

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
中小企業が開発するIoT機器に関する調査事業
報告書

MRI 三菱総合研究所

2022年3月31日

デジタル・イノベーション本部

目次

1. 調査概要	7
1.1 調査背景・目的	7
1.2 調査実施概要	7
2. 中小企業が発売する IoT 機器や IoT 機器の設計書等の調査	8
2.1 中小企業が発売する IoT 機器のリストアップ	8
2.2 中小企業へのアプローチ方策に関する検討	11
3. 中小企業への IoT 機器や IoT 機器の設計書等の提供依頼	12
3.1 中小企業に対する依頼	12
3.1.1 説明内容	12
3.1.2 依頼方法	18
4. IoT 機器のセキュリティ検証事業者のリストアップ	20
4.1 各検証事業者における対応可能性	20
4.2 各検証事業者における検証実績・検証対応意向	22
4.2.1 検証事業者 A 社	23
4.2.2 検証事業者 B 社	26
4.2.3 検証事業者 C 社	33
4.2.4 検証事業者 D 社	36
4.2.5 検証事業者 E 社	40
4.2.6 検証事業者 F 社	49
4.2.7 検証事業者 G 社	52
4.2.8 検証事業者 H 社	55
4.2.9 検証事業者 I 社	59
4.3 検証手法に関する検証事業者の対応可能性比較	65
4.4 対象機器・対象分野に関する検証事業者の実績比較	66
4.5 対象機器・対象分野に関する検証事業者の対応意向比較	70
5. まとめ	74

図 目次

図 2-1 本調査で対象とする IoT 機器の考え方	8
図 3-1 IoT 機器に対するセキュリティ対策の必要性	12
図 3-2 IoT 機器に対するセキュリティの取組状況・本事業の目的	13
図 3-3 中小企業に対する協力依頼事項	14
図 3-4 協力企業に対するメリット	14
図 3-5 IoT 機器に適用されうる一般的な検証手法	15
図 3-6 パンフレット(表面)	16
図 3-7 パンフレット(裏面)	17
図 3-8 架電フロー	18

表 目次

表 2-1 中小企業が販売する IoT 製品リストアップ結果	9
表 2-2 中小企業が販売する IoT 製品一覧例(一般消費者向け)	10
表 2-3 中小企業へのアプローチ方法	11
表 3-1 架電における FAQ 内容	19
表 4-1 各検証事業者における対応可能性	20
表 4-2 検証手法に関する対応可能性(検証事業者 A 社)	23
表 4-3 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 A 社)	24
表 4-4 産業用機器等に関する検証実績・対応意向(検証事業者 A 社)	25
表 4-5 産業用分野に関する検証実績・対応意向(検証事業者 A 社)	26
表 4-6 検証手法に関する対応可能性(検証事業者 B 社)	27
表 4-7 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 B 社)	28
表 4-8 産業用機器等に関する検証実績・対応意向(検証事業者 B 社)	31
表 4-9 産業用分野に関する検証実績・対応意向(検証事業者 B 社)	32
表 4-10 検証手法に関する対応可能性(検証事業者 C 社)	33
表 4-11 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 C 社)	34
表 4-12 産業用機器等に関する検証実績・対応意向(検証事業者 C 社)	35
表 4-13 産業用分野に関する検証実績・対応意向(検証事業者 C 社)	36
表 4-14 検証手法に関する対応可能性(検証事業者 D 社)	37
表 4-15 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 D 社)	37
表 4-16 産業用機器等に関する検証実績・対応意向(検証事業者 D 社)	39
表 4-17 産業用分野に関する検証実績・対応意向(検証事業者 D 社)	40
表 4-18 検証手法に関する対応可能性(検証事業者 E 社)	40
表 4-19 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 E 社)	41
表 4-20 産業用機器等に関する検証実績・対応意向(検証事業者 E 社)	46
表 4-21 産業用分野に関する検証実績・対応意向(検証事業者 E 社)	48
表 4-22 検証手法に関する対応可能性(検証事業者 F 社)	49
表 4-23 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 F 社)	49
表 4-24 産業用機器等に関する検証実績・対応意向(検証事業者 F 社)	51
表 4-25 産業用分野に関する検証実績・対応意向(検証事業者 F 社)	51
表 4-26 検証手法に関する対応可能性(検証事業者 G 社)	52
表 4-27 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 G 社)	53
表 4-28 産業用機器等に関する検証実績・対応意向(検証事業者 G 社)	54
表 4-29 産業用分野に関する検証実績・対応意向(検証事業者 G 社)	55
表 4-30 検証手法に関する対応可能性(検証事業者 H 社)	56
表 4-31 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 H 社)	56
表 4-32 産業用機器等に関する検証実績・対応意向(検証事業者 H 社)	58

表 4-33 産業用分野に関する検証実績・対応意向(検証事業者 H 社)	58
表 4-34 検証手法に関する対応可能性(検証事業者 I 社)	59
表 4-35 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 I 社(ファジングツール))	61
表 4-36 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 I 社(静的解析ツール))	62
表 4-37 産業用機器等に関する検証実績・対応意向(検証事業者 I 社(ファジングツール))	63
表 4-38 産業用機器等に関する検証実績・対応意向(検証事業者 I 社(静的解析ツール))	64
表 4-39 産業用分野に関する検証実績・対応意向(検証事業者 I 社(ファジングツール))	64
表 4-40 産業用分野に関する検証実績・対応意向(検証事業者 I 社(静的解析ツール))	65
表 4-41 検証手法に関する検証事業者の対応可能性比較	66
表 4-42 一般消費者向け IoT 機器等に関する検証実績比較	67
表 4-43 産業用機器に関する検証実績比較	69
表 4-44 産業分野別の検証実績比較	69
表 4-45 一般消費者向け IoT 機器等の検証に対する対応意向比較	70
表 4-46 産業用機器の検証に対する対応意向比較	72
表 4-47 産業分野別の対応意向比較	73

1. 調査概要

1.1 調査背景・目的

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

一方、一般消費者のうち IoT 機器に関する脅威を理解している者は 1 割にも満たず、日本の中小企業が発売する IoT 機器についてはセキュリティ対策が十分であるかも不明である。また、脆弱性の検証サービスの利用は中小企業にとって決して安いものではなく、費用面や開発に要する日数が増加する等の理由で現時点では必要性が理解されていない。

市場投入後に機器に脆弱性が見つければ、最低でも緊急のセキュリティアップデートの対応が求められるだけでなく、場合によっては回収等の対応を求められる可能性もあり、中小企業の経営に大きな影響を及ぼす可能性があることから、中小企業の負担軽減も考慮した効果的な検証手法の進め方の整理を早急に行う必要がある。

本事業では、効果的な検証手法の進め方の整理を円滑に実施するために、中小企業が発売する IoT 機器や IoT 機器の設計書等の調査、中小企業への IoT 機器や IoT 機器の設計書等の提供依頼、IoT 機器のセキュリティ検証事業者のリストアップを実施した。

1.2 調査実施概要

調査目的を達成するために、以下の項目に関して調査・検討・支援等を行った。

- (1) 中小企業が発売する IoT 機器や IoT 機器の設計書等の調査
- (2) 中小企業への IoT 機器や IoT 機器の設計書等の提供依頼
- (3) IoT 機器のセキュリティ検証事業者のリストアップ

2. 中小企業が発売する IoT 機器や IoT 機器の設計書等の調査

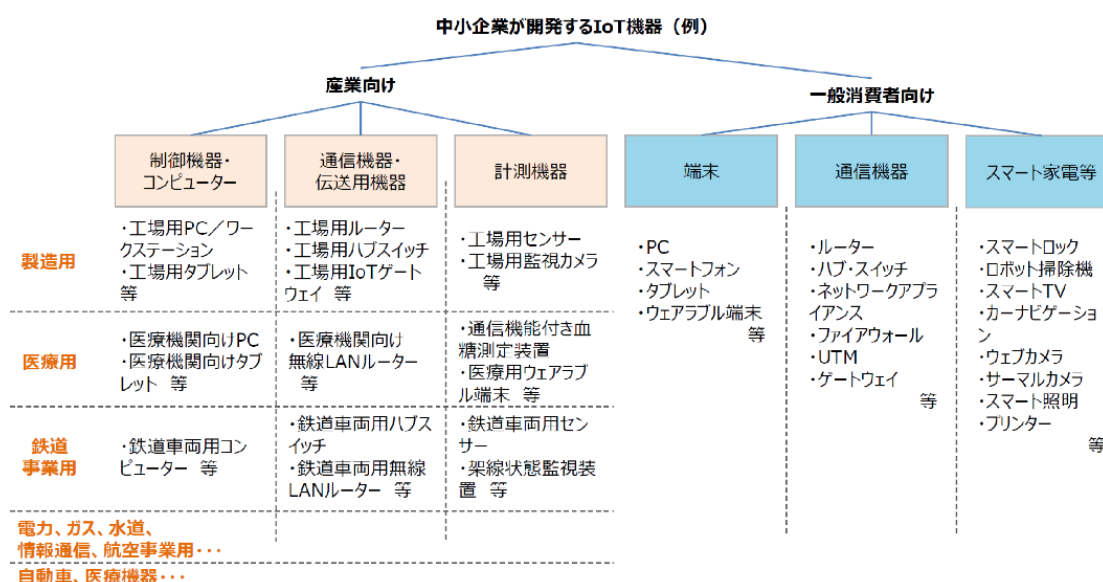
IoT 家電、産業機器、工場等で使用されるセンサー、産業用ドローン、ネットワーク機器、自動車等の車載器、タブレット等のモバイル端末、スマートデバイス、スマートトラック等脆弱性攻撃の対象となりうる中小企業が発売する IoT 機器を 20 程度の産業分野で各 20 個程度(合計400個程度)選定し、選定したものの中から 10 程度の産業分野で各 15 個程度(150 個程度)を対象とし、IoT 機器本体及び IoT 機器に関するもの(実機、設計書、仕様書、取扱説明書、マニュアル、ソースコード、プロトタイプ、システム構成図、ネットワークの設定手順等)について、調査・分析の上、とりまとめた。

2.1 中小企業が発売する IoT 機器のリストアップ

本調査で対象とする IoT 機器の対象については、IoT 機器を限定するものではなく、広く産業向け及び一般消費者向けで分類し、一般消費者向けについてはスマート家電、通信・ネットワーク機器、端末等、産業向けでは、特に高いセキュリティレベルが要求されるような自動車・医療機器等や重要インフラ分野で利用されるセンサー周りの計測機器、制御機器・コンピュータ、伝送・通信・ネットワーク機器等を想定した。

【参考】本事業で対象とするIoT機器の考え方（類型化）

- 本事業では、中小企業が開発するIoT機器を、**産業向けと一般消費者向けの大きく2つの観点から分類**。
- いずれかに該当するIoT機器に対して、当該機器を開発する中小企業にご協力をいただき、脆弱性検証を実施する。



5

図 2-1 本調査で対象とする IoT 機器の考え方

調査対象とする中小企業が販売する IoT 機器をリストアップするために、以下の情報源から対象となる機器を抽出した。

<主に産業向け>

・ipros (<https://www.ipros.jp/>)

<主に一般消費者向け>

・ビックカメラ (<https://www.biccamera.com/bc/main/>)

・マクアケ (<https://www.makuake.com/>)

ピックアップした結果は以下のとおりである。

表 2-1 中小企業が販売する IoT 製品リストアップ結果

		制御機器、 コンピュータ	通信機器・ 伝送用機器	計測機器	合計
産業向け	製造業	831	349	2	1,182
	医療	90	8	0	98
	エネルギー	4	10	0	14
	鉄道	33	19	0	52
	全般	1,414	369	26	1,809
	その他	8	0	14	22
		スマート家電	端末	合計	
一般消費者向け		38	35	73	

医療・製造等の産業分野での機器の分類が困難であるため、産業分野 6 つ、製品分野3つの、合計 18 分類で整理した。また、一般消費者向けは別途、製品分野2つに分類し、合計 20 分類とした。

なお、各カテゴリについては、以下の詳細な製品品目で分類している。

- ・ 制御機器・コンピュータ: CPU ボード、HPC、NVR、PC、PDA、PLC、ウェアラブル端末、エッジ端末、サーバー、コントローラ、パネル PC 等
- ・ 通信機器・伝送用機器: アクセスポイント、スイッチ、ルーター、ハブ、ゲートウェイ、基地局 等
- ・ 計測機器: センサー、サーマルカメラ 等

製品数が多いカテゴリについては、製品品目毎に抽出することを可能とした。

参考までに、中小企業が販売する一般消費者向けの IoT 製品のリストを次ページに示す。

表 2-2 中小企業が販売する IoT 製品一覧例(一般消費者向け)

