情報処理実習２：レポート

（フィッシングマイル）

4Ｊ ３８番　トーゴー

１．はじめに

企業や省庁、教育機関において、情報セキュリティ対策は必要不可欠なものとなっている。サイバー攻撃は高度化し、防ぐことが難しくなっており、日本では情報セキュリティ人材の不足が問題になっており、セキュリティ人材の育成が必要となっている。今回の実習では、サイバー攻撃の中でも特に多いフィッシング攻撃への対処法について、私たちが分析した。

背景

フィッシングとは、偽装されたメールを武器とするサイバー攻撃である。その目的は、メールの受信者を、例えば銀行からの依頼や会社の人からのメモなど、自分の欲しいものや必要なものであると信じ込ませ、リンクをクリックさせたり、添付ファイルをダウンロードさせたりすることにある。フィッシングと本当に違うのは、メッセージの形式だ。攻撃者はある種の信頼できる団体を装い、多くの場合、実在の人物、あるいは被害者が取引している可能性のある企業を装いる。フィッシングは、1990 年代までさかのぼる最も古いサイバー攻撃の一つだが、現在でも最も広く、悪質な攻撃の一つであり、フィッシングのメッセージや手法はますます洗練されてきている。[1]

目的

私たちの目標は、フィッシングメールを検証し、以下の疑問に対する答えを見つけることだった：

- フィッシングメールを観察しているとき、メールのどの部分を観察しているのか？
- フィッシングメールを見分けることができる人は、どこを見ているのか？
- フィッシングメールを見分けることができる人とできない人では、目の位置に違いがあるのか？

２．手法

２．１．装置

眼球運動計測装置として図 1 に示した「Tobii Pro スペクトラム」を使用した。図 1 のディスプレイ の下に設置されている装置が眼球運動計測装置である。最大で 300Hz で視線位置を計測できるが、今回 は 120Hz に設定した。実験プログラムは Tobii Pro Lab によって作成した。

図 1：Tobii Pro スペクトラム

２．２．呈示刺激

呈示刺激として、Gmail の迷惑メールフィルタで迷惑メールと判定されたメールを使用した。メールフ ァイルはメーラー（Thunderbird）で開き、そのスクリーンショットが刺激として呈示された。メール内 のリンクは、その URL をテキストボックスで明記した。

２．３．実験手続き

被験者はディスプレイの前に座り、頭部をアゴ台に載せて固定した。その後、電子メールの画像が呈示され、そのメールが怪しいメールかどうか判断し、カーソルキーで応答した。 電子メールの画像を判断している最中の視線位置を眼球運動計測装置で計測した。実験開始時に眼球 運動計測装置のキャリブレーションが実行された。 電子メールは 15 通呈示され、そのうち 10 通はフィッシングメールであり、5 通は

通常のメールであ った。実験中、電子メールの呈示順序は固定されていた。

２．４．解析方法

眼球運動計測装置の計測データを tsv ファイル（実験時に配布するのは csv ファイル）にエクスポート し、Google Colaboratory（Python）で解析した。

２．５．被験者

被験者は一関高専４J、５S の学生だった。被験者は事前に実験についてインフォームドコンセントを受け、実験目的や実験の危険性について説明を受けた。実験に参加した被験者のうち 1 名（ID000）は実 験者であり、今回の実験プログラムを作成した。

3. 計測データのまとめ

3. １．計測データ

眼球運動計測装置の計測データは表 1 のように行方向に計測時間（タイムスタンプ）、列方向に各種情報（データラベル）が記録されている。実験中のすべてのデータが記録されているため、実際にメールを読んでいる期間以外のデータも記録されている。

表 1：計測データの一部分

	Recording timestamp	Participant name	Recording duration	Recording resolution height	Recording resolution width	Average calibration accuracy (pixels)	...
0	0	ID000	207924	1080	1920	14	
1	122772	ID000	207924	1080	1920	14	
2	122772	ID000	207924	1080	1920	14	

