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

2021年3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

●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。

●本事業では、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の試行を実施し、我が国においてサプライチェーンリスク対応のための技術検証の枠組みを構築する際のガイダンス及び課題を導出する。

検証試行計画の策定

検証事業スキーム・検証プロセスの策定　検証業務プロセス・実施主体等

- 検証業務は、機器単位の検証業務プロセスと、事前の整備が必要な検証準備プロセス、定期的に実施が必要な共通業務プロセスから構成される。
- 機器に対する技術的な検証は、検証業務プロセス内の技術検証プロセスによって実施される。

プロセス	フェーズ	業務内容・手順等
検証準備プロセス （検証業務基盤整備） 事業全体の初期に1度実施	検証項目の策定	・検証要求・検証技法の体系表と検査項目の内容整理。 ・検証要求・検証技法の対応関係、検証機器・検証技法対応表
	検証事業者の要件定義	・検証事業者の能力、リソース、設備等の要件を定義
	検証対象機器の優先付け方法の策定	・検証対象機器の優先付け方法を策定
	検証結果の管理共有方法の策定	・検証結果の共有方針、共有情報の内容、共有環境
検証業務プロセス （機器単位の検証業務）	検証計画立案	・検証対象、動作環境の定義 ・検証要求分析 ・検証体制検討 ・検証計画策定
	検証体制の構築・管理	・検証管理体制の構築 ・外部委託業務の検討と検証事業者の選定 ■検証事業者との委託契約（検証仕様、情報管理の合意）
	技術検証プロセス	■ 技術検証計画（検証項目,スケジュール等の作成と受発注者による合意）
		■技術検証体制構築（検証担当者等の体制）
		■予備検証の実施（機器レビュー・簡易予備検証）
		■検証計画見直し（予備検証に基づく検証範囲最適化）
		■本検証・検証項目の遂行（検証事業者）
		■遂行管理（進捗管理・レベル管理）
		■検証レポート作成
		■検証レポートのレビュー改訂
		■第三者評価・総合評価（必要に応じて、総合判定）
	検証結果の登録	・検証評価結果を登録・共有可能にする。
共通業務プロセス （検証関連業務） 定期的に繰返し	検証結果の共有	・機器調達省庁に対して検証結果を提供する。
	助言・検証結果の問合せ対応	・機器調達省庁からの依頼に応じて助言、検証結果提供の対応を行う。
	検証対象機器の優先付け（定期見直し）	・策定した検証対象機器の優先付け方法に従い、優先付けを行う（年1回程度）
	検証要求・検証技法体系表の改訂	検証実績の蓄積等に応じて、検証要求・検証技法の粒度、網羅性を考慮して検証項目を改訂
	包括的リスク評価	技術検証結果に加え、IT機器ベンダーのエンジニアリング能力、信用評価など総合的な分析結果に基づき調達機器の評価を行う。

