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
三田 隼平	四方 順司	弱い計算量仮定を用いた閾値型鍵カプセル化メカニズムの構成に関する研究	最初に Threshold Tag-KEM を BCHK 変換を用いて Identity-Based Threshold KEM とワンタイム署名あから構成し，次に Identity-Based Threshold KEM を CBDH 仮定から構成するという 2 段構成になっている. この成果によって，閾値型公開鍵暗号を CBDH 仮定から構成することが初めて可能となる.。
青木健太	岡嶋克典	両眼視野闘争における運動速度の効果	左右の眼に異なるイメージを呈示した時，どちらか一方のみが知覚され，それが数秒毎に入れ替わる現象を両眼視野闘争と呼ぶ．この知覚交替は時間的に不規則に生じるが，静止する刺激よりも動く刺激の方がより優位に知覚される．本研究では，左右眼の闘争刺激の運動速度を様々に変化させ，運動速度が両眼視野闘争に与える影響について検討した．その結果，並進運動ならびに拡大収縮運動いずれの場合も，低速で動く刺激が優位に知覚されることが示された．
阿部宏志	松本勉	距離計のセキュリティに関する研究	距離計の計測技術は自動車の前方障害物衝突被害軽減制動制御装置といった,誤動作を起こした際に人体の安全にかかわるものにまで用いられるようになっている.民生用途に向けて開発されている計測システムにおける意図的な偽装や妨害といった攻撃の分類やそれに対する対策の検討は行われてきてはいるものの，まだ十分とは言えない. そこで本論文では，製作した PSD 方式の赤外線距離センサを用いたものと市販の位相差測定方式の距離計について，それぞれに対する攻撃の有効性を示し，対策の検討をする.
五十嵐健人	後藤敏行	仮想空間オーケストラのための人体モデルを用いた楽器演奏動作生成法	本研究では、仮想空間オーケストラにおける演奏エージェントが合奏する際の動作を楽譜からとらえた楽曲の進行と楽器の演奏ポジションから逆運動学に基づいて、人体を構成する関節の動きとして推定する方法について検討した。さらに、五線譜に奏法記号として記載される演奏情報を、拡張 MIDI メッセージとして MIDI シーケンスに埋め込むことによって、楽器の奏法に応じた演奏動作をリアルタイムに生成し、多関節人体モデル（ボーンモデル）を用いて演奏に同期して提示する手法を提案した。

石田優	四方順司	選択暗号文攻撃に対して安全な鍵失効機能付き ID ベース暗号の構成法に関する研究	３つの選択暗号文攻撃に対して安全な鍵失効機能付き ID ベース暗号の構成法を初めて提案した。本構成法は新しい現実的な脅威である復号鍵漏洩耐性を有している。１つ目と２つ目は BCHK 変換という変換手法を用いている。３つ目に関しては KEM/DEM フレームワークを用いて構成している。２つ目の構成法は強い仮定を利用する代わりに公開鍵長が定数オーダーであるという特長を有する。また、３つ目の構成法は１つ目と２つ目の構成法に対して暗号文長が短いという特徴を有する。
今泉佑介	長尾智晴	音の重畳による騒音の不快感低減に関する研究	騒音低減技術は快適な音環境を実現するために重要である.本論文では騒音に対して,別の制御音を加えることで不快感を低減する手法を提案する.提案手法では,騒音と似た特徴をもつ楽器音を制御音として合成し,騒音に重畳することで不快感の小さな音へ変化させる.主観評価実験によって提案手法の不快感低減効果を検証し,聴覚マスキングに基づく従来手法よりも,効果的に騒音の不快感を低減できることを確認した.
岩吉　拓哉	松本　勉	人工物メトリック・システムにおける耐クローン性評価に関する研究	人工物メトリクスと呼ばれる，人工物の偽造防止効果の期待される認証技術では，偽造物の作製困難性(耐クローン性)についてさまざまな観点から評価を行うことが求められる．本稿では，耐クローン性評価の新たな指標 GSR_{SM}を提案することで，従来の評価指標では評価が困難な実験結果に対して容易な評価を可能とすると共に，実際に GSR_{SM}を用いて耐クローン性の評価・比較を行い，有用性の検討を行った.
