情報通信研究機構

NICT 先端研究 ⑥⓪

マルウエア検知 精度94%

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研究マネージャー 高橋 健志

フィンランド・タンペレ工科大学、ローランド・ベルガーを経て、09年より現職。サイバーセキュリティーに関する研究開発と標準化活動に従事。早稲田大学卒。博士（国際情報通信学）。

増加の一途をたどるサイバー脅威に対応するには、セキュリティーオペレーションの自動化が必要不可欠だ。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、マルウエア分析や脆弱性の深刻度評価、DDoS攻撃の発生検知、さらには将来の攻撃予測など、さまざまな自動化技術に関する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Androidアプリ分析技術の研究開発を実施し、94・07%の精度でマルウエアを検知できる技術を開発した。この中から有効なもののみを選択して活用することにより、検知率の向上を実現してきた。

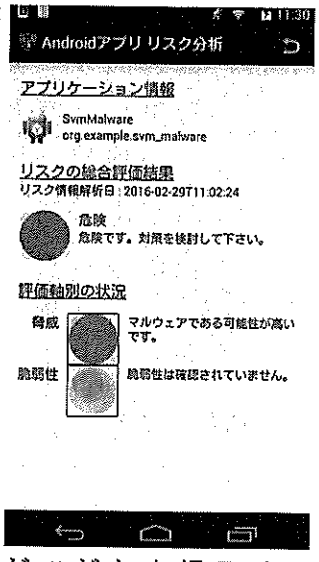
また、本技術を用い、インストールされているアプリを評価し、リスクをユーザーに可視化してくれるツールも作成している。本ツールでは、脅威と脆弱性を評価し、マルウエアである可能性が高いと判断されれば脅威の信号が、脆弱性があると判断されれば脆弱性の信号が、それぞれ赤く点灯する。

セキュリティー分野での機械学習の活用は今後急速に拡大していくことが予想され、NICTでも重点領域となっている。2017年には知能科学融合研究開発推進センター（AIS）を立ち上げ、その中でサイバーセキュリティー分野におけるAI活用の推進を最重要分野の一つに据えている。

本分野において競争力を維持していくためには、機械学習技術に関するノウハウの蓄積も重要であるが、データセットの質と量が競争力の源泉となると考えている。

そのため、我々は今後も各種のデータを継続的に収集・蓄積していくと同時に、解くべき課題を再定義して研究開発を推進し、サイバーセキュリティーオペレーションの自動化に貢献していきたい。

（火曜日に掲載）



Androidアプリのリスク分析・可視化ツール