修士論文

検索履歴認証

Search History Authentication

指導教員　　山口利恵　特任准教授

東京大学大学院 情報理工学系研究科 電子情報学専攻

48-156438　　宮野 祐輔

平成 29 年 2 月 3 日提出

内容梗概

近年，不正アクセスなどによって起こる詐欺や情報流出などの被害に対応するため，様々な認証手法が開発されてきている．しかしいずれの手法でも短所や欠点を完全に排除することはできておらず，完璧な認証手法は存在していない．そのため複数の認証要素を組み合わせることで互いの欠点を補完する多要素認証が注目されている．類似した性質の認証手法では同様の欠点を抱えており補完することが難しいので，できるだけ性質の異なる手法を組み合わせることが望ましい．

本稿では多要素認証の一要素として利用できる認証手法の候補の中でも，特に検索履歴を用いた個人認証手法について述べる．検索履歴はプライバシーや個人属性推定などの観点からは盛んに研究されてきたものの，認証に利用できるのかという点は明らかにされておらず，実際のデータを用いた分析も十分に実施されていない．ただ先行研究からユーザのプライバシー情報を検索履歴から解析できることが知られているため，認証するのに必要なだけの情報を含むと推察される．また検索履歴は検索時間や検索クエリなど多種多様な情報を含んだデータであるので，ユーザの本人性を多面的に評価できると考えられる．

本研究では検索履歴認証を多要素認証の一要素として利用する場合にどのような条件が求められるのか考察した．さらに実際の検索履歴データを分析することで考察の妥当性を確認した．

目次

Chapter 1　序論

本章では，本稿で扱う検索履歴認証の背景について述べ，以降の内容についての導入を行う．インターネットを介した通信やサービスの普及拡大に伴って増加してきた不正アクセス等のセキュリティ被害に対して，多要素認証と呼ばれる認証形態が注目を集めているため，この一要素として検索履歴認証が有効であると考えられる論拠について概説する．

1.1　不正アクセスと認証方式

近年あらゆるサービスの電子化が進んでおり，銀行の決済やインターネットショッピング，行政上の届け出など多くの手続きがインターネットを介して実現できるようになってきた．また IoT（Internet of Things; モノのインターネット）などと呼ばれるように，あらゆる機器をインターネットに接続して遠隔操作したりセンサーログを記録させたりと，物理的に直接操作することなく家や職場の状態を管理できる技術の発展も進んでいる．

このようなインターネットを介した操作性の向上にともない，不正アクセス等の被害も増大している．たとえば平成 27 年にインターネットバンキングで不正に送金された被害額は 30 億円を突破している [2]．それらの多くはパスワードを推測して本人になりすましたり，ユーザを欺いて意図しない操作へと誘導したりするなど，既存の認証方式の脆弱性を突いたり逆手に取ったりするものである．

そのため生体認証に代表されるような新しい認証技術を次々に開発し安全性や不正アクセスへの耐性を高めようという試みが盛んである．しかし開発が進んだ現在においても，実際に利用されている認証方式の多くは従来から用いられてきた ID とパスワードによる認証方式であり，新しい認証方式は導入コストやユーザの心理的抵抗などの要因で十分に進んでいないのが現状である [3]．一方でユーザのセキュリティ意識はさほど高くはなく，推測されやすいパスワードを使用する，同じパスワードを複数のサービスで使い回すなど，セキュリティ向上に伴って発生する追加的な負荷を嫌う傾向にある．そのためパスワードが推測され有名人のアカウントが不正アクセスの被害に遭ったり，“1234”, “password” など安易によく用いられるパスワードを総当たりで試行するパスワードリスト攻撃などで多くのアカウントが不正アクセスされたりする例が後を絶たない [4]．したがってセキュリティレベルの向上を考えるにあたっては，認証技術の単純な精度や再現率のみではなく，導入に伴う問題点やコスト，想定される攻撃への耐性などを総合的に考慮する必要がある．

1.2　様々な要素を組み合わせた認証手法

本節では上述した認証における利便性と安全性というトレードオフの問題に対して，近年注目を集めている多要素認証が有効な対策となると捉えここに述べる．また多要素認証の一形態として，リスクベース認証，そしてライフスタイル認証についても概説する．本節の内容については改めて第 2 章で詳細に述べる．

多要素認証　多要素認証とは，複数の認証要素を組み合わせてユーザの本人性を評価し認証する方式のことである．個別の認証要素単体では何らかの欠点や脆弱性が存在するため，すべてのセキュリティリスクを回避するのは不可能である．そのため複数の認証要素を組み合わせて相互に補完させようというのが多要素認証のポリシーである．多要素認証はすでに銀行取引やクレジットカードの決済など高いセキュリティレベルを必要とする場面で導入されているが，ユーザへ複数回認証を要求するという負荷がネックとなっている．したがってセキュリティレベルをそこまで要求されない一般的なサービスでは，デバイスにワンタイムパスワードを送信する簡易的な 2 要素認証が採用されることが多い．しかしデバイスへのワンタイムパスワード送信は結局デバイスの安全性が担保されている必要があるため，結局のところ所有物認証の域を出ない．盗難・紛失された端末でパスワードを記憶させるオートログインなどの機能を利用していた場合，そもそも不正アクセスを認識できない可能性も存在する．このため，多要素認証を構成する認証要素はできるだけ独立しており，様々な観点からユーザの本人性を評価できることが望まれる．ある一要素認証を突破することで他の認証要素をも直接的ないしは連鎖的に突破できてしまえば，多要素認証の意味は大きく損なわれる．そのため多要素認証について考えるときには，どのような要素をどのように組み合わせて利用するかが重要になる．

リスクベース認証　多要素認証の一形態として，様々なユーザ情報から総合的にリスク値を算出して追加認証の要否を判断するリスクベース認証が挙げられる．リスクベース認証は潜在的に収集できる行動履歴やアクセス環境などの情報を利用して認証するため，ユーザの負荷が追加認証時だけと小さく利便性が高い．リスクベース認証が利用されるのは基本的にユーザが何らかの認証手法でログインしたあとである．ログインしたユーザのアクセス環境，サービスの利用状況，挙動の履歴など様々な観点からユーザらしくない行動パターンを分析してリスク値を算出する．そしてそのリスク値が閾値より高くなった場合にはユーザにログイン時に使用した以外の追加認証を要求し，改めてユーザが正規ユーザであるか確認するという方式である．リスクベース認証においてはリスク値の算出が最も重要な点であるが，こちらも多要素認証として様々な要素から算出されるのが望ましい．実際に運用されているリスクベース認証の多くは端末情報や IP アドレス，位置情報やブラウザ情報などを基準にしているものが多い．リスクベース認証で様々なリスクを加味したリスク値算出を行うためには，これ以外の認証要素，なおかつそれらの情報と依存関係にない要素も加えていくことが有効であると考えられる．

ライフスタイル認証　さらに複合的な認証形態として，ライフスタイル認証 [12] と呼ばれる認証方式が提案されている．ライフスタイル認証とはユーザ側にパスワードのような明示的な認証動作を要求するのではなく，潜在的に収集できる行動履歴からユーザの習慣性を解析することでユーザの本人性を検証しようとする試みである．人間の行動習慣という新たな評価軸を設けることでより総合的に認証できると考えられている．その一方でライフスタイルは他の要素に比べて他者からの影響やゆらぎが大きく，実際に認証可能な段階まで解析するためには様々なアプローチを採る必要がある．ライフスタイル認証を視野に入れた先行研究においては，いずれもその取得するデータに対してゆらぎの小さい習慣性を分析したり，ゆらぎを吸収できるような手法を開発したりするなどして認証可能な要素であると導いている [9, 10].

1.3　検索履歴を利用した認証

検索履歴にはユーザの属性情報が多く含まれており，多くの先行研究によってプライバシー保護の必要が訴えられてきた．検索行動は電子メールや SNS への投稿などと異なり公開することを前提としないため，ユーザの行動特性や属性がより露骨な形で表れるであろうと想定される．そのため検索履歴の分析がより強いプライバシーの侵害に繋がる可能性は高く，過去には実際に公開された仮名処理済みの検索履歴から個人特定に至った例も報告されている．

これらの先行研究に基づけば，検索履歴には多くのプライバシー情報が含まれているため検索履歴を利用してユーザの個人認証が実現できるのではないかと考えられる．なおかつ先行研究で挙げられたプライバシー情報の多くがユーザの明らかな個人情報であるが，検索履歴には行動パターンなどの潜在的な情報も含まれているため，属性推定ではないユーザの推定にはこれらの情報も利用することができる．その上検索履歴はすでに広く利用されているサービスの副産物であるため，新たにデバイスを導入したりユーザに認証のための手続きを要求したりする必要がない．ユーザが普段から慣れ親しんでいる情報源を認証に利用できるというのは負荷の面から見て極めて有利な条件であるといえる．

よって本稿では，検索履歴からユーザの行動パターンを学習して認証するべく，その可能性について研究ならびに実験を行った．検索行為自体はユーザの本来行いたい動作ではなく，そのための手段として残る履歴情報である．そのため，行動パターンが類似していたり，あるいは真似ようとしていたりする悪意ある攻撃者の振る舞いに対しても普段とは異なる傾向であると判断し適切なリスク値を算出するための重要な要素と成り得ると考えられる．具体的な動作だけではなくそれ以前の予備動作まで含めて認証情報とすることで，悪意ある振る舞いを制限する働きも見込まれる．　しかし検索行動は日常の生活習慣としては周期性に乏しく，同一ユーザであってもそのゆらぎは大きいために本人性を評価するのは既存のデバイス認証などと比較すると困難である．そのため検索履歴からユーザのゆらぎを吸収して定常的に本人性を評価できる指標や特徴量を設計する必要があると想定される．そのため本研究では実際の検索履歴を用いて実験を行い，指標や特徴量の有効性やそれらの導入の妥当性について検証した．

1.4　本稿の構成

以下第 2 章では本章で述べた認証手法の現状や履歴情報からの属性推定など，検索履歴認証に関係した関連研究を紹介する．そして第 3 章では検索履歴の構成や検索履歴認証の立ち位置など，以降の内容を理解するために求められる背景知識について述べる．第 4 章で本稿における検索履歴認証へのアプローチについて説明する．具体的な処理の内容や認証の流れなどについてもこの章内で示す．第 5 章ではユーザ適性指標と呼ばれる，ユーザの検索履歴認証への適性を評価する指標を複数提案し，当該指標およびユーザ適性指標自体の有効性や妥当性について検証する．第 6 章では検索履歴認証がどの程度の精度で認証できるのか実際の検索履歴データを用いて検証する．第 7 章で第 5 章・第 6 章の結果を受け，検索履歴認証自体の有効性や実用性について議論する．第 8 章で本稿を結論付ける．

Chapter 2　関連研究

本章では，検索履歴認証を考えるにあたって参考例となる関連研究について紹介する．

まず第 2.1 節では認証として捉えるにあたって，既存の認証方式や新たに提案されている認証形態がどのような特徴や脆弱性を持つのか，そしてそれらの認証方式と検索履歴認証がどのように結びついているのか先行研究を挙げながら述べる．また第 2.2 節では，検索履歴以外の履歴情報からユーザの属性推定やユーザ特定を行っている先行研究について触れ，検索履歴認証が採るべき手法や手順の参考例として挙げる．

2.1　認証

本節では既存の認証方式について説明する．従来の認証方式は大きく以下の「知識認証」「所有物認証」「生体認証」の 3 種類に分けられる．

知識認証

本人のみが知っている情報に基づいて認証する方式である．パスワードや PIN，秘密の質問などが該当する．特殊なデバイスなどを用いないために汎用性・コスト面ともに優れていて，幅広く用いられている．一方で外部へ流出したり推測されたりリスクなどが高く，攻撃を受けやすいという面もある．人間の記憶量には限界があるため，同一のパスワードを複数のサービスで使い回す・推測されやすいパスワードを使用する・パスワードを手帳やメモに記載して管理するなどユーザがセキュリティに対して十分に高い意識を持っていない場合リスクが増大することも考えられる．実際の調査でも 93.1%のユーザがパスワードを複数のサービスで使いまわしていたり，44.2%のユーザがパスワードを手帳やノートにメモしていたりするという調査結果が得られている [5]．また不正アクセス行為の手口の内 79.5%がユーザのパスワード管理の甘さにつけ込んだものという結果も報告されており，知識認証ではユーザの意識が欠けている場合大きなセキュリティリスクに直面することとなる [6]．

所有物認証

本人のみが持っている物体によって認証する方式である．IC カードやトークン式のワンタイムパスワードなどが該当する．実在する物体であるため管理面では知識認証に比べ安全性が高いものの，偽造や盗難などのリスクが存在する．また実在する物体を所持する必要があるため，ユーザへの負荷が高く幅広いサービスで使用を求めるのは困難である．

生体認証

本人の生体的特徴を用いて認証する方式である．指紋や虹彩，静脈や顔認証などが該当する．生体認証に用いられる生体的特徴の多くが人それぞれ固有で不変の特徴であるため，なりすましなどの他者からの攻撃に対して耐性が強く，高い精度で認証可能である．一方で生体認証には特殊なデバイスを必要とするため導入コストが高い．また生体的特徴であることから，もし偽造された場合に自身の特徴を変更することが困難であること，心理的抵抗があって一般的に受け入れられづらい受容性の問題などが存在する．

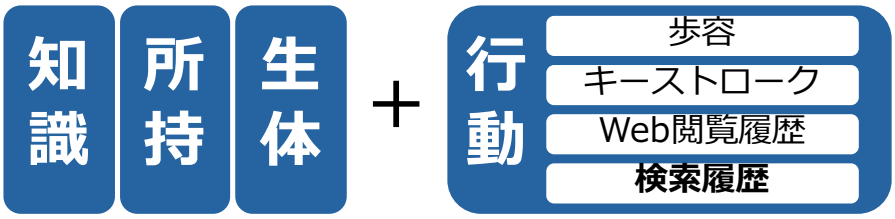

図 2.1: 既存の三要素と行動認証.

いずれの認証方式でも短所や欠点が存在するため，完璧な認証手法というものは存在しない．したがって現在では利用目的や求められるセキュリティレベルに応じていずれかの認証方式を選択し，弱点に関しては注意を換気したり負担を増加させたりするなどして受け入れているのが実情である．

2.1.1　多要素認証

多要素認証とは，複数の認証方式を組み合わせることで，認証システムの安全性や利便性を向上させる認証方式のことである [7]．単一の認証方式のみを用いた認証システムの場合，そのシステムの安全性は当該方式の特性に大きく依存する．現在広く用いられているパスワードによる認証はパスワードの漏洩や安易なパスワードの設定などのリスクがあり，単体でのセキュリティ強度には課題が残る．

一方多要素認証では複数の認証技術を用いているため，一部の認証方式に脅威が生まれたり，適切に動作しなくなったりした場合でもシステム全体として認証の安全性を維持することができる．現状広く利用されている多要素認証の形態として，認証する際にあらかじめ登録されたスマートフォンなどの端末にワンタイムパスワードを送信し，その入力をもって認証を完了するという帯域外トークンを用いるものが挙げられる [8].

