドの制度や米国で検討中の制度を参考にすると、ETSI EN 303 645 や NISTIR 8259 に基づく基準とすることが妥当であると考えられる。ETSI EN 303 645 では IoT 機器自体に求められるセキュリティ要件が中心に規定されているが、製品ベンダー自身におけるセキュリティ対策の取組を評価することも重要である。シンガポールのレベル 2 以降のラベルで求められるライフサイクル要件のように、ETSI EN 303 645 の基準に加え、別途ガイドラインに基づく要件を追加することも想定される。どのような基準を設定するかは、対象となる製品の範囲及び具体的なラベ

ルの種類によって変わってくることに留意が必要である。当該基準に満足していることの確認方法についても、対象となる製品の範囲や具体的なラベリングの種類を踏まえて検討する必要がある。

ラベリング制度の運営主体について、諸外国の制度では、CSA や TRAFICOM 等の政府機関が担っているところ、国内で制度を構築する場合も経済産業省や IPA 等の政府機関が担うことが現実的である。しかしながら、政府機関がラベルを付与した場合、ラベルを取得した製品が政府機関のお墨付きであると誤解を招く可能性があるため、ラベルの位置づけについては適切に周知する必要がある。

ラベリング制度の構築にあたっては、ラベル付与による製品及び製品メーカーのインセンティブを明確にする必要がある。既存のシンガポールやフィンランドの制度では、ラベル取得によるインセンティブとして、セキュリティ対策の明確化による競合他社製品との差別化を挙げているが、このインセンティブに加えて、有識者検討会でも意見されたとおり、政府や地方公共団体における機器の調達要件にする、補助金の対象機器とする等、より具体的なインセンティブの設計も考えられる。また、機器メーカーにおけるセキュリティ対策の取組を適切に評価する仕組みとし、ラベルを取得したメーカーに対してインセンティブを与える仕組みとするためには、ラベル取得に要する費用が機器メーカーに対して負担とならないことが必須である。そして、既存のラベリング制度と同様に、ラベルを取得したことが製品ホームページやパッケージで確認できるよう、ラベルに関するマークも設計する必要がある。

ラベル付与にあたって第三者の検証を必要とする場合、検証機関を別途認定する必要がある。シンガポールの制度では、シンガポール版の CC である SCCS のスキームに基づき認定された検証機関により検証が実施されるが、どのような基準や要件に基づき検証機関を認定するかは別途検討する必要がある。第 4.2 節で検討した仕組み（審査登録制度）は、技術要件と品質管理要件に関する最低限の要件を満足した検証事業者を登録する仕組みであるところ、CC で求められる高いレベルの検証事業者を認定する仕組みではない。他方、第 4.2 節で検討した仕組みを一部活用してラベリング制度における検証機関も認定することができれば、検証事業の活性化にも寄与すると考えられる。

ラベリング制度の設計にあたっては、ラベルの期限をどの程度に設定するか、という点も論点となる。シンガポールの制度では 3 年間が設定されている一方で、フィンランドの制度では毎年更新審査を受ける必要がある。有効期限の設定にあたっては、対象となる製品のライフサイクルや管理コスト等も勘案する必要があるが、これらに加え、検討会でも意見されたとおり、ラベルが付与された製品においてセキュリティの懸念が検出された場合の扱いについても検討する必要がある。

「その他」のカテゴリの論点として、ラベリング制度の設計にあたっては国際協調も重要となる。すでに運用されているラベリング制度が海外に存在するため、可能な限り相互運用できる制度とすることが望ましい。また、制度が構築された際には、制度を普及させるための適切なプロモーションを講じるとともに、ラベリング制度の活用促進に向けた訴求を行うことが不可欠である。シンガポールでは、制度の黎明期において取得製品数を増やすために、制度開始後一年間はラベルの申請料を無料に設定した。このように、ラベル取得にあたって金銭的支援を行うことも、制度を活用促進するうえで重要な取組である。

最後に、表 4-28 で示したラベリング制度構築に向けた論点について、米国で検討中のラベリング制度及びシンガポール・フィンランドで既に運用されているラベリング制度の取組状況を対応付けた表を表 4-29 に示す。ラベリング制度においては国際協調も重要な観点であるところ、海外の制度動向も踏まえつつ、国内の製品メーカーにおける状況や利用者のニーズを加味した検討を行うことが求められる。

表 4-29 各国ラベリング制度の比較

カテゴリ	論点	米国(検討中)	シンガポール	フィンランド
ラベリング制度の対象	どのようなIoT製品をラベル付与の対象とするか。	消費者向け IoT 製品	消費者向け IoT 製品	消費者向け IoT 製品
ラベル付与の方法	ラベルは、シンガポールの事例のように段階的なラベルとするか、フィンランドの事例のように単一のラベルとするか。	単一ラベルを推奨	段階的なラベル (4 段階)	単一ラベル
	どのような基準に基づいてラベルを付与可能とするか。	NISTIR 8259 に基づくベースライン基準が推奨されている	ETSI EN 303 645 に基づく基準＋IMDA ガイドラインに基づく基準	ETSI EN 303 645 に基づく基準
	どのような方法に基づいてラベル付与の評価を行うか。	現状未定だが、自己宣言、第三者試験・検査、第三者認証のいずれかで適合性を評価できるとしている	レベル 1・2:自己宣言のみ レベル 3・4:自己宣言＋外部事業者による検証	自己宣言＋ 外部事業者による検証
ラベリング制度の運用方法	ラベル制度の運営主体は誰が担うか。	現状未定だが、公共機関又は民間組織が担うことができるとしている	CSA	TRAFICOM
	ラベル取得による追加のインセンティブを付加するか。	現状追加のインセンティブは検討されていない	現状特別なインセンティブはない	現状特別なインセンティブはない
	ラベルの審査費用はどの程度に設定するか。	現状未定	レベル 1:$53 レベル 2:$418 レベル 3:$1,080＋検証費用 レベル 4:$3,810＋検証費用 (いずれもシンガポールドル)	700 EUR＋検証費用

カテゴリ	論点	米国（検討中）	シンガポール	フィンランド
	ラベル付与にあたってどのようなマークを用意することが必要か。	現状未定であり、消費者テストを通じて評価する必要があると言及されている。 なお、マークに加えて、URL や QR コードをラベルに記載することを推奨している。	下記ラベルの付与が可能 （レベル毎に＊マークの個数が異なる） 	下記ラベルの付与が可能 
	ラベル付与にあたって第三者の検証を必要とする場合、検証機関をどのように認定するか。	現状未定	Singapore Common Criteria Scheme（SCCS）に基づき CSA が認定	フィンランドの法律に基づき、TRAFICOM が認定
	ラベルの期限は設定するか。設定する場合、どの程度の期限とするか。	現状未定	ラベルの有効期限は 3 年	ラベルの有効期限は明示されていないが、毎年更新審査を受ける必要がある
	ラベル付与した製品において、付与後にセキュリティの懸念が検出された場合にどのように扱うか。	現状未定だが、消費者に対して提供が推奨される情報として、新たなサイバーセキュリティ脅威や脆弱性による影響を含めることを推奨している	CSA による無作為のサーベイランスが実施され、ラベル要件に適していないと判断された場合には取り消しがなされる	詳細は不明だが、毎年の更新審査で担保していると想定される
その他	海外のラベリング制度と、どのように相互運用すべきか。	現状未定だが、NIST は、他の制度との相互運用を検討することを推奨している	シンガポールのラベリング制度とフィンランドのラベリング制度にて相互運用がなされている （シンガポールの制度におけるレベル 3 のラベルが、フィンランドの制度におけるラベル付与に対応）	

カテゴリ	論点	米国（検討中）	シンガポール	フィンランド
	ラベリング制度が構築された後、いかに制度のプロモーションや活用訴求を行うか。	現状未定だが、適切な消費者教育キャンペーンの開発・実施の必要性が言及されている	ラベル取得製品数を増やす目的で最初 1 年間の申請料は無料としたほか、海外の会議等でも積極的にラベリング制度のプロモーションを行った	制度開始前のパイロットプログラムに協力したメーカーを巻き込んだプロモーションを実施

（2）IoT 機器のセキュリティに関するスキル・知識の可視化

国内機器メーカーが抱える人材不足の課題を解決しうるセキュリティ人材支援施策について、本項に示すスキル・知識の可視化のほか、次項に示すような機器に対して検証、分析、解析等が実施できる検証ラボの構築が効果的であると考えられる。有識者検討会で意見されたとおり、機器のサイバーセキュリティ確保のために求められる取組として、IoT 機器のセキュリティに関するスキルを可視化することは重要であり、諸外国においてもスキルの可視化は精力的に検討されている。セキュリティのスキル・知識の可視化に関する国内の代表的な取組としては、JNSA の SecBoK（Security Body of Knowledge）が挙げられる[81]。SecBoK は、セキュリティ関連業務に従事する人材に求められる 1,000 を超える知識項目の集合であり、想定されるセキュリティ関連業務の分類が提示されているほか、それぞれのロール（役割）において要求される／会得しているべき知識項目との対応関係が提示されている。また、グローバル標準との連携として、NIST の NICE フレームワーク（4.3.2（3）1）参照）との対応関係も整理されている。2021 年に改訂された SecBoK 2021 では知識分野カテゴリが改訂されたほか、ジョブディスクリプションに基づくジョブ型採用の際に活用できる具体の職種例が提示されている。

現状の SecBoK では、IoT 機器のセキュリティに関する知識項目は複数設定されているものの、知識項目分野やロール（役割）として明確に IoT 機器のセキュリティが位置づけられているわけではない。セキュリティ人材不足を課題に感じる機器メーカーに対し、セキュアな機器の開発に向けてどのようなスキル・知識を持った人材が必要であるかを明確化するために、IoT 機器のセキュリティに関する知識項目分野やロール（役割）を追加するよう JNSA に働きかけることも重要であると考えられる。

（3）機器に対する検証、分析、解析等が実施できる検証ラボの構築

有識者検討会において意見されたとおり、IoT 機器のセキュリティに関する人材の育成を行うためには、セキュリティ人材に求められる知識を可視化するだけではなく、その知識を獲得できる環境を整備することが求められる。具体的には、機器に対する検証、分析、解析等ができる検証ラボの構築に関する意見が有識者検討会では多数挙げられた。国内では、ネットワンシステムズ株式会社により運用されている愛知県の「ネットワン IoT 豊田ラボ」[82]、一般社団法人 IIoT によって沖縄県で運用されている検証ラボ[83]等、民間企業によっていくつかの検証ラボが運用されている。ネットワン IoT 豊田ラボは 2016 年に設立された工場向け IoT 機器の動作検証を無償で行うことができる検証ラボであり、ラボでは、工場向けイーサネットに対応したネットワーク環境が構築されているほか、負荷試験装置、無線 LAN、サーバ仮想化基盤も活用することができる。一般社団法人 IIoT は沖縄県の補助事業者としては 2012 年に設立され、IIoT 会員企業に対して検証機材、検証ツール、ナレッジデータベース、検証環境を沖縄県うるま市沖縄 IT 津梁パークの施設にて提供している[84]。本施設内に「IIoT ラボ」と呼ばれる共有スペースを構築し、IIoT 会員企業はその場で検証機器・ツールを活用するほか、自社に持ち帰り使用することも可能である。自社では整備が困難な IIoT の機材やツールを活用することで、短期間・低コスト・高品質な検証を行うことができるとしている。検証機材としては、Android 端末や iOS 端末等のモバイル端

[81] https://www.jnsa.org/result/skillmap/
[82] https://www.netone.co.jp/knowledge-center/files/6.pdf
[83] https://www.iiot.or.jp/
[84] 高橋 宏輔、IoT 時代の検証エコシステム：一般社団法人 IIoT https://www.ipa.go.jp/files/000065986.pdf

末のほか、スマート家電、自動車関連機器等が用意され、検証ツールとしては、テスト自動化ツールや車載器脆弱性診断ツール、Android 端末ログ解析ツール等が用意されている。このラボ設立の効果として、設立後 2 年間(2014 年 3 月末時点)で 7 億 8,000 万円の売上を産み出し、沖縄県内で 215 人の雇用を創出したとしている。当該検証ラボを活用できる企業は IIoT 会員企業に限られるが、IIoT の会員になるためには、最低年間 20 万円＋入会金 10 万円(会員区分:B 会員の場合)が必要となる[85]。

関連する公的機関における取組として、国内では東京都立産業技術研究センターにより試験装置の共用公開がなされており、ハードウェア解析に活用できる電気測定機器(オシロスコープ、スペクトルアナライザ等)を共用利用することができる。シンガポールでは、シンガポール国立研究財団(National Research Foundation of Singapore)の支援を受けたシンガポール国立大学(NUS)により、National Cybersecurity R&D Laboratory が運用されている[86]。このラボでは、共用利用可能なクラウドコンピューティングサービス(ノード数約 200)が提供され、Heartbleed や ImageTragick 等の既知の脆弱性を含んだネットワーク環境、スマートグリッドを模倣した仮想環境、病院システムを模倣した仮想環境などが提供されている。ホワイトハッカーが既知の脆弱性を含んだネットワーク環境を利用することで、ペネトレーションテストの能力を確認できるほか、病院システムを模倣した仮想環境を活用することで、セキュリティの評価を実施できるとしている。1 時間・1 ノードあたりの料金設定となっており、事前予約なしの場合は 1 時間・1 ノードあたり 0.12 シンガポールドル(約 10 円)、事前予約ありの場合は半額の 0.06 シンガポールドル(約 5 円)で利用できる。

このような検証に関連するラボを構築することで、セキュリティ人材がいない機器メーカーにおいても一定の品質を満たした検証を低コストで行うことができると考えられる。有識者検討会では、検証ラボを国内複数箇所に構築することを望む意見が挙げられた。国内複数箇所に構築することで、その土地の産業に特化した効果的なラボを設計することができるほか、一般社団法人 IIoT の実績のとおり、その土地の雇用創出にも寄与すると考えられる。他方、調査した範囲では、諸外国においても IoT 機器の検証に特化した政府により運用される共用利用可能な検証ラボは存在しない。国内において IoT 機器の検証に特化した検証ラボを構築するとしたとき、必ずしも政府が直接的に検証ラボを構築・運用するのではなく、間接的な支援も想定される。具体的には、上述したような既存の検証ラボの支援を行うほか、民間企業に対して検証ラボの構築を支援し、民間企業が運用者となるスキームも想定される。国内において IoT 機器の検証に特化した検証ラボを構築し、政府として支援するとした場合、当該ラボの意義・目的・目標・対象範囲について明確化したうえで、政府としての支援範囲を検討することが望まれる。

4.3.5 機器におけるセキュリティ・アシュアランスの観点

前述のとおり、ラベリング制度の構築にあたって特に重要となる論点が「どのような製品をラベル付与の対象とするか」という点である。逆説的に言えば、どのような製品にとって、ラベルが付与されることのメリットが存在するかを考える必要がある。ラベリング制度では、第三者的にセキュリティ対策に関する取組が評価されるところ、適切なセキュリティ対策が施されていることを明確化するだけではなく、製品のセキュリティ・アシュアランスの確保が期待される。ここで、製品のセキュリティ・アシュアランスとは、求

[85] https://www.iiot.or.jp/wp-content/uploads/2015/05/%EF%BC%A9%EF%BC%A9%EF%BC%AF%EF%BC%B4%E5%85%A5%E4%BC%9A%E3%81%AE%E3%81%94%E6%A1%88%E5%86%85.pdf
[86] https://ncl.sg/

められるセキュリティ基準を明確化したうえで、検証結果などの客観的なエビデンスに基づきセキュリティ対策の取組を説明することである。製品に対してラベルが付与されることにより、製品のセキュリティ・アシュアランス確保につながることを踏まえると、セキュリティ・アシュアランスの観点が、ラベリング制度の対象を検討するうえで参考になると考えられる。

以降では、セキュリティ・アシュアランスの確保が望まれる機器の観点について分析するとともに、その観点を踏まえ、具体的なラベリング制度の対象機器候補について検討する。まず、セキュリティ・アシュアランスの確保が望まれる機器の観点について、経済産業省の IoT-SSF で示された 2 つの観点(観点 A.及び観点 B.)に基づいた整理が効果的であると考えられる。IoT-SSF で示された 2 つの観点は図 4-28 に示すとおりであり、機器においてインシデントが発生した場合の影響を踏まえて整理される。観点 A.の「発生したインシデントによる経済的影響(社会の混乱、機器メーカーへの賠償金等)が高い機器」については、高いセキュリティ・アシュアランスレベルが求められるほか、同様に、観点 B.の「発生したインシデントの回復困難性の度合い(個人情報や人命・安全に対する影響等)が高い機器」についても、高いセキュリティ・アシュアランスレベルが必要である。本整理では、それぞれの観点に関して、求められるセキュリティ・アシュアランスレベルの高さを確認するための具体的な確認項目を図 4-28 のように整理した。そして、表 4-30 に示すとおり、各項目に対する具体的なレベル案を検討した。

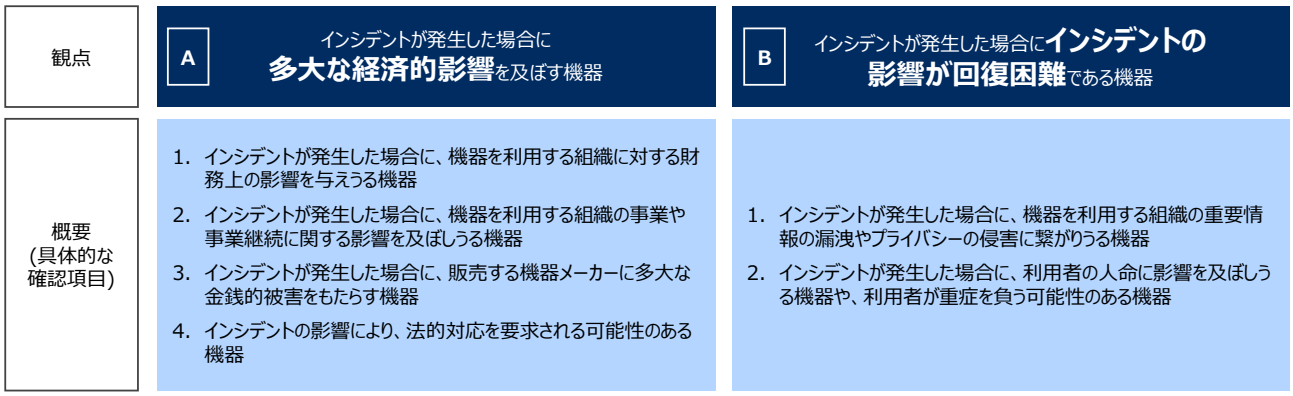


図 4-28 機器のセキュリティ・アシュアランスレベルを判断するための観点

表 4-30 各確認項目に対するレベル案

観点	具体的な確認項目	レベル			
		該当なし	低位	中位	高位
A. インシデントが発生した場合に多大な経済的影響を及ぼす機器	1. インシデントが発生した場合に、機器を利用する組織に対する財務上の影響を与えうる機器	インシデントが発生した場合に、機器を利用する組織に対して、損失や賠償責任が生じる可能性はない。	インシデントが発生した場合に、機器を利用する組織に対して、軽微又は若干の財務上の損失や賠償責任が生じる可能性がある。	インシデントが発生した場合に、機器を利用する組織に対して、深刻な財務上の損失や賠償責任が生じる可能性がある。	インシデントが発生した場合に、機器を利用する組織に対して、壊滅的な財務上の損失や賠償責任が生じる可能性がある。
	2. インシデントが発生した場合に、機器を利用する組織の事業や事業継続に関する影響を及ぼしうる機器	インシデントが発生した場合に、機器を利用する組織が対応に当惑する可能性はない。	インシデントが発生した場合に、機器を利用する組織が対応に当惑する可能性がある。	インシデントが発生した場合に、機器を利用する組織に対して、限定的かつ短期間の活動停止を引き起こす恐れや、組織の地位や評判に一定程度の影響を及ぼす可能性がある。	インシデントが発生した場合に、機器を利用する組織に対して、深刻又は長期間の活動停止を引き起こす恐れや、組織の地位や評判に多大な影響を及ぼす可能性がある。
	3. インシデントが発生した場合に、販売する機器メーカーに多大な金銭的被害をもたらす機器	インシデントが発生した場合に、機器を販売するメーカーに対して、損失や賠償責任が生じる可能性はない。	インシデントが発生した場合に、機器を販売するメーカーに対して、軽微又は若干の財務上の損失や賠償責任が生じる可能性がある。	インシデントが発生した場合に、機器を販売するメーカーに対して、深刻な財務上の損失や賠償責任が生じる可能性がある。	インシデントが発生した場合に、機器を販売するメーカーに対して、壊滅的な財務上の損失や賠償責任が生じる可能性がある。

観点	具体的な確認項目	レベル			
		該当なし	低位	中位	高位
	4. インシデントの影響により、法的対応を要求される可能性のある機器	インシデントの影響により、民事上又は刑事上の法的対応が要求される可能性はない。	インシデントの影響により、法執行の対象とならないような性質の民事上又は刑事上の法的対応が要求される可能性がある。	インシデントの影響により、民事上又は刑事上の法的対応が要求される可能性がある。	インシデントの影響により、特に重要な民事上又は刑事上の法的対応が要求される可能性がある。
B. インシデントが発生した場合にインシデントの影響が回復困難である機器	1. インシデントが発生した場合に、機器を利用する組織の重要情報の漏洩やプライバシーの侵害に繋がりうる機器	インシデントが発生した場合に、個人情報、政府の機密情報又は企業秘密の公開、プライバシーの侵害等の可能性はない。	インシデントが発生した場合に、個人情報、政府の機密情報又は企業秘密の限定的な公開、プライバシーの侵害等により、機器を利用する組織に対して、限定的な悪影響をもたらす可能性がある。	インシデントが発生した場合に、個人情報、政府の機密情報又は企業秘密の公開、プライバシーの侵害等により、機器を利用する組織に対して、重大な悪影響をもたらす可能性がある。	インシデントが発生した場合に、個人情報、政府の機密情報又は企業秘密の公開、プライバシーの侵害等により、機器を利用する組織に対して、致命的又は壊滅的な悪影響をもたらす可能性がある。
	2.インシデントが発生した場合に、利用者の人命に影響を及ぼしうる機器や、利用者が重症を負う可能性のある機器	インシデントが発生した場合に、利用者の安全性に対して、影響を与える可能性はない。	インシデントが発生した場合に、利用者に対して、医療措置を必要としない軽症の影響を与える可能性がある。	インシデントが発生した場合に、利用者に対して、軽症が生じる中程度のリスク又は医療措置を必要とする負傷が生じる限定的な影響を与える可能性がある。	インシデントが発生した場合に、利用者に対して、深刻な負傷、又は利用者が死に至る可能性がある。

そして、図 4-29 に示すとおり具体的な確認項目に基づき、製品のセキュリティ・アシュアランスレベ

ルを確認できるようにするための Yes/No チャートの案を作成した。本チャートでは、製品のセキュリティ・アシュアランスレベルを 4 段階に分けた。アシュアランスレベル 1 においては、適切なセキュリティ対策を施すとともに、その対策状況を自己宣言できるレベルが望まれる。アシュアランスレベル 2 では、セキュリティ対策状況について客観的な評価が求められることに加え、アシュアランスレベル 3 では、セキュリティ対策に関する説明責任が強く求められる。例えば、大手ネットワーク機器メーカーが開発・販売する電力会社の発電監視制御システムで用いられるルータであれば、A-2 や B-2 の項目が「高位」に分類されると考えられるため、「アシュアランスレベル 3」となる。また、スタートアップ企業が開発・販売する主に一般家庭で用いられるスマートロックの場合、A-3、A-4、B-1 の項目が「中位」に分類されると考えられるため「アシュアランスレベル 2」となる。そして、大手家電メーカーが開発・販売する主に一般家庭で用いられるスマート TV の場合、B-1 の項目が「低位」に分類されると考えられるため「アシュアランスレベル 1」となる。

