新技術説明会
New Technology Presentation Meetings!

最新のマルウェアを検知する更新可能なAI回路

工学院大学　情報学部　コンピュータ科学科
教授　小林　良太郎

2023年9月19日

本発表のキーワード

- 情報分野
  - セキュリティーシステム
    - マルウェア検知
    - AI
  - ハードウェア
    - LSI
- IoTデバイス
  - 産業用途、コンシューマー、自動車、医療

研究分野の背景

- IoTデバイスの急速な普及[1]
  - 産業用途、コンシューマー、等での高成長が予測
- 近年、Linuxマルウェアが650%急増[2]
  - ➡ クラウド、IoTデバイスへの脅威
- IoTデバイスへの攻撃が急増
  - 1組織当たり週平均攻撃数：2022年54件 ➡ 2023年1-2月91件 [3]
  - 1日当たりMirai感染ホスト数：2022年数百台～5千台 [4]
- IoTセキュリティ関連の法律や基準が策定

[1] 2023年総務省情報通信白書
[2] 2022年7月AtlasVPNの報告
[3] 2023年5月Check Point Researchの報告
[4] 2022年5月情報通信研究機構の報告

本技術の概要

IoT機器に搭載

- 小型・高速・高精度なセキュリティ対策を提供
- マルウェア検知に特化
- ハードウェア実装によるシステムの小型化、高速化
- AI回路を搭載
  - ランダムフォレストを使用
  - AI回路の小型化と高速化、マルウェア検知の精度向上

新たに発生したマルウェアに対応可能

- マルウェア検知に必要なデータを更新する機能を持つ

従来技術と競合技術

従来技術

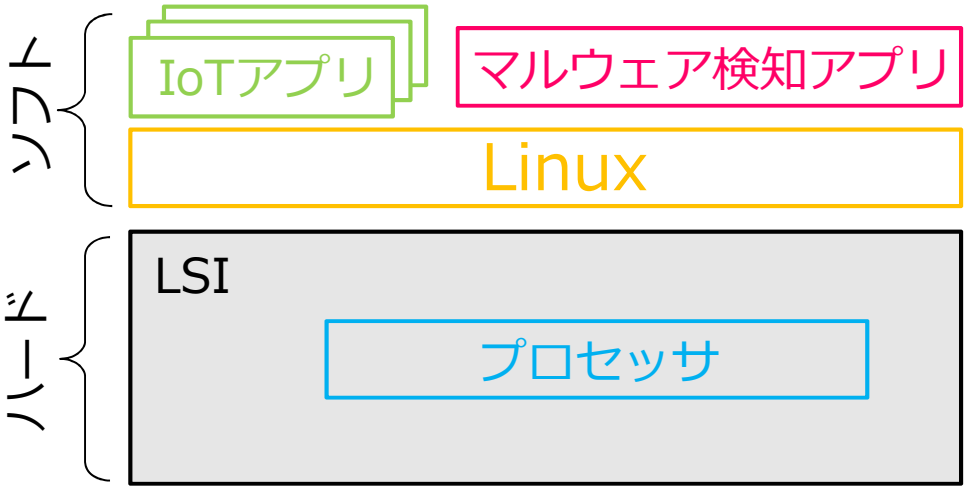
- ソフトウェアベースのマルウェア検知技術が存在
- 問題点：複雑なソフトウェアであるため、IoT機器への搭載は現実的ではない

競合技術

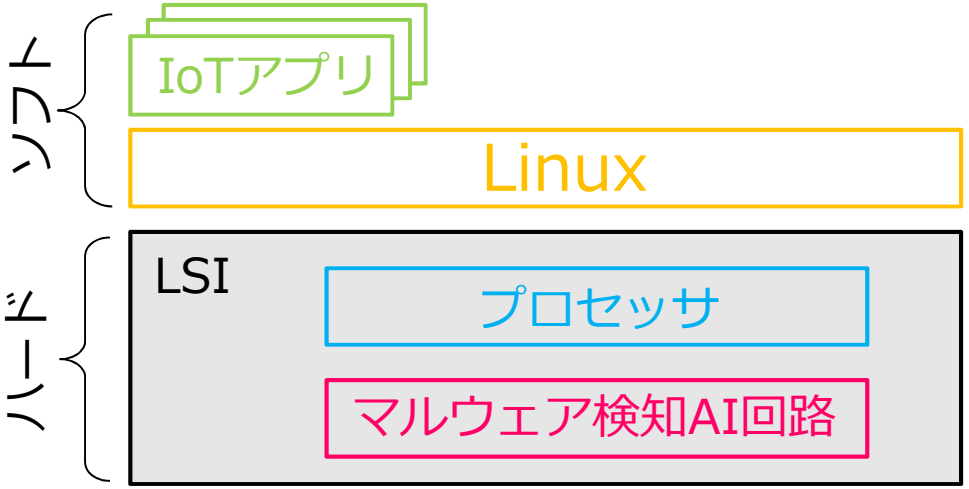
- 本技術の前身となったマルウェア検知AI回路が存在
- 問題点：マルウェア検知用のデータを回路内部に焼き付けるため、新たなマルウェアに対応できない

