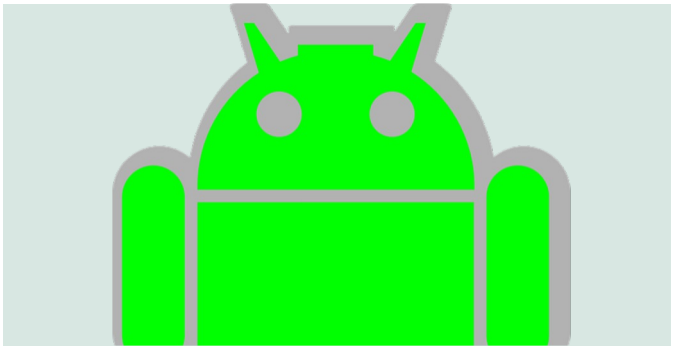


2024年度
毛利研究室　紹介

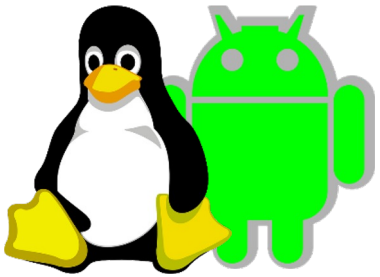
本日の流れ

- 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，Unikernel，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）
  - マルウェアの解析システム
  - ファームウェアの脆弱性対策
  - 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



研究グループの主なエリア2024

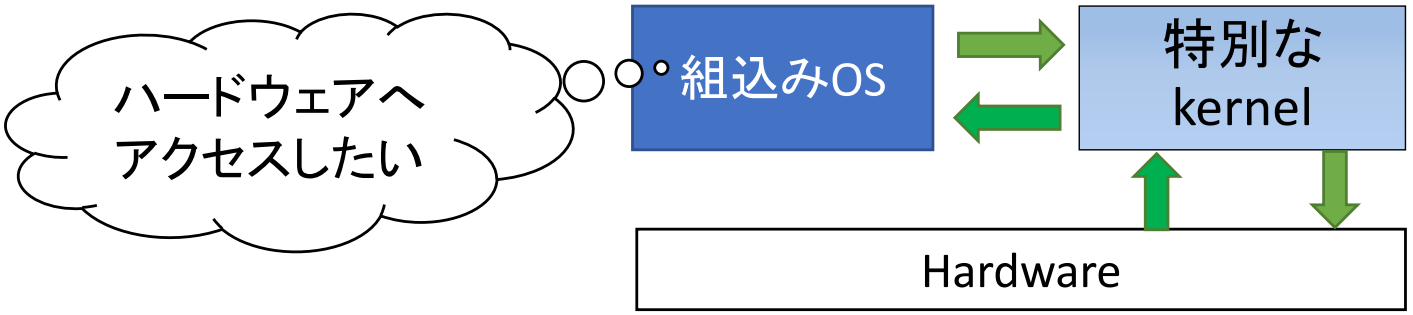
- Lavender
  - オペレーティングシステム
  - 仮想化技術
  - TEE，　eBPF
- Alkanet
  - Windowsの挙動観測・セキュリティ
  - マルウェア動的解析
  - ライブフォレンジックス
- Salvia
  - ネットワークセキュリティ
  - OSINTの集約
  - 標的型攻撃・IoTマルウェア関連
- Network
  - マルウェア動的解析環境
  - 耐解析機能を逆用したマルウェア対策

