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
阿部祐也	岡嶋克典	車載電子ミラー用ディスプレイの設置条件と奥行き感向上に関する研究	近年、車載用ミラーの電子化が検討されてきている。ミラーの電子化には安全面において多くの利点がある反面、いくつかの問題点も抱えている。本研究では、電子ルームミラー表示における視認性を評価し、電子ミラーの特性を活かした最適な設置条件を導出し、視認性のシミュレートを可能にするモデルを提案した。また、電子サイドミラーが奥行き感に乏しいという問題点について、曲面化という方法で奥行き感の向上を図れることを示した。
飯田俊祐	マーティン・ロジャー	日本語の状態動詞のアスペクトに関する研究	本研究の目的は、日本語の動詞を分類する新たなテストを提案し、特に状態動詞のアスペクト特性を明らかにすることである。英語の〝V-ing〟と日本語の〝V-ている〟の違いに着目することにより、日本語の状態動詞を正しく分類することができるテストを作成することができた。また、状態動詞でも、状態のみのアスペクトを持つ動詞と状態とその状態に至るまでの過程の両方のアスペクトを持つ動詞の２種類の状態動詞があることがわかった。
池田　祐一	森　辰則	派生・新語を考慮した 日本語オノマトペの自動抽出手法の検討	日本語のテキストに出現するオノマトペの出現位置を同定する手法について検討を行った。特に解析の難しい３モーラ以下の未知オノマトペに対応する手法の実現のために、音素情報やオノマトペパターン分類、系列ラベリングといった要素技術を用いた手法を検討し、評価実験により有効性を示した。また、派生オノマトペの抽出実現のために、派生オノマトペの変形規則を考慮した手法を検討し、評価実験により有効性と今後の課題を明らかにした。
井田潤一	四方順司	対話型署名機能付き暗号化方式	近年、対話型の公開鍵暗号方式と認証方式が提案された。対話型の方式の利点として、非対話型のものと比べ、弱い暗号プリミティブから強い安全性を満たす方式を構成することが可能である。しかし，公開鍵暗号とディジタル署名の両機能を効率的に同時に達成する方式である署名機能付き暗号化方式に関しては、対話型のものは未だ報告されていない。そこで、本稿では対話型の署名機能付き暗号化方式を新たに提案し、構成法を提案する。

尾亦智弘	森辰則	社会情勢の変化を表す表現の自動収集と可視化	知的財産を活用する際には、社会情勢の変化を把握することが必要となる。しかし、社会情勢の変化が現れる対象は多岐にわたる上に、統計情報のように解釈の仕方から議論しなければならないような情報もある。そこで本研究では、Web 上の文書群から、社会情勢の変化を表すものであると書き手が解釈しているであろう表現を自動的に収集する手法を検討する。また、収集した社会情勢の変化を表す表現を利用者に見やすく提示するために可視化についての検討も行う。
小山大良	吉岡克成	標的型メール攻撃に使用されるマルウェアと囮文書の分析に関する研究	
川沼大輝	富井直志	EV エネルギー消費ログ DB を用いたデータ分析手法の実装と評価	我々は電気自動車の消費エネルギーを推定する ECOLOG システムを提案・運用してきた．本研究ではこのデータベースを用いたデータ分析手法を提案する．提案する分析手法はエネルギー損失と運転時間の相関の可視化や、エネルギー損失の詳細な要因の可視化行うものである．この可視化手法を用いたモバイルアプリを設計・実装し，機能が満たされているか評価を行った．
北島大	富井尚志	ライフログを用いたマイクログリッド導入効果検討が可能な DB の構築と情報提示	近年マイクログリッドの導入が進んでいる．しかしマイクログリッドの導入効果を事前に検討するには，「そこだけ，その時だけ」のログを用いて分析する必要がある．本研究では，自動車での通勤ログや建物の需要電力量のようなライフログと，気象ログや社会的な電力需要のようなオープンデータを蓄積する統合データベースを設計し，太陽光パネルと EV を構成要素としたマイクログリッドの導入効果を事前に検討可能なシステムを構築した．
