第 8 班

非文字資料研究のコミュニティにおける知識とサービスの効率的な検索と安全安心な流通研究

(1) 共同研究員名

研究代表者：木下宏揚
共同研究員：能登正人　佐野賢治　森住哲也
客員研究員：宮田純子
研究協力者：小松大介

(2) 研究目的

《知識とサービス、物の流通と価値交換》

非文字資料を研究者間および一般ユーザと知識、サービス、資料をやり取りするためにゲーム理論によりモデル化を行う。また、ビットコインで注目されている自律分散的に事象や価値の移転を記録するブロックチェーンの技術を用いて安全安心な価値交換を行うシステムを構築する。

《知識とサービスの検索とマイニング》

非文字資料のデータベースや研究者が資料を検索する際に、作業の流れであるコンテキストの一面に着目して情報の類似度などに基づいてファイルの自己組織化などによりユーザに対して最適な情報を提示する。

《個人情報や重要情報、著作権の管理》

ブロックチェーンを用いたアクセス履歴管理を行うことで個人情報に対するハイパーグラフを用いた推論攻撃検出の実装を容易にする。また、ブロックチェーンによる価値移転により著作権管理を効率的に行う方法を提案する。

(3) 活動経過（目的達成のための方法、各年度の研究・調査経過、成果の公開状況等）

1　2017 年度研究経過

1.1　ブロックチェーンを応用した流通と著作権

デジタル化された著作物がオリジナルであるという証明や二次著作物、不正使用の対策には埋め込みの順序の証明に意味を持つが電子透かしのみでの実現は困難である。先行研究では、信頼できる第三者により解決しているが、プライバシー、結託、第三者の存続性の問題があるため完全に信頼することが難しい。信頼できる第三者を必要としない方法を提案するために、本研究では、ビットコイン

などに用いられているブロックチェーンの仕組みを電子透かしに用いる方法について考察する。ブロックチェーンは、記録する情報をハッシュ関数により圧縮するが、画像など冗長性の多いデータは単にハッシュ関数を求めただけでは不可逆な圧縮符号化や電子透かしの埋め込みなどにより同一の画像にもかかわらず異なるハッシュ値となってしまう。そこで画像の特徴量に基づくフィンガープリントを生成し、これのハッシュ値を用いることで電子透かしの埋め込みにも対応可能となる。フィンガープリントを生成する手法として、python の anaconda 環境において著作物を Bag-of-words 表現の SIFT を用いて登録する。画像一枚の特徴を抽出し得られた特徴量からハッシュ値を生成し、このハッシュ値をブロックチェーンに登録するという方法を採用する。今年度は画像の特徴量抽出について検討を行った。

1.2　大規模クラウドに於ける新しい情報セキュリティを潜在的な非文字概念から探究

非文字として表象されるテクストとは何か？この問いに対し、今年度は下記に示す主要な成果（論文 3 点、他）が得られた。即ちまず、「非文字」とはテクストに陽に書かれていない潜在的なテクストであると見做す。その潜在性を工学的に示す試みの 1 つとして、AI で使用される確率的モデルに着目する。非文字に於ける潜在性は潜在的ディリクレ配分法に於ける潜在的パラメータと呼ばれる確率変数によって示される。本論文では次に示す 4 つの仮説に基づいてこの問題に取り組んだ：

1. 『意味』は『作用』とともに変動する。
2. 思考と言語的振る舞いには情報理論的な相関がある。
3. 実在を指示するテクストの、「語」を命題の変項と見做し、「語」と言う変項を『確率変数として見る』。
4. テクストを構成する語は事前的な語と事後的な語の相互情報量が最大になる様に生成される。

潜在的なデータを顕在化させる取り組みの具体化の 1 つとして非文字データの分類整理のみならず、情報セキュリティに於けるセキュリティモデルの根本的な見直しにも取り組んだ。即ち隠れチャネルモデルと推論攻撃モデルの統合である。この取り組みは非文字とは無関係である様に見えるが、根本は類似した現象である。重要な手掛りは、ウィトゲンシュタインの『家族的類似概念』、及び、『私的言語の捉え方』である。「テクストのあつまり」とは、＜私＞と他者の言語的振る舞いが映し出された object であり、かつ＜私＞と他者の「その時々」が示された「対象領域」:『ウィトゲンシュタインの言語ゲームに類する帰結』である。次にこの「対象領域」の分析手法の必要条件としてテクストが生成、結合、消滅する過程を確率測度空間の写像、即ち確率変数で表現し、潜在的ディリクレ配分法に基づく確率的モデルで記述する方法を提案した。さてこの様にして探究してきた確率的モデルは論理学的モデルと如何なる関係にあるのだろうか？私たちは日常的存在者を如何に捉え様々な規則に対峙するべきなのだろうか？言い換えれば、「世界を確率的に捉える事」は、倫理として如何に捉えられるべきであろうか？今季は、この問いに対する試論にまでたどり着いた。即ち：＜私＞的言語のパラドクスを認めながらも、実はその治療法たる“ 文法像 ”と言う概念が＜私＞そのものを示すパターンであり、そのパターンを示す必要条件が確率測度空間であること。確率測度空間における倫理とは、確率的存在者に嵌める制約、或いは「枠」であり、自他それぞれにとっての振る舞いの調和が映し出された“ 文法像 ”の 1 つの表現形式であることである。

