第 6 班

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

共同研究員名

研究代表者：木下宏揚

共同研究員：能登正人　森住哲也

客員研究員：宮田純子　佐野賢治

研究協力者：小松大介

1　研究目的

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。

2　研究経過

2.1　2020 年度

2.1.1　ブロックチェーンの著作権管理や資料、サービスの流通への応用

ブロックチェーンの基盤技術であるコンセンサスアルゴリズムを計算量に基づく PoW から保有量に基づく PoS に変更することで分散ファイルシステムの IPFS の処理速度を向上させた。

2.1.2　深層学習などの機械学習を用いた効率のいい検索サービスと情報漏洩の検出と防止

情報間の推論による情報漏洩では、推論規則の獲得が重要な課題となる。そこで、文書に含まれる単語の関連性の確率分布を解析することにより推論規則を獲得する手法を提案した。日本語の単語における多義性を解消することによる単語の推論精度の向上のために、大量の一般的な文章からなるコ

ーパス（文章を構造化し大規模に集積したもの）と特定分野に関した少量のコーパスの 2 種類を用いて単語の分散表現である Word2vec を再学習させた。文書に対する権利をアクセス制御モデルの Take-Grant Model により表現し、さらに各文書の情報量に着目し、アクセス権の矛盾による情報漏洩である Covert channel を検出するシステムを提案した。トピックモデルに注目し、LDA 分析によって covert channel を評価し、アクセス権の矛盾を解消する情報フィルタを選択するというモデルを提案した。推論規則生成のために文書のトピックを抽出するために Multi-Label Learning を用い確率的なセキュリティモデルを定義し、潜在的な情報漏洩を顕在化させた。

2.1.3 深層学習の中間層の状態に基づいた新しい知覚ハッシュ関数の構成法

著作権管理にはコンテンツが同一のものかどうか判定する枠組みが不可欠である。視覚的に同一と認識できれば加工編集されていても同一の画像と判定されるメッセージダイジェスト（情報の指紋）を生成する新しい知覚ハッシュの構成法について提案した。機械学習で用いられる畳み込みニューラルネットワーク（CNN）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。対象画像と加工編集画像で転移学習した CNN の中間層を含めてすべてのノードの重み係数の系列の暗号学的ハッシュ値を知覚ハッシュとする方式を提案した。中間層のデータを主成分分析と k-means アルゴリズムでクラスタリングした後、図形の位相構造の特徴量を抽出する手法であるホモロジーによる位相データの情報を取り出し、知覚ハッシュのベースとなる情報の抽出を行った。同一の著作物内の画像を一括して管理できるように、複数の画像を一括して転移学習させることで、複数の画像に対して同一のハッシュ値を生成可能な手法を提案した。また、これを応用して YouTube など加工編集して投稿された動画像に対する知覚ハッシュを提案した。CNN から出力された知覚ハッシュ値をクラス分類に用いる機械学習アルゴリズムの K 近傍法を使用することで著作権管理で必要となる加工編集された類似画像の検索を高い精度で行えるようになった。CNN の重み係数を利用した知覚ハッシュを応用して、加工編集に対して耐性のある電子透かしの構成法を提案した。

2.1.4 民具オントロジーの属性値を考慮した検索システム

民具の登録情報の属性値の見直しを行い、RDF 化する民具カードに新たな属性値として使用時期と使用対象を追加し、それに伴い民具オントロジーを作成し、農耕用具以外の民具でも推論による自動分類が可能な情報検索システムの提案と実験を行った。

2.1.5 言語と身体性について（工学的に善く生きるとは何か）

「非文字」、「情報セキュリティ」、「世阿弥三体」、これらの共通点は「潜在的なテクスト」である。この研究では潜在的なテクストを顕在化するために「演繹推論」に着目してきた。2020 年度は単語間、文書間の演繹推論に於ける必要条件、即ち：「単語、文書の推移律」を人工知能で分析する「確率的情報セキュリティモデル」の設計に的を絞り、七割方成果を得た。

2.2　2021 年度

2.2.1　機械学習とオントロジー、ブロックチェーンを用いた情報検索、著作権管理、サービスの流通

非文字資料に対して情報検索するという工学的テーマの設計のために次の三つのツールを使用した。

⑴　人工知能（機械学習）を適用した：非文字を工学的に扱う「ツール」として、単語の出現確率分布の機械学習評価、単語の共起確率分布の機械学習評価、を導入した。確率分布から非文字への射は潜在的確率変数（潜在的チャネル）である。「非文字資料に於ける潜在的チャネル」はトピックモデル、word2vec によって計算した。

⑵　潜在的チャネルの顕在化のためにオントロジー（概念辞書）を適用した：潜在的チャネルは単語の集合に対して紐付けられるプログラム上の（潜在的確率）変数である。したがって、潜在的チャネルを単語として顕在化しなければならない。今回はその試みとして単語集合と概念辞書を使用して非文字としての概念単語を計算した。

⑶　意思決定支援分析（AHP：Analytic Hierarchy Process）を適用した：潜在的チャネル（非文字）を人間自身がどの様に解釈するか、は「個人的経験が関与する非文字検索」に於いて不可欠である。そこで、潜在的チャネルの価値順位を AHP で評価した。

2.2.2　深層学習などの機械学習を用いた効率のいい検索サービスと情報漏洩の検出と防止

「情報間の推論による情報漏洩の経路を、単語の出現確率分布、或いは単語の共起確率分布で評価する」と定義する。確率分布から情報漏えい経路への射は潜在的確率変数（潜在的チャネル）である、と解釈する。「テクストに於ける潜在的チャネル」はトピックモデル、word2vec によって計算する事にした。一方、この様に定義した「テクストに於ける潜在的チャネル」を人間自身がどの様に解釈するか、という評価は、クラウドを睨んだアクセス制御システムを設計する上で不可欠である。そこで、ユーザがテクストに要求する情報セキュリティの属性（競合、役割、階層、所有、プライバシ）の価値順位を意思決定支援分析（Analytic Hierarchy Process）した。最終的に、「潜在的なチャネル」と「情報セキュリティの価値順位」のバランスを計算するために、強化学習を導入し、ある状態に於けるたまさかな潜在的チャネルをフィルタリングするシステムを確立した。

2.2.3　知覚ハッシュとその応用

- 知覚ハッシュは画像を加工編集しても変化しないメッセージダイジェスト（画像の指紋のようなもの）であり著作権管理の要素技術である。原画像と加工・編集された画像の同一性を証明するために、電子透かしと著作権管理などのセキュリティシステムに適した CNN モデルの重みとバイアスに基づく知覚ハッシュスキームを拡張し同一のコンテンツ内の画像に対して共通の知覚ハッシュ値を生成する方式を提案した。またこれを応用し、同一画像内の複数のオブジェクトを R-CNN を用いて抽出し、同一コンテンツ内の複数画像とみなすことで知覚ハッシュの精度を向上させた。
- CNN による知覚ハッシュの計算量を削減するために、画像分類のために学習した CNN モデルの出力の確率変数を用いた知覚ハッシュスキームを提案した。
- 知覚ハッシュの検証時に必要な CNN モデルの共有データのサイズを削減するために、CNN の

モデル圧縮技術のうち量子化を導入して、データの削減量と知覚ハッシュの精度への影響を検討した。

- CNN の学習過程でクラス分類に寄与した領域を抽出する Grad-Cam で得られる情報を画像の特徴と考えこれに基づいた知覚ハッシュ生成法を提案した。また、入力画像に対する CNN の中間層のレスポンスを VAE で解析し、エンコーダで得られる潜在変数に基づいた知覚ハッシュを提案した。
- AI 技術を用いて作成された Deepfake の検出

  Deepfake はニュースなどの動画を偽造する技術である。AI 技術の一つである深層学習 Contrastive Learning を用いた学習モデルにより、ネットワークで配布するための圧縮加工に耐性のある Deepfake 検出器を提案した。
- 移動体を考慮した 2 種の電子透かし埋め込み切り替え方式

  電子透かしを用いた動画改ざん検出 Macroblock（MB）と呼ばれる処理単位に対して情報を埋め込むことで検出を行う。本研究では、フレーム間で隣り合う MB への改ざんに適した検出手法と単一色で構成されている MB への改ざんに適した手法を移動体の有無によって適切に切り替える手法を提案した。
- M 系列と DCT 領域を用いた相関型ステガノグラフィの強度係数の改善

  ステガノグラフィとは、画像や動画などのマルチメディアデータにデータを隠蔽することによって秘匿通信を実現する技術である。相関型ステガノグラフィにおいて、画質劣化を低減させるべく埋め込みに必要な強度係数を低減するために三種の手法を検討し比較を行った。

2.2.4　言語と身体性について（工学的に善く生きるとは何か）

「潜在的テクストから演繹推論的な決定をする人工知能」を設計するためには、⑴確率的世界、と⑵決定論的世界のたまさかなバランスを取る装置が必要である。そのための必要条件として下記三つの概念装置を結論付けた：

⑴　超越的〈私〉という身体性は「私の意思」として表明された言語として表現される。

⑵　超越論的事実は、決定の空間の現象として現れると同時に、確率空間に於ける事象として現れる。確率空間の事象は人工知能による確率変数の学習、によって計算される。

確率変数の「状態」を、決定プロセスと見做す時、超越的〈私〉と超越論的事実のバランスを取る装置として強化学習が必要である。

2.3　2022 年度

2.3.1　機械学習とオントロジー、ブロックチェーンを用いた情報検索、著作権管理、サービスの流通

- NFT コンテンツの真贋性を保証する PKI の構築

NFT（Non-Fungible Token）が保証する「真正性」は、デジタルコンテンツと結びつけることで、これまで容易ではなかった「クリエイター A が作成した本物のデジタル作品」と証明することを可能にする。本研究では、特にデジタルアートに注目し、ブロックチェーンで普及している Ethereum を活用した非中央集権下でのデジタル署名や NFT コンテンツ発行の制御を行った。これによ

り NFT の発行者が本物の作者であることを保証することができる。

2.3.2 機械学習の検索、情報漏洩防止への応用

• 民俗学資料研究支援のためのトピックモデルによる検索

従来の検索法ではテクストが持つ概念的意味自体が文脈の中に現れる場合の検索（行間を読む）という行為に類似な検索（潜在的テクスト検索と呼ぶ事にする）は不可能である。対応付けが困難な潜在的テクストを確率変数と見做し、潜在的確率変数は潜在的なテクストに対する確率的なカテゴリーであり、トピックモデルが適用される。一方、オントロジーと確率空間の間は互いに随伴関係（ある種の依存関係）にあると定義し、オントロジー側から確率変数を解釈する事により潜在的テクストを表現する。本論文では確率空間側のエントロピー的共起をオントロジーとして関連付けるモデルを提案し、トピックモデルのトピック数の変動によって生じるトピック同士のエントロピーの変化を共起性と定義した場合の妥当性について示した。

• トピックモデルと意思決定を組み込んだ強化学習によるアクセス制御

クラウドに於いて、ユーザが文書やデータをやり取りする上でアクセス制御する必要がある場合、隠れチャネル、或いは推論攻撃により、情報漏えい・情報改ざんが生じる（Latent Channel 問題）。従来の論理学的に latent channel を評価するアプローチでは、文書の内容までは立ち入らないので演繹推論による latent channel が生じる。本研究では、latent channel を論理学的な空間と確率的な空間の随伴関係として捉えるモデルを提案し、強化学習で評価する情報フィルタとして実装した。

• ブロックチェーンに基づくアクセス権の遷移を考慮したアクセス制御モデル

従来の情報漏洩解析は、アクセス制御リストのアクセス権が変化しないことを前提とした静的な解析なので、アクセス権の変更やアクセス履歴は考慮されていない。そこでユーザ（Subject）、ファイル（Object）、アクセス権、遷移のタイミングの関係を記述した Authorization quad を定義し、アクセス権の遷移を考慮して、情報漏洩（Covert channel）を分析することを提案した。また、推論攻撃とアクセス権の遷移を考慮したブロックチェーンによる Covert channel 解析のための管理方式を提案した。

2.3.3 知覚ハッシュとその応用

• CNN に基づく知覚ハッシュの枝刈りによるモデル圧縮

安全で利便性の高いデジタルコンテンツの著作権管理には、画像を識別するメッセージダイジェストが必要不可欠である。流通過程での加工編集を考慮すると通常の暗号学的ハッシュ関数のみでは不十分で、人間の知覚特性を考慮したコンテンツの同一性を判断可能な知覚ハッシュが必要不可欠となる。従来の知覚ハッシュの手法では加工編集に対する耐性が不十分であったが、畳み込みニューラルネットワーク（CNN）の重み係数に基づく知覚ハッシュでは十分な耐性を有している。しかし、生成者側と検証者側との間では学習済みのモデルを共有する必要があり、共有データのサイズ削減が課題となっている。本研究では CNN モデルのモデル圧縮の手法のうち枝刈りに着目して共有データサイズの削減を行い、知覚ハッシュの識別の精度と圧縮率の関係について評価を行った。

• CNN を利用した電子透かしの stirmark による攻撃の加工耐性の検証

SNS 等の普及によりインターネット上でデジタルコンテンツの不正コピーや不正配信などの著作権侵害が問題となっている。これを防ぐため、著作権保護技術として電子透かしが用いられている。電子透かしの最大の問題点は、加工編集などによる透かし情報の耐性が不十分なことである。すべての加工項目に対して耐性のある電子透かしの構成は極めて困難である。本研究では、CNN を利用した知覚ハッシュを応用した電子透かしの構成法において電子透かしの耐性評価法である stirmark に対する透かし情報の耐性の検証を行った。

• 相関型ステガノグラフィにおける JPEG 圧縮耐性の検証

インターネットの進歩により情報保護への感心が高まる中、マルチメディアデータに情報を隠蔽する、情報保護技術のステガノグラフィに関して、多くの提案がされている。既存の相関型ステガノグラフィでは、M 系列での情報符号化と DCT 領域への埋め込みにより秘匿性向上が確認されたが、ステゴ画像の圧縮といった画像加工耐性が未検証で、情報量削減が求められる情報の送受信などの使用時に、正しい情報復元が可能かわからないという問題がある。また、画質の劣化は秘密情報の存在が暴かれやすくなる原因で、秘匿性向上においてはより抑制することが重要である。そこで本研究は、ステゴ画像の圧縮耐性を情報の埋め込み位置や圧縮率を変化させることで検証し、それに伴い生じた劣化について対策を提案した。

2.3.4　言語と身体性について（工学的に善く生きるとは何か）

アクセス制御行列は存在量化子と普遍量化子がない述語論理の形式として捉えることができる。そしてアクセス制御行列内に生じる潜在的チャネルは、ウィトゲンシュタインの「語り得ぬもの」に相当する。ウィトゲンシュタインの言語ゲームは分析対象とするテクストの集まりを家族的類似というクラスターでダイナミックに捉えることができる。したがって、常に変動するクラウドのテクストをアクセス制御するための道具の必要条件として、「存在論とトピックモデル・強化学習の随伴関係」が論理的側面に於いて妥当であることを明らかにした。

2.4　成果の公開

1．Zhaoxiong Meng, Tetsuya Morizumi, Sumiko Miyata, Hirotsugu Kinoshita, An Improved Design Scheme for Perceptual Hashing based on CNN for Digital Watermarking, 2020 IEEE 44th Annual Computers, Software, and Applications Conference（COMPSAC）, pp. 1789–1794, 13–17, July 2020. DOI：10.1109/COMPSAC48688.2020.00048.

2．Zhaoxiong Meng, Tetsuya Morizumi, Sumiko Miyata, Hirotsugu Kinoshita, Design Scheme of Perceptual Hashing based on Output of CNN for Digital Watermarking, 2021 IEEE 45th Annual Computers, Software, and Applications Conference（COMPSAC）, pp. 1345–1350, 12–16 July 2021, DOI：10.1109/COMPSAC51774.2021.00189.

3．大沼海仁、宮田純子、“DCT ブロックに適応的にゲインを乗じる周波数領域利用型ステガノグラフィの検討、”信学技報、vol. 121, no. 119, SITE2021–31, pp. 167–173、2021 年 7 月。

4．KINOSHITA Hirotsugu, MORIZUMI Tetsuya, “An access control model considering with transitions of access rights based on the blockchain,” 2022 IEEE 46th Annual Computers,

Software, and Applications Conference（COMPSAC）, 2022, pp. 1792–1797, doi：10.1109/COMPSAC54236.2022.00285.

5．相川真莉子、宮田純子、木下宏揚、相関型ステガノグラフィにおける JPEG 圧縮耐性の検証、画像符号化シンポジウム PCSJ2022, P2–20、2022 年 10 月。

6．苅谷優太、森住哲也、木下宏揚、トピックモデルと意思決定を組み込んだ強化学習によるアクセス制御、暗号と情報セキュリティシンポジウム、SCIS2023, 4D2–2、2023 年 1 月。

7．小松純也、森住哲也、木下宏揚、民俗学資料研究支援のためのトピックモデルによる検索、信学技報、技術と社会倫理研究会信学技報、vol. 122, no. 433, SITE2022–56, pp. 15–20、2023 年 3 月、Online edition：ISSN 2432–6380。

8．三品翔大、森住哲也、木下宏揚、CNN に基づく知覚ハッシュの枝刈りによるモデル圧縮、信学技報、技術と社会倫理研究会、vol. 122, no. 433, SITE2022–59, pp. 28–34、2023 年 3 月、Online edition：ISSN 2432–6380。

9．相川真莉子、宮田純子、木下宏揚、相関型ステガノグラフィにおける JPEG 圧縮耐性の検証、電子情報通信学会総合大会 NOLTA ソサエティ、N–2–8、2023 年 3 月。

3　研究成果 1：NFT コンテンツの真贋性を保証する PKI の構築

3.1　まえがき

近年、ERC–721 Non-Fungible Token（NFT）を用いた取り組みが増えつつある。NFT が保証する「真正性」は、デジタルコンテンツと結びつけることで、これまで容易ではなかった「クリエイター A が作成した本物のデジタル作品」と証明することを可能にする。NFT の登場はコンテンツや権利の流通革命といわれ、毎日の様にゲームのアイテムやデジタルアート、トレーディングカード、音楽、各種の会員権、ファッションなど、さまざまな領域で急速に新規ビジネスが立ち上がっている現状にある[1]。

NFT が抱える問題点の一つとして、トークンと結びつけられるデジタルコンテンツへの本人性の担保が挙げられる。NFT がコンテンツに対して与えるものは、そのコンテンツがトークン作成者のアドレスと紐づけられている、すなわち「A がコンテンツに唯一無二なトークンを紐づけた」ということを証明するのみである。NFT はコンテンツの真贋に関与しないことから、現状、大手マーケットプレイス「OpenSea」では、NFT の 8 割が贋作であったと発表されているほど、NFT アートの分野では悪意を持った第三者による多くの贋作が流通している。そのため、デジタルコンテンツそのものに限らず、クリエイターの本人性についても保証した上で、NFT コンテンツを流通させていく必要があると考える[2]。

本研究ではデジタルアートに焦点を当て、コンテンツのクリエイターである「本人性」と、NFT がもつコンテンツへの「唯一性、真正性」をそれぞれ保証した上での NFT アートの流通を目指す。先行研究 ETHERST を用いて、本人性の証明の手段としては公開鍵暗号方式からなるデジタル署名を、更に NFT 発行時に信頼されていないアドレスからの NFTmint を行わせない様に制御することで、非中央集権下での安全な NFT コンテンツの流通を実現することを目的とする。

3.2　先行研究

先行研究 ETHERST は、ERC-20 トークンを用いた報酬と罰則によって本人性を保証する研究の一つである。大まかな概要は、図 3.1.1 と図 3.1.2 に示す通りである。自身の身分を証明したいノード A は、名前や識別子など自由な個人の情報を属性 ID として登録し、その属性 ID を引数として署名 ID を作成する。この署名 ID について、各ノードは属性 ID などの情報から Trust、Untrust とい

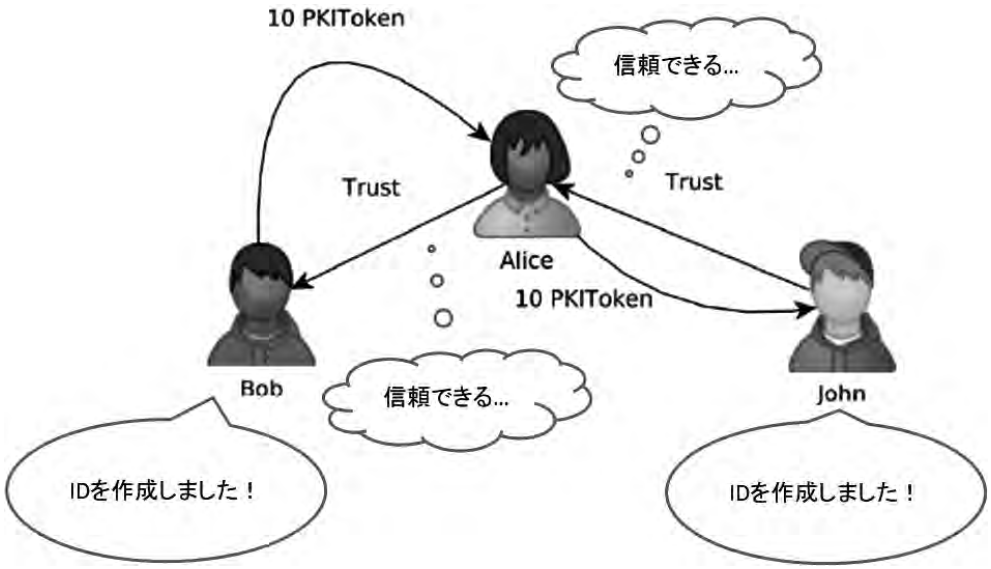


図 3.1.1　Trust 処理の概要

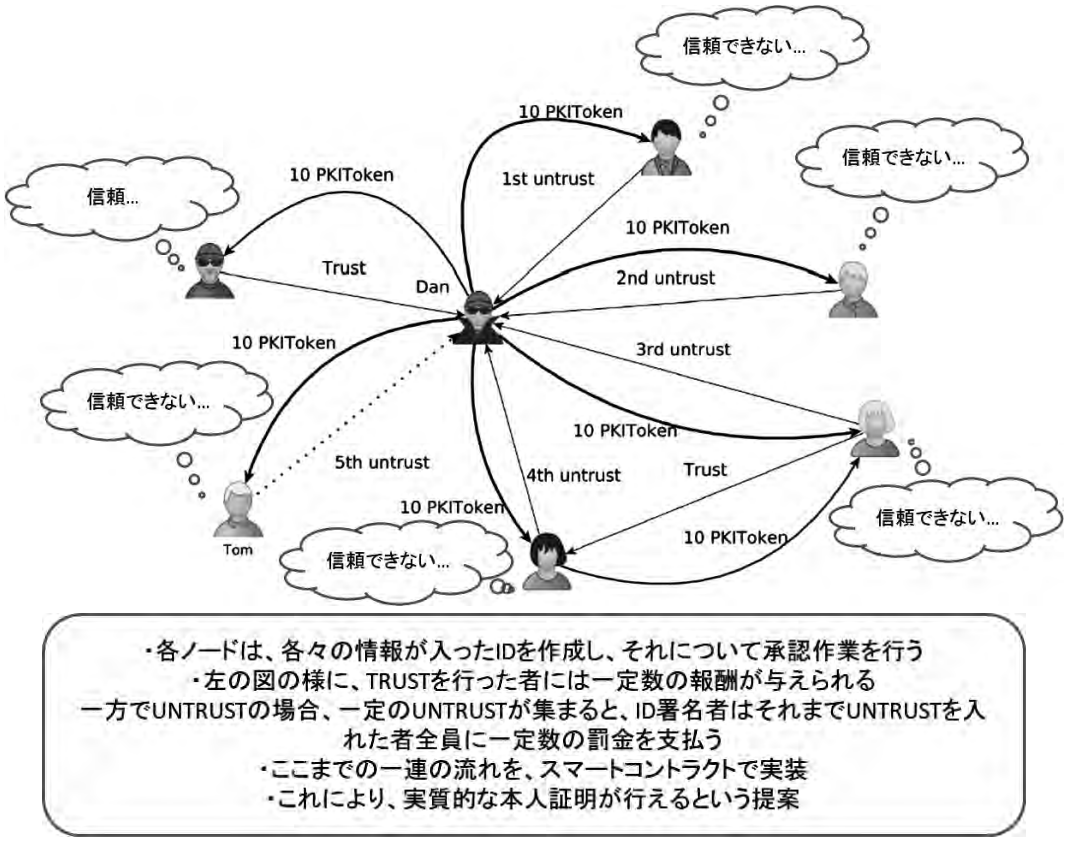


図 3.1.2　Untrust 処理の概要

った承認作業を行う。図 3.1.1 の様に、Trust を得たノードは各ノードに報酬を与える。反対に、Untrust を得てしまった場合、図 3.1.2 に示すように一定数の Untrust 票に達した点で、ノード A は罰として Untrust 票を入れたすべてのノードにトークンの支払いを行う。これにより事実上、非中央集権的に本人証明を行うことが可能になる。この ETHERST の様なシステムを用いることで、アカウントアドレスには信頼されたアドレスと信頼されていないアドレスの二つの要素が付与されるようになる。[3]