しかし一方で多要素認証の弱点として，精度を上げるために要素を増やせば増やすほど個別の認証に要するコストが増大するという問題がある．セキュリティコストの上昇は結果としてユーザがセキュリティのレベルを下げ，全体の安全性が低下する要因になりうる．したがって多要素認証の要素技術として，ユーザへの負担が小さい行動認証などの要素を検討する必要がある．

2.1.2　行動認証

行動認証とはユーザの行動特性を用いた認証手法のことである．代表例としては物理的な行動に基づく歩容認証，ハードウェアを利用する際の特徴に基づくキーストローク認証，そしてソフトウェアの利用履歴にそして Web 閲覧履歴認証などが挙げられる．近年ではスマートフォンや活動量計などのモバイルデバイスが広く普及したため，それらの端末から得られた活動量 [9] や Wi-Fi アクセスポイント情報 [10] を用いた認証も提案されている．行動認証はユーザの行動特性を利用するため，パスワードを記憶したりデバイスを保持したりする必要がない．そのためユーザに対する負荷が小さく，多要素認証の要素技術として近年研究が盛んに行われている．

リスクベース認証

行動認証の一形態として，ユーザの行動特性や利用環境などからリスク評価を行い，一定以上のリスクが想定される場合に追加的な認証を行う**リスクベース認証**が普及している．リスクベース認証は通常通りにサービスを利用している場合には認証プロセスが発生しないため，認証を要求される回数が増えてしまうという多要素認証の弱点を補いうると期待されている．

実際に運用されているリスクベース認証の多くは端末情報や IP アドレス，位置情報やブラウザ情報などを基準にしているものが多い．すでに認証によって確かにユーザ本人からのアクセスであるということが確認されたアクセスのログをデータベースに管理しておき，そのログデータからユーザのアクセス環境が取り得る変動を分析して求めておく．そして新たにアクセスのリクエストがあった場合，そのリクエストに含まれる属性情報からユーザの現在のアクセス環境を特徴として抽出し，事前に求めたユーザのアクセス環境変動と比較する．ユーザのアクセス環境が登録されている，あるいは許容可能な変動幅以内であれば認証状態を維持し，一定の許容幅を超え著しく異なるアクセス環境からのリクエストに対しては新たに別要素での認証（前述した帯域外トークンなどによる認証）を求めるというものである．別要素での認証が成功した場合にはそのログデータもデータベースに保管され，次回以降のリクエストでは正常にリクエストを受け付け，追加的な認証を求めることはしない．また近年ではキーストローク認証やマウス操作パターン認証を取り入れたリスクベース認証モデルも提案されている [11].

ライフスタイル認証

検索履歴は本来認証に用いるために収集されたデータではなく，ユーザの日々の行動を記録したものである．したがって検索履歴を用いた認証を実用のサービスとして導入した場合，ユーザが認証目的で新たにデータを生成する必要はなく，通常通りの生活を送っていれば認証に必要なデータが揃うこととなる．このようにユーザが明示的に認証のための動作を行ったりデータを生成したりする必要なく，日々の生活パターンから認証を行う認証方式のことをライフスタイル認証という [12]．ライフスタイル認証は多要素認証における認証コストの増大という問題を緩和する効果が期待できる．

2.2　履歴情報からの属性推定手法

本節では，履歴情報から本人の属性を推定する手法について関連研究を挙げる．第 2.2.1 小節では検索履歴から特定のユーザ属性を推測した研究を，第 2.2.2 小節では文章からその著者を特定する著者同定という研究について取り上げる．

2.2.1　検索履歴とプライバシー

本小節では検索履歴からユーザのプライバシー情報を推定した研究について取り上げる．研究対象となる検索履歴は一般の研究者が手に入れることは困難であるため，主に以下の 2 種類のデータが利用されることが多い．

1. 検索エンジンサービスを提供している会社が自社のデータを利用する例
2. 公開されたデータセットを利用する例

特に 2 で挙がったデータセットとして AOL が 2006 年に公開した検索履歴データが利用されることが多い．この AOL の検索履歴データセットについては詳細を第 2.2.1 小節にて後述するが，すでに一般公開を撤回したデータであるため研究に用いることへの倫理的な問題が指摘されている．

年齢，性別，住所の推定

Jones らは，自社の検索履歴から検索クエリで用いられた単語を分析することでユーザの年齢，性別，住所を推定した [13]．分析の結果得られた年齢，性別，住所の推定情報を利用して，ユーザの身元特定が可能であるか検証している．この実験に使用されたデータセットは Yahoo! が保持しているユーザのプロフィールと検索履歴を突き合わせたものである．ユーザのプロフィールは全件で 6650 万件取得したが，実験に際してはプロフィールの記載事項や取得した 79 日間の検索状況から 74.4 万件まで絞り込んだ上で実験を行った．

年齢推定はクエリに含まれる単語の，正規化された Bag-of-Words (BoW) を用いた機械学習によって推定されている．全データの 10%を抽出してラベルを付与したものをトレーニングデータとして，SVM による教師ありの回帰分析を行った結果，年齢推定の誤差は平均で 7.0 歳となった．

性別推定は年齢と同じく，クエリに含まれる単語の BoW を用いた 機械学習によって推定された．その結果テストデータに対して 83.8%の精度で性別を判定できた．結果から考察すると，男性が “NFL”, “ESPN”, “golf” などスポーツに関連する単語を，女性が “bridal”, “makeup”, “yoga” など結婚や美容法などに関連する単語を異性と比べて多く検索していることが分かった．

住所推定についてはアメリカの郵便公社が使用する郵便番号（ZIP コード）を対象としている．クエリに含まれる地名などを分析した結果，54.1%の確率でユーザの ZIP コードを 3 択にまで絞り込むことができた．

Jones らは検索履歴に対する攻撃として **trace attack** と **trace attack** を挙げている．trace attack とは，匿名化された検索履歴情報から検索したユーザの個人情報を明らかにする攻撃手法のことである．trace attack はユーザ属性の分析を利用した攻撃であり，その手法は後述する研究で紹介するものと同一か，類似したものである．具体的にはユーザの住所，年齢，居住地などを，クエリに含まれる情報から推定するものである．検索履歴を介したプライバシー侵害への対策として検索元である自分のユーザ名や ID を匿名化する手法 [14] や匿名化に利用できるツール [15, 16] も存在するが，自らの氏名や電話番号などを検索するとたとえ匿名化されていても直接的にプライバシー侵害を行うことが可能である [17]．また多くのユーザが自らの個人情報が含まれた検索をしていることが知られており，こうしたプライバシー侵害は特定のユーザにのみ限られるというものではない [18, 19]．

一方 person attack とは，事前知識としてユーザの情報を保持している攻撃者が，当該ユーザによる検索クエリを推定するという攻撃手法のことである．事前知識には公にされている性別や年齢，SNS などのプロフィールデータや，公開していない個人間の会話の盗聴内容や行動観察などで得られた知見などが挙げられる．同一のクエリで検索を行うユーザが多ければ k-匿名性 [20] の観点から身元が判明する可能性は低いが，特徴的な検索クエリを使用すると身元が判明するおそれがある [21]．また異なるクエリの組み合わせによっては同一のクエリで検索するユーザの数は減少するため危険性は増加する．

健康状態の推定

Biega らは，クエリに含まれる単語からユーザが現在どのような状態にあるのか，確率的に求める手法を開発した [22]．実験では AOL の 3ヶ月間の検索履歴データに対して，各ユーザの全検索クエリを確認し，アルコール依存，鬱，妊娠のいずれかの状態にあると判断した場合，そのユーザに対して状態ラベルを付加した．その後事前に用意した特定単語との共起関係を元に，検索クエリに含まれている単語からユーザの健康状態についての確率を計算した．その確率に基づき，各ユーザの健康状態を推定した．

実験結果として，各状態に対しての精度はアルコール依存では 60%，鬱では 67%，妊娠では 50%であった．一方で再現率は 75%，33%，83%であった．鬱状態の精度が高く再現率が低いのは，実験に用いた対象単語が他の 2 つに比べるとより専門的で，鬱状態でない人が検索しづらかったためと考えられる．一方で妊娠の精度が低く再現率が高いのは，妊娠していない人でも検索しやすい単語が多く対象単語に含まれていたためだと考えられる．

ユーザの本人性分析

検索履歴からユーザ属性を推定されるリスクを軽減させるため，ノイズとなる検索クエリを混ぜる手法が存在し，そのためのツール [23, 24] も配布されている．この個人情報保護手法はクエリ難読化と呼ばれている [25]．Gervais らは，このクエリ難読化の有効性を検証するために，検索クエリ同士の関連性を用いた実験を行った [21]．そのために Linkage Function という概念を導入し,「同じユーザによる検索クエリであれば関連性が存在し，ランダムに付加されるノイズクエリであれば関連性が薄れるために両者は区別できる」と主張した．この主張を証明するため，Gervais らはクエリの内容のみではなく，検索された時刻や検索結果のクリック数などの情報を含めて解析している．時刻情報やクリック数など検索内容から独立したユーザの特性を表す特徴量を**行動的特徴量 (Behavioural features)**，クエリや訪問先のサイトの意味内容からユーザの興味関心を表現した特徴量を**意味的特徴量 (Semantic features)** としている．これらの特徴量を総合的にランダムフォレストで評価し，ユーザ本人のクエリかどうかを判定している．

実験には AOL の検索履歴データを用いている．クエリ難読化の手法は，クエリ難読化ツールとして代表的な TrackMeNot を利用した場合と，他のユーザの検索クエリを混ぜた場合の 2 種類で実験している．その結果いずれの場合においても，本来のクエリとダミーのクエリを判別するのには時間情報が重要であることが示されている．しかしこの結果はノイズとなるクエリがランダムないしはユーザの検索行動とは無関係に挿入されたことによって不自然な時間感覚で履歴に残っているためであると考えられる．そのためユーザの検索とノイズとなる検索が同居する今回のシチュエーションではなく，一定時間攻撃者によって検索行動が乗っ取られていた場合などには有効に機能しない可能性も考えられる．

2.2.2　著者同定

著者同定とは，著者が不明である文章の書き手を推定する手法のことである．著者同定自体の歴史は古いが，文献の特徴量を数値として算出し分析を行う統計学的手法が本格的に用いられるようになったのは 19 世紀ごろである．このような研究を計量文献学と呼ぶ．計量文献学が始まった当時では 1000 語未満の文章から著者同定を行うことは難しいと考えられていたが，計算機の性能向上や機械学習などの新規手法開発に伴い，数百語からなる文章でも高い精度で著

者同定が可能になってきている [26].

著者同定は小説や詩などの文学作品のみを対象とするのではなく，近年ではサイバー犯罪対策としてメールや SMS などの電子メッセージを対象とするように変化してきた．このような電子メッセージは文学作品に比べて文字数が少なく，文章のフォーマットも定まっていないことから，既存の手法では十分に効果を発揮しないものもあった．しかし一方で絵文字や時刻など，各メッセージに固有の特徴を数値化して分析することで一定程度の精度を得られるようになった.

以下では Twitter[1] 上におけるツイートの著者同定を行った関連研究を紹介する [26].

ツイートの著者同定

Layton らは Twitter 上でつぶやかれたツイートを分析することで，ツイートをしたユーザの推定を行った．この実験に用いられたデータセットは Twiiter のユーザ 14000 名の 200 ツイートを収集し，その中からランダムに抽出されたユーザのツイートからなる．著者同定するにあたって利用した特徴量は，一般の著者同定においても広く用いられている n-gram ($n = 2, 3, \cdots, 7$), そしてツイートに特有な「リプライ」および「ハッシュタグ」の情報である.

著者同定の精度を検証するため，50 人のユーザを抽出し，各ユーザのツイートから学習してユーザを推定する実験を行った．全ツイートの中から 20 ツイートをテスト用として残したうえで学習した場合，56%の確率でユーザを推定することができた．なおリプライ情報は精度に対して一定程度の寄与があったものの，ハッシュタグについてはほとんどユーザ情報を含まないという結果が得られた.

また，学習に使用するツイートによってもその精度は大きく変化し，おおよそ 120 以上のツイートを用いて学習した場合には精度が 70%前後を記録することが分かった.

[1] https://www.twitter.com/

Chapter 3　準備

本章では，第 4 章にて行う手法提案に先立ち，検索履歴や検索履歴認証，その構造やデータの有用性など提案手法の議論にあたって必要な周辺知識を説明する．

3.1　検索履歴

3.1.1　概要

検索履歴とは，ある一定期間においてユーザが行った検索行動の集合である．多くのユーザが情報を得る手段として検索行動を行っている．検索は様々な端末やサービスで広く一般的に使われており，インターネットの利用や情報へのアクセスと密接に結びついている．検索は以前より Web サイトへのアクセス参照元の大部分を占めており，ソーシャルネットワーキングサービス (SNS) が普及した近年においてもサイトアクセスの 4 割ほどが検索からのアクセスである [27]．このことから，検索行動がユーザが興味のある事柄について情報を取得する手段の代表格の一つとなっているといえる．

検索履歴はユーザが興味や関心によって能動的にアクションを起こした結果の履歴情報であるため，行動パターンをよく反映したデータであると考えられている．そのため検索履歴に対する研究は様々な形で行われているが，そのうち代表的なものを以下で例示する．

ユーザの意図理解 [28–30]
検索結果に対する満足度を向上させるためには，ユーザがどのような意図を持って検索したかを十分に理解，あるいはユーザごとに表示結果をカスタマイズする必要がある．検索クエリデータには検索したユーザが最終的にどのページへ遷移したのかが記録されているため，検索クエリとクリック先の関係性をデータマイニングによって明らかにして，関連性の強いクリック先へのリンクを上位に表示したり，ユーザごとに異なる結果を表示したりする研究が行われている．

クエリ推薦 [31–33]
よく知らない単語について検索するユーザにとって，正確にクエリを入力しなければその単語についての望む結果が得られないということであれば，検索サービスの満足度は低下する．また検索する概念自体が既知であったとしても，入力ミスや名称の変更などで思い通りの結果が出てこないのは不便である．そのためクエリ内容とクリック先のコンテンツ，入力ミスを訂正するような一連の入力などを学習によって分析し，よりユーザにとって望ましいクエリの候補を提示するような研究が行われている．

クエリ再構成 [34]
検索を行う際に，ユーザが当初入力したクエリに応じた検索結果が望む結果でない場合がある．このときユーザはクエリを書き換えて再試行することで望ましい結果を得ようとする．これをクエリ再構成というが，クエリ再構成にはどのようなパターンが存在するのか，どのパターンが効果的なのかなどを多くのユーザの検索履歴から評価を行う研究が行われている．

行動ターゲティング広告 [35]

新聞や CM などの従来の広告では対象となる全ユーザに対して画一的に広告を配信してきたが，広告内容に興味の無い多くのユーザにまで配信してしまうためにクリック率も低く効率が悪かった．しかしインターネットを介した広告配信では，検索履歴や Web の閲覧履歴などからユーザの興味や関心を推定しパーソナライズされた広告を配信することでより広告効果を高めようという研究が行われている．

3.1.2　検索履歴のデータセット

検索履歴は検索サービスのログとして生成されるデータのため，検索サービスを保持していない一般の研究者が入手することは難しい．協力者を募って日頃の検索履歴を収集・提出させることも技術的には可能だが，集められる人数が小規模にとどまってしまう，極めてプライベートな内容を含むために協力者が現れにくいという障壁が存在し容易ではない．そのため検索サービスを提供している会社内の研究でない限りは，公開されているデータセットを利用するのが一般的である．中でも代表的な検索履歴データセットが AOL によるデータセットである．