1.3　推論攻撃を考慮した重要情報漏えい保護

一般に推論攻撃によってどのような情報が得られるかは明白ではないためデータベース管理者は、扱う機密情報に対して推論攻撃が成功する可能性をあらかじめ考慮して情報を管理しなければならない。

そのためには、データベース管理者（情報発信者）が機密情報間の依存関係をあらかじめ把握しておくことが重要だと考える。先行研究では、このような推論攻撃に対抗するためには膨大な情報群とその間にオブジェクト間の推論関係を検知して警告するようなシステムが必須であると述べた上で、グラフにリスト着色を施すことで推論経路を検出し、アクセス制御をする手法が提案されているが、そもそものオブジェクト間に存在する推論関係というものはあらかじめ人間が定義した上で推論経路を検出している。本研究では、昨今の扱うデータの多様性に対応すべく、対象とするデータを単語レベルから文書レベルにまで拡張し、推論規則を求めるために必要となるオブジェクト間（情報間）の関連性を確率的に求める手法としてトピックモデル（潜在的ディリクレ配分法）を用いた。これにより、情報漏えいを引き起こす危険な投稿を未然に防ぐ事ができる。

1.4　コンテクストに基づくファイル管理

トピックモデルは潜在意味解析などに用いられていることから、検索シーンにおいてユーザが潜在的データの検索が可能だと考える。先行研究ではトピックモデルの画像分類への適用や画像のトピックを抽出し、トピック分布により類似画像を検索する方法が提案されている。文献では画像の特徴量である SIFT を抽出しベクトル量子化を Bag-of-words 表現（BOW 表現）できる形式にし、k 平均法でクラスタリングしてトピックモデルを用いて画像を分類している。画像だけでなく文書の情報を加えることにより、画像もしくは文書データからのみでは発見することが困難な潜在的な画像発見が可能となる。本研究では、文書と画像を BOW 表現しトピックモデルに適応させる。画像においては SIFT により特徴量を抽出し、ベクトル量子化を用いることで BOW 表現できる形へ変換する。文書と画像から BOW 表現により統合し単語集合を抽出し、これに対してトピックモデルを適用し、潜在的データを検索するためのフレームワークの提案を行う。これにより Wikipedia など文書が画像を説明しているようなウェブサイトなどから関連または潜在的な情報を抽出することでユーザに新たな発見を促すことができる。

1.5　テクストの相互情報量により非文字オントロジー間を接続する概念の提案とそのケーススタディ

研究の目的に鑑み、最も根本的な問題：「非文字を分析可能なテクストとして如何に捉え処理するか」、と言う問題に対し、確率論的解決の試みを示す。即ち、非文字オントロジーを含む大量の日常的テクストを想定し、そこから語と語の間の局所的で相対的な自己相互情報量により語の連鎖を生成する。そして語の連鎖が生成するテクストを情報理論的な相互情報量として評価する手順を示す。非文字データベースの検索はこの手順で生成される大規模なグラフの検索問題に帰着される。本論文では、異なる木構造の間をテクストの集合に於ける語と語の自己相互情報量と言う内積の連鎖で接続し、

生成した語の経路が生成される事後確率密度、及び経路から潜在的テクストが生成される事後確率密度を潜在的ディリクレ分布配置法（LDA）でベイズ推定する方法を示す。更に、自己相互情報量の計算によって異なるオントロジー語間を連鎖させて接続するアルゴリズムについて、自己相互情報量を計算する関数を再帰的に使用するアルゴリズムを提案する。また、異なるオントロジー語間の経路作成が可能であることを case study によって示す。

2　2018 年度研究経過

2.1　自己組織化ファイルシステム

作業のコンテキストに応じたファイルのクラスタリングとディスプレイへのアイコン配置の最適化の手法として、群知能のうち PSO を用い、目的関数に Boid 的要素を用いるモデルの提案を行った。

2.2　Topic Model とオントロジーを用いた非文字検索システム

先行研究では福島県只見町の民具を対象とした民具オントロジーを考慮したデータベース (以下、DB) 検索方法が提案されている。しかし先行研究の民具オントロジー (以下、既存オントロジー) では概念系の定義が不透明なため、検索できない民具がある。一方で、農作業概念を記した語彙体系である Agriculture activity ontology(以下、AAO) を用いることで、正確に情報の意味を考慮し、結果を推論する意味的検索を実現できる可能性がある。本研究では、生産用途民具を対象とし、AAO ベースの民具オントロジー (以下、民具 AAO) の構築、それに対応した DB 構造を提案し、高度な意味的検索実現を目的とした。現状の研究では民具という「扱い難い性質」をオントロジーという木構造の分類整理手法によって表現する、その手法自体に限界がある。本研究では非文字の本質を情報理論的に捉える。言い換えれば、木構造の分類整理法ではなく、民具などの対象物の分類をクラスター分析として確率論的に捉える。対象物のクラスターを確率分布として捉えることにより、この問題は Bayesian 機械学習の問題に還元される。この研究では非文字の意味を確率論的な潜在性として再定義し、対象物のクラスターの中の潜在的な非文字の確率変数によって木構造で表現される概念をつなぐモデルを示し、それを実現するシステムを提案した。