製品カテゴリ	製品名	メーカー	用途	業種
プリンタ	小型モバイルプリンター『SM4-31』※無線LAN標準装備	三栄電機株式会社	スマート家電	一般消費者向け
スマート温度計	専用アプリ付きスマート温度計	テイクワンテクノロジ株式会社	スマート家電	一般消費者向け
スマート照明	スマートライト「popIn Aladdin」	popIn株式会社	スマート家電	一般消費者向け
スマート照明	進化するIoTスマート照明「onia」	onia	スマート家電	一般消費者向け
スマート照明	【手軽に照明をIoTに】誰でも使えるマルチコントロール スマートLED電球！	株式会社日昇	スマート家電	一般消費者向け
スマート照明	Siriで簡単操作LEDシーリングライト	株式会社ビームテック	スマート家電	一般消費者向け
スマートスピーカー	ハンズフリー・スマートアシストスピーカー ブラック EMBS-HFSASBK [Bluetooth対応]	Elut エルト(MSネット株式会社)	スマート家電	一般消費者向け
スマートスピーカー	スマートスピーカー ASC-S5 [Bluetooth対応 /Wi-Fi対応]	ラックスマン LUXMAN	スマート家電	一般消費者向け
スマート体重計	スマート体重計 CANZ-S11	LNTTECH	スマート家電	一般消費者向け
スマートリモコン	Switchbot ハブミニ スマートリモコン Switch Bot ホワイト W0202200-GH	SwitchBot スイッチボット	スマート家電	一般消費者向け
スマートリモコン	Nature Remo 3 家電コントローラー REMO-1W3	NATURE ネイチャー	スマート家電	一般消費者向け
スマートリモコン	Nature Remo mini 2 REMO-2W2	NATURE ネイチャー	スマート家電	一般消費者向け
スマートリモコン	eRemote mini イーリモートミニ MINI 家電コントローラー	リンクジャパン LINKS JAPAN	スマート家電	一般消費者向け
スマートリモコン	スマートリモコン	櫻村 KASHIMURA	スマート家電	一般消費者向け
スマートリモコン	eRemote WiFi学習リモコン	リンクジャパン LINKS JAPAN	スマート家電	一般消費者向け
スマートリモコン	スマートプラグ	櫻村 KASHIMURA	スマート家電	一般消費者向け
スマートリモコン	自宅の家電をIoT化「スマート家電リモコン」RS-WFIREX4	ラックシステム RATOC Systems	スマート家電	一般消費者向け
スマートリモコン	Nature Remo mini 2 Premium REMO-2B2	NATURE ネイチャー	スマート家電	一般消費者向け
スマートリモコン	Nature Remo mini 2 Premium REMO-2N2	NATURE ネイチャー	スマート家電	一般消費者向け
スマートリモコン	スマート機器を自在に操る、最新鋭スマートリモコン「LitZERO X」	株式会社ブルーティウム	スマート家電	一般消費者向け
スマートリモコン	どこでも持ち歩けるジェスチャー操作スマートコントローラー「Lit ZERO」	株式会社ブルーティウム	スマート家電	一般消費者向け
スマートリモコン	スマホで家電をコントロール！ オンオフも見えるスマートリモコンeRemotePro	株式会社リンクジャパン	スマート家電	一般消費者向け
スマートリモコン	スマートリモコン「Nature Remo」	Nature Japan 株式会社	スマート家電	一般消費者向け
スマートリモコン	家をまるごとスマートホーム化する「alyssa.play」	株式会社アクセルラボ	スマート家電	一般消費者向け
スマートロック	【Google Assistant対応】スマートロック Qrio Lock (キュリオ ロック) Q-SL2	Qrio キュリオ	スマート家電	一般消費者向け
スマートロック	Qrio Lock専用リモコンキー Qrio Key (キュリオ キー) Q-K1	Qrio キュリオ	スマート家電	一般消費者向け
スマートロック	指紋認証スマートロック付電動アシスト自転車『WELB』ICT連携アプリ	アベントゥーライフ株式会社	スマート家電	一般消費者向け
スマートロック	指紋認証で楽々解錠! スマート バイク ロック	合同会社NEXT WALL	スマート家電	一般消費者向け
スマートロック	鍵の要らない指紋認証型スマート南京錠「TouchLock (タッチロック)」	BIO-key	スマート家電	一般消費者向け
スマートロック	常識をくつがえすスマートロック！	株式会社ビットキー	スマート家電	一般消費者向け
スマートロック	鍵の必要ない時代へ。アプリで鍵を管理！ 自転車スマートロック【bisecu】	bisecu	スマート家電	一般消費者向け
スマートロック	アプリで鍵を管理！ スマートロックSESAME セサミmini	CANDY HOUSE JAPAN	スマート家電	一般消費者向け
スマートロック	次世代スマートロックGIMDOWジンドウ	GIMDOW	スマート家電	一般消費者向け
ロボット掃除機	VR300 ロボット掃除機 コーボルト	フォアベルク VORWERK	スマート家電	一般消費者向け
ロボット掃除機	ロボット掃除機 Take-One ブラック X5	TakeOne テイクワン(テイクワンテクノロジ)	スマート家電	一般消費者向け
ロボット掃除機	VR300 ロボット掃除機 コーボルト	フォアベルク VORWERK	スマート家電	一般消費者向け
ロボット掃除機	X7 ロボット掃除機 Take-One ブラック	TakeOne テイクワン(テイクワンテクノロジ)	スマート家電	一般消費者向け
ロボット掃除機	C28 ロボット掃除機 MAMORU (マモル) ホワイト	Xrobot	スマート家電	一般消費者向け
スマートウォッチ	HMI-AFGTSPK【日本正規品】スマートウォッチ Amazfit GTS ピンク	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170033C01 スマートウォッチ GTR2e Amazfit ブラック	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170025C01 スマートウォッチ Bip U Amazfit ブラック	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170036C01 スマートウォッチ T-Rex Pro ブラック	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170023C01 スマートウォッチ NEO Amazfit ブラック	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170034C10 スマートウォッチ GTS2e Amazfit パープル	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170028C23 スマートウォッチ GTS2 Amazfit ゴールド	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170027Q05 スマートウォッチ GTR2スポーツ Amazfit ブラック	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	SP170029C01 スマートウォッチ X Amazfit ブラック	AMAZFIT アマズフィット	端末	一般消費者向け
スマートウォッチ	NY17BK スマートウォッチ ブラック	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	NY07BK スマートウォッチ SMART R	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	B20BK スマートウォッチ SMART R	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	F18BKGY スマートウォッチ SMART R	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	NY08 SMART R NY08 SMART R	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	W12 SMART R スマートウォッチ ブラック	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	H1BK SMART R スマートウォッチ ブラック	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	Y39PK SMART R スマートウォッチ ピンク	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	Z30 SMART R Z30 SMART R	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	Y13 SMART R Y13 SMART R	スマートR Smart R	端末	一般消費者向け
スマートウォッチ	アリアス スマートウォッチ ブラック WW19041S-BK	アリアス ALIAS	端末	一般消費者向け
スマートウォッチ	アリアス スマートウォッチ ブラック WW20131S-BK	アリアス ALIAS	端末	一般消費者向け
スマートウォッチ	アリアス スマートウォッチ ピンク WW19043S-PK	アリアス ALIAS	端末	一般消費者向け
スマートウォッチ	アリアス スマートウォッチ ブラックガンメタ WW20130S-BKGM	アリアス ALIAS	端末	一般消費者向け
スマートウォッチ	アリアス スマートウォッチ ブラック WW19042S-BK	アリアス ALIAS	端末	一般消費者向け
スマートウォッチ	アリアス スマートウォッチ ファッションネイビー WW20136S-NV	アリアス ALIAS	端末	一般消費者向け
スマートウォッチ	スマートウォッチ P18 ブラック ARW-P18JP-BK	AREA エアリア	端末	一般消費者向け
スマートウォッチ	スマートウォッチ P10 ブラック ARW-P10JP-BK	AREA エアリア	端末	一般消費者向け
スマートウォッチ	スマートウォッチ V23 ブラック ARW-V23JP-BK	AREA エアリア	端末	一般消費者向け
スマートウォッチ	コラン スマートウォッチ ブラック CP-2K	ファーストラニング Fast Running	端末	一般消費者向け
スマートウォッチ	FM5600-2V フランク三浦 スマートウォッチ	フランク三浦 Frank Miura(株式会社ディ)	端末	一般消費者向け
スマートウォッチ	WATCH1-BK スマートウォッチ SOUNDPEATS Watch 1 ブラック	SOUNDPEATS サウンドピーツ(深圳市音)	端末	一般消費者向け
スマートウォッチ	WATCHPRO1-BK スマートウォッチ ブラック	SOUNDPEATS サウンドピーツ(深圳市音)	端末	一般消費者向け
スマートウォッチ	RMA207BK realme Watch S ブラック	realme(シンガ・ジャパン)	端末	一般消費者向け
スマートウォッチ	GOBE2-BL-001 スマートウォッチ GOBE2 ブラック	GOBE ゴビー	端末	一般消費者向け
スマートウォッチ	VSC14DM-DBL0 スマートウォッチ SERENDIPITY Model CX Indigo Sky	ヴェルト VELDT	端末	一般消費者向け

なお、公開情報から選定した製品に加え、以下の情報からも IoT 製品を製造している可能性があるとして、IoT 製品を調査するためのリストを追加で作成した。

(ア) ものづくり補助金の採択者のうち、IoT 関連の製品を製造・販売している可能性がある事業者(477 社)

(イ) IIFES(オートメーション総合展「システム コントロール フェア(SCF)」と「計測展 TOKYO」が統合した展示会)における出展事業者(120 社)

2.2 中小企業へのアプローチ方策に関する検討

その他、本事業に協力可能な中小企業にアプローチする方策を検討するため、IoT 製品のメーカー取引のある可能性がある事業者(メーカー、システムインテグレータ等)、IoT プラットフォーム/サービス事業者、関連団体へのヒアリングを実施し、以下の意見が得られた。

表 2-3 中小企業へのアプローチ方法

事業者名	中小企業へのアプローチに関するご意見
大手メーカーA 社	・ 取引先のセキュリティ確保は課題として考えているが、まずグループ会社のセキュリティ確保が先の課題である。グループ会社の中小企業も対象とできるならば、是非案内したい。
大手メーカーB 社	・ 開発時点からのセキュリティ確保の必要性については課題意識として強く持っている。社内の PSIRT として実施すべきことに関して、中小企業に協力依頼を行う方向は考えられる。
IoT プラットフォーム事業者 C 社	・ サービス提供の際に、複数の IoT 機器を用いており、そのうち中小企業のメーカーもいるため、セキュリティ検証を行うことで、サービスのセキュリティ向上が期待できる。
IoT 関連団体 D	・ 検証事業者及び中小企業を会員に含むため、中小企業への協力依頼は可能。 ・ メールマガジン有しているため、会員以外にも広く事業の案内が可能。
IoT 関連団体 E	・ 組み込み機器のメーカーを会員に含むため、そのうち中小企業への協力依頼は可能。

ただし、大手事業者の多くは中小企業との取引の状況を把握しておらず、自社の製品・システムから見える範囲ではアプローチするには遠いという意見が多かった。また、取引先への依頼は、下請法等の関係もあり、慎重に対応する必要があるという意見も複数得られた。

3. 中小企業へのIoT 機器やIoT 機器の設計書等の提供依頼

第2章において調査・分析を行ったIoT 機器及びIoT 機器に関するもの(実機、設計書、仕様書、取扱説明書、マニュアル、ソースコード、プロトタイプ、システム構成図、ネットワークの設定手順等)の提供依頼を中小企業へ実施した。この際、本事業の内容を中小企業に説明を行った。

3.1 中小企業に対する依頼

3.1.1 説明内容

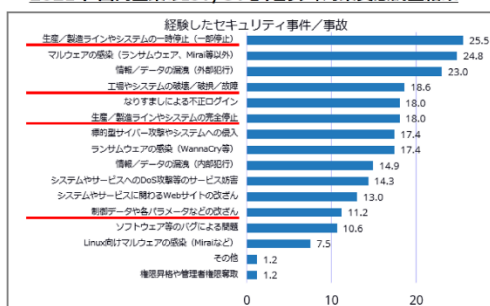
第2章において調査・分析を行ったIoT 機器の製造事業者に対して、IoT 機器及びIoT 機器に関するものの提供依頼を行うために、資料を作成し、説明を実施した。

まず、IoT 機器に対するセキュリティ確保の必要性について理解を促すために、国内企業においてIoT/OTのセキュリティ対策が進んでいない実態やセキュリティ対策の不備による事業への深刻な影響等の事例を説明した。

IoT機器に対するセキュリティ対策の必要性

- DXの進展により、インターネットとIoT機器が繋がりはじめたところであるものの、**セキュリティ事件/事故によるIoT機器やOTシステムの一時停止を約25%の企業が経験している**といった調査結果からも、**こうした機器やシステムでセキュリティ対策を多くの者が導入している**とは言い難い状況。
- 機器に対する十分なセキュリティ対策が実施されず、脆弱性が残存した場合、悪意ある攻撃者によって不正操作や誤作動が実行され、**機器の利用者へ影響を及ぼす恐れ**がある。
- また、**開発企業は脆弱性の対応に追われることとなる**。過去には、**脆弱性によりリコールや利用者による訴訟に発展した事例**もあり、最悪の場合、**開発企業の経営に対して影響を与える可能性**もある。
- 今後さらなる脅威の増加・高度化が想定されるところ、**機器に対するセキュリティ対策の具備が不可欠**。

2021年 国内企業のIoT/OTセキュリティ対策実態調査結果



セキュリティ対策の不備により開発企業に影響を及ぼした事例

- 自動車における脆弱性の検出による140万台のリコール**
販売中の自動車に対して外部から不正アクセス可能な脆弱性が公開された。**顧客からの問い合わせが殺到し、開発企業は140万台のリコールを実施した。リコールの対応には1,000万ドル以上の費用を要した。**
- 心臓ペースメーカーにおける脆弱性の検出による46.5万台のリコール**
販売中の心臓ペースメーカーに対して心拍リズムを外部から制御可能な脆弱性が公開された。**開発企業は市場に流通している46.5万台を対象にリコールを実施した。**
- 脆弱な家庭用ネットワークカメラのメーカーに対する訴訟**
家庭用ネットワークカメラにおいて、認証不備に関する脆弱性が内在し、脆弱性を悪用した不正アクセスが行われた。不正アクセスの被害を受けた複数の利用者により、**開発企業に対して500万ドルを求める集団訴訟**が起こされた。

IDC「2021年 国内企業のIoT/OTセキュリティ対策実態調査」<https://www.idc.com/getdoc.jsp?containerId=prJ147631521>
※ 調査実施：2021年2月、調査対象：国内企業443社

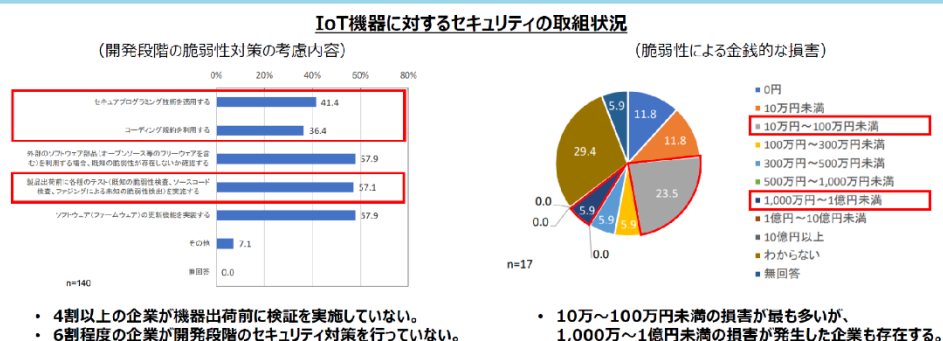
0

図 3-1 IoT 機器に対するセキュリティ対策の必要性

特に、IoT 機器に対する開発段階からの脆弱性対策としては、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があるが、実施は 4 割程度にとどまり、製品出荷前のテスト(6 割弱の実施)と比較して実施率が低い状況にある。十分な脆弱性対策が実施されていないことにより、1,000 万円以上の損害に繋がった事例も存在することを示した。

IoT機器に対するセキュリティの取組状況・本事業の目的

- IoT機器に対するセキュリティの取組においては、「**セキュリティ・バイ・デザイン**」の考えに基づき、設計・開発段階で**セキュリティ対策が適切に導入されていることが必要**。
- 他方で、**開発段階でセキュリティ対策を行っている企業は現状限定的**であり、十分な脆弱性対策が実施されていないことにより、**1,000万円以上の損害に繋がった企業も存在する**。
- 本事業は、セキュリティ・バイ・デザインの考えに立脚し、**開発段階からの脆弱性検証を試験的に実施することで効果的な検証手法を整理するとともに、その効果を可視化し、中小企業による発売前のIoT機器の脆弱性検証を促進すること**を目的とする。



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」<https://www.ipa.go.jp/files/000065094.pdf>
 ※調査実施：2017年11月、調査対象：国内企業205社

