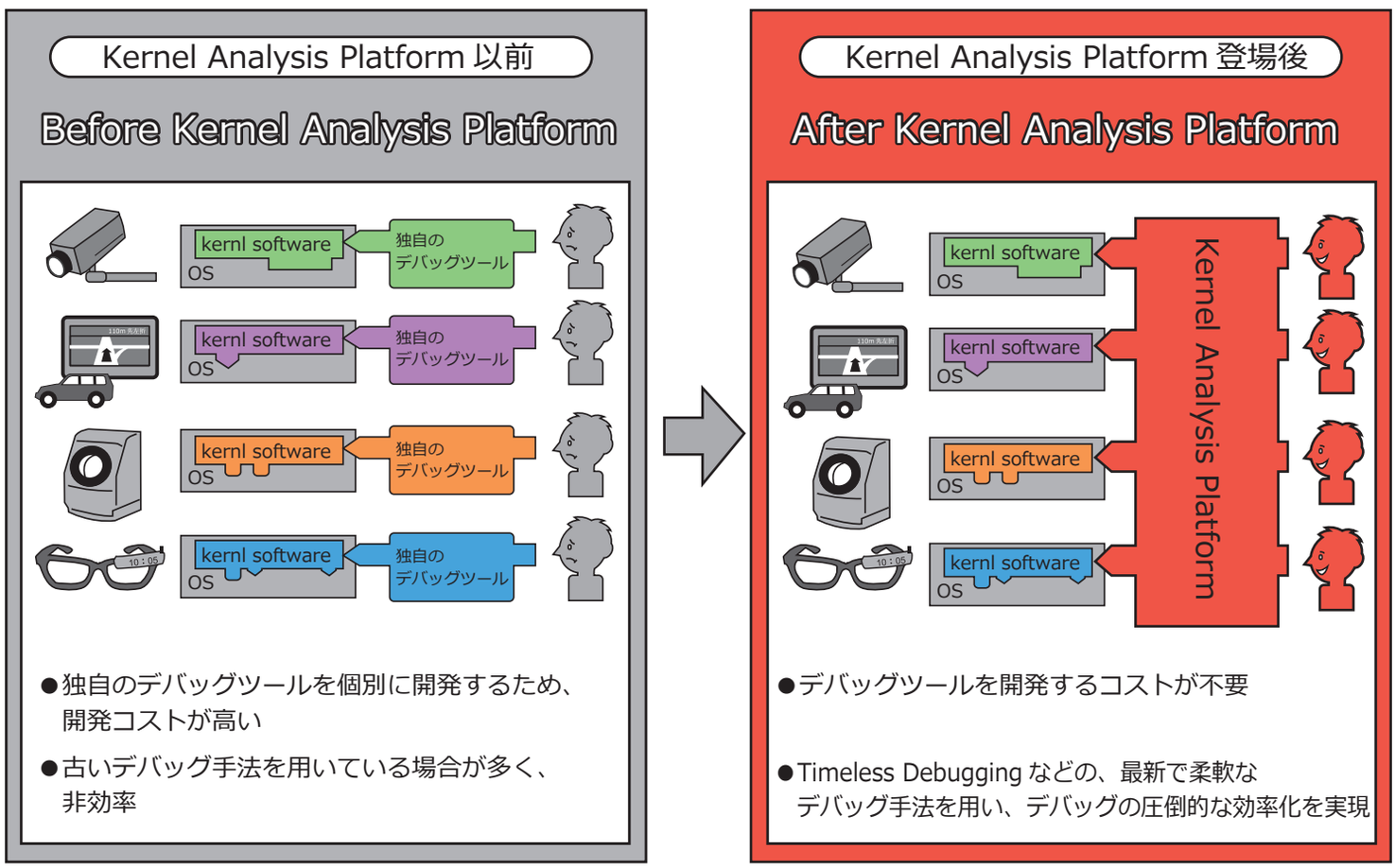
木村　廉　氏
神戸大学 大学院 科学技術イノベーション研究科

IoT 社会を加速させる、 ハードウェア制御用プログラムのデバッグ、 テスト、 解析プラットフォーム「Kernel Analysis Platform（カーネル アナリシス プラットフォーム）」の開発

デバイスドライバなど OS 内で動作するソフトウェアの開発を支援するための開発プラットフォーム「Kernel Analysis Platform」を開発した。「Kernel Analysis Platform」により、ハードウェアベンダにおけるデバイスドライバの開発コストが下がり、 より多くの機器の登場が期待できる。 また、「Kernel Analysis Platform」を利用することで、 既存のソフトウェアに対しても、 多くのバグが発見できる可能性もある。