計測データは大量の情報を出力するため、今回は演習に必要な情報に絞り、csv ファイルに変換し

た。今回使用するデータラベルを下記に列挙する。

- Recording timestamp:　レコード中のタイムスタンプ　[µs]
- Recording date: レコード月 日
- Participant name: 被験者 名
- Recording duration: 総レコード時間 [ms]
- Recording resolution height: データ分解能（高さ）　[pix]
- Recording resolution width: データ分解能（幅）　[pix]
- Average calibration accuracy (pixels): キャリブレーション正確度 [pix]
- Average calibration precision SD (pixels): キャリブレーション精度 [pix]
- Event: イベント（キーボード押し、刺激呈示など）
- Event value: イベント詳細（どのキーボード入力か？どの刺激呈示か？など）
- Gaze point X:　視線位置（X 方向）左上が [0, 0]
- Gaze point Y: 視線位置（Y 方向）
- Presented Media name: 提示されていたメディア名（画像ファイル名など）
- Eye movement type:　眼球運動の分類
    - Fixation:　固視
    - Saccade: サッケード（見たい物を網膜中心で捉えるための急速眼球運動）

- EyesNotFound: 眼球が観測てきていない（瞬きやキャリブレーション精度が悪いために生じる）

3. 2. 被験者応答「課題１」

今回の実験において、被験者キーボード応答を使用してフィッシングメールかどうか判断した。メールが怪しくないと思ったら左（Left）、怪しいと思ったら右（Right）と応答するように教示した。これら被験者応答はデータラベルの「Event Value」に記録されている。

被験者の応答結果について、パフォーマンスを計算をするため表 2 に示した被験者応答の分類を計算し、正答率・適合率・再現率・F 値を計算した。「課題１」

表２：被験者応答の分類（いわゆる混同行列）

		実際の分類結果	
		フィッシングメール	フィッシングメールではない
被験者の予測結果応答	怪しい	TP (True Positive)	FP (False Positive)
	怪しくない	FN (False Negative)	TN (True Negative)

正答率（Accuracy）

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

適合率　(Precision)

再現率（Recall）

$$Recall = \frac{TP}{TP + FN}$$

F 値（F-measure）

$$F = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall}$$

被験者はディスプレイの前に座り、頭部をアゴ台に載せて固定した。その後、電子メールの画像が呈示され、そのメールが怪しいメールかどうか判断し、カーソルキーで応答した。 電子メールの画像を判断している最中の視線位置を眼球運動計測装置で計測した。実験開始時に眼球 運動計測装置のキャリブレーションが実行された。 電子メールは 15 通呈示され、そのうち 10 通はフィッシングメールであり、5 通は通常のメールであ った。実験中、電子メールの呈示順序は固定されていた。

3. 3. TOI（Time Of Interest）「課題 2」

計測データはメールを読んでいる期間以外のデータも記録されている。従って、メールを読んでいる期間を抽出する必要がある。このように、実験目的に沿ったデータ期間を Time Of Interest（TOI）という。今回のデータの場合、データラベル「Presented Media name」でフィルタリングすれば電子メールを読んでいる期間を抽出できる。

今回使用した画像のファイル名を下記に列挙する。

- 01_Kyoumu_T.png
- 02_Amazon2_F.png
- 03_Amazon3_F.png
- 04_Rakuten2_F.png
- 05_ticket_T.png
- 06_Rakuten_F.png
- 07_Rakuten_T.png
- 08_yodobasi_F.png
- 09_Apple_F.png
- 10_Kankou_T.png
- 11_LINE_F.png
- 12_Kyufu2_F.png

- 13_ponta_T.png
- 14_Kyufu_F.png
- 15_SMBC_F.png

「課題２」抽出した TOI から視線位置をプロットし、また、ヒートマップを作製する。ヒートマップは実際の呈示刺激画像と重ね合わせ、どのような部分を観察していたかわかるようにする。

３．４．AOI（Area Of Interest）「課題３」

ヒートマップの作製によって、画像刺激でどこに視線が集中していたのかがわかった。それでは、画像に含まれる特定の情報にどの程度視線が集中していたのだろうか？これを解析するのが Area Of Interest（AOI）である。今回は、Tobii Pro の機能で AOI を設定した。AOI として設定したのは、

