黒澤　馨　教授

Kaoru Kurosawa　Professor

プロフィール

東京工業大学博士課程、同大学助手、講師、助教授、
教授を経て茨城大学教授（情報工学科）

専門分野

現代暗号理論｜公開鍵暗号｜デジタル署名｜認証｜ID
ベース暗号｜完全準同型暗号

ライフワーク

インターネット社会が便利になればなるほど、情報セキュリティに関する脅威が増しています。この要請を背景に、現代暗号理論は今やコンピュータサイエンスの一大分野に成長し、計算量理論と融合しつつ、数学的に非常に高度になってきています。理論的に高度で、かつ実際に役に立つという意味の「Theory meets Practice」を目指し、情報セキュリティ向上のため、現代暗号理論の研究に取り組んでいます。

最近の研究は、暗号文同士の四則演算が平文同士の四則演算になるという完全準同型暗号や、ファイルを暗号化したままキーワード検索が可能な検索可能暗号などで、どちらも、クラウドサービスへの応用が期待されている分野です。

完全準同型暗号を利用すると、たとえば医療データ等を暗号化したまま、平均などの統計処理や、さらに複雑な演算をクラウドサーバに代行させることができます。これに関する論文は、Eurocrypt 2015というトップレベルの国際会議に採択されました。

また、検索可能暗号に関しては、2015年6月にイタリアで開催されるclosedのワークショップに、日本人として唯一人、招待されています。

さらに、2016年２月にドイツで開催される現代暗号に関するclosedのワークショップにも招待されています。

世界をリードする研究者の一人として、国際暗号学会主催のAsiacrypt 2007やPKC 2013など多くの国際会議のプログラム委員長を務めてきました。このような世界的レベルの国際会議を、日立または茨城で開催することも、目標の一つです。

代表的な研究内容

提案したメッセージ認証コーがアメリカ政府に採用され、 CMACと命名されました。これは、事実上の世界標準であり、Windows, プレステ3などグローバルに使用されています。

また、黒澤デスメット・ハイブリッド暗号は、現在、最も優れた公開鍵暗号方式として世界中に広く知られています。

上田　賀一　教授

Yoshikazu Ueda　Professor

専門分野

ソフトウェア工学｜組込みソフトウェア｜ソフトウェアモデル検証｜ソフトウェア開発方法論｜ソフトウェアプロジェクトマネジメント

プロフィール

名古屋工業大学博士後期課程電気情報工学専攻修了，同大学助手，茨城大学工学部情報工学科講師，准教授を経て，教授．

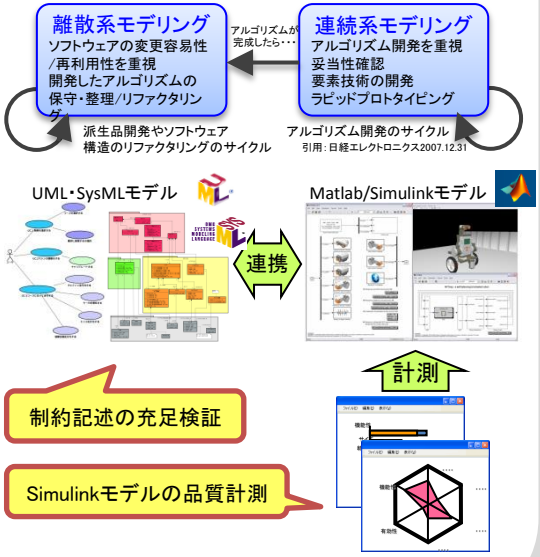
ライフワーク

ソフトウェア開発・保守の生産性や品質の向上といった要求に応えるため，モデル駆動アプローチを基礎にソフトウェアライフサイクルを技術者視点で支援する研究を進めています．また，高度ソフトウェア技術者育成は，産学間連携を基礎とする恒常的課題であると考えており，育成教育にはしっかりと関わっていきたいと考えています．