Lavender

組込みOSのための既存のデバイスドライバの機能のみを持つkernelの開発

- 組込みOSのためのデバイスドライバの開発は多くの時間と労力を要する
  - デバイスドライバの開発にはデバイスの知識が必要
  - 日々のメンテナンスが必要

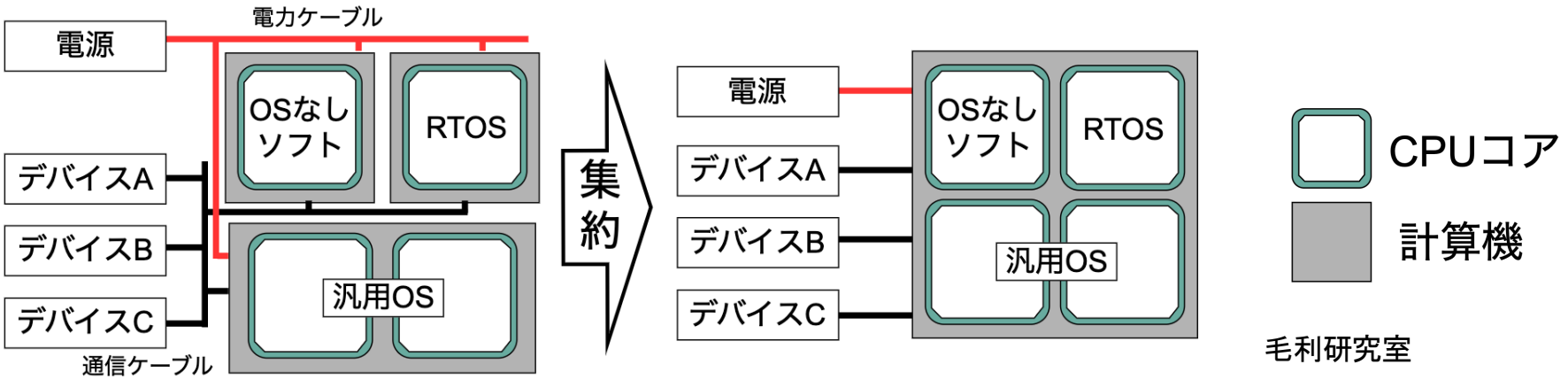
- Linuxデバイスドライバのような多くの開発者によって開発されている既存のデバイスドライバを組込みOSから利用できる特別なkernelの開発を行っている



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における高性能化/多機能化
  →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
- 組込み向けプロセッサのマルチコア化
  →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**」を研究開発
  - 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
  - 基本はLPARでリアルタイム性を確保/それ以外の一部機能は準仮想化



システムソフトウェアにおけるRustの安全性調査

- Rust言語は高いメモリ安全性を持つ
  - 性能的はC/C++言語と同等
- RustでOSを書き換える流れがある
  - 低レイヤのメモリ操作にはメモリ安全性がチェックされない unsafeコードを記述する必要がある
- unsafeで記述されたコードの安全性は？

unsafeなコードを安全に記述するための条件を明らかにする

安全要件は？

```
#[no_mangle]
fn __rust_alloc(size: usize, _align: usize) -> *mut u8 {
        unsafe { bindings::krealloc(core::ptr::null(), size, bindings::GFP_KERNEL) as *mut u8 }
}
```

linux/rust/kernel/allocator.rs

RISC-V上でRTOSと汎用OSを動作させるハイパーバイザ

- 組込み機器で要求される構成が複雑化
  - 単一プロセッサ上でRTOSと汎用OSを複数実行
  - 柔軟な構成変更
- RISC-V
  - オープンなCPUアーキテクチャ
    - ライセンス料を支払わずに自由に利用, 機能拡張が可能

