

ビットコインのミキシングにおける資金移動の分析

廣澤 龍典^{1,a)} 上原 哲太郎^{2,b)}

概要：ビットコインにはプライバシー保護のためのミキシングという手法が存在する。しかし、ミキシングはプライバシー保護のためではなく、犯罪によって得たビットコインの追跡を困難にするマネーロンダリングのために用いられることがある。本論文では、実際にミキシングを行い、ミキシングされたビットコインの追跡可能性を考察する。加えて、ミキシングサービス事業者に対してどのような法的規制が存在するかを考察する。その上で、ビットコインのミキシングに対する追跡モデルの提案を行う。

キーワード：ビットコイン, ミキシング, マネーロンダリング

Analysis of fund transfers in Bitcoin mixing

HIROSAWA TATSUNORI^{1,a)} UEHARA TETSUTARO^{2,b)}

Abstract: Mixing is a technique used for privacy in Bitcoin. But the technique is also used for money laundering of ransoms obtained by Ransoms. In this paper, we discuss the possibility to trace transactions of Bitcoin which is applied mixing to enhance privacy. We also discuss about the legal regulations to rule those mixing-service providers. Lastlly, we propose models to trace Bitcoins even when they are applied mixing techniques.

Keywords: Bitcoin, Mixing, Money Laundering

1. はじめに

暗号通貨の中でもビットコインは広く普及しているが、犯罪行為にも広く使われている。特に最近被害の多いランサムウェアでは、身代金がビットコインで支払われる例が多いが、犯罪者はこれによって得た収益をミキシングという手法を用いてマネーロンダリングすることがある。マネーロンダリングとはある収益が、犯罪行為による収益だと捜査機関等にわからないようにすることである。ビットコインは全取引が公開されているため追跡性があるが、ミキシングはこの取引の流れを複雑にして誰から誰に資金が流れたのかわかりにくくするため、マネーロンダリングが可能になる。そこで、本論文ではランサムウェアによる被害の縮小を目的として、ビットコインのミキシングに対す

る追跡モデルの提案を行う。

2. 背景

2.1 ビットコインとミキシング

ビットコインは2008年にSatoshi Nakamotoが発表した論文“Bitcoin: A Peer-to-Peer Electronic Cash System”[1]にて提唱され、この論文に基づき2009年に実運用が始まった仮想通貨である。ビットコインの取引内容は公開されているため、一度アドレスが個人情報と結びつくとなすべての取引を追跡される恐れがある。第三者による追跡を防ぎ、プライバシーを保護するためにミキシングという概念が存在する。ミキシングとは、ビットコインを自分が保有するアドレスと全く関係のない複数のアドレスとの間で複雑な取引を繰り返したあと受け取ることで、そのアドレスに蓄積されたビットコインが元々どのアドレスから送金されたものかをわかりにくくする行為である。実際にミキシングをサービスとして提供しているサイトは多数あり、そ

¹ 立命館大学大学院 情報理工学研究科

² 立命館大学 情報理工学部

^{a)} hiroawa@cysec.cs.ritsumei.ac.jp

^{b)} t-uehara@fc.ritsumei.ac.jp

これらの仕組みは以下の通りである。

- (1) ミキシングサービス事業者（以下、MS 事業者）は顧客からミキシングしてほしいビットコインを受け取る。
- (2) MS 事業者は複数の顧客から受け取ったビットコインを合算してから複数のアドレスとの間で取引を繰り返し、取引の流れを分かりにくくする。
- (3) MS 事業者は顧客の指定したアドレスに、受け取った額から手数料を差し引いて送金する。

ミキシングにおいて、MS 事業者が受け取るために指定するアドレスおよび顧客が返送してもらうために指定するアドレスは、共に未使用である。ミキシングによって取引の追跡が困難になることにより、顧客が MS 事業者への送金に利用したアドレスと、顧客が MS 事業者からのビットコイン受取に利用したアドレスとの相関が断ち切られるようになっている。

3. 実験

ビットコインをミキシングした場合、ビットコインがどのように移動するのかを明らかにすることで、ランサムウェア犯罪者がビットコインを支払い方法に指定することへの抑止力となる。本章では、実際にミキシングサービスを利用して得られた結果を示し、追跡の困難さについて考察を行う。使用した MS 事業者は以下の 3 つである。

- Coinmixer^{*1}
- BitcoinCloak^{*2}
- HelixLight^{*3}

なお、HelixLight はサービスを終了したため、現在は使用できない。

3.1 実験手順

以下に、ビットコインをミキシングするために行った手順を示す。実験はサービスや金額を変えて複数回行った。

- (1) MS 事業者のホームページへアクセスし、ミキシングの申し込みを行った。申し込みが完了するとビットコインを送信する MS 事業者のアドレスが指定された。申し込みの際には、MS 事業者へ送信するビットコインの金額（サービスによっては、MS 事業者から受け取りたいビットコインの金額）・MS 事業者からビットコインを受け取るアドレス（未使用のもの。以下、受信アドレス）・MS 事業者へビットコインを送信してから、自らがビットコインを受け取るまでに意図的にずらす時間を各受信アドレス毎に指定した。
- (2) ウォレットソフトウェアを用いて MS 事業者から指定されたアドレスを送信先としてビットコインを送信した。