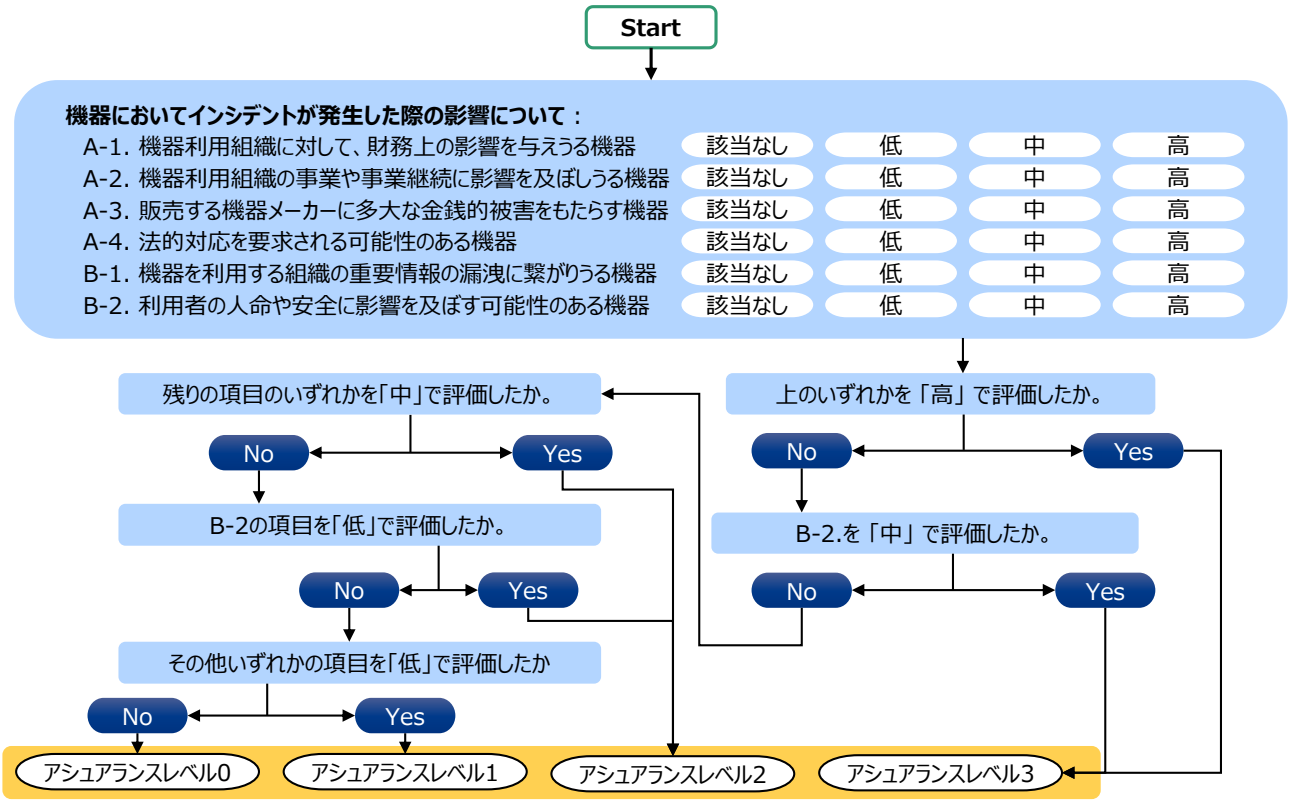


図 4-29 セキュリティ・アシュアランスレベルの判定に関する Yes/No チャート案

本チャートは現状案であるため今後精緻化することが必要であるが、レベル 1～3 に該当する製品はセキュリティ・アシュアランスの確保が求められる。諸外国の取組を踏まえると、アシュアランスレベル 3 のようなハイアシュアランスの機器をラベリング制度の対象に含めるかは詳細な議論が必要だが、少なくともレベル 1 に分類されるような製品はラベリング制度の対象に含めるべきである。また、セキュリティ・アシュアランスレベルの考えに基づき、ラベリング制度を設計する方針も想定される。すなわち、それぞれのアシュアランスレベルで対象となる IoT 製品やそのユースケースを明確化するとともに、シンガポールのラベリング制度を参考に、アシュアランスレベル毎に、求められる基準や評価内容を変更することも想定される。

4.4 検証サービスに係るガイドラインの普及、啓発手法について

検証サービスビジネスの発展を目的として、過年度事業で作成された「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」の普及・啓発に係る手法の調査・検討を行った。検証サービスビジネスのさらなる発展にあたっては、検証サービス事業者及び機器メーカーの両方において、検証に係るスキル・知識の向上が不可欠であり、手引きでは、検証サービス事業者及び検証人材に対して実施すべき事項や手法等を示すこと、そして検証依頼者である機器メーカーに対しても検証依頼にあたって実施すべき事項や留意事項等を示すことを目的としており、両者のスキル・知識の向上に資する内容が含まれている。

本調査項目では、検証に関するスキルや知識の向上のために、手引きの活用にあたっての課題等を調査・整理した。具体的には、手引きを活用しうる機器メーカーに対してヒアリング調査を実施し、手引きの活用状況、活用にあたっての課題等を聴取した。ヒアリングで得られた意見は以下のとおりである。

- 昨年度策定された手引きは、検証事業者への依頼時だけでなく、機器メーカー内部での検証にあたっても活用できる。ただし、「機器メーカー」とひと括りにはできないと考えている。ハードウェアやソフトウェアの設計・開発をすべて国内で実施しているメーカーもいれば、国内メーカーだが実態は海外から輸入した機器を販売しているのみのメーカーも存在する。後者のメーカーにおいては、内部で検証を実施することが難しいのではないか。
- 手引きに関して、関連企業より問い合わせがあった。内容についてまだ十分に認知されておらず、今後周知していく必要があると考えている。
- 手引きが日本語のみで良いのか、という問題もあるであろう。国内外問わず様々なメーカーのデバイスが増え、海外メーカーでも技適の要件を満たすデバイスが増えてきたが、検証を求めた際に、どの程度対応できるかは疑問である。海外デバイスの阻害要因にならないことも重要である。

手引きでは機器検証において実施すべき事項が詳細に記載されているところ、検証事業者への依頼時だけでなく、機器メーカー内部での検証にあたっても活用できるとの意見が得られた。第 4.3.1 項で示したとおり、IPA の調査結果によれば、製品出荷前に検証を実施している機器メーカーは 60%未満であり、40%以上のメーカーが機器検証を実施せず製品を出荷している。検証を実施していないメーカーは、「検証の重要性を認識しつつも、検証を実施していない機器メーカー」と「そもそも検証の重要性を認識していない機器メーカー」の大きく 2 つに分類されると考えられるが、前者の機器メーカーに対しては、手引きを適切に周知し、製品出荷前の検証において活用いただくことが期待される。現状の手引きには、網羅的な内容が記載されているものの、セキュリティに関する専門知識を有さない担当者が内容を理解し、業務に活用するには一定のハードルが存在する。そのため、手引きを周知するためには、手引きの内容をより噛み砕いたプラクティス集や、実際に機器メーカーで活用した際の事例集を作成することが効果的である。後者の「そもそも検証の重要性を認識していない機器メーカー」に対しては、IoT 機器等におけるセキュリティ脅威やセキュリティ対策の重要性、脆弱性が存在・悪用された場合に機器メーカーに与える影響を適切に周知する必要がある。具体的な周知方法として、セミナー等の開催のほか、検証のコスト負担を可能な限り軽減するために、検証にあたって活用できる補助金と併せて周知

することが効果的であると考えられる。

5. まとめ・考察

本調査では、国内外の IoT 機器等に対する先進的手法を用いた脆弱性等の検証技術等について調査を行い、セキュリティ検証方法の技術動向や、機器ごとに効果的な検証手法等の考え方を整理した。そしてこの整理結果を踏まえ、検証サービス事業者等に向けたガイドラインである「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。さらに、我が国における検証サービス事業の効果・信頼性を向上させ、検証サービスビジネスを重要な産業として活性化させることを目的に、信頼できる検証主体（検証者・検証サービス事業者等）を確認する仕組み等について検討を行った。

5.1 IoT 機器等に対する先進的手法を用いた脆弱性等の検証の現状に関する調査

スマートTV、スマートリモコン、カーナビゲーションシステム及び産業用無線ルータ・産業用コントローラの 4 機器区分に対して、民間検証サービス事業者における脆弱性等の検証の取組について調査を行ったうえで、これらを比較・整理した。調査は、三社の検証サービス事業者による有償の検証結果報告書に基づき、それぞれの機器に対する検証手法及び検証に必要なシステム環境について整理を行った。加えて、整理結果に基づき検証者に求められる知識やスキルを分析した。

調査を行った民間検証サービス事業者の検証結果報告書すべてにおいて同様の検証手法を採用しているわけではなく、それぞれの事業者の得意分野や実績等に応じて、各機器に適した検証手法を選定していることが確認された。一方で、多くの事業者の検証結果報告書において、検証実施前での検証対象機器に関する情報収集や想定脅威の分析に関する内容が記載されており、その重要性が確認できた。いずれの検証対象であっても、機器に対する理解の深化や想定される脆弱性を事前に把握した後に検証を実施することで、効率的な検証を行うことができると考えられる。

検証手法としては、ハードウェアに対する調査及びファームウェアに対するバイナリ解析の記載が目立った。ハードウェア基盤の調査を行い、IC の型番を特定して BIOS を推測するほか、機器のデバッグ端子を介したファームウェアの抽出可否の確認が多く実施されていた。抽出されたファームウェアに対するバイナリ解析では、実装の不備による脆弱性、既知脆弱性の存在、ファームウェアアップデート時のコード署名の有無、当該コード署名の暗号化方式、認証情報の特定可能性等が確認された。バイナリ解析は手動での解析が中心となるため、すべての実行パスについて網羅的に解析することは現実的に不可能である。そのため、検証の精度や脆弱性の検出有無は検証者のスキル・知識や実績・経験に依存する。

本調査では IoT 機器等本体への検証の取組について、検証サービス事業者による有償の検証結果報告書に基づき整理を行ったため、IoT 機器等が接続する先のサーバやクラウドサービスに対するペネトレーションテスト等の検証の現状については十分な調査ができていない。しかしながら、近年の IoT 機器等の多くはクラウドサービスに接続しており、クラウドサービスに障害が発生することで機器の運用や制御に影響を与える可能性もある。今後、機器本体だけでなく、接続先のクラウドサービス等も含めた IoT システム全体を対象とした検証について検討を行うことが望まれる。

5.2 検証サービスに係るガイドラインの拡充

IoT 機器等に対する先進的手法を用いた脆弱性等の検証の現状に関する調査の結果を踏まえ、令和 2 年度事業で作成した「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」の拡充を行った。具体的には、手引きの付録 5.1「機器固有の検証手法等」において、本事業で選定したスマートTV、スマートリモコン、カーナビゲーションシステム及び産業用無線ルータ・産業用コントローラの 4 機器区分に関し、検証者に求められる知識・能力、具体的な検証手順、検証にあたっての留意点等を追記した。

今後、策定した手引きの活用を促す取組を行うことが望まれる。第 4.4 節で記載したとおり、本事業を通じて手引きの普及・啓発に係るヒアリング調査を実施した。ヒアリングにおいては、手引きは十分に認知されておらず、今後も周知する必要性が提起された。あわせて、手引きでは機器検証において実施すべき事項が詳細に記載されているところ、検証事業者への依頼時だけでなく、機器メーカー内部での検証にあたっても活用できるとの意見が得られた。現状の手引きには、網羅的な内容が記載されているものの、セキュリティに関する専門知識を有さない担当者が内容を理解し、業務に活用するには一定のハードルが存在する。そのため、機器メーカーに対して手引きを周知するためには、手引きの内容をより噛み砕いたプラクティス集や、実際に機器メーカーで活用した際の事例集を作成することが効果的である。また、機器メーカーの中には、そもそも検証の重要性を認識していないメーカーも存在すると考えられる。このようなメーカーに対しては、検証の必要性以前に、IoT 機器等におけるセキュリティ脅威やセキュリティ対策の重要性、脆弱性が存在・悪用された場合に機器メーカーに与える影響を適切に周知する必要がある。具体的な周知方法として、セミナー等の開催のほか、検証のコスト負担を可能な限り軽減するために、検証にあたって活用できる補助金と併せて周知することが効果的であると考えられる。

5.3 検証サービスビジネスの発展に関する調査・検討

産業として重要になっていくと考えられる検証サービスビジネスを、更に発展させ利用を促進していくために必要な事項について調査・検討を行った。具体的には、信頼できる検証事業者を確認する仕組みや機器のサイバーセキュリティ確保のために求められる取組、検証サービスに係るガイドラインの普及・啓発手法に関して調査・検討を行った。

5.3.1 信頼できる検証事業者を確認する仕組みについて

まず信頼できる検証事業者を確認する仕組みの調査・検討結果の概要及び考察について記載する。この仕組みに関して、以下の 5 つの論点を設定した調査・検討を行った。

1. 信頼できる検証事業者に求められる要件は何か。また、各要件についてどの程度のレベルが、どの対象に対して求められるか。
2. 構築した仕組みは、どのような目的で、どの依頼者によって活用されるべきか。
3. 検証事業者の信頼性を誰が、どのように確認し、可視化するか。
4. 検証依頼者が、信頼できる検証事業者を選定するために必要な仕組みは何か。
5. 信頼できる検証事業者に対して、どのようなインセンティブが考えられるか。

諸外国の制度で用いられている信頼性要件、検証事業者や検証依頼者に対するヒアリング結果、有識者検討会での議論及び審査登録機関に対するヒアリング結果を踏まえて各論点について検討を行い、IoT 機器等に対して検証を実施する検証事業者の信頼性を確認する仕組みの案を作成した。

前提となる仕組みの位置づけとして、今回考える仕組みは、既に国内で運用されている情報セキュリティサービス基準審査登録制度に追加する方針とした。具体的には、今回検討した IoT 機器等に対する検証サービスを「機器検証サービス」として、情報セキュリティサービス基準に新たに追加する方針とした。論点 1 に関して、現行の審査登録制度で求められる要件区分である「技術要件」と「品質管理要件」の 2 区分に基づき、具体的な要件項目及び審査基準を設定した。具体的な要件及び審査基準の案は 4.2.8(2)に記載している。また、本仕組みで求めるレベルについて、現状で IoT 機器等に対する検証サービスが国内で十分に成熟していない状況を踏まえ、技術要件及び品質要件に係る最低限の信頼性を有した検証事業者を確認できる仕組みを目指すこととした。そのため、論点 2 について、IoT 機器等のベンダーが機器に対して検証を実施する際に、適切な品質管理及び情報管理に努めている検証事業者の選定するために活用する目的を対象とし、重要インフラ事業者等が高信頼な検証事業者を選定するために活用する目的は検討のスコープ外とした。

論点 3 に関して、情報セキュリティサービス基準審査登録制度に追加する方針を踏まえ、現行の審査登録制度のスキームと同様に、情報セキュリティサービスに関する審査登録機関により確認する方針とした。具体的な確認スキームを図 4-8 に、各要件項目の審査にあたって検証事業者による提出が必要な資料を表 4-14 に、事業者の登録・更新プロセスをそれぞれ表 4-15・表 4-16 に記載している。

論点 4 に関して、検証依頼者である機器メーカーに対するヒアリング調査において、検証依頼者の選定にあたっては、自社が展開する製品に関する分野の検証実績があるかを重視するとの意見が挙げられた。そのため、検証依頼者である機器メーカーが自社の製品の検証に適した検証事業者を選定できるよう、今回の機器検証サービスでは、情報セキュリティサービス基準適合サービスリストにおいて登録された各検証事業者が過去に機器検証サービスにて検証を実施した実績のある機器について記載することを想定した。機器検証サービスにおける情報セキュリティサービス基準適合サービスリストのイメージは図 4-9 のとおりであり、過去に機器検証サービスにて検証を実施した実績のある機器も併記することを想定した。

最後に論点 5 に関して、検証事業者に対するヒアリング調査において、適合サービスリストに掲載されることで検証依頼者からの信頼獲得につながり、結果として自社の売上につながることがインセンティブになりうるとの意見が挙げられた。この意見からも分かるとおり、検証事業者にとっての登録のインセンティブは、登録されることで自社の売上向上に寄与するかどうかという点であるため、今回検討した仕組みを構築するだけではなく、構築した仕組みを検証依頼者において活用いただき、検証事業の利用をさらに促進していく必要がある。したがって、本事業では制度の利用促進に向けた課題及び解決方向性についても検討した。具体的な検討結果は 4.2.8(4)に示すとおりである。

今後、4.2.8(4)で記載した方向性を踏まえ、検証サービスの利用促進に向けた取組を実行することが望まれる。4.2.8(4)で記載したとおり、制度の活用促進に関する課題と、制度を活用した適切な機器検証の推進に関する課題の大きく 2 つの課題が存在する。前者の課題に対しては産業分野個別のガイドラインにおける訴求や中小企業に対する直接的な検証の訴求、後者の課題に対しては検証ビジネス契約に関する「モデル取引・契約書」の新規策定や検証人材の育成に向けた取組について今後検討することが望まれる。なお、本事業において検討した信頼できる検証事業者を確認する仕組みは、前述のとお

り、審査登録制度に追加する方針であるため、技術要件及び品質要件に係る最低限の信頼性を有した検証事業者を確認できる仕組みに過ぎない。そのため、今年度の検討においては、重要インフラ事業者等が高信頼な検証事業者を選定するために活用する仕組みの検討はスコープ外とした。他方で、令和4 年 2 月 25 日に通常国会に提出された「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律案（経済安全保障推進法案）」の動向からも分かるとおり、重要インフラ等の基幹インフラに納入される重要設備のセキュリティを確保することは非常に重要であり、そのような重要設備に対する検証サービスも今後さらに必要性が増すことが想定される。重要設備に対して検証を実施する検証事業者を確認する仕組みを構築するとしたとき、今年度検討した仕組みより更にレベルの高い要件や確認方法を設ける必要がある。具体的には、検証可能なプラットフォームや無線通信機能を細分化し、どの項目に対してどの程度の検証が可能かを確認するほか、情報管理の側面では、英国の CHECK 制度と同様にセキュリティクリアランスに関連する要件を設定することも想定される。また、具体的な要件の確認方法として、有識者検討会や検証事業者へのヒアリングで意見されたとおり、実機に対する検証の試験を設けることで、検証人材の技術力を測ることも一案である。今回検討した信頼できる検証事業者を確認する仕組みは、国内の検証サービス活性化に向けた一つの基盤であるため、今後も検証のニーズを踏まえて仕組みを発展させることが必要である。

5.3.2 機器のサイバーセキュリティ確保のために求められる取組について

IoT 機器等に対する検証により機器における脆弱性の有無や脅威に対する対策の妥当性を確認できるものの、機器検証は機器におけるセキュリティ対策状況を確認する一つの手法に過ぎず、機器のセキュリティ確保のためには、その他の取組も推進することが必要不可欠である。有識者検討会においても、IoT 機器等のセキュリティ確保や信頼の繋がりの確保のためには、機器検証だけでなく、その他のセキュリティ対策の取組についても考慮すべきとの意見が挙げられた。これらを踏まえ、大局的な視点から、機器検証に限らず機器のサイバーセキュリティ確保のために求められる取組について調査・検討を行った。このために、国内機器メーカーにおけるセキュリティ対策状況や機器メーカーが抱えている課題について調査するとともに、国内外における機器のセキュリティ確保・向上に係る代表的な取組について調査し、国内で取り組むべき施策の方向性について検討した。

国内機器メーカーが抱える機器のセキュリティ対策における課題に関して、半数程度の機器メーカーが、セキュリティ対策に要するコスト負担や、セキュリティ対策にあたっての人材不足の側面で課題を抱えていることが分かった。前者の課題に対して、セキュリティ対策に要するコスト負担は製品の販売価格に反映されるところ、機器メーカーにおける機器開発へのセキュリティ対策の取組を適切に評価するとともに、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製品が積極的に導入されるような社会の仕組みを構築することが望まれる。諸外国での取組を参考にすると、このような仕組みの一候補として、IoT 製品に対するセキュリティラベリング制度が考えられる。我が国におけるラベリング制度の構築に関して有識者検討会で議論したところ、有識者より賛成の意見が多数挙げられた。今後、ラベリング制度の構築に向けた検討を進めることが望まれる。ラベリング制度の構築に向けた論点について、表4-28 に示したとおり、対象とする製品区分を決定するほか、ラベル付与の方法や制度の運用方法について検討する必要がある。これらの論点の検討にあたっては、既に制度が開始しているシンガポールやフィンランドの取組を参考にするほか、現在制度の構築が検討されている米国の状況を参考にすることに加え、国内機器メーカーや消費者のニーズを適切に抽出する必要がある。IoT 機器のセキュリティ対

策に関する消費者ニーズの調査に関して、MS&AD インターリスク総研株式会社が 2021 年に 1,000 名を対象に実施したアンケート調査[87]では、「『IoT 機器や IoT 機器を使ったサービスは、政府や業界団体が推奨、要求するサイバーセキュリティガイドラインなどの規格や標準を満たしているべきである』という考え方をどう思いますか」という質問に対して、60%以上の回答者が「ガイドライン対応すべきと考える」と回答しており、一定程度の消費者は、ガイドライン等に基づく IoT 機器に対するセキュリティ対策の必要性を理解していることが分かる。このような消費者に対しては、セキュリティ対策が講じられていることを、ラベルの付与によって明確化することは重要であると考えられる。一方で、どの程度製品価格が上昇したとしても、一定のセキュリティ対策が講じられている製品を購入したいかという消費者の意向に関する明確なデータは明らかになっていない。ラベリング制度の構築にあたっては、どの程度の価格差であれば、一定のセキュリティ対策が講じられた製品を購入するか、消費者のニーズを調査することも重要であり、このような調査結果を踏まえ、ラベルの審査費用や消費者に対して周知すべき情報等を検討することが望まれる。

機器メーカーが抱える人材不足の課題に関して、機器のライフサイクル全体で求められるセキュリティ対策にあたって必要なスキル・知識を可視化するほか、そのようなスキル・知識を獲得できる環境として、機器に対する検証、分析、解析等が実施できる検証ラボの構築が有効であると考えられる。検証に関連するラボを構築することで、セキュリティ人材がいない機器メーカーにおいても一定の品質を満たした検証を低コストで行うことができるほか、検証人材のスキルアップにも寄与すると考えられる。有識者検討会では、検証ラボを国内複数箇所に構築することを望む意見が挙げられた。国内において検証ラボを複数箇所に構築するとしたとき、必ずしも政府が直接的に検証ラボを構築・運用するのではなく、間接的な支援も考えられる。具体的には、既存の検証ラボの支援を行うほか、民間企業に対して検証ラボの構築を支援し、民間企業が運用者となるスキームも想定される。今後、国内において IoT 機器の検証に特化した検証ラボを構築し、政府として支援するとした場合、当該ラボの意義・目的・目標・対象範囲について明確化したうえで、政府としての支援範囲を検討することが望まれる。

[87] MS&AD インターリスク総研株式会社、個人向け IoT 機器に関するサイバーセキュリティ対策の意識調査報告書 https://www.irric.co.jp/pdf/reason/research/2021_cyber_security.pdf

別紙 1

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

（令和４年３月 拡充版）

経済産業省 商務情報政策局

サイバーセキュリティ課

目次

「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」 の策定にあたって

○ サイバー空間とフィジカル空間の高度な融合に伴い、フィジカル空間に点在する機器がサイバー攻撃の新たな対象となるリスクが顕在化している。機器のセキュリティを脅かす事例は多く発生しており、利用者に被害を与えるだけでなく、機器を介してネットワークに接続している他の機器に対しても影響が及んでいる。そして、その影響はサイバー空間にとどまらず、フィジカル空間にまで及ぶ可能性がある。

○ セキュリティ脅威に繋がりうる脆弱性の有無やセキュリティ対策の妥当性を確認する方法としては、機器に対するセキュリティ検証が有効である。機器メーカにおいては、出荷以前の機器に対してセキュリティ検証を行うことで、機器における脆弱性の有無や妥当なセキュリティ対策を確認することが可能となる。これにより、当該機器の脆弱性を狙った攻撃による被害をあらかじめ低減することができるほか、出荷後に脆弱性を修正することに対するコストを低減できる。

○ 一方で、現在までのセキュリティ検証サービスは、検証人材の暗黙知に依存している部分が大きく、効果的な検証手法や実施すべき事項については統一的な整理がなされていない状況にある。

○ 検証を依頼する立場にある機器メーカ等の検証依頼者においては、信頼できる検証サービス事業者を選定するための基準や検証サービスの目標が不明瞭であり、依頼者が求める品質や結果と実際のサービス内容に差異が生じている。

○ また、適切な検証サービスを受けるためには、検証依頼者も一定の知識を有し、適切な検証目的の下で検証依頼を行うことが望ましいものの、現状では十分な目標や目的なく依頼を行っているケースもあり、依頼者が求める結果が得られないことも多い。

○ こうした問題意識から、本手引きは、検証サービス事業者のサービス高度化を目的として、機器のセキュリティ検証において検証サービス事業者が実施すべき事項や、より良い検証サービスを受けるために必要な検証依頼者が実施すべき事項や持つべき知識、並びに検証サービス事業者・検証依頼者間の適切なコミュニケーションのために二者間で共有すべき情報や留意すべき事項について示したものである。

○ 本手引きを検証サービス事業者及び検証依頼者が活用することで、国内の検証サービス水準向上に寄与するとともに、二者間の適切な検証体制が構築されることが期待される。

1 背景と目的

1.1 背景

ネットワーク化や IoT（Internet of Things）の利活用が進む中、サイバー空間とフィジカル空間との相互作用が急速に拡大している。我が国においても、平成 28 年 1 月 22 日に閣議決定された「第 5 期科学技術基本計画」において、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」を提唱している。さらに、「Society5.0」へ向けて、様々なつながりによって新たな付加価値を創出する「Connected Industries」の実現に向けた新たな産業構造の構築が求められている。「Society5.0」では、IoT ですべてのヒトとモノが繋がり、サイバー空間とフィジカル空間が高度に融合する中で、様々な知識や情報が共有されることで、新たな価値が創出される。これにより、企業を中心に付加価値を創造するための一連の活動であるサプライチェーンも、その姿を変えることになり、これまでのように供給者が企画・設計するという固定的なものではなく、より柔軟で動的なサプライチェーンを構成することが可能となる。

