2024 年度年次報告書
社会変革に向けた ICT 基盤強化
2023 年度採択研究代表者

矢内 直人

パナソニックホールディングス（株） 技術部門テクノロジー本部
主幹技師

スマートコントラクトを用いた攻撃とその対策の検討

研究成果の概要

スマートコントラクトにおける新たな攻撃の模索と現実世界における実態調査という課題において、2024 年度は実態調査を主に進めた。とくにブロックチェーン技術として最大規模の市場を持つ Ethereum において、暗号資産を不正に操作するバックドア攻撃がどれだけ行われているかを調査した。現状の調査では 42.2% の暗号資産が潜在的な脅威の下にあるという結果になった。この成果は国際会議 NDSS 2025 で速報値としてポスター発表している 1)。また、分析を進めた結果を国際会議論文として BSCI 2025 に投稿も行っている。今後は実際の金銭被害などより詳細な分析を進めることで国際論文誌への採録も実施する。関連する成果として、2023 年度から継続していた脆弱性の調査論文もブロックチェーン専門の国際論文誌 ACM DLT に採録されている 2)。

上記の研究とは独立に、ブロックチェーンの中核技術の検討として、ブロックの書き込みを行うコンセンサスアルゴリズムとディジタル署名の設計についても新たな技術検討に着手した。コンセンサスアルゴリズムの設計については、従来のハッシュ関数の計算に代わり AI モデルの学習を用いる Proof-of-Deep-Learning に注目し、特に AI の分散学習において AI モデルの秘匿と正当性の検証を両立させるアルゴリズムを新たに設計し、その性能についても簡易なデータセットを用いて検証を行った。この成果は通信分野の高レベル会議である ICC に採録されている 3)。

また、並行して機械学習モデルのセキュリティ応用についても検討を行った。特にブロックチェーンの応用ともなる Web3 として悪性ドメインの検知を、海外の大学と連携して検討を行った。機械学習の特徴量選定を行うことで既存手法よりも高速かつ高精度な方式を実現し、ブラウザのアドオンツールとして実装を行っている。当該成果は情報セキュリティ分野のトップ論文誌である Computer&Security に採録されている 4)。

【代表的な原著論文情報】

1) Naoto Yanai, Naohisa Nishida, Yuji Unagami, “An Empirical Study of Backdoor Attacks on Ethereum Smart Contracts,” The Network and Distributed System Security (NDSS) Symposium 2025, 2025 年 2 月.
2) Chihiro Kado, Naoto Yanai, Jason Paul Cruz, Kyosuke Yamashita, Shingo Okamura, “Empirical Study of Impact of Solidity Compiler Updates on Vulnerabilities in Ethereum Smart Contracts,” Distributed Ledger Technologies: Research and Practice, ACM, 2024 年 8 月.
3) Yasushi Takahashi, Naohisa Nishida, Yuji Unagami, Naoto Yanai, “Aggregated Zero-Knowledge Proofs toward Distributed Proof-of-Deep-Learning,” 2025 IEEE International Conference on Communications (ICC 2025), 2025 年 6 月
4) Janaka Senanayake, Sampath Rajapaksha, Naoto Yanai, Harsha Kalutarage, Chika Komiya , “MADONNA: Browser-based malicious domain detection using Optimized Neural Network by leveraging AI and feature analysis,” Computers & Security, Vol.152, pp.104371-104371, 2025 年 5 月.5)