従来技術との比較

従来技術：ソフトウェア実装
- OS上で動作
- 入力：ファイル、振舞い、等
- 他のアプリとリソース共有
- 一定のマシンスペックが必要



本技術：ハードウェア実装
- LSI上の回路として動作
- 入力：プロセッサ情報
- アプリとのリソース共有なし
- LSI上の回路面積が必要



プロセッサ情報

- AI回路の入力となるデータ
- 以下2通りに分けられる
  - プロセッサ内部の回路から直接得られる生データ

    例：プログラムカウンタ、ヒット/ミス情報、命令の種類、等
  - 生データを加工して得られるデータ

    例：命令キャッシュヒット率、データキャッシュヒット率、等
- 入力の組合せは変更可能、新たな入力の作成可能
  - プロトタイプ：3～22種類から組合せを決定
- 環境に合わせて新たな入力を導入することが可能
  - カーネルの命令キャッシュヒット率、等

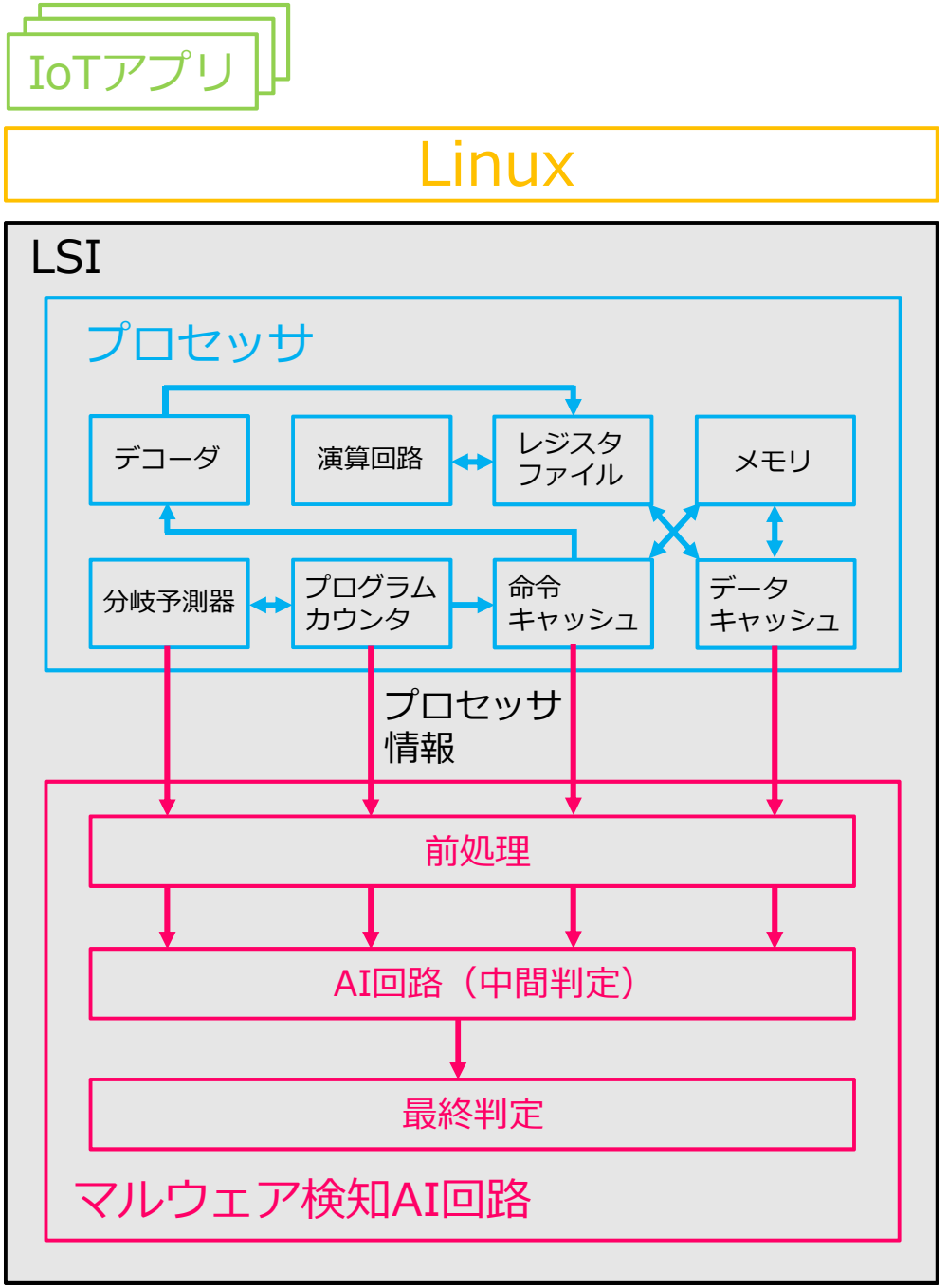
競合技術について

- 競合技術は本技術の前身となる技術
  - 両技術の発明者は同一
  - 両技術の基本的な仕組みは同一
