様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １９ 日現在

機関番号：５２６０１
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１２１８６

研究課題名（和文）深層学習と力覚で異常値判定を行いサイバーセキュリティ学習を支援するシステムの開発

研究課題名（英文）Development of a system to support cyber security learning by using deep learning and force sensing to determine anomalous values.

研究代表者
石原　学（ISHIHARA, MANABU）

東京工業高等専門学校・電気工学科・特任教授

研究者番号：２０２１１０４７

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：ネットワーク環境中で、攻撃された、または踏み台となった情報端末の攻撃挙動についてネットワーク内でのトラフィック解析を行うことや、基本的なセキュリティ技術の訓練システムを構築した。次に、日本語のメールを迷惑メールと通常メールとに分類する方法を考案した。迷惑メールのフィルタはメール本文のテキストを用い、メール本文のテキストの前処理・形態素解析・分類学習の3つで分類を行い分析した。
さらに、力覚装置の実験およびフラットパネル上での触感覚の実験で、表面粗さの認識精度について検討し、試作および評価実験を行い明らかにした。その結果、表面粗さの違いを判定できるシステム構築の基準を構築することができた。

研究成果の学術的意義や社会的意義
サイバーセキュリティは、現代社会における重要な課題である。本研究では、サイバーセキュリティ学習のためのプラットフォームを構築し、攻撃された状態・踏み台となったPC・水飲み場攻撃、スパムメールなどを再現して学習できるシステムを構築した。さらに、スパムメールを分析して、スパムメール判別のためのフィルタを設計して評価実験を行った。これらの現象からトラフィック異常値を検出することを試みた。異常値をネットワーク上で感知したら、その異常値を出力する方法として、力覚や触覚を利用したインタフェースを検討した。変化の大きさから知覚できる範囲を明らかにした。これらの成果は、判定結果を認知する方法として有効である。

研究成果の概要（英文）：Attacks occur in internetwork environments. Traffic analysis was performed within the network to examine the attack behavior of stepping stone information terminals.  A training system for basic security techniques was constructed.
A method was devised to classify Japanese emails into spam and regular emails. The spam filter uses the text of the email body, and classification and analysis are performed using three steps: preprocessing of the text in the email body, morphological analysis, and classification learning. Furthermore, experiments with a force-sensing device and tactile sensations on a flat panel were used to examine the accuracy of recognizing surface roughness, and standards were established for building a system that can determine differences in surface roughness.

研究分野：感性情報学

キーワード：サイバーセキュリティ　スパムメール　力覚　触覚　機械学習

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

コロナ禍以降に、小中高大の遠隔授業および企業のテレワークの稼働により、ネットワーク初心者の利用が急増している。さらに、セキュリティ教育や熟練の程度により、ネットワークインシデントの発生が懸念される。そこで、最近増加している標的型攻撃メール等のインシデント行為について、脅威評価と自動分析を行い、その結果を用いて、サイバーセキュリティの学習を支援するシステムを開発することを目的とする。情報セキュリティ教育は一般的に、情報倫理教育との関係から紙ベースや、ディジタルデータを利用した演習方式（パワーポイントや実験など）を通して理解させる教材が多い。

また､サイバーセキュリティの重要性は､十分に述べられているものの､現在の研究としては、ウイルス等への感染防止やウイルスの性質の知識の理解におかれている。また、システムとしても、ディジタル技術の観点から情報の安全性（暗号化を含む）の開発関係などが行われている。サイバーセキュリティ教育においても、プラットホームの開発やクラウドの仮想化技術を使用するシステムなどの研究が行われている。クラウドを含むサイバーセキュリティの可視化については、国立研究開発法人情報通信研究機構の NICTER において可視化による大きな成果が得られているものの経費は高額であり、一般の普及や教育の利用については、まだほとんど行われていない。

