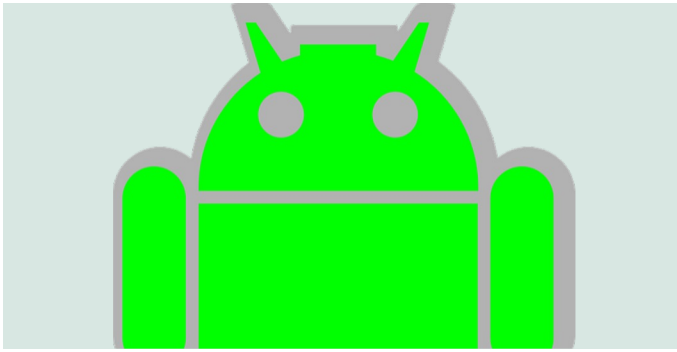


# 2023年度
# 毛利研究室　紹介

# 本日の流れ

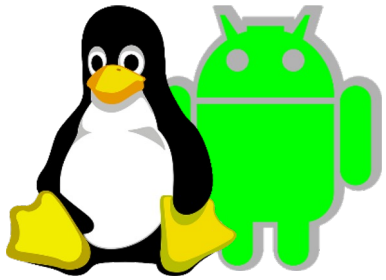
- 研究紹介
- 研究室情報紹介
- アンケートのお願い

# 研究分野



- システムソフトウェア
  - オペレーティングシステム
  - ハイパーバイザ・仮想計算機モニタなど仮想化技術
  - TEEなどCPU拡張機能，eBPF，コンパイラも範疇！
- コンピュータセキュリティ
  ＆　ネットワークセキュリティ

  ソフトウェアの仕組みや動作に基づくもの全て
  - マルウェア解析（動的解析・静的解析・ハニーポット）
  - ファームウェアの脆弱性調査
  - 標的型攻撃の侵入者行動解析と解析環境開発
  - ハニーポットによるIoTマルウェアの実態調査
  - 情報漏洩防止



# 研究グループの主なエリア2023



- Lavender
  - オペレーティングシステム
  - 仮想化技術
  - TEE，　eBPF
- Alkanet
  - Windowsの挙動観測・セキュリティ
  - マルウェア動的解析
  - ライブフォレンジックス
- Salvia/Network
  - OSINT
  - ネットワークセキュリティ
  - 標的型攻撃・IoTマルウェア関連
  - OSの信頼性向上

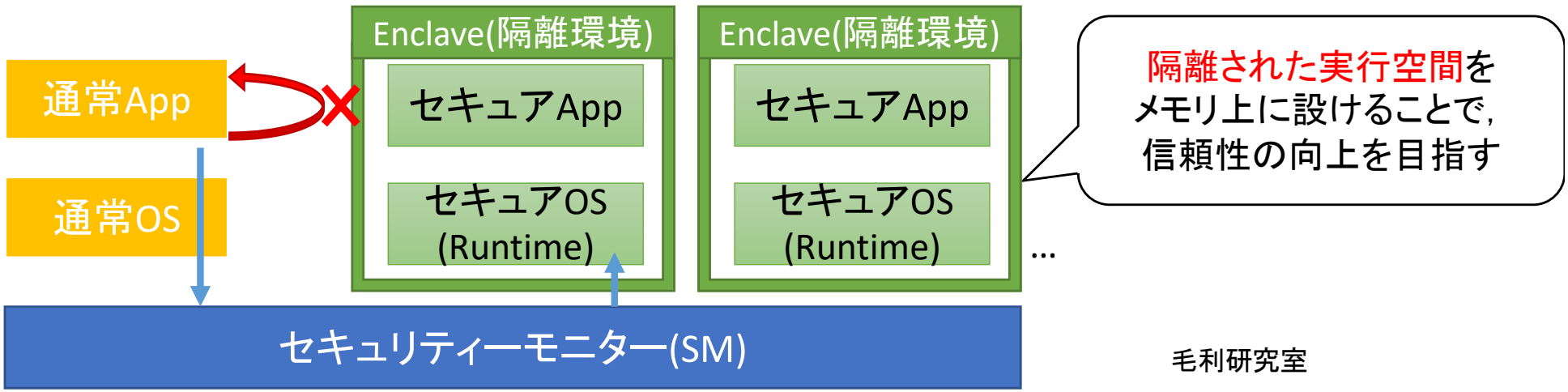
# Lavender

# IoT機器向け隔離実行基盤



- ハードウェアを用いたデータ保護手法の一種に，
  Trusted Execution Environment(TEE)技術がある
  - TEEは，メモリを保護することでデータの信頼性を向上させる
  - TEEはIntelやArmなどの各命令セットアーキテクチャ(ISA)ごとに設計されている
- RISC-V命令セットは仕様がオープンソースで拡張性が高い
  - 組み込み機器での広い利用が予測される

