サプライチェーンリスク対応のための
技術検証に係る調査報告書

2020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。

技術動向に関する調査

IT製品の信頼性に関する検証技術の調査

- **IT製品の信頼性をソフトウェア・ハードウェアの観点からそれぞれ検証する技術について調査した。**
- **調査においては、検証項目の網羅性を高めるため、検証技術の公開情報に加え、関連ガイドラインや基準等に基づき調査・整理を行った。**
- **最新技術を把握するために、Blackhat等でのセキュリティカンファレンスでの発表資料や技術論文の調査も行い、IT製品の検証に有効と考えられる38の検証技術を整理した。**

関連ガイドライン・研究動向等

- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment
- OWASP Application Security Verification Standard 4.0
- OWASP Testing Guide v4
- PCI Security Standards Council Penetration Testing Guidance
- BlackhatやDefconでの発表資料
- 技術論文

検証カテゴリ・検証技術を整理

検証カテゴリ（12個）

- モデル／ソースコード解析
- 設計書レビュー
- ログレビュー
- バイナリ解析／リバースエンジニアリング
- ネットワークスキャン
- 脆弱性スキャン
- ファジング
- ペネトレーションテスト
- パスワードクラッキング
- ネットワークキャプチャ
- 暗号モジュール解析
- ハードウェア解析

検証技術（38個）

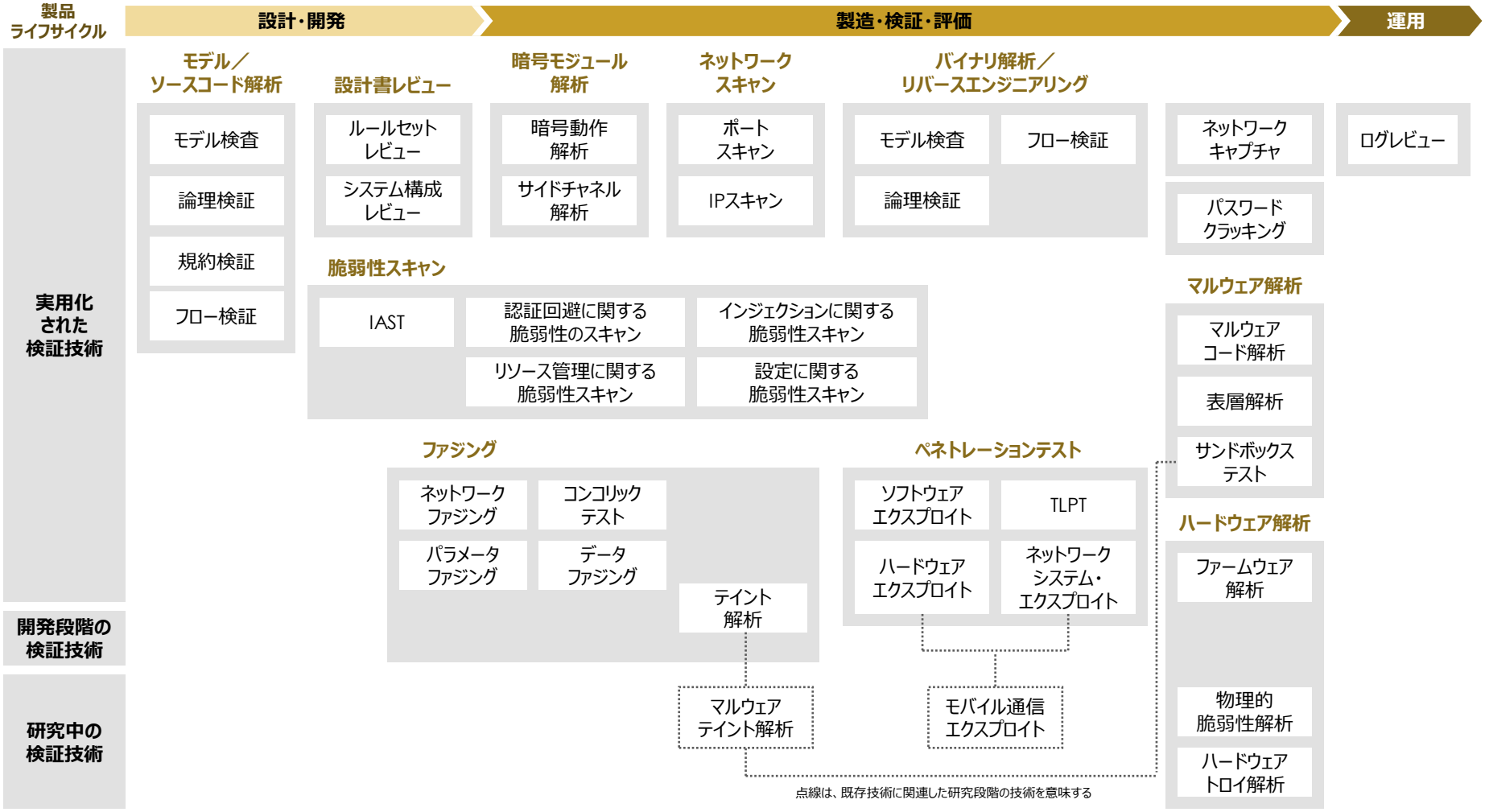
- モデル検査
- フロー検証
- 論理検証
- 規約検証
- ルールセットレビュー
- システム構成レビュー
- ⋮