    LSI上のAI回路、プロセッサ情報を使用、マルウェア検知、等
- 重要な相違点（新マルウェアへの適応力の違い）
  - AI回路はマルウェアを検知するために必要な情報を保持
  - 上記は、競合技術では更新不可、本技術は更新可能
- 基本的仕組みの説明 → 相違点の説明
- 応用例と検証結果として、公開済みである競合技術（基本的仕組みは同一）を紹介

本技術の構成

プロトタイプの回路構成

- 前処理回路
  - LSI上の配線を介して、プロセッサ情報を取得
  - データの前処理
- AI回路（中間判定）
  - 1命令単位で攻撃/正常判定
  - ランダムフォレストベース
- 最終判定回路
  - 中間判定結果を集計
  - 実行中のプログラムがマルウェアかどうかを判定



本技術の動作例

プロトタイプの回路動作例

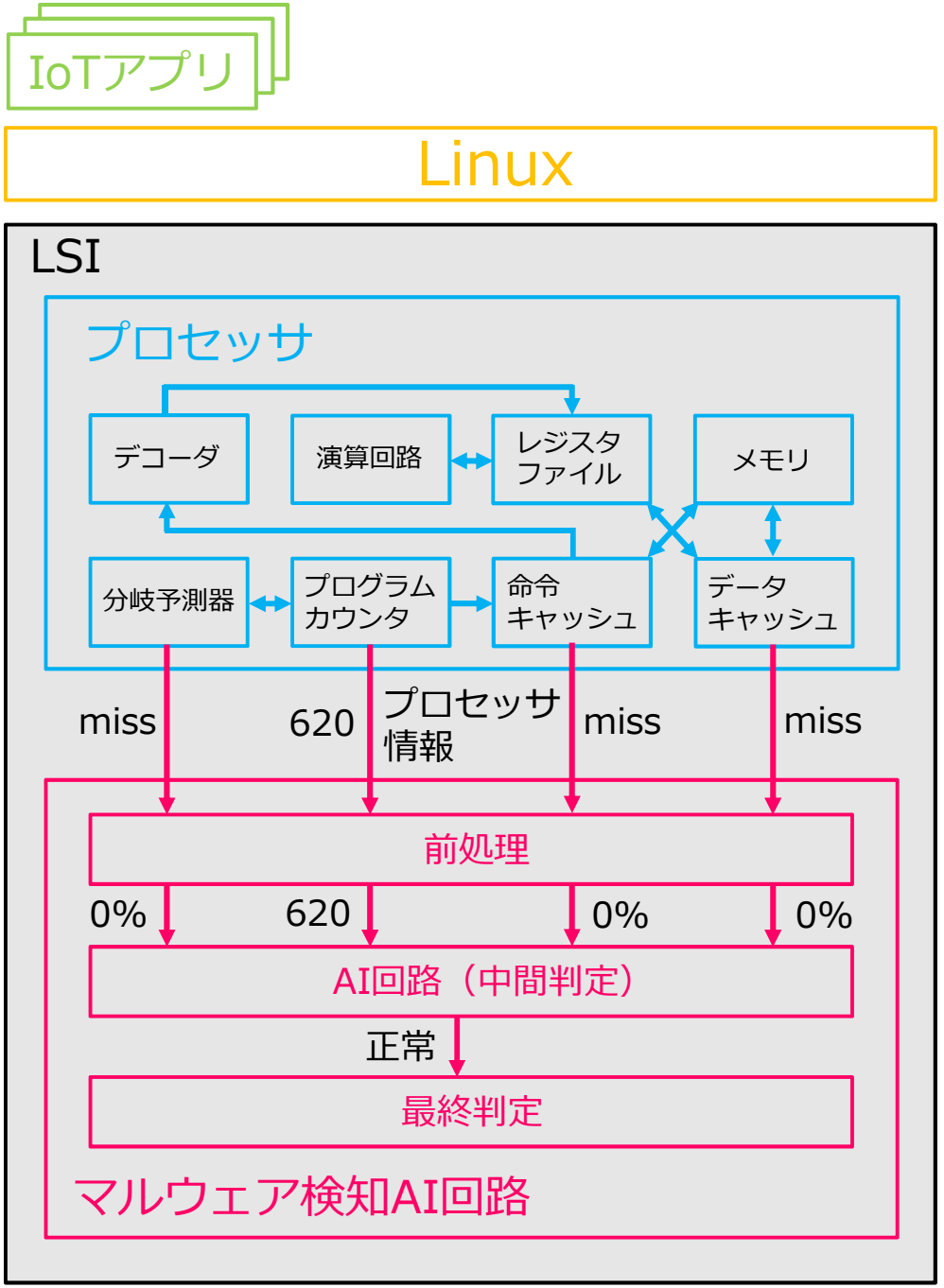
- **1サイクル目**
  プロセッサ: 命令Xを実行
  プロセッサ情報: {miss, 620, miss, miss}
  前処理出力: {0%, 620, 0%, 0%}
  AI回路出力（中間判定）：正常

