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
内閣官房 内閣サイバーセキュリティセンター（NISC）

※本調査はNISCの委託により、株式会社三菱総合研究所が実施したものです。

調査概要・目的・スコープ

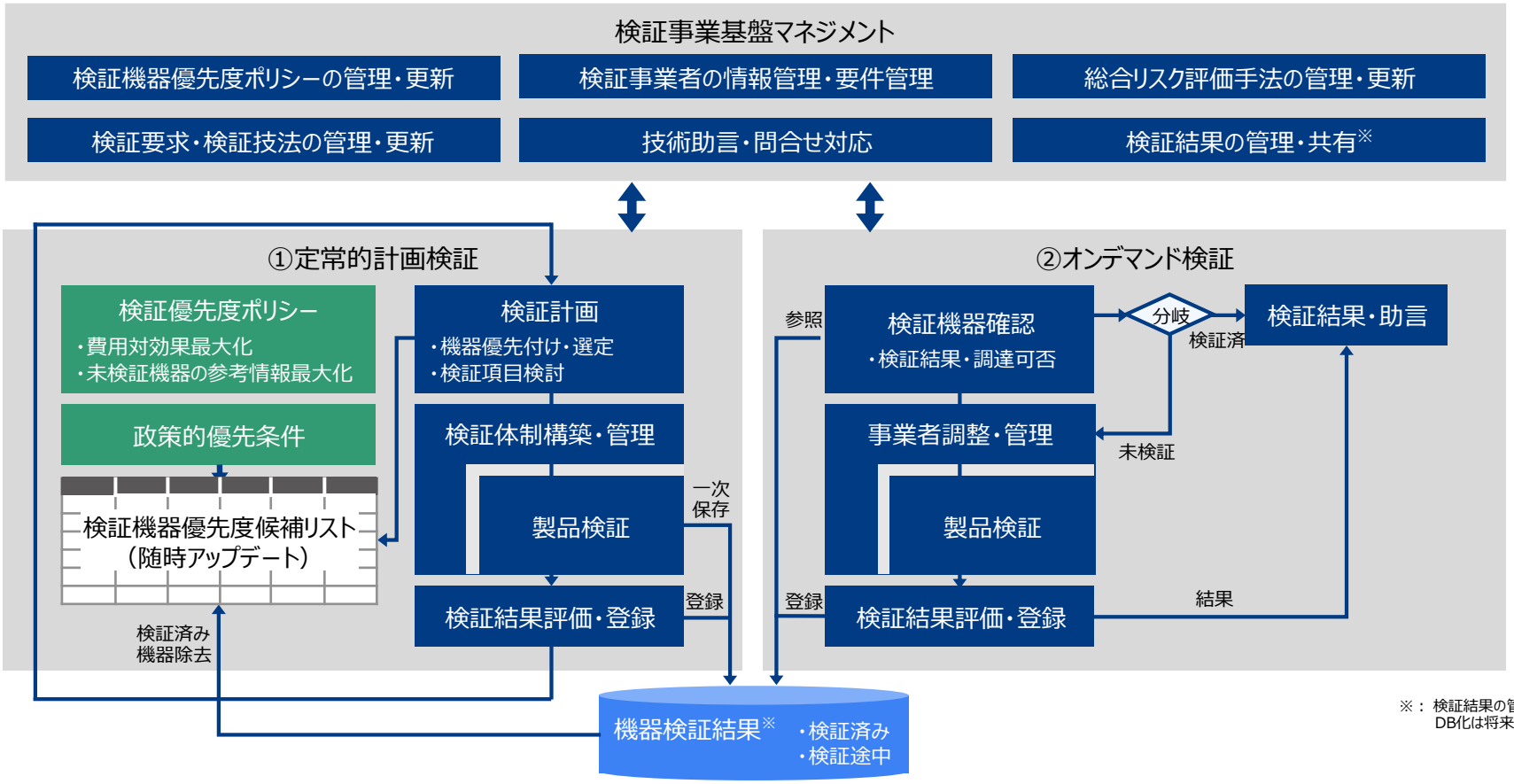
サイバー空間と実空間の一体化が加速的に進展し、情報通信機器のみならず様々な機器がサイバー空間を介して国民の生活に結びついている現状において、これらの機器の信頼性を確保することはより一層不可欠なものとなっている。また、機器の信頼性を確保するためには、サプライチェーンリスクについても技術的な検証により信頼性が確保されていることが不可欠である。

本件は、機器のサプライチェーンリスクに係る信頼性確保に対し、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ものである。

検証スキームの全体像（改訂）と具体化項目の対応関係

- IT機器について、限られた予算で技術検証によりセキュリティリスクを最小化するため、費用対効果の高い機器の優先付けに基づき定常的な検証を行うとともに、オンデマンドで必要な時に検証を行う２つのプロセスを同時並行で推進する。検証機器優先度ポリシー、検証項目、事業者要件に関わる管理更新は検証事業基盤マネジメントで実施。
- 昨年度からの主な改訂として、①定常的計画検証および②オンデマンド検証の個々の機器検証とは別に、共通的なプロセスとして、検証事業基盤マネジメントを分離・再整理した点が挙げられる。

