第 1 章

既存研究

1.1 ReDoS 脆弱性

文字列のパターンマッチングにかなり時間がかかってしまうような正規表現が存在することが知られている．そのような正規表現を ReDoS(regular expression denial-of-service) 脆弱な正規表現と呼ぶ．本節ではまず文字列のパターンマッチングはどのようなアルゴリズムで行われているかを紹介し，その次に正規表現の脆弱性について定式化を行う．

1.1.1 バックトラック探索

大抵のプログラミング言語が正規表現ライブラリを提供している．そのうち多くの正規表現ライブラリはバックトラック探索アルゴリズムを用いて文字列のパターンマッチングを行っている．バックトラック探索アルゴリズムがどのようなものなのかを [1] の論文で紹介されていた例を用いて説明する．バックトラック探索アルゴリズムについての詳細は [2] を参照されたい (プログラミング言語 Java におけるバックトラック探索アルゴリズムを用いた文字列パターンマッチングについて詳細に述べられている).

1.1.2 ReDoS 脆弱性の定式化

1.2 ReDoS 脆弱な正規表現の修正

1.2.1 REMEDY

参考文献

[1] Cristian-Alexandru Staicu and Michael Pradel. Freezing the web: A study of redos vulnerabilities in javascript-based web servers. In *Proceedings of the 27th USENIX Conference on Security Symposium*, 2018.

[2] Martin Berglund, Frank Drewes, and Brink Van Der Merwe. Analyzing catastrophic backtracking behavior in practical regular expression matching. *Electronic Proceedings in Theoretical Computer Science*, Vol. 151, , 05 2014.