Copyright ©2017 The Institute of Electronics,
Information and Communication Engineers

SCIS 2017 2017 Symposium on
Cryptography and Information Security
Naha, Japan, Jan. 24 - 27, 2017
The Institute of Electronics,
Information and Communication Engineers

認知心理学とサイバーセキュリティに関する一考察：視線分析の事例
A Consideration for Cognitive Psychology and Cybersecurity a case of eye movement

宮本大輔 *
Daisuke Miyamoto

あらまし 本研究ではエンドユーザを狙って行われるサイバー攻撃やエンドユーザによって引き起こされるインシデントについて，技術的な要因ではなく人的要因から分析し，そのために認知心理学に基づいた手法の利用について考察する．近年，様々な生体情報デバイス・バイオセンサーが普及しており，疲労やストレス，体調などの管理に役立てられている．サイバーセキュリティ分野でも生体情報を分析し，人間に内在する精神状態を推測できれば，リスキーなコンピュータ操作を防止しうるのではと考える．本研究では視線分析技術とフィッシング対策技術の関係の研究を報告し，著者らが行ってきたフィッシングサイト判別実験から検知技術及び対策技術の検討を行う．また，フィッシング対策分野以外における有効性について考察するため，サイバーセキュリティ分野でも実施可能な生体情報観測技術について議論する．

キーワード フィッシング対策, 視線分析, 認知心理学

1 はじめに

コンピュータシステムではなく，コンピュータのユーザを狙ったサイバー攻撃が行われている．フィッシング詐欺と呼ばれる攻撃では，攻撃者が銀行などの金融機関を装った偽のメールを送信し，ユーザを悪意のあるウェブサイトにおびき寄せる．攻撃者はこのウェブサイトを本物そっくりに作成することでエンドユーザを騙し，金融口座やクレジットカード番号などの情報を搾取する．標的型メール攻撃やビジネスメール詐欺と呼ばれる攻撃では，攻撃者は不特定多数のユーザではなく特定の組織に属する個人にメールを送信し，メール文面が本当の内容であると信じ込ませ，添付されているマルウェア又はマルウェアを含む文書を開かせたり，金融口座にお金を振り込ませようと試みる．

このようなエンドユーザへの攻撃に対し，サイバーセキュリティ研究者らは何十年にも渡って，危険なウェブサイトの防御やマルウェアの検知，あるいは攻撃の発信源であるボットネットのテイクダウンなど様々なアプローチで対策に取り組んできた．しかし，攻撃は未だに続いており，被害は報告され続けている．この原因には様々なものが考えられるが，技術的な側面からのサイバーセキュリティへの取り組みだけではなく，人的要因あるいは組織的要因からの取り組みが求められると考える．例えば，Hawkey らの研究グループは情報セキュリティ管理において人的要因，組織的要因，そして技術的要因の研究課題及びそれらの交絡関係について述べている [1,2]．人的要因としては，訓練や経験の不足，組織内の文化による要因，コミュニケーションに関する問題などが挙げられている．組織に所属しない個人を狙った攻撃などを考える際にも，フィッシング攻撃に対しては知識の不足が原因と言われる [3]．従って，人的要因の側面としてはサイバーセキュリティの教育を目的とした教材開発などが行われている．

一方で，認知心理学が注目を集めている．この研究領域には様々なチャレンジがあるが，その 1 つに「人間の観測される情報から，人間の精神状態を推測する」という課題がある．例えば人間の精神的負荷の高まりを眼球運動や脳波，血圧，呼吸，顔表面温度などから分析する研究が行われている．ストレスの増加など精神的負荷の高まりは過失を引き起こしやすいとされており，このような課題は人的要因の解決を行っているとも考えられる．さらに，近年の IoT 技術の普及に伴い，人間から健康に関するデータを取得する様々な生体センサーの技術開発が進んでいる．この情報を認知心理学の観点から活用すれば，情報機器を利用するユーザが今まさに何を考えているのか，どのような情報を入手し，どのような根拠

* 東京大学 情報基盤センター 〒 113-8658 東京都文京区弥生 2-11-16. Information Technology Center, the University of Tokyo, 2-11-16, Yayoi, Bunkyo-ku, Tokyo 113-8695, Japan daisu-mi@nc.u-tokyo.ac.jp

で，どのような意思決定をしようとしているのかを推測できると思われる．

これまでのサイバーセキュリティ対策では，エンドユーザがどのような状態あるかは考えていないが，仮に「まさに騙されそうな状態にあるユーザ」がわかるのであればどうか．普段は，正常なプログラムをマルウェアであると，正規サイトをフィッシングサイトであるといった誤検知を減らすべく工夫されているセキュリティ技術や製品も，この時ばかりは誤検知を承知の上で注意喚起ができるのではないか．このような工夫によって，人的要因によって起こるインシデントは減らせるのではないか．