一方で、サイバーセキュリティの観点では、サイバー空間とフィジカル空間の高度な融合によって、サイバー空間の影響がフィジカル空間に及ぶ可能性も増大する。「Society5.0」における新たなサプライチェーンに対する脅威は、これまで直面していた定型的・直線的なものから複雑化し、脅威によって発生した被害が影響する範囲も広くなっていく。経済産業省は、この新たなサプライチェーンをバリュークリエイションプロセスと定義し、このプロセスに関わる全要素についてセキュリティ確保及び信頼性（Trustworthiness）確保を目的として、「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）」を平成 31 年 4 月 18 日に策定した。このフレームワークでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデルを三層構造と 6 つの構成要素として提示し、それぞれにおいて守るべきもの、直面するリスク源、対応方針等を整理した。

バリュークリエイションプロセス全体を俯瞰したセキュリティ対策を円滑に行うためには、必要な機器・部品等が円滑に調達できる環境や仕組みが必要となる。このためには、当該機器・部品の安全性・有効性を確認し検証する仕組みの構築が不可欠である。令和元年 6 月 7 日の「デジタル時代の新たな IT 政策大綱」において、高水準・高信頼のセキュリティ機器の検証サービスの基盤を日本に構築する「Proven in Japan」の推進について述べられたとおり、検証する仕組みの高度化はバリュークリエイションプロセス全体のセキュリティ対策に寄与するものであり、ひいては「Society5.0」を支える信頼の価値創出につながるものである。

1.2 本手引きの目的

本手引きは、検証サービス事業者のサービス高度化を目的として、機器のセキュリティを検証するセキュリティ検証（以降、省略し「検証」という）における、検証サービス事業者が実施すべき事項を示すものである。現在までの検証サービスは、検証人材の暗黙知に依存していることが多く、効果的な検証手法

については統一的な整理がなされていない状況にある。また、検証依頼者においては、信頼できる検証サービス事業者を選定するための基準や検証サービスの目標が不明瞭なため、依頼者が求める品質と実際のサービス内容に差異があることも事実である。加えて、適切な検証体制の構築のためには、検証依頼者も一定の知識を有し、適切な検証目的の下で検証依頼を行うことが望ましいものの、現状では十分な目標や目的なく依頼しているケースも少なくない。本手引きでは、適切な目標や目的に基づき、より良い検証サービスを受けるために、検証依頼者が実施すべき事項や持つべき知識についても示している。

本手引きは、本文書（以降、「本編」という）に加えて、三つの別冊によって構成される。表 1-1 に示すとおり、本編では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記載するが、詳細な検証手順や脅威分析の手法等は記載していない。具体的な検証に係る手順や脅威分析の手法は別冊 1 にて示す。本手引きでは、IoT 機器等に適用される検証手法のうち、特にソフトウェア及びファームウェアに関する検証手法について具体的な手順等を示す。また、主な検証依頼者である機器メーカが、検証を依頼するにあたって実施すべき事項や用意すべき情報等を別冊 2 にて示す。加えて、別冊 3 では、検証サービス事業者における検証人材の育成にフォーカスを当て、検証人材のキャリアを構想・設計する上で考慮すべき観点を示す。

表 1-1 手引きの本編・別冊の概要

本編（本文書） **「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」**	• 検証サービス事業者が実施すべき事項や、検証依頼者が実施すべき事項や用意すべき情報、二者間のコミュニケーションにおいて留意すべき事項等を示す。 • 信頼できる検証サービス事業者を判断するための基準を記載する。
別冊 1 **「脅威分析及びセキュリティ検証の** **詳細解説書」**	• 検証サービス事業者が実施すべき脅威分析の手法や実施すべき検証項目、検証の流れを詳細に示す。 • 機器全般に汎用的に活用できる整理を目標とするが、対象の例としてネットワークカメラを実例とした手法の適用結果も示す。
別冊 2 **「機器メーカに向けた脅威分析及び** **セキュリティ検証の解説書」**	• 機器メーカが実施すべき事項や用意すべき情報等、意図した検証を依頼するために必要な事項を詳細に示す。 • 攻撃手法への対策例や、検証結果を踏まえたリスク評価等の対応方針を示す。

別冊 3 **「検証人材の育成に向けた手引き」**	• 検証人材に求められるスキル・知識を示し、それらのスキル・知識を獲得するために望まれる取り組みを示す。 • 検証人材のキャリアを構想・設計する上で考慮すべき観点を示し、検証人材のキャリアの可能性を示す。

本編及び三つの別冊を検証サービス事業者及び検証依頼者が活用することで、国内の検証サービス水準向上に寄与するとともに、二者間の適切な検証体制が構築されることが期待される。

1.3 本手引きで対象とする機器

本手引きの対象は、図 1-1 に示すとおり、IoT 機器をはじめとするネットワークに常時接続する機器、及びその関連サービスとする。

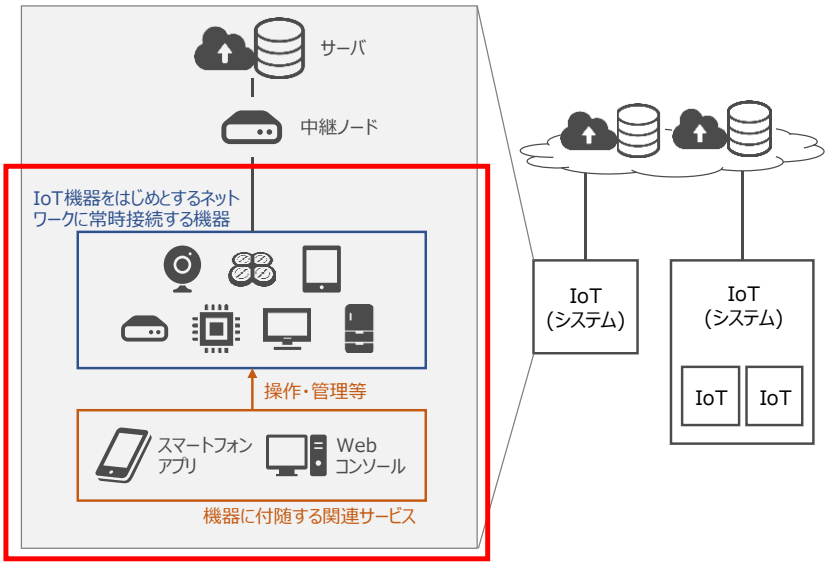


図 1-1 本手引きの対象機器イメージ[1]

本手引きでは、機器のサイバーセキュリティ確保に焦点を当てた記載を中心とし、IoT 機器等が接続するクラウドサーバや、機器を組み合わせたシステム全体の検証については対象外とする。一方で、サイバー空間とフィジカル空間全体のバリュークリエイションプロセスの信頼性確保のためには、フィジカル空間とサイバー空間の境界における転写の役割を担う IoT 機器・システムだけでなく、サイバー空間上のクラウドシステムやフィジカル空間上の組織に対してもセキュリティ対策を検証することが望まれる。また、IoT セキュリ

[1] IoT 推進コンソーシアム、総務省、経済産業省、IoT セキュリティガイドライン ver1.0 を参考に作成
https://www.soumu.go.jp/main_content/000428393.pdf

ティガイドラインで示されているように、IoT は他の IoT と繋がり新たな価値を生むという System of Systems（SoS）としての性質を有していることに留意が必要である。そのため、バリュークリエイションプロセス全体の信頼性を検証するにあたっては、単一機器・システムに対する検証だけでなく、SoS としての IoT に対して検証することが効果的である。

1.4 対象者

本手引きは、機器検証を実施する検証サービス事業者、及びこの事業者に対して機器検証を依頼するメーカの開発者、検証担当者、品質保証担当者、セキュリティ担当者等の検証依頼者を特に対象とする。表 1-2 に示すとおり、別冊 1 及び別冊 3 は特に検証サービス事業者、別冊 2 は検証依頼者を対象にしている。また、本手引きでは機器のセキュリティ確保に向けて実施すべき事項についても一部記載している。そのため、メーカの機器設計、構築の担当者、サプライチェーン管理に係る担当者等も参照できる。

表 1-2 本手引きの対象者

組織	対象者	本編	別冊 1	別冊 2	別冊 3
検証サービス事業者	検証のマネジメントを行う担当者	✓	✓		✓
	検証の実務に係る担当者	✓	✓	✓	✓
機器メーカ（検証依頼者）	機器の開発責任者	✓		✓	
	機器の開発・品質保証、検証、セキュリティ担当者	✓	✓	✓	
	機器の設計・構築の担当者	✓		✓	
	機器のサプライチェーン管理に係る担当者	✓		✓	

1.5 本手引きの活用方法

本手引きは、検証サービスの高度化を目的とし、検証サービス事業者及び検証依頼者が実施すべき事項を整理したものである。併せて、二者が適切な検証体制を構築するために、二者間のコミュニケーションにおける留意事項等を示したものである。

検証サービス事業者においては、検証実施のフェーズだけではなく、検証に向けた準備のフェーズや検証後の報告フェーズにおいて必要となるスキルや実施すべき事項を確認することで、自組織のサービスレベルを向上することができる。また、別冊 1 で示される検証の詳細手順や検証における留意点を確認することで、適切な検証サービスを依頼者に提供することができる。さらに、別冊 3 では、検証人材に求められるスキル・知識やキャリアの可能性を示しており、検証人材のスキル・知識の向上に向けた取り組みや検証人材のキャリアデザインの上で必要な観点を確認できる。これらにより、質の高い検証サービスを行うことができるというビジネスの信頼性、及び適切な情報管理等に基づきサービスを提供するという情報管理の観点での信頼性という二つの信頼性向上が期待される。

適切な検証体制の構築のためには、検証サービス事業者だけではなく、検証依頼者も一定の知識を有し、適切な検証目的の下で検証依頼を行うことが必要である。検証依頼者においては、本編及び別冊 2 を参照することで、目的に則した検証結果を得るために必要となる実施事項や正しい知識を確認することができる。併せて、別冊 2 では、検証結果を踏まえて機器メーカが考慮すべき事項や取るべき対応について確認することができる。加えて、本編では信頼できる検証サービス事業者を判断・選択するための指針も示しており、自組織が目的とする検証に則した検証サービス事業者を選定する際に活用することができる。

加えて、本手引きが、検証サービス事業者及び検証依頼者間の共通言語として活用されることが期待される。特に本編においては、検証の見積もり段階で検証依頼者が伝えるべき情報、契約締結後に二者間で共有されるべき情報、検証後に検証結果を報告する際に検証サービス事業者が伝えるべき情報、二者間の連絡体制を構築する際の留意事項等、二者が適切なコミュニケーションを行うための情報を示している。それぞれの項目を確認し、適切な検証体制が構築されることが期待される。

1.6 本手引き・本編の構成

本手引きのうち本編及び別冊 1・別冊 2 は、図 1-1 に示すとおり、機器開発プロセスにおける「検証」のフェーズに焦点を当て、検証において検証サービス事業者が実施すべき事項及び機器メーカが検証依頼のために準備すべき事項等を整理している。加えて、別冊 1 及び別冊 2 では、機器に対する脅威分析手法についても示している。機器への脅威分析は、機器の要件定義や設計のフェーズで実施すべきであり、開発プロセスの初期段階で実施することで、効果的な検証を実施することができるほか、後工程での手戻りを削減できる。別冊 3 では、検証サービス事業者が高品質な検証サービスを提供するにあたって検証人材に求められるスキル・知識や、検証人材のキャリアの可能性を示す。

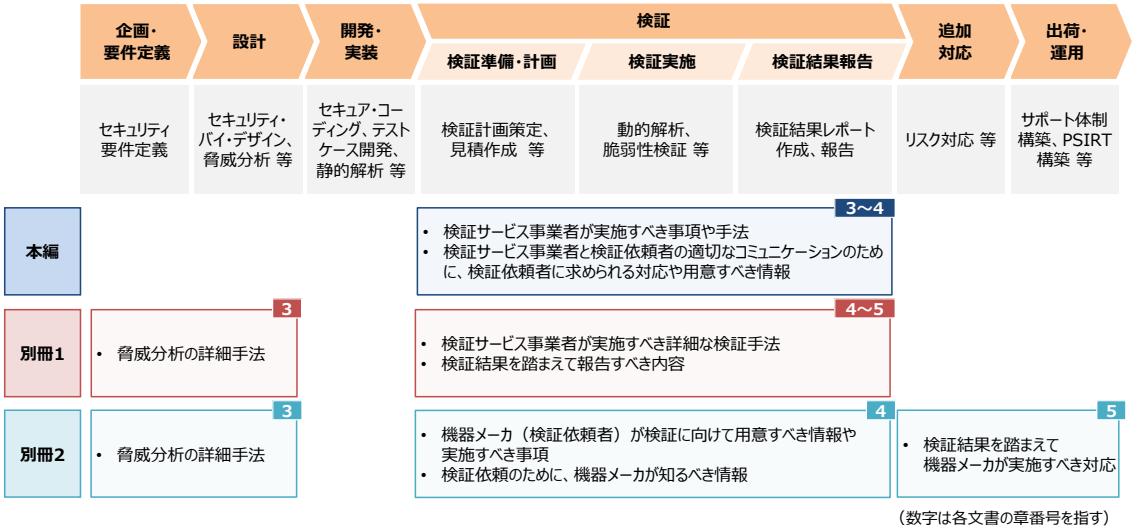


図 1-2 機器開発プロセスにおける本編及び別冊 1・別冊 2 のスコープ

このうち、本編の第 1 章においては、本手引き全体の背景や目的、対象とする機器、対象者、そして活用方法を示した。

第 2 章においては、一般的な機器検証の目的を示し、機器検証において遵守すべき最低限の原則を記載する。また、機器検証に適用できる一般的な検証手法を示す。

第 3 章においては、機器メーカが自社の製品に対して検証依頼を実施する場合の一連の検証ステップについて記載し、その中で検証サービス事業者及び検証依頼者が実施すべき事項を整理する。また、二者が適切な検証体制を構築するために必要な、二者間のコミュニケーションにおける留意事項等を示す。加えて、留意すべき法令等や脆弱性情報の取扱いの関連情報を記載する。

第 4 章においては、検証実施後に検証結果を報告するにあたって、検証サービス事業者及び検証依頼者が留意すべき事項を記載する。

第 5 章においては、付録として機器固有の検証手法等を示す。加えて、本編で使用する用語の定義と本編で参考とした文書を示す。

なお、本編第 3 章及び第 4 章の各節においては、検証サービス事業者及び検証依頼者が特に実施すべき事項を抽出して記載している。それぞれの担当者は、実施すべき事項を理解した上で、検証準備、検証計画の策定、検証実施、そして検証結果の報告という、検証の一連のステップをたどることが期待される。

2 機器検証とは

2.1 検証の目的

サイバー空間とフィジカル空間の高度な融合に伴い、フィジカル空間に点在する機器がサイバー攻撃の新たな対象となるリスクが顕在化している。事実、2016 年には固定された設定のルータやウェブカメラがマルウェア「Mirai」に感染し、感染した機器が発信源となり大規模な DDoS 攻撃が発生した。他にも「Bashlite」、「BrickerBot」、「Mirai」の亜種等のマルウェアが IoT 機器のセキュリティを脅かす事例は多く発生しており、IoT 機器の利用者に直接被害を与えるだけでなく、マルウェアに感染した機器を介してネットワークに接続している他の機器に対しても影響が及んでいる。そして、その影響はサイバー空間にとどまらず、フィジカル空間にまで及ぶ可能性がある。したがって、セキュリティ脅威に繋がりうる脆弱性が発見された場合には適切な対策が施されている必要があるが、脆弱性を発見する一つの方法として機器の検証が有効となる。

機器検証の目的は、機器における脆弱性の有無と脅威に対する対策の妥当性を確認することにあるが、具体的な目的や検証による効果は場面によって異なる。開発された機器に対して検証する場合、出荷以前に脆弱性を発見し、適切な対策を施すことが主な目的となる。これにより、当該機器の脆弱性を狙った攻撃による被害をあらかじめ低減することができるほか、出荷後に脆弱性を修正することに対するコストを低減できる。「DevSecOps」の概念のように開発段階でセキュリティ検証を行う場合、脆弱性を早期に発見することにより、手戻りによる開発遅延の防止や修正コストの低減が目的となる。また、機器の利用者自身がセキュリティ検証を行うことも想定される。機器導入段階で検証を行う場合、導入する機器のセキュリティ要件を確認することが主な目的となる。機器の運用段階で検証を行う場合も、適切な対策が施されることを確認すること及び脆弱性の有無を確認することが目的となるが、これにより自組織又はシステムの納入先に対するサイバー攻撃が成功するリスクを低減することができ、攻撃による影響を低減することができる。

機器メーカが自社の製品に対して検証依頼を行う場合、自社で開発した機器のセキュリティ対策が十分であるかを第三者による検証によって確認し、脆弱性の有無を確認することが目的となることが多い。この場合、検証の目標は、最も重要な機能において脆弱性が存在しないことを検証すること、又は幅広い機能やサービスに対して検証を行うことの大きく二つに分けられる。網羅性を担保することは重要であるが、検証にかけられるコストや機器の特性によって目標は変わるものであり、汎用品すべてに対して幅広い機能やサービスに対する検証を行うことは現実的ではない。反対に、攻撃を受けることで人命に影響を与えかねないメーカの基幹製品である場合、広範囲の機能やサービスに対して検証を行うことが望まれる。このように、検証の具体的な目的や目標はシーンや機器の特性、依頼背景等によって様々であるが、脆弱性の有無を確認するという共通目的に資するために最低限の原則は遵守する必要がある。これには以下のような項目が含まれる。

- **検証の目的・目標を事前に明確化する**：検証依頼者は、検証の目的・目標を自組織内で検討し、検証サービス事業者に伝える必要がある。
- **適切なコミュニケーションを行う**：質の高い検証は、検証サービス事業者と検証依頼者との適切

なコミュニケーションの上に成り立つ。検証のすべてのフェーズにおいて、二者間でコミュニケーションを取ることが必要である。

- **可能な限りの情報を活用する**：検証サービス事業者は、対象機器の構成情報や脆弱性情報をはじめとして、可能な限り多くの情報に基づき検証を行うことが必要である。検証費用や検証スケジュールを踏まえ、検証依頼者は、適切な情報を事業者に対して提供することが期待される。
- **複数の視点を持つ**：検証サービス事業者は、攻撃者の視点や機器利用者の視点等、複数の視点に基づき検証を行うことで、広範な脆弱性の検出や対策の検討が可能となる。
- **検証結果を文書化する**：検証サービス事業者は、検証の記録を残す必要がある。事前に、報告文書様式を検証依頼者と合意することが望ましい。併せて、結果報告後における脆弱性修正の確認対応についても、事前に定めておくことが望ましい。検証結果の文書化において実施すべき事項は、第 4 章にて具体的に記載する。
- **検証がセキュリティを完全に保証するものではないことを理解する**：検証依頼者は、検証項目を 100%網羅的に検証することは不可能であり、検証が機器のセキュリティを完全に保証するものではないことを理解する必要がある。最も重要な機能において脆弱性が存在しないことを確認することを目標とした検証、幅広い機能やサービスにおいて脆弱性が存在しないことを確認することを目標とした検証のいずれにおいても、それぞれの目標を 100%達成することは不可能であり、検証によって問題が発見されなかった場合でも、継続的にセキュリティ対策を行う必要がある。

2.2 一般的な検証手法

機器の検証手法は、機器を実際に動作させることなく、それを構成する設計書やソースコード等のロジックに基づいて実施する静的手法と、実際に機器を動作させた上で脆弱性の有無を確認する動的手法に大別される。一般的な機器検証手法の概要と代表的なツールを表 2-1 に示す。検証サービス事業者は、依頼者の目的や検証にかかるコスト、検証人材のスキル、そして既存の検証サービス等を踏まえて適切な検証手法を選択する必要がある。

別冊 1 では、それぞれの動的検証手法に関して、一般的に使用されるツールの操作方法やコマンドレベルでの解説とともに詳細な検証手法について記載する。また別冊 2 では、各動的検証手法の依頼にあたって機器メーカとして実施すべき事項や準備すべき情報を示しているほか、各検証手法の結果を踏まえて機器メーカにて実施すべき対応についても記載している。詳細な内容については、表 2-1 に示したそれぞれの別冊の記載箇所を参照されたい。

表 2-1 一般的な機器検証手法

分類	一般的な検証手法	概要	ツールの例	本編における記載書	別冊 1 における記載箇所	別冊 2 における記載箇所
静的手法	設計文書レビュー	機器の設計書を確認し、不適切なサービスや不適切な設定が存在しないか、適切なセキュリティ対策が組み込まれているかどうかを確認する。	–	第 3.4.1 項	–	–
	ソースコード解析	ソースコードを確認し、要求を満たすか、環境固有値やエラーが存在しないか、処理フローに問題が無いか、規約違反が存在しないかを確認する。ソフトウェアの安全性を論理的に保証する形式手法やモデル検査[2]も含まれる。	• CodeSonar • Coverity • Fortify Static Code Analyzer • Veracode	第 3.4.2 項	–	–
	ファームウェア解析	機器のファームウェアを抽出する。脆弱性が含まれてないかを確認するために、バイナリ解析手法と併せて行われることが多い。クラウドプラットフォームを活用した自動解析ツールも存在する。	• binwalk • Binwalk Enterprise • VDOO Vision	第 3.4.3 項	第 4.3 節	依頼時の留意点 第 4.2 節 結果への対応： 第 5.3 節

[2] 機器の動作や状態をモデルとして捉え、考えられるモデル（システムがとり得る状態）について、問題や異常が無いかを判定する手法。

分類	一般的な検証手法	概要	ツールの例	本編における記載書	別冊 1 における記載箇所	別冊 2 における記載箇所
	バイナリ解析	ファームウェア等のバイナリコードについて、実行パスに異常は無いか、不正なアドレス命令が無いかを静的に確認する。既存の実行ファイルについて実施する場合は、リバースエンジニアリングが必要となる。	• angr • Ghidra • IDA Pro	第 3.4.4 項	第 4.4 節	依頼時の留意点 第 4.3 節 結果への対応： 第 5.4 節
動的手法	ネットワークスキャン	どのポートに対して通信可能か、接続が許可されていない機器やサービスが存在しないかを確認する。	• arp-scan • nmap	第 3.4.5 項	第 4.5 節	依頼時の留意点 第 4.4 節 結果への対応： 第 5.5 節
	既知脆弱性の診断	既知の脆弱性が機器に内在しうるかを調べ、実際に悪用可能かを確認する。自動化ツールでは検出が難しい脆弱性も存在するため、自動化ツールと手動による解析を組み合わせた検証が望まれる。	• Nessus • Vuls • Hydra • Metasploit	第 3.4.6 項	第 4.6 節	依頼時の留意点 第 4.5 節 結果への対応： 第 5.6 節

分類	一般的な検証手法	概要	ツールの例	本編における記載書	別冊 1 における記載箇所	別冊 2 における記載箇所
	ファジング	極端に長い文字列や記号の組み合わせ等、問題が起こりそうなデータや改変したデータを挿入し、その挙動を確認する。	• American Fuzzy Lop • beStorm • Defensics • Peach Fuzzer • Raven	第 3.4.7 項	第 4.7 節	依頼時の留意点 第 4.6 節 結果への対応： 第 5.7 節
	ネットワークキャプチャ	機器やサービスのネットワークパケットを取得し、不審なパケットが無いかを確認する。	• tcpdump • Wireshark	第 3.4.8 項	第 4.8 節	依頼時の留意点 第 4.7 節 結果への対応： 第 5.8 節

※ 一部の検証手法に対応するツールについては、Open Web Application Security Project (OWASP)「Testing Guide」[3]の Appendix A においても記載されている。また、ファジングに係る検証ツールについては、情報処理推進機構（IPA）「ファジング活用の手引き」[4]にも記載されており、それぞれ本手引きと合わせての参照を推奨する。

[3] OWASP, Testing Guide v4 https://www.owasp.org/images/1/19/OTGv4.pdf
第 3 版については日本語版が公開されている https://www.owasp.org/images/1/1e/OTGv3Japanese.pdf

[4] IPA, ファジング活用の手引き https://www.ipa.go.jp/security/vuln/documents/fuzzing-guide.pdf

2.3 その他の検証手法

表 2-1 で示した一般的な検証手法のほかに、サイドチャネル攻撃等を想定したハードウェア解析も IoT 機器等に適用されうる検証手法として挙げられる。この手法では、システム LSI に対してレーザ光や電波を照射し、セキュリティ機能が解析される。近年では機器のサプライチェーンの経路中にハードウェアトロイと呼ばれる不正チップを組み込む脅威も注目を集めている。不正チップを埋め込まれた結果、機器に格納されている機密情報を外部に送信される危険性や、周囲の関連機器に対して攻撃を行う危険性が考えられる。現在までに発見されたハードウェアトロイの事例はほとんど存在しないが、サプライチェーンのさらなる複雑化やチップの小型化に伴い、このような脅威の顕在化も懸念される。