- Header：差出人などのヘッダー
- HeaderTime：受信日時
- Footer：署名などのフッター
- URL：本文中のリンク（画像によって最大 URL 4

まである）の 4 つである。

AOI にはいくつか種類があるが今回は「Total_duration_of_fixations」に注目する。Total_duration_of_fixations は AOI の範囲で視線が固定された総時間 [ms] である。従って、どの程度AOI の部分を観察し

ていたかが定量化できる。

解析するときは各画像刺激の AOI の値を平均したいが、そもそも各画像刺激を観察していた時間が異なる。従って、各画像刺激を観察していた総時間で各 AOI を正規化することで平均を算出する。

「課題 3」各 AOI を画像刺激間で平均し、被験者ごとの AOI 時間を記録せよ。記録するときは課題 1 で作成した被験者のパフォーマンスのシートを使用する。

４．結果

フィッシングメールを見ているときに、視線はどこに集中しているかを強調するため、ヒートマップで 18 人の受験者の視線位置を使って示した。そして被験者の応答結果について、パフォーマンスを計算をするため被験者応答の分類を計算し、正答率・適合率・再現率・F 値を計算した「課題１」。次には計測データはメールを読んでいる期間以外のデータも記録されている。従って、メールを読んでいる期間を抽出し抽出した TOI から視線位置をプロットし、また、ヒートマップを作製した「課題 2 と 3」。最後には横軸を被験者パフォーマンス、縦軸を AOI として散布図を作り相関解析した「課題 4」。

４．１．課題「１」の結果

/ID１０１の被験者に関している例として一個だけのデータを表示した/

被験者の応答結果についてパフォーマンスの計算：

TP＝１０　　Accuracy: 1.0

FN＝０　　Precision: 1.0

FP＝０　　Recall:1.0

TN＝５　　Fmeasure:1.0

４．２．課題「２」の結果

/ID１０１の被験者に関している例として一個だけのデータを表示した/

視線位置のプロット:

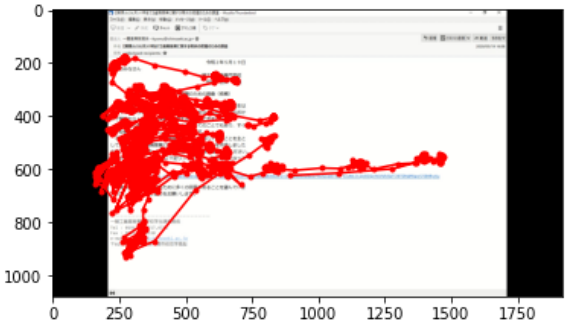


図１

Ｉヒートマップの作製：

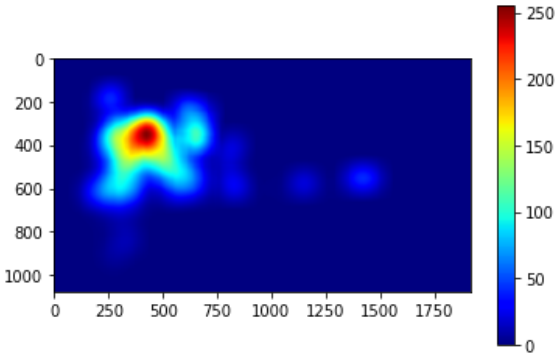


図３．１

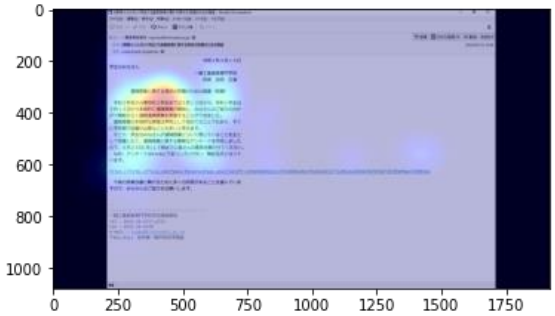


図３．２

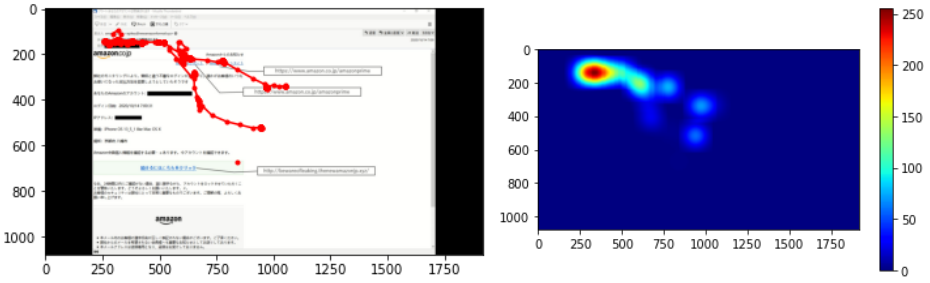
エラー：

ヒートマップを作る時出たエラー：

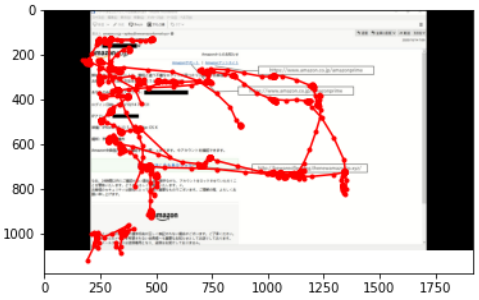
コード：`heatmap[yy, xx] = heatmap[yy, xx] + 1` には

エラー：`IndexError: index 1090 is out of bounds for axis 0 with size 1080`

普通に視線位置が次のように出ている時ヒートマップがうまくつくられる：



エラーが発生する場合は次の時：



ヒートマップを作る時のエラーは視線位置のフレームがあってないと思ったけど解決をできませんでした。

４．３．課題「３」の結果

AOI の解析

TOI	Header	Header time	Footer	URL
01_Kyoumu_T	0.000000	0.0	0.007075	0.015566
02_Amazon2_F	0.000000	0.0	0.000000	0.145524
03_Amazon3_F	0.000000	0.0	0.000000	0.000000
04_Rakuten2_F	0.000000	0.0	0.000000	0.215935
05_ticket_T	0.000000	0.0	0.000000	0.054339
06_Rakuten_F	0.000000	0.0	0.000000	0.143761
07_Rakuten_T	0.000000	0.0	0.000000	0.040495
08_yodobasi_F	0.000000	0.0	0.000000	0.000000
09_Apple_F	0.000000	0.0	0.000000	0.069101
10_Kankou_T	0.000000	0.0	0.000000	0.026421
11_LINE_F	0.000000	0.0	0.000000	0.108794
12_Kyufu2_F	0.000000	0.0	0.000000	0.019404
13_ponta_T	0.024651	0.0	0.001380	0.009022
14_Kyufu_F	0.000000	0.0	0.000000	0.087385

15_SMBC_F	0.000000	0.0	0.000000	0.008571
01_Kyoumu_T	0.000000	0.0	0.007075	0.015566
02_Amazon2_F	0.000000	0.0	0.000000	0.145524

表３

/ID１０１の被験者に関している例として一個だけのデータの表を示した/

４．４．課題「４」の結果

横軸を被験者パフォーマンス、縦軸を AOI として散布図():

ID	Accuracy	Precision	Recall	F-measure	TP	FN	FP	TN	KM	Header	HeaderTime	Footer	URL
0	1	1	1	1	10	0	0	4	1	0.161	0.11	0.010857	0.061108
101	1	1	1	1	10	0	0	5		0.001	0	0.000564	0.062954
104	1	1	1	1	10	0	0	5		0.162	0.016	0.008084	0.056517
7	1	1	1	1	10	0	0	5		0.277	0.002	0.010344	0.121632
5	0.93	1	0.9	0.95	9	1	0	5		0.133	0.004	0.010651	0.038228
1	0.867	0.83	1	0.91	10	0	2	3		0.336	0.037	0.008798	0.068012
4	0.867	0.9	0.9	0.9	9	1	1	4		0.074	0.008	0.006482	0.053351
103	0.8	1	0.7	0.82	7	3	0	5		0.046	0	0.007157	0.102572
105	0.8	1	0.7	0.82	7	3	0	5		0.08	0.001	0.00208	0.102621
8	0.8	1	0.7	0.82	7	3	0	5		0.126	0.012	0.017656	0.089009
0	1	1	1	1	10	0	0	4	1	0.161	0.110	0.010857	0.061108
9	0.8	1	0.7	0.82	7	3	0	5		0.206	0.005	0	0.07266