- 検証カテゴリに紐づく形式で、質的に異なる38の検証技術を整理
- それぞれの検証技術について、代表的なツールや検出可能な脆弱性の例などを整理
- 既存の検証技術だけではなく、研究中の検証技術についても整理

出所）請負者作成

技術俯瞰図の作成・類型化

- 一般論として主な検証カテゴリ及び検証技術は以下のように整理できる。 ※検証技術全てを網羅するものではない。
- それぞれの検証技術が有効なタイミングは製品ライフサイクルに依存する。



出所）請負者作成

検証体制・制度に関する調査

主要国の検証体制・制度の比較分析

- **国際規格に基づくIT製品の検証・認証制度として、CC認証や暗号モジュール認証が官民で活用されており、各国間での相互認証や共同認証等も行われている。**
- **認証制度とは別に諸外国の政府機関が主体となった独自のIT製品の検証制度が運用されている。**

各国独自のIT製品の検証制度

国	制度名・制度の概要
米国	**DHS/CISA/National Cybersecurity Assessments and Technical Services（NCATS）** 政府機関及び重要インフラが保有するIT／OTシステムに対して、各種セキュリティ検証サービスを無償で提供する仕組み。
	GSA/Highly Adaptive Cybersecurity Services（HACS） GSAが政府機関向けに提供するIT調達スキームの中で提供されるセキュリティサービス群。
英国	**NCSC/CHECK The IT Health Check Service（CHECK）** 政府機関や重要インフラのシステムに対して提供されるペネトレーションテストサービス
	NCSC/Certified Assisted Products（CAPS） 政府機関や国防省のユーザが保有する機密性の高い製品に対して、NCSCが直接検証を行う制度
フランス	**ANSSI/Security Visa Qualification** サイバーセキュリティ製品・サービスに対するフランス政府としての推奨を与える制度。
カナダ	**CSE/CCCS/COMSEC** 通信の安全性に関わる製品（重要無線や暗号製品等）に対する、政府機関による調達及び運用上の管理制度。
	CSE/CCCS/SCI リスクアセスメントプログラム 政府機関がICT製品の調達に際の判断の支援として、CCCSが製品リスク分析を行うプログラム
豪州	**ASD/ACSC/High Assurance Evaluation Program（HA）** 機密情報を保護するICT製品を対象とする評価スキーム
	ASD/ACSC/ASD Cryptographic Evaluation Program（ACE） 暗号機能を有するICT製品を対象とする評価スキーム

出所）各種資料に基づき請負者作成