論文名：Web Application Firewall using Character-level　Convolutional Neural Network
著者名：Michiaki Ito* and Hitoshi Iyatomi　（*: 理工学部応用情報工学科 4 年生）
受賞名：　IEEE CSPA 2018 Best Paper Award

概要：　Web システムは、日々様々な脅威にさらされている。通常の Firewall では防ぐことが困難な脅威に対して、アプリケーションレベルで攻撃の検知、防御を行う Web application firewall（WAF）が広く併用されるようになってきた。しかしながら WAF は遮断する通信を事前に正規表現で定義する必要があるため、導入コストがとても高いだけでなく、新たな攻撃や亜種の攻撃に万全とはいえない。そこで我々は、画像認識分野で近年用いられている深層学習の技術を文字列処理に適用し、WAF の機能を実現する高速、高精度な識別器を構築した。私たちのシステムは主に独自の character-level convolutional neural network (CLCNN)から構成され、公開されている http トランザクションのデータセットである HTTP　DATASET CSIS 2010（通常 36000 件、悪意のある通信 25000 件、計 61000 件）を用いて評価を行った。その結果、私たちの手法は同じデータセットを用いた state-of-the-art（従来研究の最善の結果：82%）を大幅に上回る検出精度 98.8%を達成した。本手法は、WAF を構築する際に、攻撃の定義などの手間が一切不要となるため、導入コストが従来手法より圧倒的に低く、また高速に動作(2.35msec/件)可能、さらに学習に基づく手法のため、未知であっても類似の攻撃に対しては耐性が期待できる大変期待できる技術である。今後様々な環境で実用化を踏まえた研究、検討を行っていく。