設計・製造におけるチップの脆弱性検知手法の研究開発

実施研究機関：早稲田大学、(株)KDDI総合研究所、(株)ラック
研究開発期間：R1年度
研究開発費：R1年1.99億円　計1.99億円
担当課室名：サイバーセキュリティ統括官室

1．研究開発概要

1. 目的

Society 5.0は、サイバー空間とフィジカル空間が高度に融合したサイバーフィジカルシステムにより実現される。全ての「モノ」がネットワークに接続され、その電子機器の数は、2020年には400億を超えると言われている。新しい価値やサービスが次々と創出され人々に豊かさをもたらす一方で、複雑化するサプライチェーン全体のセキュリティの確保は重要な課題となっている。

電子機器のハードウェア上に組み込まれた不正なチップは、製品出荷後に交換・修正することが難しく、その影響は極めて深刻になる可能性があることから、サプライチェーン上の脅威となっている。また、チップに仕込まれた不正な回路や部品を検出する技術は確立しておらず、産学官で連携して研究開発を加速し、社会実装を進めることが急務となっている。

本研究開発ではハードウェアチップの設計・製造における脆弱性検知手法を確立するとともに、当該技術の社会実装を加速し、サプライチェーン全体のセキュリティ確保に資することを目的とする。

2. 政策的位置付け

- 「未来投資戦略2018」(平成30年6月15日 閣議決定)や「サイバーセキュリティ戦略」(平成30年7月27日 閣議決定)では、サプライチェーン全体のセキュリティ強化のための研究開発を進めることとされている。また、「AI戦略2019」(令和元年6月11日 統合イノベーション戦略推進会議決定)において、AIを活用した高効率かつ精緻な対策技術の確立が目標とされており、国として加速化して重点的に取り組むべき研究開発とされている。
- 「統合イノベーション戦略」(平成30年6月15日 閣議決定)において官民研究開発投資拡大プログラム(PRISM)が推進されているところ、「設計・製造におけるチップの脆弱性検知手法の研究開発」に取り組むことが期待されている。

3. 研究開発目標(アウトプット目標・最終目標)

課題Ⅰ：回路情報を用いて不正回路を検知する技術：外部から調達した設計ツールや設計部品を用いたチップ設計全体の安全性を担保するために、回路情報の中に不正に改変された回路(以下「不正回路」という。)が含まれるか、機械学習等のAIを活用して検知する技術。

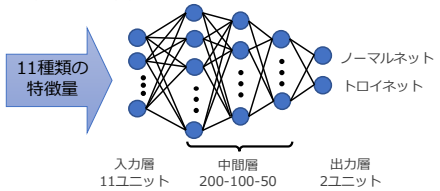
課題Ⅱ：電子機器の外部から観測される情報を用いて不正動作を検知する技術：市販の組込みマイコン等の、回路情報が入手できないチップの安全性を担保するために、不正回路が組み込まれたチップにより構成される電子機器に対し、電力波形の特定部分の電力量や継続時間等、電子機器の外部から観測される情報(以下「外部情報」という。)を用いて、不正動作を機械学習等のAIを活用して検知する技術。

2．研究開発成果概要

課題Ⅰ－ア)①不正回路を識別するための特徴量抽出技術に関する要素技術開発

- ベンチマーク回路を使い、11種類の特徴量を用いることで、ニューラルネットワーク識別器によるトロイ信号線を識別(識別した信号線数は合計で数十万以上のデータ)

多層ニューラルネットワークを用いた識別結果
TPR(True Positive Rate) 84%以上、TNR(True Negative Rate) 95%以上(見逃し確率16%以下、誤検知率5%以下)



課題Ⅰ－ア)②設計・製造におけるチップの脆弱性検知手法に関する動向調査

- ハードウェアトロイの機能ごとに、サプライチェーン上の影響の分析を実施し、研究開発の実用化に反映
  - 情報の機密性及び安全性を脅かす機能はサプライチェーン上流のメーカに法的責任が生じ得るため、対処が必要
  - 今後の実用化・社会実装に向け、機密性を損なう回路／派生回路および安全性を損なう回路／派生回路を検知する技術を確立する

