修士論文概要 「環境情報からのメッセージ」情報環境専攻

名前	指導教員	論題	論文要約
松崎 太一	岡嶋　克典	指合わせ MR 文字入力インターフェースの開発	HMD を用いた複合現実 (MR) においては,仮想キーボードを用いた文字入力が主流であるが,視野の制限や腕の疲労等様々な問題がある.本研究では,そのような課題を解決し,さらにより使いやすいひらがなの入力インターフェースを開発し,その有用性を検討した.提案するインターフェースは右手の指先と左手の指先・指関節を接触させることによってひらがな入力できる.前方への注意が必要な状況を想定した実験において仮想キーボード文字入力と今回開発した方法の比較を行った結果,今回開発したインターフェースの方がユーザビリティが高いことが示された.
石川 裕也	長尾 智晴	eGFR の変動に基づく慢性腎臓病患者の状態推移の可視化と解析	近年，慢性腎臓病患者の増加が危惧されており，症状進行の解明と将来の重症度予測が求められている．患者をクラスタリングし症状を解析する従来研究は，クラスタ単位の解析であり個人の詳しい解析には向いていない．本論文では，慢性腎臓病の重症度指標 eGFR の変動に基づく患者の状態推移の可視化手法と，その状態推移の評価手法を提案する．実験では，提案手法の有効性の検証と，1 年後の eGFR の予測精度の検証を行った.

石田 真規	森 辰則	会話スレッドに着目した皮肉の文脈生成のための 言語アイロニーの収集と検出	Twitter などのマイクロブログ上での発話は文脈が欠落していることが多い。我々は発話自体に皮肉の意図を持つ言語アイロニーとその文脈を一連の会話の中に登場するものとみなして会話データを収集した。収集方法にはクエリの指定方法など更なる改善点が見つかった。また、収集した会話データから言語アイロニーを検出する判定器も作成した。判定結果は概ね良好だったが、誤分類されたデータを分析したところ人間の無意識な文脈補完が原因でラベル付けに問題が見つかった。より高品質な言語アイロニーを抽出するためには字面の情報のみから文意を読み取る必要があると考えられる。
稲澤 朋也	吉岡 克成	IoT セキュリティ診断 Web サービス am I infected? の有用性に関する研究	家庭用 IoT 機器のマルウェア感染を背景として、近年、一般消費者による機器のセキュリティ改善が重要課題となっている。しかし、一般消費者にとって、自身で機器の設定等を見直し、適切な対策を講じることは極めて困難である。そこで本研究では、家庭内 IoT 機器のセキュリティ診断と必要な対策の把握を可能にする Web サービスを提案し、約 10 万人の一般消費者に提供してきた。本稿では、ユーザスタディやデータ分析を通じて、サービスの高い有用性を示す。
岩橋 虎	松本 勉	耐クローン性に優れたナノ人工物メトリックシステムの構築	人工物メトリクスとは，人工物固有の物理的特徴を用いて当該人工物の認証を行う技術であり，本物と同等の値が測定される別の物体（クローン）を作製することが極めて困難であるとする「耐クローン性」を有することが期待されている．本稿では，ナノメートルスケールの特徴を用いる「ナノ人工物メトリクス」において，新たな照合手法と画像の前処理を提案し，最も耐クローン性に優れたナノ人工物メトリックシステムを構築した．

岩山 大樹	森 辰則	議会会議録における二次情報の真偽判定手法の検討	議会会議録の二次情報文に対するファクトチェックの需要は高い。本研究では、議会会議録の質疑応答セッションの質問要約、答弁原文、そして関連情報から、答弁要約の内容の真偽を判定する手法を検討する。大規模言語モデル(LLM)を用いて、プロンプトの形式、及び用いる関連情報に関しての実験を行った。実験では答弁要約と答弁原文全文を用いた含意関係認識タスクと、答弁要約と質問要約の関係性判定タスクの二つに分け、結果を統合する手法が有効性を示した。
打越 天音	松本 勉	メタバースにおけるアバター操作者とワールドの認証に関する研究	様々なプロバイダによって、メタバースサービスが提供されている。メタバースサービス内でユーザの操作するアバターが第三者によって盗難される事例や、ユーザが作成したワールドの偽ワールドが作成され訪問者を騙す事例が問題となっている。本稿では、メタバースサービスを利用するユーザの心理的負担に配慮しつつ、ユーザと、ユーザの所有するアバターの認証に生体認証を利用する手法、およびワールド訪問者がワールドの正当性を検証できる手法を提案する。
内田 佳秀	森 辰則	短答式記述問題の自動採点における学習データ拡張手法の検討	近年、記述形式の試験の重要性が高まるとともに自動採点への注目が集まっている。しかし、学習データの確保が困難であり、未だ少数のデータを用いた研究では高精度の採点を実現するに至っていない。我々は既存のデータセットから逆翻訳や文節の入れ替え・結合により新たな解答を生成する手法を試した。提案手法で生成したデータを用いた学習では採点精度の向上が確認でき、さらに過学習により文の意味ではなく位置を学習してしまうという課題を解決する可能性を示すことができた。

