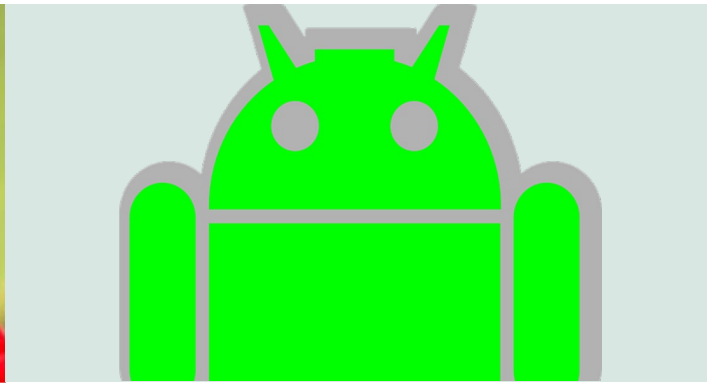
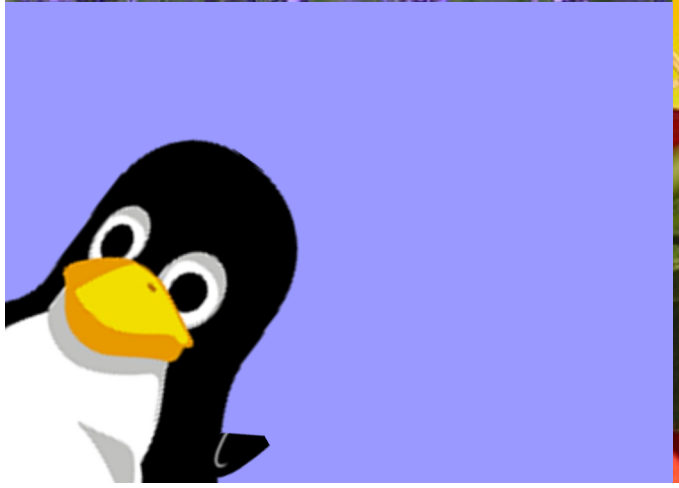


2026年度
毛利研究室紹介



本日の流れ

- 研究室全体紹介
- アンケートのお願い
- 研究紹介＆デモ＆先輩セッション
  - Lavender
  - Alkanet
  - Salvia
  - Network

研究のススメ

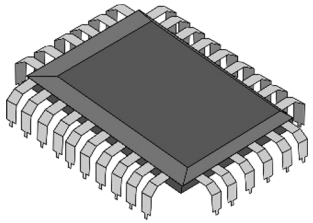
- 実験とは違い、研究は
  - 自分(と教員)で、先端技術の未知の課題を設定し
  - 課題解決に向け、一歩一歩、正しさを確認しながら進み
  - その正しさを客観的根拠を示して説得(知見の蓄積を)する行為
- 先端技術だし未知なので
  - 課題を理解することも難しい。課題の理解度向上が鍵
  - どれだけ進めるのかは推測できない
  - 進んだからこそ、課題の修正がなされることも
  - 課題を達成したら、そこには次の課題が。研究は終わらない
- なので
  - 思い切って飛び込むこと、そして、必至に泳ぐのが大切
  - どんなに遅い歩みでも、進んでさえいれば、必ず陸に到達する
  - これを初めて1周するのが卒論、さらに2周するのが修士、さらに3周するのが博士。

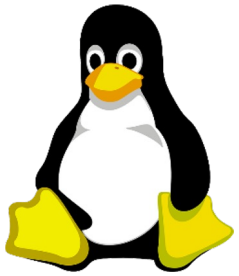
解決法として妥当か

進学お勧め

グループとキーワードで見る研究分野

- Lavender
  - オペレーティングシステム
  - ハイパーバイザ、仮想化技術
  - TEE、eBPF、Unikernel、LLVM（コンパイラ）
- Alkanet
  - Windowsセキュリティ、ライブフォレンジックス
  - マルウェア動的解析・静的解析・解析システム
  - 最新ハードウェア調査と活用（RDMA、DPU、SmartSSD）
- Salvia
  - ネットワークセキュリティ、Linux等のセキュリティ
  - ハニーポット設置、標的型攻撃誘引、攻撃者追
  - ファームウェア解析
- Network
  - ネットワークシミュレータ
  - セキュアネットワークコーディング





産官学連携と成果

期待大きい！
就職も安心

- 共同研究・外部資金等（共同研究・受託研究）
  - 三菱電機① 情報総研　　DPUとRDMAを用いた信頼性向上技術
  - 三菱電機②　〃　　RISC-V リアルタイムOS向け仮想化技術
  - アドソル日進　　SGL/AGL、Unikernel
  - 情報通信研究機構(NICT)　STARDUST、CURE、ファームウェア評価
  - 日立製作所（予定）　　サイバー攻撃監視向けログ管理法
- 研究連携・メンバシップ
  - 名古屋工業大学、奈良女子大学、龍谷大学
  - Linux Foundation、ELISA
- 対外発表（2021年度～）
  - 査読付きジャーナル論文 5件
  - 国際会議 5件
  - 国内シンポジウム・研究会・全国大会 50件（うち受賞12件）