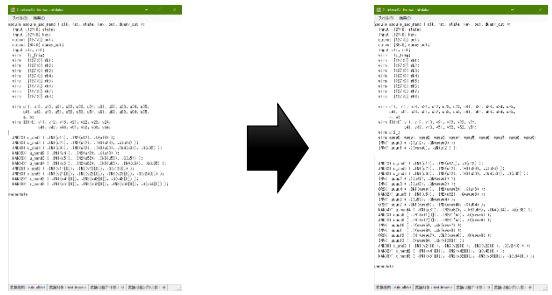
課題Ⅰ－イ)AI/機械学習に基づく不正回路検知技術

(1) 不正回路の体系化を完了
・Trust-HUBから取得した88個のサンプルを詳細に分析し、分類

(2) 不正回路の新規サンプル(12種類)の実装を完了
・IoT開発ボード向け6種類、FPGA開発ボード向け3種類、FPGA搭載ネットワークボード向け3種類を実装

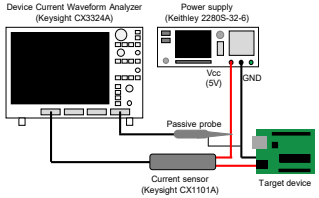


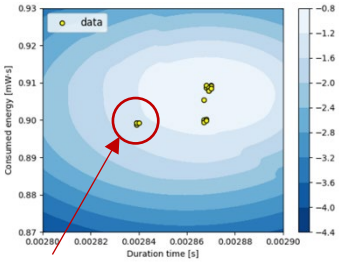
(3) 亜種生成ツールを開発
・不正回路の回路情報(ゲートレベル記述のVerilog-HDL)から、亜種の回路情報を自動生成するツールを開発。



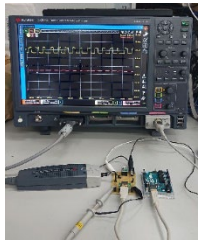
課題Ⅱ－ア)外部情報を取得する電子機器の動作のモデル化技術

(1) 単一組込みマイコンの動作モデル化
(2)消費電力を利用した異常動作の検知手法の確立
(3)複数の組込みマイコンを用いた異常動作検知の実証





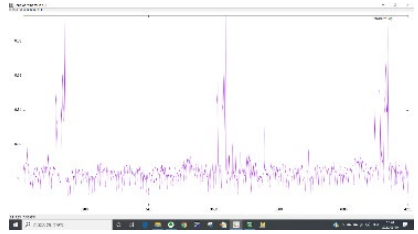
異常動作の検知に成功



動作モデルのもと、組込みマイコンの異常動作検知に成功

課題Ⅱ－イ)AI/機械学習に基づく不正動作検知技術に関する研究開発

(1) 高精度アナログモジュールの実装
(2)次年度に必要となるAIの実現のための事前調査の実施
(3)分野横断的な電子機器の調査と不正プログラムの動向調査の実施



AI実現のための事前調査の実施
AI機能についてニューラルネットワークをFPGAに対して現実的な数となるか検討。事前研究結果からFPGAのLUT数の要求数を検討したところ、15,000個のLUTを用意する事で可能。LUT数を増やしても変わらず、ソフトウェアの高速化の方向としては意義はあると考える

電子機器に利用されるICチップの調査と不正プログラムの動向調査の実施
不正プログラムは複数アーキテクチャにおいて1000個の不正ソフトウエアの収集を行った。電子機器に利用されるICチップの調査にてICチップそのものを不正にコピーして流通させることが行われている事から、不正回路の実在を裏付ける脅威として捉える

3．政策目標の達成状況（経済的・社会的な効果）等 (1/2)

■政策目標（アウトカム目標）の達成状況

政策目標（要約）	現在の進捗状況	達成状況
チップ設計・製造、及びその利用における脆弱性検知手法、並びにサプライチェーン上での運用技術を確立するとともに、当該技術の社会実装を加速する。	• 本プロジェクトで体制と基礎技術を確認。その結果、後続プロジェクトとして、総務省 請負事業（R2～R4年度）を通じて**一連の技術を確立**。さらに、NICT 委託研究（R4～R7年度）を通じて、**確立された技術を実証**。 • 本プロジェクトの成果として得られた知見も活用し、R2年12月に東芝情報システム株式会社が「HTfinder」サービスを開始。**年間数件の検査実績**あり。	○
安全なチップの設計・製造に関する特許取得、業界標準化、国際標準化等を通じて、同分野における我が国の国際競争力強化を図る。	• 標準化活動を継続して実施。R6年、ISO/IEC JTC1/SC27/WG3での活動を通じて、本プロジェクトの成果を含むテクニカルレポートを発行。	○