小林隼人	森辰則	内容の類似性を考慮したネットワーク構造の発見に基づく Web 文書群の関係の可視化	近年、計算機の高性能化やネットワークの発達に伴い電子化された文書が増大しており、大量の文書群から利用者が必要な情報に効率よくアクセスする技術が必要とされている。その一つである情報検索によって得られる文書は、観点の多様性や詳細度がまちまちである。以上の背景に対し、多様な観点を網羅した文書とその文書中の観点について詳細な文書群を関連付けて提示することで、効率よく内容を把握するための出力の組織化を提案する。
後藤彰太	四方順司	汎用的結合可能安全性及びゲーム理論的安全性を有する暗号プロトコルの研究	従来，暗号プロトコルの安全性はプロトコルの参加者がアルゴリズムに従う限り，攻撃者の振る舞いを考慮した場合においても，秘匿性や正当性といった性質が保証されるというものであるが，近年，暗号プロトコルにおいて合理的な攻撃者を想定するゲーム理論的安全性も研究されている．本論文では，ゲーム理論的安全性を有するプロトコル同士の結合を考えた場合，結合後のプロトコルはゲーム理論的な意味で安全だと示すことができるのか考察する．

斎藤翠	長尾智晴	進化的画像処理による拡大画像生成	画像の拡大処理を行う際，低解像度のドットパターンは情報が落ちているために推定される拡大画像は複数考えることができ，高倍率になるにつれてその推定される解は膨大な数になる．本研究では，進化計算法を用いて画像処理プロセスを自動構築する手法である進化的画像処理を用いて，解を複数獲得する．また，画像を生成する際の制約条件としてフラクタル次元を用いることで，画像の複雑さを制御して様々な拡大画像を生成する．
坂本純一	松本勉	IoT 末端機器の耐タンパー性と軽量暗号実装に関する研究	本研究は二つの領域から構成される．IoT 末端機器のような計算資源の少ない機器では十分な暗号機能を利用できない場合があるが，一部の軽量暗号は極限的に計算資源が制限された環境であっても実行可能であることをに明らかにする．続いて，レーザーと電力解析を用いてメモリから値を奪取する攻撃を提案する．同機器は攻撃者によって物理的にアクセスされやすいため，提案攻撃等に対する耐タンパー性が重要であることを示す．
崎津実穂	長尾智晴	Cartesian Genetic Programming を用いた 3DCT 画像からの 4DCT 画像推定	近年，がん治療において肺などの臓器の時間的な変動を観察可能な 4DCT が注目されている．しかし 4DCT 画像の撮影は被曝量が多く，患者への負担も大きい．そこで本論文では，Cartesian Genetic Programming (CGP) を用いて 3DCT 画像から 4DCT 画像を推定する手法を提案する．4DCT 画像から複数の特徴点を抽出し，その特徴点が 3 次元空間内で描く移動軌跡を CGP で学習する．3DCT 画像から 4DCT 画像を推定する際は，画像から特徴点を抽出した後，学習した CGP で移動軌跡を推定する．
佐藤 慎悟	四方 順司	格子問題に基づく署名機能付き暗号化方式に関する研究	署名機能付き暗号化方式(Signryption)は公開鍵暗号とディジタル署名の両機能を達成する方式であり，重要かつ基盤となる暗号プロトコルである．一方，格子暗号技術は格子問題の困難性に基づき，量子コンピュータを用いた攻撃に耐性がある．本稿では，格子問題に基づく Signcryption の構成法を提案する．鍵長と暗号文長について，既存の構成法と比較し提案方式が最も効率が良いことを示す．