12	0.79	1	0.67	0.8	6	3	0	5		0.214	0.002	0.009078	0.070306
102	0.67	0.86	0.6	0.71	6	4	1	4		0.092	0	0.008079	0.012592
3	0.67	0.86	0.6	0.71	6	4	1	4		0	0	0	0
11	0.67	1	0.5	0.67	5	5	0	5		0.158	0.002	0.011281	0.097545
2	0.6	0.83	0.5	0.625	5	5	1	4		0.113	0.037	0	0.025315
6	0.6	0.83	0.5	0.625	5	5	1	4		0.048	0.006	0.012775	0.096716

表４

相関解析・横軸を F 値、縦軸を AOI にしてプロット：

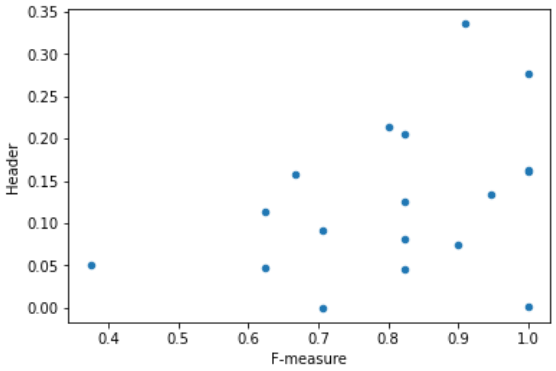


図４．１

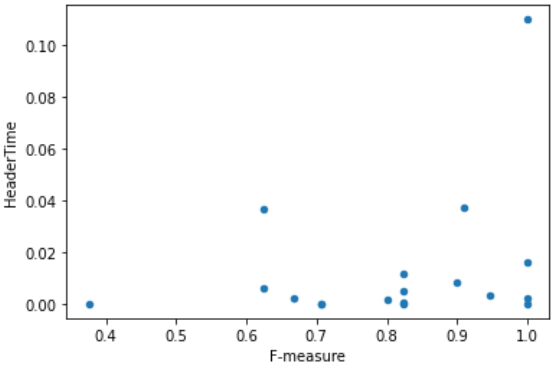


図４．２

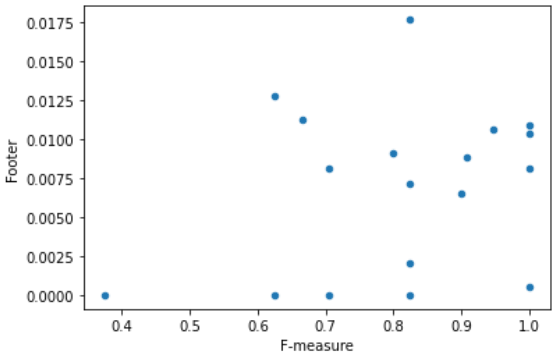


図４．３

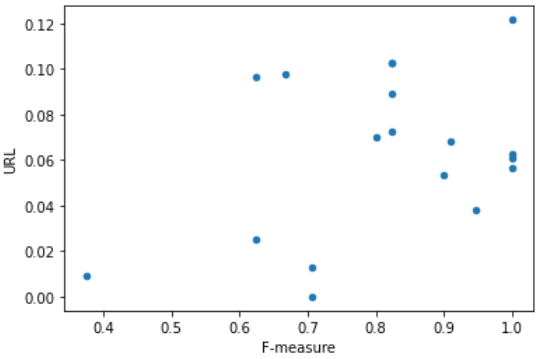


図４．４

相関係数の算出

	ID	Accuracy	Precision	Recall	F-measure	TP	FN	FP	TN	KeyMiss	Header	HeaderTime	Footer	URL
ID	1.000000	0.211111	0.243931	0.150830	0.209381	0.157917	-0.146956	-0.276720	0.329455	NaN	-0.347056	-0.284208	-0.196523	0.097231
Accuracy	0.211111	1.000000	0.788237	0.956341	0.997399	0.948628	-0.958387	-0.677029	0.598961	NaN	0.366425	0.286415	0.289176	0.401143
Precision	0.243931	0.788237	1.000000	0.584657	0.769558	0.569035	-0.591418	-0.959273	0.924053	NaN	0.237908	0.075190	0.360117	0.577496
Recall	0.150830	0.956341	0.584657	1.000000	0.965685	0.997454	-0.999350	-0.432583	0.351939	NaN	0.410077	0.342974	0.230182	0.274505
F-measure	0.209381	0.997399	0.769558	0.965685	1.000000	0.958562	-0.967414	-0.645456	0.571116	NaN	0.369036	0.281879	0.278588	0.377773