■新たな市場の形成、売上げの発生、国民生活水準の向上

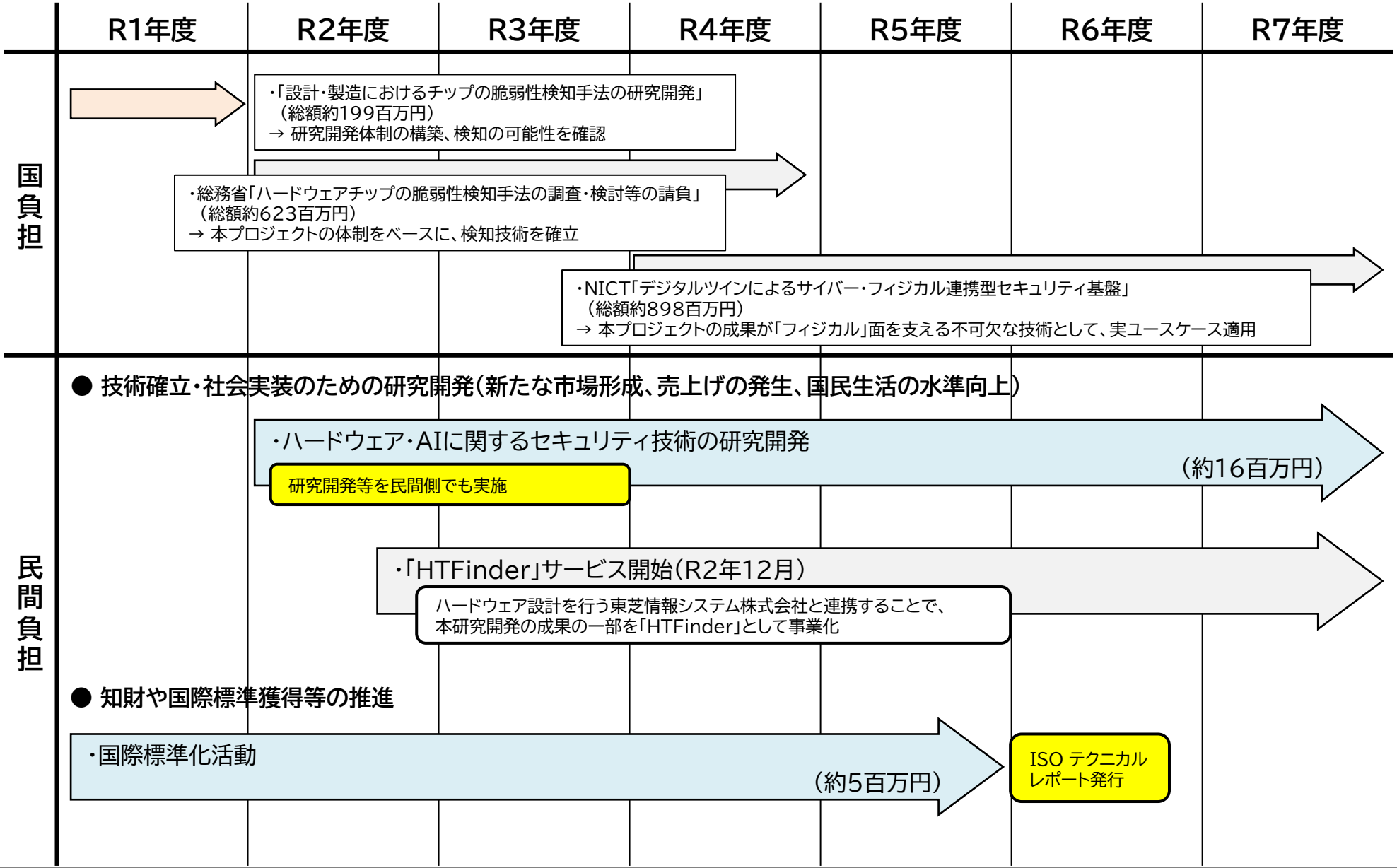
- 本プロジェクトの成果として得られた、チップ設計における脆弱性検知手法に関する知見も活用し、R2年12月に東芝情報システム株式会社が「HTfinder」サービスを事業化。R7年11月末時点もサービスを継続して提供中。
- KDDI総合研究所は民間企業としてハードウェア・AIに関するセキュリティ技術の研究開発に従事。本プロジェクトの成果として得られたコア技術を活用することで、AIに関するセキュリティ（AIセキュリティ）研究に応用している。AIセキュリティ研究に関する成果の一部は、KDDI総合研究所ならびに親会社の事業での活用やサービス化を検討している。