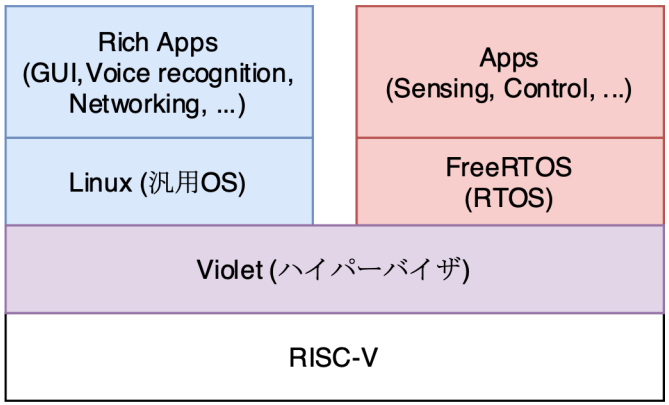
  → 組込みシステムで普及してきている

RISC-VではRTOSと汎用OSの同時実行と柔軟な構成変更が可能な手法が存在しない

RISC-V上でのRTOSと汎用OSの同時実行をハイパーバイザによって実現

課題

- リアルタイム性の保証
  - 仮想化オーバヘッド
    - RISC-V特有の要因
    - 他のアーキテクチャと共通の要因

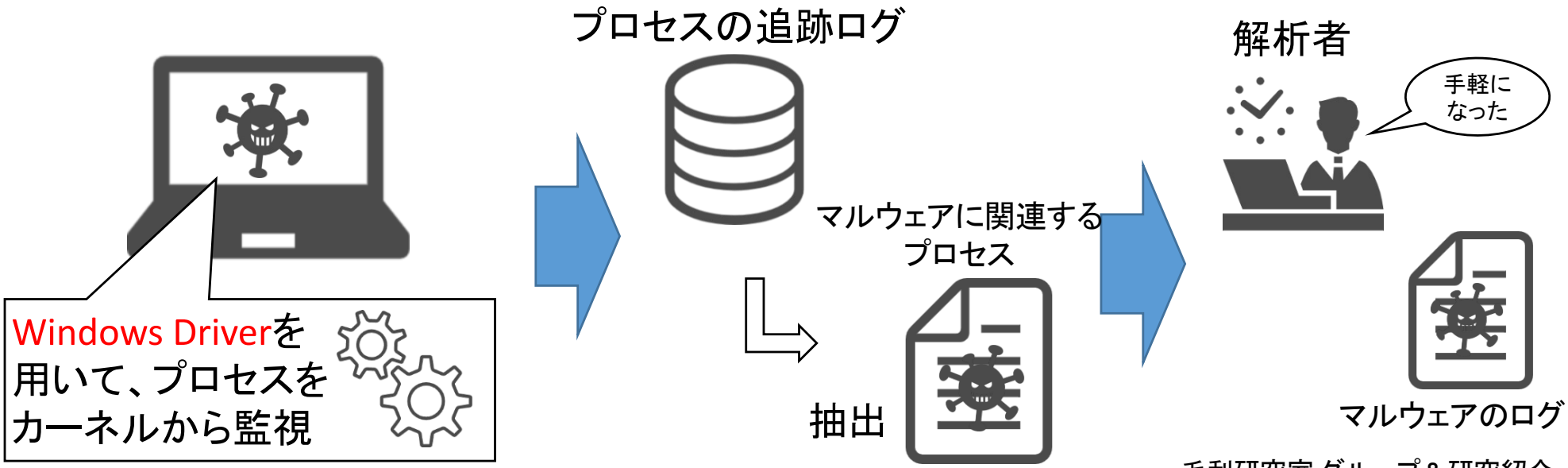


Alkanet

マルウェアのプロセス追跡

- マルウェアによるインシデントが発生！ログから影響範囲を特定する必要あり！
- ログがたくさんある中でどのプロセスがマルウェアと関係するかわからない…
- マルウェアが経由したプロセスの情報が欲しい！