- (3) 指定したアドレスに MS 事業者がビットコインを送信したことを可視化サイト^{*4}を用いて確認した。

3.2 実験結果

行った実験のうち 1 つを取り上げて実験結果を示す。ミキシングの申し込み内容は表 1 の通りである。

表 1 実験におけるミキシングの申し込み内容

MS 事業者	MS 事業者への送信金額	MS 事業者から受け取る金額
BitCloak	0.016 BTC	0.01253941 BTC

MS 事業者へビットコインを送信したトランザクション^{*5}“0c08fcc2f9f274915dcff3bba5713a7257bce0f6fb04f8603b9bc4fa6fe29601”およびその後のトランザクションを図 1 に示す。BitcoinCloak に送信したビットコインは、まず 2 つのアドレスに分配され、分配されたビットコインはそれ

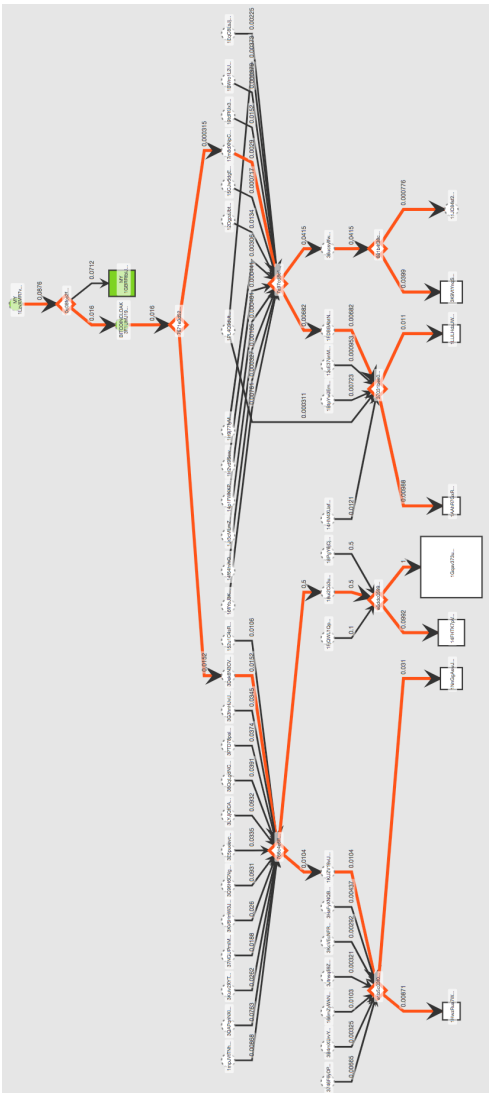


図 1 実験のトランザクション（送信）

^{*1} <http://coinmixibh45abn7.onion/en/>
^{*2} <http://bitcloak43blmhm.onion/>
^{*3} <http://grams7enufi7jmdl.onion/helix/light/>

^{*4} <https://www.blockseer.com/>
^{*5} あるアドレスからあるアドレスへのビットコインの送信を示すデータ

ぞれ 12 個のアドレスが所持するビットコインと混ぜ合わせられた。

なお，MS 事業者からビットコインを受信した際のトランザクションは“a880e1a4ff5306878aad539e7a9e934d0e66600da1c3c712f7e4489e2f98a91a”である．以上 2 つのトランザクションで表 1 に示したとおりのビットコインを送受信した。

3.3 追跡の困難性

身代金を追跡するには，MS 事業者がビットコインを送信したトランザクションとそのトランザクションの後のビットコインの流れを追う必要がある．3.2 節で示した以外の実験回の実験全てにおいて，そのビットコインの流れは図 2 のように表される取引が行われていた。

すべての実験結果で MS 事業者へ送信したビットコインが，いくつかのトランザクションを経て大量のアドレス間で取引され，結果として 1 つもしくは 2 つのアドレスにまとめて格納されていた．2 つのアドレスにまとめられたビットコインについて，片方のアドレスには多額のビットコインが送信され，もう片方のアドレスには少額のビットコインが送信されていた．そして，小額のビットコインが入ったアドレス多数から，1 つまたは 2 つのアドレスに向けてビットコインが集められていた．ビットコインはその構造上，あるアドレスが所持しているビットコインを，該当アドレスに関わる全てのトランザクションから算出しているだけで，特定のビットコインを識別することはできない．そのため，身代金であるビットコインとそうではないビットコインを合わせて再分配されてしまうと，身代金で