凡例：■ 検証事業者が関わる項目

検証要求・検証技法の体系整理　検証要求と検証技法の位置付け

- 「検証要求」は検証対象IT機器に求められる条件・性質、「検証技法」は、検証事業者・ツールに求められる条件であり、相互に関連するが視点が異なる。

検証対象機器
（例：ルータ）

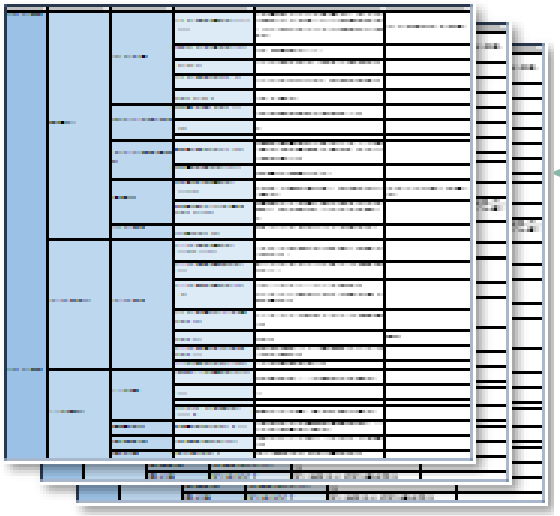
画像：Cisco

検証ツール・技術
（例：脆弱性検査ツール）

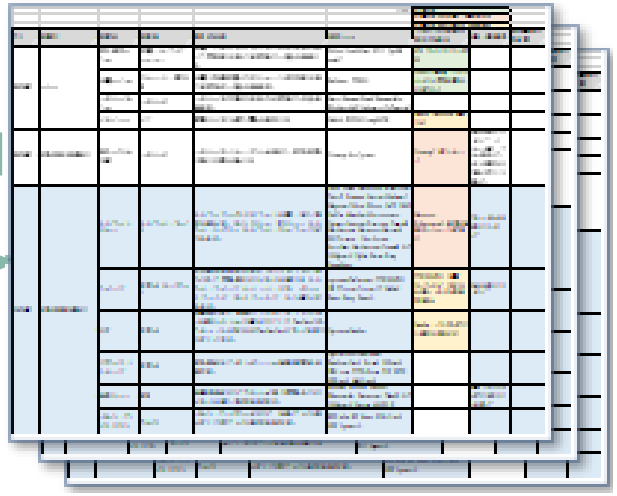
画像：Netsparker

検証

検証要求
＝対象機器に求められる条件



検証技法
＝検証事業者・検証ツールに求められる条件



検証項目体系表
（検証要求・検証技法）

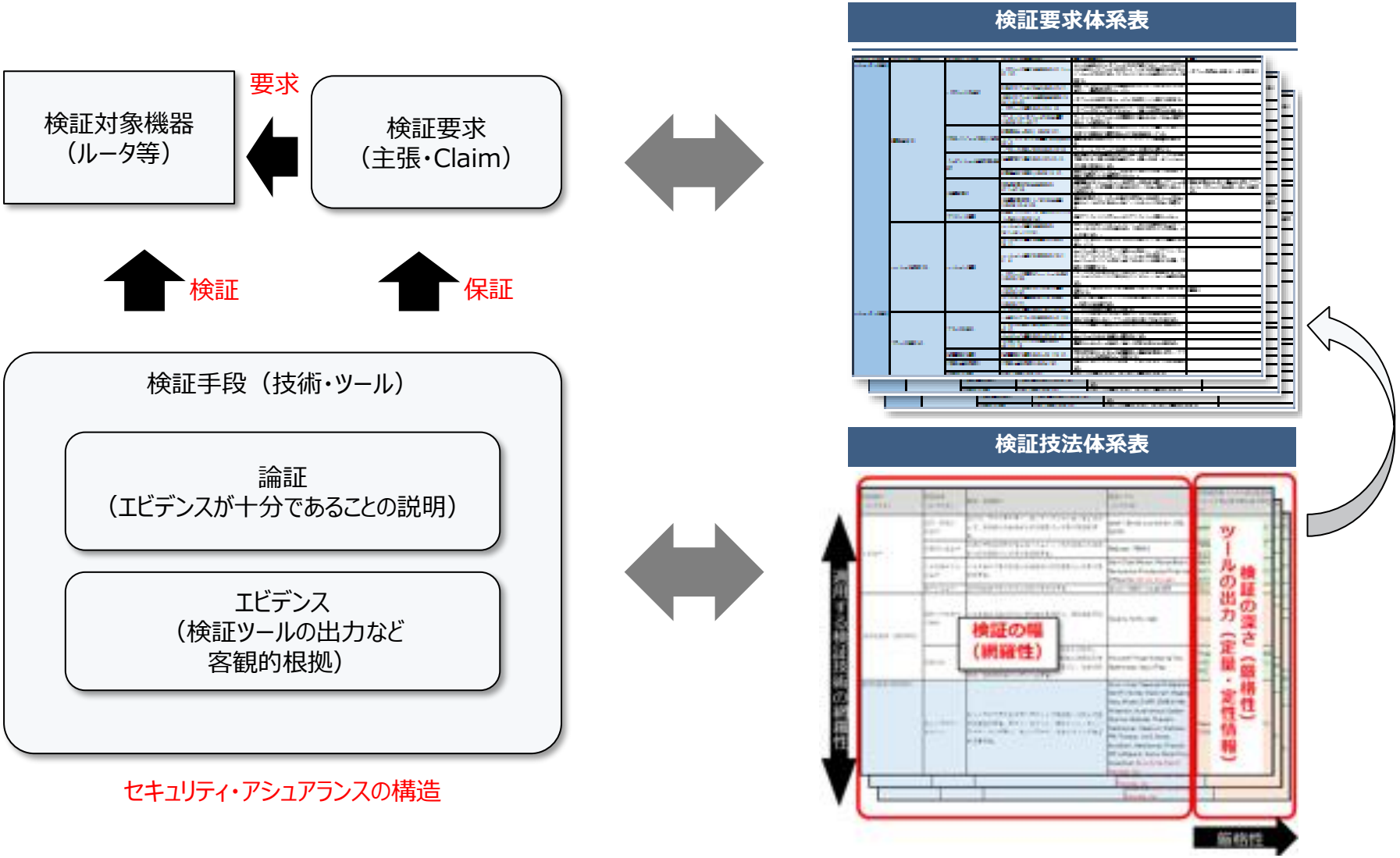
要求の充足

技術に対するニーズ

検証要求・検証技法の体系整理

検証要求・検証技法の体系整理

- 検証対象機器に応じて検証要求が定義（選定）され、検証対象機器に対して検証技法（技術・ツール）を適用することで、検証の達成度に応じて、検証要求を保証（見える化）する。



セキュリティ・アシュアランスの構造

検証試行と検証結果のとりまとめ

セキュリティ検証に求められる2つの方向性（整理）

検証の方向性（排他的では無い）	脆弱性の検出 ⟷	セキュリティ・アシュアランス
概要	問題を発見する。 （脆弱性等を発見する。）	問題が無いことの確からしさを見える化する（後述）。 セキュリティ機能が正しく実現され、脆弱性などが無いことの確からしさを、検証の達成度により見える化する。
効果	懸念機器であることの根拠（問題）を明示できる。	脆弱性が偶然見つかったのではなく、体系的に検証し、検証達成度の高さかを示すことで、推奨できる機器であることの確信を高める。