検証事業プロセスの全体像（デュアル・プロセス）



※： 検証結果の管理・共有は、検証報告書による。
DB化は将来課題

総合評価ロジック（脆弱性評価と検証達成度評価に基づく分析）

昨年度の総合評価区分をアップデートして以下の設定した。改訂点は、脆弱性評価における「懸念あり」を細分化したことである。

①【脆弱性評価】 脆弱性の懸念が大きいか（許容できないか）？
②【検証達成度評価】 検証達成度は十分か？

			②検証達成度評価	
			検証達成度 高	検証達成度 低
①脆弱性評価		4) 脆弱性の懸念が低い	調達許容 （ホワイト） Trustworthy	検証不十分 （グレー） Assurance Deficit
	懸念あり	3) エンジニアリング成熟度に懸念がある	懸念 Middle （ブラック） Untrustworthy Middle	
		2) 脆弱性の深刻度が相対的に高い	懸念 High （ブラック） Untrustworthy High	
		1) 許容できない脆弱性が残存	懸念 Critical （ブラック） Untrustworthy Critical	

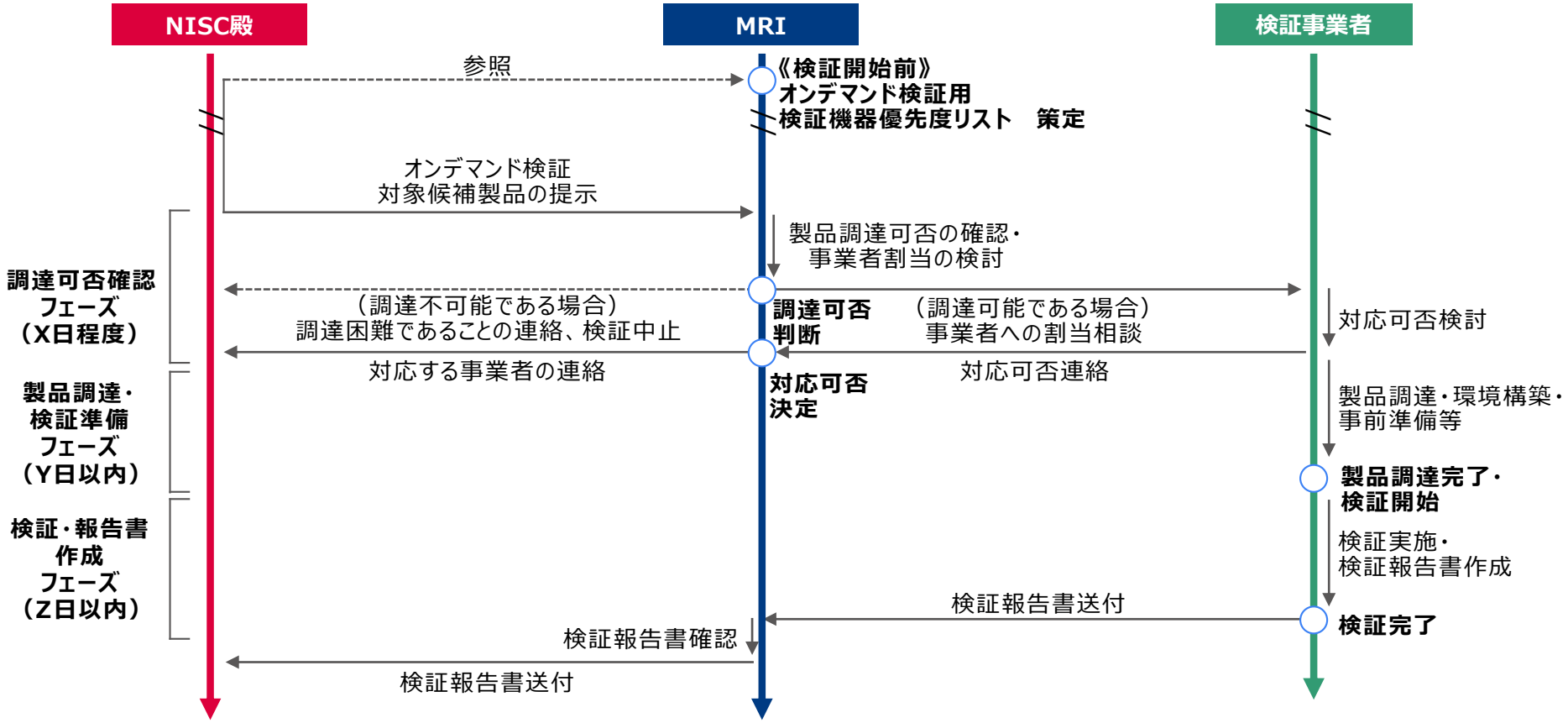
定常計画検証の全体プロセス

- 定常計画検証の全体プロセスは以下のとおり。
- 対象製品の選定・割当を行った後、各製品に適用する検証内容（検証技法）を決定した。
- 実際の検証は前期・後期の2フェーズに分けて実施した。
- 検証結果を踏まえ、検出された脆弱性の分析や検証達成度の分析を実施した。

