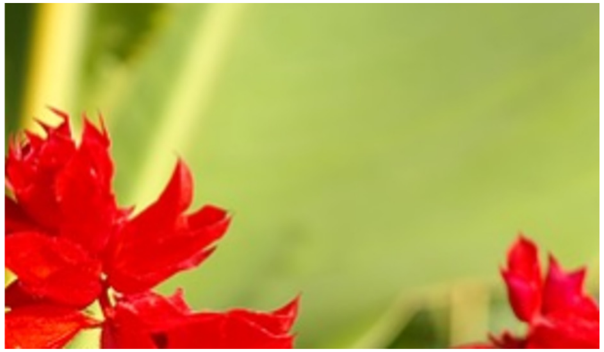
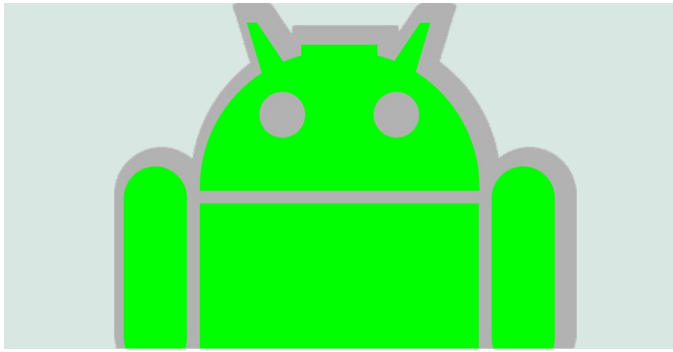




2022年度
毛利研究室　紹介

本日の流れ

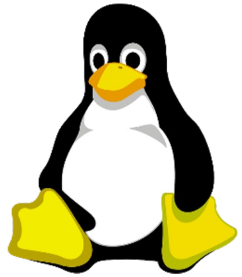
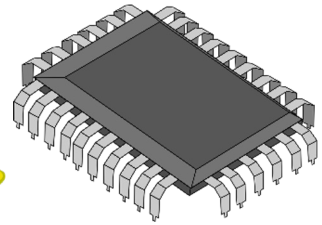
- 研究紹介
- 研究室情報紹介
- アンケートのお願い

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
  - 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2022

- Lavender
  - オペレーティングシステム
  - 仮想化技術
  - TEE
- Salvia
  - ネットワークセキュリティ
  - 標的型攻撃系セキュリティ
- Alkanet
  - WindowsやLinuxのセキュリティ
  - マルウェア解析