問題点	脆弱性等が発見できない場合、脆弱性が存在しないことやその他のことについて示される情報が少ない。	定量的な言及が難しい場合がある。（定量評価と定性評価の組合せにより、全体としてのレベル感を示す。）

サプライチェーン・セキュリティで求められる事

- サプライチェーン・セキュリティの確保においては、調達者などのステークホルダーに対して、機器や組織のトラスト（信頼）を確保することが求められる。そのためには、セキュリティ自体の向上に加え、他のステークホルダーに対するセキュリティの説明力の向上が求められる。両者は独立した概念（セキュリティが高くても、説明力が低ければ信頼は得られない。）
- サプライチェーン・セキュリティを確保するためには、脆弱性を検出だけでなく、セキュリティ・アシュアランスが重要になる。
- 脆弱性等の検出のみに意識が向き、セキュリティ・アシュアランスの意識が低いと、脆弱性が見つからなければ、検証した努力が有効に活かせない。
- 検証で求められることは、たまたま脆弱性を発見したり、脆弱性が発見されない時何も言えないということではなく、然るべくして脆弱性を発見し、脆弱性が発見されない場合においても、どの程度検証できたのか体系的に見える化することで確信を与えること。
- そのためには、属人的に脆弱性を発見するのではなく、体系化された脅威分析手法（Attack Tree, SDL, MITRE ATT&CK等）の適用により、どの程度検証を行ったか他のステークホルダーに見える化することが重要である。

(NISTの定義） **Trustworthiness** = The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