梅村彰宏	長尾智晴	視線データを基にした視覚的顕著性マップの作成に関する研究	人の視覚的注意をモデル化する，顕著性マップに関する研究が盛んに行われている．本研究では，人の視覚野に関する知見を基にしたモデルに，人の注視領域の学習によって作成した補完画像を統合することによる顕著性マップの作成手法を提案する．顕著性マップの作成実験によって，統合前の二者それぞれのみを考慮したモデルと比べ，統合後のモデルの方が人の注視領域に近い顕著性マップを作成できていることを検証した.
河西真瑠那	四方順司	代理人再暗号化方式の一般的構成法に関する研究	代理人再暗号化方式（Proxy Re-Encryption、PRE）は，ある利用者宛の暗号文を，一度も復号することなく,別の利用者宛の暗号文に変換する機能（再暗号化処理）を有する公開鍵暗号方式である.本論文では，ID ベース暗号を自然に拡張した閾値階層型 ID ベース暗号の概念とその具体的構成法を示し，その閾値階層型 ID ベース暗号と公開鍵暗号とワンタイム署名を用いた標準的な CCA 安全性を有する PRE の一般的構成法を提案した.

加治　昂	後藤敏行	鉱山走行車両における車載センサ情報と環境地図を用いた位置推定法	大型の鉱山走行車両は死角が大きく、路肩や構造物など危険個所までの距離を把握しにくいことからセンサ情報に基づく安全対策技術の実現が期待されている。本研究では、鉱山走行路で自動生成された形状マップと、車載カメラで捉えた距離画像を用いて車両の走行位置を推定する手法について検討した。本手法では ICP マッチングの持つ計算量の問題に対して、高低差マップの各構成点群に対してボロノイマップを利用することで高精度かつ高速な手法を提案している
川上奈津子	吉岡克成	標的型攻撃対策に関する研究	近年，標的型サイバー攻撃は巧妙化しており，攻撃対象を欺く偽の文書ファイル（囮文書）も多様なものとなっている。本研究では，標的型マルウェア検体の実行時に表示される囮文書の内容に着目した分析を行い，囮文書の内容から多くの検体について攻撃対象を推測できることを示す．また部外者が通常知り得ない非公開情報を含む囮文書が存在することから，当該情報の所有者が既に攻撃により侵入を受けており，流出した情報が悪用されている可能性を指摘する．
菊地陽介	吉岡克成	Androidマーケットの安全性評価に関する研究	Android マーケットは世界中に数多く存在する．しかし，マーケットには正規のアプリに紛れてマルウェアが含まれている場合がある．マルウェアによる被害から身を守るためには，ユーザはより安全なマーケットを利用するべきである．そのためマーケットのセキュリティ面における評価を行うことは有益といえる．そこで本稿では，マーケットの行っているセキュリティ対策の実態の検証やその安全性評価を行う．
吉川 亮太	松本 勉	組織内の複数ホストから得られる内部挙動に着目した標的型攻撃の検知手法に関する研究	近年，企業の重要情報を狙った標的型攻撃が脅威となっている．この攻撃は侵入を防ぐことが難しく，感染を前提とした対策が重要である．対策の一例として組織内の各機器のログを収集・解析することで不正侵入を検知する対策がある．しかし，検知能力が管理者の設定に依存するため，汎用的に利用可能な検知手法が希求されている．本論文では組織内の複数ホストから得られる内部挙動に関する情報を利用した検知手法を 2 つ提案する．
小池　良太	長尾　智晴	株価予測に有効な特徴空間の構成に関する研究	株価変動は，市場参加者間の相互作用による複雑系から生じる時系列とみなすことができる．本論文では複雑系を取り扱うカオス解析における相空間に代わる，特徴空間への埋め込みを提案する．提案手法では，特徴空間を用いた予測によって，従来の相空間よりも精度の高い予測を行うことを目指す．実験によって提案手法では，従来の埋め込みに対してより予測に有効な特徴空間の構成が可能であることを示した．

小出駿	吉岡克成	不正通信の検知と分類に関する研究	インターネット上の不正活動の対策のためには,不正通信の観測による攻撃の実態把握が重要である．本研究では，パケットヘッダの特徴から送信元のマルウェアを特定する分析，TCP を悪用した DRDoS 攻撃である TCP リフレクション攻撃の存在をハニーポットを用いて明らかにする分析,DRDoS 攻撃を観測可能なダークネットを用いてプロトコルごとの攻撃の特徴や踏み台として悪用されている脆弱な組込み機器の分析を行う.