2006 年に AOL は，ユーザ約 65 万人分の検索履歴を研究向けとして一般公開した [36,37]．検索ログには仮名化されたユーザ ID，検索クエリ内容，検索時刻が含まれていた．ユーザが検索結果のリンク一覧からいずれかを選択した場合，そのリンク先のドメインと表示順位も情報として含まれていた．仮名化は行われていたものの，検索クエリの匿名化処理は十分でなかったため，何人かのユーザについては分析の結果個人情報に相当する属性を抽出することができた．中には具体的な身元まで特定されたユーザが実名でメディアに登場したことで関係者が処分される事態に発展した．

AOL の検索履歴公開以降，研究用のデータとしての検索履歴は世界でもほとんど公開されることはなくなった．日本では 2015 年，Yahoo! JAPAN が国立情報学研究所の開催するワークショップに対して検索クエリデータを無償提供した [38]．データは十分な匿名加工がなされており，ワークショップで設定された研究課題に関連性の高い検索クエリが抽出されているため，この中から特定のユーザを識別するのは困難である．一方で今回のデータセットは特定の研究課題に特化したものであり，なおかつワークショップの参加者に限定的に公開されたものなので，一般に公開された汎用的に使用できる検索履歴の大規模データセットは貴重である．なお後述するように本稿の実験でも Yahoo! JAPAN の検索履歴データを利用しているが，このワークショップに提供されたデータとは別物である．

3.1.3　データ構造

検索履歴の要素となる検索行動を $e : \{u, t, q\}$ と表現する．このとき u はユーザの識別子であり，ユーザ ID や MAC アドレスなどがこれに相当する．t は検索を行った時間であり，q は検索の際に入力した文字列（検索クエリ）である．検索履歴にはこの他にも Cookie 情報や IP アドレスなどが含まれることがあるが，本稿では時刻および検索クエリ以外の情報については対象外とした．理由については後述する．

以上より，ユーザ U による検索履歴は，e を用いて以下のように表される．

$$S_U = \{e_1, e_2, \cdots, e_n\} \tag{3.1}$$

このとき履歴長は n である．また本稿では検索履歴を単独のユーザによるものであり，その順序は検索時刻順にソートされているとして扱う．

3.1.4　本稿におけるデータセット

本節では実験に用いたデータセットの詳細について述べる．

本研究では，Yahoo! JAPAN[1] で検索された検索履歴データを用いて実験した．対象として Yahoo! JAPAN ID（以降，YID と省略する）でログインしているユーザのうち，2016 年 4 月 27 日から 7 月 26 日までの 91 日間において毎日 1 件以上検索したユーザの検索履歴を収集した．実験に用いるにあたってユーザを 1000 人ランダムにサンプリングした．今回取得した検索履歴データには仮名化された YID，検索に用いたデバイスの Cookie および種別，検索日時，検索クエリが含まれている．

Cookie と YID は 1 対 1 に対応しておらず，複数の端末から同じ YID によって検索されたり，逆に同一の端末から複数の YID を用いて検索されたりすることがある．本研究では端末を複数所持するユーザや，目的に応じて YID を使い分けるユーザを考慮して，YID をユーザ単位として用いた．

実験に使用するデータとして，各ユーザの 1 日分の検索クエリから名詞を抽出しクエリ文書を作成した．このとき実験に使用する doc2vec が単語の位置に基づいて学習するモデルであるため，クエリ文書は Bag-of-Words 形式ではなく名詞の出現する順番を保持したリスト形式とした．形態素解析には Yahoo! JAPAN が提供している形態素解析ツールを用いた．

本実験における処理では Python，機械学習用の Python ライブラリである scikit-learn[2]，ベクトル空間モデル用の Python ライブラリである gensim[3] を用いた．

なお，先述したように検索履歴データに含まれている YID は仮名化されており，ユーザ本人を特定することはできない．また Yahoo! JAPAN の外部へと検索履歴データの持ち出しはしておらず，実験はすべて Yahoo! JAPAN 内部のサーバにて分析が完結している．本稿に記載する実験結果はすべて，本人特定に繋がる YID や Cookie，検索クエリなどを含まないことを確認された統計的なものであり，ユーザのプライバシーを侵害しないような形で掲載されている．

3.2　検索履歴認証の概要

検索履歴認証は，検索履歴からユーザの行動パターンを分析して認証する行動認証の一つである．登録された検索履歴と，認証時に提示される認証サンプルとしての検索履歴を比較し，その類似性を評価することでユーザが登録された本人であるか確認する手法である．検索行動単体であると情報量も極めて限られており認証は困難であると考えられるため，原則として検索履歴認証では一定期間の検索行動を集約した検索履歴を用いる．そのため検索履歴認証の適用としては，ログインの際にパスワードや指紋を提示するような認証の形態ではなく，ユーザの行動履歴を記録してユーザの本人性を評価するリスク値を算出するリスクベース認証が考えられる．検索履歴は多種多様な情報を含み，またユーザが無意識的に行っている行動の履歴であるため，リスクベース認証においてユーザの本人性，リスク値を評価するにあたって有効な指標と成り得る．そのため本稿では，リスクベース認証を検索履歴認証の最も有力な用途の一つとして捉え，検索履歴認証がリスクベース認証の要素として求められる要件を満たすことを目標として設定した．

検索履歴認証の全体像を図 3.1 に示す．まず登録フェーズにおいて，ユーザの検索履歴から行動パターンを分析しテンプレートを作成する．認証リクエストがあったときには，ユーザ

[1] http://www.yahoo.co.jp/
[2] http://scikit-learn.org/
[3] https://radimrehurek.com/gensim/

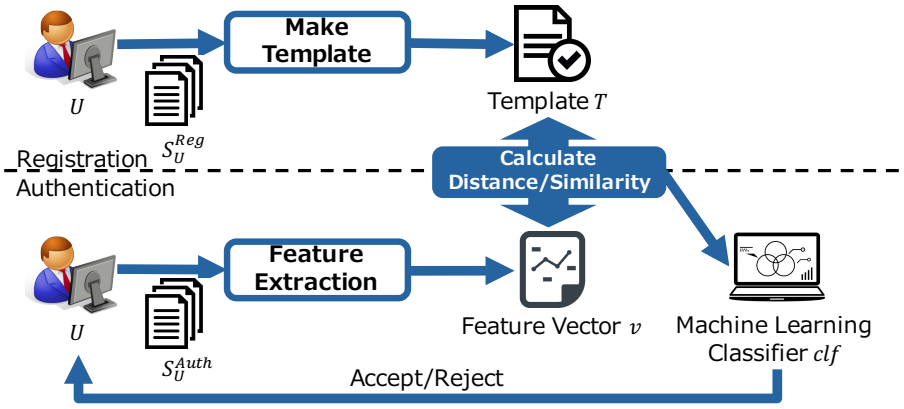

図 3.1: 検索履歴認証の全体像.

から提出されたないしはサーバ側で保持していた直近の検索履歴から得られた特徴ベクトルをテンプレートと比較し，登録パターンとの類似度を算出する．その類似度から機械学習などによって生成された判別器を用いてリクエストしたユーザが本人かどうか判断させ認証する．特徴ベクトルの算出や類似度を含めて判別器に計算させることも考えられる．

検索履歴を用いた行動認証は，今まで考案されてきた行動認証の手法と比較して以下の様な優位性がある．

特別なデバイスを持つ必要がない

行動認証に利用するために新たなセンサやそれを備えたデバイスを開発しても，それが広くユーザに利用されなくては肝心のデータを収集することは難しい．しかし検索はすでに様々なサービスのなかで用いられており，ユーザが行動認証のためにわざわざ改めて導入する必要がなく負荷が小さい．

多様なデバイスで収集できる

検索はコンピュータやスマートフォン，タブレットなど，様々なデバイスで利用されている．これにより特定のデバイスを保持しなければならないという制約が緩和され，ユーザの行動をよりシームレスに追跡することができる．

分析のノウハウが多数存在する

今まで利用されてこなかったセンサ情報や履歴データを分析する場合，分析に用いる特徴量や手法を一から検討する必要がある．一方で検索クエリはクエリ推薦 [31] や検索の意図推定 [29] など，認証以外の分野で広く研究されており，分析のノウハウが蓄積されている．

ユーザ本来の性質を強く反映している

検索行動は SNS での投稿などとは異なり，基本的に秘匿される内容である．そのためユーザ本来の興味が反映される可能性が高く，より強く本人性を表すデータであると考えられる．

多様な属性情報が含まれている

検索履歴にはユーザの使っているデバイスの種別，Cookie，IP アドレスなどのように所有物の属性を示す情報のほか，検索した時間，ならびに検索クエリなど多種の属性情報

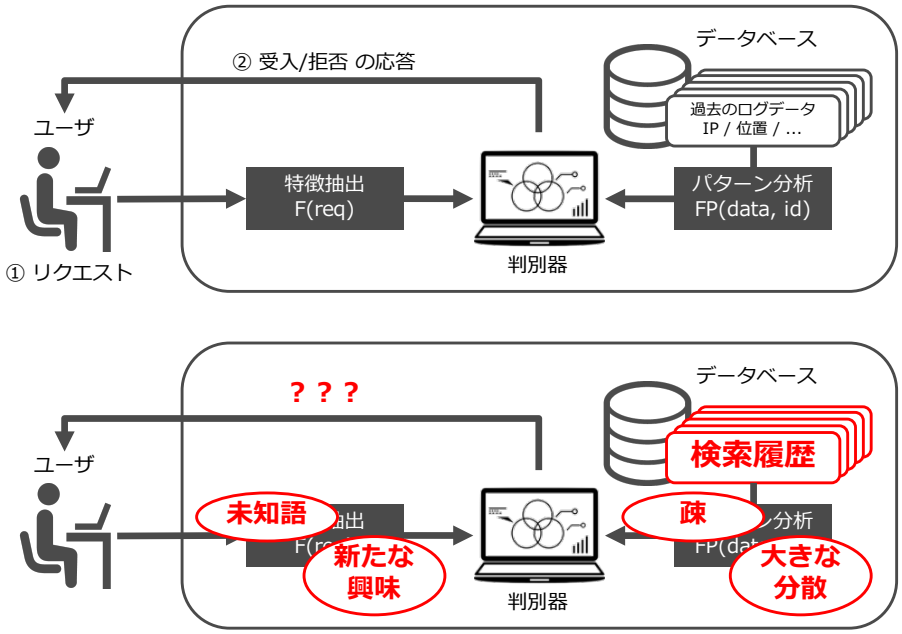

図 3.2: リスクベース認証との比較.

が含まれている．これらの情報は組み合わせることで全体の認証精度を高めたり，特定の情報源に対する攻撃への耐性を強めたりすることができる．

3.2.1　リスクベースとの比較

行動認証の一形態として，ユーザの行動特性や利用環境などからリスク評価を行い，一定以上のリスクが想定される場合に追加的な認証を行う**リスクベース認証**が普及している．リスクベース認証は通常通りにサービスを利用している場合には認証プロセスが発生しないため，認証を要求される回数が増えてしまうという多要素認証の弱点を補いうると期待されている．

実際に運用されているリスクベース認証の多くは端末情報や IP アドレス，位置情報やブラウザ情報などを基準にしているものが多い．すでに認証によって確かにユーザ本人からのアクセスであるということが確認されたアクセスのログをデータベースに管理しておき，そのログデータからユーザのアクセス環境が取り得る変動を分析して求めておく．そして新たにアクセスのリクエストがあった場合，そのリクエストに含まれる属性情報からユーザの現在のアクセス環境を特徴として抽出し，事前に求めたユーザのアクセス環境変動と比較する．ユーザのアクセス環境が登録されている，あるいは許容可能な変動幅以内であれば認証状態を維持し，一定の許容幅を超え著しく異なるアクセス環境からのリクエストに対しては新たに別要素での認証（前述した帯域外トークンなどによる認証）を求めるというものである．別要素での認証が成功した場合にはそのログデータもデータベースに保管され，次回以降のリクエストでは正常にリクエストを受け付け，追加的な認証を求めることはしない．また近年ではキーストローク認証やマウス操作パターン認証を取り入れたリスクベース認証モデルも提案されている [11].

検索履歴を用いた認証は形態としては行動認証にあたるため，リスクベース認証への適用が考えられる．リスクベース認証として捉える場合，事前の検索履歴から学習したユーザモデルとの類似度を算出し，ユーザが行った検索行動のリスクとして評価する必要がある．しかし現在一般的なリスクベース認証と検索履歴を用いた認証とで大きく異なる点のひとつとして，

時間経過に伴うゆらぎが大きい点が挙げられる．ログインする端末に基づくリスクベース認証であれば，今まで利用したことのない端末から操作する機会というのは毎日のように行う検索ほどは多くないため，新たな端末を利用する度に追加的に登録するという操作が大きな負荷とはならない．一方で検索行動というものは時間経過や外的刺激によって大きく変化するので，どの程度のゆらぎであれば許容するないしは拒絶するのかという判断が困難である．

そのため検索履歴を用いたリスクベース認証を実現するためには，こういったゆらぎをどうやって吸収するか，あるいはどのような評価指標を設ければゆらぎに左右されないユーザの本人性を評価できるかを考えなければならない．本研究でのゆらぎ吸収に関するアプローチについては第 4.4 節に詳しい．

Chapter 4　検索履歴認証

本章では今回提案する検索履歴認証の内容について説明する．第 3 章で述べた一般的な検索履歴認証に対して，本研究で扱うデータの特徴量や処理方法，認証手順などについて説明する．

4.1　検索履歴における特徴量

本節では検索履歴における特徴量について述べる．1 回の検索行動に含まれる情報は極めて少なく，また検索行動自体が散発的であるために個別の検索行動同士の関係をそのまま表現することは難しい．したがって検索行動から計算可能な特徴量を用いて検索行動の類似性を評価する手法が一般的である．本稿では検索履歴から計算可能な特徴量を以下の 3 種類に分類する．各特徴量種の詳細は以下に述べる．

4.1.1　入力傾向

入力傾向とは，検索する際に文字列をどのように入力するかという傾向である．検索する際に入力される検索クエリ文字列は，同様の検索を行う場合でもユーザの入力習慣によって大きく変化する．その代表的な例として文字種（e.g. 猫，ねこ，ネコ，neko）や表記揺れ（e.g. ユーザ，ユーザー），そしてスペースを入れる割合が挙げられる [39]．日本語では通常，英語など他の言語と異なりスペースによって文字列を区切る分かち書きを行わない．しかしより詳細な検索をしたい場合には，複数のキーワードをスペースで区切って検索することが推奨されている [40]．そのため検索行為に熟達しているユーザであればスペースで区切ったクエリによる検索が多く，反対に不慣れなユーザや大まかな検索をしたいユーザであればスペースを含まないクエリによる検索が多くなると考えられる．この考えに基づき，全検索クエリのうちスペースを含まないクエリの割合を特徴量とすることがあり，単一クエリ率（SQR; Single Query Rate）と呼称される．単一クエリ率はユーザの検索熟達度合だけでなく，デバイスに応じて変化することもある．スマートフォンなどで広く用いられている音声入力による検索の場合，スペースを含まない検索クエリで検索されることが多く，単一クエリ率は小さくなる傾向がある．

