



廣友 雅徳 准教授らの研究発表が
情報通信システムセキュリティ研究賞を受賞

【概要】

情報部門の廣友 雅徳 准教授らが発表したメモリへのサイドチャネル攻撃に関する研究発表が、電子情報通信学会の情報通信システムセキュリティ研究賞を受賞しました。

【本文】

情報部門 廣友 雅徳 准教授と、神戸大学、兵庫県立大学による共同研究グループが電子情報通信学会 情報通信システムセキュリティ（ICSS）研究会で発表した研究が、2019 年度情報通信システムセキュリティ研究賞を受賞しました。本賞は、ICSS 研究会で発表された優れた研究や将来性のある研究を対象に表彰するものです。

表彰対象の研究は、メモリへのサイドチャネル攻撃に関するものです。本研究では、RAMBleed と呼ばれる物理メモリに記録されている機密情報を読み取る攻撃手法について、それを改良し更に効果的な手法を提案するとともに、その手法の読み取り精度、攻撃実行時間、実現可能性を評価しています。情報セキュリティにおいて、攻撃手法の能力を正確に評価することは、情報システムを安全に利用するために重要です。このような内容が重要な研究成果として評価され、本賞を受賞しました。

○情報通信システムセキュリティ研究賞

発表題目：効果的な single-sided RAMBleed の提案

著 者：長濱 拓季（神戸大）、瀧田 慎（兵庫県立大）、廣友 雅徳（佐賀大）、森井 昌克（神戸大）

掲 載 誌：電子情報通信学会技術研究報告，vol.119，no.437，pp.145-150，March 2020

賞のホームページ：<https://www.ieice.org/iss/icss/award.html>



表彰状

【用語解説】

サイドチャネル攻撃：

情報システムの計算処理時間や消費電力などの物理的な特性を観測し測定することによって、機密情報を取得する攻撃手法。

RAMBleed：

物理メモリに繰り返しアクセスすることによってビット反転が誘発する現象を利用して、機密情報を取得するサイドチャネル攻撃。