■知財や国際標準獲得等の推進

- 標準化活動を継続して実施して実施した結果、ISO/IEC JTC1/SC27/WG3での活動を通じて、R6年に本プロジェクトの成果を含むテクニカルレポート「Information security, cybersecurity and privacy protection — Hardware monitoring technology for hardware security assessment」を発行した。このテクニカルレポートは、中国の代表が発行を提案し、自らエディタを務め、セキュリティ監視用チップに関する要素技術を体系的に整理したものである。一方、セキュリティ監視用チップ自体が新たなセキュリティリスクの要因となることも懸念される。そこで、KDDI総合研究所の実施者が共同エディタとして参画し、議論を主導することで、当該チップに起因するリスクと本研究開発の成果を踏まえたチップの安全性評価手法をテクニカルレポートに盛り込むことに成功した。

3．政策目標の達成状況（経済的・社会的な効果）等 (2/2)

○ 成果の社会展開に向けた取組状況の線表



4．研究開発成果（アウトプット目標）から生み出された科学的・技術的な効果

■ 研究開発成果から生み出された技術的成果

□ 本プロジェクトにおける技術的成果

・課題I：グラフ学習を適用することにより、ベンチマーク回路に関してTPR89%以上、TNR99%を達成した（当面の目標をクリア）

・課題II：時系列波形データを学習することにより、FPGA・組み込みCPUを対象に、複数のアプリケーションが動作するモデルで異常検知に成功

□ 新たな政府系研究開発プロジェクトへの展開

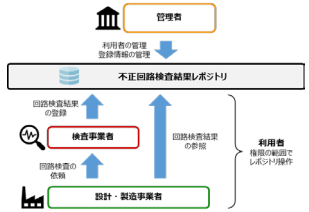
本プロジェクトでは不正回路・不正動作検知に関する研究開発体制を構築し、実際にAIによるハードウェアトロイ検知の可能性を確認した。これをベースに、後続プロジェクトを円滑に実施し、継続的に科学的・技術的成果を生み出した。

● 総務省 請負事業「ハードウェアチップの脆弱性検知手法の調査・検討等の請負」（R2年度～R4年度、KDDI総合研究所（代表）、早稲田大、ラック）

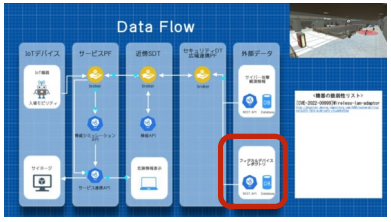
（1）不正回路検知技術の検討及び検証と社会実装に向けた実証、（2）電子機器の外部から観測される情報を用いた不正動作検知技術の検討及び検証と社会実装に向けた実証、（3）認証スキーム等の社会実装の枠組み構築に向けた調査・活動等に取り組んだ。その結果、請負事業の目標を達成し、社会実装に向けた課題を抽出した。

● NICT 委託研究「デジタルツインによるサイバー・フィジカル連携型セキュリティ基盤」（R4年度～R7年度、KDDI総合研究所（代表）、横浜国立大、早稲田大、芝浦工業大）

この委託研究では、サイバーフィジカルシステムにおけるセキュリティ技術の実証を目指すものであり、本プロジェクトの成果が「フィジカル」面を支える不可欠な技術として、実ユースケース適用につなげている。R7年度にモビリティシステム（一人乗り自律走行カート）を対象とした実証を予定している。



