Title	暗号資産 (特にBitcoin) を使った詐欺犯罪の探索的分析とセキュリティ向上への提言
Sub Title	
Author	江原, 貴史(Ehara, Takashi) 高橋, 大志(Takahashi, Hiroshi)
Publisher	慶應義塾大学大学院経営管理研究科
Publication year	2022
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2022年度経営学 第3945号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40003001-00002022-3945

慶應義塾大学大学院経営管理研究科修士課程

学位論文（　　2022　年度）

論文題名

暗号資産(特にBitcoin)を使った詐欺犯罪の探索的分析とセキュリティ向上への提言

主　査	高橋 大志
副　査	大林 厚臣
副　査	小幡 績
副　査	

氏　名	江原 貴史

論 文 要 旨

所属ゼミ	高橋大志 研究会	氏名	江原　貴史

（論文題名）
暗号資産(特に Bitcoin)を使った詐欺犯罪の探索的分析とセキュリティ向上への提言

（内容の要旨）

ビットコインは，2008 年にサトシ ナカモトによって発案されて以来，注目を集めてきた．WEB3 の中核インフラである暗号資産等の法整備は今後も進んでいくと思われる．一方で，暗号資産に絡んだ，資金洗浄，ハッキング，詐欺などの違法，不正取引は後を絶たない．その背後には犯罪組織，ならず者国家，テロ組織の存在も指摘されている．

ビットコインの特徴の一つとして匿名性が挙げられる．暗号資産の取引情報はブロックチェーン上にすべて記録され，取引の当事者以外でも，取引の流れを追跡できるが，アドレス所有者を特定することは困難である．それゆえに，犯罪や不正行為を規制するのが難しい．暗号資産がより普及するためには犯罪取引を特定し，取り締まることが必要である．そのための技術は，注目されており，世界各国の犯罪当局は，民間の暗号資産追跡サービスを使用している．また民間の金融機関や暗号資産取引所においても Anti Money Laundering のためにそのようなサービスを使用している．

本論文では，世界最大のビットコインデータである Elliptic Dataset（違法取引 4,545 合法取引 42,019 件,違法合法不明取引 157,205 件）について機械学習の手法を使い，取引の違法・合法の分類精度の向上を試みた．先行研究においては，以下の２点が示されている．

① 各種機械学習モデルのうちランダムフォレスト法による分類精度が最も高い．グラフ情報を加味することができ，高い分類精度を期待できるはずの GCN 法（グラフコンボリューションネットワーク）の分類精度よりもランダムフォレスト法による分類精度が上回る．

② 取引の時間帯によって著しく分類精度が低くなる．

本論文においても，分析データとして Elliptic Dataset を対象とし，①②について分類精度の向上を試み，以下のような結果を得た．

① について，教師あり学習の各種手法についてアンサンブル学習手法を施した．また，違法取引の件数が合法取引と比べて少ない不均衡データであることから， SMOTE 法によってオーバーサンプリングすることによってランダムフォレスト単体の場合よりも分類精度が向上することを確認した．また教師なし学習の手法であるクラスタリング手法を組み合わせることで，分類精度が向上することを確認した．

② について，教師あり学習とそのアンサンブル学習手法，オーバーサンプリング手法で精度の向上は確認できなかった．学習データと予測データの区切りを細かくして実験したところ，違法取引のパターンが時間帯によって大きく異なる可能性が示唆された．異常検知の手法によっても分類を試みたが，再構成誤差が合法取引よりも低く，違法分類できないことが示唆された．グラフ情報（次数分析など）からも分類を試みたが，有益な情報は得られなかった．

上記結果を踏まえ，セキュリティ向上についての考察と提言を以下のようにまとめる．

既知の違法取引の分類精度は教師あり学習で高めることができる，ビットコインの不正情報を収集する公的機関を設置し，その情報を即時的に共有し犯罪特定に活用することを提言する．

未知の違法取引に対しては異常検知の手法においても検出することが困難であったが，これはビットコインのアドレス生成が無制限にでき，小口化分散化が容易であることに起因すると考える．アドレスの生成にペナルティを課すことで，犯罪アカウントの小口化，分散化を抑止でき，追跡も容易にすることを提言する．

目次

第１章　はじめに 6
第２章　先行研究 8
２-１ 先行研究の概略 8
２-２ 本研究で使用する Elliptic Data Set に関する先行研究 8
第３章　目的 10
第４章　データ 11
４-１ 取引件数と種別 11
４-２ 特徴量 11
４-３ グラフ情報 12
第５章　分析方法 13
５-１ 本研究で使用した機械学習モデルの概要 13
５-１-１ 教師あり学習 13
５-１-２ 教師なし学習 14
５-１-３ 半教師あり学習 14
５-１-４ 不均衡データにおける分類手法 14
５-１-５ 教師あり学習における不均衡データの扱い方 15
５-１-６ 教師なし学習における不均衡データの扱い方 15
５-２ データサンプリング（訓練データとテストデータの切り分け） 15
５-３ 評価指標 16
５-３-１ 教師あり学習および半教師あり学習 16
５-３-２ 教師なし学習 16
５-４ 本研究における各分析の見取り図 16
第６章　分析１-時系列を考慮せず，分類精度の高さを追求 18
６-１ 教師あり学習による分類精度測定 18
６-１-１ 各種教師あり学習モデルによる分類精度測定 18
６-１-２ パラメータチューニング 18
６-１-３ アンサンブル学習①バギング 19
６-１-４ アンサンブル学習②ブースティング 20
６-１-５ アンサンブル学習③スタッキング 21
６-２ Smote 法によるオーバーサンプリング 22
６-３ 半教師あり学習による分類精度測定 23
６-３-１ ラベル拡散法（Label Spreading） 23
６-４ 第６章のまとめ 24

第７章　時系列を考慮した上での分類精度向上について 25
7-1 分析①前章の手法での精度確認 25
7-1-1 トレーニングデータ，テストデータの分割 25
7-1-2 分析方法 25
7-1-3 結果と考察 26
7-2 分析②時間帯毎のデータの特性分析Ⅰ 27
7-2-1 データセットのトレーニング，テストの分割方法 27
7-2-2 分析方法 27
7-2-3 結果と考察 28
7-3 分析③時間帯毎のデータの特性分析Ⅱ 29
7-3-1 データセットのトレーニングデータ，テストデータの分割 29
7-3-2 分析方法 30
7-3-3 結果と考察 33
7-4 教師あり学習と教師なし学習のハイブリッド手法 33
7-4-1 クラスター分析（教師なし学習）と PCA による次元圧縮によるノイズ除去と Random Forest（教師あり学習）のハイブリッド学習 33
7-4-2 クラスター分析と Random Forest によるハイブリッド手法（PCA による次元圧縮なし） 36
7-4-3 クラスター分析の結果のみを特徴量とした場合の分類精度 37
7-5 半教師あり学習 37
7-5-1 ラベル拡散法（Label Spreading）オーバーサンプルなし 37
7-6 第７章のまとめ 38
第８章　異常検知手法での分類精度向上への取り組み 39
8-1 異常検知手法 39
8-1-1 主成分分析による次元削減，復元時の再構成誤差について 39
第９章　グラフデータの分析 42
9-1 各種次数分析 42
9-1-1 各種次数について 42
9-1-2 各種次数の集計 43
9-2 グラフ情報の視覚化 47
第１０章　まとめと提言 49
参考文献 52
Appendix　詐欺メールとその違法アカウントに対する予備調査 56
データ 56
分析項目 56

分析例 57
分析結果 62
メールの送信情報 62
詐欺の成功可能性 62
詐欺メールの言語と被害者の居住地 62
不正アカウントのビットコイン送信先属性 62
AMLBot のリスクスコア 62
A1　詐欺メール，IP，不正アドレス等の集計表 64
A2　詐欺アドレスのリスクスコアリング 66
謝辞 74
図表目次 76

第１章　　はじめに

ビットコインは，２００８年にサトシ　ナカモトによって発案されて以来，注目を集めてきた．[1]

日本においても，経済活動の中に急速に組み込まれている．２０１７年４月に資金決済法において，“仮想通貨”という箇所が付け加えられ，法律的に合法的な決済手段として認められた．仮想通貨交換業者は一定の要件を満たし，総理大臣の登録を受けなければならなくなった．また税金の課税方法も確立された．さらに，２０２２年６月３日に可決された改正資金決済法では，ステーブルコインについての規制が規定され，いよいよ法定通貨と暗号資産が円貨の決済においても共存，競争する時代に入ってきている．

また，岸田政権のみならず，野党までもが WEB3 への関心を示しており，その中核にある暗号資産周辺の法整備やサポートが進んでいくことが期待される．[2] [3]

ビットコインの時価総額は３０００億ドル程度であるのに対して伝統的な資産として数千年の歴史を持つ金の投資可能額は ２兆６０００億ドル程度と推定されており，金の１０％強程度の価値を持つまでになってきている．ビットコインだけでなく種々の暗号資産の時価総額は８０００億ドル程度（過去１年間だと３兆ドルから８０００億ドルの間で推移）しており，金の投資可能額に迫るまでの資産に成長してきている．[4] [5]

ロシアのウクライナ侵攻時には，ビットコインがロシアにとっては経済封鎖網，資金凍結網の抜け穴として働き，対するウクライナにとっては，ビットコインで世界から寄付を集める手段となっている．

一方で，MtGOX 社や Coin Check 社，さらに最近は FTX 社の事件など，世界中で日々，暗号資産がハック（盗難）されており，その背後に国家も含め様々な犯罪組織やテロリスト組織がいるとされている．またランサムウェアの身代金の振り込み先，振り込め詐欺など様々な犯罪資金洗浄先としてもビットコインは悪名高い．身近な例としては，ランサムウェア等を私の PC もしくは携帯端末に埋め込み，私のプライベートな情報を抜き出したことを装い，情報の拡散や，PC のロックをされたくなければ犯罪者が指定したビットコインアドレスに数十万円相当のビットコインを振り込むように要求する振り込め詐欺と脅迫を併せ持ったメールを受け取ることがある．

ビットコインの主な特徴の一つとして匿名性が挙げられる．暗号資産の取引

情報はブロックチェーン上にすべて記録されており，取引の当事者以外でも，取引の流れを追跡できる．しかし，その取引のアドレスを誰が所有しているのかを特定することは困難である．それゆえに犯罪にビットコインが利用され，それを防止するための規制も充分に行き届かない．

今後，ビットコインが社会に普及していく中で，取引の安全性や，資産価値を保持するために，ビットコインネットワーク内の不正なアドレスを特定し，排除することが必要である．商用サービスとして，詐欺，ランサムウェア，ダークネット関係の不正アドレスであるか否かのスコアリングを有料で行うサービスが存在する．どのような手法でスコアリングしているのかは，定かではないが，アメリカをはじめ先進国では，犯罪当局が捜査において，また暗号資産取引所が AML（Anti Money Laundering）の要件を満たすべく，AMLBot や Elliptic，Chainalysis のような民間のサービスをいくつか複合的に利用している． [6] [7]

第２章　　先行研究

２-１　先行研究の概略

[8]によると，ビットコインをはじめとする暗号資産において，ブロックチェーン上にすべての取引情報が記録され，取引当事者でなくても取引の流れを追跡できるが，取引当事者である実際の個人を特定することは困難である．最近では，暗号資産の取引に付随する情報を用いることなどにより，取引当事者をある程度絞り込むことができるとする研究成果が見られる一方で，取引の追跡困難性を高める新たな手法も提案されている．

[9] によると，不正なアドレスを特定するための研究は，２つのカテゴリーに分けることができる．

① 異常なユーザーとトランザクションを検出すること．

[10]は，異常な行動が疑わしい行動の代理変数だとみなし，ユーザーをノードとしたビットコイン取引ネットワークグラフと，取引をノードとしたビットコイン取引ネットワークに対して，教師なし機械学習である，K-Means clustering，マハラノビス距離，SVM を使って，窃盗と，流出の検出を試みているが，３０件の既知の窃盗，流出のうち検出できたのは３件となっている．[11]も同様に K-Means clustering によって不正取引の検出を試みている．

② 詐欺，ランサムウェア，ダークネット市場，ハッキングなどの不正なアドレスに焦点を当て検出すること．

[12]は 200K 以上のビットコイン取引（ノード）、23K 以上のビットコイン取引（ノード）の時系列グラフのデータセット（Elliptic Data set [13]）を作成，使用して，ロジスティック回帰，Random Forest，多層パーセプトロン，グラフ畳み込みネットワークなどの様々な手法で分析を試みている．本修士論文では Elliptic Data Set を分析対象とする．

２-２　本研究で使用する Elliptic Data Set に関する先行研究

[12]によると Elliptic Data Set における違法合法の分類精度に関して，以下の２点を示した．

①　各種機械学習モデルのうちランダムフォレスト法による分類精度が最

も高い．グラフ情報を加味することができ，高い分類精度を期待できるはずの GCN 法（グラフコンボリューションネットワーク）の分類精度をもランダムフォレスト法による分類精度が上回る．

② 取引の時間帯によって著しく分類精度が低くなる．

[14]は [12]を踏まえ，Elliptic Data Set における違法合法の分類精度に関して，サンプリング手法と，変数選択について様々なパターンで測定し，アンダーサンプリングと変数選択によって精度の向上できることを示した．

[15]は [12]を踏まえ，Elliptic Data Set における違法合法の分類精度に関して，Extreme Gradient Boosting 法を改良し，またオーバーサンプリング法によって精度の向上できることを示した．

第３章　　目的

今後，暗号資産が一般に受け入れられるためには，マネーロンダリングや窃盗,詐欺などの犯罪を抑え込むために,違法取引を特定することが必要である．そのために，本研究では下記を明らかにすることを目的とする．

- 合法取引と違法取引の分類を，機械学習を使って行い，分類精度の向上を目指す．[12]を踏まえて，分析を進める．第４章，第５章，第６章，第７章，第８章，第９章で論じる．
- 犯罪を減らすために制度面でできることがないかを考察する．第１０章で論じる．
- 詐欺グループのビットコイン取引のパターンをまとめる．Appendix で論じる．

第４章　　データ

本稿では, ビットコインの取引データである Elliptic Dataset [12] [13] [16] を使用する.

４-１　取引件数と種別

ビットコインの取引をノードと呼び, ノードの種別, 件数は以下の通りである.

- 全ノード数 :203,769 件
- 違法取引　:4,545 件　（図 1 の赤）
- 合法取引　:42,019 件　（図 1 の緑）
- 違法か合法かの区別が不明な取引：157,205 件　（図 1 の橙）

教師あり学習では違法取引と合法取引について扱い，不明取引については扱わない．教師なし学習においては不明取引も扱う.

違法取引と不明取引の件数の比率は 1:9 であり，不均衡データである.

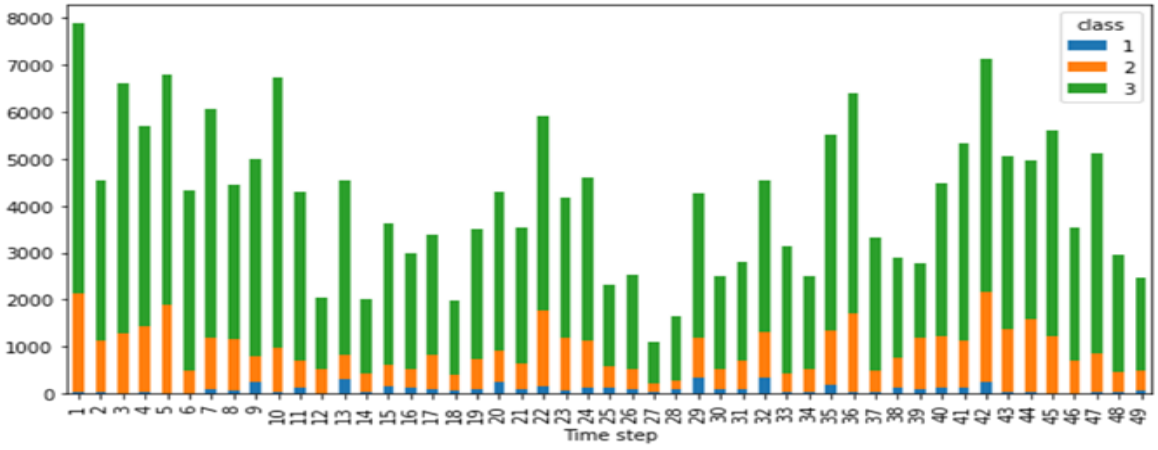


Fig　4-1　Number of Illicit, Licit, Unknown trades.

４-２　特徴量

特徴量についてタイムステップ以外の特徴量の具体的な計算方法などは知的財産の関係で非公開となっている．データ提供者である Elliptic 社 [12] [13] [16]で示されているデータの概略は，以下の通りである.

- 特徴量：166

- ローカルな情報を含む特徴量：９４個
  - 94 の特徴量はトランザクションに関するローカルな情報を表している.
    - 時間情報：タイムスタンプ１～４９（１ステップ当たり約３時間，全期間で約２週間）ただし具体的な期間の年月日は公開されていない.
    - インプット／アウトプット数、トランザクション手数料、アウトプット量、インプット／アウトプットが受け取った平均 BTC, インプット／アウトプットに関連するトランザクションの平均入出数を平均ゼロ標準偏差１に標準化されている.
- 非ローカルな情報を含む特徴量：７２個
  - グラフ情報（取引同士の関係）を集約したもので，センターノードから１ホップ前後の取引情報を用いて，入出力数，取引手数料などに対する近隣取引の最大最小，標準偏差，相関係数などを含み，それらが，平均０，標準偏差１に標準化されている.

４-３　グラフ情報

ビットコインのノード（取引）同士の繋がりをエッジという.

- ノード：203,769 件
- エッジ：234,355 件

ノード同士の関係は１対１ではなく１対多数であるのでエッジ数＞ノード数である.

第５章　　分析方法

５-１　本研究で使用した機械学習モデルの概要

機械学習は，何かしらの目的を達成するための知識や行動を，データを読み込むことで機械に獲得させるための技術である．機械学習には大きく，①教師あり学習，②教師なし学習，③強化学習がある．

本研究においては教師あり学習，教師なし学習さらにそのハイブリッドである半教師あり学習を扱う．

５-１-１　教師あり学習

教師あり学習は，説明変数（X）から目的変数（Y）を予測するモデルを求める手法である．モデルに訓練データの説明変数を入力し，そのモデルからの出力が訓練データの目的変数に近づくようにモデルのパラメータを調整することで学習していく．本研究では，１６６個の特徴量を説明変数（X）とし，違法取引，合法取引の別を目的変数（Y）とし，その分類精度を上げるようにモデルを訓練させる．

本研究では Decision Tree，Logistic Regression, Support Vector Machine, Gradient Boosting Tree，k-Nearest Neighbors，Random Forest を扱う．

①　教師あり学習におけるアンサンブル学習

弱い学習器（例えば決定木，ロジスティック回帰など）を複数束ねて強い学習器を作る手法である．

①-1　Bagging 法

Bootstrap 法により複数回抽出されたデータにより学習した弱い学習器を並列に扱い，その分類結果を多数決して最終的な分類結果として出力する．[17]　Random Forest は Tree を Bagging したモデルである．本研究では Tree, Logistic Regression , Random Forest, Gradient Boosting などの学習器を Bagging して分類精度の向上を試みる．

①-2　Boosting 法

一つの弱学習器で予測した結果を次に作成する学習器に引継ぎ逐次学習していく．[17] Gradient Boosting は Tree を Boosting したモデルである．本研究では Random Forest, Logistic Regression，Tree を Boosting して分類精度

の向上を試みる.

①-3　Stacking 法

二段階以上にわたって学習器を配置して学習する．第一段階で学習させたモデルによる出力結果を第二段階の入力とし第二段階の学習器を学習させその出力結果をもとに分類を行う． [17] [18]

5-1-2　教師なし学習

入力データそのものに着目し，データに潜むパターンや示唆を見出す手法である．多数のデータをいくつかの類似グループに分けるクラスタリングや，データ次元を，元のデータの情報を失わないように少数の次元に縮約するのに使われる．本研究では主成分分析，K-Means 法，を扱う.

