L-002

犯罪者の活動地域を推測するための暗号資産アドレス分析手法の提案
Estimating Geographic Locations of Criminal Activity through Cryptocurrency Address Analysis

森 博志† 熊谷 裕志† 神薗 雅紀†‡ 田中 俊昭‡
Hiroshi Mori Hiroshi Kumagai Masaki Kamizono Toshiaki Tanaka

1. はじめに

暗号資産は他の金融資産と比較して匿名性が高く，資産の追跡が難しい．そのため，犯罪者はランサムウェアやセクストーションによる恐喝の際に暗号資産を要求したり，DDoS 代行サービスや Exploit Kit の販売等の CaaS(Crime as a Service)をはじめとする違法な商品やサービスの決済手段として暗号資産を利用したりする．このような犯罪活動を行なう組織の中には，一般企業のように就業時間が定められている組織も存在する[1]．そこで著者らは犯罪者が一般的な就業時間帯である日中に犯罪活動を行い，暗号資産の送金手続きも日中に行うことが多いと考えた．

本研究では犯罪者が管理する暗号資産の送金時間帯から犯罪者の活動地域を推測する手法を提案する．提案手法では犯罪者は暗号資産の送金手続きを日中に行うと仮定し，その送金時間帯から犯罪者がどのタイムゾーンで活動しているのかを推測する．

本稿では提案手法を説明し，活動タイムゾーンが既知である犯罪者アドレスについて，提案手法によりタイムゾーンを推測した際の精度評価結果について述べる．また，日本国内の犯罪に関与したと見られるアドレスについて，提案手法による分析事例を示す．なお本研究では暗号資産の中でも人気が高く，犯罪に悪用されることも多い Bitcoin を研究対象とする．

本稿の構成は以下の通りである．まず 2 章で研究対象である Bitcoin の概要を述べる．次に 3 章で提案手法について説明し， 4 章では犯罪者が管理する Bitcoin アドレスについて，提案手法を適用して推測精度を検証する．5 章では日本国内で犯罪への関与があったと見られるアドレスについて，提案手法を適用した分析事例を紹介する．そして 6 章で考察，7 章で提案手法の関連研究について述べる．最後に 8 章でまとめとする．

2. Bitcoin

Bitcoin はナカモトサトシという人物が書いたとされる論文 [2]で提案されたブロックチェーン技術を利用した暗号資産であり，暗号資産の中でも利用者が多く，エルサルバドル共和国では法定通貨として採用されている．

2.1 ブロックチェーン

ブロックチェーンは鎖状に連結したブロックと呼ばれるデータで構成されている．各ブロックは，前のブロックのハッシュ値を格納しており，時系列順に連結されている．したがって，もしあるブロックのデータが改変されたとしても，その後のブロックに記録されているハッシュ値が異なるため，ブロックチェーンのデータ改ざんを検知することができる．Bitcoin は，利用者によるハッシュ値計算に基づき承認されたトランザクション(以降では TX と表記)が，ブロックチェーン上のブロックとして管理されている．

2.2 匿名性

Bitcoin ブロックチェーン(以降では単にブロックチェーンと表記)は公開情報であり，誰でも閲覧できる．すなわち，どの TX において，どのアドレスからどのアドレスへ，どれだけの Bitcoin をいつ送金したのかを調べることができる．しかし TX の目的や TX に含まれるアドレスの管理者が誰であるかといった情報は記録されない．さらに Bitcoin アドレスは個人が無制限に生成できるため，Bitcoin 利用者は自身が生成した複数のアドレスを経由して送金することにより，TX の匿名性を高めることができる．加えて，ミキシングと呼ばれる手法を用いることによりマネーフローを複雑化させることもできる．ミキシングは，1 つの TX に管理者が異なるアドレスを複数参加させることで取引を複雑化し，さらにその複雑化した取引を繰り返すことにより，匿名性をより高める手法である．Bitcoin では複数のミキシングサービスが存在することが報告されている [3].

2.3 アドレスクラスタリング

マルチインプットクラスタリングと呼ばれる手法を用いることで，アドレスを管理者ごとに分類できる[4]~[6]．マルチインプットクラスタリングは，「TX において共同で送金しているアドレスの管理者は同一である」という仮定によりアドレスを分類する．犯罪者は，Bitcoin の追跡を困難にするために複数のアドレスを使い分けることがあるが，当該クラスタリング手法により，同一犯罪者が管理する異なるアドレスを 1 つのクラスタにできる場合がある．ただし当該クラスタリング手法はミキシングサービスのような関係性のないアドレスが同一 TX で送金を行う場合，意図したクラスタを作成できない制限がある．

3. 提案手法

提案手法では，犯罪者は日中に自身が管理する暗号資産の送金処理を行うと仮定し，その送金時間帯から犯罪者の活動地域のタイムゾーンを推測する．具体的には，犯罪者が管理する Bitcoin アドレスを入力とし，犯罪者の活動タイムゾーンを UTC+X の形で出力する(図 1).

