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年度　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、四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。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。加えて、別冊４では、令和４年度に実施した中小企業等が開発するIoT機器等に対する検証の実証結果を踏まえ、代表的なIoT機器に対して検証事業者が実施すべき事項や留意すべき事項を示す。

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。
別冊 4 「機器個別のセキュリティ検証プラクティス集」	• 令和 4 年度に実施した中小企業等が開発する IoT 機器等に対する検証の実証結果を踏まえ、代表的な IoT 機器に対して検証事業者が実施すべき事項や留意すべき事項を示す。 • 実証で実際に検出された脆弱性の情報に基づき、当該脆弱性が悪用された場合に想定される影響や脆弱性検出に至った検証プロセスを示す。

本編及び四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。

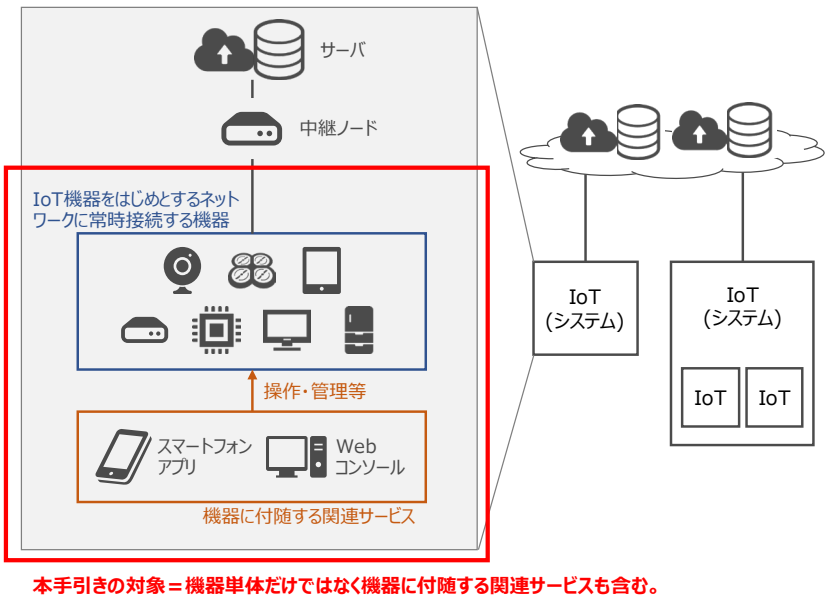

図 1-1 本手引きの対象機器イメージ [1]

[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

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。機器メーカについて、大企業だけでなく中小企業が検証を依頼する際にも活用できる内容となっている。表 1-2 に示すとおり、別冊 1、別冊 3 及び別冊 4 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	別冊 4
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。別冊 4 で示される脆弱性の情報や推奨事項を確認することで、代表的な IoT 機器等に対する検証を実施する際に、効果的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。また、別冊 4 では、令和 4 年度の実証で検出された深刻度の高い脆弱性の情報を基に、当該脆弱性の検出に至った検証プロセス、脆弱性を悪用された場合に想定される影響、脆弱性に対する推奨事項を示す。