みんなも
世界と戦える！

研究室の現メンバと研究グループ

- スタッフ
  - 教授　毛利 公一
    - IoTセキュリティ研究センター長
    - NICT 招へい専門員・協力研究員
  - 客員准教授　瀧本 栄二（奈良女子大）
  - 客員研究員　芝　公仁（龍谷大）
  - 客員研究員　竹久 達也（㈱ニッシン/NICT）
- 学生
  - D2: 1名
  - M1: 4名、M2: 5名
  - B4: 8名

強力なスタッフ陣！

身近で頼れる先輩！

日常の研究活動概要

- グループゼミ
  - グループ毎に週1回開催
  - 毎回，進捗状況や論文輪読等をミニプレゼン
  - グループメンバでディスカッション

  ※ 研究テーマは個人毎に決めます．プロジェクト開発ではありません

  ※ グループ数・メンバは技術内容・規模等に応じて柔軟に変化します

日常的な細やかなアドバイスが得られる！
近い分野のメンバで関連技術もゲット!

- 全体ゼミ
  - 週2回開催
  - ローテーションで（月1回程度）研究状況のプレゼン
  - 全員でディスカッション

普段の研究活動の成果を全員でshare!
プレゼン技術・ドキュメンテーション技術もゲット！

- 共同研究ゼミ
  - 企業・他大学との研究交流（互いにプレゼン・ディスカッション等）

