学位論文概要「環境情報からのメッセージ」

情報メディア環境学専攻　情報メディア学コース

名前	指導教員	論題	論文要約
大鹿智央	四方順司	ID ベース準同型暗号を用いた高機能暗号の構成に関する研究	ネットワーク技術の発展に伴い、盗聴者が存在する通信路を用いた情報の送受信が頻繁に行われている。このような盗聴者に対する情報の秘匿を目的とした技術が暗号化技術であり、多様な盗聴者に対応できるような安全な暗号技術の開発が求められている。近年では、安全性だけでなく機能性にも重きが置かれており、暗号化したまま平文の演算が可能な準同型暗号などが盛んに研究されている。私は、この準同型暗号が他のさまざまな機能を同時に持ち得るのかについて研究した。
肖 遥	吉岡克成	標的型メール攻撃のソーシャルエンジニアリング手法の分析に関する研究	近年、特定の個人や組織の機密情報を狙った標的型攻撃が増加している。標的型攻撃の手法が様々であるが、マルウェアを添付したメールを標的に送付する標的型メール攻撃が最も多いと言われる。マルウェアが受信者によって実行された際、標的に関連のある内容を含む囮の文書を表示し、感染の事実を気づかれないようにする場合が多い。囮文書はその性質から攻撃の標的に関連する情報を含んでいる場合が多く、その内容を分析することでマルウェア検体が送付された文脈や標的を推測できる。
楊　志勇	吉岡克成	ホームネットワークにおけるサイバー攻撃の観測と検証	近年、一般家庭では IoT 機器が増加しているに伴い、これらの機器へのサイバー攻撃が懸念されている。しかし，ホームネットワークにおけるサイバー攻撃の調査、分析、研究は十分ではなく、その実態は明らかでない。そこで我々は、家庭環境を模擬したテストベッドを構築し、想定されるサイバー攻撃について検討し、疑似的な攻撃を試行することで機器への影響を検証する。さらに、家庭向けのセキュリティ製品の効果を検証する枠組みを検討する。
阿久津諒平	岡嶋克典	文字の極性と観察者の年齢を考慮した視認性評価式	極性の異なるさまざまな条件で文字を呈示し、視認性を回答する実験を行い、テキストの極性を統合した新たな視認性評価式を得た。また、視認性評価式の文字サイズに関する特性と適用範囲を明らかにした。最後に高齢者を対象に実験を行った。若年者には見られない特性は、透光体混濁による白黒反転効果によるものと推測された。この効果と全体的なコントラスト感度の変化を考慮することで、高齢者向けの極性を問わない視認性評価式を得た。

飯塚 章裕	森辰則	指定語句に関連する文書部分に関する検索の検討	本研究では、東大入試世界史大論述問題の自動解答システムにおける検索部で、指定語句の構成語に分解したクエリの利用と、検索により獲得したパッセージのフィードバックによる検索質問拡張を用いた擬似関連性フィードバック手法を提案した。評価実験の結果、指定語句のに関連するパッセージの情報を付与することで検索における再現率が向上した。
飯塚洸平	長尾智晴	解析性を重視した画像特徴量抽出器の自動構築	工業への画像処理の応用の中で、解析性の高いモデルが重要となってきている。本論分では、解析性を重視した画像特徴量抽出器の自動構築手法を提案する。提案モデルは木構造状画像変換（GMA）と特徴量抽出器（SIFTER）をベースとして構築している。機能を限定した手法と比較して精度評価を行い、提案手法の有効性を確認した。
磯部康太	富井尚志	未知道路に対する EV の消費電力量推定システムの構築	本研究では、走行経験のない未知道路における電気自動車(EV)の消費電力量を事前推定するシステムを構築した。EV で未知道路を電欠の心配なしに走行するには事前に消費電力量に基づく走行計画を立てる必要がある。本稿では，設定したルートを走行する際の最小・最大消費電力量をシミュレーションから求めることで、電欠になる可能性がある範囲を実走行せずに提示する。これにより、計画作成の支援を行う。提案システムを用いた EV による実走実験を行い、本システムが提示する消費電力量の検証を行う。
伊藤有気	長尾智晴	ベイズ最適化を用いた植物工場における収穫量最大化	植物工場は収益増加が大きな課題であるが、収穫量最大化のための栽培実験はコストが大きく実験回数の制約が非常に強い。本研究では、こうした問題を対象とした、ベイズ最適化に距離制限を加える改良手法を提案する。ベンチマーク関数での評価実験では、最適解更新が頻繁であり、また最終的な解精度にも優れることを確認した。また、植物工場における収穫量最大化実験にも適用し、専門家の設定による栽培実験よりも乾燥重量で 40% 上回る環境条件設定を発見した。
茨木隆兵	富井尚志	スマートグリッド導入効果検討を目的としたエネルギーライフログ DB の構築	近年 IoT 技術の発達により、身の回りのエネルギーに関する記録(エネルギーライフログ）を容易に取得することが可能となった。本研究では，これらのログを、時間粒度を統一して蓄積する統合データベースを構築し、スマートグリッドにおけるエネルギーバランスのシミュレーションに適用する。また，本稿では、実データを用いてスマートグリッドの構成要素の導入量に応じたエネルギーバランスの分析を行い、統合データベースがスマートグリッド導入時の意思決定に有用であることを示した。