ICT社会においてソフトウェアが占める役割が高まるにつれ，ソフトウェア開発・保守が難しい状況・立場に追いやられています．ソフトウェアの生産性向上や品質向上といった要求に応えるため，ソフトウェア開発や保守を支援するさまざまなアプローチに取り組んできています．ここ数年は，特にモデル駆動アプローチを基礎に組込みシステム内のソフトウェアの品質改善に関わる研究として，(1) 社会的インフラとなる情報制御システムの大規模ソフトウェアを対象としたモデル検査手法の実用化，(2) 組込みソフトウェア開発を対象とした設計仕様策定支援のためのハイブリッド協調解析手法の開発，(3) 組込みシステム産業界で主流となっているSimulinkモデルを対象としたメトリクス計測と品質評価手法の開発などを進めています．加えて，ソフトウェア開発・保守の業務改善アプローチについて企業固有の状況に応じた対策の検討にも協力できます．

代表的な研究内容

組込みソフトウェアの設計を支援するハイブリッド協調解析手法や設計モデルのメトリクス計測と品質評価手法．



齋藤 修　特命教授

Osamu　Saitou　Professor

プロフィール 2009 年茨城大学大学院理工学研究科博士後期課程終了｜2005 年まで日立製作所グループで25 年間勤務。原子力計装設計後に情報系に。主にネットワーク装置設計、生産管理システム構築に従事｜2009 -2010年茨城大学地球変動適応科学研究機関科学技術振興研究員｜2012 年特命准教授　|2013 年特命教授 現在に至る

専門分野

｜土木技術｜防災｜橋梁｜地盤特性｜モニタリング｜監視システム｜環境情報可視化｜センサ｜RFID｜ICタグ｜センサネットワーク｜UAV

ライフワーク

産学官民連携の異分野融合による新しい仕組造り・新しい技術や市場、ヒューマンリレーションシップそして人材を作り出すことが使命と考えています。茨城大学工学部で指導する空手道も人材育成と自分磨きの一つです。

環境情報の可視化のための各種センサやRFIDと組み合わせた小型・低価格のセンサICタグの開発を行っています。

橋梁のモニタリングや地中を伝わる振動の変化よる地盤特性把握、地域のCO2 のモニタリング、内水氾濫監視システムを実現しています。また多分野に利用できるセンサネットワークシステムの応用研究や、UAVを用いた防災システム・構造物長寿命化のための試みを行っています。

情報通信、電気・機械技術と土木技術の融合は新たな技術やビジネスのチャンスを生み出します。

代表的な研究内容

共同研究
・加速度センサーを用いた斜面崩壊メカニズム・地盤特性解析に関する研究
・環境情報可視化のためのセンサICタグ開発：水位・CO2・加速度・気圧
・UAVによるダム長寿命化のためのクラックマップ作成

（独）防災科学技術研究所

鎌田 賢　教授

Masaru　Kamada　Professor

専門分野

|信号・画像処理 | 標本化理論
| ウェブサービス | 動的システム

プロフィール 筑波大学助手、同講師を経て、1992 年茨城大学工学部助教授、2005 年同教授、現在に至る。2005 年から2013年まで㈲ラーニングアイ取締役。2009 年1月からIEEE Transactions on Industrial Electronics 編集委員

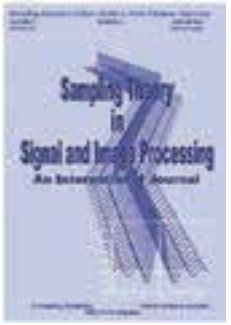
ライフワーク

電子工作好きの小・中学生でしたが、だんだん柔らかくなって現在はソフトウェアを作っています。アナログとディジタルの狭間での数学的で実用的な仕事を得意としています。

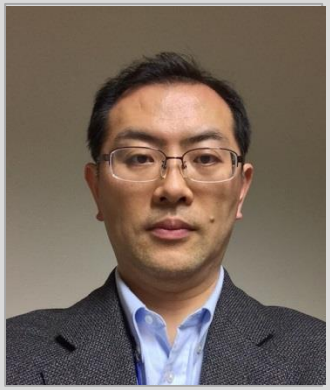
センサネットワークでのデータ収集から、一般社会向けのウェブ表示、スマートフォンのアプリまで幅広く研究・開発を行っています。現在、内水氾濫監視システムの実証実験ウェブサイトを運用中です。震災を経験したからこそわかる、役立つ地域防災のための通信インフラおよび個人ユーザ向け防災アプリをいっしょにつくり、普及させましょう。他社がまねできない強みをもっている企業のみなさん、おもしろいこと、新しいことをいっしょにやりましょう。