小笹哲哉	森辰則	並列分散処理を用いた大規模日本語コーパスにおける可変長単語 N-gram 頻度計算手法	日本語を対象とする自然言語処理において,文脈に応じて必要な長さを用いるような可変長単語 N-gram 頻度が求められている.しかし,大規模日本語文章において可変長単語 N-gram 頻度を従来手法にて計算する場合,単語の組合せが増え,限られた計算資源で計算するのは時間や主記憶容量の面で難しいという問題がある.そこで,我々は大規模日本語文章における可変長単語 N-gram 頻度を並列分散処理により求める手法を述べる.
小林優希	松本　勉	車載ネットワークにおける脆弱性検証手法に関する研究	近年の自動車は，様々な機器の制御を行う ECU（Electronic Control Unit）を多数搭載し，それらを CAN（Controller Area Network）などの車載ネットワークで接続し通信を行っている．CAN ではセキュリティ上の脆弱性検証手法が確立されていないため，本研究では CAN における脆弱性検証手法を提案し，実験用の車載ネットと実機の ECU にて実験を行い，手法の有効性を確かめた．また，脆弱性検証手法を利用した新たな攻撃手法を提案し，既存手法と合わせて効果を評価した.
佐々木一真	白崎 実	水面付近の魚の自律推進・跳躍運動の大規模並列解析	水棲生物の遊泳に関する謎や未解決の問題の解明を目的として,水面付近を遊泳し跳躍する魚まわりの流れを，計算流体力学の視点から解析した．スーパーコンピュータを利用した並列計算により総格子数が 1 億点を超える大規模な問題を扱った．水面にできる波と魚の遊泳速度は大きな関係があり,特に水面に近い位置を推進する場合は遊泳速度によって異なる性質の波をつくることを示し，跳躍を含む遊泳が水面付近の水中を遊泳するよりも効率が良い可能性があることを示した.
柴原健一	吉岡克成	能動的観測による悪性ネットワークの分析に関する研究	攻撃者はサイバー攻撃のために多くのリソースを必要としており，その実態の解明は対策に繋がる．我々は能動的観測により攻撃者が用いるリソースの分析を行う. 悪性ネットワーク上の脅威 Drive-by Download 攻撃は Exploit Kit により流行している．本稿では Exploit Kit 検知用シグネチャを自動作成する手法を提案する．また，大量にポート開放を行うホストが多数存在するネットワークを悪性ネットワークと定義し,効率のよい悪性ネットワーク探索手法を提案する.

