別紙１

設計・製造におけるチップの脆弱性検知手法の研究開発
基本計画書

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）において、サプライチェーン（バリュークリエーションプロセス）全体でのセキュリティ対策の強化のため、個別の機器・サービス等がセキュリティ要件を満たしていることを確認することで信頼を創出する仕組み、信頼が証明された機器・サービス等のリストの作成、トレーサビリティの確保について、所要の研究開発を進めることとされている。

「サイバーセキュリティ戦略」（平成 30 年７月 27 日　閣議決定）において、サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発を進めるほか、機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発を行うこととされている。

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、

「ハードウェアの動作特性把握による不正機能検出等」が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。

なお「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、PRISM 運営委員会等の議論を経て、「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．目　標

（１）政策目標（アウトカム目標）

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。本研究開発では産学官連携により、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。

（２）研究開発目標（アウトプット目標）

本研究開発では、以下の技術を確立する。

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

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

４．研究開発内容

電子機器を構成するチップの回路情報は、論理ゲートやフリップフロップ、入出力端子等の接続情報によって与えられる。もし回路情報が不正に改変されると、回路内部の情報を外部に漏洩したり、あるいは出力を強制的にゼロにしたりする等の利用者

の意図しない不正動作が引き起こされる。このように不正に改変された回路を検出するためには、一般に検査対象の回路情報を既知の不正回路情報と比較し、不正の有無を判定する手法が用いられる。しかしこの方法では新しく見つかった不正回路の情報を都度入手し、検査用データとして登録しておく必要があり、現実的な運用が難しい。また、従来から知られている故障診断技術を用いる手法では、不正を検知するための計算量が膨大となってしまうため、近似を用いる必要があり、必ずしも不正回路を検知できるとは限らない等の課題がある。

そこで本研究開発では、不正回路を含む回路情報の特徴量を抽出し、AI による学習を繰り返すことで不正回路を検知する技術の研究開発を実施する（課題Ⅰ）。また、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の外部情報を用いて特徴量を抽出し、AI による学習を繰り返すことで不正動作を検知する技術の研究開発を実施する（課題Ⅱ）。

AI 技術を用いることで、人手では見い出すことが不可能であるような不正回路及び不正動作の識別技術を研究開発することが期待される。

Ⅰ.　回路情報を用いて不正回路を検知する技術

①　概要

グローバル化が進むハードウェアチップの設計・製造分野では、動作が完全に保証された内製の設計ツールや内製の設計部品だけでなく、外部設計ツールや外部設計部品を利用することが一般的になっている。本研究課題では、外部設計ツールや外部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、回路情報の中に不正回路が含まれるかを AI を用いて検知する技術を研究開発する。検知対象の不正回路については、不正の種類及びその機能を具体的に明示して提案する。また、学習に用いる回路情報データについては、その妥当性について客観的に評価可能なデータを用いる必要があるため、どのような回路情報データをどの程度の規模で用いるかを具体的に提案する。

②　技術課題

ア）不正回路を識別するための特徴量抽出技術

利用者の意図しない不正動作を引き起こす不正回路について、どのような不正を行うか、その種類及び機能を明確化した上で、多数の不正回路の情報及び不正が組み込まれていない回路の情報より、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（論理ゲートの入出力数等）を抽出する技術を研究開発する。その際には、下記イ）の結果も反映し、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を最小化する。さらに敵対的サンプル攻撃を想定し、こうした攻撃があったとしても上記の誤検知率と見逃し確率を悪化させない特徴量の抽出技術を確立する。

イ）AI/機械学習に基づく不正回路検知技術

回路情報が与えられたとき、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技術を研究開発する。さらに、検知技術を実装するにあたり、実行時間・メモリ使用量等を最適化する。その際には、上記ア）の結果も反映し、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を最小化する。さらに敵対的サンプル攻撃を想定し、こうした攻撃があったとしても上記の誤検知率と見逃し確率を悪化させない検知技術を確立する。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。

③　到達目標

下記の到達目標における誤検知率及び見逃し確率については、用いる回路情報データにより変動するため、その妥当性について客観的に評価可能なデータを用い、どのような回路情報データをどの程度の規模で用いるかを具体的に提案する。

ア）不正回路を識別するための特徴量抽出技術

（１年目）回路設計に標準的なベンチマーク回路等を用いて、不正回路の種類及びその機能を明確化し、不正回路と不正でない回路を識別するための特徴量を抽出する技術を開発する。

（２年目）ベンチマーク回路等から対象を拡大し、実設計回路を含む回路情報を用いて、より多くの不正回路の種類及びその機能を明確化する。また、ベンチマーク回路等を用いて、不正回路と不正でない回路を識別するための特徴量を抽出する技術を開発し、１年目より見逃し確率の小さい特徴量を見い出す。