⋮

- **nサイクル目**
  プロセッサ: 命令Yを実行
  プロセッサ情報: {hit, 9228, hit, miss}
  前処理出力: {91%, 9228, 99%, 84%}
  AI回路出力（中間判定）：攻撃

⋮

- **5000サイクル目**
  最終判定：集計（中間判定の80%が攻撃）
  ➡ 実行中のアプリはマルウェア



公開済みの情報

本技術の基本的仕組み（類似技術と共通）は公開済み

- プロセッサとしてARMを使用した応用例1件
  - FPGAを用いてAI回路を実装(2022年)
    https://doi.org/10.1007/s10207-021-00577-0
- プロセッサとしてRISC-Vを使用した応用例2件
  - マルウェア検知回路とRISC-VをFPGA上に実装(2022年)
    https://doi.org/10.15803/ijnc.12.2_253
  - 回路や電力の削減等を行い、FPGA上に実装(2023年)
    https://doi.org/10.15803/ijnc.13.2_149
- 類似技術との相違点（更新機能）については未公開
  - 特願2023-052449

プロセッサとしてARMを使用した応用例
- 評価した環境 -

- 詳細： https://doi.org/10.1007/s10207-021-00577-0
- 用意したプロセッサ情報は18種類
- 回路設計の方針
  - 最終目標はカスタムLSIの設計であるが、設計や動作確認の容易さからFPGAを使用。設計対象はAI回路。
- 評価項目
  - 検知性能：エミュレータを使用して評価
  - 回路設計：ツールとして Vivado、FPGA として XC7Z020-2CLG484I を用いて評価

プロセッサとしてARMを使用した応用例 - 得られた結果 -

- 詳細： https://doi.org/10.1007/s10207-021-00577-0
- エミュレータを用いた検知性能の評価
  - マルウェアの検知率100%、誤検知率0%
  - 予測検知により検知時間を19%以下に削減可能
  - 中間判定のサンプリングにより稼働時間を99%削減可能
- FPGAを用いたAI回路の回路規模の評価
  - 中間判定を行うAI回路の実装が可能であることを確認
  - AI回路の規模を大幅に削減できることを確認

プロセッサとしてRISC-Vを使用した応用例 - 評価した環境 -

- 詳細： https://doi.org/10.15803/ijnc.12.2_253
- 用意したプロセッサ情報は3～7種類
- 回路設計の方針
  - オープンなプロセッサであるRISC-Vを使用
  - プロセッサとマルウェア検知機構をFPGAに実装
- 評価項目
  - 検知性能：エミュレータを使用して評価
  - 回路設計：ツールとして Vivado、FPGA として XC7Z020CLG484-1 を用いて評価