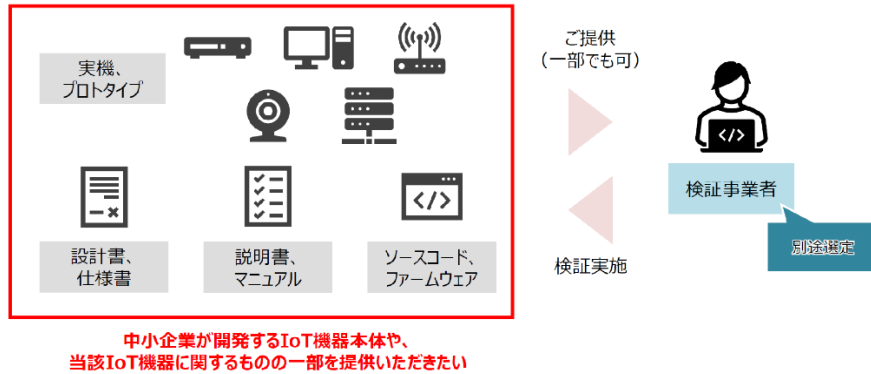
1

図 3-2 IoT 機器に対するセキュリティの取組状況・本事業の目的

中小企業に対する依頼事項としては、開発する IoT 機器に対する脆弱性検証を試験的に実施するために、検証に必要な IoT 機器本体や、当該機器に関するもの(設計書、仕様書、取り扱い説明書、マニュアル、ソースコード、ファームウェア、プロトタイプ、システム構成図、ネットワークの設定手順等)を提供いただきたい旨を示した。提供された IoT 機器に関するものは、別途選定される検証事業者によりセキュリティ検証が実施され、その結果が中小企業にフィードバックされる点を伝えた。また、提供された機器に対する取り扱い(廃棄等)や IoT 機器に関する情報やセキュリティ検証の結果等の機微な情報に関する取り扱いについては、事務局の管理の下、秘密保持契約の締結等の手続きを行う旨を伝えた。

中小企業に対するご協力依頼事項

- 本事業では、**中小企業が開発するIoT機器に対する脆弱性検証を試験的に実施する。**
- **検証に必要なIoT機器本体や、当該IoT機器に関するもの**（設計書、仕様書、取扱説明書、マニュアル、ソースコード、ファームウェア、プロトタイプ、システム構成図、ネットワークの設定手順等）を、**ご協力いただける中小企業よりご提供いただきたい。**（一部のご提供でも可能。）



2

図 3-3 中小企業に対する協力依頼事項

協力企業に対するメリットは、開発する IoT 機器のセキュリティが向上できること、そして第三者の視点によるセキュリティ検証を行うことで、一定レベルのセキュリティが確保できていることを説明可能となる点を伝えた。また、最終的に脆弱性が判明した場合と比較し、開発時点で早期に脆弱性が発見できれば、開発遅延の低減や脆弱性対応工数・コストの削減につながる点もメリットとした。

ご協力いただいた企業に対するメリット

- 本事業で実施するIoT機器に対する脆弱性検証では、中小企業から**ご提供いただいた機器・情報等を踏まえ、一般的な検証手法から適用する検証手法を選定・実施する。**
- 中小企業に協力をいただき、検証を実施することで、**機器やファームウェア等に含まれる脆弱性や脆弱性につながりうるセキュリティ上の懸念事項の検出が想定される。**設計・開発段階にこれらが明らかになることで、**機器のセキュリティレベルの向上**だけでなく、第三者的な検証による**アシュアランス※レベルの向上**が期待される。
- 併せて、開発企業における**開発遅延の低減や対応にかかる工数・コストの削減**につながる。

※ 第三者により実施された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。

ご提供の機器・情報等	想定される検証手法	想定される結果・備考	想定される検証の効果・メリット
設計書、仕様書	設計文書レビュー	機器における不適切なサービスや設定の有無や、不適切なセキュリティ対策の実装の有無等、脆弱性ではないものの、脆弱性につながるセキュリティ上の懸念事項が検出される。 検証範囲は限定的となるが、設計文書のみで検証が可能となるため、機器の調達などの検証準備に係る手間が軽減される。	セキュリティ設計の不備による 開発の遅れや修正にかかるコストを低減 できる 機器全体のセキュリティレベル・アシュアランスレベルを向上 できる
ファームウェア	バイナリ解析	ファームウェアに起因する脆弱性が検出される。（インジェクションの脆弱性、オーバーフローに関する脆弱性、外部ライブラリに依存した脆弱性 等） 検証範囲は限定的となるが、ファームウェアのみで検証が可能となるため、機器の調達などの検証準備に係る手間が軽減される。	脆弱性対応のための 開発の遅れや修正にかかるコストを低減 できる ファームウェアのセキュリティレベルを向上 できる
実機、プロトタイプ	ファームウェア解析、既知脆弱性の診断 等	ソフトウェア、ハードウェア、ファームウェアに内在する様々な脆弱性が検出される。 幅広い範囲を検証可能な一方で、機器の調達などの検証準備に手間がかかる可能性がある。	脆弱性対応のための 開発の遅れや修正にかかるコストを低減 できる 機器全体のセキュリティレベル・アシュアランスレベルを向上 できる

3

図 3-4 協力企業に対するメリット

参考として、IoT 機器に適用される一般的な検証手法を静的手法と動的手法に分類して示した。

【参考】IoT機器に適用されうる一般的な検証手法

分類	一般的な 検証手法	概要	当該検証に最低限必要となる 主な機器・関連情報など
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。	説明書、仕様書等の設計文書
	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。	ソースコード
	ファームウェア解析	機器のファームウェアを抽出する。脆弱性が含まれてい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。	実機／プロトタイプ
	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、不正なアドレス命令が無いことを静的に確認する。	ファームウェア
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。	実機／プロトタイプ
	既知脆弱性の診断	既知の脆弱性が機器に内在しているかを調べ、実際に悪用可能かを確認する。	実機／プロトタイプ
	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。	実機／プロトタイプ
	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。	実機／プロトタイプ

4

図 3-5 IoT 機器に適用されうる一般的な検証手法

なお、本事業の概要や参加するメリットを分かりやすく示すために、中小企業に向けた A4 両面のパンフレットを作成し、説明資料として活用した。

サイバーセキュリティ
のための

IoT機器等に対する 脆弱性検証にご協力いただける 中小企業を募集します

概要・ご協力いただいた場合のメリット

- 中小企業が開発するIoT機器等に対して、**専門家による脆弱性検証を無償で実施**します
- 脆弱性検証を実施することで、機器に含まれる**脆弱性の有無を確認**でき、**機器におけるセキュリティ事故の発生可能性を低減**できるだけでなく、出荷後に脆弱性を修正することに対する**工数やコストの削減**につながります
- 脆弱性検証の結果明らかとなった脆弱性に対して、**検証を実施した専門家により対応策や改善策のご提案**も行います
- 本事業を通じて、**中小企業が保有する重要技術や重要情報が外部に明らかになることはありません**

対象となる「IoT機器等」の例



本事業では、産業用・一般消費者用問わず、ネットワークに常時接続される機器を対象とします

事業概要は以下をご覧ください。
経済産業省 令和3年度補正予算の事業概要(P55)
「開発段階におけるIoT機器の脆弱性検証促進事業」
https://www.meti.go.jp/main/yosan/yosan_fy2021/hosei/pdf/hosei_yosan_pr.pdf

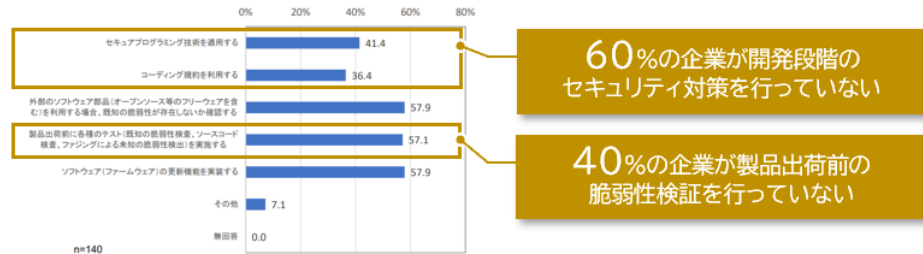


<本事業に関するお問合せ先>
株式会社三菱総合研究所
サイバーセキュリティ戦略グループ
「開発段階におけるIoT機器の脆弱性検証促進事業」事務局
Tel : 03-6858-3578
Email : iot-sec@ml.mri.co.jp

図 3-6 パンフレット(表面)

多くの企業では、開発段階でのセキュリティ対策を実施せず、機器出荷前の検証も実施していません

機器の開発段階における脆弱性対策の考慮状況



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」(2017年)

機器に対する十分な脆弱性対策が実施されていないことで、1,000万円以上の損害につながった企業も存在します

機器に脆弱性が存在した際の金銭的な損害



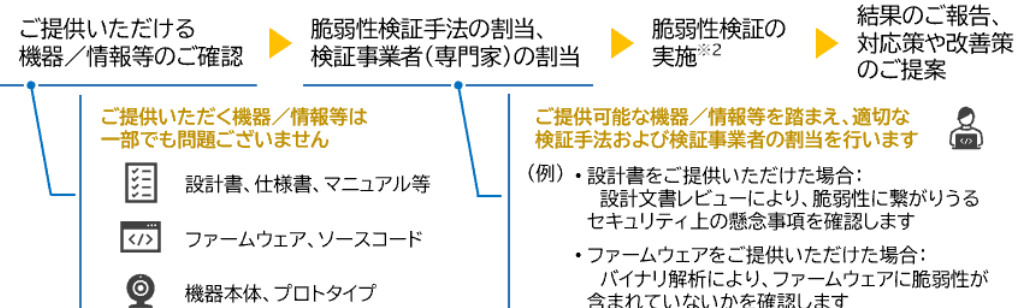
IPA「IoT製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」(2017年)

機器に脆弱性が残存することで、利用者による信頼低下や企業経営に対して影響を及ぼす可能性もあるため、開発段階において機器に対して脆弱性検証を行うことが重要です

本事業にご協力いただくことで・・・

- 通常100万円～700万円を要する脆弱性検証を無償で実施いただけます
- セキュリティ事故の発生可能性を低減できるほか、出荷後に脆弱性を修正することに対する工数やコストの削減につながります
- 明らかとなった脆弱性に対する対応策や改善策の提案を受けることが可能です※1

本事業における脆弱性検証の実施プロセス



※1 脆弱性の修正対応は応募いただいた中小企業様自身にて実施いただきます。

なお、脆弱性への対応にあたっては、中小企業庁「ものづくり補助金」等、別途補助金をご活用いただける可能性もございます。

※2 脆弱性検証は、機器に内在するすべての脆弱性を網羅的に確認できるものではありません。

また、脆弱性検証期間は1ヶ月～3ヶ月程度を予定しています。本事業の募集時期・実施時期は決まり次第別途ご連絡いたします。

図 3-7 パンフレット(裏面)

3.1.2 依頼方法

中小企業に対して架電により依頼を行った。架電リストは代表電話であるため、製品のセキュリティ担当もしくは製品の営業担当、政策や渉外担当等の担当者につながることを依頼し、担当者に対して事業説明を実施した。そこで、関心を持っていた企業の方には、個別にウェブを通じて参加依頼を行う流れとした。

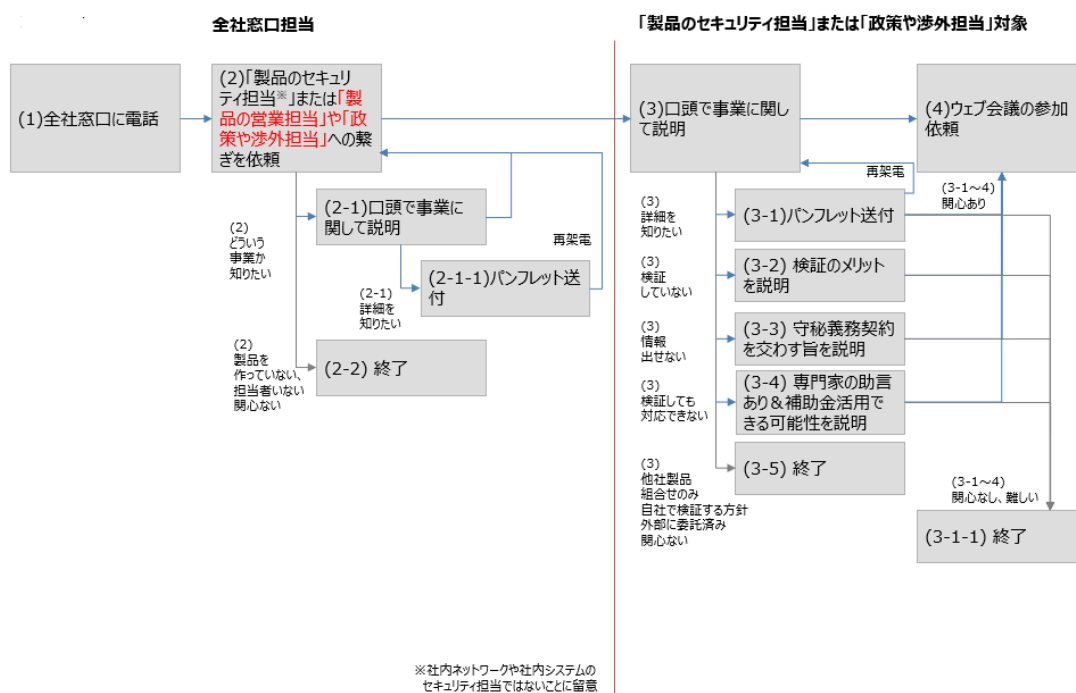


図 3-8 架電フロー

また、電話での対応をスムーズに行うために、FAQ を用意の上、対応を行った。FAQ の内容は以下のとおりである。

表 3-1 架電における FAQ 内容

質問	回答
Q1. セキュリティ検証は有料か。	A1. 無料で実施可能です。
Q2. セキュリティ検証のスケジュールはどうか。	A2. 本事業へのご応募は 4 月以降に開始する予定でして、実際に専門家に確認いただく時期は、2022 年 5 月以降、随時実施していくことになります。確認期間は機器にも依りますが、1 ヶ月～1.5 ヶ月を想定しています。
Q3. 対象とする機器はどのようなものか。	A3. IoT 機器全般を対象としており、一般消費者向けの IoT 機器では、スマート家電、ネットワーク機器、端末等を想定しています。産業用向けでは、制御機器・産業用 PC、通信・ネットワーク機器、センサー周りの計測機器等、幅広く対象としています。
Q4. どのようなものを専門家に提供すればよいのか。	A4. 検証に必要な IoT 機器本体や、当該 IoT 機器に関するもの（設計書、仕様書、取扱説明書、マニュアル、ソースコード、ファームウェア、プロトタイプ、システム構成図、ネットワークの設定手順等）を想定しています。ご協力いただける方が提供可能なもので構いません。
Q5. 専門家から何をもらえるのか。	A5. セキュリティの検証結果レポートと、もしセキュリティ上の課題等があった場合は対応策や改善策についてご提案します。
Q6. 情報の管理はどのように行うのか。	A6. 応募いただいた方と、セキュリティの専門家、及び事務局と、それぞれ守秘義務契約を交わす予定です。
Q7. セキュリティ検証結果は公表されるのか。	A7. セキュリティ検証結果が公表されることはありません。
Q8. 応募者の社名・製品名は公表されるのか。	A8. 現時点で公表の予定はなく、今後も応募者の同意なくして公表することはありません。

