2017 年 12 月 6 日

ビットコインに関連する犯罪の例

創法律事務所
弁護士　斎藤　創

Ⅰ　始めに

ビットコインに関して取引所が関連する犯罪を大きく分けると
①　取引所に対する犯罪
②　取引所のユーザーに対する犯罪
③　取引所ユーザー以外への犯罪で取引所をその後の手段として利用する犯罪
の 3 つが考えられる。

また、
④　①や②に類似の犯罪として個人のウォレットに仮想通貨を保管していた場合のハッキング
もある

それ以外の仮想通貨関係の犯罪としては
⑤　単なる詐欺 - 全く存在もしていない仮想通貨を値上がりすると言って販売する等
⑥　単なる犯罪 - ランサムウェアの身代金として仮想通貨を要求、薬物・ポルノを仮想通貨で販売等
⑦　犯罪か否かは不明だが一部から問題視される取引 - ネットワーキングビジネスでの販売、High Yield Investment Program(HYIP)等と呼ばれる取引
等、様々なものがある。今回のセミナーでは①～③を主として取り上げる。

Ⅱ　取引所に対する犯罪

1　内部犯行と外部犯行

内部犯行
取引所の内部者が自社のビットコイン、又は顧客からの預かり資産であるビットコインを横領する

外部犯行
取引所に外部からハッキングをし、取引所から仮想通貨を盗み出す(外部のアカウントに送付させる)。

2　内部犯行の例

2013年2月 (MtGox事件)
当時世界最大の取引所MTGOXが破綻。当初は外部からのハッキングと報道されていたが、実際には内部犯行であったよう。
→　報道等による。但し、刑事裁判手続中であり、被告は無罪を主張している。また外部に犯人がいる等の報道もされている[1]。

2016年4月
両替所ShapeShiftのホットウォレットから約2,300万円の通貨が流出、この事件では内部の元従業員による犯行であったことが判明？

3　外部犯行の例

外部からの犯行については、取引所は多額のビットコインを保管しており、毎日のようにハッキング攻撃のトライを受けているという状況。これを水際で防いでいる。

筆者の知る限り日本の著名取引所で大きなハッキング被害があった事例はない。
海外事例は例えば下記のような例。このうちThe DAOやBitfinexは著名事例。小規模な事例は多数あるものと思われる。

2016年5月
香港にて運営を行うGatecoinが200万ドル相当のビットコイン、イーサリウムのハッキング被害

2016年6月(The DAO事件)
正確には取引所ではないが、The DAOという仮想通貨を利用したドイツの自律型ファンド(150億円以上を調達し、非常に期待されていたプロジェクト)が、2016年6月にイーサリウムの脆弱性を付かれて3分の1のコインを盗まれ、その後、破綻

2016年8月(Bitfinex事件)
Bitfinexという当時ドル取引高世界No1の香港の取引所が2016年8月に119,756BTC(約6347万ドル、約71億円)のハッキングを受けた。
なお、被害部分を額に比べて相当程度の資本や収益があったこと等から、債権者の同意を得て被害相当部分に関して独自トークンを渡す、Equity化する等で営業を継続。その後の収益により現在は損害部分は回復したよう。

2017年4月
韓国のビットコイン取「YAPIZON」がハッキング被害。ユーザーの資産の37%にあたる3816.2028ビットコイン(約500万ドル、約5.6億円)を盗み出された。上記Bitfinexの例と同様のトークンを出す方法で考えているが、Bitfinexとの金融ステータスとの違いから議論

1　http://btcnews.jp/kc27s5ye11945/

が大きいよう[2]。

2017 年 7 月

韓国最大の取引所が「Bithumb」がハッキングされ、多数のユーザーアカウントが漏洩し、100 万ドル(約 1 億 1000 万円)分以上の仮想通貨が盗み出された。

2017 年 11 月 19 日

USD Tether という USD にペッグする仮想通貨 3100 万ドル分がその発行者であるテザー社の金庫ウォレットから不正に外部に送付される　→　発行者がいる案件であり、ハードフォークで対応し大きな問題はなかったよう。

4　対策・防止策

ハッキングは取引所として会社破綻に繋がりうる重要な事象である

通常の取引所であれば、これらに対しては細心の注意を払って対応する必要がある

内部犯行対策
権限の分配、信頼できる者の採用、システム設計(ログの保持、コールドウォレットの利用など)、帳簿作成、バグ対策、内部監査、外部監査、不正サイトへのアクセス及び不正行為検出・記録・アラート通知体制