RISC-V版のTEEを用いて，
組み込み機器向けの高信頼な実行基盤を構築する

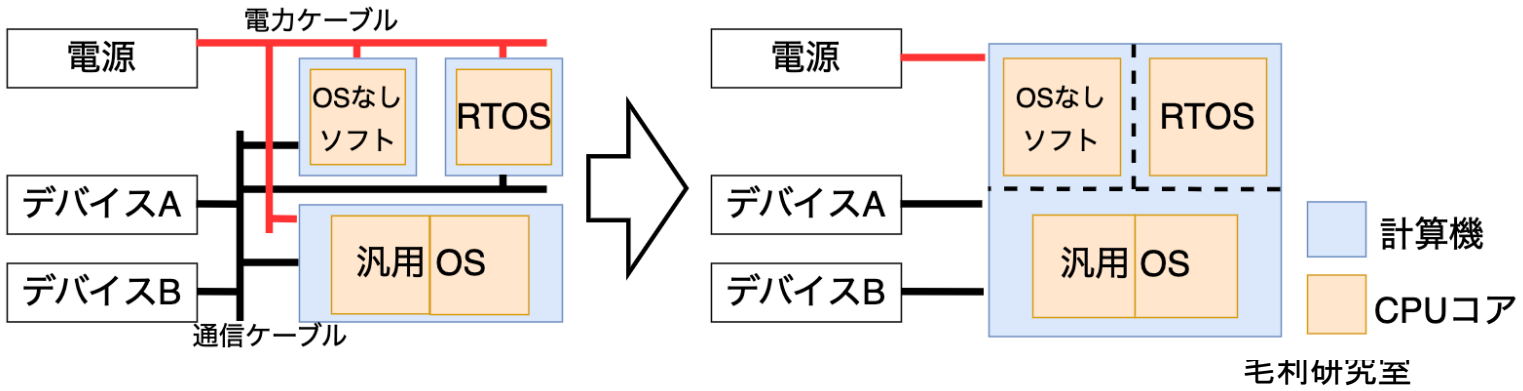


# 組込みシステム集約のための制御基盤



- 自動車等の組込みシステムで高性能化/多機能化が進んでい
  →機器/配線量の増加による内部スペース圧迫や重量化の問題
- プロセッサのマルチコア化が進んでいる
  →既存の組込みソフトでマルチコアを十分活かせていない現状

- マルチコアプロセッサ上で，既存の複数の組込みソフトを
  容易に集約可能とする基盤ソフトとして**誉**を開発している
  - マルチコアを活かすために，コアに依存しない柔軟なコア割り当てを実現
  - LPARでリアルタイム性を確保/LPARで実現できない機能は仮想化で実現

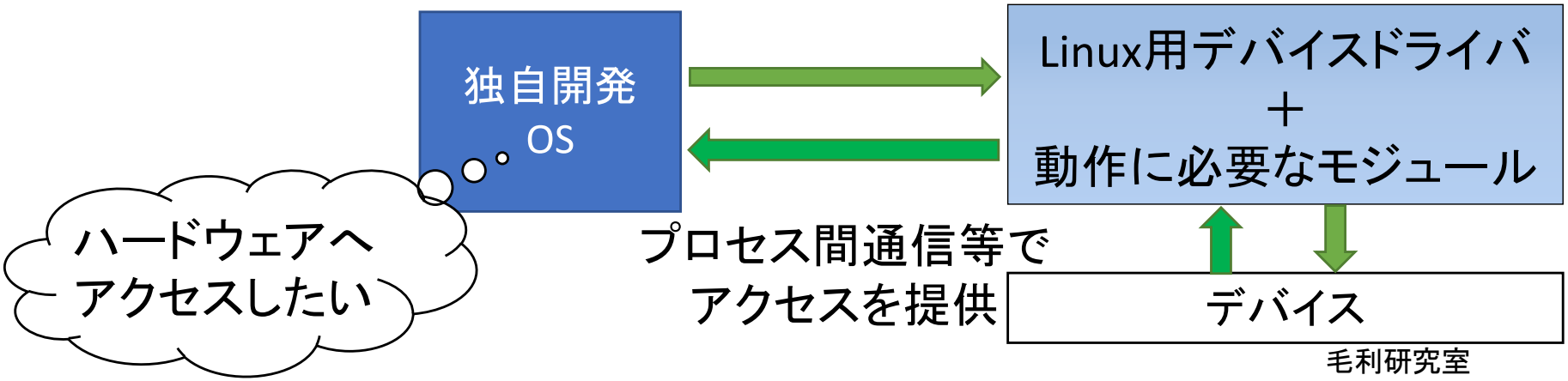


# Linuxデバイスドライバ向けUnikernel



- OSの独自開発での大きな問題点の一つはデバイスドライバ
  - デバイスドライバは，多種多様なデバイスに固有
  - デバイスのベンダが提供してくれるわけではない
  - バードウェアの仕様が公開されるとは限らない
  - 開発の手間，メンテナンスの手間が大きい

- Linuxでは広くデバイスドライバが提供されるので，それを活用できないか？
- Unikernelのコンセプトが活用できないか？

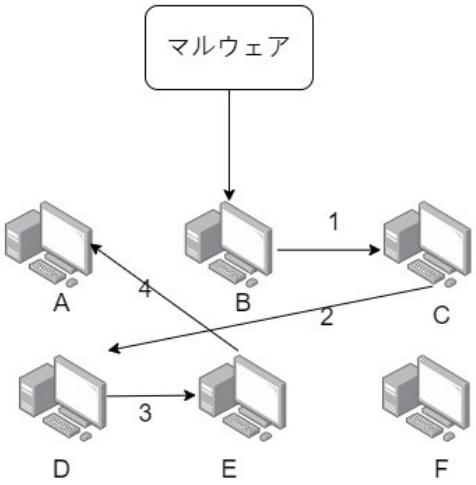


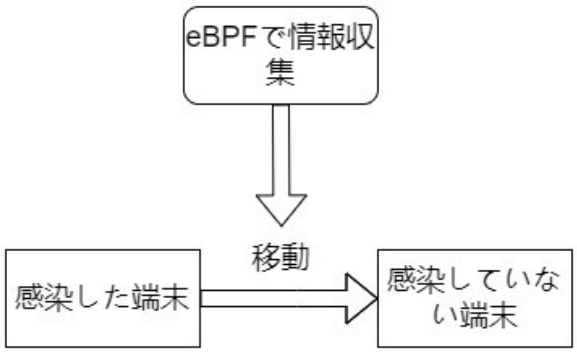
# マルウェア感染経路追跡



- 自動車などのECUが多数搭載された機器もサイバー攻撃の対象
- マルウェア感染時に全ECUを停止・再起動することは，
  運転機能を失うなどの危険が大きい
  - 感染したECU，およびその侵入経路となったECUのみに限って対処をしたい