検証方針の検討、対象製品の選定	検証事業者の割当、検証内容の決定	前期定常計画検証 (2021.10～2021.11)	後期定常計画検証 (2021.12～2022.1)	検証結果の整理
● 定常計画検証全体の進め方について検討した ● 検証対象機器の優先度付けを実施し、検証対象製品を特定した	○ 検証事業者に対して、選定した検証対象製品の割当を行った ○ 各製品に適用する検証技法について、各製品の特性や検証事業者の能力を基に割当を行った	● 割当を行った検証技法に基づき、検証事業者による製品への前期定常計画検証を実施した ● 検証の状況について、適宜進捗状況を確認した	● 割当を行った検証技法に基づき、検証事業者による製品への後期定常計画検証を実施した ● 検証の状況について、適宜進捗状況を確認した	● 検証結果の比較整理を実施した ● 検出された脆弱性の分析や検証達成度の分析を実施した ● 検証により得られた知見に基づき、今後の課題を整理した

オンデマンド検証の全体プロセス

- オンデマンド検証は短期間の検証であるため、調達可否確認のフェーズ、製品調達・検証準備のフェーズ、検証・報告書作成のフェーズの3つのそれぞれフェーズにおいて、期間制約（上限日数）が存在。（それぞれ営業日換算でX日、Y日、Z日と定義。）
- 今年度事業では、それぞれの期間制約についてX=3、Y=7、Z=7と仮置きした。（ただし、要望があれば追加対応を実施した。）
- また、検証開始前に、オンデマンド検証が可能な機器区分（オンデマンド対象機器リスト）を整理した。