5-1-3　半教師あり学習

半教師あり学習は､教師あり学習と教師なし学習を組み合わせた手法である。
学習データとして、正解ラベルがついているデータと正解ラベルがついていないデータの両方を使う。一部の正解ラベルの付いたデータを用い，正解ラベル無のデータのラベルを事前に予測し，正解ラベル付きデータと統合する.

① Label Spreading 法

半教師あり学習の手法として Label propagation 法と Label spreading 法がある．両方式ともに，ひとつひとつのデータをノード，データの類似度をエッジ（の重み）としたグラフを構成して，このグラフ上でラベルを伝播（コピー）する．あるデータのラベルをその近傍にあるラベルのないデータにコピーすることで，少量のラベル付きデータからモデルを学習する． [19] [20]. 本研究では計算機の計算能力の関係で Label spreading 法を使用した.

5-1-4　不均衡データにおける分類手法

本研究で扱うデータは違法取引件数と合法取引数の割合が約１：９の不均衡データである．教師あり学習を使う場合と教師なし学習の場合の手法について概説する.

5-1-5　教師あり学習における不均衡データの扱い方

不均衡データを，教師あり学習の分類モデルに学習させると，少数派の分類精度が低いモデルが生成されやすいことが知られている．この問題を克服するための方法として以下の２つの手法が使われている．

- ✧ オーバーサンプリング手法およびアンダーサンプリング手法を使って両カテゴリーのデータ数を等しくしたうえで，機械学習モデルを生成する．
- ✧ 機械学習モデルの損失関数のパラメータ調整をする．

①　SMOTE 法

本研究ではオーバーサンプリング手法のうち，SMOTE 法(Synthetic Minority Oversampling Technique) [21]とその拡張版である Borderline Smote,　SVM Smote, ADASYN を使用した．

5-1-6　　教師なし学習における不均衡データの扱い方

教師なし学習により不均衡データで少数派の分類をする場合には，少数派のデータを外れ値として扱う異常検知の方法と，クラスタリングによる方法が知られている．

①　異常検知の手法

主成分分析によって多数派データを正常データとみなし，多数派データの特徴量ベクトルから固有値ベクトルを算出し．その固有値ベクトルを利用して次元圧縮し逆行列で特徴量ベクトルを復元した際に，特徴量ベクトルの損失（再構成誤差）が大きいものを外れ値とみなす．　[22]

②　クラスタリングの手法

K-Means 等のクラスタリング手法により少数データと多数データでクラスタリングされることを期待する．

5-2　データサンプリング（訓練データとテストデータの切り分け）

本研究では，データ全体を訓練データとテストデータを２つに切り分ける際に以下の２つの方法を用いた．

① データの時系列の順番を考慮せず : データ全体から訓練データとテスト

データを無作為に切り分けた．例えば，データ全体から８５％を無作為に抽出し訓練データとし，テストデータを残りの１５％とした．

② データの時系列を考慮：データ全体の前半８５％を訓練データ，後半１５％をテストデータとした．将来起こる違法取引について現在までの情報を用いて分類，予測できるかを測定するためである．

5-3　評価指標

5-3-1　教師あり学習および半教師あり学習

Accuracy, precision, recall, F1-score について主に結果に掲載する．不均衡データにおいて accuracy が高く出るので（ただし高ければ高いほど優秀なモデルではある），本研究では，不均衡データの分類問題で重要とされる F1-score（precision と recall の調和平均）を最重要な指標とする．不正取引の検出力は recall で測定されるので，F1-score に次いで重要と考える．

5-3-2　教師なし学習

主成分分析による異常検知においては再構成誤差を評価指標とする．

5-4　本研究における各分析の見取り図

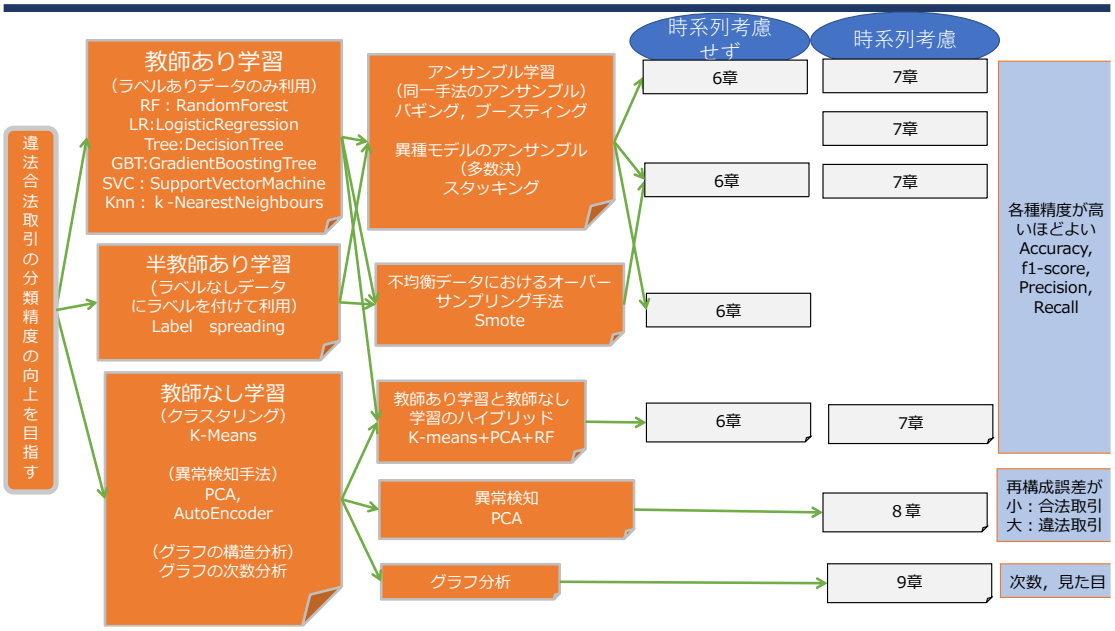


Fig 5-1　本研究における各分析の見取り図

第６章　　分析１-時系列を考慮せず，分類精度の高さを追求

本章では，先行研究で行われている通り，時系列を考慮せず，データ全体に対して分類精度の高いモデルを構築することを目的とする．

先行研究では Random Forest の分類精度が高いことが確認されている．本章では教師あり学習の各種手法による分類精度を測定し，Random Forest による分類精度が高いことを確認し，その上でさらに高い分類精度を実現するために，①パラメータチューニングを②バギング，ブースティング，スタッキングなどアンサンブル学習，③オーバーサンプリングの各種手法による分類精度を測定する．

６-１　教師あり学習による分類精度測定

６-１-１　各種教師あり学習モデルによる分類精度測定

①方法

各種教師あり学習モデルによる分類精度を測定した．データは訓練データ８５％，テストデータを残り１５％とした．

Table 6-1 Supervised learning models classification performance

shuffle=true,train:test=0.85:0.15	accuracy	precision	recall	F1Score
DecisionTree	0.98	0.884	0.923	0.903
GradientBoost	0.987	0.992	0.882	0.934
kNN	0.976	0.899	0.862	0.88
LogisticRegr	0.965	0.856	0.781	0.817
RandomForest default	0.989	1	0.893	0.944

②結果

いずれの評価指標（accuracy, precision, recall, F1Score）でも Random Forest,が最も高い分類精度を示しており，先行研究と一致する．

６-１-２　パラメータチューニング

Random Forest の分類精度が高いことが確認できた．次に，Random Forest

においてパラメータチューニングによる精度向上を試みる.

① 方法

Random Forest でパラメータのうち，木の本数を[50, 100, 200, 250, 300, 400, 500, 600,1000]の９通り，木の深さを[10, 20, 30, 40, 50, 60, 80, 100, 150]の９通りの組み合わせ（８１通り）に対して正答率を算出した.

② 結果

最も正答率の高い組み合わせ、最も正答率の低い組み合わせを下記に示す。

最も正答率の高い組み合わせ：

木の本数:300，深さ:max150，正答率:0.9874，　　計算時間 47 秒

最も正答率の低い組み合わせ：

木の本数:50，　深さ:max10，正答率:0.9844，　　計算時間 7 秒

③ 考察

正答率は 0.003 しか違わず，計算時間は 7 倍程度の差があった．Random Forest のパラメータチューニングだけでは精度向上は確認できなかった.

6-1-3　アンサンブル学習①バギング

次に，代表的なアンサンブル学習の一つであるバギングを各種モデルに適用して精度向上を試みた.

① 方法

バギングを決定木，SVM，k-NN,ロジスティック回帰，Random Forest，グラディエントブースティングに適用し，精度向上を試みた.

Table 6 -2 Bagging enhanced performance on Decision Tree, Logistic, k-NN, SVM

shuffle=true,train:test=0.85:0.15	accuracy	precision	recall	**F1Score**
GradientBoost	0.987	0.992	0.882	**0.934**
bagging GradientBoost	**0.987**	**0.992**	**0.880**	**0.933**
RandomForest	0.9893	1.000	0.89316	**0.9436**
bagging RandomForest	0.987	**1.000**	**0.873**	**0.932**
DecisionTree	0.980	0.884	0.923	**0.903**
bagging DecisionTree	**0.990**	**0.988**	**0.910**	**0.947**
LogisticRegr	0.965	0.855	0.781	**0.816**
bagging LogisticRegr	**0.965**	**0.858**	**0.781**	**0.817**
kNN	0.976	0.905	0.850	**0.877**
bagging kNN	**0.977**	**0.911**	**0.849**	**0.879**
SVM	0.971	0.901	0.801	**0.848**
bagging SVM	**0.972**	**0.900**	**0.808**	**0.851**

②結果

Accuracy, Precision, Recall, F1 スコアについて表にまとめた．F 1 スコアについで見ると，決定木，SVM，k-NN，ロジスティック回帰についてはバギングにより精度が向上した．ただしリコールを見ると SVM 以外のモデルではバギングによって精度が下がった．各指標についてモデル毎の精度を比較すると，Accuracy,Precision,F1 においてバギングした決定木の精度が一番高く，Recall においては，単純な決定木の精度が高かった．

6 - 1 - 4　アンサンブル学習②ブースティング

① 方法

ブースティングを Random Forest, 決定木, ロジスティック回帰, に適用し，精度向上を試みた．

Table 6-3 Boosting reduced accuracy.

shuffle=true,train:test=0.85:0.15	accuracy	precision	recall	F1Score
RandomForest	0.989	1.000	0.893	0.944
AdaBoost RandomForest	0.989	1.000	0.890	0.942
DecisionTree	0.9801	0.884	0.92310	0.9031
AdaBoost DecisionTree	0.980	0.887	0.916	0.901
LogisticRegr	0.965	0.856	0.781	0.817
AdaBoost LogisticRegr	0.913	0.717	0.224	0.341

② 結果

ブースティングによる精度の向上は確認できなかった.

6-1-5 アンサンブル学習③スタッキング

① 方法

スタッキング法を行う．第一の学習器と第二の学習器にそれぞれ，Random Forest, Support Vector Machine, Linear Support Vector Machine, Support Vector Machine, Logistic Regression, Gradient Boosting Tree を使って，様々な組み合わせで実験を行った．表中では以下のように略語を使った.

rf: Random Forest, lr: Logistic Regression, svc: Support Vector Machine, svr: Linear Support Machine, gbt: Gradient Boosting Tree

Table 6-4 Stacking enhanced F1Scores.

	shuffle=true,train:test=0.85:0.15	accuracy	precision	recall	F1Score
StackingClassifier	estimators={rf, lr, knn, svc} final_estimator={rf}	0.990	0.976	0.922	0.948
StackingClassifier	estimators={rf, lr_l1, lr_l2} final_estimator={rf}	0.990	0.982	0.922	0.951
StackingClassifier	estimator={rf, lr_l1, lr_l2 , gbt, svr, svc} final_estimator={rf} f1=0.950	0.991	0.988	0.920	0.953

② 結果

スタッキングにより，バギング，ブースティングよりも良い結果を得た.

F1score をはじめ，その他すべての指標で最高の精度を達成した．

６-２　Smote 法によるオーバーサンプリング

①　方法

特徴量データを訓練データ８５％，テストデータ１５％に分割する．訓練データについてのみ，Borderline Smote 法を使い，違法取引データのみオーバーサンプリングする．その訓練データを各種教師あり学習モデルに学習させ，テストデータにおける分類精度を測定した．

②　結果

オーバーサンプリングする前の F1score の最高値は 0.953 であったが，オーバーサンプリングしたデータで，Random Forest を Bagging したものと，Random Forest，ロジスティック回帰，グラディエントブースト，サポートベクターマシンを組み合わせたスタッキングによるモデルが，F1score＝0.959 となりオーバーサンプリングによって F1score を 0.006 向上させた．

Table ６-5　Over sampling + Bagging　enhanced F1Score

BoarderlineSMOTE	*accuracy*	*precision*	*recall*	*F1Score*
GradientBoost	0.984	0.915	0.922	0.918
bagging GradientBoost	**0.983**	**0.916**	**0.919**	**0.918**
RandomForest	0.992	0.994	0.922	0.956
bagging RandomForest	0.992	**0.994**	**0.926**	**0.959**
DecisionTree	0.975	0.851	0.916	0.882
bagging DecisionTree	**0.990**	**0.976**	**0.922**	**0.948**
LogisticRegr	0.909	0.527	0.949	0.678
bagging LogisticRegr	**0.910**	**0.528**	**0.949**	**0.678**
kNN	0.944	0.656	0.926	0.768
bagging knn	**0.944**	**0.658**	**0.929**	**0.770**
SVM	0.932	0.603	0.939	0.734
bagging SVM	**0.931**	**0.598**	**0.940**	**0.731**

Table 6-6 Over sampling + Stacking enhanced F1Score

Borderline SMOTE shuffle=true,train:test=0.85:0.15	accuracy	precision	recall	F1Score
estimators={rf, lr, knn, svc} final_estimator={rf}	0.990	0.983	0.916	0.948
estimators={rf, lr_l1, lr_l2} final_estimator={rf}	0.991	0.979	0.930	0.954
estimator={rf, lr_l1, lr_l2 , gbt, svr, svc} final_estimator={rf}	0.992	0.988	0.932	0.959
estimator={rf, lr_l1, lr_l2 , gbt, svr, svc} final_estimator={rf} f1=0.950	0.990	0.985	0.917	0.950

6-3 半教師あり学習による分類精度測定

ここではラベルなしデータ（違法か合法か不明の取引）のラベルを，ラベルありデータの特徴量とラベルを使って推定することで，学習できるデータ量を増やして，テストデータに対する違法取引の検出精度の向上を目指す.

6-3-1 ラベル拡散法（Label Spreading）

①方法

分析対象データは，本節までは，違法，合法のラベルの付いた，46,564 件であった．本節では違法か合法か不明の 157,205 件を含めて，203,769 件を対象とする.203769 件から無作為に 81.97%を抽出し訓練データとし,残り 18.03%をテストデータとする．この時，ラベル付き，ラベルなしとも混在している．訓練データに対してラベル拡散法を使って，不明のラベルに対してラベル付けを行う．テストデータに関してはテストデータのうちラベルなしのデータに対しては除去し，分類精度の評価にはラベルありデータのみを使う.

訓練データにラベル拡散法を施したものを，Random Forest モデルで学習する．その学習済みの分類器にテストデータの特徴量を投入しラベルを予測し，実際のラベルと比較する.

②結果

今までの Random Forest を使ったどの手法よりも F1score が低くラベル拡散法は効果的ではないと考えられる.

Table 6-7 Label spreading

	shuffle=true,train:test=0.8197:0.1803	accuracy	precision	recall	F1Score
label spreading	RandomForest	0.980	0.971	0.813	0.885

6-4 第6章のまとめ

Weber [12]によると，本データセットにおいて Random Forest の分類精度が最大であることが示されており，それを確認した．更なる分類精度の向上に向けて，機械学習の代表的な分類問題の学習器にアンサンブル学習と，オーバーサンプリング手法である SMOTE を適用することにより，F1score を 0.944 から 0.959 まで 0.015（1.5%）向上させることができた．

第７章　　時系列を考慮した上での分類精度向上について

Weber [12]は，本データセットにおいて Time step １～４９のうち Time step４３から～４９（データセットのデータ数の最後のおおむね１５％）において分類精度が低下することが指摘している．この時間帯の精度の向上を試みた論文は筆者の調べた範囲内では存在しない．本章では訓練データとテストデータの切り分け方について，訓練データは，テストデータより時系列として前の時間帯のものとなるように抽出する．複数のパターンにおいて分類精度が変わるかを実験し，分類精度向上を試みる．またどうして向上させられないのかについて考察する．

７-１　分析①前章の手法での精度確認

７-１-１　トレーニングデータ，テストデータの分割

第６章ではデータセットをシャッフルし，時間帯を考慮していなかった．本章ではデータセットのシャッフルを行わない．テストデータはトレーニングデータより時系列として後に位置するように抽出する．前半８５％のデータをトレーニングデータ，後半１５％のデータをテストデータとする．

７-１-２　分析方法

第６章で使った手法でどの程度の精度が出せるか実験した．

Table 7-1 Various ensemble models

shuffle=false,train:test=0.85:0.15	accuracy	precision	recall	F1Score
GradientBoost	0.972	0.467	0.109	0.176
bagging GradientBoost	0.972	0.500	0.109	0.179
RandomForest	0.9750	0.808	0.10900	0.1920
bagging RandomForest	0.975	0.778	0.109	0.191
DecisionTree	0.892	0.082	0.285	0.128
bagging DecisionTree	0.961	0.250	0.202	0.223
LogisticRegr	0.957	0.161	0.130	0.144
bagging LogisticRegr	0.957	0.159	0.130	0.143
kNN	0.961	0.210	0.150	0.175
bagging knn	0.963	0.226	0.145	0.177
SVM	0.965	0.230	0.119	0.157
bagging SVM	0.965	0.232	0.119	0.158
RandomForest(cluster=5)	0.975	0.786	0.114	0.199

Table 7-2 Stacking models

	shuffle=true,train:test=0.85:0.15	accuracy	precision	recall	F1Score
StackingClassifier	estimators={rf, lr, knn, svc} final_estimator={rf}	0.974	0.667	0.114	0.195
StackingClassifier	estimators={rf, lr_l1, lr_l2} final_estimator={rf}	0.974	0.611	0.114	0.192
StackingClassifier	estimator={rf, lr_l1, lr_l2 , gbt, svr, svc} final_estimator={rf}	0.974	0.688	0.114	0.196

Table 7-3 Stacking and SMOTE

			Borderline SMOTE shuffle=False,train:test=0.85:0.15	accuracy	precision	recall	F1Score
stacking	BorderlineSMOTE	StackingClassifier	estimators={rf, lr, knn, svc} final_estimator={rf}	0.974	0.667	0.114	0.195
stacking	BorderlineSMOTE	StackingClassifier	estimators={rf, lr_l1, lr_l2} final_estimator={rf}	0.974	0.611	0.114	0.192
stacking	BorderlineSMOTE	StackingClassifier	estimator={rf, lr_l1, lr_l2 , gbt, svr, svc} final_estimator={rf}	0.974	0.710	0.114	0.196
stacking	BorderlineSMOTE	StackingClassifier	estimators={rf, LR_l1, LR_l2 , GBT} final_estimator={rf}	0.974	0.629	0.114	0.193
stacking	BorderlineSMOTE	3分割	estimators={svc, knn, LR, rf} final_estimator={rf}	0.975	0.793	0.119	0.207

7-1-3 結果と考察

決定木をバギングしたモデルが最高の F1score を出したが，F1score＝0.223

と低く，２番目の Random Forest も F1score＝0.192 と低い.

7-2　分析②時間帯毎のデータの特性分析 I

7-2-1　データセットのトレーニング，テストの分割方法

① トレーニングデータとテストデータの比率を変えて予測精度を測定する. Table 7-4
② トレーニングデータ５％に対して,時系列として直後のテストデータ５％を予測し，予測精度を測定する．Table 7-5

7-2-2　分析方法

上記のトレーニング，テストデータの分割方法に従ってデータを分割し，それをランダムフォレストで訓練させた.