正式テーマ名：カーネルソフトウェア開発支援ツール

6 木村 廉 氏（神戸大学 大学院 科学技術イノベーション研究科）

IoT 社会を加速させる、ハードウェア制御用プログラムのデバッグ、テスト、解析プラットフォーム「Kernel Analysis Platform（カーネル アナリシス プラットフォーム）」
（正式プロジェクト名：カーネルソフトウェア開発支援ツール）

デバイスドライバなど OS 内で動作するソフトウェア（以降「カーネルソフトウェア」と呼ぶ）の開発を支援するための開発プラットフォーム「Kernel Analysis Platform」を開発した。
IoT 社会の広がりにともない、制御、接続されるハードウェアは多様化、複雑化している。それらハードウェアは、カーネルソフトウェアを介して OS の中で制御されることで、開発者は容易にそれらを使用するプログラムを開発することができる。しかし、このカーネルソフトウェアにバグがあると、OS を巻き込んだ重大なクラッシュにつながる場合が多いため、カーネルソフトウェアの開発では入念なデバッグやテストが必要である。従来、ハードウェアベンダは自社専用のデバッグ、テストツールを開発し、利用してきたが、標準的かつ効率的に扱えるカーネルソフトウェアのデバッグ、テストツールは少なかった。また、カーネルソフトウェアはハードウェアの制御を伴うため、オフィスソフトウェアやゲームなど、ハードウェア制御を考慮する必要がない OS 上で動くソフトウェアのデバッグに用いられる Timeless Debugging などの、最新で柔軟なデバッグ手法を用いたデバッグツールの存在は皆無であった。
本プロジェクトでは、上記の Timeless Debugging などのデバッグ手法をカーネルソフトウェアの開発にも取り入れた。また、仮想化技術を駆使することで、OS に依存しない柔軟なデバッグ、テストツールを実現した。
この成果により、ハードウェアベンダにおけるデバイスドライバの開発コストが下がり、より多くの機器の登場が期待できる。また、既存のソフトウェアに対しても、本成果を利用することで、多くのバグが発見できる可能性もある。

評価ポイント（担当プロジェクトマネージャー　後藤 真孝 氏）：
デバイスドライバなどのカーネル空間で動作するソフトウェアの開発を支援するためのカーネルソフトウェア開発支援ツール「Kernel Analysis Platform」を木村君は実現した。ソフトウェア開発においてデバッグは不可欠だが、カーネルソフトウェアのデバッグの場合には、通常のユーザ空間でのデバッグを効率化する動的解析ツールの利用が困難という問題があった。木村君は、この問題を解決するために、開発者が利用するユーザインタフェースであるフロントエンドと、カーネルソフトウェアの動作情報を記録する基盤技術であるバックエンドで構成される「Kernel Analysis Platform」を実現することに成功した。フロントエンドとしては、カーネルソフトウェア専用のデバッガ「KlareDbg」および自動テストツール「kvalgrind」の二つを開発した。特に KlareDbg では、従来はユーザ空間でのデバッグにしか用いられていなかった Timeless Debugging というデバッグ手法を実装することで、任意の命令に自在にカーソルを移動して実行時の状態を復元・確認可能にした点が優れている。さらにバックエンドでは、当初の計画では、仮想マシン（VM）で OS ごとエミュレートさせる「QEMU 改」のみの開発であったにも関わらず、実機を用いた効率的なデバッグも可能にした方が開発者の利便性が高いことから、ハイパーバイザにより実機を利用しつつ解析対象のカーネルソフトウェアのみエミュレート（インタプリタ実行）させる「K2E」も木村君は開発した。しかも K2E では、開発者が容易にテストを拡張でき

るようにプラグイン機構を提供し、そのプラグイン開発を円滑にできるように、C++の標準ライブラリまで自力で移植してしまうなど、非常に大規模なソフトウェア開発を木村君は成し遂げた。VM には QEMU、ハイパーバイザには BitVisor という既存の優れたソフトウェアをベースにしながら、木村君自身がそれらのソフトウェアを読解して深く理解することで、従来は実現されていなかった改造・拡張を可能にし、二つのバックエンドを実現したことは、当初の想定を大きく上回る特筆すべき成果である。既に GitHub にて一般公開中であり、フィードバックを得ながら開発を進めるなど、カーネルソフトウェア開発を的確に支援する素晴らしい成果をあげた。その木村君の才能と卓越した構想力、達成力、プレゼン力、情熱、開発実装力を、極めて高く評価する。