神貴久	森辰則	階層的固有表現抽出における抽出器群の組み合わせに関する研究	一般的な固有表現抽出の研究では，ある固有表現が複合語である場合，その固有表現内に含まれる固有表現には注目していない．しかし、このような固有表現も抽出することができれば，質問応答システムや重要文抽出などの処理において役立つと考えられる。そのような研究として、複合語の固有表現を階層的に抽出する階層的固有表現抽出が提案されている。本研究では、階層的固有表現抽出において、階層構造の違い、抽出する順番の違いによる効果について検討した．
鈴木愛斗	森辰則	政治情報システムのための会議録の発言の分割と総合計画との対応付け	地方議会が国会よりも情報が少ないことを受け，利用者の政治判断に有用な情報を提示する地方議会会議録を用いた政治情報システムの研究を行っている．その中で本研究では利用者の関心に応じた会議録中の発言の提示を扱う．まず(1)各発言は複数の話題に言及するので話題毎に発言を分割し，(2)地方自治体の総合計画中の施策・事業と各発言を対応付ける．それぞれ、会議録固有の手がかり表現、総合計画の観点情報が有効であることを示した．
鈴木将吾	吉岡克成	組み込み機器への攻撃のハニーポットによる観測に関する研究	本研究では，組込み機器への攻撃を観測するためのハニーポットである IoTPOT を提案する．検証実験の結果，263 日間の観測で，145,814 ホストから 5,234,103 回のマルウェアダウンロード試行を観測し，1,027 検体ものマルウェアを収集することができた．分析の結果，組込み機器を悪用し，DDoS 攻撃を行う異なる 6 個のマルウェアファミリを特定することができ，サイバー攻撃に悪用されている組込み機器は 60 種類以上におよぶことが確認された．
土屋大樹	長尾智晴	遺伝的プログラミングを用いた画像分類のための進化的特徴抽出	本論文では，画像分類のための進化的特徴抽出手法を提案する．提案手法は，画像変換処理をグラフ構造の遺伝的プログラミングを用いて構築し，その出力画像に対する特徴抽出処理を進化的に選択する．そして，得られた特徴量を分類器に入力することで分類を行う．テクスチャ画像分類とシーン画像分類問題において，提案手法は従来手法と同等以上の性能を示した．また，提案手法では分類対象に応じて適切な特徴量が選択されることを示した．
筒見拓也	吉岡克成	能動的観測と受動的観測の連携によるサイバー攻撃の実態把握に関する研究	近年，インターネットにおけるサイバー攻撃による被害が深刻となっている．こうしたサイバー攻撃の分析や情報収集を行う研究は数多く存在するが，いずれも単一の観測手法による研究を中心に行われてきている．そこで本論文では，能動的観測と受動的観測，およびそれらに関連する観測手法を連携して，サイバー攻撃の観測・分析を行い，その実態把握を行った．

富田信一朗	四方順司	情報理論的に安全な順序検証型アグリゲートメッセージ認証方式	順序検証型アグリゲート署名は， 複数の署名をひとつに圧縮し， またその署名の生成順序も検証可能なプロトコルである． 既存のプロトコルは計算量的安全性に基づいて構成されているが， この安全性は計算技術の発展によって危殆化する恐れがある． そこで， 計算能力に依存しない安全性である情報理論的安全性の枠組みの中で， 順序検証型アグリゲート署名と類似の機能を持つ順序検証型アグリゲートメッセージ認証を提案する．
西澤昌宏	岡嶋克典	3次元パッケージの視認性評価のための投影型拡張現実感システムの開発	近年，商品パッケージにユニバーサルデザイン（ＵＤ）を考慮することが求められている．しかしＵＤの評価には大量の試作品を多くの人に評価してもらう必要があり，多大なコストを要する．本研究ではこの問題を，モックアップに高齢者や色覚異常者の見えを模擬したパッケージ画像をプロジェクタ投影することで解決し，パッケージの視認性を実環境下でリアルタイムに評価できる投影型拡張現実感システムを実現した．
西本直樹	富井尚志	IoTのミクロデータを用いた状況別電力評価が可能な DB の構築とスマートグリッドへの応用	社会的な電力削減要求が高まる中，太陽光や風力などの再生可能エネルギーによる発電設備の導入が進められている．これらを家庭・オフィス・学校など小規模な単位で導入し電力網を形成するマイクログリッドに関する研究が行われている．そこで本研究では，日常的に取得されるライフログやオープンデータを統合したデータベースを構築した．これにより太陽光や電気自動車を構成要素としたマイクログリッドの導入効果を定量的に導出した．
