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

# 勾配ブースティング決定木と識別結果伝搬法によるハードウェアトロイ識別

根岸 良太郎 * 栗原 樹 * 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，勾配ブースティング決定木，XGBoost，LightGBM，CatBoost

## あらまし

テクノロジー機器は人々の生活に深く浸透しており需要は年々拡大している．テクノロジー機器に欠かせないIC 製造の外部委託によりハードウェアトロイの組み込みを招く危険性が指摘されている．本稿ではゲートレベルネットリストの特徴を利用した機械学習によるハードウェアトロイ識別手法における最適な特徴量セットを提案する．機械学習手法として勾配ブースティング決定木であるXGBoost，LightGBM，CatBoost を利用する．さらに，機械学習により得られた結果を元に，ネットリストのグラフ情報を利用しハードウェアトロイの識別精度を向上させる．Trust-HUB で公開されているネットリストを対象とした評価実験を行い，平均 F-measure 0.861 を示した．

* 早稲田大学, 東京都新宿区大久保 3-4-1