別紙様式第２号

学位論文及び審査結果の要旨

横浜国立大学

氏　　名	坂本 純一
学 位 の 種 類	博士（情報学）
学 位 記 番 号	環情博甲第 2138 号
学位授与年月日	令和２年３月 24 日
学位授与の根拠	学位規則（昭和 28 年４月１日文部省令第９号）第４条第１項及び横浜国立大学学位規則第５条第１項　（論博の場合は第２項）
学 府・専 攻 名	環境情報学府　情報メディア環境学専攻
学 位 論 文 題 目	組込みプロセッサに対するレーザーフォールト攻撃と対策に関する研究
論 文 審 査 委 員	主査　横浜国立大学　教　授　松本　勉
	横浜国立大学　教　授　森　辰則
	横浜国立大学　教　授　四方順司
	横浜国立大学　准教授　吉岡克成
	横浜国立大学　講　師　白川真一

論文及び審査結果の要旨

スマートフォンやクレジットカードなど、重要な情報を格納するデバイスは、紛失や盗難時にも内部の秘密情報を漏らすことのないよう暗号化やアクセス制御などの論理的セキュリティ技術によってデータの秘匿性を担保している。しかし論理的なセキュリティ技術は物理的な実体を持つデバイス上に実装され動作するため、実世界では論理的な世界では考慮されていなかった攻撃（物理的な攻撃）が可能である。デバイスの動作に意図的にフォールトを注入する攻撃をフォールト攻撃という。フォールト攻撃はデバイスに想定外の動作を引き起こすため対策が難しく、さらに対策部分の動作すら誤る恐れがあることから極めて強力な攻撃であるとみなされている。本論文はレーザーを用いたフォールト攻撃とその対策について総合的に行った研究成果を示すものであり全６章から構成されている。

まず、フォールト攻撃とそれを取り巻く関連研究を１章で体系的に紹介している。２章ではデバイスにレーザーを照射する装置について論じている。市販のレーザー装置は非常に精密な制御が可能であるが、非常に高価であり一部の攻撃者しか利用できないものである。本論文では独自にレーザー装置の部品を選定し、制御ソフトウェアを開発して安価なレーザーフォールト注入装置を提案している。構築したレーザー装置は市販品に劣らない精度を持ちながら価格を抑えることに成功している。さらに回路上の 2 点を同時に照射できるダブルスポットのレーザー装置も新たに開発している。

３章ではレーザーフォールト攻撃の対象となり得るデバイスの構成について論じている。まず組込みプロセッサのアーキテクチャを示し、ペアリング暗号と呼ばれる高機能暗号システム高速化のための専用コアの開発を記述している。このようなアクセラレータもレーザーフォールト攻撃の対象となり、またアクセラレータに直接フォールト攻撃せずとも、ROM にレーザーを照射することで命令改変攻撃が可能であることを示している。

４章では２章で示した装置を用いて３章の攻撃対象を攻撃した際にどのような効果が得られるかを説明している。レーザーの照射場所として、多くの組込みプロセッサでプログラム格納領域として利用されている NOR フラッシュメモリに着目している。フラッシュメモリへのレーザー照射は実行される命令を“改変”することができる。従来の研究では命令改

変のようなフォールトは精密な制御が必要であるため実現不可能であると結論づけられていたが、本論文では安価なレーザー装置でも命令改変攻撃が可能であることを示している。

5 章ではレーザー攻撃に対する対策手法を示している。IoT 社会のエッジノードなどに利用される低コストデバイスにも導入できるような、ソフトウェア上で低いコストのレーザーフォールト対策にニーズがあると考え、4 章で示した命令改変攻撃に対に適切な制約を与えることでソフトウェア上での対策を提案し、シミュレーションによる効果の検証を行っている。本論文の総括が 6 章でなされている。

以上のように、本論文は、命令改変攻撃と呼ばれる強力なフォールト注入が、低いコストのレーザー照射で実現できることを示し、さらに命令改変攻撃に対するソフトウェア上での対策を提案している。市販のレーザー攻撃評価用装置はなるべく精密なレーザー照射を行うことを目指しているため非常に高価であるが、攻撃方法によってはそれほどの精密さが要求されずより低コストに実行可能な場合がある。適切にセキュリティ評価を行うには、攻撃に必要なコストの下限を知ることが重要であり、本論文はこの意味で、極めて大きな成果を含むものといえる。また、本論文を構成する主要な研究成果は、1 篇の査読付国際論文誌論文、2 篇の査読付国際会議論文、および 4 篇の電子情報通信学会の国内会議論文により公表され、高い評価を受けている。

よって、本論文は博士（情報学）の学位論文として十分な価値を有すると論文審査委員全員一致で認め、令和 2 年 2 月 5 日（水）15 時から 16 時 20 分までの環境情報 1 号棟 305 号室における博士論文発表会終了後の 16 時 25 分から 16 時 50 分まで、同棟 3 階 304 室において審査委員全員出席のもとで、坂本純一氏の最終試験を行った。50 名の参加者を得て充実した質疑応答がなされた博士論文発表会を踏まえ、学力試験として情報セキュリティを中心とする専門分野および情報工学関連分野における口頭試問を行い、これらの分野の研究に関する深い専門知識と理解力、表現力、および質疑応答における適切な対応能力を同氏が有することを確認した。外国語は、英語論文執筆と国際会議において英語にて発表していることをもって、十分な学力を有すると判定した。また博士課程後期修了に必要な単位をすべて取得していることを確認した。これらから、坂本純一氏は最終試験に合格であると、審査委員全員一致で判定した。

以上の論文審査委員会の結論に基づき、令和 2 年 2 月 17 日（月）に開催の環境情報学府情報メディア環境学専攻会議にて審議し、全員一致で本論文を博士（情報学）の学位論文としての価値があるものとして環境情報学府教授会に付議することを決定した。その後、環境情報学府学務委員会での確認を経て、令和 2 年 3 月 2 日（月）に開催された環境情報学府教授会において審議を行い、無記名投票により、坂本純一氏に博士（情報学）の学位を授与することを決定した。