代表的な研究内容

状態遷移図によるキャラクタ記述に基づく子供向けプログラミング言語、極近距離・超高速ディジタル無線通信方式、画像補間向け可変張力スプライン関数



最強のリソースは、ウェブ情報技術、ネットワーク関連技術を備えた優秀な大学院生の頭脳です。



大瀧 保広 准教授

Yasuhiro Ohtaki Associate Professor

専門分野

暗号応用システム | ディジタル情報の権利保護システム | ネットワークセキュリティ | Webシステム | 情報漏洩対策 | 個人情報保護

プロフィール

筑波大学大学院博士課程（電子・情報工学専攻）修了後、
茨城大学工学部情報工学科 助手、同講師を経て、現在
IT基盤センター 准教授

ライフワーク

さまざまなセキュリティ技術を組み合わせることで、情報を適切に管理・蓄積し、利用をコントロールする方法について研究をしています。

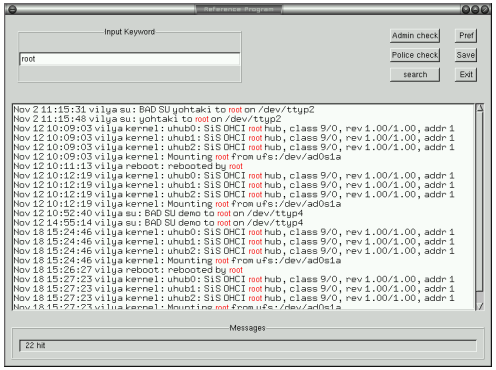
インターネットでは大量の個人情報が取り扱われています。サービスを提供する側のコンピュータでは、どこからアクセスしてきたのか、どのデータにアクセスしたか、どのようなサービスを利用したのかなど、詳細な情報が記録されています。意識的にユーザ登録をした場合でなくとも、一般の人々が大きな危機意識なしに発信した情報から、個人情報が漏洩することもあります。情報活用と情報漏洩の問題を解決するには、情報にアクセスできる範囲を適切にコントロールする技術が必要です。

「検索可能な暗号化方式」の研究では、情報を暗号化して記録・蓄積し、指定したキーワードを含む部分だけを選択的に取り出す方法を開発しています。

情報の利用をコントロールする技術としては、利用者同士でのコピーを正当な流通経路として利用する、次世代のコンテンツ流通システムがあります。インターネットを利用したコンテンツ流通での問題点は、コピーをどうやって防止するかではなく、実は、著作権者に正当な対価が支払われる仕組みをどうやって実現するか、です。つまり、許諾を与えた人（対価を支払った人）にのみコンテンツの利用を許可し、それ以外の人には利用させない。これを実現する基本的な仕組みの構築を目指しています。

代表的な研究内容

部分開示が可能な検索可能暗号方式



藤芳 明生　准教授

Akio Fujiyoshi Associate Professor

専門分野

形式言語理論｜木文法｜木オートマトン｜グラフ文法｜グラフオートマトン｜グラフアルゴリズム

プロフィール

2000年3月 電気通信大学大学院修了 博士（理学）
2000年5月～2005年6月 茨城大学工学部（助手）
2005年7月～2011年3月 茨城大学工学部（講師）
2011年4月～ 茨城大学工学部（准教授）

ライフワーク

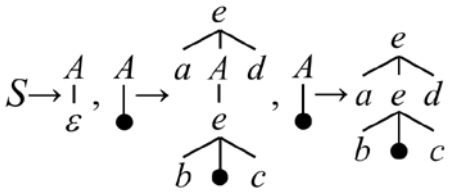
形式文法およびオートマトンの理論的な研究を行うとともに、それらを現実社会に役立てるための応用に関する研究を行っている。

木文法／木オートマトン → 数式の構造解析に木文法を活用した数式OCRの開発
2次元ピクチャー文法 → PDFドキュメントのレイアウト解析
グラフ文法／グラフオートマトン → 化学構造式向け正規表現による構造検索

研究室の学生とともに、読字障害（dyslexia）の児童生徒のために、音声ペンを使った2次元コード形式の音声付教科書の開発を行っています。これは、教科書紙面に見えない2次元コードを重ねて印刷し、音声ペン(2次元コードスキャナ内蔵デジタルオーディオプレーヤ)で対応する朗読音声や詳細説明を聞くことができる教科書です。「紙面を読む」と「対応する音声を聞く」という2つのモードを組み合わせ、視覚と聴覚を複合的に用いることで、能動的かつ自由な読書を可能にしています。