4. IoT 機器のセキュリティ検証事業者のリストアップ

IoT 機器に関するもの(実機、設計書、仕様書、取扱説明書、マニュアル、ソースコード、プロトタイプ、システム構成図、ネットワークの設定手順等)に対するセキュリティに関するレビューができる検証事業者を選定し、実績(分野、工数等)、手法、対応可能スケジュール、検証実施の意向等を整理した。本事業では 9 社を選定し、実績、手法、対応可能スケジュール、検証実施の意向等を確認した。

4.1 各検証事業者における対応可能性

各検証事業者における検証の対応可能性として、検証可能な期間、検証可能な製品数、検証を希望する製品数、対応可能な機器メーカーの地域及び一製品あたりの検証予算見込みを確認した。確認結果は表 4-1 に示すとおりである。

検証スケジュールに関して、検証対象となる製品やメーカーより提示される情報によって変動するものの、半数程度の企業が 2022 年 4 月から 2023 年 3 月にかけて各月 2～3 製品程度、合計 15 製品～20 製品程度対応可能とのことであった。対応可能な製品数が限定的な事業者も存在した一方で、各月 5 製品程度、計 60 製品を対応可能との検証事業者も存在した。対応可能な機器メーカーの地域について、機器の郵送が可能である場合、地域に関わらず対応可能であったとした検証事業者が多かった。ただし、機器メーカーの本社や工場など、現地での作業が必要な場合は調整を要することが分かった。

表 4-1 各検証事業者における対応可能性

企業名	検証可能な期間	検証可能な製品数	検証を希望する製品数	対応可能な機器メーカーの地域
1. 検証事業者 A 社	2022 年 4 月 ～ 2023 年 3 月まで	各月 2～3 製品、総計 20 製品程度	20 製品	関東圏及び、大阪を希望。
2. 検証事業者 B 社	2022 年 5 月 ～ 2023 年 2 月まで	3 製品/月	30 製品	機器の郵送が可能である場合は日本全国の機器メーカーの製品について対応可能。現地での作業が必要な場合は要調整。

企業名	検証可能な期間	検証可能な製品数	検証を希望する製品数	対応可能な機器メーカーの地域
3. 検証事業者 C 社	2022 年 4 月 ~ 2023 年 3 月	5 製品/月程度(ハードウェア解析、ネットワークキャプチャ、スキャン、ファームウェア解析まで実施する場合の想定数。ハードウェア解析のみ等の場合さらに実施することも可能。)	60 製品 (内容によってはさらに実施することも可能)	機器郵送が可能であれば機器メーカーに関わらず対応可能。
4. 検証事業者 D 社	2022 年 5 月 ~ 2022 年 3 月まで	2022 年 5 月:1 製品/月、他期間:2 製品/月	21 機種	弊社にて検証を実施させていただきたいため、機器を発送可能であるメーカー様が対象となる。また、検証作業は弊社内で実施を想定。(オンサイトは非対応。)
5. 検証事業者 E 社	2022 年 5 月 ~ 2022 年 12 月まで	2022 年 5 月~2022 年 9 月:3 製品/月 2022 年 10 月~2022 年 12 月:2 製品/月	20 製品	機器の郵送が可能である場合は日本全国の機器メーカーの製品について対応可能。現地対応が必要な場合は、追加費用含め調整させていただく。
6. 検証事業者 F 社	2022 年 4 月 ~ 2023 年 3 月	3 製品/月	指定なし	国内であれば可。
7. 検証事業者 G 社	2022 年 4 月 ~ 2022 年 12 月	期間内に 5 製品	期間内に 5 製品	関東(東京)であれば可。

企業名		検証可能な期間	検証可能な製品数	検証を希望する製品数	対応可能な機器メーカーの地域
8. 検証事業者 H 社		2022 年 4 月 ~ 2023 年 3 月末(通年対応可能だが、実施時期は都度調整。)	期間内に 9 製品	期間内に 6 製品	機器の郵送が可能である場合は日本全国の機器メーカーの製品について対応可能。
9. 検証事業者 I 社	ファジングツールを用いた検証の場合	2022 年 4 月 ~ 2022 年 11 月	2~4 製品/月	14~28 製品	出張対応は離島以外なら OK、機器の郵送が可能である場合は日本全国の機器メーカーの製品について対応可能
	静的解析ツールを用いた検証の場合	2022 年 5 月 ~ 2022 年 12 月	ソースコード規模に依存。50 万行程度なら月 2 製品程度可能。	10 製品	原則オンラインにてソースコードもしくはバイナリ提供可能なものに限定。

4.2 各検証事業者における検証実績・検証対応意向

本節では、選定した各検証事業者における検証手法に関する対応可能性、対象機器・対象分野に関する実績・対応意向の確認結果を示す。

検証手法に関する対応可能性について、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」¹の表 2-1 で記載された一般的な検証手法に対して、「1:対応可能」、「2:条件付きで対応可能」、「3:対応不可」の 3 段階で確認するとともに、「2:条件付きで対応可能」である場合は具体的な条件を確認した。また、検証にあたっての工夫や想定される使用ツールについても確認した。

対象機器・対象分野に関する検証実績については、整理した一般消費者向け IoT 機器・産業用機器・産業分野それぞれに対して「1:実績あり」、「2:実績なし」のどちらに該当するかを確認した。そして、対象機器・対象分野に関する対応意向に関しては、各一般消費者向け IoT 機器・産業用機器・産業分野に対して、「1:是非検証を実施したい」、「2:可能であれば検証を実施したい」、「3:可能であれば検証を実施したくない」、「4:検証を実施したくない(検証実施が困難)」の 4 段階で意向を確認した。なお、すべての事業者の確認結果の比較については次節以降で示す。

¹ <https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html>

4.2.1 検証事業者 A 社

(1) 検証手法に関する対応可能性

検証事業者 A 社において対応可能な検証手法の確認結果を以下に示す。ファームウェア解析・バイナリ解析及びハードウェア解析については、対応不可であるとのことであった。また、静的ソースコードについて、ツールによるコーディング規約の確認やセキュアコーディングの確認が主体であれば対応可能とのことであった。その他の対応可能な検証手法について、Nmap や Wireshark 等の既存のツールを活用した検証を行うほか、規格や過去実績から蓄積されたノウハウを活用することが確認できた。

表 4-2 検証手法に関する対応可能性(検証事業者 A 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	1. 対応可能	—	規格や過去実績から蓄積されたノウハウの活用
静的ソースコード解析	2. 条件付きで対応可能	ツールによるコーディング規約、セキュアコーディングチェック主体	SonarQube、ESLint 等
ファームウェア解析・バイナリ解析	3. 対応不可	—	—
ネットワークスキャン	1. 対応可能	—	Nmap
ファジング	1. 対応可能	—	規格や過去実績から蓄積されたノウハウの活用
ネットワークキャプチャ(通信内容解析)	1. 対応可能	—	Wireshark
ハードウェア解析	3. 対応不可	—	—

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 A 社の検証実績及び検証意向を以下に示す。検証の実績を有さない機器として、ルーター、ハブ・スイッチ、UTM、ゲートウェイ等の通信関連機器が挙げられる一方で、スマートロックやロボット掃除機、スマート TV 等の家庭用 IoT 機器に関して、幅広い実績を有する。検証の実績がない機器を含む多くの機器について、「1. 是非検証を実施したい」又は「2. 可能であれば検証を実施したい」の意向を確認したが、唯一サーマルカメラの検証意向については「4. 検証を実施したくない(検証実施が困難)」であることを確認した。

表 4-3 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 A 社)

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
PC	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
スマートフォン	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
タブレット端末	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
ウェアラブル端末	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
ルーター	2. 実績なし	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
ハブ・スイッチ	2. 実績なし	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
ファイアウォール	1. 実績あり	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
UTM	2. 実績あり	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
ゲートウェイ	2. 実績なし	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
スマートロック	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
ロボット掃除機	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
スマート TV	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
カーナビゲーション	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
サーマルカメラ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
スマート照明	2. 実績なし	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
スマートスピーカー	2. 実績なし	1. 是非検証を実施したい	規格や過去実績から蓄積されたノウハウの活用

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
プリンター	1. 実績あり	1. 是非検証を実施したい	規格や過去実績から蓄積されたノウハウの活用
ドローン	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
その他スマート家電 (冷蔵庫、洗濯機 等)	1. 実績あり	1. 是非検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等

産業用機器等に関する検証事業者 A 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業用機器は産業用のタブレット端末に限られ、実績を有する産業用機器は限定的であった。産業用ルーター、産業用ハブ・スイッチ及び産業用 IoT ゲートウェイの 3 機器については、「4. 検証を実施したくない(検証実施が困難)」という意向を確認した。

表 4-4 産業用機器等に関する検証実績・対応意向(検証事業者 A 社)

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	2. 実績なし	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
産業用タブレット端末	1. 実績あり	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
産業用ルーター	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用ハブ・スイッチ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用 IoT ゲートウェイ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用センサー	2. 実績なし	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等
産業用ウェブカメラ	2. 実績なし	2. 可能であれば検証を実施したい	項目書に沿った機能テスト、探索型テスト、自動テスト等

産業分野に関する検証事業者 A 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は製造業、医療、情報通信事業、自動車、鉄道事業、航空事業の 6 分野であった。検証の実績がない分野を含む多くの分野について、「1. 是非検証を実施したい」又は「2. 可能であれば検証を実施したい」の意向を確認したが、唯一医療分野の検証意向については「4. 検証を実施したくない(検証実施が困難)」であることを確認した。

表 4-5 産業用分野に関する検証実績・対応意向(検証事業者 A 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	1. 実績あり	FA ツール向けソフトウェア検証、券売機等	2. 可能であれば検証を実施したい
医療	1. 実績あり	電子顕微鏡等	4. 検証を実施したくない (検証実施が困難)
電気事業	2. 実績なし	—	2. 可能であれば検証を実施したい
ガス事業	2. 実績なし	—	2. 可能であれば検証を実施したい
水道事業	2. 実績なし	—	2. 可能であれば検証を実施したい
情報通信事業	1. 実績あり	EC サイト、顧客管理システム等	1. 是非検証を実施したい
自動車	1. 実績あり	車載器、ドライブレコーダー、ナビゲーションアプリ、音声認識 AI 等	1. 是非検証を実施したい
鉄道事業	1. 実績あり	FeliCa に付随するサービスの検証等	1. 是非検証を実施したい
航空事業	1. 実績あり	航空券予約システムの検証等	1. 是非検証を実施したい

4.2.2 検証事業者 B 社

(1) 検証手法に関する対応可能性

検証事業者 B 社において対応可能な検証手法の確認結果を以下に示す。静的ソースコード解析については、対応不可であるとのことであった。また、設計文書レビューについては、レビュー対象の文書が 20 ページ程度に収まり、かつ、不明点が生じた場合にメーカーと相談できる体制があること、ファームウェア解析・バイナリ解析については、暗号化されていないファームウェアやバイナリファイルが提供されること、ファジングについては、Web インタフェースに対するファジングであること、ハードウェア解析については、破壊して問題ない機器を複数提供いただき、かつ、UART、SPI、JTAG 等のインタフェースが基板上に存在する場合にそれぞれ対応可能であるとのことであった。その他の対応可能な検証手法について、Nmap や Wireshark 等の既存のツールを活用した検証を行うことが確認できた。

表 4-6 検証手法に関する対応可能性(検証事業者 B 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	2. 条件付きで対応可能	レビュー対象の文書の合計ページ数が 20 ページ程度に収まること。また、不明点が生じた場合にメーカー様と QA 対応できる体制であること。(専門用語や社内用語の理解に齟齬が生じる可能性があるため。)	特定の観点に基づく人手でのレビュー。例えば、認証のロジックに着目し、不備がないか確認する、機微な情報(秘密鍵等)の管理方法が適切であるか確認する、等。
静的ソースコード解析	3. 対応不可	—	—
ファームウェア解析・バイナリ解析	2. 条件付きで対応可能	暗号化されていないファームウェア、バイナリファイルをご提供頂けること。	Binwalk によるファームウェア展開、クレデンシャルの取得可否確認。 Ghidra によるバイナリ解析。クレデンシャルのハードコードや脆弱性の有無確認等。脆弱性の可能性がある場合、機器を動作させて検証できれば、必要に応じて PoC による検証。
ネットワークスキャン	1. 対応可能	—	Nmap による動作サービスの特定。また、各サービスの既知脆弱性調査。
ファジング	2. 条件付きで対応可能	Web インタフェースに対するファジング(動的スキャン等)であれば対応可能。	OWASP ZAP を用いた動的スキャン。また、探索的にパラメータを変更し、問題が発生しないかを確認。
ネットワークキャプチャ(通信内容解析)	1. 対応可能	—	Wireshark による通信の暗号化有無の確認。通信内容が確認できる場合、機微な情報が窃取できないか、通信内容が改ざんされた場合の挙動に問題がないか等の確認。

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
ハードウェア解析	2. 条件付きで対応可能	破壊して問題ない機器を複数台ご提供頂けること。 また、右記のインタフェースが基板上に存在しなかった場合は検証が実施できない。	UART、SPI、JTAG の存在有無を確認し、これらのインタフェースが存在した場合、悪用可否（例：シェルへのアクセス、ファームウェアの抽出等）を確認。

（2）対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 B 社の検証実績及び検証意向を以下に示す。検証の実績を有さない機器として、PC、ウェアラブル端末のほか、ハブ・スイッチ、ファイアウォール、UTM、ゲートウェイ等の通信関連機器が挙げられた。他方で、スマートフォンやタブレット端末、ルーター、スマート TV、カーナビゲーション等の機器については検証の実績を有するとのことであった。表に記載した以外の機器における検証実績について、携帯用ゲーム機や Wi-Fi 付き SD カード、双眼鏡等に対しても検証実績を有するとのことであった。検証の実績がない機器を含む多くの機器について、「2. 可能であれば検証を実施したい」の意向を確認したが、PC については、「3. 可能であれば検証を実施したくない」、そして、ハブ・スイッチ及びスマートロックについては、「4. 検証を実施したくない（検証実施が困難）」であることが確認できた。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法を確認できた。多くの機器に対して、バイナリ解析、ネットワークスキャン及びネットワークキャプチャが実施される。なお、スマートフォンやタブレット端末のアプリに関する解析は Android 端末に限るとのことであった。

表 4-7 一般消費者向け IoT 機器等に関する検証実績・対応意向（検証事業者 B 社）

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ（適用する検証手法、使用ツール 等）
PC	2. 実績なし	3. 可能であれば検証を実施したくない	・バイナリ解析（デスクトップアプリ解析） ・ネットワークスキャン ・ネットワークキャプチャ
スマートフォン	1. 実績あり	2. 可能であれば検証を実施したい	・バイナリ解析（アプリ解析、ただし Android に限る） ・ネットワークスキャン ・ネットワークキャプチャ
タブレット端末	1. 実績あり	2. 可能であれば検証を実施したい	・バイナリ解析（アプリ解析、ただし Android に限る） ・ネットワークスキャン ・ネットワークキャプチャ

