長崎県立大学
UNIVERSITY OF NAGASAKI

長崎県立大学　情報システム学部
研究シーズ集
2024

～ 情報システム学部　目次 ～

イチゴ収穫台車による圃場の計測と可視化

研究分野：実世界情報処理、ヒューマンインタフェース、農業情報学

キーワード：サイバーフィジカルシステム、スマート農業、計測、可視化

貢献できるSDGsの区分：

情報システム学部　情報システム学科　教授　有田　大作

教員情報URL　https://sun.ac.jp/researchinfo/arita/

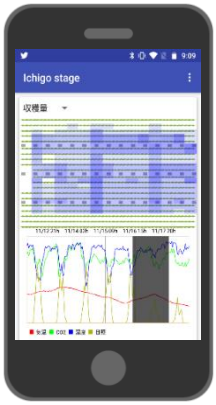
研究概要

イチゴ収穫台車に計測装置を搭載し（右上図参照）、イチゴ収穫時にハウス内を移動しながら以下のデータを毎日計測し、インターネット上のサーバに蓄積する。

- 温度、湿度、二酸化炭素濃度
- 収穫コンテナの重量（つまり、イチゴ収穫量）
- イチゴ棚の画像
- 収穫台車の位置

これらのデータを基に、以下のような情報の可視化することで農業経営を支援することを目指す。

- イチゴハウス内の温度、湿度、二酸化炭素濃度、収穫量をヒートマップによって可視化することで（右下図参照）、環境や収穫量の場所によるばらつきや相関がわかる。
- 毎日のイチゴの様子を画像で記録することで、一つ一つのイチゴ果実を過去にさかのぼって見返すことができる。



産学連携の可能性（アピールポイント）

2者間の共同研究から国プロ応募への参加まで対応可能ですが、まずは「とりあえず一緒にやってみる」ところから始められたらと思っています。

外部との連携実績等

- 農林水産省スマート農業実証プロジェクト「日本産イチゴの輸出拡大を強力に後押しするスマート高品質生産・出荷体系の構築」などのプロジェクトに、大学、公的研究所、民間企業、農家とともに参加
- 長崎県、長崎市、地元農家などとの連携

VDT画面デザインのアクセシビリティに関する研究

研究分野：デザイン学、人間工学

キーワード：色彩情報、アクセシビリティ、ユーザビリティ、VDT、人間中心設計

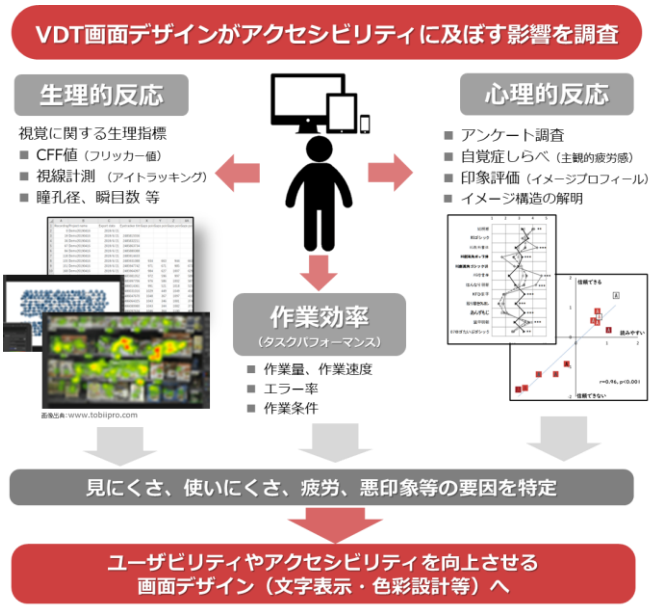
貢献できるSDGsの区分：

情報システム学部　情報システム学科　教授　片山　徹也

教員情報URL　https://sun.ac.jp/researchinfo/katayama/

研究概要

社会の幅広い領域でデジタル化が進んでいる高度情報社会において、コンピュータやスマートフォン等のディスプレイや公共空間に設置されたタッチパネル等を介して提供されるWebサイト等の情報コンテンツにおいて、誰もが快適に利用できる画面デザインは重要である。本研究では、VDT（Visual Display Terminals）の画面デザインを構成する諸要素に着目し、デザイン学的視座と人間工学的視座において、ユーザビリティやアクセシビリティの高いユーザインタフェースを提供するための画面や文字表示、色彩設計を明らかにすることを目的とする。



産学連携の可能性（アピールポイント）

①VDT画面デザインにおける諸要素がユーザビリティやアクセシビリティに及ぼす影響を明らかにすることで、タッチパネル等のディスプレイを有する製品を介して提供されるコンテンツの画面設計において誰もが快適に操作できるユーザインタフェース、適切な文字表示・色彩デザインへ適用できる。