2.3　ハイパーグラフを用いた推論攻撃検出

情報漏えいの原因として注目されている推論攻撃をハイパーグラフを用いて解析する手法を開発してきたが、推論規則の獲得手法について検討を行った。ベイジアンモデルによる情報漏えい分析のための機械学習では、確率測度空間上のベイズ主義的な事象と見做す。即ち、機密にすべき事前的、潜在的なクラスターが機密を包摂するクラスターの族と言う事後的なクラスターを形成すると解釈し、潜在的な確率変数を推定する。現象をこの様に捉えるベイジアンモデルにより、観測されたテクストデータを条件とする covert channel と inference channel の潜在的な確率変数の事後確率を統一的に機械学習するモデルを提案した。更に提案モデルの事後確率は word2vec により機械学習可能であることを示した。さらに、自己相互情報量 (PMI) をベースに PMMI(Pointwise Mutal Multiple Information) という指標を用いた評価方法の提案を行い、統計的に分析をすることで機密情報に対する推論規則生成に適用した。次に、米国や英国をはじめとした世界各国で標準化されたデータ形式である Linked

OpenData(LOD) に基づいたデータ公開が行われている。LOD はデータのオープン化、分野内でのデータ共有、そして分野を横断したデータの共有を促進するという特徴を持っている。本研究では、Ubuntu、OpenRefine、Google ドライブの環境下で LOD を実装し、コミュニティでの LOD と公共の LOD のリンクによって起こる Covert Channel を分析し、情報漏えいの防止を目的とした。OpenRene の Reconciliation Service API(名寄せ) アルゴリズムの中にコミュニティでの LOD と公共の LOD の間の Covert Channel を分析し、アクセスを制御するアルゴリズムを考察した。

2.4　ブロックチェーンを用いた推論攻撃の検出法

情報漏えいが発生した際、情報の持ち主が自分の情報が漏えいした事実を知らないため、詐欺などに遭う可能性が高い。ブロックチェーンはアクセス履歴の信ぴょう性を保証してくれるため、それに記録されたアクセス履歴に基づいて情報が漏えいする可能性があるかどうかを確認できるだけでなく、ユーザに自分の情報が漏えいするかもしれないということを警告することによって詐欺などからユーザを守ることもできる。情報漏えいが発生する原因としては、アクセス権の矛盾に起因する Covert Channel がある。従来はアクセス権の設定が固定された静的な Covert Channel 解析を行っていたが、アクセス権の変化をブロックチェーンに記録し、動的な Covert Channel 解析を行うことで静的な解析では検出できなかった情報漏えいの検出を可能にした。通常のオンラインストレージは管理者がユーザごとにアクセス権を分離して割り当てているため情報漏えいは発生しないが、共同研究の情報共有に必要不可欠なオンラインストレージの招待機能はファイルに対して複数のユーザのアクセスを許可するため意図しない情報漏えいが起こる。招待によって起こる第三者への情報漏えいを防ぎ、アクセス権の変更をスマートコントラクトを用いて自動化を目的とするシステムを提案した。スマートコントラクトの特徴である決めた条件を満たしたら、契約内容を自動的に実行することを利用して情報漏洩を防ぐためにアクセス権を自動的に変更できる。また自動的にアクセス権が変更できるため、管理者が必要なく、ユーザ間で自由に招待でき、安全に情報共有ができる。

2.5　ブロックチェーンに基づくデジタル画像の著作権管理システム

オリジナルの著作物をもとに、新たな著作物を創作する二次著作物、三次著作物に電子透かしを埋め込む場合、著作物が作成され新たに埋め込まれた電子透かしの順序関係を明確にする必要がある。従来は信頼できる第三者が透かし埋め込みの順序を保証していたが、自律分散型のシステムでは望ましくない。そこで、透かし埋め込みの順序をブロックチェーンに記録することで、これを解決するシステムを提案した。また、透かし情報を別の画像に流用できないように、人間が同じ情報と感じれば同じメッセージダイジェストを生成する知覚ハッシュ関数に基づいた透かし情報を利用している。また、セキュリティモデルに Take-Grant モデルを採用することで、デジタルコンテンツのやり取りにおいて利用権などの改ざんがされていないかを確認することを目的とした。

2.6　ファイアウォールのポリシー設定問題

ファイアウォールのポリシー設定問題は、先行研究では機械学習のナイーブベイズを使用して、確率的性質からアクセスコントロールリスト (ACL) を更新する手法が試みられている。しかし確率を

使用するため、ポリシーに従わない異常なルールが作成される場合がある。そこで教師あり機械学習のランダムフォレストを用いて、ポリシーを満たしたルールを自動で ACL に適用することができると考える。よって本研究ではランダムフォレストを用いてポリシーを満たすルールの作成と ACL への自動適用を目的とするシステムの提案を行った。また、このファイアウォールを仮想環境化するにはどのようにすればよいかも提案した。