本論文では，筆者の研究グループがこれまでに行ってきた視線分析の研究について，その学際領域の背景及びこれを利用した研究について説明する．また，視線分析に基づいてユーザごとに異なるサイバー防御を提供するシステムを提案し，この評価実験を行う．この方式の短所についても考察を行い，課題を克服する方針について説明する．さらに，生体センサーによる情報を認知科学により分析した結果をサイバーセキュリティ技術に活用する方法について，視線以外の方式についても説明し，そのために必要な要件について検討する．この上で，さらに研究を進める上でのデータセット，生体情報を分析することに対するプライバシーの懸念といった問題について議論する．

以下，2 節において視線分析に関連する技術をまとめ，3 節においてこれを活かしたフィッシングサイト対策技術について調査を行う．4 節ではこの研究を推進する諸問題について議論を行い，最後に 5 節についてまとめと今後の課題を述べる．

2 関連研究

本研究では，視線分析技術を取り上げ，認知心理学とサイバーセキュリティの関係について考察する．このため，視線分析技術の動向を 2.1 節に述べ，視線分析のアプリケーションを 2.2 節に述べ，フィッシングサイト対策の研究に活用する事例を 2.3 説に述べる．

2.1 視線分析技術

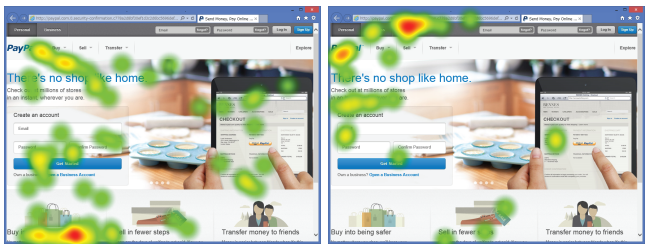
視線分析の研究は，1880 年頃に Javal らが文章を読む際の視線移動を分析したことが最初の事例とされる [4]．Javal らは角膜系を開発して観測を行い，視線は継続的は移動するのではなく，素早い動きと滞留を繰り返すことを発見した．この素早い動きは「サッカード」，滞留は「注視」 と呼ばれている．視線分析技術の進化とともに，様々な分野への応用が進められている．従来は研究実験や概念実証のような利用が多くみられていたが，視線分析装置の小型化，高精度化，そして低価格化によりより広い範囲の分野に普及しつつある．とりわけ HCI 分野への応用は顕著である [5]．

視線追跡装置の動作原理は，角膜反射法と呼ばれる手法に基づくものが一般的である [6]．代表的な例としては，ディスプレイに装着した赤外線カメラを用い，ソフトウェアによる画像処理を行って視線の特徴を識別し，視線位置や状態，移動報告を観測する．この場合，赤外線カメラは発行ダイオードにより赤外線を照射し，強い反射が得られたところから瞳孔を，小さな反射が得られたところから角膜位置を特定する．ソフトウェアはその後，瞳孔の中心と角膜の距離を計算し，人間の注視点を三角測量により分析する．瞳孔の位置や角膜との距離は個人差があるため，視線追跡装置を用いる際にはキャリブレーションを行い，個人差を吸収する手法が一般的である．このような視線追跡カメラは高価なものが多かったが，近年は EyeTribe [7]，Tobii EyeX [8] など数万円以下の安価なデバイスが販売されている．

また，近年の画像処理技術や機械学習技術の向上に伴い，赤外線カメラを使わず，一般的なウェブカメラを用いた手法も活発に開発されている．2005 年には注視点の識別精度が低いとされていた [9] が，2010 年代前半にはキャリブレーションの代わりに顕著性マップを用いることによる視覚情報の獲得技術 [10, 11] の高度化もあり，2015 年から 2016 年にかけて PACE [12], TurkeyGaze [13], WebGazer [14] などの赤外線カメラを用いなくとも視線追跡が高い精度で行えるようになった．とりわけ WebGazer はオープンソースで利用可能となっており [15]，今後の普及が期待される．また，スマートフォンに内蔵されるカメラによる視線追跡も研究されている [16]．