上野航	吉岡克成	サイバー攻撃分析機構を回避するマルウェアへの対策に関する研究	増大するサイバー攻撃に対応するために、防御側は囮のシステムであるハニーポットなどのサイバー攻撃分析機構を用いてサイバー攻撃の分析を行なっている。しかしながら、攻撃者は自らの攻撃手法が防御側に露見することを防ぐために、様々な手法でサイバー攻撃分析機構を検知し、回避を行うことが報告されている。そこで，本論文では攻撃者に回避されにくいサイバー攻撃分析機構について検討、実装、評価を行なった。
打越忠宏	四方順司	ハイブリッド暗号の理論的枠組みの拡張による高機能暗号の構成に関する研究	高機能暗号を KEM/DEM フレームワークを用いて構成する際、KEM と DEM をどのように構成し、組み合わせる必要があるかについて明らかになっていない。本論文では、フォワード安全公開鍵暗号と匿名型放送暗号を KEM/DEM フレームワークで構成し、KEM と DEM それぞれの満たすべき条件について解析を行う。その結果、KEM がそれら機能を持てば、構成される公開鍵暗号もその機能を持つことを示す。
海老名将宏	四方順司	弱い計算量仮定に基づく効率的なしきい値公開鍵暗号に関する研究	公開鍵暗号は何らかの計算量仮定に基づいて構成される。計算技術が著しく発展している現代において、できる限り弱い計算量仮定に基づいて構成することは重要な研究方針の一つである。この修士論文では，探索問題の困難に基づく、選択暗号文攻撃に対して安全なしきい値公開鍵暗号の効率的な構成法を提案する。さらに一部のパラメータ長をより効率的にするような構成法についても示し、既存研究との比較を行う。
奥冨賢哉	松本勉	AES 及びペアリング暗号の耐タンパーハードウェアに関する研究	近年、様々な情報機器にはその内部の情報や通信内容を守るため暗号技術が用いられている。しかし、情報機器に対し物理的な情報を用いたサイドチャネル攻撃が脅威となっている。情報機器の解読のしにくさを表す耐タンパー性という言葉が用いられている。耐タンパー性を向上させるために、現状で使用されている AES、今後使用が期待されるペアリング暗号に対し新たな脅威となりうる攻撃手法について検討する。
加藤里奈	吉岡克成	インフラ施設の遠隔監視制御システムを模したハニーポットの研究	本研究では、遠隔監視制御システムを模したハニーポットを実際の遠隔監視制御に用いるデータロガーや PLC を用いて構築し、当該システムへのアクセスの観測を試みた。観測されたアクセスのうち、特に人間がブラウザ等により行っていることが推測される通信に着目し、アクセス者の挙動を分析した。その結果，攻撃性の高い通信を躊躇なく行うアクセス者や調査目的と思われるアクセス者を観測し実際に運用状況の漏えいや不正な操作が行われる可能性があることがわかった。