2.7　画像処理に影響を受けない特徴量の抽出の基礎的研究

Deep Learning が注目された大きな理由は識別に有効な特徴量を機械が自ら学習することにある。従来の機械学習では識別に有効な特徴量を選択する必要があった。その先駆けとなる手法の一種として Convolutional Neural Network（CNN）がある。CNN は特に画像識別に特化していて、識別精度が高いともいわれている。その識別精度が高い理由としては中間層に畳み込み層とプーリング層という 2 種類の層を用いていることである。しかし、中間層に着目した研究が少ない。そこで CNN の中間層を抽出しその特徴量を報酬とみなし､学習させるシステムを検討した｡サンプル画像に対してアフィン変換、ノイズの付加など様々な加工をした画像データを CNN の実装である Caffe や Keras を用いて中間層を抽出する。その抽出した中間層の特徴量を報酬とみなして、ベイジアン逆強化学習で学習させ、そこで不変量が得られるかどうか調べるためのシステムを検討した。

2.8　只見町の調査、研究打ち合わせ

9 月 19 日から 20 日にかけて只見町に調査、研究打ち合わせの出張を行った。旧朝日公民館で民具資料の展示方法、分類方法、聞き取り方法の調査と主な民具の製造過程や使用方法について聞き取りを行った。只見町役場において現状報告などの打ち合わせを行った。また町長、副町長を交えて情報交換を行った。只見町役場において只見カードの調査と今後の方針について打ち合わせを行った。数年後に新設される只見町の博物館において研究成果を取り入れたシステムを設置できればということになった。只見ブナセンターにおいて新国氏より展示方法や資料収集方法について説明を受けた。

2.9　潜在的なテクストのパターンを AI により健在化し、分類評価する研究 (パターンランゲージの研究)

(1) ノンパラメトリックベイズによる「『多重な』潜在的ディリクレ過程」を詳細設計した。具体的には PMI の評価指標によって生成する単語の連鎖によって 2 つのオントロジー語彙をディリクレ過程により接続するモデルを学会発表（9 月）した。

(2) パターンランゲージとは、言い換えれば「非文字を確率測度空間から測度空間へ写像する確率変数である」と捉える言語である。或いは、パターンランゲージは大量のテクストの中に潜む潜在的な確率変数である、とも言える。潜在的な確率変数は既知ではないので、まず機械学習させるテクストを効率よく収集するシステムが必要である。本年度は単語間の PMI により単語の連鎖を生成し、単語の連鎖の KL 情報量により単語連鎖の Boid（但し、各単語はそれらが帰属するテクストに紐付けられていなければならない）を生成する手法を提案した（卒研テーマ)。

(3) パターンランゲージは自他のための新しい言語である。それはウィトゲンシュタインの家族的

類似概念によって言語ゲームを実践する場所を提供しなければならない。そのためには大量のテクストの潜在的なパラメータを確率変数とし、上記（2）の処理の後、テクストのクラスターの確率分布を機械学習させる。今年度はこのモデルとして Blei の supervised LDA の潜在的確率変数を強化学習のアクションの潜在的なパラメータと解釈し、かつ Ramage の Labeled LDA を強化学習の状態 S のラベルとして解釈する、教師ありベイジアン逆強化学習（Supervised Bayesian Inverse Reinforcement Learning(S-BIRL）と呼ぶ事にする）のグラフィカルモデルを提案した（3 月学会発表)。

(4) 上記に示すモデルは＜私＞という視点を人工知能的システムに組み込む「離見の見」の概念を実現するためのアプローチである。即ちそれは､「それぞれの＜私＞が他者を如何に解釈するか」という問いに対し、ウィトゲンシュタインの言語ゲームに於ける家族的類似の概念と世阿弥の「離見の見」の概念を確率モデルによって設計するという位置付けにある。この研究では、そのような設計が、“ ただ設計するのではなく、善く設計していることになるのか？ ”という倫理的考察を、ウィトゲンシュタイン、ベルグソン、マルクスガブリエル、坂部恵、等を手掛かりに考察を継続し、設計に反映させた (学会発表)。

3　2019 年度研究経過

3.1　ブロックチェーンの電子透かしへの応用

ブロックチェーンは信頼できる第三者に依存することなく、権利の移転などのイベント発生の時系列の保証を行うことができる。ブロックチェーン技術に基づいた仮想通貨やスマートコントラクトが普及してきており、著作権管理の分野にも利用され始めている。これを電子透かしを含むデジタルコンテンツの著作権管理に応用した。

ブロックチェーンによる電子透かし管理システムの改善と透かし情報の削減

昨年度提案したブロックチェーンを用いた多重電子透かし管理システムの、電子透かし、ブロックチェーン、および知覚ハッシュに基づくデジタル著作権管理システムの 3 つの相互関係について検討を行いプロトコルの改良を行った。電子透かしの透かし情報のデータサイズと電子透かしの耐性はトレードオフの関係にある。そこで､ブロックチェーンによる透かし情報の保存と管理の手法において、透かし情報はブロックチェーンに記録し、実際に埋め込む透かしは、その暗号学的ハッシュ値を用いることで、透かし情報のデータサイズを大幅に削減することが可能となった。

新しい知覚ハッシュ関数

信頼できる第三者が不要な多重電子透かし二次著作物など複数の権利者が介在している場合、創作や加工の順序を明示する必要がある。従来は信頼できる第三者が情報を管理していたが、コストやプライバシー保護、セキュリティの観点から望ましくない。ブロックチェーンにコンテンツのメッセージダイジェストを記録することで、これを解決できるが、SHA256 などの暗号学的一方向性ハッシュ関数を冗長性の高い画像情報などに適用すると、加工および符号化により視覚的には差異を検出できなくても異なるハッシュ値となってしまう。そこでコンテンツの加工に耐性のある知覚ハッシュが必