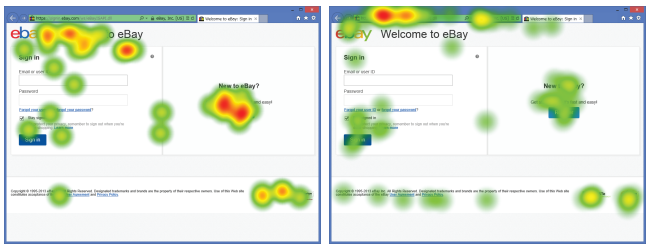
2.2 視線分析のアプリケーション

視線分析の主な用途の 1 つに，ユーザインタフェース等のデザインの評価が挙げられる．Pooler らのサーベイ [17] によれば，注視が示す意味はコンテキストによって異なる．まず，注視の回数が多いことは，インタフェースが最適でなく，情報の検索の効率性が低いとされる [18]．しかし，特定箇所の注視の回数は，その箇所が閲覧者に他の領域より重要であることを示す [19]．しかし，その特定箇所が画像ではなく文章であるとき，読む量が多いから注視されているか，認識しづらいため注視されている可能性もある [19]．注視時間の合計は様々な箇所の注意を比較するのに用いられ，状況認識の期待の尺度としても利用される [20,21]．ある箇所を見て，別の箇所を見て，また元の箇所に戻るような場合，その最初にみられていた箇所は視認性が不足している [18]．また，画面において最初の注視にかかる時間は関心を集めることに成功していると考えられる [22]．Lee らの研究



(a) 初心者　(b) 熟練者

図 1: フィッシングサイト閲覧時の視線移動



(a) 初心者　(b) 熟練者

図 2: 正規サイト閲覧時の視線移動

グループでは，注視の際の時間と回数の両方からユーザの意図を読み取ろうとしている [23]．ユーザの意図は何か特別な意図をもって情報を調べている Information 型と，漠然と眺めている Navigation 型に分類され [24]，主に注視の回数と時間からどの意図で分析しているかを識別する．

もう一つの著名な眼球運動であるサッカードについては，回数が多いほど情報の検索を行っているとされる [18]．より大きなサッカード運動は注意が引き出されている重要な情報提示であり [6]，元の場所に戻るサッカード運動は反対に重要ではない情報提示を意味する [25]．90 度以上の突然の異なる方向への移動は，閲覧者が目的としていた箇所が変更したか，インタフェースのレイアウトがユーザの期待にそぐわなかったことを示す [26]．

2.3　フィッシングサイト対策と視線分析

筆者の研究グループでは，エンドユーザが URL や SSL の鍵アイコンが表示されるアドレスバーを閲覧することの有効性の評価を行った [27]．エンドユーザの視線情報を収集するため，2013 年 11 月から 2014 年 2 月までの期間，東京大学の構内掲示板にて被験者を募集した．実験参加者は 23 人であり，そのうち 20 人が男性，3 人が女性であった．また，22 人が 20 代であり，残りの 1 人が 30 代であった．延べ 331 回のアドレスバーを目視した回数のうち，誤判定があったのは 89 回であった．フィッシングサイトに限定していえば 200 回のアドレスバーを目視した回数のうち 61 回が誤判定であり，残りの 131 回の正規サイトにおいてアドレスバーを目視した場合の誤判定は 28 回であった．従って，エラー率，False Positive 率，False Negative 率はそれぞれ 26.9%，21.4%，30.5%となる．反対にアドレスバーを見ない場合は，41.1%（129 回中 53 回），18.9%（53 回中 10 回），56.6%（76 回中 43 回）であった．False Positive 率ではごくわずかにアドレスバーを見ない場合が低くなっているが，フィッシングサイトのコンテンツは正規サイトと見た目が区別しにくいため，アドレスバーを見ない限り False Positive 率が高くなっている．結論として，アドレスバーを見ることは効果的であると考えられる．

また，2.2 節に述べた Lee らの研究成果を用い，Internet Explorer に表示されるウェブサイトの真贋判定における意図抽出を試みた [28]．この実験の概略を図 3 に示す．

まず，関心領域（Area of Interest, AoI) を図 4 のように定義し，その画面における注視時間と回数を調べ，Support Vector Machines [29] によるパターン認識を試みた．例えばアドレスバーを見たユーザが URL に基づいた判定を行ったかをアンケートで調べた所，およそ 85.5% の確率で予想できることがわかった．また，アドレスバーでの目視を確認するだけで 75.9% の確率でこのユーザが正しく判定できるか否かを予想できることがわかった．

3　視線分析によるフィッシング防御システムの実装と評価

この解析で得られた知見を元に，エンドユーザがどの程度危険を認識しているかを判別することは可能と考え，また，その認識の程度によってサイバー防御を切り分けることを考えた．

筆者は文献 [30] において，様々なヒューリスティクスを用いて調査し，その結果を Random Forest [31] により組み合わせてフィッシングサイトか否かを識別するシステムを実装した．ヒューリスティクスとはフィッシングサイトらしさを計算するためにもちいられる情報であり，例として「ドットの数」という経験則が知られている [32]．フィッシングサイトの FQDN に含まれる数のドットは正規サイトに比べ多くなる傾向にある．このようなヒューリスティクスを機械学習により組み合わせることによりパターン認識の精度が高くなる一方で，識別にかかる時間は増加する．一方で，ドットの数だけに頼るアルゴリズムは機械学習によるアルゴリズムと比較すると，識別の精度は低いものの，識別に必要な時間は短い．また，正規サイトをフィッシングサイトであると間違えて判定する可能性が極端に低い．検知の目安である適合率と再現率は，機械学習による方式ではそれぞれ 0.86，0.76 であったのに対し，ドットの数による方式は

1.00, 0.06 であった [33].