3.3 提案手法

3.3.1 コンテンツへのデジタル署名

実験 1 として、クリエイターの本人性を証明するために行うデジタル署名の流れについて説明をする。今回、NFT アートを作成したいクリエイター A は、図 3.2.1 に示す様に、以下の操作を行うものとする。

- A は、自身の NFT 化したいアートからハッシュ値を取得する
- A は、ハッシュに対して自身の Ethereum アカウントからなる秘密鍵で暗号化を行う
- A は、アートを IPFS（NFTstorage）にアップロードする
- A は、アートの URL と、自身の暗号文を metadata に記載し、metadata も IPFS にアップロードする

このデジタル署名によって、まずはアートについて、A が本物のクリエイターであることを保証する。先行研究 ETHERST は、このクリエイター A の持つアドレス（addressA）を保証する。各ノード間で非中央集権的に承認作業を行うことによって、このアドレス A についても、従来のデジタル署名とは異なり、認証局（Certificate Authority：CA）を持たない状態にすることが出来る。これ

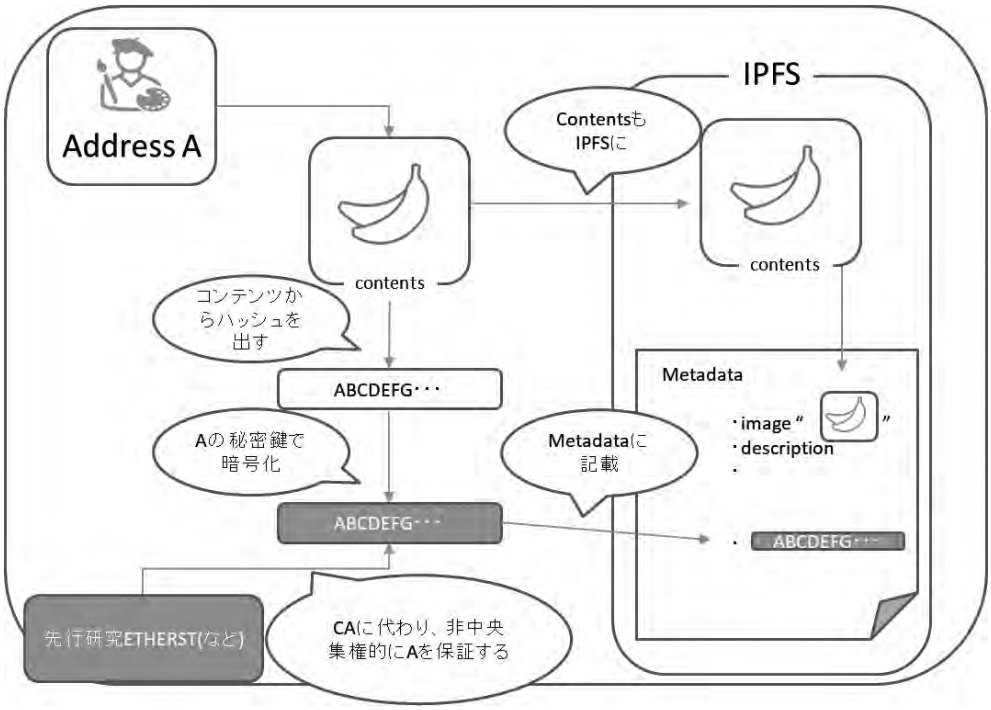


図 3.2.1　非中央集権下での PKI の概要

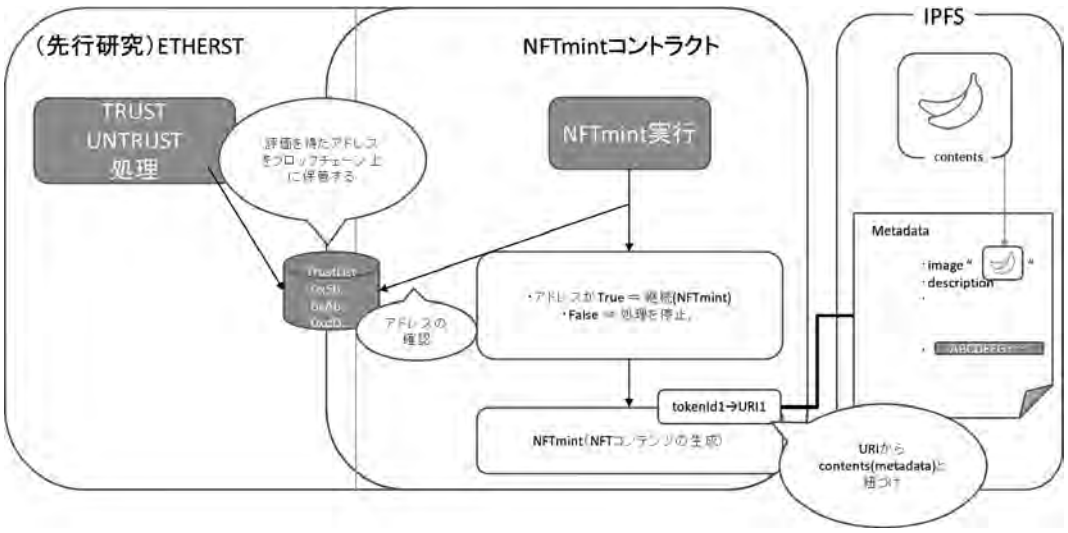


図 3.2.2　NFTmint スマートコントラクトの概要

により、非中央集権的にデジタル署名を行うことを目的とする。本研究では、時間の都合上 Pure-Python ecdsa を用いて簡易的な署名を行う。

3.3.2　NFTmint スマートコントラクトによる mint の制御

次に実験 2 として、NFTmint スマートコントラクトについて概要を説明する。本研究では、クリエイターの本人性の保証のみではなく、その後のコンテンツの流通についても、ETHERST を一つの例として考える。実験は従来の NFT アートを作成する手順の一つである独自コントラクトを作成し、それに追記していく形で行う。図 3.2.2 に示す様に、以下動作を行う。

クリエイター A（addressA）は、NFTmint スマートコントラクトから NFTmint 関数を実行する

- スマートコントラクトは、コントラクト内で Trust List を参照する
- 参照時、関数実行者（ここでは AddressA）がリストに存在するか、存在する場合その状態は「True」であるかを確認する
- 「True」の場合、処理を継続し、トークンと紐づけられた NFT アートを生成する
- 「False」の場合、処理を中断する

3.3.3　テストネットを使用した NFT アートの公開

最後に実験 3 として、実験 2 と実験 3 によって本人性と真正性が担保できるものとし、MetaMask から Ethereum テストネットワークへの接続を行い、OpenSea テストネットへの NFT アートの公開を試みる。

3.4　実験

3.4.1　環境構築

実装環境と各バージョンを以下に示す。

OS：Windows 10 Home、プロセッサ：Intel（R）Core（TM）i7-7700K CPU@4.20 GHz 4.20 GHz、GPU：NVIDIA GeForce GTX 1070、Solidity：0.8.14、Python：3.9

3.4.2 実験 1 の環境設定

本実験では、時間の都合上 Pure-Python ECDSA を用いて署名検証を行うため、Jupyter Notebook を用いて実験を行う。多量の計測をする必要はないため、自身の環境に Anaconda をインストールし、その後 Jupyter Notebook を起動し実験を行っていく。

3.4.3 実験 2-Remix の設定

実験 2 では、Rimix IDE を用いて実験を行う。Remix IDE のウェブページにアクセスをし、今回用意したコントラクトコード「NFTmint.sol」をインポートする。本研究での Solidity および OpenZeppelin のバージョンは 0.8.14 で行う。コードを記述した後、左側のメニューバーから「SOLIDITY COMPILER」へ移動し、バージョンを 0.8.14 に指定して「Compile」ボタンを押す。コンパイルに成功するとメニューバーにチェックが入るため、「DEPLOY & RUN TRUNSACTIONS」から「Remix VM（London）」とアカウントの選択をし、「Deploy」ボタンからデプロイをし、実験を行っていく。

3.4.4 実験 2 コンテンツの準備

実験 2 では、実際にデジタルアートを用意し、そのアートのメタデータをスマートコントラクトで紐づけることで、NFT アートを作成していく。本研究で使用するイラストは図 3.3.1 である。

図 3.3.1 実験で使用するイラスト

まず、NFTStorage に今回使用するイラストをアップロードする。NFTStorage のサイトへアクセスし、アカウントの作成もしくはログインを行う。その後、「＋Up-load」からイラストをアップロードする。次に、アップロードされたファイルの「Actions」から、「Copy IPFS URL」を選択する。
次に、メタデータの準備を行う。今回作成するメタデータは、OpenSea へ公開することを考え、「name」「image」「description」「attributes」の四つから構成される Json 形式を用意する。そのメタデータ内に、実験 1 で得られた署名暗号文を追記し、再度 NFTStorage へアクセス、Json ファイルのアップロードを行う。

3.4.5 実験 3 の環境設定

実験 3 では、実際に MetaMask を用いたテストネットワークへの接続、および OpenSea テストネットでの NFT アートの公開を行う。その為の準備を以下に記していく。まず初めに、MetaMask アカウントを作成する。Chrome の場合、Chrome ウェブストアから拡張機能に追加を行う。追加後、拡張機能から狐のマークの MetaMask を起動し、指示に従ってアカウントを作成する。アカウント

作成後、上の方にある「イーサリアムメインネット」を選択し、「Goerli テストネットワーク」に変更を行う。次に、Remix の設定を行う。「DEPLOY ＆ RUN TRUNSACTIONS」の「ENVIRONMENT」を「Injected Provider - MetaMask」に変更し、MetaMask との接続を行う。最後に、OpenSea の設定を行う。OpenSea テストネットへアクセスし、右上のアイコンのところから MetaMask との接続を行う。これにより、共有コントラクトを使用する場合は、Gas 代の消費を考えることなく、自由に NFT アートを作成することができるようになる。本研究では、独自コントラクトを用いて NFT アートの Mint および公開を行っていく関係上、Gas 代が発生する。その為、あらかじめ Goerli Faucet と呼ばれるサイトでテスト用のイーサリアムを取得しておく。

Goerli Fauset：https://goerlifaucet.com/

3.4.6 スマートコントラクトの詳細

スマートコントラクト「NFTmint」について説明する。このコントラクトは基本的に OpenZeppelin ライブラリを用いた NFTmint を行うスマートコントラクトである。そのコントラクト内に、Require 文によって関数の制御を行える様にした。OpenZeppelin から使用したライブラリの中で、特に本研究で使用するものは以下に示す通りである。

- ERC721.sol　ERC721（NFT）の基本ライブラリ
- Ownable.sol　コントラクトをデプロイしたアドレスのみが実行出来る関数を作成できるようにする
- URIStorage.sol　ERC721 と URI を関連づける。
- Burnable.sol　ERC721（NFT）を削除。また、コントラクト内で使用する関数について以下に示す
- NFTmint　NFT アートを作成するメインとなる関数。ERC721 とコントラクト内で示した URI とを紐づける
- burn　作成した NFT を削除する
- checkverify　true, false を割り振ったアカウントアドレスを登録する

3.4.7 実験 1 デジタル署名の実験

まずはクリエイター本人であることを証明するためのデジタル署名の実験を行う。本実験では時間の都合上、Ethereum アドレスに代わり、Pure-Python ECDSA と呼ばれるものを用いる。署名用の鍵（秘密鍵）生成、証明用の鍵（公開鍵）生成、楕円曲線 SECP256k1 をパラメータ指定するためのパッケージをインポートし、用意したアートのハッシュへ署名を行うこととする。実際に今回生成した鍵とハッシュは以下の通りである。ハッシュは SHA256 で算出している。

- 秘密鍵

  ”2135b5d81ff01f2820ec1656f3ac2c5bb509ec6500b3bac306bf3f33121b329d”
- 公開鍵

  ”3ae74f98a783b9a5a279a50dc2a5eba37c53530d30acbfd205928a66a5f8dd82
  0520cf6ada9826efe3edd4022363dcfa9fc3662cbb992efa31f96b8a94f59f0e”

- イラストのハッシュ値

"d29438953bbd77a1bcab3495cbf4908c81c8089418a1dd5a8e52de849e2fec2f"

3.4.8 出力結果

生成された秘密鍵から署名を行った結果は図 3.3.2 の通りである。

```
deta = "d29438953bbd77a1bcab3495cbf4908c81c8089418a1dd5a8e52de849e2fec2f"
signature = secret_key.sign(deta_bytes)
print(signature)
```

```
b'¥xc3¥xb9¥x91¥xa4 ¥xa8¥xe8¥xf2¥x11¥xa3¥xa4¥xaa¥xe6¥xf5Z¥x91N¥xcb¥xa5¥xfc¥xcb¥xbca¥x
9d¥x9b,¥xcdEzg¥x9c¥x1d¥t¥x0b¥x13j¥xabv¥xd0.¥xcbt¥xbb¥xd6s¥xf0k¥x0eM¥xb2¥xdeU¥xc16c¥x
a5¥xe1>¥x0b¥xba[¥x13¥xe75'
```

図 3.3.2 署名結果（バイト形式）

結果はバイト形式で出力されているが、実験 2 でメタデータに記載する際のことを考え、次の様に 16 進数に変換する。

```
signatire_str = signature.hex()
signature = binascii.unhexlify(signatire_str)
print(signatire_str)
```

```
7c4ecee2ae393454bb1b95564ee63ebc290b276bd51f47611c5b870b85a14efaf453f3ef59a9979d5a5e
bb2e7cb228c2ff7f41d92ed579a447d5b83e4448b58d
```

図 3.3.3 署名結果（16 進数形式）

図 3.3.4 と図 3.3.5 では、公開鍵を用いて署名の検証を行っている。

```
public_key.verify(signature, deta_bytes)
```

```
True
```

図 3.3.4 検証結果

図 3.3.4 では公開鍵によって復号、そしてその復号値が元データのハッシュ値と正しいことを確認できる。図 3.3.5 では、元ハッシュ値の冒頭「d29」の 3 文字目を 9 から 8 に一文字変えた際の状態であり、正しくその改ざんを検知している。

3.4.9 実験 2 NFTmint の実験

次に、NFTmint スマートコントラクト内で、アドレスの制御を行っていく。今回、Remix であらかじめ用意されているアカウントのうち、三つのアカウントにそれぞれ ETHERST によって承認処理が行われたとして準備を行っていく。本コントラクトでは、Gas 代の消費が大きくないため、リストについてはハードコーディングしている。本実験では、以下のアカウントを使用する。

アカウント 1：0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

アカウント 2：0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2

アカウント 3：0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2

アカウント 1 の属性："True"

```
changed_deta = "d28438953bbd77a1bcab3495cbf4908c81c8089418a1dd5a8e52de849e2fec2f"
changed_deta_bytes = bytes(changed_deta, encoding = "utf-8")
public_key.verify(signature, changed_deta_bytes)
```

```
---------------------------------------------------------------------------
BadSignatureError                         Traceback (most recent call last)
~¥AppData¥Local¥Temp¥ipykernel_5444¥776398569.py in <module>
      1 changed_deta = "d28438953bbd77a1bcab3495cbf4908c81c8089418a1dd5a8e52de849e
2fec2f"
      2 changed_deta_bytes = bytes(changed_deta, encoding = "utf-8")
----> 3 public_key.verify(signature, changed_deta_bytes)

~¥anaconda3¥lib¥site-packages¥ecdsa¥keys.py in verify(self, signature, data, hash
func, sigdecode, allow_truncate)
    671         hashfunc = hashfunc or self.default_hashfunc
    672         digest = hashfunc(data).digest()
--> 673         return self.verify_digest(signature, digest, sigdecode, allow_trunc
ate)
    674
    675     def verify_digest(

~¥anaconda3¥lib¥site-packages¥ecdsa¥keys.py in verify_digest(self, signature, dige
st, sigdecode, allow_truncate)
    727         if self.pubkey.verifies(number, sig):
    728             return True
--> 729         raise BadSignatureError("Signature verification failed")
    730
    731

BadSignatureError: Signature verification failed
```

図 3.3.5　改ざんの検知

アカウント 2 の属性："False"

アカウント 3 の属性："True"

3.4.10　出力結果

checkverify 関数によってアドレスの状態を登録後、NFTmint 関数を実行した結果はそれぞれ次の様になった。OpenZeppelin により、NFTmint 関数はコントラクトをデプロイしたアドレスにのみ実行可能なため、各アカウントでそれぞれデプロイ、登録、関数の実行を行った。

3.4.11　アカウント 1 の実行結果

アカウント 1 は ETHERST によって承認がされたと仮定したアドレスである。出力結果は、NFT-mint の処理が継続され、メタデータとの紐づけが行われていることを表している。

図 3.3.6　アカウント 1 の実行結果

3.4.12　アカウント 2 の実行結果

図 3.3.7　アカウント 2 の実行結果

アカウント 2 は ETHERST によって承認が行われていないと仮定したアドレスである。出力結果は、処理が途中で中断されており、「This address is not trusted」と、true ではないときに出力する様に用意したエラー文が出力されており、NFT とメタデータの紐づけが行われていないことも確認できる。

3.4.13　アカウント 3 の実行結果

図 3.3.8　アカウント 3 の実行結果

アカウント 1 は ETHERST によって承認がされたと仮定したアドレスである。出力結果は、NFT-mint の処理が継続され、メタデータとの紐づけが行われていることを表している。

3.4.14　実験 3 NFT アートの公開

実験 3 の準備は実験 2 と手順は同様であるが、MetaMask のウォレットを使用するため、

ETHERST によって信頼されたと仮定するアドレスを以下の様に変更する。また、Gas 代消費の点から、今回はアカウントを二つで行う。

アカウント 1：0x969b09c0DeC536943e720D57094c0CCCe417aF14

アカウント 2：0x99FA68D0bEB51Ab362822Cba5761D7AFcEA51dc8

アカウント 1 の属性："True"

アカウント 2 の属性："False"

3.4.15　出力結果

checkverify 関数によってアドレスの状態を登録後、NFTmint 関数を実行した結果はそれぞれ次の様になった。OpenZeppelin により、NFTmint 関数はコントラクトをデプロイしたアドレスにのみ実行可能なため、各アカウントでそれぞれデプロイ、登録、関数の実行を行った。

3.4.16　アカウント 1 の実行結果


```
{
        "from": "0x7653d37806eDE84Daa2d921bCA367ef4766E495e",
        "topic": "0x8b781fcc9d1a958b4e7e04390a81f45bdec2dc61341e7b423a537074275dc70d",
        "event": "TokenURIChanged",
        "args": {
                "0": "0x969b09c0DeC536943e720D57094c0CCCe417aF14",
                "1": "1",
                "2": "metadatastarMeta1.json",
                "sender": "0x969b09c0DeC536943e720D57094c0CCCe417aF14",
                "tokenId": "1",
                "uri": "metadatastarMeta1.json"
        }
}
```


図 3.3.9　アカウント 1 の実行結果

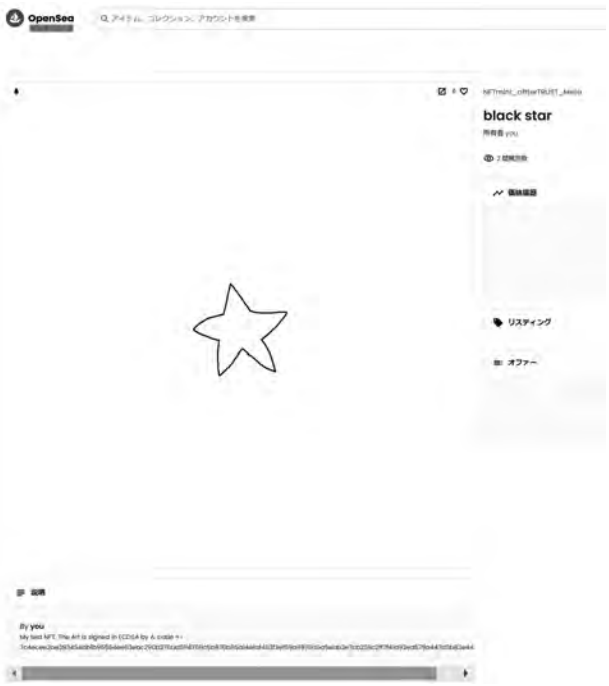


図 3.3.10　OpenSea テストネットでの NFT アートの表示

アカウント 1 は ETHERST によって承認がされたと仮定したアドレスである。出力結果は、NFT-mint の処理が継続され、メタデータとの紐づけが行われていることを表している。また、OpenSea テストネットで確認してみると、実際に NFT アートの公開が出来ていることも確認できる。説明欄には metadata 内に記載した署名暗号文が表示されており、各ユーザはクリエイターの公開鍵を用いて本人性の検証を行うことが可能となっている。