２．研究の目的

本研究は、サイバーセキュリティ教育に仮想現実の手法を取り入れ、標的型攻撃のシナリオの自動生成や Dos/DDos 攻撃等を体験できるシステムを構築することで、通常目に見えないディジタル情報の安全について理解させるシステムの構築を目的とする。攻撃されるネットワーク回線のパケット量を力覚量（押し付ける力の量）に変換し、攻撃が強くなると手に受ける力を大きく感じるものとする。さらに最近増加している標的型攻撃のメール等の埋め込みによる有害データの感染を誘う攻撃型メール予防訓練システムを試作する。現在まで、①仮想現実と②攻撃型インシデント事項を連動させた体験型のシステムについての開発例は無く、本システムは従来の可視化技術の次にある仮想現実を導入することで、サイバーセキュリティの理解を深めることと初心者に対する教育システムの構築を目指している。コロナ禍において、標的型攻撃メール等は増加している。その適切な対応ができていないことによるサイバーセキュリティリスクが高まり、ウイルス感染を始めとするリスク情報報告が後を絶たない。本研究では、①ネットワーク内の異常値検出を、CPU 動作やパケットの振る舞い、ヘッダ等に埋め込まれた悪意情報の双方について抽出する。その後、②認識された結果を基に、悪意ある部分を機械学習を用いて判定する。③その分析結果を基にして、埋め込み型攻撃やパケットの異常値検出を、仮想現実である力覚・触覚の特性を使って観察者に通知するシステムの基本的な特性を示す。

３．研究の方法

3.1　サイバーセキュリティ演習システム

サイバーセキュリティ教材は各種の方法が提案されている[(1) (2)]。サイバーセキュリティを中心に、学習できる範囲を以下のような「不正アクセス」「迷惑メール」「情報漏洩・改ざん」「過剰負荷攻撃」の４項目について実現する。ハードウェア構成として､図 1 のようなハードウェアにより構成される。基本構成は、1 台のサーバ PC、50 台のクライアント PC、5 台のスイッチングハブ（クライアント 10 台に対して 1 台）としている。また、サーバ・クライアント間は、演習中に外部ネットワークへの影響を与えないように閉じたネットワークとし、ローカルなネットワークとすることで、DoS(DDoS)攻撃などのネットワーク負荷を与えるものとしている。また、ソフトウェアはフリーソフトウェアを主として構成し「不正アクセス」「迷惑メール」「情報漏洩・改ざん」「過剰負荷攻撃」などの手法、及び、それらの攻撃に対する防御を行う手法について演習するシステムを構築した。これらを体験しながら、異常値を観測できるようにしている。

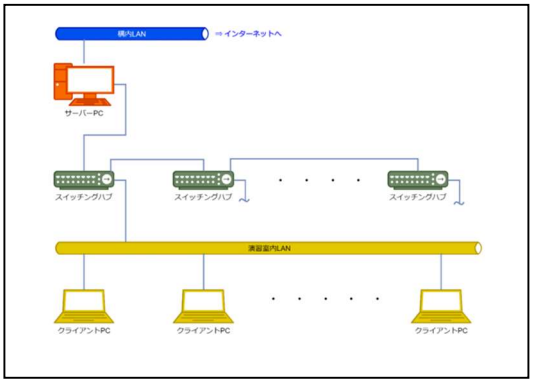


図１　システム概要図

訓練できることを以下に示す。

１）偽 Web サイト作成、URL 偽装、偽サイト誘導メール送信、これらの訓練が出来る。

・Web サイトをクローンする方法等の訓練と、その対象ウェブサイトの脆弱性の判断および注意点について訓練する。これらの訓練では、どのようにクローンが作成されるかの理解と、対応策について訓練することを含む。

２）ファイル改ざん、ファイル削除、これらの訓練が出来る。

・電子ファイルが改ざんされていないかをチェックする方法を理解させる。

・ファイルの扱いを理解させることで、OS や HP などの脆弱性を理解し、その対処法を会得させ

る。
３）標的型攻撃メールの訓練が出来る。
・標的型攻撃メールの代表的なものとして、特定の企業を標的とし、添付ファイルや URL にてウィルスを侵入させる等の攻撃手段が存在する。そのような標的型攻撃メールの見分け方や対策、作成などの訓練を通して、対策を検討できるようにする。
４）疑似ウイルス作成の訓練が出来る。
・コンピュータウイルスの原理等を理解させ、それに対抗するシステムを構築できるよう訓練する。
５）ネットワークアタック（Dos）の訓練が出来る。
・DoS 攻撃や DDoS 攻撃の環境や手法を理解させ、それらに対抗できる手法について訓練する。
６）記録(log)を見やすいように提示でき、対象者が攻撃された内容等について CSV または TXT データ等に記録できる。
・攻撃ログなどの一覧を見やすいように表示できる。訓練に使用した状況について把握することができる。