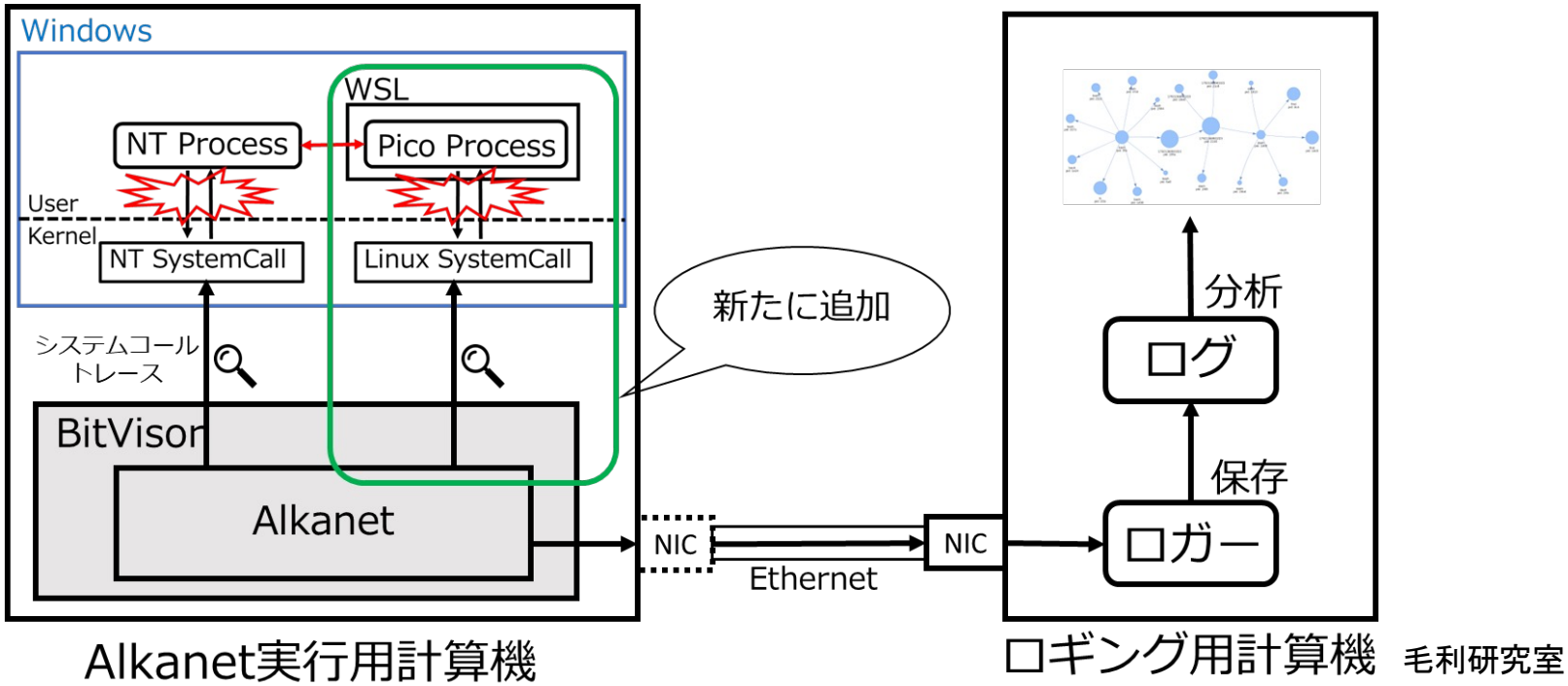
プロセスの動作を実行時に記録することで、
マルウェアが経由したプロセスを容易に特定



WSL1の動的解析

- WSLを使用することでWindows上でLinux環境を利用できる
- WSL上ではマルウェアも実行可能
- WSL上で動作するマルウェアを動的解析可能なシステムはない

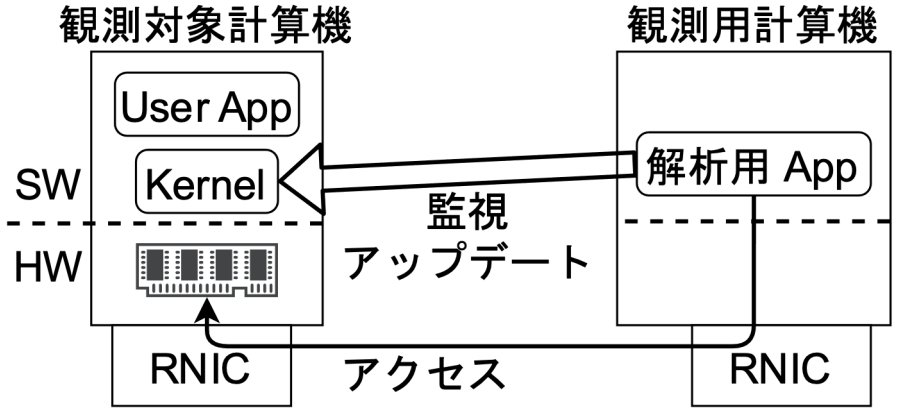
WSL1上で動作するマルウェアを動的解析する



RDMA の信頼性への貢献

- 信頼性・可用性を高めるために、様々な技術が開発されてきた
  - プロセスの状態を監視して、怪しいものを発見
  - システムを止めないで、アップデートを実行
- 仮想化ソフトウェアを使った方法が一般的
  - 仮想化ソフトの規模が大きくなり、バグが増えるリスクが上昇
  - 仮想化ソフトで処理をしている間、システムは停止する
- RDMA という技術を利用することで、遠隔からメモリを読み書きできる

RDMA を用いた、信頼性・可用性を高める手法を提案する



RDMA に利用するハードウェア (RNIC)