7-2-3　結果と考察

Table 7-4 Classification performance under different Train/Test data size

TrainData period	TestData period	Accuracy	Precision	Recall	F1-Score
0~0.95(Size=0.95)	0.95~1.0(Size=0.05)	0.951	1	0.009	**0.017**
0~0.9(Size=0.9)	0.9~1.0(Size=0.1)	0.97	0.25	0.014	**0.027**
0~0.85(Size=0.85)	0.85~1.0(Size=0.15)	0.975	0.808	0.109	**0.192**
0~0.8(Size=0.8)	0.8~1.0(Size=0.2)	0.976	0.969	0.535	**0.689**
0~0.75(Size=0.75)	0.75~1.0(Size=0.25)	0.976	0.981	0.605	**0.748**
0~0.7(Size=0.7)	0.7~1.0(Size=0.3)	0.977	0.984	0.645	**0.779**
0~0.65(Size=0.65)	0.65~1.0(Size=0.35)	0.981	0.979	0.712	**0.824**
0~0.6(Size=0.6)	0.6~1.0(Size=0.4)	0.981	0.977	0.772	**0.862**
0~0.55(Size=0.55)	0.55~1.0(Size=0.45)	0.981	0.97	0.814	**0.885**
0~0.5(Size=0.5)	0.5~1.0(Size=0.5)	0.981	0.985	0.823	**0.897**
0~0.45(Size=0.45)	0.45~1.0(Size=0.55)	0.964	0.984	0.654	**0.786**
0~0.4(Size=0.4)	0.4~1.0(Size=0.6)	0.965	0.976	0.68	**0.802**
0~0.35(Size=0.35)	0.35~1.0(Size=0.65)	0.962	0.981	0.654	**0.785**
0~0.3(Size=0.3)	0.3~1.0(Size=0.7)	0.963	0.984	0.694	**0.814**
0~0.25(Size=0.25)	0.25~1.0(Size=0.75)	0.965	0.978	0.71	**0.823**
0~0.2(Size=0.2)	0.2~1.0(Size=0.8)	0.96	0.937	0.709	**0.807**
0~0.15(Size=0.15)	0.15~1.0(Size=0.85)	0.878	0.061	0.006	**0.011**
0~0.1(Size=0.1)	0.1~1.0(Size=0.9)	0.884	0.143	0.015	**0.028**
0~0.05(Size=0.05)	0.05~1.0(Size=0.95)	0.898	0.379	0.002	**0.005**

Table 7-4 において，様々な訓練データとテストデータのサイズの組み合わせで予測精度がどのように変化するかを見ることができる．訓練データはテストデータよりも時系列的に過去に行われた取引である．

一番上の行に関してみると，全体の９５％のデータを使って訓練した Random Forest 分類器で時系列的に最後の５％のデータから不正取引の検出を試みると F1Score で 0.017 という極めて低い精度しか得られなかった．Table 7-4 の３行目（訓練データが８５％，テストデータが１５％）でも F1Score は 0.192 と低い精度である．これに対して Table 7-4 中の行の中央付近にある訓練データ５０％，テストデータ５０％では F1Score0.897 と上述の場合と比べて少ない訓練データで高い精度を実現した．後半の１５％のデータにおける不正取引には前半８５％の不正取引のもつ特徴とは違う特徴をもつ可能性がある．

Table 7-5 Classification performance using most recent data as train data.

TrainData period	TestData period	Accuracy	Precision	Recall	F1-Score
0~0.05(size=0.05)	0.05~0.1(size=0.05)	0.991	1.000	0.25	**0.4**
0.05~0.1(size=0.05)	0.1~0.15(size=0.05)	0.992	1.000	0.424	**0.596**
0.1~0.15(size=0.05)	0.15~0.2(size=0.05)	0.965	1.000	0.012	**0.024**
0.15~0.2(size=0.05)	0.2~0.25(size=0.05)	0.973	0.983	0.832	**0.901**
0.2~0.25(size=0.05)	0.25~0.3(size=0.05)	0.991	0.992	0.921	**0.955**
0.25~0.3(size=0.05)	0.3~0.35(size=0.05)	0.985	0.994	0.941	**0.967**
0.3~0.35(size=0.05)	0.35~0.4(size=0.05)	0.966	0.986	0.798	**0.882**
0.35~0.4(size=0.05)	0.4~0.45(size=0.05)	0.984	0.977	0.907	**0.941**
0.4~0.45(size=0.05)	0.45~0.5(size=0.05)	0.955	0.957	0.471	**0.631**
0.45~0.5(size=0.05)	0.5~0.55(size=0.05)	0.971	0.988	0.864	**0.922**
0.5~0.55(size=0.05)	0.55~0.6(size=0.05)	0.983	0.978	0.94	**0.959**
0.55~0.6(size=0.05)	0.6~0.65(size=0.05)	0.985	0.988	0.915	**0.95**
0.6~0.65(size=0.05)	0.65~0.7(size=0.05)	0.996	0.994	0.951	**0.972**
0.65~0.7(size=0.05)	0.7~0.75(size=0.05)	0.976	0.98	0.741	**0.844**
0.7~0.75(size=0.05)	0.75~0.8(size=0.05)	0.972	0.993	0.683	**0.809**
0.75~0.8(size=0.05)	0.8~0.85(size=0.05)	0.974	0.982	0.796	**0.879**
0.8~0.85(size=0.05)	0.85~0.9(size=0.05)	0.983	0.947	0.321	**0.48**
0.85~0.9(size=0.05)	0.9~0.95(size=0.05)	0.991	1	0.043	**0.083**
0.9~0.95(size=0.05)	0.95~1(size=0.05)	0.951	0	0	**0**

Table 7-5 においては時系列として直近の５％の取引データを訓練データとして，直後５％の取引に関して違法取引を検出することができるかについて分析を試みた.その結果時系列的に直近のデータを訓練データとすると，１５％～８５％の時間帯に関しては高い予測精度を実現できた．しかしながら，５％～１０％の時間帯，８５％～１００％の時間帯の予測精度は低かった.

7-3 分析③時間帯毎のデータの特性分析Ⅱ

7-3-1 データセットのトレーニングデータ，テストデータの分割

そこでさらに訓練データとテストデータの組み合わせを増やす．Table 7-5 では直近のデータで直後のデータを予測していたが，Table 7-6 では，一番上

の列は時間帯０～５％のデータを訓練データとしてモデルを訓練し，５％～１０％，１０％～１５％…９５％～１００％のそれぞれの時間帯での予測精度を実験した．以下，２列目以降も同様に，１０%~１５％の時間帯のデータを訓練データとしてそれ以後の各時間帯の予測をした．

７-３-２　分析方法

Random Forest，サポートベクターマシン，ロジスティック回帰，グラディエントブーストを用いた．

Table 7 -6 Classification performance with various combination of time steps Random Forest

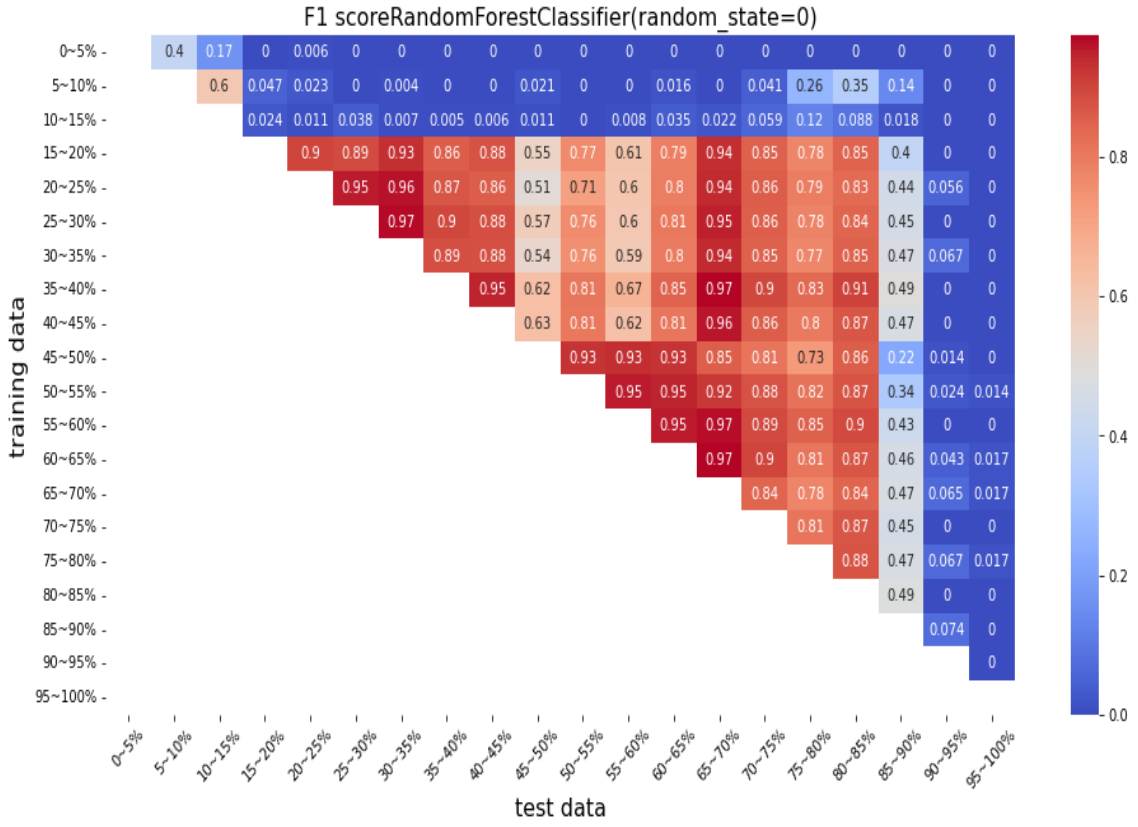


Table 7-6 からは，５～１０％，１０～１５％，１５％～２０％の時間帯及び，８５％～９０％，９０～９５％，９５～１００％の時間帯の予測精度をさせることは，どの時間帯の情報を学習データとして使っても難しそうだということが推察される．

もしも Random Forest 以外のモデルであれば予測精度を上げられるかもしれないと考え，Random Forest 以外のモデル（LR, Linear SVC, GBT, k-NN,

AdaBoosting）でも同様な実験を試みた.

Table 7 -7 Classification performance with various combination of time steps Logistic Regression

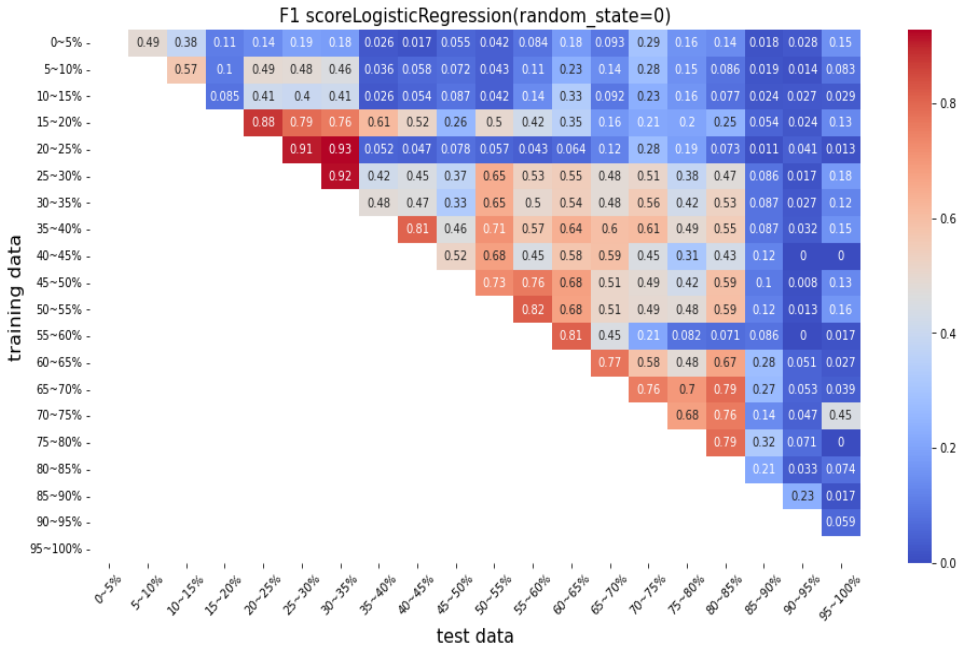


Table 7 -8 Classification performance with various combination of time steps Gradient Boosting

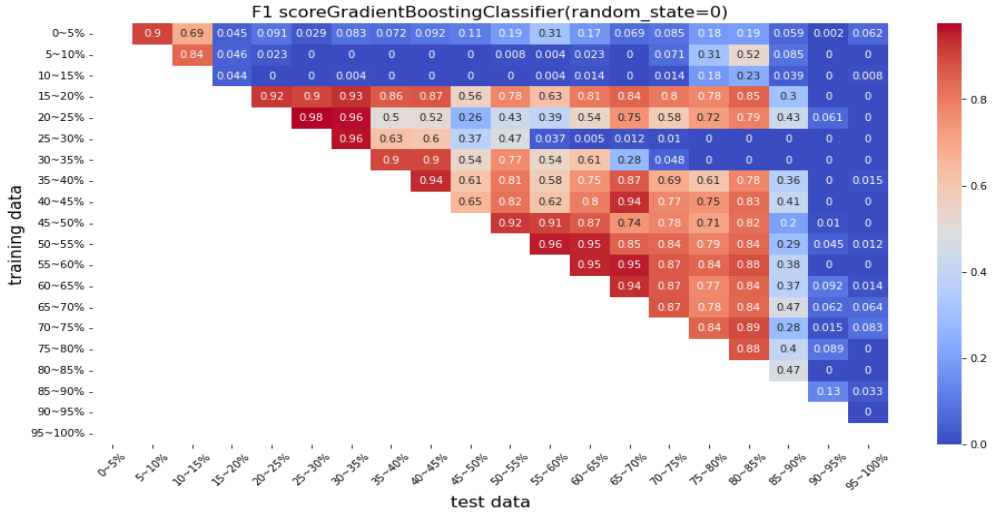


Table 7 -9 Classification performance with various combination of time steps AdaBoost

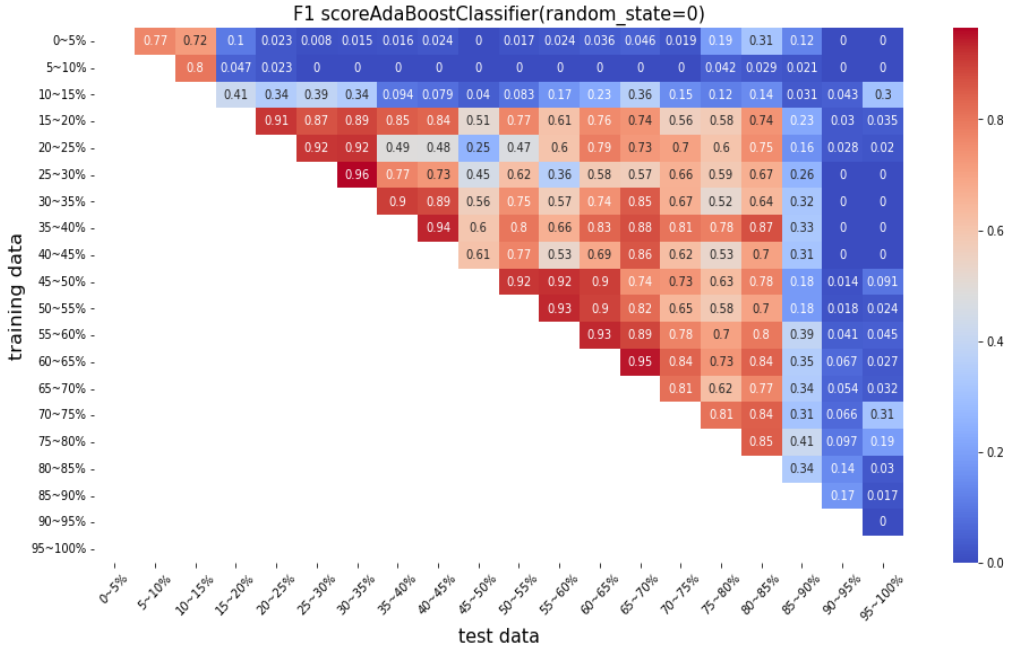


Table 7 -10 Classification performance with various combination of time steps LinearSVC

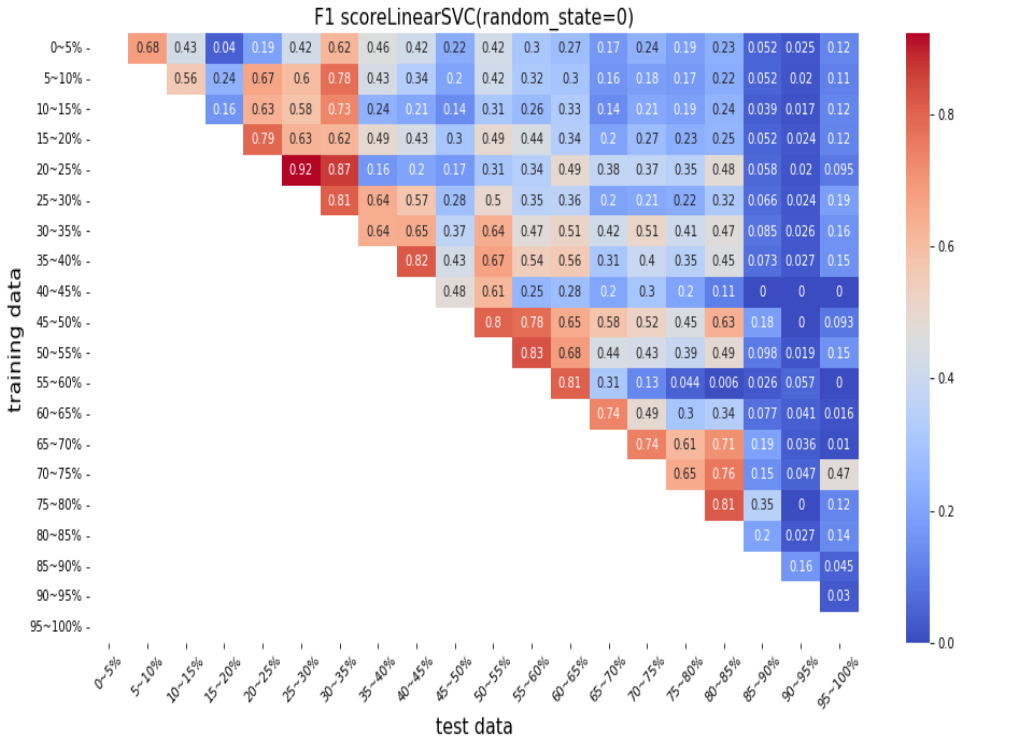
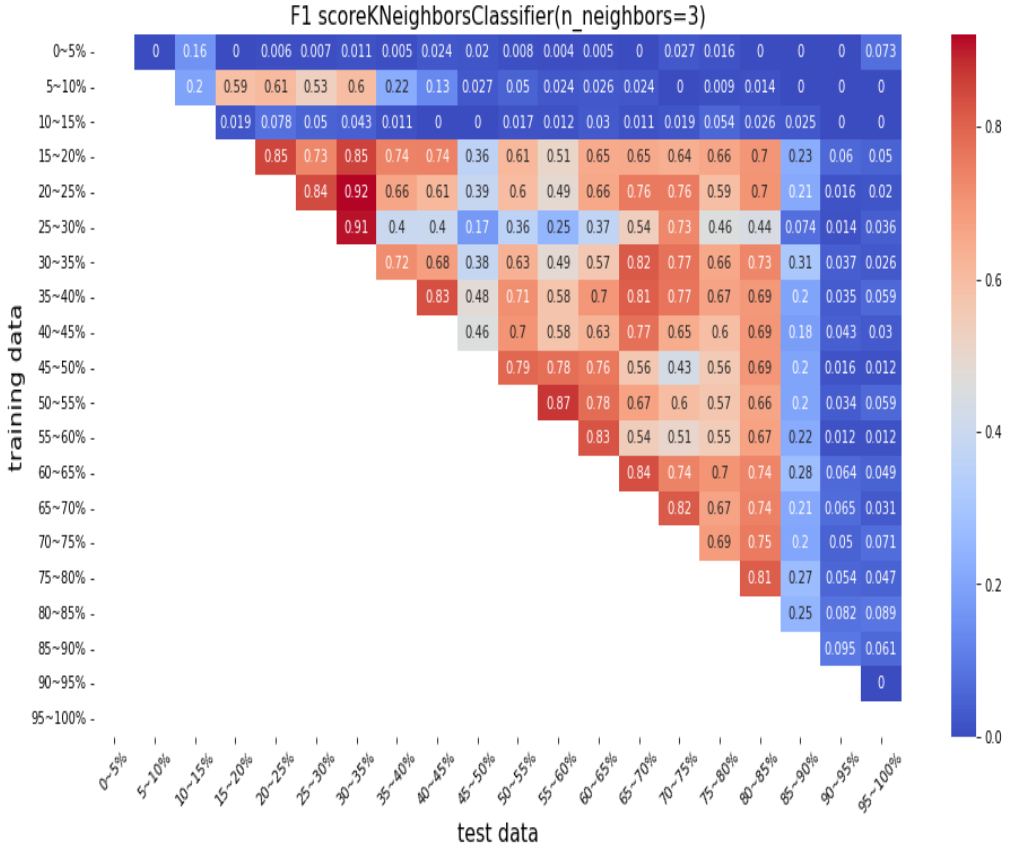