要となる。深層学習が画像認識などの分野で普及が進んでいるが、畳み込みニューラルネットワークの処理過程で得られる中間層の出力は画像に固有の構造情報が含まれている。そこで、中間層出力から知覚ハッシュに利用可能な最適な組み合わせを検討し、透かし情報に適した知覚ハッシュ構成法を検討する。既に大規模なデータセットで学習済みの CNN を、本実験用に転移学習したものを利用する。転移学習とは、既に大量の画像データセットで画像の分類について学習した CNN のモデルを、別の画像データセットの分類に利用する手法であり、少ないデータセットでも高い分類精度が期待できる。また、CNN はフィルタを通して画像の特徴を抽出する畳み込み層と、特徴毎にさらに小さな画像を生成していくプーリング層からなる。プーリング層では、畳み込み層で抽出した特徴を小さな画像にまとめており、浅い層では入力画像とほとんど同じ画像であるが、層が深くなるにつれて、画像がより小さく単純な構造になっていくことから、知覚ハッシュに利用する中間層は最も深いプーリング層を利用する。これに主成分分析を適用し、確率分布を解析することで、加工編集に対して耐性のあるプーリング層のノードを抽出し、これをもとにハッシュ値を導出した。また、CNN 中間層出力データの位相幾何学的構造のクラスター群から不変的なクラスターを抽出し、それをベイズ統計手法によって機械学習推定することにより知覚ハッシュを生成する手法を考案した。

CNN における認識率向上のための層数と Loss 関数の選定

画像認識の発展は、自動運転の実現など産業革命の分野の発展においても必要不可欠である。また、人間をも上回る認識率を誇り、近年大きな注目を集めている。しかし、層数や容量の多い学習済みモデルを利用した画像認識は、時間がかかり効率的とは言い難い。本研究では、9 層の CNN をベースモデルに利用し、少ない層数による効率的で、現実的な画像認識を目的として、畳み込み層追加と選定、ε の最適値の選定を提案し認識率向上を図った。さらに実験結果を比較検証し、提案手法の有効性を示した。

3.2 ブロックチェーンを用いたデジタルコンテンツの流通

デジタルコンテンツとその著作者を保護するため、様々な DRM（デジタル著作権管理）が提案されているが、現在広く普及している DRM では、コンテンツの配信事業者がコンテンツの利用制限を行い、利用者間でのコンテンツの受け渡しは制限されている。これらを改善するため、新たな手法としてブロックチェーンに基づく著作権の移転を可能にするスマートプロパティや、権利に基づくコンテンツに対する操作を保証するスマートコントラクトが DRM に用いられ始めている。従来の DRM を用いて、信頼できる第三者を必要とせず、デジタルコンテンツの著作権や利用者がコンテンツに対する権利を証明することは困難である。これらの問題点を解決するため、先行研究ではスマートプロパティやスマートコントラクトを用いたシステムやビットコインのプロトコルの 1 つである Open Assets Protocol を用いたシステムが提案されている。しかし、ユーザに対してデジタルコンテンツの利用を制限するシステムは提案されているが、デジタルコンテンツが他のデジタルコンテンツの利用を制限することはできない。例えば、音楽配信サービスと楽曲のような関係の場合、コンテンツ利用の制限は音楽配信サービスに依存し、楽曲そのものに著作者は制限をかけることが困難である。よって、コンテンツとその利用者、コンテンツとそれを利用するコンテンツの関係を明確にしてデジタル

コンテンツを保護する必要があると考える。提案するシステムを通してデジタルコンテンツを流通させるかぎり、利用者間、コンテンツ間、利用者とコンテンツの 3 つの関係を合わせた中でコンテンツが保護できるようなシステムを目指す。本研究では、権利の移転を、主体を利用者、対象をデジタルコンテンツとした Take-GrantModel で表現し、不正なコンテンツ利用を Covert channel にモデル化することでコンテンツの著作者が意図しない権利の流通を分析し、流通の防止を可能とすること、これらのシステムをブロックチェーン技術であるスマートコントラクト内で実行することで、利用者は取引実行の有無とコンテンツに対する権利を証明し、安全で効率の良いコンテンツの流通を実現することが目的である。

3.3　非文字資料の検索 : LDA を用いた非文字資料検索法

近年、インターネット上に日々大量の情報が増えてきている。紙の文書も電子データに変換する試みも増え、書籍を調べるよりもインターネットを利用して調べるほうが素早く多くの情報を比較できる。正確で早い検索を可能にする、文書の意味をメタデータに記述する方法や、文書中の単語を意味解析し自動で分類する方法が研究されている。トピックモデルは文書が複数の潜在的なトピックから確率的に生成しているという考え方で、pLSA や LDA という手法を用いることでコンピュータで文書のトピックモデルを計算することができ、文書のトピック分布を比較することにより文書間の類似度を測れる。そこで LDA の出力にベイズの定理を用いることにより算出される“単語を構成するトピック分布”を用いて単語と文書の類似度を測れるのではないかと予想した。本研究では、LDA の出力にベイズの定理を用いることにより算出される“単語を構成するトピック分布”と文書を構成するトピック分布の類似度から、文書中の特定の単語に注目した時に現れる類似した文書を提示するシステムのモデルを提案した。