遠藤 祐輝	吉岡 克成	IoT ボットネットを制御する攻撃者の活動分析に関する研究	近年，IoT ボットネットによるサイバー攻撃が大きな脅威となっている中で，その運用を行っている攻撃者の挙動を把握することが対策を行う上で重要である． 本研究では，IoT マルウェアの動的解析中の通信から機械学習により C&C サーバの特定を行う手法を提案する．また，継続的な C&C サーバの監視やハニーポット，動的解析結果などから得た情報を元に IoT ボットネットの攻撃インフラや攻撃活動の実態を分析する．
大迫 翔	小関 健太	極大外平面グラフにおける odd-coloring	Odd-coloring と呼ばれる、頂点彩色に加えて近傍に奇数個存在する色が必ずあるという条件付きの彩色を考える。全ての頂点が外領域と接している外平面グラフは、5 色で odd-coloring 出来ることが示されている。本研究では、odd-coloring は辺を増やすことで必要な色数が減ることがある性質を利用して、外平面グラフに辺をどのように加えても外平面グラフではなくなる極大外平面グラフが 4 色で odd-coloring 出来ることを証明した。
大城 陽斗	野間 淳	Ideal sheaf として 3 曲面の共通部分になる空間曲線を含まない liaison class の構成	射影空間内の曲線 C,C'に対して，ある完全交叉 V が存在して C∪C^'=V を満たすとき，C,C'は liaison の関係にあるという．この liaison は同値関係であり，同値類(liaison class)の研究が盛んに行われている．本研究では，Ideal sheaf として 3 曲面の共通部分になる曲線に着目し，これを全く含まないような liaison class がどのようになるか研究した．Class と対応する R-加群 M の形で表すことで結果が得られ(R は 4 変数多項式環)，以下に，その具体的な結果を示す； (1) M=R/(X,Y,Z,T^m) ただし，m は 2 以上の整数 (2) M=R/(X,Y^2,Z^2,T^m) ただし，m は 2 または 4 以上の整数 これらの一般化された結果は現時点では得ることができず，今後の研究課題である．

大橋 俊介	松井 和己	周波数領域法によるカーテンウォールの疲労損傷評価	カーテンウォールの疲労強度を定量的に評価するために，変動する風圧を外力とする構造解析により，局所的な応力を求め，疲労評価を行った．風のようなランダム振動において，時間領域による疲労評価では，十分に長い時系列を入力としなければ，実際より危険側を示す可能性がある．本研究では，応力時系列を，応力パワースペクトル密度に変換し，周波数領域法による疲労評価を行い，本手法の傾向や時系列の選択範囲に対する依存性を調査した
大原 広嗣	森 辰則	発話文口調変換タスクにおける教師なしテキストスタイル変換手法の比較検討	対話システムの応答口調を適切に制御できれば、システムがより自然で親しい会話を実現することに繋がる。我々は教師なしテキストスタイル変換手法に着目し、特定口調を持つ発話文から深層学習で口調変換モデルを生成する手法について、使用するデータの種類や量などを比較しながら教師あり手法を含めて複数手法を検討した。実験の結果、逆翻訳による対訳データ生成手法が教師あり手法に匹敵する高い変換性能を示し、データ量が限られる場合では ChatGPT を使用した Few-shot 学習が最も有効だと判明した。
小笠 原匠	原下 秀士	楕円曲線の二重被覆曲線として得られる種数４の超特別曲線	暗号理論や符号理論への応用が期待される「超特別曲線」の存在性について研究を行った。先行研究によって種数３以下の曲線は超特別曲線の分類がなされているが、種数４の場合は一般には未解決である。本研究では、種数 4 の曲線のうち楕円曲線の二重被覆曲線として得られる曲線 : DCEC について研究を行った。代数計算機システム Magma を用いて、DCEC の非特異性の条件式、および標数 5 から 23 までの超特別な DCEC の同型類の個数の数え上げに成功した。