3.1 基本アルゴリズム

提案手法ではタイムゾーンの推測対象として指定された Bitcoin アドレスについて，ブロックチェーンを分析し TX 情報を取得する．そして当該アドレスが送金に参加した

†デロイト トーマツ サイバー合同会社
Deloitte Tohmatsu Cyber LLC
‡兵庫県立大学大学院 情報科学研究科
Graduate School of Information Science, University of Hyogo

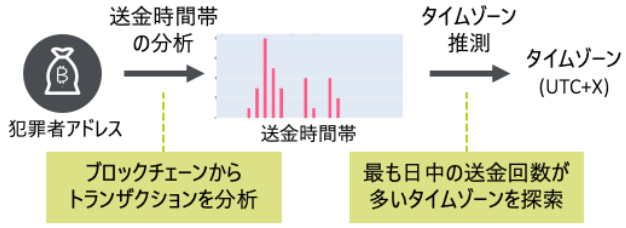

図 1　提案手法の概要図

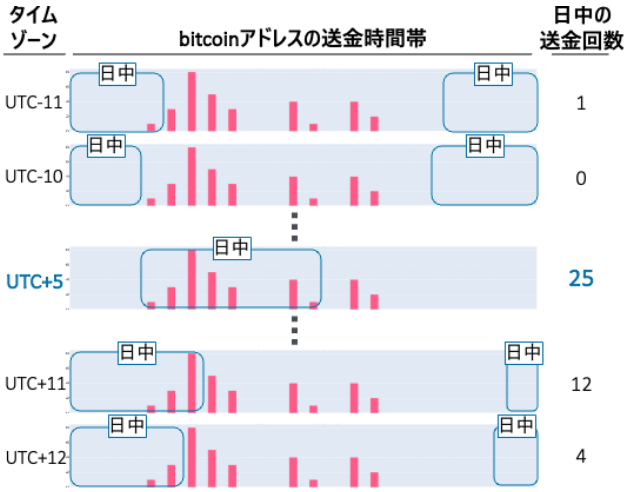

図 2　タイムゾーン算出の概念図

TX(以降では送金 TX と表記する)の時刻を取得する．次に，取得した時刻を 0 時から 23 時の 24 通りの時間帯に分け，これらの時間帯について UTC-11 から UTC+12 の 24 通りのタイムゾーンにおいて，最も日中に送金 TX 数が多くなるタイムゾーンを算出し，それを推測タイムゾーンとする(図 2)．なお本研究では日中を 9 時から 17 時の時間帯と定義し，推測によるタイムゾーンの候補が複数ある場合はそれらの中央値を最終的な推測結果とする．また，時刻情報は循環する値であるため角度統計により平均値等の統計量を算出する．

本アルゴリズムでは対象のアドレスが 1 回でも送金 TX に参加していれば適用可能であるが，送金 TX 数が 1 回しかない場合，情報量が足りずタイムゾーン候補の絞り込みが困難であるため，推測不可とする．

3.2 アドレスクラスタの活用

3.1 節のアルゴリズムはアドレスの送金 TX 時刻を基に推測を行うため，送金 TX 数が少ない場合，情報量が足りず推測精度が低くなると考えられる．そこで本研究ではアドレス単体での推測手法に加えて，アドレスクラスタを活用した推測手法を提案する．当該手法では 2.3 節のアドレスクラスタリング手法により，推測対象のアドレスと管理者が同じアドレス群を特定し，これらのアドレスの送金 TX を加味した 2 つのタイムゾーン推測手法も検討する．以降では，推測対象のアドレスの送金 TX にのみ基づいてタイムゾーンを推測する手法をアドレス単体推測，アドレスクラスタリング手法により特定した，同一の犯罪者が所有するアドレス群の送金 TX に基づく 2 つの推測手法をそれぞれ，アドレスクラスタ個別推測，アドレスクラスタ統合推測と呼ぶ．

3.2.1 アドレスクラスタ個別推測

推測対象アドレスが含まれるアドレスクラスタについて，クラスタ内の全アドレスに対して 3.1 節のアルゴリズムによりタイムゾーンを推測し，その平均値を最終的な推測結果とする．当該手法を本研究ではアドレスクラスタ個別推測と呼ぶ(図 3)．ただしクラスタ内のアドレスのうち，送金 TX 数が 1 以下のアドレスについては，推測精度が低下する要因となると考え，推測処理から除外する．