Salvia

WannaCryランサムウェア攻撃の実態調査

- 2017年に流行したWannaCry攻撃は現在も一定に観測されている
  - SMBプロトコル(ファイル共有など)の脆弱性を利用した攻撃
  - このランサムウェアが未だに使われているのはなぜか？
    - どういう意図があるのか？

- 実際のWannaCry攻撃を解析し，攻撃パターンを明らかにする
  - ハニーポットを用いた攻撃の観測
  - ダウンロードされるマルウェアや攻撃者情報の取得
  - どのような攻撃者からどのようなマルウェアが送られてくるのか？
    - 何か関連はあるか？
  - マルウェアが送り込まれる手段は共通しているか？

マルウェアの鮮度と攻撃者の挙動の関連分析

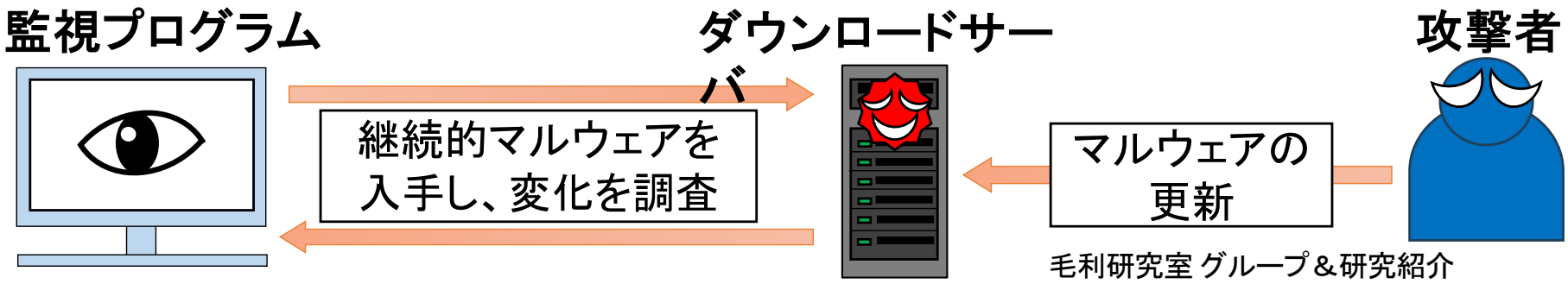
- マルウェア解析者の悩み・・・
  - マルウェアを動的解析しても，必ず攻撃者が攻撃してくれるとは限らない
  - 攻撃に関する知見が溜まらない
- 攻撃者の挙動を観測しやすいマルウェアの特徴はないか
  - 新しいマルウェアならば解析に成功する可能性が上がるのでは？

組織のネットワーク環境を精巧に模した解析基盤

IoTマルウェアの変遷調査

- IoTマルウェアの中には、ソースコードが公開され、多くの亜種が生み出されているものがある
- 直近に公表された脆弱性を使用する亜種も発見されており、状況に合わせてマルウェアも変化していくことが推測できる

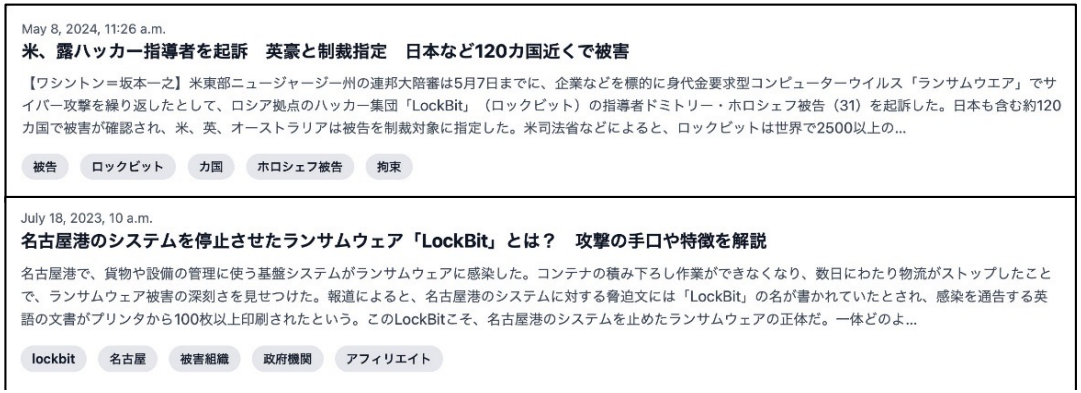
マルウェアの配布元であるダウンロードサーバを継続的に監視し、マルウェアにどのような変化が起こるか調査する



