早稲田大学 Press RELEASE　ご取材案内

配布先：文部科学記者会、科学記者会、
報道各社：科学部・社会部　ご担当者　各位

2019 年 10 月 25 日
学校法人早稲田大学
株式会社 KDDI 総合研究所
株式会社ラック

ハードウェアチップの脆弱性検知手法の研究開発に採択

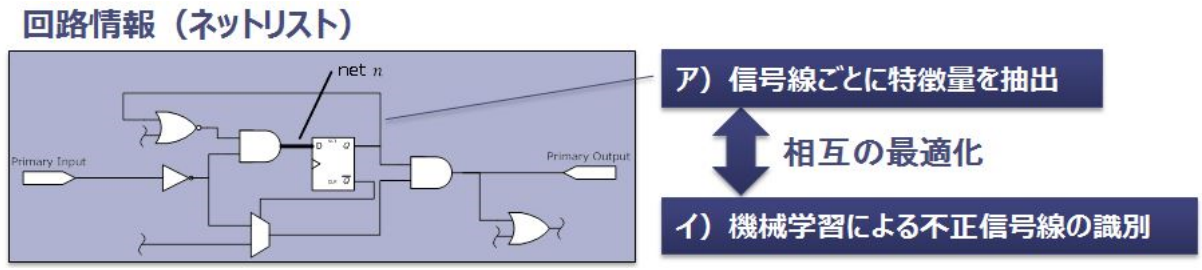
手法の確立と社会実装を加速しサプライチェーン全体のサイバーセキュリティ確保を目指す

発表のポイント

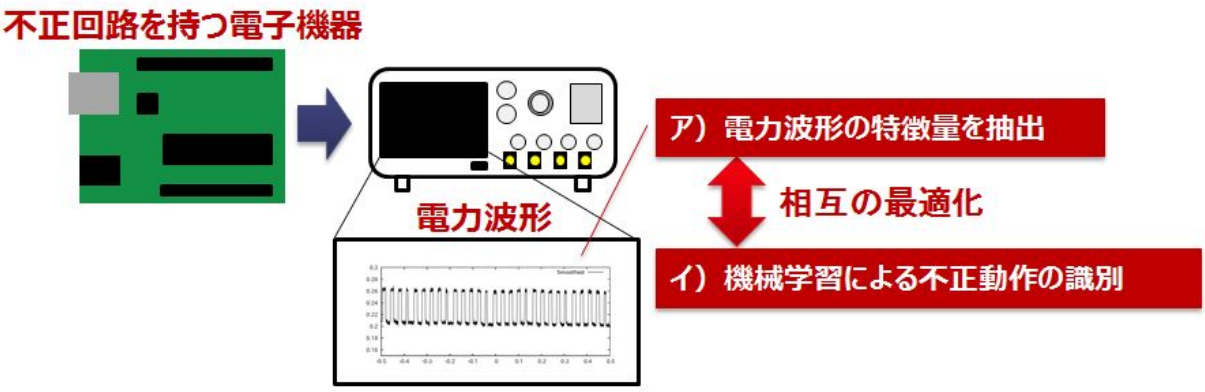
- ハードウェアチップに組み込まれた不正回路がサプライチェーン上での脅威になっている
- 産学官連携でハードウェアチップの設計・製造の脆弱性検知手法確立に取り組む
- 当該技術の社会実装を加速しサプライチェーン全体のサイバーセキュリティ確保に資する

2019 年 9 月 18 日、学校法人早稲田大学を代表研究機関（研究責任者：理工学術院　戸川望教授、以下、早稲田大学）とし、株式会社 KDDI 総合研究所（以下、KDDI 総合研究所）および株式会社ラック（以下、ラック）は、総務省が 2019 年度に実施する内閣府事業 PRISM（官民研究開発投資拡大プログラム）の対象研究開発課題「設計・製造におけるチップの脆弱性検知手法の研究開発」の委託先として選定されました。
http://www.soumu.go.jp/menu_news/s-news/01tsushin03_02000286.html

【課題Ⅰ　回路情報を用いて不正回路を検知する技術】



【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】



（１）社会的背景、これまでの経緯

- 全世界の電子機器の個数は 2020 年には 400 億個を超えると予測され、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確保が重要な課題となっています。特に、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、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されています。

（２）今回の研究で新たに実現しようとすること

- 回路情報のなか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の確立を目指します。
  - **課題Ⅰ　回路情報を用いて不正回路を検知する技術**

    (ア) 不正回路について、その種類及び機能を明確化したうえで、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技術の研究開発。

    (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技術の研究開発。

- 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の確立を目指します。
  - **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) 組み込みマイコンや FPGA 等のチップに不正回路が含まれることを想定し、その動作をモデル化。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技術の研究開発。

    (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技術の研究開発。

（３）この研究により期待されること

- サプライチェーン運用技術の確立
  - 産学官連携により、ハードウェアチップの設計・製造、およびその利用における脆弱性検知手法、なら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。
- 国際競争力強化
  - 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、情報発信等を通じて、同分野における「国際的ハブ」の構築を図り、これを活用し国内外の半導体設計メーカーが参画する仕組みを構築。これによって我が国の国際競争力強化に寄与する。

（４）各機関の役割

- 早稲田大学
  - 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
  - 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
- KDDI 総合研究所
  - 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
  - 課題Ⅰ－イ　：AI／機械学習に基づく不正回路検知技術に関する研究開発
- ラック
  - 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

（５）用語解説

内閣府事業 PRISM（官民研究開発投資拡大プログラム）

- 平成 28 年 12 月に総合科学技術･イノベーション会議と経済財政諮問会議が合同でとりまとめた「科学技術イノベーション官民投資拡大イニシアティブ」に基づき、600 兆円経済の実現に向けた科学技術イノベーションの創出に向け、官民の研究開発投資と拡大などを目指して平成 30 年度に創設された制度です。https://www8.cao.go.jp/cstp/prism/index.html

ハードウェアトロイ

- IoT の普及に伴って、ハードウェアの設計・製造の外注化が進んでいます。その結果、悪意ある第三者によってハードウェアトロイが挿入される危険性が指摘されています。ハードウェアトロイとはハードウェアに組み込まれた悪意のある機能のことで、IC チップの動作改変や IC チップの故障、機密情報の流出を引き起こすなど多方面へリスクが広がる可能性があります。

（６）共同研究機関

- 早稲田大学（本部：東京都新宿区、総長：田中愛治）
- KDDI 総合研究所（本社：埼玉県ふじみ野市、代表取締役所長：中島康之）
- ラック（本社：東京都千代田区、代表取締役社長：西本逸郎）

【内容に関するお問い合わせ先・発信元】

- 早稲田大学 広報室広報課　E-mail：koho@list.waseda.jp
- KDDI 総合研究所　営業・広報部　E-mail：inquiry@kddi-research.jp
- ラック　コーポレート・コミュニケーション室 E-mail：pr@lac.co.jp