その他の入力傾向として以下の特徴量を例示する．

文字長
: 1 クエリあたりに含まれる文字数の平均．

単語長
: 1 クエリあたりに含まれる形態素の数の平均．英語など分かち書きをする言語ではおおむね下記するクエリ長と等しくなる．

クエリ長
: スペースによって区切られた文字列の個数．単一クエリ率はクエリ長が 1 となるクエリの割合である．

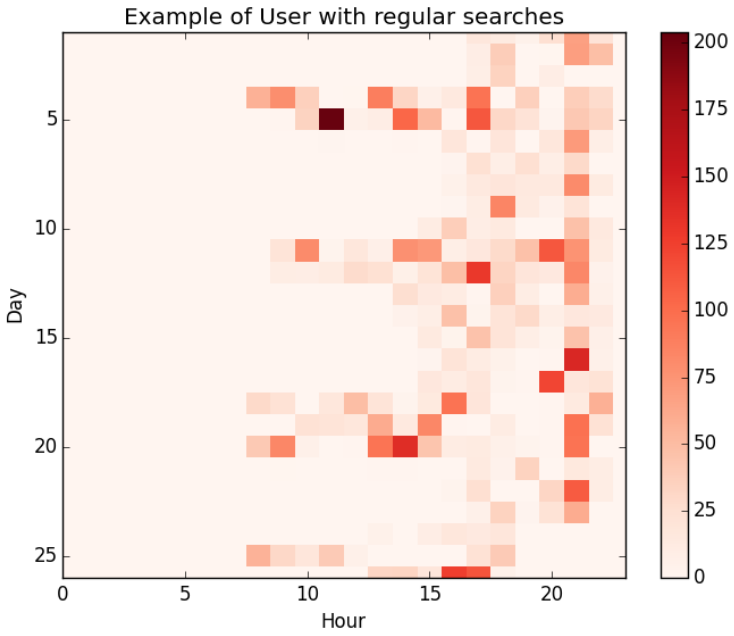

図 4.1: 習慣的な検索行動を取るユーザの検索時間ヒートマップ（2015 年 7 月分）．横軸が 24 時間，縦軸が対象期間の日付を表しており，各グリッドの色が濃いほど当該時間により多く検索していることを示す．

4.1.2　検索行為傾向

検索行為傾向とは，どのような状況で検索するかという傾向である．検索クエリ以外の情報から取得できる検索行為傾向の特徴量として，使用しているデバイス，検索した日付や時間，位置情報などが挙げられる．検索行為傾向は既存のリスクベース認証で用いられている特徴量に最も近く，機械的に判定する指標として有効であると考えられる．

以下では検索行為傾向の一つとして，検索時間について述べる．図 4.1 に習慣的な検索行動を取っているあるユーザの検索時間ヒートマップを示す．この図からは当該ユーザが時間に関して一定の規則性を持った検索行動をしてることが分かる．このユーザは平日であれば 17 時台，休日であれば 8 時台から検索行動を開始していることが読み取れる．よって基本的には 5 日間（平日）→2 日間（土日）の習慣がグラフにも表れているが，海の日を含む 3 連休であった 7 月 18 日〜20 日は祝日である月曜日も休日として 8 時台から検索行動が行われている．

このように特に検索履歴に関しては，曜日ごとに検索する時間や時間帯について規則性を持つユーザが一定数存在する．そのため検索行為傾向を考える際には曜日や時間帯によっての行動パターンの変化を考慮する必要がある．

4.1.3　意味傾向

意味傾向とは，どのような検索内容であるかという傾向である．意味傾向については自然言語処理からのアプローチが採用されることが多く，代表的な特徴量として頻出語や BoW，TF-IDF や内容のジャンルなどが挙げられる．しかし検索履歴は通常の自然言語と異なって独特の文法で入力されることが多く，文脈も検索クエリからだけでは評価が難しい．このため既存の特徴

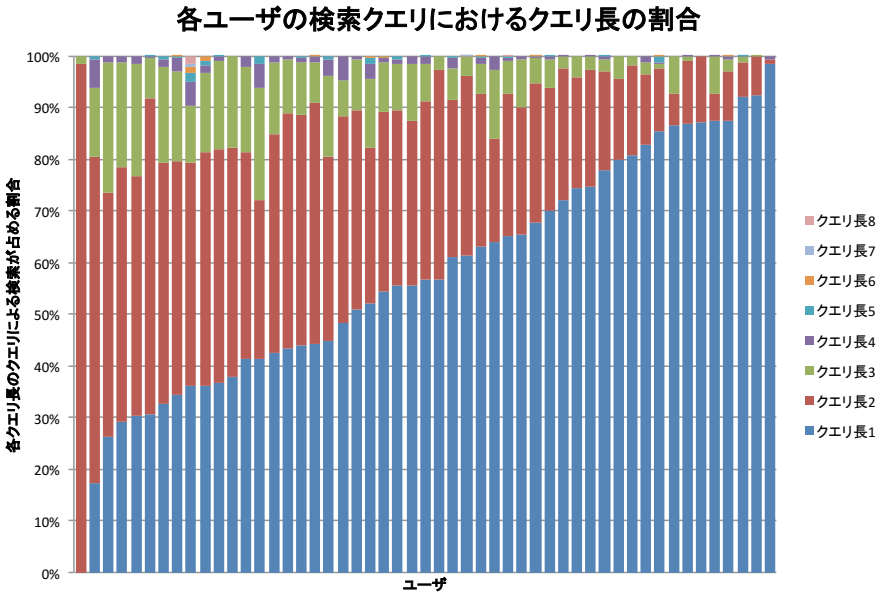

図 4.2: 各ユーザのクエリ長の分布 [39].

量の有効性は信頼できるものとは言えず，実際の検索履歴に適用して検証する必要がある．

4.2　データ処理

本節では今回使用した検索履歴から得られる特徴量とその計算手法，またそれらの取捨選択について解説する．

4.2.1　単一クエリ率

単一クエリ率は第 4.1.1 小節でも述べたように，全検索クエリのうちスペースを含まないクエリの割合である．ユーザごとにスペースを入れる割合というのは大きく異なっており，そのユーザの本人性を表す指標の一つとして有効であると考えられている [39]．図 4.2 は各ユーザのクエリ長の分布を表したグラフであり，この図から特にクエリ長が 1 のクエリの割合（単一クエリ率）がユーザごとに異なっていることがわかる．

一方で同じくクエリ長に注目した指標の一つとして平均クエリ長が挙げられるが，検索履歴におけるスペースの個数よりも，スペースを入れた検索の割合という点の方が本人性を強く反映していると考えられるため本稿では単一クエリ率を採用した．その理由としてクエリ長の大きさが熟達度合いに比例して増加するものではないこと，そもそもクエリ長が 3 以上のクエリがほとんど存在せず平均値に有意な差が出るとは考えにくいことが挙げられる．

4.2.2　検索時間ベクトル

本稿における検索時間ベクトルとは，ある 1 日のうちで各時間帯に検索された回数から構成されるベクトルのことである．本実験では特に記載のない限り，1 日を 1 時間幅のセグメントに 24 等分し，各セグメントの時間枠の中で検索された回数から構成されるベクトルを用いた．他

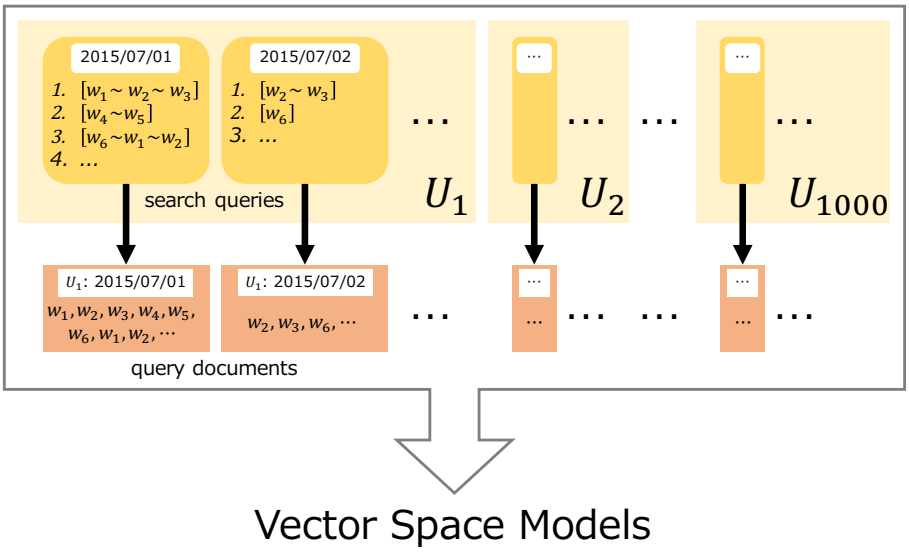

図 4.3: 検索履歴を利用したベクトル空間モデルの構築.

にも 1 日を 6 時間幅のセグメントに 4 等分した例や [39]，検索回数ではなく検索したかどうかの 0/1 から構成されるベクトルを用いた例 [41] などが存在する．今回 1 時間幅のセグメントを設定した理由としては，何時ちょうどという 1 時間おきのタイミングが人間の行動パターンが最も強く切り替わるタイミングであると考えられるからである．これより短い 30 分単位などの場合にはバラツキの大きい検索履歴の特性上上手く機能せず，またこれより長い数時間幅のセグメントを採用すると個人性が大きく失われ不正アクセスに対する鋭敏性も損なわれると考えられる．またマンガの閲覧などとは異なり，ユーザの検索回数はその時間にその程度活発に検索しているかの指標となるため 0/1 の 2 値で評価するのは検索履歴認証にとって損失が大きいと推測される．

4.2.3　検索クエリ

検索クエリの類似度を求める手法は，検索クエリのという特異性はあるものの文章間の類似度を求めるという点では自然言語処理ですでに研究された手法が候補として挙げられる．代表的な指標としてレーベンシュタイン距離，BoW (Bag-of-Words) や特徴語との一致率などがあるものの，これらは散発的な検索クエリに対してはさほど有用ではなく，類似度の評価についても難点が存在する．

よって本稿ではベクトル空間モデルという手法を用いて検索クエリをベクトルとして表現し，そのベクトルの類似度をもって検索クエリの類似度と扱った．

ベクトル空間モデル [42]

ベクトル空間モデルとは文書を何らかの形でベクトル表現に置き換え，それらの類似度や距離を計算することで文書間の関係性を表現するモデルである．ベクトル空間モデルは情報検索の分野で幅広く用いられており，その手法や類似度の算出手法は多岐に渡る．以下では代表的なベクトル空間モデルについてそれぞれ述べる．

潜在的ディリクレ配分法 [43]　潜在的ディリクレ配分法 (LDA; Latent Dirichlet Allocation) とは，自然言語処理におけるトピックモデルの 1 つである．トピックモデルは文章が生成される過程でその背後に潜在的なトピック（話題）が存在し，そのトピックの分布に応じて単語や文書が生成されるという考えに基づいている．LDA は 1 つの文書に対して複数のトピックが存在すると想定した確率的モデルである．LDA を用いることで個別の単語のゆらぎではなくあるユーザが検索対象としているトピックの割合や傾向を分析の対象とすることができるので，検索対象の分散や遷移が激しい検索履歴に対しても有効に機能することが期待される．

word2vec [44–46]　Tomas Mikolov らによって提案された word2vec とは，単語を固定長の実数ベクトルで表現するためのアルゴリズムである．このように単語をベクトルで表現することは，**分散表現**ないしは**単語埋め込み**と呼ばれる．

word2vec によって生成された単語ベクトルは性別や首都，比較級の表現などを表しうることが先行研究によって示されており，「*king* − *man* + *woman* = *queen*」などのように加減算にも対応しているなど有用な性質を保持していることが知られている．

また，単語単位で分散表現を行う word2vec を文書単位で分散表現できるよう拡張した doc2vec [47] も発表されている．

4.2.4　特徴量同士の比較

多要素認証では多種多様な特徴量を用いることが推奨されていることは既に述べたが，既存の研究で挙げられた特徴量ならびに今回新たに加えたクエリ類似度がそれぞれどの程度独立して機能しているのか，その相関性を予備実験により求めた [48].

[48] で使用された 7 種類の特徴量において，互いの相関係数（ピアソンの積率相関係数）を算出した．そのなかでも相関係数の絶対値が 0.5 を超え一定程度の相関がある特徴量の組を挙げると，(単語数，文字数) が 0.95，(単語数，単一クエリ率) が 0.58，(文字数，単一クエリ率) が 0.57 となった．これに次いで (doc2vec, LDA) が 0.47 という相関係数の値を取っている．

文字数，単語数，単一クエリ率はそれぞれ高い相関があり，ランダムフォレストにおける判別への寄与度も低いため，認証の要素としてこれら 3 種類を同時に用いる有用性は低いと考えられる．

また，2 つの手法に基づくクエリ類似度の相関は中程度であることが分かった．検索クエリの意味内容というほぼ同一の対象に関するベクトル表現であるにもかかわらず中程度の相関に留まったということは，両者が異なる観点から検索クエリを分析していることを表していると考えられる．

4.3　テンプレート

本節では検索履歴認証に用いるテンプレートの詳細について述べる．

4.3.1　概要

本稿ではテンプレートの要素として以下の 4 要素を利用した．

- 検索回数

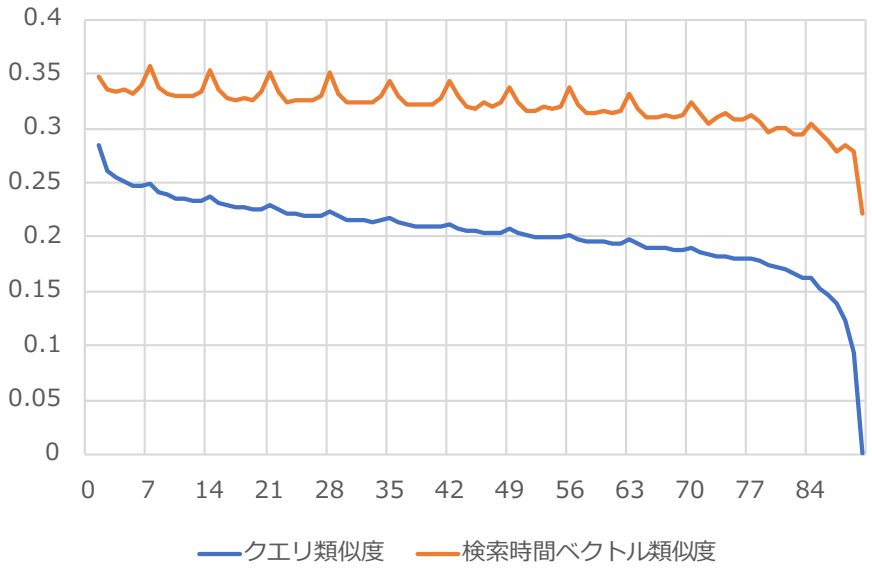

図 4.4: クエリ類似度と検索時間ベクトル類似度の経時変化.