総務省 請負事業において、本プロジェクトで開発した技術を用いて得られる不正検知結果を管理するレポジトリを構築



NICT 委託研究において、レポジトリ（図中の赤枠）をデジタルツイン連携基盤で活用する研究開発を実施

5．副次的な波及効果

■ 複数企業の連携

- ハードウェア設計・製造に関するソリューションサービスを提供する東芝情報システム株式会社と連携することで、本プロジェクトの成果の一部を事業化した。**年間数件の検査実績**がある。
  参考URL: https://www.tjsys.co.jp/lsi/htfinder/index_j.htm

■ 博士人材育成

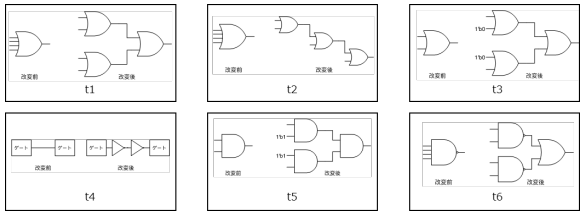
- 博士人材育成に関して、早稲田大学より当該分野ならびに関連分野で継続して博士人材を輩出している。
  実績：R1年度1名、R2年度1名、R3年度2名、R4年度1名、R6年度3名

■ 異分野融合

- 本プロジェクトの成果で得られたコア技術を活用して、AIに関するセキュリティ（AIセキュリティ）研究に応用している。
  - R2-R4年度に受託した総務省 請負事業において、不正回路検知技術に対する敵対的サンプル攻撃を実証した。
  - ここまでに得られたAI技術を活用し、① システムのセキュリティ適合性を自動的に検証する技術や、② システムに対するレッドチーム検証技術を開発した。これら応用研究について、KDDI総合研究所ならびに親会社の株式会社KDDIの協力を得て事業化を検討している。

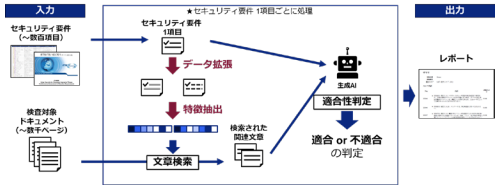
課題I・課題II
AIを活用した
検知技術の開発
（本プロジェクトの成果）

敵対的サンプル攻撃の実証
（本プロジェクトの成果の応用）

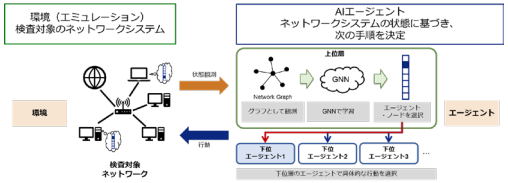


評価に用いた敵対的サンプルの例

システムのセキュリティ適合性検証技術
（波及的に得られた技術①）



AIを活用したレッドチーム検証技術
（波及的に得られた技術②）



6．アウトカム目標の達成に向けた取組計画の達成状況等

■ アウトカム目標に向けた取組計画の達成状況

- R4年度には国内外の半導体関連事業者15社に対してヒアリング調査を実施した。その結果、本プロジェクトの成果に関するニーズと課題を抽出した。これらは、R4年度総務省請負事業において出口戦略として報告書にまとめた。
- 標準化活動や上記ヒアリング調査において、ビジネスプロデューサーより適切なアドバイスを受けた。そのため、ビジネスプロデューサーの設置は有効であった。

■ 周知広報活動の実績

後続プロジェクト等を通じて学会発表等を継続的に行い、R7年9月末までに査読付き論文誌6件、査読付き口頭発表19件、口頭発表・その他37件を発表。加えて、一般書籍を含む以下の外部発表を行い一般にも展開。さらにR4年度の調査の際、国内外の半導体関連事業者15社に対して本プロジェクトの取り組み・成果を紹介した。