- 通信イベント（システムコールの利用）を記録し，
  感染発覚時にはその感染経路を明らかにする機能が必要
  - 今回はOSのイベントを観測できるeBPFを活用して実現
  - socket, bind, listen, accept
  - connect
  - send, recv



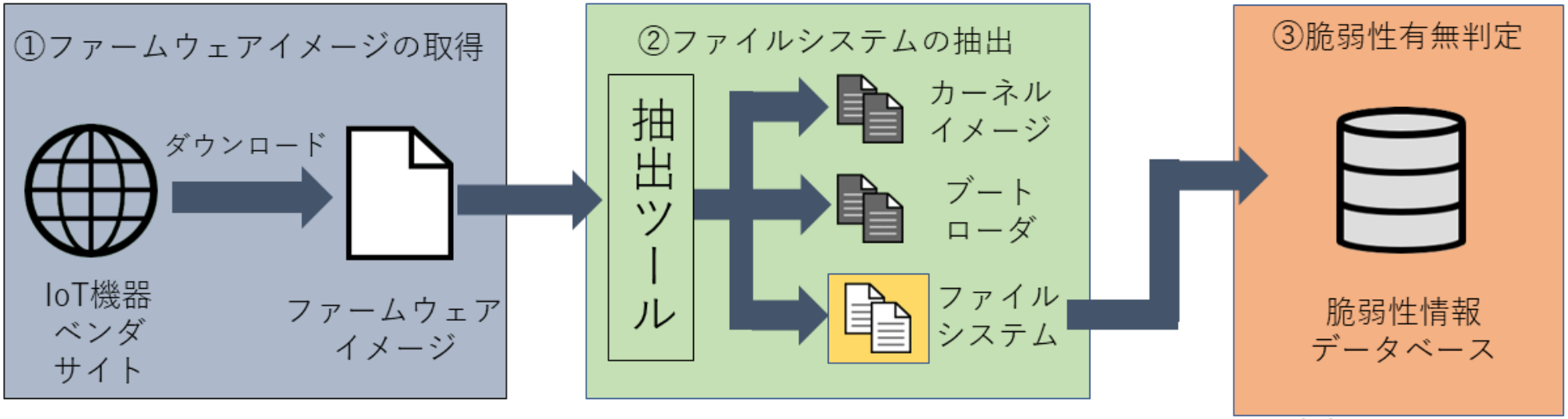



# ファームウェアの脆弱性評価



- IoT機器等のベンダは製品にOSS(Open Source Software)を積極的に活用
- OSSの脆弱性が発見されると各開発コミュニティが対策を実施
- 一方で，ベンダは自社製品ににその対策を適用しているのか？

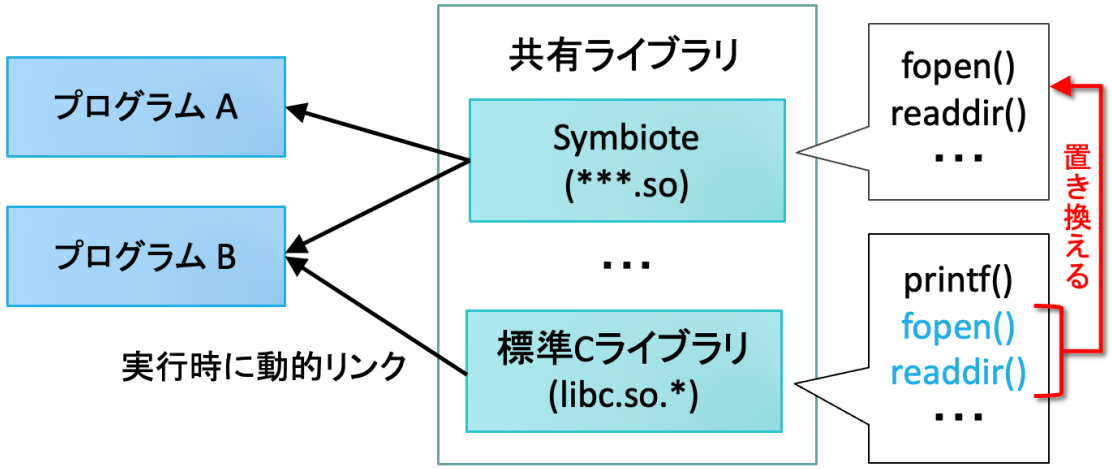
ファームウェア内のOSSについて，
既知の脆弱性に対し適切な対応がなされているか評価が必要



# 発見困難なマルウェアSymbioteの解析



- Linux上で動作するマルウェアは増加している.
  - サーバやルータ，IoTデバイス，スマートフォン
- 近年は高度な攻撃・潜伏機能を持つLinuxマルウェアが出現.
  特にSymbiote（2021年）は，極めて検出が困難とされる.
  - 悪意のある共有ライブラリを一般のプログラムにロード
  - 正当なプロセスの下で
    ファイルの隠蔽や
    認証情報の収集を行う.