- 単一クエリ率
- 検索時間ベクトル
- 検索クエリベクトル

4.3.2　テンプレート作成方法

テンプレートを作成するためには，まずテンプレート作成に用いられるデータのウィンドウ幅を考慮する必要がある [49]．本研究ではデータのウィンドウ幅を 28 日（4 週間分）と設定した．曜日依存の習慣性を持つユーザの行動パターンを学習するためには少なくとも 1ヶ月程度テンプレート作成に当てる必要があり，既存の類似研究でも 1ヶ月幅のテンプレートが使用されている [41]．またテンプレート期間のデータをすべて使用してテンプレートを作成するのではなく，各特徴量の性質を反映してテンプレートを作成した．その具体例として以下にクエリ類似度のテンプレート作成について述べる．

図 4.4 はある 2 日分のクエリ類似度と検索時間ベクトル類似度を，同一ユーザ内で全通り計算した上で，その 2 日の間隔ごとに平均値を取ったものである．右に行けば行くほど比較した 2 日の間隔は空いており，それに伴って双方の類似度が低下していることが分かる．そして特にクエリ類似度において顕著であるが，7 の倍数日分だけ間を空けた際の類似度に一定の周期的なピークが現れており，これは多くのユーザが同一曜日には類似度の高い検索を行っているということを示している．そのためクエリベクトルのテンプレートに関してはユーザごとに直近 7 日間のデータに加えて同一曜日のデータ 4 週分を含めたテンプレートを曜日別で 7 種類作成した．

また今回は一度作成したテンプレートを一定期間使い回すことはせず，認証要求の度にそのタイミングから直近のデータを利用してテンプレートを作成した．

4.4　ゆらぎ吸収

行動認証はユーザの行動パターンを利用している性質上，行動パターンのゆらぎによる影響を受ける．したがって行動認証手法においてはこのゆらぎを吸収するような方式を採用する必要がある．特に検索履歴認証におけるゆらぎの吸収手法として考えられる 3 種類の手法について以下説明する．

4.4.1　テンプレート更新 [1]

人間の行動パターンは年月の経過とともに変化していくと考えられる．そのため一度作成したテンプレートを長い間使用し続けることで，作成当時と認証時のユーザ行動パターンとの間で差異が拡大していくと想定される．したがってテンプレートは順次更新していく必要がある．これによりユーザの経時的なゆらぎを吸収し，長期間に渡って認証できると考えられる．

また，行動認証ならびにテンプレート更新にとっての大きな課題として，行動変化に対してどの程度鋭敏に反応すべきかという点が挙げられる．たとえばあるユーザが 1 週間の出張に行ったときに多くの場合ユーザの行動範囲や習慣が変化しているため，行動認証での認証はできなくなる．これは行動認証の構造的に当然の事態であり，その間に関しては出張に影響されない認証要素を用いて認証すれば良いのだが，出張の間にテンプレートが更新されてしまうと普段の生活に戻った際に改めて行動認証が機能しなくなってしまう．一方でいつまでもテンプレートが更新されないと，出張が長期間に渡る場合や，そのまま居住地を移す引っ越しなどの場合に行動認証が機能不全に陥る可能性がある．したがってテンプレート更新の鋭敏さはユーザへの負荷やストレスに直結すると考えられる．その対策として，今回クエリベクトルに対して曜日ごとにテンプレートを作成したように，複数のテンプレートを共存・併用させるという方式がある．ただテンプレートの絶対数や範囲を増加させると他人受入率が上昇してしまい悪意ある攻撃者によるリスクが上昇してしまうので，テンプレートの使われる機会やタイミング，そのテンプレートの重要性についても学習が行われると望ましい．たとえば普段の生活をしている場合にはテンプレート A であるが，出張時にはテンプレート C を使い，その間数日間はテンプレート B に沿った行動を取るなどという関係が挙げられる．テンプレート自体がユーザのある一定の，数日ないしは数週間の行動習慣を反映しているものであるが，このテンプレートをどう利用するかの習慣性についても学習が行えるような枠組みが必要である．

今回使用している特徴量は小規模で単純なものでありテンプレート作成が比較的低コストで行えるため，毎回新しくテンプレートを作成するという手法を採用することができた．今後認証形態が複雑化してテンプレート更新に多大なコストが求められるようになってきた場合，既存のテンプレートを利用して加重平均を用いるなど，計算コストを抑える工夫が必要となる．

4.4.2　連続値の利用

検索履歴における特徴語の一致など，特定の単語が含まれるか否かという 0/1 の評価基準では，対象とする語群があまりに疎で検索行動のゆらぎを十分に捉えられないと考えられる．たとえば「東北　旅行」と検索していたユーザが数日後に「秋田　温泉」と検索していた場合，人の目から見ればユーザが旅行の目的地を絞り込んだのだといったように判断できるものの，単語の一致は存在しないため機械的な判別では全くの別ユーザであるというように判断されかねない．

同様の問題は既存のリスクベース認証における位置情報の利用においても存在する．リス

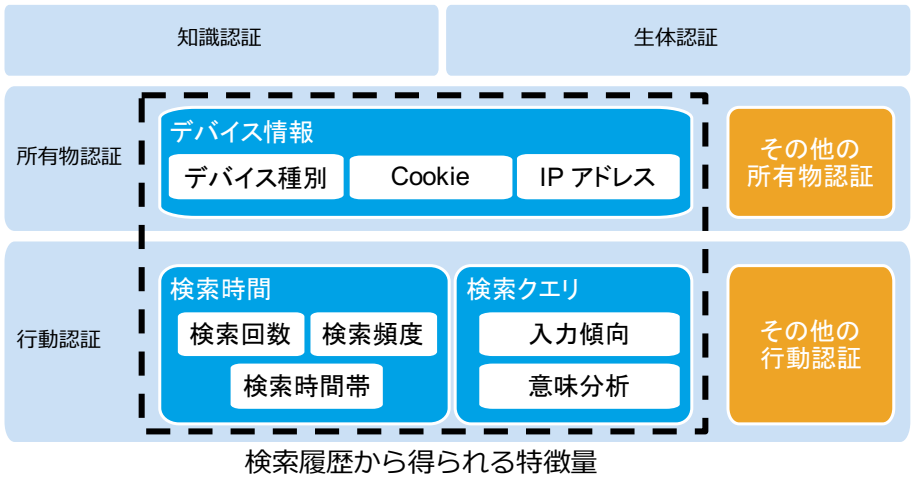

図 4.5: 検索履歴の多要素認証における役割

クベース認証に位置情報を用いる場合，GPS に基づく緯度経度などのように厳密な値ではなく，都道府県や市区町村単位でデータを取り扱うことが多い．これはユーザの位置というものが一定程度のゆらぎを持つ情報であり，そのゆらぎを吸収するために位置情報の粒度を荒くすることでゆらぎに対応する必要があるからである．

本研究ではこの位置情報の抽象化に倣い，検索クエリに現れる個別の単語ではなく検索クエリ自体が持つ検索意図・潜在的な興味関心に基づいて本人かどうか判別する．上述した例であれば「東北　旅行」と「秋田　温泉」がいずれも「(国内) 旅行」「レジャー」「観光」などといったより大きなジャンルでくくられることで，同一のユーザであるかどうかを判別しやすくするといったものである．

また検索行動自体はなりすましが容易なため，特徴語を一度だけ検索しただけでも本人と判定してしまうおそれがある．こういった状況でも検索全体の検索対象，ジャンル，傾向等を特徴量として捉えることができれば特徴語を推測してなりすます攻撃にも対応が可能である．

4.4.3　複数要素の組み合わせ

検索履歴は検索クエリの他，検索時間や使用したデバイス種など，様々な情報を含んだデータである．単一の情報源から認証した場合には行動パターンが変化した本人を誤って排除したりする可能性が考えられるが，複数の要素を組み合わせることでユーザの行動パターン変化を柔軟に吸収することができる．たとえば検索時間が大きく変化したユーザがいた場合に，検索時間だけを用いて認証すると当該ユーザはたとえ本人であろうとも排除されてしまう．この時にユーザの検索内容がほとんど同じであれば，おそらく同一のユーザであるものの時間的なライフスタイルが一時的ないしは長期的に変動したと考えられるのでリスク値は上昇するものの閾値に収まれば本人であると判別できる．一方であまりにも多くの要素で本人ではないと思われる行動習慣が確認された場合，たとえどんなに信頼性のおける認証要素で本人であると判断されても全体として本人ではないという結論に達する場合も考えられる．

検索履歴認証自体も多要素認証の一要素として利用されることを想定して研究されているが，検索履歴認証の内部でも複数の指標を統合して認証すべきか否か判断している．あらゆる認証要素がそれぞれ持つ個別の指標を総合して認証評価を行えば，理想的には最適な解が得ら

れるものの，実際に膨大な指標の妥当性を普遍的に評価できる万能の判別器を作成することは困難である．その上そのような判別器は認証要素を動的に変更するという多要素認証の枠組みの中では再学習を行うコストが大きく膨れ上がるため，個別の認証要素の内部で完結させ抽象化した結果を出力させることが望ましい．その結果検索履歴認証をはじめとした認証要素がそれぞれ独立した多要素認証のような働きを持ち，ユーザの行動パターン変化を柔軟に吸収しつつ認証システムとして利用しやすいモジュール化も果たすことができる．

Chapter 5　検索履歴におけるユーザ適性

本章では検索履歴におけるユーザ適性について述べた．検索履歴認証へのユーザの適性を評価するための指標を提案し，その指標がユーザの認証しやすさを反映しているかどうか，そもそも認証しやすいユーザとはどのようなユーザであるかについて説明し，実際の検索履歴データを用いてその有効性について検証した．

5.1　入力傾向

本節では入力傾向について，検索回数をユーザ適性分析の対象とした．

5.1.1　評価基準

今回は検索回数の分析指標として変動係数（Coefficient of Variation; CV）を用いた．変動係数とは標準偏差 σ を平均 μ で割った値である．相対標準偏差（Relative Standard Deviation; RSD）とも呼ばれる．一般的に平均の絶対値が大きいほど標準偏差は大きくなる傾向があるが，標準偏差をを平均で割ることでデータの相対的なばらつきを評価できる．

$$CV = \frac{\sigma}{\mu} \tag{5.1}$$

変動係数は平均からのデータのズレを評価する指標であるため，変動係数が小さい場合，そのデータは平均周辺に集中しているということを意味する．先行研究では検索回数のテンプレートを作成するにあたってテンプレート内データの平均を用いていた．したがって変動係数が小さければ，既存のテンプレートを用いた認証手法で認証しやすいユーザであると考えられる．

5.1.2　検証手順

全ユーザに対して，実験期間 91 日分の検索回数を 1 日ごとに求めた．そうして得られた検索回数から平均と標準偏差を算出し，変動係数を求めた．ユーザの中でも変動係数が極めて高いないしは低いユーザの検索回数を棒グラフとして出力し，検索回数の変動係数がどのような行動パターンを反映しているものか確認した．またテンプレートと認証サンプルを比較した結果から簡易的に認証を行った場合の精度と変動係数の相関について調べた．今回は簡易的な認証として，テンプレート（テンプレート期間における検索回数の平均）に対する認証サンプル（認証する日ないしは前日の検索回数）の比が 0.5〜1.5 の間にあれば本人と判断している．他人とのサンプルとの比較を行っていないため，この簡易認証は本人性の評価のみを目的にしたものである．

5.1.3　検証結果

図 5.1 は変動係数が小さいあるユーザの検索回数を例として棒グラフで表現したものである．横軸は対象期間の各日付に対応しており，当該ユーザは全期間を通じて 1 日 180 回前後の検索

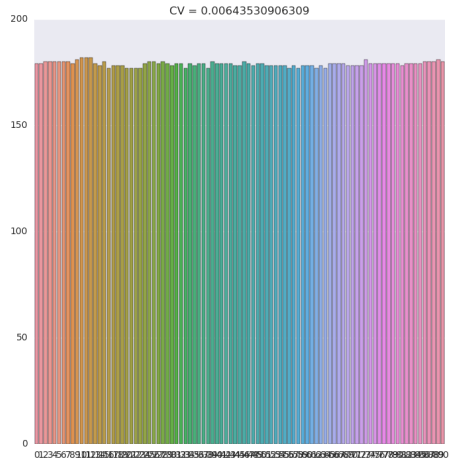

図 5.1: 変動係数が小さいユーザの検索回数.

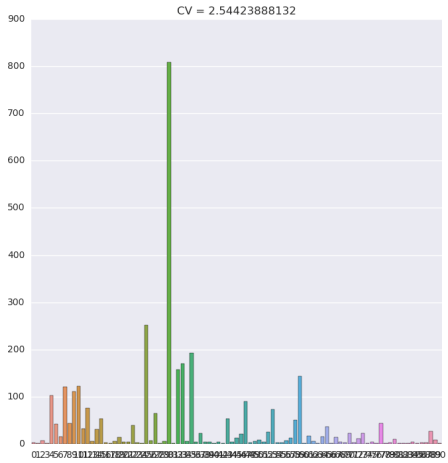

図 5.2: 変動係数が大きいユーザの検索回数.

をしていることがグラフから読み取れる．一方で図 5.2 は変動係数がある大きいユーザの検索回数を同様にグラフに表現したものである．先程のユーザとは異なって当該ユーザは検索回数が日によって大きく変動しており，検索回数から個人認証・異常検知を行うのは難しい．しかし一方でこのユーザの検索回数は数〜数十回の低程度，100〜200 回の中程度，そして突出した 800 回程度と大まかなパターンに分けることができ，そのパターン内のばらつきであれば認証可能な程度に収まっている可能性も想定される．すなわち今回導入した変動係数は検索回数が全期間を通じて一定なユーザを選抜するためのものであり，複数の検索回数パターンを持つユーザに対しては異なる指標を適用したり指標の適応方法を工夫したりすることで今回低評価されたユーザに対しても認証可能なフレームワークを提供できると考えられる．

また図 5.3 からは，変動係数と簡易認証精度の相関が見受けられる．相関係数 $R = -0.73$ ということから，変動係数が大きいほど簡易認証の精度がそれに伴って低下しているという強い相関があることが分かる．ただ一方でユーザの大多数は変動係数と簡易認証精度がともに中程度である箇所に分布しており，検索回数のみでの認証において変動係数でユーザを選抜する効果は限定的であると言わざるをえない．

5.2　検索行為傾向

本節では検索行為傾向について，検索時間ベクトル類似度をユーザ適性分析の対象とした．

5.2.1　評価基準

今回は検索時間ベクトル類似度の分析指標として自己類似度を用いた．自己類似度（Self Similarity）とは，テンプレートの内部でどの程度ばらつきが存在するかを示す指標である．各日の検索履歴データ n 日分の検索履歴から作成されたテンプレート $T = \{t_i \mid 1 \leq i \leq n\}$ を考えたとき，自己類似度を以下のように定義した．

