IPA

2017 年度 未踏 IT 人材発掘・育成事業 採択案件評価書

1. 担当 PM

竹迫 良範（株式会社リクルートマーケティングパートナーズ 専門役員）

2. 契約者氏名

クリエータ：師尾 彬（東京理科大学 大学院）

3. 委託金支払額

2,304,000 円

4. テーマ名

自由な PC 向けファームウェアの開発

5. 関連 Web サイト

https://github.com/yabits/uefi

6. テーマ概要

現在普及しているコンピュータにはハードウェアのリセットから OS の起動までを担う、ファームウェアが搭載されている。ファームウェアは通常ハードウェアベンダにより、プロプライエタリなソフトウェアとして提供されており、ユーザに対してはそのソースコードが公開されてはいないため、ユーザがファームウェアを修正することは困難となっている。16bit 時代から続く IBM PC/AT 互換機のファームウェアでデファクトスタンダードだった BIOS は使われることが少なくなり、最近の 64bit マシンでは BIOS の代わりに UEFI のファームウェアが搭載されることが普通になってきた。現在の一般的な PC 向けファームウェアの規格である UEFI に対応するオープンソースのファームウェアは Intel により開発が進められている TianoCore のみである。各マザーボードベンダーが開発しているプロプライエタリなファームウェアは TianoCore をリファレンスとして実装されているものが多く、TianoCore の UEFI 実装に脆弱性が存在した場合、その影響は非常に大きいものとなる。

本プロジェクトでは、coreboot 上に TianoCore に置き換わる UEFI 対応のコンパクトでオープンな payload を開発する。

7. 採択理由

16bit の MS-DOS 時代から続く IBM PC/AT 互換機のファームウェアでデファクトスタンダードだった BIOS は使われることが少なくなり、最近の 64bit マシンでは BIOS の代わりに UEFI のファームウェアが搭載されることが普通になってきた。既存の UEFI のリファレンス実装の一つである TianoCore とは別のオープンソースの UEFI 実装をフルスクラッチで行なうという提案である。サブセットで小さなものを作るというよりも、ベアボーンとプラグインによる実装で必要なものだけを選んでフットプリントの小さいファームウェアを自由に構築できるというところがポイントである。PXE ブートなどのネットワークブートの仕組みと絡めると、BareMetal クラウドへの応用が広がるかもしれない。地味なプロジェクトに感じられるかもしれないが、コツコツと開発を続け、PC ファームウェアの世界でもオープンソースによる自由な開発が進む流れの一翼を担うことを期待し、採択した。

8. 開発目標

UEFI の規格は非常に巨大であるが、通常の OS の起動には使われていない機能も多い。そのため、Attack Surface を減らすためにも、UEFI 規格のうち必要最小限の機能を備えたベアボーンとして payload を実装し、その他の機能は必要に応じてプラグインとして追加できるようにする。コンパクトでオープンなファームウェアを実現することを目標とする。

9. 進捗概要

本プロジェクトでは OS の起動にのみフォーカスした必要最小限の機能を持った UEFI 実装 yabits/uefi を coreboot payload として開発した。coreboot がサポートしていれば QEMU などの仮想マシンを含め、どのようなマシンでも動作する。実際に yabits は QEMU や Lenovo ThinkPad X230 で動作することを確認した（図 1、図 2）。

OS を起動させるためには、通常の UEFI と同等のインターフェースを持っている必要があり、BootServices や RuntimeServices、EFI System Table 対応や GUID Partition Table Disk Layout 対応などの機能を一通り実装した。一方で、今後は UEFI に取って代わられるであろう古い Legacy BIOS との互換性は持たせておらず、純粋な UEFI として実装されている。