ハードウェア解析に必要な機器は非常に高価な場合もあり、検証の精度はこれらの機器に依存する部分が大きい。動作中の消費電力や放射電磁波等を測定して秘密情報を抽出するサイドチャネル攻撃を実施するためにはデジタルオシロスコープをはじめとする機器が必要になる。また、チップに対して規定外の電圧を与える攻撃（グリッチ攻撃）や電磁波照射攻撃、レーザ照射攻撃等によりチップを誤作動させ秘密情報を取り出す検証の場合、さらに高価な設備が必要となる。学術機関を中心に研究が進められているハードウェアトロイ解析も同様であり、ハードウェア解析は他の検証手法に比べ、検証にかかる金銭的コスト及び人的コストが非常に大きい。機器メーカがハードウェア解析を依頼する場合、すべての検証サービス事業者がハードウェア解析を実施するための設備を有しているわけではないため、ハードウェア解析を行うことができる事業者を選定して依頼する必要がある。

その他の検証手法として、組織が有するすべてのシステムや、指定されたシステム全体を対象とし、明確な意図を持った攻撃者によって、その目的が達成されうるかを確認するペネトレーションテスト[5]と呼ばれる手法も存在する。この手法では、システムに対する攻撃シナリオを検討した後、既知脆弱性の診断等で明らかになったシステムの脆弱性やソーシャルエンジニアリング等を悪用して攻撃者の目的を達成できるかどうかの確認を行う。その際、本手引きで対象としている IoT 機器等を侵入の入り口として想定する場合もある。ペネトレーションテストの場合、実際の攻撃者と同様の攻撃を模擬するため、システム全体の脆弱性だけでなく、運用面での脆弱性が明らかになり、組織のセキュリティレベルが顕在化するという特徴がある。これにより、攻撃により侵入された際の、組織のレジリエンスを測ることができる。

ペネトレーションテストは、脆弱性を網羅的に洗い出すことを目的とした検証ではなく、脆弱性を悪用することで、明確な意図を持った攻撃者がその目的を達成することが可能であるかを確認する。そのため、ペネトレーションテストにかかる費用や期間は、対象とするシステムの規模や範囲だけでなく、設定される攻撃者の目的によって左右される。ペネトレーションテストのステップや注意事項等は、ISOG-J 及び OWASP Japan による「ペネトレーションテストについて」[6]で示されている。近年では、TLPT（Thread-Led Penetration Test）と呼ばれる実在の攻撃者の戦術、テクニック、手順等を模倣し、組織のサイバーレジリエンスを侵害しようとすることを目的としたペネトレーションテストも注目を集めている。組織のセキュリティ対策状況に応じて、このような高度な検証の実施も考慮することが望ましい。

---

[5] ペネトレーションテストに使うツールとしては、Metasploit や Achilles Test Platform 等が挙げられる。TLPT（Threat-Led Penetration Test）等の高度なテストの場合、多くはサービスとして提供されている。

[6] ISOG-J 及び OWASP Japan, ペネトレーションテストについて https://github.com/ueno1000/about_PenetrationTest

3 検証の実施

3.1 検証手順

機器メーカが製品出荷前の自社の製品に対して検証依頼を実施する場合、その検証手順は図 3-1 に示すように実施される。検証サービスの品質を上げるためには、機器に対して実施する検証の質だけでなく、検証実施前の準備や計画、及び検証実施後の分析や整理についても品質を向上させることが必要である。また、一連の検証ステップにおいて、検証サービス事業者と検証依頼者間で適切なコミュニケーションを行う必要がある。なお、本章で示す検証の手順は、図 1-2 のうち「検証」で示されるプロセスにおける手順であり、その前段階で機器に対する脅威分析が実施されているという前提に立脚していることに留意する必要がある。具体的な脅威分析手法については別冊 1 や別冊 2 にて記載している。

- **準備**：契約締結に向けて、必要な情報の整理や検証目的の明確化を行う。検証サービス事業者は、依頼者の要望を踏まえて、見積もりを作成する。この際、見積もりの精度を上げるためにも、秘密保持契約（NDA）に基づき対象となる機器の機能仕様や提供される情報の一覧を受け取り、検証スコープについて検討・合意することが望ましい。見積もりに問題がなければ、検証について契約を締結する。
- **計画**：契約締結後、検証体制及び検証環境を構築する。また、検証の実施に向けた検証項目や検証手法の策定を行う。このために、検証依頼者は検証対象機器や必要情報を提供することが望ましい。また、検証を実施する前に、検証報告書の項目について二者間で確認しておくことが望ましい。このフェーズでは検証内容を合意するために二者間で定期的なコミュニケーション機会を設けることが望まれる。
- **検証実施**：検証依頼者の要望を踏まえ、表 2-1 で挙げられた項目等の検証を実施する。検証サービス事業者は、本検証で明らかになったリスクを適宜依頼者に報告することが望ましい。
- **分析**：検証サービス事業者は検証結果に基づき、特定・検出された脆弱性や詳細検証によって明らかになった脅威に対して、想定される影響や対応策の案を分析する。
- **報告**：検証サービス事業者は分析・整理された検証結果に基づき、検証報告書を作成する。この報告書は「計画」段階で作成した項目に基づき作成するが、必要に応じて項目の追加を行う。最後に、検証依頼者に対して、検証結果及び分析結果を報告する。必要に応じて、検証サービス事業者は報告会後にも事後対応を行う。

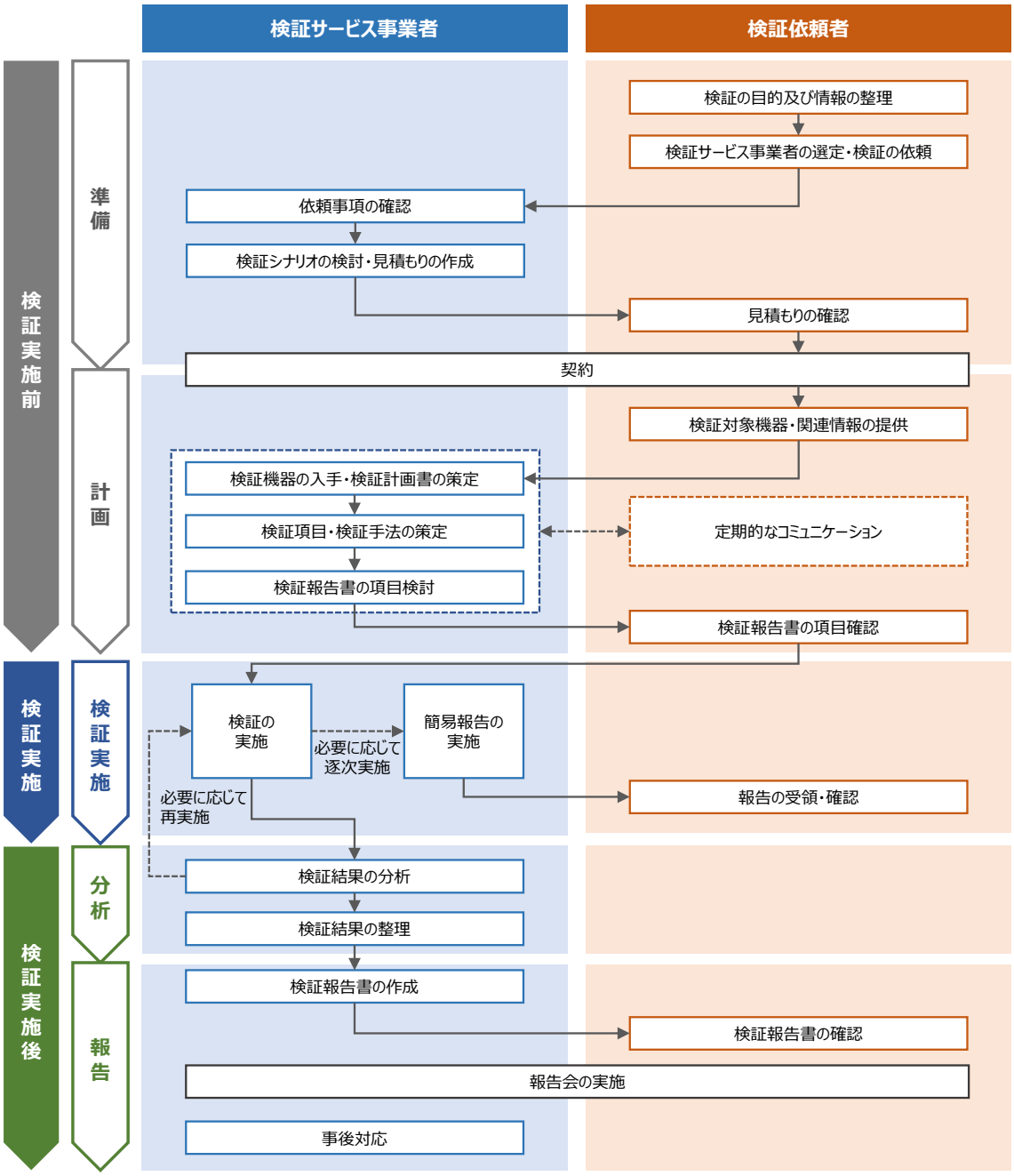


図 3-1 機器検証の実施手順

3.2 検証に向けた準備

検証サービス事業者が実施すべき事項

- 検証依頼者の要望、及び検証の目的・目標を確認し、依頼者の要望やコスト、スケジュールを踏まえ、説得力のある見積もりを作成する。必要に応じて、依頼者の要望や検証目標を確認するためのヒアリングを実施する。

- 検証依頼者との秘密保持契約、免責事項、禁止事項等を締結する。
- 機器の脆弱性が検出された場合の取扱いについて検証依頼者と合意する。
- 検証対象機器の機能仕様や提供される情報を踏まえ、検証スコープについて検討・合意することが望ましい。

検証依頼者が実施すべき事項

- 検証サービス事業者への依頼前に、検証目的、検証目標、想定コスト、検証結果の報告会の要否、及び想定するスケジュールをあらかじめ自組織内で検討する。自組織で検討した検証目的・目標等に加え、検証サービス事業者の信頼性を勘案し、検証サービス事業者を選定する。
- 検証対象機器のうち、検証を行う仕様及びファームウェアバージョンを決定する。
- 検証サービス事業者との秘密保持契約、免責事項、禁止事項等を締結する。
- 機器の脆弱性が検出された場合の取扱いについて検証サービス事業者と合意する。
- 検証希望時期が決まっている場合、自組織内での検討及び検証サービス事業者への依頼は可能な限り早期に実施することが望ましい。
- 検証機器に関する情報（脅威分析結果、設計書、ソースコード、関連アプリ等）の提供範囲を明確にし、当該機器に関する情報を検証サービス事業者に提示することが望ましい。

3.2.1 検証に向けた情報整理

上述のとおり、検証の目的や目標に応じて、検証スコープや検証手法は変化し、検証にかかるコストやスケジュールも変化する。一般的には、検証スコープと関連するサービスであっても、スコープに含まれていないサービスについては、検証は実施されない。ネットワークに常時接続する機器の場合、その機器が通信を行う通信先サーバが存在するため、そのサーバにおいても適切な対策がなされているかを確認することが望ましい。多くの機器が接続されている場合、サーバに侵入し掌握することに成功すれば、複数の機器に対して攻撃を行うことができるため、影響の深刻度の観点ではサーバのほうが高い。一方で、外部サーバにスキャンを行う場合、他のシステムや利用者に影響を及ぼす可能性があるほか、検証にかかるコストは機器自体の検証と比べて膨大なものとなる。同様にして、機器に関連するアプリケーションやファームウェアについても検証を行うかどうかで、検証手法は大きく変わり、それによって検証にかかる期間やコストが変動する。

検証手法や検証スコープを定めるために、検証依頼者は依頼段階において、検証目的、検証目標、想定コスト、検証結果の報告会の要否、及び想定するスケジュールをあらかじめ自組織内で検討し、検証サービス事業者に伝える必要がある。多くの場合の検証目標は、検証項目の網羅性は無いが最も重要な機能に対する対策の妥当性を検証すること、網羅性を担保した検証を行うことの大きく二つに分けられるが、依頼者はどちらの方針で検証を依頼したいかを検討する必要がある。この際、機器のうち守るべき資産が何かを整理することが有効である。機器そのもの、機器に含まれる機密情報、機器に接続されうる他の機器やシステム、機器内に含まれるアルゴリズム等、守るべき資産は依頼の背景によって変わるが、どの資産の優先順位が高いかを整理することが必要である。併せて、想定する攻撃者や脅威につ

いても整理することが望ましい。例えば、ルータに対して検証を行うとしたとき、インターネットからの侵入のみを脅威として扱うか、無線に対する接続を脅威として扱うか、物理的な破壊も考慮に入れるのかによって、検証手法や検証スコープは大きく変化する。また、どのバージョンの機器に対して検証を行うかを決定する必要がある。一つの機器で複数の仕様やファームウェアバージョンを有している場合があるが、異なる仕様やファームウェアの機器に対して検証を行う場合は、別の機器として扱われ、追加のコストや時間を要する可能性がある。そのため、どのファームウェアバージョンの機器に対して検証を行うかも事前に決める必要がある。

3.2.2 検証サービス事業者の選定・検証の依頼

検証依頼者は、検証手法や検証スコープがある程度定まった段階で、検証を依頼する検証サービス事業者を選定することになる。信頼性のある検証サービス事業者を選定すべきであるが、上述のとおり、検証サービス事業者の信頼性には、質の高い検証サービスを行うことができるというビジネスの信頼性、及び適切な情報管理等に基づきサービスを提供するという情報管理の観点での信頼性の二つが存在し、これらを勘案して適切な検証サービス事業者を選定すべきである。

（1） ビジネスの信頼性の観点

検証依頼者が、検証を依頼する段階において、検証サービス事業者のビジネスの信頼性を第三者的に確認・判断する基準としては、検証サービス事業者の実績、過去の依頼実績、事業者が有するツールや機器の充実度、サービスの柔軟性等が挙げられる。

検証サービス事業者における知識やスキルは一朝一夕に習得できるものではなく、検証の中で醸成され、暗黙知として蓄積されるものである。実績が多ければ、様々な検証依頼に対応できると考えられるが、過去の実施件数等の量的な実績だけでなく、個別の機器に対する検証実施等の質的な実績も重要な判断基準となる。例えば、自動車の車載機器に対して検証を依頼するとしたとき、過去に車載機器の検証を実施したことがある検証サービス事業者であれば信頼性は高い。自動車に関する検証実績がある事業者であれば、自動車に関する脆弱性やエントリポイントをある程度把握しているため、複数の観点に基づく検証実施が期待される。また、検証以外の開発等の実績があればなお良い。自動車の例でいえば、過去に開発に関わった人物が検証サービス事業者に在籍していれば、機器の扱い方を把握しているだけでなく、異なる視点からの検証を行うことができる。その他の実績としては、セキュリティコンテストやCTF（Capture the Flag）等のハッキングイベントでの受賞歴が挙げられる。受賞歴は、機器検証に対する知識やスキルを直接的に保証するものではないので、事業者を選定する際の判断基準とすることは難しいが、知識やスキルを有した事業者を評価する基準になりうる。

過去に依頼した検証サービス事業者がいる場合、その事業者に対して依頼することも一つの選定基準になりうる。過去の依頼を通じて、知識やスキルのレベルを把握しており、同様の依頼を行う場合には、信頼性をある程度保証した検証が期待できる。一方で、検証プロセスや手法が属人的になることには留意が必要である。第 2.1 節で示したとおり、検証サービス事業者は複数の視点を持つことが重要であるため、特定の検証サービス事業者や検証人材に依頼した場合、多角的な観点に基づいた検証がなされない可能性がある。知識やスキル、暗黙知等は、検証人材個人に紐づく部分が大きいため、特定の個

人に対する依頼も想定されるが、そのような状況においても、複数の視点から検証がなされるよう、依頼を工夫する必要がある。

また、検証サービス事業者が有するツールや機器、検証のための環境等も選定基準となりうる。特殊な検証を行うツールが必要な場合や、あらかじめ依頼者において使用するツールが決定している場合、そのツールを有した検証サービス事業者に依頼することになる。特に、ハードウェア解析等の高度な検証の場合、ツールや検証に用いる機器自体が高価なものが多く、所有している事業者は限定されるため、特殊なツールを用いた検証が必要となる場合には、当該ツールを所有している検証サービス事業者を選定する必要がある。また、事業者が有する検証環境も選定基準の一つとなりうる。無線通信に関する検証で電波暗室が必要な場合や、機器を安全に管理・稼働できる環境が必要な場合等、検証のために特殊な環境が必要な場合には、当該環境を用意できる事業者を選定する必要がある。

加えて、検証依頼者の想定するスケジュールに対して柔軟に対応できるかという観点も、検証サービス事業者の評価の際の基準となりうる。検証にかかる期間は検証目的や目標によって変わるものの、検証計画の策定や報告等、検証実施以外のフェーズに要する時間も踏まえると、短期間での実施依頼では十分な結果が得られない場合が多い。その一方で、限られた期間での検証依頼にならざるを得ないケースもあり、想定スケジュールでの実施が可能な検証サービス事業者が限られる場合もある。このような場合では、依頼者の想定する期間で対応できる検証サービス事業者を選定することが望ましい。なお、依頼にあたっては機器の開発ライフサイクルを踏まえ、適切な時期に検証を依頼する必要があり、機器の出荷直前での依頼は、問題が見つかったとしても十分な対応を行うことが困難なため、避けるべきである。限られた期間の中での依頼であっても、問題が見つかった場合の事態を想定し、適切なスケジュールのもと依頼を行う必要がある。

（2） 情報管理の信頼性の観点

検証においては検証依頼者の機密情報を検証サービス事業者に提供する場合がある。また、検証サービス事業者は検出された脆弱性情報を適切に管理・報告する必要がある。そのため、検証においては、ビジネスにおける信頼性だけではなく、情報管理の信頼性も、検証サービス事業者を選定する際には重要となる。ISMS 認証等の情報管理を保証する認証の取得有無によって、検証依頼者は一定の情報管理能力を確認することができる。特別な情報管理が必要な機器については、セキュリティルームの設置等、物理的領域の排他が想定されるが、このような情報管理の要望に対応できる事業者も選定基準の一つになりうる。最終的には、契約書において適切な情報管理に係る契約を締結する必要があるが、依頼の段階では検証サービス事業者での外注や再委託の有無を確認すべきである。機密情報や脆弱性情報の第三者への開示を防ぐという観点では、外注や再委託は実施しないことが好ましい。仮に実施する場合でも、検証サービス事業者は外注先や再委託先も含めた情報管理を徹底する必要があり、検証依頼者はどのような方針で管理がなされるかを確認することが望ましい。情報管理に対して懸念がある場合には、当該事業者への依頼は避けるべきである。

検証依頼者は、これらの信頼性の観点や検証目的及び目標、機器の特性等を総合的に勘案し、検証サービス事業者の選定・検証依頼を行うことが望ましい。

3.2.3 依頼事項の確認

検証依頼者から検証の依頼を受けた際、検証サービス事業者はまず依頼者の要望を確認する必要がある。この際、検証依頼者は、検証対象に関する情報をどこまで検証サービス事業者に提示できるかも明確にすることが望まれる。特に、機器の設計段階等で実施した脅威分析の結果やセキュリティ要求事項の検討結果を、検証サービス事業者に対して提示できるかを明確にする必要がある。機器に存在しうる脅威や脆弱性の確認にあたっては、検証前に実施された脅威分析の結果やセキュリティ要求事項の検討結果を活用することが効果的である。そのため、これらの情報を検証サービス事業者に提示することで、検証にかかるコストを低減することができる。脅威分析が実施されていない場合、必要に応じて、簡易的な脅威分析を行い、その結果を検証に活用することが望まれる。簡易的な脅威分析を検証サービス事業者に依頼する場合、契約の前段階で検証サービス事業者に伝えておく必要がある。また、検証依頼者が機器に関するソースコードや設計書の情報を提供できるかに応じて、実施する検証手法が変わる場合があるほか、機器の動作に関連するスマートフォンのアプリ等が存在する場合、当該アプリを検証サービス事業者が入手できるかによって、検証手法及び検証の精度が大きく変化する。検証依頼者はこれらの情報を検証サービス事業者に提示できるかどうかを自組織内で事前に確認することが望まれる。

検証には可能な限り多くの情報を活用することが望ましいが、検証機器に関する情報は機密情報であることが一般的なため、二者間で秘密保持契約を締結し、製品に関する情報や脆弱性情報を厳格に管理する。

3.2.4 見積もりの作成・契約締結

検証サービス事業者は、依頼者の要望やコスト、スケジュールを踏まえ、見積もりを作成する。必要に応じて、依頼者の要望や検証目標を確認するためのヒアリングを実施することが望まれる。また、機器に関する情報を踏まえ、この段階で検証に必要となる工数見込みを検討するとともに、検証スコープについて検証依頼者と合意することが必要である。

検証に向けた十分な時間や費用があり、精緻な見積もりを作成する必要があるものの、依頼者による検証依頼が曖昧で適切な見積もりを作成することが困難な場合、検証対象機器や関連機器に関する公開情報を収集し、どのようなサービスが稼働しているか、関連機器について既に報告されている脆弱性が無いか等を事前に確認することが望ましい。また、機器が入手可能である場合、この段階で簡易な事前調査（ポートの空き状況の確認、インタフェース有無の確認 等）を実施することが望ましい。これらにより、機器検証に必要な項目を絞り込めるだけではなく、機器の特性を把握することができるため、精度の高い説得力のある見積もりが可能となる。

契約締結の前段階で、機器の脆弱性が検出された場合の取扱いについて二者で合意することが望まれる。検証サービス事業者が脆弱性を発見した場合、検証がすべて完了していなくても早急に報告することが望ましいが、機器の特性や検証期間によっては、すべての脆弱性情報を逐次報告することは困難な場合もある。逐次的な報告は、発見された脆弱性に関する簡易報告であり、その脆弱性に関するすべての情報を報告する必要はない。脆弱性評価の基準を事前に二者間で定め、それに基づきどの脆弱

性を逐次報告の対象とするかを二者間で合意しておくことが望まれる。脆弱性評価の基準の例として表3-1 のような基準や CVSS v3 等既存の評価システム[7]が挙げられる。例えば、「緊急」又は「重大」の脆弱性が検出された場合には逐次的に報告する、等を事前に二者間で合意しておくことが望ましい。

表 3-1 脆弱性評価基準の例

レベル名	概要	具体例
緊急	脆弱性が悪用されることで、当該機器を介して組織内ネットワークに侵入可能など、機器の侵害のみならず多大な影響が発生する場合。	• リモートから任意のコードが実行可能
重大	脆弱性が悪用されることで、複数の情報が窃取されるなど、機器運用に多大な影響が発生する場合。	• リモートから認証情報を窃取可能 • アクセス制御を回避可能
警告	脆弱性が悪用されることで、一部の情報が窃取される、悪用された場合に一部の損失が発生する場合など、機器運用に影響が発生する場合。あるいは、「重大」レベルと同程度の影響が引き起こされるが、複雑な前提条件を必要とする場合。	• ブルートフォース攻撃等により認証情報を窃取可能 • 通信内容を傍受・改ざん可能
注意	当該の脅威単体では影響が発生しないが、組み合わされることで「警告」レベル以上の影響に繋がりかねない場合。	• 弱い暗号スイートの使用 • 設定情報が窃取可能
情報	脆弱性が悪用されることで、不適切な実装がなされている、不要な機能が含まれている等、依頼者に伝えておくべき情報が発見された場合。	• 過度な頻度での死活監視機能

検証依頼者は作成された見積もりを確認し、問題がなければ契約を締結する。また、検証における禁止事項や免責事項が存在する場合、二者間でこれについて合意しておく必要がある。禁止事項の例として、検証機器の破壊が挙げられる。攻撃者の視点では、機器を破壊しないという制約は無いため、検証においても機器が壊れる前提での実施が望ましい。一方で、機器自体が高価である場合や、実環境において検証を実施する場合等、機器を破壊することを禁止する場合もある。また、免責事項の例として、通信先サーバへの影響が挙げられる。上述のとおり、ネットワークに常時接続する機器の場合、その機器が通信を行う通信先サーバが存在するが、このサーバが既に運用されている場合、検証によって悪影響を及ぼす可能性もあり、検証環境と実運用環境を分離して検証を実施するべきである。分離が難しい場合、サーバに対する検証を禁じ、機器のみに検証を行うこととなるが、検証の影響が運用されているサーバへと波及する恐れもある。影響が波及した場合に責任を負わないこととする場合、免責事項として明