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプ ローチ(適用する検証手法、使用ツール 等)
ウェアラブル端末	2. 実績なし	2. 可能であれば検 証を実施したい	—
ルーター	1. 実績あり	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
ハブ・スイッチ	2. 実績なし	4. 検証を実施した くない(検証実施が 困難)	—
ファイアウォール	2. 実績なし	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
UTM	2. 実績なし	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
ゲートウェイ	2. 実績なし	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
スマートロック	2. 実績なし	4. 検証を実施した くない(検証実施が 困難)	—
ロボット掃除機	2. 実績なし	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプロー チ(適用する検証手法、使用ツール 等)
スマート TV	2. 実績なし	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
カーナビゲーション	1. 実績あり	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
ウェブカメラ	1. 実績あり	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
サーマルカメラ	1. 実績あり	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
スマート照明	2. 実績なし	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
スマートスピーカー	1. 実績あり	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
プリンター	1. 実績あり	2. 可能であれば検 証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
ドローン	1. 実績あり	2. 可能であれば検証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
その他スマート家電 (冷蔵庫、洗濯機 等)	1. 実績あり	2. 可能であれば検証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析

産業用機器等に関する検証事業者 B 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業用機器は産業用センサーに限られ、実績を有する産業用機器は限定的であった。他方、検証の意向に関して、ほとんどの機器について「1. 是非検証を実施したい」の意向であることを確認し、「4. 検証を実施したくない(検証実施が困難)」は産業用ハブ・スイッチのみであることを確認した。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法を確認できた。多くの機器に対して、バイナリ解析、ネットワークスキャン及びネットワークキャプチャが実施される。なお、産業用タブレット端末のアプリに関する解析は Android 端末に限るとのことであった。

表 4-8 産業用機器等に関する検証実績・対応意向(検証事業者 B 社)

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	2. 実績なし	1. 是非検証を実施したい	・バイナリ解析(デスクトップアプリ解析) ・ネットワークスキャン ・ネットワークキャプチャ
産業用タブレット端末	2. 実績なし	1. 是非検証を実施したい	・バイナリ解析(アプリ解析、ただし Android に限る) ・ネットワークスキャン ・ネットワークキャプチャ
産業用ルーター	2. 実績なし	1. 是非検証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール等)
産業用ハブ・スイッチ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用 IoT ゲートウェイ	2. 実績なし	1. 是非検証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
産業用センサー	1. 実績あり	1. 是非検証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析
産業用ウェブカメラ	2. 実績なし	1. 是非検証を実施したい	・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 ・ファジング ・ネットワークキャプチャ ・ハードウェア解析

産業分野に関する検証事業者 B 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は製造業、電気事業、情報通信事業、自動車の 4 分野であった。検証の実績がない分野を含む多くの分野について、「2. 可能であれば検証を実施したい」の意向を確認したが、鉄道事業と航空事業の検証意向については「4. 検証を実施したくない(検証実施が困難)」であることを確認した。

表 4-9 産業用分野に関する検証実績・対応意向(検証事業者 B 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	1. 実績あり	産業用 PLC	2. 可能であれば検証を実施したい
医療	2. 実績なし	—	2. 可能であれば検証を実施したい
電気事業	1. 実績あり	スマートメーター	2. 可能であれば検証を実施したい
ガス事業	2. 実績なし	—	2. 可能であれば検証を実施したい
水道事業	2. 実績なし	—	2. 可能であれば検証を実施したい
情報通信事業	1. 実績あり	ルーター	2. 可能であれば検証を実施したい
自動車	1. 実績あり	カーナビ	2. 可能であれば検証を実施したい
鉄道事業	2. 実績なし	—	4. 検証を実施したくない(検証実施が困難)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
航空事業	2. 実績なし	—	4. 検証を実施したくない(検証実施が困難)

4.2.3 検証事業者 C 社

(1) 検証手法に関する対応可能性

検証事業者 C 社において対応可能な検証手法の確認結果を以下に示す。ファジングを除くすべての検証手法について「1. 対応可能」であり、ファジングについても「2. 条件付きで対応可能」とのことであった。ファジングについては、グレーボックスファジングであれば対応可能だが、ブラックボックスファジングの場合、通信プロトコルに応じて相談とのことであった。具体的には、CAN や TCP/IP 等であればブラックボックスファジングであっても対応可能だが、Bluetooth や Wi-Fi は応相談とのことであった。その他の対応可能な検証手法について、IDA Pro、Nmap、Nessus、tcpdump、Wireshark 等の既存のツールを活用した検証を行うことが確認できた。

表 4-10 検証手法に関する対応可能性(検証事業者 C 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	1. 対応可能	—	—
静的ソースコード解析	1. 対応可能	—	—
ファームウェア解析・バイナリ解析	1. 対応可能	—	IDA Pro
ネットワークスキャン	1. 対応可能	—	Nmap、Nessus
ファジング	2. 条件付きで対応可能	グレーボックスファジング：可能、ブラックボックスファジング：通信プロトコルに応じて相談(CAN、TCP/IP 等可能、BL、Wi-Fi 応相談)	AFL、cangen
ネットワークキャプチャ(通信内容解析)	1. 対応可能	—	tcpdump、Wireshark
ハードウェア解析	1. 対応可能	—	—

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 C 社の検証実績及び検証意向を以下に示す。検証の実績を有さない機器は、ウェアラブル端末、UTM、サーマルカメラ、スマート照明、スマートスピーカーの 5 機器と限定的であり、多くの機器に関する検証実績を有していることを確認した。表に記載した以外の機器における検証実績について、スマートリモコン、プロ用のカメラ、ゲーム機等に対しても検

証実績を有するとのことであった。検証の実績がない機器を含むすべての機器について、「1. 是非検証を実施したい」の意向を確認した。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法を確認できた。多くの機器に対して、ファームウェアの静的・動的解析、通信解析、ファジングが実施されることを確認した。

表 4-11 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 C 社)

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
PC	1. 実績あり	1. 是非検証を実施したい	アプリケーションの静的・動的解析、通信解析、ファジング
スマートフォン	1. 実績あり	1. 是非検証を実施したい	アプリケーションの静的・動的解析、通信解析、ファジング
タブレット端末	1. 実績あり	1. 是非検証を実施したい	アプリケーションの静的・動的解析、通信解析、ファジング
ウェアラブル端末	2. 実績なし	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
ルーター	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
ハブ・スイッチ	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
ファイアウォール	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
UTM	2. 実績なし	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
ゲートウェイ	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
スマートロック	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
ロボット掃除機	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
スマート TV	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
カーナビゲーション	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
サーマルカメラ	2. 実績なし	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
スマート照明	2. 実績なし	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
スマートスピーカー	2. 実績なし	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
プリンター	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
ドローン	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
その他スマート家電 (冷蔵庫、洗濯機 等)	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング

産業用機器等に関する検証事業者 C 社の検証実績及び検証意向を以下に示す。検証の実績がない産業用機器は産業用センサーに限られ、多くの機器について検証実績があることを確認できた。表に記載以外の機器に関する実績について、車載 ECU に関する検証実績を有するとのことであった。そして、検証の意向に関して、すべての機器について「1. 是非検証を実施したい」の意向であることを確認した。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法を確認できた。多くの機器に対して、ファームウェアの静的・動的解析、通信解析、ファジングが実施されることを確認した。

表 4-12 産業用機器等に関する検証実績・対応意向(検証事業者 C 社)

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	1. 実績あり	1. 是非検証を実施したい	アプリケーションの静的・動的解析、通信解析、ファジング
産業用タブレット端末	1. 実績あり	1. 是非検証を実施したい	アプリケーションの静的・動的解析、通信解析、ファジング
産業用ルーター	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
産業用ハブ・スイッチ	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
産業用 IoT ゲートウェイ	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング
産業用センサー	2. 実績なし	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	ファームウェアの静的・動的解析、通信解析、ファジング

産業分野に関する検証事業者 C 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は製造業、電気事業、情報通信事業、自動車の 4 分野であったが、検証の実績がない分野を含むすべての分野について、「1. 是非検証を実施したい」の意向を確認した。

表 4-13 産業用分野に関する検証実績・対応意向(検証事業者 C 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	1. 実績あり	工場用 PC	1. 是非検証を実施したい
医療	2. 実績なし	—	1. 是非検証を実施したい
電気事業	1. 実績あり	電力メーター、従業員現地操作用タブレット	1. 是非検証を実施したい
ガス事業	2. 実績なし	—	1. 是非検証を実施したい
水道事業	2. 実績なし	—	1. 是非検証を実施したい
情報通信事業	1. 実績あり	産業用ルーター、スイッチ	1. 是非検証を実施したい
自動車	1. 実績あり	自動車 ECU、自動車本体	1. 是非検証を実施したい
鉄道事業	2. 実績なし	—	1. 是非検証を実施したい
航空事業	2. 実績なし	—	1. 是非検証を実施したい

4.2.4 検証事業者 D 社

(1) 検証手法に関する対応可能性

検証事業者 D 社において対応可能な検証手法の確認結果を以下に示す。設計文書レビュー及び静的ソースコード解析については、対応不可であるとのことであった。また、ファジングについては、ファームウェア解析やバイナリ解析を実施した上で必要があると判断した場合に実施、ハードウェア解析についてはデバッグポートの検証の範囲内で対応可能であるとのことであった。その他の対応可能な検証手法について、Ghidra、Nmap、netstat、Wireshark 等の既存のツールを活用した検証を行うことが確認できたほか、ファジングについては独自プログラムを作成することで検証する方針が確認できた。

表 4-14 検証手法に関する対応可能性(検証事業者 D 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	3. 対応不可	—	—
静的ソースコード解析	3. 対応不可	—	—
ファームウェア解析・バイナリ解析	1. 対応可能	—	Ghidra
ネットワークスキャン	1. 対応可能	—	Nmap、netstat
ファジング	2. 条件付きで対応可能	ファームウェア解析やバイナリ解析を行った上で必要である場合に実施を行います。	ファームウェア解析やバイナリ解析により独自プログラムを作成し検証を行います。
ネットワークキャプチャ(通信内容解析)	1. 対応可能	—	Wireshark
ハードウェア解析	2. 条件付きで対応可能	デバッグポートの検証を想定しています。	JTAG ツール

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 D 社の検証実績及び検証意向を以下に示す。検証の実績を有さない機器は、スマートフォン、ウェアラブル端末、ファイアウォール、スマート照明、スマートスピーカー、プリンターの 6 機器と限定的であり、多くの機器に関する検証実績を有していることを確認した。表に記載した以外の機器における検証実績について、モバイル Wi-Fi ルーター、スマートリモコン、エアコン等に対しても検証実績を有するとのことであった。検証の実績がない機器を含め多くの機器について、「1. 是非検証を実施したい」又は「2. 可能であれば検証を実施したい」の意向であることを確認した。一方で、実績のないスマートフォン及びプリンターについては、「4. 検証を実施したくない(検証実施が困難)」の意向であることを確認した。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法を確認できた。ルーター、ハブ・スイッチ等のネットワーク関連機器に対しては Web 管理画面の脆弱性確認が中心となるほか、その他の機器については、ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証等が実施されることを確認した。

表 4-15 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 D 社)

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
PC	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、既知の脆弱性スキャン、バイナリ解析
スマートフォン	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
タブレット端末	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、既知の脆弱性スキャン、バイナリ解析
ウェアラブル端末	2. 実績なし	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
ルーター	1. 実績あり	2. 可能であれば検証を実施したい	Web 管理画面の脆弱性確認のみを想定。
ハブ・スイッチ	1. 実績あり	2. 可能であれば検証を実施したい	Web 管理画面の脆弱性確認のみを想定。
ファイアウォール	2. 実績なし	2. 可能であれば検証を実施したい	Web 管理画面の脆弱性確認のみを想定。
UTM	1. 実績あり	2. 可能であれば検証を実施したい	Web 管理画面の脆弱性確認のみを想定。
ゲートウェイ	1. 実績あり	2. 可能であれば検証を実施したい	Web 管理画面の脆弱性確認のみを想定。
スマートロック	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
ロボット掃除機	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
スマート TV	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
カーナビゲーション	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
サーマルカメラ	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
スマート照明	2. 実績なし	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
スマートスピーカー	2. 実績なし	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
プリンター	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ドローン	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
その他スマート家電(冷蔵庫、洗濯機 等)	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証

産業用機器等に関する検証事業者 D 社の検証実績及び検証意向を以下に示す。検証の実績がない産業用機器は産業用タブレット端末及び産業用センサーに限られ、多くの機器について検証実績があることを確認できた。表に記載以外の機器に関する実績について、車載 ECU、産業用サーバー、入退室管理システムに関する検証実績を有するとのことであった。そして、検証の意向に関して、すべての機器について「1. 是非検証を実施したい」の意向であることを確認した。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法を確認できた。多くの機器に対して、ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証が実施されることを確認した。

表 4-16 産業用機器等に関する検証実績・対応意向(検証事業者 D 社)

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、既知の脆弱性スキャン、バイナリ解析
産業用タブレット端末	2. 実績なし	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、既知の脆弱性スキャン、バイナリ解析
産業用ルーター	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
産業用ハブ・スイッチ	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
産業用 IoT ゲートウェイ	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
産業用センサー	2. 実績なし	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証
産業用ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	ネットワークスキャン、通信内容解析、バイナリ解析、デバッグポートの検証

産業分野に関する検証事業者 D 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は医療、情報通信事業、自動車の 3 分野であったが、検証の実績がない分野を含むすべての分野について、「1. 是非検証を実施したい」の意向を確認した。

表 4-17 産業用分野に関する検証実績・対応意向(検証事業者 D 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	2. 実績なし	—	1. 是非検証を実施したい
医療	1. 実績あり	AED、医療系カメラ本体、システム全体	1. 是非検証を実施したい
電気事業	2. 実績なし	—	1. 是非検証を実施したい
ガス事業	2. 実績なし	—	1. 是非検証を実施したい
水道事業	2. 実績なし	—	1. 是非検証を実施したい
情報通信事業	1. 実績あり	基地局	1. 是非検証を実施したい
自動車	1. 実績あり	自動車 ECU、自動車本体	1. 是非検証を実施したい
鉄道事業	2. 実績なし	—	1. 是非検証を実施したい
航空事業	2. 実績なし	—	1. 是非検証を実施したい

4.2.5 検証事業者 E 社

(1) 検証手法に関する対応可能性

検証事業者 E 社において対応可能な検証手法の確認結果を以下に示す。設計文書レビューを除くすべての検証手法について「1. 対応可能」であり、設計文書レビューについても「2. 条件付きで対応可能」とのことであった。設計文書レビューについては、リスクの洗い出しまでの対応であれば可能とのことであった。その他の対応可能な検証手法について、Klockwork、Binwalk、IDA Pro、Ghidra、Nessus、Nmap、Defensics、Wireshark 等の既存のツールを活用した検証を行うことが確認できた。

