Copyright ©2022 The Institute of Electronics,
Information and Communication Engineers

SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

実環境を想定したトロイ回路を対象とした機械学習によるハードウェアトロイ識別

栗原 樹 * 長谷川 健人 † 福島 和英 † 清本 晋作 † 戸川 望 *

キーワード ハードウェアトロイ，ゲートレベルネットリスト，機械学習，ランダムフォレスト，ニューラルネットワーク

あらまし

近年，IoT デバイスの普及に伴い，日常の様々なものに組み込みハードウェアが利用されている．組込み機器の需要増加により設計や製造の一部を第三者に外部委託するようになっている．これにより悪意ある第三者により回路中に悪意ある機能をもつ回路，すなわちハードウェアトロイが挿入される危険性が増大している．本稿では，ゲートレベルネットリストにおけるハードウェアトロイが持つ特徴を機械学習で学習し，ハードウェアトロイが挿入された回路のゲートレベルネットリストをトロイネット (ハードウェアトロイを構成するネット) とノーマルネット (正常な回路を構成するネット) に分類する．Trust-HUB ベンチマーク回路に加え，実環境を想定したハードウェアトロイ回路から抽出した特徴量に対し，オーバーサンプリングを適用した上でランダムフォレストおよびニューラルネットワークで学習した．計算機実験による識別評価の結果を示す．

* 早稲田大学大学院 基幹理工学研究科 情報理工・情報通信専攻，〒 169–8555 東京都新宿区大久保 3–4–1.
† 株式会社 KDDI 総合研究所，〒 356–8502 埼玉県ふじみ野市大原 2–1–15.