柏木 啓吾	岡嶋 克典	色透明視と色順応に基づく色恒常性の計算モデル	照明光が変化しても同じ物体の色は安定して白色照明下と同じ色として知覚できる現象を色恒常性という.色順応が働いた際の色恒常性を予測する順応型モデルは存在するが,瞬間的に生じる色恒常性はこのモデルでは説明がつかない.本研究は瞬間的に生じる色恒常性を 2 種の色マッチング法を用いて実験した.結果から,瞬間的な色順応条件下では Surface color match において部分的な色恒常性が見られた. また色順応条件下での色恒常性も測定 したところ Appearance color match においても色恒常性が生じ,Surface color match においても色恒常性が向上した.これらの結果は色透明視に基づく計算モデルで定量的に予測できることがわかった.
金子 拓未	中本 敦浩	アニュラスの直交分割とそのグラフ表現	平面直交分割とは、長方形の中に鉛直線分と水平線分を配置し、それらの線分の両端点は他の線分か境界の線分の内点と一致しているものである。この平面直行分割の線分の接触関係により作られたグラフは、内点の出次数が 2 の有向平面四角形分割となる。一方、その有向平面四角形分割は平面直交分割の表現をもつことが知られている。本研究では、アニュラス上の境界に円周を配置し、曲面には鉛直線分と水平線分を配置した幾何学的対象を用意し、同様な議論ができないか研究を行った。
岸本 泰俊	白川 真一	Neural Additive Models を用いた表現力が高い局所的説明手法の提案	ブラックボックスモデルの予測根拠を説明する手法として Local Interpretable Model-Agnostic Explanations (LIME) がある. LIME はモデルの予測を線形モデルで局所的に近似する手法だが,線形関数による説明に限られる.本研究では,非線形関数による説明が可能な Neural Additive Models (NAM) やその改良手法である特徴選択つき NAM を用いたより表現力が高い局所的説明手法を提案する.

小島 雅大	山田 貴博	モード分析手法を用いた都市キャノピー内外に形成される乱流構造の分析	本研究では，都市キャノピーを再現した一様に並ぶブロック群における流速場に対して，データを低次元基底に分割する固有直交分解（POD）を用いることで，都市キャノピー内外に形成される乱流構造の分析を行った．乱流境界層と都市キャノピーによるコヒーレント渦に起因する流れ構造を調べた．また，POD モードから 5 つの低次モデル（ROM）を生成し、ROM による元の流れ場の再現性を評価した．
小永井 周	中本 敦浩	メビウスバンド上のグラフにおける *star coloring*	グラフ G の *star coloring* とは、G の頂点彩色で、任意の 2 色から誘導される部分グラフが star になるという制約を追加したものであり、acyclic coloring の条件をより厳しくしたものとして知られている。*star coloring* の染色数について、あまり多くは知られていないが、外平面二部グラフが、染色数の上界と下界が一致する例として先行研究で示されていた。本研究は、メビウスバンド上のグラフで、外平面二部グラフと同様の構造を持つ二部グラフを対象に研究を進めた。
才納 明英	吉岡 克成	Web 検索から偽ショッピングサイトへの誘導に関する分析	本研究では，実ユーザの Web アクセスログを分析することで，Web 検索から偽ショッピングサイトへと到達する可能性のある状況についての実態調査を行った． 分析の結果，検索結果ページの約 5%に偽ショッピングサイトに到達する踏み台サイトの URL が含まれていたことを確認し，身近な脅威であることを確認した． また，偽ショッピングサイトへの到達前後の行動からは，商品やその情報を得ようとして様々な Web 検索を試みて様々なサイトへアクセスする振る舞いが伺えた．

坂田 元希	白川 真一	話者の周囲の環境情報を考慮したジェスチャ生成モデルの提案	ジェスチャ生成モデルは発話音声や発話テキストのような発話情報や，話者に関する情報を入力としてジェスチャを出力する．人間のジェスチャはモニタの位置などの周囲の環境に影響を受け変化すると考えられる．しかし，既存のジェスチャ生成モデルはこれを考慮していないため，環境に適したジェスチャの生成は困難である．本研究では，発話情報に加えて話者の周囲の環境に関する情報を反映するジェスチャ生成モデルを提案する．
白石 一真	四方 順司	指定演算者型の準同型署名に関する研究	本研究では， 署名者が演算者を指定可能， かつ任意の演算に対応できる準同型署名方式及びマルチキーを用いた方式のモデルと構成を示した． また， 本研究では線形準同型署名と指定開示者型の関数型コミットメントを基に指定演算者型準同型署名を構成できる事を示した． これにより， 任意の演算に対応し， かつ格子に基づいた耐量子 性の準同型署名の構成が得られる． すなわち， 量子コンピュータでも解けない安全性を持ち， 任意の第三者に演算ができない，任意の演算が行える準同型 署名の構成が可能となる．
鈴木 雄大	白川 真一	ヒト iPS 細胞由来神経細胞を用いた化合物の神経毒性評価への機械学習の応用	化合物の神経毒性評価における動物実験の代替法として，ヒト iPS 細胞由来神経細胞を用いた評価法が注目されている．この評価には神経細胞より取得した電気信号から検出される特徴が利用されている．本研究では，神経細胞の電気信号からの特徴抽出法を開発し，その特徴量を用いて機械学習による化合物の神経毒性評価を行う．そして，化合物ごとの正解率の分析や機械学習モデルの予測の説明を行う．