代表的な研究内容

- 木文法、木オートマトン及び木変換機の理論に関する研究
- グラフ文法、グラフオートマトンの理論に関する研究
- 科学技術文章の光学文字認識(OCR)に関する研究
- テストのユニバーサルデザインに関する研究
- 教科書のユニバーサルデザインに関する研究
- 視覚障害者向けの触読図の作図システムの開発に関する研究



石田　智行　講師

Tomoyuki Ishida　Lecturer

プロフィール

博士（ソフトウェア情報学）．宮城県出身．2003年～2006年：情報通信研究機構岩手IT研究開発支援センター，2006年～2013年：岩手県滝沢市，2013年～：茨城大学工学部情報工学科（助教）

専門分野

自然災害科学｜防災管理支援｜ネバーダイネットワーク｜GIS｜社会システム工学・安全システム｜バーチャルリアリティ｜オーグメンテッドリアリティ｜テレイマージョン｜タイルドディスプレイ｜共同作業バーチャル環境（CVE）｜感性情報学・ソフトコンピューティング

ライフワーク

様々な情報ネットワーク環境をデザインし，それを利用した新しいマルチメディア技術に関する研究を行っています．現在は，「総合災害管理支援システム」，「WEB-GIS災害情報共有システム」，「災害時ネバーダイネットワーク」，「AR技術によるユビキタスデジタルコンテンツシステム」の4つの研究テーマに日々取り組んでいます．

■研究テーマ①：防災・減災総合情報システムの構築

本研究テーマでは，大規模自然災害を教訓に，大規模自然災害時における防災・減災総合情報システムの構築に取り組んでいます．

■研究テーマ②：モバイル版伝統工芸システムの構築

本研究テーマでは，石川県七尾市の建具を例にとり，室内空間における伝統工芸プレゼンシステムの構築に取り組んでいます．

■研究テーマ③：動物園アプリ＆動物園内部業務支援システムの構築

本研究テーマでは，動物園における散策ナビシステムの構築および動物園業務統合型共通プラットフォームの構築に取り組んでいます．

■研究テーマ④：オープンデータ可視化システムの構築

本研究テーマでは，地方公共団体が公開しているオープンデータを可視化するシステムの構築に取り組んでいます．

■研究テーマ⑤：バーチャル博物館ARシステムの構築

本研究テーマでは，デジタルアーカイブにARとメディアを融合させた，メディア融合型歴史資料提示ARシステムを構築しています

■研究テーマ⑥：HMDによる臨場感システムの構築

本研究テーマでは，ヘッドマウントディスプレイを利用した高臨場感システムの構築に取り組んでいます．

代表的な研究内容

☆総合災害管理支援システム

☆伝統工芸システム

岡田 信一郎 講師

Shinichiro Okada　Lecturer

専門分野

知識工学｜教育工学

プロフィール

北見工業大学大学院電気電子工学専攻修了、博士（工学）（北海道大学）。北見工業大学助手を経て現職。

ライフワーク

ITエンジニアの教育、とくにプログラミングやデータベースに関する教育をコンピュータで支援する方法を研究しています。

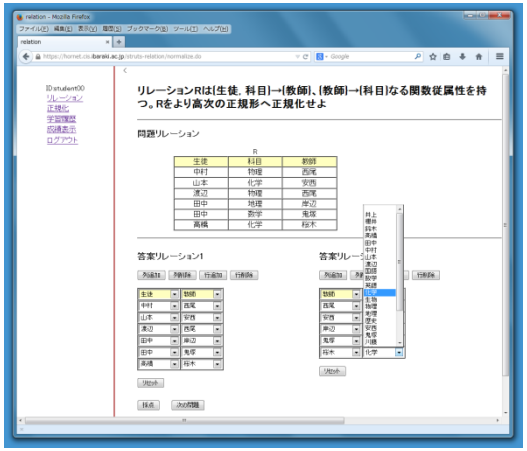
現在は、主にデータベースエンジニア教育のためのSQL実習支援システムとリレーショナルデータモデル演習システムの開発と評価を行っています。SQLとはデータベース操作言語で、リレーショナルデータモデルとはデータベース設計の基礎理論です。これらの技術はデータベースエンジニアにとっては手足のように使えなければならない技術ですが、習得には数多くの実習、演習を必要とします。前述のシステムは初学者を対象に基礎的な問題を多数出題し、繰り返し学習を行わせることで基礎力を固めることを目的としており、そのための問題生成機能、正誤判定機能などを備えています。