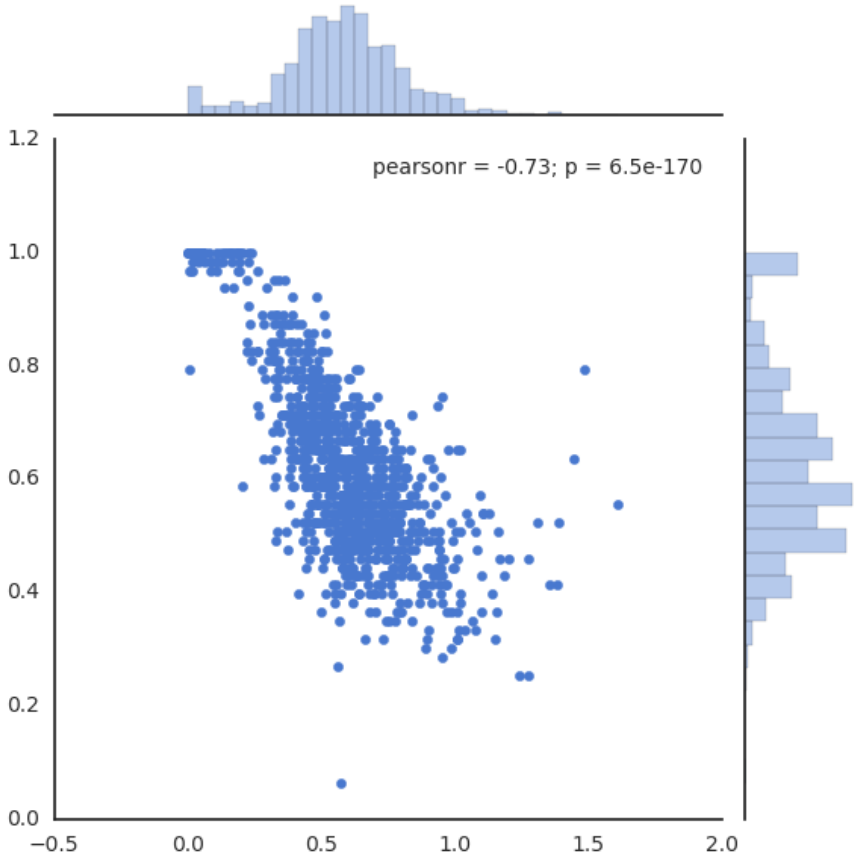

図 5.3: 検索回数の変動係数および閾値を用いた簡易認証の精度との関係．横軸が変動係数，縦軸が簡易認証の精度であり，各点はユーザ 1000 人を示している．

$$SelfSimilarity = \frac{1}{(n-1)n} \sum_{j=i+1}^{n} \sum_{i=1}^{n} sim(t_i, t_j) \tag{5.2}$$

ただし類似度関数 $sim(x, y)$ は実験対象に応じて適宜選択する．本節では検索時間ベクトルについての類似度であるので，ベクトル同士の類似度を比較する指標としてよく用いられるコサイン類似度を使用した．コサイン類似度はベクトル $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)^{\mathrm{T}}, \boldsymbol{b} = (b_1, b_2, \cdots, b_n)^{\mathrm{T}}$ を与えられたとき，以下のように定義される．

$$CosineSimilarity(\boldsymbol{a}, \boldsymbol{b}) = \frac{\boldsymbol{a} \cdot \boldsymbol{b}}{|\boldsymbol{a}||\boldsymbol{b}|} = \frac{\sum_{i=1}^{n} a_i b_i}{\sqrt{\sum_{i=1}^{n} {a_i}^2} \sqrt{\sum_{i=1}^{n} {b_i}^2}} \tag{5.3}$$

5.2.2　検証手順

自己類似度はテンプレートを作成して初めて算出できる値であるので，最初 28 日間をテンプレート作成のための期間として認証サンプルに使用しなかった．そして 29 日目以降の認証サンプル（検索時間ベクトル）に対して作成済みのテンプレートとのコサイン類似度を算出した．

そうして得られた検索時間ベクトル類似度の本人性を評価するため，テンプレート内の自己類似度とテンプレートと認証サンプルを比較した際の類似度を箱ひげ図として表現した．箱ひげ図の横軸はテンプレート内の自己類似度を四捨五入し 11 段階に割り振ったものであり，右の箱ひげほどより自己類似度が高いユーザの検索時間ベクトル類似度に関するものである．縦軸は各段階のテンプレートと認証サンプルの検索時間ベクトル類似度を表している．

またテンプレートと認証サンプルを比較した結果から簡易的に認証を行った場合の精度と自己類似度の相関について調べた．今回は簡易的な認証として，テンプレートに対する認証サンプルとの類似度が 0.5 以上であれば本人と判断している．他人とのサンプルとの比較を行っていないため，この簡易認証は本人性の評価のみを目的にしたものである．

5.2.3　検証結果

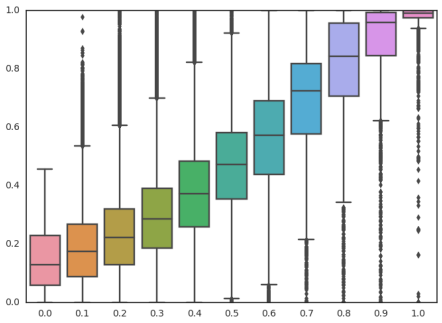

図 5.4: 検索時間ベクトルの自己類似度とその後の検索時間ベクトル類似度．

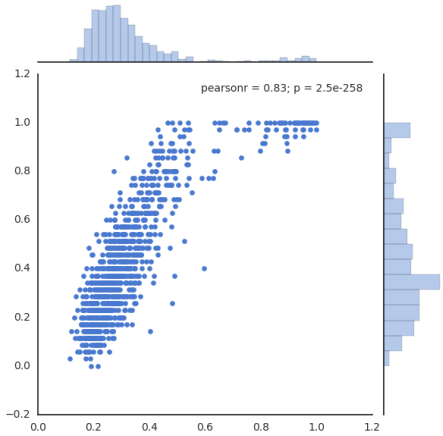

図 5.5: 検索時間ベクトルの自己類似度および簡易認証の精度．

自己類似度の値域

図 5.4 は検索時間ベクトルの自己類似度と，その後の検索時間ベクトル類似度がどのような関係を持つかを箱ひげ図として表現したものである．この図は自己類似度が高ければ高いほど，テンプレートと比較した場合のその後の検索時間ベクトル類似度も高くなる傾向を示している．このことからユーザの自己類似度はおおむね同程度の値を維持する傾向があることが分かる．また四分位範囲は自己類似度が極めて高い場合のみに小さくなっており，その他の部分では大きな差は見られない．これは検索時間ベクトルが 24 次元とクエリベクトル（200 次元）と比較した場合低次元であること，個人差はあろうとも検索時間についてはおおよその人間本来のバイオリズムが存在しそれを大きく逸脱した散発的な検索行動は取りにくいためだと考えられる．

自己類似度と認証精度

図 5.5 では変動係数の場合の同様に，実験対象期間において検索時間ベクトルの類似度がテンプレートと比較した時に 0.5 以上となる日の割合を簡易認証の精度とみなし散布図として表し

ている．相関係数は $R = 0.83$ と，自己類似度と認証精度が強い相関を持つことを示している．またおおよそ自己類似度が 0.6 を超えると認証精度が 1.0 付近で高止まりしていることから，自己類似度が一定程度を超えて高いユーザは，極めて周期性の強い検索行動を取っていることが分かった．

5.3　意味傾向

本節では意味傾向について，doc2vec に基づくクエリベクトルをユーザ適性分析の対象とした．

5.3.1　評価基準

今回はクエリ類似度の分析指標として自己類似度を用いた．自己類似度は第 5.2.1 小節および式 5.2 で先述した指標である．

クエリベクトルのテンプレートは直近 1 週間の全日および直近 1ヶ月での同じ曜日の日のデータが使用されているので，今回の自己類似度は 45 通りの類似度の平均となる．

5.3.2　評価手順

自己類似度はテンプレートを作成して初めて算出できる値であるので，最初 28 日間をテンプレート作成のための期間として認証サンプルに使用しなかった．そして 29 日目以降の認証サンプル（クエリベクトル）に対して作成済みのテンプレートとのコサイン類似度を算出した．そうして得られた検索時間ベクトル類似度の本人性を評価するため，テンプレート内の自己類似度とテンプレートと認証サンプルを比較した際の類似度を箱ひげ図として表現した．箱ひげ図の横軸はテンプレート内の自己類似度を四捨五入し 11 段階に割り振ったものであり，右の箱ひげほどより自己類似度が高いユーザの検索時間ベクトル類似度に関するものである．縦軸は各段階のテンプレートと認証サンプルの検索時間ベクトル類似度を表している．

またテンプレートと認証サンプルを比較した結果から簡易的に認証を行った場合の精度と自己類似度の相関について調べた．今回は簡易的な認証として，テンプレートに対する認証サンプルとの類似度が 0.5 以上であれば本人と判断している．他人とのサンプルとの比較を行っていないため，この簡易認証は本人性の評価のみを目的にしたものである．

5.3.3　検証結果

自己類似度の値域

図 5.6 はクエリベクトルに関してのテンプレートの自己類似度と，その後のクエリ類似度がどのような関係を持つかを箱ひげ図として表現したものである．図 5.4 と同様に，クエリベクトルの自己類似度とその後のクエリ類似度の間には相関関係が存在することが見て取れる．一方で特に自己類似度が大きい場合と小さい場合については箱ひげ図の四分位範囲が小さくなっており，意味内容は時間的制約よりも極端なユーザ層で習慣性が出やすいと考えられる．ある一定の目的を持って同様の検索を繰り返すユーザを想定した場合，検索内容が大きく変化することは稀だが検索時間がずれることは大いに考えられる．そういった点では検索クエリの方が周囲の環境変化や時間的制約に左右されにくい要素だと考えられ，特に何らかの法則性を強く持っている自己類似度の極端なユーザ層で強い習慣性が出たものと考えられる．ただしこれは全体を総括した場合の話であって，個別のユーザを比較した場合クエリベクトルよりも検索時

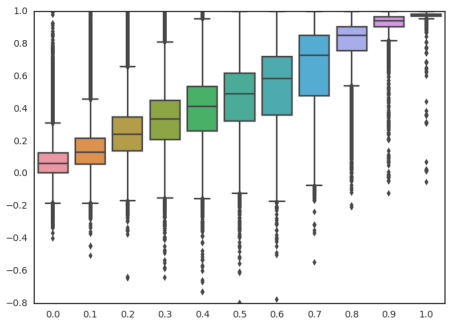

図 5.6: クエリベクトルの自己類似度とその後のクエリ類似度.

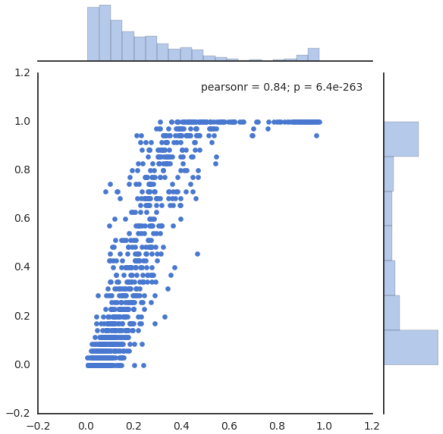

図 5.7: クエリベクトルの自己類似度および簡易認証の精度.

間ベクトルの類似度のほうが本人性・習慣性を強く反映している可能性も大いにある．そのようなユーザ例については，第 6 章に各特徴量の重要性とともに例示してある．

自己類似度と認証精度

図 5.7 については図 5.5 と同様に，実験対象期間においてクエリベクトルの類似度がテンプレートと比較した時に 0.5 以上となる日の割合を簡易認証の精度とみなし散布図として表している．おおむね図 5.5 と同様の相関関係が表れている．しかしクエリ類似度に関しても自己類似度が 0.5 以上のユーザでは認証精度が高止まりしているが，その止まり方がクエリ類似度のほうが急激でかつ高い精度で認証できているユーザが多いことが分かる．相関係数自体は $R = 0.84$ と大差はないものの，認証への有効性という観点からはクエリ類似度のほうがより有効であるとこの図から読み取ることができる．ただしこれもまた前小々節と同様全体を総括した場合であり，個別のユーザ全員に普遍的に言える傾向ではない．

5.4　結論

本章では 2 種類のユーザ適性指標を考案し，その指標がユーザの認証しやすさ，ある特徴量にユーザの本人性がどの程度表れているかを示す値となっているか実際の検索履歴に適用して検証した．その結果いずれの指標も簡易認証の精度と強い相関関係にあり，ユーザ適性指標を算出すれば事前に認証の精度を大まかに推測することができることが分かった．

一方でユーザ適性指標の高いユーザに関しては本人性が強く表れていることも分かったが，ユーザ適性指標の低いユーザについては本人性が強く表れているユーザと弱くしか表れていないユーザが混在していることが分かった．このため現状のユーザ適性指標では認証精度の高いユーザを抽出することはできるものの，全体の認証精度を低下させる不向きなユーザを除外することは難しいと考えられる．

その原因として，

- 行動パターンが複数存在し，テンプレート作成および評価指標が対応できなかった

- 「毎日脈絡の弱い検索を行う」という本人性があり，今回利用した類似度という指標では不十分だった

などが挙げられる．
この点については第 7 章で改めて議論する．

Chapter 6　データ検証

本章では実際の検索履歴を用いてユーザ判別を行い，先述してきた特徴量を用いて検索履歴認証がどのような精度で実施できるのか，実現可能であるかどうかを検証した．

6.1　検証方法

本稿ではデータ検証として機械学習した判別器による 1 対 1 の 2 値分類問題を解くことで評価した．対象ユーザ 1000 人から任意の 2 人組（全 499500 組）に対してそれぞれテンプレートと認証サンプルを比較した特徴量からなる特徴ベクトルを作成し，29 日目〜56 日目までのデータをトレーニング期間，57 日目〜91 日目までのデータをテスト期間と設定してその精度を確認した．テンプレートの作成には認証サンプル以前のデータ 28 日分が必要であるため，1 日目〜28 日目のデータはテンプレートの作成には利用するものの認証サンプルとしては使用していない．また，特徴ベクトルは本人のテンプレートと認証サンプル同士を比較したものと，他人のテンプレートと認証サンプルを比較したものが存在する．2 人組を仮に Alice と Bob と設定した場合，Alice のテンプレート を Bob の認証サンプルと比較した結果と，逆に Bob のテンプレートを Alice の認証サンプルと比較した結果とでは，いずれも他人のテンプレートと認証サンプルを比較したという意味では負例であるが，認証として考えた場合これらは区別されるものであると考えられるので学習器は別々に作成し学習して実験に使用した．

なお，本実験に利用した Python のソースコードは付録 A に掲載した．

6.2　検証結果

上記した識別の結果を表 6.1 に示す．全体の精度（適合率）は 0.938，再現率は 0.920 となった．

実験期間の短い検索履歴認証では正答率が 85.5%であったことから正答率が 93.0%という今回の結果は，実験期間を長くしそれに伴ってテンプレートの作成方法を変更したことによる精度の向上が表れていると言える．一方で [41] で挙げられていたような FRR が高く本人拒否されやすい “Goat” と呼ばれるユーザや FAR が高く他人になりすまされやすい “Lamb” と呼ばれるユーザはそれほど確認されなかった [50].

ユーザごとの誤識別率を表した棒グラフを図 6.1 に示す．うち 79 名は誤識別率が 0%だった．特に識別精度が低かったユーザに関しては誤識別率のピークが見受けられるが，このようなユーザに対して検索履歴認証を適用することは非常に困難であると考えられる．同様のピークは他の行動認証に関する研究でも確認されており，一定数のユーザ群にはこのように認証困難なユーザが一部含まれると推察される．

表 6.1: ランダムフォレストでの識別結果の合計.