Table 7-11 Classification performance with various combination of time steps k-NN



7-3-3　結果と考察

Random Forest 以外の各モデルでも，前半５～１５％と８５～１００％までの時間帯の F1-score を上げることは難しそうに見えた．ただし，各モデル間でそれぞれの時間帯の予測精度にバラツキがあることから，各モデルを組み合わせる手法であるスタッキングによる精度の向上を図れるのではないかとも考えられる．実際に 7-1-3　によると精度は向上した．

7-4　教師あり学習と教師なし学習のハイブリッド手法

7-4-1　クラスター分析（教師なし学習）と PCA による次元圧縮によるノイ

ズ除去と Random Forest（教師あり学習）のハイブリッド学習

①方法

教師なし学習手法である，K-Means 法により，特徴量を学習させ，そのクラスター番号を新たな特徴量として特徴量に加える．その特徴量を PCA で次元圧縮し，そのデータを Random Forest によって分類を試みた．PCA によって次元圧縮を試みたのは, PCA によって特徴量の中のノイズを削減する効果を期待してのことである．

①-1　：K-Means によるクラスタリング

K-Means 法でクラスター数を５に指定し, 特徴量の訓練データにおいてクラスター重心計算を行う（K-Means モデルを構築する）．

K-Means モデルによるクラスター番号をダミー変数として, 訓練データおよびテストデータに特徴量として付け足す．

①-2　：主成分分析による次元圧縮

新たに K-Means 法で得られたクラスター番号を含む訓練データを主成分分析によって次元圧縮した．特徴量ベクトルから固有ベクトルを算出し，１７１次元の特徴量を（５次元から１６９次元に圧縮した）．例えば５次元に圧縮した場合は　１７１次元－５次元＝１６６次元の次元削減であり，１６６次元はノイズであると判断しているということである．

①-3　：Random Forest やロジスティック回帰，などの分類器による分類，分類精度測定

主成分分析により次元圧縮した特徴量で Random Forest 分類器によるモデルを構築した．そしてそのモデルにテストデータの特徴量を上記方法で訓練データから得られた主成分分析の固有ベクトルによって次元圧縮し，それを訓練データで構築された Random Forest 分類器で分類精度を測定した．

Table 7 -12 Classified by K-Means, PCA, Random Forest

PC数	accuracy	precision	recall	f1_score
2	0.935	0.026	0.036	0.030
3	0.963	0.120	0.052	0.072
4	0.968	0.200	0.052	0.082
5	0.969	0.244	0.052	0.085
6	0.972	0.481	0.067	0.118
7	0.972	0.500	0.067	0.119
8	0.973	0.538	0.073	0.128
9	0.972	0.467	0.073	0.126
10	0.971	0.385	0.078	0.129
11	0.971	0.409	0.093	0.152
12	0.972	0.439	0.093	0.154
13	0.972	0.439	0.093	0.154
14	0.972	0.462	0.093	0.155
15	0.973	0.531	0.088	0.151
16	0.971	0.400	0.093	0.151
17	0.971	0.400	0.093	0.151
18	0.971	0.383	0.093	0.150
19	0.971	0.400	0.093	0.151
20	0.973	0.514	0.093	0.158
21	0.972	0.450	0.093	0.155
22	0.971	0.419	0.093	0.153
23	0.972	0.450	0.093	0.155
24	0.973	0.514	0.093	0.158
25	0.973	0.563	0.093	0.160
26	0.972	0.486	0.093	0.157
27	0.973	0.514	0.093	0.158
28	0.972	0.500	0.093	0.157
29	0.973	0.600	0.093	0.161
30	0.973	0.621	0.093	0.162
31	0.973	0.621	0.093	0.162
32	0.973	0.600	0.093	0.161
33	0.974	0.667	0.093	0.164
34	0.974	0.643	0.093	0.163
35	0.972	0.500	0.093	0.157
36	0.973	0.581	0.093	0.161
37	0.973	0.621	0.093	0.162
38	0.974	0.643	0.093	0.163
39	0.973	0.529	0.093	0.159
40	0.973	0.621	0.093	0.162
41	0.973	0.600	0.093	0.161
42	0.974	0.643	0.093	0.163
43	0.974	0.643	0.093	0.163
44	0.974	0.667	0.093	0.164
45	0.973	0.545	0.093	0.159
46	0.974	0.692	0.093	0.164
47	0.973	0.621	0.093	0.162
48	0.974	0.643	0.093	0.163
49	0.974	0.720	0.093	0.165
50	0.973	0.600	0.093	0.161
51	0.974	0.720	0.093	0.165
52	0.974	0.708	0.088	0.157
53	0.974	0.692	0.093	0.164
54	0.974	0.643	0.093	0.163
55	0.974	0.667	0.093	0.164
56	0.974	0.750	0.093	0.166
57	0.973	0.581	0.093	0.161
58	0.974	0.667	0.093	0.164
59	0.974	0.692	0.093	0.164
60	0.974	0.720	0.093	0.165
61	0.974	0.750	0.093	0.166
62	0.974	0.750	0.093	0.166
63	0.974	0.783	0.093	0.167
64	0.974	0.643	0.093	0.163
65	0.974	0.692	0.093	0.164
66	0.974	0.750	0.093	0.166
67	0.974	0.750	0.093	0.166
68	0.975	0.857	0.093	0.168
69	0.974	0.818	0.093	0.167
70	0.974	0.773	0.088	0.158
71	0.975	0.947	0.093	0.170
72	0.975	0.857	0.093	0.168
73	0.974	0.810	0.088	0.159
74	0.975	0.900	0.093	0.169
75	0.975	0.947	0.093	0.170
76	0.975	0.900	0.093	0.169
77	0.974	0.842	0.083	0.151
78	0.975	0.895	0.088	0.160
79	0.974	0.842	0.083	0.151
80	0.975	0.947	0.093	0.170
81	0.974	0.783	0.093	0.167
82	0.974	0.938	0.078	0.144
83	0.975	0.895	0.088	0.160
84	0.974	0.842	0.083	0.151
85	0.975	0.895	0.088	0.160
86	0.974	0.842	0.083	0.151
87	0.974	0.833	0.078	0.142
88	0.974	0.750	0.078	0.141
89	0.975	0.941	0.083	0.152
90	0.974	0.938	0.078	0.144
91	0.974	0.882	0.078	0.143
92	0.974	0.889	0.083	0.152
93	0.974	0.933	0.073	0.135
94	0.974	1.000	0.067	0.126
95	0.975	1.000	0.078	0.144
96	0.974	1.000	0.067	0.126
97	0.973	1.000	0.031	0.060
98	0.973	1.000	0.016	0.031
99	0.974	0.846	0.057	0.107
100	0.974	1.000	0.047	0.089
101	0.973	1.000	0.005	0.010
102	0.973	1.000	0.010	0.021
103	0.972	0.000	0.000	0.000
104	0.972	0.000	0.000	0.000
105	0.973	1.000	0.005	0.010
106	0.973	0.750	0.016	0.030
107	0.973	1.000	0.010	0.021
108	0.972	0.000	0.000	0.000
109	0.973	1.000	0.010	0.021
110	0.973	1.000	0.005	0.010
111	0.972	0.000	0.000	0.000
112	0.973	1.000	0.005	0.010
113	0.973	1.000	0.010	0.021
114	0.973	1.000	0.010	0.021
115	0.973	1.000	0.005	0.010
116	0.973	1.000	0.005	0.010
117	0.973	1.000	0.005	0.010
118	0.973	1.000	0.005	0.010
119	0.972	0.000	0.000	0.000
120	0.972	0.000	0.000	0.000
121	0.973	1.000	0.010	0.021
122	0.972	0.000	0.000	0.000
123	0.973	1.000	0.005	0.010
124	0.973	1.000	0.005	0.010
125	0.973	1.000	0.005	0.010
126	0.973	1.000	0.005	0.010
127	0.972	0.000	0.000	0.000
128	0.973	1.000	0.005	0.010
129	0.972	0.000	0.000	0.000
130	0.972	0.000	0.000	0.000
131	0.972	0.000	0.000	0.000
132	0.973	1.000	0.005	0.010
133	0.972	0.000	0.000	0.000
134	0.973	1.000	0.005	0.010
135	0.972	0.000	0.000	0.000
136	0.972	0.000	0.000	0.000
137	0.972	0.000	0.000	0.000
138	0.972	0.000	0.000	0.000
139	0.973	1.000	0.005	0.010
140	0.972	0.000	0.000	0.000
141	0.972	0.000	0.000	0.000
142	0.972	0.000	0.000	0.000
143	0.972	0.000	0.000	0.000
144	0.972	0.000	0.000	0.000
145	0.972	0.000	0.000	0.000
146	0.972	0.000	0.000	0.000
147	0.972	0.000	0.000	0.000
148	0.973	1.000	0.005	0.010
149	0.972	0.000	0.000	0.000
150	0.972	0.000	0.000	0.000
151	0.972	0.000	0.000	0.000
152	0.972	0.000	0.000	0.000
153	0.972	0.000	0.000	0.000
154	0.972	0.000	0.000	0.000
155	0.972	0.000	0.000	0.000
156	0.972	0.000	0.000	0.000
157	0.972	0.000	0.000	0.000
158	0.972	0.000	0.000	0.000
159	0.972	0.000	0.000	0.000
160	0.972	0.000	0.000	0.000
161	0.973	1.000	0.005	0.010
162	0.972	0.000	0.000	0.000
163	0.973	1.000	0.005	0.010
164	0.972	0.000	0.000	0.000
165	0.973	1.000	0.005	0.010
166	0.972	0.000	0.000	0.000
167	0.972	0.000	0.000	0.000
168	0.972	0.000	0.000	0.000
169	0.972	0.000	0.000	0.000
170	0.972	0.000	0.000	0.000

②結果：

１７０次元から７１次元に次元を落とした場合に F1-score＝0.170 となり精度が最も高かった．しかし，7‐1‐3　において Random Forest 単体を用いた場合の F1-score＝0.190 を下回った．また次元を１７０に近づけても元 F1-score が 0.190 に近づくどころか，０に張り付いてしまい，PCA によって次元圧縮だけでなく，計算過程での丸目誤差が拡大していることが懸念される．

7‐4‐2　クラスター分析と Random Forest によるハイブリッド手法（PCA による次元圧縮なし）

7‐4‐1　においての結果が芳しくなかったため，ラスター分析と Random Forest によるハイブリッド手法で PCA による次元圧縮なしの場合について精度を実験した．

①分析方法

7‐4‐1　での手法において，主成分分析による次元圧縮をしない場合の精度を見る．

7‐4‐1　では次元圧縮によりノイズを取り除くことを意図したが，分類精度が従来の教師あり学習と比べて低下した．そこで主成分分析による次元圧縮をせずに特徴量１７１次元をそのまま用い，クラスター数を２～１０個で分類精度を測定した．

Table 7‐13 Classified by K-Means and Random Forest

クラスター数	accuracy	precision	recall	f1_score
2	0.975	0.778	0.109	0.191
3	0.974	0.750	0.109	0.190
4	0.975	0.759	0.114	0.198
5	0.975	0.786	0.114	0.199
7	0.975	0.786	0.114	0.199
10	0.975	0.778	0.109	0.191

②結果

分類精度が 7‐4‐1　では F1-score=0.170 であったのが, F1-score=0.199 に 0.029 上がった．7‐1‐3　では F1-score＝0.193 だったのと比べると 0.006 上

がった.

7-4-3　クラスター分析の結果のみを特徴量とした場合の分類精度

7-4-2　では，オリジナルの特徴量と，オリジナルの特徴量をクラスター分析した結果を組み合わせた特徴量を Random Forest で学習することで，分類精度が上がることが分かった．クラスター分析の結果を特徴量として，Random Forest により分類をした場合の精度についても検証した.

①　分析方法

7-4-1　7-4-2　で使った，K-Means 法によるクラスタリング結果のみを Random Forest に学習させて分類精度を測定した.

②　結果

違法取引を一件も検出できず，すべての取引を合法と判定してしまった．クラスタリングの結果のみでは，学習がうまくできないことが分かった.

Table 7-14 Classified by K-Means

クラスター数	accuracy	precision	recall	f1_score
10	0.899	0.000	0.000	0.000

7-5　半教師あり学習

7-5-1　ラベル拡散法（Label Spreading）オーバーサンプルなし

①　方法１，オーバーサンプリング手法なし

分析対象データは，本節までは，違法，合法のラベルの付いた，46,564 件であった．本節では違法か合法か不明の 157,205 件を含めて，203,769 件を対象とする. 203769 件の時系列を保ち, 前半 81.97%を抽出し訓練データとする．ラベル付き，ラベルなしとも混在している．訓練データに対してラベル拡散法を使って，不明のラベルに対してラベル付けを行う．テストデータは，前節までの分析と平仄を合わせるために，ラベル付きデータのうちの後半１５％とする．この時訓練データとテストデータは重複していない.

訓練データにラベル拡散法を施したものを，Random Forest モデルで学習する．その学習済みの分類器にテストデータの特徴量を投入しラベルを予測し，

実際のラベルと比較する.

② 方法２，オーバーサンプリング手法あり

上記方法１の訓練データに対してオーバーサンプリング手法（SMOTE 法）を施し精度の向上を試みた.

③ 結果

今までの Random Forest を使ったどの手法よりも F1score が低くラベル拡散法は効果的ではないと考えられる.

Table 7-15 Label spreading and SMOTE

		shuffle=False,train:test=0.8197:0.1003 train:test=0.85:0.15(Labeled data)	accuracy	precision	recall	F1Score
	label spreading	RandomForest(random_state=0,n_estimators=100	0.972	0.457	0.109	0.176
SMOTE	label spreading	RandomForest(random_state=0,n_estimators=100	0.969	0.343	0.124	0.183
BorderlineSMOTE	label spreading	RandomForest(random_state=0,n_estimators=100	0.972	0.5	0.104	0.172
Adasyn_SMOTE	label spreading	RandomForest(random_state=0,n_estimators=100	0.971	0.39	0.119	0.183
SVM_SMOTE	label spreading	RandomForest(random_state=0,n_estimators=100	0.965	0.255	0.13	0.172

7-6 第７章のまとめ

第６章と同様に，バギング法やスタッキング法は単体のモデルよりも F1-score の向上させた．しかし，F1-score の絶対値の水準は０．２０と低く，それを向上させるには至らなかった．また Table 7-6 からは，本章で精度を上げようとした時間帯の違法取引のパターンはデータセットの他の時間帯には存在していないようである．当たり前の事かもしれないが，未知のパターンは教師あり学習では分類できないということである．教師なし学習による検出を試みる必要がある.

第８章　　異常検知手法での分類精度向上への取り組み

第７章では，教師あり学習の手法を核にして，教師なし学習の手法も組み合わせて，後半１５％の違法取引の分類精度の向上を目指した．

本章では，異常検知の手法（主成分分析）を使い，分類精度向上に取り組む．

８-１　異常検知手法

違法取引のデータは合法取引に比べて稀な取引である．大半を占める合法取引と違法な取引では何か違いがあるはずだという仮定から，取引が異常であればあるほど，より不正らしいと考える．

８-１-１　主成分分析による次元削減，復元時の再構成誤差について

主成分分析により，次元削減し，それを再構成した場合の再構成誤差を以下のように定義する．

$$d = \left|\left|\hat{X} - X\right|\right| = \left|\left|F^T F X - X\right|\right|$$

ただし，特徴量行列を正規化した行列:X を X の固有行列:F により元の（n）次元から（m）次元に（n-m）次元削減しそれを元の特徴量行列:$\hat{X}$に再構成した際の誤差:d である．この d が大きければ異常度が高く，違法取引の特徴量に対しては d が大きければそれによって，違法取引を検知することが可能になる．[22]

①分析方法

主成分分析における再構成誤差を各違法取引，各合法取引について算出し，その一取引あたりの平均を算出した．

②結果

再構成誤差は合法取引の方が違法取引より高い．合法取引を異常取引とみなしてしまうことからこの手法は使えない．

Table ８-1　Reconstruction Error

	合法取引	違法取引	差
１６５次元から１６０次元に５次元削減	11.47711	11.47711	0.0000
１６５次元から１２５次元に４０次元削減	11.54564	11.47913	0.0665
１６５次元から５次元に１６０次元削減	239.9419	58.09417	181.8477

再構成誤差は合法取引の方が違法取引より高い．合法取引を異常取引とみな

してしまう．当手法では違法取引を異常値として検知することが困難であることが示唆される．

③可視化：違法取引，合法取引の主成分得点の分布

再構成誤差によると，合法取引の異常度の方が高い．このことを主成分得点の分布の散布図から確認する．違法取引（赤点は前半８５％の違法取引，黄色点は後半１５％の違法取引）は合法取引（青色点前半８５％の合法取引，緑色点は後半１５％の違法取引）である．違法取引の散らばりが合法取引よりも少ない様子がわかる．また後半１５％の取引は前章までの議論で検出が難しかったことから異常検知の方法で分類できることを期待したが，分類できなかった．