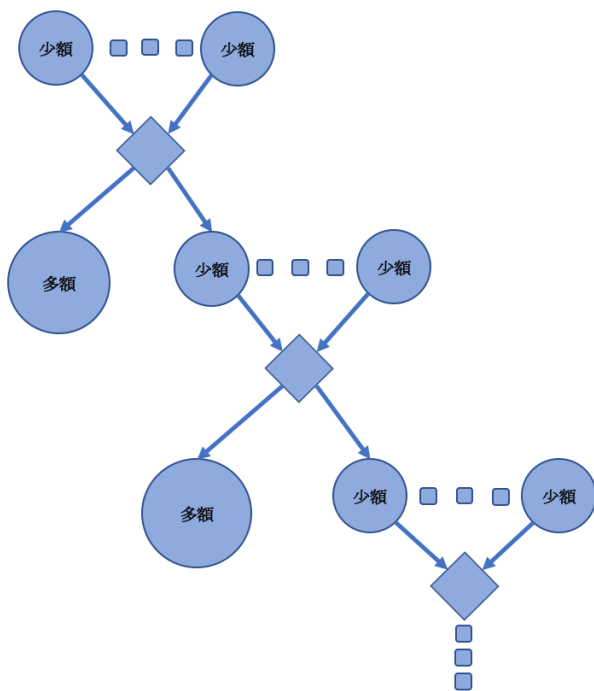


図 2 ミキシングによるビットコインの流れ

あるビットコインが送信された可能性のあるアドレスはすべて確認できるが，それらのアドレスのうち，どのアドレスに身代金であるビットコインが送信されたのか区別することはできない．このようなビットコインの流れで身代金であるビットコインは，ミキシング（マネーロンダリング）される。

身代金追跡を続けることで以上のような明らかに不自然な量のアドレスとビットコインをやりとりしているのが見られた場合，ミキシングを利用したことを推測できる．しかし，MS 事業者がミキシングしてほしいビットコインを受け取る際に指定するアドレスは特異なものではない．加えて，ミキシングの申し込みごとに未使用のものを作成するため，仮に MS 事業者のアドレスをすべて記録していたとしてもその記録と一致することはなく，アドレスのみでは MS 事業者のものだと断定することはできない．また，MS 事業者が作成したと思われる大量のアドレスによって，筆者がビットコインを MS 事業者へ送信したトランザクションから，MS 事業者が筆者へビットコインを送信したトランザクションまで追跡することはできなかった．仮に追跡できたとしてもミキシングの利用者は自身のアドレスをすべて識別できるので追跡できたことを確認できるが，第三者には複数のアドレスの所有者が同一であると確認することはできないため第三者による追跡は成功しない．ただし，MS 事業者のアドレスから MS 事業者のものでないアドレスにビットコインが送信された場合，そのアドレスからは前述したような大量のアドレスとの混ぜ合わせというトランザクションは生じないので，そのアドレスが MS 事業者からビットコインを受け取ったことは推測できる．これにより MS 事業者が作成したものでないアドレスを発見することができるので，あるアドレスが MS 事業者へ送信した金額とほぼ同額のあるアドレスを受け取っているという推測から，それらのアドレスの所有者が同一であると推測することはできる．しかし，MS 事業者は手数料を一定のパーセンテージの間でランダムにしているほか，ミキシングされたビットコインを受け取るアドレスの数を複数個にするよう推奨している．これにより，送信金額のみでは複数のアドレスの所有者が同一であると断定できなくなっている。

以上のことからミキシング特有の流れを識別することで，MS 事業者のものではないアドレスを発見することはできる可能性はあるが，数千個のアドレスおよびトランザクションが MS 事業者によって作られることで，追跡は事実上不可能であり，また発見したアドレスの所有者を断定することはできないため，犯罪者がランサムウェアによって得た身代金をミキシングによってマネーロンダリングした場合，身代金の追跡は極めて難しい．しかし，MS 事業者はミキシングの申し込み内容から犯罪者がミキシングされたビットコインを受け取るアドレスを把握している．そ

のため、追跡している身代金がミキシングされたと分かった場合、MS 事業者がミキシングの申し込み内容の記録（以下、ログ）を提供してもらうことで、犯罪者のアドレスを把握することができるので追跡を続けることができる。しかし、実験に使った3つのMS事業者は匿名性確保の観点から、一定時間が過ぎたらログを消去し保持しないと明言しておりログの提供を受けることは難しい。ログの保持には記録媒体などのコストがかかることを考慮すると、MS事業者が積極的にログを保持する理由はない。本来、マネーロンダリングに使われる可能性のある事業者は、本人確認や取引記録の保持が義務付けられている。次章で、現在の日本の法律ではMS事業者がどのような義務を負うかおよび、MS事業者をどのように規制できるのかを考察する。