そこで，一定時間以内にアドレスバーを閲覧したエンドユーザは正しく判定できる可能性が高いと考え，明白にフィッシングサイトと思われるもののみを除外することが可能な「ドットの数による方式」によるフィッシングサイト対策を提供する．反対に，アドレスバーを閲覧しなかったエンドユーザは誤った判定を行う可能性が高いと考え,「機械学習による方式」を適用する．また，フィッシングサイトと判定された場合，防御システムはページの閲覧を完全にブロックするのではなく，文献 [27, 34] に述べられていた，個人情報を入力可能なコンテンツを無効化する方式を採用した．

防御システムのアーキテクチャを図 5 に示す．システムは，視線追跡カメラを制御することによりエンドユーザの注視箇所を計測する Eye-Tracking モジュールと，この結果からどの検知アルゴリズムを使うかを決定する Policy Decision Point (PDP) モジュール，そして実際のサイバー防御を行うためにエンドユーザが閲覧しているウェブサイトのコンテンツを無効化する Browser Extention モジュールによって構築した．Browser Extention モジュールは Google Chrome ウェブブラウザの拡張機能として実装し，Eye-Tracing モジュールは視線追跡カメラ EyeTribe [7] に用意されている SDK を用いて開発した．また，Analysis モジュールとして実装された機械学習及びドットの数による検知アルゴリズムは，PDP モジュールとはサイバー脅威交換フォーマットである n6 [35] を用いて情報交換を行った．具体的には，PDP モジュールが検知依頼を送信し，Analysis モジュールが検知結果を返信した．なお，実装はオープンソースで公開 [1] で公開されている．

2015 年 12 月から 2016 年 3 月までの期間，東京大学の構内掲示板にて被験者を募集した．応募があった被験者には，実験の目的として，「セキュリティ技術の研究開発を目的としたウェブサイトを閲覧した際のエンドユーザの挙動の観測」であることを説明し，作業内容として「ウェブサイトの画面を閲覧してもらい，正規のサイトか，あるいは偽サイトかを判定していただきます．またその際に　判定基準をアンケート形式でお答えいただきます」と説明した．この実験に関する個人に属する情報として，性別，年代（10 代，20 代，30 代……60 代以上），ウェブサイトを見た際の判定結果（正規サイト，偽サイト），視線の動き（判定時の目線の動き），アンケートによる回答を取得し，個人を特定可能な情報は記録しないことを説明した．実験参加者 21 名のうち 13 人が男性，8 人が女性であった．また，20 代が 13 人，30 代が 6 人，40 代・50 代が 1 人ずつであった．なお実験につかった表示装置はタブレット型の PC である Microsoft Surface 3 Pro であった．

アルゴリズムを実装したシステムの性能としては，1 回あたりのリクエストにかかる時間を評価した．ここでは，HTTPS プロトコルにより n6 でのリクエストを 100 回送信する場合について，並列度を 1,10,20,30,40,50 に変更しながら評価を行った．結果を図 6 に示す．URL に基づいた調査を行うドットによる判定のアルゴリズムの場合は最大で 0.23 秒のオーバヘッドが，機械学習によるアルゴリズムの場合は最大で 2.6 秒程度のオーバヘッドが観測された．

この遅延はフィッシングサイトを誤って判定しそうなユーザに対してのみ行われるものであり，その場合もウェブコンテンツは入力を受け付けないだけで，画像や文言は表示されている．このため，利便性の低下は限定的であると考えられる．この仮説を確認するため，防御システムを利用した被験者に対してアンケートを行い,「不便に思うか」という質問を行い，この解答を「全く思わない（１）」「あまり思わない（２）」「どちらでもない（３）」「ややそう思う（４）」「強くそう思う（５）」の五段階指標により解答させた．図 7 に示す結果の通り，「あまり思わない」が大半であり，残りは「全く思わない」「どちらでもない」がほぼ同じという結果が得られた．一般に，利便性と安全性はトレードオフの関係にるため,「安全だと思うか」という質問も行った．結果は,「ややそう思う」が大半で，ついで「強くそう思う」が多いという結果が観測された．