コミュニティが広がる！視野が広がる！
技術が深まる！これぞ醍醐味！

お知らせ

6月10日（水）6限（18:25～）打ち上げします

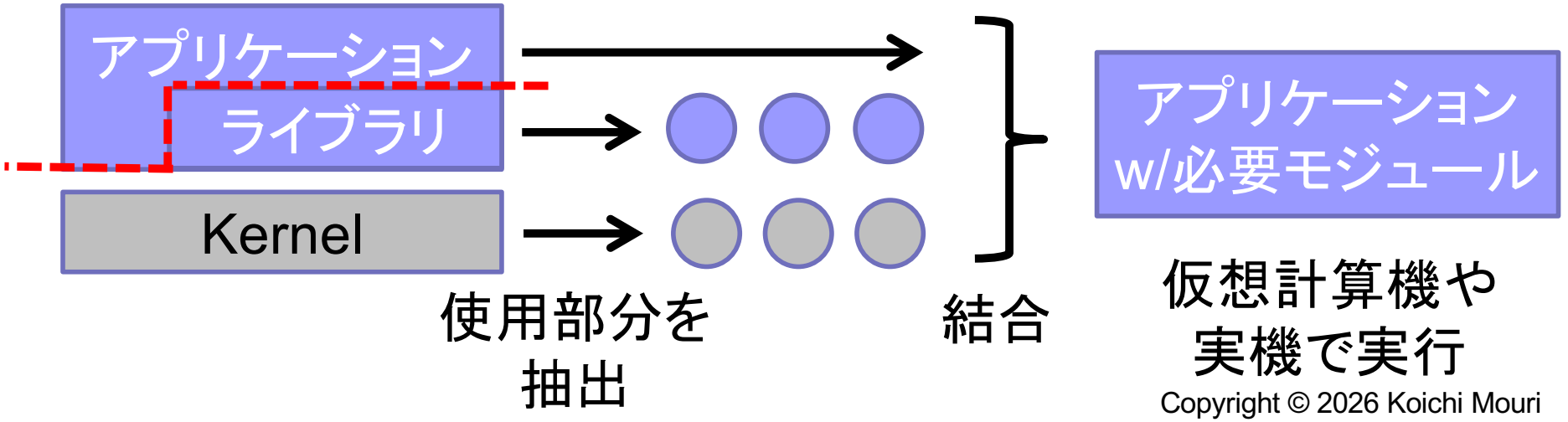
たこパか、ピザパか、両方か

3回生の皆さんも welcome！

Lavender

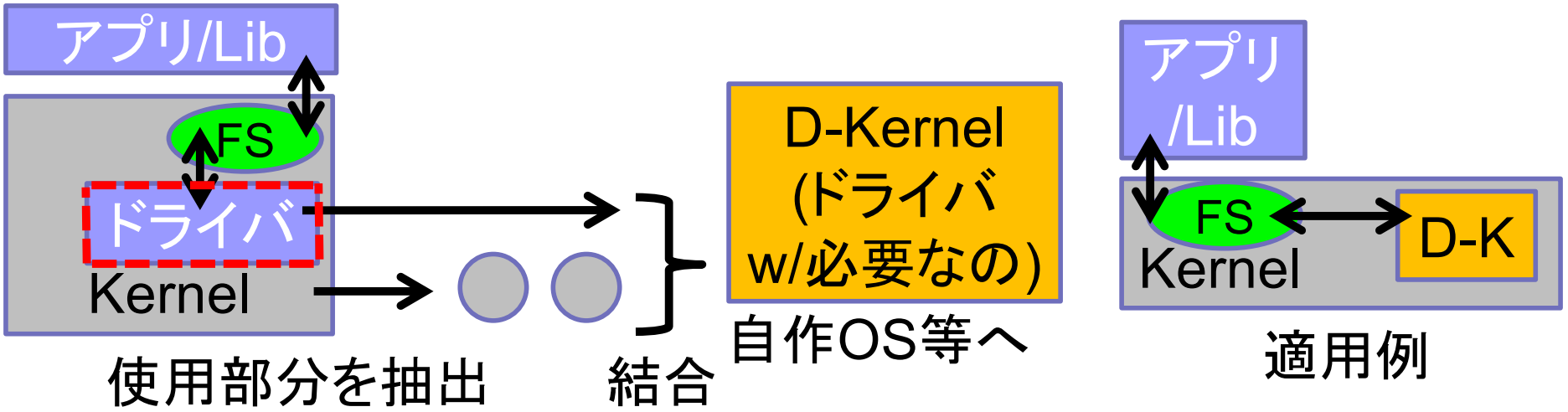
Unikernel的デバイスドライバ 背景

- Unikernelは下記から成る実行モジュール
  - アプリケーションプログラム
  - 必要とするライブラリやカーネルモジュール
    - Docker同様、アプリ単位で配布等ができたり、OS全体のセットアップ等が不要なところが便利
- 切り口：API（ライブラリ、システムコール）



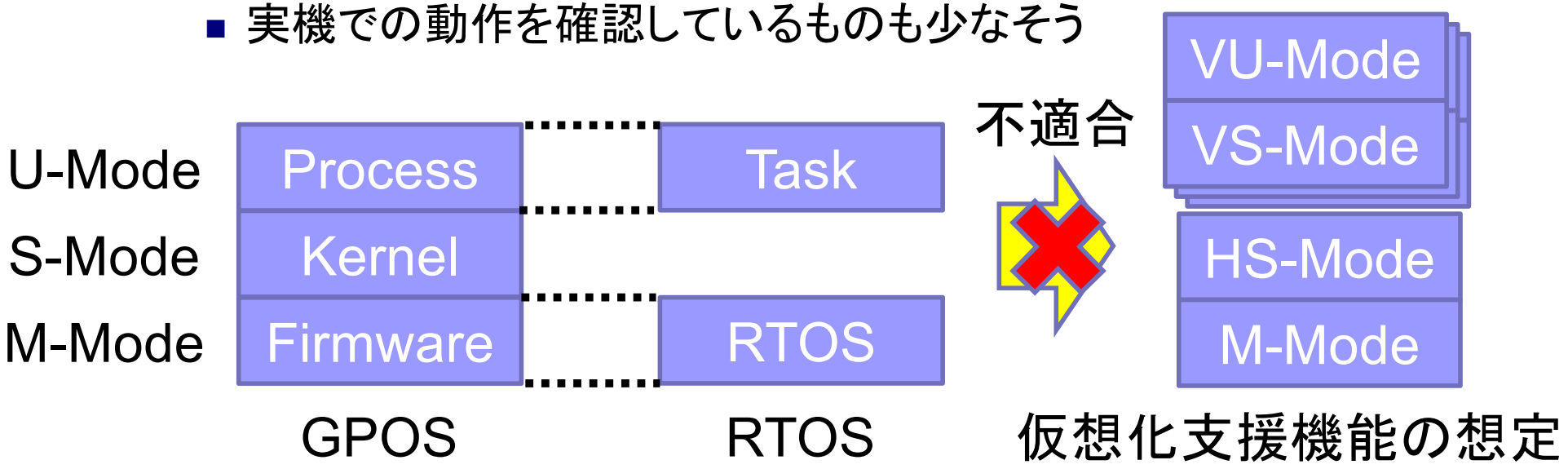
Unikernel的デバイスドライバ

- OS毎にデバイス毎にデバイスドライバを作るのが大変
- 充実したLinuxのデバドラ、流用できたら革命的なんだけどな
- 「デバイスドライバ＋OS」の実行モジュールを作って流用！
  - Linuxデバイスドライバ（LKM; 後からロード可能な形式）
  - 必要とするカーネルモジュール
- 切り口：カーネル内インタフェース（関数）