4. MS事業者の法的規制

捜査機関がミキシングされたビットコインを追跡できるようにするためには、MS事業者が「ミキシング依頼者のアドレス」および「ミキシングしたビットコインをミキシング依頼者が受信するアドレス」のペアを、ログとして削除せず保持する必要がある。またそのログを捜査機関が必要な時に閲覧できなければならない。

ログに相当するものとして、法定通貨を扱う金融機関等には、本人確認記録や取引記録がある。金融機関等はこれらを一定期間保持している。保持している理由は、金融機関等が犯罪による収益の移転防止に関する法律 [2]（以下、犯収法）における特定事業者に指定されており、記録等の保持が義務付けられているからである。つまり、MS事業者が特定事業者に該当すれば、MS事業者も本人確認記録や取引記録の保持が義務付けられると考えることができる。犯収法第二条第2項には、47種類の業種が特定事業者として定義されている。

4.1 MS事業者は特定事業者に該当するか

仮想通貨交換業者および資金移動業者は、資金決済法 [3] に定義されており、犯収法における特定事業者に該当する。資金決済法は仮想通貨の定義や、仮想通貨の売買を行う事業者に対しての規制や義務を定めているが、MS事業者およびミキシングについては明確に定義していない。同法に載っている仮想通貨に関連すると思われる事業者2つについて、MS事業者が当てはまるか考察を行う。

4.1.1 MS事業者は仮想通貨交換業者に該当するか

仮想通貨交換業者とは、内閣総理大臣の許可を受けて仮想通貨交換業を行う者である（資金決済法第二条第8項および同法第六十三条の二）。同法第二条第7項第一号は仮想通貨交換業を「仮想通貨の売買又は他の仮想通貨との交換」と定義しており、同項第二号は「第一号の行為の媒介・取次又は代理」と定義している。同項第一号の「仮想通貨の売買」は仮想通貨と法定通貨の交換と考えられるため、

ミキシングはこれに該当しない。同号の後半の「他の仮想通貨との交換」については、少なくとも実験で使用したミキシングはビットコインとビットコインの交換であり、同種ではない仮想通貨との交換ではない。同号の後半は、他の「種類の」仮想通貨との売買（例えば仮想通貨Aを売って仮想通貨Bを買う取引）を示していると考えられるべきである。したがって、MS事業者は仮想通貨交換業者に該当しないと考えられる。

4.1.2 MS事業者は資金移動業者に該当するか

資金移動業者とは、内閣総理大臣の許可を受けて資金移動業を営む者である（資金決済法第二条第3項および同法第三十七条）。資金移動業とは「銀行等以外の者が為替取引（少額の取引として政令で定めるものに限る。）を業として営むこと」をいう（同法第二条第2項）。つまり、ミキシングが為替取引に該当すればMS事業者は資金移動業者となり、特定事業者に該当すると考えることができる。為替取引について銀行法の中に明確な定義はないが、最高裁判例 [4] において「銀行法2条2項2号にいう『為替取引を行うこと』とは、顧客から、隔地者間で直接現金を輸送せずに資金を移動する仕組みを利用して資金を移動することを内容とする依頼を受けて、これを引き受けること、又はこれを引き受けて遂行することをいう」と示された。隔地者とは「意思伝達を行うのに時間を要する場所・状態にある相手方」[5] のことであり、ミキシングにおいてミキシング依頼者と、そのミキシングされたコインを受け取る人は同一であるため、ミキシングは為替取引に該当しない。したがって、MS事業者は資金移動業者に該当しないと考えられる。

4.2 MS事業者は信託会社に該当するか

4.1節で述べたとおり、仮想通貨交換業者および資金移動業者にはMS事業者は該当しないと考えられることから、MS事業者は特定事業者に該当しない可能性がある。しかし、犯収法の特定事業者には仮想通貨交換業者・資金移動業者以外にも「信託会社」が存在する。本節では信託について考察を行う。

4.2.1 信託の基本

信託法 [6] において「信託」とは「特定の者が一定の目的（専らその者の利益を図る目的を除く）に従い財産の管理又は処分及びその他の当該目的の達成のために必要な行為をすべきものとすること」（信託法第二条）をいう。以下に、信託に関する基本的な用語を信託用語集 [7] より引用する。

委託者

財産を受託者に移転し、信託目的に従い受益者のために受託者にその財産（信託財産）の管理・処分などをさせる者。

受託者

信託行為の定めに従い、信託財産に属する財産の管理または処分およびその他の信託の目的の

達成のために必要な行為をすべき者。

受益者

受託者から信託行為に基づいて信託利益の給付を受ける権利と、このような権利を確保するために受託者に対して帳簿閲覧請求や信託違反行為の差止請求などをする権利を有する者。