外部犯行対策
システム設計(セキュリティー対策、コールドウォレットの利用等)、バグ対策(常に最新の情報の入手、対応等)、帳簿作成(ずれるとすぐ判る)、定期的なチェック、システム監査など

＊参考(権限の分配)
例えば仮想通貨法では、業態によるものの取締役会の設置、営業と管理の分離、コンプライアンスオフィサーの設置、内部監査室の設置、外部監査(会計監査、分別管理監査)などで二重三重の権限分離を要求

＊参考(コールドウォレット)
インターネット等のネット環境に接続していないウォレット。ネットに接続していないため外部からハッキングされる可能性が極めて低い。
多くの取引所では例えば顧客預かり資産の 80～90％等をコールドウォレットに保管

コールドウォレットからホットウォレット(ネットに繋がったウォレット)への移動の回数は可能な限り低くする(運用によるが月に 1 度～年に 1 度など限定的)

2　https://www.cryptocoinsnews.com/south-korea-yapizon-bitcoin-exchange-hack/

Ⅲ　取引所ユーザーに対する犯罪

1　ユーザーのパスワード等の盗難

取引所ユーザーのアカウントがハッキング等され、無権限の者が当該ユーザーに代わって取引所にログインし、コインを送付する等の事案がある

会社の内部犯行
自社の内部者が会社のアカウントとパスワードを利用して、会社の PC で取引所からコインを送付

外部犯行(外部からのハッキング)
総当り攻撃、ウィルス、キーロガー、メールのハッキング、フィッシングサイト等々

(2)　ユーザー側の対応策

ネットを利用するための基本
① ウィルス対策ソフト、セキュリティー対策ソフトを入れる
② 最新の OS を利用する
③ 不審なファイルを開かない
④ 不審なリンクを踏まない
⑤ アカウント番号やパスワードを他者に教えない
⑥ パスワードを他のサイトと共用しない
⑦ PC やスマホを放置したり失くしたりしない、パスワードをかける
⑧ 定期的にログイン記録を確認し、自分以外のアクセスがないかをチェックする

金融取引の場合に重要
⑨ 2 段階認証/2 要素認証を設定する

よりセキュアな方法
⑩ できるだけクリーンな PC やスマートフォンで取引を行う
　→ 本当に多額の金額の取引を行う場合、専用の完全にクリーンな PC を利用し、かつ、当該 PC にアクセスできる者を限定する等が望ましい

2　取引所側の対応策の例

ユーザーに対するハッキングは取引所では対応できない部分も多いが、例えば下記のような対策をとって、よりセキュアにする例がある

① パスワードの強度が低い場合(例えば英語の大文字小文字、数字、記号の全てを必須とし、文字数を 8 文字以上にする等)には受け付けない
② パスワードが推測されやすい単語を含んでいる場合には受け付けない
③ パスワードの試行回数を限定し、一定回数以上の誤りについてはロック(総当り攻撃対策)
④ 2 段階認証/2 要素認証を強制する/強く推奨する
⑤ 通常不使用の IP アドレスからのログインを弾く、ユーザーに通知して注意を促す等
⑥ ユーザーにユーザーが対応すべきセキュリティーを教育

⑦ サイバーセキュリティ保険の導入
⑧ パスワード保存の暗号化(ハッシュ化等、内部の者でもわからない状態に暗号化
→ 取引所に対してハッキングしその後ユーザー側をハッキングするケースの防止)

3 問題点

セキュリティーは、利便性と安全性のバランスを取る必要がある。

① 例としてパスワードは難しくすれば難しくするほどセキュリティーは安全になる。複雑なパスワードの場合、ユーザーが他サイトで使用している覚えやすいパスワードは弾かれることになり流用も防止しやすくなる
他方、ユーザー自身が覚えられないパスワードしか設定できず利便性が低下し、紙に書いておく等で別途のセキュリティーリスクが発生することがある
② ユーザーがパスワードを忘れた場合、再発行の手続きを行うが、パスワードの再発行手続きが容易であればパスワードのハッキングリスクが増す。厳格化した場合、再発行が著しく面倒になる
③ 2段階認証/2要素認証の方法として例えばメール、SMS、ボイス、ワンタイムパスワード等があるが、メールがハッキングされている場合には認証の効果が薄れる。SMS、ボイス認証についてもハッキング事例が報告されているよう。
④ ユーザーのPCにトロイの木馬、フィッシング、キーロガーなどを入れられてしまうと対応は極めて困難。取引専用のクリーンなPCの利用等を求めることは現実的ではない
⑤ 保険についてはコストや引受手の有無の問題。またユーザーがハッキング被害にあった、と虚偽の申告をしてくる可能性がある

