TYPE OF INDUSTRY

科学技術・大学

情報通信研究機構

NICT先端研究 ⑭⑭

AIでIoTマルウエア解析

無線通信技術の向上により、家電などのさまざまな設備がインターネットデバイスへと変化し、このようなデバイスがつながるネットワークはIoT（モノのインターネット）として知られる。IoTを利活用することにより、効率的に生産性を向上させることができ、より便利で豊かな社会へと進化・発展を遂げてきている。

一方、業務や用途に特化したIoTデバイスを開発する場面では、セキュリティーへの考慮が不十分で、脆弱性が意図せず作り込まれてしまうことが多い。また、マルウエアに感染したIoTデバイスがサイバー攻撃に悪用されるケースが急増している。

サイバー攻撃の被害を未然に防ぐ、もしくは軽減することを目的に、我々は機械学習を中心とした人工知能（AI）技術を活用することにより、IoTセキュリティー対策技術の研究開発に取り組んでいる。

これらの研究の一つとして、我々はIoTマルウエア分析技術の研究開発を実施している。マルウエア感染を防ぐためには、実行可能プログラムからマルウエアを検出・隔離することで、拡散を防止することが望ましい。

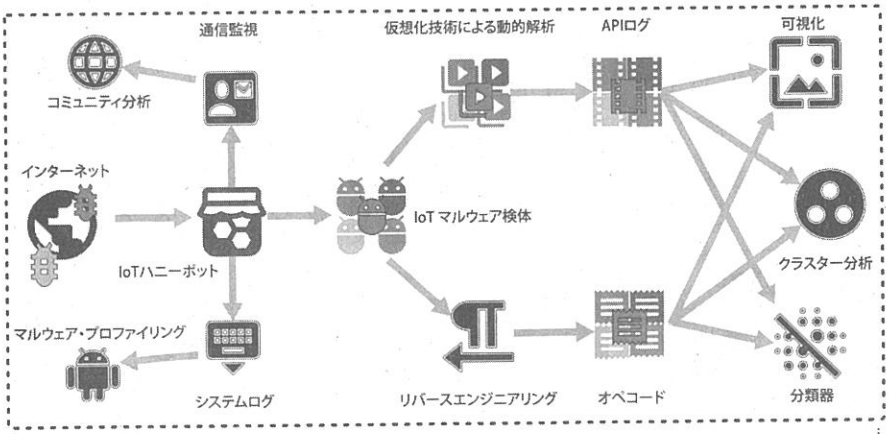
ただし、IoTセキュリティーでは従来のWindowsセキュリティーとは異なる、取り組むべき重要な研究課題が二つ挙げられる。一つ目はハードウエアリソースに制約のあるデバイス上で動作する軽量なセキュリティー対策技術の実現、二つ目は異なるCPUアーキテクチャーで横断的に機能するセキュリティー対策技術の実現である。

そこで我々はこれら二つの課題を解決すべく、実行ファイルのバイナリコードなどの静的な情報に基づいた軽量な機械学習技術を開発した。本技術を用いることで99%の精度でマルウエアが検知できることに加え、マルウエアの実行時の情報を組み合わせる場合は98%の精度でマルウエア名の特定まで可能である。

「超高速・多数同時接続・超低遅延」を特徴とする5Gの高性能を生かすIoT技術により、新たなビジネスが創出されることが期待される。IoTの利活用に当たってはこれまでのセキュリティー対策を徹底するだけではなく、新しい脅威に対して備える必要がある。

我々はAI技術の研究開発によって、IoTセキュリティーの確保に寄与していく。

（火曜日に掲載）



IoTマルウエア分析フレームワーク

サイバーセキュリティ研究所・サイバーセキュリティ研究室 主任研究員 班涛（バン トウ）

2006年神戸大学大学院博士後期課程を修了。同年より現職。サイバー攻撃対策、マルウエア分析、機械学習に関する研究に従事する。博士（工学）。