佐野僚	森辰則	対話型条件結論マップ生成に向けた条件表現の詳細・一般関係の認識	Web 情報の信憑性を利用者が判断することを支援するために、我々は対話型条件結論マップの研究を行っている．このシステムでは利用者が着目した言明に対して，その言明から導かれる結論や，その言明が結論となる条件を Web 上から抽出して提示し，利用者が言明を実践するか否かの意思決定支援を行う．本論文では，条件結論マップにおいて各言明を整理する際に必要となる、言明間の詳細・一般関係を認識する手法を提案する．

清水智史	長尾智晴	部分領域間の関係性を考慮した類似図面検索	図面検索では，図面に対して事前に付与されたキーワードを利用したテキスト検索が一般的に行われる．このテキスト検索によってある程度の検索候補に絞り込むことができるが，更に絞り込むためには図面情報は非常に有益である．本論文では特許図面を検索対象として使用し，部分領域間の関係性を考慮した類似図面検索を行う．複数の図形の配置で記述したクエリ画像を使用し，図面の空間構造を考慮した汎用性の高い図面検索手法を目指した．
白沢将人	四方順司	情報理論的安全性をもつ準同型暗号についての研究	完全準同型暗号は特定の暗号化された情報に対して処理機能を付与する暗号技術の一つであり，暗号文を平文に復号することなく，暗号文どうしの加減乗除演算処理を行うことができる暗号方式である．本論文では情報理論的安全性に基づく完全準同型暗号について完全秘匿性の安全性定義を新たに提案するとともにこの定義の妥当性について示す．また完全準同型暗号の具体的な構成法を提案し，この構成法が定義した安全性を達成することを示す．
戸松研人	長尾智晴	楽曲構造を考慮した進化的自動作曲	独自の音楽作成に対するニーズから，コンピュータによる自動作曲の発展が期待されている．本論文では，「A メロ - B メロ - サビ」の構造をもつ楽曲を遺伝的アルゴリズムによって自動で生成する．音楽理論の観点からのみではなく，パートらしさやパート間の繋がりの観点から個体を評価する適応度関数を導入することで，構造を考慮した楽曲を生成する．また，生成された楽曲に対し，ユーザの評価を取り入れながら修正を加えることで，少ない負担でユーザの望む楽曲を獲得することを目指す．
中川原里沙	四方順司	ハイブリッド暗号の一般的構成法における KDM 安全性の解析	暗号技術は，ディジタルデータのやりとりを安全に実現するために必要である．暗号技術は公開鍵暗号と共通鍵暗号に分類される． ここで強い安全性を満たす公開鍵暗号として，これまで藤崎，岡本により 3 種類の FO 変換が提案された． 一方，近年さらに KDM 安全性は重要だと認識されている．2016 年に，これまでと同じ安全性の条件の下， 1 つの FO 変換は KDM 安全性を満たさず，もう一つは KDM 安全性を満たすと示された．本論文では残りの FO 変換が KDM 安全性を満たすことを示す．
中山 淑文	松本 勉	車載ネットワークの電気的セキュリティ	最近の自動車は IT の活用が盛んであり，自動運転技術などが注目を浴びている．その一方で，自動車の電子制御化や IoT 化により，自動車がサイバー攻撃の対象となる危険性が高まっていて，自動車の情報セキュリティ技術の必要性が高まっている．そこで本論文では，自動車内部の制御ネットワークに広く用いられている CAN (Controller Area Network)の電気信号に着目した“電気的データ改竄”という攻撃の脅威を指摘する．そして，この攻撃から自動車を保護する多層的なセキュリティ強化策について，独自手法の提案も交えつつ考察を行う．

西添友美	吉岡克成	DRDoS 攻撃の観測手法の改善と被害者分析に関する研究	DRDoS 攻撃は 2013 年頃から急増し，インターネット上の深刻な脅威となっている．DRDoS 攻撃に対抗するためには，その実態を正しく把握することが重要である．本研究では，第三者による DRDoS 攻撃の観測を可能にする DRDoS ハニーポットの改善と，被害者の分析に取り組む．まず，プロトコルに依存しない DRDoS ハニーポットを提案する．次に，CDN を回避して配信元 Web サーバを直接狙う場合に焦点を当て，実態を調査する．