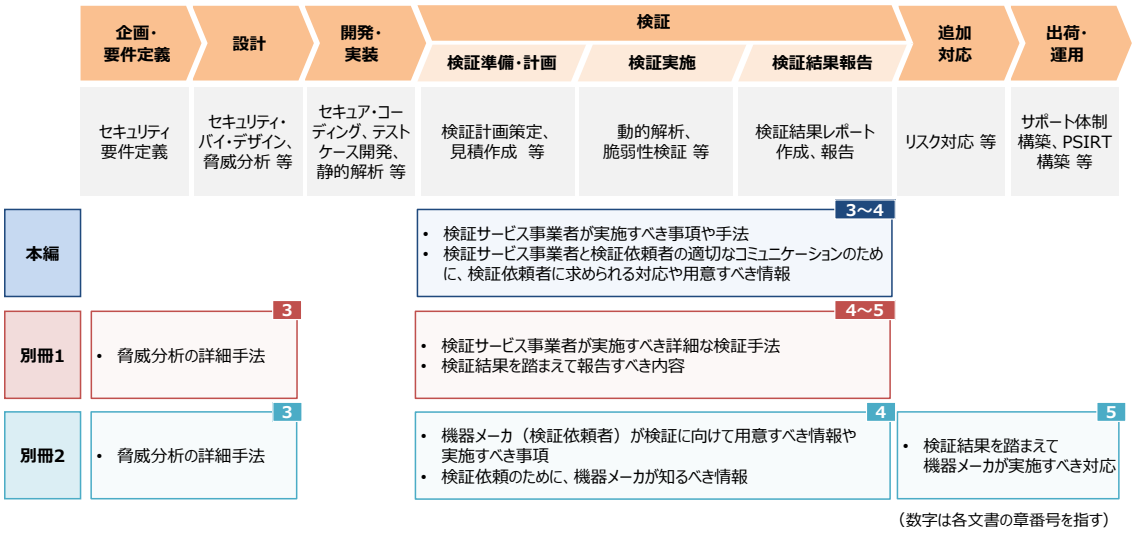

図 1-2 機器開発プロセスにおける本編及び別冊 1･別冊 2 のスコープ

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。検証サービス事業者においては、検証が 100%のセキュリティを保証するものではないことを依頼者に適切に伝える必要がある。

