A-019

ゼータ分布を利用したSQLインジェクション攻撃の特徴抽出について
Feature of SQL Injection Attacks and Zeta Distribution

松田　健 †
Takeshi Matsuda

1. まえがき

SQL インジェクション攻撃は web アプリケーションのデータベースに不正にアクセスする web アプリケーション攻撃の一種であり，インターネット利用人口の増加とともに SQL インジェクション攻撃の被害報告数も増加の一途を辿っている．

近年，機械学習やパターン認識などの統計的推測の手法を用いた SQL インジェクション攻撃の検出手法について盛んに研究されるようになっている [1] [2]．しかし，統計的推測を用いた検出手法には，その検出ルールをすり抜ける攻撃が新たに開発されることになるだけでなく，過去に観測されたことのない攻撃パターンの新しい攻撃を検出できる可能性は低くなることが問題としてあげられる．

そこで本研究では，SQL インジェクション攻撃の文字列（以下，攻撃文字列）と SQL インジェクション攻撃でない文字列（以下，正常文字列）を解析し，それぞれの文字列がもつ特徴を表す分布について調査した．SQL インジェクション攻撃では悪意のある SQL クエリを通常の SQL クエリに追加するという手法が多いため，そのようなことを実現するためにはいくつかの特殊な記号を利用する機会が必然的に多くなる傾向がある．以上のことから SQL クエリに頻出する記号に着目し，データ解析のために収集したサンプルデータに対して攻撃文字列と正常文字列の記号の出現頻度を調べることを試みた．その結果，出現頻度の多い記号に $1, 2, \cdots$ とラベル付けし，そのラベルを横軸にとり，その記号の出現頻度を縦軸にとったところ，攻撃文字列の分布はゼータ分布の形に近いものになることを確認した．

2.SQL インジェクション攻撃

データベース駆動型の Web アプリケーションでは，ユーザの Web ページの入力にしたがって SQL 文が生成される仕組みになっていることが多い．Web アプリケーションの開発時に，開発者がユーザの入力をすべて想定することは難しいことであるが，SQL の文法には特殊な記号を用いることで一度 SQL 文を区切り，その後に他の SQL クエリを追加することができる Web アプリケーションも存在する．したがって，SQL インジェクション攻撃の対策が不十分な Web アプリケーションでは，Web ページに上記のようなことを実現する入力がなされた場合に Web アプリケーションのデータベースに不正にアクセスされてしまう危険性が存在することになる．その他の SQL インジェクション攻撃についても，エンコード化などの特殊なケースを除けば，攻撃に区切り文字の役割をもつ特殊な記号が用いられることが多いという特徴をもっている．本研究では，SQL インジェクションがもつ記号の性質をゼータ関数を用いて調べていく．

3. ゼータ分布

x を自然数，a を 1 より大きな実数とする．このとき，

$$p(x|a) = \frac{1}{\zeta(a)x^a} \tag{1}$$

で定義される確率分布をゼータ分布という．ここで $\zeta(a)$ はリーマン・ゼータ関数であり，

$$\zeta(a) = \sum_{x=1}^{\infty} \frac{1}{x^a} \tag{2}$$

と定義される．ゼータ分布は Zipf's の法則 [3] [4] という名前で知られており，経済学や社会学におけるデータの性質を表すものとして利用されている．

4.SQL インジェクション攻撃の記号の分布

本章では [5], [6] などから収集した 624 個の SQL インジェクションの攻撃文字列に含まれる記号の出現頻度に関する分布について調べる．また，攻撃文字列の記号の分布の特徴を調べるために，正常文字列の記号の分布についても調べる．正常文字列は住所・電話番号・メールアドレス・顔文字・Wiki 文法など，Web ページのフォームに入力される文字列を想定して 234 個の正常文字列を人工的に生成した．攻撃文字列と正常文字列の特徴を分析するために図 1, 2 の横軸にある 22 個の記号を利用した．記号の出現頻度の高い順に $1, 2, 3, \cdots, 22$ とラベル付けをそれをグラフの横軸にとり，グラフの縦軸を

$$T(s_j) = \sum_{i=1}^{I} \frac{x_i(s_j)}{|l_i| \cdot I},$$

として表したものが図 1 と図 2 である．ここで l_i は文字列，$|l_i|$ は文字列長，I はデータ数，s_j は記号を表し，$x_i(s_j)$ は文字列 l_i における記号 s_j の出現頻度を表すものとする．

攻撃文字列と正常文字列の分布を比較すると，正常文字列に顔文字や Wiki の文法に含めたために出現頻度は異なるものの攻撃文字列にも正常文字列にも同じような記号が利用されていることがわかる．したがって，入力文字制限やリスティング方式による攻撃の検出法では攻撃を正常と判断したり，正常を攻撃と誤って検出する可能性が高くなることが推察される．