西山誠人	富井尚志	エネルギーライフログの状況細分化に基づく電力量分布の有用性評価	社会的な電力削減要求の高まりから、オフィスなどの業務部門においては仕事の生産性を損なわず，状況に応じた減り張りのある電力の使い方が求められている．一方で，近年のセンサ技術の発達により，電力使用に関するライフログが取得可能となった．そこで我々は前述のログを DB に保存し，状況をキーとした電力の検索・集約により消費電力を可視化するシステムを構築した．本稿では前述のシステムを用いて，状況に応じた電力の使い方を直感的に把握できる電力量分布を提案し，その効果を削減電力量として定量的に導出することで有用性を示す．
原田耕也	吉岡克成	統合型マルウェア検査サービスを用いた悪性ドメインの検知	近年，DNS の通信を行って不正活動を行うマルウェアが増加している．ドメインのブラック化などの対策はされているが，マルウェアの増加によって迅速な更新が困難になっている．そこで本論文では統合型マルウェア検査サービスを用いて悪性ドメインを早期に検知し，自動的に抽出する手法を提案し，既知のブラックリストより早く悪性ドメインを検知可能である事を示した．
平川大樹	田村直良	小説テキストにおける登場人物の同一指示解析	小説テキスト中の登場人物は、氏名を表す固有名詞や言い換えの表現として用いられる代名詞等さまざまな形で表現される。このように指示対象が同一である表現間の関係を同一指示関係と呼ぶ。本研究では同一指示関係を３つのアプローチで解析する手法を提案した。また、発話文と地の文の違いを考慮した外界照応を定義し、照応解析、同一指示解析の精度向上を図った。外界照応を考慮しないモデルとの比較実験では、提案手法が良い結果を示した。
北條聡	岡嶋克典	動的視覚情報を変調させた飲料のクロスモーダル効果	飲料喫飲時の動的な視覚情報が風味などに与える影響について実験的に検討した．カメラ画像から AR マーカーの情報を基にコップを検出し，仮想湯気や視覚的な増粘効果を画像処理で加える．リアルタイムに処理した画像をヘッドマウントディスプレイに出力し被験者に提示することで，見たときの温度感や粘り気ならびに実際に飲んだときの風味が変化することがわかった．

本田達識	後藤敏行	仮想空間オーケストラにおける純正律を考慮した音響出力法	本研究は，純正律に基づいた音響出力の手法を提案する．純正律に関する予備実験において，現代人は純正律に慣れていないため，楽曲のメロディを純正律で演奏するのは異様に聞こえるという結果が得られた．そこで本研究は，楽曲のメロディを平均律，その伴奏を純正律で演奏する手法をとる．また，その手法で楽曲のメロディと伴奏の音長の違いによりうなりが発生する箇所は，それに対応したビブラートを用いて出力する．以上の要件を満たすシステムを試作し，主観評価実験を実施した．
八幡篤司	吉岡克成	サンドボックス解析回避への耐性を高めるツール SandVeil の提案	近年増加しているセキュリティインシデントの多くに，高度に機能化された悪意のあるソフトウェア，通称マルウェアが関係しており対策が求められている．マルウェア対策のため，サンドボックスを用いたマルウェア動的解析や検知が行われているが，マルウェア作成者は解析を妨害・回避するための機能をマルウェアに搭載するようになっている．本研究では，サンドボックスをユーザマシンの環境に近づけることや，サンドボックスの多くに共通して見られる特徴を変更することでサンドボックス解析回避を困難にするツール SandVeil を提案する．
横山日明	吉岡克成	解析環境の特徴に着目したセキュリティ検査の回避に関する研究	本論文では，実行環境の様々な情報を取得するツール SandPrint を提案する．これを用いて実運用されているサンドボックスから様々な情報を収集し，サンドボックスの特徴を用いた解析回避の可能性について検証する．収集した情報から，一般ユーザには見られないがサンドボックスに共通して見られるようなサンドボックス固有の特徴が多数確認され，それら特徴を用いた解析回避の可能性が確認できた．