4　考察

4.1　本手法の問題点

本研究では視線分析によってユーザの意図の抽出が行えることを前提としているが，この手法には 4 つの課題が考えられる．

まず，熟練により意思決定にかける時間が極めて短いユーザの場合，アドレスバーの閲覧が高速に終了する場合が考えられる．とりわけ，著者の所属するグループでは，フィッシング対策研究者，フィッシング対策の教育の講師及び受講者，及びセキュリティに関する業務を行う者が多く，彼らにフィッシングサイト判別実験を行った所，比較的短時間にアドレスバーの確認を終了する事例が観測された．すなわち,「注視の回数・時間が少ない」場合であっても，アドレスバーの確認が短時間で終了したのか，アドレスバーをあまり閲覧できなかったのかが問題となる．文献 [28] の実験環境ではセキュリティに関する実験ということで被験者が集まったこともあり，意思決定にある程度の時間をかけていたが，例えば短時間で判定しなければならないという制約を設けることによって，違いを見つけることができる可能性がある．ま

[1] https://github.com/necoma

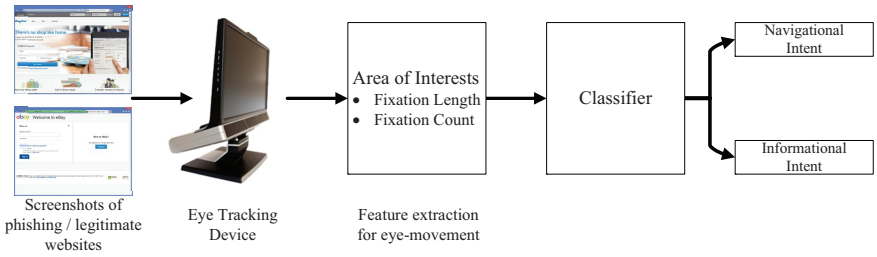
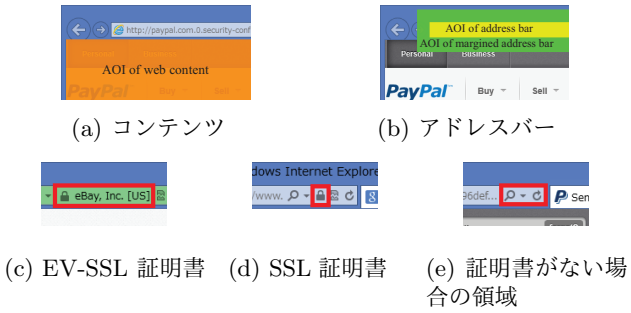


図 3: 実験のブロックダイアグラム図



(a) コンテンツ (b) アドレスバー

(c) EV-SSL 証明書 (d) SSL 証明書 (e) 証明書がない場合の領域

図 4: 関心領域の設定

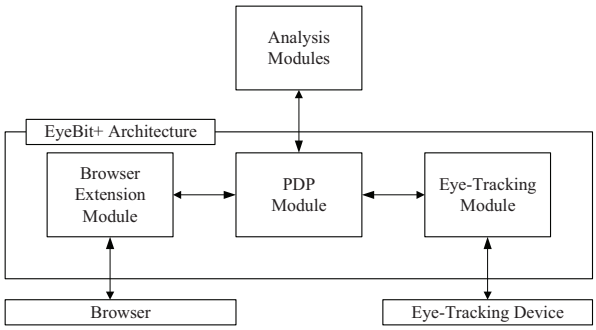


図 5: 防御システムのアーキテクチャ

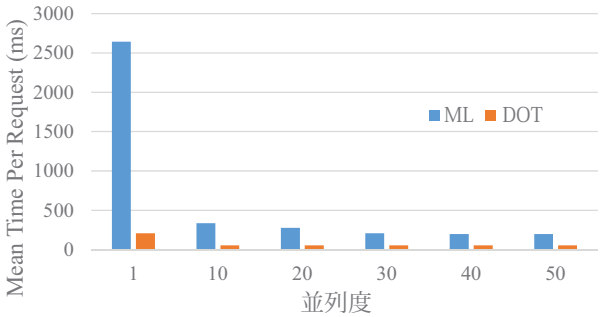


図 6: 防御システムの応答速度

た，意思決定を予測する説明変数として最初の注視までの時間や，意思決定に至るまでの注視している時間の割合を用いる方法が考えられる．

第 2 の課題は，アドレスバーに記載される URL がユーザが注意深く見ても視認不可能な場合である．例えば文献 [36] で示されるような国際化ドメインを用いたフィッシングサイトが考えられる．図 8 は，アルファベットで `Daisuke` という文字を表示しているが，アルファベットの `a` を表示しているもの，そしてその代わりにキリル文字の `a` を表示している場合である．一部の日本語フォントでは識別可能なものがあるが，英字フォントや一部の日本語フォントでは識別が難しい．これらの場合，URL をいくら注意深くみても識別不可能である．ただし，近年のウェブブラウザはアドレスバーにセキュリティ情報を表示している．このため，アドレスバーの目視を確認することで，フィッシングサイトの判別が可能となることも考えられる．また，この課題については人的要因で解決することではなく，技術的要因で解決する考え方もある．第 3 の課題は，色彩認識と注視の関係である．例えば EV-SSL 証明書などを認識する場合に「緑色」という色が果たす役割は大きいが，色彩の認識は必ずしも注視を必要とせず，サッケードの状態でも行え得る [37]．特定の色の果たす役割は大きく，安全は緑，警告は赤が好ましいとされている [38]．