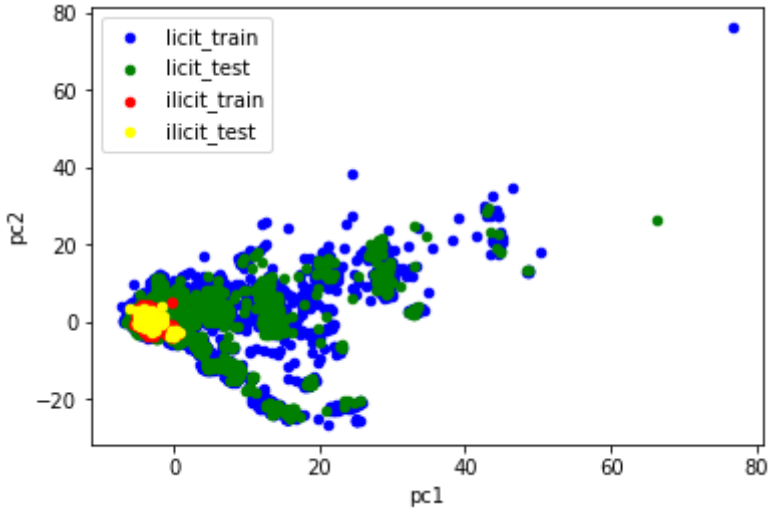


Fig　8 -1 pc1,pc2 score of Licit /Illicit transactions

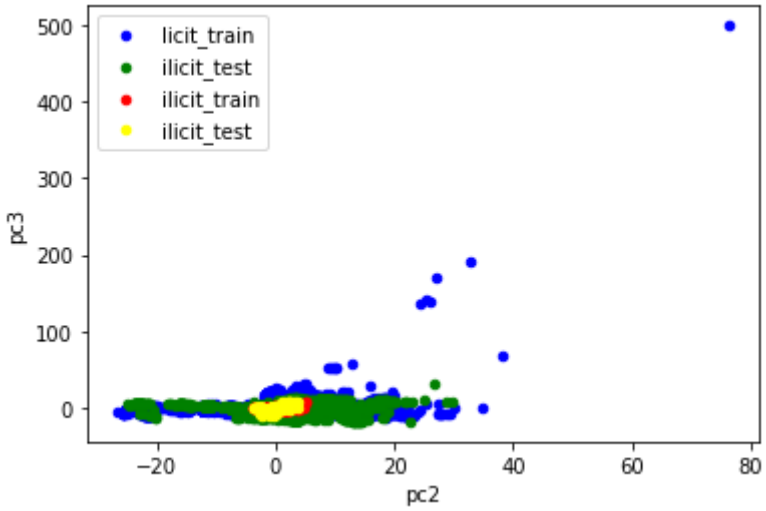


Fig　8 -2 pc2,pc3 score of Licit /Illicit transactions

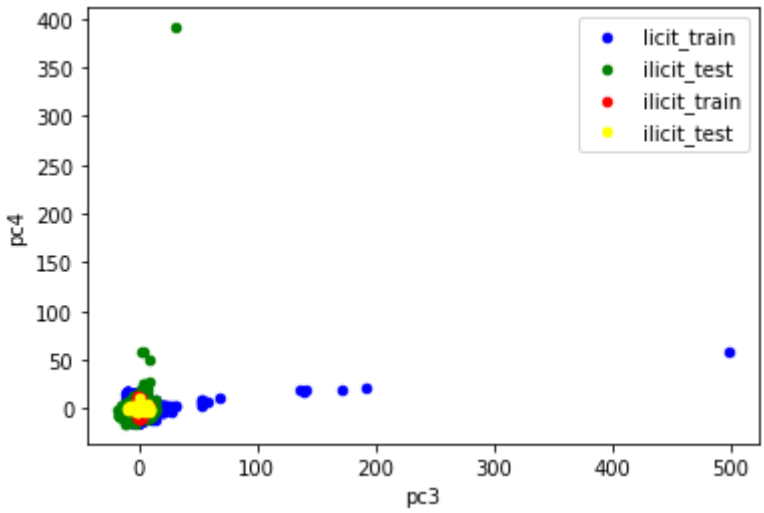


Fig 8 -3 pc3,pc4 score of Licit /Illicit transactions

第９章　　グラフデータの分析

前章までは，取引同士のグラフ情報を graph-embedding 手法により特徴量化した特徴量行列を分析対象としていた．本節では違法取引，合法取引の取引同士の繋がり（グラフ）を分析対象とする．7-3　でも明らかなように特に検出精度が低い０～１０％の時間帯，８０－９０％，９０％～１００％の時間帯についてグラフ分析し，どのような特徴を持つかを明らかにする．

９-１　各種次数分析

９-１-１　各種次数について

各種次数について算出した．[23] [24]

①次数

次数（k_i）は各ノードが持つエッジの数である．

②次数中心性

次数中心性（$k_i/(N-1)$）は各ノードが持つエッジの数（＝次数）を N−1 で割って，正規化したものである．ただし N はノード数．

③近接中心性

近接中心性は，あるノードから他の全てのノードへの距離（最短経路長）の平均値の逆数をとったものである．平均的な距離が短いほど近接中心性は大きくなる．

④媒介中心性

媒介中心性は，注目しているノードがそれ以外の 2 つのノード間の最短経路にどのくらいの割合で入っているかを数値にしたものである．注目しているノードをノード１とした時，ノード１を除いて選んだ 2 点（始点ノード２と終点ノード３）を結ぶ最短経路の中でノード１を通る度合いがノード１の媒介中心性である．

⑤固有ベクトル中心性

固有ベクトル中心性（x^{eigen_i}）は隣接するノードの中心性を加味する中心性である．ノード（i）の固有ベクトル中心性 x^{eigen_i} は，ノードの隣接行列を A とした時 $Ax^{eigen}=\lambda x^{eigen}$　$\Leftrightarrow$ $x^{eigen}=(1/\lambda)Ax^{eigen}$ の x(の i 番目の要素)．x^{eigen} は A の固有ベクトル，λは A の固有値である．

⑥PageRank

PageRank(x^{page_i}) は固有ベクトル中心性が隣接ノードの固有ベクトル中心性が０だと０になってしまうという欠点を補うために，定数項 α と D^{-1}（ノードの次数 k_i の逆数を対角成分に持つ正方行列）を導入したものである． $x^{page}= \alpha AD^{-1} x^{page} +(1- \alpha)$ (本研究では α =0.85 を使用) を解くことで得られる．

９-１-２　各種次数の集計

①方法

取引ごとの各種次数を算出し，各時間帯，違法／合法別に平均を算出，規格化する．（Table ９-1，Table ９-2）

主成分分析を行う．主成分得点, 因子負荷量を算出する．(Table ９-3 , Table ９-4）

②結果

① 主成分得点 Table ９-3 から，違法取引は第一主成分が高く，合法取引は低い．
② 検出精度の低い違法取引の０～１０％の時間帯，８０－９０％，９０％～１００％の時間帯は，他の時間帯の違法取引に比べて第一主成分が高い．（Table ９-3）
③ 検出精度の低い違法取引の０～１０％の時間帯，８０－９０％，９０％～１００％の時間帯は，次数中心性，近接中心性，PageRank が高い．（Table ９-2）

Table 9 -1 Average degree of transactions

次数正規化前

	次数	次数中心性	媒介中心性	近接中心性	PageRank	固有ベクトル中心性
tx=0~10%	1.8070000	0.0002986	0.0000001	0.0002148	0.0001652	0.0002200
tx=10~20%	1.7820000	0.0003630	0.0000004	0.0002269	0.0002036	0.0002899
tx=20~30%	1.8300000	0.0004300	0.0000004	0.0002872	0.0002349	0.0003493
tx=30~40%	1.9530000	0.0004838	0.0000030	0.0003449	0.0002476	0.0003646
tx=40~50%	2.0400000	0.0003934	0.0000002	0.0002615	0.0001928	0.0002560
tx=50~60%	1.8920000	0.0004145	0.0000014	0.0002769	0.0002190	0.0003217
tx=60~70%	1.9320000	0.0003892	0.0000014	0.0002481	0.0002015	0.0003016
tx=70~80%	2.0030000	0.0003137	0.0000009	0.0002286	0.0001566	0.0002387
tx=80~90%	1.9490000	0.0002956	0.0000005	0.0002553	0.0001516	0.0002519
tx=90~100%	2.1070000	0.0004516	0.0000021	0.0004284	0.0002143	0.0003119
illicit tx=0~10%	1.1428571	0.0165631	0.0000000	0.0082816	0.0142857	0.0740331
illicit tx=10~20%	1.5166667	0.0127451	0.0000326	0.0067793	0.0083333	0.0085508
illicit tx=20~30%	1.6448087	0.0045063	0.0000007	0.0023036	0.0027322	0.0031867
illicit tx=30~40%	1.7185629	0.0025766	0.0000002	0.0012952	0.0014970	0.0016279
illicit tx=40~50%	1.6782450	0.0030737	0.0000018	0.0016810	0.0018281	0.0019273
illicit tx=50~60%	1.7361111	0.0020117	0.0016827	0.0013997	0.0011574	0.0015404
illicit tx=60~70%	1.7239165	0.0027716	0.0008653	0.0017886	0.0016051	0.0019696
illicit tx=70~80%	1.5699659	0.0053766	0.0000024	0.0028333	0.0034130	0.0050406
illicit tx=80~90%	1.6437500	0.0051528	0.0000024	0.0027245	0.0031250	0.0035044
illicit tx=90~100%	1.6800000	0.0112752	0.0000048	0.0058641	0.0066667	0.0071062

Table 9 -2 Degree of transactions(normalized)

次数（正規化後）

	次数	次数中心性	媒介中心性	近接中心性	PageRank	固有ベクトル中心性
0-10%	0.186	-0.693	-0.323	-0.716	-0.615	-0.337
10-20%	0.068	-0.679	-0.322	-0.711	-0.604	-0.332
20-30%	0.294	-0.665	-0.322	-0.685	-0.595	-0.329
30-40%	0.873	-0.653	-0.316	-0.660	-0.592	-0.328
40-50%	1.282	-0.673	-0.323	-0.696	-0.607	-0.335
50-60%	0.586	-0.668	-0.320	-0.689	-0.600	-0.330
60-70%	0.774	-0.674	-0.320	-0.702	-0.605	-0.332
70-80%	1.108	-0.690	-0.321	-0.710	-0.618	-0.336
80-90%	0.854	-0.694	-0.322	-0.699	-0.619	-0.335
90-100%	1.597	-0.660	-0.318	-0.624	-0.601	-0.331
illicit0-10%	-2.938	2.836	-0.323	2.739	3.395	4.310
illicit10-20%	-1.180	2.007	-0.242	2.096	1.704	0.188
illicit20-30%	-0.577	0.220	-0.322	0.179	0.114	-0.150
illicit30-40%	-0.230	-0.199	-0.323	-0.253	-0.237	-0.248
illicit40-50%	-0.420	-0.091	-0.319	-0.088	-0.143	-0.229
illicit50-60%	-0.148	-0.322	3.856	-0.208	-0.333	-0.254
illicit60-70%	-0.205	-0.157	1.826	-0.042	-0.206	-0.227
illicit70-80%	-0.929	0.408	-0.317	0.406	0.307	-0.033
illicit80-90%	-0.582	0.360	-0.317	0.359	0.225	-0.130
illicit90-100%	-0.412	1.688	-0.311	1.704	1.231	0.097

Table 9-3 PCA scores

Scores PCA

	pc1	pc2	pc3	pc4	pc5
0-10%	-1.147	-0.314	0.231	-0.396	0.008
10-20%	-1.080	-0.298	0.227	-0.494	0.007
20-30%	-1.154	-0.329	0.216	-0.280	0.005
30-40%	-1.385	-0.400	0.207	0.246	0.002
40-50%	-1.597	-0.462	0.224	0.592	0.008
50-60%	-1.286	-0.365	0.219	-0.023	0.005
60-70%	-1.378	-0.391	0.226	0.139	0.007
70-80%	-1.542	-0.436	0.234	0.428	0.009
80-90%	-1.429	-0.403	0.230	0.203	0.006
90-100%	-1.691	-0.499	0.197	0.896	-0.002
illicit0-10%	7.206	-0.194	1.547	0.157	-0.001
illicit10-20%	3.283	-0.136	-1.393	0.256	0.081
illicit20-30%	0.434	-0.239	-0.290	-0.471	-0.009
illicit30-40%	-0.312	-0.273	-0.053	-0.451	-0.009
illicit40-50%	-0.053	-0.246	-0.141	-0.532	-0.013
illicit50-60%	-0.552	3.856	0.115	0.148	0.008
illicit60-70%	-0.245	1.851	-0.057	-0.068	-0.018
illicit70-80%	0.916	-0.196	-0.349	-0.625	-0.004
illicit80-90%	0.644	-0.237	-0.393	-0.374	-0.016
illicit90-100%	2.366	-0.292	-1.197	0.650	-0.074

Table 9-4 PCA Loadings

loadings

	pc1	pc2	pc3	pc4	pc5
次数	-0.432	-0.135	0.006	0.892	0.006
次数中心性	0.462	-0.018	-0.342	0.215	-0.484
媒介中心性	-0.029	0.989	0.035	0.135	0.010
近接中心性	0.458	0.018	-0.387	0.243	-0.145
PageRank	0.471	-0.029	-0.024	0.214	0.829
固有ベクトル中心性	0.409	-0.039	0.855	0.190	-0.237

９-２　グラフ情報の視覚化

グラフ情報からノード（取引，点で表示）とエッジ（取引間の繋がり，矢印）を可視化した．０～２０％，９０～１００％の時間帯については視覚的には特徴的であるようにも見える．次数分析と本視覚情報から違法取引の検出を行うアルゴリズムの構築が今後の課題だと考える．

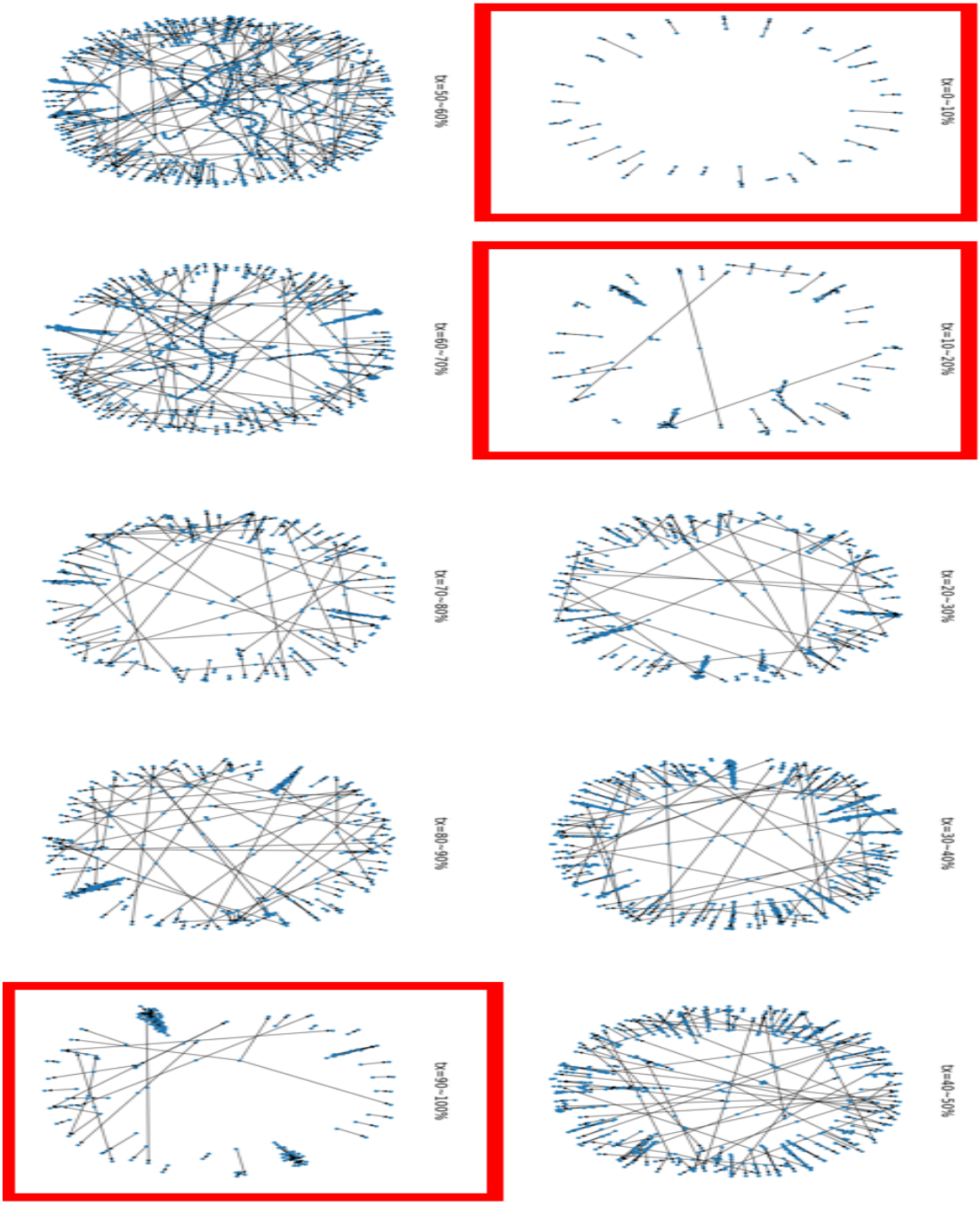


Fig　9-1 Graph of illicit transactions

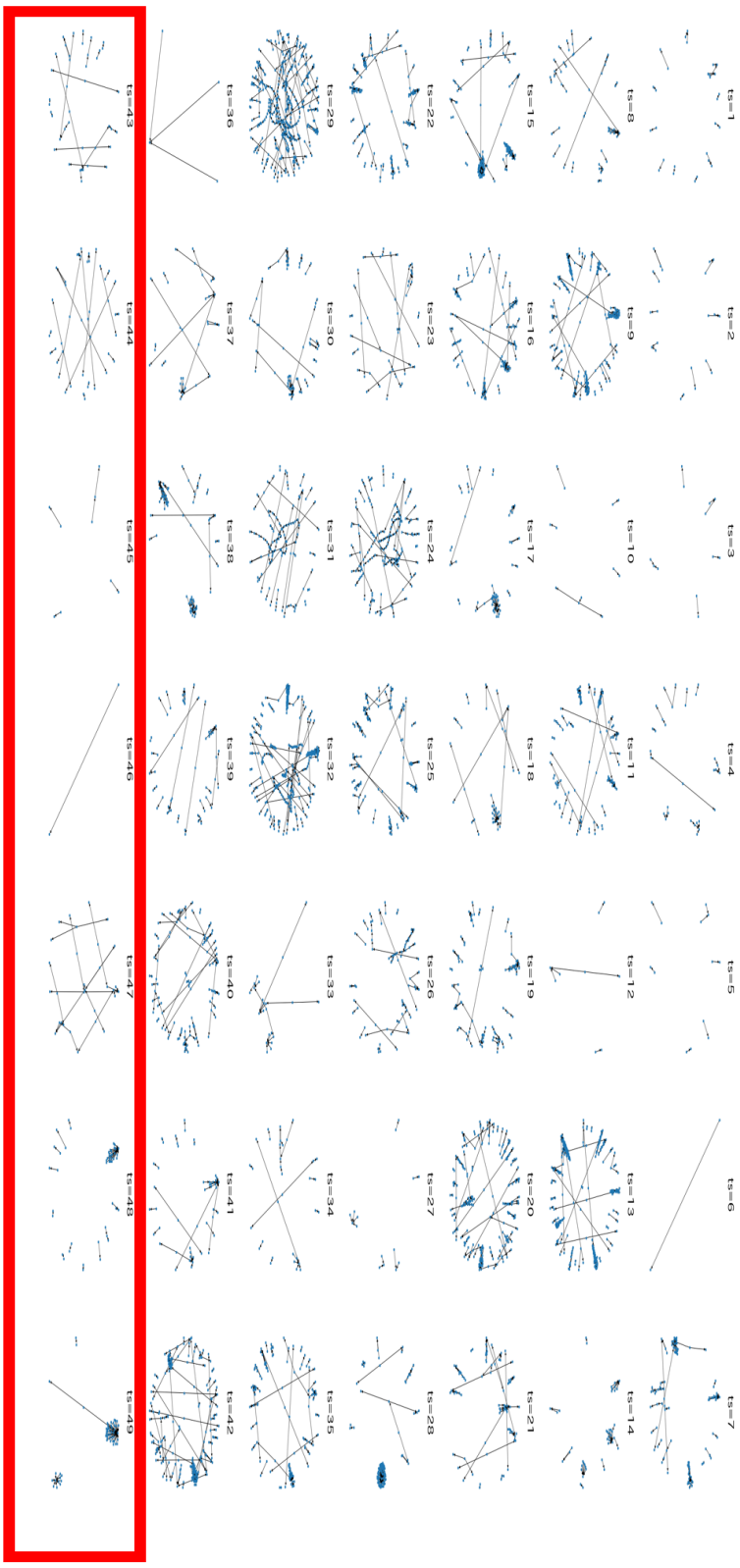


Fig 9 -2 Graph of illicit transactions(by Time Step)

第１０章　　まとめと提言

本研究では Elliptic 社が提供している半教師ありデータを利用し，ビットコインの違法，合法取引の分類に関して，機械学習の各種手法を組み合わせることにより精度を向上させることができることを示した．また．それでも，時間帯によっては，様々な工夫にも関わらず違法取引の検出力を上げることができず，違法取引の取引パターンによってはうまく検出できないことも示した．また，異常検知の手法による教師なし学習による違法取引の検知の結果が芳しくないことから，機械学習の方法は，新しい違法取引のパターンに対して脆弱である可能性を示した．

本研究で不正取引の９割以上を特定できたことから，Elliptic Dataset のようなラベル付きデータベース（教師データ）をビットコイン業界が協力して構築し続けていければ，更なる精度の向上は可能であると考える．本データセットで検出できなかった違法取引についても，さらに大きな学習データセットがあれば検出できる可能性は高まるであろう．また検出できない違法取引に関しては，このデータセットが考慮していない情報を使うことで特定することができるかもしれないと考えられる．

従来型の金融である，銀行取引やクレジットカード取引とビットコインの取引を対比すると，①従来型の金融は匿名性がなく，また違法取引をするにも不正に銀行口座を開いたり，クレジットカード番号を取得する必要があるが，AML 対策が厳しい昨今ではそのような口座開設は容易ではない．ゆえに，犯罪秘匿のために小口化できない．一方で②ビットコインは匿名性があり，また口座を無限に無料で開設することができ，取引の小口化も容易であり，取引を目立たなくすることは容易である．ゆえに，本研究でも異常検知の手法で判別するのが困難であったのではないかと考えられる．

上記から，２点，セキュリティ向上への提言としたい．

- 公的機関や暗号資産取引所などの業界が，ランサムウェア詐欺などの犯罪の振り込み先に指定されたアドレスを，被害者が通報し皆で共有できるウェブサイトを作ることである．登録された違法，犯罪アカウントを直接的に知ることで，犯罪の被害を抑止しやすくすることと，そのようなアカウントの挙動を違法取引検出モデルに速やかに学習させることで，匿名性のあるビットコインの性質をもってしても，違法アカウントを特定，無効化できる（業者はそのような匿名アカウントと取引しないというガイドラインを設ける）可能性は高まると考える．
- ビットコインにおいてアドレスの生成にペナルティ（コストをかける）を

課し，小口化を困難にすること．

これらの提言はビットコインの分散化の思想と相いれないが，一般への普及には必要だと考える．

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] “岸田首相のシティー講演要旨 「強く持続的な資本主義へ」,” *日本経済新聞 (nikkei.com),* p. https://www.nikkei.com/article/DGXZQOUA043HO0U2A500C2000000/, 5 5 2022.