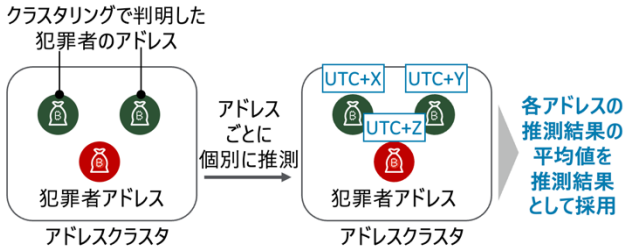

図 3　アドレスクラスタ個別推測

3.2.2 アドレスクラスタ統合推測

推測対象アドレスが含まれるアドレスクラスタについて，クラスタ内の全アドレスの送金 TX 情報を 1 つに統合する．そしてそれらの送金 TX 時刻から 3.1 節のアルゴリズムによりタイムゾーンを推測する．当該手法を本研究ではアドレスクラスタ統合推測と呼ぶ(図 4)．なお本手法では送金 TX を統合した際に TX ID が重複することがあるが，その場合は重複分の TX を推測処理から除外する．

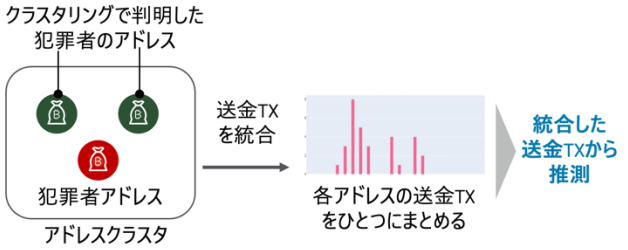

図 4　アドレスクラスタ統合推測

3.3 送金 TX と推測精度についての仮説

提案手法では犯罪者は日中に自身が管理する暗号資産の送金処理を行うと考え，その送金時間帯から犯罪者の活動地域のタイムゾーンを推測する．そのため提案手法の推測精度は，推測対象アドレスの送金 TX 数や送金時間帯の集中度合いの影響を受けると考えられる．

送金 TX 数

提案手法では送金 TX の時刻情報を基に推測を行う．従って送金 TX 数が多いほど推測に用いるデータが多くなり推測精度が高くなると考えられる．

送金時間分散

提案手法は推測対象である犯罪者のアドレスの送金時間帯が日中に集中していることを前提としている．そのため，推測対象のアドレスの送金時間帯が特定の時間帯に集中していない場合，提案手法によるタイムゾーン推測の精度が低くなると考えられる．そこで本研究では推測対象のアドレスについて送金時間帯の分散を計算し，これを送金時間分散と呼ぶ．送金時間分散が大きい場合，推測対象のアドレスの送金 TX の時間帯が集中しておらず，提案手法によるタイムゾーン推測の精度が低くなると考えられる．