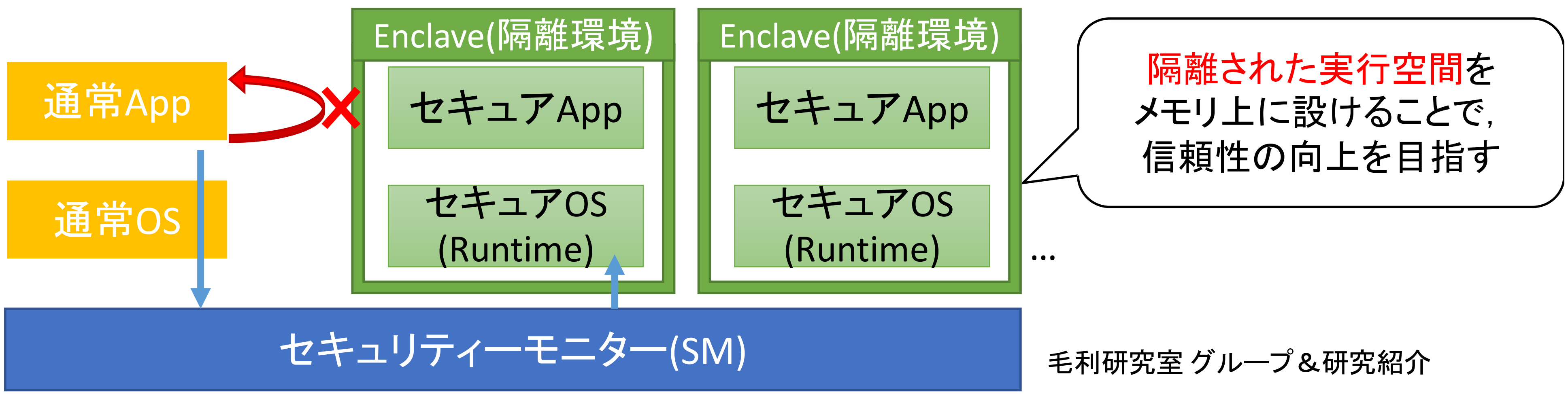


Lavender

組込み機器向けの隔離実行環境の構築

- ハードウェアを用いた実行環境保護手法の一種に，Trusted Execution Environment(TEE)技術がある
  - ➢ TEEは，メモリを保護することで実行環境の安全性を向上させる
  - ➢ Intel SGXやArm Trustzoneなどアーキテクチャ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 Keystoneを用いて，組み込み機器向けの高信頼な実行環境を構築する



IoT機器のセキュリティ向上

IoT機器の
ボード例

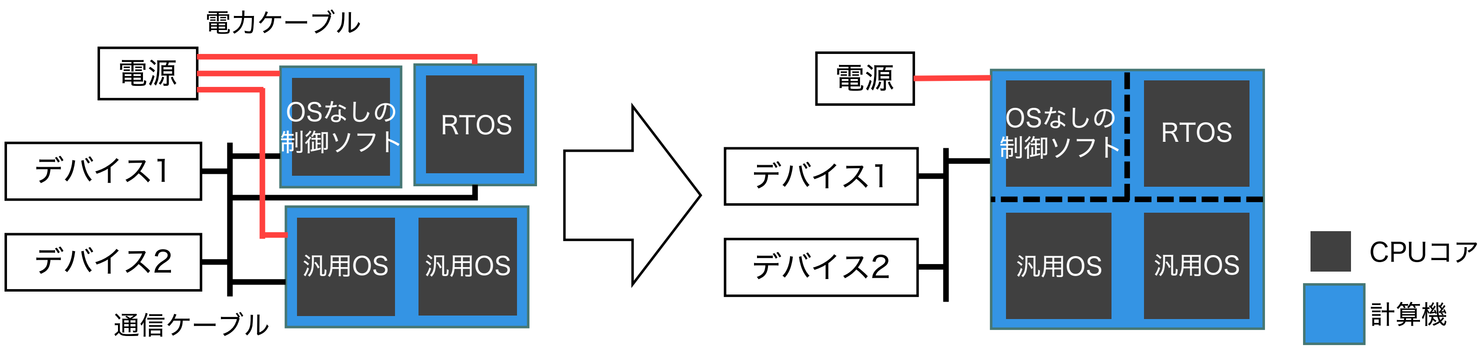
- **個人及び産業用のIoT機器が増加している.**
- **IoT機器は汎用PCと比べて制限がある.**
  - 非力なCPU，少ないメモリ
  - IoT機器で使用されるOS：FreeRTOS，RIOT，Zephyr など.
  - IoT機器で使用するOSはLinuxより軽量・省電力性・リアルタイム性が必要.
- **ハードウェア・OSに求める機能が異なるため，**
  汎用PCなどで動作する**セキュリティ機能がそのまま使えない**.
- **Armプロセッサが持つセキュリティ拡張機能TrustZoneに着目**
  - ハードウェアとして実行空間を分割することが可能

IoT機器で広く利用されるCPUである
Arm Cortex-Mシリーズが持つ
TrustZoneを用いて隔離実行環境を構築する

組込みシステム集約のための制御基盤

- 組込み機器で高性能化や多機能化が進んでいる
  →内部スペースの圧迫，ハードウェアの複雑化
- プロセッサのマルチコア化が進んでいる
  →組込みソフトウェアではマルチコアを活かせてない