動的解析によって，高度な潜伏機能を持つSymbioteの
挙動を明らかにし，検知・対策手法の発見を目指す

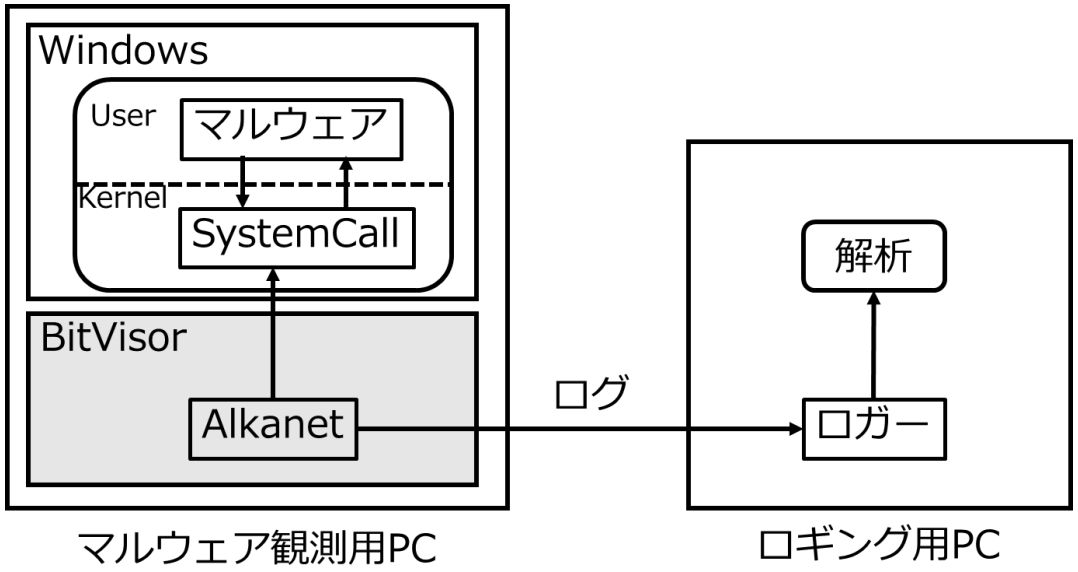
# Alkanet

# 動的解析環境 Alkanet



- マルウェアの数は亜種の登場により増加している
- マルウェアの手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



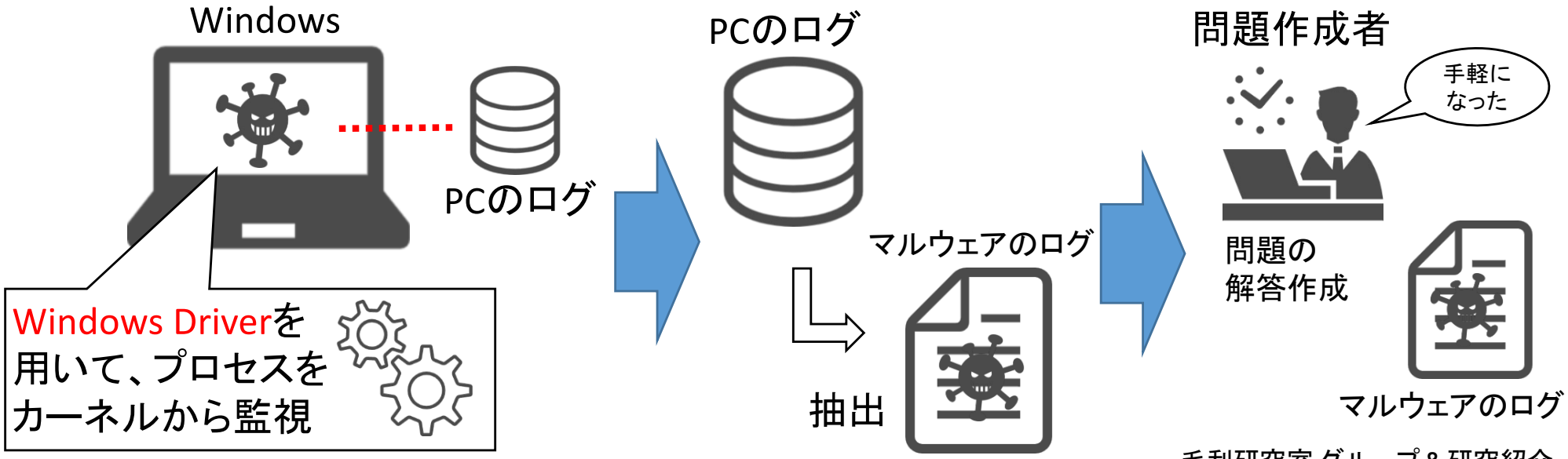

- **システムコールトレース**
- **システムコールの詳細情報取得**
  - 引数，発行元プロセスの取得
- **スタックトレース**
  - コードインジェクションの解析
  - システムコール発行までの関数呼び出しの追跡
- **スナップショット**
- **ログの送信**

# ログの生成元プロセス特定



- インシデント対応可能な人材育成のためのフォレンジックス演習
  - 各種のログファイルのエントリから，マルウェアの実行ファイルを特定する
- 演習のパターンが1種類だけだと解答を覚えるなど効果が出ない．一方で多数のパターンを作成しようとすると解答作成が手間…
- 解答作成者の支援を目的として解答作成の自動化を目指す