曽我 紗代子	富井 尚志	EVライフログを用いたEVのエネルギー変換効率推定	本稿では、電気自動車（Electric Vehicle：EV）の走行中の内部データを EV のライフログとして収集・蓄積し、それを用いて EV のモータ・インバータ総合効率マップを推定した。さらに、推定したマップを用いて消費エネルギー推定を行い、その精度評価を行った。このマップにより、消費エネルギーの要因の内訳が明らかとなり、速度や加減速の方法といった運転改善の判断材料に有用である。
曽我部 亮	森 辰則	言語モデルを用いた生成タスクにおける繰り返し問題改善に関する研究	Scaling Law が示されて以降、言語モデルの大規模化が進んできているが、社会実装においては費用対効果の観点で、軽量かつ高性能な言語モデルの需要が高い。そのような言語モデルを用いた生成タスクにおいて、繰り返し同じ単語や系列が生成されてしまうという現象が存在する。本研究では、その問題に対して学習データのラベルバランスの側面からアプローチし、生成型要約において繰り返し問題を改善する結果を示すことが出来た。
高木 優磨	長尾 智晴	VAE による潜在空間を介した曲調変更手法の提案	自動作曲において、生成する楽曲のコントロールについては未だ研究の余地がある．本論文では、楽曲の曲調を変更する手法について提案する．本研究では、まず拍子を対象とし、4 拍子の曲の 3 拍子へのアレンジを目標とした．提案手法では、まず楽曲が 3 拍子と 4 拍子どちらであるかを判定する 2 クラス分類器を獲得し、分類器が 3 拍子と判定するようなメロディを生成するように、学習済みの VAE のファインチューニングを行う．主観評価によって、原曲を維持しつつ、3 拍子へのアレンジが達成されていることを確認した．

高安 雅人	長尾 智晴	ユーザの嗜好によって最適化された音楽評価関数の作成	昨今，生成モデルの学習に用いるデータの著作権について，問題視されている．また，生成モデルの普及に伴ったコンテンツの急増が懸念されており，推薦システムの需要が高まっているが，既存の推薦手法はコールドスタートの課題がある．そこで本論文では，元データを復元できない特徴量を用いてモデルを学習し，ユーザの嗜好情報を模倣する手法として，ユーザの評価によって最適化された音楽評価関数を提案する．実験では，軽量性，学習容易性，予測精度，データ復元不可能性の 4 つの観点から，音楽評価関数の有効性を検証する．
瀧山 輝	山田 貴博	縫合手技の力学的評価における実験手法の構築	縫合手技を力学的データから定量的に評価するための実験手法を構築した．臓器の代わりに模擬臓器を使用して実際の縫合手技を模擬した実験を行った．評価指標となる力学的データとして臓器表面の変形状態に着目し，縫合時の模擬臓器の表面ひずみを実験により計測した．また，実験内容だが、異なる条件の手技で縫合を行った時の変形状態を比較することで，各条件が変形状態へ与える影響を考察し，手技の評価を行った．
谷崎 俊介	吉岡 克成	二重脅迫型ランサムウェアに対するエンドポイントセキュリティ製品の振る舞い検知機能の評価	ファイルの暗号化や削除に加えてファイルの外部送信を行う二重脅迫型ランサムウェアは脅威である．本研究は 7 つのアンチウイルスソフトと 1 つの EDR を対象にエンドポイントセキュリティ製品が二重脅迫型ランサムウェアに対してどの程度有効なのかを調査した．製品がインストールされているマシン上でランサムウェアのテスト検体を実行したところ，テスト検体の振る舞いを検知し実行を阻止できた製品は少なかった．