5. 考察

前章では SQL インジェクションの攻撃文字列と正常文字列に含まれる記号の分布を図 1，2 に示した．本章

†静岡理工科大学総合情報学部コンピュータシステム学科

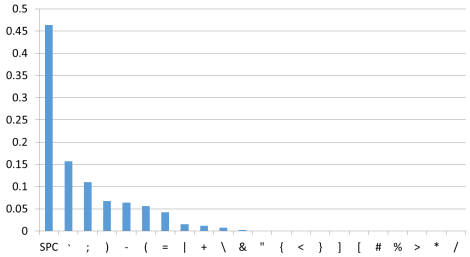

図 1: 攻撃文字列中の記号の分布

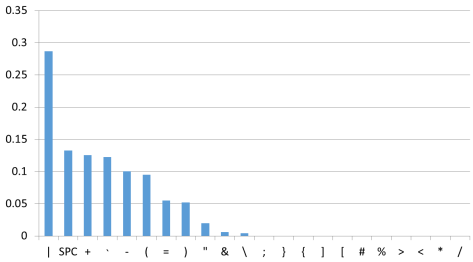

図 2: 正常文字列中の記号の分布

では攻撃文字列と正常文字列の記号の分布がもつ性質を調べていく．いま，文字列に含まれる記号の分布が $q(x)$ という確率分布で表されているとする．確率分布 $q(x)$ は未知であるため，確率分布 $p(x|\theta)$ を用いて $q(x)$ を近似する関数を探すという問題を考える．ここで θ は確率分布のパラメータであり，$\theta \in \mathbf{R}^d$ であると仮定する．2 つの確率分布の差を測るものは様々なものが考えられるが，本研究ではカルバック情報量

$$\mathbf{KL}(\theta) = \sum_x q(x) \log \frac{q(x)}{p(x|\theta)}$$

を用いる．任意の確率分布 $q(x), p(x|\theta)$ に対して $\mathbf{KL}(\theta) \geq 0$ となることと，$q(x) = p(x|\theta)$ のときに $\mathbf{KL}(\theta) = 0$ となることから，$\mathbf{KL}(\theta)$ を最小にする $p(x|\theta)$ と $\theta \in \mathbf{R}^d$ を見つけることが $q(x)$ を近似する関数 $p(x|\theta)$ を求めることになる．$p(x|a)$ を 3 章で定義したゼータ分布として $\mathbf{KL}(a)$ を考えると，$\mathbf{KL}(a)$ は唯一の最小値をもつことが分かり [7]，図 1 で与えられるデータを用いて $\mathbf{KL}(a)$ を計算すると $a \in [2.1, 2.3]$ で最小値をとることを確認することができる [7]．さらに，$\mathbf{KL}(a)$ の値は $a = 2.2$ の近くで最小となり，$\mathbf{KL}(2.2)$ の値は近似的に 0.2524 となることが分かった．$\mathbf{KL}(a)$ の計算にはゼータ関数の計算が必要であるが，実数におけるゼータ関数の値は偶数や奇数などの特殊値以外のものを求めることは非常に困難である．そこで本論文では，$\mathbf{KL}(2.2)$ の値を $\mathbf{KL}(a)$ の最小値として扱うこととする．$\mathbf{KL}(2.2)$ の値はおよそ 0.2524 であることから，ゼータ分布 $p(x|2.2)$ は攻撃文字列の分布 $q(x)$ を近似する関数といっても問題はないと考えられるが，他の確率分布を用いて $q(x)$ を近似した場合についても比較実験のために示すこととする．図 1 は横軸の値が小さいときに大きな値をとる関数といえ，ポアソン分布も同様な傾向をもつ関数であることから

$$p(x|\lambda) = \frac{\lambda^x e^{-\lambda}}{x!}$$

として，パラメータ λ は最尤推定量 $\lambda_{\mathrm{m.l.e}} = 2.4464$ を用いて $\mathbf{KL}(\lambda_{\mathrm{m.l.e}})$ を計算すると，

$$\mathbf{KL}(\lambda_{\mathrm{m.l.e}}) = 0.3812$$

となった．さらに，$\mathbf{KL}(\lambda)$ の値は数値実験の結果 $\mathbf{KL}(\lambda_{\mathrm{m.l.e}})$ の付近で極小値に近い値であることが確認できたため，今回の実験においてはポアソン分布よりもゼータ分布の方がカルバック情報量を小さくするという意味で攻撃文字列の記号の分布を近似していると言える．

6. まとめと今後の課題

本研究では，SQL インジェクション攻撃の攻撃文字列と正常文字列に含まれる記号の分布を調べ，攻撃文字列の記号の分布をゼータ分布で近似する手法を提案した．今後の課題として正常文字列の分析と，記号の分布の特徴を活かした攻撃検出法を確立することなどが挙げられる．

参考文献

[1] Yi Wang, Zhoujun Li *SQL Injection Detection via Program Tracing and Machine Learning*, Internet and Distributed Computing Systems, Lecture Notes in Computer Science Volume 7646, pp 264-274, 2012.

[2] R. Komiya, I. Paik, M. Hisada, *Classification of malicious web code by machine learning*, IEEE 3rd International Conference on Awareness Science and Technology, 406-411, 2011.

[3] Clauset, A., Shalizi, C. R., Newman, M. E. J. *Power-law distributions in empirical data*, SIAM Review 51, pp.661-703, 2009.

[4] Saichev, A., Malevergne, Y., Sornette, D. *Theory of Zipf's law and beyond* Lecture Notes in Economics and Mathematical Systems 632, Springer, Heidelberg, Germany, 2010.

[5] Justin Clarke,: *SQL Injection Attacks And Defense*, Syngress Publishing Inc., 2009.

[6] *SQL Injection Cheat Sheet*, http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/.

[7] Takeshi Matsuda, *Feature Extraction of Web Application Attacks Based on Zeta Distribution* World Congress on Internet Security (WorldCIS-2013) (To Appear)