※**アシュアランス**とは、他のステークホルダに対して、明示された基準が満たされていることについてエビデンスに基づき確信を与えること（信頼性の付与）

ガイダンスの策定と課題の整理

検証に関するガイダンスの策定

- 本事業において、検証事業推進のための以下のようなガイダンス類を策定し、試行検証を通じて検証事業者から意見を踏まえて、ガイダンス類の改訂を行った。
  - 検証事業スキーム・検証業務プロセス
  - 検証要求・検証技法体系（検証項目）
  - 検証要求・検証技法対応表、 検証機器・検証技法対応表、 検証ツール選択法
  - 検証対象機器の選定方法
  - 検証レポートフォーマット、検証事業者に対する要件書（下記）

検証レポートフォーマットの構成

1. 目的
2. 本書の位置付け
3. レポートの構成内容及びフォーマット等
   - 3.1 目的・観点
   - 3.2 対象機器と想定する利用環境
   - 3.3 検証範囲
   - 3.4 検証の前提とリスク
   - 3.5 テスト環境とテスト装置
   - 3.6 レポートの構成
   - 3.7 検証組織と体制（担当者）
   - 3.8 テストスケジュール（計画）
   - 3.9 結果要点
   - 3.10 技術検証結果
     - 3.10.1 検証項目と検証要求の対応関係一覧
     - 3.10.2 検証項目ごとの結果
       - (1) 検証項目の概要
       - (2) 対応する検証基準（検証要求・検証手段）
       - (3) 検証条件
         - 1） 検証技術・ツールの条件
         - 2） 検証データ
         - 3） 検証結果の再現に必要となる条件（その他）
       - (4) 検証結果と根拠説明
       - (5) 検証の達成度とリスク
       - (6) 付録：検証結果出力データ
4. まとめ
5. 付録

検証業務における検証事業者に対する要件の構成

1. 目的
2. 検証事業者の位置付け
3. 引用規格・規定等
4. 検証事業者に対する要件
   - 4.1 一般
   - 4.2 適用範囲
   - 4.3 技術的記録
   - 4.4 要員の適格性及び資格
   - 4.5 要員の教育・訓練・ノウハウ継承
   - 4.6 施設および環境条件
   - 4.7 検証の方法・妥当性の確認
   - 4.8 設備・装置の保有・維持・トレーサビリティ
   - 4.9 検証品目の取り扱い及び識別および保管
   - 4.10 検証結果の報告
   - 4.11 その他

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（不正機能に関する調査）報告書

2021年3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。

スコープ

（仕様書の「目的及び内容」から抜粋）

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検証体制の構築を進めている。本事業では、特に、実装技術、検知技術及びプロセス分析などの観点から、不正機能に関して技術的な調査を実施する。

対象機器：
- 情報通信機器
- IoTデバイス
- OT機器
- PC/サーバー

など

対象機能：
サプライチェーン上で機器に混入する不正機能

調査分析対象：
- 不正機能の実装技術
- 個別実装の検知技術
- 検知プロセス
- 調査プロセス

ア　不正機能に関する技術面を含む詳細な体系整理

- 調査範囲
  - MITRE ATT&CKの活用
    - Enterprise、Mobile、ICS
- 調査した個別技術の数：595個
- 体系的整理のための分類
  - 攻撃手法の目的（Defense Evasion、Lateral Movement等MITRE ATT&CKのTacticsから）
  - 前提環境（OS、権限等）
  - セキュリティ機能（FW、認証機構等）

ア　不正機能に関する技術面を含む詳細な体系整理

- イ工程に進めるための選別に用いた整理・分類
  - 対象外
    - 「初期感染のみの手法」「機器外からの攻撃」「攻撃手法ではない」
  - 優先度
    - 高：5つの適用基準（「非常に高い権限の取得」等）
    - 中：3つの適用基準（「抽象的な定義」等）
    - 低：8つの適用基準（「検知方法が明確」等）
- 選別結果
  - 優先度高のもの：146個
  - 優先度高ではないが選定された項目：13個
  - 優先度高だが除外された項目：17個