信託財産

受託者に属する財産であり、信託により管理又は処分すべき一切の財産。

信託目的

委託者が信託設定によって達成しようとする目標であり、受託者の行動の指針となるもの。

4.2.2 受益者の定めのない信託

信託には、受益者の定めのない信託が存在する（信託法第二百五十八条）。これを目的信託という。目的信託は旧信託法において、公益目的以外の目的信託は無効とされていたが、2006年12月の改正により公益目的以外の目的信託も可能になった。ただし、公益目的以外の目的信託は「別に法律で定める日までの間、当該信託に関する信託事務を適正に処理するに足りる財産的基礎及び人的構成を有する者として政令で定める法人以外の者を受託者としてすることができない」（同法附則第三項）と制限が設けられている。

ミキシングを信託と考える場合、受益者（受託者であるMS事業者が生み出す利益を享受する者）を明確に定めることはできないため、通常の信託と考えることができない。しかし、目的信託であれば受益者を定めなくて良いので、ミキシングを信託と考えることができる。表2にミキシングを「ビットコインのプライバシーを保護するための目的信託」と考えた場合の構成を示す。

表2 ミキシングを目的信託と考えた場合の構成内容

信託財産	信託目的	委託者	受託者	受益者
ビットコイン	ミキシング	ミキシング依頼者	MS事業者	不定

以上のように当てはめると、MS事業者は「ビットコインのプライバシーを保護するための目的信託」の引き受けを行う営業をする信託会社と考えることができる。

4.3 MS事業者が信託会社であると考えた場合の規制

MS事業者を信託会社と考えた場合、信託業法[8]および犯収法の規制の対象となる。本節ではこれらの法律によってMS事業者がどのような規制を受けるかについて考察する。

4.3.1 信託業法における規制

信託の引き受けを行う営業（信託業）は、内閣総理大臣の免許を受けた者でなければ営むことはできない（信託業法第三条）。同法第三条の免許を受けた者を信託会社とい

う（同法第二条第二項）。すなわち、ミキシングが信託と考えられる場合、MS事業者がミキシングの引き受けを行う営業をするには免許が必要となる。免許を受ける場合、受けようとする業者は同法第四条に定められた申請書を提出しなければならない。また、同法第三十四条は、業務及び財産の状況に関する事項として内閣府令で定めるものを記載した説明書類を作成し、不特定多数の者が提供を受けることができる状態にすることを信託会社に義務付けている。また、同法第四十二条から第四十四条に基づき、内閣総理大臣は以下の事柄を当該職員もしくは信託会社に命ずることができる。

- 報告または資料の提出
- 施設への立入検査
- 業務改善命令
- 業務停止命令
- 取締役や監査役の解任
- 同法第三条による免許の取り消し

これらの規制により、行政機関はMS事業者の運営母体や経営状態を知ることができ、不適切な事柄があれば指導などを行うことができる。

4.3.2 犯収法における規制

犯収法の特定事業者には、信託会社が含まれているため、MS事業者を信託会社と考えることで、MS事業者は特定事業者と該当すると考えられる。MS事業者が特定事業者と考えられる場合、行政庁（同法第二十二条により、信託会社の行政庁は内閣総理大臣）は、同法第十五条から第十八条に基づき、以下の事柄を当該職員もしくは信託会社に命ずることができる。

- 報告または資料の提出
- 施設への立入検査
- 必要な指導・助言および勧告
- 違反を是正するため必要な措置

これらの命令等に違反した者には罰則が設けられている（同法第二十五条・第二十六条）。また、特定事業者に課せられている同法第四条から八条の義務について、MS事業者に適用して考察する。

取引時確認（同法第四条）

MS事業者は、本人特定事項の確認・ミキシングを行う目的・職業（ユーザが個人である場合、法人である場合は事業内容）を確認しなければならない。

取引の拒否（同法第五条）

上記の取引時確認をミキシング依頼者が拒んだ場合、MS事業者はその取引を拒むことができる。

確認記録の作成および保存（同法第六条）

上記の取引時確認を行った場合、確認記録を作成および保存しなければならない。

取引記録の作成および保存（同法第七条）

ミキシングを行った場合、ミキシング依頼者の確認記

録を検索するための事項・日時などミキシング内容に関する記録を作成および保存しなければならない
疑わしい取引の届出（同法第八条）

ミキシングを依頼されたビットコインが犯罪による収益である疑いが認められる場合、速やかに行政庁に届け出なければならない。また、届け出を行おうとすることまたは行ったことを、ミキシング依頼者またはその関係者に漏らしてはならない。

ミキシングされたビットコインの追跡に必要なログの保持は、同法第七条の「取引記録の作成及び保存」に該当すると考える。犯罪による収益の移転防止に関する法律施行規則 [9] の第二十四条は、取引記録の記録事項について、以下のように定義している（同法施行規則第二十四条より抜粋）。