[3] “首相、暗号資産の税制改正に意欲 国民・玉木氏が要求,” *日本経済新聞 (nikkei.com),* p. https://www.nikkei.com/article/DGXZQOUA043HO0U2A500C2000000/, 28 5 2022.

[4] A. Worrachate, “ビットコイン 10 万ドルは実現可能、金のシェア奪う公算－ゴールドマン,” *Bloomberg,* pp. https://www.bloomberg.co.jp/news/articles/2022-01-04/R57GONDWX2PU01, 5 1 2022.

[5] “仮想通貨、世界の時価総額 1 兆ドル消失 米利上げで逆流: 日本経済新聞 (nikkei.com),” *日本経済新聞 (nikkei.com),* p. https://www.nikkei.com/article/DGXZQOUB2592A0V20C22A5000000/, 29 5 2022.

[6] W. Yakowicz, “Inc.,” [オンライン]. Available: https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html. [アクセス日: 10 6 2022].

[7] “Wikipedia-Blockchain analysis,” [オンライン]. Available: https://en.wikipedia.org/wiki/Blockchain_analysis. [アクセス日: 12 6 2022].

[8] 宇根正志, “暗号資産における取引の追跡困難性と匿名性：研究動向と課題,” 日本銀行, 2019.

[9] L. Yang, C. Yue, T. Hao, X. Gengsheng and Z. Zibin, "Identifying Illicit Addresses in Bitcoin Network," Springer Nature Singapore, 2020.

[10] T. T. Pham , S. Lee, “Anomaly detection in bitcoin network using

unsupervised learning methods.,” 2022.

[11] P. Monamo, V. Marivate , B. Twala, “Unsupervised learning for robust bitcoin fraud detection,” IEEE, 2016.

[12] M. Weber, D. K. I. Weidele, G. Domeniconi, C. Bellei, C. E. Leiserson, J. Chen and T. Robinson, "Anti-money laundering in bitcoin: experimenting with graph convolutional networks for financial forens," Association for Computing Machinery, 2019.

[13] Elliptic, www.elliptic.co..

[14] I. Alarab , P. Simant, “Effect of data resampling on feature importance in imbalanced blockchain data: Comparison studies of resampling techniques,” Data Science and Management Volume 5, Issue 2, June 2022, Pages 66-76, 2022.

[15] D. Vassallo, V. Vella , J. Ellul, “Application of Gradient Boosting Algorithms for Anti-money Laundering in Cryptocurrencies,” Springer, SN Computer Science, 2021.

[16] Elliptic, “Elliptic Data Set,” 31 7 2019. [オンライン]. Available: https://www.kaggle.com/datasets/ellipticco/elliptic-data-set. [アクセス日: 30 7 2022].

[17] C. C. Aggarwal, Data classification : algorithms and applications. 1st edition, CRC Press, 2015.

[18] R. Sebastian, “mlxtend,” [オンライン]. Available: http://rasbt.github.io/mlxtend/user_guide/classifier/StackingClassifier/. [アクセス日: 25 12 2022].

[19] scikit-learn.org, “1.14. Semi-supervised learning,” [オンライン]. Available: https://scikit-learn.org/stable/modules/semi_supervised.html#label-propagation. [アクセス日: 5 12 2022].

[20] scikit-learn.org, “sklearn.semi_supervised.LabelSpreading,” [オンライン]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.semi_supervised.LabelSpreading.html. [アクセス日: 5 12 2022].

[21] V. N. Chawla, K. ,. Bowyer, L. O. Hall , W. P. Kegelmeyer, “SMOTE: synthetic minority over-sampling technique.,” 2022.

[22] 曽. 曽我部東馬, Python による異常検知, オーム社, 2021.

[23] 村田剛志, Python で学ぶネットワーク分析 Colaboratory と NetworkX を使った実践入門, オーム社, 2019.

[24] networkx.org, “NetworkX pagerank,” [オンライン]. Available: https://networkx.org/documentation/stable/reference/algorithms/generated/networkx.algorithms.link_analysis.pagerank_alg.pagerank.html. [アクセス日: 10 12 2022].

[25] “ウクライナ侵攻とテクノロジー 浮き彫りにした課題,” *日本経済新聞 (nikkei.com),* p. https://www.nikkei.com/article/DGXZQOUC191UM0Z10C22A3000000/, 22 3 2022.

[26] 佐藤大河 ; 吉浦紀晃, “分散型 Bitcoin 資金洗浄サービスの出金先アドレスの検出と絞り込み,” 2022.

[27] 全珠美 , 水野貴之, “仮想通貨送金モデル化と責任ある市場の創出,” 2022.

[28] P. Xia, H. Wang, B. Zhang, R. Ji, B. Gao, L. Wu, X. Luo , G. Xu, “Characterizing cryptocurrency exchange scams,” 2020.

[29] 江原貴史 , 高橋大志, “ビットコインの取引データにおける違法取引と合法取引の分類問題の経路依存性に関する分析,” 2022.

[30] 江原貴史 , 高橋大志, “ビットコインの取引データにおける違法取引と合法取引の経路依存性に関する分析,” 2022.

[31] Z. Dengyong, B. Olivier, N. L. Thomas, W. Jason , S. Bernhard, “Learning with local and global consistency,” *Neural Information Processing Systems 16,* 2004.

[32] M. Malte, “Anonimity of Bitcoin Transactions,” 2013.

[33] 永田倖大 , 菊地浩明, “Bitcoin アドレスの送金先集合に基づく匿名性の評価,” 2018.

Appendix　詐欺メールとその違法アカウントに対する予備調査

筆者に届いた詐欺メール（犯罪者にビットコインを振り込むことを要求されている物）について分析した．

データ

筆者の携帯電話キャリアメールに 2021 年 1 月から 2022 年 6 月 11 日までに届いた，詐欺グループからの詐欺メール 17 件（メール本文中には振込先のビットコイン不正アドレスが記載されてある）について分析する．これら１７件は詐欺メールの教師データであり，かつメール本文中のアドレスは，不正アドレスの教師データとみなせる．

分析項目

① メールのヘッダー情報の IP アドレスから詐欺グループの所在地について検討する．
② メール本文から詐欺グループのビットコインアドレスを取り出す．
③ 詐欺グループのビットコインアドレスの取引履歴を https://explorer.btc.com/en で調べる．
④ 詐欺グループのビットコインアドレスを AMLBot(https://amlbot.com/) という AML Corporation 社が提供する詐欺，ランサムウェア，ダークネット関係の不正アドレスであるかであるか否かのスコアリングをするサイトでスコアリングする．AMLBot が，不正アドレスをどのように評価（スコアリング）するかを調べる．AMLBot が表示する不正アドレスの取引先の属性を元に，取引の背景を考察する．

分析例

以下実際のデータを見ていく.

図 0-1　分析対象詐欺メール

☐	takashie555…	デバイスがハッキングされました それ…	5月31日
☐	izumi@hakar…	未払いがございます。債務の決済が必要で す。 &#1237…	5月20日
☐	atose8508@…	未払いがございます。債務の決済が必要で す。 &#1237…	5月20日
☐	m0651002@…	未払いがございます。債務の決済が必要で す。 &#1237…	5月20日
☐	sale2@kano…	You have an outstanding payment. Debt settlement …	5月 4日
☐	chelseydave…	アカウントからのお支払い。未払いがありま す &#1237…	4月18日
☐	nizzcmmytof…	アカウントからのお支払い。未払いがありま す &#1237…	4月18日
☐	jkcas@strike…	アカウントからのお支払い。未払いがありま す &#1237…	4月18日
☐	fcc8578c@ry…	アカウントからのお支払い。未払いがありま す &#1237…	4月18日
☐	takashie555…	情報リクエストに関する個人的な ご覧…	4月 5日
☐	takashie555…	Pending for payment.	3月18日
☐	gvallex@stri…	Subject: Help Ukraine	3月 9日
☐	takashie555…	You have an outstanding payment.	21/10/31
☐	takashie555…	重要なニュース 初めま&#12…	21/05/01
☐	takashie555…	重要なニュース 初めま&#12…	21/04/28
☐	takashie555…	重要なニュース 初めま&#12…	21/04/16
☐	takashie555…	情報リクエストに関する個人的な ご覧…	21/01/06

出所：筆者あてに届いた詐欺メール

表示される送信者名（本来の詐欺グループのメールアドレスが表示されるべき場所）に筆者のアドレスがあったりして，でたらめであることがわかる.

タイトルは，“支払い”，“未払い債務”，“payment”，”ハッキング“などいかにも詐欺的だが，心理的に動揺を誘う文句が並んでいる.

図 0-2　分析対象詐欺メール本文例

From takashie55555takashie55555@docomo.ne.jp

To takashie55555takashie55555@docomo.ne.jp

件名 デバイスがハッキングされました

それが起こったのです。ゼロクリックの脆弱性と特別なコードを使用して、Webサイトを介してあなたのデバイスをハッキングしました。
私の正確なスキルを必要とする複雑なソフトウェア。
このエクスプロイトは、特別に作成された一意のコードを使用してチェーンで機能し、このようなタイプの攻撃は検出されません。
Webサイトにアクセスしただけで感染してしまいましたが、残念なことに、私にとっては非常に容易いことです。
あなたは標的にされたのではなく、そのWebページを介してハッキングされた多くの不運な人々の一人になったのです。
これはすべて8月に起こりました。そのため、情報収集には十分な時間がありました。

次に何が起こるかはもうご存知だと思います。
数ヶ月間、私のソフトウェアは、あなたの習慣、あなたが訪問するウェブサイト、ウェブ検索、あなたが送るテキストなどの情報を静かに収集していました。
他にもまだまだありますが、これがどれほど深刻であるかを理解していただくために、いくつかの理由を挙げました。

明確に言うと、私のソフトウェアはあなたのカメラとマイクも制御しました。

プライバシーを侵害するのはちょうど良いタイミングでした。
あなたを主演とした価値あるPORNHUBビデオをいくつか作成しました。

すでに十分に待ったので、これに決着をつける時が来たと思い立ちました。
こちらが私からのご提案です。 これを、私が希望するコンサルティング料金と名付け、これまでに集めてきたメディアコンテンツを削除したいと思います。

私が支払いを受け取れば、あなたのプライバシーは守られます。
そうでなければ、私はあなたの連絡先に最も有害なコンテンツを漏らし、変質者が見ることができるようにそれを公開ウェブサイトに投稿します。

あなたも私も、これによってあなたが被る損害の大きさを認識しています。あなたのプライバシー保護にあたってそれほど多くの金額は要されません。
私はあなたに個人的な関与をしません。そのため、私が所有するあらゆるファイルやあなたのデバイス上のソフトウェアが、転送を受けた直後に削除されることについてご信頼ください。

私の適切なコンサルティング料金は、ビットコインで送金される1750ドルです。 振込時の為替レート。
この金額をウォレットに送る必要がありますBTC 1FDYfTJ6U4Bgzy5tkwy5ucBu2xvTAPgEe3

定められた料金は変更できません。2営業日以内に支払うものとされます。 支払いを受け取る事だけが重要です。

言うまでもなく、プライバシーを侵害されたく無ければ、誰かに助けを求めようとするのはやめてください。
支払いを受け取るまであなたの動きを全て監視しています。 契約の期限を守れば、二度と私から連絡が来ることはありません。

どうぞ良い一日をお過ごしください。

出所：筆者にあてに届いたメール

本文中に詐欺グループの身代金要求額（上記１７５０ドル）と振込先ビットコインアドレス 1FDYfTJ6U4Bgzy5tkwy5ucBu2xvTAPgEe3 が記載されている．

図 0-3　詐欺メールヘッダー情報例

```
From: <takashie55555takashie55555@docomo.ne.jp>
Subject: =?utf-8?B?44OH44OQ44Kk44K544GM44OP44OD44Kt44Oz44Kw44GV44KM44G+?=
 =?utf-8?B?44GX44Gf?=
MIME-Version: 1.0
Date: 31 May 2022 03:28:04 +0200
Message-ID: <003c01d8748f$02f09761$d194eda6$@docomo.ne.jp>
Authentication-Results: docomo.ne.jp;
 spf=softfail smtp.mailfrom=takashie55555takashie55555@docomo.ne.jp smtp.helo=[87.70
 dkim=none header.d=;
 dmarc=fail header.from=docomo.ne.jp;spf=relaxed adkim=relaxed
Received: from [87.70.107.42] ([87.70.107.42])
 by mfsmax.docomo.ne.jp(DOCOMO Mail Server Ver2.0) with SMTP id 0e1c0009628a6a598051
 for <takashie55555takashie55555>; Tue, 31 May 2022 07:38:11 +0900 (JST)
X-Filterd-Tracker: gggruggvucftvghtrhhoucdtuddrgedvfedrkeejgdduvdcutefuodetggd
 otefrodftvfcurfhrohhfihhlvgemucffqfevqffoqfdppffqggftiffpkfenuceurghilhhouhht
 mecufedttdenucgspfgrthgthhelucdlfedttddmnecujfgurhephffvufffkfggtgfothfqsegrt
 dhgpedvtddvnecuhfhrohhmpeeothgrkhgrshhhihgvheehheehhehtrghkrghshhhivgehheehhe
 ehseguohgtohhmohdrnhgvrdhjpheqnecuggftrfgrthhtvghrnhepgeffueffvdeifeeuteekuee
 lffdvuedugeekgffgjeegvdegleeihfekvdduveeunecukfhppeekjedrjedtrddutdejrdegvden
 ucevlhhushhtvghrufhiiigvpedtnecurfgrrhgrmhepihhnvghtpeekjedrjedtrddutdejrdegv
 ddphhgvlhhopeglkeejrdejtddruddtjedrgedvngdpmhgrihhlfhhrohhmpehtrghkrghshhhivg
 ehheehheehthgrkhgrshhhihgvheehheehheesughotghomhhordhnvgdrjhhppdhnsggprhgtphh
 tthhopedupdhrtghpthhtohepthgrkhgrshhhihgvheehheehhehtrghkrghshhhivgehheehheeh
 seguohgtohhmohdrnhgvrdhjph
X-DCMSpam: 202
To: <takashie55555takashie55555@docomo.ne.jp>
X-Mailer: Microsoft Office Outlook 11
Thread-Index: AcZ1Z1j5nc7g1s71Z1Z1j5nc7g1s7l==
X-MimeOLE: Produced By Microsoft MimeOLE V6.1.7601.17514
Content-Type: multipart/alternative; boundary="----=_NextPart_000_0039_01D8748F.02ED
Content-Transfer-Encoding: 7bit
```

出所：筆者あてに届いたメール

ヘッダー情報を参照すると，SPF(送信ドメイン認証)が spf=none となっており，送信元アドレスを認証するための情報が登録されていない．つまり，何らかの不透明性をもっていることを示唆する．spf=pass が通常である．

IP アドレスについてもメールによってさまざまな細工が見られた．説明は今後付加していく．

IP アドレスからロケーション，サーバー情報も探索した．こちらについても今後まとめて報告する．

図 0-4　不正アドレスの BTC 受取発送状況

出所：BTC.COM

https://explorer.btc.com/ja/btc/address/1FDYfTJ6U4Bgzy5tkwy5ucBu2xvTAPgEe でビットコインアドレス 1FDYfTJ6U4Bgzy5tkwy5ucBu2xvTAPgEe3 について調べた．総受取量を見ると当該不正アドレスには，0.05244684BTC 振り込まれていることが確認できる．また総発送量を見ると 0 BTC とあることから，詐欺グループはこの BTC を寝かせたままにしていることがわかる．

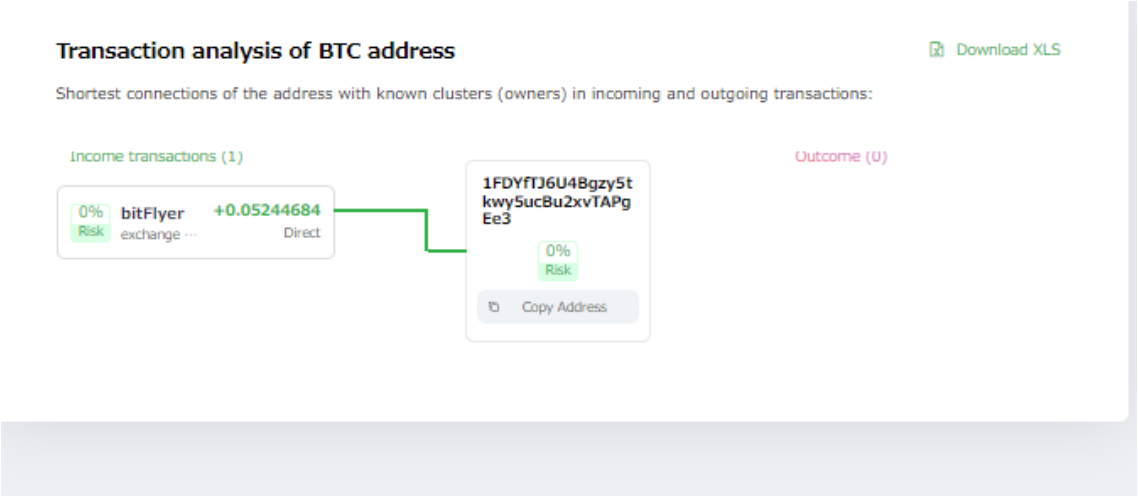
図 0-5　不正アドレスの取引例

出所：BTC.COM

次に，入力と出力について見ると，詐欺の被害者は入力側にいるビットコインアドレス bc1qwqdg6squsna38e46ulcc7kytlcckxswvvzej であることがわかる．

次に，1FDYfTJ6U4Bgzy5tkwy5ucBu2xvTAPgEe3 が AML 社のサイト https://web.amlbot.com/investigations でどのようなリスクスコアで示されるか試してみる．（１つのアドレスのリスクスコアを算出するのに１０米ドル課金される）

図 0-6　不正アドレスと取引先のリスクスコア例



出所：https://amlbot.com/

このサイト上では, 被害者は日本のビットコイン交換業者である bit Flyer 社にアカウントを持っており，そこで日本円からビットコインを購入し詐欺アカウントに振り込んだことがわかる．またこのサイトでは，詐欺グループのアドレスは Risk=0%と表示されている通り，リスクが無いと評価されている．また被害者のアドレスも Risk＝０％と表示されているのは，bit Flyer は日本の法律に従って，顧客の身元確認（KYC）をしているからである．ビットコイン交換業者のアドレスでも，その交換業者自体のリスクが高いと Risk の評価は高い数値が出てくる．