→ **イ工程の対象：142個**

イ　個別技術に関する実装内容の調査・整理

- 調査対象数：142個
- 機能ごとの分類

分類	個数	概要
通信にかかわる個別技術	16	攻撃者から接続する通信技術、および不正機能による通信傍受技術、C&Cサーバーとの通信など
Active Directoryにかかわる個別技術	9	Active Directoryが管理する情報を攻撃者が不正に取得するための技術や、不正認証を可能にする技術など
認証・認可にかかわる個別技術	18	不正な認証を行う技術、認証を回避する技術、およびバックドアアカウントと呼ばれる隠しアカウントなど
プログラムの実行にかかわる個別技術	46	プログラムを直接実行する技術、不正機能を含むファイルを別の正規プログラムに不正に読み込ませることで間接的に実行する技術、カーネルやファームウェアに不正機能を実装するための技術など
検知回避にかかわる個別技術	39	正規のプログラムに見せかけて実行するための技術、データを検知困難にする技術、活動記録を改ざん・消去する技術など
解析困難化にかかわる個別技術	10	データを加工して解析実施者による読み取りを困難にする技術、解析用環境では不正機能が動作しないようにする技術など
サービス拒否にかかわる個別技術	2	データの破壊あるいは読み取り困難化によって業務継続が困難となる技術
情報の窃取にかかわる個別技術	2	モバイル端末における攻撃事例があった情報窃取技術

ウ　個別技術に関する検知方法の調査・整理

- 検知方法
  - 監視・観測する場所（機器内・機器外）
  - 監視・観測するタイミング（機器導入時・不正機能実行時）
  - 取得すべき情報（ログ・パケット）
  - 分析・把握するための技術
    - 静的解析
      - 例：実行ファイルの解析、ポートスキャン
      - 詳細な解析が可能だが、リアルタイム検知には不向き
      - 攻撃発生の前に検知できるため、可能な限り静的解析を優先する
    - 動的解析
      - 例：ログ解析、パケット解析
      - リアルタイムに検知できるが、不正機能が実行されるまで検知できない

エ　個別技術に関する検知の難易度の分析・スコアリング

- 以下の項目について0または+1のスコアを定義し、各検知方法についてスコアリングを行った
  - 監視・観測
    - 既定のコマンドやツール等で監視・観測可能なものは+1
  - 情報取得
    - 取得が容易なものは+1
  - 分析・把握技術
    - 取得した情報単体で分析・把握が可能なものは+1
  - ツール化
    - 比較的容易に情報取得・分析の自動化が可能なものは+1
  - 検知可否
    - 自動的に高い精度で検知できるものは+1

オ　不正機能調査に関する各プロセスの分析と課題・知見の抽出

今後継続的な調査を実施していくことを想定した調査活動自体の分析と課題抽出：

- KPT法によるふりかえり
  - 洗い出したProblemは共通点を持つもの同士をグループ化する
  - グループに対するTryを検討することで汎用的・網羅的な対策を立案
  - 対策には実施条件や必要事項、制限・不足事項を明確に記載する

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（未知の脆弱性に関する調査）報告書

2021年3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、国立研究開発法人産業技術総合研究所が実施したものです。

