「サプライチェーンセキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」に関する研究開発構想（個別研究型）

令和 5 年 3 月
内閣府
文部科学省

目次

1　構想の背景、目的、内容

1.1　構想の目的

1.1.1　政策的な重要性

ICT 機器・システムのサプライチェーンの複雑化、グローバル化、また、オープン API (Application Programming Interface)や OSS (Open Source Software)の普及など、サイバー分野におけるサプライチェーンを取り巻く環境は一層複雑化し、サプライチェーンの過程で不正機能等が埋め込まれるリスクなど、サプライチェーン・リスクが顕在化している。このようなリスクに対応するサプライチェーンセキュリティ技術は、我が国のサイバーセキュリティ研究開発戦略（改訂）（令和 3 年 5 月 13 日サイバーセキュリティ戦略本部）においても重点的な研究領域とされている。

あらゆる産業において複雑かつグローバルなサプライチェーンを経由する製品・サービスの拡大・浸透、IoT 機器の利用拡大が進む中では、検証技術等の他国に容易に依存できない技術について、我が国技術の優位性の獲得も念頭に、産学官の技術力を高め、自律性を確保する必要がある。他方、現状は必ずしもその技術の体系化はなされていない。

本構想は、個別研究型として、こうした背景の下、ICT 機器・システムを構成するファームウェア・ソフトウェアにおいてバックドア等の不正機能（本構想において、「不正機能」とは、仕様上想定されない機能であって、サイバー攻撃に使用され得る機能のことを言い、バックドア（例：正規でないアクセス方法)、不正ロジック（例：特定の条件下で強制的に終了させる機能)、無断通信（例：仕様に定義されていない通信）などが想定される。）が仕込まれていないかを検証する技術の確保に資する支援対象とする技術として研究開発ビジョン（第一次）において定められた「不正機能検証技術（ファームウェア・ソフトウェア）」において、我が国の優位性獲得も念頭に自律性確保を目指すものである。

1.1.2　我が国の状況

内閣官房内閣サイバーセキュリティセンター（NISC）と関係省庁が連携し、ICT 機器・サービスの信頼性を確保するための技術開発と推進体制の構築を進めている。

NISC においては、機器のサプライチェーンに係る信頼性の確保に対し、

実際の製品に不正機能や当該機能につながりうる未知の脆弱性等が存在しないかどうかの技術的検証を実施しつつ、その体制構築に資する検討を行うため、「サプライチェーンリスク対応のための技術検証体制構築等に関する調査」を実施している。当該調査においては、これまでに不正機能等の検証プロセスの検討や、検証要求・技法等の整理・共通言語化、不正機能につながり得る未知の脆弱性の発見、信頼できる国内検証事業者の掘り起こし、といった取組を進めており、今後の課題としては、①発見された不正機能が意図をもって埋め込まれたものであるかどうかを評価する手法の検討、②検証対象機器の拡大・検証内容の高度化などが挙げられている。

①については、ソフトウェア等において脆弱性が発見された場合にも、それが悪意を持って埋め込まれた不正機能なのか、過失によるものか、技術的に決定できない場合が多く、発見された不正機能の意図性を技術的に評価することができれば、意図的な脅威に対する抑止力としての効果が期待される。しかし、脆弱性に係る意図性があるものと確証することは本質的な困難性を伴うものであり、国内外でもこれに係る技術は実現していない。

②については、公的機関で多く利用されている機器や安全保障の観点から関心の高い機器を中心に検証対象機器を拡大することが求められるが、そのためには信頼できる事業者の拡大と検証技術の多様化が必要となる。近年は SBOM（ソフトウェア部品表）を利用したソフトウェア管理が注目され、国内でも普及に向けた取組が始まっているが、高度な不正機能の検証のためには、SBOM の普及のみならずソフトウェア構成のより詳細な情報を活用した検証技術の開発が求められる。

情報セキュリティ製品の我が国市場におけるシェアについては、図１のとおり、2019 年・2020 年ともに外資系企業のシェアが高く、国内のサイバーセキュリティ製品はその多くを海外に依存している状況が引き続いていると言える。