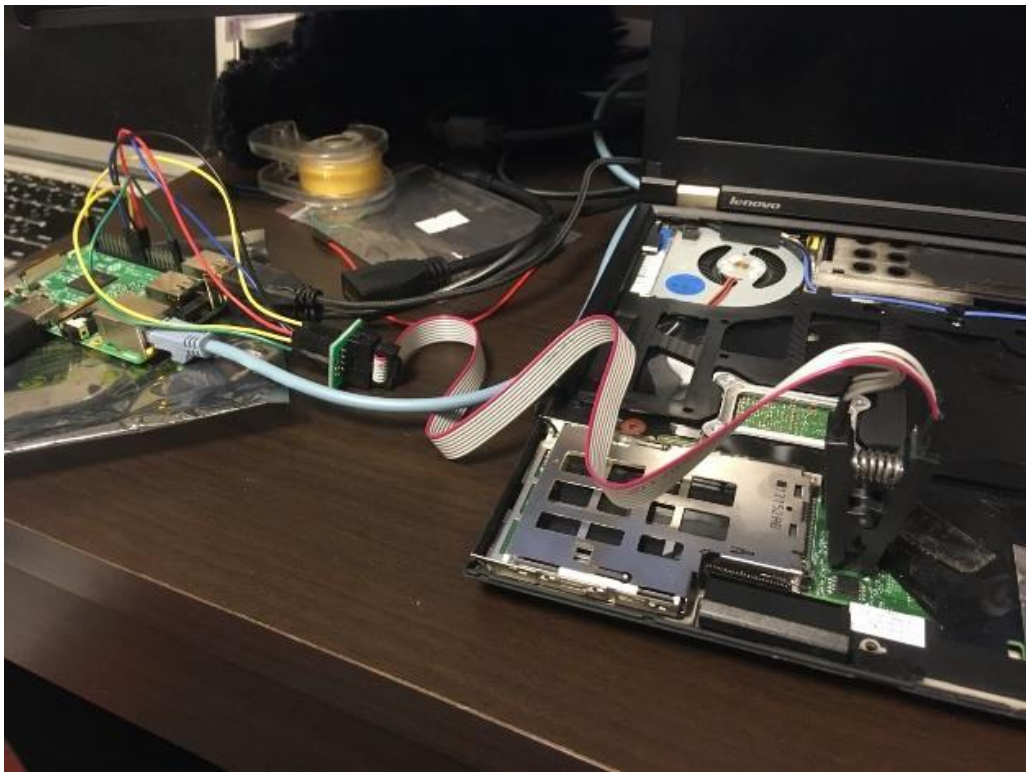

図 1. Raspberry Pi 経由で自作ファームウェアを書き込んでいる様子

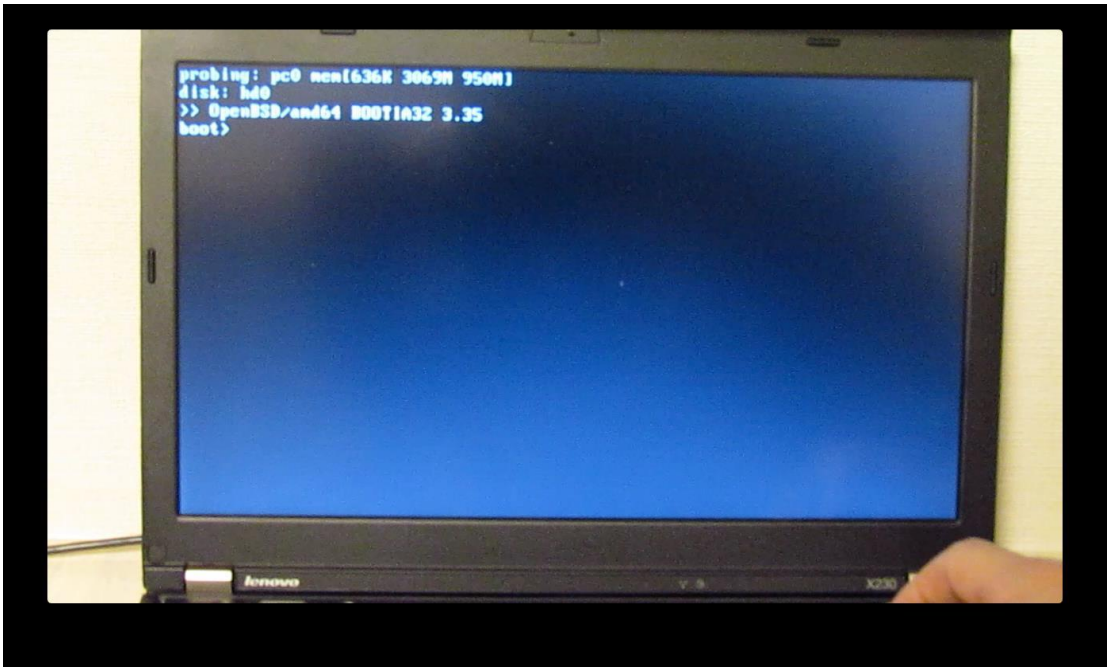

図 2. 自作 UEFI 経由で OpenBSD が起動した Lenovo ThinkPad X230

yabits/uefi は、既存の UEFI 実装 TianoCore と比較して 2 倍以上高速に起動して、かつフットプリントのサイズが約 1/10 へと軽量となった。ハードウェアがリセットされてから OS が起動するまでを担うという点においては既存のファームウェアと大きな差はないが、一方で、既存の UEFI 実装と比較してフット

プリントが小さいことから、一般的な PC のみならず組み込みデバイスなどでの利用も考えられる。また、起動時間が短いことから、ベアメタルクラウドにおいてインスタンスを起動した際の起動時間の短縮やコストカットが見込まれる。

本システムの開発により、これまであまり考慮されることの少なかったファームウェアなどの分野においてもオープンソース化の流れが一層強まり、ハードウェアにバックドアが仕込まれていないことを各人が検証できるようになることが期待される。

10. プロジェクト評価

長らくエミュレータ QEMU でのプロトタイプ開発を実施していたが、プロジェクト終盤においては、Lenovo ThinkPad X230 でのファームウェア書き換えを実施し、実際に自分の作った UEFI ファームウェアが実機で動作することまで確認できた。未踏プロジェクト期間中にも PC 向けハードウェアに一般的に搭載されている Intel のチップに存在するロプライエタリなファームウェアの脆弱性が公開されることがあり、社会的な関心を集めた。Google も類似プロジェクトを開始したが、自分の手で検証でき、自分でソースコードを確認し修正できるオープンでオルタネイティブな実装を複数持つことは社会的に意義が大きい。

11. 今後の課題

今後は一人で開発していくにはリソースが足りないため、国内外のカンファレンスでの登壇や、Web 上での情報発信活動を積極的に行い、オープンソース開発コミュニティの形成に努めることが課題である。また、既存の BIOS ベンダに積極的にアプローチし、デフォルトの BIOS として採用されることが望ましい。