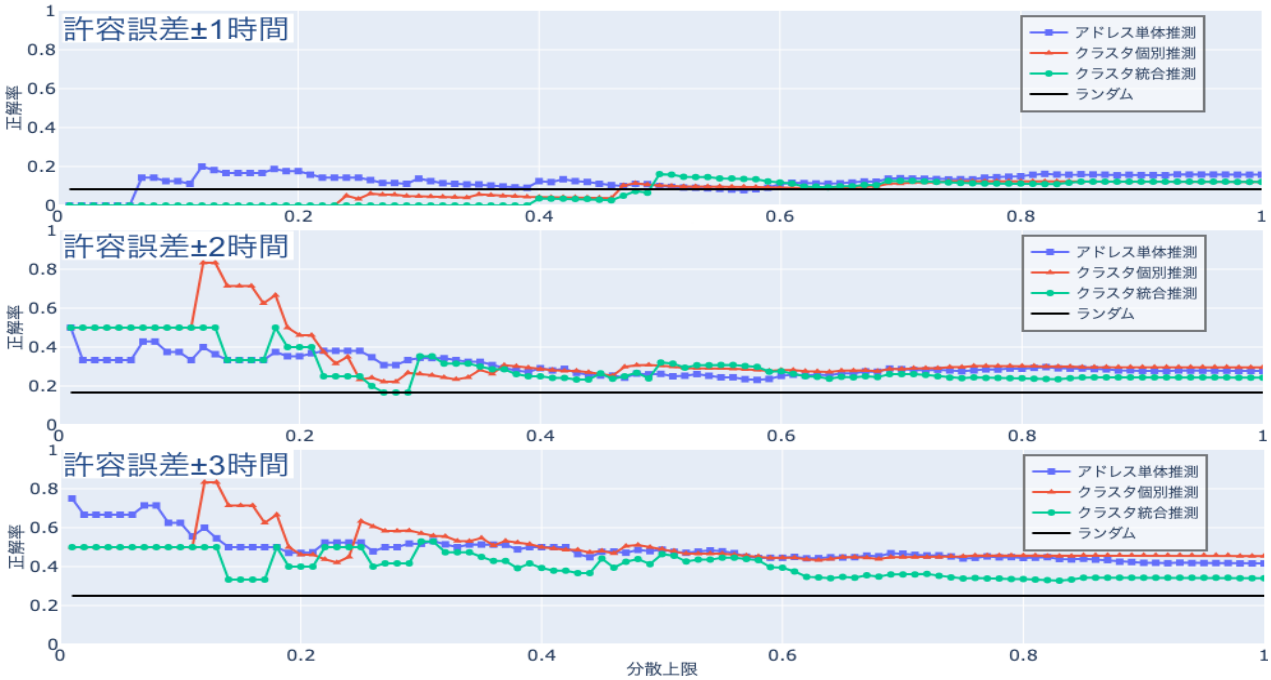

図 5　許容誤差ごとの正解率

送金 TX 数と送金時間分散の推測精度への影響については次章で検証する．

4. 精度検証

本章では提案手法によるタイムゾーンの推測精度の検証結果を述べる．

4.1 正解データセット

提案手法によるタイムゾーンの推測精度を評価するためには，犯罪者が管理する暗号資産アドレスと犯罪者の活動タイムゾーンの情報が正解データとして必要となる．そこで著者らはアメリカ財務省が公開している経済制裁リスト [7] から正解データセットを作成した．

アメリカでは違法薬物の密売やサイバー攻撃，テロ活動等を行う個人または組織に対して経済制裁を行なっている．アメリカ財務省では経済制裁の対象を公開しており，公開されている情報には Bitcoin アドレスや制裁対象の所在国や所在地域の情報が含まれている場合がある．そこで経済制裁リストのうち Bitcoin アドレスと所在国や所在地域が分かるデータについて抽出しデータセットを作成した．

所在国・所在地域のタイムゾーンへの変換

日本の東京と大阪では経度が異なるため，およそ 20 分程度の時差があるが，どちらの地域でもタイムゾーンとして UTC+9 が採用されている．一方で国土が広いロシアにおいては，モスクワでは UTC+3，ウラジオストクでは UTC+10 がタイムゾーンとして採用されている．このように同一国であっても経度の差から時差が存在し，また国によっては同一国内でも地域によって採用しているタイムゾーンが異なる場合がある．そこでデータセットを作成するにあたり以下のルールを定め，制裁対象の所在国や所在地域からタイムゾーンを算出した．

タイムゾーン算出ルール

ア．所在国のみ分かる場合は首都で採用されているタイムゾーンとする．

イ．所在地域が分かる場合はその地域で採用されているタイムゾーンとする．地域でタイムゾーンが採用されていない場合は首都で採用されているタイムゾーンとする．

ウ．複数の所在国や所在地域が記載されている場合は，アとイにより個別にタイムゾーンを求め，その平均値とする．

以上のルールにより国や地域情報からタイムゾーンを算出し，アドレスとそれに対応するタイムゾーンからなる 375 件のデータセットを作成した．

4.2 精度評価

前節で作成した正解データセットの Bitcoin アドレスに対して，3 つの提案手法(アドレス単体推測，アドレスクラスタ個別推測，アドレスクラスタ統合推測)によりタイムゾーンを推測した．そして提案手法により推測したタイムゾーンと正解データセットのタイムゾーンについて，差を計算し，これを推測誤差とする．また，推測誤差が許容誤差内に収まっている場合を正解とし，そうでない場合を不正解とすることで正解率を算出する．本研究ではこれを推測精度と呼ぶこととする．例えば正解データセットのアドレスに対応するタイムゾーンが UTC+1 で，提案手法による推測結果が UTC-1 の場合，推測誤差は 2 時間となる．この場合，許容誤差を ± 1 時間とすると不正解であり，許容誤差を ± 2 時間とすると正解となる．

図 5 に正解データセットのうち，送金 TX 数が 2 回以上のアドレスに対する，提案手法によるタイムゾーン推測の正解率を示す．図 5 には上から順に許容誤差を ± 1 時間以内，± 2 時間以内，± 3 時間以内とした場合の正解率を 3 つの折れ線グラフで描画している．横軸は提案手法により推測を行うアドレスの送金時間分散の閾値を示しており，