3.4.17　アカウント 2 の実行結果

アカウント 2 は ETHERST によって承認が行われていないと仮定したアドレスである。出力結果は、図 3.3.11 の様に、「Gas estimatin failed」という形で動作を停止した。エラーメッセージとして実験 2 のアドレス 2 同様の出力がされているため、信頼されていないアドレスとして関数の実行を停止していることが確認できる。

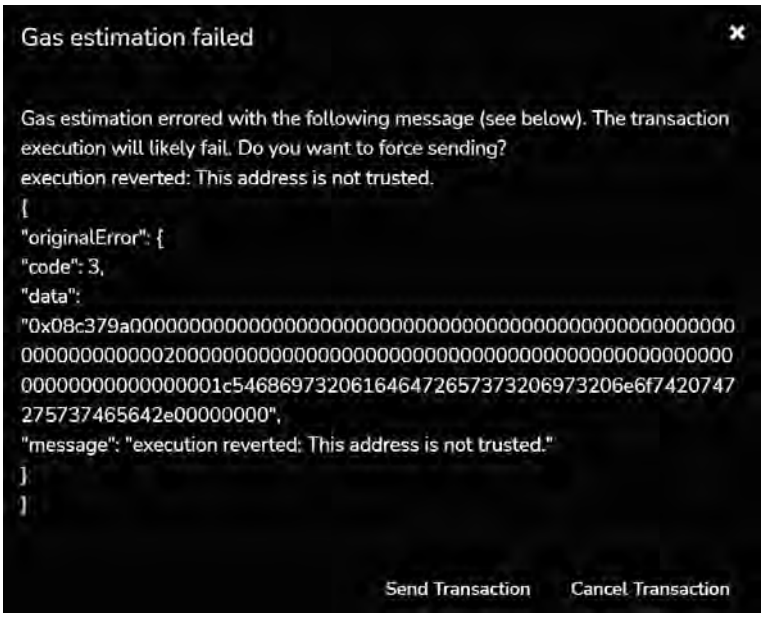


図 3.3.11　アカウント 2 の実行結果

3.5　考察

実験 1 では、Ethereum アカウントからなる秘密鍵の代わりとして、Python で簡易的な署名検証作業を行った。結果的にはアートから得られたハッシュ値を暗号化し、それを公開鍵で復号することに成功しており、改ざんの検知にも成功している。この鍵について、今現在使われている Ethereum アカウントの秘密鍵および公開鍵を用いれば、その鍵の所有者の証明は認証局 CA に代わり、ETHERST の様なシステムによって保証されるため、非中央集権下でのデジタル署名を実現できるのではないかと考える。実験 2 と 3 では、NFTmint スマートコントラクトから、NFT の mint を行い、処理中にリストを参照することで、信頼されていないアカウントによる NFT アートの作成を阻止することが出来た。また、実験 3 では実験 1 で生成した暗号文をメタデータに記載することで、どのユーザにもクリエイターの公開鍵があればその NFT アートが本当に本人によって作成されたものなのかを確認することができるようになった。ただし、今回の流れでアドレスをリストに登録してい

く場合、そこにかかるGas代の量も膨大な量を必要としてしまうため、このリスト化するという手段について、更に良い方法を検討していく必要がある。すべての実験を通して、ETHERSTの様な認証局CAを排除したアカウントの承認システムを用いることで、本研究では完全に非中央集権下での本人性、そして真正性、唯一性の担保が行えたのではないかと考える。

3.6 結論

本研究では、NFTアートを一例として、まず初めにデジタルアートへの署名を、次に署名済みデータを用いたNFTアート発行の制御を行い、最後に実際のテストネット環境での実装を行ってきた。これらの結果から、当初目的としていた、クリエイター本人であることの証明をしながらも、NFTの強みであるコンテンツへの「真正性、唯一性」を持つNFTアートの流通が行うことができると考える。本研究の根底にはETHERSTの様な認証システムが深く関係しており、これによって認証局を排除した完全な非中央集権下でのデジタル署名やNFTアートの制御、および流通を実現することが出来た。

今後の課題として、実際にEthereumアドレスを用いての署名や、Gas消費を抑えられる効率の良いスマートコントラクトの構築について考える必要がある。更には、ERC735と呼ばれる分散型IDを用いたスマートコントラクトの作成についても、一つの選択肢として検討を行う必要がある。

参考文献

［1］ 天羽健介、増田雅史、“NFTの教科書ビジネス・ブロックチェーン・法律・会計までデジタルデータが資産になる未来”、朝日新聞出版、2021。

［2］ OpenSea, Jan. 28. 2022、https://twitter.com/opensea/status/1486843204062236676、参照：Jan. 23, 2023.

［3］ Chong-Gee Koa, Swee-Huay Heng、Ji-Jian Chin, ETHERST Ethereum-Based Public Key Infrastructure Identity Management with a Reward-and-Punishment Mechanism, Symmetry 2021, 13, 1640。

4 研究成果2：CNNを利用した電子透かしのstirmarkによる攻撃の加工耐性の検証

4.1 まえがき

近年、ネットワーク上のデジタルコンテンツの流通の普及により、誰もが簡単にSNS上で画像、動画、音楽、映画、本などのデジタルコンテンツを利用できたり、自身が作成したデジタルコンテンツをSNS上に発信することができるようになってきている。しかし違法なコンテンツをダウンロードしてしまうことや、著作権保護のかかったデジタルコンテンツを無断で編集してSNS上に発信することが問題となっている。このような著作権問題を保護するような対策として電子透かしという技術がある。電子透かし技術は人の視覚では判断できないように電子透かしを埋め込みコンテンツを保護する技術である。しかし一般的な電子透かしでは透かし情報がコピーされて他のコンテンツに流用される可能性がある。また、二次利用により多重に埋め込まれた電子透かしの優先順位や加工内容との対応関係を明確にできないという問題点がある[1]。これらを解決するために信頼できる第三者が透かし情報あるいはコンテンツのメタ情報などを管理する方法が考えられるがコストやプライバシー保

護、セキュリティ、サービスの継続性の担保などの観点から望ましくない。さらに電子透かしの構成で考慮すべき点として、加工、符号化、攻撃に対して、透かし情報を検出し著作権情報を確認できること、必要な情報量を埋め込み可能なこと等が挙げられるが、透かし情報の埋め込み手法、検出および認証方法、符号化、加工、攻撃に対する耐性などについて改善の余地がある[2]。そのため透かし情報は、セキュリティ上の必要性から画像に固有の情報に基づいて生成される必要がある。情報の指紋であるメッセージダイジェスト（ハッシュ値）は、セキュリティシステムの様々な場面で利用される要素技術である。暗号学的ハッシュ値を用いた手法では加工編集などによりハッシュ値が大幅に変化するため加工編集には対応できないため著作権を保護するのに適していない。一方で、知覚ハッシュでは加工、編集、非可逆符号化などを行っても人間が同じ画像と判断できる画像に対しては原画像と同様のハッシュ値を得られるため著作権管理に適している[3]。先行研究[4]ではCNNを利用した知覚ハッシュを応用して新しい電子透かしの構成法を提案していた。どう応用していたかというと知覚ハッシュでは対象画像を受理とラベル付けするように学習、無関係画像だと棄却とラベル付けするように学習し出力されていたが、先行研究ではこの受理と棄却の部分がビット列を出力するようにラベル付けしてその出力が電子透かし情報の埋め込みとみなしていた。しかしプログラムのアルゴリズムに問題があり、1か0の1ビットしか出力せず本来やりたかった複数のビットが出力するようにはなっていなかった。本研究では、CNNを利用した知覚ハッシュを応用した新しい電子透かしの構成法において新しいfine-tuningの適応法を提案し、電子透かしの耐性の評価法であるstirmarkの攻撃を行った場合の透かし情報の耐性について検証を行い、本研究のCNNを利用した新しい電子透かしの構成法が加工に対して優れた耐性があるということを示す。

4.2 stirmark

stirmarkとは、電子透かしの耐性検証ツールとして広く用いられているものである。画像に対してJPEG圧縮、ノイズ付加、メディアンフィルタリングなどの非幾何学的改変を複合的、かつランダムに施すことができるツールである[5]。本研究で使用するstirmarkの攻撃とパラメータを説明する。stirmarkの攻撃の例を以下に示す。

- Affine：画像の拡大縮小、回転、平行移動などを行列を使って座標を変換する。実験では以下のパラメータを使用する。

$$\begin{vmatrix} x' \\ y' \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \begin{vmatrix} x \\ y \end{vmatrix} + \begin{vmatrix} e \\ d \end{vmatrix}$$

mat = a, b, d　　c, d, e

mat1 = 1, 0, 0　　0.01, 1, 0

- Conv：正方形のカーネル（またはフィルタと呼ぶ）を用いた「スライディングウィンドウ処理」を通して、入力画像の各参照画素（x, y）の近傍において「カーネル値と参照画素値による、局所的な畳み込み演算（積和）」を行う。これにより、カーネルの値に沿って入力画像を変換する処理である。実験では以下の二つのフィルタを使用する。
- Noise：画像のざらつき。実験ではノイズの強さを20に設定している。
- Jpeg：非可逆圧縮という、人間の目では見えない視覚情報を取り除き、色の変化を平均化する

1	2	1
2	4	2
1	2	1

Conv1

0	−1	0
−1	−5	−1
0	1	0

Conv2

品質パラメータを数値 1〜100 で指定できる。値が小さいほど低画品質つまり画像は劣化する。実験ではパラメータを 15 に設定している。

- Rotation：画像の回転。実験では 90 度回転させている。
- Cropping：切り取り。実験では中心の 10% の切り取りと 50% の切り取りを行っている。
- Median：周辺画素値の大小比較を行って中央値の画素に変換するフィルタ処理。実験では 3×3 のフィルタで行っている。

4.3 提案方法

4.3.1 提案方法の概要

電子透かしの埋め込み、抽出の流れを下の図に示す。

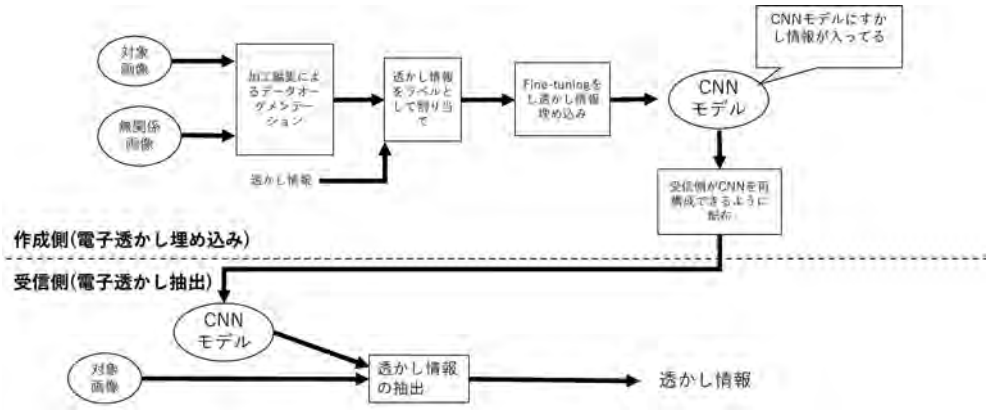


図 4.1　提案方式の概要

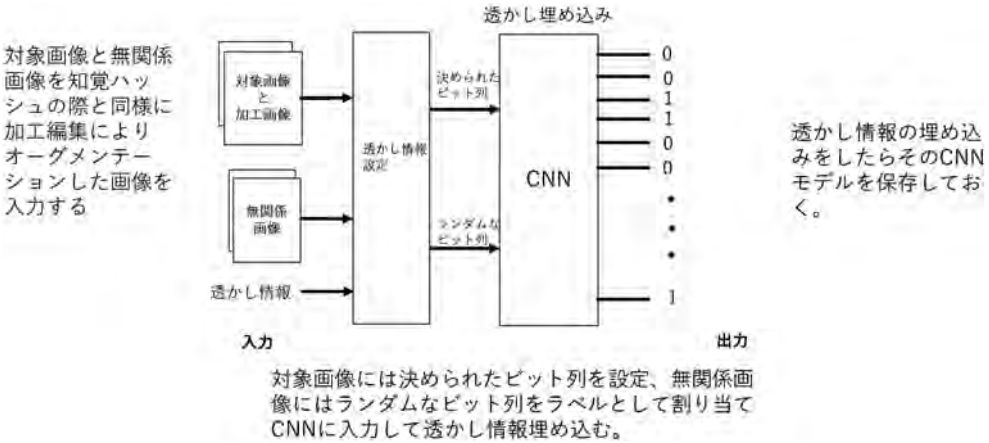


図 4.2　電子透かしの埋め込み法

4.3.2 作成側（電子透かしの埋め込み）

電子透かしを埋め込みたい画像と無関係な画像を用意する。様々な加工編集に対応させるために、想定される符号化、回転、フィルタリングなどの加工編集をパラメータを様々に変更して、データオーグメンテーションを行って画像を水増しする。次に電子透かしを埋め込みたい対象画像は決められたビット列、無関係画像にはランダムなビット列を埋め込むようにラベルを割り当て fine-tuning を行い CNN モデルを作成する。学習済み CNN モデルを可逆圧縮し受信者側に配布する。

4.3.3 受信側（透かし情報の抽出）

作成側から配布された CNN モデルを入手する。次に入手した CNN モデルを再構成し検証したい画像を CNN モデルに入力すると埋め込んだ透かし情報のビット列が抽出されるか調べる。

4.4 実験と考察

4.4.1 実験環境

実装環境と各ソフトウェアのバージョンは Python：3.7.3、CUDA：10.2、Keras：2.3.1、Tensor-Flow-GPU：2.2.0 を用いた。

4.4.2 実験 1 電子透かしの埋め込み

• 画像の生成（augmentation）

図 4.3 に lena、japan、cherries の原画像を示す。また augmentation した画像を図 4.4 に示す。lena、cherries、japan の電子透かしを埋め込みたい画像と 10 種類の無関係画像を用意し、それぞれ augmentation する。augmentation を行った画像は、training 用と test 用で分けてそれぞれ使用する。training のフォルダは画像特徴学習用で、test のフォルダは画像分類予測用である。また対象画像とする lena、cherries、japan の augmentation した画像は、training に 16000 枚、test に 4000 枚それぞれ生成してフォルダにまとめる。10 種類の無関係画像を augmentation した画像は、training に 16000 枚、test に 4000 枚としてまとめる。

図 4.3 lena、cherries、japan の原画像

• 透かしの埋め込み（fine-tuning）

augmentation で生成された training 用と test 用の画像を使用して Fine-Tuning を行う。このとき図 4.5 のように、lena の画像に対してはビット列 0101010101 を埋め込むようにラベルを割り当て、cherries の画像に対してはビット列 1111100000 を埋め込むようにラベルを割り当て、japan の画像に対してはビット列 0000011111 を割り当てる。また無関係画像はランダムなビット列を埋め込むよう

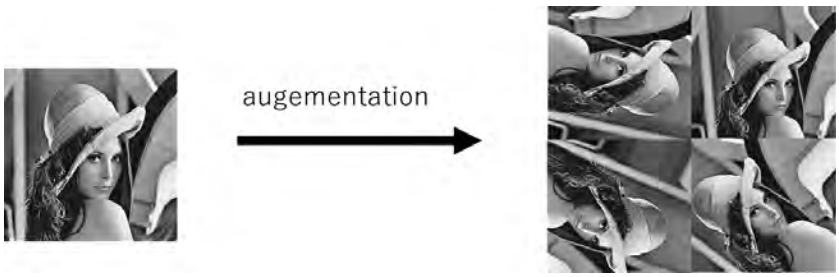


図 4.4　augmentation で加工した画像

にラベルを割り当てる。

Fine-Tuning の精度を図 4.6 に示し、Fine-Tuning の結果から学習済みの CNN モデルの構造 json ファイルと重み h5 ファイルが生成される。

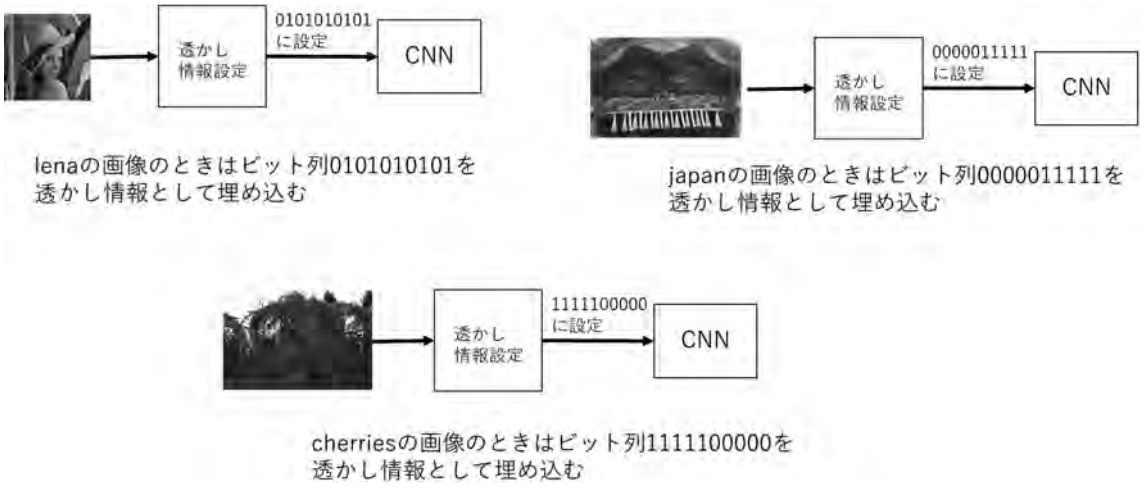


図 4.5　ビット列の割り当て

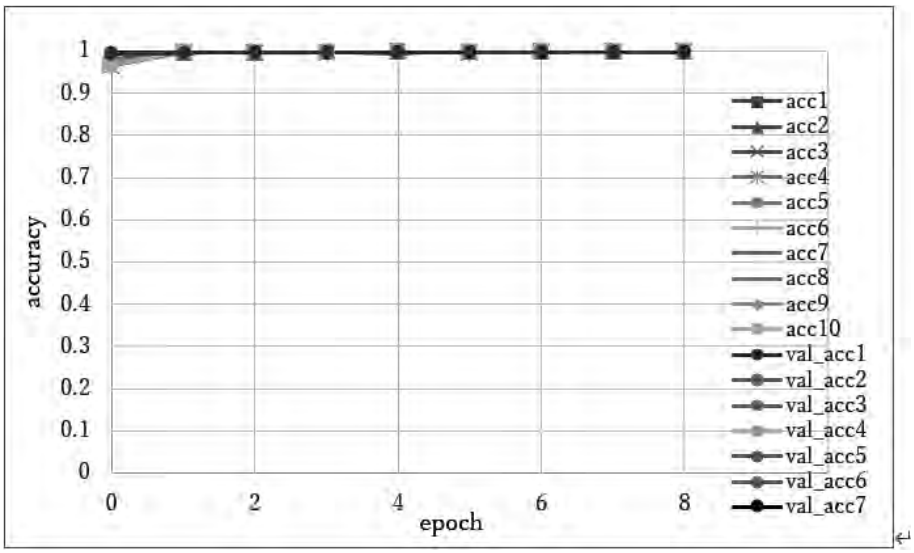


図 4.6　実験 1 の fine-tuning の精度

4.4.3　実験 1 透かし情報の抽出

Stirmark による攻撃を行った lena、japan、cherries の画像を図 4.7、図 4.8、図 4.9 に示す。ここ

図 4.7　Stirmark による攻撃を行った lena の画像

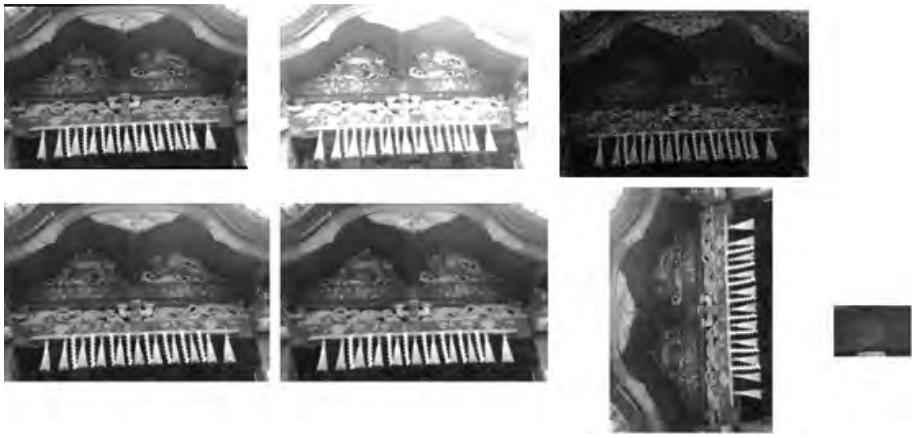


図 4.8　Stirmark による攻撃を行った japan の画像

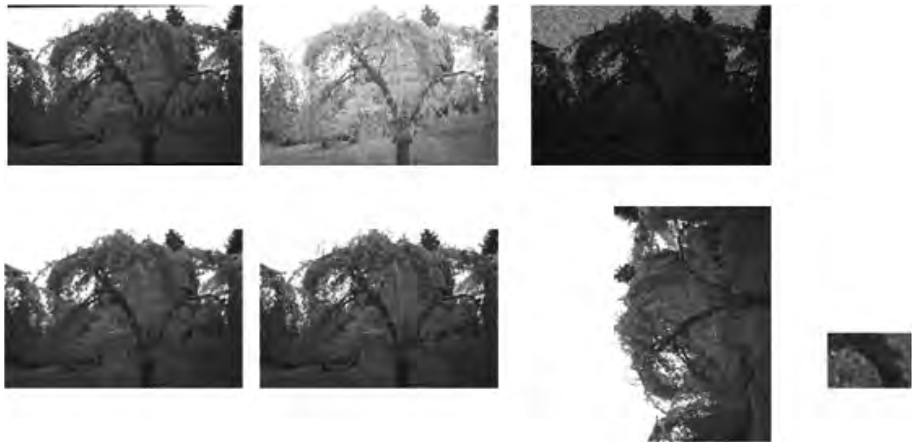


図 4.9　Stirmark による攻撃を行った cherries の画像

では、AFFINE、CONV、NOISE、JPEG、MEDIAN、ROT、CROP の攻撃に対する出力を検証する。

4.4.4　実験 2-電子透かし埋め込み

実験 2 では実験 1 の加工方法に CROP10、CROP50、CONV2 により加工した画像を加えたもので augmentation する。以下実験 1 と手順は同じである。図 4.10 に実験 2 の fine-tuning の精度を示す。