最後の課題は，視覚障害者への適応が考えられる．著者らは視覚障害者にヒアリングを行い，彼らの環境におけるフィッシング対策について調査を行った．当初，筆者らはスクリーンリーダを用いて音声を読み上げるのが一般的と思われ，証明書の情報をやアドレスバーの情報を読み上げることによってフィッシングサイト判定を行うのではないかと考えた．しかし，スクリーンリーダはウェブブラウザのコンテンツの情報を読み上げることは出来ても，証明書の情報を読み上げることは難しいことがわかった．これは，様々なブラウザが情報へのアクセシビリティを高めるよう，OS のサポートの API を使って開発 [39, 40] が行われているところではあるが，アドレスバーについてはこれらの API がサポートされていないからである．一方で，コンテンツへのアクセシビリティを高めるための国際標準 [41]，証明書をどのように取得するかといった基準 [42] は存在するものの，証明書をどのようにアドレスバーに表示すればよいかの検討が必要である．そして，それがスクリーンリーダから読みやすなって初めて，エンドユーザがその情報をどのよう

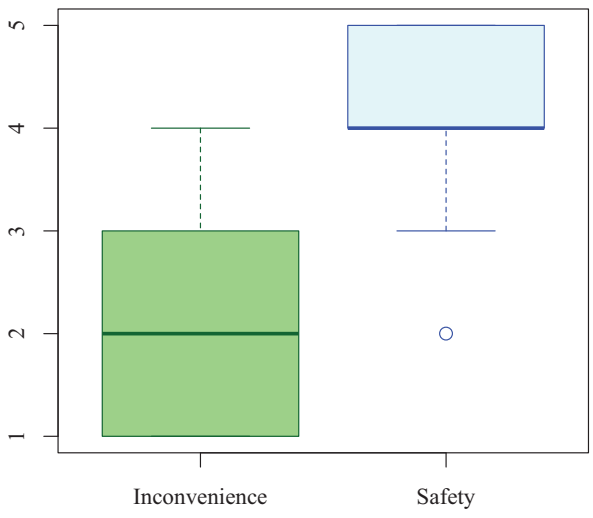


図 7: 防御システムのアンケート調査

	アルファベットの a	キリル文字の a
ＭＳ明朝	Daisuke	Ｄａisuke
ＭＳゴシック	Daisuke	Ｄａisuke
メイリオ	Daisuke	Daisuke
Century	Daisuke	Daisuke
Times New Roman	Daisuke	Daisuke
Arial	Daisuke	Daisuke

図 8: 難識別文字の例

に認知したかを計測可能となる．

4.2　生体センサーへの要件について

本研究では視線情報をフィッシングサイト対策に用いたが，サイバーセキュリティ分野で人的要因に対応する必要性は高まっている．特にフィッシングサイトではなくアプリケーションの脆弱性を利用してマルウェアに感染させるウェブサイトに誘導する標的型メール，ストレス等を原因として発生するとされるサイバー事故，あるいは故意に行われるインサイダー攻撃などの解決が求められる．

これまでのサイバーセキュリティ技術は，暗号技術により信頼性を表示したり，解析技術により悪意を発見したりする等，機械的な対策に重点が置かれてきた．しかし，守るべき対象が人間である以上，この人間の意図を解析する，人間に内在する状態を推測する先行研究により提案された方式のサイバーセキュリティ分野への応用が急務であると考えられる．

この応用の障壁の 1 つに，セキュリティ分野と認知心理学分野では方式に求められる要件の違いがあると考えられる．そこで，セキュリティ分野で必須とされる機密性，完全性，可用性の観点から要件を考察する．

機密性要件としては，視線などの生体情報を取得することへの社会的受容が求められる．取得情報の内容，データの保存方法，方式のメリットやデメリットがユーザに周知されることが求められる．完全性要件としては，否定的評価の恐怖により生体情報を偽って取得させようとする試みへの耐性が求められる．可用性要件としては，方式が ICT 活用場面で利用可能であることが望まれる．人体への挿入・浸透を行なうデバイスは避けるべきであり，着用型のデバイスであれば重量や締め付けの観点から数時間の利用に耐えられるべきであろう．