表 4-18 検証手法に関する対応可能性(検証事業者 E 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	2. 条件付きで対応可能	リスクの洗い出しまでの対応なら可能	脅威分析・リスクアセスメントにより残存リスクがあるかを検証
静的ソースコード解析	1. 対応可能	—	Klocwork、Fortify SCA、Coverity、Sparrow SAST
ファームウェア解析・バイナリ解析	1. 対応可能	—	Binwalk、IDA Pro、Ghidra、Binary Ninja

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
ネットワークスキャン	1. 対応可能	—	Nessus、Nmap
ファジング	1. 対応可能	—	Defensics、Mayhem
ネットワークキャプチャ(通信内容解析)	1. 対応可能	—	Wireshark、無線通信キャプチャ(Bluetooth、Wi-Fi、ZigBee)
ハードウェア解析	1. 対応可能	—	Attify BadgeREX-USB61/62、Saleae Logic Pro8

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 E 社の検証実績及び検証意向を以下に示す。検証の実績を有する機器として、スマートフォン、タブレット端末等のモバイル端末のほか、ルーター、ハブ・スイッチ等の通信機器、カーナビゲーションシステムやサーマルカメラ等に関する実績も挙げられた。表に記載した以外の機器における検証実績について、ヘルスケア機器(血圧計等)や空調リモートコントローラに対しても検証実績を有するとのことであった。検証の実績がない機器を含むすべての機器について、「1. 是非検証を実施したい」の意向を確認した。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法及び具体的な使用ツールを確認できた。

表 4-19 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 E 社)

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
PC	2. 実績なし	1. 是非検証を実施したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析)(Wireshark、Burp Suite) ・無線通信解析(Wireshark) ・ファジング(Protocol fuzzer community edition) ・パスワード解析(John the Ripper、hashcat) ・認証回避(Hydra、Wireshark) ・振舞い解析(Wireshark、Burp Suite) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(Binwalk、Ghidra)

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適 用する検証手法、使用ツール 等)
スマートフォン	1. 実績あり	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite) ・無線通信解析(tcpdump、hcidump) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio、 SQLMap、ADB-tools) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF、ADB-tools、 apktool、Android Studio、Xcode、 appie、Strings)
タブレット端末	1. 実績あり	1. 是非検証を実施 したい	同上
ウェアラブル端末	2. 実績なし	1. 是非検証を実施 したい	同上
ルーター	1. 実績あり	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite) ・無線通信解析(Wireshark) ・ファジング(Protocol fuzzer community edition) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(Hydra、Wireshark) ・振舞い解析(Wireshark、Burp Suite) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(Binwalk、Ghidra)
ハブ・スイッチ	1. 実績あり	1. 是非検証を実施 したい	同上
ファイアウォール	1. 実績あり	1. 是非検証を実施 したい	同上

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適 用する検証手法、使用ツール 等)
UTM	2. 実績なし	1. 是非検証を実施 したい	同上
ゲートウェイ	1. 実績あり	1. 是非検証を実施 したい	同上
スマートロック	2. 実績なし	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite) ・無線通信解析(tcpdump) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF)
ロボット掃除機	2. 実績なし	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite) ・無線通信解析(tcpdump) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF、ADB-tools、 apktool、Android Studio、Xcode、 appie、Strings)

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適 用する検証手法、使用ツール 等)
スマート TV	2. 実績なし	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite) ・無線通信解析(tcpdump) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF)
カーナビゲーション	1. 実績あり	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus、 Nikto) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite、Kismet) ・無線通信解析(Wireshark、ubertooth- tools、bluez-tools、Kismet) ・ファジング(Protocol fuzzer community edition) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(Hydra、Wireshark) ・振舞い解析(Wireshark、Burp Suite) ・ストレージ・データ解析(SQLite、SQLMap、 Tera Term、dd) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(Binwalk、Ghidra、 MobSF、Strings)

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適 用する検証手法、使用ツール 等)
ウェブカメラ	2. 実績なし	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite) ・無線通信解析(tcpdump) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF)
サーマルカメラ	1. 実績あり	1. 是非検証を実施 したい	同上
スマート照明	1. 実績あり	1. 是非検証を実施 したい	同上
スマートスピー カー	2. 実績なし	1. 是非検証を実施 したい	同上
プリンター	2. 実績なし	1. 是非検証を実施 したい	同上
ドローン	1. 実績あり	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析) (Wireshark、Burp Suite) ・無線通信解析(tcpdump、ubertooth- tools、Hackrf-tools) ・パスワード解析(John the Ripper、 hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio、 SQLMap、ADB-tools) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF、Binwalk、 Strings)

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
その他スマート家電(冷蔵庫、洗濯機 等)	2. 実績なし	1. 是非検証を実施したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析)(Wireshark、Burp Suite) ・無線通信解析(tcpdump) ・パスワード解析(John the Ripper、hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio、SQLMap) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF)

産業用機器等に関する検証事業者 E 社の検証実績及び検証意向を以下に示す。検証の実績がある産業用機器として、産業用 PC・ワークステーションや産業用ルーター、産業用ハブ・スイッチ、産業用 IoT ゲートウェイが挙げられた。表に記載以外の機器に関する実績について、表示器やローカル 5G システムに関する検証実績を有するとのことであった。そして、検証の意向に関して、すべての機器について「1. 是非検証を実施したい」の意向であることを確認した。また、各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法及び具体的な使用ツールを確認できた。

表 4-20 産業用機器等に関する検証実績・対応意向(検証事業者 E 社)

産業用機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	1. 実績あり	1. 是非検証を実施したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析)(Wireshark、Burp Suite) ・無線通信解析(Wireshark) ・ファジング(Protocol fuzzer community edition) ・パスワード解析(John the Ripper、hashcat) ・認証回避(Hydra、Wireshark) ・振舞い解析(Wireshark、Burp Suite) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(Binwalk、Ghidra)

産業用機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール等)
産業用タブレット 端末	2. 実績なし	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析)(Wireshark、Burp Suite) ・無線通信解析(tcpdump、hcidump、bluez-tools) ・パスワード解析(John the Ripper、hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio、SQLMap、ADB-tools) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF、ADB-tools、apktool、Android Studio、Xcode、appie、Strings)
産業用ルーター	1. 実績あり	1. 是非検証を実施 したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析)(Wireshark) ・無線通信解析(Wireshark) ・ファジング(Protocol fuzzer community edition) ・パスワード解析(John the Ripper、hashcat) ・認証回避(Hydra、Wireshark) ・振舞い解析(Wireshark、Burp Suite) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(Binwalk、Ghidra)
産業用ハブ・スイッチ	1. 実績あり	1. 是非検証を実施 したい	同上
産業用 IoT ゲート ウェイ	1. 実績あり	1. 是非検証を実施 したい	同上

産業用機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用センサー	2. 実績なし	1. 是非検証を実施したい	・通信内容解析(ペイロード解析)(Wireshark、Burp Suite) ・無線通信解析(tcpdump、ubertooth-tools、Hackrf-tools、Killerbee) ・振舞い解析(tcpdump)
産業用ウェブカメラ	2. 実績なし	1. 是非検証を実施したい	・ネットワークスキャン(Nmap、Nessus) ・通信内容解析(ペイロード解析)(Wireshark、Burp Suite) ・無線通信解析(tcpdump) ・パスワード解析(John the Ripper、hashcat) ・認証回避(tcpdump) ・振舞い解析(tcpdump) ・ストレージ・データ解析(DB Browser for SQLite、MongoDB Realm Studio、SQLMap) ・既知の脆弱性スキャン(Nessus) ・コードパターン解析(MobSF)

産業分野に関する検証事業者 E 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は製造業、医療、情報通信事業、自動車の 4 分野であったが、検証の実績がない分野を含むすべての分野について、「1. 是非検証を実施したい」の意向を確認した。

表 4-21 産業用分野に関する検証実績・対応意向(検証事業者 E 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	1. 実績あり	産業機器	1. 是非検証を実施したい
医療	1. 実績あり	ヘルスケア機器	1. 是非検証を実施したい
電気事業	2. 実績なし	—	1. 是非検証を実施したい
ガス事業	2. 実績なし	—	1. 是非検証を実施したい
水道事業	2. 実績なし	—	1. 是非検証を実施したい
情報通信事業	1. 実績あり	ルーター等	1. 是非検証を実施したい
自動車	1. 実績あり	自動車 ECU	1. 是非検証を実施したい
鉄道事業	2. 実績なし	—	1. 是非検証を実施したい
航空事業	2. 実績なし	—	1. 是非検証を実施したい

4.2.6 検証事業者 F 社

(1) 検証手法に関する対応可能性

検証事業者 F 社において対応可能な検証手法の確認結果を以下に示す。なお、検証事業者 F 社では、所属企業である大日本印刷、サイバートラスト、ベルウクリエイティブ、ストーンビートセキュリティの検証者によって診断予定とのことであった。確認の結果、すべての検証手法について対応可能であるとのことであった。

表 4-22 検証手法に関する対応可能性(検証事業者 F 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	1. 対応可能	—	—
静的ソースコード解析	1. 対応可能	—	—
ファームウェア解析・バイナリ解析	1. 対応可能	—	—
ネットワークスキャン	1. 対応可能	—	専任の診断員が対応、ツールは非公開
ファジング	1. 対応可能	—	—
ネットワークキャプチャ(通信内容解析)	1. 対応可能	—	専任の診断員が対応、ツールは非公開
ハードウェア解析	1. 対応可能	—	—

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 F 社の検証実績及び検証意向を以下に示す。検証実績を有する機器として、PC、スマートフォン、タブレット端末等の情報端末や、ルーター、ハブ・スイッチ、UTM といったネットワーク機器、そしてスマートロックやロボット掃除機等の家庭用 IoT 機器などが挙げられた。検証の実績がない機器を含む多くの機器について、「1. 是非検証を実施したい」の意向を確認したが、唯一ファイアウォールの検証意向については「3. 可能であれば検証を実施したくない」であることを確認した。

表 4-23 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 F 社)

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
PC	1. 実績あり	1. 是非検証を実施したい	—

一般消費者向け IoT 機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプ ローチ(適用する検証手法、使用ツール 等)
スマートフォン	1. 実績あり	1. 是非検証を実施 したい	—
タブレット端末	1. 実績あり	1. 是非検証を実施 したい	—
ウェアラブル端末	1. 実績あり	1. 是非検証を実施 したい	—
ルーター	1. 実績あり	1. 是非検証を実施 したい	—
ハブ・スイッチ	1. 実績あり	1. 是非検証を実施 したい	—
ファイアウォール	2. 実績なし	3. 可能であれば検 証を実施したくない	—
UTM	1. 実績あり	1. 是非検証を実施 したい	—
ゲートウェイ	2. 実績なし	1. 是非検証を実施 したい	—
スマートロック	1. 実績あり	1. 是非検証を実施 したい	—
ロボット掃除機	1. 実績あり	1. 是非検証を実施 したい	—
スマート TV	2. 実績なし	1. 是非検証を実施 したい	—
カーナビゲーション	1. 実績あり	1. 是非検証を実施 したい	—
ウェブカメラ	1. 実績あり	1. 是非検証を実施 したい	—
サーマルカメラ	2. 実績なし	1. 是非検証を実施 したい	—
スマート照明	2. 実績なし	1. 是非検証を実施 したい	—
スマートスピーカー	2. 実績なし	1. 是非検証を実施 したい	—
プリンター	2. 実績なし	1. 是非検証を実施 したい	—
ドローン	1. 実績あり	1. 是非検証を実施 したい	—

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
その他スマート家電(冷蔵庫、洗濯機 等)	2. 実績なし	1. 是非検証を実施したい	—

産業用機器等に関する検証事業者 F 社の検証実績及び検証意向を以下に示す。確認の結果、すべての産業用機器に関する実績を有しており、また、すべての産業用機器に対する検証意向について「1. 是非検証を実施したい」の意向であることが分かった。また、表に記載以外の機器に関する実績について、ロボットアームやムービングベルトに関する検証実績を有するとのことであった。

表 4-24 産業用機器等に関する検証実績・対応意向(検証事業者 F 社)

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	1. 実績あり	1. 是非検証を実施したい	—
産業用タブレット端末	1. 実績あり	1. 是非検証を実施したい	—
産業用ルーター	1. 実績あり	1. 是非検証を実施したい	—
産業用ハブ・スイッチ	1. 実績あり	1. 是非検証を実施したい	—
産業用 IoT ゲートウェイ	1. 実績あり	1. 是非検証を実施したい	—
産業用センサー	1. 実績あり	1. 是非検証を実施したい	—
産業用ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	—

産業分野に関する検証事業者 F 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は製造業、医療、電気事業、水道事業、情報通信事業、自動車の 6 分野であった。検証の実績がない分野を含むすべての分野について、「1. 是非検証を実施したい」の意向であること確認した。

表 4-25 産業用分野に関する検証実績・対応意向(検証事業者 F 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	1. 実績あり	工場用 PC、サーバー、産業用機械	1. 是非検証を実施したい

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
医療	1. 実績あり	通信機器	1. 是非検証を実施したい
電気事業	1. 実績あり	通信機器	1. 是非検証を実施したい
ガス事業	2. 実績なし	—	1. 是非検証を実施したい
水道事業	1. 実績あり	通信機器、スマートメーター	1. 是非検証を実施したい
情報通信事業	1. 実績あり	通信機器	1. 是非検証を実施したい
自動車	1. 実績あり	通信機器、車載器	1. 是非検証を実施したい
鉄道事業	2. 実績なし	—	1. 是非検証を実施したい
航空事業	2. 実績なし	—	1. 是非検証を実施したい

4.2.7 検証事業者 G 社

(1) 検証手法に関する対応可能性

検証事業者 G 社において対応可能な検証手法の確認結果を以下に示す。確認の結果、対応可能な検証手法は、ネットワークスキャン、ファジング、ネットワークキャプチャの 3 手法であり、静的ソースコード解析とファームウェア解析・バイナリ解析については、機種に依存して対応可能とのことであった。

表 4-26 検証手法に関する対応可能性(検証事業者 G 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	3. 対応不可	—	—
静的ソースコード解析	2. 条件付きで対応可能	機種に依る	—
ファームウェア解析・バイナリ解析	2. 条件付きで対応可能	機種に依る	—
ネットワークスキャン	1. 対応可能	—	—
ファジング	1. 対応可能	—	—
ネットワークキャプチャ(通信内容解析)	1. 対応可能	—	—
ハードウェア解析	3. 対応不可	—	—

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 G 社の検証実績及び検証意向を以下に示す。確認の結果、検証実績を有する機器は存在せず、検証の意向がある機器はタブレット端末のみであることが分かった。

表 4-27 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 G 社)

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
PC	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
スマートフォン	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
タブレット端末	2. 実績なし	2. 可能であれば検証を実施したい	—
ウェアラブル端末	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ルーター	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ハブ・スイッチ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ファイアウォール	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
UTM	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ゲートウェイ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
スマートロック	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ロボット掃除機	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
スマート TV	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
カーナビゲーション	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ウェブカメラ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
サーマルカメラ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
スマート照明	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
スマートスピーカー	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
プリンター	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ドローン	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
その他スマート家電 (冷蔵庫、洗濯機 等)	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—