後続のプロジェクトを含む外部発表数

	査読付き論文誌	査読付き口頭発表	口頭発表・その他
R2	3	2	4
R3	0	0	5
R4	1	2	8
R5	2	2	8
R6	0	5	6
R7	0	8	5

＊R3は体制変化の影響を受け一時的に減少

左表以外の代表的な実績

- **[Web公開]** 木田 良一, 「産学官連携で実施した、設計・製造におけるチップ脆弱性検知手法の研究開発」, 2021年4月, https://www.lac.co.jp/lacwatch/people/20210428_002599.html
- 長谷川 健人, 「ハードウェアサプライチェーンにおける脅威と対策」, 電子情報通信学会Webinar チュートリアルシリーズ, 2022年8月.
- **[一般雑誌]** 長谷川 健人, 福島 和英, 戸川 望, 「ハードウェア版マルウェア ハードウェア・トロイとFPGA」, FPGAマガジン 特別版No. 1, CQ出版社, 2023年10月.
- **[一般書籍]** 戸川 望, 長谷川 健人, 永田 真一, 「ハードウェアトロイ検知 半導体設計情報に潜むハードウェア版マルウェアの見つけ方」, オーム社, 2024年11月.
- Kento Hasegawa, Nozomu Togawa, “Cybersecurity,” Artificial Intelligence in Surgery, pp. 69-81, 2025年.

■ その他の特記事項に係る履行状況

特記事項（要約）	履行状況	達成状況
① 課題I「回路情報を用いて不正回路を検知する技術」と課題II「電子機器の外部から観測される情報を用いて不正動作を検知する技術」について、受託者間で相互に連携、協力して研究開発を行う。	• R2年度からR4年度にかけて、総務省請負事業「ハードウェアチップの脆弱性検知手法の調査・検討等の請負」を受託し、本プロジェクト終了後も連携、協力して研究開発を行った。	◎
② 社会実装を加速するため研究機関・企業・大学等との連携を促進する体制を構築する。また、コミュニティ形成等を通じて、不正回路・不正動作の継続的なデータ収集、検知技術の改良を行う体制作り等を含む本技術の実用化に向けた取組を実施する。	• 東芝情報システム株式会社と連携し、本プロジェクトの成果の一部を「HTfinder」として実用化。年間数件の検査実績あり。 • 後続のプロジェクトとして総務省請負事業やNICT委託研究を受託することで、継続して検知技術の改良に取り組んだ。	◎

7．政策へのフィードバック (1/2)

■ 国家プロジェクト・プロジェクト設定の妥当性

- 国家プロジェクトとして技術開発を行った成果の一部を「HTfinder」サービスとして**実用化**
- 国内外の半導体サプライチェーン事業者15社にヒアリングした結果、**セキュリティ保証へのニーズを確認**

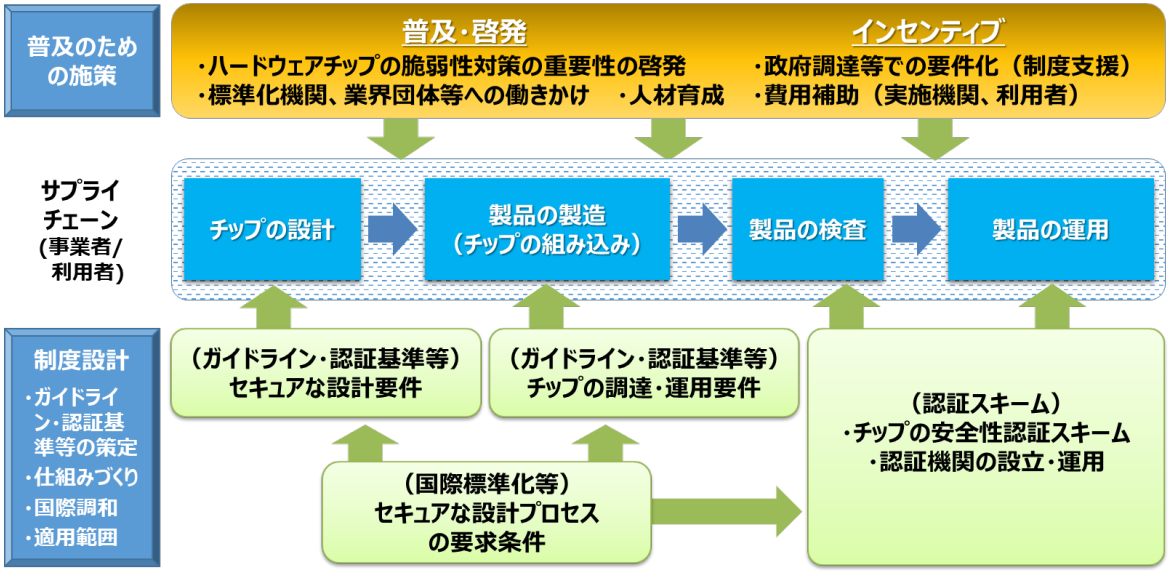
以上のことから、本研究開発で取り組んだ内容は半導体チップの設計・開発において重要であり、国家プロジェクトのテーマ設定としても妥当であった。

