Phishing URL 攻撃パターンの自動分類とその評価

山本 悠太 †　　菊池 浩明 †

明治大学 総合数理学部 先端メディアサイエンス学科 †

1　研究背景

近年フィッシング攻撃による被害は増加傾向を取り続けている. 佐野 [1] によると, 2022 年度は 968,832 件のフィッシングサイトが報告されており, これは前年度の約 2 倍にも上る. フィッシングに用いられる URL には, 打ち間違いを想定したものや IP アドレスを直接指定するものなど多岐にわたっている.

そこで, 本稿では, それらの攻撃手法を割り出して攻撃者の傾向を掴み, フィッシング対策へ活用することを目的とし, JPCERT より提示された最新の Phishing URL 群 [3] に対し攻撃手法パターンについての分析を行う. Phishtank[4] によって提示されたグローバルな URL 群についても同様に分析をし, 海外と日本の差を明らかにする.

2　攻撃パターン自動分類機構

本研究では与えられた Phishing URL に対し, その攻撃手法がタイポスクワッティング, コンボスクワッティング, IP アドレス挿入, ランダム文字攻撃, その他の 5 つの分類のうちどれに属するかを判別する. 本分類は佐野による分類である. [1]

分類にはその他を除く各分類につき 1 つずつ作成した, 4 つの検出モジュールを用いる.

2.1　タイポスクワッティング検知モジュール

タイポスクワッティングは, 攻撃者が正規のブランド名へとアクセスする際の打ち間違いを期待して, 正規のブランド名から一部分を変更した文字列を持たせた URL を生成する攻撃手法である. 正規ブランドと Phishing URL のドメイン部間のレーベンシュタイン距離 d をとり, d が閾値を下回る場合をタイポスクワッティング攻撃と分類する.

レーベンシュタイン距離 [2] とは, 2 つの文字列 x, x' について, x を x' に変換するのに必要な削除, 挿入, 置換の数である. 例えば x ='levenshtein', x ='levanshte' とすると, x を x' にするために必要な操作は置換 1 回, 挿入 2 回であるため, レーベンシュタイン距離 d は $d = 3$ となる. 本稿では正規ブランド名とのレーベンシュタイン距離 d が $d \leq 2$ を満たす場合, タイポスクワッティングとみなした.

2.2　コンボスクワッティング検知モジュール

コンボスクワッティングは, 正規のブランド名に一見信頼できる単語を付加する攻撃手法である. 正規ブランド名にコンボスクワッティングで比較的高頻度で用いられる単語を付加していた場合に検知する.

2.3　IP アドレス挿入検知モジュール

IP アドレス挿入は, URL に直接 IP アドレスを挿入する URL 作成手法である. URL が数字と特殊文字列のみで構成されている場合に検知する.

2.4　ランダム文字攻撃検知モジュール

ランダム文字攻撃は, ランダムに生成された文字列を作成する手法である. 文字列 $a_1, a_2, .., a_n$ について k 次の文字遷移確率を $p = P_r[a_1|a_2, .., a_k]$ とする. 全ての部分文字列について $p < 0.075$ の時, ランダム文字攻撃と判定する. 本稿では URL 文字列のドメイン部について, 文字遷移確率 p を計算する Python ライブラリ texttrans を用いた.

以上 4 つの分類に含まれない Phishing URL を「その他」の分類とする.

3　実験

3.1　プログラムと実験の流れ

本実験は JPCERT によって提示された最新の Phishing URL 群 [3] を用いる. 2019 年 3 月から 2023 年 9 月までの 55 か月間のデータに含まれている Phishing URL 群について自動分類を行う. 検知に使用する正規ブランド名のリストは Python ライブラリの request と Beautifulsoup を用いて, 与えられた Phishing URL の偽装元である正規ブランド名について, google 検索を行い,

---

Analysis and Automatic classification of Phishing URL generation patterns,

†Yuta Yamamoto and Hiroaki Kikuchi.