（３年目）ベンチマーク回路等から対象を拡大し、実設計回路を含む回路情報を用いて、不正回路と不正でない回路を識別するための特徴量を抽出する技術を開発する。さらに、敵対的サンプル攻撃を想定し、本技術を高度化する。

（４年目）３年目までに開発した技術を更に高度化し、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を確立する。

イ）AI/機械学習に基づく不正回路検知技術

（１年目）ベンチマーク回路等を用いて、AI により回路情報から不正回路を検知する技術を開発する。

（２年目）ベンチマーク回路等を用いて、AI により回路情報から不正回路を検知する技術を開発し、１年目より見逃し確率の小さい検知技術を開発する。

（３年目）ベンチマーク回路等から対象を拡大し、実設計回路を含む回路情報を用いて、AI により回路情報から不正回路を検知する技術を開発する。さらに、敵対的サンプル攻撃を想定し、本技術を高度化する。加えて、不正回路検知技術の実証に向けて、基礎検討を行う。

（４年目）３年目までに開発した技術を更に高度化し、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%以下を実現する検知技術を確立する。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。

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

①　概要

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の外部情報を用いて、AI 技術により不正動作を検知する技術を研究開発する。また、具体的に入出力としてどのような外部情報が有効かを調査し（一例として、電力波形の特定部分の電力量や継続時間が考えられるが、それ以外の有効な外部情報を提案しても良い。）、不正動作の特定方法を含めて提案する。

②　技術課題

ア）外部情報を取得する電子機器の動作のモデル化技術

組込みマイコンやFPGA（Field-Programmable Gate Array）等のチップに不正回路が含まれていることを想定し、これらを用いて電子機器を構成した上で、その動作をモデル化する。このような動作モデルは、組込みマイコンやFPGA 上で動作するアプリケーションプログラムの種類や不正回路の種類によって多数想定されるところ、例えば、特定のチップの内部状態の遷移等をとらえ、正常とは異なる動作（不正動作）をモデル化する。またモデル化にあたっては、特定のチップに限定せず、広範囲に適用できる汎用的なモデル化手法を確立する。

当該モデルに基づいた電子機器の外部情報より、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を研究開発する。その際には、下記イ）の結果も反映し、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を最小化する。

イ）AI/機械学習に基づく不正動作検知技術

電子機器の外部情報が与えられたとき、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、外部情報の中から不正動作の位置を検知する技術を研究開発する。さらに、検知技術を実装するにあたり、実行時間・メモリ使用量等を最適化する。その際には、上記ア）の結果も反映し、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を最小化する。

③　到達目標

下記の到達目標における誤検知率及び見逃し確率については、用いる外部情報データにより変動するため、その妥当性について客観的に評価可能なデータを用い、どのような外部情報データをどの程度の規模で用いるかを具体的に提案する。

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年目）単独の組込みマイコン等、比較的簡易な電子機器の動作のもと、見逃し確率を最小化するような電子機器の外部情報の特徴量を抽出する技術を開発する。

（２年目）種類の異なる組込みマイコンやFPGA チップ等、複数の種類の電子機器の動作のもと、見逃し確率を最小化するような電子機器の外部情報の特徴量を抽出する技術を開発する。

（３年目）組込みマイコンやFPGA チップ等の複数のチップが搭載された電子機器の動作のもと、見逃し確率を最小化するような電子機器の外部情報の特徴量を抽出し、２年目より見逃し確率の小さい特徴量を見い出す。加えて、広範囲に適用できる汎用的なモデル化手法の確立に向けて、基礎検討を行う。

（４年目）３年目までに設計された電子機器に加えて、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情報の特徴量抽出技術を確立する。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。

イ） AI/機械学習に基づく不正動作検知技術

（１年目）単独の組込みマイコン等、比較的簡易な電子機器の動作のもと、見逃し確率を最小化するように、AI により外部情報から不正動作を検知する技術の基本検討を行う。

（２年目）単独の組込みマイコン等、比較的簡易な電子機器の動作のもと、見逃し確率を最小化するように、AI により外部情報から不正動作を検知する技術を実装する。

（３年目）種類の異なる組込みマイコンやFPGA チップ等、複数の種類の電子機器の動作、及び複数のチップが搭載された電子機器の動作のもと、２年目より見逃し確率が小さくなるよう、AI により外部情報から不正動作を検知する技術を改良する。

（４年目）３年目までに設計された電子機器から対象を拡大し、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、不正動作を検知する技術を確立する。