TP	0.157917	0.948628	0.569035	0.997454	0.958562	1.000000	-0.994236	-0.417392	0.336172	NaN	0.389423	0.348099	0.220861	0.268714
FN	-0.146956	-0.958387	-0.591418	-0.999350	-0.967414	-0.994236	1.000000	0.439422	-0.359225	NaN	-0.419720	-0.339720	-0.234446	-0.276900
FP	-0.276720	-0.677029	-0.959273	-0.432583	-0.645456	-0.417392	0.439422	1.000000	-0.961820	NaN	-0.088289	-0.021727	-0.310390	-0.547722
TN	0.329455	0.598961	0.924053	0.351939	0.571116	0.336172	-0.359225	-0.961820	1.000000	NaN	0.062756	-0.228220	0.260510	0.555795
KeyMiss	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN
Header	-0.347056	0.366425	0.237908	0.410077	0.369036	0.389423	-0.419720	-0.088289	0.062756	NaN	1.000000	0.279440	0.354547	0.349522
HeaderTime	-0.284208	0.286415	0.075190	0.342974	0.281879	0.348099	-0.339720	-0.021727	-0.228220	NaN	0.279440	1.000000	0.178385	-0.060356
Footer	-0.196523	0.289176	0.360117	0.230182	0.278588	0.220861	-0.234446	-0.310390	0.260510	NaN	0.354547	0.178385	1.000000	0.474583
URL	0.097231	0.401143	0.577496	0.274505	0.377773	0.268714	-0.276900	-0.547722	0.555795	NaN	0.349522	-0.060356	0.474583	1.000000

表 5

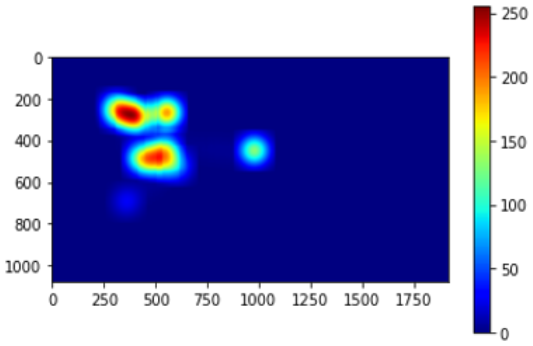
５．考察

まず、表 4 からフィッシングメールの認識が得意な人を調べ、正確さと精度のスコアが 1 の ID104 と ID007 を選んで、フィッシングメールの見分けがつかない人を正確さと精度のスコアが低い ID010 と ID002 を選んで検討した。