産業用機器等に関する検証事業者 G 社の検証実績及び検証意向を以下に示す。確認の結果、検証実績を有する産業用機器は存在せず、検証の意向がある機器は産業用 PC・ワークステーションと産業用 IoT ゲートウェイであることが分かった。

表 4-28 産業用機器等に関する検証実績・対応意向(検証事業者 G 社)

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	2. 実績なし	2. 可能であれば検証を実施したい	—
産業用タブレット端末	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用ルーター	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用ハブ・スイッチ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用 IoT ゲートウェイ	2. 実績なし	2. 可能であれば検証を実施したい	—
産業用センサー	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
産業用ウェブカメラ	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—

産業分野に関する検証事業者 G 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は存在しないが、製造業、医療、情報通信事業の 3 分野において「2. 可能であれば検証を実施

したい」の意向であることを確認した。

表 4-29 産業用分野に関する検証実績・対応意向(検証事業者 G 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	2. 実績なし	—	2. 可能であれば検証を実施したい
医療	2. 実績なし	—	2. 可能であれば検証を実施したい
電気事業	2. 実績なし	—	4. 検証を実施したくない (検証実施が困難)
ガス事業	2. 実績なし	—	4. 検証を実施したくない (検証実施が困難)
水道事業	2. 実績なし	—	4. 検証を実施したくない (検証実施が困難)
情報通信事業	2. 実績なし	—	2. 可能であれば検証を実施したい
自動車	2. 実績なし	—	4. 検証を実施したくない (検証実施が困難)
鉄道事業	2. 実績なし	—	4. 検証を実施したくない (検証実施が困難)
航空事業	2. 実績なし	—	4. 検証を実施したくない (検証実施が困難)

4.2.8 検証事業者 H 社

(1) 検証手法に関する対応可能性

検証事業者 H 社において対応可能な検証手法の確認結果を以下に示す。静的ソースコード解析及びハードウェア解析をすべての検証手法について「1. 対応可能」もしくは「2. 条件付きで対応可能」であることを確認した。ファームウェア解析・バイナリ解析については、INTEL 系 CPU に限ること、ネットワークスキャン、ファジング、ネットワークキャプチャについては、TCP/IP 及び一般的な上位プロトコルの場合に対応可能であることを確認した。具体的な使用ツールについて、Ghidra、Nmap、Nessus、Wireshark 等の既存のツールを活用した検証を行うことが確認できた。

表 4-30 検証手法に関する対応可能性(検証事業者 H 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	1. 対応可能	—	脅威分析、アセスメント
静的ソースコード解析	3. 対応不可	—	—
ファームウェア解析・バイナリ解析	2. 条件付きで対応可能	INTEL 系 CPU に限る	Ghidra などのリバースエンジニアリングツール
ネットワークスキャン	2. 条件付きで対応可能	TCP/IP 及び一般的な上位プロトコルに限る	Nmap, Nessus などの脆弱性スキャンツール
ファジング	2. 条件付きで対応可能	TCP/IP 及び一般的な上位プロトコルに限る	プロトコルに応じた各種ツール
ネットワークキャプチャ(通信内容解析)	2. 条件付きで対応可能	TCP/IP 及び一般的な上位プロトコルに限る	Wireshark などのネットワークアナライザ
ハードウェア解析	3. 対応不可	—	—

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向け IoT 機器等に関する検証事業者 H 社の検証実績及び検証意向を以下に示す。検証の実績を有する機器として、PC、ウェブカメラ、その他スマート家電(冷蔵庫、洗濯機等)に関する実績を有することを確認した。検証の意向に関して、実績のある PC、ウェブカメラ、その他スマート家電(冷蔵庫、洗濯機等)については、「1. 是非検証を実施したい」の意向、ルーター、ハブ・スイッチ、ファイアウォールについては、「2. 可能であれば検証を実施したい」の意向であることを確認した。各機器の検証実施にあたって想定されるアプローチについて、適用する検証手法及び具体的な使用ツールを確認できた。

表 4-31 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 H 社)

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール等)
PC	1. 実績あり	1. 是非検証を実施したい	ペネトレーションテストツール全般を利用する
スマートフォン	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
タブレット端末	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ウェアラブル端末	2. 実績なし	4. 検証を実施したくない(検証実施が困難)	—
ルーター	2. 実績なし	2. 可能であれば検証を実施したい	ファジングやペネトレーションによるテストを実施する。

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証 実施の意向	検証実施にあたって想定されるアプローチ (適用する検証手法、使用ツール 等)
ハブ・スイッチ	2. 実績なし	2. 可能であれば検証を 実施したい	ファジングやペネトレーションによるテスト を実施する。
ファイアウォール	2. 実績なし	2. 可能であれば検証を 実施したい	ファジングやペネトレーションによるテスト を実施する。
UTM	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
ゲートウェイ	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
スマートロック	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
ロボット掃除機	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
スマート TV	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
カーナビゲーショ ン	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
ウェブカメラ	1. 実績あり	1. 是非検証を実施した い	Nmap、Metasploit、製品固有の攻撃実 証コード等
サーマルカメラ	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
スマート照明	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
スマートスピー カー	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
プリンター	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
ドローン	2. 実績なし	4. 検証を実施したくな い(検証実施が困難)	—
その他スマート家 電(冷蔵庫、洗濯 機 等)	1. 実績あり	1. 是非検証を実施した い	脅威分析、アセスメント、ペネトレーション テストツール全般

産業用機器等に関する検証事業者 H 社の検証実績及び検証意向を以下に示す。検証の実績がある産業用機器として、産業用 PC・ワークステーションや産業用 IoT ゲートウェイ、産業用センサー、産業用ウェブカメラが挙げられた。検証の意向に関して、すべての機器について「1. 是非検証を実施したい」又は「2. 可能であれば検証を実施したい」の意向であることを確認した。また、各機器の検証実施にあ

たって想定されるアプローチについて、適用する検証手法及び具体的な使用ツールを確認できた。

表 4-32 産業用機器等に関する検証実績・対応意向(検証事業者 H 社)

産業用機器等	検証実績	当該機器に対する 検証実施の意向	検証実施にあたって想定されるアプローチ(適 用する検証手法、使用ツール 等)
産業用PC・ワーク ステーション	1. 実績あり	1. 是非検証を実施 したい	Nmap、Metasploit、ICSSploit、Python ラ イブラリ等 脅威分析、アセスメント
産業用タブレット 端末	2. 実績なし	2. 可能であれば検 証を実施したい	—
産業用ルーター	2. 実績なし	2. 可能であれば検 証を実施したい	—
産業用ハブ・ス イッチ	2. 実績なし	2. 可能であれば検 証を実施したい	—
産業用IoT ゲート ウェイ	1. 実績あり	1. 是非検証を実施 したい	脅威分析、アセスメント
産業用センサー	1. 実績あり	1. 是非検証を実施 したい	脅威分析、アセスメント
産業用ウェブカメ ラ	1. 実績あり	1. 是非検証を実施 したい	脅威分析、アセスメント

産業分野に関する検証事業者 H 社の検証実績及び検証意向を以下に示す。検証の実績を有する産業分野は製造業、医療、電気事業、情報通信事業、自動車の 4 分野であったが、検証の実績がない分野を含むすべての分野について、「1. 是非検証を実施したい」又は「2. 可能であれば検証を実施したい」の意向であることを確認した。

表 4-33 産業用分野に関する検証実績・対応意向(検証事業者 H 社)

産業分野等	検証実績	「1. 検証実績あり」の場合、具体 的な機器区分	当該産業分野の機器に対する検 証実施の意向
製造業	1. 実績あり	OPC サーバー、HMI、PLC、コ ントローラ、エンジニアリングワー クステーション	1. 是非検証を実施したい
医療	1. 実績あり	内視鏡システム	1. 是非検証を実施したい
電気事業	1. 実績あり	ストリング監視システム、地中線 監視システム	1. 是非検証を実施したい
ガス事業	2. 実績なし	—	2. 可能であれば検証を実施し たい

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
水道事業	2. 実績なし	—	2. 可能であれば検証を実施したい
情報通信事業	2. 実績なし	—	2. 可能であれば検証を実施したい
自動車	1. 実績あり	自動車 ECU	1. 是非検証を実施したい
鉄道事業	2. 実績なし	—	2. 可能であれば検証を実施したい
航空事業	2. 実績なし	—	2. 可能であれば検証を実施したい

4.2.9 検証事業者 I 社

(1) 検証手法に関する対応可能性

検証事業者 I 社において対応可能な検証手法の確認結果を以下に示す。確認の結果、ファジングについて「1. 対応可能」、静的ソースコード解析及びファームウェア解析・バイナリ解析について「2. 条件付きで対応可能」であることが分かった。ファームウェア解析・バイナリ解析については、C/C++/java/C#のみ対応可能であること、ファームウェア解析・バイナリ解析については、ネイティブバイナリ(x86/64、ARMv7/v8)に対する解析やネイティブバイナリに対するソフトウェアコンポジション解析であれば対応可能であることを確認した。

表 4-34 検証手法に関する対応可能性(検証事業者 I 社)

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
設計文書レビュー	3. 対応不可	—	—
静的ソースコード解析	2. 条件付きで対応可能	C/C++/java/C#のみ対応可能	静的ソースコード解析ツール
ファームウェア解析・バイナリ解析	2. 条件付きで対応可能	・ ネイティブ バイナリ (x86/64、ARMv7/v8)に対する解析 ・ ネイティブバイナリに対するソフトウェアコンポジション解析	バイナリ解析ツール
ネットワークスキャン	3. 対応不可	—	—
ファジング	1. 対応可能	—	脆弱性検証ツール

検証手法	対応可否	「2. 条件付きで対応可能」な場合の具体的な条件	検証にあたっての工夫、想定される使用ツール
ネットワークキャプチャ(通信内容解析)	3. 対応不可	—	—
ハードウェア解析	3. 対応不可	—	—

(2) 対象機器・対象分野に関する実績・対応意向

一般消費者向けIoT機器等に関する検証事業者I社の検証実績及び検証意向を以下に示す。まず、ファジングツールを用いた検証の実績や検証意向に関する確認結果を示す。ファジングツールを用いた検証の実績を有する機器として、PC、タブレット端末、ルーター、ハブ・スイッチ、ゲートウェイ、スマートロック等の幅広い機器に関する検証実績を有することを確認した。検証の意向に関して、すべての機器について、「1. 是非検証を実施したい」の意向であることを確認した。

表 4-35 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 I 社(ファジニングツール))

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実 施の意向	検証実施にあたって想定されるアプロー チ(適用する検証手法、使用ツール 等)
PC	1. 実績あり	1. 是非検証を実施したい	脆弱性検証ツール
スマートフォン	2. 実績なし	1. 是非検証を実施したい	同上
タブレット端末	1. 実績あり	1. 是非検証を実施したい	同上
ウェアラブル端末	2. 実績なし	1. 是非検証を実施したい	同上
ルーター	1. 実績あり	1. 是非検証を実施したい	同上
ハブ・スイッチ	1. 実績あり	1. 是非検証を実施したい	同上
ファイアウォール	2. 実績なし	1. 是非検証を実施したい	同上
UTM	2. 実績なし	1. 是非検証を実施したい	同上
ゲートウェイ	1. 実績あり	1. 是非検証を実施したい	同上
スマートロック	1. 実績あり	1. 是非検証を実施したい	同上
ロボット掃除機	2. 実績なし	1. 是非検証を実施したい	同上
スマート TV	2. 実績なし	1. 是非検証を実施したい	同上
カーナビゲーショ ン	1. 実績あり	1. 是非検証を実施したい	同上
ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	同上
サーマルカメラ	2. 実績なし	1. 是非検証を実施したい	同上
スマート照明	2. 実績なし	1. 是非検証を実施したい	同上
スマートスピー カー	1. 実績あり	1. 是非検証を実施したい	同上
プリンター	1. 実績あり	1. 是非検証を実施したい	同上
ドローン	2. 実績なし	1. 是非検証を実施したい	同上
その他スマート家 電(冷蔵庫、洗濯 機 等)	2. 実績なし	1. 是非検証を実施したい	同上

次に、静的解析ツールを用いた検証の実績や検証意向に関する確認結果を示す。静的解析ツールを用いた検証の実績を有する機器として、ルーター、ハブ・スイッチ、カーナビゲーションシステムに関する検証実績を有することを確認した。検証の意向に関して、すべての機器について、「2. 可能であれば検証を実施したい」の意向であることを確認した。

表 4-36 一般消費者向け IoT 機器等に関する検証実績・対応意向(検証事業者 I 社(静的解析ツール))

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実 施の意向	検証実施にあたって想定されるアプロー チ(適用する検証手法、使用ツール 等)
PC	2. 実績なし	2. 可能であれば検証を 実施したい	静的解析ツールを用いた脆弱性調査。 ただし基本的にはターゲット全体ではな くライブラリやアプリケーション単位、か つ、解析対象言語で実装されたソース コードが存在する場合のみ対応可。
スマートフォン	2. 実績なし	2. 可能であれば検証を 実施したい	同上
タブレット端末	2. 実績なし	2. 可能であれば検証を 実施したい	同上
ウェアラブル端末	2. 実績なし	2. 可能であれば検証を 実施したい	同上
ルーター	1. 実績あり	2. 可能であれば検証を 実施したい	同上
ハブ・スイッチ	1. 実績あり	2. 可能であれば検証を 実施したい	同上
ファイアウォール	2. 実績なし	2. 可能であれば検証を 実施したい	同上
UTM	2. 実績なし	2. 可能であれば検証を 実施したい	同上
ゲートウェイ	2. 実績なし	2. 可能であれば検証を 実施したい	同上
スマートロック	2. 実績なし	2. 可能であれば検証を 実施したい	同上
ロボット掃除機	2. 実績なし	2. 可能であれば検証を 実施したい	同上
スマート TV	2. 実績なし	2. 可能であれば検証を 実施したい	同上
カーナビゲーショ ン	1. 実績あり	2. 可能であれば検証を 実施したい	同上
ウェブカメラ	2. 実績なし	2. 可能であれば検証を 実施したい	同上
サーマルカメラ	2. 実績なし	2. 可能であれば検証を 実施したい	同上
スマート照明	2. 実績なし	2. 可能であれば検証を 実施したい	同上

一般消費者向け IoT 機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
スマートスピーカー	2. 実績なし	2. 可能であれば検証を実施したい	同上
プリンター	2. 実績なし	2. 可能であれば検証を実施したい	同上
ドローン	2. 実績なし	2. 可能であれば検証を実施したい	同上
その他スマート家電(冷蔵庫、洗濯機 等)	2. 実績なし	2. 可能であれば検証を実施したい	同上

産業用機器等に関する検証事業者 I 社の検証実績及び検証意向を以下に示す。まず、ファジングツールを用いた検証の実績や検証意向に関する確認結果を示す。ファジングツールを用いた検証の実績を有する産業用機器として、産業用 PC・ワークステーション、産業用タブレット端末、産業用ルーター、産業用センサー、産業用ウェブカメラが挙げられた。検証の意向に関して、すべての機器について、「1. 是非検証を実施したい」の意向であることを確認した。