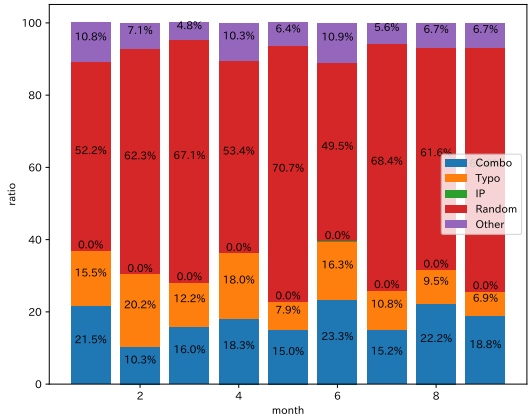

図 1　2019 年の攻撃手法比率

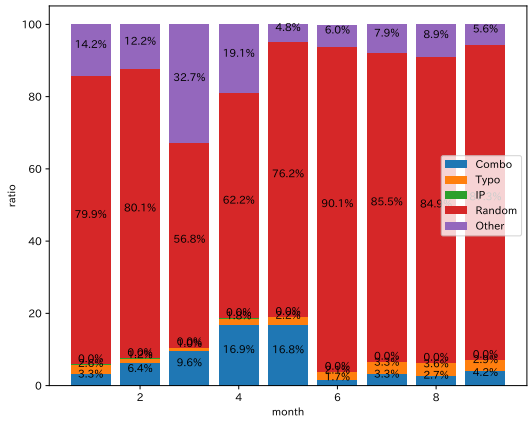

図 2　2023 年の攻撃手法比率

その結果の一番上位のサイトのドメイン部を自動収集する方法で作成する．Phishtank[4] から得た 2023 年 12 月以前の最新 38,962 件の Phishing URL 群についても同様の分類を行い, 2023 年 9 月度の JPCERT の URL 群 6,024 件との比較を行う。

3.2　結果

攻撃手法の自動分類の結果を図 1(2019 年度), 図 2(2023 年度) に示す。図に示すように, 2019 年, 2023 年ともに最も大きい割合を占める手法はランダム文字である．2019 年度では平均 20 %の割合を占めていたタイポスクワッティング, コンボスクワッティングの手法が, 2023 年度では 10 %にまで減少している．本検知機構で判別できなかったその他の攻撃手法は, 2019 年から 2023 年にかけて 2 倍程度に増加している．

Phishtank と JPCERT データセットの各攻撃手法の占める割合を表 1 に示す．JPCERT に代表される日本の Phishing URL は, タイポスクワッティング攻撃の割合が Phishtank よりも 20 %程度低く, ランダム文字攻撃が 20 %程度高い．

表 1　Phishtank と JPCERT 最新の攻撃手法割合比較 (単位: %)

	Typo	Combo	IP	Random	Other
JPCERT	5.4	6.9	0.0	82.6	5.0
Phishtank	24.8	6.8	0.0	59.3	9.1

3.3　考察

実験から得られた結果から, 攻撃者の用いている Phishing URL 生成手法は大きく変遷していることがわかった．[1] で示されていた結果や 2019 年の分析と, 2023 年の分析とを比較すると, ランダム文字攻撃, その他の割合が増加している．その他の割合が増加しているのは, 提案方式では分類できない新しい手法が多く出現していることが原因と推察する．

海外と日本国内の Phishing URL 攻撃手法の傾向の差は．ランダム文字攻撃, タイポスクワッティング攻撃の割合であった．地域による攻撃者の傾向の差によるものに加え, 判定に用いた辞書が不十分であったと推察する．

4　結論

本稿では攻撃者の傾向がどのように変遷しているかについて掴むことができた．しかし, 作成した辞書と, 検知モジュールの網羅性に不十分な点が発見されたため, これら 2 点を改善することを今後の課題とする．

参考文献

[1] 佐野 智弥, “最近のフィッシング URL の生成手口を分析！よくある攻撃パターンとは？”（https://www.lac.co.jp/lacwatch/people/20230303_003297.html, 2023 年 10 月参照）

[2] Rishin Haldar, Debajyoti Mukhopadhyay, Levenshtein Distance Technique in Dictionary Lookup Methods: An Improved Approach, (https://doi.org/10.48550/arXiv.1101.1232, 2011).

[3] JPCERT/CC Phishing URL dataset (https://github.com/JPCERTCC/phishurl-list/, 2023 年 10 月参照)

[4] PhishTank (https://phishtank.org, 2023 年 11 月参照)