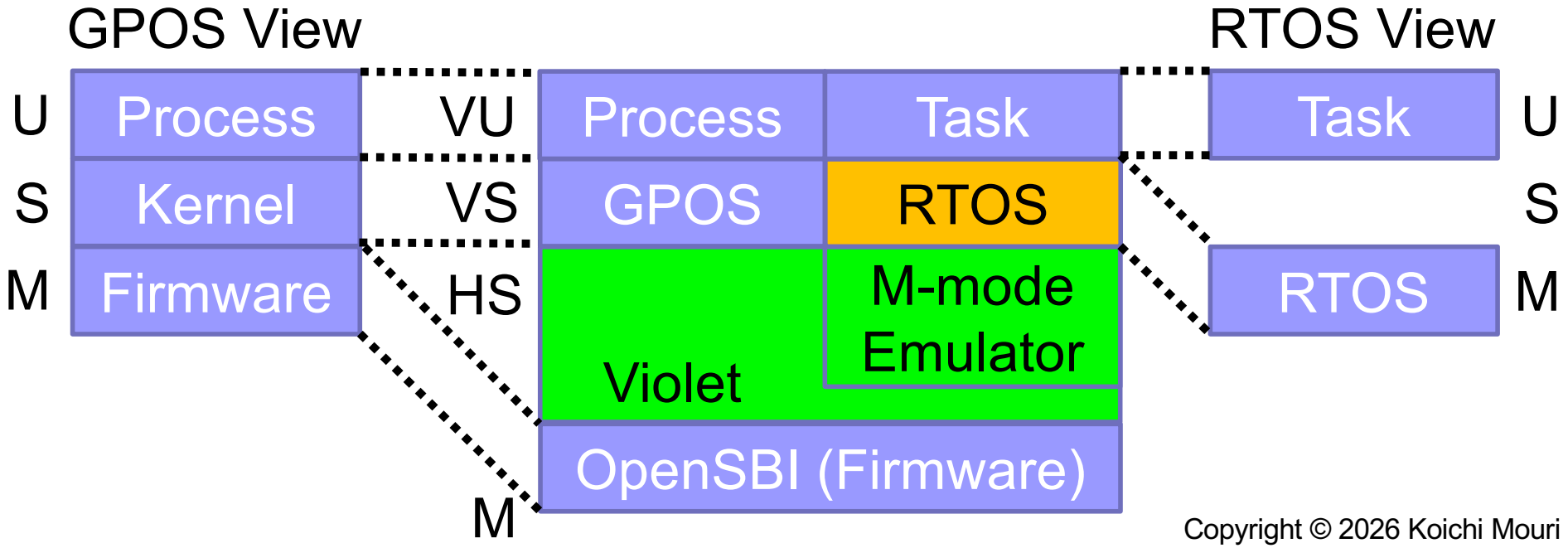
RISC-V向けハイパーバイザ 背景

- RISC-Vは仮想化支援機能を提供
  - Linux等GPOS（S-Modeで実行）の仮想化を想定。
    FreeRTOS等リアルタイムOS（M-Modeで実行）は想定せず
  - そもそもハイパーバイザの実装も限られる
    - KVM、Bao Hypervisor等
    - 実機での動作を確認しているものも少なそう



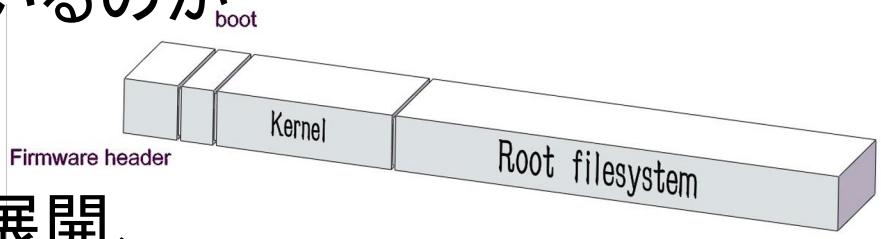
RISC-V向けハイパーバイザ

- RTOSを実行可能な仮想化を実現したい
  - GPOSはS(HS)-Modeで、RTOSはM-Modeで実行されているようにエミュレーション
  - 複数のVMを実行可能とすること
  - 実機実装すること

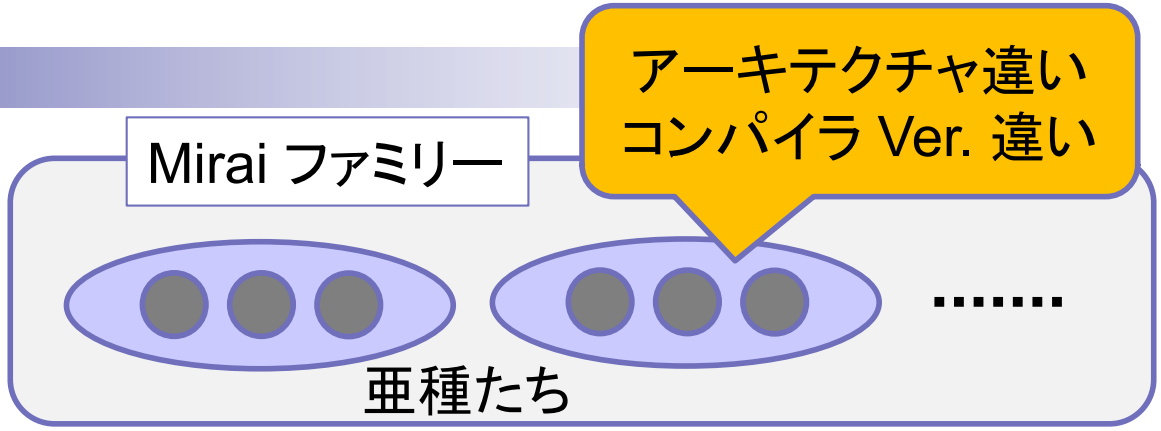


ファームウェアの安全性評価

- ファームウェア（OS、アプリの集合）は安全か？
  - OS、アプリ、ライブラリの更新に追いついているか
  - アプリとライブラリの関連性は正しく管理されているか
  - 独自拡張部分はどうか
  - 設定ファイルに依存する関連性はどうか
  - リリースノートと実態は合っているのか
- アプローチ
  - ファームウェア収集、ファイル展開、アプリ・バージョン特定
  - カスタマイズの有無の調査、ライブラリの関連性調査
  - 設定ファイル等の調査、実質的（実行時）関連性調査
  - CVEとの対応付け、バグ部分・修正部分の特定、など