→ いずれにせよユーザーと取引所の両方の協力、不断の努力が必要

＊(参考)2段階認証と2要素認証[3]

認証要素	認証の具体的な方法
利用者が知っていること (Something You Know：SYK)	固定パスワードや暗証番号、認証用IDなど、利用者が知っている情報を認証要素として活用
利用者が持っているもの (Something You Have：SYH)	ハードウェアトークン(小さな認証用器具)、ソフトウェアトークン(スマートフォンなどにインストールする認証用ソフト)、スマートカード(クレジットカードタイプの認証カードなど)、電子証明書など、利用者が持っているものを認証要素として活用
利用者の身体的特徴(Something You Are：SYA)	指紋、静脈、網膜、音声など、利用者個人の特徴を認証要素として活用

このSYK、SYH、SYAのうち別の2つ以上を使う認証を2要素認証
別の要素かは意識せず、例えばパスワード＋パスワードなどでも良いのが2段階認証

現在、ヨーロッパでは(一定の金額以下の決済や高速道路料金等の決済を除き)Payment Serviceに関しては2要素認証(Knowledge、Possession、Inheritance)を

[3] 参考 http://mikado.hatenablog.jp/entry/2014/09/02/211916、
http://www.terilogy.com/product/vasco/2fa.html

要求することが検討されている。
“Regulatory Technical Standards on strong customer authentication and secure communication under PSD2[4]”

とはいえヨーロッパでも現時点で必須な訳ではなく、また日本でも現在は 2 要素認証が必須という訳ではない[5]。

[4] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

[5] 本年 4 月施行の仮想通貨法ガイドラインでは「インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。・可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式、・取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証、・ログインパスワードとは別の取引用パスワードの採用 等」と規定(II-2-3-1-2(5))。
→ 必ずしも 2 段階認証でも 2 要素認証でもない場合があるように見受けられる。

Ⅳ　取引所ユーザーでない者に対する犯罪

1　銀行口座ハッキング事案

① 取引所ユーザーではない者Aのインターネットバンキングをハッキング
② ビットコイン取引所のB名義の口座に金銭を送付
③ B名義の口座でビットコインを購入
④ B名義口座からビットコインを引き出し

2　コンビニ振込詐欺等の事案

① 取引所にはペイジー入金システムがあるものがあり、例えば入金額と、ペイジーの番号が出され、それにコンビニ等で振り込むことができる
② 取引所の名義人であるBは、ペイジー入金をする旨を取引所に連絡
③ 犯人Cが取引所ユーザーではないAに対して振込詐欺。上記②のペイジー入金の番号を教える
④ Aはコンビニで入金
⑤ Bが入金されたお金でビットコインを購入、引き出し
(現在は、例えば振り込み金額について1週間の引き出しを禁止するなどにより基本的には解決されていると理解)

3　問題点

上記のBが本人であれば通常は逮捕が容易。他方、
(a) Bが報酬を貰った出し子として行動するが、実際の犯人は他のC
(b) Bが生活困窮者等で本人確認書類をCに売却、又はCに騙されて本人確認書類等を渡しているケース(融資をします、融資のためにこの情報が必要です等)
(c) Bが外国人等で帰国時にCに口座を売却するケース
など、Cを突き止めることは必ずしも容易ではない

<u>銀行口座ハッキング</u>
インターネットバンキングのハッキングは何故起きるのか？
銀行によっては例えば振込用カードでの番号入力やワンタイムパスワード等での2段階認証/2要素認証をしていると思われる。そのようなものがない事例？対応していたがウィルス、フィッシング等で破られた事例？

取引所としては振込人Aの名義と口座Bの名義が異なれば入金を拒否するが、そもそも日本の銀行送金システムで第三者名義での送金ができる
→ 海外ではできないケースが多いと聞いている。日本の送金システムの便利な点でもあり、他方、セキュリティー上の欠点でもあると思われる