近野 真生	松本 勉	FPGA に実装可能な レーザー検知センサに関する研究	レーザーフォールト攻撃を検知するためのデジタルセンサが提案されおり，デジタルセンサの一つにリングオシレータを用いたものが提案されている．本研究では，先行研究で提案されたリングオシレータを用いたレーザー検知センサがレーザーの検知が十分に行えていないこと，レーザーのパルス幅やパワーを小さくするとレーザー検知が十分に行えなくなることを示す．また，改善案を提案し，その有効性を示す．
知久 奏斗	四方 順司	ID ベースマッチメイキング暗号の安全性向上に関する研究	ID ベースマッチメイキング暗号(IB-ME)は送信者と受信者が相互に ID を指定できる暗号方式である．IB-ME において，鍵生成局と呼ばれる第 3 者機関が各ユーザーの秘密鍵を生成することから，鍵エスクロー問題と呼ばれる課題がある．また，一般的な暗号化方式や署名方式に求められる安全性を満たしていないという問題点も挙げられる．そこで本研究では，鍵エスクロー問題を回避する IB-ME 方式や強い安全性を満たす IB-ME 方式を構成した．
東明 幸太	森 辰則	回答自動生成のための 事故事例の構造化･可視化システムの構築	製造業などの企業では、現場で発生した事故についての問い合わせに対して人手で回答しており、非効率的である。そのため、自動回答を行うシステムの需要が大きい。本研究では、システム回答に構造化した事故の流れの可視表現を含めることで原因等を分かりやすく示すことを目指している。そのためのプレインテキストから事故の流れを構造化するための注釈付けの枠組みを検討し、『失敗知識データベース』の一部の事例に対し注釈付けを行い、コーパスを整備した。また、GPT-4 を利用し、構造化を行うためのシステムを構築した。システムの性能を測定した評価実験では、改善の余地があることが示された。

中田 勇気	原下 秀士	ゴナリティが 4 の種数 5 の曲線の 6 次モデルの分類	3 つの 5 変数 2 次式が定める種数が 5 の曲線は、ある平面 6 次曲線と双有理同値であることが知られている。本研究では、その平面 6 次曲線の特異点の分類を理論的・実験的手法を用いて試みており、具体的には、分類された特異点のタイプごとの曲線の空間の次元の計算を、コンピュータプログラムを用いて行った。結果として、標数 0 の全 7 種の特異点のタイプに対する次元の決定に成功した。今後の課題として、他の標数における次元の結果の計算等が挙げられる。
中西 諒	長尾 智晴	人の知識に基づいた植物工場における栽培条件の最適化	人工光型植物工場ではさまざまな栽培条件を精密に制御でき，安定して植物を栽培できる．一方で，費用が高く，それに対して収益が低いことが課題である．本論文では収益向上のために植物の成長速度を高める栽培条件を求める手法を提案する．提案手法では，あらかじめ集約，分析した人の知識に基づいた制約によって栽培データ数の少なさを補う．本手法を栽培データに適用した結果，従来よりも高い成長率が期待される栽培条件を発見した．
西村 伶	長尾 智晴	テキストによる 3D モーションの性質強化	近年，人間の 3D モデルや３D モーションは様々な分野で研究・活用されている．また、高度な技術や高価な機材を必要とせず，僅かな入力からユーザが簡単に３D モーションを作成できるようになる AI モデルも数多く研究されている．その中でも自然言語テキストを入力として 3D モーションを生成するモデルの学習に作用して，生成されるモーションの動きの性質を強化するテキストデータセットの作成手法について提案する．

二宮 聡太	藤井友比呂	英語疑問文形成規則に対する競合仮説のモデル構築とその比較: ベイズ推定によるアプローチ	ベイズ推定を用いたアプローチにより英語疑問文形成規則の仮説獲得モデルを構築し、定量的な仮説獲得の検証を行った。このモデルは、変形規則の単純性、コーパスへの適合度のトレードオフを評価する。実験の結果、線形規則が単純性の観点で優位性を示したが、現実コーパスから大人の発話だけを頼りに英語話者が実際に用いている主節の助動詞を先頭に動かす構造仮説を獲得できることが示唆された。
橋本 春輝	岡嶋 克典	HMD 装着時の輻輳特性を考慮した焦点ボケのシミュレーションとその応用	HMD で VR 環境を観察時に視点位置から輻輳距離を計測すると，注視点までの距離と「ずれ」が生じる．本研究では，輻輳距離を補正して仮想空間内における注視点までの距離を取得する手法を開発し，適切な焦点ボケを付加させる VR システムを開発した．このキャリブレーションシステムの有用性を確かめるために，VR 環境と実環境で実験を行い，提案する輻輳距離の補正システムで，従来の焦点ボケがない VR 環境よりも現実に近い見え方を再現でき，有効性を示した．
廣居 樹	富井 尚志	PV と EV を統合する負荷平準指向 VGIDB を用いたスマートグリッド導入効果の多角的定量化	本研究では、PV と EV を統合した新しいスマートグリッドのあり方である VGI を評価するための DB 設計とシミュレーション評価を行った。 シミュレーションでは EV 台数や PV 導入量をパラメータとし、その結果を DB に格納して定型質問処理を行い、導入効果を定量化した。 複数の評価指標を設定し、多角的に定量評価することで、PV と EV が同時に増加すればするほど効果が大きくなることなどを定量的に示した。