- (1) 口座番号その他の顧客等の確認記録を検索するための事項（確認記録がない場合にあっては、氏名その他の顧客等又は取引若しくは特定受任行為の代理等を特定するに足りる事項）
- (2) 取引又は特定受任行為の代理等の日付
- (3) 取引又は特定受任行為の代理等の種類
- (4) 取引又は特定受任行為の代理等に係る財産の価額
- (5) 財産移転（令第十五条第一項第一号に規定する財産移転をいう。）を伴う取引又は特定受任行為の代理等にあっては、当該取引又は特定受任行為の代理等及び当該財産移転に係る移転元又は移転先（当該特定事業者が行う取引又は特定受任行為の代理等が当該財産移転に係る取引、行為又は手続の一部分である場合は、それを行った際に知り得た限度において最初の移転元又は最後の移転先をいう。以下この条において同じ。）の名義その他の当該財産移転に係る移転元又は移転先を特定するに足りる事項

問題となるのは上記の記録事項に、ミキシングされたビットコインを追跡するために必要な情報が定められていないことである。よって、捜査機関がミキシングされたビットコインを追跡できるようにするために、MS 事業者が保持すべき情報を詳細に定義しておく必要がある。

関係機関は、MS 事業者が「ミキシング依頼者のアドレス」および「ミキシングしたビットコインをミキシング依頼者が受信するアドレス」のペアを取引記録として保持する義務を負うように、犯収法における取引記録に載せるべき情報の追加について検討すべきである。

5. 身代金追跡モデルの提案

本章では、身代金の追跡モデルを提案する。

5.1 身代金の追跡のシナリオ

被害者の端末がランサムウェアに感染し、身代金を要求されたとする。被害者は、被害状況を確認し身代金を支払

うかどうかを決定する。身代金を払うべきでないという意見もあるがシナリオ上、被害者は身代金を支払うことに決めたとする。被害者は、取引所でビットコインを購入し、ランサムウェアが指定するアドレスに送信する。

犯罪者は MS 事業者により、受け取ったビットコインのミキシングを依頼し、ミキシングされたコインを仮想通貨交換所などで法定通貨に換える。仮想通貨交換業者は本人確認や取引記録の保持を行う。捜査機関は身代金を受け取るアドレスを監視しようとしても、ミキシングによって監視すべきアドレスが攪乱されているため、仮想通貨交換業者が保持している記録等が意味をなさない可能性がある。つまり、追跡は成功しない可能性が高い。

よって、身代金の追跡を可能とするモデルを 2 つ提案する。1 つ目は 4 章で述べた「MS 事業者が特定事業者となり、ログの保持が義務付けられる」という仮定を用いるモデルである。2 つ目は身代金の入ったアドレスとの取引を仮想通貨交換業者に行わないよう通達を行うモデルである。

5.2 提案モデル 1

当モデルでは 4 章で述べた「MS 事業者が特定事業者となり、ログの保持が義務付けられる」という仮定を用いる。提案する「追跡センター」は、身代金の追跡を行う専門捜査機関とする。当モデルにおける追跡センターの最大の目的は犯罪者の検挙である。目的を達成するために追跡センターの構成員には、搜索差押令状の請求権・逮捕令状の請求権・警察権・仮想通貨交換業者および MS 事業者に対して命令を行う権利が必要である。追跡センターの構成員には、ビットコインを技術的に深く理解しておりビットコインを推進しようとする者（例えばビットコイン財団）および警察官が適していると考えられる。被害者・犯罪者のとる行動は基本的に 5.1 節と同じとし、追跡センターを加えた提案モデルを図 3 に示す。

図 3 において、黄色の矢印はビットコインの流れを示し、緑色の矢印は情報や通達の流れを示す。矢印の中にある番号は、以下の追跡の流れを示した箇条書きの番号に対応している。以下に追跡の流れを説明する。

- (1) 被害者は身代金を支払うと同時に、ランサムウェアが指定したアドレスを含んだ被害届を追跡センターに提出する。
- (2) 追跡センターは被害届を受理し、当該アドレスの追跡を開始する。同時に MS 事業者および仮想通貨交換業者に当該アドレスを通達し、当該アドレスと取引を起した場合、追跡センターに届け出を行うようにしてもらう。
- (3) 犯罪者は MS 事業者により身代金のミキシングを依頼する。MS 事業者はミキシングしたビットコインを犯罪者に送信する。
- (4) 依頼を受けた MS 事業者は本人確認を行いログを保持