OSINT収集システムにおける検索精度向上

- メディアなどが投稿するセキュリティに関連した記事(OSINT)を集め，Webアプリ内で検索をすることでサイバー攻撃対策に役立てることができる
- しかし，異表記(DDoS攻撃と分散型サービス拒否攻撃など)が存在することにより，検索の精度が低下してしまう

定期的に更新できる異表記辞書を自動的に作成し，検索に利用し，精度向上を図る

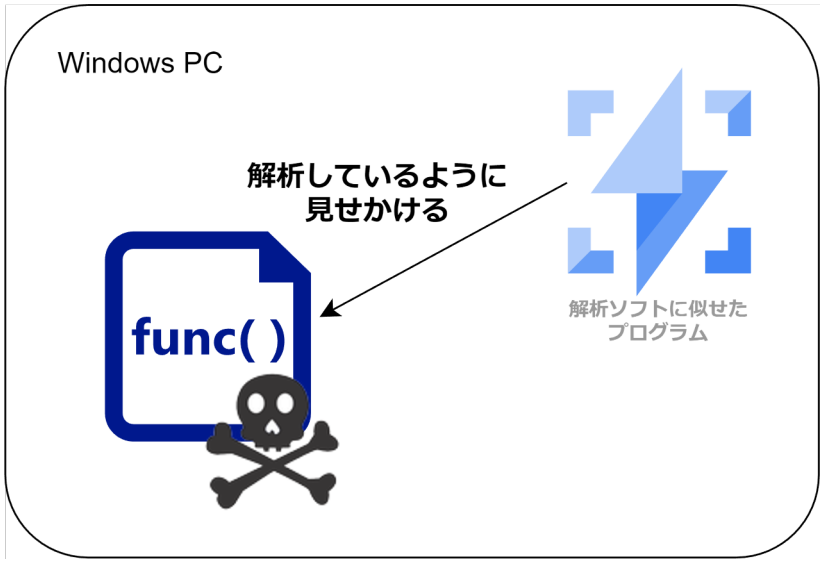


ロックビットと
lockbitを同じタグ
にしたい!!

Network

マルウェアの耐解析処理における逆用

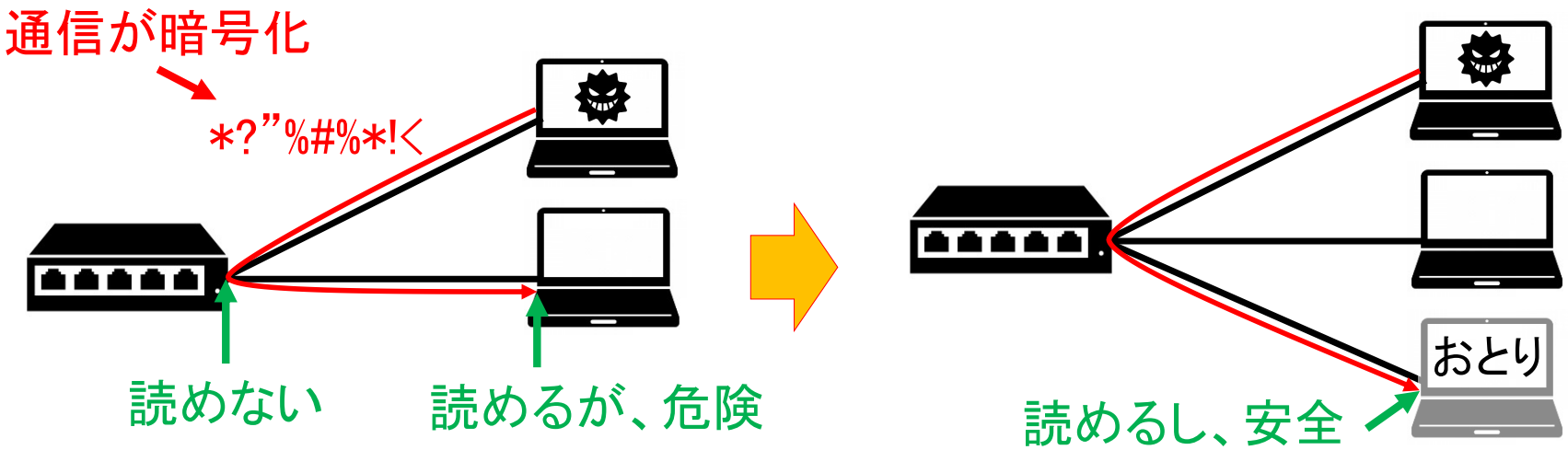
- 一部のマルウェアには、マルウェア解析から守る耐解析処理と呼ばれる処理が実装されている
- マルウェアが解析されていると判断した場合
  - マルウェアとしての動作を停止
  - 自身の動作を停止