②誰もが快適に操作できるデジタルコンテンツの画面設計のための新しい指針及びガイドライン策定のための基礎資料となる。

外部との連携実績等

外部資金実績

科研費基盤（C）（研究代表者）

・公共空間におけるタッチパネル画面のユーザビリティを高める配色パターンの開発（2019-2023）

・タブレット画面の文字色と背景色の色彩がアクセシビリティと生理心理反応に及ぼす影響（2016-2020）

・有彩色によるVDT画面が作業効率と生理的心理的反応に及ぼす影響（2012-2015）

外部委員等

ながさきデザイン会議委員、長崎市景観審議会委員、佐世保市景観審議会委員、大村市都市景観デザイン専門家会議委員、ながさきピース文化祭2025ロゴデザイン等制作業務委託に係る審査委員、長崎県内就職の魅力発信パンフレット等制作業務提携の公募型プロポーザルに係る審査委員等

数理的造形の研究

研究分野：数理的造形　芸術工学

キーワード：抽象アート　数学　プログラミング　CG

貢献できるSDGsの区分：

情報システム学部　情報システム学科　教授　金子 照之

教員情報URL　https://sun.ac.jp/researchinfo/kane-teru/

研究概要

フラクタル、カオス、複雑に組み合わせた関数、独自に定義した超複素数など、数学的手法による数理的造形を研究しています。研究者というより、デジタルアーティストとして活動していて、個展やグループ展などでの作品発表や様々なコンペに応募し続けています。国内外で多数受賞。数理的造形のためのアルゴリズムを考案することも楽しく、Linuxパソコンを駆使して、C言語、JavaScript、shell script、Pythonなどで描画プログラムを自作し、抽象アートのシミュレーションを繰り返し、パラメータを調整していきます。自由な発想によるコンピュータグラフィックスに没頭しています。数理的造形によって新たな抽象アート領域を切り拓くことに取り組んでいます。

産学連携の可能性（アピールポイント）

・自作プログラムによる数理的造形の体験ワークショップ
・数理的造形の講演

外部との連携実績等

・青少年のための科学の祭典への「きれいなもようをえがこう」ブース参加
・高校での出前講義や市民講座での数理的造形の解説
・国内外での作品展示、アート交流

地理空間情報を用いた地域活性化に関する研究

研究分野：空間情報工学、画像工学、地域工学

キーワード：地理情報システム、リモートセンシング、地域活性化、地域防災、ノンフォトリアリスティックレンダリング

貢献できるSDGsの区分：

情報システム学部　情報システム学科　教授　平岡透

教員情報URL　https://sun.ac.jp/researchinfo/hiraoka/

研究概要

現在、大きく下記の二つの研究を行っている。

① 誤差拡散による新しいタイプの非写実的な画像を生成する手法を開発している。また、これらの手法を動画や三次元データに拡張する手法も開発している。さらに。アイトラッカーを用いて非写実的な画像を生理心理的に評価する手法の開発も行っている。

② アンケート調査を用いたまちづくりDXに関する研究を行っている。

産学連携の可能性（アピールポイント）

民間企業で16年勤務した経験がある。具体的には、建設コンサルタントや地図関連事業などに従事し、地理情報システム開発の業務も行った経験もある。また、民間企業に勤務中に、測量士、技術士（情報工学部門）、データベーススペシャリスト、個人情報保護士、食品衛生責任者などの資格も取得している。

外部との連携実績等

＜外部資金実績＞

- 独立行政法人日本学術振興会，科学研究費助成事業・学術研究助成基金助成金（基盤研究（C）），研究代表者，“復元誤差と生成モデリングによる新しいタイプの非写実的な画像の開発と生理心理評価”，2023年度～2025年度.
- 公益財団法人大林財団，研究代表者，“長崎市東山手・南山手地区における歴史まちづくり計画のためのデータ分析に関する研究”，2023年度.
- 財団法人電気通信普及財団，研究代表者，“復元誤差によるノンフォトリアリスティックレンダリングの開発”，2023年度.
- 一般社団法人九州地方計画協会，令和3年度支援対象事業採択事業（調査・研究活動），研究代表者，“一ツ瀬川ダムにおけるアオコ発生の機械学習を用いた要因分析と予測”，2021年度.
- 公益財団法人高橋産業経済研究財団，研究助成事業，研究代表者，“都城盆地の地下水中の硝酸性窒素濃度の見える化と機械学習を用いた分析”，2019年度～2020年度.

＜外部委員＞

- 長崎県産業労働部，ながさき半導体ネットワーク，会員，2023.
- 長与町教育委員会，令和3年度長与町地域子ども教室運営委員会，委員，2023.
- 長崎市長崎創生推進室，令和3年度長崎市まち・ひと・しごと創生総合戦略審議会，委員，2023.
- 長崎市教育委員会，長崎市立長崎商業高等学校学科改編審議会，会長，2020・
- 長崎県物産ブランド推進課，長崎県産品データベースサイト構築業務委託プロポーザル審査委員会，委員，2020.