ログの出力過程を記録しログの生成元を自動特定する技術の確立



# RDMAによるライブフォレンジックス

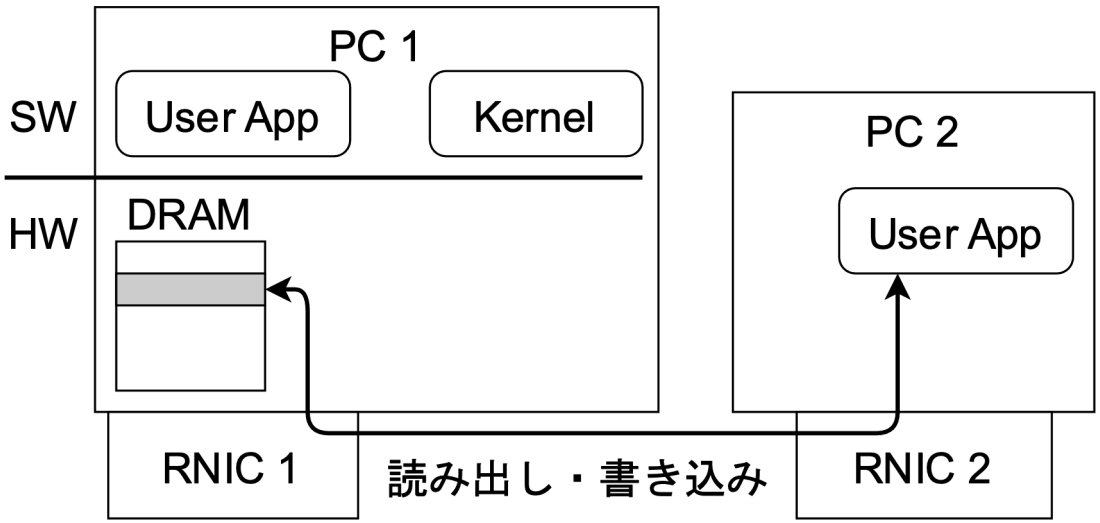


- RDMAでは，ネットワーク接続された
  別のコンピュータのメモリを読み書きできる
- 最大 100Gbps と高帯域幅で、信頼性も高い

⇩

**リモートマシンの実行環境を監視，自動複製など高信頼化を目指す**

RDMA の動作イメージ




RDMA NIC（RNIC）

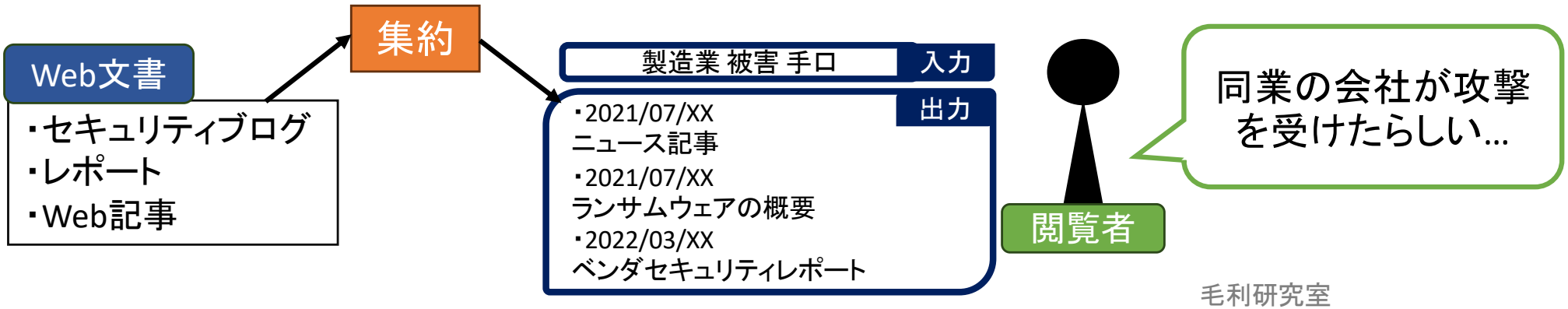
# Salvia Network

# ランサムウェア向けOSINT自動集約



- 大きな脅威となるランサムウェアの情報がWeb上に多く存在
  → **OSINT(Open-Source Intelligence)**
- 情報が遍在するため情報収集には複数文書の収集が必要
- Web上に散らばるOSINTを収集・集約し、
  脅威の防御に必要な情報を素早く得られるシステムが必要

ランサムウェア攻撃の対策考案・インシデント発生時の
効率的な情報収集に貢献する

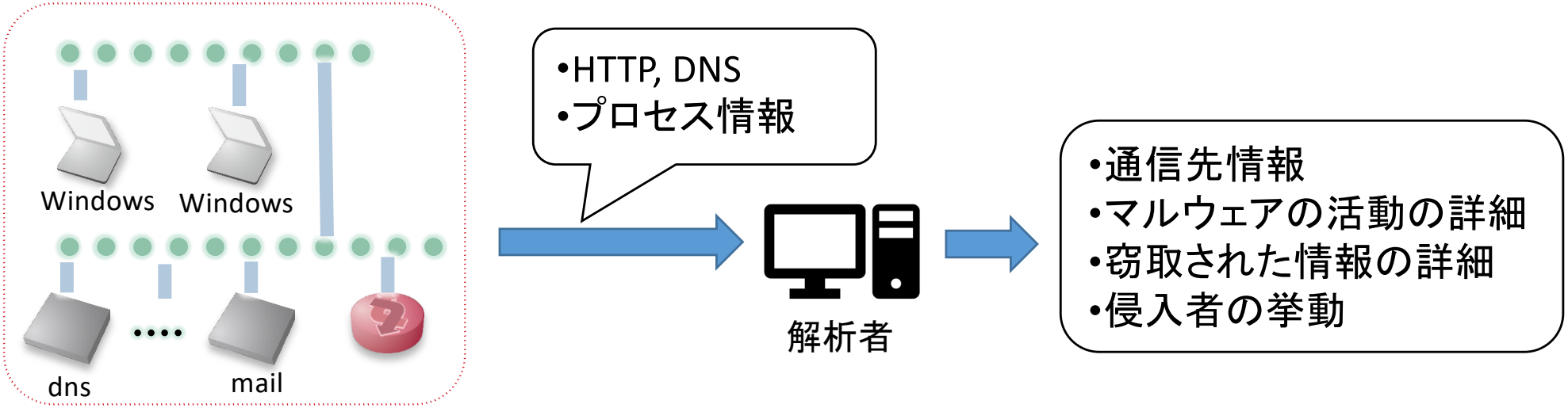


# 攻撃者誘引と攻撃者の挙動解析



- 組織を狙った標的型攻撃による被害が深刻になっている
- 攻撃の本質を知るには、マルウェアの解析と
  そのマルウェアを使う攻撃者の挙動観測が重要となる

- 組織を精巧に模したネットワーク環境でマルウェア挙動や
  攻撃者の挙動を解析する



# 自然な囮環境の実現



- 標的型攻撃の解析
  - 攻撃を解析するために，攻撃者を囮の環境へ誘引する
- ユーザーの操作を再現
  - 攻撃者が「囮用の環境」であると気付くと，攻撃を中断してしまう
  - 攻撃の中断を防ぐために，囮環境で「ユーザが実際に行うような操作」を再現する → **偽装を施す**
  - ユーザーの操作を再現するために，実際にユーザーのログを取り，そこから操作のモデルを作成する