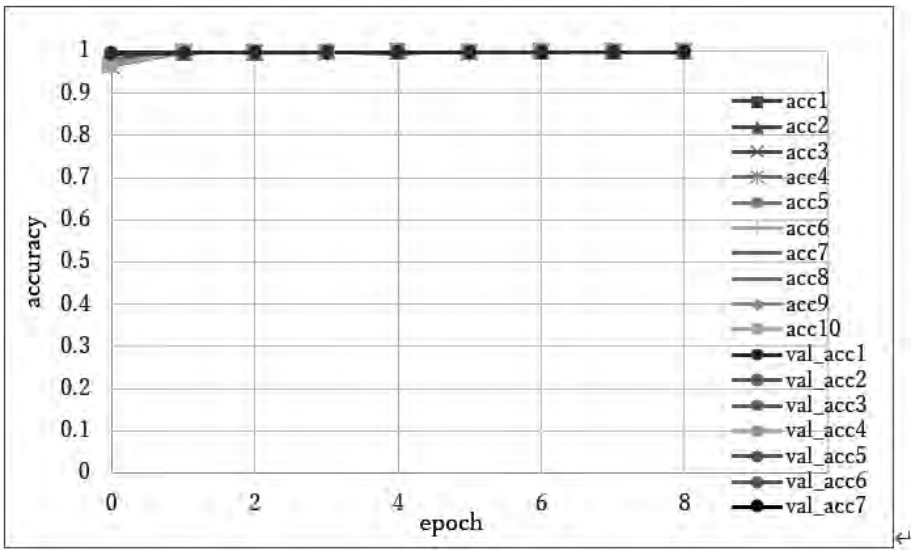


図 4.10　実験 2 の fine-tuning の精度

4.4.5　実験 2 透かし情報の抽出

実験 1 と同様に、AFFINE、CONV、NOISE、JPEG、MEDIAN、ROT、CROP の攻撃に対する出力を検証する。

4.4.6　実験結果

実験 1 と実験 2 の対象画像 lena、japan、cherries に対するビット列は、0101010101、0000011111、1111100000 を透かし情報とした場合の抽出結果を表 4.1 と表 4.2 に示す。抽出できたものは○、抽出できなかったものは×で示している。

表 4.1　実験 1 の透かし情報抽出した結果

	AFFINE	ROT	NOISE	CROP10	CROP50	CONV1	CONV2	MEDIAN	JPEG
lena	○	○	○	×	○	○	×	○	○
japan	○	○	○	×	×	○	×	○	○
cherries	○	○	○	×	○	○	×	○	○

表 4.2　実験 2 の透かし情報抽出した結果

	AFFINE	ROT	NOISE	CROP10	CROP50	CONV1	CONV2	MEDIAN	JPEG
lena	○	○	○	○	○	○	○	○	○
japan	○	○	○	○	○	○	○	○	○
cherries	○	○	○	○	○	○	○	○	○

4.5 考察

表 4.1 より、実験 1 では stirmark の攻撃を行った画像に対して、幾何学的に画像を歪ませる処理 CROP や強すぎる加工 CONV2 に対しては弱く、画素レベルの処理に対しては耐性があることがわかったが今回使用した stirmark のすべての攻撃に対して対応しきれていないことが確認できる。抽出できなかった stirmark の攻撃の画像がどのくらい違ったかをハミング距離として表 4.3 で示す。

図 4.11 実験 1 で透かし情報を抽出できなかった stirmark の攻撃

表 4.3 ハミング距離を求めた結果

	CROP10	CROP50	CONV2
lena	5	0	7
japan	7	7	2
cherries	10	0	8

表 4.3 より、ハミング距離を求めた結果はほとんど画像が全体の 10 ビットの半分以上が違うビットを抽出していた。CROP のような小さく画像を切り取る加工や CONV2 のような強い加工だとコンピュータが他の違う画像だと認識し違うビットが抽出されたと考えられる。表 4.2 より、実験 2 では実験 1 で透かし情報を抽出できなかった stirmark の攻撃 CROP10、CROP500、CONV2 の画像を加えたもので augmentation し fine-tuning して学習させることで、今回使用した stirmark の攻撃すべてに対して透かし情報を確認できたので加工耐性が十分あるといえる。実験 2 の結果からあらかじめ強く加工編集に対応させるため原画像と一緒に強く加工編集された画像を augmentation し fine-tuning して学習させることで、今回使用した stirmark の攻撃だけでなく他の stirmark の攻撃や stirmark 以外の強い加工編集にも耐性が十分あると考えられる。

4.6 むすび

今回の実験では CNN を利用した電子透かしの構成法において電子透かしの耐性評価法である stirmark に対する透かし情報の耐性の検証を行った。実験 1 では原画像だけを augmentation し fine-tuning して学習させたが幾何学的に画像を歪ませる処理 CROP や強すぎる加工 CONV2 に対しては透かし情報が抽出できず、画素レベルの処理に対しては透かし情報が抽出できたのである程度の耐性はあるが、今回使用した stirmark の攻撃 AFFINE、CONV、NOISE、JPEG、MEDIAN、ROT、CROP すべてに対応できていなかったことが分かる。実験 2 では原画像だけでなく実験 1 で透かし情報を抽出できなかった CROP10、CROP50、CONV2 の画像を一緒に augmentation し fine-tuning すること

で実験 1 では透かし情報を抽出できなかった stirmark の攻撃にも対応することができ、今回使用した stirmark の攻撃すべてにおいて透かし情報が抽出できたので加工耐性が十分あるといえる。実験 2 で使用した方法をすればどんなに強い加工だとしても透かし情報を抽出できる電子透かしだと考えられる。今後の課題としては、今回の実験では 10 ビットで電子透かしを埋め込んだがこのビット数を 100 ビット、1000 ビットまで増やし、増やしたときの fine-tuning の精度や加工編集による透かし情報の耐性を検証する必要がある。

参考文献

［1］ 中谷憲、“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”、2019 年度神奈川大学修士論文。

［2］ Meng Zhaoxiong, Morizumi Tetsuya, Miyata Sumiko and Kinoshita Hirotsugu, “Design scheme of copyright management system based on digital watermarkingand blockchain,” IEEE, 2018 IEEE 42nd Annual Computer Software and Applications Conference（COMPSAC), Vol. 2, DOI：10. 1109/COMPSAC. 2018. 10258, 2018.

［3］ 中谷憲、“機械学習に基づく新しい知覚ハッシュ関数の構成と電子透かしへの応用”、神奈川大学、平成 30 年度卒業論文。

［4］ 山本大勢、“CNN を用いた電子透かしの加工耐性の検証”、神奈川大学、2021 年度卒業論文。

［5］ “The information hiding homepage” https://www.petitcolas.net/watermarking/stirmark/ 参照 Dec. 15, 2022.

5　研究成果 3：非文字資料を使った共起ネットワークとオントロジによる非文字検索

5. 1　まえがき

インターネットの普及に伴い様々な資料のデジタルアーカイブ化による保存活動がされている[1]。また近年では、企業サービスとして絵本や漫画を電子書籍として提供するネット図書館と呼ばれるようなサービスが普及している。また国としての取り組みとして「国立国会図書館」がある[4]。令和 3 年 12 月より「国立国会図書館のデジタル化資料個人送信に関する合意書」に基づき令和 4 年 5 月よりデジタル化資料送信サービスが開始されている[4]。ここで行政、企業だけでなく学術分野にも視点をおいてみると、歴史資料や学術資料のデジタル化を行い保存することで、自然災害などの外的要因の影響をうけることなくいかに後世に残していくかという点や、遠方でも資料閲覧が可能となるなどその重要性は高まっている。一方、神奈川大学においても「神奈川大学 21 世紀 COE プログラム」の発足に伴い、人間の営みに関する非文字資料が『年報　非文字資料研究』『非文字資料研究』（以下、年報）としてまとめられている[5][6]。このように、年報やネット図書館のようなデジタルアーカイブ化における問題点は、サーバーにおけるデータ量の増加やデータ損失が挙げられるが、データ量の増加などの蓄積変化に対しても、利用者の目的に応じて必要な情報を獲得するような、よりユーザに即したインターラクティブな資料検索は必須である。このような利用者の目的に応じて、必要な情報を獲得し利用するためには、利用者が求めている関心に対して、必要な情報を正確に読み取り検索結果を返すだけでなく[1]、ユーザが求めている情報以上の検索結果や発見を返すことは、利便性向上につながる。

そこでインタラクティブな資料検索を実現する検索手法として、従来のようなキーワード検索や全文検索が一例として挙げられるが、これだけでは利用者が求めているような関心を必ずしも表示しているとは限らないため過不足である。また神奈川大学における従来研究において「非文字資料に適したデジタルアーカイブの構築」[木下慶子、2006]、「民具データベースの RDF 化とオントロジを導入した情報検索システム」[神保理恵、2014]、「リレーショナルモデルによるデジタルアーカイブのための民具データベースの構築」[羽生敏英、2015] によるとデータベースやメタデータ生成を用いて、オントロジに紐づけられた潜在語の研究がなされていたが、キーワード検索やこれら従来研究における潜在語の検索手法では、本研究で定義する「共起性」や「潜在性」は、両方向で考慮されていない[1][2][3]。共起性のみでは潜在性が考慮されていないため、単語の出現頻度や単語同士の類似度によって、共起ネットワークを構築した際に、共起化された単語だけでは実際にそのコンテンツを示唆しているのかは不透明である。そのため潜在性を図るという行為は必要となる。よって本研究で提案するのは、「共起性」や「潜在性」を考慮した検索手法として、オントロジと共起ネットワークを用いていく。このような神奈川大学木下研究室における従来研究や本研究を用いることで、ネット図書館のような資料検索においても、利用者が求める関心に対して、単語同士の類似度を「共起性」として測定し、そこに潜在単語を含む資料同士の繋がりを「潜在性」として提示することで、利用者がキーワード検索だけでは気づきを得なかった発見を促し、ユーザインタラクティブな参照を可能としていく。このような検索システム構築や提案が、昨今のデジタルアーカイブ化における技術発展において最も渇望されている。

本研究では、非文字資料を対象としたオントロジと共起ネットワークを用いた非文字検索システムを提案している。ここで、神奈川大学非文字資料研究センターウェブページの“非文字資料研究(旧：年報)”には、非文字資料のレポートが刊行物として公開されているため、一部サンプルデータを本研究における非文字検索で使用する[6]。そこで本研究の一つ目の目的は「潜在性」および「共起性」に焦点を当て、非文字資料から潜在単語や潜在的な非文字資料を検索結果として表示することである。最終的に、非文字検索の随伴関係におけるシステム設計図を用いて、オントロジと共起ネットワークの両方向から相互に潜在単語を考察することが望ましい。本研究の二つ目の目的は、構築したオントロジから、二つの単語（W_0, W_1）のオントロジの経路の検索と経路パターンの比較を行い、潜在単語や非文字資料同士の繋がりや関係性を考察することである。本研究の三つ目は、オントロジの経路の検索結果と共起における 2 単語の平均情報量の計算結果を、随伴関係における結果として相互に考察することである。本研究では、非文字資料を対象としたオントロジと共起ネットワークを用いた非文字検索システムを提案している。よって本説では神奈川大学木下研究室における非文字に関する研究事例を紹介し、本研究の位置付けと新規性を明確にする。本研究室内での従来研究としては、潜在単語検索の研究に焦点を当ててみると、「非文字資料に適したデジタルアーカイブの構築」[木下慶子、2006]、「リレーショナルモデルによるデジタルアーカイブのための民具データベースの構築」[羽生敏英、2015] や「非文字資料に適したデジタルアーカイブの構築」[木下慶子、2014] では、データベースやメタデータ生成、モデリング分析を用いた潜在単語検索や、オントロジに着目した概念付与によって潜在単語検索を模索している[1][2][3]。しかし、これらの従来研究ではオントロジのみに着目しており、潜在性や共起性までは考慮されていない。そのため本研究では、潜在性および共起性

という２点に焦点を当てて、オントロジと共起ネットワークを用いてシステム設計を考えるという点で、神奈川大学での従来の潜在研究と比較して新規性がある。また本研究室外での従来研究では、立命館大学・樋口耕一准教授が開発した社会研究を目的とした計量テキスト分析ツール KHCoder というソフトウェアが存在する。

KHCoder は、出現する単語について共起図を作成し可視化することが、プログラムを組まなくとも直感的な操作が可能である[24]。そこで本研究のオリジナリティは、オントロジを構築または共起図を作成した際に、オントロジや共起図からは見逃されてしまっている潜在単語にも焦点を当てることで、実際に共起図では出現頻度や類似度によって表現されなかった単語も、その文書資料を位置づける単語として実は重要である、潜在単語を探しあげることで、ユーザにとって資料同士の関係性の新たな発見を導き出すことが本研究室外における先行研究との違いである。

5.2　先行研究

5.2.1　民具データベースの RDF 化とオントロジを導入した情報検索システム、神保理恵、2014

本研究では只見町の民具データベースを対象に他のデータベースとの横断検索の実現や専門知識を持たないユーザによる検索を容易にすることを目的として、RDF 化したデータベースとオントロジから構成される。意味に基づいた情報処理を行う情報検索システムの提案と実験を行った。実験の結果からは、提案システムでは推論による民具の自動的な分類や分類名による検索が可能であることが確かめられた。これらの結果から、本研究の目的はおおむね達成することができたと結論付けられる。しかし一方では、実際に「只見町インターネット・エコミュージアム」で公開されている民具の情報検索システムと提案システムの技術的な比較が不十分であるという問題がある。このことは提案システムの実用化を考える上で今後解決すべき課題である。また、横断検索や専門知識を持たないユーザによる高度な検索は、様々な分野における博物館資料データベースに要求される機能であるため、本研究は民具データベースのみならず博物館資料データベース全体に対してデータベースの RDF 化とオントロジを導入した情報検索システムの有用性を示すことができたと言える[1]。

5.2.2　リレーショナルモデルによるデジタルアーカイブのための民具データベースの構築、羽生敏英、2015

デジタルアーカイブ化が浸透する中で、情報統合する上での課題はコンテンツの利活用及び連携を容易にするため、項目定義や語群の標準化が必要である。しかし本研究の題材とする民具資料に関しては、一意に分類できず標準名が存在しないため、資料情報を統合する点で不十分である。そこで本研究ではリレーショナルモデルを用いて、只見町民具データベースの構築及びデータモデリング分析、デジタルアーカイブ化の三つを行った。本研究では、民俗資料はモノ情報とコト情報の和集合として考えることで資料情報の構造化が図れると考え、データモデリングという手法を用いたことで、トップダウン分析、ボトムアップ分析の二つを行えるようにデータ整理を行った。資料情報の構造化により、記載される項目ごとに属性整理を可能としたが、民具資料をデジタルアーカイブ化する際にも標準名を決めるべきである。またデータ整理において、複数の分類方法は同居可能であると考えた。本研究では、データモデリングによる二つの分析方法を用いて、最適なリレーション構築を目指した[2]。

5.2.3 非文字資料に適したデジタルアーカイブの構築、木下慶子、2006

神奈川大学 21 世紀 COE プログラム「人類文化研究のための非文字資料の体系化」が保有する非文字資料の情報発信の分析を支援するための民俗学分野に特化した Ontology 構築を行った。非文字資料は、メタデータと真のデータの関係性から推論する事で再構成される民俗学研究特有の性質を持っている。そこで本研究では、非文字資料に適した Ontology 構築を行う事で、新たな知見・関連性の発見支援を目指した。多領域においてメタデータが生成されているため、情報資源を正確に管理するには、できるだけ詳細な記述のできるメタデータ生成が必要である。よって非文字資料のメタデータにおいても何が必要で適切なのかの検証は必要不可欠である。さらに本研究では、非文字資料の中でも民具における Context 間の関連性に着目し、Ontology とシソーラスを用いた民具に適した Ontology 構築を行う事で、民具間の関連性を導き出した。Ontology は様々な知識を関係付ける基盤としての役割を果たしている。しかし対象とした非文字資料には、同一対象においても異なる概念化が複数存在した。Ontology によって概念化を表現するためには、シソーラスを含めて、より高度な意味論を考慮した枠組みが必要である。今後の課題としては、Context 間の関連をモデル化し、大規模データベースにおける探索効率の向上を目指す事である。[3]

5.3 先行研究の問題点

5.3.1 共起性

共起性とは、2 単語から単語同士の共通点や類似度、単語の出現頻度を Jaccard 係数や networkX を用いて共起分析した際の共起の度合いを「共起性」と本研究では定義する。また、ノードで結んだオントロジ関係のある単語同士を「共起」という。

5.3.2 潜在性

潜在性とは、二つの単語（W_0、W_1）のオントロジの経路から外れている潜在単語や潜在単語集合が、オントロジの経路の周辺層に、どの程度含まれているかどうか定量的な度合いを潜在性と本研究では定義する。オントロジの経路から外れた 2 単語（W_0、W_1）の周辺の単語を潜在単語と呼称する。また、オントロジの経路から外れる潜在単語や潜在単語集合が属していた元資料のことを潜在資料と呼称する。ここで本研究における潜在性は、オントロジの経路の検索および経路パターン表を利用した考察によって潜在性を測っていく。オントロジの経路上において、潜在単語が属する資料同士の関係性が高い場合や他の経路と比較して属する資料数を多く含んでいる場合を「潜在性が高い」という。

5.3.3 非文字検索

本研究における非文字検索は、検索手法として提案する「随伴関係」を本研究では「非文字検索」と定義する。この随伴関係は、オントロジと共起ネットワークの比較によって表現される。以下にオントロジと共起ネットワークの比較を図 5.1 に示す。またオントロジと共起図を比較した際、二つの単語（W_0、W_1）のオントロジの経路上に出現する潜在資料または、オントロジの経路からは外れているが、ノードでは接続されている周辺の潜在単語集合や潜在単語を検索することを「随伴関

係における非文字検索」と定義する。神奈川大学木下研究室の従来研究における潜在語検索は、オントロジにおける「潜在性」のみに着眼点を置くことで非文字検索と定義していた。しかし本研究の背景でも述べたように、これらの従来研究における潜在語の検索では、「共起性」は考慮されていても、本研究で定義する「潜在性」までは考慮されていない。そこで本研究における非文字検索は、「随伴関係」を取り入れた潜在語や潜在資料の検索を、本研究では非文字検索と再定義する。「随伴関係」には「共起性」や「潜在性」が考慮されている点が、従来の非文字検索の定義との大きな違いである。そのため本研究における非文字検索を理解するには、まずは「随伴関係」の仕組みを理解する必要がある。この「随伴関係」を取り入れた検索システムの説明は提案システムで解説する。

左図がオントロジ、右図が共起ネットワークである。この二つの関係が随伴関係である。

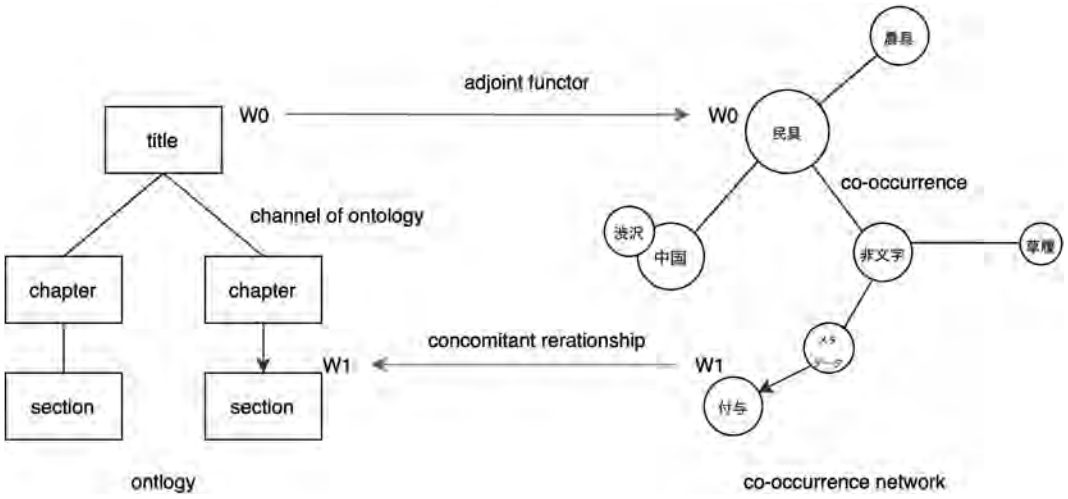


図 5.1　オントロジと共起ネットワークの比較の例

5.3.4　共起ネットワークの現状の問題点と改善点

共起ネットワークだけでは、単語の類似度や出現頻度によって共起性のみしか測定できない。そのため本研究における潜在単語および潜在資料の検索において重要な、潜在性を図るという点は考慮されていない。そこで従来研究からの改善点として本研究では、非文字資料からリレーショナルデータベースを用いて、オントロジおよびオントロジの経路を表現することで、潜在性の測定という点を補っていく。

5.3.5　非文字資料のキーワード検索や全文検索における問題点

非文字資料研究センターのホームページにおいて、キーワード検索で 2 単語を指定し検索をしたところキーワード検索では、本研究で使用する非文字資料の年報 No. 3 は検索結果として出力されなかった。今回は一見関係なさそうな検索単語として Word1＝「中国」、Word2＝「メタデータ」を入力した。以下にキーワード検索の実例を示す。

また全文検索では、本研究で使用する非文字資料の年報 No. 3 は、検索結果として資料がいくつも出力されたが年報 No. 3 の資料同士が直接関係コンテンツと断定するのかまでは検索結果からはわからない。以下に全文検索の実例を示す。

図 5.2　非文字資料研究センターにおけるキーワード検索の例

図 5.3　非文字資料研究センターにおける全文検索の例

非文字資料研究センターのキーワード検索などでは、一見関係なさそうな 2 単語の検索単語からは No. 3 の資料は二つ以上出力されなかった。実際のキーワード検索において「中国」「メタデータ」と検索した際に、No. 3 の非文字資料における以下の 2 資料のみで検索結果は表示されなかった。