ICTによる地域コミュニティの活性化と人材育成

研究分野：人間情報学、観光学、社会システム工学、教育工学、サービス情報学

キーワード：イベントデザイン、Webデザイン、映像制作、バーチャル観光、
プログラミング教育

貢献できるSDGsの区分：

情報システム学部　情報システム学科　教授　吉村　元秀

教員情報URL　https://sun.ac.jp/researchinfo/yxsimura/

研究概要

地域の住民である「ヒト」、地域の活動である「コト（イベント）」、地域に広がる「モノ（サービス）」がスマートに連動する住みよい「まち」をデザインし、その要素となるシステムを設計・開発しています。「まち」には、QRコードやICタグを利用したキャッシュレス決済やスマートなレジシステム、交通系のICカードが普及しています。学習機能をもったスマートスピーカーが家庭に普及し、自動車の完全自動運転も夢ではありません。そんな「まち」づくりのためのデザインやシステムのコンセプトを提案し、日々、技術開発を行うのが吉村研究室です。

近年では、以下のテーマを主たる研究テーマとして、まちづくり工学研究室として、公共団体並びに地域企業との連携を図っています。

①プログラミング教育のためのコンテンツ開発とワークショップのデザイン
②映像や写真などのメディアを動的に活用したものがたりWebシステムの開発とデザイン
③360度コンテンツを活用したバーチャル観光ツーリズムのデザイン
④IoT機器を利用した社会機能をスマート化するIoTソリューションの企画・開発

産学連携の可能性（アピールポイント）

まちづくり工学は、近年の産学官民を複合的に推進する横断型研究の最たる取り組みです。100年に一度の長崎の変革が叫ばれる中、これからのみらい長崎をデザインする重要な要素が「ヒト」「コト」「モノ」を中心にまちのいたるところに散在しています。これまで長崎において20年弱継続しているまちとの協業の経験を活かし、先進的教育、ものがたりデザイン、スマート観光、IoTソリューションという要素を活用した未来都市長崎を一緒に創造しましょう！

外部との連携実績等

〈外部資金実績〉

2021-2023年度　科研費基盤(C)大学における災害時情報共有教育システムの構築（研究代表者）
2021-2022年度　長崎市広報広聴課連携事業　長崎市PR動画制作（研究代表者）外部委員
2021-2022年度　長崎市提案型協働事業等選定審査会　審査委員
2018-2022年度　渋谷TANPEN映画祭Climax at 佐世保　実行委員
2017-2022年度　ながさき・愛の映画祭　実行委員

触感定量化とその応用に関する研究

研究分野：感性情報学，情報工学

キーワード：感性，触感，機械学習

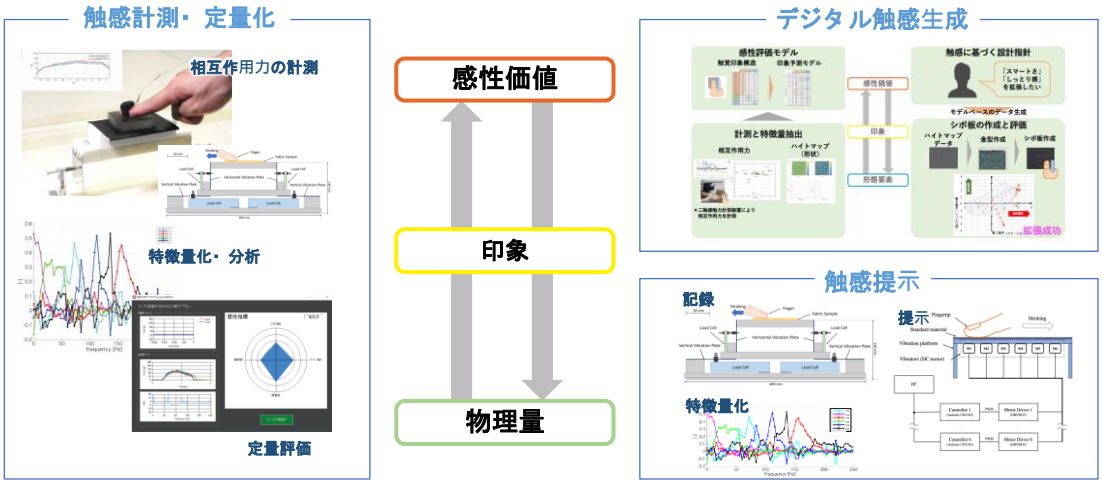
貢献できるSDGsの区分：

情報システム学部　情報システム学科　准教授　山﨑　陽一

教員情報URL　https://sun.ac.jp/researchinfo/yama-youi/

研究概要

ヒトが触れる製品のプロダクトデザインにおいて，触感は製品の良さ・好ましさといった感性価値を評価する上で重要な要素の一つです．本研究は，物体に触れた際に指先に加わる相互作用力を時間周波数空間での特徴量を抽出し，触感指標と対応づけることで定量化を実現します．これにより製品が提供する触感計測，製品デザイン，触感提示などへの応用展開が可能になります．