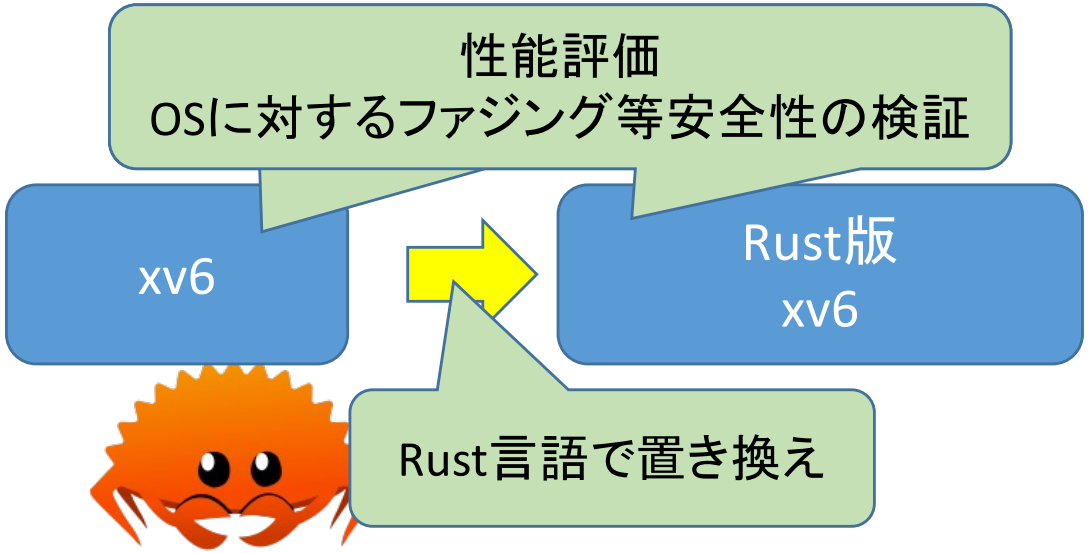
**研究の目標**

囮環境を偽装を目指して，ユーザの操作ログを取得する

# 低レイヤ層ソフト開発でのRust言語への置き換え



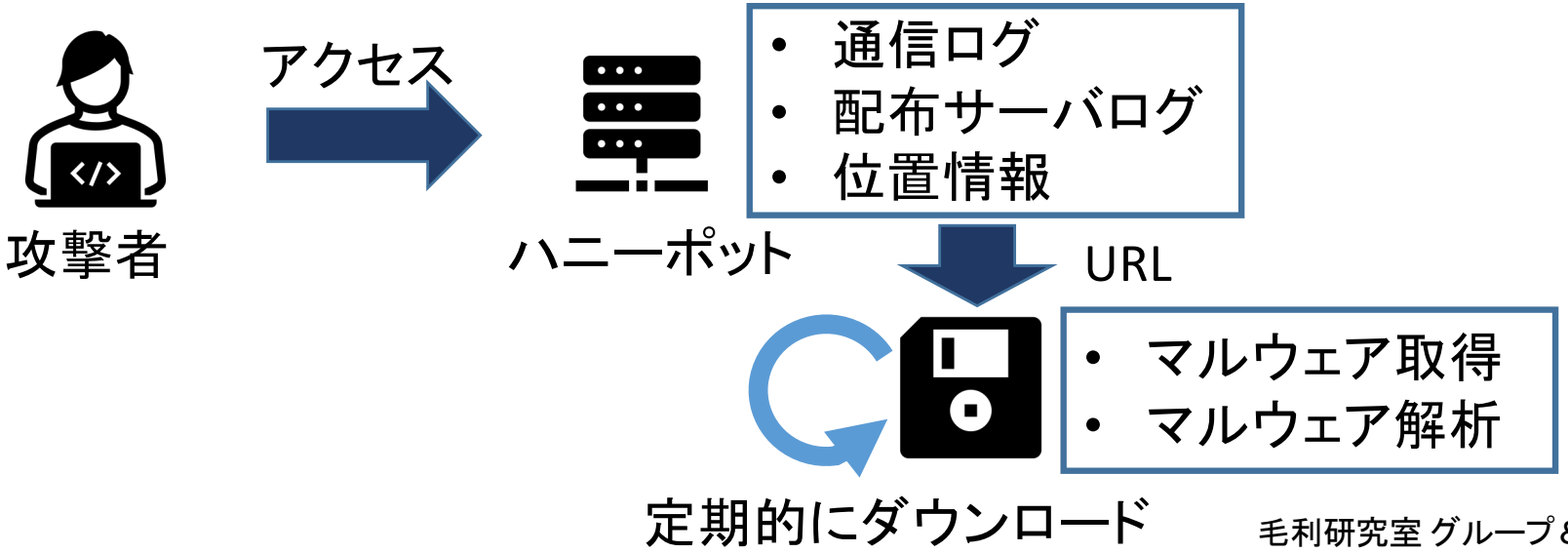
- Rust言語は高いメモリ安全性を持つ
  - 性能的にもC/C++言語と同等の性能を出すことできる
  - 並行性を効率的に取り扱える
- LinuxではRustでOSを書き換える流れも
- しかし，実際にどれくらい安全になると言えるのだろうか？？どう評価・証明していくべきか？



# IoTマルウェアの実態解析



- MiraiなどIoTマルウェアが流行っていましてね
  - 数多く配置され，十分な管理体制じゃなかったり，放置だったり
  - IoT機器を乗っ取って多方面に攻撃をするような状況
- IoTマルウェアと攻撃者の動向をなんとかつかんで応戦したい
  - ハニーポットを用いた攻撃の観測と，マルウェア配布サーバの監視
  - ダウンロードされるIoTマルウェアの取得の変化・進化を観測したい