福谷 勇輝	山田 貴博	シミュレーションモデルに対する信ぴょう性評価	本研究ではV&Vの最下層である材料レベルの問題において，材料試験とそれに基づいて材料パラメータを同定した「較正済み材料モデル」の認識論的不確かさを定量化にすることにより，信ぴょう性を評価する．材料試験で同定に利用する応答だけでなくそれ以外の応答も計測し，較正した材料モデルがその応答をどの程度再現できるかを確認することで認識論的不確かさを定量化する．認識論的不確かさを定量化することで，そのシミュレーションモデルを用いた予測に対する信ぴょう性が高くなることを示す．
藤本 春樹	四方 順司	LPN 問題に基づくプロキシ再暗号化の構成に関する研究	Learning Parity with Noise (LPN) 問題の困難性に基づくプロキシ再暗号化 方式を提案する．耐量子性を持った PRE としてこれまでは格子に基づく方式しか提案されていない．提案方式は LPN に基づく最初の PRE 方式である． 本研究では，Dottling et al. (ASIACRYPT 2012) による LPN ベース公開鍵暗号方式に対して構成し，正当性と CPA 安全性を示す．
前田 理玖	岡嶋 克典	自律神経系の変調が味覚に与える影響	五感と自律神経系は人間の行動、感情、健康に深く関わっており、特に味覚は日常生活において重要な感覚の一つである。本研究は、味覚と自律神経系の相互作用を明らかにするために、運動による味覚感覚の変化に着目し、心拍数と味覚閾値の相関を検証した。味覚閾値の時間変化の結果から自律神経系の変調が味覚に影響を与えている可能性を示した。また味覚感度が変わる仕組みについて脳や体の反応を基に考察した。

松岡 耀志朗	四方 順司	鍵圧縮およびデータ圧縮を可能にするメッセージ認証方式に関する研究	本論文では，鍵圧縮とデータ圧縮を同時に実現するプロキシ再認証方式を提案する．この方式では，プロキシを介して送信者のもつ秘密鍵で生成したデータ認証子を異なる秘密鍵をもつ受信者が検証可能な認証子に変換することで，鍵圧縮を実現する．さらに，集約メッセージ認証のアイデアを基にして，複数の認証子を集約することで送受信時のデータの圧縮も実現可能であることを示す． 本論文ではプロキシ再認証方式の具体的な構成として，鍵準同型疑似ランダム関数に基づいた構成と離散対数問題の困難性に基づいた構成の二つを提案する．
松本 悠汰	白川 真一	最適輸送を用いたサンプル重み付け手法の複雑な分布シフトのための改良	分布シフトは学習データの分布とテストデータの分布が異なる問題のことであり，機械学 習モデルの性能を低下させる．サンプル重み付けはデータに重みを与えることで，各デー タが機械学習モデルの更新に与える影響を変える手法であり，適切な重みを与えることで 分布シフトに対して有効な手法である．本研究では最適輸送を用いた既存手法を改良し， ラベルノイズとクラス不均衡が混在する複雑な設定においても有効な手法を提案する．
松本 涼	長尾 智晴	新興感染症バイタルデータのシミュレーションモデルの構築	昨今の新型コロナウイルス感染症のパンデミックを契機に，新興感染症の流行下でひっ迫した医療現場でのニーズを満たすモデルを構築する研究が進められている．本論文では，患者の予後ごとにバイタルデータの時系列変化をシミュレーションするモデルの構築によって，各ニーズを医学的に具体性のある形で満たすことを目的とする．データリソースを効率的に活用したシミュレーションモデルの構築を提案し，これによって比較的高い水準でニーズを満たせる可能性を確認した．