LLVMコンパイラとマルウェア



- マルウェアのあるある
  - ソースコードはない
  - 亜種が多い
  - 同種だけど、
    アーキテクチャ違いのバイナリを構築
  - 同種、同一アークテクチャでもコンパイラのバージョンが異なる
- そんな中で、現状のハッシュ値でのマルウェア比較は限界
  - プログラムの内容的に比較したい
  - アーキテクチャが異なるバイナリ同士も比較したい
  - コンパイラが違ってもバイナリ同士を比較したい
- 動的解析？静的解析？ソースに戻して（デコンパイル）？
  - 中立的なちょうどいいところで比較！

宇宙向けOSの開発

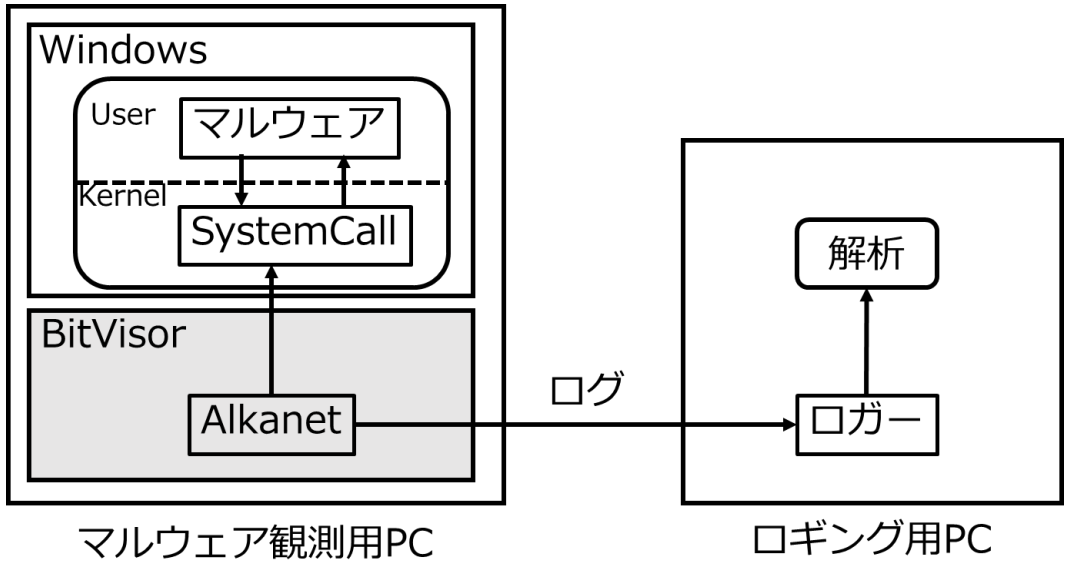
- Space Grade Linux (Linux Foundation/ELISA)
  - 宇宙（人工衛星、宇宙機）向けLinuxディストリビューション
  - 安全認証の取得、共通のツール・プロセス・基準の作成、標準化などを目的に
- 一定の安全性に向けた取組がなされている
  - 自動ビルド、カーネルの設定・最小化手法
  - ソフトウェア構成管理（SBOM）・品質管理の導入
- しかし、宇宙空間でのシビアな環境でLinuxのような高機能なOS＋アプリを動かすにはさらに機能の安全性を高める必要がある
  - 宇宙線対策、温度、電力、長時間稼働、通信方式、操作法の違い

Alkanet

動的解析環境 Alkanet

- マルウェアの素早い解析には動的解析が重要
- 動的解析では，対解析機能を持つマルウェアに悟られずに解析することが必要

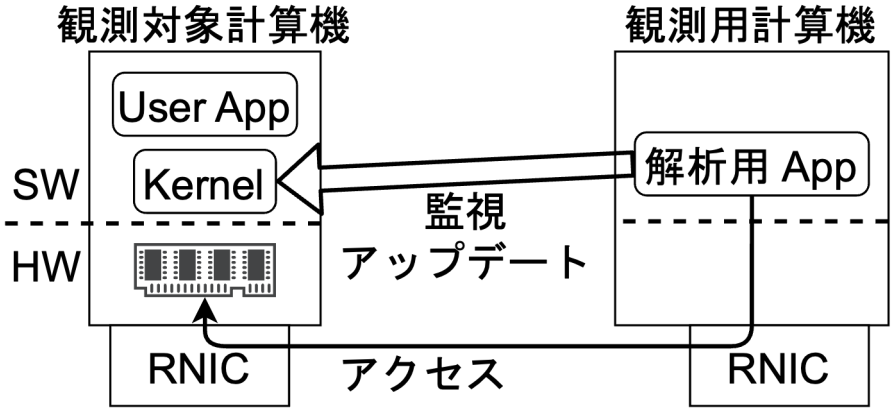
システムコールに着目し、仮想化技術を活用した
動的解析を行うAlkanetを開発



- **システムコールトレース**
- **システムコールの詳細情報取得**
  - 引数，発行元プロセスの取得
- **スタックトレース**
  - コードインジェクションの解析
  - システムコール発行までの関数呼び出しの追跡
- **スナップショット**
- **ログの送信**

