

読者の心的態度を用いた文章の構造分析による 詐欺特徴の抽出に関する研究

A Study on Extracting Scam Features by Structural Analysis of Texts
Using Readers' Mental Attitudes

藤巻 壮・ネットワーク分科会・中央大学

With the rapid development of technology, phishing is becoming more and more of a threat every year as more and more personal information is handled on the Internet. With the spread of generative AI, even non-technical people or people living abroad can easily create phishing e-mails in other languages. Although various countermeasures against phishing e-mails are still in use, they are mainly based on header information and URLs, and attackers are using various methods to escape from these countermeasures. We analyzed phishing e-mails by defining the mental attitude that readers feel when they read the text, and analyzed the differences in characteristics between normal e-mails and fraudulent e-mails.

研究背景・目的

SlashNext社の調査[1]によると、ChatGPTのリリース後、フィッシングメールの件数が1,265%増加したことが判明した。
→フィッシングの脅威は年々高まっている。

フィッシングメールには、

- ・ 受信者を焦らせて情報を送信させる
 - ・ 受信者にメリットを提示して情報を送信させる
- といった構造的な特徴がある。

本研究では、このような特徴を抽出することで、正常メールと詐欺メールの分類、その特徴差異の分析を行う。

心的態度の定義

	心的態度	単語例
1	導入	いつも、日頃
2	依頼	ください
3	理由	そのため、ため、により
4	強制	必要
5	示唆	場合
6	不利益	解約、停止、できなくなる
7	了承	ご了承
8	完了	しました
9	提示	お知らせ、ご覧
10	待機	お待ち

これらのラベルをメール中の単語に対して付与し、

- ・ ラベルの頻度ベクトル
 - ・ ラベルの2-gramによる頻度ベクトル
- に変換し、メールの分類を行う。

参考文献

[1] | SlashNext, SlashNext, <https://slashnext.com/press-release/slashnexts-2023-state-of-phishing-report-reveals-a-1265-increase-in-phishing-emails-since-the-launch-of-chatgpt-in-november-2022-signaling-a-new-era-of-cybercrime-fueled-by-generative-ai/>

分類結果

分類精度は層化3分割交差検証により計測した。

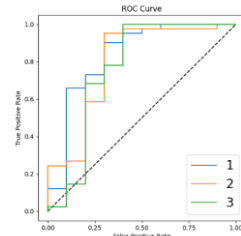


図1. ラベル頻度による分類のROC曲線

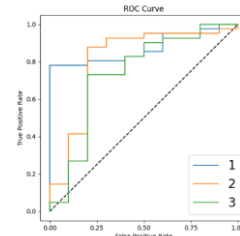


図2. 2-gramによる分類のROC曲線

特徴ベクトル	Accur acy	Precisi on	Recall	F1 Score	AUC
頻度	0.86	0.90	0.94	0.92	0.80
2-gram	0.81	0.86	0.91	0.89	0.81

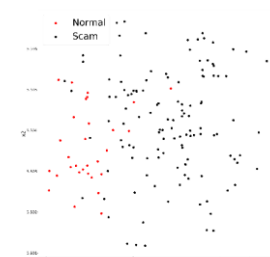


図1. ラベル頻度のUMAPIによる可視化

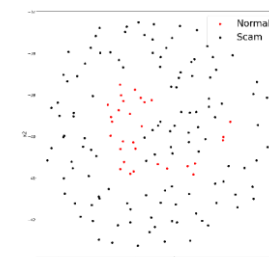


図2. 2-gramのUMAPIによる可視化

統計的因果探索

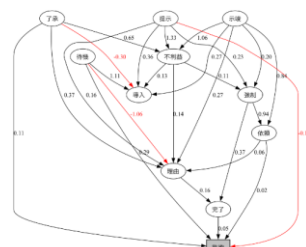


図1. ラベル頻度によるLiNGAMの因果グラフ

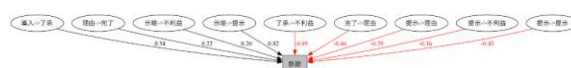


図2. 2-gramによるLiNGAMの因果グラフ