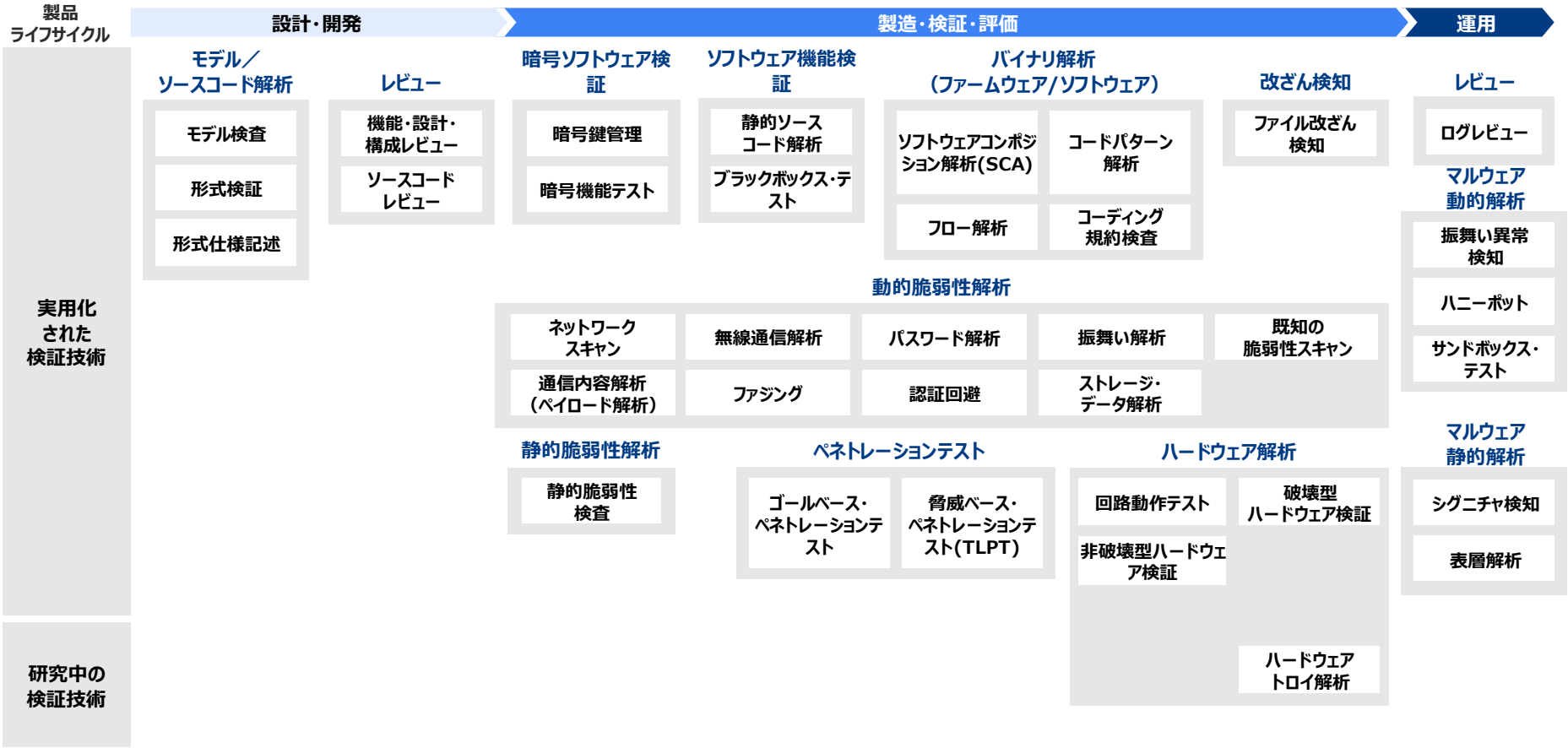


課題の全体像

- 本年度事業を通じて集約・整理した主な課題について、課題分類（技術・運用、組織・人材）と実施時期（短期、中長期）に基づき全体像を以下に示す。

	短期課題（3年程度）	中長期課題（３年以上）
検証実施（技術・運用）	• 検証ポートフォリオ・マネジメント • 総合リスク評価・助言支援ナレッジベースシステム • 不正機能の分類整理と検証技法のマッピング • 不正機能の意図性評価手法 • オンデマンド検証における検証内容の詳細化 • 機器ベンダが提供するTransparency Centerを利用したホワイトボックス解析の活用方法 • 検証達成度を確保するための運用方法等	• 不正機能の検出手法の高度化 • 未知の脆弱性の検出性能の向上 • 検証要求・検証技法の幅と深さの最適化手法
体制構築（組織・体制）	• 検証対象と検証事業者の検証能力に応じた検証の最適化手法 • 検証者の人材リソース・マネジメントの効率化 • 検証事業者の拡大・知見の整備 • 検証技術・人材について、内製化と外部リソース活用の方針検討	

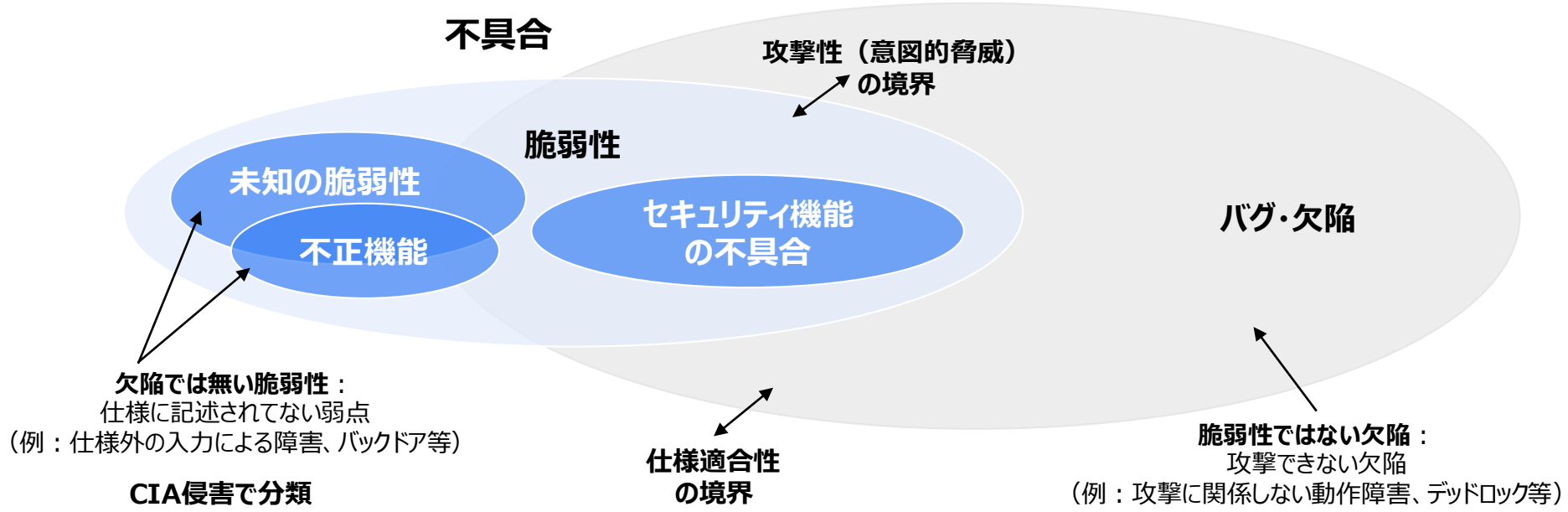
【参考】検証技法の俯瞰図



出所）三菱総合研究所作成

【参考】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。



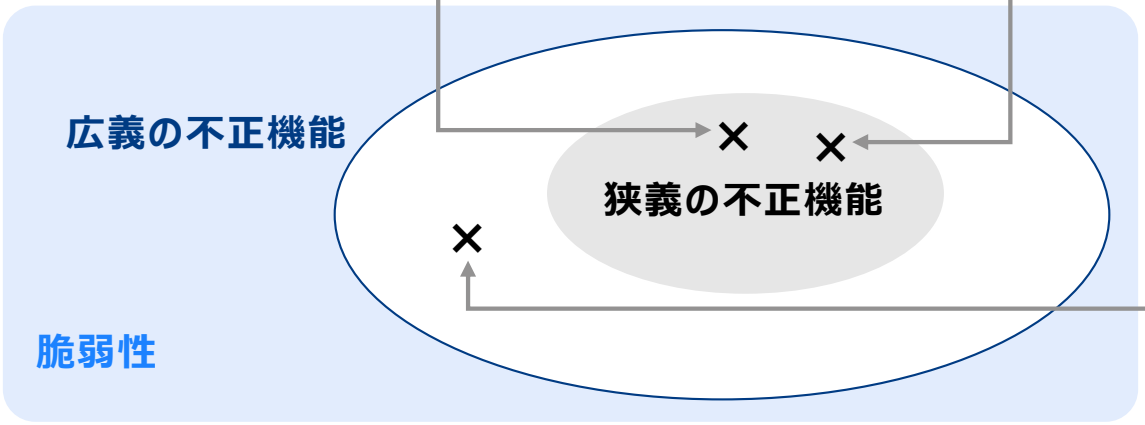
※1 Defect: An imperfection or deficiency in a work product where it does not meet its requirements or specifications.
※2 Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threats, where an asset is anything that has value to the organization, its business operations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