産学連携の可能性（アピールポイント）

本研究は幅広い応用展開が可能です．一部ですが実施例を以下に紹介します．

① 衣服や化粧品など触感が重視される製品の開発において，ユーザの触感嗜好を考慮することが価値向上の鍵になります．本研究を活用することで，触感による価値向上を狙った製品デザインが可能になります．

② 本研究は触感情報をデジタル化にも繋がり，触感を理解するAIの開発への展開が期待できます．

外部との連携実績等

① 自動車・化粧品・家電メーカー等14社以上との共同研究

② 科研費等の競争的学部資金獲得（研究代表3件，分担1件）

③ 計測・分析技術に関するセミナー講師の経験あり

④ 日本顔学会関西支部実行委員，World Haptics 2021でWorkshopのオーガナイザーなど

次世代無線通信における信号検出法の解析と改良

研究分野：通信工学，非線形物理学，信号処理

キーワード：大容量無線通信，Belief Propagation法

貢献できるSDGsの区分：

情報システム学部　情報システム学科　講師　迫田和之

教員情報URL　https://sun.ac.jp/researchinfo/sako-kazu/

研究概要

近年，様々なモノがネットワークに繋がるようになり，その多くが無線でネットワークに接続されている。今後もその傾向が続くとされ，無線通信の需要は増える一方である。それらの通信容量も増大しており，多数の接続かつ大容量の通信を成立させるため，次世代の大容量無線通信が盛んに研究されている。

本研究では，次世代の無線通信における信号処理の一つである，信号検出（受信側で送信信号を推定する技術）に注目し，提案されている信号検出法（Belief Propagation法を用いた信号検出）の解析や改良を行っている。その信号検出のアルゴリズムは，複雑でなぜ上手くいくのか明らかになっていないため，アルゴリズムの動きを可視化し詳細に調査している。また，その調査結果から改良点を提案し，次世代無線通信のさらなる性能向上を目指している。

産学連携の可能性（アピールポイント）

① 次世代無線通信に関するシミュレーション
② アルゴリズムの可視化

外部との連携実績等

① 日本学術振興協会，科学研究費助成事業　若手研究（研究代表者），大規模MIMOにおける特定の誤りに収束するBP信号検出の開発（2024年4月～2027年3月）
② 電気通信普及財団，研究調査助成（研究代表者），大容量無線通信に用いる新たなBP信号絵検出へのDNNを用いた学習の応用（2022年4月～2024年3月）

エンタメ作品視聴印象のリアルタイム評価

研究分野：実験心理学、音響心理学、音楽心理学

キーワード：エンターテインメント、音楽聴取、印象評価、リアルタイム評価

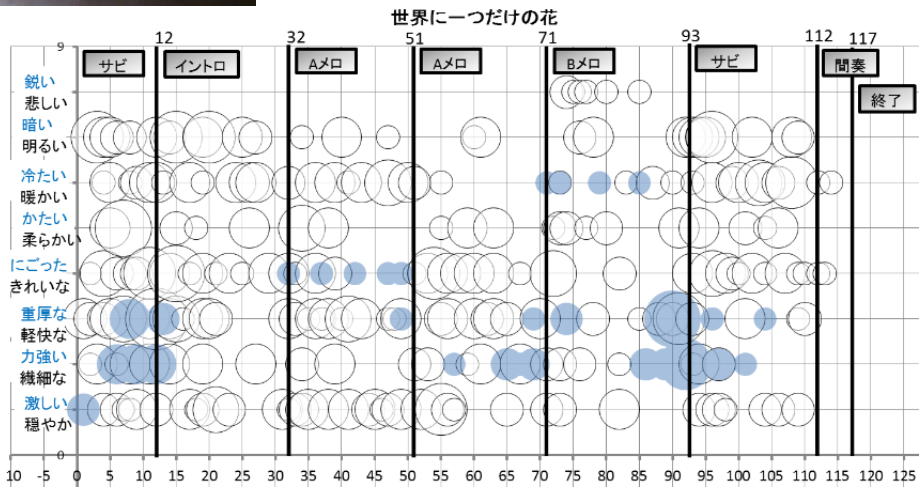
貢献できるSDGsの区分：

情報システム学部　情報システム学科　講師　藤沢　望

教員情報URL　https://sun.ac.jp/researchinfo/n-f/

研究概要

誰でも簡便に行えるリアルタイムの心理評価手法として、印象評価語を貼り付けたMIDIキーボードによる連続印象評価法を用いる。被験者は音楽等を視聴しながら、キーボードに貼られた印象を感じた時点でキーを押す。強い印象を感じた場合は、その強度に従って複数回キーを押す。このようにして得られたデータはバブルチャートにより表現され、作品中のどの部分でどのような印象が想起されたのかを視覚的に把握することが出来る。