[7] IPA 共通脆弱性評価システム CVSS v3 概説 https://www.ipa.go.jp/security/vuln/CVSSv3.html

示することが必要である。

3.3 検証計画の策定

検証サービス事業者が実施すべき事項

- 契約締結後に、検証依頼者とのキックオフミーティング等を開催する。また、二者間の連絡体制を明確化し、検証内容を合意するために定期的なコミュニケーション機会を設ける。
- 機器のデータ入出力やインタフェース、通信プロトコルの特性等、検証対象機器の特性を確認する。
- 脅威分析の結果等を踏まえ、機器に存在しうる脅威や脆弱性を確認する。
- 検証にかかるコストやスケジュールを踏まえ、検証項目及び検証手法を決定する。優先順位を踏まえ、検証しない項目が存在する場合には、事前に検証依頼者に伝える。
- 検証体制及び検証環境を構築する。検証体制の構築にあたっては、検証人材の得意分野が相互に補われる形で体制を構築することが望ましい。
- 検証実施前に検証依頼者との打合せの場を設け、検証計画に問題ないかを確認する。このタイミングで、検証計画だけではなく、最終的な検証報告書の作成方針についても二者間である程度合意を取る。

検証依頼者が実施すべき事項

- 契約締結後に、検証サービス事業者とのキックオフミーティング等を開催する。また、二者間の連絡体制を明確化し、検証内容を合意するために定期的なコミュニケーション機会を設ける。連絡体制の構築においては、機器の仕様や特性を理解した担当者を含めることが望ましい。
- 機器が停止・故障する可能性を踏まえ、工場出荷時への復元方法等を検証サービス事業者に提示する。
- 検証サービス事業者が検証を実施する前に打合せの場を設け、検証計画に問題ないかを確認する。このタイミングで、検証計画だけではなく、最終的な検証報告書の作成方針についても確認を行う。

契約が締結された段階でキックオフミーティング等を開催し、考えをすりあわせる機会を設けることが望ましい。併せて、二者間の連絡体制を明確化し、検証内容を合意するまで定期的なコミュニケーション機会を設けることが望まれる。検証サービス事業者が、検証依頼者に対して検証対象機器に関する情報や機器の構成を確認することが発生するため、連絡体制の構築にあたっては、検証依頼者は検証対象機器の仕様や特性を理解している担当者を体制に含めることが望ましい。仕様を理解している担当者を含めない場合、情報確認に時間を要する場合もあり、実際の検証に十分な時間をかけることができない可能性がある。

3.3.1 検証機器の入手・検証計画書の策定

契約締結後、検証サービス事業者は検証対象機器を入手するとともに、検証実施に向けた計画を立て、検証計画書を策定する必要がある。機器の入手について、一般的には依頼者であるメーカから検証対象機器が提供される。なお、機器が壊れる前提での実施が望ましく、一部を破壊することを前提とした複数台の入手や、代替機との交換手順等を検証依頼者と相談することが望まれる。また、検証によって機器が停止・故障する可能性を踏まえ、工場出荷時への復元方法等を確認する必要がある。

検証計画書について、計画書内に含むべき項目例としては表 3-2 のとおりであり、それぞれの項目について検証実施前に検討する必要がある。検証項目や検証手法の策定は、脅威分析の結果やセキュリティ要求事項の検討結果に基づき実施することが効果的である。策定方法は次項で記載する。

表 3-2 検証計画書の項目例

項目	記載内容
検証目的	検証の目的について記載する。
検証期間	検証を実施する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記載する。これには、製品名、メーカ、製造年月、シリアルナンバー・機器番号及びファームウェアバージョンを含める必要がある。
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を記載する。
使用ツール	検証に使用するツールの名称及びバージョンを記載する。
禁止事項	検証にあたっての禁止事項を記載する。
連絡体制	検証依頼者側の担当者、コミュニケーション手段、報告を行う条件等を記載する。
脆弱性の取扱	脆弱性が検出された場合の取扱方針について記載する。
既知情報	検証機器の設計図、関連機器において既に報告されている脆弱性等、検証にあたって活用可能となる既知の情報を整理する。
想定される脅威	機器に想定される脅威を分析し、記載する。
検証項目	想定される脅威や脆弱性の存在を確認するための検証項目を記載する。
検証手法	実施する検証手法（既知脆弱性の診断等）の項目を記載する。
検証体制・役割分担	検証を実施する際の体制と、その中での役割分担を記載する。ここでは、責任範囲も明確にすることが必要である。検証スケジュールと対応付けて、進捗を把握できる状態が望ましい。

3.3.2 検証項目・検証手法の策定

検証の目的は、第一に機器に脆弱性が内在しないことを確認すること、第二に脆弱性が存在した場合に対策や緩和策等の適切なセキュリティ要求が施されていることを確認することにある。このフェーズにお

いてはまず、機器のデータ入出力、インタフェース、及び通信プロトコルの特性を踏まえ、機器に存在しうる脅威や脆弱性を確認する。機器に存在しうる脅威や脆弱性の確認にあたっては、検証前に実施された脅威分析の結果やセキュリティ要求事項の検討結果を活用することが効果的である。機器全般に存在する代表的な脅威としては、情報漏えい、通信の盗聴・改ざん、第三者による不正アクセス、及びマルウェア感染が挙げられる。これらの脅威に起因する代表的な脆弱性としては以下が挙げられる。

- **アクセス制御の不備**：機器内に保存されている情報について、権限の無い第三者がアクセス可能な状態。Android アプリの脆弱性に関するレポートでは、Android アプリの脆弱性のうち 7 割がアクセス制限の不備であったことが報告されている[8]。
- **入力検証の不備**：第三者が正常でない情報を入力し、機器の挙動を意図的に操作することができる状態。主に機器に付随する Web コンソールに対する脆弱性である。
- **不要通信の設定**：本来意図していない接続先に対して、機器の機密情報を送信してしまう状態。機器が不要通信を行っていることは、利用者に公開されていない場合がある。
- **通信暗号化機能の欠如**：適切な暗号化設定が行われていないことで、通信の内容が第三者によって盗聴・改ざんできてしまう状態。
- **不要サービス・ポートの開放**：本来使用しないサービスやポートが開放している状態。2016 年に世界中で猛威をふるった IoT 機器に対するマルウェアである Mirai は、telnet サービスを悪用して感染を拡大したが、一部機器では telnet サービスが開放されていることは利用者に公開されていなかった。
- **認証情報管理の不備**：ログイン ID/パスワードの認証情報がプログラム等に埋め込まれているハードコーディングの状態等、認証情報が適切に管理されていない状態。利用者によるパスワード変更ができない場合もあり、上述の Mirai はこの脆弱性を悪用し、典型的なユーザ名とパスワードを用いて IoT 機器へログインの試行をした。
- **認証設定の不備**：不正な機器や不正な利用者が、正規の機器や利用者をそれぞれなりすますことができる状態。
- **ファームウェアの検証不備**：ファームウェアが検証されずに機器で更新される状態。これにより攻撃者がファームウェアに不正なプログラム等を混入し、機器に挿入することが可能となる。
- **不適切なデータ処理**：プログラムのデータ処理の不備によって、オーバーフローや不適切なメモリ処理が発生する状態。これにより、機器がサービス不能の状態に陥る可能性があるほか、権限が乗っ取られる可能性もある。

機器に存在しうる脅威や機器が満たすべきセキュリティ要求事項を踏まえ、検証項目及び検証手法を策定する。ここで、機器に存在しうるすべての脅威や脆弱性に対して検証を行うことは現実的ではなく、検証項目の絞り込みを行う必要がある。脅威分析の段階で、DREAD 等に基づき脅威のスコアリングを行った場合、優先的に検証すべき項目を定量的に選定することができる。そうでない場合でも、以下の観

[8] IPA, IPA テクニカルウォッチ「Android アプリの脆弱性」に関するレポート https://www.ipa.go.jp/files/000024744.pdf

点等を参考に、脅威を評価し、検証する項目の優先度を決定することが望まれる。

- **脅威が与える影響の種類**：脅威が機器に対してどのような影響を与えるかを考慮する。これは機器の特性にも依存するものである。脅威が顕在化した場合でも、発生する影響が限定的である場合はその優先度は低いが、攻撃によって個人情報の漏えいや利用者の損害等に結びつく脅威は優先度が高い。その中でも、人命に影響を及ぼすような脅威や重症を与えかねない脅威については特に優先度が高い。
- **前提条件の有無**：現実的でない前提条件を必要とする脅威の場合、その脅威に関する検証の優先度は低い。一方で、前提条件を必要としない脅威については、検証の優先度が高い。
- **攻撃の容易性**：特殊技能や特殊な知識を必要とする脅威の場合、脅威が実行されるリスクは低く、検証の優先度も低い。一方で、このような技能や知識を必要とせず比較的容易に実行される脅威については、検証の優先度が高い。
- **脅威の受動性・能動性**：攻撃者以外の操作を要する受動的な攻撃の場合、攻撃者のみで脅威が完結する能動的な攻撃に比べて、攻撃が成立するリスクが小さいため、検証の優先度は低い。
- **脅威の直接的影響・間接的影響**：脅威の発生によって及ぼされる影響が直接的な場合、優先度は高い。一方、単独の脅威では重大事に至らないと考えられる等、その影響が間接的な場合、検証の優先度は低い。

例えば、通信経路上での盗聴が優先度の高い脅威として考えられる場合、第三者により通信内容が窃取できるかどうかをネットワークスキャンによって検証することが望まれる。機器に対する既知の脆弱性を悪用した攻撃が優先度の高い脅威として考えられる場合、既知脆弱性の診断を実施することが望まれる。脅威分析の結果やセキュリティ要求事項の検討結果に基づく検証項目・検証手法の策定方法については、別紙 1 及び別紙 2 にてネットワークカメラを対象とした例を示しているので、併せて参照いただきたい。なお、検証項目の優先度決定により、検証しない項目が存在する場合、検証しない理由を検証依頼者に伝えることが望ましい。

検証項目及び検証手法の策定後、又は並行して、検証体制及び検証環境を構築する。構築すべき検証体制は依頼者の要望や対象機器、コストによって変化するものの、専門性や適切な資格を有した人物を含めることが望まれる。上述のとおり、検証の知識やスキル、暗黙知等は、検証人材個人に紐づく部分が大きく、それぞれの検証人材に得意分野が存在するため、得意分野を相互に補われる形で体制を構築することが望まれる。また、資格の例として、情報セキュリティサービス審査登録制度における「脆弱性診断サービス」に係る審査基準[9]や日本セキュリティオペレーション事業者協議会（ISOG-J）及び OWASP Japan による「脆弱性診断士」[10]の要件等が挙げられる。また、検証体制の構築にあた

[9] 経済産業省、情報セキュリティサービス審査登録制度 情報セキュリティサービス基準
https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf
[10] ISOG-J 及び OWASP Japan、脆弱性診断士スキルマッププロジェクト
https://www.owasp.org/index.php/Pentester_Skillmap_Project_JP

っては、検証結果の再現性も考慮する必要がある。検証で得られた結果が後日でも再現できるように、検証手順、通信パケット、ログ、検証結果の画面キャプチャ等を保存しておくことは不可欠であるが、検証自体を二つのグループに分けて実施することも再現性を確保する方法の一つである。

3.3.3 検証報告書の項目検討

検証実施前に検証サービス事業者と検証依頼者の二者による打合せ等の機会を設け、検証計画に問題が無いかを確認することが望ましい。このタイミングでは、検証計画だけではなく、最終的な報告書の作成方針についても二者間である程度合意を取ることが望ましい。検証報告書に含めるべき項目例を表 3-3 に示すが、どのような項目を報告書に含めるか、ある程度二者間で方針を決めておくことが望ましい。報告書作成の際の留意点等は第 4 章で示す。

表 3-3 検証報告書の項目例

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、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を記載する。
	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	検証を行うにあ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。

大項目	項目	記載内容
	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。

3.4 検証実施

検証サービス事業者が実施すべき事項

- 自動化ツールで得られた脆弱性の結果が、機器の機能や運用にどのように影響を与えるか、攻撃シナリオにどのように寄与するか等を分析する。また、自動化ツールを活用した脆弱性の特定を行いつつ、自動化ツールでは検証が難しい脆弱性の検証については手動での検証を実施することが望ましい。
- 使用するツールについて、検証目的・目標や検証にかかるコスト・期間、機器の特性等を踏まえ、適切なツールを採用する。
- 攻撃者の視点に立ち、検証を行う。検出された脆弱性は攻撃の手段の一つに過ぎず、検出された脆弱性を悪用することで、機器に対してどのような影響が与えられるかを分析する。
- 既知脆弱性の診断やネットワークスキャンにおいては、自動化ツールが出力した脆弱性の根本原因を手動で解析する等によって、脆弱性の「誤検知」を減らすことが望まれる。また、複数の視点からの検証を行うことにより脆弱性の「見逃し」を減らすことが望まれる。
- バイナリ解析等の高度な検証の実施前に、ファジング等で怪しいと思われる点を事前に推察し、効率的に検証を実施することが望まれる。

検証サービス事業者と検証依頼者の二者による打合せ等により、検証計画及び検証報告書の記載方針について合意を取った後、検証サービス事業者は実際に機器に対して検証を開始する。

本項では、表 2-1 に示した一般的な機器検証手法毎に、検証において実施すべき項目や持つべきスキル、知識等を記載する。多くの検証手法においては自動化されたツールが広く活用できるものの、手動による検証も効果的である場合が多い。検証にかかるコストにも依存するが、自動化ツールを活用した脆弱性の特定を行いつつ、その結果を踏まえて手動での検証を実施することが望ましい。また、検証サービス事業者は、既に提供しているサービスを組み合わせて検証手法を選択することも可能となる。IoT 機器の場合、ネットワークとの常時接続を行うことが多いため、ネットワークに関する検証を実施する際には、既存のネットワーク検証サービスが活用できる場合がある。同様に、機器の動作に関連するスマートフォンのアプリが存在し、アプリに対する検証サービスを既に提供している場合には、このサービスと組み合わせた

検証実施が想定される。

なお、動的検証手法については、それぞれの手法の詳細手順を記載した別冊 1 の該当箇所を示している。また、各手法を機器メーカが依頼する際に機器メーカとして実施すべき事項や、各検証手法の結果を踏まえて機器メーカにて実施すべき対応についても記載してした別冊 2 の該当箇所も示している。本編記載の内容だけでなく、それぞれの別冊の記載箇所も併せて確認されたい。

3.4.1 設計文書レビュー

脆弱性評価や検証は機器の特性を踏まえて実施されるため、効率的な検証の実施のために、機器の設計書を確認することが望ましい。特に IoT 機器の場合、その用途は多岐にわたり、機器構成も様々であるため、設計書が無いと機器の動作原理が分からない場合もある。そのため、検証依頼者は、著作権の観点から設計書を検証サービス事業者に提示できない場合でも、機器がどのような機能を有しているのか、どのような通信を行うのか、そしてどのような情報が格納されているかを検証サービス事業者に伝えることが望ましい。

設計書をレビューすることで確認できる項目としては、不要なサービスやアプリケーションの存在、不適切な認証情報の管理、暗号化方式の妥当性、不適切なログ設定やバックアップ設定等が挙げられる。設計書レビューにおいて直接的な脆弱性が見つかることは限定的であるが、脆弱性に繋がりうるセキュリティの欠如が明らかになる可能性がある。また、設計文書レビューは、機器開発着手前に実施可能な検証であり、むしろこのタイミングでの実施が最も望まれる。セキュリティ仕様について十分に検討が行われていない機器の場合、開発が進んでからセキュリティの懸念事項が明らかになったとしても、その修正には大幅なコストや時間を要することとなる。開発着手前にレビューを実施することで、セキュリティ設計不備による開発プロセスの遅れや修正にかかるコストを最小限にすることができる。検証段階で設計文書レビューを行う場合でも、検証実施の前段階で検証対象機器の特性等を確認するために実施することが望まれる。

設計書レビューは人の目によって確認されるため、結果の判断が主観的となる。依頼者に対して客観的な結果を報告するためには、複数人によるレビューを実施することが望ましく、適切な根拠に基づきレビューを行うことが望まれる。IoT 機器の場合、ネットワークに常時接続されるため、複数のネットワークサービスが搭載されるが、意図する目的に基づき開放されており、適切な認証メカニズムが設定されている場合は不要なサービスとは判定できない。機器の運用方法や背景を踏まえたレビューの実施が望まれる。

3.4.2 ソースコード解析

検証サービス事業者は、検証依頼者からソースコードを受領した場合、機器の特性をソースコードから確認するだけではなく、脆弱性が含まれていないかを静的に解析することが望まれる。ソースコード解析では、自動化ツールを活用してソースコードに含まれる特定のパターンを抽出することで、脆弱性を検出する。検出できる代表的な脆弱性として、「入力検証の不備」や「不適切なデータ処理」の脆弱性のほか、間接的に悪用されうる潜在的な脆弱性も検出可能である。ソースコード解析による効果として脆弱性の低減が期待できるほか、形式手法やモデル検査等の高度な論理的解析手法を併用することで、品質の向上も期待できる。また、これら解析の多くは、解析対象のスケーラビリティが高く、ソースコードが大規模な

ものであっても、解析可能であるという特徴を有する。

ほとんどのソースコード解析ツールは自動化されており、一部のツールでは関数間のすべてのパスを自動実行して網羅的な解析を行うため、結果を得ること自体は難しくない。一方で、脆弱性スキャンと同様に、「誤検知」をどのように減らすかが重要となる。誤検知について、代表的なツールにおいても 15~35%程度の誤検知率であることが知られている[11]。また、ソースコード解析においては、ツールが指摘した事項は正しい検出結果であるものの、ソースコードの修正は必要ないという「過検知」をどう扱うかも重要な観点である。これらを減らす取り組みとして、二種類以上のツールを活用した解析の実施等が挙げられるが、最も重要となるのが、自動化ツールが出した結果を人の目で確認し、脆弱性であるかを判断することである。そのため、解析結果を判定する人材においては、代表的な脆弱性に関する知見だけではなく、どのようなソースコード原理で脆弱性が生じうるかについて理解する必要がある。

一方で、ソースコードは検証依頼者の著作物であり機密情報でもある。また、一般的にはソースコード解析ツールは高価であり、誤検知や見逃しを減らすために人の目で確認する時間も含めると、解析にかかる工数は少なくない。ソースコード解析に関する IPA のレポート[12]においては、10 年以上に及び利用される可能性がある機器、セキュリティパッチの適用やソフトウェアの更新が困難な機器、サイバー攻撃を受けることで人命に影響を与えかねない機器、そしてサイバー攻撃を受けることで金銭被害を受ける可能性のある機器については、ソースコード解析は避けて通れないとしており、これらに関連する機器についてはソースコード解析の実施が望まれる。その他の機器については、検証目的・目標や検証にかかるコスト・期間、機器の特性等を踏まえて、ソースコード解析の実施要否を決定することが望まれる。

3.4.3 ファームウェア解析

ファームウェアとは、機器の機能を制御するために ROM やフラッシュメモリ等に書き込まれるプログラムの総称であるが、近年では、サイバー攻撃の主要エントリポイントの一つとなりつつある。これは、OS やソフトウェア等に比べてファームウェアのセキュリティが軽視される傾向があり、それ故に多くの脆弱性が見過ごされていることに起因する。事実、Information Systems Audit and Control Association (ISACA) による 750 社を対象とした調査によれば、8%の企業のみがファームウェア関連の脆弱性に対して十分な準備を施していると回答した[13]。機器ファームウェアの脆弱性に関する調査としては、米国の非営利組織 American Consumer Institute (ACI) が、米国で販売されている 14 社の Wi-Fi ルータ 186 機種のファームウェアを調査し、そのうち 83%の 155 機種のファームウェアが脆弱性を有していることを特定した[14]。このようにファームウェアセキュリティが軽視されている状況にあるが、ファームウェアに起因した脅威

---

[11] 古賀国秀、山元和子、ソースコード静的解析技術 https://www.toshiba.co.jp/tech/review/2009/04/64_04pdf/b05.pdf

[12] IPA, IPA テクニカルウォッチ「ソースコードセキュリティ検査」に関するレポート https://www.ipa.go.jp/files/000009378.pdf

[13] ISACA, Firmware Security Risks and Mitigation: Enterprise Practices and Challenges http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/firmware-security-risks-and-mitigation.aspx

[14] ACI, Securing IoT Devices: How Safe Is Your Wi-Fi Router? https://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf

も数多く報告されており、機器全体のセキュリティ確保のためにも、ファームウェアの脆弱性有無を確認することは重要なプロセスとなる。

多くの場合、機器から対象のファームウェアを取得することは容易ではない。そのため、ファームウェア解析を行う場合には、検証すべきファームウェアファイルを依頼者が提供することが望ましい。ファームウェアを検証サービス事業者が自ら抽出する場合、多くの機器において、本体を分解後、UART（Universal Asynchronous Receiver/Transmitter）端子や JTAG（Joint Test Action Group）端子等のシリアル通信端子にアクセスしてチップ内に格納されているファームウェアを抽出する必要がある。そのため、電子回路に関する知識や抽出のためのツールを使いこなすスキルが必要となる。

近年では、クラウドプラットフォームを活用した自動解析ツールも登場している。これは、ファームウェアファイルをクラウド上にアップロードすることで、自動で脆弱性の検証を実施するツールである。この場合、自動解析ツールで得られたファームウェア脆弱性の結果が、機器の機能や運用にどのように影響を与えるか、攻撃シナリオにどのように寄与するか等を分析することが重要となる。

なお、ファームウェア解析技術に関する具体的な手法等を別冊 1 の第 4.3 節に示す。また、検証依頼者である機器メーカの立場から、ファームウェア解析依頼時に知るべき留意点を別冊 2 の第 4.2 節、ファームウェア解析の結果を踏まえた対応方針を第 5.3 節に記載する。

検証サービス事業者向け：
ファームウェア解析に関する具体的な手法等：別冊 1 第 4.3 節

検証依頼者（機器メーカ）者向け：
ファームウェア解析の検証依頼時に知るべき留意点：別冊 2 第 4.2 節
ファームウェア解析の結果を踏まえた対応方針：別冊 2 第 5.3 節

3.4.4 バイナリ解析

一般的にバイナリ解析とは、機械語の実行ファイルを、人間が解読可能な高級プログラミング言語に逆コンパイル、又はアセンブリ言語に逆アセンブルし、それらを静的解析する手法である。ファームウェアも一種のバイナリファイルであるため、ファームウェアを静的に解析することをバイナリ解析と呼ぶことも多い。近年では、実行ファイルだけではなく、マルウェアを逆コンパイルし、その挙動を解析する手法もバイナリ解析と呼ばれることがある。セキュリティの観点では、バイナリ解析によって、既知脆弱性の診断等では検出が難しい外部ライブラリに依存した脆弱性や悪意あるコードに起因する脆弱性の検出が期待される。特に、ファームウェアには実行するサービスのバイナリコードや初期設定パスワード、証明書等、検証において有益な情報が含まれている場合が多く、ファームウェアをバイナリ解析することで、他の検証手法を実施するより効率的に脆弱性を発見できる場合もある。効率的な解析のためには、検証人材のスキルだけではなく広範な知識も必要となるため、ファームウェアに起因した脆弱性に関する知見も有していることが望ましい。

バイナリ解析の実施要否は、検証依頼者から対象機器のソースコードの入手可否に依存する。これは、逆コンパイラの精度は 100%ではないためであり、ソースコードが検証依頼者から受領できる場合は、そ

のソースコードをレビューし、解析を行うことが望ましい。一方で、ソースコードを検証サービス事業者に与えること無く、バイナリ解析を行う場合、検証依頼者は自社が著作権を有するソースコードを他者に晒すこと無く解析を依頼できるという特徴がある。ただし、バイナリ解析の実施についてソフトウェア利用許諾契約（EULA）等にて禁止されている場合もある。バイナリ解析を実施する場合、ソフトウェア利用許諾契約等を確認した上で、事前に検証依頼者と合意することが望まれる。

バイナリ解析の際に使用するツールとして、逆コンパイルを行い、実行パスを可視化するツールは複数存在するが、解析自体を自動で行うツールはほとんど無く、検出の精度は検証人材のスキルに大きく依存する。得られたアセンブリ言語を網羅的に解析することが望まれるが、コストを踏まえるとすべてのプログラム実行パスを確認することは現実的に不可能である。そのため、怪しいと思われる箇所を推察し、効率的に検証を実施する必要がある。効率的なバイナリ解析を実施するためには、ファジング等で怪しい兆候を事前に把握し、それに関連しそうな箇所を分析することが望まれる。また、検証人材には、アセンブリ言語に関する知識だけではなく、CPU 命令に関する知識や OS のメモリ管理に関する知識等、広範な知識が必要となる。加えて、バイナリ解析やソースコードレビュー等の静的解析に共通する点であるが、構文を読み解くスキルも必要となる。検証人材は十分な知識やスキルを有した上で、効率的に検証・解析を実施することが望まれる。

なお、バイナリ解析技術に関する具体的な手法等を別冊 1 の第 4.4 節に示す。また、検証依頼者である機器メーカの立場から、バイナリ解析の検証依頼時に知るべき留意点を別冊 2 の第 4.3 節、バイナリ解析の検証結果を踏まえた対応方針を第 5.4 節に記載する。

検証サービス事業者向け：
バイナリ解析に関する具体的な手法等：別冊 1 第 4.4 節

検証依頼者（機器メーカ）者向け：
バイナリ解析の検証依頼時に知るべき留意点：別冊 2 第 4.3 節
バイナリ解析の検証結果を踏まえた対応方針：別冊 2 第 5.4 節