５．研究開発期間

令和元年度から令和４年度までの４年間

６．その他　特記事項

（１）特記事項

① 提案者は、下記課題Ⅰ-ア） Ⅰ-イ）、Ⅱ-ア）、Ⅱ-イ）のいずれか又は複数の課題に提案することができる。なお、いずれの研究開発の受託者も相互に連携、協力して研究開発を行う。また、課題Ⅰ-ア）の受託者は、本研究開発課題全体の取りまとめを行うものとする。

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

イ）AI/機械学習に基づく不正回路検知技術

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

イ）AI/機械学習に基づく不正動作検知技術

② 研究開発の実施に当たっては、PRISMの趣旨を踏まえ、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ための体制を構築すること。また、関係する研究開発分野との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こと。なお、本件について不明点がある場合は、本研究開発の担当課室まで問い合わせること。

（２）提案及び研究開発に当たっての留意点

① 提案に当たっては、基本計画書に記されているアウトプット目標に対する達成度を評価することが可能な具体的な評価項目を設定し、各評価項目に対して可能な限り数値目標を定めるとともに、目標を達成するための研究方法、実用的な成果を導出するための共同研究体制又は研究協力体制及び達成度を客観的に評価するための実験方法について、具体的に提案書に記載すること。

② アウトカム目標の達成に向けた適切な研究成果の取扱方策（研究開発課題の分野の特性をふまえたオープン･クローズ戦略を含む）について提案書に記載すること。また、本研究開発成果を確実に展開し、アウトカム目標を達成するため、事業化目標年度、事業化に至るまでの実効的な取組計画（体制、資金等）についても具体的に提案書に記載すること。その際、関連技術に関する技術開発動向や市場動向を踏まえ、また、本研究開発成果を活用した製品やサービスの国際的な普及展開、国際的な標準化活動のための活動に当たっては、学識経験者、有識者等の意見を踏まえ、有効性のある具体的な取組計画を作成すること。

③ 複数機関による共同研究を提案する際には、研究開発全体を整合的かつ一体的に行えるよう参加機関の役割分担を明確にし、研究開発期間を通じて継続的に連携するための方法について具体的に提案書に記載すること。

④ 本研究開発は総務省施策の一環として取り組むものであることから、総務省が受託者に対して指示する、研究開発に関する情報及び研究開発成果の開示、関係研究

開発プロジェクトとのミーティングへの出席、シンポジウム等での研究発表、共同実証実験への参加等に可能な限り応じること。

⑤　研究開発の実施に当たっては、関連する要素技術間の調整、成果の取りまとめ方等研究開発全体の方針・進め方について幅広い観点から助言を頂くとともに、研究開発成果の利用・普及に向けた意見や要望等を頂くため、学識経験者、研究開発成果の利用者等の参加を得て研究開発運営委員会等を開催すること。

（３）人材の確保・育成への配慮

①　研究開発によって十分な成果が創出されるためには、優れた人材の確保が必要である。このため、本研究開発の実施に際し、人事、施設、予算等のあらゆる面で、優れた人材が確保される環境整備に関して具体的に提案書に記載すること。特に、世界的に人材不足とされているAI 分野の研究員の確保の方策について､提案すること。

②　若手の人材育成の観点から行う部外研究員受け入れや招へい制度、インターンシップ制度等による人員の活用を推奨する。また、可能な限り本研究開発の概要を学会誌の解説論文で公表するなどの将来の人材育成に向けた啓発活動についても十分に配慮すること。これらの取組予定の有無や計画について提案書において提案すること。

（４）研究開発成果の情報発信

①　本研究開発で確立した技術の普及啓発活動を実施するとともに、実用化に向けて必要と思われる研究開発課題への取組も実施し、その活動計画・方策については具体的に提案書に記載すること。

②　研究開発成果については、原則として、総務省としてインターネット等により発信を行うとともに、マスコミを通じた研究開発成果の発表、講演会での発表等により、広く一般国民へ研究開発成果を分かりやすく伝える予定であることから、当該提案書には、研究成果に関する分かりやすい説明資料や図表等の素材、英訳文書等を作成し、研究成果報告書の一部として報告する旨の活動が含まれていること。さらに、総務省が別途指定する成果発表会等の場において研究開発の進捗状況や成果について説明等を行う旨を提案書に記載すること。

③　本研究開発終了後に成果を論文発表、プレス発表、製品化、Web サイト掲載等を行う際には「本技術は、総務省の「設計・製造におけるチップの脆弱性検知手法の研究開発」による委託を受けて実施した研究開発による成果です。」という内容の注記を発表資料等に都度付すこととする旨を提案書に明記すること。