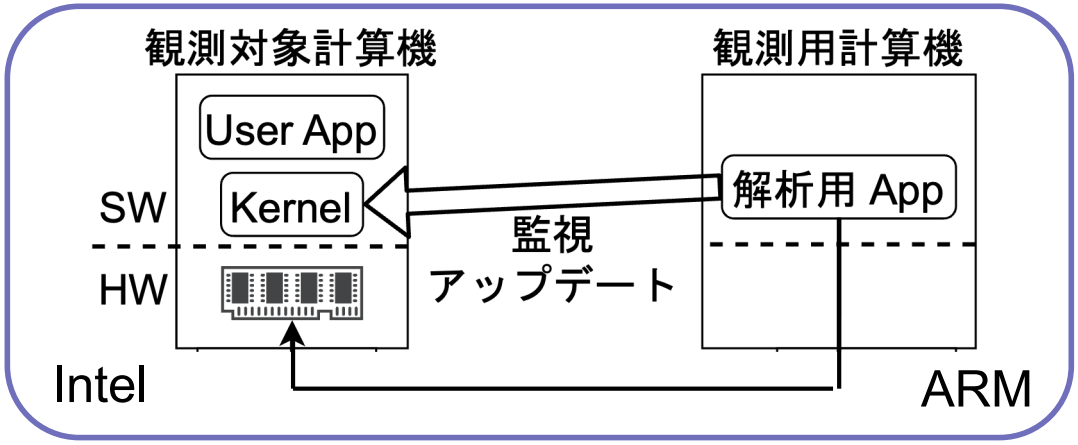
RDMAを用いた信頼性向上技術

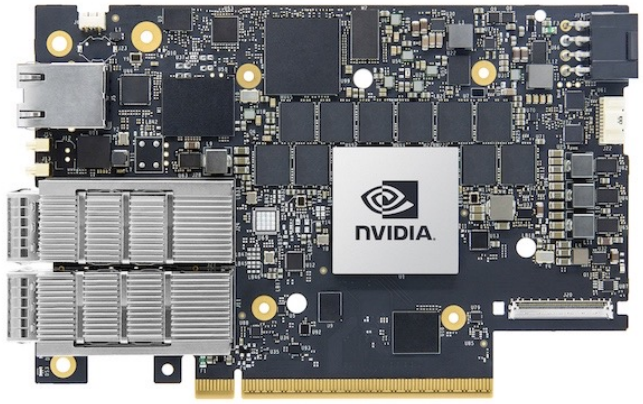
- プロセスの監視・更新は信頼性向上技術として一般的
  - 同一OS上、または同一ホスト内
- RDMA技術の活用
  - ネットワーク経由で、複数台のメモリの監視、更新が可能
  - 動的パッチ、チェックポイント、移動など、
    読み書きを必要とする高度な手法を実現
- これを使った動的パッチシステムの開発



DPUを用いた信頼性向上技術

- 前ページのも面白いが、さらにこちらはもっと近くなったらどうなるか・・・ NVIDIA Bluefield-3
- RDMA技術に似ているが
  - アクセスが圧倒的に速いため、膨大なデータの操作の可能性が視野に入る
  - 例えば、チェックポイントとロールバック機能など
- 学習中のAIモデルバックアップ方式の開発



