令和元年度新規研究開発課題に係る基本計画書概要　【サイバーセキュリティ統括官室】

別紙1参考

設計・製造におけるチップの脆弱性検知手法の研究開発

研究開発の背景・目標

背景

ハードウェアチップに故意に組み込まれた脆弱性は、サプライチェーン上の大きな脅威であり、製品に実装された不正回路は後から対処するのが困難であることから、設計・製造におけるチップの脆弱性検知手法の確立は急務となっている。

政策目標（アウトカム目標）

産学官連携により、ハードウェアチップの設計・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。

また、安全なハードウェアチップの設計・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。

研究開発目標（アウトプット目標）

回路情報の中に不正に改変された回路が含まれるか、機械学習等のAIを活用して検知する技術 及び 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を確立する。

技術課題

○課題Ⅰ　回路情報を用いて不正回路を検知する技術

ア）不正回路を識別するための特徴量抽出技術

回路情報より、不正回路と不正でない回路を識別するために有意となる特徴量を抽出する技術

イ）AI/機械学習に基づく不正回路検知技術

AIを活用し回路の特徴量を学習することにより、不正回路の有無及び不正回路の存在する位置を検知する技術

○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

ア）外部情報を取得する電子機器の動作のモデル化技術

電子機器の動作をモデル化し、当該モデルに基づいた電子機器の外部から観測される情報より、不正動作と正常動作を識別するために有意となる特徴量を抽出する技術

イ）AI/機械学習に基づく不正動作検知技術

AIを活用し電子機器の動作の特徴量を学習することにより、電子機器の外部から観測される情報の中から不正動作の位置を検知する技術

到達目標

○課題Ⅰ　回路情報を用いて不正回路を検知する技術

実設計回路を用いて、不正でない回路を不正と判定する誤検知率が5%以下という条件のもと、不正回路を見逃す見逃し確率10%以下を実現する特徴量抽出技術及び不正回路検知技術を確立する。さらに、敵対的サンプル攻撃を想定し、上記の誤検知率と見逃し確率を悪化させないよう、技術を高度化する。

加えて、不正回路検知技術の実証を行い、実用化に向けた運用技術を確立する。

○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

市販されている電子機器を含めて、正常動作を不正動作と判定する誤検知率が5%以下という条件のもと、不正動作を見逃す見逃し確率10%以下を実現する、電子機器の外部から観測される情報の特徴量抽出技術及び不正動作検知技術を確立する。

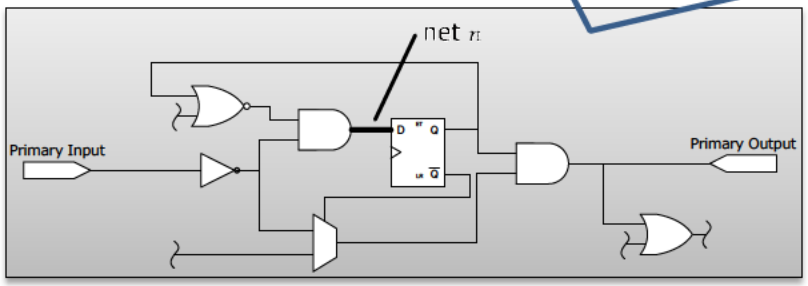
加えて、広範囲に適用できる汎用的なモデル化手法を確立する。

（参考）設計・製造におけるチップの脆弱性検知手法の研究開発（イメージ図）

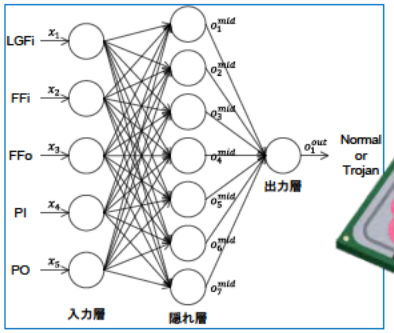
電子機器のハードウェア上に組み込まれた不正なチップは、製品出荷後に交換・修正することが難しく、その影響は極めて深刻になる可能性があることから、サプライチェーン上の脅威となっている。本研究開発ではハードウェアチップの設計・製造における脆弱性検知手法を確立するとともに、当該技術の社会実装を加速し、サプライチェーン全体のセキュリティ確保に資する。

課題Ⅰ　回路情報を用いて不正回路を検知する技術

Ⅰ－ア） 不正回路について、その種類及び機能を明確化した上で、不正回路と不正でない回路とを識別するための特徴量を抽出する。

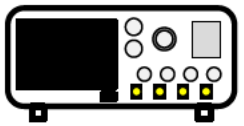


不正回路を見逃す見逃し確率を最小化する。

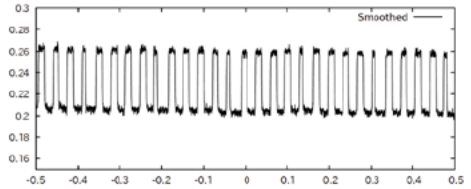


Ⅰ－イ） AIを活用し不正回路の特徴量と不正でない回路の特徴量を学習することにより、不正回路の有無及び不正回路の存在する位置を検知する。

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

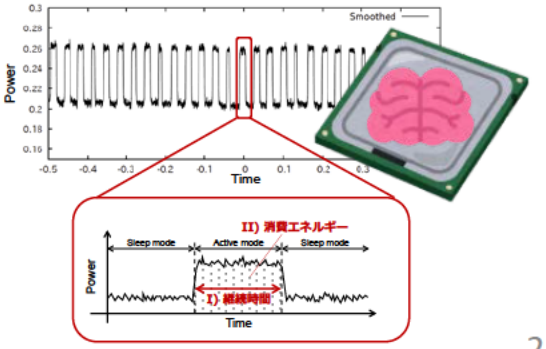


Ⅱ－ア） 組込みマイコンやFPGA等のチップに不正回路が含まれていることを想定し、その動作をモデル化する。当該モデルに基づき、電子機器の外部から観測される情報より、不正動作と正常動作を識別するために有意となる特徴量を抽出する。



不正動作を見逃す見逃し確率を最小化する。

Ⅱ－イ） AIを活用し不正動作の特徴量と正常動作の特徴量を学習することにより、電子機器の外部から観測される情報の中から不正動作の位置を検知する。



<u>所要経費</u>　2.0億円（令和元年度）

<u>研究開発期間</u>　令和元年度～令和4年度

アウトカム目標の達成に向けた総務省の取組について

政策目標の達成に向けた取組方針

○研究開発期間中

- 受託者が設置する研究開発運営委員会において、学識経験者、研究開発成果の利用者等の参加を得て、これら参加者の助言や政策方針等を踏まえながら、研究開発を推進する。
- 官民研究開発投資拡大プログラム（PRISM）の趣旨を踏まえ、研究機関・企業・大学等との連携を促進するための体制構築を支援し、社会実装を加速する。
- 戦略的イノベーション創造プログラム（SIP）のプログラムディレクターと定期的な意見交換等を実施することにより、SIPと相乗的に研究開発を推進する。

○研究開発期間終了後

- 研究開発終了年度の翌年度に、今後の研究開発・社会展開の計画等について外部有識者等による助言を得るための終了評価を実施する。
- 追跡調査・評価において、受託者に製品化等の成果展開状況を確認するとともに、学識経験者や有識者の助言を得ながら、社会実装の取組を推進する。
- 研究開発成果展開の機会を増やすために、ニーズとシーズのマッチングを推進する。具体的には、受託者に対して、関連業界団体等が開催する国内外会議、展示会への発表や出展、関連事業者への研究開発成果のプレゼンテーション実施等を促す。