【参考】本事業における不正機能の定義

- 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**）



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（不正機能事例に関する調査）に関する調査報告書

2022年5月
内閣官房 内閣サイバーセキュリティセンター（NISC）

※本調査はNISCの委託により、株式会社ＦＦＲＩセキュリティが実施したものです。

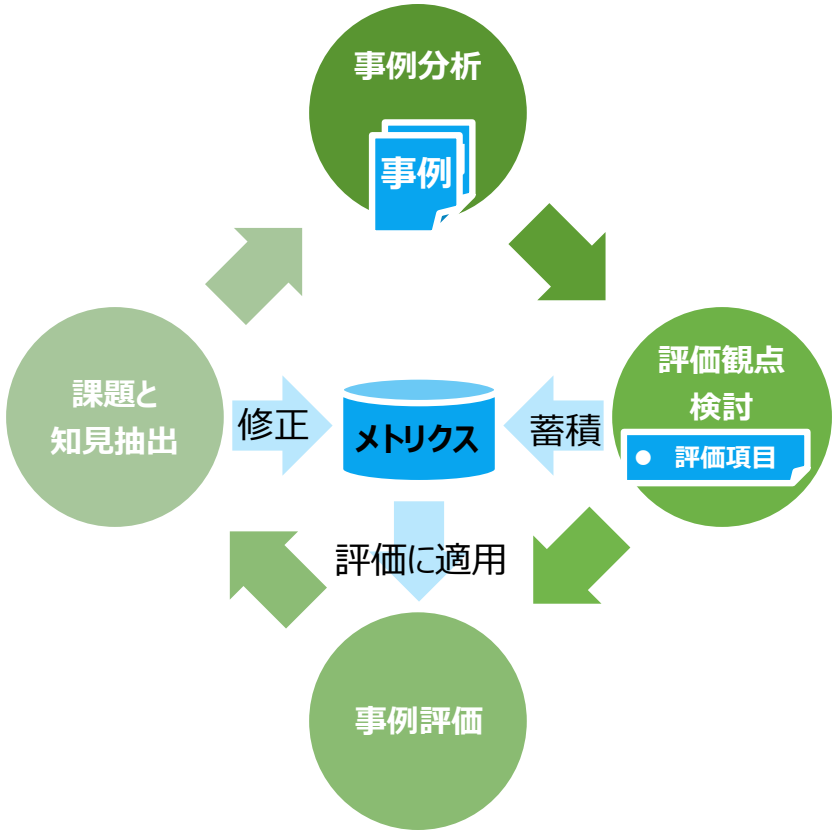
事業概要

○ 不正機能事例に関する情報の蓄積が少なく、事例の**情報収集・分析**から着手

○ 不正機能が存在すると疑われる機器やソフトウェアを分析して、**不正機能と判断する評価観点の抽出**および**評価メトリクスの定義**を実施、さらに実際に**事例に適用することでその有効性を評価**