吉澤貴博	四方順司	情報理論的に安全な 検索可能暗号に関する研究	検索可能暗号はドキュメントを暗号化したまま検索可能な方式であり、2000 年代から研究が進められ，クラウドコンピューティング等で利用されている．既存の検索可能暗号は計算量的安全性の枠組みで研究されており，情報理論的安全性を持つ検索可能暗号は提案されていない．そこで我々は世界で初めて情報理論的安全性を持つ検索可能暗号を提案する。具体的には，モデル，3 つの安全性定義とそれを満たす構成法，鍵長の下界を提案する．
吉住　亮祐	岡嶋　克典	マルチスペクトル光源を用いた質感知覚における分光分布と ipRGC の影響に関する研究	物体の視覚情報を正確に得るためには適切な照明光が必要である。そこで本研究 では、様々な分光分布の照明光を、マルチスペクトル光源を用いて作成し、観察者に照明下の物体の鮮度や光沢感などを主観評価させた。その結果、照明光の色度が同じでも分光分布が異なる照明間で鮮度等の評価データに有意な差が見られ た。解析の結果、ipRGC 作用度が光沢感等の質感に影響することを示した。

吉田翔太	長尾智晴	大型貨物船の目的地予測	マルチエージェントシミュレーションを用いて現実世界の様々な事象を再現し，その事象の分析や将来の動向の予測に利用する研究が盛んに行われている．本研究では大型の貨物船を対象に，実際の航海データや海運市況データを用いて確率モデルによって船の行動モデルを構築する．そして，構築したモデルを用いて目的地予測実験を行った．実験結果から，貨物船の目的地予測に有効な情報の検討を行った．
渡邉　直紀	松本　勉	動的命令呼び出しを用いたソフトウェア耐タンパー化手法	セキュリティ機能がソフトウェアに実装されパソコンや組み込み機器で利用されることが今日増えているが，セキュリティ機能自体も攻撃者からの改変に強い必要が求められる．このようなセキュリティの指標として耐タンパー性というものがある．本研究では，耐タンパー性を高めるために，従来の耐タンパー化技術の改良と，動的命令呼び出しにより耐タンパー化適用可能なシステムの範囲を広げる手法の提案を行った．
和田勝貴	長尾智晴	距離カメラを用いた感性計測	近年，人の感情を推定する感情推定の研究が盛んに行われている．本研究では，困惑感情に着目し，自然に表出する困惑表情から困惑状態の推定を目的とした．脳科学者の意見を参考に自然な困惑表情誘発アプリケーションの作成を行い，被験者から自然な困惑表情のデータを収集した．その後，収集したデータに対して SVM を用いて困惑表情の分類実験を行い，また SVM と感情推移モデルを組み合わせた困惑状態の推定を行った．
造酒裕貴	長尾智晴	深層強化学習を用いた株式売買戦略の構築	本稿では，深層強化学習を用いた株式売買戦略の構築手法を提案する．深層強化学習では，入力が高次元であっても教師なしで過去の経験から将来の報酬を最大化する行動規則を学習することができる．本手法では，株価などの時系列データから，利益率を最大化するような売買戦略を学習する．さらに，従来手法のように全所持金で株を購入し，売却時は全ての株を売るといった単純な売買戦略ではなく，売買株数の最適化も含めて売買戦略の構築を行う．
徐欣欣	長尾智晴	セルラー進化型神経回路網による CT 画像の超解像処理	医用画像は、撮影条件などの影響を受けやすいので、高精度かつ正確な高解像度画像を得るために、CT 画像の超解像技術が求められている。本稿では、セルラー進化型神経回路網による CT 画像の前処理を含める一連処理を行う超解像処理システムの構築を提案し、断層面および断層間に配置される低解像度画像から高解像度画像に超解像を行う処理回路を構築した。補間ベース、再構成ベース、学習ベースの従来手法を医用画像に適用した結果と比べ、本手法は良好な結果が得られ、医用画像に対する有効性を示した。