3.4.5 ネットワークスキャン

マルウェア Mirai では、23/TCP 及び 2323/TCP の telnet サービスを悪用され感染を拡大した。また、近年では、機器の管理用インタフェースを提供する Web サーバが動作する 80/TCP 及び 8080/TCP を狙った攻撃が増加している。本来閉塞すべきポートが開放されている場合、そのポートがバックドアとなり、外部の攻撃者からの侵入を許す可能性がある。このために、ネットワークスキャンを実施し、機器におけるアクティブなサービスやポートを識別するとともに、不要なサービスやポートについては適切な対策が施されていることを確認する。

多くのネットワークスキャンツールは、一般的なポート番号とサービスを自動でスキャンしリストアップすることが可能である。これに加え、機器の OS を特定できる場合があるため、機器に関する情報がほとんどない段階でネットワークスキャンを行うことは有益である。どのサービスやポートが開放されているかは比較的容

易に把握することができる一方で、それらのサービスやポートが適切な目的で開放されているかを判断する必要がある。また、スキャンの結果、開放しているポートやサービスが検出された場合でも、問題があることを裏付けるものではなく、実際に悪用できるまでの仮説として扱う必要がある。例えば、スキャンによって 23/TCP の telnet や 80/TCP の HTTP サービスが検出されることは一般的であるが、意図する目的に基づき開放されており、適切な認証メカニズムが設定されている場合は脆弱性とは認められない。それらのサービスに対して安易な認証情報によってアクセスできる等の試行が成功した場合にはじめて脆弱性として判断される。また、独自のポートやサービスが開放されている場合、それ自体が潜在的な脆弱性になりうることに留意する。これは、特定の独自ポートやサービスが開放していることが、何らかの方法によって悪意ある第三者に明らかになった場合、当該機器であることが第三者に特定される可能性があり、ポートやサービスの情報を悪用した攻撃に繋がりうるためである。検証サービス事業者は、機器の運用状況を踏まえ、スキャン結果が攻撃シナリオにどのように寄与するかを明確化し、検証依頼者に提示する必要がある。

なお、ネットワークスキャン技術に関する具体的な手法等を別冊 1 の第 4.5 節に示す。また、検証依頼者である機器メーカの立場から、ネットワークスキャンの検証依頼時に知るべき留意点を別冊 2 の第 4.4 節、ネットワークスキャンの検証結果を踏まえた対応方針を第 5.5 節に記載する。

検証サービス事業者向け：
ネットワークスキャンに関する具体的な手法等：別冊 1 第 4.5 節

検証依頼者（機器メーカ）者向け：
ネットワークスキャンの検証依頼時に知るべき留意点：別冊 2 第 4.4 節
ネットワークスキャンの検証結果を踏まえた対応方針：別冊 2 第 5.5 節

3.4.6 既知脆弱性の診断

既知の脆弱性が機器に内在しうるかを調べ、実際に悪用可能かを確認する。既知脆弱性の有無の確認は、脆弱性スキャンツールを活用することで効率的に実施することができる。また、脆弱性のスキャンは、機器本体だけでなく、機器に関連する Web コンソールやサービスについても調査することが望ましい。既知の脆弱性に基づいて検証を行うため、検証に用いる脆弱性情報が最新であることが必要である。多くの脆弱性スキャンツールはネットワークスキャンも兼ねており、脆弱性だけでなく、サービスやポートについても特定・検出できる。また、多くのツールは、脆弱性スキャンを自動で行うことができ、スキャン結果を視覚的に整理するため、結果を得ることは難しくない。また、他の検証手法に脆弱性スキャンで得られた結果を活用することもできるため、作業全体の効率化の観点でも自動化ツールは有益である。一方で、自動化ツールでは検出が難しい脆弱性も存在する。例えば、検出するまでにいくつかのプロセスを経由する必要がある場合の脆弱性やアクセス制御の不備に関する脆弱性等は自動化ツールでの検出が難しい。それぞれの特徴を踏まえ、自動化ツールと手動による解析を組み合わせた脆弱性スキャンが望まれる。

機器に内在しうる代表的な脆弱性の例を表 3-4 に示す。

表 3-4 機器に内在しうる代表的な脆弱性

項目	代表的な脆弱性	概要・脆弱性が悪用された場合の影響	対応するCWE
アクセス制御の不備	適切でない権限管理	特定の権限を必要とする機能やファイルに、許可されていない利用者がアクセス可能となる脆弱性。	269
	最小権限の原則の違反	最小権限の原則が守られておらず、許可されていない権限が付与されている脆弱性。	272
	適切でない認可	本来アクセスできない機能やファイルに、許可されていない利用者がアクセス可能となる脆弱性。	285
	デフォルトアクセス設定の不備	機能やファイルのデフォルトアクセス設定が適切に設定されておらず、許可されていない利用者がアクセス可能となる脆弱性。	276
入力検証の不備	クロスサイトスクリプティング	機器に付随するWebコンソールにおいて、不正なスクリプトが実行可能となる脆弱性。	79
	OS コマンドインジェクション	機器に付随するWebコンソールにおいて、不正なOSコマンドが実行可能となる脆弱性。	75
通信暗号化機能の欠如	十分でない資格情報の保護	通信上の認証資格情報が第三者によって盗聴される可能性がある脆弱性。	522
	重要情報の非暗号化	重要情報が平文で通信されており、第三者によって盗聴される可能性がある脆弱性。	311
	脆弱な暗号化方式	SSL 2.0等、使用が推奨されない暗号化方式を使用しているため、暗号を解読される可能性がある脆弱性。	327
	十分でないデータ真正性の確保	通信データに関して十分な検証がなされず、中間者攻撃によってなりすましや不正コードの挿入を受ける可能性がある脆弱性。	345
認証情報管理の不備	平文での認証情報の格納	認証情報が平文で格納されており、第三者が不正アクセス等によって窃取できる脆弱性。	256
	ハードコーディングされた認証情報	認証情報がプログラムに埋め込まれており、利用者によって変更することが難しく、悪用される可能性がある脆弱性。	259

項目	代表的な脆弱性	概要・脆弱性が悪用された場合の影響	対応するCWE
	脆弱な認証情報	第三者が容易に推測できID・パスワードが使用されており、不正アクセスを受ける可能性がある脆弱性。	521
認証設定の不備	ブルートフォース攻撃	ID・パスワードの総当たり攻撃によって、認証が回避可能な脆弱性。	307
	認証機構の迂回	正規の認証機能を迂回することができ、認証情報を有さない第三者からの不正アクセスを受ける可能性がある脆弱性。	288
不適切なデータ処理	バッファオーバーフロー	許容上以上のデータを挿入することで、メモリ上のバッファ領域を超えてデータの書き換えが可能となる脆弱性。	120
	フォーマット文字列攻撃	書式文字列関数[15]の機能を悪用し、不正コードが実行可能となる脆弱性。	134

脆弱性スキャンやネットワークスキャンにおいて重要となる二つの観点が「誤検知」と「見逃し」であり、これらを可能な限り減らすことが必要である。これらを減らす取り組みとして、二種類以上のツールを活用した脆弱性スキャンの実施、二名以上での脆弱性スキャンの実施、自動化ツールの活用と手動解析の融合などが挙げられる。また、誤検知を減らす取り組みとして、ツールが出した脆弱性の根本原因を整理・解析することは有効である。例えば、ソースコードが利用可能でクロスサイトスクリプティングの脆弱性が見つかった場合に、ソースコードのどこの部分が原因で脆弱性が存在するかを分析することで、誤検知を減らすことができる。加えて、見逃しを減らすために、検証対象機器の脆弱性に関する知識獲得も望まれる。対象機器にどのような脆弱性が存在しうるかを事前に知っておけば、機器に含まれうる脆弱性を推察することができる。

検出された既知脆弱性に対して、実際に悪用可能かを調査することもある。攻撃者の視点に立てば、攻撃の目的は脆弱性を見つけることにはなく、脆弱性を悪用して何らかの影響を与えることにある。言い換えれば、攻撃において脆弱性はあくまで手段の一つに過ぎない。検出された脆弱性は攻撃の手段の一つに過ぎず、検出された脆弱性を悪用することでどのような影響を与えることができるかを分析することも効果的である。その際、機器単体への影響だけではなく、機器が接続するサービスや、機器が導入されうるシステムを想定し、それらに与える可能性のある影響も併せて分析することが望ましい。

なお、既知脆弱性の診断技術に関する具体的な手法等を別冊 1 の第 4.6 節に示す。また、検証依頼者である機器メーカの立場から、既知脆弱性の診断の検証依頼時に知るべき留意点を別冊 2 の第 4.5 節、既知脆弱性の診断の検証結果を踏まえた対応方針を第 5.6 節に記載する。

[15] C 言語の場合、printf()関数や syslog()関数等のライブラリ関数を指す。

検証サービス事業者向け：

既知脆弱性の診断に関する具体的な手法等：別冊 1 第 4.6 節

検証依頼者（機器メーカ）者向け：

既知脆弱性の診断の検証依頼時に知るべき留意点：別冊 2 第 4.5 節

既知脆弱性の診断の検証結果を踏まえた対応方針：別冊 2 第 5.6 節

3.4.7 ファジング

ファジングとは、対象機器に対して機器の動作に問題を起こす可能性のあるデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検証手法である。脆弱性スキャンが既知の脆弱性をスキャンするのに対し、ファジングは未知の脆弱性を発見することが主な目的である。ファジングにおいても既知の脆弱性を発見することは可能であり、表 3-4 における「入力検証の不備」や「認証設定の不備」、「不適切なデータ処理」の脆弱性を理論的には検出できるが、実際にコード実行が可能かどうかの分析は検証人材がより詳細に解析する必要がある。

ファジングは、ブラックボックスファジング、ホワイトボックスファジング、そしてグレーボックスファジングの三つに分類することができる。ブラックボックスファジングとは、機器の内部構造を考慮せず、データの入出力と機器の動作から脆弱性や不具合を検出する手法であり、少ない情報量で実施できることが特徴である。ホワイトボックスファジングとは、機器の内部構造を把握した上で動作検証を行う手法であり、網羅的な検証が行える一方で、膨大な工数がかかることが特徴である。グレーボックスファジングはこれら二つの中間の位置づけであり、機器の内部構造を一部把握した上で、データの入出力と機器動作を判定する手法である。グレーボックスの場合、一部把握した内部構造によりテストケースを絞り込めるため、ホワイトボックスよりも効率的に、そしてブラックボックスよりも機器の特性に基づいた検証を行うことができるという特徴がある。検証依頼者が提示できる設計書やソースコード等の情報に依存して選択できるファジング手法は変わるが、ブラックボックスファジングで明らかになる脆弱性や不具合は限定的であり、可能であればグレーボックスファジングを実施することが望ましい。

ファジングを実施するツールの多くは自動化されており、ツールの活用により効率的に検証を行うことができる。ただし、ツールによって入力するデータの特性が大きく異なることに留意が必要である。IPA のレポート[16]で示されているとおり、入力データの取り得る範囲とデータの値によって決定するが、ツール毎の設計思想が異なり、網羅的に問題が起きそうな値を設定するツールもあれば、データを絞り込み集中的にファジングを行うツールもある。網羅的なファジングの場合、より多くの脆弱性や不具合を検出できる可能性がある一方で、集中的なファジングであれば、効率的な検出を行うことができる。また、他の検証手法においても同様であるものの、特にファジングツールについては、複数のプロトコルに対応した汎用的なツールから、特定のプロトコルやデータのみに対応したツールまで、商用・オープンソース問わず多くのツールを活用

[16] IPA, IPA テクニカルウォッチ 製品の品質を確保する「セキュリティテスト」に関するレポート
https://www.ipa.go.jp/files/000009390.pdf

することできるため、検証サービス事業者は検証目的・目標や検証にかかるコスト・期間、機器の特性等を踏まえたツールを採用する必要がある。

検出された脆弱性については、その再現性を確認するために手動にて追加検証を行うことが必要である。また、関連する脆弱性が存在しないか、追加で確認することが望ましい。手動にてファジングを行う場合のテストデータの作成には、IPA の「ファジング実践資料（テストデータ編）」[17]が参考となる。

なお、ファジング技術に関する具体的な手法等を別冊 1 の第 4.7 節に示す。また、検証依頼者である機器メーカの立場から、ファジングの検証依頼時に知るべき留意点を別冊 2 の第 4.6 節、ファジングの検証結果を踏まえた対応方針を第 5.7 節に記載する。

検証サービス事業者向け：
ファジングに関する具体的な手法等：別冊 1 第 4.7 節

検証依頼者（機器メーカ）者向け：
ファジングの検証依頼時に知るべき留意点：別冊 2 第 4.6 節
ファジングの検証結果を踏まえた対応方針：別冊 2 第 5.7 節

3.4.8 ネットワークキャプチャ

ネットワークキャプチャとは、機器やサービスのネットワークパケットを取得し、不審なパケットが無いか、重要情報が適切に保護されているか等を確認する手法である。これには、有線の通信だけでなく無線の通信も含む必要がある。多くのネットワークキャプチャツールは、機器の通信パケットを自動で取得し、どのような接続先に接続しているか、その通信はどのようなプロトコルを使用しているか等は自動で解析できるものの、不審なパケットが無いか等は人の目で分析・確認する必要がある。不審なパケットの例としては、正規の通信先サーバと過度な頻度での通信や、正規でない通信先サーバとの通信等が挙げられる。これは、機器の操作を行わずネットワークパケットだけを取得し、分析することで検出できる。一方で、ネットワークスキャンと同様に、不審なパケットが存在する場合でも、問題があることを裏付けるものではない。上述のとおり、ネットワークに常時接続する機器の場合、その機器が通信を行う通信先サーバが存在するため、定常的にサーバとの通信があることが想定されるほか、ファームウェアアップデートの確認等でそれ以外のサーバと通信することも想定される。検証サービス事業者は、不審なパケットの中身を確認し、それが不正な通信であるかを判断することが望ましい。

なお、ネットワークキャプチャ技術に関する具体的な手法等を別冊 1 の第 4.8 節に示す。また、検証依頼者である機器メーカの立場から、ネットワークキャプチャの検証依頼時に知るべき留意点を別冊 2 の第 4.7 節、ネットワークキャプチャの検証結果を踏まえた対応方針を第 5.8 節に記載する。

検証サービス事業者向け：

[17] IPA, ファジング実践資料（テストデータ編） https://www.ipa.go.jp/files/000035160.pdf

ネットワークキャプチャに関する具体的な手法等：別冊 1 第 4.8 節

検証依頼者（機器メーカ）者向け：
ネットワークキャプチャの検証依頼時に知るべき留意点：別冊 2 第 4.7 節
ネットワークキャプチャの検証結果を踏まえた対応方針：別冊 2 第 5.8 節

3.5 検証における留意点

検証サービス事業者が実施すべき事項

- 検証依頼者との秘密保持契約や免責事項を遵守するだけではなく、各種法令についても遵守する。
- ソフトウェア製品等の脆弱性関連情報に関する取扱規程や、組織の情報セキュリティ管理基準、二者間の秘密保持契約等に則り、第三者に脆弱性情報が漏えいしないよう適切に管理する。正当な理由が無い限り、第三者に脆弱性関連情報を開示してはならない。

検証サービス事業者は、検証依頼者との秘密保持契約や免責事項を遵守するだけではなく、各種法令についても遵守する必要がある。また、検証によって機器の脆弱性が検出された場合、その脆弱性を適切に管理する必要がある。本節では、検証を通じて留意すべきこれらの事項について記載する。

3.5.1 留意すべき法令等について

機器に対する検証手法を悪用することで、他のシステムや機器、情報等の資産に悪影響を与える可能性があるが、それにより法令違反につながる恐れもある。検証サービス事業者は、以下に挙げられた法令を遵守し、信頼できる検証サービスを提供する必要があるとともに、検証依頼者においても、検証サービスに関わる立場として、これらの法令について理解しておくことが望ましい。

- **不正アクセス行為の禁止等に関する法律**：不正アクセス行為者に対する処罰と、不正アクセス行為を受ける可能性のあるアクセス管理者が対策を適切に行えるような援助を目的とした法律である。不正アクセスを目的とした故意の識別符号情報（ID、パスワード等）の取得禁止も含まれている。検証依頼者の許可なき範囲（対象機器、日程、情報等）に対して検証を実施した場合、この法律に抵触する可能性もあるため、検証サービス事業者は二者間で合意した禁止事項の範囲を超えた検証をしてはならない。また、検証後は識別符号情報を含んだデータを適切に廃棄する必要がある。検証依頼者は、契約締結段階で検証の禁止事項を明確化するとともに、検証終了後、検証に使用した識別符号情報を変更・削除し、利用できないようにする必要がある。
- **威力業務妨害罪・電子計算機損壊等業務妨害罪（刑法第二三四条・第二百三十四条の二）**：威力業務妨害罪は、威力を行使して業務を妨害することに対する罪である。「業務」とは、企業の商売や個々が執行している業務だけではなく、社会生活上の地位に基づいて継続される

社会活動一般までが含まれる。この罪を、業務に使用するコンピュータやその用に供する電磁的記録に適用したものが電子計算機損壊等業務妨害罪である。この罪では、コンピュータの破壊やデータの消去に起因する物理的破壊だけでなく、不正データの送出や不正実行等により、意図しない動作が発生することも「業務の妨害」とみなされる。検証においても、ファジング等により検証機器以外の関連サービスがサービス不能に陥った場合等において、この罪の対象となる可能性がある。検証サービス事業者は、上述のとおり、二者間で合意した禁止事項の範囲を超えた検証をしてはならない。懸念がある場合には、契約締結段階で免責事項として合意しておく必要がある。

- **著作権法**：バイナリ解析においては、機械語の実行ファイルを人間が解読可能な高級プログラミング言語に逆コンパイル、又はアセンブリ言語に逆アセンブルし、それらを静的に解析するが、逆コンパイル等のリバースエンジニアリング時に留意すべき法令である。平成 31 年 1 月に施行された「著作権法の一部を改正する法律」によって、著作権法第三十条の四が改正され、技術の開発等のための試験の用に供する場合、情報解析の用に供する場合等にはその必要と認められる限度において利用することができると規定されている。具体的には、リバースエンジニアリングのようなプログラムの調査解析を目的としたプログラムの著作物を利用する行為は、権利制限の対象として挙げられるものと考えられる。この改正により、著作権を侵害せずリバースエンジニアリングすることが可能となったが、その解釈は統一的ではないという現状である。そのため、検証サービス事業者がリバースエンジニアリングを行う場合には、事前に依頼者の合意を得てから実施することが望ましい。

その他、セキュリティに関連する法令として、ウイルス・マルウェアの作成、供用等を処罰対象とした不正指令電磁的記録に関する罪（刑法第百六十八条の二及び三）や個人情報の取扱いについて定めた個人情報保護に関する法律が挙げられる。内閣サイバーセキュリティセンター（NISC）は、サイバーセキュリティに関連する法令等を整理[18]しており、検証サービスに携わる者は、関連するセキュリティ法令に関しても理解しておくことが望ましい。

加えて、検証サービスに携わる者は、検証の倫理性を常に意識する必要がある。検証技術を悪用した場合、機器の破壊だけではなく、その他の資産に対しても悪影響や損害・損失を及ぼす可能性がある。正義感と高い倫理観を持ち合わせた上で、セキュリティ向上を目的とした検証を常に心がけなければならない。

3.5.2 脆弱性情報の取扱いについて

脆弱性情報の管理については、組織の情報セキュリティ管理基準、二者間の秘密保持契約等に則り、第三者に脆弱性情報が漏えいしないよう適切に管理する。正当な理由が無い限り、第三者に脆弱性関連情報を開示してはならない。USB 等外部記憶媒体の取扱い管理を厳格に行い、外部ネットワークを介したデータの送受信は、安全性が保証されたサービスを活用することが望ましい。多くの検証サービス

[18] NISC, 関連法令等 https://www.nisc.go.jp/law/
NISC, サイバーセキュリティ関連法令 Q&A ハンドブック Ver1.0 https://www.nisc.go.jp/security-site/files/law_handbook.pdf

では、契約終了後も問い合わせ対応等を受け付けるため、検証後すぐに当該脆弱性情報を廃棄することは困難であるが、契約で定められた期間で適切に廃棄する必要がある。

脆弱性情報の取扱いについては、各種基準を従業員が理解し、適切に運用することが必要となる。そのためにも、従業員の教育を継続的に行い、その効果を測定することが望ましい。

なお、本手引きの直接的なスコープでないものの、市場に流通している製品に対して検証サービス事業者が検証を実施し脆弱性を検出した場合、経済産業省告示「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」に則り、IPA（脆弱性関連情報の受付機関）に対して脆弱性関連情報を届け出ることが望ましい。発見者から直接の届出を受け入れる旨を承諾している製品開発者[19]に対しては、直接届け出ることも可能である。脆弱性関連情報の届出を行う場合には、「情報セキュリティ早期警戒パートナーシップガイドライン」[20]を参照し、届け出る情報を明示する必要がある。特に、機器メーカが脆弱性の範囲や影響について確認するために、製品のバージョン情報や脆弱性の再現に必要な環境情報は正確に届け出る必要がある。

なお、IPA と製品開発者の両方に届け出る場合には、関係者間の調整が混乱しないよう、脆弱性の解消に向けた製品開発者との調整を自ら行うか、IPA に任せるかを、届出の際に明確にする必要がある。脆弱性関連情報は適切に管理する必要があり、製品開発者と直接やり取りした場合には、公表の内容について調整を行うことが望まれる。

IPA に脆弱性情報が届出された場合、対応することが妥当と判断した脆弱性関連情報について、IPA は速やかに JPCERT/CC（脆弱性関連情報の調整機関）に通知する。JPCERT/CC は影響のある製品の製品開発者（メーカ）に脆弱性関連情報の連絡と対応依頼を行う。製品開発者は、受け取った脆弱性関連情報に基づき、製品への影響調査と脆弱性検証を行い、その結果を JPCERT/CC に報告する。脆弱性が存在することを確認した場合、対策方法の作成や脆弱性情報流出に係るリスクを考慮しつつ、脆弱性情報の公表に関するスケジュールを検討する。脆弱性情報を公表する旨の判定がなされた場合には、公表に先立って、製品開発者から公表の内容に係る見解が聴取される。

製品開発者においては、第三者からの脆弱性関連情報を適切に受付・対処することで、製品利用者に対して対策の必要性を通知でき、製品やメーカの信頼低下を防ぐことができる。また、第三者からの脆弱性関連情報を適切に受付・対処することは、脆弱性の放置を未然に防止することにも繋がる。そのために、メーカは脆弱性情報を適切に受付・対処できる態勢を整え、第三者と調整を行えるように準備することが望まれる。第三者によって発見された脆弱性関連情報の受付・対処の手順については、IPA「脆弱性対処に向けた製品開発者向けガイド」[21]が参考となる。なお、IPA 及び JPCERT/CC を介して第三者から脆弱性関連情報を受け付ける場合、第三者から直接受け付ける場合よりも長期間を要す

---

[19] IPA 及び JPCERT/CC が提供する脆弱性対策情報ポータルサイト Japan Vulnerability Notes（JVN）における「JPCERT/CC 製品開発者リスト」として掲載されている。 https://jvn.jp/nav/

[20] IPA, JPCERT/CC, 電子情報技術産業協会、コンピュータソフトウェア協会、情報サービス産業協会、日本ネットワークセキュリティ協会 https://www.ipa.go.jp/files/000073901.pdf

[21] IPA, 脆弱性対処に向けた製品開発者向けガイド
https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

る。そのため、メーカは脆弱性関連情報を可能な限り迅速に受け付けることができるよう、JPCERT/CC の製品開発者リストにあらかじめ登録することが望まれる。

4 検証結果の報告

4.1 検証結果の分析

検証サービス事業者が実施すべき事項

- 検出された脆弱性が悪用された場合に想定される影響を特定するとともに、検出された各脆弱性に対して想定される対策を分析する。この際、検出された脆弱性が攻撃にどのように寄与するのか、それによってどのような影響が生じるのかを総合的に分析し、適切な緩和策を提示する。
- 検出された脆弱性の結果を踏まえ、検証の総合評価を依頼者に提示することが望まれる。

検証サービス事業者は、検証がすべて完了した後、検証依頼者に対して検証結果を報告するために、検証結果の分析を行う必要がある。具体的には、検出された脆弱性が悪用された場合に想定される影響を特定するとともに、検出された各脆弱性に対して想定される対策を分析し、依頼者に提示する必要がある。これらの分析結果は、表 3-3 に例として示した検証報告書の項目のうち、「検証結果の詳細」に記載される。

検出された脆弱性に対して想定される対策例として、表 3-4 に挙げた機器に存在しうる代表的な脆弱性に対する対策の例を表 4-1 に示す。なお、この表で示した対策は機器全般に適用されうる一般的な対策であるため、検証機器で検出された脆弱性すべてに適用できるものではないことを留意する必要がある。多くの場合、検出された脆弱性に対する対策は機器の特性や導入環境に依存するため、検証サービス事業者はこれらの条件を踏まえた対策の分析を行う必要がある。