調査概要

サプライチェーンリスクに関わる未知の脆弱性に関する調査

ア）不正機能に係る既知の脆弱性の体系的な整理

イ）既知の脆弱性に関する傾向分析

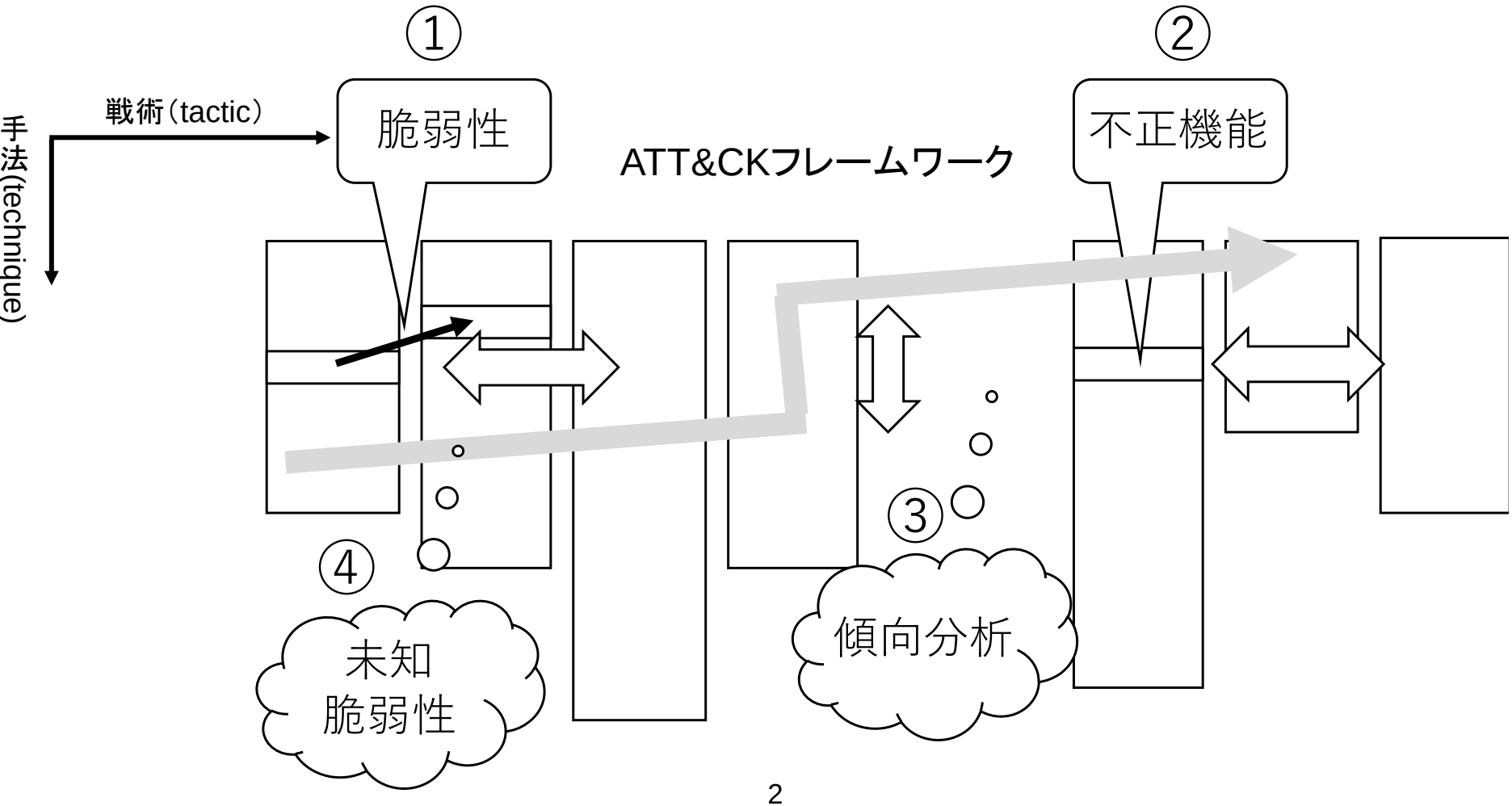
ウ）既知の脆弱性から得られる未知の脆弱性の推定調査・整理

エ）未知の脆弱性に関する検知方法の調査・整理

オ）脆弱性調査に関する各プロセスの分析と課題・知見の抽出

調査における仮説

既知の脆弱性の傾向分析から未知の脆弱性を予測



既知脆弱性の事例分析と傾向

- 近年問題となった脆弱性とそれを悪用した攻撃事例90件を調査
  - CISA CVE Top10, MITRE CWE Top25等参照
  - 古典的なバッファーオーバーフロー
  - 認証手続きの不備
  - インジェクション系、パストラバーサル系
  - Use After Free（Webブラウザのゼロデイ攻撃）
  - ソフトウェアサプライチェーン関係の攻撃
    - SolarWinds社製品へのサイバー攻撃

未知の脆弱性予測

- 攻撃者の意図と攻撃者を取り巻く状況の推測から16件の候補
  - 遠隔から簡単に安定して実行できる再利用性の高い攻撃手法
  - なるべく長い間攻撃を検知されない（ステルス性）
  - 金銭的目的、政治的目的
  - 攻撃手法の流行