表 5.1 「中国」「メタデータ」とキーワード検索した際に検索表示がされなかった 2 資料

資料 no.	資料名
16	中国内蒙古の若者の身体形状の特性
6	民俗学研究のための情報発信

そこで 2 資料の資料内容の事例を以下にそれぞれ示す。下記の事例は内容に関連性が無いので資料同士が検索されにくい。

そこで、オントロジと共起ネットワークの随伴関係による検索システムを用いた潜在性、共起性を

Ⅰ　資　料

調査対象（被験者）は中国内蒙古自治区フフホト（呼和浩特）市で日本語を学んでいる 20 代の学生である．調査は 2004 年 9 月に実施した．男子は 19.7 歳から 28.8 歳までの 45 名（平均年齢 22.1 歳），女子は 19.8 歳から 29.1 歳までの 46 名（平均年齢 22.5 歳）である．

被験者の生地は男 16%，女 4% がフフホトであるが，他はフフホト以外の内蒙古自治区であった．すなわち被験者の大多数が牧畜民の出身であり，騎馬を日常的に行っていた．また，男の 60%，女の 80% が蒙族で，他は漢族だった（ただし男には満族とダッタン族が各 1 名いた），両親とも蒙族の組み合わせは男 60%，女 80%，両親がともに漢族は男 24%，女 17%，両親が蒙族と漢族の組合せは男 9%，女 2% であった．その他，男子被験者には両親の組合せが漢族と満族が 2 名，漢

1.2　メタデータの基礎概念

本章では，書誌情報のように，情報資源を組織化・管理し，利用に提供するための情報資源の性質について述べる．また，情報資源発見のためのメタデータ規則として開発された Dublin Core について述べる．

1.2.1　メタデータの目的と種類

計算機技術の発達は計算能力の向上だけでなく，様々な応用技術を生み出した．飛躍的に増加し続ける情報資源を管理するための新しい概念として発展してきたのがメタデータである．メタデータは「データに関するデータ」と定義され情報の内容を表現すると同時に，情報を構造化するものである．(1)(2)
メタデータは情報資源管理と情報資源発見を目的としており，応用は基本的にその対象範囲を広げる事で，現在，研究等多くの分野に対象を広げている．メタデータは，ある情報に対する付加的なデータで，データを意味付けするために重要な役割を果たす．これまでのメタデータは各個人や組織，団体など限られた範囲内で限られたデータを扱うために利用されてきた．図書館や博物館は，館内あるいは同様の館同士，例えば図書館同士の整理，管理，検索を効率よく行う事を目的として独自の目録システムを構築し利用していた．ところが近年の情報の電子化は対象を選ばず急速に進んでおり，同時にこれまで独自に運用してきた情報同士を交換したり，横断的に検索したいという要求が生じてきている．各組織が独自のメタデータのまま交換しただけでは，内容に関する情報が正確でないばかりか，意味がまったく違ってしまう可能性もある．そこで近年，メタデータを国際的に共通化，標準化

図 5.4 「中国内蒙古の若者の身体形状の特性、芦澤玖美、2006」、「民俗学研究のための情報発信、木下宏揚、2006」

考慮することで、年報 No.3 において上記のような 2 資料が検索結果として出力されるかを検証する。これにより上記のような既存の資料検索における問題が解決されたかどうかが分かる。次ページにてその検索システムの設計図を説明していく。

5.4　提案システム

5.4.1　圏論を利用した共起ネットとオントロジによる随伴関係

本研究が提案する非文字検索システムは、共起ネットワークおよびオントロジの二つを圏論という概念を利用して相互作用させたものである。以下に非文字検索における共起ネットワークとオントロジを利用した随伴関係のシステム設計図を図 5.5 として示す。

この設計図は、5.3.3 で定義した図 5.1「非文字検索のオントロジと共起ネットワークの比較」

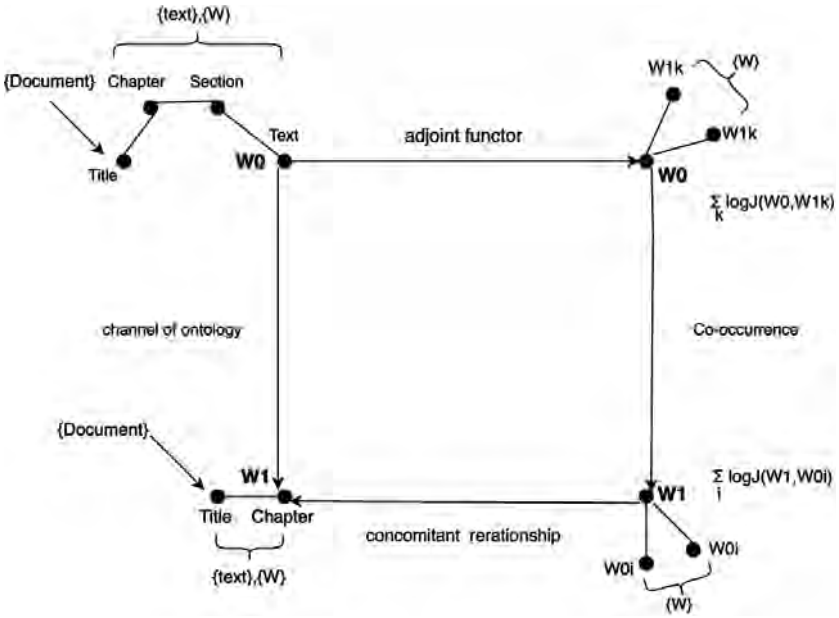


図 5.5　共起ネットとオントロジを利用した随伴関係のシステム設計図

を、よりシンプルに設計したものである。

左側をオントロジ、右側を共起ネットワークで表現する。この設計図で表される下矢印「オントロジの経路（channel of ontology）」と「共起（Co-occurrence）」は、二つの単語（W_0, W_1）の間のオントロジ関係および共起関係を用いている。そのため、左側の（W_0, W_1）の間の関係を「オントロジの経路（channel of ontology）」と定義する。「オントロジの経路（channel of ontology）」によって、オントロジ関係のある（W_0, W_1）の経路とノード周辺の潜在単語や潜在資料を検索することで潜在性が測れる。また、右側の（W_0, W_1）の間の関係を「共起（Co-occurrence）」と定義する。「共起（Co-occurrence）」によって、共起関係のある（W_0, W_1）のノード周辺の潜在単語 W_1k, W_0i を検索し、平均情報量の差分を求めることで、共起性が測れる。ここで設計図において、「潜在単語」「潜在単語集合」「潜在資料」がどこに含まれているかを説明する。左側において、オントロジの経路の「潜在単語」や「潜在単語集合」は、W_0, W_1 から外側周辺に伸びているノードの Section 層、Chapter 層、title 層のデータのことである。潜在単語は W、潜在単語集合は text の記号で表される。また、最端層である title 層のデータは「潜在資料」に該当する。右側において、共起ネットワークの「潜在単語」は、W_0, W_1 から外側周辺に伸びているノードの W_1k や W_0i といった単語のことである。次に、左側「オントロジの経路（channel of ontology）」と右側「共起（Co-occurrence）」の相互作用について説明する。この設計図で表される左右矢印「随伴関手（adjoint fuctor）」と「随伴関係（concomitant rerationship）」は圏論の考え方を用いている。二つの対象間の射からなる構造であり、W_0 同士、W_1 同士の間の関係性を表している。左側で表されている W_0 と右側で表されている W_0、左側で表されている W_1 と右側で表されている W_1 はそれぞれ同じ単語を用いているので「自然同値」である。「随伴関手（adjoint fuctor）」と「随伴関係（concomitant rerationship）」は反射律、対象律、推移律を満たしていると言える。以上より、左側のオントロジにおける二つの単語（W_0, W_1）は、右側の共起ネットワークにおける二つの単語（W_0, W_1）と相互に置き換えて使用することができるため、自然同値である（W_0, W_1）を用いることで左側では潜在性を、右側では共起性を測定して 2 性質を調べることが理論上可能である。次に、潜在性と共起性の求め方についてそれぞれ説明する。

まず、設計図右側の共起ネットワークにおける共起性の求め方を説明する。Jaccard 係数を用いて、共起された（W_0, W_1）のそれぞれの平均情報量を求めたのち、（W_0, W_1）の平均情報量の差分を求めることで共起性を測っていく。その際、W_1, W_0 に対して、周辺の単語 W_1k, W_0i を Jaccard 係数を求める際の単語セットとして使用する。以下に、（W_0, W_1k）における平均情報量の計算を式（5.1）として示す。

$$\sum_i logJ(W_0, W_1k) \tag{5.1}$$

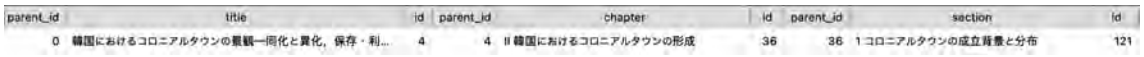
また、（W_1, W_0i）における平均情報量の計算を式（5.2）として示す。

$$\sum_k logJ(W_1, W_0i) \tag{5.2}$$

よって式（5.1）および式（5.2）より、共起された（W_0, W_1）の平均情報量の差分の計算を式（5.3）として示す。

$$\sum_i logJ(W_1,\ W_0i) - \sum_k logJ(W_0,\ W_1k) \tag{5.3}$$

続いて、左側のオントロジにおける潜在性の求め方を説明する。左側のオントロジでは（W_0, W_1）の「オントロジの経路（channel of ontology）」を求めることで潜在性を測る。オントロジの経路とは、オントロジ全体の経路のうち、共起された２単語（W_0, W_1）の経路のみを出力したものを、「オントロジの経路（channel of ontology）」と本研究では定義する。オントロジの経路の例を図 5.6 に示す。オントロジ全体の経路のうち、共起ネットワーク側で決定した二つの単語（W_0, W_1）を利用して、二つの単語（W_0, W_1）が両端層に含まれているオントロジの経路を出力する。ここで図 5.6 の例では、両端層ノードから外れている section 層より下層の text 層データなどが「潜在単語」や「潜在単語集合」に該当する。このような text 層のことを、「オントロジの経路から外れる潜在単語」などと呼称する。



parent_id	title	id	parent_id	chapter	id	parent_id	section	id
0	韓国におけるコロニアルタウンの景観―同化と異化，保存・利...	4	4	II 韓国におけるコロニアルタウンの形成	36	36	1 コロニアルタウンの成立背景と分布	121

図 5.6　オントロジの経路の例

上記の図 5.6 オントロジの経路の例では、title 層―chapter 層―section 層までをノード接続している。また（W_0, W_1）は両端層の title 層か section 層どちらかに含まれている。ここで、潜在性を求めるにあたり、オントロジの経路として出力が想定される経路パターン表を使用する。経路パターン表では、オントロジの経路に含まれている二つの潜在資料が同じ年報同士の経路か、違う年報同士の経路かどうかの２種類で分類を行う。上記の図 5.6 オントロジの経路の例のように、実際に出力されたオントロジの経路の出力結果が、設計図におけるオントロジの経路に該当する。そこで下記の表 5.1

表 5.1　オントロジの経路パターン

no	種類	経路パターン
1	同じ年報の経路	title-title
2	同じ年報の経路	chapter-chapter
3	同じ年報の経路	section-section
4	同じ年報の経路	text-text
5	同じ年報の経路	title-chapter
6	同じ年報の経路	title-chapter-section
7	同じ年報の経路	title-chapter-section-text
8	同じ年報の経路	chapter-section
9	同じ年報の経路	section-text
10	違う年報の経路	text-section-chapter-title-title-chapter-section-text
11	違う年報の経路	section-chapter-title-title-chapter-section-text
12	違う年報の経路	chapter-title-title-chapter-section-text
13	違う年報の経路	title-title-chapter-section-text
14	違う年報の経路	title-title-chapter-section
15	違う年報の経路	title-title-chapter
16	違う年報の経路	title-title
17	違う年報の経路	chapter-title-title-chapter
18	違う年報の経路	section-chapter-title-title-chapter
19	違う年報の経路	section-chapter-title-title-chapter-section
20	違う年報の経路	text-section-chapter-title-title-chapter-section

と比較をすることで、潜在単語や潜在資料の発見を行い、潜在性を測っていく。

上記表について簡単に説明する。W_0, W_1 は、上記のオントロジの経路のいずれにおいても両層端のどちらかに含んでいる。そのため、図 5.6 のオントロジの経路の例は、上記表と比較すると no. 6 の経路パターンに該当する。また、no. 1 から no. 4 の経路パターンは、同じ年報の経路において最短経路かつ（W_0, W_1）が同層であることがわかる。また同じ年報の経路では、no. 7 の経路パターンが最長経路である。違う年報の経路において、no. 16 の経路パターンが最短経路かつ違層において、潜在資料を二つ含んでいることがわかる。また違う年報の経路では、no. 10 の経路パターンが最長経路である。このように、出力された（W_0, W_1）のオントロジの経路を経路パターンと比較をすることで、経路長や潜在単語、潜在資料が含まれる層を特定し、考察することができる。以上で、非文字検索における随伴関係のシステム設計図および共起性・潜在性の求め方の説明とする。

5.4.2 提案システムにおける入力と出力

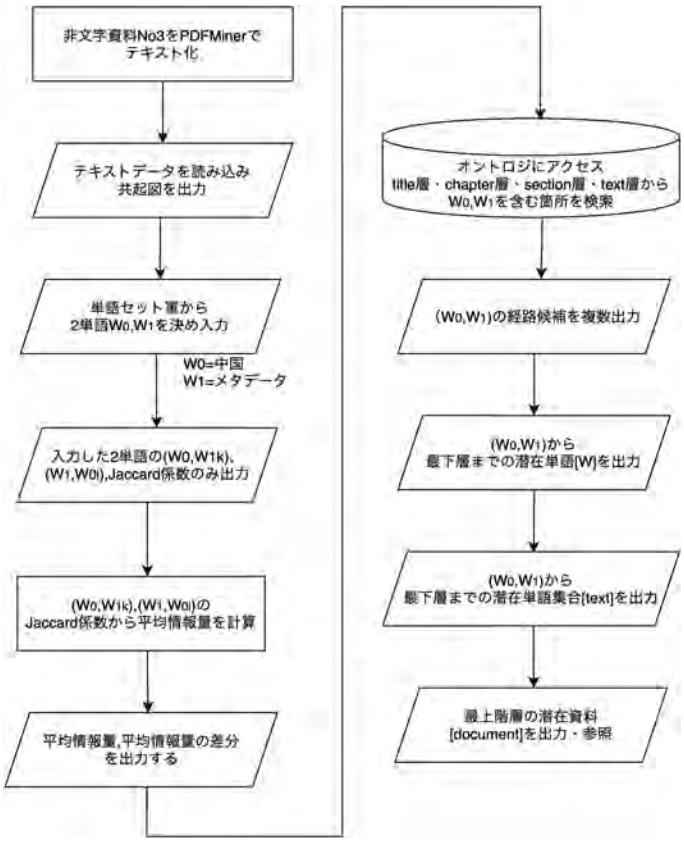


図 5.7　非文字検索システムにおけるアルゴリズム

共起ネットワークとオントロジを用いて、提案システムにおいて入力と出力をプログラム上でどう表現するかアルゴリズムをフローチャートにしている。非文字検索の提案システムおいて、以下の順序で入力と出力を行う。

1．テキストデータを読み込み、共起図を出力する

2．共起図を作成する際に利用される単語セット群から 2 単語を W_0, W_1 と決めプログラム上で単語入力する

3．入力された W_0, W_1 の単語セット（W_0, W_1k）、（W_1, W_0k）、Jaccard 係数を出力する

4．（W_0, W_1k）と（W_1, W_0k）の Jaccard 係数から平均情報量と平均情報量の差分を計算して出力する

5．オントロジのデータベースにアクセスを行い、title 層・chapter 層・section 層・text 層から W_0, W_1 の存在する層を検索する

6．ノードで接続された、W_0, W_1 のオントロジの経路を複数出力する

7．オントロジの経路の出力と同時に、最下層までの潜在単語、潜在単語集合、最上階層の潜在資料も出力する

以上のように入力と出力を行い、潜在単語、潜在単語集合、潜在資料の非文字検索を行う。ここで注意点として、図 5.7 において、PDFMiner を用いた資料のテキスト化は自身では今回行わず、木下研究室内において、事前にテキスト化された年報 no. 3 のデータを使用した。また、年報 No. 3 を使用した理由について、当初は年報 No. 1 でオントロジの作成を試みたが、PDFMiner で抽出をした際、非文字資料で使われている文字に旧字体が多く存在したことで文字化けが発生したため、No. 3 を今回の実験で採用した。

5.5　提案システムの実装

5.5.1　実装環境

上記のオントロジおよび共起ネットワークを用いた提案システムの実装は、Jupyter notebook および DB Browser SQL を用いて python 言語、SQL 言語で実装を行った。使用したソフトウェアおよび環境一覧を以下に示す。Python3 は Jupyter notebook 上で使用した。

- Ubuntsu20.16/MacOS Bigsur 11.4

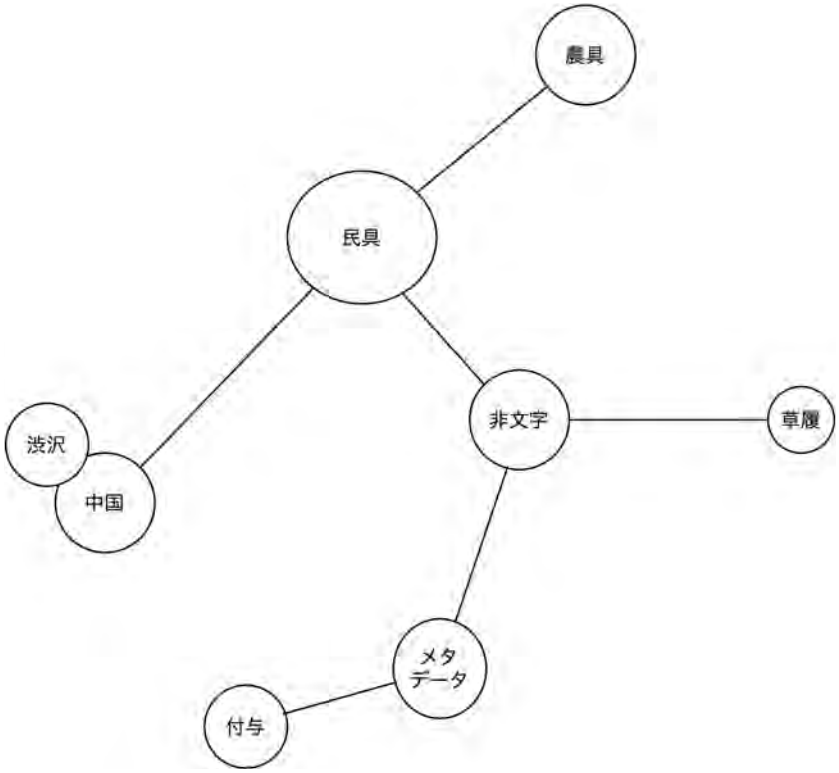


図 5.8　共起図の例

- jupyter notebook
- Python 3
- DB Browswr for SQLite

5.5.2　共起ネットワーク（共起図）の作成

本研究では、非文字資料の共起性を求める実験として、共起ネットワークを用いて共起図を作成する。共起ネットーワーク側では、非文字資料 no.1 から no.17 をテキスト化したものを読み込み、共起図の作成をプログラム上で行う。

5.5.3　共起図の作成

このように Jupyter Notebook 上にて実際に共起図を作成する。共起図作成は、KHCoder などの既存ツールではなく、python 言語を使い jupyter　notebook のプログラム環境で構築を行う。その際、janome や networkX など様々な python ライブラリをインポートして利用した。

平均情報量の差分の計算

本研究では、非文字資料の共起性を求める実験として、共起図で使われた Jaccard 係数から平均情報量と平均情報量の差分を計算する。計算はすべてプログラム上で行う。（W_0, W_1）の共起における平均情報量の差分の計算式を以下に示す。

$$\sum_i logJ(W_1, k) - \sum_k logJ(W_0, i) \tag{5.4}$$

平均情報量の差分の計算プログラムを以下に図 5.9 として示す。

上記プログラムを実行すると、W_0 と W_1 の入力を求められる。

以下に W_0 の入力画面を図 5.10 と W_1 の入力画面を図 5.11 として示す。

```
#w0w1を入力
s = input('w0を入力してください : ')
r = input('w1を入力してください : ')

#(W0,W1k),Jaccard係数のセット抽出
df0 = pd.DataFrame(df_jaccards,columns=[s])

#(W1,W0k),Jaccard係数のセット抽出
df1 = pd.DataFrame(df_jaccards,columns=[r])

#平均情報量の計算
entropy = lambda df:-reduce(
    lambda x,y:x+y,
    map(
        lambda x:(x/len(df))*math.log2(x/len(df)),
        df.iloc[:,-1].value_counts()
    )
)

#平均情報量の差分を計算
entropy_w0w1=entropy(df1)-entropy(df0)

#使用する(W0,W1k)を出力
print(df0)

#使用する(W1,W0k)を出力
print(df1)

print('W0='+str(s)+','+'W1='+str(r)+'と入力した場合の共起における平均情報量の計算結果を表示します')
#W0の平均情報量を出力
print('W0の平均情報量は'+str(entropy(df0))+'bitでした。')
#W1の平均情報量を出力
print('W1の平均情報量は'+str(entropy(df1))+'bitでした。')

#平均情報量の差分の出力
print('W0W1の平均情報量の差分は'+str(entropy_w0w1)+'bitでした。')
```

図 5.9　W_0 = 中国、W_1 = メタデータにおける平均情報量の差分の計算プログラム

図 5.10　W_0 = 中国の入力画面

図 5.11　W_1 = メタデータの入力画面

W_0 と W_1 の入力に対し、平均情報量と平均情報量の差分を計算し、結果として出力を返してくれる。

5.5.4　オントロジの構築

オントロジ全体の構築を行う。オントロジは、SQL 言語（sqlite3）を用いて、非文字資料 no. 1 から no. 17 を基に、title 層、chapter 層、section 層、text 層ごとに分離し、階層構造のオントロジとして全体を構築する。その手順を以下に説明する。

5.5.5　非文字資料の RDB 化

非文字資料を層ごとに分離しデータベース化を行うため、まずは使用した非文字資料について説明する。本研究で使用した非文字資料は、神奈川大学非文字資料研究センターに保管されている年報のうち、年報 3 における非文字資料 no. 1 から no. 17 までの 17 個の資料である。[6] [7][8][9][10][11][12][13][14][15] 実験で使用した非文字資料の名称を表 5.2 に示す。[16][17][18][19][20][21][22][23] 本研究ではこの非文字資料の内容を層ごとに分離し、すべてのデータベース化を行う。