表 4-1 代表的な脆弱性に対する対策の例

項目	代表的な脆弱性	対策の例
アクセス制御の不備	適切でない権限管理	内部機能はすべて管理者権限とせず、適切なユーザ権限を割り当てる。
	最小権限の原則の違反	最小権限の原則に則り、通常動作においては一般ユーザアカウントに限定する等の最小権限を設定する。
	適切でない認可	重要機能や重要情報においては、認証結果に基づく適切な認可パラメータを設定する。
	デフォルトアクセス設定の不備	機器の運用方法を踏まえ、適切なアクセス設定を行う。
入力検証の不備	クロスサイトスクリプティング	HTML 特殊文字をサニタイジング（エスケープ）する。

項目	代表的な脆弱性	対策の例
	OS コマンドインジェクション	OS コマンド呼出しを行わない実装を行う、又は OS コマンドに渡される特殊文字をサニタイジング（エスケープ）する。
通信暗号化機能の欠如	十分でない資格情報の保護	資格情報を適切な暗号化方式によって暗号化する。
	重要情報の非暗号化	重要情報を適切な暗号化方式によって暗号化する。
	脆弱な暗号化方式	SSL 2.0 等、使用が推奨されない暗号化方式を無効にし、一定以上の安全性が保証されている暗号化方式を使用する。
	十分でないデータ真正性の確保	HTTPS 等、なりすまし対策がなされた通信方式を採用する。
認証情報管理の不備	平文での認証情報の格納	認証情報を平文で格納しない。
	ハードコーディングされた認証情報	プログラム内にパスワードや暗号鍵等をハードコーディングしない。
	脆弱な認証情報	機器毎に異なる初期パスワードを設定する、又は初回認証時に初期パスワードの変更を必須とする。
認証設定の不備	ブルートフォース攻撃	認証試行回数や一定時間内の認証回数に制限を設ける。
	認証機構の迂回	処理実行時に認証情報を確認し、適切な認証情報が設定されていない場合は処理を許可しない。
不適切なデータ処理	バッファオーバーフロー	厳密な入力検査を行う、データ領域におけるコードの実行を防止する、又は書き込み先のバッファサイズを指定する。
	フォーマット文字列攻撃	厳密な入力検査を行う、データ領域におけるコードの実行を防止する、又は外部入力値を使用する関数を使用しない。

検証サービス事業者は、検出された各脆弱性に対して想定される対策を踏まえ、検証依頼者において実施が望まれる推奨事項を示す必要がある。この際、検出された脆弱性を悪用することで想定される総合的な影響を分析し、それに対して現実的に実施可能な推奨事項を提示することが望ましい。攻撃者が、機器に存在する脆弱性を一つだけ悪用し機器に対して大きな影響を与えることは通常困難であり、複数の脆弱性を悪用することで機器に対して影響を与えることが可能となる。複数の脆弱性が連鎖する

例として、機器の通信において重要な情報が暗号化されていないことで攻撃者が認証情報を盗聴でき、その認証情報を用いて、不正なファームウェアを対象機器に適用することが挙げられる。不正なファームウェアが適用された場合、攻撃者が機器を乗っ取り、不正に操作する可能性が考えられる。当然ながら、通信経路上の認証情報を適切に暗号化することは重要であるが、機器への直接的な影響を防ぐという観点では、不正ファームウェア適用に対して適切な対応策を講じることが望まれる。攻撃者にとっては、脆弱性は攻撃のための手段の一つでしかなく、検出された脆弱性が攻撃にどのように寄与するのか、それによってどのような影響が生じるのかを総合的に分析し、適切な緩和策を提示する必要がある。

また、検出された脆弱性の結果を踏まえ、検証の総合評価を依頼者に提示することが望まれる。検出された各脆弱性の評価に基づき、設定することが望ましく、依頼者やその上長が検証結果を一目で分かるよう、何らかの評価基準に基づき評価を決定することが期待される。想定される総合評価基準を表 4-2 に示す。総合評価は、表 3-3 に例として示した検証報告書の項目のうち、「総合評価」に記載される。

表 4-2 総合評価基準の例

総合評価レベル	概要	基準
緊急	検出された脆弱性が悪用されることで、機器そのものだけでなく、機器が導入されうるシステムに対しても影響を拡大する可能性がある、又は緊急対処が必要な脆弱性が検出された場合の評価。	脆弱性評価「緊急」の脆弱性が存在、又は脆弱性評価「重大」の脆弱性が複数存在する。
重大	検出された脆弱性が悪用されることで、機器の運用に多大な影響を及ぼす可能性がある、又は早急な対処が必要となる脆弱性が検出された場合の評価。	脆弱性評価「重大」の脆弱性が存在、又は脆弱性評価「警告」の脆弱性が複数存在する。
警告	検出された脆弱性が悪用されることで、機器の運用に影響を及ぼす、又は計画的な対策実施が推奨される脆弱性が検出された場合の評価。	脆弱性評価「警告」の脆弱性が存在、又は脆弱性評価「注意」の脆弱性が複数存在する。
注意	被害を受ける可能性は低い、又は限定的な条件の下で実行される脆弱性が検出された場合の評価。対策の要否を検討することが推奨される。	脆弱性評価「注意」の脆弱性が存在する。
情報	検証においては脆弱性が検出されず、適切な対策を継続することが望まれる場合の評価。	検証対象範囲内においては、脆弱性が存在しない。

4.2 検証結果の報告

検証サービス事業者が実施すべき事項

- 検証報告書は、検証依頼者が理解できるよう可能な限りの工夫を行うとともに、図表等を活用

し、読みやすい報告書とする。
- 対面の報告においては、論点を絞り、重要な点について説明する。検証で得られた事実に基づく内容のみを報告し、憶測等に基づく不確かな内容は含めるべきではない。
- 検出された脆弱性について、攻撃者が悪用可能であるならば、その脆弱性の対処を行わなかった場合の影響や、対策のための代替案を提示する。
- 報告会後にも、一ヶ月程度の問い合わせ対応期間を設けることが望ましい。

検証依頼者が実施すべき事項
- 報告結果を受け、機器に対するセキュリティ対応策を自社内で議論する。
- 検証の結果、ある程度対策が実施されていることが確認された場合でも、検証依頼者は継続的なセキュリティ対策を推進する

検証サービス事業者は検証結果の分析を踏まえ、検証報告書の作成及び検証依頼者に対する結果の報告を行う。検証報告書は、検証実施前に検証サービス事業者及び検証依頼者の間でその作成方針を確認した項目に基づき作成する必要があり、第 4.1 節で示した総合評価の結果等が含まれることが望ましい。それぞれの記載については、検証依頼者が理解できるよう可能な限りの工夫を行うとともに、図表等を活用し、読みやすい報告書とする必要がある。

報告においては、論点を絞り、重要な点について説明することが望まれる。この際、検証で得られた事実に基づく内容のみを報告し、憶測等に基づく不確かな内容は含めるべきではない。また、第 1.6 節に示したとおり、検証依頼者による検証依頼は、多くの場合に機器における脆弱性の有無を確認することが目的となるため、脆弱性が検出された場合の適切な対策についての道筋を提示することが望ましい。この際、検証目標も考慮した報告を行うことが望ましい。最も重要な機能に対するセキュリティ対策の妥当性を確認することを目標とした検証、網羅性の担保を目標とした検証のいずれにおいても、その目標に資する結果及び対策案を提示すべきである。併せて、報告会に出席する担当者の立場を把握しておくことが望まれる。機器の開発者、検証担当者、品質担当者、セキュリティ担当者等のうち何名かが出席することが想定されるが、それぞれが有する知識や立場が異なることを踏まえ、それぞれの担当者に効果的な説明とすることが望ましい。

検出された脆弱性について、攻撃者が現実的に悪用可能であるならば、その脆弱性について対処を行わなかった場合の影響を提示することが望ましく、脆弱性の対処を行わない場合の代替案についても提示することが望ましい。機器単体のセキュリティ対策では守りきれない部分が存在する場合、システム設計として対策を講じる必要がある領域も存在する。このような場合に対して、機器の利用者がシステム設計で対策を行う必要があることを認識しなければならず、その旨を依頼者に対して適切に伝える必要がある。

報告会後、二者間の契約期間は終了となるが、検証サービス事業者は一ヶ月程度の問い合わせ対応期間を設けることが望ましい。検証依頼者は、報告結果を受け、機器に対するセキュリティ向上策を、自社内で議論する必要がある。この際、検証の結果や総合評価が、依頼した検証の枠組みの評価であ

ることを認識する必要がある。言い換えれば、総合評価レベルが「緊急」や「重大」など、ある程度対策が実施されていることが確認された場合でも、検証依頼者は継続的なセキュリティ対策を推進する必要がある。検証結果に基づくリスク評価と対応方針の検討、並びに製品のリリースにあたって機器メーカが検討すべき内容については別冊 2 の第 5 章にて詳細に記載している。

5 付録

5.1 機器固有の検証手法等

第 3 章においては、IoT 機器等の検証における、汎用的に実施すべき事項や検証手法について記載した。本節では、以下の機器への検証を想定し、それぞれの機器特有の想定脅威や検証において実施すべき事項等を記載する。

- UTM（Unified Threat Management：統合脅威管理）
- ルータ
- ネットワークスイッチ
- ノート PC
- タブレット端末
- スマートロック
- ロボット掃除機
- ドローン
- スマート TV
- スマートリモコン
- カーナビゲーションシステム
- 産業用無線ルータ・産業用コントローラ

5.1.1 UTM

UTM とは、複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行う機器のことで、日本語では統合脅威管理と呼ばれる。ファイアウォールだけでなく、複数の脅威検知機能を有しており、ネットワークを包括的に防御することが可能となる。一般的な組織ネットワークの構成及び UTM の構成例を図 5-1 に示す。

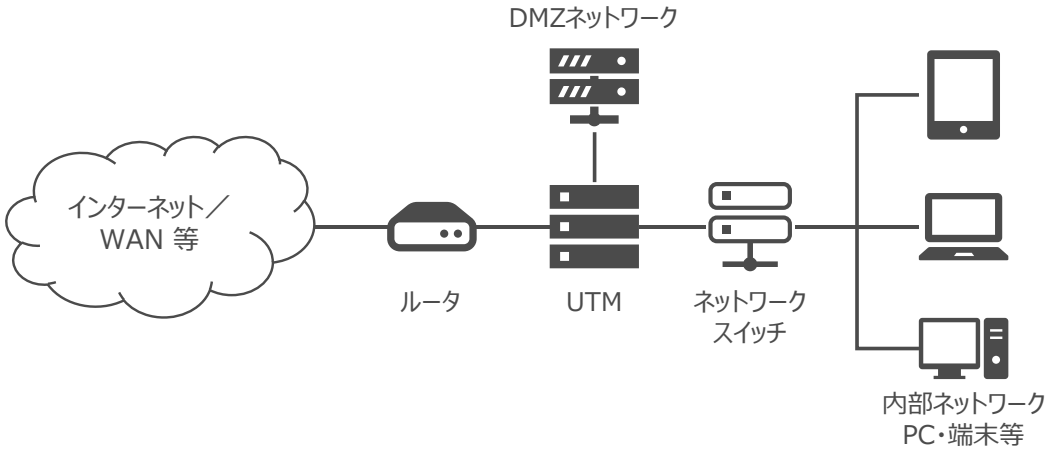


図 5-1 一般的な組織ネットワークにおけるルータ・UTM・ネットワークスイッチの構成例

UTM の運用においては、組織内外からの脅威を検知・防御し、組織におけるネットワーク機能を継続することが必要である。検証サービス事業者は、これらを阻害する脅威に繋がりうる脆弱性の有無を検証によって確認することが必要となる。

攻撃により機能を停止するためには、脆弱性を悪用して UTM 内部に侵入するほか、予期しないパケットやコマンドを UTM に送信し、機能を停止させることが考えられる。侵入方法としては、開発用機能をバックドアとして悪用する他、外部インタフェースの脆弱性を悪用する方法等が挙げられる。そのため、検証サービス事業者が機能停止に繋がる脅威について確認するためには、脆弱性を洗い出すという観点での既知脆弱性の診断やネットワークスキャン、バイナリ解析等の実施のほか、ファジングによって、未知の脆弱性が内在しないかを確認することが有効である。また、機能停止に対する防御性能を確認するためには、フラッド攻撃をはじめとする機器のリソースを消費される攻撃手法を試行し、サービス不能状態に陥ることが無いかを確認することが有効である。侵入に悪用される脆弱性としては、管理画面における認証機構の迂回や認証設定の不備、ファームウェアの検証不備等が考えられる。特に、脆弱性を悪用することで第三者が管理画面にアクセス可能な場合には、UTM を不正に操作することや、UTM を通過する通信内容の盗聴・改ざんが可能となる恐れがある。

UTM やルータ、ネットワークスイッチは、機器設定用の Web コンソールが用意されている場合が多く、Web コンソールに対する検証も製品のセキュリティを高めるという観点で重要である。Web コンソールに内在しうる脆弱性として、クロスサイトスクリプティングや OS コマンドインジェクション等の入力検証の不備が主に挙げられる。これらの脆弱性を洗い出す目的で、Web コンソールに対する既知脆弱性の診断も実施することが望ましい。

検証サービス事業者は、検証の前段階として、UTM 機能やアーキテクチャ、接続関係を調査・分析することが望まれる。具体的には、どのようにセッション維持管理がなされるか、どのように通信を監視しているか、通信内容に応じてどのような動作や通知がなされるか、どのように通信ファイルの展開処理が行われているか等の観点が含まれる。UTM が有する機能は多岐にわたるため、一つずつ検証を行うことは現実的ではない。機能を調査・分析し、検証のポイントを明確化した上で、実際の検証作業に移ることが望ましい。また、アーキテクチャの観点では、UTM がどのような OS によって動作しているかも重要となる。汎用 OS を使用している場合と独自 OS を使用している場合で、検出すべき脆弱性の特性が大きく異なるため、検証実施前に確認することが必要である。UTM は次に示すルータと機能が似ているため、同様の想定脅威や検証手法が適用できる。一方で、UTM の場合、パケットフィルタリングルールを回避する攻撃手法も登場しており、このような攻撃について検証を行うことが望まれる。関連して、パケットフィルタリングルールの更新等を行うために、外部と常時接続している場合もあり、監視・制御用の通信についても検証をすることが望ましい。

5.1.2 ルータ

ルータにおいて最も想定すべき脅威は、UTM と同様に、悪意ある第三者によってネットワーク機能や通信機能が阻害・停止されることにある。検証サービス事業者は、この脅威に繋がりうる脆弱性の有無を確

認することが必要となる。

ルータにおいても、脆弱性を悪用した内部侵入・権限昇格や、予期しないパケットやコマンドによる機能停止を検証することが必要となる。このために、脆弱性を洗い出すという観点での既知脆弱性の診断やネットワークスキャン、バイナリ解析等の実施のほか、ファジングによって、未知の脆弱性が内在しないかを確認することが有効である。機能停止に対する防御性能を確認するためには、フラッド攻撃をはじめとする機器のリソースを消費される攻撃手法を試行し、サービス不能状態に陥ることが無いかを確認することが有効である。また、Web コンソールに対する既知脆弱性の診断の実施も望まれる。加えて、検証実施前に、ルータの機能やアーキテクチャを調査・分析することも望まれる。

5.1.3 ネットワークスイッチ

ネットワークスイッチにおいても、悪意ある第三者によってネットワーク機能や通信機能が阻害・停止されることを重要な脅威として想定する必要がある。想定される攻撃手法として、特権ユーザ権限を不正に取得して不正操作を行うほか、不正パケットの送信によるサービス不能状態の発生等が考えられる。したがって、UTM やルータと同様に、脆弱性を悪用した内部侵入・権限昇格や、予期しないパケットやコマンドによる機能停止を検証することが必要となる。このために、脆弱性を洗い出すという観点での既知脆弱性の診断やネットワークスキャン、バイナリ解析等の実施が効果的である。ファジングによって、未知の脆弱性が内在しないかを確認するほか、機能停止に対する防御性能を確認するために、フラッド攻撃をはじめとする機器のリソースを消費される攻撃手法を試行し、サービス不能状態に陥ることが無いかを確認することも有効である。また、Web コンソールに対する既知脆弱性の診断の実施も望まれる。

UTM やルータ、ネットワークスイッチは独立に運用されるものではなく、その他の機器が接続されるという特性を有する。そのため、仮に脆弱性が検出された場合、その脆弱性を悪用することで、機器が導入されうるシステム全体にどのような影響を及ぼすかを深く分析することが望まれる。このような分析のために、当該機器がどのようなシステムに対して導入されることが多いかを把握することが効果的であり、機器メーカが自社の製品に対して検証依頼を実施する場合は、導入事例などを提示することが望ましい。

5.1.4 ノート PC

ノート PC の利用環境・利用目的は多岐にわたるため、メーカの責任範囲に限定して脅威分析や検証を実施する必要がある。すなわち、PC の BIOS やレジストリ、初期インストールされるソフトウェア、アップデート用ソフトウェア、メーカの証明書等のみを対象とし、OS やその他のソフトウェアは対象外とすることが一般的である。効果的な検証を行うために、メーカが検証依頼を行う際、検証の対象とする範囲を明確に検証サービス事業者に提示する必要がある。

ノート PC に想定される脅威として、第三者による端末の不正操作や利用者情報の第三者による窃取等が挙げられる。検証サービス事業者は、これらの脅威に繋がりうる脆弱性の有無を確認することが必要となる。例えば、レジストリの調査では、不正なアプリケーションの起動が許可されている設定となっていないかを確認することが望まれる。また、攻撃者が不正なデバイスドライバに置き換えて利用者のデータをフックし、データが窃取される攻撃も想定されるため、不正なデバイスドライバへの置き換え可能性につい

ても確認することが望まれる。初期インストールされるソフトウェアや、アップデート用のソフトウェアに対しては、プログラムの脆弱性を悪用して管理者権限を奪取し、不正操作や利用者の情報を窃取する脅威等が想定される。検証サービス事業者がソースコードを入手できる場合、ソースコード解析によって入力検証の不備や不適切なデータ処理等の代表的な脆弱性の有無を確認することが望まれる。ソースコードが入手できない場合はブラックボックスでの検証となるため、優先度の高い脅威に対する検証に限定して実施する必要があり、権限設定の妥当性、不正処理の実行可能性、外部からの悪用可能性等を重点的に確認することが望まれる。

5.1.5 タブレット端末

タブレット端末特有の想定脅威として、第三者による端末の不正操作や利用者の情報が悪意ある第三者によって窃取されることが挙げられる。検証サービス事業者は、この脅威に繋がりうる脆弱性の有無を確認することが必要となる。

検証においては、バイナリ解析等の他の機器においても有効な検証手法に加え、タブレット端末にインストールされるアプリの解析が重要となる。タブレット端末にインストールできるアプリは無数に存在するため、依頼者により開発されたアプリのみを検証の対象とする等、検証の工数を低減化することが必要である。検証依頼者からソースコードが入手できない場合でも、アプリのセキュリティ解析及び逆コンパイルを行えるフレームワークが公開されているため解析を行うことが可能である。手動による静的解析は時間を要するものであるため、自動化された静的解析ツールや動的解析ツールを活用して脆弱性の検出を試みることが現実的である。公開されている Android や iOS アプリの自動静的解析ツール・動的解析ツールを用いることで、アプリを再構成することなく関数の追跡やフッキングが可能となる。これにより、処理の不備の有無や利用者の認証情報が適切に保護されているかを確認することができる。

インストールされたアプリに対する検証だけではなく、不正なアプリがインストールできるかという観点も、情報窃取の脆弱性を調べる上で重要な観点である。不正なアプリのインストール可否については、一般的に端末の root 化/Jailbreak が必要となるため、これらが容易に実現できるかについても検証することが望まれる。

5.1.6 スマートロック

スマートロックとは、電気通信可能な錠で、スマートフォン等を用いて錠の開閉を行う機器である。ネットワーク構成の一例を図 5-2 に示す。市販の多くのスマートロックは Bluetooth の施錠・解錠機能を有しており、専用アプリを導入したスマートフォン等によって施解錠することができる。そのほか、Wi-Fi 接続機能を有したスマートロックの場合、同様に専用アプリを介して遠隔から施錠・解錠可能な場合もある。

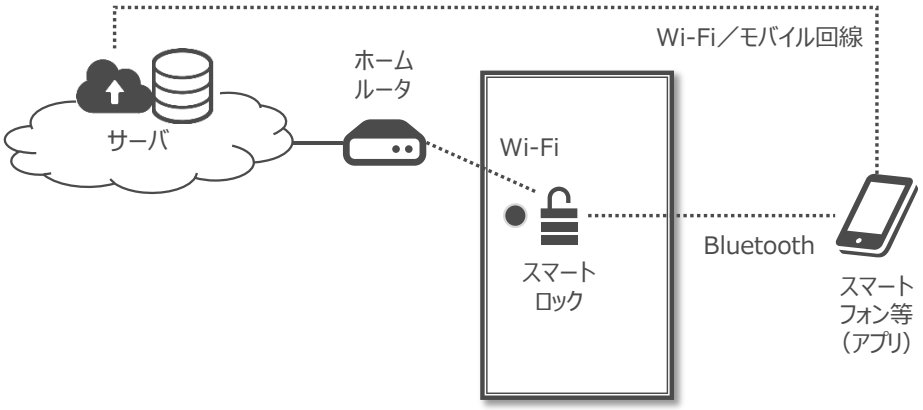


図 5-2 スマートロックのネットワーク構成例

スマートロック特有の想定脅威として、悪意ある第三者によってスマートロックが施解錠されることが挙げられる。検証サービス事業者は、この脅威に繋がりうる脆弱性の有無を確認することが必要となる。

スマートフォン等の端末を用いて施錠・解錠するという特徴を踏まえると、検証すべき観点としては、不正なスマートフォンアプリによって施錠・解錠されないか、既存のスマートフォンアプリの不正操作によって解錠されないか、スマートフォン・スマートロック間の通信の盗聴や中間者攻撃によって解錠されないか等が考えられる。既存のアプリにおける不正操作の観点では、アプリの静的解析・動的解析が効果的である。静的解析・動的解析においては、スマートロックの施錠・解錠が第三者によって可能かを確認することが必要となるため、特に通信に関するプログラムを解析することが望まれる。攻撃者の視点に立てば、悪用できるアプリに制限はない。そのため、スマートロック用のアプリが、Android や iOS 等の複数の OS で用意されている場合には、複数 OS のアプリに対して解析を行うことが望まれる。前述のとおり、公開されている Android や iOS アプリの自動静的解析ツール・動的解析ツールを用いることで、アプリを再構成することなく関数の追跡やフッキングが可能となる。

スマートフォン・スマートロック間の通信の盗聴や中間者攻撃の観点について、スマートロックの施錠・解錠のための通信は Bluetooth で行われることが多く、この通信を盗聴できるかをパケットキャプチャにより検証することが望まれる。施錠・解錠のための通信を取得する他の方法として、スマートロックになりすまし、なりすました機器を正規のスマートフォン等と接続することで通信内容を取得することが考えられる。なりすましの結果、スマートロックの施錠・解錠に必要なリクエストを入手できる場合、そのリクエストを悪用し、スマートロックに送信することで、施錠・解錠が可能かを検証することができる。

また、スマートロックは小型ゆえ、十分なメモリ容量を有していないことも想定されるため、ファジングによるオーバーフローによって、スマートロックの機能が停止され、本来の動作である施錠・解錠を受け付けない可能性もある。このような脆弱性についても併せて検証することが望まれる。

5.1.7 ロボット掃除機

ロボット掃除機には家庭用と業務用の二つが存在するが、本項では家庭用のロボット掃除機を対象に、想定脅威や検証において実施すべき事項等を記載する。家庭用ロボット掃除機のネットワーク構成例を

図 5-3 に示す。市販の多くのロボット掃除機は、赤外線センサーや超音波センサー等により調査した部屋の構造に基づき、自律的に掃除を行う。また、Wi-Fi に接続してスマートフォン等のモバイル端末とペアリングすることで、モバイル端末から遠隔で掃除の指示や、掃除のスケジューリングを行うことができる。

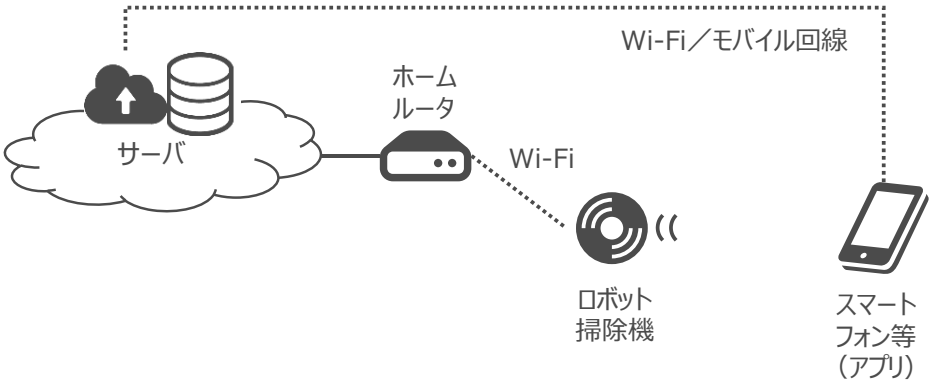


図 5-3 ロボット掃除機のネットワーク構成例

ロボット掃除機特有の想定脅威として、家庭内のロボット掃除機を攻撃者が不正に遠隔操作し、宅内の資産に対して物理的な損害を与えることが考えられる。想定される具体的な攻撃手法として、ロボット掃除機・サーバ間の通信の中間者攻撃による不正な遠隔操作や、サーバのなりすましによる不正な遠隔操作、なりすましたスマートフォンアプリによる不正な遠隔操作等が考えられる。検証サービス事業者は、これらの脅威や攻撃手法を実現しうる脆弱性の有無を確認することが必要となる。