3.4　重要情報の保護

推論攻撃の情報漏洩に着目した言語ベクトルの次元圧縮

近年では SNS などでの情報発信やビッグデータの解析などによりさまざまな恩恵が受けられる反面、プライバシーの侵害が問題になっている。従来のアクセス制御の枠組みでは扱うことが困難であった推論攻撃による情報漏えいに対処する必要がでてきた。推論規則生成を考えた場合は推移率、相関を扱えるモデルである skip-gram や c-bow 等を用いると高次元データになってしまう。自然言語処理におけるデータの高次元化は精度、計算速度の面において非常に重要な問題である。日本語のドキュメントにおける高次元ベクトルデータに対する次元圧縮の手法において、Tensor 分解を組み合わせることにより低次元に次元圧縮した際の精度の向上を目的とし研究を行った。

非文字データベースを対象とした AHP に基づく covert channel の解析

ストレージからの情報漏洩を防ぐために、アクセス制御が使われている。アクセス行列は一般に covert channel と呼ばれる情報漏洩を引き起こす経路が存在する。従来この covert channel の評価はセキュリティモデルによって行われてきた。しかし、人と人の関係、あるいは人と情報の関係を論理学的モデルによって示すことは、それによって表現される応用的現場を限定させることになり、使い勝

手が悪くなるという問題があった。本研究は神奈川大学非文字資料研究センターで行われている「非文字資料」をデータベース化するという研究に関連している。この非文字データベースにおいても、covert channel が起こり、情報漏洩につながる可能性がある。そこで、大量のテクストをトピック分析し、テクストの確率変数としてのクラスターを学習させ、クラスターの中にあるテクスト同士の類似度を確率的に求める。次に人と人の関係、人と情報の関係をセキュリティモデルの属性から役割、競合、および所有と定義する。最後に、テクストの類似度、役割、競合、所有を階層分析法（AHP）の評価基準と定義し、意思決定を支援する AHP 分析によって複数の covert channel を評価し、切断するべき covert channel を選択する、というモデルを提案した。

2 つの確率モデルの組み合わせによる Multi-Label Learning の解釈について

本研究では、提案したセキュリティモデルに新たに人間の定めたセキュリティポリシーやセキュリティ規則を確実に反映させる手法として Multi-label Learning による重み付けを行うモデルについて提案を行う。前回までのセキュリティモデルでは、人間の定めたセキュリティポリシー等が教師データに入っていたとしてもそれがアクセス制御に反映させることができているかは、確実性に欠ける点が存在していた。しかし、この重み付けを行うことによりそのセキュリティポリシー等をより確実に反映させることができ、命題および関連するテクストを含むアクセス制御を可能とした。その重み付けとして 2 つの確率モデルを使用し、テンソル分解したものとみなすことができる。これは今までの Multi-label Learning で使用されてきた 1 つの確率モデルによるテンソル分解と同じものであると言える。本研究ではその重み付けの実際にどの程度の効用が得られるかを実験によって確かめた。

ランダムフォレストを用いたファイアーウォールの規則の生成

近年、ネットワークの発達によって技術の向上がみられる反面、これを悪用したサイバー犯罪が問題となっている。そのサイバー犯罪を防衛するシステムに「ファイアーウォール」がある。ファイアーウォールのルールはセキュリティポリシーに沿って、手動で設定する。しかし手動設定では設定をし忘れるとルールは正しく作成されず、その部分をついて攻撃される危険がある。こうした問題に、先行研究では教師あり学習のランダムフォレストを用いることで、セキュリティポリシーに沿ったルールを自動で ACL（アクセスコントロールリスト）に適用するシステムを提案した。本研究ではさらに様々な条件のデータをランダムフォレストによって学習させ、より実用的なルールを作成するシステムを提案する。

3.5 潜在的なテクストのパターンを AI により健在化し、分類評価する研究（パターンランゲージの研究）

(1) 単語の局所的な部分集合を単語の連鎖と見做し、この部分集合族が得られたと仮定する。次に部分集合族の単語集合要素の評価を Boid の particle 間の強度と定義する。この様なコンセプトで人工知能の前処理（Annotation）を設計し、Python でプログラミングして動作を確認した。

(2) Boid annotation を更に精密にする方式を先行して研究した。提案方式は Boid と LDA(Latent Dirichlet Allocation）をカスケード接続する方式である。この方式は Annotation をカスケードす

ることで、Labeled-LDA の様に複雑なベイズ確率モデルを使用せず、所望の機械学習が可能になる効果を持つ。この方式を応用しセキュリティモデルに基礎付けられたテクストを教師テクストとし評価するべきテクストを情報量として評価するシステムを提案した（研究会発表済み）。

(3) VAE(Variational Autoencoder) と GAN(Generative Adversarial Networks) 導入の計画を変更し、上記 (2) に関連する LDA の研究に注力した。即ち、LDA の発展形となる Labeled-LDA、Multi-Label-Learning を調査し複数の信頼できるソースコードを入手し、動作検証、コード分析した。Label という構造は (2) の新提案システムとの組み合わせによる機械学習の精緻化が可能である。