真陽性	偽陽性	偽陰性	真陰性
32,185,031	2,141,627	2,779,969	32,823,373

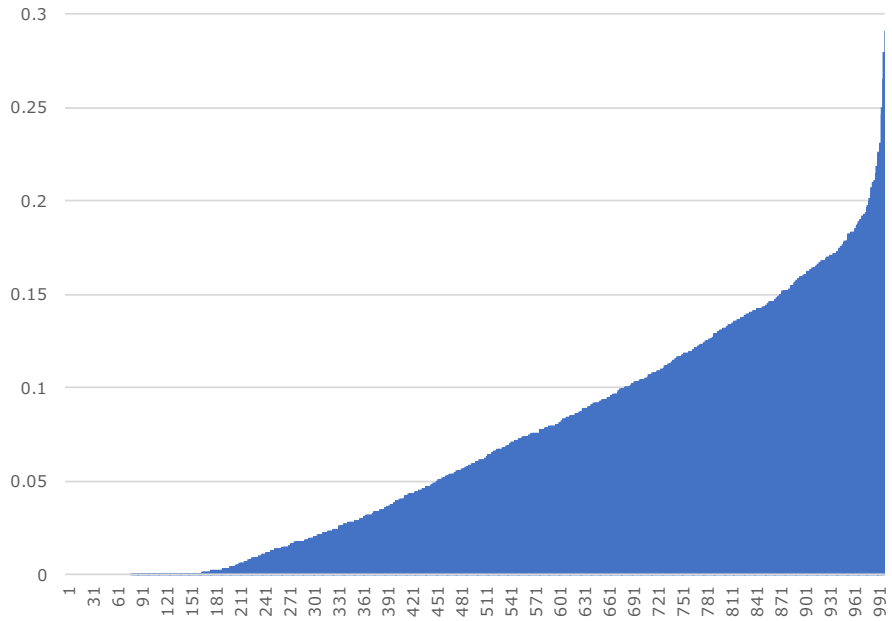

図 6.1: ユーザごとのランダムフォレストによる 2 値識別の誤識別率．横軸が誤識別率に基づくユーザ順位，縦軸が誤識別率（本人拒否＋他人受入）を示している．

表 6.2: ランダムフォレストでの各特徴量の平均寄与度，ならびに全識別器における各特徴量が最も寄与度が高かったものの割合．

	SQR	#Search	Time	Query
平均寄与度	13.5%	19.6%	6.5%	60.4%
最重要寄与度	11.3%	8.5%	0.8%	79.5%

今回の判別において特徴量がどの程度寄与したのかを示す指標として得られた寄与度を表 6.2 に示す．内容は全判別器の平均寄与度，および全判別器のうち当該特徴量が最も寄与したという判別器の割合である．

表 6.2 からはクエリ類似度が判別に大きく寄与していることが見て取れる．多くのユーザでクエリ類似度が高ければ高い精度でユーザ判別できたことが分かるが，一方でクエリ類似度が低いにも関わらず高い精度で判別されたユーザも存在する．よってここでユーザごとに重要な特徴量やその割合が異なることを示すために，1000 人のユーザの中で特徴的なユーザ#46[1] を取り上げて説明する．ユーザ#46 はクエリベクトルの自己類似度が 0.17 とそれほど高くなく（上位 47%），ユーザ識別に大きく影響するクエリ類似度の有効性は低いユーザであると考えられる．しかし一方で検索回数の変動係数が 0.05 と極めて低く（上位 2%），また検索時間ベクトルの自己類似度が 0.95 と極めて高かった（上位 3%）．このためユーザ#46 の機械学習によって 99.5%と十分に高い精度で識別することができた．これらのことからユーザ#46 は，検索内容は日ごとの変化幅が大きいものの，検索する回数および時間に関しては強い習慣性を持つユーザであると推定される．

確かにユーザ適性指標と認証制度との相関関係も重要ではあるものの，このような結果か

[1] ランダムに振られた仮 ID であり，付与されたユーザについての何らかの順位や特徴量を示す値ではない．

ら特徴量に表れる本人性に偏りがあるユーザを選抜する指標としてユーザ適性指標が大きな意味を持つことが分かる．ユーザ適性指標に応じて判別器の学習を調整し，より高い精度を実現できる可能性も考えられる．

Chapter 7　議論

7.1　類似度の高すぎる行動パターン

本研究では検索履歴から得られる行動パターンに対して類似度という指標を設定し，その値の大小で認証対象のユーザが本人であるかどうか検証した．その中で類似度の高いユーザであれば本人性が高く認証しやすいと考えられるものの，類似度の低いユーザへの対応が検索履歴認証の大きな課題の一つとなってくる．他の行動認証に関する研究でも同様の結果が得られていることから [41]，検索履歴をはじめとした行動認証手法の多くで散発的な行動パターンを取るユーザによって全体の認証精度の評価が低く見積もられていると考えられる．

しかし一方でユーザの類似度が低いという情報も，認証に活用できる可能性があると考えられる．たとえば常にテンプレートと比較した際の類似度が極めて低く，散発的な検索行動を行っていると推定されたユーザがある日を境に高いユーザ類似度を記録し続けた場合，類似度が高くともその検索を行っているユーザは本人でない可能性がある．端末に保存されていた検索履歴を元に，同様の検索，あるいは本人性が高く評価されそうななりすまし検索を行っているのではないかと推察することができる．このように類似度はあくまで特徴量の一つであるため，類似度が低ければ低いほど認証が困難であるということは出来ず，注目すべきなのは類似度ないし特徴量の取り得る値の範囲であると考えられる．

7.2　複数パターンを内在したユーザの存在

基本的に今回用いたユーザ適性指標や認証手法は「ユーザがある『1 つの』行動パターンに基づいて行動する」ことを前提としているため，検索する日としない日のギャップがあるユーザはどれほど本人性が強くても十分な精度で認証できていない可能性がある．たとえば検索回数が 1 日おきに 1 回，100 回と繰り返されるユーザが仮に存在した場合，このユーザの検索回数の平均は 50.5 回となり実際の検索回数と大きなギャップが生まれる．そのためこれほど周期的に本人性の強い検索回数パターンを持ちながら，変動係数は極めて大きくなり，検索回数による認証が困難であると適性指標によって判断されることになる．そういった意味で今回設定した指標のスコープはごく限られているため，ユーザの特徴的な行動パターンをクラスタリングなどによって分類し，各クラスタ内でのバラツキを表現することで現状精度の低いユーザの一部は認証制度が向上すると考えられる．

これは検索履歴認証のみならず，行動認証やライフスタイル認証にとって重要な課題である．第 4.4.1 小節では具体的に出張や引っ越しなど，行動パターンの変化の中でも大きなものを例として述べた．しかしより細かい時間幅であったり，変化の割合が小さかったり，極めて稀な変化であったりしたとき，これらをテンプレートとして生成するのは困難である．もし仮にテンプレートを作成したとしても，その数が増大すればするほど認証コストの増加や他人受入率の上昇リスクなど期待できるメリット以上のデメリットが発生するおそれがある．そのためユーザが内在させている行動パターンをクラスタリングさせる際には，そのクラスタのサイズや分散などによって精度やリスク，コストが変化することを考慮に入れなければならない．したがってクラスタリングをする場合には，クラスタリングのサイズ・分散・クラスタ数など

を指定できること，ないしは条件を満たすようなユーザを選抜する指標を用意できることなどが必要である．

複数パターンの内在という点で言えば，クエリベクトルのテンプレート作成はこのシチュエーションに該当している．すなわちユーザが全日同様の検索クエリで検索するのではなく，曜日依存の周期性を持っていることに注目し，同じ曜日のデータの重みを増したテンプレートを作成しているということになる．これは多くのユーザがクエリベクトルの類似度において「1 週間」という共通の周期性を持っていたため実用されたものである．この手法のように検索履歴を 2 日おき，3 日おきなど複数の周期性から評価してデータ分析することで，内在している複数のユーザパターンに合わせたテンプレートならびに認証が可能となるかもしれない．

Chapter 8　結論

本章では上述した検索履歴認証に対する考察ならびに実験結果についてまとめ，今後の課題を記す．

8.1　まとめ

本稿では多要素認証の一要素として検索履歴を用いた認証を提案し，その役割と性能について整理と検証を行った．検索履歴には様々な情報が含まれているため，それぞれを 3 種類に分類して整理し，有効であると考えられる特徴量の計算方法や類似度指標について述べた．その中で検索履歴にはユーザのライフスタイルを反映した周期性が存在することが分かった．またテンプレートを作成する際にもそれらの周期性を反映できる形態を模索した．

これらの考察についての妥当性を検証するため，実際の検索履歴データを用いて実験した．検索履歴認証は一定程度の周期性・規則性・習慣性を持つユーザしか利用できず，認証の信頼性もユーザによって大きく異なるために，ユーザごとの適性を評価するユーザ適性指標の概念を考案した上で，具体的に変動係数と自己類似度を適用した結果を元にその妥当性を評価した．その結果提案したユーザ適性指標は，適性の低いユーザを除外するには至らないものの，適性の高いユーザを抽出するためには有効な指標たりうることを確認した．

また，機械学習によって検索履歴認証におけるユーザ判別の精度を確認した．その結果先行研究などと比べても高い精度でユーザ判別することができたため，検索履歴認証が実用化できる可能性があるという結果が導かれた．

8.2　今後の課題

8.2.1　データ分析

今回使用した検索履歴に関する特徴量や類似度指標などは，いずれも一定程度の効果を発揮したことは実験結果より分かる．しかし同一の要素情報に対してあまり多くの分析手法を適用しておらず，またユーザの検索における行動モデルも確立が不充分であるため，今回採用した手法がはたして最適だったのか，あるいは様々な手法の中でどの程度有効であったかなどの評価はできない．今後は類似度や検索履歴から得られる特徴量について関連研究を広く精査し，検索履歴に有効な指標をより多く設定したい．

また今回は検索履歴以外の情報源を利用していないため，十分な情報量で検索履歴の本人性を評価できていたかは疑問が残る．たとえば検索行動の大きなモチベーションの一つとして，テレビなどのマスメディアから得られる情報があるが，これらの情報にどの程度鋭敏にどの程度の強度で反応するか，また反応するテーマやトピックの分布にどのような傾向があるかなどは検索履歴単体から推測することは困難である．そのためテレビ番組表から番組の出演者や取り上げたトピックなどを収集するなどして，クエリの意味傾向としての特徴量を算出する方法も考えられる．そういった外部情報の利用についても今後の課題とする．

その上今回の認証手法は，第 7.2 節でも述べた「あるユーザは『1 つの』行動パターンに基づいて行動する」という理念のもと設計されたために，複数の行動パターンを内在させるユーザに対して十分な精度を得られなかった．今後はクラスタリングや複数個のテンプレートを作成するなどしてそういったユーザに対する精度も向上させたい．

8.2.2　ユーザ適性指標

今回採用したユーザ適性指標は一定程度の相関を見せたが，ユーザ適性指標の本来の目的であるユーザ選抜，あるいは多認証要素における重みの設定に対しては今回の結果をもって判断することは出来ない．

また，変動係数や自己類似度はあくまで考えられるユーザ適性指標の一つとして挙げられたものであり，その相対的な妥当性や効果の程度については現状評価できる段階にはない．

さらに今回使用した指標はいずれも本人性の高さを示す指標であって，他人との区別がつきやすい弁別性の指標にはなっていない．認証といった枠組みの中で検索履歴認証を利用するためには，本人であるかどうかと並び他人でないかどうかという点も重要になってくるため，他人と類似していない独自性（Uniqueness）に関するユーザ適性指標の考案が求められる．

8.2.3　検索履歴認証に対する攻撃者の想定

今回，他者の一般的な検索履歴を負例として実験を行ったが，実際に悪意ある攻撃者を検索履歴認証が排除しようとする場合，悪意ある攻撃者はなりすました正規ユーザの検索履歴を真似て検索する可能性が考えられる．そういった通常の検索行動ではないなりすましへの耐性が検索履歴認証にどの程度あるのかについては調査できていない．この点について精緻に調査するためには，実際になりすまし攻撃に遭い被害を受けたユーザの検索履歴を利用しなければならないが，そのようなデータを入手するのは極めて困難である．そのため攻撃者が取り得る様々ななりすましのパターンを想定しできるだけ幅広く評価を行うべきであると考えられる．

Chapter A　プログラム

第 6 章において使用した Python プログラムのソースコードを掲載する．全ユーザ 1000 人から考えられるすべての 2 人組を選択する．このとき一方のユーザのみにテンプレートを作成したためプログラム上の組み合わせは順列となり 999000 組となっている．テンプレート作成期間である 28 日分を確保するため，機械学習にかけるトレーニング期間として 29〜56 日目のデータを使用し，正例・負例の特徴ベクトルを計算させる．そしてその特徴ベクトルをランダムフォレストの学習器に入力し学習させる．その後 57〜91 日目までのデータを使用してテスト用の特徴ベクトルを計算させ，学習済みの学習器で本人のテンプレートと比較したデータかどうか予測させる．その結果を各特徴量の寄与度とともに出力させ，それを結果データとして保存する．

Listing A.1: 認証実験に使用した Python プログラム

```
#!/usr/bin/env python
# -*- coding:utf-8 -*-

"""
Authentication experiment with 4 features of search history.

(c) 2017 Yusuke MIYANO, The University of Tokyo.
"""


from gensim.models import doc2vec
import numpy as np
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import confusion_matrix
from sklearn.metrics.pairwise import cosine_similarity

users = 1000

model = doc2vec.Doc2Vec.load("doc2vec.model")
timevecs = np.loadtxt("timevecs.csv", delimiter=",")
search_counts, sqrs = np.loadtxt("textual.csv",
                                 delimiter=",",
                                 unpack=True)


def template_docids(uid, d):
    """
    Return the docids for templates.

    Return the docids of the user whose id is equal to uid
    on last 7 days & last 4 days which are on the same day of the week
    of the day d.
    """
    return [users * uid + d - 28,
            users * uid + d - 21,
            users * uid + d - 14,
            users * uid + d - 7,
            users * uid + d - 6,
            users * uid + d - 5,
```

```
            users * uid + d - 4,
            users * uid + d - 3,
            users * uid + d - 2,
            users * uid + d - 1]


def template_sqr(uid, d):
    """
    Return the SQR of the user d.

    During his/her registration period of 28 days before the day d.
    """
    sqr = sqrs[uid * users + d - 28:uid * users + d]
    search_count = search_counts[uid * users + d - 28:uid * users + d]
    return 1. * np.sum(sqr * search_count) / np.sum(search_count)


def template_time(uid, d):
    """
    Return the time-template vector of the user whose id is equal to uid.

    during his/her registration period of 28 days before the day d.
    """
    user_timevecs = timevecs[users * uid + d - 28:users * uid + d:7]
    return np.sum(user_timevecs /
                  np.sum(user_timevecs, axis=1, dtype=np.float).reshape(4, -1),
                  axis=0)


def req_feature_vectors(uid1, uid2, d):
    """Return a feature vector of request in comparison with a template.

    compare the template of uid1 with the request of uid2 on day d.
    """
    day_id1 = users * uid1 + d
    day_id2 = users * uid2 + d

    _sqr = abs(template_sqr(uid1, d) - sqrs[day_id2])
    _search_count = (1. * search_counts[day_id2] /
                     np.mean(search_counts[day_id1 - 28:day_id1]))
    _cossim = cosine_similarity(template_time(uid1, d).reshape(1, -1),
                                timevecs[day_id2].reshape(1, -1))[0, 0]
    _docsim = model.docvecs.n_similarity(template_docids(uid1, d),
                                         [day_id2])

    return [_sqr, _search_count, _cossim, _docsim]


for uid1 in xrange(users):
    with open("./{}.csv".format(uid1), "a") as f:
        for uid2 in xrange(users):
            true_req_feature_vectors = [req_feature_vectors(uid1, uid1, d)
                                        for d in xrange(28, 56)]
            false_req_feature_vectors = [req_feature_vectors(uid1, uid2, d)
                                         for d in xrange(28, 56)]
            x_train = true_req_feature_vectors + false_req_feature_vectors
            y_train = [1] * 28 + [0] * 28

            clf = RandomForestClassifier(n_estimators=100,
                                         random_state=10)
            clf.fit(x_train, y_train)
```

```
101
102             true_req_feature_vectors = [req_feature_vectors(uid1, uid1, d)
103                                         for d in xrange(56, 91)]
104             false_req_feature_vectors = [req_feature_vectors(uid1, uid2, d)
105                                          for d in xrange(56, 91)]
106             x_test = true_req_feature_vectors + false_req_feature_vectors
107             y_test = [1] * 35 + [0] * 35
108
109             result = confusion_matrix(clf.predict(x_test), y_test).flatten()
110             f.write("¥{},{},{}n".format(uid2), ",".join(map(str, result)),
111                     ",".join(map(str, clf.feature_importances_)))
```