表 5.2　本実験で使用した年報 No. 3 の非文字資料一覧

no	資　料　名	著　者
1	台南道教の符籙について―放赦科儀の九龍符命とその歴史を中心に―	丸山宏
2	「渋沢フィルム」撮影地の景観変貌―韓国・蔚山を事例として―	浜田弘明
3	『模地数里』に描かれた松前―長春丸・女商人・馬―	菊池勇夫
4	韓国におけるコロニアルタウンの景観―同化と異化、保存・利用・破壊―	須山聡
5	文化情報発信システムとしてのインターネット博物館	佐野賢治
6	民俗学研究のための情報発信	木下宏揚
7	文化政策としての民俗博物館	丸山泰明
8	風俗表現における図様の伝統と創造	金貞我
9	蘇った納西族東巴教「求寿」儀式	夏宇継
10	北京市都心部および郊外農山村の景観変容	藤永豪
11	住みつづける意思―紋別市陸部における畜舎景観の成りたち―	土田拓
12	教会大学と日中戦争―「北平私立輔仁大学檔案」（1925-1952 年）から見た戦時下の学生収容―	王京
13	「姑蘇繁華図」に見る清代前期の江南地域における紡織業及びその流通―地方文献に照らして―	彭偉文
14	感性の人類学のための予備的覚え書き	川田順造
15	モーションキャプチャを使った芸能比較研究の試み	廣田律子、他
16	中国内蒙古の若者の身体形状の特性	芦澤玖美
17	旧朝鮮の神社跡地調査とその検討―全羅南道，和順郡を中心に―	津田良樹、他

非文字資料を使い、オントロジ全体をどのように階層表現するか説明する。以下の図 5.12 は、非文字資料 no.1 から no.17 を基に、実際にデータベース化した際のオントロジ全体の組織図である。この組織図は簡略図として表現されている。簡略図として表現するため、階層に実際に存在した title 層数や chapter 層数、section 層数を以下のように図 5.12 に層数として記載した。

例：Chapter×4

資料ごとに title 層・chapter 層・section 層・text 層に資料を分類し、データベース登録を行った。以下にリレーショナルデータベースによるオントロジ全体の組織図を図 5.12 に示す。

図 5.12　リレーショナルデータベースによるオントロジ全体の組織図

上記のオントロジを構築するにあたり、実際のリレーショナルデータベース上では、titile 層・chapter 層・section 層・text 層ごとに 4 テーブルを作成する。今回は以下の基準でテーブル名とした。title データを格納したテーブルを、title table とする。chapter データを格納したテーブルを、chapter table とする。section データを格納したテーブルを、section table とする。text データを格納したテーブルを、text table とする。次に、データベース作成にあたり、ER 図を以下に図 5.13 として示す。各テーブル内において title table、chapter table、section table、text table には、実際の資料データが格納されている。

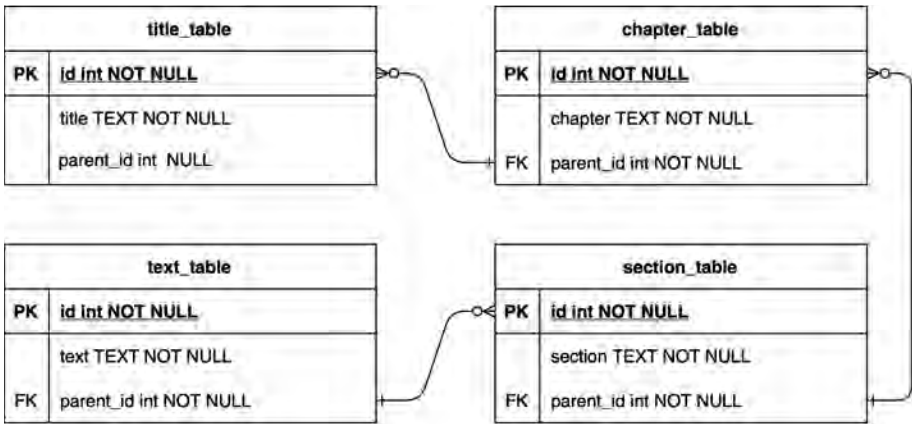


図 5.13　オントロジにおける ER 図

データベースを作成したところ、title：17 個、chapter：95 個、section：80 個、text：124 個が存在した。実際に作成したテーブル一覧を以下に図 5.14 として示す。

また、title table, chapter table, section table のテーブルデータを付録に掲載する。なお text table もデータ作成を行ったが、莫大なレコード数であるため text table のみ付録での掲載は省略する。

ここで、リレーショナルデータベースで階層構造のオントロジを再現するための表現方法を説明する。それぞれの層のデータに、そのデータを位置する ID（プライムキー）および親階層を表す parent id

図 5.14　実際に作成したテーブル一覧

のカラムを付与した。ID および parent id を付与した chapter 層のレコードの例を図 5.15 に示す。

parent_id	chapter	id
フィルター	フィルター	フィルター
7	II 民俗博物館とは何か	48

図 5.15　ID および parent id を付与したレコードの例

また、title 層はオントロジ全体での親階層であるため、title 層の parent id はすべて NULL 値になる。title 層のレコードの例を以下に図 5.16 として示す。

parent_id	title	id
フィルター	フィルター	フィ...
NULL	文化情報発信システムとしてのインターネット博物館ー大学・地域博物館の連携を中心にしてー	1

図 5.16　title 層における NULL 値の例

parent id の付与により、親レコードと子レコードのノード接続を行うことで、オントロジの親子関係をリレーショナルベース上で表現した。ノード接続のプログラムを以下に図 5.17 として示す。以下のプログラムでは、title 層―section 層―chapter 層―text 層までのノード接続を行っている。

共起図から決定した 2 単語（W_0, W_1）を用いて、オントロジの経路における検索プログラムを実行する。（W_0, W_1）を含むオントロジの経路の検索と同時に、潜在単語、潜在単語集合、潜在資料も経路上に出力される。以下にオントロジの経路となる経路パターン表の一部を表 5.3 に示す。この経路パターンを網羅したオントロジの経路の検索が望ましい。

```
SELECT title_table.*,chapter_table.*,section_table.*,text_table.*

FROM title_table
left join chapter_table on chapter_table.parent_id = title_table.id -- 1階層下
left join section_table on section_table.parent_id = chapter_table.id -- 2階層下
left join text_table on text_table.parent_id = section_table.id -- 3階層下
```

図 5.17　ノード接続のソースコード

表 5.3　オントロジの経路パターン例

no	種　類	経路パターン
1	同じ年報の経路	titile-title
2	同じ年報の経路	chapter-chapter
3	同じ年報の経路	section-section
4	同じ年報の経路	text-text
5	同じ年報の経路	tile-chapter
6	同じ年報の経路	title-chapter-section
7	同じ年報の経路	title-chapter-section-text
8	同じ年報の経路	chapter-section
9	同じ年報の経路	section-text

また、オントロジの経路の検索プログラムの一部を図 5.18 として示す。基本的に、検索条件の指定を行うことで、（W_0, W_1）を含む経路のみを出力する。

```
where title_table.title LIKE '%中国%' AND chapter_table.chapter LIKE '%メタデータ%'
OR title_table.title LIKE '%中国%' AND section_table.section LIKE '%メタデータ%'
OR title_table.title LIKE '%中国%' AND text_table.text LIKE '%メタデータ%'
OR chapter_table.chapter LIKE '%中国%' AND section_table.section LIKE '%メタデータ%'
OR section_table.section LIKE '%中国%' AND text_table.text LIKE '%メタデータ%'

OR title_table.title LIKE '%メタデータ%' AND chapter_table.chapter LIKE '%中国%'
OR title_table.title LIKE '%メタデータ%' AND section_table.section LIKE '%中国%'
OR title_table.title LIKE '%メタデータ%' AND text_table.text LIKE '%中国%'
OR chapter_table.chapter LIKE '%メタデータ%' AND section_table.section LIKE '%中国%'
OR section_table.section LIKE '%メタデータ%' AND text_table.text LIKE '%中国%'

OR title_table.title LIKE '%中国%' AND title_table.title LIKE '%メタデータ%'
OR chapter_table.chapter LIKE '%中国%' AND chapter_table.chapter LIKE '%メタデータ%'
OR section_table.section LIKE '中国%' AND section_table.section LIKE '%メタデータ%'
OR text_table.text LIKE '%中国%' AND text_table.text LIKE '%メタデータ%'
```

図 5.18　W_0, ＝中国、W_1＝メタデータにおけるオントロジの経路の検索条件

全体のオントロジにおいて、プログラムを実行することで、二つの単語（W_0, W_1）のオントロジの経路の検索が可能となる。同時に、経路上から外れた潜在単語、潜在単語集合、潜在資料がノード接続されて出力される。

5.6　実験及び実験結果

5.6.1　実験目的

共起ネットワークとオントロジを用いた随伴関係によって「潜在性」と「共起性」を求める。これにより、本実験を通して、オントロジの経路の検索を行うと同時に、潜在単語および潜在資料の検索・参照することが本実験の目的である。

5.6.2　実験方法

実験方法は以下である。アルゴリズムから作成したプログラムを実行することで、入力と出力を行う。プログラムにおいて、共起ネットワーク側では（W_0, W_1）の平均情報量の差分を計算し、オントロジ側では、（W_0, W_1）のオントロジの経路を出力する。これらを考察において比較評価する。今回は、検索結果の資料同士に関係性があるかどうかを示すために、共起ネットワーク側で共起図を作図した際に利用された単語セットの中から、W_0, W_1 を、一見単語関係がなさそうな単語として以下の 2 単語を検索単語として決定した。

W_0＝中国、W_1＝メタデータ

よって、プログラムを実行することで出力されたオントロジの経路から、実験目的である潜在単語、潜在単語集合、潜在資料の検索・参照ができる。

5.6.3　実験結果

以下に、共起ネットワークを用いた共起図の出力結果を図 5.19 として示す。

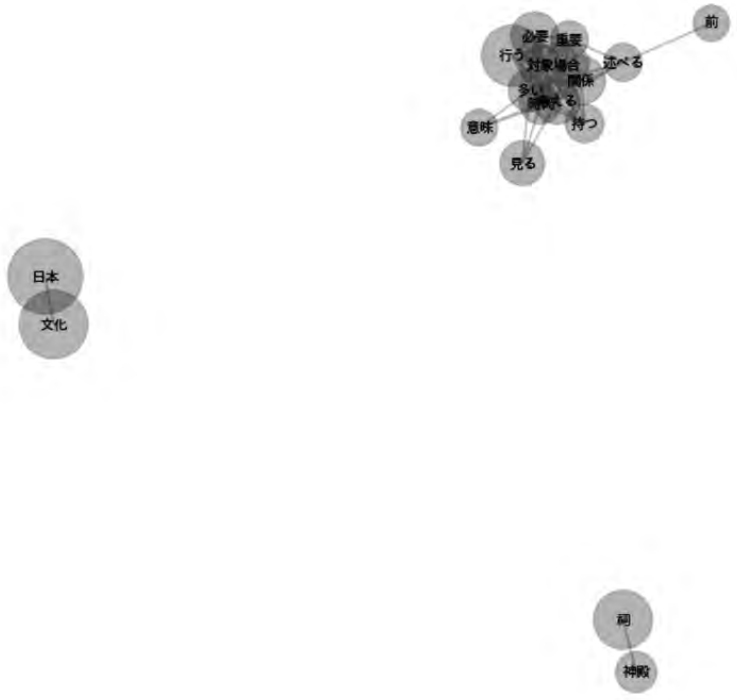


図 5.19　非文字資料 no. 1 から no. 17 による共起図の出力結果

以下に、（W_0, W_1k）、（W_1, W_0i）の候補出力結果を図 5.20 として示す。

上記は（W_0, W_1k）および（W_1, W_0i）の候補を出力したものである。上記の候補の中から、W_0＝中国、W_1＝メタデータとした時の（W_0, W_1k）および（W_1, W_0i）の列のみを取得し出力した。W_0＝中国、W_1＝メタデータと入力した場合の、平均情報量の計算結果を出力した。以下が W_0 の平均情報量、W_1 の平均情報量、（W_1, W_0i）の平均情報量の差分の計算結果である。

以下に、オントロジの経路の検索結果を図 5.22 として示す。

	メタデータ	中国	中心	儀式	写真	利用	前
メタデータ	0.000000	0.000000	0.047619	0.000000	0.071429	0.071429	0.066667
中国	0.000000	0.000000	0.500000	0.153846	0.444444	0.300000	0.500000
中心	0.047619	0.500000	0.000000	0.090909	0.666667	0.590909	0.714286
儀式	0.000000	0.153846	0.090909	0.000000	0.133333	0.062500	0.125000
写真	0.071429	0.444444	0.666667	0.133333	0.000000	0.647059	0.705882
...	...	...	...	...	...	...	...
韓国	0.000000	0.187500	0.217391	0.111111	0.312500	0.400000	0.294118
順	0.000000	0.333333	0.318182	0.222222	0.294118	0.294118	0.352941
馬	0.111111	0.166667	0.363636	0.090909	0.437500	0.437500	0.411765
鬼	0.000000	0.166667	0.095238	0.250000	0.066667	0.066667	0.133333
龍	0.000000	0.250000	0.380952	0.222222	0.375000	0.375000	0.437500

	南	博物館	命	...	都市	里	重要
メタデータ	0.000000	0.111111	0.000000	...	0.000000	0.000000	0.058824
中国	0.600000	0.235294	0.142857	...	0.400000	0.312500	0.611111
中心	0.571429	0.363636	0.190476	...	0.428571	0.363636	0.809524
儀式	0.153846	0.090909	0.166667	...	0.090909	0.200000	0.111111
写真	0.444444	0.352941	0.200000	...	0.352941	0.352941	0.722222
...	...	...	...	...	...	...	...
韓国	0.266667	0.066667	0.000000	...	0.333333	0.230769	0.263158
順	0.428571	0.062500	0.333333	...	0.133333	0.214286	0.315789
馬	0.235294	0.200000	0.300000	...	0.058824	0.285714	0.368421
鬼	0.166667	0.100000	0.200000	...	0.000000	0.100000	0.117647
龍	0.428571	0.062500	0.500000	...	0.307692	0.416667	0.388889

	関係	面	韓国	順	馬	鬼	龍
メタデータ	0.058824	0.076923	0.000000	0.000000	0.111111	0.000000	0.000000
中国	0.526316	0.470588	0.187500	0.333333	0.166667	0.166667	0.250000
中心	0.809524	0.619048	0.217391	0.318182	0.363636	0.095238	0.380952
儀式	0.111111	0.142857	0.111111	0.222222	0.090909	0.250000	0.222222
写真	0.722222	0.588235	0.312500	0.294118	0.437500	0.066667	0.375000
...	...	...	...	...	...	...	...
韓国	0.200000	0.250000	0.000000	0.153846	0.066667	0.000000	0.250000
順	0.250000	0.312500	0.153846	0.000000	0.214286	0.250000	0.454545
馬	0.444444	0.466667	0.066667	0.214286	0.000000	0.100000	0.307692
鬼	0.117647	0.071429	0.000000	0.250000	0.100000	0.000000	0.111111
龍	0.315789	0.400000	0.250000	0.454545	0.307692	0.111111	0.000000

[73 rows x 73 columns]

図 5.20　共起図で使われた（W_0, W_1k）および（W_1, W_0i）の候補一覧

```
w0を入力してください : 中国
w1を入力してください : メタデータ
                中国
メタデータ  0.000000
中国       0.000000
中心       0.500000
儀式       0.153846
写真       0.444444
...             ...
韓国       0.187500
順         0.333333
馬         0.166667
鬼         0.166667
龍         0.250000

[73 rows x 1 columns]
              メタデータ
メタデータ  0.000000
中国       0.000000
中心       0.047619
儀式       0.000000
写真       0.071429
...             ...
韓国       0.000000
順         0.000000
馬         0.111111
鬼         0.000000
龍         0.000000

[73 rows x 1 columns]
W0=中国,W1=メタデータと入力した場合の共起における平均情報量の計算結果を表示します
W0の平均情報量は5.090308634133576bitでした。
W1の平均情報量は2.9977759286244843bitでした。
W0W1の平均情報量の差分は-2.092532705509092bitでした。
```

図 5.21　W_0＝中国、W_1＝メタデータと入力した場合の（W_0, W_1k）および（W_1, W_0i）の候補と計算結果

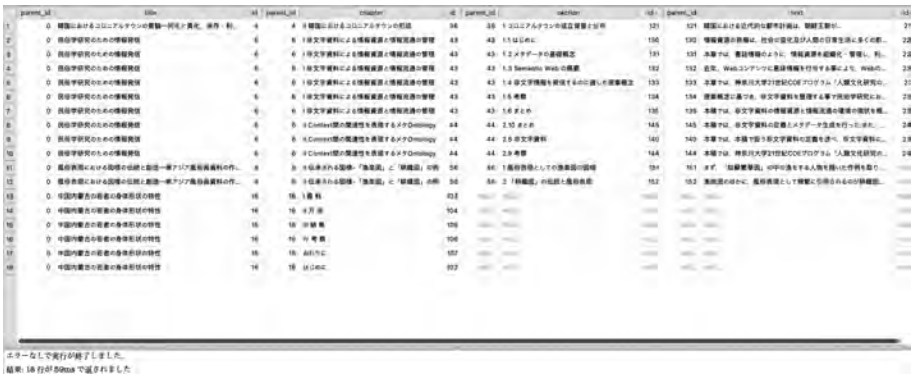


図 5.22　W_0＝中国、W_1＝メタデータで検索した時のオントロジの経路の検索結果

以上の結果から、設計図におけるオントロジの経路は、違うタイトル間を移動している W_0, W_1 を含む経路であるので、上記の図より、経路同士を接続して考えてみると色んなパターンが考えられる。その中で結果の一部を取り上げる。

［中国内蒙古の若者の身体形状の特性］―［民俗学研究のための情報発信］―［非文字資料による情報資源と情報流通の管理］―［メタデータの基礎概念］

上記は、W_0＝中国、W_1＝メタデータで検索した場合のオントロジの経路の一例であることがわかる。上記の（W_0, W_1）のオントロジの出力結果を以下に図 5.23 として示す。

図 5.23　W_0＝中国、W_1＝メタデータで検索した場合のオントロジの経路

この経路のほか、上記の検索結果からは様々な（W_0-W_1）経路が読み取れる。このオントロジの経路は、W_0＝中国は title 層に位置し、W_1＝メタデータは section 層に位置することがわかる。ここで、以下の経路パターン表と比べると、上記のオントロジの経路は、title-titlechapter-section の順でノード接続されているため、no. 6 の経路と同じであることが結果として分かる。

最後に、潜在的な資料を見てみると、図 5.23 の結果から［中国内蒙古の若者の身体形状の特性］―［民俗学研究のための情報発信］この経路上の二つの非文字資料が潜在資料であることがわかる。また最後に、オントロジの経路から外れている潜在単語を見てみると、［中国内蒙古の若者の身体形状の特性］には W_0＝中国の単語が含まれるため、その下層である chapter 層が、今回の（W_0, W_1）のオントロジの経路において外れる潜在単語であると考えられる。よって、今回の図 5.22 の結果より、［Ⅰ資料］、［Ⅱ方法］、［Ⅲ結果］、［Ⅳ考察］、［おわりに］、［はじめに］が潜在単語に該当する。この六つの潜在単語は、［中国内蒙古の若者の身体形状の特性］の潜在資料に属している。また、［民俗学研究のための情報発信］の下層の section 層には W_1＝メタデータの単語が含まれるため、その下層である text 層が、今回（W_0, W_1）のオントロジの経路において外れる潜在単語集合であると考えられる。よって、今回の図 5.22 の結果より、［本章では、書誌情報のように、情報資源を組織化・管理し…］が潜在単語集合に該当する。この一つの潜在単語集合は、［民俗学研究のための情報発信］の潜在資料に属している。なお、この潜在単語の結果はあくまでケーススタディであるためオントロジ経路上から外れる潜在単語は様々な結果が考えられる。以上が、非文字検索の実験結果である。次ページにて、非文字検索における平均情報量、潜在単語、潜在単語集合、潜在資料の結果をまとめて掲載する。

表 5.4　オントロジの経路パターン

no	種　類	経路パターン
1	同じ年報の経路	titile-title
2	同じ年報の経路	chapter-chapter
3	同じ年報の経路	section-section
4	同じ年報の経路	text-text
5	同じ年報の経路	title-chapter
6	同じ年報の経路	title-chapter-section
7	同じ年報の経路	title-chapter-section-text
8	同じ年報の経路	chapter-section
9	同じ年報の経路	section-text
10	違う年報の経路	text-section-chapter-title-title-chapter-section-text
11	違う年報の経路	section-chapter-title-title-chapter-section-text
12	違う年報の経路	chapter-title-title-chapter-section-text
13	違う年報の経路	title-title-chapter-section-text
14	違う年報の経路	title-title-chapter-section
15	違う年報の経路	title-title-chapter
16	違う年報の経路	title-title
17	違う年報の経路	chapter-title-title-chapter
18	違う年報の経路	section-chapter-title-title-chapter
19	違う年報の経路	section-chapter-title-title-chapter-section
20	違う年報の経路	text-section-chapter-title-title-chapter-section

5.6.4　提案システムに対する検索結果

以下実験結果を表にまとめて掲載する。以下に共起における平均情報量の計算結果を表 5.5 に示す。

表 5.5　平均情報量の計算結果

単　語	平均情報量	平均情報量の差分
中国	2.9977759 bit	−2.0925327
メタデータ	5.0903086 bit	

以下にオントロジの経路の一例である出力結果を図 5.24 として再び示す。

【W_0＝中国、W_1＝メタデータの場合】

図 5.24　W_0＝中国、W_1＝メタデータで検索した場合のオントロジの経路

以下に経路パターン表から取り出した no. 6 を表 5.6 して示す。

表 5.6　オントロジの経路のパターン結果

単語 W_0	単語 W_1	経路パターン	経路の検索結果
中国	メタデータ	年報が違う経路	title―title―chapter―section

以下に潜在単語、潜在単語集合および潜在資料を表 5.7、表 5.8、表 5.9 に示す。

表 5.7　潜在単語の出力結果

単語 W_0	単語 W_1	潜在単語
中国	メタデータ	I 資料、II 方法、III 結果、IV 考察、おわりに、はじめに

表 5.8　潜在単語集合の出力結果

単語 W_0	単語 W_1	潜在単語集合
中国	メタデータ	本章では、書誌情報のように、情報資源を組織化・管理し……

表 5.9　潜在資料の出力結果

単語 W_0	単語 W_1	潜在資料
中国	メタデータ	中国内蒙古の若者の身体形状の特性
中国	メタデータ	民俗学研究のための情報発信

上記二つの潜在資料の結果から、資料内容のどこに関連があるか文章の似ている実例を以下に示す。

2.3　神奈川大学 COE の取り組み

現在，神奈川大学 21 世紀 COE プログラム「人類文化研究のための非文字資料の体系化」では，非文字資料の情報共有と情報流通を目指している．COE が保有するデータベース（以下 DB とする）（図書 DB，非文字資料 DB，研究成果 DB）を，他大学や研究機関及び，研究者間で相互に情報提供・情報収集する事によって，情報発信が成されると考える．情報発信の実現には，様々な対象に関する視点からの情報利用が出来る事が求められている．また，利用者に適した電子図書館的な利用環境を作り上げる必要もある．非文字資料の情報共有・情報流通には，プライバシー保護のためのアクセス制御や，著作権保護のための知的財産権管理．情報提供のための課金が含まれる．