狩野悌久	長尾智晴	感情ラベルを用いない連続的な顔表情空間の生成	機械学習において表情を扱う場合、表情に対して教師信号であるラベルを与えることが必要となる。しかし、データセット作成のコストの面から感情に紐づけられた one-hot なラベルが施され、表情の連続性は考慮されないことが多い。そこで本研究では表情に関するラベルを用いることなく、個人の特徴と切り離された表情の連続性をモデル内部で潜在空間として獲得することで顔表情空間を生成する手法を提案する。実験では、潜在空間の可視化・画像生成・教師なし表情分類タスクを行い、分離された被験者特徴・表情特徴および顔表情空間の有効性を検証する。
川合悠生	白川真一	畳み込みニューラルネットワークの入力画像に対する画像処理フィルタの動的選択	畳み込みニューラルネットワーク（CNN）は画像認識問題で高い性能を示している。CNN の入力画像に画像処理フィルタによる前処理を施すことで性能向上が望めることが報告されているが、適切なフィルタを問題に合わせて選択するのは試行錯誤や計算コストを要する。本論文では、使用するフィルタの確率分布をネットワークの学習中に最適化することで、CNN の前処理フィルタを効率的に選択する手法を提案する。複数のデータセットによる画像分類実験から、提案手法が性能向上に寄与することを示す。
河野　太一希	岡嶋克典	色と視覚的濁りが飲料の評価に与える影響	飲料の色のクロスモーダル効果についての研究は数多く存在するが、濁りについてのクロスモーダル効果についての研究はない。そこで、本研究では飲料の色だけでなく濁りを AR で変化させた時の味覚の評価への影響について実験を行った。実験の結果、視覚的濁りによって茶の苦さや果実飲料の果実感を増やすことができる反面、視覚的濁りを濃くしすぎてしまうと評価が下がってしまうことが示された。
斉藤翔汰	白川真一	深層学習のための 正則化付き動的構造最適化	深層ニューラルネットワーク（DNN）は画像認識などに応用されている主要な機械学習モデルのひとつである。これをスマートフォンなど計算資源が制約された環境に展開する際には、性能を保ちつつ省メモリな DNN の構造が要求される。本論文では、構造を確率モデルで表現することで構造と重みを同時最適化する手法に注目し、構造の複雑さに基づく正則化項を目的関数に導入した。提案手法を画像分類のための DNN に適用した結果、誤分類率の増加を 1%以内に収めつつ、重みを約 60%削減することに成功した。

齊藤祐亮	富井尚志	EV エネルギーライフログ DB における 消費電力量推定の精度検証	我々は、車両に後付けで搭載したデバイスで取得したセンサデータを利用して「その人が電気自動車(EV)で同じ運転をしたときの消費エネルギー」を推定し、EV エネルギーライフログとしてデータベースに蓄積する ECOLOG システムを構築・運用してきた。本論文では、 ECOLOG システムにおいて消費電力量の推定に用いる EV エネルギー消費モデルの精度検証を行った。精度検証に用いるデータにクレンジングを施すことで、従来の検証と比較してモデルの推定精度が向上したことを確認した。
齋藤蕗生	田村直良	ギター練習支援のための課題曲提案システムに関する研究	ギターのような楽器を演奏する際に演奏者は楽譜の特性に依存した「難しさ」を感じるが、それがどのようなものに依るのかは明らかにされていない。本研究では楽譜統計量の観点から楽譜の難易度に関わる要素を明らかにし、楽譜の難しさを定量化することを目的とした研究を行う。 本研究では人間の難易度に対する評価尺度を分析することで難易度に影響する要素を明らかにし、楽譜からの難易度の算出を可能にした。
櫻澤聡	松本勉	ToF 距離画像カメラの計測セキュリティ評価システムに関する研究	フィジカル空間の情報をサイバー空間へ取り込み、処理結果をフィジカル空間で活用する Cyber Physical System 等では、データを計測するセンサの「計測セキュリティ」が重要となる。本論文では 3 次元測距センサである ToF 距離画像カメラに対して、計測結果の integrity を脅かす攻撃手法である測定パルスなりすましを模擬攻撃として実行し、計測セキュリティを評価するシステムを構築したことを示す。また、実機の ToF 距離画像カメラを対象とした評価結果を示す。
沢田拓朗	岡嶋克典	印象判断の時間特性と脳内メカニズムの階層性	本論文では短時間で行われる印象判断に着目し、様々な画像を短時間提示して「明るさ」「美醜」「好み」の評価を行った。結果、明るさ知覚と魅力知覚が相互に影響を与えていたことを示した。また、魅力知覚のフィードバック処理が明るさ知覚に影響を与えた可能性を示唆した。実験の結果から、明るさと魅力知覚のフィードバック・フィードフォーワード処理が行われる印象判断の脳内メカニズムについて階層構造のモデルを提案した。