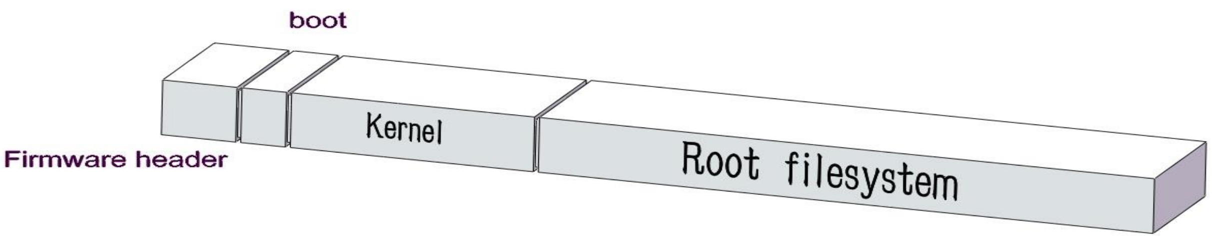
- 既存の組込みソフトウェアをマルチコア環境に集約し，
  コアの柔軟な割り当てを可能とする基盤ソフト「誉」を構築する
  - メモリ，割込み，起動補助，デバイスの共同利用などの実現が必要
  - 仮想化でデバイス共有など，LPARでオーバヘッドなしを実現



誉：High-layer On Multicore-Architecture for Recently Embedded-system

IoTファームウェアの安全性評価

- 広く利用されるようになったIoT機器にも脆弱性がある
- Windows等ならアップデートが継続的に提供されるが…
  IoT機器のファームウェアはどうだろうか？
  - 機器が長期で使われる可能性がある一方で
    ファームウェアのサポートが先に終了したり
  - ファームウェアのバージョンアップ時であっても，製品の主要機能でない部分（ライブラリ，デーモン等）は更新されなかったり
- ファームウェアの安全性をちゃんと評価しないといけないのではないか？
  - ファームウェア内で使われているソフトウェアをリストアップ
  - それらのバージョンを同定
  - 脆弱性データベースを活用し，脆弱性の種類と有無を判定
  - 利用者への注意喚起，製造・販売者への対応依頼などに

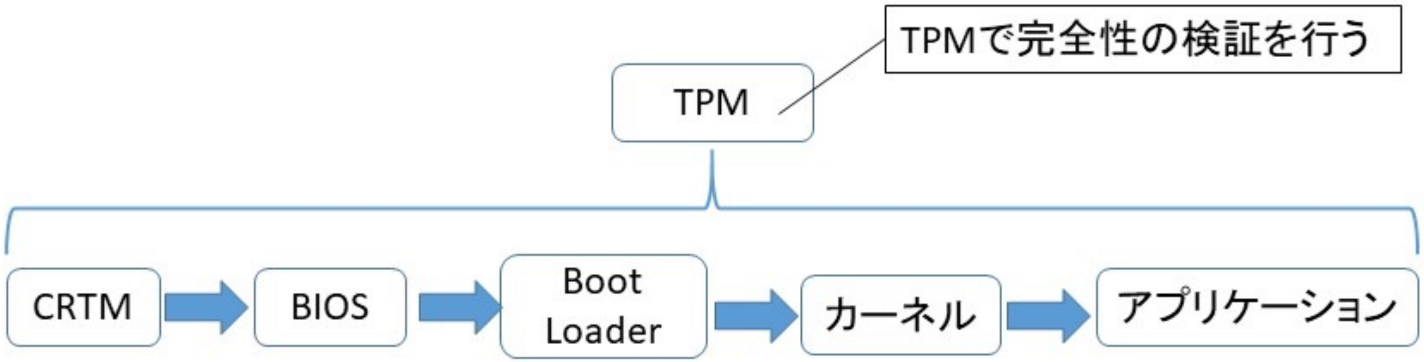


ファームウェアの構造

IoT機器の信頼性保証

- IoT機器はセンサなどの情報を扱い，その結果は実世界に反映される
  - 空調，調光，土砂災害
  - 正しいプログラムが動作していること，データが改ざんされないことが極めて重要
- プログラムの完全性
  - 起動，OSのロード，アプリのロードのフェーズを通じた確認が必要
  - それらに切れ目があってはいけない
- データの完全性も
  - 改ざんされた場合に検出できることが必要