図 1 に，非文字資料の情報発信概略図を示す．

図 5.25 「民俗学研究のための情報発信、木下宏揚、2006」

本研究は，神奈川大学 21 世紀 COE プログラム「人類文化研究のための非文字資料の体系化」を「身体技法と感性」から追究する中で，身体技法（体の使い方）が実際の体の形にどうのように反映しているかを知ることを目的として行われた．このような観点から体形

図 5.26 「中国内蒙古の若者の身体形状の特性、芦澤玖美、2006」

オントロジの経路上に含まれる、年報 No. 3 における no. 6、no. 16 の非文字資料は上記実例からも潜在的な関連性はありそうである。

5.6.5　随伴関係を利用した共起図の平均情報量とオントロジの経路の比較

出力されたオントロジの経路と同じ no. 6 のパターン経路は、違う年報同士の経路であることが結果として分かる。さらに、W_0＝中国、W_1＝メタデータと入力した際の平均情量は、W_0 と W_1 で値の開きが大きいことが結果として分かる。そのため比較して考えると、違う資料同士のオントロジの経路では、平均情報量の差分において値に開きがでる（差分が大きくなる）のではないかと考察する。

5.7　むすび

今回は提案システムでは、非文字検索における潜在単語、潜在資料等の出力をするというケーススス

タディを行った。あくまでケーススタディでの評価では、圏論という概念を用いて自然同値である二つの単語を用いることで数値や経路を取るという点で、システム設計図では潜在性や共起性が考慮されていることが理論上まかり通っているのではないかと評価する。また平均情報量やオントロジの経路の出力をすることで、実験の結果のように、潜在単語や潜在単語集合から経路を辿って潜在資料が何かを導き出せたと考える。また今回の提案システムが、従来研究での潜在語の研究の中で、潜在性だけでなく共起ネットワークを用いて共起性も考慮していくという新規性を表現できたと考える。この提案システムが、従来研究に加えて潜在語、潜在資料研究の一助になれば良いと評価する。

年報が違う資料同士のオントロジの経路は潜在性が高いとした場合では、潜在単語の属する潜在資料は、オントロジの経路上に必ず存在すると考えられる。よって潜在資料はオントロジの経路上に存在する2資料のことである。この2資料を潜在資料と呼んで良いと言える。本研究の非文字検索システムでは、2単語（W_0, W_1）のオントロジの経路上に出現する潜在資料やその周辺の潜在単語は、利用者には瞬時に発見できない「資料同士の潜在関係性の発見」という点において役立ち、検索する利用者にとって「利用者の検索傾向に囚われず、資料同士の潜在関係性を提示してあげる」という点で思いも寄らない結果を生み出した。ここで新たに定義する潜在関係性とは、資料同士の資料内容が似つかない場合や、資料同士に対する検索単語もそれぞれ違うのに、資料同士の関連はあるという現象のことである。これにより、ユーザへの資料検索においてよりインタラクティブな表示結果を与えてあげることが可能になったと結論づける。

本研究における今後の課題は二つある。一つ目は、工学的アプローチとして提案した、共起ネットワークとオントロジを利用した随伴関係によって、潜在単語や潜在資料である非文字資料を検索した際に、2単語（W_0, W_1）の決定方法が定まっていないことである。よって、2単語（W_0, W_1）は、今後も様々な単語決定が想定される。これにより、オントロジの経路の検索結果も変化してくる。よって、オントロジの経路における title 層の潜在資料もおのずと変化する可能性がある。そこで（W_0, W_1）の決定方法の基準を定めることも潜在単語、潜在資料を意図的に検索条件で絞り出す上では重要であるため、本研究における今後の課題とする。二つ目は、オントロジの経路において、最適なオントロジの経路は何であるのかという経路の選定基準が定まっていないことである。今回の実験において、オントロジの経路は18行程度と複数出力された。その場合におけるオントロジの経路の選定基準は、2単語（W_0, W_1）を含んでいる。潜在単語が一番多くノード連結されている。また、異なる年報同士の経路で2資料を含んでいる。これらをすべて満たす経路が、最適なオントロジの経路であるといった具体的な選定基準は必要である。最適なオントロジの経路の選定基準を設けることで、より潜在単語、潜在資料を検索する上での判断ができると考える。

参考文献

［1］ 神保理恵、木下宏揚、“民具データベースの RDF 化とオントロジを導入した情報検索システム”、2014年度神奈川大学卒業論文、2014。

［2］ 羽生敏英、木下宏揚、“リレーショナルモデルによるデジタルアーカイブのための民具データベースの構築”2015 年度神奈川大学卒業論文、2015。

［3］ 木下慶子、木下宏揚、“非文字資料に適したディジタルアーカイブの構築”“2006 年度神奈川大学卒業論文”、2006。

［4］“国立国会図書館”、国立国会図書館長、https://www.ndl.go.jp、参照 December, 2022。
［5］“神奈川大学 21 世紀 COE プログラム人類文化研究のための非文字資料の体系化”、神奈川大学、神奈川大学日本常民文化研究所、神奈川大学大学院歴史民俗資料学研究科、http://www.himoji.jp、参照 September, 2022。
［6］“神奈川大学日本常民文化研究所非文字資料研究センター刊行物紹介非文字資料研究（旧：年報）”、神奈川大学日本常民文化研究所、http://himoji.kanagawau.ac.jp/publication/annualreport.html、参照 September, 2022。
［7］丸山宏、“台南道教の符籙について ── 放赦科儀の九龍符命とその歴史を中心に ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［8］浜田弘明、“「渋沢フィルム」撮影地の景観変貌 ── 韓国・蔚山を事例として ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［9］菊池勇夫、“『模地数里』に描かれた松前 ── 長春丸・女商人・馬 ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［10］須山聡、“韓国におけるコロニアルタウンの景観 ── 同化と異化、保存・利用・破壊 ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［11］佐野賢治、“文化情報発信システムとしてのインターネット博物館 ── 大学・地域博物館の連携を中心にして ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［12］木下宏揚、“民俗学研究のための情報発信”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［13］丸山泰明、“文化政策としての民俗博物館 ── 国民国家日本の形成と「国立民俗博物館」構想 ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［14］金貞我、“風俗表現における図様の伝統と創造 ── 東アジア風俗画資料の作例から ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［15］夏宇継、“蘇った納西（ナシ）族東巴（トンパ）教「求寿（チィウショウ）」儀式”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［16］藤永豪、“北京市都心部および郊外農山村の景観変容”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［17］土田拓、“住みつづける意思 ── 紋別市内陸部における畜舎景観の成りたち ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［18］王京、“教会大学と日中戦争 ──「北平私立輔仁大学檔案」（1925-1952 年）から見た戦時下の学生収容 ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［19］彭偉文、“「姑蘇繁華図（コソハンカズ）」に見る清代前期の江南地域における紡織業及びその流通 ── 地方文献に照らして ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［20］川田順造、“感性の人類学のための予備的覚え書き”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［21］廣田律子、長瀬一男、海賀孝明、岡本浩一、“モーションキャプチャを使った芸能比較研究の試み”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［22］芦澤玖美、“中国内蒙古の若者の身体形状の特性”。（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［23］津田良樹、中島三千男、金花子、川村武史、“旧朝鮮の神社跡地調査とその検討 ── 全羅南道、和順郡を中心に ──”、（社）神奈川大学 21 世紀 COE プログラム研究推進会議、2006. 03。
［24］“KHCoder：計量テキスト分析・テキストマイニングのためのフリーソフトウェア”、樋口耕一、https://khcoder.net、参照 October, 2022。

6　研究成果 4：アクセス行列における Latent Channel の検出と評価

6.1　まえがき

近年、多くの企業でファイル保管やデータ共有にオンラインストレージが用いられている。扱うデータには機密情報を含んだものも多くあるため、それらの管理体制が重要となる。[1] こうしたデータを保護する情報セキュリティ対策として、アクセス制御というものが行われている。アクセス制御とは情報の不正利用を防止するために、ユーザに対してあらかじめアクセス権限を設定する方法である。しかし、アクセス権限を設定したにも関わらず、Latent Channel という現象により情報漏洩が発生してしまうことがある。この問題に対して、トピックモデルを用いた情報量を用いて、確率的に Take-Grant モデルの Latent Channel を検出するという先行研究[2]や情報量を用いた Take-Grant モデルのための情報フィルタに強化楽手を用いて利用者の意思を反映するといった先行研究[3]が行われてきた。本研究において、Latent Channel とは Covert Channel と Inference Channel を含むものである。アクセス制御を理論的に表すモデルとしてアクセスコントロールリスト及びアクセス制御行列というものがある。Latent Channel に対してアクセス制御行列を用いたセキュリティモデルにおいては、その情報漏洩の経路を論理学的に分析し、遮断することが可能である。[4] しかしすべての Latent Channel 経路を遮断するのは可用性の観点から現実的ではない。そこで検出された Latent Channel 経路による情報漏洩をトピックモデルを用いた情報量に基づいて評価し、そこに利用者の意思を含めた強化学習を実行することで、情報量および利用者の人間的な観点から危険と判断される Latent Channel 経路のみを遮断し、可用性を維持したまま機密性を向上させるためのシステムを提案する。

6.2　利用者の意思を反映したトピックモデルと強化学習を用いた Take-Grant モデルのための情報フィルタの設計

6.2.1　概念

これはクラウド環境を想定した、自己と他者の通信における Latent Channel のための情報フィルタの先行研究である。Latent Channel の確率的な振る舞いと、人間の意思を強化学習によってバランスを取りフィルタの動作を決定している。この先行研究ではクラウド上での通信を想定するため主体が自己と他者の二つのみである。本研究ではこの主体の数を拡張したアクセス行列における Latent Channel のための情報フィルタを提案する。アクセス行列上の Latent Channel の評価に以下に示す先行研究のシステムを用いる。

6.2.2　システムの流れ

システムの流れを図 6.1 に示す。

6.2.3　対象とする文書

実験で扱う文書群として、英語 Wikipedia の記事データ（2021 年 12 月 1 日付け）を用いている。Supervised Text としてカテゴリーが “Security” の記事（総数 189）を、利用者が所有している文書としてカテゴリーが T から始まる記事（総数 2101685）を用いている。

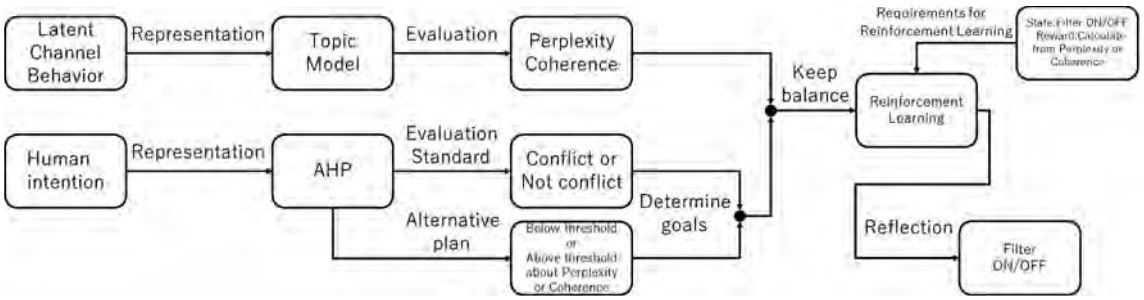


図 6.1　先行研究の Latent Channel 評価システム

6.2.4　LDA 処理

利用者が所有する文書と利用者がセキュリティに設定している文書（Supervised　Text）から辞書とコーパスを作成する。このモデルを用いて、Latent　Channel で流出する文書の Perplexity と Coherence を計算する。本研究ではこの処理を行うプログラム LDA_after_mod.py を define で定義し、Latent Channel を評価するプログラム内で呼び出している。

6.2.5　AHP による閾値に対する優先度の決定

LDA 処理により算出された情報量の、閾値との差に対する利用者の判断を数値化するために AHP が用いられている。閾値はあらかじめ任意に設定されている。選択肢は「閾値以上」と「閾値未満」の二つであり、これらにかかる優先度に従い閾値との差を判断する。判断基準は「相手が競合」と「相手が非競合」の二つである。AHP.ipynb に利用者の判断を入力し、強化学習のプログラムへ数値が受け渡されている。

6.2.6　強化学習

LDA 処理により算出された情報量に対して、AHP に入力した利用者の意思を反映させるために強化学習を行う。この強化学習によりフィルタ ON の状態価値とフィルタ OFF の状態価値がそれぞれ出力される。本研究ではこの処理を行うプログラム P_td_prediction_5kairoop_ave_mod.py，C_td_prediction_5kairoop_ave_mod.py を define で定義し、Latent　Channel を評価するプログラム内で呼び出している。

6.3　アクセス行列における Latent Channel

6.3.1　アクセス行列における Covert Channel

アクセス行列上の Covert　Channel を表すモデルを図 6.2 に示す。S_1 は O_1 に対し Read を持たないので O_1 の内容を知ることが出来ない。しかし、S_2 が O_1 を Read し O_1 の内容を O_2 へ Write することで、S_1 が O_2 を Read して O_1 の内容を知ることが出来るようになる。よって O_1 が S_2 から S_1 へ流出したことになり、これが Covert Channel となる。

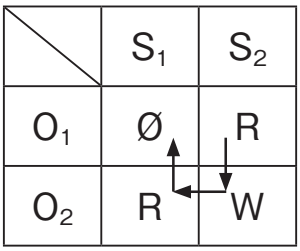


図 6.2　Covert Channel のモデル

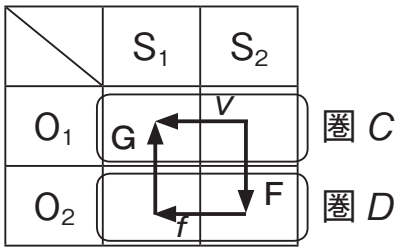


図 6.3　Inference Channel のモデル

図 6.3 は図 6.4（a）の伝搬経路を、同行上のエントリを圏 D、圏 C として可換図式で表したものである。

主体内での情報の伝搬 F、G を随伴関手として、以下の式で表現される概念図である。

$$v = G \circ f \circ F$$

$$\textit{Covert Channel} \triangleq G \circ f \circ F$$

$$\textbf{オブジェクト内容伝搬} \triangleq v$$

6.3.2　アクセス行列における Inference Channel

図 6.3 において、O_2 から O_1 の演繹推論の証明が成立すると解釈する。これを Inference Channel と呼ぶ。

$$v = G \circ f \circ F$$

$$\textit{Inference Channel} \triangleq G \circ f \circ F$$

$$\textbf{演繹推論} \triangleq v$$

6.3.3　Covert Channel と Inference Channel の統合

図 6.3 は Covert Channel と Inference Channel 双方ともに表現する可換図式である。これを Latent Channel と呼ぶ。以上より、Latent Channel は、Read を持たないエントリの同軸に Read を持つエントリがあり、対角に Write を持つエントリがある、辺の長さが可変の長方形で考えること

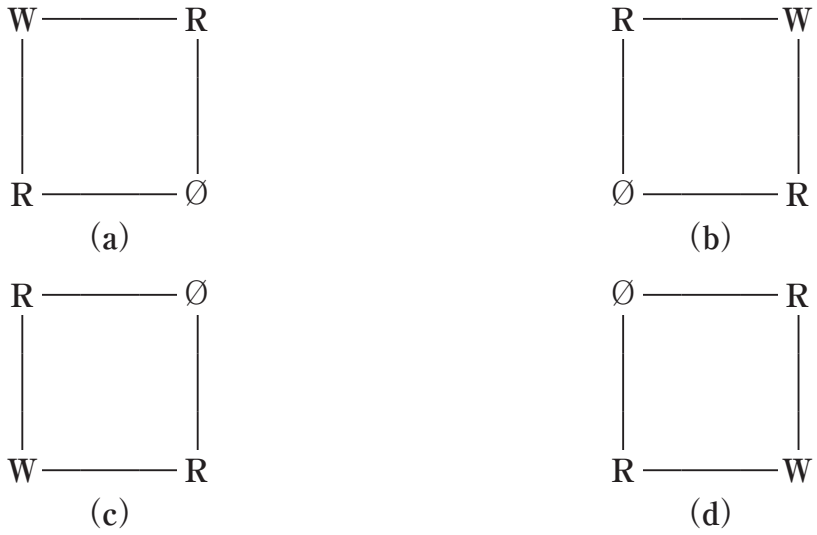


図 6.4　Latent Channel の向き

が出来る。この長方形は図 \ref{fig:square} のように四方向へ拡張することが可能である。

6.4 本研究の概念

本研究の概念は、アクセス行列における Latent Channel のための情報フィルタである。前項においてアクセス行列における Latent Channel のモデルが示された。これにより、アクセス行列上の Latent Channel を検出することが可能となる。検出された Latent Channel を遮断することでアクセス行列の秘匿性を高めることが出来るが、そのすべてを遮断するとアクセス行列の可用性が大きく損なわれてしまうため、遮断する Latent Channel を選択して情報フィルタを行う必要がある。遮断する Latent Channel を選択する方法として、Latent Channel の危険性を評価し、より危険と判断された Latent Channel のみを遮断する。よって、アクセス行列上の Latent Channel の検出と検出された Latent Channel の評価が、本研究の要点となる。

図 6.5 に本研究の概念図を示す。

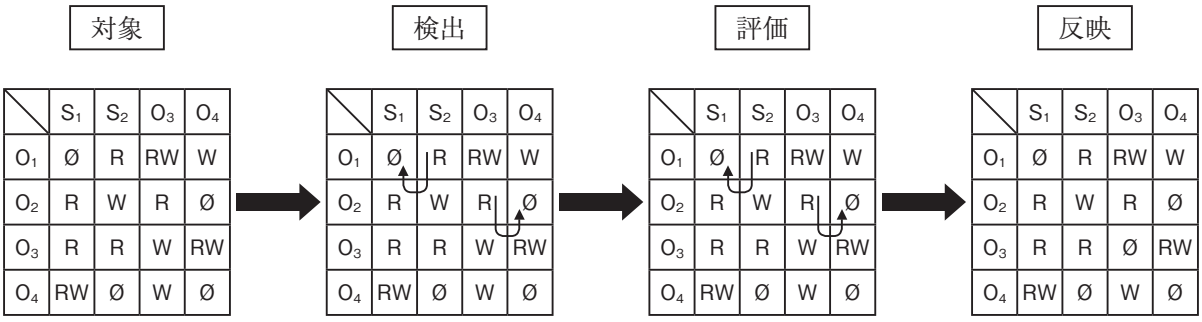


図 6.5 研究の概念図

6.5 アクセス行列上の Latent Channel の検出

図 6.4 に示したモデルで、アクセス行列上の Latent Channel は表現される。アクセス行列上の Read を持たないエントリ（流出先）へ、同じ行軸上で Read を持つエントリ（流出元）から情報が流出するという考え方のもと、Latent Channel を検出するアルゴリズムを考案する。まず流出先候補となる、Read を持たないエントリをリストアップする。一つの流出先に向かう Latent Channel をすべて検出し、それをすべての流出先候補に対して行うことでアクセス行列上のすべての Latent Channel を検出する。一つの流出先に向かう Latent Channel の検出アルゴリズムを図 6.6 に示す。

すべての Latent Channel を検出する流れを以下に示す。

1．Read を持たないエントリ（流出先候補）をリストアップ
2．流出先候補のうち一つを流出先とする
3．流出先の列の主体が Read できる文書をリストアップ
4．流出先と同じ行で Read を持つエントリ（流出元候補）をリストアップ
5．流出元候補のうち一つを流出元とする
6．流出元の列の主体が Write できる文書をリストアップ
7．3 と 6 のリストを比較
8．7 で一致したものが Latent Channel となる

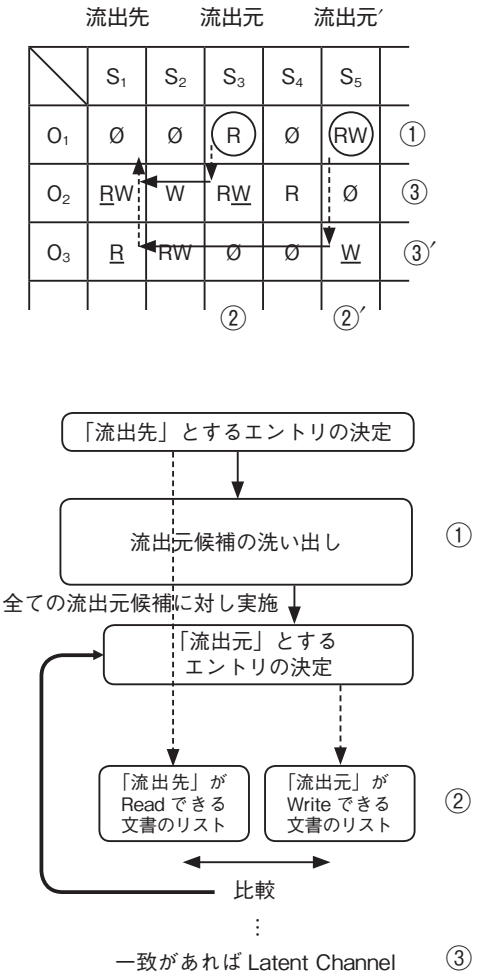


図 6.6　一つの流出先へ向かう Latent Channel の検出

9．5 から 8 をすべての流出元候補に対し実施

10．2 から 9 をすべての流出先候補に対し実施

6.6　Latent Channel の評価

アクセス行列から検出された各 Latent Channel から得られる情報として、「流出する文書」と「どの主体からどの主体へ流出するか」がある。遮断する Latent Channel を決定するため、「流出する文書の情報量」と「主体間の関係」を評価基準とした AHP を構築し、選択肢を「フィルタ ON」と「フィルタ OFF」として各 Latent Channel に対し遮断するかを決定する。Latent Channel を評価しフィルタ動作を決定する AHP の構成を図 6.7 に示す。