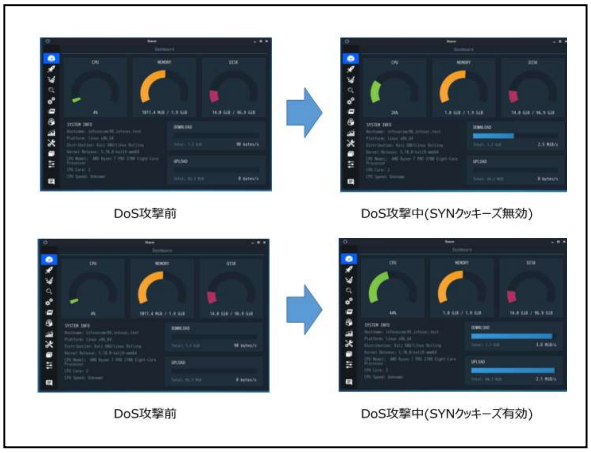

図２　異常値検出例

異常値の値として、CPU 値の様子などをモニターでき、それらを異常値として取得できる。例を図 2 に示す。

3.2　サイバーセキュリティのスパムメールの認定の性能比較

近年、インターネットの発展と電子メールの急速な普及は、スパムメールの増加に関係している。電子メールは簡単で無料にて送信できることから、悪質なユーザがメールを不特定多数に送信している場合がある。一般に踏み台攻撃やマルウェアによる不正制御などによる例も後を絶たない。受信者は、不要なメールを大量に受け取り、そのメールの内容を確認して削除する時間を費やす問題や重要なメールを見劣る問題が発生している。他にもなりすましメールやチェーンメールなどの例も現有する。これらは近年増加傾向にあり、深刻な被害が出ている [3]。現在でもファイアウォールにスパムフィルタを行って防御している。まだこれらの防御は多数あり[4,5]、機械学習を用いたフィルタリングの開発、機能比較を行う。

3.2.1 システム概要

本システムでは、まずメールを迷惑メールと通常メールとに分類するものとする。迷惑メールのフィルタはメール本文のテキストを用いる。メール本文テキストの前処理、形態素解析、分類学習の３つで分類を行う。

メール本文の頻出単語の出現頻度からフィルタリングを行う。メール本文には様々な単語や文字などが存在するが、時には意味をなさない単語や文字 (特殊文字、メールアドレスなど) が含まれる。機械にとってそれらはただの文字の羅列としか認識できないため形態素解析を行った際、ただの数字や英語、記号として別々に区切った結果となる。そのため、それらのデータの変換が不可欠になる。使用した PC の仕様を示す。CPU : AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx　2.10 GHz、RAM：8.00GB、OS：Windows 10 Home (21H1)である。

変換後の URL とメールアドレス、電話番号は形態素解析エンジンの辞書に単語として登録しておくことで、変換した文字列を 1 つの単語として認識することができる。変換処理後は形態素解析を行い意味のある単語に区切り、品詞などの特徴を判定する。形態素解析によって単語ごとに区切られているので対象のメール本文の単語の出現頻度などの特徴量を学習させる。また、先ほど変換の際に抽出した文字列を学習させることで、スパムメールの特徴と思われる URL やメールアドレスなどの特徴を把握し、フィルタリング精度の高いシステムを目指す。

使用する訓練データは、実際に自分のメールアドレスに送信されたメール 9667 件を用いる。また、学習モデルは、SVC、線形 SVC、決定木、ランダムフォレスト、ベルヌーイ分布に従ったナイーブベイズ、ロジスティック回帰を使用する。訓練データの内容の変化は 3 つのパターンを作成した。①訓練データに使用する単語の品詞を変化させた場合、②訓練データのスパム比率は変えずにメールの総数を増減させる場合、③メールの総数を変えずにスパムの比率を変更した場合の 3 つの実験を行った。本稿では、次の比

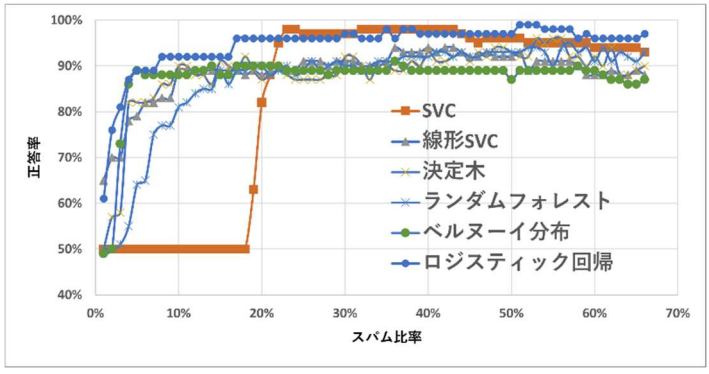

図３　各モデルのスパム比率変化における正答

率変化について示す。

3.2.2　比率変化

本実験では、分類に使用する訓練データの総数は変えず通常メールとスパムメールの比率を変化させて分類学習を行った。使用した訓練データと結果を図３に示す。

図３から訓練データのスパムの比率が増加するごとに、正答率も増加傾向にあることが分かる。スパム比率が約 20%を超えるとすべてのモデルが安定した正答率になっていることが分かる。また、SVC モデルのみ約 17%を境に正答率に大きな変化が起きていることが分かる。