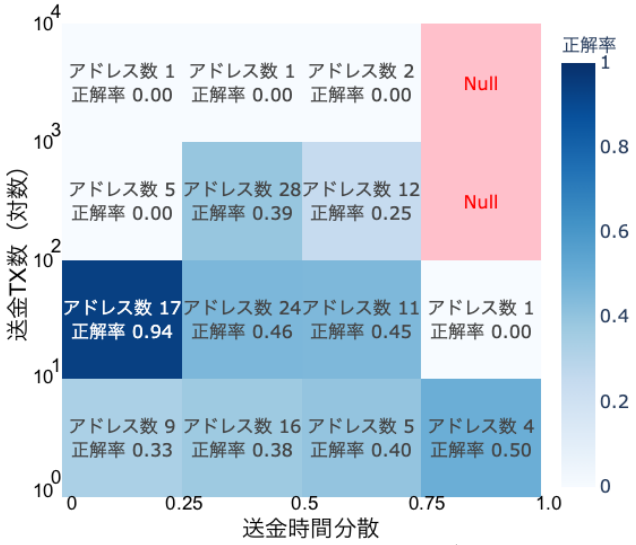

図 6　送金 TX 数と送金時間分散ごとの正解率

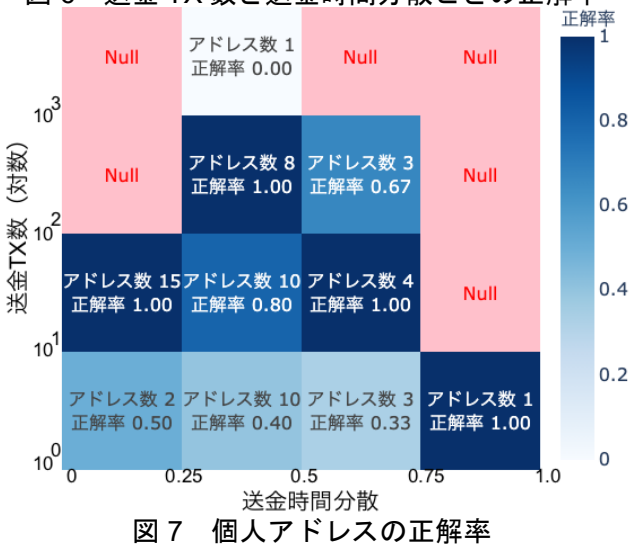

図 7　個人アドレスの正解率

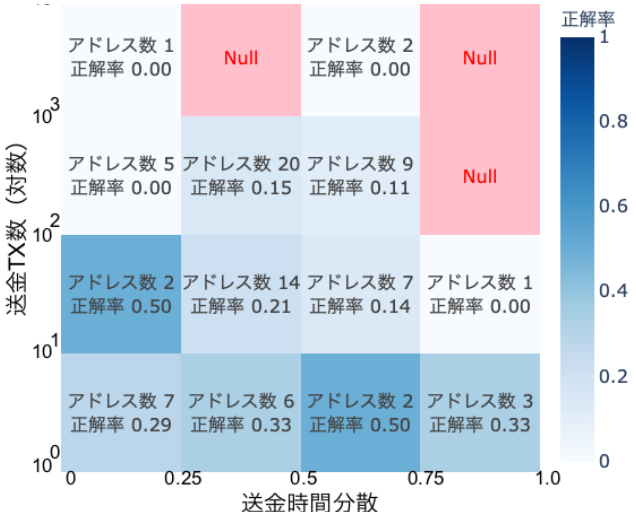

図 8　組織アドレスの正解率

送金時間分散が閾値以下となるアドレスについてのみ提案手法を適用した正解率を示す．例えば分散上限が 0.5 の場合，送金時間分散が 0.5 を超えるアドレスについては推測しない．分散上限が 1 の場合はすべてのアドレスについて推測を行う．また，提案手法の効果を確認するため，無作為にタイムゾーンを指定した場合の正解率を黒色の直線で示す．

図 5 から許容誤差が± 1 時間の場合はアドレス単体推測による正解率が高いことが分かる．一方で許容誤差を± 2 時間，± 3 時間と大きくした場合は，クラスタ個別推測による正解率が高くなり，送金時間分散の値が小さい場合に特に精度が高くなることが分かる．

4.3 送金 TX の推測精度への影響

3.3 節で述べた仮説を検証するため，正解データセットに対する提案手法の推測精度をヒートマップで示す(図 6)．ヒートマップの横軸は送金時間分散とし，縦軸を送金 TX 数の対数としている．各セルには該当する区間のアドレス数と正解率を表記し，正解率が高いほど濃い青色で表示している．また，該当するアドレスがない区間のセルは Null と表記している．なお許容推測誤差は± 3 時間とし，推測手法は 4.2 節において正解率が最も高い，アドレスクラスタ個別推測を用いた．アドレスクラスタ個別推測における送金 TX 数は，当該手法により推測に利用するアドレスクラスタ内のアドレスの送金 TX のうち，TX ID の重複を取り除いた送金 TX の合計とする．

図 6 において，送金時間分散が 0.25 未満かつ送金 TX 数が 10 回以上 100 回未満の区間では正解率が 94%と最も高く，当該区間において提案手法が有効に機能していると考えられる．一方で残りの区間で最も高い正解率は 50%であった．許容推測誤差を± 3 時間とした場合，ランダムでタイムゾーンを選択した際の正解率が 25%であることを考慮すると，残りの区間については提案手法があまり有効に機能していないと考えられる．