表 4-37 産業用機器等に関する検証実績・対応意向(検証事業者 I 社(ファジングツール))

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	1. 実績あり	1. 是非検証を実施したい	脆弱性検証ツール
産業用タブレット端末	1. 実績あり	1. 是非検証を実施したい	同上
産業用ルーター	1. 実績あり	1. 是非検証を実施したい	同上
産業用ハブ・スイッチ	2. 実績なし	1. 是非検証を実施したい	同上
産業用 IoT ゲートウェイ	2. 実績なし	1. 是非検証を実施したい	同上
産業用センサー	1. 実績あり	1. 是非検証を実施したい	同上
産業用ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	同上

次に、静的解析ツールを用いた検証の実績や検証意向に関する確認結果を示す。静的解析ツールを用いた検証の実績を有する産業用機器として、産業用ルーター、産業用ハブ・スイッチが挙げられた。検証の意向に関して、すべての機器について、「2. 可能であれば検証を実施したい」の意向であることを

確認した。

表 4-38 産業用機器等に関する検証実績・対応意向(検証事業者Ⅰ社(静的解析ツール))

産業用機器等	検証実績	当該機器に対する検証実施の意向	検証実施にあたって想定されるアプローチ(適用する検証手法、使用ツール 等)
産業用 PC・ワークステーション	1. 実績あり	1. 是非検証を実施したい	静的解析ツールを用いた脆弱性調査。 ただし基本的にはターゲット全体ではなくライブラリやアプリケーション単位、かつ、解析対象言語で実装されたソースコードが存在する場合のみ対応可。
産業用タブレット端末	1. 実績あり	1. 是非検証を実施したい	同上
産業用ルーター	1. 実績あり	1. 是非検証を実施したい	同上
産業用ハブ・スイッチ	2. 実績なし	1. 是非検証を実施したい	同上
産業用 IoT ゲートウェイ	2. 実績なし	1. 是非検証を実施したい	同上
産業用センサー	1. 実績あり	1. 是非検証を実施したい	同上
産業用ウェブカメラ	1. 実績あり	1. 是非検証を実施したい	同上

産業分野に関する検証事業者Ⅰ社の検証実績及び検証意向を以下に示す。まず、ファジングツールを用いた検証の実績や検証意向に関する確認結果を示す。検証の実績を有する産業分野は製造業、医療、ガス事業、情報通信事業、自動車の 5 分野であったが、検証の実績がない分野を含むすべての分野について、「1. 是非検証を実施したい」の意向であることを確認した。

表 4-39 産業用分野に関する検証実績・対応意向(検証事業者Ⅰ社(ファジングツール))

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	1. 実績あり	IoT 機器、検査用カメラ	1. 是非検証を実施したい
医療	1. 実績あり	医療機器	1. 是非検証を実施したい
電気事業	2. 実績なし	—	1. 是非検証を実施したい
ガス事業	1. 実績あり	ガス検知器	1. 是非検証を実施したい
水道事業	2. 実績なし	—	1. 是非検証を実施したい
情報通信事業	1. 実績あり	ルーター	1. 是非検証を実施したい
自動車	1. 実績あり	自動車 ECU	1. 是非検証を実施したい
鉄道事業	2. 実績なし	—	1. 是非検証を実施したい

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
航空事業	2. 実績なし	—	1. 是非検証を実施したい

次に、静的解析ツールを用いた検証の実績や検証意向に関する確認結果を示す。検証の実績を有する産業分野は自動車分野のみであったが、検証の実績がない分野を含むすべての分野について、「2. 可能であれば検証を実施したい」の意向であることを確認した。

表 4-40 産業用分野に関する検証実績・対応意向(検証事業者Ⅰ社(静的解析ツール))

産業分野等	検証実績	「1. 検証実績あり」の場合、具体的な機器区分	当該産業分野の機器に対する検証実施の意向
製造業	2. 実績なし	—	2. 可能であれば検証を実施したい
医療	2. 実績なし	—	2. 可能であれば検証を実施したい
電気事業	2. 実績なし	—	2. 可能であれば検証を実施したい
ガス事業	2. 実績なし	—	2. 可能であれば検証を実施したい
水道事業	2. 実績なし	—	2. 可能であれば検証を実施したい
情報通信事業	2. 実績なし	—	2. 可能であれば検証を実施したい
自動車	1. 実績あり	カーナビゲーションシステム、ECU	2. 可能であれば検証を実施したい
鉄道事業	2. 実績なし	—	2. 可能であれば検証を実施したい
航空事業	2. 実績なし	—	2. 可能であれば検証を実施したい

4.3 検証手法に関する検証事業者の対応可能性比較

本事業で調査した検証事業者における検証手法に関する対応可否の比較結果を以下に示す。今回対象とした検証事業者において実施が困難な検証手法は存在せず、それぞれの検証手法に関していずれかの検証事業者で対応可能であることが分かる。ネットワークスキャンやネットワークキャプチャは多くの検証事業者が条件なしで対応可能である一方で、設計文書レビュー、静的ソースコード解析、ハードウェア解析は対応可能な検証事業者が限定的であることが分かる。

表 4-41 検証手法に関する検証事業者の対応可能性比較

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
設計文書レビュー	1	2	1	3	2	1	3	1	3	3
静的ソースコード解析	2	3	1	3	1	1	2	3	3	2
ファームウェア解析・バイナリ解析	3	2	1	1	1	1	2	2	3	2
ネットワークスキャン	1	1	1	1	1	1	1	2	3	3
ファジング	1	2	2	2	1	1	1	2	1	3
ネットワークキャプチャ (通信内容解析)	1	1	1	1	1	1	1	2	3	3
ハードウェア解析	3	2	1	2	1	1	3	3	3	3

【凡例】 1: 対応可能、2: 条件付きで対応可能、3: 対応不可

4.4 対象機器・対象分野に関する検証事業者の実績比較

本事業で調査した検証事業者における一般消費者向け IoT 機器等に関する検証実績の比較結果を以下に示す。今回リストアップしたすべての一般消費者向け IoT 機器等について、いずれかの検証事業者で実績を有していることを確認した。多くの検証事業者が実績を有する機器としては、タブレット端末、ルーター、カーナビゲーションシステム、ウェブカメラが挙げられる一方で、実績を有する検証事業者が限定的な機器としては、ウェアラブル端末、ファイアウォール、サーマルカメラ、スマート照明、スマートスピーカーが挙げられる。

表 4-42 一般消費者向け IoT 機器等に関する検証実績比較

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
PC	1	2	1	1	2	1	2	1	1	2
スマートフォン	1	1	1	2	1	1	2	2	2	2
タブレット端末	1	1	1	1	1	1	2	2	1	2
ウェアラブル端末	1	2	2	2	2	1	2	2	2	2
ルーター	2	1	1	1	1	1	2	2	1	1
ハブ・スイッチ	2	2	1	1	1	1	2	2	1	1
ファイアウォール	1	2	1	2	1	2	2	2	2	2
UTM	2	2	2	1	2	1	2	2	2	2
ゲートウェイ	2	2	1	1	1	2	2	2	1	2
スマートロック	1	2	1	1	2	1	2	2	1	2
ロボット掃除機	1	2	1	1	2	1	2	2	2	2
スマートTV	1	2	1	1	2	2	2	2	2	2
カーナビゲーション	1	1	1	1	1	1	2	2	1	1
ウェブカメラ	1	1	1	1	2	1	2	1	1	2
サーマルカメラ	2	1	2	1	1	2	2	2	2	2
スマート照明	2	2	2	2	1	2	2	2	2	2
スマートスピーカー	2	1	2	2	2	2	2	2	1	2
プリンター	1	1	1	2	2	2	2	2	1	2
ドローン	1	1	1	1	1	1	2	2	2	2

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
その他スマート家電(冷蔵庫、洗濯機等)	1	1	1	1	2	2	2	1	2	2

【凡例】 1: 実績あり、2: 実績なし

本事業で調査した検証事業者における産業用機器に関する検証実績の比較結果を以下に示す。今回リストアップしたすべての産業用機器について、いずれかの検証事業者で実績を有していることを確認した。多くの検証事業者が実績を有する機器としては、産業用 PC・ワークステーション、産業用ルーター、産業用ハブ・スイッチ、産業用 IoT ゲートウェイ、産業用ウェブカメラが挙げられる一方で、産業用タブレット端末や産業用センサーは実績を有する検証事業者が限定的であった。

表 4-43 産業用機器に関する検証実績比較

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
産業用 PC・ワークステーション	2	2	1	1	1	1	2	1	1	2
産業用タブレット端末	1	2	1	2	2	1	2	2	1	2
産業用ルーター	2	2	1	1	1	1	2	2	1	1
産業用ハブ・スイッチ	2	2	1	1	1	1	2	2	2	1
産業用 IoT ゲートウェイ	2	2	1	1	1	1	2	1	2	2
産業用センサー	2	1	2	2	2	1	2	1	1	2
産業用ウェブカメラ	2	2	1	1	2	1	2	1	1	2

【凡例】 1: 実績あり、2: 実績なし

本事業で調査した検証事業者における産業分野別の検証実績の比較結果を以下に示す。今回リストアップしたすべての産業分野について、いずれかの検証事業者で実績を有していることを確認した。多くの検証事業者が実績を有する産業分野としては、製造業、医療、情報通信事業、自動車の 4 分野が挙げられる一方で、水道事業、鉄道事業、航空事業は実績を有する検証事業者は 1 社のみであった。

表 4-44 産業分野別の検証実績比較

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
製造業	1	1	1	2	1	1	2	1	1	2

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
医療	1	2	2	1	1	1	2	1	1	2
電気事業	2	1	1	2	2	1	2	1	2	2
ガス事業	2	2	2	2	2	2	2	2	1	2
水道事業	2	2	2	2	2	1	2	2	2	2
情報通信事業	1	1	1	1	1	1	2	2	1	2
自動車	1	1	1	1	1	1	2	1	1	1
鉄道事業	1	2	2	2	2	2	2	2	2	2
航空事業	1	2	2	2	2	2	2	2	2	2

【凡例】 1: 実績あり、2: 実績なし

4.5 対象機器・対象分野に関する検証事業者の対応意向比較

本事業で調査した検証事業者における一般消費者向け IoT 機器等の検証に関する対応意向の比較結果を以下に示す。すべての機器に対して「1. 是非検証を実施したい」と回答した事業者が複数社存在することもあり、今回リストアップしたいずれの機器に対しても、検証を要望する検証事業者が 1 社以上存在することが分かる。

表 4-45 一般消費者向け IoT 機器等の検証に対する対応意向比較

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
PC	1	3	1	1	1	1	4	1	1	2
スマートフォン	1	2	1	4	1	1	4	4	1	2
タブレット端末	1	2	1	1	1	1	2	4	1	2

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
ウェアラブル 端末	1	2	1	1	1	1	4	4	1	2
ルーター	2	2	1	2	1	1	4	2	1	2
ハブ・スイッチ	2	4	1	2	1	1	4	2	1	2
ファイア ウォール	2	2	1	2	1	3	4	2	1	2
UTM	2	2	1	2	1	1	4	4	1	2
ゲートウェイ	2	2	1	2	1	1	4	4	1	2
スマートロッ ク	1	4	1	1	1	1	4	4	1	2
ロボット掃除 機	1	2	1	1	1	1	4	4	1	2
スマートTV	1	2	1	1	1	1	4	4	1	2
カーナビゲー ション	1	2	1	1	1	1	4	4	1	2
ウェブカメラ	1	2	1	1	1	1	4	1	1	2
サーマルカメ ラ	4	2	1	1	1	1	4	4	1	2
スマート照明	1	2	1	1	1	1	4	4	1	2
スマートス ピーカー	1	2	1	1	1	1	4	4	1	2
プリンター	1	2	1	4	1	1	4	4	1	2
ドローン	1	2	1	1	1	1	4	4	1	2
その他スマー ト家電(冷蔵 庫、洗濯機 等)	1	2	1	1	1	1	4	1	1	2

【凡例】 1: 是非検証を実施したい、2: 可能であれば検証を実施したい、
3: 可能であれば検証を実施したくない、4: 検証を実施したくない(検証実施が困難)

本事業で調査した検証事業者における産業用機器の検証に関する対応意向の比較結果を以下に示

す。すべての機器に対して「1. 是非検証を実施したい」と回答した事業者が複数社存在することもあり、今回リストアップしたいずれの機器に対しても、検証を要望する検証事業者が 1 社以上存在することが分かる。

表 4-46 産業用機器の検証に対する対応意向比較

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
産業用 PC・ワークステーション	2	1	1	1	1	1	2	1	1	2
産業用タブレット端末	2	1	1	1	1	1	4	2	1	2
産業用ルーター	4	1	1	1	1	1	4	2	1	2
産業用ハブ・スイッチ	4	4	1	1	1	1	4	2	1	2
産業用 IoT ゲートウェイ	4	1	1	1	1	1	2	1	1	2
産業用センサー	2	1	1	1	1	1	4	1	1	2
産業用ウェブカメラ	2	1	1	1	1	1	4	1	1	2

【凡例】 1: 是非検証を実施したい、2: 可能であれば検証を実施したい、3: 可能であれば検証を実施したくない、4: 検証を実施したくない(検証実施が困難)

本事業で調査した検証事業者における産業分野別の検証に関する対応意向の比較結果を以下に示す。すべての分野に対して「1. 是非検証を実施したい」と回答した事業者が複数社存在することもあり、今回リストアップしたいいずれの分野に対しても、検証を要望する検証事業者が 1 社以上存在することが分かる。

表 4-47 産業分野別の対応意向比較

検証事業者	検証事業者 A 社	検証事業者 B 社	検証事業者 C 社	検証事業者 D 社	検証事業者 E 社	検証事業者 F 社	検証事業者 G 社	検証事業者 H 社	検証事業者 I 社 (ファジング)	検証事業者 I 社 (静的解析)
製造業	2	2	1	1	1	1	2	1	1	2
医療	4	2	1	1	1	1	2	1	1	2
電気事業	2	2	1	1	1	1	4	1	1	2
ガス事業	2	2	1	1	1	1	4	2	1	2
水道事業	2	2	1	1	1	1	4	2	1	2
情報通信事業	1	2	1	1	1	1	2	2	1	2
自動車	1	2	1	1	1	1	4	1	1	2
鉄道事業	1	4	1	1	1	1	4	2	1	2
航空事業	1	4	1	1	1	1	4	2	1	2

【凡例】 1: 是非検証を実施したい、2: 可能であれば検証を実施したい、
3: 可能であれば検証を実施したくない、4: 検証を実施したくない(検証実施が困難)

5. まとめ

本事業において、中小機器が販売する IoT 機器について、産業向け及び一般消費者向けを広く対象として調査を行った。

また、IoT 機器に対してセキュリティ検証を行う事業者についても調査を行い、調査対象とした IoT 機器に対して機器及び手法について不足なくカバーできることが確認できた。

本調査結果を踏まえ、中小企業の販売する IoT 機器に対して、開発時点からセキュリティ検証を行う等の効果的な検証の進め方に関して検討を進めていくことが望ましい。

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
中小企業が開発するIoT機器に関する調査事業
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