3.2.3. 考察

本実験で各モデルの特徴について整理した。今回、分類学習を行う際の訓練データについて着目して機能比較を行った。

迷惑メールの分類では、訓練データのスパム比率、使用する品詞、メールの総数に応じたモデルの選択が必要であることが分かった。

また、迷惑メールの本文に使用される単語の傾向は日々変化していることから訓練データだけでなく機能比較をするためのテストデータも日々更新していく必要があると考えられる。テストデータの更新を行うことで精度の良い分類が行える。

3.3　触覚を刺激する変化の識別判定

現在使われているディジタルデバイスは、視覚や聴覚情報を主にしている。高速なディジタル伝送や 5G の導入により、「触覚インターネット」という用語が使われるようになってきた。触覚を利用するシステムの一つに触覚ディスプレイがあり、今後様々な用途で活用が期待されている[6]。この触覚ディスプレイは、物の手触りや凹凸などの皮膚感覚を再現でき、多種にわたる将来性が期待される[7]。また、皮膚感覚には、温冷、硬軟、粗さ、摩擦があることが知られている。本研究では、粗さ感覚に着目して「ツルツル」「ザラザラ」した感覚のことを考える。粗さは振動との対応関係があることが知られている[8]。本研究では、フラットパネル上で接触している指へ振動を与えることで、接触している部位での粗さや硬さの再現について検討し、指先の皮膚感覚の再現ための条件について示す。

3.3.1　実験装置

〈1〉表面粗さ提示装置

表面粗さの提示装置として、Immersion 社の TouchSence® Touchscreen を使用する（以降、TouchSence とする）。TouchSence は、アクチュエータが内蔵されており、タッチスクリーン上を指先でタッチすることで、事前に設定してある任意の振動を発生させることが出来る仕組みとなっている。

〈2〉表面振幅の測定

表面粗さ提示装置を使用した表面の振動振幅測定を行った。オプテックス・エフエー社の赤色半導体レーザ LS-100C を用いる。LS-100C は、反射光を三角測量する光切断法を使用し、非接触な形状測定を可能としている。これらを使い表面形状での変化を測定する。図４に示す。

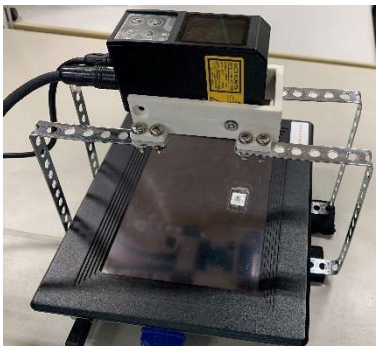

図４　粗さの表示装置

表面粗さ提示に使用した TouchSence は、設定として表面振幅は Mg 値として使用している。そこで、本実験範囲で使用する振幅 Mg 値を測定し、実際の振幅との対応について測定した。振動の設定は、波形：正弦波と三角波、周期：12 ms、振動時間 4 sec とした。Mg は 2000 から 6000 まで 500 ごとに変化させ測定した。非接触型測定器で TouchSence 表面の変位を測定後、30 データ移動平均を行い、振幅の大きさを算出した。測定結果より、Mg5000 で振幅 23μm 程度であることが分かった。振幅波形として正弦波と三角波の２種類を測定したが、ほぼ同程度の振幅値を得ており波形による差異はほとんど無い。このことから、表面粗さ提示装置としての提示範囲を設定することができる。