全１７件の詐欺メールから抽出した不正アドレス１３件について上記の操作を繰り返した．

分析結果

Appendix の[表 ０１　詐欺メール集計表]にデータをまとめた．それについて以下で説明する．

メールの送信情報

１７件の詐欺メールすべてが何らかの形で送信認証（SPF）を確認できない形にしていた（spf=none もしくは softfail）．この情報では，犯人を追跡することは困難である．

詐欺の成功可能性

１７件の詐欺メールから重複を除いて１３件の不正アドレス（詐欺グループのビットコインアドレス）を調べた．１３件のうち１１件には少なくとも１人以上の被害者（不正アカウントにビットコインを送信してしまった）が存在していた．（表 ０１の“送金元数”行参照）．

詐欺メールの言語と被害者の居住地

日本語の詐欺メールには，日本の暗号通貨交換業者の顧客が不正アカウントに送金していた．英語の詐欺メールには主に海外の通貨交換業者の顧客と，日本の交換業者の顧客から送金されていた，（表 ０１　“本文”行および“送金元”を参照）

不正アカウントのビットコイン送信先属性

詐欺に成功した１１件中７件の不正アドレスは被害者からの入金後，他のアドレスに出金せずに，放置している．（表 ０１　“総発送量”行を参照）

１１件中４件は不正アドレスから他のアドレスに送金されているが，その４件中２件は”Mixer”と呼ばれるマネーロンダリングのために，追跡困難にするサイトに送金している．（表 ０１　“送信先”行を参照）

AMLBot のリスクスコア

英文での詐欺メールのアドレスには，AMLBot は４件中３件で１００％のリ

スクスコアをつけ，残りの１件でも４３．７％と比較的高いスコアをつけている．被害者が１人でかつ，不正アドレスが受け取ったビットコインを他のアカウントに送信しなくても１００％リスクありと判定しているものもある．詐欺メールについての情報が共有されているものに関して，詐欺アカウントとして判定している可能性がある．（表 01　“リスクスコア”行を参照）

日本語の詐欺メールの不正アドレスに関しては，不正アカウントから，リスクの高いアドレス（具体的には，Mixing サービスサイト）への送信が見られたものには３０％程度のリスクを付与しているが，不正アドレスが被害者からビットコインを受け取るだけでは，リスクを０％と見積もっている．（表 01　“リスクスコア”行を参照）

以上から，英文で詐欺メールに記載されている不正アドレスは，AMLBot のスコアがよりリスクを適切に見積もっていると思われる．

A1　詐欺メール，IP，不正アドレス等の集計表

表　1　詐欺メール集計表

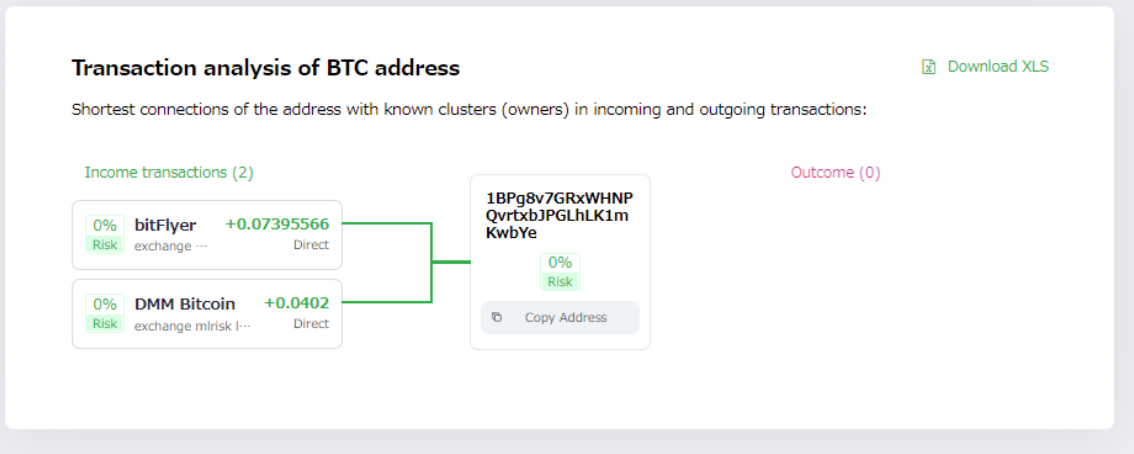
受信日時	2022年05月31日 7:38	2022年05月20日 15:29	2022年05月20日 11:05	2022年05月20日 10:12	2022年05月04日 12:58	2022年04月18日 21:19	2022年04月18日 20:40	2022年04月18日 18:11	2022年04月18日 14:42
送信者	takashie55555takashie55555@docomo.ne.jp	izumi@hakariya.co.jp	atose8508@268.jp	m0651002@edu.kit.ac.jp	sale2@kanokwanfood.com	chelseydavenport7628@mailcatch.com	nizzcmmytof@scmk.sony.co.jp	jkcas@striker.ottawa.on.ca	fcc8578c@ryugakunet.com
受信者	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp
件名	デバイスがハッキングされました	未払いがございます。債務の決済が必要です。	未払いがございます。債務の決済が必要です。	未払いがございます。債務の決済が必要です。	You have an outstanding payment. Debt settlement required.	アカウントからのお支払い。未払いがあります	アカウントからのお支払い。未払いがあります	アカウントからのお支払い。未払いがあります	アカウントからのお支払い。未払いがあります
spf=	spf=softfail	spf=none	spf=none	spf=none	spf=none	spf=none	spf=none	spf=none	spf=none
偽装した送信元					[111.119.183.41]			from static.vnpt.vn	[212.47.142.116]
送信元IP	**[87.70.107.42]**	**[106.195.33.239]**	[177.137.254.122]	[170.0.214.155]	[45.116.232.255]	[203.89.122.249]	[197.254.141.55]	[14.229.213.25]	[212.47.136.124]
送信元ロケーション									
Xmailer	**Microsoft Office Outlook 11**	**Microsoft Windows Live Mail 15.4.3508.1109**	Microsoft Outlook 14.0	Microsoft Windows Live Mail 15.4.3508.1109	Mozilla/5.0 (Windows NT 6.0; rv:14.0) Gecko/20120713 Thunderbird/14.0	Microsoft Outlook Express 6.00.2900.3672	Mozilla/5.0 (Windows NT 6.1; rv:6.0.1) Gecko/20110830 Thunderbird/6.0.1	Microsoft Outlook 15.0	Microsoft Windows Live Mail 16.4.3505.912
本文	それが起こったのです。ゼロクリックの脆弱性と特別なコードを使用して、Webサイトを介してあなたのデバイスをハッ	こんにちは！ 残念ながら、不快なお知らせがございます。 数ヶ月前、ネット閲覧に利用され	こんにちは！ 残念ながら、不快なお知らせがございます。 数ヶ月前、ネット閲覧に利用され	こんにちは！ 残念ながら、不快なお知らせがございます。 数ヶ月前、ネット閲覧に利用され	Hello! Unfortunately, I have some unpleasant news for you. Roughly several months ago	こんにちは！ 残念ながら凶報がございます。 数ヶ月前、あなたがインターネット閲覧に利用している	こんにちは！ 残念ながら凶報がございます。 数ヶ月前、あなたがインターネット閲覧に利用している	こんにちは！ 残念ながら凶報がございます。 数ヶ月前、あなたがインターネット閲覧に利用している	こんにちは！ 残念ながら凶報がございます。 数ヶ月前、あなたがインターネット閲覧に利用している
ビットコインアドレス	1FDYfTJ6U4Bgzy5tkwy5ucBu2xvTAPgEe3	14gu1L6wrKzLEyoTJkQPHWNFovN6o9mAMd	14gu1L6wrKzLEyoTJkQPHWNFovN6o9mAMd	1P4S3GyB925R51WpCkJ4QNdGoM6Yw8jRTj	1MW4maqRuqi62YiRNMaBiHT65WJJMEAvQw	1BPg8v7GRxWHNPQvrtxbJPGLhLK1mKwbYe	14su8eLbjd5n4K4KSW86quMKZpVHEc1tG	14su8eLbjd5n4K4KSW86quMKZpVHEc1tG	14su8eLbjd5n4K4KSW86quMKZpVHEc1tG
リスクスコア	0%	0%		32.80%	43.70%	0	0		
送金元	Bitflyer	NA		Bitflyer, GMO	Coinbase,OKX PAXful Luno,Coincheck,Binance etc	Bitflyer, DMM	Bitflyer		
送金元数	1	NA		3	15		1		
送信先	NA	NA		Settled	Settled	NA	NA		
残高	0.05244684	NA		0	0	0.11415566	0.03625406		
価値	¥215,395	NA		¥0	¥0	¥390,699	¥123,691		
総受取量	0.05244684	NA		0.15889114	0.39831752	0.11415566	0.03625406		
総発送量	0	NA		0.15889114	0.39831752	0	0		
Tx数	1	NA		4	16	3	1		

2022年04月05日 14:18	2022年03月18日 1:04	2022年03月09日 19:56	2021年10月31日 1:09	2021年05月01日 10:14	2021年04月28日 21:00	2021年04月16日 9:19	2021年01月06日 1:24
takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	gvallex@striker.ottawa.on.ca	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp
takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp	takashie55555takashie55555@docomo.ne.jp
情報リクエストに関する個人的な	Pending for payment.	Subject: Help Ukraine	You have an outstanding payment.	重要なニュース	重要なニュース	重要なニュース	情報リクエストに関する個人的な
spf=none	spf=none	spf=none	spf=softfail	spf=softfail	spf=softfail	spf=softfail	spf=softfail
from host-185-124-220-161.zadata.[185.124.220.161]	from 195-230-40-54.adsl.highway.telekom.[195.230.40.54]	from dynamic-ip-1868489153.cable.net.[186.84.89.153]	[1.55.109.92]	from 27-32-116-227.tpgi.com.au [27.32.116.227]	from 158-7-239-197.r.airtel.ug [197.239.7.158]	from host-static-5-56-95-20.moldtelecom.5.56.95.20	from 186-249-230-106.centurytelecom.186.249.230.106
			[1.55.109.92]				
Microsoft Outlook Express 6.00.2900.5931	Microsoft Outlook Express 6.00.2800.5473	Onkxxvsj njvfix 5.9	Microsoft Outlook Express 6.00.2600.1374		Microsoft Outlook Express 6.00.2900.2180	Microsoft Outlook Express 6.00.2900.5931	Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.9) Gecko/20100825
ご覧いただけますように、このメールはあなたご自身のアカウントから送信されています。残念なお知らせです	Greetings! Have you seen lately my e-mail to you from an account of yours? Yeah, that merely confirms that I have	Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.	Hello there! Unfortunately, there are some bad news for you. Around several months ago I have obtained access to	初めまして！ 残念なお知らせをするために、ご連絡を差し上げております。僕は、約２～３ヶ月前にネット閲	初めまして！ 残念なお知らせをするために、ご連絡を差し上げております。僕は、約２～３ヶ月前にネット閲	初めまして！ 残念なお知らせをするために、ご連絡を差し上げております。僕は、約２～３ヶ月前にネット閲	ご覧いただけますように、このメールはあなたご自身のアカウントから送信されています。残念なお知らせです
19SiHgAL3Wg9BVUmosXHumwAA2RHmcd7ng	1PUwf7ybLvvKLJ8NpWeaEChz4WFQtnC2Gx	357a3Sc2Akf7EkqvP18osJFerwAPjsU4jp	1P8zGx51BpyxEy5jBgr5ugoPXbSgyd7fpw	12wffvy5o4d5hm7KVxHJDVaijjsdJBh5yi	12wffvy5o4d5hm7KVxHJDVaijjsdJBh5yi	1KX1pFPyJVbqjtDWPJmdcAuhwJ4Y69oZDR	14Dn6nDgZcX8wZvURyMYZhVrV7MvaYi7rF
32.80%	100%RansomWare	100%RansomWare	100%Phishing	35.90%		31.60%	0%
Bitflyer	BtcTurk, Binance,BitGo,GMO, Bitflyer,Coinbase, Kucoin,Huobi etc	Unnamed entities	Binance, DMM, Coinbase, BitGo	GMO coin		DMM ,Coincheck	NA
1	12	1	10	1		2	NA
Mixer100%	NA	0.00029022	0	Mixer100%, Sanctions100% p2p		Mixer100%,exchange25%	NA
0.03556105	0.40832732	0.00029022	0.25208097	0		0	NA
¥0	¥1,393,423	¥991	¥861,401	¥0		¥0	NA
0.03556105	0.40832732	0.00029022	0.25208097	0.065		0.05705452	NA
0.03556105	0	0	0	0.065		0.0570452	NA
2	12	1	10	4		4	NA

