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 7 月 29 日
早稲田大学
東芝情報システム株式会社

早大と東芝情報システム、ハードウェアトロイ検知技術で連携 実回路での効果を確認

～ 早大オープンイノベーション機構と東芝情報システムによる産学連携成果 ～

発表のポイント

- 早大の「ハードウェアトロイ検出手法」を適用した検証ツールを東芝情報システムが開発
- ハードウェアトロイ検出の効果を確認
- 同検出手法としては、初の社会実装事例
- 今後、より安全な LSI 回路設計及び、他社製 IP の安全性確認に効果が期待される

早稲田大学（以下、早大）の戸川望（とがわのぞむ）理工学術院教授と東芝情報システム株式会社（本社：川崎市川崎区、取締役社長：渡邉 一正　以下、東芝情報システム）は、早大が開発した「ハードウェアトロイ検出手法」の設計に基づき検証ツールを共同で開発しました。また本検証ツールを用いて既知のハードウェアトロイが正しく検知できること、さらに同社設計の実製品に適用して誤検知が無いことも確認いたしました。同検出手法の社会実装としては初の事例となります。

本研究成果は、2019 年 9 月 10～13 日開催の電子情報通信学会ソサイエティ大会（大阪大学）にて発表および展示を行う予定です。

（１）社会的背景、これまでの経緯

総務省の予測では 2020 年に全世界で 400 億個を超える IoT デバイスが稼働するとされています。IoT デバイスの利用は今後も多様化が見込まれているため、ハードウェアに対するセキュリティ対策が求められています。

そうした社会背景のなかで、早大の戸川教授は LSI のハードウェアセキュリティに関する研究に長年取り組んでいます。戸川教授の研究成果のひとつに、総務省戦略的情報通信研究開発推進事業（SCOPE）のもとに「パタンマッチング」による「ハードウェアトロイ検出手法」の開発があります（平成２８年度完了）。この開発にあたっては、すでに後述の論文①および論文②として発表しており、さらに特許（５、後述）を取得しています。

一方、東芝情報システムは LSI 分野、組込みシステム分野、システムインテグレーション分野において、各種ソリューションを提供しており、本産学連携を行う LSI ソリューション事業部は、半導体集積回路の受託設計やオリジナル LSI 製品の販売を行っています。

両者は日本学術振興機構による「2018 早稲田大学 - 新技術説明会」（2018 年 6 月 21 日開催、JST 東京本部別館１F ホール）にて、戸川教授により上記の研究開発内容の発表（※）がされたことを契機として、「ハードウェアトロイ検出手法」の社会実装に向けて連携協議を開始しました。2019 年 1 月からは、早大オープンイノベーション戦略研究機構を窓口として、東芝情報システムと早大間で受託研究（2018 年度中）、ならびに共同研究（2019 年度より）を進めています。

※参照　https://shingi.jst.go.jp/kobetsu/waseda/2018_waseda.html

（２）今回の研究で新たに実現しようとしたこと、明らかになったこと

このたび、東芝情報システムは早大が開発した「ハードウェアトロイ検出手法」の設計に基づき、検証ツールの開発を行い、ハードウェアトロイ回路例を公開している Trust-Hub 掲載の既知ハードウェアトロイを正しく検知できること、さらに同社設計の実製品に適用して誤検知の無いことを確認しました。「ハードウェアトロイ検出手法」の社会実装としては初の事例となります。

従来 LSI 回路設計の現場では、外部に設計を委託した回路や他社製の IP に「悪意を持つ回路」が組み込まれていた場合、これを阻止する手段がありませんでした。今回開発したハードウェアトロイの検証ツールは、このセキュリティリスクを効率的に排除するもので、より安全な LSI 回路設計を可能とするものと期待されます。

早大と東芝情報システムは今回、研究成果の社会実装が一歩前進したことを受けて、今後「ハードウェアトロイ検出手法」の更なる高度化に取り組む予定です。東芝情報システムは本検証ツールの商用展開に向けて準備を進めて行きます。

（３）用語解説

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危険性があります。

パタンマッチング

- ゲートネットから回路構造を解析し、ハードウェアトロイの特徴的な構造と一致させて検出する手法です。

Trust-Hub

- アメリカ国立科学財団（National Science Foundation）が運営するサイトのハードウェアセキュリティ領域と信頼性領域で、技術開発をしている有志フォーラムです。

早稲田大学オープンイノベーション戦略研究機構

- 早大が 2018 年に設置。同機構は、産学連携活動により早大研究成果の社会実装を実現するイノベーションを推進し、現代社会における課題解決の加速と価値創造の拡大を目指しています。https://www.waseda.jp/inst/oi/about

（４）論文情報

【論文①】

雑誌名：IEICE Transactions on Fundamentals、vol. 99-A、no. 12、pp. 2335-2347、2016

論文名：Hardware-Trojans Rank: Quantitative Evaluation of Security Threats at Gate-Level Netlists by Pattern Matching

執筆者：Masaru Oya、 Noritaka Yamashita、 Toshihiko Okamura、 Yukiyasu Tsunoo、 Masao Yanagisawa、 and Nozomu Togawa、

ＤＯＩ：10.1587/transfun.E99.A.2335

【論文②】

雑誌名：Proceedings of the IEEE/ACM 2015 Design、 Automation & Test in Europe Conference & Exhibition (DATE 2015)、 pp. 465-470、 2015

論文名：A Score-Based Classification Method for Identifying Hardware-Trojans at Gate-Level Netlists

執筆者：Masaru Oya、 Youhua Shi、 Masao Yanagisawa、 and Nozomu Togawa、

ＤＯＩ：10.7873/DATE.2015.0352

（５）特許情報
特願 2014-233953、 "ハードウェアトロイの検出方法、ハードウェアトロイ の検出プログラム、およびハードウェアトロイの検出装置、" 2014.11.18 出願.
https://jstore.jst.go.jp/nationalPatentDetail.html?pat_id=36205&_ssn=UC211P21S010_2

（６）研究助成
研究費名：総務省・戦略的情報通信研究開発推進事業(SCOPE)
研究課題名： 設計工程に侵入したハードウェアトロイの検出と耐ハードウェアトロイ設計技術の研究開発(H26 年度～H28 年度)
研究代表者名（所属機関名）：戸川望（早稲田大学）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/scope/subject/s_h26.html

【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
Tel：03-3202-5454　E-mail：koho@list.waseda.jp

東芝情報システム株式会社　LSI ソリューション事業部　商品企画部
Tel：044-200-5433　E-mail：TJ-lsiproductplan@tjsys.co.jp