プロセッサとしてRISC-Vを使用した応用例 - 得られた結果その１ -

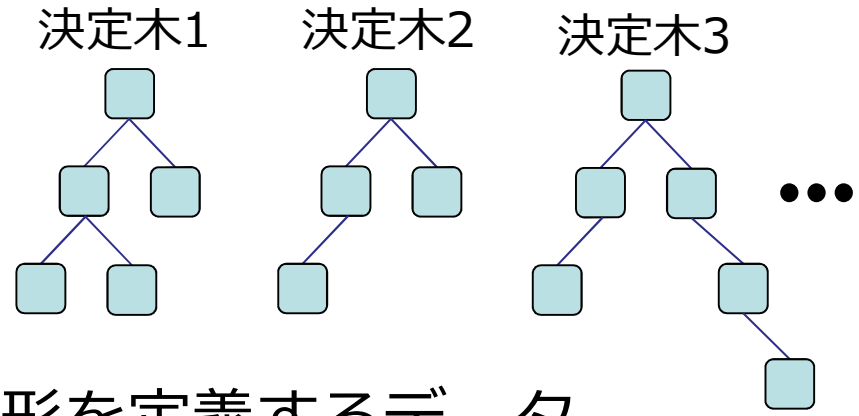
- 詳細： https://doi.org/10.15803/ijnc.12.2_253
- エミュレータを用いた検知性能の評価結果
  - 3種類のプロセッサ情報でマルウェアの判定が可能
- FPGAを用いたプロセッサとマルウェア検知AI回路の回路規模の評価
  - プロセッサとマルウェア検知AI回路を1つのFPGA上に実装可能
  - プロセッサに比べ、マルウェア検知AI回路は、メモリブロックが同程度、それ以外の回路が数%未満

プロセッサとしてRISC-Vを使用した応用例 - 得られた結果その２ -

- 詳細： https://doi.org/10.15803/ijnc.12.2_253
- エミュレータを用いた検知性能の評価結果
  - パラメータによっては検知性能が低い場合が存在するが、プロセッサ情報を増やしたり、学習するデータセットを変更することで正解率100%にすることが可能
- FPGAを用いたマルウェア検知AI回路の電力の評価
  - 前処理回路の電力を9割以上削減
  - 中間判定を行うAI回路の電力を3割ほど削減

競合技術との相違点（更新機能の有無）

AI回路の前提



- カスタムLSI上に実装
- 複数の決定木を用いて検知
- 検知に必要な情報
  - 決定木（ノードと線で構成）の形を定義するデータ
  - 各ノードで行う計算式のデータ

競合技術

- 検知に必要な情報をLSI上に焼き付けるため更新不可

本技術

- 検知に必要な情報を回路の工夫により随時更新可能

➡ 新たなマルウェアへの対応が可能

新技術の特徴（まとめ）

- 小規模な回路、検知用の情報を更新可能
- IoT機器の動作環境を考慮して、AI回路に送るマルウェア検知用のデータをカスタマイズできる
- AI回路の入力データを変更することで、検知対象をマルウェア以外に変更できる

想定される用途

- 安価で高精度なマルウェア検知が必要な分野（コンシューマー）
- 複数のマイクロコントローラ使用する分野（自動車、医療機器など）
- AI回路の入力データ変更 ➡ 多用途への展開
  - IoT機器での悪性通信検知
  - 画像認識、音声認識、音響認識（故障検査等）

実用化に向けた課題

- 現在、ハードウェアについてFPGA上で実装が可能なところまで開発済み。しかし、さらなる低コスト化、LSI実装、他用途への展開、各種マイコンへの対応が未解決である。
- 今後、低コスト化、LSI実装、多用途への応用について実験データを取得し、コストと精度を両立させる条件設定を行っていく。
- 実用化に向けて、各種マイコンに対応するための技術を確立する必要もあり。

企業への期待

- 未解決である各種マイコンへの対応、周辺回路の設計、ツール等については、企業の保有するノウハウにより克服可能と考えている。
- 回路設計技術を持つ企業との共同研究を希望
- また、マイコン等を開発中の企業、車載・医療用セキュリティ分野への展開を考えている企業には、本技術の導入が有効と思われる。

本技術に関する知的財産権

- 発明の名称　：検知回路
- 出願番号　　：特願2023-052449
- 出願人　　：工学院大学、長崎県立大学
- 発明者　　：小林良太郎、加藤雅彦

お問い合わせ先

工学院大学
総合企画部　産学連携室

ＴＥＬ　042－628 － 4928
ＦＡＸ　042－626 － 6726
e-mail　sangaku@sc.kogakuin.ac.jp

研究・産学連携各種情報

新技術のまとめ

- IoT機器においてマルウェアを検知
- 小規模回路での実装
  → IoT機器に搭載
- 検知用データの更新が可能
  → 最新のマルウェアへの対応
- マルウェア以外への展開も可能

ご清聴ありがとうございました