西山拓人	後藤敏行	移動環境における複数物体の形状および運動の分離推定法	３次元センサの普及により、さまざまの用途で距離画像が使われるようになったが、異なる動きをする複数の移動物体を分離して解析できる技術の確立が望まれる。本研究では、最初に複数の移動物体から誤検出の移動ベクトルや他の物体の影響を回避しながら、フレーム間で対応関係を評価することで、画素レベルで移動物体の画像領域を抽出する手法を提案した。さらに、対応関係を確率として表現しフレーム間で統合することによって、抽出精度を向上させる方法について検討した。
橋田啓佑	吉岡克成	Androidの実機を利用した動的解析に関する研究	近年の Android を狙ったマルウェアが急速に増加、機能の高度化を進めている．それらのマルウェアの動的解析には実機を利用した解析環境を利用することでより効果的な解析ができるようになる可能性が高い。本研究では Android マルウェアの実機上での動的解析環境の利点と欠点についてまとめ、それに基づいた解析環境の構築をおこなった。また実機を利用した解析環境の有効性を示すため、実機を利用した解析環境とエミュレータを利用した解析環境で同時に解析を行い、その結果に差異について検証した。

廣兼優里	長尾智晴	パーツ間の関係性を考慮した人物属性分類	近年動画像中の人物属性が様々な分野に利用されている．特に，自動運転化に向けて歩行者属性をドライバに提示することが今後必要になる．本論文では，歩行者属性データセットを作成し，歩行者認識で重要な『性別』『前方不注意の有無』『持ち物の有無』『補助器具の有無』の属性を付与し，分類を行う．その際人の向きや遮蔽に対応するためにパーツを用い，それらパーツの関係性を用いて出力を数値で得ることで人間らしい認識を行う．
古野遼太	長尾智晴	勾配情報に基づく 物体認識のための特徴量最適化	機械学習を用いた物体認識において，認識対象となる物体に応じた適切な特徴量の設計が必要となる．本論文では，画像の勾配情報に基づく特徴量最適化手法を提案する．提案手法は，特徴量を抽出する参照領域と特徴量として用いる勾配ヒストグラムの勾配方向成分の組合せを，遺伝的アルゴリズムを用いて最適化することで認識に有効な特徴量の選択を行う．提案手法を物体認識問題に適用し，獲得した低次元かつ低計算コストの特徴量が良好な認識精度を示すことを確認した．
前鼻航	長尾智晴	画像処理による画像誘導放射線治療の精度向上に関する研究	画像誘導放射線治療において，放射線照射野中心（radiation isocenter：RI）と X 線画像中心（imaging isocenter：II）の一致，および視認性の高い X 線画像が求められる．しかしながら，RI と II の整合性を一度に評価する手法は提案されておらず，X 線画像は治療寝台の陰影を含む．本論文では，画像処理による，RI と II の整合性の評価手法，ならびに陰影の除去手法を提案する．提案手法により，RI と II の整合性の評価，および X 線画像中の陰影の除去が可能となった．
松井 兵庫	森 辰則	質問応答システムを用いた 大学入試問題に対する解答生成手法	我々は，大学入試問題を対象とした Factoid 型質問応答において，従来の質問型より詳細な「分野特有の質問型」を用いた解答候補の絞り込み手法と，解答候補に対する解答候補と注目語句の距離を用いたスコア付け手法を提案した．評価実験の結果，分野特有の質問型を用いることで，解答候補の絞り込み精度が向上した．また，提案したスコア付け手法を用いて，大学入試問題に解答することで，正答率が向上した．
山崎拓也	岡嶋克典	力覚呈示デバイスを用いた素材感の記録･再現に関する研究	触覚は接触物体の物理特性が複雑に関与するため，何をどのように記録・再現できるかを明らかにする必要がある．そこで本研究では，硬さと粗さの二つの刺激を記録・再現することを目的に，力覚呈示デバイス PHANToM を用いて，ディスプレイ内にある物体に実物と同様の触覚刺激を再現するシステムを試作した．最初に被験者は実物の物体と同じ触感になるよう PHANToM のパラメータを調整した．次に物体の圧力と剪断力を測定し，その値から PHANToM のパラメータに変換する式を導出して、物理量から触覚を再現することが可能となった．