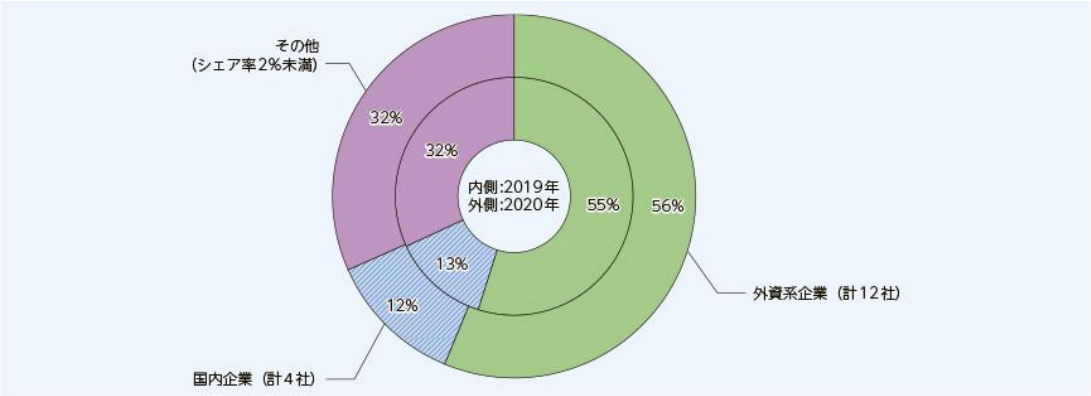


図１：国内情報セキュリティ製品市場シェア（売上額）　2019～2020

（出典）令和 4 年版情報通信白書

1.1.3　世界の取組状況

米国は活動が最も顕著である。国防高等研究計画局（DARPA）の研究プログラムにもサプライチェーンセキュリティが採択され、ガイドライン作成やブロックチェーン連携等の研究促進を実施している。2022 年 4 月には、国務省にサイバー空間・デジタル政策局（Bureau of Cyberspace and Digital Policy）を設置し、サプライチェーンセキュリティの推進にも取り組むこととしている。

欧州では、サプライチェーン全体を対象としたセキュリティ研究よりも、ソフトウェア検証等の要素技術の研究が盛んに行われている。また、2022 年 11 月 28 日に、欧州連合理事会において、主として重要インフラを対象としたセキュリティ強化のため、ネットワークと情報システムのセキュリティに関する新たな指令である「A high common level of cybersecurity across the Union」が決定されているほか、重要インフラ以外の分野も含めた汎用的な IoT 製品に対するセキュリティ要件を定める「Cyber Resilience Act」も、同年 9 月 15 日に草案が公開され、その適合性を評価する一つの手法として認証フレームワークの策定（法制化）も実施している。

1.1.4　構想のねらい

本構想では、ICT 機器・システムを構成するファームウェア・ソフトウェアについて、不正機能に関する技術検証体制の構築に資するため、NISC の調査において挙げられている技術課題の解決に向けて、①不正機能の意図性に関する評価手法、②ソフトウェア構成の情報を活用した不正機能の検

証手法の獲得を目指す。

一方で、全ての不正機能の組込みを事前に検知することは難しく、運用開始後に不正機能が組み込まれるリスクを含めて、仮に運用開始前に検知・無害化できなかったとしても、システム・サービス全体として被害を最小限に抑え、運用を維持・継続できるレジリエンス性を高めるための手法の獲得を目指す（③）。

これらについては、産学官の連携によりチームを構成し、データ・知見の共有・蓄積を含めた技術体系の整理と高度化を進め、「不正機能検証技術（ファームウェア・ソフトウェア）」において、我が国の優位性獲得も念頭に自律性の確保を狙う。

これにより、ICT 機器・システムを構成するファームウェア・ソフトウェアにおいて、バックドア等の不正機能が仕込まれていないかを検証するための国内検証事業者のサービス高度化や新規サービス創出等に繋がり、政府機関による ICT 機器・システムの不正機能検証等の公的利用に加え、民間企業等による自らの ICT 機器・システムの検証等の民生利用に活用されることが期待される。