TPM（Trusted Platform Module）を用いた完全性確保を目指す！



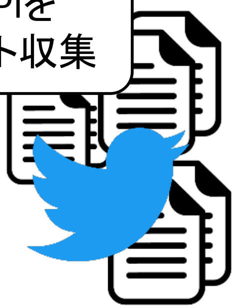
Salvia

Twitterを用いたサイバー脅威情報の解析

- Cyber Threat Intelligence(CTI)という概念が注目されている
  - 攻撃者などの脅威情報について分析を行なったもの
  - 企業や公的機関で攻撃防御のために活用されている
- CTIを作成するために収集する情報の種類の1つに Open-Souce Intelligence(OSINT)がある
  - 公的に利用可能な情報源から収集されるデータ群

OSINTとしてTwitterのデータを収集し，分析を行うことで
攻撃者の痕跡や動向を探る

①TwitterAPIを
用いてツイート収集

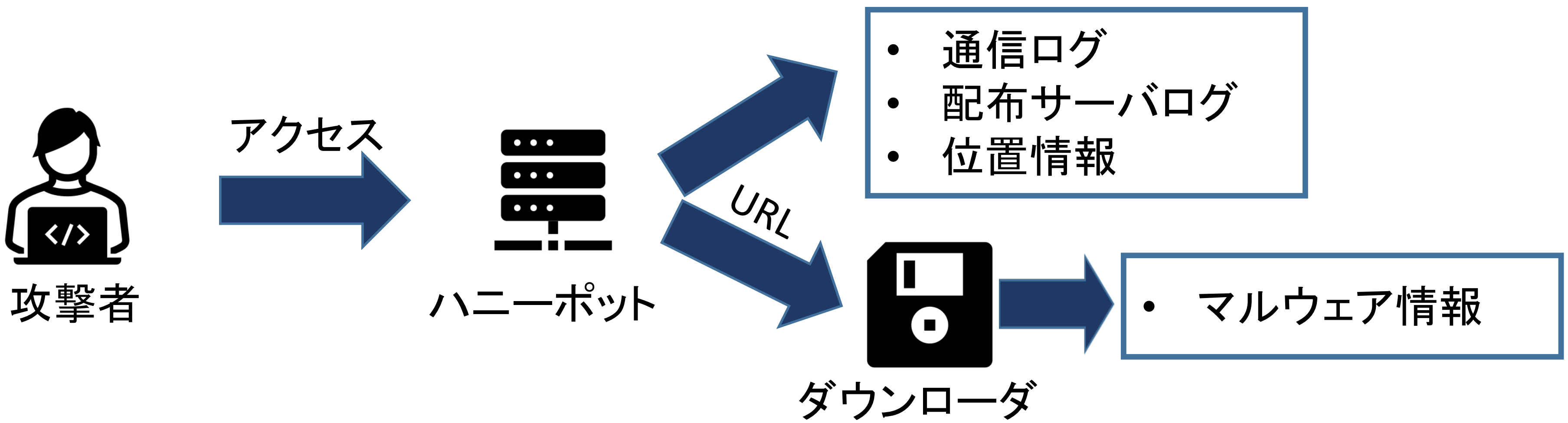


②収集したツイート群
の蓄積・データ整形

③整形したデータの分析
- 時系列
- 発生しているインシデントの傾向
- 発信者の属性 etc…