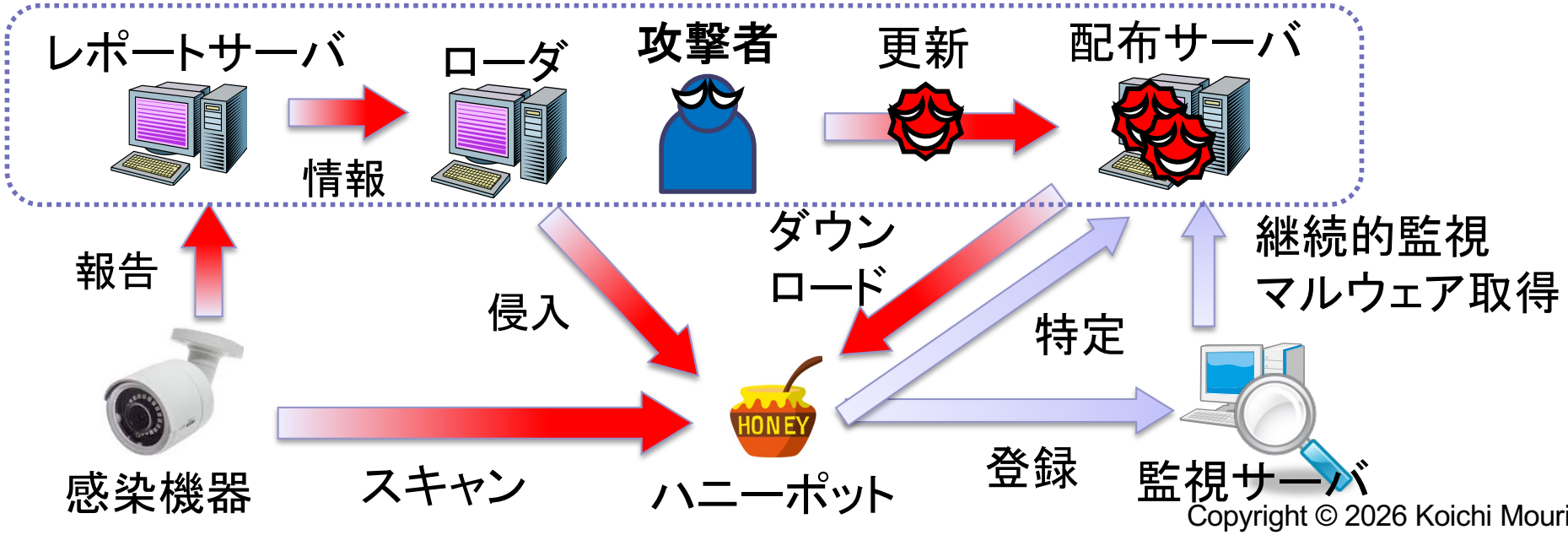


Salvia

IoTマルウェアの亜種追跡

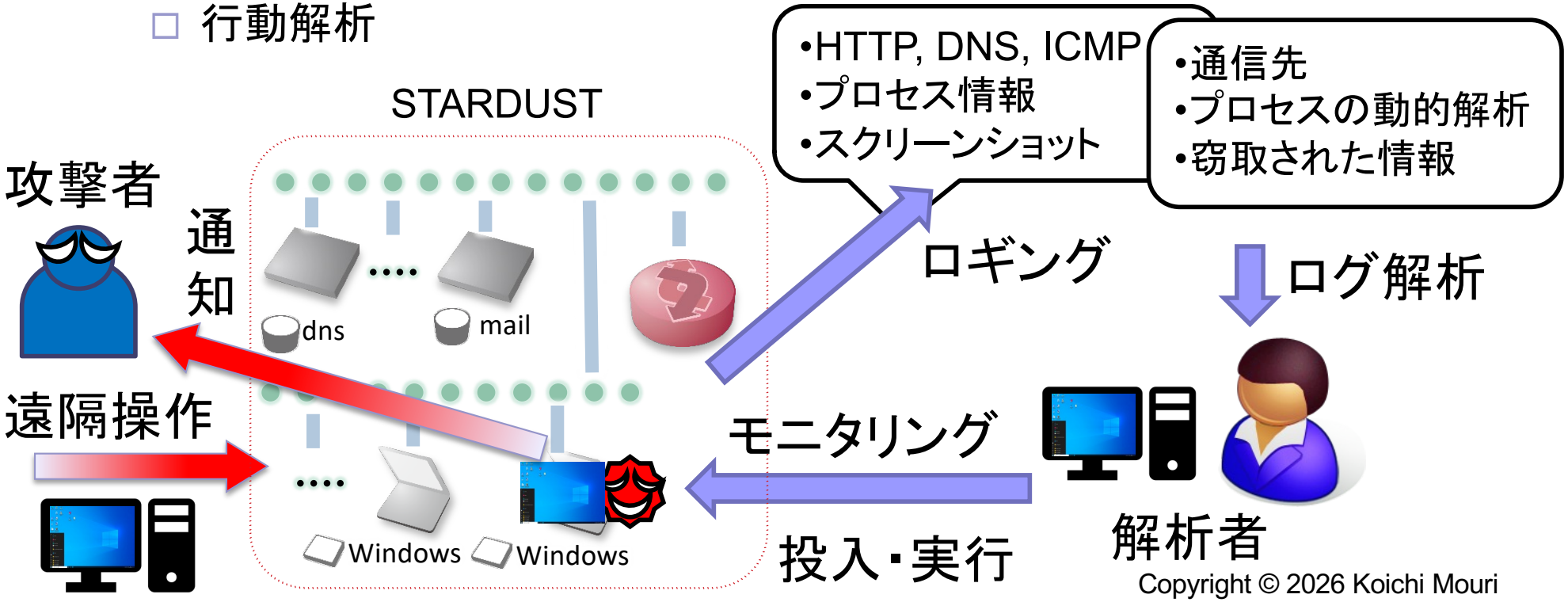
- マルウェアは亜種の発生が繰り返される
  - では、何が変わっているのだろうか？

- ハニーポットを設置し、マルウェア配布サーバを特定
- 配布サーバを継続的に監視、配布されるマルウェアの変化を追跡
- 静的解析・動的解析を用い、その変化を明らかにし、早期対策に結びつける