鈴木誠也	森辰則	Web 文書における引用記述の抽出手法の検討	Web 文書の情報信憑性判断のために、出典情報を提示するという研究がある。しかし、先行研究ではユーザによる Web 文書上の部分的な記述の入力を必要とし、それに対する出典情報（本研究では，引用されている記述とそれがもともと記述されていた引用元文書の組）を提示していた。それに対し、本研究は Web 文書から引用されていると考えられる記述を抽出する手法を提案し、先行研究と合わせた Web 文書に対する出典情報抽出全体の完成を目指した。
田中亮大	四方順司	認証子圧縮符号化および情報秘匿符号化に関する研究	近年、IoT 機器の普及や計算機の計算能力向上に伴い、情報の通信量が飛躍的に増加している。これに対し、情報の符号化理論を用いることで、長期的に計算機から情報を守る安全性と暗号通信に必要な通信コストや計算コストの効率性を向上させる暗号・認証技術が注目されている。本研究では、暗号・認証技術のそれぞれに対して符号理論的な手法を用いることで、新たに鍵無しで能動的攻撃者を考慮した情報秘匿符号化および異常デバイスの追跡機能を持つ認証子圧縮符号化を提案する。
田宮　和樹	吉岡克成	IoT 機器へのサイバー攻撃の実機を用いた観測と対策に関する研究	近年 IoT 機器に対するサイバー攻撃が増加している。攻撃を受けた IoT 機器はマルウェアに感染したり乗っ取られるなどして大きな問題となっている。本研究では IoT 機器に関するサイバー攻撃の「観測」と「対策」の 2 つの観点から研究を行なった。「観測」に関する研究では、囮の IP カメラを用い，IP カメラの覗き見の観測と分析を行なった。「対策」に関する研究では IoT マルウェア駆除と感染防止手法を提案し実機を用いてその有効性を検証した。
中嶋萌花	岡嶋克典	顔の表情認知における感情強度と向きの影響	現在の表情認識研究では顔向きや感情強度について考慮されていないものが多い。本研究ではこれらが表情認識に与える影響について検討した。顔向きについては正面顔と比較した際に横顔の感情認識が苦手な理由を検証すべく知覚学習実験を行なった。その結果、横顔表情認識が苦手な要因の一つに横顔を見る経験が不足していることが示唆された。また、Neutral から各表情顔へとモーフィングさせた刺激を用いて感情強度に関する実験を行った結果、顔特徴点の位置が各基本表情の方向へ近づくほど人もその感情を強く感じた.