機密性要件は実験計画によって異なると思われるが，本研究で用いた非接触型の視線追跡デバイスや，顔の表面温度の計測による手法が完全性，可用性の要件を満たしやすいと思われる．とりわけ，眼球運動については，精神状態の遷移や意思決定と関連付けた研究は多い．この知見を活かし，システムがユーザの正しい手続きで意思決定を行っていることを監査し，人的要因によって起こる問題の解決が今後の課題である．

5　まとめ

本研究では，誤った判断に起因するサイバー攻撃に対して，人間の生体情報の観測から意思決定を推測することで，より高度なセキュリティ対策を行うことを目的として行われた．今回の研究では視線分析を例に取り上げ，視線の意図抽出する先行研究からフィッシングサイトの防御を行うシステムを実装した．このシステムの特徴は，ユーザの認知の段階に応じて提供する防御を変えるというものであり，これにより利便性の低下が限定的になると考えられること，また，利便性の低下によってもたらされる安全性の低下も少ないことから，安心かつ便利に使える防御システムに貢献したと考える．

今までは守るべきエンドユーザの状態を把握せずに防御を適用していたが，エンドユーザがどのような精神状態にありどのような意思決定を行うかを予想できるようになれば，より高度なサイバー防御が可能になるという仮説は，今後も様々な角度から検証が必要であろう．4 説に考察した課題だけでなく，標的型メール攻撃やインサイダー攻撃など様々な人的要因に起因する問題をエンドユーザの観測により未然に防御する方法も今後の課題である．

謝辞

本研究は，総務省の戦略的国際連携型研究開よって発推進事業及び欧州連合 (EU) の第 7 次研究枠組み計画 (FP7) からの助成 (助成番号 608533:NECOMA) により得られた成果である．

参考文献

[1] K. Hawkey, D. Botta, R. Werlinger, K. Muldner, A. Gagne and K. Beznosov: "Human, Organizational, and Technological factors of IT security", Extended Abstracts on Human Factors in Computing Systems, pp. 3639–3644 (2008).

[2] R. Werlinger, K. Hawkey, D. Botta and K. Beznosov: "Security Practitioners in Context: Their Activities and Interactions with Other Stakeholders within Organizations", International Journal of Human-Computer Studies, **67**, pp. 584–606 (2009).

[3] R. Dhamija, J. D. Tygar and M. A. Hearst: "Why Phishing Works.", Proceedings of Conference On Human Factors In Computing Systems (2006).

[4] L. E. Javal and H. Schiötz: "Un opthalmomètre pratique, paris", Annales d'Oculistique, pp. 5–21 (1881).

[5] R. G. Lupu and F. Ungureanu: "A survey of eye tracking methods and applications", Bul Inst Polit Iasi, pp. 71–86 (2013).

[6] J. H. Goldberg and A. M. Wichansky: "Eye tracking in usability evaluation: A practitioner's guide", The mind's eye: Cognitive and applied aspects of eye movement research, Elsevier (2002).

[7] The EyeTribe: "The Eye Tribe Tracker", Availabel at: `https://theeyetribe.com`.

[8] Tobii Technology: "Tobii EyeX", Available at: `http://www.tobii.com`.

[9] D. W. Hansen and A. E. Pece: "Eye tracking in the wild", Computer Vision and Image Understanding, **98**, (2005).

[10] Y. Sugano, Y. Matsushita and Y. Sato: "Calibration-free gaze sensing using saliency maps", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2667–2674 (2010).

[11] F. Alnajar, T. Gevers, R. Valenti and S. Ghebreab: "Calibration-free gaze estimation using human gaze patterns", Proceedings of the International Conference on Computer Vision (ICCV), pp. 137–144 (2013).

[12] M. X. Huang, T. C. Kwok, G. Ngai, S. C. Chan and H. V. Leong: "Building a Personalized, Auto-Calibrating Eye Tracker from User Interactions", Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 5169–5179 (2016).

[13] P. Xu, K. A. Ehinger, Y. Zhang, A. Finkelstein, S. R. Kulkarni, and J. Xiao: "Turkergaze: Crowdsourcing saliency with webcam based eye tracking", Technical report, arXiv preprint arXiv:1504.06755 (2015).

[14] A. Papoutsaki, P. Sangkloy, J. Laskey, N. Daskalova, J. Huang and J. Hays: "WebGazer: ScalableWebcam Eye Tracking Using User Interactions", Proceedings of the 25th International Joint Conference in Artificial Intelligence (IJCAI) (2016).

[15] WebGazer.js: "Democratizing Webcam Eye Tracking on the Browser", Online Available at: `https://webgazer.cs.brown.edu/` (2016).