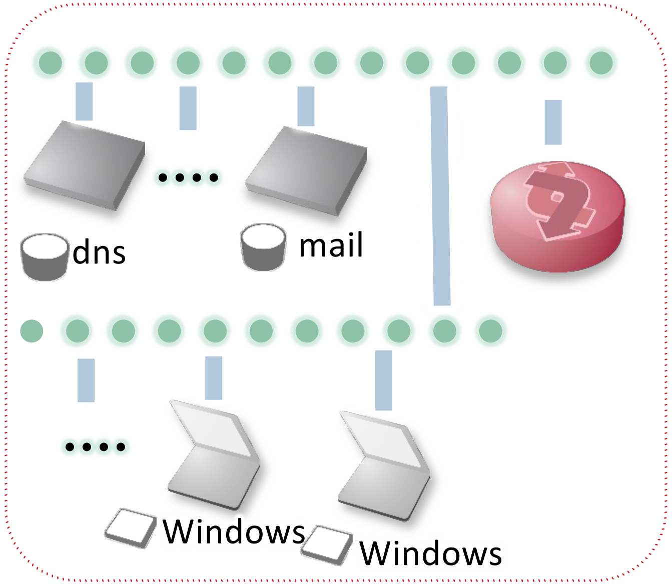
IoTマルウェアの実態解析

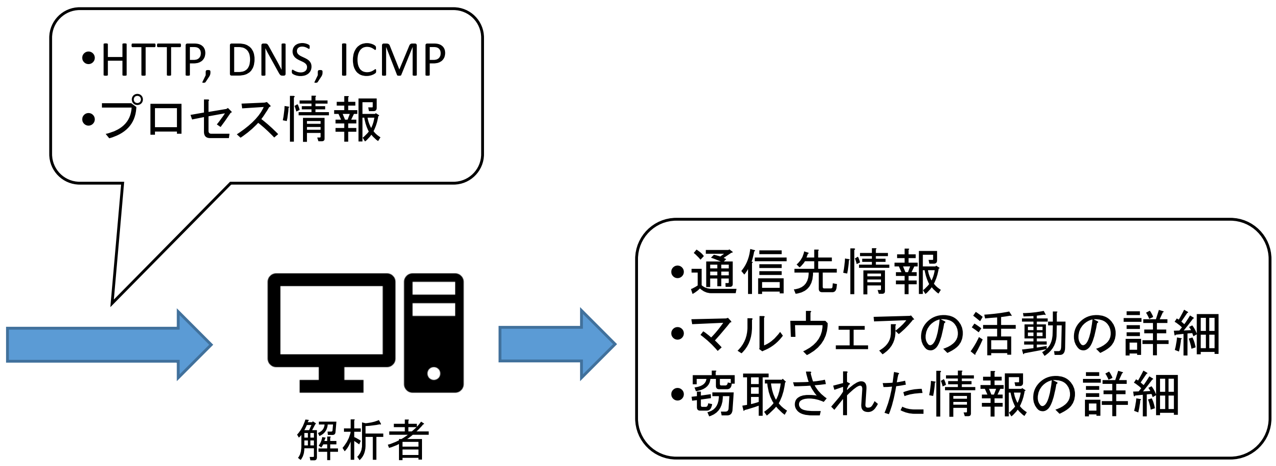
- IoTマルウェアが流行っていましてね
  - 数多く配置され，十分な管理体制じゃなかったり，放置だったり
  - IoT機器を乗っ取って多方面に攻撃をするような状況
- IoTマルウェアと攻撃者の動向をなんとかつかんで応戦したい
  - ハニーポットを用いた攻撃の観測
  - ダウンロードされるIoTマルウェアの取得
  - マルウェア配布サーバに配置されるIoTマルウェアの変化の監視



標的型マルウェアを用いた攻撃者誘引

- 標的型攻撃って簡単にしてもらえそうに思います？
  - マルウェアを実行しても攻撃者のサーバ(C2サーバ)が動いていないことも
- 効果的に攻撃者を誘引して，行動を観測したい！！！
  - マルウェアを動かしてC2サーバの情報(IPアドレス)を収集
  - C2サーバの稼働状況を監視
  - C2サーバが動き出したときにあわせてマルウェアを動かす！