1.2 構想の目標

1.2.1 アウトプット目標

本構想では、国内の事業者が利用できる技術・ツール等の獲得に繋げるため、目標は以下のとおりとする。これにより、その後の展開あるいは社会実装に繋げていく。

＜不正機能の意図性に関する評価手法＞

多様な過去の事例（100 件以上）の分析に基づき、不正機能が意図的に埋め込まれた可能性を 2 段階以上で評価するツールを開発する。

なお、ツール開発においては、以下の項目に留意すること。

- 過去の事例や外部環境等から想定される不正機能の体系化・類型化を行う。
- 評価する方法論（インプット、評価プロセス、アウトプット）を整理し、反映する。
- 当該ツールは、国内の関連する事業者が提供する各種サービス等に簡易に組込みが可能なものが望ましい。

＜ソフトウェア構成の情報を活用した不正機能の検証手法＞

不正機能の検証の効率化・高度化につながるソフトウェア構成情報を活用した不正機能検証ツールを開発する。

なお、当該ツールは、以下の事項のうち、１つ以上の機能を有すること。

① OSS およびソースコードが利用可能なプロプライエタリソフトウェアの検証が可能であること

② ブラックボックス環境（ソースコードを入手できず、バイナリコードを検証するケース）での活用が可能であること

③ 難読化されたバイナリコードの検証が可能であること

また、ツール開発においては、以下の項目に留意すること。

- 不正機能の検証の効率化・高度化につながるソフトウェア構成情報を活用する方法論を整理し、反映する。
- 当該ツールは、国内の関連する事業者が提供する各種サービス等に簡易に組込みが可能なものが望ましい。

＜システム・サービスのレジリエンス性の確保に関する手法＞

重要インフラ分野における制御システムについて、インシデント発生時のシステム・サービスへの影響を最小限に留めるためのツールを開発する。

なお、ツール開発においては、以下の項目に留意すること。

- システム全体の俯瞰によりインシデント発生時のシステム・サービスへの影響を最小限に留める方法論を整理し、反映する。
- 当該ツールは、インシデント発生時に、残存するリスクを最小化するための対策候補を自動的に生成し、提案する機能を有することとする。
- 当該ツールは、国内の関連する事業者が提供する各種サービス等に簡易に組込みが可能なものが望ましい。

1.2.2 アウトカム目標

上記のアウトプット目標により、本構想で研究開発する技術で、国内検証事業者のサービスの高度化や新規サービス創出、能力向上等を実現し、これにより、幅広い事業主体（政府機関や民間企業、インフラ関係等）による国内の信頼できる検証事業者を拡大するとともに、検証技術の多様化を目指す。また、その際、我が国における不正機能検証技術に関する産学官の連携

促進や人材育成プログラムの開発等にも資することを目指す。

1.3 研究開発の内容

1.3.1 研究開発の必要性

不正機能の意図性に関する評価手法については、技術的な観点から機器の挙動などを動的解析する手法でも、ソフトウェアエンジニアリングの観点から静的解析する手法でも、発見された不正機能が悪意を持って埋め込まれたものかどうかなどの意図性を確証することは本質的に困難であり、国内外でも手法は確立しておらず、我が国が先駆けて技術を獲得すれば、科学技術の観点だけでなく、経済安全保障の観点からもゲームチェンジャーとなり得る。不正機能の意図性に関する評価手法を確立するためには、不正機能に係るデータを収集するとともに、当該データの整理・分析により意図性を評価するための基準を整備し、評価手法をツール化する取組が考えられるが、どのようにして必要となるデータを収集するのかといったデータ収集に係る方策を含めた研究開発の推進が必要となる。