西田 慎	吉岡克成	IoT 機器のセキュリティ不備をユーザへ通知する方法に関する研究	セキュリティ設定に不備のある IoT 機器やマルウェア感染した機器をネットワーク観測によって発見し、当該機器のユーザに対して対策のための通知や情報提供を行う活動の重要性が高まっている。この際、メールや SMS，専用サイトへの誘導といった通知方法が考えられ，それぞれの効果を比較する研究が行われている。本研究では、端末にインストールされた専用クライアントを通じて直接ユーザに通知を行う方法に着目する。ユーザ参加型のセキュリティプロジェクトである WarpDrive における通知実験を想定し、その効果測定方法を検討する。
西村晋平	長尾智晴	内発的動機づけとして「逃避」を導入した強化学習	本研究では、内発的動機づけの要素の 1 つである「逃避」のモデリングを行い、強化学習に適用することで、方策の学習性能を向上させる手法を提案する。逃避のモデリングはストレスとよばれる概念の導入およびストレスに基づいた学習タスクの切り替えで構成される。提案手法を導入した強化学習を用いて、シミュレーション環境で方策の学習を行ったところ、提案手法を取り入れなかった場合と比較して、学習性能の向上が確認できた。また、内発的動機づけの従来手法を導入した強化学習と比較して、ほぼ同程度の学習性能であることが確認できた。
野平浩生	松本勉	ステレオカメラの計測セキュリティに関する研究	ステレオカメラは、人命にかかわる、あるいは稼働できなくなると金銭的損害の大きいシステムで用いられている。そのため、ステレオカメラの計測セキュリティを高めることは社会的意義があるといえる。本稿では、ステレオカメラの計測原理やその実装の構成を洗い出したうえで、各実装の構成要素からどのような攻撃が考えられるかを示す。そして、その攻撃が脅威となる攻撃であることを実証する。さらに、攻撃手法の検討結果からステレオカメラの計測セキュリティの評価方法の確立に役立てる。
濱崎裕太	富井尚志	多変量データを SPJ 質問により統合する平行座標プロット型情報可視化システム	現在、センサ・ストレージ技術の発達やオープンデータの公開により、多くの属性を含むデータをすべて蓄積可能になった。しかしながら、多変量データの分析は一般に困難であり、可視化システムによる支援が不可欠である。これに対し本研究では、可視化手法の 1 つである PCP を SQL における SPJ に相当する表現力を持ち、操作結果の保存・再現できるよう拡張した情報可視化システムを提案する。また、小袖屏風と、自動車走行ログという異なる 2 つのコンテンツについて情報提示を行うことにより本システムの有用性を示す。

平山千明	長尾智晴	クラシファイアシステムを用いた搬送用ロボット群の渋滞緩和	搬送ロボット群の渋滞緩和および搬送時間の向上は、物流センターなどの実社会への導入に伴い、より重要性が増している。提案手法では、各ロボットの走行経路決定時に使用するダイクストラ法のパスコストを、ある定点上での周囲状態をもとに動的に変動させることで、渋滞を緩和させる経路の決定を行う。動的変動のためのルール獲得にはクラシファイアシステムを用いる。従来手法と比較して提案手法では、平均搬送時間が2.9%、一搬送にかかる最大時間が 7%以上減少した。
福原優太	森辰則	世界史大論述問題を解くための質問応答システムにおける各国史の利用	近年、大学入試（世界史分野）の大論述問題を解く質問応答の取り組みが盛んである。先行研究では問題を解くために教科書を検索するが、解答に含めるべき記述を取りこぼすという問題がある。そこで、本稿では各国史を新たな知識源として追加し、取りこぼした記述を網羅的に抽出することを検討する。
保泉 拓哉	吉岡克成	ネットワークスキャンを用いたユーザ環境の判別に関する研究	近年、十分なセキュリティ対策が施されていない IoT 機器を狙ったサイバー攻撃が脅威となっている。これは，個人が所有する IoT 機器について、これらのセキュリティ状態を把握せずに使用しているユーザが多いことが理由として考えられる。本研究では、通知の効率の向上を目的とし、個人の端末にインストールしたソフトウェアが取得する情報に基づいてネットワークスキャンを行い、結果を同一のネットワーク環境ごとに分類し、ユーザの使用頻度が高いネットワーク環境を推定する手法を提案する。
宮地　遼	松本勉	耐量子計算機暗号の耐タンパー実装に関する研究	量子計算機の実現に備え耐量子計算機暗号が注目されている。中でも Ring-LWE 方式に基づく暗号は他の方式と比べて効率性の高さから組込み機器への実装が進んでいる。組込み機器のようなネットワーク上の中小規模ノードで暗号を運用する際、暗号の実装手法に基づく脆弱性によりシステムのセキュリティが欠損する可能性がある。本研究では耐量子計算機暗号の耐タンパー実装を目的として、サイドチャネルセキュリティ評価を行う。
盛本岳志	森辰則	オノマトペ抽出技術における認識誤りの改善と印象推定	日本語コミュニケーションにおいて、擬音語・擬態語(オノマトペ)は重要な役割を担っている。文書中のオノマトペを扱う研究者や日本語学習者にとってオノマトペの出現位置の特定と印象の推定が不可欠だが、それらを自動的かつ正確に行う手法は確立されていない。そこで本稿では、オノマトペの自動抽出の精度向上と印象推定手法について検討する。

