SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

fastText と LSTM を用いたマルウェア検知手法の提案
Proposal of Malware Detection Method Using fastText and LSTM to PE Strings

岸端 晃毅 *　　成田 匡輝 *
Koki Kishibata　　Masaki Narita

キーワード　マルウェア検知，表層解析，文字列，fastText，LSTM

あらまし

亜種を含む新規のマルウェアは日々多く観測されており，解析の人的及び時間的なコストは非常に高い．マルウェア解析は表層解析，動的解析，静的解析に分類でき，表層解析は動的解析や静的解析と比較して解析コストが低い．表層解析による類似性の高い検体の除外はその後の工程を適用する検体数が減少するため解析コストの削減につながる．本研究では表層解析を利用して取得した文字列に対して fastText と LSTM を用いたマルウェア検知手法を提案する．本稿には 2 種類の手法が含まれ，それらに対して評価実験により性能評価を行う．教師あり fastText[2] を用いた手法は fastText の軽量性に着目した低負荷な検知手法である．教師なし fastText[1] による単語の埋め込みと LSTM を用いた手法は教師ありの手法と比較してより詳細な文字列の構造に着目した検知手法である．本手法を利用することで文字列間の類似度の数値化や解析対象のマルウェア数の削減による解析のコストの減少が期待できる．

参考文献

[1] A.Joulin, E.Grave, P.Bojanowski and T.Mikolov, “Enriching Word Vectors with Subword Information”, arXiv:1607.04606, 2016.

[2] A.Joulin, E.Grave, P.Bojanowski and T.Mikolov, “Bag of Tricks for Efficient Text Classification”, arXiv:1607.01759, 2016.

* 岩手県立大学 ソフトウェア情報学研究科, 〒 020-0693 岩手県滝沢市巣子 152-52, Iwate Prefectural University, Graduate School of Software and Information Science, Sugo, Takizawa City, Iwate 020-0693