産学連携の可能性（アピールポイント）

①楽や映像作品等の心理印象の収集
②収集した心理印象の活用

プレゼン行動における非言語行動による表現の個人差要因の特定と可視化

研究分野：画像処理、視覚メディア、メディア情報処理、可視化、信号処理

キーワード：画像工学、視覚メディア、メディア情報学、感性工学

貢献できるSDGsの区分：

情報システム学部　情報システム学科　講師　　前村　葉子

教員情報URL　https://sun.ac.jp/researchinfo/hazuki/

研究概要

プレゼンテーション、演技などのパフォーマンスは非言語行動により感情を豊かに表現するスキルを学習するひとつの機会となり、人間の発達を押し上げる効果があるとされる。本研究では,プレゼンテーションのひとつとして、紙芝居上演の演者のパフォーマンスに着目し、パフォーマンスに寄与する要素のなかで観測可能な非言語行動を測定し可視化する。

また紙芝居の場面転換にともなう場面感情の状態遷移を軸として演者の動作、表情、音声などのマルチモーダルな信号を観測し熟達差にかかわる特徴を抽出する.これらの数理モデル化を行うことにより新たな入力演技信号に対する非言語行動の各要素の熟達度を推定し提示するシステムの構築を目指す。

産学連携の可能性（アピールポイント）

①人物モーション分析（被験者数1・屋内・歩行無し）

②プレゼンにおける非言語行動抽出(被験者数1)

③汎用ウェアラブルセンサによる生体信号処理(被験者数1)

外部との連携実績等

なし

Society5.0の実現に向けた セキュリティ対策を確立するための研究

研究分野：情報通信 / 情報セキュリティ

キーワード：CPS、IoT、制御システム、組込みシステム、Zero Trust

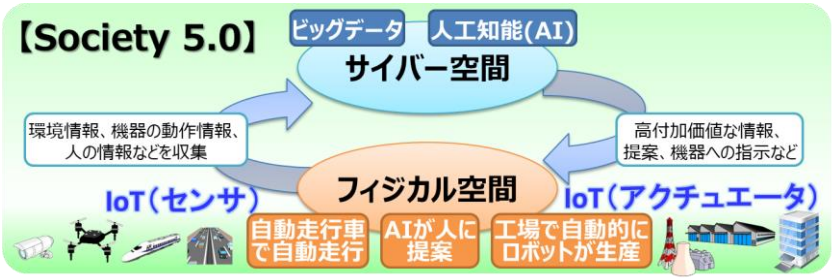
貢献できるSDGsの区分：

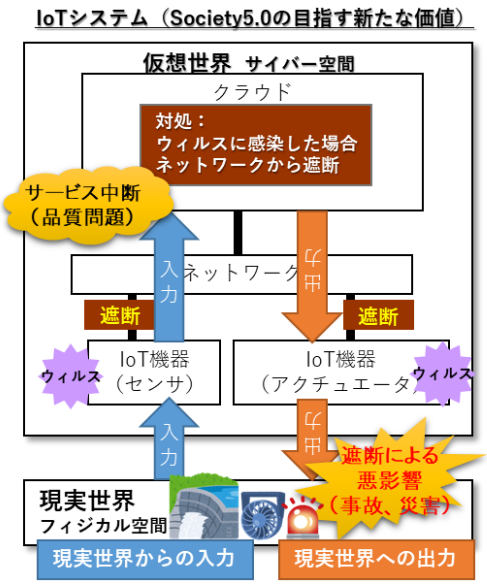
情報システム学部　情報セキュリティ学科　教授　小林　信博

教員情報URL　https://sun.ac.jp/researchinfo/koba-nobu/

研究概要

〇我が国が目指すべき社会の姿として掲げているSociety 5.0 は、「サイバー空間とフィジカル空間（現実世界）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する人間中心の社会」と定義されており、一例として、現実世界のセンサーから IoTを通じてあらゆる情報が集積（ビッグデータ）され、AIがビックデータを解析し、機器の制御などを再び現実世界に戻すことが示されています。





〇一方で、悪意によるサイバー攻撃を受けた場合に、現実社会にもたらされる被害が増大することが懸念されます。そこで、Society5.0の実現に向けてIoT制御システムの弱点となる脆弱性を発見し、そのセキュリティ対策を確立するための研究に取り組んでいます。