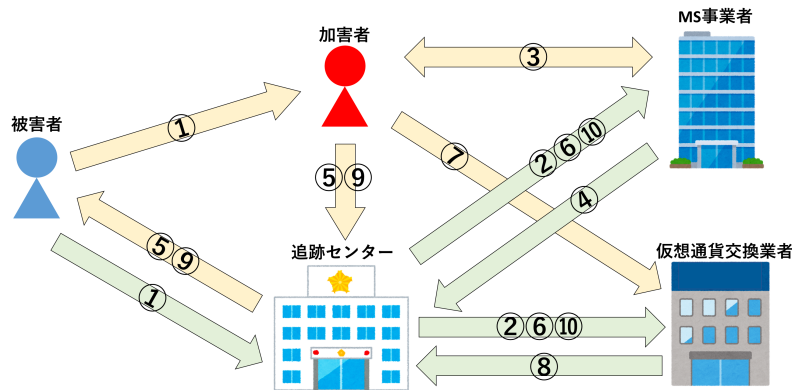


図 3 提案モデル 1 における追跡の流れ

する。また、追跡センターから通達があったアドレスであることを確認し追跡センターに届け出を行う。

- (5) 追跡センターは犯罪者を検挙し、身代金を押収する。追跡センターは身代金を被害者に返す。
- (6) 検挙できなかった場合、追跡センターは監視するアドレスを、犯罪者がミキシングされたビットコインを受け取ったアドレスに変更し追跡を続行する。また、そのアドレスを MS 事業者および仮想通貨交換業者に通達する。
- (7) 犯罪者は仮想通貨交換業者にてミキシングされたビットコインを法定通貨に換えようとする。
- (8) 仮想通貨交換業者は本人確認を取引記録を保持する。また、追跡センターから通達があったアドレスであることを確認し追跡センターに届け出を行う。
- (9) 追跡センターは犯罪者を検挙し、身代金を押収する。追跡センターは身代金を被害者に返す。
- (10) 検挙できなかった場合、追跡センターは追跡を続行し、必要に応じて MS 事業者および仮想通貨交換業者に通達を行う。

追跡センターが身代金の入ったアドレスの情報を集約し、仮想通貨を扱う業者に通達を行い検挙に繋げることが重要である。上記の説明は、犯罪者が身代金をミキシングし法定通貨に換えることを前提に記述した。犯罪者が複数回のミキシングを行うなど他の行動を取った場合でも、追跡センターが MS 事業者もしくは仮想通貨交換業者から通報を受け検挙する、もしくは MS 事業者からログの提供を受け新たなアドレスを監視対象にするという基本は変わらない。

特定事業者が、前述のステップで述べたような、疑わしい取引の届け出を行う義務は犯収法第八条第 1 項に定義されている。疑わしい取引かどうかおよび、届出を行うかどうかの判断基準は、「取引時確認の結果、当該取引の態様その他の事情及び第三条第三項に規定する犯罪収益移転危険度調査書の内容を勘案し、かつ、主務省令で定める項目に従って当該取引に疑わしい点があるかどうかを確認する方法その他の主務省令で定める方法により行わなければならない

ない」(同法第八条第 2 項)となっている。主務省令で定める項目および方法は、犯収法施行規則第二十六条および第二十七条に定義されている。よって、追跡センターからの通達があったアドレスとの取引を確実に届け出てもらうためには、同法施行規則にその旨を定義する必要があると考えられる。

5.3 提案モデル 2

当モデルでは、4 章で述べた、MS 事業者が記録を保持するという仮定は使用しない。また、提案モデル 1 で述べた、追跡センターを当モデルでも利用する。ただし、当モデルにおける追跡センターの目的は、身代金を手にした者が仮想通貨交換業者で法定通貨もしくは他の仮想通貨へ交換できないようにすることであり、犯罪者の検挙ではない。そのため、追跡センターの構成員には、仮想通貨交換業者および MS 事業者に対して命令を行う権利が必要である。被害者・犯罪者のとる行動は基本的に 5.1 節と同じとし、追跡センターを加えた提案モデルを図 4 に示す。

図 4 において、矢印および番号は図 3 と同じ意味を持つ。以下に追跡の流れを説明する。

- (1) 被害者は身代金を支払うと同時に、ランサムウェアが指定したアドレスを含んだ被害届を追跡センターに提出する。
- (2) 追跡センターは被害届を受理し、当該アドレスの追跡を開始する。同時に、追跡しているアドレス全てのリストを公開し、仮想通貨交換業者にはそれらのアドレスから入金された身代金は、追跡センターに渡すように命じる(仮想通貨交換業者に対して当該アドレスとの取引禁止を命じる)。
- (3) 犯罪者は MS 事業者に身代金のミキシングを依頼する。しかし、MS 事業者は追跡センターが公開したリストの中に、犯罪者のアドレスがあることを知り、身代金のミキシングをせずに犯罪者に返す(詳細は後述)。
- (4) ミキシングされなかったことで、犯罪者にとって身代金を仮想通貨交換業者にて法定通貨に換えると、検挙