ソフトウェア構成の情報を活用した不正機能の検証手法については、ライセンス・既知脆弱性の管理を目的とした SBOM の普及が進んでいるが、不正機能の技術検証での活用を想定したものは見られない。加えて、既存の SBOM 作成ツールは OSS の情報のみが対象となっているものが多いが、例えば OSS のバージョン情報だけで脆弱性の存在を予測しても、バージョン番号を変更せずに暗黙的にパッチが適用されることがあるため、バージョン番号に基づく脆弱性評価では誤検知が発生することが大規模なファームウェア分析によって定量的に示されている。さらに、技術検証においては、OSS だけでなくプロプライエタリソフトウェアも検証の対象となり得るため、それらへの対応も必要となる。したがって、SBOM に限らず、ソフトウェアの部品構成に関する情報を用いた検証手法の開発が必要となる。また、既存のソフトウェアコンポジション解析などの技術は、精密な検査を行うためにはユーザーに必要とされる技術・手間が多すぎるため、容易かつ効率的な検査や誤検出の回避、精密な検査の自動化が重要となる。

システム・サービスのレジリエンス性の確保に関する手法については、サイバー攻撃が多様化・高度化する中で、システム・サービスの運用を維持・継続し、事業への影響を最小限に留めるためには、従来のように脆弱性を利

用したインシデントが発生した後に対応するだけでなく、インシデントの発生中に影響把握や必須機能の確保、原因箇所の特定・分離などが求められる。実運用上、インシデントの原因及び影響をリアルタイムかつ高精度で分析する技術の開発が必要となる。

国内検証事業者のサービスの高度化・新規サービス創出や能力向上及びその成果の公的利用・民生利用に繋げるためにも、産学官の連携による技術・ツールの開発等を進めていくことが必要である。

1.3.2 研究開発の具体的内容例

海外のコア技術やインテリジェンスに依存する現状を脱却し、我が国の自律性・優位性を高める観点から、我が国発の革新的な手法によるコア技術の実現を目指す。以下の課題について、産学官の連携によりチームを構成し、データ・知見共有・蓄積を含めた検証技術の高度化を行う。

各課題について、手法のツール化に向けたプロトタイプの研究開発を行い、具体的な事例に適用し、その妥当性の実証を行う。実証に当たっては、定量的にその妥当性を判断することが難しい場合は、例えば、複数の有識者による多面的なレビューを行うなど、開発したツールの性能評価が妥当であることの客観性を確保する。

また、開発したツールが、国内の検証事業者が提供する各種検証サービス等に簡易に組込みが可能なものになるよう、例えば、プロセスの自動化やツールのソフトウェアパッケージ化などに努める。

＜不正機能の意図性に関する評価手法＞

- 意図性に関する評価のためには、評価の枠組みを定義するためのデータを継続的に確保することが極めて重要となることから、必要となる不正機能事例に関するデータを収集するための手法を研究開発するとともに、各種機器・サービスが利用しているファームウェア・ソフトウェアに仕様外の機能や仕様未満の機能、実装ミスを装った脆弱性等が含まれている事例などを収集し、意図性に関する評価手法開発のために必要となるデータを抽出・分析する。
- 分析したデータをもとに、不正機能の体系化・類型化を行うとともに、不正機能が悪意を持って埋め込まれたものか、保守管理を目的として意図的に埋め込まれたものか、過失によるものかといった意図性の程度を

細分化し、不正機能の意図性を判断する観点を抽出することで、評価基準を整理する。

- 当該基準に基づき、検出した脆弱性が意図的なものであるかどうかを可能な範囲で定量的に評価する手法を研究開発する。

＜ソフトウェア構成の情報を活用した不正機能の検証手法＞

- 不正機能が埋め込まれているかどうかを検証するために、どのようなソフトウェアの部品構成に関する情報を、どのような方法で活用すると有効な検出が可能となるのかを研究する。その際、例えば、既知の脆弱性だけでなく、未知の脆弱性や不正機能の可能性も抽出する機能や、一つの OSS が他の OSS やライブラリの機能を利用するなどソフトウェア間の依存関係が生じる場合の対応、公開された脆弱性に関する情報がリアルタイムに反映されず OSS のバージョン情報に基づく評価により誤検知が生じる場合の回避など、可能な限り漏れが少なく、高精度な検出が可能なものを目指す。また、OSS に限らずプロプライエタリソフトウェアも対象とすることが望ましい。
- 当該研究の結果を踏まえ、必要なソフトウェアの部品構成に関する情報を解析する手法を研究開発する。