(4) “ ただ設計するのではなく、善く設計するとは何か？ ” という倫理的考察を、ウィトゲンシュタイン、ベルグソン、等を手掛かりに研究する過程に於いて、ジャン＝リュック・ナンシーの哲学が言語と身体性を連関させるという点で大きな意味を持つことが明らかになってきた。即ち、「言語ゲームとして普遍を見るとは何か」を考察する上で、分有ロゴスと身体性論は不可欠の概念であることに行き着いたのである（研究会発表済み）。

(4) 研究成果（成果物、獲得された知見、収集資料の解題等）

1. KINOSHITA Hirotsugu, MORIZUMI Tetsuya,"Access Control Model for the Inference Attacks with Access Histories", Proc. of IEEE COMPSAC 2014,10.1109/COMPSAC.2017.41, Jul. 2017.
2. 宋　先波、森住哲也、木下宏揚、“ テクストの相互情報量により非文字オントロジー間を接続する概念の提案とそのケーススダディ：潜在的テクストを確率変数として見る場合 ”、信学技報、vol. 117, no. 126, SITE2017－18, pp. 135－140, 7 月。
3. 矢田一貴、木下宏揚、森住哲也、“ トピックモデルを用いた潜在的関連性を考慮した情報検索 ”、第 80 回情報処理学会全国大会、7B-03、2018 年 3 月。
4. 松下智樹、木下宏揚、森住哲也、“ 機械学習を用いる推論を考慮した情報漏洩の検出 ”、第 80 回情報処理学会全国大会、2E-06、2018 年 3 月。
5. 森住哲也、木下宏揚、“ 確率的セキュリティモデルの可能性について ”、2018 年暗号と情報セキュリティシンポジウム (SCIS2018)、1C2-2、2018 年 1 月。
6. 森住哲也、“ 論理学的存在者から見る確率的存在者の倫理とは何か ”、信学技報、技術と社会・倫理研究会 (SITE) 、 3 月。
7. 辻順平、能登正人、“ テーマパーク問題におけるパレート最適性を考慮した滞在時間短縮フレームワーク ”、人工知能学会論文誌、Vol.33, No.2, pp.C-H98-1-9 (2018).
8. Zhaoxiong Meng, Tetsuya Morizumi, Sumiko Miyata, Hirotsugu Kinoshita, \Design Scheme of Copyright Management System Based on Digital Watermarking and Blockchain", 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Vol.2, pp. 359－364、2018
9. 森住哲也、“ 論理学的存在者から見る確率的存在者の倫理とは何か ”、信学技報、vol. 117, no. 471,SITE2017-76, pp. 213－219, 2018 年 3 月 .
10. 森住哲也、木下宏揚、“ 確率測度空間に於いて脱構築装置を内在するアクセス制御について ”、

信学技報、vol. 118, no. 152, SITE2018-28, pp. 281－287, 2018 年 7 月。
11. 中谷憲・森住哲也・木下宏揚、“ ベイジアンモデルによる情報漏えい分析のための機械学習 ”、電子情報通信学会ソサイエティ大会、A-12-1、2018 年 9 月。
12. 森住哲也、“ 確率測度的テクストと決定論的テクストを循環させる逆強化学習システムの倫理とは何か ”、信学技報、vol.118,no.345, SITE2018-62, 2018-12-06, pp.17－23, (2018)。
13. 森住哲也、“ 情報理論的尺度に基づく家族的類似クラスターの順序関係の学習可能性について 〜 ベイジアン逆強化学習の報酬を家族的類似度と見做すこととは何か？ ”、2019-02-28 (SITE, IA), (2018).
14. MENG Zhaoxiong, MORIZUMI Tetsuya, KINOSHITA Hirotsugu, MIYATA Sumiko,\Perceptual Hashing based on Machine Learning for Blockchain and DigitalWatermarking",IEEE 2019 ThirdWorld Conference on Smart Trends in Systems Security and Sustainablity (WorldS4) DOI: 10.1109/WorldS4.2019.8903993, July 2019)
15. 紅林宏祐、森住哲也、木下宏揚、“ Boid 的アノーテーションと Labeled-LDA による家族的類似の推論規則生成: 推論攻撃分析と covert channel 攻撃分析を統合する機械学習的アプローチ〜 ”、信学技報、vol. 119, no. 141, SITE2019-36, pp. 243－249, 2019 年 7 月。
16. 森住哲也、“ 必ずしも完全に分有されないロゴスと言語ゲームをつなぐ確率的存在者：セキュリティモデルの限界と人工知能の可能性 ” 信学技報、vol. 119, no. 141, SITE2019-43, pp. 317－324, 2019 年 7 月。
17. 森住哲也、“ 論理空間の存在者及び確率測度空間の中の存在者として存在する事 : 身体性の必要条件としての言語ゲーム上の分有ロゴス ”、信学技報、vol. 119, no. 329, SITE2019-86, pp. 41－46, 2019 年 12 月。
18. 紅林宏祐、森住哲也、木下宏揚、“ 2 つの確率モデルの組み合わせによる Multi-Label Learning の解釈について : ラベルを教師データとみなし、評価テクストを解釈するアプローチ ”、信学技報、vol. 119,no. 329, SITE2019-81, pp. 7－12, 2019 年 12 月。
19. Zhaoxiong Meng,Tetsuya Morizumi,Sumiko Miyata,Hirotsugu Kinoshita,\A Scheme of Digital Copyright Management System Based on Blockchain and Digital Watermarking { Research on Improvement Method of Perceptual Hashing based on Machine Learning {", 信学技報 , vol. 119, no. 329, SITE2019-83, pp. 21－27, 2019 年 12 月 .
20. 中谷　憲、孟　昭雄、森住哲也、木下宏揚、“ 畳み込みニューラルネットワークを用いた知覚ハッシュのための中間層の分析 "、信学技報、vol. 119, no. 329, SITE2019-80, pp. 1－6, 2019 年 12 月。