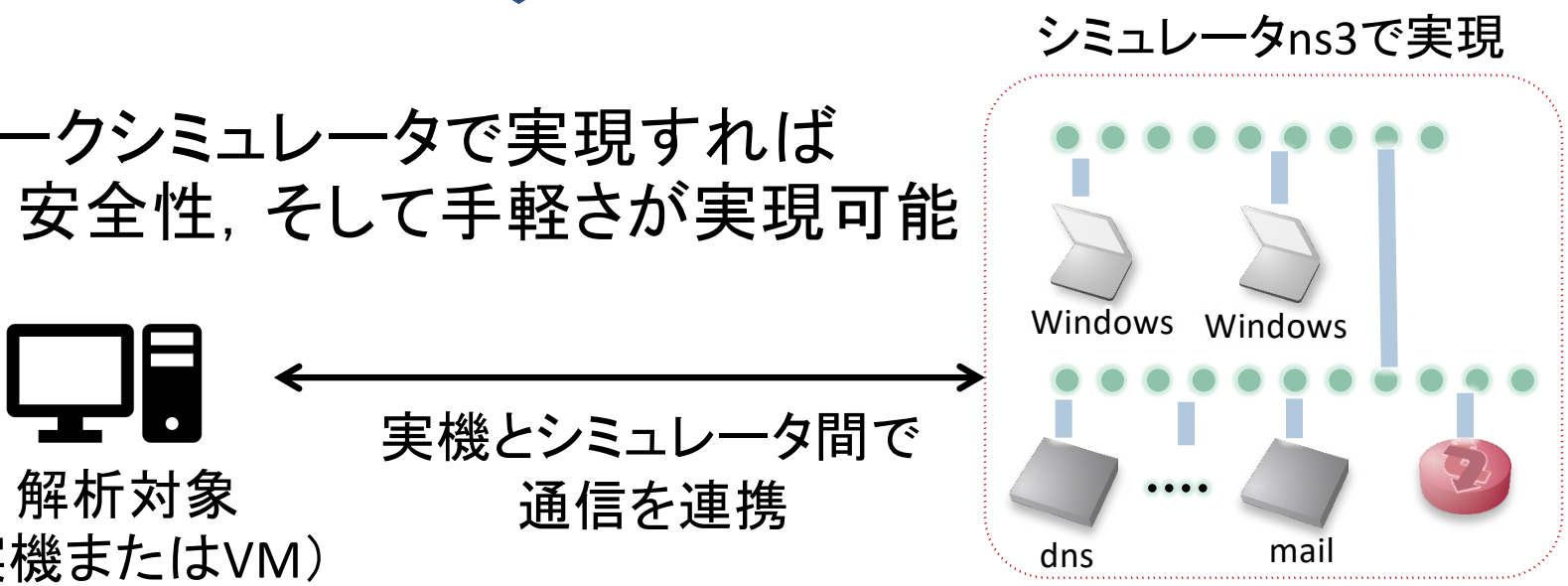


# サイバー攻撃観測用ネットワークシミュレータ



- マルウェアの動的解析をするときに，
  外部ホストとの通信が重要となるケースは多い
  - DNS（含・DDNS），Webサービス（含・GeoIP），C2サーバ，攻撃対象
- これらがないと攻撃の挙動が解析できない
  - 本物のサーバと通信させるわけにも行かない
  - といって，個別にPCを用意したり，VMをセットアップするのは大変手間とコストがかかる

- ネットワークシミュレータで実現すれば
  機能性，安全性，そして手軽さが実現可能



# 研究室メンバ

- 先生方＆スタッフ
  - 毛利 公一 教授
  - 客員研究員　瀧本 栄二（奈良女子大）
  - 客員研究員　竹久 達也
  - 客員研究員　津田 侑
  - 研究補助員　金城 聖
- 頼りになる先輩方
  - D3　　1人
  - M2　　5人
  - M1　　7人
  - 学部生　　8人（M0　3人＋1人）
  - 計21人

# 研究室のゼミ



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!

- グループゼミ
  - グループ毎に週1回開催
  - 進捗状況をミニプレゼン
  - グループメンバでディスカッション＆アドバイス

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！

- 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
  - 研究室全体で研究内容の共有＆ディスカッション