<u>取引所の疑わしい取引確認について</u>
取引所の方でSuspicious Activityを発見し、自主的に取引をストップさせることはしばしばある
しかしながら、業者によってもそのレベル感は異なると思われ、更にブラッシュアップが必要

Ⅴ　ウォレットに対するハッキング

個人保有のウォレットがセキュリティーリスクや脆弱性をつかれハッキングを受けるケース

2017年6月 複数の仮想通貨を管理できるウォレットJaxxが40万ドル分盗まれる http://cryptocurrencymagazine.com/users-report-losing-400000-due-to-jaxx-wallet-vulnerability 2017年7月20日 イーサリアムクライアントのParityが提供するマルチシグウォレットにてセキュリティバグがありウォレットがハッキングにあい、約34億円が盗難にあったケース https://ethereum-japan.net/ethereum/parity-maltisig-vulnerability-hacked-150keth/

Ⅵ　その他の最近の犯罪事例

(1) 最近はICO(Initial Coin Offering)という資金調達のために新しいコインやトークンを発行し、その対価をBitcoinやEtherで受け取る事例が増えている。犯罪者が虚偽の受取アドレスをTelegramサイト等で掲示して、そこにBitcoin等を送付させる例

(2) BLOGなどにマイニングのソフトウェアを埋め込み、ブログにアクセスした人のPCを使用し、勝手にマイニングを行なう

Ⅶ　犯罪等で盗まれたビットコインの行き先/犯人の調査方法

1　前提

ブロックチェーン上の取引記録

① ビットコインは全取引がブロックチェーン上に記録される
② 但し、ブロックチェーン上には32桁の英数字のアドレスとアドレスに関する取引(に対応したデータ)で記載されるのみ。秘密鍵を管理する者の名前や住所等のデータが載っている訳では勿論ない
③ アドレス間のコインの移動のチェックは誰でもできる。ツールも例えばChainFlyer[6]などが公開されている。但し、転々と移動をされた場合、チェックは労力を要する

本邦取引所の本人確認

④ 本邦取引所は現在、犯収法に従い、アカウント開設者の名称、住所、生年月日等の本人確認書類(免許証等)での確認、申告による取引目的、職業等の確認を行い、かつ、転送不要郵便等で住所の実在を確認している。かつ、犯収法に従い、疑わしい取引のチェックなどを行っている
⑤ 本人確認については3月以前は自主規制で、例えば免許証によるチェック+IDセ

6 https://chainflyer.bitflyer.jp/。なお、海外のブロックチェーン企業が犯罪捜査等を目的のツールを販売している例(Chain Analysis、https://www.chainalysis.com/)も各種あると聞いている。

ルフィーによるチェック
⑥ 潜りの取引所(規制を守る気のない取引所等)の中には本人確認をしていない取引所があるかもしれない。10 月以降、厳しい指導が必要となる

海外の取引所の本人確認
⑦ 海外の取引所が本人確認/疑わしい取引をチェックしているかは各国の法規制等による。米国では FinCEN の要求により厳しい本人確認/疑わしい取引のチェックをしているよう
⑧ いずれにせよ各国の主要取引所は何らかの形で本人確認を行っていると理解
⑨ 但し、全ての国、取引所が本人確認をしているかは不明
⑩ FATF は加盟各国に取引所についての免許制又は登録制、本人確認義務を導入することを勧告している。全世界的に本人確認は必須化していくと思われる

2 調査

上記のように、ビットコインのブロックチェーン上の移動は全て記録され、転々と移動された場合に調査に労力は必要なものの、理論的には全て調査可能

問題は、そのアドレスと持ち主をどう紐付けるか

日本国内の取引所であれば捜査事項照会を送付すれば、取引所としては返答可能な筈
→ アドレス、そのアドレスの持ち主、そのアドレスとの間で●月●日から●月●日に取引があった内容等)
→ 素早いご返答のために、各取引所と警察で取引所に聞く捜査事項照会書の様式を共有化している最中

海外の取引所でも、各国ごとの捜査協力で情報を得られる(と聞いている)

将来的にビットコインがビットコインのまま使用されるようになると取引所の本人確認のみでは不足になる可能性があるが、少なくとも現在のところビットコインをビットコインのまま使用するニーズは少ない
最終的には換金をする以上、どこかの取引所を使う必要があることが通常

→ 調査方法等は警察等関係者と議論させて頂ければ我々としても可能な限り協力したい

以 上