解析環境であるかのようにマルウェアをだますことが出来れば、マルウェアの動作を抑止できる

ネットワークに潜む悪意のある通信の発見

- 企業など、組織のネットワークに侵入した攻撃者は、同じネットワーク内の他の機器にも侵入しようとする
- 通信経路上で、悪意のある通信を検知したいが、暗号化されているなど、判別が難しい場合がある



おとりとなるホストが攻撃元と通信することで、悪意のある通信を発見できるのではないか

研究室メンバ

- 先生方＆スタッフ
  - 教授　毛利 公一
  - 客員准教授　瀧本 栄二（奈良女子大）
  - 客員研究員　竹久 達也（㈱ニッシン）
  - 客員研究員　津田　侑（Turnt Up Technologies㈱）
  - 客員研究員　芝　公仁（龍谷大）
  - 研究補助員　金城 聖

- 頼りになる先輩方
  - D3　1人
  - M2　7人（進学予定1名）
  - M1　4人
  - 学部生　8人（進学予定5名）

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

  ※ 研究テーマは個人毎です。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・規模等で柔軟に変化します

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！
技術が深まる！これぞ醍醐味！

- 共同研究ゼミ
  - 企業・他大学と研究交流（プレゼン・ディスカッション）

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）

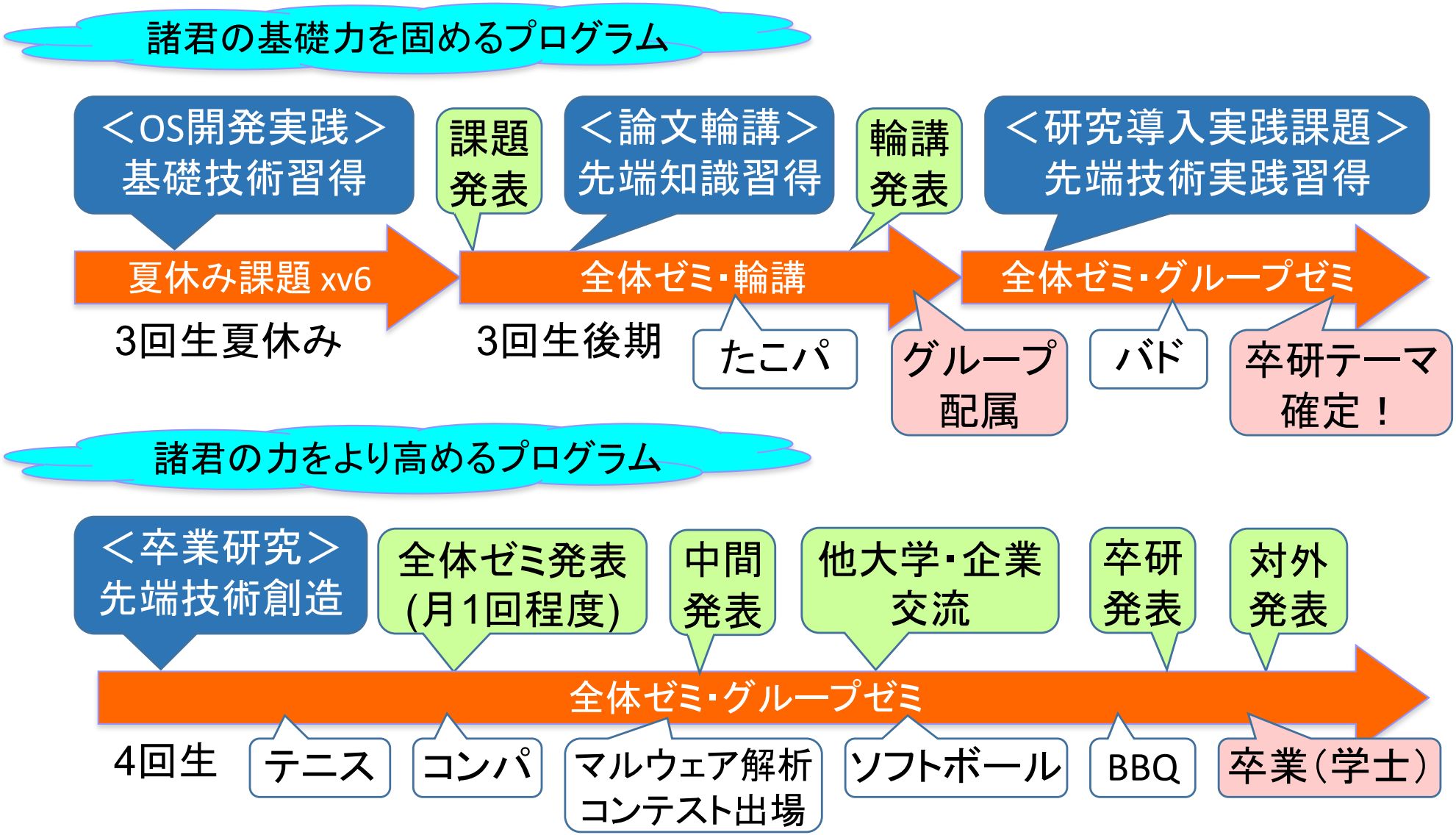
期待大きい！

  - 三菱電機①　組込みシステムにおけるセキュリティ
  - 三菱電機②　レジリエント（回復力のある）な組込みシステム
  - 三菱電機③　最新ハードウェアの信頼性技術への応用
  - 三菱電機④　RISC-Vと仮想化技術
  - アドソル日進　Rustによる信頼性向上技術・Unikernel
  - 日本電気(NEC)　サイバー攻撃演習のためのログ収集
  - 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　・・・他