出所：筆者集計

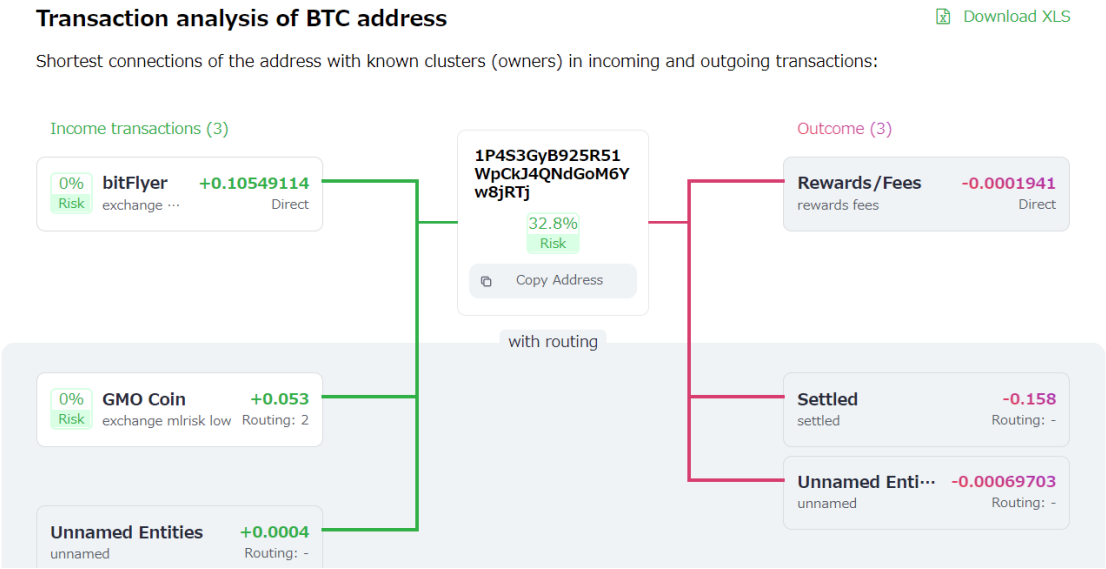
A2　詐欺アドレスのリスクスコアリング

リスクスコアリング 1



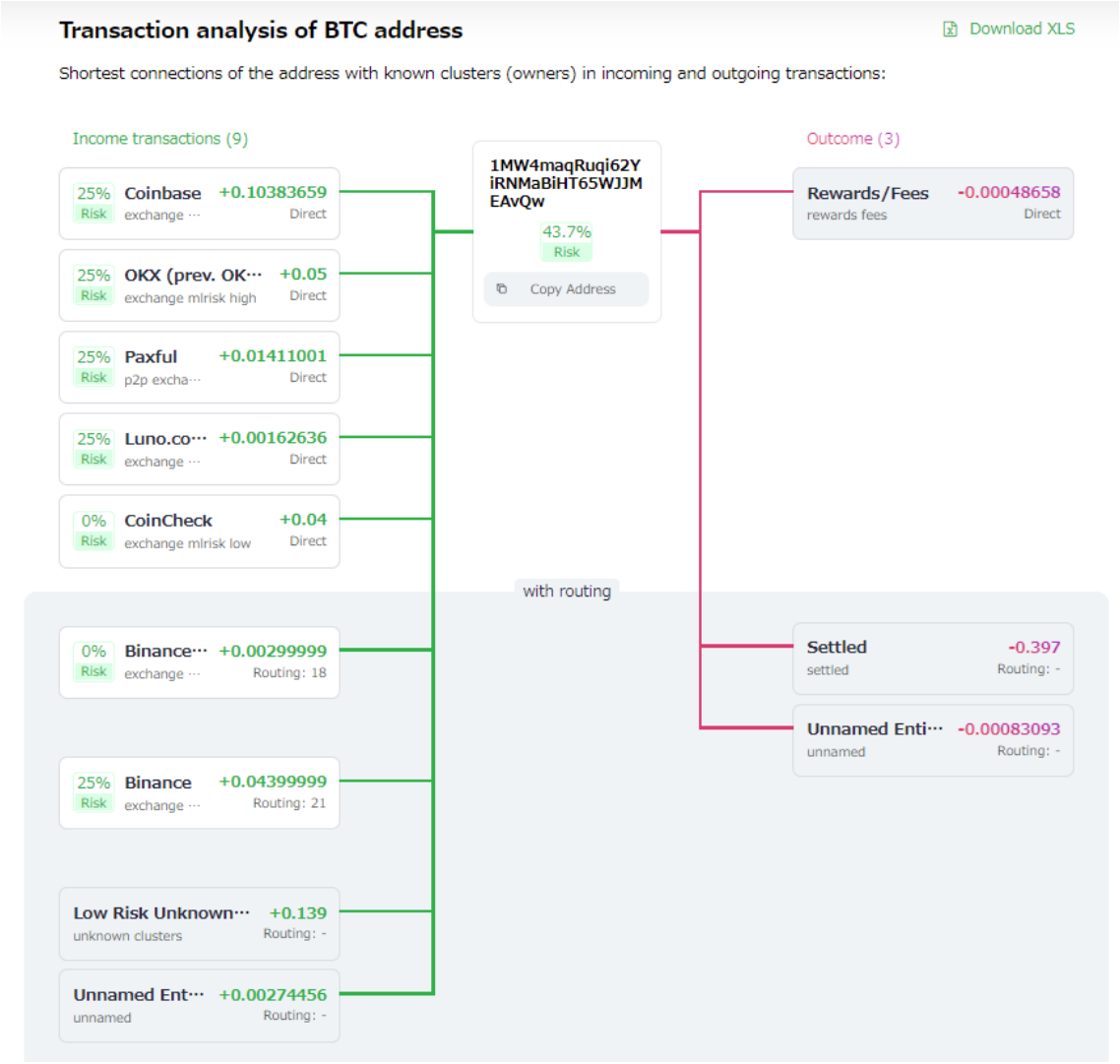
出所：https://amlbot.com/

リスクスコアリング 2



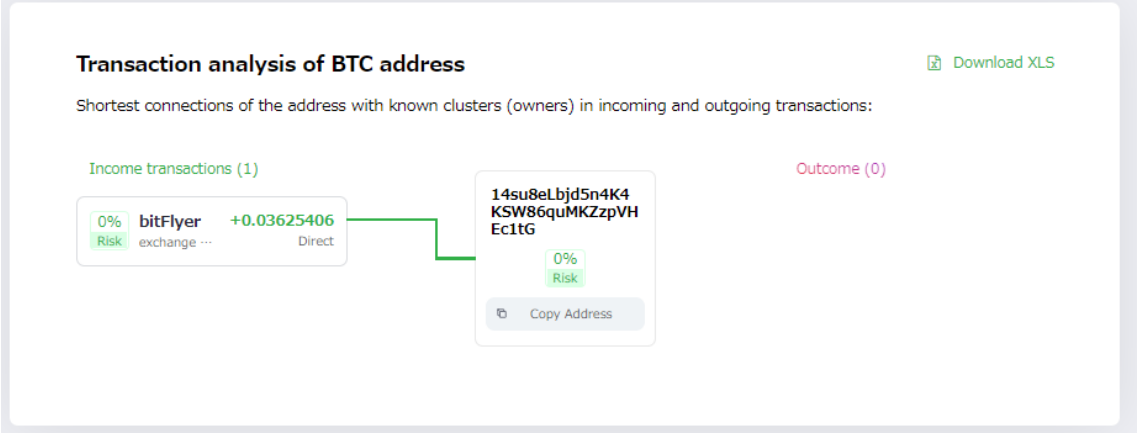
出所：https://amlbot.com/

リスクスコアリング 3



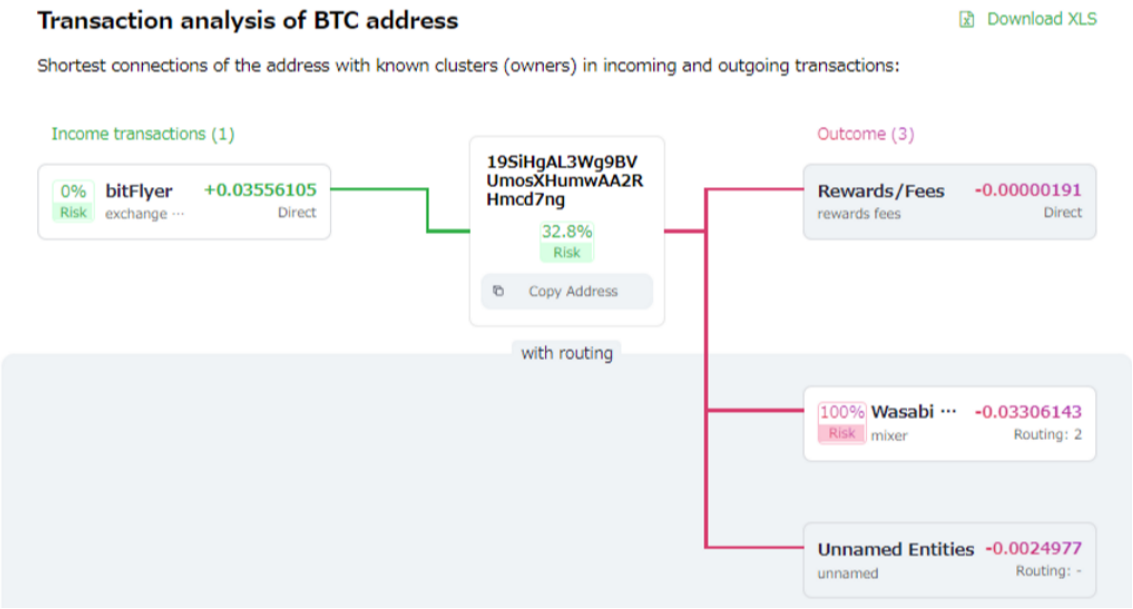
出所：https://amlbot.com/

リスクスコアリング 4



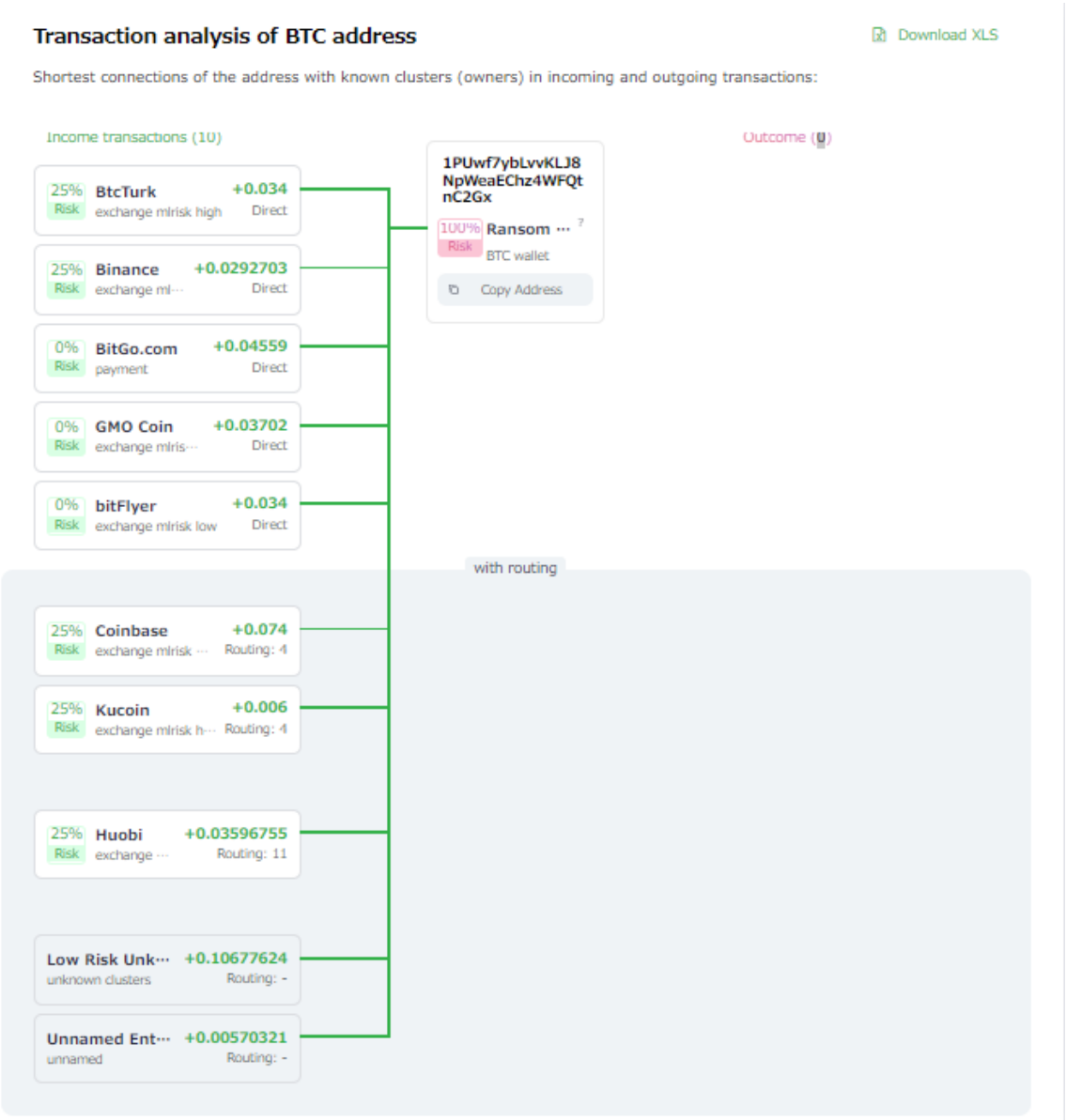
出所：https://amlbot.com/

リスクスコアリング 5



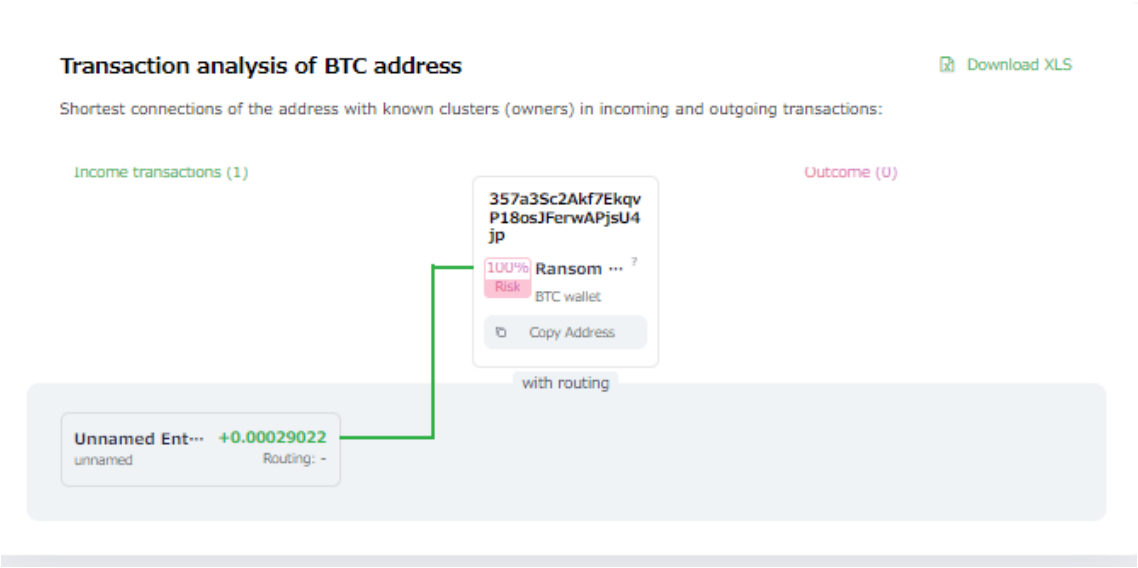
出所：https://amlbot.com/

リスクスコアリング 6



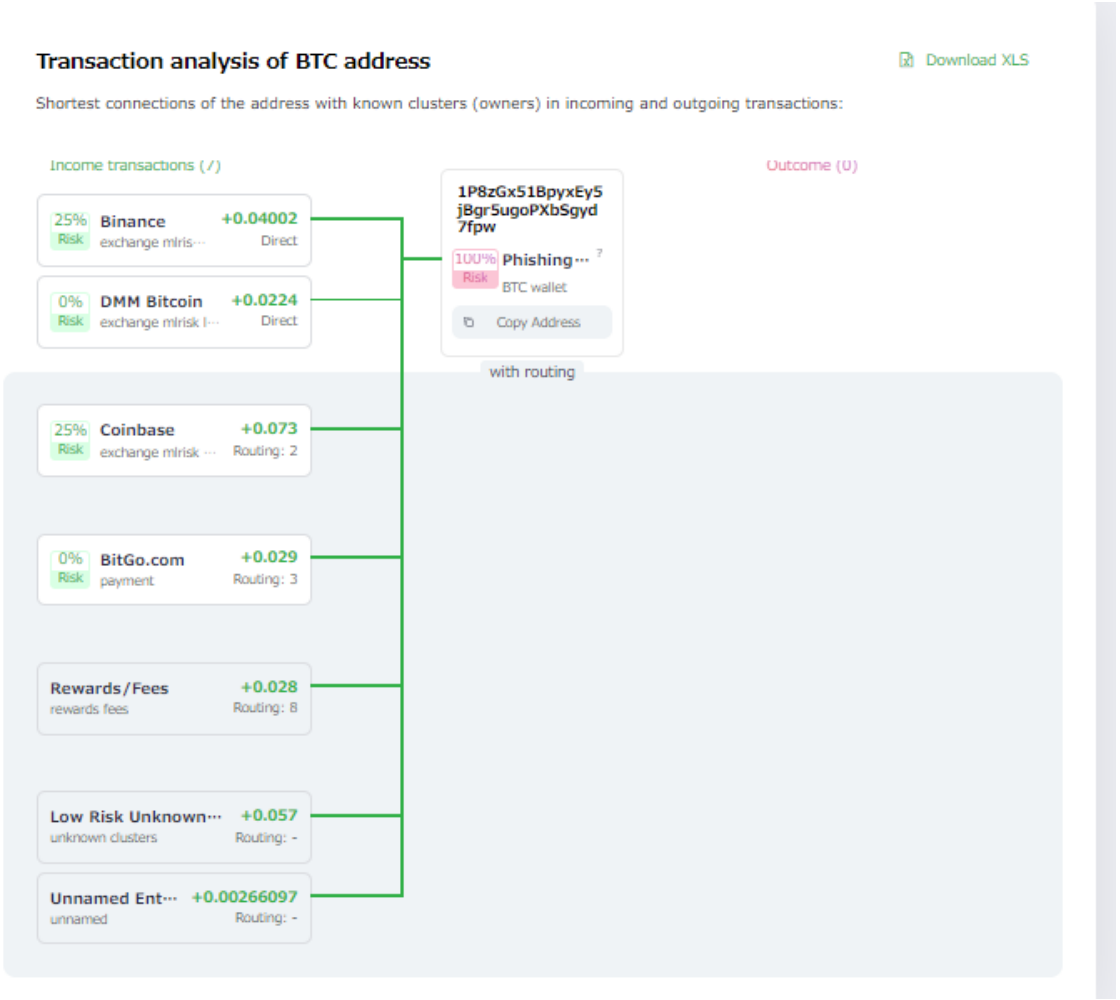
出所：https://amlbot.com/

リスクスコアリング 7



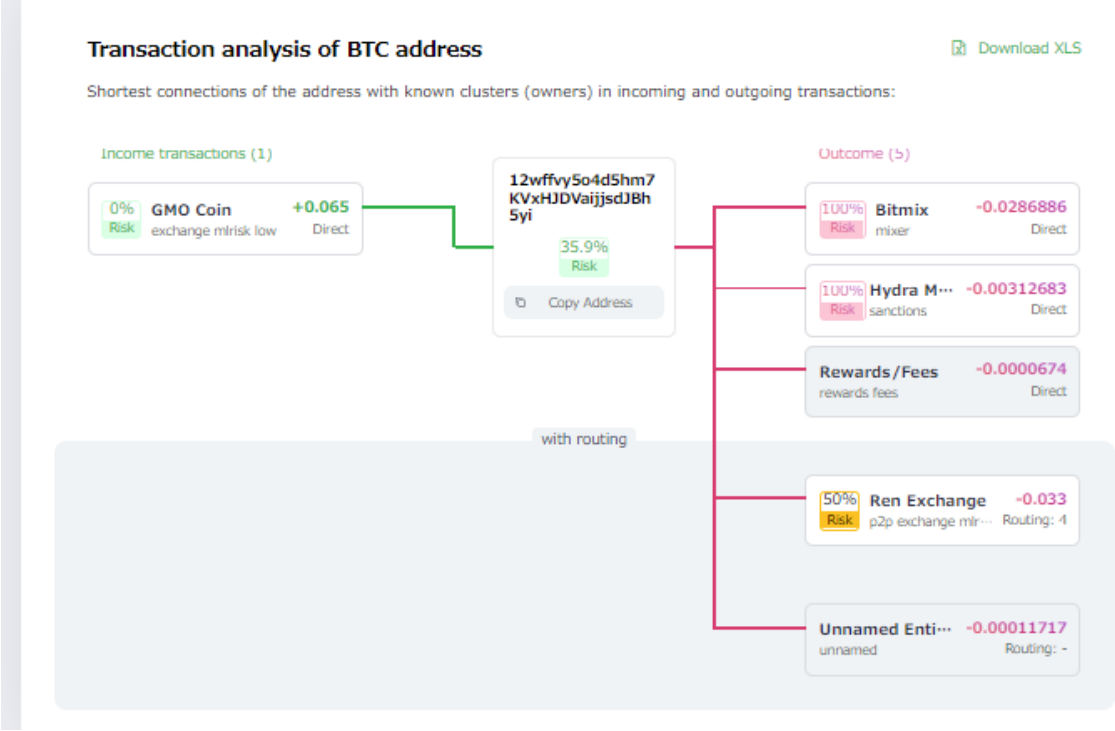
出所：https://amlbot.com/

リスクスコアリング 8



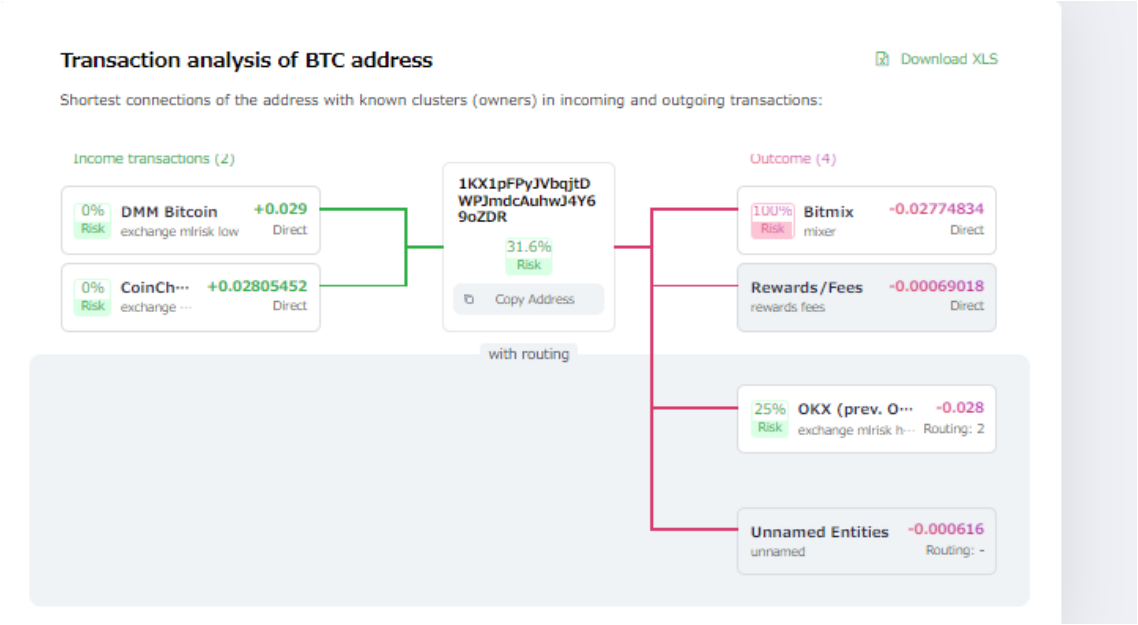
出所：https://amlbot.com/

リスクスコアリング 9



出所：https://amlbot.com/

リスクスコアリング 10



出所：https://amlbot.com/

謝辞

本研究を行うにあたり、常に親身にご指導頂いた高橋大志教授に心より御礼申し上げます。また、ご助言頂きました副査である大林厚臣教授、小幡績准教授にお礼申し上げます。支えてくださった妻，長男，長女に感謝を申し上げます。有益なアドバイスをくださった友人にも感謝を申し上げます.

図表目次

Table 6-1 Supervised learning models classification performance . 18
Table 6-2 Bagging enhanced performance on Decision Tree, Logistic, k-NN, SVM..... 20
Table 6-3 Boosting reduced accuracy..... 21
Table 6-4 Stacking enhanced F1Scores..... 21
Table 6-5 Over sampling + Bagging enhanced F1Score..... 22
Table 6-6 Over sampling + Stacking enhanced F1Score..... 23
Table 6-7 Label spreading..... 24
Table 7-1 Various ensemble models 26
Table 7-2 Stacking models 26
Table 7-3 Stacking and SMOTE 26
Table 7-4 Classification performance under different Train/Test data size 28
Table 7-5 Classification performance using most recent data as train data. 29
Table 7-6 Classification performance with various combination of time steps Random Forest 30
Table 7-7 Classification performance with various combination of time steps Logistic Regression..... 31
Table 7-8 Classification performance with various combination of time steps Gradient Boosting 31
Table 7-9 Classification performance with various combination of time steps AdaBoost 32
Table 7-10 Classification performance with various combination of time steps LinearSVC..... 32
Table 7-11 Classification performance with various combination of time steps k-NN 33
Table 7-12 Classified by K-Means, PCA, Random Forest..... 35
Table 7-13 Classified by K-Means and Random Forest 36
Table 7-14 Classified by K-Means..... 37
Table 7-15 Label spreading and SMOTE 38
Table 8-1 Reconstruction Error 39
Table 9-1 Average degree of transactions 44

Table 9-2 Degree of transactions(normalized) 45
Table 9-3 PCA scores 46
Table 9-4 PCA Loadings 46

Fig 4-1 Number of Illicit, Licit, Unknown trades. 11
Fig 5-1 本研究における各分析の見取り図 16
Fig 8-1 pc1,pc2 score of Licit /Illicit transactions 40
Fig 8-2 pc2,pc3 score of Licit /Illicit transactions 40
Fig 8-3 pc3,pc4 score of Licit /Illicit transactions 41
Fig 9-1 Graph of illicit transactions 47
Fig 9-2 Graph of illicit transactions(by Time Step) 48

図 12-1 分析対象詐欺メール 57
図 12-2 分析対象詐欺メール本文例 58
図 12-3 詐欺メールヘッダー情報例 59
図 12-4 不正アドレスの BTC 受取発送状況 60
図 12-5 不正アドレスの取引例 60
図 12-6 不正アドレスと取引先のリスクスコア例 61