Faculty of Health Data Science, Juntendo University

サイバーセキュリティ研究室
Cyber Security Research Laboratory

教授　加藤雅彦
Masahiko Kato Ph.D.
E-mail: m.kato.ug@juntendo.ac.jp

研究概要 / Research overview

サイバー空間で行われる様々な攻撃の対策を研究しています。サイバー攻撃手法の解明、攻撃予測、フィッシング対策、IoTセキュリティ検査自動化、異常動作検知機構内臓CPU開発など。

We research countermeasures against various types of attacks conducted in cyberspace. The themes are: automating IoT security inspections, implementing CPU-embedded anomaly detection mechanisms, forecasting cyber attack, and so on.

研究の流れ / Research flow

サイバー空間には様々な脅威が存在します。特定の脅威に焦点を当て攻撃手法や先行研究を調査し、新たな対策を検討します。検討した対策が有効に機能するかどうか、実際にシステムを構築して検証を行い、その成果を公表していきます。

theme selection 課題調査
survey 先行研究調査
proposal 対策立案
implementation 対策の実装
evaluation 評価（対策効果測定）
consideration 考察
paper 論文化

Various threats exist in cyberspace. We focus on specific threats, investigate attack methods and previous research, and propose new countermeasures. To clarify the effectiveness of these countermeasures, we build the system and evaluate the countermeasures.

研究成果 / Research outputs

IoT機器のセキュリティ対策として、機械学習によるアンチウイルス機能を内蔵したCPUを開発し、以下を明らかにしました。

1) 異常検知に利用可能なCPU内部情報
2) 異常検知に適した機械学習方式
3) CPUと機械学習回路の接続方法
4) 異常検知回路の規模や消費電力算出
5) 異常検知回路の小型化手法
6) 異常検知回路を再学習させる方法
7) FPGA実装によるプロトタイプ実装

As a security measure for IoT devices, we developed a CPU with built-in antivirus functionality utilizing machine learning, and we clarified the following points. 1) CPU internal information can be used for attack detection. 2) Machine learning method suitable for attack detection. 3) How to connect CPU and machine learning circuit. 4) Calculating the scale and power consumption of the detection circuit. 5) Methods for miniaturizing detection circuit. 6) How to retrain the detection circuit. 7) Prototype implementation using FPGA.