正解データセットのアドレスは，経済制裁対象となっている個人のアドレスと組織のアドレスに分類することができる．そこで個人アドレスと組織アドレスでの正解率を比較するために個人アドレスについての正解率を図 7 で，組織アドレスについての正解率を図 8 で示す．

図 7，図 8 から提案手法は個人のアドレスに対しては複数の区間において正解率が高いことが分かる．一方で組織のアドレスに対しては正解率が 25%程度かそれを下回る値であり，組織のアドレスに対して提案手法が有効に機能しているとは言えない．

次に提案手法が有効に機能している，個人アドレスに対する推測結果(図 7)から，送金 TX 数と送金時間分散による正解率への影響を検証する．まず送金 TX 数について見ると送金 TX 数が 1 以上 10 未満の区間では他の区間より正解率が低く，仮説の通り，提案手法は送金 TX 数が少な過ぎる場合，正解率が低下する．次に送金時間分散について見ると，分散が小さい区間の方が正解率が高い傾向にあると言える．一方で送金 TX 数が 10 以上ある場合，どの区間においても正解率が 67%以上あることから，送金時間分散による正解率への影響は送金 TX 数よりも小さいと考えられる．

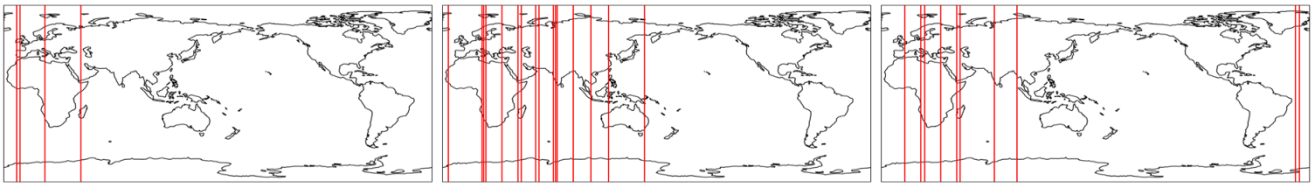

図 9　提案手法による犯罪者の活動地域の推測結果

4.4 処理制限

提案手法により正解データセットのアドレスについて，タイムゾーンを推測するにあたり以下の処理制限を実施することでタイムゾーンの推測に必要な処理を削減した．

制限 1　上限 TX 数の設定

アドレスごとに参加する TX 数は大きく異なり，TX 数が多いほど推測処理に時間がかかる．そこで 1 アドレス毎の分析 TX 数の上限を 1,000TX に制限し，1,000TX を超える場合は直近の 1,000TX のみ推測処理の対象とした．

制限 2　アドレスクラスタからのアドレスサンプリング

アドレスクラスタについて，アドレス数が 1,000 を超える場合，アドレスクラスタから 1,000 アドレスをランダムに抽出し，それらのアドレスのみを推測処理の対象とした．

5. 分析事例

本章では日本国内において犯罪への関与があったと見られる Bitcoin アドレスについて，提案手法により犯罪者の活動タイムゾーンを推測した結果を分析事例として示す．

本分析では 2021 年 1 月から 2024 年 2 月までの期間において，犯罪に関与したと見られるものとして，国内で確認されたアドレスを分析の対象とし，その中でも，件数が多かったセクストーション，フィッシング詐欺，投資詐欺のいずれかの犯罪への関与があったと見られる 76 アドレスについて分析する．なお本分析は 2024 年 6 月に実施した．

5.1 分析方法

提案手法は対象アドレスの送金 TX 数や送金時間分散により推測精度が増減する．本分析では推測精度を確保するために 4 章の検証結果を参考にし，送金 TX 数が 5 回以上かつ，送金時間分散が 0.9 以下のアドレスに対してのみ推測する．推測にはアドレスクラスタ個別推測手法を用いるが，対象アドレスにアドレスクラスタが存在しない場合は代わりにアドレス単体推測手法により推測する．

5.2 分析結果

犯罪カテゴリの一つであるセクストーションでは，当該犯罪への関与があったと見られる 37 アドレスの内 29 アドレスについては少なくとも 1 回は TX に参加している．一方で残りの 8 アドレスは一切 TX に参加しておらず，未使用のアドレスと言える．未使用アドレスや 5.1 節で定めた条件を満たさないアドレスは推測対象から除外するため，推測できるアドレスは限られる．犯罪カテゴリごとの推測の可否を表 1 に示す．

次に犯罪カテゴリごとの推測結果を図 9 に示す．図 9 ではアドレスごとに推測したタイムゾーンに対応する位置を赤い縦線で示している．なお，同一犯罪カテゴリにおいて複数のアドレスで推測結果が同じタイムゾーンとなった場合は，縦線の位置が重複し区別がつかなくなるため，縦線の位置を少しずらして描画している．