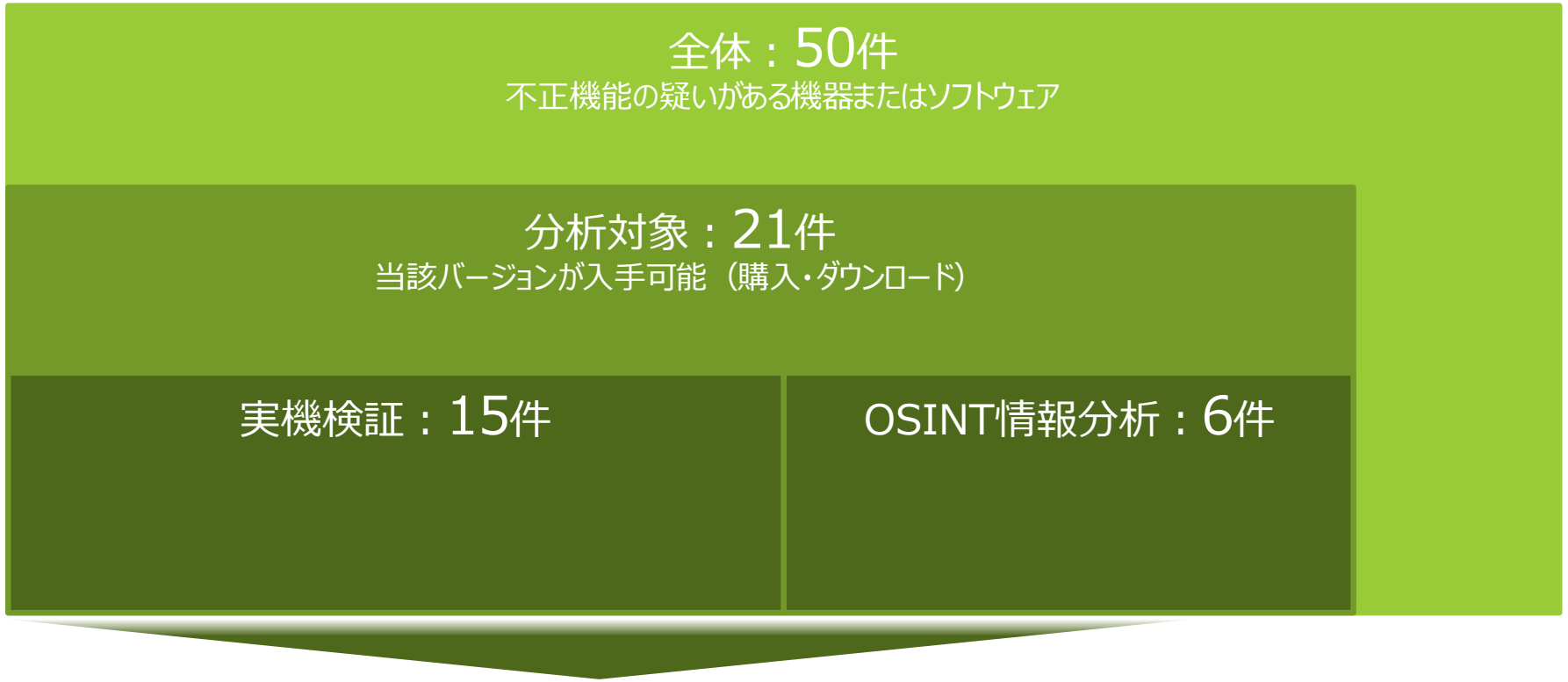
○ 分析～評価のサイクルを繰り返すことにより、基準の妥当性確認や不足する観点の追加等、精度を向上

- 事例分析
  - インターネットに公開されているセキュリティ関係の記事や研究を収集
  - 機器またはソフトウェア（ファームウェア含む）の実機検証結果あるいはOSINT情報の分析により不正機能の程度を定性的に判断
- 評価観点検討
  - 当該機能が不正機能と判別できる評価観点を検討
  - 当該機器そのものの情報だけではなく、販売ベンダー等に関する周辺情報も活用する
- 事例評価
  - 事例に対して評価観点を確認し、不正機能の程度の判断に有効であることを評価
  - 評価観点毎に、不正機能の程度に与える影響（重み）を検討
- 課題と知見抽出
  - 分析～評価のサイクルにおいて明らかとなった課題及び得られた知見を整理
  - 次のサイクルの改善に活用する



事例分析

- ○ 実機検証またはOSINTで得られた情報を基に、設計の意図および悪意の有無を分析
- ○ 分析結果は不正機能／脆弱性／正規機能に分類、特に不正機能に関しては特に意図性があるものを狭義の不正機能と定義して分類
- ○ また、得られた情報および分析結果は評価観点として活用



評価観点検討

○ 実機検証またはOSINTで得られた情報を基に、当該機能が不正機能と判別できる評価観点を検討
  ○ 発生する事象や、発動条件、検出しにくさといった観点で抽出した評価観点を分類
○ 評価するうえで、当該機器だけではなく、販売ベンダー等に関する周辺情報も有用であると考えられる