馬渕 優希	白川 真一	SNS ダンスデータセットの作成とダンス生成モデル学習への適用	振付家によるダンスの創作を補助するために，機械学習を用いて音楽に合ったダンスを自動的に生成する研究が行われている．近年，SNS 等で短時間かつキャッチーなダンスの需要が高くなっている．しかし，ダンスの自動生成モデルのデータセットは長時間かつ複雑な動きが収録されており，SNS 等に適したダンスを生成することが困難である．本研究では，短時間かつキャッチーな振付のデータセットを作成し，学習したモデルの評価を行う．
宮田 大翔	松本 勉	リソース制約のある IoT 機器におけるペアリング計算の 実装と評価	IoT 機器間の通信にペアリング暗号が利用されることがあるが、核となるペアリング計算は計算コストが高く、小さな RAM 容量を持つ IoT デバイスでの実装が難しいことがある。 本研究では、将来の長期的な安全性確保に向けて 256 ビットセキュリティが検討されていることを踏まえ、128 ビットセキュリティ程度の GMT8-542、256 ビットセキュリティの BLS48-581 曲線を使用し、最小限の計算リソースを持つデバイス向けの実装を提案した上で、セキュリティレベルと計算コストの関係を明らかにする。
宮野 光太	牛越 惠理佳	3 次元空間における接合部を持つ弾性体の固有振動の漸近挙動	均質等方弾性体の固有振動の数理解析は古くから多くの研究が展開されてきた．その中で Kerdid(1997)により 2 本の直方体をＬ字型に接合した状態の固有振動の解析がなされ，そして近年になって Jimbo-Rodriguez Mulet(2020)により、非一様な断面を持つ柱状の弾性体の解析が可能となった。そこで本研究では、より一般的な形状の接合部をもつ弾性体の固有振動に対する数理解析の土台を作り，固有値の漸近オーダーの導出に成功した．

村田 基	岡嶋 克典	三次元追従可能な非同軸プロジェクションカメラ食品仮装システムの開発と クロスモーダル効果の検証	三次元追従可能な動的プロジェクションマッピングには主に同軸プロジェクタ・カメラシステムが用いられるが，繊細な光軸調整が必要である.そこで本研究では非同軸プロジェクタ・カメラシステムを用いて，導入しやすく高精度な三次元追従を可能とした動的プロジェクションマッピングシステムを開発した.本システムを用いて食品の外観を操作することで味覚や食感へのクロスモーダル効果を検証し， 食体験の向上を示した.
森 悠太	山田 貴博	模擬臓器の押込み試験によるモデル化の信憑性評価	非均質な臓器の物性値を取得するために，低侵襲押込み試験および逆解析を用いた物性同定法の開発を行った．本研究では，まず均質体レベルで物性同定法の妥当性確認を行った．均質材料で作成した模擬臓器に対して押込み試験を行い，反力と変形を計測した．模擬臓器の材料パラメータを引張試験から同定し，順解析を行った．実験結果と解析結果の応答を比較することで物性同定法の妥当性確認を均質体レベルで行った.
森井 裕大	吉岡 克成	OSS脆弱性に対するIoT機器メーカの対応に関する分析	本研究では，脆弱性管理手法の一つとして近年注目を集めるSoftware Composition AnalysisツールをIoT機器のファームウェアに適用し，Open Source Softwareの脆弱性に対するIoTメーカの対応状況に関する分析を行った．その結果，ファームウェアリリース時の公知の脆弱性の対応状況にメーカ間の差異が存在すること，ファームウェア更新によって脆弱性が増加する事例が存在することが確認された.

安井 浩基	吉岡 克成	実機を用いた攻撃観測による IoT マルウェアの活動実態把握に関する研究	近年の IoT マルウェアは高度な機能をもち仮想環境による実験だけでは明らかにできない実態がある。本研究では IoT 機器の実機を囮とする観測システムを運用し、IoT ランサムウェアの実態調査と IoT ボットの生存競争の調査を行った。前者では攻撃インフラの運用が自動化され利益の最大化が図られていることを明らかにし、後者では攻撃者による主導権争いによって脆弱機器の感染状態が観測時期や機器固有の性質によって大きく変わることを明らかにした。
吉田 洋生	長尾 智晴	拡散モデルに対する概念制約の導入による錦鯉評価システムのための疑似画像生成	近年，錦鯉文化の国際的な需要拡大に伴い，オンラインでの錦鯉品評会の必要性が生じている．オンライン品評会では機械学習による公平な評定が期待される一方で，その学習に必要な大量の画像データの確保に課題がある．そこで本論文では，既知の個体から錦鯉固有の概念を学習し，条件として与えることで現実的で高品質な擬似画像データを生成する手法を提案する．実験では，生成画像の定性的な比較と知覚的な定量指標によって有効性の検証と有用な条件の特定を行う．
芳谷 和哉	山田 貴博	はり･板の動的解析のための混合型有限要素法に対する分離型時間積分	本研究では，Timoshenko はり要素と Mindlin-Reissner 板要素に対して，せん断応力と軸方向応力の両方か一方を独立変数とする混合型有限要素法を採用し，分離型時間積分を適用する．このとき，曲げ変形について陽的時間積分，その他の変形について陰的時間積分となる手法が得られ，陽解法における時間刻みの制約が緩和される．また，数値実験により，提案する手法の数値特性を評価する．