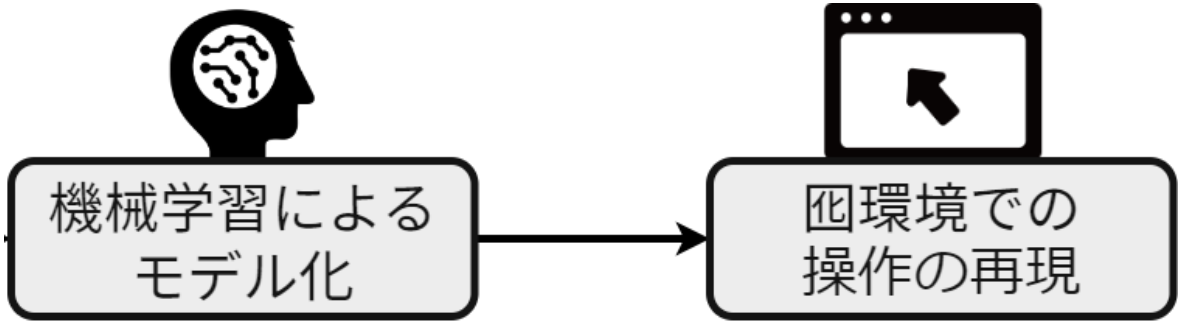
標的型攻撃の誘引と監視

- NICT（国立研究法人 情報通信研究機構）と共同研究で、ハニーネットSTARDUSTを利用し観測
  - RATなどのマルウェアを実際に実行し、攻撃者を誘引
  - 誘引できたら、その挙動を記録（STARDUST)
  - 行動解析



標的型誘引環境の構築

- 標的型攻撃による攻撃者の行動観測の困難さ。
  誘引したコンピュータの環境が行動に影響
  - デスクトップやフォルダに何があるのか
  - ブラウザの参照履歴はどうなっているか
  - メールのやりとりはどうなっているか
  - ユーザが今まさに操作しているように見せられるか
- これらの環境の模擬、および滞在時間の関連性調査
  - LLMを用いた、リアリティのある文書・メールなどの生成
  - ブラウザの参照履歴生成
  - ユーザのマウス操作・キーボード操作の模擬



セキュリティ情報融合基盤（DB）

- 主な情報源
  - ハニーポット　　無差別型攻撃通信
  - Haguregumo　　全ポート待ち受け型
  - AmpPot　　リフレクション攻撃
  - EXIST　　OSINT情報
  - NICTER　　ダークネット観測パケット
  - NIRVANA改　　セキュリティ機器のアラート
  - STARDUST　　標的型攻撃者の活動やC2通信
  - CHORUS　　配布サイトから配布されるマルウェア

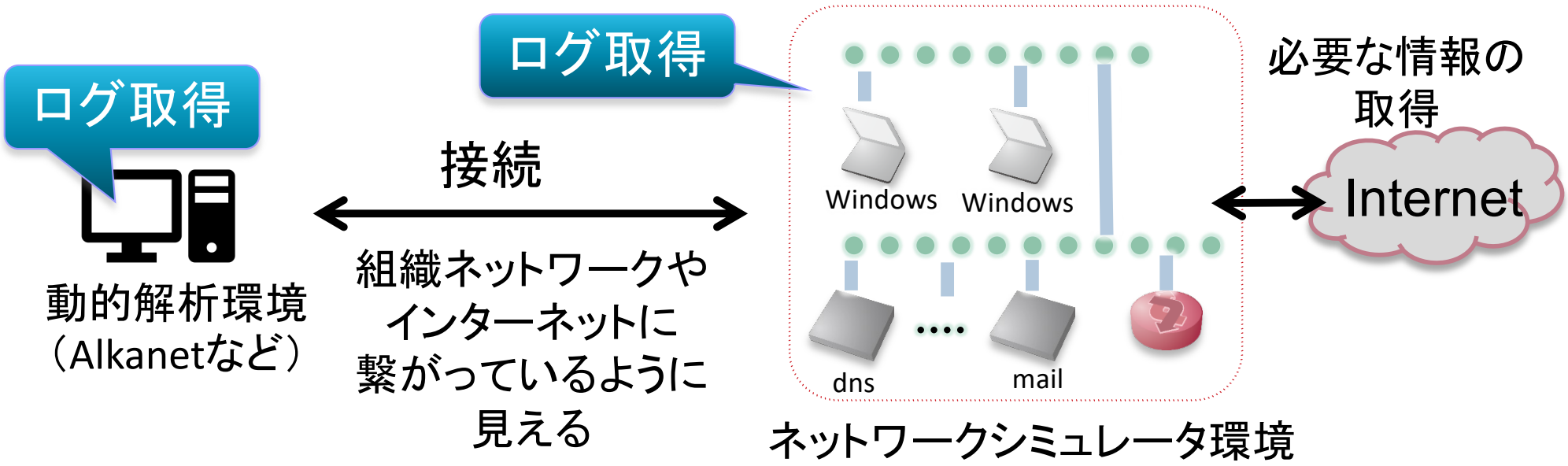
- CUREの持つ情報
  - IPアドレス、ドメイン名、ファイルハッシュ値、メールアドレス、キーワード、タグ
- これらのデータを関連性に基づいて結びつけ、攻撃者や攻撃状況の時系列変化の調査

Network

マルウェアとネットワークシミュレータ

- 動的解析では通信が重要・必要となるケースは多い
  - DNS、Web、GeoIP、C2サーバ、攻撃対象
- 本物のサーバと通信させるわけにも行かない
- 実験用の実機やVMの構築はコスト大

- ネットワークシミュレータにより、機能性，安全性，手軽さを実現



マルウェアの耐解析処理の逆用

- マルウェアには、解析されないようにする「耐解析」機能を持つものがある
  - マルウェアが解析されていると判断した場合、動作を停止する
- なので、逆に、解析環境と錯覚させれれば、マルウェア対策になる