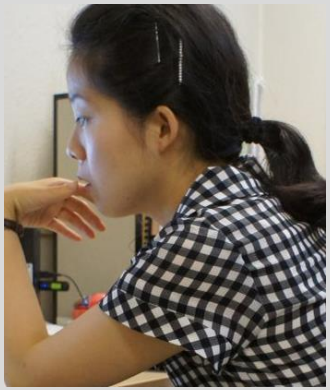
さらにこれらのテーマに関連して、繰り返し学習を効率よく行う学習支援方法の検討も行っています。

代表的な研究内容

SQL実習支援システム、リレーショナルデータモデル演習システムの開発・評価。効果的な反復学習の支援方法の研究等。

<リレーショナルデータモデル演習システム>





古宮　嘉那子 講師

Kanako　Komiya　Lecturer

専門分野

自然言語処理｜データマイニング｜ 機械学習｜人工知能 ｜語義曖昧性解消｜領域適応｜ゲーム情報処理

プロフィール

東京農工大学博士課程，東京工業大学科研費研究員，東京農工大学特任助教を経て茨城大学講師（情報工学科）

ライフワーク

状況やデータの性質にあった機械学習の研究をしています．特に，言葉に関する処理をコンピュータで行う研究をしています．

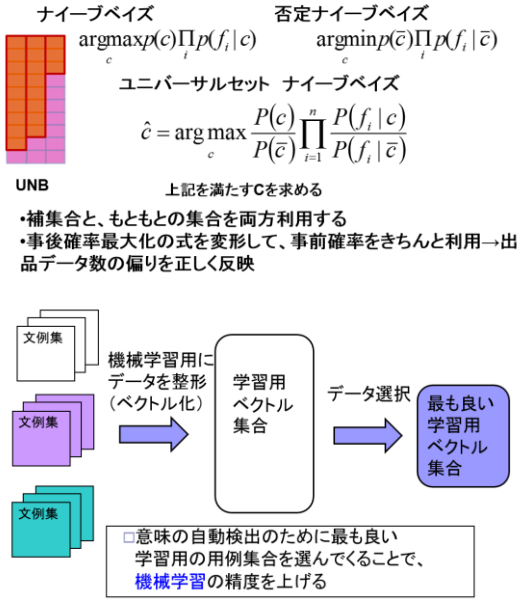
2014年度からできた研究室です．主に「自然言語処理」という言葉に関する処理をコンピュータで行う研究をしています．また，データマイニングといって，大量にあるデータの中から，コンピュータを使って人にとって役に立つ情報を抽出する研究もしています．また，茨城大学に来る前は，コンピュータ将棋やコンピュータ囲碁についても少し研究を行っていました．

これらに共通しているのは，「人工知能」の一分野であるという点と，「状況やデータによる適切な機械学習」を利用しているという点です．機械学習というのは，コンピュータにたくさんのデータを与えて，コンピュータが数理的にパターンを学習し，知識を自分のものにしていくという技術です．

当研究室では，他大学やデータマイニングを行っている企業とも議論を重ねて，さまざまなことに挑戦していきます．

代表的な研究内容

・否定ナイーブベイズ
・語義曖昧性解消の領域適応の訓練事例の選択の研究．



佐々木　稔　講師

Minoru　Sasaki　Lecturer

専門分野

自然言語処理｜データマイニング｜知識発見・分析｜情報検索｜機械学習

プロフィール

徳島大学大学院博士後期課程修了。
茨城大学工学部情報工学科助教を経て、
現在講師。

ライフワーク

大量に存在する文書や画像などのデータから、必要とする情報を効率的、効果的に抽出する手法についての研究、開発を進めています。

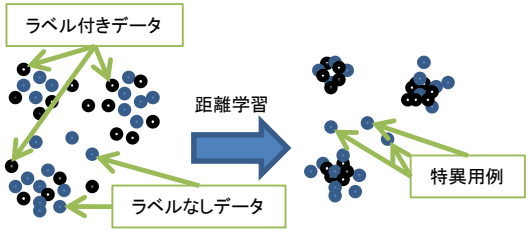
人が日常生活に使う言葉をコンピュータが理解できるように処理方法を考える「自然言語処理」という研究分野があります。現在、この分野における「語義曖昧性解消」の研究を行っています。