＜システム・サービスのレジリエンス性の確保に関する手法＞

- 「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月 17 日　サイバーセキュリティ戦略本部）において、「重要インフラ分野」として特定されている 14 分野の中から 1 つ以上を選定し、選定した分野において活用されるシステムを想定し、システム全体を俯瞰した上で、優先的に維持すべき機能と当該機能の停止時の影響範囲を前もって把握するために必要な情報の精査を行う。
- 精査された情報をもとに、インシデント発生時にシステム・サービス全体へ与える影響や、特定部分の切離・代替措置等の対策による残存リスクを、より高い精度で分析する手法の研究開発を行う。また、残存リスクを最も効果的に減少させる対策候補を自動的に生成し提案する技術等の研究開発を行う。
- さらに、開発した技術を用いて、故障やサイバー攻撃により複数の ICT 機器が停止しても、事業への影響を最小限に留められる事業継続管理計

画（BCMP）や事業継続計画（BCP）の実現に必要な体制を構築する手法を研究開発する。

- 実証に当たっては、中間評価までに選定した分野における事業者の参画を得て、可能な限り実際のシステムに近い環境で行うように努める。

1.3.3 研究開発の達成目標

本構想により、国内検証事業者による一定の有効性と効率性を有した不正機能検証に係るサービスが提供可能となることを目指し、革新的な手法に基づく検証ツールや、システム・サービスのレジリエンス性の確保に関するツール等を開発することを目指す。

より具体的には、提案者の設定した個別の達成目標を基本としつつ、文部科学省及び JST のサポートの下、採択後、研究開発を開始するにあたって行う研究計画の調整にて定めると共に、研究開発開始後においては、協議会における意見交換の結果も踏まえ、必要な場合、見直しを行う。

2 研究開発の実施方法、実施期間、評価

2.1 研究開発の実施・体制

公募により研究開発の実施主体をそれぞれ決定する。当該公募に当たっては、大学、民間企業など産学官の連携による提案を求めるものとする。なお、採択にあたっては、複数の研究開発課題の採択も検討する。

さらに、不正機能等の事例の共有、研究開発成果の公開等の取扱いに関する事項等について、協議会で情報共有や意見交換を行い、その結果に基づき研究開発を行う。

PO の指揮・監督の下、研究代表者（研究開発課題の実施責任を法人が担う場合は当該法人を含む。以下同じ。）が研究開発構想の実現に向け責任を持って研究開発を推進する。JST 等の助言に基づき、研究代表者は、適切な技術流出対策を行うよう体制を整備するとともに、研究インテグリティの確保に努め、適切な安全保障貿易管理を行うよう、これらを推進するとともに、研究開発に必要な事項を行う。

研究開発成果を民生利用のみならず公的利用につなげていくことを指向し、社会実装や市場の誘導につなげていく視点を重視するという本プログラムの趣旨に則り、研究代表者は PO 及び研究分担者との協議の上、知的財

産権の利活用方針を定めることとする。その際には、研究開発途中及び終了後を含め、知的財産権の利活用を円滑に進めることができるように努めることとする。

なお、研究開発成果の利活用にあたりその成果にバックグラウンド知的財産権が含まれる場合には、その利活用についても同様に努めることとする。

また、当該分野における民間企業等における処遇水準を踏まえ、研究開発に従事するリサーチ・アシスタント（RA）等大学から人件費の支弁を受ける者には、その報酬等について、海外の事例[1]なども考慮し、これに相応しい水準を支弁する。具体的には、担当する PO が研究計画を踏まえ調整した上で、JST が決定するものとする。