(5)　今後の課題と展望（自己点検・評価）

1　自己点検 · 評価

第三期共同研究では、インターネットエコミュージアムや只見町に開設予定の民俗博物館において必要なデータマイニングやデータの入力や検索に適したユーザインタフェースなどの基盤技術を開発することが目的であった。

知識とサービス、物の流通と価値交換

非文字資料を研究者間および一般ユーザと知識、サービス、資料をやり取りするために、ゲーム理論によりモデル化と解析および、自律分散的に事象や価値の移転を記録するブロックチェーンの技術を用いる計画であった。ブロックチェーンの利用に関しては、所有権の移転を保証するスマートプロパティや契約の履行を保証するスマートコントラクトを応用して著作物としてのコンテンツの流通を管理する手法などを提案できたので、要素技術については概ね目標を達成できた。サービスの流通については具体的な着手はできなかったので次期共同研究で行う予定である。一方、ゲーム理論に基づくモデル化は、ほとんど進展はしなかったので、次期共同研究で引き続き行う予定である。

知識とサービスの検索とマイニング

非文字資料のデータベースや研究者が資料を検索する際に、作業の流れであるコンテキストの一面に着目して情報の類似度などに基づいてユーザに対して最適な情報を提示することを目的としていた。情報検索では、意味解析において有望なトピックモデルを文書中に含まれるテキストと画像の両方に適用し、これを組み合わせることで潜在的データを抽出する手法、木構造のテキスト検索を行う際に非文字用のオントロジーに基づいた語と語の自己相互情報量による関連性の抽出、トピックモデルに基づく文書間の関連性の解析などを行うことができたので概ね目標は達成できた。次期共同研究では、これらを実装した実用レベルの検索システムを構築し、実データでの有効性を検証していく必要がある。サービスの検索については具体的な着手はできなかったので次期共同研究で行う予定である。

個人情報や重要情報、著作権の管理

情報保護や著作権管理にブロックチェーンや確率的な解析を行ったり、ブロックチェーンと組み合わせた新しい電子透かしシステムを応用することを目的とした。個人情報と重要情報の保護に関しては、推論攻撃の防止のために、文書レベルの確率的な関連性のトピックモデルによる解析、推論規則獲得のための Linked Open Data の活用、ブロックチェーンによるアクセス履歴の管理をベースとする推論攻撃の解析やスマートコントラクトを応用したアクセス制御など要素技術の提案を行った。電子透かしについては、ブロックチェーンに基づく電子透かしにより、従来問題となっていた透かし情報のデータサイズの拡張や多重電子透かしの管理の問題を解決し、このシステムに必要不可欠な機械学習に基づく新しい知覚ハッシュを提案した。また、機械学習に基づく新しいファイアウォールの構築法を提案した。よって、目標は達成されたと考えられる。次期共同研究では、これらの成果をさらに発展させていく予定である。

潜在的な text のパターンを AI により健在化し、分類評価する研究 (パターンランゲージの研究)

この研究は、テーマ :「知識とサービスの検索とマイニング」および、テーマ :「個人情報や重要情報、著作権の管理」にとって、それらを概念設計する場合の必要条件としての「理念」を考察することに貢献した。その哲学的理念を示す成果は、技術研究報告という論文で既に発表済みである。具体

的な「パターンランゲージ」は今だ実現するに至っていないが、その設計理念とビジョンは、より具体的な非文字関連の他の上記テーマを考察する形で関わりあうことにより、煮詰まりつつあると言える。

2　第 5 期事業計画

第 4 期の研究成果を踏まえて、「非文字資料の流通過程における諸問題を解決するための機械学習やブロックチェーンなどを応用した基盤技術に関する研究」というテーマで研究を行う。非文字資料研究において研究者と一般の資料提供者が協力して資料の収集整理を行い、その研究成果を社会に発信し還元するためには、「資料の関連性や作業内容に即した検索とマイニング」、資料提供者や研究者の個人情報や重要情報、著作権の管理、資料提供や作業の対価やインセンティブとなる「多様な価値観に基づく地域通貨的価値交換」が必要となる。本研究では、「知識とサービス、物の流通と価値交換」、「知識とサービスの検索とマイニング」、「個人情報や重要情報、著作権の管理」で必要な基盤技術に機械学習とブロックチェーンなどを応用する。具体的にはアクセス制御で必要な資料間の関係性や電子透かしで必要な画像固有の情報の抽出に機械学習を利用したり、流通過程のコンテンツの作成、登録、利用、譲渡、二次利用などの時系列をともなう事象の発生をブロックチェーンを利用して信頼できる第三者を仮定することなく行うことなどが挙げられる。