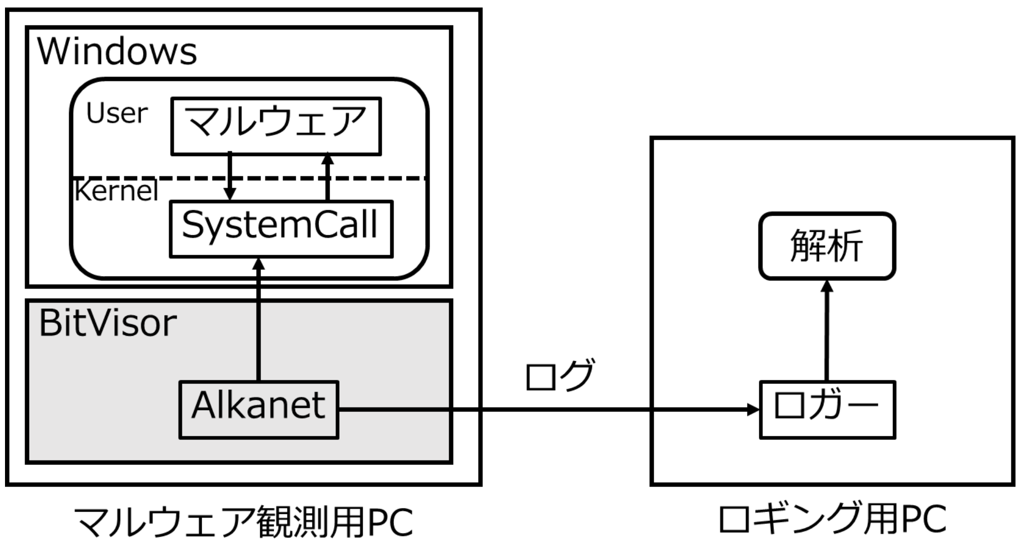
Alkanet

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1つ1つに対して静的解析をするのは時間がかかりすぎるため，動的解析を行うことが必要
- 対解析機能を持つマルウェアに悟られずに解析を行うことが必要

システムコールに着目した動的解析を行うAlkanetが開発された

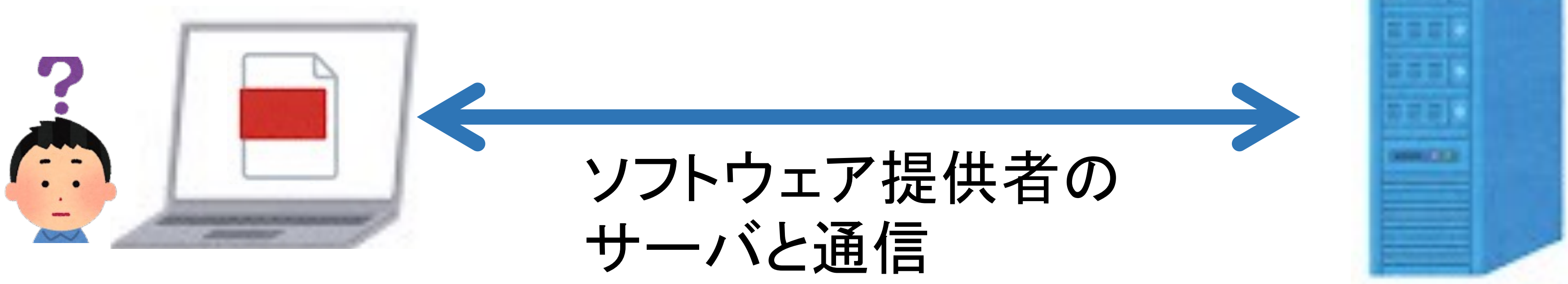
Alkanetの構成



- **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**
  - 引数解析
- **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**

フツーのソフトは本当に普通なのか

- 健全とされるソフトが利用者の情報を収集していたとか最近よく聞く話だけど・・・実態は如何に？



	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.30.85.65	54.95.144.31	TLSv1.2	110	Application Data
2	0.003473	172.30.85.65	54.95.144.31	TLSv1.2	110	Application Data
3	0.005423	172.30.85.65	54.95.144.31	TLSv1.2	110	Application Data