2.2　研究開発の実施期間

研究開発開始から 5 年以内とする。構想全体で最大 25 億円程度の予算を措置する。

2.3　評価に関する事項

自己評価は毎年実施する。外部評価の実施時期は原則、研究開発の開始から 3 年目を中間評価とし、研究開発終了年に事後評価を実施する。具体的な時期については、担当する PO が採択時点でマイルストーンを含む研究計画とともに調整した上で、JST が決定するものとする。

2.4　社会実装に向けた取組

本構想は、革新的な手法に基づく検証技術等や未知の脆弱性対応のための手法の研究開発を通じて、公的利用・民生利用が可能な国内検証事業者のサービス高度化や新規サービス創出等を目指すものである。このためには、研究代表者と潜在的な社会実装の担い手として想定される関係行政機関や

---

[1]「米国高等教育における博士課程学生への経済支援に関する研究」（令和 3 年度学生支援の推進に資する調査研究事業（JASSO リサーチ）研究成果報告書）
https://www.jasso.go.jp/statistics/jasso-research/__icsFiles/afieldfile/2022/03/25/r3jasso-research_report2.pdf

民間企業等との間で、不正機能に関する事例やその対策手法等の情報共有や、社会実装イメージ、研究開発の進め方を議論・共有する取組等の伴走支援が有効である。

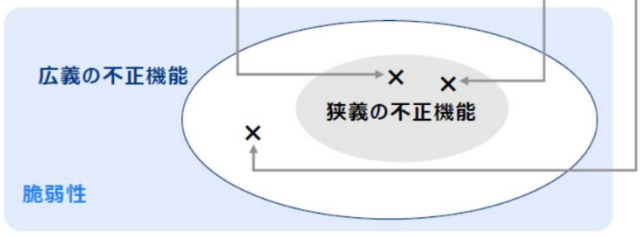
したがって、今後設置される協議会を活用し、参加者間で機微な情報も含め、社会実装に向けて研究開発を進める上で有用な情報の交換や協議を安心して円滑に行うことのできるパートナーシップを確立することが重要であり、関係者において十分にこの仕組みの運用を検討する必要がある。なお、協議会の詳細は別に示す。また、PO は研究マネジメントを実施する際には、協議会における意見交換の結果も踏まえるものとする。

（参考１）不正機能の定義

- 脆弱性について、悪意を持って埋め込まれた不正機能か、過失によるものか、技術的には決定できない場合が多い。不正機能に関してコンセンサスの得られた明確な定義は未だ存在しないが、ここでは、以下の2段階の定義により、リスク管理上の漏れを回避する。

① **広義の不正機能**
不正機能の可能性がある脆弱性。検証要求のうち第1階層(p.8)が不正機能のカテゴリに該当するバックドア、無断送信、不正ロジック等の脆弱性。（具体例は検証要求の第4階層の検証項目に該当するもの。）これらの脆弱性のうち、**悪意が低いと想定されるものであっても、悪意が無いと立証することは難しい**ため、グレイなものも含めて管理漏れが無いように不正機能の可能性のあるものを広く対象とする。（例えば、解放ポートの残存など、故意か過失か判断は難しい）

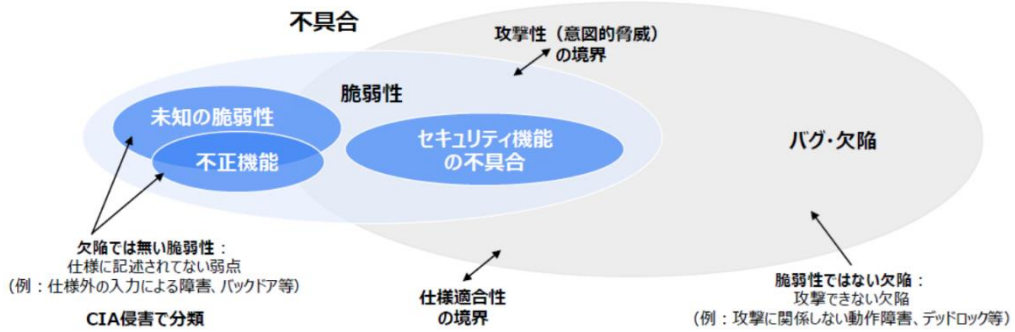
② **狭義の不正機能（一般的に認識される不正機能）**
広義の不正機能のうち、悪意の可能性が高いと説明できる脆弱性。（例えば、機能仕様上必要のないレジストリ情報の外部送信や、セキュリティ成熟度の高いベンダーが、管理者パスワードをハードコードする初歩的な脆弱性など、**存在する正当な理由が説明できない脆弱性**）