産学連携の可能性（アピールポイント）

〇CPS および IoT のサイバーセキュリティ確保に係るアドバイス、実証実験、スタートアップ支援
〇情報処理安全確保支援士 第004158号 2017年4月（取得）

外部との連携実績等

〇長崎市DX推進委員会 委員長（ 2021年7月 － 現在 ）
〇IoTセンサーネットワークにかかる実証試験、長崎県長与町・株式会社ラック（ 2021年5月 － 現在 ）
〇電子情報通信学会 情報・システムソサイエティ 情報通信システムセキュリティ研究専門委員会 専門委員（ 2022年6月 － 現在 ）
〇情報処理学会論文誌ジャーナル/JIP編集委員会（ネットワークグループ） 論文誌ジャーナル/JIP 編集委員（ 2022年6月 － 現在 ）
〇情報処理学会　コンシューマ・デバイス＆システム（CDS）研究会 運営委員（ 2022年4月 － 現在 ）
〇企業との個別共同研究（ 現在、4件実施中 ）

人に注目したサイバーセキュリティ対策の研究

研究分野：情報セキュリティ、サイバーセキュリティ

キーワード：リスクマネジメント、セキュリティ教育、人材育成

貢献できるSDGsの区分： 

情報システム学部　情報セキュリティ学科　教授　島　成佳

教員情報URL　https://sun.ac.jp/shim-shig/

研究概要

安全なサイバー空間を維持するには、年々複雑化・巧妙化するサイバー攻撃の脅威に対抗するため、3つの観点（技術・制度・人）から成るセキュリティ対策を、社会・組織・個人のそれぞれで実施する必要がある。しかし年々変化する脅威に、社会・組織・個人はどのように対応していけばよいかを判断することが難しい状況にある。

また、技術面や制度面の対策強化が進んでいる一方で、人の対策は利用者の知識の更新や新たにITサービスを利用しはじめる世代への教育等、簡単に強化が進まず時間もかかる状況である。

さらに、攻撃は判断ミス等の人を狙う傾向が強まっており、巧妙化にもなっており、人への対策の重要性が高まっている。そして、複雑化・巧妙化する攻撃に対応できるセキュリティ人材の不足も深刻化している。

本研究では、サイバーセキュリティをリスクマネジメントの観点から捉え、リスクの評価や受容等の手法やリスク判断する指標を考案している。また、セキュリティ教育や人材育成に関しては、サイバー演習によって人の成熟度を測る手法の考案やコンテンツの創出を行っている。

産学連携の可能性（アピールポイント）

①サイバーセキュリティ対策をリスクマネジメントに係るリスク指標の提案やリスクを評価を行います。
②セキュリティ教育や人材育成に係る成熟度を測る手法や教育コンテンツを提案します。
③情報処理安全確保支援士を取得しております。

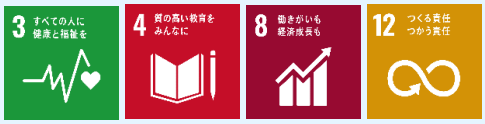
外部との連携実績等

〈2021年～現在〉
　国立研究開発法人情報通信機構（NICT）　共同研究
〈2021年～現在〉
　独立行政法人情報処理推進機構（IPA）　専門委員

導入・運用コストを抑えた安心・安全な働き方改革を推進するための研究

研究分野：データベース関連、情報セキュリティ関連

キーワード：データベースシステム、コンテンツ管理、情報検索、最適化、アクセス制御

貢献できるSDGsの区分： 

情報システム学部 情報セキュリティ学科　教授　C.ソムチャイ

教員情報URL　https://sun.ac.jp/researchinfo/somchaic/

研究概要

「深刻な人手不足問題」「長時間労働問題」を解決するために、多くの組織が「働き方改革」に取り組んでいます。組織の情報資産を守り、生産性を向上させるために、さまざまな分野に適した働き方改革をどのように進めていくかを研究しています。

意味的検索技術を使って、組織のコンピュータ内にある多様な情報を正確に収集し、構造化および半構造化データモデルなどでそれらの情報を統合することができます。統合された情報から、最適なソリューションを導き出すことができます。また、経営戦略に関わる全てのデータを数値化し、これまで勘に頼っていた部分を数値に基づいて合理的に経営戦略を構築することができ、生産性の高い業務を遂行することができます。さらに、オープンソースのデータベースソフトウェアや低価格のツールを活用することで、人件費や経費の削減を実現するとともに、従業員の仕事と家庭（プライベート）の両立をより柔軟なワークスタイルで実現することができます。