[16] K. Krafka, A. Khosla, P. Kellnhofer and H. Kannan: "Eye tracking for everyone", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2016).

[17] A. Poole and L. J. Ball: "Eye Tracking in Human-Computer Interaction and Usability Research: Current Status and Future", Encyclopedia of Human-Computer Interaction (2005).

[18] J. H. Goldberg and X. P. Kotval: "Computer interface evaluation using eye movements: Methods and constructs", International Journal of Industrial Ergonomics, **24**, pp. 631–645 (1999).

[19] A. Poole, L. J. Ball and P. Phillips: "In search of salience: A response time and eye movement analysis of bookmark recognition", People and Computers XVIII-Design for Life: Proceedings of HCI 2004 (2004).

[20] C. Mello-Thoms, C. F. Nodine and H. L. Kundel: "What attracts the eye to the location of missed and reported breast cancers ?", Proceedings of the symposium on Eye tracking research & applications, pp. 111–117 (2002).

[21] G. Hauland: "Measuring team situation awareness by means of eye movement data", Proceedings of HCI International Conference, pp. 230–234 (2003).

[22] M. D. Byrne, J. R. Anderson, S. Douglass and M. Matessa: "Eye tracking the visual search of click-down menus", Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pp. 402–409 (1999).

[23] U. Park, R. Mallipeddi and M. Lee: "Human Implicit Intent Discrimination Using EEG and Eye Movement", Proceedings of the 21st International Conference on Neural Information Processing (2014).

[24] Y.-M. Jang, R. Mallipeddi, S. Lee, H.-W. Kwak and M. Lee: "Human intention recognition based on eyeball movement pattern and pupil size variation", Neurocomputing, **128**, pp. 421–432 (2014).

[25] J. L. Sibert, M. Gokturk and R. A. Lavine: "The reading assistant: Eye gaze triggered auditory prompting for reading remediation", Proceedings of the 13th annual ACM symposium on User interface software and technology, pp. 101–107 (2000).

[26] L. Cowen, L. J. Ball and J. Delin: "An eye-movement analysis of web-page usability", Proceedings of HCI International Conference, pp. 317–335 (2002).

[27] D. Miyamoto, T. Iimura, H. Tazaki, G. Blanc and Y. Kadobayashi: "EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits", Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (2014).

[28] D. Miyamoto, G. Blanc and Y. Kadobayashi: "Eye Can Tell: On the Correlation between Eye Movement and Phishing Identification", Proceedings of the 22nd International Conference on Neural Information Processing of the Asia-Pacific Neural Network Assembly (2015).

[29] C. Cortes and V. Vapnik: "Support-vector networks", Machine Learning, **20**, 3, pp. 273–297 (1995).

[30] D. Miyamoto, H. Hazeyama and Y. Kadobayashi: "An Evaluation of Machine Learning-based Methods for Detection of Phishing Sites", Australian Journal of Intelligent Information Processing Systems, **10**, 2, pp. 54–63 (2008).

[31] L. Breiman: "Random Forests", Machine Learning, **45**, 1, pp. 5–32 (2001).

[32] Y. Zhang, J. Hong and L. Cranor: "CANTINA: A Content-Based Approach to Detect Phishing Web Sites", Proceedings of the 16th World Wide Web Conference (2007).

[33] A. Kozakiewicz and R. Fontugne: "Threat analysis", Technical report.

[34] D. Miyamoto, H. Hazeyama and Y. Kadobayashi: "SPS: A Simple Filtering Algorithm Thwart Phishing Attacks", Proceedings of ASIAN INTERNET ENGINEERING CONFERENCE 2005 (2005).

[35] CERT Polska: "n6", Available at: `https://n6.cert.pl`.

[36] V. Krammer: "Phishing Defense against IDN Address Spoofing Attacks", Proceedings of the 4th Annual Conference on Privacy, Security, and Trust (2006).

[37] V. Lederberg: "Color Recognition during Voluntary Saccades", Journal of the Optical Society of America, **60**, pp. 835–842 (1970).

[38] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant and S. Consolvo: "Rethinking connection security indicators" (2016).

[39] Microsoft: "Microsoft Active Accessibility", Available at: `https://msdn.microsoft.com/ja-jp/library/cc401822.aspx`.

[40] Linux Foundation: "IAccessible2", Available at: `https://wiki.linuxfoundation.org/accessibility/iaccessible2/start`.

[41] ISO/IEC 40500:2012: "Information technology – W3C Web Content Accessibility Guidelines (WCAG) 2.0", Available at: `http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=58625`.

[42] CA/Browser Forum: "Baseline Requirements Documents, v.1.4.1", Available at: `https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.4.1.pdf`.