

文字列のランダム性を考慮した パスワード脆弱性評価手法の提案

A Proposal of Password Vulnerability Assessment Method Considering String Randomness

藤巻 壮・ネットワーク分科会・中央大学大学院

1. 研究背景・目的

AI技術の進歩とともに、AIが悪意を持ったサイバー犯罪者に利用されている。AIはパスワードの解読にも利用可能で、ゲームサイトから流出した1568万件のパスワードのうち4~17文字のパスワード51%を1分以内に解析するモデル^{*1}も登場している。

このような攻撃も含めてパスワードの強度を判定するため、独自に定義したランダム性を用いたパスワードの脆弱性判定手法を提案する。

*1: <https://github.com/brannondorsey/PassGAN>

2. 提案手法

以下の3つのランダム性についてそれぞれ文字列からスコアを出力する関数を定義する。

- 単語の文字遷移を考慮したランダム性
- キーボード上での文字のランダム性
- 123, abcなどの順序規則を考慮したランダム性

これらの関数を利用し作成した特徴ベクトルを機械学習モデルに学習させることで、パスワードの脆弱性評価を行う。

3. 今後の方針

- 既出のパスワード脆弱性判断システムとの比較実験を行う。
- AIを用いたパスワード解析を行い算出した脆弱性の正当性を検証する。