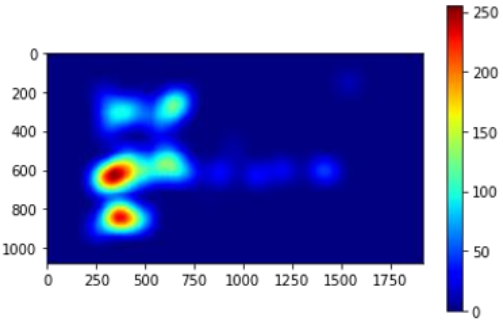
そして、その四人のヒートマップを比べてみた（以下の 4 個図）。ヒートマップからわかるように、ID104 と ID007 は主に URL に注目しているのに対し、ID010 は主にメールの主要部分、ID002 はメールの下部を見ていることがわかった。このことから、URL はメールの信頼性を証明することができると推測された。そして、いろいろな被験者のヒートマップを作って見たのに判断出来なかった。けれども、検討中解析対象外（ID003）が出てきてその理由を調べたところ視線位置の情報(Gaze point X, Gaze point Y)が取得できず、正しい視線位置のプロット、ヒートマップの作成ができなかったからだった。その理由を「メガネの反射

で正しい測定ができなかった」私たち判断した。

正答率低い

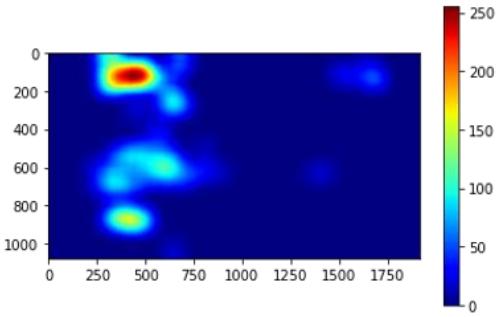


被験者ID010

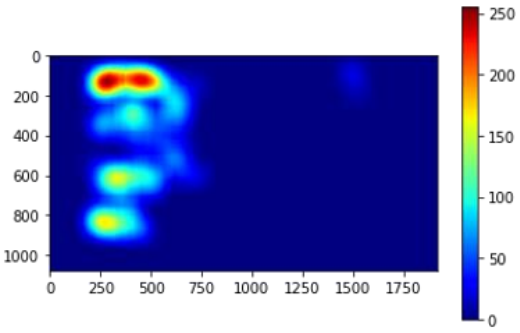


被験者ID002

正答率高い



被験者ID104



被験者ID107

そこで、この仮定が正しいかどうかを確認するために、 相関解析・横軸を F 値、縦軸を AOI にしてのプ

ロット（図４． １から 図４． ４）と相関係数の算出の表を検討した。 図 ４． １ （ヘッダー、F 値）と図 ４． ３ （フッター、F 値）からは、プロットが均等に分かれているため、明確に結論を出すことができなかったが、図４． 2 (headertime, F 値)と図 4.4(URL, F 値)では、変数間の相関が明瞭に見て取れる。しかし、headertime と F 値は、多少関係があっても、それを裏付けるようなものは見つからなかったので落とした。しかし、F 値と URL の相関は図４． 4 には明らかにみえるため、「URL を見ている時間が長いほど、フィッシングメールを見分ける精度が高くなる」ということを言える。また、表 5 （相関係数の算出）から、Accuracy、Precision と URL の相関はそれぞれ 0.401143、0.577496 と最も高いことがわかる。URL と Accuracy の関係、F 値と URL の関係、またはヒートマップから、URL はフィッシングメールを認識するために最も重要な部分であると結論した。

　または、ヒートマップと原画を比較することで、URL 以外のフィッシングメールを見分ける別の手がかりを探した。見分けがつきやすいメールを調べてみると、そのメールには独特のデザインが施されていることがわかった。例えば、次のような大きなボタンや奇妙な色など。

正答率が最も高い画像(15_SMBC_F_Stim.png)

正答率が最も低い画像(01_Kyoumu_T_Stim.png)

従って被験者応答の分類を計算し、正答率・適合率・再現率・F 値の計算、抽出した TOI から視線位置のプロット、ヒートマップの作成、または相関解析を使って分析した。その上フィッシングマイルを見分けるため送ってきたマイルの内容へ進む前 URL を確認し、奇妙なデザインを持っているかを検索した後マイルに反応をすればフィッシング攻撃を防止できると私たちが思った。

参考文献

[1] https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/ 2021/12/26