当該機器に関する評価観点の分類

(1) 発生する事象
- 「正規機能を正規方法で利用すること」からの逸脱度合いを評価する観点

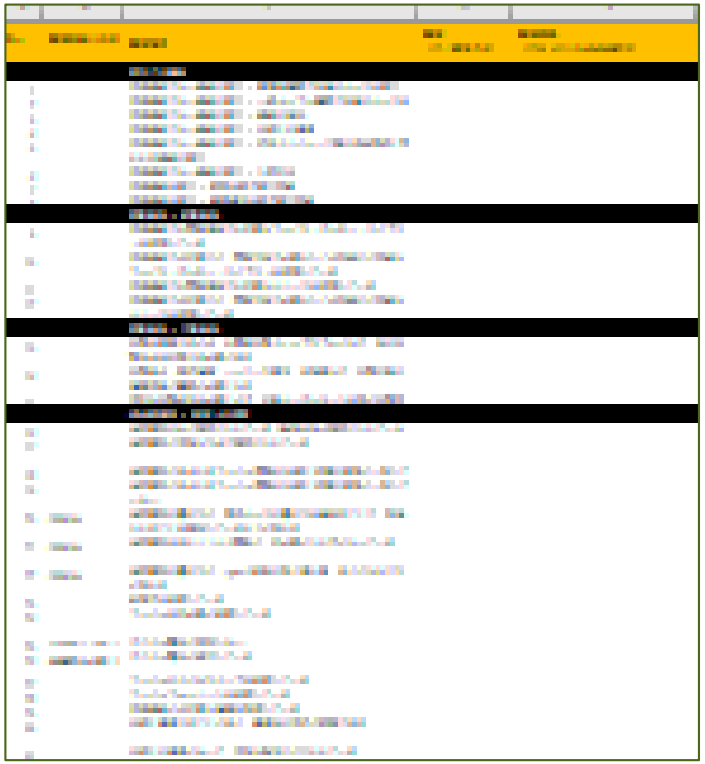
(2) 発動条件
- 当該箇所を利用する難易度を評価する観点

(3) 検出しにくさ
- 当該箇所の存在に気付かれたくない「意図」の有無を評価する観点

(4) 影響度が高まる環境要因
- 当該箇所を利用した攻撃への動機付けを評価する観点

販売ベンダー等に関する周辺情報

- セキュリティ開発スキル（アドバイザリ公開、脆弱性対応プロセス等）
  など



事例評価

- 各事例の「不正機能の程度」の定量化
  - 評価観点毎の「不正機能の程度への影響」を数値化して重み付けする
  - 各事例が該当する評価観点の重みの和を、「不正機能の程度」のスコアとする

正機能の程度への影響度合い	重み付けの値
不正機能の程度は極めて大きく高まる	3
不正機能の程度は大きく高まる	2
不正機能の程度は高まる	1
不正機能の程度は変わらない	0
不正機能の程度は大きく下がる	-2

  - 注意点
    - 順位尺度を変換しているため厳密な数値ではなく、あくまで定量化の試行
    - 2021年度調査では傾向をみるために実施

知見と課題

- 知見

#	カテゴリ	知見
1	定量化	定量化の試行結果では不正機能との一定の相関
2	評価基準	既存フレームワーク（CVSS）との差異
3	事例評価	製品カテゴリ・製造国の文化の考慮
4	事例分析	分析開始時に事前収集すべき情報

- 課題

#	カテゴリ	課題
1	事例分析	事例分析数の積増し
2	評価基準	周辺情報記載方法の改善
3	定量化	評価項目の組合せの考慮
4	評価基準	「不正機能の程度」の細分化
5	定量化	実用的な定量化式
6	事例分析	実機調達による分析の効率化
7	事例分析	解析ツール調達/開発

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評価技術動向調査に関する調査報告書

2022年5月
内閣官房 内閣サイバーセキュリティセンター（NISC）

※本調査はNISCの委託により、株式会社ＦＦＲＩセキュリティが実施したものです。

本報告書の概要

- 背景
  - 昨今、IoT機器の普及やビッグデータの活用促進、またそれによるAIの発展による社会のデジタルトランスフォーメーション（DX）化が進んでいる
  - サイバー空間と実空間の一体化が加速的に進展しており、情報通信機器のみならず様々な機器と社会インフラがサイバー空間を介して国民の生活に結びついている
  - そのような中、社会インフラで利用する情報通信機器の信頼性を確保することが不可欠である
  - 信頼性確保のためには、サプライチェーンを含む関係者が、情報通信機器の脆弱性などのセキュリティリスクの影響を理解し、緊急性や重要性から対策の優先度の判断をする必要がある
  - そのため、セキュリティリスクの定量化等による客観的な評価技術が必要であり、今後の客観的な評価技術の実現に向けた課題や解決策を検討・整理する

- 本報告書の内容と構成
  - セキュリティリスクの評価技術についての国内外の研究機関における研究や、セキュリティベンダーによって提供されているセキュリティリスクの評価サービスについて、8個の事例を調査した
  - 調査結果を体系的に整理し、大局的かつ定量化等による客観的な評価技術の研究やシステム開発を見据え、現時点の課題や本課題に対する解決策を検討・整理した

評価手法の選定

- ８つの評価手法の選定においては、以下の４つの観点における分類の要素が必ず一度は出現するように、公開情報の充実度とヒアリングの可能性に基づいて調査対象の候補を選定した

Ⅰ.リスク評価としての性質
分類：潜在的リスク評価　／　顕在的リスク評価
※潜在的リスク評価：金額として算出していない潜在的なリスクの評価
顕在的リスク評価：金額として算出した、損害額として顕在化するリスクの評価

Ⅱ.評価手法の提供主体
分類：民間事業者／政府機関（パブリックセクター）／大学等研究機関

Ⅲ.国内及び海外
分類：日本国内　／　海外

Ⅳ.評価手法の提供形態
分類：サービス　／　研究　／　その他

評価手法の選定

本報告書における調査対象

		分類の観点			
評価手法	評価の対象範囲	Ⅰ	Ⅱ	Ⅲ	Ⅳ
米国国防総省 CMMC 2.0	組織・ システム（運用・管理）	潜在的	政府機関	海外	その他
株式会社ラック 情報セキュリティプランニング	組織・ システム（運用・管理）	潜在的	民間事業者	日本	サービス
日本電気株式会社 サイバー攻撃ルート診断サービス	システム（技術）	潜在的	民間事業者	日本	サービス
あいおいニッセイ同和損害保険株式会社 サイバーセキュリティ保険及び予想最大損失額（PML）の算出	インシデント	顕在的	民間事業者	日本	サービス
株式会社日立研究所 セキュリティリスクマネジメント態勢を支援するリスク評価・リスク可視化技術/サイバーインシデントの損害発生モデルシミュレータによるサイバーリスク評価手法	システム（技術）	顕在的	民間事業者	日本	研究
ISOG-J日本セキュリティオペレーション事業者協議会 セキュリティ対応組織の成熟度診断	組織	潜在的	民間事業者（協議会）	日本	その他
東邦大学 金岡晃准教授 Networked-system Security Quantification model	システム（技術）	潜在的	大学	日本	研究
特定非営利活動法人 日本ネットワークセキュリティ協会(JNSA) インシデント損害額調査レポート 2021年版	インシデント	顕在的	民間事業者（NPO）	日本	その他