表 1　分析対象のアドレスの内訳

犯罪カテゴリ	分析対象アドレス数	TX数が1以上のアドレス数	推測できたアドレス数
セクストーション	37	29	4
フィッシング詐欺	28	28	16
投資詐欺	11	11	10

セクストーション

当該犯罪では，犯罪者は被害者の性的な画像をばら撒く等の脅迫により暗号資産を恐喝する．前述の通り，当該犯罪アドレスのうち 8 アドレスは TX に参加していないため推測の対象外である．さらに別の 25 アドレスは TX 数が少なくとも 1 回あるが，アドレス単体とアドレスクラスタの両方において送金 TX 数が 5 回未満であるため，これらのアドレスも推測の対象から除外した．最終的に 4 アドレスについてアドレスクラスタ個別推測によりタイムゾーンを推測できた．推測できた 4 アドレスのうち 2 アドレスは，アドレス数 44 の同一のアドレスクラスタに所属していた．

今回分析した当該犯罪カテゴリのアドレスは，送金 TX 数が少ない傾向にあった．そのため犯罪者の活動タイムゾーンを推測できたアドレス数は少ない．推測できた 4 アドレスについても上述の 2 アドレスはアドレス単体での送金 TX 数は 1 回のみであった．これら 4 アドレスの推測結果のタイムゾーンはヨーロッパやアフリカ大陸がある経度に集中している．

フィッシング詐欺

当該犯罪では，犯罪者は被害者をフィッシングサイトに誘導し，ID とパスワードを窃取した後，暗号資産取引所等にアクセスし，ウォレット内の暗号資産を別のウォレットに送金する．当該犯罪アドレスは 28 アドレスあり，いずれのアドレスについてもアドレスクラスタが存在しなかった．従ってアドレスクラスタ個別推測はできず，アドレス単体推測により推測した．12 アドレスについては送金 TX 数が 5 回未満であったため推測できず，推測できたのは約半数の 16 アドレスであった．

推測結果のタイムゾーンはユーラシア大陸広域およびアフリカ大陸がある経度に集中している．

投資詐欺

当該犯罪では，犯罪者はマッチングアプリ等で知り合った被害者を，実態のない暗号資産投資に勧誘し，投資資金の名目で暗号資産を送金させて詐取する．当該犯罪アドレスは 11 アドレスありそのうち 1 アドレスについては送金 TX 数が 2 回のみであったため推測できなかった．

残りの 10 アドレスはアドレスクラス個別推測により推測できたが，そのうち 1 アドレスは送金時間分散が異常に小さかった．当該アドレスはアドレス数が 494 のアドレスクラスタに所属しており，これらのアドレスの送金 TX 数は 51 回ある．しかし，これらの送金 TX の送金時間分散は

0.0004 と異常に小さい．そこで当該アドレスクラスタの送金 TX 時刻について詳細に確認したところ，送金 TX 時刻が UTC+0 の 0 時 0 分頃に集中していることが判明した．このことから当該アドレスクラスタに所属するアドレスは，何らかの条件を満たすと，自動的に UTC+0 の 0 時 0 分頃に送金処理を行うように犯罪者により設定されていると考えられる．そのため提案手法による当該アドレスに対するタイムゾーンの推測は有効でない．

6. 考察

4 章では提案手法の精度について評価するために，正解データセットを作成し，正解率を評価した．許容誤差が±１時間の場合はアドレス単体による推測精度が高く，許容誤差を±２時間や±３時間に増やした場合，アドレスクラスタ個別推測による精度が高かった．アドレスクラスタ個別推測では，推測対象のアドレスだけでなく，同一クラスタのアドレスも含め推測を行う．そのため，推測に利用できる送金 TX 情報が多くなり，推測精度が向上すると考えられる．一方でアドレスクラスタには，管理者が異なるアドレスが混入する可能性もあり，その場合は推測対象以外のアドレスの送金 TX 情報も加味されてしまうため，推測タイムゾーンの誤差が大きくなると考えられる．以上の理由により，許容誤差が小さい場合は，無関係のアドレスの送金 TX 情報が推測に使われる余地がない，アドレス単体推測の精度が最も高い結果となったと考えられる．

アドレスクラスタ統合推測は多くの場合においてアドレスクラスタ個別推測よりも低い精度であった．この原因は不明であるが，アドレスクラスタ統合推測ではアドレスクラスタ個別推測とは異なり，送金 TX 数が 1 回しかないアドレスの TX 時刻も推測に利用する．そのため送金 TX 数が少ないアドレスが推測精度の低下の原因となっている可能性が考えられる．