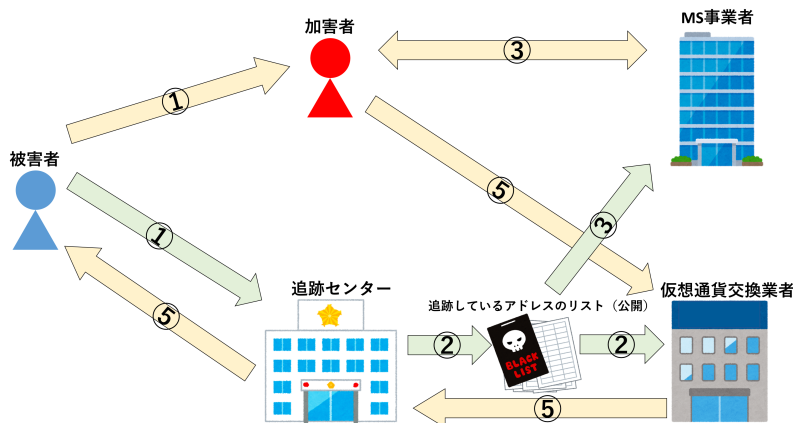


図 4 提案モデル 2 における追跡の流れ

されるリスクは非常に高くなる。よって犯罪者は身代金を法定通貨に換えることはできなくなる。

- (5) 仮に、仮想通貨交換業者は追跡センターから通達のあったアドレスから入金を受けた場合、法定通貨に換えることはせずに受け取ったビットコインを追跡センターに渡す。追跡センターは受けたビットコインを被害者に返す。

ビットコインはミキシングをした場合でも、移動したアドレスの全てを確認することができる。そこで追跡センターは、被害届にあったアドレスに入っている身代金について、ミキシングによって作られたアドレスを含め身代金が送信されたアドレスを全て追跡する。追跡センターは追跡したアドレスを全て公開し、仮想通貨交換業者にそれらのアドレスから入金された身代金は追跡センターに渡すように命じる。このようにすることで、MS事業者も犯罪者から受け取ったビットコインを、仮想通貨交換業者で法定通貨などに換えることができず、利益を享受することができなくなる。つまり、MS事業者にとって身代金の入ったアドレスから受け取ったビットコインを積極的にミキシングする理由はなくなる。よって、MS事業者に身代金のミキシングをさせないようにすることができる。また、MS事業者にログの保持を義務付ける必要はない。

6. おわりに

本論文では、ミキシングを実際に行い、ビットコインの資金移動について分析を行い、ミキシングされたビットコインの追跡困難性を考察した。また、MS事業者に対する法的規制について考察した。最後に、それらを踏まえてミキシングされたビットコインに対する追跡モデルの提案を行った。提案モデル 1 では、法整備を行い、専門捜査機関を設立することで、MS事業者を無くすことなくマネーロンダリングを防止することができる。提案モデル 2 では、専門捜査機関を設立し、追跡対象となっているアドレスのリストに掲載されているアドレスとの取引を拒否するとい

う習慣を浸透させることで、MS事業者を無くすことなくマネーロンダリングを防止することができる。つまり、両モデルにおいてプライバシー保護を目的としてミキシングを使用する人のために、MS事業者を残すことができる。

参考文献

- [1] Satoshi Nakamoto : Bitcoin: A Peer-to-Peer Electronic Cash System, 入手先 (<https://bitcoin.org/bitcoin.pdf>) (参照 2018-01-29).
- [2] 電子政府の総合窓口 e-Gov イーガブ: 犯罪による収益移転防止に関する法律
入手先 (http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=419AC0000000022) (参照 2018-01-29).
- [3] 電子政府の総合窓口 e-Gov イーガブ: 資金決済に関する法律
入手先 (http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=421AC0000000059) (参照 2018-01-29).
- [4] 裁判所: 裁判例情報 (薬事法違反, 銀行法違反被告事件)
入手先 (http://www.courts.go.jp/app/hanrei_jp/detail2?id=50024) (参照 2018-01-29).
- [5] 弁護士ドットコム: 隔地者入手先
(<https://www.bengo4.com/other/1146/1288/d.4161/>) (参照 2018-01-29).
- [6] 電子政府の総合窓口 e-Gov イーガブ: 信託法
入手先 (http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=418AC0000000108) (参照 2018-01-29).
- [7] 一般社団法人 信託協会「信託用語集」入手先
(<http://www.shintaku-kyokai.or.jp/trust/trust04.html>) (参照 2018-01-29).
- [8] 電子政府の総合窓口 e-Gov イーガブ: 信託業法
入手先 (http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=416AC0000000154) (参照 2018-01-29).
- [9] 電子政府の総合窓口 e-Gov イーガブ: 犯罪による収益の移転防止に関する法律施行規則
入手先 (http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=420M60000f5a001) (参照 2018-01-29).