※ 分類の観点：

Ⅰ.リスク評価としての性質　Ⅱ.評価手法の提供主体　Ⅲ.国内または海外　Ⅳ.評価手法の提供形態

課題と考察（１／３）

Ⅰ.評価のためのデータ取得の課題

❶法令や運用の壁などにより手法の作成・改善・研究のためのデータの収集が難しいという課題

- データの共有をしやすくする法令や運用の改正、リスク評価で使用できるデータセットの作成が解決策としてあげられており、総じて産官学の連携が不可欠である
- 法令や運用の改正については慎重な議論が求められる一方で、ウクライナ情勢に関連した攻撃が激化するなど 、サイバーセキュリティをめぐる情勢は刻々と変化・激化しており、損害保険会社や損害保険料率算出機構などのステークホルダーを含めた議論を始める必要がある
- リスク評価で使用できるデータセットの作成については産学連携が必要であるが、データセットの存在によって、作成した手法を他の手法と評価しやすくなることで、分野全体での評価手法の改善が促進され、その分野の研究を活発化させると考えられる

❷コストが高い、システムのスキャンが難しいなどにより評価する上で必要なデータの収集が難しいという課題

- 技術的なデータ取得の難易度の課題、人によるデータ取得の難易度の課題及びデータ取得のコストの課題に分けられる
- 技術的なデータ取得の難易度の課題は、対象のデータの計測が難しいといったものであり、これらについては、既存手法との連携や、さらなる研究が必要である
- 人によるデータ取得の運用上の難易度の課題ついてはトレーニングの提供により解決することが望ましい
- データ取得のコストの課題については、既存手法との組み合わせ（チェックシートの作成、エージェントレスでのデータ取得）が有効である

❸その他

- 経営者の多くが、評価手法の精度など技術的な観点ではなく評価指標そのものの権威性を重要視するといった課題については、実績を積むことや、国や公的機関による権威性の付与、またはすでに権威性のある他の手法との組み合わせによって解決しうる

課題と考察（２／３）

Ⅱ.評価手法そのものの課題

❶評価対象・基準の妥当性の課題

- 国及び公的機関あるいは業界団体による権威性のあるガイドラインがあると、それを評価範囲・基準の根拠として用いることができる

❷評価コスト（Ⅰ- ❷のデータ取得のコストは除く）の課題

- AIの活用が解決策としてあげられており、こうした自動化による評価コストの削減が方向性として考えられる
- 端末を集約して計算する手法を取り入れることで問題が緩和される

❸リスク計算の課題

- 各手法で課題の性質が大きく異なる
- リスク計算という評価手法のコアの部分であり、統一的な方向性ではなく、各課題について考えられる解決策をそれぞれ考慮するべきである

❹その他

- 「企業がパッチの適用ができていない」「システムの「塩漬け」が行われている」「自身のIT資産や、インシデントにおける損害額を把握できていない」などの、企業のセキュリティ態勢の問題に起因して、損害額の算定が難しいケースがある
- 国や公的機関がガイドラインを出す、古いシステムのリプレイスに補助金を出すといったパブリックアプローチによって、企業のセキュリティ態勢を強化することが重要である

課題と考察（３／３）

Ⅲ.リスクコミュニケーション上の課題

- 経営層や投資家等が他の経営リスクと比較しセキュリティリスクを重視していないことが要因である
- 予想される損害額の算出が有効であると考えられる一方で、定量化という面だけでなく復旧時間などの視覚的な情報などの「リスクの見せ方」も重要になる。このため、セキュリティ心理学も踏まえて、定量的リスク値以外の有効なリスクコミュニケーションも考慮すべきである
- 意思決定について分析する理論（決定理論）では、不確実性下における意思決定において、期待効用最大化原理や、マクシマックス原理などの意思決定原理に沿って分析できるため、今回調査したような手法と組み合わせ、具体的な値を代入することで、各原理に基づいた合理的な意思決定が提示されうる
- 投資家へのリスクコミュニケーションにおいては、サイバー攻撃による被害が年々深刻化することによって意識をせざるを得なくなることを期待する

Ⅳ.時系列性による課題

- マルウェアのトレンドが変わっていくなど、サイバーセキュリティをめぐる環境が時間とともに変化していくことで、評価結果の信頼性・妥当性が時間とともに落ちていく
- 現状では、再評価を定期的に行う以外に対処法がないため、評価手法の実施コストを下げることで、再評価をしやすくすることが必要である
- 時系列データの分析に知見のあると考えられる統計学者・計量経済学等との連携により、時系列的な情報を考慮したセキュリティリスクのモデリングを進めていくことが重要である