提案手法は犯罪者が一般企業のように組織だって活動するため，活動時間が日中に集中するという仮定に基づいて推測を行う．しかし 4.3 節において提案手法は組織に紐づけられているアドレスに対する推測精度が低かった．従って，正解データセットにおいて，組織に紐づけられているアドレスの多くが，仮定とは異なる運用をされていると考えられる．

5 章では分析事例として，日本国内において犯罪に関与したと見られるアドレスについて，提案手法により犯罪者の活動タイムゾーンを推測した結果を示した．分析の過程で，各犯罪カテゴリで送金 TX 数やアドレスクラスタの有無に特徴があり，犯罪カテゴリにより有効な推測手法が異なることが判明した．また，どの犯罪カテゴリの推測結果も日本以西のタイムゾーンに偏っており，日本やアメリカ大陸付近のタイムゾーンはほとんどなかった．

提案手法による推測の幅は広く，国を特定することはできないが，どの地域で犯罪者が活動をしているのか大まかに推測できる．

7. 関連研究

文献[8]ではサイバー犯罪組織が配布したマルウェアのコンパイル時間やドメイン登録時間に基づき，犯罪組織の活動国を推測している．文献[9]では攻撃対象組織の関係者になりすまし，電子メールにより侵入を試みる犯罪者の活動地域について，犯罪者からの連絡時間から推測している．これらの分析は時間情報から犯罪者の活動地域を推測している点において本研究に類似している．

文献[10]~[11]では Bitcoin の取引時間から取引所のタイムゾーンの推測を行う．当該研究では取引所ユーザによる取引タイミングはインターネット利用時間帯と相関があると仮定して推測を行なっている．また文献[12]では Bitcoin アドレスとそのアドレスクラスタの送金 TX 時刻からタイムゾーンを推測している．これらの研究は Bitcoin の取引時間からタイムゾーンを推測する点や Bitcoin アドレスのクラスタを利用する点について本研究と類似している．一方で本研究では推測の対象を犯罪者とし，犯罪者のアドレスが含まれるデータセットを用いて精度を検証している．またタイムゾーンを推測する手法を複数提案し，それぞれの手法やアドレスの送金時間分散と送金 TX 数による正解率の違いを検証している点において異なる．

8. まとめと今後の課題

本稿では暗号資産の送金時間帯から犯罪者の活動地域を推測する手法を提案し，送金 TX 数と送金時間分散の違いによる推測精度への影響について，検証結果を示した．また，提案手法による分析事例として，日本国内で犯罪へ関与したと見られるアドレスについて，提案手法によりタイムゾーンを推測した結果を示した．

提案手法では送金 TX に複数回参加している，犯罪に利用された任意のアドレスについてタイムゾーンを推測可能である．しかし対象とするアドレスが日中に運用されていない場合は正解率が低下する．そのため，アドレスの運用方法の検知や，検知した運用方法に合わせた効果的なタイムゾーン推測アルゴリズムの提案が課題である．

参考文献

[1] トレンドマイクロ, “近代的なサイバー犯罪グループの組織構造を解明する”, https://www.trendmicro.com/ja_jp/research/23/k/unpacking-the-structure-of-modern-cybercrime-organizations--.html

[2] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, (2008).

[3] 廣澤 龍典, 上原 哲太郎, “ビットコインのミキシングにおける資金移動の分析”, 第 81 回 CSEC・第 41 回 IOT 研究発表会, (2018).

[4] Androulaki Elli, et al, "Evaluating user privacy in bitcoin", Financial Cryptography and Data Security, (2013).

[5] Reid Fergal, Martin Harrigan, “An analysis of anonymity in the bitcoin system”, Springer New York, (2013).

[6] Ron Dorit, Adi Shamir, “Quantitative analysis of the full bitcoin transaction graph”, Financial Cryptography and Data Security, (2013).

[7] アメリカ合衆国財務省, “OFAC Sanctions List Service”, https://sanctionslist.ofac.treas.gov/Home/

[8] PwC サイバーサービス, “Operation Cloud Hopper”, https://www.pwc.com/jp/ja/japan-service/cyber-security/assets/pdf/operation-cloud-hopper.pdf

[9] Google, “Exposing initial access broker with ties to Conti”, https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/

[10] 井垣秀星, 永田幸大, 菊池浩明, “平均取引時間分布の相関を用いた Bitcoin ユーザのタイムゾーンの推定”, 第 81 回全国大会講演論文集, (2019).

[11] 山崎孝順, et al, “取引件数の時間分布の相関を用いた Bitcoin 取引所のユーザの属性推定”, 第 82 回全国大会講演論文集, (2020).

[12] DuPont Jules, Anna Cinzia Squicciarini, "Toward de-anonymizing bitcoin by mapping users location", Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, (2015).