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。

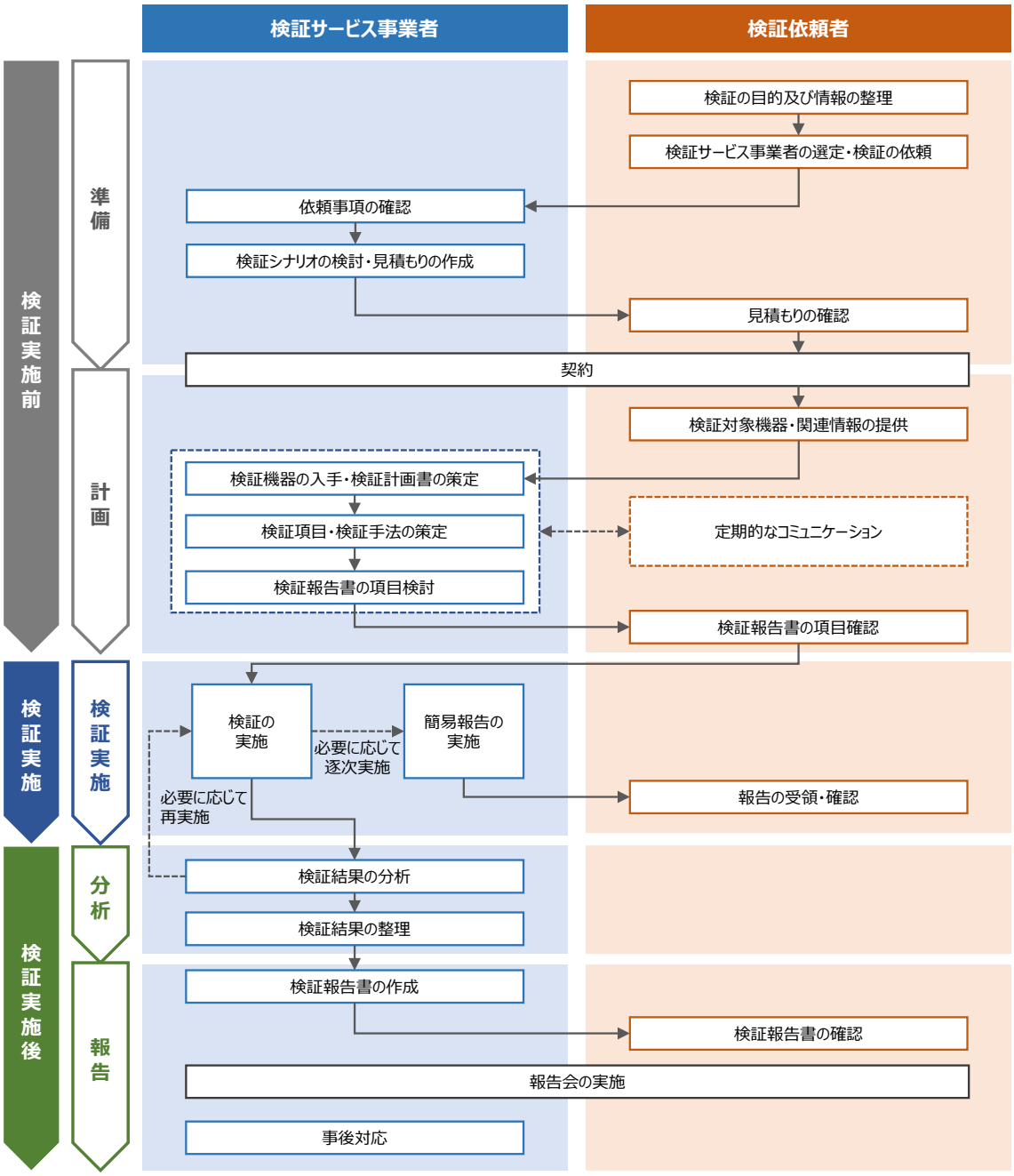

図 3-1 機器検証の実施手順

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。中小企業等の検証に不慣れなメーカが依頼者の場合、具体的な依頼内容や検証の要望が決まっていない場合があるため、依頼者の要望を引き出しつつ、どのような検証が求められるかを検証事業者で検討し、提示する必要がある。なお、このようなメーカが依頼者である場合、可能な限り平易な用語を用いて説明を行うことが望まれる。検証依頼者としては、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。検証に不慣れなメーカが依頼者の場合、秘密保持管理に向けた手続きなど、検証に向けて必要な手続きを検証事業者から提示する必要がある。

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が、仮に報告を行う場合には、その脆弱性が悪用された場合に想定される影響も含めて連絡することが望まれる。脆弱性の報告に関して、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。契約に関して、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

[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

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。検証依頼者としては、機器に対する破壊的検証の可否を事前に検証サービス事業者に伝えることが望ましい。また、検証サービス事業者の視点では、仮に破壊的検証を実施する場合は事前に依頼者に伝え、破壊する場合の留意事項や免責事項について依頼者と合意の上で、検証を進める必要がある。その他の禁止事項の例として、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おそれもある。影響が波及した場合に責任を負わないこととする場合、免責事項として明示することが必要である。そのほか、契約時に合意しておくべき免責事項として、検証が 100%のセキュリティを保証するものではないことや、対象機器の品質を保証するものではないことが挙げられる。

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。また、検証サービス事業者は、検証期間中にどのような連絡を行う可能性があるかをあらかじめ検証依頼者に伝えることが望ましい。

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。

項目	記載内容
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

[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

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。

[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

大項目	項目	記載内容
	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。
	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。

---

[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

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

---

[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

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。依頼者によっては、検証依頼前に脅威分析を実施していないケースもある。この場合に、まず脆弱性スキャンツールを用いて自動スキャンを行い、脆弱性が含まれる箇所のあたりをつけた上で詳細な検証を実施することで、効率的な検証を進めることができる。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

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
	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
	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

[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。

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。

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

[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

[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

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：
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おそれもある。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

---

[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

[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

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。

[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

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。

表 4-3 検証報告書の項目例（表 3-3 の再掲）

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。

大項目	項目	記載内容
	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。
	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。

報告においては、可能な限り平易な用語を用いつつ、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。特に、中小企業等の検証に不慣れなメーカが検証依頼者の場合、対策の必要性や方向性を検証サービス事業者が検討し、提案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 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。

- **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]

5.2 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