コミュニティが広がる！視野が広がる！
活動範囲が広がる！技術が深まる！
これぞ醍醐味！

- 共同研究ゼミ
  - 不定期開催
  - 企業・他大学と研究交流（プレゼン・ディスカッション）
  - 院生・大学院進学予定者など

# 企業・他大学との連携および成果

- 共同研究・外部資金等（本年度の予定を含む）

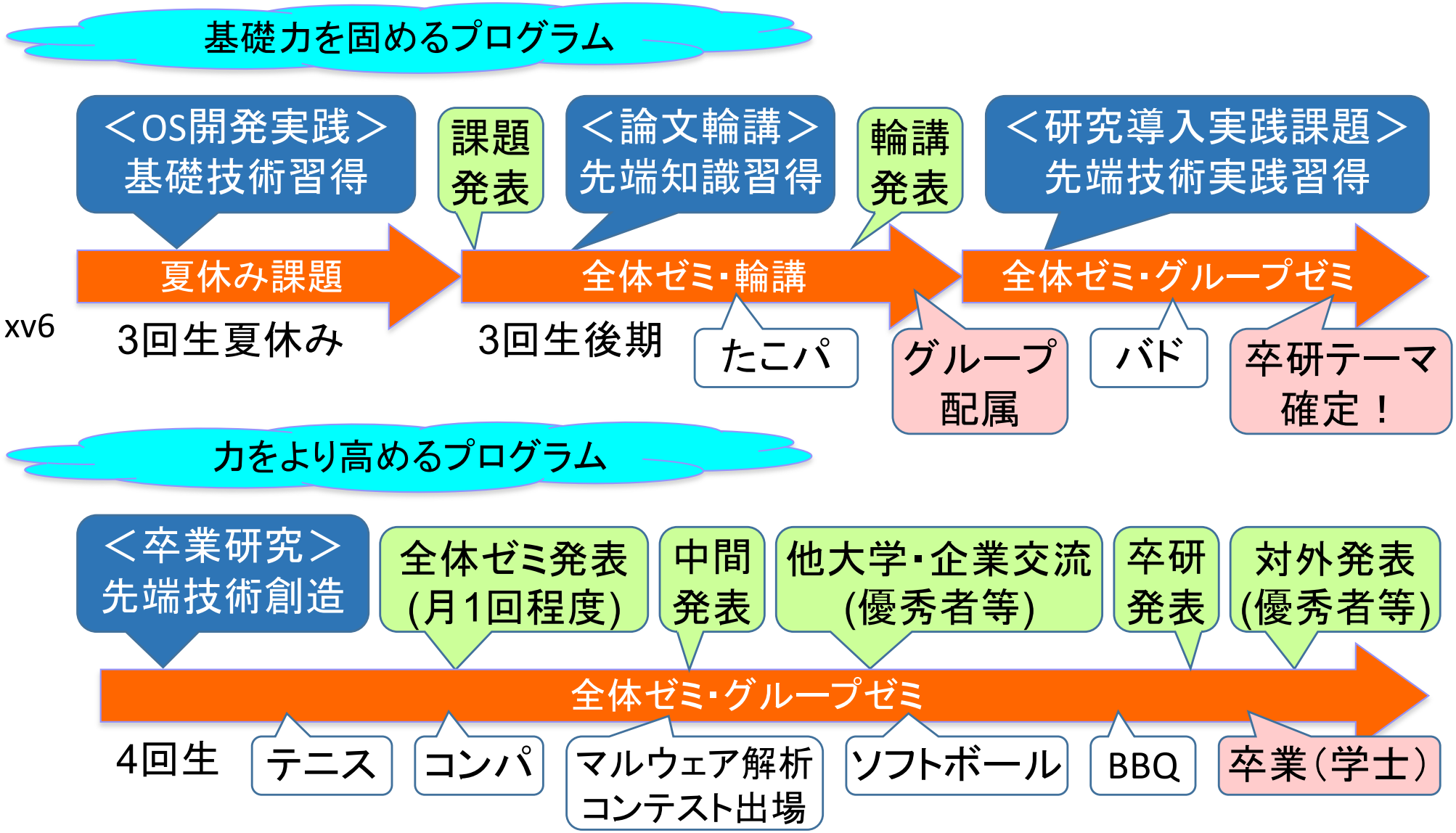
期待大きい！

  - 三菱電機①　組込みシステムとセキュリティ
  - 三菱電機②　仮想化と信頼性
  - 三菱電機③　信頼性向上技術・メモリフォレンジックス
  - アドソル日進　信頼性向上技術・Unikernel
  - 日本電気(NEC)　サイバー攻撃演習
  - 情報通信研究機構(NICT)　ダークネット観測，ハニーポット（STARDUST）
  - 名古屋工業大学　OS・仮想化・高信頼性システム
  - 奈良女子大学　ネットワーク・セキュリティ　・・・他

みんなも
世界と戦える！

- 対外発表（2017年度～）
  - 査読付きジャーナル論文 10件
  - 国際会議 9件（うち受賞2件）
  - 国内シンポジウム・研究会・全国大会 57件（うち受賞11件）

# 研究の階段を上るためのプログラム



# 卒業後の進路



- 大学院博士課程修了
  - NTT　セキュアプラットホーム研究所
  - トヨタ自動車
- 大学院修士課程修了
  - KDDI，IIJ，ケイ・オプティコム
  - NTT（サイバースペース研究所），NTTコミュニケーションズ，NTT東
  - 東芝，三菱電機，NEC，船井電機，日本IBM
  - 大和総研，日本総研，野村総研，オージス総研
  - 任天堂，三菱重工業，トレンドマイクロ，アドソル日進　他
- 学部卒
  - 進学
  - 三菱重工業，日本IBM，日立製作所，富士通，大日本印刷
  - DeNA，カプコン，任天堂，ぐるなび，ヤフー
  - 日立ソリューションズ，三菱電機コントロールソフトウェア
  - NECシステムテクノロジー，NTTデータフロンティア　　他

ただし，会社名が同じでも
キャリアパスは異なります

# スケジュール

○：研究室・研究紹介 with 教員　　☆：先輩相談・交流会

ゼミも全部公開！（全体ゼミCC102，他：システムソフトウェア研究室）

OH：オフィスアワー（アポなしで教員と何かお話しできる）

| | 5(月) | 6(火) | 7(水) | 8(木) | 9(金) | 12(月) | 13(火) | 14(水) |
|---|---|---|---|---|---|---|---|---|
| 1コマ（9:00～） | | | | | | | | |
| 2コマ（10:40～） | Nゼミ | | | Lゼミ | | Nゼミ | | |
| 昼休み | | | OH | OH | OH | OH | | OH |
| 3コマ（13:00～） | | 全体ゼミ | | | | | 全体ゼミ | |
| 4コマ（14:40～） | | Aゼミ | Sゼミ | | | | Aゼミ | 全体ゼミ |
| 5コマ（16:20～） | ○ | ☆ | ○ | | | ☆ | | Sゼミ |
| 6コマ（18:00～） | ☆ | ○ | ☆ | ○ | ○ | タコパ | | |


http://www.asl.cs.ritsumei.ac.jp/

# URLの案内

- 研究室Webトップページ
  - https://www.asl.cs.ritsumei.ac.jp/

- 配属案内ページ・本資料・スケジュール
  - https://bit.ly/2XK64C1

# アンケートのお願い

- 3回生以上（研究室配属の対象）の方
  - 記名式で，進路予定・感想等を記入
  - 研究室配属の希望者が定員を超えた場合に参考にしますので必ず！
- 1・2回生の方
  - 匿名で，感想等を記入
  - 人数カウントのために，感想等がなくても（空欄のままでも）協力をお願いします．

いずれもこちらへ！　→　https://bit.ly/3pmV21C