検証においては、ロボット掃除機・サーバ間の通信をネットワークキャプチャにより確認し、通信に適切な暗号化方式が実装されているかを確認することが望まれる。また、ファームウェアのバイナリ解析や既知脆弱性の診断により、通信における脆弱性を特定することも有効である。適切な暗号化方式が実装されていない場合、サーバをなりすまして不正な制御信号を発出できる可能性があるほか、不正なファームウェアを送信して、ロボット掃除機上のファームウェアを不正に書き換える攻撃も想定される。そのため、バイナリ解析によりファームウェアアップデート時の検証について確認することが望まれるほか、正規のファームウェアが機器から抽出できないかをファームウェア解析により確認することが望まれる。

なりすましたスマートフォンアプリによる不正な遠隔操作に対する検証としては、まず、正規アプリの静的解析・動的解析を実施することが効果的である。公開されている Android や iOS アプリの自動静的解析ツール・動的解析ツールを用いて、ペアリング時や遠隔操作時の通信方式の妥当性、処理の不備の有無、利用者認証情報の適切な保護等を確認することが望まれる。

5.1.8 ドローン

航空法では、200g 以上の人が乗ることができない飛行機、回転翼航空機、滑空機、飛行船のうち、遠隔操作又は自動操縦により飛行させることができるものが「無人航空機」として定義され、機体重量が 200g 未満の航空機（一般的に「トイドローン」と呼ばれる）は模型航空機に分類される。本項では、

特に複数の回転翼を有したマルチコプターと呼ばれる無人航空機のうち、主に空撮に用いられる航空機をドローンと呼び、想定脅威や検証において実施すべき事項等を記載する。ドローンのネットワーク構成例を図 5-4 に示す。

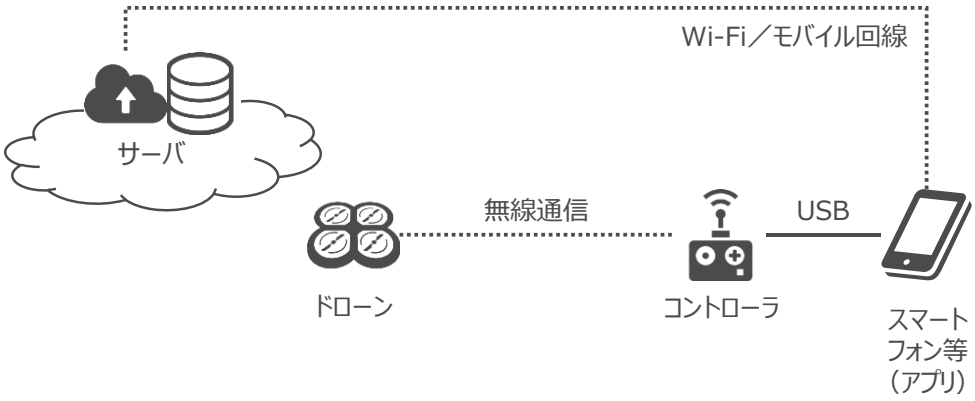


図 5-4 ドローンのネットワーク構成例

ドローン特有の想定脅威として、ドローンを攻撃者が不正に操作し、ドローン自体や周辺の資産に対して物理的な損害を与えることが考えられる。また、フライトログデータ等の重要データを窃取する脅威も想定される。前者の脅威については、なりすましたコントローラやスマートフォンアプリによる不正操作が攻撃手法として考えられる。後者の脅威については、スマートフォン等のアプリとサーバ間の通信の中間者攻撃による情報窃取が考えられる。検証サービス事業者は、これらの脅威や攻撃手法を実現しうる脆弱性の有無を確認することが必要となる。

なりすましたコントローラやスマートフォンアプリによる不正操作の検証にあたっては、コントローラやドローン本体のファームウェアのバイナリ解析や既知脆弱性の診断により、ユーザの権限設定が適切に実装されているか、不正なペアリング実装方式となっていないかを確認することが望まれる。ドローン本体やコントローラに直接アクセスできる攻撃者を仮定する場合、ドローン本体やコントローラのファームウェアを不正に書き換えることができないかを確認することも望まれる。なお、ドローン本体とコントローラ間の通信に汎用プロトコルを用いている場合、当該プロトコルに対する中間者攻撃の可能性をネットワークキャプチャや既知脆弱性の診断により確認することが望まれる。

スマートフォン等のアプリとサーバ間の通信の中間者攻撃による情報窃取に対する検証においては、ネットワークキャプチャや既知脆弱性の診断により通信の脆弱性が存在しないかを確認するほか、正規アプリの静的解析・動的解析を実施することが効果的である。前項のロボット掃除機と同様に、公開されている自動静的解析ツール・動的解析ツールを用いて、サーバへの通信方式の妥当性、フライトログデータの保管方法の妥当性、利用者認証情報の適切な保護等を確認することが望まれる。

5.1.9 スマート TV

スマート TV は、インターネットへの接続機能を備え、多機能・双方向の利用を可能にしたテレビ受像

機である。スマート TV のネットワーク構成の一例を図 5-5 に示す。

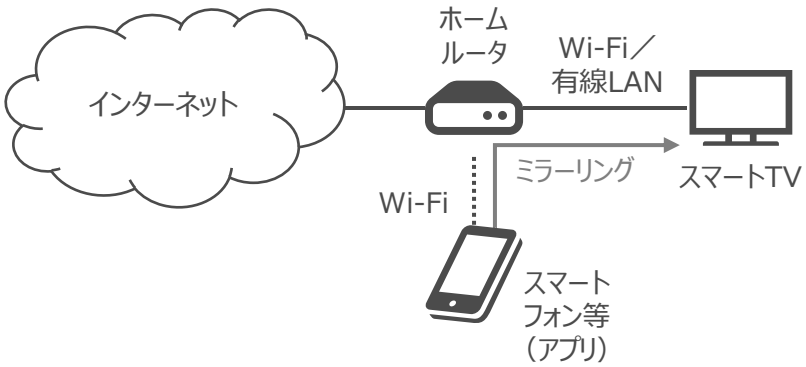


図 5-5 スマート TV のネットワーク構成例

インターネットへの接続機能を有しているスマート TV では、想定される攻撃手法として、有線 LAN・Wi-Fi を介した不正操作を考慮する必要がある。また、特権ユーザ権限は、いわゆるペアレンタル設定以外には存在しないものの、メンテナンス用の権限が存在する場合も想定されるため、JTAG 端子などのデバッグポートなどの検証等も必要である。また、スマート TV の特徴として、USB などで接続する外部ストレージが存在することが挙げられる。そのため、USB 接続の外部ストレージに対する情報窃取の脆弱性や不正なアプリがインストールできるかという観点も重要である。一般的な通信だけではなく、スマート TV に多く実装されている DIAL（Discovery-and-Launch）プロトコル等もついても検証することが求められる。さらに、他の機器と同様に、ファームウェアのアップデート機能が実装されている場合は、バイナリ解析によりファームウェアアップデート時の検証について確認することが望まれる。加えて、正規のファームウェアが機器から抽出できないかをファームウェア解析や証明書の利用により確認することが望まれる。

5.1.10 スマートリモコン

スマートリモコンは、家電・照明などを外部のリモコン専用機器やスマホ、AI スピーカーなどからコントロールする機器である。本項では、特にスマホの専用アプリを用いて宅内の家電・照明など制御可能で、AI スピーカー機能を有していないスマートリモコンに関する想定脅威や検証において実施すべき事項等を記載する。スマートリモコンのネットワーク構成例を図 5-6 に示す。

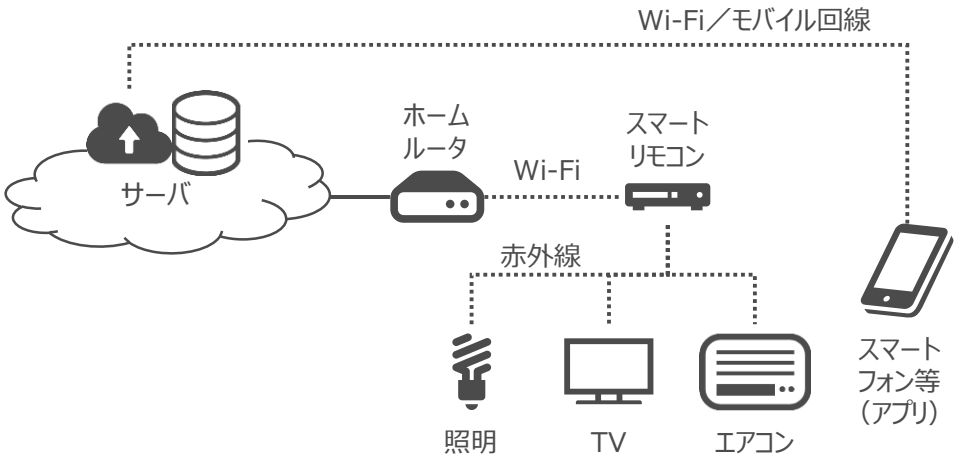


図 5-6 スマートリモコンのネットワーク構成例

スマートリモコンは、Wi-Fi ルータ、Bluetooth 接続機器及びスマートフォンとスマートフォンアプリを介して遠隔からコントロールするため、遠隔操作の可能性及び中間者攻撃による操作内容の改ざん等の脅威を考慮する必要がある。この観点は、前述した市販のスマートロックにも共通する検証が含まれる。スマートロックでは、主に Bluetooth の施錠・解錠機能及び専用アプリを導入したスマートフォン等による施解錠について検証していたが、スマートリモコンは宅内・宅外からの操作を考慮する必要があり、スマートリモコンの Wi-Fi 電波範囲内からスマートリモコンを不正に操作する脅威や、不正にペアリング操作を行い、機器を不正操作する脅威を考慮することが望まれる。

5.1.11 カーナビゲーションシステム

カーナビゲーションシステム（Car Navigation System）は、自動車に搭載される情報機器の一種で、道順を案内することで運転者を支援する機器である。電子的に自動車の走行時に現在位置や目的地への経路案内を行う機器のことであり、USB や Bluetooth 等のインタフェースを有する。スマートリモコンのネットワーク構成例を図 5-7 に示す。

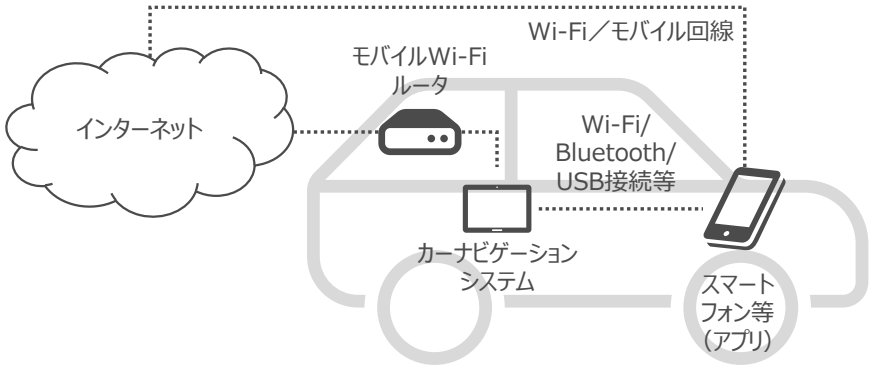


図 5-7 カーナビゲーションシステムのネットワーク構成例

カーナビゲーションシステムに想定される脅威として、カーナビゲーションシステム本体のファームウェアにおける脅威のほか、デバッグ機能やカーナビゲーションシステムのインタフェースで侵入・攻撃のポイントになるSD カードスロットとの通信に対する脅威、Wi-Fi、USB、Bluetooth 等を介したスマートフォンとの通信に対する脅威が想定される。スマートフォンとの通信については、スマートフォンアプリとのペアリングや通信仕様を考慮する必要があり、一部には、スマートフォンアプリの解析も必要になる場合も考えられる。

また、カーナビゲーションシステムにはファームウェアのアップデートも可能な機器もあり、OTA（Over The Air）によるアップデートや、外部フラッシュメモリによるアップデートなどの方法が考えられる。これらのアップデートについては、バイナリ解析によりファームウェアアップデート時の検証について確認することが望まれるほか、正規のファームウェアが機器から抽出できないかをファームウェア解析や証明書の利用により確認することが望まれる。

他の機器との違いとしてカーナビゲーションシステムは、運転者を支援する機器であるため、可用性や即時性も求められる。したがって、前述の攻撃や不正操作により、運転者を支援する機能や表示に対して与える影響も分析することが重要である。

5.1.12　産業用無線ルータ・産業用コントローラ

産業用無線ルータは、産業用機器を無線 LAN やインターネットに接続する機器である。産業用コントローラは、産業機器の稼動及び制御する機器である。産業用無線ルータ・産業用コントローラのネットワーク構成例を図 5-8 に示す。

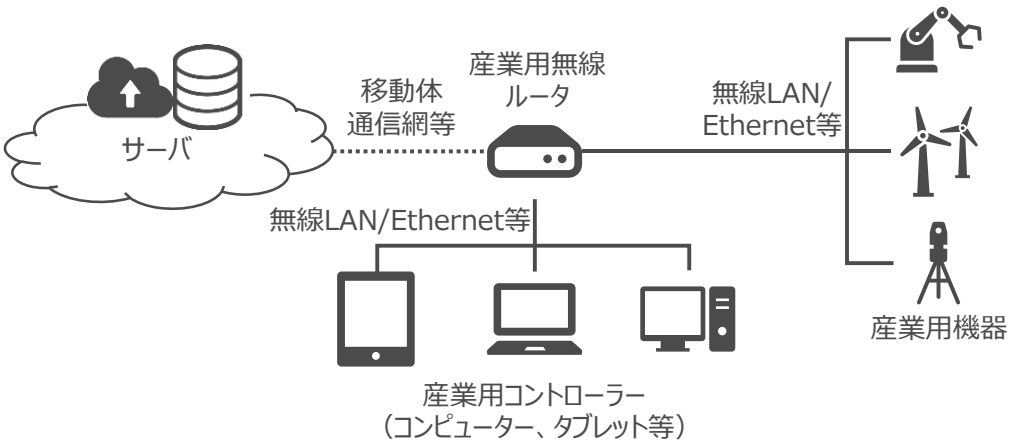


図 5-8　産業用無線ルータ・産業用コントローラのネットワーク構成例

産業用コントローラにおいては、USB や RS232C などのインタフェースも存在するため、一般的な PC の検証と同じ検証手法が適用できる。産業用コントローラは、一般的には単体で利用できるものではなく、各種の機能を備えた I/O ユニットや専用のアプリケーションの基で動作が可能となる。そのため、どのような動作環境を用意し、どのような脅威を想定するかをあらかじめ設定・分析しておくことが重要である。特に、産業用機器については、特定組織内で外部のネットワークとは遮断された環境に設置され、専用の管理

者が操作することを想定している場合もある。検証対象となる機器の仕様や想定動作環境については、検証依頼者との調整を充分に行う必要がある。

また、産業用無線ルータは、製品により利用できるインタフェースは異なるものの、Wi-Fi や無線 LAN など複数のインタフェースを介した通信が可能であり、一般的なルータの検証と同じ検証手法が適用できる。さらに、一般的なルータと同様に、設定用の Web コンソールが提供されている場合もあり、設定機能についても検証対象となる。

5.2 用語集

- **CC（Common Criteria）**
  セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための仕組み。国際規格 ISO/IEC 15408 に規定されている。

- **CTF（Capture the Flag）**
  情報セキュリティの技術を競い合う競技であり、自らのスキル・知識を駆使して埋め込まれた答え（Flag）を探索するゲーム・競技。個人で Flag を探索する形式もあれば、チームに分かれて Flag を奪い合う形式も存在する。

- **CVSS（Common Vulnerability Scoring System）**
  脆弱性の深刻度を同一の基準の下で定量的に比較できる評価方法であり、0.0～10.0 の間でスコアが定まる。FIRST（Forum of Incident Response and Security Teams)が管理。

- **CWE（Common Weakness Enumeration）**
  Common Weakness Enumeration の略。ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準。米国非営利団体 MITRE を中心として仕様策定。

- **DIAL（Discovery-and-Launch）**
  クライアントとサーバが共に接続するサブネットにおいてアプリケーションを検出でき、スマート TV においてはタブレット PC やスマートフォンなどのセカンドスクリーンデバイスにコンテンツを送信できる。

- **DREAD**
  Damage、Reproducibility、Exploitability、Affected users、Discoverability の五つの観点の頭文字から構成される用語で、これら五つの観点に基づきリスクのスコアリングを行う手法。

- **JTAG (Joint Test Action Group)**
  IEEE1149.1 で標準化されているポートの通称。IC チップとその周辺の集積回路を含むチップセットとの相互通信や IC チップ自体の検査、回路動作に対する監視及び書き換えを行うこと等が可能。

- **OWASP（Open Web Application Security Project）**
  Web をはじめとするソフトウェアのセキュリティ関する情報共有と普及啓発を目的とした、オープンソース・ソフトウェアコミュニティ。

- **IoT（Internet of Things）**
  既存又は開発中の相互運用可能な情報通信技術により、物理的又は仮想的なモノをネットワーク接続した、高度なサービスを実現するグローバルインフラ。[IoT セキュリティガイドライン ver 1.0]

- **IoT 機器**
  IoT を構成する、ネットワークに接続される機器。

- **ISMS（Information Security Management System）**
  組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組み。国際規格 ISO/IEC 27001 に要求事項が定められている。

- **STRIDE**
  Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏えい）、Denial of Service（サービス拒否）、Elevation of Privilege（権限昇格）の六つの脅威の性質の頭文字から構成され、これら六点の性質から脅威を洗い出していく手法。

- **TLPT（Threat-Led Penetration Test）**
  実在の攻撃者の戦術、テクニック、手順等を模倣し、組織のサイバーレジリエンスを侵害しようとすることを目的としたペネトレーションテスト。攻撃側（Red Team）の脅威情報に基づく現実的な攻撃に対して、防御側（Blue Team）は組織として防御、検知、対応等を行い、組織全体のレジリエンス能力を評価する。

- **UART (Universal Asynchronous Receiver/Transmitter)**
  デバッグ等を目的として、外部端末から回路基板にアクセスするために使用されるシリアル信号とパラレル信号の変換を行う集積回路。

- **脅威（Threat）**
  システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。[JIS Q 27000:2014]

- **脅威情報（Threat Intelligence）**
  脅威からの保護、攻撃者の活動検知、脅威への対応等に役立つ可能性のある情報。[NIST SP 800-150]

- **脅威分析（Threat Analysis）**
  機器やソフトウェア、システム等に対する脅威を抽出し、その影響を評価すること。主に、製品の要件定義、設計フェーズにて行われる。

- **サイバー攻撃（Cyber Attack）**

資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000:2014]

- **サイバーセキュリティ（Cybersecurity）**
  電子データの漏えい・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。

- **サプライチェーン（Supply Chain）**
  複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達にはじまり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れ。[ISO 28001:2007, NIST SP 800-53 Rev.4]

- **シグネチャ（Signature）**
  通信パケットに含まれる、攻撃に関係する認識可能で特徴的なパターン。ウイルス中のバイナリ文字列や、システムへの不正アクセスを得るために使用する特定のキーストロークなど。[NIST SP 800-61 Rev.1]

- **脆弱性（Vulnerability）**
  一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JIS Q 27000:2014]

- **脆弱性検証（Vulnerability Validation）**
  脆弱性の存在を確認するアクティブなセキュリティ検証手法。[NIST SP 800-115]
  脆弱性を洗い出すことを目的とする。

- **セキュリティ検証（Security Validation）**
  機器、システム、組織における脅威に対するセキュリティ対策の妥当性や脆弱性の有無を確認する手法。本手引きでは、特に機器に対するセキュリティ検証について記載している。

- **認証（Authentication）**
  エンティティの主張する特性が正しいという保証の提供。[JIS Q 27000:2014]

- **認可（Authorization）**
  アクセス権限に基づいたアクセス機能の提供を含む権限の付与 [ISO 7498-2:1989]

- **バックドア（Backdoor）**
  機器に設けられた、正規のログイン方法ではない非公表のアクセス方法。潜在的なセキュリティリスクとなりうる。[NIST SP 800-82 Rev.2]

- **ファジング（Fuzzing）**
  検証対象の機器やソフトウェアに脆弱性を引き起こしうるデータ（ファズデータ）を送り込み、その挙

動を確認することで脆弱性を検出する手法。

- **プロトコル（Protocol）**
  複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。

- **ペネトレーションテスト（Penetration Test）**
  組織が有するすべてのシステムや、指定されたシステム全体を対象とし、明確な意図を持った攻撃者によって、その目的が達成されうるかを確認するセキュリティ検証手法。

- **マルウェア（Malware）**
  許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェア又はファームウェア。[NIST SP 800-53 Rev.4]
  セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。

- **リスク（Risk）**
  目的に対する不確かさの影響。[JIS Q 27000:2014]

- **レジリエンス（Resilience）**
  システムが以下の状態を維持できること：①悪条件下にあっても、あるいは負荷がかかった状態であっても、（顕著に低下した状態又は無力化したような状態に陥ったとしても）稼働して、基礎的な運用能力を維持すること。②ミッションニーズと平仄が合う時間内に、有効的に運用されている状態に復旧すること。[NIST SP 800-53 Rev.4]

5.3 参考文書

- **サイバー・フィジカル・セキュリティ対策フレームワーク（経済産業省）**
  https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

- **IoT セキュリティガイドライン ver1.0（IoT 推進コンソーシアム、総務省、経済産業省）**
  https://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

- **OWASP テスティングガイド 第 3 版（OWASP）**
  https://www.owasp.org/images/1/1e/OTGv3Japanese.pdf

- **NIST SP 800-115: Technical Guide to Information Security Testing and Assessment（NIST）**
  https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

- **脆弱性診断士スキルマッププロジェクト（ISOG-J 及び OWASP Japan）**

https://wiki.owasp.org/index.php/Pentester_Skillmap_Project_JP

- **情報セキュリティサービス審査登録制度 情報セキュリティサービス基準（経済産業省）**
  https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf
- **IoT 開発におけるセキュリティ設計の手引き （IPA）**
  https://www.ipa.go.jp/files/000052459.pdf
- **つながる世界の開発指針 第 2 版（IPA）**
  https://www.ipa.go.jp/files/000060387.pdf
- **Internet of Things (IoT) Project（OWASP）**
  https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- **ファジング活用の手引き（IPA）**
  https://www.ipa.go.jp/security/vuln/documents/fuzzing-guide.pdf

（様式２）

二次利用未承諾リスト

令和３年度サイバー・フィジカル・セキュリティ対策促進事業
先進的手法を用いたセキュリティ検証及び検証サービスビジネスの発展に関する調査 報告書

令和３年度サイバー・フィジカル・セキュリティ対策促進事業（先進的手法を用いたセキュリティ検証及び検証サービスビジネスの発展に関する調査）

株式会社三菱総合研究所

頁	図表番号	タイトル
57	図4-12	機器メーカーにおける企画・設計段階、製造段階でのセキュリティ方針・基準の有無
57	図4-13	機器メーカーにおける脆弱性対策の実施状況
58	図4-14	機器メーカーにおけるセキュリティ担当部門の関与状況
58	図4-15	機器メーカーにおける製品販売後に脆弱性が発見された経験の有無
59	図4-16	機器メーカーにおけるサポート時のセキュリティ対策費用の有無
59	図4-17	機器メーカーにおけるセキュリティ対策の課題
62	図4-18	機器開発プロセスにおける手引き本編及び別冊 1・別冊 2 のスコープ
64	図4-19	端末設備等規則（第34条の10）に係る技術基準適合認定等の対象機器の範囲のイメージ
69	図4-20	NIST “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”の概要
71	図4-21	消費者向けIoTラベリングの制度オーナーが既存のリソースを利用する方法を示した図
75	図4-22	IT Security Labelのイメージ図
76	図4-23	CLSにおいて求められるサイバーセキュリティレベルの概要
84	図4-25	Cyberseekプロジェクトの概要
85	図4-26	NICCS Education and Training Catalogの検索画面
89	図4-27	UL：IoTセキュリティレーティングサービスにおける5つのラベル
97	表4-29	各国ラベリング制度の比較

令和３年度サイバー・フィジカル・セキュリティ対策促進事業

先進的手法を用いたセキュリティ検証及び検証サービスビジネスの発展に関する調査

報告書

2022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