謝辞

本研究を遂行するにあたり，日頃からご指導をいただきました東京大学ソーシャル ICT 研究センターの山口利恵特任准教授に深謝いたします．山口先生には研究に対するご指摘やアドバイスのみならず，大学院生としてどう立ち振る舞うべきかなどあらゆる観点からご指導いただいたり，また新しいことへの挑戦や外部への発信など自身の可能性を広げるお手伝いを積極的にこなしてくださったりするなど，そのお力添えもありまして極めて有意義な大学院生活を送ることができました．

また共同研究を行わせていただいたヤフー株式会社の皆様に感謝いたします．特に Yahoo! JAPAN 研究所の五味秀仁さん，坪内孝太さん，笹谷奈翁美さん，山口修司さんにおかれましては，定期ミーティングでのディスカッションにご参加いただいたりデータの扱い方や研究手法などについてご指導を賜ったりするなど，企業の規模・視点から研究を行うという大変貴重な機会を設けていただきました．ならびにこの共同研究をサポートしてくださった皆様にも重ねて御礼申し上げます．

寄付講座という形で研究室をサポートしてくださった三菱 UFJ ニコス株式会社様には心から感謝いたしております．金銭面のみならず様々なシンポジウムなどで貴重な機会やお話をいただきまして，おかげさまでセキュリティに対する視野を広げることができました．

そして山口研究室でのミーティングで活発な議論を交わした学術支援専門職員である鈴木宏哉さん，小林良輔さん，博士課程学生である疋田敏朗さん，同期の崔誠云くん，修士課程学生の西山双輝くんにも感謝しきれぬ思いでいっぱいです．また日々の研究室運営から学会参加まで幅広く円滑に進められるようご助力いただいた山口研究室秘書の田中美鈴さんにも厚く御礼申し上げます．皆様には研究室を離れたイベントでもお世話になりまして，楽しい 2 年間を過ごすことができました．

最後に，様々な困難や障害を迎えてもなお，長々と学生生活を送る我が儘を暖かく見守ってくれた家族に心から感謝します．

参考文献

[1] 小林良輔, 疋田敏朗, 鈴木宏哉, 山口利恵. ライフスタイル認証におけるゆらぎ吸収を目的としたテンプレート更新手法の提案. コンピュータセキュリティシンポジウム 2016 (CSS2016), 2016.

[2] 警察庁. 平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について, March 2016. https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf 2017 年 2 月 6 日閲覧.

[3] 株式会社シマンテック／日本ベリサイン株式会社. 「個人・企業のパスワード管理」に関する意識調査結果のご報告, October 2013. https://www.jp.websecurity.symantec.com/welcome/pdf/password_management_survey.pdf 2017 年 2 月 1 日閲覧.

[4] 警察庁, 総務省, 経済産業省. 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況, March 2016. http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000105.html 2017 年 2 月 6 日閲覧.

[5] トレンドマイクロ株式会社. パスワードの利用実態調査 2014, June 2014. http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20140609010140.html 2017 年 2 月 1 日閲覧.

[6] 独立行政法人情報処理推進機構. オンライン本人認証方式の実態調査 報告書, August 2014. https://www.ipa.go.jp/files/000040778.pdf 2017 年 2 月 1 日閲覧.

[7] 山口利恵, 鈴木宏哉, 小林良輔. 認証精度の違う多要素・段階認証. コンピュータセキュリティシンポジウム 2015 (CSS2015), 2015.

[8] Google. Google 2 段階認証プロセス. http://www.google.com/intl/ja/landing/2step/ 2017 年 2 月 1 日閲覧.

[9] Hiroya Susuki and Rie Shigetomi Yamaguchi. Cost-effective modeling for authentication and its application to activity tracker. In *Information Security Applications*, pp. 373–385. Springer, 2015.

[10] RYOSUKE Kobayashi and RS Yamaguchi. A behavior authentication method using wi-fi bssids around smartphone carried by a user. In *2015 Third International Symposium on Computing and Networking (CANDAR)*, pp. 463–469. IEEE, 2015.

[11] Issa Traore, Isaac Woungang, Mohammad S Obaidat, Youssef Nakkabi, and Iris Lai. Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments. In *Digital Home (ICDH), 2012 Fourth International Conference on*, pp. 138–145. IEEE, 2012.

[12] 小林良輔, 疋田敏朗, 鈴木宏哉, 山口利恵. 行動センシングログを元にしたライフスタイル認証の提案. コンピュータセキュリティシンポジウム 2016 (CSS2016), 2016.

[13] Rosie Jones, Ravi Kumar, Bo Pang, and Andrew Tomkins. "I Know What You Did Last Summer": Query Logs and User Privacy. In *Proceedings of the Sixteenth ACM Conference on Conference on Information and Knowledge Management*, CIKM '07, pp. 909–914, 2007.

[14] Sai Teja Peddinti and Nitesh Saxena. On the Effectiveness of Anonymizing Networks for Web Search Privacy. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pp. 483–489, 2011.

[15] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The Second-generation Onion Router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, SSYM'04, pp. 21–21, 2004.

[16] The Tor Project, Inc. Tor Project: Anonymity Online, September 2002. `https://www.torproject.org` 2017 年 2 月 1 日閲覧.

[17] Rosie Jones, Ravi Kumar, Bo Pang, and Andrew Tomkins. Vanity Fair: Privacy in Querylog Bundles. In *Proceedings of the 17th ACM Conference on Information and Knowledge Management*, CIKM '08, pp. 853–862, 2008.

[18] Christopher Soghoian. The problem of anonymous vanity searches, January 2007. Available at SSRN: `http://ssrn.com/abstract=953673`.

[19] Tara Whalen and Carrie Gates. Private lives: User attitudes towards personal information on the web. Technical report, 2005.

[20] Latanya Sweeney. K-anonymity: A Model for Protecting Privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, Vol. 10, No. 5, pp. 557–570, October 2002.

[21] Arthur Gervais, Reza Shokri, Adish Singla, Srdjan Capkun, and Vincent Lenders. Quantifying Web-Search Privacy. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pp. 966–977, 2014.

[22] Joanna Biega, Ida Mele, and Gerhard Weikum. Probabilistic Prediction of Privacy Risks in User Search Histories. In *Proceedings of the First International Workshop on Privacy and Security of Big Data*, PSBD '14, pp. 29–36, 2014.

[23] Vincent Toubiana, Lakshminarayanan Subramanian, and Helen Nissenbaum. TrackMeNot: Enhancing the privacy of Web Search. *CoRR*, Vol. abs/1109.4677, , 2011.

[24] Daniel C. Howe and Helen Nissenbaum. TrackMeNot, 2006. `https://cs.nyu.edu/trackmenot/` 2017 年 2 月 1 日閲覧.

[25] Sai Teja Peddinti and Nitesh Saxena. On the Privacy of Web Search Based on Query Obfuscation: A Case Study of TrackMeNot. In *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*, PETS'10, pp. 19–37, 2010.

[26] Robert Layton, Paul Watters, and Richard Dazeley. Authorship Attribution for Twitter in 140 Characters or Less. In *Proceedings of the 2010 Second Cybercrime and Trustworthy Computing Workshop*, CTC '10, pp. 1–8, 2010.

[27] Parse.ly. The State of Tags in Digital Media. Technical report, Parse.ly, 2015. http://www.parsely.com/resources/authority-report-8/ 2017 年 2 月 1 日閲覧.

[28] Azin Ashkan, Charles L. A. Clarke, Eugene Agichtein, and Qi Guo. Classifying and Characterizing Query Intent. In *Advances in Information Retrieval, 31th European Conference on IR Research, ECIR 2009, Toulouse, France, April 6-9, 2009. Proceedings*, pp. 578–586, 2009.

[29] David J. Brenes, Daniel Gayo-Avello, and Kilian Pérez-González. Survey and Evaluation of Query Intent Detection Methods. In *Proceedings of the 2009 Workshop on Web Search Click Data*, WSCD '09, pp. 1–7, 2009.

[30] Juan Zamora, Marcelo Mendoza, and Héctor Allende. Query Intent Detection Based on Query Log Mining. *J. Web Eng.*, Vol. 13, No. 1&2, pp. 24–52, 2014.

[31] Ricardo Baeza-Yates, Carlos Hurtado, and Marcelo Mendoza. Query Recommendation Using Query Logs in Search Engines. In *Proceedings of the 2004 International Conference on Current Trends in Database Technology*, EDBT'04, pp. 588–596, 2004.

[32] Zhiyong Zhang and Olfa Nasraoui. Mining Search Engine Query Logs for Query Recommendation. In *Proceedings of the 15th International Conference on World Wide Web*, WWW '06, pp. 1039–1040, 2006.

[33] Qi He, Daxin Jiang, Zhen Liao, Steven C. H. Hoi, Kuiyu Chang, Ee-Peng Lim, and Hang Li. Web Query Recommendation via Sequential Query Prediction. In *Proceedings of the 2009 IEEE International Conference on Data Engineering*, ICDE '09, pp. 1443–1454, 2009.

[34] Jeff Huang and Efthimis N. Efthimiadis. Analyzing and Evaluating Query Reformulation Strategies in Web Search Logs. In *Proceedings of the 18th ACM Conference on Information and Knowledge Management*, CIKM '09, pp. 77–86, 2009.

[35] Ye Chen, Dmitry Pavlov, and John F. Canny. Large-scale behavioral targeting. In *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '09, pp. 209–218, 2009.

[36] Alissa Cooper. A Survey of Query Log Privacy-enhancing Techniques from a Policy Perspective. *ACM Trans. Web*, Vol. 2, No. 4, pp. 19:1–19:27, October 2008.

[37] Michael BARBARO and Tom Zeller Jr. A Face Is Exposed for AOL Searcher No. 4417749, August 2006. http://www.nytimes.com/2006/08/09/technology/09aol.html 2017 年 2 月 1 日閲覧.

[38] ヤフー株式会社. NII と Yahoo! JAPAN が検索技術研究のために新たな提携「Yahoo!検索」の検索クエリデータを NII のワークショップに無償提供, 2015. http://pr.yahoo.co.jp/release/2015/07/17a/ 2017 年 2 月 1 日閲覧.

[39] 宮野祐輔, 山口利恵, 坪内孝太, 五味秀仁. 個人認証を見据えた検索履歴からの行動分析. 暗号と情報セキュリティシンポジウム 2016 (SCIS2016), 2016.

[40] ヤフー株式会社. Yahoo!検索ヘルプ - ウェブ検索の基本的な使い方, 2015. https://www.yahoo-help.jp/app/answers/detail/a_id/42785/p/595 2017 年 2 月 1 日閲覧.

[41] 小林良輔, 山口利恵. マンガアプリにおける閲覧ならびにその他の利用履歴情報を活用した個人認証手法の提案. 暗号と情報セキュリティシンポジウム 2017 (SCIS2017), 2017.

[42] Gerard Salton and Michael J. McGill. *Introduction to Modern Information Retrieval*. McGraw-Hill, Inc., New York, NY, USA, 1986.

[43] David M Blei, Andrew Y Ng, and Michael I Jordan. Latent dirichlet allocation. *Journal of machine Learning research*, Vol. 3, No. Jan, pp. 993–1022, 2003.

[44] Tomas Mikolov, Wen-tau Yih, and Geoffrey Zweig. Linguistic regularities in continuous space word representations. In *Human Language Technologies: Conference of the North American Chapter of the Association of Computational Linguistics, Proceedings, June 9-14, 2013, Westin Peachtree Plaza Hotel, Atlanta, Georgia, USA*, pp. 746–751, 2013.

[45] Tomas Mikolov, Kai Chen, Greg Corrado, and Jeffrey Dean. Efficient estimation of word representations in vector space. *CoRR*, Vol. abs/1301.3781, , 2013.

[46] Tomas Mikolov, Ilya Sutskever, Kai Chen, Gregory S. Corrado, and Jeffrey Dean. Distributed representations of words and phrases and their compositionality. In *Advances in Neural Information Processing Systems 26: 27th Annual Conference on Neural Information Processing Systems 2013. Proceedings of a meeting held December 5-8, 2013, Lake Tahoe, Nevada, United States.*, pp. 3111–3119, 2013.

[47] Quoc V. Le and Tomas Mikolov. Distributed representations of sentences and documents. *CoRR*, Vol. abs/1405.4053, , 2014.

[48] 宮野祐輔, 山口利恵, 坪内孝太, 五味秀仁. 個人認証を見据えた検索クエリの類似性評価. コンピュータセキュリティシンポジウム 2016 (CSS2016), 2016.

[49] 鈴木宏哉, 山口利恵. 履歴データを用いた個人認証におけるウィンドウ幅のモデル化. 暗号と情報セキュリティシンポジウム 2017 (SCIS2017), 2017.

[50] George Doddington, Walter Liggett, Alvin Martin, Mark Przybocki, and Douglas Reynolds. Sheep, goats, lambs and wolves a statistical analysis of speaker performance in the nist 1998 speaker recognition evaluation. In *INTERNATIONAL CONFERENCE ON SPOKEN LANGUAGE PROCESSING*, 1998.

発表文献

国内会議

i 宮野祐輔, 崔誠云, 疋田敏朗, 小林良輔, 鈴木宏哉, 山口利恵. “日本の東西分割を通じた機械学習手法の評価”, 第 57 回プログラミング・シンポジウム 予稿集. 静岡, 1 月, 2016 年.

ii 宮野祐輔, 山口利恵, 坪内孝太, 五味秀仁. “個人認証を見据えた検索履歴からの行動分析”, 2016 年 暗号と情報セキュリティシンポジウム (SCIS2016) 予稿集, 2C2. 熊本, 1 月, 2016 年.

iii 宮野祐輔, 山口利恵, 坪内孝太, 五味秀仁. “個人認証を見据えた検索クエリの類似性評価”, 2016 年 コンピュータセキュリティシンポジウム (CSS2016) 予稿集, 3E4. 秋田, 10 月, 2016 年.

iv 宮野祐輔, 山口利恵, 坪内孝太, 五味秀仁. “検索履歴認証に対するユーザ適性指標”, 2017 年 暗号と情報セキュリティシンポジウム (SCIS2017) 予稿集, 4D2. 沖縄, 1 月, 2017 年.