みんなも
世界と戦える！

- 対外発表（2019年度～）
  - 査読付きジャーナル論文 6件
  - 国際会議 5件（うち受賞2件）
  - 国内シンポジウム・研究会・全国大会 51件（うち受賞8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（研究所），NTTコミュニケーションズ，NTT東，NTT西
  - 東芝，三菱電機，NEC，船井電機，日本IBM，三菱重工業
  - 大和総研，日本総研，野村総研，オージス総研，トレンドマイクロ
  - 任天堂，ディンプス，コーエーテクモホールディングス　他
- 学部卒
  - 進学
  - 日本IBM，日立製作所，富士通，三菱重工業，大日本印刷
  - 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
  - 野村総研，キャップジェミニ，FFRIセキュリティ
  - DeNA，カプコン，任天堂，ぐるなび，ヤフー　他

院卒と学部卒では、会社名が同じでも、キャリアパスが異なります

スケジュール

「我こそは」と思う者集まれ！

○ 研究室・研究紹介 with 教員　　☆ 先輩相談・交流会

ゼミも全部公開！

OH オフィスアワー（アポなしで教員と何かお話しできる）

	3(月)	4(火)	5(水)	6(木)	7(金)	10(月)	11(火)	12(水)
1コマ（9:00～）								
2コマ（10:40～）			★	Nゼミ				
昼休み	OH		OH	OH	OH		OH	
3コマ（13:00～）			全体ゼミ	Lゼミ				全体ゼミ
4コマ（14:40～）		Aゼミ					Aゼミ	
5コマ（16:20～）	全体ゼミ	○	Sゼミ	○	○	全体ゼミ	★	Sゼミ
6コマ（18:00～）	○	★	○	★	★	★		

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/
  - 先輩の卒論タイトル一覧、修論タイトル一覧あります
  - 対外発表のタイトルや受賞一覧もあります
- 配属案内ページ・本資料・スケジュール
  - https://www.asl.cs.ritsumei.ac.jp/研究室配属について

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．