■ 政策へのフィードバック

半導体チップの**サプライチェーンセキュリティは国家戦略上きわめて重要**である。しかしながら半導体サプライチェーン事業者へのヒアリング調査によると、チップベンダや設計ベンダにとって、チップ設計の**コストを押し上げるセキュリティ保証の導入に前向きではない**ことが明らかとなった。そのため、チップセキュリティに関する研究開発は、一部のセキュリティに関心の高いベンダを除いて、積極的ではない。セキュリティ保証の導入に前向きでないベンダであっても、政府調達における要件などの規則があれば、それに従うという意見があった。

社会実装にあたっては**コストの問題が大きく、当該分野においては国による積極的な支援が必要**と思われる。

国の半導体に関する施策と相まって、継続的に本事業ならびに発展事業を継続することが重要である。



R4年度に実施した事業者へのヒアリング等を通じてまとめた出口戦略

7．政策へのフィードバック (2/2)

■（参考）ハードウェアセキュリティに関する事例とその傾向

ハードウェアに起因すると思われる事例は、最近のものも含め報道や論文等で報告がある。

- 電気バスが遠隔操作可能になった事例
  https://www.asahi.com/articles/ASTC810C7TC8UHBI00PM.html
- サーバに挿入された不審なチップの事例
  https://www.bloomberg.com/jp/news/articles/2018-10-09/PGCCIQ6S972A01
- センサーモジュールに挿入された不審なチップの事例
  J. Villasenor and M. Tehranipoor, “Chop shop electronics,” in IEEE Spectrum, vol. 50, no. 10, pp. 41-45, October 2013, doi: 10.1109/MSPEC.2013.6607015.
- 監視レーダー装置に挿入された不審な機能の事例
  S. Adee, “The Hunt For The Kill Switch,” in IEEE Spectrum, vol. 45, no. 5, pp. 34-39, May 2008, doi: 10.1109/MSPEC.2008.4505310.

さらに、その他の事例も報告されている。

- ✓ オーストラリアの下水処理会社で勤務する従業員が、システムを不正に遠隔操作し、80万リットルの汚水を地元の公園に流出
- ✓ イギリスで軍事衛星システムが乗っ取られ、軍事通信用の衛星回線情報を改竄
- ✓ ポーランドで14歳の少年がテレビのリモコンを改造して路面電車システムに侵入し、4車両が脱線
- ✓ イランのウラン濃縮器がマルウェアを使ったサイバー攻撃によって物理的に破壊され、核開発を妨害
- ✓ フィンランドのビルで、DDoS攻撃により暖房が停止
- ✓ 米国の収容所で、収容房のドアがリモートで解除され、対立するギャングの抗争が勃発
- ✓ GPSスプーフィングによる船舶航行の妨害
- ✓ インターネットに接続された水槽を介し、カジノのデータベースへの不正アクセスが発生
- ✓ ランサムウェア攻撃より、天然ガスパイプラインのダウン、物流会社の配送の遅延、鉄鋼生産の中断、ホテルの客室ドアの施錠・開錠の妨害等が発生

上記の事例では大きく分けて、遠隔操作などインターネットに接続された電子機器への攻撃と、国防に関する制御機器への攻撃が報告されている。そのため、**ネットワーク機器やサーバ、また国防に関するハードウェアセキュリティが特に重要**と言える。

半導体は国の重要戦略であると同時に、経済安全保障の観点から安全なサプライチェーン構築は不可欠である。このような観点から、継続してハードウェアセキュリティ技術の研究開発が必要と言える。