（出典）サプライチェーン・リスク対応のための技術検証体制構築に関する調査報告書（2022 年 5 月）

（参考２）脆弱性（未知・既知）、不正機能、バグ・欠陥等の定義と関係性

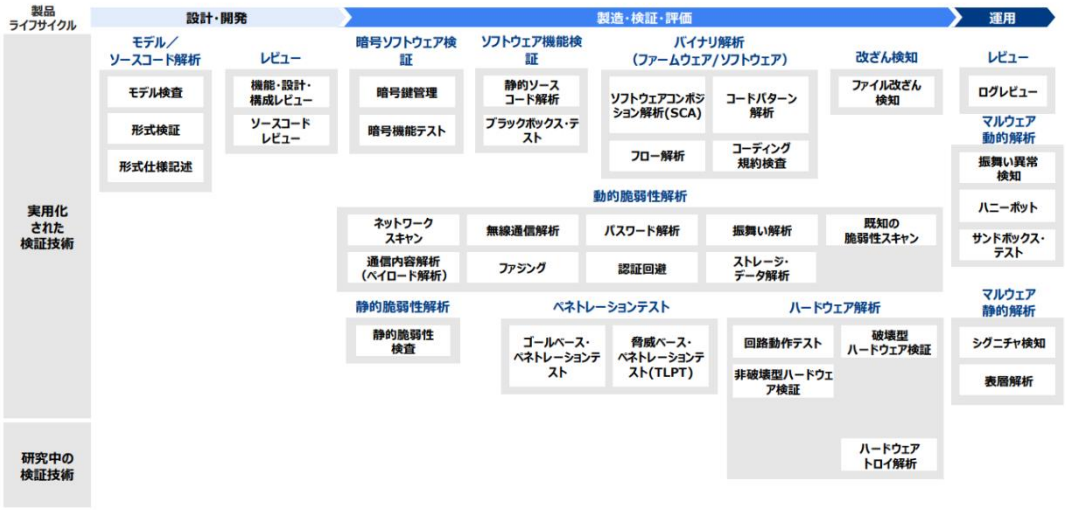
- 欠陥（≒バグ）：要求仕様に適合していないこと。（ISTQB※１, ISO 9000等）
- 脆弱性：攻撃されうる弱点（ISO/IEC 27005※2, IETF RFC 4949, NIST SP 800-30等）
  - 既知の脆弱性：一般に公開されている脆弱性（NVD等）。既知のルールやパターンで検出する。
  - 未知の脆弱性：一般に公開されていない脆弱性。一部の攻撃者のみが知っているゼロデイ攻撃の対象となる弱点（ゼロデイ脆弱性）の他、誰も認知しない脆弱性（真に未知の脆弱性）などがある。技術的には、既知のルールやパターンで検出できない。探索、アノマリー検出、脅威分析等に基づくヒューリスティクス、危険の定義に基づく形式検証などによる。前者については、Threat intelligence （未公開の情弱性へのExploit, Virus情報など） による検証もあり得る。



※1 Defect: An imperfection or deficiency in a work product where it does not meet its requirements or specifications.
※2 Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threats, where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission.

（出典）サプライチェーン・リスク対応のための技術検証体制構築に関する調査報告書（2022 年 5 月）

（参考３）検証技法の俯瞰的整理



（出典）サプライチェーン・リスク対応のための技術検証体制構築に関する調査報告書（2022 年 5 月）