対象単語を含む文が与えられたときに、その単語が辞書のどの意味に属するか自動的に識別するシステムを構築しています。

機械学習手法の利用、辞書の整備・構築など、様々なアプローチで攻略し、人間が行う意味の解釈に近いシステムを目指します。

代表的な研究内容

Minoru Sasaki, Hiroyuki Shinnou, “Detection of Peculiar Word Sense by Distance Metric Learning with Labeled Examples”, Proceedings of the Eight International Conference on Language Resources and Evaluation (LREC'12)



Minoru Sasaki, Katsumune Terauchi, Kanako Komiya, Hiroyuki Shinnou, “Word Sense Disambiguation Using Active Learning with Pseudo Examples”, The Tenth International Conference on Advances in Semantic Processing (SEMAPRO 2016)

芝軒　太郎　講師

Taro Shibanoki Lecturer

専門分野

次元削減｜生体信号解析｜ヒューマン・マシン・インタフェース｜医療診断支援システム｜リハビリテーション工学

プロフィール

日本学術振興会特別研究員（DC2），同特別研究員（PD），広島大学大学院工学研究院特任助教，茨城大学工学部助教を経て，現在，同講師（情報工学科）．

ライフワーク

筋電義手をはじめとする生体生理情報を利用したヒューマン・マシン・インタフェースを発展させ，ヒトとシステムが相互に学習することで，より高度なシステムへと昇華できる「共創インタフェース」の開発に取り組んでいます．

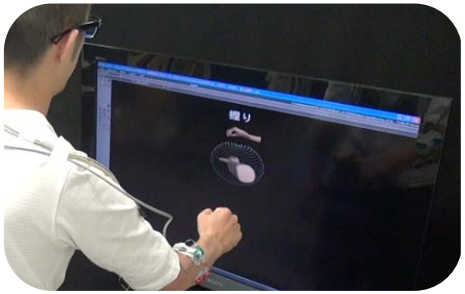
肢体不自由者の生活支援を目的として注目されている，生体生理情報を利用したマン・マシン・インタフェースに関する研究開発に取り組んでいます．

このような生体信号を利用したインタフェースにおいては，使用者それぞれの特徴に合わせてシステムを構築することに加え，使用者自身がシステム操作に慣れるための訓練を行う必要があります．そこで，これまでに情報選択のための新たな情報量：偏Kullback-Leibler（KL）情報量を提案し，使用者個々に適した生体信号の計測位置および機器制御に用いる動作を選定可能な方法論を構築するとともに，筋電義手や環境制御装置などの制御法について検討してきました．また，使用者の操作能力向上を目的としてvirtual reality (VR) 技術を利用した訓練システムを開発し，実用化に向けた取り組みを行っています．その他，生体生理情報の解析技術を応用した病床の診断支援システムやリハビリシステムの研究開発に携わっています．

現在，他研究機関や医療機関等と連携し，開発したシステムの実用化を視野に研究を行っています．

代表的な研究内容

VR筋電義手訓練システム



音声操作型環境制御装置

小澤　佑介　助教

Yusuke Kozawa Assistant Professor

専門分野

情報通信工学｜ディジタル変復調｜無線通信システム｜光無線通信システム

プロフィール

茨城県出身。2012年3月：茨城大学大学院修了、博士（工学）。 2012年4月～2017年1月:東京理科大学理工学部電気電子情報工学科（助教），2017年2月～：茨城大学工学部情報工学科（助教）

ライフワーク

研究分野は情報通信工学（物理層～ネットワーク層）であり、これまでとくに、

（A） 光空間通信：数十km以上の地上間、地上-宇宙での通信手法

（B） 可視光通信：数十m内の限られたエリア（スポット）での通信手法

における、変復調・信号処理・符号化技術の研究を行っています。また、提案方式について、理論解析・シミュレーション解析と基礎実験解析の両面から評価を行っております。これら研究概要の一部を以下に紹介します。

（A-1）光符号分割多元接続(CDMA)のための疑似雑音(PN)符号の研究：

光CDMA方式は光ファイバ通信、光空間通信における多元接続方式として着目されています(右上図)。しかしながら、光は非負信号のためRF通信用のPN符号を適用できません。本研究では、**新しいPN符号の設計基準として「光パルスの衝突を許容しつつ直交関係を達成するPN符号」を考案**し、従来法に比べ多くのPN符号（符号長に対してほぼ同数の符号数）を用いた大容量通信を実現しています。