鷲巣 正顕	岡嶋 克典	色知覚と形状知覚を用いた動的聴覚誘発視覚像錯視メカニズムの解明	連続する3つの音によって、同期する２つの光が3つに見える視聴覚連動錯視は、クロスモーダル効果による事後予測で生じる錯視である。しかし、視覚刺激の１つめと2つめの色や形状が違う光刺激の場合にも、その錯視が生じるかは不明であった。本研究では、前後の光錯視の色や形が違っていても視聴覚連動錯視は発生することを示すとともに、前後の光刺激のどちらが優勢に中間に補完されるかは個人によって異なることを示す。
何 鎮洋	松井 和己	多結晶体に対する剛性･強度の確率的評価に関する研究	現時点では、セラミックス材料の内部構造の解明に使われる手法による破壊は不可逆的なので、元の実験体における Verification ができなくなる。そこで本研究は、Voronoi 分割を応用し、後方散乱電子回折法から得られたマイクロカンチレバーの Top Surface の情報に基づいて、内部構造を推測する。また、多結晶体モデルに対する剛性・強度評価シミュレーションを行う際に必要な高速化技術（共役勾配法）に取り組む。
カン ミンジェ	四方 順司	高速フーリエ変換法またはハイブリッドサンプラーを利用した検索可能暗号の高速化に関する研究	近年は量子コンピュータの技術の進歩により、多くの暗号アルゴリズムが量子コンピュータによる攻撃で破られる可能性があることが示されている。このため、耐量子計算機暗号に関する研究が多く進められている。検索可能な公開鍵暗号(PEKS)に対しても、耐量子性を持つ格子暗号の中の一つである NTRU 暗号を基盤とする研究が進められている。しかし、既存の NTRU 基盤の検索可能な公開鍵暗号(PEKS)はトラップドア生成の際に O(n^2)時間がかかるガウシアンサンプラーを使用しているため、本論文では FALCON の高速フーリエサンプラーと ANTRAG のハイブリッドサンプラーを適用してトラップドア生成時間を O(n log n) に向上する構造を提案する。そして、これら 2 方式の効率性を比較評価する。

黄 犇	岡嶋 克典	仮想空間コミュニケーションシステムにおけるアバターの実画像化	仮想現実システムにおけるコミュニケーションの真実度を高めるため，アバターを実画像化する新たな手法を提案する．３台のカメラを用いてアバターを写実化し，HMD を用いずとも臨場感が高い新たな仮想空間コミュニケーションシステムを開発した．性能測定の結果，提案モデルは，リアルタイム処理可能であり，従来の仮想現実システムよりも真実度と没入感が高いことが示された．
謝 ニノ	長尾 智晴	人の判断根拠を活用した画像分類における悪影響画像検出	CNN を用いた画像分類において，大量の学習データが必要であり，モデルの判断根拠が解釈しにくいという課題がある．本論文は，人の判断根拠領域アノテーションとヒートマップを活用して，悪影響を及ぼす可能性のある画像を検出する手法を提案する．具体的には，アノテーションによって人の意見が分かれる画像とヒートマップを用いて同一物体が多数存在する画像を特定し，データセットから除外することで，モデルの精度向上を目指す．
CHEN YEN-HSIU	白川 真一	Split Inference のための離散的埋め込み表現を 用いたニューラルネットワークの構造探索	Split inference は，AI モデルを分割し，エッジデバイスとサーバ側にそれぞれを設置して推論を行う手法である．この手法により，cloud computing のプライバシー問題や大量のデータ転送に伴う遅延を軽減することができる．また，モデルの構造や分割点によってデータ転送量や演算量が変化する．一方，既存のモデルが split inference に適しているわけではない．本研究では，多様なモデルで split inference を活用するため，split inference に適したモデル構造を自動的に探索し，データ転送量を削減してモデル全体の遅延を削減する手法を提案する．

劉 屹	富井 尚志	風況を考慮したEVのエネルギーベースラインマップの作成と長期間実走行データによる精度検証	我々の先行研究では，道路勾配が説明する必須となるエネルギー消費を地図上に可視化したEVのエネルギーベースラインマップ(Energy Baseline Map: EBM)を提案した.EBMには風の影響を考慮しないという欠点があった. 本稿では,公開されている気象データを利用して，EBMの空気抵抗算出部分を改善し,風の影響を考慮したエネルギーベースラインマップ(Energy Baseline Map-Corection of Airspeed: EBM-CA)を提案する．長期間に渡って蓄積したEVの実走行データを用いて，EBM-CAとEBMを比較したところ，EBM-CAの予測精度が向上したことが確認された.さらにEBM-CAを利用して場所ごとに可視化し，季節風によるEVのエネルギー消費への影響を示した.