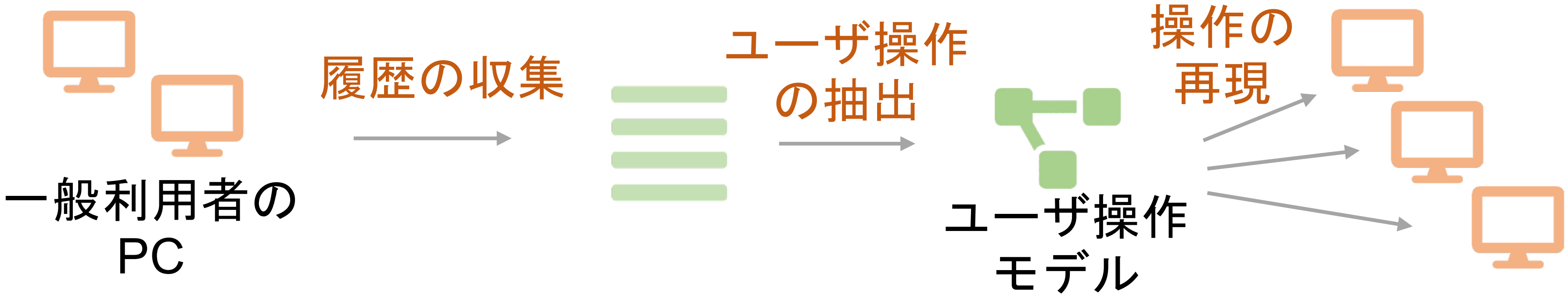
このソフトは・・・
・なぜこのサーバと通信をしているんだ？
・なぜこのタイミングで通信をする必要があるんだ？
・通信をする前にファイルやレジストリにアクセスしているぞ！
なんてことがあるかも

ユーザ操作のモデル化による擬似ログ生成

- 標的型攻撃の観測には，
  攻撃者に侵入してもらわないといけないが…
  - 侵入される環境が「誰も使っていない環境」だとすぐ逃げられる
  - といって「使用感のある環境」を作るのは大変
  - どう使用感を醸し出すと良いかは組織によって異なるし

組織特有の使用感を持つ
標的型攻撃誘引環境を作らねば！

- 組織の人のPCの操作履歴を収集し，そこから操作モデルを構築
- 操作モデルを使ってPCを自動操作して目的達成したい



研究室メンバー

- 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）
  - 研究補助員　金城 聖
- 頼りになる先輩方
  - D3　1人
  - M2　1人
  - M1　6人
  - 学部生　12人 (M0　7人)
  - 計20人

研究室のゼミ

- 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

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
  - 研究室全体で研究内容の共有＆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
  - 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

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！

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）

• 三菱電機	OS・仮想化・組込みシステム・セキュリティ
• アドソル日進	OS・仮想化・組込みシステム
• 東芝	OS・仮想化・組込みシステム・セキュリティ
• 日本電気(NEC)	OS・コンピュータセキュリティ，サイバー攻撃
• 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

- 対外発表（2017年度～）
  - 査読付きジャーナル論文 9件
  - 国際会議 7件（うち受賞2件）
  - 国内シンポジウム・研究会・全国大会 48件（うち受賞10件）

研究の階段を上るためのプログラム

基礎力を固めるプログラム

＜OS開発実践＞
基礎技術習得

課題
発表

＜論文輪講＞
先端知識習得

輪講
発表

＜研究導入実践課題＞
先端技術実践習得

夏休み課題 → 全体ゼミ・輪講 → 全体ゼミ・グループゼミ

3回生夏休み

3回生後期

たこパ

グループ
配属

バド

卒研テーマ
確定！

力をより高めるプログラム

＜卒業研究＞
先端技術創造

全体ゼミ発表
(月1回程度)

中間
発表

他大学・企業交流
(優秀者等)

卒研
発表

対外発表
(優秀者等)

全体ゼミ・グループゼミ

4回生

テニス

コンパ

マルウェア解析
コンテスト出場

ソフトボール

BBQ

卒業(学士)

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

スケジュール

〇：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）

	6(月)	7(火)	8(水)	9(木)	10(金)	13(月)	14(火)	15(水)
1コマ（9:00～）								
2コマ（10:40～）			☆	Lゼミ	Sゼミ		○	
昼休み	OH	OH	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					Aゼミ
5コマ（16:20～）	○	☆	○	☆	全体ゼミ			
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/

- 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