吉本亘汰	富井尚志	マップマッチングによる EV エネルギー消費ログ DB の精度向上と精度評価	我々は，既存の自動車の走行ログから仮に EV に置き換えた際の走行エネルギー量を推定・蓄積するデータベースを構築した(以下 ECOLOG システムと呼ぶ)．本研究では，この ECOLOG システムを評価するための正解データの取得，推定精度の改善方法，評価方法について述べた．また，ECOLOG システムによる推定消費エネルギーの誤差原因についても述べた． 不明な点がありましたら環境情報学府係までお願いします。
米澤美貴	岡嶋克典	肌の色分布が肌印象に与える影響	顔の肌の色分布が肌印象にどのような影響を及ぼすかを調べるために、主観評価実験を行った。まず、肌の色分布の大きさを変化させ、色分布の大きさが異なる画像刺激を作成した。被験者は、提示される肌画像刺激を見て、それらの肌印象の主観評価を行った。その結果、各肌印象を最適にする肌の色分布の大きさが存在することが示唆された。また、最適な色分布の大きさは元々の肌の色分布に依存する。
渡邉満紀	後藤敏行	NMI 弾性マッチングを用いた医用画像の異種モダリティ・レジストレーション	相互情報量（NMI）は，異種モダリティ間のマッチングに有効とされるが，頭部などの変形の少ない画像を対象とした研究例が多い．本研究では，NMI が従来の類似性尺度と比較してローカルな情報に感度が高いこと，また，SN 比のウィンドウサイズへの依存性が高いという性質を考慮して，変形をともなう異種モダリティに対して高精度な対応付けを実現する手法を提案するとともに，肺野領域の 3DCT 画像と 3D 造影 MR 画像に適用し有効性を確認した．
姜　婉婷	岡嶋 克典	マーカーレス投影型拡張現実感システムの食環境への応用	食品の美味しさは，味や香りだけでは決まらず，喫食する人の五感や環境など，様々な要因に影響される．特に視覚情報である食品の外観は影響が大きいことが知られている．そこで本研究では，プロジェクタ投影によって食品や食器等の外観をリアルタイムに変更可能な拡張現実感システムを開発した．食品の外観を操作することで，食欲増進・偏食改善・食品開発の効率化等への応用が期待される．
蘇　佳瑋	吉岡克成	情報理論的指標と異常検知に基づく難読化悪性 JavaScript 検知に関する研究	Drive-by-download 攻撃を起こすための悪性 JavaScript は、セキュリティシステムの検知を回避するために難読化される場合が多い。本研究では、従来の難読化悪性 JavaScript 検知手法の短所を改善し、情報理論と異常検知に基づく新しい難読化悪性 JavaScript 検知方法を提案する。分析の結果，我々が構築した二つの検知システムは高い検知率を持ちながら、検知速度も非常に速いということがわかり、実際に新規の難読化 JavaScript 発見に応用できることを示した。

ド タン ロン	四方順司	階層型グループ署名に関する研究	利用者のプライバシを秘匿したディジタル署名方式としてグループ署名方式がある． グループを管理しているマネージャが 1 人しかいない通常のグループ署名と違い，複数人のマネージャを階層的に配置されたグループ署名を，階層型グループ署名と呼ぶ．しかし，階層型グループ署名において，メンバの追加が可能な既存研究はない．そこで，本稿では，動的にメンバの追加が可能な階層型グループ署名を提案する．本方式では，グループメンバだけではなく，マネージャも追加可能である．
符静慈	岡嶋克典	疲労・集中力・覚醒度における ipRGC の影響	ipRGC(内因性光感受性網膜神経節細胞)の出力によってメラトニン分泌、覚醒、瞳孔反射など光の非視覚的作用が生じる。本研究では、ipRGC 刺激量および基本的な照明要件である相関色温度と照度に着目して、照明における疲労、集中力、覚醒度に与える影響を検討した。実験 1 において、紙上の視作業による眼疲労に対しては、照明の相関色温度の影響が大きいことが示された。実験 2&3 の結果から、集中力を向上する ipRGC 刺激量の最適値が存在する可能性を示された。
張芸	マーティン ロジャー	中国語における疑似所有格	所有構文に出現する中国語における疑似所有格（FP）を考察した。本論文では、FP が非所有の特徴的な解釈を許し、特定の所有文の構造において、解釈が可能になるという仮説を基に、文献で扱っている言語事象以外にも新たな証拠を上げて分析し、FP の様々な特徴を説明し、FP の分布を統一的に示した。さらに、日本語、英語と中国語の FP の比較分析から、意味的な類似性として主格的な意味が読み取れることに加え、統語論上の構成要素の違いを提示した。