個人研究

スマート社会

人工知能の情報セキュリティ技術への応用

人工知能（ＡＩ）により、従来技術では検出できなかった攻撃が検知できるようになったり、人間に解析できないものが解析できるようになってきました。一方、誤った評価や、ＡＩによる判断の過信という弊害も起きており、問題解決と問題提起の両面で研究を行っています。

KEYWORDS 情報セキュリティ

RESEARCHER

コンピュータサイエンス学部 講師　宇田隆哉

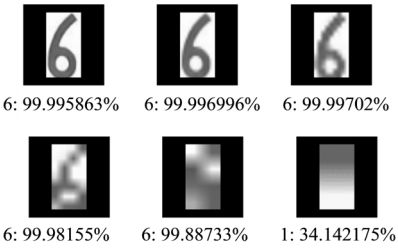
https://www.teu.ac.jp/info/lab/project/com/dep.html?id=121

学会発表・論文・著書・社会活動

[1] S. Akaishi and R. Uda, Classification of XSS Attacks by Machine Learning with Frequency of Appearance and Co-occurrence, In Proc. of the 53rd Annual Conference on Information Sciences and Systems (CISS), 2019.
[2] 白石将貴, 宇田隆哉, 藤川真樹, Kinectを用いた行動座標によるピッキング行為の検知, 情報処理学会論文誌, Vol.61, No.2, pp.486-499, 2020.
[3] T. Azakami, C. Shibata and R. Uda, Evaluation of Ergonomically Designed CAPTCHAs using Deep Learning Technology, Journal of Information Processing, Vol.59, No.9, 2018.

01 AIでナンバープレートを識別する

犯行現場近くの監視カメラに、犯行に使われた自動車が写っていたとしても、ナンバープレートがはっきり写っていなく、人間には読み取ることが難しかったりします。そのような場合でも、人工知能でよく使用されるようになった畳み込みニューラルネットワークを用いて、高い精度で数字の識別を行う研究をしています。



02 AIでマルウェアの亜種を検出する

マルウェア（コンピュータウイルスなどの総称）の中には、パターンマッチングで発見されないように、バイナリパターンを少し変える亜種と呼ばれるものがあります。畳み込みニューラルネットワークを用いて、実際に流行した亜種のマルウェアを見分ける研究を行っています。