（A-2）高信頼な光空間通信のための誤り訂正符号・階層型変復調法の研究：

光空間通信路では大気の乱流による光のゆらぎ、雲・霧・太陽光等の影響によって一時的に通信品質が大きく変動します。本研究では、低速に変化する大気変動に対して**1)差動符号復調を用いた誤り訂正符号技術、**通信路環境が劣悪になった場合でも、情報の要点だけは取得可能な**2)情報の格付けやメディア毎に適した情報伝送を用いる階層型変復調法**、等による高信頼通信を目指しています。

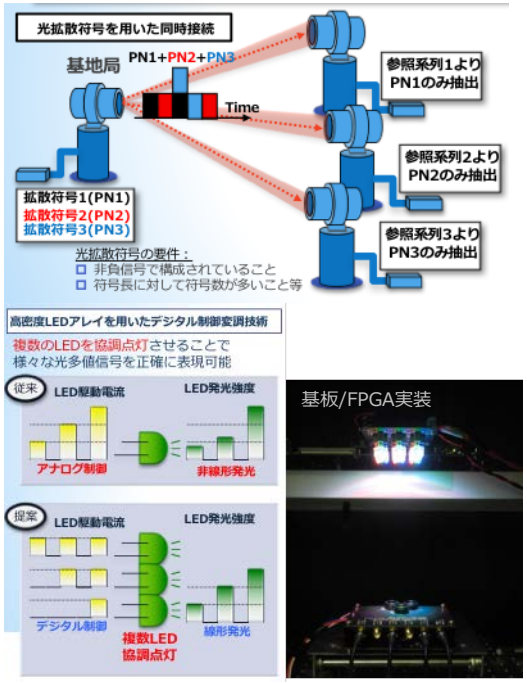
（B-1）高密度LEDアレイを用いたデジタル制御型変復調技術の研究：

可視光通信の送信デバイスとして使用されるLEDは、大容量通信に必須な振幅変調（多値光強度）時に、駆動電流に対する非線形発光により送信信号精度が大きく劣化します。本研究では、**複数LEDを協調利用することで、LEDのオンオフ動作のみで多値光強度を表現**（デジタル制御型変調）し、 非線形問題を解決しています（右下図）。

（B-2）人間の知覚量を考慮した照明可視光通信のための変復調技術の研究：

可視光通信では変調した光信号が人間の目に知覚されることから、通信性能に加えて、優れた照明性能を同時に満たす変復調技術の提案が必要不可欠です。本研究では、上記(B-1)の変復調法等に**調光/調色制御を付加した様々な照明用の変復調法の提案**を行っています。

代表的な研究内容



堀田　大貴　助教

Hiroki Horita　Assistant Professor

専門分野

経営情報学｜ソフトウェア工学｜ビジネスプロセスマネジメント｜プロセスマイニング｜要求工学｜

プロフィール

電気通信大学情報システム学研究科博士後期課程修了．茨城大学工学部情報工学科助教．

ライフワーク

概念的なモデルと実際に行われた事象を記録したデータという2つの側面からビジネスプロセスや情報システムの構築や検証を行う研究をしています．

情報システムは様々な企業や官公庁で利用されており，それぞれの業務を支援する役割を果たします．このような状況下では，実際の業務において真に有用な情報システムを開発するためには，情報システムの開発とビジネスプロセスの設計をそれぞれ独立して行うのではなく，組織の目標を達成するためのビジネスプロセスを設計し，それに合わせてビジネスプロセスの実行を効率的に支援するための情報システムを構築する必要があります．そのために，(1)ゴール指向要求分析技術によるビジネスプロセス設計，(2)プロセスマイニング技術によるビジネスプロセス実行ログの検証，に関する研究に取り組んでいます．概念的なモデルを利用して要求を漏れなく網羅的に満たしたビジネスプロセスや情報システムの設計をトップダウンに行うと共に，組織において実際に行われたデータを分析することで，現実的な側面からボトムアップにビジネスプロセスや情報システムの改善を行う方法論の確立を目指しています．

代表的な研究内容

リファインメントパターンに基づくKAOSゴールモデルからBPMNモデルへの変換