〈3〉官能評価を用いた周波数変化と粗さ感覚

本実験では、周波数変化が粗さ感覚にどのような影響を及ぼすか調べる。また、粗さ感覚と周波数の相関や個人差の有無について分析を行った。

指先の皮膚感覚では 10 Hz から 300 Hz 程度の範囲で医学的に振動検出閾値が分かっている。そのため実験では、振幅を 23μm 一定とし、周波数を 1 から 250 Hz で変化させる条件とした。提示する振動は、波形：正弦波、周波数：1, 10, 20, 40, 50, 100, 200, 250 Hz のように 8 段階とする。提示方法は，TouchSence のディスプレイに異なる刺激の周波数を A から H まで乱数で再現するように設定した。解析方法は Scheffé の一対比較法の中屋の変法を用いる[6]。中屋の変法では評価対象を 2 つずつ相対比較していくことで平均評価点を得る。図５に 5 段階評価スケールを示す。アンケートはそれぞれの健常者で年齢 19 から 22 歳までの 15 名を評価者とし，一人で 28 回比較を行う。粗さの評価は、


図５　５段階評価スケール

5 段階評価での回答とし、粗さ感覚の心理尺度を求める。

〈4〉 実験結果

振幅 23μm の心理尺度図を図 6 及びグループ分けしたものを図 7 に示す。この図は、間隔尺度であり、横軸の距離の差が大きさの違いを示す。この間隔尺度では、粗さ感覚は右に行くほど強く、左側が弱いため、100 Hz が一番強く、200 Hz が一番弱いことを示している。多重比較より危険率 1%のヤードスティックは図中の大きさであり、この値以上に大きく離れている場合に、順番が入れ替わらない有意差がある。また、この結果は 15 人全体のデータであり、分散分析で個人差が検出されるため、それぞれグループに分け個人差を可視化したものを図 7 に示す。

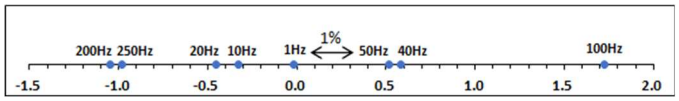


図 6　心理尺度図

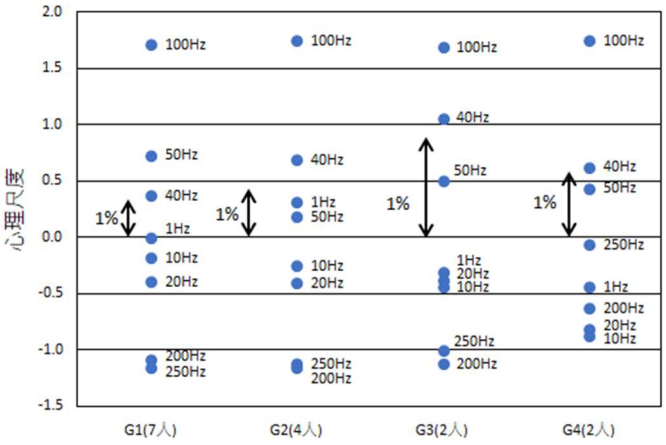


図 7　グループごとの心理尺度分類

図 7 で、グループを G1, G2, G3, G4 と分けた。G1 は 40 Hz と 50 Hz が入れ替わっており、G2 は 50 Hz と 1 Hz の差が小さい、G4 では 250 Hz と 200 Hz が 10, 20 Hz より感覚が大きいといった個人差がある。

全体の傾向がみられないもののグループ分けをすることでその傾向を見出す可能性を示した。

3.3.3　おわりに

表面粗さの再生系装置として TouchSence を使用して、人間の指先に感じる感覚を分析した。本実験では、23μm の振幅のとき、周波数ごとの振動で粗さが判別できていそうである。しかし、個人間の差が大きいことも示している。今回の提示装置は、接触面が抵抗膜方式タッチパネルの形状になっており、接触面の硬さや面積などの検討を行っていない。本実験では、振動を用いた指先への刺激による形状や凹凸の再現について検討した。解剖学的所見による振動値を刺激として与えることで、接触面が滑らかな形状にざらつき感を持たせることが出来ることを示した。

４．研究成果

(1)サイバーセキュリティ演習装置を構築し、実際に訓練システムへと発展させた。また、このシステム内で発生する異常値を検出することができた。

(2)実際の電子メールを対象に、スパムメール判定アルゴリズムを用いて判定比較を行い、アルゴリズムの有効性を示した。これらのスパムメールを分類して異常値として取得可能と思われる。

(3)人の指の触覚は、振動を与えることで物体表面の凹凸を判定し、表面形状の状態を例えば「ざらざら感」であるとかの感覚を取得することができる。これらの再現機構を利用することで、異常値判定を人に通知するための機構として利用することができる。