産学連携の可能性（アピールポイント）

以下の研究成果は、導入・運用コストを抑えた安心・安全な働き方に関するものです。

①表計算ソフトを用いた効率的なデータベース照会・更新インタフェースの研究開発

②ショッピングサイトの商品比較効率化を図る新たな検索用インタフェースに関する研究開発

③パターンマッチングに基づいたWebデータ自動抽出手法の提案　― 複数の就活ナビサイトからの求人情報・企業情報を収集するケース ―

④ユーザーの検索意図に沿ったオフィス文書の検索方法に関する研究

外部との連携実績等

〈2006年4月～2011年3月〉

「情報爆発に対応するコンテンツ融合と操作環境融合に関する研究」

研究代表者:京都大学大学院情報学研究科 田中克己教授

分担者：　チャットウィチェンチャイ　ソムチャイ

情報漏えいの人的要因に対する対策研究

研究分野：ユーザブルセキュリティ、サイバーセキュリティ

キーワード：セキュリティ対策行動促進、ヒューマンファクター、行動経済学

貢献できるSDGsの区分：

情報システム学部　情報セキュリティ学科　教授　寺田　剛陽

教員情報URL　https://sun.ac.jp/tera-take/

研究概要

サイバー攻撃検知やアクセス制御の技術は高度化し、組織マネジメントのガイドラインは洗練されてきているにもかかわらず、個人・機密情報の漏えい、詐欺被害、ランサムウェアなどによる業務停止の報道は後を絶たない。

その主な要因の1つに、ITシステムを利用する人間の不合理さにある。具体的な行動としては誤操作や権限設定ミス、ルール違反などであり、その背後には攻撃手口に関する知識不足のほか、作業忘れや対策先延ばし、正当化などがある。

本研究ではこういった人的要因による被害発生を減らすため、人間工学などの観点から被害の発生点（メールソフトやサーバ管理画面、アプリなど）における「不親切さ」を抽出し、それを補うツールを開発することで、人間の行動原理に沿ったITシステムの実現をめざす。

産学連携の可能性（アピールポイント）

①セキュリティポリシー順守状況と人間工学的観点に基づく対策行動促進ツールの提案・開発
②従業員の生産性を犠牲にしない日常的な情報リテラシー教育ツールの提案・開発
③ビジネスメール詐欺検知ツールの提案・開発

外部との連携実績等

・共同研究・委託研究：エムオーテックス株式会社（2023～）、総務省（2013～2016）
・講師：株式会社富士通エフサス（標的型メール訓練、2022）、中央大学 JEITA IT講座「電子社会と情報セキュリティ」（2017）、FUJITSUファミリ会関東支部 セキュリティ対策講座（2014,2015）
・IWSEC（International Workshop on Security） 実行委員（2015）

安全性と機能を両立する暗号技術の開発

研究分野：情報学基礎論、情報セキュリティ

キーワード：高機能暗号、軽量暗号、耐量子計算機暗号

貢献できるSDGsの区分：

情報システム学部　情報セキュリティ学科　教授　星野　文学

教員情報URL　https://sun.ac.jp/researchinfo/hosh-fumi/

研究概要

情報セキュリティは大雑把に言うと、権限のない人が情報を勝手に読めない性質「機密性」、権限のない人が情報を勝手に操作できない性質「完全性」、権限のある人が情報をいつでも自由に読んだり操作できる性質「可用性」の三つの要素から構成されると考えられています。

一般に暗号技術においては機密性と完全性は非常に重視されますが可用性は軽視される傾向があります。機密性や完全性を守るために、特定の人以外一切情報を読んだり書いたり出来なくしてしまう、即ち可用性を犠牲にして機密性や完全性を確保するのが暗号の機能です。この意味で可用性は機密性や完全性とは一種のトレードオフの関係にあります。

実は機密性や完全性を損なわずに、如何に可用性を拡張するか？というのが近年の暗号研究の一つの大きな流れとなっています。高機能暗号はそのような背景の元で形成された概念で、高機能暗号を用いると きめ細かな権限の設定が出来たり、暗号文同士で何らかの演算が可能であったりします。本研究ではそのような暗号について研究します。

$$Enc(m_0) \times Enc(m_1) = Enc(m_0 + m_1)$$

図：高機能暗号のイメージ

産学連携の可能性（アピールポイント）

①本研究にて開発した暗号技術を用いることで、従来の暗号技術では解決が困難であった実社会の問題解決を図るシステムやアプリケーションの開発ができるようになることが期待できる。

②開発した暗号技術を活用した新たなアプリケーションを実現できることも期待できる。

外部との連携実績等

共同研究実績：

- 2023年度、長崎県立大学・文教大学・群馬大学・NTT社会情報研究所、「光演算処理を用いたセキュリティ技術の共同研究」
- 2023年度、長崎県立大学・東京大学・九州大学・NTT社会情報研究所、「QR-UOVに関する共同研究」

