

西坂 龍太郎

セキュリティリサーチャー・株式会社リチエルカセキュリティ

Email: ryutaro.nishizaka@gmail.com・LinkedIn: www.linkedin.com/in/ryutaro-nishizaka・GitHub: github.com/KuonRuri・Google Scholar: scholar.google.com/citations?user=ZKCKiloAAAAJ・ORCID: orcid.org/0009-0007-9166-8848

CV

経歴

2026/07 – 現在	第10期生 孫正義育英財団
2025/04 – 現在	運営 SECCON Beginners
2024/07 – 現在	パートタイムセキュリティリサーチャー 株式会社リチエルカセキュリティ
2024/04 – 現在	立教新座高等学校
2024/03	立教新座中学校 卒業 — 優等賞受賞

論文

査読付き国際会議・ワークショップ

DeMeSSAI
EuroS&P '26 併催
2026年7月

How Far Can LLM Agents Go in Binary Exploitation? A CTF-Based Evaluation

Ryutaro Nishizaka, Yudai Fujiwara, Yuichi Sugiyama
5th International Workshop on Designing and Measuring Security in Systems with AI
(EuroS&P 2026 併催)

IEEE S&P '26
ポスターセッション
2026年5月

Poster: Where Do LLM Agents Fail in Binary Exploitation?

Yudai Fujiwara, Ryutaro Nishizaka, Yuichi Sugiyama
47th IEEE Symposium on Security and Privacy

PDF

SBFT
ICSE '26 併催
2026年4月

IPSM-Based Test Case Minimization for Network Protocol Implementations

Ryutaro Nishizaka, Kazushi Kato, Yuichi Sugiyama
19th International Workshop on Search-Based and Fuzz Testing (SBFT) (ICSE 2026 併催)
[doi:10.1145/3786155.3788580](https://doi.org/10.1145/3786155.3788580)

BAR
NDSS '26 併催
2026年2月

Towards LLM-Resistant Software Protection: Agent Failure Patterns in CTF Reverse Engineering

Ryutaro Nishizaka, Yudai Fujiwara, Takuya Shimizu, Kazushi Kato, Yuichi Sugiyama
Workshop on Binary Analysis Research (BAR) 2026 (NDSS Symposium 2026 併催)

査読なし国内学会

CSS 2025
2025年10月

RowHammer を用いた RISC-V Keystone TEE に対する特権昇格手法の検討

西坂 龍太郎, 川崎 秀昌, 高前田 伸也, 穂山 空道
コンピュータセキュリティシンポジウム 2025 (CSS) · pp. 1875-1882

CSS 優秀論文賞

[IPSJ 電子図書館](#)

[CiNii](#)

CSS 2025
2025年10月

ネットワークプロトコル実装における状態を考慮したテストケース最小化手法

西坂 龍太郎, 加藤 和志, 杉山 優一
コンピュータセキュリティシンポジウム 2025 (CSS) · pp. 937-944

[IPSJ 電子図書館](#)

[CiNii](#)

2026

★ 孫正義育英財団 全国から33名

10～20歳を対象とする第10期生に選出。

★ 情報処理学会 第88回全国大会

最優秀ポスター発表賞を受賞。

BAR 2026

NDSS 2026 併催の Workshop on Binary Analysis Research において主著論文を発表。

- ・ Towards LLM-Resistant Software Protection: Agent Failure Patterns in CTF Reverse Engineering

SBFT 2026

ICSE 2026 併催の International Workshop on Search-Based and Fuzz Testing において主著論文を発表。

- ・ IPSM-Based Test Case Minimization for Network Protocol Implementations

DeMeSSAI 2026

EuroS&P 2026 併催の International Workshop on Designing and Measuring Security in Systems with AI において主著論文を発表。

- ・ How Far Can LLM Agents Go in Binary Exploitation? A CTF-Based Evaluation

2025

★ コンピュータセキュリティシンポジウム 2025 (CSS2025) 270件超中13件

主著論文を2本発表。うち1本が歴代最年少で優秀論文賞を受賞。

- ・ RowHammer を用いた RISC-V Keystone TEE に対する特権昇格手法の検討 — CSS 優秀論文賞
- ・ ネットワークプロトコル実装における状態を考慮したテストケース最小化手法

★ SecHack365 30作品中6作品

学習コース坂井ゼミに採択。優秀修了生に選出。

- ・ Hisame: RISC-V 最高特権ファームウェアに対するファジングフレームワーク

情報処理学会 第87回全国大会

ポスター発表。

- ・ Keystone に対する RowHammer の攻撃可能性の評価

SECCON Beginners CTF 2025 (CTF4b)

運営として参加し、Pwn を3問出題 (pivot4b / pivot4b++ / TimeOfControl)。

情報科学の達人

第二段階 修了。

取材

二度目の取材が学校ホームページに掲載。

- ・ 道を切り開く力が育まれる学び舎 高校生×教員対談 ～立教新座の学び

2024

★ CognitiveHack Japan 2024

中学部門/中学学校別部門 優勝。

情報科学の達人 全国から40名程度

5期生に採択、第一段階を修了。

情報オリンピック

本戦出場。

Machine Learning Specialization

修了。

UK-Japan Young Scientists Workshop

修了。

2023

★ 情報処理安全確保支援士

歴代最年少で合格し、登録セキスペに。

セキュリティ・キャンプ全国大会

Cクラス (脅威解析) 修了。

セキュリティ・ミニキャンプ in 東京

Cトラック (マルウェア解析) 修了。

取材

学校ホームページに掲載。

- ・ 「情報処理安全確保支援士」最年少合格 サイバーセキュリティで社会貢献したい

資格

- ・ 情報処理安全確保支援士 — 第026794号
- ・ 応用情報技術者