これらの研究から、異常値の抽出および判定が行うことができた。さらに、それを人に提示する装置として触覚の特性から振動装置を利用し、感覚量として再現可能であることを示した。これらの結果から、システムに組み込むことができると考えられる。

参考文献

(1) 中田、他：ディジタルプラクティス，11，2,414-433(2020.4)
(2) 干川、他：サービス拒否攻撃演習システムの実装とそのアクティブラーニングシナリオによるセキュリティ技術教育，信学論 B，J103-B，4，180-183 (2020.4)
(3) David Crocker,（訳：景山忠史他),情報処理，46，7，739-791 (2005)
(4) 山口他，ベイズフィルタと決定木分類による併用メールフィルタの判定方式の改善と効果，IEICE technical report 111(453)，23-28(2012-03)
(5) 杉井他，機械学習によるスパムメールの特徴の決定木表現，情報処理学会研究報告，DPS,マルチメディア通信と分散処理研究会報告 130，183-188 (2007.03)
(6) 高木 英行：使える!統計検定・機械学習-III ： 主観評価実験のための有意差検定，一般社団法人システム制御情報学会，58，12，514-520 (2014)
(7) 梶本裕之：触覚ディスプレイ,計測と制御，47,7，566-571(2008)
(8) 田中真美：触覚・触感のメカニズムの解明とセンサシステムの開発に関する研究，精密工学会誌，82，1，20-25(2016.01)

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　0件）

| | |
|---|---|
| １．著者名<br>Manabu Ishihara | ４．巻<br>1 |
| ２．論文標題<br>Changes in Display Surface Shape and Sensory Volume | ５．発行年<br>2023年 |
| ３．雑誌名<br>Proceedings of 2023 IEEE 12th Global Conference on Consumer Electronics (GCCE) | ６．最初と最後の頁<br>813-814 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/GCCE59613.2023 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Manabu Ishihara | ４．巻<br>1 |
| ２．論文標題<br>Reproduction and experience of a classic Japanese-style room and sound environment | ５．発行年<br>2023年 |
| ３．雑誌名<br>Proc. Inter-Noise2023 | ６．最初と最後の頁<br>2513-2519 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.3397/IN_2023_0368 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Manabu Ishihara and Kazuhiro Owada | ４．巻<br>- |
| ２．論文標題<br>Tactile Angle Characteristics for Reproduction by Force Sensation | ５．発行年<br>2023年 |
| ３．雑誌名<br>International Conference on Human-Computer Interaction | ６．最初と最後の頁<br>230-238 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/978-3-031-35989-7_29 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>MANABU ISHIHARA , YUKI ISO | ４．巻<br>1 |
| ２．論文標題<br>Reproduce the movement of the injection needle with a haptic device | ５．発行年<br>2022年 |
| ３．雑誌名<br>Proc. of The 2022 IEEE 4th Global Conference on Life Sciences and Technologies (LifeTech 2022) | ６．最初と最後の頁<br>627-629 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/LifeTech53646.2022 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

〔学会発表〕　計5件（うち招待講演　0件／うち国際学会　0件）

| |
|---|
| 1．発表者名<br>石原学 |
| 2．発表標題<br>表面粗さの変化と感覚量の関係について |
| 3．学会等名<br>2023年　電気学会　電子・情報・システム部門大会 |
| 4．発表年<br>2023年 |

| |
|---|
| 1．発表者名<br>大和田一裕、飯島洋祐、石原学 |
| 2．発表標題<br>力覚で再現する触覚特性について |
| 3．学会等名<br>2022年 電気学会 電子・情報・システム部門大会 |
| 4．発表年<br>2022年 |

| |
|---|
| 1．発表者名<br>掛川祐亮，石原 学 |
| 2．発表標題<br>ディスプレイ表面形状の変化と感覚量について |
| 3．学会等名<br>2021年度（第12回）電気学会東京支部 群馬支所・栃木支所 合同研究発表会 |
| 4．発表年<br>2022年 |

| |
|---|
| 1．発表者名<br>石原 学，干川尚人 |
| 2．発表標題<br>サイバーセキュリティ演習システムの開発 |
| 3．学会等名<br>令和4年電気学会全国大会講演論文集 |
| 4．発表年<br>2022年 |

| |
|---|
| １．発表者名<br>小保方俊介，石原 学 |
| ２．発表標題<br>機械学習によるスパムメール認定の機能比較 |
| ３．学会等名<br>令和4年電気学会全国大会講演論文集 |
| ４．発表年<br>2022年 |

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|