ブロックチェーンの鍵管理と応用に関する研究

研究分野：暗号応用技術，ブロックチェーン，プライバシ保護

キーワード：ブロックチェーン，鍵管理，鍵紛失

貢献できるSDGsの区分：

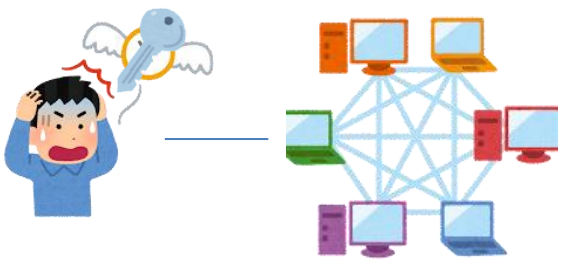
情報システム学部　情報セキュリティ学科　教授　松崎　なつめ

教員情報URL　https://sun.ac.jp/researchinfo/matsuzaki/

研究概要

近年，暗号資産の基盤技術である「ブロックチェーン」を用いた応用開発が盛んである．ブロックチェーンでは，複数のノードに信頼を分散することでシステムの安全性を確保する一方，そこでやり取りされる価値の安全性は個々のユーザの秘密鍵管理にゆだねられる．

本研究では，**「秘密鍵の紛失対策」**に着目し，安全で利便性の高い方法を研究している．具体的にはブロックチェーンの上で動作するプログラムを用いて，自動的に鍵を退避する方法を考案し，実装評価している．



産学連携の可能性（アピールポイント）

・ブロックチェーンの応用システム（例えば，サプライチェーンや認証など）の開発や，その安全性に関して提案・評価をします．
・安全で利便性の高い鍵管理方法を開発し，実装評価します．
・鍵管理において，ユーザ自身のプライバシ保護にも配慮した方法を開発します．

外部との連携実績等

・科研基礎研究(C)，「ブロックチェーンに適した分散管理システム用鍵管理方法の設計と評価の研究，2020.4～2024.3.
・長崎市個人情報保護審議会委員（2017年～現在）
・長崎県個人情報保護審査会委員（2023年～現在）

新たなディジタル署名技術の開発

研究分野：情報学基礎論，情報セキュリティ

キーワード：ディジタル署名，耐量子計算機暗号，高機能署名，ディジタル署名の応用

貢献できるSDGsの区分：

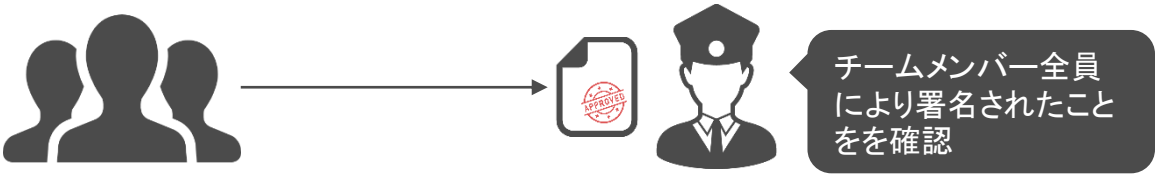
情報システム学部　情報セキュリティ学科　准教授　福光正幸

教員情報URL　https://sun.ac.jp/researchinfo/fuku-masa/

研究概要

ディジタル署名は，なりすましや改ざんがないことを保証する暗号技術の一種であり，SSHやFIDOなどの認証プロトコルやブロックチェーン，電子契約システムなどさまざまなシステムの基盤技術として活用されている．一方，暗号研究の中では，「なりすましと改ざんがないこと」+αの保証を実現する署名技術（以降，高機能署名と呼ぶ）の開発が進んでいる．その一例として，「マルチ署名」を挙げる．これは，複数人で構成されるチームメンバー全員によりデータを保証するための技術である．

本研究では，これまでに実現されている高機能署名を更に発展させることによる，新たな高機能署名技術の開発や，既存のディジタル署名技術を用いた新たなアプリケーションの開発を行う．



図：マルチ署名のイメージ

産学連携の可能性（アピールポイント）

- 本研究にて開発したディジタル署名技術を基盤とすることで、従来のディジタル署名技術では困難であった新たなシステムやアプリケーションが実現されることが期待できる。
- 高機能署名の開発のアプローチには近年報告されているディジタル署名技術を進化させる方向性もあるが、本研究では実社会の問題をベースにこれを解決できる新たな高機能署名を開発するアプローチも視野に入れている。
- 近年著しく研究開発が進む量子コンピュータを用いた攻撃について考える必要があるが、本研究においても、量子コンピュータを用いた攻撃に耐性のある高機能署名技術の開発を進めている。

外部との連携実績等

- 日本学術振興会，科学研究費助成事業　基盤研究(C)，AIデータの保証に特化した暗号技術の開発（2023年度～）．
- 電子情報通信学会などのゲストエディタ・プログラム委員への就任