山田憲一	四方順司	ロバストかつエントロピーロスの少ないファジー抽出器に関する研究	ファジー抽出器とは、偏りのある情報源から一定で一様な乱数を抽出するものであり、情報源のエントロピーと出力のエントロピーの差であるエントロピーロスが少ないことが求められる。それに加え、ロバストファジー抽出器は、補助情報の改ざんも検出できるものである。本論文では情報源の確率分布知識があるという仮定のもと、新たなロバストファジー抽出器を構成する。結果として、既存研究と比較してエントロピーロスがより低いものとなったことを示す。
吉澤慎一郎	藤井友比呂	尺度推意の破棄可能性について	本修士論文は、理論言語学における語用論の分野で議論されている尺度推意とその破棄を論じる。Gazdar（1979）は、尺度推意の破棄がいつ起こるかを予測するモデルを提案している。一方、Levinson（2000）はモデルの反例を挙げている。本稿は、まずLevinsonが考慮していない、Gazdarのモデルの修正版が問題を解決する可能性を指摘する。次に、それでもなお、修正版モデルは問題点の真の解決にはならないことを示す。本稿の貢献は、LevinsonによるGazdar批判をサポートする経験的な議論を提出したことにある。
和賀一也	森辰則	トピック分析を用いた短い文書情報の背景にある事物の推定手法の検討	マイクロブログは、ユーザーが簡単に情報を発信できることで人気があるメディアである。その特性上短い文書であることが多く、文書の背景にある事物について明言しないことがある。そこで本研究では、短い文書情報の背景にある事物を推定する手法を検討する。文中に含まれる単語を用いてWeb検索を行い、トピック分析によって背景の事物の候補の絞り込む手法を提案する。
エレメーエヴァ・エカテリーナ	藤井友比呂	「日本語における否定的丁寧さと肯定的丁寧さ」	本論文は、Brown・Levinson 1987がフェイス概念を援用し提唱したポライトネス理論を日本語の観点から検討する。Matsumoto 1988は同理論を批判し、日本語の丁寧さはフェイスに由来するのではなく、話者が聞き手との社会的関係を維持しようとするために発動するものであるとした。本稿は、Matsumotoを詳細に検討し、批判は当てはまらないと主張する。また、謝罪・感謝の表現「すみません」と終助詞「ね」を取り上げ、それぞれ否定的丁寧さと肯定的丁寧さとして自然な分析が可能なことを示す。

夏 正男	岡嶋克典	聴覚が風覚に与える影響と風の強さ感の決定メカニズム	人間は風を感じる際に、聴覚と風覚を利用しているため、マルチモーダル現象が必ず起こっているが、クロスモーダル現象が起こっているかは分からない。本研究では、聴覚が風覚に与える影響を検討し、風を感じる際にクロスモーダル現象が起こっていることを確認した。さらに、「風の強さ感」などの定式化を行った。本研究の結果に基づき、風音のみを変えることにより、「風の強さ感」を制御することができるため、映画館やVRシステムなど、高い臨場感が必要とされる場合への応用が期待できる。
杜 冰清	長尾智晴	深層学習を用いた図面画像の類似度検索	図面検索問題において、検索候補を絞り込むために、図面に事前付与されたキーワードを利用したテキストベースの画像検索が一般的に使われる。更に絞り込むには、画像情報を利用したコンテンツベースの画像検索も用いられている。本論文では特許図面を検索対象とし、長年で蓄積した特許文献から得られる大量の画像データを考慮し、深層学習モデルによって図面特徴を抽出し利用する手法を試み、汎用的な図面類似度を算出するモデルの構築を目指した。
熊　佳	吉岡克成	ホームネットワークにおける脅威の実証実験に基づく分析	近年、様々な機器をインターネットに接続する事で、多様なサービスを提供するモノのインターネット(IoT) が注目されており、一般家庭にもIoT機器が増加している。これらのIoT機器の脆弱性を突くサイバー攻撃が脅威となっている。本研究ではIoTマルウェア検体の動的解析、テストベッド内への攻撃の引き込み実験、疑似攻撃の試行結果に基づき、ホームネットワークにおける脅威分析を行う。次に、実際のIoT機器を動的解析環境として用いる際に考慮すべき事項を整理する。いくつかのIoT機器について解析環境としての利用可否を検証し、実マルウェアを解析した結果を示す。