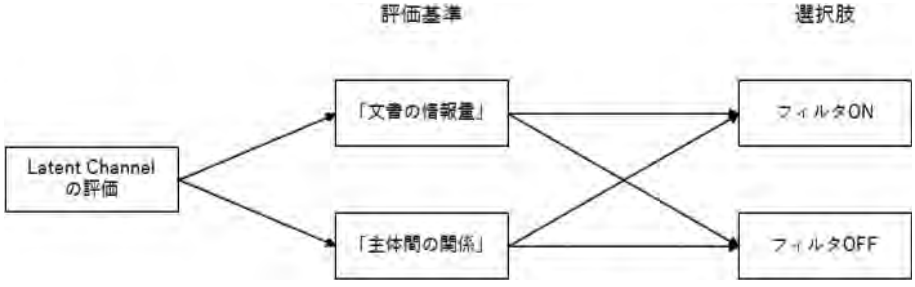


図 6.7　Latent Channel を評価する AHP の構成

6.6.1　流出し得る文書の評価

上述の先行研究のシステムを用いて、トピックモデルに基づいた文書自体の危険性を算出する。強化学習の結果としてフィルタ ON の状態価値とフィルタ OFF の状態価値が算出されるため、この比を選択肢への重み付けとする。

6.6.2　主体間の関係の評価

主体間の関係を反映する情報フィルタを実現するため、主体間に差が存在するような簡潔なモデルを用意する。本研究では、「主体間に役職の差がある」「アクセス行列上の列が離れるほど役職差が大きくなる」という条件のアクセス行列を想定し、主体間の関係を評価する。役職差が大きい主体間の Latent Channel は危険である（遮断するべきである）という判断を、許容可能な差の上限を基準値とした以下の数式で数値化する。

$$2^{(|[\text{流出先の列番号}]-[\text{流出元の列番号}]|-[\text{基準値}])} \tag{6.1}$$

式 6.1 を用いることで、主体間の差が基準値未満の場合 1 より小さくなり、主体間の差が基準値以上で 1 より大きくなる数字が得られる。式 6.1 をフィルタ ON への重み付けとし、フィルタ OFF への重み付けを 1 とする。

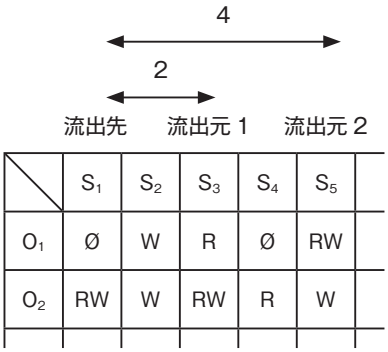
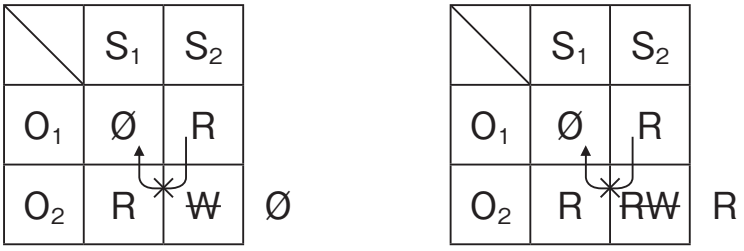


図 6.8　主体間の距離

6.6.3　アクセス行列への反映

Latent Channel の評価でフィルタ ON と決定した Latent Channel を遮断する。Latent Channel を遮断する方法として、アクセス行列上で対象の経路を構成しているエントリを変更することで行う。具体的には、図 6.9 に示すように流出元の持つ Write 権を削除することで行う。



（a）　変更するエントリが W の場合　　（b）　変更するエントリが RW の場合

図 6.9　アクセス行列における Latent Channel の遮断方法

図 6.10 のように同一の流出先と流出元に対して複数の経路が存在する場合には、そのすべてを遮断する。

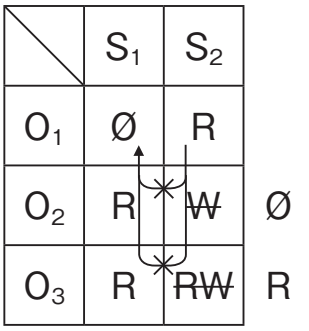


図 6.10　同一の流出先と流出元にて複数の経路が存在する場合

6.7　実験方法

6.7.1　目的

実験の目的を以下に示す。

- アクセス行列から Latent Channel を検出するプログラムの作成とその動作確認
- 検出された Latent Channel を評価しアクセス行列に反映するプログラムの作成とその動作確認
- Latent Channel の評価に対する評価基準の影響を確認する

6.7.2　環境構築

実験環境を以下に示す。Windows 11 Home 22H2, CPU：Intel（R）Core（TM）i3-8100 CPU @ 3.60 GHz 3.60 GHz, Ubuntu：20.04.5 LTS, Python：3.8.8, Anaconda：4.12.0, jupyter-lab：3.3.2

6.7.3　使用データ

使用するデータとして英語 Wikipedia の記事データを用いる。カテゴリーが “Security” の記事を Supervised Text とし、カテゴリーが T から始まる記事をアクセス行列の文書番号に対して割り当てる。データ配列の都合で、記事番号 0〜189 が Supervised Text のものであるため、アクセス行列の文書番号（行数）0〜に対し記事番号 190〜を割り当てている。

6.7.4　LDA 処理

使用データの文書群から Gensim を用いて辞書とコーパスを作成し、LDA のモデルを作成した。

6.7.5　先行研究の AHP への入力

評価基準に対する重み付けは以下のものを用いた。競合：非競合＝10：1、Perplexity について、競合の場合、閾値未満：閾値以上＝10：1、非競合の場合、閾値未満：閾値以上＝0.1：1、Coherence について、競合の場合、閾値未満：閾値以上＝0.1：1、非競合の場合、閾値未満：閾値以上＝10：1

6.7.6　閾値設定

LDA 処理の結果に対する閾値設定は、Perplexity・Coherence の分布より以下のように設定した。Perplexity の閾値：5500、Coherence の閾値：－2.5

6.7.7　主体間の関係の評価式

先行研究と同様に基準値を以下のように設定する。［基準値］＝［アクセス行列の総列数］/2

6.7.8　アクセス行列の生成

実験で用いるアクセス行列は、以下のプログラム Create_matrix.py を用いてランダム生成する Ø→0, W→1, R→2, RW→3 で表すものとし、行数と列数を指定して各エントリを 0〜3 のランダムな数字で埋めることで生成している。

6.7.9　Latent Channel 検出プログラムの動作確認

アクセス行列上の Latent Channel 検出について、アクセス行列上の Latent Channel の検出で示したアルゴリズムに基づいて以下のプログラム Search_channel.py を作成した。このプログラムから各 Latent Channel について（流出先、流出元、流出文書、経路となる行）のタプルがリストで出力される。プログラムの整合性を確かめるために、アクセス行列の生成のプログラムで生成したアクセス行列に対して Latent Channel の検出を実行した。結果を図 6.11 に示す。

```
(keras-2) takagaki-yuma@TY-DTPC:                                $ python test1.py
対象となるアクセス行列：
['Ø ', 'RW', 'Ø ', 'Ø ', 'RW']
['Ø ', 'Ø ', 'Ø ', 'RW', 'R ']
['Ø ', 'RW', 'W ', 'W ', 'Ø ']
['W ', 'Ø ', 'R ', 'RW', 'W ']
['RW', 'W ', 'W ', 'Ø ', 'R ']

検出されたLatent Channel(文書番号,流出先,流出元,経路となる行)：
[(0, 0, 1, [4]), (0, 2, 4, [3]), (0, 3, 4, [3]), (1, 1, 3, [2]), (1, 1, 4, [0]), (1, 2, 3, [3]),
(1, 2, 4, [3]), (2, 0, 1, [4]), (2, 4, 1, [0, 4]), (3, 0, 2, [4]), (3, 1, 2, [2]), (3, 1, 3, [2])
, (3, 4, 2, [4]), (3, 4, 3, [1]), (4, 1, 4, [0]), (4, 2, 0, [3]), (4, 2, 4, [3]), (4, 3, 0, [3]),
 (4, 3, 4, [3])]
```

図 6.11　Latent Channel 検出プログラムの出力

上記のほかにも複数のアクセス行列に対してプログラムを実行し、その結果から Latent Channel 検出の整合性を確認した。

6.8　全体の動作

Latent Channel の検出、評価とアクセス行列への反映を行うプログラム main.py を作成した。このプログラムから、検出された各 Latent Channel に対する評価と、変更後のアクセス行列が出力される。図 6.11 と同じアクセス行列に対するプログラムの出力を図 6.12 に示す。

遮断された Latent Channel と変更されたエントリの対応を確認した。

6.8.1　Latent Channel の評価に関する比較実験

Latent Channel の評価に対する評価基準の影響を確認する。「文書の情報量」と「主体間の関係」という二つの評価基準に対して、それらへの重み付けの比を以下のように変更して実験を行う。

```
遮断されたLatent Channel：
[(2, 0, 1, [4]), (2, 4, 1, [0, 4]), (3, 0, 2, [4]), (3, 1, 2, [2]), (3, 1, 3, [2]), (3, 4, 2, [4]
), (3, 4, 3, [1])]
変更後のアクセス行列：
['Ø ', 'R ', 'Ø ', 'Ø ', 'RW']
['Ø ', 'Ø ', 'Ø ', 'R ', 'R ']
['Ø ', 'RW', 'Ø ', 'Ø ', 'Ø ']
['W ', 'Ø ', 'R ', 'RW', 'W ']
['RW', 'Ø ', 'Ø ', 'Ø ', 'R ']
元のアクセス行列：
['Ø ', 'RW', 'Ø ', 'Ø ', 'RW']
['Ø ', 'Ø ', 'Ø ', 'RW', 'R ']
['Ø ', 'RW', 'W ', 'W ', 'Ø ']
['W ', 'Ø ', 'R ', 'RW', 'W ']
['RW', 'W ', 'W ', 'Ø ', 'R ']
変更されたエントリの座標：
{(0, 1), (1, 3), (4, 2), (2, 3), (2, 2), (4, 1)}
```

図 6.12　Latent Channel の評価とアクセス行列への反映

- 「文書の情報量」:「主体間の関係」＝1：1
- 「文書の情報量」:「主体間の関係」＝10：1
- 「文書の情報量」:「主体間の関係」＝1：10

比較検証のため、すべての条件で図 6.13 のアクセス行列を対象として用いた。

```
(keras-2) takagaki-yuma@TY-DTPC:                                    $ python main.py
対象となるアクセス行列：
['R ', 'RW', 'RW', 'RW', 'W ', 'Ø ', 'RW', 'RW']
['R ', 'R ', 'RW', 'RW', 'R ', 'Ø ', 'RW', 'Ø ']
['RW', 'R ', 'Ø ', 'Ø ', 'Ø ', 'RW', 'R ', 'Ø ']
['R ', 'RW', 'R ', 'R ', 'RW', 'Ø ', 'W ', 'R ']
```

図 6.13　比較実験の対象とするアクセス行列

6.9　結果と考察

Latent Channel の評価を比較するため、各 Latent Channel についての数値を出力させたものを比較する。Blocked とついているものが遮断された Latent Channel である。情報量：及び主体間：の項目は、それぞれの判断基準から選択肢への重み付けを、フィルタ ON/フィルタ OFF で表している。同一のアクセス行列における Latent Channel を評価しているため、検出された Latent Channel の総数と各数値はすべての条件でほぼ同一であり、どの Latent Channel が遮断されているかという点のみが変化している（文書の情報量に関して強化学習が行われているため多少数値が変動する）。

6.9.1　「文書の情報量」:「主体間の関係」＝1：1 の場合

文書番号が同じ Latent Channel については情報量の項目の数値も等しくなっている。遮断された Latent Channel に着目すると、文書番号 2 と文書番号 3 についての Latent Channel であることが分かる。それらの Latent Channel の情報量の数値は 1 以上であり、これは文書番号 2、3 の文書がセキュリティに設定した文書に関連していて流出が危険であると判断されたことを意味する。このことから判断基準の一つである「文書の情報量」の影響が確認できる。

また、文書番号 2、3 の Latent Channel のなかで遮断されていない Latent Channel も存在する。遮断されていない Latent Channel の流出先と流出元の列番号を見るとその差は 1 であり、流出先と流出元の距離が極端に近い場合には、流出する文書が危険であっても遮断されないと考えられる。このことからもう一つの判断基準である「主体間の関係」の影響も確認できる。

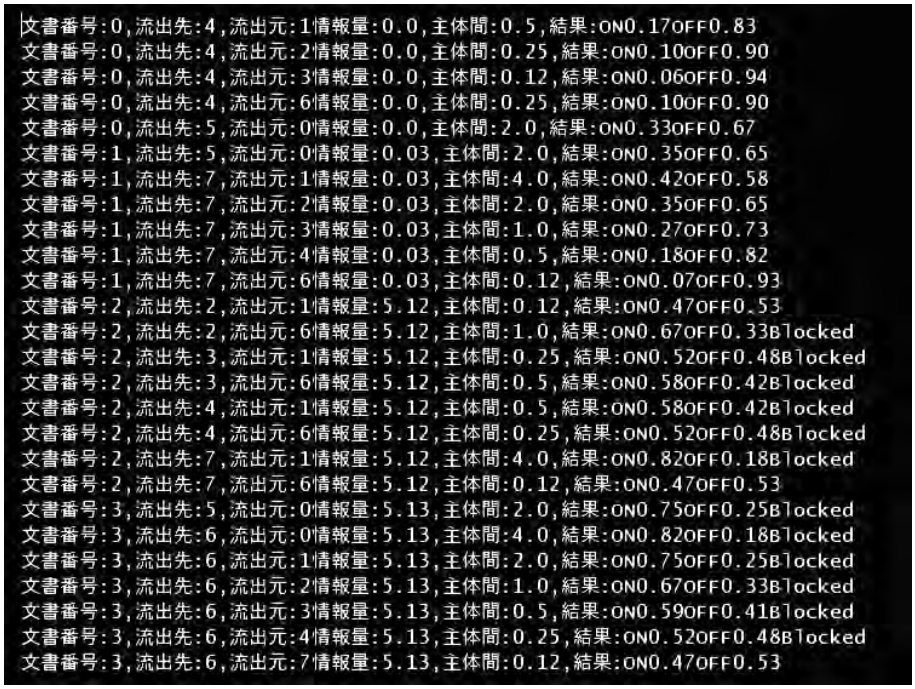


図 6.14 「文書の情報量」:「主体間の関係」＝1：1 での評価

6.9.2 「文書の情報量」:「主体間の関係」＝10：1 の場合

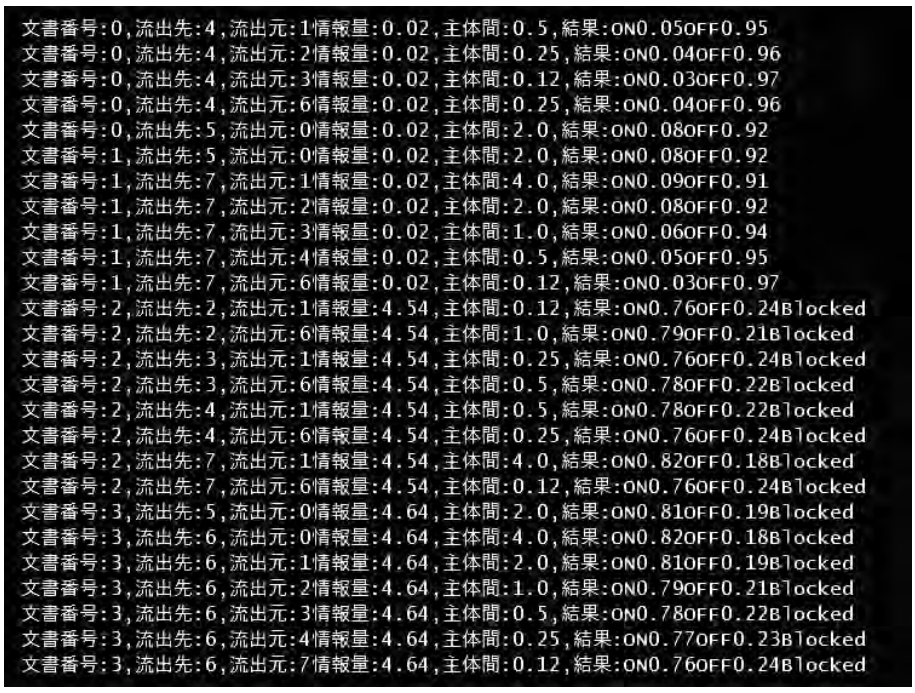


図 6.15 「文書の情報量」:「主体間の関係」＝10：1 での評価

文書番号 2 と文書番号 3 についての Latent Channel がすべて遮断されている。そのため、「主体間の関係」の影響は確認できないといえる。

6.9.3 「文書の情報量」:「主体間の関係」＝1：10 の場合

流出先と流出元の距離が大きい Latent Channel が遮断されていることが確認できる。文書番号：1、流出先：7、流出元：3 の Latent Channel のみ、流出先と流出元の距離が 4 でありながら遮断さ

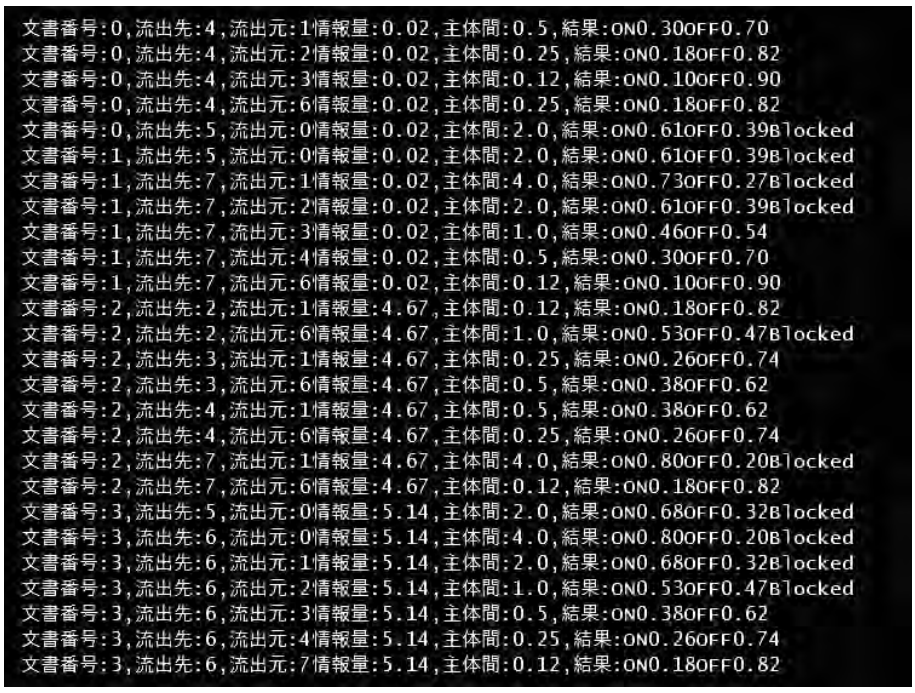


図 6.16 「文書の情報量」:「主体間の関係」=1:10 での評価

れていないが、これは情報量の項目の数値が 1 未満で小さいためであり、「文書の情報量」の影響であると言える。

6.9.4 統括

二つの判断基準に基づいて Latent Channel の遮断が決定されていることが確認できた。

判断基準への重み付けの比を変更することで、遮断される Latent Channel の傾向を選択することが出来ると言える。

6.10 むすび

実験結果より、本研究で提案したアクセス行列上の Latent Channel の検出と評価、及びアクセス行列への反映を実現できたと言える。先行研究では、Latent Channel の評価に関して、文書の情報量に対する強化学習の結果が拮抗した場合にフィルタ動作を判断しかねるという課題が提言されていた。これについて本研究では、主体間の関係という新たな評価基準を導入することにより、アクセス行列のモデルにおいて流出する文書の情報量以外の判断基準を提案することが出来たと考える。ただし本研究で示した主体間の関係は行列上の距離を用いた簡素なモデルであり、他にも様々な主体間の関係の評価方法が存在すると思われる。また、Latent Channel を評価する AHP の評価基準である「文書の情報量」と「主体間の関係」について、それぞれから選択肢への重み付けとする数値のとりうる範囲が異なっている。本研究で示した AHP は評価基準 2、選択肢 2 の AHP であるため一対比較行列が成り立っているが、評価基準を増やすことを考慮すると選択肢への重み付けのスケールを統一するような数式を考える必要がある。

参考文献

［1］ 国民のためのサーバーセキュリティーサイト“情報セキュリティの概念｜組織幹部のための情報セキュリティ対策｜企業・組織の対策｜総務省”、https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_02.html, 参照 Jan. 7, 2023。

［2］ 佐野公亮、“情報量に着目した Take-Grant Model によるアクセス権の管理”、神奈川大学 2020 年度卒業論文、2020。

［3］ 苅谷優太、“利用者の意思を反映したトピックモデルと強化学習を用いた Take-Grant モデルのための情報フィルタの設計”、神奈川大学 2021 年度卒業論文、2021。

［4］ 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講演論文、2018。

7 今後の課題と展望

非文字資料の研究とその成果の利用の過程における情報の体系化と検索、新しい知見の発見およびセキュリティの確保と著作権の管理に機械学習やブロックチェーン技術などを適用し、研究者と利用者を支援するための基盤技術を構築した。目的達成のため要素技術の開発は、当初の目標にそった成果が得られた。一方、実際の非文字資料への適用は限定的な事例に着手を始めた段階である。したがって、非文字資料研究全般にわたって、研究成果で得られた技術を応用していくことが期待される。今後の展望としては、第五期までの成果を生かし以下のような発展的な研究を行う。(1) 画像などのコンテンツを識別するための固有の情報の知覚ハッシュに基づく著作権管理システム。(2) 画像に様々な情報を埋め込む電子透かしやステガノグラフィにおいて画質と耐性を両立した手法を構築する。(3) 情報を体系化し関連付けを行うためにオントロジーとトピックモデルなどを組み合わせた検索手法や論文推薦システムや新しい知見の発見支援手法の構築と年報などの研究成果の動向の視覚化などを行う。(4) アクセス権の矛盾や情報間の推論に起因する情報漏洩を防止するためにトピックモデルを用いて非文字資料の文書間の関連性を抽出しアクセス制御に適用する。(5) テクストに内在する潜在性を確率論的アプローチと決定論的アプローチの関連から捉える概念装置の研究。

謝辞

2022 年度の研究については一部 JSPS 科研費 JP22K12036（2022〜2026 年度基盤研究（C）加工編集に耐性のある深層学習に基づくメッセージダイジェストと著作権管理への応用）の助成を受けた。